

54/108Mbps Super G Wireless LAN Managed Access Point

WAP-4060PE

User's Manual



Copyright

Copyright© 2005 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes..

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission 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 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 instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which 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:

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

FCC Caution:

To assure continued compliance.(example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm(8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Revision

User's Manual for PLANET 802.11g Wireless LAN Managed Access Point

Model: WAP-4060PE

Rev: 1.0 (January, 2005)

Part No. EM-WAP4060

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1
1.1 Package Contents	1
1.2 System Requirements	1
1.3 Features	1
1.4 Physical Details	2
1.5 Specification	3
1.6 Wireless Performance	4
CHAPTER 2 INSTALLATION	6
2.1 General Installation	6
2.2 Using PoE (Power over Ethernet)	6
CHAPTER 3 ACCESS POINT SETUP	7
3.1 Overview	7
3.2 Setup using the Windows Utility	7
3.2.1 Main Screen	7
3.2.2 Setup Procedure	8
3.3 Setup using a Web Browser	8
3.3.1 Setup Procedure	8
3.4 Access Control	10
3.4.1 Trusted Wireless Stations	10
3.5 Security Profiles	12
3.5.1 VLAN Configuration Screen	14
3.6 Configure Security Profile	16
3.6.1 Profile Data	16
3.6.2 Security Settings	16
3.6.3 Security Settings - None	17
3.6.4 Radius MAC Authentication	17
3.6.5 UAM	19
3.6.6 Security Settings - WEP	21
3.6.7 Security Settings - WPA-PSK	23
3.6.8 Security Settings - WPA-802.1x	24
3.6.9 Security Settings - 802.1x	27
3.7 System Screen	29
3.8 2.4GHz Wireless	30
3.8.1 Basic Settings Screen	30
3.8.2 Advanced Settings	33
CHAPTER 4 PC AND SERVER CONFIGURATION	36
4.1 Overview	36
4.2 Using WEP	36
4.3 Using WPA-PSK	36
4.4 Using WPA-802.1x	37
4.5 802.1x Server Setup (Windows 2000 Server)	37
4.5.1 Windows 2000 Domain Controller Setup	38
4.5.2 Services Installation	38
4.5.3 DHCP server configuration	39
4.5.4 Certificate Authority Setup	41
4.5.5 Internet Authentication Service (Radius) Setup	44
4.5.6 Grant Remote Access for Users	45
4.6 802.1x Client Setup on Windows XP	46
4.6.1 Client Certificate Setup	46

4.6.2 802.1x Authentication Setup	49
4.7 Using 802.1x Mode (without WPA)	52
CHAPTER 5 OPERATION AND STATUS	53
5.1 Operation	53
5.2 Status Screen	53
5.3.1 Statistics Screen	55
5.3.2 Profile Status.....	56
5.3.3 Activity Log.....	57
5.3.4 Station List	58
CHAPTER 6 MANAGEMENT.....	59
6.1 Overview	59
6.2 Admin Login Screen	59
6.3 Auto Config/Update	60
6.4 Config File.....	62
6.5 Log Settings (Syslog)	64
6.6 Rogue APs	64
6.7 SNMP.....	65
6.8 Upgrade Firmware.....	67
APPENDIX A SPECIFICATIONS	68
APPENDIX B TROUBLESHOOTING	70
APPENDIX C COMMAND LINE INTERFACE	71
C.1 Using the CLI - Telnet	71
C.2 Using the CLI - Serial Port	71
C.3 Command Reference.....	72

Chapter 1

Introduction



WAP-4060PE is an IEEE 802.11g Wireless Access Point with PoE. Catering to the enterprise demands, WAP-4060PE enhances security and management features, including multiple SSIDs, VLAN support, WPA support, RADIUS MAC authentication, rogue AP detection, and so on. The LAN port of WAP-4060PE is 802.3af compliant. Therefore, it can be installed anywhere without the constraint on power socket. Provided with one reversed-polarity SMA male connector, WAP-4060PE is easy to connect external antenna and booster to extend the wireless distance.

1.1 Package Contents

Make sure that you have the following items:

- WAP-4060PE
- Dipole Antenna
- Quick Installation Guide
- User's manual CD-ROM
- Power Adapter

Note:

If any of the above items are missing, contact your supplier as soon as possible.

1.2 System Requirements

Before installation, please check the following requirements with your equipment.

- Pentium Based (And Above) IBM-Compatible PC System
- CD-ROM drive
- Windows 98/ME/2000/XP Operating System with TCP/IP protocol

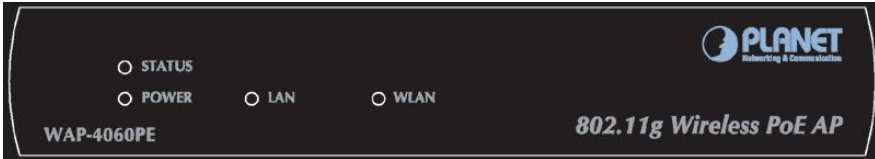
1.3 Features

- Wireless LAN IEEE802.11g and IEEE802.11b compliant
- Support PoE port (IEEE802.3af compliant)
- Support IEEE802.11d standard (Worldwide mode)
- Strong network security with 802.1X authentication, and 64/128-bit WEP encryption
- Supports WPA (Wi-Fi Protected Access) for both 802.1x and WPA-PSK
- One detachable reverse-polarity SMA connectors can connect to external antenna for expanding connection distance
- Super G mode efficiently raises the data transfer rate up to 108Mbps
- Five operation modes selectable: AP / AP Client / Wireless Bridge / Multiple Bridge / Repeater
- Adjustable output power level
- Support Multiple SSIDs, Multiple SSID isolation, 802.1Q VLAN, RADIUS MAC authentication, Rogue AP detection, Access Control

- Provide Windows-base utility, Web, and CLI (Command Line Interface) Configuration
- SNMP support

1.4 Physical Details

Front panel



- STATUS** **On** - Error condition.
 Off - Normal operation.
 Blinking - During start up, and when the Firmware is being upgraded.
- POWER** **On** - Normal operation.
 Off - No power
- LAN** **On** - The LAN (Ethernet) port is active.
 Off - No active connection on the LAN (Ethernet) port.
 Flashing - Data is being transmitted or received via the corresponding LAN (Ethernet) port.
- WLAN** **On** - Idle
 Off - Error- Wireless connection is not available.
 Flashing - Data is being transmitted or received via the Wireless access point. Data includes "network traffic" as well as user data.

Rear panel



- ANT** One dipole antenna is supplied. Best results are usually obtained with the antenna in a vertical position.
- CONSOLE** DB9 female RS232 port.
- RESET Button** This button has two (2) functions:
- **Reboot.** When pressed and released, the WAP-4060PE will reboot (restart).
 - **Reset to Factory Defaults.** This button can also be used to clear ALL data and restore ALL settings to the factory default values.
- To Clear All Data and restore the factory default values:**
1. Power Off the WAP-4060PE.
 2. Hold the Reset Button down while you Power On the device.

3. Continue holding the Reset Button until the Status (Red) LED blinks TWICE.
4. Release the Reset Button.
The factory default configuration has now been restored, and the WAP-4060PE is ready for use.

LAN (PoE) Use a standard LAN cable (RJ45 connectors) to connect this port to a 10BaseT or 100BaseT hub on your LAN.

Power port Connect the supplied power adapter here.

1.5 Specification

Standard	IEEE 802.11b, 802.11g	
Signal Type	DSSS (Direct Sequence Spread Spectrum)	
Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK	
Port	10/100Mbps RJ-45 port * 1, 802.3af compliant	
Antenna Connector	Reverse SMA male * 1	
Output Power	18dBm	
Sensitivity	802.11b	11 Mbps (CCK): -85dBm 5.5 Mbps (QPSK): - 89dBm 1, 2 Mbps (BPSK): - 90dBm (typically @PER < 8% packet size 1024 and @25°C ± 5°C)
	802.11g	54 Mbps: -72dBm 48 Mbps: - 72dBm 36 Mbps: -76dBm 24 Mbps: -79dBm 18 Mbps: -82dBm 12 Mbps: -86dBm 9 Mbps: -89dBm 6 Mbps: -90dBm (typically @PER < 8% packet size 1024 and @25°C + 5°C)
Operating Mode	AP, AP Client, Wireless Bridge, Multiple Bridge, Repeater	
Security	Open, shared, WPA, and WPA-PSK authentication 802.1x support EAP-TLS, EAP-TTLS, PEAP Block inter-wireless station communication Block SSID broadcast	

Management	Web based configuration RADIUS Accounting RADIUS-On feature RADIUS Accounting update CLI Message Log Access Control list file support Configuration file Backup/Restore Statistics support Device discovery program Windows Utility	
Data Rate	Super G mode	Up to 108Mbps
	802.11g	Up to 54Mbps (6/9/12/18/24/36/48/54)
	802.11b	Up to 11Mbps (1/2/5.5/11)
Dimensions (L x W x H)	150 x 102 x 30mm	
Weight	210g	
Environmental Specification	Operating temperature: 0 – 40 degree C	
	Storage temperature: -20 – 70 degree C	
	Relative humidity: 0% – 90% (non-condensing)	
Power Requirement	24V DC, 0.5A	
Electromagnetic Compatibility	FCC, CE	

1.6 Wireless Performance

The following information will help you utilizing the wireless performance, and operating coverage of WAP-4060PE.

1. Site selection

To avoid interferences, please locate WAP-4060PE and wireless clients away from transformers, microwave ovens, heavy-duty motors, refrigerators, fluorescent lights, and other industrial equipments. Keep the number of walls, or ceilings between AP and clients as few as possible; otherwise the signal strength may be seriously reduced. Place WAP-4060PE in open space or add additional WAP-4060PE as needed to improve the coverage.

2. Environmental factors

The wireless network is easily affected by many environmental factors. Every environment is unique with different obstacles, construction materials, weather, etc. It is hard to determine the exact operating range of WAP-4060PE in a specific location without testing.

3. Antenna adjustment

The bundled antenna of WAP-4060PE is adjustable. Firstly install the antenna pointing straight up, then smoothly adjust it if the radio signal strength is poor. But the signal reception is definitely weak in some certain areas, such as location right down the antenna.

Moreover, the original antenna of WAP-4060PE can be replaced with other external antennas to extend the coverage. Please check the specification of the antenna you want to use, and make sure it can be used on WAP-4060PE.

4. WLAN type

If WAP-4060PE is installed in an 802.11b and 802.11g mixed WLAN, its performance will be reduced significantly. Because every 802.11g OFDM packet needs to be preceded by an RTS-CTS or CTS packet exchange that can be recognized by legacy 802.11b devices. This additional overhead lowers the speed. If there are no 802.11b devices connected, or if connections to all 802.11b devices are denied so that WAP-4060PE can operate in 11g-only mode, then its data rate should actually be 54Mbps and 108Mbps in Super G mode.

Chapter 2

Installation

2

2.1 General Installation

Before you proceed with the installation, it is necessary that you have enough information about the WAP-4060PE.

- 1. Locate an optimum location for the WAP-4060PE.** The best place for your WAP-4060PE is usually at the center of your wireless network, with line of sight to all of your mobile stations.
- 2. Assemble the antenna to WAP-4060PE.** Try to place them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity.
- 3. Connect RJ-45 cable to WAP-4060PE.** Connect this WAP-4060PE to your LAN switch/hub or a single PC.
- 4. Plug in power adapter and connect to power source.** After power on, WAP-4060PE will start to operate.

