Instant Wireless™ Series

Wireless Network Access Point

Use this guide to install: WAP11

User Guide

LINKSYS®

COPYRIGHT & TRADEMARKS
Copyright © 2001 Linksys, All Rights Reserved. Instant Wireless™ is a registered trademark of Linksys. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. All other trademarks and brand names are the property of their respective proprietors.

LIMITED WARRANTY
Linksys guarantees that every Wireless Network Access Point is free from physical defects in material and workmanship under normal use for one year from the date of purchase. If the product proves defective during this warranty period, call Linksys Customer Support in order to obtain a Return Authorization Number. 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. When returning a product, mark the Return Authorization Number clearly on the outside of the package and include your original proof of purchase. All customers located outside of the United States of America and Canada shall be held responsible for shipping and handling charges.

IN NO EVENT SHALL LINKSYS' 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 makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Linksys reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to:

Linksys P.O. Box 18558, Irvine, CA 92623.

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

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

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

UG-WAP11-011005E JL

Table of Contents

Introduction **1**
The Instant Wireless™ Wireless Network Access Point 1
Features 1
Package Contents 2
System Requirements 2

Planning Your Wireless Network **3**
Network Topology 3
Roaming 3

Getting to Know the Wireless Network Access Point **4**
The Wireless Access Point's Rear Panel 4
The Wireless Access Point's Front Panel 6

Connecting and Setting Up the Wireless Network Access Point **7**

Installing the USB Drivers for the Wireless Network Access Point **8**
Installing the Driver Software for Windows 98 8
Installing the Driver Software for Windows Millennium 10
Installing the Driver Software for Windows 2000 11

Configuring the Wireless Network Access Point **14**
Installing the Configuration Utility 14

The USB Configuration Utility **18**
Configuring the Wireless Network Access Point with the USB Configuration Utility 18

The Access Point's SNMP Configuration Utility **31**
Creating a Temporary IP Address 31
Configuring the Wireless Network Access Point with the Access Point's SNMP Configuration Utility 32

Troubleshooting **47**
Common Problems and Solutions 47
Frequently Asked Questions 47

Glossary **51**

Specifications **56**
Environmental 57

Warranty Information **58**

Contact Information **59**

Introduction

The Instant Wireless™ Wireless Network Access Point

Don't be bound by cabling restrictions any longer! The Instant Wireless™ Network Access Point from Linksys delivers the freedom to configure your network ***your*** way. Utilization of state-of-the-art wireless technology gives you the ability to set up workstations in ways you never though possible; no cables to install means fewer expenses and fewer hassles.

The Instant Wireless™ Network Access Point's high-powered antennae offer a range of operation of up to 457 meters, providing seamless roaming throughout your LAN infrastructure. Advanced user authentication ensures a high level of security for wireless networking, while easy-to-use Windows-based diagnostics and statistic tools ensure that you'll always be in control. Best of all, the Instant Wireless Network Access Point features easy installation—just plug it in and you're ready to go!

When all these features come together in one compact, lightweight, and power-efficient unit, you have the ultimate in flexible networking—the Linksys Instant Wireless™ Network Access Point.

Features

- Highly Efficient Dipole Antennae Provide Extensive Range of Operation
- Enjoy Your Wireless Office Beyond the Range of Ethernet Networking
- Auto Fall-Back Data Rate for Long-Distance Communication and Noisy Environments
- High-Speed Data Transfer Rate Up to 11 Mbps
- Interoperable with IEEE 802.11b (DSSS) 2.4GHz-Compliant Equipment
- Features Roaming, Best Access Point Selection, Load Balancing, and Network Traffic Filtering
- Extensive Operating Range Supports 150m (Indoors) and 500m (Outdoors)
- 64-Bit Wired Equivalent Privacy
- Free Software Driver Upgrades
- Compatible with Virtually All Major Operating Systems
- Free Technical Support—24 Hours a Day, 7 Days a Week for North America Only
- 1-Year Limited Warranty

Package Contents

- One Instant Wireless™ Network Access Point
- One AC Power Adapter
- One Setup CD-ROM
- One User Guide
- One Quick Installation and Registration Card (not shown)
- Two Detachable Antennae
- One USB Cable

System Requirements

- A PC with USB Support or Ethernet Connection
- Windows 95, 98, Millennium, NT version 4.0, or 2000 Professional
- 500 kbytes of free disk space for utility and driver installation
- A 10 Mbps Category 3 or Better network RJ-45 connection

Linux/Unix Users: *Though these operating systems are not supported by Linksys, the Wireless Access Point should work in these environments. The WAP11 can be configured under these operating systems using SNMP. A configurable Management Information Base file (MIB) named* AT76C510.MIB *can be found on the Setup Utility CD.* ***This file is for Linux/Unix users only, and is not necessary for any Windows installation.***

Planning Your Wireless Network

Network Topology

A wireless LAN is a group of computers, each equipped with one Instant Wireless™ Series Adapter. Computers in a wireless LAN must be configured to share the same radio channel.

The Instant Wireless™ Series Adapter provides access to a wired LAN for wireless workstations. An integrated wireless and wired LAN is called an Infrastructure configuration. A group of Instant Wireless™ Series Adapter users and an Instant Wireless™ Network Access Point compose a Basic Service Set (BSS). Each Instant Wireless™ Series Adapter PC in a BSS can talk to any computer in a wired LAN infrastructure via the Instant Wireless™ Network Access Point.

An infrastructure configuration extends the accessibility of an Instant Wireless™ Series Adapter PC to a wired LAN, and doubles the effective wireless transmission range for two Instant Wireless™ Series Adapter PCs. Since the Wireless Network Access Point is able to forward data within its BSS, the effective transmission range in an infrastructure LAN is doubled.

The use of a unique ID in a BSS is essential. All Instant Wireless™ Series Adapter PCs configured without roaming options in an independent BSS must be configured with a BSS ID used in the BSS.

The wireless LAN Infrastructure configuration is appropriate for enterprise-scale wireless access to a central database, or as a wireless application for mobile users.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. More than one BSS can be configured as an Extended Service Set (ESS). This continuous network allows users to roam freely within an ESS. All Instant Wireless™ Series Adapter PCs within one ESS must be configured with the same ESS ID and use the same radio channel.

Before enabling an ESS with roaming capability, choosing a feasible radio channel and optimum Wireless Network Access Point position is recommended. Proper Wireless Network Access Point positioning combined with a clear radio signal will greatly enhance performance.

Getting to Know the Wireless Network Access Point

The Wireless Access Point's Rear Panel

Your Access Point's ports, where network cables are connected, are located on the rear panel of your Access Point.

The Wireless Network Access Point's Ports

Dipole Antenna Connectors — These two round connections are where the antennae are connected to the Access Point.

LAN — This **LAN** (Local Area Network) port connects to Ethernet network devices, such as a hub, switch, or router.

Power — The **Power** port is where you will connect the power adapter. Be sure to connect the power cord to the power adapter before plugging it in.

Configuration Port — The **Configuration Port** is a USB port (Type B-slave) which connects to a USB-ready PC in order to configure the Access Point's settings. To work with USB ports, your PC must be running Windows 98, 2000, or Millennium.

Note: The **Configuration Port** *does not* connect your Access Point to your PC (or any other device) for networking purposes. Its only function is to allow you to configure your Access Point's settings. Once the Access Point is configured, you may remove the USB cable connecting the Access Point to your PC.

Your Access Point comes with a USB cable that has two different types of connectors. Type A, the master connector, is shaped like a rectangle and plugs into your PC's USB port. Type B, the slave connector, resembles a square and connects to the USB port on the rear panel of your Wireless Network Access Point.

USB Compatibility with Your PC

To use the USB port on the Wireless Network Access Point, you must have Windows 98, 2000, or Millennium installed on your PC. USB is not supported in a Windows 95 or NT environment.

Also, your PC must have a USB port installed and enabled. Some PCs may have a disabled USB port. If your port doesn't seem to be working, there may be jumpers on the motherboard or a menu option in the BIOS to enable a PC's USB port.

Other motherboards have USB interfaces, but no ports. You can install your own USB port and attach it to your PC's motherboard using hardware purchased at retail computer stores. See your PC's User Guide for instructions.

USB Type A

USB Type B

There is no USB Support on PCs running Windows 95 or Windows NT.

The Wireless Access Point's Front Panel

The LAN Indicators

Power *Red*. The **Power** LED lights up when the Access Point is powered on.

ACT *Green*. The **ACT** LED is lit to show that other wireless devices are accessing the Access Point. If the LED is flickering, the Access Point is actively sending or receiving data to or from one of the wireless devices on the network.

LINK *Amber*. The **LINK** LED serves two purposes. If the LED is continuously lit up, the Access Point is successfully connected to a device through the LAN port. If the LED is flickering, it is an indication of any network activity.

Connecting and Setting Up the Wireless Network Access Point

1. **Locate an optimum location for the Wireless Network Access Point.** The best place for your Wireless Network Access Point is usually at the center of your wireless network, with line of sight to all of your mobile stations.

2. **Fix the direction of the antenna.** Try to place it in a position which can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.

3. **Connect a standard UTP cable to the Wireless Network Access Point.** Then, connect the other end of the Ethernet cable to a switch or hub. The Wireless Network Access Point will then be connected to your 10/100 Network.

4. **Connect the AC Power Adapter to the Wireless Network Access Point's Power Socket.** Only use the power adapter supplied with the Wireless Network Access Point. Use of a different adapter may result in product damage.

5. **Connect the appropriate end of the USB Cable to the Wireless Network Access Point's Configuration Port.** Connect the other end to the USB port on your PC. If your USB port is working properly, your system should immediately recognize the Access Point and attempt to install drivers for it. Continue to the next section for instructions on how to install the drivers.

