

LINKSYS®

A Division of Cisco Systems, Inc.



Dual-Band
5GHz/2.4GHz
802.11a / 802.11g

Dual-Band
Wireless-N

Gigabit Router with
Storage Link

User Guide



Model No. **WRT600N**



Copyright and Trademarks

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

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

How to Use This User Guide

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



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



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



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

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

word: definition.

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

Figure 0-1: Sample Figure Description

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

Table of Contents

Chapter 1: Introduction	1
Welcome	1
What's in this User Guide?	2
Chapter 2: Planning Your Wireless Network	4
Network Topology	4
Ad-Hoc versus Infrastructure Mode	4
Network Layout	5
Chapter 3: Getting to Know the Wireless-N Gigabit Router with Storage Link	6
The Back Panel	6
The Front Panel	7
The Top Panel	7
Chapter 4: Connecting the Wireless-N Gigabit Router with Storage Link	8
Hardware Installation	8
Chapter 5: Configuring the Wireless-N Gigabit Router with Storage Link	9
Overview	9
How to Access the Web-based Utility	11
The Setup Tab - Basic Setup	11
The Setup Tab - DDNS	17
The Setup Tab - MAC Address Clone	19
The Setup Tab - Advanced Routing	20
The Wireless Tab - Basic Wireless Settings	22
The Wireless Tab - Wireless Security	24
The Wireless Tab - Wireless MAC Filter	27
The Wireless Tab - Advanced Wireless Settings	28
The Security Tab - Firewall	30
The Security Tab - VPN Passthrough	31
The Storage Tab - Disk	32
The Storage Tab - Media Server	33
The Storage Tab - FTP Server	34
The Storage Tab - Administration	36
The Access Restrictions Tab - Internet Access Policy	38
The Applications & Gaming Tab - Single Port Forwarding	40

The Applications & Gaming Tab - Port Range Forwarding	41
The Applications & Gaming Tab - Port Range Triggering	42
The Applications & Gaming Tab - DMZ	43
The Applications and Gaming Tab - QoS	44
The Administration Tab - Management	47
The Administration Tab - Log	49
The Administration Tab - Diagnostics	50
The Administration Tab - Factory Defaults	51
The Administration Tab - Firmware Upgrade	52
The Status Tab - Router	53
The Status Tab - Local Network	54
The Status Tab - Wireless	55
Appendix A: Troubleshooting	56
Common Problems and Solutions	56
Frequently Asked Questions	64
Appendix B: Wireless Security	70
Security Precautions	70
Security Threats Facing Wireless Networks	70
Appendix C: Upgrading Firmware	73
Appendix D: Windows Help	74
Appendix E: Finding the MAC Address and IP Address for your Ethernet Adapter	75
Windows 98SE or Me Instructions	75
Windows 2000 or XP Instructions	76
For the Router's Web-based Utility	76
Appendix F: Glossary	77
Appendix G: Specifications	82
Appendix H: Warranty Information	84
Appendix I: Regulatory Information	85
Appendix J: Contact Information	91

List of Figures

Figure 3-1: The Router's Back Panel	6
Figure 3-2: The Router's Front Panel	7
Figure 3-3: The Router's Top Panel	7
Figure 4-1: Connect the USB cable	8
Figure 4-2: Connect the internet	8
Figure 4-3: Connect the ethernet	8
Figure 4-4: Connect the power	8
Figure 5-1: Router Login	11
Figure 5-2: Setup Tab - Basic Setup (Automatic Configuration - DHCP)	11
Figure 5-3: Static IP	12
Figure 5-4: PPPoE	12
Figure 5-5: PPTP	13
Figure 5-6: Telstra Cable	14
Figure 5-7: L2TP	14
Figure 5-8: DHCP Reservation	16
Figure 5-9: Setup Tab - DynDNS.org	17
Figure 5-10: Setup Tab - TZO.com	18
Figure 5-11: Setup Tab - MAC Clone	19
Figure 5-12: Setup Tab - Advanced Routing	20
Figure 5-13: Routing Table	21
Figure 5-14: Wireless Tab - Basic Wireless Settings	22
Figure 5-15: Wireless Tab - Wireless Security (WPA-Personal)	24
Figure 5-16: Wireless Security - WPA2-Personal	24
Figure 5-17: Wireless Security - WPA-Enterprise	25
Figure 5-18: Wireless Security - WPA2-Enterprise	25
Figure 5-19: Wireless Security - RADIUS	26
Figure 5-20: Wireless Security - WEP	26
Figure 5-21: Wireless Tab - Wireless MAC Filter	27
Figure 5-22: Wireless Client List	27
Figure 5-23: Wireless Tab - Advanced Wireless Settings	28
Figure 5-24: Security Tab - Firewall	30

Figure 5-25: VPN Passthrough	31
Figure 5-26: Storage Tab - Disk	32
Figure 5-27: Storage Tab - Shared Folder	32
Figure 5-28: Storage Tab - Media Server	33
Figure 5-29: Media Folder	33
Figure 5-30: Storage Tab - FTP Server	34
Figure 5-31: FTP Folder	34
Figure 5-32: Storage Tab - Administration	36
Figure 5-33: User Account	36
Figure 5-34: Group Account	37
Figure 5-35: Access Restrictions Tab - Internet Access Policy	38
Figure 5-36: Summary	38
Figure 5-37: List of PCs	39
Figure 5-38: Applications & Gaming Tab - Single Port Forwarding	40
Figure 5-39: Applications & Gaming Tab - Port Range Forwarding	41
Figure 5-40: Applications & Gaming Tab - Port Range Triggering	42
Figure 5-41: Applications & Gaming Tab - DMZ	43
Figure 5-42: DHCP Client Table	43
Figure 5-43: Applications & Gaming Tab - QoS (Applications)	44
Figure 5-44: QoS - Applications (Add a New Application)	45
Figure 5-45: QoS - Online Games	45
Figure 5-46: QoS - MAC Address	45
Figure 5-47: QoS - Ethernet	45
Figure 5-48: QoS - Voice Device	46
Figure 5-49: Administration Tab - Management	47
Figure 5-50: Administration Tab - Log	49
Figure 5-51: View Log	49
Figure 5-52: Administration Tab - Diagnostics	50
Figure 5-53: Ping Test	50
Figure 5-54: Traceroute Test	50
Figure 5-55: Administration Tab - Factory Defaults	51
Figure 5-56: Administration Tab - Firmware Upgrade	52
Figure 5-57: Status Tab - Router	53
Figure 5-58: Status Tab - Local Network	54

Figure 5-59: DHCP Client Table	54
Figure 5-60: Status Tab - Wireless Network	55
Figure C-1: Firmware Upgrade	73
Figure E-1: IP Configuration Screen	75
Figure E-2: MAC Address/Adapter Address	75
Figure E-3: MAC Address/Physical Address	75
Figure E-4: Wireless MAC Filter	76
Figure E-5: MAC Address Cloning	76

Chapter 1: Introduction

Welcome

The Dual-Band Wireless-N Gigabit Router with Storage Link is really four devices in one box. First, there's the Wireless Access Point, which lets you connect to the network without wires. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices together. The Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

We've also included a Storage Link that lets you easily add gigabytes of storage space onto your network using readily available USB 2.0 hard drives -- or plug in a USB flash disk for a convenient way to access your portable data files. The built-in Media Server streams music, video, and photos from the attached storage device to any UPnP compatible media adapter. And you can get to your files from anywhere in the world through the Internet.

The Access Point built into the Router uses the very latest wireless networking technology, Wireless-N (draft 802.11n). By overlaying the signals of multiple radios, Wireless-N's "Multiple In, Multiple Out" (MIMO) technology multiplies the effective 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 4 times farther than standard Wireless-G.

With Wireless-N, the farther away you are, the more speed advantage you get. It also works great with standard Wireless-A, Wireless-G and -B equipment, but when both ends of the wireless link are Wireless-N, the router can increase the throughput even more by using twice as much radio band, yielding speeds up to 12 times as fast as standard Wireless-G. But unlike other speed-enhanced technologies, Wireless-N can dynamically enable this double-speed mode for Wireless-N devices, while still connecting to other wireless devices at their respective fastest speeds. In congested areas, the "good neighbor" mode ensures that the Router checks for other wireless devices in the area before gobbling up the radio band.

To help protect your data and privacy, the Router can encode all wireless transmissions with industrial-strength 256-bit encryption. It can serve as your network's DHCP Server, has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks, and supports VPN pass-through. Configuration is a snap with the web browser-based configuration utility.

The incredible speed of Wireless-N makes it ideal for media-centric applications like streaming video, gaming, and Voice over IP telephony, and gives you plenty of headroom to run multiple media-intense data streams through the network at the same time, with no degradation in performance. With the Linksys Wireless-N Gigabit Router with Storage Link at the center of your home or office network, you can easily add storage, share a high-speed Internet connection, files, printers and multi-player games, and run media-intensive applications at faster than 10/100 wired network speeds, without the hassle of stringing wires!

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

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

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

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

What's in this User Guide?

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

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

Dual-Band Wireless-N Gigabit Router with Storage Link

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

Chapter 2: Planning Your Wireless Network

Network Topology

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

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

Ad-Hoc versus Infrastructure Mode

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

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

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

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

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

Network Layout

The Wireless-N Gigabit Router with Storage Link has been specifically designed for use with your Wireless-N, Wireless-G, and Wireless-B products. It will work with notebook adapters for your laptop computers, PCI adapters for your desktop computers, and USB adapters for your USB connectivity needs. The Router can also communicate with other devices, such as wireless print servers and bridges.

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

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

Chapter 3: Getting to Know the Wireless-N Gigabit Router with Storage Link

The Back Panel

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

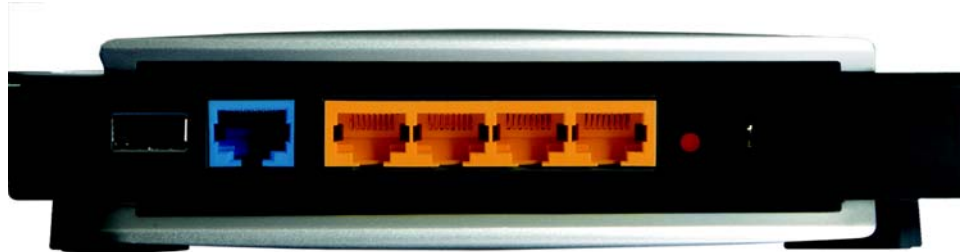


Figure 3-1: The Router's Back Panel

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



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

The Front Panel

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



Figure 3-2: The Router's Front Panel

- POWER** Green. The **POWER** LED lights up and will stay on while the Router is powered on.
- ETHERNET 1, 2, 3, 4** Green, Orange. These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve three purposes: (1) The green LED lights up when the Router is connected to a device through the corresponding port at 10/100, (2) The orange LED lights up when you are connected at 1,000 Mbps (1 Gigabit), and (3) If the LED is flashing, then the Router is sending or receiving data over that port.
- INTERNET** Green. The **INTERNET** LED lights up when there is a connection through the Internet port.
- WIRELESS** Green. The **WIRELESS** LED lights up when there is a wireless connection. If the LED is flashing, the Router is sending or receiving data over the wireless network.
- USB** Green. The **USB** LED lights up when a USB drive is connected through the USB port. If the LED is flashing, the Router is actively sending or receiving data over the USB connection.
- SECURITY** Green. The **SECURITY** LED indicates when wireless security is enabled.

