

Wireless LAN Access Point

User Guide

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 64C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When nearby persons has to be kept to ensure RF exposure compliance, in order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 20 cm.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

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

Export restrictions

This product or software contains encryption code that may not be exported or transferred from the US of Canada without an approved US Department of Commerce export license.

Safety Statements

Federal Communications Commission Statement

This device complies with FCC Rules Part 15. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Safety Information

Your device contains a low power transmitter. When device is transmitted it sends out radio frequency (RF) signal.

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

TABLE OF CONTENT

About This Guide.....	1
Purpose.....	1
Overview of this User's Guide.....	1
Unpacking and Setup	3
Unpacking	3
Setup	3
Hardware Instalation	5
Front View	5
Rear Panel	6
Hardware connections.....	7
Connect to the Switch/Hub	7
Check the installation.....	7
Configuring the Wireless LAN Access Point	9
Installing the AP Utility and SNMP Manager	9
Configuring through the AP Utility	10
Configuring through the SNMP Manager.....	13
Technical Specifications	27

ABOUT THIS GUIDE

Congratulations on your purchase of this IEEE 802.11b Wireless LAN Access Point. This manual helps to features the innovating wireless technology that can help you build a wireless network easily! This manual contains detailed instructions in operation of this product. Please keep this manual for future reference.

With a WLAN (IEEE 802.11b) Access Point, a mobile computer can share data with another mobile computer in a wireless way. Easy-to-use utilities are bundled with WLAN Access Point for configuration and monitoring purposes.

WLAN networking can wirelessly transmit and receive data, minimizing the need for wired connections, at a speed of up to eleven megabit per second. With WLAN networking, you can locate your PC wherever you want without wires and cables.

WLAN networking provides users with an access to real-time information anywhere in their organization. The mobility provides productivity and service, which are not available under wired networks.

Purpose

This manual discusses how to install the WLAN Access Point.

Overview of this User's Guide

Introduction. Describes the WLAN Access Point and its features.

Unpacking and Setup. Helps you get started with the basic installation of the WLAN Access Point.

Hardware Installation. Describes the LED indicators of the AP.

Software Installation. Tells how to setup the driver and the utility setting.

Technical Specifications. Lists the technical (general, physical and environmental) specifications of the WLAN Access Point.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Access Point.

Unpacking

Open the box of the Access Point and carefully unpack it. The box should contain the following items:

- ◆ One Wireless Access Point
- ◆ One external power adapter
- ◆ One USB cable (A type to B type)
- ◆ One Installation CD (Driver & Utility + User's guide)
- ◆ One Quick Installation Guide
- ◆ Two SMA reverse type antenna (2dBi) (for optional external antenna of WLAN Access Point)

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the WLAN Access Point can be performed using the following steps:

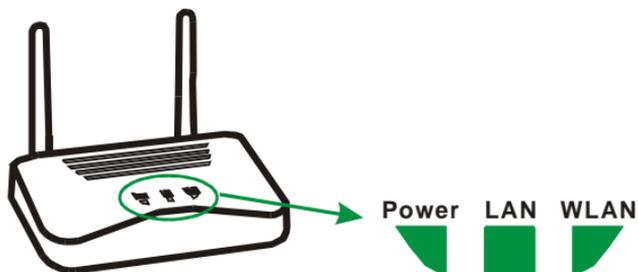
- ◆ Locate an optimum location for the Wireless LAN Access Point (AP). The best place for your AP is usually the center of your wireless network, with line of sight to all of your mobile stations.
 - ◆ Visually inspect the USB or Ethernet RJ45 port connector and make sure that it is fully plugged in to the system's USB port or Ethernet switch/hub port.
-

- ◆ Fix the direction of the antennas. Try to place the AP in a position that 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.
- ◆ Visually inspect if the Power Adaptor was fully plugged to the device power jack.

HARDWARE INSTALATION

Front View

The figure below shows the front view of the WLAN Access Point.



Front View

POWER

This indicator lights green when the Access Point receives power. Otherwise, it turns off.

