

LINKSYS®

A Division of Cisco Systems, Inc.



2.4GHz
802.11g

Wireless-G



WIRELESS

ADSL Gateway with 2 Phone Ports

User Guide

Model No. **WAG54GP2**

CISCO SYSTEMS



Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2005 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

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

How to Use This User Guide

This User Guide has been designed to make understanding networking with the Wireless-G ADSL Gateway with 2 Phone Ports easier than ever. Look for the following items when reading this User Guide:



This checkmark means there is a note of interest and is something you should pay special attention to while using the Wireless-G ADSL Gateway with 2 Phone Ports.



This exclamation point means there is a caution or warning and is something that could damage your property or the Wireless-G ADSL Gateway with 2 Phone Ports.



This question mark provides you with a reminder about something you might need to do while using the Wireless-G ADSL Gateway with 2 Phone Ports.

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

word: definition.

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

Figure 0-1: Sample Figure Description

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

Table of Contents

Chapter 1: Planning Your Network	1
The Gateway's Functions	1
IP Addresses	1
What is a VPN?	2
Why do I need a VPN?	4
Chapter 2: Getting to Know the Wireless-G ADSL Gateway with 2 Phone Ports	6
The Back Panel	6
The Front Panel	7
Chapter 3: Connecting the Wireless-G ADSL Gateway	8
Overview	8
Wired Connection to a Computer	9
Wireless Connection to a Computer	10
Chapter 4: Configuring the Gateway	11
Overview	11
How to Access the Web-based Utility	13
The Setup Tab	14
The Wireless Tab	28
The Security Tab	34
The Access Restrictions Tab	39
The Applications and Gaming Tab	42
The Administration Tab	46
The Status Tab	52
The Voice Tab	55
Chapter 5: Using the Linksys Parental Control Service	56
Overview	56
Introduction	56
Signing up for the Linksys Parental Control Service	57
Signing up for the Linksys Parental Control Service	58
Managing Linksys Parental Controls	61
Support Center	62
Activity Reports	64
Family Settings	66

Suggest a Rating	74
Using the Parental Control Service	74
Appendix A: Troubleshooting	77
Common Problems and Solutions	77
Frequently Asked Questions	85
Chapter 6: Wireless Security	91
Important Information for Wireless Products	91
Appendix B: Configuring IPSec between a Windows 2000 or XP Computer and the Gateway	94
Introduction	94
Environment	94
How to Establish a Secure IPSec Tunnel	95
Appendix C: Finding the MAC Address and IP Address for Your Ethernet Adapter	105
Windows 98 or Me Instructions	105
Windows 2000 or XP Instructions	106
Appendix D: Upgrading Firmware	107
Appendix E: Windows Help	108
Appendix F: Glossary	109
Appendix G: Specifications	114
Appendix H: Warranty Information	116
Appendix I: Regulatory Information	117
Appendix J: Contact Information	119

List of Figures

Figure 1-1: Network	1
Figure 1-2: Computer-to-VPN Gateway	3
Figure 1-3: VPN Gateway-to-VPN Gateway	4
Figure 2-1: Back Panel	6
Figure 2-2: Front Panel	7
Figure 3-1: Connecting your networking devices	9
Figure 3-2: Connecting your ADSL line	9
Figure 3-3: Connecting your phones	9
Figure 3-4: Connecting the power	9
Figure 4-1: Password Screen	13
Figure 4-2: Setup Tab - Basic Setup	14
Figure 4-3: Basic Setup Tab - RFC 1483 Bridged	15
Figure 4-4: Basic Setup Tab - RFC 1483 Routed	17
Figure 4-5: Basic Setup Tab - IPoA	18
Figure 4-6: Basic Setup Tab - RFC 2516 PPPoE	19
Figure 4-7: Basic Setup Tab - RFC 2364 PPPoA	21
Figure 4-8: Basic Setup Tab - Bridged Mode Only	22
Figure 4-9: Basic Setup Tab - DNS Proxy and Optional Settings	23
Figure 4-10: Basic Setup Tab - Network Setup	24
Figure 4-11: Setup Tab - DDNS (DynDNS.org)	25
Figure 4-12: Setup Tab - DDNS (TZO.com)	25
Figure 4-13: Setup Tab - Advanced Routing	26
Figure 4-14: Routing Table	27
Figure 4-15: PVC Selection Table	27
Figure 4-16: Wireless Tab - Wireless Network	28
Figure 4-17: Wireless Tab - Wireless Security (WPA Pre-Shared Key)	29
Figure 4-18: Wireless Tab - Wireless Security (WPA RADIUS)	29
Figure 4-19: Wireless Tab - Wireless Security (WPA2 Professional)	30
Figure 4-20: Wireless Tab - Wireless Security (WPA2 Enterprise)	30
Figure 4-21: Wireless Tab - Wireless Security (WEP)	31

Figure 4-22: Wireless Tab - Wireless Network Access	32
Figure 4-23: MAC Address Access/Filter List	32
Figure 4-24: Wireless Tab - Advanced Wireless Settings	33
Figure 4-25: Security Tab - Firewall	34
Figure 4-26: Security Tab - VPN	35
Figure 4-27: VPN Settings Summary	35
Figure 4-28: Auto Key Management	36
Figure 4-29: Manual Key Management	36
Figure 4-30: System Log	37
Figure 4-31: Advanced VPN Tunnel Setup	37
Figure 4-32: Access Restrictions Tab - Parental Control	39
Figure 4-33: Access Restrictions Tab - Internet Access	40
Figure 4-34: Internet Policy Summary	40
Figure 4-35: List of PCs	41
Figure 4-36: Port Services	41
Figure 4-37: Applications and Gaming Tab - Single Port Forwarding	42
Figure 4-38: Applications and Gaming Tab - Port Range Forwarding	43
Figure 4-39: Applications and Gaming Tab - Port Triggering	43
Figure 4-40: Applications and Gaming Tab - DMZ	44
Figure 4-41: Applications and Gaming Tab - QOS	44
Figure 4-42: Applications and Gaming Tab - QOS Function	45
Figure 4-43: Administration Tab - Management	46
Figure 4-44: Administration Tab - Reporting	49
Figure 4-45: System Log	49
Figure 4-46: Administration Tab - Diagnostics	50
Figure 4-47: Administration Tab - Backup&Restore	50
Figure 4-48: Administration Tab - Factory Defaults	50
Figure 4-49: Administration Tab - Firmware Upgrade	51
Figure 4-50: Administration Tab - Reboot	51
Figure 4-51: Status Tab - Gateway	52
Figure 4-52: Status Tab - Local Network	52
Figure 4-53: Status Tab - Wireless	53
Figure 4-54: Status Tab - DSL Connection	53

Figure 4-55: Status Tab - Voice	54
Figure 4-56: Voice Tab - Voice Authentication	55
Figure 5-1: Safe Surfing	57
Figure 5-2: Access Restrictions Tab - Parental Control	57
Figure 5-3: Linksys Service Agreement	58
Figure 5-4: Sign Up	58
Figure 5-5: Purchase Service	59
Figure 5-6: Connecting to the Parental Control Service	60
Figure 5-7: Congratulations	60
Figure 5-8: Parental Controls Login	61
Figure 5-9: Support Center	62
Figure 5-10: Subscribe to Service	62
Figure 5-11: Update Contact Information	63
Figure 5-12: Cancel Your Parental Control Account	63
Figure 5-13: Activity Reports	64
Figure 5-14: Types of Reports	64
Figure 5-15: Web Report	65
Figure 5-16: Family Settings	66
Figure 5-17: New Family Member	66
Figure 5-18: All Settings	67
Figure 5-19: Online Reporting	67
Figure 5-20: Maturity Level	68
Figure 5-21: Time Restrictions	69
Figure 5-22: Web Browsing Restrictions	70
Figure 5-23: Web Site Categories	70
Figure 5-24: Blocked & Allowed Web Sites	71
Figure 5-25: E-mail Restrictions	72
Figure 5-26: E-mail Settings	72
Figure 5-27: Instant-Messaging Restrictions	73
Figure 5-28: Password	73
Figure 5-29: Suggest a Rating	74
Figure 5-30: Security Warning	74
Figure 5-31: Welcome to Parental Controls	75

Figure 5-32: Tray Icon	75
Figure 5-33: Pop-up Screen (Login)	75
Figure 5-34: Pop-up Screen (Sign Out)	76
Figure 5-35: Right-Click Tray Icon	76
Figure 5-36: Re-activate Tray Icon	76
Figure C-1: Local Security Screen	95
Figure C-2: Rules Tab	95
Figure C-3: IP Filter List Tab	95
Figure C-4: IP Filter List	96
Figure C-5: Filters Properties	96
Figure C-6: New Rule Properties	96
Figure C-7: IP Filter List	97
Figure C-8: Filters Properties	97
Figure C-9: New Rule Properties	97
Figure C-10: IP Filter List Tab	98
Figure C-11: Filter Action Tab	98
Figure C-12: Security Methods Tab	98
Figure C-13: Authentication Methods	99
Figure C-14: Preshared Key	99
Figure C-15: New Preshared Key	99
Figure C-16: Tunnel Setting Tab	100
Figure C-17: Connection Type Tab	100
Figure C-18: Properties Screen	100
Figure C-19: IP Filter List Tab	101
Figure C-20: Filter Action Tab	101
Figure C-21: Authentication Methods Tab	101
Figure C-22: Preshared Key	102
Figure C-23: New Preshared Key	102
Figure C-24: Tunnel Setting Tab	102
Figure C-25: Connection Type	103
Figure C-26: Rules	103
Figure C-27: Local Computer	103
Figure C-28: VPN Tab	104

Wireless-G ADSL Gateway with 2 Phone Ports

Figure D-1: IP Configuration Screen	105
Figure D-2: MAC Address/Adapter Address	105
Figure D-3: MAC Address/Physical Address	106
Figure E-1: Upgrade Firmware	107

Chapter 1: Planning Your Network

The Gateway's Functions

A Gateway is a network device that connects two networks.

This Gateway connects your local network, 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 your network.

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

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 network 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.



Figure 1-1: Network



NOTE: Since the Gateway is a device that connects two networks, it needs two IP addresses—one for your network, and one for the Internet. In this User Guide, you'll see references to these 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 4: Configuring the Gateway*.

Since you use the Gateway to share your DSL 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.

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 networking 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 4: Configuring the Gateway*.

What is a VPN?

A VPN, or Virtual Private Network, is a connection between two endpoints - a VPN Gateway, for instance - in different networks that allows private data to be sent securely between networks. This establishes a private network that can send data securely between these two locations or networks.

This is done by creating a “tunnel”. A VPN tunnel connects the two computers or networks and allows data to be transmitted over the Internet as if it were still within those networks. While not a literal tunnel, this is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques - IPSec, short for IP Security - the VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. Virtual Private Networking can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN Gateway using any computer with VPN client software that supports IPSec, such as SSH Sentinel.)

There are two basic ways to create a VPN connection:

- VPN Gateway to VPN Gateway
- Computer (using VPN client software that supports IPSec) to VPN Gateway

The VPN Gateway creates a “tunnel” or channel between two endpoints, so that data transmissions between them are secure. A computer with VPN client software that supports IPSec can be one of the two endpoints. Any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN Gateway to create a VPN tunnel using IPSec (refer to *Appendix C: Configuring IPSec between a Windows 2000 or XP computer and the VPN Gateway*). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

Computer (using VPN client software that supports IPSec) to VPN Gateway

The following is an example of a computer-to-VPN Gateway VPN. In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has VPN client software that is configured with her office's VPN settings. She accesses the VPN client software that supports IPSec and connects to the VPN Gateway at the central office. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office's network, as if she were physically connected.



Figure 1-2: Computer-to-VPN Gateway



IMPORTANT: You must have at least one VPN Gateway on one end of the VPN tunnel. At the other end of the VPN tunnel, you must have a second VPN Gateway or a computer with VPN client software that supports IPSec.

VPN Gateway to VPN Gateway

An example of a VPN Gateway-to-VPN Gateway VPN would be as follows. At home, a telecommuter uses his VPN Gateway for his always-on Internet connection. His Gateway is configured with his office's VPN settings. When he connects to his office's Gateway, the two Gateways create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected.

For additional information and instructions about creating your own VPN, please visit Linksys's website at www.linksys.com or refer to *Appendix C: Configuring IPSec between a Windows 2000 or XP computer and the VPN Gateway*.

Why do I need a VPN?

With the flexibility that comes with computer networking, there is also an increased risk in security. This is why firewalls were first introduced. Firewalls help to protect data inside of a local network. But what do you do once information is sent outside of your local network, when emails are sent to their destination, or when you have to connect to your company's network when you are out on the road? How is your data protected?

That is when a VPN can help. VPNs secure data moving outside of your network as if it were still within that network.

When data is sent out across the Internet from your computer, it is always open to attacks. You may already have a firewall, which will help protect data moving around or held within your network from being corrupted or intercepted by entities outside of your network, but once data moves outside of your network - when you send data to someone via email or communicate with an individual over the Internet - the firewall will no longer protect that data.

At this point, your data becomes open to hackers using a variety of methods to steal not only the data you are transmitting but also your network login and security data. Some of the most common methods are as follows:

1) MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

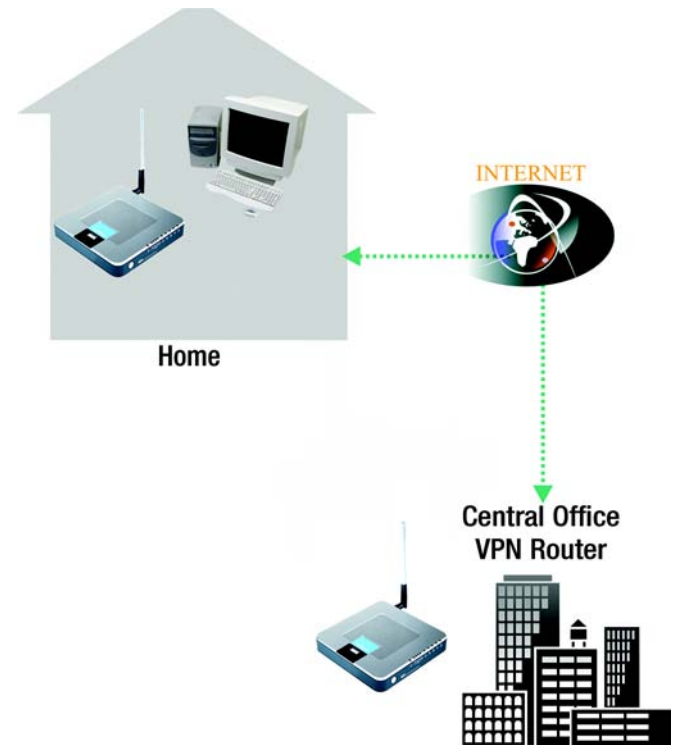


Figure 1-3: VPN Gateway-to-VPN Gateway

2) Data Sniffing

Data “sniffing” is a method used by hackers to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text.

3) Man in the Middle Attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a “man in the middle” attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the data to a new destination. Even though the data is not received by its intended recipient, it appears that way to the person sending the data.

These are only a few of the methods hackers use and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet will often pass through many different servers around the world before reaching its final destination. That's a long way to go for unsecured data and this is when a VPN serves its purpose.

Chapter 2: Getting to Know the Wireless-G ADSL Gateway with 2 Phone Ports

The Back Panel

The Gateway's ports, where a network cable is connected, are located on the back panel. The Gateway's Reset button is also located on the back panel.

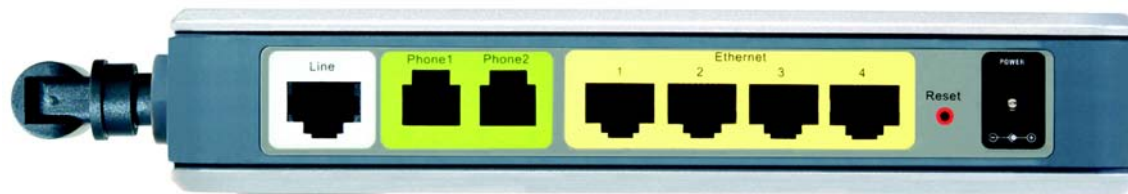


Figure 2-1: Back Panel

- LINE** The **LINE** port connects to the ADSL line.
- Phone (1 and 2)** The **Phone** ports connect to phones you wish to connect to your network.
- Ethernet (1-4)** The **Ethernet** ports connect to your computer and other network devices.
- Reset Button** There are two ways to Reset the Gateway's factory defaults. Either press the **Reset Button**, for approximately ten seconds, or restore the defaults from the Factory Defaults screen of the Administration tab in the Gateway's Web-Based Utility.
- Power** The **Power** port is where you will connect the power adapter.



Important: Resetting the Gateway to factory defaults will erase all of your settings (WEP Encryption, Wireless and Wired network settings, etc.) 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, where information about network activity is displayed, are located on the front panel.



Figure 2-2: Front Panel

Power	Green. The Power LED lights up when the Gateway is powered on.
Ethernet (1-4)	Green. The Ethernet LEDs serve two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through the network ports. If the LED is blinking, it is an indication of any network activity.
Wireless	Green. The Wireless LED lights up whenever there is a successful wireless connection. If the LED is blinking, the Gateway is actively sending or receiving data to or from one of the devices on the network.
Phone 1 and 2	Green. The Phone LEDs light up when a phone is connected to the corresponding port on the back panel
DSL	Green. The DSL LED lights up whenever there is a successful DSL connection. The LED blinks while establishing the ADSL connection.
Internet	Green. The Internet LED lights up green when an Internet connection to the Internet Service Provider (ISP) session is established. The Internet LED lights up red when the connection to the ISP fails.

Chapter 3: Connecting the Wireless-G ADSL Gateway

Overview

The Gateway's setup consists of more than simply plugging hardware together. You will have to configure your networked computers to accept the IP addresses that the Gateway assigns them (if applicable), and you will also have to 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 your modem 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 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."

Wired 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 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.
3. Connect a phone cable from the Line port on the Gateway's back panel to the wall jack of the ADSL line.



NOTE: A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.



IMPORTANT: For countries that have phone jacks with RJ-11 connectors, make sure to only place the microfilters between the phone and the wall jack and **not** between the Modem and the wall jack or your ADSL will not connect.

For countries that do **not** have phone jacks with RJ-11 connectors (e.g. France, Sweden, Switzerland, United Kingdom, etc.), except for ISDN users, the microfilter has to be used between the modem and the wall jack, because the microfilter will have the RJ-11 connector.

Annex B users must use the included special cable to connect the gateway to the wall jack (RJ-45 to RJ-12). If you require splitters or special jacks, please contact your service provider.

4. Connect any telephones you wish to run through your ADSL line to the Gateway's Phone ports.
5. Connect the power adapter to the Gateway's Power port, and then plug the power adapter into a power outlet. Turn the On/Off switch to On.

The Power LED on the front panel will light up green as soon as the power adapter is connected properly and the switch is turned on. The Power LED will flash for a few seconds, then it will light up steady when the self-test is complete. If the LED flashes for one minute or longer, see *Appendix A: Troubleshooting*.

6. Power on one of your computers that is connected to the Gateway.

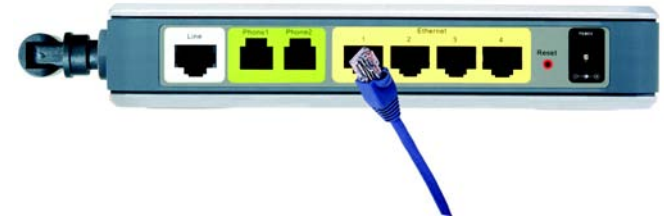


Figure 3-1: Connecting your networking devices



Figure 3-2: Connecting your ADSL line



Figure 3-3: Connecting your phones



Figure 3-4: Connecting the power



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 a phone cable from the Line port on the Gateway's back panel to the wall jack of the ADSL line.



NOTE: A small device called a microfilter (not included) may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.



NOTE: You should always change the SSID from its default, *linksys*, and enable WEP encryption.



IMPORTANT: For countries that have phone jacks with RJ-11 connectors, make sure to only place the microfilters between the phone and the wall jack and **not** between the Modem and the wall jack or your ADSL will not connect.

