

Your Installation Guide to Access Point

Version 2.1 – January 2002

Copyright Statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the prior writing of the publisher.

Windows 95/98 and Windows 2000 are trademarks of Microsoft Corp.

Pentium is trademark of Intel.

All copyright reserved.

Notes:

The Product is passed CE and able to be used in these countries as following:

North America: US, Canada

Europe: Germany, France, Italy, England, Spain, Austria, Danish, Finland, Iceland, Luxembourg, Netherlands, Norway, Sweden, Switzerland

Asia: Hongkong, Taiwan, Korea, Singapore

Australia, New Zealand



Radio Channel Selection Table

	Regulatory domains					
Channel_ID	U.S.A.	Canada	Most of Europe	Spain	France	Japan
1	X	X	X	-	-	X
2	X	X	X	-	-	X
3	X	X	X	-	-	X
4	X	X	X	-	-	X
5	X	X	X	-	-	X
6	X	X	X	-	-	X
7	X	X	X	-	-	X
8	X	X	X	-	-	X
9	X	X	X	-	-	X
10	X	X	X	X	X	X
11	X	X	X	X	X	X
12	-	-	X	-	X	X
13	-	-	X	-	X	X
14	-	-	-	-	-	-

Table of Contents

Table of Contents	3
Regulatory information	4
<u>1. Welcome</u>	5
1.1 Advantages for Using Wireless Network	5
1.2 About Access Point	6
1.3 Verifying kit contents	6
1.4 Wireless Adapter	6
1.5 System Interoperability	6
<u>2. Step-by-Step Installation Guide</u>	7
<u>3. Access Point SNMP Manager</u>	8
3.1 About Access Point SNMP Manager	8
3.2 Install SNMP Manager	9
3.3 Uninstall SNMP Manager	13
<u>4. Using Access Point SNMP Manager</u>	14
4.1 Connecting to Access Point	14
4.2 Configuring the Access Point	16
4.2.1 Setting the IP address of the Access Point	16
4.2.2 File menu	16
4.2.3 Setup menu	17
4.2.4 Commands menu	22
4.2.5 Info menu	23
4.2.6 Traps menu	27
4.2.7 Network menu	27
4.2.8 Window menu	27
4.2.9 Help menu	27
<u>5. Glossary</u>	28
<u>6. Technical Specifications</u>	30

Regulatory Information

The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device or the substitution or attachment of connecting cables and equipment other than specified. The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user. Built-in antennas, whether installed indoors or out, should be installed only by experienced antenna installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities.

USA – Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for Class B Digital Devices, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, 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 to correct the interference by one or more of the following measures:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION STATEMENT

RF Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Canada – Industry Canada (IC)

This class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations.

1. Welcome

Thank you for purchasing Access Point! Access Point is easy to install and easy to operate—in no time you will have your own wireless network.

This guide will lead you through the installation process in detail. Please read this manual carefully and keep it for future reference.

You need to have a basic knowledge of installation procedures for network operating systems under Microsoft Windows 95 (or up) and Windows NT.

1.1 Advantages for Using Wireless Network

Advantages for Using a Wireless Network:

- *For hard to wire areas:* Access Point provides access to network services in areas otherwise hard or expensive to wire, such as historic buildings with asbestos and classrooms.
- *Flexible workgroups:* Lower total cost of ownership for workspaces that are frequently reconfigured.
- *Networked conference rooms:* users can access the network as they move from meeting to meeting, can get up-to-date access to information and can communicate while ‘on the go’.
- *Easy Network:* with quick network setup and collaboration software, on site consultants and small workgroups increase efficiency and productivity.
- *Branch office networking:* provides an easy to install, use and maintain network for a remote or sales office.
- *Campus-wide network mobility:* roaming capabilities allow enterprises to set up easy-to-use wireless networks that cover the entire campus transparently.

1.2 About Access Point

The Access Point is a modular unit with an integrated Ethernet interface that enables you to use your Access Point with your adaptors. The Antennas are built-in which creates further wireless atmosphere and a cleaner look. The Access Point is a wired to wireless bridge that you can use to connect wireless cells to one another or to a wired (Ethernet) Local Area Network. The Access Point can serve mobile wireless clients roaming between various locations within network premises.

1.3 Kit Contents

The contents of the box should include the following items:

- User's Guide
- Quick Start Guide
- Access Point (with the MAC-address in the back)
- Power Line
- CD: containing Installation Driver and SNMP Manager Software

If you find any incorrect, missing or damaged parts, please contact the vendor immediately.

1.4 Wireless Adaptor

Adaptor comes in separate packages. It is a wireless network adapter, that allows sharing of Internet access and peripherals through access point. Adaptor comes in two types: PC Card and USB Adapter. PC Card is for the use of notebook only, whereas USB is compatible for both computer and notebook.

1.5 System Interoperatability

Access Point is able to integrate with other brand's wireless network communication systems.

2. Step-by-Step Installation Guide

This section helps you with the installation of the Access Point. Please follow the instructions on how to install your Access Point:

1. Mount the Access Point firmly to the wall on the desired position. A drill model is supplied as a separate sheet with this manual.
2. Connect Ethernet cable to Access Point's RJ-45 Port
3. Connect power adapter to Access Point, and "Power" LED of Access Point will turn green.

Is your Installation Successful?

At the front of Access Point you will see three LEDs.

If the installation is successful, the "Power" LED is green, and the "RF" LED and the "Ethernet" LED flash whenever there is traffic on the respective network.¹

How to Select Wired Network?

Access Point will automatically select the medium attached. When the cable network is detected, the "Ethernet" LED will turn yellow.

Factory Settings

You can reset Access Point to factory default settings by pushing a paperclip into the little hole next to the power switch when Access Point is turned off. Hold until the lights of the 3 LEDs at the front of the Access Point are off. When you push a paperclip in the reset hole while the Access Point is switched on, only the lock set Access Point SNMP Manager is deactivated.



¹ The –insert pic- flash at least 10 times per second for the wireless LAN because of so-called 'beacons'

3. Access Point SNMP Manager

3.1 About Access Point SNMP Manager

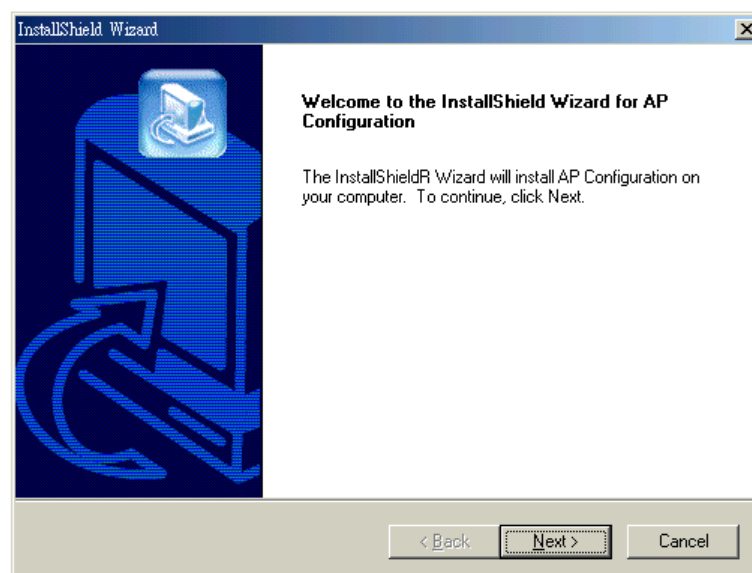
Access Point SNMP Manager allows users to view contents of all wireless networks under Windows system (e.g. how many Access Points there are in a WLAN). You can use it to control a large number of IEEE 802.11b Access Points from a single location. Further more, the Access Points are remotely updated through the SNMP automatically. All indicate a simpler management for your wireless LAN. Access Point SNMP Manager is easy to operate and understand.

