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>Vodafone</td>
<td><a href="http://www.vodafone.com">www.vodafone.com</a></td>
</tr>
<tr>
<td>Linksys</td>
<td><a href="http://www.linksys.com/vodafone">www.linksys.com/vodafone</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>
<thead>
<tr>
<th>Appendix B: Specifications</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix C: Warranty Information</td>
<td>38</td>
</tr>
<tr>
<td>Limited Warranty</td>
<td>38</td>
</tr>
<tr>
<td>Exclusions and Limitations</td>
<td>38</td>
</tr>
<tr>
<td>Obtaining Warranty Service</td>
<td>38</td>
</tr>
<tr>
<td>Technical Support</td>
<td>39</td>
</tr>
<tr>
<td>Appendix D: Regulatory Information</td>
<td>40</td>
</tr>
<tr>
<td>FCC Statement</td>
<td>40</td>
</tr>
<tr>
<td>Industry Canada Statement</td>
<td>40</td>
</tr>
<tr>
<td>Avis d’Industrie Canada</td>
<td>40</td>
</tr>
<tr>
<td>Wireless Disclaimer</td>
<td>41</td>
</tr>
<tr>
<td>Avis de non-responsabilité concernant les appareils sans fil</td>
<td>41</td>
</tr>
<tr>
<td>Safety Notices</td>
<td>41</td>
</tr>
<tr>
<td>Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&amp;TTE Directive)</td>
<td>42</td>
</tr>
<tr>
<td>CE Marking</td>
<td>43</td>
</tr>
<tr>
<td>IDA Standards</td>
<td>43</td>
</tr>
<tr>
<td>Product Usage Restrictions</td>
<td>44</td>
</tr>
<tr>
<td>Technical Documents on <a href="http://www.linksys.com/international">www.linksys.com/international</a></td>
<td>44</td>
</tr>
<tr>
<td>Appendix E: Software License Agreement</td>
<td>49</td>
</tr>
<tr>
<td>Software in Linksys Products</td>
<td>49</td>
</tr>
<tr>
<td>Software Licenses</td>
<td>49</td>
</tr>
<tr>
<td>Appendix E: Contact Information</td>
<td>56</td>
</tr>
<tr>
<td>Vodafone Online Resource</td>
<td>56</td>
</tr>
<tr>
<td>Vodafone Technical Support</td>
<td>56</td>
</tr>
</tbody>
</table>
Chapter 1: Product Overview

Thank you for choosing the Linksys Wireless-G Router for 3G/UMTS Broadband. The Wireless-G Router for 3G/UMTS Broadband, lets you access the Internet through either your HSDPA/3G/UMTS or GPRS service (requires a Vodafone Mobile Connect HSDPA/3G/UMTS data card, available separately), or you can use a cable or DSL modem for broadband service. Plus, this access can be shared over the four switched ports or via the wireless broadcast at up to 54Mbps for Wireless-G or up to 11Mbps for Wireless-B.

A variety of security features help to protect your data and your privacy while online. Security features include WPA2 (Wi-Fi Protected Access 2) security, a Stateful Packet Inspection (SPI) firewall, and NAT technology. Configuring the Router is easy using the Setup Wizard or through the provided browser-based utility.

Top Panel

If you have a Vodafone data card, use the PC Card slot. If you have a Vodafone USB adapter, use one of the USB ports.

**NOTE:** The Router supports a single mobile broadband device. Connect either a data card or a USB adapter—do not connect both at the same time.

**3G/UMTS USB Ports** Insert the Vodafone Mobile Connect HSDPA/3G/UMTS data card (available separately) into this port if the Router will connect to a HSDPA/3G/UMTS or GPRS service.

**Mobile PC Card Slot** If the Router will connect to a mobile broadband service, insert the mobile broadband data card (available separately) into this slot. After the data card is inserted, the eject button will pop up. To remove the data card, press the eject button.

**Mobile Connect/Disconnect Button** Press this button to connect to and disconnect from the mobile network. (You can also use the Basic Setup screen of the Router’s web-based utility.)

Side Panel

- **USB Port** Reserved for future use.
- **Power** (Green) The Power LED lights up and stays on while the Router is powered on.
- **Ethernet 1-4** (Green) These numbered LEDs, corresponding with the numbered ports on the Router’s back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. It flashes to indicate network activity over that port.
- **Wireless** (Green) The Wireless LED lights up when the wireless feature is enabled. It flashes when the Router is actively sending or receiving data over the wireless network.
- **Modem Internet** (Green) The Modem LED lights up and stays on when there is a connection made through the Modem port. It flashes to indicate network activity over the Modem port.
- **3G/UMTS Internet** (Blue/Green) The 3G/UMTS LED flashes as the Router connects to the mobile network. When the LED stops flashing and stays on, then the connection is active. When the LED is blue, a 3G/UTMS/HSDPA connection has been established. When the LED is green, a GPRS connection has been established.

If the LED flashes quickly, the Router is not connected to the mobile network. Before pressing the Mobile Connect/Disconnect button, make sure the mobile broadband data card or USB adapter is already installed.
Opposite Side Panel with Antenna

**Modem** The Modem port is where you will connect your cable or DSL modem.

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

**Security Bracket** The security bracket labeled “Reset” clips onto the Router. It covers the Reset button and the security slot on the Router’s top panel. You can remove the security bracket to access the Reset button.

**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 the *Administration > Factory Defaults* screen of the Router’s web-based utility.

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

Front Panel

**Security Slot** To protect the Router from theft, you can attach a lock to the Router using the security slot.

Bottom Panel

To place the Router in a vertical position, rotate the stand 90 degrees.
Placement Positions

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

Horizontal Placement

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

Vertical Placement

The Router has a stand on the panel opposite to the antenna. Rotate the stand 90 degrees, and place the Router on a level surface near an electrical outlet.

Wall-Mounting Placement

The Router has four wall-mount slots on its back panel. The distance between two adjacent slots is 68 mm (2.68 inches).

Two screws are needed to mount the Router.

<table>
<thead>
<tr>
<th>Suggested Mounting Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-5 mm</td>
</tr>
<tr>
<td>1-1.5 mm</td>
</tr>
<tr>
<td>2.5-3.0 mm</td>
</tr>
</tbody>
</table>

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

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

Follow these instructions:

1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.
2. Drill two holes into the wall. Make sure the holes are 68 mm (2.68 inches) apart.
3. Insert a screw into each hole and leave 3 mm (0.12 inches) of its head exposed.
4. Maneuver the Router so two of the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.

Print this page at 100% size. Cut along the dotted line, and place on the wall to drill precise spacing.
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, routers, and gateways, 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 and gateways 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.

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 login screen will appear. (Non-Windows XP users will see a similar screen.) Enter **admin** (the default) in both the **Username** and **Password** fields. (You can set a new password on 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.

**3G/UMTS Setup**

Configure the HSDPA/3G/UMTS and/or GPRS settings for the Router in this section.

