Advanced Wireless

The *Advanced Wireless* screen allows you to customize data transmission settings and access the *802.1x Configuration* screen. In most cases, the advanced wireless settings on this screen should remain at their default values.

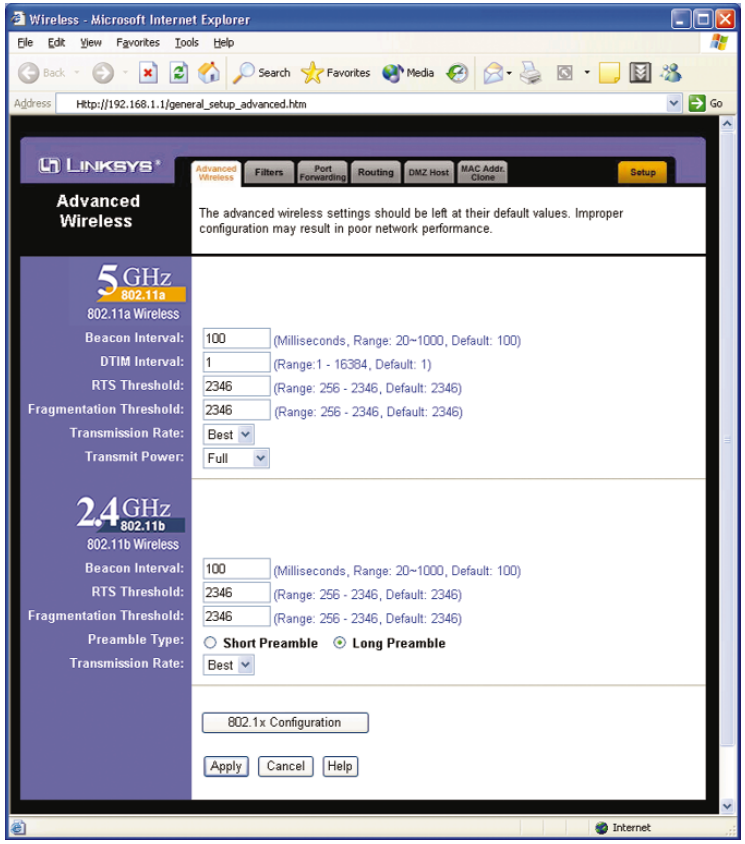

Figure 6-19

5GHz, 802.11a

Beacon Interval The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network. The default value is **100**.

DTIM Interval This value, between 1 and 16384, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, 2346, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2346**.

Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

Transmission Rate The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds (**6**, **9**, **12**, **18**, **24**, **36**, **48**, or **54**Mbps), or you can select **Best** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Best**.

Transmit Power The greater the transmit power used, the larger the area a wireless network covers. To minimize the likelihood of eavesdropping by unauthorized wireless users, do not use more transmit power than necessary to cover the range needed for your wireless network. Try using the Router at different levels of transmit power, and determine how much transmit power is needed to reach the wireless client, such as a PC, or access point that is farthest from the Router. Then select the appropriate level of transmit power (**Full**, **Half**, **Quarter**, **Eighth**, or **Min**) from the drop-down menu. The default value is **Full**.

2.4GHz, 802.11b

Beacon Interval The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network. The default value is **100**.

RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, 2346, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2346**.

Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of this value is recommended. In most cases, it should remain at its default value of **2346**.

Preamble Type The preamble defines the length of the CRC block for communication between the Router and a roaming wireless network adapter. Select the appropriate preamble type for your wireless network. (High network traffic areas should use the shorter preamble type.) The default is **Long Preamble**.

Transmission Rate The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds (**1**, **2**, **5.5**, or **11**Mbps), or you can select **Best** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default setting is **Best**.

To apply any of the settings you change on this page, click the **Apply** button. To cancel any changes you've entered on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

802.1x Configuration

802.1x Configuration Click the **802.1x Configuration** button to customize the Router's 802.1x feature (see Figure 6-20).

Note: If your wireless network does not have a RADIUS server, the 802.1x feature is not applicable to your network. (802.1x is an advanced data security measure and not essential for router operation.)

802.1x Configuration

The *802.1x Configuration* screen allows you to alter the 802.1x settings for your wireless network(s). Based on the Extensible Authentication Protocol (EAP), the 802.1x standard specifies an authentication framework for a wireless client to access a network, so network security is enhanced.

To access a network with 802.1x enabled, wireless clients, such as PCs, must use 802.1x client software or Windows XP, which supports 802.1x.

Note: For more details about 802.1x, refer to "Appendix C: Configuring Wireless Security."

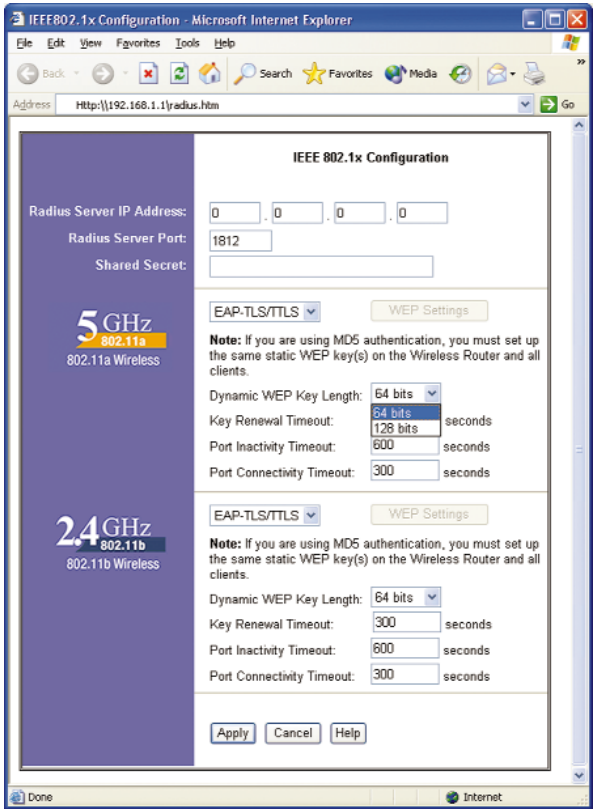

Figure 6-20

Important: The Router's 802.1x feature works with Windows XP. It may also work with other Windows operating systems, depending on the specifics of your PC's operating system and the 802.1x client software being used.

RADIUS Server

The Router's 802.1x feature works with a RADIUS server. It may also work with other types of authentication servers, depending on the specifics of each authentication server.

RADIUS Server IP Address Enter the IP Address of the RADIUS server in the field provided.

RADIUS Server Port Enter the Port Number of the RADIUS server in the field provided. The default is 1812.

Shared Secret Enter the Shared Secret Key used by the Router and RADIUS server during the authentication process.

5GHz, 802.11a

Disable/EAP-MD5/EAP-TLS/TTLS Select **EAP-MD5** to enable use of 802.1x with MD5 authentication for the 5GHz, 802.11a network connection between a wireless client and a RADIUS server (the Router acts as an authenticator). Select **EAP-TLS/TTLS** to enable use of 802.1x with TLS or TTLS authentication for the 5GHz, 802.11a network connection between a wireless client and a RADIUS server (the Router acts as an authenticator). To disable 802.1x authentication for your 5GHz, 802.11a network, keep the default setting, **Disable**.

Note: Many authentication methods work within the 802.1x framework. The Router supports MD5 and certificate-based (TLS or TTLS) authentication methods. Using MD5 authentication is less secure than using certificate-based authentication (TLS or TTLS), because keys are not changed automatically.

WEP Settings If you are using 802.1x with MD5 authentication, then you must click the **WEP Settings** button and set up a static key for WEP encryption. This static key must be set on the Router's *5GHz, 802.11a WEP Settings* screen and on all 5GHz, 802.11a wireless clients.

Dynamic WEP Key Length When 5GHz, 802.11a wireless clients are using certificate-based authentication (EAP-TLS or EAP-TTLS), dynamic WEP keys are automatically generated. Select the length of the Dynamic Key (**64** or **128**-bit) from the drop-down menu.

Key Renewal Timeout If you are using dynamic WEP keys (available only for EAP-TLS or EAP-TTLS authentication), enter the number of seconds that will elapse before the Dynamic Key automatically changes. The default is **300** seconds.

Port Inactivity Timeout After the wireless client has been authenticated, the Router monitors activity on the port being used. In the *Port Inactivity Timeout* field, enter the number of seconds the port can be inactive before the client automatically forced to reauthenticate. The default is **600** seconds.

Port Connectivity Timeout After the Router requests the identity of a wireless client, the client must respond with an identity message within a certain length of time. In the *Port Connectivity Timeout* field, enter the number of seconds the client has to respond within before the connection is terminated. The default is **300** seconds.

2.4GHz, 802.11b

Disable/EAP-MD5/EAP-TLS/TTLS Select **EAP-MD5** to enable use of 802.1x with MD5 authentication for the 2.4GHz, 802.11b network connection between a wireless client and a RADIUS server (the Router acts as an authenticator). Select **EAP-TLS/TTLS** to enable use of 802.1x with TLS or TTLS authentication for the 2.4GHz, 802.11b network connection between a wireless client and a RADIUS server (the Router acts as an authenticator). To disable 802.1x authentication for your 2.4GHz, 802.11b network, keep the default setting, **Disable**

Note: Using MD5 authentication is less secure than using certificate-based authentication (TLS or TTLS), because keys are not changed automatically.

WEP Settings If you are using 802.1x with MD5 authentication, then you must click the **WEP Settings** button and set up a static key for WEP encryption. This static key must be set on the Router's *2.4GHz, 802.11b WEP Settings* screen and on all 2.4GHz, 802.11b wireless clients.

Dynamic WEP Key Length When 2.4GHz, 802.11b wireless clients are using certificate-based authentication (EAP-TLS or EAP-TTLS), dynamic WEP keys are automatically generated. Select the length of the Dynamic Key (**64** or **128**-bit) from the drop-down menu.

Key Renewal Timeout If you are using dynamic WEP keys (available only for EAP-TLS or EAP-TTLS authentication), enter the number of seconds that will elapse before the Dynamic Key automatically changes. The default is **300** seconds.

