

Instant Broadband™ Series

ADSL Gateway

Modem / Router / 4-Port Switch / Wireless-Ready



Use this guide to install the following product:

BEFDSR41W

User Guide

COPYRIGHT & TRADEMARKS

Copyright © 2002 Linksys, All Rights Reserved. Instant Broadband is a trademark of Linksys. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. All other trademarks and brand names are the property of their respective proprietors.

LIMITED WARRANTY

Linksys guarantees that every Instant Broadband ADSL Gateway with Modem / Router / 4-Port Switch / Wireless-Ready will be free from physical defects in material and workmanship for one year from the date of purchase, when used within the limits set forth in the Specifications section of this User Guide. If the product proves defective during this warranty period, call Linksys Technical Support in order to obtain a Return Authorization number. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. When returning a 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. All customers located outside of the United States of America and Canada shall be held responsible for shipping and handling charges.

IN NO EVENT SHALL LINKSYS'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS OFFERS NO REFUNDS FOR ITS PRODUCTS. Linksys makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Linksys reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to:

Linksys P.O. Box 18558, Irvine, CA 92623.

FCC PART 15 CLASS B STATEMENT

In compliance with the Federal Communications Commission (FCC), the following FCC Part 15 Regulations are provided regarding the installation and operation of the Linksys BEFDSR41W ADSL Gateway.

This equipment has been tested and found to comply with the limits 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 in accordance with 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 can be determined 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 and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult a dealer or an experienced radio/TV technician for assistance.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC PART 68 STATEMENT

This equipment complies with Part 68 of the FCC Rules. A label is attached to the equipment that contains, among other information, its FCC registration number and ringer equivalence number. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC Jack: RJ-11.

An FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack, which is FCC Part 68 compliant. Connection to the telephone network should be made by using the standard modular telephone jack.

The REN is useful to determine the quantity of devices that may be connected to the telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of RENs should not exceed 5. To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

In the event this equipment should fail to operate properly, disconnect the unit from the telephone line. Try using another FCC approved device in the same telephone jack. If the trouble persists, call the telephone company repair service bureau. If the trouble does not persist and appears to be with this unit, disconnect the unit from the telephone line and discontinue use of the unit until it is repaired. Please note that the telephone company may ask that you disconnect the equipment from the telephone network until the problem has been corrected or until you are sure that the equipment is not malfunctioning. The user must use the accessories and cables supplied by the manufacturer to get optimum performance from the product.

No repairs may be done by the customer. If trouble is experienced with this equipment, please contact your authorized support provider for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you remove the equipment from the network until the problem is resolved. This equipment cannot be used on telephone company provided coin service. Connection to Party Line Service is subject to state tariffs.

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 products (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

Table of Contents

Chapter 1: Introduction	1	Filtering	47
The Linksys ADSL Gateway with Modem / Router / 4-Port Switch / Wireless-Ready	1	Forwarding	49
Features	1	Dynamic Routing	51
Package Contents	2	Static Routing	53
Minimum Requirements	2	DMZ Host	55
An Introduction to LANs and WANs	2	Firewall	56
IP Addresses	3	Link Test	57
Network Setup Overview	5		
Chapter 2: Getting to Know the ADSL Gateway		Appendix A: Troubleshooting	58
with Modem / Router / 4-Port Switch / Wireless-Ready	6	Common Problems and Solutions	58
The Gateway's Back Panel Ports	6	Frequently Asked Questions	60
The Gateway's Front Panel LEDs	7		
 		Appendix B: Configuring Wireless Security	64
Chapter 3: Connecting the Gateway	9	Configuring Wireless Security in Windows XP	68
Chapter 4: Configuring the PCs	12	Appendix C: Installing the TCP/IP Protocol	73
Overview	12		
Windows 95, Windows 98, Windows Millennium	13	Appendix D: Finding the MAC Address and IP	
Windows 2000	15	Address for Your Ethernet Adapter	75
Windows XP	17		
 		Appendix E: Specifications	79
Chapter 5: Configuring the Gateway	19	Environmental Specifications	80
Chapter 6: Using the Gateway's Web-based		Appendix F: Warranty Information	81
Utility	25		
Quick and Easy Gateway Administration	25	Appendix G: Contact Information	82
Setup	26		
Password	34		
Status	36		
DHCP	38		
Log	40		
UPnP	41		
Help	42		
Wireless	44		
Advanced	46		

Chapter 1: Introduction

The Linksys ADSL Gateway with Modem / Router / 4-Port Switch / Wireless-Ready

Thank you for choosing the Instant Broadband™ ADSL Gateway with Modem / Router / 4-Port Switch / Wireless-Ready. This Gateway allows you to set up a network with your PCs and share your Internet connection.

The Gateway does this by connecting to your ADSL line, and using the Gateway's Ethernet ports to connect your PCs; it's like each PC is connected directly to the Internet. This way, you have an Ethernet network where you have several PCs utilizing one Internet connection simultaneously. Plus, if you add a Linksys wireless PC Card, it can be used as an Access Point and the Gateway can bridge your Ethernet network with your wireless PCs.

The PCs that you connect to the Gateway's four LAN ports, when properly configured, create a LAN, or Local Area Network. They are connected with an Ethernet cable plugged into your computer's Ethernet adapter at one end and into one of the Gateway's LAN ports (numbered from one to four) at the other end. The term "Ethernet" is used to refer to your network accessories, such as cables and adapters, because Ethernet refers to the type of network that you are setting up. Ethernet refers to the accessories that transfer computer data from 10Mbps to 100Mbps (speeds used by network devices.)

The Gateway allows you to share your ADSL connection using a built-in ADSL modem, and can plug directly into your ADSL-enabled wall jack (DSL service line). The PCs that are connected to the Gateway share this connection.

Features

- Download Speeds of up to 8Mbps
- Upload Speeds of up to 800kbps
- Prevents DoS (Denial of Service) Attacks
- E-mail and Web-based Logging of Security Events
- MAC Address Filtering, Port Forwarding, DMZ Support
- Configurable through Your Networked PC's Web Browser
- Supports VPN Pass-Through for IPSec, PPTP, and L2TP Protocols
- Internal 4-Port Switch Dramatically Speeds Up Your Network
- DHCP Server Capability to Assign IP Addresses Automatically
- Wireless Capabilities Available with Use of Optional WPC11 (sold separately)
 - Supports a High Data Rate of up to 11Mbps for up to 28 Simultaneous Wireless Connections
 - Capable of 64 and 128-Bit WEP Encryption
- Compliant with ANSI T1.413i2, ITU-T G.dmt (G.992.1), and ITU G.lite (G.992.2) Standards
- Supports RFC 1483, RFC 2364 PPPoA, RFC 2516 PPPoE Protocols



Figure 1-1

Package Contents

- One ADSL Gateway with Modem / Router / 4-Port Switch / Wireless-Ready
- One Power Adapter
- One RJ-11 Phone Cable
- One User Guide
- One Fast Start and Registration Card (not shown)

Minimum Requirements

- Network Adapter with Ethernet (UTP CAT 5) Cabling and TCP/IP Protocol Installed per PC
- Internet Explorer 4.0 or Netscape Navigator 4.7 or Higher for Web-based Configuration
- ADSL Connection and Activated Account
- Optional Wireless Network PC Card Model WPC11 for Wireless Connection (sold separately)

An Introduction to LANs and WANs

Simply put, a **router** is a network device that connects two networks together.

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

Think of the Gateway as a network device with two sides: the first side is made up of your private **Local Area Network (LAN)** of PCs. The other, public side is the Internet, or the **Wide Area Network (WAN)**, outside of your home or office.

The Gateway's firewall (NAT) protects your network of PCs so users on the public, Internet side cannot "see" your PCs. This is how your LAN, or network, remains private. The Gateway protects your network by inspecting the first packet coming in through the WAN port before delivery to the final destination on the LAN port. 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 PC on the LAN side.

IP Addresses

What's an IP Address?

IP stands for Internet Protocol. Every device on an IP-based network, including PCs, print servers, and routers, requires an **IP address** to identify its "location," or address, on the network. This applies to both the WAN and LAN connections. There are two ways of assigning an IP address to your network devices.

Static IP Addresses

A **static IP address** is a fixed IP address that you assign manually to a PC 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 are commonly used with network devices such as server PCs or print servers.

When using the Gateway to share your ADSL 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 the information from your ISP.



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

Since the Gateway has firewall security (NAT), the only IP address that can be seen from the Internet for your network is the Gateway's WAN IP address.

However, even this WAN IP address for the Gateway can be blocked, so that the Gateway and network seem invisible to the Internet—see the IP Filtering section in "Chapter 6: Using the Gateway's Web-based Utility."

Dynamic IP Addresses

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

For ADSL users, many ISPs may require you to log on with a user name and password to gain access to the Internet. This is a dedicated, high-speed connection type called Point to Point Protocol over Ethernet (PPPoE). PPPoE is similar to a dial-up connection, but PPPoE does not dial a phone number when establishing a connection. PPPoE also will provide the Gateway with a dynamic IP address to establish a connection to the Internet. Point to Point Protocol over ATM, or PPPoA, is a similar login method also used for some ADSL connections.

DHCP (Dynamic Host Configuration Protocol) Servers

DHCP frees you from having to assign IP addresses manually every time a new user is added to your network. PCs and other network devices using dynamic IP addressing are assigned a new IP address by a **DHCP server**. The PC or network device obtaining an IP address is called the **DHCP client**. By default, the Gateway’s WAN setting is DHCP client.

A DHCP server can either be a designated PC on the network or another network device, such as the Gateway. By default, a DHCP server (LAN side) is enabled on the Gateway. 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 6: Using the Gateway’s Web-based Utility.”



Note: Even if you assign a static IP address to a PC, other PCs can still use DHCP’s dynamic IP addressing, as long as the static IP address is not within the DHCP range of the LAN IP Address.

If the dynamic IP addressing fails to provide a dynamic IP address, refer to “Appendix A: Troubleshooting.”

Network Setup Overview

This user guide covers the basic steps for setting up a network with a Gateway. After going through the “Getting to Know the Gateway” chapter, most users will only need to use the following chapters:

- Chapter 3: Connecting the Gateway
This chapter instructs you on how to connect the ADSL line to the Gateway and connect the PC(s) to the Gateway.
- Chapter 4: Configuring the PCs
This chapter instructs you on how to configure your PC(s) for a DHCP connection, if the network settings are not already set to DHCP.
- Chapter 5: Configuring the Gateway
This chapter explains how to configure the Gateway using your web browser and the Gateway’s web-based utility. You will configure the Gateway using the settings provided by your ISP.

When you’re finished with the basic steps, then you are ready to connect to the Internet. After the PC(s) can access the Internet through the Gateway, you can alter the Gateway’s settings further; for example, you can adjust security features and other settings to enable online gaming, run Internet servers, configure a wireless LAN (WPC11 required) and more!



Chapter 2: Getting to Know the ADSL Gateway with Modem / Router / 4-Port Switch / Wireless-Ready

The Gateway's Back Panel Ports

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



Figure 2-1

ADSL	The ADSL port is where you will connect your ADSL line.
Ports 1-4	These four LAN (Local Area Network) ports connect to network devices, such as PCs, print servers, and remote hard drives.
Power	The Power port is where you will connect the power adapter.
On/Off Switch	This switch is used for turning the Gateway on and off.
PC Card Slot	This is where you can connect the optional wireless PC card (not included) for wireless features.