**Mobile Connection** This button enables you to connect to and disconnect from the HSDPA/3G/UMTS or GPRS network through the Web-based Utility (you can also connect and disconnect using the hardware button on the Router). It will also indicate the status of the Router's HSDPA/3G/UMTS or GPRS connection.

**Service** If you want the Router to connect to a HSDPA/3G/UMTS signal when available Select HSDPA/3G/UMTS Preferred (recommended). If the HSDPA/3G/UMTS signal is not available, then Router will use a GPRS connection. If the Router is having problems maintaining a connection, you can select HSDPA/3G/UMTS Only or GPRS Only. Then the Router will be able to connect to only one type of signal.

**Mobile Network Bearer** The name of the mobile network bearer the Router is using is displayed.

**Network Name** The name of the HSDPA/3G/UMTS or GPRS network the Router is using is displayed.
**Signal Strength**  This indicates the strength of the HSDPA/3G/UMTS or GPRS signal that the Router is receiving

**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. These are the available types:

- 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.)

**Static IP**

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

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

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

**Default Gateway**  Your ISP will provide you with the IP address of the ISP server.

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

**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.

**Username and Password**  Enter the Username 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 **15** 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, 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 IP Address  This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP address you need to specify here.

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

Default Gateway  Your ISP will provide you with the IP address of the ISP server.

Username and Password  Enter the Username and Password provided by your ISP.

Connect on Demand: Max Idle Time  You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 15 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, 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.

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

Username and Password  Enter the Username and Password provided by your ISP.

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

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

L2TP

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

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

### Optional Settings

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

**MTU** MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the Router select the best MTU for your Internet connection, keep the default, Auto.

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

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

### Network Setup

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

**Router IP**

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

**DHCP Server Settings**

This setting determines how the clients (network devices) use DNS/WINS.

**Mode 1 - Fixed configuration (Default)** Select this option if you want the Router to advertise itself as the DNS server to use and handle upstream changes automatically.

**Mode 2 - Network Supplied** Select this option if you want the Router to pass through the DNS server values (learned from the Modem port or mobile network) to the client, depending on how the Router is currently connected.

**NOTE:** If the upstream DNS servers change between connections, the clients may become unable to resolve addresses because they have valid DHCP leases that use the old server values.

**Mode 3 - Manual configuration** Select this option if you want to set arbitrary DNS/WINS values for the clients to use. These values are not validated by the Router.

**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 default. If you already have a DHCP server on your network, or you don’t want a DHCP server, then select Disabled (no other DHCP features will be available).

**DHCP Reservation** Click this button if you want to assign a fixed local IP address to a MAC address.

**DHCP Reservation** You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address.
Select Clients from DHCP Table  Click the Select check box to reserve a client’s IP address. Then click Add Clients.

Manually Adding Client  To manually assign an IP address, enter the client’s name in the Enter Client Name field. Enter the IP address you want it to have in the Assign IP Address field. Enter its MAC address in the To This MAC Address field. Then click Add.

Clients Already Reserved  
A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click Remove.

Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. To view the most up-to-date information, click Refresh. To exit this screen, click Close.

Start IP Address  Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router’s default IP address is 192.168.1.100, the Start IP Address must be 192.168.1.101 or greater, but smaller than 192.168.1.253. The default is 192.168.1.100.

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

IP Address Range  Displayed here is the range of available IP addresses.

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  These settings are available if you selected Mode 3 - Manual configuration for the DHCP Server Setting. 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 0-1  These settings are available if you selected Mode 3 - Manual configuration for the DHCP Server Setting. 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. You can enter up to two WINS server IP addresses here. Otherwise, leave these fields blank.

Time Setting

Time Zone  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 > Mobile Network

Configure mobile network settings and view status information for your mobile broadband service and device (data card or USB adapter). Some of these settings will be automatically configured by the Router and, in most cases, should not be changed unless you are instructed to do so.

**Auto Connect**  If this feature is enabled, the Router will automatically connect to the default HSDPA/3G/UMTS or GPRS network when it powers on. The default is **Disabled**. You can use the Mobile Connect/Disconnect button on the Router to connect and disconnect from the mobile network.

**Connect on Demand: Max Idle Time** You can configure the Router to cut the mobile network connection after it has been inactive for a specified period of time (Max Idle Time). If your mobile network 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 mobile network connection terminates. The default Max Idle Time is 60 minutes.

**Keep Alive: Redial Period** If you select this option, you can specify how often the Router will periodically check your mobile network connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**.

- **Reset data card**  To reset the data card after a number of failed attempts, select this option. The default number of failed connection attempts is 5.

- **Link Check**  You can have the Keep Alive Server link checked through **LCP** (Link Control Protocol) or **ICMP** (Internet Control Message Protocol). The server will be pinged in the number of seconds specified. The default is 30 seconds. After the number of tries specified with no response, (default is 3), the LCP or ICMP will attempt to re-establish the connection. For ICMP you can also choose to automatically reboot your connection if a specified number of seconds have passed since the last reply. The default is 300. You can also enter up to two server IP addresses to use.

**Disconnect if idle for**  If you want to disconnect the Router from the HSDPA/3G/UMTS or GPRS network if no data has been sent or received from the Vodafone network for a specific period of time, then enter the number of minutes you want to specify in the field provided. The default is 0.

**PAP or CHAP Authentication**

Select the authentication type used by your service provider: PAP or CHAP. If you do not know which type to use, select Auto.

**APN Configuration**

Configure how the Router will select its Access Point Name (APN) or network.

**APN Selection Mode**  If you want the Router to select a suitable APN based on the current SIM card, select Auto. If you want to override the automatic selection, select Manual. Then select a suitable APN from the Home Network drop-down menu. If you want to specify values that may not be in the standard configuration (such as a corporate APN), select Custom Values. Then complete the APN Name, Username, Password, DNS Supplied by Network, and DNS 1-2 fields as needed.

If you selected Custom Values, complete the following:

**APN Name**  The APN (Access Point Name) Name is automatically entered by the Router. Do not change this
setting unless told to do so by either Vodafone or Linksys technical support, or the IT manager of your company. If you have access to a private APN, you can enter its name here.

Username The Username is automatically entered by the Router. Do not change this setting unless told to do so by either Vodafone or Linksys technical support, or the IT manager of your company. If you have access to a private APN, you can enter the new Username here.

Password The Password is automatically entered by the Router. Do not change this setting unless told to do so by either Vodafone or Linksys technical support, or the IT manager of your company. If you have access to a private APN, you can enter the new Password here.

DNS Supplied by Network If the network automatically supplies the DNS address(es), click Enable (default). If you need to specify the DNS address(es), remove the checkmark, and enter the DNS address(es) in the DNS 1-2 fields.

DNS 1-2 Enter the DNS address(es) you want the Router to use.

PIN Code If required, enter the PIN code of your SIM card. The code will be stored here for future reference by the Router, and you will not have to re-enter this unless you change SIM cards.

