

# LINKSYS®

A Division of Cisco Systems, Inc.



2,4GHz  
802.11g

## Wireless-G

### Router for 3G/UMTS Broadband

# User Guide



Model No. **WRT54G3G (EM)**



## Copyright and Trademarks

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

## How to Use This User Guide

This User Guide has been designed to make understanding networking with the Wireless-G Router for 3G/UMTS Broadband easier than ever. Look for the following items when reading this User Guide:



This checkmark means there is a note of interest and is something you should pay special attention to while using the Wireless-G Router for 3G/UMTS Broadband.



This exclamation point means there is a caution or warning and is something that could damage your property or the Wireless-G Router for 3G/UMTS Broadband.



This question mark provides you with a reminder about something you might need to do while using the Wireless-G Router for 3G/UMTS Broadband.

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

***word:*** *definition.*

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

### **Figure 0-1: Sample Figure Description**

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

# Table of Contents

Chapter 1: Introduction	1
Welcome	1
What's in this User Guide?	2
Chapter 2: Planning Your Wireless Network	4
Network Topology	4
Ad-Hoc versus Infrastructure Mode	4
Network Layout	4
Chapter 3: Getting to Know the Wireless-G Router for 3G/UMTS Broadband	6
The Router's Ports	6
The Router's LEDs	7
The Router's 3G/UMTS Slot	8
Chapter 4: Connecting the Wireless-G Router for 3G/UMTS Broadband	9
Overview	9
Hardware Installation for Use of the HSDPA/3G/UMTS or GPRS Service	9
Hardware Installation for Connection to Your Broadband Modem	11
Hardware Installation for Connection to Another Router	13
Placement Options	15
Chapter 5: Configuring the Wireless-G Router for 3G/UMTS Broadband	17
Overview	17
The Setup Tab - Basic Setup	18
The Setup Tab - 3G/UMTS Network	24
The Setup Tab - DDNS	27
The Setup Tab - MAC Address Clone	28
The Setup Tab - Advanced Routing	29
The Wireless Tab - Basic Wireless Settings	30
The Wireless Tab - Wireless Security	31
The Wireless Tab - Wireless MAC Filter	35
The Wireless Tab - Advanced Wireless Settings	36
The Security Tab - Firewall	38
The Security Tab - VPN Passthrough	39
The Access Restrictions Tab - Internet Access	39

The Applications and Gaming Tab - Port Range Forward	41
The Applications & Gaming Tab - Port Triggering	42
The Applications and Gaming Tab - DMZ	43
The Applications and Gaming Tab - QoS	43
The Administration Tab - Management	45
The Administration Tab - Log	46
The Administration Tab - Diagnostics	47
The Administration Tab - Factory Defaults	48
The Administration Tab - Firmware Upgrade	48
The Administration Tab - Config Management	48
The Status Tab - 3G/UMTS	49
The Status Tab - Router	50
The Status Tab - Local Network	51
The Status Tab - Wireless	52
<b>Appendix A: Troubleshooting</b>	<b>53</b>
Common Problems and Solutions	53
Frequently Asked Questions	61
<b>Appendix B: Wireless Security</b>	<b>69</b>
Security Precautions	69
Security Threats Facing Wireless Networks	69
<b>Appendix C: Upgrading Firmware</b>	<b>72</b>
<b>Appendix D: Windows Help</b>	<b>73</b>
<b>Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter</b>	<b>74</b>
Windows 2000 or XP Instructions	74
For the Router's Web-based Utility	74
<b>Appendix F: Glossary</b>	<b>76</b>
<b>Appendix G: Specifications</b>	<b>81</b>
<b>Appendix H: Warranty Information</b>	<b>83</b>
<b>Appendix I: Regulatory Information</b>	<b>84</b>
<b>Appendix J: Contact Information</b>	<b>97</b>

# List of Figures

Figure 3-1: The Router's Ports	6
Figure 3-2: The Router's Front Panel	6
Figure 3-3: The Router's LEDs	7
Figure 3-4: The Router's LEDs	8
Figure 4-1: Connect Your Computer	10
Figure 4-2: Connect the Power	10
Figure 4-3: Connect the Broadband Modem	11
Figure 4-4: Connect Your Computer	12
Figure 4-5: Connect the Power	12
Figure 4-6: Diagram for Connection to Another Router	13
Figure 4-7: Connect Another Router	13
Figure 4-8: Connect Your Computer	14
Figure 4-9: Connect the Power	14
Figure 4-10: Stand Attached to the Router	15
Figure 4-11: Measurement between Wall-Mount Slots	16
Figure 5-1: Password Screen	17
Figure 5-2: Setup Tab - Basic Setup	18
Figure 5-3: DHCP Connection Type	18
Figure 5-4: Static IP Connection Type	19
Figure 5-5: PPPoE Connection Type	19
Figure 5-6: PPTP Connection Type	19
Figure 5-7: Telstra Connection Type	20
Figure 5-8: L2TP Connection Type	20
Figure 5-9: Optional Settings	21
Figure 5-10: Router IP	21
Figure 5-11: DHCP Server Settings	22
Figure 5-12: Network Address Server Settings	22
Figure 5-13: Time Setting	23
Figure 5-14: Setup Tab - 3G/UMTS	24
Figure 5-15: Setup Tab - PAP or CHAP	24
Figure 5-16: APN Configuration	25

Figure 5-17: Setup Tab - DDNS (DynDNS.org)	27
Figure 5-18: Setup Tab - DDNS (TZO.org)	27
Figure 5-19: Setup Tab - MAC Address Clone	28
Figure 5-20: Setup Tab - Advanced Routing (Gateway)	29
Figure 5-21: Setup Tab - Advanced Routing (Router)	29
Figure 5-22: Wireless Tab - Basic Wireless Settings	30
Figure 5-23: Wireless Tab - Wireless Security (WPA Personal - TKIP)	31
Figure 5-24: Wireless Tab - Wireless Security (WPA Personal - AES)	31
Figure 5-25: Wireless Tab - Wireless Security (WPA2 Personal)	31
Figure 5-26: Wireless Tab - Wireless Security (WPA Enterprise - TKIP)	32
Figure 5-27: Wireless Tab - Wireless Security (WPA Enterprise - AES)	32
Figure 5-28: Wireless Tab - Wireless Security (WPA2 Enterprise - TKIP)	33
Figure 5-29: Wireless Tab - Wireless Security (WPA2 Enterprise - AES)	33
Figure 5-30: Wireless Tab - Wireless Security (RADIUS)	34
Figure 5-31: Wireless Tab - Wireless Security (WEP)	34
Figure 5-32: Wireless Tab - Wireless MAC Filter	35
Figure 5-33: MAC Address Filter List	35
Figure 5-34: Wireless Tab - Advanced Wireless Settings	36
Figure 5-35: Security Tab - Firewall	38
Figure 5-36: Security Tab - VPN Passthrough	39
Figure 5-37: Access Restrictions Tab - Internet Access	39
Figure 5-38: Internet Policy Summary	40
Figure 5-39: List of PCs	40
Figure 5-40: Port Services	40
Figure 5-41: Applications and Gaming Tab - Port Range Forward	41
Figure 5-42: Applications and Gaming Tab - Port Triggering	42
Figure 5-43: Applications and Gaming Tab - DMZ	43
Figure 5-44: Applications and Gaming Tab - QoS	43
Figure 5-45: Administration Tab - Management	45
Figure 5-46: Administration Tab - Log	46
Figure 5-47: Administration Tab - Diagnostics	47
Figure 5-48: Ping Test	47
Figure 5-49: Traceroute Test	47
Figure 5-50: Administration Tab - Factory Defaults	48

Figure 5-51: Administration Tab - Firmware Upgrade	48
Figure 5-52: Administration Tab - Config Management	48
Figure 5-53: Status Tab - 3G/UMTS	49
Figure 5-54: Status Tab - Router	50
Figure 5-55: Status Tab - Local Network	51
Figure 5-56: Status Tab - Wireless	52
Figure C-1: Upgrade Firmware	72
Figure E-1: MAC Address/Physical Address	74
Figure E-2: MAC Address Filter List	74
Figure E-3: MAC Address Clone	75

# Chapter 1: Introduction

## Welcome

Thank you for choosing the Linksys Wireless-G Router for 3G/UMTS Broadband. The Wireless-G Router for 3G/UMTS Broadband will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely.

How does the Wireless-G Router for 3G/UMTS Broadband do all of this? A router is a device that allows access to an Internet connection over a network. With the Wireless-G Router for 3G/UMTS Broadband, you can access the Internet through either your HSDPA/3G/UMTS or GPRS service (requires an 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.

Use the WPA or WPA2 standard to secure your wireless network while the whole network is protected through a Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) technology. Access the Router's features through the easy-to-use, browser-based utility.

But what does all of this mean?

Networks are useful tools for sharing computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun.

PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired".

PCs equipped with wireless cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wireless Local Area Network. The Wireless-G Router for 3G/UMTS Broadband bridges wireless networks of both 802.11b and 802.11g standards and wired networks, allowing them to communicate with each other.

With your networks all connected, wired, wireless, and the Internet, you can now share files and Internet access—and even play games. All the while, the Wireless-G Router for 3G/UMTS Broadband protects your networks from unauthorised and unwelcome users.

**wpa** (*wi-fi protected access*): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

**spi** (*stateful packet inspection*) **firewall**: a technology that inspects incoming packets of information before allowing them to enter the network.

**firewall**: Security measures that protect the resources of a local network from intruders.

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

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



Use the instructions in the User Guide to help you connect and set up the Router. These instructions should be all you need to get the most out of the Wireless-G Router for 3G/UMTS Broadband.

## What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G Router for 3G/UMTS Broadband.

- **Chapter 1: Introduction**  
This chapter describes the Router's applications and this User Guide.
- **Chapter 2: Planning Your Wireless Network**  
This chapter describes the basics of wireless networking.
- **Chapter 3: Getting to Know the Wireless-G Router for 3G/UMTS Broadband**  
This chapter describes the physical features of the Router.
- **Chapter 4: Connecting the Wireless-G Router for 3G/UMTS Broadband**  
This chapter instructs you on how to connect the Router to your network.
- **Chapter 5: Configuring the Wireless-G Router for 3G/UMTS Broadband**  
This chapter explains how to use the Web-based Utility to configure the settings on the Wireless-G Router for 3G/UMTS Broadband.
- **Appendix A: Troubleshooting**  
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G Router for 3G/UMTS Broadband.
- **Appendix B: Wireless Security**  
This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- **Appendix C: Upgrading Firmware**  
This appendix instructs you on how to upgrade the firmware on the Router should you need to do so.
- **Appendix D: Windows Help**  
This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- **Appendix E: Finding the MAC Address and IP Address for your Ethernet Adapter.**  
This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router.

- **Appendix F: Glossary**  
This appendix gives a brief glossary of terms frequently used in networking.
- **Appendix G: Specifications**  
This appendix provides the technical specifications for the Router.
- **Appendix H: Warranty Information**  
This appendix supplies the warranty information for the Router.
- **Appendix I: Regulatory Information**  
This appendix supplies the regulatory information regarding the Router.
- **Appendix J: Contact Information**  
This appendix provides contact information for a variety of Linksys resources, including Technical Support.