Note: ONLY use the power adapter supplied with the WAP-4060PE. Otherwise, the product may be damaged.

2.2 Using PoE (Power over Ethernet)

The LAN port of WAP-4060PE supports PoE. Before you proceed with the PoE installation, please make sure the PoE adapter or switch is 802.3af compliant.

1. Do not connect the supplied power adapter to the WAP-4060PE.
2. Connect one end of a standard (category 5) LAN cable to the Ethernet port on the WAP-4060PE.
3. Connect the other end of the LAN cable to the powered Ethernet port on a suitable PoE Adapter or switch. (IEEE 802.3af compliant)
4. Connect the unpowered Ethernet port on the PoE adapter to your Hub or switch.
5. Connect the power supply to the PoE adapter and power up.
6. Check the LEDs on the WAP-4060PE to see it is drawing power via the Ethernet connection.



Chapter 3

Access Point Setup

3

3.1 Overview

This chapter describes the setup procedure to make the WAP-4060PE a valid device on your LAN, and to function as an Access Point for your Wireless Stations.

The WAP-4060PE can be configured using either the supplied Windows utility or the Web Browser

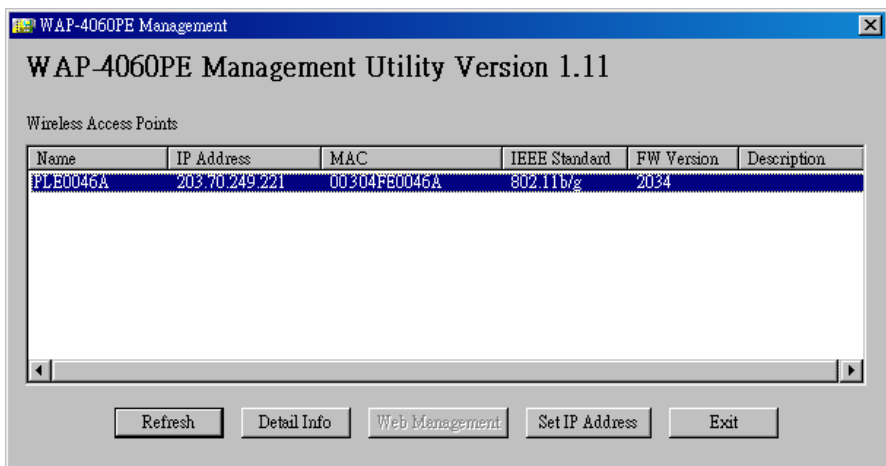
3.2 Setup using the Windows Utility

A simple Windows setup utility is supplied on the CD-ROM. This utility can be used to assign a suitable IP address to the WAP-4060PE. Using this utility is recommended, because it can locate the WAP-4060PE even if it has an invalid IP address.

1. Insert the User's Manual and Utility CD into the CD-ROM drive.
2. Once the menu screen appears, click on the "WAP-4060PE Manager" hyperlink for installation. If the menu screen does not appear, you can click the **Start** button and choose **Run**. When the dialog box appears, enter **E:\Utility\setup.exe** (Assume "E" is your CD-ROM drive). Follow the prompts to complete the installation.
3. After the installation completes, you can start this utility from "Start">"Program Files">"Planet">"WAP-4060PE Manager".

3.2.1 Main Screen

When the utility is executed, it searches the network for all active WAP-4060PE, and lists them on screen, as shown by the example below.



Wireless Access Points

The main panel displays a list of all Wireless Access Points found on the network. For each Access Point, the following data is shown:

Name	The device name of the WAP-4060PE.
------	------------------------------------

IP address	The IP address for the WAP-4060PE.
MAC Address	The hardware or physical address of the WAP-4060PE.
IEEE Standard	The wireless standard or standards used by the WAP-4060PE (e.g. 802.11b, 802.11g)
FW Version	The current Firmware version installed in the WAP-4060PE.
Description	Any extra information for the WAP-4060PE, entered by the administrator.

Note: If the desired device is not listed, check that the device is installed and powered on, then update the list by clicking the *Refresh* button.

Buttons

Refresh	Click this button to update the Wireless Access Point device listing after changing the name or IP Address.
Detail Info	When clicked, additional information about the selected device will be displayed.
Web Management	Use this button to connect to the WAP-4060PE's Web-based management interface.
Set IP Address	Click this button if you want to change the IP Address of the Wireless Access Point.
Exit	Exit the Management utility program by clicking this button.

3.2.2 Setup Procedure

1. Select the desired Wireless Access Point from the list.
2. Click the Set IP Address button.
3. If prompted, enter the user name and password. The default values are "admin" for the User Name, and "password" for the Password.
4. Ensure the IP address, Network Mask, and Gateway settings are correct for your LAN. Save any changes.
5. The initial IP address setup is now completed. You can click on the "Web Management" button to access the web interface of WAP-4060PE for more configurations.

3.3 Setup using a Web Browser

Your Browser must support JavaScript. The configuration program has been tested on the following browsers:

- Netscape V4.08 or later
- Internet Explorer V4 or later

3.3.1 Setup Procedure

Before proceeding, please install the WAP-4060PE in your LAN, as described previously.

1. Use a PC which is already connected to your LAN, and start the Web browser.
2. In the *Address* box, enter the IP address of the WAP-4060PE you want to cobnfigure.
3. You should then see a login prompt, which will ask for a *User Name* and *Password*. Enter **admin** for the *User Name*, and **password** for the *Password*.

These are the default values. The password can and should be changed. Always enter the current user name and password, as set on the *Admin Login* screen.

- You will then see the *Status* screen, which displays the current settings and status. No data input is possible on this screen.

PLANET Networking & Communication **802.11g PoE Access Point**

Access Control

Security Profiles

System

Status

2.4 GHz Wireless

- Basic
- Advanced

Management

- Admin Login
- Auto Config/Update
- Config File
- Log Settings
- Rogue APs
- SNMP
- Upgrade Firmware

Status

Access Point

Access Point Name PLE0046A
 MAC Address 00:30:4F:E0:04:6A
 Domain Unspecified
 Firmware Version Version 2.0 Release 34

TCP/IP

IP Address 192.168.99.26
 Subnet Mask 255.255.255.0
 Gateway 192.168.99.253
 DHCP Client Disabled

Wireless

Channel/Frequency 1 (Automatic)
 Wireless Mode 802.11b and 802.11g
 AP Mode Access Point
 Bridge Mode None (disable)

Security Profiles

2.4 GHz Statistics

Name	SSID	Status
wireless	wireless	Enabled
Profile02	wireless	Disabled

Logout

- From the menu, check the following screens, and configure as necessary for your environment. Details of these screens and settings are described in the following subsections of this chapter.
 - Access Control** - MAC level access control.
 - Security Profiles** - Wireless security.
 - System** - Identification, location, and Network settings
 - Wireless** - Basic & Advanced
- You may also need to set the admin password and administration connection options. These are on the *Admin Login* screen accessed from the **Management** menu. See Chapter 6 for details of the screens and features available on the **Management** menu.
- Use the **Apply/Restart** button on the menu to apply your changes and restart the Wireless Access Point.

If you can't connect:

It is likely that your PC's IP address is incompatible with the WAP-4060PE's IP address. This can happen if your LAN does not have a DHCP Server. The default IP address of the Wireless Access Point is 192.168.0.228, with a Network Mask of 255.255.255.0.

If your PC's IP address is not compatible with this, you must change your PC's IP address to an unused value in the range 192.168.0.1 ~ 192.168.0.254, with a Network Mask of 255.255.255.0.

3.4 Access Control

This feature allows you to block certain access from unknown or distrusted wireless stations.

Click *Access Control* on the menu to view a screen like the following.

Access Control

Enable Enable Access Control by MAC Address

Trusted Stations

Name	Mac Address	Connected
------	-------------	-----------

Modify List

Read from File Write to File

Save Cancel Help

Data - Access Control Screen

Enable	Use this checkbox to Enable or Disable this feature as desired. Warning: Ensure your own PC is in the "Trusted Wireless Stations" list before enabling this feature.
Trusted Stations	This table lists any Wireless Stations you have designated as "Trusted". If you have not added any stations, this table will be empty. For each Wireless station, the following data is displayed: <ul style="list-style-type: none">• MAC Address - the MAC or physical address of each Wireless station.• Connected - this indicates whether or not the Wireless station is currently associates with this Access Point.
Buttons	
Modify List	To change the list of Trusted Stations (Add, Edit, or Delete a Wireless Station or Stations), click this button. You will then see the <i>Trusted Wireless Stations</i> screen, described below.
Read from File	To upload a list of Trusted Stations from a file on your PC, click this button.
Write to File	To download the current list of Trusted Stations from the WAP-4060PE to a file on your PC, click this button.

3.4.1 Trusted Wireless Stations

To change the list of trusted wireless stations, use the *Modify List* button on the *Access Control* screen. You will see a screen like the sample below.

Trusted Wireless Stations

Data - Trusted Wireless Stations

Trusted Wireless Stations	Here lists all Wireless Stations which you have designated as "Trusted".
Other Wireless Stations	Here lists all Wireless Stations detected by the WAP-4060PE, which you have not designated as "Trusted".
Name	The name assigned to the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Address	The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Buttons	
<<	<p>Add a Trusted Wireless Station (move from the "Other Stations" list).</p> <ul style="list-style-type: none"> Select an entry (or entries) in the "Other Stations" list, and click the "<<" button. Enter the Address (MAC or physical address) of the wireless station, and click the "Add" button.
>>	<p>Delete a Trusted Wireless Station from the list (move to the "Other Stations" list).</p> <ul style="list-style-type: none"> Select an entry (or entries) in the "Trusted Stations" list. Click the ">>" button.
Select All	Select all of the Stations listed in the "Other Stations" list.
Select None	De-select any Stations currently selected in the "Other Stations" list.
Edit	<p>To change an existing entry in the "Trusted Stations" list, select it and click this button.</p> <ol style="list-style-type: none"> Select the Station in the "Trusted Station" list. Click the "Edit" button. The address will be copied to the "Address" field, and the "Add" button will change to "Update". Edit the address (MAC or physical address) as required. Click "Update" to save your changes.

Add	To add a Trusted Station which is not in the "Other Wireless Stations" list, enter the required data and click this button.
Clear	Clear the <i>Name</i> and <i>Address</i> fields.

3.5 Security Profiles

Security Profiles contain the SSID and all the security settings of this WAP-4060PE.

- Up to eight (8) Security Profiles can be defined.
- Up to four (4) Security Profiles can be enabled at one time, allowing up to 4 different SSIDs to be used simultaneously.

Security Profiles

Profiles	Profile Name [SSID] Security [Band]
	*wireless [wireless] None [2.4 GHz]
	Profile02 [wireless] None [2.4 GHz]
	Profile03 [wireless] None [2.4 GHz]
	Profile04 [wireless] None [2.4 GHz]
	Profile05 [wireless] None [2.4 GHz]
	Profile06 [wireless] None [2.4 GHz]

* Indicates profile is currently enabled.

Primary Profile	802.11b/g AP Mode:	802.11b/g Bridge Mode:
	wireless [wireless]	wireless [wireless]

These settings have no effect unless the appropriate mode is enabled. If enabled, the selected Profile/SSID is used for the beacon.