SNMP Manager allows you to edit your WLAN in the following areas:

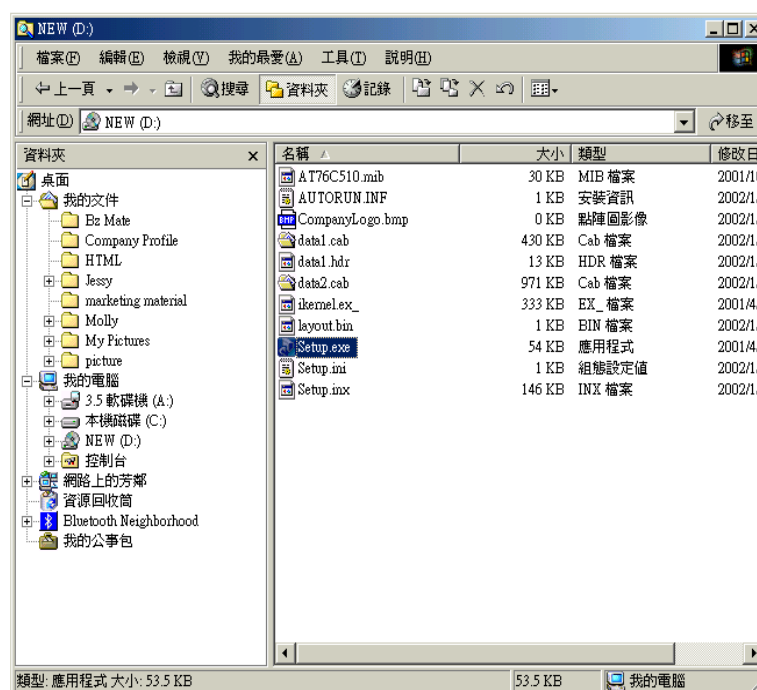
- Adding and removing Access Points from WLAN
- Restricting access to the Wireless network
- Managing data protection options such as IEEE 802.11b
- Assigning radio channel for optimal cell management
- Grouping the wireless network into multiple WLANs with individual access control and security options
- Programming an Access Point with a specified IP address
- Setting the SNMP Write Community String
- Storing the Access Point configuration on disk
- Verifying the status of all Access Points in the network

3.2 Install SNMP Manager

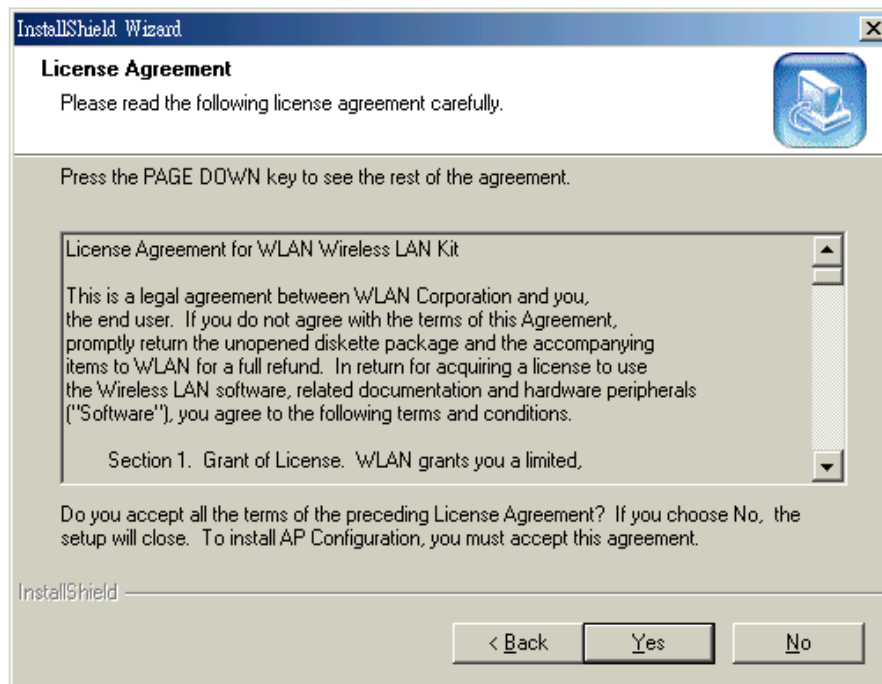
Step 1. To Install Access Point SNMP Manager, please insert CD containing SNMP Manager into one computer of the LAN. Wait a few seconds for the screen below to show up. Click Next.



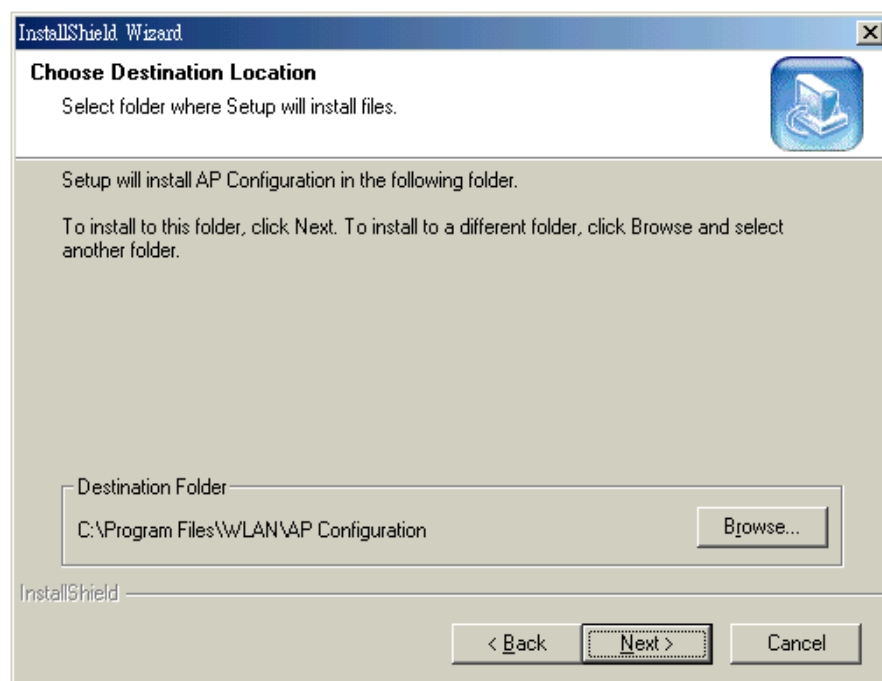
If InstallShield Wizard window doesn't display, please go to 'My Computer' and double click on CD-ROM drive. Run "Setup.exe".



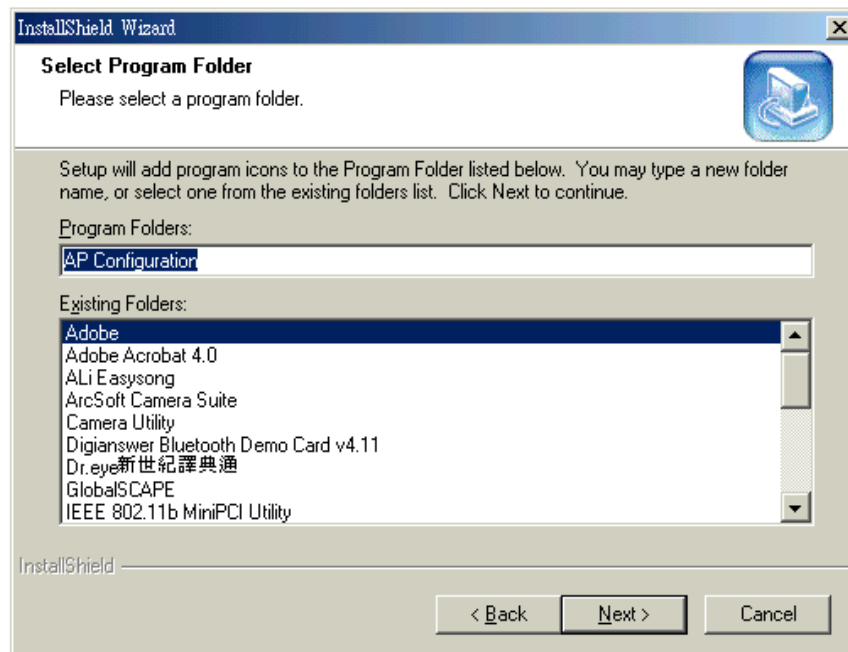
Step 2. Read the License Agreement and click Yes if you accept the terms.



