

LINKSYS®

A Division of Cisco Systems, Inc.



2.4GHz
802.11g

Wireless-G

Broadband Router with RangeBooster

User Guide



Model No. WRT54GR ver. 1.1



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-G Broadband Router with RangeBooster easier than ever. Look for the following items when reading this User Guide:



This checkmark means there is a note of interest and is something you should pay special attention to while using the Wireless-G Broadband Router with RangeBooster.



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



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

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 | 4 |
| Chapter 3: Getting to Know the Wireless-G Broadband Router with RangeBooster | 6 |
| The Back Panel | 6 |
| The Front Panel | 7 |
| Chapter 4: Connecting the Wireless-G Broadband Router with RangeBooster | 8 |
| Hardware Installation for Connection to Your Broadband Modem | 8 |
| Chapter 5: Configuring the Wireless-G Broadband Router with RangeBooster | 10 |
| Overview | 10 |
| The Setup Tab - Basic Setup | 11 |
| The Setup Tab - DDNS | 15 |
| The Setup Tab - MAC Address Clone | 16 |
| The Setup Tab - Advanced Routing | 17 |
| The Wireless Tab - Basic Wireless Settings | 18 |
| The Wireless Tab - Wireless Security | 19 |
| The Wireless Tab - Wireless MAC Filter | 22 |
| The Wireless Tab - Advanced Wireless Settings | 23 |
| The Security Tab - Firewall | 25 |
| The Security Tab - VPN Passthrough | 26 |
| The Access Restrictions Tab - Internet Access Policy | 26 |
| The Applications and Gaming Tab - Single Port Forwarding | 28 |
| The Applications and Gaming Tab - Port Range Forwarding | 29 |
| The Applications & Gaming Tab - Port Range Triggering | 30 |
| The Applications and Gaming Tab - DMZ | 30 |
| The Administration Tab - Management | 31 |
| The Administration Tab - Log | 33 |
| The Administration Tab - Diagnostics | 34 |

| | |
|---|-----------|
| The Administration Tab - Factory Defaults | 35 |
| The Administration Tab - Firmware Upgrade | 35 |
| The Status Tab - Router | 36 |
| The Status Tab - Local Network | 37 |
| The Status Tab - Wireless Network | 37 |
| Appendix A: Troubleshooting | 38 |
| Common Problems and Solutions | 38 |
| Frequently Asked Questions | 46 |
| Appendix B: Wireless Security | 53 |
| Security Precautions | 53 |
| Security Threats Facing Wireless Networks | 53 |
| Appendix C: Upgrading Firmware | 56 |
| Appendix D: Windows Help | 57 |
| Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter | 58 |
| Windows 98SE or Me Instructions | 58 |
| Windows 2000 or XP Instructions | 58 |
| For the Router's Web-based Utility | 59 |
| Appendix F: Glossary | 60 |
| Appendix G: Specifications | 67 |
| Appendix H: Warranty Information | 69 |
| Appendix I: Regulatory Information | 70 |
| Appendix J: Contact Information | 72 |

List of Figures

| | |
|--|----|
| Figure 3-1: The Router's Back Panel | 6 |
| Figure 3-2: The Router's Front Panel | 7 |
| Figure 4-1: Connecting Your Internet Connection | 8 |
| Figure 4-2: Connecting Your Network Devices | 9 |
| Figure 4-3: Connecting the Power | 9 |
| Figure 5-1: Password Screen | 10 |
| Figure 5-2: Setup Tab - Basic Setup | 11 |
| Figure 5-3: DHCP Connection Type | 11 |
| Figure 5-4: Static IP Connection Type | 11 |
| Figure 5-5: PPPoE Connection Type | 12 |
| Figure 5-6: PPTP Connection Type | 12 |
| Figure 5-7: HeartBeat Signal Connection Type | 13 |
| Figure 5-8: Optional Settings | 13 |
| Figure 5-9: Router IP | 13 |
| Figure 5-10: DHCP Server Settings | 14 |
| Figure 5-11: Static DHCP Client List | 14 |
| Figure 5-12: DHCP Client Table | 14 |
| Figure 5-13: Time Setting | 14 |
| Figure 5-14: Setup Tab - DDNS.com | 15 |
| Figure 5-15: Setup Tab - TZO.com | 15 |
| Figure 5-16: Setup Tab - MAC Address Clone | 16 |
| Figure 5-17: Setup Tab - Advanced Routing | 17 |
| Figure 5-18: Setup Tab - Routing Table | 17 |
| Figure 5-19: Wireless Tab - Basic Wireless Settings | 18 |
| Figure 5-20: Wireless Tab - Wireless Security (WEP) | 19 |
| Figure 5-21: Wireless Tab - Wireless Security (WPA-Personal) | 19 |
| Figure 5-22: Wireless Tab - Wireless Security (PSK2) | 20 |
| Figure 5-23: Wireless Tab - Wireless Security (RPSK2-Mixed) | 20 |
| Figure 5-24: Wireless Tab - Wireless Security (WPA Enterprise) | 20 |
| Figure 5-25: Wireless Tab - Wireless Security (PSK2 + RADIUS) | 21 |
| Figure 5-26: Wireless Tab - Wireless Security (RADIUS) | 21 |

