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.

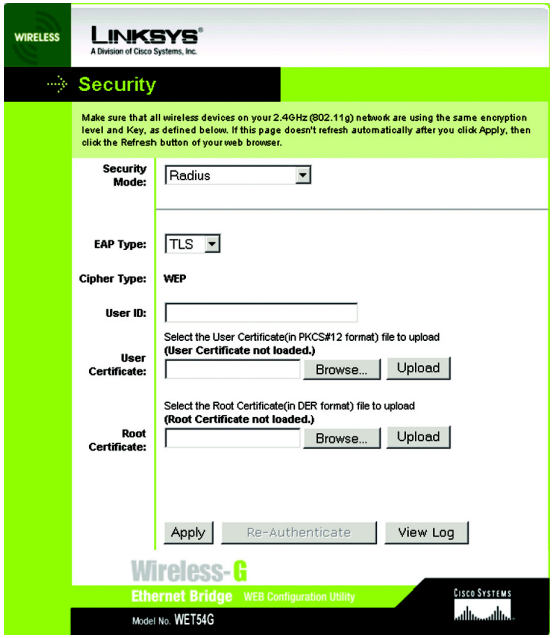

Figure 7-9: RADIUS-TLS

TLS (Transport **L**ayer **S**ecurity) - A mutual authentication method that uses digital certificates.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

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.

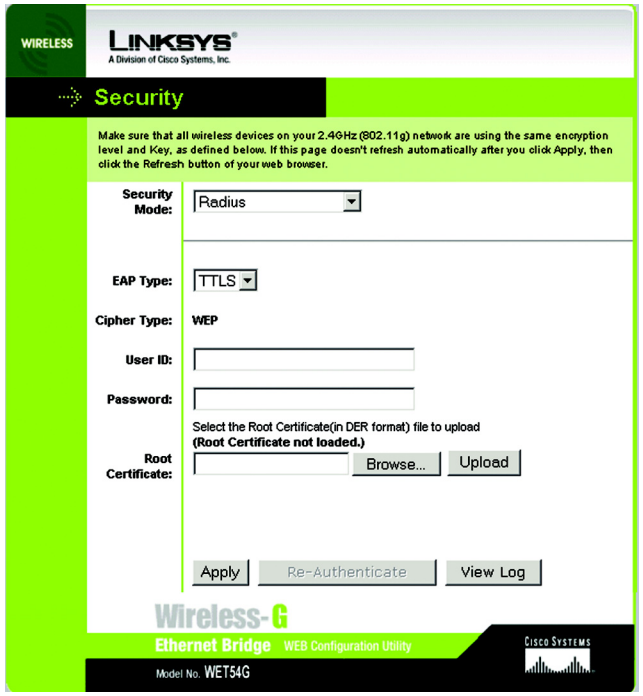

Figure 7-10: RADIUS-TTLS

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.

Password

The *Password* screen, shown in Figure 7-11, lets you change the Bridge's Password and restore the factory default settings.

- 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.

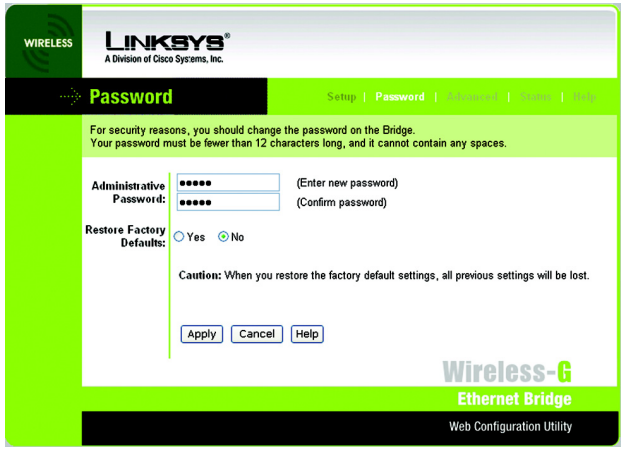

Figure 7-11: Password Tab

Advanced Settings

Use the *Advanced Settings* screen, shown in Figure 7-12, to customize advanced wireless settings and clone a MAC address onto the Bridge.