# Chapter 2: Planning Your Wireless Network

## Network Topology

A wireless local area network (WLAN) is exactly like a regular local area network (LAN), except that each computer in the WLAN uses a wireless device to connect to the network. Computers in a WLAN share the same frequency channel and SSID, which is an identification name shared by the wireless devices belonging to the same wireless network.

*ssid (service set identifier): your wireless network's name.*

## Ad-Hoc versus Infrastructure Mode

Unlike wired networks, wireless networks have two different modes in which they may be set up: infrastructure and ad-hoc. An infrastructure configuration is a WLAN and wired LAN communicating to each other through an access point. An ad-hoc configuration is wireless-equipped computers communicating directly with each other. Choosing between these two modes depends on whether or not the wireless network needs to share data or peripherals with a wired network or not.

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

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

If the computers on the wireless network need to be accessible by a wired network or need to share a peripheral, such as a printer, with the wired network computers, the wireless network should be set up in Infrastructure mode. The basis of Infrastructure mode centers around a wireless router or an access point, such as the Wireless-G Router for 3G/UMTS Broadband, which serves as the main point of communications in a wireless network. The Router transmits data to PCs equipped with wireless network adapters, which can roam within a certain radial range of the Router. You can arrange the Router and multiple access points to work in succession to extend the roaming range, and you can set up your wireless network to communicate with your Ethernet hardware as well.

If the wireless network is relatively small and needs to share resources only with the other computers on the wireless network, then the Ad-Hoc mode can be used. Ad-Hoc mode allows computers equipped with wireless transmitters and receivers to communicate directly with each other, eliminating the need for a wireless router or access point. The drawback of this mode is that in Ad-Hoc mode, wireless-equipped computers are not able to communicate with computers on a wired network. And, of course, communication between the wireless-equipped computers is limited by the distance and interference directly between them.

## Network Layout

The Wireless-G Router for 3G/UMTS Broadband has been specifically designed for use with both your 802.11b and 802.11g products. It is compatible with all 802.11g and 802.11b adapters, such as the notebook adapters for

## Wireless-G Router for 3G/UMTS Broadband

your laptop computers, PCI adapters for your desktop PCs, and USB adapters when you want to enjoy USB connectivity. The Router will also communicate with the Wireless PrintServer and Wireless Ethernet Bridges.

When you wish to connect your wireless network with your wired network, you can use the Wireless-G Router for 3G/UMTS Broadband's four Ethernet LAN ports. To add more ports, any of the Router's LAN ports can be connected to any of Linksys's switches.

With these, and many other Linksys products, your networking options are limitless. Go to the Linksys website at [www.linksys.com/international](http://www.linksys.com/international) for more information about products that work with the Wireless-G Router for 3G/UMTS Broadband.

# Chapter3:GettingtoKnowtheWireless-GRouterfor3G/UMTS Broadband

## The Router's Ports

The Router's ports and Reset button are located on the side panel with the antenna port.

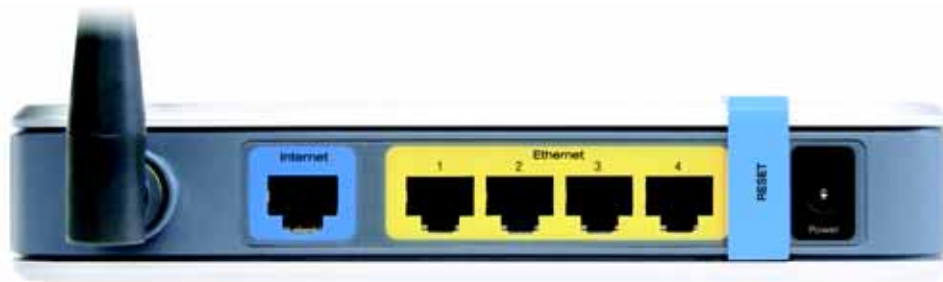


Figure 3-1: The Router's Ports

- |                                |   |
|--------------------------------|---|
| <b>(Antenna)</b>               | The antenna port is where you will attach the Router's antenna.   |
| <b>Internet</b>                | The <b>Internet</b> port is where you will connect your broadband Internet connection, if you are using broadband WAN service.  |
| <b>Ethernet<br/>1, 2, 3, 4</b> | These ports (1, 2, 3, 4) connect the Router to your PCs and other Ethernet network devices.   |
| <b>Security Bracket</b>        | The red bracket labeled "RESET" clips onto the Router. It covers the Reset button and the security slot on the Router's front panel. You can remove the security bracket to access the Reset button. To protect the Router from theft, you can attach a lock to the Router using the security slot and bracket. |
| <b>Reset Button</b>            | There are two ways to reset the Router's factory defaults. Either press the <b>Reset</b> button, for approximately five seconds, or restore the defaults from the Administration tab - Factory Defaults tab in the Router's Web-based Utility.  |
| <b>Power</b>                   | The <b>Power</b> port is where you will connect the power adapter.  |



Figure 3-2: The Router's Front Panel



**IMPORTANT:** Resetting the Router will erase all of your settings (Internet connection, wireless security, and other settings) and replace them with the factory defaults. Do not reset the Router if you want to retain these settings.

## The Router's LEDs

The Router's LEDs are located on the Router's other side panel.



Figure 3-3: The Router's LEDs

**3G/UMTS Button** This button allows you to connect to and disconnect from the HSDPA/3G/UMTS or GPRS network (you can also use the Basic Setup tab of the Router's Web-based Utility).

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

**ETHERNET 1, 2, 3, 4** Green. These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port.

**DMZ** Green. The **DMZ** LED lights up and will remain lit while the Router uses its DMZ function.

**WIRELESS** Green. The **WIRELESS** LED lights up whenever there is a successful wireless connection. If the LED is flashing, the Router is actively sending or receiving data over the wireless network.

**3G/UMTS** Blue/Green. The **3G/UMTS** LED flashes as the Router connects to the mobile network. It is solidly lit when the connection is established. The LED lights up blue if the Router connects to a HSDPA/3G/UMTS network. It lights up green if the Router connects to a GPRS network.

If the LED quickly flashes, alternating between blue and green, and the Router does not have a connection to the mobile network, then either the Router's PIN code is incorrect, or there is no HSDPA/3G/UMTS data or SIM card inserted when you push the 3G/UMTS Connect/Disconnect button. Contact your mobile service provider for assistance.

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

## The Router's 3G/UMTS Slot

The Router's 3G/UMTS slot is located on the Router's top panel.



**Figure 3-4: The Router's LEDs**

**3G/UMTS Slot** Insert the HSDPA/3G/UMTS data card (available separately) into this slot if the Router will connect to a HSDPA/3G/UMTS or GPRS service.

# Chapter 4: Connecting the Wireless-G Router for 3G/UMTS Broadband

## Overview

This chapter includes three sets of instructions. If the Router will use the HSDPA/3G/UMTS or GPRS service only, follow the instructions in “Hardware Installation for Use of the HSDPA/3G/UMTS or GPRS Service.” If the Router will be the only router in your network and you have a broadband modem, follow the instructions in “Hardware Installation for Connection to Your Broadband Modem.” If you want to install the Wireless-G Router for 3G/UMTS Broadband behind another router in your network, then follow the instructions in “Hardware Installation for Connection to Another Router.”

## Hardware Installation for Use of the HSDPA/3G/UMTS or GPRS Service

1. Power down your network devices.
2. Locate an optimum location for the Router. The best place for the Router is usually at the center of your wireless network, with line of sight to all of your mobile stations.
3. Attach the antenna and fix its direction. Try to place the Router in a position that will best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be.
4. Insert the SIM card into your mobile card as needed, following your card's instructions. Then insert your mobile card into the Router's 3G/UMTS slot.



5. Connect your PCs or other devices to the Router's numbered ports with standard Ethernet network cables.



Figure 4-1: Connect Your Computer

6. Connect the power adapter to the Router's Power port, and plug the other end into an electrical outlet. Only use the power adapter supplied with the Router. Use of a different adapter may result in product damage.



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

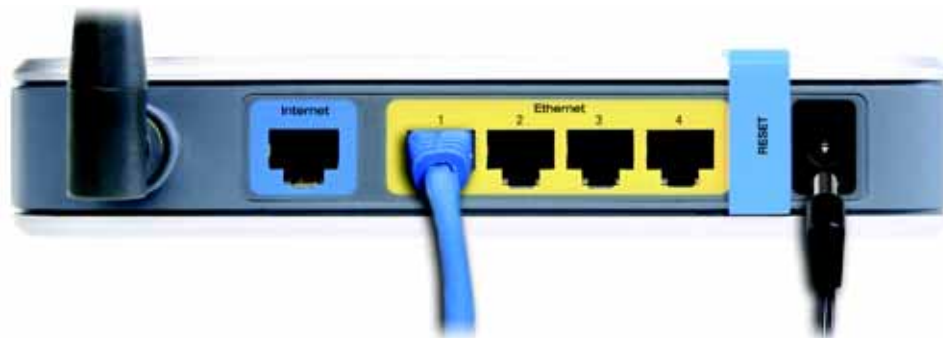


Figure 4-2: Connect the Power

Proceed to the section at the end of this chapter, "Placement Options."

## Hardware Installation for Connection to Your Broadband Modem

1. Power down your network devices.
2. Locate an optimum location for the Router. The best place for the Router is usually at the center of your wireless network, with line of sight to all of your mobile stations.
3. Attach the antenna and fix its direction. Try to place the Router in a position that will best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be.
4. Connect a standard Ethernet network cable to the Router's Internet port. Then, connect the other end of the Ethernet cable to your cable or DSL broadband modem.



Figure 4-3: Connect the Broadband Modem

5. Connect your network PCs or Ethernet devices to the Router's numbered ports using standard Ethernet network cabling.

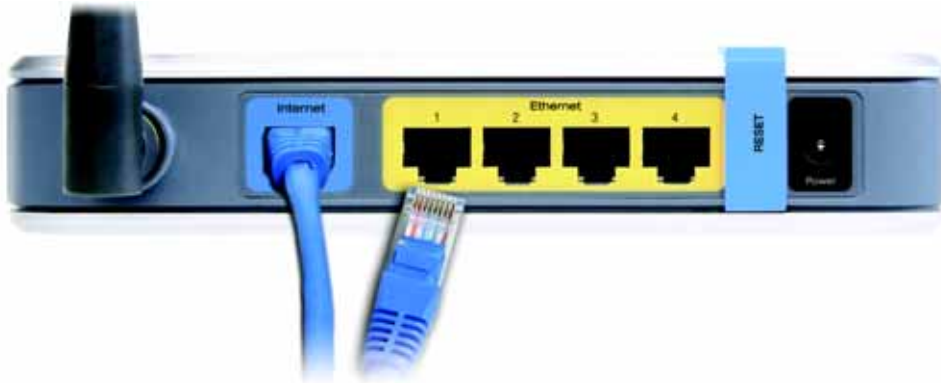


Figure 4-4: Connect Your Computer

6. Connect the power adapter to the Router's Power port, and plug the other end into an electrical outlet. Only use the power adapter supplied with the Router. Use of a different adapter may result in product damage.



