

LINKSYS® by Cisco



USER GUIDE

Wireless-G Broadband Router

Model: WRT54G2



About This Guide

Icon Descriptions

While reading through the User Guide you may see various icons that call attention to specific items. Below is a description of these icons:



NOTE: This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.



WARNING: This exclamation point indicates that there is a caution or warning and it is something that could damage your property or product.



WEB: This globe icon indicates a noteworthy website address or e-mail address.

Online Resources

Most web browsers allow you to enter the web address without adding the `http://` in front of the address. This User Guide will refer to websites without including `http://` in front of the address. Some older web browsers may require you to add it.

Resource	Website
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

Copyright and Trademarks



Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2008 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

Chapter 1: Product Overview	1
Front Panel	1
Back Panel	1
Placement Positions	1
Chapter 2: Wireless Security Checklist	3
General Network Security Guidelines	3
Additional Security Tips	3
Chapter 3: Advanced Configuration	4
Setup > Basic Setup	4
Setup > DDNS	7
Setup > MAC Address Clone	8
Setup > Advanced Routing	9
Wireless > Basic Wireless Settings	10
Wireless > Wireless Security	11
Wireless > Wireless MAC Filter	13
Wireless > Advanced Wireless Settings	14
Security > Firewall	15
Firewall	15
Security > VPN Passthrough	15
Access Restrictions > Internet Access	16
Applications and Gaming > Port Range Forward	17
Applications & Gaming > Port Triggering	17
Applications and Gaming > DMZ	18
Applications and Gaming > QoS	18
Administration > Management	19
Administration > Log	20
Administration > Diagnostics	20
Administration > Factory Defaults	21
Administration > Upgrade Firmware	21
Administration > Config Management	21
Status > Router	22
Status > Local Network	22
Status > Wireless	23
Appendix A: Troubleshooting	24
Appendix B: Specifications	25
Appendix C: Warranty Information	26
Limited Warranty	26

Appendix D: Regulatory Information	28
FCC Statement28
FCC Radiation Exposure Statement28
Safety Notices28
Industry Canada Statement28
Avis d'Industrie Canada29
Wireless Disclaimer29
Avis de non-responsabilité concernant les appareils sans fil29
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)30
Appendix E: Software License Agreement	34
Software in Linksys Products34
Software Licenses34

Chapter 1: Product Overview

Thank you for choosing the Linksys Wireless-G Broadband Router. The Router lets you access the Internet via a wireless connection, broadcast at up to 54 Mbps, or through one of its four switched ports. You can also use the Router to share resources such as computers, printers and files. A variety of security features help to protect your data and your privacy while online. Security features include WPA2 security, a Stateful Packet Inspection (SPI) firewall and NAT technology. Configuring the Router is easy using the provided browser-based utility

Front Panel



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.

Wi-Fi Protected Setup Button If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network(s).

To use Wi-Fi Protected Setup, run the Setup Wizard, or refer to the "Wireless > Basic Wireless Settings" section of "Chapter 3: Advanced Configuration".

Wi-Fi Protected Setup LED (Green/Amber) It lights up green when wireless security is enabled. The LED flashes green for two minutes during Wi-Fi Protected Setup.

The LED lights up amber if there is an error during the Wi-Fi Protected Setup process. Make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again.

The LED flashes amber when a Wi-Fi Protected Setup session is active, and a second session begins. The Router supports one session at a time. Wait until the LED is off before starting the next Wi-Fi Protected Setup session.

Wireless (Green) The Wireless LED lights up when the wireless feature is enabled. If the LED is flashing, the Router is actively sending or receiving data over the network.

Internet (Green) The Internet LED lights up when there is a connection made through the Internet port. A flashing LED indicates network activity over 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.

Back Panel



Internet The Internet port is where you will connect your cable or DSL Internet connection.

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

Reset There are two ways to reset the Router's factory defaults. Either press and hold the Reset Button for approximately five seconds, or restore the defaults from Administration > Factory Defaults in the Router's web-based utility.

Power The Power port is where you will connect the power adapter.

Placement Positions

There are two ways to physically install the Router. The first way is to place the Router horizontally on a surface. The second way is to mount the Router on a wall.

