Note: In Wireless Bridge mode, the Access Point can **ONLY** be accessed by another access point in Wireless Bridge mode. In order for your other wireless devices to access the Access Point, you must reset it to Access Point mode. The two modes are mutually exclusive.

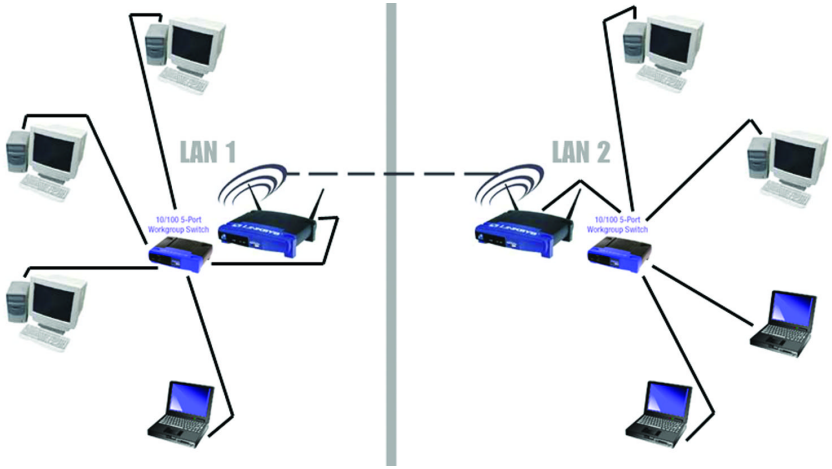

Figure 6-7

The Status Tab

The *Status* tab, shown in Figure 6-8, will display current information on the Access Point, its settings, and its performance.

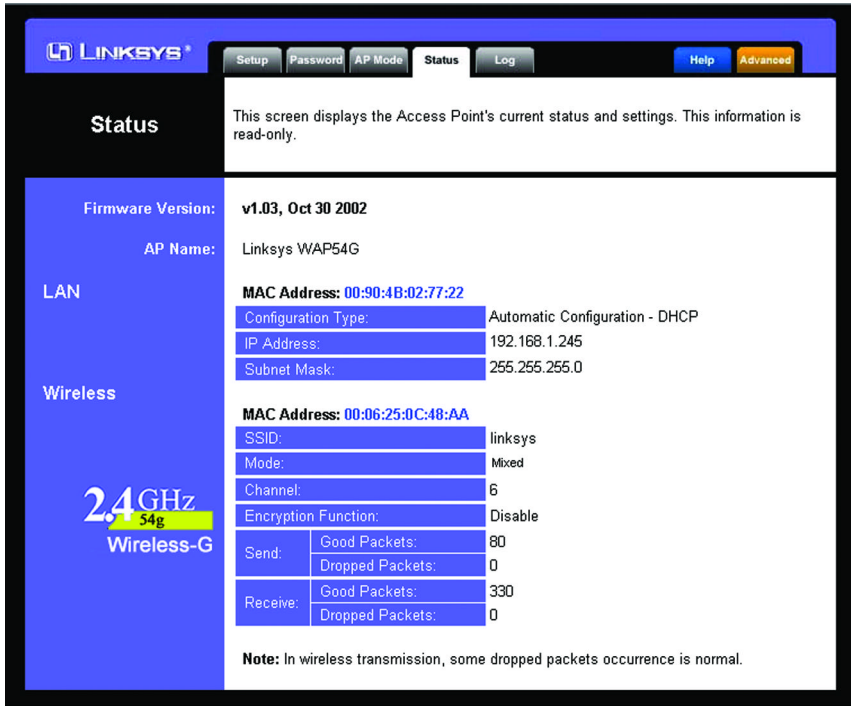

Figure 6-8

- **Firmware Version.** The current version of the Access Point's firmware is displayed. Firmware should only be upgraded from the *Help* tab if you experience problems with the Access Point.

- **AP Name.** This displays the name you assigned to the Access Point.

LAN

- **MAC Address**. The MAC Address of the LAN interface is displayed here.
- **Configuration Type**. This displays how the Access Point is assigned an IP address, either Automatic Configuration - DHCP, if assigned by DHCP server, or Static IP Address and its IP Address, Subnet Mask, and Default Gateway address, if assigned by Static IP Address server.
- **IP Address**. This IP address is the unique IP address of the Access Point.
- **Subnet Mask**. The Access Point's Subnet Mask (also known as an IP Mask), matches the Subnet Mask of your Ethernet network.