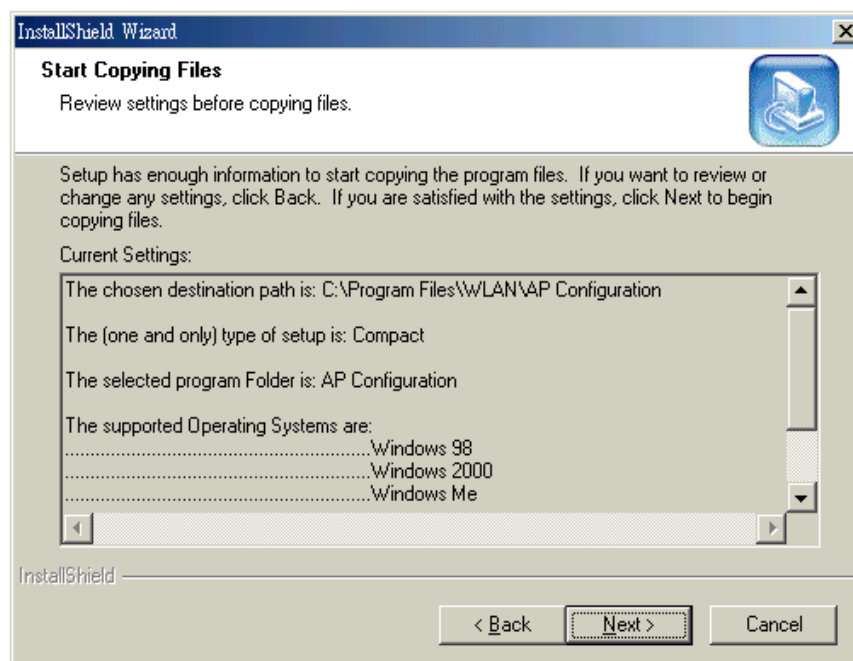
Step 3. Choose Destination Location. Click Browse to choose a destination folder and click “Next” to install AP Configuration.



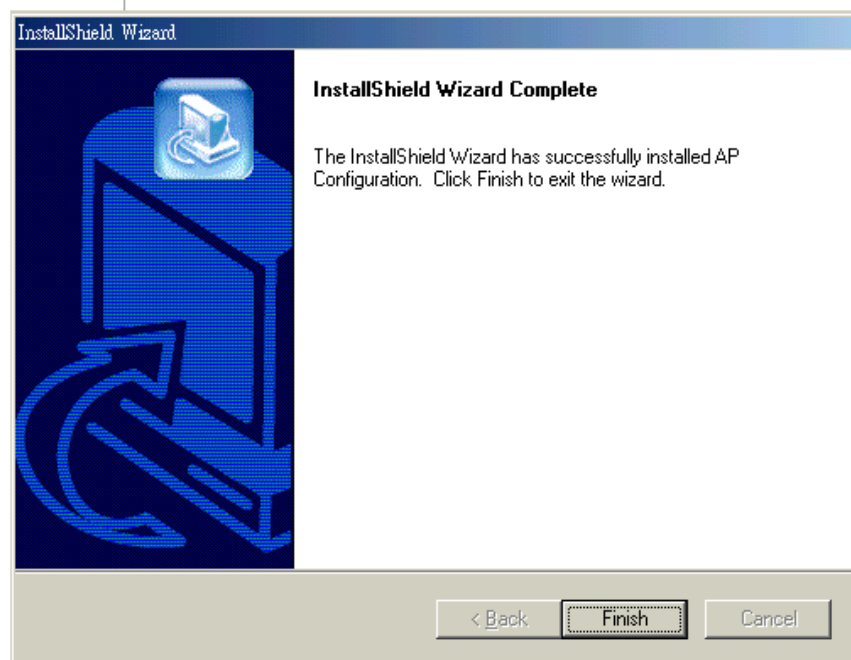
- Step 4.** Select Program Folder: Type a new folder name or select one from the Existing Folders list. Click “Next”.



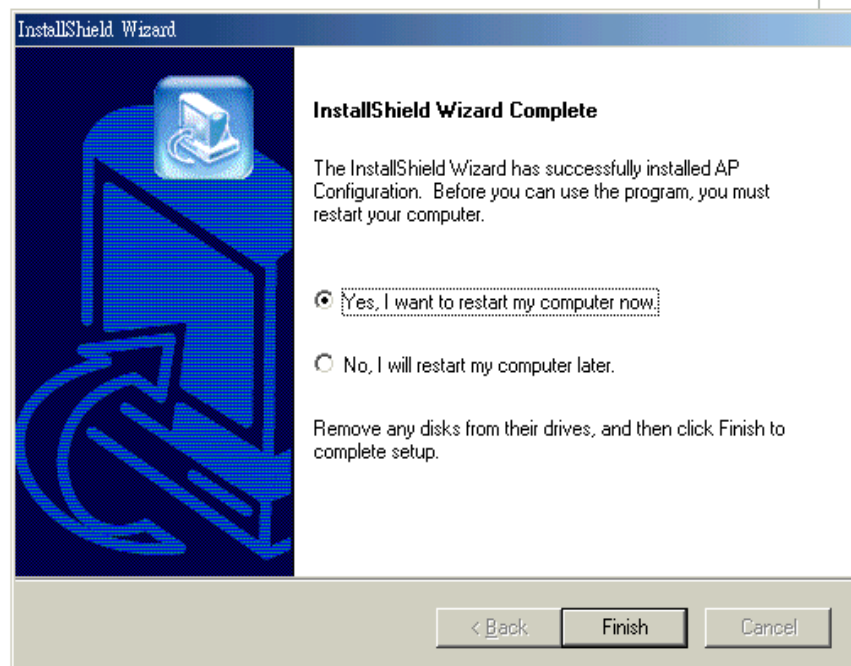
- Step 5.** Start Copying Files: Review the settings before copying files. If necessary, click “Back” to make changes. Click “Next” to star copying.



Step 6. Congratulations, AP Configuration is successfully installed! Click “Finish”.

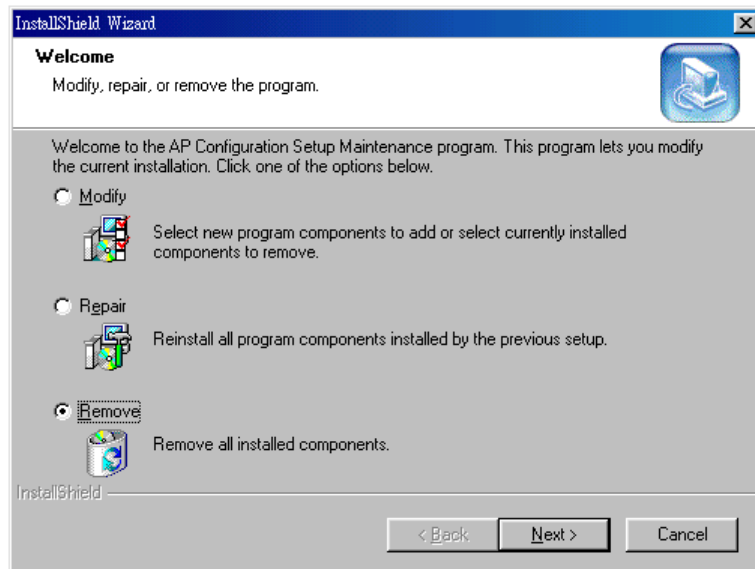


Step 7. You have to restart your computer. Choose to restart now or later. Click “Finish”.

