

Wireless Access Point

User's Guide



Table of Contents

INTRODUCTION	1
WIRELESS LAN	1
THE WIRELESS ACCESS POINT	2
WIRELESS ACCESS POINT HARDWARE	3
<i>Front Panel</i>	3
<i>Rear Panel</i>	4
INSTALLATION AND MANAGEMENT	5
SYSTEM REQUIREMENTS	5
PACKAGE CONTENTS	5
INSTALLATION CONSIDERATIONS	5
WIRELESS LAN BASICS	6
<i>Radio Transmission</i>	6
<i>Range</i>	6
NETWORK TOPOLOGY	7
<i>IBSS</i>	7
<i>BSS</i>	7
<i>ESS</i>	7
OPERATION MODES	8
<i>Access Point</i>	8
<i>Wireless Bridge</i>	8
<i>Access Point Client Mode</i>	9
NETWORK FUNCTIONS OF THE ACCESS POINT	10
INSTALLATION	12
CONFIGURE WIRELESS AP	14
USING THE USB CONFIGURATION UTILITY	14
<i>USB Utility Menus</i>	16
USING THE SNMP MANAGEMENT UTILITY	20
<i>Accessing the SNMP Manager</i>	20
<i>SNMP Utility Menus</i>	21
<i>Device Information</i>	21
<i>Authorized MAC Address</i>	27

Introduction

In addition to a general description of the Wireless Access Point, this section provides a brief description of Wireless Local Area Network (wireless LAN or WLAN) technology, its benefits, capabilities and limitations.

Wireless LAN

A wireless LAN is a cellular computer network that facilitates communication with radio signals instead of wires. Wireless LANs are used increasingly in both home and corporate environments. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. The advantage of high mobility and the absence of cabling and other fixed infrastructure has proven to be a boon for many users.

Wireless LAN users can use the same network applications they use on an Ethernet LAN. Wireless LAN adapter cards used on laptop and desktop systems, support the same protocols as Ethernet adapter cards. For most users, there is no noticeable functional difference between a wired Ethernet desktop computer or mobile WLAN workstation other than the added benefit of the ability to roam within the WLAN. Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order use servers, printers or an Internet connection supplied through the wired LAN. The Wireless Access Point is a device used to provide this link.

People use wireless LAN technology for many different purposes. Two of the main advantages of using wireless LAN technology are its mobility and low cost.

Mobility Productivity increases when people have access to data in any location within the operating range of the WLAN. Ad-hoc management decisions based on real-time information can significantly improve worker efficiency.

Low Implementation Costs WLANs are easy to set up, manage, change and relocate. Networks that frequently change, both physically and logically, can benefit from WLANs ease of implementation. WLANs can operate in locations where installation of wiring may be impractical. Furthermore, IEEE standardization mandates interoperability of all WLAN devices that conform to the 802.11b set of standards.

Our full range of Wireless LAN products include:

- ✂ ✂ Wireless PC card used with laptop computers
- ✂ ✂ Wireless PCI used with desktop computers
- ✂ ✂ Wireless Access Point
- ✂ ✂ Wireless Home Gateway

The Wireless Access Point

A Wireless Access Point may be used to serve different functions, including:

- ✂✂ **Bridge** The Wireless Access Point can be used to provide access to the shared network facilities of an Ethernet LAN.
- ✂✂ **Wireless LAN Extension** The effective communication range of wireless workstations can be increased.
- ✂✂ **Improve Signal Quality** Providing a central relay station can provide a communication path for WLAN components that otherwise might be prevented from “seeing” other WLAN members.
- ✂✂ **Wireless LAN Security** The Wireless Access Point can be configured to use encryption for improved security on a WLAN.

Features and Standards

Wireless LAN technology is based on the internationally recognized IEEE 802.11 set of standards for wireless LANs. The Wireless Access Point is fully compliant with the IEEE 802.1b standard and can inter-operate with other compliant equipment.

The Wireless Access Point also complies with the following regulatory standards:

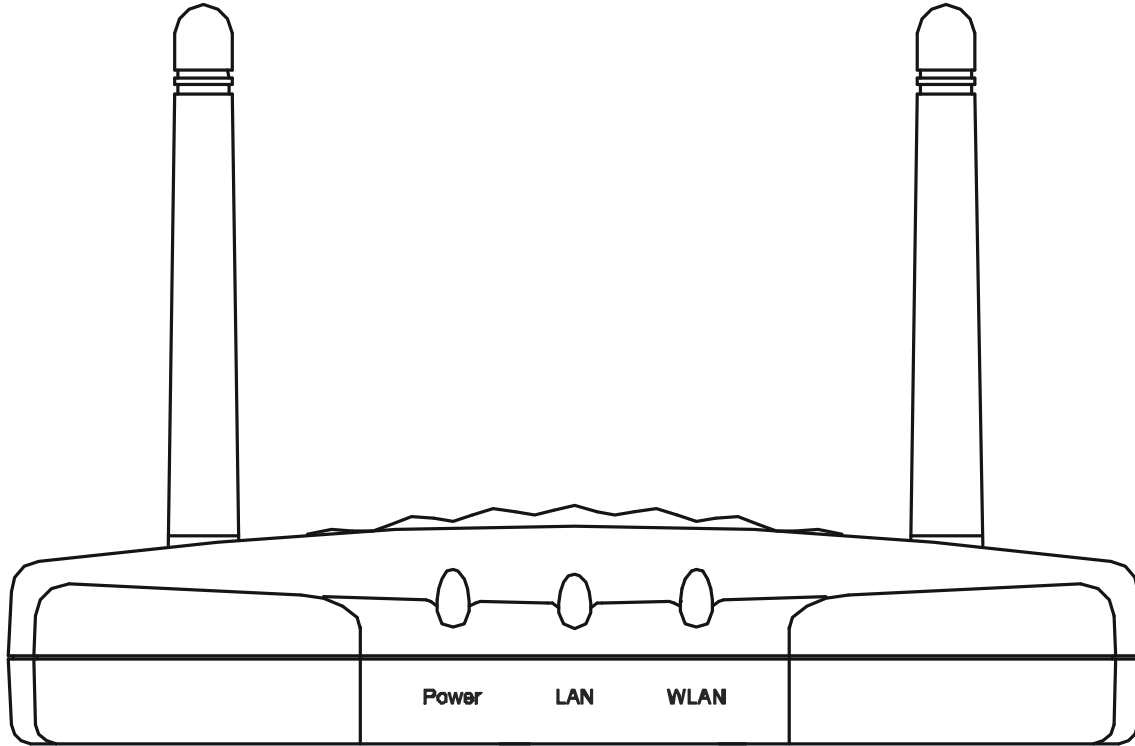
- ✂✂ FCC part 15 Class A with no external shielding
- ✂✂ FCC part 15 Class B, ETS 300-339 compliance, including CE mark
- ✂✂ The regulatory requirements for Japan, Europe and many other areas of the world

The Wireless Access Point features include:

- ✂✂ Data transfer rates of up to 11 Mbps
- ✂✂ An effective range of up to 300 meters (900 feet) outdoors or 100 meters (300 feet) indoors
- ✂✂ 10BaseT Ethernet port interface for bridging Wireless LAN to an Ethernet LAN
- ✂✂ Seamless roaming for notebook computers, wireless PCs, and other computers equipped with Wireless LAN-equipped
- ✂✂ Built-in diagnostics including a power-up self-check
- ✂✂ Dual antenna assembly with optional diversity
- ✂✂ Firmware can be upgraded easily in the field
- ✂✂ Data encryption (WEP 64 and WEP 128)
- ✂✂ SNMP support
- ✂✂ DHCP support (client)
- ✂✂ Optional Short RF preamble
- ✂✂ USB Configuration