For countries that do **not** have phone jacks with RJ-11 connectors (e.g. France, Sweden, Switzerland, United Kingdom, etc.), except for ISDN users, the microfilter has to be used between the modem and the wall jack, because the microfilter will have the RJ-11 connector.

Annex B users must use the included special cable to connect the gateway to the wall jack (RJ-45 to RJ-12). If you require splitters or special jacks, please contact your service provider.

3. Connect any telephones you wish to run through your ADSL line to the Gateway's Phone ports.
4. Connect the power adapter to the Power port, and then plug the power adapter into a power outlet. Turn the On/Off switch to On.

The Power LED on the front panel will light up green as soon as the power adapter is connected properly and the switch is turned on. The Power LED will flash for a few seconds, then light up steady when the self-test is complete. If the LED flashes for one minute or longer, see *Appendix A: Troubleshooting*.

5. Power on one of the computers on your wireless network(s).
6. 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 that Wireless Security 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.

The Gateway's hardware installation is now complete.

Go to *Chapter 4: Configuring the Gateway*.

Chapter 4: Configuring the 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:

- **Basic Setup.** On the Basic Setup screen, enter the settings provided by your ISP.
- **Management.** Click the **Administration** tab and then the **Management** tab. The 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, Status and Voice. Additional tabs will be available after you click one of the main tabs.

Setup

- **Basic Setup.** Enter the Internet connection and network settings on this screen.
- **DDNS.** To enable the Gateway's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.
- **Advanced Routing.** On this screen, you can alter Dynamic Routing, and Static Routing configurations.

Wireless

- **Basic Wireless Settings.** You can choose your Wireless Network Mode and Wireless Security on this screen.
- **Wireless Security.** There are three Wireless Security settings for configuring the security of your wireless network: WPA Pre-Shared Key, WPA RADIUS, and WEP.
- **Wireless Network Access.** This screen displays your wireless network access list.
- **Advanced Wireless Settings.** On this screen you can access the Advanced Wireless features.



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.

Security

- **Firewall.** This screen contains Filters and Block WAN Requests. Filters block specific internal users from accessing the Internet and block anonymous Internet requests.
- **VPN.** To enable or disable IPSec, PPPoE, L2TP, and/or PPTP Pass-through, and set up VPN tunnels, use this screen.

Access Restrictions

- **Parental Control.** This screen allows parents to manage Internet access by all of the network's users.
- **Internet Access.** This screen allows you to prevent or permit only certain users from attaching to your network.

Applications & Gaming

- **Single Port Forwarding.** Use this screen to set up common services or applications on your network.
- **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.
- **QoS.** This allows prioritization of applications on your network.

Administration

- **Management.** On this screen, alter Gateway access privileges, SNMP, UPnP, and WT-82 settings.
- **Reporting.** If you want to view or save activity logs, click this tab.
- **Diagnostics.** Use this screen to do a Ping Test.
- **Backup & Restore.** From this screen, you can backup and restore the Gateway's settings.
- **Factory Defaults.** If you want to restore the Gateway's factory defaults, use this screen.
- **Firmware Upgrade.** Click this tab if you want to upgrade the Gateway's firmware.

Wireless-G ADSL Gateway with 2 Phone Ports

- **Reboot.** From this screen, you can reboot the Gateway.

Status

- **Gateway.** This screen provides status information about the Gateway.
- **Local Network.** This provides status information about the local network.
- **Wireless.** This screen provides status information about the wireless network.
- **DSL Connection.** This screen provides status information about the DSL connection.
- **Vocie.** This screen provides status information about the voice features.

Voice

- **Voice Authentication.** This screen is used by your ISP to set voice configuration

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, 192.168.1.1, in the Address field. Then press Enter.

A password request page will appear. (Windows XP users will see a slightly different screen.) Enter **admin** (the default user name) in the User Name field, and enter **admin** (the default password) in the Password field. Then, click the **OK** button.



Figure 4-1: 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.

Internet Setup

PVC Connection. Select a PVC connection number from the drop-down menu. Then, select the **Enable Now** to enable the connection.

Internet Connection Type. The Gateway supports six types (or Encapsulations): RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA, IPoA, and Bridged Mode Only. Each Basic Setup screen and available features will differ depending on what type of encapsulation you select.

The screenshot shows the 'Basic Setup' tab in the Linksys configuration interface. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', 'Status', and 'Voice'. The 'Setup' tab is selected, and the 'Basic Setup' sub-tab is active. The interface is organized into several sections:

- Internet Setup:**
 - PVC Connection:** 'Please Select a Connection:' dropdown menu.
 - Internet Connection Type:** 'Encapsulation:' dropdown menu (set to RFC1483 Bridged), 'Multiplexing:' radio buttons (LLC selected), 'QoS Type:' dropdown menu (UBR), 'Per Rate:' and 'Scr Rate:' input fields (both 0 cps), 'AutoDetect:' radio buttons (Disable selected), 'Virtual Circuit:' input field (0), 'VPI (Range 0-255):' input field (35), 'VCI (Range 32-65535):' input field (35), 'DSL Modulation:' dropdown menu (G.dmt).
 - IP Settings:** 'Obtain an IP Address Automatically' radio button selected; 'Use the following IP Address:' radio button unselected. Fields for Internet IP Address, Subnet Mask, Gateway, Primary DNS, and Secondary DNS.
 - DNS Proxy:** 'DNS Proxy:' radio buttons (Enable selected).
 - Optional Settings (required by some ISPs):** Fields for Host Name, Domain Name, MTU (Auto), and Size (1500).
- Network Setup:**
 - Router IP:** 'Local IP Address:' (192.168.1.1) and 'Subnet Mask:' (255.255.255.0).
 - Network Address Server Settings (DHCP):** 'Local DHCP Server:' radio buttons (Enable selected), 'DHCP Relay Server:' radio buttons (Disable selected), 'AutoDetect LAN DHCP Server:' radio buttons (Enable selected), 'Starting IP Address:' (192.168.1.64), 'Maximum Number of DHCP Users:' (191), 'Client Lease Time:' (0 minutes), 'Static DNS 1, 2, 3:' input fields (all 0), 'WINS:' input fields (all 0).
- Time Setting:**
 - 'Time Zone:' dropdown menu (GMT-08:00 Pacific Time (USA & Canada)).
 - 'Time Interval:' input field (3600 seconds).
 - Checkbox for 'Automatically adjust clock for daylight saving changes' (checked).

At the bottom right, there are 'Save Settings' and 'Cancel Changes' buttons, and the Cisco Systems logo.

Figure 4-2: Setup Tab - Basic Setup

RFC 1483 Bridged

VC Settings. You will configure your Virtual Circuit (VC) settings in this section.

- **Multiplexing.** Select **LLC** or **VC**, depending on your ISP.
- **QoS Type.** Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are not time sensitive, such as e-mail; or **VBR** (Variable Bite Rate) for Bursty traffic and bandwidth-sharing with other applications.
- **Pcr (Peak Cell Rate) Rate.** If required by your service provider, divide the DSL line rate by 424 to get the maximum rate at which the sender can send cells. Enter the rate in this field.
- **Scr (Sustain Cell Rate) Rate.** The average cell rate that can be transmitted, this value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
- **Autodetect:** Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
- **Virtual Circuit.** These fields consist of two items: **VPI** (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.
- **DSL Modulation.** Select from the drop-down menu: **Multimode**, **T1.413**, **G.dmt**, or **G.lite**. The default value is Multimode. Your ISP may provide custom setting for this field.

Internet Connection Type

VC Settings

Encapsulation: RFC 1483 Bridged

Multiplexing: LLC VC

QoS Type: UBR

Pcr Rate: 0 cps

Scr Rate: 0 cps

Autodetect: Enable Disable

Virtual Circuit: 0 VPI (Range 0-255)

35 VCI (Range 32-65535)

DSL Modulation: G.dmt

IP Settings

Obtain an IP Address Automatically

Use the following IP Address:

Internet IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

PPPoE Session: Disable

Figure 4-3: Basic Setup Tab - RFC 1483 Bridged

IP Settings. Follow the instructions in the section for your type of encapsulation.

Select **Obtain an IP Address Automatically** if you are connecting through a dynamic IP address. If you are required to use a permanent (static) IP address to connect to the Internet, select **Use the following IP Address**.

- Internet IP Address. This is the Gateway's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.
- 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.
- PPPoE Session. To connect using a PPPoE Session, select **Enable** from the drop-down menu. Configure the Service Name, User Name, and Password settings provided by your ISP. Enter the domain name in the Match Domain Name field.
Connect on Demand. If you want the Router to end the Internet connection after it has been inactive for a period of time, select Connect on Demand and designate the number of minutes you want that period of inactivity to last.
Keep Alive. If you want the Router to periodically check your Internet connection, select Keep Alive. Then specify how often you want the Router to check the Internet connection. If the connection is down, the Router will automatically re-establish your connection.

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.

RFC 1483 Routed

VC Settings. You will configure your Virtual Circuit (VC) settings in this section.

- **Multiplexing.** Select **LLC** or **VC**, depending on your ISP.
- **QoS Type.** Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are not time sensitive, such as e-mail; or **VBR** (Variable Bite Rate) for Bursty traffic and bandwidth-sharing with other applications.
- **Pcr (Peak Cell Rate) Rate.** If required by your service provider, divide the DSL line rate by 424 to get the maximum rate at which the sender can send cells. Enter the rate in this field.
- **Scr (Sustain Cell Rate) Rate.** The average cell rate that can be transmitted, this value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
- **Autodetect:** Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
- **Virtual Circuit.** These fields consist of two items: **VPI** (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.
- **DSL Modulation.** Select from the drop-down menu: **Multimode**, **T1.413**, **G.dmt**, or **G.lite**. The default value is Multimode. Your ISP may provide custom setting for this field.

IP Settings. Follow the instructions in the section for your type of encapsulation.

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

Internet Connection Type	
VC Settings	
Encapsulation:	RFC 1483 Routed
Multiplexing:	<input checked="" type="radio"/> LLC <input type="radio"/> VC
Qos Type:	UBR
Pcr Rate:	0 cps
Scr Rate:	0 cps
Autodetect:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual Circuit:	0 VPI (Range 0-255)
	35 VCI (Range 32-65535)
DSL Modulation:	G.dmt
IP Settings	
Internet IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Gateway:	0 . 0 . 0 . 0
Primary DNS:	0 . 0 . 0 . 0
Secondary DNS:	0 . 0 . 0 . 0

Figure 4-4: Basic Setup Tab - RFC 1483 Routed

IPoA

If you are required to use IPoA (IP over ATM), then select IPoA.

VC Settings. You will configure your Virtual Circuit (VC) settings in this section.

- Multiplexing. Select **LLC** or **VC**, depending on your ISP.
- QoS Type. Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are not time sensitive, such as e-mail; or **VBR** (Variable Bite Rate) for Bursty traffic and bandwidth-sharing with other applications.
- Pcr (Peak Cell Rate) Rate. If required by your service provider, divide the DSL line rate by 424 to get the maximum rate at which the sender can send cells. Enter the rate in this field.
- Scr (Sustain Cell Rate) Rate. The average cell rate that can be transmitted, this value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
- Autodetect: Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
- Virtual Circuit. These fields consist of two items: **VPI** (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.
- DSL Modulation. Select from the drop-down menu: **Multimode**, **T1.413**, **G.dmt**, or **G.lite**. The default value is Multimode. Your ISP may provide custom setting for this field.

The screenshot shows the configuration interface for IPoA. On the left, a sidebar indicates the current section is 'VC Settings'. The main area is divided into two sections: 'VC Settings' and 'IP Settings'. Under 'VC Settings', the following options are visible: Encapsulation is set to 'IPoA'; Multiplexing has radio buttons for 'LLC' (selected) and 'VC'; QoS Type is a dropdown menu set to 'UBR'; Pcr Rate and Scr Rate are input fields both set to '0' with units 'cps'; Autodetect has radio buttons for 'Enable' and 'Disable' (selected); Virtual Circuit consists of two input fields: 'VPI (Range 0-255)' set to '0' and 'VCI (Range 32-65535)' set to '35'; DSL Modulation is a dropdown menu set to 'G.dmt'. Under 'IP Settings', there are five input fields for IP addresses: 'Internet IP Address', 'Subnet Mask', 'Gateway', 'Primary DNS', and 'Secondary DNS', all of which are set to '0.0.0.0'.

Figure 4-5: Basic Setup Tab - IPoA

IP Settings. Follow the instructions in the section for your type of encapsulation.

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

RFC 2516 PPPoE

VC Settings. You will configure your Virtual Circuit (VC) settings in this section.

- **Multiplexing.** Select **LLC** or **VC**, depending on your ISP.
- **QoS Type.** Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are not time sensitive, such as e-mail; or **VBR** (Variable Bite Rate) for Bursty traffic and bandwidth-sharing with other applications.
- **Pcr (Peak Cell Rate) Rate.** If required by your service provider, divide the DSL line rate by 424 to get the maximum rate at which the sender can send cells. Enter the rate in this field.
- **Scr (Sustain Cell Rate) Rate.** The average cell rate that can be transmitted, this value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
- **Autodetect:** Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
- **Virtual Circuit.** These fields consist of two items: **VPI** (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.
- **DSL Modulation.** Select from the drop-down menu: **Multimode**, **T1.413**, **G.dmt**, or **G.lite**. The default value is Multimode. Your ISP may provide custom setting for this field.

Internet Connection Type	
VC Settings	
Encapsulation:	RFC 2516 PPPoE
Multiplexing:	<input checked="" type="radio"/> LLC <input type="radio"/> VC
Qos Type:	UBR
Pcr Rate:	0 cps
Scr Rate:	0 cps
Autodetect:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual Circuit:	0 VPI (Range 0-255)
	35 VCI (Range 32-65535)
DSL Modulation:	G.dmt
PPPoE Settings	
Service Name:	
User Name:	
Password:	
<input checked="" type="radio"/> Connect on Demand: Max Idle Time 20 Min.	
<input type="radio"/> Keep Alive: Redial Period 20 Sec.	
Second PPPoE:	Enable
Service Name:	
User Name:	
Password:	
Match Domain Name:	
<input checked="" type="radio"/> Connect on Demand: Max Idle Time 20 Min.	
<input type="radio"/> Keep Alive: Redial Period 20 Sec.	

Figure 4-6: Basic Setup Tab - RFC 2516 PPPoE

PPPoE Settings. Follow the instructions in the section for your type of encapsulation.

- **PPPoE Session.** Configure the Service Name, User Name, and Password settings provided by your ISP. Enter the domain name in the Match Domain Name field.
Connect on Demand. If you want the Router to end the Internet connection after it has been inactive for a period of time, select Connect on Demand and designate the number of minutes you want that period of inactivity to last.
Keep Alive. If you want the Router to periodically check your Internet connection, select Keep Alive. Then specify how often you want the Router to check the Internet connection. If the connection is down, the Router will automatically re-establish your connection.
- **Second PPPoE.** To use a second PPPoE, select **Enable** from the drop-down menu. Configure the Service Name, User Name, and Password settings. Enter the domain name in the Match Domain Name field.
Connect on Demand. If you want the Router to end the Internet connection after it has been inactive for a period of time, select Connect on Demand and designate the number of minutes you want that period of inactivity to last.
Keep Alive. If you want the Router to periodically check your Internet connection, select Keep Alive. Then specify how often you want the Router to check the Internet connection. If the connection is down, the Router will automatically re-establish your connection.

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.

RFC 2364 PPPoA

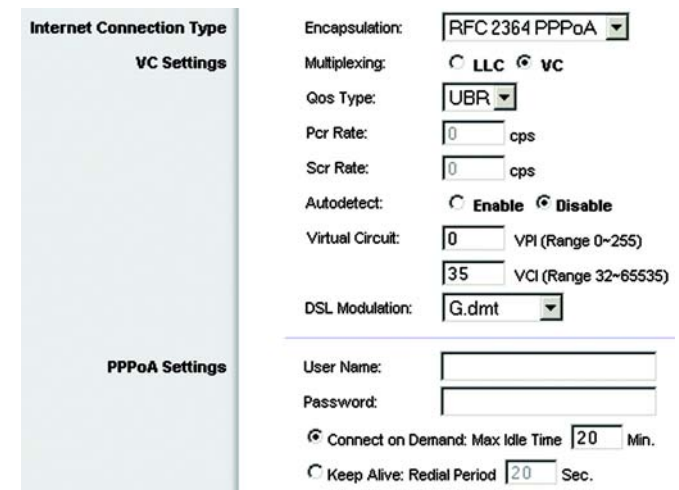
VC Settings. You will configure your Virtual Circuit (VC) settings in this section.

- **Multiplexing.** Select **LLC** or **VC**, depending on your ISP.
- **QoS Type.** Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are not time sensitive, such as e-mail; or **VBR** (Variable Bite Rate) for Bursty traffic and bandwidth-sharing with other applications.
- **Pcr (Peak Cell Rate) Rate.** If required by your service provider, divide the DSL line rate by 424 to get the maximum rate at which the sender can send cells. Enter the rate in this field.
- **Scr (Sustain Cell Rate) Rate.** The average cell rate that can be transmitted, this value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
- **Autodetect:** Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
- **Virtual Circuit.** These fields consist of two items: **VPI** (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.
- **DSL Modulation.** Select from the drop-down menu: **Multimode**, **T1.413**, **G.dmt**, or **G.lite**. The default value is Multimode. Your ISP may provide custom setting for this field.

PPPoA Settings. Follow the instructions in the section for your type of encapsulation.

- **PPPoA Session.** Configure the Service Name, User Name, and Password settings provided by your ISP. Enter the domain name in the Match Domain Name field.
Connect on Demand. If you want the Router to end the Internet connection after it has been inactive for a period of time, select Connect on Demand and designate the number of minutes you want that period of inactivity to last.
Keep Alive. If you want the Router to periodically check your Internet connection, select Keep Alive. Then specify how often you want the Router to check the Internet connection. If the connection is down, the Router will automatically re-establish your connection.

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.



Internet Connection Type

VC Settings

Encapsulation: RFC 2364 PPPoA

Multiplexing: LLC VC

Qos Type: UBR

Pcr Rate: 0 cps

Scr Rate: 0 cps

Autodetect: Enable Disable

Virtual Circuit: 0 VPI (Range 0~255)
35 VCI (Range 32~65535)

DSL Modulation: G.dmt

PPPoA Settings

User Name:

Password:

Connect on Demand: Max Idle Time 20 Min.

Keep Alive: Redial Period 20 Sec.

Figure 4-7: Basic Setup Tab - RFC 2364 PPPoA

Bridged Mode Only

If you are using your Gateway as a bridge, which makes the Gateway act like a standalone modem, select **Bridged Mode Only**. All NAT and routing is disabled in this mode.

VC Settings. You will configure your Virtual Circuit (VC) settings in this section.

- Multiplexing. Select **LLC** or **VC**, depending on your ISP.
- QoS Type. Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are not time sensitive, such as e-mail; or **VBR** (Variable Bite Rate) for Bursty traffic and bandwidth-sharing with other applications.
- Pcr (Peak Cell Rate) Rate. If required by your service provider, divide the DSL line rate by 424 to get the maximum rate at which the sender can send cells. Enter the rate in this field.
- Scr (Sustain Cell Rate) Rate. The average cell rate that can be transmitted, this value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).
- Autodetect: Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.
- Virtual Circuit. These fields consist of two items: **VPI** (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields.
- DSL Modulation. Select from the drop-down menu: **Multimode**, **T1.413**, **G.dmt**, or **G.lite**. The default value is Multimode. Your ISP may provide custom setting for this field.

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 screenshot shows the 'Internet Connection Type' tab with the 'VC Settings' section expanded. The configuration is as follows:

Encapsulation:	Bridge Mode Only
Multiplexing:	<input checked="" type="radio"/> LLC <input type="radio"/> VC
Qos Type:	UBR
Pcr Rate:	0 cps
Scr Rate:	0 cps
Autodetect:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Virtual Circuit:	0 VPI (Range 0~255)
	35 VCI (Range 32~65535)
DSL Modulation:	G.dmt

Figure 4-8: Basic Setup Tab - Bridged Mode Only

DNS Proxy

If the PCs on your network are enabled with DNS, enable the DNS Proxy to forward the DNS entries.

