Chapter 6: Configuring the Dual-Band Wireless A + G Access Point

Note: The Access Point is designed to function properly after using the Setup Wizard. This chapter is provided solely for those who wish to perform more advanced configuration or monitoring.

The Access Point's settings can be configured through your web browser with the Web-Based Utility. This chapter explains how to configure the Access Point in this manner.

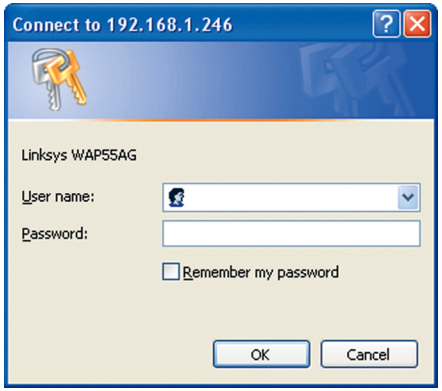

Figure 6-1

Type the Access Point's IP Address into your web browser's address field. (The default IP address is 192.168.1.246.) (Should you need to learn what IP Address the Access Point presently uses, run the Setup Wizard. It will scan the Access Point and give you its IP Address.) Press the **Enter** key and the following screen, shown in Figure 6-1, will appear. Leave the User Name field blank. The first time you open the Web-Based Utility, use the default password **admin**. You can set a new password from the Password tab.

The Setup Tab

The first screen that appears, shown in Figure 6-2, displays the *Setup* tab. This allows you to change the Access Point's general settings. These settings are described here. Click the **Apply** button to apply your changes or **Cancel** to cancel your changes. If you require online help, click the **Help** button.

Firmware. This will display the Access Point's current firmware version. Firmware can be upgraded from the Help tab.

Access Point Name. You may assign any name to the Access Point, which is how the Access Point is identified on your network. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. Verify this is the name you wish to use and click the **Apply** button to set it.

MAC Address. The MAC Address of the LAN interface - connected through the LAN Port - is displayed here.

Configuration Type. This selection tells the Access Point how IP Addresses are determined on your network. If you are using a DHCP server on your network to automatically generate different IP Addresses to each device, select **Automatic Configuration - DHCP**. Select **Static IP Address** if each device uses its own IP Address. The Access Point's default IP Address, Subnet Mask, and Default Gateway will appear in the appropriate fields.

Figure 6-2

Fields for configuring your wireless connections, both 802.11a and 802.11g-draft are located under this information. You must configure any wireless standard you are using on your network.

MAC Address. The first line of data provided about both wireless standards is the MAC Address of the wireless interface.

SSID. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.

Channel. Select the appropriate channel from the list provided to correspond with your network settings. This should be between 1 and 11 (in North America) for 2.4GHz/802.11b devices and 36 and 64 (in North America) for 5GHz/802.11a devices. All points in your wireless network must use the same channel in order to function correctly.

WEP. The WEP Encryption method is **Disabled** by default. To enable WEP, click the **WEP Key Setting** button.

Mode. This option works only for 802.11b and 802.11g-draft devices in your wireless network. Select **Mixed** and both Wireless-G and Wireless-B computers will be allowed on the network, but the speed will be reduced. Select **G-Only** for maximum speed, but no Wireless-B users will be allowed on the network.

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

WEP Encryption

Setting WEP Encryption through the Web-based Browser Utility is done by clicking the **WEP Key Setting** button on the Setup Screen for any type of wireless device used on your network.

This will open the WEP key setting screen. This screen is shown in Figure 6-3 for 802.11a wireless products and Figure 6-4 for 802.11g-draft wireless products. Select the WEP encryption for the type(s) of wireless technology you are using. From this screen, you can select the type of WEP encryption to use as well as set the WEP Key for that encryption.

