

LINKSYS[®]
A Division of Cisco Systems, Inc.



2.4GHz
802.11g

Wireless-G

**Ethernet Bridge
with 5-Port Switch**

User Guide

WIRELESS

Model No. **WET54GS5**

CISCO SYSTEMS



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 © 2004 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

How to Use this Guide

Your guide to the Wireless-G Ethernet Bridge has been designed to make understanding networking with the Wireless-G Ethernet Bridge easier than ever. Look for the following items when reading this guide:



This checkmark means there is a Note of interest and is something you should pay special attention to while using the Wireless-G Ethernet Bridge.



This exclamation point means there is a Caution or warning and is something that could damage your property or the Wireless-G Ethernet Bridge.



This question mark provides you with a reminder about something you might need to do while using the Wireless-G Ethernet Bridge.

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 Guide?	2
Chapter 2: Planning Your Wireless Network	4
Network Topology	4
Network Layout	5
Chapter 3: Getting to Know the Wireless-G Ethernet Bridge with 5-Port Switch	6
The Back Panel	6
The Front Panel	7
The Side Panel	9
Chapter 4: Connecting the Wireless-G Ethernet Bridge for Setup	10
Chapter 5: Setting Up the Wireless-G Ethernet Bridge	12
Chapter 6: Connecting the Wireless-G Ethernet Bridge for Network Use	18
Connection to a Network Device	18
Wall Mount Placement Option	18
Chapter 7: Using the Wireless-G Ethernet Bridge	
Web-based Utility	19
Overview	19
Starting the Web-based Utility	19
Setup	20
Password	29
Wireless	30
Port Mirroring	38
Access List	39
Wireless Status	40
SNMP	41
Help	42
Appendix A: Troubleshooting	43
Common Problems and Solutions	43
Frequently Asked Questions	44
Appendix B: Wireless Security	47

Wireless-G Ethernet Bridge with 5-Port Switch

Security Precautions	47
Security Threats Facing Wireless Networks	47
Appendix C: Upgrading Firmware	50
Appendix D: Windows Help	51
Appendix E: Glossary	52
Appendix F: Specifications	59
Appendix G: Warranty Information	61
Appendix H: Regulatory Information	62
FCC Statement	62
Industry Canada (Canada)	62
Appendix I: Contact Information	63

List of Figures

Figure 2-1: Infrastructure Network	4
Figure 2-2: Ad-Hoc Network	5
Figure 2-3: Network Using Wireless Bridging	5
Figure 3-1: Back Panel	6
Figure 3-2: Front Panel	7
Figure 3-3: Side Panel	8
Figure 4-1: Connect to the Network	10
Figure 4-2: Connect the Power	11
Figure 5-1: Welcome	12
Figure 5-2: Connection	12
Figure 5-3: List of Bridges	13
Figure 5-4: Password	13
Figure 5-5: Mode Settings	14
Figure 5-6: Wireless Settings	15
Figure 5-7: IP Settings	15
Figure 5-8: Security Settings	16
Figure 5-9: Security Settings	16
Figure 5-10: Confirmation	17
Figure 5-11: Congratulations	17
Figure 6-1: Wall Placement	18
Figure 7-1: Password Screen	19
Figure 7-2: Setup Tab	20
Figure 7-3: 802.1x Screen	20
Figure 7-4: Site Survey	21
Figure 7-5: WEP	22
Figure 7-6: RADIUS-MD5	23
Figure 7-7: RADIUS-TLS	24
Figure 7-8: RADIUS-TTLS	25
Figure 7-9: WPA RADIUS-TLS	26

Wireless-G Ethernet Bridge with 5-Port Switch

Figure 7-10: WPA RADIUS-TTLS	27
Figure 7-11: WPA Pre-Shared Key	28
Figure 7-12: Log Table	28
Figure 7-13: Password Tab	29
Figure 7-14: Wireless Tab	30
Figure 7-15: Spanning Tree Protocol Tab	31
Figure 7-16: QOS Tab	32
Figure 7-17: Switch Table Tab	33
Figure 7-18: VLAN Tab	34
Figure 7-19: RMON Statistics Tab	36
Figure 7-20: Port Mirroring Tab	38
Figure 7-21: Access List Tab	39
Figure 7-22: Wireless Status Tab	40
Figure 7-23: SNMP Tab	41
Figure 7-24: Help Tab	42
Figure 7-25: Firmware Upgrade	42
Figure C-1: Firmware Upgrade	50

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G Ethernet Bridge with 5-port Switch. The Wireless-G Ethernet Bridge with 5-port Switch can make any wired Ethernet-equipped device a part of your wireless 802.11b or 802.11g network. At home, use the Bridge to connect game consoles or computers to your Wireless-G network and its shared high-speed Internet connection. In the office, convert your Ethernet-wired printer, camera, notebook or desktop into a wireless networked device.

The Wireless-G Ethernet Bridge with 5-port Switch can be used for connecting remote areas together. You can connect up to 5 Ethernet-equipped computers directly to the high-speed 10/100 switch ports on the Wireless-G Ethernet Bridge. Put another one (or a Wireless-G Access Point, or our one-port Wireless-G Ethernet Bridge) at the other end, and those 5 computers are connected to your main network.

And those 5 switch ports can support devices other than PCs. Since there are no drivers to load, you can make any wired-Ethernet device, such as a printer or network attached storage device, into a wireless network device. All five ports are auto-speed negotiating, and have automatic MDI/MDI-X crossover detection, so you don't have to worry about the cable type. To protect your data and privacy, all wireless transmissions can be secured with up to 128-bit WEP encryption, Pre-Shared Key, or RADIUS.

Use the instructions in this Guide to help you set up and connect the Wireless-G Ethernet Bridge with 5-port Switch. These instructions should be all you need to get the most out of the Wireless-G Ethernet Bridge with 5-port Switch.

802.11g: an IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

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

What's in this Guide?

This user guide covers the steps for setting up and using the Wireless-G Ethernet Bridge with 5-Port Switch.

- **Chapter 1: Introduction**
This chapter describes the Wireless-G Ethernet Bridge 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 Ethernet Bridge with 5-Port Switch**
This chapter describes the physical features of the Bridge.
- **Chapter 4: Connecting the Wireless-G Ethernet Bridge for Setup**
This chapter instructs you on how to connect the Bridge to your network for setup.
- **Chapter 5: Setting Up the Wireless-G Ethernet Bridge with 5-Port Switch**
This chapter explains how to set up the Bridge using the Setup Wizard.
- **Chapter 6: Connecting the Wireless-G Ethernet Bridge for Network Use**
This chapter explains how to connect the Bridge to a network device so the device can join your wireless network. It also describes placement options for the Bridge.
- **Chapter 7: Using the Wireless-G Ethernet Bridge Web-based Utility**
This chapter explains how to use the Web-based Utility so you can change the Bridge's settings or advanced configuration.
- **Appendix A: Troubleshooting**
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G Ethernet Bridge.
- **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 Bridge 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.

Wireless-G Ethernet Bridge with 5-Port Switch

- **Appendix E: Glossary**
This appendix gives a brief glossary of terms frequently used in networking.
- **Appendix F: Specifications**
This appendix provides the technical specifications for the Bridge.
- **Appendix G: Warranty Information**
This appendix supplies the warranty information for the Bridge.
- **Appendix H: Regulatory Information**
This appendix supplies the regulatory information regarding the Bridge.
- **Appendix I: 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.

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.

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 an access point, which serves as the main point of communications in a wireless network (see Figure 2-1). Access points transmit data to PCs equipped with wireless network cards, which can roam within a certain radial range of the access point. Multiple access points can be arranged to work in succession to extend the roaming range, and can be set up 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 an 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.

Figure 2-2 shows a typical scenario of four Wireless-G Ethernet Bridges in ad-hoc mode. Figure 2-3 shows a typical wireless bridging scenario using two Wireless-G Ethernet Bridges. Each wireless network is connected to a Wireless-G Ethernet Bridge through a switch. A separate notebook computer is equipped with a wireless network adapter and can communicate with either wireless network when it is configured with the appropriate SSID and channel.

LAN (Local Area Network): the computers and networking products that make up your local network.

SSID: your wireless network's name.

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

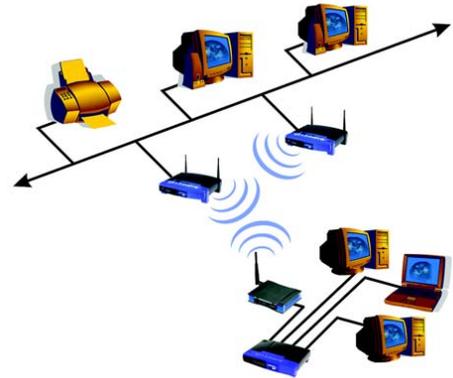


Figure 2-1: Infrastructure Network

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

Network Layout

The Wireless-G Ethernet Bridge is compatible with all 802.11b and 802.11g routers, such as model numbers BEFW11S4 and WRT54G, as well as access points, including model numbers WAP11 and WAP54G. The Bridge will also communicate with network adapters, such as the Wireless-B and Wireless-G Network Adapters (model numbers WPC11 and WPC54G) for your laptop computers, Wireless-B and Wireless-G PCI Adapters (model numbers WMP11 and WMP54G) for your desktop PCs, and Wireless-B and Wireless-G USB Adapters (model numbers WUSB11 and WUSB54G) for your computers when you want to enjoy USB connectivity.

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 Ethernet Bridge with 5-Port Switch.



Figure 2-2: Ad-Hoc Network



Figure 2-3: Network Using Wireless Bridging

Chapter 3: Getting to Know the Wireless-G Ethernet Bridge with 5-Port Switch

The Back Panel

All network connections to the Bridge are made through the ports on its back panel, shown in Figure 3-1. The reset button is also located here.

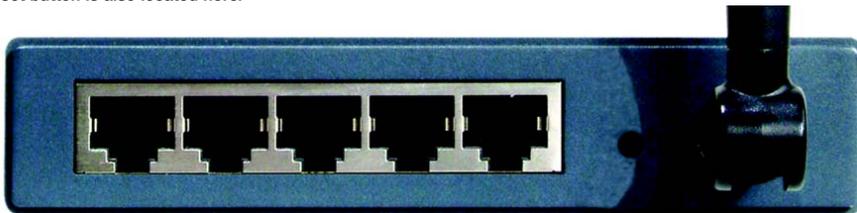


Figure 3-1: Back Panel



Important: If you reset the Wireless-G Ethernet Bridge, you will erase all of your settings (WEP encryption, wireless settings, etc.) and replace them with the factory defaults. Do not reset the Wireless-G Ethernet Bridge if you want to retain these settings.