Optional Settings

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

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

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

Network Setup

The Network Setup section changes the settings on the network connected to the Router's Ethernet ports. Wireless Setup is performed through the Wireless tab.

Router IP

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

Network Address Server Settings (DHCP)

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, you must configure all of your network PCs to connect to a DHCP server (the Router), and make sure there is no other DHCP server on your network.

Local DHCP Server. 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, you should leave the Gateway enabled as a DHCP server.

DHCP Relay Server. If you have a local DHCP server that you would like to use instead, enable the DHCP Relay mode for the Local DHCP Server setting and enter the IP address of the DHCP server.

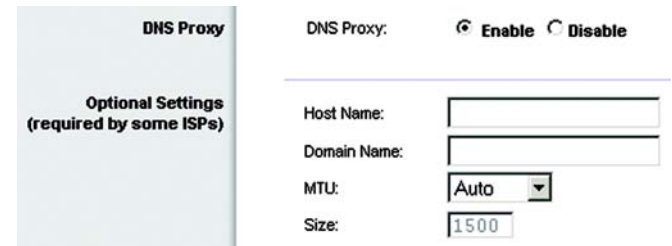


Figure 4-9: Basic Setup Tab - DNS Proxy and Optional Settings

AutoDetect LAN DHCP Server. If you want the Gateway to automatically detect a DHCP server on the local network, then select the **Enable** radio button. (When this feature is enabled, the **DHCP Relay** radio button for the *Local DHCP Server* setting will be unavailable.) Otherwise, keep the default, **Disable**.

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

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

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

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

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

Time Setting

Change the time zone in which your network functions from this pull-down menu. (You can even automatically adjust for daylight savings time.)

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 screenshot shows the 'Network Setup' configuration page. It is split into two main sections: 'Network Address Server Settings (DHCP)' and 'Time Setting'.
In the DHCP section:
- Local IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Local DHCP Server: Radio buttons for 'Enable', 'Disable', and 'DHCP Relay'. 'Disable' is selected.
- DHCP Relay Server: 0.0.0.0 with an 'Advanced' button.
- AutoDetect LAN DHCP Server: Radio buttons for 'Enable' and 'Disable'. 'Disable' is selected.
- Starting IP Address: 192.168.1.64
- Maximum Number of DHCP Users: 191
- Client Lease Time: 0 minutes (0 means one day)
- Static DNS 1, 2, and 3: All set to 0.0.0.0
- WINS: 0.0.0.0
In the Time Setting section:
- Time Zone: (GMT-08:00) Pacific Time (USA & Canada)
- Time Interval: 3600 seconds
- A checkbox 'Automatically adjust clock for daylight saving changes' is checked.

Figure 4-10: Basic Setup Tab - Network Setup

The DDNS Tab

The Gateway offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Gateway.

Before you can use this feature, you need to sign up for DDNS service at DynDNS.org or TZO.com.

DDNS

DDNS Service. Select your DDNS service, either DynDNS.org or TZO.com, from the drop-down menu. To disable DDNS Service, select **Disabled**.

DynDNS.org. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org in the spaces provided. The Gateway's current Internet IP Address and DDNS service connection status will be displayed beneath.

TZO.com. Enter the Email Address, TZO Password Key, and Domain Name of the service you set up with TZO. The Gateway's current Internet IP Address and DDNS service connection status will be displayed beneath.

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 4-11: Setup Tab - DDNS (DynDNS.org)



Figure 4-12: Setup Tab - DDNS (TZO.com)

Advanced Routing Tab

The Advanced Routing screen allows you to configure the dynamic routing and static routing settings.

Advanced Routing

Operating Mode. NAT is a security feature that is enabled by default. It enables the Gateway to translate IP addresses of your local area network to a different IP address for the Internet. To disable NAT, click the **Disabled** radio button.

Dynamic Routing/RIP. With Dynamic Routing you can enable the Gateway to automatically adjust to physical changes in the network's layout. The Gateway, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other Gateways on the network. To enable RIP, click **Enabled**. To disable RIP, click **Disabled**.

- Transmit RIP Version. To transmit RIP messages, select the protocol you want: **RIP1**, **RIP1-Compatible**, or **RIP2**. If you don't want to transmit RIP messages, select **Disable**.
- Receive RIP Version. To receive RIP messages, select the protocol you want: **RIP1** or **RIP2**. If you don't want to receive RIP messages, select **Disable**.

Static Routing. If the Gateway is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To create a static route, change the following settings:

- Select set number. Select the number of the static route from the drop-down menu. The Gateway supports up to 20 static route entries. If you need to delete a route, after selecting the entry, click the **Delete This Entry** button.
- Destination IP Address. The Destination IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, set the network portion of the IP address to 0.
- Subnet Mask. The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway. This IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host.



Figure 4-13: Setup Tab - Advanced Routing

Wireless-G ADSL Gateway with 2 Phone Ports

- **Hop Count.** Hop Count is the number of hops to each node until the destination is reached (16 hops maximum). Enter the Hop Count in the field.
- **Show Routing Table.** Click the **Show Routing Table** button to open a screen displaying how data is routed through your network. For each route, the Destination IP address, Subnet Mask, Gateway, and Interface are displayed. Click the **Refresh** button to update the information. Click the **Close** button to return to the previous screen.

PVC Routing Policy. PVC stands for "Permanent Virtual Circuit". It is a virtual circuit link between two nodes for ATM (Asynchronous Transfer Mode) network. Each PVC functions as a separate Internet connection. PVC settings are for **ADVANCED USERS ONLY**. The PVC routing table allows you to select which traffic type to be forwarded to which PVC. Click the **PVC Routing Setting** button to open the PVC Routing table.

- Please select active connection. Select your active Internet connection from this pull-down menu.
- **Destination.** Enter the destination Internet IP Address and Network Mask where this PVC will send data.
- **Source.** Enter the source IP Address and Network Mask where this PVC will originate.
- **Source Mac.** Enter the source MAC Address of the network PC where the data originates.
- **Protocol.** Enter the data's protocol, either TCP,UDP or ALL.
- **Dst Port.** Enter the destination port number where this PVC will send data.
- **Src Port.** Enter the source port number where this PVC will originate.
- **802.1D User Priority.** This uses the 802.1D header requirement to set prioritization. The number range is 0~7 depending on the type of services, with 7 having the highest priority.
- **802.3 Type/Length.** Enter the Ethernet type for a specific protocol.
- **802.1Q Vlan ID.** This is the ID for VLANs, from 0 ~ 4095
- **PacketLength.** This is the total packet length of an IP packet, from 20byte~65535bytes.
- **DSCP.** Enter the TOS (Type of Service) in the IP header here. Possible values are 0x00 to 0x3f, the last two Hex values are the variables.
- **Apply.** Check this and click the **Save** button to apply your changes

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.

Destination LAN IP	Subnet Mask	Gateway	Hop count	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	LAN & Wireless

Figure 4-14: Routing Table

Destination	Source	Protocol	Dst Port	Src Port	User Priority	802.3 Type/Length	802.1Q Vlan ID	PacketLength	DSCP	Apply
0.0.0.0	0.0.0.0	ALL								
0.0.0.0	0.0.0.0	TCP								
0.0.0.0	0.0.0.0	UDP								
0.0.0.0	0.0.0.0	ALL								

Figure 4-15: PVC Selection Table

The Wireless Tab

Basic Wireless Settings Tab

This screen allows you to choose your wireless network mode and wireless security.

Wireless Network

Wireless Network Mode. 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**.

Wireless Network Name (SSID). Enter the name for your wireless network into the field. The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. 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, between 1 and 11 (in North America). 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 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**.

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 4-16: Wireless Tab - Wireless Network

Wireless Security Tab

The Gateway's wireless security settings configure the security of your wireless network. There are three wireless security mode options supported by the Gateway: WPA Pre-Shared Key, WPA RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) These 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 **Disable** from the drop-down menu for Security Mode.

WPA Pre-Shared Key. Enter a WPA Shared Key of 8-32 characters. Then, enter a Group Key Renewal period, which instructs the Gateway how often it should change the encryption keys.



Figure 4-17: Wireless Tab - Wireless Security (WPA Pre-Shared Key)

WPA RADIUS. This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Gateway.) Enter the RADIUS server's IP Address and port number, along with a key shared between the Gateway and the server. Then, enter a Key Renewal Timeout, which instructs the Gateway how often it should change the encryption keys.



Figure 4-18: Wireless Tab - Wireless Security (WPA RADIUS)

Wireless-G ADSL Gateway with 2 Phone Ports

WPA2 Professional. WPA2 gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES, or TKIP + AES. Enter a WPA Shared Key of 8-63 characters. Then enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys.

WPA2 Enterprise. This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) First, select the type of WPA2 algorithm you want to use, AES, or TKIP + AES. Enter the RADIUS server's IP Address and port number, along with a key shared between the Router and the server. Last, enter a Key Renewal Timeout, which instructs the Router how often it should change the encryption keys.

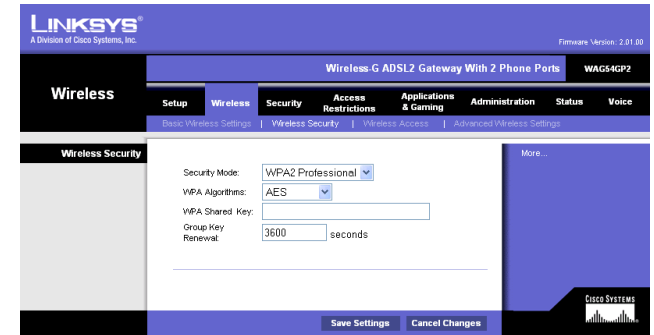


Figure 4-19: Wireless Tab - Wireless Security (WPA2 Professional)

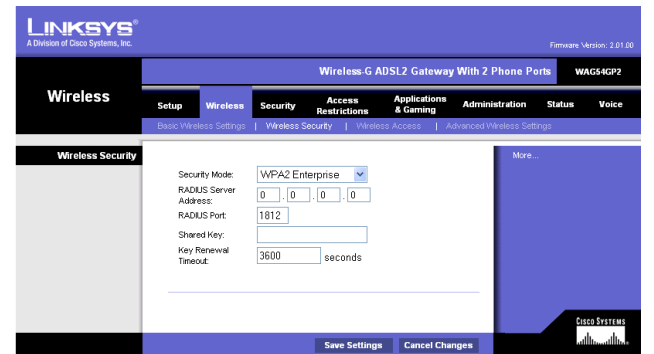


Figure 4-20: Wireless Tab - Wireless Security (WPA2 Enterprise)

WEP. WEP is a basic encryption method, which is not as secure as WPA. To use WEP, select a Default Key (choose which Key to use), and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Then either generate a WEP key using a Passphrase or enter the WEP key manually.

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

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



Figure 4-21: Wireless Tab - Wireless Security (WEP)

Wireless Access Tab

Wireless Network Access

Selecting **Allow All**, from the Wireless Access tab, allows access to the wireless network from any PC. To restrict access to the network, select **Restrict Access**, then select **Prevent** to prevent access or **Permit only** to permit access. Click the **Edit MAC Address Access List** button, and the screen will appear.

Select the MAC Address from the list and click **Wireless Client MAC List**.

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 4-22: Wireless Tab - Wireless Network Access



Figure 4-23: MAC Address Access/Filter List

Advanced Wireless Settings Tab

Advanced Wireless

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

Authentication Type. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient won't use a WEP key for authentication but can use WEP for data encryption. If you want to allow Open System authentication, select **Open System**. For Shared Key authentication, the sender and recipient use a WEP key for both authentication and data encryption. If you want to use only Shared Key authentication, select **Shared Key**. This option should be left in the default (Auto) mode, as some clients cannot be configured for Shared Key.

Control Tx Rates. The default transmission rate is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. Select from the range of speeds, or have the Gateway automatically use the fastest possible data rate, be default, and enable the Auto-Fallback feature.

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, 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 of a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

RTS Threshold. This value should remain at its default setting of **2347**. The range is 0-2347 bytes. If you encounter inconsistent data flow, only make minor modifications. 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.



Figure 4-24: Wireless Tab - Advanced Wireless Settings

The Security Tab

Firewall

When you click the *Security* tab, you will see the *Firewall* screen. This screen contains Filters and the option to Block WAN Requests. Filters block specific Internet data types and block anonymous Internet requests. To add Firewall Protection, click **Enable**. If you do not want Firewall Protection, click **Disable**.

Additional Filters

Filter Proxy. Use of proxy servers may compromise the Gateway's security. If this box is checked, you will be unable to access any proxy servers. To enable proxy filtering, click **Enabled**.

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 **Enabled**.

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 this programming language. To enable Java Applet filtering, click **Enabled**.

Filter ActiveX. ActiveX is a programming language for websites. If you enable ActiveX filtering, you may not have access to Internet sites created using this programming language. To enable ActiveX filtering, click **Enabled**.

Block WAN requests

Block Anonymous Internet Requests. This keeps your network from being “pinged” or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to discover your network. Select **Block Anonymous Internet Requests** to block anonymous Internet requests or de-select it 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.



Figure 4-25: Security Tab - Firewall

VPN

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.

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.

PPPoE Passthrough. The PPPoE (Point-to-Point Protocol over Ethernet) option is included for those users who wish to disable PPPoE sessions. This option is enabled by default. To disable PPPoE 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.

L2TP Passthrough. Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used to enable the operation of a VPN over the Internet. To allow L2TP Passthrough, click the **Enable** button. To disable L2TP Passthrough, click the **Disable** button.

IPSec VPN Tunnel

The VPN Gateway creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure.

To establish this tunnel, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. It is possible to create up to five simultaneous tunnels. Then click **Enabled** to enable the IPSec VPN tunnel. Once the tunnel is enabled, enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel. To delete a tunnel entry, select the tunnel, then click **Delete**. To view a summary of the settings, click **Summary**.

Local Secure Group and Remote Secure Group. The Local Secure Group is the computer(s) on your network that can access the tunnel. The Remote Secure Group is the computer(s) on the remote end of the tunnel that can access the tunnel. These computers can be specified by a Subnet, specific IP address, or range.

Local Security Gateway. This pull-down menu will provide you with your available Internet connection options.

The screenshot shows the Linksys Security Tab - VPN configuration page. The page is divided into several sections:

- VPN Passthrough:** Includes checkboxes for IPSec Passthrough, PPPoE Passthrough, PPTP Passthrough, and L2TP Passthrough, each with 'Enable' and 'Disable' radio buttons.
- IPSec VPN Tunnel:** Features a 'Select Tunnel Entry' dropdown menu (set to '1 (-)'), a 'Delete' button, and a 'Summary' button. Below this are fields for 'IPSec VPN Tunnel' (Enabled/Disabled) and 'Tunnel Name'.
- Local Secure Group:** Includes a 'Subnet' dropdown and IP/Mask input fields.
- Local Security Gateway:** A dropdown menu currently set to 'No WAN Connection'.
- Remote Secure Group:** Includes a 'Subnet' dropdown and IP/Mask input fields.
- Remote Security Gateway:** Includes an 'IP Addr.' dropdown and IP input fields.
- Key Management:** Includes an 'Encryption' dropdown (set to 'DES'), an 'Authentication' dropdown (set to 'MD5'), and a 'Key Management' dropdown (set to 'Auto (IKE)').
- Status:** Shows 'Disconnected' with 'Connect', 'View Logs', and 'Advanced Settings' buttons.

Figure 4-26: Security Tab - VPN

The screenshot shows the VPN Settings Summary page. It includes a 'Refresh' button and a table with the following structure:

No.	Tunnel Name	Status	Local Group	Remote Group	Remote Gateway	Security Method
WAN IP: 0.0.0.0						

Figure 4-27: VPN Settings Summary

Remote Security Gateway. The Remote Security Gateway is the VPN device, such as a second VPN Gateway, on the remote end of the VPN tunnel. Enter the IP Address or Domain of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Gateway, a VPN Server, or a computer with VPN client software that supports IPSec. The IP Address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Gateway, but the IP Address of the remote VPN Gateway or device with which you wish to communicate. If you enter an IP address, only the specific IP Address will be able to access the tunnel. If you select **Any**, any IP Address can access the tunnel.

- **Encryption.** Using Encryption also helps make your connection more secure. There are two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable. DES is selected by default.
- **Authentication.** Authentication acts as another level of security. There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, if the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication. In the Manual Key Management screen, MD5 (the default) has been selected.

Key Management. Select **Auto (IKE)** or **Manual** from the drop-down menu. The two methods are described below.

- **Auto (IKE).** Select **Auto (IKE)** and enter a series of numbers or letters in the Pre-shared Key field. Based on this word, which **MUST** be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may select to have the key expire at the end of a time period. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely. Check the box next to PFS (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure.
- **Manual.** Select **Manual**, then select the Encryption Algorithm from the drop-down menu. Enter the Encryption Key in the field (if you chose DES for your Encryption Algorithm, enter 16 hexadecimal characters, if you chose 3DES, enter 48 hexadecimal characters). Select the Authentication Algorithm from the drop-down menu. Enter the Authentication Key in the field (if you chose MD5 for your Authentication Algorithm, enter 32 hexadecimal characters, if you chose SHA1, enter 40 hexadecimal characters). Enter the Inbound and Outbound SPIs in the respective fields.

Status. The status of the connection is shown.

The screenshot shows the 'Key Management' configuration window. At the top, a dropdown menu is set to 'Auto (IKE)'. Below it, there are three main sections: 'PFS:' with radio buttons for 'Enabled' and 'Disabled' (where 'Disabled' is selected); 'Pre-shared Key:' with an empty text input field; and 'Key Lifetime:' with a text input field containing '3600' and a 'Sec.' label to its right.

Figure 4-28: Auto Key Management

The screenshot shows the 'Key Management' configuration window with the dropdown menu set to 'Manual'. It features four input fields: 'Encryption Key:' (empty), 'Authentication Key:' (empty), 'Inbound SPI:' (with '0x' on the left and '(0x100-0xFFFF)' on the right), and 'Outbound SPI:' (with '0x' on the left and '(0x100-0xFFFF)' on the right).

Figure 4-29: Manual Key Management

Click the **Connect** button to connect your VPN tunnel. Click **View Logs** to view system, UPnP, VPN, firewall, access, or all logs. Click the **Advanced Settings** button and the Advanced IPsec VPN Tunnel Setup screen will appear.

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.

Advanced VPN Tunnel Setup

From the Advanced IPsec VPN Tunnel Setup screen you can adjust the settings for specific VPN tunnels.

Phase 1

Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPsec SAs, which are then used to key IPsec sessions.

Operation Mode. There are two modes: **Main** and **Aggressive**, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Gateway will accept both Main and Aggressive requests from the remote VPN device.

Encryption. Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: **DES** and **3DES**. 3DES is recommended because it is more secure.

Authentication. Select the method used to authenticate ESP packets. There are two choices: **MD5** and **SHA**. SHA is recommended because it is more secure.

Group. There are two Diffie-Hellman Groups to choose from: **768-bit** and **1024-bit**. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Life Time. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Phase 2

Encryption. The encryption method selected in Phase 1 will be displayed.

Authentication. The authentication method selected in Phase 1 will be displayed.

PFS. The status of PFS will be displayed.



Figure 4-30: System Log

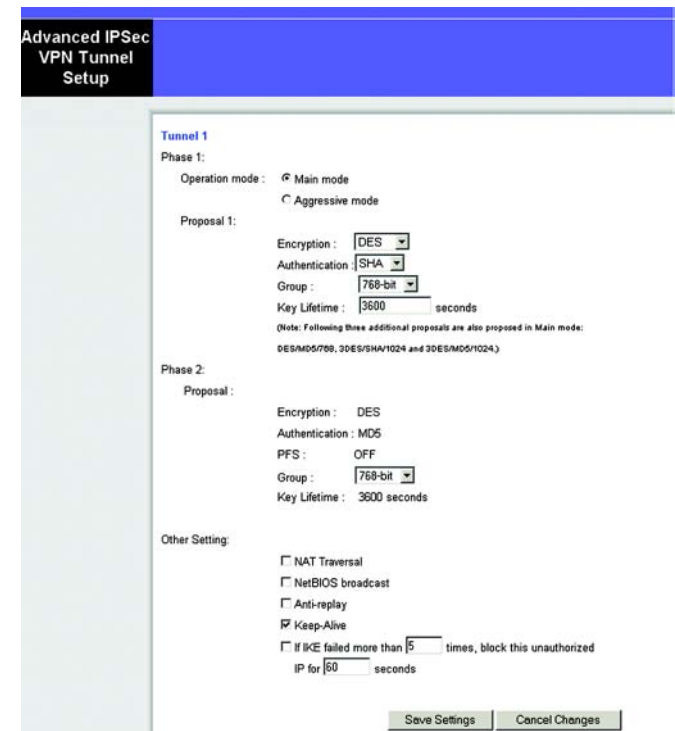


Figure 4-31: Advanced VPN Tunnel Setup

Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Life Time. The number in the Key Lifetime field, shows the amount of seconds the key will be used until a re-key negotiation is completed.