The Top Panel

The Router has a button reserved for a future function.

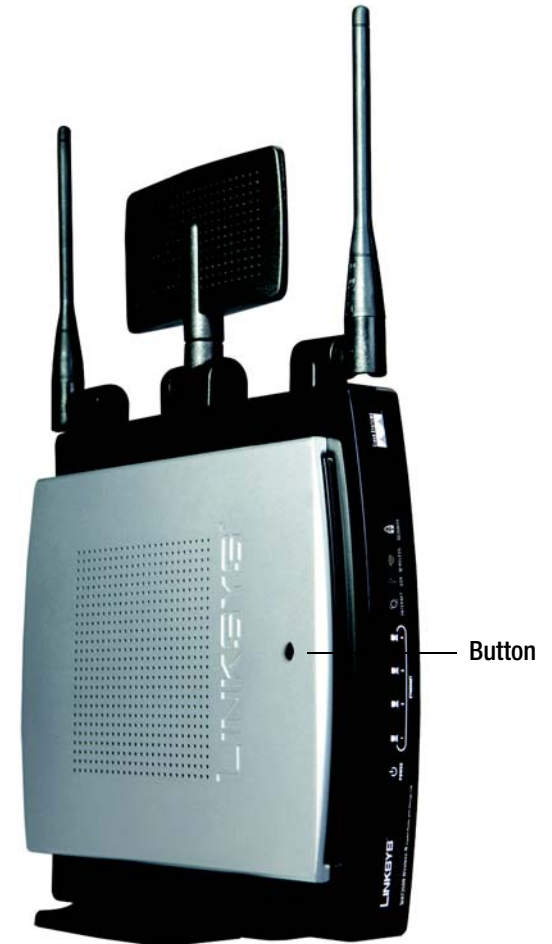


Figure 3-3: The Router's Top Panel

Chapter 4: Connecting the Wireless-N Gigabit Router with Storage Link

Hardware Installation

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

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

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

Proceed to "Chapter 5: Configuring the Wireless-N Gigabit Router with Storage Link".



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



Figure 4-1: Connect the USB cable



Figure 4-2: Connect the internet



Figure 4-3: Connect the ethernet



Figure 4-4: Connect the power

Chapter 5: Configuring the Wireless-N Gigabit Router with Storage Link

Overview

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

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

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

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

Setup

- **Basic Setup.** Enter the Internet connection and network settings on this screen.
- **DDNS.** Enable the Router's Dynamic Domain Name System (DDNS) feature on this screen.
- **MAC Address Clone.** If you need to clone a MAC address onto the Router, use this screen.
- **Advanced Routing.** Use this screen to alter dynamic and static routing configurations.

Wireless

- **Basic Wireless Settings.** Enter the basic settings for your wireless network on this screen.
- **Wireless Security.** Enable and configure the security settings for your wireless network.
- **Wireless MAC Filter.** Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.
- **Advanced Wireless Settings.** For advanced users, you can alter data transmission settings on this screen.

Security

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

Storage

- **Disk.** Describes the disk currently attached to the Router.
- **Media Server.** Scans for contents using a built-in media server.
- **FTP Server.** Creates an FTP server that can be accessed through the Internet.
- **Administration.** Manages the user and groups of users that can access the shares.

Access Restrictions

Internet Access Policy. Create policies to control Internet access for your local network users.

Applications & Gaming

- **Single Port Forwarding.** This allows you to do port mapping and forwarding for a single service port.
- **Port Range Forwarding.** Set up public services or other specialized Internet applications on your network.
- **Port Range Triggering.** Configure the Router to watch outgoing data for specific port numbers.

Dual-Band Wireless-N Gigabit Router with Storage Link

- **DMZ.** Click this tab to allow one local user to be exposed to the Internet for use of special-purpose services.
- **QoS.** Quality of Service (QoS) ensures better service to high-priority types of network traffic.

Administration

- **Management.** On this screen, alter the Router's password, access privileges, and UPnP settings. You can also use this screen to back up and restore the Router's configuration file.
- **Log.** If you want to view or save activity logs, click this tab.
- **Diagnostics.** If you want to run a ping or traceroute test, then use this screen.
- **Factory Defaults.** If you want to restore the Router's factory defaults, then use this screen.
- **Firmware Upgrade.** Click this tab if you want to upgrade the Router's firmware.

Status

- **Router.** This screen provides status information about the Router.
- **Local Network.** This provides status information about the local network.
- **Wireless Network.** This provides status information about the wireless network.

How to Access the Web-based Utility

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

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

Make the necessary changes through the Utility. When you have finished making changes to a screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For information on a tab, click **Help**.

The Setup Tab - Basic Setup

The *Basic Setup* screen is the first screen you see when you access the Web-based Utility.



Figure 5-1: Router Login

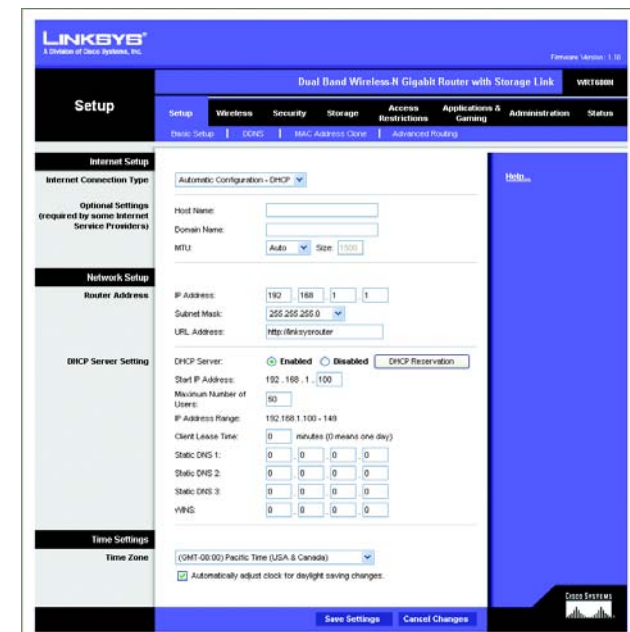


Figure 5-2: Setup Tab - Basic Setup
(Automatic Configuration - DHCP)



NOTE: Some of these connection types may not be available in your area.

Internet Setup

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

Internet Connection Type

The Router supports six connection types: Automatic Configuration - DHCP, Static IP, PPPoE, PPTP, Telstra Cable, and L2TP. Each *Basic Setup* screen and available features will differ depending on what kind of connection type you select.

Automatic Configuration - DHCP

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

Static IP

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

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

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

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

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 for end-users. If you use a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable it.

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



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

The screenshot shows the 'Internet Setup' window with 'Internet Connection Type' set to 'Static IP'. The fields are as follows:

Internet IP Address:	0	.	0	.	0	.	0
Subnet Mask:	0	.	0	.	0	.	0
Default Gateway:	0	.	0	.	0	.	0
DNS 1:	0	.	0	.	0	.	0
DNS 2 (Optional):	0	.	0	.	0	.	0
DNS 3 (Optional):	0	.	0	.	0	.	0

Figure 5-3: Static IP

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

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

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

The screenshot shows the 'Internet Setup' window with 'Internet Connection Type' set to 'PPPoE'. The fields are as follows:

Username:	
Password:	
Service Name (Optional):	
<input type="radio"/> Connect on Demand: Max Idle Time	15 Minutes.
<input checked="" type="radio"/> Keep Alive: Redial Period	30 Seconds.

Figure 5-4: PPPoE

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

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

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

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

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.

PPTP

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

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

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

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

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

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

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

The screenshot shows the 'Internet Setup' page with the 'Internet Connection Type' dropdown set to 'PPTP'. The configuration fields are as follows:

- Server IP Address: 0 . 0 . 0 . 0
- Subnet Mask: 0 . 0 . 0 . 0
- Default Gateway: 0 . 0 . 0 . 0
- Username: [Empty field]
- Password: [Empty field]
- Connect on Demand: Max Idle Time 15 Minutes.
- Keep Alive: Redial Period 30 Seconds.

Figure 5-5: PPTP

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.

Telstra Cable

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

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

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

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries. Check with your ISP for the necessary setup information.

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

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

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

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

Click the **Save Settings** button. Then click the **Status** tab, and click the **Connect** button.

Optional Settings

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



Figure 5-6: Telstra Cable

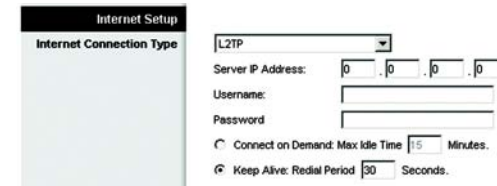


Figure 5-7: L2TP

packet: a unit of data sent over a network.

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

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

Network Setup

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

Router IP

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

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

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

DHCP Server Setting

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

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

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

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

Client Lease Time. The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

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

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

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

DHCP Reservation. Click the **DHCP Reservation** button if you want to assign a fixed local IP address to a MAC address. You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address. Click the **Select** checkbox to reserve a client's IP address. Then click the **Add Clients** button.

If you want to manually assign an IP address, enter the client's name in the *Enter Client Name* field. Enter the IP address you want it to have in the *Assign IP Address* field. Enter its MAC Address in the *To This MAC Address* field. Click the **Add** button.

A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click the **Remove** button.

When you have finished your changes, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel your changes. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

Time Setting

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

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

Figure 5-8: DHCP Reservation



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

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 one of two DDNS service providers, DynDNS.org or TZO.com. If you do not want to use this feature, keep the default setting, **Disable**.

DDNS

DDNS Service

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

DynDNS.org

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

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

Mail Exchange (Optional). Enter the address of your mail exchange server, so e-mails to your DynDNS address go to your mail server.

Backup MX. This feature allows the mail exchange server to be a backup. To enable this feature, keep the default, **Enabled**. To disable the feature, select **Disabled**. If you are not sure which setting to select, keep the default, **Enabled**.

Wildcard. This setting enables or disables wildcards for your host. For example, if your DDNS address is *myplace.dyndns.org* and you enable wildcards, then *x.myplace.dyndns.org* will work as well (*x* is the wildcard). To enable wildcards, keep the default, **Enabled**. To disable wildcards, select **Disabled**. If you are not sure which setting to select, keep the default, **Enabled**.