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

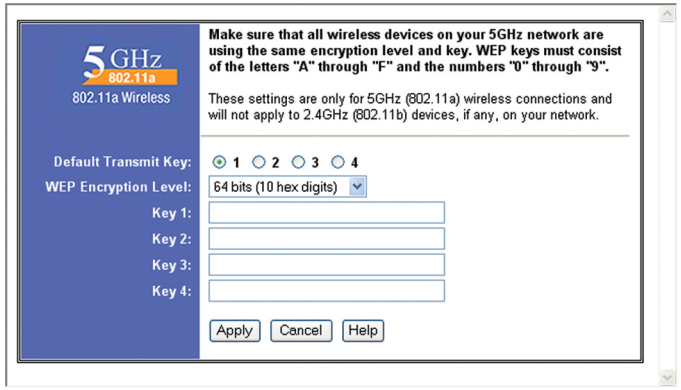

Figure 6-3

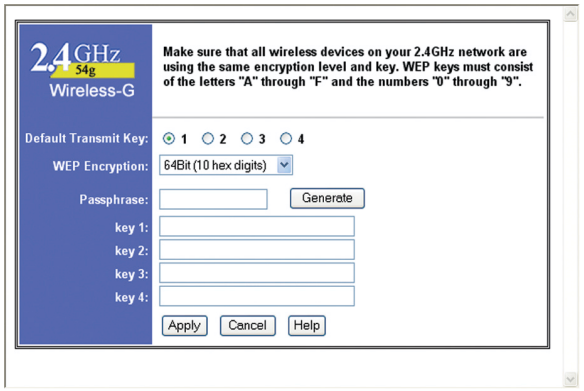

Figure 6-4

From the pull-down menu, select the type of WEP encryption you wish to use.

If you are using 802.11a wireless technology, you will need to enter the key manually.

If you are using 802.11g-draft wireless technology and wish to use a WEP Passphrase, it can be a maximum of 16 alphanumeric characters. This passphrase may not work with non-Linksys products due to possible incompatibility with other vendors' passphrase generators. The WEP Key can be generated using your Passphrase or you can enter it manually. Type that here.

The WEP key must consist of the letters “A” through “F” and the numbers “0” through “9” and should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption. (When using 802.11a wireless technology, 152-bit encryption is also available. The WEP key under this setting should be 32 characters in length.) All points in your wireless network must use the same WEP key to utilize WEP encryption.

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

Click the **Apply** button to apply your changes and return to the Setup tab or **Cancel** to cancel your changes. To clear any of the information you’ve typed but not yet applied, click the **Clear** button.

The Password Tab

The *Password* tab, shown in Figure 6-5, allows you to change the Access Point’s password and restore factory defaults.

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

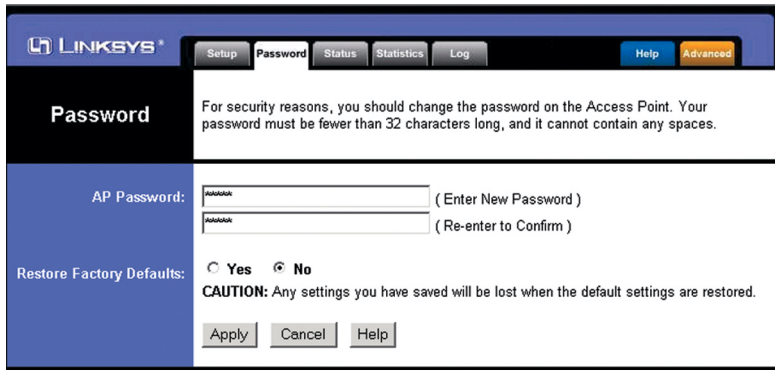

Figure 6-5

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

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

Important: Restoring the Access Point’s factory defaults will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.), and replace them with the factory defaults.

The Status Tab

The *Status* tab, shown in Figure 6-6, displays current information on the Access Point, its settings and performance.

The information displayed in these fields reflects the settings that you saved on the Setup tab. For any information about what these settings mean, turn back to the appropriate heading in the section for the Setup tab.

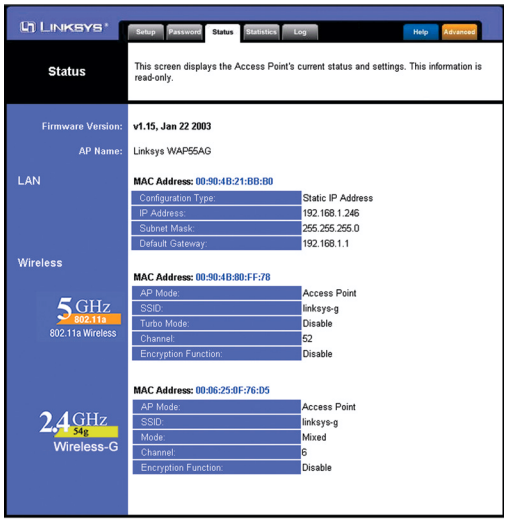

Figure 6-6

The Statistics Tab

The *Statistics* tab, shown in Figure 6-7, displays information on how well the Access Point is transmitting data. It shows the amount of data packets dropped with those transmitted. Remember, some packet loss is common in networking.