- Reset** When pressed, the Reset button resets the Bridge to its factory default settings.
- LAN (1-5)** The LAN ports are where you will connect the Ethernet network cables.

The Front Panel

The LEDs indicate network activity experienced by the Bridge. (See Figure 3-2.)



Figure 3-2: Front Panel

- | | |
|------------------------|---|
| Power | Green. The Power LED will light up when the Bridge is powered on. While the Bridge is booting up and performing a self-test, the Power LED will flash. It will stop flashing and remain lit when the self-test has ended. |
| Diag | Green. The Ethernet LED will light up when there is an error with the Bridge. |
| Wireless-G LINK | Green. The Wireless-G LED will be lit steadily when the Bridge is connected to the wireless network. The LED will flash when there is wireless network traffic. |
| Wireless-G ACT | Green. The Wireless-G LED will be lit steadily when the Bridge is connected to the wireless network. The LED will flash when there is wireless network traffic. |
| LAN 1-5 | Green. The LAN LED will be lit steadily when the Bridge is connected to the wired network. The LED will flash when there is wired network traffic. |

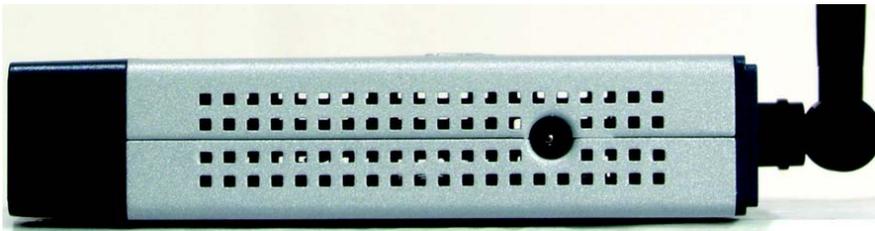


Figure 3-3: Side Panel



NOTE: If you use a Power over Ethernet (PoE) device to supply data and power through the Ethernet network cable, then you do not need to use the Power port.

The Side Panel

The Power port is on the side panel. (See Figure 3-3.)

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

Chapter 4: Connecting the Wireless-G Ethernet Bridge for Setup

1. Attach the Bridge's antenna.
2. Plug the included Ethernet network cable into one of the five LAN ports on the back panel of the Bridge, shown in Figure 4-1.

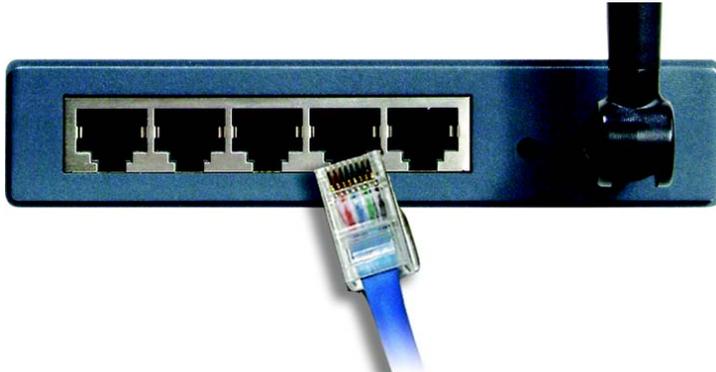


Figure 4-1: Connect to the Network

3. Plug the other end of the Ethernet network cable into the RJ-45 port of the hub, switch, or PC you wish to use to configure the Bridge.

Wireless-G Ethernet Bridge with 5-Port Switch

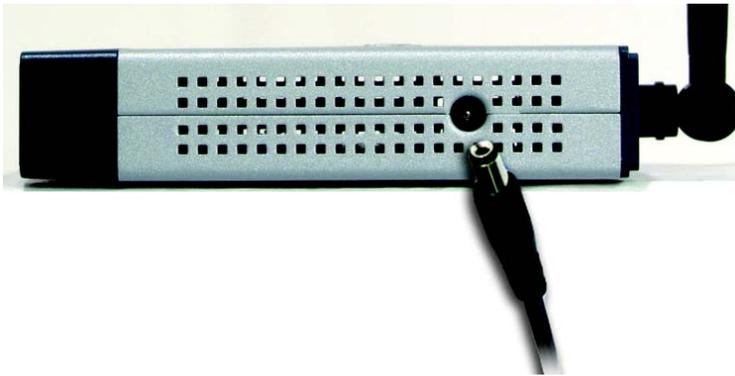


Figure 4-2: Connect the Power

4. Plug the supplied power cable into the Power port on the side panel of the Bridge, shown in Figure 4-2. Then plug the other end into an electrical outlet.

Proceed to “Chapter 5: Setting Up the Wireless-G Ethernet Bridge.”

Chapter 5: Setting Up the Wireless-G Ethernet Bridge

Now that you've connected the Wireless-G Ethernet Bridge to your wired network, you are ready to set it up. The Setup Wizard will guide you through all the necessary steps.

1. Insert the Setup CD-ROM into your PC's CD-ROM drive. The Setup Utility should run automatically, and the screen in Figure 5-1 should appear. If it does not, click the **Start** button and choose **Run**. In the field that appears, enter **D:\setup.exe** (if "D" is the letter of your CD-ROM drive).
 - Setup - Click the **Setup** button to proceed with the Setup Wizard.
 - User Guide - Click the **User Guide** button to open the PDF file of this User Guide.
 - LINKSYS Web - Click the **LINKSYS Web** button to access the Linksys website using an active Internet connection.
 - Exit - Click the **Exit** button to exit the Setup Wizard.
2. Click the **Setup** button to begin the setup process.
3. Make sure the Bridge is correctly connected to your wired network (see Figure 5-2). Then click the **Next** button.



Note: While the Wireless-G Ethernet Bridge has been designed to work correctly right out of the box, setting it up on a wireless computer will require you to use the Linksys default settings (SSID: linksys and mode: infrastructure). These settings can then be changed through the Bridge's Setup Wizard or Web-based Utility.



Figure 5-1: Welcome



Figure 5-2: Connection

Wireless-G Ethernet Bridge with 5-Port Switch

- The screen shown in Figure 5-3 displays a list of Wireless-G Ethernet Bridges on your network, along with the status information for each Bridge. (If you have only one Bridge on your network, it will be the only one displayed.) Select the Bridge you are currently installing by clicking its name in the *Selection* box. Write down the IP address of the Wireless-G Ethernet Bridge, so you can use it to access the Web-based Utility later. Then click the **Yes** button.



Figure 5-3: List of Bridges

- For security purposes, you will be asked for your password in order to access the Bridge, as shown in Figure 5-4. In lowercase letters, enter **admin** in the *Password* field (later you can change the password through the Web-based Utility). Then click the **Enter** button.



Figure 5-4: Password

Wireless-G Ethernet Bridge with 5-Port Switch

- The screen shown in Figure 5-5 shows a choice of two wireless modes. Click the **Infrastructure** radio button if you want your wireless computers to network with computers on your wired network using a wireless access point. Click the **Ad-Hoc** radio button if you want multiple wireless computers to network directly with each other. Do not use the Ad-Hoc mode if you want to network your wireless computers with computers on your wired network.

In the *WB Name* field, enter a unique name for the Bridge. Memorable names are helpful, especially if you are using multiple bridges on the same network. Click the **Next** button to continue or the **Back** button to return to the previous screen.

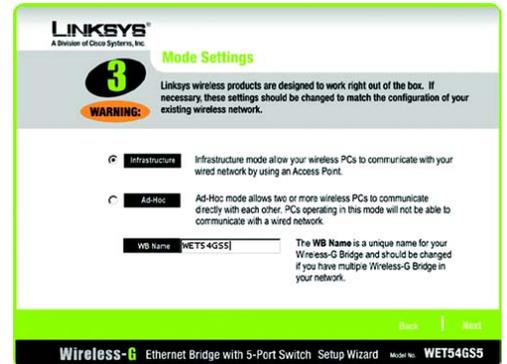


Figure 5-5: Mode Settings

Wireless-G Ethernet Bridge with 5-Port Switch

7. The *Wireless Settings* screen, shown in Figure 5-6, will now appear. Enter your wireless network's SSID. If you chose Ad-Hoc mode, select the channel at which the network broadcasts its wireless signal.

If you have Wireless-G (802.11g) and Wireless-B (802.11b) devices in your network, then keep the default *Network Mode* setting, **Mixed**. If you have only Wireless-G devices, select **G-Only**. Then click the **Next** button to continue or the **Back** button to return to the previous screen.

- **SSID** - The SSID is the unique 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 alphanumeric characters, which can be any keyboard character.
- **Channel** - From the drop-down menu, select the appropriate channel to match your network settings (available for Ad-Hoc mode only). All devices in your wireless network must use the same channel in order to communicate.
- **Network Mode** - Keep the default setting, **Mixed**, if you have Wireless-G and Wireless-B devices in your network. Select **G-Only** if you have only Wireless-G devices in your network.

8. The *IP Settings* screen will appear next, shown in Figure 5-7. If your network has a DHCP server, click the radio button next to **Automatically obtain an IP address (DHCP)**. Click the **Next** button to continue or the **Back** button to return to the previous screen. Then proceed to step 9. The Bridge's default IP address is 192.168.1.116.

If your network does not have a DHCP server, click the radio button next to **Set IP configuration manually** to **select this option**. Enter an IP Address, IP Mask, and Gateway appropriate to your network. You must specify an IP address on this screen. If you are unsure about the IP Mask and Gateway, it is better to leave these two fields blank. Click the **Next** button to continue or the **Back** button to return to the previous screen. Then proceed to step 9.

- **IP Address** - This IP address must be unique to your network.
- **IP Mask** - The Bridge's IP Mask (also known as Subnet Mask) must be the same as your wired network's Subnet Mask.
- **Gateway** - Enter the IP address of your network's Gateway (usually this is your router's LAN IP address).

LINKSYS
A Division of Cisco Systems, Inc.

4 Wireless Settings

WARNING: For the Wireless-G Bridge to function properly, these settings must be identical to those of your existing wireless network. Make sure you remember these settings as they will be needed when setting up your network!

SSID: [linksys] The SSID is a unique identification shared among all computers within your wireless network and must be the same for all those computers. The SSID is case sensitive and should not exceed 32 characters.

Channel: [6] The Channel setting is a unique number shared among all computers within your wireless network. If you experience poor performance on a certain channel, try changing to another channel. Channels 1, 6, and 11 are preferred.