| | |
|---|----|
| Figure 5-27: Wireless Tab - Wireless MAC Filter | 22 |
| Figure 5-28: Wireless Client List | 22 |
| Figure 5-29: Wireless Tab - Advanced Wireless Settings | 23 |
| Figure 5-30: Security Tab - Firewall | 25 |
| Figure 5-31: Security Tab - VPN Passthrough | 26 |
| Figure 5-32: Access Restrictions Tab - Internet Access Policy | 26 |
| Figure 5-33: Internet Policy Summary | 27 |
| Figure 5-34: List of PCs | 27 |
| Figure 5-35: Applications and Gaming Tab - Single Port Forwarding | 28 |
| Figure 5-36: Applications and Gaming Tab - Port Range Forward | 29 |
| Figure 5-37: Applications and Gaming Tab - Port Triggering | 30 |
| Figure 5-38: Applications and Gaming Tab - DMZ | 30 |
| Figure 5-39: Administration Tab - Management | 31 |
| Figure 5-40: Administration Tab - Log | 33 |
| Figure 5-41: Administration Tab - Incoming Log | 33 |
| Figure 5-42: Administration Tab - Diagnostics | 34 |
| Figure 5-43: The Ping Test | 34 |
| Figure 5-44: The Traceroute Test | 34 |
| Figure 5-45: Administration Tab - Factory Defaults | 35 |
| Figure 5-46: Administration Tab - Firmware Upgrade | 35 |
| Figure 5-47: Status Tab - Router | 36 |
| Figure 5-48: Status Tab - Router with PPPoE IP Connection | 36 |
| Figure 5-49: Status Tab - Local Network | 37 |
| Figure 5-50: DHCP Clients Table | 37 |
| Figure 5-51: Status Tab - Wireless Network | 37 |
| Figure C-1: Upgrade Firmware | 56 |
| Figure E-1: IP Configuration Screen | 58 |
| Figure E-2: MAC Address/Adapter Address | 58 |
| Figure E-3: MAC Address/Physical Address | 58 |
| Figure E-4: MAC Address Filter List | 59 |
| Figure E-5: Wireless Client List | 59 |
| Figure E-6: MAC Address Cloning | 59 |

Chapter 1: Introduction

Welcome

Thank you for choosing the Linksys Wireless-G Broadband Router with RangeBooster. The Wireless-G Broadband Router with RangeBooster will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely and with a greater range of up to twice as far as standard Wireless-G.

How does the Wireless-G Broadband Router with RangeBooster do all of this? A router is a device that allows access to an Internet connection over a network. With the Wireless-G Broadband Router with RangeBooster, this access can be shared over the four switched ports or via the wireless broadcast at up to 11Mbps for Wireless-B or up to 54Mbps for Wireless-G.

Use the WPA standard to secure your wireless network while the whole network is protected through a Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) technology. You can also access the Router's features through the easy-to-use, browser-based utility.

But what does all of this mean?

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

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

PCs equipped with wireless cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wireless Local Area Network. The Wireless-G Broadband Router with RangeBooster bridges wireless networks of both 802.11b and 802.11g standards and wired networks, allowing them to communicate with each other.

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 use the instructions in this Guide to help you connect the Wireless-G Broadband Router with RangeBooster, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Wireless-G Broadband Router with RangeBooster.

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

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

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

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

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

What's in this User Guide?

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

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

Wireless-G Broadband Router with RangeBooster

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

Wireless-G Broadband Router with RangeBooster

The Wireless-G Broadband Router with RangeBooster is compatible with all 802.11b and 802.11g adapters, such as the Notebook Adapters (WPC54G, WPC11) for your laptop computers, PCI Adapter (WMP54G, WMP11) for your desktop PC, and USB Adapter (WUSB54G, WUSB11) when you want to enjoy USB connectivity. The Broadband Router will also communicate with the Wireless PrintServer (WPS54G) and Wireless Ethernet Bridges (WET54G, WET11).

When you wish to connect your wireless network with your wired network, you can use the Wireless-G Broadband Router with RangeBooster's four LAN ports. To add more ports, any of the Wireless-G Broadband Router with RangeBooster's LAN ports can be connected to any of Linksys's switches (such as the SD205 or SD208).

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

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

The Back Panel

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

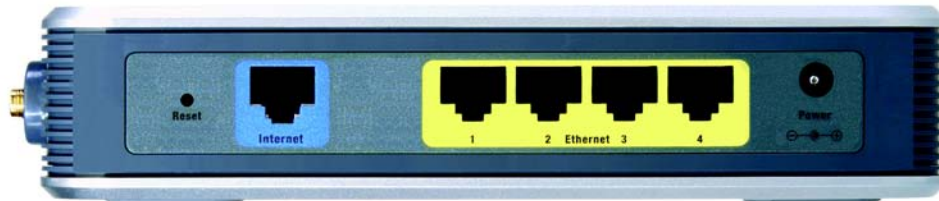


Figure 3-1: The Router's Back Panel

- 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 tab - Factory Defaults in the Router's Web-based Utility.
- Internet** The **Internet** port is where you will connect your broadband Internet connection.
- Ethernet 1, 2, 3, 4** These ports (1, 2, 3, 4) connect the Router to your networked PCs and other Ethernet network devices.
- 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

