LINKSYS®

A Division of Cisco Systems, Inc.

2.4 GHz 54Mbps

Wireless-G

VPN Router

User Guide

WIRELESS

Model No. **WRV54G**

CISCO SYSTEMS

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Wireless-G is the upcoming 54Mbps wireless networking standard that's almost five times faster than the widely deployed Wireless-B (802.11b) products found in homes, businesses, and public wireless hotspots around the country—but since they share the same 2.4GHz radio band, Wireless-G devices can also interoperate with existing 11Mbps Wireless-B equipment.

Since both standards are built in, you can protect your investment in existing 802.11b infrastructure, and migrate to the new screaming fast Wireless-G standard as your needs grow.

The Linksys Wireless-G Broadband VPN Router is really three devices in one box. First, there's the Wireless Access Point, which lets you connect Wireless-G or Wireless-B devices to the network. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices. Connect four PCs directly, or daisy-chain out to more hubs and switches to create as big a network as you need. Finally, the Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

To protect your data and privacy, the Wireless-G Broadband VPN Router can encrypt all wireless transmissions. The Router can serve as a DHCP Server, has NAT technology to protect against Internet intruders, supports VPN pass-through, and can be configured to filter internal users' access to the Internet. Configuration is a snap with the web browser-based configuration utility.

With the Linksys Wireless-G Broadband VPN Router at the center of your home or office network, you can share a high-speed Internet connection, files, printers, and multi-player games with the flexibility, speed, and security you need!

Chapter 2: Planning your Wireless Network

The Router's Functions

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

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

The Router's NAT feature protects your network of PCs so users on the public, Internet side cannot "see" your PCs. This is how your network remains private. The Router protects your network by inspecting every packet coming in through the Internet port before delivery to the appropriate PC on your network. The Router 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.

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

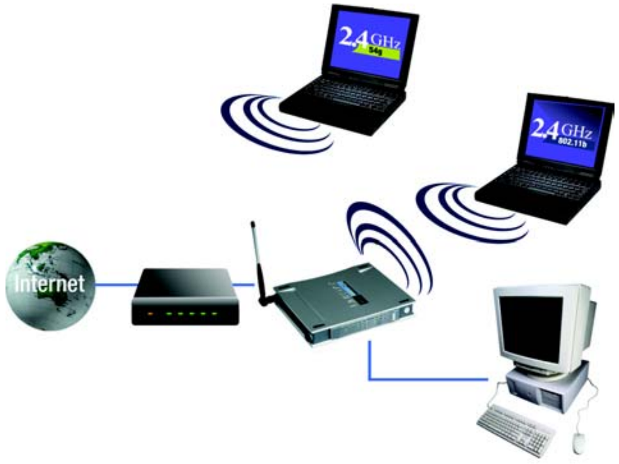


Figure 2-1: Network

IP Addresses

What's an IP Address?

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

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 must be unique and are commonly used with network devices such as server PCs or print servers.

***LAN**: the computers and networking products that make up your local network*

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

Since the Router uses NAT technology, the only IP address that can be seen from the Internet for your network is the Router's Internet IP address. However, even this Internet IP address can be blocked, so that the Router and network seem invisible to the Internet—see the Block WAN Requests description under Filters in "Chapter 6: The Router's Web-based Utility."

Chapter 6: Configuring the Router’s Basic Settings

This chapter will show you how to configure the Router to function in your network and gain access to the Internet through your Internet Service Provider (ISP). Detailed description of the Router’s web-based utility can be found in “Chapter 6: The Router’s Web-based Utility.”

The instructions from your ISP tell you how to set up your PC for Internet access. Because you are now using the Router to share Internet access among several computers, you will use the setup information to configure the Router instead of your PC. You only need to configure the Router once using the first computer you set up.

1.Open your web browser. Enter http://192.168.1.1 (the Router’s default IP address) in the web browser’s Address field. Press the Enter key.

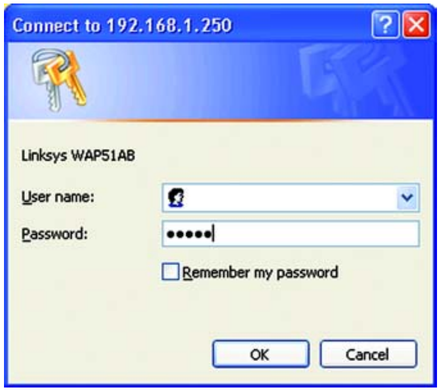
2.An Enter Network Password window, shown in Figure 5-2, will appear. (Windows XP users will see a similar screen.) Leave the User Name field empty, and enter admin in lowercase letters in the Password field (admin is the default password). Then, click the OK button.

3.The web-based utility will appear with the Setup tab selected. Select the time zone for your location. If your location experiences daylight savings, leave the checkmark in the box next to Automatically adjust clock for daylight saving changes.

4.Based on the setup instructions from your ISP, you may need to provide the Host Name and Domain Name (usually cable ISPs require them). These fields allow you to provide a host name and domain name for the Router and are usually left blank.

The values for the Router’s LAN IP Address and Subnet Mask are shown on the Setup screen. The default values are 192.168.1.1 for the IP Address and 255.255.255.0 for the Subnet Mask.

5.The Router supports four connection types: Automatic Configuration - DHCP (obtain an IP automatically), Static IP, PPPoE, and PPTP. These types are listed in the drop-down menu for the Configuration Type setting. Each Setup screen and available features will differ depending on what kind of connection type you select. Proceed to the instructions for the connection type you are using, and then continue to step 6.


Connect to 192.168.1.250

Linksys WAP51AB

User name:

Password: •••••

☐ Remember my password

Figure 6-1: Password Screen

Note: For added security, you should change the password through the Security screen of the web-based utility.

IMPORTANT: If you have previously enabled any Internet-sharing proxy server software on any of your PCs, you must disable it now. Some examples of Internet-sharing software are Internet LanBridge, Wingate, ICS, and Sygate. To disable your Internet-sharing software:

- If you are running Netscape Navigator, click Edit, Preferences, Advanced, and Proxies. Click Direct Connection to the Internet.

- If you are running Internet Explorer 5.x or higher, click Tools, Settings, Control Panel, Internet Options, Connections, and LAN Settings. Remove checkmarks from all three boxes. Click the OK button to continue.

You must also disable any Internet log-on software (such as Ivasion Winpoet or Enternet 300) and any firewall software (such as ZoneAlarm and Watchdog) on all of your PCs.

The Setup Tab

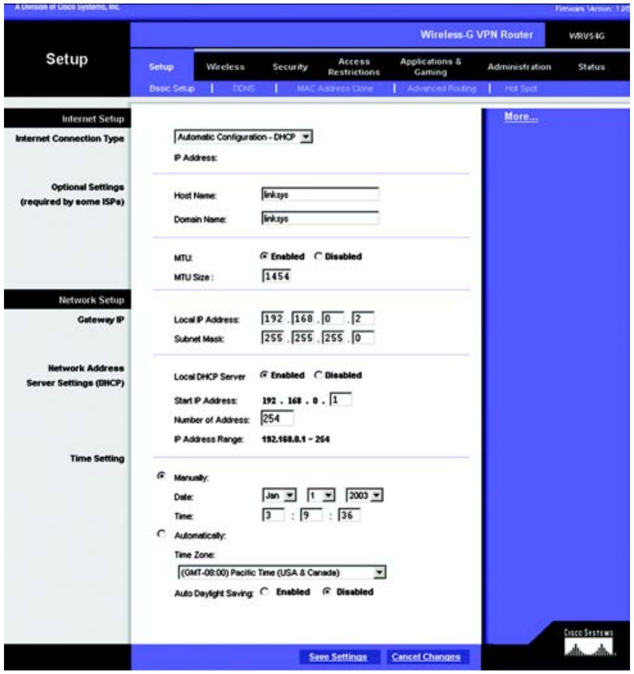
The first screen that appears displays the Setup tab. This allows you to change the Access Point's general settings. Change these settings as described here and click the **Apply** button to apply your changes or **Cancel** to cancel your changes. If you require online help, click the **Help** button.

- Firmware. This will display the Access Point's current firmware version. Firmware can be upgraded from the Help tab.
- Access Point Name. You may assign any name to the Access Point. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. Verify this is the name you wish to use and click the **Apply** button to set it.
- Static IP Address. This IP address must be unique to your network. (The default IP address is 192.168.1.250. As this is a private IP address, there is no need to purchase a separate IP address from your service provider.) Verify the address and click the **Apply** button to save changes.
- Subnet Mask. The Access Point's Subnet Mask must be the same as your Ethernet (wired) network. Verify this is correct and click the **Apply** button to set it.

5GHz/802.11a Wireless Settings

- SSID. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure that this setting is the same for all points in your wireless network.
- Channel. Select the appropriate channel from the list provided to correspond with your network settings. This should be between 36 and 64 (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 **WEP Key Setting** button. For more information on WEP and wireless security, refer to Appendix B: Wireless Security.

Click the **Apply** button to apply your changes or **Cancel** to cancel your changes. If you require online help, click the **Help** button.



Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

IP Address:

Optional Settings (required by some ISPs)

Host Name: linksys

Domain Name: linksys

MTU: ● Enabled ○ Disabled

MTU Size : 1454

Network Setup

Gateway IP

Local IP Address: 192 . 168 . 0 . 2

Subnet Mask: 255 . 255 . 255 . 0

Network Address Server Settings (DHCP)

Local DHCP Server ● Enabled ○ Disabled

Start IP Address: 192 . 168 . 0 . 1

Number of Address: 254

IP Address Range: 192.168.0.1 - 254

Time Setting

● Manually:

Date: Jan 1 2003

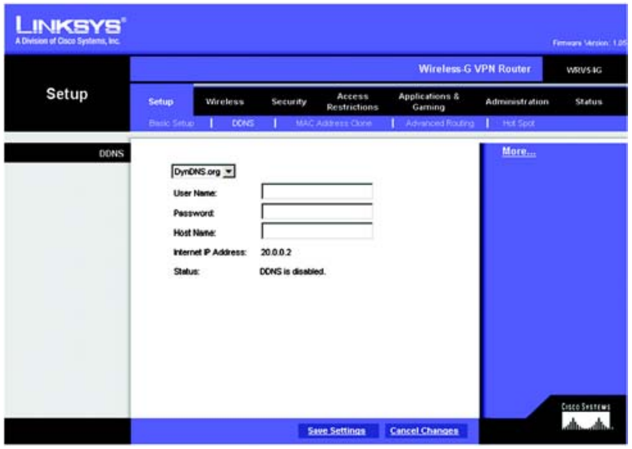
Time: 3 : 9 : 36

○ Automatically:

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

Auto Daylight Saving: ○ Enabled ● Disabled

Figure 6-2: Setup Tab



DDNS

DynDNS.org

User Name:

Password:

Host Name:

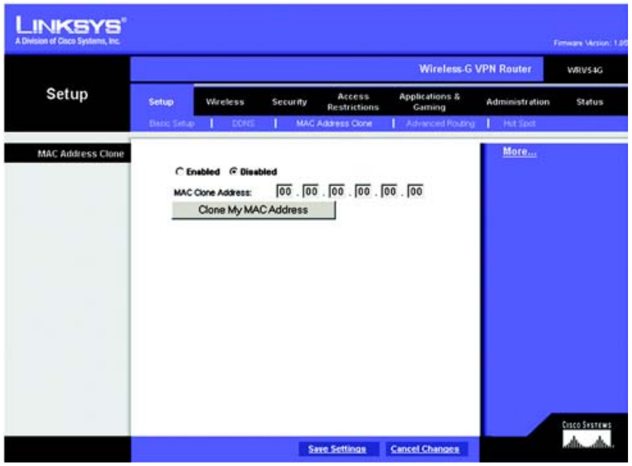
Internet IP Address: 20.0.0.2

Status: DDNS is disabled.

2.4GHz/802.11b Wireless Settings

- SSID. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.
- Channel. Select the appropriate channel from the list provided to correspond with your network settings. This should be 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 WEP Key Setting button. For more information on WEP and wireless security, refer to Appendix B: Wireless Security.

Click the Apply button to apply your changes or Cancel to cancel your changes. If you require online help, click the Help button.



○ Enabled ● Disabled

MAC Clone Address: 00 . 00 . 00 . 00 . 00 . 00

Figure 6-3: 802.11b Wireless Settings

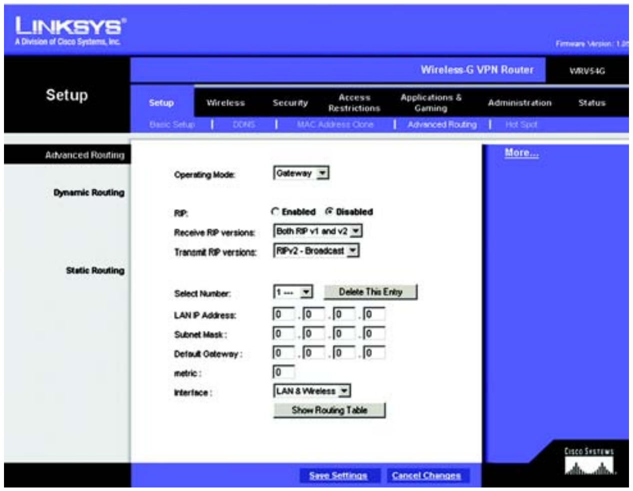
The Password Tab

The Password tab allows you to change the Access Point's password and restore factory defaults.

Changing the sign-on password for the Access Point is as easy as typing the password into the AP Password field. Then, type it again into the second field to confirm.

To restore the Access Point's factory default settings, click the Yes button beside Restore Factory Defaults.

Click the Apply button to apply your changes or Cancel to cancel your changes. If you require online help, click the Help button.



Operating Mode: Gateway

RIP: ○ Enabled ● Disabled

Receive RIP versions: Both RIP v1 and v2

Transmit RIP versions: RIPv2 - Broadcast

Select Number: 1 ---

LAN IP Address: 0 . 0 . 0 . 0

Subnet Mask : 0 . 0 . 0 . 0

Default Gateway : 0 . 0 . 0 . 0

metric : 0

Interface : LAN & Wireless

Figure 6-4: Password Tab

The Status Tab

The Status tab will display current information on the Access Point, its settings and performance.

- Firmware Version. This displays the current version of the Access Point's firmware. Firmware should only be upgraded if you experience problems with the Access Point and can be upgraded from the Help tab.
- IP Address. This IP address is the unique address to your network.
- Subnet Mask. This is the Access Point's Subnet Mask, which is the same as that on your Ethernet network.
- SSID. The SSID is the unique name shared among all points in a wireless network.
- Encryption Function. The encryption method you chose in the Setup Wizard or changed from the Setup tab of this Web-based Utility is displayed here.
- Channel. This is the channel at which your wireless network broadcasts. All points in your wireless network must use the same channel in order to function correctly.

Figure 6-5: Status Tab

The Help Tab

For help on the various tabs in this Web-based Utility, along with upgrading the Access Point's firmware and viewing this Guide, click the Help tab.

The help files for the various tabs in this Web-based Utility are listed by tab name on the left-hand side of the screen.

The following resources require an Internet connection in order to access them.

Click the Linksys Website link to connect to the Linksys homepage for Knowledgebase help files and information about other Linksys products.

For an Online Manual in PDF format, click that text link. The manual will appear in Adobe pdf format. If you do not have the Adobe PDF Reader installed on your computer, click the Adobe Website link to download this software.

