

Wireless LAN Access Point

User Manual

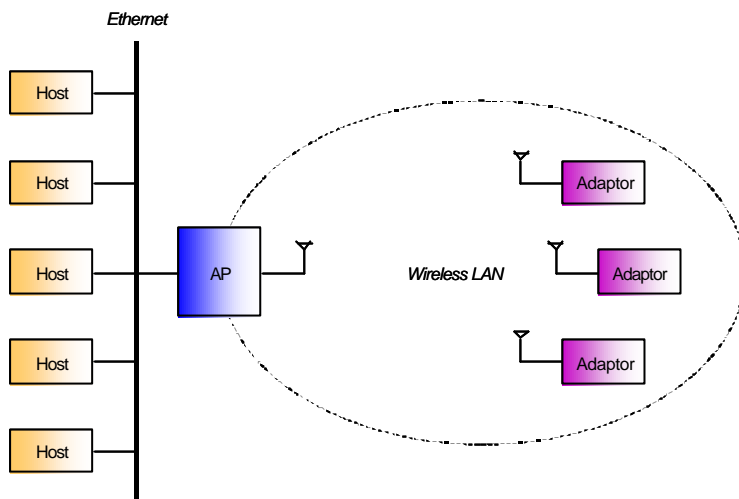


Version 1.0
December 2002

Table of Contents

1. Introduction	2
1.1 System Requirements.....	2
2. Installation Overview	3
2.1 Features.....	3
3. Installation Procedure	4
3.1 What You Will Need.....	4
3.2 Application Installation.....	4
3.3 Connect Access Point (AP) to Computer.....	7
3.4 Setting Up IP address of Windows 2000.....	7
4. Using the AP RFMD Configuration	9
4.1 Connect to AP.....	10
4.2 AP RFMD Configuration Menus.....	11
4.2.1 File Menu.....	11
4.2.2 Setup Menu.....	12
4.2.3 Commands Menu.....	19
4.2.4 Info Menu.....	19
4.2.5 Traps Menu.....	21
4.2.6 Network Menu.....	21
4.2.7 Window Menu.....	21
4.2.8 Help Menu.....	21
5. Wireless Lan AP Operation Modes	22
5.1 Wireless LAN Access Point Mode.....	22
5.2 AP Client Mode.....	22
5.3 AP Bridge Mode.....	23
5.3.1 Bridge Connection Example 1.....	23
5.3.2 Bridge Connection Example 2.....	24
6. Glossary	25
7. Specifications	28

1、 Introduction



The AP (IEEE 802.11b, 11 Mbps WLAN Access Point) is a longrange, high performance LAN product, which provides Access Point services to a 2,4 GHz RF network and bridges to an Ethernet backbone. With the AP, ATMEL gives the AP RFMD Configuration utility, a SNMP Manager, that is used to configure the AP.

This document describes the installation and usage of the AP RFMD Configuration utility.

1.1 System Requirements

- Operating System: Windows 98/Me, Windows 2000, Windows NT4.0 (with Service Pack 4 or later) or Windows XP.
- Desktop PC or notebook PC with CD-ROM drive.
- Ethernet or a RJ-45 Cross-Over cable
- An Ethernet port.

2、 Installation Overview

This section provides a quick step by step guide on how to install the AP RFMD Configuration. Please follow the steps described below and refer to the appropriate sections for further details:

- Power on the computer.
- Install the application:
Insert the given Installation CD into your CD-ROM drive. Select the Utilities & Drivers folder.
Locate the executable file “setup.exe” and double click it.
Follow the installation instructions from the InstallShield Wizard by pressing the “Next” button.
Provide the destination path of where the application will be installed. To set the path of your choice select Browse and then Next.
Finish the installation.
- Connect the AP to the Ethernet port.
Refer to section 3 for more details on the installation and configuration under Microsoft® Windows®. Also, refer to section 4 for detailed instructions for the usage of AP RFMD Configuration utility.

2.1 Features:

- Comply with 11 Mbps IEEE802.11b high data rate specification
- Seamless roaming within the 802.11 and 802.11b wireless LAN infrastructure
- Support 10Base-T networks
- Optimized wired-to-wireless data transfer
- Independent network operating system
- Enables roaming capability
- Antenna diversity for maximum communication, reliability and operating range
- Support SNMP and web-based management
- Watchdog timer
- Easy to install and user friendly
- Bridge function including point-to-point, and point-to-multipoint.
- Wireless Repeater Mode increases the coverage area of an ESS.

3. Installation Procedure

The procedure described in this section can be used in order to install the AP RFMD Configuration utility under Microsoft®Windows®

3.1 What You Will Need

- In this section it is assumed that you have a basic working knowledge of Microsoft Windows.
- During the installation, you may be prompted to load operating system files from the Windows installation disk. Please keep this disk handy.
- You will need the CD provided with your Kit.

3.2 Application Installation

The setup procedure described below installs the AP RFMD Configuration utility:

1. Insert the provided CD into your CD-ROM drive and locate the executable file “setup.exe” under “AP_Uilities/AP_Configuration_xxxx”.
2. Follow the installation instructions from the InstallShield Wizard by pressing the “Next” button (*Figure 3-1*).