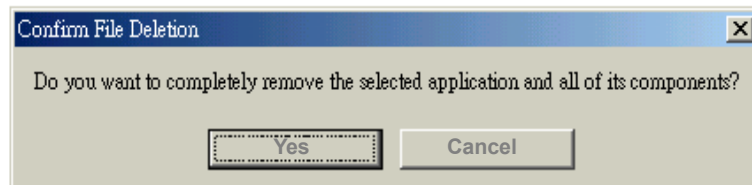


3.3 Uninstall SNMP Manager

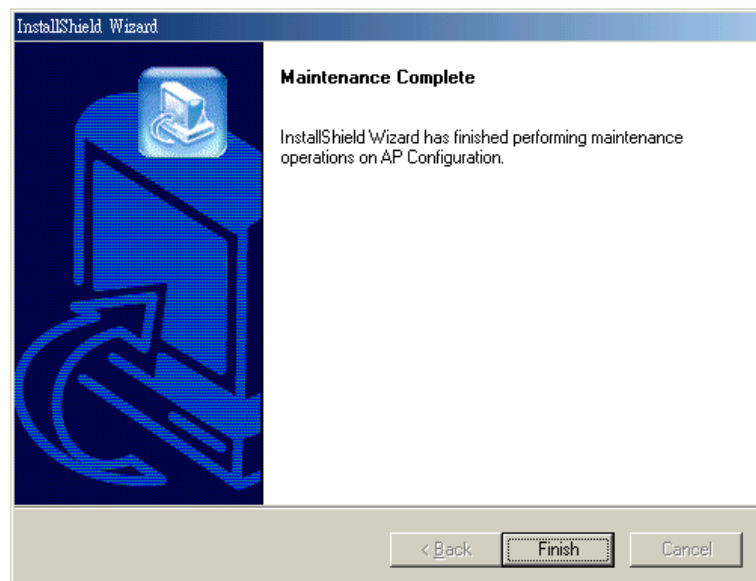
Step1. Click Start>Programs>IEEE802.11b WLAN Utilities>AP Configuration>Uninstall AP Configuration. Select “Remove” and Click “Next”



Step 2. Click “Yes”.



Step 3. Uninstallation is complete. Click “Finish”.



4. Using Access Point SNMP Manager

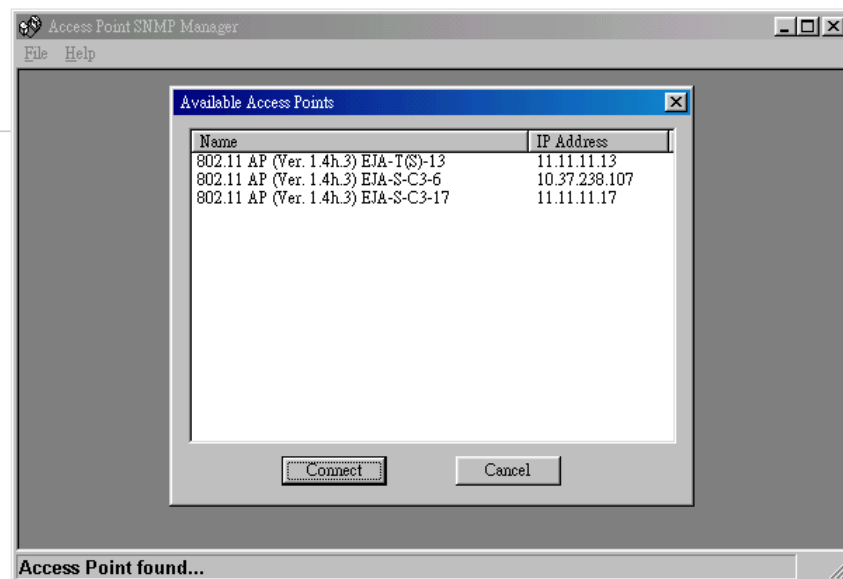
4.1 Connecting to the Access Point

- Follow the steps to connect to the Access Point:

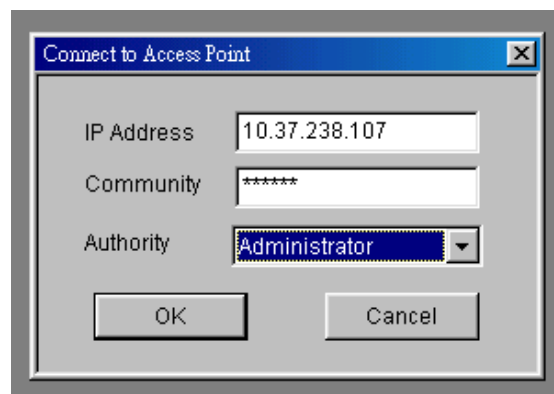
Step 1. On the Start Menu, click Start>Programs>IEEE802.11b WLAN Utilities>AP Configuration>AP Configuration.

Step 2. On the File Menu, click File>Find Access Point. After searching, you can see the list of all available Access Points.

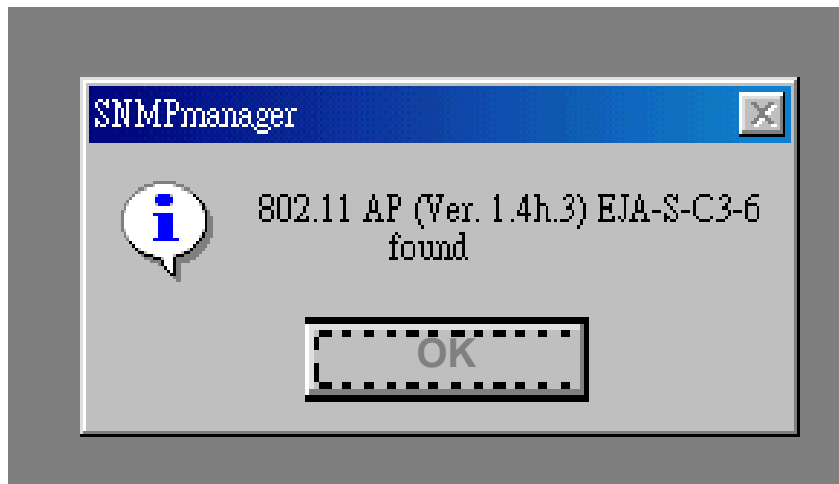
Step 3. Select one Access Point and click on it's Name and click Connect or simply double click on the Name.



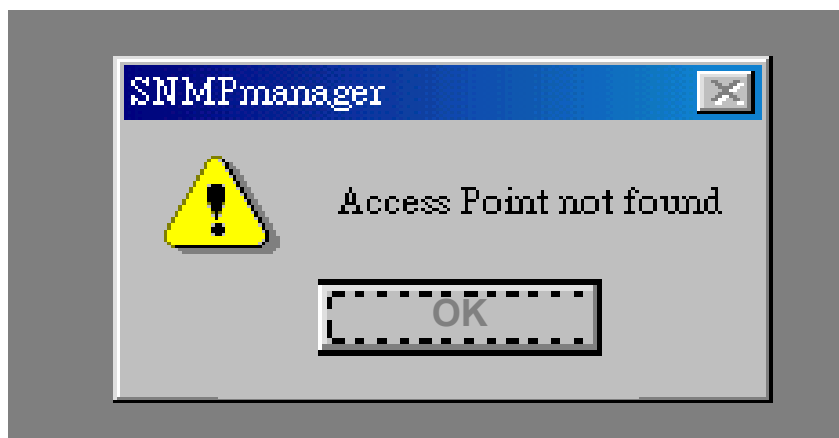
Step 4. The IP address of the Access Point will be shown automatically. Type “public” in the Community field. Select “User” or “Administrator” in Authority field and then press OK.



Step 5. When the chosen Access Point is found, click “OK”



If the designated Access Point is not found, an error message appears. Click “OK” and try to find another Access Point.



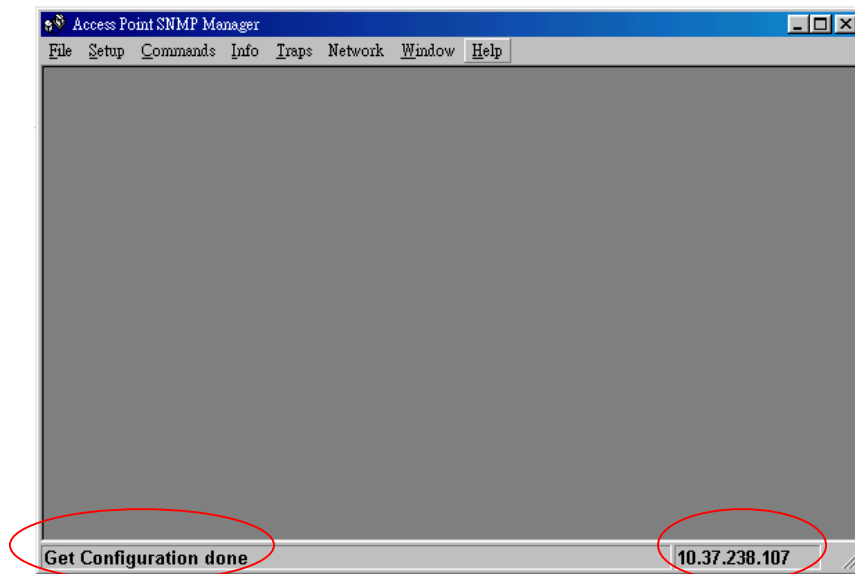
Note! You may ping the Access Point to see if the Access Point has the correct IP address and is connected to the network properly.