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

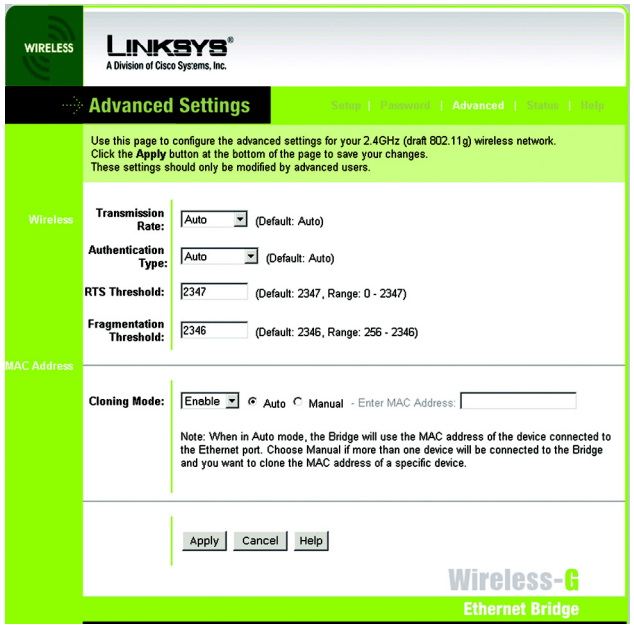

Figure 7-12: Advanced Settings Tab

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 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 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 a switch or a hub.

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.

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. Firmware updates are posted at www.linksys.com. Firmware should be upgraded ONLY if you experience problems with the Bridge. To upgrade the Bridge's firmware, use the ***Help*** screen.
- 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.

LAN 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.
- Security- The status of the Bridge's security is displayed here.
- TX Rate - The Bridge's transmission rate is displayed here.

Figure 7-13: Status Tab

- Link Quality - The quality of the Bridge's connection is displayed here.

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

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.(See Figure 7-14.)

- 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 7-15 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.

Figure 7-14: Help Tab

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

Figure 7-15: 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 **Advanced** 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 its Xbox, the Bridge will automatically clone the Xbox's MAC address.
   - 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 Setup."

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.

Security Threats Facing Wireless Networks

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

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

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

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you one 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.

WPA Pre-Shared Key. If you do not have a RADIUS server, Select the type of algorithm, TKIP, and 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 - 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 - This is 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.

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 - The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Bit - A binary digit.

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

Bridge - A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet network.

Broadband - An always-on, fast Internet connection.

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

Buffer - A block of memory that temporarily holds data to be worked on later when a device is currently too busy to accept the data.

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 loss in a network.

CTS (Clear To Send) - A signal sent by a device to indicate 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) - The capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name.

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

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

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) - A type of radio transmission technology that includes a redundant bit pattern to lessen the probability of data lost during transmission. Used in 802.11b networking.

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.

Encryption - Encoding data to prevent it from being read by unauthorized people.

Ethernet - An 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 - Security measures that protect the resources of a local network from intruders.

Firmware - 1. In network devices, the programming that runs the device. 2. Programming loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

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 standard protocol for sending files between computers over a TCP/IP network and the Internet.

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

Gateway - A system that interconnects networks.

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.

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

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network 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 band used in wireless networking transmissions.

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

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

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.

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.

OFDM (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

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 protocol used to retrieve e-mail stored on a mail server.

Port - 1. The connection point on a computer or networking device used for plugging in a cable or an adapter. 2. The virtual connection point through which a computer uses a specific application on a server.

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.

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, such as a local network and the Internet.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

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.

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

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. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

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

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 uses UDP and has no directory or password capability.

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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 data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Millennium 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.

Appendix F: Specifications

Model	WET54GS5
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Ports	One 10/100 Auto-Cross Over (MDI/MDI-X) Port, Power Port
Buttons	Reset Button
Cabling Type	Category 5 or better
LEDs	Power, Ethernet, Wireless-G
Transmit Power	16 ± 1 dBm @ 11Mbps CCK 12 ± 1 dBm @ 54Mbps OFDM
Security Feature	WEP Encryption, WPA, RADIUS
WEP Key Bits	64/128-bit
Protocols	802.11b: CCK (11Mbps), CCK (5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps) 802.11g: OFDM (54Mbps)
Dimensions	4.96" x 1.06" x 4.21" (126 mm x 27 mm x 107 mm)
Unit Weight	8.50 oz. (0.24 kg)
Power	5V DC
Certifications	FCC, CE
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	3 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

CANADA (INDUSTRY)
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.

EC DECLARATION OF CONFORMITY (EUROPE)
Linksys declares that the Wireless-G ADSL Gateway conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:
EN 301 489-1, 301 489-17 General EMC requirements for Radio equipment.
EN 609 50 Safety

The equipment version marketed in US is restricted to usage of the channels 1-11 only

EN 300-328-1, EN 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

Linksys vakuuttaa täten että Wireless-G ADSL Gateway tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys Group déclare la Passerelle ADSL sans fil-G est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

Belgique:

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

France:

2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le département. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

SAFETY NOTICES

Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.

Do not use this product near water, for example, in a wet basement or near a swimming pool.
Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

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
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: Don't wish to call? You can e-mail us at:	800-326-7114 support@linksys.com
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