The Gateway's Front Panel LEDs



Figure 2-2

Power	<i>Green.</i> The Power LED lights up when the Gateway is powered on.
Diag	<i>Green.</i> The Diag LED flashes when the Gateway is booting up. If this flashes or stays solid after the bootup phase, the Gateway may be malfunctioning. See “Appendix A: Troubleshooting” if you encounter this problem.
Link/Act	<i>Green.</i> The Link/Act LED serves two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through the corresponding port (1 , 2 , 3 or 4). If the LED is flickering, the Gateway is actively sending or receiving data over that port.
Full/Col	<i>Green.</i> The Full/Col LED also serves two purposes. If this LED is lit up continuously, the connection made through the corresponding port is running in Full Duplex mode. If the LED flickers, the connection is experiencing collisions. Infrequent collisions are normal.
100	<i>Green.</i> The 100 LED lights up when a successful 100Mbps connection is made through the corresponding port. If this LED does not light up, then your connection speed is 10 Mbps.
WLAN Link	<i>Green.</i> This LED is solidly lit when a wireless PC Card is inserted and functioning in the Gateway.
WLAN Act	<i>Green.</i> This LED flashes when there is wireless activity.

- ADSL Session** *Green.* This LED is solidly lit when a PPPoE session is established.
- ADSL Link** *Green.* This LED is off when an ADSL line is not detected. It flashes when the Gateway is attempting to make an ADSL connection. The LED is solidly lit when an ADSL connection has been successfully established.
- ADSL Act** *Green.* This LED flashes when there is activity across the ADSL connection.

Proceed to “Chapter 3: Connecting the Gateway.”

The Reset Button

Briefly pressing the Reset Button or rebooting the Gateway will refresh the Gateway’s connections. If the Gateway locks up, simply press the Reset Button or power it down for three to five seconds. Leaving the power off for too long could result in the loss of network connections.

Pressing the Reset Button and holding it in for a few seconds will clear all of the Gateway’s data and restore the factory defaults. This should be done only if you are experiencing heavy routing problems, and only after you have exhausted all of the other troubleshooting options. By resetting the Gateway, you run the risk of creating conflicts between your PCs’ actual IP Addresses and what the Gateway thinks their IP Addresses should be. You may be forced to reboot each network PC.

Chapter 3: Connecting the Gateway

Connecting Your Hardware and Booting Up

You will connect the Gateway to your ADSL line and to the computers in your home or business.

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

1. Connect one end of the provided phone cable to the ADSL (RJ-11 phone) port that is on the back of the Gateway.



Figure 3-1

2. Connect the other end of the phone cable to the wall jack with ADSL service.



Figure 3-2

3. Connect one end of an Ethernet cable to your PC's Ethernet adapter. Connect the other end of the cable to one of the LAN ports on the back of the Gateway. Repeat this process for every PC that you want to connect to the Gateway.

Note: If your PC's Ethernet adapter is not set up, please refer to the Ethernet adapter's user guide for more information.



Figure 3-3



Figure 3-4

If you are connecting more than four PCs to the Gateway, you will also need to connect a hub or switch to the Gateway.



Note: If you have a Linksys wireless PC Card (WPC11), be sure to fully insert it into the PC Card slot on the back of the Gateway before turning on the power. You must have this card inserted in order to use the Gateway's wireless features.

4. Connect the power adapter to the Gateway. Plug the power adapter into the electrical outlet.



Figure 3-5



Figure 3-6

5. Turn on the Gateway. Then, turn on the first PC that you want to use to configure the Gateway.

Go to “Chapter 4: Configuring the PCs.”



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: The ADSL Gateway (with optional WPC11) is configured by default to work out of the box with all Linksys Wireless Adapters. If you have changed the defaults on your Linksys Wireless Adapters, or are using other wireless adapters, you must temporarily change your wireless adapter settings to: (SSID = linksys) in order to initially access the Gateway wirelessly. After you have accessed the Gateway with the default settings, you can change the Gateway settings to coincide with your Network settings and reset your adapters.

Chapter 4: Configuring the PCs

Overview

The instructions in this chapter will help you configure each of your computers to be able to communicate with the Gateway.

To do this, you need to configure your PC's network settings to obtain an IP (or TCP/IP) address automatically (called DHCP). Computers use IP addresses to communicate with each other across a network or the Internet.

You will need to know which operating system your computer is running, such as Windows 95, 98, Millennium, 2000, or XP. One way to find out which operating system you have is by clicking the **Start** button and then going to the **Settings** option. Then click **Control Panel**, and then double-click the **System** icon.

You may need to do this for each computer you are connecting to the Gateway.

The next few pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using.

If your operating system is not referenced here, refer to your operating system documentation.

Once you've configured your computers, continue to "Chapter 5: Configuring the Gateway."

Windows 95, Windows 98, Windows Millennium

1. Go to the Network screen by clicking the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network** icon.
2. On the Configuration tab, select the **TCP/IP line** for the applicable Ethernet adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. If the word **TCP/IP** appears by itself, select that line. (If there is no TCP/IP line listed, refer to "Appendix C: Installing the TCP/IP Protocol" or your Ethernet adapter's user guide to install TCP/IP now.) Click the **Properties** button.

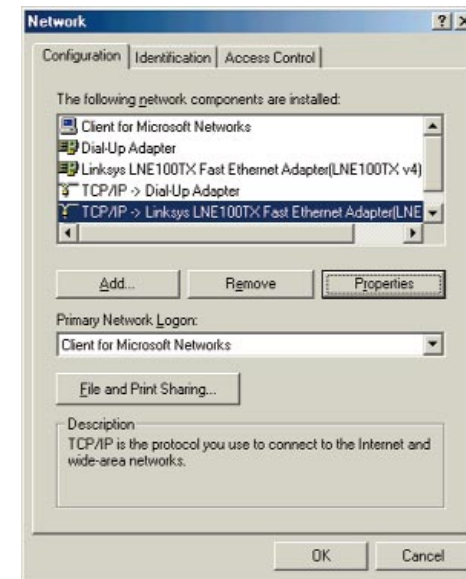


Figure 4-1

- Click the **IP Address** tab. Select **Obtain an IP address automatically**.

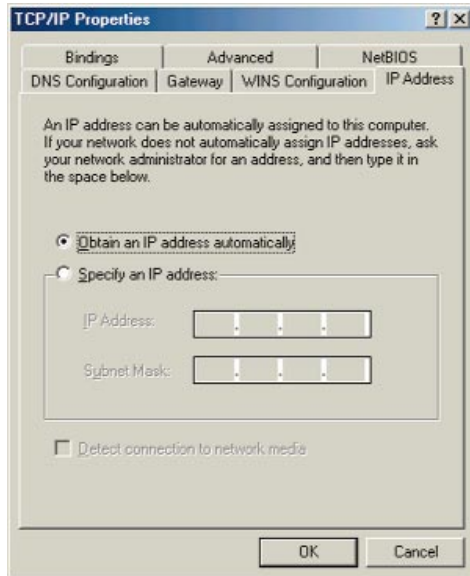


Figure 4-2

- Now click the **Gateway** tab to ensure that the Installed Gateway field is left blank. Click the **OK** button.
- Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Supply them by pointing to the correct file location, e.g., D:\win98, D:\win9x, c:\windows\options\cabs, etc. (if “D” is the letter of your CD-ROM drive).
- Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

Go to “Chapter 5: Configuring the Gateway.”

Windows 2000

- Go to the Network screen by clicking the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network and Dial-up Connections** icon.
- Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. Double-click the **Local Area Connection**.

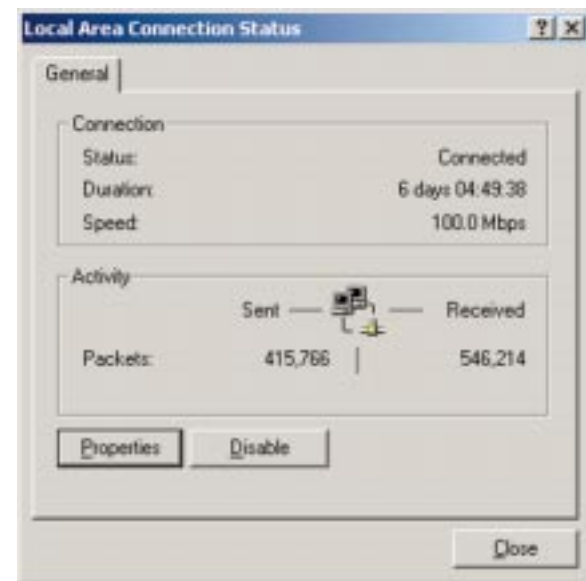


Figure 4-3

- The Local Area Connection Status screen will appear. Click the **Properties** button.

4. Select **Internet Protocol (TCP/IP)**, and click the **Properties** button.

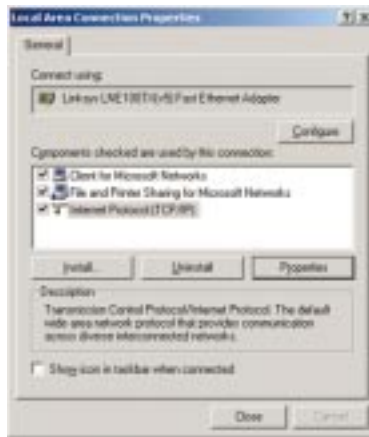


Figure 4-4

5. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.



Figure 4-5

6. Restart your computer.

Go to “Chapter 5: Configuring the Gateway.”

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 to the Network screen by clicking the **Start** button and then **Control Panel**. From there, click the **Network and Internet Connections** icon and then the **Network Connections** icon.
2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button.

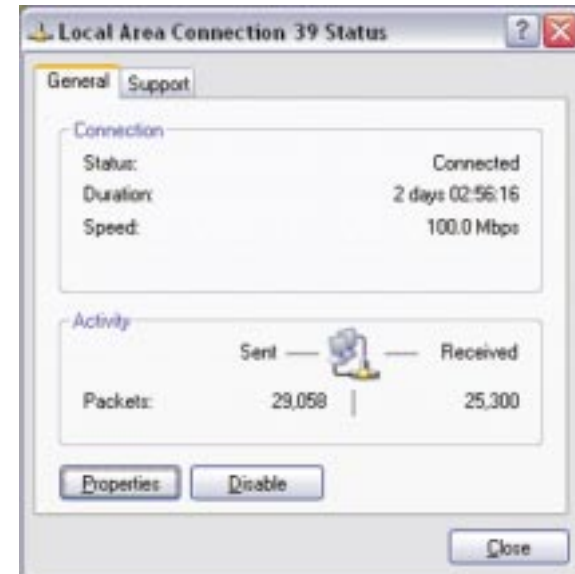


Figure 4-6

3. The Local Area Connection Status screen will appear. Click the **Properties** button.

4. Select **Internet Protocol (TCP/IP)**, and click the **Properties** button.

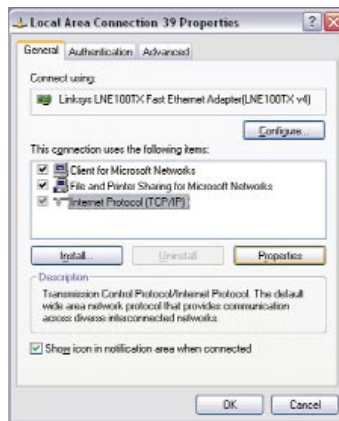


Figure 4-7

5. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again (or the **Close** button if any settings were changed) to complete the PC configuration.