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

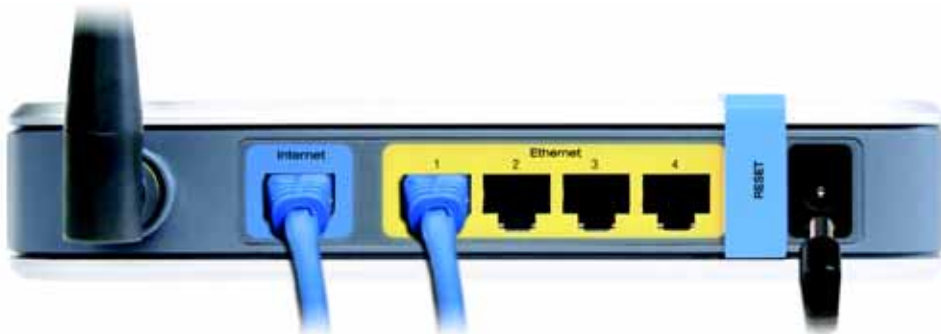


Figure 4-5: Connect the Power

Proceed to the section at the end of this chapter, "Placement Options."

## Hardware Installation for Connection to Another Router

Before you install the Wireless-G Router for 3G/UMTS Broadband, change the default IP address of the other router. This is mandatory because both routers may be set to the same IP address by default. If you do not change the other router's default IP address, then you may not be able to set up the Router.

Make sure the Router is NOT connected to your network. Then follow these instructions:

1. To access the other router's Web-based Utility, launch your web browser, and enter the other router's default IP address, **192.168.1.1**, in the *Address* field. Then press **Enter**.
2. To log in, leave the *User Name* field blank. Enter the password (the default is **admin**). Click the **OK** button.
3. The first screen that appears will display the Setup tab. In the *Network Setup* section, there is a setting called *Local IP Address*, which is set to 192.168.1.1. Change this to **192.168.2.1**.
4. Click the **Save Settings** button to save your change, and then exit the Web-based Utility.
5. Power down your network devices.
6. Locate an optimum location for the Router. The best place for the Router is usually at the center of your wireless network, with line of sight to all of your mobile stations.
7. Attach the antenna and fix its direction. Try to place the Router in a position that will best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be.
8. Connect a standard Ethernet network cable to the Router's Internet port. Then, connect the other end of the Ethernet cable to one of the numbered Ethernet ports on your other router.



Figure 4-7: Connect Another Router



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

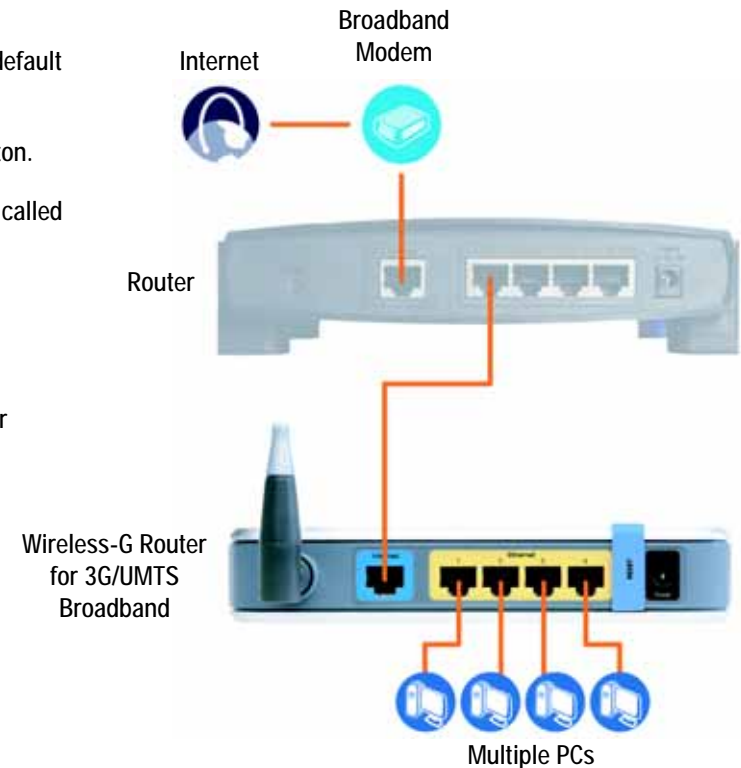


Figure 4-6: Diagram for Connection to Another Router

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

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



Figure 4-8: Connect Your Computer

10. Connect the power adapter to the Router's Power port, and plug the other end into an electrical outlet. Only use the power adapter supplied with the Router. Use of a different adapter may result in product damage.



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

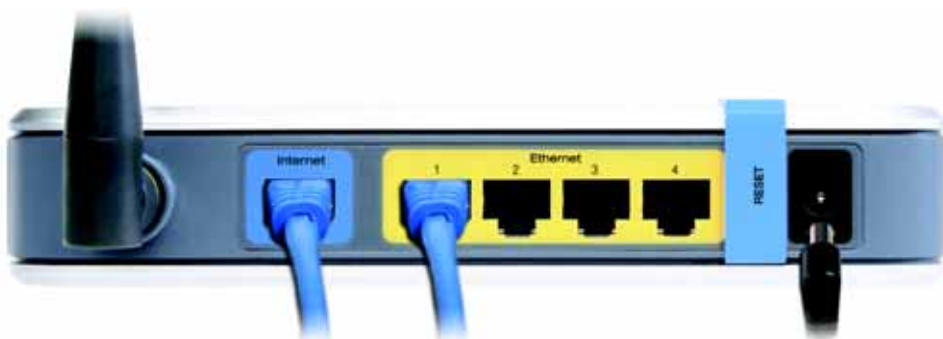


Figure 4-9: Connect the Power

Proceed to the next section, "Placement Options."

## Placement Options

There are three ways to place the Router. The first way is to place it horizontally on a surface, so it sits on its four rubber feet. The second way is to stand the Router vertically on a surface. The third way is to mount it on a wall. The second and third options are explained in further detail below.

### Stand Option

1. Line up the center of the Router's stand with the center of the Router's labeled edge.
2. Insert the Router into the stand.

**To set up the Router, proceed to "Chapter 5: Configuring the Wireless-G Router for 3G/UMTS Broadband."**



**Figure 4-10: Stand Attached to the Router**

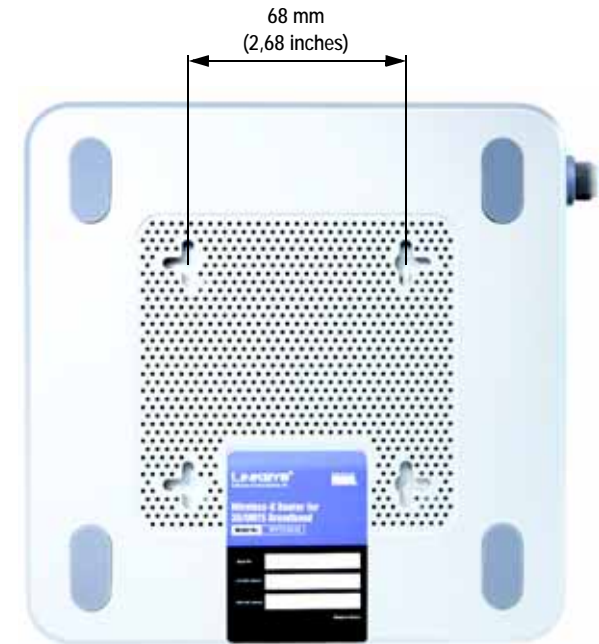
## Wall-Mount Option

The Router has four wall-mount slots on its bottom panel. The distance between two adjacent slots is 68 mm (2,68 inches).

Before you begin, make sure you have two screws that are size #4—this indicates a diameter measurement of 2,845 mm (0,112 inches).

1. Determine where you want to mount the Router.
2. Drill two holes into the wall. Make sure adjacent holes are 68 mm (2,68 inches) apart.
3. Insert a screw into each hole, and leave 5 mm (0,2 inches) of its head exposed.
4. Maneuver the Router so the top 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.

**To set up the Router, proceed to “Chapter 5: Configuring the Wireless-G Router for 3G/UMTS Broadband.”**



**Figure 4-11: Measurement between Wall-Mount Slots**

# Chapter 5: Configuring the Wireless-G Router for 3G/UMTS Broadband

## Overview

Use the Web-based Utility to configure the Router.

This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users will use these two screens of the Utility:

- **Basic Setup.** On the *Basic Setup* screen, enter the settings provided by your Internet Service Provider (ISP).
- **Management.** Click the **Administration** tab and then the **Management** tab. The Router's default password is **admin**. To secure the Router, change the Password from its default.

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

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

A password request page will appear. Leave the *User Name* field blank. The first time you open the Web-based Utility, use the default password **admin**. (You can set a new password from the Administration tab's *Management* screen.) Then click the **OK** button.



Figure 5-1: Password Screen



## The Setup Tab - Basic Setup

The first screen that appears displays the Basic Setup tab, which lets you 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.** Select **HSDPA/3G/UMTS Preferred (recommended)** if you want the Router to connect to a HSDPA/3G/UMTS signal when available. 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.** Displayed here is the name of the mobile network bearer the Router is using.

**Network Name.** Displayed here is the name of the HSDPA/3G/UMTS or GPRS network the Router is using.

**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

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

- **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.



Figure 5-2: Setup Tab - Basic Setup



Figure 5-3: DHCP Connection Type

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Internet Connection Type: Static IP

Internet IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

Static DNS 1: 0.0.0.0

Static DNS 2: 0.0.0.0

Static DNS 3: 0.0.0.0

Figure 5-4: Static IP Connection Type

*Static IP address: a fixed address assigned to a computer or device connected to a network.*

Internet Connection Type: PPPoE

User Name:

Password:

Service Name:

☒ Connect on Demand: Max Idle Time 5 Min.

☐ Keep Alive: Redial Period 30 Sec.

Figure 5-5: PPPoE Connection Type

Internet Connection Type: PPTP

Internet IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

Static DNS 1: 0.0.0.0

Static DNS 2: 0.0.0.0

Static DNS 3: 0.0.0.0

User Name:

Password:

☒ Connect on Demand: Max Idle Time 5 Min.

☐ Keep Alive: Redial Period 30 Sec.

Figure 5-6: PPTP Connection Type

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

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

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

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

**Heart Beat Server.** This is the IP address that the Router has, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

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

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

- **L2TP.** Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries.

**Server IP Address.** Enter the IP address of your ISP's server. This is provided by your ISP.

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

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

Figure 5-7: Telstra Connection Type

Figure 5-8: L2TP Connection Type

soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates.

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

## Optional Settings

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

**Router Name.** In this field, you can type a name of up to 39 characters to represent the Router.

**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. The default setting, **Manual**, allows you to enter the largest packet size that will be transmitted. The recommended size, entered in the *Size* field, is 1492. You should leave this value in the 1200 to 1500 range. To have the Router select the best MTU for your Internet connection, select **Auto**.

## 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 displays both the Router's IP Address and Subnet Mask as seen by your network.



The screenshot shows the 'Optional Settings' section, which is noted as being required by some ISPs. It contains five fields: 'Router Name' with the value 'WRT54G3G-EM', 'Host Name' (empty), 'Domain Name' (empty), 'MTU' set to 'Auto' via a dropdown menu, and 'Size' set to '1500'.

Figure 5-9: Optional Settings



The screenshot shows the 'Router IP' section. It displays the 'Local IP Address' as '192.168.1.1' and the 'Subnet Mask' as '255.255.255.0'.

Figure 5-10: Router IP

## DHCP Server Settings

The Router can be used as a Dynamic Host Configuration Protocol (DHCP) server for your network. A DHCP server automatically assigns an IP address to each computer on your network. Select the mode you want the Router to use for its DHCP server function. If you are not sure which mode to select, keep the default, **Mode 1 - Fixed configuration (Default)**.

