LINKSYS®

A Division of Cisco Systems, Inc.

Compact Wireless- G Broadband Router

WIRELESS

User Guide

CISCO SYSTEMS

Model No. **WRT54GC ver. 2.0**

Copyright and Trademarks

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

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

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

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

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

word: *definition.*

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

Figure 0-1: Sample Figure Description

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

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

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

How does the Compact Wireless-G Broadband Router do all of this? A router is a device that allows access to an Internet connection over a network. With the Compact Wireless-G Broadband Router, this access can be shared over the four switched ports or via the wireless broadcast at either up to 11Mbps for Wireless-B or up to 54Mbps for Wireless-G. In addition, the whole network is protected by NAT technology. For wireless networking, you also have a choice of wireless security methods. Additional security features, as well as configuration options, are accessible 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 Compact Wireless-G Broadband Router bridges wireless networks of 802.11a, 802.11b, and 802.11g standards and wired networks, allowing them to communicate with each other.

With your wired and wireless networks connected to each other and the Internet, you can now share files and Internet access—and even play games. All the while, the Compact Wireless-G Broadband Router protects your networks from unauthorized and unwelcome users.

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 Compact Wireless-G Broadband Router, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Compact Wireless-G Broadband Router.

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

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

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

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

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

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

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

What's in this Guide?

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

- Chapter 1: Introduction
  This chapter describes the Router's applications and this User Guide.

- Chapter 2: Planning Your Wireless Network
  This chapter describes the basics of wireless networking.

- Chapter 3: Getting to Know the Compact Wireless-G Broadband Router
  This chapter describes the physical features of the Router.

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

- Chapter 5: Configuring the Compact Wireless-G Broadband Router
  This chapter explains how to use the Web-Based Utility to configure the settings on the Compact Wireless-G Broadband Router.

- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Compact Wireless-G Broadband Router.

- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.

- Appendix C: Upgrading Firmware
  This appendix instructs you on how to upgrade the 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.

- 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.

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.

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 Compact Wireless-G Broadband Router, which serves as the main point of communications in a wireless network. The Router transmits data to PCs equipped with wireless network adapters, which can roam within a certain radial range of the Router. You can arrange the Router and multiple access points to work in succession to extend the roaming range, and you can set up your wireless network to communicate with your Ethernet hardware as well.

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

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

***ssid**: your wireless network’s name.*

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

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

***adapter**: a device that adds network functionality to your PC.*

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

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

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

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

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

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

The Back Panel

The Router's ports are located on the back panel of the Router.

***port**: the connection point on a computer or networking device used for plugging in cables or adapters.*

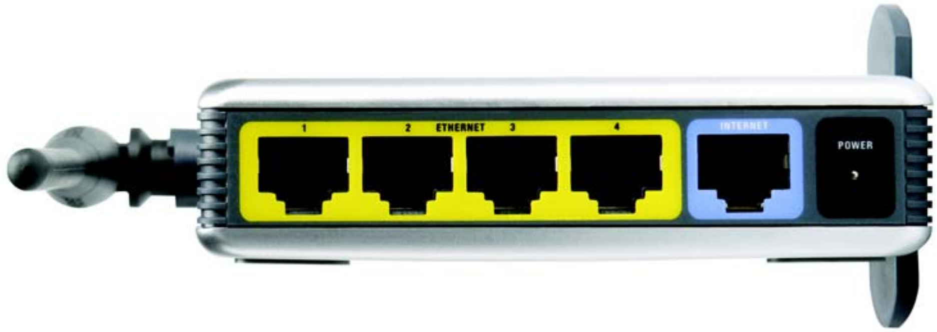


Figure 3-1: The Router's Back Panel

ETHERNET 1, 2, 3, 4 These ports (1, 2, 3, 4) connect the Router to your networked PCs and other Ethernet network devices.

INTERNET The **Internet** port is where you will connect your broadband Internet connection.

***broadband**: an always-on, fast Internet connection.*

POWER The **POWER** port is where you will connect the power adapter.

The Front Panel

The Router’s LEDs, which indicate the status of the Router and network activities, are located on the front panel.

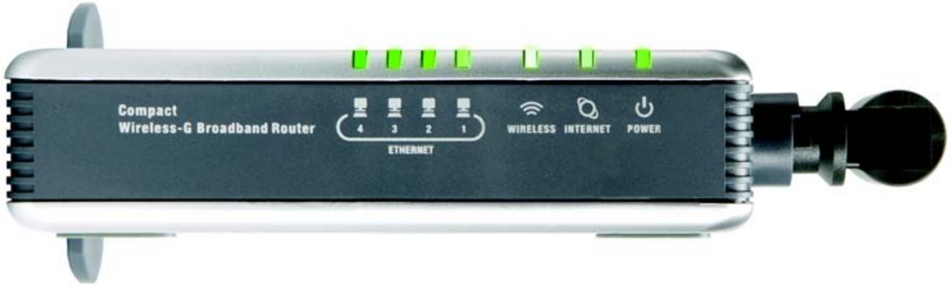


Figure 3-2: The Router’s Front Panel

ETHERNET 1-4 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 connected to a device through that port. A flashing LED indicates network activity over that port.

WIRELESS Green. The **WIRELESS** LED flashes when there is a successful wireless connection.

INTERNET Green. The **INTERNET** LED lights up when there is a connection through the Internet port.

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

The Bottom Panel

The Router's Reset button is located on the bottom panel. To access the button, turn the stand perpendicular to the Router. Use a sharp object like a pencil to push in the button.

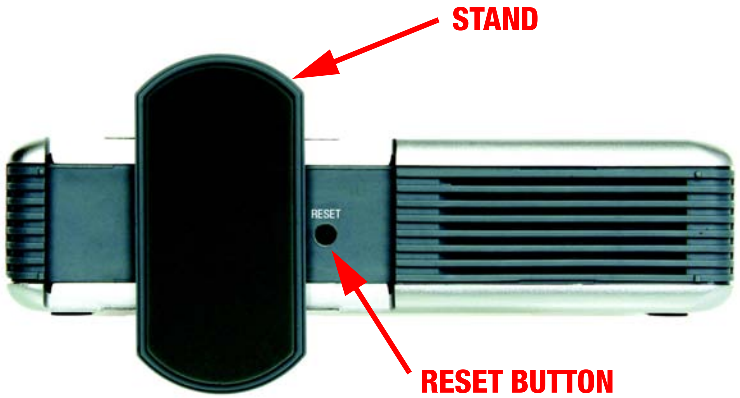


Figure 3-3: The Router's Bottom Panel

RESET Button There are two ways to reset the Router's factory defaults. Either press the **RESET button**, for approximately eight seconds, or restore the defaults from the Administration tab - Factory Defaults in the Router's Web-based Utility.

⚠ **IMPORTANT:** If you reset the Router, all of your settings, including Internet connection, wireless, and security, will be deleted and replaced with the factory defaults. Do not reset the Router if you want to retain these settings.

Chapter 4: Connecting the Compact Wireless-G Broadband Router

Overview

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

This chapter includes two sets of instructions. If the Compact Wireless-G Broadband Router will be the only router in your network, follow the instructions in “Hardware Installation for Connection to Your Broadband Modem.” If you want to install the Compact Wireless-G Broadband Router behind another router in your network, then follow the instructions in “Hardware Installation for Connection to Another Router.”

