USER GUIDE

Wireless-G Broadband Router

Model: WRT54GL
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

Website addresses in this document are listed without http:// in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add http:// in front of the web address.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linksys International</td>
<td><a href="http://www.linksys.com/international">www.linksys.com/international</a></td>
</tr>
<tr>
<td>Glossary</td>
<td><a href="http://www.linksys.com/glossary">www.linksys.com/glossary</a></td>
</tr>
<tr>
<td>Network Security</td>
<td><a href="http://www.linksys.com/security">www.linksys.com/security</a></td>
</tr>
</tbody>
</table>

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.
# Table of Contents

## Chapter 1: Product Overview
- Front Panel .................................................. 3
- Back Panel ................................................... 3

## Chapter 2: Wireless Security Checklist
- General Network Security Guidelines ......................... 4
- Additional Security Tips ........................................ 4

## Chapter 3: Advanced Configuration
- Setup > Basic Setup ........................................ 5
- Setup > DDNS .................................................. 8
- Setup > MAC Address Clone ................................... 9
- Setup > Advanced Routing ..................................... 10
- Wireless > Basic Wireless Settings ......................... 10
- Wireless > Wireless Security .................................. 11
- Wireless > Wireless MAC Filter .............................. 13
- Wireless > Advanced Wireless Settings ..................... 14
- Security > 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 ......................... 20
- Administration > Firmware Upgrade ....................... 21
- Administration > Config Management .................... 21
- Status > Router .............................................. 21
- Status > Local Network ...................................... 22
- Status > Wireless ............................................. 22

## Appendix A: Troubleshooting ................................ 23

## Appendix B: Specifications .................................. 24

## Appendix C: Warranty Information ......................... 25
- Limited Warranty ........................................... 25

## Appendix D: Regulatory Information ....................... 27
- FCC Statement ............................................. 27
- FCC Radiation Exposure Statement ..................... 27
- Safety Notices .............................................. 27
- Industry Canada Statement .............................. 27
Avis d’Industrie Canada ................................................................. 28
Wireless Disclaimer ........................................................................ 28
Avis de non-responsabilité concernant les appareils sans fil ........ 28

**Appendix E: Software License Agreement**

Software in Linksys Products ......................................................... 33
Software Licenses .......................................................................... 33
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

SecureEasySetup (Orange/White) The Cisco logo is the Router’s SecureEasySetup button. It lights up and will stay orange when the Router is powered on. The color orange indicates that the Router is not using the SecureEasySetup feature, while the color white indicates that the Router is using the SecureEasySetup feature. When the Router enters SecureEasySetup mode, the Cisco logo will turn white and start flashing. After the Router has generated the SSID and WPA Personal key, the Cisco logo will stop flashing and stay white.

To clear the SSID and WPA Personal key, press and hold down the Cisco logo for five seconds. The Cisco logo will flash slowly as the Router resets itself. The Cisco logo will turn orange to indicate a successful reset.

NOTE: SecureEasySetup is a feature that makes it easy to set up your wireless network. If you have SecureEasySetup devices, run the Router’s Setup Wizard CD-ROM and follow the on-screen instructions to use SecureEasySetup.

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.

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

WLAN (Green) The WLAN 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.

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.

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.

Back Panel

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.

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.

Power The Power port is where you will connect the power adapter.
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](http://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.

Setup > Basic Setup

The first screen that appears is the Basic Setup screen. 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 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.)
Chapter 3
Advanced Configuration

Static IP

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

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

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

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

**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**.

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

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

**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**.

PPPoE

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

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

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

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

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

**Connect on Demand: Max Idle Time**  You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. 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**.
Chapter 3

Advanced Configuration

L2TP

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

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.

Optional Settings

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

Router Name In this field, you can 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
Advanced Configuration

Chapter 3

- 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.

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.

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.)

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 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

**System** Select the DynDNS service you use: **Dynamic**, **Static**, or **Custom**. The default selection is **Dynamic**.

**User Name** Enter the User Name for your DDNS account.

**Password** Enter the Password for your DDNS account.

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

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

**Backup MX** This feature allows the mail exchange server to be a backup. To disable this feature, keep the default, **No**. To enable the feature, select **Yes**. If you are not sure which setting to select, keep the default, **No**.

