

- **Starting MAC Filter.** This option will allow you to prevent wireless users on your network from accessing the Router's functions.

Clicking the **Active MAC Table** button will display the MAC Addresses of all users on your wireless network. Addresses in green show access to the Router, while addresses in red do not have access.

To filter users, click the **Edit MAC Filter Setting** button.

Click the **Wireless MAC Entry** drop-down menu to select a range of entries for your network. From within this range, select the entry for which you'd like to manage access. Verify that the appropriate **MAC Address** is entered into the MAC Address field. Click the **Filter** checkbox beside that MAC Address. Now, this user will be prevented from accessing the Router. All other users will have access. To allow only that user and deny access to all others, leave **Filter** unchecked.

Click the **Apply** button to set these changes or **Undo** if you do not wish these changes to go into effect.

To apply any of the settings you've changed on this page, click the **Apply** button. To cancel any values you've entered on this page, click the **Cancel** button. If you should need any further information about anything on this screen, click the **Help** button.

Appendix A: Troubleshooting

Common Problems and Solutions

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems regarding the installation and operation of the Router. If your situation is described here, the problem should be solved by applying the corresponding solution. If you can't find an answer here, check the Network Everywhere website at www.netwerkeverywhere.com.

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

The Router, by default, assigns an IP address range of 192.168.1.100 to 192.168.1.149 using the DHCP server on the Router. To set a static IP address, you can only use the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Each PC or network device that uses TCP/IP must have a unique address to identify itself in a network. If the IP address is not unique to a network, Windows will generate an IP conflict error message. You can assign a static IP address to a PC by performing the following steps:

For Windows 98 SE and Me:

- Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
- 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.
- 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.
- 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.
- 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.
- Click the **OK** button in the *TCP/IP properties* window, and click **Close** or the **OK** button for the Network window.
- Restart the computer when prompted.

For Windows 2000:

- A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
- B. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
- C. 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.
- D. 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.
- E. Enter the Subnet Mask, **255.255.255.0**.
- F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
- G. 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.
- H. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
- I. 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.

- A. Click **Start** and **Control Panel**.
- B. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
- C. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
- D. In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
- E. 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.
- F. Enter the Subnet Mask, **255.255.255.0**.
- G. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
- H. 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.

- I. 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 SE and Me:

Refer to your Ethernet adapter's documentation for details. Make sure **Obtain IP address automatically** is selected in the settings.

For Windows 2000:

- Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
- Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
- In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
- Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
- 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.

- Click **Start** and **Control Panel**.
- Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
- Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
- In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

- Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
 - Restart the computer if asked.
- B. Open a command prompt.
- For **Windows 98 SE** 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 2000** and **XP**, please click **Start** and **Run**. In the Open field, type **cmd**. Press the **Enter** key or click the **OK** button.
- C. 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 IP address and press the **Enter** key. The WAN (or Internet) IP Address can be found in the web interface of the Router. For example, if your 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 MAC Address Clone section of “Chapter 5: The Router’s Web-based Utility” for details.

- C. Make sure you are using the right Internet 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 5: The Router’s Web-based Utility” for details on Internet settings.
- D. Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link 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 interface shows a valid IP address from your ISP.
- F. Turn off the computer, Router, and Broadband 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 Router’s web interface Setup page.

- 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 **Advanced => Filter** 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 Network Everywhere website for more information at www.networkeverywhere.com.

6. I need to set up a server behind my Router.

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 => Forwarding** tab and click the **View Port Range Forwarding** button.
- B. Enter any **name** you want to use for the Customized Application.
- C. Enter the **Ext. 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:

Customized Application	Ext. 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 **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 => Forwarding** tab and click the **View Port Range Forwarding** button.
- B. Enter any **name** you want to use for the Customized Application.
- C. Enter the **Ext. 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:

Customized Application	Ext. 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 **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:

- 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 => Forwarding** tab and click the **View Port Range Forwarding** button.
- Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
- Click the **DMZ Host** tab.
- Enter the Ethernet adapter's **IP address** of the computer you want exposed to the Internet. This will bypass the NAT firewall 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 saving settings to the Router.