Horizontal Placement

The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical outlet.





Wall-Mounting Placement

The Router has two wall-mount slots on its bottom panel. The distance between the slots is 152 mm (6 inches).

Two screws are needed to mount the Router.

Suggested Mounting Hardware

		2.5-3.0 mm
4-5 mm	1-1.5 mm	

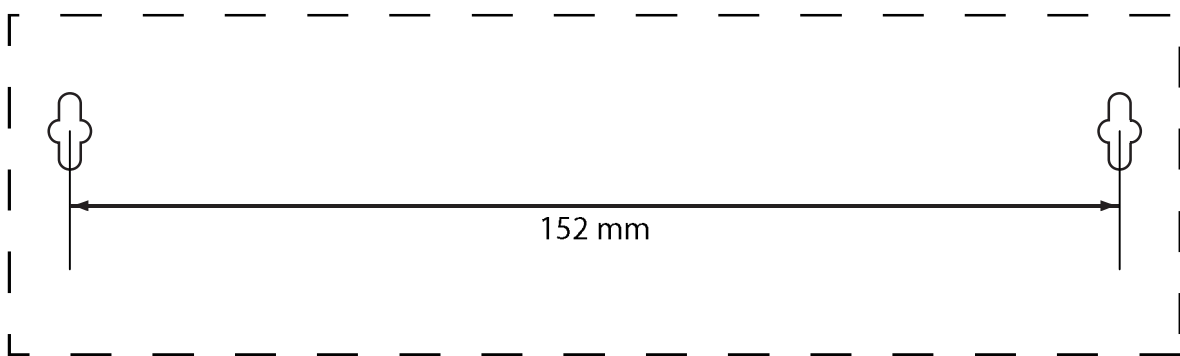
†Note: Mounting hardware illustrations are not true to scale.



NOTE: Linksys is not responsible for damages incurred by insecure wall-mounting hardware.

Follow these instructions:

1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.
2. Drill two holes into the wall. Make sure the holes are 152 mm (6 inches) apart.
3. Insert a screw into each hole and leave 3 mm (0.12 inches) of its head exposed.
4. Maneuver the Router so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.



Print this page at 100% size.

Cut along the dotted line, and place on the wall to drill precise spacing.

Wall Mounting Template

Chapter 2: Wireless Security Checklist

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.



1. Change the default wireless network name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use **linksys** as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.



2. Change the default password

For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Linksys default password is **admin**. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.



3. Enable MAC address filtering

Linksys routers give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.



4. Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication. Currently, devices that are Wi-Fi certified are required to support WPA2, but are not required to support WEP.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure.

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

- Keep wireless routers, access points, or gateways away from exterior walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.



WEB: For more information on wireless security, visit www.linksys.com/security

Chapter 3: Advanced Configuration

After setting up the Router with the Setup Wizard (located on the CD-ROM), the Router will be ready for use. However, if you'd like to change its advanced settings, use the Router's web-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the Router.

The web-based utility has these 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.



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

How to Access the Web-Based Utility

To access the web-based utility, launch the web browser on your computer, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Then, press **Enter**.

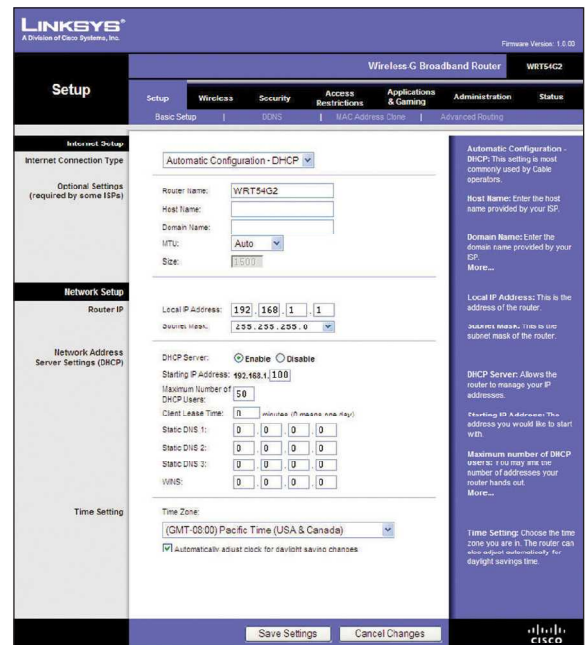
A password request screen will appear. (Non-Windows XP users will see a similar screen.) Leave the *User name* field blank. The first time you open the Web-based utility, use the default password **admin**. (You can set a new password from the Administration tab's *Management* screen.) Click **OK** to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