Firmware can be upgraded by clicking the Upgrade Firmware link. Do not upgrade your firmware unless you are experiencing problems with the Access Point. For more information about upgrading firmware, refer to Appendix C: Upgrading Firmware.

IMPORTANT: Restoring the Access Point's factory default settings will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.), and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings.

Figure 6-6: Help Tab

The Filter Tab

The Filter tab allows you to block and allow certain computers, by their MAC Address, from communicating with the Access Point.

To enable filtering of computers by their MAC Addresses, click the Enable radio button. To disable this feature, click the radio button by Disable.

Type the MAC Addresses for those PCs you wish to allow access to the Access Point in the MAC Address fields. As long as Filtering is enabled, PCs with MAC Addresses not entered in the MAC Address field will not be allowed to communicate with the Access Point.

When you've completed making any changes on this tab, click the Apply button to save those changes or Cancel to exit the Web-based Utility without saving changes. To clear any of the information you've typed by not yet applied, click the Clear button. For more information on this tab, you can click the Help button.

Figure 6-7: Filter Tab

The Wireless Tab

Before making any changes to the Wireless tab, please check your wireless settings on other systems, as these changes will alter the effectiveness of the Access Point. In most cases, these settings do not need to be changed.

- Beacon Interval. This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).
- RTS Threshold. This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2,346. Should you encounter inconsistent data flow, only minor modifications are recommended.
- Fragmentation Length. This specifies the maximum size a data packet will be before splitting and creating a new packet and should remain at its default setting of 2,346. A smaller setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.
- Data Beacon Rate. (5GHz/802.11a only) This value, between 1 and 16384, indicates the interval of the Delivery Traffic Indication Message. A Data Beacon Rate field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next message with a rate value. Access Point Clients hear the beacons and awaken to receive the broadcast and multicast messages.
- Turbo Mode. (5GHz/802.11a only) Click the radio button beside Enable to increase the speed of your wireless transmissions to 72 Mbps, keeping in mind that the Access Point's range diminishes in Turbo Mode. If you do not wish to utilize Turbo Mode, make sure the radio button beside Disable is selected.
- DTIM Interval. (2.4GHz/802.11b only) This value indicates how often the Access Point sends out a Delivery Traffic Indication Message. Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions.
- Transmission Rates. The basic transfer rates should be set depending on the speed of your wireless network. You can select from a range of transmission speeds or select Best to have the Access Point automatically engage the network's optimum speed.

Figure 6-8: Wireless Tab

- Preamble Type. (2.4GHz/802.11b only) The preamble synchronizes network traffic for more efficient communication. Small networks benefit most from Short preambles. Large networks benefit from Long preambles. All points in your wireless network must be set to the same preamble type.

- Authentication Type. You may choose between Open System or Shared Key. The Authentication Type default is set to Open System, in which the sender and the recipient do NOT share a secret key. Each party generates its own key-pair and asks the receiver to accept the randomly generated key. Once accepted, this key is used for a short time only. Then a new key is generated and agreed upon. Shared Key is when both the sender and the recipient share a secret key.

When you've completed making any changes on this tab, click the Apply button to save those changes or Cancel to exit the Web-based Utility without saving changes. For more information on this tab, you can click the Help button.

Figure 6-9:

Figure 6-10:

Figure 6-11:

Figure 6-12:

Figure 6-13:

Figure 6-14:

Figure 6-15:

Chapter 5: Configuring the PCs

Overview

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

To do this, you need to configure your PC’s network settings to obtain an IP (or TCP/IP) address automatically, so your PC can function as a DHCP client. Computers use IP addresses to communicate with the Router and each other across a network, such as the Internet.

First, find out which Windows operating system your computer is running. You can find out by clicking the **Start** button. Read the side panel of the Start menu to find out which operating system your PC is running.

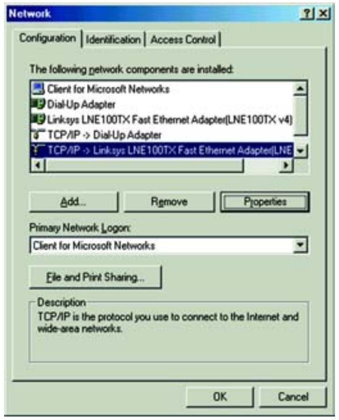
You may need to do this for each computer you are connecting to the Router.

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. Make sure that an Ethernet or wireless adapter (also known as a network adapter) has been successfully installed in each PC you will configure. Once you’ve configured your computers, continue to “Chapter 5: Configure the Router’s Basic Settings.”

Configuring Windows 98 and Millennium PCs

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. 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. Click the **Properties** button.

IMPORTANT: Important: By default Windows 98, 2000, Me, and XP has TCP/IP installed and set to obtain an IP address automatically. If your PC does not have TCP/IP installed, click Start and then Help. Search for the keyword TCP/IP. Then follow the instructions to install TCP/IP.



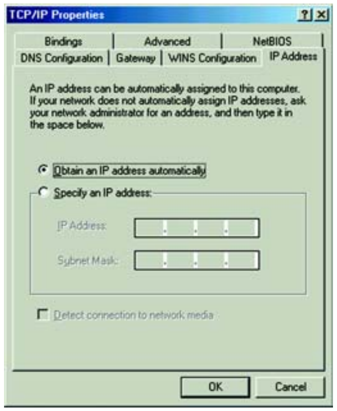
The following network components are installed:

- Client for Microsoft Networks
- Dial-Up Adapter
- Linksys LNE100TX Fast Ethernet Adapter(LNE100TX v4)
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Linksys LNE100TX Fast Ethernet Adapter(LNE

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Figure 5-1: Welcome



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically
○ Specify an IP address:
IP Address: . . .
Subnet Mask: . . .

□ Detect connection to network media

Figure 5-2: Connecting

Chapter 4: Connecting the Wireless-G Broadband Router

Overview

The Router's setup consists of more than simply plugging hardware together. You will have to configure your networked PCs to accept the IP addresses that the Router assigns them (if applicable), and you will also have to configure the Router with setting(s) provided by your Internet Service Provider (ISP).

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

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

If you want to use a PC with an Ethernet adapter to configure the Router, go to "Wired Connection to a PC." If you want to use a PC with a wireless adapter to configure the Router, go to "Wireless Connection to a PC and Boot-Up."

Wired Connection to a PC

1.Before you begin, make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.

2.Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the Router, and the other end to an Ethernet port on a PC.

Repeat this step to connect more PCs, a switch, or other network devices to the Router.

3.Connect a different Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel. This is the only port that will work for your modem connection.

4.Power on the cable or DSL modem.

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

•The Power LED on the front panel will light up green as soon as the power adapter is connected properly.

•The Diag LED will light up red for a few seconds. It will turn off when the self-test is complete. If this LED stays on for one minute or longer, see "Appendix A: Troubleshooting."

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

HAVE YOU: r.Have you checked that the Link/ Act LEDs for all your LAN connections and the Link LED for your Internet connection light up?

If all of your Link LEDs are not lighting up, make sure that all your cables are securely plugged in, and that all of your hardware is powered on properly. Verify that the modem is plugged into the Internet port on the Router.

Chapter 3: Getting to Know the Wireless-G Broadband VPN Router

The Back Panel

The Router’s ports, where a network cable is connected, are located on the back panel.

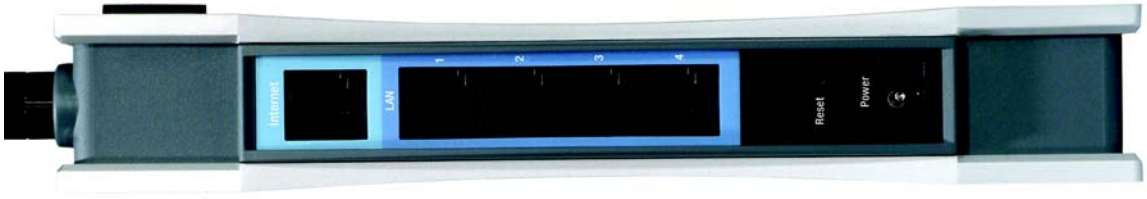


Figure 3-1: Back Panel

Important: Resetting the Access Point will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.) and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings.

Internet The **Internet** port connects to your modem.

LAN (1-4) The **LAN** (Local Area Network) ports connect to your PC and other network devices.

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

Reset Button There are two ways to Reset the Router's factory defaults. Either press the **Reset Button**, for approximately ten seconds, or restore the defaults from the Password tab in the Access Point's Web-Based Utility.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at www.linksys.com for more information about products that work with the Access Point.

The Front Panel

The Router's LEDs, where information about network activity is displayed, are located on the front panel.

Chapter 7: Configuring the Router's Web-Based Utility

Overview

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

• Basic Setup. On the Basic Setup screen, enter the settings provided by your ISP.

• Management. Click the Administration tab and then the Management tab. The Router's default password is admin. To secure the Router, change the Password from its default.

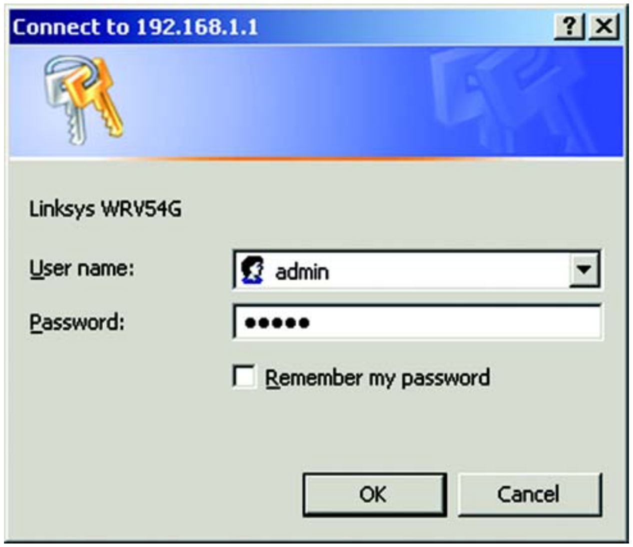
There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

Setup

- Basic Setup. Enter the Internet connection and network settings on this screen.
- DDNS. To enable the Router's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.
- MAC Address Clone. If you need to clone a MAC address onto the Router, use this screen.
- Advanced Routing. On this screen, you can alter Network Address Translation (NAT), Dynamic Routing, and Static Routing configurations.
- Hot Spot. Register your Hot Spot service provider on this screen.

Wireless

- Basic Wireless Settings. You can choose your Wireless Network Mode and Wireless Security on this screen.
- Wireless Network Access. This screen displays your network access list.



Connect to 192.168.1.1

Linksys WRV54G

User name: admin

Password: •••••

☐ Remember my password

Figure 7-1: Password Screen

Note: For added security, you should change the password through the Security screen of the web-based utility.

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

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

Security

- Filter. To block specific users from Internet access, you can set up IP address, port, and MAC address filtering on the Filter screen.
- VPN Passthrough. To enable or disable IPSec, PPPoE, and/or PPTP Pass-through, use this screen.

Access Restrictions

- Access Restriction

Applications & Gaming

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

Administration

- Management. On this screen, alter router access privileges and UPnP settings.
- Log. If you want to view or save activity logs, click this tab.
- Factory Defaults. If you want to restore the Router’s factory defaults, then use this screen.
- Firmware Upgrade. Click this tab if you want to upgrade the Router’s firmware.

Status

- Router. This screen provides status information about the Router.

Beacon Interval :*The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.*

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

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

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

- Local Network. This provides status information about the local network.

How to Access the Web-based Utility

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Router’s default IP address, 192.168.1.1, in the Address field. Then press Enter.

A password request page, shown in Figure 6-2 will pop up. (non-Windows XP users will see a similar screen.) Leave the User Name field blank, and enter admin (the default password) in the Password field. Then click the OK button.

To save your changes on any page, click the **Apply** button. To cancel any unsaved changes on any page, click the Cancel button.

The Setup Tab

The Basic Setup Tab

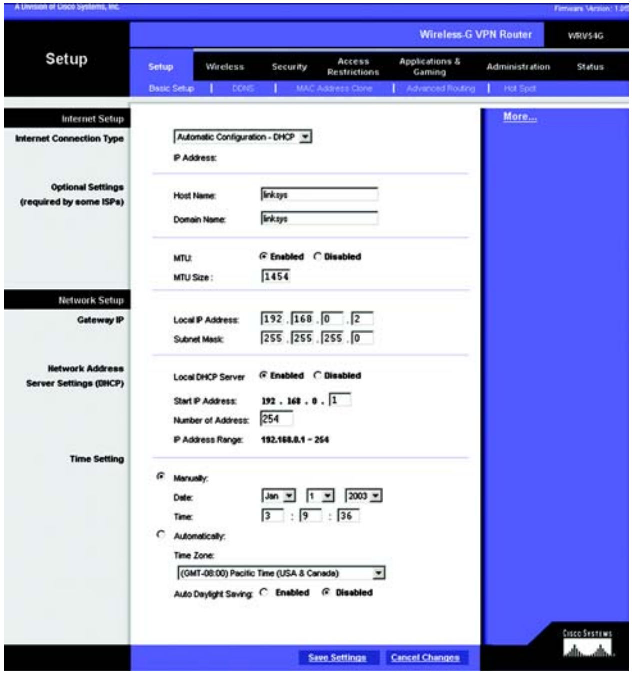
The first screen that appears is the Basic Setup tab. This tab allows you to change the Router's general settings. Change these settings as described here and click the **Save Settings** button to save your changes or **Cancel Changes** to cancel your changes.

Internet Setup

- Internet Connection Type. The Router supports four connection types: Automatic Configuration - DHCP (the default connection type), PPPoE, Static IP, and PPTP. Each Basic Setup screen and available features will differ depending on what kind of connection type you select.

  Automatic Configuration - DHCP

  By default, the Router’s Configuration Type is set to Automatic Configuration - DHCP, and it should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.



Internet Setup
Internet Connection Type: Automatic Configuration - DHCP
IP Address:

Optional Settings (required by some ISPs)
Host Name: linksys
Domain Name: linksys
MTU: ● Enabled ○ Disabled
MTU Size : 1454

Network Setup
Gateway IP
Local IP Address: 192 . 168 . 0 . 2
Subnet Mask: 255 . 255 . 255 . 0

Network Address Server Settings (DHCP)
Local DHCP Server ● Enabled ○ Disabled
Start IP Address: 192 . 168 . 0 . 1
Number of Address: 254
IP Address Range: 192.168.0.1 - 254

Time Setting
● Manually:
Date: Jan 1 2003
Time: 3 : 9 : 36
○ Automatically:
Time Zone: (GMT-08:00) Pacific Time (USA & Canada)
Auto Daylight Saving: ○ Enabled ● Disabled

Figure 7-2: Setup Tab/DHCP Internet Connection Type

Static

If you are required to use a permanent IP address to connect to the Internet, then select Static IP.