Network Mode: [G-Only] In **Mixed** mode, both Wireless-B and Wireless-G equipped computers can join the wireless network. In **G-Only** mode, no Wireless-B computers will be able to join the network.

Back | Next

Wireless-G Ethernet Bridge with 5-Port Switch Setup Wizard Model No. WET54GS5

Figure 5-6: Wireless Settings

LINKSYS
A Division of Cisco Systems, Inc.

5 IP Settings

WARNING: Changes to the settings below may disrupt the settings of your existing wireless network. Make sure you remember these settings as they will be needed when setting up your wireless computers!

Set IP configuration manually Automatically obtain an IP address (DHCP)

IP Address: [192.168.1.226] An IP address must be specified in order to manage the Wireless Access Point from the network.

IP Mask: [255.255.255.0] If you are familiar with how your network is set up (DHCP or Static) you can modify these settings through your web browser at a later date. If you are unsure, it is better to skip this section by clicking on Next.

Gateway: [0.0.0.0]

Back | Next

Wireless-G Ethernet Bridge with 5-Port Switch Setup Wizard Model No. WET54GS5

Figure 5-7: IP Settings

Wireless-G Ethernet Bridge with 5-Port Switch

- The *Security Settings (Optional)* screen, shown in Figure 5-8, appears next. From the drop-down menu, select one of the wireless security mode options supported by the Bridge: WPA PSK (Pre-Shared Key) and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy. If you do not want to use the security function, keep the default setting, **Disabled**. The security modes are briefly discussed below. For more detailed instructions on configuring wireless security for the Bridge, refer to "Appendix B: Wireless Security."

WEP (64-bit WEP/128-bit WEP) - In order to utilize WEP encryption, select **64-bit** or **128-bit WEP** from the drop-down menu. Then, enter a Passphrase. (If you want to enter a WEP key manually, leave the *Passphrase* field blank, and complete the *Key 1* field.) Click the **Next** button to continue.

- Passphrase - Instead of manually entering a WEP key, you can enter a Passphrase, so a WEP key will be automatically generated. The Passphrase is case-sensitive and should have 16 or fewer alphanumeric characters. It must match the passphrase of your wireless network and is compatible with Linksys wireless products only. (You will have to enter the WEP key(s) manually on any non-Linksys wireless products.

If you want to manually enter a WEP key, leave the *Passphrase* field blank and complete the *Key 1* field.

- Key 1 - If you entered a Passphrase, then you will see the automatically generated WEP key. Click the **Next** button, and proceed to step 10.

If you did not enter a Passphrase, then enter a WEP key in the *Key 1* field. If you are using 64-bit WEP encryption, then the key must consist of exactly 10 hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0"- "9" and "A"- "F". Then click the **Next** button, and proceed to step 10.

WPA PSK - In order to utilize WPA PSK, select WPA PSK from the drop-down menu. WPA PSK gives you one encryption method, TKIP, with dynamic encryption keys. Select the type of algorithm, **TKIP**, then enter a Pre-Shared Key of 8-32 characters. (See Figure 5-9.)

The screenshot shows the 'Security Settings (Optional)' page for a Linksys device. The 'Security' dropdown menu is set to 'WEP (64-bit)'. The 'Passphrase' field contains 'linksys' and the 'Key 1' field contains '743DE2A348'. The page includes instructions for WEP configuration and a 'Next' button.

Figure 5-8: Security Settings

The screenshot shows the 'Security Settings (Optional)' page for a Linksys device. The 'Security' dropdown menu is set to 'WPA-PSK'. The 'Encryption' dropdown menu is set to 'TKIP'. The 'Pre-Shared Key' field is empty. The page includes instructions for WPA-PSK configuration and a 'Next' button.

Figure 5-9: Security Settings

Wireless-G Ethernet Bridge with 5-Port Switch

10. Review your settings on the *Confirmation* screen, shown in Figure 5-10. Write down the Bridge's IP Address if you want to configure advanced settings through the Bridge's Web-based Utility. Click the **Yes** button to save these settings. Click the **No** button to exit the Setup Wizard.



Figure 5-10: Confirmation

11. The next screen, shown in Figure 5-11, shows that the configuration is complete. To configure any other Wireless-G Ethernet Bridges on your network, run this Setup Wizard again. To register the Bridge, click the **Online Registration** button. To exit the Setup Wizard, click the **Exit** button.



Figure 5-11: Congratulations

The Wireless-G Ethernet Bridge is now successfully configured for your network.

For advanced configuration, proceed to “Chapter 7: Using the Wireless-G Ethernet Bridge Web-based Utility.” Otherwise, go to “Chapter 6: Connecting the Wireless-G Ethernet Bridge for Network Use.”

Chapter 6: Connecting the Wireless-G Ethernet Bridge for Network Use

Connection to a Network Device

1. After configuration, unplug the power cable from the electrical outlet, and unplug the Ethernet network cable from the PC.
2. Plug the Ethernet network cable into the RJ-45 port on the Ethernet-ready network device you wish to add to the wireless network. You can connect up to five devices.
3. Plug the power cable into a local electrical outlet.

The installation of the Wireless-G Ethernet Bridge is complete.

Wall Mount Placement Option

Besides placing the Bridge horizontally on a surface, you can also hang the Bridge on a wall.

1. Attach two screws to the wall, so that they line up with the Bridge's two wall-mount slots.
2. Place the Bridge over the screws.
3. If necessary, adjust the antenna so that it points straight up in the air.

The placement of the Wireless-G Ethernet Bridge is complete.

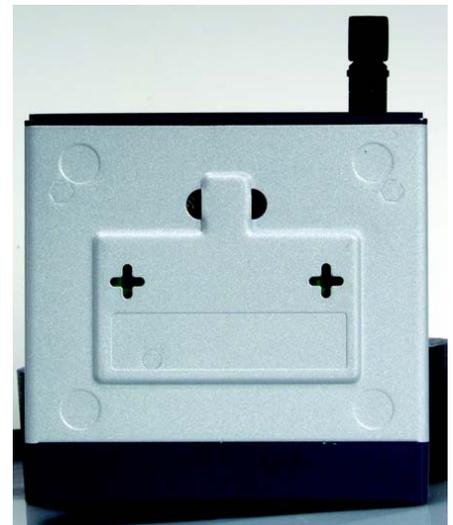


Figure 6-1: Wall Placement

Chapter 7: Using the Wireless-G Ethernet Bridge Web-based Utility

Overview

The Bridge is designed to function properly after you configure it using the Setup Wizard. However, if you would like to change these basic settings or make advanced configuration changes, use your web browser and the Wireless-G Ethernet Bridge Web-based Utility. This chapter explains how to use the Utility.

Starting the Web-based Utility

1. Open your web browser, and enter the IP address of the Wireless-G Ethernet Bridge (the default is **192.168.1.226**). Press the **Enter** key, and a screen similar to the one shown in Figure 7-1 will appear. In lowercase letters, enter the default, **admin**, in the *User name* and *Password* fields. Click the **OK** button. You can set a new password on the *Password* screen later.
2. The Utility's *Setup* screen, shown in Figure 7-2, will appear.



Figure 7-1: Password Screen

The Utility provides a convenient, web-browser-based way to alter the Bridge's settings. It offers seven main tabs:

- **Setup** - Enables you to configure the IP address and wireless settings.
- **Password** - Allows you to change the password or reset all settings to factory defaults.
- **Wireless** - Lets you change the advanced wireless settings and clone a MAC address onto the Bridge.
- **Switch** - This screen allows you to configure the following settings on the switch: QOS, Switch Table, VLAN, RMON Statistics, Port Mirroring, and Access List.
- **Wireless Status** - Displays the Bridge's current wireless settings.
- **SNMP** - This screen is used to configure the SNMP trap settings for the Bridge.
- **Help** - Provides explanations of various configuration settings and links to online technical support resources. You can also upgrade the Bridge's firmware using the *Help* screen.



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.



Note: The Wireless-G Ethernet Bridge is designed to function properly after you use the Setup Wizard. However, if you would like to change its basic settings or make advanced configuration changes, use your web browser and the Wireless-G Ethernet Bridge Web-based Utility.

Setup

The *Setup* screen, shown in Figure 7-2, lets you configure the wired and wireless network settings for the Bridge.

When finished making your changes on this tab, click the **Apply** button to save these changes, or click the **Cancel** button to undo your changes.

- **Firmware** - The version number of the Bridge's firmware is displayed here. Firmware should be upgraded **ONLY** if you experience problems with the Bridge. Firmware updates are posted at www.linksys.com.
- **MAC Address** - The MAC Address of the Bridge is displayed here.
- **System Uptime** - The amount of time the Bridge has been running is displayed here.

LAN

- **Device Name** - You may assign any name to the Bridge. Unique, memorable names are helpful, especially if you are using multiple bridges on the same wireless network.
- **Configuration Type** - If the Bridge will obtain an IP address automatically from a DHCP server, such as a router, then select **Automatic Configuration-DHCP**. If you are assigning the Bridge a static IP address, then select **Static IP Address**, and enter an IP Address, Subnet Mask, and Gateway address in the *IP Address*, *Subnet Mask*, and *Gateway* fields.
- **802.1x** (See Figure 7-3.) - To change your 801.1x settings, click the **Edit 802.1x Settings** button. Figure 7-3 will appear. To change the settings, select **Enable 801.x Service**.

- **Radius Server**. Enter the *Radius Server IP Address* in the fields.
- **Radius Server Port**. Enter the *Radius Server Port* in the field.
- **Shared Key**. Enter the key that you use for your wireless network in the field.
- **Reauthentication Timeout**. Enter the time in seconds for key authentication.

Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **View Log** button to view a log.



Figure 7-2: Setup Tab

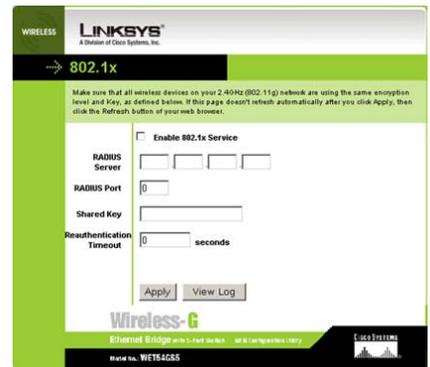


Figure 7-3: 802.1x Screen

Wireless

- **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 alphanumeric characters, which may be any keyboard character (do not use any spaces). Make sure this setting is the same for all devices in your wireless network. For added security, Linksys recommends that you change the default SSID (linksys) to a name of your choice.

