LINKSYS®
A Division of Cisco Systems, Inc.

2.4GHz 802.11g

Wireless-G

Cable Gateway

User Guide

WIRELESS

Model No. **WCG200**

CISCO SYSTEMS

Copyright and Trademarks

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

How to Use this Guide

Your Guide to the Wireless-G Cable Gateway has been designed to make understanding networking with the Gateway easier than ever. Look for the following items when reading this User Guide:

This checkmark means there is a Note of interest and is something you should pay special attention to while using the Gateway.

This exclamation point means there is a Caution or Warning and is something that could damage your property or the Gateway.

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

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

List of Figures

Chapter 1: Introduction

Welcome

The Linksys Wireless-G Cable Gateway is the all-in-one solution for Internet connectivity in your home. The Cable Modem function gives you a blazing fast connection to the Internet, far faster than a dial-up, and without tying up your phone line.

How does the Wireless-G Cable Gateway do all of this? A gateway is a device that allows access to a cable Internet connection over a network. With the Gateway, this access can be shared to wireless clients at either up to 11Mbps for Wireless-B or up to 54Mbps for Wireless-G. In addition, the WPA standard provides greater security opportunities while the whole network is protected through a Stateful Packet Inspection (SPI) firewall and NAT technology.

The Gateway's firewall protects your network of PCs so users on the public, Internet side cannot "see" your PCs. This is how your local network remains private. The Gateway protects your network by inspecting the first packet coming in through the Cable port before delivery to the final destination in the local network. The Gateway inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, will forward the packet to the appropriate PC on the LAN side. All of these security features, as well as full configurability, are accessed through the easy-to-use browser-based utility.

You can also connect your computer to the Wireless-G Cable Gateway via USB, or use the built-in 4-port 10/100 Ethernet Switch to start your home network. You can connect four PCs directly, or daisy-chain out to more hubs and switches to create as big a network as you need.

But what does all of this mean?

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

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

PCs equipped with wireless cards and adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wired Local Area Network. The access point bridges wireless networks of both 802.11b and 802.11g standards and wired networks.

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

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

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

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

Use the instructions in this Guide to help you connect the Gateway, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Gateway.

What's in this Guide?

- Chapter 1: Introduction
  This chapter describes the Wireless-G Cable Gateway applications and this User Guide.

- Chapter 2: Planning Your Network
  This chapter describes the basics of networking.

- Chapter 3: Getting to Know the Wireless-G Cable Gateway
  This chapter describes the physical features of the Gateway.

- Chapter 4: Connecting the Wireless-G Cable Gateway
  This chapter instructs you on how to connect the Gateway to your network.

- Chapter 5: Configuring the Wireless-G Cable Gateway
  This chapter explains how to use the Web-based Utility to configure the settings on the Gateway.

- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G Cable Gateway.

- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.

- Appendix C: Finding the MAC Address and IP Address for your Ethernet Adapter
  This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Gateway.

- Appendix D: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.

- Appendix E: Specifications
  This appendix provides the technical specifications for the Gateway.

- Appendix F: Warranty Information
  This appendix supplies the warranty information for the Gateway.

- Appendix G: Regulatory Information
  This appendix supplies the regulatory information regarding the Gateway.

- Appendix H: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Network

The Gateway's Functions

A Gateway is a network device that connects two networks together.

In this instance, the Gateway connects your Local Area Network (LAN), or the group of computers in your home or office, to the Internet. The Gateway processes and regulates the data that travels between these two networks.

The Gateway's NAT feature protects your network of computers so users on the public, Internet side cannot "see" your computers. This is how your network remains private. The Gateway protects your network by inspecting every packet coming in through the Internet port before delivery to the appropriate computer on your network. The Gateway inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate computer on the LAN side.

Remember that the Gateway's ports connect to two sides. The LAN ports connect to the LAN, and the Cable port connects to the Internet. The LAN ports transmit data at 10/100Mbps.

Figure 2-1: Network

IP Addresses

What's an IP Address?

IP stands for Internet Protocol. Every device on an IP-based network, including computers, print servers, and Gateways, requires an IP address to identify its "location," or address, on the network. This applies to both the Internet and LAN connections. There are two ways of assigning an IP address to your network devices. You can assign static IP addresses or use the Gateway to assign IP addresses dynamically.

Static IP Addresses

A static IP address is a fixed IP address that you assign manually to a computer or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses must be unique and are commonly used with network devices such as server computers or print servers.

NOTE: Since the Gateway is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address."

Since the Gateway uses NAT technology, the only IP address that can be seen from the Internet for your network is the Gateway's Internet IP address. However, even this Internet IP address can be blocked, so that the Gateway and network seem invisible to the Internet—see the Block WAN Requests description under Security in "Chapter 5: Configuring the Gateway."

***static ip address**: a fixed address assigned to a computer or device that is connected to a network.*

Since you use the Gateway to share your cable Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Gateway. You can get that information from your ISP.

Dynamic IP Addresses

A dynamic IP address is automatically assigned to a device on the network, such as computers and print servers. These IP addresses are called "dynamic" because they are only temporarily assigned to the computer or device. After a certain time period, they expire and may change. If a computer logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will automatically assign it a new dynamic IP address.

dynamic ip address*: a temporary IP address assigned by a DHCP server.*

DHCP (Dynamic Host Configuration Protocol) Servers

Computers and other network devices using dynamic IP addressing are assigned a new IP address by a DHCP server. The computer or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

A DHCP server can either be a designated computer on the network or another network device, such as the Gateway. By default, the Gateway's DHCP Server function is enabled.

If you already have a DHCP server running on your network, you must disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Gateway, see the DHCP section in "Chapter 5: Configuring the Gateway."

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.*

Chapter 3: Getting to Know the Wireless-G Cable Gateway

The Back Panel

The Gateway's buttons and ports, where network cables are connected, are located on the back panel.

Figure 3-1: Back Panel

On/Off Switch This switch is used for turning the Gateway on and off.

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

Reset Press this button and hold it in for five seconds to restore the Gateway to its factory default settings.

Ports 1-4 These four ports are used to connect network devices, such as PCs, print servers, and remote hard drives to your local area network (LAN).

USB This is where you can use a USB cable to connect the Gateway.

Cable The Cable port is where you will connect your coaxial Cable line.

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

The Front Panel

The Gateway's LEDs, which displays information about network activity, are located on the front panel.

Figure 3-2: Front Panel

Power Green or red. The green Power LED is solidly lit when the Gateway is powered on. If the LED lights up red, there is an error.

Internet, DS Green. The DS (Downstream) LED lights up and flashes when the Gateway is trying to lock on a downstream signal. The LED stays solidly lit when it has locked on the signal.

Internet, US Green. The US (Upstream) LED lights up and flashes when the Gateway is trying to lock on an upstream signal. The LED stays solidly lit when it has locked on the signal.

Internet, Online Green. The Online LED flashes when the Gateway is establishing a connection to your cable ISP. It is solidly lit when the Gateway is synchronized with your cable ISP.

Ethernet-1-4 Green or red. Ethernet 1-4 LED serves multiple purposes. If the LED is solid green, the Gateway is successfully connected to a device through the corresponding port (1, 2, 3, or 4). If the LED is flashing green, the Gateway is actively sending or receiving data over that port. If the LED lights up red, there is a collision.

USB Green or red. The LED is solid green when a PC is connected to the Gateway via USB, and drivers are installed. If the LED flashes red, the cable is connected, but the driver isn't loaded.

Wireless Green or red. The LED flashes green during wireless activity. If the LED flashes red, there is an error.

NOTE: If the US and DS LEDs are flashing, the Gateway is still operating, but your Internet service has been disabled by your Internet Service Provider (ISP).

NOTE: If the US, DS, and Online LEDs are flashing, the Gateway is performing a self-test.

Chapter 4: Connecting the Wireless-G Cable Gateway

Overview

To set up the Gateway, you will have to connect the Gateway to your Cable line, computers, and other network devices, as well as configure the Gateway with setting(s) provided by your Internet Service Provider (ISP).

The installation technician from your ISP should have left the setup information for the Gateway with you after installing your broadband connection. If not, you can call your ISP to request that data.

After you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Gateway.

If you want to use a computer with an Ethernet adapter to configure the Gateway, continue to "Wired Ethernet Connection to a Computer." If you want to use a computer with a wireless adapter to configure the Gateway, continue to "Wireless Connection to a Computer." If you want to use a USB connection to configure the Gateway, continue to "Wired USB Connection to a Computer."

Wired Ethernet Connection to a Computer

1. Before you begin, make sure that all of your network's hardware is powered off, including the Gateway and all computers.

2. Connect the coaxial cable from your ISP or cable company to the Cable port on the back panel of the Gateway. (The other end of the coaxial cable should be connected according to the cable company's instructions.)