Mobile Network Status

Mobile Network Bearer The name of the mobile network bearer the Router is using is displayed.

Network Name The name of the HSDPA/3G/UMTS or GPRS network the Router is using is displayed. To select a different network, click the Select Network button and follow the on-screen instructions.

Signal Strength The strength of the HSDPA/3G/UMTS or GPRS signal that the Router is receiving is displayed.

Connection Time The length of time the Router has been connected to the HSDPA/3G/UMTS or GPRS network since your last connection is displayed.

Current Session Usage The amount of data that has been sent to and received from the HSDPA/3G/UMTS or GPRS network since your last connection is displayed.

3G/UMTS Card Status

Card Model The model number of your Vodafone card is displayed.

Card Revision The revision number of your Vodafone card is displayed.

Card Firmware The firmware version of your Vodafone card is displayed.

IMSI IMSI (International Mobile Subscriber Identity) is a fixed identification number and is read automatically from the Vodafone card.

Click Refresh to update the on-screen information.

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, Disabled.

**DDNS**

**DDNS Service**

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

DynDNS.org

Username Enter the Username for your DDNS account.

Password Enter the Password for your DDNS account.

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

System Select the DynDNS service you use: Dynamic, Static, or Custom. The default is Dynamic.
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, Disabled. To enable the feature, select Enabled. If you are not sure which setting to select, keep the default, Disabled.

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, Disabled. To enable wildcards, select Enabled. If you are not sure which setting to select, keep the default, Disabled.

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.

Update To manually trigger an update, click this button. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

Setup > MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.

Setup > 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.

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.

Update To manually trigger an update, click this button. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.
Advanced Routing

NAT

Enabled/Disabled If this Router is hosting your network’s connection to the Internet, keep the default, Enabled. If another router exists on your network, select Disabled. When the NAT setting is disabled, dynamic routing will be enabled.

Dynamic Routing (RIP)

Enabled/Disabled This feature enables the Router to automatically adjust to physical changes in the network’s layout and exchange routing tables with the other router(s). The Router determines the network packets’ route based on the fewest number of hops between the source and the destination. When the NAT setting is enabled, the Dynamic Routing feature is automatically disabled. When the NAT setting is disabled, this feature is available. Select Enabled to use the Dynamic Routing feature.

Static Routing

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.

Route Entries To set up a static route between the Router and another network, select a number from the drop-down list. Click Delete This Entry to delete a static route.

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

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

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

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

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

Click Show Routing Table to view the static routes you have already set up.

Routing Table

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.

Basic Wireless Settings

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

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.

Standard Channel Select the channel you want to use for wireless networking.
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, Enabled. If you do not want to broadcast the Router’s SSID, then select Disabled.

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

Wireless > Wireless Security

The Wireless Security screen configures the security of your wireless network. There are six wireless security mode options supported by the Router: WPA Personal, WPA2 Personal, WPA Enterprise, WPA2 Enterprise, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security method 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.”

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 passphrase, or else the network will not function properly.

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

Passphrase Enter a Passphrase of 8-63 characters.

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

WPA2 Personal

Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or AES or TKIP. The default is AES or TKIP.

Passphrase Enter a Passphrase of 8-63 characters.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default 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.)

Encryption 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 Enter the IP address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default is 1812.
**Shared Secret**  Enter the key shared between the Router and the server.

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

### Encryption

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

**RADIUS Server**  Enter the IP address of the RADIUS server.

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

**Shared Secret**  Enter the key shared between the Router and the server.

**Key Renewal**  Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default 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**  Enter the IP address of the RADIUS server.

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

**Shared Secret**  Enter the key shared between the Router and the server.

**Encryption**  Select a level of WEP encryption, 40/64 bits (10 hex digits) or 104/128 bits (26 hex digits). The default is 40/64 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.

**TX Key**  Select which TX (Transmit) Key to use. The default is 1.
WEP

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

**Encryption** Select a level of WEP encryption, 40/64 bits (10 hex digits) or 104/128 bits (26 hex digits). The default is 40/64 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.

**TX Key** Select which TX (Transmit) Key to use. The default is 1.

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.

**Enabled/Disabled** To filter wireless users by MAC Address, either permitting or blocking access, select **Enabled**. To not filter users by MAC Address, keep the default, **Disabled**.

**Access Restriction**

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

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

**MAC Address Filter List**

**Wireless Client List** Click this to open the **Wireless Client List** screen.
Chapter 3

Advanced Configuration

Wireless Client List

This screen shows computers and other devices on the wireless network. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Status.

Select Save to MAC Address Filter List for any device you want to add to the MAC Address Filter List. Then click Add.

To retrieve the most up-to-date information, click Refresh. To exit this screen and return to the Wireless MAC Filter screen, click Close.

MAC 01-50 Enter the MAC addresses of the devices whose wireless access you want to block or allow.

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

Wireless > Advanced Wireless Settings

This 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

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 Enabled. AP Isolation is disabled by default.

Frame Burst Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use this option, keep the default, Enabled. Otherwise, select Disabled.

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. Select Shared Key to only use Shared Key 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 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 is Auto.

CTS Protection Mode The Router will automatically use CTS (Clear-To-Send) Protection Mode when your Wireless-N and Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance. The default is Auto.

Beacon Interval 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. The default is 100.

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 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 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.

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

**Security > Firewall**

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

**Firewall**

**SPI Firewall Protection**  To use firewall protection, keep the default, **Enabled**. To turn off firewall protection, select **Disabled**.

**Internet Filter**

**Filter 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. Select this feature to filter multicasting. This feature is not selected by default.

**Filter Internet NAT Redirection**  This feature uses port forwarding to block access to local servers from local networked computers. Select this feature to filter Internet NAT redirection. It 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.

**Web Filter**

**Proxy**  Use of WAN proxy servers may compromise the Gateway’s security. Denying Proxy will disable access to any WAN proxy servers. Select this feature to enable proxy filtering. Deselect the feature to allow proxy access.

**Java**  Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable Java filtering. Deselect the feature to allow Java usage.

**ActiveX**  ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable ActiveX filtering. Deselect the feature to allow ActiveX usage.

**Cookies**  A cookie is data stored on your computer and used by Internet sites when you interact with them. Select this feature to filter cookies. Deselect the feature to allow cookie usage.

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

**Security > VPN Passthrough**

The **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, **Enabled**.

**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, **Enabled**.
**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, **Enabled**.

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

**Security > PPTP Mobile**

The **PPTP Mobile** screen allows you to enable PPTP Mobile server information to pass through the Router’s firewall.

**Security > L2TP Mobile**

The **L2TP Mobile** screen allows you to enable L2TP Mobile server information to pass through the Router’s firewall.

**Login Status** To log in to L2TP Mobile, click Connect.

**Username** Enter your L2TP Mobile username in the field.

**Password** Enter your L2TP Mobile password in the field.

**L2TP Server** Enter the name of the L2TP server.

**Auto Connect** Select Enable to automatically connect to the server.

**Keep Alive: Redial Period** If you select this option, you can specify how often the Router will periodically check your mobile network connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**.
Access Restrictions > Internet Access

The 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 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 This Policy. To view all the policies, click Summary.