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

**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

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

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

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

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.

**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.
Chapter 3

Advanced Configuration

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 functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing automatically adjusts 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 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. Selecting **Both** enables dynamic routing for both networks, as well as data from the Internet.

**Static Routing**

**Select set number** To set up a static route between the Router and another network, select a number from the 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 **Delete This Entry** 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)**.

Click **Show Routing Table** to view the Static Routes you have already set up.

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.
Wireless Network

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

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

Wireless Channel Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to communicate.

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

SecureEasySetup If you did not utilize this network connection feature during the Setup Wizard, you may use it here by clicking the green logo. When you are prompted to start the push button setup, click OK.

Reset Security Use this button to reset the security settings on your network. You will need to run SecureEasySetup again on each device on your network to re-associate it with your network.

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

Wireless Security

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. WEP stands for Wired Equivalent Privacy, while 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.”

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.

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

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.

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

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 **TKIP + 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.

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 **TKIP + 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.)
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.

---

**Wireless > Wireless MAC Filter**

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

**MAC Address 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.

**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.

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.

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.

**SecureEasySetup** This feature allows you to enable or disable the SecureEasySetup feature. Select Disabled to disable the feature and turn off the button's light. The feature is Enabled 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.

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 IDENT (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.

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.
Chapter 3

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.

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.)

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.

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

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

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

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

**Website Blocking by URL Address**

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

**Website Blocking by Keyword**

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

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

**Applications and Gaming > Port Range Forward**

The **Applications and Gaming > Port Range Forward** 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.)

**Port Range Forward**

To forward a port, enter the information on each line for the criteria required.

- **Application** In this field, enter the name you wish to give the application. Each name can be up to 12 characters.
- **Start/End** This is the port range. Enter the number that starts the port range in the Start column and the number that ends the range in the End column.
- **Protocol** Select the protocol used for this application, either **TCP** or **UDP**, or **Both**.
- **IP Address** For each application, enter the IP Address of the PC running the specific application.
- **Enable** Select **Enable** to enable port forwarding for the relevant application.

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

**Applications and Gaming > Port Triggering**

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

- **Application** 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.
Start Port  Enter the starting port number of the Triggered Range.

End Port  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.

Start Port  Enter the starting port number of the Forwarded Range.

End Port  Enter the ending port number of the Forwarded Range.

Enable  Select Enable to enable port triggering for the applicable application.

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

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

DMZ
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.

To expose one PC, select Enable. Then, enter the computer’s IP address in the DMZ Host IP Address field. This feature is disabled by default.

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

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

There are three types of QoS available: Device Priority, Ethernet Port Priority, and Application Priority.

Wired QoS
Enable/Disable  To enable QoS, select Enable. Otherwise, select Disable. QoS is disabled by default.

Upstream Bandwidth  Select Auto or Manual from the drop-down menu. Manual allows you to specify the maximum outgoing bandwidth that applications can utilize.

Device Priority
Enter the name of your network device in the Device name field, enter its MAC Address, and then select its priority from the drop-down menu.

Ethernet Port Priority
Ethernet Port Priority QoS allows you to prioritize performance for the Router’s four ports, LAN Ports 1-4. For each port, select the priority and flow control setting.
Priority Select High or Low in the Priority column. The Router's four ports have been assigned low priority by default.

Flow Control If you want the Router to control the transmission of data between network devices, select Enabled. To disable this feature, select Disabled. Ethernet Port Priority QoS does not require support from your ISP because the prioritized ports LAN ports 1-4 are in your network. This feature is enabled by default.

Application Priority
Application Priority QoS manages information as it is transmitted and received. Depending on the settings of the QoS screen, this feature will assign information a high or low priority for the applications that you specify.

Optimize Gaming Applications Select this to automatically allow common game application ports to have a higher priority. These games include, but are not limited to: Counter-Strike, Half-Life, Age of Empires, Everquest, Quake2/Quake3, and Diablo II. The default setting is unselected.

Application Name Enter the name you wish to give the application in the Application Name field.

Priority Select High or Low to assign priority to the application. The default selection is Low.

Specific Port # Enter the port number for the application.