NOTE: For first-time installation of the Router, Linksys recommends using the Setup Wizard on the Setup CD-ROM.

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 wireless devices. Normally, the higher you place the antenna, the better the performance will be.

3. Connect a standard Ethernet network cable from the Router’s Internet port to your broadband modem.

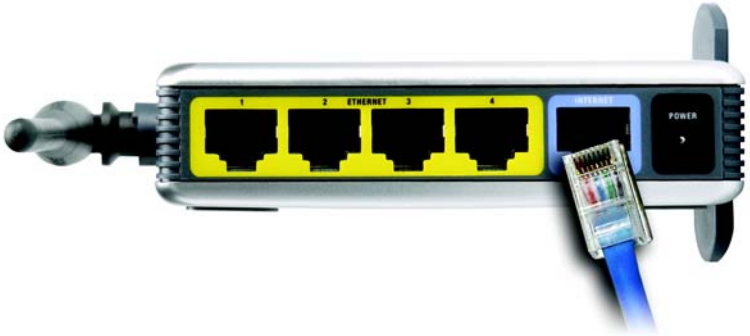


Figure 4-1: Connecting your Broadband Modem

4. Connect a standard Ethernet network cable from one of the Router’s numbered ports to your network PC or Ethernet device.

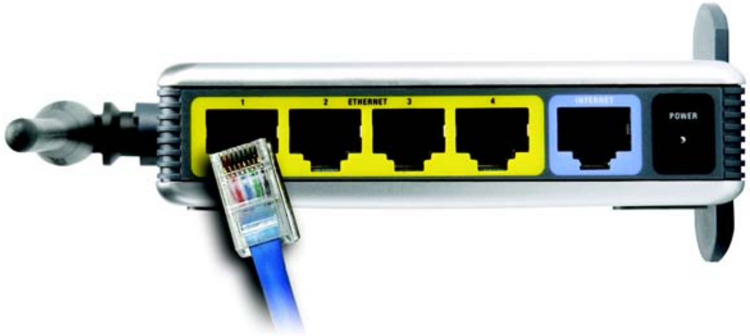


Figure 4-2: Connecting Your Network Devices

5. Connect the AC power adapter to the Router's Power port. Then connect the other end to an electrical outlet. Only use the power adapter supplied with the Router. Use of a different adapter can cause product damage.

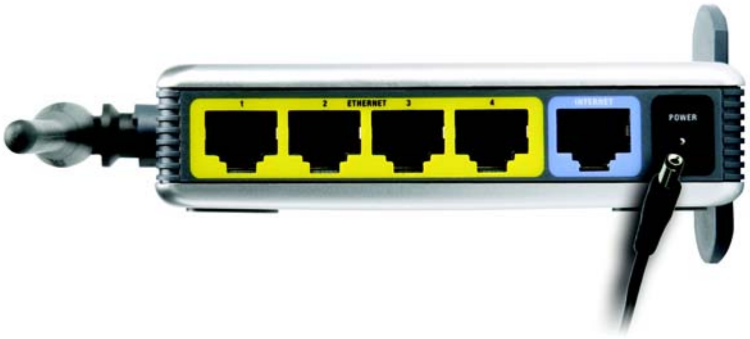


Figure 4-3: Connecting the Power

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

Now that the hardware installation is complete, proceed to “Chapter 5: Configuring the Compact Wireless-G Broadband Router.”

Hardware Installation for Connection to Another Router

Before you install the Router, you must change the default IP address of the other router. This is mandatory because both routers may be set to the same IP address by default. If you do not change the other router's default IP address, then you may not be able to set up the Router.

First, make sure the Router is NOT connected to your network. Then follow these instructions:

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

2. A password request page will appear. Leave the *User Name* field blank. In the *Password* field, enter the password you have set (the default password is **admin**). Then click the **OK** button.

3. The first screen that appears will display the Setup tab. In the *Network Setup* section, there is a setting called *Local IP Address* (also called *Router IP*), which is set to 192.168.1.1. Change this to **192.168.2.1**.

4. Click the **Save Settings** button to save your change, and then exit the Web-based Utility.

5. Power down your network devices. Now you will begin the hardware installation of the Router.

6. 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. Normally, the higher you place the antenna, the better the performance will be.

7. Connect a standard Ethernet network cable to the Router's Internet port. Then, connect the other end of the Ethernet cable to one of the numbered Ethernet ports on your other router.

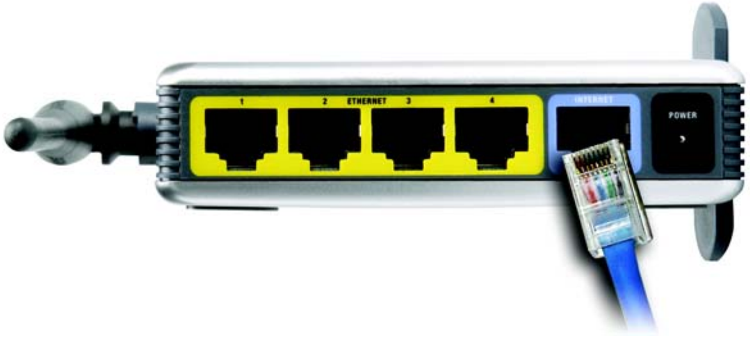


Figure 4-5: Connecting Another Router

NOTE: Steps 1-4 are instructions for a typical Linksys router; however, if you are using a non-Linksys router, refer to the other router's documentation for instructions on how to change its local IP address to 192.168.2.1.

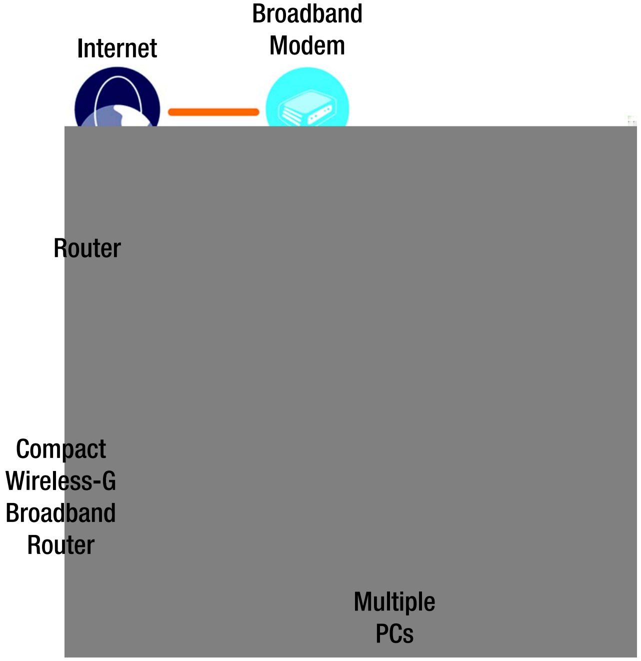


Figure 4-4: Diagram for Connection to Another Router

8. Decide which network computers or Ethernet devices you want to connect to the Router.

   Disconnect the selected computers or devices from the other router, and then connect them to the Router's numbered ports using standard Ethernet network cabling.