Figure 3-1. InstallShield – Start

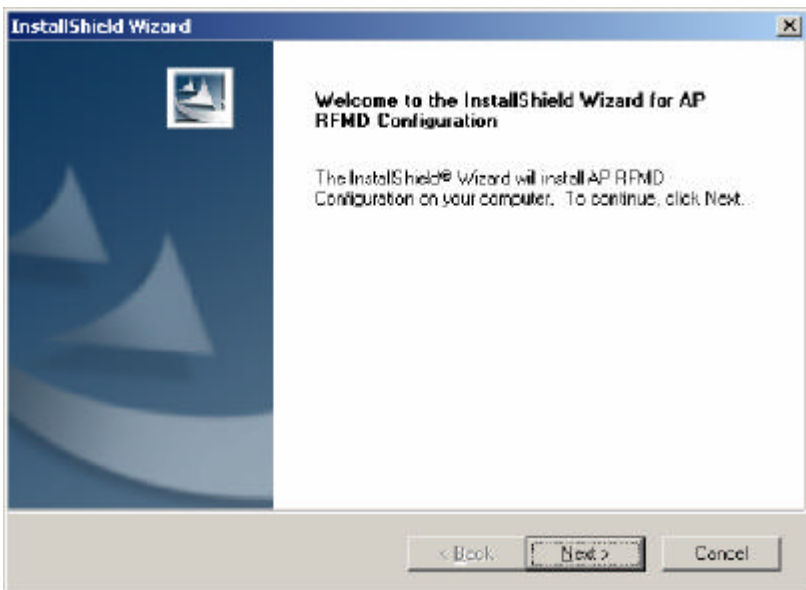
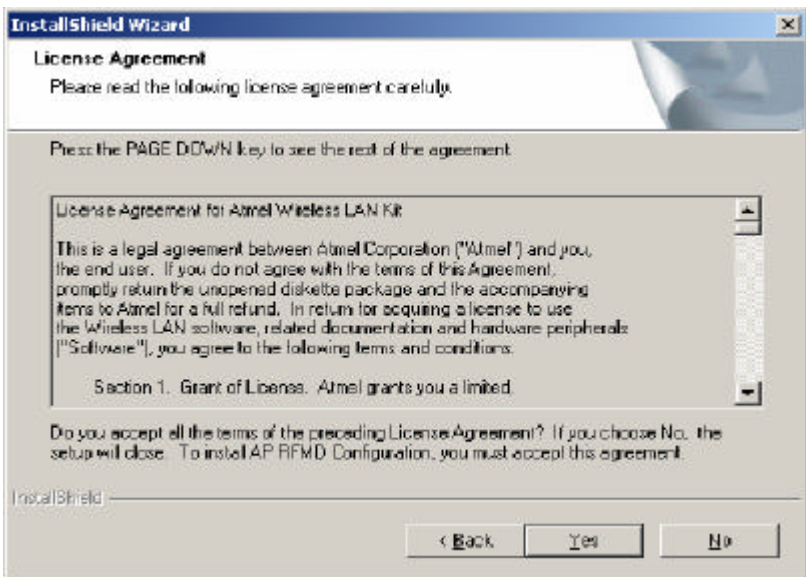
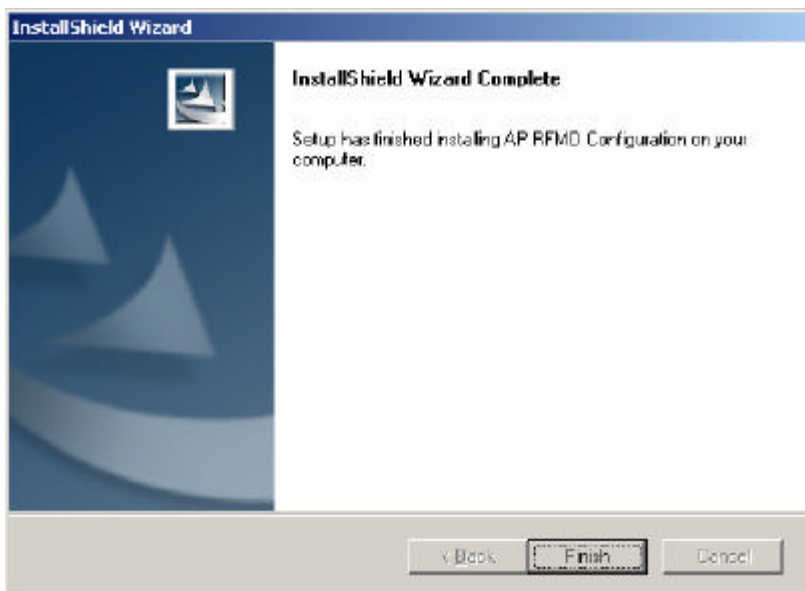


Figure 3-2. InstallShield - License Agreement



3. Next, click "Yes" in order to agree with the License Agreement.

Figure 3-3. InstallShield – Finished



4. Continue to follow the instructions from the InstallShield wizard and clicking the "Next" button, in order to complete the installation (Figure 3-3).

Installation procedure for AP RFMD Configuration utility is now completed, you can see section 4 for usage information.

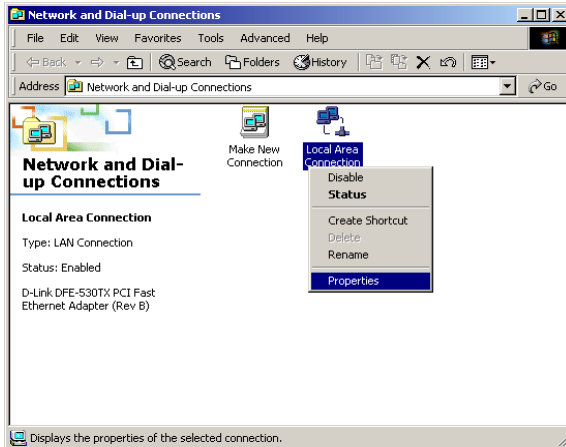
Quick Start to Connect Access Point:

3.3 Connect Access Point (AP) to Computer

You can either connect AP to an Ethernet or AP to a computer by RJ-45 Cross-Over cable. Please avoid other computers to use any IP addresses on the Ethernet.

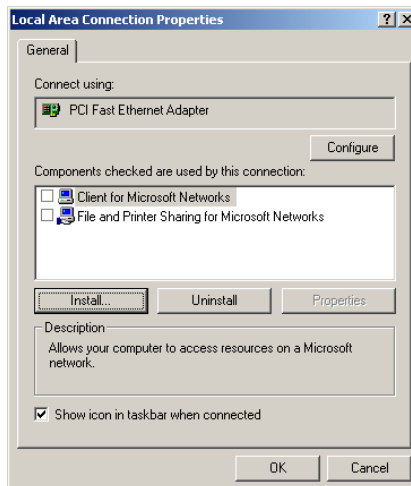
3.4 Setting Up IP address of Windows 2000

Figure 3-4. Open Network Properties



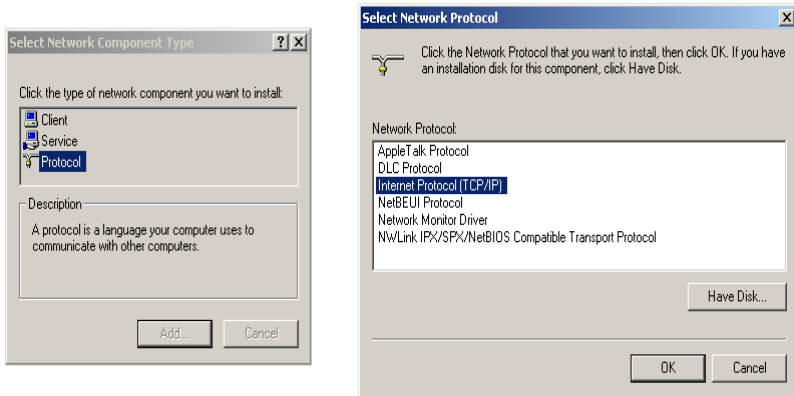
Double-click on **Network and Dial-up Connections** on **Control Panel** And Right-Click on the connection and select **Properties**.