Wireless Access Point Hardware

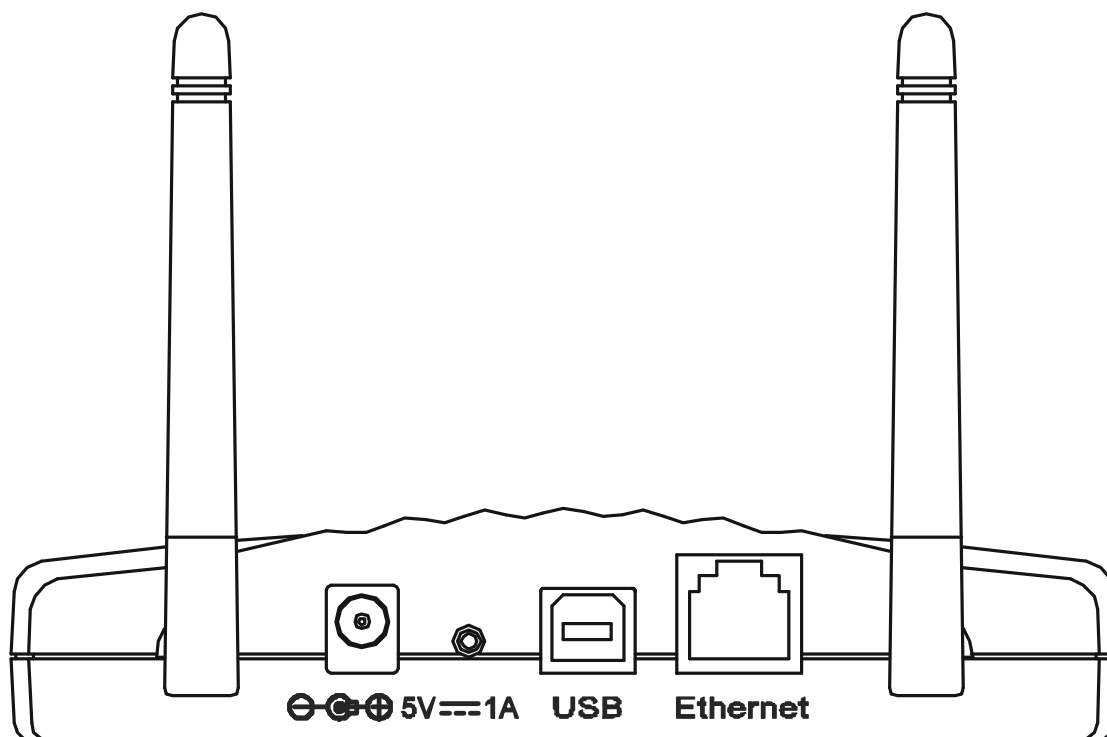
Front Panel



LED Display

	On	Blink	Off
Power	Unit is plugged in and working normally	Unit is booting up and running self diagnostic test	Unit is not plugged in and it is off
LAN	Ethernet Cable is plugged in and there is a valid network connection	The Ethernet port is active	Ethernet cable not plugged in or the connection is not valid
WLAN	N/A	Detecting Wireless LAN network activities	No Wireless LAN network available in the vicinity

Rear Panel



Connections

Power	Plug in the AC/DC adapter here. Please make sure to plug in adapter to the Wireless Access Point before plugging the other end of the power adapter to an electrical wall outlet or power strip.
USB	The USB port is used to make the USB connection from the device to a computer with the USB cable for first time configuration and configuration using the Wireless AP USB Utility.
Ethernet	The Ethernet port is used to connect the Wireless Access Point to the Ethernet LAN or a single computer using an Ethernet cable (RJ-45).

Note: To use the USB port on the Wireless Access Point, the computer that performs the configuration must have a USB interface or Windows 98, 2000, or ME installed. USB is not supported under Windows NT or Windows 95.

CAUTION: USE ONLY THE POWER ADAPTER INCLUDED WITH THE DEVICE !

Installation and Management

The wireless access point installs quickly and easily. All software is Plug and Play. Once the device has been installed, it may be managed via the password-protected configuration utility. The access point can be managed using any either the USB, Ethernet or WLAN interface.

The following is a summary of the installation process:

1. Connect the wireless access point power cord and USB cable
2. Install a software driver that allows communication through the USB port
3. Install configuration utilities enabling configuration of the device
4. Configure the wireless access point

System Requirements

Be sure to have the following:

PC with USB port

Microsoft Windows 98, ME, 2000, or NT 4.0

Package Contents

Please verify that the package contains the following items:

1. Wireless Access Point
2. AC Adapter
3. USB Cable
4. Installation CD containing software and this User's Guide
5. Quick Installation Guide

Installation Considerations

The device can be placed on a shelf or desktop for optimal positioning. Be certain to place the device within reach of an available power outlet.

Designed to go up to 100 meters indoors and up to 300 meters outdoors, Wireless LAN lets you access your network from anywhere you want. Keep in mind, however, that the number of walls, ceilings, or other objects that the wireless signals must pass through can limit signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. To realize the maximum possible range, follow these basic principles:

1. **Keep the number of walls and ceilings to a minimum:**
The signal emitted from Wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range Wireless LAN devices from 1 to 30M. Position your Access Points, Residential Gateways, and Computers so that the number of walls or ceilings obstructing the signal path is minimized.

2. **Consider the direct line between Access Points, Residential Gateways, and Computers:** A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it is over 14 meters thick. Be careful to position the Access Point and Adapters so the signal can travel straight through (90° angle) a wall or ceiling for better reception.
3. **Building Materials make a difference:** Buildings constructed using metal framing or doors can reduce effective range of the device. Always position Access Points, Residential Gateways, and Computers so that their signal can pass through drywall or open doorways, avoid positioning them so that their signal must pass through metallic materials.
4. **Make sure that the antennae are positioned for best reception.**
5. **Keep your product away (at least 1-2 meters) from electrical devices:** Position WLAN devices away from devices that generate RF noise, like microwaves, monitors, electric motors, etc.

Wireless LAN Basics

In order to set up and use your the wireless access point you should have some basic understanding of WLAN technology and the various functions the device can perform on your network.

Radio Transmission

WLAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive signals. When a wireless access point is present, it becomes a base station for the WLAN nodes in its broadcast range. WLAN nodes transmit digital data using FM (frequency modulation) radio signals. WLAN devices generate a carrier wave and modulate this signal using various techniques. In this way, digital data can then be superimposed onto the carrier signal. The radio signal carries data to wireless-capable devices within its range. The antennae of wireless-equipped devices listen for and receive the signal. The signal is demodulated and the transmitted data extracted. The transmission method used by the access point is called Direct Sequence Spread Spectrum (DSSS) and operates in a range of the radio spectrum between 2.4GHz and 2.5GHz for transmission.

Range

In an average American 4-bedroom home, range should not be a problem. If you experience low or no signal strength in areas of your home that you wish to access, consider positioning the Access Point in a location directly between the Residential Gateways and Wireless Adapter equipped Computers. Adding Access Points to rooms where the signal does not appear as strong as desired can improve signal strength.

Network Topology

The IEEE 802.11 standard supports three basic topologies for WLANs—the Independent Basic Service Set (IBSS), the Basic Service Set (BSS), and the Extended Service Set (ESS). Wireless LAN components can be used to extend, enhance or entirely replace existing Ethernet infrastructure. The wireless access point can accommodate any WLAN topology.

IBSS

An Independent Basic Service Set or ad-hoc network consists of two or more wireless stations that communicate directly, peer-to-peer, without the services of a wireless access point. An example of an ad-hoc network or IBSS would be a group of wireless-equipped laptop computers at a trade show set up to share information. In this arrangement, one of the WLAN units is elected to act as a controller or base station, similar to the function of a wireless access point except there is no connection to a wired Ethernet LAN. Ad-hoc networks are very easy to set up and require minimal involvement by network administrators or MIS personnel.