Password Screen

Setup > Basic Setup

The first screen that appears is the *Basic Setup* screen. This allows you to change the Router's general settings.



Setup > Basic Setup

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

Select the type of Internet connection your ISP provides from the drop-down menu. The available types are:

- Automatic Configuration - DHCP
- Static IP
- PPPoE
- PPTP
- L2TP
- Telstra Cable

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. (This option usually applies to cable connections.)

Internet Connection Type	Automatic Configuration - DHCP
--------------------------	--------------------------------

Internet Connection Type > Automatic Configuration - DHCP

Static IP

If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.

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

Internet Connection Type > Static IP

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

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

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

DNS 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**.

Internet Connection Type	PPPoE
User Name:	linksys
Password:	••••••••••••••••
<input type="radio"/> Connect on Demand: Max Idle Time	5 Min.
<input checked="" type="radio"/> Keep Alive: Redial Period	30 Sec.

Internet Connection Type > 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. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed

before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive: 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, select **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.

Internet Connection Type	PPTP
<input type="radio"/> Obtain an IP Address Automatically	
<input checked="" type="radio"/> Specify an IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0
DNS 1:	0 . 0 . 0 . 0
DNS 2:	0 . 0 . 0 . 0
DNS 3:	0 . 0 . 0 . 0
PPTP Server IP Address:	0 . 0 . 0 . 0
Username:	
Password:	
<input type="radio"/> Connect on Demand: Max Idle Time	5 Minute.
<input checked="" type="radio"/> Keep Alive: Redial Period	30 Second.

Internet Connection Type > PPTP

If your ISP supports DHCP or you are connecting through a dynamic IP address, then select **Obtain an IP Address Automatically**. If you are required to use a permanent IP address to connect to the Internet, then select **Specify an IP Address**. Then configure the following:

- **Specify an 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 IP address of the ISP server.
- **DNS 1-3** Your ISP will provide you with at least one DNS (Domain Name System) server IP address.

PPTP Server IP Address Your ISP will provide you with the IP address of the PPTP server.

Username and Password Enter the Username 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. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive: 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, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default value is **30** seconds.

L2TP

L2TP is a service that applies to connections in Israel only.

Internet Connection Type > L2TP

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

L2TP Server This is the IP address of the L2TP Server. Your ISP will provide you with the IP Address you need to specify here.

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. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes

Keep Alive: 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, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

Telstra Cable

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

Internet Connection Type > Telstra Cable

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

Heart Beat Server This is the IP address of the Heartbeat Server. Your ISP will provide you with the IP Address you need to specify here.

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. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes

Keep Alive: 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, select **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.

Optional Settings

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

Optional Settings

Router Name In this field, you can enter 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. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the Router select the best MTU for your Internet connection, keep the default setting, **Auto**.

Size When Manual is selected in the *MTU* field, this option is enabled. Leave this value in the 1200 to 1500 range. The default size depends on the Internet Connection Type:

- DHCP, Static IP, or Telstra: **1500**
- PPPoE: **1492**
- PPTP or L2TP: **1460**

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.

Router IP Address	Local IP Address:	192 . 168 . 1 . 1
	Subnet Mask:	255 . 255 . 255 . 0

Router IP Address

Network Address Server Settings (DHCP)

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

Network Address Server Settings (DHCP)	DHCP Server:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Starting IP Address:	192.168.1.100
	Maximum Number of DHCP Users:	50
	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	

Network Address Server Settings (DHCP)

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 **Disable** (no other DHCP features will be available).

Starting IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's

default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default Starting IP Address is **192.168.1.100**.

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

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

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, enter that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS The Windows Internet Naming Service (WINS) 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.

