



2.4GHz
802.11g

Wireless-G



Media Storage Link Router
with SpeedBooster

User Guide

Model No. **WRTSL54GS**



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 © 2005 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

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

How to Use This User Guide

This User Guide has been designed to make understanding networking with the Wireless-G Media Storage Link Router with SpeedBooster 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 Router.



This exclamation point means there is a caution or warning and is something that could damage your property or the Router.



This question mark provides you with a reminder about something you might need to do while using the Router.

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 Media Storage Link Router	6
The Back Panel	6
The Front Panel	7
Chapter 4: Connecting the Wireless-G Media Storage Link Router	8
Instructions for Connecting the Router	8
Placement Options	10
Chapter 5: Configuring the Wireless-G Media Storage Link Router	12
Overview	12
The Setup Tab - Basic Setup	13
The Setup Tab - DDNS	18
The Setup Tab - MAC Address Clone	19
The Setup Tab - Advanced Routing	20
The Wireless Tab - Basic Wireless Settings	22
The Wireless Tab - Wireless Security	24
The Wireless Tab - Wireless MAC Filter	27
The Wireless Tab - Advanced Wireless Settings	28
The Security Tab - Firewall	30
The Security Tab - VPN Passthrough	31
The Storage Tab - Disk	32
The Storage Tab - Share	33
The Storage Tab - Administration	34
The Storage Tab - Media Server	36
The Access Restrictions Tab - Internet Access	37
The Applications and Gaming Tab - Port Range Forward	39
The Applications & Gaming Tab - Port Triggering	40

The Applications and Gaming Tab - DMZ	41
The Applications and Gaming Tab - QoS	42
The Administration Tab - Management	44
The Administration Tab - Log	45
The Administration Tab - Diagnostics	46
The Administration Tab - Factory Defaults	47
The Administration Tab - Firmware Upgrade	47
The Administration Tab - Config Management	47
The Status Tab - Router	48
The Status Tab - Local Network	49
The Status Tab - Wireless	50
Appendix A: Troubleshooting	51
Common Problems and Solutions	51
Frequently Asked Questions	59
Appendix B: Wireless Security	67
Security Precautions	67
Security Threats Facing Wireless Networks	67
Appendix C: Upgrading Firmware	70
Appendix D: Windows Help	71
Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter	72
Windows 98SE or Me Instructions	72
Windows 2000 or XP Instructions	72
For the Router's Web-based Utility	73
Appendix F: Glossary	74
Appendix G: Specifications	79
Appendix H: Warranty Information	81
Appendix I: Regulatory Information	82
Appendix J: Contact Information	88

List of Figures

Figure 3-1: The Router's Back Panel	6
Figure 3-2: The Router's Front Panel	7
Figure 4-1: Connect the USB Disk	8
Figure 4-2: Connect the Broadband Modem	9
Figure 4-3: Connect Your Network Devices	9
Figure 4-4: Connect the Power	10
Figure 4-5: Stand in Closed Position	10
Figure 4-6: Wall-Mount Slots	11
Figure 5-1: Login Screen	12
Figure 5-2: Setup Tab - Basic Setup	13
Figure 5-3: DHCP Connection Type	13
Figure 5-4: Static IP Connection Type	13
Figure 5-5: PPPoE Connection Type	14
Figure 5-6: PPTP Connection Type	14
Figure 5-7: L2TP Connection Type	15
Figure 5-8: Telstra Cable Connection Type	15
Figure 5-9: Optional Settings	16
Figure 5-10: Router IP	16
Figure 5-11: Network Address Server Settings	16
Figure 5-12: Time Setting	17
Figure 5-13: Setup Tab - DDNS (DynDNS.org)	18
Figure 5-14: Setup Tab - DDNS (TZO.com)	18
Figure 5-15: Setup Tab - MAC Address Clone	19
Figure 5-16: Setup Tab - Advanced Routing (Gateway)	20
Figure 5-17: Setup Tab - Advanced Routing (Router)	20
Figure 5-18: Routing Table Entry List	21
Figure 5-19: Wireless Tab - Basic Wireless Settings	22
Figure 5-20: SecureEasySetup Ready Screen	23
Figure 5-21: Wireless Tab - Wireless Security (WPA Personal)	24
Figure 5-22: Wireless Tab - Wireless Security (WPA Enterprise)	24
Figure 5-23: Wireless Tab - Wireless Security (WPA2 Personal)	25

Figure 5-24: Wireless Tab - Wireless Security (WPA2 Enterprise)	25
Figure 5-25: Wireless Tab - Wireless Security (RADIUS)	26
Figure 5-26: Wireless Tab - Wireless Security (WEP)	26
Figure 5-27: Wireless Tab - Wireless MAC Filter	27
Figure 5-28: MAC Address Filter List	27
Figure 5-29: Wireless Tab - Advanced Wireless Settings	28
Figure 5-30: Security Tab - Firewall	30
Figure 5-31: Security Tab - VPN Passthrough	31
Figure 5-32: Storage Tab - Disk	32
Figure 5-33: Claim Disk	32
Figure 5-34: Storage Tab - Claimed Disk	32
Figure 5-35: Storage Tab - Share	33
Figure 5-36: Share Properties	33
Figure 5-37: Share Access	33
Figure 5-38: Storage Tab - Administration	34
Figure 5-39: User Properties	34
Figure 5-40: Modify - Group Properties	34
Figure 5-41: Create New Group - Group Properties	35
Figure 5-42: Storage Tab - Media Server	36
Figure 5-43: Partition List	36
Figure 5-44: Access Restrictions Tab - Internet Access	37
Figure 5-45: Internet Policy Summary	37
Figure 5-46: List of PCs	38
Figure 5-47: Port Services	38
Figure 5-48: Applications and Gaming Tab - Port Range Forward	39
Figure 5-49: Applications and Gaming Tab - Port Triggering	40
Figure 5-50: Applications and Gaming Tab - DMZ	41
Figure 5-51: Applications and Gaming Tab - QOS	42
Figure 5-52: Administration Tab - Management	44
Figure 5-53: Administration Tab - Log	45
Figure 5-54: Incoming Log Table	45
Figure 5-55: Outgoing Log Table	45
Figure 5-56: Administration Tab - Diagnostics	46
Figure 5-57: The Ping Test	46

Figure 5-58: The Traceroute Test	46
Figure 5-59: Administration Tab - Factory Defaults	47
Figure 5-60: Administration Tab - Firmware Upgrade	47
Figure 5-61: Administration Tab - Config Management	47
Figure 5-62: Status Tab - Router	48
Figure 5-63: Status Tab - Local Network	49
Figure 5-64: DHCP Clients Table	49
Figure 5-65: Status Tab - Wireless	50
Figure C-1: Upgrade Firmware	70
Figure E-1: IP Configuration Screen	72
Figure E-2: MAC Address/Adapter Address	72
Figure E-3: MAC Address/Physical Address	72
Figure E-4: MAC Address Filter List	73
Figure E-5: MAC Address Clone	73

Chapter 1: Introduction

Welcome

Thank you for choosing the Linksys Wireless-G Media Storage Link Router with SpeedBooster. The Router will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely.