- | | |
|----------------------------|---|
| Ethernet 1, 2, 3, 4 | Green. These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port. |
| DMZ | Green. The DMZ LED indicates when the DMZ function is being used. This LED will remain lit as long as DMZ is enabled. |
| Internet | Green. The Internet LED lights up when there is a connection made through the Internet port. |
| Wireless | Green. The Wireless LED lights up whenever there is a successful wireless connection. If the LED is flashing, the Router is actively sending or receiving data over the network. |
| Power | Green. The Power LED lights up and will stay on while the Router is powered on. |

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

Hardware Installation for Connection to Your Broadband Modem

1. Power down your network devices.
2. Locate an optimum location for the Router. The best place for the Router is usually at the center of your wireless network, with line of sight to all of your mobile stations.
3. Fix the direction of the antennas. Place the antennas at a 45 degree angle for best performance.
4. Connect a standard Ethernet network cable to the Router's Internet port. Then, connect the other end of the Ethernet cable to your cable or DSL broadband modem.

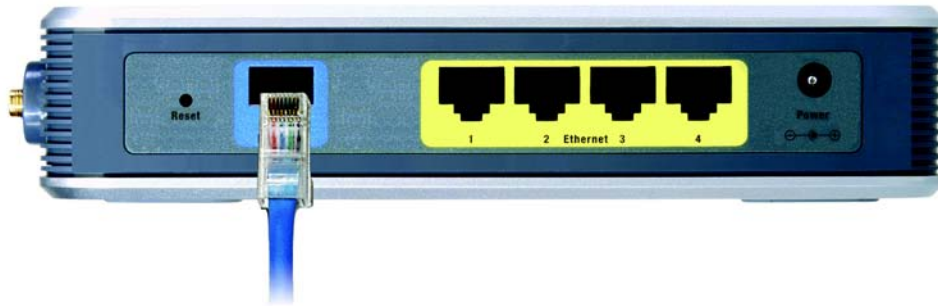


Figure 4-1: Connecting Your Internet Connection

Wireless-G Broadband Router with RangeBooster

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

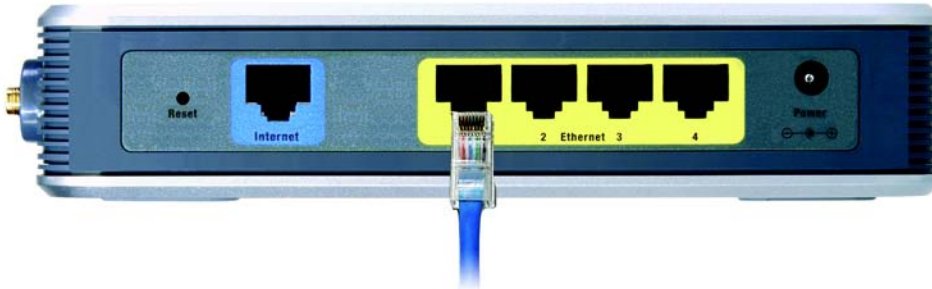


Figure 4-2: Connecting Your Network Devices

6. Connect the AC power adapter to the Router's Power port and the other end into an electrical outlet. Only use the power adapter supplied with the Router. Use of a different adapter may result in product damage.



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

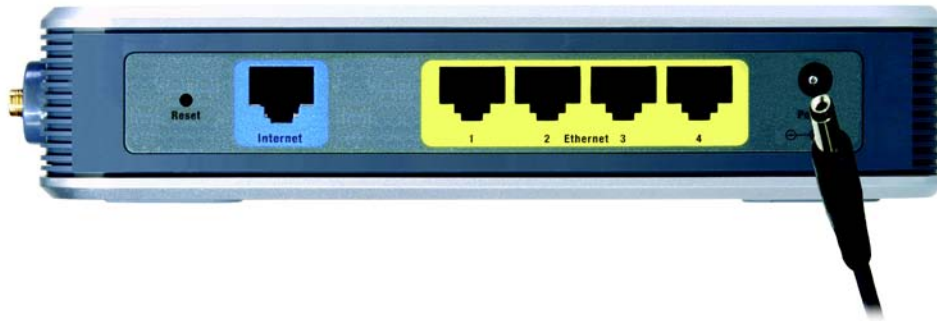


Figure 4-3: Connecting the Power

Now that the hardware installation is complete, proceed to “Chapter 5: Setting up the Wireless-G Broadband Router with RangeBooster,” for directions on how to configure the Router.

Chapter 5: Configuring the Wireless-G Broadband Router with RangeBooster

Overview



NOTE: For first-time installation, Linksys recommends using the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the Web-based Utility.



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

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 in the Utility and each page’s key functions. The utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users will use these two screens of the Utility:

- **Basic Setup.** On the *Basic Setup* screen, enter the settings provided by your ISP.
- **Management.** Click the **Administration** tab and then the **Management** tab. The Router’s default password is **admin**. To secure the Router, change the Password from its default.

