The Administration Tab

Management

The Management screen, shown in Figure 6-30, 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.

- User Name. Enter the default **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.
- Get Community. Enter the password that allows read-only access to the Router's SNMP information.
- Set Community. Enter the password that allows read/write access to the Router's SNMP information.
- SNMP Trusted Host. You can restrict access to the Router's SNMP information by IP address. Enter the IP address in the SNMP Trusted Host field. If this field is left blank, then access is permitted from any IP address.

Figure 6-30: Management

- SNMP Trap-Community. Enter the password required by the remote host computer that will receive trap messages or notices sent by the Router.
- SNMP Trap-Destination. Enter the IP address of the remote host computer that will receive the trap messages.

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 6-31, 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.

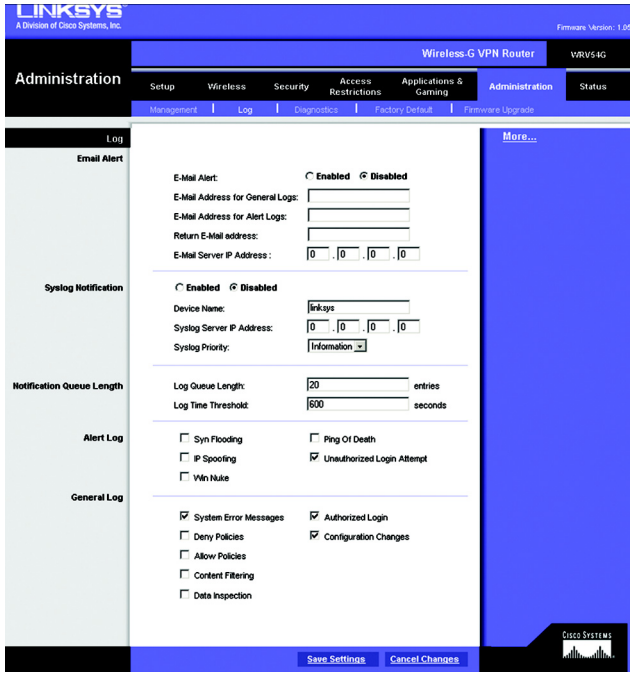

Figure 6-31: Log

- Syslog Server IP Address. Enter the **IP Address of the Syslog Server**.
- Syslog Priority. Select the **priority** from the drop-down list.

Notification Queue 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 type of attacks that you want to be alerted to. Select Syn Flooding, IP Spoofing, Win Nuke, Ping of Death, or Unauthorized Login attempt.

General Log.

Select the type of activity you would like to log. 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 (See Figure 6-32.)

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 packets.

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 **Clear Result** button to clear the results. The results of the test will display in the window.

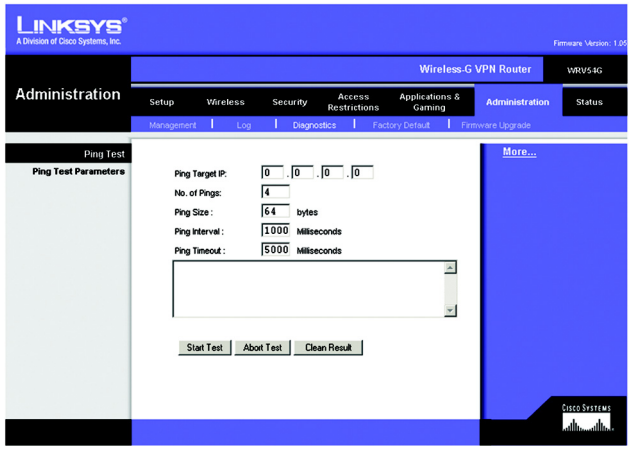

Figure 6-32: Ping Test

Factory Default (See Figure 6-33.)

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.