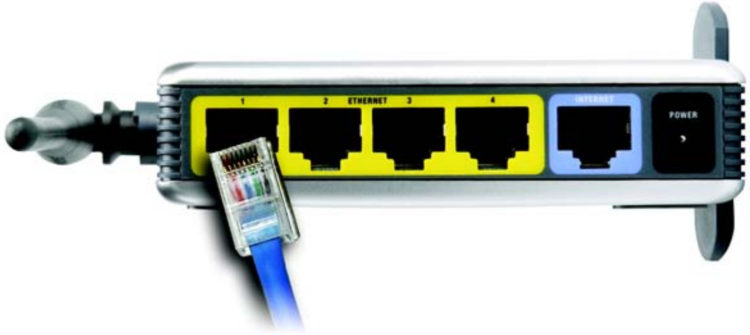


Figure 4-6: Connecting Your Network Devices

9. 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.

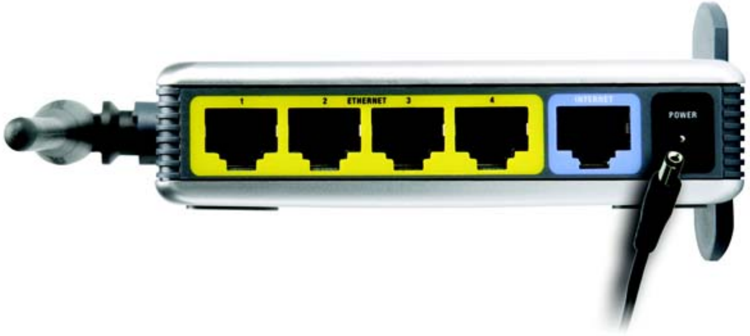


Figure 4-7: Connecting the Power

Now that the hardware installation is complete, proceed to "Chapter 5: Configuring the Compact Wireless-G Broadband Router."

Chapter 5: Configuring the Compact Wireless-G Broadband Router

Overview

Linksys recommends using the Setup Wizard on the Setup CD-ROM for first-time installation of the Router. For advanced users, you may follow the instructions in the previous chapter, “Chapter 4: Connecting the Compact Wireless-G Broadband Router”, and then configure the Router through its 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.

Make the necessary changes through the Web-based Utility. On each screen, 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.

NOTE: For first-time installation of the Router, Linksys recommends using the Setup Wizard on the Setup CD-ROM.

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.

How to Access the Web-based Utility

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

A password request page will appear. 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.

The Setup Tab - Basic Setup

The first screen that appears displays the Setup tab. This allows you to change the Router's general settings.

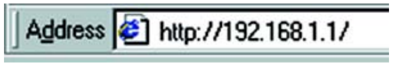
Internet Setup

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

Internet Connection Type

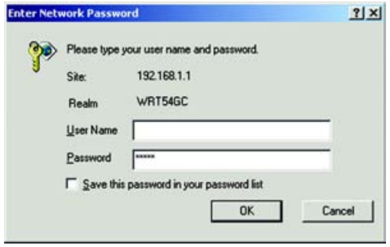
Choose the type of Internet connection your ISP provides from the drop-down menu.

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



Address http://192.168.1.1/

Figure 5-1: Router's IP Address



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm WRT54GC

User Name

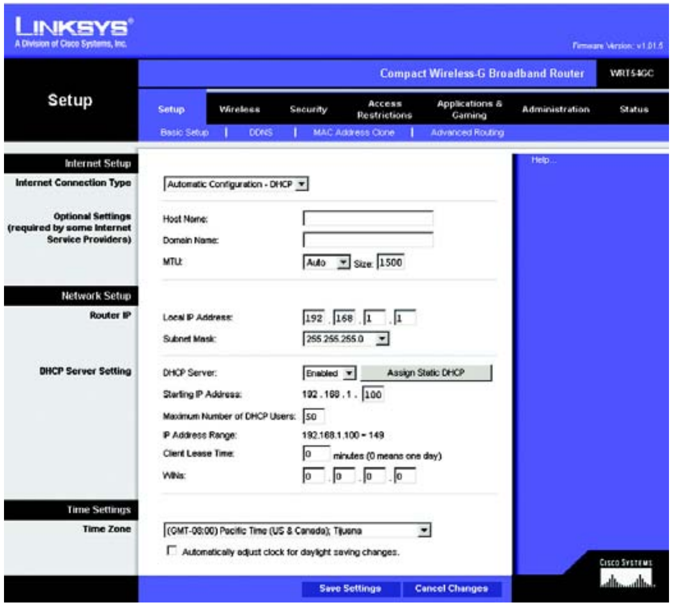
Password *****

□ Save this password in your password list

Figure 5-2: Router Login Screen

***ip** (internet protocol): a protocol used to send data over a network.*

***ip address**: the address used to identify a computer or device on a network.*



Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

Network Setup

Router IP

Local IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

DHCP Server Setting

DHCP Server: Enabled

Starting IP Address: 192 . 168 . 1 . 100

Maximum Number of DHCP Users: 50

IP Address Range: 192.168.1.100 ~ 149

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

WINs: 0 . 0 . 0 . 0

Time Settings

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

□ Automatically adjust clock for daylight saving changes.

Figure 5-3: Setup Tab - Basic Setup

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

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

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

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

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

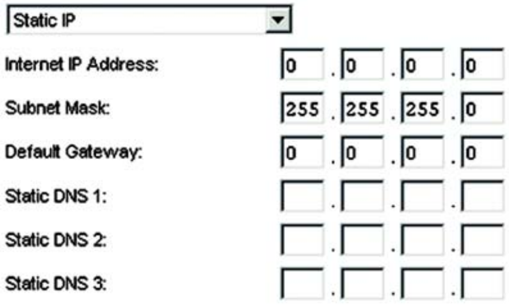
- **PPTP**. Point-to-Point Tunneling Protocol (**PPTP**) is a service that applies to connections in Europe only.

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

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

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

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



Static IP

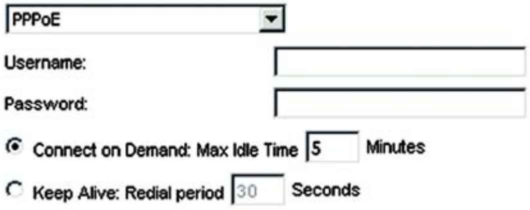
Internet IP Address:	0 . 0 . 0 . 0
Subnet Mask:	255 . 255 . 255 . 0
Default Gateway:	0 . 0 . 0 . 0
Static DNS 1:	. . .
Static DNS 2:	. . .
Static DNS 3:	. . .

Figure 5-4: Static IP Connection Type

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

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

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



PPPoE

Username:

Password:

● Connect on Demand: Max Idle Time 5 Minutes

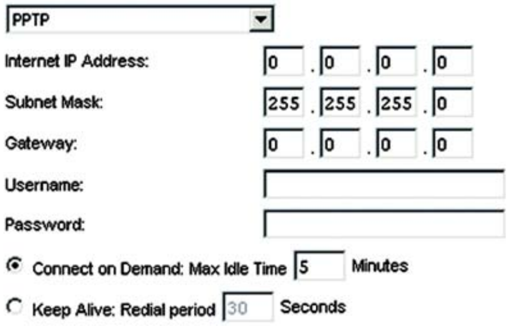
○ Keep Alive: Redial period 30 Seconds

Figure 5-5: PPPoE Connection Type

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

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 ▼

Internet IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 0 . 0 . 0 . 0

Username:

Password:

● Connect on Demand: Max Idle Time 5 Minutes

○ Keep Alive: Redial period 30 Seconds

Figure 5-6: PPTP Connection Type

Optional Settings

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

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

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

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

Network Setup

The Network Setup section changes the Router’s local network settings. Changes to the Router’s wireless network settings are performed through the Wireless tab.