How does the Router do all of this? A router is a device that allows access to an Internet connection over a network. With the Router, this access can be shared over the four switched ports or via the wireless broadcast at up to 11Mbps for Wireless-B or up to 54Mbps for Wireless-G.

The Router also has a built-in media server, so it can stream music, video, and pictures from a USB hard disk to a Universal Plug-and-Play (UPnP)-compatible media adapter. You won't need a computer to manage the content; instead, let the Router can do that for you.

Use the WPA 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. The Router's SecureEasySetup™ feature makes it a snap to set up WPA when you have other SecureEasySetup devices—notebooks, printers, other peripherals—comprising your network. Run the Setup Wizard and it will guide you through the steps. You can also 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 Router 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 Router protects your networks from unauthorized 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.

Linksys recommends using the Setup CD-ROM for first-time installation of the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then use the instructions in this Guide to help you connect the Router, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Wireless-G Media Storage Link Router with SpeedBooster.

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G Media Storage Link Router with SpeedBooster.

- **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 Media Storage Link Router**
This chapter describes the physical features of the Router.
- **Chapter 4: Connecting the Wireless-G Media Storage Link Router**
This chapter instructs you on how to connect the Router to your network.
- **Chapter 5: Configuring the Wireless-G Media Storage Link Router**
This chapter explains how to use the Web-based Utility to configure the settings on the Router.
- **Appendix A: Troubleshooting**
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Router.
- **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 Media Storage Link Router with SpeedBooster, 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 Media Storage Link Router with SpeedBooster has been specifically designed for use with both your 802.11b and 802.11g products. The Router is compatible with all 802.11b and 802.11g adapters, such as the

Wireless-G Media Storage Link Router with SpeedBooster

Notebook Adapters for 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 Router's four Ethernet LAN ports. To add more ports, any of the Router's Ethernet 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 for more information about products that work with the Wireless-G Media Storage Link Router with SpeedBooster.

Chapter 3: Getting to Know the Wireless-G Media Storage Link Router

The Back Panel

The Router's ports, where the cables are connected, are located on the back panel.

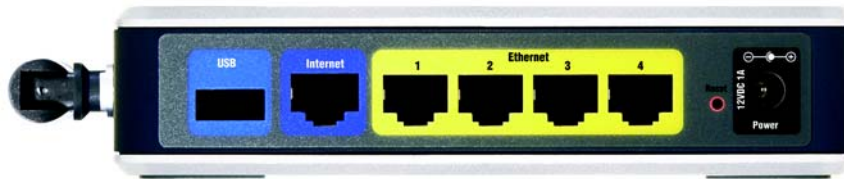


Figure 3-1: The Router's Back Panel

USB	The USB port is where you will connect a USB flash disk or hard drive. You can attach a disk containing media files, so you can stream music, video, or pictures to a media adapter without using a computer.
Internet	The Internet port is where you will connect your broadband Internet connection.
1, 2, 3, 4	These ports (1, 2, 3, 4) connect the Router to your networked PCs and other Ethernet network devices.
Reset Button	There are two ways to reset the Router's factory defaults. Either press the Reset Button , for approximately five seconds, or restore the defaults from the Administration tab - Factory Defaults in the Router's Web-based Utility.
Power	The Power port is where you will connect the power adapter.



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 Front Panel

The Router's SecureEasySetup button and LEDs are located on the front panel.



Figure 3-2: The Router's Front Panel

SecureEasySetup Orange/White. SecureEasySetup configures the Router with a wireless network name (also called an SSID) and wireless security settings using a method called WPA-Personal.

The Router's SecureEasySetup button lights up and will stay orange when the Router is powered on. The color orange indicates that the Router is not using SecureEasySetup, while the color white indicates that the Router is using SecureEasySetup. When the Router enters SecureEasySetup mode, the button will turn white and start flashing. After the Router has generated new wireless settings, the button will stop flashing and stay white.

To clear the SecureEasySetup settings, press and hold down the SecureEasySetup button for five seconds. The button will flash slowly as the Router resets its wireless settings to the factory defaults. The button will turn orange to indicate a successful reset.



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

Power	Green. The Power LED lights up and will stay on while the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, this LED will flash. When the diagnostic is complete, the LED will be solidly lit.
USB	Green. The USB LED lights up when a USB drive is connected through the USB port. If the LED is flashing, the Router is actively sending or receiving data over the USB connection.
DMZ	Green. The DMZ LED lights up and will stay on while the DMZ function is being used.
G	Green. The G 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 network.
1, 2, 3, 4	Green. These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port.
Internet	Green. The Internet LED lights up when there is a connection made through the Internet port.

Chapter 4: Connecting the Wireless-G Media Storage Link Router

Instructions for Connecting the Router

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. Fix the direction of the antenna. 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 USB cable to the Router's USB port. Then, connect the other end of the USB cable to the USB hard disk. (If you have a USB flash drive, you can connect it directly to the Router.)

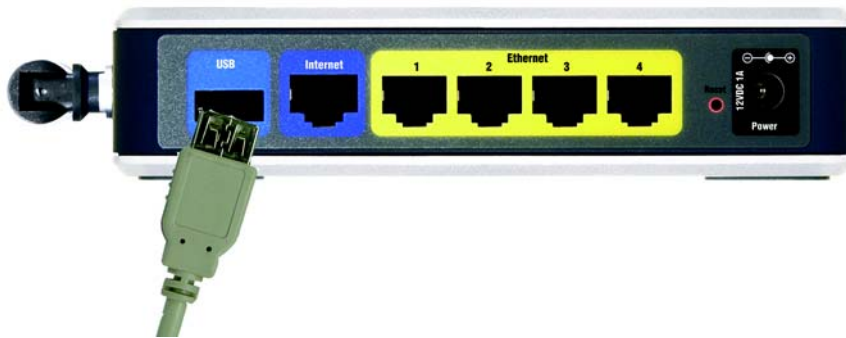


Figure 4-1: Connect the USB Disk

5. 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 modem.