Wireless QoS
WMM Support Wi-Fi Multimedia (WMM), formerly known as Wireless Multimedia Extensions (WME), is a Wi-Fi Alliance certified feature, based on the IEEE 802.11e standard. This feature provides QoS to wireless networks. It is especially suitable for voice, music and video applications; for example, Voice over IP (VoIP), video streaming, and interactive gaming. If you have other devices on your wireless network that support WMM, select Enabled. Otherwise, keep the default, Disabled.

No Acknowledgement This feature prevents the Router from re-sending data if an error occurs. To use this feature, select Enabled. Otherwise, keep the default setting, Disabled.

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

Administration > Management

The Administration > Management screen allows the network's administrator to manage specific Router functions for access and security.
Administration > Log

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

Log

Log To disable the Log function, keep the default setting, Disable. To monitor traffic between the network and the Internet, select Enable.

When you wish to view the logs, click Incoming Log or Outgoing Log, depending on which you wish to view.

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

Administration > Diagnostics

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

Ping Test

Ping The Ping test checks the status of a connection. Click Ping to open the Ping Test screen. Enter the address of the PC whose connection you wish to test and how many times you wish to test it. Then, click Ping. The Ping Test screen will show if the test was successful. To stop the test, click Stop. Click Clear Log to clear the screen. Click Close to return to the Diagnostics screen.

Traceroute Test

Traceroute To test the performance of a connection, click Traceroute to open the Traceroute Test screen. Enter the address of the PC whose connection you wish to test and click Traceroute. The Traceroute Test screen will show if the test was successful. To stop the test, click Stop. Click Clear Log to clear the screen. Click Close to return to the Diagnostics screen.

Administration > Factory Defaults

The Administration > Factory Defaults screen allows you to restore the Router’s configuration to its factory default settings.

Factory Defaults

Restore Factory Defaults To reset the Router’s settings to the default values, select Yes, and then click Save Settings. Any settings you have saved will be lost when the default settings are restored.
Administration > Firmware Upgrade

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


Upgrade Firmware

Please select a file to upgrade  Click Browse and select the extracted firmware upgrade file. Then click Upgrade and follow the on-screen instructions.

Administration > Config Management

This screen is used to back up or restore the Router's configuration file.

Backup Configuration

To back up the Router's configuration file, click Backup. Then follow the on-screen instructions.

Restore Configuration

Please select a file to restore  Click Browse and select the configuration file. Then click Restore.

Status > Router

The Status > Router screen displays the Router's current status.

Router Information

Firmware Version  This is the Router's current firmware.

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

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

Router Name  This is the specific name for the Router, which you set on the Setup tab.

Host Name  If required by your ISP, this would have been entered on the Setup tab.

Domain Name  If required by your ISP, this would have been entered on the Setup tab.

Internet

Configuration Type

This section shows the current network information stored in the Router. The information varies depending on the Internet connection type selected on the Setup > Basic Setup screen.

Click Refresh to update the on-screen information.
**Status > Local Network**

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

**Local Network**

- **MAC Address**  This is the Router’s MAC Address, as seen on your local, Ethernet network.
- **IP Address**  This shows the Router’s IP Address, as it appears on your local, Ethernet network.
- **Subnet Mask**  This shows the current subnet mask being configured for your local network.
- **DHCP Server**  If you are using the Router as a DHCP server, that will be displayed here.
- **Start IP Address**  For the range of IP Addresses used by devices on your local, Ethernet network, the beginning of that range is shown here.
- **End IP Address**  For the range of IP Addresses used by devices on your local, Ethernet network, the end of that range is shown here.
- **DHCP Clients Table**  Clicking this button will open a screen to show you which PCs are utilizing the Router as a DHCP server. You can delete PCs from that list, and sever their connections, by checking a Delete box and clicking the Delete button.

Click **Refresh** to update the on-screen information.