BSS

In a Basic Service Set, a wireless access point performs multiple tasks; it is a base station and network access controller for the wireless stations in the BSS. The access point can also provide a connection to a wired Ethernet LAN for the BSS member stations. An example of a BSS might be a business meeting conducted in a room with only a single Ethernet port available. Each participant has a wireless laptop computer and requires simultaneous access to a data server on the Ethernet LAN. A wireless access point provides the connection to the Ethernet and acts as the network control station for the BSS members.

In a BSS, the wireless access point performs functions similar to an Ethernet switch. The access point controls network access and maintains a dynamically updated list of all the members of the BSS. Members of each BSS are added or deleted from the list as they join or leave the BSS. Wireless stations in the BSS are identified by their MAC address.

ESS

An Extended Service Set is a series of two or more basic service sets networked on an Ethernet or other type of LAN. Each access point provides connection to the Ethernet LAN for their respective BSS.

Each BSS is identified by a unique number, the BSS-ID (the MAC address of the Wireless Access Point). Wireless stations on an ESS automatically select the access point or BSS that can best serve them. If no access point can be found the device will scan for a usable access point.

An ESS can be set up so that wireless stations can roam anywhere within the range of any of access points, that is, to any member BSS, and still maintain links to both the WLAN and the Ethernet. In this case, each station shares a common ESS. The ESS is identified by an ESS ID number used by all stations in the ESS.

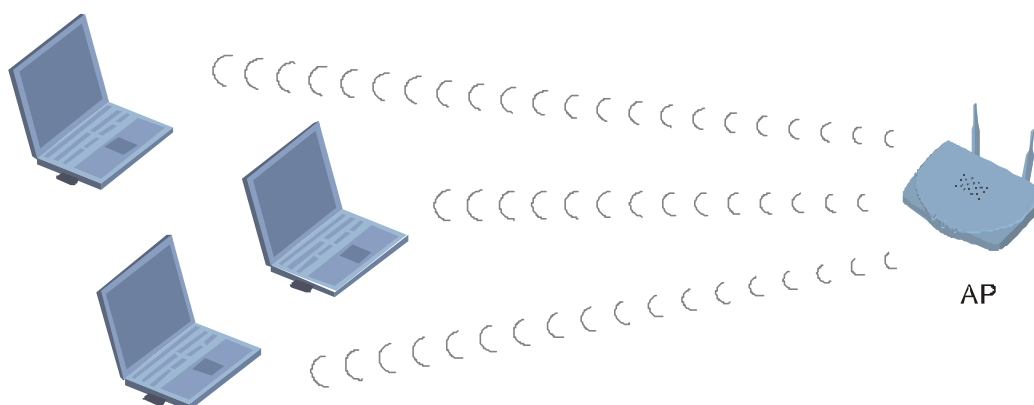
Wireless access points can also be used to segment a wireless network. Under such circumstances, more than one ESS might be used. Two or more separate Extended Service Sets can occupy the same physical space. Each station on a wireless LAN can only use one ESS.

Operation Modes

Flexibility is fundamental to a wireless network. For this reason, the wireless access point can be configured to perform different functions and customized according to the needs of your network.

Access Point

In this mode, the access point provides access for wireless stations to wired LANs and from wired LANs to wireless stations. Wireless stations within the range of the access point may communicate with each other via the access point. This is the default operation mode of the device.

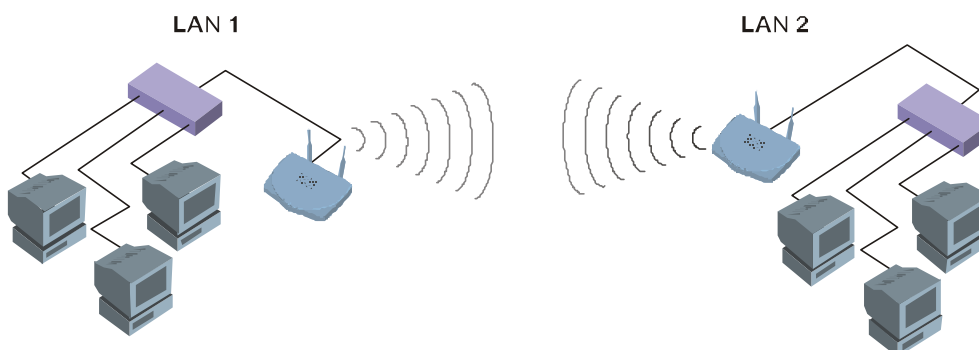


Simple Wireless Access Point

Wireless Bridge

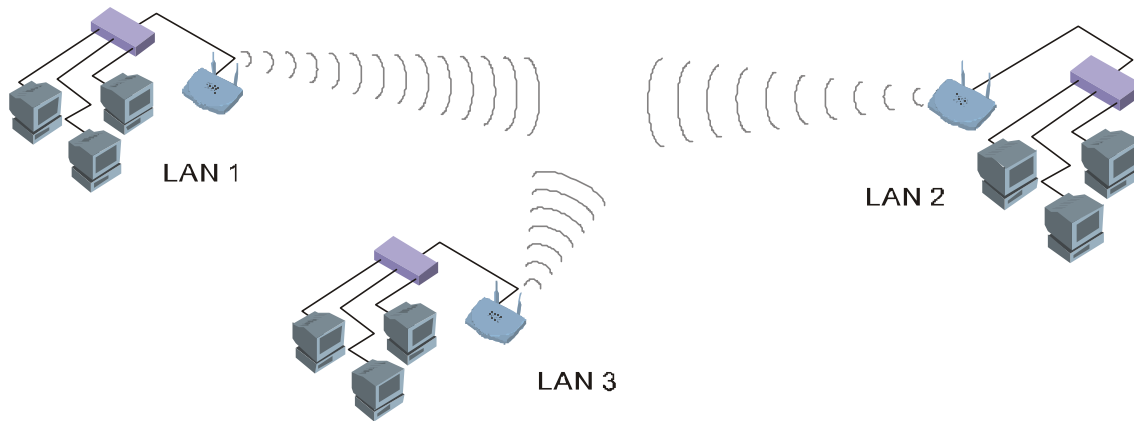
Wireless Bridge mode allows two types of connections:

1. **WB Point-to-Point:** The wireless bridge is configured to communicate with a specific remote MAC address.
- 2.



Wireless Bridge Point-to-Point mode

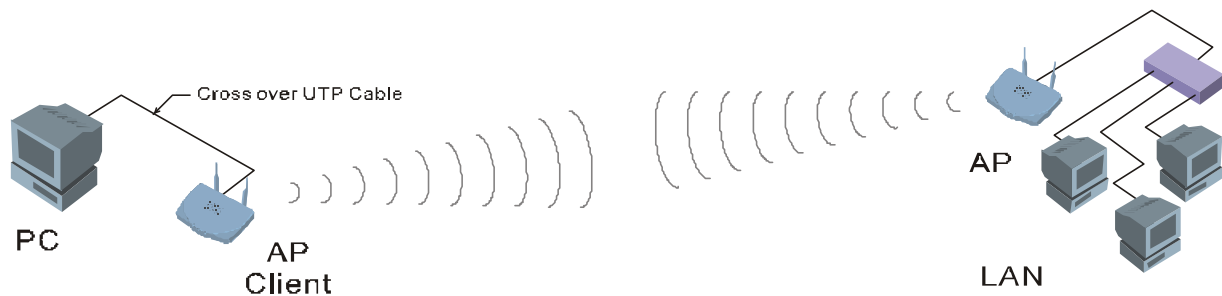
3. **Wireless Bridge Point to Multipoint:** The wireless bridge is configured to communicate with any wireless bridge available on the same channel and using the same ESS ID.



Wireless Bridge Point-to-Multipoint mode

Access Point Client Mode

The access point can also act as a client on a wireless LAN. When configured as a client the access point functions in the capacity of a wireless end station only. Communication through the wireless interface of the device can only be accomplished using another Access Point functioning in AP mode. When configured as a client, the access point connects to a single computer or an Ethernet LAN via the Ethernet interface. An access point configured to be a wireless client connected to a single computer is illustrated in the figure below.