- IP Address. This is the Router’s IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Router’s Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
- Default Gateway. Your ISP will provide you with the Default Gateway Address, which is the ISP server’s IP address.
- Primary DNS. (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

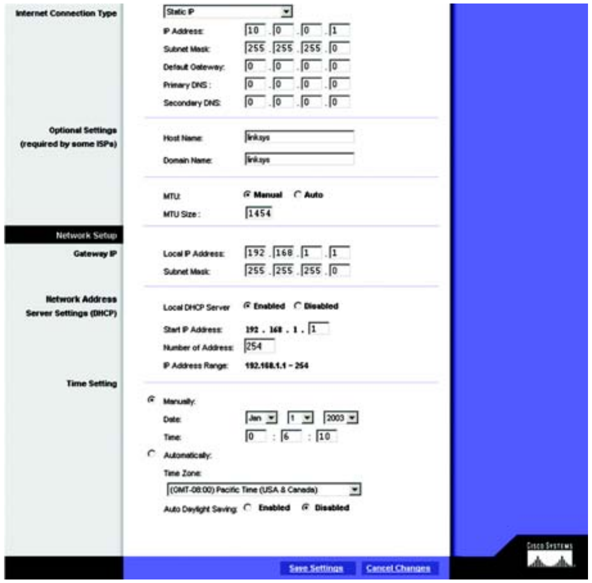
To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the Cancel button.

PPPOE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.

- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the Cancel button. To get more information about the features, click the Help button.



Internet Connection Type: Static IP

IP Address: 10 . 0 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

Primary DNS : 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

Host Name: linksys

Domain Name: linksys

MTU: ● Manual ○ Auto

MTU Size : 1454

Local IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Local DHCP Server ● Enabled ○ Disabled

Start IP Address: 192 . 168 . 1 . 1

Number of Address: 254

IP Address Range: 192.168.1.1 ~ 254

● Manually:

Date: Jan 1 2003

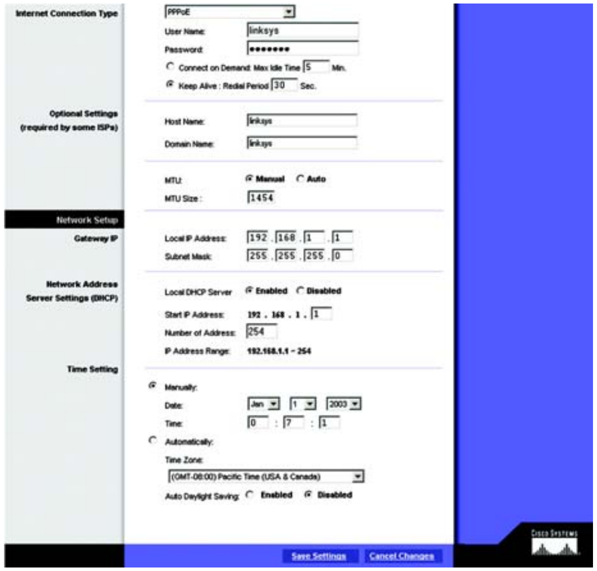
Time: 0 : 6 : 10

○ Automatically:

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

Auto Daylight Saving: ○ Enabled ● Disabled

Figure 7-3: Static Internet Connection Type



Internet Connection Type: PPPoE

User Name: linksys

Password: •••••••

○ Connect on Demand: Max Idle Time 5 Min.

● Keep Alive : Redial Period 30 Sec.

Host Name: linksys

Domain Name: linksys

MTU: ● Manual ○ Auto

MTU Size : 1454

Local IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Local DHCP Server ● Enabled ○ Disabled

Start IP Address: 192 . 168 . 1 . 1

Number of Address: 254

IP Address Range: 192.168.1.1 ~ 254

● Manually:

Date: Jan 1 2003

Time: 0 : 7 : 1

○ Automatically:

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

Auto Daylight Saving: ○ Enabled ● Disabled

Figure 7-4: PPPoE Internet Connection Type

PPPTP

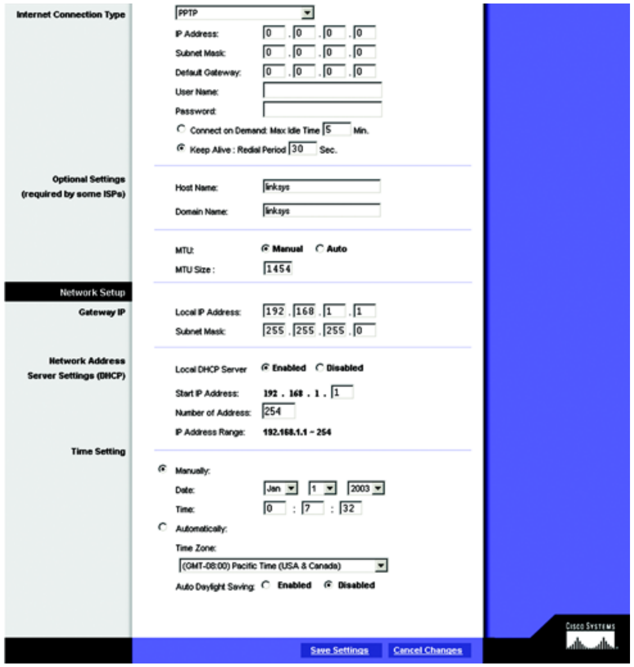
Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only (see Figure 6-8).

- Internet IP Address. This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
- Default Gateway. Your ISP will provide you with the Default Gateway Address.
- User Name and Passwor. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive Option: Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to Keep Alive. To use this option, click the radio button next to Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

To save your changes on this page, click the **Apply** button. To cancel any unsaved changes on this page, click the Cancel button. To get more information about the features, click the Help button.

Optional Settings (Required by some ISPs)

- Host Name and Domain Name. These fields allow you to supply a host and domain name for the Router. 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.
- MTU. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Enabled** and enter the value desired. It is recommended that you leave this value in the



Internet Connection Type: PPTP
IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Default Gateway: 0 . 0 . 0 . 0
User Name:
Password:
○ Connect on Demand: Max Idle Time 5 Min.
● Keep Alive : Redial Period 30 Sec.

Optional Settings (required by some ISPs)
Host Name: linksys
Domain Name: linksys
MTU: ● Manual ○ Auto
MTU Size : 1454

Network Setup
Gateway IP
Local IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255 . 255 . 255 . 0

Network Address Server Settings (DHCP)
Local DHCP Server ● Enabled ○ Disabled
Start IP Address: 192 . 168 . 1 . 1
Number of Address: 254
IP Address Range: 192.168.1.1 ~ 254

Time Setting
● Manually:
Date: Jan 1 2003
Time: 0 : 7 : 32
○ Automatically:
Time Zone:
(GMT-08:00) Pacific Time (USA & Canada)
Auto Daylight Saving: ○ Enabled ● Disabled

Figure 7-5: PPTP Internet Connection Type

1200 to 1500 range. For most DSL users, it is recommended to use the value 1492. By default, MTU is set at 1500 when disabled.

Network Setup

- Gateway IP. The values for the Router's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.
- Local IP Address. The default value is 192.168.1.1.
- Subnet Mask. The default value is 255.255.255.0.
- Network Address Server Settings (DHCP). A Dynamic Host Configuration Protocol (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 Router enabled as a DHCP server.
- Local DHCP Server. DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to Disable. If you disable DHCP, remember to assign a static IP address to the Router.
- Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1. 2 or greater, because the default IP address for the Router is 192.168.1.1.
- Number of Address (Optional). Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users. By default, as shown in Figure 6-9, add 100 to 50, and the range is 192.168.1.100 to 192.168.1.149.
- DHCP Address Range. The range of DHCP addresses is displayed here.
- Time Setting. This is where you set the time for your Router. You can set it manually or automatically.

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

The DDNS Tab

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

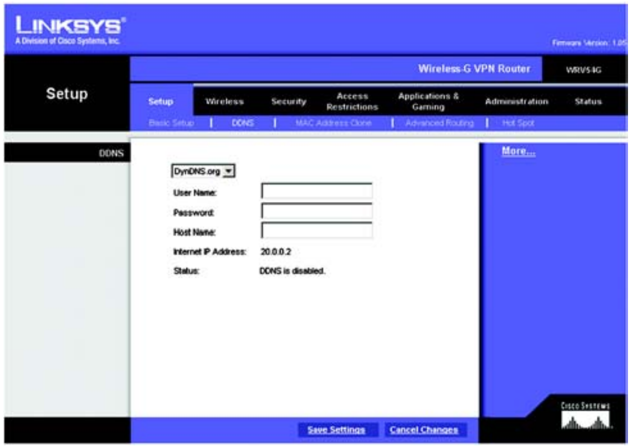
Before you can use this feature, you need to sign up for DDNS service at one of two DDNS service providers, DynDNS.org or TZO.com.

DDNS

DDNS Service. If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** in the drop-down menu. If your DDNS service is provided by TZO, then select **TZO.com**. The features available on the DDNS screen will vary, depending on which DDNS service provider you use.

- User Name, Password, and Host Name. Enter the **User Name, Password, and Host Name** of the account you set up with DynDNS.org.
- Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, it will change.
- Status. The status of the DDNS service connection is displayed here.

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



DynDNS.org

User Name:

Password:

Host Name:

Internet IP Address: 20.0.0.2

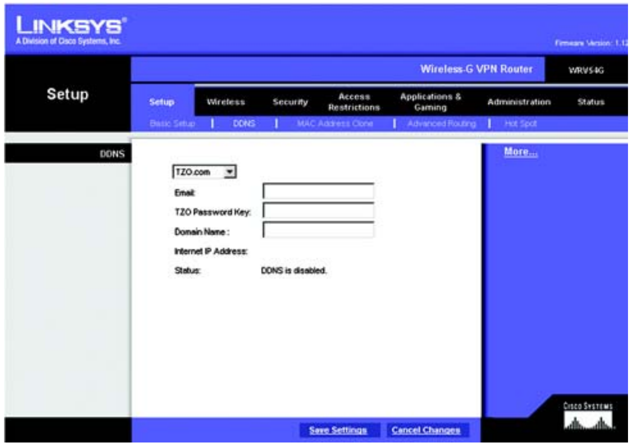
Status: DDNS is disabled.

Figure 7-6: DynDNS.org

TZO.com Tab

- Email Address, TZO Password Key, and Domain Name. Enter the **Email Address, TZO Password Key, and Domain Name** of the service you set up with TZO.
- Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, this will change.
- Status. The status of the DDNS service connection is displayed here.

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



TZO.com

Email:

TZO Password Key:

Domain Name :

Internet IP Address:

Status: DDNS is disabled.

Figure 7-7: TZO.com

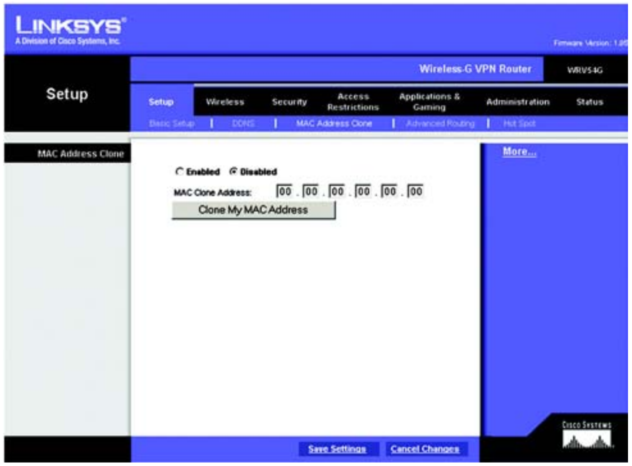
MAC Address Clone Tab

The Router’s MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. If your ISP requires MAC address registration, find your adapter’s MAC address by following the instructions in “Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter.”

MAC Clone

- MAC Clone Service. To use MAC address cloning, select **Enable**.
- MAC Address. To manually clone a MAC address, enter the 12 digits of your adapter’s MAC address in the on-screen fields (see Figure 6-25). Then click the **Save Settings** button.
- Clone My MAC Address. If you want to clone the MAC address of the PC you are currently using to configure the Router, then click the **Clone My MAC Address** button. The Router will automatically detect your PC’s MAC address, so you do NOT have to call your ISP to change the registered MAC address to the Router’s MAC address. It is recommended that the PC registered with the ISP is used to open the MAC Address Clone tab.

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



○ Enabled ● Disabled

MAC Clone Address: 00 . 00 . 00 . 00 . 00 . 00

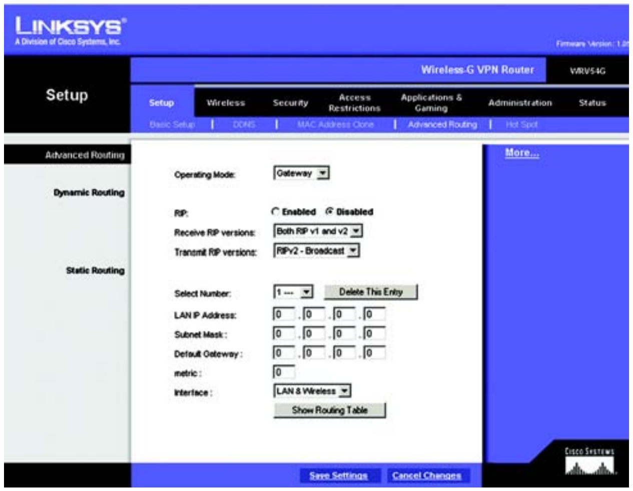
Figure 7-8: MAC Address Clone

Advanced Routing Tab

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

Advanced Routing

- Operating Mode. Select the Operating Mode__________ from the drop-down menu.
- Dynamic Routing. With Dynamic Routing you can enable the Router to automatically adjust to physical changes in the network’s layout. The Router, 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.
- Receive RIP Version To use dynamic routing for reception of network data, select the protocol you want: **RIP1** or **RIP2**.
- Transmit RIP Version. To use dynamic routing for transmission of network data, select the protocol you want: **RIP1, RIP1-Compatible, or RIP2**.



Operating Mode: Gateway

RIP: ○ Enabled ● Disabled

Receive RIP versions: Both RIP v1 and v2

Transmit RIP versions: RIPv2 - Broadcast

Select Number: 1 ---

LAN IP Address: 0 . 0 . 0 . 0

Subnet Mask : 0 . 0 . 0 . 0

Default Gateway : 0 . 0 . 0 . 0

metric : 0

Interface : LAN & Wireless

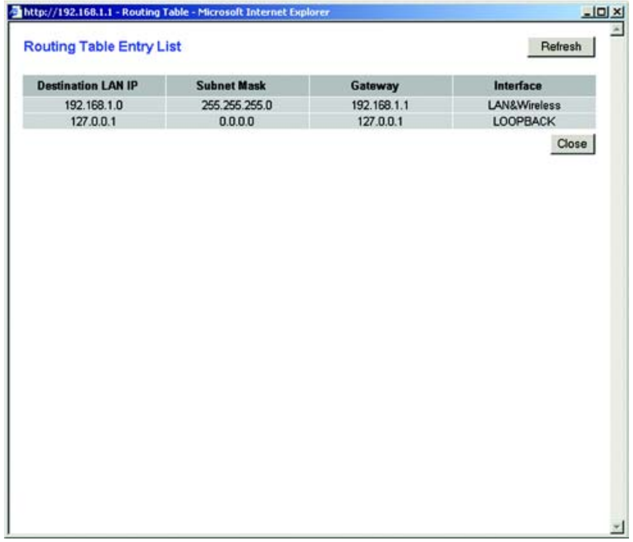
Figure 7-9:

Static Routing

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

- Select Number. Select the **number** of the static route from the drop-down menu. The Router supports up to 20 static route entries.
- Delete This Entry. If you need to delete a route, select its **number** from the drop-down menu, and click the **Delete Entry** button.
- LAN IP Address. The LAN IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0. For example, the Router's standard IP address is 192.168.1.1. Based on this address, the address of the routed network is 192.168.1, with the last digit determining the Router's place on the network. Therefore you would enter the IP address 192.168.1.0 if you wanted to route to the Router's entire network, rather than just to the Router.
- Subnet Mask. The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion. Take, for example, a network in which the Subnet Mask is 255.255.255.0. This determines (by using the values 255) that the first three numbers of a network IP address identify this particular network, while the last digit (from 1 to 254) identifies the specific host.
- Default Gateway. This IP address should be the IP address of the gateway device that allows for contact between the Router and the remote network or host.
- metric. 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._____?????
- Interface. Select **LAN & Wireless** or **Internet**, depending on the location of the static route's final destination.
- Show Routing Table. Click the **Show Routing Table** button to open a screen displaying how data is routed through your LAN. For each route, the Destination LAN IP address, Subnet Mask, Default Gateway, and Interface are displayed. Click the **Refresh** button to update the information. See Figure 6-15.