Port Inactivity Timeout After the wireless client has been authenticated, the Router monitors activity on the port being used. In the *Port Inactivity Timeout* field, enter the number of seconds the port can be inactive before the client automatically forced to reauthenticate. The default is **600** seconds.

Port Connectivity Timeout After the Router requests the identity of a wireless client, the client must respond with an identity message within a certain length of time. In the *Port Connectivity Timeout* field, enter the number of seconds the client has to respond within before the connection is terminated. The default is **300** seconds.

To apply any of the settings you change on this page, click the **Apply** button. To cancel any changes you've entered on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Filters

The *Filters* screen allows you to block specific internal users from accessing the Internet. You can set up filters by using MAC addresses, IP addresses, or network port numbers (or a range of ports).

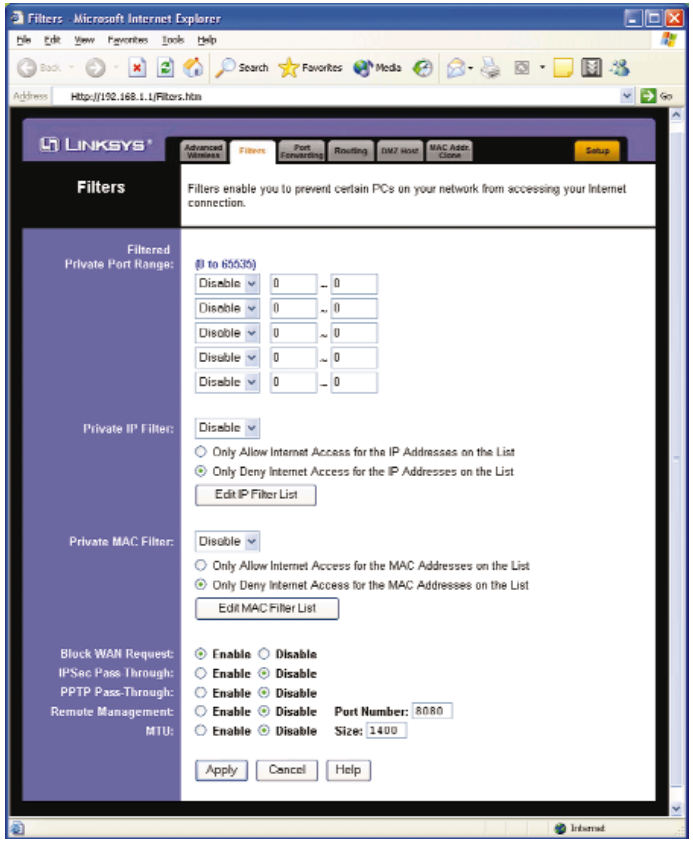

Figure 6-21

Filtered Private Port Range To filter users by network port number, select **Both**, **TCP**, or **UDP**, depending on which protocols you want to filter. Then enter the port numbers you want to filter into the port number fields. Users connected to the Router will no longer be able to access any port number listed there. To disable a filter, select **Disable**.

Private IP Filter To set up a filter using IP addresses, select **Enable**. Then select **Only Allow Internet Access for the IP Addresses on the List** or **Only Deny Internet Access for the IP Addresses on the List**.

Click the **Edit IP Filter List** button. Enter the appropriate IP addresses into the IP address fields (see Figure 6-22). Each IP address should be entered in this format: xxx.xxx.xxx.xxx (the x's represent the actual digits of the IP address).

If you want to enter more than ten IP addresses, select **IP Addresses 1-10**, **11-20**, **21-30**, **31-40**, or **41-50** from the drop-down menu to enter additional IP addresses, up to a maximum of 50. Then click the **Apply** button to save the IP addresses.

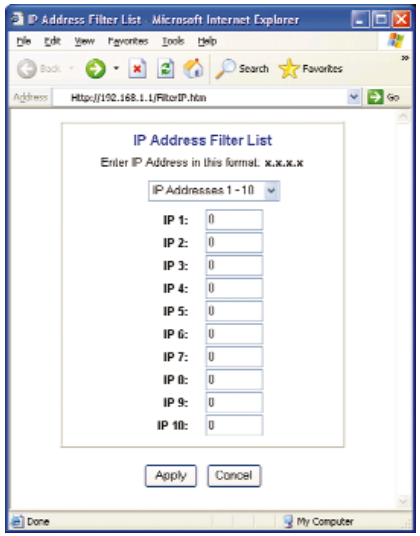

Figure 6-22

To disable Private IP Filtering, select **Disable**.

Private MAC Filter To set up a filter using MAC addresses, select **Enable**. Then select **Only Allow Internet Access for the MAC Addresses on the List** or **Only Deny Internet Access for the IP Addresses on the List**. Click the **Edit MAC Filter List** button. Enter the appropriate MAC addresses into the MAC address fields (see Figure 6-23). Each MAC address should be entered in this format: xx:xx:xx:xx:xx:xx (the x's represent the actual characters of the MAC address).

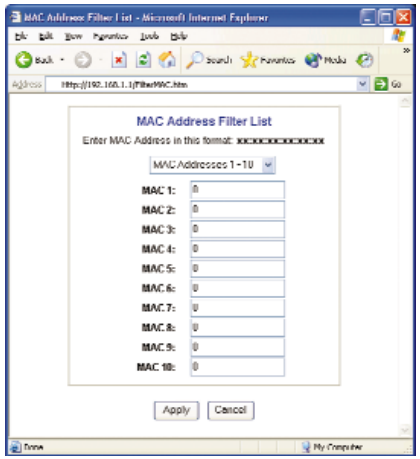

Figure 6-23

If you want to enter more than ten MAC addresses, select **MAC Addresses 1-10**, **11-20**, **21-30**, **31-40**, or **41-50** from the drop-down menu to enter additional MAC addresses, up to a maximum of 50. Then click the **Apply** button to save the MAC addresses.

To disable Private MAC Filtering, select **Disable**.

Block WAN Request By enabling the Block WAN Request feature, you can prevent your network from being "pinged," or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network. The default is **Enable**.

IPSec Pass-Through The Router supports IPSec Pass-Through. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer, and it is one of the methods used to enable Virtual Private Networking (VPN) tunnels. IPSec is more secure than PPTP. The default is **Enable**.

PPTP Pass-Through The Router supports PPTP Pass-Through. Point-to-Point Tunneling Protocol (PPTP) is one of the methods used to enable VPN tunnels. PPTP is less secure than IPSec. The default is **Enable**.

Remote Management This feature allows you to manage the Router from a remote location, via the Internet. To enable this feature, select **Enable**, and use the specified port (default is **8080**) on your PC to remotely manage the Router. The default is **Disable**.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for network transmission. To use this feature, select **Enable**, and enter the value desired. You should leave this value in the 572 to 1492 range. The default is **Disable**.

To apply any of the settings you change on this page, click the **Apply** button. To cancel any changes you've entered on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Port Forwarding

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

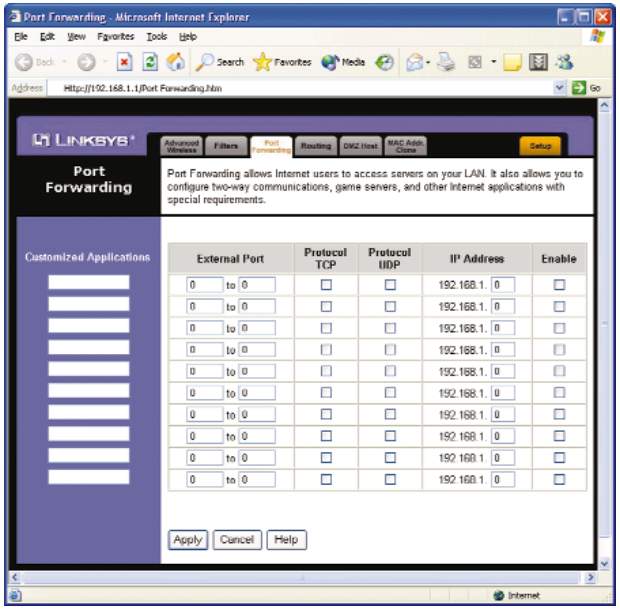

Figure 6-24

Note: Any PC whose port is being forwarded should have its DHCP client function disabled and a new static IP address assigned to it because its IP address may change when using the DHCP function.

Customized Applications In the field provided, enter the name you wish to give each application.

External Port For each application, enter the number of the External Ports (the port numbers seen by users on the Internet) in the appropriate fields. (To find out the port range, check your application's documentation.) If there is only one External Port, enter its number in both *External Port* fields.

TCP Protocol Click this checkbox if you want to forward the data transmissions that use the TCP protocol.

UDP Protocol Click this checkbox if you want to forward the data transmissions that use the UDP protocol.

IP Address For each application, enter the **IP Address** of the PC running the specific application.

Enable Click the **Enable** checkbox to enable port forwarding for the relevant application.

The following table shows the typical port forwarding settings for common Internet applications.

Applications	External Port	TCP Protocol	UDP Protocol
FTP	21	√	
Telnet	23	√	
SMTP	25	√	
DNS	53		√
TFTP	69		√
Finger	79	√	
HTTP	80	√	
POP3	110	√	
NNTP	119	√	
SNMP	161		√

To apply any of the settings you change on this page, click the **Apply** button. To cancel any changes you've entered on this page, click the **Cancel** button. To get more information about the features, click the **Help** button.

Routing

On the *Routing* screen, you can set the routing mode of the Router. *Gateway* mode is recommended for most users.