Figure 3-5. Check the Existence of Internet Protocol (TCP/IP)



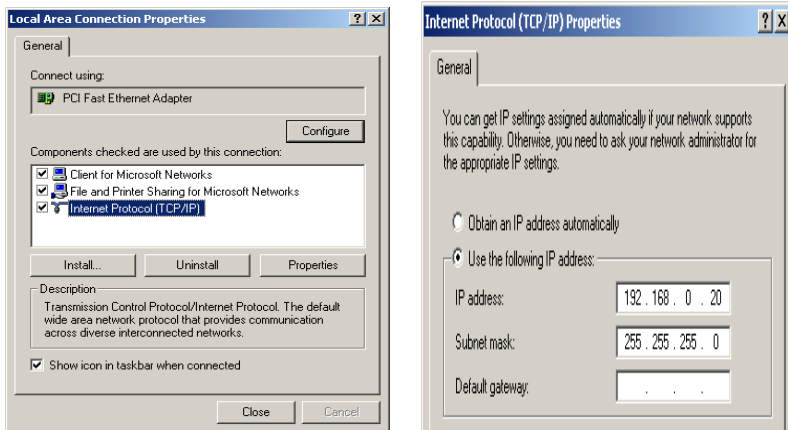
If Internet Protocol (TCP/IP) exists, please skip to **Figure 3-7**. If Internet Protocol (TCP/IP) does not exist, please continue the procedure of **Figure 3-6**.

Figure 3-6. Install Internet Protocol (TCP/IP)



Click **Install...** in connection properties frame. Select **Protocol** and click **Add...** After all the procedures, select **Internet Protocol (TCP/IP)** and click **OK**. Windows 2000 will install TCP/IP protocol.

Figure 3-7. Set Up Configurations of Internet Protocol (TCP/IP)



Select **Internet Protocol (TCP/IP)**, and click **Properties**.

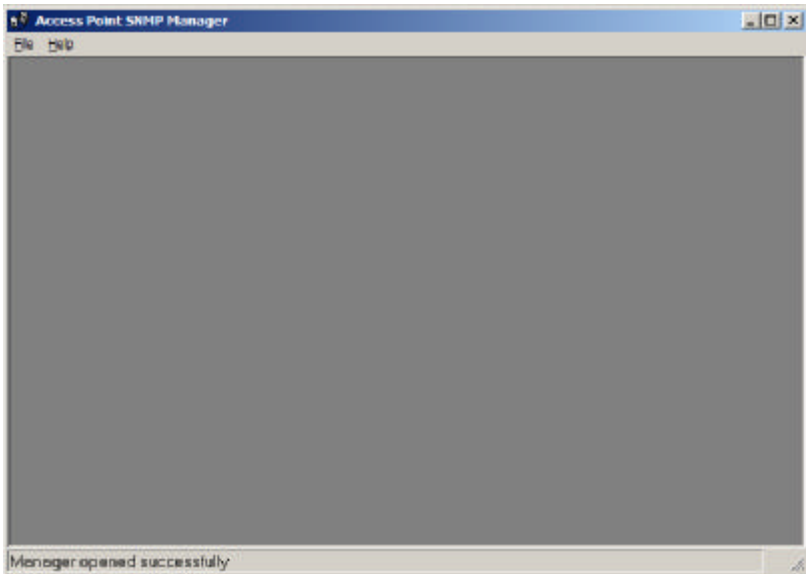
Select DHCP server in your network.

Internet Protocol (TCP/IP) settings for Windows 95/98/ME/XP are similar to Windows 2000. Please refer to User Manual of Windows 95/98/ME/XP to learn more.

4. Using the AP RFMD Configuration

The AP RFMD Configuration utility is a SNMP manager used for the configuration of an ATMEL FastVNET AP. In this section you can see the usage of the AP RFMD Configuration utility.

Figure 4-1. AP RFMD Configuration – Opened



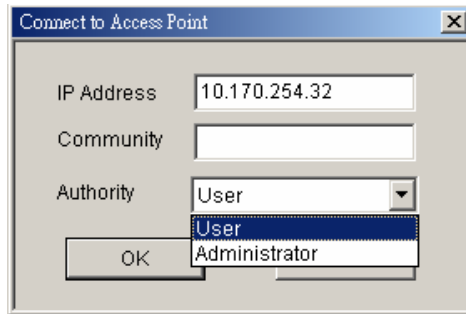
4.1 Connect to AP

There are two ways to connect with the AP RFMD Configuration utility with an ATMEL FastVNET AP.

The first is to know the IP of the AP and use the File -> Connect to Access Point option and enter the IP, the Community and the Authority (Figure 4-2).

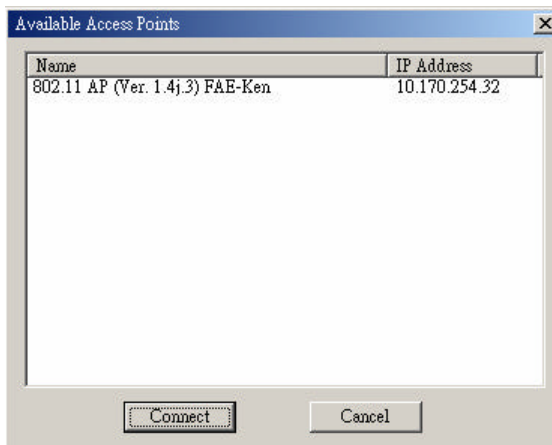
- IP Address: Type IP address of AP (10.170.254.32 IP Address)
- Community: Type a password to connect AP. (The default password is "public")

Figure 4-2. File - Connect to Access Point



The other way is used when you don't know the IP for the AP and you select the File-> Find Access Point. After a while a window with the APs that the AP RFMD Configuration utility found will be displayed (Figure 4-3).