To update the statistics, click the **Refresh** button. Click the **Help** button for more information about this screen

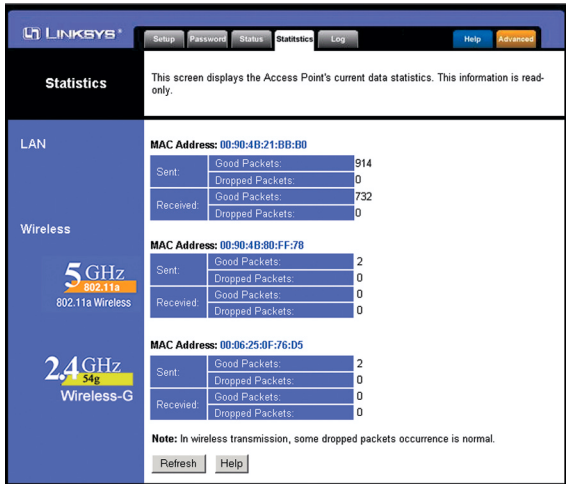

Figure 6-7

The Log Tab

To view a log of the Access Point's activity, select the **Log** tab, shown in Figure 6-8.

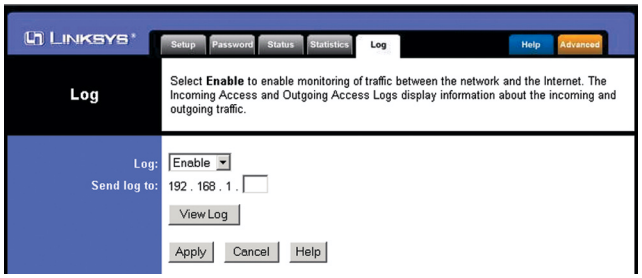

Figure 6-8

Log. To enable permanent logging activity, click the **Enable** radio button beside *Log*. The default setting for this function is **Disable**.

If you have chosen to monitor the Access Point's traffic, then you can designate a PC that will receive permanent log files periodically. In the *Send Log to* field, enter the IP address of this PC. To view these permanent logs, you must use Logviewer software, which can be downloaded free of charge from *www.linksys.com*.

To see a temporary log of the Access Point's most recent activities, click the **View Log** button.

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

The Help Tab

For help on the various tabs in this Web-based Utility, along with upgrading the Access Point's firmware and viewing this User Guide, click the *Help* tab, shown in Figure 6-9.

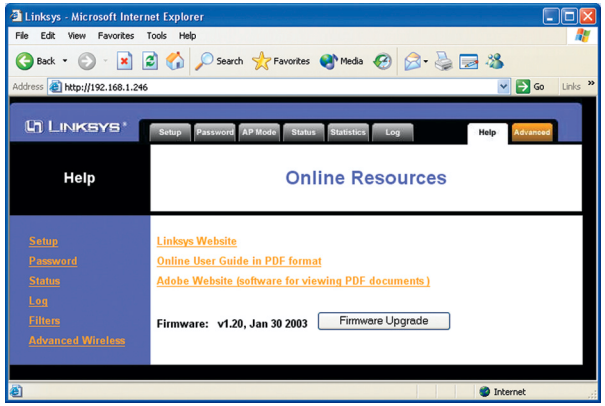

Figure 6-9

Clicking the names of the tabs on the left-hand side of the screen brings up help for those tabs.

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

Click the **Linksys Website** link to connect to the Linksys homepage.

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

Firmware can be upgraded by clicking the **Upgrade Firmware** link. Do not upgrade your firmware unless you are experiencing problems with the Access Point.

UPGRADING FIRMWARE:

Before upgrading the Access Point's firmware, be sure to download the firmware from Linksys's website at www.linksys.com.

Once that is done, click the **Upgrade Firmware** link on the Help Tab. This will bring up the screen shown in Figure 6-10.