Wireless Access Point used as a Client

Network Functions of the Access Point

The wireless access point performs key network functions controlling access to both the wireless and Ethernet LANs. The following paragraphs elaborate on the network function of the wireless access point.

MAC Layer Bridging

The Wireless Access Point functions as an intelligent bridge. It listens to all data traffic on all its interfaces and maintains a MAC address database in much the same way that an Ethernet switch maintains a MAC address table. MAC address information is updated dynamically and MAC addresses that are inactive for a specified period are deleted from the database or “aged out”. The MAC address database also indicates the type of interface being used by each entry (either WLAN or Ethernet). Packets destined for unknown MAC Addresses are forwarded to the Ethernet interface.

When necessary, the Wireless Access Point uses the Address Resolution Protocol (ARP) to match IP addresses to MAC addresses and stores ARP information in its database as well. ARP information is likewise aged out of the database.

Filtering and Access Control

The wireless access point can limit the wireless devices that associate with it and the data packets that are forwarded through it. Filters can provide a degree of security and improve network performance by eliminating broadcast/multicast packets from the radio network.

The ACL (Access Control List) contains the MAC address of every wireless device allowed to associate with the access point. This prevents unauthorized access to network resources.

The access point can discriminate based on the destination address of packets it handles by maintaining a list of disallowed destinations. This can improve efficiency by eliminating unnecessary transmission of data packets.

The type of packet forwarded through the access point can be controlled using a filter. Type Filtering prevents specific packets from being processed. Certain packet types such as broadcast packets from devices not important to the wireless LAN are discarded to preserve bandwidth. Filtering out unnecessary frames can improve overall network performance.

DHCP Support

The access point supports the Dynamic Host Configuration Protocol (DHCP) used to obtain a leased IP address and network configuration information from a remote server. When DHCP is enabled, the access point sends out a DHCP request to obtain the IP settings and network configuration information. The access point can be configured to download two additional files when a boot takes place, the firmware file and an HTML file. DHCP or BOOTP servers can be programmed to transfer these two files when a DHCP request is made.

Media Types

The wireless access point can be used to bridge the wired Ethernet LAN and wireless LAN radio network. The 10BASE-T Ethernet interface fully complies with Ethernet Rev. 2 and IEEE 802.3 specifications and operates in full duplex. The radio interface conforms to IEEE 802.11b specifications for wireless LAN. The WLAN interface operates at speeds of up to 11 Mbps using direct sequence radio technology. The wireless access point supports multiple-cell operations with fast roaming between cells. With the direct sequence system, each cell operates independently. Adding cells to the network can increase the coverage area and total system capacity.

The access point supports wireless devices operating in Continuously Aware or Power Save modes.

Media Access Control

All WLAN devices, like all Ethernet devices, have a unique, hardware-encoded Media Access Control (MAC) address. Wireless LAN algorithms employ carrier sense and collision avoidance techniques (CSMA/CA) to ensure network access to all devices and error checking (CRC) for accuracy of data transmissions. The method of access control used in WLAN is called the Distributed Coordination Function (DCF).

Data Transfer Rates

The actual rate at which data transmission occurs varies according to the strength of signal transmitting the data. Distance and environment can effect the strength of the signal that can be transmitted and received. The signal strength determines the type of modulation technique used to encode data, which effects the volume of data (i.e. the number of bits) that can be encoded in a given space of the carrier signal. The IEEE 802.11b standard specifies that WLAN devices adapt the rate of transmission to use the best rate achievable. Each wireless device first determines if conditions diminish signal strength and then chooses one of four possible bit rates (1, 2, 5.5, or 11 Mbps) based on this learned information.

Installation

The installation process consists of three phases:

1. **Connection.** Connect the power cable and USB cable
2. **Software Installation.** Install a driver for the USB link, then install software used to manage the device
3. **Device Configuration.** Configure device settings to suit your network

Initial configuration of the access point must first be done using the USB interface. Once the device has been configured the password-protected management software can also be used to configure the access point via the wireless LAN or Ethernet interfaces.

To configure the device via the USB cable, two software installations are required. First you will install a USB driver to enable the communication link. Then you will install software that enables configuration of the device via the USB link.

Connect the Device

All cables including the power adapter cable connect to the access point on the back of the unit. Look on the back of the device and you will see three connection points:

1. Power cable connection for 5V adapter
2. USB port
3. Ethernet port

For the initial configuration, you will use only the USB cable

Follow these steps in order:

1. Insert the Installation CD into the CD-ROM drive on the computer you will link to the access point.
2. Connect the power adapter cable to the access point.
3. Connect the power adapter cable to a suitable power source (power strip or electric outlet).
4. Connect the USB port on the access point to the USB port on the computer with the USB cable. When the USB link is established, the computer should automatically detect the connection and begin the installation of the USB driver.

Install USB Driver

After the computer-to-access point USB connection has been made, the "Add New Hardware Wizard" window will be displayed. Insert the Installation Disk into the CD-ROM drive and click the **Next** button.

1. Select the "Search for the best driver..." option by clicking inside the circle to the left of it, and click the **Next** button.
2. In the "Add New Hardware" menu, click **Next**.
3. This window informs you that the device driver is ready for installation. Click **Next** to install the USB driver.
4. After the driver has been installed, you will be presented with a window informing of its completion. Click **Finish** to continue to the "Properties" window.

Install Configuration Utilities

The Installation CD contains software needed to set up and manage the access point. Two separate configuration utilities will be installed simultaneously. One utility is used to configure the device through the USB interface, the other operates through the Ethernet interface. This software is Plug and Play. This will be a familiar process for anyone experienced with Plug and Play installations. The following is a step by step description of the management software installation:

1. Click on the **My Computer** icon on your desktop. Click on the icon representing your CD-ROM to open it. Open the Wireless AP folder, find the **Setup** icon and click on it to launch the Setup program.
2. The **Welcome** screen informs you that the Wireless AP Setup program is ready to begin. Close all other windows that are open and quit any programs that may interfere with installation before you continue. Click the **Next** button to go to the next step.
3. In the **User Information** screen, enter a name and company name then click on the **Next** button.
4. In the **Choose Destination Location Screen** you are asked to confirm the **Destination Directory** for the application software. If you wish, you may *Browse* to select another location for the directory.
5. The **Select Program Folder** screen suggests the program folder Wireless AP be used as a location for the program icon. You may use this folder, rename it by typing in a new name, or choose a different folder from the list. Click **Next** to select the program folder.
6. The **Start Copying Files** screen informs you that the files are ready to be copied. You can review the program setup information here. If you are satisfied with the information listed, click **Next** to begin copying the program files.
7. When the files have been copied, the **Setup Complete** screen will offer the option of launching the management program upon finishing the installation. Check the "Yes, launch the program..." box if you wish to start the program now and click the **Finish** button.