Router IP

IP Address and Subnet Mask. This shows both the Router’s IP Address and Subnet Mask, as seen by your network. The default IP Address is **192.168.1.1**, and the default Subnet Mask is **255.255.255.0**. In most cases, keeping the default values will work.

DHCP Server Settings

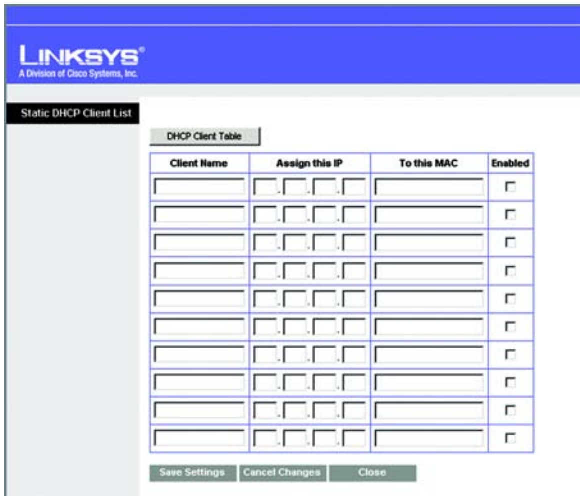
The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option,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

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

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 select **Disabled** (no other DHCP features will be available).

Assign Static DHCP. Every time a PC reboots, it is assigned a new local IP address by the Router. If you want a PC to be assigned the same IP address every time it reboots, then click the **Assign Static IP** button.

On the *Static DHCP Client List* screen, enter a client name, then 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.



Client Name	Assign this IP	To this MAC	Enabled
	. . .		☐
	. . .		☐
	. . .		☐
	. . .		☐
	. . .		☐
	. . .		☐
	. . .		☐
	. . .		☐
	. . .		☐
	. . .		☐

Figure 5-7: Static DHCP Client List

If you want to see a list of DHCP clients, click the **DHCP Client Table** button. On the *DHCP Client Table* screen, you will see a list of DHCP clients with the following information: Client Names, Interfaces, IP Addresses, and MAC Addresses. From the *To Sort by* drop-down menu, you can sort the table by Client Name, Interface, IP Address, or MAC Address. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

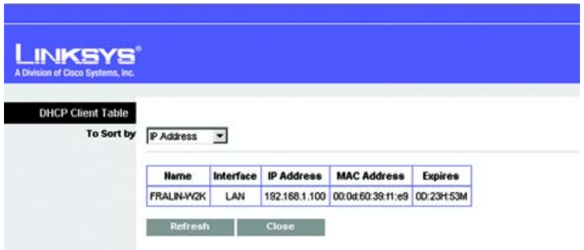
Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. The default Starting IP Address is **192.168.1.100.**

Maximum Number of 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.**

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

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.

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.



To Sort by: IP Address

Name	Interface	IP Address	MAC Address	Expires
FRALIN-W2K	LAN	192.168.1.100	00:0d:60:39:f1:e9	0D:23H:53M

Figure 5-8: DHCP Client Table

Time Settings

Change the time zone in which your network functions from this pull-down menu. Click the checkbox if you want the Router to automatically adjust for daylight savings time.

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.

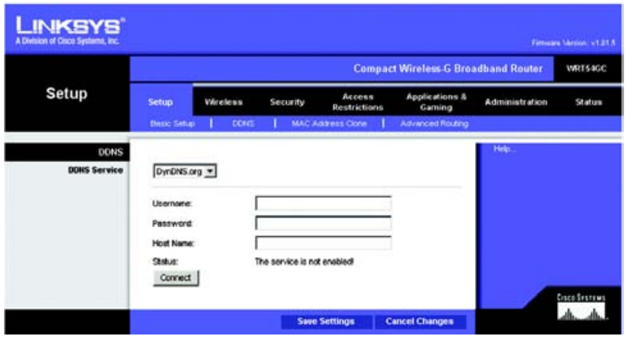
The Setup Tab - DDNS

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.



DDNS

DDNS Service: DynDNS.org

Username:

Password:

Host Name:

Status: The service is not enabled!

Figure 5-9: DynDNS.org

DynDNS.org

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

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

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

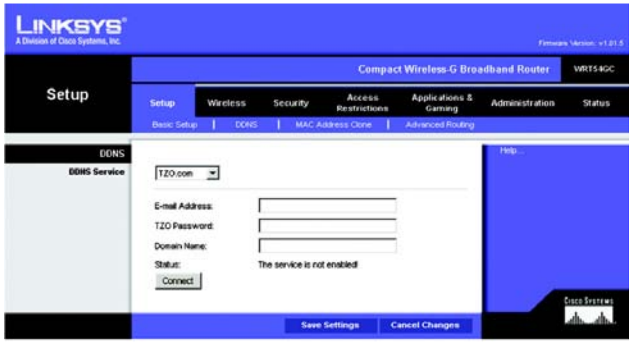
TZO.com

E-mail Address, Password, and Domain Name. Enter the Email Address, Password, and 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. The status of the DDNS service connection is displayed here.

When you have finished making changes to this screen, 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.



DDNS Service: TZO.com

E-mail Address:

TZO Password:

Domain Name:

Status: The service is not enabled!

Figure 5-10: 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.

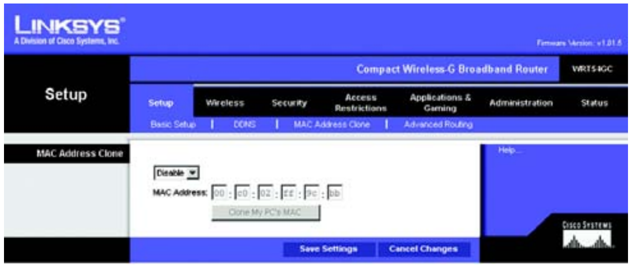
MAC Address Clone

Enabled/Disabled. To have the MAC Address cloned, select **Enabled** from the drop-down menu.

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

Clone My PC's MAC. Clicking this button will clone the MAC address of the PC you are currently using.

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.



MAC Address Clone: Disable

MAC Address: 00 : c0 : 02 : ff : 9c : bb

Figure 5-11: Setup Tab - MAC Address Clone

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

The Setup Tab - Advanced Routing

This tab is used to set up the Router's advanced functions. 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.

Operating Mode. Select the mode in which this Router will function. If this Router is hosting your network's connection to the Internet, select **Gateway**. If another Router exists on your network, select **Router**. When Router is chosen, **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. This feature is **Disabled** by default. From the drop-down menu, you can also select **LAN & Wireless**, which performs dynamic routing over your Ethernet and wireless networks. You can also select **WAN**, which performs dynamic routing with data coming from the Internet. Finally, selecting **Both** enables dynamic routing for both networks, as well as data from the Internet.

Static Routing. To set up a static route between the Router and another network, select a number from the *Static Routing* 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.