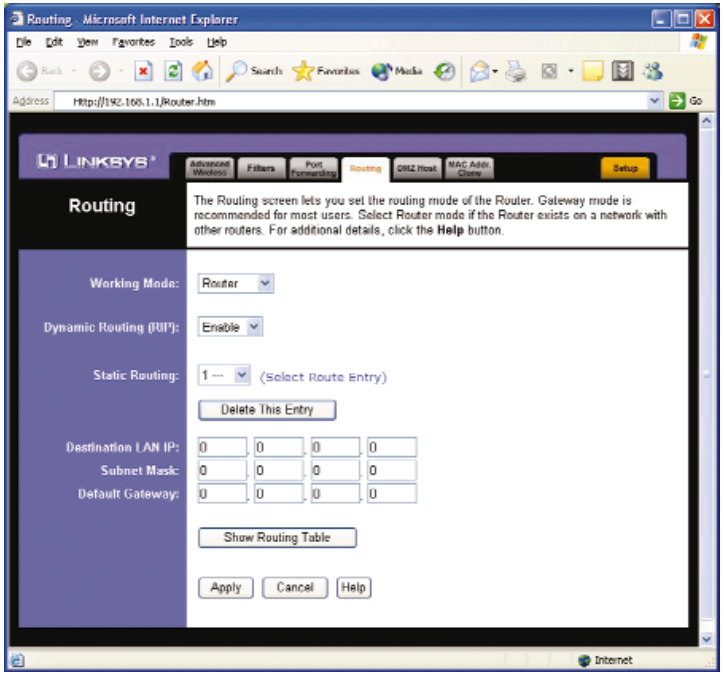

Figure 6-25

Note: The *Routing* screen and available features will vary depending on which mode you select.

To set up routing:

1. Choose the correct working mode. Select **Gateway** if the Router is hosting your network's connection to the Internet (recommended for most users). Select **Router** if the Router exists on a network with other routers.

Note: If you have more than one router on your network, you should select **Router** for the working mode.

2. If you selected the *Gateway* mode, click the **Apply** button. If you selected the *Router* mode, proceed to step 3.

3. For *Dynamic Routing*, the default is **Enable**. The Dynamic Routing feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. Select **Disable** to disable the Dynamic Routing feature for data transmissions.

4. To set up a static route between the Router and another network, select a number from the *Static Routing* drop-down list. (A static route is a predetermined pathway that network information must travel to reach a specific host or network.)

5. Enter the following data:

   - **Destination LAN IP -** The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

   - **Subnet Mask -** The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

   - **Default Gateway -** This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

6. To cancel your changes, click the **Cancel** button. To save your changes, click the **Apply** button. To get more information about the features, click the **Help** button.

To delete a static route entry:

1. From the *Static Routing* drop-down list, select the entry number of the static route.

2. Click the **Delete This Entry** button.

3. To cancel a deletion, click the **Cancel** button. To save a deletion, click the **Apply** button. To get more information about the features, click the **Help** button.

Show Routing Table Click the **Show Routing Table** button to view all of the valid dynamic and static route entries in use (see Figure 6-26). The Destination LAN IP address, Subnet Mask, Gateway, and Interface information are displayed for each entry. Click the **Refresh** button to display the most up-to-date data.

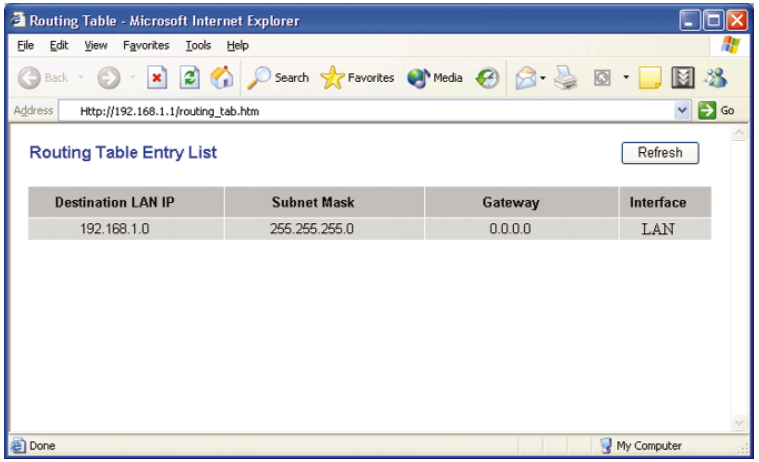

Figure 6-26

DMZ Host

The *DMZ Host* screen lets you enable the DMZ hosting feature, which allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. Whereas port forwarding can only forward a maximum of ten port ranges, DMZ hosting forwards all the ports to one PC simultaneously. It is recommended to use Port Forwarding whenever possible because it is more secure.

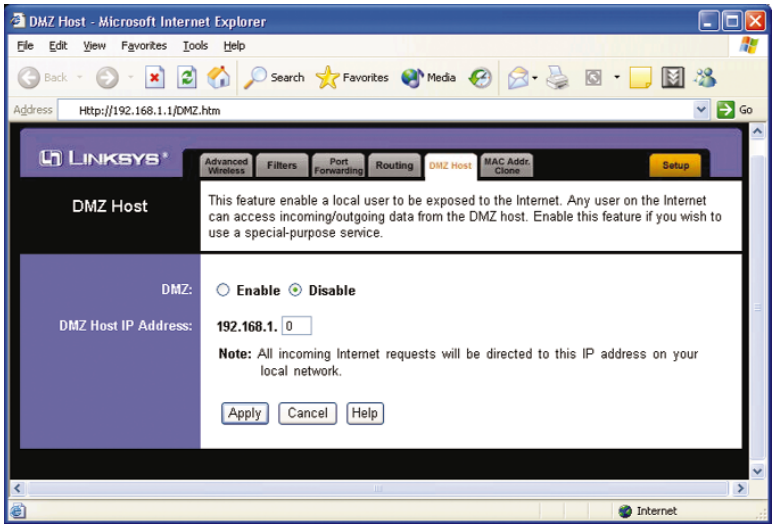

Figure 6-27

Note: Any PC whose ports are being forwarded should have its DHCP client function disabled and a new static IP address assigned to it because its IP address may change when using the DHCP client function.

To expose one PC to the Internet:

1. Click the **Enable** radio button.

2. Enter the computer's IP address in the *DMZ Host IP Address* field.

3. To cancel your changes, click the **Cancel** button. To save your new settings, click the **Apply** button. To get more information about the features, click the **Help** button.

MAC Address Clone

On the *MAC Address Clone* screen, you can clone the MAC address of your PC's network adapter onto the Router.

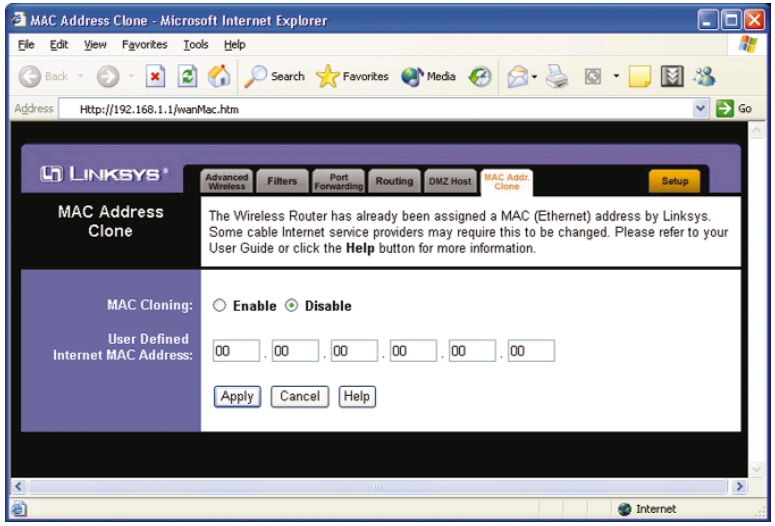

Figure 6-28

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. Some ISPs require that you register the MAC address of your PC's network adapter, which was connected to your cable or DSL modem during installation. To avoid calling your ISP and changing the MAC address that is registered with the ISP, follow these instructions:

1. Click the **Enable** radio button.

2. Enter your adapter's MAC address in the *User Defined Internet MAC Address* field.

3. To cancel your changes, click the **Cancel** button. To save your new settings, click the **Apply** button. To get more information about the features, click the **Help** button.

To disable MAC address cloning, click the **Disable** radio button.

If you do not know your adapter's MAC address, follow these instructions:

1. Click the **Start** button, and select **Run**.

2. Enter **command** in the field provided, and press the **OK** button.

3. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.

4. Write down your adapter's physical address; it is the adapter's MAC address.

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 that may occur during the installation and operation of the Router. Read the descriptions below to help solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.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 192.168.1.150 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 and Me:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
B. 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.
C. 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.
D. 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.
E. 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.
F. Click the **OK** button in the *TCP/IP properties* window, and click **Close** or the **OK** button for the Network window.
G. Restart the computer when asked.

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 NT 4.0:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
B. Click the **Protocol** tab, and double-click **TCP/IP Protocol**.
C. When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter.
D. Select **Specify an IP address**, and enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
E. Enter the Subnet Mask, **255.255.255.0**.
F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
G. Click the **DNS** tab, and enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Under DNS Service Search Order, click the **Add** button. Enter the **DNS IP address** in the *DNS Server* field, and click the **Add** button. Repeat this action for all DNS IP addresses given by your ISP.
H. Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* 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, Me, 2000, and XP:
Refer to "Chapter 4: Configure the PCs" for details. Make sure **Obtain IP address automatically** is selected in the settings.

For Windows NT 4.0:
- Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
- Click the **Protocol** tab, and double-click on **TCP/IP Protocol**.
- When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter and set it for **Obtain an IP address from a DHCP server**.
- Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.
- Restart the computer if asked.

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

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

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

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

A. Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
B. If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix D: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Router, see the MAC Address Clone section of "Chapter 6: The Router's Web-based Utility" for details.
C. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Chapter 6: The Router's Web-based Utility" for details on Internet connection settings.

D. Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.
E. Make sure the cable connecting from your cable or DSL modem is connected to the Router's Internet port. Verify that the Status page of the Router's web-based utility shows a valid IP address from your ISP.
F. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router's web-based utility to see if you get an IP address.

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

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

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

Access the Router's web interface by going to **http://192.168.1.1** or the **IP address** of the Router, and go to the **Advanced => Filters** 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.

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

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

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 **Apply** button.

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

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

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

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 **Apply** button.