Now that the hardware installation is complete, proceed to **Installing the USB Drivers for the Wireless Network Access Point** and **The USB Configuration Utility** for configuring the Access Point through your PC's USB port. To configure the Access Point through an Ethernet or Wireless connection, proceed to **The Access Point's SNMP Configuration Utility**.

The Hardware Installation is complete.

Note: Once your Access Point is installed and configured, the USB cable may be removed.

Installing the USB Drivers for the Wireless Network Access Point

Installing the Driver Software for Windows 98

1. Windows 98 will automatically identify the Wireless Network Access Point, once it is connected to the PC via the USB cable, and prompt you to install the necessary driver. Make sure that the **Setup Utility CD** is inserted into your CD-ROM drive and click the **Next** button on the **Add New Hardware Wizard** screen to proceed. *(When you insert the Setup Utility CD, the installation may try to run automatically. If it does, exit out of the program and return here.)*

2. Select **Search for the best driver...** and click the **Next** button. This will search for the Windows 98 driver.

3. Windows will now ask you where to search for the driver software. Select **Specify a location** and type in the blank field **D:\WAP11\WIN9X** (where "D" specifies your CD-ROM). Then, click the **Next** button.

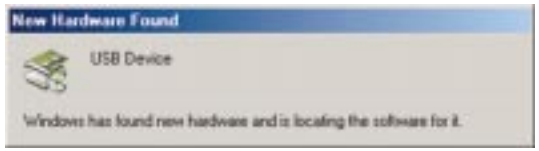
4. Windows will now search for the driver. After Windows has acknowledged finding the driver, click the **Next** button.

5. Windows will now install the driver files. Click the **Finish** button when completed.

6. Continue to the **Configuring the Wireless Network Access Point** section for software installation.

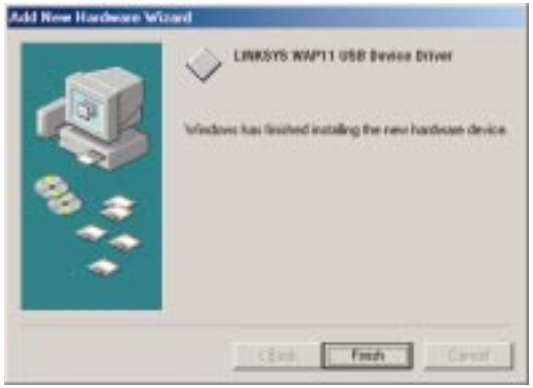
Installing the Driver Software for Windows Millennium

1. Windows Millennium will automatically identify the Wireless Network Access Point, once it is connected to the PC via the USB cable, and prompt you to install the necessary driver.



2. Select **Automatic Search for a better driver (Recommended)** and click the **Next** button. This will search for the Windows Millennium driver.

3. Windows will now install the driver files. Click the **Finish** button when completed. Windows may ask for the driver, which is located at "D:\WAP11\usbdrv" (where "D" specifies your CD-ROM drive). Click **OK**.



4. Continue to the **Configuring the Wireless Network Access Point** section for software installation now.

Installing the Driver Software for Windows 2000

1. Windows 2000 will automatically identify the Wireless Network Access Point, once it is connected to the PC via the USB cable, and prompt you to install the necessary driver. Make sure that the **Setup Utility CD** is inserted into your CD-ROM drive and click the **Next** button on the **Found New Hardware Wizard** screen to proceed.

2. Select **Search for a suitable driver...** and click the **Next** button. This will search for the Windows 2000 driver.

3. Under "Optional Search Locations," select **Specify a location** and click the **Next** button.

4. You will be prompted to enter a path; type "**D:\WAP11\usbdrv**" (where D: is the letter of your CD-ROM drive) and click **OK**. Windows will now search for the driver. After Windows has acknowledged finding the driver, click the **Next** button.

5. Windows will now install the driver files. Click the **Finish** button when completed.

6. Continue to the **Configuring the Wireless Network Access Point** section for software installation.

Configuring the Wireless Network Access Point

The Wireless Network Access Point can be configured one of two ways, through the USB Utility or the Access Point SNMP Configuration Utility.

USB Utility

The USB Utility can be used when configuring the Wireless Network Access Point through a USB connection and is compatible with Windows 98, Millennium, and 2000.

Access Point SNMP Configuration Utility

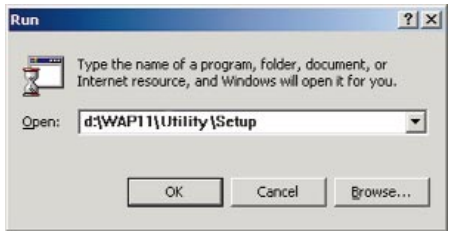
The Access Point SNMP Configuration Utility can be used when configuring the Wireless Network Access Point through an Ethernet connection and is compatible with all Windows Operating Systems. You may also configure the Access Point through its wireless connections.

Note: In order for all other wireless devices to communicate with the Wireless Network Access Point, those devices must be operating in the **Infrastructure Mode**. If any wireless devices are configured in the **Ad Hoc Mode**, they *will not* be recognized by the Access Point.

Linux/Unix Users: *Since the Configuration Utility is written for Windows users, you will have to configure the Wireless Access Point using SNMP. A configurable MIB file* (AT76C510.MIB) *can be found on the Setup Utility CD. Remember, Linksys does not support Linux or Unix as an operating system.* ***This file is for Linux/Unix users only, and is not necessary for any Windows installation.***

Installing the Configuration Utility

Insert the **Setup Utility CD** into your CD-ROM Drive. The Setup Utility should run automatically and the screen shown on the top of the next page should appear. If it does not, click the **Start** button and choose **Run**. In the box that appears, enter **D:\setup.exe** (where "D" is the letter of your CD-ROM drive).



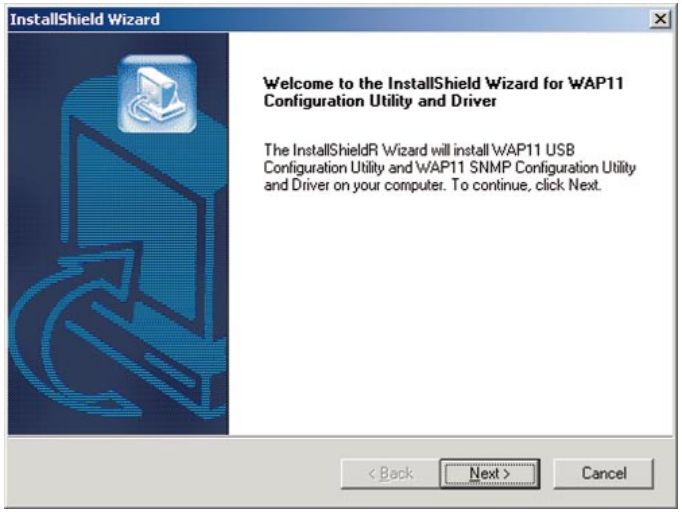
1. The following screen should appear.

Click on the **WAP11** product button in the column on the left to select it.

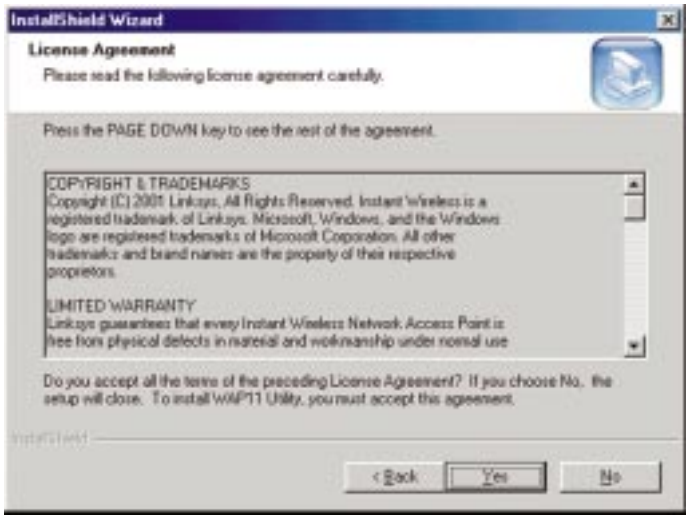
2. When this screen appears, click on the **Install** tab to start the setup.

Note: This useful menu screen can be accessed at any time, simply by inserting the Setup Utility CD into your CD-ROM drive. From this menu, software can be uninstalled, and you may view online documentation and contact information. Your AP will still work after uninstalling the Utility.

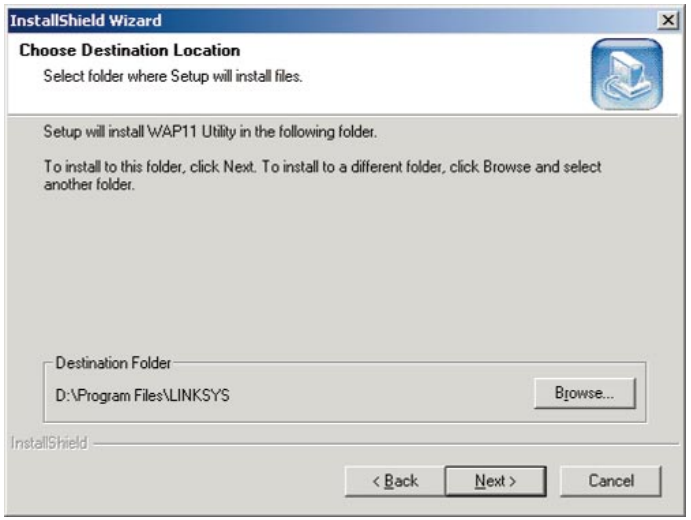
3. When the Welcome screen appears, click **Next** to continue.