LAN (Link/ACT)

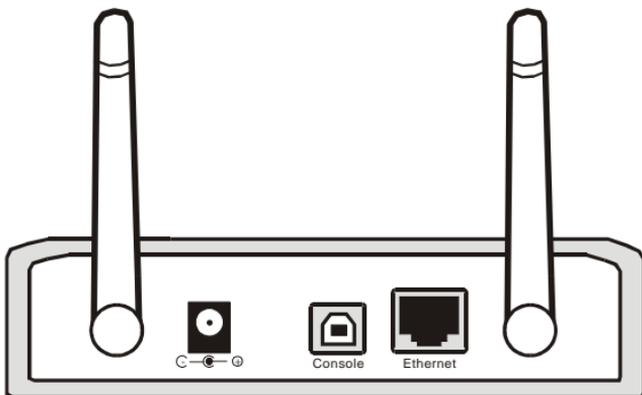
The indicator lights green when the LAN port is connected to a 10Mbps Ethernet station, the indicator blinks green while transmitting or receiving data on the 10Mbps Ethernet network.

WLAN (Link)

The indicator blinks green when the wireless station connected to the AP, the AP is always transmitting or receiving data once a wireless device is connected, otherwise, the light turns off.

Rear Panel

The figure below shows the rear panel of the Access Point



Rear Panel

Ethernet

Ethernet uplink port with auto-sensing for connecting to either 10Mbps Ethernet connections, connect this port to switch/hub.

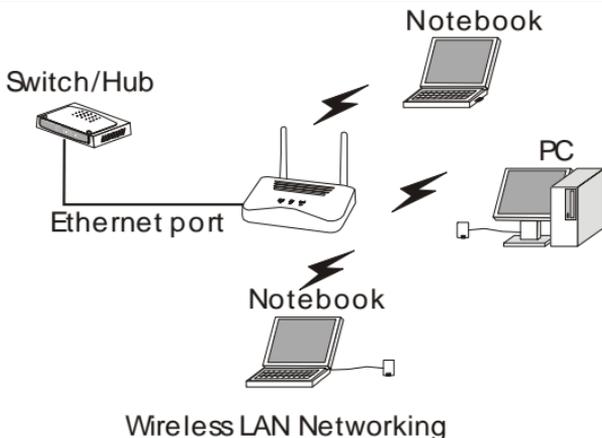
Console

The Console port is using USB “B” type connector, through this port, you can manage your Access Point by using AP utility.

DC Power

Connect the AC Power Adapter to the AP’s power jack.

Hardware connections



Connect to the Switch/Hub

1. Plug in one end of the RJ45 network cable to the Switch/Hub port,
2. Plug in the other end of the RJ45 network cable to the Wireless Access Point.

Check the installation

The control LEDs of the Access Point are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected, the Power, LAN and WLAN port link LEDs of the Internet Broadband Router will light up indicating a normal status.
2. If the LAN Port's Link indicator does not light up then check the RJ-45 cable if it is firmly feed to the RJ45 port, while the LAN is link up to the Switch/Hub, the LAN port's LED will light up.

CONFIGURING THE WIRELESS LAN ACCESS POINT

There are two ways to configure the Wireless Access Point, configuring through AP utility and SNMP Manager.

Installing the AP Utility and SNMP Manager

The AP Utility and SNMP Manager will help you to configure the Wireless LAN Access Point through the USB port or Ethernet port.

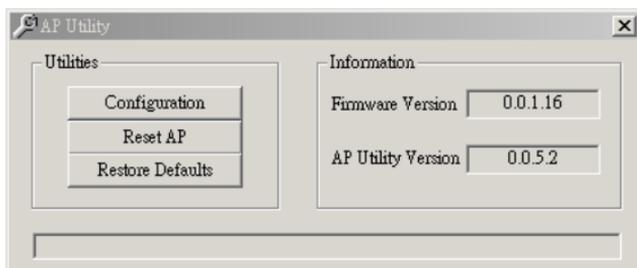
Note: Please configure through AP Utility before you start using the device. When the AP is connected to the USB port, the operating system will search the driver when detecting the device. Put the driver CD into your CD-ROM, the installation will start automatically. Afterwards, configure through the AP Utility to get the AP started.