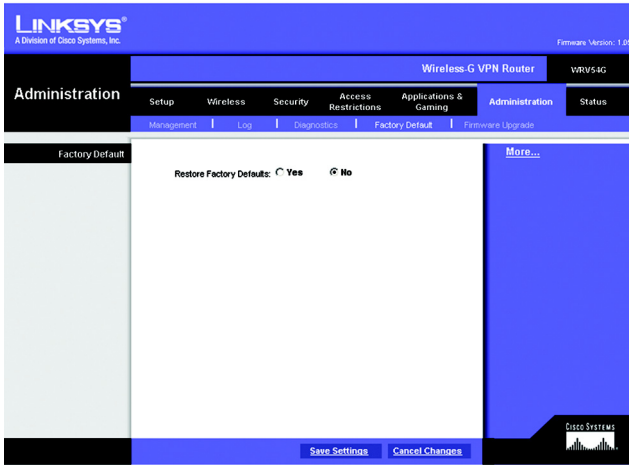

Figure 6-33: Factory Default

Firmware Upgrade (See Figure 6-34.)

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.

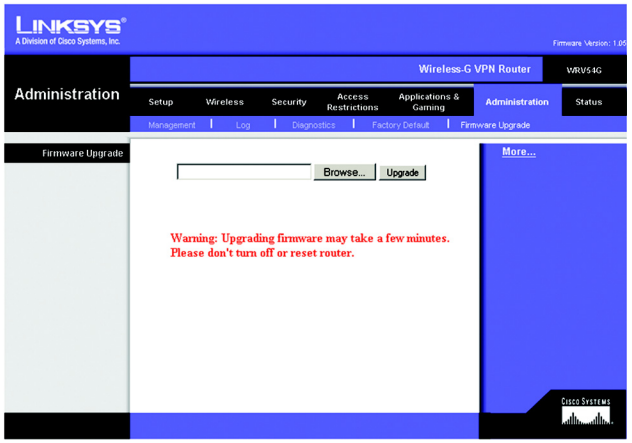

Figure 6-34: Firmware Upgrade

Status

Router

This screen displays information about your Router and its WAN (Internet) Connections. (See Figure 6-35.)

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.

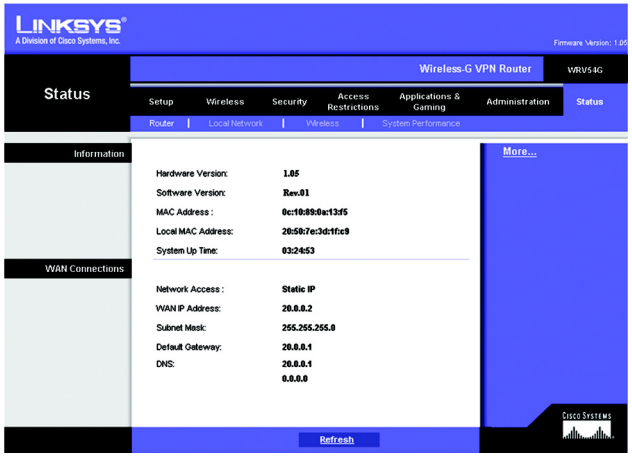

Figure 6-35: Router

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 6-36.

The DHCP Active IP Table, Figure 6-37, displays the computer name, IP Address, MAC Address and the expiration time. Click the **Close** button to return to the Local Network screen.