Figure 4-3. File - Find Access Point



From that window you can select the AP that you want to configure and click the connect button. Next you must enter the Community and the Authority in order to get access to the function of the AP RFMD Configuration utility (Figure 4-2).

In both cases after the authentication process you shall see a confirmation message (Figure 4- 4) if success or an error message (Figure 4- 4).

Figure 4-4. AP RFMD Configuration - AP Found

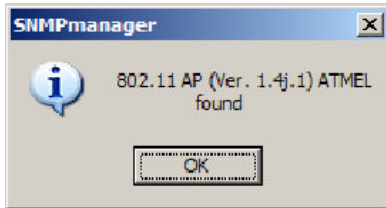
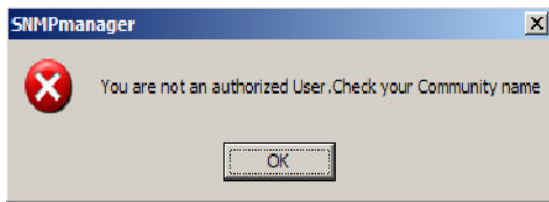


Figure 4-5. AP RFMD Configuration - Not authorized access



Now, you are connected to the AP you shall see that the AP RFMD Configuration utility has more menus available. Below is a description of those menus.

4.2 AP RFMD Configuration Menus

Below you will find the available menus of the AP RFMD Configuration utility.

4.2.1 File Menu Under this menu you can find the following options:

- **Connect to Access Point** - Using this option you can directly connect with the AP. First, type its IP Address in the panel which appears (Figure 4-2). Then, type the appropriate password in the Community field (The default password is "public"). Finally, you have to select either User or Administrator Authority in the Authority combo-box.
 - User Authority allows you to view but not to set or save changes to the AP RFMD Configuration.
 - Administrator Authority allows you to either view or set changes to the AP RFMD Configuration.
- **Find Access Point** - This option allows you to find and connect with an AP without the necessity of knowing its IP Address. Choose this option in order to find the APs available for connection (Figure 4-3). Select one of the available APs and press "Connect". Then, the IP of the selected AP is passed to the IP field of the panel in figure 4-2, and prompting you to select Authority and to write the appropriate password at the community field.
- **Close Connection AP** - Terminates the connection with the AP.

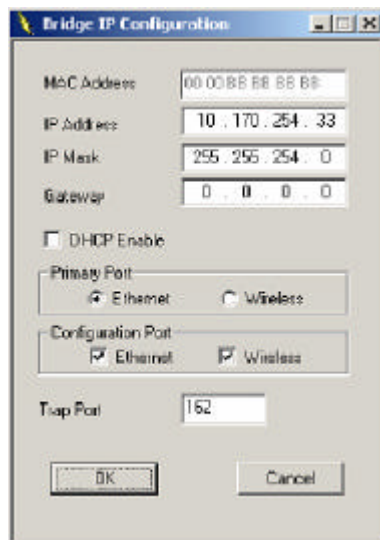
- **Download Changes** - When all the desired values of the parameters have been set you are able to download the changes (save the changes) to the AP by selecting this option.
- **Refresh** - Renews the display.
- **Options** - Defines the polling interval according to which the AP RFMD Configuration polls the AP in order to update the statistics and the Associated Stations List.
- **Exit** - Terminates the connection with the AP and exits the application.

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

4.2.2.1 Bridge Under the “Bridge” submenu, there are two options:

- **IP Configuration** - Under this window you see and change the followings: The IP Address, IP Mask and Gateway of the AP. The option to enable or not the DHCP client function of the AP. Additionally you have to select the Primary Port, which is the interface that determines the DHCP server. Also you can select which port (Ethernet and/or Wireless) will be used for the AP configuration. And finally the Trap port is UDP port that the AP will use to send the SNMP traps.

Figure 4-6. Bridge - IP Configuration



If you make any changes, you need to select “Download Changes” under the “File” menu in order to save them (Figure 4- 6).

- **Filtering** - Under this window you can set the filtering options that the AP will use (Figure 4-7).

IP Filtering: Only the IP protocol packets will pass through the WLAN and any other protocol will be filtered out.

Figure 4-7. Bridge – Filtering



Broadcast Forwarding: The AP should not forward broadcast traffic to the air.

Send Back Broadcast: The AP should not send back to the air broadcast traffic received from the air.

Send Back Unicast: The AP should not send back to the air Unicast traffic received from the air.

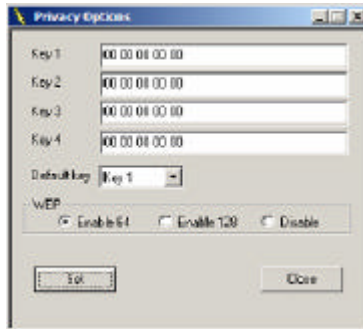
4.2.2.2 Wireless LAN Under this submenu the following three options are available:

- **Privacy Options** - Here you can enter the encryption key values using the Wireless Equivalent Privacy (WEP) Option window (Figure 4-8), write the values and press "Set" to download (WEP key is write-only, so it is not possible to retrieve the key values).

There are four 5 Hex digit encryption keys available if you select 64bit WEP and there are four 13 Hex digit encryption keys available if you select 128bit WEP.

The key is enabled only if you select it in the "Default key" option. Enable the WEP (Wired Equivalent Privacy) option in order to activate WEP encryption for transmissions between the stations and the AP. WEP is an authentication algorithm which protects authorized Wireless LAN users against eavesdropping.

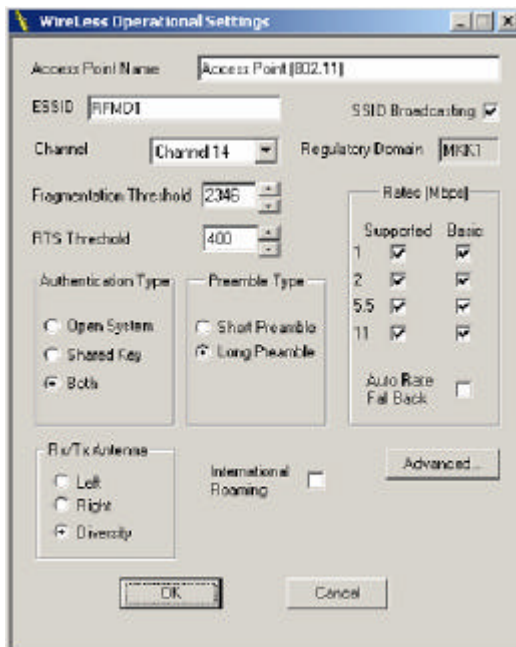
Figure 4-8. Wireless LAN - Privacy Options



Note:Valid for firmware version 1.4g and SNMP version 1.7.4.1 and all subsequent versions.