Isolation	Profile (SSID) Isolation:
	<input checked="" type="radio"/> No isolation <input type="radio"/> Isolate all Profiles (SSIDs) from each other <input type="radio"/> Use VLAN (802.1Q) standard

Data - Security Profiles Screen

Profile	
Profile List	<p>All available profiles are listed. For each profile, the following data is displayed:</p> <ul style="list-style-type: none"> * (star sign) If displayed before the name of the profile, this indicates the profile is currently enabled. If not displayed, the profile is currently disabled. Profile Name The current profile name is displayed. [SSID] The current SSID associated with this profile. Security System The current security system (e.g. WPA-PSK) is displayed. [Frequency Band] The Wireless Band (2.4 GHz) for this profile is displayed.
Buttons	<ul style="list-style-type: none"> Enable - enable the selected profile. Configure - change the settings for the selected profile. Disable - disable the selected profile.
Primary Profile	
802.11b/g AP Mode	<p>Select the primary profile for 802.11b and 802.11g AP mode. Only enabled profiles are listed. The SSID associated with this profile will be broadcast if the "Broadcast SSID" setting on the Basic screen is enabled.</p>

802.11b/g Bridge Mode	Select the primary profile for 802.11b and 802.11g Bridge Mode. This setting determines the SSID and security settings used for the Bridge connection to the remote AP.
Isolation	
None	If this option is selected, wireless clients using different profiles (different SSIDs) are not isolated, so they will be able to communicate with each other.
Isolate all	If this option is selected, wireless clients using different profiles (different SSIDs) are isolated from each other, so they will NOT be able to communicate. They will still be able to communicate with other clients using the same profile, unless the "Wireless Separation" setting on the "Advanced" screen has been enabled.
Use VLAN	This option is only useful if the hubs/switches on your LAN support the VLAN (802.1Q) standard. When VLAN is used, you must select the desired VLAN for each security profile when configuring the profile. (If VLAN is not selected, the VLAN setting for each profile is ignored.) Click the <i>Configure VLAN</i> button to configure the IDs used by each VLAN. See below for further details.

3.5.1 VLAN Configuration Screen

This screen is accessed via the *Configure VLAN* button on the *Security Profiles* screen.

- The settings on this screen will be ignored unless the *Use VLAN* option on the *Security Profiles* screen is selected.
- If using the VLAN option, these setting determine which VLAN traffic is assigned to.

VLAN Configuration

VLAN - Client Traffic

Profile	VLAN ID	Profile	VLAN ID
wireless	<input type="text"/>	Profile05	<input type="text"/>
Profile02	<input type="text"/>	Profile06	<input type="text"/>
Profile03	<input type="text"/>	Profile07	<input type="text"/>
Profile04	<input type="text"/>	Profile08	<input type="text"/>

IDs must be in the range 1 ~ 4095.

VLAN - AP Traffic

VLAN Tag for Traffic generated by this AP.

- No VLAN Tag
 Replicate packets on all VLANs above
 Specified VLAN ID

Save

Cancel

Help

Close

Data - VLAN Configuration Screen

VLAN – Client Traffic	
Profile	Each profile is listed, whether currently enabled or not. You can assign traffic from each profile (SSID) to a different VLAN if desired. To assign multiple profiles to the same VLAN, just enter the same VLAN ID for each profile.
VLAN ID	Enter the desired VLAN ID, as used on your network. IDs must be in the range 1 ~ 4095. These IDs must match the IDs used by other network devices.
VLAN – AP Traffic	
No VLAN Tag	Traffic generated by this AP will not have a VLAN tag (no VLAN ID).
Replicate...	If selected, each packet generated by this AP will be sent over each active VLAN, as defined in the client VLAN table above. This requires that each packet be replicated (up to 8 times). This has a detrimental effect on performance, so should only be used if necessary.

Specified VLAN ID	If selected, you can enter the desired VLAN ID. Normally, this ID should be one of the client VLAN IDs defined above.
--------------------------	---

3.6 Configure Security Profile

This screen is displayed when you select a Profile on the Security Profiles screen, and click the *Configure* button.

3.6.1 Profile Data

Enter the desired settings for each of the following:

Profile Name	Enter a suitable name for this profile.
SSID	Enter the desired SSID. Each profile must have an unique SSID.
Wireless Band	Displays the wireless band for this profile.

3.6.2 Security Settings

Select the desired option, and then enter the settings for the selected method.

The available options are:

- **None** - No security is used. Anyone using the correct SSID can connect to your network.
- **WEP** - The 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.
- **WPA-PSK** - Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes periodically.
- **WPA-802.1x** - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

If this option is selected:

- This WAP-4060PE must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.
- All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.
- **802.1x** - This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption.

If this option is selected:

- This WAP-4060PE must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.
- All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

3.6.3 Security Settings - None

Security Profile

Profile
Profile Name: wireless
SSID: wireless
Wireless Band: 2.4 GHz

Security System
Wireless Security System: None

Security Settings

Radius MAC
Current Status: Disabled

UAM
Current Status: Disabled

No security is used. Anyone using the correct SSID can connect to your network.

The only settings available from this screen are **Radius MAC Authentication** and **UAM** (Universal Access Method).

3.6.4 Radius MAC Authentication

Radius MAC Authentication provides for MAC address checking which is centralized on your Radius server. If you don't have a Radius Server, you cannot use this feature.

Using MAC authentication

5. Ensure the WAP-4060PE can login to your Radius Server.
 - Add a RADIUS client on the RADIUS server, using the IP address or name of the WAP-4060PE, and the same shared key as pre-configured.
 - Ensure the WAP-4060PE has the correct address, port number, and shared key for login to your Radius Server. These parameters are entered either on

the Security page, or the Radius-based MAC authentication sub-screen, depending on the security method used.

- On the WAP-4060PE, enable the Radius-based MAC authentication feature on the screen below.
6. Add Users on the Radius server as required. The username must be the MAC address of the Wireless client you wish to allow, and the password must be blank.
 7. When clients try to associate with the WAP-4060PE, their MAC address is passed to the Radius Server for authentication.
 - If successful, “xx:xx:xx:xx:xx:xx MAC authentication” is entered in the log, and client station status would show as “authenticated” on the station list table;
 - If not successful, “xx:xx:xx:xx:xx:xx MAC authentication failed” is entered in the log, and station status is shown as “authenticating” on the station list table.

Radius-based MAC authentication Screen

This screen will look different depending on the current security setting. If you have already provided the address of your Radius server, you won't be prompted for it again. Otherwise, you must enter the details of your Radius Server on this screen.

Radius-based MAC Authentication

Enable Radius-based MAC authentication

Radius Server Address:

Radius Port:

Client Login Name:

Shared Key:

Data - Radius-based MAC Authentication Screen

Enable ...	Enable this if you want to use Radius-based MAC authentication.
Radius Server Address	If this field is visible, enter the name or IP address of the Radius Server on your network.
Radius Port	If this field is visible, enter the port number used for connections to the Radius Server.
Client Login Name	If this field is visible, it displays the name used for the Client Login on the Radius Server. This Login name must be created on the Radius Server.
Shared Key	If this field is visible, it is used for the Client Login on the Radius Server. Enter the key value to match the value on the Radius Server.
WEP Key	If this field is visible, it is for the WEP key used to encrypt data transmissions to the Radius Server. Enter the desired key value in HEX, and ensure the Radius Server has the same value.

WEP Key Index	If this field is visible, select the desired key index. Any value can be used, provided it matches the value on the Radius Server.
----------------------	--

3.6.5 UAM

UAM (Universal Access Method) is intended for use in Internet cafes, Hot Spots, and other sites where the WAP-4060PE is used to provide Internet Access.

If enabled, then HTTP (TCP, port 80) connections are checked. (UAM only works on HTTP connections; all other traffic is ignored.) If the user has not been authenticated, Internet access is blocked, and the user is re-directed to another web page. Typically, this web page is on your Web server, and explains how to pay for and obtain Internet access.

To use UAM, you need a Radius Server for Authentication. The "Radius Server Setup" must be completed before you can use UAM. The required setup depends on whether you are using "Internal" or "External" authentication.

- **Internal authentication** uses the web page built in the WAP-4060PE.
- **External authentication** uses a web page on your Web server. Generally, you should use External authentication, as this allows you to provide relevant and helpful information to users.

UAM authentication - Internal

1. Ensure the WAP-4060PE can login to your Radius Server.
 - Add a RADIUS client on RADIUS server, using the IP address or name of the WAP-4060PE, and the same shared key as pre-configured.
 - Ensure the WAP-4060PE has the correct address, port number, and shared key for login to your Radius Server. These parameters are entered either on the Security page, or the UAM sub-screen, depending on the security method used.
2. Add users on your RADIUS server as required, and allow access by these users.
3. Client PCs must have the correct Wireless settings in order to associate with the WAP-4060PE.
4. When an associated client tries to use HTTP (TCP, port 80) connections, they will be re-directed to a user login page.
5. The client (user) must then enter the user name and password, as defined on the Radius Server. (You must provide some system to let users know the correct name and password to use.)
6. If the user name and password is correct, Internet access is allowed. Otherwise, the user remains on the login page.
 - Clients which pass the authentication are listed as "xx:xx:xx:xx:xx:xx WEB authentication" in the log table, and station status would show as "Authenticated" on the station list table.
 - If a client fails authentication, "xx:xx:xx:xx:xx:xx WEB authentication failed" shown in the log, and station status is shown as "Authenticating" on the station list table.

UAM authentication - External

1. Ensure the WAP-4060PE can login to your Radius Server.
 - Add a RADIUS client on RADIUS server, using the IP address or name of the WAP-4060PE, and the same shared key as pre-configured.

- Ensure the WAP-4060PE has the correct address, port number, and shared key for login to your Radius Server. These parameters are entered either on the Security page, or the UAM sub-screen, depending on the security method used.
2. On your Web Server, create a suitable welcome page. The welcome page must have a link or button to allow the user to input their user name and password on the uamlogon.htm page on the WAP-4060PE.
 3. On the WAP-4060PE's UAM screen, select External Web-based Authentication, and enter the URL for the welcome page on your Web server.
 4. Add users on your RADIUS server as required, and allow access by these users.
 5. Client PCs must have the correct Wireless settings in order to associate with the WAP-4060PE.
 6. When an associated client tries to use HTTP (TCP, port 80) connections, they will be re-directed to the welcome page on your Web Server.
 7. The client (user) must then enter the user name and password, as defined on the Radius Server. (You must provide some system to let users know the correct name and password to use.)
 8. If the user name and password is correct, Internet access is allowed. Otherwise, the user remains on the login page.
 - Clients which pass the authentication are listed as "xx:xx:xx:xx:xx:xx WEB authentication" in the log table, and station status would show as "Authenticated" on the station list table.
 - If a client fails authentication, "xx:xx:xx:xx:xx:xx WEB authentication failed" is shown in the log, and station status is shown as "Authenticating" on the station list table.

UAM Screen

The UAM screen will look different depending on the current security setting. If you have already provided the address of your Radius server, you won't be prompted for it again.