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

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

A. Access the Router's web-based utility by going to **http://192.168.1.1** or the **IP address** of the Router. Go to the **Advanced => Port Forwarding** tab.
B. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
C. Click the **DMZ Host** tab.
D. 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 I am saving settings to the Router.

Reset the Router to factory default by pressing the **Reset** button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

A. Access the Router's web-based utility by going to **http://192.168.1.1** or the **IP address** of the Router. Enter the default password **admin**, and click the **Password** tab.
B. Enter a **different password** in the *Router Password* field, and enter the same password in the second field to confirm the password.
C. Click the **Apply** button.

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

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

For Microsoft Internet Explorer 5.0 or higher:

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

For Netscape 4.7 or higher:

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

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

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

12. I need to upgrade the firmware.

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

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

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

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

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

IP Address: 192.168.1.50
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1

C. Perform the upgrade using the TFTP program or the Router's web-based utility through its 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. On the *Setup* screen, select the option **Keep Alive**, and set the **Redial Period** option at **20** (seconds).
D. Click the **Apply** button.
E. Click the **Status** tab, and click the **Connect** button.
F. You may see the login status display as **Connecting**. Press the **F5** key to refresh the screen, until you see the login status display as **Connected**.
G. Click the **Apply** button to continue.

If the connection is lost again, follow steps E to G to re-establish connection.

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

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you are having some difficulties, perform the following steps:

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the **IP address** of the Router.
B. Enter the password, if asked. (The default password is **admin**.)
C. Click the **Advanced => Filters** 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. The Diag LED stays lit continuously.

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

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

- Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.

- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

18. The Full/Col LED keeps flickering continuously.

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

Frequently Asked Questions

What is the maximum number of IP addresses that the Router will support?

The Router will support up to 253 IP addresses.

Is IPSec Pass-Through supported by the Router?

Yes, it is a built-in feature that the Router automatically enables.

Where is the Router installed on the network?

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

Does the Router support IPX or AppleTalk?

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

Does the Internet connection of the Router support 100Mbps Ethernet?

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

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

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

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

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

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

How do I get *Half-Life: Team Fortress* to work with the Router?
The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. *One problem:* Version 1.0.1.6 won't let multiple computers with the

same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

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

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

If all else fails in the installation, what can I do?
Reset the Router by holding down the reset button until the Diag LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys website, *www.linksys.com*.

How will I be notified of new Router firmware upgrades?
All Linksys firmware upgrades are posted on the Linksys website at *www.linksys.com*, where they can be downloaded for free. To upgrade the Router's firmware, use the Help tab of the Router's web-based utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

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

I am not able to get the web configuration screen for the Router. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that

your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

What is DMZ Hosting?

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

If DMZ Hosting is used, does the exposed user share the public IP with the Router?

No.

Does the Router pass PPTP packets or actively route PPTP sessions?

The Router allows PPTP packets to pass through.

Is the Router cross-platform compatible?

Any platform that supports Ethernet and TCP/IP is compatible with the Router.

How many ports can be simultaneously forwarded?

Theoretically, the Router can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

Does the Router replace a modem? Is there a cable or DSL modem in the Router?

No, the Router must work in conjunction with a cable or DSL modem.

Which modems are compatible with the Router?

The Router is compatible with virtually any cable or DSL modem that supports Ethernet.

What are the advanced features of the Router?

The Router's advanced features include Advanced Wireless settings, Filtering, Port Forwarding, 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 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 802.11a standard?

It is one of the IEEE standards for wireless networks. The 802.11a standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11a standard. The 802.11a standard states a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

What is the IEEE 802.11b standard?

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

What IEEE 802.11a features are supported?

The product supports the following IEEE 802.11a functions:

- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation

What IEEE 802.11b features are supported?

The product supports the following IEEE 802.11b functions:

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

What is ad-hoc mode?

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

What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is roaming?

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

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

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment

from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is ISM band?

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

What is Spread Spectrum?

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

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

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

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

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

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

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

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

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

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

You may also try using different channels, as this may eliminate interference affecting only one channel. Also, due to FCC regulations, more power may be transmitted, using 802.11a, on channels 52, 56, 60 and 64, than on the lower channels. Lastly, click the **Advanced** tab of the web-based utility and make sure that FULL is selected in the *Transmission Power* field.

Does the Turbo Mode work with Windows XP PCs?
No. The Turbo Mode does not work with Windows XP PCs.

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, 128, or 152) are being used on all nodes of your wireless network.

How many channels/frequencies are available with the Router?
Using 802.11a, there are eight available channels, ranging from 36 to 64. Using 802.11b, there are eleven available channels, ranging from 1 to 11.

What is Turbo Mode?
Turbo Mode allows high-speed connections, but severely limits range. To work, Turbo Mode must be enabled on both the Router and the wireless PCs. Turbo Mode is not compatible with Windows XP and may only function with Linksys 5GHz wireless adapters.

What is the difference in range between 802.11a and 802.11b products?
Overall, range will be a little less in a typical environment, and while higher speeds may be achieved with 802.11a, throughput degrades more quickly. (See Figure A-1.)

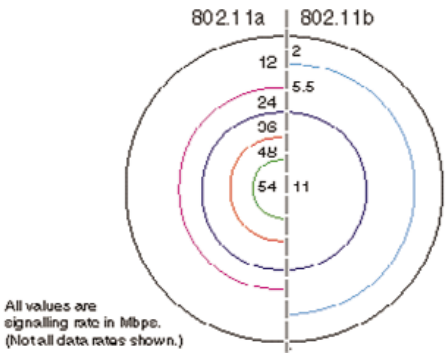

Figure A-1

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

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

Virtually all Internet addresses are configured with words or characters (e.g., *www.linksys.com*, *www.yahoo.com*, etc.) In actuality, however, these Internet addresses are assigned to IP addresses, which are the true addresses on the Internet. For example, www.yahoo.com is 66.218.71.87 (this IP address may change). Type it into your web browser and you will wind up at the Linksys home page every time. There are servers that translate the URL to an IP address; this is called the Domain Name System (DNS).

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 ISPs code words. You can determine the IP and web addresses of your ISP's servers by "pinging" them.

Important: 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** and then **Run**. Type **command** in the **Open** field. 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 the **Enter** key. 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
```

Figure B-1

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
```

Figure B-2

2. Write down the web address returned by the ping command. (In the example in Figure C-2, *mail.msnv3.occa.home.com* is the web address.) 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

Background

The Router offers two wireless security features. The basic feature is Wired Equivalent Privacy (WEP) encryption, an encryption method used to protect your wireless data communications. WEP uses 64-bit, 128-bit, or 152-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 key. Higher encryption levels mean higher levels of security, but due to the complexity of the encryption, they may mean decreased network performance.

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

Note: WEP encryption is an additional data security measure and not essential for router operation; however, Linksys recommends the use of WEP encryption.

The second wireless security feature is 802.1x. The IEEE 802.1x standard specifies authentication methods for a wireless client, such as a PC, to access a network, so network security is enhanced. Based on the Extensible Authentication Protocol (EAP), 802.1x designates how a client accesses a network server, frequently a RADIUS server, with the Router acting as an authenticator. When a network uses 802.1x, the identity of the client is verified before the client is allowed network access.

For example, a wireless user may use one of the authentication methods to access a wireless network protected by an authentication server. The user's PC sends a request to the Router (an access point can be used instead). The Router sends an identification request back to the PC. After the PC sends the Router the identification message, the Router forwards the identification message to the server. If the server accepts the identification message, then the PC is permitted access to the wireless network.

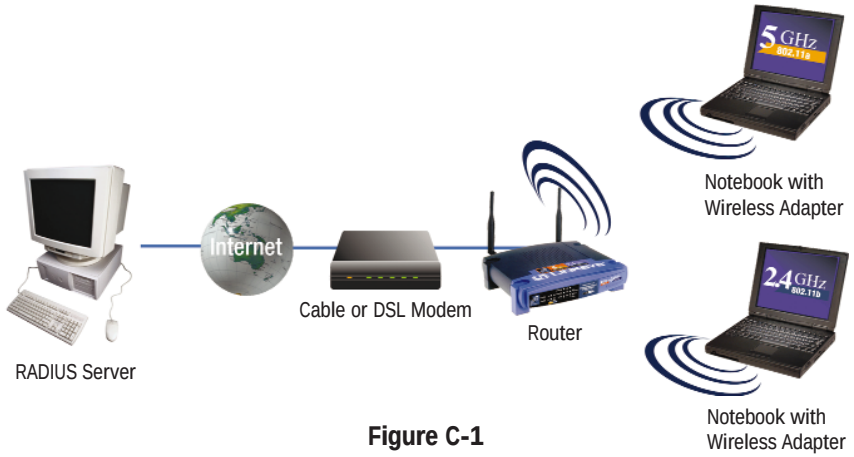

Figure C-1

Note: 802.1x is an advanced data security measure and not essential for router operation. It will, however, increase network security.

Note: If you are roaming between access points, you will have to go through the 802.1x authentication procedure each time your computer connects to a new access point.

There are two types of WEP encryption for 802.1x, static and dynamic. Static WEP keys are more vulnerable and can only be changed manually on all devices, including the Router. If you are using MD5 authentication, then you can only use static WEP keys. Dynamic WEP keys are keys that are renewed automatically on a periodic basis. This makes the WEP key(s) more difficult to break, so network security is strengthened. To enable dynamic WEP keys, you must use 802.1x certificate-based authentication methods, such as TLS or TTLS.

WEP Encryption

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

On a wireless network, a 128-bit WEP encrypted device will NOT communicate with a 64-bit WEP encrypted device. Therefore, make sure that all of the wireless devices on each network are using the same encryption level.

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

- Change the SSID from the default “linksys”
- Change the SSID on a regular basis
- Change the WEP key regularly
- Enable MAC address filtering (if your wireless products allow it)

For instructions on how to configure the Router’s WEP settings, go to the “Setup” section of “Chapter 6: The Router’s Web-Based Utility.” For instructions on how to configure the WEP settings of your PC’s wireless adapter, refer to your wireless adapter’s documentation.