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

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

A password request page, shown in Figure 5-1 will appear. (Non-Windows XP users will see a similar screen.) Leave the *User Name* field blank. The first time you open the Web-based Utility, use the default password **admin**. (You can set a new password from the Administration tab’s *Management* screen.) Then click the **OK** button.



Figure 5-1: Password Screen

The Setup Tab - Basic Setup

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

Internet Setup

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

Internet Connection Type

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

- **DHCP.** By default, the Router's Internet Connection Type is set to **Automatic Configuration - DHCP**, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.
- **Static IP.** If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.

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

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

Default Gateway. Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.

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



Figure 5-2: Setup Tab - Basic Setup



Figure 5-3: DHCP Connection Type

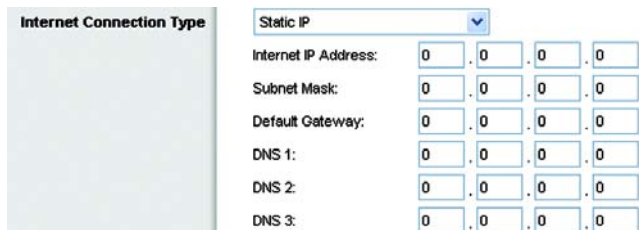


Figure 5-4: Static IP Connection Type

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

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

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

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

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

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

Server IP Address. This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

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

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

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

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

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

Figure 5-5: PPPoE Connection Type

Figure 5-6: PPTP Connection Type

- **HeartBeat Signal.** HeartBeat Signal (HBS) is a service that applies to connections in Australia only. If your ISP is Telstra, then select **HeartBeat Signal**.

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

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.

Optional Settings

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

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

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

MTU. MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The default setting, **Manual**, allows you to enter the largest packet size that will be transmitted. You should leave this value in the 1200 to 1500 range. To have the Router select the best MTU for your Internet connection, select **Auto**.

Network Setup

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

Router IP

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

DHCP Server Settings

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

Internet Connection Type: Heart Beat Signal
Server IP Address: 0 . 0 . 0 . 0
Username:
Password:

Figure 5-7: HeartBeat Signal Connection Type

Optional Settings (required by some Internet Service Providers)
Host Name:
Domain Name:
MTU: Auto Size: 1500

Figure 5-8: Optional Settings

Router IP
IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0

Figure 5-9: Router IP

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

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

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

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

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. If you wish to use another, type that IP Address in one of these fields. You can type 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) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

Static DHCP Client button. The **Static DHCP Client** button is used if you want to assign a fixed IP address to a MAC address. Enter the static local IP address in the *Assign this IP* field, and enter the MAC address of the PC in the *To this MAC* field. Then click the **Enabled** checkbox. When you have finished your entries, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel your changes. To exit this screen, click the **Close** button.

DHCP Client Table button. On the *DHCP Client Table* screen, you will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address. From the *Sort by* drop-down menu, you can sort the table by Client Name, Interface, IP Address, or MAC Address. If you want to add any of the DHCP clients to the Static DHCP Client List, then click the **Save to Static DHCP Client List** checkbox and then click the **Save Settings** button. 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

Change the time zone in which your network functions from this pull-down menu. (You can even automatically adjust for daylight savings time.)

DHCP Server Setting

DHCP Server: Enabled Disabled **Static DHCP**

Start IP Address: 192.168.1.100

Maximum Number of Users: 50

IP Address Range: 192.168.1.100 ~ 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0.0.0.0

Static DNS 2: 0.0.0.0

Static DNS 3: 0.0.0.0

WINS: 0.0.0.0

Figure 5-10: DHCP Server Settings

Static DHCP Client List

DHCP Client Table

| Assign this IP | To this MAC | Enabled |
|----------------|-------------------|--------------------------|
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |
| 192.168.1.0 | 00:00:00:00:00:00 | <input type="checkbox"/> |

Save Settings Cancel Changes Close

Figure 5-11: Static DHCP Client List

DHCP Client Table

Sort by: IP Address

| Client Name | Interface | IP Address | MAC Address | Save to Static DHCP Client List |
|-------------|------------|---------------|-------------------|---------------------------------|
| Linksys 1 | LAN | 192.168.1.100 | 00:40:05:35:0E:01 | <input type="checkbox"/> |
| Linksys 2 | Wireless-A | 192.168.1.101 | 00:40:05:35:0E:02 | <input type="checkbox"/> |
| Linksys 3 | Wireless-B | 192.168.1.102 | 00:40:05:35:0E:03 | <input type="checkbox"/> |
| Linksys 4 | Wireless-D | 192.168.1.103 | 00:40:05:35:0E:02 | <input type="checkbox"/> |

Add Refresh Close

Figure 5-12: DHCP Client Table

Time Zone (GMT-08:00) Pacific Time (USA & Canada)

Automatically adjust clock for daylight saving changes.

Figure 5-13: Time Setting

The Setup Tab - DDNS

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

DDNS.com

DDNS Service. From this pull-down menu, enter the DDNS service with which you have membership.

User Name. Enter the User Name for your DDNS account

Password. Enter the Password for your DDNS account.

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

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

Status. This displays the status of the DDNS connection.

Connect button. Click this button to connect to the service.

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

TZO.com

Email Address. Enter the Email Address of the service you set up with TZO.