Step 6. If you want to exit Access Point SNMP Manager, select File>Exit.

- To view the version of the Access Point SNMP Manager, click Help>About SNMP Manager.
- To get help with connecting to the Access Point, click Help>Help Topics.

4.2 Configuring the Access Point

Once the connection has been completed, you can see two messages in the bottom of the window. The one in the left indicates “Get Configuration done”; the other one in the right display the IP address of the connected Access Point.



4.2.1 Setting the IP address of the Access Point

To set the IP address of the Access Point, follow the steps:

Step 1. Click Setup>Bridge>IP Configuration

Step 2. When Bridge IP Configuration page displays, set the new IP address, IP Mask, and Gateway, and then click OK. If the network uses DHCP server, simply select the check box of the “DHCP Enable” and click OK. In DHCP network, the IP address will be assigned automatically.

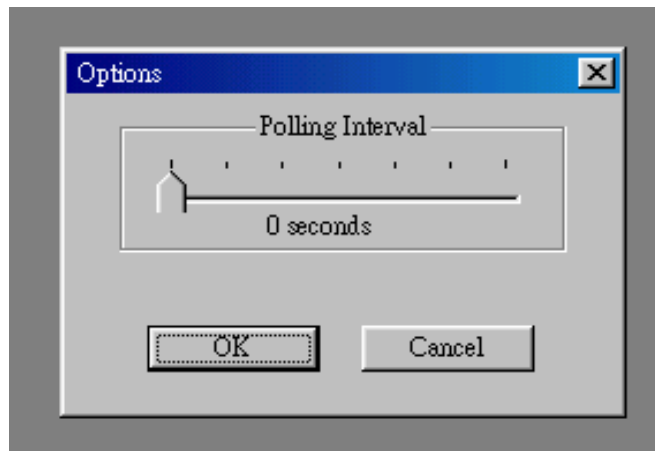
Step 3. Click File>Download Changes to save and implement the changes.

Details of each submenus are listed as follows:

4.2.2 File Menu

- **Close Connection AP:** Terminates the connection with the Access Point.
- **Download Changes:** Allows you to save any changes made for settings.
- **Refresh:** Used when you want to close the current connection and reconnect to the Access Point again.

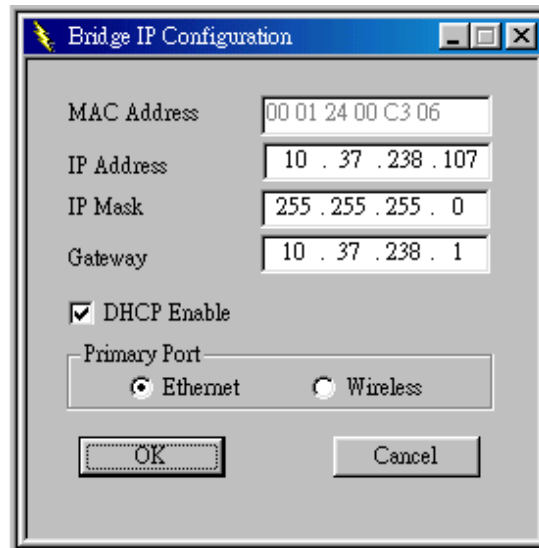
- **Options:** Indicates the polling interval according to which the SNMP Manager polls the Access Point in order to update the statistics and the Associated Stations List. The default value is 0 seconds.



- **Exit:** Exits Access Point SNMP Manager.

4.2.3 Setup Menu

- **IP Configuration:** Click Setup>Bridge>IP Configuration. If you modify any settings in this window, don't forget to save them by clicking File>Download Changes.

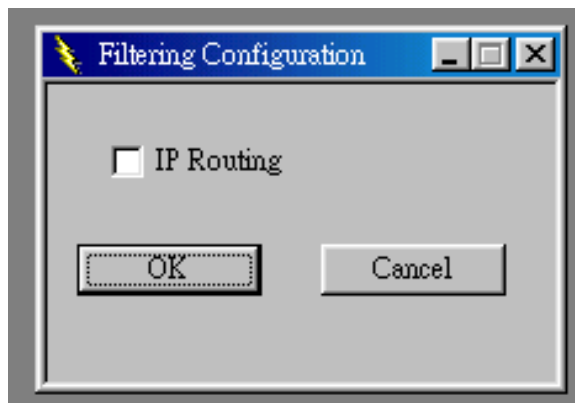


1. **MAC Address:** Stands for Media Access Control. The physical address of a device connected to a network expressed as a 48-bit hexadecimal number. This parameter cannot be changed.
2. **IP Address:** Indicates the Network-assigned Internet Protocol address of the Access Point.
3. **IP Mask:** A number used to identify a subnetwork when multiple networks share an IP address.

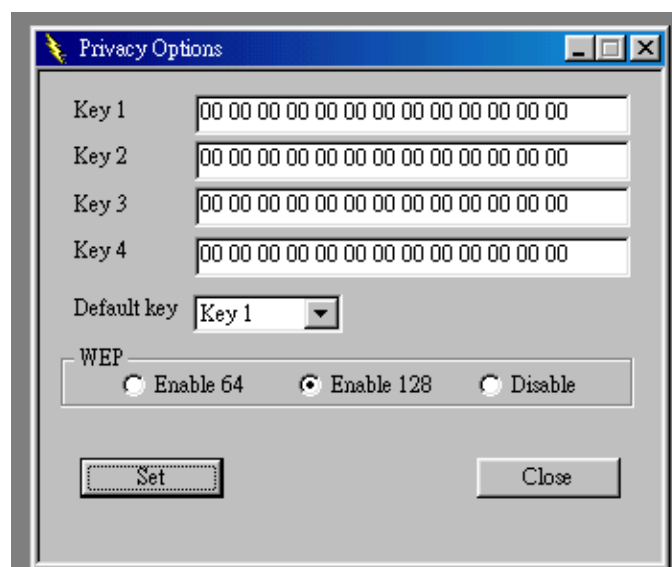
4. **Gateway:** Indicates the IP address of the gateway been used currently.
5. **DHCP Enable:** DHCP stands for Dynamic Host Configuration Protocol. Select the check box to enable DHCP which automatically assigns an IP address to each device connected to the network.

- **Filtering:** Click Setup>Bridge>Filtering.