UAM (Universal Access Method)

UAM (Universal Access Method)

Internal Web-based Authentication
 External Web-based Authentication

Login URL:

Login Failure URL:

Radius Server Address:

Radius Port:

Client Login Name:

Shared Key:

Data - UAM Screen

Enable	Enable this if you want to use this feature. See the section above for details of using UAM.
Internal Web-based Authentication	If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the built-in login page. The logon data is then sent to the Radius Server for authentication.
External Web-based Authentication	If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the URL below. This needs to be on your own local Web Server. The page must also link back to the built-in login page on this device to complete the login procedure.
Login URL	Enter the URL of the page on your local Web Server. When users attempt to access the Internet, they will see this page, but are not logged in.
Login Failure URL	Enter the URL of the page on your local Web Server you wish users to see if their login fails. (This may be the same URL as the Login URL).

3.6.6 Security Settings - WEP

This is the 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.

Security Profile

Profile	Profile Name: <input type="text" value="wireless"/> SSID: <input type="text" value="wireless"/> Wireless Band: <input type="text" value="2.4 GHz"/>
Security System	Wireless Security System: <input type="text" value="WEP"/>
Security Settings	WEP Data Encryption: <input type="text" value="64 bit"/> Authentication: <input type="text" value="Open System"/> WEP Keys Key input: <input checked="" type="radio"/> Hex (0~9 and A~F) <input type="radio"/> ASCII Key 1: <input checked="" type="radio"/> <input type="text"/> Key 2: <input type="radio"/> <input type="text"/> Key 3: <input type="radio"/> <input type="text"/> Key 4: <input type="radio"/> <input type="text"/> Passphrase: <input type="text"/> <input type="button" value="Generate Key"/>
Radius MAC	Current Status: Disabled <input type="button" value="Configure"/>
UAM	Current Status: Disabled <input type="button" value="Configure"/>

Data - WEP Screen

WEP	
Data Encryption	Select the desired option, and ensure your Wireless stations have the identical setting: <ul style="list-style-type: none"> 64 Bit Encryption - Keys are 10 Hex (5 ASCII) characters. 128 Bit Encryption - Keys are 26 Hex (13 ASCII) characters. 152 Bit Encryption - Keys are 32 Hex (16 ASCII) characters.
Authentication	Normally, you can leave this at "Automatic", so that Wireless Stations can use either method ("Open System" or "Shared Key"). If you wish to use a particular method, select the appropriate value - "Open System" or "Shared Key". All Wireless stations must then be set to use the same method.
Key Input	Select "Hex" or "ASCII" depending on your input method. (All keys are converted to Hex, ASCII input is only for convenience.)
Key Value	Enter the key values you want to use. The default key, selected by the radio button, is required. The other keys are optional. Other stations must have matching key values.

Passphrase	Use this to generate a key or keys, instead of entering them directly. Enter a word or group of printable characters in the Passphrase box and click the "Generate Key" button to automatically configure the WEP Key(s).
Radius MAC Authentication	The current status is displayed. Click the "Configure" button to configure this feature if required.
UAM	The current status is displayed. Click the "Configure" button to configure this feature if required.

3.6.7 Security Settings - WPA-PSK

Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.

Security Profile

Profile
 Profile Name: wireless
 SSID: wireless
 Wireless Band: 2.4 GHz

Security System
 Wireless Security System: WPA - PSK

Security Settings
 WPA - PSK (Pre-shared Key)
 Network Key:
 WPA Encryption: TKIP

Key Updates
 Group Key Update Key Lifetime: 30 minutes
 Update Group Key when any membership terminates

Radius MAC
 Current Status: Disabled Configure

UAM
 Current Status: Disabled Configure

Back Save Cancel Help

Data - WPA-PSK Screen

WPA-PSK	
Network Key	Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.
WPA Encryption	Select the desired option. Other Wireless Stations must use the same method.

	<ul style="list-style-type: none"> • TKIP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are not encrypted. • TKIP + 64 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 64 bit WEP. • TKIP + 128 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 128 bit WEP. • AES - CCMP - CCMP is the most common sub-type of AES (Advanced Encryption System). Most systems will simply say "AES". If selected, both Unicast (point-to-point) and multicast (broadcast) transmissions are encrypted using AES. • AES - CCMP + TKIP - If selected, Unicast (point-to-point) uses AES-CCMP and multicast (broadcast) transmissions are encrypted using TKIP.
Group Key Update	This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often the Group key is dynamically updated. Enter the desired value.
Update Group key when any membership terminates	If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the WAP-4060PE.
Radius MAC Authentication	The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPA-PSK.
UAM	The current status is displayed. This will always be "Disabled", because UAM is not available with WPA-PSK. The <i>Configure</i> button for this feature will also be disabled.

3.6.8 Security Settings - WPA-802.1x

This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

If this option is selected:

- This WAP-4060PE must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server. Normally, a Certificate is used to authenticate each user.
- Each user's wireless client must support 802.1x.
- All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

Security Profile

Profile	Profile Name: <input type="text" value="wireless"/> SSID: <input type="text" value="wireless"/> Wireless Band: <input type="text" value="2.4 GHz"/>
Security System	Wireless Security System: <input type="text" value="WPA - 802.1x"/>
Security Settings	WPA - 802.1x Radius Server Address: <input type="text"/> Radius Port: <input type="text" value="1812"/> Client Login Name: PLE0046A Shared Key: <input type="text"/> WPA Encryption: <input type="text" value="TKIP"/>
Radius MAC	Key Updates <input type="checkbox"/> Group Key Update Key Lifetime: <input type="text" value="30"/> minutes <input type="checkbox"/> Update Group Key when any membership terminates Radius Accounting <input type="checkbox"/> Enable Radius Accounting: Radius Accounting Port: <input type="text" value="1813"/> <input checked="" type="checkbox"/> Update Report every <input type="text" value="5"/> Minutes Current Status: Disabled

Data - WPA-802.1x Screen

WPA-802.1x	
Radius Server Address	Enter the name or IP address of the Radius Server on your network.
Radius Port	Enter the port number used for connections to the Radius Server.
Client Login Name	This read-only field displays the current login name, which is the same as the name of the WAP-4060PE. The Radius Server must be configured to accept this login.
Shared Key	This is used for the <i>Client Login</i> on the Radius Server. Enter the key value to match the Radius Server.

WPA Encryption	<p>Select the desired option. Other Wireless Stations must use the same method.</p> <ul style="list-style-type: none"> • TKIP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are not encrypted. • TKIP + 64 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 64 bit WEP. • TKIP + 128 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 128 bit WEP. • AES - CCMP - CCMP is the most common sub-type of AES (Advanced Encryption System). Most systems will simply say "AES". If selected, both Unicast (point-to-point) and multicast (broadcast) transmissions are encrypted using AES. • AES - TKIP - If selected, Unicast (point-to-point) uses AES-CCMP and multicast (broadcast) transmissions are encrypted using TKIP.
Group Key Update	This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly.
Key Lifetime	This field determines how often the Group key is dynamically updated. Enter the desired value.
Update Group key when any membership terminates	If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the WAP-4060PE.
Radius Accounting	<p>Enable this if you want this WAP-4060PE to send accounting data to the Radius Server.</p> <p>If enabled, the port used by your Radius Server must be entered in the "Radius Accounting Port" field.</p>
Update Report every ...	If Radius accounting is enabled, you can enable this and enter the desired update interval. This WAP-4060PE will then send updates according to the specified time period.
Radius MAC Authentication	The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPA-802.1x. The <i>Configure</i> button for this feature will also be disabled.
UAM	The current status is displayed. This will always be "Disabled", because UAM is not available with WPA-802.1x. The <i>Configure</i> button for this feature will also be disabled.

3.6.9 Security Settings - 802.1x

This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption.

If this option is selected:

- This WAP-4060PE must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server. Normally, a Certificate is used to authenticate each user.
- Each wireless client must support 802.1x.
- All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

Security Profile

Profile	Profile Name: <input type="text" value="wireless"/>
	SSID: <input type="text" value="wireless"/>
	Wireless Band: <input type="text" value="2.4 GHz"/>
Security System	Wireless Security System: <input type="text" value="802.1x"/>
Security Settings	802.1x
	Radius Server Address: <input type="text"/>
	Radius Port: <input type="text" value="1812"/>
	Client Login Name: <input type="text" value="PLE0046A"/>
	Shared Key: <input type="text"/>
	WEP Key Size: <input type="text" value="64 bit"/>
	<input type="checkbox"/> Dynamic WEP key (EAP-TLS, PEAP etc)
	<input checked="" type="checkbox"/> Key Exchange with lifetime of <input type="text" value="20"/> minutes
	<input type="checkbox"/> Static WEP Key (EAP-MD5)
	WEP Key : <input type="text"/> (hex)
	WEP Key Index: <input type="text" value="1"/>

Data - 802.1x Screen

802.1x	
Radius Server Address	Enter the name or IP address of the Radius Server on your network.
Radius Port	Enter the port number used for connections to the Radius Server.
Client Login Name	This read-only field displays the current login name, which is the same as the name of the WAP-4060PE. The Radius Server must be configured to accept this login.
Shared Key	This is used for the <i>Client Login</i> on the Radius Server. Enter the key value to match the Radius Server.

WEP Key Size	<p>Select the desired option:</p> <ul style="list-style-type: none"> • 64 Bit - Keys are 10 Hex (5 ASCII) characters. • 128 Bit - Keys are 26 Hex (13 ASCII) characters. • 152 Bit - Keys are 32 Hex (16 ASCII) characters.
Dynamic WEP Key	<p>Click this if you want the WEP keys to be automatically generated.</p> <ul style="list-style-type: none"> • The key exchange will be negotiated. The most widely supported protocol is EAP-TLS. • The following Key Exchange setting determines how often the keys are changed. • Both Dynamic and Static keys can be used simultaneously, allowing clients using either method to use the WAP-4060PE.
Key Exchange	<p>This setting is only available if using Dynamic WEP Keys. If you want the Dynamic WEP keys to be updated regularly, enable this and enter the desired lifetime (in minutes).</p>
Static WEP Key (EAP-MD5)	<p>Enable this if some wireless clients use a fixed (static) WEP key, using EAP-MD5.</p> <p>Note: both Dynamic and Static keys can be used simultaneously, allowing clients using either method to use the WAP-4060PE.</p>
WEP Key	<p>Enter the WEP key according to the WEP Key Size setting above. Wireless stations must use the same key.</p>
WEP Key Index	<p>Select the desired index value. Wireless stations must use the same key index.</p>
Radius Accounting	<p>Enable this if you want this WAP-4060PE to send accounting data to the Radius Server.</p> <p>If enabled, the port used by your Radius Server must be entered in the Radius Accounting Port field.</p>
Update Report every ...	<p>If Radius accounting is enabled, you can enable this and enter the desired update interval. This WAP-4060PE will then send updates according to the specified time period.</p>
Radius MAC Authentication	<p>The current status is displayed.</p> <p>Click the <i>Configure</i> button to configure this feature if required.</p>
UAM	<p>The current status is displayed.</p> <p>Click the <i>Configure</i> button to configure this feature if required.</p>

3.7 System Screen

Click System on the menu to view a screen like the following.

Data - System Screen

Identification	
Access Point Name	Enter a suitable name for this WAP-4060PE.
Description	If desired, you can enter a description for the WAP-4060PE.
Country Domain	Select the country or domain matching your current location.
IP Address	
DHCP Client	Select this option if you have a DHCP Server on your LAN, and you want the WAP-4060PE to obtain an IP address automatically.
Fixed	<p>If selected, the following data must be entered.</p> <ul style="list-style-type: none"> • IP Address - The IP Address of this device. Enter an unused IP address from the address range on your LAN. • Subnet Mask - The Network Mask associated with the IP Address above. Enter the value used by other devices on your LAN. • Gateway - The IP Address of your Gateway or Router. Enter the value used by other devices on your LAN. • DNS - Enter the DNS (Domain Name Server) used by PCs on your LAN.