Time Setting

Select the time zone in which your network functions from this drop-down menu. (You can even automatically adjust for daylight saving time.)

Time Setting	Time Zone:
	(GMT-08:00) Pacific Time (USA & Canada)
	<input checked="" type="checkbox"/> Automatically adjust clock for daylight saving changes

Time Setting

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > 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. If you do not want to use this feature, keep the default setting, **Disable**.

DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain

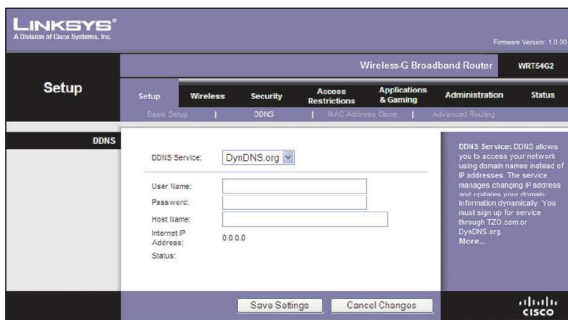
name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router.

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 Service

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

DynDNS.org



Setup > DDNS > DynDNS

User Name Enter the User Name for your DDNS account.

Password Enter the Password for your DDNS account.

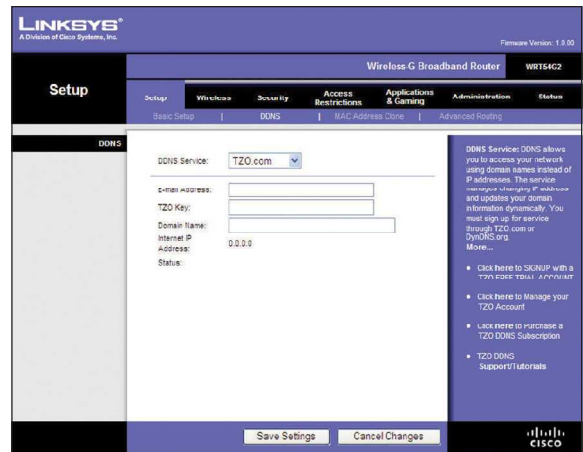
Host Name This is the DDNS URL assigned by the DDNS service.

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

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

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

TZO.com



Setup > DDNS > TZO

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

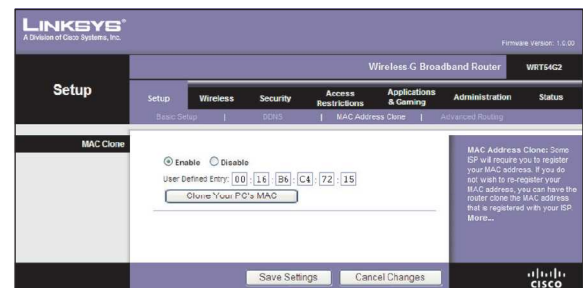
Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

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

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > 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.



Setup > MAC Address Clone

MAC Address Clone

Enable/Disable To have the MAC Address cloned, select **Enable**.

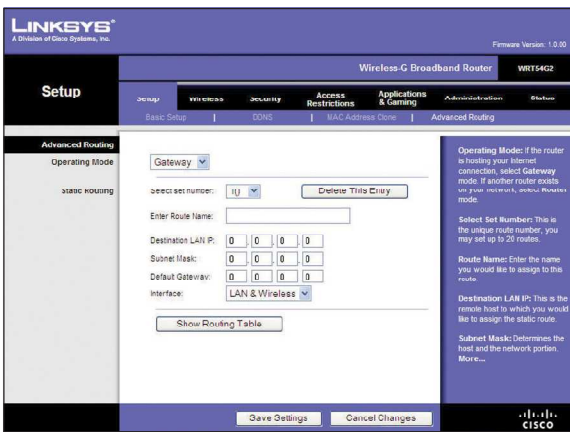
User Defined Entry Enter the MAC Address registered with your ISP here.