Figure 4-8

6. Restart your computer.

Go to “Chapter 5: Configuring the Gateway.”

Chapter 5: Configuring the Gateway

Configuring the Gateway

In this chapter, you will configure the Linksys ADSL Gateway to be able to gain access to the Internet through your Internet Service Provider (ISP). **You will need the setup information provided by your ADSL ISP:**

- Your ADSL line VPI and VCI
- Your ADSL encapsulation type and multiplexing

For **PPPoA** or **PPPoE** users, you also need these values from your ISP:

- Your username and password

For **RFC 1483** users, you may need these values from your ISP:

- Your ADSL fixed Internet IP address
- Your Subnet Mask
- Your Default Gateway
- Your primary DNS IP address

The above information should have been provided by your ADSL ISP. If not, contact your ISP and they will be able to supply you with the correct settings. The instructions from your ISP tell you how to set up your PC for Internet access. Because you are now using the Gateway to share Internet access among several computers, you will use the setup information to configure the Gateway instead of your PC. You only need to configure the Gateway once using the first computer you set up.



Figure 5-1

1. Open your web browser. (It is all right if you get an error message at this point. Continue following these directions.) Enter **http://192.168.1.1** in the web browser's Address field. Press the **Enter** key.



Figure 5-2

2. An Enter Network Password window, shown in Figure 5-3, will appear (Windows XP users will see a Connect to 192.168.1.1 window, shown in Figure 5-4). Enter **admin** in lowercase letters in the User Name field, and enter **admin** in lowercase letters in the Password field (**admin** is the default user name and password). Then, click the **OK** button.



Figure 5-3



Figure 5-4

3. The Gateway configuration screen will appear with the Setup tab selected. Based on the setup instructions from your ISP, you may need to provide the following information.

Host Name and **Domain Name** These fields allow you to provide a host name and domain name for the Gateway. These fields are usually left blank. If requested by your ISP, complete these two fields.

Virtual Circuit ID (VPI and VCI) These fields consist of two items: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). Your ISP will provide the correct settings for this field.

4. The Gateway supports five modes of Encapsulation: RFC 1483 Bridged, RFC 1483 Routed, RFC2364 PPPoA, RFC2516 PPPoE, and Bridged Mode Only. These modes are listed in the drop-down menu for the **Encapsulation** setting. Each Setup screen and available features will differ depending on what kind of connection mode you select. The instructions for RFC 1483 Bridged, RFC2516 PPPoE, and RFC2364 PPPoA are listed below; if the instructions for your connection mode is not explained here, then proceed to “Chapter 6: Using the Gateway’s Web Based Utility.”

A. RFC 1483 Bridged

This mode supports two types of WAN IP Addresses: Dynamic IP Address or Static IP Address. Follow the directions for the type of WAN IP Address you need to use.

Dynamic IP Address

If your ISP says that you are connecting through a dynamic IP address, follow these steps:

1. Select **Dynamic IP Address** as the WAN IP Address.
2. Click the **Apply** and **Continue** buttons to save the settings.

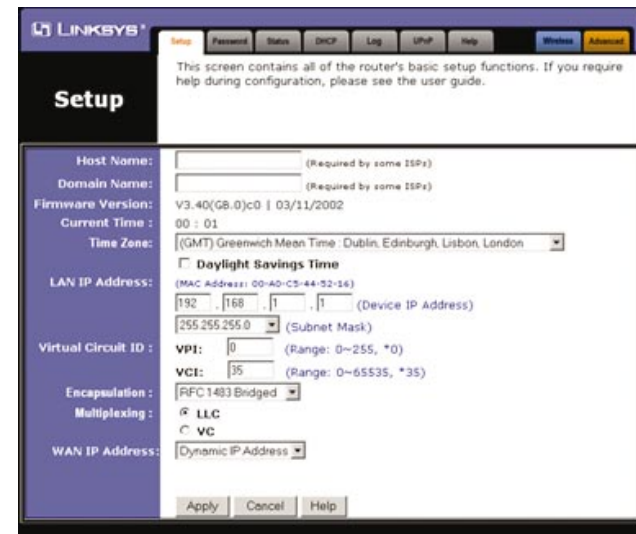


Figure 5-5

Static IP Address

If your ISP says that you are connecting through a static or fixed IP address from your ISP, follow these steps:

1. Select **Static IP** Address as the WAN IP Address.
2. Enter the **IP Address**.
3. Enter the **Default Gateway Address**.
4. Enter the **DNS** in the **1** and/or **2** fields. You need to enter at least one DNS address.
5. Click the **Apply** and **Continue** buttons to save the settings.

The screenshot shows the Linksys Setup page with the following configuration options visible:

- Host Name: (Required by some ISPs)
- Domain Name: (Required by some ISPs)
- Firmware Version: V3.40(GB.0)c0 | 03/11/2002
- Current Time: 00 : 01
- Time Zone: [(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London]
- Daylight Savings Time:
- LAN IP Address: (MAC Address: 00-A0-C5-44-52-16) 192 . 168 . 1 . 1 (Device IP Address)
- Subnet Mask: 255.255.255.0 (Subnet Mask)
- Virtual Circuit ID: VPI: 0 (Range: 0~255, *0); VCI: 35 (Range: 0~65535, *35)
- Encapsulation: RFC1483 Bridged
- Multiplexing: LLC; VC
- WAN IP Address: Static IP Address
- Specify an IP Address: [0] . [0] . [0] . [0]
- Default Gateway Address: [0] . [0] . [0] . [0]
- DNS 1: [0] . [0] . [0] . [0]
- DNS 2: [0] . [0] . [0] . [0]

Figure 5-6

B. RFC 2516 PPPoE or RFC 2364 PPPoA

If your ISP says that you are connecting through PPPoE or PPPoA, or if you normally enter a user name and password to access the Internet, follow these steps:

1. Select **PPPoE or PPPoA** as appropriate for the WAN Connection Type.
2. If you selected **PPPoE**, enter the **Service Name** (if required).
3. Enter the **User Name**.
4. Enter the **Password**.
5. Click the **Apply** and **Continue** buttons to save the settings.

The screenshot shows the Linksys Setup page with the following configuration options visible:

- Host Name: (Required by some ISPs)
- Domain Name: (Required by some ISPs)
- Firmware Version: V3.40(GB.0)c0 | 03/11/2002
- Current Time: 00 : 01
- Time Zone: [(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London]
- Daylight Savings Time:
- LAN IP Address: (MAC Address: 00-A0-C5-44-52-16) 192 . 168 . 1 . 1 (Device IP Address)
- Subnet Mask: 255.255.255.0 (Subnet Mask)
- Virtual Circuit ID: VPI: 0 (Range: 0~255, *0); VCI: 35 (Range: 0~65535, *35)
- Encapsulation: RFC 2516 PPPoE
- Multiplexing: LLC; VC
- Login: Service Name: (Required by some ISPs); User Name: ; Password:
- Connection: Connect on Demand: Max Idle Time 5 Min.; Keep Alive

Figure 5-7

5. If you haven't already done so, click the **Apply** button and then the **Continue** button to save your Setup settings. Close the web browser.
6. Congratulations! You've successfully configured the Gateway. Test the setup by opening your web browser from any computer and entering *www.linksys.com/registration*.



Figure 5-8

If you need advanced setting information, please refer to “Chapter 6: Using the Gateway’s Web-Based Utility” or the Linksys support website at *support.linksys.com*.

If you are unable to reach our website, you may want to review what you did in this section or refer to “Appendix A: Troubleshooting.”

Go to “Chapter 6: Using the Gateway’s Web-based Utility” for more details and advanced settings information.

Chapter 6: Using the Gateway’s Web-based Utility

Quick and Easy Gateway Administration

For your convenience, an administrative utility has been programmed into the Gateway where all Gateway-based administrative tasks are performed. This chapter will explain all of the functions in this utility. The web utility can be accessed by an PC on the network by typing the Gateway’s default IP address **192.168.1.1** in the PC’s web browser address window, as shown in Figure 6-1. Press the **Enter** key.

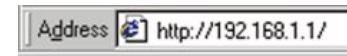


Figure 6-1

An Enter Network Password window, shown in Figure 6-2, will appear (Windows XP users will see a Connect to 192.168.1.1 window, shown in Figure 6-3). Enter **admin** in lowercase letters in the User Name field, and enter **admin** in lowercase letters in the Password field (**admin** is the default user name and password). Then, click the **OK** button.



Figure 6-2



Figure 6-3

In the following sections, you’ll find brief descriptions of each web page in the utility and each page’s key functions. More detailed explanations and instructions can be found by clicking each page’s **Help** button or on Linksys’s website at *www.linksys.com*. To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you’ve entered on any page, click the **Cancel** button.

Setup

The Setup screen is the first screen you see when you access the web-based utility. If you have already installed and set up the Gateway, you have already seen this screen and properly configured each of the values.

- **Host Name & Domain Name** These fields allow you to supply a host and domain name for the Gateway. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.
- **Firmware Version** This entry shows the version and date of the firmware you are using. Future versions of the Gateway's firmware will be posted and available for download on the Linksys website at www.linksys.com.
- **Current Time** The Gateway will try to reach an Internet timeserver and display the current time in this location. If a timeserver cannot be reached, this will show the time elapsed since the Gateway was powered on.
- **Time Zone** Set your local time zone in this field. If your region participates in Daylight Savings Time (DST), check the box next to **Daylight Savings Time**.
- **LAN IP Address and Subnet Mask** The values for the Gateway's IP Address and Subnet Mask as seen on the internal LAN are shown here. The default values are **192.168.1.1** for the Device IP Address and **255.255.255.0** for the Subnet Mask.
- **Virtual Circuit ID** 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.

VPI Enter the number provided by your ISP. The number will be in the range of 0 to 255.

VCI Enter the number provided by your ISP. The number will be in the range of 0 to 65535.

The screenshot shows the Linksys Setup page with the following fields and values:

- Host Name: (Empty)
- Domain Name: (Empty)
- Firmware Version: V3.40(G8.0)c0 | 03/11/2002
- Current Time: 00 : 01
- Time Zone: [(GMT) Greenwich Mean Time - Dublin, Edinburgh, Lisbon, London]
- Daylight Savings Time:
- LAN IP Address: 192.168.1.1 (Device IP Address)
- Subnet Mask: 255.255.255.0 (Subnet Mask)
- Virtual Circuit ID: VPI: 0 (Range: 0-255, *0); VCI: 35 (Range: 0-65535, *35)
- Encapsulation: RFC1483 Bridged
- Multiplexing: LLC; VC
- WAN IP Address: Dynamic IP Address

Figure 6-4



Note: The screen you see may vary depending on what kind of connection mode you select.

- **Encapsulation** The Gateway supports five encapsulation modes: **RFC 1483 Bridged**, **RFC 1483 Routed**, **RFC 2364 PPPoA**, **RFC2516 PPPoE**, and **Bridged Mode Only**. These modes can be selected from the drop-down menu next to the **Encapsulation** setting. Each Setup screen and available features will differ depending on what kind of connection mode you select. Each mode is described on the following pages.
- **Multiplexing** The Gateway supports both VC and LLC multiplexing. Your ISP will provide the correct selection for this setting.



Note: After setup, you can test and see if the settings are correct by successfully connecting to the Internet.