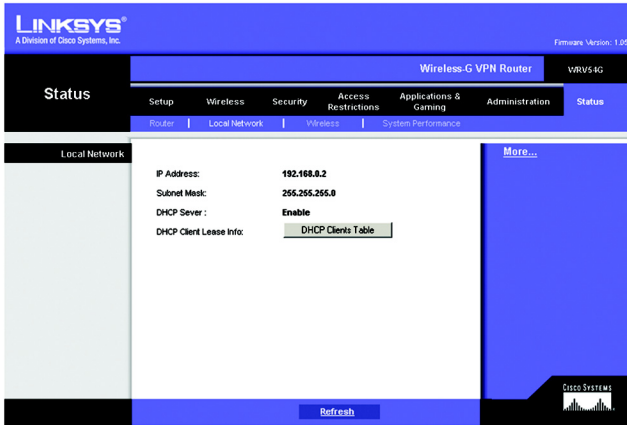

Figure 6-36: Local Network

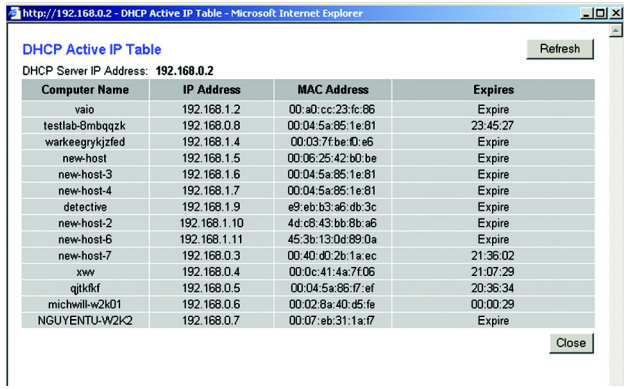

Figure 6-37: DHCP Active IP Table

Wireless

The Wireless Network information that is displayed is the MAC Address, Mode, SSID, Channel, and Encryption Function. (See Figure 6-38.)

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

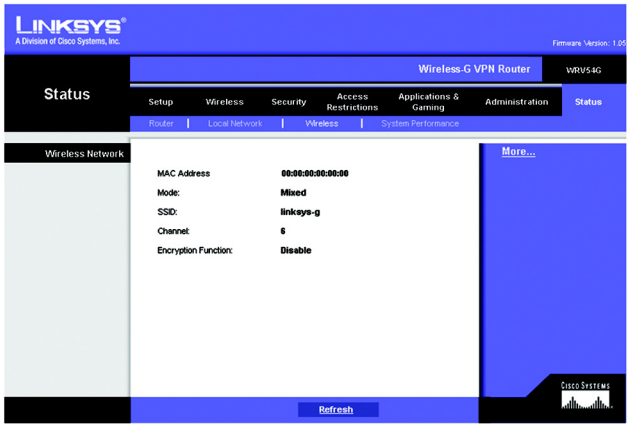

Figure 6-38: Wireless

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. (See Figure 6-39.)

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

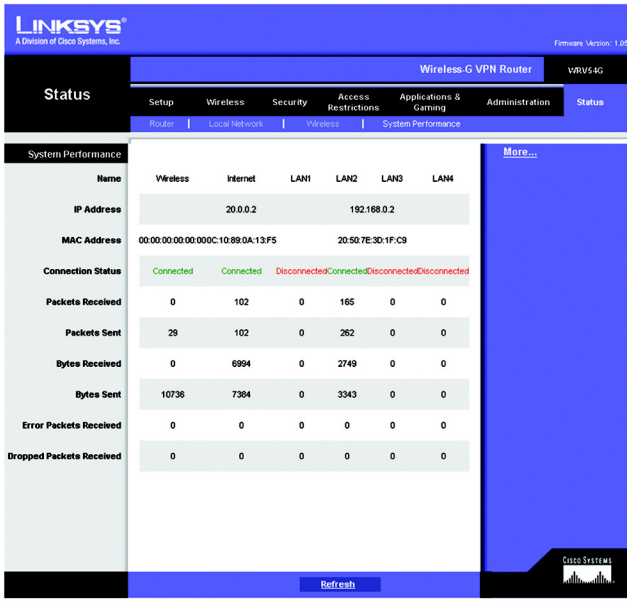

Figure 6-39: System Performance

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. 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.
   - 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.
     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 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.
  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.

2. I want to test my Internet connection.

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

B Open a command prompt.

For Windows 98 and Me:

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

For Windows NT, 2000, and XP:

- Click **Start** and **Run**. In the Open field, type cmd. Press the **Enter** key or click the **OK** button. In the command prompt, type ping 192.168.1.1 and press the Enter key.
- If you get a reply, the computer is communicating with the 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.

C 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.

D In the command prompt, type ping www.yahoo.com and press the **Enter** key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

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

- Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
  1. 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.
  2. 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.
  3. Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.
  4. 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.
  5. 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.

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

5. I can't get my Virtual Private Network (VPN) working through the 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.
  1. 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 Applications and Gaming => Port Forwarding tab.

2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the 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.
6. Check the Enable option for the port services you want to use. Consider the example below:

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

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

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

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the 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:

1. Access the Router's web interface by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications and Gaming => Port Forwarding tab.
2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the 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.
6. Check the **Enable** option for the port services you want to use. Consider the example below:

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

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

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

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one 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:
  1. 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 Applications and Gaming => DMZ tab.
  2. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
- Once completed with the configuration, click the **Save Settings** button.