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

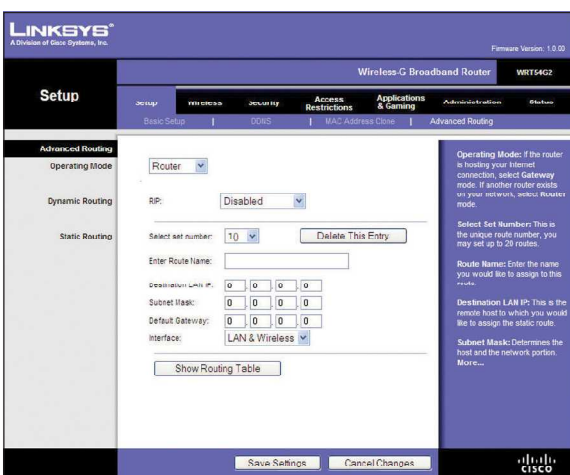
Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > Advanced Routing

This screen is used to set up the Router's advanced routing functions. NAT routes the host Router's network connection to the Internet. Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination.



Setup > Advanced Routing (Gateway)



Setup > Advanced Routing (Router)

Advanced Routing

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 available as an option.

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. 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 (Internet)**, 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.

Select set number 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) or the **WAN (Internet)**.

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

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

Routing Table Entry List			
Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.100	255.255.255.0	192.168.1.1	LAN & Wireless

Routing Table

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Basic Wireless Settings

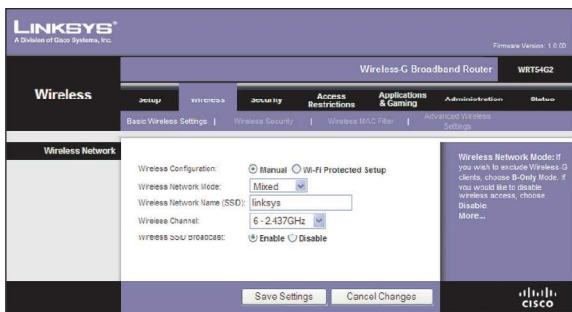
The basic settings for wireless networking are set on this screen.

There are two ways to configure the Router's wireless network(s), manual and Wi-Fi Protected Setup.

Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup.

Wireless Configuration To manually configure your wireless network, select **Manual**. Proceed to the "Basic Wireless Settings" section. To use Wi-Fi Protected Setup, select **Wi-Fi Protected Setup**. Proceed to the "Wi-Fi Protected Setup" section.

Basic Wireless Settings



Wireless > Basic Wireless Settings (Manual Setup)

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

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

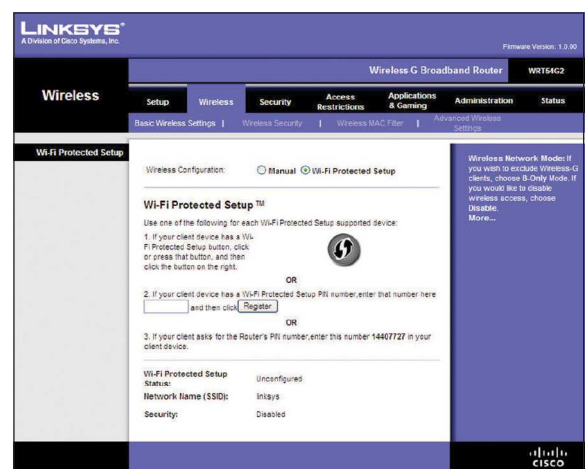
Wireless Channel Select the channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on the same channel in order to function correctly.

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

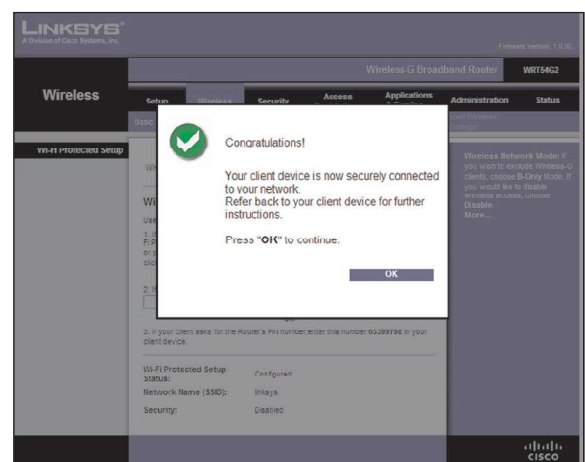
Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wi-Fi Protected Setup

There are three methods available. Use the method that applies to the client device you are configuring.



Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)



Wi-Fi Protected Setup > Congratulations



NOTE: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup.

Method #1

Use this method if your client device has a Wi-Fi Protected Setup button.

1. Click or press the **Wi-Fi Protected Setup** button on the client device.
2. Click the **Wi-Fi Protected Setup** button on this screen.
3. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

Method #2

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

1. Enter the PIN number in the field on this screen.
2. Click **Register**.
3. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

Method #3

Use this method if your client device asks for the Router's PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.)
2. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

The Wi-Fi Protected Setup Status, Network Name (SSID), Security, Encryption, and Passphrase are displayed at the bottom of the screen.



NOTE: If you have client devices that do not support Wi-Fi Protected Setup, note the wireless settings, and then manually configure those client devices.

Wireless > Wireless Security

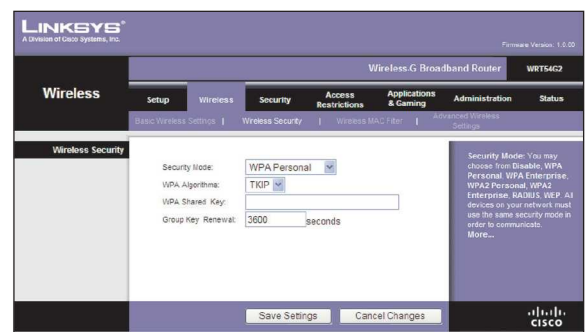
The Wireless Security settings configure the security of your wireless network. There are six wireless security mode options supported by the Router: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WPA2 is a more advanced, more secure version of WPA. WEP stands for Wired Equivalent Privacy, and RADIUS stands for Remote Authentication Dial-In User Service.) These six are briefly discussed here. For detailed instructions on configuring wireless security for the Router, refer to "Chapter 2: Wireless Security."

Wireless Security**Security Mode**

Select the security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

WPA Personal

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



Security Mode > WPA Personal

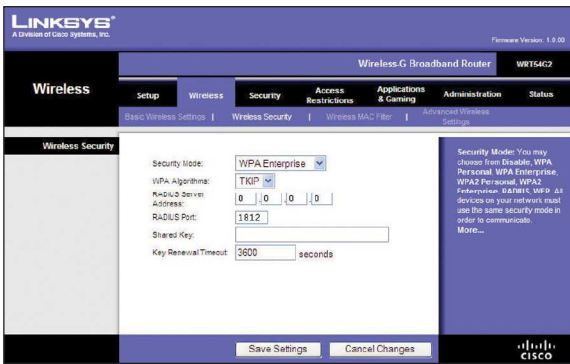
WPA Algorithm WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

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

Group Key Renewal Enter a Key Renewal period, which tells the Router how often it should change the encryption keys. The default Group Key Renewal period is **3600** seconds.

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.)



Security Mode > WPA Enterprise

WPA Algorithm WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP)

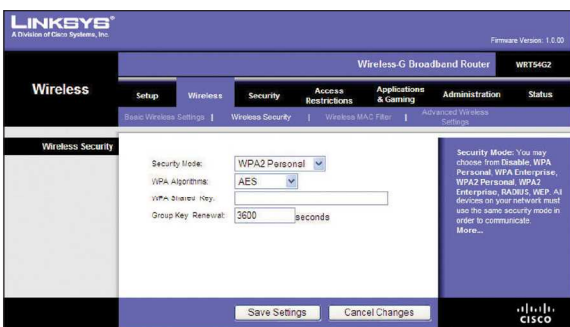
RADIUS Server Address Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys. The default Key Renewal Timeout period is **3600** seconds.

WPA2 Personal



Security Mode > WPA2 Personal

WPA Algorithm WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES**, or **TKIP + AES**. The default selection is **AES**.