RFC 1483 Bridged

This mode supports two additional mode selections in the drop-down menu for the WAN IP Address setting, Dynamic IP Address and Static IP Address. The Setup screen and features displayed will differ depending on which mode you select.

Dynamic IP Address Choose this option if your ISP assigns IP addresses via DHCP.

Figure 6-5

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button. For more information on this tab, you can click the **Help** button.

Static IP Address Choose this option if your ISP provided you with the following information: IP Address, Default Gateway Address, and DNS Server Address(es).

1. Enter the **IP address** provided by the ISP in the Specify an IP Address field.
2. Enter the **Default Gateway Address** in the Default Gateway Address field.
3. Enter the **DNS Server Address(es)** in the DNS 1 and DNS 2 fields.

Figure 6-6

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button. For more information on this tab, you can click the **Help** button.

RFC 1483 Routed

Choose this option if your ISP told you to use this mode of encapsulation. Use the IP address and DNS Server Address(es) provided by your ISP.

1. Enter the **IP address** provided by the ISP in the Specify an IP Address field.
2. Enter the **DNS Server Address(es)** in the DNS 1 and DNS 2 fields.

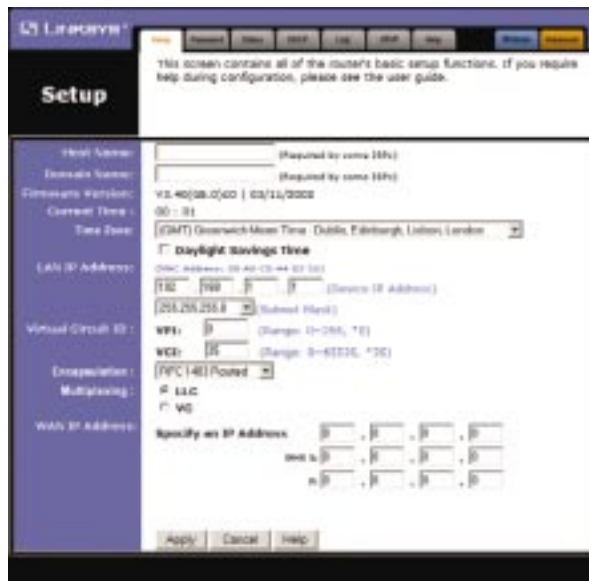


Figure 6-7

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button. For more information on this tab, you can click the **Help** button.

RFC 2364 PPPoA

Choose this option if your ISP told you to use this mode of encapsulation. Use the User Name and Password provided by your ISP.

1. Enter the **User Name** in the Specify an IP Address field.
2. Enter the **Password** in the Password field.
3. Choose either **Connect on Demand** or **Keep Alive** to determine how the Gateway will maintain your Internet connection during any period of inactivity. If you have been disconnected due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. You can configure the Gateway to cut your connection with your ISP after a specific period of time (Max Idle Time). The Keep Alive option keeps your Internet Access connected indefinitely, even when it sits idle.

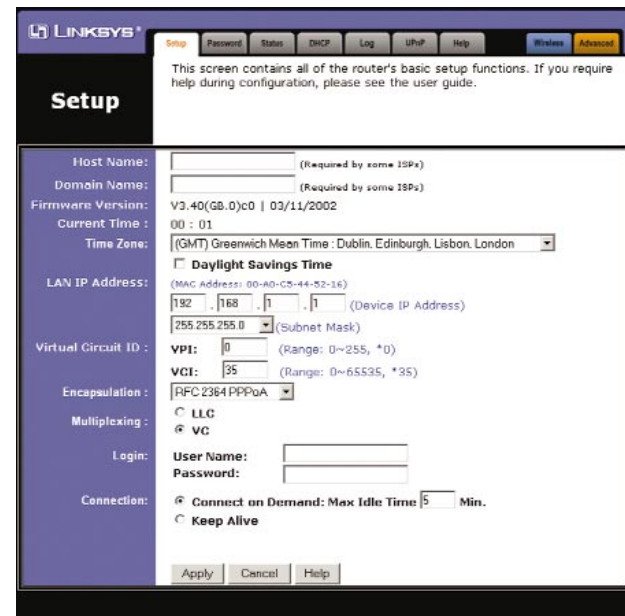


Figure 6-8

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button. For more information on this tab, you can click the **Help** button.

RFC 2516 PPPoE

Choose this option if your ISP told you to use this mode of encapsulation. Use the User Name, Password, and Service Name (if applicable) provided by your ISP.



Figure 6-9

1. Enter the **Service Name** (if provided) in the field.
2. Enter the **User Name** in the Specify an IP Address field.
3. Enter the **Password** in the Password field.
4. Choose either **Connect on Demand** or **Keep Alive** to determine how the Gateway will maintain your Internet connection during any period of inactivity. If you have been disconnected due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. You can configure the Gateway to cut your connection with your ISP after a specified period of time (Max Idle Time). The Keep Alive option keeps your Internet access connected indefinitely, even when it sits idle.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button. For more information on this tab, you can click the **Help** button.

Bridged Mode Only

Choose this option if your ISP told you to use this mode of encapsulation. This mode is used to configure the Gateway as an RFC1483 bridge, when the Gateway's routing and NAT capabilities need to be disabled.

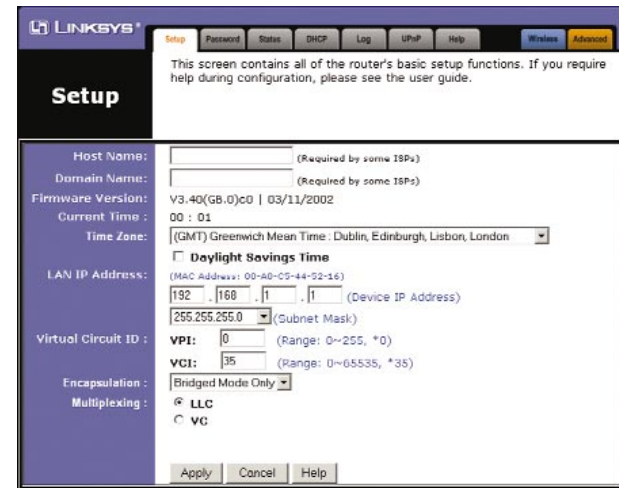


Figure 6-10

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button. For more information on this tab, you can click the **Help** button.

Password

On the Password screen, you can change the Gateway's password, configure SNMP settings, and restore the Gateway's factory default settings.

Figure 6-11

- **Router Password** It is *strongly* recommended that you set a password for the Gateway. The default password is **admin**. If you don't change the password, all users on your network will be able to access the Gateway using the default password **admin**. Re-enter the new password in the second field.
- **SNMP Get Community** Set the read-only community string for SNMP. It is strongly recommended to change this field to a name that cannot be easily guessed. The default string is **public**.
- **SNMP Set Community** Set the read/write community string for SNMP. It is strongly recommended to change this field to a name that cannot be easily guessed. The default string is **private**.
- **SNMP Trusted Host** If you enter a trusted host address here, the Gateway will only respond to SNMP messages from this IP address. If you leave the field blank (which is the default), the Gateway will respond to all SNMP messages it receives, regardless of source.

- **SNMP Trap Community** Enter the password sent with each trap to the SNMP manager.
- **SNMP Trap Destination** Enter the IP address of the station that receives the SNMP traps sent by the Gateway.
- **Restore Factory Defaults** If you select the Restore Factory Defaults option and click the **Apply** button, you will clear all of the Gateway's settings.

Do not restore the factory defaults unless you are having difficulties with the Gateway and have exhausted all other troubleshooting measures. Once the Gateway is reset, you will have to re-enter all of your configuration data.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button. For more information on this tab, you can click the **Help** button.

Status

This screen displays the current status of the Gateway; it reflects the data and selections you've entered using the Setup screen and provides an option for DHCP users.



Note: The information provided and buttons available may vary depending on the Gateway's settings.

All of the information provided on this screen is read-only. To make changes, select the Setup tab.

- **Host Name** This field shows the name of the Gateway.
- **Firmware Version** This field shows the installed version and date of the firmware. Version dates are slightly more accurate than version numbers.
- **Link Status** This indicates the status of the ADSL link. It tells you if the ADSL Gateway is disconnected, attempting to connect, or connected.
- **Upstream Speed** This indicates the maximum speed at which the ADSL Gateway will transmit data.



Figure 6-12

- **Downstream Speed** This indicates the maximum speed at which the ADSL Gateway will receive data.
- **Login** This indicates the status of the PPPoA or PPPoE login (if applicable).
- **LAN** These fields display the current MAC Address, LAN IP Address, and Subnet Mask of the Gateway, as seen by users on your local area network. The status of the DHCP Server is also displayed, if applicable.
- **WAN** These fields display the WAN IP Address, WAN Subnet Mask, and WAN Default Gateway IP Address of the Gateway, as seen by external users on the Internet. The DNS (Domain Name System) IP Address field(s) show the IP address(es) of the DNS currently used by the Gateway. Multiple DNS IP settings are common. In most cases, the first available DNS entry is used.
- **DHCP Clients Table** Click the **DHCP Clients Table** button to view the list of PCs that were given IP addresses by the Gateway.

DHCP

The Gateway can be set up as a DHCP (Dynamic Host Configuration Protocol) server on your network. A DHCP server automatically assigns an IP address to each PC on your network for you. Unless you already have one, it is highly recommended that you leave the Gateway enabled as a DHCP server.

If you choose to enable the DHCP server option, you must configure all of the PCs on your LAN to connect to a DHCP server, or to obtain their IP addresses automatically. See “Chapter 4: Configuring the PCs” for more information.

If the Gateway’s DHCP server function is disabled, you have to carefully configure the IP address, Subnet Mask and DNS settings of every computer on your network. Do not assign the same IP address to more than one computer.



Figure 6-13

- **DHCP Server** DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Gateway’s DHCP option to **Disable**.
- **Starting IP Address** Enter a value for the DHCP server to start with when issuing IP addresses.

- **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.

- **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 all network clients using the DHCP server. (This data is stored in temporary memory and changes periodically.)

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you’ve entered on any page, click the **Cancel** button. For more information on this tab, you can click the **Help** button.

Log

The Log tab provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.



Figure 6-14

- **Access Log** To log incoming and outgoing traffic, select the **Enable** option next to Access Log. This function can be disabled by clicking the **Disable** radio button.
- **Send Log to** The log can be forwarded to the IP address of a specific computer.
- **Incoming Access Log and Outgoing Access Log** With logging enabled, you can choose to view temporary logs. Temporary logs can be accessed from the Log screen by clicking either the **Incoming Access Log** or **Outgoing Access Log** button. The Incoming Access Log is a log of all the Internet traffic entering the Gateway on the ADSL side. The Outgoing Access Log is a log of all traffic entering the Gateway on the LAN side.

To clear any values you've entered on any page, click **Cancel** and re-enter information. To apply any settings you've altered on any page, click the **Apply** button. Once all settings are correct, click **Continue**. For more information on this tab, you can click the **Help** button.

UPnP



Figure 6-15

Universal Plug and Play (UPnP) allows operating systems with UPnP support to automatically detect and configure the Gateway. UPnP allows UPnP-enabled applications, such as gaming and videoconferencing, to automatically manage the Gateway. See your operating system's documentation for instructions on how to enable this feature on your system.