TZO Password. Enter the TZO Password Key of the service you set up with TZO.

Domain Name. Enter the Domain Name of the service you set up with TZO.

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

Status. This displays the status of the DDNS connection.

Connect button. Click this button to connect to the service.



Figure 5-14: Setup Tab - DDNS.com



Figure 5-15: 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. 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.

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

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

Clone My PC's MAC. Clicking this button will clone the MAC address.

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



Figure 5-16: Setup Tab - MAC Address Clone

The Setup Tab - Advanced Routing

This tab is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing will automatically adjust how packets travel on your network. Static Routing sets up a fixed route to another network destination.

NAT. If this Router is hosting your network's connection to the Internet, select **Enable**. If another Router exists on your network, select **Disable**. When Router is chosen, **Dynamic Routing** will be enabled.

Dynamic Routing (RIP). 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. When setting this up, remember that the settings on the receiving and transmitting side **must** be the same.

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

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

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

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

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

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

Click the **Show Routing Table** button to view the Static Routes you've already set up. Click the **Refresh** button to refresh the screen. Click the **Close** button to close the window and return to the *Advanced Routing* screen.

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

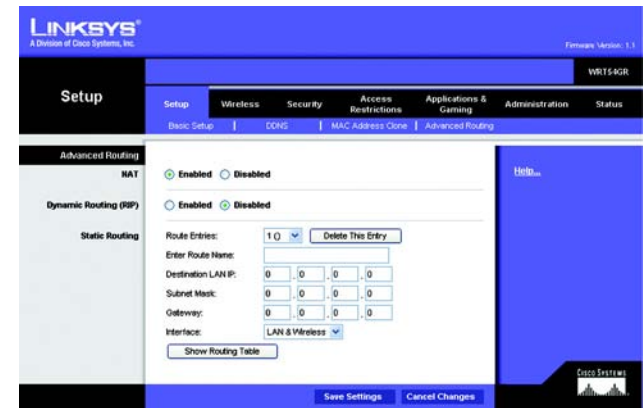


Figure 5-17: Setup Tab - Advanced Routing



Figure 5-18: Setup Tab - Routing Table

The Wireless Tab - Basic Wireless Settings

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

Wireless. Select **Enabled** to enable wireless capabilities or **Disabled** to disable wireless.

Network Mode. From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed**. If you have only 802.11g devices, select **Wireless G-Only**. If you have only 802.11b devices, select **Wireless B-Only**. If you do not have any 802.11g and 802.11b devices in your network, select **Disable**.

Wireless Network Name (SSID). The SSID is the network name shared among all devices 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 devices in your wireless network. For added security, you should change the default SSID (**linksys**) to a unique name.

Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on the same channel in order to function correctly.

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

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



Figure 5-19: Wireless Tab - Basic Wireless Settings

The Wireless Tab - Wireless Security

The Wireless Security settings configure the security of your wireless network. There are four wireless security mode options supported by the Router: WEP, WPA Personal, PSK2, PSK2-Mixed, WPA-Enterprise, PSK2 + RADIUS, and RADIUS. (WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA is a stronger security method than WEP. PSK2 stands for Pre-shared Key 2, and is stronger than WPA-Personal. RADIUS stands for Remote Authentication Dial-In User Service.) These seven are briefly discussed here.

WEP. WEP is a basic encryption method, which is not as secure as WPA Personal. To use WEP, select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**. Then either generate a WEP key using the Passphrase or enter the WEP key manually and select a TX (Transmit) Key (choose which Key to use).

WPA-Personal. WPA gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of encryption, **TKIP** or **AES**. Enter a passphrase (pre-shared key) of 8-63 characters. Then enter a Key Renewal period, which instructs the Router how often it should change the encryption keys.



IMPORTANT: If you are using WEP encryption, always remember that each device in your wireless network **MUST** use the same WEP encryption method and encryption key, or else your wireless network will not function properly.



Figure 5-20: Wireless Tab - Wireless Security (WEP)



Figure 5-21: Wireless Tab - Wireless Security (WPA-Personal)



IMPORTANT: If you are using WPA Personal, always remember that each device in your wireless network **MUST** use the same WPA Personal method and passphrase, or else the network will not function properly.

PSK2. PSK2 is stronger than WPA Personal and gives you one encryption method, AES, with dynamic encryption keys. Enter a Passphrase of 8-63 characters. Then enter a Key Renewal period, which instructs the Router how often it should change the encryption keys.

PSK2-Mixed. PSK2-Mixed gives you either WPA-Personal (TKIP) or PSK2 (AES) encryption. Enter a Passphrase of 8-63 characters. Then enter a Key Renewal period, which instructs the Router how often it should change the encryption keys.

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.) First, select the type of WPA encryption you want to use, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a shared secret (authentication key) between the Router and the server. Last, enter a Key Renewal Timeout, which instructs the Router how often it should change the encryption keys.



Figure 5-22: Wireless Tab - Wireless Security (PSK2)



Figure 5-23: Wireless Tab - Wireless Security (RPSK2-Mixed)



Figure 5-24: Wireless Tab - Wireless Security (WPA Enterprise)

PSK2 + RADIUS. This option features a PSK2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) AES is the type of encryption method used. Enter the RADIUS server's IP address and port number, along with the shared secret (authentication key) shared by the Router and the server. Last, enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.