To search for available wireless networks, click the **Site Survey** button.

Site Survey

The *Site Survey* screen, shown in Figure 7-4 shows all the wireless networks detected by the Bridge and their general information. You can use this screen to connect to one of these networks.

For each wireless network detected, the following information is displayed:

- **SSID** - The network name. To join a wireless network, click its SSID.
- **MAC Address** - The MAC address of the network's access point.
- **Channel** - The channel setting.
- **Signal Strength (%)** - The percentage of wireless signal strength.
- **Mode** - The type of wireless standard, network mode, and status of WEP encryption.
- Click the **Refresh** button to obtain the most up-to-date data. Click the **Close** button to close this screen. Click the **Help** button for additional on-screen information.
- **Network Type** - Choose a wireless operating mode for the Bridge. Keep the default setting, **Infrastructure**, if you want your wireless-equipped device to communicate with computers and other devices on your wired network using a wireless access point. Select **Ad-Hoc** button if you want multiple wireless-equipped devices to communicate directly with each other.

If you chose Ad-Hoc mode, then select the correct operating channel for your network from the *Channel* drop-down menu. This should match the channel setting of the other devices in your wireless network.

Select the appropriate network mode. Keep the default, **Mixed**, if you have Wireless-G (802.11g) and

SSID	MAC Address	Channel	Signal Strength(%)	Mode
wag54g-12	00:06:25:FD:D1:90	6	100%	802.11g, Intra
maggotr54gz2	00:30:4C:60:04:01	6	100%	802.11g, Intra
linksys-g	00:0C:41:15:61:4F	6	100%	802.11g, Intra, Security
linksys-g	00:0C:41:8F:73:0D	6	100%	802.11g, Intra
linksys	00:90:A2:99:88:77	6	100%	802.11b, Intra
linksys	00:0C:41:3F:2A:2C	6	96%	802.11g, Intra
demo	00:06:25:FD:4B:E2	1	71%	802.11g, Intra
linksys	00:06:25:FD:D6:FD	6	58%	802.11g, Intra
WMP54G	00:0C:41:7F:53:84	6	53%	802.11g, Intra

Note: To connect to one of the wireless networks listed, click its SSID.

Refresh Help Close

Wireless-G
Ethernet Bridge with 5-Port Switch - Web Configuration Utility
Model No. WRT54G85

Figure 7-4: Site Survey

Wireless-G Ethernet Bridge with 5-Port Switch

Wireless-B (802.11b) devices in your network. Select **G-Only** if you have only Wireless-G devices in your network.

- Security - To enable security, select **Enable**, then click **Edit Security Settings**. To disable security, select **Disable**.

The Security screen, as shown in Figure 7-5, will appear. From the drop-down menu, select one of the four wireless security modes supported by the Bridge: WEP, RADIUS, WPA RADIUS, and WPA Pre-Shared Key. (WEP stands for Wired Equivalent Privacy, RADIUS stands for Remote Authentication Dial-In User Service, and WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption). The four security modes are briefly discussed here. For detailed instructions on configuring wireless security for the Bridge, turn to "Appendix B: Wireless Security."

WEP

Use the *WEP* screen, shown in Figure 7-5, to configure the WEP encryption for the Bridge. 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 a *Passphrase* or enter the WEP key manually.

- Default Transmit Key - Select which WEP key (1-4) will be used when the Bridge sends data. Make sure the other wireless-equipped devices are using the same key.
- WEP Encryption - In order to use WEP encryption, select **64-Bit (10 hex digits)** or **128-Bit (26 hex digits)** from the drop-down menu.
- Passphrase - Instead of manually entering WEP keys, you can enter a Passphrase. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (The Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, you will need to enter your WEP key manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP key(s).
- Keys 1-4 - If you are not using a Passphrase, then you can enter one or more WEP keys manually.

In each key field, manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.) If you are using 64-bit WEP encryption, then each key must consist of exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then each key must consist of exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"- "9" and "A"- "F".



NOTE: Make sure that your security choice matches the security choice of the wireless network you want to join. Otherwise, the connection will fail.

The screenshot shows the 'Security' configuration page for a Linksys Wireless-G Ethernet Bridge. The page has a green header with the Linksys logo and 'A Division of Cisco Systems, Inc.'. Below the header, the title 'Security' is displayed. A warning message states: 'Make sure that all wireless devices on your 2.4GHz (802.11g) network are using the same encryption level and Key, as defined below. If this page doesn't refresh automatically after you click Apply, then click the Refresh button of your web browser.' The configuration options include: 'Security Mode' set to 'WEP'; 'Default Transmit Key' with radio buttons for keys 1, 2, 3, and 4; 'WEP Encryption' set to '64-Bit (10 hex digits)'; a 'Passphrase' field with a 'Generate' button; and four 'Key' fields (Key 1 through Key 4), each containing ten zeros. An 'Apply' button is at the bottom. The footer of the page includes 'Wireless-G Ethernet Bridge with 5-Port Switch', 'v1.0 Configuration Utility', and 'LINKSYS'.

Figure 7-5: WEP

Wireless-G Ethernet Bridge with 5-Port Switch

If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **Apply** button to save your changes and close the screen.

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.) It offers three authentication methods: MD5, TLS, and TTLS.

EAP Type

MD5

Select a Default 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 a Passphrase or enter the WEP key manually. (See Figure 7-6.)

- **Default Transmit Key** Select which WEP key (1-4) will be used when the Bridge sends data. Make sure that the receiving device (wireless client) is using the same key.
- **WEP Encryption.** An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode data transmissions, all devices in a network must use an identical WEP key. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance. Select **64 bits (10 hex digits)** or **128 bits (26 hex digits)**.
- **Passphrase.** Instead of manually entering WEP keys, you can enter a passphrase. This passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 32 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only and cannot be used with Windows XP Zero Configuration. If you want to communicate with non-Linksys wireless products or Windows XP Zero Configuration, make a note of the WEP key generated in the Key 1 field, and enter it manually in the wireless client.) After you enter the Passphrase, click the **Generate** button to create WEP keys.
- **Keys 1-4.** WEP keys enable you to create an encryption scheme for wireless network transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes; they are not valid key values.) If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"- "9" and "A"- "F".

The screenshot shows the Linksys Security configuration page. At the top, it says "LINKSYS A Division of Cisco Systems, Inc." and "Security". Below that, a warning message states: "Make sure that all wireless devices on your 2.4GHz (802.11g) network are using the same encryption level and Key, as defined below. If this page doesn't refresh automatically after you click Apply, then click the Refresh button of your web browser." The configuration fields are: Security Mode: RADIUS; EAP Type: MD5; Cipher Type: WEP; Default Transmit Key: 1; WEP Encryption: 64-Bit (10 hex digits); Passphrase: (empty) with a Generate button; Key 1: 0000000000; Key 2: 0000000000; Key 3: 0000000000; Key 4: 0000000000; User ID: (empty); Password: (empty). At the bottom, there are buttons for Apply, Re-Authenticate, and View Log. The footer includes "Wireless-G Ethernet Bridge with 5-Port Switch" and "Model No. WRT54GSS".

Figure 7-6: RADIUS-MD5

Wireless-G Ethernet Bridge with 5-Port Switch

- **User ID and Password.** A user identification and password are required for your security. Enter the ID in the *User ID* field, then the password in the *Password* field.

When finished making your changes on this tab, click the **Apply** button to save these changes.

TLS

TLS is a mutual authentication method that uses digital certificates. Select TLS from the EAP Type drop-down menu. Enter the Login name of your wireless network in the *User ID* field. Enter the *User Certificate and Root Certificate* in the fields or click the **Browse** button to browse for it, then upload it.

- **EAP Type** - The authentication method that your network uses. Select **TLS** from the drop-down menu.
- **User ID** -Your User ID is the Login name of your wireless network. Enter the Login name of your wireless network in the *User ID* field.
- **User Certificate** - Enter the user certificate you have installed to authenticate you on your wireless network or click the **Browse** button to browse for it. Click the **Upload** button to upload the certificate.
- **Root Certificate** - Enter the root certificate you have installed to authenticate you on your wireless network or click the **Browse** button to browse for it. Click the **Upload** button to upload the certificate.

Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **View Log** button to view a log.

The screenshot shows the 'Security' configuration page for a Linksys Wireless-G Ethernet Bridge with 5-Port Switch. The page is titled 'Security' and features a green header with the Linksys logo. Below the header, there is a warning message: 'Make sure that all wireless devices on your 2.4GHz (802.11g) network are using the same encryption level and Key, as defined below. If this page doesn't refresh automatically after you click Apply, then click the Refresh button of your web browser.' The main configuration area includes a 'Security Mode' dropdown menu set to 'Radius', an 'EAP Type' dropdown menu set to 'TLS', and a 'Cipher Type' dropdown menu set to 'WEP'. There are two text input fields for 'User ID' and 'Root Certificate', each with a 'Browse...' button and an 'Upload' button. Below these fields, there are instructions: 'Select the User Certificate (in PKCS#12 format) file to upload (User Certificate not loaded.)' and 'Select the Root Certificate (in DER format) file to upload (Root Certificate not loaded.)'. At the bottom of the configuration area, there are three buttons: 'Apply', 'Re-Authenticate', and 'View Log'. The footer of the page includes the 'Wireless-G' logo, the model number 'WET54G55', and the 'Cisco SYSTEMS' logo.

Figure 7-7: RADIUS-TLS

Encryption - Encoding data transmitted in a network.

TTLS

TTLS is a mutual authentication method that uses digital certificates. Select TTLS from the EAP Type drop-down menu. Enter the Login name of your wireless network in the *User ID* field and the password in the *Password* field. Enter the *Root Certificate* in the field or click the **Browse** button to browse for it, then upload it.

- EAP Type - The authentication method that your network uses. Select **TTLS** from the drop-down menu.
- User ID -Your User ID is the Login name of your wireless network. Enter the Login name of your wireless network in the *User ID* field.
- Password - This is the password used for your wireless network. Enter the password in the *Password* field.
- Root Certificate - Enter the root certificate you have installed to authenticate you on your wireless network or click the **Browse** button to browse for it. Click the **Upload** button to upload the certificate.

Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **View Log** button to view a log.