To clear any values you've entered on any page, click **Cancel** and re-enter information. To apply any settings you've altered on any page, click the **Apply** button. Once all settings are correct, click **Continue**. For more information on this tab, you can click the **Help** button.

Help



Figure 6-16

Under the Help tab, you'll find links to all of the Gateway's internal support documentation, including the application that upgrades the Gateway's firmware.

New firmware versions are posted at www.linksys.com and can be downloaded for free. If the Gateway can access the Internet already, there's no need to download a newer firmware version, unless that version has a new feature that you want to use. Loading new firmware onto the Gateway does not enhance the speed or the quality of your connection speed.



Note: By upgrading the Gateway's firmware, you may lose the Gateway's configuration settings.

To upgrade the Gateway's firmware:

1. Select the **Help** tab (see Figure 6-16).
2. Click **Upgrade Firmware** to display a new window (see Figure 6-17).

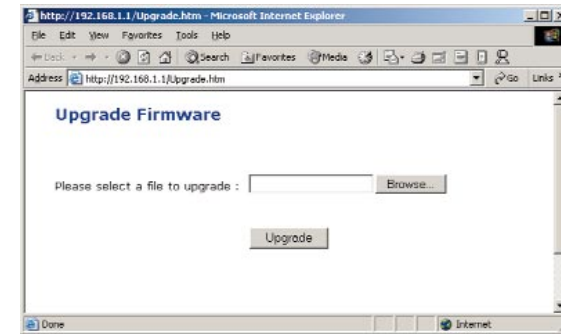


Figure 6-17

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

Wireless

Use the Wireless screen to configure the Gateway for your wireless network.



Note: You must insert the Linksys wireless PC card in the PC card slot on the back of the Gateway before you can use the wireless features.

The screenshot shows the Linksys Wireless configuration interface. At the top, it says 'WIRELESS' and provides a brief description: 'The Wireless page allows configuration of the Service Set ID (SSID), as well as setting the wireless channel number. In addition, WEP can be enabled to allow increased security for data transferred across the wireless network.' Below this, there are several configuration fields: 'SSID' is set to 'linksys'; 'Channel' is set to 5, with a note '(Channel: USA, FCC)'; 'WEP' is set to 'Disable', with a 'WEP Key Setting' button; 'RTS Threshold' is set to 2432, with a note '(range: 0-2432, *2432)'; and 'Fragmentation Threshold' is set to 2432, with a note '(range: 256-2432, *2432, even number only)'. At the bottom, there are 'Apply', 'Cancel', and 'Help' buttons. A note at the bottom left says '*: default value'.

Figure 6-18

- **SSID** The Service Set Identifier (SSID) is the unique name shared among all clients and access points in a wireless network. The SSID must be identical for all clients and access points participating in the same network. The SSID is case-sensitive and must not exceed 30 characters.

For security reasons, it is recommended that you change the SSID from the default “linksys”, and avoid common names (e.g. Company name).

- **Channel** This specifies the channel (frequency) used for the wireless network. Select the appropriate channel to correspond with your network settings, between 1 and 11 (in North America). All points in your wireless network must use the same channel in order to function correctly.
- **WEP** The WEP Encryption method is **Disabled** by default. To enable WEP, click the **Mandatory** radio button. Click the **WEP Key Setting** button to configure the WEP key settings.

On the *WEP Key Setting* screen, you can make the following choices:

- Select 64- or 128-bit WEP encryption.
- Select Passphrase generation for easy setup of encryption fields.
- Configure the manual entry of WEP encryption keys.
- Configure the default transmit WEP key.



Note: For further details on configuring wireless security using WEP, refer to “Appendix B: Configuring Wireless Security.”

- **Firmware Version** The wireless card’s firmware version is listed in this field.
- **RTS Threshold.** This value should remain at its default setting of 2432. Should you encounter inconsistent data flow, only minor modifications are recommended.
- **Fragmentation Threshold.** This value should remain at its default setting of 2432. It specifies the maximum size a data packet will be before splitting and creating a new packet. A smaller setting means smaller packets, which will create more packets for each transmission. Only minor modifications of this value are recommended.

To clear any values you’ve entered on any page, click **Cancel** and re-enter information. To apply any settings you’ve altered on any page, click the **Apply** button. Once all settings are correct, click **Continue**. For more information on this tab, you can click the **Help** button.

Advanced

The following instructions are for advanced users or users whose setup needs require special configuration. When you click the Advanced tab, you will be able to set up these features. There are seven additional tabs available.

- Filters - Block specific internal users from Internet access and enable Virtual Private Network (VPN) sessions.
- Forwarding - Sets up public services on your network.
- Dynamic Routing - Sets up the Gateway so it will automatically adjust to physical changes in the network's layout.
- Static Routing - Sets up static routes needed when network information must travel to a specific host or network.
- DMZ Host - Allows one local user to be exposed to the Internet for use of special-purpose services such as online gaming or videoconferencing.
- Firewall - Allows the Gateway to use Stateful Packet Inspection (SPI) to automatically detect and block Denial of Service (DoS) and hacking attempts.
- Link Test - Allows an advanced user or technician to perform advanced diagnostics of the ADSL Gateway and perform connectivity tests.

Filtering



Important: This is an Advanced Function. No changes should be made to this tab without a thorough understanding of network concepts.

Filters block specific internal users from accessing the Internet and enable Virtual Private Network (VPN) sessions. You can set up filters by using IP addresses, network port numbers (or a range of ports), or MAC addresses.

Figure 6-19

Setting Up Filters

- **Filtered Private IP Range** To set up a filter using IP addresses, enter the range of IP addresses you wish to filter in the IP address fields. Users who have filtered IP addresses will not be able to access the Internet at all. If you only want to filter one IP address instead of a range of IP addresses, enter the same value into both fields.

- **Filtered Private Port Range** To filter users by network port number, enter a network port number or a range of network ports. Select the protocol for each port number you want to filter, TCP or UDP. Enter the port numbers you want to filter in the port numbers fields. Users connected to the Gateway will no longer be able to access any port number listed there.

Private MAC Filter

- Click the **Edit MAC Filter Setting** button to filter users by entering their physical addresses.

In the MAC Filter Setting screen, enter the **MAC addresses** that you want to filter in the MAC address fields. The users with the filtered MAC addresses will not be able to access the Internet. Click the **Apply** button and the **Continue** button, before closing the window.

Block WAN Requests

- This feature is designed to protect users from Internet hackers and other attacks. When enabled, the Gateway will ignore both unknown TCP and ICMP packets from the WAN side. By enabling the Block WAN Request feature, you can prevent your network from being “pinged,” or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network.

Remote Management

- This feature allows you to manage or configure the Gateway from a remote location, via the Internet. To enable management through the WAN connection, click **Enable**, and use port 8080 on the remote PC you are using for remote management.

Remote Upgrade

- This feature allows you to upgrade the Gateway’s firmware from a remote location. To enable Remote Upgrade, click **Enable**.

Telnet Configuration

- This feature enables or disables telnet access to the Gateway.

To clear any values you’ve entered on any page, click **Cancel** and re-enter information. To apply any settings you’ve altered on any page, click the **Apply** button. Once all settings are correct, click **Continue**. For more information on this tab, you can click the **Help** button.

Forwarding



Important: This is an Advanced Function. No changes should be made to this tab without a thorough understanding of network concepts.

Port Range Forwarding 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 PC.

You may use this feature to establish a web server or FTP server for Internet users to access. Be sure that you enter a valid IP address; you may need to establish a static IP address with your ISP in order to properly run an Internet server. For added security, Internet users will be able to communicate with the server, but they will not actually be connected. The packets will be forwarded through the Gateway instead. If you need to forward all ports to one PC, see the “DMZ” section.

LINKSYS®

Port Range FORWARDING

Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your router, they will be redirected to the specified IP.

This page is for setting up Multiple Port only.

Customized Applications	Ext. Port	IP Address
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1
	0 To 0	192.168.1.1

Apply Cancel Help

Figure 6-20

To add a server using Port Range Forwarding:

1. Enter the **name** of the application in the appropriate Customized Applications field. This field is a description field only.
2. Next to the name of the application, enter the **range** of the external port(s) used by the server or Internet application in the Ext. Port column. Check with the Internet application software documentation for more information.
3. Enter the **IP address** of the server that you want the Internet users to be able to access. To find the IP address, go to “Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter.”
4. Configure as many entries as needed—the Gateway supports up to 11 ranges of ports. Click the **Apply** button and **Continue** button when you are done.

To delete a server entry, enter **0** in the Ext. Port and IP Address fields.

To clear any values you’ve entered on any page, click **Cancel** and re-enter information. To apply any settings you’ve altered on any page, click the **Apply** button. Once all settings are correct, click **Continue**. For more information on this tab, you can click the **Help** button.

Dynamic Routing



Important: This is an Advanced Function. No changes should be made to this tab without a thorough understanding of network concepts.

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 routers on the network. Select the RIP directions and versions for the LAN and WAN sides.

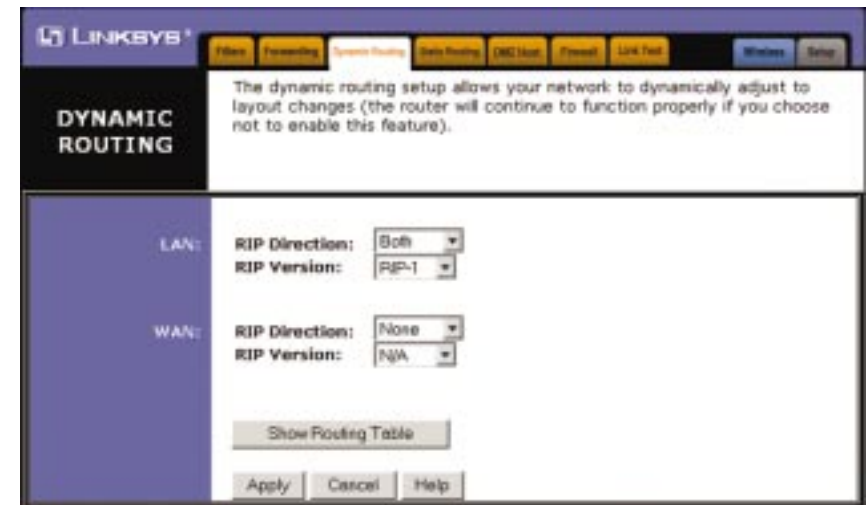


Figure 6-21

RIP Direction

Determines the direction that RIP routes will be updated.

- **None** RIP is disabled.
- **Both** The Gateway will incorporate received RIP information and send out updated RIP information.
- **In Only** The Gateway will only incorporate received RIP information.
- **Out Only** The Gateway will only send out RIP information.

RIP Version

Select the version of IP you want to use.

- **RIP-1** Routing data will be sent in RIPv1 format.
- **RIP-2B** Routing data will be sent in RIPv2 format using subnet broadcasting.
- **RIP-2M** Routing data will be sent in RIPv2 format using multicasting.
- **N/A** Routing data will not be sent.

Click the **Show Routing Table** button to open a chart displaying how data is routed through your LAN.

When finished making your changes on this tab, click the **Apply** button followed by the **Continue** button to save these changes, or click the **Cancel** button to undo your changes. For further help on this tab, click the **Help** button.

Static Routing

Important: This is an Advanced Function. No changes should be made to this tab without a thorough understanding of network concepts.

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. You can use static routing to allow different IP domain users to access the Internet through the Gateway.