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

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

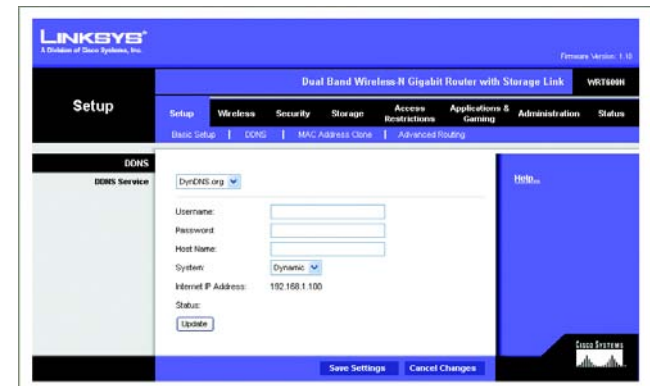


Figure 5-9: Setup Tab - DynDDNS.org

Dual-Band Wireless-N Gigabit Router with Storage Link

TZO.com

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

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

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

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

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

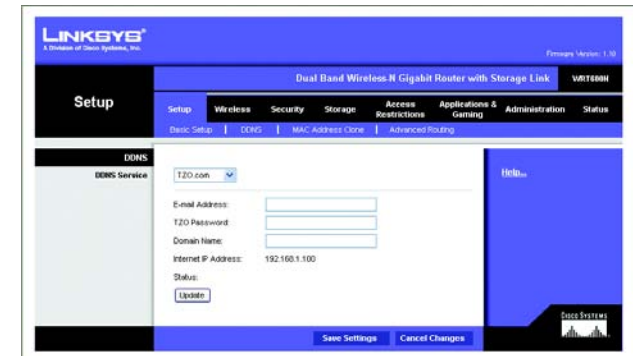


Figure 5-10: Setup Tab - TZO.com

The Setup Tab - MAC Address Clone

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

MAC Address Clone

To use MAC address cloning, select **Enabled**. Otherwise, keep the default, **Disabled**.

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

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

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

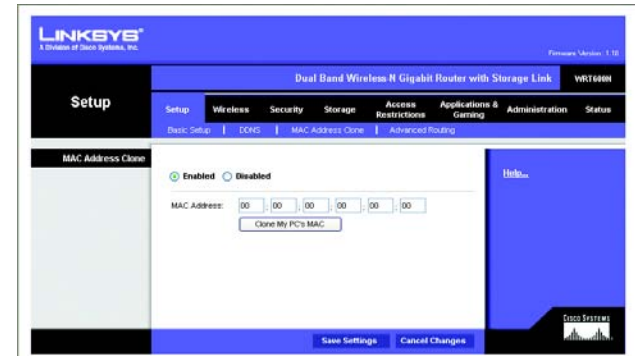


Figure 5-11: Setup Tab - MAC Clone

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

The Setup Tab - Advanced Routing

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

Advanced Routing

NAT

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

Dynamic Routing

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

Static Routing

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

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

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

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

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

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

Delete This Entry. To delete a route, select its number from the drop-down menu, and click this button.



Figure 5-12: Setup Tab - Advanced Routing

Dual-Band Wireless-N Gigabit Router with Storage Link

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

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



Destination LAN IP	Subnet Mask	Gateway	Interface
10.10.10.100	255.255.255.0	10.10.10.1	Internet (WAN)
192.168.1.100	255.255.255.0	192.168.1.1	LAN & Wireless

Figure 5-13: Routing Table

The Wireless Tab - Basic Wireless Settings

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

5GHz Wireless Settings

Network Mode. If your network devices have multiple modes, keep the default setting, **Mixed**. If you have Wireless-A only, select **Wireless-A**. If you have Wireless-N only, select **Wireless-N**. If you do not have any wireless devices in your network, select **Disabled**.

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.

Radio Band. For best performance in a network using Wireless-A and Wireless-N (5GHz) devices, keep the default, Auto, and the Wide Channel and Standard Channel will be selected automatically.

Wide Channel. If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N (5GHz) channel. Select any channel from the drop-down menu.

Standard Channel. Select the channel for Wireless-A and Wireless-N (5GHz) networking. If you selected Wide - 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N (5GHz).

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

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

2.4 GHz Wireless Settings

Network Mode. If your network devices have multiple modes, keep the default setting, **Mixed**. If you have Wireless-B only, select **Wireless-B**. If you have Wireless-G only, select **Wireless-G**. If you have Wireless-N only, select **Wireless-N**. If you do not have any wireless devices in your network, select **Disabled**.

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

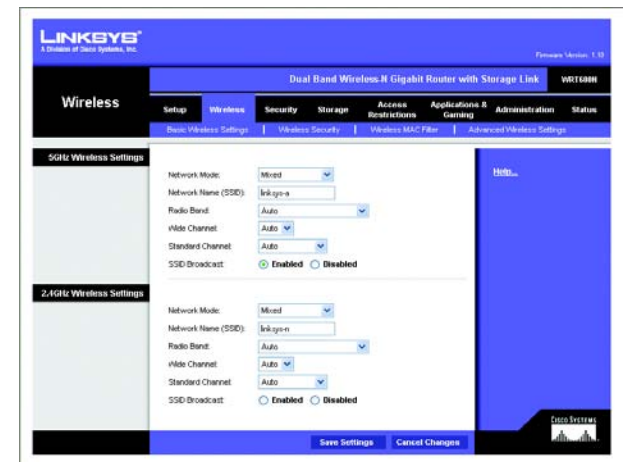


Figure 5-14: Wireless Tab - Basic Wireless Settings



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

Dual-Band Wireless-N Gigabit Router with Storage Link

(use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (**linksys**) to a unique name.

Radio Band. For best performance in a network using Wireless-N (2.4GHz), Wireless-G and Wireless-B devices, keep the default, Auto, and the Wide Channel and Standard Channel will be selected automatically.

Wide Channel. If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N (2.4GHz) channel. Select any channel from the drop-down menu.

Standard Channel. Select the channel for Wireless-N (2.4 GHz), Wireless-G, and Wireless-B networking. If you selected Wide – 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N (2.4GHz).

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

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

The Wireless Tab - Wireless Security

These settings configure the security of your wireless network. There are six wireless security modes supported by the Router: WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) For details on configuring wireless security for the Router, turn to “Appendix B: Wireless Security.” If you do not want to use wireless security, select **Disabled**.

Wireless Security

Security Mode. Select the mode you want to use: **WPA-Personal**, **WPA2-Personal**, **WPA-Enterprise**, **WPA2-Enterprise**, **RADIUS**, or **WEP**. WPA2 is a more advanced, more secure version of WPA.

Follow the instructions for the security method you want to use.

WPA-Personal

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

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

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

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

WPA2-Personal

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

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

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

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

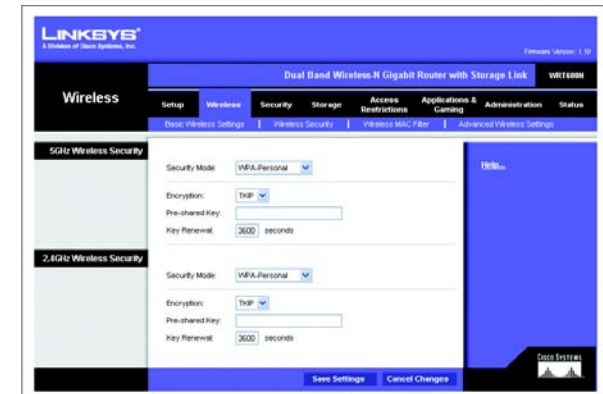


Figure 5-15: Wireless Tab - Wireless Security (WPA-Personal)