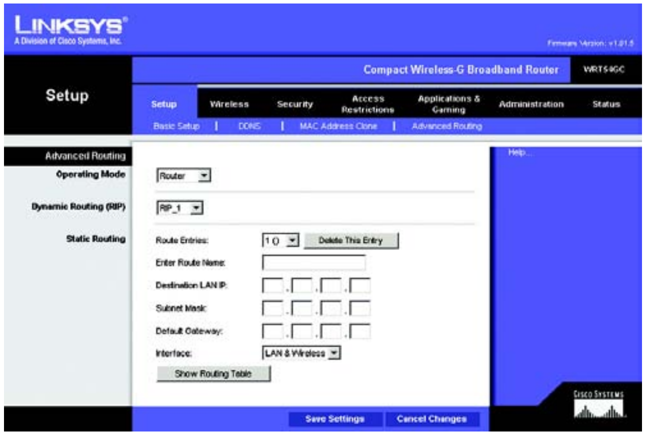
Subnet Mask. The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

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

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

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

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



Operating Mode: Router

Dynamic Routing (RIP): RIP_1

Static Routing

Route Entries: 1 ( )

Enter Route Name:

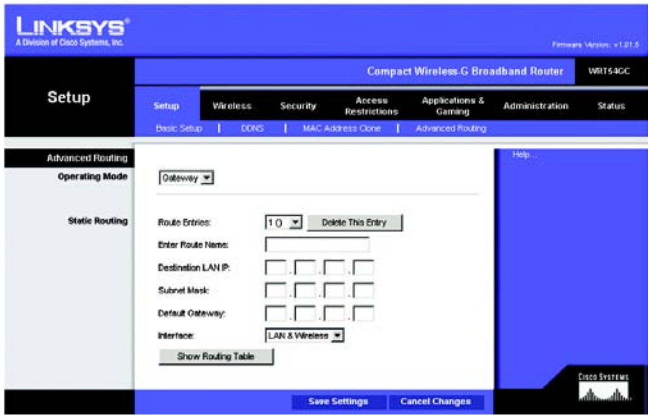
Destination LAN IP: . . .

Subnet Mask: . . .

Default Gateway: . . .

Interface: LAN & Wireless

Figure 5-12: Setup Tab - Advanced Routing (Gateway)



Operating Mode: Gateway

Static Routing

Route Entries: 1 ( )

Enter Route Name:

Destination LAN IP: . . .

Subnet Mask: . . .

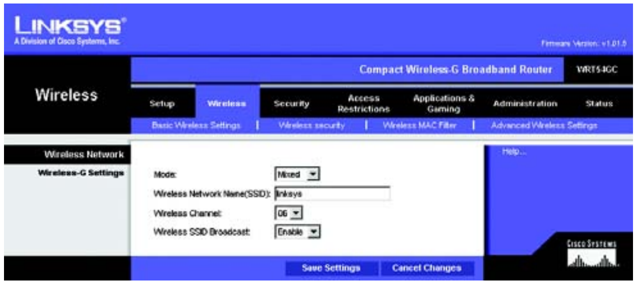
Default Gateway: . . .

Interface: LAN & Wireless

Figure 5-13: Setup Tab - Advanced Routing (Router)

The Wireless Tab - Basic Wireless Settings

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



Mode: Mixed

Wireless Network Name(SSID): linksys

Wireless Channel: 06

Wireless SSID Broadcast: Enable

Figure 5-14: Wireless Tab - Basic Wireless Settings

Wireless Network

Wireless-G Settings

Mode. From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed.** If you have only 802.11g devices, select **G Only.** If you have only 802.11b devices, select **B Only.**

Network Name (SSID). The SSID is the network name shared by 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 keyboard characters in length. 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 broadcast on the same channel in order to communicate.

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.**

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.

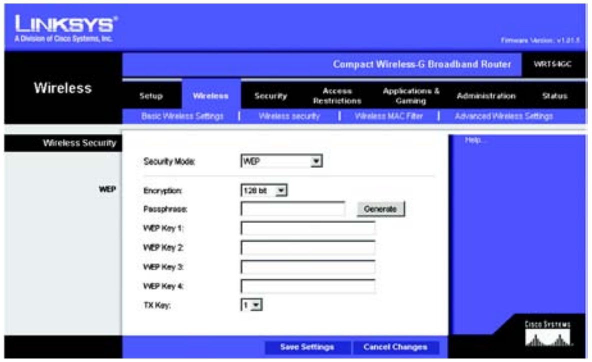
The Wireless Tab - Wireless Security

The Wireless Security settings configure the security of your wireless network. There are three wireless security mode options supported by the Router: WPA Personal, WPA2 Personal, WPA2 Mixed Mode and WEP. (WEP stands for Wired Equivalent Privacy). These four are briefly discussed here. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."

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

Wireless Security

WEP. WEP is a basic encryption method. Select a level of WEP encryption, **64-bit** or **128-bit**. If you want to use a Passphrase, then enter it in the *Passphrase* field and click the **Generate** button. If you want to enter the WEP key manually, then enter it in the *WEP Key 1-4* field(s). To indicate which WEP key to use, select the appropriate *TX Key* number.



Security Mode: WEP

Encryption: 128 bit

Passphrase:

WEP Key 1:

WEP Key 2:

WEP Key 3:

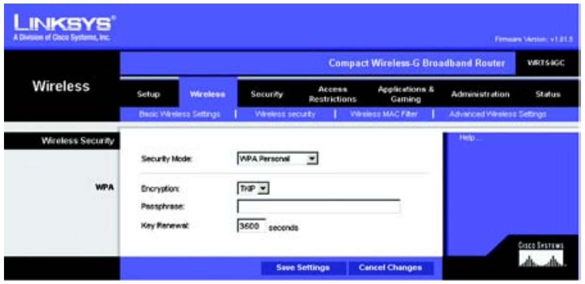
WEP Key 4:

TX Key: 1

Figure 5-15: Wireless Tab - Wireless Security (WEP)

wep *(wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.*

WPA Personal. This method offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of encryption method you want to use, **TKIP** or **AES**. Enter the Passphrase, which can have 8 to 63 characters. Then enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.



Security Mode: WPA Personal

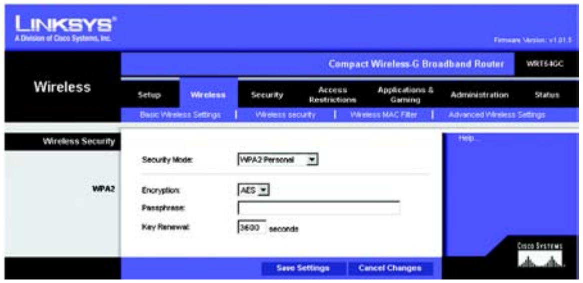
Encryption: TKIP

Passphrase:

Key Renewal: 3600 seconds

Figure 5-16: Wireless Tab - Wireless Security (WPA Personal)

WPA2 Personal. WPA2 gives you one encryption method, AES, with dynamic encryption keys. Enter a Passphrase of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.