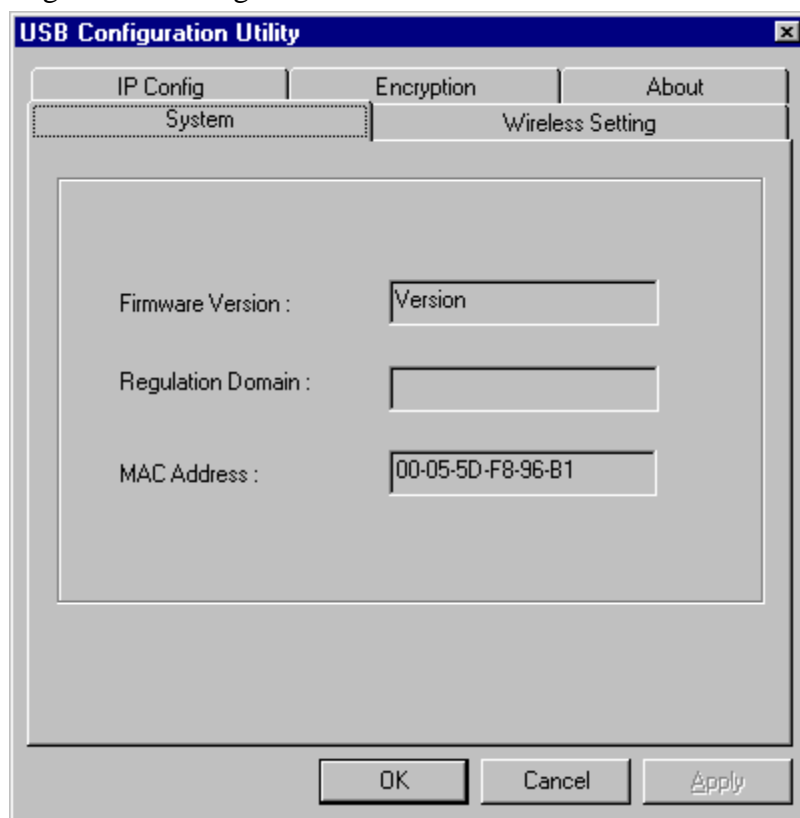
Configure Wireless AP

When the Wireless AP USB Configuration Utility and Wireless AP SNMP Utility have been installed you can configure settings for the access point. Before you can use the SNMP Utility, you must configure the device IP address. The IP address of the device must be on the same subnet and use the same subnet mask as the computer using the SNMP Utility.

Using the USB Configuration Utility

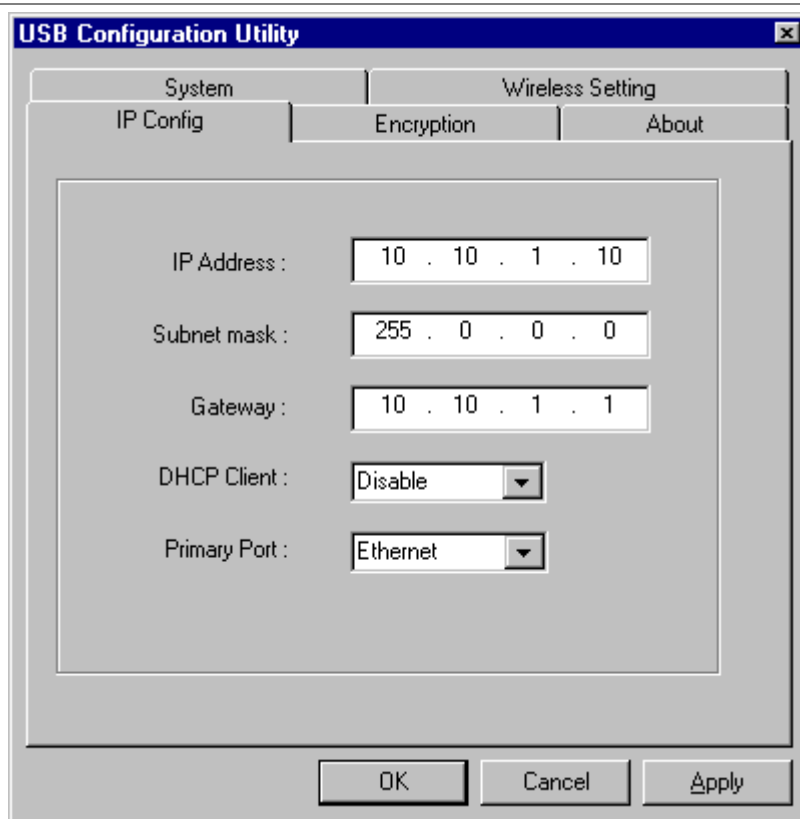
To use the USB Configuration Utility and change the IP settings of the Access Point, follow these steps:

1. To launch the USB Configuration Utility, go to your **Start** menu, open **Programs**, find the **Wireless AP** folder and open it. You will see two new icons have been placed in this folder. Scroll to the **Wireless AP USB Utility** and click on it to launch the program.
2. The **Admin Password** screen will ask you for a password. The default password is "public" (all lower case), type this in the space and click **OK**.
3. The **USB Configuration Utility** management interface will appear displaying system information about the Wireless Access Point. To access any of the menus listed just click on the tab. If you intend to use the SNMP Utility to manage and configure the device you must first change the IP settings.



4. Click the **IP Config** tab to change the IP settings of the device.

If you do not intend to use the device as an extension of or connection to a wired network, you may not need to configure IP settings. IP settings are required only if the device will be used with other network devices that use the TCP/IP suite of protocols for network functions.



5. Change the IP settings of the access point. You may elect to use a DHCP server to determine the IP settings, or set them according to the requirements of your IP addressing scheme.

To configure the device as a DHCP client, select **Enable** from the **DHCP Client:** pull-down menu.

To manually assign the IP settings, you must **Disable** the DHCP client function and set the IP address and subnet mask. If necessary, you can assign a **Gateway** IP address for the device here as well.

Finally, if you are using DHCP to assign IP settings, you must select the port used for communication with the DHCP server. Change the **Primary Port:** setting to **Ethernet** (set by default) or **Wireless**, according to how the device will receive DHCP information.

Note: If you are planning to use the Wireless AP SNMP Utility for further configuration, please skip ahead to the section about the SNMP Utility.

USB Utility Menus

If you do not plan to connect the Wireless Access Point to a wired network via the Ethernet interface you can use the Wireless AP USB Utility to configure all the settings required for wireless operation. To view any menu, click on the tab associated with it. The remaining menus useful for wireless operation are discussed here.

Wireless Setting

Use the Wireless Operation menu to set parameters that enable the Access Point to communicate with other stations on the wireless LAN.

The screenshot shows the 'USB Configuration Utility' window. It has a title bar with a close button. Below the title bar are four tabs: 'IP Config', 'Encryption', 'About', and 'Wireless Setting'. The 'Wireless Setting' tab is selected. Inside this tab, there are several input fields and buttons. The 'Access Point Name' field is empty. The 'Wireless ESSID' field is empty. The 'Operational Rate Set' is a dropdown menu set to 'Auto'. The 'Wireless Channel' is a dropdown menu set to 'Channel 3'. Below these is the 'Operational Mode' dropdown menu set to 'Access Point'. The 'Preferred BSSID' is a field with six boxes containing the values '00', '00', '22', '22', '22', and '55'. There is an 'Advanced' button to the right of the BSSID field. At the bottom of the window are three buttons: 'OK', 'Cancel', and 'Apply'.

Define these Wireless parameters:

Access Point Name: The Access Point can be assigned a name for easy reference here.

Wireless ESSID: The ESS ID is used by all wireless devices within the ESS or extended wireless LAN. This can be any alpha-numeric value of up to 32 long. Use this to prevent cross communication between two or more WLANs in one area.

Operational Rate Set: By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, or 11 Mbps. For most networks the default setting, Auto will be the best choice. When **Auto** (Rate Fall Back) is enabled the transmission rate will select the optimum rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.

Wireless Channel: There are 14 channels available for with the Access Point. All devices communicating with the device must use the same channel. There may be restrictions on which channel can be used in some countries. In Canada and the US, channels 1 - 11 are authorized for use by the IC and the FCC.

Operation Mode

Use this menu to select how the Access Point will function on your WLAN. The previous discussion of Operations Modes contains illustrated examples of the four available operation modes. Click **Apply** to put the changes into effect.

Choose one of the following from the **Operation Mode** pull-down menu:

Access Point

This mode provides access for wireless stations to a wired Ethernet LAN and from the wired LAN to the wireless stations. Furthermore, wireless stations within the range of the Access Point will communicate with each other through the device. This is the default operation mode of the Access Point.