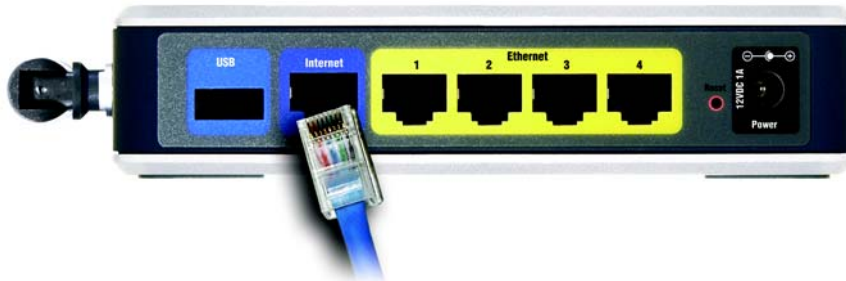


Figure 4-2: Connect the Broadband Modem

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

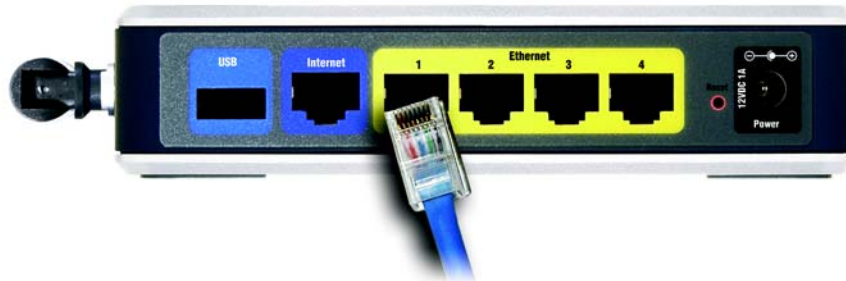


Figure 4-3: Connect Your Network Devices

7. Connect the AC power adapter to the Router's Power port and 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.

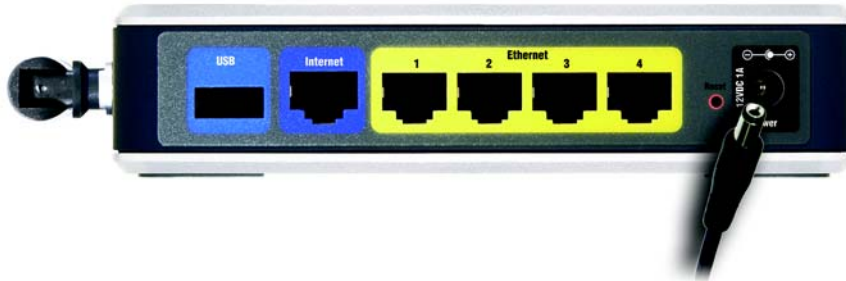


Figure 4-4: Connect the Power



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

Proceed to the following 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 (this uses its built-in stand). The third way is to mount it on a wall. The second and third options are explained in further detail below.

Stand Option

If you place the Gateway flat on a surface, then you can leave the stand in the closed position. However, if you want the Gateway to be upright, swivel the stand clockwise 90° and position the Gateway accordingly.

Now that the hardware installation is complete, proceed to “Chapter 5: Configuring the Wireless-G Media Storage Link Router,” for directions on how to configure the Router.



Figure 4-5: Stand in Closed Position

Wall-Mount Option

The Router has four wall-mount slots on its bottom panel. The distance between two adjacent slots is 2.36 inches (60 mm).

Before you begin, make sure you have two screws that are size #4—this indicates a diameter measurement of 0.112 inches (2.845 mm).

1. Determine where you want to mount the Router.

Wireless-G Media Storage Link Router with SpeedBooster

2. Drill two holes into the wall. Make sure adjacent holes are 2.36 inches (60 mm) apart.
3. Insert a screw into each hole, and leave 0.2 inches (5 mm) of its head exposed.
4. Maneuver the Router so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.

Now that the hardware installation is complete, proceed to “Chapter 5: Configuring the Wireless-G Media Storage Link Router,” for directions on how to configure the Router.



Figure 4-6: Wall-Mount Slots

Chapter 5: Configuring the Wireless-G Media Storage Link Router

Overview

Linksys recommends using the Setup CD-ROM for first-time installation of the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then you can use the Web-based Utility to configure the Router. For advanced users, you may configure the Router's advanced settings through the Web-based Utility.

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 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 eight main tabs: Setup, Wireless, Security, Storage, 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 login screen will appear. (Non-Windows XP users will see a similar screen.) Leave the *User Name* field blank. The first time you open the Web-based Utility, use the default password **admin**. (You can set a new password from the Administration tab's *Management* screen.) Then click the **OK** button.



NOTE: For first-time installation, Linksys recommends using the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the Web-based Utility.



HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix D: Windows Help" for more information on TCP/IP.



Figure 5-1: Login Screen

The Setup Tab - Basic Setup

The first screen that appears displays the Setup tab. This allows you to change the Router's general settings. After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

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.
- **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.

Static DNS 1-3. Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Figure 5-2: Setup Tab - Basic Setup

Figure 5-3: DHCP Connection Type

Figure 5-4: Static IP Connection Type

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

- **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.

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

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

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

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

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

The screenshot shows the 'Internet Connection Type' configuration window. The 'Internet Connection Type' dropdown is set to 'PPPoE'. Below it, there are input fields for 'User Name' and 'Password'. At the bottom, there are two radio buttons: 'Connect on Demand : Max Idle Time' (selected) with a value of '5' Min., and 'Keep Alive : Redial Period' with a value of '30' Sec.

Figure 5-5: PPPoE Connection Type

The screenshot shows the 'Internet Connection Type' configuration window. The 'Internet Connection Type' dropdown is set to 'PPTP'. Below it, there are input fields for 'Internet IP Address' (0.0.0.0), 'Subnet Mask' (0.0.0.0), and 'Gateway' (0.0.0.0). There are also input fields for 'User Name' and 'Password'. At the bottom, there are two radio buttons: 'Connect on Demand : Max Idle Time' (selected) with a value of '5' Min., and 'Keep Alive : Redial Period' with a value of '30' Sec.

Figure 5-6: PPTP Connection Type

- **L2TP.** If you are using an L2TP (Layer 2 Tunneling Protocol) connection, then select **L2TP**.