Security Mode: WPA2 Personal

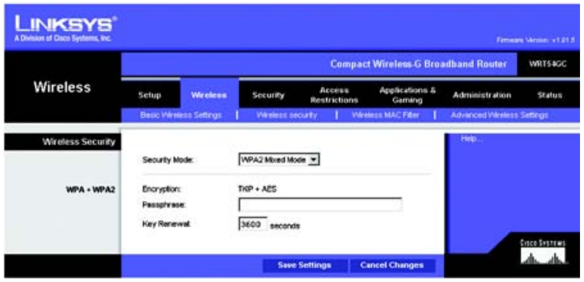
Encryption: AES

Passphrase:

Key Renewal: 3600 seconds

Figure 5-17: Wireless Tab - Wireless Security (WPA2 Personal)

WPA2 Mixed Mode. WPA2 gives you TKIP+AES encryption. Enter a Passphrase of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.



Security Mode: WPA2 Mixed Mode

Encryption: TKIP + AES

Passphrase:

Key Renewal: 3600 seconds

Figure 5-18: Wireless Tab - Wireless Security (WPA2 Mixed Mode)

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.

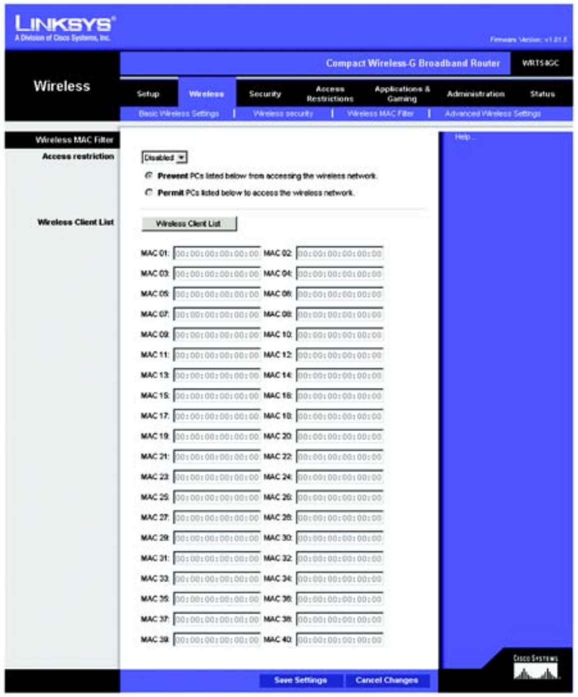
Wireless MAC Filter

Access Restrictions

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.**

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

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



Access restriction: Disabled

● **Prevent** PCs listed below from accessing the wireless network.

○ **Permit** PCs listed below to access the wireless network.

Wireless Client List: Wireless Client List

MAC 01:	00:00:00:00:00:00	MAC 02:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 04:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 06:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 08:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 10:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 12:	00:00:00:00:00:00
MAC 13:	00:00:00:00:00:00	MAC 14:	00:00:00:00:00:00
MAC 15:	00:00:00:00:00:00	MAC 16:	00:00:00:00:00:00
MAC 17:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00
MAC 19:	00:00:00:00:00:00	MAC 20:	00:00:00:00:00:00
MAC 21:	00:00:00:00:00:00	MAC 22:	00:00:00:00:00:00
MAC 23:	00:00:00:00:00:00	MAC 24:	00:00:00:00:00:00
MAC 25:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 27:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 29:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 31:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 33:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00
MAC 35:	00:00:00:00:00:00	MAC 36:	00:00:00:00:00:00
MAC 37:	00:00:00:00:00:00	MAC 38:	00:00:00:00:00:00
MAC 39:	00:00:00:00:00:00	MAC 40:	00:00:00:00:00:00

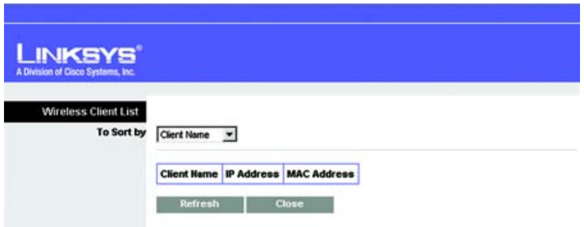
Figure 5-19: Wireless Tab - Wireless MAC Filter

Wireless Client List

Wireless Client List. Click the **Wireless Client MAC List** button to display a list of network users by MAC Address.From the *To Sort by* drop-down menu, you can sort the table by Client Name, IP Address, or MAC Address. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

List users, by MAC Address, whose wireless access you want to control.

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.



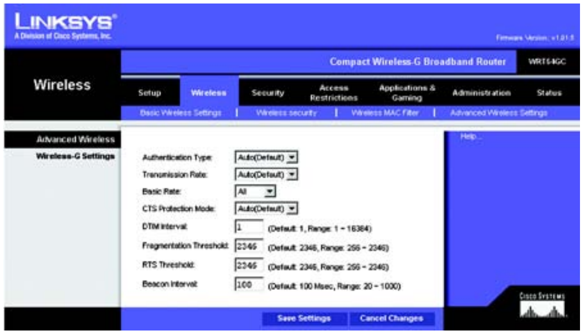
To Sort by: Client Name

Client Name	IP Address	MAC Address

Figure 5-20: Wireless Tab - 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.



Authentication Type: Auto(Default)
Transmission Rate: Auto(Default)
Basic Rate: All
CTS Protection Mode: Auto(Default)
DTIM Interval: 1 (Default: 1, Range: 1 - 16384)
Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
RTS Threshold: 2346 (Default: 2346, Range: 256 - 2346)
Beacon Interval: 100 (Default: 100 Msec, Range: 20 - 1000)

Figure 5-21: Wireless Tab - Advanced Wireless Settings

Advanced Wireless

Wireless-G Settings

Authentication Type. The default is set to **Auto (Default)**, 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.

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 (Default)** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto (Default)**.

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.

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode should be set to **Auto (Default).** 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.

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.**

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

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

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

Beacon Interval. The default value is **100.** 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.

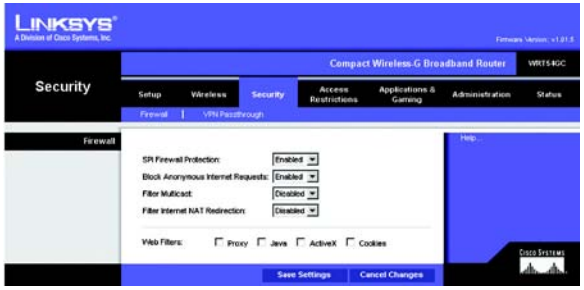
Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen.

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

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

The Security Tab - Firewall

The *Firewall* screen offers Filters and the option to Block WAN Requests. Filters block specific Internet data types and block anonymous Internet requests. To enable a feature, select **Enabled** from the drop-down menu. To disable a feature, select **Disabled** from the drop-down menu.



SPI Firewall Protection: Enabled

Block Anonymous Internet Requests: Enabled

Filter Multicast: Disabled

Filter Internet NAT Redirection: Disabled

Web Filters: □ Proxy □ Java □ ActiveX □ Cookies

Figure 5-22: Security Tab - Firewall

Firewall

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

- Block 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 Enable to filter multicasting, or Disable to disable this feature.

- Filter Internet NAT Redirection. This feature uses port forwarding to block access to local servers from local networked computers. Check the box to enable filter Internet NAT redirection, or uncheck the box 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.

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 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.