802.1x Authentication

Many authentication methods, including passwords, certificates, and smart cards (plastic cards that hold data), work within the 802.1x framework. The Router supports two authentication types: MD5 and certificate-based (TLS or TTLS).

MD5 authentication is a type of one-way authentication method that employs user names and passwords. TLS and TTLS authentication are two-way authentication methods that employ digital certificates to verify the identity of a client. TLS, or EAP-TLS, exclusively uses digital certificates, while TTLS, or EAP-TTLS, uses a combination of certificates and another method, such as passwords, for authentication. MD5 authentication is not as secure as either certificate-based authentication method, and TLS is more secure than TTLS authentication.

To use 802.1x authentication, you have to enable the 802.1x feature on the Router as well as your wireless-equipped PCs. For instructions on how to configure the Router’s 802.1x settings, go to the “Advanced Wireless” section of “Chapter 6: The Router’s Web-Based Utility.”

Important: The Router’s 802.1x feature works with Windows XP. It may also work with other Windows operating systems, depending on the specifics of your PC’s operating system and the 802.1x client software being used.

Important: The Router’s 802.1x feature works with a RADIUS server. It may also work with other types of authentication servers, depending on the specifics of each authentication server.

Windows XP supports 802.1x with MD5 or TLS authentication. In this appendix, the following sections will discuss 802.1x configuration for PCs running Windows XP. If you are using MD5 authentication, proceed to "MD5 Authentication for Windows XP." If you are using TLS authentication, go to the appropriate section, "Digital Certificate Installation" or "TLS Authentication for Windows XP," depending on whether or not you have already installed a digital certificate on your PC.

If your PC is not running Windows XP, then your PC must use third-party 802.1x client software. For instructions on how to configure 802.1x through third-party software, refer to that application's documentation.

MD5 Authentication for Windows XP

Important: Make sure you have the User name, Password, Logon domain (if applicable), and WEP key needed to access the appropriate wireless network. If you need any of this information, contact your network administrator beforehand.

1. Make sure you have installed the wireless adapter correctly into your PC. Click the **Wireless Network Connection** icon located in your computer's system tray.

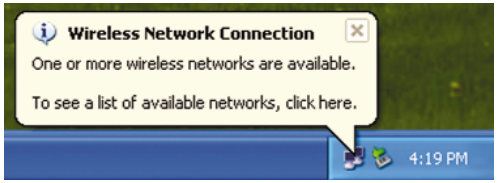

Figure C-2

Note: These are the instructions and screenshots for Windows XP without Service Pack 1 installed. If you have already installed Service Pack 1, enter the keyword **802.1x** in the Windows XP search engine for your 802.1x setup instructions.

2. The screen that appears will show any available wireless network. Select the appropriate network, and click the **Advanced...** button.

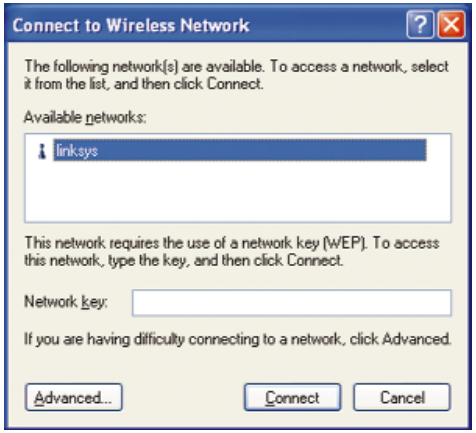

Figure C-3

3. Click the **Authentication** tab. Make sure the box next to **Enable network access control using IEEE 802.1X** is checked. In the drop-down box next to *EAP type*, select **MD5-Challenge**. Make sure the box next to **Authenticate as computer when computer information is available** is checked. Then click the **OK** button.

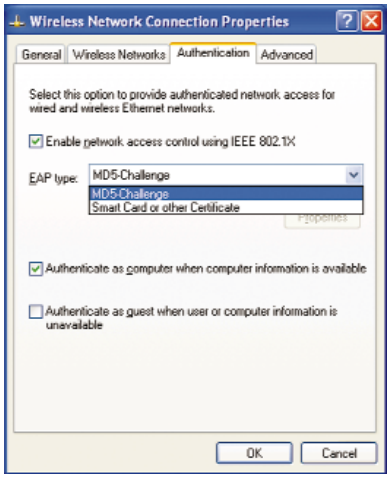

Figure C-4

4. Click the **Wireless Networks** tab. Select the wireless network you want to connect to, and click the **Configure** button. If you don't see the wireless network you want, then click the **Refresh** button.

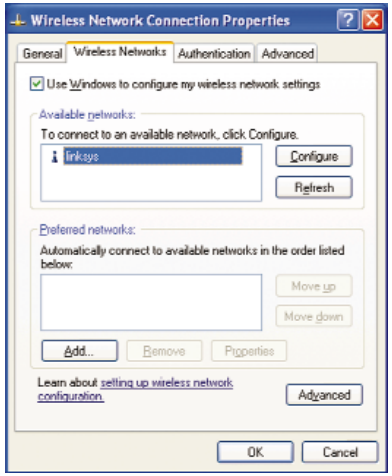

Figure C-5

5. Make sure the box next to **Data encryption (WEP enabled)** is checked. Uncheck the box next to **The key is provided for me automatically**.

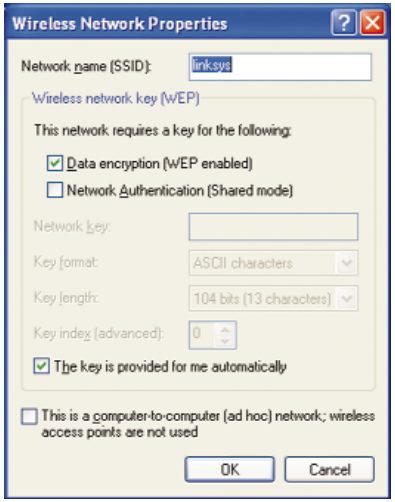

Figure C-6

6. Enter the WEP key in the *Network key* field. Then click the **OK** button.

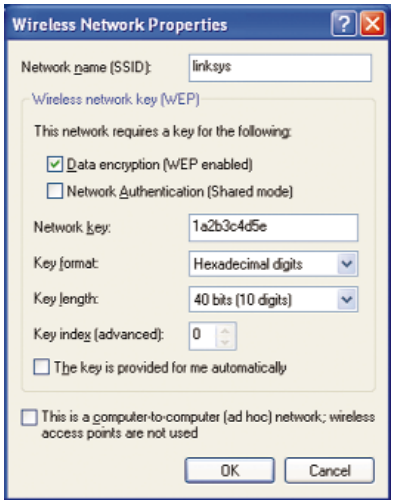

Figure C-7

7. Make sure the network you want is selected in the *Preferred networks* box, and then click the **OK** button.

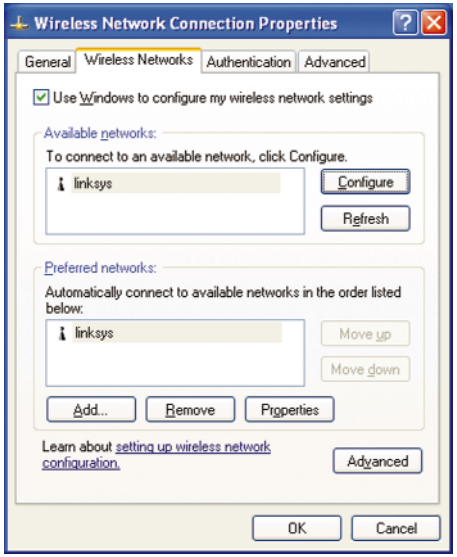

Figure C-8

8. Click the **Wireless Network Connection** icon located in your computer's system tray.

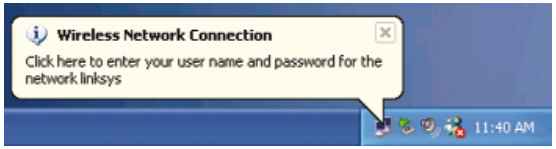

Figure C-9

9. Complete the *User name* and *Password* fields. Complete the *Logon domain* field if necessary. Then click the **OK** button.

Figure C-10

10. Open your PC's web browser and test your Internet connection. If you are unable to connect to the Internet, double-check the settings you configured through Windows XP and the Router's web-based utility.

For more details about wireless networking or 802.1x on a Windows XP computer, enter the keyword **wireless** or **802.1x** in the Windows XP search engine.

Digital Certificate Installation

Before accessing the wireless network, you must have a digital certificate installed on your PC. Proceed to step 1 for instructions on how to request a digital certificate from a Windows 2000 RADIUS server through the Internet. If you need to request a digital certificate using a different method, contact your network administrator. If you already have a certificate installed, proceed to the "TLS Authentication for Windows XP" section.

Important: Before you install the digital certificate, make sure you have the IP address, User name, and Password for the RADIUS server of the wireless network. If you need any of this information, contact your network administrator beforehand.

Important: To request a digital certificate from a Windows 2000 RADIUS server, you must use an active Internet connection.

1. Open your PC's web browser. In the *Address* field, enter **http:*IP address of the RADIUS server*\certsrv**. For example, if the IP address of the RADIUS server is 10.10.10.2, then enter http:\\10.10.10.2\certsrv.

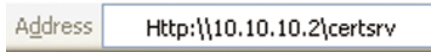

Figure C-11

2. Complete the *User name* and *Password* fields. Then click the **OK** button.

Figure C-12

3. Click the radio button next to **Request a certificate**, and then click the **Next** button.

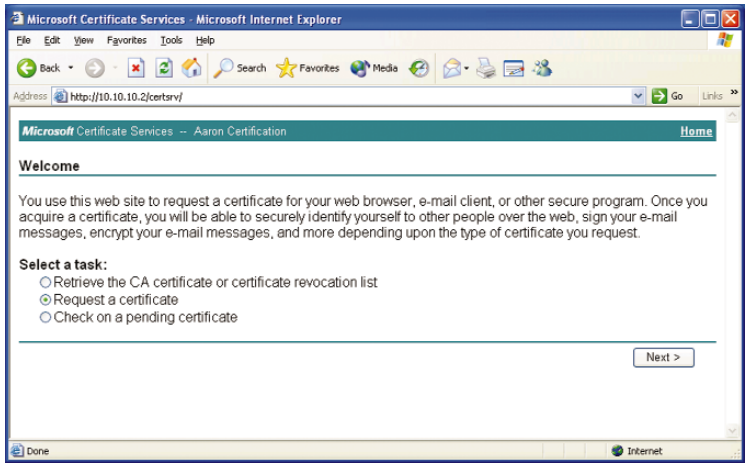

Figure C-13

4. Click the radio button next to **User certificate request:**, and make sure *User Certificate* is selected. Then click the **Next** button.

