Icon Descriptions

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

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

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

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

Online Resources

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

<table>
<thead>
<tr>
<th>Resource</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linksys</td>
<td><a href="http://www.linksys.com">www.linksys.com</a></td>
</tr>
<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

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2007 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.
Appendix C: Warranty and Regulatory Information

Limited Warranty .................................................. 24
Wireless Disclaimer .................................................. 25
FCC Statement ...................................................... 25
Safety Notices .......................................................... 25
Industry Canada (Canada) .............................................. 25
IC Statement ............................................................. 25
Règlement d’Industry Canada ........................................ 25
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
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.
**Static IP**

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

![Internet Connection Type > Static IP](image)

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

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

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

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

**PPPoE**

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

![Internet Connection Type > PPPoE](image)

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

**Connect on Demand: Max Idle Time** You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the **Max Idle Time** field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

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

**PPTP**

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

![Internet Connection Type > PPTP](image)

**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.
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.

Telstra Cable

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

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

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

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes.

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

Optional Settings

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

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

**DDNS Service**

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

**DynDNS.org**

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

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

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

**Internet IP Address**  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, TZO Key, and Domain Name**  Enter the settings of the account you set up with TZO.

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

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

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

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.

**MAC Address Clone**

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

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

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

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

**Setup > Advanced Routing**

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

Operating Mode Select the mode in which this Router will function. If this Router is hosting your network's connection to the Internet, select Gateway. If another Router exists on your network, select Router. When Router is chosen, Dynamic Routing will be available as an option.

Dynamic Routing

RIP This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. This feature is Disabled by default. From the drop-down menu, you can also select LAN & Wireless, which performs dynamic routing over your Ethernet and wireless networks. You can also select WAN (Internet), which performs dynamic routing with data coming from the Internet. Finally, selecting Both enables dynamic routing for both networks, as well as data from the Internet.

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

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

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

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

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

Interface This interface tells you whether the Destination IP Address is on the LAN & Wireless (Ethernet and wireless networks) or the WAN (Internet).

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

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

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

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

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

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

**Wireless SSID Broadcast** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router’s SSID, keep the default setting, *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 to your network.

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

### Wireless > Wireless Security

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

### Wireless Security

**Security Mode**

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

**WPA Personal**

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

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

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

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

**WPA Enterprise**

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

- **WPA Algorithm**  WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)
- **RADIUS Server Address** Enter the IP Address of the RADIUS server.
- **RADIUS Port** Enter the port number of the RADIUS server. The default value is **82**.
- **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 **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**

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

---

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

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

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

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

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

---

**Wireless > Wireless MAC Filter**

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

**Wireless MAC Filter**

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

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

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

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.

**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**

**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 & 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 & Gaming > Port Triggering

The Applications & 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.
Port Triggering

**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.

**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.
Advanced Configuration

Chapter 3

Applications and Gaming > QoS

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.
Router Password

Local Router Access

Router Password  Enter a new Password for the Router.
Re-enter to confirm  Enter the Password again to confirm.

Web Access

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

Wireless Access Web  If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router’s web-based utility. You will only be able to access the web-based utility via a wired connection if you disable the setting. Keep the default, Enable, to enable wireless access to the Router’s web-based utility, or select Disable to disable wireless access to the utility.

Remote Router Access

Remote Management  To access the Router remotely, from outside the network, select Enable.

Management Port  Enter the port number that will be open to outside access. You will need to enter the Router’s password when accessing the Router this way, as usual.

Use HTTPS  To require the use of HTTPS for remote access, select this feature.

UPnP

UPnP  Keep the default, Enable to enable the UPnP feature; otherwise, select Disable.
Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

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.

![The Traceroute Test](image)

**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 > Factory Defaults](image)

**Administration > Upgrade Firmware**

The **Administration > Upgrade Firmware** 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.

![Administration > Upgrade Firmware](image)

Before upgrading the firmware, download the Router’s firmware upgrade file from the Linksys website, [www.linksys.com](http://www.linksys.com). Then extract the file.

**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.

![Administration > Config Management](image)

**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.

![Status > Wireless](image)

**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>WRT54G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
<td>IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b</td>
</tr>
<tr>
<td>Channels</td>
<td>11 Channels (US, Canada)</td>
</tr>
<tr>
<td></td>
<td>13 Channels (Europe, Japan)</td>
</tr>
<tr>
<td>Ports</td>
<td>Internet: One 10/100 RJ-45 Port</td>
</tr>
<tr>
<td></td>
<td>LAN: Four 10/100 RJ-45 Switched Ports</td>
</tr>
<tr>
<td></td>
<td>One Power Port</td>
</tr>
<tr>
<td>Button</td>
<td>Reset, SecureEasySetup</td>
</tr>
<tr>
<td>Cabling Type</td>
<td>CAT5</td>
</tr>
<tr>
<td>LEDs</td>
<td>Power, DMZ, WLAN, LAN (1-4), Internet, SecureEasySetup</td>
</tr>
<tr>
<td>RF Power Output</td>
<td>18 dBm</td>
</tr>
<tr>
<td>UPnP able/cert</td>
<td>Able</td>
</tr>
<tr>
<td>Security Features</td>
<td>Stateful Packet Inspection (SPI)</td>
</tr>
<tr>
<td></td>
<td>Firewall, Internet Policy</td>
</tr>
<tr>
<td>Wireless Security</td>
<td>Wi-Fi Protected Access™2 (WPA2), WEP, Wireless MAC Filtering</td>
</tr>
</tbody>
</table>