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


http://192.168.1.1 - Routing Table - Microsoft Internet Explorer
Refresh
Close

Routing Table Entry List

Destination LAN IP	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	192.168.1.1	LAN&Wireless
127.0.0.1	0.0.0.0	127.0.0.1	LOOPBACK

Figure 7-10:

Hot Spot

Hot Spot Service Provider. Select the **Hot Spot Provider** from the drop-down menu.

Hot Spot Sevice Provider URL. Enter the **Hot Spot Sevice Provider URL** in the field.

Hot Spot Object ID. Enter the **Hot Spot Object ID** in the field.

Click **Register** to ______________________________. Click **Hot Spot Status** to view the status. Click the **Clear** button to clear the information you've entered.

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

The Wireless Tab

Basic Wireless Settings

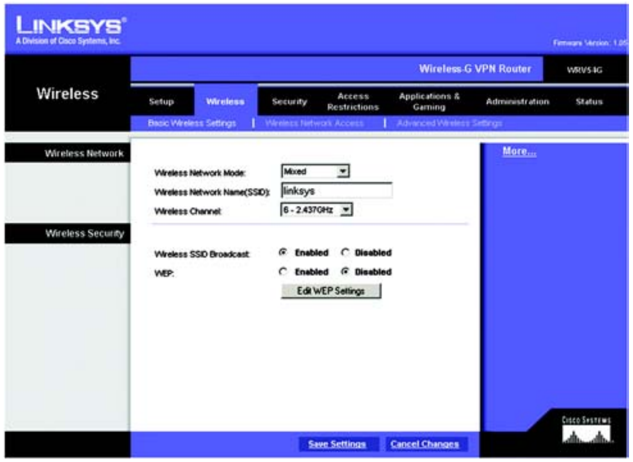
This screen allows you to choose your wireless network mode and wireless security.

Wireless Network

- Wireless Network Mode. If you have Wireless-G and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only Wireless-G devices, select **G-Only**. If you want to disable wireless networking, select **Disable**.

- Wireless Network Name. Enter the **Wireless Network Name (SSID)** into the field. The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. For added security, Linksys recommends that you change the default SSID (linksys) to a unique name of your choice.

- Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All devices in your wireless network must use the same channel in order to function correctly.



Wireless Network Mode: Mixed

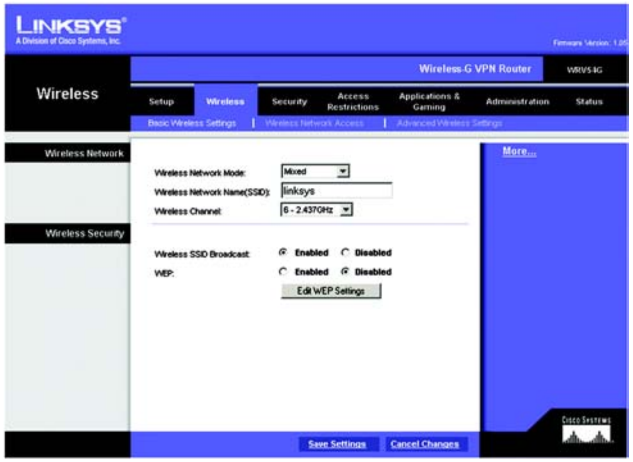
Wireless Network Name(SSID): linksys

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ● Enabled ○ Disabled

WEP: ○ Enabled ● Disabled

Figure 7-11:



Wireless Network Mode: Mixed

Wireless Network Name(SSID): linksys

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ● Enabled ○ Disabled

WEP: ○ Enabled ● Disabled

Figure 7-12:

Wireless Security

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

- WEP. An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode data transmissions, all devices-Wireless-G and 802.11b-in a network must use an identical WEP key. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance. To enable WEP encryption, click the **Enabled** radio button. Then click the **Edit WEP Settings** button to configure the WEP settings. To disable WEP encryption, keep the default setting, **Disabled**.

WEP

The WEP screen allows you to configure your WEP settings. WEP encryption should always be enabled to increase the security of your wireless network. Default Transmit Key Select which WEP key (1-4) will be used when the Router sends data. Make sure the receiving device is using the same key.

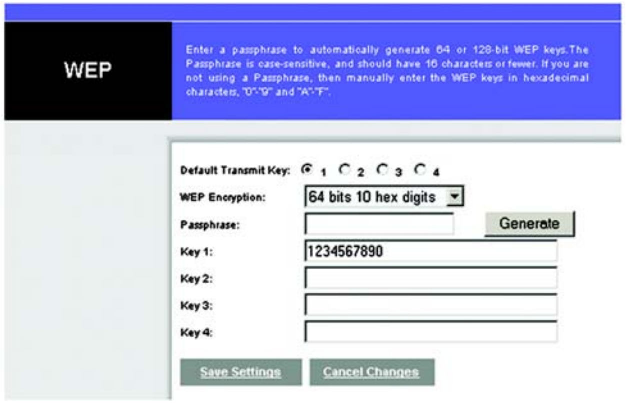
- WEP Encryption. Select the level of WEP encryption you wish to use, 64-bit 10 hex digits or 128-bit 26 hex digits. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

- Passphrase. Instead of manually entering WEP keys, you can enter a Passphrase. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, enter the WEP key manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

- Keys 1-4. WEP keys enable you to create an encryption scheme for wireless LAN transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.)

  If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.

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



WEP

Enter a passphrase to automatically generate 64 or 128-bit WEP keys.The Passphrase is case-sensitive, and should have 16 characters or fewer. If you are not using a Passphrase, then manually enter the WEP keys in hexadecimal characters, "0"-"9" and "A"-"F".

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 64 bits 10 hex digits

Passphrase:

Key 1: 1234567890

Key 2:

Key 3:

Key 4:

Figure 7-13:

Wireless Network Access

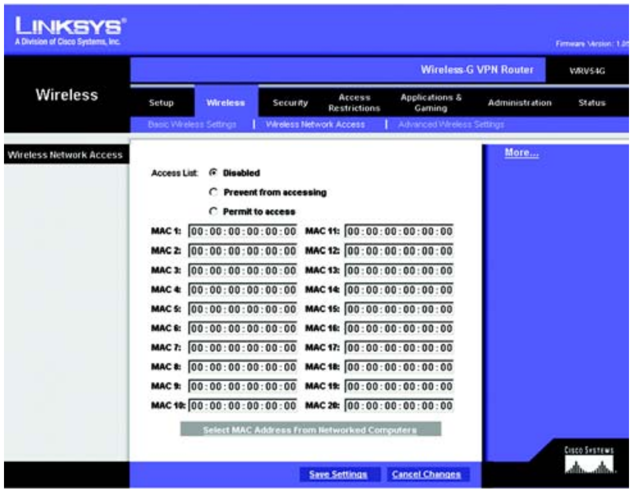
Wireless Network Access. If this function is enabled, only the computers on the list will be allowed access to the wireless network. To add a computer to the network, click the **Permit to access** button, and enter the MAC address in the fields. Click the **Select MAC Address From Networked Computers** button, and the screen in figure 7-15 will appear.

Select the **MAC Address** from the list and click the **Select** button.

To prevent access, click the **Prevent from accessing** button, then click **Select MAC Address from the list.** From the screen in figure 7-15, select the **MAC Address** from the list, and click the **Select** button.

Click the **Refresh** button if you want to refresh the screen. Click the **Close** button to return to th previous screen.

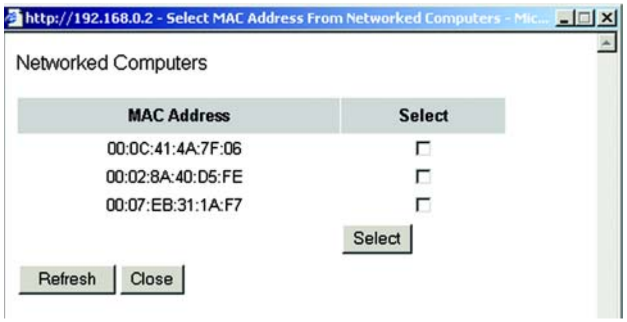
When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Access List: ● Disabled
○ Prevent from accessing
○ Permit to access

MAC 1:	00:00:00:00:00:00	MAC 11:	00:00:00:00:00:00
MAC 2:	00:00:00:00:00:00	MAC 12:	00:00:00:00:00:00
MAC 3:	00:00:00:00:00:00	MAC 13:	00:00:00:00:00:00
MAC 4:	00:00:00:00:00:00	MAC 14:	00:00:00:00:00:00
MAC 5:	00:00:00:00:00:00	MAC 15:	00:00:00:00:00:00
MAC 6:	00:00:00:00:00:00	MAC 16:	00:00:00:00:00:00
MAC 7:	00:00:00:00:00:00	MAC 17:	00:00:00:00:00:00
MAC 8:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00
MAC 9:	00:00:00:00:00:00	MAC 19:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 20:	00:00:00:00:00:00

Figure 7-14:



http://192.168.0.2 - Select MAC Address From Networked Computers - Mic...

Networked Computers

MAC Address	Select
00:0C:41:4A:7F:06	□
00:02:8A:40:D5:FE	□
00:07:EB:31:1A:F7	□

Figure 7-15:

Advanced Wireless Settings

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

- Authentication Type. The default is set to Auto, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. For Shared Key authentication, the sender and recipient use a WEP key for authentication. If you want to use only Shared Key authentication, then select **Shared Key**.

- Basic Data Rates.

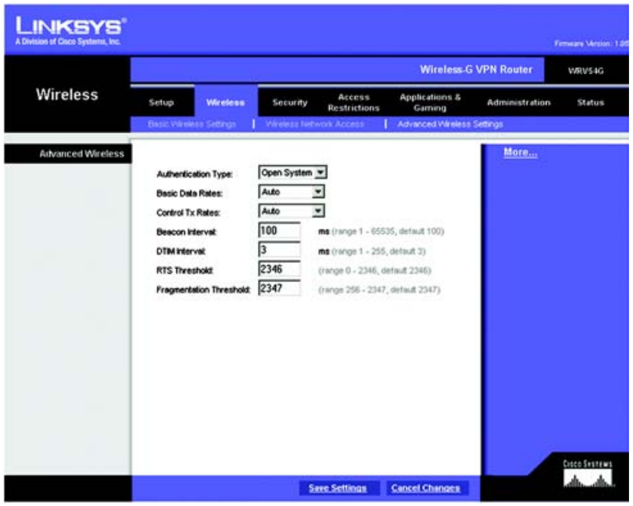
- Control Tx Rates. The default transmission rate is Auto. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, Auto, to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client.

- Beacon Interval. The default value is 100. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

- DTIM Interval The default value is 3. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

- RTS Threshold This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

- Fragmentation Threshold This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.



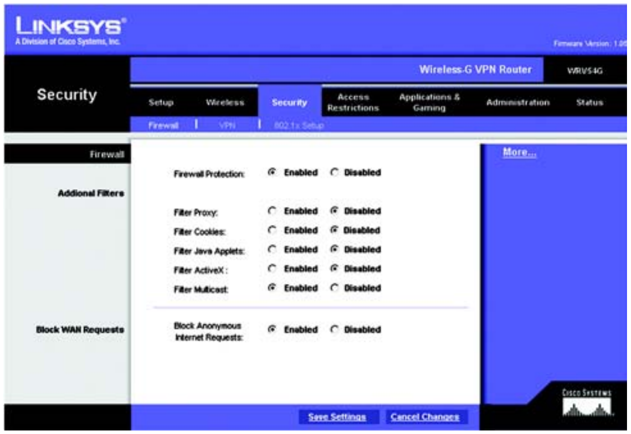
Authentication Type: Open System ▼
Basic Data Rates: Auto ▼
Control Tx Rates: Auto ▼
Beacon Interval: 100 ms (range 1 - 65535, default 100)
DTIM Interval: 3 ms (range 1 - 255, default 3)
RTS Threshold: 2346 (range 0 - 2346, default 2346)
Fragmentation Threshold: 2347 (range 256 - 2347, default 2347)

Figure 7-16:

The Security Tab

Firewall

When you click the Security tab, you will see the Firewall screen (see Figure 6-16). This screen contains Filters and Block WAN Requests. Filters block specific internal users from accessing the Internet and block anonymous Internet requests and/or multicasting.



Firewall

Firewall Protection: ● Enabled ○ Disabled

Addional Filters

Filter Proxy: ○ Enabled ● Disabled

Filter Cookies: ○ Enabled ● Disabled

Filter Java Applets: ○ Enabled ● Disabled

Filter ActiveX : ○ Enabled ● Disabled

Filter Multicast: ● Enabled ○ Disabled

Block WAN Requests

Block Anonymous Internet Requests: ● Enabled ○ Disabled

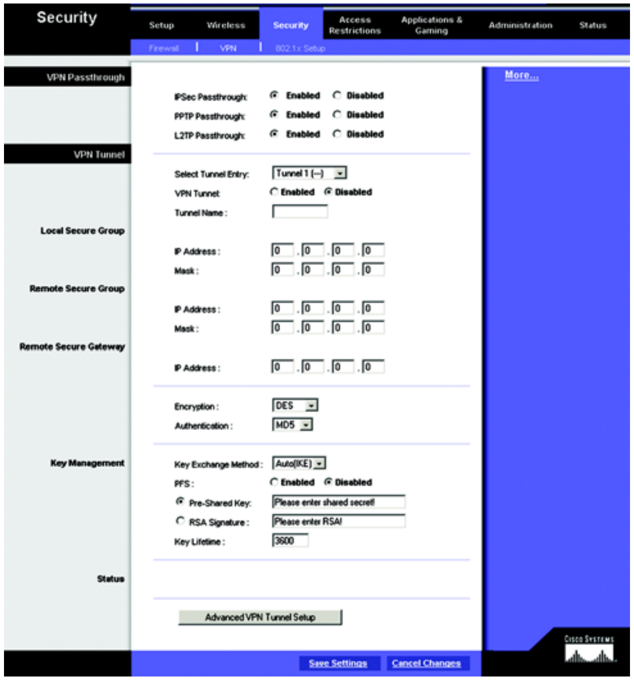
Figure 7-17:

- Firewall. To add Firewall Protection, click **Enabled**. If you do not want Firewall Protection, click **Disabled**.
- Filter Proxy. Use of WAN proxy servers may compromise the Router's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click **Enabled**.
- Filter Cookies. A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click **Enabled**.
- Filter Java Applets. Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language. To enable Java Applet filtering, click **Enabled**.
- Filter ActiveX. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click **Enabled**.
- Filter Multicast. Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. Select **Enabled** to filter multicasting, or **Disabled** to disable this feature.
- Block Anonymous Internet Requests. This keeps your network from being “pinged” or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to work their way into your network. Select **Enabled** to block anonymous Internet requests, or **Disabled** to allow anonymous Internet requests.