**Status > Wireless**

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

**Wireless**

- **MAC Address**  This is the Router’s MAC Address, as seen on your local, wireless network.
- **Mode**  As selected from the *Wireless > Basic Wireless Settings* screen, this displays the wireless mode (Mixed, G-Only, or Disabled) used by the network.
- **SSID**  As entered on the *Wireless > Basic Wireless Settings* screen, this displays the wireless network name or SSID.
- **DHCP Server**  The status of the DHCP server function is displayed here.
- **Channel**  As entered on the *Wireless > Basic Wireless Settings* screen, this displays the channel on which your wireless network is broadcasting.
- **Encryption Function**  As selected on the *Wireless > Wireless Security* screen, this displays the status of the Router’s wireless security.

Click **Refresh** to update the on-screen information.
Appendix A: Troubleshooting

Your computer cannot connect to the Internet.

Follow these instructions until your computer can connect to the Internet:

- Make sure that the Router is powered on. The Power LED should be green and not flashing.
- If the Power LED is flashing, then power off all of your network devices, including the modem, Router, and computers. Then power on each device in the following order:
  1. Cable or DSL modem
  2. Router
  3. Computer
- Check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Router, and the modem must be connected to the Internet port on the Router.

The modem does not have an Ethernet port.

The modem is a dial-up modem for traditional dial-up service. To use the Router, you need a cable/DSL modem and high-speed Internet connection.

You cannot use the DSL service to connect manually to the Internet.

After you have installed the Router, it will automatically connect to your Internet Service Provider (ISP), so you no longer need to connect manually.

The DSL telephone line does not fit into the Router's Internet port.

The Router does not replace your modem. You still need your DSL modem in order to use the Router. Connect the telephone line to the DSL modem, insert the setup CD into your computer, and then follow the on-screen instructions.

When you double-click the web browser, you are prompted for a username and password. If you want to get rid of the prompt, follow these instructions.

Launch the web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers):

1. Select Tools > Internet Options.
2. Click the Connections tab.
3. Select Never dial a connection.
4. Click OK.

The Router does not have a coaxial port for the cable connection.

The Router does not replace your modem. You still need your cable modem in order to use the Router. Connect your cable connection to the cable modem, insert the setup CD into your computer, and then follow the on-screen instructions.

The computer cannot connect wirelessly to the network.

Make sure the wireless network name or SSID is the same on both the computer and the Router. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Router.

You need to modify the settings on the Router.

Open the web browser (for example, Internet Explorer or Firefox), and enter the Router’s IP address in the address field (the default IP address is 192.168.1.1). When prompted, leave the User name field blank and enter the password to the Router (the default is admin). Click the appropriate tab to change the settings.

WEB: If your questions are not addressed here, refer to the Linksys website, www.linksys.com.
## Appendix B: Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>WRT54GL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
<td>IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b</td>
</tr>
</tbody>
</table>
| Channels         | 11 Channels (US, Canada)  
                 | 13 Channels (Europe, Japan) |
| Ports            | Internet: One 10/100 RJ-45 Port  
                 | LAN: Four 10/100 RJ-45 Switched Ports  
                 | One Power Port |
| Button           | Reset, SecureEasySetup |
| Cabling Type     | CAT5     |
| LEDs             | Power, DMZ, WLAN, LAN (1–4), Internet, SecureEasySetup |
| RF Power Output  | 18 dBm   |
| UPnP able/cert   | Able     |
| Security Features| Stateful Packet Inspection (SPI), Firewall, Internet Policy |
| Wireless Security| Wi-Fi Protected Access™2 (WPA2), WEP, Wireless MAC Filtering |

### Environmental

| Dimensions       | 7.32" x 1.89" x 6.06"  
                 | (186 x 48 x 154 mm) |
| Weight           | 13.8 oz (391 g) |
| Power            | External, 12V DC, 0.5A |
| Certifications   | FCC, ICES-003, CE, Wi-Fi (802.11b, 802.11g), WPA2, WMM |
| Operating Temp.  | 32 to 104°F (0 to 40°C) |
| Storage Temp.    | -4 to 158°F (-20 to 70°C) |
| Operating Humidity| 10 to 85%, Noncondensing |
| Storage Humidity | 5 to 90%, Noncondensing |
Appendix C: Warranty Information

Limited Warranty WRT54GL User Guide

Linksys warrants this Linksys hardware product against defects in materials and workmanship under normal use for the Warranty Period, which begins on the date of purchase by the original end-user purchaser and lasts for the period specified below:

- One (1) year for new product
- Ninety (90) days for refurbished product

This limited warranty is non-transferable and extends only to the original end-user purchaser. Your exclusive remedy and Linksys’ entire liability under this limited warranty will be for Linksys, at its option, to (a) repair the product with new or refurbished parts, (b) replace the product with a reasonably available equivalent new or refurbished Linksys product, or (c) refund the purchase price of the product less any rebates. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. All products and parts that are replaced become the property of Linksys.