1. IP Routing: Select or clean the check box of IP Routing.

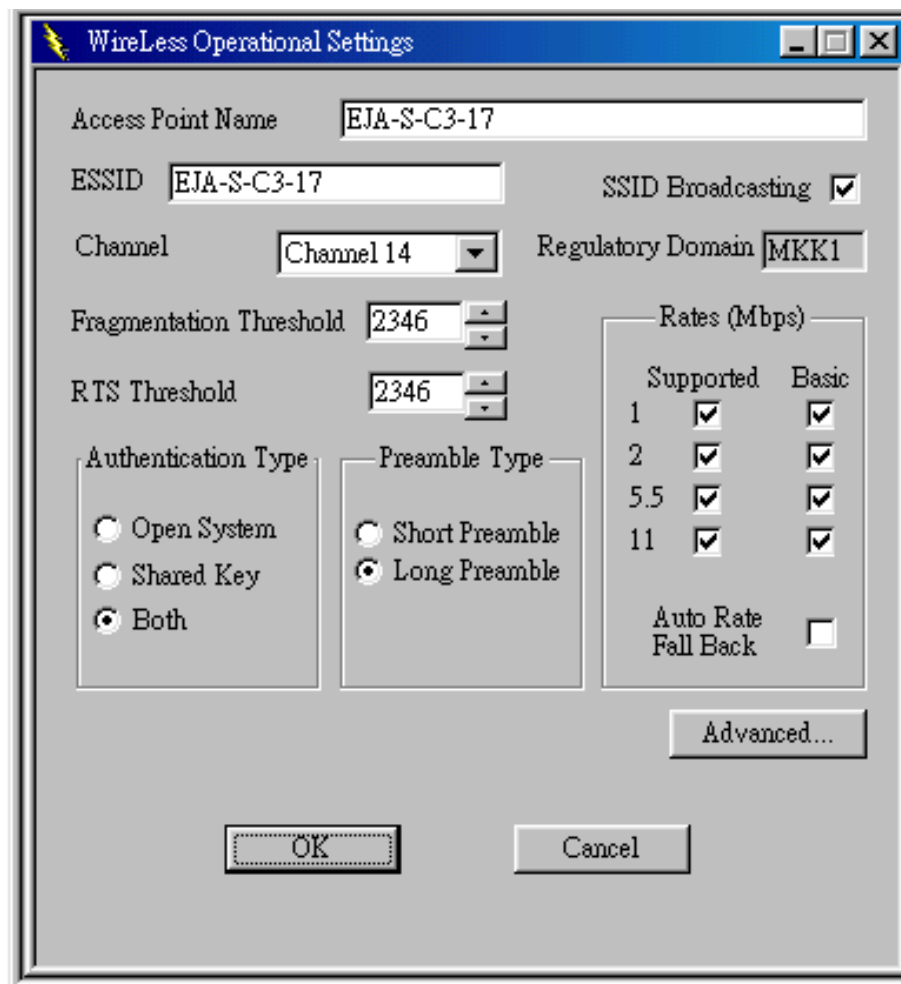


- **Privacy Options:** Click Setup>Wireless LAN>Privacy Option to set the WEP to secure the transmissions between the stations and the Access Point. In Privacy Options, define the encryption key values of your choice. Key1~Key4 are four 5 Hex digit encryption keys. The key is enabled only if it is selected in the "Default key" field. Press Set to save the encryption key data.



1. **Enable 64 (64-bit):** When 64-bit is selected, the user is required to type 10 hexadecimal values in the following range (0~F). Tap Apply to save and implement the encryption key data.
2. **Enable 128 (128-bit):** When 128-bit is selected, the user is required to type 26 hexadecimal values in the following range (0~F). The 128-bit encryption option provides a higher level of security than 64-bit encryption while maintaining an 11 Mbps data rate. Tap Apply to save the encryption key data.
3. **Disable:** This is the default setting. When Disable is selected, the encryption is disabled.

- **Operational settings:** Click Setup>Wireless LAN>Operational settings



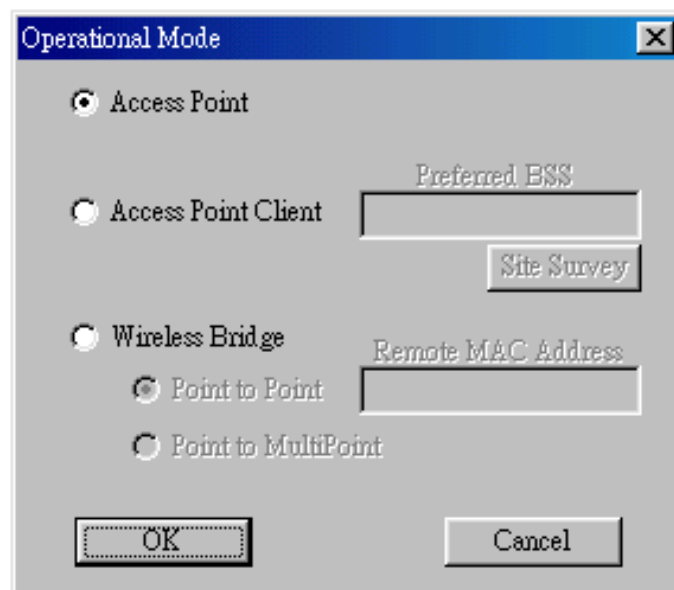
The image shows a Windows-style dialog box titled "WireLess Operational Settings". It contains various configuration fields for a wireless network. The "Access Point Name" and "ESSID" fields both contain the text "EJA-S-C3-17". The "Channel" is set to "Channel 14" and the "Regulatory Domain" is set to "MKK1". The "Fragmentation Threshold" and "RTS Threshold" are both set to "2346". The "Authentication Type" section has three radio buttons: "Open System", "Shared Key", and "Both", with "Both" selected. The "Preamble Type" section has two radio buttons: "Short Preamble" and "Long Preamble", with "Long Preamble" selected. The "Rates (Mbps)" section has a table with two columns: "Supported" and "Basic". The rows are "1", "2", "5.5", and "11", all of which have checkboxes checked in both columns. There is also an "Auto Rate Fall Back" checkbox which is unchecked. At the bottom of the dialog are "OK" and "Cancel" buttons, and an "Advanced..." button is located above the "OK" button.

Rates (Mbps)		
	Supported	Basic
1	☒	☒
2	☒	☒
5.5	☒	☒
11	☒	☒
Auto Rate Fall Back		☐

1. **Access Point Name:** Indicates the name of the Access Point been used currently.
2. **ESSID:** Enter an ESSID in this field. The ESSID is a 32-character (maximum) string identifying the wireless local area network. The

ESSID value should be the same in all stations and Access Point in the extended WLAN.

3. **Channel:** There are 14 channels available. The channels differ from country to country. Please don't illegally use the channel.
4. **Fragmentation threshold:** Indicates the size at which packets will be fragmented. You may select one within a range of 256 to 2346 bytes.
5. **RTS Threshold:** RTS stands for Request To Send. This field indicates the minimum packet size to require an RTS. When packets are smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the WLAN.
6. **Authentication Type:** Select Open System, Shared Key or Both.
Open System: Allows any station in the WLAN to associate with an Access Point and receive and transmit data.
Shared Key: Allows only stations using a shared key encryption identified by the Access Point to associate with it.
Both: Allows stations communicate with the Access Point either with or without data encryption.
7. **Preamble Type:** Select Short Preamble or Long Preamble. The short Preamble option improves throughput performance.
8. **SSID Broadcasting:** Check this box to ensure the Access Point will be found when Site-survey is executed.
9. **Regulatory Domain:** This value is set and cannot be modified.
10. **Rate:** The default setting allows the unit to adaptively select the highest possible rate. You have 4 options: 1, 2, 5.5 or 11 Mbps.
11. **Auto Rate Fall Back:** Automatically adjust the data rate depending on the transmission distance.
12. **Advanced:**



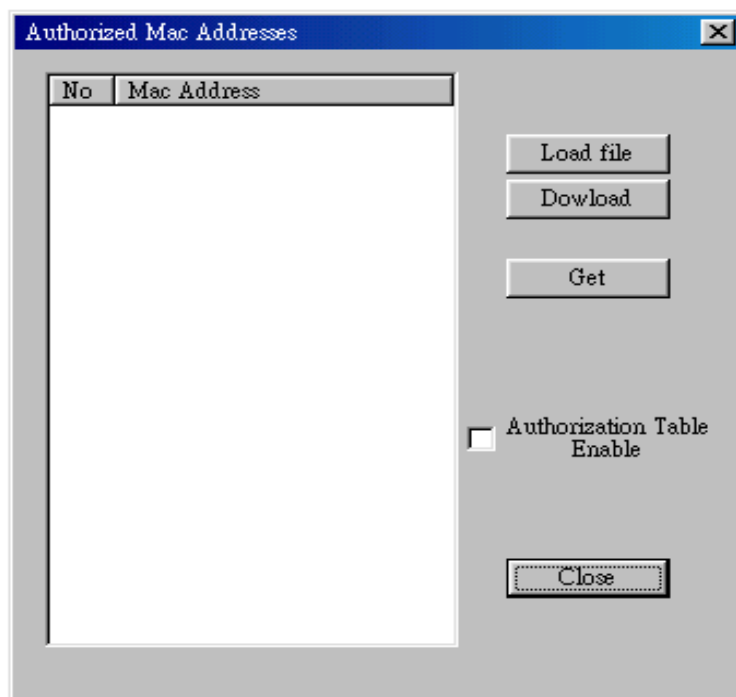
If you want to use the Access Point as a Repeater, select “Access Point Client”, and enter a proper BSSID.