**Mode 1 - Fixed configuration (Default).** In this mode, the Router will advertise itself as the DNS server for the clients (computers) to use. The clients will contact the Router for DNS, and its DNS caching server will resolve the addresses for them. This mode is recommended for networks whose UMTS upstream DNS servers change on a connection-by-connection basis, such as networks in the UK.

**Mode 2- Network Supplied.** Via DHCP, the Router will advertise the DNS and WINS servers it is using. This mode may be suitable for networks whose DNS servers have static addresses.

**Mode 3- Manual configuration.** You can designate the settings advertised to the clients via DHCP. Complete the *Static DNS* and *WINS* fields that will appear. You can specify up to three DNS servers and up to two WINS servers. Make sure these values do not depend on the Router's static settings.

## Network Address Server Settings (DHCP)

The settings allow you to configure the Router's DHCP server function. If you choose to enable the Router's DHCP server option, you must configure all of your network PCs to connect to a DHCP server (the Router), and make sure there is no other DHCP server on your network.

**DHCP Server.** DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then click the **Disable** radio button (no other DHCP features will be available).

**Starting IP Address.** Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default Starting IP Address is **192.168.1.100**.

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

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



Figure 5-11: DHCP Server Settings

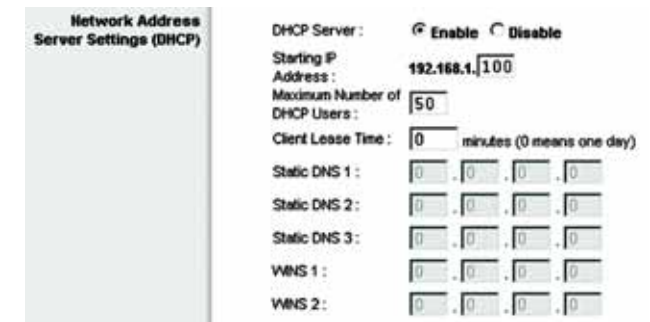


Figure 5-12: Network Address Server Settings

**Static DNS (1-3).** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that IP Address in one of these fields. You can type up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

**WINS.** The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

### Time Setting

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

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

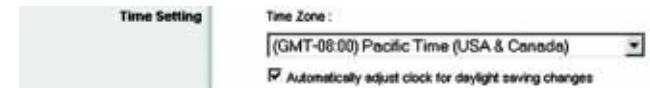


Figure 5-13: Time Setting



## The Setup Tab - 3G/UMTS Network

On this screen, you can configure mobile network settings and view mobile status information for the Router. Some of these settings will be automatically configured by the Router and, in most cases, do not need to be changed unless you are instructed to do so.

### Mobile Network Settings

**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 **Disable**.

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

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

**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 mobile network for a specific period of time, then enter the number of minutes you want to specify in the field provided.

### 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. Complete the *APN Name*, *User Name*, *Password*, *DNS Supplied by Network*, and *DNS 1-2* fields as needed.

**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 the technical support of your mobile service provider or Linksys, or the IT manager of your company. If you have access to a private APN, you can enter its name here.



Figure 5-14: Setup Tab - 3G/UMTS

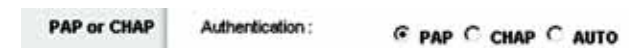


Figure 5-15: Setup Tab - PAP or CHAP

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

**Password.** The Password is automatically entered by the Router. Do not change this setting unless told to do so by either the technical support of your mobile service provider or Linksys, 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 the checkbox. 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

This section indicates whether the Router is using a mobile network bearer or a HSDPA/3G/UMTS or GPRS network.

**Mobile Network Bearer.** Displayed here is the name of the mobile network bearer the Router is using.

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

**Signal Strength.** This indicates the strength of the HSDPA/3G/UMTS or GPRS signal that the Router is receiving.

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

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

## 3G/UMTS Card Status

**Card Model.** Displayed here is the model number of your mobile card.

**Card Revision.** This is the revision number of your mobile card.

**Card Firmware.** This is the firmware version of your mobile card.

The screenshot shows the 'APN Configuration' section of a router's web interface. It contains the following fields and values:

- APN Name :** internet
- User Name :** web
- Password :** (masked with asterisks)
- DNS Supplied by Network :** ☒
- DNS 1 :** 0 . 0 . 0 . 0
- DNS 2 :** 0 . 0 . 0 . 0

Figure 5-16: APN Configuration



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

To update the screen with the latest status information, click the **Refresh** button.

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

## The Setup Tab - DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, [www.dyndns.org](http://www.dyndns.org) or [www.TZO.com](http://www.TZO.com).

### DynDNS.org

**DDNS Service.** From this pull-down menu, enter the DDNS service with which you have membership.

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

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

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

**Internet IP Address.** This is the Router's current IP Address as seen on the Internet.

**Status.** This displays the status of the DDNS connection.

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

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

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

### TZO.com

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

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

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

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



Figure 5-17: Setup Tab - DDNS (DynDNS.org)



Figure 5-18: Setup Tab - DDNS (TZO.org)

## The Setup Tab - MAC Address Clone

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

### MAC Clone

**Enable/Disable.** To have the MAC Address cloned, click the radio button beside *Enable*.

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

**Clone Your PC's MAC.** Clicking this button will clone the MAC address.

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



Figure 5-19: Setup Tab - MAC Address Clone

## The Setup Tab - Advanced Routing

This tab is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing will automatically adjust how packets travel on your network. Static Routing sets up a fixed route to another network destination.

### Advanced Routing

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

### Dynamic Routing

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

### Static Routing

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

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

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

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

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



Figure 5-20: Setup Tab - Advanced Routing (Gateway)



Figure 5-21: Setup Tab - Advanced Routing (Router)

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

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

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

## The Wireless Tab - Basic Wireless Settings

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

### Wireless Network

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

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

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

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

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



Figure 5-22: Wireless Tab - Basic Wireless Settings

## The Wireless Tab - Wireless Security

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



**IMPORTANT:** Linksys strongly recommends that you enable wireless security on your wireless network. Otherwise, unauthorised users may be able to access the Internet using your service and incur additional charges. You are liable for any and all additional charges from your service provider.

### Wireless Security

**WPA Personal.** WPA gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, TKIP or AES. Enter a WPA Shared Key of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.

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



**IMPORTANT:** If you are using WPA or WPA2, always remember that each device in your wireless network MUST use the same WPA method and shared key, or else the network will not function properly.

**WPA2 Personal.** WPA2 automatically uses TKIP + AES with dynamic encryption keys. Enter a WPA Shared Key of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.

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



Figure 5-23: Wireless Tab - Wireless Security (WPA Personal - TKIP)



Figure 5-24: Wireless Tab - Wireless Security (WPA Personal - AES)



Figure 5-25: Wireless Tab - Wireless Security (WPA2 Personal)

**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.) First, select the type of WPA algorithm you want to use, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the Router and the server. Last, enter a Key Renewal Timeout, which instructs the Router how often it should change the encryption keys.

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



Figure 5-26: Wireless Tab - Wireless Security (WPA Enterprise - TKIP)



Figure 5-27: Wireless Tab - Wireless Security (WPA Enterprise - AES)

**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.) WPA2 automatically uses TKIP + AES with dynamic encryption keys. Enter the RADIUS server's IP Address and port number, along with a key shared between the Router and the server. Last, enter a Key Renewal Timeout, which instructs the Router how often it should change the encryption keys.

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



Figure 5-28: Wireless Tab - Wireless Security (WPA2 Enterprise - TKIP)



Figure 5-29: Wireless Tab - Wireless Security (WPA2 Enterprise - AES)



**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.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the Router and the server. Then, select a Default Transmit Key (choose which Key to use), and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Last, either generate a WEP key using the Passphrase or enter the WEP key manually. If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F".

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



**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.

**WEP.** WEP is a basic encryption method, which is not as secure as WPA. To use WEP, select a Default Transmit Key (choose which Key to use), and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Then either generate a WEP key using the Passphrase or enter the WEP key manually. If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F".

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

For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."



Figure 5-30: Wireless Tab - Wireless Security (RADIUS)



Figure 5-31: Wireless Tab - Wireless Security (WEP)

## The Wireless Tab - Wireless MAC Filter

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

### Wireless MAC Filter

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

**Prevent.** Clicking this button will block wireless access by MAC Address.

**Permit Only.** Clicking this button will allow wireless access by MAC Address.

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

To save your list of MAC addresses, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes.

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



Figure 5-32: Wireless Tab - Wireless MAC Filter



Figure 5-33: MAC Address Filter List

## The Wireless Tab - Advanced Wireless Settings

This tab is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

### Advanced Wireless

**Authentication Type.** The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With **Open System** authentication, the sender and the recipient do NOT use a WEP key for authentication. With **Shared Key** authentication, the sender and recipient use a WEP key for authentication.

**Basic Rate.** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

**Transmission Rate.** The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

**CTS Protection Mode.** CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your Wireless-G products not being able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance.

**Frame Burst.** Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, **Disable**.

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

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



Figure 5-34: Wireless Tab - Advanced Wireless Settings

sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

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

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

**AP Isolation.** This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, select **On**. AP Isolation is **Off** by default.

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

## The Security Tab - Firewall

### Firewall

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

### Block WAN Requests

**Block Anonymous Internet Requests.** Use this feature to prevent your network from being “pinged,” or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Remove the checkmark to allow anonymous Internet requests.

**Filter Multicast.** Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. This feature is enabled by default. Remove the checkmark to disable this feature.

**Filter Internet NAT Redirection.** This feature uses port forwarding to block access to local servers from local networked computers. Click the checkbox to filter Internet NAT redirection, or remove the checkmark to disable this feature.

**Filter IDENT (Port 113).** This feature keeps port 113 from being scanned by devices outside of your local network. This feature is enabled by default. Remove the checkmark to disable this feature.

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



Figure 5-35: Security Tab - Firewall

## The Security Tab - VPN Passthrough

Use this screen to allow 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, click **Enable**. IPSec Passthrough is enabled by default.

**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, click **Enable**. PPTP Passthrough is enabled by default.

**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, click **Enable**. L2TP Passthrough is enabled by default.

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

## The Access Restrictions Tab - 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, websites, and inbound traffic during specific days and times.

### Internet Access

**Internet Access Policy.** Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the **Save Settings** button is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete** button. To view all the policies, click the **Summary** button. (Policies can be deleted from the *Summary* screen by selecting the policy or policies and clicking the **Delete** button. To return to the Internet Access tab, click the **Close** button.)

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

To create an Internet Access policy:

1. Select a number from the *Internet Access Policy* drop-down menu.



Figure 5-36: Security Tab - VPN Passthrough



Figure 5-37: Access Restrictions Tab - Internet Access

2. To enable this policy, click the radio button beside *Enable*.
3. Enter a Policy Name in the field provided.
4. Click the **Edit List of PCs** button to select which PCs will be affected by the policy. The *List of PCs* screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button.
5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
7. You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to *Blocked Services*. Then enter the range of ports you want to filter.

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

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

To modify a service, select it from the list on the right. Make changes, and then click the **Modify** button.

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

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

8. If you want to block websites with specific URL addresses, enter each URL in a separate field next to *Website Blocking by URL Address*.
9. If you want to block websites using specific keywords, enter each keyword in a separate field next to *Website Blocking by Keyword*.
10. Click the **Save Settings** button to save the policy's settings. To cancel the policy's settings, click the **Cancel Changes** button.