The Gateway is also capable of dynamic routing (see the Dynamic Routing tab). It is usually better to use dynamic routing because it allows the Gateway to automatically adjust to physical changes in the network's layout.

To set up static routing, you should add routing entries in the Gateway's table, so the Gateway knows where to send all incoming packets.

Figure 6-22

To create a static route entry:

1. Select a **Static Route Entry** from the drop-down list. The Gateway supports up to eight static route entries.

2. Enter the following data to create a new static route.

Destination LAN IP: The Destination LAN IP is the address of the remote network or host to which you want to assign a static route. Enter the **IP address** of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP, while the last field should be 0.

Subnet Mask: The Subnet Mask (also known as the Network Mask) identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0.

Gateway IP: 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.

Hop Count: This determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network, such as PCs, print servers, routers, etc.

From the Static Routing tab, click the **Show Routing Table** button to view the current static routing configuration.

To delete a Static Routing entry, select an **entry**, and click the **Delete This Entry** button.

When finished making your changes on this tab, click the **Apply** button followed by the **Continue** button to save these changes, or click the **Cancel** button to undo your changes. For further help on this tab, click the **Help** button.

DMZ Host



Important: This is an Advanced Function. No changes should be made to this tab without a thorough understanding of network concepts.

The DMZ Hosting function allows for a server attached to Port 4 of the Gateway to be fully accessible from the Internet. The Gateway supports an Advanced form of DMZ, allowing the system attached to Port 4 to be on a secure subnet, separate from the computers attached to the other 3 ports.

Port 4 Status Selecting **DMZ** enables the advanced DMZ function for the switched Port 4. Selecting **LAN** disables the advanced DMZ function, and Port 4 acts as a normal switched port.

DMZ IP Address Enter the **IP Address** that is assigned to the Gateway's Port 4. Enter the **Subnet Mask** associated with the DMZ network.

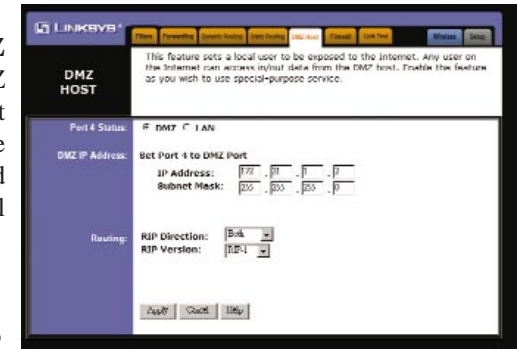


Figure 6-23

Routing This setting is only applicable to the DMZ network.

RIP Direction Determines the direction that RIP routes will be updated.


- **None** RIP is disabled.
- **Both** The Gateway will incorporate received RIP information and send out updated RIP information.
- **In Only** The Gateway will only incorporate received RIP information.
- **Out Only** The Gateway will only send out RIP information.

RIP Version Select the version of IP you want to use.

- **RIP-1** Routing data will be sent in RIPv1 format.
- **RIP-2B** Routing data will be sent in RIPv2 format using subnet broadcasting.
- **RIP-2M** Routing data will be sent in RIPv2 format using multicasting.
- **N/A** Routing data will not be sent.

When finished making your changes on this tab, click the **Apply** button followed by the **Continue** button to save these changes, or click the **Cancel** button to undo your changes. For further help on this tab, click the **Help** button.

Firewall

 **Important:** This is an Advanced Function. No changes should be made to this tab without a thorough understanding of network concepts.

The Firewall screen allows you to enable the advanced firewall functions of the Gateway, so it can use Stateful Packet Inspection (SPI) to automatically detect and block Denial of Service (DoS) and hacker attacks. Also, you can enable the Gateway to maintain a security log, which can be viewed by clicking the Show Firewall Log Table button. The security log can also be e-mailed to a specific address, whose information should be entered in the Address Info setting.




Figure 6-24

- **Firewall Service** Enable or disable the advanced firewall functions.
- **Address Info** You can specify that the security log be e-mailed to a specific address by completing the Mail Server, Mail Subject, Email Alert To, and Return Address fields.
- **Log Timer** Depending on how often you want the security log e-mailed, complete the Log Schedule, Day for Sending Alerts, and/or Time for Sending Alerts fields.

Click the **Show Firewall Log Table** button to view the security log.

When finished making your changes on this tab, click the **Apply** button followed by the **Continue** button to save these changes, or click the **Cancel** button to undo your changes. For further help on this tab, click the **Help** button.

Link Test

 **Important:** This is an Advanced Function. No changes should be made to this tab without a thorough understanding of network concepts.

The Link Test page allows an advanced user or technician to perform advanced diagnostics of the ADSL Gateway and perform connectivity tests.

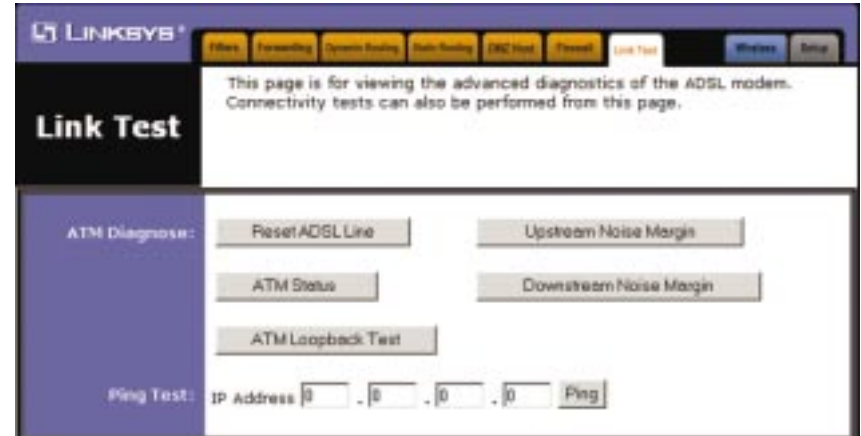


Figure 6-25

The information provided by these tests is not discussed in this document.

Appendix A: Troubleshooting

Common Problems and Solutions

This section provides possible solutions to problems regarding the Gateway's installation and operation. If your situation is described here, the problem should be solved by applying the corresponding solution. If you can't find an answer here, check the Linksys website at www.linksys.com.

1. The Gateway is not working.
 - Verify that the Power cord and other network cables are plugged in.
 - Check the LAN and WAN LEDs on the Gateway's front and verify that they are lit appropriately.
 - Check the settings on your PC.
 - Check the Gateway's settings.
2. I can't connect to the Gateway.
 - Verify that the Gateway is properly installed; LAN connections are OK, and it is powered ON.
 - Make sure that your PC and the Gateway are on the same network segment. If you are not sure, initiate the DHCP function, and let the PC get the IP address automatically.
 - Make sure that your PC is using an IP address within the default range of 192.168.1.2 to 192.168.1.254 and thus compatible with the Gateway default IP Address of 192.168.1.1
 - Also, the Subnet Mask should be set to 255.255.255.0 to match the Gateway. For the Gateway, you can check these settings by using Control Panel-Network to check the Properties for the TCP/IP protocol.
3. The Diag LED stays lit when it shouldn't.
 - The Diag LED lights up when the device is first powered up. Meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED turns off to show the system is working fine. If the LED remains lit after this time, the device is not working properly. Try to re-flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware again. If that doesn't help, contact your dealer for further inspection.
4. The ADSL Link LED will not go solid.
 - Verify that the RJ-11 cable is firmly plugged into the ADSL jack of the Gateway, with the other end plugged directly into the ADSL wall jack.

Make sure that you do NOT have a microfilter plugged in between the Gateway and the wall jack. Verify that your ADSL account is active with your ISP.

5. I can't browse through the Gateway.
 - Check if both ends of the network cable and power adapter are properly connected. Check if the status LEDs on the front panel are functioning properly.
 - If using Windows 95, 98 or Millennium, check the TCP/IP setup on the client side. Run **winiipcfg** by clicking on the **Start** button, selecting **Run**, and typing **winiipcfg** in the Run field. Press **Enter**. The PC should have an IP address of 192.168.1.xxx ("xxx" is from 2 to 254.). The Subnet Mask is 255.255.255.0; the default gateway IP should be the Gateway's IP Address, and check that the DNS is correct.
 - Check the same setup values in the Gateway's Status page.
6. When I enter a URL or IP address, I get a time out error.
 - Check to see if your other PCs work. If they do, verify that your PC's IP settings are correct (IP address, Subnet Mask, Default Gateway, and DNS)
 - If the PCs are configured correctly, but still not working, check the Gateway. Make sure that it is connected and ON. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
 - If the Gateway is configured correctly, check your Internet connection to see that it is working correctly.
 - Manually configure the TCP/IP with a DNS address provided by your ISP.
7. I can't obtain an IP address from my ADSL line.
 - Verify that all of your cabling is properly connected and that all of the Gateway's ADSL and Link LEDs are correctly illuminated.
 - Power down your Gateway for a few seconds. Turn it back on. After the Gateway goes through its self-test, check to see if you now have an IP address.
 - Verify that the VPI/VCI and Encapsulation settings are correct in the Setup page of the Web-based Utility. Go to the **Setup** section of the Web-based Utility chapter for more information.
 - If you are configured for PPPoE or PPPoA, verify that the username and password are entered correctly in the Setup page of the Web-based Utility. Go to the **Setup** section of the Web-based Utility chapter for more information.

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 Pass-Through supported by the Gateway? Yes, it is a built-in feature that the Gateway automatically enables.

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

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

Does the Gateway support any operating system other than Windows 95, Windows 98, Windows 2000, Windows NT, or Windows XP? Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

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

How do I get Napster to work with the Gateway? Napster is fully compatible with the Gateway, but you must make sure that, during installation, you select “no idea” when asked about your firewall selection. Set your proxy settings to “No Proxy Server” in your *File>Preferences*.

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

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

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

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

If all else fails in the installation, what can I do? Reset the Gateway by holding down the reset button until the Diag LED fully turns on and off. Obtain and flash the latest firmware release that is readily available on the Linksys website, www.linksys.com.

How will I be notified of new Gateway firmware upgrades? All Linksys firmware upgrades are posted on the Linksys website at www.linksys.com, where they can be downloaded for free. The Gateway's firmware can be upgraded with TFTP programs.

Will the Gateway function in a Macintosh environment? Yes, but the Gateway's setup pages are accessible only through Internet Explorer v4.0 or Netscape Navigator v4.0 or higher for Macintosh. NOTE: Linksys does not provide technical support for Macintosh computers.

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

Does the Gateway do Stateful Packet Inspection? Yes. Enable the Firewall function of the Gateway.

I am not able to access the Gateway's web configuration screen. What can I do? You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation.

What is DMZ? 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.

If DMZ 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.

Will the Gateway allow me to use my own public IPs and Domain, or do I have to use the IPs provided by the Gateway? The Gateway allows for customization of your public IPs and Domain.

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

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

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

Does Linksys provide syslog support? No, Linksys does not currently provide syslog support.

How can I check whether I have static or dynamic IP Addresses? Consult your ISP to confirm the information.

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

Can I guess my encapsulation type and VPI/VCI? These settings are dependent on your telephone company, ADSL ISP, service level, and when your line was installed. It is typically not something that can be guessed or found through trial and error. It is best to contact your ISP to find these settings.