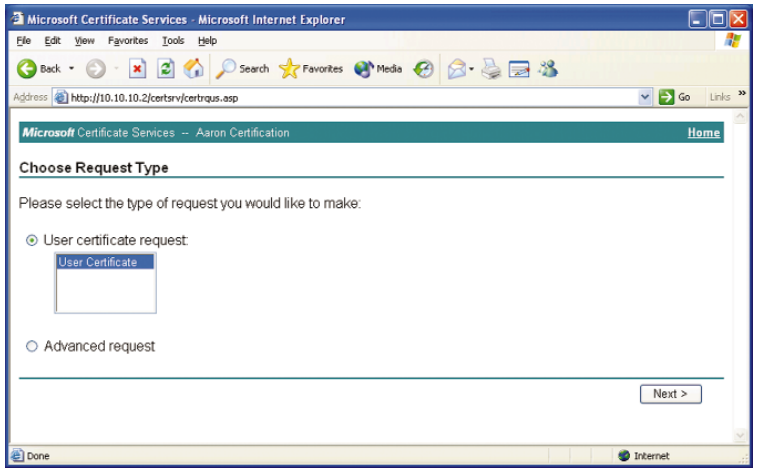

Figure C-14

5. Click the **Submit** button.

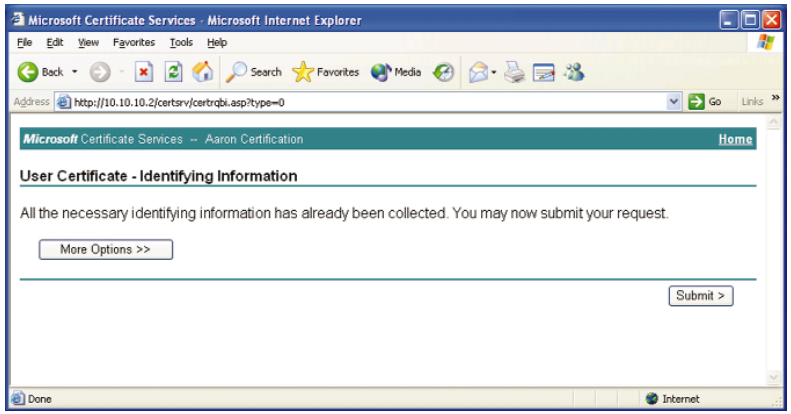

Figure C-15

6. Click **Install this certificate**.

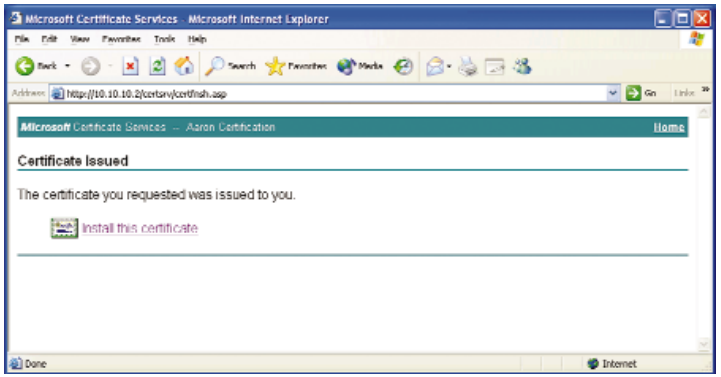

Figure C-16

7. You will be asked if you want to add the certificate to the Root Store. Click the **Yes** button.

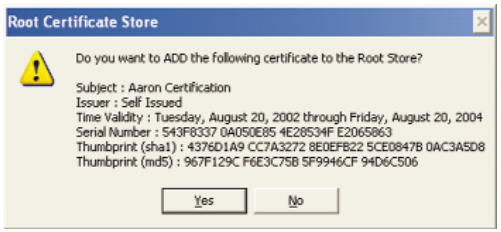

Figure C-17

8. You will be informed when the certificate has been successfully installed. Then close your PC's web browser.

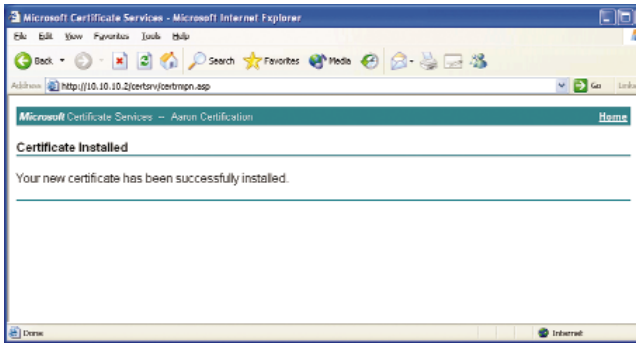

Figure C-18

Proceed to the next section, "TLS Authentication for Windows XP."

TLS Authentication for Windows XP

Important: Make sure you have a digital certificated installed on your PC. If you need to request a digital certificate, go to the previous section, "Digital Certificate Installation."

1. Make sure you have installed the wireless adapter correctly into your PC. Click the **Wireless Network Connection** icon located in your computer's system tray.

Figure C-19

2. The screen that appears will show any available wireless network. Select the appropriate network, and click the **Advanced...** button.

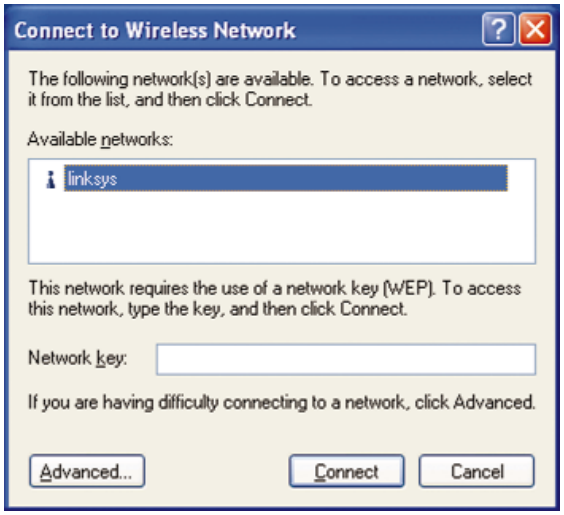

Figure C-20

Note: These are the instructions and screenshots for Windows XP without Service Pack 1 installed. If you have already installed Service Pack 1, enter the keyword **802.1x** in the Windows XP search engine for your 802.1x setup instructions.

3. Click the **Authentication** tab. Make sure the box next to **Enable network access control using IEEE 802.1X** is checked. In the drop-down box next to *EAP type*, select **Smart Card or other Certificate**. Make sure the box next to **Authenticate as computer when computer information is available** is checked. Then click the **OK** button.

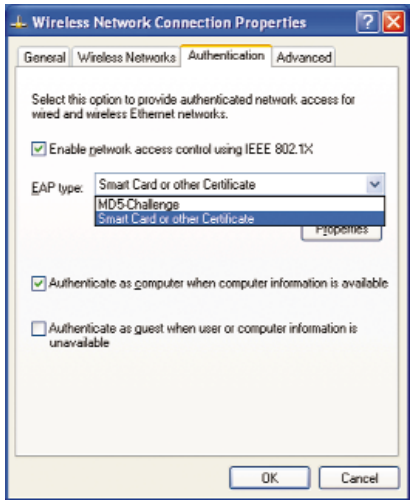

Figure C-21

4. Click the **Wireless Networks** tab. Select the wireless network you want to connect to, and click the **Configure** button.

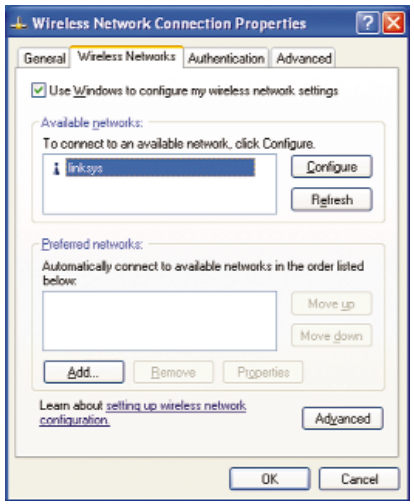

Figure C-22

5. Make sure the box next to **Data encryption (WEP enabled)** is checked. Make sure the box next to **The key is provided for me automatically** is checked. Then click the **OK** button.

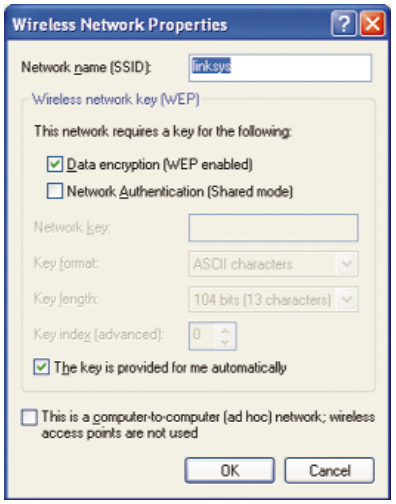

Figure C-23

6. Make sure the appropriate network is selected, and click the **OK** button.

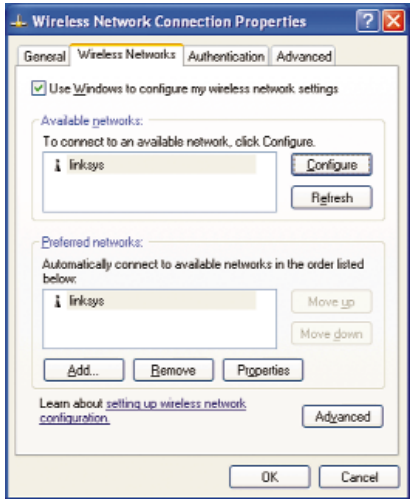

Figure C-24

7. Click the **Wireless Network Connection** icon located in your computer's system tray.

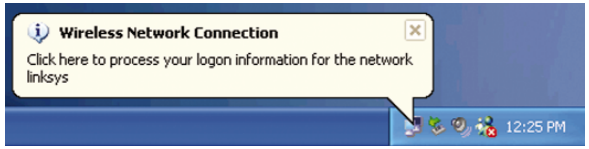

Figure C-25

8. If this is the first time you are using this 802.1x connection, you will be asked if you want to accept the wireless network connection. Click the **OK** button.