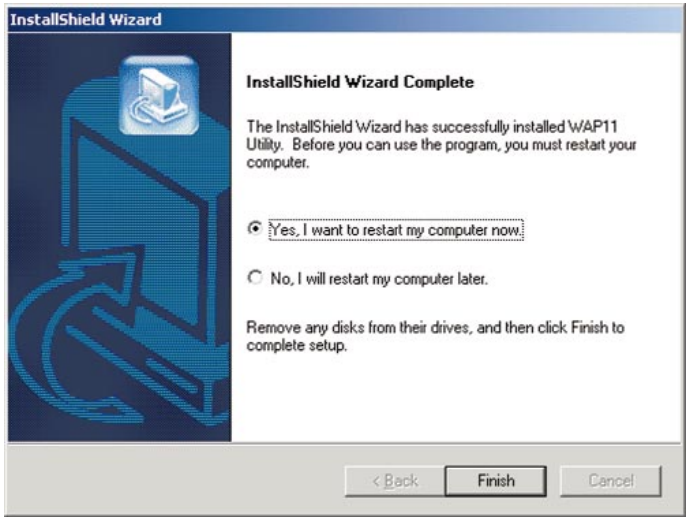
4. Read the terms of the License Agreement, and if you agree, click **Yes**; otherwise, click **No** to cancel the configuration process.



5. The **Choose Destination Location** screen will show you the default destination chosen by the utility. It is recommended that you leave the default destination, but if you want to install this in another location, click the **Browse** button and select an alternate destination. When you are ready to continue, click the **Next** button.



6. The Configuration Utility has now been installed. Select **Yes** to restart your PC and then click **Finish**.



The USB Configuration Utility

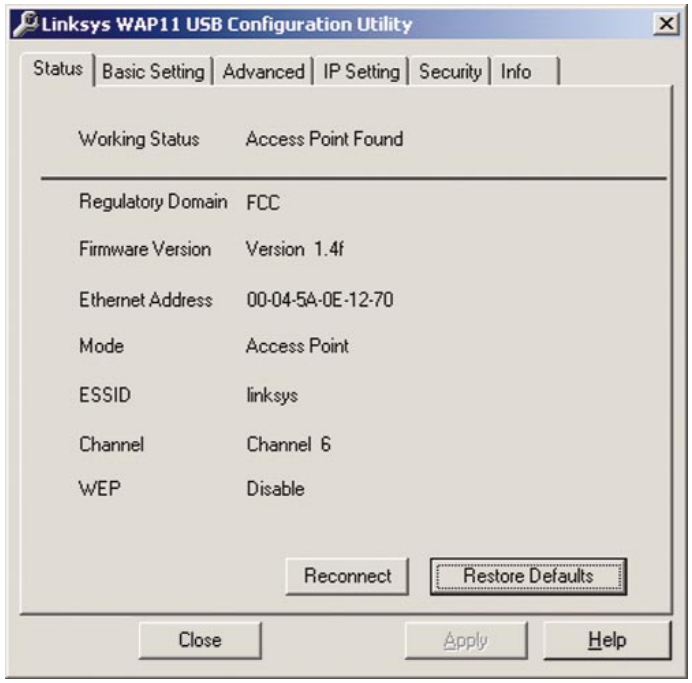
The **USB Configuration Utility** is provided to allow you further customization of the Wireless Network Access Point and your wireless network through your USB port.

Configuring the Wireless Network Access Point with the USB Configuration Utility

THE STATUS TAB

The Status tab displays the Wireless Network Access Point's current status. From this tab, you can view the status information along with reconnecting to the Wireless Network Access Point and restoring its default settings.

- **Working Status.** This displays your current connection status, notifying you of any problems with the connection.
- **Regulatory Domain.** This status shows the regulatory domain preset by the manufacturer for the country the product was purchased in.
- **Firmware Version.** This displays the present version of the Access Point's firmware and is limited to a maximum of four characters.
- **MAC Address.** This displays the MAC Address of your current WAP11.
- **Mode.** This displays the mode your WAP11 is currently configured for: Access Point, Access Point Client, or Wireless Bridge.
- **ESSID.** The unique name shared among all points in your wireless network is displayed here.
- **Channel.** The wireless channel shared by all of the points in your wireless network is displayed here.



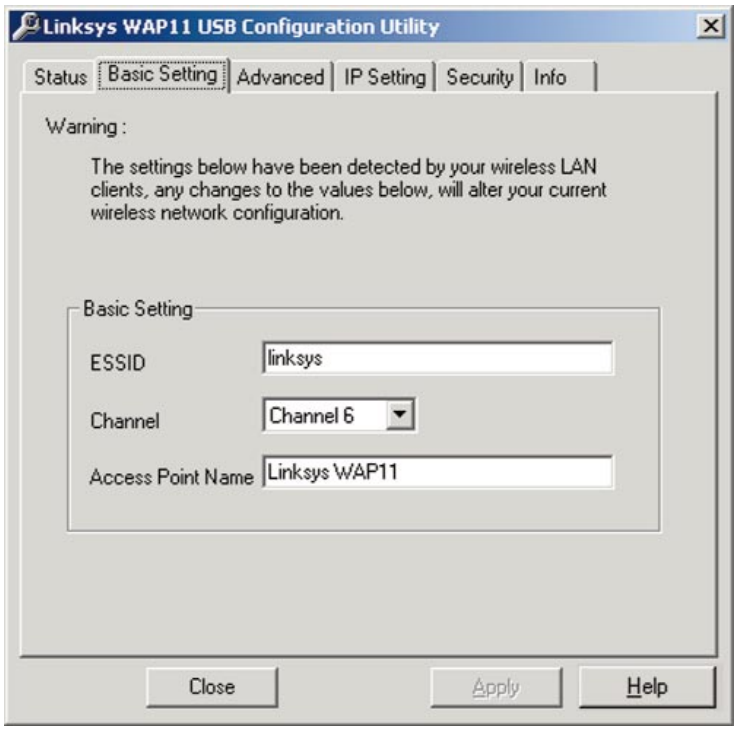
- **WEP.** If you have not enabled WEP encryption, this will read Disabled. When you are using WEP encryption, it will read Enabled and list the level of encryption in use.
- **Reconnect.** If the USB connection to the Access Point is disconnected, you can reconnect the USB cable and click the **Reconnect** button. This will retrieve the most recently saved configuration from the Access Point so you will be ready to use the USB Configuration Utility again.
- **Restore Defaults.** Click this button to restore the Access Point's default settings. If this button is clicked, any setting you may have made through the USB Utility will be lost.

Click the **Apply** button to store the information. A new dialog box will appear. Click the **Yes** button to accept the changes.

If you have not already clicked the **Apply** button, the **Close** button will close the USB Utility without saving any changes.

Click the **Help** button for assistance.

THE BASIC SETTING TAB



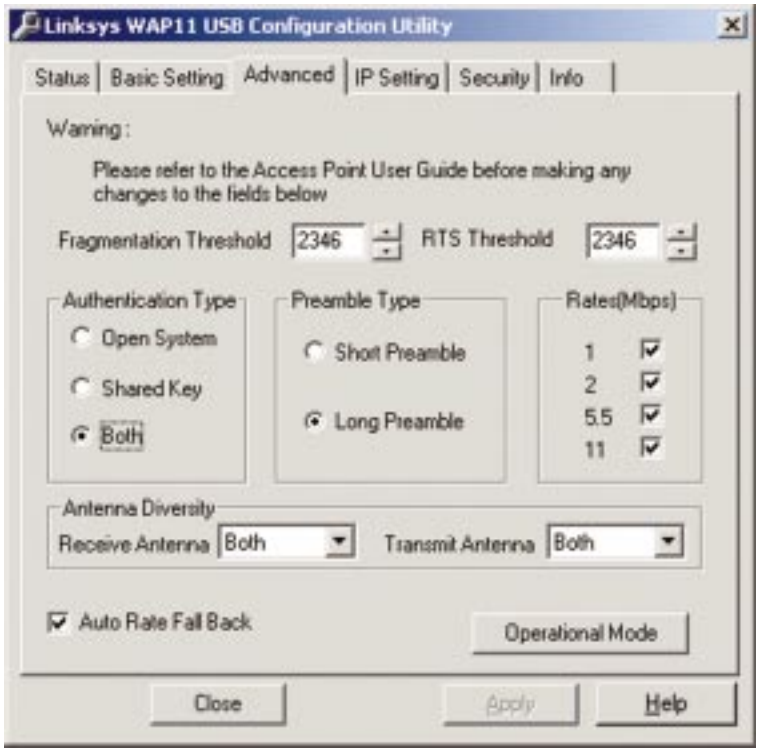
The Access Point automatically detects the settings to your wireless network. Changing these values will alter your current wireless network configuration.

- **ESSID.** The ESSID or SSID is the unique name shared among all points in a wireless network. The ESSID must be identical for all points in the wireless network. It is case sensitive and must not exceed 30 characters, which may be any keyboard character. Make sure this setting for all points in the wireless network are the same. Verify that you're using the correct ESSID and click the **Apply** button to set it.

- **Channel.** Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All points in your wireless network must use the same channel in order to function correctly. Verify that the correct channel is selected and click the **Apply** button to set it. A new dialog box will appear. Click the **Yes** button to accept the changes.

- **Access Point Name.** You may assign any name to your Access Point. Unique, memorable names are helpful, especially if you are employing multiple Access Points on the same network.

THE ADVANCED TAB



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

- **Fragmentation Threshold.** This value indicates how much of the Access Point's resources are devoted to recovering packet errors. The value should remain at its default setting of 2,346. 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.