If you want to use the Access Point as a Bridge, select “Wireless Bridge”.

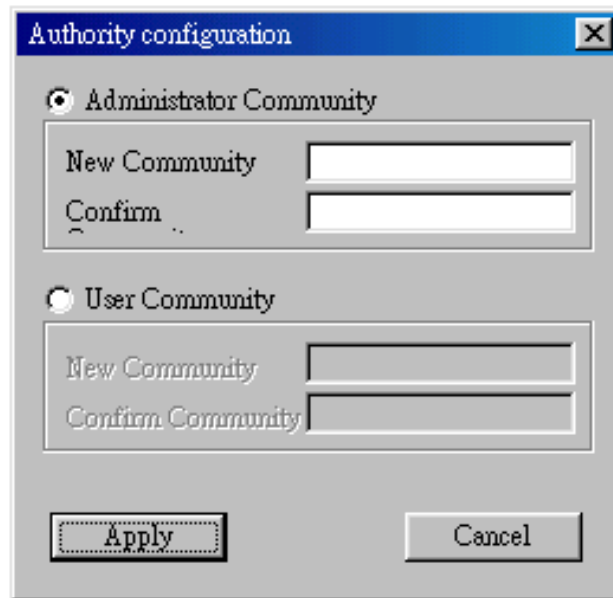
- a. Point to Point: Select Point to Point when the Access Point is connecting to the network in which has only one Access Point.
- b. Point to MultiPoint: Select Point to MultiPoint when the Access Point is connecting to the network which has more than one Access Point.

- **Authorized Mac Addresses:** Click Setup>Wireless LAN>Authorized Mac Addresses.

1. Load file: used to retrieve the MAC address list from files.
2. Download: used to assign which MAC addresses are allowed to connect to the Access Point.
3. Get: used to get all the MAC addresses of devices connecting to the Access Point currently.
4. Authorization Table Enable: Check this box to implement the function.



- **Enable SNMP Traps:** Click Setup>Enable SNMP Traps to select enable or disable SNMP Traps which are messages indicate that an action related to the Access Point took place. You can find the messages in the right bottom corner of the window.
- **Authorization:** Click Setup>Authorization.



The default code of Community is “public”. You can change the setting in this page. Once it’s been changed, next time you’ll need to enter the new community code to connect with the Access Point.

4.2.4 Commands menu

- **Reset Device:** Used to reset the Access Point. Click Commands>Reset Device.
- **Restore Defaults:** Used to restore the original default values of the Access Point. Click Commands>Restore Defaults.

4.2.5 Info menu

- **Wireless Statistics:** Where you can see the statistics report of the Wireless activity.

WireLess Statistics	
Unicast Transmitted Packets	1012
Broadcast Transmitted Packets	76876
Multicast Transmitted Packets	73344
Transmitted Beacon	82408
Transmitted ACK	1293
Transmitted RTS	0
Transmitted CTS	20
ACK Failure	121
CTS Failure	0
Retry Packets	0
FCS Error	73860
Unicast Received Packets	1388
Broadcast Received Packets	178163
Multicast Received Packets	26572
Received Beacon	0
Received ACK	1184
Received RTS	20
Received CTS	0
Received Duplicate	0
Failed Packets	0
Aged Packets	1
Invalid PLCP	77019

OK

Reset failed 10.37.238.11 1 <Trap Received>

1. **Unicast Transmitted Packets:** Indicates the number of unicast packets successfully transmitted.
2. **Broadcast Transmitted Packets:** Indicates the number of Broadcast packets transmitted.
3. **Multicast Transmitted Packets:** Indicates the number of multicast packets transmitted.
4. **Transmitted Beacon:** Indicates the number of Beacon packets transmitted.
5. **Transmitted ACK:** Indicates the number of ACK packets transmitted in response to successfully received packets.
6. **Transmitted RTS:** Indicates the number of RTS packets transmitted successfully.
7. **Transmitted CTS:** Indicates the number of CTS packets transmitted successfully.

8. **ACK Failure:** Indicates the number of packets transmitted that did not have their corresponding ACK packet received successfully.
9. **CTS Failure:** Indicates the number of packets for which no CTS packet was received in response to a RTS packet being sent.
10. **Retry Packets:** Indicate the number of packets that were retransmitted.
11. **FCS Errors:** Indicates the number of frames received with checksum errors.
12. **Unicast Received Packets:** Indicates the number of unicast packets that were successfully received.
13. **Broadcast Received:** Indicates the number of broadcast packets received successfully.
14. **Multicast Received:** Indicates the number of multicast packets received successfully.
15. **Received Beacon:** Indicates the number of Beacon packets received.
16. **Received ACK:** Indicates the number of packets transmitted that had their corresponding ACK packet received successfully.
17. **Received RTS:** Indicates the number of RTS received packets.
18. **Received CTS:** Indicates the number of CTS packets received in response to a RTS.
19. **Receive Duplicate:** Indicates the number of duplicate frames received.
20. **Failed Packets:** Indicates the number of packets not transmitted successfully.
21. **Invalid PLCP:** Indicates the number of packets received with invalid PLCP.

- **Ethernet Statistics:** Where you can read the statistics report of the Ethernet port activity.

Received Packets		Transmitted Packets	
Total Bytes	121703377	Total Bytes	154811
Total Packets	300975	Total Packets	1256
Packet CRC Errors	88	Packet CRC Errors	0
Multicast Packets	79414	Multicast Packets	37
Broadcast Packets	78940	Broadcast Packets	95
Control Frames	0	Unicast Packets	1124
Pause Frames	0	Pause Frames	0
UnknownOP Code	0	SingleDefer Packets	10
Alignment Error	49	MultiDefer Packets	0
Length Out Of Range	57490	Single Collisions	3
Code Error	0	Multi Collisions	5
False Carrier	0	Late Collisions	0
Undersize Packets	0	Excessive Collisions	0
Oversize Packets	0	Total Collisions	14
Total Fragments	88		
Total Jabber	0		

Reset failed 10.37.238.11 1 <Trap Received>

Received Packets:

1. **Total bytes:** Indicates the number of received bytes in the frames.
2. **Total packets:** Indicates total number of received packets.
3. **Packet CRC Error:** Indicates the number of packets with CRC Errors.
4. **Multicast Packets:** Indicates the number of successfully received multicast packets.
5. **Broadcast Packets:** Indicates the number of broadcast packets received.
6. **Control Frames:** Indicates the number of control frames received.
7. **Pause Frames:** Indicates the number of pause frames received successfully.
8. **Unknown OP Code:** Indicates the number of frames received which contains an opcode other than a pause.
9. **Alignment Error:** Indicates the number of alignment errors.
10. **Length Out of range:** Indicates the number of frames received in which the 802.3 length field did not match the number of data bytes actually received.
11. **Code Error:** Indicates the number of code errors received.
12. **False Carrier:** Indicates the number of false carriers.
13. **Undersize Packets:** Indicates the number of packets received which are less than 64 bytes in length and contains a valid FCS and were well formed.