- **Operational settings** - Using this option you can either view or modify the Wireless LAN parameters of the AP (Figure 4-9). These parameters are described below:

Figure 4-9. Wireless LAN - Operational Settings



Access Point Name - The name of the AP.

ESSID - 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 ESSID value must be the same in all stations and AP in the extended WLAN. Select the ESSID to be used.

SSID Broadcasting - When checked the AP broadcasts the ESSID to the stations, if not checked then the stations must know the AP ESSID in advance.

Channel - Select the channel to be used. Depending on the Regulatory Domain of the AP the number of available channels can be 1 - 14.

Fragmentation Threshold - The size at which packets will be fragmented. Choose a setting within a range of 256 to 2346 bytes.

RTS Threshold - Minimum packet size to require an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the WLAN. This is the option for the RTS Threshold activation.

Authentication Type - Select Open System, Shared Key, or Both:

Open System: With this setting any station in the WLAN can associate with an AP and receive and transmit data (null authentication).

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

Both: With this setting stations communicate with the AP either with or without data encryption.

Preamble Type (Short/Long) - Preamble is the first subfield 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.

Rate - By default the unit adaptively selects the highest possible rate for transmission. Select the basic & supported rates to be used among the following options 1 - 2 - 5.5 - 11 (Mbps).

Auto Rate Fall Back - When this is enabled the transmission rate is the optimum rate. In case of obstacles or interference, the system will automatically fall back.

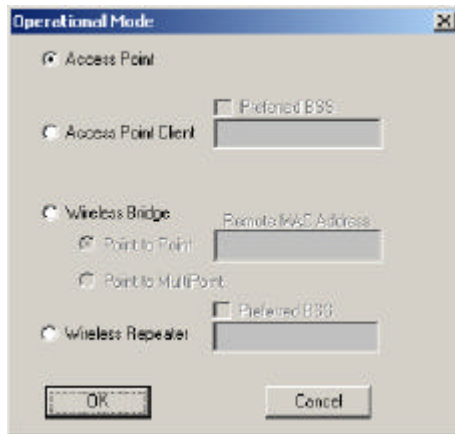
Regulatory Domain - The value of this field is already set and can not be modified.

Rx/Tx Antenna - Here you can decide how the AP will use each Antenna.

International Roaming (IEEE 802.11d): The ATMEL AP can support the International Roaming function if this option is enabled.

Advanced - The following four operational modes are available (Figure 4-10). For each mode you can either view or modify the Wireless LAN parameters of the Wireless Operational Settings window:

Figure 4-10. Operational Settings – Advanced

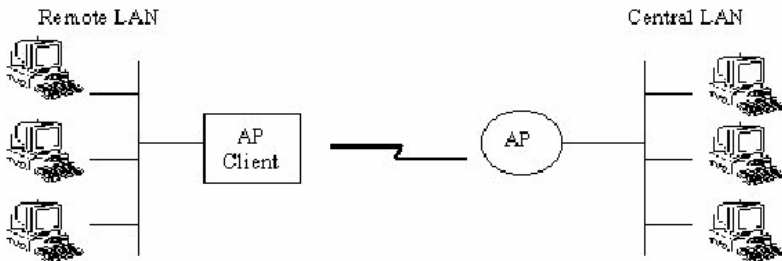


Access Point - This mode provides access from Wireless Stations to Wired LANs and from Wired LANs to Wireless Stations. Furthermore, Wireless Stations within the range of the AP device may communicate with each other via the AP.

Access Point Client - This mode allows the connection of one or more remote LANs with a central LAN, creating thus an extended single virtual LAN (Figure 4-11). In this way, any station of the Remote LAN can successfully communicate with any station of the central LAN, as if all of them belonged to the same physical LAN. Wireless Stations can't be associated 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.

Figure 4-11. Access Point Client Mode



Wireless Bridge- This mode (Figure 4-12) 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 any Wireless Bridge available in the same channel. When the Authorization Algorithm (See the next menu - Authorized MAC Address), is enabled, the Wireless Bridge can communicate with any Wireless Bridge whose MAC Address exists in the Authorization Table.

Figure 4-12. Wireless Bridge Mode

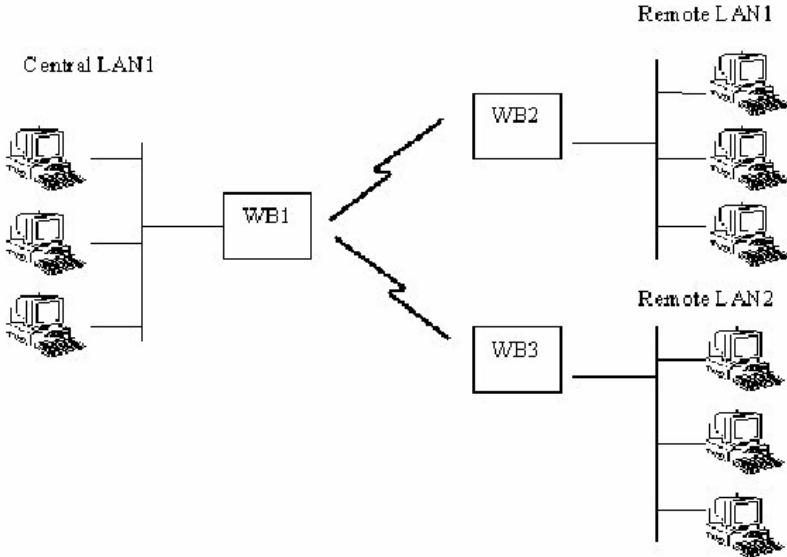
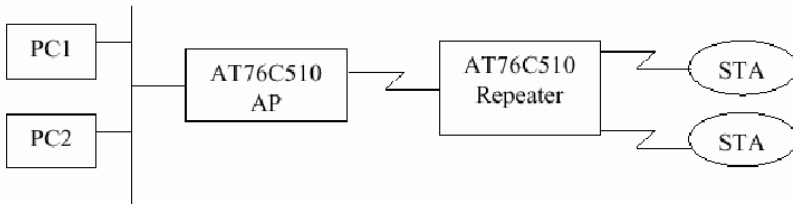


Figure 4-13. Wireless Repeater mode



Wireless Repeater Mode: 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). The AT76C510 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.