Figure 5-38: Internet Policy Summary



Figure 5-39: List of PCs



Figure 5-40: Port Services



## The Applications and Gaming Tab - Port Range Forward

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

### Port Range Forward

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

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

**Start/End.** This is the port range. Enter the number that starts the port range under **Start** and the number that ends the range under **End**.

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

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

**Enable.** Click the **Enable** checkbox to enable port forwarding for the relevant application.

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



Figure 5-41: Applications and Gaming Tab - Port Range Forward



## The Applications & Gaming Tab - Port Triggering

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

### Port Triggering

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

### Triggered Range

For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

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

**End Port.** Enter the ending port number of the Triggered Range.

### Forwarded Range

For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

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

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

**Enable.** Click the **Enable** checkbox to enable port triggering for the relevant application.

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

Application	Triggered Range		Forwarded Range		Enable
	Start Port	End Port	Start Port	End Port	

**Port Triggering**  
 Description: Enter the application name of the trigger. Triggered Range: Enter the port number range. Forwarded Range: Enter the port number range. Enable: Check the Enable checkbox to enable port triggering for the relevant application.  
 Instructions: Enter the application name of the trigger. Enter the port number range of the triggered range. Enter the port number range of the forwarded range. Check the Enable checkbox to enable port triggering for the relevant application.  
 Start Port: Enter the starting port number of the triggered range. End Port: Enter the ending port number of the triggered range.  
 Start Port: Enter the starting port number of the forwarded range. End Port: Enter the ending port number of the forwarded range.

Save Settings Cancel Changes

Figure 5-42: Applications and Gaming Tab - Port Triggering

## The Applications and Gaming Tab - DMZ

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

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

### DMZ

To expose one PC, select **Enable**. Then, enter the computer's IP address in the *DMZ Host IP Address* field.

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



Figure 5-43: Applications and Gaming Tab - DMZ

## The Applications and Gaming Tab - QoS

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

There are three types of Wired QoS available, Device Priority, Application Priority, and Ethernet Port Priority. You can also configure Wireless QoS on this page.

### Wired QoS

**Enable/Disable.** To limit outgoing bandwidth for the QoS policies in use, select **Enable**. Otherwise, select **Disable**.

**Upstream Bandwidth.** Select the bandwidth to be used from the drop-down menu. This setting allows you to limit the outgoing bandwidth for the QoS policies in use, so you can control how much bandwidth a particular application is allowed to use.

### Device Priority

**Device name, Priority, and MAC Address.** For each device, enter the name of your network device in the *Device name* field. Then select its Priority and enter its MAC Address.

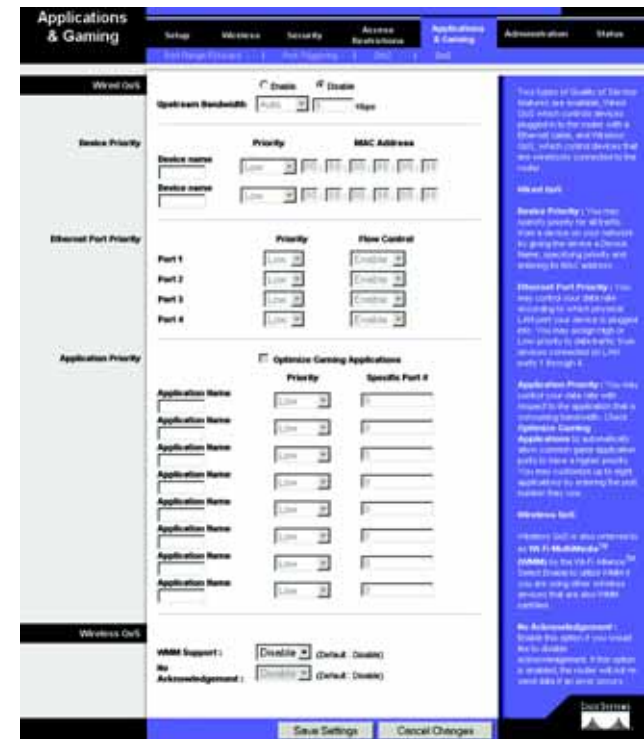


Figure 5-44: Applications and Gaming Tab - QoS

## Ethernet Port Priority

**Port 1-4, Priority, and Flow Control.** Ethernet Port Priority QoS allows you to prioritize performance for four of the Router's ports, Ethernet (LAN) Ports 1-4. For each of these ports, select **High** or **Low** for *Priority*. For Flow Control, if you want the Router to control the transmission of data between network devices, select **Enable**. To disable this feature, select **Disable**.

Ethernet Port Priority QoS does not require support from your ISP because the prioritized ports are LAN ports going out to your network.

## Application Priority

Application Priority QoS manages information as it is transmitted and received. You can have gaming application ports assigned higher priority. You can also configure the Router to assign high or low priority to ports for applications that you specify.

**Optimize Gaming Applications.** Click this checkbox if you want the Router to automatically assign higher priority to common game application ports.

**Application Name, Priority, and Specific Port #.** Enter the name of the application in the *Application Name* field. For each application, select **High** or **Low** for *Priority* and enter its respective port number in the *Specific Port#* fields.

## Wireless QoS

You can configure the WMM™ (Wi-Fi Multimedia) support and No Acknowledgement settings in this section.

**WMM Support.** If you have other devices that support WMM on your network, select **Enable** from the drop-down menu. Otherwise, keep the default, **Disable**.

**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 **Enable** from the drop-down menu. Otherwise, keep the default, **Disable**.

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

## The Administration Tab - Management

This section of the Administration tab allows the network's administrator to manage specific Router functions for access and security.

### Router Password

#### Local Router Access

**Router Password and Re-enter to confirm.** You can change the Router's password from here. Enter a new Router password and then type it again in the *Re-enter to confirm* field to confirm.

#### Web Access

**Access Server.** HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS is a similar protocol, but it uses SSL (Secured Socket Layer) to encrypt transmitted data, so security is increased. Select the protocol you want to use, **HTTP** or **HTTPS**.

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

#### Remote Router Access

**Remote Management and Management Port.** To access the Router remotely, from outside the network, verify that **Enable** is selected. Then, enter the port number that will be open to outside access. You will need to enter the Router's password when accessing the Router this way, as usual.

**Use https.** If you want to require the use of SSL (Secured Socket Layer) to encrypt transmitted data, click the checkbox.

### UPnP

**UPnP.** When using UPnP features, select **Enable**. Because allowing this may present a risk to security, this feature is disabled by default.

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



Figure 5-45: Administration Tab - Management

## The Administration Tab - Log

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

### Log

**Log.** To disable the Log function, keep the default setting, **Disable**. To monitor traffic between the network and the Internet, select **Enable**. When you wish to view the logs, click **Incoming Log** or **Outgoing Log**, depending on which you wish to view.

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



Figure 5-46: Administration Tab - Log

## The Administration Tab - Diagnostics

The Diagnostics screen lets you reboot the Router and run diagnostic tests, which allow you to check the connections of your network components.

### Reboot

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

### Ping Test

**Ping Parameters.** The Ping test will check the status of a connection. Click the **Ping** button to open the *Ping Test* screen. Enter the address of the PC whose connection you wish to test and how many times you wish to test it. Then, click the **Ping** button. The *Ping Test* screen will then display the test results. To stop the test, click the **Stop** button. Click the **Clear Log** button to clear the screen. Click the **Close** button to return to the *Diagnostics* screen.

### Traceroute Test

**Traceroute Parameters.** To test the performance of a connection, click the **Traceroute** button. Enter the address of the PC whose connection you wish to test and click the **Traceroute** button. The *Traceroute* screen will then display the test results. To stop the test, click the **Stop** button. Click the **Clear Log** button to clear the screen. Click the **Close** button to return to the *Diagnostics* screen.



Figure 5-47: Administration Tab - Diagnostics



Figure 5-48: Ping Test



Figure 5-49: Traceroute Test

## The Administration Tab - Factory Defaults

### Factory Defaults

**Restore Factory Defaults.** Click the **Yes** button to reset all configuration settings to their default values, and then click the **Save Settings** button. Any settings you have saved will be lost when the default settings are restored. This feature is disabled by default. Click the **Cancel Changes** button to cancel your change.

## The Administration Tab - Firmware Upgrade

### Upgrade Firmware

To upgrade the Router's firmware, first download the firmware from the Linksys website. Then extract the file on your computer. Do not upgrade your firmware unless you are experiencing problems with the Router.

**Please select a file to upgrade.** Click the **Browse** button to find the extracted firmware file. Then click the **Upgrade** button. For more information about upgrading firmware, refer to "Appendix C: Upgrading Firmware".



**IMPORTANT:** After you upgrade the Router's firmware, follow these instructions:

1. Unplug its power adapter to power off the Router.
2. Plug in the power adapter to power on the Router.
3. Access the Router's Web-based Utility.
4. Click the **Administration** tab.
5. Click the **Factory Defaults** tab.
6. Click the **Yes** button to reset the Router to its factory default settings.

## The Administration Tab - Config Management

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

### Backup Configuration

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

### Router Configuration

To restore the Router's configuration file, click the **Browse** button to locate the file, and follow the on-screen instructions. After you have selected the file, click the **Restore** button.



Figure 5-50: Administration Tab - Factory Defaults



Figure 5-51: Administration Tab - Firmware Upgrade



Figure 5-52: Administration Tab - Config Management

## The Status Tab - 3G/UMTS

The *3G/UMTS* screen on the Status Tab displays the Router's current mobile network and HSDPA/3G/UMTS card status.

### Mobile Network Status

**Mobile Network Bearer.** Displayed here is the name of the mobile network bearer the Router is using.

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

**Signal Strength.** This indicates the strength of the HSDPA/3G/UMTS or GPRS signal that the Router is receiving.

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

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

### 3G/UMTS Card Status

**Card Model.** Displayed here is the model number of your mobile card.

**Card Revision.** This is the revision number of your mobile card.

**Card Firmware.** This is the firmware version of your mobile card.

**IMSI.** This identifies your mobile card on the network.

Click the **Refresh** button to view the latest status information.



Figure 5-53: Status Tab - 3G/UMTS



## The Status Tab - Router

The *Router* screen on the Status Tab displays the Router's current status.

### Router Information

**Firmware Version.** This is the Router's current firmware.

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

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

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

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

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

### Internet

**Configuration Type.** Displayed here is the information required by your ISP for connection to the Internet. This information was entered on the Setup Tab. Depending on the type of connection you use, the **Connect** or **Disconnect** button will appear so you can start or end your Internet connection, or the **DHCP Release** and **DHCP Renew** buttons will appear so you can release or renew the Internet IP address from this screen.

Click the **Refresh** button to view the latest status information.



Figure 5-54: Status Tab - Router

## The Status Tab - Local Network

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

### Local Network

**MAC Address.** This is the Router's MAC Address, as seen on your local, Ethernet network.

**IP Address.** This shows the Router's IP Address, as it appears on your local, Ethernet network.

**Subnet Mask.** When the Router is using a Subnet Mask, it is shown here.

**DHCP Server.** If you are using the Router as a DHCP server, that will be displayed here.

**Start IP Address.** For the range of IP Addresses used by devices on your local, Ethernet network, the beginning of that range is shown here.