1. Power on your computer and allow Window 98/Me/2000/XP to load fully. Be sure that there is no AP connected to the computer at this stage.
2. Insert the driver CD into the CD-ROM and it will execute the installation program automatically or refer to the "D:\Setup.exe" in the dialog box (D:\ will depends on where the CD-ROM drive is located). Follow the instruction of the instruction step by step.
3. At last, a message will notify you to restart your computer. Select "Yes" to restart your computer.

Configuring through the AP Utility

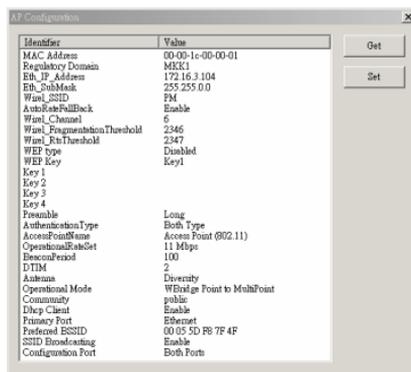
The AP Utility helps you configure the Wireless LAN Access Point through the USB port.

On the Windows Start Menu Program 802.11 Wireless LAN Access Point Utility, choose the AP Utility, and the following dialog box will appear.



AP Utility Main Menu

1. Click the “Configuration” and the Configuration dialog will pop up.



Configuration

2. You may double click the value parameter on the right side as shown in the figure for advanced settings; some Identifier's value may not be modified and some value will be in a range that to shown in the dialog box.
 - ◆ MAC Address: showing the MAC ID of the device.
 - ◆ Regulatory Domain: showing the domain code of the device.
 - ◆ Eth_IP Address: to set the IP address used by the AP.
 - ◆ Eth_Submask: to set the subnet address.
 - ◆ Wirel_SSID: to set the SSID of the Access Point.
 - ◆ Auto Rate Fallback: to enable or disable the transfer rate auto fallback.
 - ◆ Wirel_Channel: to set the channel of the Access Point.
 - ◆ Wirel_Fragmentation Threshold: the size at which packets will be fragmented. Choose a setting within a range of 256 to 2346 bytes.
 - ◆ Wirel_RTS Threshold: Choose a setting within a range of 0 to 2432 bytes. It is recommended limiting a long packet to prevent each station waiting too long to transmit a data.
 - ◆ WEP type: to set WEP to be 64 bit, 128 bit or no encryption.
 - ◆ WEP key: to select which WEP key to be used.
 - ◆ Key 1 ~ 4: to input the WEP key parameter from key 1 to key 4
 - ◆ Preamble: to limit the packet size of the data to transmit. It is recommended to choose the short preamble when the link quality is bad.
 - ◆ Authentication type: to choose which authentication algorithm will be used, open system, shared key or both type.
 - ◆ Access Point name: to appoint a name for the device.

- ◆ Operational Rate Set: to select the transfer rate from 11, 5.5, 2 and 1Mbps.
 - ◆ Beacon Period: to select the time of beacon signal from 20-1000 (Typical 100 millisecond).
 - ◆ DTIM: Set the DTIM period. Determines at which interval the AP will send its broadcast traffic. Default value is 4 beacons.
 - ◆ Antenna: to determine which antennas are used, Left, Right or Diversity.
 - ◆ Operational mode: Set one of the following operational modes on the AP: Access Point / Access Point Client / Wireless Bridge / Wireless Repeater.
 - ◆ Community: to assign the community's password. The default password is "public".
 - ◆ DHCP Client: Enable/Disable automatic IP address assignment by the DHCP server
 - ◆ Primary Port: The interface to determine the DHCP server (Ethernet Port/ Wireless Port) Authorization Algorithm.
 - ◆ Preferred BSSID: Remote MAC Address for connection, in Access Point Client or Wireless Bridge Operational modes.
 - ◆ SSID Broadcasting: to enable / disable the SSID ID of the device.
 - ◆ Configuration Port: to select where the device can be configure, USB or Ethernet.
 - ◆ Press "GET" button to display the current setting of the AP.
 - ◆ Press "SET" button to set the new setting of the AP.
3. Press "RESET AP" to reset the device.
 4. Press "Restore Default" to set the default setting back on the device.