- **Authorized MAC Address (MAC Address Filter)** - 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).

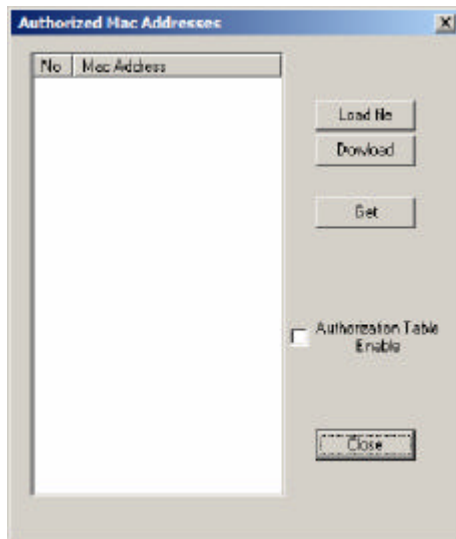
The txt file must have one MAC address at a line and with the following format: 000425000146 not 00-04-25-00-01-46 or 00 04 25 00 01 46.

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.

Figure 4-14. Authorized MAC Address



- **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 Resuscitation: This trap message is sent when a Station's resuscitation 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.

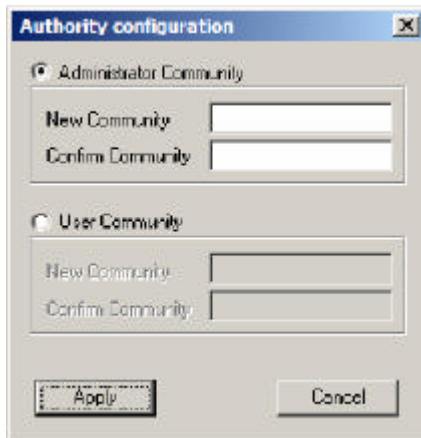
Trap Reset: This trap message is sent when the AP resets.

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.

- **Authorization** - Using this option (Figure 4-14) the Administrator can change the passwords used in the community field of the "Connect to AP" window for the User and the Administrator Authority.

●
Figure 4-15. Authorization



The image shows a dialog box titled "Authority configuration". It has a blue title bar with a close button (X) on the right. The dialog is divided into two sections. The first section is "Administrator Community", which is selected with a radio button. It contains two text input fields: "New Community" and "Confirm Community". The second section is "User Community", which is not selected. It also contains two text input fields: "New Community" and "Confirm Community". At the bottom of the dialog, there are two buttons: "Apply" and "Cancel".

4.2.3 Commands Menu Under this menu there are two options.

- **Reset Device** - You can reset the AP.
- **Restore Defaults** - You can restore the factory default values of the AP.

4.2.4 Info Menu This menu lets you view Wireless and Ethernet statistics.

- **Wireless statistics:** This option reports the statistics concerning the unit's Wireless activity (Figure 5-16).

Figure 4-16. Wireless statistics

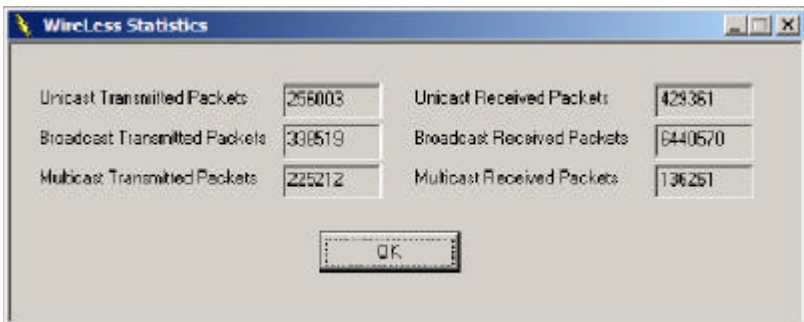


Table 4-1. Wireless statistics

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.

- **Ethernet statistics:** This option reports the statistics concerning the unit's Ethernet port activity (Figure 5-17).

Figure 4-17. Ethernet statistics

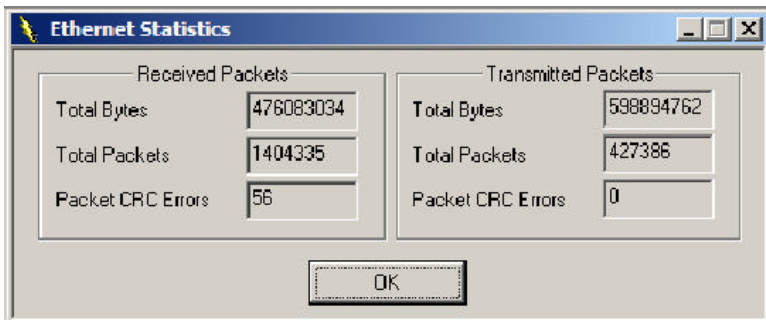


Table 4-2. Ethernet statistics

Field	Description
Received Packets:	
Total Bytes	The number of bytes in the frames that were received
Total Packets	Total number of received packets
Packet CRC Errors	The number of packets with CRC Errors
Transmitted Packets:	
Total Bytes	The number of bytes in the frames that were transmitted
Total Packets	Total number of transmitted packets
Packet CRC Errors	The number of packets with CRC Errors

4.2.5 Traps Menu Provides information for trap messages

- **View Record** - You can see additional information for every Trap Message

4.2.6 Network Menu Provides information about the Network.

- **Associated stations**- Using this option you can view the MAC Addresses of the associated stations with the AP.