VPN Passthrough

IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Pass-Through is enabled by default. To disable IPSec Passthrough, select **Disabled.**

L2TP Passthrough. Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass-Through is enabled by default. To disable L2TP Passthrough, select **Disabled.**

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

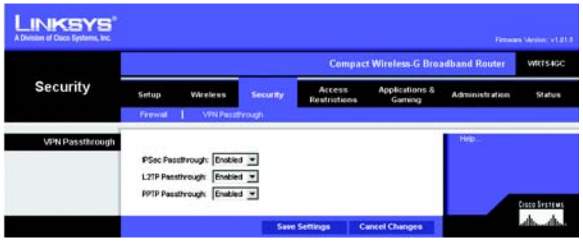
The Access Restrictions Tab - Internet Access Policy

The *Internet Access Policy* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated applications, 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). You can change the type of access, days, and times of a policy. To activate 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 tab, click the **Close** button. To view the list of PCs for a specific policy, click the **PCs List** button.

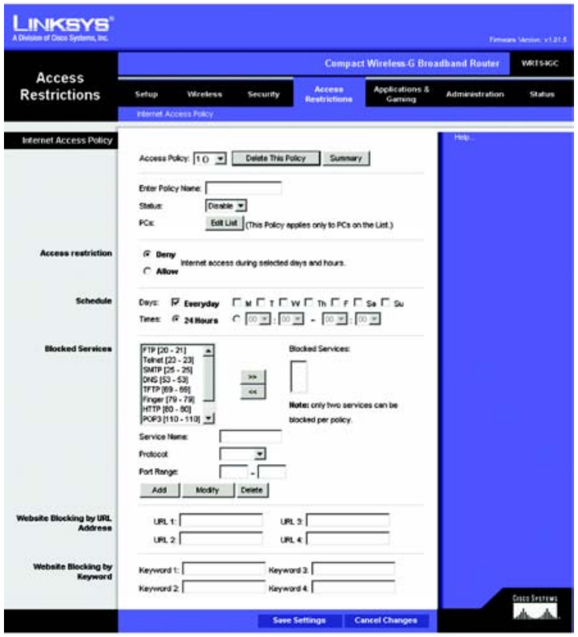


IPSec Passthrough: Enabled
L2TP Passthrough: Enabled
PPTP Passthrough: Enabled

Figure 5-23: Security Tab - VPN Passthrough

***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.*



Access Policy: 1 ()
Enter Policy Name:
Status: Disable
PCs: (This Policy applies only to PCs on the List.)

Access restriction
● Deny
○ Allow
Internet access during selected days and hours.

Schedule
Days: ☑ Everyday □ M □ T □ W □ Th □ F □ Sa □ Su
Times: ● 24 Hours ○ 00 : 00 - 00 : 00

Blocked Services
FTP [20 - 21]
Telnet [23 - 23]
SMTP [25 - 25]
DNS [53 - 53]
TFTP [69 - 69]
Finger [79 - 79]
HTTP [80 - 80]
POP3 [110 - 110]
Blocked Services:
Note: only two services can be blocked per policy.
Service Name:
Protocol:
Port Range: -

Website Blocking by URL Address
URL 1:
URL 2:
URL 3:
URL 4:

Website Blocking by Keyword
Keyword 1:
Keyword 2:
Keyword 3:
Keyword 4:

Figure 5-24: Access Restrictions Tab - Internet Access Policy

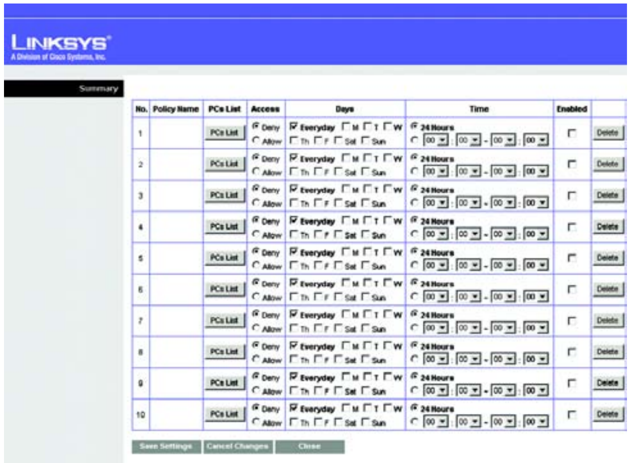
On the *Internet Access PCs List* screen, you can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Click the **Close** button to exit this screen.

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, select **Enable** from the *Status* drop-down menu.
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 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 next to *Blocked Application Port*.

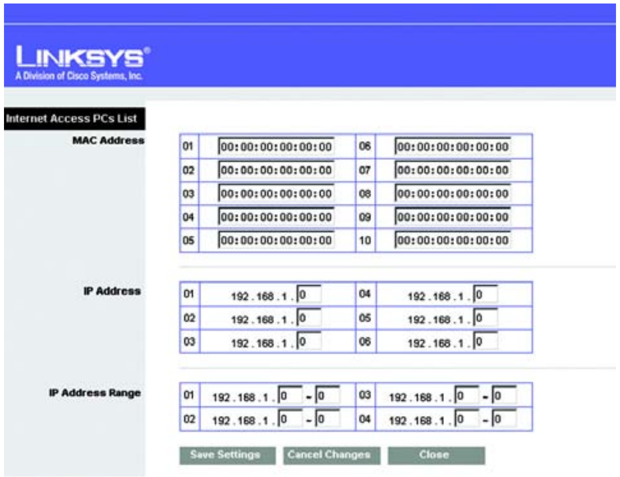
   The Block Services menu offers a choice of ten preset applications. For the preset applications you select, the appropriate range of ports will automatically be displayed. Click the **>>** button to add to the Blocked Services list.

   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 a Service Name, Protocol, and Port Range. Then, click **Add.**
8. 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.
9. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.



No.	Policy Name	PCs List	Access	Days	Time	Enabled	
1		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
2		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
3		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
4		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
5		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
6		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
7		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
8		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
9		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete
10		PCs List	● Deny ○ Allow	☑ Everyday □ M □ T □ W □ Th □ F □ Sat □ Sun	● 24 Hours ○ 00 : 00 - 00 : 00	□	Delete

Figure 5-25: Access Restrictions Tab - Summary



MAC Address

01	00:00:00:00:00:00	06	00:00:00:00:00:00
02	00:00:00:00:00:00	07	00:00:00:00:00:00
03	00:00:00:00:00:00	08	00:00:00:00:00:00
04	00:00:00:00:00:00	09	00:00:00:00:00:00
05	00:00:00:00:00:00	10	00:00:00:00:00:00

IP Address

01	192 . 168 . 1 . 0	04	192 . 168 . 1 . 0
02	192 . 168 . 1 . 0	05	192 . 168 . 1 . 0
03	192 . 168 . 1 . 0	06	192 . 168 . 1 . 0

IP Address Range

01	192 . 168 . 1 . 0 - 0	03	192 . 168 . 1 . 0 - 0
02	192 . 168 . 1 . 0 - 0	04	192 . 168 . 1 . 0 - 0

Figure 5-26: Access Restrictions Tab - Internet Access PCs List

The Applications and Gaming Tab - Port Range Forwarding

The *Port Range Forwarding* screen 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.)

Before using forwarding, you should assign static IP addresses to the designated PCs.