Figure 4-1: Cable Connection

3. Connect one end of an Ethernet network cable to one of the Ethernet ports (labeled 1-4) on the back of the Gateway, and the other end to an Ethernet port on a computer. Repeat this step to connect more computers, a switch, or other network devices to the Gateway.

NOTE: If your PC's Ethernet adapter is not set up, please refer to your Ethernet adapter's documentation for more information.

4. Connect the power adapter to the Gateway's Power port, and then plug the power adapter into a power outlet.

5. Turn the On/Off switch to **On**.

IMPORTANT: Make sure to contact your Cable ISP with the Gateway's MAC address after the Gateway is powered on, so they can activate your account or you will not have Internet access.

6. Contact your Cable ISP to activate your account. Your Cable ISP will need what is called a MAC Address for the cable modem capability of the Gateway in order to set up your account. The 12-digit modem MAC address is printed on a bar code label on the bottom of the Gateway. Once you have given them this number, your Cable ISP should be able to activate your account.

   The Online LED flashes when the Gateway is establishing a connection to your cable ISP. When the Cable is synchronized with your cable ISP, the LED will be solidly lit.

7. Then, turn on the PC that you want to use to configure the Gateway.

The Gateway's hardware installation is now complete. Go to "Chapter 5: Configuring the Gateway."

Figure 4-2: Ethernet Connection

Figure 4-3: Power Connection

NOTE: You should always plug the Gateway's power adapter into a power strip with surge protection.

Wireless Connection to a Computer

If you want to use a wireless connection to access the Gateway, follow these instructions:

1. Before you begin, make sure that all of your network's hardware is powered off, including the Gateway and all computers.
2. Connect the coaxial cable that is provided by your cable service provider to the Cable port that is on the back of the Gateway.
3. Connect the power adapter to the Gateway's Power port, and then plug the power adapter into a power outlet.
4. Turn the On/Off switch to **On**.

IMPORTANT: Make sure to contact your Cable ISP with the Gateway's MAC address after the Gateway is powered on, so they can activate your account or you will not have Internet access.

5. Contact your Cable ISP to activate your account. Your Cable ISP will need what is called a MAC Address for the cable modem capability of the Gateway in order to set up your account. The 12-digit modem MAC address is printed on a bar code label on the bottom of the Gateway. Once you have given them this number, your Cable ISP should be able to activate your account.

   The Online LED flashes when the Gateway is establishing a connection to your cable ISP. When the Cable is synchronized with your cable ISP, the LED will be solidly lit.

6. Then, turn on the PC that you want to use to configure the Gateway.
7. For initial access to the Gateway through a wireless connection, make sure the computer's wireless adapter has its SSID set to **linksys** (the Gateway's default setting), and its encryption is disabled. After you have accessed the Gateway, you can change the Gateway and this computer's adapter settings to match the your usual network settings.

NOTE: If the Gateway was provided to you by your Cable ISP, it may require different wireless settings. If you're experiencing problems connecting wirelessly, you may need to connect to the Gateway with a wired connection so you can change the settings.

The Gateway's hardware installation is now complete. Go to "Chapter 5: Configuring the Gateway."

Figure 4-4: Cable Connection

Figure 4-5: Power Connection

NOTE: After configuration, you should always change the SSID from its default, **linksys**, and enable encryption.

Wired USB Connection to a Computer

First, make sure that all the devices that you'll be working with are powered down, including your PCs and the Gateway.

1. Connect the coaxial cable that is provided by your cable service provider to the Cable port that is on the back of the Gateway.
2. Connect one end of a USB cable to your PC's USB port and connect the other end of the USB cable to the USB port on the back of the Gateway.
3. Connect the power adapter to the Gateway. Plug the other end of the power adapter into the electrical outlet, preferably a surge protector.
4. Turn on the Gateway. Then, turn on your PC.
5. During the boot-up process, your computer should recognize the device and ask for driver installation.
6. Next, you will need to install the USB driver. Continue to the section for your Windows operating system.

Figure 4-6: Cable Connection

Figure 4-7: USB Connection

Figure 4-8: Power Connection

Installing the USB Drivers for Windows 98

1. When the *Add New Hardware Wizard* window appears, insert the Setup CD into your CD-ROM drive and click **Next**.

Figure 4-9: Add New Hardware Wizard

2. Select **Search for the best driver for your device (Recommended)** and click the **Next** button.

Figure 4-10: Search for Driver

3. Select **CD-ROM drive** as the only location where Windows will search for the driver software and click the **Next** button.

Figure 4-11: CD-ROM Drive

4. Windows will notify you that it has identified multiple drivers. Select **The updated driver (Recommended)** as the appropriate driver. Click the **Next** button.

Figure 4-12: Select Updated Driver

5. Windows is now ready to install the driver. Click the **Next** button.

6. Windows will begin installing the driver for the Gateway. At this point, the installation may require files from your Windows 98 CD-ROM. If prompted, insert your Windows 98 CD-ROM into your CD-ROM drive and enter **d:\win98** in the box that appears (if "d" is the letter of your CD-ROM drive). If you were not supplied with a Windows 98 CD-ROM, your Windows files may have been placed on your hard drive by your computer manufacturer. While the location of these files may vary, many manufacturers use c:\windows\options\cabs as the path. Try entering this path into the box. If no files are found, check your computer's documentation or contact your computer manufacturer for more information.

Figure 4-13: Install Driver

7. After Windows has completed installing this driver, click **Finish**.

8. When asked if you want to restart your PC, remove all CD-ROMs from the PC and click **Yes**. If Windows does not ask you to restart your PC, click the **Start** button, choose **Shut Down**, choose **Restart**, and then click **Yes**.

9. The Windows 98 driver installation is complete.

IMPORTANT: Make sure to contact your Cable ISP with the Gateway's MAC address after the Gateway is powered on, so they can activate your account or you will not have Internet access.

10. Contact your Cable ISP to activate your account. Your Cable ISP will need what is called a MAC Address for the cable modem capability of the Gateway in order to set up your account. The 12-digit modem MAC address is printed on a bar code label on the bottom of the Gateway. Once you have given them this number, your Cable ISP should be able to activate your account.

    The Online LED flashes when the Gateway is establishing a connection to your cable ISP. When the Cable is synchronized with your cable ISP, the LED will be solidly lit.

The Gateway's hardware installation is now complete. Go to "Chapter 5: Configuring the Gateway."

Figure 4-14: Driver Installation Complete

Installing the USB Driver for Windows Millennium

1. Start up your PC in Windows Millennium. Windows will detect new hardware connected to your PC. Insert the Setup CD into your CD-ROM drive.

Figure 4-15: New Hardware Found

2. Select **Automatic search for a better driver (Recommended)** and click the **Next** button.

3. Windows will begin installing the driver for the modem. At this point, the installation may require files from your Windows Millennium CD-ROM. If prompted, insert your Windows Millennium CD-ROM into your CD-ROM drive and enter **d:\win9x** in the box that appears (if "d" is the letter of your CD-ROM drive). If you were not supplied with a Windows CD-ROM, your Windows files may have been placed on your hard drive by your computer manufacturer. While the location of these files may vary, many manufacturers use c:\windows\options\install as the path. Try entering this path into the box. If no files are found, check your computer's documentation or contact your computer manufacturer for more information.

Figure 4-16: Search for Driver

4. When Windows finishes installing the driver, click **Finish**.

5. When asked if you want to restart your PC, remove all CD-ROMs from the PC and click **Yes**. If Windows does not ask you to restart your PC, click the **Start** button, choose **Shut Down**, choose **Restart**, and then click **Yes**.

6. The Windows Millennium driver installation is complete.

IMPORTANT: Make sure to contact your Cable ISP with the Gateway's MAC address after the Gateway is powered on, so they can activate your account or you will not have Internet access.

7. Contact your Cable ISP to activate your account. Your Cable ISP will need what is called a MAC Address for the cable modem capability of the Gateway in order to set up your account. The 12-digit modem MAC address is printed on a bar code label on the bottom of the Gateway. Once you have given them this number, your Cable ISP should be able to activate your account.

   The Online LED flashes when the Gateway is establishing a connection to your cable ISP. When the Cable is synchronized with your cable ISP, the LED will be solidly lit.

Figure 4-17: Driver Installation Complete

The Gateway's hardware installation is now complete. Go to "Chapter 5: Configuring the Gateway."

Installing the USB Driver for Windows 2000

1. Start up your PC. Windows will notify you that it has detected new hardware. Insert the Setup CD into the CD-ROM drive.

Figure 4-18: Found New Hardware

2. When the *Welcome to the Found New Hardware Wizard* screen appears to confirm that the device has been identified by your PC, click **Next**.