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

VPN

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. This connection is very specific as far as its settings are concerned; this is what creates the security.   The VPN screen, shown in Figure 7-18, allows you to configure your VPN settings to make your network more secure.



VPN Passthrough

IPSec Passthrough: ● Enabled ○ Disabled

PPTP Passthrough: ● Enabled ○ Disabled

L2TP Passthrough: ● Enabled ○ Disabled

VPN Tunnel

Select Tunnel Entry: Tunnel 1 (--)

VPN Tunnel: ○ Enabled ● Disabled

Tunnel Name :

Local Secure Group

IP Address : 0 . 0 . 0 . 0

Mask : 0 . 0 . 0 . 0

Remote Secure Group

IP Address : 0 . 0 . 0 . 0

Mask : 0 . 0 . 0 . 0

Remote Secure Gateway

IP Address : 0 . 0 . 0 . 0

Encryption : DES

Authentication : MD5

Key Management

Key Exchange Method : Auto(IKE)

PFS : ○ Enabled ● Disabled

● Pre-Shared Key: Please enter shared secret!

○ RSA Signature : Please enter RSA!

Key Lifetime : 3600

Status

Figure 7-18:

VPN PassThrough

- IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enabled** button. To disable IPSec Passthrough, click the **Disabled** button.

- PPTP Pass Through. Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enabled** button. To disable PPTP Passthrough, click the **Disabled** button.

- L2TP Pass Through. Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by to enable the operation of a virtual private network (VPN) over the Internet.To allow L2TP Passthrough, click the **Enabled** button. To disable L2TP Passthrough, click the **Disabled** button.

VPN Tunnel

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

- To establish this tunnel, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. It is possible to create up to 70 simultaneous tunnels. Then click **Enabled** to enable the tunnel. Once the tunnel is enabled, enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

- Local Secure Group and Remote Secure Group. The Local Secure Group is the computer(s) on your LAN that can access the tunnel. The Remote Secure Group is the computer (s) on the remote end of the tunnel that can access the tunnel. Enter the **IP Address** and **Subnet Mask** of the local VPN Router in the fields.

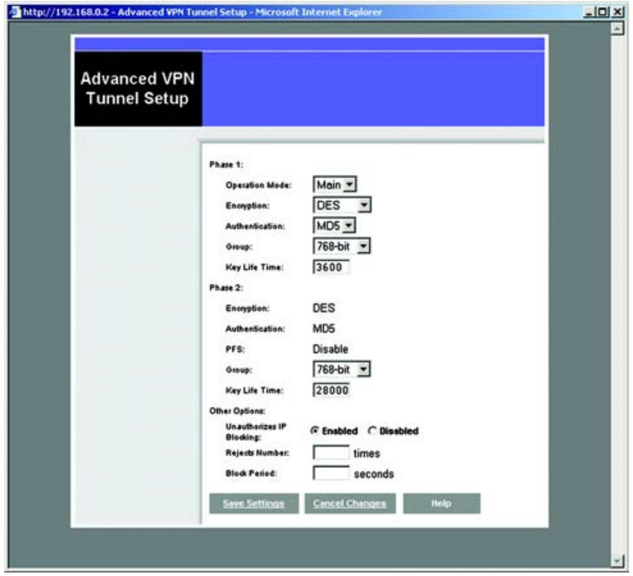
- Remote Security Gateway. The Remote Security Gateway is the VPN device, such as a second VPN Router, on the remote end of the VPN tunnel. Enter the IP Address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client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

- Encryption. Using Encryption also helps make your connection more secure. There are two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable. In Figure 6-16, DES (which is the default) has been selected.
- Authentication. Authentication acts as another level of security. There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication. In Figure 6-16, MD5 (the default) has been selected.
- Key Management. Select Auto (IKE) and enter a series of numbers or letters in the Pre-shared Key field. Check the box next to PFS (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. In the example shown in Figure 6-17, the word MyTest is used. Based on this word, which MUST be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.
- Status. Click the **Advanced VPN Tunnel Setup** key and the Advanced VPN Tunnel Setup screen will appear.

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

Advanced VPN Tunnel Setup

From the Advance VPN Tunnel Setup screen, shown in Figure 7-19, you can adjust the settings for specific VPN tunnels.



http://192.168.0.2 - Advanced VPN Tunnel Setup - Microsoft Internet Explorer

Advanced VPN Tunnel Setup

Phase 1:

Operation Mode: Main

Encryption: DES

Authentication: MD5

Group: 768-bit

Key Life Time: 3600

Phase 2:

Encryption: DES

Authentication: MD5

PFS: Disable

Group: 768-bit

Key Life Time: 28000

Other Options:

Unauthorizes IP Blocking: ● Enabled ○ Disabled

Rejects Number: times

Block Period: seconds

Figure 7-19:

Phase 1

- Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.
- Operation Mode. There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Router will accept both Main and Aggressive requests from the remote VPN device.
- Encryption. Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.
- Authentication. Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.
- Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.
- Key Life Time. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Phase 2

- Encryption. The encryption method selected in Phase 1 will be displayed.
- Authentication. The authentication method selected in Phase 1 will be displayed.
- Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.
- Key Life Time. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Other Options

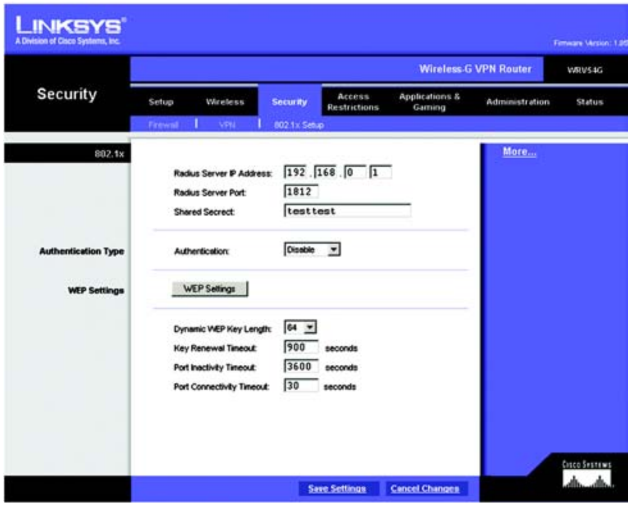
- Unauthorizes IP Blocking. Click **Enabled** to block unauthorized IP addresses. Enter in the Rejects Number field to specify how many times IKE must fail before blocking that unauthorized IP address. Enter the length of time that you specify (in seconds) in the Block Period field.

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

Security

802.1x

- Radius Server IP Address. Enter the Radius Server IP Address in the fields.
- Radius Server Port. Enter the Radius Server Port in the field.
- Shared Secret. Enter the Shared Secret in the field.
- Authentication Type. To enable EAP-TLS, click EAP-TLS. To enable EAP-TTLS, click EAP-TTLS. To enable EAP-MD5, click EAP-MD5,. To disable authentication, click Disable.
- WEP Settings. Click the **WEP Settings** button to edit the settings and Figure 7-21 will appear.
- Dynamic WEP Key Length. Select **64** or **128** bits from the drop-down menu.
- Key Renewal Timeout. Enter the time in seconds for key renewal.
- Port Inactivity Timeout. Enter the time in seconds for port inactivity.
- Port Connectivity Timeout. Enter the time in seconds for port connectivity.



Radius Server IP Address: 192 . 168 . 0 . 1
Radius Server Port: 1812
Shared Secrect: testtest
Authentication: Disable
Dynamic WEP Key Length: 64
Key Renewal Timeout: 900 seconds
Port Inactivity Timeout: 3600 seconds
Port Connectivity Timeout: 30 seconds

Figure 7-20:

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

WEP

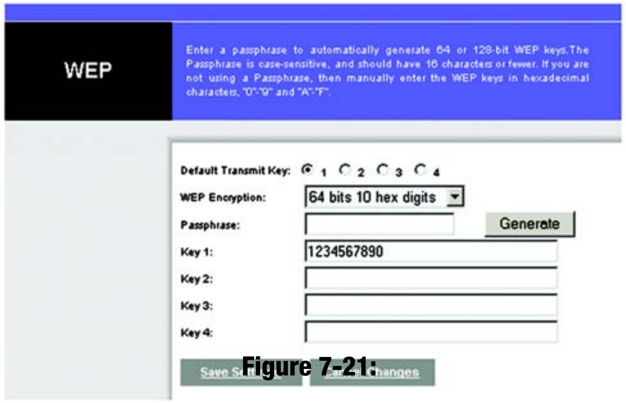
The WEP screen allows you to configure your WEP settings. WEP encryption should always be enabled to increase the security of your wireless network. Default Transmit Key. Select which WEP key (1-4) will be used when the Router sends data. Make sure that the receiving device is using the same key.

- WEP Encryption. Select the level of WEP encryption you wish to use, **64-bit 10 hex digits** or 1**28-bit 26 hex digits.** Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

- Passphrase. Instead of manually entering WEP keys, you can enter a Passphrase. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, enter the WEP key manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

- Keys 1-4. WEP keys enable you to create an encryption scheme for wireless LAN transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.)

  If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.



Enter a passphrase to automatically generate 64 or 128-bit WEP keys.The Passphrase is case-sensitive, and should have 16 characters or fewer. If you are not using a Passphrase, then manually enter the WEP keys in hexadecimal characters, "0"-"9" and "A"-"F".

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4
WEP Encryption: 64 bits 10 hex digits
Passphrase:
Key 1: 1234567890
Key 2:
Key 3:
Key 4:

Figure 7-21:

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

Access Restrictions

Access Restriction

The Access Restrictions tab, shown in Figure 7-22, allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific PCs and set up filters by using network port numbers.

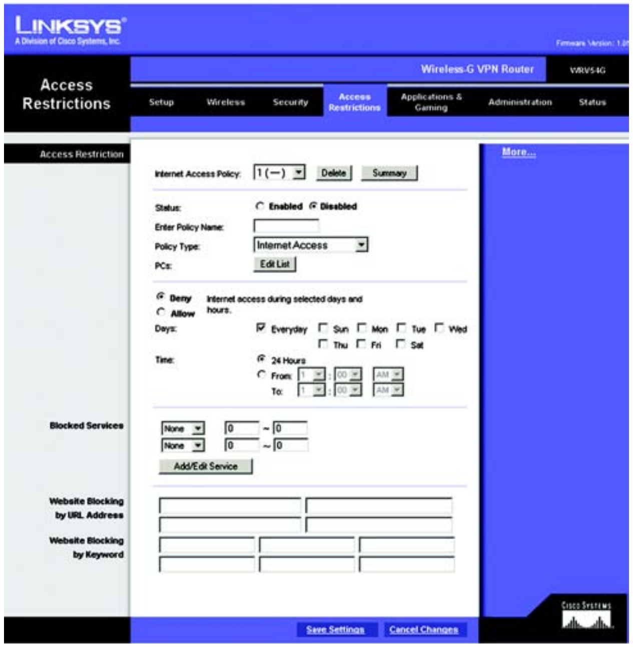
- Internet Access Policy. Multiple Filters can be saved as Internet Access Policies. When you wish to edit one, select the number of the Policy from the drop-down menu. The tab will change to reflect the settings of this Policy. If you wish to delete this Policy, click the Delete button. To see a summary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

  The summaries are listed on this screen, shown in Figure 7-23, with their name and settings. To return to the Filters tab, click the **Close** button.

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

  To create an Internet Access policy:

1. Enter a Policy Name in the field provided. Select **Internet Access** as the Policy Type.



Internet Access Policy: 1 (—)
Status: ○ Enabled ● Disabled
Enter Policy Name:
Policy Type: Internet Access
PCs:
● Deny ○ Allow Internet access during selected days and hours.
Days: ☑ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Time: ● 24 Hours ○ From: 1 : 00 AM To: 1 : 00 AM
Blocked Services: None 0 ~ 0
None 0 ~ 0
Website Blocking by URL Address
Website Blocking by Keyword

Figure 7-22:

2. Click the **Edit List** button. This will open the List of PCs screen, shown in Figure 7-23. From this screen, you can enter the IP address or MAC address of any PC to which this policy will apply. You can even enter ranges of PCs by IP address. Click the **Apply** button to save your settings, the **Cancel** button to undo any changes, and the **Close** button to return to the Filters tab.

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

4. You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting a service from the drop-down menus next to Blocked Services. If a service isn't listed, you can click the **Add Service** button to open the Service screen, shown in Figure 7-24, and add a service to the list. You will need to enter a Service name, as well as the Protocol and Port Range used by the service.

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

6. Lastly, click the **Save Settings** button to activate the policy.

   To create an Inbound Traffic Policy

1. Enter a Policy Name in the field provided. Select **Inbound Traffic** as the Policy Type.

2. Enter the **IP Address** from which you want to block. Select the Protocol: **TCP**, **UDP**, or **Both**. Enter the **port** number or select **Any**. Enter the IP Address to which you want to block.

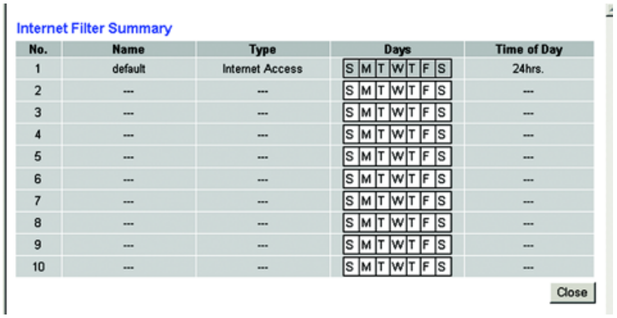
3. Select **Deny** or **Allow** as appropriate.

4. By selecting the appropriate setting next to Days and Time, choose when the Inbound Traffic will be filtered.

   Lastly, click the **Save Settings** button to activate the policy.