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

L2TP Server. Enter the IP address of the L2TP server you are using; this should be 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.

- **Telstra Cable.** Telstra Cable is a service that applies to connections in Australia only. If your ISP uses Heart Beat Signal, then select **Telstra Cable**.

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

Heart Beat Server. Enter the IP address of the Heart Beat Server you are using; this should be 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.

The screenshot shows the 'Internet Connection Type' configuration page. On the left is a grey box labeled 'Internet Connection Type'. On the right, the 'L2TP' option is selected in a dropdown menu. Below this are fields for 'User Name' and 'Password'. The 'L2TP Server' field is set to '0.0.0.0'. There are two radio buttons: 'Connect on Demand : Max Idle Time' (selected) with a value of '5' Min., and 'Keep Alive : Redial Period' with a value of '30' Sec.

Figure 5-7: L2TP Connection Type

The screenshot shows the 'Internet Connection Type' configuration page. On the left is a grey box labeled 'Internet Connection Type'. On the right, the 'Telstra Cable' option is selected in a dropdown menu. Below this are fields for 'User Name', 'Password', and 'Heart Beat Server'. There are two radio buttons: 'Connect on Demand : Max Idle Time' (selected) with a value of '5' Min., and 'Keep Alive : Redial Period' with a value of '30' Sec.

Figure 5-8: Telstra Cable Connection Type

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

Network Address Server Settings (DHCP)

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, 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**.

Figure 5-9: Optional Settings

Figure 5-10: Router IP

Figure 5-11: Network Address Server Settings

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

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

Static DNS (1-3). The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, 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. (You can even automatically adjust for daylight savings time.)

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

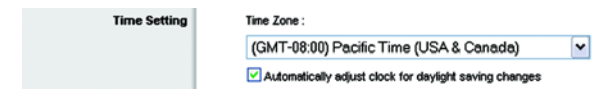


Figure 5-12: Time Setting

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 or www.TZO.com.

DDNS

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

DynDNS.org

User Name. Enter the User Name for your DDNS account

Password. Enter the Password for your DDNS account.

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

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

Status. This displays the status of the DDNS connection.

TZO.com

E-mail Address. Enter the E-mail Address for your DDNS account

Password. Enter the Password for your DDNS account.

Domain Name. Enter the Domain Name for your 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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.



Figure 5-13: Setup Tab - DDNS (DynDNS.org)



Figure 5-14: Setup Tab - DDNS (TZO.com)

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.



Figure 5-15: 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

This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination.

RIP. 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

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.



Figure 5-16: Setup Tab - Advanced Routing (Gateway)

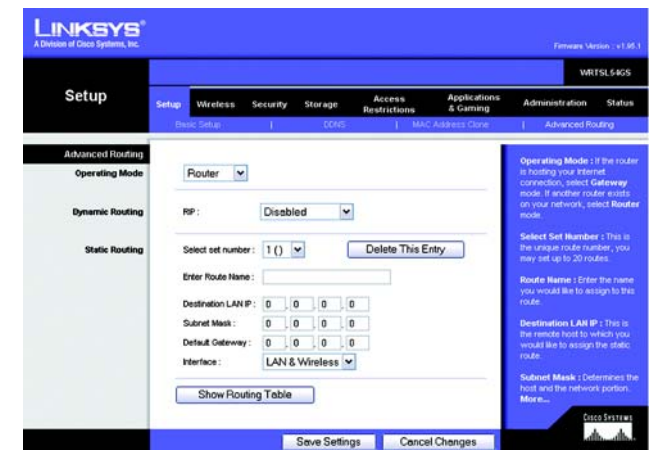


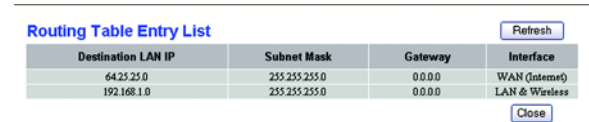
Figure 5-17: Setup Tab - Advanced Routing (Router)

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

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

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.



Destination LAN IP	Subnet Mask	Gateway	Interface
64.25.25.0	255.255.255.0	0.0.0.0	WAN (Internet)
192.168.1.0	255.255.255.0	0.0.0.0	LAN & Wireless

Figure 5-18: Routing Table Entry List

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**.

SecureEasySetup Button. The status of the Router's SecureEasySetup feature is displayed here. If you want to use the Router's SecureEasySetup feature, click the **SecureEasySetup** button.



NOTE: SecureEasySetup uses WPA Personal encryption. If your current wireless devices do not support WPA Personal security, then you cannot use SecureEasySetup on your network. You will need to manually configure your network security using the encryption supported by your existing devices.

You will be asked to press the SecureEasySetup button (hardware or software) on your wireless client (computer or other network device) within two minutes to complete the SecureEasySetup process. Click the **OK** button to continue.



Figure 5-19: Wireless Tab - Basic Wireless Settings

A new screen will be displayed while the Router is waiting for you to push the SecureEasySetup button on your wireless client.



NOTE: You can only add one SecureEasySetup device at a time. For additional devices, click the **SecureEasySetup** button on the *Basic Wireless Settings* screen and repeat the process.

When the SecureEasySetup process is complete, the *Basic Wireless Settings* screen will appear, and the Status information will be updated. The Router is now configured with a new wireless network name (SSID) and wireless security settings (WPA-Personal).

Reset Security. If you already set up the network using the Router's SecureEasySetup feature and you want to replace the current settings with the Router's factory defaults, click the **Reset Security** button. A new screen will appear. You will be asked to confirm that you want to reset the wireless security settings. Click the **OK** button to continue.

The Router will be reset to its factory default wireless settings (the SSID is **linksys**, and wireless security is disabled). To configure your wireless network using SecureEasySetup, return to the previous page of this User Guide and follow the instructions for the SecureEasySetup button.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

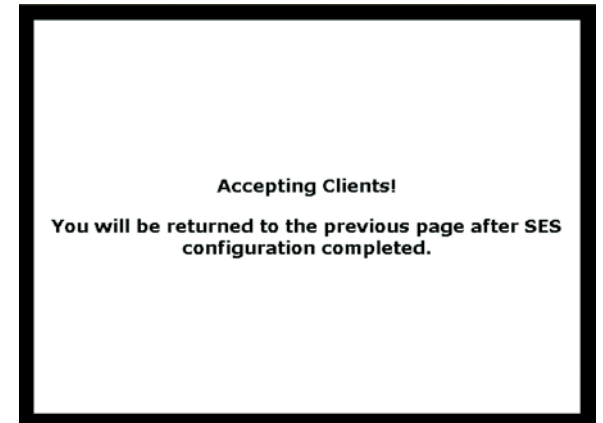


Figure 5-20: SecureEasySetup Ready Screen

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, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, and WEP. (WEP stands for Wired Equivalent Privacy, WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WPA2 is stronger than WPA. WPA Enterprise is WPA used in coordination with a RADIUS server. RADIUS stands for Remote Authentication Dial-In User Service.) These are briefly discussed here. For detailed instructions on configuring wireless security for the Router, turn to “Appendix B: Wireless Security.”