Figure 4-19: Welcome

3. Select **Search for a suitable driver for my device (recommended)** and click the **Next** button.

Figure 4-20: Search for Driver

4. Windows will now search for the driver software. Select only **CD-ROM drives** and click the **Next** button.

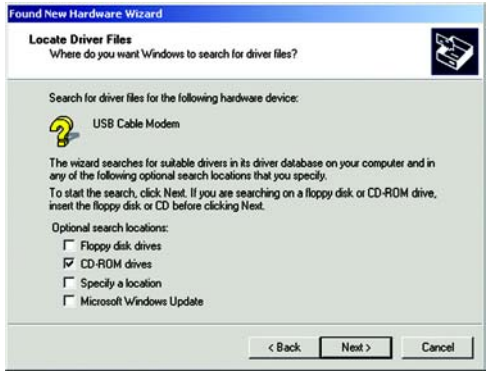

Figure 4-21: CD-ROM Drives

5. Windows will notify you that it has located the appropriate driver and is ready to install it. Click the **Next** button.

Figure 4-22: Driver Located

6. When Windows has completed installing the driver, click the **Finish** button.

7. The Windows 2000 driver installation is complete.

IMPORTANT: Make sure to contact your Cable ISP with the Gateway's MAC address after the Gateway is powered on, so they can activate your account or you will not have Internet access.

8. Contact your Cable ISP to activate your account. Your Cable ISP will need what is called a MAC Address for the cable modem capability of the Gateway in order to set up your account. The 12-digit modem MAC address is printed on a bar code label on the bottom of the Gateway. Once you have given them this number, your Cable ISP should be able to activate your account.

   The Online LED flashes when the Gateway is establishing a connection to your cable ISP. When the Cable is synchronized with your cable ISP, the LED will be solidly lit.

Figure 4-23: Driver Installation Complete

The Gateway's hardware installation is now complete. Go to "Chapter 5: Configuring the Gateway."

Installing the USB Driver for Windows XP

1. Start up your PC. Windows will notify you that it has detected new hardware. Insert the Setup CD into the CD-ROM drive.

Figure 4-24: Found New Hardware

2. When the *Welcome to the Found New Hardware Wizard* screen appears to confirm that the device has been identified by your PC, click the **Next** button.

Figure 4-25: Welcome

3. Windows will now search for the driver software.

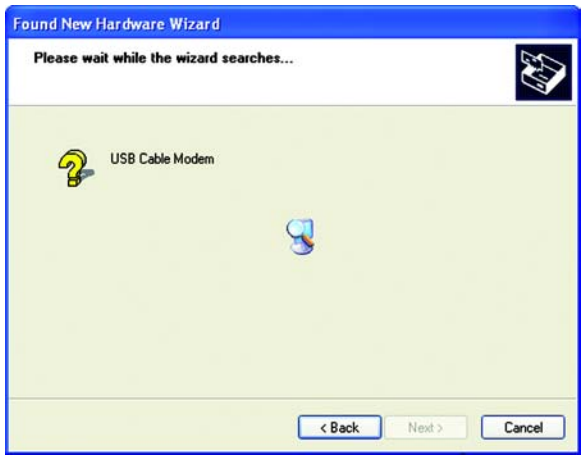

Figure 4-26: Searching for Driver

4. When Windows has completed installing the driver, click the **Finish** button.

5. The Windows XP driver installation is complete.

IMPORTANT: Make sure to contact your Cable ISP with the Gateway's MAC address after the Gateway is powered on, so they can activate your account or you will not have Internet access.

6. Contact your Cable ISP to activate your account. Your Cable ISP will need what is called a MAC Address for the cable modem capability of the Gateway in order to set up your account. The 12-digit modem MAC address is printed on a bar code label on the bottom of the Gateway. Once you have given them this number, your Cable ISP should be able to activate your account.

   The Online LED flashes when the Gateway is establishing a connection to your cable ISP. When the Cable is synchronized with your cable ISP, the LED will be solidly lit.

The Gateway's hardware installation is now complete. Go to "Chapter 5: Configuring the Gateway."

Figure 4-27: Driver Installation Complete

Chapter 5: Configuring the Wireless-G Cable Gateway

Overview

Follow the steps in this chapter and use the Gateway's web-based utility to configure the Gateway. This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Gateway. For a basic network setup, most users only have to use the following screens of the Utility:

- Setup. On the Setup screen, enter the settings provided by your ISP.
- Security. Click the **Administration** tab and then the **Security** tab. The Gateway's default username and password is admin. To secure the Gateway, change the Password from its default.

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

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

NOTE: For added security, you should change the password through the Administration tab.

Setup

- Setup. Enter the Internet connection settings on this screen.

NOTE: Depending on your service provider, some features and functions in the Web-based Utility may not be available or may perform differently than described in the User Guide.

Wireless

- Basic Wireless Settings. You can choose your wireless network settings on this screen.
- Wireless Security. This screen allows you to choose your wireless security mode.
- Wireless Network Access. This screen displays your wireless network access list.
- Advanced Wireless Settings. On this screen you can access the advanced wireless features.
- WDS. The wireless distribution system feature is accessed on this screen.

Security

- Firewall. This screen contains filters and the Block WAN Requests feature. Filters block specific internal users from accessing the Internet and block anonymous Internet requests.
- VPN Passthrough. To enable or disable IPSec and/or PPTP Passthrough, use this screen.

Access Restrictions

- Website Blocking. You are allowed to filter website access on this screen.
- Timed Access. This screen allows you to limit the days or hours of access to the network.
- Filter Internet Traffic. You can filter or block ports from Internet access by IP address or port range on this screen.

Applications & Gaming

- Port Range Forwarding. To set up public services or other specialized Internet applications on your network, click this tab.
- Port Triggering. To set up triggered ranges and forwarded ranges for Internet applications, click this tab.
- DMZ. To allow one local user to be exposed to the Internet for use of special-purpose services, use this screen.

Administration

- Security. On this screen, alter Gateway access privileges, UPnP settings, Reporting settings, and Log settings.
- Diagnostics. Use this screen to do a Ping Test.
- Factory Defaults. If you want to restore the Gateway's factory defaults, use this screen.
- Advanced. This screen allows you to perform the advanced administration functions of Restore Factory Defaults, as well as Routing and NAT disabling.

Status

- Gateway. This screen provides general and status information about the Gateway.
- Connection. This screen provides information about the cable connection.
- Local Network. This screen allows you to release a DHCP client from the local network server.
- Modem Log. This screen provides a log of the built-in modem's activity.

How to Access the Web-based Utility

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Gateway's default IP address, **192.168.0.1**, in the Address field. Then press **Enter.**

A password request page will appear. (Non-Windows XP users will see a similar screen.) Leave the *User Name* field blank, and enter **admin** (the default password) in the *Password* field. Then click the **OK** button.

NOTE: Depending on your service provider, some features and functions in the Web-based Utility may not be available or may perform differently than described in the User Guide.

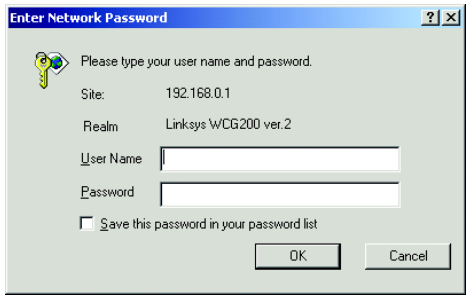

Figure 5-1: Password Screen

The Setup Tab

The Basic Setup Tab

The first screen that appears is the Basic Setup tab. This tab allows you to change the Gateway's general settings. Change these settings as described here and click the **Save Settings** button to save your changes or **Cancel Changes** to cancel your changes.

Figure 5-2: Dynamic IP

Internet Setup

Internet Connection Type. The Gateway supports Dynamic IP and Static IP. Each Basic Setup screen and available features will differ depending on what type you select.

Dynamic IP

IP Settings. Select **Obtain IP Address Automatically** if your ISP says you are connecting through a dynamic IP address.

Static IP

If you are required to use a permanent (static) IP address to connect to the Internet, then select **Set Static IP Manually**.

- Internet IP Address. This is the Gateway's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.

- Default Gateway. Your ISP will provide you with the default Gateway Address, which is the ISP server's IP address.
- Primary DNS. (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

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

Optional Settings (Required by some ISPs)

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

Network Setup

- Gateway IP. The value for the Gateway's Local IP Address are shown here.
- Network Address Server Settings (DHCP). A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each computer on your network for you. Unless you already have one, it is highly recommended that you leave the Gateway enabled as a DHCP server.
  - Local DHCP Server. If you enable the DHCP Server for the Local DHCP server, enter the IP address for the DHCP server in the fields provided.
  - Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.0.2 or greater, because the default IP address for the Gateway is 192.168.0.1.
  - Number of Address. Enter the maximum number of computers that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. By default, the range is 192.168.0.10 to 192.168.0.254.
  - IP Address Range. The range of DHCP addresses is displayed here.