9. I forgot my password, or the password prompt always appears when I am saving settings to the 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:
  1. 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 **Administrations** => **Management** tab.
  2. Enter a different password in the Router Password field, and enter the same password in the second field to confirm the password.
  3. Click the **Save Settings** button.

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

If you have proxy settings, you need to disable these on your computer. Because the 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:
  1. Click **Start, Settings**, and **Control Panel**. Double-click Internet Options.
  2. Click the **Connections** tab.
  3. Click the **LAN settings** button and remove anything that is checked.
  4. Click the **OK** button to go back to the previous screen.
  5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.
- For Netscape 4.7 or higher:
  1. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
  2. Make sure you have Direct connection to the Internet selected on this screen.
  3. Close all the windows to finish.

11. To start over, I need to set the 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:
  1. Go to the Linksys website at http://www.linksys.com and download the latest firmware.
  2. 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 Power LED is flashing.

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

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the 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
- Perform the upgrade using the TFTP program or the Router's web-based utility through its Administration tab.

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

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

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.
  1. To connect to the Router, go to the web browser, and enter http://192.168.1.1 or the IP address of the Router.
  2. Enter the password, if asked. (The default password is admin.)
  3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
  4. Click the **Save Settings** button.
  5. Click the **Status** tab, and click the **Connect** button.
  6. 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.
- Click the **Save Settings** button to continue.
- If the connection is lost again, follow steps 1- 6 to re-establish connection.

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

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492.

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

16. The Power LED flashes continuously.

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

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

- Check if other 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**.

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 98SE, Windows Millennium, Windows 2000, or Windows XP?

Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the 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 Power 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.

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

What IEEE 802.11b 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 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 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.

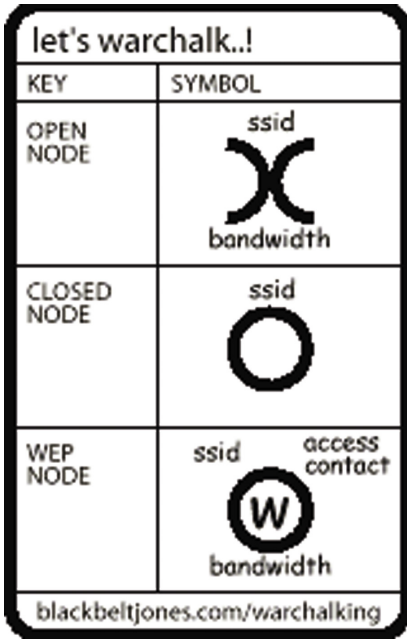

Figure B-1: Warchalking

But even WEP has its problems. WEP's encryption algorithm is referred to as "simple", which also means "weak", because the technology that scrambles the wireless signal isn't too hard to crack for a persistent hacker.

There are five common ways that hackers can break into your network and steal your bandwidth as well as your data. The five attacks are popularly known as:

1. Passive Attacks
2. Jamming Attacks
3. Active Attacks
4. Dictionary-building or Table Attacks
5. Man-in-the-Middle Attacks

Passive Attacks

There's no way to detect a passive attack because the hacker is not breaking into your network. He is simply listening (eavesdropping, if you will) to the information your network broadcasts. There are applications easily available on the Internet that can allow a person to listen into your wireless network and the information it broadcasts. Information such as MAC addresses, IP addresses, usernames, passwords, instant message conversations, emails, account information, and any data transmitted wirelessly, can easily be seen by someone outside of your network because it is often broadcast in clear text. Simply put, any information transmitted on a wireless network leaves both the network and individual users vulnerable to attack. All a hacker needs is a "packet sniffer", software available on the Internet, along with other freeware or shareware hacking utilities available on the Internet, to acquire your WEP keys and other network information to defeat security.

Jamming Attacks

Jamming Attacks, when a powerful signal is sent directly into your wireless network, can effectively shut down your wireless network. This type of attack is not always intentional and can often come about simply due to the technology. This is especially possible in the 2.4 GHz frequency, where phones, baby monitors, and microwave ovens can create a great deal of interference and jam transmissions on your wireless network. One way to resolve this is by moving your wireless devices into the 5 GHz frequency, which is dedicated solely to information transmissions.