Type in the location of the firmware's file or click the **Browse** button to find the file. Then, click the **Upgrade** button to upgrade the firmware. To cancel the procedure, click **Cancel** or for more information, click **Help**.

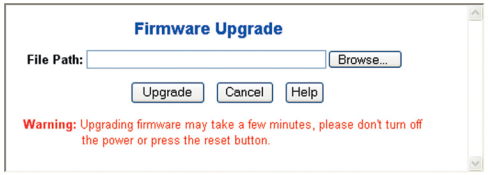

Figure 6-10

The Filters Tab

The *Filters* tab, shown in Figure 6-11, allows you to block and allow certain computers, by their MAC Address, from communicating with the Access Point.

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

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

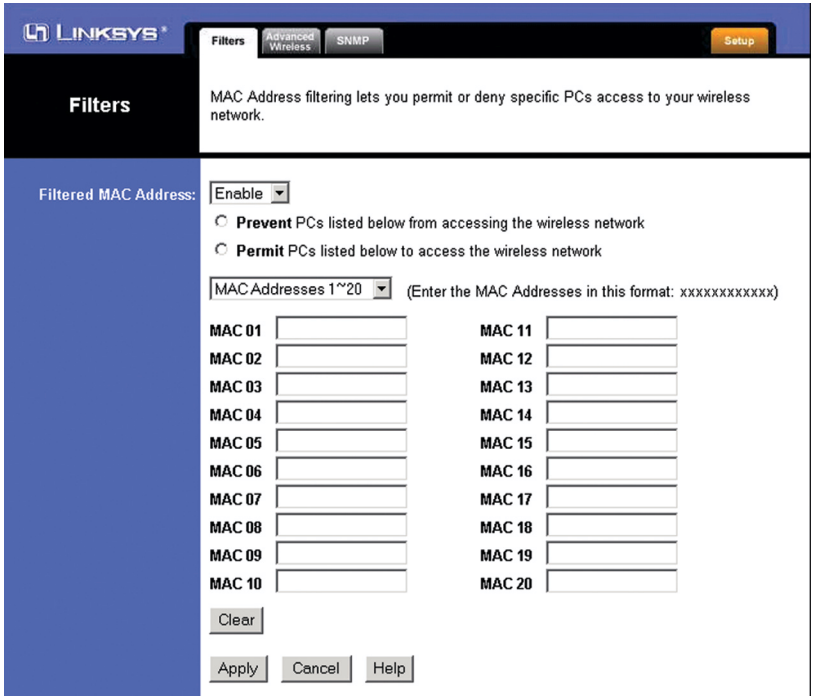

Figure 6-11

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

The Advanced Wireless Tab

Before making any changes to the *Advanced Wireless* tab, shown in Figure 6-12, please check your wireless settings on other systems, as these changes will alter the effectiveness of the Access Point. In most cases, these settings do not need to be changed.

The following settings are used in both wireless settings:

Transmission Rates. The basic transfer rates should be set depending on the speed of your wireless network. You can select from a range of transmission speeds or select **Best** to have the Access Point automatically engage the network's optimum speed.

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**.

Authentication Type. This setting allows the Access Point to authenticate communication with the wireless devices in your network. You may choose between **Auto**, **Open System** or **Shared Key**. With the **Shared Key** setting, all wireless devices must have the same WEP keys so that the Access Point and the client can authenticate each other and start transmitting data. With the **Open System** setting, any device can join a network without performing any security check. The Authentication Type default setting is to **Auto**, which means that the Access Point will automatically detect whether a wireless device is set to **Shared Key**, **Open System**, and transmit data appropriately.

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

RTS Threshold. This value should remain at its default setting of 2,346. Should you encounter inconsistent data flow, only minor modifications are recommended.