5. In the information dialog box, it will display out the firmware version and the utility software version.

Configuring through the SNMP Manager

The Access Point SNMP Manager is provided to manage the Wireless LAN Access Point through Ethernet.

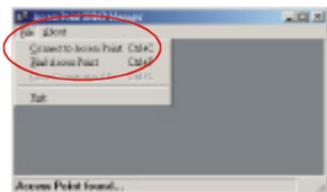
Note: Before using the SNMP manager to configure the AP, please check with your network administrator to have enough information for the setting.

1. On the Windows Start Menu Program 802.11 Wireless LAN Access Point Utility, choose the SNMP Manager and the following windows will pop up.



SNMP Manager

2. On the Task Manager, select “File Find Access Point” to find the Access Point.



The submenu allows you to find and connect to the AP without knowing its IP address. Choose this submenu in order to find the AP and click “Connect”. Window appears indicating the IP Address of the selected AP and prompting you select Authority and appropriate password at the community field. Then click “OK”, the default appropriate password is “public”.



➤ File Menu:

The file menu contains the following enabled submenus:

- 1.) Close Connection AP: Terminates the connection with the AP.
- 2.) Exit: Terminates the connection with the AP and exits the SNMP Manager.

➤ Setup Menu:

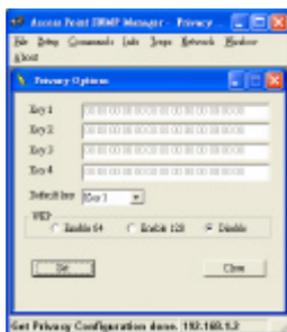
As soon as the connection has been established, you are able to start viewing or setting the AP parameters.

- 1.) Bridge: Under this submenu, there is IP configuration option.
 - **IP Configuration:** In this window you can see and change the IP Address and IP Mask of the AP.

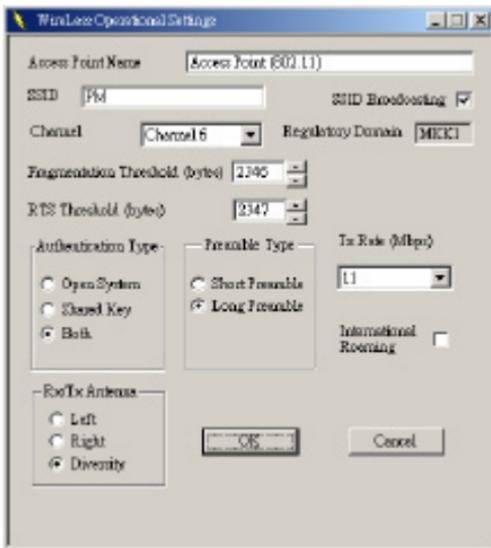


This option enables / disables the DHCP client function of the AP. Additionally you have to select the Primary Port, which is the interface that determines the DHCP server. You can also choose to use either Ethernet and/or Wireless port for the AP configuration.

- 2.) Wireless LAN: In this submenu, you can configure the Privacy Options, AP Operational Setting and Authorized MAC Address.
- Privacy Options: This function is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network, and it can be achieved by using the Encryption function.
 - ◆ **Key1 ~ Key4:** You can type the key that you want to use from Key#1 to Key #4, and the key that you type will be the encryption between the station that you connected with.
 - ◆ **Default Key:** Select the default key that you need to communicate between your wireless stations.
 - ◆ **WEP:** If you select 64bit, you must type 10 values in the following range (0~F, hexadecimal) on Key 1 to 4. Besides, if you select 128bit, you must type 26 values (0~F, hexadecimal) on Key 1 to 4.