Figure C-26

9. Open your PC's web browser and test your Internet connection. If you are unable to connect to the Internet, double-check the settings you configured through Windows XP and the Router's web-based utility.

For more details about wireless networking or 802.1x on a Windows XP computer, enter the keyword **wireless** or **802.1x** in the Windows XP search engine.

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 address 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 the steps in this appendix to find the MAC address or IP address for your adapter in Windows 95, 98, Me, NT, 2000, and XP.

For Windows 95, 98, and Me:

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

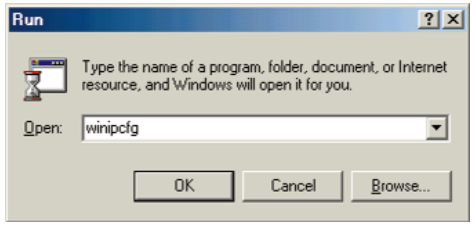

Figure D-1

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

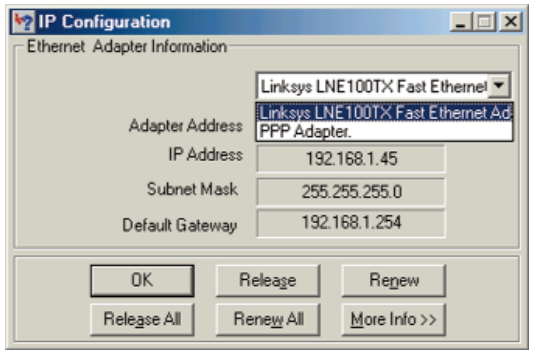

Figure D-2

3. Write down the Adapter Address as shown on your computer screen (see Figure E-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.

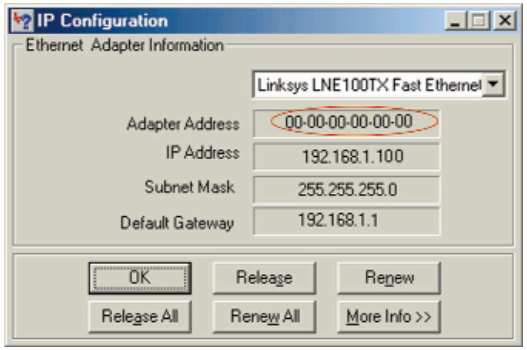

Figure D-3

   Write down the IP Address as shown on your computer screen. The example in Figure E-3 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

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

For Windows NT, 2000, and XP:

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

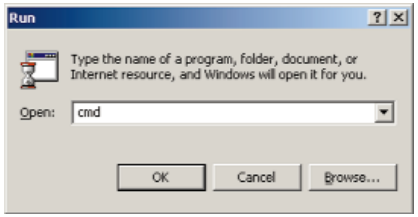

Figure D-4

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

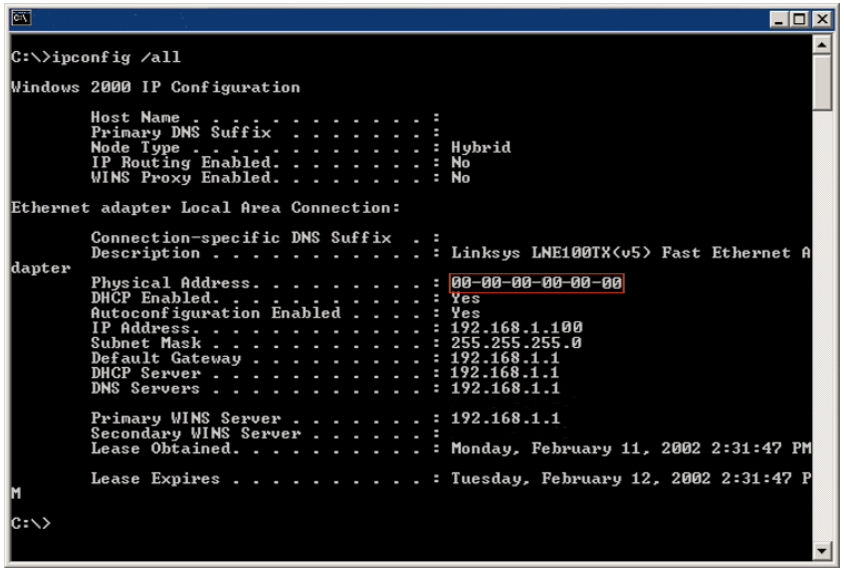

Figure D-5

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.

   Write down the IP Address as shown on your computer screen. The example in Figure E-5 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

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 UTP or STP wire.

802.11a - One of the IEEE standards for wireless networking hardware. Products that adhere to a specific IEEE standard will work with each other, even if they are manufactured by different companies. It specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz. The 802.11a standard uses the Orthogonal Frequency Division Multiplexing (OFDM) transmission method. Additionally, the 802.11a standard supports 802.11 features such as WEP encryption for security.

802.11b - One of the IEEE standards for wireless networking hardware. Products that adhere to a specific IEEE standard will work with each other, even if they are manufactured by different companies. The 802.11b standard specifies a maximum data transfer rate of 11Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

802.1x - Based on the Extensible Authentication Protocol (EAP), the 802.1x standard is one of the IEEE standards for network authentication and key management. It establishes a framework that supports multiple authentication methods. This standard can be incorporated into any type of network to enhance its security.

For example, a wireless user may use one of the authentication methods to access a wireless network protected by an authentication server. The user, also called the supplicant, sends a request to an access point or wireless router, also called the authenticator. The authenticator sends an identification request back to the user. After the user sends the authenticator the identification message, the authenticator forwards the user's identification message to the authentication server. If the server accepts the identification message, then the user is permitted access to the wireless network. The 802.1x standard can also support encryption key management to strengthen wireless network encryption services.

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

(NIC) is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

Ad-hoc Network - An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.

Automatic Fall-back - A feature provided by some wireless products to increase connection reliability. Automatic fall-back enables a device to dynamically shift between various data transfer rates. It works by decreasing the data transfer rate when interference increases, distance increases, and other factors undermine signal strength and quality.

Auto-MDI/MDIX - On a network hub or switch, an auto-MDI/MDIX port automatically senses if it needs to act as a MDI or MDIX port. The auto-MDI/MDIX capability eliminates the need for crossover cables.

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

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

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

Beacon Interval - A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

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.

Bottleneck – A traffic slowdown that results when too many network nodes try to access a single node, often a server node, at once.

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.

Buffer - A buffer is a shared or assigned memory area used by hardware devices or program processes that operate at different speeds or with different sets of priorities. The buffer allows each device or process to operate without being held up by the other. In order for a buffer to be effective, the size of the buffer and the algorithms for moving data into and out of the buffer need to be considered by the buffer designer. Like a cache, a buffer is a "midpoint holding place" but exists not so much to accelerate the speed of an activity as to support the coordination of separate activities.

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.

CPU (**C**entral **P**rocessing **U**nit) - The computing part of the computer. Also called the "processor," it is made up of the control unit and ALU.

CSMA/CD (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection) - 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.

CTS (**C**lear **T**o **S**end) - An RS-232 signal sent from the receiving station to the transmitting station that indicates it is ready to accept data.

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

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 (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - 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 - (**D**e**M**ilitarized **Z**one) 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.

Driver - A workstation or server software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific NIC, and is installed during the initial installation of a network-compatible client or server operating system.

DSSS (**D**irect-**S**equence **S**pread **S**pectrum) - DSSS generates a redundant bit pattern for all transmitted data. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver 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. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages.

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.

EAP (**E**xtensible **A**uthentication **P**rotocol) - An IETF standard that establishes an authentication protocol for network access. Many authentication methods, including passwords, certificates, and smart cards, work within this framework.

EAP-TLS - One type of mutual authentication method using the Extensible Authentication Protocol (EAP) and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses digital certificates and is more secure than MD5 authentication, which uses passwords. EAP-TLS authentication supports dynamic WEP key management.

EAP-TTLS - One type of mutual authentication method using the Extensible Authentication Protocol (EAP) and Tunneled Transport Layer Security (TTLS). EAP-TTLS uses a combination of certificates and another method, such as passwords. It is more secure than MD5 authentication, which uses passwords, and less secure than EAP-TLS authentication, which exclusively uses certificates. EAP-TTLS authentication supports dynamic WEP key management.

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

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.

Fast Ethernet - A 100 Mbps technology based on the 10Base-T Ethernet CSMA/CD network access method.

FHSS (**F**requency **H**opping **S**pread **S**pectrum) - FHSS continuously changes (hops) the carrier frequency of a conventional carrier several times per second according to a pseudo-random set of channels. Because a fixed frequency is not used, and only the transmitter and receiver know the hop patterns, interception of FHSS is extremely difficult.

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 programmable 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 (**F**ile **T**ransfer **P**rotocol) - 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.

Hub - The device that serves as the central location for attaching wires from workstations. Can be passive, where there is no amplification of the signals; or active, where the hubs are used like repeaters to provide an extension of the cable that connects to a workstation.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - 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—promoting 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.

Infrastructure Network - An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.

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 (**I**nternet **P**rotocol **Sec**urity) - A suite of protocols used to implement secure exchange of packets at the IP layer. IPSec supports two basic modes: Transport and Tunnel. Transport encrypts the payload of each packet, leaving the header untouched, while Tunnel mode encrypts both the header and the payload and is therefore more secure. IPSec must be supported on both transmitter and receiver and must share a public key. Tunnel mode is widely deployed in VPNs (Virtual Private Networks).