Fragmentation Length. This specifies the maximum size a data packet will be before splitting and creating a new packet and should remain at its default setting of 2,346. A smaller setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

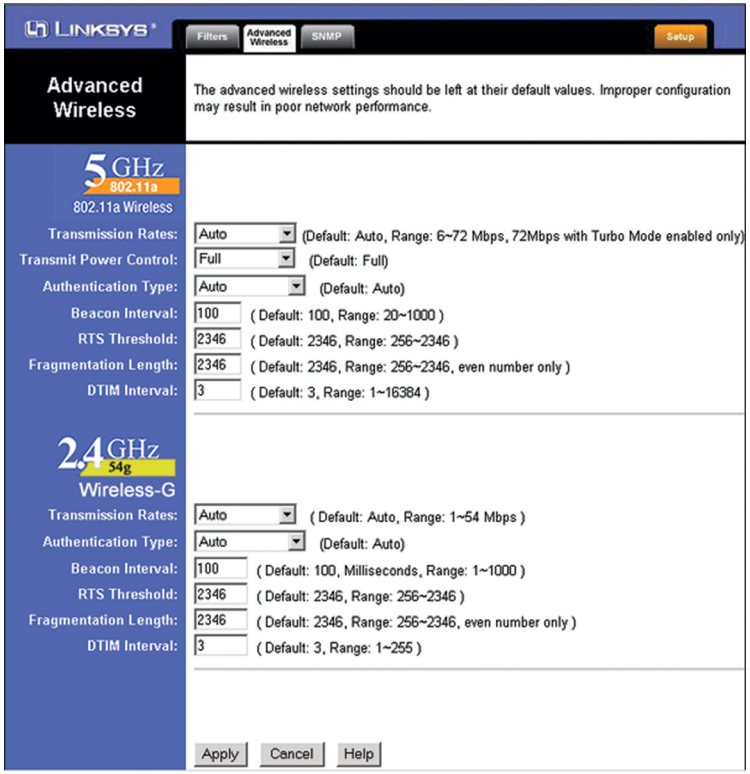

Figure 6-14

DTIM Interval. This value 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 Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Access Point Clients hear the beacons and awaken to receive the broadcast and multicast messages.

Transmission Power. (This applies to 5GHz/802.11a devices only.) This option allows you to set the power at which the Access Point transmits. This will allow you to prevent transmission outside your network radius and possible lapses in network security. Selecting a value other than FULL may limit the coverage area and data rates of your wireless PCs.

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

The SNMP Tab

The *SNMP* tab, shown in Figure 6-15, allows you to customize the Simple Network Management Protocol (SNMP) settings. SNMP is a popular network monitoring and management protocol.

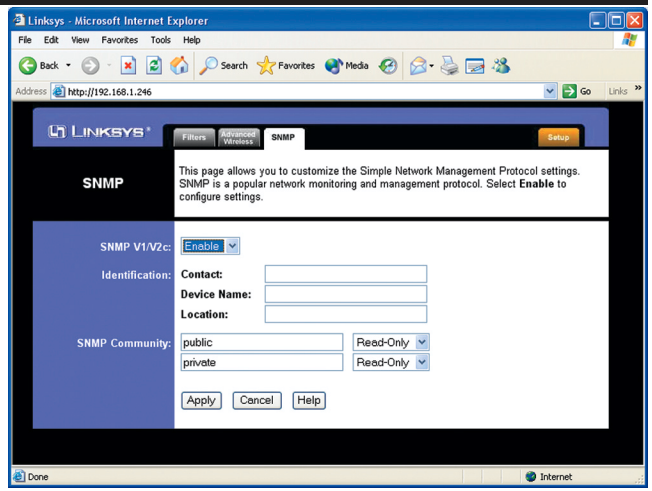

Figure 6-15

The Identification settings let you designate the Contact, Device Name, and Location information for the Access Point. The SNMP Community settings allow names to be assigned to any SNMP communities that have been set up in the network. You can define two different SNMP communities, with the default names being Public and Private.

SNMP V1/V2c. To enable the SNMP support feature, select **Enable**. Otherwise, select **Disable**.

Identification. In the *Contact* field, enter contact information for the Access Point. In the *Device Name* field, enter the name of the Access Point. In the *Location* field, specify the area or location where the Access Point resides.

SNMP Community. You may change the name from its default, Public. Enter a new name in the *Public* field. Then configure the community's access as either Read-Only or Read-Write.You may change the name from its default, Private. Enter a new name in the *Private* field. Then configure the community's access as either Read-Only or Read-Write.

When you've completed making any changes on this tab, click the **Apply** button to save those changes or **Cancel** to cancel your changes. For more information on this tab, you can click the **Help** button.