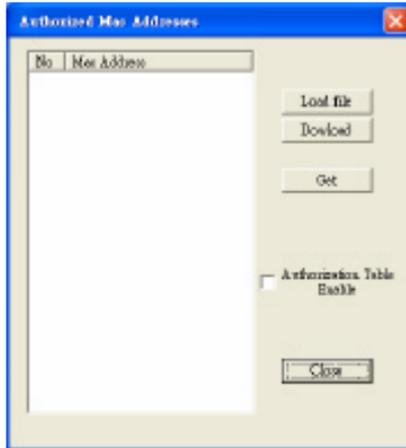
- **Operational Settings:** In this submenu, you can select to configure the advance feature of the Access Point.



- ◆ **Access Point Name:** appoint a name for the AP.
- ◆ **SSID:** It is an ASCII string up to 32 characters used to identify a WLAN that prevents the unintentional merging of two co-located WLANs. The SSID value must be the same in all stations and AP in the extended WLAN.
- ◆ **SSID Broadcasting:** When checked this item, the AP broadcasts the SSID to the stations, if not, the stations must know the AP SSID in advance.
- ◆ **Channel:** There are 14 channels available. The channels differ from country to country. Select the channel to be used.
- ◆ **Regulatory Domain:** To display where your AP is set the domain.

- ◆ **Fragmentation Threshold:** the size at which packets will be fragmented. Choose a setting within a range of 256 to 2346 bytes.
- ◆ **RTS Threshold:** Choose a setting within a range of 0 to 2432 bytes. It is recommended limiting a long packet to prevent each station waiting too long to transmit a data.
- ◆ **Authentication type:** to choose which authentication algorithm will be used, open system, shared key or both type.
- ◆ **Preamble type:** to limit the packet size of the data to transmit. It is recommended to choose the short preamble when the link quality is bad.
- ◆ **TX Rate:** to select the transfer rate from 11, 5.5, 2 and 1Mbps.
- ◆ **International Roaming:** When enable the International Roaming function, it allows users of the AP to travel to a foreign country to use their channels.
- ◆ **RX/TX Antenna:** to determine which antennas are used, Left, Right or Diversity.

- **Authorized MAC Address:** For security reasons the AP can use the Authorization Table option. The AP allows only authorized stations to get associated to it. Under the Authorized MAC Address option you may press the following buttons:

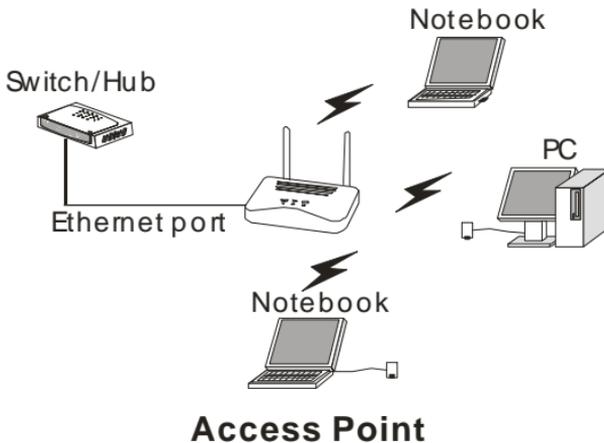


- ◆ **Load File:** Use this button in order to load a txt file with the MAC Addresses that can be associated with the AP (Authorized MAC Addresses). The txt file must have one MAC address at a line and with the following format: 000425000146, not 00-04-25-00-01-46 or 00 04 25 00 01 46.
- ◆ **Download:** Use this button in order to download the Authorized MAC Address to the AP.
- ◆ **Get:** Use this button in order to get from the AP the Authorized MAC Addresses.
- ◆ **Authorization Table Enable:** If this option is enabled, the AP allows only authorized stations to get associated to it.