Other Setting

- NAT Traversal.
- NetBIOS broadcast. Check the box next to NetBIOS broadcast to enable NetBIOS traffic to pass through the VPN tunnel.
- Anti-replay. Check the box next to Anti-replay to enable the Anti-replay protection. This feature keeps track of sequence numbers as packets arrive, ensuring security at the IP packet-level.
- Keep-Alive. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection.
- Check this box to block unauthorized IP addresses. Enter in the field to specify how many times IKE must fail before blocking that unauthorized IP address. Enter the length of time that you specify (in seconds) in the field.

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. For further help on this tab, click the **Help** button.

The Access Restrictions Tab

Parental Control

(This service is available in the United States and Canada ONLY.)

The *Parental Control* screen allows you to sign up and manage your Linksys Parental Controls account. The Linksys Parental Control Service* gives you powerful tools to control the availability of Internet services, access, and features, customizable for each member of your family. For more information, refer to *Chapter 5: Using the Linksys Parental Control Service*.

The Linksys Parental Control Service supersedes the Router's Internet Access Policies. In other words, if you are using the Linksys Parental Control Service, then the Internet Access Policies on the Access Restrictions Tab - Internet Access screen will be disabled.

To sign up or manage your Linksys Parental Controls account, you will need an active Internet connection.

Enable/Disable. If you want to use the Linksys Parental Control feature, click the **Enable** radio button. If you want to disable the Linksys Parental Control feature, click the **Disable** radio button.

Sign Up for Parental Control Service. To sign up for a free trial of the Linksys Parental Control Service, click this link. You will be automatically taken to a website where you can create your account. For more information, refer to *Chapter 5: Using the Linksys Parental Control Service*.

More info. If you would like more information about the Linksys Parental Control Service, click the **More info** button.

Status. Displayed here is the status of your Linksys Parental Controls account.

Manage Account. If you have already set up your Parental Controls account, click the **Manage Account** button to access it and make changes.

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

* Available in US and Canada only.

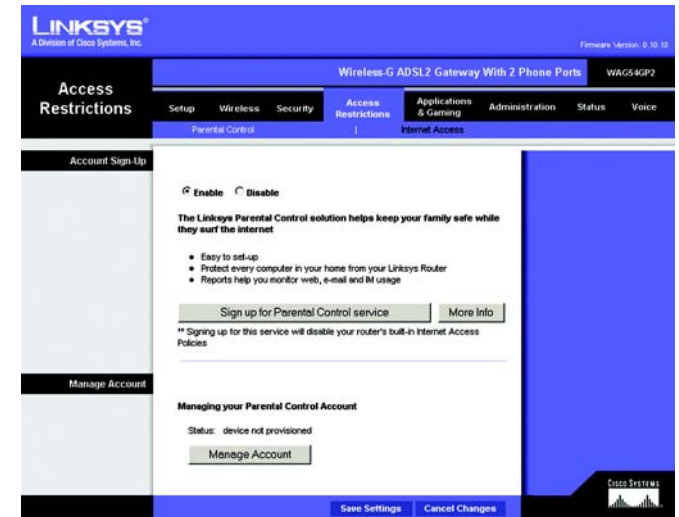


Figure 4-32: Access Restrictions Tab - Parental Control

Internet Access

The *Internet Access* 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.

Internet Access Policy. Multiple Filters can be saved as Internet Access Policies. When you wish to edit one, select the number of the Policy from the drop-down menu. The tab will change to reflect the settings of this Policy. If you wish to delete this Policy, click the **Delete** button. To see a summary of all Policies, click the **Summary** button.

The summaries are listed on this screen with their name and settings. To return to the *Internet Access* tab, click the **Close** button.

Enter Policy Name. Policies are created from the fields presented here.

To create an Internet Access policy:

1. Enable the policy by selecting **Enable** next to *Status*.
2. Enter a Policy Name in the field provided. Select **Internet Access** as the Policy Type.
3. Click the **Edit List of PCs** button. This will open the List of PCs screen. From this screen, you can enter the IP address or MAC address of any computer to which this policy will apply. You can even enter ranges of computers by IP address. Click the **Save Settings** button to save your settings, the **Cancel Changes** button to undo any changes and return to the *Internet Access* tab.

The screenshot shows the 'Internet Access' configuration page. At the top, there's a navigation bar with 'Access Restrictions' selected. Below it, the 'Internet Access' sub-tab is active. The main content area includes:

- Internet Access Policy:** A dropdown menu showing '1 ()', with 'Delete' and 'Summary' buttons.
- Status:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Enter Policy Name:** A text input field.
- PCs:** An 'Edit List of PCs' button.
- Internet access during selected days and hours:**
 - Days:** Radio buttons for 'Deny' and 'Allow' (selected). Below are checkboxes for 'Everyday', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'.
 - Times:** Radio buttons for '24 Hours' (selected) and 'From: To:'. The 'From' and 'To' fields are set to '0:00'.
- Website Blocking by URL Address:** Two empty text input fields.
- Website Blocking by Keyword:** Two empty text input fields.
- Blocked Services:** Two dropdown menus set to 'None', with an 'Add/Edit Service' button below.

 At the bottom right, there are 'Save Settings' and 'Cancel Changes' buttons.

Figure 4-33: Access Restrictions Tab - Internet Access

Internet Policy Summary				
No.	Policy Name	Days	Time of Day	Delete
1.	--	S M T W T F S	--	☐
2.	--	S M T W T F S	--	☐
3.	--	S M T W T F S	--	☐
4.	--	S M T W T F S	--	☐
5.	--	S M T W T F S	--	☐
6.	--	S M T W T F S	--	☐
7.	--	S M T W T F S	--	☐
8.	--	S M T W T F S	--	☐
9.	--	S M T W T F S	--	☐
10.	--	S M T W T F S	--	☐

Close

Figure 4-34: Internet Policy Summary

4. If you wish to Deny or Allow Internet access for those computers you listed on the List of PCs screen, click the option.

5. You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting a service from the drop-down menus next to Blocked Services. If a service isn't listed, you can click the **Add/Edit Service** button to open the Port Services screen and add a service to the list. You will need to enter a Service name, as well as the Protocol and Port Range used by the service.

6. By selecting the appropriate setting next to Days and Time, choose when Internet access will be filtered.

7. Click the **Save Settings** button to activate the policy.

Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the Website Blocking by URL Address fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the Website Blocking by Keyword fields.

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 4-35: List of PCs

Figure 4-36: Port Services

The Applications and Gaming Tab

Single Port Forwarding

PVC Connection Select

PVC stands for "Permanent Virtual Circuit". It is a virtual circuit link between two nodes for ATM (Asynchronous Transfer Mode) network. Each PVC functions as a separate Internet connection. You may set up to eight PVCs on the Gateway.

PortMap List

The Single Port Forwarding screen provides options for customization of port services for common applications.

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.

Choose or enter the Application in the field. Then, enter the External and Internal Port numbers in the fields. Select the type of protocol you wish to use for each application: **TCP** or **UDP**. Enter the IP Address in the field. Click **Enabled** to enable Forwarding for the chosen application.

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.

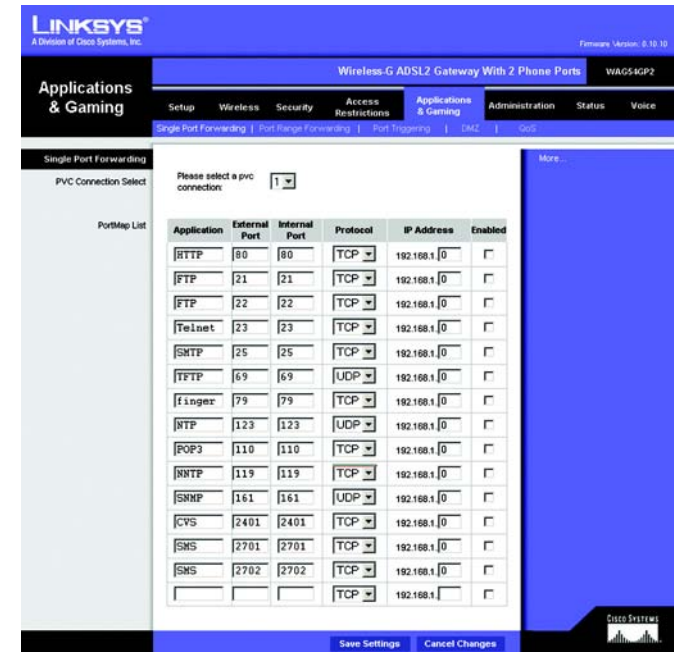


Figure 4-37: Applications and Gaming Tab - Single Port Forwarding

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.
- Port Range (Start and End). Enter the starting and ending numbers of the port 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 for the application.

Click **Enable** to enable that application.

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.

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 you wish to forward.

Click **Enable** to enable that application.

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.

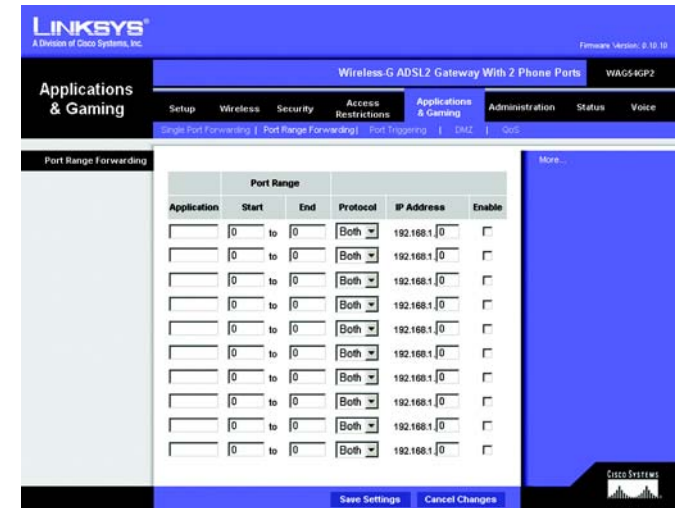


Figure 4-38: Applications and Gaming Tab - Port Range Forwarding

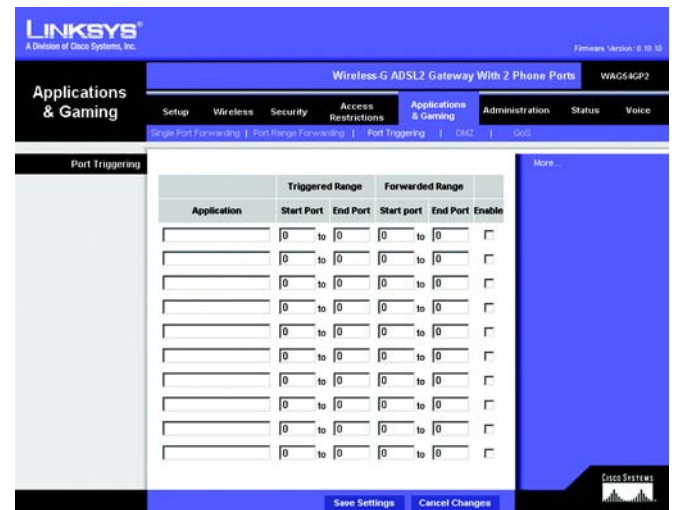


Figure 4-39: Applications and Gaming Tab - Port Triggering

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 **Enabled**. To disable DMZ, select **Disabled**.

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 D: 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 4-40: Applications and Gaming Tab - DMZ

QoS

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

Enabled/Disabled. To utilize QoS on the Gateway, select **Enabled**. Otherwise, keep the default, **Disabled**.

PVC QoS Priority

PVC-based QoS assigns different levels of priority, or precedence, to different PVC (Permanent Virtual Circuit). This is useful when you have, for example, one PVC set up for traditional Internet Services (Web Browsing, E-mail) and another PVC set up to carry time delay sensitive data, such as VoIP or IPTV stream. And give the second PVC a higher level priority helps to ensure the best possibility voice or picture quality. Select from **None**, **Low**, **Medium**, and **High**.

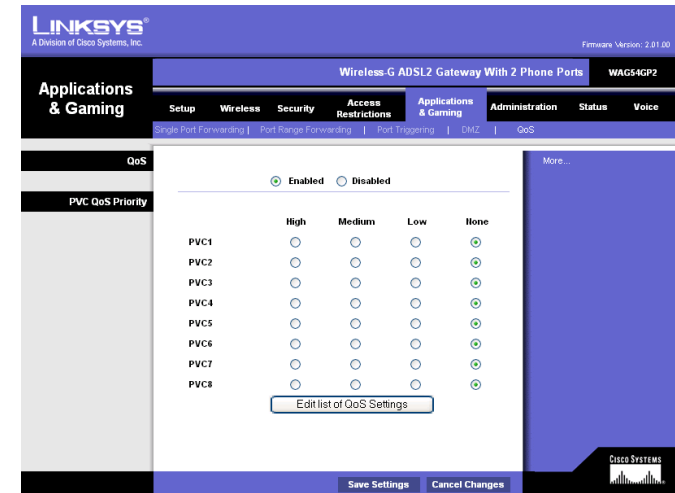


Figure 4-41: Applications and Gaming Tab - QoS

Edit list of QoS Settings

In addition to PVC-based QoS, you can assign different levels of priority to different packets based on information in the packets. To do this, click the **Edit list of QoS Settings** button. The QoS Function screen will appear.

This screen will let you set the priority for packets selected by any of the following criteria, alone or in combination:

- Destination (IP address and address mask, FQDN-fully qualified domain name, or MAC address)
- Source (IP address and address mask, or MAC address)
- Transport protocol (TCP, UDP, or All)
- Destination port and/or source port (if protocol is set to TCP or UDP)
- Ethernet Type value (the value in the 13th and 14th octets of an Ethernet frame)
- Triggering of a particular application layer gateway (FTP, TFTP, H.323, IRC, MMS, GRE, PPTP or SIP)
- Presence of a specified IEEE 802.1D user priority marker
- Presence of a specified IEEE 802.1Q virtual LAN (VLAN) ID
- Packet length between specified minimum and maximum numbers of octets.

Fragment packets' size of AF and BE traffic to be equal to the size of EF traffic:

Enable this option and input a packet size to have large Assured Forwarding (medium priority) and Best Effort (low priority) packets fragmented so they will not delay Expedited Forwarding (high priority) packets. The value you enter should be from 68 to 1492.

When you have finished making changes on this screen, click the **Save** button to save the changes, or click the **Cancel** button to undo your changes. Then click **Close**.

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.

Destination	Source	Source Port	Destination Port	Protocol	Use Port	Use Port	Ethernet Type	Min	Max	Min	Max	Priority
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal
192.168.1.1	192.168.1.1			All			All	68	1492	0	7	Normal

Fragment packet size of AF and BE traffic to be equal to the size of EF traffic:

Save Cancel Close

Figure 4-42: Applications and Gaming Tab - QoS Function

The Administration Tab

Management

The Management screen allows you to change the Gateway's access settings as well as configure the SNMP (Simple Network Management Protocol) and UPnP (Universal Plug and Play) features.

Gateway Access

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

Gateway Username. Enter the default **admin**. You should change the default username for increased security.

Gateway Password. You should set your own password for increased security.

Re-enter to confirm. Re-enter the Gateway's new Password to confirm it.

Remote Management. This feature allows you to access the Gateway from a remote location, via the Internet.



IMPORTANT: Enabling remote management allows anyone with access to your password to configure the Gateway from somewhere else on the Internet.

Remote Username. Enter the default **admin**. You should change the default username for increased security.

Remote Password. You should set your own password for increased security.

Re-enter to confirm. Re-enter the Gateway's new Password to confirm it.

Management Port. Enter the port number you will use to remotely access the Gateway.

Allowed IP. Specify the IP address(es) allowed to remotely manage the Gateway. To allow all IP addresses with no restrictions, select **All**. To specify a single IP address, select **IP address** and enter the IP address in the fields provided. To specify a range of IP addresses, select **IP range** and enter the range of IP addresses in the fields provided.

Use HTTPS. Enable this option to enable HTTPS.

Remote Upgrade. This feature allows the Gateway's firmware to be upgraded remotely by a TFTP server. To enable Remote Upgrade, click **Enable**.

Figure 4-43: Administration Tab - Management

SNMP

SNMP is a popular network monitoring and management protocol. To enable SNMP, click **Enabled**. To disable SNMP, click **Disabled**.

If enabled, then specify the IP address(es) allowed to have SNMP access. Select **All** to allow all IP addresses with no restrictions, **IP address** to specify a single IP address, or **IP range** to specify a range of IP addresses.

Device Name. Enter the name of the Gateway.

Get Community. Enter the password that allows read-only access to the Gateway's SNMP information.

Set Community. Enter the password that allows read/write access to the Gateway's SNMP information.

SNMP v3: Rw User. Enter the user name of the user with read/write access.

Authentication Protocol. Select the method used to authenticate the read/write user.

Authentication Password. Enter the actual password that will authenticate the read/write user.

Privacy Password. Enter a second password for added security. This will be associated with the DES privacy protocol.

Trap Management: Trap to. Enter the IP address of the remote host computer that will receive the trap messages.

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**.

Please select a PVC connection to bind. The Gateway uses one Permanent Virtual Circuit (PVC) connection, so select the number **1** from the drop-down menu.

IGMP-Proxy

If your multimedia application or device is not working properly behind the Gateway, then you can enable IGMPProxy to allow multicast traffic through the Gateway.

PVC Available. The Gateway uses one Permanent Virtual Circuit (PVC) connection, so select the number 1 from the drop-down menu.

IGMP Proxy. To use this feature, select Enable. Otherwise, select Disable.

TR-069

TR-069 is a protocol for communication between a Customer Premise Equipment (CPE) and Auto-Configuration Server (ACS) that encompasses secure auto-configuration as well as other CPE management functions within a common framework. The Gateway is the CPE, which uses this protocol.

TR-069. To enable this feature, select **Enable**.

ACS URL. Enter the URL of the ACS. Your ISP will provide you with the ACS URL.

ACS Username. Enter the username to connect to the ACS. Your ISP will provide you with your ACS Username.

ACS Password. Enter the password to connect to the ACS. Your ISP will provide you with your ACS Password.

WLAN

Management via WLAN. Enabling this feature allows the Gateway to be managed by a wireless computer on the local network when it logs into the Gateway's Web-based Utility.

TELNET

Enabling this feature allows the user to use Telnet and CLI (Command Line Interface) to control the functionality of the Gateway.

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.

Reporting

The Reporting tab provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection. It also provides logs for VPN and firewall events.

Log. To enable log reporting, click **Enabled**.

Logviewer IP Address. Enter the IP Address that will receive logs into the field.

Email Alerts

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

Denial of Service Thresholds. Enter the thresholds of events you want to receive.

SMTP Mail Server. Enter the IP Address of the SMTP server in the field.

E-Mail Address for Alert Logs. Enter the e-mail address for alert logs in the field.

Return E-Mail address. Enter the address for the return e-mail.

To view the logs, click the **View Logs** 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.



Figure 4-44: Administration Tab - Reporting

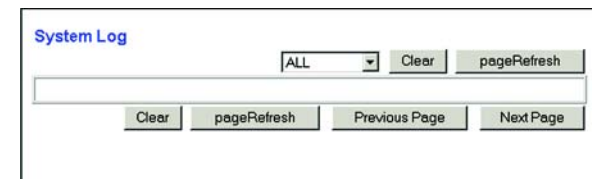


Figure 4-45: System Log

Diagnostics

Ping Test

Ping Test Parameters

Ping Target IP. Enter the IP Address that you want to ping in the field. This can be either a local IP or an Internet IP address.