Figure 5-25: Wireless Tab - Wireless Security (PSK2 + RADIUS)

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.) First, enter the RADIUS server's IP Address and port number, along with a shared secret (authentic key) shared between the Router and the server. Then, select a level of WEP encryption, **40/64 bits 10 hex digits** or **104/128 bits 26 hex digits** and either generate a WEP key using the Passphrase or enter the WEP key manually, and lastly, select a Default Transmit Key (choose which Key to use).



Figure 5-26: Wireless Tab - Wireless Security (RADIUS)

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

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 Restriction

Prevent PCs listed below from accessing the wireless network. Clicking this button will block wireless access by MAC Address.

Permit PCs listed below to access the wireless network. Clicking this button will allow wireless access by MAC Address.

MAC Address Filter List

You can manually enter a MAC address to filter or you can select one from the Wireless Client List.

Wireless Client List. Click the **Wireless Client MAC List** button to display a list of wireless network users. From the *To Sort by* drop-down menu, you can sort the table by Client Name, IP Address, MAC Address, Interface, or Client Name. To add a client's MAC Address to your MAC Address Filter list, click the **Save to MAC Address Filter List** checkbox and click the **Add** button. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

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

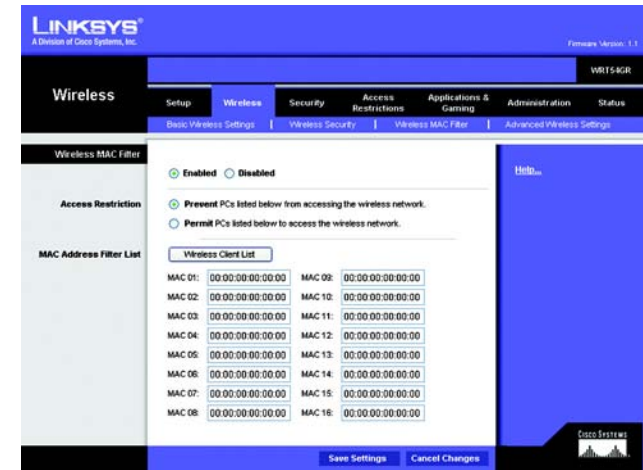


Figure 5-27: Wireless Tab - Wireless MAC Filter

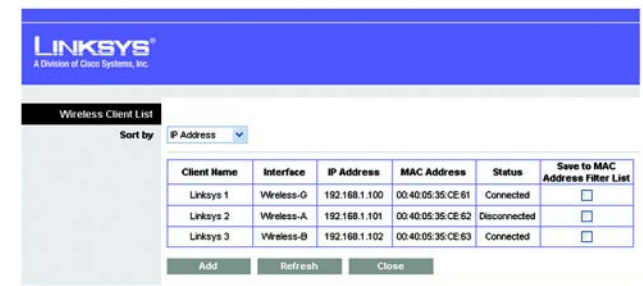


Figure 5-28: Wireless Client List

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

Frame Burst Mode. Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. The default setting is **Enabled**.

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.

Authentication Type. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With **Open System** authentication, the sender and the recipient do NOT use a WEP key for authentication. With **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. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

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**.

Transmission Power. The greater the transmission power used, the larger the area a wireless network covers. To minimize the likelihood of eavesdropping by unauthorized wireless users, do not use more transmission power than necessary to cover the range needed by your wireless network. Try using the Router at different levels of transmission power, and determine how much power is needed to reach the wireless client, such as a PC or access point, that is farthest from the Router. Then select the appropriate level, **Full**, **Half**, **Quarter**, **Eighth**, or **Min**, from the drop-down menu. The default setting is **Full**.

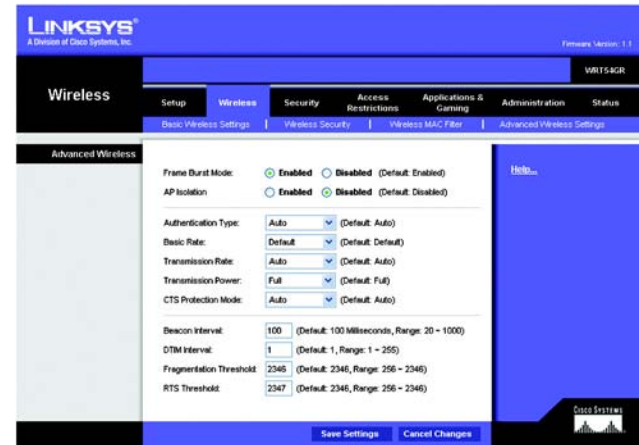


Figure 5-29: Wireless Tab - Advanced Wireless Settings

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-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance.

Beacon Interval. 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 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. The default value is **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. The default value is **2346**.

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

The Security Tab - Firewall

The *Firewall* screen offers filters that block specific Internet data types and block anonymous Internet requests. Select the checkbox to enable a feature.

Firewall

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

Internet Filter

Filter Anonymous Internet Requests. When enabled, this feature keeps your network from being “pinged,” or detected, by other Internet users. It also reinforces your network security by hiding your network ports. Both functions of this feature make it more difficult for outside users to work their way into your network. This feature 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 Filters

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.