Wireless

- **MAC Address**. The MAC Address of the LAN interface is displayed here.
- **SSID.** The unique name shared among all points in your wireless network is displayed here.
- **Mode.** The Access Point's mode is displayed here.
- **Channel.** The wireless channel shared by all wireless devices connected to this Access Point is displayed here.
- **Encryption Function.** The encryption method you chose in the Setup Wizard or changed from the *Setup* tab of this Web-based Utility is displayed here.
- **Send and Receive**. The *Send* and *Receive* fields display the number of successful or dropped packets that have been sent or received. Some packet loss is normal in wireless networking.

The Log Tab

To view a log of the Access Point's activity, select the **Log** tab, shown in Figure 6-9.

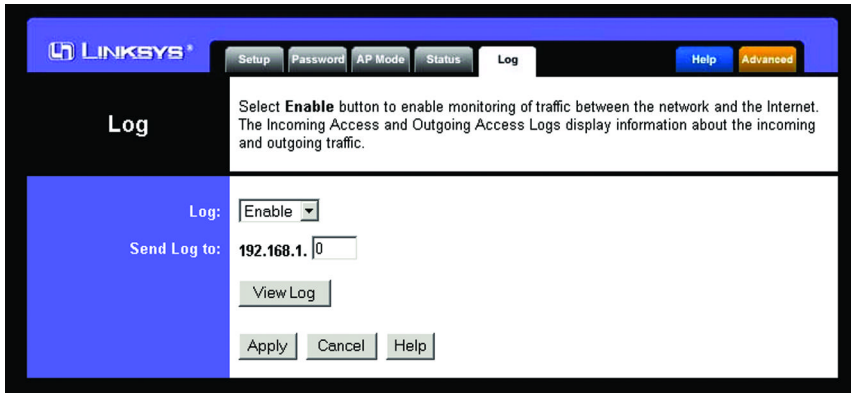

Figure 6-9

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 6-10.

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

Figure 6-10

Click the **Linksys Website** link to connect to the Linksys home page for Knowledgebase help files and information about other Linksys products, provided you have an active Internet connection.

For an **Online manual in PDF format**, click that text link. The User Guide will appear in Adobe pdf format. If you do not have the Adobe PDF Reader installed on your computer, click the **Adobe Website** link or go to the Setup Wizard CD-ROM to download this software. (To access the Adobe website, you will need an active Internet connection.) To download from the CD-ROM, click the **Start** button and select **Run**. Type **D:\Acrobat** (if "D" is the letter of your CD-ROM drive).

New firmware versions are posted at *www.linksys.com* and can be downloaded for free. If the Access Point is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use. Loading new firmware does not always enhance the speed or quality of your Internet connection.

Note: When you upgrade the Access Point's firmware, you may lose the Access Point's current configuration settings.

To upgrade the Access Point's firmware:

1. Download the firmware upgrade file from the Linksys website.
2. Extract the firmware upgrade file.
3. Click the **Upgrade Firmware** button on the *Help* screen.

Figure 6-11

4. Enter the location of the firmware upgrade file in the *File Path* field, or click the **Browse** button to find the firmware upgrade file.
5. Double-click the firmware upgrade file.
6. Click the **Upgrade** button, and follow the on-screen instructions.

Click the **Cancel** button to cancel the firmware upgrade.

The Filter Tab

To access the *Filter* tab, first click the **Advanced** tab. The *Filter* tab, shown in Figure 6-12, allows you to control which computers may or may not communicate with the Access Point—depending on their MAC addresses.

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

Next, determine if the Access Point will **Prevent** or **Permit** access to the PCs you will specify. If you want to block specific PCs from communicating with with the Access Point, click the radio button next to ***Prevent PCs listed below from accessing the wireless network.*** If you want to allow specific PCs from communicating with with the Access Point, click the radio button next to ***Permit PCs listed below from accessing the wireless network.***