Ping Size. Enter the size of the ping packets.

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 time in milliseconds.

Ping Result. The results of the ping test will be shown here.

Click the **Start Test** button to start the Ping Test.

Backup&Restore

The Backup&Restore tab allows you to back up and restore the Gateway's configuration file.

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

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

Factory Defaults

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.



Figure 4-46: Administration Tab - Diagnostics

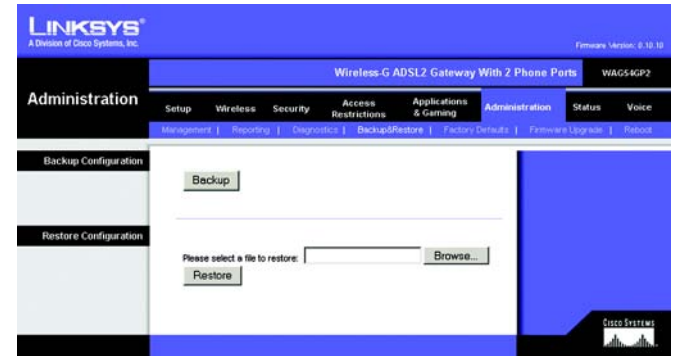


Figure 4-47: Administration Tab - Backup&Restore



Figure 4-48: Administration Tab - Factory Defaults

Firmware Upgrade

The ADSL Gateway allows you to upgrade firmware for the Gateway's network functions.

To upgrade the Gateway's firmware:

1. Click the **Browse** button to find the firmware upgrade file that you downloaded from the Linksys website and then extracted.
2. Double-click the firmware file you downloaded and extracted. Click the **Upgrade** button, and follow the instructions there.



Figure 4-49: Administration Tab - Firmware Upgrade

Reboot

This tab allows you to do a soft or hard reboot of your Gateway.

Reboot Mode. To reboot your Gateway, select **Hard** or **Soft**. Choose hard to power cycle the Gateway or soft to restart it without a power cycle.

To begin the reboot process, click the **Save Settings** button. When a screen appears asking you if you really want to reboot the device. Click **OK**.

Click the **Cancel Changes** button if you want to undo your changes.



Figure 4-50: Administration Tab - Reboot

The Status Tab

Gateway

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

Gateway Information

Gateway Information displays the Software Version, MAC Address, and Current Time.

Internet Connections

The Internet Connections will be displayed after selecting the Internet connection number from the drop-down menu. They are the Login Type, interface, IP Address, Subnet Mask, Default Gateway, and DNS 1, 2, and 3 servers.

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

DHCP Release. Click the **DHCP Release** button to delete your Gateway's current IP address.

Click the **Refresh** button if you want to Refresh your screen.

Local Network

The Local Network information that is displayed is the local Mac Address, IP Address, Subnet Mask, and DHCP Server, Start IP Address, and End IP Address. To view the DHCP Clients Table, click the **DHCP Clients Table** button.

DHCP Clients Table. Click the **DHCP Clients Table** button to show the current DHCP Client data. You will see the MAC address, computer name, and IP address of the network clients using the DHCP server. (This data is stored in temporary memory and changes periodically.) To delete a client from the DHCP server, select the client, then click the **Delete** button.

Click the **Refresh** button if you want to Refresh your screen. Click the **Close** button to close the screen.

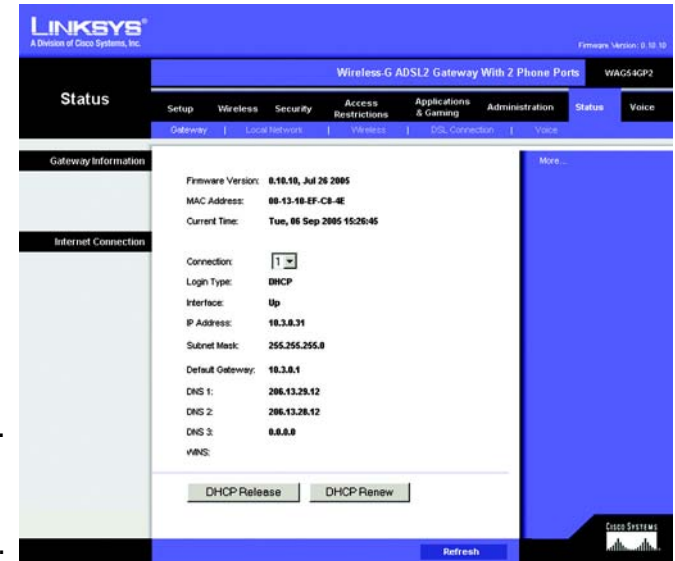


Figure 4-51: Status Tab - Gateway



Figure 4-52: Status Tab - Local Network

Wireless

The Wireless network information that is displayed is the Wireless Firmware Version, MAC Address, Mode, SSID, DHCP Server, Channel, and Encryption Function.

Click the **Wireless Clients Connected** button to view the wireless clients connected to the Gateway.

Click the **Refresh** button if you want to Refresh your screen. Click the **Close** button to close the screen.



Figure 4-53: Status Tab - Wireless

DSL Connection

The DSL Connection information that is displayed is the Status, Downstream Rate, and Upstream Rate.

The PVC Connection information that is displayed is Encapsulation, Multiplexing, QoS, Pcr Rate, Scr Rate, Autodetect, VPI, VCI, and PVC Status.

Click the **Refresh** button if you want to Refresh your screen.

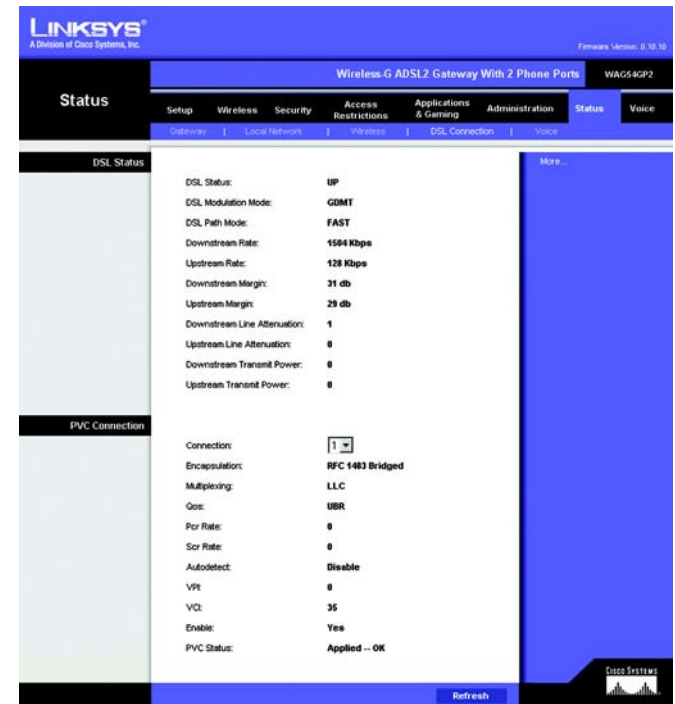


Figure 4-54: Status Tab - DSL Connection

Wireless-G ADSL Gateway with 2 Phone Ports

Voice

The Voice screen displays Information, Line 1 Status, and Line 2 Status status.

Click the **Refresh** button if you want to Refresh your screen.



Figure 4-55: Status Tab - Voice

The Voice Tab

Voice Authentication

The Voice Authentication feature is used by your ISP for configuring the Gateway's voice features. Login to these features is accomplished on this screen.



Figure 4-56: Voice Tab - Voice Authentication

Chapter 5: Using the Linksys Parental Control Service

Overview

This chapter will describe the Linksys Parental Control Service*, as well as explain how to sign up for the Service, manage your account, and use the Internet when the Service is actively controlling Internet traffic and messages.

Introduction

The Linksys Parental Control Service makes it easy for you to keep your family safe on the Internet. The Service gives you powerful tools to control the availability of Internet services, access, and features, customizable for each member of the family.

Choosing from 16 different web content categories, you control what each family member is allowed to see. Each website request triggers a search through our constantly updated database, which determines whether or not to allow the content through, based on who's logged in. You can also manually block or allow specific websites based on your own judgment.

To protect your family from unsolicited messages, you can set up e-mail and Instant Message filters. You select who can send messages to, and receive messages from, your family. If your children are spending too much time online, you can set time restrictions by hour and day of the week.

To keep you informed of your family's online activities, full reports are available to view or download. You can see each family member's blocked and unblocked Internet activities, to keep you "in the loop" on their changing interests. Setting up and customizing each family member's settings is a snap with the friendly web-based menus—even if you're not the family's usual network administrator. Because the Parental Control Service is based in the Router, not your PCs, it can't be bypassed and keeps every Internet device in your household equally protected.

* Available in US and Canada only.

database: *a collection of data that is organized so that its contents can easily be accessed, managed, and updated.*

Signing up for the Linksys Parental Control Service

There are two ways to access the website you will use to sign up for your Linksys Parental Controls account.

Setup Wizard

At the end of the Setup Wizard, you will see the *Safe Surfing* screen. Click the **Linksys Parental Control Service** button to sign up for a free trial service. You will be automatically taken to a website where you can create your account. For additional instructions, go to the “Signing up for the Linksys Parental Control Service” section. After you have signed up, you will be asked if you want to manage your account. If so, then you can go directly to the login screen for Linksys Parental Controls Billing and Support Center. Refer to the “Managing Linksys Parental Controls” section.

Web-based Utility

If you are using the Router’s Web-based Utility, go to the Access Restrictions tab - Parental Control screen. Click the **Enable** radio button and then the **Save Settings** button. Then click the **Sign up for Parental Control Service** button. You will be automatically taken to a website where you can create your account. For additional instructions, go to the “Signing up for the Linksys Parental Control Service” section. If you would like more information about the Linksys Parental Control Service, click the **More info** button. If you have already set up your Parental Controls account, click the **Manage Account** button to access it and make changes. For more information, go to the “Managing Linksys Parental Controls” section.



Note: To sign up for your Linksys Parental Controls account, you will need an active Internet connection.



Figure 5-1: Safe Surfing

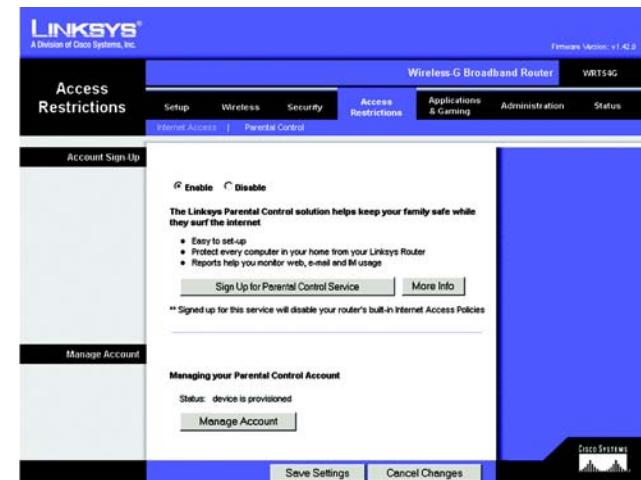


Figure 5-2: Access Restrictions Tab - Parental Control

Signing up for the Linksys Parental Control Service

To sign up for your Linksys Parental Controls account, you will need an active Internet connection. Then follow these instructions:

1. After you click *Linksys Parental Control Service* from the Setup Wizard or the *Sign Up for Parental Control Service* button from the Web-based Utility, the *Linksys Service Agreement* screen will appear. You must scroll down the entire agreement before you can accept the Agreement. Then click the **Accept** button. If you do not want to accept the Agreement, click the **Cancel** button.
2. The *Sign Up* screen will appear. Enter a User Name and Password for your account. Enter the Password again in the *Confirm Password* field. Then enter your e-mail address in the *Email* field (service e-mail notifications will be sent to this e-mail address) and enter it again in the *Confirm Email* field.

You have a choice of two payment plans, **Pay Now** or **Pay Later**. (If the Router you are using is not eligible for the free trial, then you have one choice, Pay Now.)

If you click Pay Now, go to step 3.

If you click Pay Later, go to step 4.

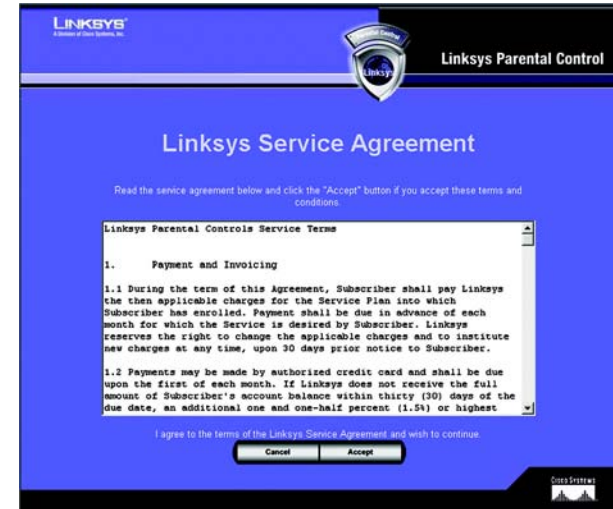


Figure 5-3: Linksys Service Agreement



Figure 5-4: Sign Up

3. To pay now, complete the form on the *Purchase Service* screen. Your account information will automatically appear.

In the *User Information* section, enter your address in the *Address1*, *Address2* (if necessary), *City*, *State/Prov*, and *Zip Code* fields. Select your country from the *Country* drop-down menu. (Your phone number is optional.)

In the *Billing Information* section, select your credit card from the *Credit Card* drop-down menu. Complete the *Credit Card Number* field. From the *Expiration Date* drop-down menus, select the month and year your credit card expires. In the *Full Name on Card* field, enter the complete name that appears on the credit card you are using.

Then click the **Finish** button. To cancel your sign-up, click the **Cancel** button.

The screenshot shows the 'Purchase Service' page for Linksys Parental Control. The page has a blue header with the Linksys logo and 'Linksys Parental Control' text. Below the header, there's a section titled 'Purchase Service' with a sub-heading and a paragraph of text. Underneath, there's a 'Select your subscription option' section with three radio button choices: \$24.95 for 6 months, \$39.95 for 1 year, and \$59.95 for 2 years. The page is divided into three main sections: 'Account Information' (with fields for User Name, Password, Confirm Password, and Email), 'User Information' (with fields for Address, City, State/Prov, Zip Code, and Country), and 'Billing Information' (with fields for Credit Card, Credit Card Number, Expiration Date, and Full Name on Card). At the bottom right, there are 'Cancel' and 'Finish' buttons.

Figure 5-5: Purchase Service

4. The Router will now connect to the Parental Control Service.



Figure 5-6: Connecting to the Parental Control Service

5. When the sign-up process is complete, you will receive an e-mail message, and you will see the *Congratulations* screen.

If you want to create user profiles for your family members now, click the **Create Profiles** button. For additional instructions, proceed to step 4 of the “Managing Linksys Parental Controls” section.

If you want to access the Internet immediately, click the **Sign in and Surf** button. For more information, go to the “Using the Linksys Parental Control Service” section.



Figure 5-7: Congratulations

Managing Linksys Parental Controls

To manage your Linksys Parental Controls account, you will need an active Internet connection. Then follow these instructions:

1. Open the Router's Web-based Utility.
2. Click the **Access Restrictions** tab.
3. Click the **Manage Account** button on the *Parental Controls* screen. (This screen also lists the status of your Parental Controls account.)
4. The login screen will appear. For future reference, create a bookmark through your web browser. Complete the *Name* (E-mail address) and *Password* fields.
5. Then click the **Go** button. The *Support Center* screen will appear.

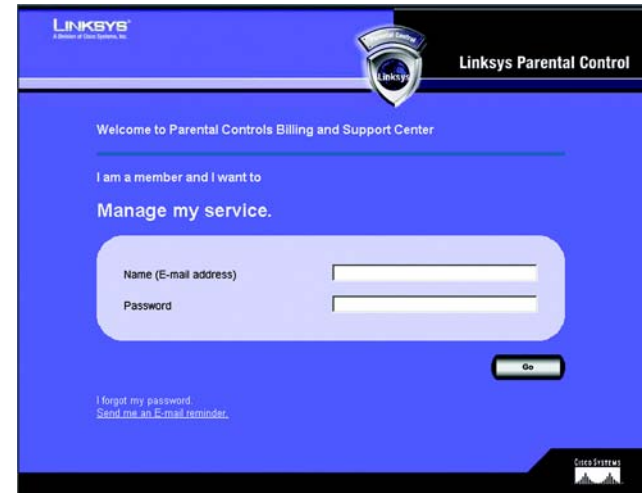


Figure 5-8: Parental Controls Login



Note: If you have forgotten your password, click **Send me an E-mail reminder** and follow the on-screen instructions.

Support Center

On the left of the *Support Center* screen, you can access the Activity Reports, Family Settings, and Suggest a Rating webpages. These and the Support Center webpage are accessible from every screen. (Click **Billing and Support** to return to the Support Center webpage.)

On the *Support Center* screen, you also have access to the following:

Subscribe to Service

Click **Subscribe to Service** to sign up for your Parental Controls subscription before your free trial period expires. The *Purchase Linksys Parental Control Service* screen will appear. Follow these instructions:

1. Select a subscription option.
2. Complete the *Billing Contact Info* and *Billing Information* sections. (Fields marked with an asterisk must be filled out.)
3. Click the **Update** button to save your changes, or click the **Cancel** button to cancel changes.

Ask for Help

If you need more information about the Parental Control Service, click this link.

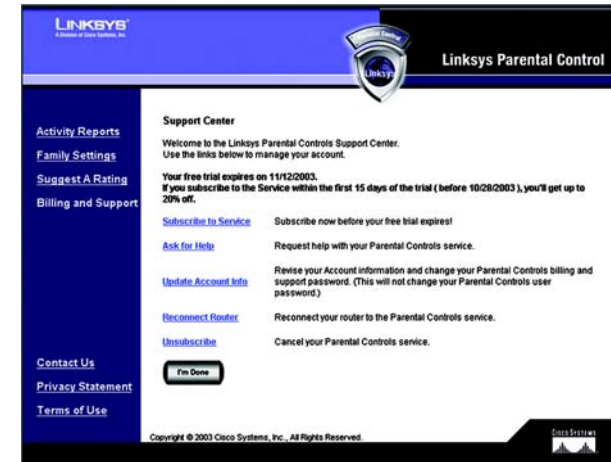


Figure 5-9: Support Center



Figure 5-10: Subscribe to Service

Update Account Info

Click this link to update your contact information or change your Parental Controls billing and support password (this is separate from your Parental Controls user password). The *Update Contact Information* screen will appear. Follow these instructions:

1. Complete the *First Name* and *Last Name* fields. (Fields marked with an asterisk must be filled out.)
2. Enter your new billing and support password in the *Parental Control Password* field. Re-enter the new password in the *Confirm Password* field.
3. Complete the *Email* field (the e-mail address you enter will receive service administration notices only).
4. Click the **Save** button to save your changes, or click the **Cancel** button to cancel changes.

Reconnect Router

If the Router has lost its connection to the Parental Control Service or if you have reset the Router back to its factory default settings after you have signed up for Parental Control Service, click **Reconnect Router** to regain the connection.

Unsubscribe

If you want to cancel your Parental Control Service account, click this link. Click the **Proceed** button on the following screen to cancel your Parental Control Service.

Figure 5-11: Update Contact Information

Figure 5-12: Cancel Your Parental Control Account

Activity Reports

On the *Activity Reports* screen, you will be able to view a report of Internet activities for your entire family or a specific family member. Click **Family** to view family reports, or click an individual's name to view his or her reports. After you have selected Family or a specific name, you will see a choice of reports to view.

Reports

For the family or a specific family member, these are the reports you can view:

- Summary (not available if you selected Family)
- Web Report
- Instant-Messaging Report
- E-mail Report

Summary

Click this link to view a summary of Internet activities, including Top Allowed or Blocked E-mail Addresses, Top Allowed or Blocked Instant-Message Addresses, and Alerts. (This report is not available for the entire family.)