Active Attacks

Hackers use Active Attacks for three purposes: 1) stealing data, 2) using your network, and 3) modifying your network so it's easier to hack in the next time.

In an Active Attack, the hacker has gained access to all of your network settings (SSID, WEP keys, etc.) and is in your network. Once in your wireless network, the hacker has access to all open resources and transmitted data on the network. In addition, if the wireless network's router is connected to a switch, the hacker will also have access to data in the wired network.

Further, spammers can use your Internet connection and your ISP's mail server to send tens of thousands of e-mails from your network without your knowledge.

Lastly, the hacker could make hacking into your network even easier by changing or removing safeguards such as MAC address filters and WEP encryption. He can even steal passwords and user names for the next time he wants to hack in.

Dictionary-Building or Table Attacks

Dictionary-building, or Table attacks, is a method of gaining network settings (SSID, WEP keys, etc.) by analyzing about a day's worth of network traffic, mostly in the case of business networks. Over time, the hacker can build up a table of network data and be able to decrypt all of your wireless transmissions. This type of attack is more effective with networks that transmit more data, such as businesses.

Man-in-the-Middle Attacks

A hacker doesn't need to log into your network as a user - he can appear as one of the network's own routers, setting himself up as the man-in-the-middle. To do this, the hacker simply needs to rig an router with your network's settings and send out a stronger signal that your router. In this way, some of your network's PCs may associate with this rogue router, not knowing the difference, and may begin sending data through it and to this hacker.

The trade-off for the convenience and flexibility wireless networking provides is the possibility of being hacked into through one of the methods described here. With wireless networks, even with WEP encryption, open to the persistent hacker, how can you protect your data? The following section will tell you how to do just that.

Maximizing Wireless Security

Security experts will all tell you the same thing: Nothing is guaranteed. No technology is secure by itself. An unfortunate axiom is that building the better mousetrap can often create a better mouse. This is why, in the

examples below, your implementation and administration of network security measures is the key to maximizing wireless security.

No preventative measure will guarantee network security but it will make it more difficult for someone to hack into your network. Often, hackers are looking for an easy target. Making your network less attractive to hackers, by making it harder for them to get in, will make them look elsewhere.

How do you do this? Before discussing WEP, let's look at a few security measures often overlooked.

1) Network Content

Now that you know the risks assumed when networking wirelessly, you should view wireless networks as you would the Internet. Don't host any systems or provide access to data on a wireless network that you wouldn't put on the Internet.

2) Network Layout

When you first lay out your network, keep in mind where your wireless PCs are going to be located and try to position your router towards the center of that network radius. Remember that access points transmit indiscriminately in a radius; placing an access point at the edge of the physical network area reduces network performance and leaves an opening for any hacker smart enough to discover where the router is transmitting.

This is an invitation for a man-in-the-middle attack, as described in the previous section. To perform this type of attack, the hacker has to be physically close to your network. So, monitoring both your network and your property is important. Furthermore, if you are suspicious of unauthorized network traffic, most wireless products come with a log function, with which you can view activity on your network and verify if any unauthorized users have had access.

3) Network Devices

With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. If they get into the hands of a hacker, so do all of your settings. So keep an eye on them.

4) Administrator passwords

Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

5) SSID

There are a few things you can do to make your SSID more secure:

a. Disable Broadcast

b. Make it unique

c. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. This is a option for convenience, allowing anyone to log into your wireless network. In this case, however, anyone includes hackers. So don't broadcast the SSID.

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

Changing your SSID regularly will force any hacker attempting to gain access to your wireless network to start looking for that new SSID.

With these three steps in mind, please remember that while SSIDs are good for segmenting networks, they fall short with regards to security. Hackers can usually find them quite easily.

6) MAC addresses

Enable MAC address filtering if your wireless products allow it. MAC address filtering will allow you to provide access to only those wireless nodes with certain MAC addresses. This makes it harder for a hacker using a random MAC address or spoofing (faking) a MAC address.

7) Firewalls

You can use the same firewall technology to protect your wired network from hackers coming in through your wireless network as you did for the Internet. The firewall will protect your network from any transmissions entering via your wireless network.