Reset the Router to factory default by pressing the **Reset** button for 30 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

- Access the Router's web interface by going to **http://192.168.1.1** or the **IP address** of the Router. Enter the default password **admin**, and click the **Password** tab.
- Enter a **different password** in the Router Password field, and enter this new password in the second field to confirm the password.
- 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:

- Click **Start, Settings**, and **Control Panel**. Double-click **Internet Options**.
- Click the **Connections** tab.
- Click the **LAN settings** button and remove anything that is checked.
- Click the **OK** button to go back to the previous screen.
- Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:

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

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

Hold the **Reset** button for up to 30 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 Network Everywhere website and download the latest firmware at www.networkeverywhere.com. Follow these steps:

- A. Go to the Linksys website at **<http://www.networkeverywhere.com>** and download the latest firmware.
- B. To upgrade the firmware, follow the steps in the Help section found in “Chapter 5: 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 Help 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. In the Setup tab, 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 email, 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 **Advanced => Filter** tab.
- D. Look for the MTU option, and select **Enable**. 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. I need to use port triggering.

Port triggering looks at the outgoing port services used and will trigger the Router to open a specific port, depending on which port an Internet application uses. Follow these 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 **Advanced => Forwarding** tab, and click the **Port Trigger** button.
- D. Enter any **name** you want to use for the Application Name.
- E. Enter the **Triggered Port Range**. Check with your Internet application provider for more information on which outgoing port services it is using.
- F. Enter the **Incoming Port Range**. Check with your Internet Application provider for more information on which incoming port services are required by the Internet application.

17. The Diag LED stays lit continuously.

- The Diag LED lights up when the device is first powered on. Then, 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.

18. 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 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 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**.

19. The Full/Col LED keeps flickering continuously.

- Check the Category 5 Ethernet 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 Internet to LAN.

What is Network Address Translation and what is it used for? Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the 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 98 SE, Windows 2000, Windows NT, or Windows XP? Yes, but Network Everywhere 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 (8080 usually works well but is used for remote admin. You may have to disable this.), and then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the 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.

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 for about 30 seconds. 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 Network Everywhere website, www.netwerkeverywhere.com.

How will I be notified of new Router firmware upgrades? All Network Everywhere firmware upgrades are posted on the Linksys website at www.netwerkeverywhere.com, where they can be downloaded for free. The Router’s firmware can be upgraded with TFTP programs. 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, this version of 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 IP Filtering, Port Range Forwarding, Dynamic Routing, Static Routing, DMZ hosting, and MAC Address Cloning.

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 Range 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? The IEEE 802.11b Wireless LAN standards subcommittee formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufacturers to communicate.

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

- CSMA/CA plus Acknowledge protocol

- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is BSS ID? A specific Ad-hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

What is SSID? An Infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an Extended Service Set (ESS). Users within an ESS could roam freely between BSSs while maintaining a continuous connection to the wireless network stations and Access Points.

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. 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 variations, 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.

ered. 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.

Would the information be intercepted while transmitting on 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, the WLAN series offers the encryption function (WEP) to enhance security and access control. Users can set it up depending upon their needs.

What is WEP? WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40/64 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 on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

**If your questions are not addressed here,
refer to the Network Everywhere website,
www.networkeverywhere.com.**

Appendix B: How to Ping Your ISP's E-mail and Web Addresses

Virtually all Internet addresses are configured with words or characters (i.e., www.networkeverywhere.com, www.yahoo.com, etc.) In actuality, however, these Internet addresses are assigned to IP addresses, which are the true addresses on the Internet.

IP and web addresses, however, can sometimes be long and hard to remember. Because of this, certain ISPs will shorten their server addresses to single words or codes on their users' web browser or e-mail configurations. If your ISP's e-mail and web server addresses are configured with single words ("www," "e-mail," "home," "pop3," etc.) rather than whole Internet Addresses or IP Addresses, the Router may have problems sending or receiving mail and accessing the Internet. This happens because the Router has not been configured by your ISP to accept their abbreviated server addresses.

The solution is to determine the true web addresses behind your ISP's code words. You can determine the IP and web addresses of your ISP's servers by "pinging" them.



Note: If you don't have your ISP's web and e-mail IP addresses, you must either get them from your ISP or follow these steps prior to connecting the Router to your network.

Step One: Pinging an IP Address

The first step to determining your ISP's web and e-mail server address is to ping its IP address.

1. **Power on the computer and the cable or DSL modem**, and restore the network configuration set by your ISP if you have since changed it.
2. **Click Start**, then **Run**, and type "command." This will bring up the DOS window.