### Environmental

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>7.32&quot; x 1.89&quot; x 6.06&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(186 x 48 x 154 mm)</td>
</tr>
<tr>
<td>Weight</td>
<td>11.2 oz (317 g)</td>
</tr>
<tr>
<td>Power</td>
<td>External, 12V DC, 0.5A</td>
</tr>
<tr>
<td>Certifications</td>
<td>FCC, IC-03, CE, Wi-Fi (802.11b, 802.11g), WPA2, WMM</td>
</tr>
<tr>
<td>Operating Temp.</td>
<td>32 to 104°F (0 to 40°C)</td>
</tr>
<tr>
<td>Storage Temp.</td>
<td>-4 to 158°F (-20 to 70°C)</td>
</tr>
<tr>
<td>Operating Humidity</td>
<td>10 to 85%, Noncondensing</td>
</tr>
<tr>
<td>Storage Humidity</td>
<td>5 to 90%, Noncondensing</td>
</tr>
</tbody>
</table>
Appendix C: Warranty and Regulatory Information

Limited Warranty

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

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

All implied warranties and conditions of merchantability or fitness for a particular purpose are limited to the duration of the warranty period. All other express or implied conditions, representations and warranties, including any implied warranty of non-infringement, are disclaimed. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

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

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

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.
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, interference and other adverse conditions.

FCC Statement

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

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

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 (Canada)

This device complies with Industry Canada ICES-003 rule. Cet appareil est conforme à la norme NMB003 d’Industrie Canada.

IC Statement

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.

Règlement d’Industry Canada

Le fonctionnement est soumis aux conditions suivantes :

1. Ce périphérique ne doit pas causer d’interférences;
2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d’entrainer un fonctionnement indésirable.
User Information for Consumer Products
Covered by EU Directive 2002/96/EC on
Waste Electric and Electronic Equipment
(WEEE)

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

![WEEE Symbol]

English - Environmental Information for Customers in the European Union

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

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

Европейска директива 2002/96/ЕС изисква уредите, носещи този символ на продукта или на опаковката му, да не се изхвърлят с несортираните битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от обикновените битови отпадъци. Вашата отговорност е да уреждате уреждането на този и другите електрически и електронни уреди в определена местност, въвеждана от вашите местни власти. Коректно уреждане и рециклиране ще допринесат за предотвратяване на евентуални негативни резултати за околната среда и здравето на населението. За по-допълнителна информация относно уреждането на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.

Čeština (Czech) - Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

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

Dansk (Danish) - Miljøinformation for kunder i EU


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

Eesti (Estonian) - Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele


Español (Spanish) - Información medioambiental para clientes de la Unión Europea

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

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

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι το εξοπλισμός ο ποιός φέρει αυτό το σύμβολο ∋ στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινωνικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν δεν πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος προϊόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη και προστασία της καταστάσης από το οποίο αγοράσατε το προϊόν.

Français (French) - Informations environnementales pour les clients de l’Union européenne

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

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

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

Latviešu valoda (Latvian) - Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Warranty and Regulatory Information

Appendix C

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

Europos direktyva 2002/96/EC numato, kad įranko, kurį ir ☐ kurios pakuotė yra pažymėta šiuo simboliu (iveskite simbolį), negalima šaltinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminio reikia šaltinti atskirai nuo bendro buitiniojų atliekų srauto. Jūs privalote užtikrinti, kad ši iki elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemos. Tinkamai šalinti ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiaus informacijos apie įrankio šalinimo ir jo reciklingą pateikia vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduočiavusvės, kuriose įsigijote šį gaminį.

Malti (Maltese) - Informazzjoni Ambjentali ghal Klijenti fl-Unjoni Ewropea


Magyar (Hungarian) - Környezetvédelmi információ az euópai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megbízóvá, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke ☐ megjelenik, illosz a többi szeléktálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kiadásakor a szokványos háztartási hulladékkal együtt kidobható. A megfelelő hulladékdolgozás segít a környezet és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékdolgozási szolgálattal, vagy azonnal üzzetlet, ahol a terméket vásarolta.

Nederlands (Dutch) - Milieu-informatie voor klanten in de Europese Unie

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

Norsk (Norwegian) - Miljøinformasjon for kunder i EU


Polski (Polish) - Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrekttywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem ☐ znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucony razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu na własną rękę, bez zgody lokalnych władz, jest zakazane i karane przez państwo.
Warranty and Regulatory Information

Appendix C

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

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

Română (Romanian) - Informaţii de mediu pentru clienţii din Uniunea Europeană


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

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