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

- **Authentication Type.** You may choose between **Open System**, **Shared Key**, and **Both**. The Authentication Type default is set to **Open System**, in which the sender and the recipient do NOT share a secret key. Each party generates its own key-pair and asks the receiver to accept the randomly-generated key. Once accepted, this key is used for a short time only. Then a new key is generated and agreed upon. **Shared Key** is when both the sender and the recipient share a secret key.

- **Preamble Type.** The preamble defines the length of the CRC block for communication between the Access Point and the roaming Network Card. (High network traffic areas should use the shorter preamble type.) Select the appropriate preamble type and click the **Apply** button to set it.

- **Basic Rates.** The basic transfer rates should be set depending on the speed of your wireless network. Set the correct basic rate for your wireless network and click the **Apply** button to set it.

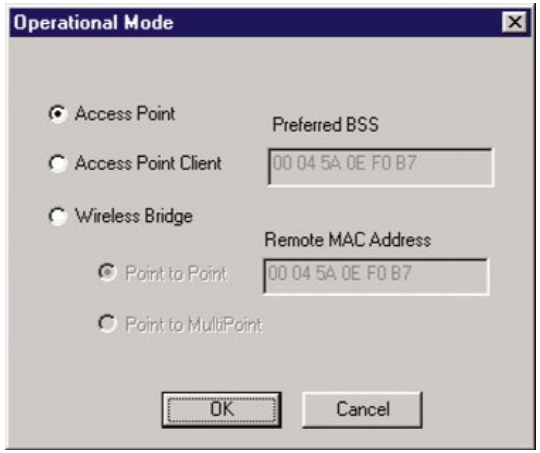
- **Antenna Diversity.** These two settings determine whether either or both antennae will be used to transmit or receive. The default setting, **Both**, means that the antennae are set to both **Transmit** and **Receive**; this is the recommended setting. The WAP11 will auto-detect which antenna to use based on signal strength.

- **Auto Rate Fall Back** setting should be checked to make your wireless network flexible for roaming wireless devices. As wireless devices move away from the Wireless Network Access Point, the transfer rate will automatically fall back to the most optimum rate allowed.

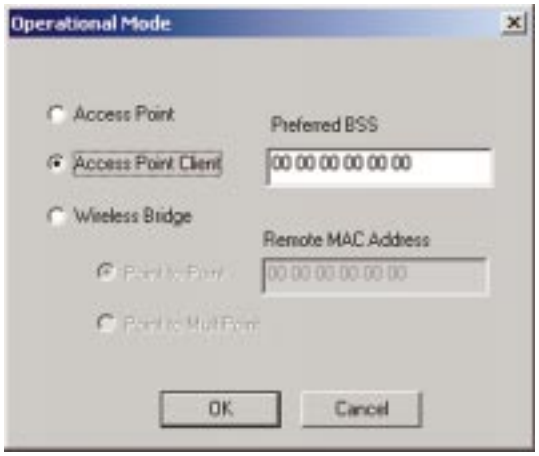
THE MODE TAB

The WAP11 offers three modes of operation: Access Point, Access Point Client, and Wireless Bridge.

- **Access Point -** The **Operational Mode** is set to **Access Point** by default. This connects your wireless PCs to a wired network. In most cases, no change is necessary.



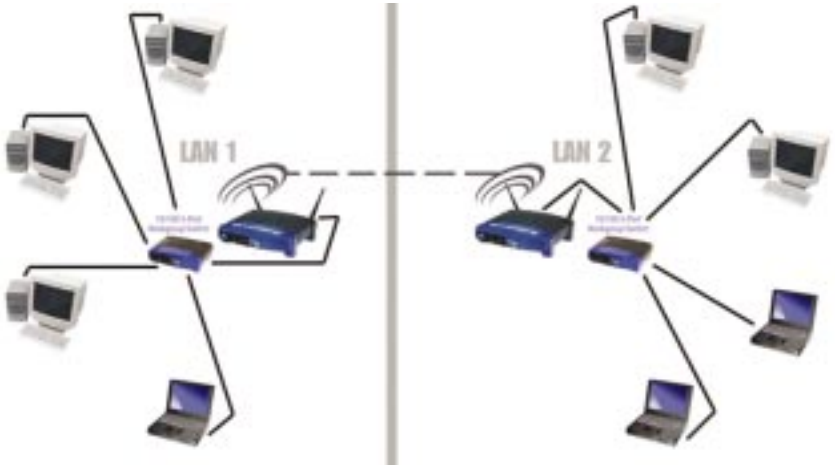
- **Access Point Client -** A WAP11 set to Access Point Client mode is able to talk to one main WAP11 and wireless clients within its range. This mode allows your WAP11 to act as a client of a main WAP11. A LAN attached to your WAP11 client can then be wirelessly bridged to the main WAP11. Enter the required MAC address of the main WAP11.



- **Wireless Bridge -** If you are trying to make a wireless connection between two or more wired networks, select **Wireless Bridge**. There are two options: Point to Point and Point to MultiPoint.

Point to Point

This mode connects two physically separated LAN segments by using two WAP11 units.



To configure a Point to Point bridged environment:

1. Click **Point to Point**.

2. Set the MAC Address of the Access Point in LAN 1 to look for the MAC Address of the Access Point in LAN 2.

3. Set the MAC address of the Access Point in LAN 2 to look for the MAC Address of the Access Point in LAN 1.

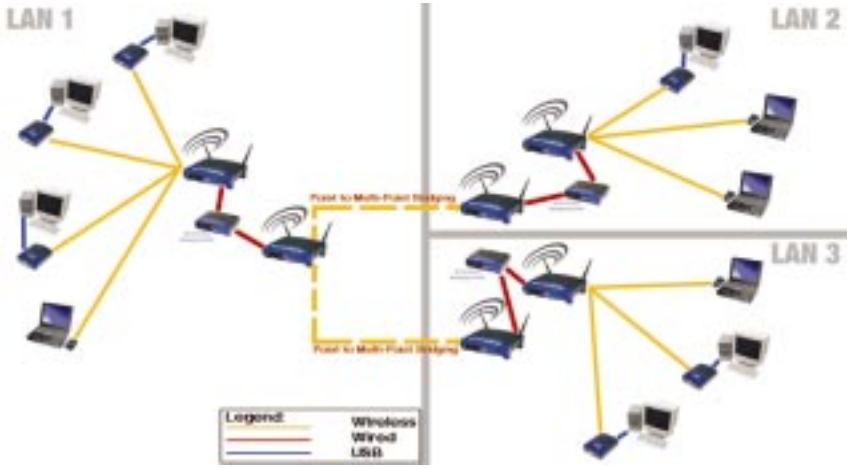
4. On the Operational Mode tab, enter the **Remote MAC Address** of the remote Access Point. The remote Access Point also needs to be set up as a Wireless Bridge.

Note: All devices on each LAN must be connected through a hub or switch.

Note: In Wireless Bridge mode, the WAP11 can **ONLY** be accessed by another wireless bridge. In order for your other wireless devices to access the WAP11, you must reset it to Access Point mode. The two modes are mutually exclusive.

Point to MultiPoint

This mode allows you to construct a network that has multiple WAP11 units bridging wirelessly.



To configure a Point to MultiPoint bridged environment:

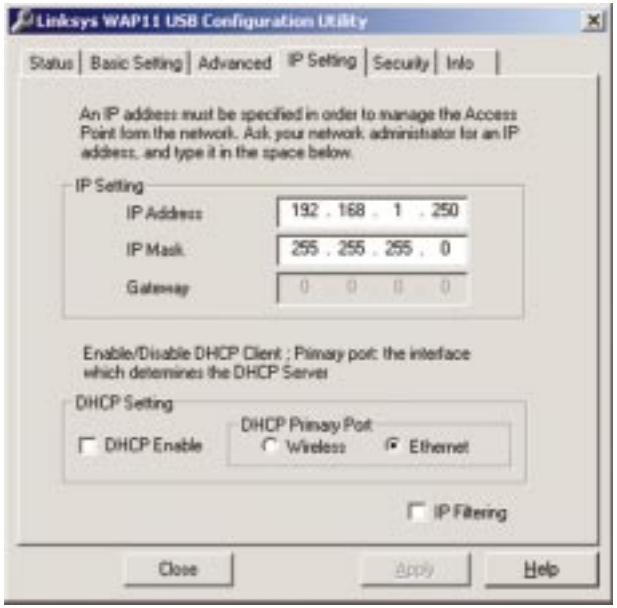
1. Click **Point to MultiPoint** for the WAP11 used in LAN 1. No MAC Address binding is needed.

2. Set the Access Points in LAN 2 and LAN 3 to Point to Point, and have them look for the MAC Address of the Access Point in LAN 1.

Only one of the Access Points must be in Point to MultiPoint mode. For all other bridged Access Points, select the **Point to Point** option, and enter the **Remote MAC Address** of the Access Point set to Point to MultiPoint.

Click the **Apply** button to store the information. A new dialog box will appear. Click the **Yes** button to accept the changes.

THE IP SETTING TAB



The IP settings for the Wireless Network Access Point are made from this tab.

- **IP Address.** This IP address must be unique to your network. We suggest you use the default IP address of 192.168.1.250. As this is a private IP address, there is no need to purchase a separate IP address from your service provider. Verify the address and click the **Apply** button to save changes.

- **IP Mask.** Your Access Point's Subnet Mask must be the same as your Ethernet network. Verify this is correct and click the **Apply** button to set it.