Summary

The policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, select Enabled. To delete a policy, click Delete. Click Save Settings to save your changes, or click Cancel Changes to cancel your changes. To return to the Internet Access Policy screen, click Close.

List of PCs

5. Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select Everyday. Then enter a range of hours and minutes during which the policy will be in effect, or select 24 Hours.

7. You can block websites with specific URL addresses. Enter each URL in a separate Website Blocking by URL Address field.

8. You can also block websites using specific keywords. Enter each keyword in a separate Website Blocking by Keyword field.

9. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.)

From the Applications list, select the application you want to block. Then click the >> button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the << button.

10. If the application you want to block is not listed or you want to edit a service’s settings, enter the application name in the Port Range fields. Select its protocol from the Protocol drop-down menu. Then click Add.

To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click Modify.

To delete a service, select it from the Application list. Then click Delete.

11. Click Save Settings to save the policy’s settings. To cancel the policy’s settings, click Cancel Changes.

Applications and Gaming > Single Port Forwarding

The Single Port Forwarding screen allows you to customize port services for common applications on this screen.

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen).

Applications and Gaming > Single Port Forwarding

Common applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Select Enabled to activate this entry.

For additional applications, complete the following fields:

**Application Name** Enter the name you wish to give the application. Each name can be up to 12 characters.

**External Port** Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.

**Internal Port** Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.

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

**To IP Address** For each application, enter the IP address of the PC that should receive the requests. If you assigned a static IP address to the PC, then you can click DHCP Reservation on the Basic Setup screen to look up its static IP address.
**Enabled** For each application, select Enabled to enable port forwarding.

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

**Applications and Gaming > Port Range Forwarding**

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

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).

If you need to forward all ports to one computer, click the **DMZ** tab.

**Port Range Forwarding**

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

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

**Start-End Port** Enter the number or range of port(s) used by the server or Internet applications. Check with the Internet application documentation for more information.

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

**To IP Address** For each application, enter the IP address of the PC running the specific application. If you assigned a static IP address to the PC, then you can click **DHCP Reservation** on the *Basic Setup* screen to look up its static IP address.

**Enabled** Select Enabled to enable port forwarding for the applications you have defined.

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

**Applications & Gaming > Port Range Triggering**

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

**Port Range Triggering**

**Application Name** Enter the application name of the trigger.

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

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

**Enabled** Select Enabled to enable port triggering for the applications you have defined.

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

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.

Enabled/Disabled To disable DMZ hosting, select Disabled. To expose one PC, select Enabled. Then configure the following settings:

Source IP Address If you want any IP address to be the source, select Any IP Address. If you want to specify an IP address or range of IP addresses as the designated source, select and complete the IP address range fields.

Destination If you want to specify the DMZ host by IP address, select IP Address and enter the IP address in the field provided. If you want to specify the DMZ host by MAC address, select MAC Address and enter the MAC address in the field provided. To retrieve this information, click DHCP Client Table.

DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, or MAC Address. To select a DHCP client, click Select. To retrieve the most up-to-date information, click Refresh. To exit this screen and return to the DMZ screen, click Close.

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.

QoS (Quality of Service)

Wireless

Wireless QoS If you have other devices on your network that support Wireless QoS, select Enabled. Otherwise, keep the default, Disabled.

No Acknowledgement If you want to disable the Router’s Acknowledgement feature, so the Router will not re-send
data if an error occurs, then select **Enabled**. Otherwise, keep the default, **Disabled**.

**Internet Access Priority**

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels priority: High, Medium, Normal, or Low. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.

**Enabled/Disabled** To use the QoS policies you have set, keep the default, **Enabled**. Otherwise, select **Disabled**.

**Category**

There are five categories available when you click on **Enabled**. Select one of the following: **Applications**, **Online Games**, **MAC Address**, **Ethernet Port**, or **Voice Device**. Proceed to the instructions for your selection.

**Applications**

- **Applications** Select the appropriate application.
- **Priority** Select the appropriate priority: **High**, **Medium (Recommended)**, **Normal**, or **Low**.
- Click **Add** to save your changes. Your new entry will appear in the Summary list.

**Online Games**

- **Game** Select the appropriate application from the drop down menu.
- **Priority** Select the appropriate priority: **High**, **Medium (Recommended)**, **Normal**, or **Low**.
- Click **Add** to save your changes. Your new entry will appear in the Summary list.

**MAC Address**

- **Enter a Name** Enter a name for your device.
- **MAC Address** Enter the MAC address of your device.
- **Priority** Select the appropriate priority: **High**, **Medium (Recommended)**, **Normal**, or **Low**.
- Click **Add** to save your changes. Your new entry will appear in the Summary list.
Ethernet Port

Select the appropriate Ethernet port.

Priority Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Voice Device

Enter a Name Enter a name for your voice device.

MAC Address Enter the MAC address of your voice device.

Priority Select the appropriate priority: **High (Recommend)**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Summary

This lists the QoS entries you have created for your applications and devices.

**Priority** This column displays the bandwidth priority of High, Medium, Normal, or Low.

Name This column displays the application, device, or port name.

Information This column displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.

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

Applications and Gaming > SMS

The Router allows SMS (Short Message Service) commands to phones. Click **New** to send a new message, click **Reply** to answer a message, then click **Send** or to cancel the message, click **Cancel**. You can reply with or without sending back the original message. Click **Delete** to delete a message.
Administration > Management

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

**Router Management**

**Router Access**

To ensure the Router’s security, you will be asked for your password when you access the Router’s web-based utility. The default is *admin*.

**Router Password** Enter a new password for the Router.

**Re-enter to confirm** Enter the password again to confirm.

**Management Access**

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

**Remote Management Access**

**Remote Management** To permit remote access of the Router, from outside the local network, select Enabled. Otherwise, keep the default, Disabled.

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

**Remote Upgrade** If you want to be able to upgrade the Router remotely, from outside the local network, select Enabled. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default, Disabled.

**Allowed Remote IP Address** If you want to be able to access the Router from any external IP address, select Any IP Address. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

**Remote Management Port** Enter the port number that will be open to outside access.

---

**NOTE:** When you are in a remote location and wish to manage the Router, enter `http://<Internet_IP_address>:port` or `https://<Internet_IP_address>:port`, depending on whether you use HTTP or HTTPS. Enter the Router’s specific Internet IP address in place of `<Internet_IP_address>`, and enter the Remote Management Port number in place of the word port.

**UPnP**

Universal Plug and Play (UPnP) allows Windows XP or Vista to automatically configure the Router for various Internet applications, such as gaming and videoconferencing.

**UPnP** If you want to use UPnP, keep the default, Enabled. Otherwise, select Disabled.

**Allow Users to Configure** Keep the default, Enabled, if you want to be able to make manual changes to the Router while using the UPnP feature. Otherwise, select Disabled.
**Allow Users to Disable Internet Access**  Select **Enabled**, if you want to be able to prohibit any and all Internet connections. Otherwise, keep the default, **Disabled**.