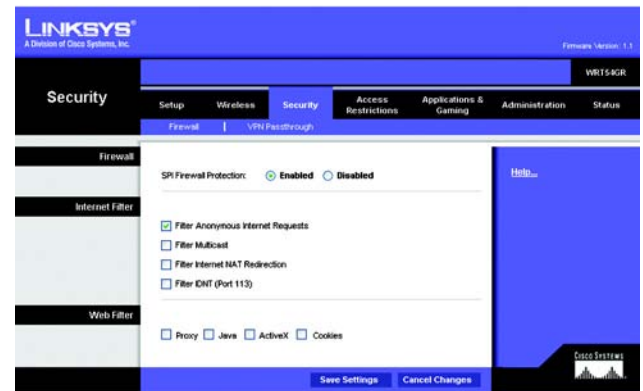


Figure 5-30: Security Tab - Firewall

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

The Security Tab - VPN Passthrough

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

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

L2TP Pass-through. Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, click **Enable**. L2TP Pass-Through is enabled by default.

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

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

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, and websites 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 view. 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 tab, click the **Close** button.



Figure 5-31: Security Tab - VPN Passthrough



Figure 5-32: Access Restrictions Tab - Internet Access Policy

To create an Internet Access 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 **Enabled**.
4. Click the **Edit List** button to select which PCs will be affected by the policy. The *Internet Access PCs List* screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button.
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**.
7. You can also block access by URL address by entering it in the *Website Blocking by URL Address* field or by Keyword by entering it in the *Website Blocking by Keyword* field. Click the >> button to add a selection to the Blocked Applications list.
8. You can filter access to various applications accessed over the Internet, such as FTP or telnet, by selecting up to three applications from the drop-down menus under *Applications*.

If the application you want to block is not listed or you want to edit an application's settings, then create a new one by entering an Application Name, Port Range, and Protocol. Then, click **Add**.

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



Figure 5-33: Internet Policy Summary

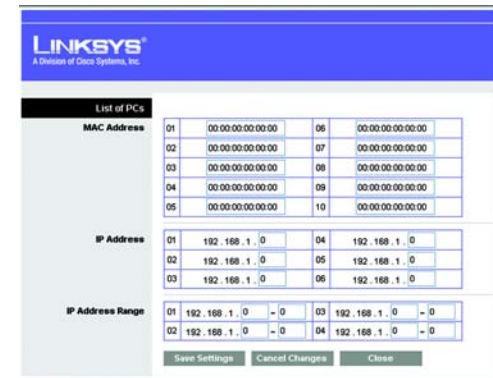


Figure 5-34: List of PCs

The Applications and Gaming Tab - Single Port Forwarding

Single Port Forwarding

The Single Port Forwarding screen provides options for customization of port services for common applications.

When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate computer. Any computer whose port is being forwarded should 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.

Select the pre-configured Application, or manually enter it in the field. Then, enter the External and Internal Port numbers in the fields. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**. Enter the IP Address in the field. Click **Enabled** to enable Forwarding for the chosen application.

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

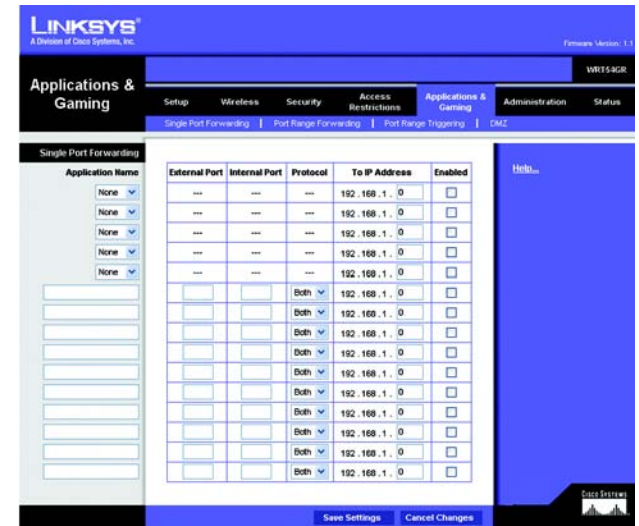


Figure 5-35: Applications and Gaming Tab - Single Port Forwarding

The Applications and Gaming Tab - Port Range Forwarding

The Applications and Gaming Tab allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

To forward a port, enter the information on each line for the criteria required. The criteria are described here.

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

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

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

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

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

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

| Application Name | Start - End Port | Protocol | To IP Address | Enabled |
|----------------------|---|----------|---------------|--------------------------|
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> - <input type="text"/> | Both | 192.168.1.0 | <input type="checkbox"/> |

Figure 5-36: Applications and Gaming Tab - Port Range Forward

The Applications & Gaming Tab - Port Range Triggering

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

Port Triggering Range

Application Name. Enter the application name of the trigger.

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

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

Enabled. Select **Enabled** to enable the application.

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

The Applications and Gaming Tab - DMZ

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

To expose one PC, select **Enabled**.