Web Report

Click this link to view all web-browsing activities. Each entry lists details under five column headings: Date, Family Member, Reason, Web Site, and Web Category. You can click a column heading to sort entries. To view the activities during a specific time period, use the *Day Range* drop-down menu. Click the **Refresh** button to update the report. To delete specific entries, click the checkbox next to specific entries, and then click the **Delete** button. To save all reports to your computer, click the **Download** button. The reports will be saved as a tab-delimited text file called PcReport. To scroll through the entries, click **First**, **Previous**, or **Next**.

Instant-Messaging Report

Click **Instant-Messaging Report** to see all activities with Instant Messages. Each entry lists details under five column headings: Date, Family Member, Reason, Local Screen Name, and Remote Screen Name. You can click a column heading to sort entries. To view the activities during a specific time period, use the *Day Range* drop-down menu. Click the **Refresh** button to update the report. To delete specific entries, click the checkbox next to specific entries, and then click the **Delete** button. To save all reports to your computer, click the **Download** button. The reports will be saved as a tab-delimited text file called PcReport. To scroll through the entries, click **First**, **Previous**, or **Next**.



Figure 5-13: Activity Reports

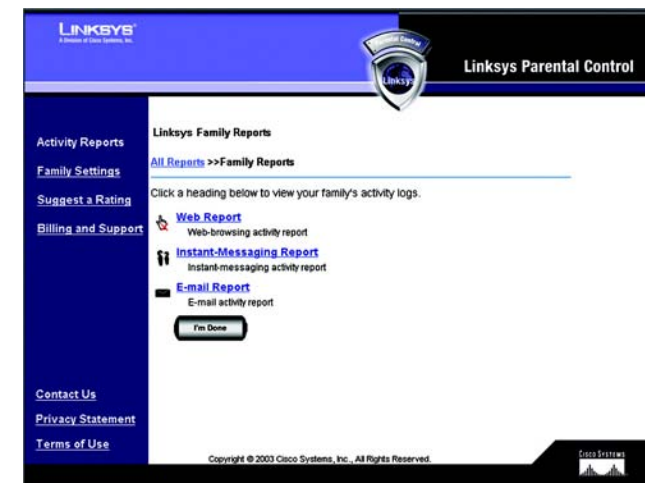


Figure 5-14: Types of Reports

E-mail Report

Click this link to view all e-mail activities. Each entry lists details under five column headings: Date, Family Member, Reason, Sender's E-mail Address, and Receiver's E-mail Address. You can click a column heading to sort entries. To view the activities during a specific time period, use the *Day Range* drop-down menu. Click the **Refresh** button to update the report. To delete specific entries, click the checkbox next to specific entries, and then click the **Delete** button. To save all reports to your computer, click the **Download** button. The reports will be saved as a tab-delimited text file called PcReport. To scroll through the entries, click **First**, **Previous**, or **Next**.

LINKSYS
Power to Your Network

Linksys Parental Control

Linksys Family Web Report

All Reports >> Family Reports >> Family Web Report

Click a column heading to sort its entries. Limit the report to a certain time period using the Day Range list. Click Delete Selected to delete the selected records (indicated by check marks). Click Delete All to delete all Web reports. Click Download to save all reports to your computer as a tab-delimited text file called PcReport.bt.

Day Range: --All Days--

<input type="checkbox"/>	Date	Family Member	Reason	Web Site	Web Category
<input type="checkbox"/>	10-10-03 02:48 PM	child	Blk Type	WWW.VICTORIASSECRET.COM	Lingerie, Swimsuits
<input type="checkbox"/>	10-10-03 02:48 PM	child	OK Type	WWW.MSN.COM	Unknown
<input type="checkbox"/>	10-10-03 02:48 PM	child	OK Type	HOME.MICROSOFT.COM	Unknown
<input type="checkbox"/>	10-10-03 02:23 PM	child	OK Type	WWW.GOOGLE.COM	General Interest
<input type="checkbox"/>	10-10-03 02:22 PM	child	OK Type	WWW.MSN.COM	Unknown
<input type="checkbox"/>	10-10-03 02:22 PM	child	OK Type	HOME.MICROSOFT.COM	Unknown
<input type="checkbox"/>	10-10-03 02:22 PM	child	Blk Type	WWW.GOOGLE.COM	Adult Content
<input type="checkbox"/>	10-10-03 02:22 PM	child	OK Type	WWW.GOOGLE.COM	General Interest
<input type="checkbox"/>	10-10-03 02:22 PM	child	OK Type	VIEWATDNT.COM	Unknown
<input type="checkbox"/>	10-10-03 02:22 PM	child	OK Type	WWW.MSN.COM	Unknown

Page: 1 (1 - 10 records)

Records per page: 10

Contact Us
Privacy Statement
Terms of Use

Copyright © 2003 Cisco Systems, Inc. All Rights Reserved. Cisco Systems

Figure 5-15: Web Report

Family Settings

On the *Family Settings* screen, you will be able to change the settings for a family member or add a new family member. Click a family member's name to change his or her Internet privileges. You will see the *All Settings* screen, which lists several categories of settings. Refer to the "All Settings" section for more information.

New Family Member

To add a new family member, click the **New Family Member** button. On the *Name & Password* screen, follow these instructions:

1. Enter the nickname and password that the new family member will use to access the Internet. Re-enter the Password in the *Re-enter Password* field. Click the **Cancel** button to cancel your changes. Click the **Next** button to continue.
2. Click the radio button next to the appropriate age category for the new family member. There are five categories: Child (under 12), Youth (12-15), Mature Teen (16-17), Adult, and Family Manager. Read the online category descriptions to learn what types of restrictions are enabled for each category, or refer to the "Maturity Level" section.
3. Click the **Back** button to return to the previous screen. Click the **Cancel** button to cancel your change. Click the **Finish** button to save this new family member profile (the default restrictions of the age category you select will be active).

If you want to customize the restrictions for the new family member, click the **Customize** button. You will see the *All Settings* screen, which lists several categories of settings, such as Time, Web Browsing, E-mail, and Instant-Messaging Restrictions. Follow the on-screen instructions; for more information, refer to the "Time Restrictions," "Web Browsing Restrictions," "E-mail Restrictions," and "Instant-Messaging Restrictions" sections. Click the **I'm Done** button when you are finished with your changes.

I'm Done. When you have finished making changes to your Parental Controls account, click the **I'm Done** button to exit the Parental Controls Billing & Support Center website.



Figure 5-16: Family Settings

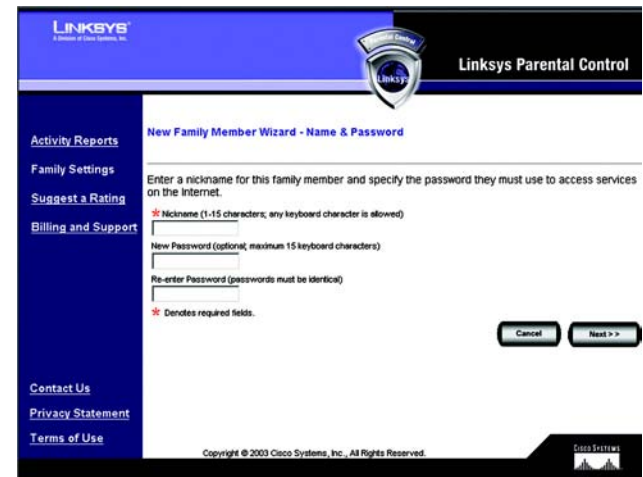


Figure 5-17: New Family Member

All Settings

For each family member you will be able to customize the following privileges:

- Online Reporting
- Maturity Level
- Time Restrictions
- Web Browsing Restrictions
- E-mail Restrictions
- Instant-Messaging Restrictions
- Password
- Delete

I'm Done. When you have finished making changes to your Parental Controls account, click the **I'm Done** button to exit the Parental Controls Billing & Support Center website.

Online Reporting

On the *Online Reporting* screen you can select the kinds of activities you want to monitor. There are three categories: Web Browsing Restrictions, E-mail, and Instant Messaging. For each category, you have three levels of monitoring available. Click the radio button next to your choice in each category.

Web Browsing Restrictions. Select one of the following: **No reporting of Web sites visited**, **Report only blocked Web sites**, or **Report all Web sites visited**.

E-mail. Select one of the following: **No e-mail Reporting**, **Report only Blocked e-mail activity**, or **Report All e-mail activity**.

Instant Messaging. Select one of the following: **No Instant-Messaging/Chat reporting**, **Report only Blocked Instant-Messaging/Chat activity**, or **Report all Instant-Messaging/Chat activity**.

Click the **Save** button to save your changes, or click the **Cancel** button to cancel your changes.



Figure 5-18: All Settings



Figure 5-19: Online Reporting

Maturity Level

On the *Maturity Level* screen, click the radio button next to the appropriate age category for the designated family member. There are five categories:

Child (under 12). Web browsing is limited to general interest and unlisted sites. E-mail and instant-messaging services are prohibited. Internet access is allowed from 3 PM to 8 PM on weekdays and from 8 AM to 9 PM on weekends.

Youth (12-15). Web browsing is limited to “Child” categories plus sex education sites. E-mail services are prohibited. Instant-messaging services are restricted to a list of approved correspondents. Internet access is allowed from 3 PM to 10 PM on weekdays, and from 8 AM to 10 PM on weekends.

Mature Teen (16-17). Web browsing is limited to “Youth” categories plus games, lingerie and swimsuits, nudity, and web communication sites. E-mail and instant-messaging services are prohibited. Internet access is allowed from 3 PM to 11 PM on weekdays and from 8 AM to 11 PM on weekends.

Adult. All services are unrestricted. This category is recommended for adults only.

Family Manager. All services are unrestricted. Access to the Parental Controls settings is permitted. This category is recommended for adults only.

Click the **Save** button to save your changes, or click the **Cancel** button to cancel your changes. After you select and save the Maturity Level setting, then you can customize the other settings, such as Time, Web Browsing, E-mail, and Instant-Messaging Restrictions.



Figure 5-20: Maturity Level

Time Restrictions

On the *Time Restrictions* screen, click any hour to allow or deny Internet access (green indicates allowed Internet access, and red indicates blocked Internet access). To allow Internet access for an entire day, click the day of the week in the *Allow All Day* row. To block Internet access for an entire day, click the day of the week in the *Block All Day* row. If you want to reset the Time Restrictions to the default settings for a specific age category, click the appropriate age category in the *Reset to* row. If you want to always block Internet access, click **Always Block**. If you want to always allow Internet access, click **Always Allow**.

To cancel your changes, click **Undo Changes**. Click the **Cancel** button to cancel your changes and return to the previous screen. Click the **Save** button to save your changes.

LINKSYS
A Division of Cisco Systems, Inc.

Linksys Parental Control

Change Family Member Privileges: child

All Family Members >> All Settings >> Time Restrictions

Click any hour of the week to control whether this family member may access the internet during that hour. Or click an Allow All Day or Block All Day shortcut to allow or block internet access for a full day at a time.

	12AM - 2AM	3AM - 5AM	6AM - 8AM	9AM - 11AM	12PM - 2PM	3PM - 5PM	6PM - 8PM	9PM - 11PM
Sunday	Green	Green	Green	Green	Green	Green	Green	Green
Monday	Green	Green	Green	Green	Green	Red	Red	Green
Tuesday	Green	Green	Green	Green	Green	Red	Red	Green
Wednesday	Green	Green	Green	Green	Green	Red	Red	Green
Thursday	Green	Green	Green	Green	Green	Red	Red	Green
Friday	Green	Green	Green	Green	Green	Red	Red	Green
Saturday	Green	Green	Green	Green	Green	Green	Green	Green

Legend: ■ = Web Access Allowed ■ = Web Access Blocked

Allow All Day: [Sunday](#) [Monday](#) [Tuesday](#) [Wednesday](#) [Thursday](#) [Friday](#) [Saturday](#)

Block All Day: [Sunday](#) [Monday](#) [Tuesday](#) [Wednesday](#) [Thursday](#) [Friday](#) [Saturday](#)

Reset to: [Child](#) [Youth](#) [Mature Teen](#) [Adult](#)

[Always Block](#) [Always Allow](#) [Undo Changes](#)

Contact Us
Privacy Statement
Terms of Use

Copyright © 2003 Cisco Systems, Inc. All Rights Reserved.

Figure 5-21: Time Restrictions

Web Browsing Restrictions

On the *Web Browsing Restrictions* screen, click **Web Site Categories** if you want to block and allow Web sites by category. Click **Blocked & Allowed Web sites** if you want to block and allow specific Web sites.

Web Site Categories. On the *Web Site Categories* screen there are 16 categories listed:

- Adult Content
- Alcohol, Drugs, Tobacco
- Anonymizers
- Criminal/Illegal Skills
- Gambling
- Games
- General Interest
- Hate/Discrimination
- Lingerie, Swimsuits
- Nudity
- Personals & Dating
- Sex Education
- Unknown
- Violence
- Weapons
- Web Communications

Click a category title for an online description of the category. Click the checkbox of a category to allow or block access. A checkmark indicates an allowed category, while a stop sign indicates a blocked category. If you want to reset the category blocking to the default settings for a specific age category, click the appropriate age category in the *Reset to* row. If you want to block all categories, click **Block All**. If you want to allow all categories, click **Allow All**.

To cancel your changes, click **Undo Changes**. Click the **Cancel** button to cancel your changes and return to the previous screen. Click the **Save** button to save your changes.

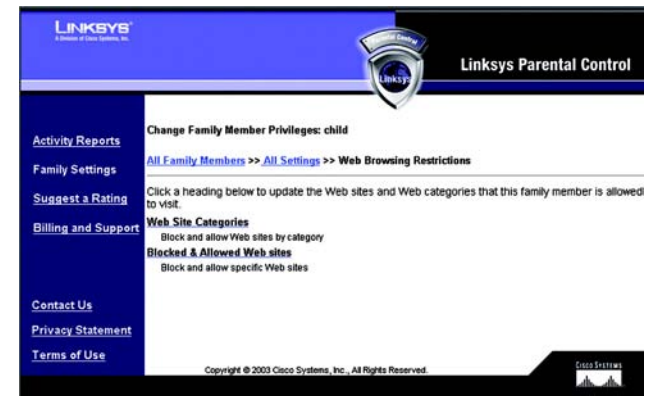


Figure 5-22: Web Browsing Restrictions



Figure 5-23: Web Site Categories

Blocked & Allowed Web Sites. From this screen, you can control access to specific Web sites. To add an allowed Web site, enter the name of the Web site in the *Allow this Web site* field. Then click the **Add** button. To remove an allowed Web site, select the name of the Web site in the *Allow Web Sites* field, and then click the **Remove** button.

To add a blocked Web site, enter the name of the Web site in the *Block this Web site* field. Then click the **Add** button. To remove a blocked Web site, select the name of the Web site in the *Blocked Web Sites* field, and then click the **Remove** button.

Click the **Cancel** button to cancel your changes. Click the **Save** button to save your changes.



Figure 5-24: Blocked & Allowed Web Sites

E-mail Restrictions

There are three levels of e-mail privileges available:

- May use e-mail freely
- May correspond with approved contacts only
- May not use e-mail

Click the radio button next to the level appropriate for the designated family member. If you restrict e-mails to a list of approved contacts, then click the word **here** of *click here to set up*, next to *May correspond with approved contacts only*. The *E-mail Settings* screen will appear. Then follow these instructions:

4. Enter the family member's e-mail address.
5. Complete the *Incoming Mail Server* and *Account Name* fields. If you are not sure, click the words **Click here** of *click here to use suggested names*. Suggestions will automatically appear in the *Incoming Mail Server* and *Account Name* fields.
6. Enter the approved contact's e-mail address. Click the **Add Address** button to add the approved contact.

To remove an approved contact, click the contact's e-mail address in the *E-mail Correspondents* field, and then click the **Remove** button.

Click the **Cancel** button to cancel your changes. Click the **Save** button to save your changes.

On the *E-mail Restrictions* screen, click the **Cancel** button to cancel your changes. Click the **Save** button to save your changes.

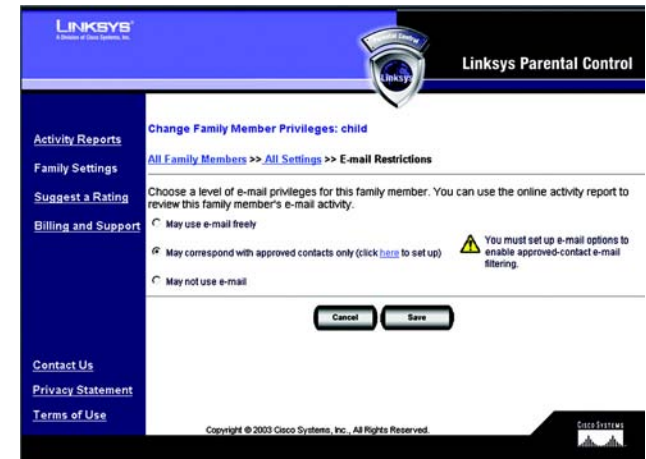


Figure 5-25: E-mail Restrictions



Figure 5-26: E-mail Settings

Instant-Messaging Restrictions

There are three levels of instant-messaging privileges available. Click the radio button next to the level appropriate for the designated family member. If you restrict instant messaging to a list of approved contacts, then follow these instructions for each approved contact:

1. Select an Instant Messaging Service: **AOL**, **Yahoo!**, **MSN**, or **ICQ**.
2. Complete the *Enter Screen Name* field.
3. Click the **Add** button to add the approved contact.

To remove an approved contact, click the contact's name in the *Instant-Messaging Correspondents* field, and then click the **Remove** button.

Click the **Cancel** button to cancel your changes. Click the **Save** button to save your changes.

Password

To access the Internet, the designated family member must use his or her password. You can change this password using the *Password* screen. Enter the new password in the *New Password* and *Re-enter Password* fields. Click the **Cancel** button to cancel your changes. Click the **Save** button to save your changes.

Delete

To delete a family member, click **Delete**.

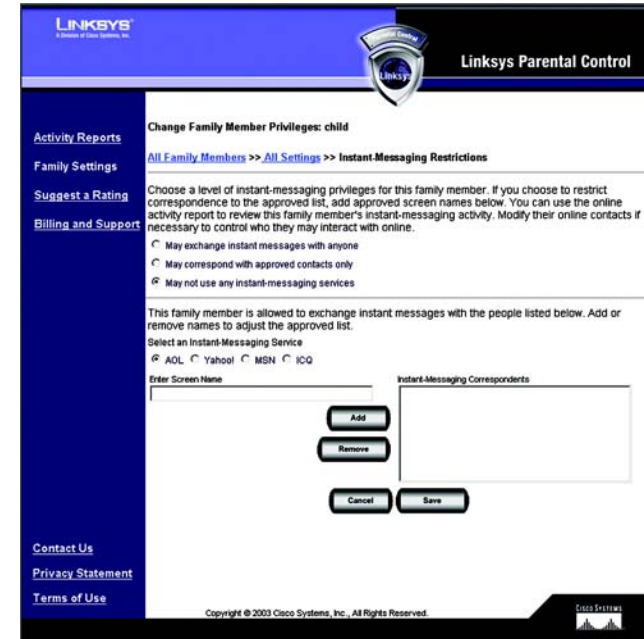


Figure 5-27: Instant-Messaging Restrictions



Figure 5-28: Password

Suggest a Rating

To find out the categorization or rating of a specific Web site, enter its address and click the **Find** button. If you would like to suggest a different rating for a site or a new rating for an unrated site, enter your comments in the comments field and click the **Submit** button. Click the **Cancel** button to cancel your changes.



Figure 5-29: Suggest a Rating

Using the Parental Control Service

When the Linksys Parental Control Service is actively managing your family's Internet activities, you must sign in with the Linksys Parental Control Service before you can access the Internet. Follow these instructions:

1. Open your web browser.
2. If you are using Internet Explorer 5.5 or higher, you will see a warning screen. It will ask you if you want to install an ActiveX plug-in, which will install an icon in the system tray of your desktop taskbar. Click the **Yes** button.

If you are not using Internet Explorer 5.5 or higher, proceed to step 3.