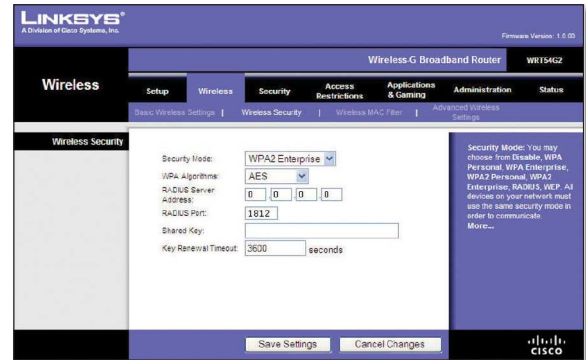
WPA Shared Key Enter a WPA Shared Key of 8-63 characters.

Group Key Renewal Enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Group Key Renewal period is **3600** seconds.

Wireless-G Broadband Router

WPA2 Enterprise

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



Security Mode > WPA2 Enterprise

WPA Algorithm WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES**, or **TKIP + AES**. The default selection is **AES**

RADIUS Server Address Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys. The default Key Renewal Timeout period is **3600** seconds.

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.)



Security Mode > RADIUS



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.

RADIUS Server Address Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Default Transmit Key Select a Default Transmit Key (choose which Key to use). The default is **1**.

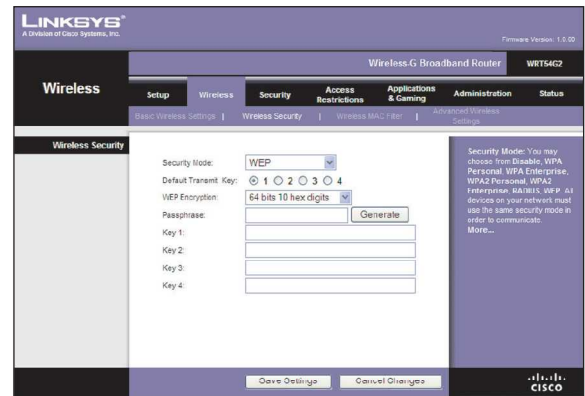
WEP Encryption Select a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. The default is **64 bits 10 hex digits**.

Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

WEP

WEP is a basic encryption method, which is not as secure as WPA.



Security Mode > WEP

Default Transmit Key Select a Default Transmit Key (choose which Key to use). The default is **1**.

WEP Encryption Select a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. The default is **64 bits 10 hex digits**.

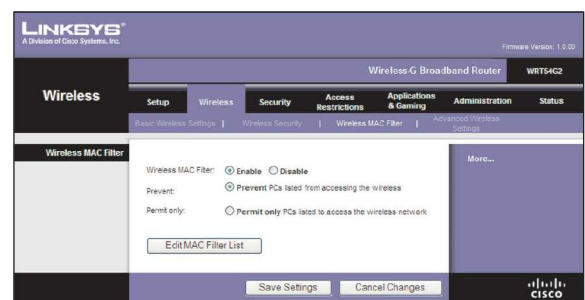
Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Wireless MAC Filter

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



Wireless > Wireless MAC Filter

Wireless MAC Filter

Wireless MAC Filter To filter wireless users by MAC Address, either permitting or blocking access, click **Enable**. If you do not wish to filter users by MAC Address, keep the default setting, **Disable**.

Prevent Select this to block wireless access by MAC Address. This button is selected by default.

Permit Only Select this to allow wireless access by MAC Address. This button is not selected by default.

Edit MAC Filter List Click this to open the *MAC Address Filter List* screen. On this screen, you can list users, by MAC Address, to whom you wish to provide or block access. For easy reference, click **Wireless Client MAC List** to display a list of network users by MAC Address.

MAC Address Filter List

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Advanced Wireless Settings

This *Wireless > Advanced Wireless Settings* screen 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.

Wireless > Advanced Wireless Settings

Advanced Wireless

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 value is **Auto**.

CTS Protection Mode CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your Wireless-G products not being 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.

Frame Burst Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To turn on the Frame Burst option, select **Enable**. The default is **Disable**.