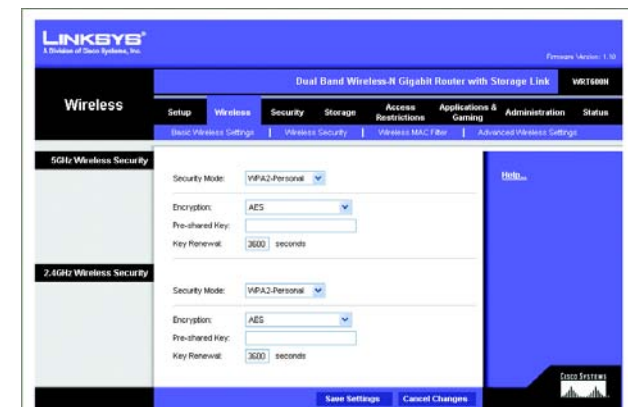


Figure 5-16: Wireless Security - WPA2-Personal

WPA-Enterprise

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

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

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

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

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

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

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

WPA2-Enterprise

This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

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

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

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

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

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

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

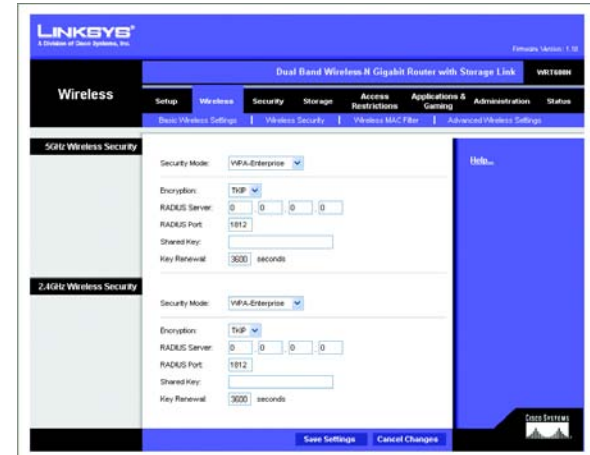


Figure 5-17: Wireless Security - WPA-Enterprise

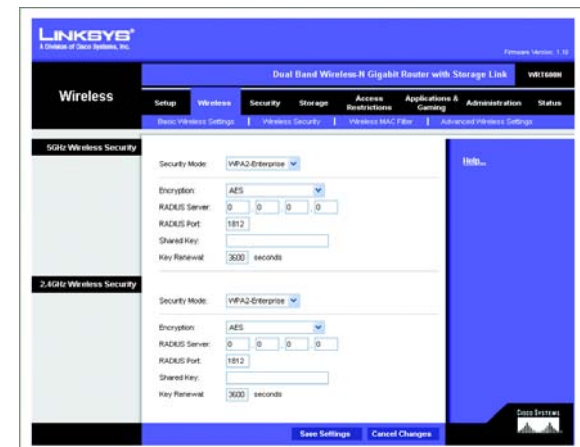


Figure 5-18: Wireless Security - WPA2-Enterprise

RADIUS

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

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

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

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

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

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

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

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

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

WEP

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

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

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

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

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

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

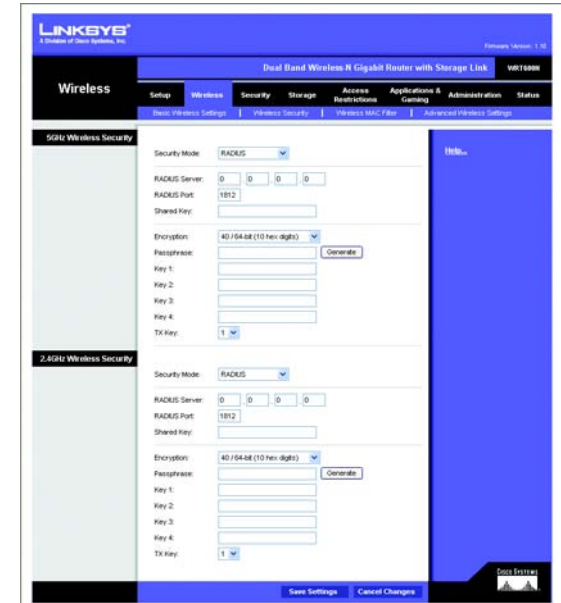


Figure 5-19: Wireless Security - RADIUS

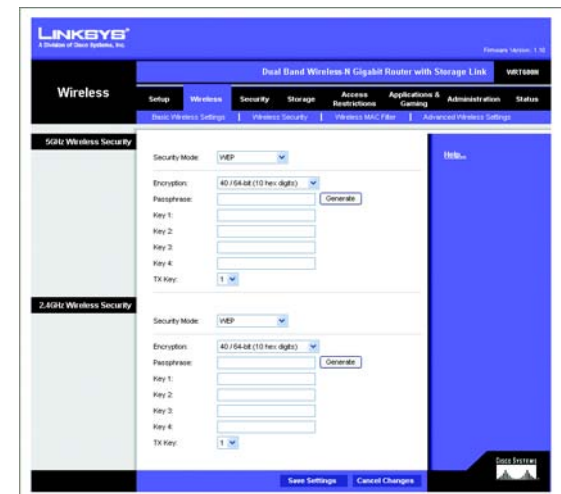


Figure 5-20: Wireless Security - WEP

The Wireless Tab - Wireless MAC Filter

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

Wireless MAC Filter

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

Access Restrictions

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

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

MAC Address Filter List

Click the **Wireless Client List** button to display the Wireless Client List. It shows computers and other devices on the wireless network. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Status. Click the **Save to MAC Address Filter List** checkbox for any device you want to add to the MAC Address Filter List. Then click the **Add** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the *Wireless MAC Filter* screen, click the **Close** button.

Then click the *Enable MAC Filter* checkbox for any device you want to add to the MAC Address Filter List. To update the information on this list, click the **Refresh** button. When you have finished making changes to the *Wireless Client MAC List* screen, click the **Update Filter List** button to save the changes. Click the **Close** button to return to the *Wireless MAC Filter* screen.

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

MAC 01-50. Enter the MAC addresses of the devices whose wireless access you want to block or allow.

When you have finished making changes to the *Wireless MAC Filter* screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

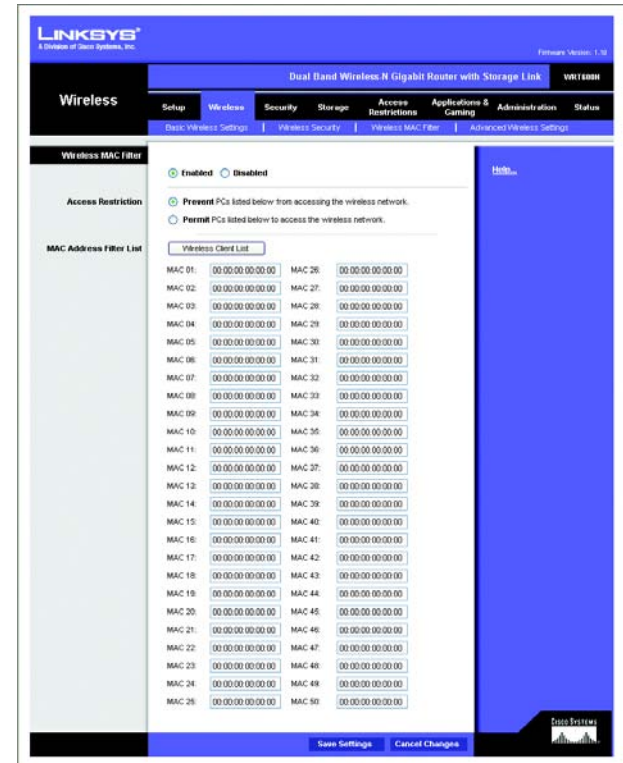


Figure 5-21: Wireless Tab - Wireless MAC Filter



Figure 5-22: Wireless Client List

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

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

Frame Burst. Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, **Disable**.

Authentication Type. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. Select **Shared Key** if you only want to use Shared Key authentication (the sender and recipient use a WEP key for authentication).

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

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

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

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

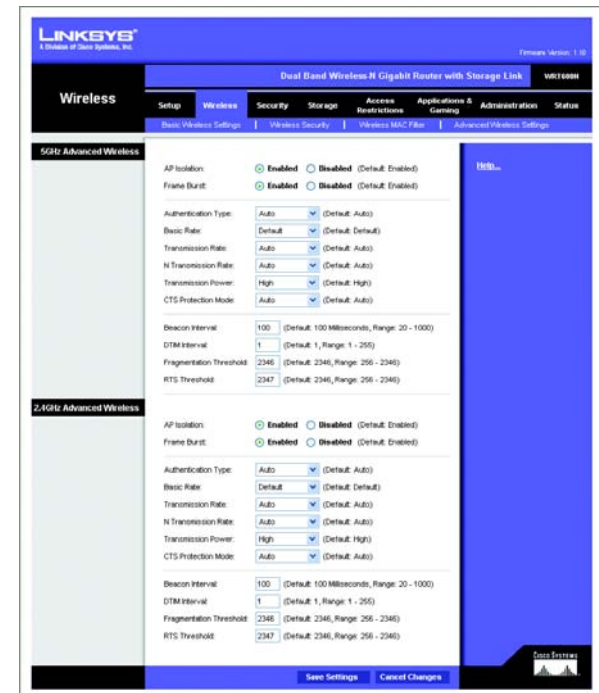


Figure 5-23: Wireless Tab - Advanced Wireless Settings

boosts the Router's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance.

Beacon Interval. Enter a value between 20-1000 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. The default value is **100**.

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**.

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

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

The Security Tab - Firewall

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

Firewall

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

Internet Filter

Filter Anonymous Internet Requests. When enabled, this feature keeps your network from being “pinged,” or detected, by other Internet users. It also hides your network ports. Both make it more difficult for outside users to enter your network. This filter is enabled by default. Select **Disabled** to allow anonymous Internet requests.

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

Filter Internet NAT Redirection. This feature uses port forwarding to block access to local servers from local networked computers. Select **Enabled** to filter Internet NAT redirection, or **Disabled** to disable this feature.

Filter IDENT (Port 113). This feature keeps port 113 from being scanned by devices outside of your local network. Select **Enabled** to filter port 113, or **Disabled** to disable this feature.

Web Filter

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

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

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

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

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

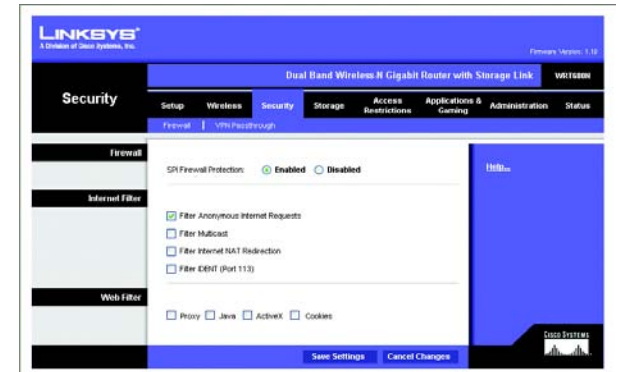


Figure 5-24: Security Tab - Firewall

The Security Tab - VPN Passthrough

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

VPN Passthrough

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

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

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

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



Figure 5-25: VPN Passthrough

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

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

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

The Storage Tab - Disk

You can attach a USB flash drive or hard disk to the Router. The *Disk* screen describes the disk currently attached to the Router. Using this screen, you can format a blank disk, safely remove a disk, or erase a disk.

Disk

Disk Detail

If a formatted disk is attached to the Router, you can view the Partition, File System, Capacity, and Free Space information for each partition of the disk. Click the **Create Share** button to create a shared folder.

If you click the **Create Share** button, the *Shared Folder* screen appears.

Enter a name and the location of the folder you want to share. The folders will appear in the table. To select a folder, select its **Select** button. To view the sub-folder, click **View**. To return to the previous folder, select **Back**. To share all folders, select **All Folders**. Click the **Save Settings** button to save the changes. Click the **Cancel Changes** button to cancel the changes.

Access. This feature allows you to control the Read and Write access to the folders for the groups that you set up on the Administration tab. You can allow Read and Write or Read Only access. Select the right arrows to allow access to a group or the left arrows to remove access to a group. Click the **Save Settings** button to save the changes. Click the **Cancel Changes** button to cancel the changes. Click the **Close** button to close the screen.

Safely Remove Disk 1. Before physically disconnecting a disk from the Router, click the **Safely Remove** button first. This prevents the possible loss of data, if the disk is removed while data is transferring to or from the disk.

Shared Folder

Each name you created on the Shared Folder screen will be listed with its partition and shared folder, which you can edit or delete. Select the **Edit** button to edit an item or **Delete** to delete the item.

If you click the **Edit** button, the *Shared Folder* screen appears.

You can view the current settings of the shared folder. To select a folder, select its **Select** button. To view a sub-folder, click **View**. To return to the previous folder, select **Back**. Click the **Save Settings** button to save the changes. Click the **Cancel Changes** button to cancel the changes.

Access. This feature allows you to control the Read and Write access to the folders for the groups that you set up on the Administration tab. You can allow Read and Write or Read Only access. Select the right arrows



Figure 5-26: Storage Tab - Disk

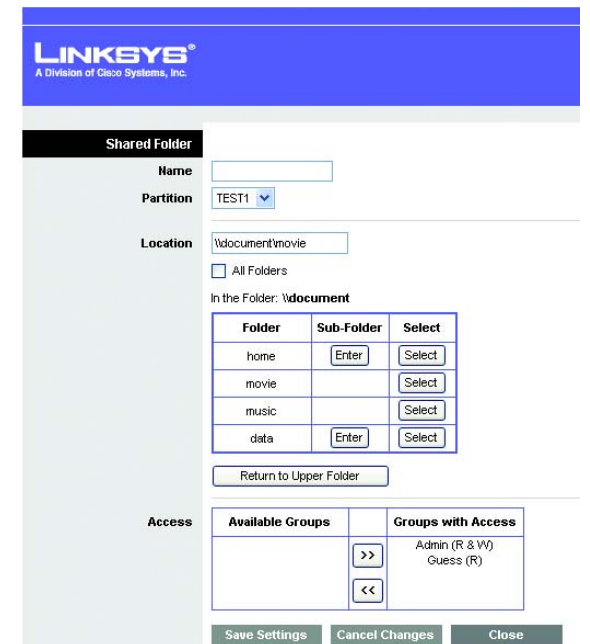


Figure 5-27: Storage Tab - Shared Folder

to allow access to a group or the left arrows to remove access to a group. Click the **Save Settings** button to save the changes. Click the **Cancel Changes** button to cancel the changes. Click the **Close** button to close the screen.

Format Disk

For a blank disk, select the disk you want to format, then click the **Format Disk** button to format the disk and create a partition.