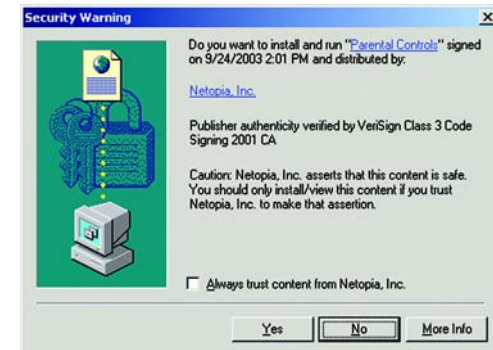


Figure 5-30: Security Warning

Wireless-G ADSL Gateway with 2 Phone Ports

3. In your web browser, a *Welcome to Parental Controls* screen will appear. Log into the Linksys Parental Control Service. Select your name from the *SIGN IN* drop-down menu, and enter your password. Select when you want to be automatically logged out. If you want a pop-screen for logout to appear, click the checkbox next to *Show Sign in status pop-up*. Then click the **Sign In** button.

If you are using Internet Explorer 5.5 or higher and installed the ActiveX plug-in, an icon will appear in the system tray, while a separate *Status* screen will appear in the upper right corner of your desktop.

4. Depending on your profile, the Linksys Parental Control Service will permit or deny Internet access, as well as regulate e-mail or Instant Messaging activities.

If you enabled the pop-up screen, then it will appear. You can click the **Status Page** button to return to the *Welcome to Parental Controls* screen and see what your login is.

When you have finished your Internet activities, make sure you sign out to securely end your session. If you have a tray icon, right-click it and click **Sign Out**. If you have a pop-up screen, click the **Sign Out** button.

For more information about the tray icon's additional features, proceed to the "Using the Tray Icon" section.



Figure 5-31: Welcome to Parental Controls

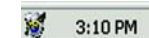


Figure 5-32: Tray Icon



Figure 5-33: Pop-up Screen (Login)

Using the Tray Icon

When you right-click the tray icon, you have other menu choices:

- **Sign In.** Click **Sign In** if you want to log into the Parental Control Service.
- **Switch User.** If you want to log in as a different user, click **Switch User**. The *Welcome to Parental Controls* screen will appear. Click the **Switch Family Members** button.
- **Administration.** If you want to manage your Parental Controls account, click **Administration**. The login screen for the Parental Control Billing & Support Center will appear.
- **Preferences.** To change your preferences for the Status screen, click **Preferences**. You will have these three choices:
 - Enabled.** Enables the *Status* screen.
 - Disabled.** Disables the *Status* screen.
 - Force to top.** Enables the *Status* screen and forces it to appear at the top of your current window.
- **About Parental Controls.** Click **About Parental Controls** to find out which version you are using.
- **Exit.** To close the tray icon, click **Exit**.

If you have exited the tray icon and want to use it, click the **Start** button, **Programs**, **Parental Controls**, and **PCT Helper**. The tray icon will re-appear.



Figure 5-34: Pop-up Screen (Sign Out)



Figure 5-35: Right-Click Tray Icon

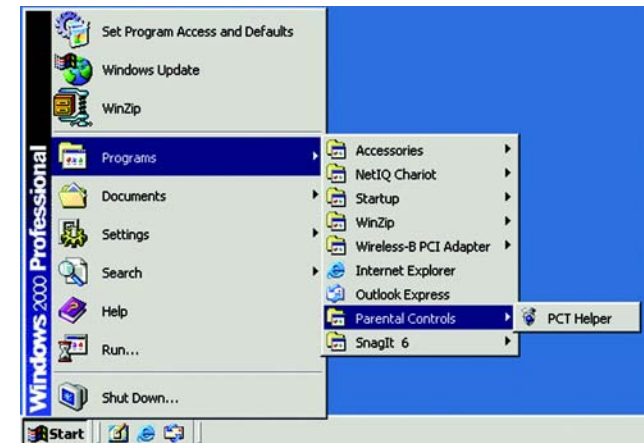


Figure 5-36: Re-activate Tray Icon

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 international website at www.linksys.com/international.

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, 192.168.1.1 (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, 192.168.1.1 (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. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

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

For Windows NT 4.0:

- Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
- Click the Protocol tab, and double-click on TCP/IP Protocol.
- When the window appears, make sure you have selected the correct Adapter for your Ethernet adapter and set it for **Obtain an IP address** from a DHCP server.
- Click the **OK** button in the TCP/IP Protocol Properties window, and click the **Close** button in the Network window.
- Restart the computer if asked.

B. Open a command prompt.

For Windows 98 and Me:

- Click **Start** and **Run**. In the Open field, type in command. Press the **Enter** key or click the **OK** button.

For Windows NT, 2000, and XP:

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

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

- Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
 1. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, IPoA or RFC 2364 PPPoA. Please refer to the Setup section of *Chapter 4: Configuring the Gateway* for details on Internet connection settings.
 2. Make sure you have the right cable. Check to see if the Gateway column has a solidly lit ADSL LED.
 3. Make sure the cable connecting from your Gateway's ADSL port is connected to the wall jack of the ADSL service line. Verify that the Status page of the Gateway's web-based utility shows a valid IP address from your ISP.
 4. Turn off the computer and Gateway. Wait 30 seconds, and then turn on the Gateway, and computer. Check the Status tab of the Gateway's web-based utility to see if you get an IP address.

4. I am not able to access the Setup page of the Gateway's web-based utility.

- Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Gateway.
 1. Refer to *Appendix D: Finding the MAC Address and IP address for Your Ethernet Adapter* to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
 2. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."
 3. Refer to "Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

5. I can't get my Virtual Private Network (VPN) working through the Gateway.

Access the Gateway's web interface by going to <http://192.168.1.1> or the IP address of the Gateway, and go to the Security tab. Make sure you have IPsec passthrough and/or PPTP pass-through enabled.

- VPNs that use IPsec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPsec session will work through the Gateway; however, simultaneous IPsec sessions may be possible, depending on the specifics of your VPNs.
- VPNs that use IPsec and AH (Authentication Header known as protocol 51) are incompatible with the Gateway. AH has limitations due to occasional incompatibility with the NAT standard.
- Change the IP address for the Gateway to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Gateway will have difficulties routing information to the right location. If you change the Gateway's IP address to 192.168.2.1, that should solve the problem. Change the Gateway's IP address through the Setup tab of the web interface.
- If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.
- Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPsec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.
- Check the Linksys international website for more information at www.linksys.com/international.

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

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

- Follow these steps to set up port forwarding through the Gateway's web-based utility. We will be setting up web, ftp, and mail servers.
 1. Access the Gateway's web-based utility by going to <http://192.168.1.1> or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
 2. Enter any name you want to use for the Customized Application.
 3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
 4. Check the protocol you will be using, TCP and/or UDP.
 5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check *Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter* for details on getting an IP address.

6. Check the Enable option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
Web server	80 to 80	X		192.168.1.100	X
FTP server	21 to 21	X		192.168.1.101	X
SMTP (outgoing)	25 to 25	X		192.168.1.102	X
POP3 (incoming)	110 to 110	X		192.168.1.102	X

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

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

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

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

Customized Application	External Port	TCP	UDP	IP Address	Enable
UT	7777 to 27900	X	X	192.168.1.100	X
Halfife	27015 to 27015	X	X	192.168.1.105	X
PC Anywhere	5631 to 5631		X	192.168.1.102	X
VPN IPSEC	500 to 500		X	192.168.1.100	X

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

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

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

- Follow these steps to set DMZ hosting:
 1. Access the Gateway's web-based utility by going to <http://192.168.1.1> or the IP address of the Gateway. Go to the Applications and Gaming => DMZ tab. Click Enabled and enter the IP of the computer.
 2. Check the Port Forwarding pages and disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
- Once completed with the configuration, click the **Save Settings** button.

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

- Reset the Gateway to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:
 1. Access the Gateway's web-based utility by going to <http://192.168.1.1> or the IP address of the Gateway. Enter the default username and password **admin**, and click the **Administrations => Management** tab.
 2. Enter a different password in the Gateway Password field, and enter the same password in the second field to confirm the password.
 3. Click the **Save Settings** button.

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

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

- For Microsoft Internet Explorer 5.0 or higher:
 1. Click **Start, Settings, and Control Panel**. Double-click Internet Options.
 2. Click the **Connections** tab.
 3. Click the **LAN settings** button and remove anything that is checked.
 4. Click the **OK** button to go back to the previous screen.
 5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.
- For Netscape 4.7 or higher:

1. Start **Netscape Navigator**, and click **Edit, Preferences, Advanced, and Proxies**.
2. Make sure you have Direct connection to the Internet selected on this screen.
3. Close all the windows to finish.

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

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

12. I need to upgrade the firmware.

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

- Follow these steps:
 1. Go to the Linksys international website at <http://www.linksys.com/international> and select your region or country.
 2. Click the **Products** tab and select the Gateway.
 3. On the Gateway's webpage, click **Firmware**, and then download the latest firmware for the Gateway.
 4. To upgrade the firmware, follow the steps in the Administration section found in *Chapter 4: Configuring the Gateway*.

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

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

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the computer; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:
IP Address: 192.168.1.50
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
- Perform the upgrade using the TFTP program or the Gateway's web-based utility through its Administration tab.

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

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

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

Wireless-G ADSL Gateway with 2 Phone Ports

1. To connect to the Gateway, go to the web browser, and enter `http://192.168.1.1` or the IP address of the Gateway.
 2. Enter the username and password, if asked. (The default username and password is admin.)
 3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
 4. Click the **Save Settings** button. Click the **Status** tab, and click the **Connect** button.
 5. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
 6. Click the **Save Settings** button to continue.
- If the connection is lost again, follow steps 1- 6 to re-establish connection.

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

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set automatically.

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

16. The Power LED flashes continuously.

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

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

- Check if other computers work. If they do, ensure that your computer's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the computers are configured correctly, but still not working, check the Gateway. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the network and power connections.)

Wireless-G ADSL Gateway with 2 Phone Ports

- If the Gateway is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Gateway to verify a direct connection.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools, Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit, Preferences, Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

Frequently Asked Questions

What is the maximum number of IP addresses that the 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.

Where is the Gateway installed on the network?

In a typical environment, the Gateway is installed between the ADSL wall jack and the network.

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 network to network connections, but those protocols cannot connect from the Internet to a network.

Do the Gateway's network connections support 100Mbps Ethernet?

The Gateway supports 100Mbps over the auto-sensing network ports.

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

Network Address Translation (NAT) translates multiple IP addresses on the private network 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 network 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?

Wireless-G ADSL Gateway with 2 Phone Ports

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 network 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 network's 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 network 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 network 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 network (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/international 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 DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys international website, www.linksys.com/international.

How will I be notified of new Gateway firmware upgrades?

All Linksys firmware upgrades are posted on the Linksys international website at www.linksys.com/international, where they can be downloaded for free. To upgrade the Gateway's firmware, use the Administration tab of the

Gateway's web-based utility. If the Gateway's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use.

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.

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 IP address, see *Appendix D: 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.

What are the advanced features of the Gateway?

The Gateway's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.

What is the maximum number of VPN sessions allowed by the Gateway?

The maximum number depends on many factors. At least one IPSec session will work through the Gateway; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

How can I check whether I have static or DHCP IP Addresses?

Consult your ISP to obtain this information.

How do I get mIRC to work with the Gateway?

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

Can the Gateway act as my DHCP server?

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

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

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

What is the IEEE 802.11g standard?

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

What IEEE 802.11b and 802.11g features are supported?

The product supports the following IEEE 802.11b and IEEE 802.11g functions:

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

What is ad-hoc mode?

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other, peer-to-peer without the use of an access point.

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.

What is roaming?

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

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

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

What is the ISM band?

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

What is Spread Spectrum?

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

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

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

Will the information be intercepted while it is being transmitted through the air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

What is WEP?

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

What is a MAC Address?

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

How do I reset the Gateway?

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

How do I resolve issues with signal loss?

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

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

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

WEP is probably enabled on the Gateway, but not on your wireless adapter (or vice versa). Verify that the same WEP keys and levels (64 or 128) are being used on all nodes of your wireless network.

How many channels/frequencies are available with the Gateway?

There are eleven available channels, ranging from 1 to 11 (in North America).

If your questions are not addressed here, refer to the Linksys international website, www.linksys.com/international.

Appendix B: Wireless Security

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

Security Precautions

The following is a complete list of security precautions to take (as shown in this User Guide) (at least steps 1 through 5 should be followed):

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

To ensure network security, steps one through five should be followed, at least.

Security Threats Facing Wireless Networks

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

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



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

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

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you 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 System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.



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

Wireless-G ADSL Gateway with 2 Phone Ports

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

WPA RADIUS. 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.) First, select the type of WPA algorithm, **TKIP** or **AES**. 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: Configuring IPSec between a Windows 2000 or XP Computer and the Gateway

Introduction

This document demonstrates how to establish a secure IPSec tunnel using preshared keys to join a private network inside the Gateway and a Windows 2000 or XP computer. You can find detailed information on configuring the Windows 2000 server at the Microsoft website:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
<http://support.microsoft.com/support/kb/articles/Q252/7/35.asp>

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
<http://support.microsoft.com/support/kb/articles/Q257/2/25.asp>

Environment

The IP addresses and other specifics mentioned in this appendix are for illustration purposes only.

Windows 2000 or Windows XP

IP Address: 140.111.1.2 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

WAG54G

WAN IP Address: 140.111.1.1 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

LAN IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0



NOTE: Keep a record of any changes you make. Those changes will be identical in the Windows “secpol” application and the Gateway’s Web-Based Utility.



NOTE: This section’s instructions and figures refer to the Gateway. Substitute “Gateway” for “Router”. Also, the text on your screen may differ from the text in your instructions for “OK or Close”; click the appropriate button on your screen.

How to Establish a Secure IPSec Tunnel

Step 1: Create an IPSec Policy

1. Click the **Start** button, select **Run**, and type **secpol.msc** in the **Open** field. The *Local Security Setting* screen will appear.
2. Right-click **IP Security Policies on Local Computer** (Win XP) or **IP Security Policies on Local Machine** (Win 2000), and click **Create IP Security Policy**.
3. Click the **Next** button, and then enter a name for your policy (for example, **to_Router**). Then, click **Next**.
4. Deselect the **Activate the default response rule** check box, and then click the **Next** button.
5. Click the **Finish** button, making sure the **Edit** check box is checked.

Step 2: Build Filter Lists

Filter List 1: win->Router

1. In the new policy's properties screen, verify that the **Rules** tab is selected. Deselect the **Use Add Wizard** check box, and click the **Add** button to create a new rule.
2. Make sure the **IP Filter List** tab is selected, and click the **Add** button. The *IP Filter List* screen should appear. Enter an appropriate name, such as **win->Router**, for the filter list, and de-select the **Use Add Wizard** check box. Then, click the **Add** button.

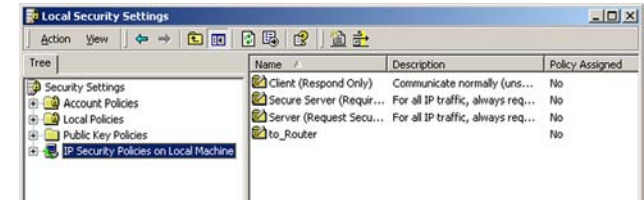


Figure C-1: Local Security Screen



NOTE: The references in this section to “win” are references to Windows 2000 and XP. Substitute the references to “Router” with “Gateway”. Also, the text on your screen may differ from the text in your instructions for “OK or Close”; click the appropriate button on your screen.

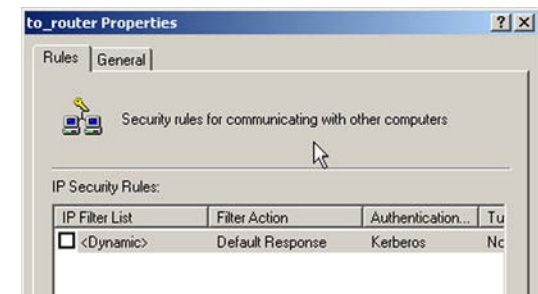


Figure C-2: Rules Tab

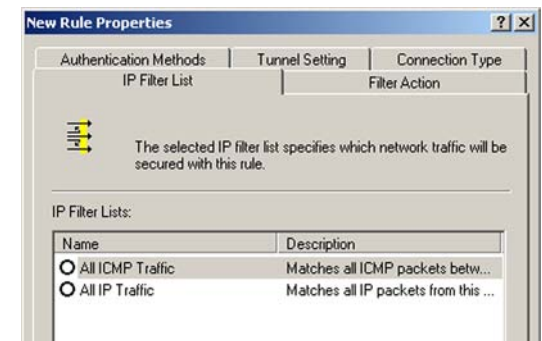


Figure C-3: IP Filter List Tab

Wireless-G ADSL Gateway with 2 Phone Ports

- The *Filters Properties* screen will appear. Select the **Addressing** tab. In the *Source address* field, select **My IP Address**. In the *Destination address* field, select **A specific IP Subnet**, and fill in the IP Address: 192.168.1.0 and Subnet mask: 255.255.255.0. (These are the Gateway's default settings. If you have changed these settings, enter your new values.)
- If you want to enter a description for your filter, click the **Description** tab and enter the description there.
- Click the **OK** button. Then, click the **OK** or **Close** button on the *IP Filter List* window.

Filter List 2: Router ->win

- The *New Rule Properties* screen will appear. Select the **IP Filter List** tab, and make sure that **win -> Router** is highlighted. Then, click the **Add** button.

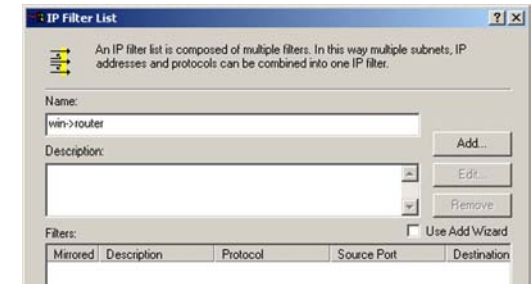


Figure C-4: IP Filter List

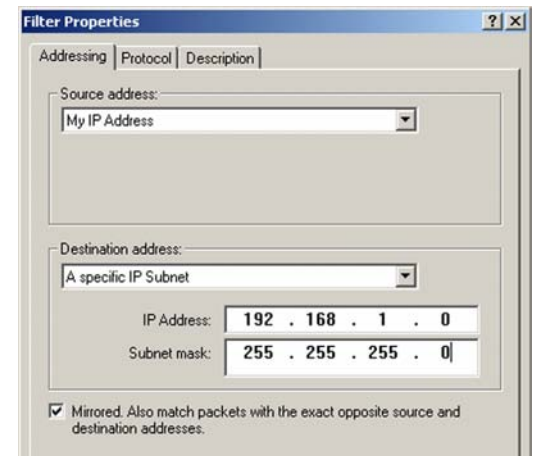


Figure C-5: Filters Properties

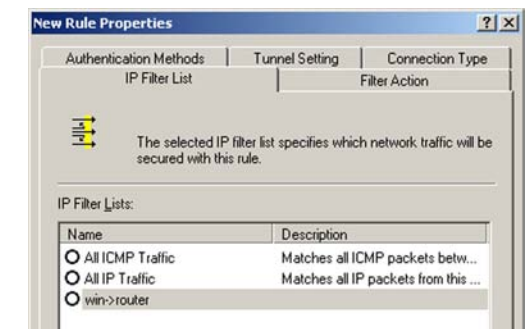


Figure C-6: New Rule Properties

7. The *IP Filter List* screen should appear. Enter an appropriate name, such as Router->win for the filter list, and de-select the **Use Add Wizard** check box. Click the **Add** button.

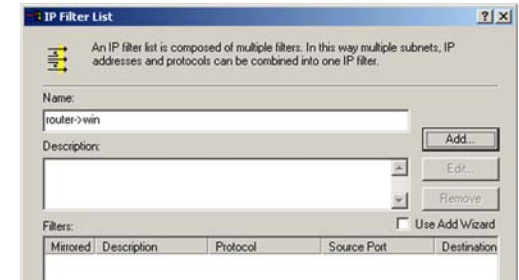


Figure C-7: IP Filter List

8. The *Filters Properties* screen will appear. Select the Addressing tab. In the *Source address* field, select **A specific IP Subnet**, and enter the IP Address: 192.168.1.0 and Subnet mask: 255.255.255.0. (Enter your new values if you have changed the default settings.) In the Destination address field, select **My IP Address**.