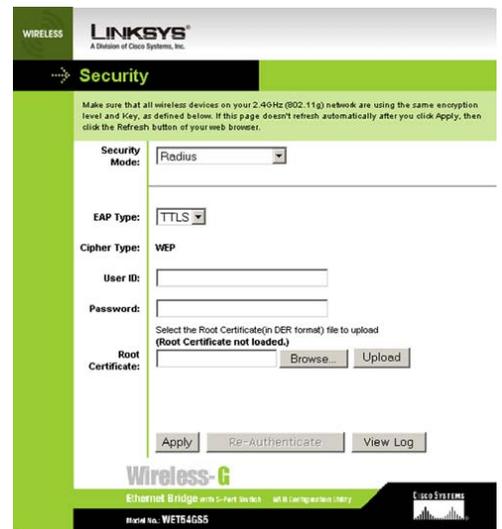


Figure 7-8: RADIUS-TTLS

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

WPA RADIUS

WPA RADIUS. 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.) The WPA algorithm used is TKIP. 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. (See Figure 7-11.)

Click the **Apply** button to save your changes. If your screen doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **View Log** button to view a log.

TLS

TLS is a mutual authentication method that uses digital certificates. Select TLS from the EAP Type drop-down menu. Enter the Login name of your wireless network in the *User ID* field. Enter the *User Certificate and Root Certificate* in the fields or click the **Browse** button to browse for it, then upload it.

- EAP Type - The authentication method that your network uses. Select **TLS** from the drop-down menu.
- WPA Algorithm - The WPA algorithm used is TKIP.
- User ID -Your User ID is the Login name of your wireless network. Enter the Login name of your wireless network in the *User ID* field.
- User Certificate - Enter the user certificate you have installed to authenticate you on your wireless network or click the **Browse** button to browse for it. Click the **Upload** button to upload the certificate.
- Root Certificate - Enter the root certificate you have installed to authenticate you on your wireless network or click the **Browse** button to browse for it. Click the **Upload** button to upload the certificate.

Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **View Log** button to view a log.



Figure 7-9: WPA RADIUS-TLS

TLS (Transport Layer Security) - A mutual authentication method that uses digital certificates.

TTLS

TTLS is a mutual authentication method that uses digital certificates. Select TTLS from the EAP Type drop-down menu. Enter the Login name of your wireless network in the *User ID* field and the password in the *Password* field. Enter the *Root Certificate* in the field or click the **Browse** button to browse for it, then upload it.

- EAP Type - The authentication method that your network uses. Select **TTLS** from the drop-down menu.
- WPA Algorithm - The WPA algorithm used is TKIP.
- User ID -Your User ID is the Login name of your wireless network. Enter the Login name of your wireless network in the *User ID* field.
- Password - This is the password used for your wireless network. Enter the password in the *Password* field.
- Root Certificate - Enter the root certificate you have installed to authenticate you on your wireless network or click the **Browse** button to browse for it. Click the **Upload** button to upload the certificate.

Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **View Log** button to view a log.



Figure 7-10: WPA RADIUS-TTLS

Wireless-G Ethernet Bridge with 5-Port Switch

WPA Pre-Shared Key

WPA gives you TKIP for the encryption method. Enter a WPA Shared Key of 8-32 characters. (See Figure 7-11.) Enter a key shared between the Bridge and the server.

Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **View Log** button to view a log.

The *Log Table* screen appears in Figure 7-12. The log shows the authentication process.

Click the **Refresh** button to refresh the screen. Click the **Close** button to return to the the previous screen.



Figure 7-11: WPA Pre-Shared Key

Log Table

No.	Log Message
1	In WPA-PSK mode
2	Set Information Element
3	Authenticator MAC Address: 000625fd66fd
4	sending EAPOL-Start frame
5	sending EAPOL-Start frame
6	sending EAPOL-Start frame

Figure 7-12: Log Table

Password

The *Password* screen, shown in Figure 7-13, lets you change the Bridge's Username and Password and restore the factory default settings.

- **Username** - It is strongly recommended that you change the factory default user name of the Bridge from admin to a new password that you create. All users who try to access the Bridge's Web-based Utility will be prompted for the Bridge's Password. The new Password must not exceed 12 characters in length and must not include any spaces.
- **Administrative Password** - It is strongly recommended that you change the factory default password of the Bridge from admin to a new password that you create. All users who try to access the Bridge's Web-based Utility will be prompted for the Bridge's Password. The new Password must not exceed 12 characters in length and must not include any spaces. Enter the new Password a second time to confirm it.



IMPORTANT: Any settings you have saved will be lost if the default settings are restored.

- **Restore Factory Defaults** - Click the **Yes** radio button to reset all configuration settings to their default values. If you do not want to restore the factory defaults, then keep the default setting, **No**.

To save your changes, click the **Apply** button. Click the **Cancel** button to cancel your changes. Click the **Help** button for additional on-screen information.



Figure 7-13: Password Tab

Wireless

Use the *Wireless* screen, shown in Figure 7-14, to customize advanced wireless settings and clone a MAC address onto the Bridge.

Advanced Wireless

- **Transmission Rate** - The default setting is **Auto**. The range is from 1 to 54Mbps. 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 keep the default setting, **Auto**, to have the Bridge automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Bridge and another wireless-equipped device.
- **Authentication Type** - The default setting is **Auto**. The choices are **Auto**, **Open**, and **Shared**. This setting allows the Bridge to authenticate communication with the wireless devices in your network. With the Shared key setting, all wireless devices must have the same WEP keys so that the Bridge and the client can authenticate each other and start transmitting data. With the Open system setting, any device can join a network without performing any security check. Using the Auto setting, the Bridge will automatically detect whether a wireless device uses shared key or open system authentication, and then it will transmit data using the appropriate authentication type.
- **RTS Threshold** - This value should remain at its default setting of **2347**. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are 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.
- **Fragmentation Threshold** - This value should remain at its default setting of **2346**. The range is 256-2346 bytes. It 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 modifications of this value are recommended.

MAC Address

- **Cloning Mode** - You can clone the MAC address of any network device onto the Bridge. To disable MAC address cloning, keep the default setting, **Disable**. To use the MAC cloning feature, select **Enable**.

If you have enabled MAC cloning, then select **Auto** if you want to clone the MAC address of the device

The screenshot shows the 'Wireless' configuration page for a Linksys Wireless-G Ethernet Bridge. The page has a green header with the Linksys logo and navigation tabs for Setup, Password, Wireless, Switch, and Wireless. Below the header, there is a section for 'Advanced Wireless' settings. The settings are as follows:

- Transmission Rate:** Auto (Default: Auto)
- Authentication Type:** Auto (Default: Auto)
- RTS Threshold:** 2347 (Default: 2347, Range: 0 - 2347)
- Fragmentation Threshold:** 2346 (Default: 2346, Range: 256 - 2346)

Below these settings is a section for 'MAC Address' with a 'Cloning Mode' dropdown menu set to 'Disable'. There are radio buttons for 'Auto' and 'Manual'. A text field for 'Enter MAC Address' contains '00:00:00:00:00:00'. A note states: 'Note: When in Auto mode, the Bridge will use the MAC Address of the device connected to the Ethernet port. Choose Manual if more than one device will be connected to the Bridge and you want to clone the MAC Address of a specific device.' At the bottom of the form are 'Apply', 'Cancel', and 'Help' buttons. The footer of the page includes the text 'Wireless-G Ethernet Bridge with 5-Port Switch' and 'Model No: WETS4GSS'.

Figure 7-14: Wireless Tab

Wireless-G Ethernet Bridge with 5-Port Switch

currently connected to the Bridge's LAN port. The Bridge will actively scan for a new MAC address to be cloned whenever you disconnect and re-connect multiple devices to the Bridge through its LAN port. Select **Manual** if you want to specify a MAC address in the *Enter MAC Address* field. This is useful when the Bridge is connected to multiple devices through the switch.

Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **Cancel** button to cancel your changes. Click the **Help** button for additional on-screen information.

Switch Tab

These screens allow you to configure settings for the managed switch feature. The settings in the Switch tabs should only be modified by advanced users.

Spanning Tree Protocol

This screen allows you to configure the Spanning Tree Protocol settings for the managed switch feature.

Spanning Tree

- STP - Select **Enable** to enable the Spanning Tree Daemon or **Disable** to disable the Spanning Tree Daemon.
- Max Age - Enter the timeout period for the information in each Hello message received from others.
- Hello Time - Enter the Hello message broadcast interval. The Spanning Tree Hello message is used to exchange the topology information between each Spanning Tree Daemon
- Forward Delay - The bridge will start from the the block state and then change to listening, learning , then forwarding. It will only forward packets in the forwarding state. Enter the delay defined by the time spent in the listening and learning state.

Click the **Apply Global Setting** button to save your settings globally.

- STP Table - For ports 1 through 6.

Priority - The priority of this port. The smaller the priority value, the higher the priority. If two ports form a loop, the port with higher priority value will change to block state, thus break the loop.

LINKSYS
A Division of Cisco Systems, Inc.

Switch

Spanning Tree Protocol

Use this page to configure the Spanning Tree Protocol settings for your managed switch feature. Click the **Apply Global Setting** button to save your global setting and **Apply Port Setting** for per port configuration. These settings should only be modified by advanced users.

Spanning Tree

STP: (Default: disable)

Max Age: (Range: 600 - 4000)

Hello Time: (Range: 100 - 1000)

Forward Delay: (Range: 400 - 3000)

STP Table	Port	Priority	Cost	State
1	<input type="text" value="128"/>	<input type="text" value="100"/>	<input type="text" value="forwarding"/>	
2	<input type="text" value="128"/>	<input type="text" value="100"/>	<input type="text" value="forwarding"/>	
3	<input type="text" value="128"/>	<input type="text" value="100"/>	<input type="text" value="forwarding"/>	
4	<input type="text" value="128"/>	<input type="text" value="100"/>	<input type="text" value="forwarding"/>	
5	<input type="text" value="128"/>	<input type="text" value="100"/>	<input type="text" value="forwarding"/>	
6	<input type="text" value="127"/>	<input type="text" value="200"/>	<input type="text" value="forwarding"/>	

Wireless-G
Ethernet Bridge with 5-Port Switch
Model No.: WET54GSS

Figure 7-15: Spanning Tree Protocol Tab

Wireless-G Ethernet Bridge with 5-Port Switch

Cost - The path cost to forward packets from this port, it's usually inversely proportional to the speed of the port.

State - The STP state determined by the Spanning Tree protocol. They are Blocking, Listening, Learning and Forwarding. This is determined by the STP Daemon.

Click the **Apply Port Setting** button to save your settings per port. Click the **Cancel** button to cancel your changes. Click the **Refresh** button to refresh your screen. Click the **Help** button for additional on-screen information.