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes. For detailed instructions on configuring wireless security for the Router, turn to “Appendix B: Wireless Security.”

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes. For detailed instructions on configuring wireless security for the Router, turn to “Appendix B: Wireless Security.”



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

encryption: encoding data transmitted in a network.

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.



Figure 5-21: Wireless Tab - Wireless Security (WPA Personal)



Figure 5-22: Wireless Tab - Wireless Security (WPA Enterprise)

WPA2 Personal. WPA2 gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **AES**, or **TKIP + 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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes. For detailed instructions on configuring wireless security for the Router, turn to “Appendix B: Wireless Security.”



Figure 5-23: Wireless Tab - Wireless Security (WPA2 Personal)

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.) First, select the type of WPA algorithm you want to use, **AES**, or **TKIP + 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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes. For detailed instructions on configuring wireless security for the Router, turn to “Appendix B: Wireless Security.”



Figure 5-24: Wireless Tab - Wireless Security (WPA2 Enterprise)

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."



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

radius (remote authentication dial-in user service): a protocol that uses an authentication server to control network access.

wep (wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.

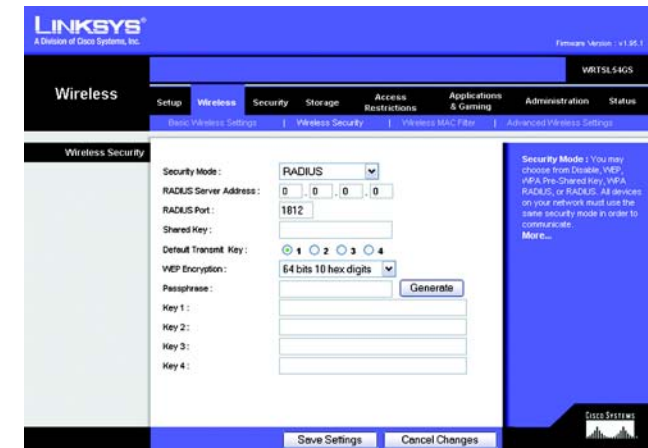


Figure 5-25: Wireless Tab - Wireless Security (RADIUS)



Figure 5-26: Wireless Tab - Wireless Security (WEP)

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes. For detailed instructions on configuring wireless security for the Router, turn to "Appendix B: Wireless Security."

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.



Figure 5-27: Wireless Tab - Wireless MAC Filter

Figure 5-28: 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 5-29: 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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

The Security Tab - Firewall

Use this screen to enable or disable the Router's firewall and various filters.

Firewall

Firewall Protection. This feature employs Stateful Packet Inspection (SPI) for a more detailed review of data packets entering your network environment. This feature is enabled by default. Select **Disabled** to disable this feature.

Block WAN Requests

Block Anonymous Requests. Check the box to enable this feature, so you can protect your network from being “pinged,” or detected, by other Internet users. This also reinforces your network security by hiding your network ports. Both functions of the Block Anonymous Requests feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Uncheck the box 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. Check the box to filter multicasting, or uncheck the box to disable this feature.

Filter Internet NAT Redirection. This feature uses port forwarding to block access to local servers from local networked computers. Check the box to filter Internet NAT redirection, or uncheck the box to disable this feature.

Filter IDENT (Port 113). This feature keeps port 113 from being scanned by devices outside of your local network. Check the box to filter port 113, or uncheck the box to disable this feature.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.



Figure 5-30: Security Tab - Firewall

The Security Tab - VPN Passthrough

Use the settings on this tab 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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.



Figure 5-31: Security Tab - VPN Passthrough

The Storage Tab - Disk

You can attach a USB flash drive or hard disk to the Router. The *Disk* screen describes the disk currently attached to the Router. Using this screen, you can format a blank disk, safely remove a disk, or erase a disk.

Disk Management

Disk Detail

If a blank disk is attached to the Router, the Disk, Make and Model, and Physical Size columns describe the disk.

Claim. For a blank disk, click the **Claim** button to create a partition that will be formatted as FAT32. On the *Claim Disk* screen, enter a name for the partition. Click the **Claim** button to save the new name, or click the **Clear** button to clear the *New Partition Name* field. Click the **Cancel** button to cancel the changes.

Safely Remove. Before physically disconnecting a disk from the Router, click the **Safely Remove** button first. This ensures that the disk is not removed while data is being transferred to or from the disk; otherwise, data may be lost.

If a formatted disk is attached to the Router, the Partition, File System, Total Space, and Free Space columns describe the partition(s) of the disk.

Create Share. Shares control access to the partition(s) of the disk. To create shares, click the **Create Share** button. Proceed to the next page for descriptions of the *Share* screen.

Erase Disk

To erase a disk, click the checkbox next to the name of the disk.

Quick Erase. To quickly free up space on the disk, click the **Quick Erase** button to remove the table of contents from the disk. (This is less secure than the Full Erase option.)

Full Erase. Click the **Full Erase** button to initiate complete removal of data from the disk. Once the removal is complete, the data cannot be recovered. The Full Erase option is recommended if the disk holds sensitive data.

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



Figure 5-32: Storage Tab - Disk



Figure 5-33: Claim Disk

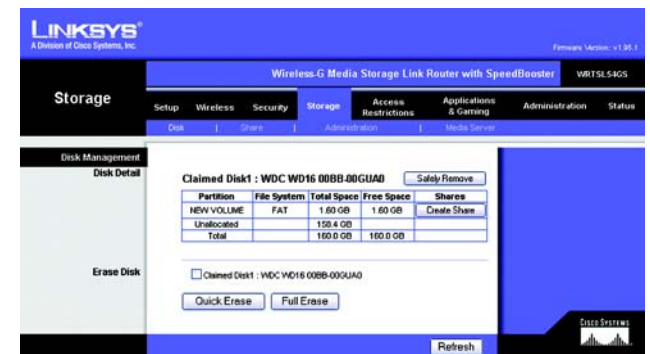


Figure 5-34: Storage Tab - Claimed Disk

The Storage Tab - Share

Shares control access to the partition(s) of the disk attached to the Router. The *Share* screen describes the current shares. Using this screen, you can create new shares, modify share properties, or delete shares.