Source IP Address. If you want to allow any Internet IP address to access the exposed computer, select **Any IP Address**. If you want to allow a specific IP address or range of IP addresses to access the exposed computer, select the second option and enter the IP address or range of IP addresses in the fields provided.

Destination. Enter the IP address or MAC Address of the computer you want to expose.

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



Figure 5-37: Applications and Gaming Tab - Port Triggering



Figure 5-38: Applications and Gaming Tab - DMZ

The Administration Tab - Management

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

Management

Router Access

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

Web Access

Web Utility Access. HTTP (HyperText Transport Protocol) - 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 your Wireless 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 web-based utility via a wired connection if you disable the setting. Select **Enable** to enable wireless access to the Router's web-based utility or **Disable** to disable wireless access to the utility.

Remote Access



Note: When you are in a remote location and wish to manage the Router, enter `http://<Internet IP Address>: port`. 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`.

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

Web Utility Access. HTTP (HyperText Transport Protocol) - 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**.

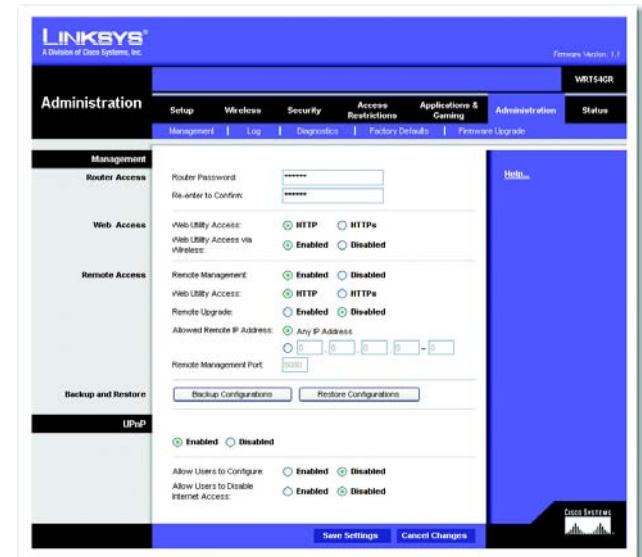


Figure 5-39: Administration Tab - Management

Allow 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.

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.)

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**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

The Administration Tab - Log

The Router can keep logs of all traffic for your Internet connection.

Log

To disable the Log function, keep the default setting, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**.

Logviewer IP Address. For a permanent record of the Router's activity logs, Logviewer software must be used. This software can be downloaded from the Linksys website, www.linksys.com. The Log viewer saves all incoming and outgoing activity in a permanent file on your PC's hard drive. In the *Logviewer IP Address* field, enter the fixed IP address of the PC running the Log viewer software. The Router will now send updated logs to that PC.

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 Port Numbers for the incoming Internet traffic. The Outgoing Log will display a temporary log of the Source IP Addresses, Destination IP Address and Port Numbers for the outgoing Internet traffic. The Security log will display the login information for the Web 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.

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



Figure 5-40: Administration Tab - Log

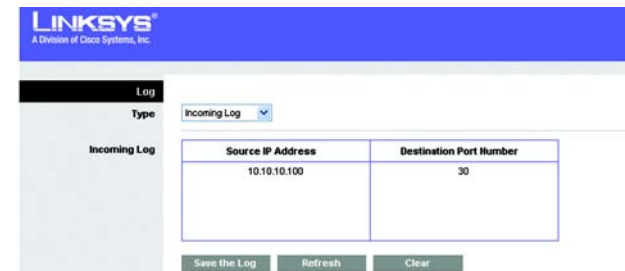


Figure 5-41: Administration Tab - Incoming Log

The Administration Tab - Diagnostics

The Ping test allows you to check the status of your Internet connection.

Ping Test. The Ping test will check the status of a connection. Enter the address of the PC whose connection you wish to test, the packet size, 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 address 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.

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



Figure 5-42: Administration Tab - Diagnostics

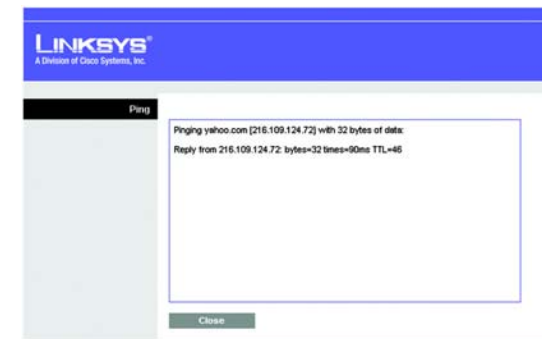


Figure 5-43: The Ping Test

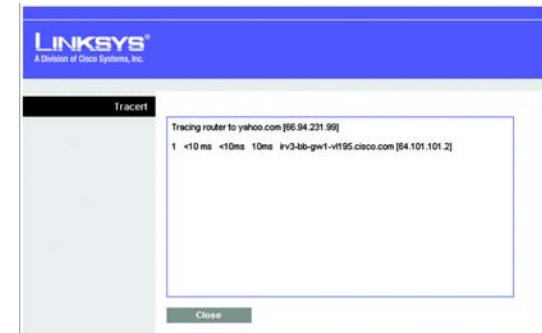


Figure 5-44: The Traceroute Test