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

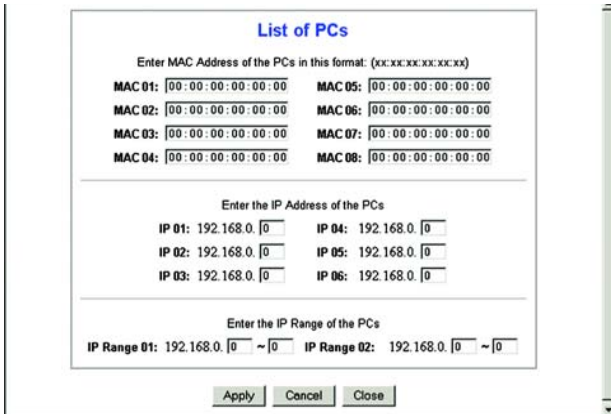
Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the Website Blocking by URL Address fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the Website Blocking by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



Internet Filter Summary

No.	Name	Type	Days	Time of Day
1	default	Internet Access	S M T W T F S	24hrs.
2	---	---	S M T W T F S	---
3	---	---	S M T W T F S	---
4	---	---	S M T W T F S	---
5	---	---	S M T W T F S	---
6	---	---	S M T W T F S	---
7	---	---	S M T W T F S	---
8	---	---	S M T W T F S	---
9	---	---	S M T W T F S	---
10	---	---	S M T W T F S	---

Figure 7-23:



List of PCs

Enter MAC Address of the PCs in this format: (xx:xx:xx:xx:xx:xx)

MAC 01: 00:00:00:00:00:00 MAC 05: 00:00:00:00:00:00
MAC 02: 00:00:00:00:00:00 MAC 06: 00:00:00:00:00:00
MAC 03: 00:00:00:00:00:00 MAC 07: 00:00:00:00:00:00
MAC 04: 00:00:00:00:00:00 MAC 08: 00:00:00:00:00:00

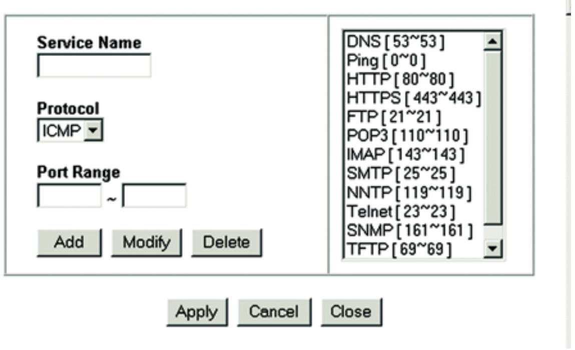
Enter the IP Address of the PCs

IP 01: 192.168.0. 0 IP 04: 192.168.0. 0
IP 02: 192.168.0. 0 IP 05: 192.168.0. 0
IP 03: 192.168.0. 0 IP 06: 192.168.0. 0

Enter the IP Range of the PCs

IP Range 01: 192.168.0. 0 ~ 0 IP Range 02: 192.168.0. 0 ~ 0

Figure 7-25:



Service Name

Protocol ICMP

Port Range ~

DNS [53~53]
Ping [0~0]
HTTP [80~80]
HTTPS [443~443]
FTP [21~21]
POP3 [110~110]
IMAP [143~143]
SMTP [25~25]
NNTP [119~119]
Telnet [23~23]
SNMP [161~161]
TFTP [69~69]

Figure 7-24:

Applications and Gaming

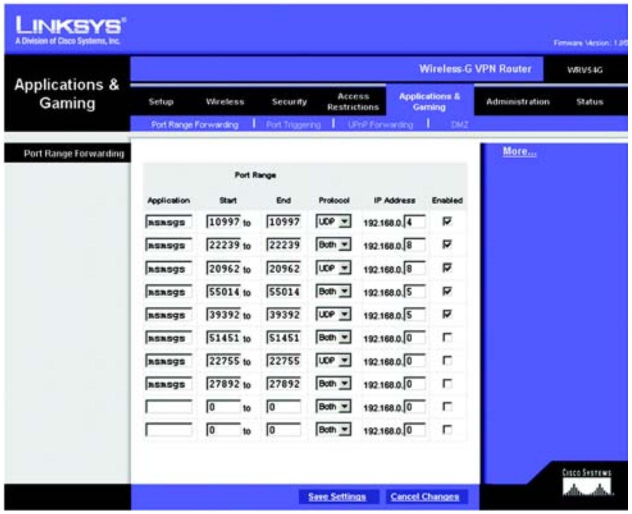
Port Range Forwarding

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

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

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

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



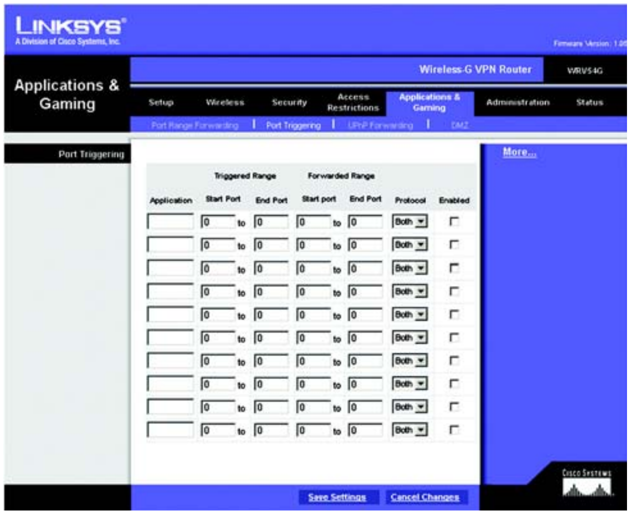
Application	Port Range Start		Port Range End	Protocol	IP Address	Enabled
msmsgs	10997	to	10997	UDP	192.168.0.4	☑
msmsgs	22239	to	22239	Both	192.168.0.8	☑
msmsgs	20962	to	20962	UDP	192.168.0.8	☑
msmsgs	55014	to	55014	Both	192.168.0.5	☑
msmsgs	39392	to	39392	UDP	192.168.0.5	☑
msmsgs	51451	to	51451	Both	192.168.0.0	□
msmsgs	22755	to	22755	UDP	192.168.0.0	□
msmsgs	27892	to	27892	Both	192.168.0.0	□
	0	to	0	Both	192.168.0.0	□
	0	to	0	Both	192.168.0.0	□

Figure 7-26:

Port Triggering

Port Triggering is used for special Internet applications whose outgoing ports differ from the incoming ports. For this feature, the Router will watch outgoing data for specific port numbers. The Router will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

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



	Triggered Range			Forwarded Range				
Application	Start Port		End Port	Start port		End Port	Protocol	Enabled
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□
	0	to	0	0	to	0	Both	□

Figure 7-27:

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

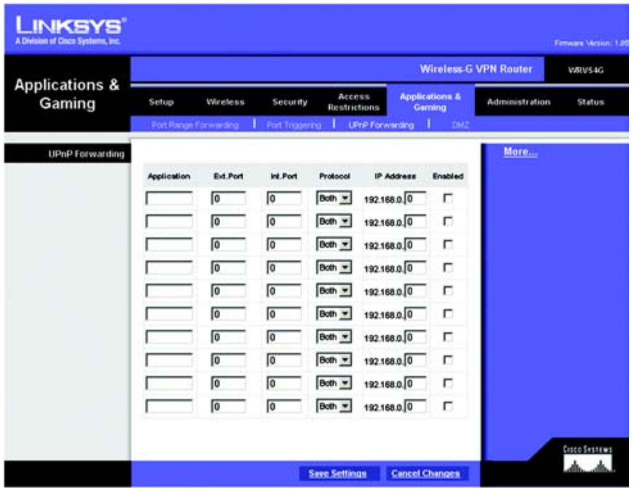
UPnP Forwarding

The UPnP screen displays preset application settings as well as options for customization of port services for other applications.

- Application. Ten preset applications are preset. You can specify up to five additional applications in the available fields.

  The preset applications are among the most widely used Internet applications. They include the following:

  - FTP (File Transfer Protocol) A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.
  - Telnet A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.
  - SMTP (Simple Mail Transfer Protocol) The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.
  - DNS (Domain Name System) The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember “handle” for an Internet address.
  - TFTP (Trivial File Transfer Protocol) A version of the TCP/IP FTP protocol that has no directory or password capability.
  - Finger A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being “fingered” must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user@domain address.
  - HTTP (HyperText Transport Protocol) The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.
  - POP3 (Post Office Protocol 3) A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system



Application	Ext.Port	Int.Port	Protocol	IP Address	Enabled
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□
	0	0	Both	192.168.0.0	□

Figure 7-28:

with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

- NNTP (Network News Transfer Protocol) The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.
- SNMP (Simple Network Management Protocol) A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

- Ext. Port and Int. Port. Enter the numbers of the port used by the server.
- Protocol. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- IP Address. Enter the IP Address and Click **Enabled**.

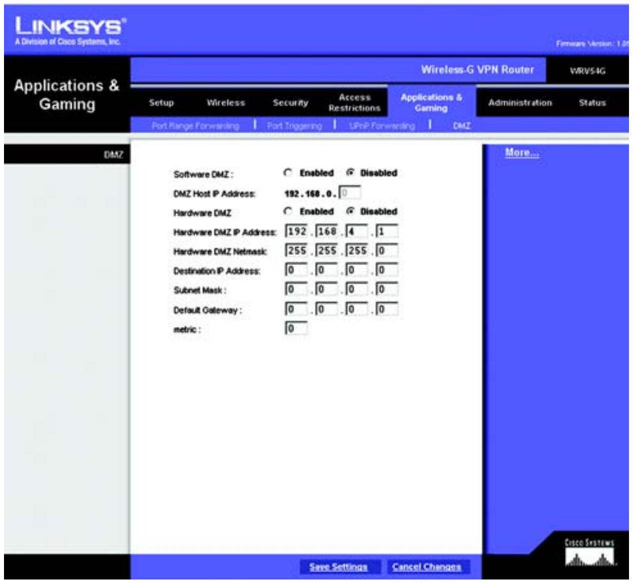
When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

DMZ

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

- Software DMZ. To use this feature, select **Enabled**. To disable DMZ , select **Disabled**.
- DMZ Host IP Address. To expose one PC, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter." Deactivate DMZ by entering a 0 in the field.
- Hardware DMZ. To use this feature, select **Enabled**. To disable DMZ , select **Disabled**.
- Hardware DMZ IP Address. Enter the IP Address in the fields.
- Hardware DMZ Netmask. Enter the Netmask in the fields.
- Destination IP Address. Enter the IP Address of the destination in the fields.
- Subnet Mask. Enter the Subnet Mask in the fields.
- Default Gateway. Enter the Default Gateway in the fields.
- metric. Enter the metric.

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



Software DMZ : ○ Enabled ● Disabled
DMZ Host IP Address: 192 . 168 . 0 . 0
Hardware DMZ ○ Enabled ● Disabled
Hardware DMZ IP Address: 192 . 168 . 4 . 1
Hardware DMZ Netmask: 255 . 255 . 255 . 0
Destination IP Address: 0 . 0 . 0 . 0
Subnet Mask : 0 . 0 . 0 . 0
Default Gateway : 0 . 0 . 0 . 0
metric : 0

Figure 7-29:

Administration

Management

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

Router Password

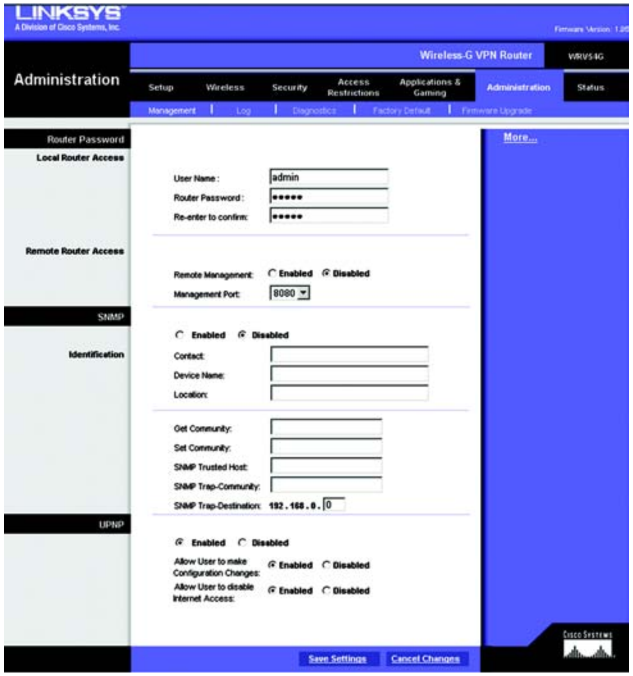
Local Router Access. To ensure the Router's security, you will be asked for your password when you access the Router's Web-based Utility. The default password is admin.

- Router Password. It is recommended that you change the default password to one of your choice.
- Re-enter to confirm. Re-enter the Router's new Password to confirm it.
- Remote Router Access. This feature allows you to access the Router from a remote location, via the Internet.
- Remote Management. This feature allows you to manage the Router from a remote location, via the Internet. To enable Remote Management, click **Enabled**.
- Mangagement Port. Select the port number you will use to remotely access the Router from the drop-down menu.

SNMP

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol. To enable SNMP, click **Enabled**. To disable SNMP, click Disabled.

- Identification. In the Contact field, enter contact information for the Router. In the Device Name field, enter the name of the Router. In the Location field, specify the area or location where the Router resides.
- SNMP Community. _________________________
- Get Community.
- Set Community.
- SNMP Trusted Host.
- SNMPTrap-Community.



Router Password

Local Router Access

User Name: admin

Router Password: •••••

Re-enter to confirm: •••••

Remote Router Access

Remote Management: ○ Enabled ● Disabled

Management Port: 8080

SNMP

○ Enabled ● Disabled

Identification

Contact:

Device Name:

Location:

Get Community:

Set Community:

SNMP Trusted Host:

SNMP Trap-Community:

SNMP Trap-Destination: 192.168.0.0

UPNP

● Enabled ○ Disabled

Allow User to make Configuration Changes: ● Enabled ○ Disabled

Allow User to disable Internet Access: ● Enabled ○ Disabled

Figure 7-30:

- SNMP Trap-Destination. Enter the **IP Address**.

UPnP

UPnP allows Windows XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. To enable UPnP, click **Enabled**.

- Allow User to make Configuration Changes. When enabled, this feature allows you to make manual changes while still using the UPnP feature.

- Allow users to disable Internet access. When enabled, this feature allows you to prohibit any and all Internet connections.

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

Log

The Log tab, shown in Figure 7-29, provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

Email Alert

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

- E-Mail Address for General Logs. Enter the **E-Mail Address for General Logs** in the field.

- E-Mail Address for Alert Logs. Enter the **E-Mail Address for Alert Logs** in the field.

- Return E-Mail address. Enter the **address for the return E-Mail**.

- E-Mail Server IP Address. Enter the **IP Address of the E-Mail Server** in the fields.

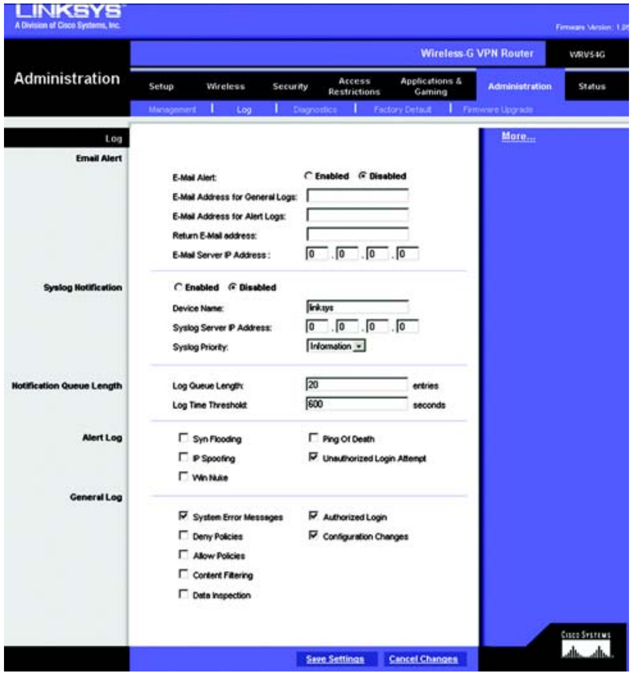
Syslog Notification

To enable Syslog, click **Enabled**.

- Device Name. Enter the **Device Name** in the field.

- Syslog Server IP Address. Enter the I**P Address of the Syslog Server**.

- Syslog Priority. Select the **priority** from the drop-down list.