3. **At the DOS command prompt**, type “ping mail” (assuming that the location for which you’re trying to find an IP address is configured as “mail”). Press **Enter**. Information such as the following data, taken from a ping of Microsoft Network’s e-mail server, will be displayed.

```
C:\>ping mail

Pinging mail [24.53.32.4] with 32 bytes of data:

Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128

Ping statistics for 24.53.32.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
    loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4. **Write down the IP address returned by the ping command.** (In the example above: 24.53.32.4.) This IP address is the actual IP address of the server “mail,” or any other word or value you have pinged.

Step Two: Pinging for a Web Address

While the IP address returned above would work as your e-mail server address, it may not be permanent. IP addresses change all the time. Web addresses, however, usually don’t. Because of this, you’re likely to have fewer problems by configuring your system with web addresses rather than IP addresses. Follow the instructions below to find the web address assigned to the IP address you just pinged.

1. **At the DOS command prompt**, type “ping -a 24.53.32.4,” where 24.53.32.4 is the IP address you just pinged. Information such as the following data will be displayed.

```
C:\>ping -a 24.53.32.4

Pinging mail.msnv3.occa.home.com [24.53.32.4] with
32 bytes of data:

Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127

Ping statistics for 24.53.32.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
    loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. **Write down the web address returned by the ping command** (in the example above: mail.msnv3.occa.home.com.). This web address is the web address assigned to the IP address you just pinged. While the IP address of “mail” could conceivably change, it is likely that this web address will not.
3. **Replace your ISP’s abbreviated server address** with this extended web address in the corresponding Internet application (web browser, e-mail application, etc.).

Once you have replaced the brief server address with the true server address, the Router should have no problem accessing the Internet through that Internet application.

Appendix C: Configuring Wireless Security



Note: WEP encryption is an additional data security measure and not essential for router operation.

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

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

Make sure your wireless network is functioning before attempting to configure WEP encryption.

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

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

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



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

Wireless-B Broadband Router

The following steps will show you how to utilize WEP encryption

1. From the Web-based Utility's Setup tab, select **Mandatory** under the WEP section.
2. Press the **WEP Key Setting** button to set the WEP Encryption type and level.

3. The screen displayed in Figure C-1 may appear, verifying that you are enabling WEP Encryption. Press the **OK** button to continue.

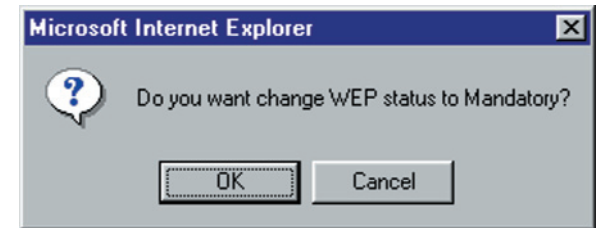


Figure C-1

4. This will display the screen shown in Figure C-2. From this screen, you will choose your WEP Encryption settings.

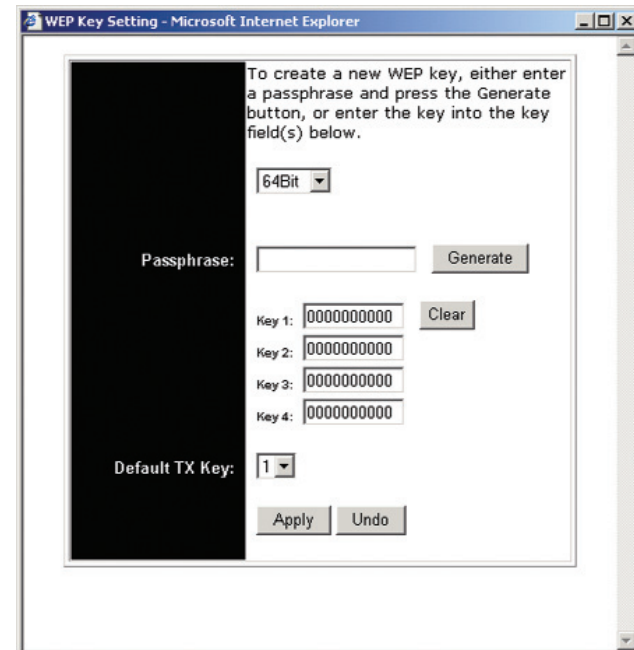


Figure C-2

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



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

The WEP Encryption key is generated in one of two ways:

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

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

2. You may enter the encryption key manually.

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

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



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

Configuring Wireless Security in Windows XP

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

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

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

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

1. As shown in Figure C-3, click the **Start** button and go to the **Control Panel**.



Figure C-3

- In the “Control Panel” window, click the **Network and Internet Connections** icon, shown in Figure C-4.