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

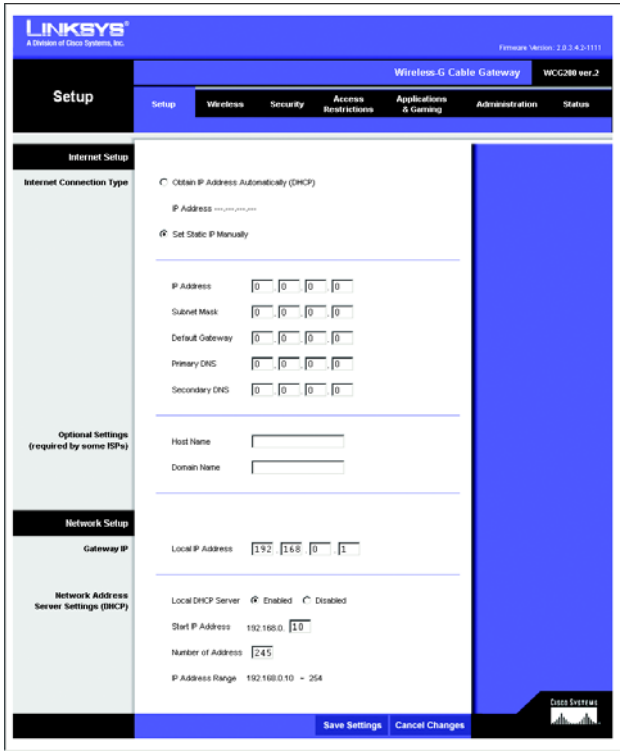

Figure 5-3: Static IP

The Wireless Tab

Basic Wireless Settings Tab

There are two ways to configure the Gateway's wireless settings, SecureEasySetup and manual configuration. If you have other SecureEasySetup devices, such as notebook adapters or printers, then you can use the Gateway's SecureEasySetup feature to configure your wireless network. Follow the instructions for the SecureEasySetup button feature.

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

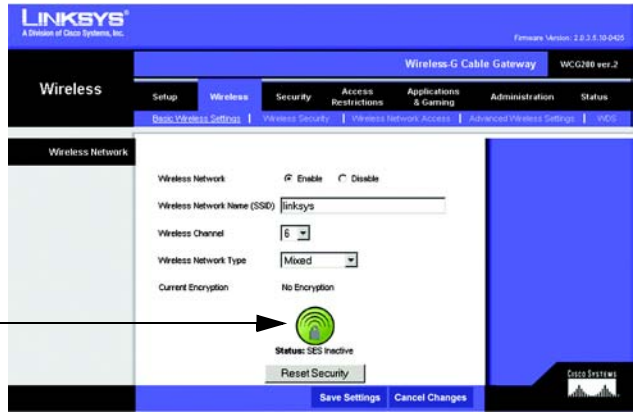

Figure 5-4: Basic Wireless Settings

If you do not have other SecureEasySetup devices, then enter your wireless settings on this screen.

- Wireless Network. Select **Enable** to enable your wireless network, or select **Disable** to disable it.
- Wireless Network Name (SSID). Enter the name for your wireless network into the field. 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. Linksys recommends that you change the default SSID (**linksys**) to a unique name of your choice.
- Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly. Linksys wireless clients will automatically detect the wireless channel of the Gateway.
- Wireless Network Type. If you have 802.11g and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only 802.11g devices, select **802.11g**. If you have only 802.11b devices, select **802.11b**. If you want to disable wireless networking, select **Disabled**.
- Current Encryption. Your wireless security encryption method will be displayed here.
- SecureEasySetup Button. The status of the Gateway's SecureEasySetup feature is displayed here. If you want to use the Gateway's SecureEasySetup feature, click the **SecureEasySetup** button.

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

NOTE: You can only add one SecureEasySetup device at a time.

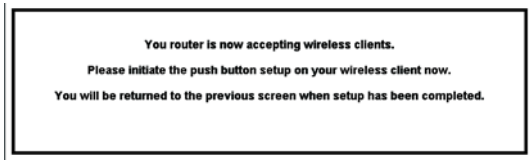

Figure 5-5: Press the SecureEasySetup Button on Only One Wireless Client

When the SecureEasySetup process is complete, the *Basic Wireless Settings* screen will appear, and the Current Encryption and Status information will be updated.

Then repeat this procedure for each additional SecureEasySetup device.

If you have non-SecureEasySetup devices to configure, then write down the Wireless Network Name (SSID) for the Gateway. Click the **Wireless Security** tab. The Gateway's WPA-Personal settings will appear on the *Wireless Security* screen. Write down the Passphrase for the Gateway. When you configure the wireless settings for your non-SecureEasySetup devices, enter the Gateway's Network Name (SSID) and Passphrase when you are asked for them.

NOTE: Some devices may call the Passphrase a Pre-Shared Key instead. They are different names for the same key.

Figure 5-6: WPA-Personal Security Enabled

- **Reset Security**. If you want to reset the Gateway to its factory default wireless settings (SSID: **linksys** and wireless security disabled), then click the **Reset Security** button.

  After the Gateway's SSID has been reset and its security disabled, you can click the SecureEasySetup button to configure your wireless network with a new SSID and Passphrase, or you can manually enter new settings on the *Basic Wireless Settings* and *Wireless Security* screens.

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

Wireless Security Tab

The Wireless Security settings configure the security of your wireless network. There are six wireless security mode options supported by the Gateway: WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WPA2 is a stronger version of WPA. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) These are briefly discussed here. For detailed instructions on configuring wireless security for the Gateway, turn to "Appendix B: Wireless Security." If you want to disable wireless security, select **Disabled** from the drop-down menu for Security Mode.

Figure 5-7: Wireless Security

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

WPA-Personal. To use WPA-Personal, select **WPA-Personal** from the *Security Mode* drop-down menu. Select a method of encryption. Then enter a Passphrase and a Key Renewal period.

- Encryption. WPA offers you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm you want to use, **TKIP** or **AES**.
- Passphrase. Enter a Passphrase (also called a WPA Shared Key) of 8-32 characters.
- Key Renewal. Enter a Key Renewal timeout period, which instructs the Gateway how often it should change the encryption keys.

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

WPA2-Personal. To use WPA2-Personal, select **WPA2-Personal** from the *Security Mode* drop-down menu. Select a method of encryption. Then enter a Passphrase and a Key Renewal period.

- Encryption. Select the encryption method you want to use, **AES** or **TKIP + AES**.
- Passphrase. Enter a Passphrase (also called a WPA Shared Key) of 8-32 characters.
- Key Renewal. Enter a Key Renewal timeout period, which instructs the Gateway how often it should change the encryption keys.

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

Figure 5-8: WPA-Personal

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

Figure 5-9: WPA2-Personal

WPA-Enterprise. This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Gateway.) To use WPA-Enterprise, select **WPA-Enterprise** from the *Security Mode* drop-down menu. Select a method of encryption and your RADIUS settings. Then enter a Shared Secret key and a Key Renewal period.

- Encryption. WPA offers you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm you want to use, **TKIP** or **AES**.
- RADIUS Server Address. Enter the RADIUS server's IP address.
- RADIUS Port. Enter the port number used by the RADIUS server.
- Shared Secret. Enter the Shared Secret key used by the Gateway and RADIUS server.
- Key Renewal. Enter a Key Renewal timeout period, which instructs the Gateway how often it should change the encryption keys.

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

WPA2-Enterprise. This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Gateway.) To use WPA2-Enterprise, select **WPA2-Enterprise** from the *Security Mode* drop-down menu. Select a method of encryption and your RADIUS settings. Then enter a Shared Secret key and a Key Renewal period.

- Encryption. Select the encryption method you want to use, **AES** or **TKIP + AES**.
- RADIUS Server Address. Enter the RADIUS server's IP address.
- RADIUS Port. Enter the port number used by the RADIUS server.
- Shared Secret. Enter the Shared Secret key used by the Gateway and RADIUS server.
- Key Renewal. Enter a Key Renewal timeout period, which instructs the Gateway how often it should change the encryption keys.