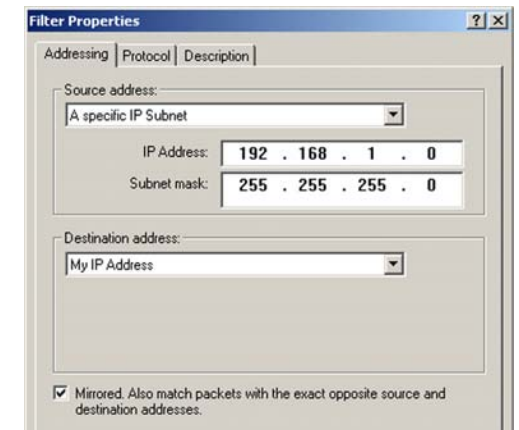


Figure C-8: Filters Properties

9. If you want to enter a description for your filter, click the *Description* tab and enter the description there.

10. Click the **OK** or **Close** button and the *New Rule Properties* screen should appear with the IP Filer List tab selected. There should now be a listing for “Router -> win” and “win -> Router”. Click the **OK** (for WinXP) or **Close** (for Win2000) button on the *IP Filter List* window.

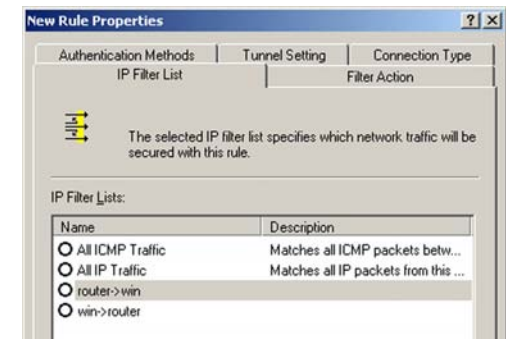


Figure C-9: New Rule Properties

Step 3: Configure Individual Tunnel Rules

Tunnel 1: win->Router

1. From the *IP Filter List* tab, click the filter list win->Router.

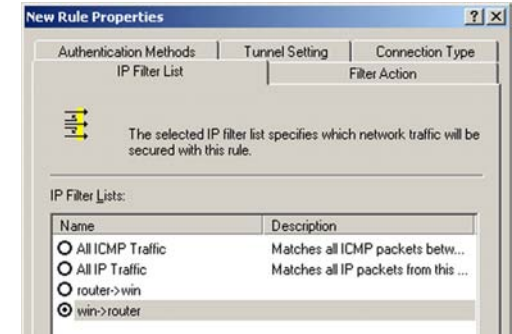


Figure C-10: IP Filter List Tab

2. Click the **Filter Action** tab, and click the filter action **Require Security** radio button. Then, click the **Edit** button.

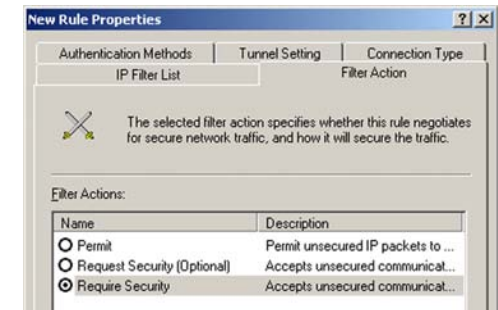


Figure C-11: Filter Acton Tab

3. From the *Security Methods* tab, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.

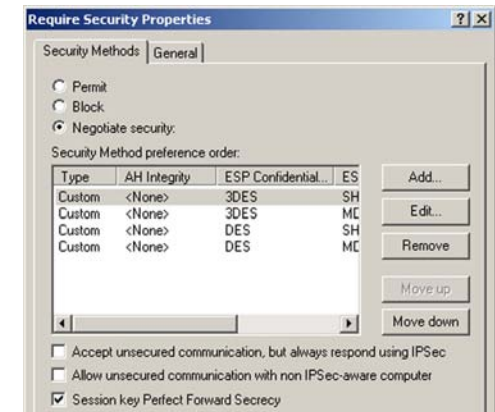


Figure C-12: Security Methods Tab

4. Select the **Authentication Methods** tab, and click the **Edit** button.

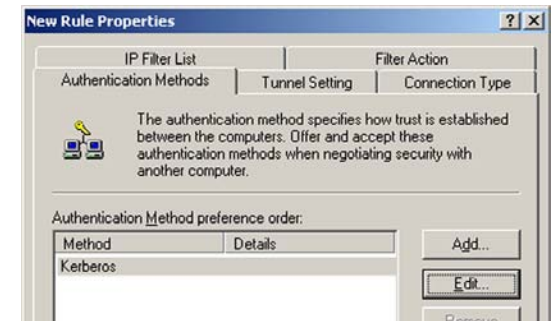


Figure C-13: Authentication Methods

5. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345. Click the **OK** button.



Figure C-14: Preshared Key

6. This new Preshared key will be displayed. Click the **Apply** button to continue, if it appears on your screen, otherwise proceed to the next step.



Figure C-15: New Preshared Key

7. Select the **Tunnel Setting** tab, and click **The tunnel endpoint is specified by this IP Address** radio button. Then, enter the WAN IP Address.

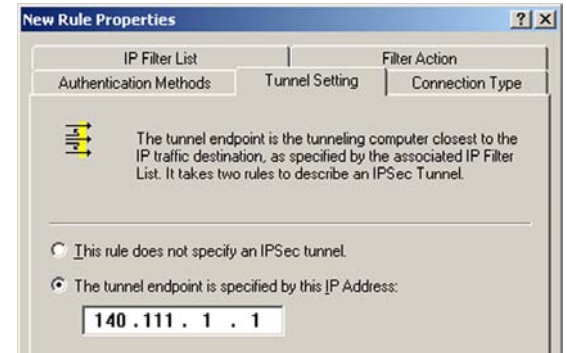


Figure C-16: Tunnel Setting Tab

8. Select the **Connection Type** tab, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.

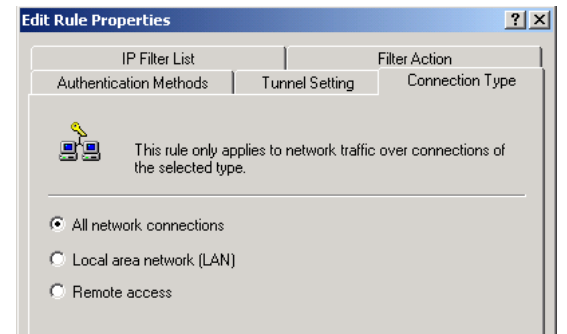


Figure C-17: Connection Type Tab

Tunnel 2: Router->win

9. In the new policy's properties screen, make sure that "win -> Router" is selected and deselect the **Use Add Wizard** check box. Then, click the **Add** button to create the second IP filter.

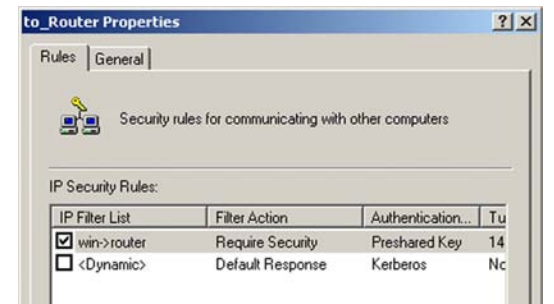


Figure C-18: Properties Screen

10. Go to the **IP Filter List** tab, and click the filter list **Router->win**.

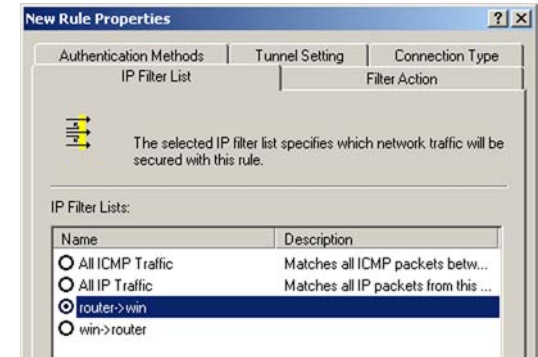


Figure C-19: IP Filter List Tab

11. Click the **Filter Action** tab, and select the filter action **Require Security**. Then, click the **Edit** button. From the **Security Methods** tab, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.

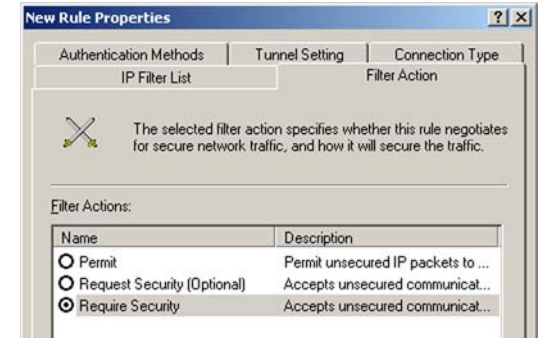


Figure C-20: Filter Action Tab

12. Click the **Authentication Methods** tab, and verify that the authentication method **Kerberos** is selected. Then, click the **Edit** button.



Figure C-21: Authentication Methods Tab

13. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345, as shown in the example. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click the **OK** button.



Figure C-22: Preshared Key

14. This new Preshared key will be displayed. Click the **Apply** button to continue, if it appears on your screen, otherwise proceed to the next step.



Figure C-23: New Preshared Key

15. Click the **Tunnel Setting** tab, click the radio button for **The tunnel endpoint is specified by this IP Address**, and enter the Windows 2000/XP computer's IP Address.

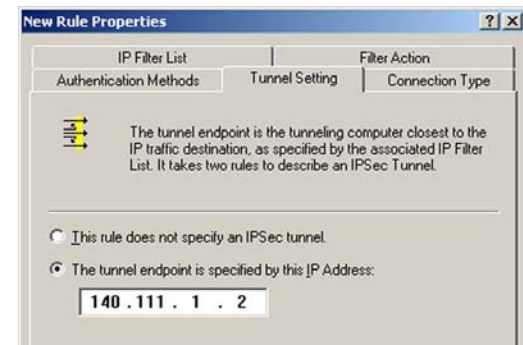


Figure C-24: Tunnel Setting Tab

16. Click the **Connection Type** tab, and select **All network connections**. Then click the **OK** or **Close** button to finish.

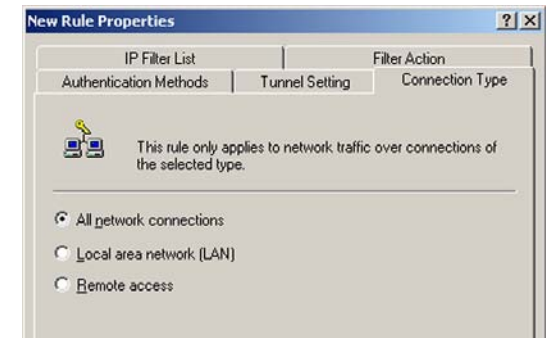


Figure C-25: Connection Type

17. From the *Rules* tab, click the **OK** or **Close** button to return to the secpol screen.

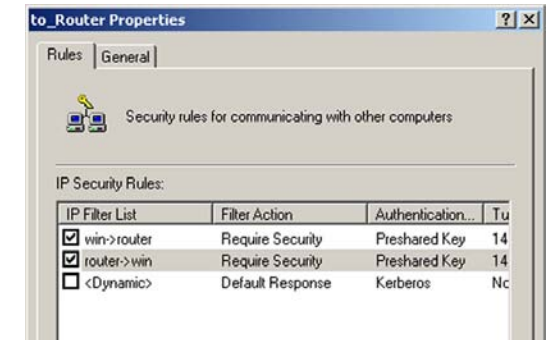


Figure C-26: Rules

Step 4: Assign New IPSec Policy

In the IP Security Policies on *Local Computer* window, right-click the policy named *to_Router*, and click **Assign**. A green arrow appears in the folder icon.

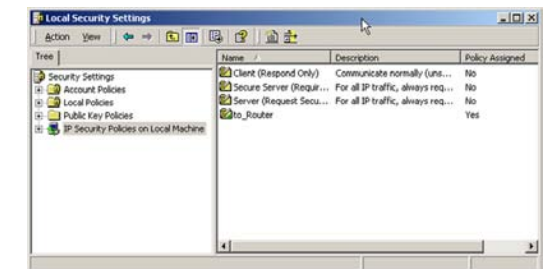


Figure C-27: Local Computer

Step 5: Create a Tunnel Through the Web-Based Utility

1. Open your web browser, and enter **192.168.1.1** in the Address field. Press the **Enter** key.
2. When the User name and Password field appears, enter the default user name and password **admin**. Press the **Enter** key.
3. From the *Setup* tab, click the **VPN** tab.
4. From the *VPN* tab, select the tunnel you wish to create in the *Select Tunnel Entry* drop-down box. Then click **Enabled**. Enter the name of the tunnel in the *Tunnel Name* field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
5. Enter the IP Address and Subnet Mask of the local VPN Router in the *Local Secure Group* fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).
6. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN Router or device with which you wish to communicate) in the *Remote Security Router* fields.
7. Select from two different types of encryption: **DES** or **3DES** (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting **Disable**.
8. Select from two types of authentication: **MD5** and **SHA** (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication.
9. Select the Key Management. Select **Auto (IKE)** and enter a series of numbers or letters in the *Pre-shared Key* field. Check the box next to **PFS** (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the *Key Lifetime* field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.
10. Click the **Save Settings** button to save these changes.

Your tunnel should now be established.

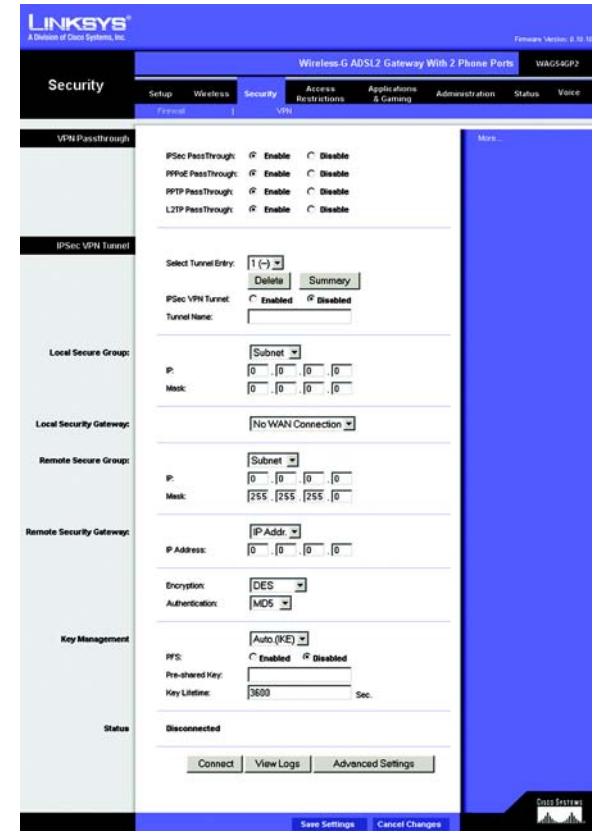


Figure C-28: VPN Tab

Appendix D: 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.
3. Write down the Adapter Address as shown on your computer screen. 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 shown displays the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

The example shown displays 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.

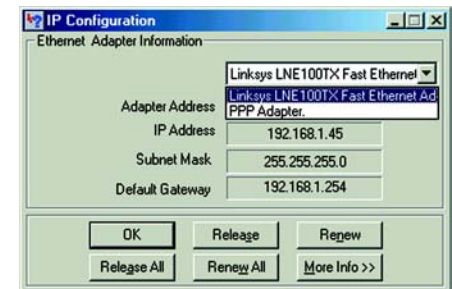


Figure D-1: IP Configuration Screen

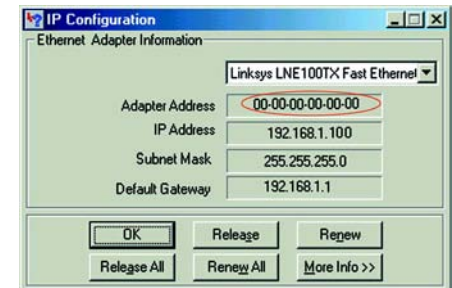


Figure D-2: MAC Address/Adapter Address

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; 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 shown displays the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

The example shown displays the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

```
C:\>ipconfig /all
Windows 2000 IP Configuration

Host Name . . . . . :
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  :
   Description . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
dapter
   Physical Address. . . . . : 00-00-00-00-00-00
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address. . . . . : 192.168.1.100
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.1.1
   DHCP Server . . . . . : 192.168.1.1
   DNS Servers . . . . . : 192.168.1.1

   Primary WINS Server . . . . . : 192.168.1.1
   Secondary WINS Server . . . . . :
   Lease Obtained. . . . . : Monday, February 11, 2002 2:31:47 PM
   Lease Expires . . . . . : Tuesday, February 12, 2002 2:31:47 PM

C:\>
```

Figure D-3: MAC Address/Physical Address

Appendix E: Upgrading Firmware

The ADSL Gateway allows you to upgrade firmware for the Gateway's networking functions through the Web-Utility's Firmware Upgrade tab from the Administration tab. Follow these instructions:

Upgrade from WAN

To upgrade the Gateway's firmware from the WAN : Enter the URL for the firmware in the URL field, then click the **Upgrade** button, and follow the instructions there.

Upgrade from LAN

1. Click the **Browse** button to find the firmware upgrade file that you downloaded from the Linksys website and then extracted.
2. Double-click the firmware file you downloaded and extracted. Click the **Upgrade** button, and follow the instructions there.



Figure E-1: Upgrade Firmware

Appendix F: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Appendix G: Glossary

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

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

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

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

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

Bit - A binary digit.

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

Broadband - An always-on, fast Internet connection.

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

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

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

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

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

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

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

Wireless-G ADSL Gateway with 2 Phone Ports

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

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

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

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

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

Encryption - Encoding data transmitted in a network.

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

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

Firmware - The programming code that runs a networking device.

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

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

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

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

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

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

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

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

Wireless-G ADSL Gateway with 2 Phone Ports

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

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

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

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

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

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

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

Packet - A unit of data sent over a network.

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

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

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

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

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

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

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

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

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

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

Wireless-G ADSL Gateway with 2 Phone Ports

Router - A networking device that connects multiple networks together.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

Wireless-G ADSL Gateway with 2 Phone Ports

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

Upload - To transmit a file over a network.

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

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

WAN (Wide Area Network)- The Internet.

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

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

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

Appendix H: Specifications

Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, IEEE 802.3, G.992.1 (G.dmt), G.992.2 (G.lite), ITU G.992.3, ITU G.992.5, ANSI T1.413i2, WAG54G-E1: Annex-B, WAG54G-DE: UR-2
Ports	Power, LINE (ADSL), Ethernet (1-4), Phone (1-2)
Buttons	One Reset Button, One On/Off Switch
Cabling Type	UTP CAT 5 or better, Phone Cable (POTS)
Data Rate	Up to 54Mbps (wireless) Up to 8Mbps downstream ADSL (G.992.1) Up to 800kbps upstream ADSL (G.992.1)
Transmit Power	18 dBm on 802.11b and 15dBm on 802.11g
LEDs	Power, Ethernet (1-4), Wireless-G (WLAN), Phone (1-2), DSL, Internet
Security Features	WEP, WPA, RADIUS
WEP Key Bits	64, 128
Dimensions	6.69" x 6.69" x 1.22" (170 mm x 130 mm x 31 mm)
Unit Weight	0.90 lbs. (0.408 kg)
Power	12VDC 1.25A
Certifications	FCC Part 15B Subpart B Class B, FCC Part 15C Subpart B, FCC Part 68, UL
Operating Temp.	0°C to 40°C

Wireless-G ADSL Gateway with 2 Phone Ports

Storage Temp. -20°C to 70°C

Operating Humidity 10% to 85% Non-Condensing

Storage Humidity 5% to 90% Non-Condensing

Appendix I: 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 USA.

Appendix J: 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 device complies with Canadian ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry 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

Wireless-G ADSL Gateway with 2 Phone Ports

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 tyypinen 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 complètement 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 soumise 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 K: Contact Information

Need to contact Linksys?

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

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

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

800-546-5797 (LINKSYS)
949-823-3002

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