Share Management

Shares

The Share Name, Partition, and Total Space columns describe the shares.

Properties - Modify. Click the **Modify** button to change the properties of a share. On the *Share Properties* screen, enter a different name for the share, and/or select a different partition from the *Resides in Partition* drop-down menu. Click the **Create Share** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

Share Access - Modify. Click the **Modify** button to change the access privileges of a share. On the *Share Access* screen, groups with no access are listed in the Other Group column, and groups with access are listed in the Group with Access column. To give a group read-only access, select the group, and click the **>> Read Only** button. To give a group read/write access, select the group, and click the **>> Read/Write** button. To strip a group of its current access privileges, select the group, and click the **<< Remove** button. Click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to exit the *Share Access* screen.

Delete. Click the **Delete** button to remove a share.

Create Share

Create New Share. Click the **Create New Share** button to create a new share. On the *Share Properties* screen, enter a name for the share, and select a partition from the *Resides in Partition* drop-down menu. Click the **Create Share** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.



Figure 5-35: Storage Tab - Share



Figure 5-36: Share Properties



Figure 5-37: Share Access

The Storage Tab - Administration

The *Administration* screen allows you to manage the users and groups of users that can access the shares.

Basic

Machine Name. Enter a name for the Router. Punctuation and other special characters (e.g., * / | \) cannot be used in the name.

Workgroup Name. Enter the Workgroup Name of your networked computers.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

User Management

The users are listed in the User Management table. There are two default users, admin (read/write access) and guest (read-only access); these cannot be deleted.

Properties - Modify. Click the **Modify** button to change the properties of a user. On the *User Properties* screen, enter a different name for the user, change the password, and/or select a different group from the *Group* drop-down menu. Click the **Create User** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

Delete. Click the **Delete** button to remove a user.

Create New User. Click the **Create New User** button to create a new user. On the *User Properties* screen, enter a name for the user. Then enter a password and enter it again in the *Re-enter to confirm* field. Select a group from the *Group* drop-down menu. Click the **Create User** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

Group Management

The groups are listed in the Group Management table. There are two default groups, admin and guest; these cannot be deleted.

Properties - Modify. Click the **Modify** button to change the user membership of a group. On the *Group Properties* screen, users who are not members are listed in the Other Users column, and users who are members are listed in the Users in Group column. To add a user to the group, select the user, and click the **>> Join Group** button. To remove a user from the group, select the user, and click the **<< Remove** button. Click the **Save**

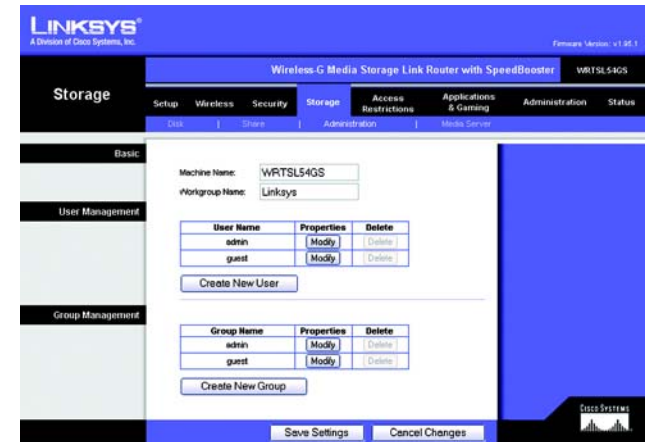


Figure 5-38: Storage Tab - Administration



Figure 5-39: User Properties

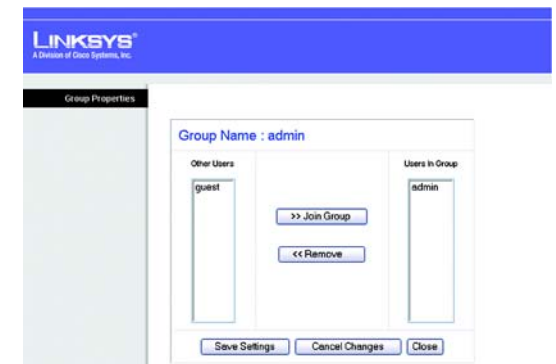


Figure 5-40: Modify - Group Properties

Settings button to save the changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to exit the *Group Properties* screen.

Delete. Click the **Delete** button to remove a user.

Create New Group. Click the **Create New Group** button to create a new group. On the *Group Properties* screen, enter a name for the group. Click the **Create Group** button to save the new name, or click the **Clear** button to clear the change. Click the **Cancel** button to cancel the change.



Figure 5-41: Create New Group - Group Properties

The Storage Tab - Media Server

The Router has a built-in media server, so it can stream music, pictures, or video from the USB hard disk to a UPnP-compatible media adapter. The *Media Server* screen lets you select shares to scan for content.

UPnP Media Server

Setup

Server Name. The name of the Router is displayed here.

UPnP Media Server. To use the Router's media server function, select **Enable**. Otherwise, select **Disable**.

Database

Select content to add to the database of the Router's media server.

Scan All Partitions. Click this button to scan all partitions of the USB hard disk for content.

Select Partitions to Scan. Click this button to select specific partitions to scan for content.

The Partition and Folder columns describe the partitions of the USB hard disk.

Scan. Click the **Scan** button to scan a specific partition for content. The *Partition List* screen will appear. Click the **Select** button to select a partition for scanning. Click the **Up List** button to move up one level in the file structure. Click the **Refresh** button to update the on-screen information. Click the **Close** button to exit the *Partition List* screen.

Delete. Click the **Delete** button to delete a specific partition from the Router's database.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.



Figure 5-42: Storage Tab - Media Server



Figure 5-43: Partition List

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 a policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, click the radio button beside *Enable*.
3. Enter a Policy Name in the field provided.

LINKSYS
A Division of Cisco Systems, Inc.

Access Restrictions

Internet Access Policy: 1 () [Delete] [Summary]

Status: ☐ Enable ☒ Disable

Enter Policy Name: []

PCs: [Edit List of PCs]

☐ Deny ☒ Allow

Internet access during selected days and hours.