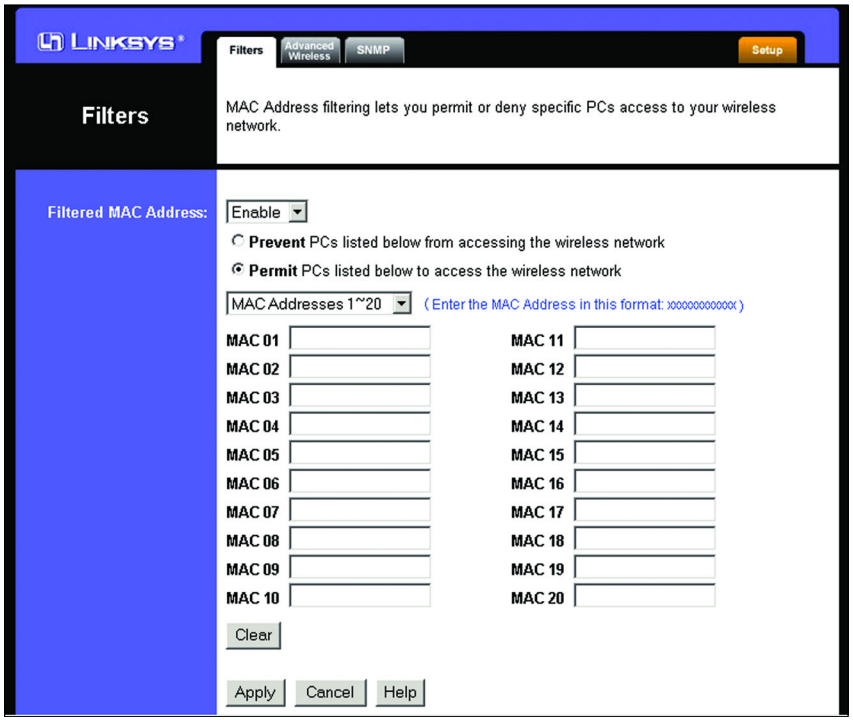

Figure 6-12

Above the *MAC Address* fields, there is a pull-down menu. This pull-down menu is for selecting the number of computers on your wireless network. For computers one through ten on your wireless network, **1~20** is selected by default. If you have more than twenty computers on your wireless network, use this pull-down menu to select **21~40**.

Then, type the MAC Address(es) you wish to filter in the *MAC Address* fields. Do not use colons when entering the digits. Use a xxxxxxxxxxxx format with the x's representing the actual characters of the MAC address. If you want to clear the MAC addresses you entered, click the **Clear** button .

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, click the **Help** button.

The Advanced Wireless Tab

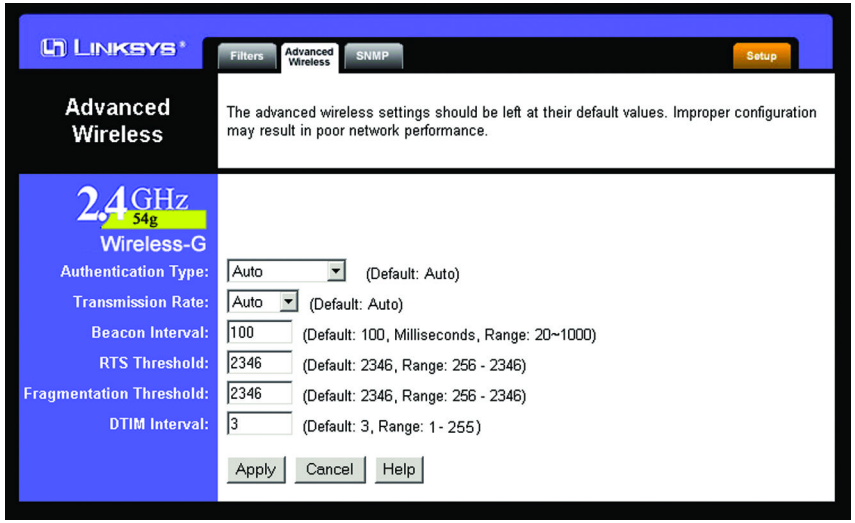

Figure 6-13

Before making any changes to the *Advanced Wireless* tab, shown in Figure 6-13, please check your wireless settings on your other systems, because these changes will alter the effectiveness of the Access Point. In most cases, these wireless settings do not need to be changed.

- **Authentication Type.** The default is set to **Auto**, where it auto-detects for **Shared Key** or **Open System.** Shared Key is when both the sender and the recipient share a WEP key for authentication. Open Key is when the sender and the recipient do not share a WEP key for authentication. All points on your network must use the same authentication type.

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

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

- **RTS Threshold.** This value should remain at its default setting of 2346. Should you encounter inconsistent data flow, only minor reductions are recommended.

- **Fragmentation Threshold.** This value specifies the maximum size for a packet before data is fragmented into multiple packets. It should remain at its default setting of 2346. A smaller setting means smaller packets, which will create more packets for each transmission. Only minor reductions of this value are recommended.