WINS	
Enable WINS	If your LAN has a WINS server, you can enable this to have this AP register with the WINS server.
WINS Server Name/IP Address	Enter the name or IP address of your WINS server.

3.8 2.4GHz Wireless

There are two configuration screens available:

- Basic Settings
- Advanced

3.8.1 Basic Settings Screen

The settings on this screen must match the settings used by Wireless Stations.

Click **Basic** on the menu to view a screen like the following.

Basic Settings - 2.4 GHz

Operation	Wireless Mode:	<input type="text" value="802.11b and 802.11g"/>
	AP Mode:	<input type="text" value="Access Point"/>
		Repeater AP
		MAC Address: <input type="text"/> <input type="button" value="Select AP"/>
		<input checked="" type="checkbox"/> Broadcast SSID
	Bridge Mode:	<input type="text" value="None (disable)"/>
		PTP Bridge AP
		MAC Address: <input type="text"/>
		<input type="checkbox"/> In PTMP mode, only allow specified APs
		<input type="button" value="Set PTMP APs"/>
Parameters	Channel No:	<input type="text" value="Automatic"/>
	Current Channel No:	10
		<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>

Data - Basic Settings Screen

Operation	
Wireless Mode	<p>Select the desired option:</p> <ul style="list-style-type: none"> Disable - select this if for some reason you do not want this AP to transmit or receive at all. 802.11b and 802.11g - this is the default setting, and will allow connections by both 802.11b and 802.1g wireless stations. 802.11b - if selected, only 802.11b clients are allowed. 802.11g wireless stations will only be able to connect if they are fully backward compatible with the 802.11b standard. 802.11g - only 802.11g clients are allowed. If you only have 802.11g, selecting this option may provide a performance improvement over using the default setting. Dynamic Super 802.11g (108Mbps) - This uses <i>Packet Bursting, FastFrame, Compression, and Channel Bonding</i> (using 2 channels) to increase throughput. Only clients supporting the "Atheros Super G" mode can connect at 108Mbps, and they will only use this speed when necessary. However, this option is backward compatible with 802.11b and (standard) 802.11g. Static Super 802.11g (108Mbps) - This uses <i>Packet Bursting, FastFrame, Compression, and Channel Bonding</i> (using 2 channels) to increase throughput. Because "Channel Bonding" is always used, this method is NOT compatible with 802.11b and (standard) 802.11g. Only clients supporting the "Atheros Super G" mode can connect at 108Mbps; they will always connect at this speed. Select this option only if all wireless stations support this "Atheros Super G" mode.

AP Mode	<p>Both Bridge mode and AP mode can be used simultaneously, unless AP mode is "Client/Repeater". Select the desired AP mode:</p> <ul style="list-style-type: none"> • None (disable) - Disable AP mode. Use this if you want this WAP-4060PE to act as Bridge only. • Access Point - operate as a normal Access Point • Client/Repeater - act as a client or repeater for another Access Point. If selected, you must provide the address (MAC address) of the other AP in the Repeater AP MAC Address field. In this mode, all traffic is sent to the specified AP. <p>Note: If using Client/Repeater mode, you cannot use Bridge Mode.</p>
Repeater AP MAC Address	<p>This is not required unless the AP Mode is "Client/Repeater". In this mode, you must provide the MAC address of the other AP in this field. You can either enter the MAC address directly, or, if the other AP is on-line and broadcasting its SSID, you can click the "Select AP" button and select from a list of available APs.</p>
Broadcast SSID	<p>If Disabled, no SSID is broadcast. If enabled, you must select the security profile whose SSID is to be broadcast. This can be done in the "Security Profiles" screen. The SSID will then be broadcast to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.</p>
Bridge Mode	<p>Both Bridge mode and AP mode can be used simultaneously, unless AP mode is "Client/Repeater". Select the desired Bridge mode:</p> <ul style="list-style-type: none"> • None (disable) - Disable Bridge mode. Use this if you want this WAP-4060PE to act as an AP only. • Point-to-Point Bridge (PTP) - Bridge to a single AP. You must provide the MAC address of the other AP in the PTP Bridge AP MAC Address field. • Point-to-Multi-Point Bridge (PTMP) - Select this only if this AP is the "Master" for a group of Bridge-mode APs. The other Bridge-mode APs must be set to Point-to-Point Bridge mode, using this AP's MAC address. They then send all traffic to this "Master". <p>If required, you can specify the MAC addresses of the APs which are allowed to connect to this AP in PTMP mode. To specify the allowed APs:</p> <ol style="list-style-type: none"> 1. Enable the checkbox "In PTMP mode, only allow specified APs". 2. Click the button "Set PTMP APs". 3. On the resulting sub-screen, enter the MAC addresses of the allowed APs.
PTP Bridge AP MAC Address	<p>This is not required unless the Bridge Mode is "Point-to-Point Bridge (PTP)". In this case, you must enter the MAC address of the other AP in this field.</p>

In PTMP mode, only allow specified APs	<p>This is only functional if using Point-to-Multi-Point Bridge (PTMP) mode. If enabled, you can specify the MAC addresses of the APs which are allowed to connect to this AP. To specify the allowed APs:</p> <ol style="list-style-type: none"> 1. Enable this checkbox 2. Click the button "Set PTMP APs". 3. On the resulting sub-screen, enter the MAC addresses of the allowed APs.
Set PTMP APs	<p>Use this to open a sub-window where you can specify the MAC addresses of the APs which are allowed to connect to this AP. This is only functional if using Point-to-Multi-Point Bridge (PTMP) mode and you has enabled the checkbox "In PTMP mode, only allow specified APs".</p>
Parameters	
Channel No	<ul style="list-style-type: none"> • If "Automatic" is selected, the WAP-4060PE will select the best available Channel. • If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with manually setting different channels to see which is the best.
Current Channel No.	<p>This displays the current channel used by the WAP-4060PE.</p>

3.8.2 Advanced Settings

Clicking the *Advanced* link on the menu will result in a screen like the following.

Advanced Settings - 2.4 GHz

Basic Rate	Basic Rate Selection: <input type="text" value="802.11b (1, 2, 5.5, 11 Mbps)"/>
Options	<input type="checkbox"/> Wireless Separation <input type="checkbox"/> Worldwide Mode (802.11d)
Parameters	Disassociated Timeout: <input type="text" value="5"/> Minutes (1 ~ 99) Fragmentation Length: <input type="text" value="2346"/> (256 ~ 2346; Default 2346) Beacon Interval: <input type="text" value="100"/> (20 ~ 1000; Default 100) RTS/CTS Threshold: <input type="text" value="2346"/> (256 ~ 2346; Default 2346) Preamble Type: <input type="text" value="Short"/> Output Power Level: <input type="text" value="Full"/> Antenna Selection: <input type="text" value="Primary"/>
802.11b	Protection Type: <input checked="" type="radio"/> CTS-only <input type="radio"/> RTS-CTS Short Slot Time: <input checked="" type="radio"/> Enable <input type="radio"/> Disable Protection Mode: <input type="text" value="Auto"/> Protection Rate: <input type="text" value="11 Mbps"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

Data - Advanced Settings Screen

Basic Rate	
Basic Rate	<p>The Basic Rate is used for broadcasting. It does not determine the data transmission rate, which is determined by the "Mode" setting on the Basic screen. Select the desired option.</p> <p>Do NOT select the "802.11g" or "OFDM" options unless ALL of your wireless clients support this. 802.11b clients will not be able to connect to the WAP-4060PE if either of these modes is selected.</p>
Options	
Wireless Separation	If enabled, each Wireless station using the WAP-4060PE is invisible to other Wireless stations. In most business situations, this setting should be Disabled.
Worldwide Mode (802.11d)	Enable this setting if you want to use this mode, and your Wireless stations also support this mode.
Parameters	
Disassociated Time-out	This determines how quickly a Wireless Station will be considered "Disassociated" with this AP, when no traffic is received. Enter the desired time period.
Fragmentation	Enter the preferred setting between 256 and 2346. Normally, this can be left at the default value.
Beacon Interval	Enter the preferred setting between 20 and 1000. Normally, this can be left at the default value.

RTS/CTS Threshold	Enter the preferred setting between 256 and 2346. Normally, this can be left at the default value.
Preamble Type	Select the desired option. The default is "Long". The "Short" setting takes less time when used in a good environment.
Output Power Level	Select the desired power output. Higher levels will give a greater range, but are also more likely to cause interference with other devices.
Antenna Selection	WAP-4060PE has only 1 antenna, there is only 1 option available.
802.11b	
Protection Type	Select the desired option. The default is CTS-only.
Short Slot Time	Enable or disable this setting as required.
Protection Mode	The Protection system is intended to prevent older 802.11b devices from interfering with 802.11g transmissions. (Older 802.11b devices may not be able to detect that an 802.11g transmission is in progress.) Normally, this should be left at "Auto".
Protection Rate	Select the desired option. The default is 11 Mbps.

Chapter 4

PC and Server Configuration



4.1 Overview

All Wireless Stations need to have settings which match the Wireless Access Point. These settings depend on the mode in which the WAP-4060PE is being used.

- If using WEP or WPA-PSK, it is only necessary to ensure that each Wireless station's settings match those of the WAP-4060PE, as described below.
- For WPA-802.1x and 802.1x modes, configuration is much more complex. The Radius Server must be configured correctly, and setup of each Wireless station is also more complex.

4.2 Using WEP

For each of the following items, each Wireless Station must have the same settings as the WAP-4060PE.

Mode	On each PC, the mode must be set to <i>Infrastructure</i> .
SSID (ESSID)	This must match the value used on the WAP-4060PE. The default value is wireless Note: The SSID is case sensitive.
Wireless Security	<ul style="list-style-type: none">• Each Wireless station must be set to use WEP data encryption.• The Key size (64 bit, 128 bit, 152 bit) must be set to match the WAP-4060PE.• The keys values on the PC must match the key values on the WAP-4060PE. Note: On some systems, the key sizes may be shown as 40bit, 104bit, and 128bit instead of 64 bit, 128 bit and 152bit. This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

4.3 Using WPA-PSK

For each of the following items, each Wireless Station must have the same settings as the WAP-4060PE.

Mode	On each PC, the mode must be set to <i>Infrastructure</i> .
SSID (ESSID)	This must match the value used on the WAP-4060PE. The default value is wireless Note: The SSID is case sensitive.
Wireless	On each client, Wireless security must be set to WPA-PSK.

Security	<ul style="list-style-type: none"> • The Pre-shared Key entered on the WAP-4060PE must also be entered on each Wireless client. • The Encryption method (e.g. TKIP, AES) must be set to match the WAP-4060PE.
-----------------	---

4.4 Using WPA-802.1x

This is the most secure and most complex system.

802.1x mode provides greater security and centralized management, but it is more complex to configure.

Wireless Station Configuration

For each of the following items, each Wireless Station must have the same settings as the WAP-4060PE.