**End IP Address.** For the range of IP Addresses used by devices on your local, Ethernet network, the end of that range is shown here.

**DHCP Clients Table.** Clicking this button will open a screen to show you which PCs are utilizing the Router as a DHCP server. You can delete PCs from that list, and sever their connections, by checking a **Delete** box and clicking the **Delete** button.

Click the **Refresh** button to view the latest status information.



Figure 5-55: Status Tab - Local Network

## The Status Tab - Wireless

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

### Wireless

**MAC Address.** This is the Router's MAC Address, as seen on your local, wireless network.

**Mode.** As selected from the Wireless tab, this will display the wireless mode (Mixed, G-Only, or Disabled) used by the network.

**SSID.** As entered on the Wireless tab, this will display the wireless network name or SSID.

**DHCP Server.** If you are using the Router as a DHCP server, that will be displayed here.

**Channel.** As entered on the Wireless tab, this will display the channel on which your wireless network is broadcasting.

**Encryption Function.** As selected on the Wireless Security Tab, this will display what type of encryption the Router uses for security.

Click the **Refresh** button to view the latest status information.



Figure 5-56: Status Tab - Wireless

# Appendix A: Troubleshooting

This appendix consists of two parts: “Common Problems and Solutions” and “Frequently Asked Questions.” Provided are possible solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help you solve your problems. If you can’t find an answer here, check the Linksys website at [www.linksys.com/international](http://www.linksys.com/international).

## Common Problems and Solutions

**1. *I’m trying to access the Router’s Web-based Utility, but I do not see the login screen. Instead, I see a screen saying, “404 Forbidden.”***

If you are using Windows Explorer, perform the following steps until you see the Web-based Utility’s login screen (Netscape Navigator will require similar steps):

1. Click **File**. Make sure *Work Offline* is NOT checked.
2. Press **CTRL + F5**. This is a hard refresh, which will force Windows Explorer to load new webpages, not cached ones.
3. Click **Tools**. Click **Internet Options**. Click the **Security** tab. Click the **Default level** button. Make sure the security level is Medium or lower. Then click the **OK** button.

**2. *I need to set a static IP address on a PC.***

You can assign a static IP address to a PC by performing the following steps:

- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the **Properties** option.
  3. In the Components checked are used by this connection box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
  5. Enter the Subnet Mask, **255.255.255.0**.
  6. Enter the Default Gateway, **192.168.1.1** (Router’s default IP address).
  7. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
  9. Restart the computer if asked.
- For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click **Start** and **Control Panel**.
2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
4. In the This connection uses the following items box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
5. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
6. Enter the Subnet Mask, **255.255.255.0**.
7. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
8. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

**3. I want to test my Internet connection.**

A Check your TCP/IP settings.

For Windows 2000, and XP:

- Refer to Windows Help for details. Make sure Obtain IP address automatically is selected in the settings.

B Open a command prompt.

For Windows 2000 and XP:

- Click **Start** and **Run**. In the *Open* field, type **cmd**. Press the **Enter** key or click the **OK** button. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.
  - If you get a reply, the computer is communicating with the Router.
  - If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.
- C In the command prompt, type **ping** followed by your Internet or WAN IP address and press the **Enter** key. The Internet or WAN IP Address can be found on the Status screen of the Router's web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.
- If you get a reply, the computer is connected to the Router.
  - If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- D In the command prompt, type **ping www.yahoo.com** and press the **Enter** key.
- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

**4. *I am not getting an IP address on the Internet with my Internet connection.***

- Refer to “Problem #3, I want to test my Internet connection” to verify that you have connectivity.
- If you need to register the MAC address of your Ethernet adapter with your ISP, please see “Appendix E: Finding the MAC address and IP Address for Your Ethernet Adapter.” If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of “Chapter 8: Configuring the Wireless-G Router for 3G/UMTS Broadband” for details.
- Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of “Chapter 8: Configuring the Wireless-G Router for 3G/UMTS Broadband” for details on Internet connection settings.
- Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.
- Make sure the cable connecting from your cable or DSL modem is connected to the Router’s Internet port. Verify that the Status page of the Router’s web-based utility shows a valid IP address from your ISP.
- Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router’s web-based utility to see if you get an IP address.

**5. I am not able to access the Setup page of the Router's web-based utility.**

- Refer to "Problem #3, I want to test my Internet connection" to verify that your computer is properly connected to the Router.
- Refer to "Appendix E: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
- Set a static IP address on your system; refer to "Problem #2: I need to set a static IP address."
- Refer to "Problem #10: I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window."

**6. I need to set up a server behind my Router and make it available to the public.**

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router. Go to the Applications & Gaming => Port Range Forward tab.
2. Enter any name you want to use for the Application.
3. Enter the Start and End Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
4. Select the protocol(s) you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enable** option for the port services you want to use. Consider the example below:

Application	Start and End	Protocol	IP Address	Enabled
Web server	80 to 80	Both	192.168.1.100	X
FTP server	21 to 21	TCP	192.168.1.101	X
SMTP (outgoing)	25 to 25	Both	192.168.1.102	X
POP3 (incoming)	110 to 110	Both	192.168.1.102	X

When you have completed the configuration, click the **Save Settings** button.

**7. I need to set up online game hosting or use other Internet applications.**

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Router's web interface by going to <http://192.168.1.1> or the IP address of the Router. Go to the Applications & Gaming => Port Range Forward tab.
2. Enter any name you want to use for the Application.
3. Enter the Start and End Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Select the protocol(s) you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enable** option for the port services you want to use. Consider the example below:

Application	Start and End	Protocol	IP Address	Enabled
UT	7777 to 27900	Both	192.168.1.100	X
Half-life	27015 to 27015	Both	192.168.1.105	X
PC Anywhere	5631 to 5631	UDP	192.168.1.102	X
VPN IPSEC	500 to 500	UDP	192.168.1.100	X

When you have completed the configuration, click the **Save Settings** button.

**8. I can't get the Internet game, server, or application to work.**

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.)



Follow these steps to set DMZ hosting:

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router. Go to the Applications & Gaming => Port Range Forward tab.
2. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
3. Go to the Applications & Gaming => DMZ tab.
4. Select **Enable** next to DMZ. In the *Client PC IP Address* field, enter the IP address of the computer you want exposed to the Internet. This will bypass the NAT technology for that computer. Please refer to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
5. Once completed with the configuration, click the **Save Settings** button.

**9. *I forgot my password, or the password prompt always appears when I am saving settings to the Router.***

Reset the Router to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router. Enter the default password admin, and click the Administration => Management tab.
2. Enter a different password in the *Router Password* field, and enter the same password in the second field to confirm the password.
3. Click the **Save Settings** button.

**10. *I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.***

If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

- For Microsoft Internet Explorer 5.0 or higher:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click Internet Options.
  2. Click the **Connections** tab.
  3. Click the **LAN settings** button and remove anything that is checked.
  4. Click the **OK** button to go back to the previous screen.
  5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.
- For Netscape 4.7 or higher:
  1. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
  2. Make sure you have Direct connection to the Internet selected on this screen.
  3. Close all the windows to finish.

**11. To start over, I need to set the Router to factory default.**

Hold the **Reset** button for 10 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

**12. I need to upgrade the firmware.**

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at [www.linksys.com/international](http://www.linksys.com/international).

Follow these steps:

1. Go to the Linksys website at <http://www.linksys.com/international> and download the latest firmware.
2. To upgrade the firmware, follow the steps in "Appendix C: Upgrading Firmware."

**13. The firmware upgrade failed, and/or the Power LED is flashing.**

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Power LED stop flashing:

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the PC; refer to "Problem #2, I need to set a static IP address." Use the following IP address settings for the computer you are using:  
IP Address: 192.168.1.50  
Subnet Mask: 255.255.255.0  
Gateway: 192.168.1.1
- Perform the upgrade using the TFTP program or the Administration tab of the Router's web-based utility.

**14. My DSL service's PPPoE is always disconnecting.**

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet.

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.
  1. To connect to the Router, go to the web browser, and enter <http://192.168.1.1> or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. On the *Setup* screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
  4. Click the **Save Settings** button.
  5. Click the **Status** tab, and click the **Connect** button.
  6. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
- Click the **Save Settings** button to continue.
- If the connection is lost again, follow steps 1- 6 to re-establish connection.

**15. I can't access my e-mail, web or I am getting corrupted data from the Internet.**

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492.

- If you are having some difficulties, perform the following steps:
  1. To connect to the Router, go to the web browser, and enter `http://192.168.1.1` or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. Look for the MTU option, and select **Manual**. In the *Size* field, enter 1492.
  4. Click the **Save Settings** button to continue.
- If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
  - 1462
  - 1400
  - 1362
  - 1300

**16. The Power LED keeps flashing.**

The Power LED flashes when the device is first powered up. Meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED stays solid to show that the system is working fine. If the LED keeps flashing after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

**17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.**

- Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

## Frequently Asked Questions

***What is the maximum number of IP addresses that the Router will support?***

The Router will support up to 253 IP addresses.

***Is IPSec Pass-Through supported by the Router?***

Yes, it is a built-in feature that the Router automatically enables.

***Where is the Router installed on the network?***

In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

***Does the Router support IPX or AppleTalk?***

No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.

***Does the Internet connection of the Router support 100Mbps Ethernet?***

The Router's current hardware design supports up to 100Mbps Ethernet on its Internet port; however, the Internet connection speed will vary depending on the speed of your broadband connection. The Router also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.

***What is Network Address Translation and what is it used for?***

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with low cost Internet accounts, such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

***Does the Router support any operating system other than Windows 2000 or Windows XP?***

Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of other operating systems.

***Does the Router support ICQ send file?***

Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Router.

***I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?***

If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

***Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?***

It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

***How do I get Half-Life: Team Fortress to work with the Router?***

The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

***How can I avoid corrupted FTP downloads?***

If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

***The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?***

Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at [www.linksys.com/international](http://www.linksys.com/international) for more information.

***If all else fails in the installation, what can I do?***

Reset the Router by holding down the reset button until the Power LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, [www.linksys.com/international](http://www.linksys.com/international).

***How will I be notified of new Router firmware upgrades?***

All Linksys firmware upgrades are posted on the Linksys website at [www.linksys.com/international](http://www.linksys.com/international), where they can be downloaded for free. To upgrade the Router's firmware, use the Administration - Firmware Upgrade tab of the Router's web-based utility. If the Router's Internet connection is working well, there is no need to download a

newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

***Will the Router function in a Macintosh environment?***

Yes, but the Router's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

***I am not able to get the web configuration screen for the Router. What can I do?***

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

***What is DMZ Hosting?***

Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter."

***If DMZ Hosting is used, does the exposed user share the public IP with the Router?***

No.

***Does the Router pass PPTP packets or actively route PPTP sessions?***

The Router allows PPTP packets to pass through.

***Is the Router cross-platform compatible?***

Any platform that supports Ethernet and TCP/IP is compatible with the Router.

***How many ports can be simultaneously forwarded?***

Theoretically, the Router can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

***What are the advanced features of the Router?***

The Router's advanced features include advanced wireless settings, filters, access restriction policies, port forwarding, advanced routing, and DDNS.

***How do I get mIRC to work with the Router?***

Under the Port Forwarding tab, set port forwarding to 113 for the PC on which you are using mIRC.

***Can the Router act as my DHCP server?***

Yes. The Router has DHCP server software built-in.