**Backup and Restore**

**Backup Configuration**  To back up the Router’s configuration settings, click this button and follow the on-screen instructions.

**Restore**  To restore the Router’s configuration settings, click this button and follow the on-screen instructions. (You must have previously backed up the Router’s configuration settings.)

**Mobile**

The Router allows SMS (Short Message Service) commands through your mobile phone. This feature allows you to select authorized users who can then command the Router to reboot, connect to a mobile network, or send a WOL packet to a device or all devices on the network.

**SMS Deletion**  Select Manual if you want to delete SMS messages manually. Select Automatic and enter a number if you want SMS text messages to be deleted after they reach a certain number.

**Accept SMS SMS-INT timer**  Enter in the field the length of time in seconds that you want between commands. **300 seconds** is the default. Select **None** to authorize no one to use this feature. Select **Anonymous** to authorize everyone to use this feature. Select **Trusted Number & RCA Encryption** to allow RCA encryption for the command and to only authorize users with the phone numbers you enter below to use this feature.

**Phone1-5**  Enter the phone numbers of those you are authorizing.

**Reboot by SMS**  Select Enable to allow a reboot.

**WOL by SMS (Wake-on-LAN)**  Select this feature to wake up the equipment on your network.

**PC1-5 MAC**  This feature is available when WOL by SMA is enabled. Enter the MAC addresses of the devices and/or PCs on your network.

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, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**. With logging enabled, you can choose to view temporary logs.

**View Log**  To view the logs, click **View Log**.

**Log**

- **Type**  Select **Incoming Log**, **Outgoing Log**, **Security Log**, or **DHCP Client Log**.

- **Type Log**  The **Incoming Log** will display a temporary log of the source IP addresses and destination port numbers for the incoming Internet traffic. The **Outgoing Log** will display a temporary log of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic. The **Security Log** will display the login information for the web-based utility. The **DHCP Client Log** will display the LAN DHCP server status information.

Click **Save the Log** to save this information to a file on your PC’s hard drive. Click **Refresh** to update the
log. Click **Clear** to clear all the information that is displayed.

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

**Administration > Diagnostics**

The diagnostic tests let you reboot your Router or run tests (Ping and Traceroute) that allow you to check the connections of your network devices, including connection to the Internet.

![Administration > Diagnostics](image)

**Reboot**

To reboot the Router, click **Reboot**.

**Ping Test**

The Ping test checks the status of a connection.

**IP or URL Address** Enter the address of the PC whose connection you wish to test.

**Packet Size** Enter the packet size you want to use. The default is **32** bytes.

**Times to Ping** Enter many times you wish to test it.

**Start to Ping** To run the test, click this button. The Ping Test screen will show if the test was successful. Click **Close** to return to the Diagnostics screen. Click **Stop** to end the test.

**Traceroute Test**

The Traceroute test tests the performance of a connection.

**Target IP or URL Address** Enter the address of the PC whose connection you wish to test.

**Start to Traceroute** To run the test, click this button. The Traceroute Test screen will show if the test was successful. Click **Close** to return to the Diagnostics screen. Click **Stop** to end the test.

**Administration > Factory Defaults**

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

![Administration > Factory Defaults](image)

**NOTE:** Do not restore the factory defaults unless you are having difficulties with the Router and have exhausted all other troubleshooting measures. Once the Router is reset, you will have to re-enter all of your configuration settings.

**Factory Defaults**

**Restore All Settings** To reset the Router’s settings to the default values, click this button and then follow the on-screen instructions. Any settings you have saved will be lost when the default settings are restored.

**Administration > Firmware Upgrade**

The **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.

![Administration > Firmware Upgrade](image)

**NOTE:** The Router may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings.
Upgrade Firmware


Please select a file to upgrade the firmware Click Browse and select the extracted firmware upgrade file.

Start to Upgrade After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Status > HSDPA/3G/UMTS

The HSDPA/3G/UMTS screen displays the status information for your mobile broadband service and device (data card or USB adapter).

Mobile Network Status

Mobile Network Bearer The name of the mobile network bearer that the Router uses, is displayed.

Network Name The name of the HSDPA/3G/UMTS or GPRS network the Router is using is displayed.

Signal Strength The strength of the HSDPA/3G/UMTS or GPRS signal that the Router receives is displayed.

Connection Time The length of time the Router has been connected to the mobile network since your last connection is displayed.

Current Session Usage The amount of data that has been sent to and received from the mobile network since your last connection is displayed.

3G/UMTS Card Status

Card Model The model number of your Vodafone card is displayed.

Card Revision The revision number of your Vodafone card is displayed.

Card Firmware The firmware version of your Vodafone card is displayed.

IMSI The IMSI (International Mobile Subscriber Identity) of your Vodafone card is displayed.

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

The **Router** screen displays information about the Router and its current settings.

![Router Screen](image)

**Router Information**

- **Firmware Version** The version number of the Router’s current firmware is displayed.
- **Current Time** The time set on the Router is displayed.
- **Internet MAC Address** The Router’s MAC Address, as seen by your ISP, is displayed.
- **Host Name** If the Router’s Host Name was entered on the **Basic Setup** screen, then it is displayed.
- **Domain Name** If the Router’s Domain Name was entered on the **Basic Setup** screen, then it is displayed.
- **DHCP Lease Time** The amount of time you designated in Network Setup for DHCP clients is displayed.

**Internet Connection**

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

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

**Status > Local Network**

The **Local Network** screen displays information about the local, wired network.

![Local Network Screen](image)

**Local Network**

- **Local MAC Address** The MAC address of the Router’s local, wired interface is displayed.
- **Router IP Address** The Router’s IP address, as it appears on your local network, is displayed.
- **Subnet Mask** The Subnet Mask of the Router is displayed.

**DHCP Server**

- **DHCP Server** The status of the Router’s DHCP server function is displayed.
- **Start IP Address** For the range of IP addresses used by devices on your local network, the starting IP address is displayed.
- **End IP Address** For the range of IP addresses used by devices on your local network, the ending IP address is displayed.

**DHCP Clients Table** Click this button to view a list of PCs that are using the Router as a DHCP server.
DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, or MAC Address. To remove a DHCP client, click Delete. To retrieve the most up-to-date information, click Refresh. To exit this screen and return to the Local Network screen, click Close.

Status > Wireless Network

The Wireless Network screen displays information about your wireless network.

Wireless Network

**MAC Address** The MAC address of the Router’s local, wireless interface is displayed.

**Mode** The wireless mode used by the network is displayed.

**Network Name (SSID)** The name of the wireless network, which is also called the SSID, is displayed.

**Standard Channel** The channel used by the Router is displayed.

**Security** The wireless security method used by the Router is displayed.

**SSID Broadcast** The status of the SSID Broadcast feature is displayed.
Appendix A: Troubleshooting

**Your computer cannot connect to the Internet.**

Check that everything is connected properly. The PC must 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.