Appendix A: Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the Access Point. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

Frequently Asked Questions

Can the Access Point act as my DHCP Server?
No. The Access Point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities.

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 user guide to determine if it supports operation over a network.

Can I play multiplayer games with other users of the wireless network?
Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

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

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

What is Infrastructure?
An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers.

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

What is 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.

Would the information be intercepted while transmitting on air?
WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, the WLAN series offers the encryption function (WEP) to enhance security and access control. Users can set it up depending upon their needs.

Can Instant Wireless products support file and printer sharing?
Instant Wireless™ products perform the same function as LAN products. Therefore, Instant Wireless™ products can work with Netware, Windows NT/2000, or other LAN operating systems to support printer or file sharing.

What is WEP?
WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared-key algorithm, as described in the IEEE 802.11 standard.

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

How do I avoid interference?
Using multiple Access Points on the same channel and in close proximity to one another will generate interference. When employing multiple Access Points, be sure to operate each one on a different channel (frequency).

How do I reset the Access Point?
Press the **Reset** button on the back of the Access Point for about ten seconds. This will reset the unit 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 an Access Point and wireless PC will create signal loss. Leaded glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with your Access Point 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, check the Advanced tab of the Web-Based Utility and make sure that FULL is selected in the Transmission Rate field.

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

Does the Access Point function as a firewall?
No. The Access Point is only a bridge from wired Ethernet to wireless clients.

I have excellent signal strength, but I cannot see my network.
WEP is probably enabled on the Access Point, 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 on your wireless network.

What is the maximum number of users the Access Point facilitates?
No more than 65, but this depends on the volume of data and may be less if many users create a large amount of network traffic.

How many channels/frequencies are available with the Access Point?
Using 802.11a, there are eight available frequencies, ranging from 5.15GHz to 5.32GHz. 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. Turbo mode must be enabled on both the Access Point and the wireless PCs to function. 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, while higher speeds may be achieved with 802.11a, throughput degrades more quickly. (See Figure A-1.)

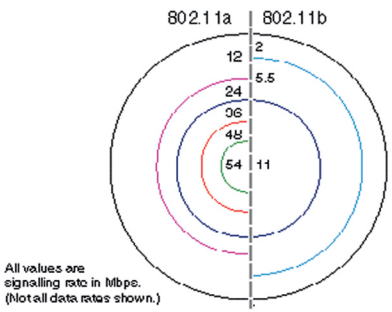

Figure A-1

Appendix B: Setting Up the TCP/IP and IPX Protocols

Setting Up TCP/IP in Windows

Before a computer can communicate with the Access Point, it must be configured with the TCP/IP protocol. If you know how to set up TCP/IP on your computers, do so now. Otherwise, use the guidelines below to help get TCP/IP installed on all of the computers that need to communicate with the Access Point. If you are unable to successfully install TCP/IP on one or more computers after following the directions, contact the manufacturer of your computers' network operating system for further assistance. Check with your network administrator for your TCP/IP settings.

The directions below provide general guidelines for coming up with IP addresses and subnet masks. Check with your network administrator to see if you need to use specific IP addresses or DHCP settings.

First, each computer on the network will require an IP address, which is a series of numbers, separated by periods, identifying the PC on the network. To make things simple, you should use the following numbering scheme:

192.168.1.X

In this example, X is a unique, arbitrarily assigned number from 1 to 254. Each computer must have its own unique X number. Note: Never use 0, 250 or 255 for X. These numbers are reserved by TCP/IP for other uses.

For example, if you have three computers, you could number them as follows:

192.168.1.17
192.168.1.44
192.168.1.126

In this case, 17, 44, and 126 are arbitrary numbers between 1 and 254.

Each computer will also require a subnet mask, which is a numerical “filter” that tells a computer what kinds of TCP/IP data packets to accept. If you’re not sure which mask to use, the following mask is recommended:

255.255.255.0

The following instructions are provided as examples for reference only. For complete instructions on installing and troubleshooting TCP/IP and IPX, consult your Windows operating system documentation.

TCP/IP Setup for Windows 95, 98, and Millennium

1. Click the **Start** button, select **Settings**, and open the **Control Panel**. Inside the Control Panel, double-click the **Network** icon.