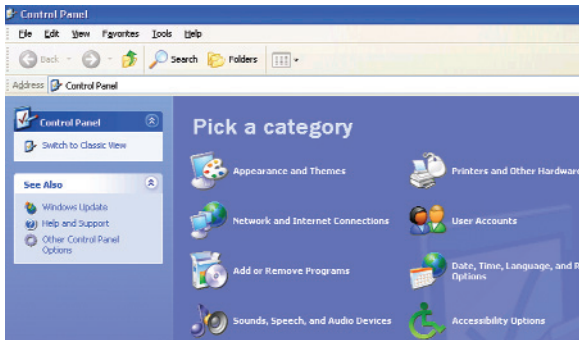


Figure C-4

- Click the **Network Connections** icon, shown in Figure C-5.

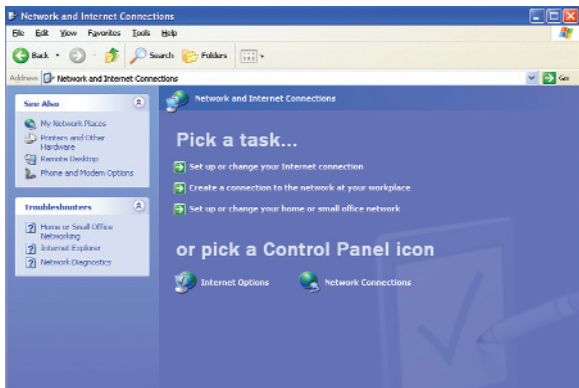


Figure C-5

- The “Network Connections” window will appear, as shown in Figure C-6. Under LAN or High-Speed Internet you will see all Network cards that are installed and operating in your computer. Double-click the **Wireless Network Connection** icon associated with your wireless adapter.

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

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

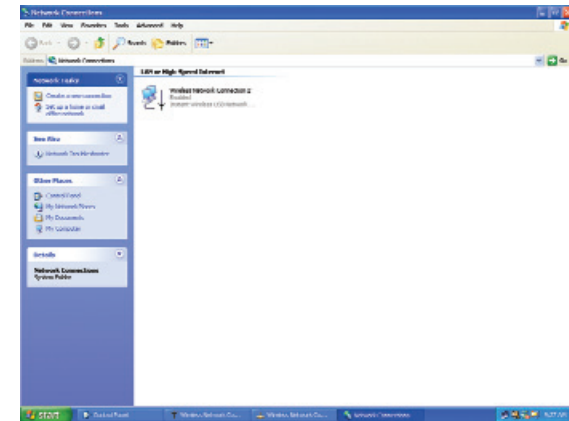


Figure C-6

- When the “Wireless Network Connection Status” window appears, as in Figure C-7, click the **Properties** button.

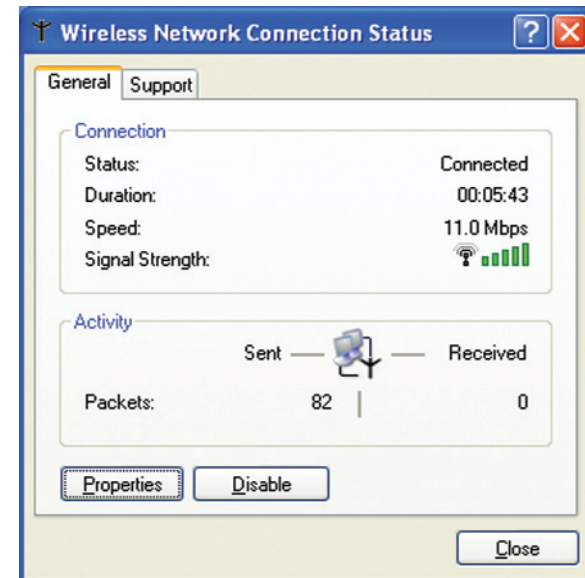


Figure C-7

6. When the “Wireless Network Connection Properties” window appears, as in Figure C-8, click the **Wireless Networks** Tab.

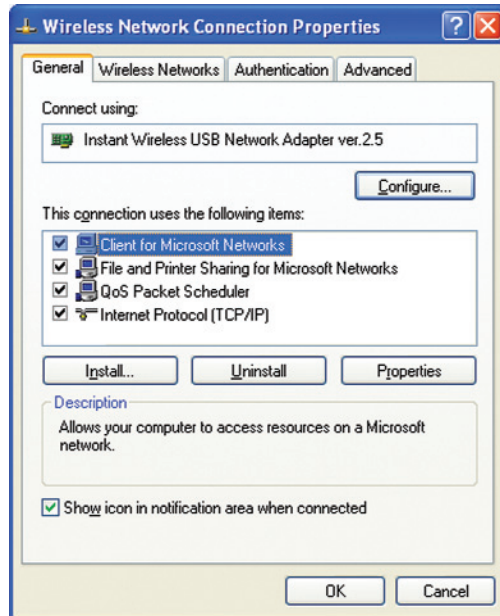


Figure C-8

7. If the appropriate wireless network, specified by the Router's SSID, is displayed in the “Preferred networks” section, as shown in Figure C-9, double-click it and continue to the next step.