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

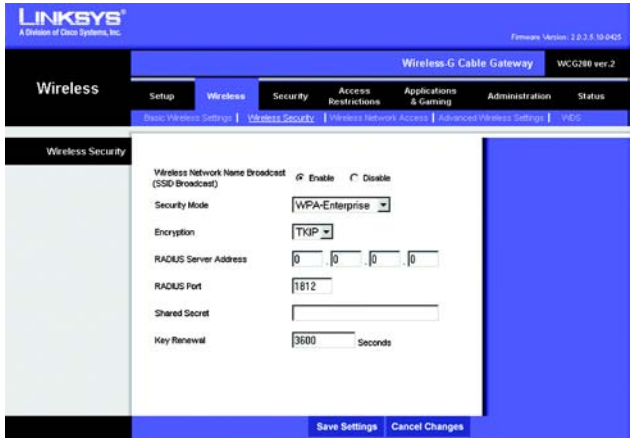

Figure 5-10: WPA-Enterprise

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

server: *any computer whose function in a network is to provide user access to files, printing, communications, and other services.*

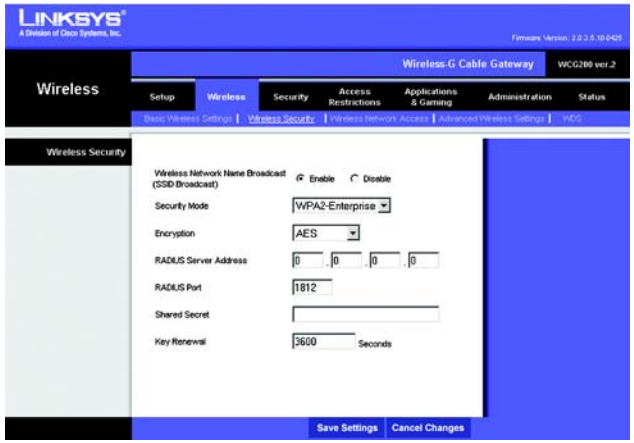

Figure 5-11: WPA2-Enterprise

RADIUS. This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Gateway.) First, enter your RADIUS settings. Select a level of WEP encryption, **64-Bit Encryption** or **128-Bit Encryption**. Then select a Default Key (choose which Key to use). Then either generate a WEP key using a Passphrase or enter the WEP key manually.

- RADIUS Server Address. Enter the RADIUS server's IP address.
- RADIUS Port. Enter the port number used by the RADIUS server.
- Shared Secret. Enter the Shared Secret key used by the Gateway and RADIUS server.
- Wireless Encryption Level. 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. To enable WEP, select **64-Bit Encryption** or **128-Bit Encryption**.
- Default Key. Select which WEP key (1-4) will be used when the Gateway sends data. Make sure that the receiving device (wireless client) is using the same key.
- Passphrase for Keys. 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 you want to use, and enter it manually in the wireless client.) After you enter the Passphrase, click the **Generate Keys** button to create WEP keys.
- Wireless WEP 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.) 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".

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

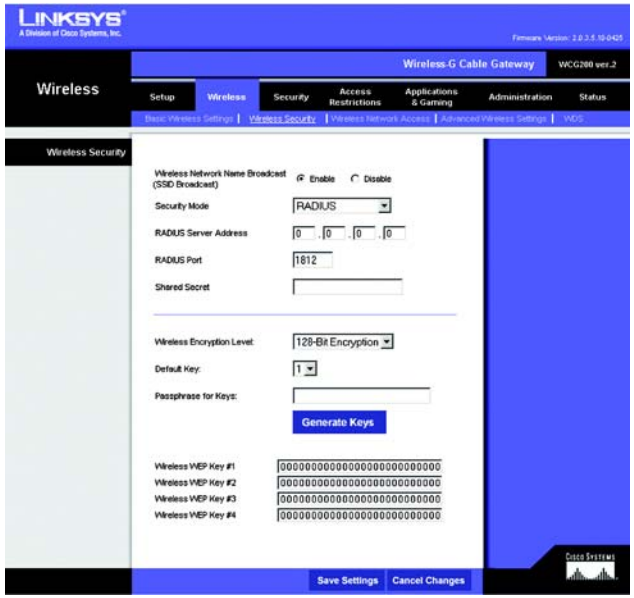

Figure 5-12: RADIUS

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

WEP. WEP is a basic encryption method, which is not as secure as WPA. To use WEP, select **WEP** from the *Security Mode* drop-down menu. Select a level of WEP encryption, **64-Bit Encryption** or **128-Bit Encryption**. Then select a Default Key (choose which Key to use). Then either generate a WEP key using a Passphrase or enter the WEP key manually.

- Wireless Encryption Level. 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. To enable WEP, select **64-Bit Encryption** or **128-Bit Encryption**.

- Default Key. Select which WEP key (1-4) will be used when the Gateway sends data. Make sure that the receiving device (wireless client) is using the same key.

- Passphrase for Keys. 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 you want to use, and enter it manually in the wireless client.) After you enter the Passphrase, click the **Generate Keys** button to create WEP keys.

- Wireless WEP 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.) 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”.

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

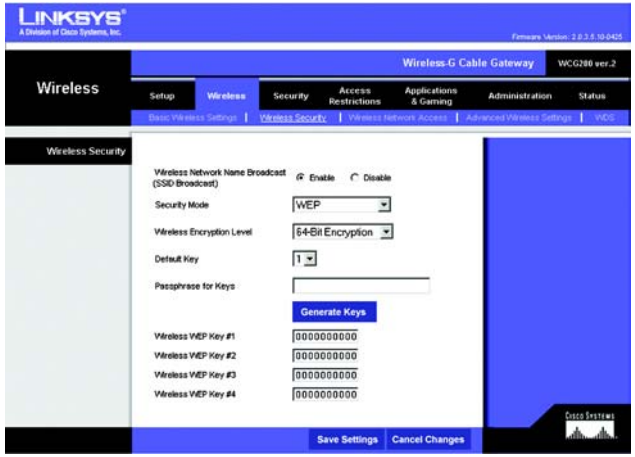

Figure 5-13: WEP

Wireless Network Access Tab

Wireless Network Access. If this function is enabled, only the computers on the list will be allowed access to the wireless network. To add a computer to the network, click **Enable** to enable the function. Then, enter the MAC addresses in the fields provided, You can also click the **Select MAC Address From Networked Computers** button.

Select the MAC Address(es) you want from the list, and click the **Add** button. Click the **Refresh** button if you want to refresh the on-screen information. Click the **Close** button to return to the previous screen.

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

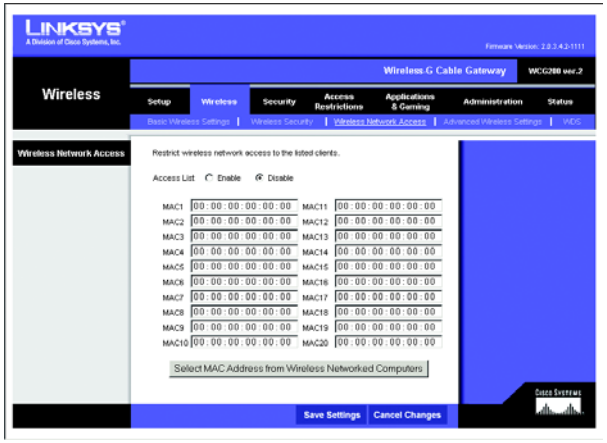

Figure 5-14: Wireless Network Access

mac address: *the unique address that a manufacturer assigns to each networking device.*

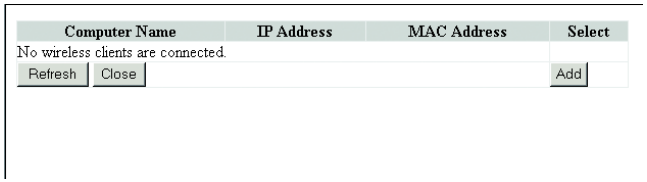

Figure 5-15: MAC Address Access List

Advanced Wireless Settings Tab

On this screen you can access the Advanced Wireless features, including Basic Data Rates, Control Tx Rates, Beacon Interval, DTIM Interval, Fragmentation Threshold, RTS Threshold, and Authentication Type.

- Basic Data Rates. Select **Min** or **All** from the drop-down menu for rate.
- Control Tx Rates. Select **Min** or **All** from the drop-down menu for the transmission rate. All will negotiate the best possible connection speed between the Gateway and a wireless client.
- Beacon Interval. The default value is **100**. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Gateway to synchronize the wireless network.
- DTIM Interval. The default value is **3**. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Gateway has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
- 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 decrease the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.
- 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 Gateway 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.
- Authentication Type. The default is set to Open System or Shared Key, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. For Shared Key authentication, the sender and recipient use a WEP key for authentication. If you want to use only Shared Key authentication, then select **Shared Key**. In most cases, you should keep the default, **Open System or Shared Key**.

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

Figure 5-16: Advanced Wireless Settings

packet: *a unit of data sent over a network.*

beacon internal: *data transmitted on your wireless network that keeps the network synchronized.*

dtim *(delivery traffic indication message): a message included in data packets that can increase wireless efficiency.*

fragmentation: *breaking a packet into smaller units when transmitting over a network.*

rts *(request to send): a networking method of coordinating large packets through the RTS Threshold setting.*

WDS Tab

Wireless Distribution System. This feature enables the Gateway to talk to a remote device within its range so it can retransmit the signal or it can enable a wireless connection between two wired networks. The other device(s) must support a compatible version of WDS bridging or WDS repeating.