Port Range Forwarding

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

Application Name. Each drop-down menu offers a choice of ten preset applications (select **None** if you do not want to use any of the preset applications). Select up to five preset applications. For custom applications, enter the name of your application in one of the available fields.

The preset applications are among the most widely used Internet applications. They include the following:

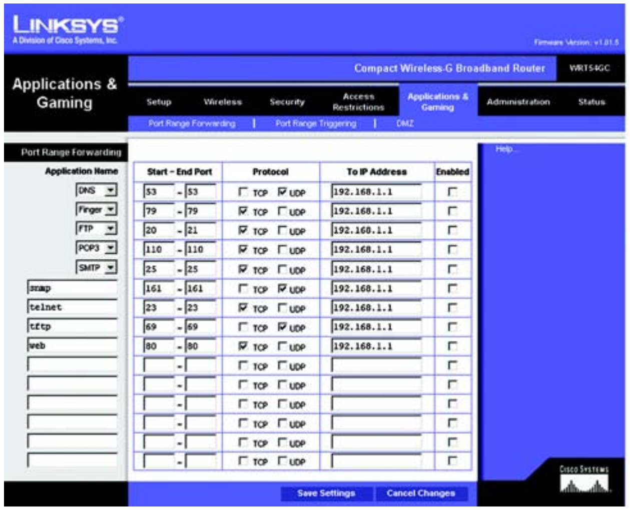
DNS (Domain Name System). The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember “handle” for an Internet address.

Finger. A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being “fingered” must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user@domain address.

FTP (File Transfer Protocol). A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

POP3 (Post Office Protocol 3). A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

SMTP (Simple Mail Transfer Protocol). The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.



Port Range Forwarding

Application Name	Start - End Port	Protocol	To IP Address	Enabled
DNS	53 - 53	☐ TCP ☑ UDP	192.168.1.1	☐
Finger	79 - 79	☑ TCP ☐ UDP	192.168.1.1	☐
FTP	20 - 21	☑ TCP ☐ UDP	192.168.1.1	☐
POP3	110 - 110	☑ TCP ☐ UDP	192.168.1.1	☐
SMTP	25 - 25	☑ TCP ☐ UDP	192.168.1.1	☐
snmp	161 - 161	☐ TCP ☑ UDP	192.168.1.1	☐
telnet	23 - 23	☑ TCP ☐ UDP	192.168.1.1	☐
tftp	69 - 69	☐ TCP ☑ UDP	192.168.1.1	☐
web	80 - 80	☑ TCP ☐ UDP	192.168.1.1	☐
	-	☐ TCP ☐ UDP		☐
	-	☐ TCP ☐ UDP		☐
	-	☐ TCP ☐ UDP		☐
	-	☐ TCP ☐ UDP		☐
	-	☐ TCP ☐ UDP		☐
	-	☐ TCP ☐ UDP		☐

Figure 5-27: Applications and Gaming Tab - Port Range Forwarding

SNMP (Simple Network Management Protocol). A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

Telnet. A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

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

Web. The Internet.

Start/End. This is the port range. Enter the port number or range of external ports used by the server or Internet application. Check with the software documentation of the Internet application for more information.

Protocol. Select the protocol(s) used for this application, **TCP** and/or **UDP**.

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

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

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 Triggering

The *Port Range 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 pulled back to the proper computer by way of IP address and port mapping rules.

Port Range Triggering

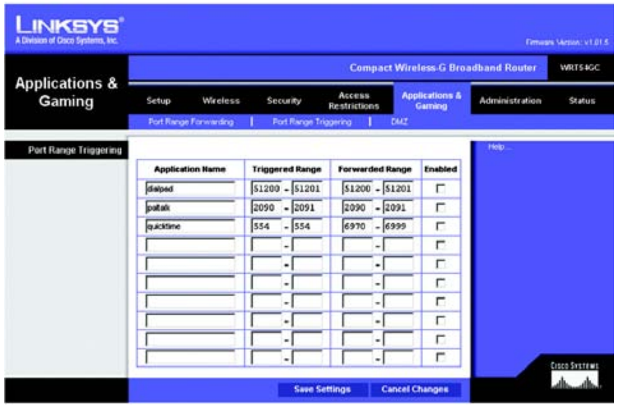
Application Name. Enter the application name of the trigger.

Triggered Range. For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Triggered Range. In the second field, enter the ending port number 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. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

Enabled. Click the **Enabled** checkbox to enable port range triggering 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. Help information is shown on the right-hand side of the screen.



Application Name	Triggered Range	Forwarded Range	Enabled
dialpad	51200 - 51201	51200 - 51201	□
paltalk	2090 - 2091	2090 - 2091	□
quicktime	554 - 554	6970 - 6999	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□

Figure 5-28: Applications and Gaming Tab - Port Triggering

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 Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

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

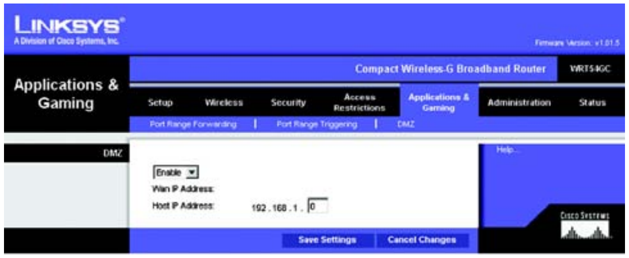
DMZ

To expose one PC, select **Enable**, then enter a WAN IP Address or Host IP Address in the field.

Wan IP Address. The Internet IP address of the computer you want to expose.

Host IP Address. Enter the IP 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. Help information is shown on the right-hand side of the screen.



Enable

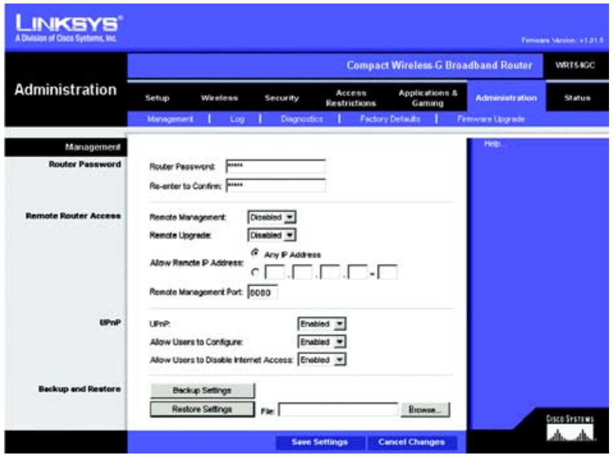
Wan IP Address:

Host IP Address: 192 . 168 . 1 . 0

Figure 5-29: 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.



Router Password: *****
Re-enter to Confirm: *****
Remote Management: Disabled
Remote Upgrade: Disabled
Allow Remote IP Address: ● Any IP Address ○ ___.___.___.___-___
Remote Management Port: 8080
UPnP: Enabled
Allow Users to Configure: Enabled
Allow Users to Disable Internet Access: Enabled

Figure 5-30: Administration Tab - Management

Management

Router Password

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.

Remote Router Access

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

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.**

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.

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. Keep the default setting, **Enabled**, if you want to be able to make manual changes to the Router while using the UPnP feature. Otherwise, select **Disabled.**

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