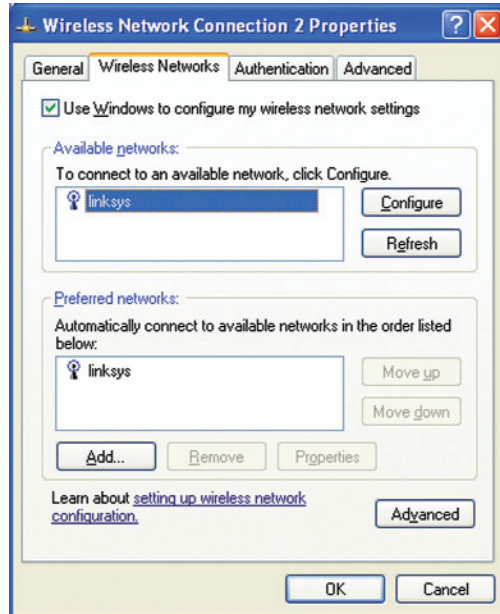


Figure C-9

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

8. The “Wireless Network Properties” window (shown in Figure C-10) will appear.

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

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

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

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

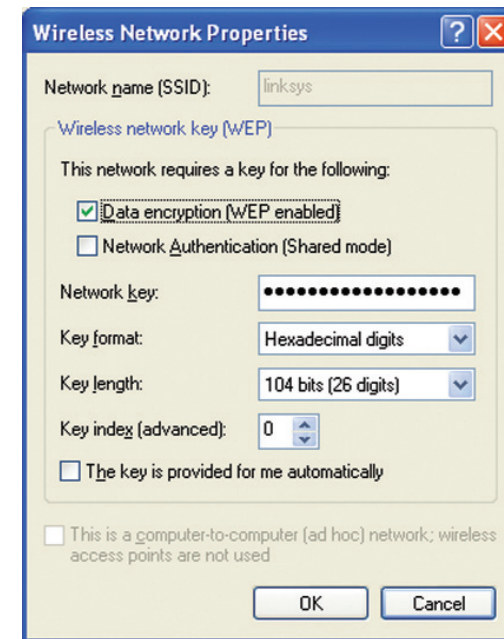


Figure C-10

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

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

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

This section describes how to find the MAC address for your Ethernet adapter to do either MAC Filtering or MAC Address Cloning for the Router and ISP. You can also find the IP address of your computer's Ethernet adapter. The IP address is used for filtering, forwarding, and DMZ. Follow these steps to find the MAC address or IP address for your adapter in Windows 98SE, ME, 2000, and XP.

For Windows 98 SE and ME:

1. Click on **Start** and **Run**. In the Open field, enter **winipcfg**, as shown in Figure D-1. Then press the **Enter** key or the **OK** button.

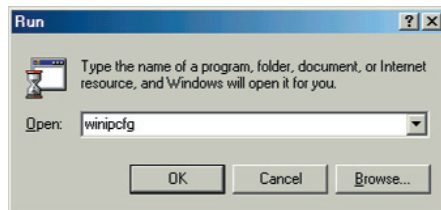


Figure D-1

2. When the IP Configuration window appears, as shown in Figure D-2, select the Ethernet adapter you are using to connect to the Router via a CAT 5 Ethernet cable.

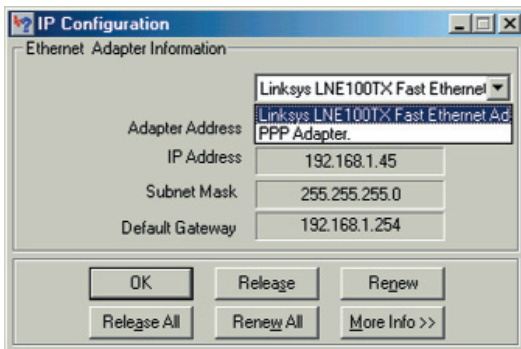


Figure D-2

Wireless-B Broadband Router

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

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

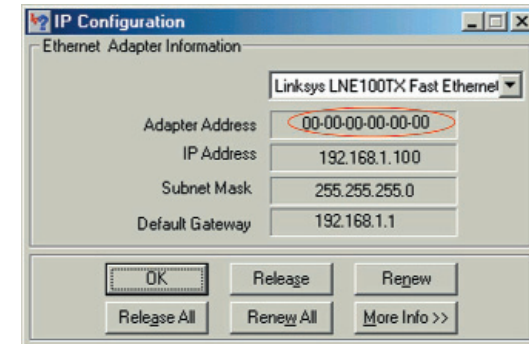


Figure D-3

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



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

For Windows 2000 and XP:

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

1. Click on **Start** and **Run**. In the Open field, enter **cmd**, as shown in Figure D-4. Press the **Enter** key or click the **OK** button.