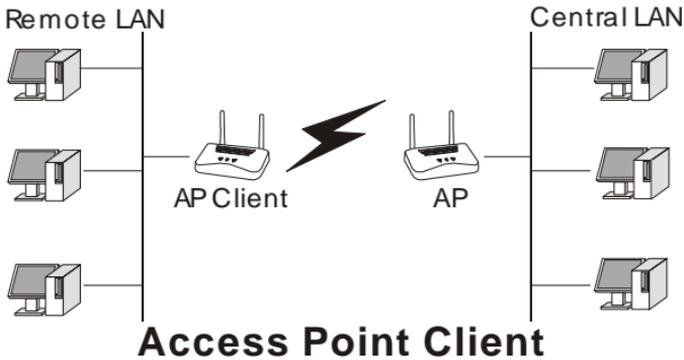
- 3.) Operation mode: The following four operational modes are available. For each mode you can either view or modify the Wireless LAN parameters of the Wireless Operational Settings window:



- ◆ **Access Point:** to set the device to Access Point operational mode.



- ◆ **Access Point Client:** This mode allows one or more remote LANs connect with a central LAN, and thus creating an extended virtual LAN. In this way, any station of the Remote LAN can successfully communicate with any station of the central LAN, as if all of them belong to the same physical LAN. Wireless Stations can't associate with AP Clients. The AP conducts the designated traffic to the appropriate wired or wireless station.
- **Preferred BSS** - It is enabled if you select the AP Client option. BSS corresponds to the MAC Address of the desired AP.

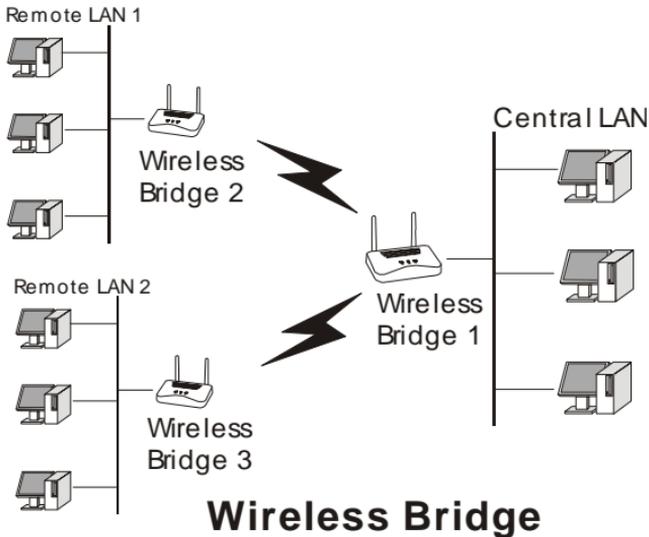


- ◆ **Wireless Bridge:** This mode enables a wireless connection between two or more Wired LANs. Two types of connections are possible:

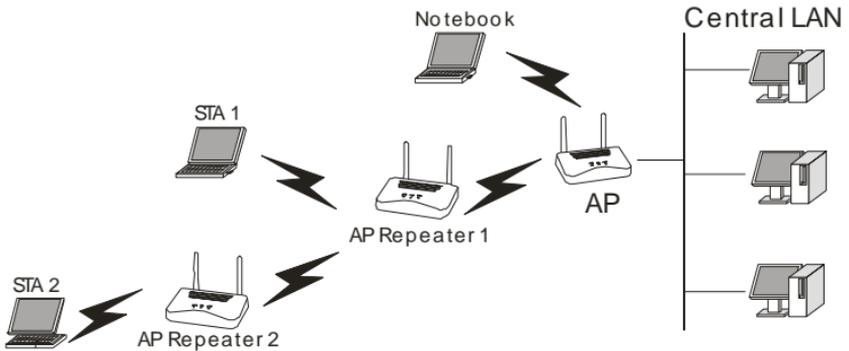
- **Point to Point** - The Wireless Bridge can communicate with a Wireless Bridge having the MAC address specified in the remote MAC address field.

**Remote MAC Address:* It is enabled if you select “Point to Point” option. It corresponds to the MAC Address of the Wireless Bridge of the Remote LAN.

- **Point to Multipoint** - The Wireless Bridge can communicate with a Wireless Bridge having the MAC address specified in the remote MAC address field.