8) WEP

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

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is

not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

Programs exist on the Internet that are designed to defeat WEP. The best known of these is AirSnort. In about a day, AirSnort can analyze enough of the wireless transmissions to crack the WEP key. Just like a dictionary-building attack, the best prevention for these types of programs is by not using static settings, periodically changing WEP keys, SSID, etc.

There are several ways that WEP can be maximized:

a) Use the highest level of encryption possible

b) Use multiple WEP keys

c) Change your WEP key regularly

Current encryption technology offers 64-bit and 128-bit WEP encryption. If you are using 64-bit WEP, swap out your old wireless units for 128-bit encryption right away. Where encryption is concerned, the bigger and more complex, the better. A WEP key is a string of hexadecimal characters that your wireless network uses in two ways. First, nodes in your wireless network are identified with a common WEP key. Second, these WEP keys encrypt and decrypt data sent over your wireless network. So, a higher level of security ensures that hackers will have a harder time breaking into your network.

Setting one, static WEP key on your wireless network leaves your network open the threats even as you think it is protecting you. While it is true that using a WEP key increases wireless security, you can increase it further by using multiple WEP keys.

Keep in mind that WEP keys are stored in the firmware of wireless cards and access points and can be used to hack into the network if a card or access point falls into the wrong hands. Also, should someone hack into your network, there would be nothing preventing someone access to the entire network, using just one static key.

The solution, then, is to segment your network up into multiple groups. If your network had 80 users and you used four WEP keys, a hacker would have access to only ¼ of your wireless network resources. In this way, multiple keys reduce your liability.

Finally, be sure to change your WEP key regularly, once a week or once a day. Using a "dynamic" WEP key, rather than one that is static, makes it even harder for a hacker to break into your network and steal your resources.

2.4GHz/802.11b and 802.11g WEP Encryption

WEP encryption for the Wireless-G VPN Broadband Router is configured through the Web-Utility's Wireless tab. Enable **WEP** from this tab and click the **Edit WEP Setting**s button, which will open the WEP screen, shown in Figure B-3.

From this screen, you can select the type of WEP encryption to use as well as set the WEP Key for that encryption.

Select which WEP key (1-4) will be used when the Router sends data, then select that number as the Default Transmit Key. Make sure the receiving device is using the same key.

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.

If you wish to use a WEP Passphrase, it can be a maximum of 16 alphanumeric characters. This passphrase may not work with non-Linksys products due to possible incompatibility with other vendors' passphrase generators. The WEP Key can be generated using your Passphrase or you can enter it manually.

If you wish to enter the WEP Key manually, type the key into the appropriate Key field on the left. The WEP key must consist of the letters "A" through "F" and the numbers "0" through "9" and should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption. All points in your wireless network must use the same WEP key to utilize WEP encryption.

Once the Passphrase is entered, click the **Generate** key to generate a WEP key.

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

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

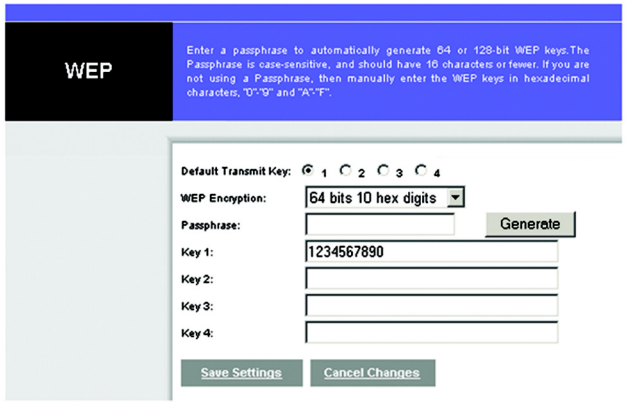

Figure B-2: WEP

Appendix C: Configuring IPSec between a Windows 2000 PC and the Router

Introduction

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

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

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

NOTE: Keep a record of any changes you make. Those changes will be identical in the Windows "secpol" application and the Router's Web-Based Utility.

Environment

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

Windows 2000 or Windows XP
IP Address: 140.111.1.2 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

BEFSX41

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

Subnet Mask: 255.255.255.0
LAN IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0