Mode	On each PC, the mode must be set to Infrastructure .
SSID (ESSID)	<p>This must match the value used on the WAP-4060PE.</p> <p>The default value is wireless</p> <p>Note: The SSID is case sensitive.</p>
802.1x Authentication	Each client must obtain a Certificate which is used for authentication for the Radius Server.
802.1x Encryption	<p>Typically, EAP-TLS is used. This is a dynamic key system, so keys do NOT have to be entered on each Wireless station.</p> <p>However, you can also use a static WEP key (EAP-MD5); the WAP-4060PE supports both methods simultaneously.</p>

Radius Server Configuration

If using **WPA-802.1x** mode, the Radius Server on your network must be configured as follow:

- It must provide and accept **Certificates** for user authentication.
- There must be a **Client Login** for the WAP-4060PE itself.
- The WAP-4060PE will use its Default Name as its Client Login name. (However, your Radius server may ignore this and use the IP address instead.)
- The *Shared Key*, set on the *Security* Screen of the WAP-4060PE, must match the *Shared Secret* value on the Radius Server.
- **Encryption** settings must be correct.

4.5 802.1x Server Setup (Windows 2000 Server)

This section describes using *Microsoft Internet Authentication Server* as the Radius Server, since it is the most common Radius Server available that supports the EAP-TLS authentication method.

The following services on the Windows 2000 Domain Controller (PDC) are also required:

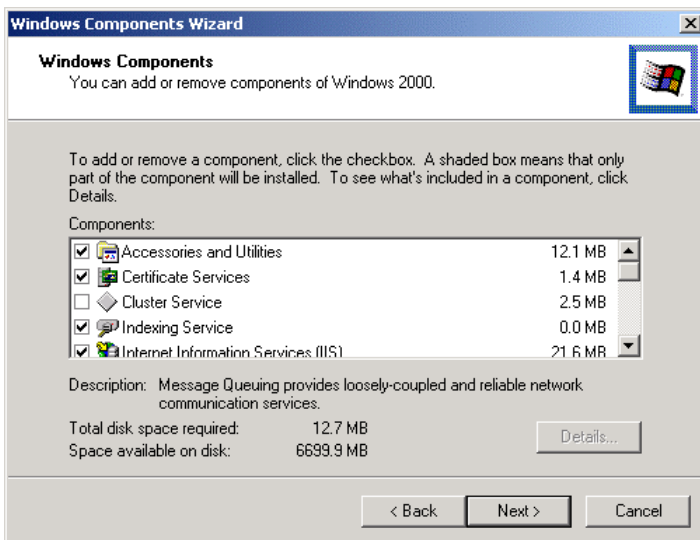
- dhcpd
- dns
- rras
- webserver (IIS)
- Radius Server (Internet Authentication Service)
- Certificate Authority

4.5.1 Windows 2000 Domain Controller Setup

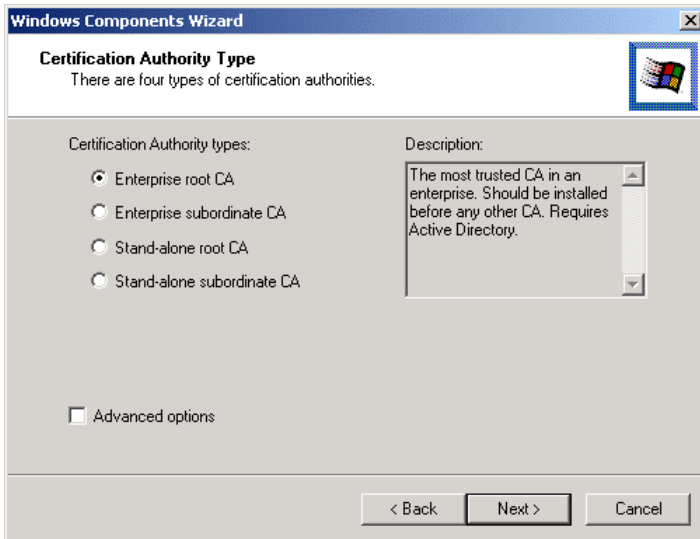
1. Run *dcpromo.exe* from the command prompt.
2. Follow all of the default prompts, ensure that DNS is installed and enabled during installation.

4.5.2 Services Installation

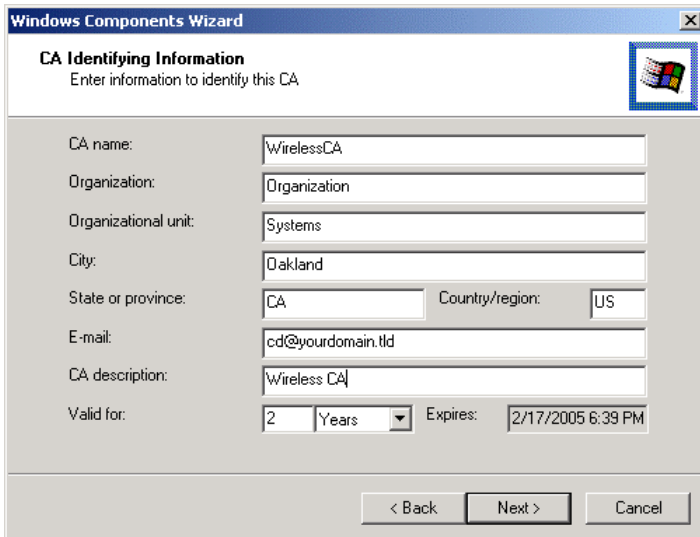
1. Select the *Control Panel - Add/Remove Programs*.
2. Click *Add/Remove Windows Components* from the left side.
3. Ensure that the following components are activated (selected):
 - *Certificate Services*. After enabling this, you will see a warning that the computer cannot be renamed and joined after installing certificate services. Select *Yes* to select certificate services and continue
 - *World Wide Web Server*. Select *World Wide Web Server* on the *Internet Information Services (IIS)* component.
 - From the *Networking Services* category, select *Dynamic Host Configuration Protocol (DHCP)*, and *Internet Authentication Service (DNS should already be selected and installed)*.



4. Click *Next*.
5. Select the *Enterprise root CA*, and click *Next*.



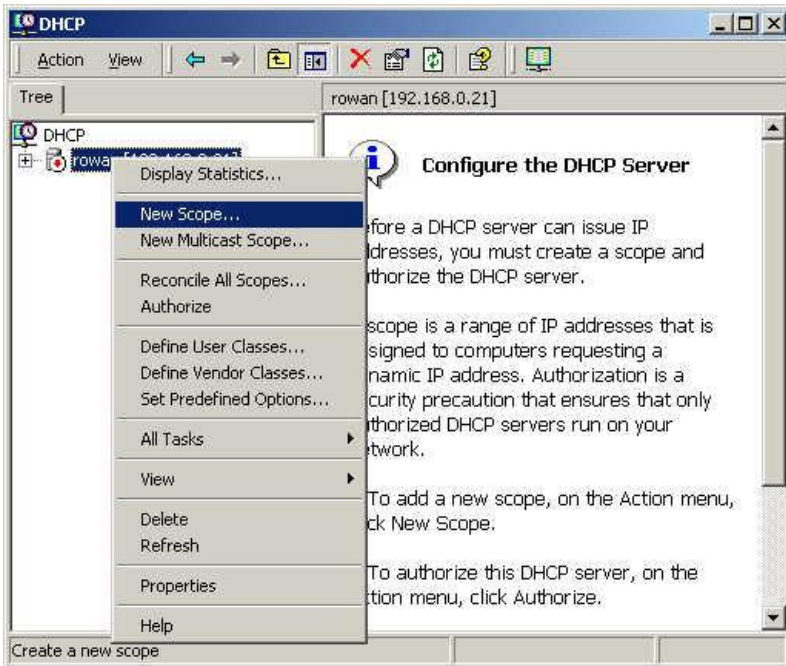
6. Enter the information for the Certificate Authority, and click *Next*.



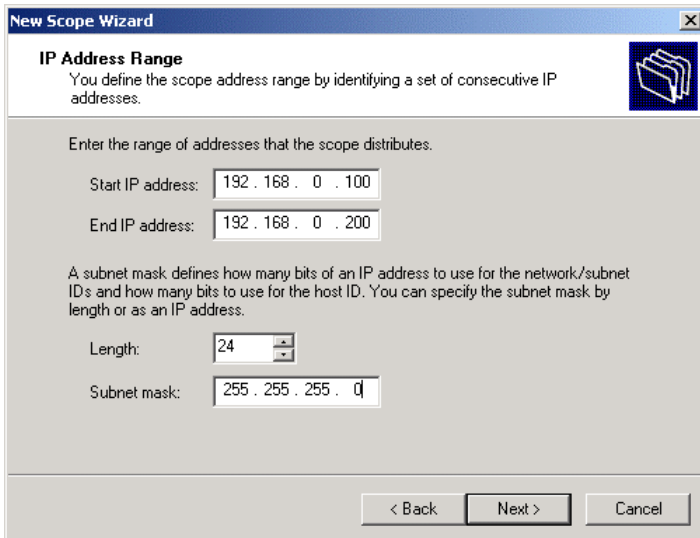
7. Click *Next* if you don't want to change the CA's configuration data.
8. Installation will warn you that Internet Information Services are running, and must be stopped before continuing. Click *Ok*, then *Finish*.

4.5.3 DHCP server configuration

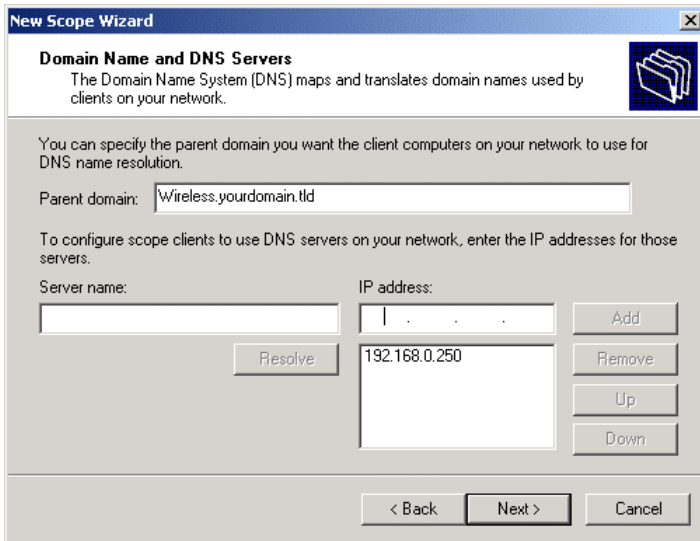
1. Click on the *Start - Programs - Administrative Tools - DHCP*
2. Right-click on the server entry as shown, and select *New Scope*.



3. Click *Next* when the New Scope Wizard Begins.
4. Enter the name and description for the scope, click *Next*.
5. Define the IP address range. Change the subnet mask if necessary. Click *Next*.