Access Point Client

This mode can be used to connect a remote Ethernet LAN or a single station with a central LAN, to create an extended single virtual LAN. In this way, any station of the Remote LAN can successfully communicate with any station of the central LAN as if they were members of the same physical LAN. Wireless end stations can not associate with an Access Point in Client mode except by means of another access point. As a client, the Access Point must operate within a BSS and therefore must use a designated BSS base station (usually another Access Point) for all communications through its wireless interface. Use the **Preferred BSS ID** entry field to define the wireless station used to direct wireless traffic of the device.

Wireless Bridge Two types of wireless bridge connections are allowed:

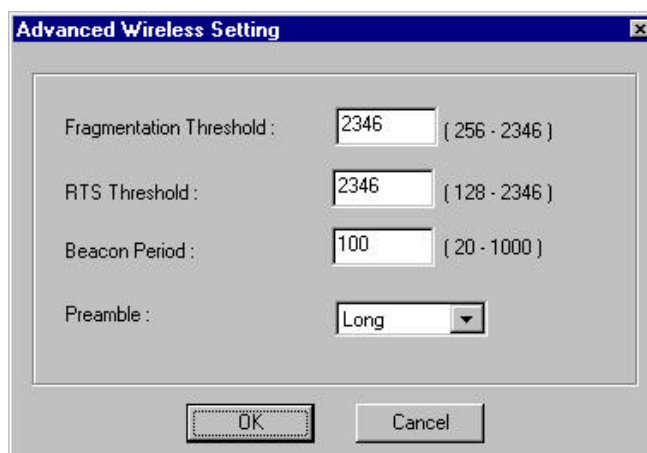
1. **Point-to-Point** The Access Point still functions as the central controller for wireless stations within its BSS, but it will only communicate with only one other wireless bridge. The designated access point with which it communicates is identified by the **Preferred BSS ID**.
2. **Point to Multipoint** The Access Point is able to communicate with any available wireless bridge on the same channel.

Advanced Wireless Operation

Click the **Advanced** button to define the parameters described below. A new window will appear. Define the following parameters:

Fragment Threshold:

Fragment Threshold defines a threshold above which the wireless packet will be split up, or fragmented. For a fragmented packet, if transmission of part of it were to be interfered with, only the portion that was successfully transmitted would need to be re-sent. Throughput will generally be lower for fragmented packets, since the fixed packet overhead consumes a higher portion of the RF bandwidth.



The image shows a dialog box titled "Advanced Wireless Setting". It contains four configuration fields:

- Fragmentation Threshold :** A text box with the value "2346" and a range indicator "(256 - 2346)".
- RTS Threshold :** A text box with the value "2346" and a range indicator "(128 - 2346)".
- Beacon Period :** A text box with the value "100" and a range indicator "(20 - 1000)".
- Preamble :** A dropdown menu currently set to "Long".

At the bottom of the dialog are two buttons: "OK" and "Cancel".

RTS Threshold: The RTS Threshold sets an upper threshold at which point the device will issue an RTS packet. The RTS (Request To Send) packet is used for the purpose of avoiding data collisions on the wireless LAN. There are several trade offs to consider when setting this parameter. Setting this parameter to a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of other network packets. However, the more often RTS packets are sent, the quicker the system can recover from interference or collisions. Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.

Beacon Period: The Beacon Period specifies the duration between beacon packets in milliseconds. The range for the beacon period is between the ranges of 20 to 1000 with a typical value of 100.

Encryption

If an additional measure of security is desired on the wireless network, WEP (Wired Equivalent Privacy) encryption can be enabled. WEP encrypts each frame transmitted from the wireless adapter using one of the keys entered in the **WEP Privacy** field. The Access Point or wireless adapter will accept only encrypted frames that it can decrypt correctly. Decrypting can take place only if the receiver has the correct key used by the transmitter.

The screenshot shows the 'USB Configuration Utility' window with the 'Wireless Setting' tab selected. The 'Encryption' sub-tab is active. The 'WEP Type' is set to 'Disable', 'Active Key ID' is 'None', and 'Authentication Type' is 'Open System'. Below these are sections for 64 bit and 128 bit keys. The 64 bit section shows four keys (Key1, Key2, Key3, Key4) each with five '00' values. The 128 bit section shows four keys (Key1, Key2, Key3, Key4) each with thirteen '11' or '22' or '33' or '44' values. At the bottom are OK, Cancel, and Apply buttons.

WEP Type: The 64 or 128-bits Wired Equivalent Privacy Algorithm. Use this enable 64-bit or 128-bit encryption. WEP is disabled by default.

Active Key: Active Key ID determines which Key (Key 1 to Key 4) encrypts and decrypts the transmitting and received by the Access Point.

Authentication Type: Choose Open System, Shared Key or Both.

Open System: With this setting any station in the Wireless LAN can associate with an

Access Point to receive and to transmit data.

Shared Key: With this setting only stations using a shared key encryption identified by the Access Point are allowed to associate with it.

Both: With this setting stations can communicate with or without data encryption.

Key 1 - Key 4

64 bit: Active Key ID 1 to 4. These values can only be edited if a WEP type is selected to 64-bits.

128 bit: Active Key ID 1 to 4. These values can only be edited if a WEP type is selected to 128-bits.

These four fields can be used to manually enter the encryption keys. This may be necessary if you wish this node to match keys in a different vendor's product. These fields also display the keys when they are generated using a Pass-phrase.

NOTE: 64 bit WEP is the same as 40 bit WEP! The lower level of WEP encryption uses a 40 bit (10 character) “secret key” (set by the user), and a 24 bit “Initialization Vector” (not under user control). The panel allows the entry of four keys for 64-bit encryption and one set for 128-bit key encryption. Each key must consist of hex digits, which means that only digits 0-9 and letters A-F are valid entries. The Configuration Utility will not apply keys that are not entered correctly.

Click **Apply** to set Encryption code settings.

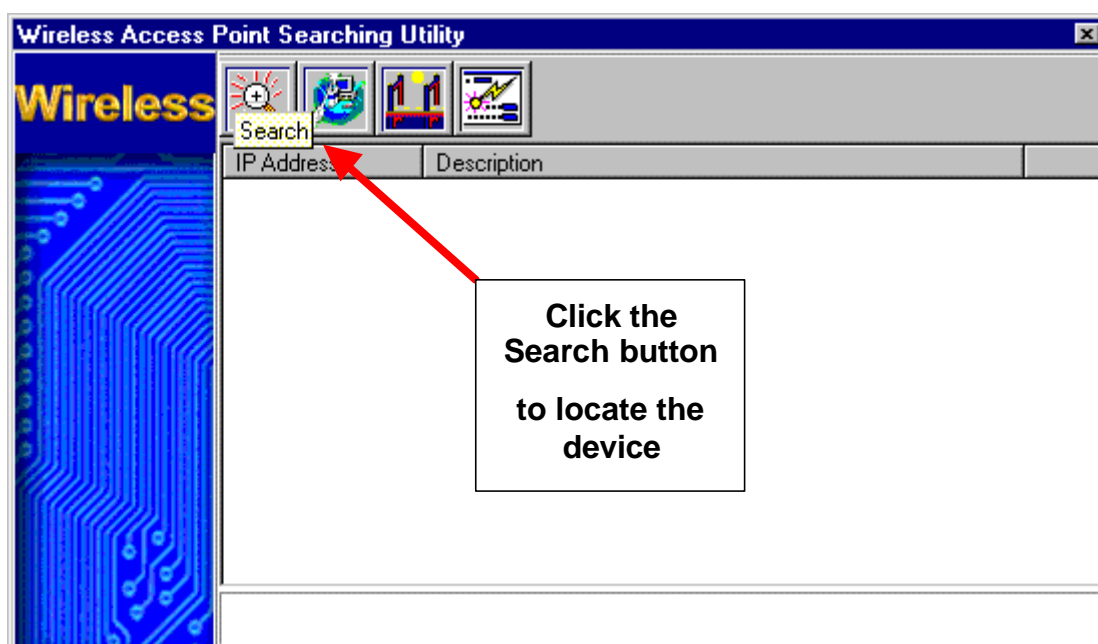
Using the SNMP Management Utility

Now that you have installed the Wireless Access Point SNMP Utility on your computer and configured the IP settings of the Access Point, you can configure the remaining settings to suit the needs of your network. The USB Configuration Utility contains the same menu options as the SNMP Utility. The settings menus are described in this section.