Exclusions and Limitations

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Linksys, (c) the product damage was caused by use with non-Linksys products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Linksys does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY LINKSYS WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Linksys does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party’s service for which this product’s use or operation may require.

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

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

Obtaining Warranty Service

If you have a question about your product or experience a problem with it, please go to www.linksys.com/support where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at www.linksys.com. Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product to Linksys at your cost and risk. You must include the RMA number and a copy of your dated proof of original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be
rejected. Do not include any other items with the product you are returning to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys’ then-current rates.

**Technical Support**

This limited warranty is neither a service nor a support contract. Information about Linksys’ current technical support offerings and policies (including any fees for support services) can be found at: [www.linksys.com/support](http://www.linksys.com/support).

This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.
Appendix D: Regulatory Information

FCC Statement
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. IEEE 802.11b or 802.11g operation of this product in the USA is firmware-limited to channels 1 through 11.

Safety Notices
- Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

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

Industry Canada Statement
This Class B digital apparatus complies with Canadian ICES-003 and RSS210.
Operation is subject to the following two conditions:
1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device. This device has been designed to operate with an antenna having a maximum gain of 2dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

Industry Canada Radiation Exposure Statement:
This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
Avis d’Industrie Canada

Cet appareil numérique de la classe B est conforme aux normes NMB-003 et RSS210 du Canada.

L’utilisation de ce dispositif est autorisée seulement aux conditions suivantes :
1. il ne doit pas produire de brouillage et
2. il doit accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif. Le dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximum de 2 dBi. Les règlements d’Industrie Canada interdisent strictement l’utilisation d’antennes dont le gain est supérieur à cette limite. L’impédance requise de l’antenne est de 50 ohms.

Afin de réduire le risque d’interférence aux autres utilisateurs, le type d’antenne et son gain doivent être choisis de façon à ce que la puissance isotope rayonnée équivalente (p.i.r.e.) ne soit pas supérieure au niveau requis pour obtenir une communication satisfaisante.

Avis d’Industrie Canada concernant l’exposition aux radiofréquences :

Ce matériel est conforme aux limites établies par IC en matière d’exposition aux radiofréquences dans un environnement non contrôlé. Ce matériel doit être installé et utilisé à une distance d’au moins 20 cm entre l’antenne et le corps de l’utilisateur.

L'émetteur ne doit pas être placé près d’une autre antenne ou d’un autre émetteur, ou fonctionner avec une autre antenne ou un autre émetteur.

Wireless Disclaimer

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Avis de non-responsabilité concernant les appareils sans fil

Les performances maximales pour les réseaux sans fil sont tirées des spécifications de la norme IEEE 802.11. Les performances réelles peuvent varier, notamment en fonction de la capacité du réseau sans fil, du débit de la transmission de données, de la portée et de la couverture. Les performances dépendent de facteurs, conditions et variables multiples, en particulier de la distance par rapport au point d'accès, du volume du trafic réseau, des matériaux utilisés dans le bâtiment et du type de construction, du système d'exploitation et de la combinaison de produits sans fil utilisés, des interférences et de toute autre condition défavorable.

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

English - Environmental Information for Customers in the European Union

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

Dansk (Danish) - Miljøinformation for kunder i EU


Deutsch (German) - Umweltinformation für Kunden innerhalb der Europäischen Union


Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/EC изисква уредите, носещи този символ \(\equiv\) върху изделието и/или опаковката му, да не се изхвърлят с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Вашата е отговорността този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общинските органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще помогнат да се предотвратят евентуални вреди за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.
Appendix D

Regulatory Information

Greek (Greek) - Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι τα εξοπλισμοί οποίοι φέρει αυτό το σύμβολο δεν πρέπει να απορρίπτονται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν δεν πρέπει να απορρίπτεται κοινωνικά μαζί με τα άλλα εξοπλισμούς. Είναι υποχρεωτικό να ανακυκλώνει το προϊόν στο ελλείποντα σύστημα συλλογής απορριμμάτων και/ή στη συσκευασία στον οποίο έχετε αγοράσει το προϊόν.