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

The Storage Tab - Media Server

The Router has a built-in media server, so it can stream music, pictures, or video from the USB hard disk to a UPnP-compatible media adapter. The *Media Server* screen lets you scan for content.

Media Server

Setup

Server Name. The name of the Router is displayed here.

UPnP Media Server. To use the Router's media server function, select **Enable**. Otherwise, select **Disable**.

Database

This section lets you select content to add to the database of the Router's media server.

Specify Partitions to Scan. Click this button to select specific partitions to scan for content.

Scan All. Click this button to scan all partitions of the USB hard disk for content.

Auto scan every. Select **Auto scan every** to automatically scan, then select whether to scan every **12 Hours**, **24 Hours**, **36 Hours**, or **48 Hours** from the drop-down menu.

You can view the Partition and Folder of the USB hard disk. Select the **Scan** button to scan an item for content or **Delete** to delete the partition from the Router's database.



Figure 5-28: Storage Tab - Media Server

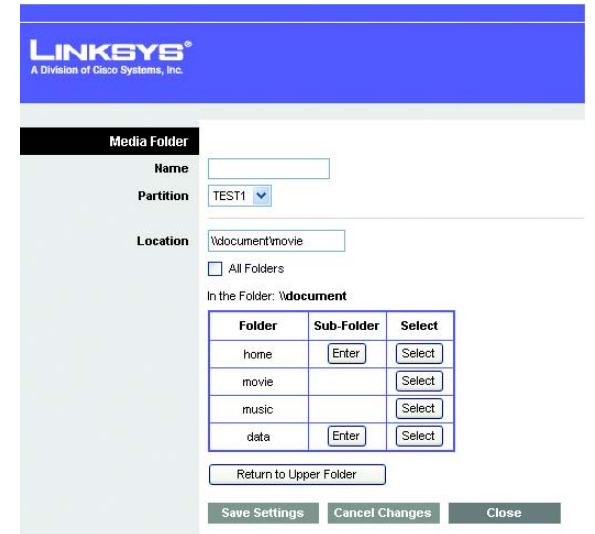


Figure 5-29: Media Folder

If you click the **Scan** button, the *Media Folder* screen appears.

Enter a name and the location of the folder you want to scan. The folders will appear in the table. To select a folder, select its **Select** button. To view the sub-folder, click **View**. To return to the previous folder, select **Back**. To scan all folders, select **Scan All**. Click the **Save Settings** button to save the changes. Click the **Cancel Changes** button to cancel the changes.

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

The Storage Tab - FTP Server

The FTP Server tab creates an FTP Server that can be accessed from the Internet or your local network.

Setup

Server Name. The name of the Router is displayed here.

FTP Server. Select **Enable** to set this Router as an FTP Server. Otherwise, select **Disable** to turn the service off. (Note: A USB drive or USB disk must be connected to the USB Port to use this service.)

Internet Access. Select **Enable** to allow access of the FTP Server from the Internet. Otherwise, select **Disable** to only allow local network access.

FTP Port. Select the Port service to use. The default port is 21.

Access

Use *Access* to allow Read Only or Read or Write access to groups. Click the **Specify Partitions to Access** button to share a specific partition or folder on the FTP server.

If you click the **Specify Partitions to Access** button, the *SFTP Folder* screen appears.

Enter a name and the location of the folder you want to share. The folders will appear in the table. To select a folder, select its **Select** button. To view the sub-folder, click **View**. To return to the previous folder, select **Back**. To select all partitions on the USB disk, select **All Folders**. Click the **Save Settings** button to save the changes. Click the **Cancel Changes** button to cancel the changes.

Access. This feature allows you to control the Read and Write access to the folders for the groups that you set up on the Administration tab. You can allow Read and Write or Read Only access. Select the right arrows to allow access to a group or the left arrows to remove access to a group. Click the **Save Settings** button to



Figure 5-30: Storage Tab - FTP Server

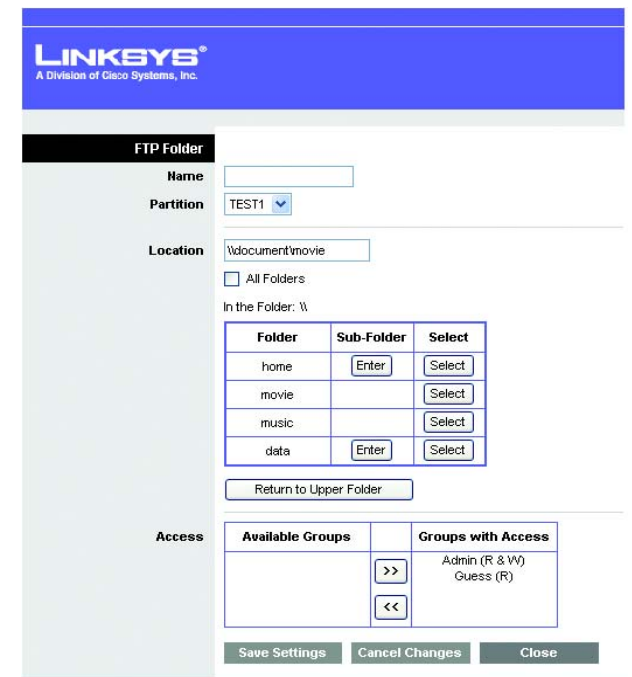


Figure 5-31: FTP Folder

Dual-Band Wireless-N Gigabit Router with Storage Link

save the changes. Click the **Cancel Changes** button to cancel the changes. Click the **Close** button to close the screen.

Each name you created on the *FTP Folder* screen will be listed with its partition and shared folder, which you can edit or delete. Select the **Edit** button to edit an item or **Delete** to delete the item.

If you click the **Edit** button, the *FTP Folder* screen appears.

You can view the current settings of the shared folder. To select a folder, select its **Select** button. To view a sub-folder, click **View**. To return to the previous folder, select **Back**. Click the **Save Settings** button to save the changes. Click the **Cancel Changes** button to cancel the changes.

Access. This feature allows you to control the Read and Write access to the folders for the groups that you set up on the Administration tab. You can allow Read and Write or Read Only access. Select the right arrows to allow access to a group or the left arrows to remove access to a group. Click the **Save Settings** button to save the changes. Click the **Cancel Changes** button to cancel the changes. Click the **Close** button to close the screen.

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

The Storage Tab - Administration

The *Administration* screen allows you to manage the users and groups of users that can access the shares.

Information

Server Name. Enter a name for the Router. Punctuation and other special characters (e.g., * / | \) cannot be used in the name.

Workgroup Name. Enter the Workgroup Name of your networked computers.

The Server LAN IP Address and the Server Internet IP Address are displayed here.

User Management

The users are listed in the User Management table. The two default users, Admin (read and write access) and Guest (read-only access) cannot be deleted. Click the **Create New User** button to create a new user.

If you click the **Create New User** button, the *User Account* screen appears.

Enter a user name for the user, then enter the name and description for the user. Then, enter a password and enter it again in the *Confirm Password* field. Select **Admin** or **Guest** from the *Group Member* drop-down menu. Click the **Save Settings** button to save the new changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to close the screen.

Each name you created on the *User Account* screen will be listed with its group, which you can edit or delete. Select the **Edit** button to edit a user or **Delete** to delete the user.

If you click the **Edit** button, the *User Account* screen appears.

Enter a different name for the user, change the password, and/or select **Admin** or **Guest** from the *Group Member* drop-down menu. Click the **Save Settings** button to save the new changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to close the screen.

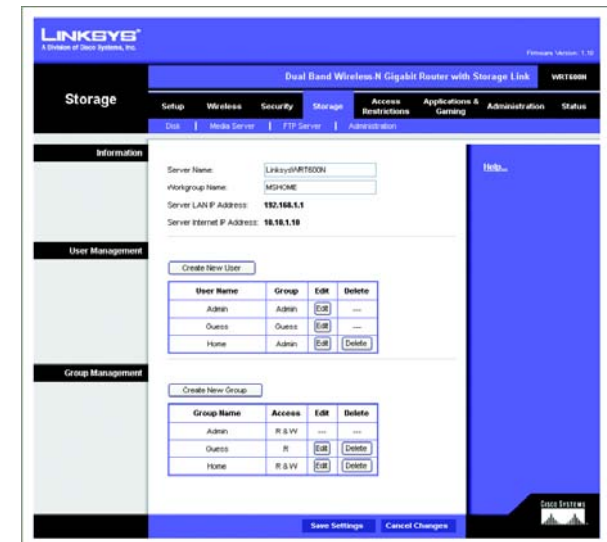


Figure 5-32: Storage Tab - Administration

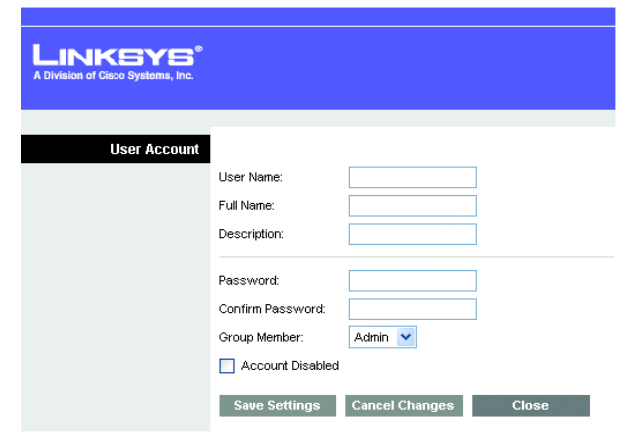


Figure 5-33: User Account

Group Management

The groups are listed in the Group Management table. There are two default groups, Admin and Guest; these cannot be deleted. Click the **Create New Group** button to create a new group.

If you click the **Create New Group** button, the *Group Account* screen appears.

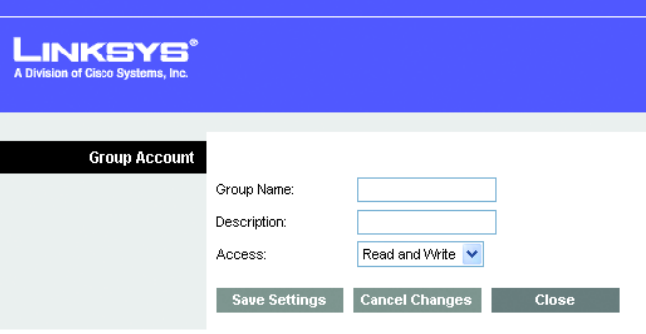
Enter the name and description for the group. Then, select **Read and Write** or **Read Only** from the *Access* drop-down menu. Click the **Save Settings** button to save the new changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to close the screen.

Each group you created on the *Group Account* screen will be listed with its access, which you can edit or delete. Select the **Edit** button to edit a user or **Delete** to delete the user.

If you click the **Edit** button, the *Group Account* screen appears.

Enter a new Group Name or Description, then select Read and Write or Read Only from the Access drop-down menu. Click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to exit the *Group Account* screen.