Accessing the SNMP Manager

Follow these steps to access the Wireless Access Point manager on the from the manager PC:

1. From the Start menu, Start > Programs > Wireless AP > Wireless AP SNMP Utility
2. A new screen, the Wireless Access Point Searching Utility, will appear. If the device does not appear listed in the screen, click the Search button. The Search button is the magnifying glass icon.



3. Double click on the device in the list you wish to configure. You will be prompted for a password in a new screen, the **Admin. Authorization Password** window. Type in the default password “public” and click **OK**.



4. The Wireless Access Point Configuration Utility menu will appear displaying the System tab.

You may now use any of the management functions available in the SNMP Configuration Utility.

SNMP Utility Menus

Click on the appropriate tab to access any menu in the Wireless Access Point SNMP Configuration Utility.

The screenshot displays the 'Wireless Access Point SNMP Utility : 10.41.44.9' window. It features a tabbed interface with 'System', 'IP Config', 'Statics', 'Wireless Operation', 'Encryption', and 'About'. The 'System' tab is active, showing 'System Reset' and 'Load Default' buttons. Below these is the 'Device Information' section with fields for 'Description' (802.11 AP (Ver. 1.4f.8)), 'Mac Address' (00055DF896B1), and 'Regulation Domain' (MKK1). Further down are 'Trap Enable', 'User Auth.', and 'Admin. Auth.' tabs. The 'Trap Enable' tab is selected, showing a checked checkbox for 'Trap Enabled' and an 'Apply' button. A 'Refresh' button is located at the bottom of the main content area. A status bar at the very bottom shows a message: 'Get:Ok!.Request:Trap Enable.Received at 03:05:05 PM.'

System

The System menu will appear whenever the SNMP Configuration Utility is first accessed or you can click on the System tab at any time to view the menu. The System menu lists the following:

System Reset

Clicking the System Reset button will reset the device and initiate any changes that have been made to the device configuration settings. Configuration settings are saved to Non-volatile RAM (NV-RAM). This should be the last thing you do when you are ready to exit the Configuration Utility.

Load Default

Clicking this button will load the factory default configuration settings into the NV-RAM of the device.

Device Information

Device information includes basic information about the Access Point including the name of the device, the firmware version currently being used, the MAC address and the regulation domain in which it resides.

Trap Enable

Use this to Enabled or Disabled SNMP traps.

User Authorized Setting

Use this to create user accounts identified by unique user names and passwords that allow read-only access to the SNMP Utility.

Admin Authorized Setting

Use this to create administrator accounts for administrator access to the SNMP Utility. Administrator privileges allow full read-write access to the SNMP Utility.

IP Configuration

Use this menu to view, set or change IP settings. You can set them manually or allow a DHCP server to assign IP settings.

Listed in the Bridging Level information field are the following:

MAC Address

Unique 48-bit, hard-coded Media Access Control address used to identify devices on the WLAN and Ethernet LAN.

IP Settings

You may change any of the IP settings by simply typing in the desired address or net mask. Click **Apply** to put the changes into effect. Remember that if you change the IP address of the device to an address that is outside the subnet of the computer you are using, you will lose access to the SNMP Utility

IP Address

Internet Protocol address of the Access Point.

Subnet mask

Four sets of three digits used to logically divide an IP network into sub-networks.

Gateway

IP address of a gateway device necessary for communication with devices outside the subnet of the Access Point. If your network is not divided into different subnets, this can remain blank.

DHCP

The Access Point can be configured as a DHCP client by choosing **Enabled** in the **DHCP enable** pull-down menu. By default DHCP support is Disabled.

If the Access Point is configured as a DHCP client, it will be necessary to decide what media will be used to transport DHCP information to the device. By default the Access Point is configured to receive IP settings from through the Ethernet port. If your network is set up so that DHCP services are supplied through the wireless LAN, you must change the **Primary port:** setting to Wireless in the pull-down menu and click **Apply** to put the change into effect.

Click **Refresh** to refresh the screen to list the most current settings.

Statistics

Various statistics concerning both Ethernet and wireless operation of the Access Point can be viewed in the Statistics window. This window can be useful for monitoring performance and diagnosing problems associated with the device or its BSS.

Wireless Access Point SNMP Utility : 10.41.44.9

System | IP Config | **Statistics** | Wireless Operation | Encryption | About

Ethernet | **Wireless**

Rx Item	Value	Tx Items	Value
TotalBytesRx	903186152	TotalBytesTx	41025
TotalPktRx	2998099	TotalPackets	296
CRCErrRx	0	CRCErr	0
Multicast	491784	Multicast	0
Broadcast	967560	Broadcast	24
ControlFrames	1	Unicast	272
PauseFrames	0	PauseFrames	0
UnknownOPC	1	SingleDefer	24
AlignmentErr	0	MultiDefer	0
OutOfRange	165004	SingleCollisions	10
CodeErrorRx	0	MultiCollisions	7
FalseCarrierRx	0	LateCollisions	0
Undersize	0	Excessive	3
Oversize	0	TotalCollisions	47
TotalFragments	0		
TotalJabber	0		

Message Get:Ok!.Request:Ethernet Packet.Received at 04:02:00 PM.

Wireless Access Point SNMP Utility : 10.41.44.9

System | IP Config | **Statistics** | Wireless Operation | Encryption | About

Ethernet | **Wireless**

Rx Item	Value	Tx Items	Value
Unicast	192	Unicast	95
Broadcast	848623	Broadcast	825427
Multicast	0	Multicast	366896
RxB Beacon	0	TxB Beacon	236330
RxACK	72	TxACK	96
RxRTS	0	TxRTS	0
RxCTS	0	TxCTS	0

Message Get:Ok!.Request:Wireless Packet.Received at 04:04:24 PM.

Wireless Operation

Use the Wireless Operation menu to set parameters that enable the Access Point to communicate with other stations on the wireless LAN.

The screenshot shows the 'Wireless Access Point SNMP Utility : 10.41.44.9' window. It has tabs for System, IP Config, Statics, Wireless Operation (selected), Encryption, and About. The Wireless Operation tab contains the following fields and controls:

- Channel ID: A dropdown menu showing 'Channel 3'.
- ESSID: An empty text input field.
- Access Point Name: An empty text input field.
- Transmit Rates: A dropdown menu showing 'Auto'.
- Operation Mode section:
 - Mode: A dropdown menu showing 'AP'.
 - BSS ID: A text input field containing '000022222255'.
- An 'Advance...' button on the right side.
- 'Refresh' and 'Apply' buttons at the bottom.
- A status bar at the very bottom with the message: 'Message Get:Ok!.Request:Wireless Group.Received at 04:09:00 PM.'

Define these Wireless parameters:

Channel ID:

There are 14 channels available for with the Access Point. All devices communicating with the device must use the same channel. There may be restrictions on which channel can be used in some countries. In Canada and the US, channels 1 - 11 are authorized for use by the IC and the FCC.

ESSID:

The ESS ID is used by all wireless devices within the ESS or extended wireless LAN. This can be any alpha-numeric value of up to 32 long. Use this to prevent cross communication between two or more WLANs in one area.

Access Point Name:

The Access Point can be assigned a name for easy reference here.

Transmit Rate:

By default the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, or 11 Mbps. For most networks the default setting, Auto will be the best choice. When **Auto** (Rate Fall Back) is enabled the transmission rate will select the optimum rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.