Italiano (Italian) - Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

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

Appendix D

**Lietuvių** (Lithuanian) - Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įranga, kurī ir ± kurios pakuotė yra pažymėta šiuo simboliu (įveskite simbolį), negalima šašinti kuriai naudojosi tos pakuotės su nerūšiutomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminin reikia šašinti atskirai nuo bendro buitinio atliekų sauso. Jūs privalote užtikrinti, kad ši į kita elektrine ar elektronine įranga buť šalinta tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų kinkimo sistemos. Tikimaišai šalinti per perdirbimą, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie juos įsakymų mažiausiai maštite sjūrių ir mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite mažiausiai maštite maž...
Appendix D

Regulatory Information

Português (Portuguese) - Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo não seja eliminado junto com os resíduos municipais. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento elétrico e eletrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudam a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Română (Romanian) - Informații de mediu pentru clienții din Uniunea Europeană

Directiva europeană 2002/96/CE impune ca echipamentele care prezintă acest simbol să fie casate separat de gunoiul menajer obişnuit. Este responsabilitatea dvs. să casăți acest produs alte echipamente electrice și electronice prin intermediul unităților de colectare speciale desemnate de guvern sau de autoritățile locale. Casarea și reciclarea corecte vor ajuta la prevenirea potențialelor consecințe negative asupra sănătății mediului și a oamenilor. Pentru mai multe informații detaliate cu privire la casarea acestui echipament vechi, se contactează autoritățile locale, serviciul de salubrizare sau magazinul de la care ați achiziționat produsul.

Slovenčina (Slovak) - Informácie o ochrane životného prostredia pre zákazníkov v Európskej unii

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

Slovenčina (Slovene) - Okoljske informacije za stranke v Evropski uniji


Suomi (Finnish) - Ympäristöä koskevia tietoja EU-alueen asiakkaille


Svenska (Swedish) - Miljöinformation för kunder i Europeiska unionen


WEB: For additional information, please visit www.linksys.com
Appendix E: Software License Agreement

Software in Linksys Products

This product from Cisco-Linksys LLC or from one of its affiliates Cisco Systems-Linksys (Asia) Pte Ltd. or Cisco-Linksys K.K. (“Linksys”) contains software (including firmware) originating from Linksys and its suppliers and may also contain software from the open source community. Any software originating from Linksys and its suppliers is licensed under the Linksys Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept that Linksys Software License Agreement upon installation of the software.

Any software from the open source community is licensed under the specific license terms applicable to that software made available by Linksys at www.linksys.com/gpl or as provided for in Schedules 2 and 3 below.

Where such specific license terms entitle you to the source code of such software, that source code is upon request available at cost from Linksys for at least three years from the purchase date of this product and may also be available for download from www.linksys.com/gpl. For detailed license terms and additional information on open source software in Linksys products please look at the Linksys public web site at: www.linksys.com/gpl/ or Schedule 2 below as applicable.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE SOFTWARE LICENSE AGREEMENTS BELOW. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

Schedule 1 - Linksys Software License Agreement

THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS LLC OR ONE OF ITS AFFILIATES CISCO SYSTEMS-LINKSYS (ASIA) PTE LTD. OR CISCO-LINKSYS K.K. (“LINKSYS”) LICENSING THE SOFTWARE INSTEAD OF CISCO-LINKSYS LLC. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

License. Subject to the terms and conditions of this Agreement, Linksys grants the original end user purchaser of the Linksys product containing the Software (“You”) a nonexclusive license to use the Software solely as embedded in or (where authorized in the applicable documentation) for communication with such product. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Linksys product containing the Software, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.

“Software” includes, and this Agreement will apply to (a) the software of Linksys or its suppliers provided in or with the applicable Linksys product, and (b) any upgrades, updates, bug fixes or modified versions (“Upgrades”) or backup copies of the Software supplied to You by Linksys or an authorized reseller, provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade.