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

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

hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

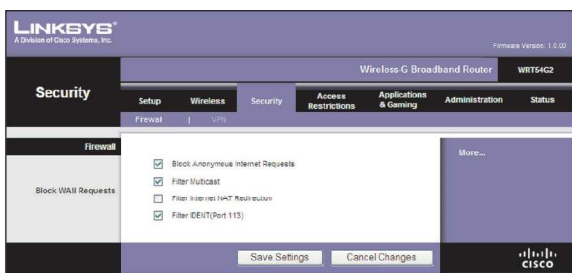
RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving 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**.

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, select **On**. AP Isolation is turned **Off** by default.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > Firewall

The *Security > Firewall* screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network.



Security > Firewall

Firewall

Firewall Protection To use firewall protection, keep the default selection, **Enable**. To turn off firewall protection, select **Disable**.

Block WAN Requests

Block Anonymous Internet Requests This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature 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. This feature is selected by default. Deselect this feature to disable it.

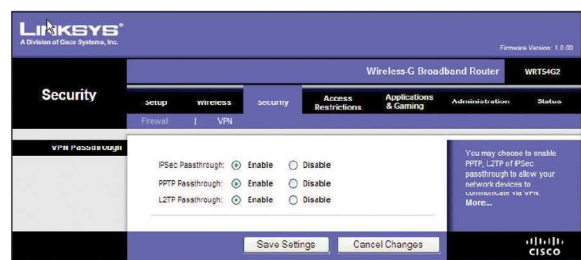
Filter Internet NAT Redirection This feature uses port forwarding to block access to local servers from local networked computers. Select **Filter Internet NAT Redirection** to filter Internet NAT redirection. This feature is not selected by default.

Filter IDET (Port 113) This feature keeps port 113 from being scanned by devices outside of your local network. This feature is selected by default. Deselect this feature to disable it.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > VPN Passthrough

The *Security > VPN Passthrough* screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.



Security > VPN Passthrough

VPN Passthrough

IPSec Passthrough 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, keep the default, **Enable**.

PPTP Passthrough 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, keep the default, **Enable**.

L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the

Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, **Enable**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Access Restrictions > Internet Access

The *Access Restrictions > Internet Access* 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.



Access Restrictions > Internet Access

Internet Access

Internet Access Policy Access can be managed by a policy. Use the settings on this screen to establish an access policy (after **Save Settings** 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 **Delete**. To view all the policies, click **Summary**. (Policies can be deleted from the *Summary* screen by selecting the policy or policies and clicking **Delete**. To return to the Internet Access tab, click **Close**.)

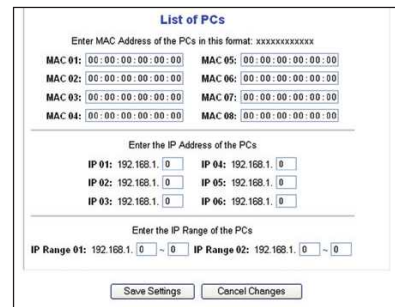
Id	Policy Name	Days	Time of Day	Enabled
1	Int	SMTWTFSS	24 Hours	<input type="checkbox"/>
2	---	SMTWTFSS	---	<input type="checkbox"/>
3	---	SMTWTFSS	---	<input type="checkbox"/>
4	---	SMTWTFSS	---	<input type="checkbox"/>
5	---	SMTWTFSS	---	<input type="checkbox"/>
6	---	SMTWTFSS	---	<input type="checkbox"/>
7	---	SMTWTFSS	---	<input type="checkbox"/>
8	---	SMTWTFSS	---	<input type="checkbox"/>
9	---	SMTWTFSS	---	<input type="checkbox"/>
10	---	SMTWTFSS	---	<input type="checkbox"/>

Internet Policy Summary

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

To create an Internet Access policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, select **Enable**.
3. Enter a Policy Name in the field provided.
4. Click **Edit List of PCs** to select which PCs will be affected by the policy. The *List of PCs* screen appears. 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 **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes. Then click **Close**.



List of PCs

5. Select 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. Select any Blocked Services or Website Blocking you wish to use.
8. Click **Save Settings** to save the policy's settings, or click **Cancel Changes** to cancel the policy's settings.

Blocked Services

You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. (You can block up to 20 services.) Then enter the range of ports you want to filter.

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