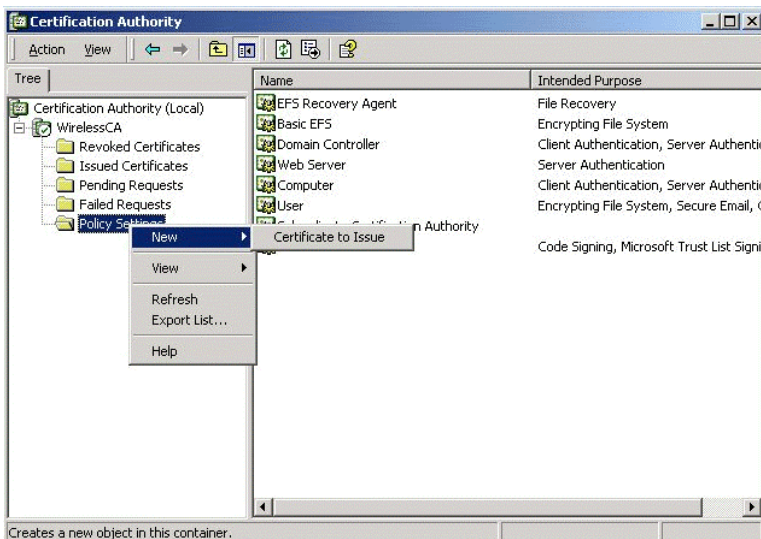
6. Add exclusions in the address fields if required. If no exclusions are required, leave it blank. Click *Next*.
7. Change the *Lease Duration* time if preferred. Click *Next*.
8. Select *Yes, I want to configure these options now*, and click *Next*.
9. Enter the router address for the current subnet. The router address may be left blank if there is no router. Click *Next*.
10. For the Parent domain, enter the domain you specified for the domain controller setup, and enter the server's address for the IP address. Click *Next*.



11. If you don't want a WINS server, just click *Next*.
12. Select *Yes, I want to activate this scope now*. Click *Next*, then *Finish*.
13. Right-click on the server, and select *Authorize*. It may take a few minutes to complete.

4.5.4 Certificate Authority Setup

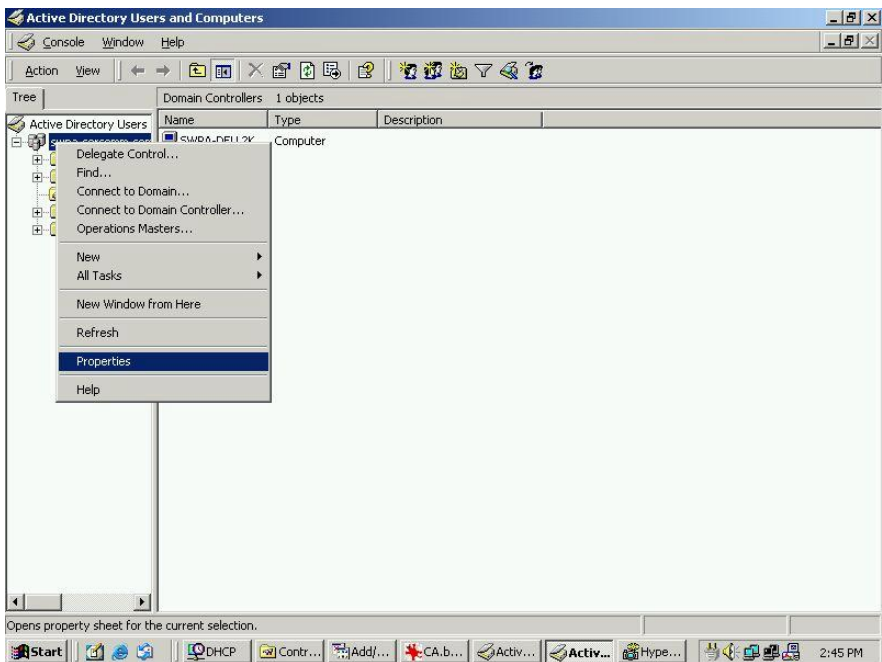
1. Select *Start - Programs - Administrative Tools - Certification Authority*.
2. Right-click *Policy Settings*, and select *New - Certificate to Issue*.



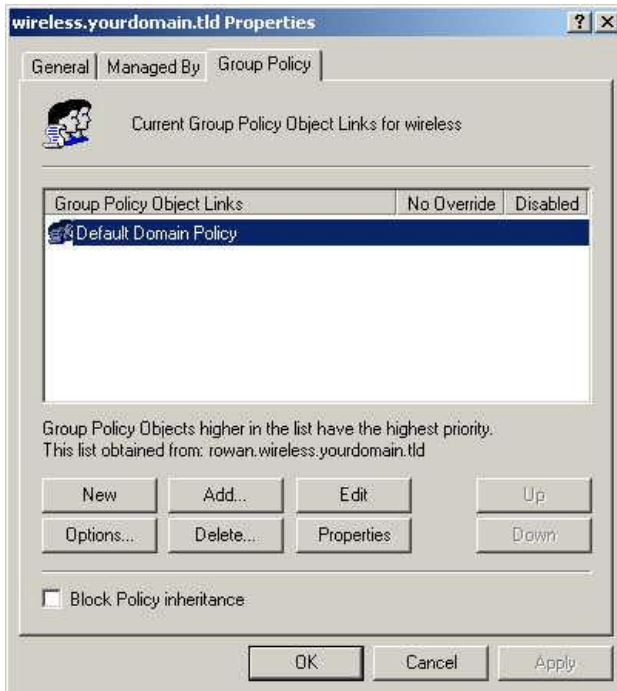
3. Select *Authenticated Session* and *Smartcard Logon* (select more than one by holding down the Ctrl key). Click *OK*.



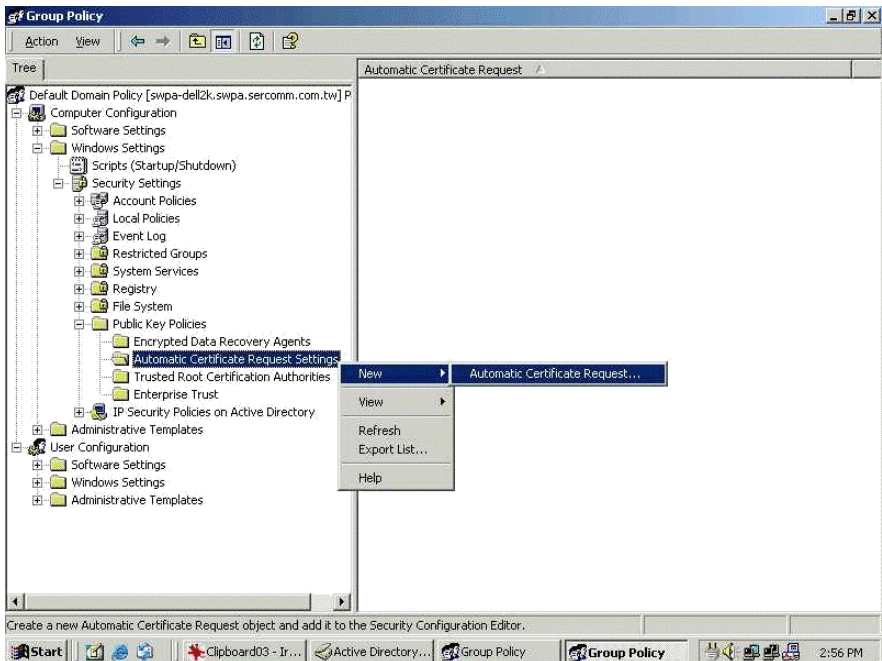
4. Select *Start - Programs - Administrative Tools - Active Directory Users and Computers*.
5. Right-click on your active directory domain, and select *Properties*.



6. Select the *Group Policy* tab, choose *Default Domain Policy* then click *Edit*.



7. Select *Computer Configuration - Windows Settings - Security Settings - Public Key Policies*, right-click *Automatic Certificate Request Settings - New - Automatic Certificate Request*.



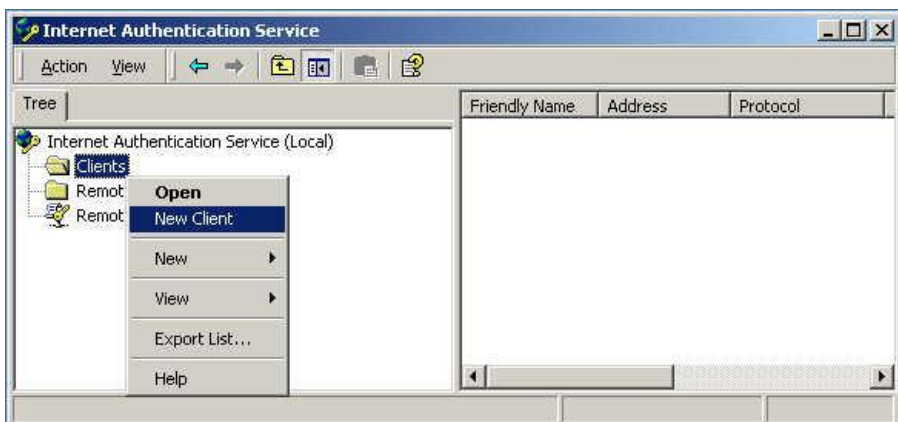
8. When the Certificate Request Wizard appears, click *Next*.
9. Select *Computer*, then click *Next*.



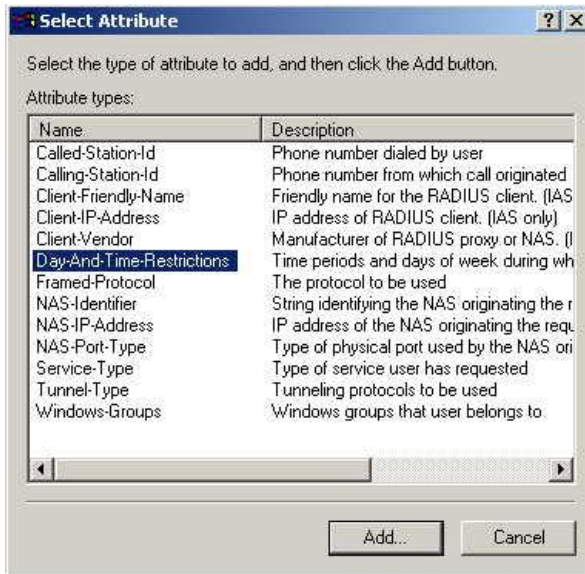
10. Ensure that your certificate authority is checked, then click *Next*.
11. Review the policy change information and click *Finish*.
12. Click *Start - Run*, type *cmd* and press enter.
Enter *secdit /refreshpolicy machine_policy*
This command may take a few minutes to take effect.

4.5.5 Internet Authentication Service (Radius) Setup

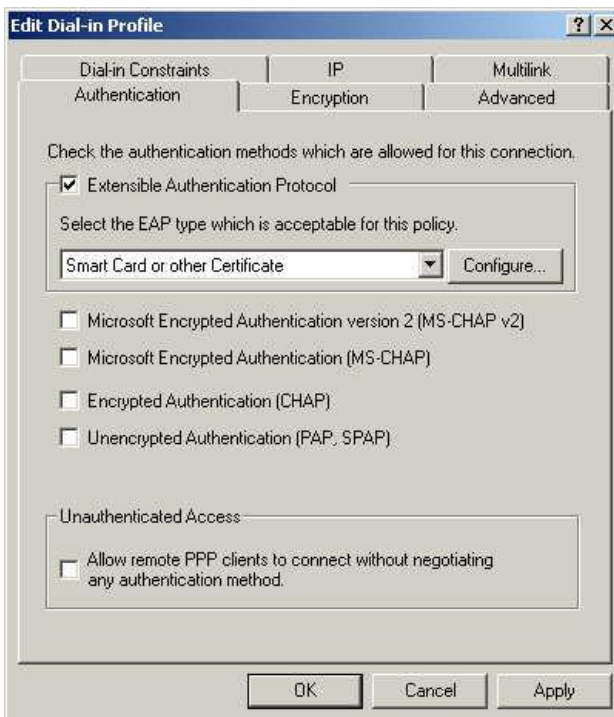
1. Select *Start - Programs - Administrative Tools - Internet Authentication Service*
2. Right-click on *Clients*, and select *New Client*.