To use this feature, click **Enable** and enter the wireless MAC address of the remote device in the *MAC* field. You can have up to four remote devices.

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

Figure 5-17: WDS Tab

The Security Tab

Firewall

On this screen, you can enable filters to block specific Internet data types and anonymous Internet requests.

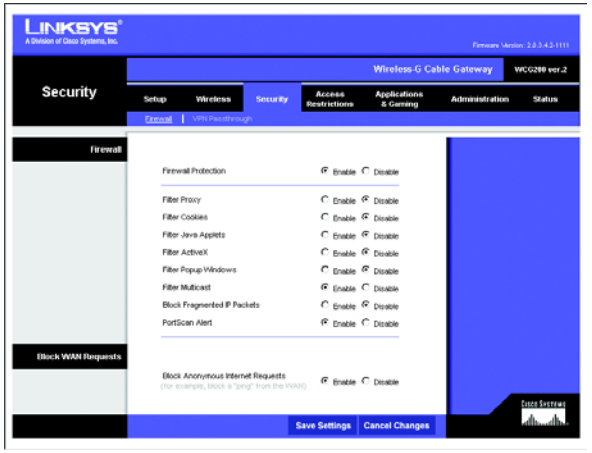

Figure 5-18: Firewall

- Firewall Protection. Enable this feature to employ Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network environment.
- Filter Proxy. Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click **Enable**.
- Filter Cookies. A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click **Enable**.
- Filter Java Applets. Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using Java. To enable Java Applet filtering, click **Enable**.
- Filter ActiveX. If you deny ActiveX, a programming language for websites, you run the risk of not having access to Internet sites created using ActiveX. To enable ActiveX filtering, click **Enabled**.
- Filter Popup Windows. When enabled, the Gateway will attempt to block the browser popup windows. Please note that not all popups may be blocked, because of the various creation methods.
- Filter Multicast. Multicasting allows for multiple transmissions to specific recipients at the same time. If this multicasting is permitted, the Gateway will allow IP multicast packets to be forwarded to the appropriate computers. Select **Enable** to filter multicasting, or **Disable** to disable this feature.
- Block Fragmented IP Packets. Enable this feature to block any incoming or outgoing fragmented packets.
- PortScan Alert. When enabled, the Gateway will put entries into the security log when it detects port scans from the Internet.
- Block WAN Requests. Enable **Block Anonymous Internet Requests** and you can prevent your network from being “pinged,” or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Uncheck the box to allow anonymous Internet requests.

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

VPN Passthrough Tab

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. The *VPN* screen allows you to configure your VPN settings to make your network more secure.

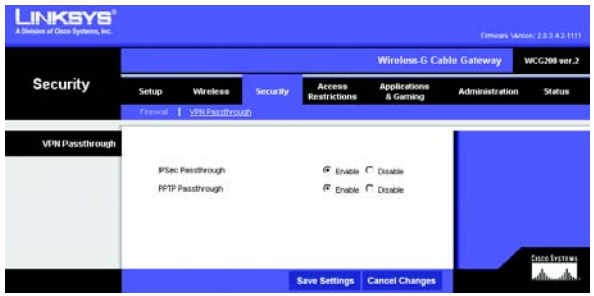

Figure 5-19: VPN

VPN Passthrough

- IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enable** button. To disable IPSec Passthrough, click the **Disable** button.
- PPTP Passthrough. Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enable** button. To disable PPTP Passthrough, click the **Disable** button.

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

The Access Restrictions Tab

The Access Restrictions tab allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific computers and set up filters by using network port numbers.

Website Blocking Tab

Website/Keyword Blocking. You can filter access to various websites accessed over the Internet. Enter the keyword or website URL in the field next to *New Website/Keyword Blocking* and click the **Add** button. The keyword or website URL will be added to the Website/Keyword List. To unblock a website or delete a keyword, highlight the keyword or website URL in the list and click the **Remove** button.

Timed Access Tab

Timed Access can be used to limit the days or hours of access to the network.

You can set up a Timed Access policy for each local MAC address. To use the feature, enter the MAC address in the field, then click the **Add** button. You can also click the **Select MAC Address from Networked Computers** button.

On the new screen that appears, select a MAC address, and click the **Add** button. Click the **Refresh** button if you want to refresh the on-screen information. Click the **Close** button to return to the previous screen.

Day to Block. Select **Everyday**, or select individual days.

Time to Block. Select **All day** or enter a specific range of hours and minutes.

When finished making your changes to a policy, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Repeat the aforementioned steps to set up a new policy. To remove a policy, select it from the drop-down menu, and click the **Remove** button.

Figure 5-20: Website Blocking

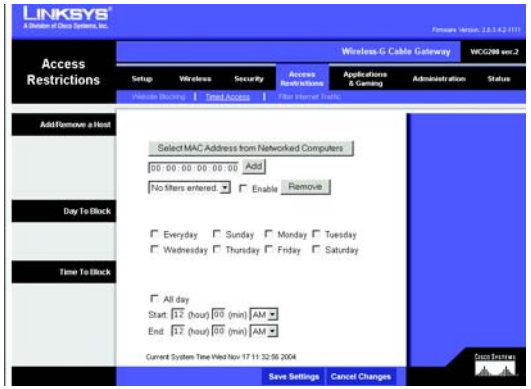

Figure 5-21: Timed Access

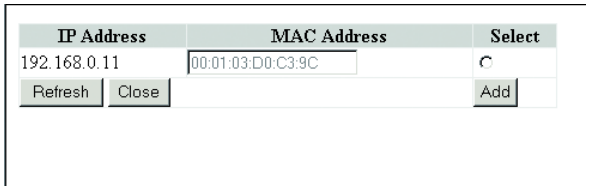

Figure 5-22: MAC Address

Filter Internet Traffic Tab

This screen is used to filter or block ports from Internet access by IP address or Port Range.

IP Address Range

To set up a filter using IP addresses, enter the range of IP addresses you wish to filter in the *Start* and *End* fields. Users who have filtered IP addresses will not be able to access the Internet at all. If you only want to filter one IP address instead of a range of IP addresses, enter the same value into both fields. For instance, if you wish to filter the PC with the IP address of 192.168.0.5, enter 5 into both fields on one line: 192.168.0.5 ~ 192.168.0.5.

Port Range

Enter the port numbers you want to filter in the *Start* and *End* fields. To filter users by network port number, select the protocol you want to filter, **TCP**, **UDP**, or **Both**, from the *Protocol* drop-down menu. Users connected to the Gateway will no longer be able to access any port number listed there.

Click the **Enable** checkbox for each filter you want the Gateway to use.

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

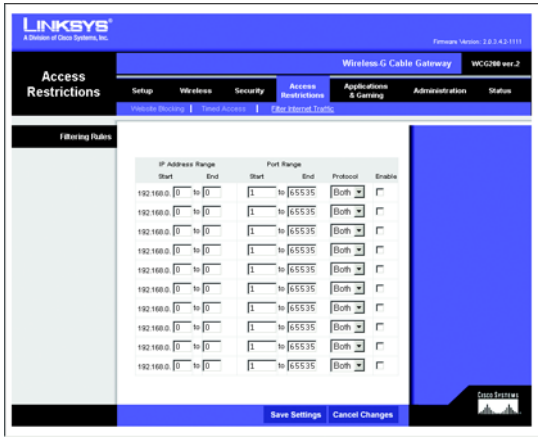

Figure 5-23: Filter Internet Traffic

The Applications and Gaming Tab

Port Range Forwarding

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

When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

- Application. Enter the name you wish to give each application.
- Start and End. Enter the starting and ending numbers of the port range you wish to forward.
- Protocol. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- IP Address. Enter the IP Address of the system to which the traffic should be forwarded.

Click the **Enable** checkbox for each port forwarding setting you want the Gateway to use.

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

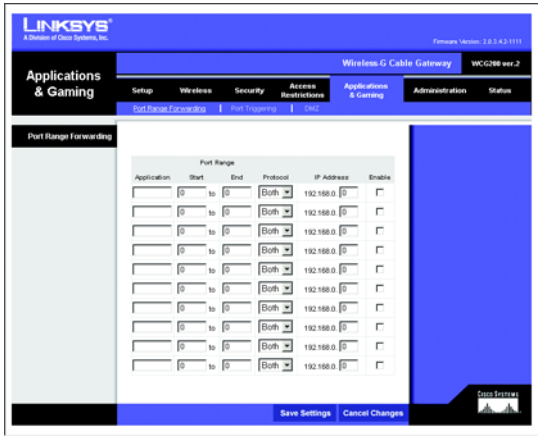

Figure 5-24: Port Range Forwarding

Port Triggering

Port Triggering is used for special applications that can request a port to be opened on demand. For this feature, the Gateway will watch outgoing data for specific port numbers. The Gateway will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Gateway, the data is pulled back to the proper computer by way of IP address and port mapping rules.