QOS

This screen is used to configure the Quality of Service (QOS), Storm Filtering, and Flow Control settings for the managed switch feature.

- **Global QOS Mode** - There are 4 output queues per port with different priority. This QOS setting will let user choose between a more evenly distributed Weighted Fair Queue or a strict Priority scheme. With Priority scheme, the packets in the higher priority queue will always be forwarded first. With Weighted Fair Queue, the switch will forward the packets with a 8:4:2:1 ratio.
- **Diff Serv Map** - Select which bit in the packets' diff serv field to map to IP Diff Serv priority.
- **802.1p PRI Map** - Select which bit in the packets' 802.1p priority field to map to 802.1p priority.

Click the **Apply Global Setting** button to save your global settings.

- **QOS Port Setting** - Ports 1 through 5 are the wired ports. Port 6 is the wireless port.

QOS Priority - Select how to determine the QOS priority of each packet.

IP Diff Serv - It will use the IPv4 Diff Serv/Tos field to determine the QOS priority if the packet is an IP packet. Otherwise, the lowest priority will be used.

802.1p - It will use the VLAN Priority Field to determine the QOS priority. Otherwise, the lowest priority will be used.

Critical/High/Medium/Low - This setting will set all packets coming into this port to this priority value. Critical is the highest and Low is the lowest.

- **Ingress Rate Mode** - This is used for rate limiting. We can limit packet rate entering a specific port. This mode will choose which packets will be limited. The limit will be set in the *Ingress Rate* field.

The screenshot displays the 'Switch' configuration page for a Linksys Wireless-G Ethernet Bridge with 5-Port Switch (Model No: WET54GSS). The page is titled 'Switch' and includes navigation links for Setup, Firewall, Wireless, Switch, and Wireless Status. The main content area is for configuring Quality of Service (QOS), Storm Filtering, and Flow Control settings. The 'Global QOS Mode' is set to 'Weighted Fair Queue (Default: Weighted Fair Queue)'. Below this, there are checkboxes for 'Diff Serv Map' (bits 0-7) and '802.1p PRI Map' (bits 0-7). An 'Apply Global Setting' button is present. The 'QOS Port Setting' section contains a table for configuring settings for ports 1 through 6 (Port 6 is the Wireless Port). The table has columns for QOS Priority, Ingress Rate Mode, Ingress Rate, Egress Rate, and Flow Control. For ports 1-5, the QOS Priority is set to 'IP diff serv', Ingress Rate Mode is 'All packets', and Ingress Rate and Egress Rate are set to 'No Limit'. For the Wireless Port (Port 6), the QOS Priority is set to 'Critical', and Ingress Rate and Egress Rate are set to 'No Limit'. At the bottom of the table, there are 'Apply Port Setting', 'Cancel', and 'Help' buttons.

QOS Port Setting	QOS Priority	Ingress Rate Mode	Ingress Rate	Egress Rate	Flow Control
Port 1	IP diff serv	All packets	No Limit	No Limit	Disable
Port 2	IP diff serv	All packets	No Limit	No Limit	Disable
Port 3	IP diff serv	All packets	No Limit	No Limit	Disable
Port 4	IP diff serv	All packets	No Limit	No Limit	Disable
Port 5	IP diff serv	All packets	No Limit	No Limit	Disable
Port 6 Wireless Port	Critical	All packets	No Limit	No Limit	Disable

Figure 7-16: QOS Tab

Wireless-G Ethernet Bridge with 5-Port Switch

- All Packets - This rate limit will be applied to all packets.
- Flooded - This rate limit will be applied to *Flooded unicast* and *Multicast and Broadcast* packets.
- Multicast - This rate limit will be applied to *Multicast and Broadcast* packets.
- Broadcast - This rate limit will be applied to *Broadcast packets* only.
- Ingress Rate - This setting allows you to choose the input data rate for a port. Packets exceeding this rate will be dropped.
- Egress Rate - This setting let user choose the output data rate for a port. Packets exceeding this rate will be dropped.
- Flow Control - When this feature is enabled, the wired LAN ports will exchange control packets with the connected port before sending packets. If the other end is not able to process more packets, our sending port will hold the packets. The mechanism will ensure that packets will not be lost on the wire. But it can still cause congestion in other part of the network, so please use this with caution.

Click the **Apply Port Setting** button to save your settings per port. Click the **Cancel** button to cancel your changes. Click the **Refresh** button to refresh your screen. Click the **Help** button for additional on-screen information.

Switch Table

Use this screen to configure the switch address table settings for the managed switch feature, and to add or delete static address table entries. Global ATU Setting is a global switch address table setting. Address Learning is used to determine if the switch should automatically learn the mac address for the packets; the default is enabled. Age Timer is used to determine the idle time out of each address entry.

- New Address Entry - Mac Address is the destination mac address. Output Port Vector is the output ports where the packet should be routed to if there is a mac address match. Note, the packets can be routed to more than 1 port. The static address entry will be locked in the table and does not idle the timeout. To add entries, select the port's check box and click the **Add New Entry** button. To delete entries, select the port's check box and click the **Delete Selected Entry** button.
- Static Address Table - This lists the static MAC address entries and the output port vector settings.
- Address Table Dump - This is a complete dump of the address table, including both the dynamic learned entries and static entries. If there is a topology change, click the **Flush Table** to button to remove all the

The screenshot shows the 'Switch' configuration page for a Linksys WET54GDS. The 'Global ATU Setting' section has 'Enable Learning' checked and 'Age timer' set to 5 minutes. The 'New Address Entry' section has a 'Mac Address' field with '00:00:00:00:00' and 'Output Port Vector' with checkboxes for ports 1-6. The 'Static Address Table' section has a table with columns 'Mac Addr', 'Port Vector 1:2:3:4:5:6', and 'Life Remaining'. Below it is an 'Address Table Dump' table with columns 'mac addr', 'port vector 1:2:3:4:5:6', and 'state'. The dump shows 10 entries with various mac addresses and port vectors.

mac addr	port vector 1:2:3:4:5:6	state
00:02:00:12:12:12	0:0:0:0:1	14
00:03:00:17:0F:78	0:0:0:0:1	12
00:08:25:F0:EB:77	0:0:0:0:1	6
00:0C:41:09:0C:CB	0:0:0:0:1	10
00:0C:41:09:0C:CD	0:0:0:0:1	10
00:0C:41:09:0C:CE	0:0:0:0:1	10
00:0C:41:3E:E3:89	1:0:0:0:0	14
00:0C:41:90:F0:80	1:0:0:0:0	11
00:0C:41:90:F0:83	1:0:0:0:0	14
00:0C:41:8F:BB:8B	0:0:0:0:1	14
00:0E:84:2B:5A:C7	0:0:0:0:1	6

Figure 7-17: Switch Table Tab

Wireless-G Ethernet Bridge with 5-Port Switch

dynamic learned entries to force it to learn again. It will only dump at most 64 entries per page. If there are already 64 entries, use *Get Next Page* to get more pages.

- **Life Remaining** - This is the life remaining before an idle time out. The value is 0-15. If the switch received any packets with the same destination MAC address, then the life value will reset to 15. If the life value decreases to 0, then it will be removed from the table. The idle timeout is configured in the Age Timer field.

A static address entry will appear as locked or locked multicast in the address table. An entry might also be added by the bridge when certain protocol (eg. spanning tree) is enabled. That entry will have a management subtitle.

VLAN

This screen is used to configure the 802.1q VLAN and port based VLAN feature, and to add and delete individual 802.1q VLAN entries.

Global VLAN Setting

- **Disable** - This will disable all VLAN function.
- **802.1q Check** - In this 802.1q mode, when a packet comes in, the switch will parse for it's VLAN tag first. If the packet does not have a VLAN tag, the default VID of the inport will be used as its VLAN ID. If the final VLAN ID is not listed in the VLAN table, this packet will be dropped. Otherwise, the switch will search the switch address table for the egress (output) port. Once the egress port is determined, the member option will be used to determine if the switch will add or remove the tag or drop the packets.
- **802.1q Secure** - This is similar to the *802.1q Check* mode. But if the incoming port is not a member of this VLAN ID, this packet will also be dropped.
- **Port Based** - Each port has an outport vector that can be configured below. Packets can only exit the ports that are enabled in the outport vector.

Click the **Apply Global Setting** button to save your global settings.

Port Based VLAN Setting

- This is to set the Port Based VLAN Map. For each port, if the output field is checked, then packets are allowed to exit that port. Packets are not allowed to enter and exit the same port.

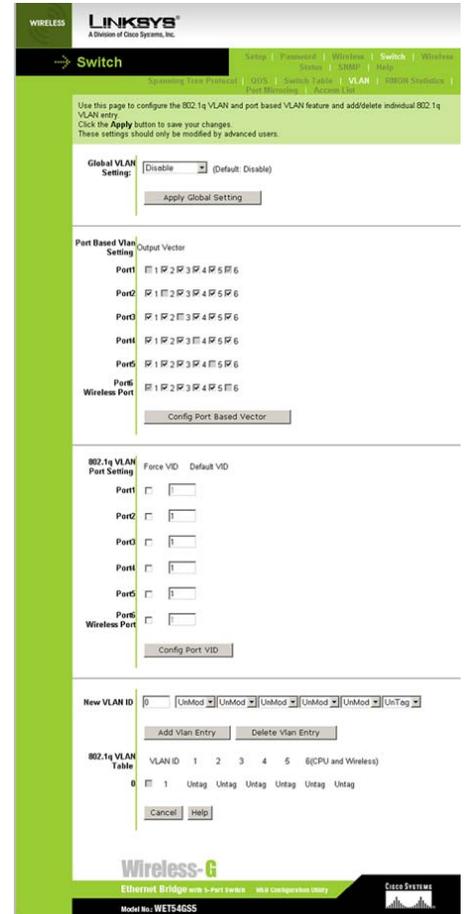


Figure 7-18: VLAN Tab

Wireless-G Ethernet Bridge with 5-Port Switch

The port1 to port6 checkbox is disabled so that the user can always use port1 as a back door to access the web config page when the port based VLAN is enabled.

- 802.1q Port VLAN Setting - Default VID is used when 802.1q is enabled but input packet does not have a VLAN tag. In this case, the Default VID will be used as the packet's VLAN tag.

Even if the input packet has a VLAN tag, user can still enable the Force VID to change the VLAN tag of the packet to the Default VID of the inport.

- New VLAN ID - This is for adding new VLAN ID and the member tag into the VLAN table. VLAN ID can be any integer between 1-4095. The maximum VLAN table size is 64. The member tag determine if a port is a member of the VLAN and how to modify the packet when it exits the switch.