***Can I run an application from a remote computer over the wireless network?***

This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

***What is the IEEE 802.11g standard?***

It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

***What is the IEEE 802.11b standard?***

It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

***What IEEE 802.11g features are supported?***

The product supports the following IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

***What IEEE 802.11b features are supported?***

The product supports the following IEEE 802.11b functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

***What is ad-hoc mode?***

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.

***What is infrastructure mode?***

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

***What is roaming?***

Roaming is the ability of a portable computer to communicate continuously while the user is moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

***What is ISM band?***

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

***What is Spread Spectrum?***

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband



transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

***What is DSSS? What is FHSS? And what are their differences?***

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

***What is WEP?***

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

***What is a MAC Address?***

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

***How do I reset the Router?***

Press the Reset button on the back panel for about five seconds. This will reset the Router to its default settings.

***How do I resolve issues with signal loss?***

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Router and a wireless PC will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Router and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel.

***I have excellent signal strength, but I cannot see my network.***

Wireless security is probably enabled on the Router, but not on your wireless adapter (or vice versa). Verify that the same wireless security method and passphrase/keys are being used on all devices of your wireless network.

***How many channels/frequencies are available with the Router?***

There are eleven available channels, ranging from 1 to 11, in North America. There are thirteen available channels, ranging from 1 to 13, in most of Europe. There may be additional channels available in other regions, subject to the regulations of your region and/or country.

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

There are three options available to connect to the mobile network.

The first option is to power on the Router with the mobile card inserted. Then press the 3G/UMTS Connect/Disconnect button on the front panel of the Router. The Router will connect to the mobile network via the mobile card. If this is successful, the 3G/UMTS LED on the Router will light up.

The second option is to log onto the Router via the Web-based Utility. On the first screen you see, the *Basic Setup* screen, click the **Connect** button near the top of the screen. The Router will connect to the mobile network via the mobile card. If this is successful, the Mobile Connection line will say, "Connected" instead of "Disconnected."

The third option is to enable the Router's Auto Connect feature. This will enable the Router to automatically connect to the mobile network whenever it is powered on. As with the second option, this can be done using the Web-based Utility of the Router. On the first screen you see, the *Basic Setup* screen, click the **3G/UMTS Network** tab. On the *3G/UMTS Network* screen, there is an Auto Connect option at the top of the screen. Click the **Enable** radio button, and then click the **Save Settings** button. After the webpage has refreshed, click the **Basic Setup** tab. On the *Basic Setup* screen, click the **Connect** button to connect to the mobile network. 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 and mobile card?***

POWER	This green LED will be solidly lit when the Router is powered on.
ETHERNET	Each of these green LEDs will be solidly lit when there is an active connection to the corresponding Ethernet port of the Router. Each LED flashes when there is network traffic passing through the corresponding port.
WIRELESS	This green LED will be solidly lit when the Router is connected to the Wireless-G (802.11g) and/or Wireless-B (802.11b) network. The LED flashes when there is network traffic passing through the wireless connection.
DMZ	This green, De-Militarised Zone (DMZ) LED will be solidly lit when the Router's DMZ function is active. The DMZ function allows one local computer to be exposed to the Internet.

**3G/UMTS** The 3G/UMTS LED flashes as the Router connects to the mobile network. It is solidly lit when the connection is established. The LED lights up blue if the Router connects to a HSDPA/3G/UMTS network. The LED lights up green if the Router connects to a GPRS network.

If the LED quickly flashes blue and green, and the Router is not connected to the mobile network, then either its PIN code is incorrect, or there is no HSDPA/3G/UMTS or SIM card inserted when you push the 3G/UMTS Connect/Disconnect button.

***How do I know which mobile network I am using?***

Log onto the Router via the Web-based Utility at <http://192.168.1.1>. The username and password should be **admin** unless you have changed them. Click the **Status** tab, and then click the **3G/UMTS** tab. In the Mobile Network Status section, on the Network Name line, you will see the name of the network you are currently using.

***The connection to the mobile network drops or frequently changes from HSDPA/3G/UMTS to GPRS. How do I control this?***

Log onto the Router via the Web-based Utility at <http://192.168.1.1>. On the *Basic Setup* screen, there are three Service options listed near the top of the screen. Select the one appropriate for your location and preferences.

**HSDPA/3G/UMTS**

**Preferred**

(recommended) The mobile card will use the HSDPA/3G/UMTS mobile network when it is available. When the signal strength from the GPRS network is significantly stronger than the HSDPA/3G/UMTS signal, the mobile card will use the GPRS network. This could result in a card changing networks frequently in areas of mixed coverage.

**HSDPA/3G/UMTS**

**Only**

The mobile card will only use the HSDPA/3G/UMTS mobile network. It will not connect to the GPRS network. You should use this option if you want to prevent the card from frequently changing networks. However, if there is no HSDPA/3G/UMTS mobile network coverage, then the card will not be able to connect to the network.

**GPRS Only**

The mobile card will use the GPRS mobile network. It will not connect to the HSDPA/3G/UMTS network. You should use this option if you want to prevent the card from frequently changing networks. However, if there is no GPRS mobile network coverage, the card will not be able to connect to the network.

***Whom should I call if there is a question or problem?***

For technical or customer support regarding the mobile card, contact your mobile service provider. If your questions about the Router are not addressed here, refer to the Linksys website, [www.linksys.com/international](http://www.linksys.com/international).

# Appendix B: Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.



**IMPORTANT:** Linksys strongly recommends that you enable wireless security on your wireless network. Otherwise, unauthorized users may be able to access the Internet using your service and incur additional charges. You are liable for any and all additional charges from your service provider.

## Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

For information on implementing these security features, refer to “Chapter 8: Configuring the Wireless-G Router for 3G/UMTS Broadband.”

## Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for “beacon messages”. These messages can be easily decrypted and contain much of the network’s information, such as the network’s SSID (Service Set Identifier). Here are the steps you can take:

**Change the administrator’s password regularly.** With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only

person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

**SSID.** There are several things to keep in mind about the SSID:

1. Disable Broadcast
2. Make it unique
3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

**MAC Addresses.** Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

**WEP Encryption.** Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Use "Shared Key" authentication
3. Change your WEP key regularly

**WPA.** Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. **WPA2** is the newer version of Wi-Fi Protected Access with stronger encryption than WPA. WPA gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which incorporates Message Integrity Code (MIC) to



**IMPORTANT:** Always remember that each device in your wireless network **MUST** use the same security method and passphrase or key; otherwise, your wireless network will not function properly.

provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. (AES is stronger than TKIP.) WPA2 uses TKIP + AES for encryption.

WPA Enterprise and WPA2 Enterprise use a RADIUS (Remote Authentication Dial-In User Service) server for authentication. RADIUS uses a RADIUS server and WEP encryption.

**WPA Personal.** Select the type of algorithm, TKIP or AES, and enter a password in the *Passphrase* field of 8-63 characters. Enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Router or other device how often it should change the encryption keys.

**WPA2 Personal.** WPA2 uses TKIP + AES, with dynamic encryption keys. Enter a *Passphrase* of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router or other device how often it should change the encryption keys.

**WPA Enterprise.** This method is WPA used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Router and its RADIUS server. Then enter a Key Renewal Timeout period, which instructs the Router or other device how often it should change the encryption keys.

**WPA2 Enterprise.** This method is WPA2 used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Router and its RADIUS server. Then enter a Key Renewal Timeout period, which instructs the Router or other device how often it should change the encryption keys.

**RADIUS.** This method is WEP used in coordination with a RADIUS server. Enter the IP address and port number of the RADIUS server. Then enter the key shared between the Gateway and its RADIUS server. Enter the WEP settings.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

# Appendix C: Upgrading Firmware

The Router's firmware is upgraded through the Web-based Utility's Administration tab. Follow these instructions:

1. Download the firmware from Linksys's website at [www.linksys.com/international](http://www.linksys.com/international).
2. Extract the firmware file on your computer.
3. Open the Router's Web-based Utility, and click the **Administration** tab.
4. Click **Firmware Upgrade**, and the *Upgrade Firmware* screen will appear.
5. Enter the location of the firmware's file or click the **Browse** button to find the file.
6. Then click the **Upgrade** button and follow the on-screen instructions.



Figure C-1: Upgrade Firmware

# Appendix D: Windows Help

Almost Linksys wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

## TCP/IP

Before a computer can communicate with the Router, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

## Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

## Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.



# Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Router's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 2000 or XP.

## Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.
2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.
3. Write down the Physical Address as shown on your computer screen (Figure E-1); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

The MAC address/Physical Address is what you will use for MAC address cloning or MAC filtering.



**NOTE:** The MAC address is also called the Physical Address.

The example in Figure E-1 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

## For the Router's Web-based Utility

For MAC filtering, enter the 12-digit MAC address in this format, XXXXXXXXXXXX, WITHOUT the hyphens. See Figure E-2.

For MAC address cloning, enter the 12-digit MAC address in the *User Defined Entry* fields provided, two digits per field. See Figure E-3.

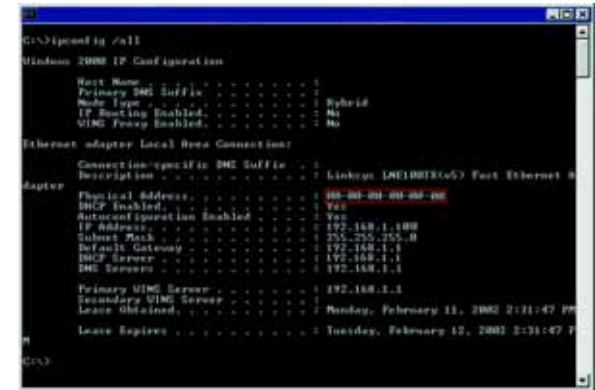


Figure E-1: MAC Address/Physical Address



Figure E-2: MAC Address Filter List



Figure E-3: MAC Address Clone

# Appendix F: Glossary

This glossary contains some basic networking terms you may come across when using this product. For more advanced terms, see the complete Linksys glossary at <http://www.linksys.com/glossary>.

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

**Ad-hoc** - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

**AES (Advanced Encryption Standard)** - A security method that uses symmetric 128-bit block data encryption.

**Bandwidth** - The transmission capacity of a given device or network.

**Bit** - A binary digit.

**Boot** - To start a device and cause it to start executing instructions.

**Broadband** - An always-on, fast Internet connection.

**Browser** - An application program that provides a way to look at and interact with all the information on the World Wide Web.

**Byte** - A unit of data that is usually eight bits long.

**Cable Modem** - A device that connects a computer to the cable television network, which in turn connects to the Internet.

**Daisy Chain** - A method used to connect devices in a series, one after the other.

**DDNS (Dynamic Domain Name System)** - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., [www.xyz.com](http://www.xyz.com)) and a dynamic IP address.

**Default Gateway** - A device that forwards Internet traffic from your local area network.

**DHCP (Dynamic Host Configuration Protocol)** - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

**DMZ (Demilitarized Zone)** - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

**DNS (Domain Name Server)** - The IP address of your ISP's server, which translates the names of websites into IP addresses.