Will this product work on an SDSL, IDSL or ISDN line? No, those types of lines are not ADSL technologies. The BEFDSR41W will only work on ADSL lines that support the T1.413i2, G.992.1 (G.dmt), or G.992.2 (G.lite) standards.

If your questions are not addressed here, refer to the contact information on the last page of this manual, or online at support.linksys.com.

Appendix B: Configuring Wireless Security



Note: WEP Encryption is an additional data security measure and not essential for Gateway operation.

An acronym for Wired Equivalent Privacy, WEP is an encryption scheme used to protect your wireless data communications. WEP uses a combination of 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode a data transmission, each point in a network must use an identical 64-bit or 128-bit key. Higher encryption levels mean higher levels of security, but due to the complexity of the encryption, they may mean decreased network performance.

You may also have heard the term “40-bit” used in conjunction with WEP Encryption. This is simply another term for 64-bit WEP encryption. This level of WEP encryption has been called 40-bit because it uses a 40-bit secret key along with a 24-bit Initialization Vector ($40 + 24 = 64$). Wireless vendors may use either name. Linksys uses the term “64-bit” when referring to this level of encryption.

If possible, make sure your wireless network is functioning before attempting to configure WEP.

A 128-bit WEP encrypted wireless network will NOT communicate with a 64-bit WEP encrypted wireless network. Therefore, make sure that all of your wireless devices are using the same encryption level. All wireless devices complying with the 802.11b standard will support 64-bit WEP.

In addition to enabling WEP, Linksys also recommends the following security implementations:

- Changing the SSID from the default “linksys”
- Changing the WEP key regularly



Note: In order for WEP Encryption to be enabled, wireless functions must first be enabled. Select **Enable** under the Wireless section before proceeding.

1. At the Wireless Screen, if you choose to enable WEP Encryption, select **Mandatory** under the WEP section.
2. Press the **WEP Key Setting** button to set the WEP Encryption type and level.

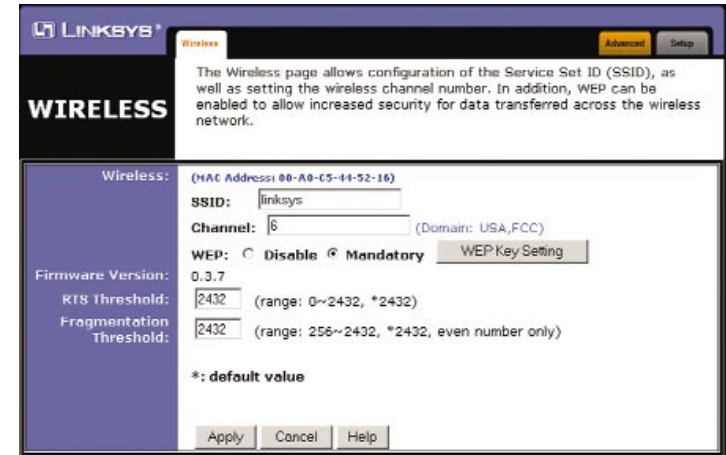


Figure B-1

3. The following screen may appear, verifying that you are enabling WEP Encryption. Press the **OK** button to continue.

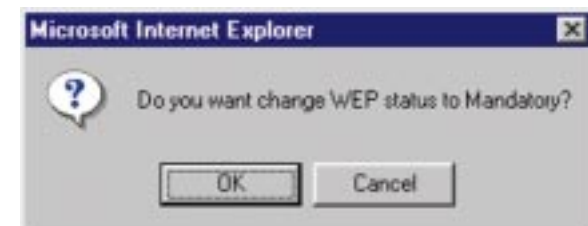


Figure B-2

4. The following screen will appear, where you will choose your WEP Encryption settings.

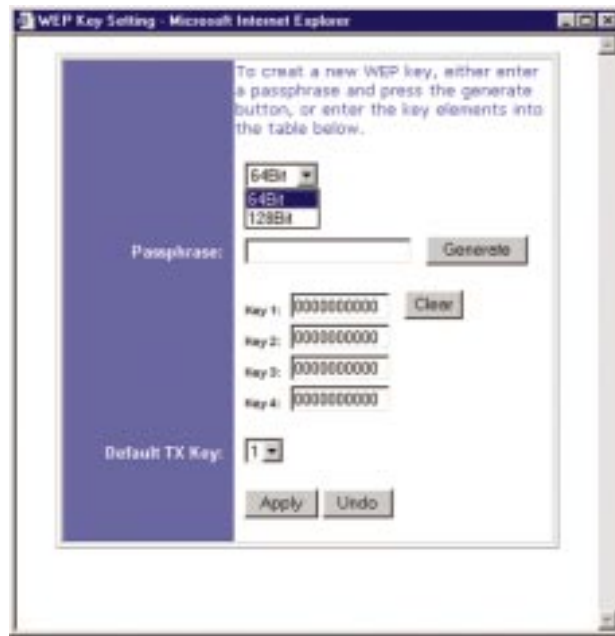


Figure B-3

- **WEP (64Bit or 128B)** Select the level of encryption from the drop-down box. 128-bit WEP encryption is unique to Linksys and may conflict with other vendors' WEP encryption.

WEP Encryption key can be generated in one of two ways:

1. You may create an encryption key by using a **Passphrase**.
 - a. Enter a Passphrase, a user-defined password, into the **Passphrase** field. The Passphrase can be a maximum of 31 letters, symbols, and numbers. No spaces can be used.
 - b. Click the **Generate** button to create a key. The key will be 10 digits if you chose 64-bit encryption, or 26 digits if you chose 128-bit encryption. This key will be used to encrypt and decrypt the data being sent between the Gateway and your network's wireless PCs.

The Key field may not display all digits. Using the mouse, click anywhere within the Key field. Move the cursor to the right to view the rest of the Key. Make sure you write down the entire Key EXACTLY the way it is displayed.

2. You may enter the encryption key manually.

Make a note of the Passphrase or Manual Key. You will need it for other wireless devices on the network, as the same WEP encryption key must be entered in all wireless devices on the network.

Once you have chosen your key encryption method and entered either the Passphrase or manual key, click the **Apply** button, and the encryption portion of the setup is complete.



Note: In order to utilize WEP encryption, all points in your wireless network must have WEP enabled and be set to the same Key Setting.



Note: In Windows XP, a 128-bit Key generated by the Gateway will be called a "104 bits (26 digits)" key, and a 64-bit Key generated by the Gateway will be called a "40 bits (10 digits)" key.

Configuring Wireless Security in Windows XP

As Windows XP does not allow for the use of the Linksys Passphrase feature with the wireless PC adapters, you will need to manually enter the key generated in the previous section.

The following steps will help you enable WEP and enter the encryption key manually for your wireless PC cards, in order to enable your Windows XP system to communicate with the Gateway wirelessly.

These steps assume that your CD-ROM drive is letter D and that you are running Windows XP in the default mode.

Be sure you have the WEP Key generated by the Gateway.

1. Click the **Start** button and go to the **Control Panel**.



Figure B-4

2. In the “Control Panel” window, click the **Network and Internet Connections** icon.



Figure B-5

3. Click on the **Network Connections** icon.

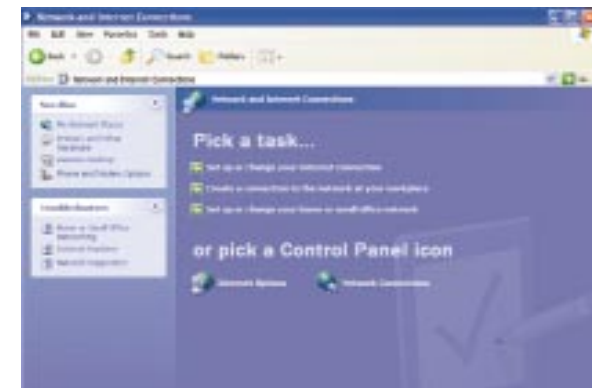


Figure B-6

4. The “Network Connections” window will appear. Under LAN or High-Speed Internet you will see all Network cards that are installed and operating in your computer. Double-click the **Wireless Network Connection** icon associated with your wireless adapter.

If the “Wireless Network Connection Status” window appears, continue to the next step.

If a “Connect to Wireless Network” window appears, in the Available Networks section, click the desired wireless network, specified by the Gateway’s SSID. Then, double-click the **Wireless Network Connection** icon.

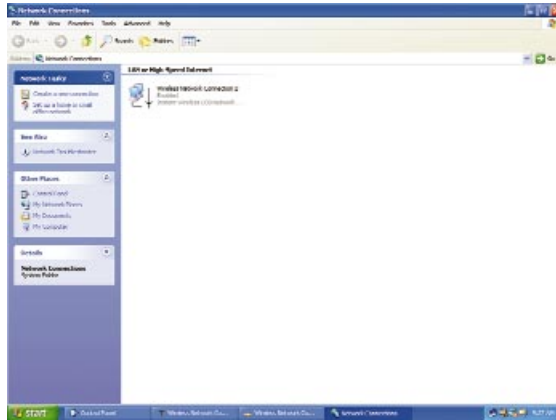


Figure B-7

- When the “Wireless Network Connection Status” window appears, click the **Properties** button.

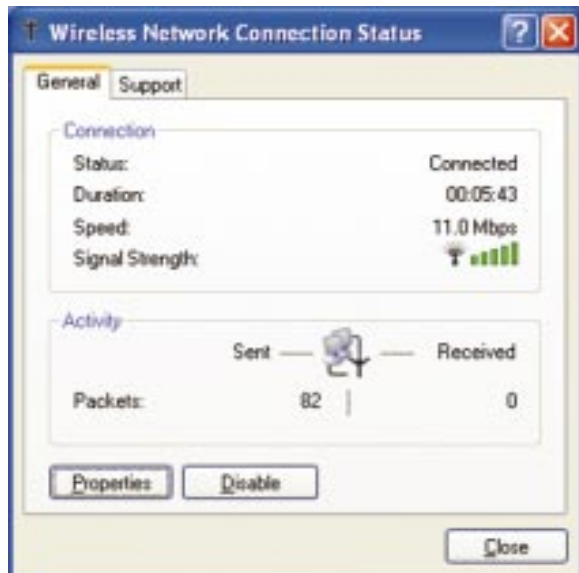


Figure B-8

- When the “Wireless Network Connection Properties” window appears, click the **Wireless Networks** Tab.

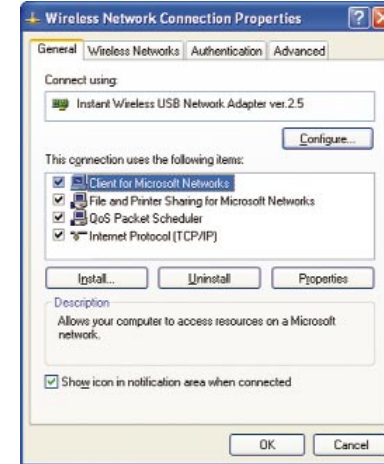


Figure B-9

- If the appropriate wireless network, specified by the Gateway’s SSID, is displayed in the “Preferred networks” section, double-click it and continue to the next step.

Otherwise, click on the appropriate wireless network, specified by the Gateway’s SSID, in the “Available networks” section. Then, click the **Configure** button.