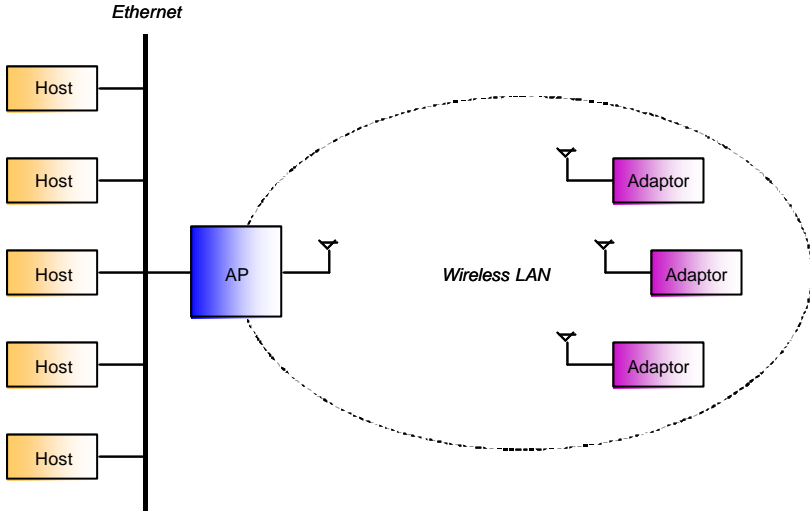
4.2.7 Window Menu Under this menu there are the following options

- **Cascade** - All opened windows are arranged on the desktop in a cascade fashion.
- **Tile** - All open windows are visible on the desktop.

4.2.8 Help Menu Provides on line help about the application.

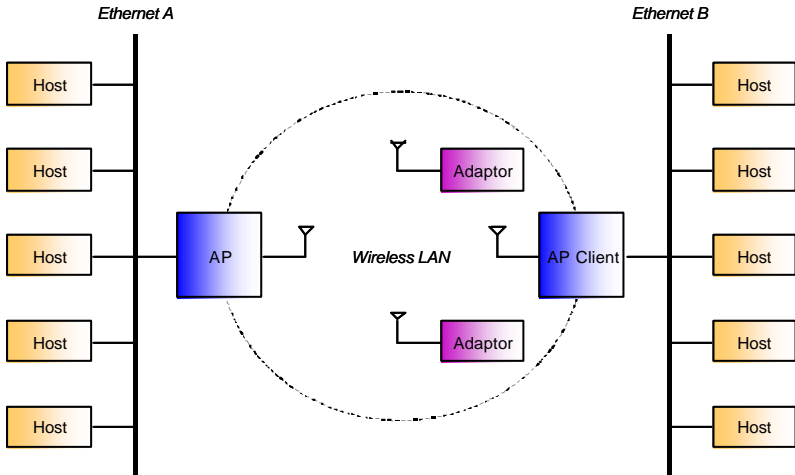
5. Wireless Lan AP Operation Modes

5.1 Wireless LAN Access Point Mode



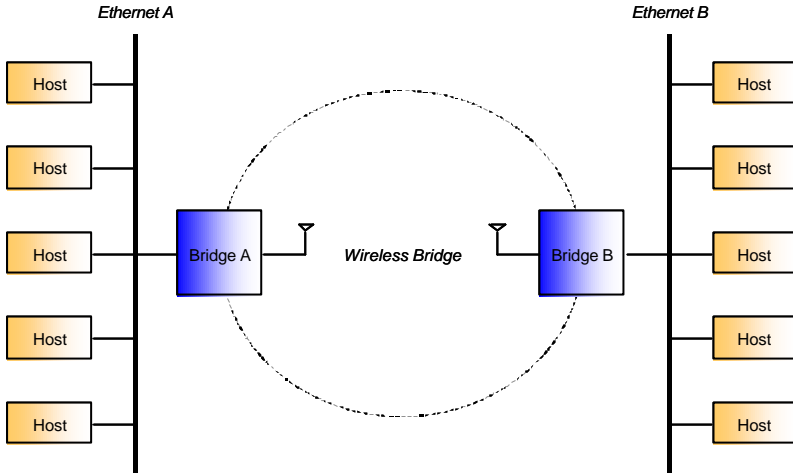
AP provides the capability of connecting Wireless LAN to Ethernet. Adaptors can connect to Ethernet through AP.

5.2 AP Client Mode



AP Client can connect to the AP like an adaptor. The figure shows that Ethernet B is connected to Ethernet A. Adaptors still could connect to the AP that the AP Client has connected to.

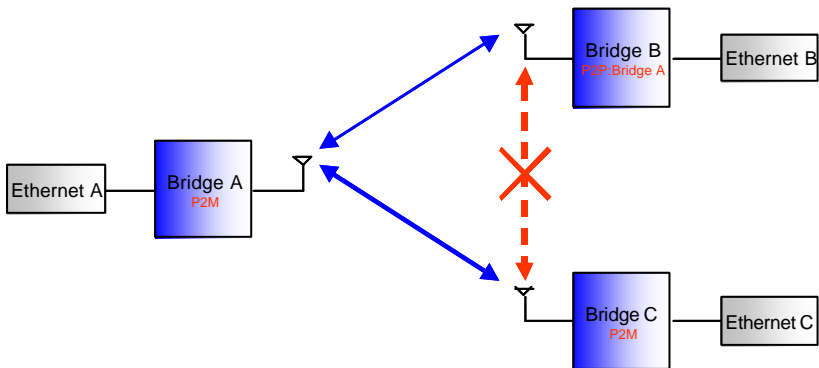
5.3 AP Bridge Mode



Different from the AP Client mode to bridge mode, no adapters could connect to any bridge in bridge mode. And there are two bridge modes.

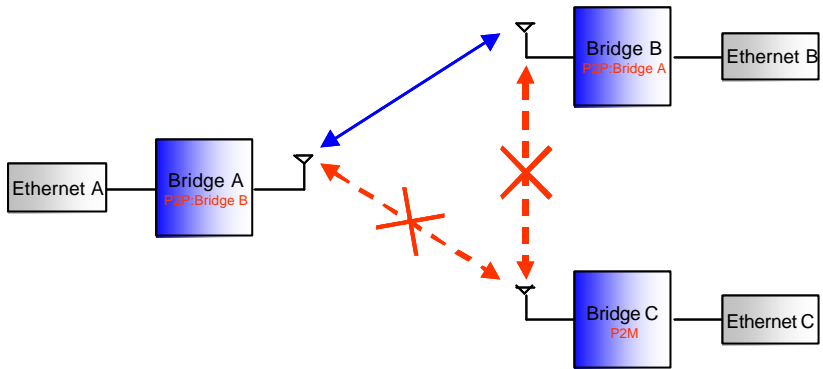
- Point-to-Point Mode
Bridge in this mode will only connect to one fixed bridge.
- Point-to-Multipoint Mode
Bridge in this mode will connect to any other bridges nearby.