UnMod - This port is a member of this VLAN, packets will exit unmodified.

Drop - This port is not a member of this VLAN.

UnTag - This port is a member of this VLAN, packets will exit with the VLAN tag removed.

Tag - This port is a member of this VLAN, packets will exit this port with the VLAN tag. The VLAN tag can be either the original one coming with the packet or the default VVID of the inport.

- 802.1q VLAN Table - This is the entire VLAN table. The user can select an entry and click **Delete VLAN Entry** to remove this VLAN ID from the table.

Click the **Apply Port Setting** button to save your settings per port. Click the **Cancel** button to cancel your changes. Click the **Refresh** button to refresh your screen. Click the **Help** button for additional on-screen information.

RMON Statistics

This screen is used to view the RMON counters for each port.

Port Selection - Select the port to display the packets statistics.

EtherStatsDropEvents - The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.

EtherStatsOctets - The total number of octets(bytes) of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization.

EtherStatsPkts - The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

EtherStatsBroadcastPkts - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

EtherStatsMulticastPkts - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

EtherStatsCRCAlignErrors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

EtherStatsUndersizePkts - The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

EtherStatsOversizePkts - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

EtherStatsFragments -The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that it is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.

EtherStatsJabbers - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of



Figure 7-19: RMON Statistics Tab

Wireless-G Ethernet Bridge with 5-Port Switch

Octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

EtherStatsCollisions - The best estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10BASE-5) and section 10.3.1.3 (10BASE-2) of IEEE standard 802.3 states that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment would. Probe location plays a much smaller role when considering 10BASE-T. 14.2.1.4 (10BASE-T) of IEEE standard 802.3 defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BASE-T station can only detect collisions when it is transmitting. Thus probes placed on a station and a repeater, should report the same number of collisions. Note also that an RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.

EtherStatsPkts64Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

EtherStatsPkts65to127Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

EtherStatsPkts128to255Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

EtherStatsPkts256to511Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

EtherStatsPkts512to1023Octets - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

EtherStatsPkts1024to1518Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Port Mirroring

This screen shows the status of each port and allows you to configure the port mirroring settings for the manage switch feature. The information here is for the wired LAN ports. For wireless status and packet counts, please refer to the Wireless Status page.

Port Information Table

Ports 1 through 5 are the wired ports. Port 6 is the wireless port.

Link - If a port is connected, then the status is up, otherwise it is down.

Duplex - The auto-negotiation result of duplex mode, can be full duplex or half duplex. Full duplex mode will allow packets sent in both way simultaneously and results in 2x throughput than half duplex mode.

Speed - The auto-negotiation result of speed. It can be 10Mbps or 100Mbps.

Rx Packets - Received packets count

Tx Packets - Transmit packets count

Port Mirroring Setting

Port mirroring will duplicate traffic from the *From Port* to the *To Port*. This is good for debugging network problems.

Type - Disable will turn off the monitor function. *Monitor egress* will only monitor traffic exiting the from that specific port.

Monitor both will monitor both directions of traffic in the From Port.

From Port - The port to be mirrored.

To Port - The port where the traffic is mirrored to.

Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **Cancel** button to cancel your changes. Click the **Help** button for additional on-screen information.

The screenshot shows the Linksys web interface for a Wireless-G Ethernet Bridge with 5-Port Switch. The main content area is titled "Port Mirroring" and contains the following elements:

Use this page to view the status of each port and configure the port monitoring settings for your managed switch feature. Click the **Apply** button at the bottom of the page to save your changes. These settings should only be modified by advanced users.

Port Information Table	Link	Duplex	Speed	RxPackets	TxPackets
Port1	Up	Full	100Mbps	2513	3486
Port2	Down	Half	10Mbps	0	0
Port3	Down	Half	10Mbps	0	0
Port4	Down	Half	10Mbps	0	0
Port5	Down	Half	10Mbps	0	0
Wireless Port	Up	Full	100Mbps	3432	2513

Port Mirroring Setting

Type: From: To:

Buttons:

Wireless-G Ethernet Bridge with 5-Port Switch WPA Configuration Utility Model No: WET546S5

Figure 7-20: Port Mirroring Tab

Access List

This screen is used to configure the access list settings between wireless and switch ports.

Access List Type - An Access List is a list of source MAC addresses. If a packet is coming from a wireless to a LAN port or vice versa, this device will check if the source MAC address of the packet matches any entry in this list. And use the match result to pass or drop this packet. However, packets from LAN port to LAN port will not be checked. If you click **Disable**, this will disable all access list functions. If you click **Accept**, only packets that match an entry on the list will be passed. All others will be dropped.

Click the **Apply Global Setting** button to save your global settings.

Block - Packets that matches an entry on the list will be dropped. All others will be passed.

Block List - The list of source MAC address that will be blocked when mode is Block.

To block a port, enter the MAC address in the *New Block Entry* field, and click the **Add Block Entry** button. To unblock the port, enter the MAC address in the *New Block Entry* field, and click the **Delete Selected Entry** button.

Pkt Count - the number of packets dropped with this blocked MAC address.

To accept a port, enter the MAC address in the *New Accept Entry* field, and click the **Add Accept Entry** button. To unaccept the port, enter the MAC address in the *New Accept Entry* field, and click the **Delete Accept Entry** button.

Accept List - The list of source mac address which will be accepted when the mode is *Accept*.

Pkt Count - The number of packets accepted with this *Accept* MAC address.

Accept Count - Counter for packets passing through this device when access list is enabled.

Drop Count - Counter for packets dropped by this device when access list is enabled.

Click the **Refresh** button to refresh the screen. Click the **Help** button for additional on-screen information.

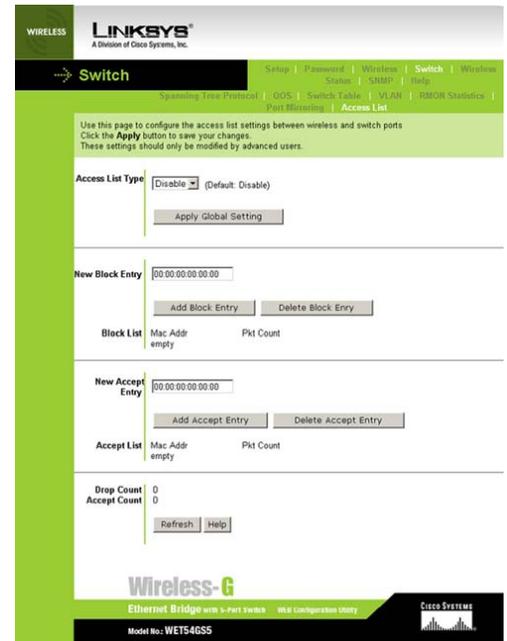


Figure 7-21: Access List Tab

Wireless Status

The *Status* screen displayed the Bridge's current status and settings. All information is read-only.

- Device Name - The name you have assigned to the Bridge is displayed here.
- Firmware Version - The version number of the Bridge's firmware is displayed here.
- MAC Address - The MAC Address of the Bridge is displayed here.

LAN Settings

- IP Address - The Bridge's IP Address is displayed here.
- Subnet Mask - The Bridge's Subnet Mask is displayed here.
- Gateway - The Gateway address for the Bridge is displayed here.

Statistics

- Ethernet TX - The number of packets transmitted to the Ethernet network is displayed here.
- Ethernet RX - The number of packets received from the Ethernet network is displayed here.
- Wireless TX - The number of packets transmitted to the wireless network is displayed here.
- Wireless RX - The number of packets received from the wireless network is displayed here.

Wireless Settings

- SSID - The Bridge's SSID is displayed here.
- Network Type - The Bridge's mode is displayed here.
- Channel - The Bridge's channel setting is displayed here.
- WEP/WPA - The status of the Bridge's security is displayed here.
- TX Rate - The Bridge's transmission rate is displayed here.
- Link Quality - The quality of the Bridge's connection is displayed here.



Figure 7-22: Wireless Status Tab

Wireless-G Ethernet Bridge with 5-Port Switch

Click the **Refresh** button to obtain the most up-to-date settings and statistics. Click the **Help** button for additional on-screen information.

SNMP

This screen is used to configure the SNMP Trap related settings for the Bridge.

SNMP Trap - Use this function to enable or disable snmp trap messages. The trap messages will be sent when there is a cold start, or link state change events.

Trap Community - This is the trap community string sent with the trap message. SNMP manager will use this string to decide if a specific trap message will be received and processed. The default is public.

Click the **Apply Global Setting** button to save your global settings.

New Address Entry - The New IP address destination for this device to send an SNMP trap to.

SNMP Trap Address Table - The list of IP addresses for the SNMP Trap Destination.

To add a new entry, enter the IP address in the *New Address Entry* field, and click the **Add New Entry** button. To delete an entry, select the IP address in the *SNMP Trap Address Table*, and click the **Delete Selected Entry** button.

Click the **Help** button for additional on-screen information.

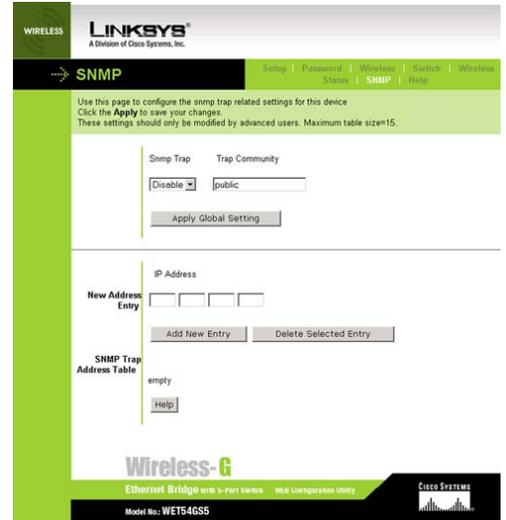


Figure 7-23: SNMP Tab

Help

The *Help* screen offers links to all of the help information for the Web-based Utility's screens and the Bridge's online technical support resources (all information is read-only). You can also upgrade the Bridge's firmware.

- **Linksys Website** - Click the **Linksys Website** link to visit Linksys's website, www.linksys.com.
- **Online manual in PDF format** - Click the **Online manual in PDF format** to view this User Guide on-screen. It is in Adobe Acrobat Portable Document File (.pdf) format, so you will need the free Adobe Acrobat Reader to view the pdf. If you do not have the Reader, click the **Adobe Website** link to download it.
- **Adobe Website** (software for viewing PDF documents) - If you need to download the Adobe Acrobat Reader to view the User Guide pdf, then click the **Adobe Website** link.
- **Firmware Upgrade** - The version number of the Bridge's firmware is displayed here. Firmware updates are posted at www.linksys.com. Firmware should be upgraded **ONLY** if you experience problems with the Bridge.