**Domain** - A specific name for a network of computers.

**Download** - To receive a file transmitted over a network.

**DSL (Digital Subscriber Line)** - An always-on broadband connection over traditional phone lines.

**Dynamic IP Address** - A temporary IP address assigned by a DHCP server.

**EAP (Extensible Authentication Protocol)** - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

**Encryption** - Encoding data transmitted in a network.

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

**Firewall** - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

**Firmware** - The programming code that runs a networking device.

**FTP (File Transfer Protocol)** - A protocol used to transfer files over a TCP/IP network.

**Full Duplex** - The ability of a networking device to receive and transmit data simultaneously.

**Gateway** - A device that interconnects networks with different, incompatible communications protocols.

**Half Duplex** - Data transmission that can occur in two directions over a single line, but only one direction at a time.

**HTTP (HyperText Transport Protocol)** - The communications protocol used to connect to servers on the World Wide Web.

**Infrastructure** - A wireless network that is bridged to a wired network via an access point.

**IP (Internet Protocol)** - A protocol used to send data over a network.

**IP Address** - The address used to identify a computer or device on a network.

**IPCONFIG** - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

**IPSec (Internet Protocol Security)** - A VPN protocol used to implement secure exchange of packets at the IP layer.

**ISP (Internet Service Provider)** - A company that provides access to the Internet.

**LAN** - The computers and networking products that make up your local network.

**MAC (Media Access Control) Address** - The unique address that a manufacturer assigns to each networking device.

**Mbps (MegaBits Per Second)** - One million bits per second; a unit of measurement for data transmission.

**NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

**Network** - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

**Packet** - A unit of data sent over a network.

**Passphrase** - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

**Ping (Packet INternet Groper)** - An Internet utility used to determine whether a particular IP address is online.

**POP3 (Post Office Protocol 3)** - A standard mail server commonly used on the Internet.

**Port** - The connection point on a computer or networking device used for plugging in cables or adapters.

**Power over Ethernet (PoE)** - A technology enabling an Ethernet network cable to deliver both data and power.

**PPPoE (Point to Point Protocol over Ethernet)** - A type of broadband connection that provides authentication (username and password) in addition to data transport.

**PPTP (Point-to-Point Tunneling Protocol)** - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

**RADIUS (Remote Authentication Dial-In User Service)** - A protocol that uses an authentication server to control network access.

**RJ-45 (Registered Jack-45)** - An Ethernet connector that holds up to eight wires.

**Roaming** - The ability to take a wireless device from one access point's range to another without losing the connection.

**Router** - A networking device that connects multiple networks together.

**Server** - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

**SMTP (Simple Mail Transfer Protocol)** - The standard e-mail protocol on the Internet.

**SNMP (Simple Network Management Protocol)** - A widely used network monitoring and control protocol.

**SPI (Stateful Packet Inspection) Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

**SSID (Service Set Identifier)** - Your wireless network's name.

**Static IP Address** - A fixed address assigned to a computer or device that is connected to a network.

**Static Routing** - Forwarding data in a network via a fixed path.

**Subnet Mask** - An address code that determines the size of the network.

**Switch** - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

**TCP (Transmission Control Protocol)** - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** - A set of instructions PCs use to communicate over a network.

**Telnet** - A user command and TCP/IP protocol used for accessing remote PCs.

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

**Throughput** - The amount of data moved successfully from one node to another in a given time period.

**TKIP (Temporal Key Integrity Protocol)** - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

**Topology** - The physical layout of a network.

**TX Rate** - Transmission Rate.

**Upgrade** - To replace existing software or firmware with a newer version.

**Upload** - To transmit a file over a network.

**URL (Uniform Resource Locator)** - The address of a file located on the Internet.

**VPN (Virtual Private Network)** - A security measure to protect data as it leaves one network and goes to another over the Internet.

**WAN (Wide Area Network)**- The Internet.

**WEP (Wired Equivalent Privacy)** - A method of encrypting network data transmitted on a wireless network for greater security.

**WLAN (Wireless Local Area Network)** - A group of computers and associated devices that communicate with each other wirelessly.

**WPA (Wi-Fi Protected Access)** - A wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

# Appendix G: Specifications

Model	WRT54G3G
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Channels	11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
Ports/Buttons	Internet: One 10/100 RJ-45 Port or PC Card Slot for any HSDPA/3G/UMTS Card LAN: Four 10/100 RJ-45 Switched Ports One Power Port, One SMA Port, One Reset Button, One 3G Connect/Disconnect Button
Cabling Type	UTP CAT 5
LEDs	Power, DMZ, Internet, 3G/UMTS Wireless, WLAN, Ethernet (1, 2, 3, 4)
RF Power Output	802.11g: Typical 13.5 dBm (+/-2) 802.11b: Typical 16.5 dBm (+/-2)
Receive Sensitivity	11Mbps @ -90 dBm Typical, 54Mbps @ -65 dBm Typical
UPnP able/cert	Able
Security Features	Stateful Packet Inspection (SPI) Firewall, Internet Policy
Wireless Security	Wi-Fi Protected Access™ (WPA/WPA2 Personal), WEP, Wireless MAC Filtering
Dimensions	170 mm x 170 mm x 33 mm (6,69" x 6,69" x 1,30")



#### Wireless-G Router for 3G/UMTS Broadband

Unit Weight	0,35 kg (12,35 oz.)
Power	External 12 V DC, 1,0 A
Certifications	FCC, IC-03, CE, Wi-Fi (802.11b, 802.11g), WPA
Operating Temp.	0° C to 40° C (32° F to 104° F)
Storage Temp.	-20° C to 70° C (-4° F to 158° F)
Operating Humidity	20% to 80% Non-Condensing
Storage Humidity	10% to 90% Non-Condensing
Warranty	1-Year Limited

# Appendix H: Warranty Information

Contact your mobile service provider for information on warranty support for this product.

# Appendix I: 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 20cm between the radiator and your body.

## 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.

## Industry Canada (Canada)

This device complies with Industry Canada ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB003 et RSS210 d'Industrie Canada.

IC Statement

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Règlement d'Industry Canada

Le fonctionnement est soumis aux conditions suivantes :

1. Ce périphérique ne doit pas causer d'interférences;
2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

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)

Declaration of Conformity with Regard to the EU Directive 1999/5/EC  
(R&TTE Directive)

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιαστικές απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Română [Romanian]:	Acest echipament este în conformitate cu cerințele esențiale și cu alte prevederi relevante ale Directivei 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

**NOTE:** For all products, the Declaration of Conformity (DofC) 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](http://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](http://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. Nevertheless, you can further reduce the power output if you wish to do so. For more information about changing the power output settings, refer to your product's documentation on its CD or [www.linksys.com/international](http://www.linksys.com/international).

#### 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 0560** ⓘ or **CE 0678** ⓘ or **CE 0336** ⓘ or **CE** ⓘ

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

## 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:

*Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:*

*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 Ausnahme 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). Table 1 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.

Table 1: Overview of Regulatory Requirements for Wireless LANs

Frequency Band (MHz)	Max Power Level (EIRP) (mW)	Indoor ONLY	Indoor & Outdoor
2400-2483.5	100		X
5150-5350 <sup>†</sup>	200	X	
5470-5725 <sup>†</sup>	1000		X

<sup>†</sup> Dynamic 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 Table 1:

Denmark

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

*I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.*

France

For 2,4 GHz, the output power is restricted to 10 mW eirp when the product is used outdoors in the band 2454 - 2483,5 MHz. There are no restrictions when used in other parts of the 2,4 GHz band. Check <http://www.arcep.fr/> for more details.

*Pour la bande 2,4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483,5 MHz. Il n'y a pas de restrictions pour des utilisations dans d'autres parties de la bande 2,4 GHz. Consultez <http://www.arcep.fr/> pour de plus amples détails.*

Table 2: Applicable Power Levels in France

Location	Frequency Range (MHz)	Power (EIRP)
Indoor (No restrictions)	2400-2483.5	100 mW (20 dBm)
Outdoor	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

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.

*Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2,4 GHz richiede una "Autorizzazione Generale". Consultare <http://www.comunicazioni.it/it/> per maggiori dettagli.*



## 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.

*2,4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas.  
Vairāk informācijas: <http://www.esd.lv>.*

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.

## Power Output of Your Device

To comply with your country's regulations, you may have to change the power output of your wireless device. Proceed to the appropriate section for your device.

**NOTE:** The power output setting may not be available on all wireless products. For more information, refer to the documentation on your product's CD.

### Wireless Adapters

For wireless adapters operating in the 2,4-GHz band, the typical radiated output power is 18 dBm EIRP, while the maximum radiated output power will not exceed 20 dBm (100 mW) EIRP. For wireless adapters operating in the 5-GHz band, the typical radiated output power is 20 dBm EIRP, while the maximum radiated output power will not exceed 23 dBm (200 mW) EIRP. If you need to alter your wireless adapter's power output, follow the appropriate instructions for your computer's operating system:

#### Windows XP

1. Double-click the **Wireless** icon in your desktop's system tray.
2. Open the *Wireless Network Connection* window.
3. Click the **Properties** button.
4. Select the **General** tab, and click the **Configure** button.
5. In the *Properties* window, click the **Advanced** tab.
6. Select **Power Output**.
7. From the pull-down menu on the right, select the adapter's power output percentage.

#### Windows 2000

1. Open the **Control Panel**.
2. Double-click **Network and Dial-Up Connections**.
3. Select your current wireless connection, and select **Properties**.
4. From the Properties screen, click the **Configure** button.
5. Click the **Advanced** tab, and select **Power Output**.
6. From the pull-down menu on the right, select the adapter's power setting.

If your computer is running Windows Millennium or 98, then refer to Windows Help for instructions on how to access the advanced settings of a network adapter.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

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

**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.

**Ceština/Czech**

**Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie**

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



**Dansk/Danish****Miljøinformation for kunder i EU**

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

**Deutsch/German****Umweltinformation für Kunden innerhalb der Europäischen Union**

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltsmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

**Eesti/Estonian****Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele**

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootet või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

**Español/Spanish****Información medioambiental para clientes de la Unión Europea**

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

**Ελληνικά/Greek****Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης**

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός, ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινотικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

**Français/French****Informations environnementales pour les clients de l'Union européenne**

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

**Italiano/Italian****Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea**

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

**Latviešu valoda/Latvian****Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā**

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķīrotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājāsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskās un elektroniskās ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmestā atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojušu aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

**Lietuvškai/Lithuanian****Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams**

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdurbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

**Malti/Maltese****Informazzjoni Ambjentali għal Kliġenti fl-Unjoni Ewropea**

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart municipli li ma għex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir iehor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' għbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riciklaġġ jghin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-hanut minn fejn xtrajt il-prodott.

**Magyar/Hungarian****Környezetvédelmi információ az európai 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 szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőrendszeren keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

**Nederlands/Dutch****Milieu-informatie voor klanten in de Europese Unie**

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

**Norsk/Norwegian****Miljøinformasjon for kunder i EU**

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

**Polski/Polish****Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska**

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwie 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 i jego recykling pomogą 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 miasta lub sklepu, w którym produkt został nabyty.

**Português/Portuguese****Informação ambiental para clientes da União Europeia**

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

**Slovenčina/Slovak****Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii**

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

**Slovenčina/Slovene****Okoljske informacije za stranke v Evropski uniji**

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

## **Suomi/Finnish**

### **Ympäristöä koskevia tietoja EU-alueen asiakkaille**

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

## **Svenska/Swedish**

### **Miljöinformation för kunder i Europeiska unionen**

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshantering eller butiken där du köpte produkten.

# Appendix J: Contact Information

For technical support contact your mobile service provider.