Log

Email Alert
E-Mail Alert: ○ Enabled ● Disabled
E-Mail Address for General Logs:
E-Mail Address for Alert Logs:
Return E-Mail address:
E-Mail Server IP Address : 0 . 0 . 0 . 0

Syslog Notification
○ Enabled ● Disabled
Device Name: linksys
Syslog Server IP Address: 0 . 0 . 0 . 0
Syslog Priority: Information

Notification Queue Length
Log Queue Length: 20 entries
Log Time Threshold: 600 seconds

Alert Log
☐ Syn Flooding ☐ Ping Of Death
☐ IP Spoofing ☑ Unauthorized Login Attempt
☐ Win Nuke

General Log
☑ System Error Messages ☑ Authorized Login
☐ Deny Policies ☑ Configuration Changes
☐ Allow Policies
☐ Content Filtering
☐ Data Inspection

Figure 7-31:

Notification Qeue Length

- Log queue Length. Enter the **number** of entries in the log queue in the field.
- Log Time Threshold. Enter the **time** for the threshold in the field.

Alert Log

Select the alert log that you want to ______. Select Syn Flooding, IP Spoofing, Win Nuke, Ping of Death, or Unauthorized Login attempt.

General Log.

Select the _________. Select System Error Messages, Deny Policies, Allow Policies, Content Filtering, Data Inspection, authorized Login, or Configuration Changes.

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

Diagnostics

Ping Test

Ping Test Parameters

Ping Target IP. Enter the IP Address that you want to ping in the field.

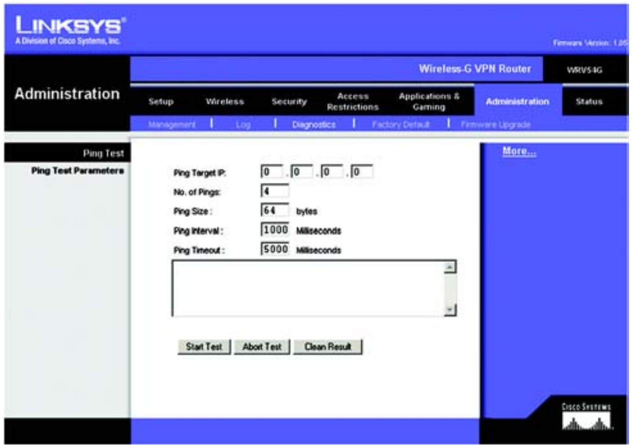
No. of Pings. Enter the number of times that you want to ping.

Ping Size. Enter the size of the ____.

Ping Interval. Enter the ping interval in Milliseconds.

Ping Timeout. Enter the time in Milliseconds.

Click the Start Test button to start the Ping Test. Click the Abort Test button to stop the test. Click the Clean Result button if _____. The results of the test will display in the window.



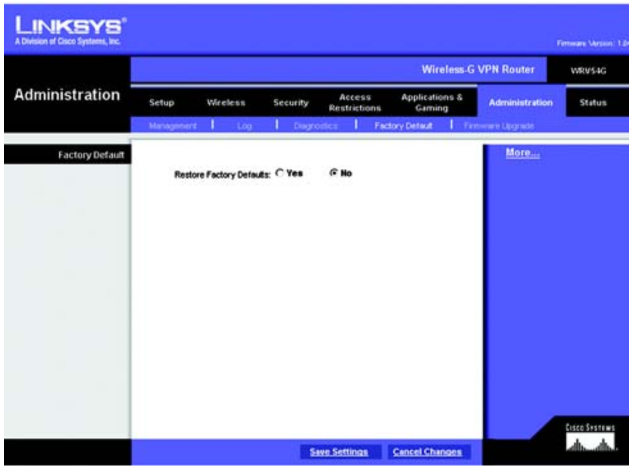
Ping Target IP: 0 . 0 . 0 . 0
No. of Pings: 4
Ping Size : 64 bytes
Ping Interval : 1000 Milliseconds
Ping Timeout : 5000 Milliseconds

Figure 7-32:

Factory Default

If you have exhausted all other options and wish to restore the Router to its factory default settings and lose all your settings, click **Yes**.

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



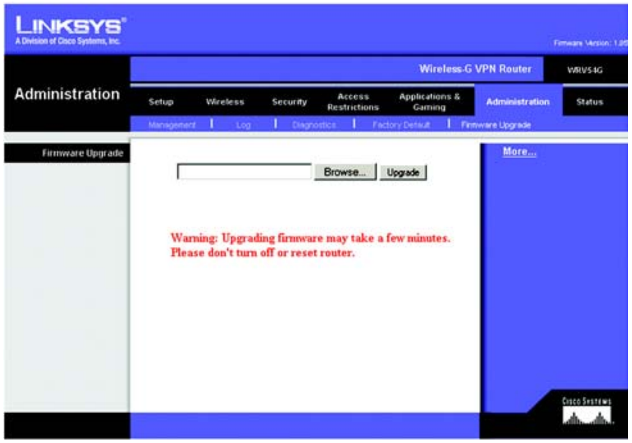
Restore Factory Defaults: ○ Yes ● No

Figure 7-33:

Firmware Upgrade

To upgrade the Router's firmware:

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



Warning: Upgrading firmware may take a few minutes.
Please don't turn off or reset router.

Figure 7-34:

Status

Router

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

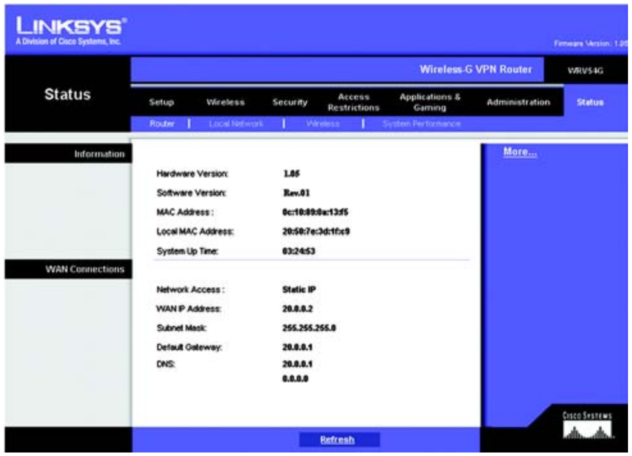
Information

The information displayed is the Hardware Version, Software Version, MAC Address, Local MAC Address, and System Up Time.

WAN Connections

The WAN Connections displayed are the Network Access, WAN IP Address, Subnet Mask, Default Gateway, and DNS.

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



Information

Hardware Version:	1.05
Software Version:	Rev.01
MAC Address :	0c:10:89:0a:13:f5
Local MAC Address:	20:50:7e:3d:1f:c9
System Up Time:	03:24:53

WAN Connections

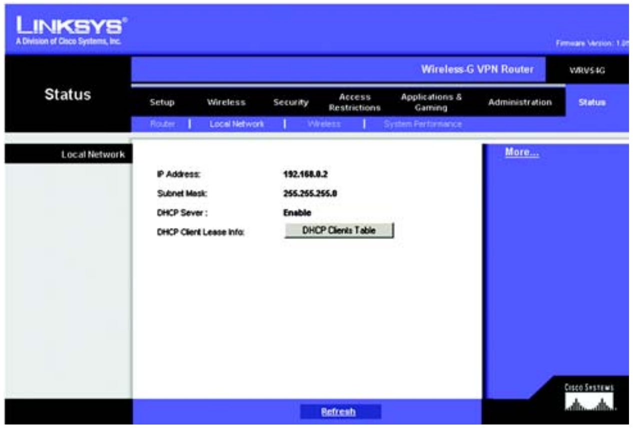
Network Access :	Static IP
WAN IP Address:	20.0.0.2
Subnet Mask:	255.255.255.0
Default Gateway:	20.0.0.1
DNS:	20.0.0.1 0.0.0.0

Figure 7-35:

Local Network

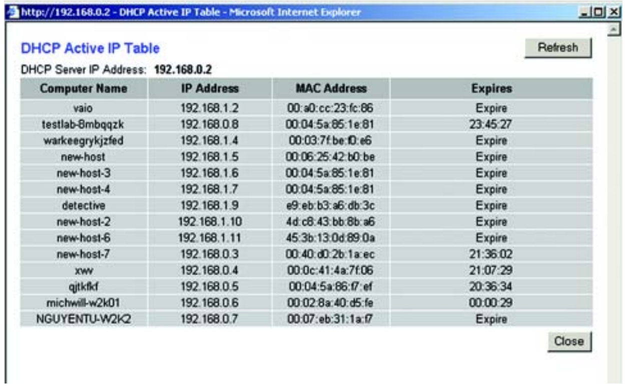
The Local Network information that is displayed is the IP Address, Subnet Mask, DHCP Server, and DHCP Client Lease Info. To view the DHCP Clients Table, click the DHCP Clients button. See Figure 7-36.

The DHCP Active IP Table, Figure 7-37, displays the computer name, IP Address, MAC Address and the expiration time. Click the **Close** button to return to the Local Network screen.



IP Address: 192.168.0.2
Subnet Mask: 255.255.255.0
DHCP Sever : Enable
DHCP Client Lease Info: DHCP Clients Table

Figure 7-36:


http://192.168.0.2 - DHCP Active IP Table - Microsoft Internet Explorer
Refresh
Close

DHCP Active IP Table

DHCP Server IP Address: 192.168.0.2

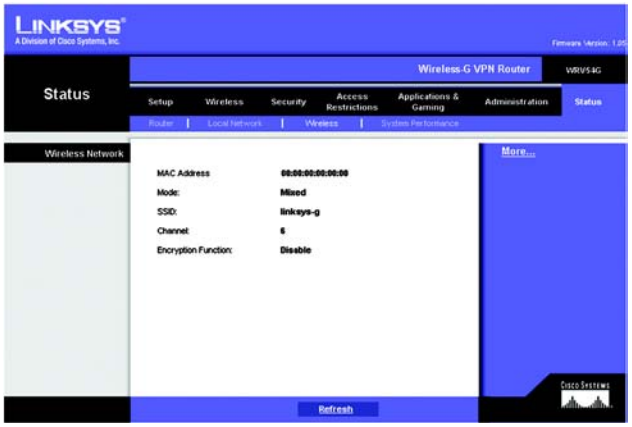
Computer Name	IP Address	MAC Address	Expires
vaio	192.168.1.2	00:a0:cc:23:fc:86	Expire
testlab-8mbqqzk	192.168.0.8	00:04:5a:85:1e:81	23:45:27
warkeegrykjzfed	192.168.1.4	00:03:7f:be:f0:e6	Expire
new-host	192.168.1.5	00:06:25:42:b0:be	Expire
new-host-3	192.168.1.6	00:04:5a:85:1e:81	Expire
new-host-4	192.168.1.7	00:04:5a:85:1e:81	Expire
detective	192.168.1.9	e9:eb:b3:a6:db:3c	Expire
new-host-2	192.168.1.10	4d:c8:43:bb:8b:a6	Expire
new-host-6	192.168.1.11	45:3b:13:0d:89:0a	Expire
new-host-7	192.168.0.3	00:40:d0:2b:1a:ec	21:36:02
xwv	192.168.0.4	00:0c:41:4a:7f:06	21:07:29
qjtkfkf	192.168.0.5	00:04:5a:86:f7:ef	20:36:34
michwill-w2k01	192.168.0.6	00:02:8a:40:d5:fe	00:00:29
NGUYENTU-W2K2	192.168.0.7	00:07:eb:31:1a:f7	Expire

Figure 7-37:

Wireless

The Wireless Network information that is displayed is the MAC Address, Mode, SSID, Channel, and Encryption Function.

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



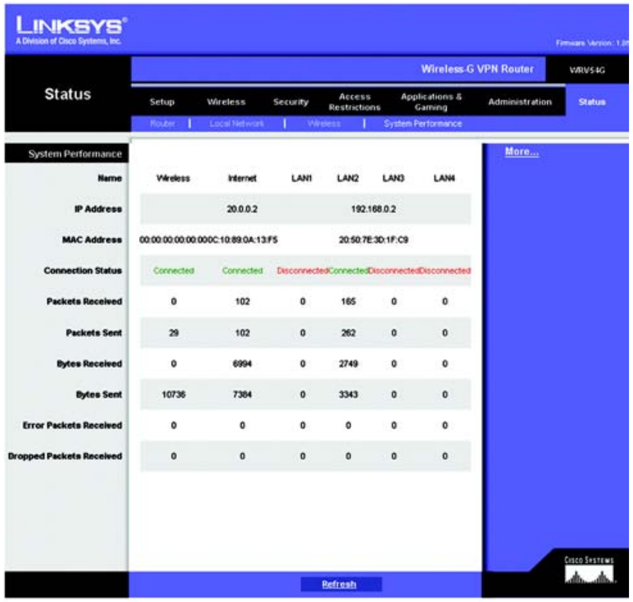
MAC Address	00:00:00:00:00:00
Mode:	Mixed
SSID:	linksys-g
Channel:	6
Encryption Function:	Disable

Figure 7-38:

System Performance

The System Peformance information that is displayed is the Wireless, Internet, and/or LAN information for the IP Address, MAC Address, Connection Status, Packets Received, Packets Sent, Bytes Received, Bytes Sent, Error Packes Received, and Dropped Packets Received.

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



Name	Wireless	Internet	LAN1	LAN2	LAN3	LAN4
IP Address		20.0.0.2	192.168.0.2			
MAC Address	00:00:00:00:00:000C:10:89:0A:13:F5		20:50:7E:3D:1F:C9			
Connection Status	Connected	Connected	Disconnected	Connected	Disconnected	Disconnected
Packets Received	0	102	0	165	0	0
Packets Sent	29	102	0	262	0	0
Bytes Received	0	6994	0	2749	0	0
Bytes Sent	10736	7384	0	3343	0	0
Error Packets Received	0	0	0	0	0	0
Dropped Packets Received	0	0	0	0	0	0

Figure 7-39:

Appendix A: Troubleshooting

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

Common Problems and Solutions

1. ***I need to set a static IP address on a PC.***

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

   For Windows 98 and Me:’

   1. Click Start, Settings, and Control Panel. Double-click Network.
   2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
   3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.   Make sure that each IP address is unique for each PC or network device.
   4. Click the Gateway tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Router. Click the Add button to accept the entry.
   5. Click the DNS tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
   6. Click the OK button in the TCP/IP properties window, and click Close or the OK button for the Network window.
   7. Restart the computer when asked.

2. ***What is Ad-hoc?***

   An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

   For Windows 2000:

   1. Click Start, Settings, and Control Panel. Double-click Network and Dial-Up Connections.
   2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
   3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the Properties button. Select Use the following IP address option.

4. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
5. Enter the Subnet Mask, 255.255.255.0.
6. Enter the Default Gateway, 192.168.1.1 (Router's default IP address).
7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
8. Click the OK button in the Internet Protocol (TCP/IP) Properties window, and click the OK button in the Local Area Connection Properties window.
9. Restart the computer if asked.

For Windows NT 4.0:

1. Click Start, Settings, and Control Panel. Double-click the Network icon.
2. Click the Protocol tab, and double-click TCP/IP Protocol.
3. When the window appears, make sure you have selected the correct Adapter for your Ethernet adapter.
4. Select Specify an IP address, and enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
5. Enter the Subnet Mask, 255.255.255.0.
6. Enter the Default Gateway, 192.168.1.1 (Router's default IP address).
7. Click the DNS tab, and enter the Host and Domain names (e.g., John for Host and home for Domain). Under DNS Service Search Order, click the Add button. Enter the DNS IP address in the DNS Server field, and click the Add button. Repeat this action for all DNS IP addresses given by your ISP.
8. Click the OK button in the TCP/IP Protocol Properties window, and click the Close button in the Network window.
9. Restart the computer if asked.
10.
11.