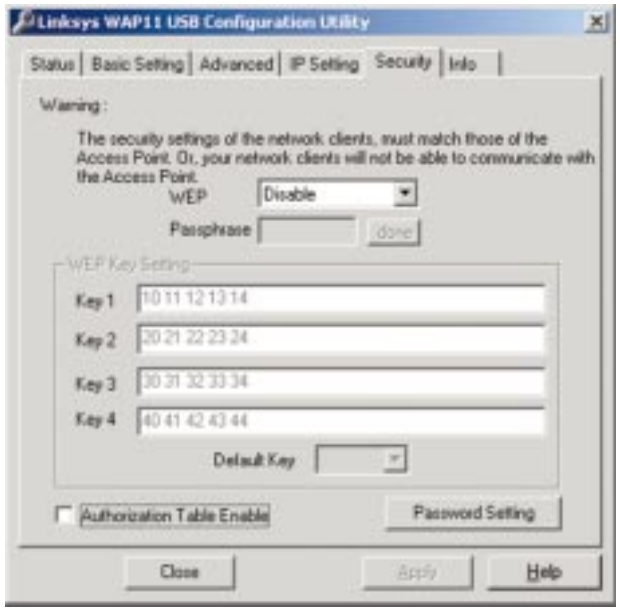
- **DHCP Setting.** Check the box next to **DHCP Enable** to allow it to obtain a dynamic IP address from a DHCP server. You may also choose how the WAP11 dynamically obtains an IP address—either **Wireless** or **Ethernet**.

- **IP Filtering.** For security, click the check box to enable IP filtering, which allows IP packets only through the Access Point.

- **Gateway.** This setting only appears when the DHCP client is enabled; it indicates the status of the gateway and is not user-adjustable.

Note: Configuring the IP address here allows you to use the SNMP Configuration Utility software. It is not necessary to make any changes to the IP address if you are not planning on using the SNMP Configuration Utility.

THE SECURITY TAB



WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802.11b standard. In order to utilize WEP encryption, all points in your wireless network must have WEP enabled and be set to the same Key Setting. For easier configuration, it is strongly recommended that you use the Passphrase feature.

- **WEP (Disable/64-bit WEP/128-bit WEP).** In order to utilize WEP encryption, select the WEP setting from the pull-down menu. If you do not wish do utilize WEP encryption, make sure **Disable** is selected. This specific WEP encryption is unique to Linksys and may conflict with other vendors' WEP encryption.

- **Passphrase.** This is the code used when a point on the wireless network wishes to log on to the network. It is a text string with a maximum of 32 alphanumeric characters. The WEP Key Settings are based upon the Passphrase determined by you. Type that here. This passphrase may not work with non-Linksys products due to possible incompatibility with other vendors' passphrase generators.

Note: For security, it is recommended that you make up your own passphrase (i.e. "Home"). You must use the same passphrase or WEP key settings for all wireless computers in order for the wireless network to function properly.

- **WEP Key Setting.** This setting is the configuration key used in accessing the wireless network via WEP encryption. To generate an encryption key:

1. Type exactly the same case sensitive Passphrase in the PassPhrase field. For security purposes, please create your own Passphrase.

2. Click the **Done** button to create the encryption keys. The Passphrase generates four unique keys.

3. Make sure that the Default Key is the same for each point on the wireless network.

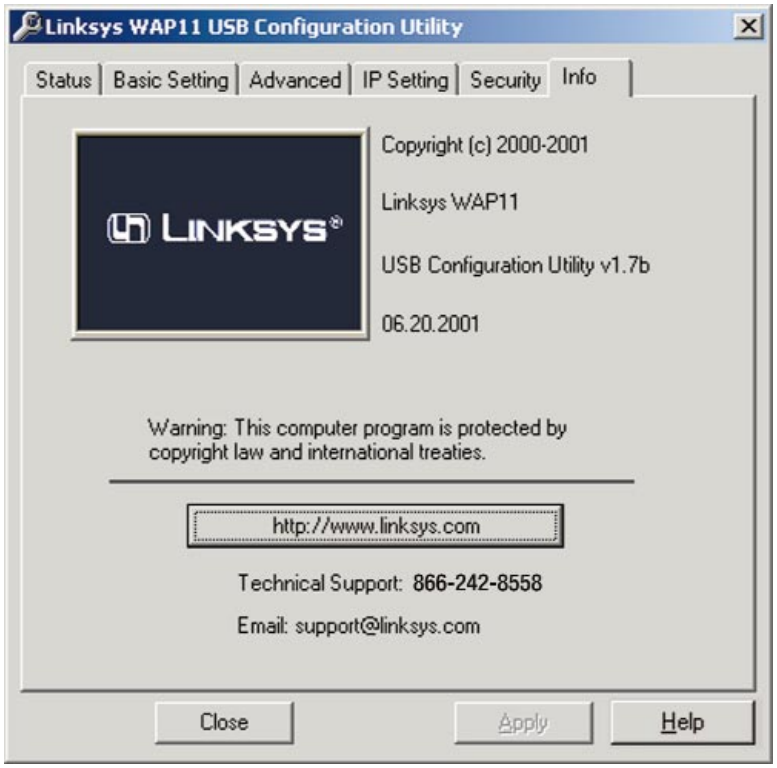
4. Click the **Apply** button to store the information.

5. Click the **Yes** button to accept the changes in the dialog box that appears.

- **Password Setting.** This option allows you to choose **Read/Write** and/or **Read Only**. It is recommended that you change both to maximize security. For both options, type in a password and confirm it.

- **Authorization Table Enable.** This setting can be enabled here, but any setting changes must be made through the SNMP Utility. It is recommended that this setting be enabled using the SNMP Utility.

THE INFO TAB



The Info tab displays general information about Linksys and the USB Utility. The USB Utility's copyright date and version number are listed as well as the Utility's firmware version. At the bottom of the screen, you will find a button that will access Linksys' web page (once your Internet connection is properly set up), the email address for technical support, and the phone number to call for technical support.

Note: Once your Access Point is installed and configured, the USB cable may be removed.

The Access Point's SNMP Configuration Utility

The **Access Point SNMP Configuration Utility** is provided to allow you further customization of the Wireless Network Access Point and your wireless network through your Ethernet or wireless connection. It is strongly recommended that you use your wireless connection to use the SNMP Configuration Utility.

Linux/Unix Users: *Though these operating systems are not supported by Linksys, the Wireless Access Point should work in these environments. The WAP11 can be configured under these operating systems using SNMP. A configurable Management Information Base file (MIB) named* AT76C510.MIB *can be found on the Setup Utility CD.* ***This file is for Linux/Unix users only, and is not necessary for any Windows installation.***

Creating a Temporary IP Address

If you wish to use the SNMP Configuration Utility to configure the Access Point, you must assign a temporary IP address to your computer.

You may need to assign the PC a temporary IP address to gain access to the Access Point.

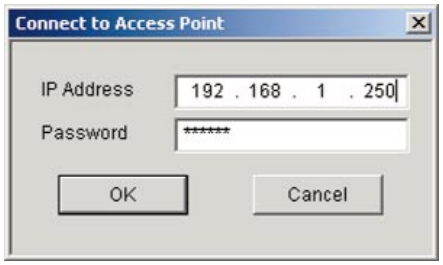
1. This can be done at **Start**, **Settings**, **Control Panel**, then **Network**.
2. Click the network adapter associated with the TCP/IP and click **Properties**.
3. Note your current settings in order to restore your TCP/IP configuration.
4. Select **Specify an IP address** and enter the following values:
   IP - 192.168.1.50, Subnet Mask- 255.255.255.0
5. Click **OK** and click **OK** again in the Network window.
6. Restart the computer when asked.

Make sure that you enter an IP address for the Access Point in order to access it at a later time. Once you have completed the IP Address Configuration, you can set the PC back to its previous settings. For example, to "Obtain an IP Address automatically."

To restore your TCP/IP configuration, follow the steps below:
1. Follow steps 1 and 2 in the instructions above.
2. Select either **Specify an IP address** or **Obtain IP address automatically** and enter the original values you noted earlier.
3. Click **OK** and click **OK** again in the Network window.
4. Restart your computer.

Configuring the Wireless Network Access Point with the Access Point's SNMP Configuration Utility

If you wish to run the SNMP Configuration Utility, click **Start**, **Programs**, **WAP11 Configuration Utility**, and **WAP11 SNMP**.



When you first start the Access Point SNMP Configuration Utility, a screen will appear asking you to enter the Wireless Network Access Point's IP Address.

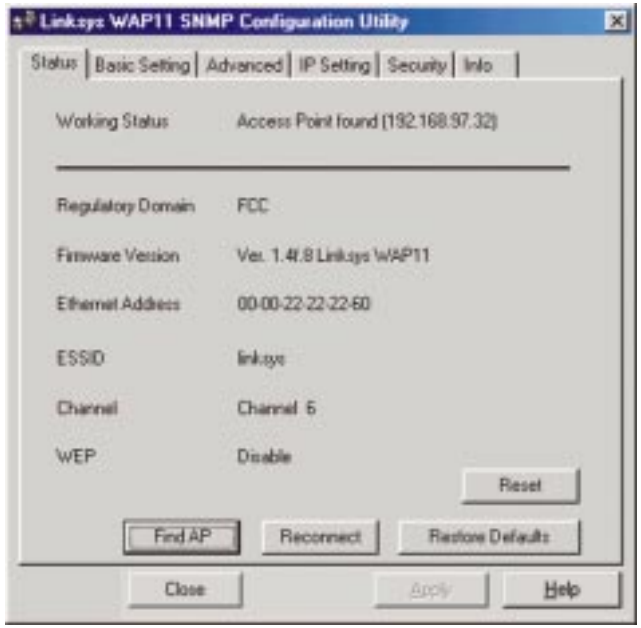
Enter the IP Address—**192.168.1.250** is the default setting—and Password—**public** is the default password—and then click the **OK** button to continue.