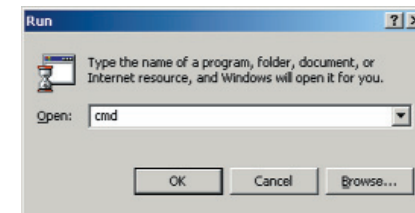


Figure D-4

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

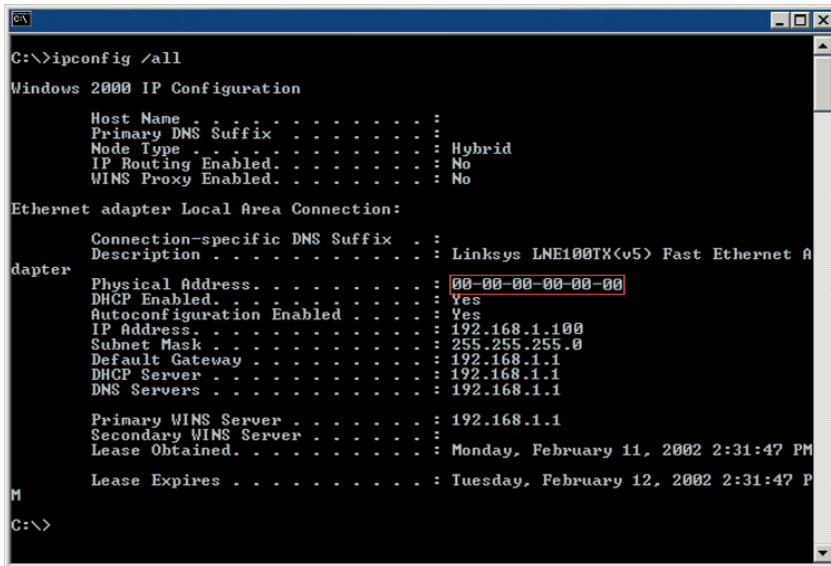


Figure D-5

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

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



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

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

When entering the information using the Router's web-based utility, you will type the **12-digit MAC address** in this format, XXXXXXXXXXXX *without the hyphens* for MAC Filtering. See Figure D-6.

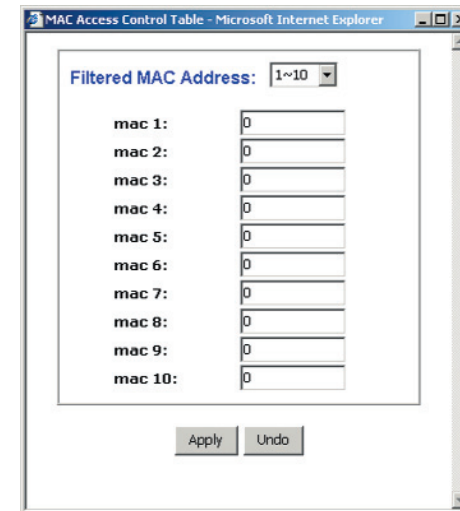


Figure D-6

When entering information for MAC Address Cloning, type the **12-digit MAC address** (see Figure D-7).

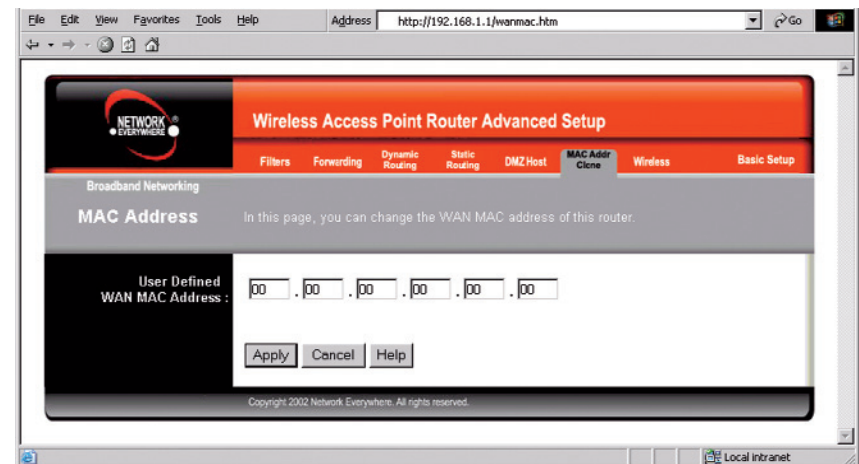


Figure D-7

Appendix E: Glossary

10BaseT - An Ethernet standard that uses twisted wire pairs.