Protection of Information. The Software and documentation contain trade secrets and/or copyrighted materials of Linksys or its suppliers. You will not copy or modify the Software or decompile, decrypt, reverse engineer or disassemble the Software (except to the extent expressly permitted by law notwithstanding this provision), and You will not disclose or make available such trade secrets or copyrighted material in any form to any third party. Title to and ownership of the Software and documentation and any portion thereof, will remain solely with Linksys or its suppliers.

Collection and Processing of Information. You agree that Linksys and/or its affiliates may, from time to time, collect and process information about your Linksys product and/or the Software and/or your use of either in order (i) to enable Linksys to offer you Upgrades; (ii) to ensure that your Linksys product and/or the Software is being...
used in accordance with the terms of this Agreement; (iii) to provide improvements to the way Linksys delivers technology to you and to other Linksys customers; (iv) to enable Linksys to comply with the terms of any agreements it has with any third parties regarding your Linksys product and/or Software and/or (v) to enable Linksys to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Linksys and/or its affiliates may collect and process this information provided that it does not identify you personally. Your use of your Linksys product and/or the Software constitutes this consent by you to Linksys and/or its affiliates’ collection and use of such information and, for EEA customers, to the transfer of such information to a location outside the EEA.

**Software Upgrades etc.** If the Software enables you to receive Upgrades, you may elect at any time to receive these Upgrades either automatically or manually. If you elect to receive Upgrades manually or you otherwise elect not to receive or be notified of any Upgrades, you may expose your Linksys product and/or the Software to serious security threats and/or some features within your Linksys product and/or Software may become inaccessible. There may be circumstances where we apply an Upgrade automatically in order to comply with changes in legislation, legal or regulatory requirements or as a result of requirements to comply with the terms of any agreements Linksys has with any third parties regarding your Linksys product and/or the Software. You will always be notified of any Upgrades being delivered to you. The terms of this license will apply to any such Upgrade unless the Upgrade in question is accompanied by a separate license, in which event the terms of that license will apply.

**Open Source Software.** The GPL or other open source code incorporated into the Software and the open source license for such source code are available for free download at [http://www.linksys.com/gpl](http://www.linksys.com/gpl). If You would like a copy of the GPL or other open source code in this Software on a CD, Linksys will mail to You a CD with such code for $9.99 plus the cost of shipping, upon request.

**Term and Termination.** You may terminate this License at any time by destroying all copies of the Software and documentation. Your rights under this License will terminate immediately without notice from Linksys if You fail to comply with any provision of this Agreement.

**Limited Warranty.** The warranty terms and period specified in the applicable Linksys Product User Guide shall also apply to the Software.

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

**Export.** Software, including technical data, may be subject to U.S. export control laws and regulations and/or export or import regulations in other countries. You agree to comply strictly with all such laws and regulations.

**U.S. Government Users.** The Software and documentation qualify as ‘commercial items’ as defined at 48 C.F.R. 2.101 and 48 C.F.R. 12.212. All Government users acquire the Software and documentation with only those rights herein that apply to non-governmental customers.

**General Terms.** This Agreement will be governed by and construed in accordance with the laws of the State of California, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions will remain in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Software and supersedes any conflicting or additional terms contained in any purchase order or elsewhere.

**END OF SCHEDULE 1**

**Schedule 2**

If this Linksys product contains open source software licensed under Version 2 of the ‘GNU General Public License’ then the license terms below in this Schedule 2 will apply to that open source software. The license terms below in this Schedule 2 are from the public web site at [http://www.gnu.org/copyleft/gpl.html](http://www.gnu.org/copyleft/gpl.html)

**GNU GENERAL PUBLIC LICENSE**

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

**Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your
freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
Appendix E

Software License Agreement

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   c. Accompany it with the information you received as to the offer to distribute corresponding source code.

   (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients’ exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to let software distributed through that system remain under this License.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 2

Schedule 3

If this Linksys product contains open source software licensed under the OpenSSL license:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit: (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
Appendix E

Software License Agreement

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

In addition, if this Linksys product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at http://www.openssl.org/source/license.html.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)."
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)."

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, Ihash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

END OF SCHEDULE 3