(As this is a private IP address, you do not need to purchase an additional IP Address from your service provider.)

DEFAULT SETTINGS
Default IP Address: **192.168.1.250**
Default SubNet Mask: **255.255.255.0**

THE STATUS TAB

The Status tab displays the Wireless Network Access Point's current status. From this tab, you can view the status information along with reconnecting to the Wireless Network Access Point and restoring its default settings.



- **Working Status.** This displays your current connection status, notifying you of any problems with the connection.
- **Regulatory Domain.** This status shows the regulatory domain preset by the manufacturer for the country the product was purchased in.
- **Firmware Version.** This displays the present version of the Access Point's firmware and is limited to a maximum of four characters. It also shows the Access Point's assigned name.
- **MAC Address.** This displays the MAC Address of your current WAP11.
- **ESSID.** The unique name shared among all points in your wireless network is displayed here.

- **Channel.** The wireless channel shared by all wireless devices connected to this Access Point is displayed here.

- **WEP.** If you have not enabled the WEP encryption protocol, this will read Disabled. When you are using WEP encryption, it will read Enabled and list the level of encryption in use.

- **Reset.** If you are experiencing problems with your wireless connection, click the **Reset** button to reset the system.

- **Find AP.** If you have changed the default settings of your Access Point and do not have the information at hand, pressing this button will locate all Access Points on your wired network and display their IP addresses and common name.

- **Reconnect.** If, for any reason, the Ethernet connection to the Wireless Network Access Point is disconnected, you can reconnect the Ethernet cable and click the **Reconnect** button here. This will retrieve the most recently saved configuration from the Access Point so you will be ready to use the Access Point SNMP Configuration Utility again.

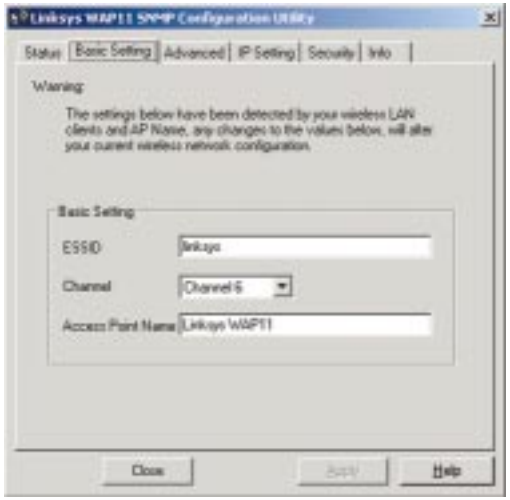
- **Restore Defaults.** Click this button to restore the Access Point's default settings. If this button is clicked, any setting you may have made through the Access Point SNMP Configuration Utility will be lost.

If you have not already clicked the **Apply** button, the **Close** button will close the SNMP Utility without saving any changes.

Click the **Apply** button to store the information. A new dialog box will appear. Then click the **Yes** button to accept the changes.

Click the **Help** button for assistance.

THE BASIC SETTING TAB



The Wireless Network Access Point will automatically detect the settings to your wireless network. Changing these values will alter your current wireless network configuration.

- **ESSID.** The ESSID or SSID is the unique name shared among all points in a wireless network. The ESSID must be identical for all points in the network. It is case sensitive and must not exceed 30 characters, which may be any keyboard character. Make sure this setting for all points in the network are the same. Verify that you're using the correct ESSID, and click the **Apply** button to set it.

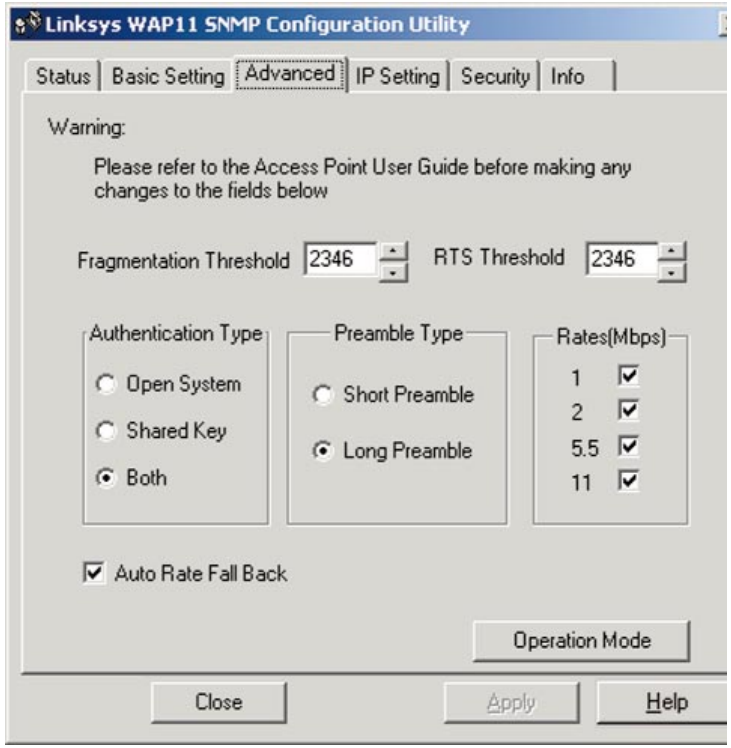
- **Channel.** Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All devices that communicate with this Access Point must use the same channel in order to work correctly. Verify that the correct channel is selected before clicking the **Apply** button.

If you have not already clicked the **Apply** button, the **Close** button will close the SNMP Utility without saving any changes.

Click the **Apply** button to store the information, then click the **Yes** button to accept the changes in the dialog box that appears.

Click the **Help** button for assistance.

THE ADVANCED TAB



Before making any changes to the Advanced tab, please check your wireless settings as these changes will alter the effectiveness of the Wireless Network Access Point. In most cases, these settings do not need to be changed.

- **Fragmentation Threshold Value.** The value should remain at its default setting of **2,346**. 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.

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

- **Authentication Type.** You may choose between **Open System**, **Shared Key**, and **Both**. The Authentication Type default is set to **Open System**, in which the sender and the recipient do NOT share a secret key. Each party generates its own key-pair and asks the receiver to accept the randomly-generated key. Once accepted, this key is used for a short time only. Then a new key is generated and agreed upon. **Shared Key** is when both the sender and the recipient share a secret key.

- **Preamble Type.** The preamble defines the length of the CRC block for communication between the Access Point and the roaming Network Card. (High network traffic areas should use the shorter preamble type.) Select the appropriate preamble type and click the **Apply** button to set it.

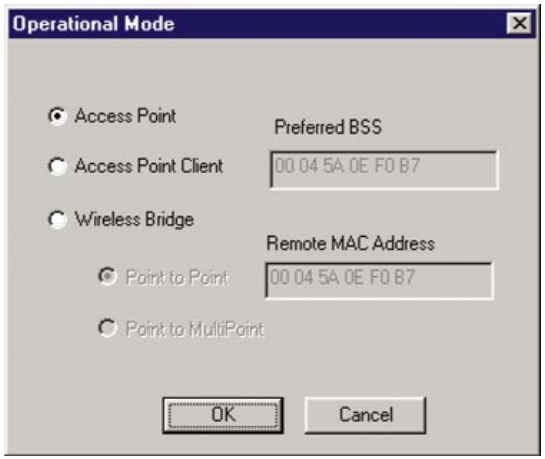
- **Basic Rates.** The basic transfer rates should be set depending on the speed of your wireless network. Verify that you've set the correct basic rate for your wireless network before clicking the **Apply** button.

- The **Auto Rate Fall Back** setting should be checked to make your wireless network flexible for roaming wireless devices. As wireless devices move away from the Access Point, the transfer rate will automatically fall back to the most optimum rate allowed.

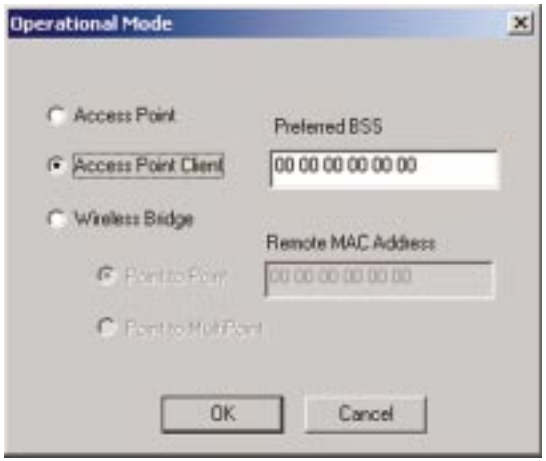
THE MODE TAB

The WAP11 offers three modes of operation: Access Point, Access Point Client, and Wireless Bridge.

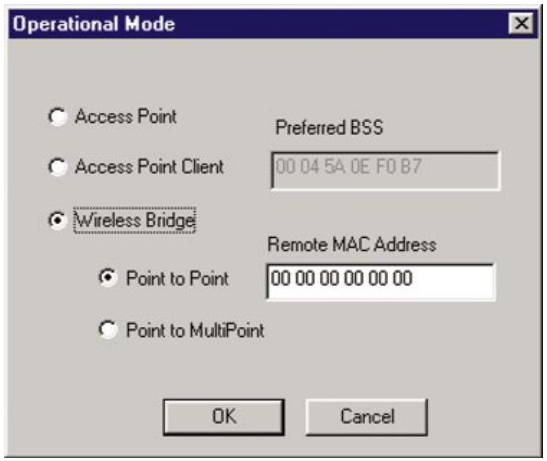
- **AP Point** - The **Operational Mode** is set to **Access Point** by default. This connects your wireless PCs to a wired network. In most cases, no change is necessary.