- ◆ **Wireless Repeater:** This mode is used in order to increase the coverage area of an ESS. The Wireless Repeater starts acting as an AP after it has associated itself with another AP (Parent AP). From that point on, STAs can get associated to it and the user can configure the device with the utilities available (SNMP Manager, AP Utility).

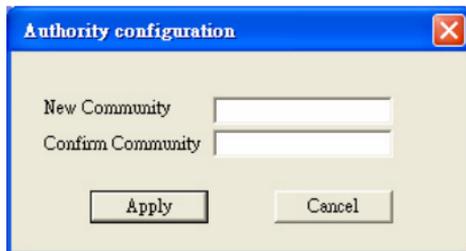


Wireless Repeater

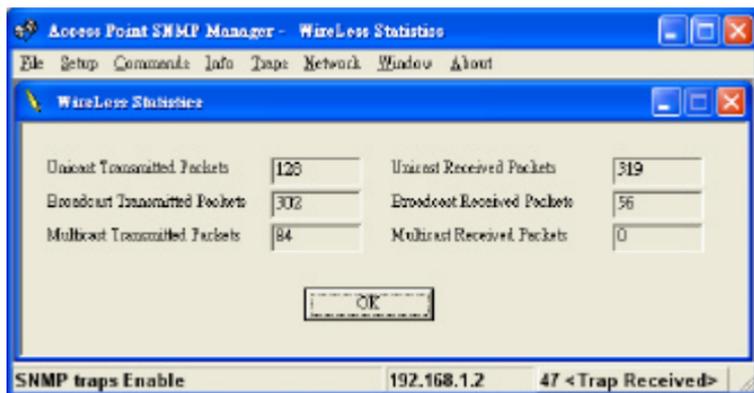
The AP Repeater can be configured with the AP RFMD Configuration through the wireless STAs associated to it or the PCs in the Wired LAN behind the Parent AP.

Note: **When using the Repeater Mode, the Ethernet port will not be activated.*

- 4.) **Enable SNMP Traps:** Using this option you can either enable or disable SNMP traps which are messages displayed in the right bottom corner of the main window indicating that an action related to the AP took place. Permitted messages are:
- **Trap Re-association:** This trap message is sent when a station's re-association request is received from the AP-Bridge.
 - **Trap Association:** Indicates the reception of an association request packet.
 - **Trap Disassociation:** This trap message is sent when a disassociation notification packet is received from a station.
 - **Trap Reset:** This trap message is sent when the AP resets.
 - **Trap Setting IP Address with Ping:** This trap message is sent when the AP-Bridge IP Address is set with the transmission of a ping message.
 - **Trap Start Up:** This trap message is sent when the AP starts up.
- 5.) **Authorization:** Using this option the Administrator can change the passwords used in the community field of the "Connect to AP" window for the User and the Administrator Authority. The default password is "public".

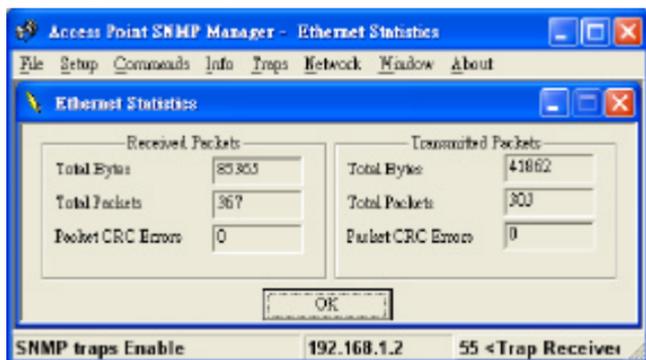


- **Commands Menu:** Under this menu there are two options.
 - 1.) **Reset Device:** You can reset the AP.
 - 2.) **Restore Defaults:** You can restore the factory default values of the AP.
- **Info:** There are two statistic in this menu.
 - 1.) **Wireless statistics:** This option reports the statistics concerning the unit's Wireless activity.