Power down everything, then power on each device in the following order, waiting for each device to completely startup before turning on the next:

1. DSL or cable modem
2. Router
3. PC

- Check the LEDs on the front panel of the Router. Make sure the Power, DSL, and at least one of the numbered LEDs are lit. If they are not, then check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Router, and the Line port of the Router must be connected to the ADSL line.

**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**.

**You are using a static IP address and cannot connect.**

Refer to Windows Help and change your Internet Protocol (TCP/IP) Properties to Obtain an IP address automatically.

**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 basic settings on the Router.**

Run the Setup Wizard on the Setup CD-ROM.

**You need to modify the advanced 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, complete the **Username** and **Password** fields (the default username and password is admin). Click the appropriate tab to change the settings.

**How do you connect to the mobile network?**

There are three options available.

First Option Using the Front Panel Button

1. Power on the Router with the mobile broadband data card or USB adapter installed.
2. Press the **Mobile Connect/Disconnect** button on the front panel of the Router.
3. The Router will connect to the mobile network via the mobile broadband data card or USB adapter. If this is successful, the Internet Mobile LED on the Router will light up.

Second Option Using the Web-Based Utility

1. Open the web browser.
2. Enter the Router’s IP address in the **Address** field (the default IP address is 192.168.1.1). Press **Enter**.
3. When prompted, complete the **Username** and **Password** fields (the default username and password is admin). Click **OK**.
4. On the first screen you see, the **Basic Setup** screen, click the **Connect** button near the top of the screen.
5. The Router will connect to the mobile network via the mobile broadband data card or USB adapter. If this is successful, the Mobile Connection line will say, “Connected” instead of “Disconnected.”

Third Option Using the Auto Connect Feature

The Router’s Auto Connect feature enables the Router to automatically connect to the mobile network whenever it is powered on.

1. Open the web browser.
2. Enter the Router’s IP address in the **Address** field (the default IP address is 192.168.1.1). Press **Enter**.
3. When prompted, complete the **Username** and **Password** fields (the default username and password is admin). Click **OK**.
4. On the first screen you see, the Basic Setup screen, click the Mobile Network tab.

5. On the Mobile Network screen, there is an Auto Connect option at the top of the screen. Select Auto, and then click Save Settings.

6. After the webpage has refreshed, click the Basic Setup tab.

7. On the Basic Setup screen, click the Connect button to connect to the mobile network.

8. The next time the Router is powered on, it will automatically connect to the mobile network.

What do the indicator LEDs signify on the Router?

- **Power** (Green) The Power LED lights up and stays on while the Router is powered on.
- **Ethernet 1-4** (Green) These numbered LEDs, corresponding with the numbered ports on the Router’s back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. It flashes to indicate network activity over that port.
- **Wireless** (Green) The Wireless LED lights up when the wireless feature is enabled. It flashes when the Router is actively sending or receiving data over the wireless network.
- **Modem Internet** (Green) The Modem LED lights up and stays on when there is a connection made through the Modem port. It flashes to indicate network activity over the Modem port.
- **3G/UMTS Internet** (Blue/Green) The 3G/UMTS LED flashes as the Router connects to the mobile network. When the LED stops flashing and stays on, then the connection is active. When the LED is blue, a 3G/UTMS/HSDPA connection has been established. When the LED is green, a GPRS connection has been established. If the LED flashes quickly, the Router is not connected to the mobile network. Before pressing the Mobile Connect/Disconnect button, make sure the mobile broadband data card or USB adapter is already installed.

How do you know which mobile network you are using?

1. Log on to the Router using your web browser. Go to Status > 3G/UMTS. The Network Name field displays the name of the network to which you are currently connected.

2. Click the Status tab.

3. Click the Mobile Network tab. In the Mobile Network Status section, on the Network Name line, you will see the name of the network you are currently using.

Whom should you call if there is a question or problem?

For technical support, please contact your reseller. If you have questions about your mobile service or billing, please contact your service provider.

WEB: If your questions are not addressed here, refer to the website [www.linksys.com/vodafone](http://www.linksys.com/vodafone).
Appendix B: Specifications

Model Number: WRT54G3GV2-VF

Standards:
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11g
- IEEE 802.11b
- WPA
- WPA2
- WMM

Ports:
- Modem, Ethernet (4), PC Card, USB 2.0 (3), Power, and Reverse Polarity Antenna (RP-SMA)

Buttons:
- 3G/UMTS Connect/Disconnect, Reset

LEDs:
- Power, Ethernet (1-4), Wireless, Modem Internet, 3G/UMTS Internet

Cabling Type: UTP CAT 5

No. of Antennas: 1

Connector Type: RP-SMA

Detachable (Y/N): Yes

RF Pwr (EIRP) in dBm:
- 802.11g: Typical 14 dBm (±1.5), 802.11b: Typical 16 dBm (±1.5)

Antenna Gain in dBi: 3.3

UPnP: Able

Security Features:
- Stateful Packet Inspection (SPI)
- Firewall, Internet Policy, WEP, WPA, WPA2

Security Key Bits: 256-bits (WPA)

Environmental

Dimensions: 170 x 170 x 33 mm (6.69" x 6.69" x 1.30")

Weight: 392 g (13.83 oz) 0.86 lbs

Power:
- External 12V DC, 1.5A

Certification:
- Wi-Fi (802.11b, 802.11g, WPA - Personal and Enterprise, WPA2 - Personal and Enterprise, WMM), CE, FCC, IC-03, IDA, C-Tick, E-Mark, CB, UL, cUL, WEEE, RoHS

Operating Temp.: 0 to 40°C (32 to 104°F)

Storage Temp.: -20 to 60°C (-4 to 140°F)

Operating Humidity: 10 to 85%, Relative Humidity, Noncondensing

Storage Humidity: 5 to 90% Noncondensing

Specifications are subject to change without notice.
Appendix C: Warranty Information

Limited Warranty

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 any questions about the services provided by your Service Provider or your Linksys product, please contact your Service Provider that provided the Linksys product to you. You also will find a variety of online support tools and information to assist you with your product at www.linksys.com/support. If the product proves defective during the Warranty Period, contact your Service Provider for instructions on how to obtain warranty service. The telephone number for your Service Provider in your area can be found in the written documentation included with your Linksys product.

Have your product serial number and proof of purchase (if applicable) on hand when calling your Service Provider. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number and instructions for shipping the product to your Service Provider. You are responsible for properly packaging and shipping your product at your cost and risk. You must include the RMA number and a copy of your dated proof.
of original purchase (if applicable) when returning your product. Products received without a RMA number and dated proof of original purchase (if applicable) will be rejected. Do not include any other items with the product you are returning. 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 for your product 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 Linksys 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 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 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 20 cm between the radiator and your body.

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.

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 20 cm 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, mêmesicebrouillageestsusceptibledecompromettre fonctionnement du dispositif.
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 isotrope 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.