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click Start and Control Panel.
2. Click the Network and Internet Connections icon and then the Network Connections icon.
3. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.

4. In the This connection uses the following items box, highlight Internet Protocol (TCP/IP). Click the Properties button.
5. Enter a unique IP address that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
6. Enter the Subnet Mask, 255.255.255.0.
7. Enter the Default Gateway, 192.168.1.1 (Router's default IP address).
8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
9. Click the OK button in the Internet Protocol (TCP/IP) Properties window. Click the OK button in the Local Area Connection Properties window.

3. *I want to test my Internet connection.*

Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

Refer to "Chapter 4: Configure the PCs" for details. Make sure Obtain IP address automatically is selected in the settings.

For Windows NT 4.0:

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

4. *Open a command prompt.*

- For Windows 98 and Me, please click Start and Run. In the Open field, type in command. Press the Enter key or click the OK button.
- For Windows NT, 2000, and XP, please click Start and Run. In the Open field, type cmd. Press the Enter key or click the OK button.

5. *In the command prompt, type ping 192.168.1.1 and press the Enter key.*

- If you get a reply, the computer is communicating with the Router.
- If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

D.In the command prompt, type ping followed by your Internet or WAN IP address and press the Enter key. The Internet or WAN IP Address can be found on the Status screen of the Router’s web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter ping 1.2.3.4 and press the Enter key.
• If you get a reply, the computer is connected to the Router.
• If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

E.In the command prompt, type ping www.yahoo.com and press the Enter key.
• If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
• If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. I am not getting an IP address on the Internet with my Internet connection.
A.Refer to “Problem #2, I want to test my Internet connection” to verify that you have connectivity.
B.If you need to register the MAC address of your Ethernet adapter with your ISP, please see “Appendix D: Finding the MAC address and IP Address for Your Ethernet Adapter.” If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of “Chapter 6: The Router’s Web-based Utility” for details.
C.Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of “Chapter 6: The Router’s Web-based Utility” for details on Internet connection settings.
D.Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.
E.Make sure the cable connecting from your cable or DSL modem is connected to the Router’s Internet port. Verify that the Status page of the Router’s web-based utility shows a valid IP address from your ISP.
F.Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router’s web-based utility to see if you get an IP address.

4. I am not able to access the Setup page of the Router’s web-based utility.
A.Refer to “Problem #2, I want to test my Internet connection” to verify that your computer is properly connected to the Router.
B.Refer to “Appendix D: Finding the MAC Address and IP address for Your Ethernet Adapter” to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
C.Set a static IP address on your system; refer to “Problem #1: I need to set a static IP address.”
D.Refer to “Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users).”

5. I can’t get my Virtual Private Network (VPN) working through the Router.
Access the Router’s web interface by going to http://192.168.1.1 or the IP address of the Router, and go to the Security tab. Make sure you have IPsec pass-through and/or PPTP pass-through enabled.

VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.

Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Setup tab

of the web interface. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.

Check the Linksys website for more information at www.linksys.com.

6. I need to set up a server behind my Router and make it available to the public.
To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed. Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.

A.Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Advanced => Port Forwarding tab.
B.Enter any name you want to use for the Customized Application.
C.Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
D.Check the protocol you will be using, TCP and/or UDP.
E.Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
F.Check the Enable option for the port services you want to use. Consider the example below:

CustomizedExternal PortTCPUDPIP AddressEnable
Application
Web server80 to 80X X192.168.1.100X
FTP server21 to 21X192.168.1.101X
SMTP (outgoing)25 to 25XX192.168.1.102X
POP3 (incoming)110 to 110XX192.168.1.102X

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

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

CustomizedExternal PortTCPUDPIP AddressEnable
Application
UT7777 to 27900XX192.168.1.100X
Halflife27015 to 27015XX192.168.1.105X
PC Anywhere5631 to 5631X192.168.1.102X
VPN IPSEC500 to 500X192.168.1.100X

When you have completed the configuration, click the Apply button.

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

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

A.Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Go to the Advanced => Port Forwarding tab.
B.Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
C.Go to the Setup => Security tab.
D.Select Enable next to DMZ. In the DMZ Host IP Address field, enter the IP address of the computer you want exposed to the Internet. This will bypass the NAT technology for that computer. Please refer to "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

Once completed with the configuration, click the Apply button.

9. I forgot my password, or the password prompt always appears when I am saving settings to the Router.
Reset the Router to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

A.Access the Router's web-based utility by going to http://192.168.1.1 or the IP address of the Router. Enter the default password admin, and click the Security tab.
B.Enter a different password in the Router Password field, and enter the same password in the second field to confirm the password.
C.Click the Apply button.
10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.
If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:
A.Click Start, Settings, and Control Panel. Double-click Internet Options.
B.Click the Connections tab.
C.Click the LAN settings button and remove anything that is checked.
D.Click the OK button to go back to the previous screen.
E.Click the option Never dial a connection. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:
A.Start Netscape Navigator, and click Edit, Preferences, Advanced, and Proxies.
B.Make sure you have Direct connection to the Internet selected on this screen.
C.Close all the windows to finish.

11. To start over, I need to set the Router to factory default.
Hold the Reset button for 10 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

12. I need to upgrade the firmware.
In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at www.linksys.com. Follow these steps:

A.Go to the Linksys website at http://www.linksys.com and download the latest firmware.
B.To upgrade the firmware, follow the steps in the System section found in "Chapter 6: The Router's Web-based Utility."

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

A.If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
B.Set a static IP address on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:

IP Address: 192.168.1.50
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1

C.Perform the upgrade using the TFTP program or the Router's web-based utility through its System tab.

14. My DSL service's PPPoE is always disconnecting.
PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

A.To connect to the Router, go to the web browser, and enter http://192.168.1.1 or the IP address of the Router.

B.Enter the password, if asked. (The default password is admin.)
C.On the Setup screen, select the option Keep Alive, and set the Redial Period option at 20 (seconds).
D.Click the Apply button.
E.Click the Status tab, and click the Connect button.
F.You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
G.Click the Apply button to continue.

If the connection is lost again, follow steps E to G to re-establish connection.
15. I can’t access my e-mail, web, or VPN, or I am getting corrupted data from the Internet.
The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you are having some difficulties, perform the following steps:

A.To connect to the Router, go to the web browser, and enter http://192.168.1.1 or the IP address of the Router.
B.Enter the password, if asked. (The default password is admin.)
C.Click the System tab.
D.Look for the MTU option, and select Manual. In the Size field, enter 1492.
E.Click the Apply button to continue.

If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
1462
1400
1362
1300

16. The Diag LED stays lit continuously.
• 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 that the system is working fine. If the LED remains lit after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.
• Check if other PCs work. If they do, ensure that your workstation’s IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
• If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)

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

18. The Full/Col LED keeps flickering continuously.

- Check the Category 5 Ethernet network cable and its RJ-45 connectors.
- There may be interference with other network devices. Try removing other PCs or network devices to see if the problem persists. Eliminate each network device one at a time to determine the cause.

Frequently Asked Questions

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

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

Where is the Router installed on the network?
In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

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

Does the Internet connection of the Router support 100Mbps Ethernet?
The Router's current hardware design supports up to 100Mbps Ethernet on its Internet port; however, the Internet connection speed will vary depending on the speed of your broadband connection. The Router also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.

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 Router to be used with low cost Internet accounts, such as DSL or cable modems, 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 Router support any operating system other than Windows 95, Windows 98, Windows Millennium, 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 Router 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 Router.

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

How can I block corrupted FTP downloads?
If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

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 Router by holding down the reset button until the Diag LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. 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 Router firmware upgrades?
All Linksys firmware upgrades are posted on the Linksys website at www.linksys.com, where they can be downloaded for free. To upgrade the Router’s firmware, use the System tab of the Router’s web-based utility. If the Router’s Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

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

I am not able to get the web configuration screen for the Router. 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, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

What is DMZ Hosting?
Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see “Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter.”

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

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

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

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

Does the Router replace a modem? Is there a cable or DSL modem in the Router? No, the Router must work in conjunction with a cable or DSL modem.

Which modems are compatible with the Router?
The Router is compatible with virtually any cable or DSL modem that supports Ethernet.

What are the advanced features of the Router?
The Router's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.

What is the maximum number of VPN sessions allowed by the Router?
The maximum number depends on many factors. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.
How can I check whether I have static or DHCP IP Addresses?
Consult your ISP to obtain this information.

How do I get mIRC to work with the Router?
Under the Port Forwarding tab, set port forwarding to 113 for the PC on which you are using mIRC.

Can the Router act as my DHCP server?
Yes. The Router has DHCP server software built-in.

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

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

What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11b functions:

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

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

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

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

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

What is ISM band?
The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available

worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?
Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not

tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

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

Will the information be intercepted while it is being transmitted through the air?
WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

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

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

How do I avoid interference?

If you are using the Router and one or more Access Points in close proximity to one another, and they are set on the same channel, interference will be generated. To avoid interference, be sure to set the Router and all Access Points to different channels (frequencies); in other words, assign a unique channel to the Router and each Access Point.

How do I reset the Router?

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

How do I resolve issues with signal loss?

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

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

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

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

How many channels/frequencies are available with the Router?

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

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

Appendix H: Regulatory Information

FCC STATEMENT

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

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

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys Group declares that the Instant Wireless™ Series products included in the Instant Wireless™ Series conform to the specifications listed below, following the provisions of the EMC Directive 89/336/EEC and Low Voltage Directive 73/23/EEC:

ETS 300-826, 301 489-1 General EMC requirements for Radio equipment.

EN 609 50 Safety

ETS 300-328-2 Technical requirements for Radio equipment.

Appendix G: Warranty Information

LIMITED WARRANTY

Linksys warrants to the original end user purchaser ("You") that, for a period of [ ], (the "Warranty Period") Your Linksys product will be free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys's entire liability under this warranty will be for Linksys at its option to repair or replace the product or refund Your purchase price less any rebates.

If the product proves defective during the 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. You are responsible for shipping defective products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

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

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT.

The foregoing limitations will apply even if any warranty or remedy provided under this Section fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

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

Appendix F: Specifications

Standards	IEEE 802.3, 802.3u, 802.11a and 802.11b	
Channels	802.11a	8 Channels (US, Canada)
	802.11b	11 Channels (US, Canada)
		13 Channels (Europe)
		14 Channels (Japan)
Ports/Buttons	One 10/100 RJ-45 Port, One Power Port, One Reset Button, One Power Switch	
Cabling Type	UTP CAT 5 or better	
Data Rate	Up to 54Mbps (up to 72 Mbps in Turbo Mode)	
Transmit Power	802.11a	18dBm
	802.11b	17dBm
LEDs	Power, Diag 802.11a: Act, Link 802.11b: Act, Link LAN: Link/Act, Full/Col, 100	
Dimensions (L x W x H)	7.31" x 1.88" x 6.88" (186 mm x 48 mm x 175 mm)	
Antenna Height	4.5" (114 mm)	
Unit Weight	15 oz. (0.42 kg)	
Power	External, 5V DC, 2.5A	
Certifications	FCC, Canada	

Appendix E: Glossary

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

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

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

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

Adapter - This is a device that adds network functionality to your PC.

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

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

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

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

Bit - A binary digit.

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

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

Broadband - An always-on, fast Internet connection.

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

Appendix D: Windows Help

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

TCP/IP

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

Shared Resources

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

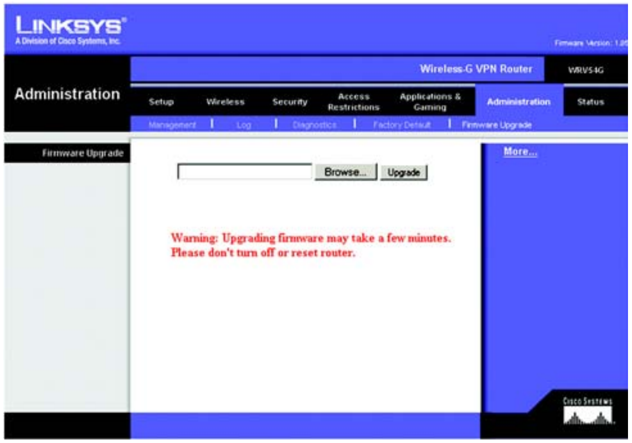
Network Neighborhood/My Network Places

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

Appendix C: Upgrading Firmware

The Access Point's firmware is upgraded through the Web-Utility's Firmware Upgrade tab from the Administration tab. Follow these instructions:

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



Warning: Upgrading firmware may take a few minutes.
Please don't turn off or reset router.

Figure C-1: Upgrade Firmware

Appendix B: Wireless Security

A Brief Overview

Whenever data - in the form of files, emails, or messages - is transmitted over your wireless network, it is open to attacks. Wireless networking is inherently risky because it broadcasts information on radio waves. Just like signals from your cellular or cordless phone can be intercepted, signals from your wireless network can also be compromised. What are the risks inherent in wireless networking? Read on.

What Are The Risks?

Computer network hacking is nothing new. With the advent of wireless networking, hackers use methods both old and new to do everything from stealing your bandwidth to stealing your data. There are many ways this is done, some simple, some complex. As a wireless user, you should be aware of the many ways they do this.

Every time a wireless transmission is broadcast, signals are sent out from your wireless PC or router, but not always directly to its destination. The receiving PC or router can hear the signal because it is within that radius. Just as with a cordless phone, cellular phone, or any kind of radio device, anyone else within that radius, who has their device set to the same channel or bandwidth can also receive those transmission.

Wireless networks are easy to find. Hackers know that, in order to join a wireless network, your wireless PC will typically first listen for "beacon messages". These are identifying packets transmitted from the wireless network to announce its presence to wireless nodes looking to connect. These beacon frames are unencrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier) and the IP address of the network PC or router. The SSID is analogous to the network's name. With this information broadcast to anyone within range, hackers are often provided with just the information they need to access that network.

One result of this, seen in many large cities and business districts, is called "Warchalking". This is the term used for hackers looking to access free bandwidth and free Internet access through your wireless network. The marks they chalk into the city streets are well documented in the Internet and communicate exactly where available wireless bandwidth is located for the taking.

Even keeping your network settings, such as the SSID and the channel, secret won't prevent a hacker from listening for those beacon messages and stealing that information. This is why most experts in wireless networking strongly recommend the use of WEP (Wireless Equivalent Privacy). WEP encryption scrambles your wireless signals so they can only be recognized within your wireless network.

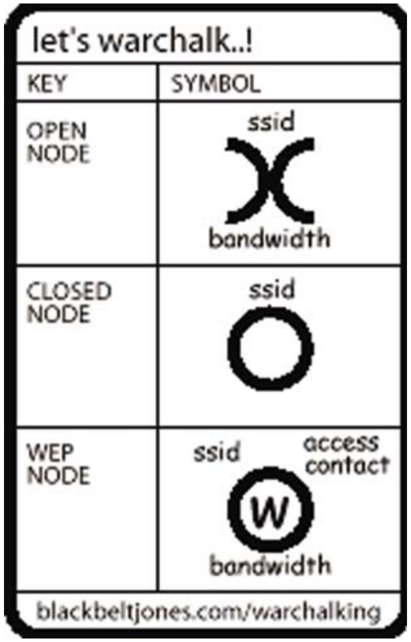


Figure B-1: Warchalking

Chapter I: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:	800-546-5797 (LINKSYS)
Or fax your request in to:	949-261-8868
If you experience problems with any Linksys product, you can call us at:	800-326-7114
Don't wish to call? You can e-mail us at:	support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-261-1288

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.