Operation Mode

Use this menu to select how the Access Point will function on your WLAN. The previous discussion of Operations Modes contains illustrated examples of the four available operation modes. Click **Apply** to put the changes into effect.

Mode: Choose one of the following:

Access Point:

This mode provides access for wireless stations to a wired Ethernet LAN and from the wired LAN to the wireless stations. Furthermore, wireless stations within the range of the Access Point will communicate with each other through the device. This is the default operation mode of the Access Point.

Access Point Client:

This mode can be used to connect a remote Ethernet LAN or a single station with a central LAN, to create an extended single virtual LAN. In this way, any station of the Remote LAN can successfully communicate with any station of the central LAN as if they were members of the same physical LAN. Wireless end stations can not associate with an Access Point in Client mode except by means of another access point. As a client, the Access Point must operate within a BSS and therefore must use a designated BSS base station (usually another Access Point) for all communications through its wireless interface. Use the **BSS ID:** entry field to define the wireless station used to direct wireless traffic of the device.

Wireless Bridge: Two types of wireless bridge connections are allowed:

3. **Point-to-Point:** The Access Point still functions as the central controller for wireless stations within its BSS, but it will only communicate with only one other wireless bridge. The designated access point with which it communicates is identified by the **BSS ID**.
4. **Point to Multipoint:** The Access Point is able to communicate with any available wireless bridge on the same channel.

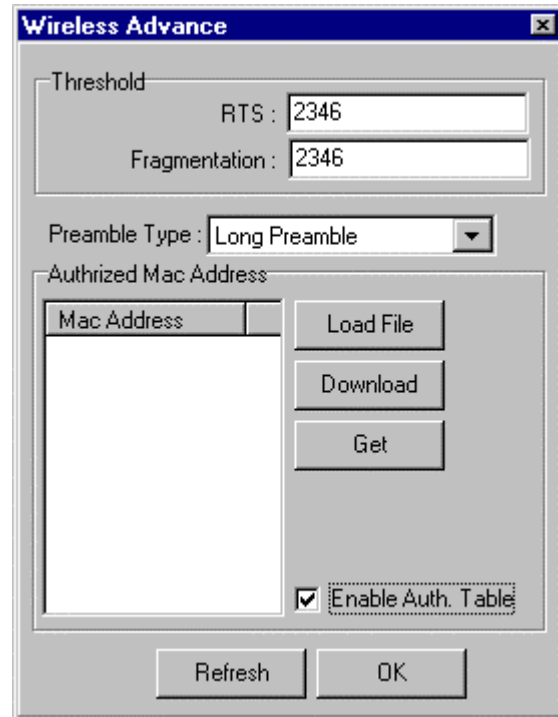
Advanced Wireless Operation

Click the **Advanced** button to define the parameters described below. A new window will appear.

In the **Threshold** field define the following parameters:

RTS:

The RTS Threshold sets an upper threshold at which point the device will issue an RTS packet. The RTS (Request To Send) packet is used for the purpose of avoiding data collisions on the wireless LAN. There are several trade offs to consider when setting this parameter. Setting this parameter to a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of other network packets. However, the more often RTS packets are sent, the quicker the system can recover from interference or collisions. Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.

A screenshot of the 'Wireless Advance' configuration window. The window has a title bar with the text 'Wireless Advance' and a close button. Inside, there are several sections. The 'Threshold' section contains two input fields: 'RTS : 2346' and 'Fragmentation : 2346'. Below this is a 'Preamble Type' dropdown menu set to 'Long Preamble'. The 'Authorized Mac Address' section features a table with a header 'Mac Address' and an empty body. To the right of the table are three buttons: 'Load File', 'Download', and 'Get'. Below the table is a checkbox labeled 'Enable Auth. Table' which is checked. At the bottom of the window are two buttons: 'Refresh' and 'OK'.

Fragment Threshold:

Fragment Threshold defines a threshold above which the wireless packet will be split up, or fragmented. For a fragmented packet, if transmission of part of it were to be interfered with, only the portion that was successfully transmitted would need to be re-sent. Throughput will generally be lower for fragmented packets, since the fixed packet overhead consumes a higher portion of the RF bandwidth.

Preamble Type:

Preamble is the first sub-field of PPDU, which is the appropriate frame format for transmission to PHY (Physical layer). There are two options, **Short Preamble** and **Long Preamble**. The Short Preamble option improves throughput performance.

Authorized MAC Address

For security purposes the Access Point can discriminate its associations with other wireless stations. The Authorized MAC Address lets you select which stations are allowed throughput on the wireless interface. First you must enable the MAC address authorization table by checking the Enable Auth. Table box. When you want to leave this menu click **OK** to use the table. The table is maintained manually and can be updated and edited by downloading MAC addresses to the data table. This is described below.

You can supply a list of authorized MAC addresses to the Access Point. Perform the following tasks:

1. Click the **Load file:** button and enter the file name and location of the file you want to load. The file should contain the MAC addresses you wish to add to the table of authorized addresses. The file should be a simple text document with each MAC address written on a separate line.
2. Once the file has been loaded, click the **Download:** button to download the Authorized MAC Address file to the Access Point.

Click on the **Get:** to obtain a list of the Authorized MAC Addresses currently entered on the table.

Encryption

If an additional measure of security is desired on the wireless network, WEP (Wired Equivalent Privacy) encryption can be enabled. WEP encrypts each frame transmitted from the wireless adapter using one of the keys entered in the **WEP Privacy** field. The Access Point or wireless adapter will accept only encrypted frames that it can decrypt correctly. Decrypting can take place only if the receiver has the correct key used by the transmitter.

The screenshot shows the 'Encryption' tab of the 'Wireless Access Point SNMP Utility : 10.41.44.9' window. The 'WEP Privacy' section contains three dropdown menus: 'Active Key' set to 'None', 'WEP Type' set to 'Disable', and 'Authentication Type' set to 'Open System'. Below these are four rows of key input fields, labeled 'Key 1' through 'Key 4', each containing 12 hexadecimal digits (all currently '00'). At the bottom are 'Refresh' and 'Apply' buttons. A message bar at the very bottom displays the text: 'Message Get:Ok!.Request:Privacy Group.Received at 04:24:53 PM.'

Active Key: Active Key ID determines which Key (Key 1 to Key 4) encrypts and decrypts the transmitting and received by the Access Point.

WEP Type: The 64 or 128-bits Wired Equivalent Privacy Algorithm. Use this enable 64-bit or 128-bit encryption. WEP is disabled by default.

Authentication Type: Choose Open System, Shared Key or Both.

Open System: With this setting any station in the Wireless LAN can associate with an Access Point to receive and to transmit data.

Shared Key: With this setting only stations using a shared key encryption identified by the Access Point are allowed to associate with it.

Both: With this setting stations can communicate with or without data encryption.

Key 1 - Key 4

64 bit: Active Key ID 1 to 4. These values can only be edited if a WEP type is selected to 64-bits.

128 bit: Active Key ID 1 to 4. These values can only be edited if a WEP type is selected to 128-bits.

These four fields can be used to manually enter the encryption keys. This may be necessary if you wish this node to match keys in a different vendor's product. These fields also display the keys when they are generated using a Pass-phrase.

NOTE: 64 bit WEP is the same as 40 bit WEP! The lower level of WEP encryption uses a 40 bit (10 character) "secret key" (set by the user), and a 24 bit "Initialization Vector" (not under user control). The panel allows the entry of four keys for 64-bit encryption and one set for 128-bit key encryption. Each key must consist of hex digits, which means that only digits 0-9 and letters A-F are valid entries. The Configuration Utility will not apply keys that are not entered correctly.

About

About tab displays general information about SNMP Manager. This screen also displays the software version of SNMP Manager and the firmware version of the Wireless Access Point.