2. If the *TCP/IP Protocol* is listed for your network adapter, go to step five. Otherwise, click the **Add** button.

3. When the **Component Type** window appears, select **Protocol** and click the **Add** button.

4. Select **Microsoft** in the Manufacturers list and choose **TCP/IP** in the Network Protocols list. Then, click the **OK** button.

5. When the Network window reappears, click **TCP/IP**. Then, click the **Properties** button.

6. Select **Specify an IP Address**.

7. Enter an IP Address for the computer, along with a Subnet Mask. Click the **OK** button. If you do not have these values, consult your network administrator.

8. When the Network window reappears, click the **OK** button. Restart your machine. TCP/IP has now been successfully installed.

IPX Setup for Windows 95, 98, and Millennium

1. Click the **Start** button, select **Settings**, and open the **Control Panel**. Inside the Control Panel, double-click the **Network** icon.

2. If the *TCP/IP Protocol* is listed for your network adapter, go to step four. Otherwise, click the **Add** button.

3. When the **Component Type** window appears, select **Protocol** and click the **Add** button.

4. Select **Microsoft** in the Manufacturers list and choose **IPX/SPX protocol** in the Network Protocols list. Then, click the **OK** button.

TCP/IP Setup for Windows NT 4.0

1. Click the **Start** button, select **Settings**, and open the **Control Panel**. Inside the Control Panel, double-click the **Network** icon.

2. When the **Network** window appears, click the **Protocols** tab. Then, click the **Add** button.

3. Find the **TCP/IP protocol** in the **Select Network Protocol** field. Click it once and then click the **OK** button.

4. When asked if you want to use DHCP, choose **No**.

5. If asked to supply your Windows NT CD, do so. NT will copy the necessary files to your system. You may have to switch between the Access Point's Setup CD and the NT CD.

6. When TCP/IP appears in the **Network Protocols** window, click the **Bindings** tab. Windows will store your new bindings.

7. Click the **Protocols** tab. Then, select **TCP/IP**.

8. Click the **Properties** button. Select the type of network adapter you have from the Adapters box and select **Specify an IP Address**.

9. Enter the computer's IP Address and Subnet Mask. Check with your network administrator for your settings.

10. Enter your Default Gateway if you have one.

Note: a Default Gateway is not required. Check with your network administrator.

11. When you finish, click the **OK** button. If NT asks about WINS, ignore it.

12. When the **Network** window reappears, click the **Close** button. Restart your computer when prompted. TCP/IP has now been successfully installed.

IPX Setup for Windows NT 4.0

1. Click the **Start** button, select **Settings**, and open the **Control Panel**. Inside the Control Panel, double-click the **Network** icon.

2. When the **Network** window appears, click the **Protocols** tab. Then, click the **Add** button.

3. Find the **IPX/SPX protocol** in the **Select Network Protocol** field. Click it once and click the **OK** button.

TCP/IP Setup for Windows 2000

1. At the Windows 2000 desktop, right click **My Network Places** and select **Properties**. Then, right click **Local Area Connection**. Choose **Properties**.

2. If the *TCP/IP Protocol* is listed for your network adapter, go to step five. Otherwise, click the **Install** button.

3. When the **Component Type** window appears, select **Protocol**, and click the **Add** button.

4. Select **Internet Protocol (TCP/IP)** from the list and click the **OK** button.

5. When the **Local Area Connection Properties** window reappears, select **TCP/IP**, and click the **Properties** button.

6. Select **Use the following IP Address**.

7. Enter an IP Address for the computer, along with a Subnet Mask and Default Gateway. Then, click the **OK** button. If you do not have these values, consult your network administrator.

8. When the **Local Area Connection Properties** window reappears, click the **OK** button. TCP/IP has now been successfully installed.

IPX Setup for Windows 2000

1. At the Windows 2000 desktop, right click **My Network Places**. Then right click **Local Area Connection**. Choose **Properties**.

2. If the *NWLink IPX/SPX/NetBIOS Compatible Transport Protocol* is listed for your network adapter, click the **Cancel** button. Otherwise, click the **Install** button.

3. When the Component Type window appears, select **Protocol** and click the **Install** button.

4. Select **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol** from the list and click the **OK** button.

5. When the **Network** window reappears, click the **OK** button. Restart your computer. NWLink IPX/SPX/NetBIOS Compatible Transport Protocol has now been successfully installed.