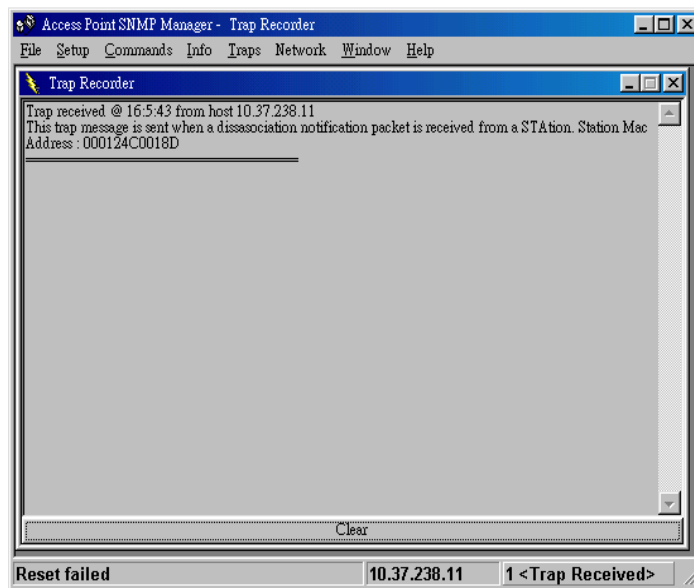
14. **Oversize Packets:** Indicates the number of packets received with exceeded 1518 bytes and contains a valid FCS and were otherwise well formed.
15. **Total Fragments:** Indicates the number of packets received, which are less than 64 bytes in length and contain an invalid FCS (include integral and non-integral lengths).
16. **Total Jabber:** Corresponds to the number of packets received, which exceed the 1518 byte length and contain an invalid FCS (include alignment errors).

Transmitted Packets:

1. **Total bytes:** Indicates the number of received bytes in the frames.
2. **Total packets:** Indicates total number of transmitted packets.
3. **Packet CRC Error:** Indicates the number of packets transmitted with CRC Errors.
4. **Multicast Packets:** Indicates the number of Multicast packets being transmitted successfully (excluded Broadcast packets).
5. **Broadcast Packets:** Indicates the number of Broadcast packets transmitted (excluding Multicast packets)
6. **Unicast Packets:** Indicates the number of unicast packets that were transmitted successfully.
7. **Pause Frame:** Indicates the number of pause control frames being transmitted.
8. **SingleDefer Packets:** Indicates the number of packets which were deferred on the first transmission attempt and did not experience any subsequence collisions during transmission.
9. **MultiDefer Packets:** Indicates the number of packets aborted which were deferred for an excessive period of time.
10. **Single Collision:** Indicates the number of single collision packets. The statistic counter register is incremented during transmission.
11. **Multi Collision:** Indicates the number of Multiple Collision Packets. It is incremented for each frame transmitted which had 2-15 collisions (including any late collisions) during transmission.
12. **Late Collision:** Indicates the number of late collision packets. It is incremented for each packet transmitted which had a late collision during a transmission attempt.
13. **Excessive Collision:** Indicates the number of Excessive Collision packets. It is incremented for each frame which had 16 collisions during transmission and was aborted.
14. **Total Collision:** Indicates the number of collisions occurred during the transmission of a frame defined as the simultaneous presence of signals on the DO and RD circuits.

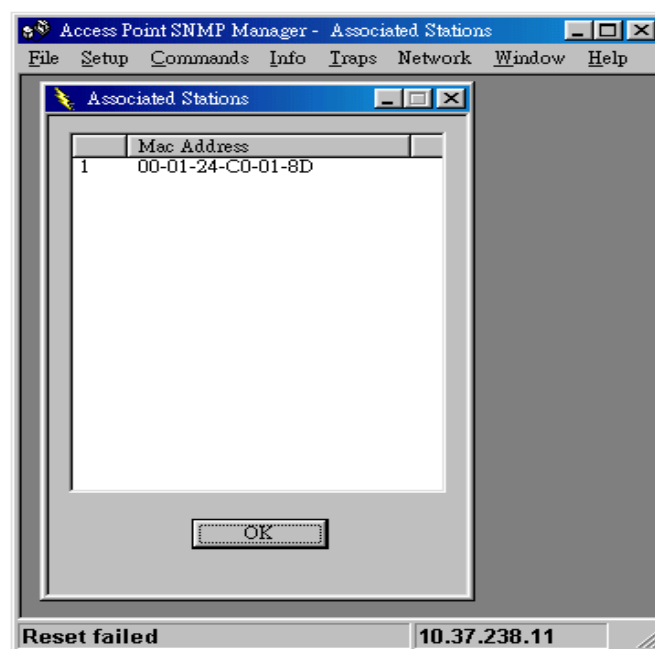
4.2.6 Traps menu

- View Record: Provides additional information for every Trap Message.



4.2.7 Network menu:

- Associated Stations: Provides MAC Addresses of the Associated stations with the Access Point.



4.2.8 Window menu

- Cascade: Windows been opened are positioned in a cascade fashion.
- Tile: All opened windows are visible on the desktop.

4.2.9 Help menu: Provides on line help.

5. Glossary

BSS	‘Basic Service Set’. A set of 802.11-compliant stations that operate as a fully-connected wireless network.
Cell	Area in which the radio signal of an Access Point is sufficiently good to join with it.
ESS	‘Extended Service Set’. A group of Access Points with identical settings among which a client system can roam. An ESS forms the heart of WLAN
Shared Key Algorithm	Encryption scheme for which both sender and receiver need to know the (same) encryption key
SNMP	Simple Network Management Protocol
WLAN	‘Wireless LAN’ the set of Access Points and Wireless Clients that form a local area network.
Write Community String	SNMP Password
WEP	‘Wired Equivalent Protection’ Data privacy mechanism based on a 64bit shared key algorithm, as described in the IEEE 802.11b standard

More about Cells

Each Access Point in the network forms the center of a cell, or BSS. The Cells should overlap slightly to guarantee seamless wireless connectivity everywhere. Nearby Access Points should preferably send and receive on different channels for maximum

throughput.

Creating a cell plan for your site can be complicated, and is usually done by experts employing special measuring equipment.

Furthermore, the radio channels you may use depend on both the capabilities of the PC-Cards you are deploying, as well as the regulations in your area. The following table may be of help:

<u>Regulatory Domain</u>	<u>Area</u>	<u>Permissible Channels</u>	<u>Preferred channels</u>
FCC	United States	1 ~ 11	1, 6, 11
IC	Canada	1 ~ 11	1, 6, 11
ETSI	Europe except Spain and France	1 ~ 13	1, 7, 13
SPAIN	Spain	10 ~ 11	11
FRANCE	France	10 ~ 13	11
MKK	Japan	1 ~ 13	1, 7, 13

6. Technical Specifications

Frequency range	2.4G ~ 2.4835Ghz	
Modulation technique	DQPSK/DBPSK/CCK	
Form factor	EJA-B housing	EJA-A housing
Channels support	- US/Canada: 11 (1 ~ 11) - Major European country: 13 (1 ~ 13) - France: 4 (10 ~ 13) - Spain: 2 (10 ~ 11) - Japan: 13 (1 ~ 13) or 1 (14th)	
Operation voltage	5V	
Operation range	- Indoor: 35 meter @ 11Mbps - Outdoor: 150 meter @ 11Mbps	- Indoor: 35 meter @ 11Mbps - Outdoor: 150 meter @ 11Mbps
Operation system	➤ ThreatX RTOS inside ➤ Support Windows 98SE, Me, 2K, XP subject to support without notify	
Dimension	146.5mm(L)*220mm(W)*34.7mm(H)	120.5mm(L)*82mm(W)*29.2mm(H)
Network protocol	Support SNMP	
Security	WEP-64, WEP-128 encryption	
Transfer data rate	11Mbps, 5.5Mbps, 2Mbps, 1Mbps , auto-rate	
Operation temperature range	0°C ~ 60°C	
Storage temperature range	-20°C ~ 70°C	
Storage Humidity	95% max	
Warranty	1 year standard warranty, 3 years optional	
Logo	Wi-Fi compliant	
EMC certificate	- FCC part 15 (USA) - IC RSS210 (Canada) - ETSI 300 328, ETSI300 826 (Europe) - TELEC (Japan) - << above certificate to be submit upon requested>>	
Media access protocol	CSMA/CA with ACK	

architecture	32-bit MAC	
LED indicator	<u>three LED on front panel:</u> Power LED: indicate power connector is plugged Wired LED: indicate wired 802.3 active Wireless TX/RX LED: wireless networking activity	
Antenna	External diversity antenna with connectors for replacing a building-to-building antenna (optional)	Internal diversity embedded antenna
Rear outlay	RJ-45 for 10/100-baseT DC connector Hard reset	RJ-45 for 10/100-baseT DC connector Hard reset