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.
- Do not place the wireless router in environments where the use of mobile devices is prohibited. Follow any local regulations or rules relating to mobile phones and wireless devices to prevent interference with medical equipment.
- To ensure compliance with exposure limits to radio frequency fields, the antenna(s) of your Linksys wireless product(s) should be no closer than 20 cm to your body during use.

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.
Appendix D

Regulatory Information


Compliance Information for 2.4-GHz and 5-GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

<table>
<thead>
<tr>
<th>Language</th>
<th>Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Български</td>
<td>Това оборудване отговаря на съществените изисквания и приложимите клуazi на Директива 1999/5/EC.</td>
</tr>
<tr>
<td>Česky</td>
<td>Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.</td>
</tr>
<tr>
<td>Dansk</td>
<td>Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.</td>
</tr>
<tr>
<td>Deutsch</td>
<td>Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.</td>
</tr>
<tr>
<td>Eesti</td>
<td>See seade vastab direktiivi 1999/5/EU olulistele nõuetele ja teistele asjakohastele sätetele.</td>
</tr>
<tr>
<td>English</td>
<td>This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.</td>
</tr>
<tr>
<td>Español</td>
<td>Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/EC.</td>
</tr>
<tr>
<td>Ελληνική</td>
<td>Αυτός ο εξοπλισµός είναι σε συµµόρφωση µε τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.</td>
</tr>
<tr>
<td>Français</td>
<td>Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.</td>
</tr>
<tr>
<td>IJselska</td>
<td>Petta tæki er samkvæmt grunnkröfum og öðrum vibeigandi ákvæðum Tílskipunar 1999/5/EC.</td>
</tr>
<tr>
<td>Italiano</td>
<td>Questo apparato è conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.</td>
</tr>
<tr>
<td>Latviski</td>
<td>Šī iekārta atbilst Direktivas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</td>
</tr>
<tr>
<td>Lietuvių</td>
<td>Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.</td>
</tr>
<tr>
<td>Nederlands</td>
<td>Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.</td>
</tr>
<tr>
<td>Malti</td>
<td>Dan l-apparat huwa konformi mal-htijiet essenzjali u l-provedimenti l-ohra rilevanti tad-Direttiva 1999/5/EC.</td>
</tr>
<tr>
<td>Magyar</td>
<td>Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.</td>
</tr>
<tr>
<td>Polski</td>
<td>Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczegółowymi warunkami określonymi Dyrektywą UE: 1999/5/EC.</td>
</tr>
<tr>
<td>Português</td>
<td>Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.</td>
</tr>
<tr>
<td>Română</td>
<td>Acest echipament este în conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 1999/5/EC.</td>
</tr>
<tr>
<td>Slovenščina</td>
<td>Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.</td>
</tr>
<tr>
<td>Slovak</td>
<td>Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.</td>
</tr>
<tr>
<td>Suomi</td>
<td>Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.</td>
</tr>
<tr>
<td>Svenska</td>
<td>Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.</td>
</tr>
</tbody>
</table>

For all products, the Declaration of Conformity (DoC) is available through one or more of these options:

- A pdf file is included on the product’s CD.
- A print copy is included with the product.
- A pdf file is available on the product’s webpage. Visit www.linksys.com/international and select your country or region. Then select your product.

If you need any other technical documentation, see the “Technical Documents on www.linksys.com/international” section, as shown later in this appendix.
The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328 and/or EN 301 893 as applicable
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950 and either EN 50385 or EN 50371

Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) are required for operation in the 5 GHz band.

DFS: The equipment meets the DFS requirements as defined in ETSI EN 301 893. This feature is required by the regulations to avoid interference with Radio Location Services (radars).

TPC: For operation in the 5 GHz band, the maximum power level is 3 dB or more below the applicable limit. As such, TPC is not required.

**CE Marking**

For the Linksys Wireless-N, -G, -B, and/or -A products, the following CE mark, notified body number (where applicable), and class 2 identifier are added to the equipment.

![CE Mark](image_url)

Check the CE label on the product to find out which notified body was involved during the assessment.

**IDA Standards**

Complies with IDA Standards DB101520

---

**National Restrictions**

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

*Pour le Linksys Wireless-N, -G, -B, et/ou -A, les marques CE suivantes, numéro de corps (si applicable), ainsi que l'identification de la classe 2 sont ajoutées au logiciel.*

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1999/5/CE folgen) mit Aufnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2,4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). The table labeled “Overview of Regulatory Requirements for Wireless LANs” provides an overview of the regulatory requirements applicable for the 2,4- and 5-GHz bands.

Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. Linksys recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

**Overview of Regulatory Requirements for Wireless LANs**

<table>
<thead>
<tr>
<th>Frequency Band (MHz)</th>
<th>Max Power Level (EIRP) (mW)</th>
<th>Indoor ONLY</th>
<th>Indoor &amp; Outdoor</th>
</tr>
</thead>
<tbody>
<tr>
<td>2400-2483.5</td>
<td>100</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>5150-5350¹</td>
<td>200</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>5470-5725¹</td>
<td>1000</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

¹Dynamic Frequency Selection and Transmit Power Control are required in the frequency ranges of 5250-5350 MHz and 5470-5725 MHz.

The following countries have restrictions and/or requirements in addition to those given in the table labeled “Overview of Regulatory Requirements for Wireless LANs”:

**Denmark**

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

*Idanmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.*
France
For 2.4 GHz, the product should not be used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used in other parts of the 2.4 GHz band when used indoors. Check http://www.arcep.fr/ for more details.

Pour la bande 2.4 GHz, l’équipement ne doit pas être utilisé en extérieur dans la bande 2454 - 2483,5 MHz. Il n’y a pas de restrictions pour des utilisations en intérieur dans d’autres parties de la bande 2,4GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

<table>
<thead>
<tr>
<th>Location</th>
<th>Frequency Range (MHz)</th>
<th>Power (EIRP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indoor (No restrictions)</td>
<td>2400-2483.5</td>
<td>100 mW (20 dBm)</td>
</tr>
<tr>
<td>Outdoor</td>
<td>2400-2454</td>
<td>100 mW (20 dBm)</td>
</tr>
<tr>
<td></td>
<td>2454-2483.5</td>
<td>10 mW (10 dBm)</td>
</tr>
</tbody>
</table>

Italy
This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this 2.4-GHz wireless LAN product is operating within the boundaries of the owner’s property, its use requires a “general authorization”. Please check http://www.comunicazioni.it/it/ for more details.


Latvia
The outdoor usage of the 2,4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.


Notes:
1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Product Usage Restrictions
This product is designed for indoor usage only. Outdoor usage is not recommended, unless otherwise noted.