IRQ (**I**nterrupt **R**e**Q**uest) - A hardware interrupt on a PC. There are 16 IRQ lines used to signal the CPU that a peripheral event has started or terminated. Except for PCI devices, two devices cannot use the same line.

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.

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 (**M**ega**B**its **P**er **S**econd) - One million bits per second; unit of measurement for data transmission.

MD5 - A type of one-way authentication method that uses passwords. MD5 authentication is not as secure as the EAP-TLS or EAP/TTLS authentication methods. MD5 authentication does not support dynamic WEP key management.

MDI (**M**edium **D**ependent **I**nterface) - On a network hub or switch, a MDI port, also known as an uplink port, connects to another hub or switch using a straight-through cable. To connect a MDI port to a computer, use a crossover cable.

MDIX (**M**edium **D**ependent **I**nterface Crossed) - On a network hub or switch, a MDIX port connects to a computer using a straight-through cable. To connect a MDIX port to another hub or switch, use a crossover cable.

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

Motherboard - A motherboard is the physical arrangement in a computer that contains the computer's basic circuitry and components.

Multicasting - Sending data to a group of nodes instead of a single destination.

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.

NetBEUI (**NetB**IOS **E**xtended **U**ser **I**nterface) - The transport layer for NetBIOS. NetBIOS and NetBEUI were originally part of a single protocol suite that was later separated. NetBIOS sessions can be transported over NetBEUI, TCP/IP, and SPX/IPX protocols.

NetBIOS - The native networking protocol in DOS and Windows networks. Although originally combined with its transport layer protocol (NetBEUI), NetBIOS today provides a programming interface for applications at the session layer (layer 5). NetBIOS can ride over NetBEUI, its native transport, which is not routable, or over TCP/IP and IPX/SPX, which are routable protocols.

NetBIOS computers are identified by a unique 15-character name, and Windows machines (NetBIOS machines) periodically broadcast their names over the network so that Network Neighborhood can catalog them. For TCP/IP networks, NetBIOS names are turned into IP addresses via manual configuration in an LMHOSTS file or a WINS server.

There are two NetBIOS modes. The Datagram mode is the fastest mode, but does not guarantee delivery. It uses a self-contained packet with send and receive name, usually limited to 512 bytes. If the recipient device is not listening for messages, the datagram is lost. The Session mode establishes a connection until broken. It guarantees delivery of messages up to 64KB long.

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

Network Mask - Also known as the "Subnet Mask."

NIC (**N**etwork **I**nterface **C**ard) - A board installed in a computer system, usually a PC, to provide network communication capabilities to and from that computer system. Also called an adapter.

Node - A network junction or connection point, typically a computer or work station.

Notebook (PC) - A notebook computer is a battery-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, at temporary offices, and at meetings. A notebook computer, sometimes called a laptop computer, typically weighs less than five pounds and is three inches or less in thickness.

OFDM - Developed for wireless applications, Orthogonal Frequency Division Multiplexing (OFDM) technology offers superior performance-increased data rates and more reliable transmissions-than previous technologies, such as DSSS. OFDM is a scheme in which numerous signals of different frequencies are combined to form a single signal for transmission on the medium.

OFDM works by breaking one high-speed data stream into a number of lower-speed data streams, which are then transmitted in parallel. Each lower speed stream is used to modulate a subcarrier. Essentially, this creates a multi-carrier transmission by dividing a wide frequency band or channel into a number of narrower frequency bands or sub-channels. OFDM is also used for other applications, including powerline networking.

Packet - A unit of data routed between an origin and a destination in a network.

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

Partitioning - To divide a resource or application into smaller pieces.

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

PC Card - A credit-card sized removable module that contains memory, I/O, or a hard disk.

PCI (**P**eripheral **C**omponent **I**nterconnect) - A peripheral bus commonly used in PCs, Macintoshes and workstations. It was designed primarily by Intel and first appeared on PCs in late 1993. PCI provides a high-speed data path between the CPU and peripheral devices (video, disk, network, etc.). There are typically three or four PCI slots on the motherboard. In a Pentium PC, there is generally a mix of PCI and ISA slots or PCI and EISA slots. Early on, the PCI bus was known as a "local bus."

PCI provides "plug-and-play" capability, automatically configuring the PCI cards at startup. When PCI is used with the ISA bus, the only thing that is generally required is to indicate in the CMOS memory which IRQs are already in use by ISA cards. PCI takes care of the rest.

PCI allows IRQs to be shared, which helps to solve the problem of limited IRQs available on a PC. For example, if there were only one IRQ left over after ISA devices were given their required IRQs, all PCI devices could share it. In a PCI-only machine, there cannot be insufficient IRQs, as all can be shared.

PCMCIA - The PCMCIA (Personal Computer Memory Card International Association) is an industry group organized in 1989 to promote standards for a credit card-size memory or I/O device that would fit into a personal computer, usually a notebook or laptop computer.

Ping (**P**acket **IN**ternet **G**roper) - 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.

Plug-and-Play - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

POP3 (**P**ost **O**ffice **P**rotocol **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.

Port Mirroring - Port mirroring, also known as a roving analysis port, is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - 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 (**P**oint-to-**P**oint **T**unneling **P**rotocol) - 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 mode). One example of a tunneling service is secure access from a remote small office network to a headquarters corporate intranet via a Virtual Private Network (VPN) that traverses the Internet. However, tunneling services are not restricted to corporate environments and may also be used for personal (i.e., non-business) applications.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol used to control network access. RADIUS enables servers to authenticate users, so only legitimate users are granted network access. RADIUS servers are frequently used in 802.1x implementations; however, they are not specified by the 802.1x standard.

RIP (**R**outing **I**nformation **P**rotocol) - 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-11 (**R**egistered **J**ack-**11**) - A telephone connector that holds up to six wires. The RJ-11 is the common connector used to plug a telephone into a wall.

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

Roaming - In an infrastructure mode wireless network, this refers to the ability to move out of one access point's range and into another and transparently reassociate and reauthenticate to the new access point. This reassociation and reauthentication should occur without user intervention and ideally without interruption to network connectivity. A typical scenario would be a location with multiple access points, where users can physically relocate from one area to another and easily maintain connectivity.

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.

RTS (**R**equest **T**o **S**end) - An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

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

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - 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 (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are

hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

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.

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

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).

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.

Storage - The semi-permanent or permanent holding place for digital data.

STP (**S**hielded **T**wisted **P**air) - Telephone wire that is wrapped in a metal sheath to eliminate external interference.

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.

Swapping - Replacing one segment of a program in memory with another and restoring it back to the original when required.

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 (**T**ransmission **C**ontrol **P**rotocol) - 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 (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - 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 (**T**rivial **F**ile **T**ransfer **P**rotocol) - 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 hubs, 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 (**U**ser **D**atagram **P**rotocol) - 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 (**U**niform **R**esource **L**ocator) - 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.

UTP - Unshielded twisted pair is the most common kind of copper telephone wiring. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable.

VPN (**V**irtual **P**rivate **N**etwork) - A technique that allows two or more LANs to be extended over public communication channels by creating private communication subchannels (tunnels). Effectively, these LANs can use a WAN as a single large "virtually private" LAN. This removes the need to use leased lines for WAN communications through secure use of a publicly available WAN (such as the Internet). Examples of VPN technology are: PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (Internet Protocol Security).

WAN (**W**ide **A**rea **N**etwork) - 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.

WEP (**W**ired **E**quivalent **P**rivacy) - A data privacy mechanism based on a 64-bit or 128-bi shared key algorithm, as described in the IEEE 802.11 standard.

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.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

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

Appendix F: Specifications

Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11a, IEEE 802.11b
Ports	
Internet:	One 10/100 RJ-45 Port for Cable/DSL Modem
LAN:	Four 10/100 RJ-45 Switched Ports One Power Port
Button	One Reset Button
Cabling Type	Category 5 Ethernet Network Cable or better
Transmit Power	
802.11a:	15 dBm
802.11b:	12 dBm
Receive Sensitivity	
802.11a:	1 Mbps: -93 dBm 2 Mbps: -91 dBm 5.5 Mbps: -88 dBm 11 Mbps: -84 dBm
802.11b:	6 Mbps: -86dBm 9 Mbps: -85dBm 12 Mbps: -84dBm 18 Mbps: -82dBm 24 Mbps: -80dBm 36 Mbps: -75dBm 48 Mbps: -68dBm 54 Mbps: -67dBm
Modulation	
802.11a:	BPSK, QPSK, 16-QAM, 64-QAM
802.11b:	CCK, QPSK, BPSK

Network Protocols	
802.11a:	TCP/IP, NetBEUI, IPX/SPX
802.11b:	TCP/IP, NetBEUI, IPX/SPX
LED Indicators	Power, Diag
Internet:	Link/Act, 100
LAN:	Link/Act, Full/Col, 100
802.11a:	Act, Link
802.11b:	Act, Link

Environmental

Dimensions	7.32" x 1.89" x 6.89" (186 mm x 48 mm x 175 mm)
Unit Weight	14.1 oz. (0.4 kg)
Power	External, 5V DC, 2.5 A
Certifications	FCC Class B, CE Mark
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 LINKSYS'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS DOES NOT OFFER REFUNDS FOR ANY PRODUCT.

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

Appendix H: Contact Information

For help with the installation or operation of the Dual-Band Wireless A+B Broadband Router, contact Linksys Technical Support at one of the phone numbers or Internet addresses below.

Sales Information	800-546-5797 (1-800-LINKSYS)
Technical Support	800-326-7114
RMA Issues	949-271-5461
Fax	949-265-6655
Email	support@linksys.com
Web site	http://www.linksys.com
FTP site	ftp://ftp.linksys.com

Federal Communication Commission Interference Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

The use of this device is restricted to indoor operations, and that outdoor operations are prohibited under FCC rules and regulations.

www.linksys.com

© Copyright 2002 Linksys, All Rights Reserved.