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



The screenshot shows the Linksys Group Account configuration page. At the top is the Linksys logo with the text "A Division of Cisco Systems, Inc." Below the logo is a blue header bar. The main content area has a dark grey header with the text "Group Account". To the left of the form is a light grey sidebar. The form contains three input fields: "Group Name:" with an empty text box, "Description:" with an empty text box, and "Access:" with a dropdown menu showing "Read and Write". Below the form are three buttons: "Save Settings", "Cancel Changes", and "Close".

Figure 5-34: Group Account

The Access Restrictions Tab - Internet Access Policy

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

Internet Access Policy

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 This Policy** button. To view all the policies, click the **Summary** button.

On the *Summary* screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, click the **Enabled** checkbox. To delete a policy, click its **Delete** button. Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to cancel your changes. To return to the *Internet Access Policy* screen, 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 *Enabled*.

To create a policy:

1. Select a number from the *Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, click the radio button beside *Enabled*.
4. Click the **Edit List** 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.
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.
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**.

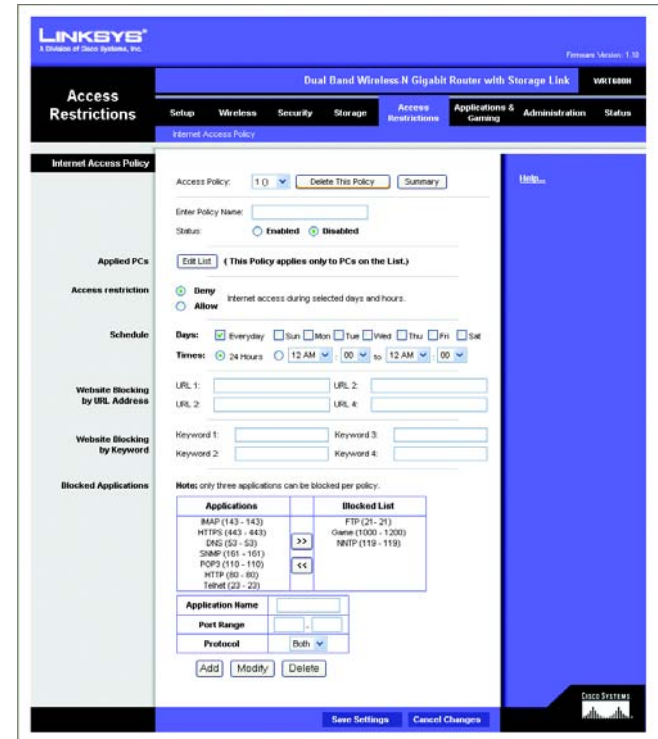


Figure 5-35: Access Restrictions Tab - Internet Access Policy

No.	Policy Name	Access	Days	Time	Enabled	Delete
1	Home	Deny	Everyday	24 Hours	<input checked="" type="checkbox"/>	Delete
2	Guest	Allow	Sun, Mon, Tue, Wed, Thu, Fri, Sat	12:00 - 20:00	<input checked="" type="checkbox"/>	Delete
3	Children	Allow	Tue, Wed	08:00 - 10:00	<input type="checkbox"/>	Delete
4	---	---	---	---	<input type="checkbox"/>	Delete
5	---	---	---	---	<input type="checkbox"/>	Delete
6	---	---	---	---	<input type="checkbox"/>	Delete
7	---	---	---	---	<input type="checkbox"/>	Delete
8	---	---	---	---	<input type="checkbox"/>	Delete
9	---	---	---	---	<input type="checkbox"/>	Delete
10	---	---	---	---	<input type="checkbox"/>	Delete

Figure 5-36: Summary

7. You can block websites with specific URL addresses. Enter each URL in a separate field next to *Website Blocking by URL Address*.
8. You can also block websites using specific keywords. Enter each keyword in a separate field next to *Website Blocking by Keyword*.
9. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.)

From the Applications list, select the application you want to block. Then click the >> button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the << button.

10. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the *Application Name* field. Enter its range in the *Port Range* fields. Select its protocol from the *Protocol* drop-down menu. Then click the **Add** button.

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

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

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

For more information, click **Help**.

The screenshot shows the 'List of PCs' configuration page. At the top, there is a blue header with the Linksys logo and 'A Division of Cisco Systems, Inc.'. Below the header, the page title 'List of PCs' is displayed. The main content area is divided into three sections: 'MAC Address', 'IP Address', and 'IP Address Range'. Each section contains a table with columns for an ID, a value field, and a 'to' field. The 'MAC Address' section has 10 rows with values '00:00:00:00:00:00'. The 'IP Address' section has 6 rows with values '192.168.1.0'. The 'IP Address Range' section has 4 rows with values '192.168.1.0 to 0'. At the bottom of the page, there are three buttons: 'Save Settings', 'Cancel Changes', and 'Close'.

Figure 5-37: List of PCs

The Applications & Gaming Tab - Single Port Forwarding

When you click the Applications & Gaming tab, you will see the *Single Port Forwarding* screen. You can customize port services for common applications on this screen.

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

Single Port Forwarding

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

For additional applications, complete the following fields:

Application Name. Enter the name of the application.

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

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

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

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

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

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

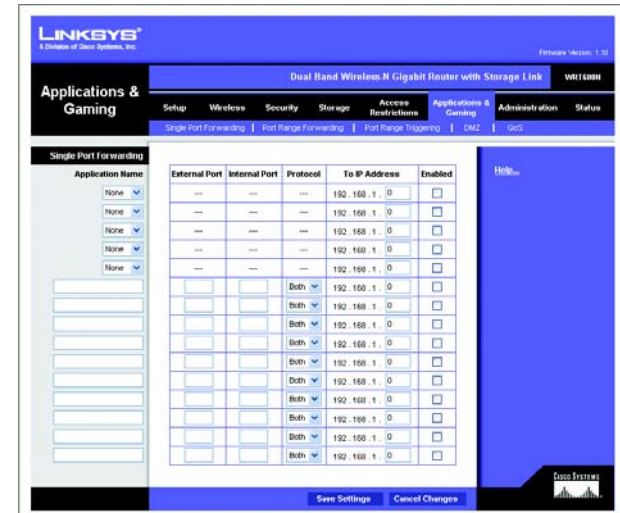


Figure 5-38: Applications & Gaming Tab - Single Port Forwarding

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

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

The Applications & Gaming Tab - Port Range Forwarding

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

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

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

Port Range Forwarding

To add an application, complete the following fields:

Application Name. Enter the name of the application.

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

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

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

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

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

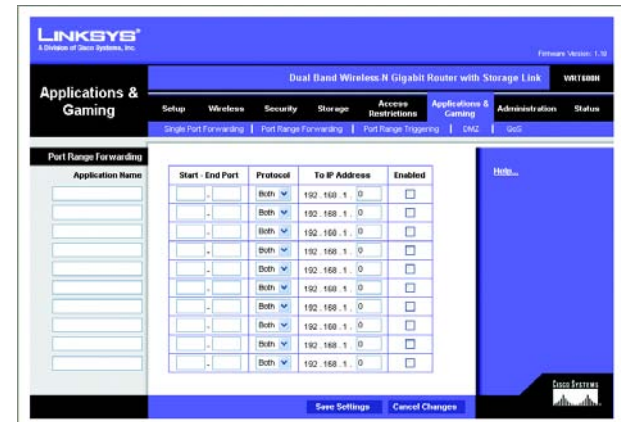


Figure 5-39: Applications & Gaming Tab - Port Range Forwarding

The Applications & Gaming Tab - Port Range Triggering

This screen instructs the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is sent to the proper computer by way of IP address and port mapping rules.

Port Range Triggering

To add an application, complete the following fields:

Application Name. Enter the name of the application.

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

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

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

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

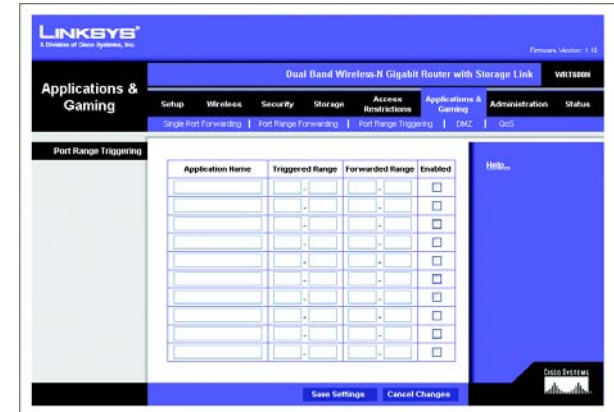


Figure 5-40: Applications & Gaming Tab - Port Range Triggering

The Applications & Gaming Tab - DMZ

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

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

DMZ

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

Source IP Address. If you want any IP address to be the source, select **Any IP Address**. If you want to specify an IP address or range of IP addresses as the designated source, click the second radio button, and enter the IP address(es) in the fields provided.

Destination. If you want to specify the DMZ host by IP address, select **IP Address** and complete the IP address in the field provided. If you want to specify the DMZ host by MAC address, select **MAC Address** and enter the MAC address in the field provided. To retrieve this information, click the **DHCP Client Table** button.

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired Time (how much time is left for the current IP address). To select a DHCP client, click the **Select** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the *DMZ* screen, click the **Close** button.

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



Figure 5-41: Applications & Gaming Tab - DMZ

Client Name	Interface	IP Address	MAC Address	
Linksys 1	LAN	192.168.1.100	00:40:05:35:CE:61	Select
Linksys 2	Wireless-A	192.168.1.101	00:40:05:35:CE:62	Select
Linksys 3	Wireless-G	192.168.1.102	00:40:05:35:CE:63	Select
Linksys 4	Wireless-B	192.168.1.103	00:40:05:35:CE:62	Select

Figure 5-42: DHCP Client Table

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

The Router features Wireless QoS. The No Acknowledgement feature is available only when the Wireless QoS Support feature is enabled.

Wireless QoS. If you have other devices on your network that support Wireless QoS, select **Enabled**. Otherwise, keep the default, **Disabled**.

No Acknowledgement. If you want to disable the Router's Acknowledgement feature, so the Router will not re-send data if an error occurs, then keep the default, **Enabled**. Otherwise, select **Disabled**.

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels priority: High, Medium, Normal, or Low. When you set priority, do not 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.

Enabled/Disabled. To use the QoS policies you have set, select **Enabled**. Otherwise, select **Disabled**.

Category

There are four categories available. Select one of the following: **Applications**, **Online Games**, **MAC Address**, **Ethernet Port**, or **Voice Device**. Proceed to the instructions for your selection.

Applications

Applications. Select the appropriate application. If you select Add a New Application, follow the Add a New Application instructions.

Priority. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.



Figure 5-43: Applications & Gaming Tab - QoS (Applications)

Add a New Application

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

Port Range 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.

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

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

Online Games

Games. Select the appropriate game.

Priority. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

MAC Address

Enter a Name. Enter a name for your device.

MAC Address. Enter the MAC address of your device.

Priority. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

Ethernet Port

Ethernet. Select the appropriate Ethernet port.