- Application. Enter the name you wish to give each application.
- Start Port and End Port. Enter the starting and ending Triggered Range numbers and the Incoming Forwarded Range numbers of the port(s) you wish to forward.
- Protocol. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.

Click the **Enable** checkbox for each port triggering setting you want the Gateway to use.

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

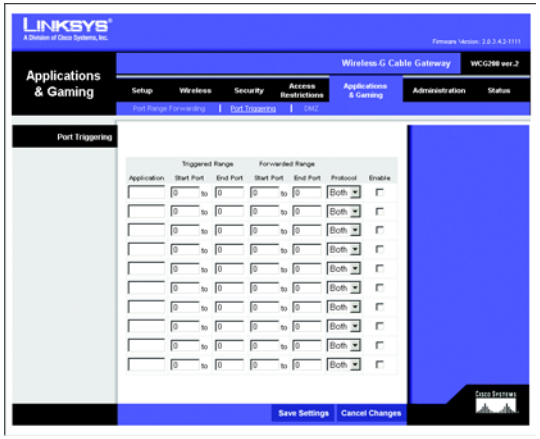

Figure 5-25: Port Triggering

DMZ

The DMZ screen allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing through DMZ Hosting. DMZ hosting forwards all the ports for one computer at the same time, which differs from Port Range Forwarding, which can only forward a maximum of 10 ranges of ports.

- DMZ Hosting. This feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enable**. To disable DMZ, select **Disable**.
- DMZ Host IP Address. To expose one computer, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

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

Figure 5-26: DMZ

The Administration Tab

Security Tab

The *Security* screen allows you to change the Gateway's access settings as well as configure the UPnP (Universal Plug and Play) and Reporting features.

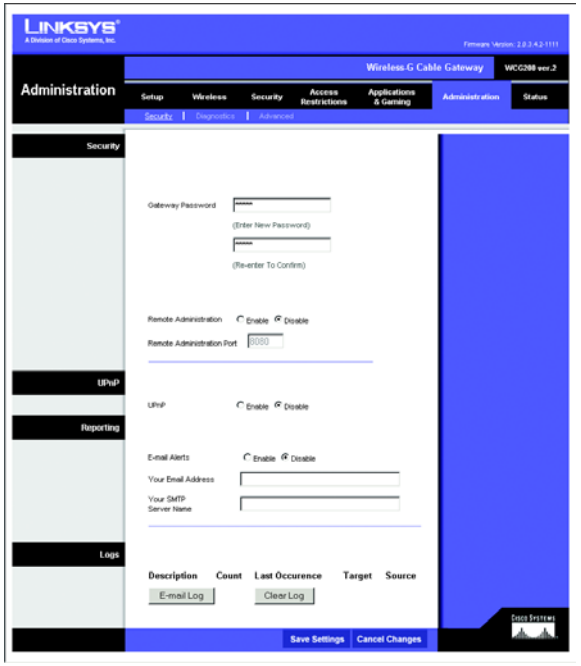

Figure 5-27: Security

Security

To ensure the Gateway's security, you will be asked for your password when you access the Gateway's Web-based Utility. The default password is **admin**.

- Gateway Password. It is recommended that you change the default password to one of your choice.
- Re-enter to confirm. Re-enter the Gateway's new Password to confirm it.
- Remote Administration. When enabled, the Web-based Utility can be accessed from the Internet. To connect, type **http://127.0.0.1:8080** in the web browser's *Address* field, but replace 127.0.0.1 with the WAN (Internet) IP address of the Gateway.
- Administration Port. Enter the port number you will use to remotely access the Gateway. The default is **8080**.

UPnP

UPnP allows Windows XP to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing.

UPnP. To enable UPnP, click **Enable**.

Reporting

E-Mail Alerts. To enable E-Mail Alerts, click **Enable**.

- Your E-Mail Address. Enter the e-mail address that will receive alert logs in the field provided.
- Your SMTP Server Name. Enter the IP Address of the SMTP server.

Logs

You can view security events and have logs e-mailed to you.

To send the logs, click the **E-mail Log** button. To clear the log entries displayed on this screen, click the **Clear Log** button.

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

Diagnostics Tab

Use this screen to run a ping test.

Ping Test

Ping Test Parameters

- Ping Target. Enter the IP Address that you want to ping in the field provided. This can be either a local (LAN) IP or an Internet (WAN) IP address.
- Ping Size. Enter the size of the ping packets you want to use.
- Number of Pings. Enter the number of times that you want to ping.
- Ping Interval. Enter the ping interval in milliseconds.
- Ping Timeout. Enter the timeout period in milliseconds.
- Ping Result. The results of the ping test will be shown here.

Click the **Start Test** button to start the Ping Test. Click the **Abort Test** button to stop the test. Click the **Refresh** button to refresh the screen. Click the **Clear Results** button to clear the screen.

Figure 5-28: Ping Test

Advanced

On this screen you can restore factory defaults or disable NAT and routing functions of the Gateway.

Restore Factory Defaults. If you wish to restore the Gateway to its factory default settings and lose all your settings, click **Yes**.

To begin the restore process, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Routing and NAT. Click **Disable** to disable all NAT and routing functions of the Gateway, and allow only the cable modem function. The IP address of the device will change to 192.168.100.1.

Click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Figure 5-29: Advanced Administration

The Status Tab

Gateway

This screen displays information about your Gateway and its WAN (Internet) Connections.

Information

This section displays the Standard Specification Compliance, Hardware Version, Software Version, Cable Modem MAC Address, Cable Modem Serial Number, and CM Certification.

Standard Specification Compliant. The specification is displayed here.

Hardware Version. The current hardware version is displayed here.

Software Version. The current software version is displayed here.

Cable Modem MAC Address. The MAC Address of the cable modem is displayed here.

Cable Modem Serial Number. The serial number of the cable modem is displayed here.

CM Certificate. The installation status of the CM certificate is displayed here.

Figure 5-30: Gateway

Status

The Internet connection status information is displayed. This section indicates the System Up Time, Network Access, WAN IP Address, Subnet Mask, Gateway IP Address, DNS server(s), WAN DHCP IP Address Lease, and WAN DHCP IP Expiration.

System Up Time. This indicates how long the Gateway has been active.

Network Access. This indicates whether access to the network has been achieved.

WAN IP Address. This indicates the IP Address that is assigned to the Gateway.

Subnet Mask. The Subnet Mask of the Gateway is displayed here.

Gateway IP Address. The IP Address of the Gateway is shown here.

DNS Server(s). The IP address(es) of the DNS server(s) are displayed here.

WAN DHCP IP Address Lease. This indicates how long the lease is.

WAN DHCP IP Expires. This indicates when the lease expires.

Renew DHCP Lease. Click the **Renew DHCP Lease** button to replace your Gateway's current IP address with a new IP address.

Connection

The cable connection information is displayed.

The Startup Procedure information displayed is Acquire Downstream Channel, Connectivity State, Boot State, and Security.

The Downstream Channel information displayed is the Lock Status, Modulation, Channel ID, Provisioned Rate, Symbol Rate, Downstream Power, and SNR.

The Upstream Channel information that is displayed is Lock Status, Modulation, Channel ID, Provisioned Rate, Symbol Rate, and Upstream Power.

Figure 5-31: Connection

Local Network

This feature is used to release a DHCP client from the server.

Select the DHCP Client whose IP address that you want to release, and then click the **Release** button.

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

Figure 5-32: Local Network

Modem Log

The Modem log displays a log of Modem activity.

Click the **Refresh** button if you want to refresh your screen. To delete all log entries, click the **Clear Log** button.

Figure 5-33: Modem Log

Appendix A: Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems that may occur during the installation and operation of the Gateway. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

Common Problems and Solutions

1. I need to set a static IP address on a computer.

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

- For Windows 98 and Me:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
  2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
  3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway. Make sure that each IP address is unique for each computer or network device.
  4. Click the **Gateway** tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Gateway. Click the Add button to accept the entry.
  5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
  6. Click the **OK** button in the TCP/IP properties window, and click Close or the OK button for the Network window.
  7. Restart the computer when asked.
- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
  3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
  5. Enter the Subnet Mask, 255.255.255.0.
  6. Enter the Default Gateway, 192.168.0.1 (Gateway's default IP address).

7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
9. Restart the computer if asked.