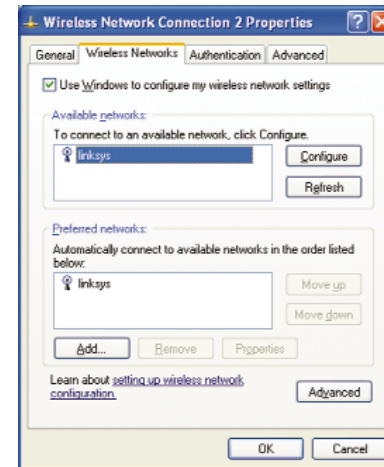


Figure B-10

8. The “Wireless Network Properties” window will appear.

Click the check box for the **Data encryption (WEP enabled)** option.

Remove the check from the **Network Authentication (Shared mode)** and **The key is provided for me automatically** fields.

In the “Network key” field, enter the exact Key (all 10 or 26 digits, depending on the level of encryption) generated by the Gateway.

Verify that the “Key format” field displays “Hexadecimal digits” and that the “Key length” field displays either “40 bits (10 digits)” or “104 bits (26 digits)”. If this is not displayed, you have entered the key incorrectly.



Figure B-11

Click the **OK** button to save the settings. Click on **OK** buttons until you get back to the “Wireless Network Connection Status” window. Close any open windows to get back to the Windows XP desktop.

Close any applications and reboot your PC. After reboot, WEP configuration is complete and you should be able to connect wirelessly to the Gateway.

Appendix C: Installing the TCP/IP Protocol

Follow these instructions to install the TCP/IP protocol on one of your PCs *only* after a network card has been successfully installed inside the PC. These instructions are for Windows 95, Windows 98, and Windows Me. For TCP/IP setup under Windows NT, 2000, and XP, see your Windows manual.

1. Click the **Start** button. Choose **Settings** and then **Control Panel**.
2. Double-click on the **Network** icon to bring up your Network window. Select the **Configuration** tab.



Figure C-1

3. Click the **Add** button.
4. Double-click on **Protocol**.
5. Highlight **Microsoft** under the list of manufacturers.

6. Find and double-click **TCP/IP** in the list to the right (see Figure C-2).

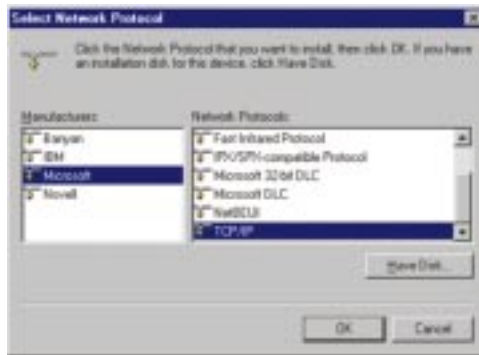


Figure C-2

7. After a few seconds, the main Network window will appear. The TCP/IP Protocol should now be listed.



Figure C-3

8. Click the **OK** button. Windows may ask for original Windows installation files. Supply them as needed, e.g., c:\windows\options\cabs, D:\win98, D:\win95.
9. Windows will ask you to restart the PC. Click the **Yes** button.

The TCP/IP installation is now complete.

Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your Ethernet adapter to do either MAC Filtering for the Gateway and ISP. You can also find the IP address of your computer's Ethernet adapter. The IP address is used for filtering. Follow the steps in this appendix to find the MAC address or IP address for your adapter in Windows 95, 98, Me, NT, 2000, and XP.

For Windows 95, 98, and Me:

1. Click on **Start** and **Run**. In the Open field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.

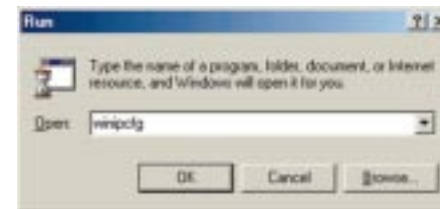


Figure D-1

2. When the IP Configuration window appears, select the Ethernet adapter you are using to connect to the Gateway via a CAT 5 Ethernet cable.

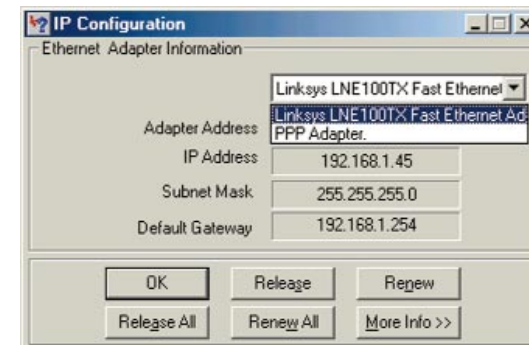


Figure D-2

- Write down the Adapter Address as shown on your computer screen (see Figure D-3). This is the MAC address for your Ethernet adapter and will be shown as a series of numbers and letters.

The MAC address/Adapter Address is what you will use for MAC Filtering.

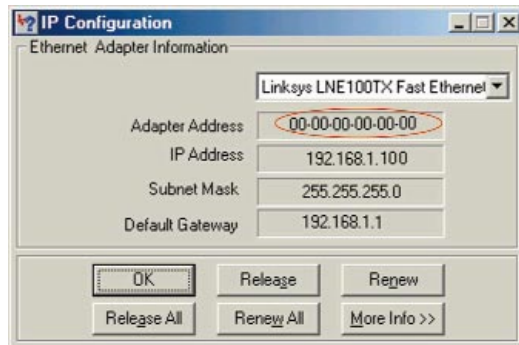


Figure D-3

The example in Figure D-3 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.



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

For Windows NT, 2000, and XP:

The following steps show an alternative way of obtaining the MAC address and IP address for your Ethernet adapter.

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



Figure D-4

- In the command prompt, enter **ipconfig /all**. Then press the **Enter** key.

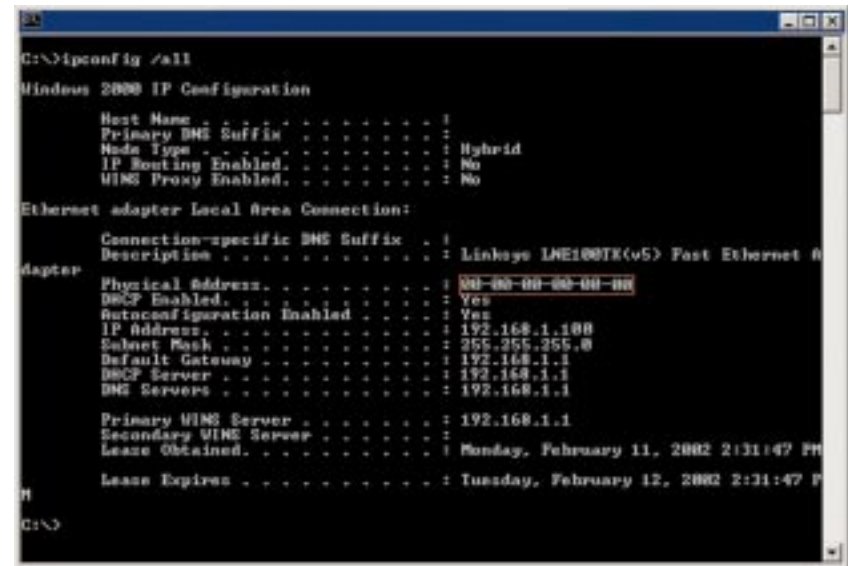


Figure D-5

- Write down the Physical Address as shown on your computer screen; it is the MAC address for your Ethernet adapter. This will appear as a series of letters and numbers.

The MAC address/Physical Address is what you will use for MAC Filtering.



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

The example in Figure D-5 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

When entering the information using the Router's web-based utility, you will type the **12-digit MAC address** in this format, XXXXXXXXXXXX *without the hyphens* for MAC Filtering.

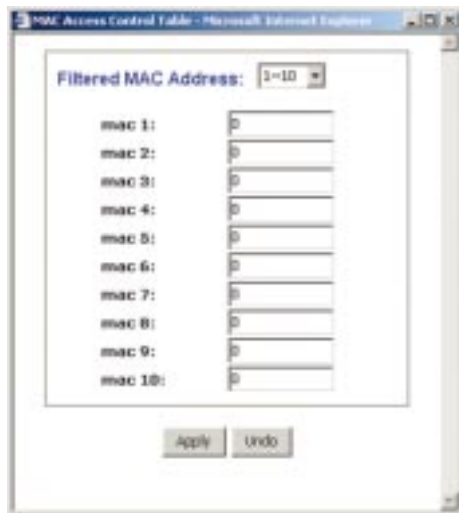


Figure D-6

Appendix E: Specifications

Standards:	ANSI T1.413i2, ITU-T G.dmt (G.992.1), ITU G.lite (G.992.2), PC Card 16-bit standard, IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), IEEE 802.11b (Wireless)*
Protocols:	RFC 1483, RFC 2364 PPPoA, RFC 2516 PPPoE
Ports/Switches/Buttons:	
ADSL:	RJ-11 ADSL Port
LAN:	Four 10/100 RJ-45 Switched Ports
PCMCIA:	Type II Slot (for use with Linksys WPC11 only)
Switch:	On/Off
Button:	Reset
Speed:	
ADSL:	8 Mbps downstream, 800 kbps upstream
LAN:	10/100 Mbps (Half/Full Duplex)
Wireless*:	Up to 11 Mbps
Cabling Type:	
ADSL:	Standard Telephone Cable
LAN:	UTP Category 5 or better
LEDs:	
ADSL:	Power, Diag Session, Link, Act
LAN:	100, Full/Col, Link/Act
WLAN:	Link, Act

* Requires Optional WPC11 (sold separately) for Wireless Connectivity

Environmental

Dimensions:	7.32" x 6.06" x 2.52" (186 mm x 154 mm x 62 mm)
Unit Weight:	14.4 oz. (0.40 kg)
Power:	External, 12V AC, 1.25 A
Certifications:	FCC Class B, Part 68, CE Mark
Operating Temp.:	0°C to 40°C (32°F to 104°F)
Storage Temp.:	0°C to 60°C (32°F to 140°F)
Operating Humidity:	10% to 85%, Non-Condensing
Storage Humidity:	10% to 90%, Non-Condensing

Appendix F: Warranty Information

BE SURE TO HAVE YOUR PROOF OF PURCHASE AND A BARCODE FROM THE PRODUCT'S PACKAGING ON HAND WHEN CALLING. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE.

IN NO EVENT SHALL LINKSYS'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS DOES NOT OFFER REFUNDS FOR ANY PRODUCT.

LINKSYS OFFERS CROSS SHIPMENTS, A FASTER PROCESS FOR PROCESSING AND RECEIVING YOUR REPLACEMENT. LINKSYS PAYS FOR UPS GROUND ONLY. ALL CUSTOMERS LOCATED OUTSIDE OF THE UNITED STATES OF AMERICA AND CANADA SHALL BE HELD RESPONSIBLE FOR SHIPPING AND HANDLING CHARGES. PLEASE CALL LINKSYS FOR MORE DETAILS.

Appendix G: Contact Information

For help with the installation or operation of your ADSL Gateway with Modem / Router / 4-Port Switch / Wireless-Ready, contact Linksys Technical Support at one of the phone numbers or Internet addresses below.

Sales Information	800-546-5797 (1-800-LINKSYS)
Technical Support	800-326-7114 (toll free from U.S. or Canada) 949-271-5465 (6:00 am to 5:00 pm PST)
RMA Issues	949-271-5461
Fax	949-265-6655
Email	support@linksys.com
Web site	http://www.linksys.com http://support.linksys.com
FTP site	ftp://ftp.linksys.com



www.linksys.com

© Copyright 2002 Linksys, All Rights Reserved.