Days: ☒ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Times: ☒ 24 Hours ☐ From: 12 :00 :00 AM To: 12 :00 :00 AM

Blocked Services: [None] - [] [Add/Edit Service]

Website Blocking by URL Address: [] []

Website Blocking by Keyword: [] [] [] []

Internet Access Policy: You may define up to 10 access policies. Click **Delete** to delete a policy or **Summary** to see a summary of the policy.

Status: Enable or disable a policy.

Policy Name: You may assign a name to your policy.

Policy Type: Choose from Internet Access or Inbound Traffic. More...

Days: Choose the day of the week you would like your policy to be applied.

Times: Enter the time of the day you would like your policy to apply.

Blocked Services: You may choose to block access to certain services. Click **Add/Edit** Services to modify these settings.

Website Blocking by URL: You can block access to certain websites by entering their URL.

Website Blocking by Keyword: You can block access to certain websites by the keywords contained in their webpage.

[Save Settings] [Cancel Changes]

Figure 5-44: Access Restrictions Tab - Internet Access

Internet Policy Summary

No.	Policy Name	Days	Time of Day	Delete
1.	---	SMTWTFSS	---	☐
2.	---	SMTWTFSS	---	☐
3.	---	SMTWTFSS	---	☐
4.	---	SMTWTFSS	---	☐
5.	---	SMTWTFSS	---	☐
6.	---	SMTWTFSS	---	☐
7.	---	SMTWTFSS	---	☐
8.	---	SMTWTFSS	---	☐
9.	---	SMTWTFSS	---	☐
10.	---	SMTWTFSS	---	☐

[Close]

Figure 5-45: Internet Policy Summary

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*. (You can block up to 20 services.) Then enter the range of ports you want to filter.

If the service you want to block is not listed or you want to edit a service's settings, then click 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. Change its name, protocol setting, or port range. 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.

List of PCs

Enter MAC Address of the PCs in this format : xxxxxxxxxx

MAC 01 : 00:00:00:00:00:00	MAC 05 : 00:00:00:00:00:00
MAC 02 : 00:00:00:00:00:00	MAC 06 : 00:00:00:00:00:00
MAC 03 : 00:00:00:00:00:00	MAC 07 : 00:00:00:00:00:00
MAC 04 : 00:00:00:00:00:00	MAC 08 : 00:00:00:00:00:00

Enter the IP Address of the PCs

IP 01 : 192.168.1.0	IP 04 : 192.168.1.0
IP 02 : 192.168.1.0	IP 05 : 192.168.1.0
IP 03 : 192.168.1.0	IP 06 : 192.168.1.0

Enter the IP Range of the PCs

IP Range 01 : 192.168.1.0 ~ 0 IP Range 02 : 192.168.1.0 ~ 0

Save Settings **Cancel Changes**

Figure 5-46: List of PCs

Port Services

Service Name:

Protocol:

Port Range: -

Add **Modify** **Delete**

Apply **Cancel** **Close**

DNS [53 ~ 53]
 Ping [0 ~ 0]
 HTTP [80 ~ 80]
 HTTPS [443 ~ 443]
 FTP [21 ~ 21]
 POP3 [110 ~ 110]
 IMAP [143 ~ 143]
 SMTP [25 ~ 25]
 NNTP [119 ~ 119]
 Telnet [23 ~ 23]
 SNMP [161 ~ 161]
 TFTP [69 ~ 69]

Figure 5-47: 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.

Port Range

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

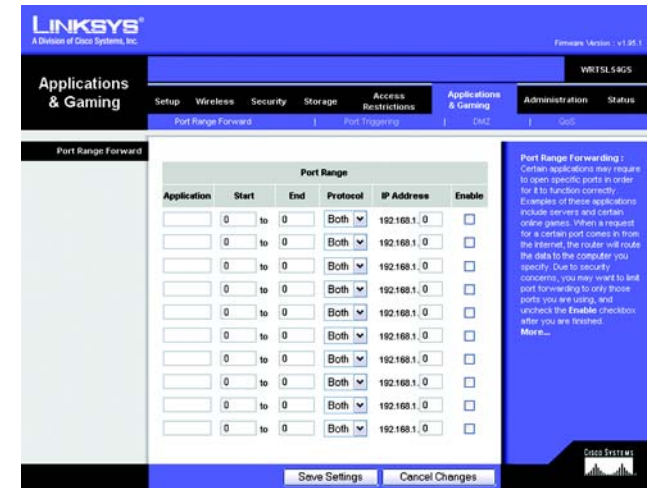


Figure 5-48: Applications and Gaming Tab - Port Range Forward

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

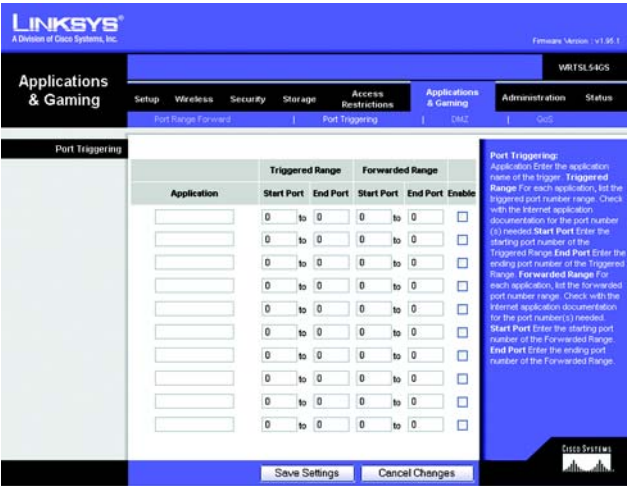


Figure 5-49: Applications and Gaming Tab - Port Triggering

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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.



Figure 5-50: 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. Enter the name of your network device in the *Device name* field.

Priority. Select its priority level from the drop-down menu.

MAC Address. Enter its MAC Address in the fields provided.

Ethernet Port Priority

Ethernet Port Priority QoS allows you to prioritize performance for four of the Router's ports, LAN Ports 1-4. (Ethernet Port Priority QoS does not require support from your ISP because the prioritized ports are LAN ports going out to your network.)

Priority. For each port, select its priority level from the drop-down menu.

Flow Control. If you want the Router to control the transmission of data between network devices, select **Enable**. To disable this feature, select **Disable**.