TCP/IP Setup for Windows XP

1. Click the **Start** button and open the **Control Panel**.

2. Double click the **Network and Internet Connections** icon.

3. Double click the **Network Connections** icon.

4. Right click the **Local Area Connection** icon and select **Properties**.

5. If the *TCP/IP Protocol* is listed for your network adapter, go to step five. Otherwise, click the **Install** button.

6. When the **Component Type** window appears, select **Protocol**, and click the **Add** button.

7. Select **Internet Protocol (TCP/IP)** from the list and click the **OK** button.

8. When the **Local Area Connection Properties** window reappears, select **TCP/IP**, and click the **Properties** button.

9. Select **Use the following IP Address**.

10. Enter an IP Address for the computer, along with a Subnet Mask and Default Gateway. Then, click the **OK** button. If you do not have these values, consult your network administrator.

11. When the **Local Area Connection Properties** window reappears, click the **OK** button. TCP/IP has now been successfully installed..

Appendix C: Glossary

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.

802.11g - A proposed, but as yet unratified extension of the IEEE 802.11 standard for wireless networking hardware. The draft 802.11g specifications used by Linksys specify a maximum data transfer rate of 54Mbps using OFDM modulation, an operating frequency of 2.4GHz, backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

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

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.

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.

Bridge - A device that interconnects different networks together.

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.

BSS (**B**asic **S**ervice **S**et) - An infrastructure network connecting wireless devices to a wired network using a single access point.

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.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - In local area networking, this is the CSMA technique that combines slotted time-division multiplexing with carrier sense multiple access/collision detection (CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

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 manage centrally 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.

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

DSSS (**D**irect-**S**equence **S**pread **S**pectrum) - DSSS generates a redundant bit pattern for all data transmitted. 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 end-

point), 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.

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.

ESS (**E**xtended **S**ervice **S**et) - A set of more than two or more BSSs (multiple access points) forming a single network.

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.

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.

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.

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.

Hop - The link between two network nodes.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - 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 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 (**I**nternet **P**rotocol) - The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to be able to understand each other.

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 packet 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.

IPX (**I**nternetwork **P**acket E**X**change) - A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another.

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.

LAN (**L**ocal **A**rea **N**etwork) - 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).

MAC (**M**edia **A**ccess **C**ontrol) **Address** - 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.

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

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.

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

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.

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

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.

RJ-45 (**R**egistered **J**ack-**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.

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).

SSID (**S**ervice **S**et **ID**entifier) - A unique name shared among all points in a wireless network. The SSID must be identical for each point in the wireless network and is case-sensitive.

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

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

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

TCP (**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 devices over a network. 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.

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.

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

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

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

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

Appendix D: Specifications

Standards	IEEE 802.11a, IEEE802.11b, draft IEEE 802.11g, 802.3, IEEE 802.u
Ports	One 10/100 RJ-45 Port, One Power Port
Buttons	One Reset Button
Cabling Type	Ethernet Network Cable
LEDs	Power, Diag LAN: Link/Act, Full/Col, 100 802.11a: Act, Link 802.11g: Act, Link
Transmit Power	802.11a: Max. 15dBm 802.11g: typical 20dBm 802.11b: typical 16dBm
Security Features	MAC address filtering, WEP Encryption
WEP Key Bits	64/128/152-Bit

Environmental

Dimensions	7.32" x 1.89" x 6.89" (186 mm x 48 mm x 175 mm)
Unit Weight	14.11 oz. (0.4 kg)
Power	External, 5V DC, 2.5A
Certifications	FCC
Operating Temp.	32ºF to 104ºF (0ºC to 40ºC)
Storage Temp.	-4ºF to 158ºF (-20ºC to 70ºC)
Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing

Appendix E: 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 F: Contact Information

For help with the installation or operation of this product, contact Linksys Technical Support at one of the phone numbers or Internet addresses below.

Sales Information	800-546-5797 (LINKSYS)
Technical Support	800-326-7114
RMA (Return Merchandise Authorization) Issues	www.linksys.com (or call 949-271-5461)
Fax	949-261-8868
Email	support@linksys.com
Web	http://www.linksys.com
FTP Site	ftp.linksys.com

LINKSYS®

http://www.linksys.com

© Copyright 2003 Linksys, All Rights Reserved.