100BaseTX - IEEE physical layer specification for 100 Mbps over two pairs of Category 5 cable.

Adapter - Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC. In a networked environment, a network interface card is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

Auto-negotiate - To automatically determine the correct settings. The term is often used with communications and networking. For example, Ethernet 10/100 cards and switches can determine the highest speed of the node they are connected to and adjust their transmission rate accordingly.

Bandwidth - The transmission capacity of a given facility, in terms of how much data the facility can transmit in a fixed amount of time; expressed in bits per second (bps).

Bit - A binary digit. The value—0 or 1—used in the binary numbering system. Also, the smallest form of data.

Boot - To cause the computer to start executing instructions. Personal computers contain built-in instructions in a ROM chip that are automatically executed on startup. These instructions search for the operating system, load it, and pass control to it.

Bridge - A device that interconnects different networks together.

Broadband - A data-transmission scheme in which multiple signals share the bandwidth of a medium. This allows the transmission of voice, data, and video signals over a single medium. Cable television uses broadband techniques to deliver dozens of channels over one cable.

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 or PC. The word “browser” seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet. Once connected, cable modem users have a continuous connection to the Internet. Cable modems feature

asymmetric transfer rates: around 36 Mbps downstream (from the Internet to the computer), and from 200 Kbps to 2 Mbps upstream (from the computer to the Internet).

CAT 5 - ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify “categories” (the singular is commonly referred to as “CAT”) of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 5 cable has a maximum throughput of 100 Mbps and is usually utilized for 100BaseTX networks.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection) - The LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and each waits a random amount of time before retrying.

Data Packet - One frame in a packet-switched message. Most data communications is based on dividing the transmitted message into packets. For example, an Ethernet packet can be from 64 to 1518 bytes in length.

Default Gateway - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a “lease” or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DMZ - (DeMilitarized Zone) allows one IP address (or 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 address if you want to use DMZ Hosting.

DNS - The Domain Name System (DNS) is the way that Internet domain names are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember “handle” for an Internet address.

Domain - A subnetwork comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Download - To receive a file transmitted over a network. In a communications session, download means receive, and upload means transmit.

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

Dynamic Routing - The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Has a transfer rate of 10 Mbps. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

Firewall - A firewall is a set of related programs, located at a network gateway server, that protects the resources of a network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access.

Basically, a firewall, working closely with a router, examines each network packet to determine whether to forward it toward its destination.

Firmware - Code that is written onto read-only memory (ROM) or program-mable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off.

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

FTP (File Transfer Protocol) - A 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.

FTP includes functions to log onto the network, list directories, and copy files. It can also convert between the ASCII and EBCDIC character codes. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. FTP transfers can also be initiated from within a Web browser by entering the URL preceded with ftp://.

Unlike e-mail programs in which graphics and program files have to be “attached,” FTP is designed to handle binary files directly and does not add the overhead of encoding and decoding the data.

Full Duplex - The ability of a device or line to transmit data simultaneously in both directions.

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

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

Hardware - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the “box” and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

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 browser.

IEEE - The Institute of Electrical and Electronics Engineers. The IEEE describes itself as “the world's largest technical professional society—promot-

ing the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members.”

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and has several large societies in special areas, such as the IEEE Computer Society.

IP Address - In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IPCONFIG - A utility that provides for querying, defining and managing IP addresses within a network. A commonly used utility, under Windows NT and 2000, for configuring networks with static IP addresses.

IPSec (Internet Protocol Security) - IPSec is a developing standard for security at the network or packet processing layer of network communication. A big advantage of IPSec is that security arrangements can be handled without requiring changes to individual user computers.

ISP - An ISP (Internet service provider) is a company that provides individuals and companies access to the Internet and other related services such as website building and virtual hosting.

LAN - A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

Latency - The time delay between when the first bit of a packet is received and the last bit is forwarded.

MAC Address - The MAC (Media Access Control) 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.