- **DTIM Interval.** The default value is 3. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the 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.

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.

The SNMP Tab

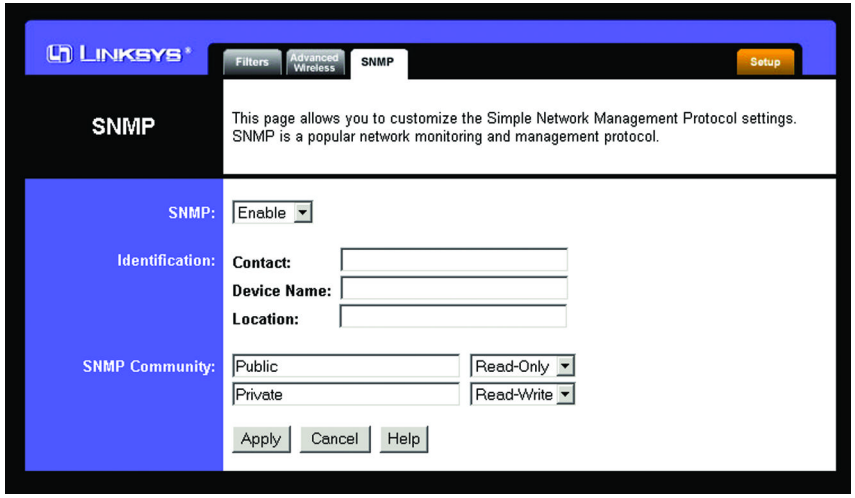

Figure 6-14

Protocol (SNMP) settings. SNMP is a popular network monitoring and management protocol.

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.** 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 802.11b 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 ESSID?
An Infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an Extended Service Set (ESS). Users within an ESS could roam freely between BSSs while maintaining a continuous connection to the wireless network stations and Access Points.

What is ISM band?
The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. 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 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 or 128) 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 802.11b or draft 802.11g, there are eleven available channels, ranging from 1 to 11.

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 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 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

802.11b - 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 wireless network or other small network in which some of the network devices are part of the network only for the duration of a communications session while in some close proximity to the rest of the network.

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.

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) - A group of wireless Network PC Card users and an 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.

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 wait 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.

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.

Driver - A workstation or server software module that provides an interface between a device and the upper-layer protocol software running in the computer; it is designed for a specific device, 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 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.

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.

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 - More than one BSS in a 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 the center frequency of a conventional carrier several times per second according to a pseudo-random set of channels, while chirp spread spectrum changes the carrier frequency. Because a fixed frequency is not used, illegal monitoring of spread spectrum signals is extremely difficult, if not downright impossible depending on the particular method.

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.

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.

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.

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 - An infrastructure network is a wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point which connects them to the rest of the network.

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.

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 - 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).
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.

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 - OFDM (Orthogonal Frequency Division Muliplexing) 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.

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.

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

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 - The ability to use a wireless device and be able to move from one access point's range to another without losing the connection.

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.

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 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 Internet Protocol (Internet Protocol) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual

units of data (called packet) that a message is divided into for efficient routing through the Internet.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/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.

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.

WEP (**W**ired **E**quivalent **P**rivacy) - A data privacy mechanism based on a 64-bit, 128-bit, or 256-bit shared key algorithm, as described in the IEEE 802.11 standard.

Appendix D: Specifications

Standards	Draft 802.11g, 802.11b
Channels	11 Channels (USA) 13 Channels (Europe) 14 Channels (Japan)
Port	One 10/100, Auto-Crossover (MDI/MDI-X) Port
Cabling Type	Category 5 or better
Data Rate	Up to 54Mbps (Wireless), 10/100Mbps (Ethernet)
LEDs	Power, Diag
LAN	Link/Act, Full/Col, 100
WLAN	Act, Link
Transmit Power	18 dBm
Receive Sensitivity (typical)	11Mbps: -80 dBm 54Mbps: -65 dBm
Modulation	CCK, DQPSK, DBPSK, OFDM
Network Protocols	TCP/IP, IPX, NetBEUI

Environmental

Dimensions	7.32" x 6.89" x 1.89" (186 mm x 175 mm x 48 mm)
Unit Weight	18.25 oz. (0.51 kg)
Certifications	FCC Class B
Operating Temp.	32ºF to 104ºF (0ºC to 40ºC)
Storage Temp.	-4ºF to 158ºF (-20ºC to 70ºC)
Operating Humidity	10% to 80%, 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

http://www.linksys.com