Priority. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

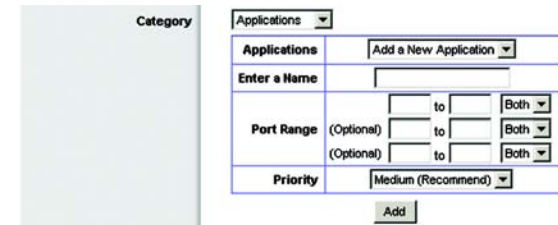


Figure 5-44: QoS - Applications (Add a New Application)

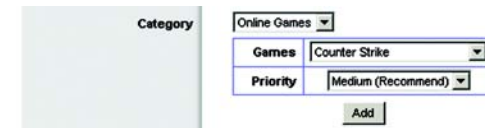


Figure 5-45: QoS - Online Games



Figure 5-46: QoS - MAC Address

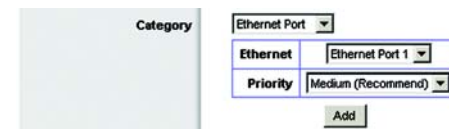


Figure 5-47: QoS - Ethernet

Voice Device

Enter a Name. Enter a name for your voice device.

MAC Address. Enter the MAC address of your voice device.

Priority. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

Summary

This lists the QoS entries you have created for your applications and devices.

Priority This displays the bandwidth priority of High, Medium, Normal, or Low.

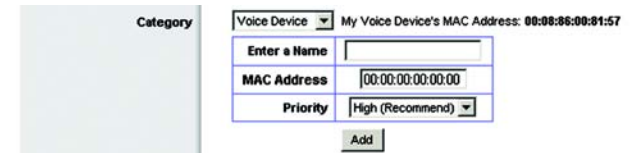
Name This displays the application, device, or port name.

Information This displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.

Remove Click this button to remove an entry.

Edit Click this button to make changes.

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



The screenshot shows a web-based configuration form for adding a voice device. On the left, there is a grey box labeled 'Category'. To its right, a dropdown menu is set to 'Voice Device', with the text 'My Voice Device's MAC Address: 00:08:86:00:81:57' displayed next to it. Below this, there are three input fields: 'Enter a Name' (empty), 'MAC Address' (containing '00:00:00:00:00:00'), and 'Priority' (a dropdown menu set to 'High (Recommend)'). At the bottom right of the form is an 'Add' button.

Figure 5-48: QoS - Voice Device

The Administration Tab - Management

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

Management

Router Access

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

Router Password.

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

Web Access

Web Utility Access. HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**.

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

Remote Access

Remote Management. To permit remote access of the Router, from outside the local network, select **Enabled**. Otherwise, keep the default setting, **Disabled**.

Web Utility Access. HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**.

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

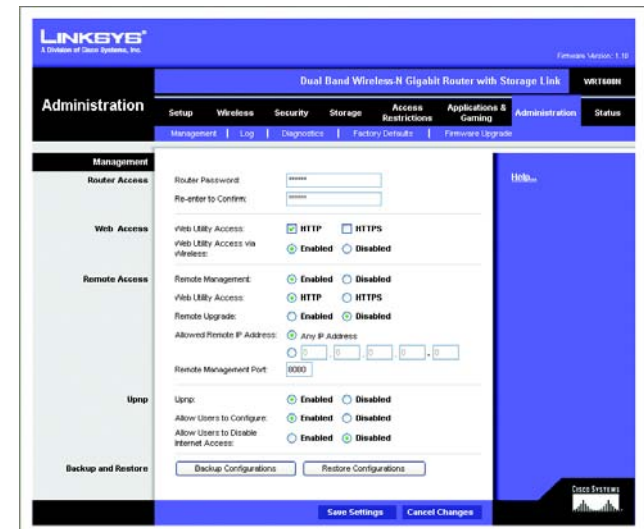


Figure 5-49: Administration Tab - Management

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

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



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

UPnP

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

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

Allow Users to Configure. Select **Enabled**, if you want to be able to make manual changes to the Router while using the UPnP feature. Otherwise, keep the default setting, **Disabled**.

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

Backup and Restore

Backup Configurations. To back up the Router's configuration settings, click this button and follow the on-screen instructions.

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

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

The Administration Tab - Log

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

Log

Log. To access activity logs, select the **Enabled** radio button. With logging enabled, you can choose to view temporary logs or keep a permanent record using the Logviewer software. Click the **Disabled** button to disable this function.

View Log. When you wish to view the logs, click **View Log**. A new screen will appear. Select **Incoming Log**, **Outgoing Log**, **Security Log**, or **DHCP Client Log** from the *Type* drop-down menu. The Incoming Log will display a temporary log of the source IP addresses and destination port numbers for the incoming Internet traffic. The Outgoing Log will display a temporary log of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic. The Security log will display the login information for the Web-based Utility. The DHCP Client Log will display the LAN DHCP server status information.

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

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



Figure 5-50: Administration Tab - Log

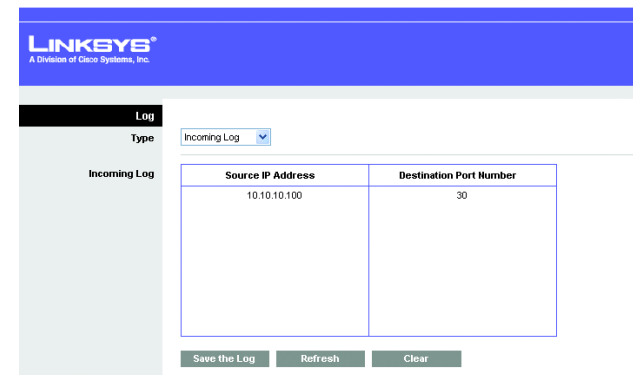


Figure 5-51: View Log

The Administration Tab - Diagnostics

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

Ping Test. The Ping test will check the status of a connection. Enter the IP address or URL of the PC whose connection you wish to test, the packet size (default is **32** bytes), and how many times you wish to test it. Then, click the **Start to Ping** button. The *Ping* screen will then display the test results. Click the **Close** button to return to the *Diagnostics* screen.

Traceroute Test. To test the performance of a connect, enter the IP address or URL of the PC whose connection you wish to test and click the **Start to Traceroute** button. The *Traceroute* screen will then display the test results. Click the **Close** button to return to the *Diagnostics* screen.

For more information, click **Help**.



Figure 5-52: Administration Tab - Diagnostics



Figure 5-53: Ping Test



Figure 5-54: Traceroute Test

The Administration Tab - Factory Defaults

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



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

Factory Defaults

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

Help information is shown on the right-hand side of the screen.



Figure 5-55: Administration Tab - Factory Defaults

The Administration Tab - Firmware Upgrade

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

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

Upgrade Firmware



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

Please Select a File to Upgrade. In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.

Start to Upgrade. After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Help information is shown on the right-hand side of the screen.



Figure 5-56: Administration Tab - Firmware Upgrade

firmware: the programming code that runs a networking device.

download: to receive a file transmitted over a network.

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

The Status Tab - Router

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

Router Information

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

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

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

Host Name. If required by your ISP, this was entered on the *Basic Setup* screen.

Domain Name. If required by your ISP, this was entered on the *Basic Setup* screen.

Internet Connection

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

For dial-up style connections such as PPPoE or PPTP, there is a Connect button to click if there is no connection and you want to establish an Internet connection.

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

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

DNS1-3. Shown here are the DNS (Domain Name System) IP addresses currently used by the Router.

MTU. Shown here is the MTU (Maximum Transmission Unit) setting for the Router.

DHCP Lease Time. Displays how long the lease is for the IP address that your ISP automatically assigned you.

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

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

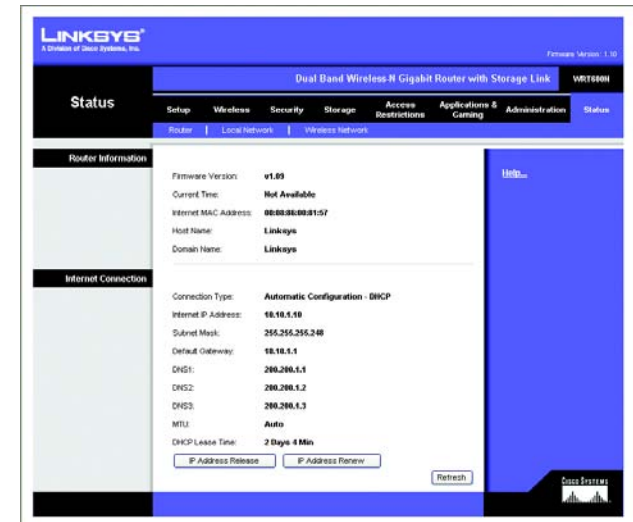


Figure 5-57: Status Tab - Router

For PPoE, PPTP, L2TP, and Telstra Cable Internet Connection types, a connect and disconnect button will be available to establish a connection to your ISP.

Click the **Refresh** button to update the on-screen information. For more information, click **Help**.

The Status Tab - Local Network

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

Local Network

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

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

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

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

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

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

DHCP Client Table. Click the **DHCP Clients Table** button to view the DHCP Client Table. It lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired Time (how much time is left for the current IP address). To remove a DHCP client, click the **Delete** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the *Local Network* screen, click the **Close** button.

For more information, click **Help**.

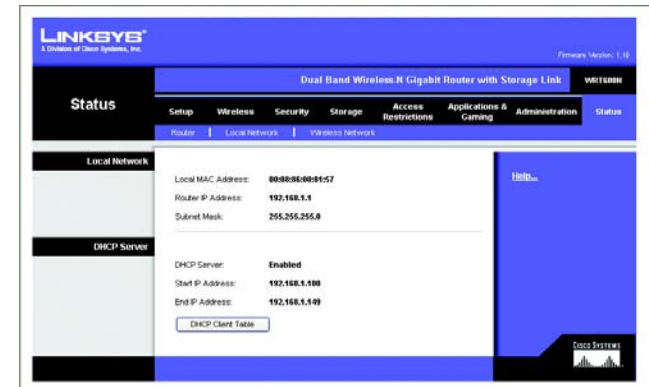


Figure 5-58: Status Tab - Local Network



Figure 5-59: DHCP Client Table

The Status Tab - Wireless

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

Wireless

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

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

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

Radio Band. Displayed here is the Radio Band setting selected on the *Basic Wireless Settings* screen.

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

Standard Channel. Shown here is the Standard Channel setting selected on the *Basic Wireless Settings* screen.

Security. Displayed here is the wireless security method used by the Router.

SSID Broadcast. Displayed here is the status of the SSID Broadcast feature.

For more information, click **Help**.