- **Access Point Client** - A WAP11 set to Access Point Client mode is able to talk to one main WAP11 and wireless clients within its range. This mode allows your WAP11 to act as a client of a main WAP11. A LAN attached to your WAP11 client can then be wirelessly bridged to the main WAP11. Enter the required MAC address of the main WAP11.



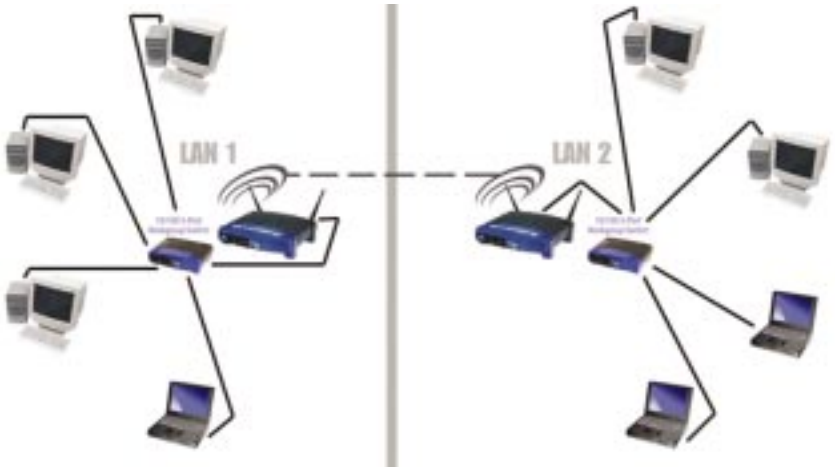
- **Wireless Bridge** - If you are trying to make a wireless connection between two wired networks, select **Wireless Bridge**. There are two options: Point to Point and Point to MultiPoint.



Note: In Wireless Bridge mode, the WAP11 can **ONLY** be accessed by another wireless bridge. In order for your other wireless devices to access the WAP11, you must reset it to Access Point mode. The two modes are mutually exclusive.

Point to Point

This mode connects two physically separated LAN segments by using two WAP11 units.



To configure a Point to Point bridged environment:

1. Click **Point to Point**.

2. Set the MAC Address of the Access Point in LAN 1 to look for the MAC Address of the Access Point in LAN 2.

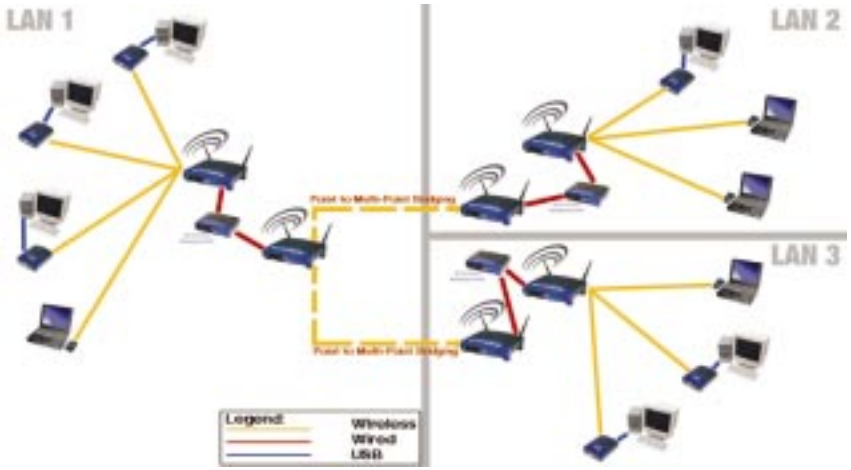
3. Set the MAC address of the Access Point in LAN 2 to look for the MAC Address of the Access Point in LAN 1.

4. On the Operational Mode tab, enter the **Remote MAC Address** of the remote Access Point. The remote Access Point also needs to be set up as a Wireless Bridge.

Note: All devices on each LAN must be connected through a hub or switch.

Point to MultiPoint

This mode allows you to construct a network that has multiple WAP11 units bridging wirelessly.



To configure a Point to MultiPoint bridged environment:

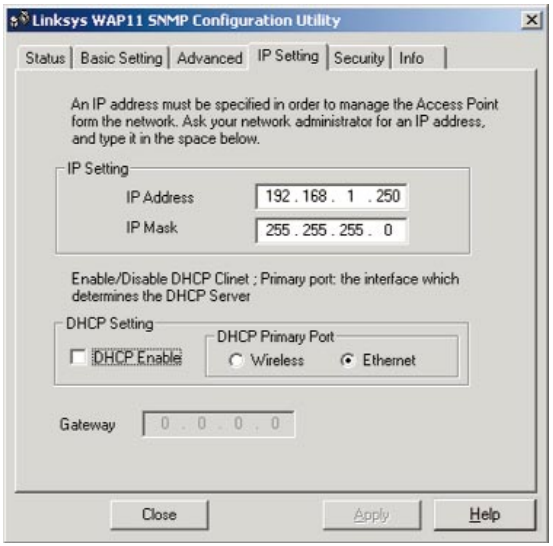
1. Click **Point to MultiPoint** for the WAP11 used in LAN 1. No MAC Address binding is needed.

2. Set the Access Points in LAN 2 and LAN 3 to Point to Point, and have them look for the MAC Address of the Access Point in LAN 1.

Only one of the Access Points must be in Point to MultiPoint mode. For all other bridged Access Points, select the **Point to Point** option, and enter the **Remote MAC Address** of the Access Point set to Point to MultiPoint.

Click the **Apply** button to store the information. A new dialog box will appear. Click the **Yes** button to accept the changes.

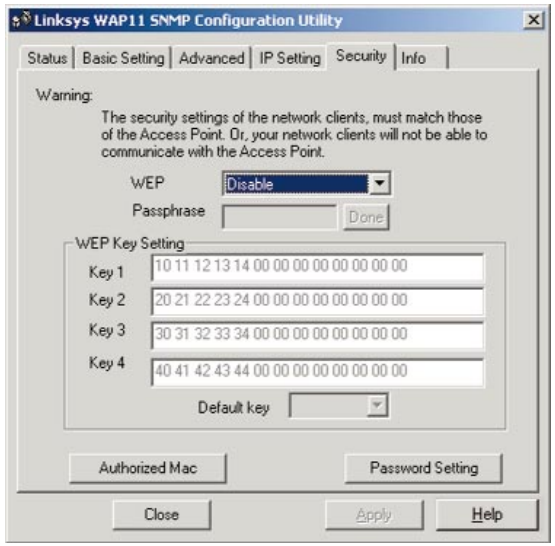
THE IP SETTING TAB



The IP settings for the Access Point are made from this tab. This is for the SNMP Configuration Utility use only.

- **IP Address.** This IP address must be unique to your network. We suggest you use the default IP address of 192.168.1.250. As this is a private IP address, there is no need to purchase a separate IP address from your service provider. Verify the address and click the **Apply** button to save changes.
- **IP Mask.** Your Access Point's Subnet Mask must be the same as your Ethernet network. Verify this is correct and click the **Apply** button to set it.
- **DHCP Setting.** Check the box next to **DHCP Enable** to allow it to obtain a dynamic IP address from a DHCP server. You may also choose how the WAP11 dynamically obtains an IP address—either **Wireless** or **Ethernet**.
- **IP Filtering.** For security, click the check box to enable IP filtering, which allows IP packets only through the Access Point.
- **Gateway.** This setting only appears when the DHCP client is enabled; it indicates the status of the gateway and is not user-adjustable.

THE SECURITY TAB



WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 64/128-bit shared key algorithm, as described in the IEEE 802.11 standard. In order to utilize WEP encryption, all points in your wireless network must have WEP enabled and be set to the same Key Setting.

- **WEP (Disable/64-bit/128-bit).** To use WEP encryption, select **Enable**. For no WEP encryption, select **Disable**. This specific WEP encryption is unique to Linksys and may conflict with other vendors' WEP encryption.
- **Passphrase.** This is the code used when a point on the wireless network wishes to log on to the network. It is a text string with a maximum of 32 alphanumeric characters. The WEP Key Settings are based upon the Passphrase determined by you. Type that here. This passphrase may not work with non-Linksys products due to possible incompatibility with other vendors' passphrase generators.
- **WEP Key Setting.** This setting is the configuration key used in accessing the wireless network via WEP encryption. To generate an encryption key:

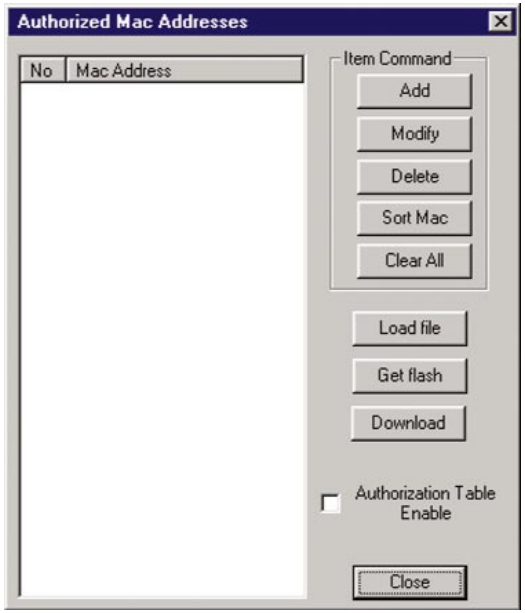
1. Type exactly the same case sensitive Passphrase in the PassPhrase field. For security purposes, please create your own Passphrase.
2. Click the **Done** button to create the encryption keys. The Passphrase generates four unique keys.