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

mIRC - mIRC runs under Windows and provides a graphical interface for logging onto IRC servers and listing, joining, and leaving channels.

NAT - NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

Network - A system that transmits any combination of voice, video, and/or data between users.

Packet Filtering - Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.).

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

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

Port - A pathway into and out of the computer or a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems, and printers.

PPPoE (Point to Point Protocol over Ethernet) - PPPoE is a method for the encapsulation of PPP packets over Ethernet frames from the user to the ISP over the Internet. One reason PPPoE is preferred by ISPs is because it provides authentication (username and password) in addition to data transport. A PPPoE session can be initiated by either a client application residing on a PC, or by client firmware residing on a modem or router.

PPTP (Point-to-Point Tunneling Protocol) - A protocol which allows the Point to Point Protocol (PPP) to be tunneled through an IP network. PPTP does not specify any changes to the PPP protocol but rather describes a “tunneling service” for carrying PPP (a tunneling service is any network service enabled by tunneling protocols such as PPTP, L2F, L2TP, and IPSEC tunnel

RIP (Routing Information Protocol) - A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers.

RJ-45 - A connector similar to a telephone connector that holds up to eight wires, used for connecting Ethernet devices.

Router - Protocol-dependent device that connects subnetworks together. Routers are useful in breaking down a very large network into smaller subnetworks; they introduce longer delays and typically have much lower throughput rates than bridges.

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

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

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 (switch, 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.).

Software - Instructions for the computer. A series of instructions that performs a particular task is called a “program.” The two major categories of software are “system software” and “application software.” System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user.

A common misconception is that software is data. It is not. Software tells the hardware how to process the data.

Static IP Address - A permanent IP address that is assigned to a node in a TCP/IP network.

Static Routing - Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

Subnet Mask - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

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

TCP (Transmission Control Protocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. TCP is known as a “connection oriented” protocol due to requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet resulting in transmission control.

TCP/IP (Transmission Control Protocol/Internet Protocol) - The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

Telnet - A terminal emulation protocol commonly used on the 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.

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

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

Topology - A network’s topology is a logical characterization of how the devices on the network are connected and the distances between them. The most common network devices include switches, routers, and gateways. Most large networks contain several levels of interconnection, the most important of which include edge connections, backbone connections, and wide-area connections.

TX Rate – Transmission Rate.

UDP (User Datagram Protocol) - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling

the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. UDP is known as a “connection-less” protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP).

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

Upload - To send a file transmitted over a network. In a communications session, upload means transmit, and download means receive.

URL (Uniform Resource Locator) - The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.

WAN (Wide Area Network) - A communications network that covers a relatively large geographic area, consisting of two or more LANs. Broadband communication over the WAN is often through public networks such as the telephone (DSL) or cable systems, or through leased lines or satellites. In its most basic definition, the Internet could be considered a WAN.

WINIPCFG - Configuration utility based on the Win32 API for querying, defining, and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

Workgroup - Two or more individuals that share files and databases.

Appendix F: Specifications

Standards	IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), IEEE 802.11b (Wireless)
Ports	Four 10/100 switch ports, One Internet Port
Buttons	Reset
Cabling Type	Ethernet Category 5 or better
LED Indicators	Power, Wireless-B, Ethernet, Internet
Modulation	CCK, QPSK, BPSK
Network Protocols	TCP/IP, NetBEUI, IPX/SPX
WEP Key Bits	64-bit and 128-bit

Environmental

Dimensions	6.30" x 14.33" x 1.38"
(W x H x D)	(160 mm x 110 mm x 35 mm)
Unit Weight	8.82 oz. (0.25 kg)
Power	External, 12V DC, 1A
Certifications	FCC Class B
Operating Temp.	0°C to 40°C (32°F to 104°F)
Storage Temp.	-20°C to 70°C (-4°F to 158°F)
Operating Humidity	10% to 85%, Non-condensing
Storage Humidity	5% to 90%, Non-condensing

Appendix G: Warranty Information

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

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

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

Appendix H: Contact Information

For help with the installation or operation of the Wireless Broadband Router, contact Network Everywhere Technical Support at one of the phone numbers or Internet addresses below.

Technical Support	949-271-5470, M-F, 8:00 am to 5:00 pm (PST)
Fax	949-265-6655
Email	support@NetworkEverywhere.com
Web site	http://www.NetworkEverywhere.com

FCC RF Radiation Exposure Statement:

The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.



<http://www.NetworkEverywhere.com>

Copyright © 2003 Network Everywhere. All rights reserved.