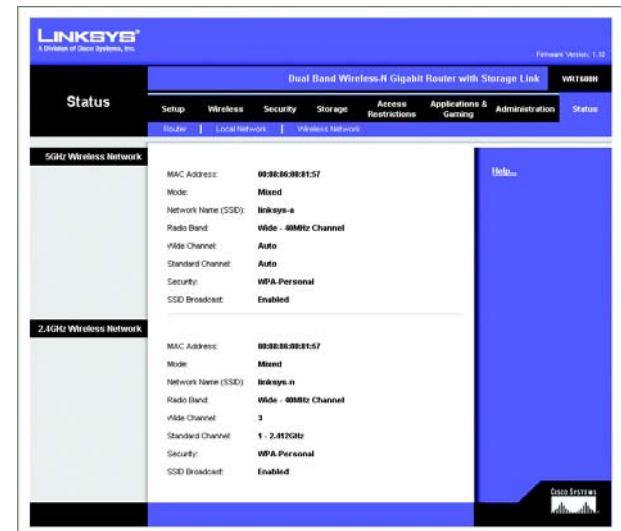


Figure 5-60: Status Tab - Wireless Network

Appendix A: Troubleshooting

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

Common Problems and Solutions

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

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

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

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

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

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

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

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

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

3. I want to test my Internet connection.

A Check your TCP/IP settings.

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

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

B Open a command prompt.

For Windows 98SE and Me:

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

For Windows 2000 and XP:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Follow these steps to set DMZ hosting:

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

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

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

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

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

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

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

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

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

12. I need to upgrade the firmware.

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

Follow these steps:

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

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

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

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

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

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

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

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

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

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

16. The Power LED keeps flashing.

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

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

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

Frequently Asked Questions

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

The Router will support up to 253 IP addresses.

Is IPsec Pass-Through supported by the Router?

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

Where is the Router installed on the network?

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

Does the Router support IPX or AppleTalk?

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

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

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

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

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

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

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

Does the Router support ICQ send file?

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

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

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

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

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

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

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

How can I block corrupted FTP downloads?

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

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

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

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

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

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 Administration - Firmware Upgrade tab of the Router's web-based utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a

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

Will the Router function in a Macintosh environment?

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

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

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

What is DMZ Hosting?

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

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

No.

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

The Router allows PPTP packets to pass through.

Is the Router cross-platform compatible?

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

How many ports can be simultaneously forwarded?

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

What are the advanced features of the Router?

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

How do I get mIRC to work with the Router?

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

Can the Router act as my DHCP server?

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

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

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

What is the draft IEEE 802.11n standard?

It is a draft IEEE standard for wireless networks. 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput and increased operating ranges. The real data throughput is estimated to be 540Mbps, which is 10 times faster than 802.11a.

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

Dual-Band Wireless-N Gigabit Router with Storage Link

- RTS/CTS feature
- Fragmentation
- Power Management

What is ad-hoc mode?

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

What is infrastructure mode?

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

What is roaming?

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

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

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

What is ISM band?

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

What is Spread Spectrum?

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

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

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

What is a MAC Address?

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

How do I reset the Router?

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

How do I resolve issues with signal loss?

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

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

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

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

Dual-Band Wireless-N Gigabit Router with Storage Link

How many channels/frequencies are available with the Router?

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

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

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-N Gigabit Router with Storage Link.”

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. WPA is stronger than WEP encryption, and WPA2 has stronger encryption than WPA. WPA and WPA2 gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. (AES is stronger than TKIP.)

WPA-Enterprise and WPA2-Enterprise use a RADIUS (Remote Authentication Dial-In User Service) server for authentication. RADIUS uses a RADIUS server and WEP encryption.



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

Dual-Band Wireless-N Gigabit Router with Storage Link

WPA/WPA2-Personal. Select the type of algorithm, **TKIP** or **AES**, and enter a password in the *Pre-shared Key* field of 8-63 characters. Enter a Key Renewal period time between 0 and 99,999 seconds, which instructs the Router or other device how often it should change the encryption keys.

WPA/WPA2-Enterprise. This method is WPA or WPA2 used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Router and its RADIUS server. Then enter a Key Renewal period, which instructs the Router or other device how often it should change the encryption keys.

RADIUS. This method is WEP used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Router and its RADIUS server. Enter the WEP settings.

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

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

Appendix C: Upgrading Firmware

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

1. Download the firmware from Linksys's website at www.linksys.com.
2. Extract the firmware file on your computer.
3. Open the Router's Web-based Utility, and click the **Administration** tab.
4. Click the **Firmware Upgrade** tab, and the *Firmware Upgrade* screen will appear.
5. Enter the location of the firmware's file, or click the **Browse** button to find the file.
6. Click the **Start to Upgrade** button, and follow the on-screen instructions.



Figure C-1: Firmware Upgrade

Appendix D: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

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

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Router's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 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. See Figure E-1.
3. Write down the Adapter Address as shown on your computer screen (see Figure E-2). This is the MAC address for your Ethernet adapter and is shown as a series of numbers and letters.

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

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



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

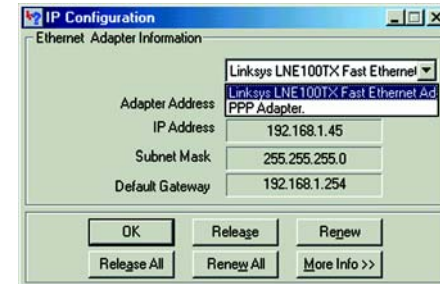


Figure E-1: IP Configuration Screen

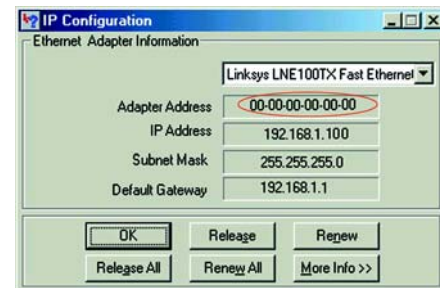


Figure E-2: MAC Address/Adapter Address

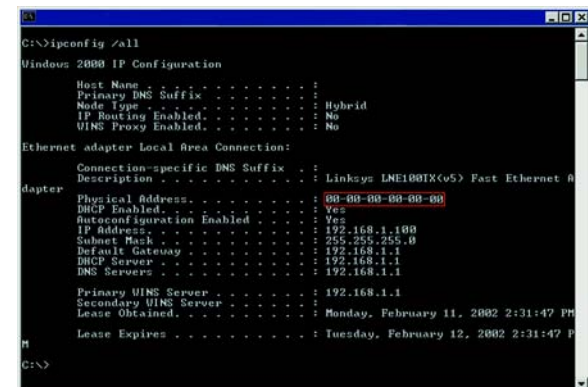


Figure E-3: MAC Address/Physical Address

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 (Figure E-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

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



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

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

For the Router's Web-based Utility

For MAC filtering, enter the 12-digit MAC address in the appropriate *MAC* field on the *Wireless MAC Filter* screen.

For MAC address cloning, enter the MAC address in the *MAC Address* fields on the *MAC Address Clone* screen.

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

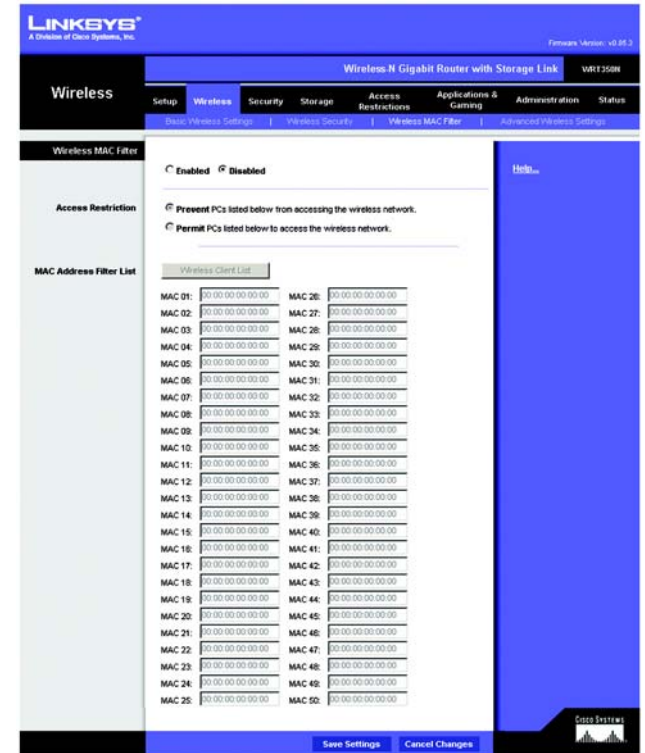


Figure E-4: Wireless MAC Filter



Figure E-5: MAC Address Cloning

Appendix F: Glossary

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

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

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

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

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

Bit - A binary digit.

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

Broadband - An always-on, fast Internet connection.

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

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

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

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

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

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

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

Dual-Band Wireless-N Gigabit Router with Storage Link

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

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

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

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

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

Encryption - Encoding data transmitted in a network.

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

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

Firmware - The programming code that runs a networking device.

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

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

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

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

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

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

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

Dual-Band Wireless-N Gigabit Router with Storage Link

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

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

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

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

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

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

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

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

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

Packet - A unit of data sent over a network.

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

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

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

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

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

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

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

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

Dual-Band Wireless-N Gigabit Router with Storage Link

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

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

Router - A networking device that connects multiple networks together.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Dual-Band Wireless-N Gigabit Router with Storage Link

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

Upload - To transmit a file over a network.

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

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

WAN (Wide Area Network)- The Internet.

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

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

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

Appendix G: Specifications

Model	WRT350N
Standards	Draft 802.11n, 802.11a, 802.11g, 802.11b, 802.3, 802.3u
Ports	Power, Internet, Ethernet, USB
Button	Reset
LEDs	Power, Ethernet (1-4), Internet, USB 5GHz: Wireless, Security 2.4GHz: Wireless, Security
# of Antennas	3
RF Pwr (EIRP) in dBm	17 dBm
Antenna Gain in dBi	1.8 dBm
UPnP able/cert	Able
Security Features	WEP, WPA, WPA2
WEP Key Bits	128, 256
Dimensions	7.40 x 1.89 x 6.93 in (188 mm x 48 mm x 176 mm)
Unit Weight	0. (0. kg)
Power	12V
Certifications	FCC, IC-03

Dual-Band Wireless-N Gigabit Router with Storage Link

Operating Temp.	0° C to 40° C (32° F to 104° F)
Storage Temp.	-20° C to 60° C (-4° F to 140° F)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix H: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix I: Regulatory Information

FCC Statement

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

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

FCC Radiation Exposure Statement

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

Safety Notices

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

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

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

Industry Canada (Canada)

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

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

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

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

English

Environmental Information for Customers in the European Union

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

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

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



Dansk/Danish

Miljøinformation for kunder i EU

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

Deutsch/German

Umweltinformation für Kunden innerhalb der Europäischen Union

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

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

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

Español/Spanish

Información medioambiental para clientes de la Unión Europea

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

Ελληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

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

Français/French

Informations environnementales pour les clients de l'Union européenne

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

Italiano/Italian

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

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

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķīrotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par 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 perdurbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Kliġenti fl-Unjoni Ewropea

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

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

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

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

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

Norsk/Norwegian

Miljøinformasjon for kunder i EU

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

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

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

Português/Portuguese

Informação ambiental para clientes da União Europeia

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

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

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

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

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

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

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

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

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

For more information, visit www.linksys.com.

Appendix J: Contact Information

Need to contact Linksys?

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

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

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

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

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

800-859-2379
support@linksys.com

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

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

949-823-3000