To upgrade the firmware, follow these instructions:

1. Download the Bridge's firmware upgrade file from the Linksys website, www.linksys.com. Then extract the file.
2. On the *Help* screen, click the **Firmware Upgrade** button.
3. The screen shown in Figure 7-25 will appear. In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.
4. After you have selected the appropriate file, click the **Upgrade** button, and follow the on-screen instructions.



NOTE: If you upgrade the Bridge's firmware, you may lose its configuration settings.

Figure 7-24: Help Tab



Figure 7-25: Firmware Upgrade

Appendix A: Troubleshooting

This appendix consists of two parts: “Common Problems and Solutions” and “Frequently Asked Questions.” This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Ethernet Bridge. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

Common Problems and Solutions

1. *I can't connect to the access point.*

Open the Web-based Utility. On the Setup tab, perform the following steps:

- Verify that the operating mode is set to Infrastructure mode.
- Make sure that the SSID is the same as the SSID of the access point.
- On the *WEP Encryption* screen, make sure that all of the WEP settings are the same as the WEP settings of the access point.

2. *I want to play head-to-head (ad-hoc) gaming with two Xboxes, but they won't communicate.*

Perform the following steps:

- Make sure both Bridges are set to the same SSID, network mode (Ad-Hoc), channel setting, and WEP settings.
- Verify that the Bridges are set to different IP addresses.
- You need to enable MAC address cloning on the Bridge for each Xbox. Follow these instructions:
 1. Open the Web-based Utility for one of the Bridges.
 2. Click the **Wireless** tab.
 3. Select **Enable** from the *MAC Address Cloning Mode* drop-down menu.
 4. Click the **Auto** radio button.
 5. Click the **Apply** button to save your changes. When you connect the Bridge to the Xbox, the Bridge will automatically clone the Xbox's MAC address. Make sure that the Xbox is connected to Port 1.
- Repeat steps 1-5 for the other Bridge.

3. *I don't know how to change the Bridge's IP address.*

You have two ways to change the Bridge's IP address.

- Open the Web-based Utility. On the *Setup* screen, click the **Static IP Address** radio button, and change the IP address there.
- If you encounter problems, power the Bridge off and on again, or push the Reset button. Then try to change the IP address again.

4. The Bridge-enabled PC won't communicate with a wireless-enabled PC or printer.

Perform the following steps:

- Check that the wireless-enabled PC or printer is on the same wireless network as the PC using the Bridge.
- Make sure that the SSID and network mode are the same for all devices connected to the same wireless network.
- If the wireless LAN settings are okay, make sure that all the devices are on the same IP network.

5. The Web-based Utility won't open.

Make sure you correctly entered the Bridge's IP address in the *Address* field of your web browser. If you are not sure what the Bridge's IP address is, then run the Setup Wizard. Follow the on-screen instructions until you see a screen that lists all the Wireless-G Ethernet Bridges on your network. Select the Bridge you want to access, and its IP address will appear in the Status box. Enter this IP address in your web browser's *Address* field. For details, refer to "Chapter 5: Setting Up the Wireless-G Ethernet Bridge."

6. The Web-based Utility does not recognize my password.

The password is case-sensitive. Make sure that you are using the correct case(s) when entering the password. If you forget your password, you can push the Bridge's Reset button. This will reset the password to the default setting; however, all other Bridge settings will be reset to the factory defaults as well. To use the default setting, enter **admin** in the *Password* field.

7. After I make changes through the Web-based Utility, the new settings aren't displayed on-screen.

Click the **Refresh** button of your web browser. If the new settings aren't displayed, then unplug the power adapter from the Bridge. Plug the power adapter back in, and then click the **Refresh** button again.

Frequently Asked Questions

What is the IEEE 802.11g standard?

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

What is the IEEE 802.11b standard?

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

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

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

Can I play multiplayer games with other users of the wireless network?

Yes, as long as the game supports multiple players over a LAN. Refer to the game's user guide for more information.

What is ad-hoc mode?

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

What is infrastructure mode?

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

What is roaming?

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

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

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

What is ISM band?

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

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

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

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

Would the information be intercepted while transmitting on air?

Linksys products feature two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, Linksys products offer the encryption function (WEP) to enhance security and access control. Users can set it up depending upon their needs.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40/64 bit shared key algorithm, as described in the IEEE 802.11 standard.

Appendix B: Wireless Security

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

Security Precautions

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

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

For information on implementing these security features, refer to “Chapter 7: Using the Wireless-G Ethernet Bridge Web-based Utility.” The wireless security can be set up on this page.

Security Threats Facing Wireless Networks

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

Change the administrator’s password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator’s password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator’s password regularly.



Note: Some of these security features are available only through the network router or access point. Refer to the router or access point’s documentation for more information.

Wireless-G Ethernet Bridge with 5-Port Switch

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

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you the encryption method TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP or WEP.



Important: Always remember that each device in your wireless network **MUST** use the same encryption method and encryption key or your wireless network will not function properly.

Wireless-G Ethernet Bridge with 5-Port Switch

WPA Pre-Shared Key. If you do not have a RADIUS server, enter a password in the Pre-Shared key field of 8-64 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Router or other device how often it should change the encryption keys.

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, select a WEP key and a level of WEP encryption, and either generate a WEP key through the Passphrase or enter the WEP key manually.

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

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

Appendix C: Upgrading Firmware

You can use the Bridge's Web-based Utility to upgrade the firmware; however, firmware should be upgraded **ONLY** if you experience problems with the Bridge.

To upgrade the Bridge's firmware, follow these instructions:

1. Download the Bridge's firmware upgrade file from the Linksys website, www.linksys.com.
2. Extract the file on your computer.
3. Open the Bridge's Web-based Utility, and click the **Help** tab.
4. On the *Help* screen, click the **Firmware Upgrade** button.
5. The screen shown in Figure C-1 will appear. In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.
6. After you have selected the appropriate file, click the **Upgrade** button, and follow the on-screen instructions.



NOTE: If you upgrade the Bridge's firmware, you may lose its configuration settings.



Figure C-1: Firmware Upgrade

Appendix D: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Appendix E: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

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

Adapter - A device that adds network functionality to your PC.

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

AES (Advanced Encryption Standard) - A method that uses up to 256-bit key encryption to secure data.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

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

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

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

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

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

Wireless-G Ethernet Bridge with 5-Port Switch

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

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

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

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data collisions.

CTS (Clear To Send) - A signal sent by a wireless device, signifying that it is ready to receive data.

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

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

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

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

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

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

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

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

DSSS (Direct-Sequence Spread-Spectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

Wireless-G Ethernet Bridge with 5-Port Switch

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

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

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

EAP-PEAP (Extensible Authentication Protocol-Protected Extensible Authentication Protocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data transmitted in a network.

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

Finger - A program that tells you the name associated with an e-mail address.

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

Firmware - The programming code that runs a networking device.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

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

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

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

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

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

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

Wireless-G Ethernet Bridge with 5-Port Switch

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

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

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

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

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

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

ISM band - Radio bandwidth utilized in wireless transmissions.

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

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

LEAP (Lightweight Extensible Authentication Protocol) - A mutual authentication method that uses a username and password system.

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

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

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

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

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

NNTP (Network News Transfer Protocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

Wireless-G Ethernet Bridge with 5-Port Switch

OFDM (Orthogonal Frequency Division Multiplexing) - Frequency transmission that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel to prevent information from being lost in transit.

Packet - A unit of data sent over a network.

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

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

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

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

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

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

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

Preamble - Part of the wireless signal that synchronizes network traffic.

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

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

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

Router - A networking device that connects multiple networks together.

RTS (Request To Send) - A networking method of coordinating large packets through the RTS Threshold setting.

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

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

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

Wireless-G Ethernet Bridge with 5-Port Switch

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

SOHO (Small Office/Home Office) - Market segment of professionals who work at home or in small offices.

SPI (Stateful Packet Inspection) Firewall - A technology that inspects every incoming packet of information before allowing it to enter the network.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

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

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

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

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

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

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

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

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

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

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

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

Wireless-G Ethernet Bridge with 5-Port Switch

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

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

Upload - To transmit a file over a network.

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

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

WAN (Wide Area Network)- The Internet.

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

WINIPCFG - A Windows 98 and Me utility that displays the IP address for a particular networking device.

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

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

Appendix F: Specifications

Model	WET54GS5
Standards	IEEE 802.3, 802.3u, 802.11g, 802.11b, 802.1Q, 802.1d, 802.1p
Ports	5 10/100 Ports with Auto MDI/MDIX support, Power
Buttons	Reset Button
Cabling Type	Category 5 or better
LEDs	Power, Diag, Wireless-G Link, Wireless-G Act, 1-5
Transmit Power	802.11g: Typical 12 ± 1 dBm @ Normal Temp Range, 802.11b: Typical 16 ± 1 dBm @ Normal Temp Range
Security Feature	Wired Equivalent Privacy, also supports PSK-TKIP and RADIUS (not an authenticator for connected nodes, only for the Bridge itself)
WEP Key Bits	64 and 128-bit
Protocols	802.11b: CCK (11Mbps), CCK (5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps) 802.11g: OFDM (54Mbps)
Dimensions	5.20" x 1.14" x 5.12" (132 mm x 29 mm x 130 mm)
Unit Weight	13.6 oz. (0.39 kg)
Power	5V DC 2A
Certifications	FCC Class B, CE Class B, VCCI Class B

Wireless-G Ethernet Bridge with 5-Port Switch

Operating Temp.	32°F to 104°F (0°C to 40°C)
Storage Temp.	-4°F to 158°F (-20°C to 70°C)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing
Warranty	1 Year Limited Warranty

Appendix G: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix H: Regulatory Information

FCC Statement

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

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

FCC Radiation Exposure Statement

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

Industry Canada (Canada)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

Appendix I: Contact Information

Need to contact Linksys?

Visit us online for information on the latest products and updates to your existing products at:

<http://www.linksys.com> or
[ftp.linksys.com](ftp://ftp.linksys.com)

Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:
Or fax your request in to:

800-546-5797 (LINKSYS)
949-261-8868

If you experience problems with any Linksys product, you can call us at:

800-326-7114
support@linksys.com

Don't wish to call? You can e-mail us at:

If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at:
(Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)

949-261-1288