3. Verify the Default Key is the same for each point on the wireless network.

- **Password Setting.** Choose **Read/Write** and/or **Read Only**. It is recommended that you change both to maximize security. For both options, type in a password and confirm it.

Note: When WEP settings are changed, you will lose network access until WEP settings are updated on the PCs. You must reconfigure your wireless PCs to the new WEP settings. If you are configuring this wirelessly, you will lose your connection.

- **Authorized MAC.** You may authorize who can gain network access through the Access Point by using *MAC Address filtering*. Only MAC addresses in the Authorization table will be allowed to communicate with the WAP11. Click the **Authorize MAC** button to view the Authorized MAC Addresses screen.



Add - Click the **Add** button to authorize more MAC addresses.

Delete - Click the **Delete** button to remove MAC addresses.

Modify - Use the **Modify** button to edit any MAC address.

Sort MAC - The **Sort MAC** button arranges the MAC addresses in numerical order.

Clear All -This button removes all MAC addresses from the table.

Get flash - To view the table of currently authorized MAC addresses, click the **Get flash** button.

Authorization Table Enable - Check the box next to **Authorization Table Enable** to activate *MAC Address filtering*.

To create a load file, follow these steps:

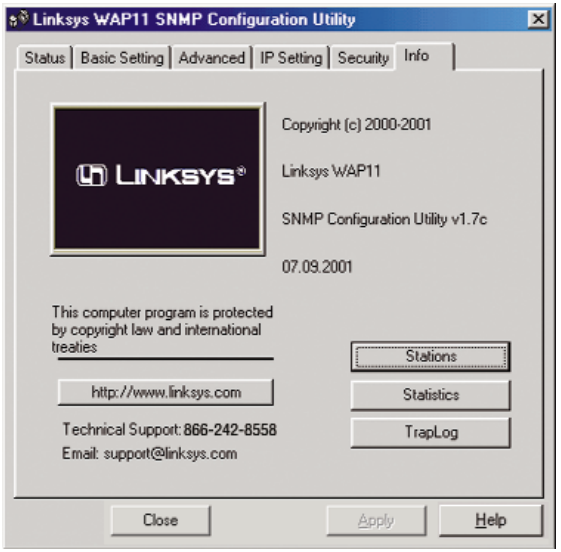
1. Create a text file (e.g., MAC.TXT) using Notepad or another text editor.
2. Enter the 10 digit MAC address of each adapter that you wish to authorize communication with the Access Point. ONE PER LINE!!!!!!!!
3. Save the file. Be sure to note the full path to the saved file.
4. Click the **Load File** button.
5. A screen will pop-up prompting you to browse for the file (e.g. MAC.TXT). Once you have located the file, highlight it and click **Open**.
6. All the MAC addresses that you entered into the text file should now appear in the window.
7. Click the **Download** button to save these addresses in your Authorization Table.
8. Make sure the Authorization Table Enable box is checked.
9. Click the **Close** button.
10. When asked to confirm your choice, click the **Yes** button.
11. Click the **Apply** button on the security tab.
12. If you ever decide to change the entries on the table, simply edit the text file and reload it using steps 4-11.

If you have not already clicked the **Apply** button, the **Close** button will close the SNMP Configuration Utility without saving any changes.

Click the **Apply** button to store the information. A new dialog box will appear. Then click the **Yes** button to accept the changes.

Click the **Help** button for assistance.

THE INFO TAB



The Info tab displays general information about Linksys and the Access Point SNMP Manager. The SNMP Configuration Utility's copyright date and version number are listed as well as the Utility's firmware version. At the bottom of the screen, you will find a button that will access Linksys' web page (once your Internet connection is properly set up), the email address for technical support, and the phone number to call for technical support.

- **Stations**. This shows the MAC addresses of those machines making wireless connections to the Access Point.
- **Statistics**. This displays the connection statistics for your wireless and Ethernet connections.
- **TrapLog**. This displays the information on any SNMP messages read by your Access Point.

Troubleshooting

Common Problems and Solutions

This chapter provides solutions to problems usually encountered during the installation and operation of the Wireless Network 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.

What is the purpose of antenna diversity and when should it be used? When used, how should it be set-up?

The dual antennae on the Access Point are probably best explained using this example. Take television, if you have ever had the old "rabbit ear type of antenna" and saw reflections on TV (called "ghosts"), then you moved the antenna and the reflections "went away." (Using two antennae allows us to "MOVE AWAY" from reflections that cause us to lose or have to retransmit data.) They should be used indoors as outdoor reflections are rare. As long as both antennae cover roughly the same area, this is fine.

Frequently Asked Questions

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

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

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

What is 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 Wireless Network Access Point. Before using the roaming function, the workstation must make sure that it is the same channel number as the Wireless Network 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 Wireless Network 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 Wireless Network 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 Wireless Network Access Point and the distance of each Wireless Network Access Point to the wired backbone. Based on that information, the node next selects the right Wireless Network 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 Wireless Network Access Point or whether it should seek a new one. When a node no longer receives acknowledgment from its original Wireless Network Access Point, it undertakes a new search. Upon finding a new Wireless Network 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 Wireless Network 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.

Glossary

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 others stay in close proximity to the rest of the network.

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

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

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

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

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

DSSS - Also known as "Direct Sequence Spread Spectrum," this is a variety of radio transmission methods that continuously change frequencies or signal patterns. Direct Sequence Spread Spectrum (DSSS), which is used in CDMA, multiplies the data bits by a very fast, pseudo-random bit pattern (PN sequence) that "spreads" the data into a large coded stream that takes the full bandwidth of the channel.

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.

ESS - More than one BSS in a network.

FHSS - Also known as "Frequency Hopping Spread Spectrum." Frequency Hopping Spread Spectrum (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 - Programming that is inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

IEEE - The Institute of Electrical and Electronics Engineers. The IEEE describes itself as "the world's largest technical professional society—promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members."

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

Infrastructure - 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 an Access Point that connects them to the rest of the network.

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

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

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

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

MAC Address - The MAC (Media Access Control) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

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

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

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

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

RJ-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.

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

TCP (Transmission Control Protocol) - 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 packets) that a message is divided into for efficient routing through the Internet.

TCP/IP - Transmission Control Protocol/Internet Protocol (TCP/IP) is 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.

UDP (User Datagram Protocol) - A communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP.

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 (Wired Equivalent Privacy) - A data privacy mechanism based on a 64-bit shared key algorithm, as described in the IEEE 802.11 standard.

WINIPCFG - Configuration utility based on the Win32 API for querying, defining, and managing IP addresses within a network. A commonly used utility, under Windows 95, 98, and Millennium, for configuring networks with static IP addresses.

Specifications

Standards:	IEEE 802.3 (10BaseT), IEEE 802.11b (Wireless)	
Channels:	11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)	
Ports:	One 10BaseT RJ-45 Port, One USB Port	
Cabling Type:	10BaseT:	UTP Category 3 or Better
	USB:	USB Cable
Operating Range (Wireless):	Indoors:	Up to 30M (100 ft.) @ 11 Mbps
		Up to 50M (165 ft.) @ 5.5 Mbps
		Up to 70M (230 ft.) @ 2 Mbps
		Up to 91M (300 ft.) @ 1 Mbps
	Outdoors:	Up to 152M (500 ft.) @ 11 Mbps
		Up to 270M (885ft.) @ 5.5 Mbps
		Up to 396M (1300 ft.) @ 2 Mbps
		Up to 457M (1500 ft.) @ 1 Mbps
Data Rate:	Up to 11Mbps (Wireless), 10Mbps (Ethernet)	
LEDs:	Power, Act, Link (Wired - Link/Activity)	

RF Specification

1.1 General

Emission Type:	Direct Sequence Spread Spectrum (DSSS)
RF Frequency:	2471MHz - 2497MHz - Japan Band 2400MHz - 2483.5MHz - North America, Europe, Korea and Extended Japan Band 2455MHz - 2475MHz - Spain 2446.5MHz - 2483.5MHz - France
Operating Channel:	11 Channels (US, Canada) 13 Channels (Europe, Korea) 14 Channels (Japan)
Radio Chipset:	Intersil PRISM II

Baseband Processor:	HFA 3861B or HFA 3863
MAC Controller:	MAC Atmel AT76C510
Radiation Power:	13 - 20 dBm at maximum radiation direction

1.2 Transmitter

RF Output Power:	4 mW/MHz
Frequency Stability:	Within + 25 ppm
Data Modulation Type:	BPSK (1/5.5Mbps) / QPSK (2/11 Mbps) CCK (5.5/11 Mbps)

1.3 Power

Power Voltage:	DC 5.0 Volt + 5%, AC Adapter AC 100V-240V
Power Consumption:	5.0 Volt, 2.0A (Typical)

Environmental

Dimensions:	7.31" x 6.16" x 1.88" (186mm x 154mm x 48mm)
Unit Weight:	20.5 oz. (0.58 kg)
Power:	5V, 550mA TX, 230mA RX
Certifications:	FCC Class B, FCC Class C, CE Mark Commercial
Operating Temp.:	0ºC to 55ºC (32ºF to 131ºF)
Storage Temp.:	0ºC to 70ºC (32ºF to 158ºF)
Operating Humidity:	0% to 70% Non-Condensing
Storage Humidity:	0% to 95% Non-Condensing

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' 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.

Contact Information

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

Sales Information	800-546-5797 (LINKSYS)
Tech Support	866-242-8558
RMA Issues	949-261-1288
Fax	949-261-8868
Email	support@linksys.com
Web	http://www.linksys.com
FTP Site	ftp.linksys.com

http://www.linksys.com

© Copyright 2001 Linksys, All Rights Reserved.