Field Name	Description
Unicast Transmitted Packets	The number of unicast packets successfully transmitted.
Broadcast Transmitted Packets	The number of broadcast packets transmitted.
Multicast Transmitted Packets	The number of multicast packets transmitted.
Unicast Received Packets	The number of unicast packets that were successfully received.
Broadcast Received	The number of broadcast packets that were successfully received.
Multicast Received	The number of multicast packets that were successfully received.

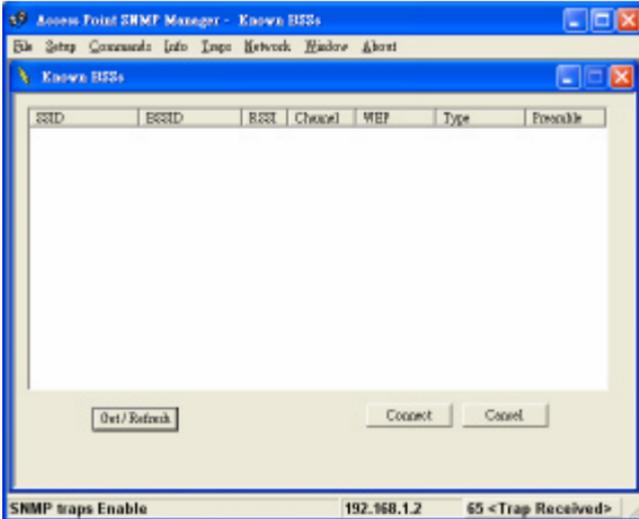
- 2.) Ethernet Statistic: This submenu reports the current statistics of Ethernet port activity.



Field Name	Description
Received Packets:	
Total Bytes	The number of bytes in the frame that were received.
Total Packets	Total number of received packets
Packet CRC Error	The number of packets with CRC error
Transmitted Packets:	
Total Bytes	The number of bytes in the frame that were transmitted.
Total Packets	Total number of transmitted packets
Packet CRC Error	The number of packets with CRC error

- Traps Menu: Provides information for trap messages.
 - View Record: You can see additional information for every Trap Message
- Network Menu: Provides information about the current Network.
 - Associated Stations: Using this option you can view the MAC Addresses of the Associated stations with this AP.

- **Known BBS:** Through this function, you can easily figure out all the information of the Associated stations behind this AP.



- **Get/ Refresh** – Through this button, you can get or refresh new information of the Associated stations behind this AP.
- **Connect** – Press this button to connect to the selected SSID.
- **Cancel** – Press this button to cancellation any action.
- **Windows Menu:** Under this menu there are the following options.
 - **Cascade:** All opened windows will be arranged on the desktop in a cascade fashion.
 - **Tile:** All open windows are visible on the desktop.
 - **About:** Figuring the version of the SNMP Manager.

TECHNICAL SPECIFICATIONS

General	
Standards	Standard: IEEE 802.11b IEEE 802.3 10BASE-T Ethernet
Signal Type:	DSSS (Direct Sequence Spread Spectrum)
Modulation:	QPSK / BPSK / CCK
LED Indicators:	Power, LAN (Link/Activity), WLAN (Link)
Frequency Band:	2.4 GHz
Channel:	1 ~ 11 Channels (US, Canada) 1 ~ 13 Channels (Europe) 1 ~ 14 Channels (Japan)
Data Encryption:	64 bit / 128 bit WEP Encryption
Data Transfer Rate	Ethernet: 10Mbps Wireless: Up to 11Mbps (with Automatic Scale Back)
Transmission Range:	Outdoor: 100~300M Indoor: 40~100M
Operation Mode:	AP / AP Client / Wireless Bridge / Wireless Repeater
Network Cables	10BASET: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA- 568 100-ohm STP (100 m) A to B type USB Cable
Number of Ports	1 x 10Mbps RJ45 port , 1 x B type USB port
Antenna:	2 x 2dBi Dipole Antenna 2 x 2dBi Reverse SMA type Dipole Antenna (optional)

Physical and Environmental

DC inputs	DC 5V /1.0A
Power Consumption	3.5W (Max)
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	171 x 98 x 29 mm (W x H x D)
EMI:	FCC Class B, CE Mark B,