- For Windows XP:
  The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.
  1. Click **Start** and **Control Panel**.
  2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
  3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the Properties option.
  4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
  5. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
  6. Enter the Subnet Mask, 255.255.255.0.
  7. Enter the Default Gateway, 192.168.0.1 (Gateway's default IP address).
  8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

2. The Gateway is not working.

- Verify that the Power cord and other network cables are plugged in.
- Check the LEDs on the Gateway's front and verify that they are lit appropriately.
- Check the settings on your PC.
- Check the Gateway's settings.
- Verify that your cable ISP has been given the correct MAC Address for the cable modem function.

3. I can't connect to the Gateway.

- Verify that the Gateway is properly installed; LAN connections are OK, and it is powered ON.
- Make sure that your PC and the Gateway are on the same network segment. If you are not sure, initiate the DHCP function, and let the PC get the IP address automatically.

- Make sure that your PC is using an IP address within the default range of 192.168.0.2 to 192.168.0.254 and thus compatible with the Gateway default IP Address of 192.168.0.1
- Also, the Subnet Mask should be set to 255.255.255.0 to match the Gateway. For the Gateway, you can check these settings by using Control Panel-Network to check the Properties for the TCP/IP protocol.

4. The Power LED stays red when it shouldn't.

- The Power LED lights up when the device is first powered up. The system will boot up itself and check for proper operation. After finishing the checking procedure, the Power LED turns green to show the system is working fine. If the LED remains red after this time, the device is not working properly.

5. The Online LED will not go solid.

- Verify that the coaxial cable is firmly plugged into the Gateway's cable port, with the other end plugged directly into the Cable wall jack.
- Verify that your Cable account is active.
- Verify that your cable ISP has been given the correct MAC Address for the cable modem function.

6. I can't access the Internet from the Gateway.

- Check if both ends of the network cable and power adapter are properly connected. Check if the status LEDs on the front panel are functioning properly.
- If using Windows 95, 98 or Me, check the TCP/IP setup on the client side. Run winipcfg by clicking on the Start button, selecting Run, and typing winipcfg in the Run field. Press Enter. The PC should have an IP address of 192.168.0.xxx ("xxx" is from 2 to 254.). The Subnet Mask is 255.255.255.0; the default gateway IP should be the Gateway's IP Address, and check that the DNS is correct.
- Check the same setup values on the Gateway's Status page.

7. When I enter a URL or IP address, I get a time out error.

- Check to see if your other PCs work. If they do, verify that your PC's IP settings are correct (IP address, Subnet Mask, Default Gateway, and DNS)
- If the PCs are configured correctly, but still not working, check the Gateway. Make sure that it is connected and ON. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Gateway is configured correctly, check your Internet connection to see that it is working correctly.
- Manually configure the TCP/IP with a DNS address provided by your ISP.

Frequently Asked Questions

What is the maximum number of IP addresses that the Gateway will support?
The Gateway will support up to 253 IP addresses.

Is IPSec Passthrough supported by the Gateway?
Yes, it is a built-in feature that is enabled by default.

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

What is Network Address Translation and what is it used for?
Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a computer connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Gateway to be used with low cost Internet accounts when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Gateway support any operating system other than Windows 98SE, Windows Millennium, Windows 2000, or Windows XP?
Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

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

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?
If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Gateway from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

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

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?
Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.linksys.com for more information.

If all else fails in the installation, what can I do?
Reset the Gateway by holding down the reset button until the Power LED fully turns on and off. Reset your Gateway by powering the unit off and then on.

Will the Gateway function in a Macintosh environment?
Yes, but the Gateway's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

With which type of firewall is the Gateway equipped?
The Gateway uses NAT and TCP/IP port inspections. It also has SPI (Stateful Packet Inspection).

I am not able to get the web configuration screen for the Gateway. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

What is DMZ Hosting?
Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you

want to use DMZ Hosting. To get the LAN IP address, see "Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter."

If DMZ Hosting is used, does the exposed user share the public IP with the Gateway?
No.

Does the Gateway pass PPTP packets or actively route PPTP sessions?
The Gateway allows PPTP packets to pass through.

Is the Gateway cross-platform compatible?
Any platform that supports Ethernet and TCP/IP is compatible with the Gateway.

How many ports can be simultaneously forwarded?
Theoretically, the Gateway can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

Does the Gateway replace a modem? Is there a cable modem in the Gateway?
Yes. The Gateway has an integrated cable modem, so this product will replace your current cable modem.

What are the advanced features of the Gateway?
The Gateway's advanced features include Filters, Forwarding, and DMZ host.

How do I get mIRC to work with the Gateway?
Set port forwarding to 113 for the computer on which you are using mIRC. If you are experiencing difficulty after setting the port forwarding, try changing the Direct Client-to-Client (DCC) settings to a range from 1024 to 1030 on the DCC option and Forwarding page of the Web-based Setup Utility.

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

What is 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, peer-to-peer without the use of an access point. Ad-hoc mode is not used with the Gateway.

What is infrastructure mode?
When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a network through a wireless access point. Infrastructure mode is used with the Gateway.

What is a MAC Address?

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

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 encryption keys periodically.

For information on implementing these security features, refer to "Chapter 5: Configuring the Wireless-G Cable Gateway."

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. Five modes are available: WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, and RADIUS. WPA-Personal gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption Standard), which utilizes a symmetric 128-Bit block data encryption. WPA2-Personal only uses AES encryption, which is stronger than TKIP. WPA-Enterprise offers two encryption methods, TKIP and AES,

with dynamic encryption keys, while WPA2-Enterprise only uses AES encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication.

WPA-Personal. If you do not have a RADIUS server, select the type of algorithm you want to use, TKIP or AES, and enter a password in the *Passphrase* field of 8-63 characters.

WPA2-Personal. Enter a password in the *Passphrase* field of 8-63 characters.

WPA-Enterprise. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) WPA-Enterprise offers two encryption methods, TKIP and AES, with dynamic encryption keys. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

WPA2-Enterprise. WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) WPA-Enterprise offers two encryption methods, AES and TKIP + AES, with dynamic encryption keys. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the 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: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering feature of the Gateway. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Gateway's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98 or Me Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.
2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Gateway via a CAT 5 Ethernet network cable. See Figure E-1.
3. Write down the Adapter Address as shown on your computer screen (see Figure E-2). This is the MAC address for your Ethernet adapter and is shown in hexadecimal as a series of numbers and letters.

   The MAC address/Adapter Address is what you will use for MAC filtering. The example in Figure D-2 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

   The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

NOTE: The MAC address is also called the Adapter Address.

Figure C-1: IP Configuration Screen

Figure C-2: MAC Address/Adapter Address

Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.

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

2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.
3. Write down the Physical Address as shown on your computer screen (Figure D-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

   The MAC address/Physical Address is what you will use for MAC filtering. The example in Figure D-3 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

   The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

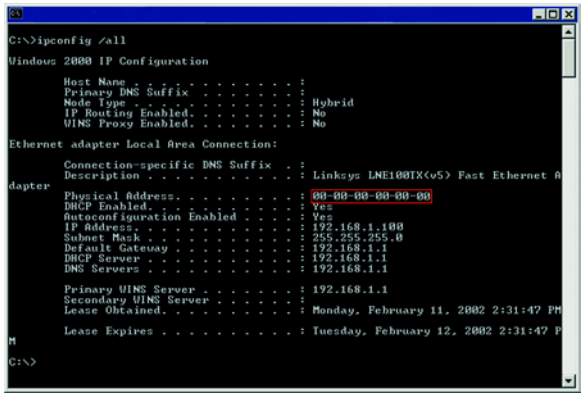

Figure C-3: MAC Address/Physical Address

Appendix D: 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 computer.

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 Gateway 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 Gateway's firewall protection from one computer, 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 computers.

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 E: Specifications

Standards	DOCSIS 1.0, DOCSIS 1.1 Certified, DOCSIS 2.0 Certified, 802.11g, 802.11b
Ports	4 RJ-45 10/100, 1 USB, 1 Female Coax F-Connector
Buttons	Power ON/OFF switch, Reset
Cabling Type	CAT5, USB, Coax
LEDs	Power, DS, US, Online, Ethernet, USB, Wireless
Security	WPA, WPA2, WEP, MAC address filtering, SPI Firewall, SecureEasySetup
WEP key bits	64/128
Dimensions	7.32" x 2.48" x 6.08" (186 mm x 63 mm x 155 mm)
Unit Weight	1.0 lb (0.45 kg)
Power	External, 12V DC, 1A
Certifications	DOCSIS 1.1, DOCSIS 2.0, FCC Part 15B Class B, UL 1950, EN60950, CE EN 55022 Class B, VCCI, IC-03
Operating Temp.	0ºC to 40ºC (32ºF to 104ºF)
Storage Temp.	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity	20% to 90% Non-Condensing
Storage Humidity	20% to 90% Non-Condensing

Appendix F: 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 G: 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, RSS210.
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 this product 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

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 dieses produkt tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys Group déclare que le produit 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 H: 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) 949-823-3002
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.)	949-823-3000