Application Port Priority

Application Port Priority QoS manages information as it is transmitted and received. Depending on the settings of the *QoS* screen, this feature will assign information a high or low priority for up to eight applications.

The screenshot shows the 'Applications & Gaming' tab with the 'QoS' sub-tab selected. The 'Wired QoS' section is active, showing 'Enable' selected for QoS. Under 'Upstream Bandwidth', 'Auto' is selected. The 'Device Priority' section has two entries, each with a 'Device name' field, a 'Priority' dropdown set to 'Low', and a 'MAC Address' field. The 'Ethernet Port Priority' section shows four ports, each with a 'Priority' dropdown set to 'Low' and a 'Flow Control' dropdown set to 'Enable'. The 'Application Priority' section has a table with 8 rows, each with an 'Application Name' field, a 'Priority' dropdown set to 'Low', and a 'Specific Port #' field. The 'Wireless QoS' section at the bottom has 'WMM Support', 'No Acknowledgement', and 'APSD Support' all set to 'Disable'. A sidebar on the right provides detailed explanations for each section. The bottom of the page has 'Save Settings' and 'Cancel Changes' buttons.

Figure 5-51: Applications and Gaming Tab - QoS

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

Application Name. Enter the name of the application.

Priority. For each port, select its priority level from the drop-down menu.

Specific Port #. Enter the respective port number in the *Specific Port#* field.

Wireless QoS

The Router features Wi-Fi Multimedia (WMM™) Support. The No Acknowledgement and Automatic Power Save Delivery (APSD) Support features are available only when the WMM Support feature is enabled.

WMM Support. If you have other devices on your network that support WMM, 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**.

APSD Support. APSD (Automatic Power Save Delivery) is a feature that enhances the power-saving capabilities of wireless devices. If you have other devices on your network that support APSD, select **Enable** from the drop-down menu. Otherwise, keep the default, **Disable**.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button 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) - The communications protocol used to connect to servers on the World Wide Web. HTTPS - Uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**.

Wireless Access Web. If you are using your Wireless 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. To access the Router remotely, from outside the network, verify that **Enable** is selected.

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

Use https. 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.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

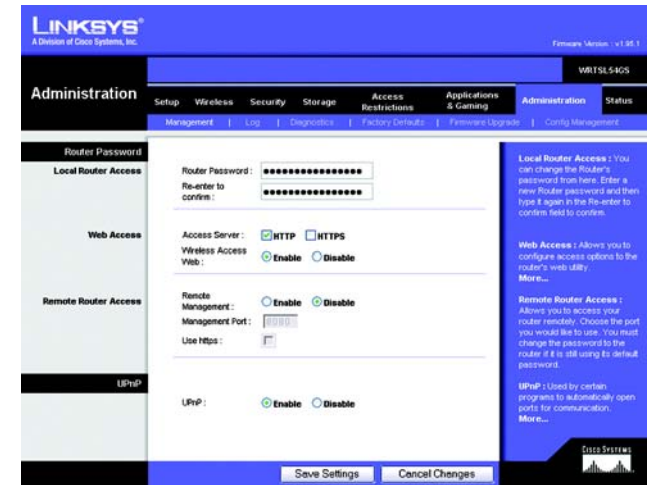


Figure 5-52: Administration Tab - Management

The Administration Tab - Log

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

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.

After you have made your change, click the **Save Settings** button to apply your change, or click the **Cancel Changes** button to cancel your change.



Figure 5-53: Administration Tab - Log



Figure 5-54: Incoming Log Table



Figure 5-55: Outgoing Log Table

The Administration Tab - Diagnostics

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

Ping Test

Ping Parameters

Ping. 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

Traceroute. To test the performance of a connect, 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 5-56: Administration Tab - Diagnostics



Figure 5-57: The Ping Test

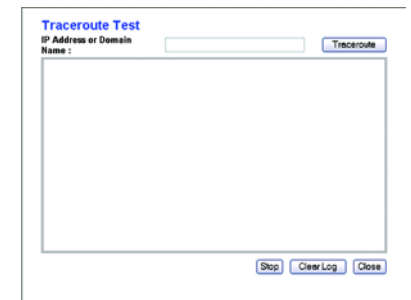


Figure 5-58: The Traceroute Test

The Administration Tab - Factory Defaults

You can reset the Router to its factory default settings using this screen.

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.

To cancel the reset to factory defaults, click the **Cancel Changes** button.

The Administration Tab - Firmware Upgrade

If you want to upgrade the Router's firmware, use this screen.

Upgrade Firmware

Please select a file to upgrade. Firmware can be upgraded by clicking the **Upgrade** button after browsing for the firmware, which you can download from the Linksys website. Do not upgrade your firmware unless you are experiencing problems with the Router. For more information about upgrading firmware, refer to "Appendix C: Upgrading Firmware".

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.

Restore 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 5-59: Administration Tab - Factory Defaults



Figure 5-60: Administration Tab - Firmware Upgrade

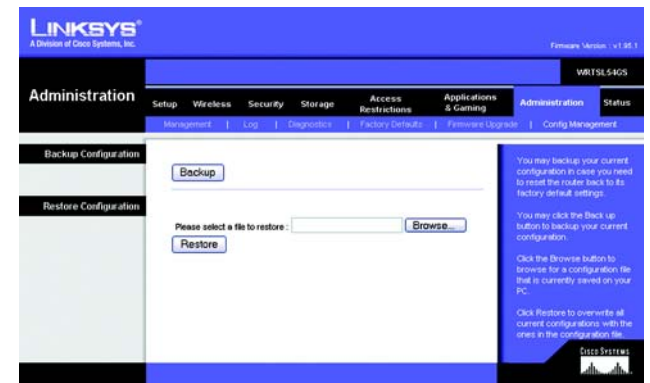


Figure 5-61: Administration Tab - Config Management

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 entered on the Setup Tab and required by your ISP for connection to the Internet. This status information may vary depending on the connection type you are using.

If the Login Type is Automatic Configuration - DHCP, you can click the **DHCP Release** button to release the Router's Internet IP address, and click the **DHCP Renew** button to renew the Router's Internet IP address. For dial-up type connections such as PPPoE, you can click the **Connect** to have the Router connect to the Internet, or click the **Disconnect** button to have the Router disconnect from the Internet.

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



Figure 5-62: 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 update the on-screen information.



Figure 5-63: Status Tab - Local Network



Figure 5-64: DHCP Clients Table

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 Security Tab, this will display what type of encryption the Router uses for security.

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



Figure 5-65: Status Tab - Wireless