5.3.1 Bridge Connection Example 1



Bridge A and Bridge C are in Point-to-Multipoint mode, Bridge B is in Point-to-Point mode that only connect to Bridge A. In this case, Bridge A could connect to both Bridge B and Bridge C, but Bridge C could only connect to Bridge A.

5.3.2 Bridge Connection Example 2



If we set Bridge A to be Point-to-Point mode that only connects to Bridge B. Bridge C can't connect to either Bridge A or Bridge B.
(Note: Please refer to 6.2.2 Modify Operational Settings for more information.)

6. Glossary

A

Ad-Hoc Mode - A client setting that provides independent peer to peer connectivity in a wireless LAN. An alternative setup is where PCs communicate with each other through an access point.

B

Bandwidth - The transmission capacity of a given facility, in terms of how much data the facility can transmit in a fixed amount of time; expressed in bits per second (bps).

Bit - A binary digit. The value - 0 or 1-used in the binary numbering system. Also, the smallest form of data.

D

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

DHCP server and client - DHCP stands for Dynamic Host Configuration Protocol. This protocol is designed to automatically load parameters for the TCP/IP network, including the IP address, host name, domain name, net mask, default gateway, and name server address. The machine that provides this service is called the DHCP server, and its client computers are called DHCP clients. If client computers support DHCP, a TCP/IP configuration is not needed on each client computer.

Domain - A sub network comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Driver - A workstation or server software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific NIC, and is installed during the initial installation of a network compatible client or server operating system.

DSSS (Direct-Sequencing Spread-Spectrum) - DSSS operate over the radio airwaves in the unlicensed ISM band (industrial, scientific, medical). DSSS uses a radio transmitter to spread data packets over a fixed range of frequency band.

E

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

Ethernet - The most widely used LAN access method which is defined by the IEEE 802.3 standards. Ethernet is normally a shared media LAN meaning all devices on the network segment share total bandwidth. Ethernet networks operate at 10Mbps using CSMA/CD to run over 10Base T cables.

F

Firmware - Program that is inserted into programmable read-only memory (programmable read-only memory), thus becoming a permanent part of a computing device.

Fragmentation Threshold Value - Indicates how much of the network resources is devoted to recovering packet errors. The value should remain at its default setting of 2,432. If you experience high packet error rates, you can decrease this value but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

I

IEEE - The Institute of Electrical and Electronics Engineers.

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

Infrastructure Mode - A client setting providing connectivity to an Access Point. As compared to Ad-Hoc Mode where PCs communicate directly with each other clients set in infrastructure Mode all pass data through a central Access Point. The Access Point not only mediates Wireless network traffic in the immediate neighborhood but also provides communication with the wired network.

IP Address - An IP address is a 32-bit number that identifies each sender & receiver of information that is sent across the Internet. An IP address has two parts: the identifier of a particular network on the Internet and one identifier of a particular device (which can be a server or a workstation within that network).

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.

L

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).

M

MAC Address - 12-digit hexadecimal number that identifies a networking product on the network.

Mbps (Megabits per second) - One million bits per second; unit of measurement for data transmission.

N

Network - A system that transmits any combination of voice, video and/or data between users.

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

O

Open System - Is when 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 (usually randomly) generated key. Once accepted, this key is used for a short time only; then a new key is generated and agreed upon.

P

Packet - A unit of data routed between an origin and a destination in a network.

PCMCIA - Personal Computer Memory Card International Association

Plug and Play - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

R

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.

RTS/CTS Threshold Value- Should remain at its default setting of 2,347. A preamble is a signal used to synchronize the transmission timing between two or more systems. A series of transmission pulses is sent before the data to indicate that "someone is about transmitting data." This ensures that systems receiving the information correctly when the data transmission starts.

S

Shared Key - Is when both the sender and recipient share a secret key. Both units use this key for an extended length of time, sometimes indefinitely. Any eavesdropper that discovers the key may decipher all packets until the key is changed.

Signal Strength - The signal level indicates the strength of the signal as received at the wireless network interface.

SNMP (Simple Network Management Protocol) - A standard network protocol that can be used to manage networks locally, or worldwide via the Internet.

SSID (Service Set Identifier) - Is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the network. It is case sensitive and must not exceed 32 characters.

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

Subnet - A subnet is a logical sub-division of a Local Area Network that has been divided by means of routers or gateways. A subnet may include multiple LAN segments. Each subnet is identified by the Subnet Mask.

T

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

W

WEP (Wired Equivalent Privacy) - The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired LAN medium that does not employ cryptographic techniques to enhance privacy.

Windows workgroup - A Windows workgroup can consist of either wireless or wired network connections or a combination of the two. Usually a Windows workgroup consists of members who are related because of a shared function, e.g. members of the same department. For a Windows workgroup it is not relevant where the workgroup participants are located, since the members of a Windows workgroup are identified by their workgroup name only.

7、Specifications

Standard compatibility	
	IEEE802.11b, FCC, RTSI, Wi-Fi compatible
	All major networking standards, including IP, IPX
	Wireless Network Interface: IEEE 802.11b (CSMA/CA)
	Wired Network Interface: RJ45(10Base-T)
	Encryption: 64-bit WEP and 128-bit WEP
Environmental	
	Operating Temperature is from 32 to 131 (0 to 55)
	Humidity (non-condensing): 10 to 90%
Power specification	
	Power Consumption: 5V±5%@700mA
	Power Requirements: 110-120V/220-240V
Radio Specifications	
	RF Output Power: 17 dBm (Normal) @ -30 dB Side lobe
	Modulation Technique: Direct Sequence Spread Spectrum CCK@5Mbps/11Mbps DQPSK@2Mbps DBPSK@1Mbps
	Typical Range: *50m indoors, 100m outdoors when 11Mbps (May vary depending on operation environment)
	Frequency range: 2.4-2.4835 GHz
	Number of channels :14 channels
	Antenna: Embedded Antenna Modulation with diversity support
Physical Dimensions	
	Length: 130mm*Height 190mm*Width 66mm
	Weight: 330g
Other Function	
	Led Indicators: Status, network activity and RF Activity