2.4 GHz Restrictions
This product is designed for use with the standard, integral or dedicated (external) antenna(s) that is/are shipped together with the equipment. However, some applications may require the antenna(s), if removable, to be separated from the product and installed remotely from the device by using extension cables. For these applications, Linksys offers an R-SMA extension cable (AC9SMA) and an R-TNC extension cable (AC9TNC). Both of these cables are 9 meters long and have a cable loss (attenuation) of 5 dB. To compensate for the attenuation, Linksys also offers higher gain antennas, the HGA7S (with R-SMA connector) and HGA7T (with R-TNC connector). These antennas have a gain of 7 dBi and may only be used with either the R-SMA or R-TNC extension cable.

Combinations of extension cables and antennas resulting in a radiated power level exceeding 100 mW EIRP are illegal.

Third-Party Software or Firmware
The use of software or firmware not supported/provided by Linksys may result that the equipment is no longer compliant with the regulatory requirements.

Technical Documents on www.linksys.com/international
Follow these steps to access technical documents:
1. Enter http://www.linksys.com/international in your web browser.
2. Select the country or region in which you live.
3. Click the Products tab.
4. Select the appropriate product category.
5. Select the product sub-category, if necessary.
6. Select the product.
7. Select the type of documentation you want from the More Information section. The document will open in PDF format if you have Adobe Acrobat installed on your computer.

NOTE: If you have questions regarding the compliance of this product or you cannot find the information you need, please contact your local sales office or visit www.linksys.com/international

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:

![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 (Bulgarian) - Информация относно оцертането на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/ЕС изисква уредите, носещи този символ ☑ върху изделието и/или опаковката му, да не се изхвърлят с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от смесените битови отпадъци. Вашата ежедневна работа и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Коректното изхвърляне и рециклиране ще се допомогат да се предотвратят евентуални вреди за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обрнете към местните власти, службите за смесено събиране или магазинове, 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 témtří 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

Wireless-G Router for 3G/UMTS Broadband

Appendix D

Regulatory Information

Eesti (Estonian) - Keskonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidi direktiivi 2002/96/EÜ nõute kohaselt on seadmeid, millel on tootel või pakendid käesolev sümbol \( \mathbb{X} \), keelatud kõrvaldata koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldata eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldata kõhaleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt este nähtud kogumispunktide kaudu. Seadmete korrekte kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervele. Vanade seadmete kõrvaldamise kohta täpsem informatsiooni saamiseks võtke palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palun palu
Lietuviškai (Lithuanian) - Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir ≠ kurios pakuotė yra pažymėta šiuo simboliu (iveskite simbolį), negalima šaisti kartu su nerūšiuotomis komunalinėmis atliekos. Šis simbolis rodo, kad gaminin reikia šaisti atskirai nuo bendro buitinio atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemų. Tinkamai šaistingi ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose jūs gijote tą 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 megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke ≠ megjelenik, tilos a többi sZEletétallat lévakodási hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékmellett együtt kidobni. A címke azt felelőssé, hogy ezt, és más elektromos és elektronikus rendszerek, amelyeken, és/vagy amelyek csomagolásán, a felülírások negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékdolgozó szolgáltattal, vagy azzal üzlettel, ahol a termék vásárolta.

Nederlands (Dutch) - Milieuinformatie 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.

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

Dyrektwa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem ≠ znajdującym się na produkcie lub jego opakowaniu nie był wyrzucać 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 we właściwy sposób, jego recykling pomaga zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania lub sklepu, w którym produkt został nabyty.

Wireless-G Router for 3G/UMTS Broadband

47
Appendix D

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

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo \[\text{\textcircled{W}}\] 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 eletrónico e eletrónico 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 como eliminar este e qualquer outro equipamento eléctrico e electrónico, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

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


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

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom \[\text{\textcircled{W}}\] na produkci a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelené od bežného odpadu z domácnosti. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostrednictvom špeciálizovaných zbierkov zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia môže zabrániť pripadnému negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráte sa, prosím, na miestne orgány, organizácie zaobslužnice sa likvidáciov 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/nternatonal
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.lnksys.com/gpl](http://www.lnksys.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.lnksys.com/gpl](http://www.lnksys.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.lnksys.com/gpl](http://www.lnksys.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.

Software Licenses

The software Licenses applicable to software from Linksys are made available at the Linksys public web site at: [www.lnksys.com](http://www.lnksys.com) and [www.lnksys.com/gpl](http://www.lnksys.com/gpl) respectively. For your convenience of reference, a copy of the Linksys Software License Agreement and the main open source code licenses used by Linksys in its products are contained in the Schedules below.

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.
c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage medium does not bring the other work under the scope of this License.

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,

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, you may choose any version ever published by the Free Software Foundation.

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
Appendix E: Contact Information

Vodafone Online Resource

Vodafone Technical Support

<table>
<thead>
<tr>
<th>Vodafone</th>
<th>Mobile</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>1555</td>
<td>+355 69 144</td>
<td><a href="http://www.vodafone.al/mobileconnect">www.vodafone.al/mobileconnect</a></td>
</tr>
<tr>
<td>France</td>
<td>900</td>
<td>+33 6 1000 1900</td>
<td><a href="http://www.sfr.fr">www.sfr.fr</a></td>
</tr>
<tr>
<td>Germany</td>
<td>1234</td>
<td>+49 800 172 1234</td>
<td><a href="http://www.vodafone.de">www.vodafone.de</a></td>
</tr>
<tr>
<td>Greece</td>
<td>1399</td>
<td>+30 6944 40 1399</td>
<td><a href="http://www.vodafone.gr">www.vodafone.gr</a></td>
</tr>
<tr>
<td>Ireland</td>
<td>1850 287 000</td>
<td>+353 429331999</td>
<td><a href="http://www.vodafone.ie/business">www.vodafone.ie/business</a></td>
</tr>
<tr>
<td>Italy</td>
<td>42005</td>
<td>800-100195</td>
<td><a href="http://www.vodafone.it">www.vodafone.it</a></td>
</tr>
<tr>
<td>Netherlands</td>
<td>1200</td>
<td>+31 654 500 100</td>
<td><a href="http://www.vodafone.nl">www.vodafone.nl</a></td>
</tr>
<tr>
<td>New Zealand</td>
<td>0800-921-021</td>
<td>+64 9 355 2007</td>
<td><a href="http://www.vodafone.co.nz/3grouter">www.vodafone.co.nz/3grouter</a></td>
</tr>
<tr>
<td>Portugal</td>
<td>1214</td>
<td>+351911214000</td>
<td><a href="http://www.vodafone.pt">www.vodafone.pt</a></td>
</tr>
<tr>
<td>Spain</td>
<td>122</td>
<td>+34 607 122 000</td>
<td><a href="http://www.empresas.vodafone.es">www.empresas.vodafone.es</a></td>
</tr>
<tr>
<td>Sweden</td>
<td>222</td>
<td>+46 708 222 222</td>
<td><a href="http://www.telenor.se">www.telenor.se</a></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>191</td>
<td>+44 7836 191 191</td>
<td><a href="http://www.vodafone.co.uk/mobileconnect">www.vodafone.co.uk/mobileconnect</a></td>
</tr>
</tbody>
</table>