3. Enter a name for the access point, click *Next*.
4. Enter the IP address of the WAP-4060PE, and set the shared secret, as entered on the Security Profile screen of the WAP-4060PE.
5. Click *Finish*.
6. Right-click on *Remote Access Policies*, select *New Remote Access Policy*.
7. Assuming you are using EAP-TLS, name the policy *eap-tls*, and click *Next*.
8. Click *Add...*
If you don't want to set any restrictions and a condition is required, select *Day-And-Time-Restrictions*, and click *Add...*



9. Click *Permitted*, then *OK*. Select *Next*.
10. Select *Grant remote access permission*. Click *Next*.
11. Click *Edit Profile...* and select the *Authentication* tab. Enable *Extensible Authentication Protocol*, and select *Smart Card or other Certificate*. Deselect other authentication methods listed. Click *OK*.

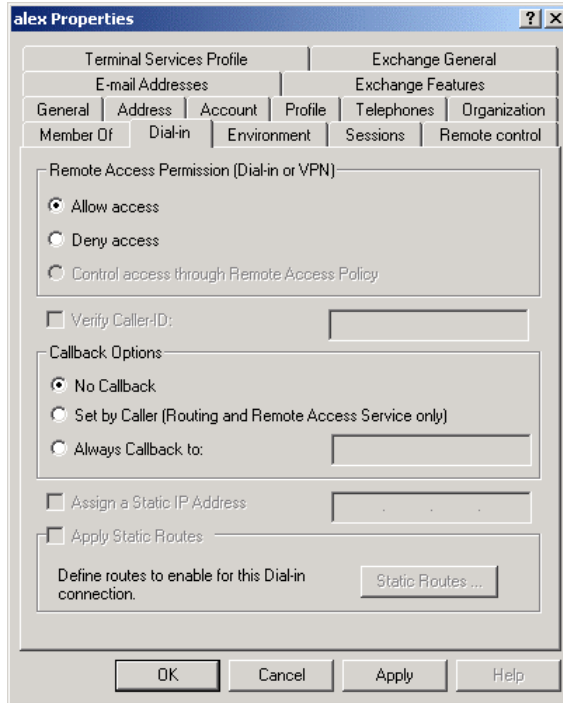


12. Select *No* if you don't want to view the help for EAP. Click *Finish*.

4.5.6 Grant Remote Access for Users

1. Select *Start - Programs - Administrative Tools- Active Directory Users and Computers*.
2. Double click on the user who you want to enable.

3. Select the *Dial-in* tab, and enable *Allow access*. Click *OK*.



4.6 802.1x Client Setup on Windows XP

Windows XP ships with a complete 802.1x client implementation. If using Windows 2000, you can install SP3 (Service Pack 3) to gain the same functionality.

If you don't have either of these systems, you must use the 802.1x client software provided with your wireless adapter. Refer to the documentation of your wireless adapter for setup instructions.

The following instructions assume that:

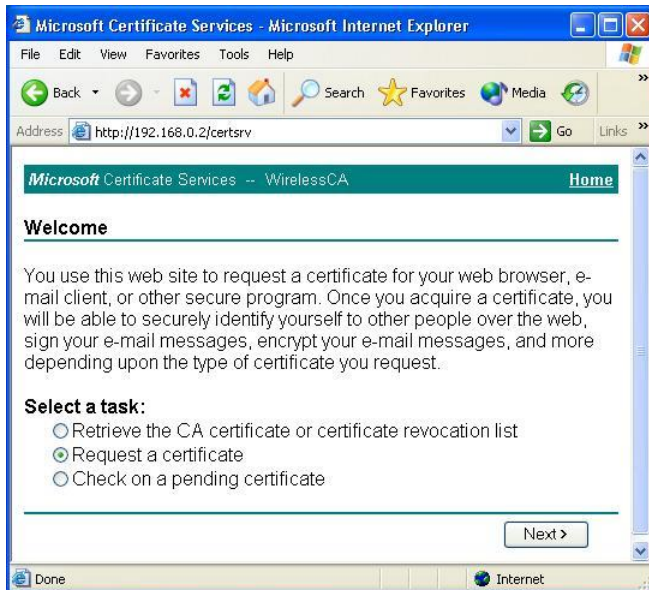
- You are using Windows XP
- You are connecting to a Windows 2000 server for authentication.
- You already have a login (User name and password) on the Windows 2000 server.

4.6.1 Client Certificate Setup

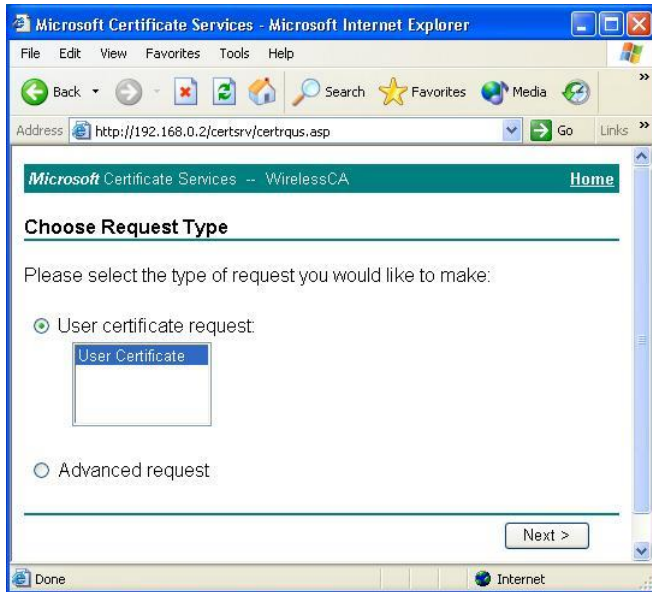
1. Connect to a network which doesn't require port authentication.
2. Start your Web Browser. In the *Address* box, enter the IP address of the Windows 2000 Server, followed by */certsrv*
For example: `http://192.168.0.2/certsrv`
3. You will be prompted for a user name and password. Enter the *User name* and *Password* assigned to you by your network administrator, and click *OK*.



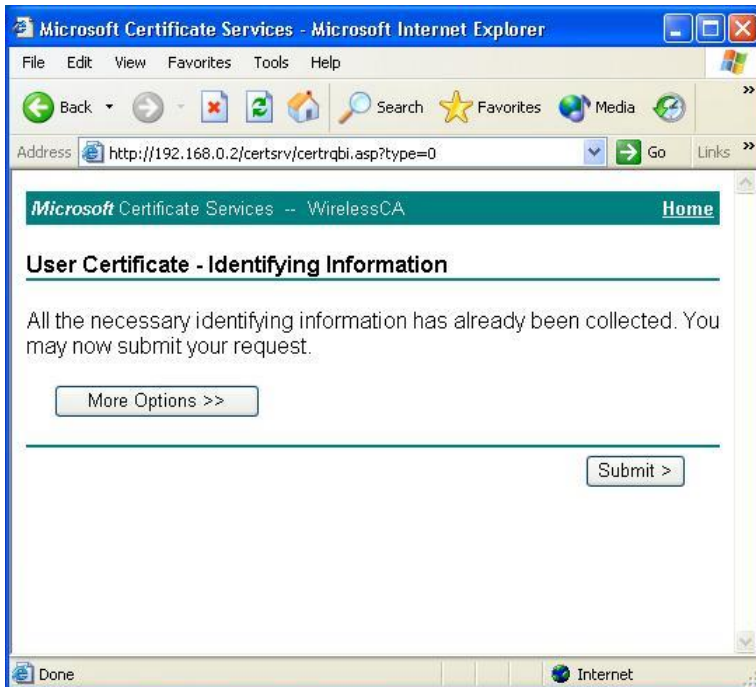
4. On the first screen (below), select *Request a certificate*, click *Next*.



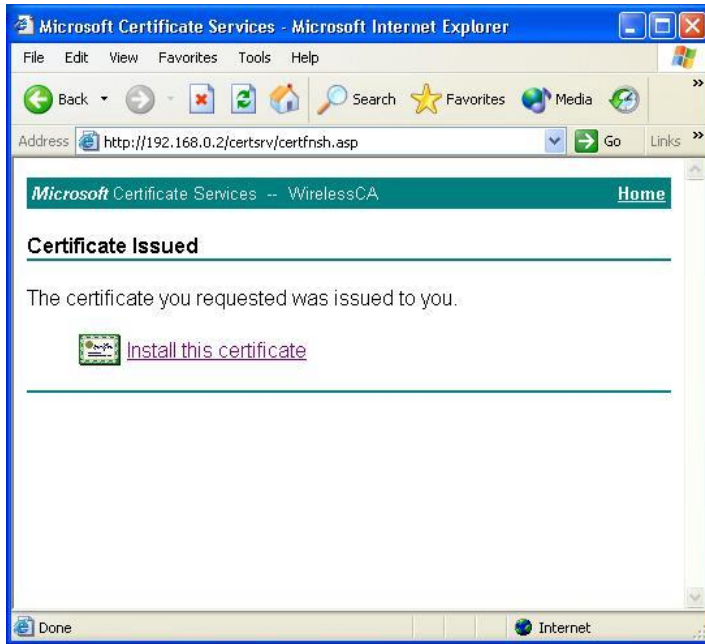
5. Select *User certificate request* and select *User Certificate*, the click *Next*.



6. Click *Submit*.



7. A message will be displayed, then the certificate will be returned to you. Click *Install this certificate*.



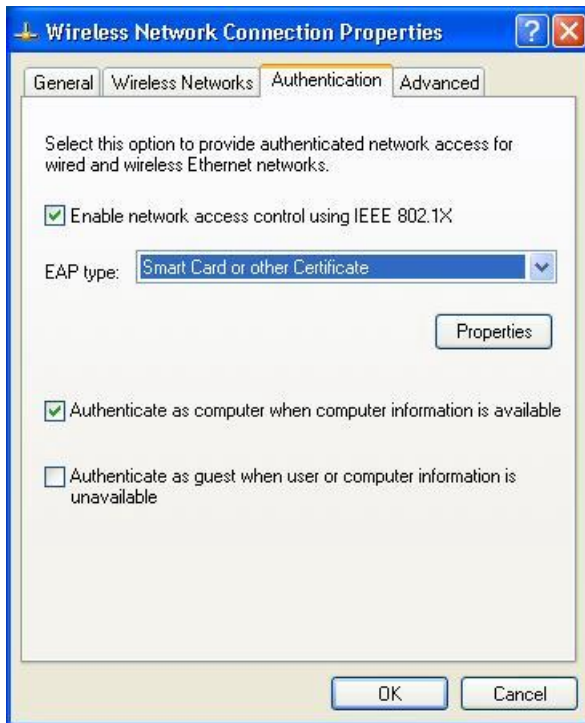
- . You will receive a confirmation message. Click Yes.



- Certificate setup is now complete.

4.6.2 802.1x Authentication Setup

- Open the properties for the wireless connection, by selecting *Start - Control Panel - Network Connections*.
- Right Click on the *Wireless Network Connection*, and select *Properties*.
- Select the *Authentication Tab*, and ensure that *Enable network access control using IEEE 802.1X* is selected, and *Smart Card or other Certificate* is selected from the EAP type.



Encryption Settings

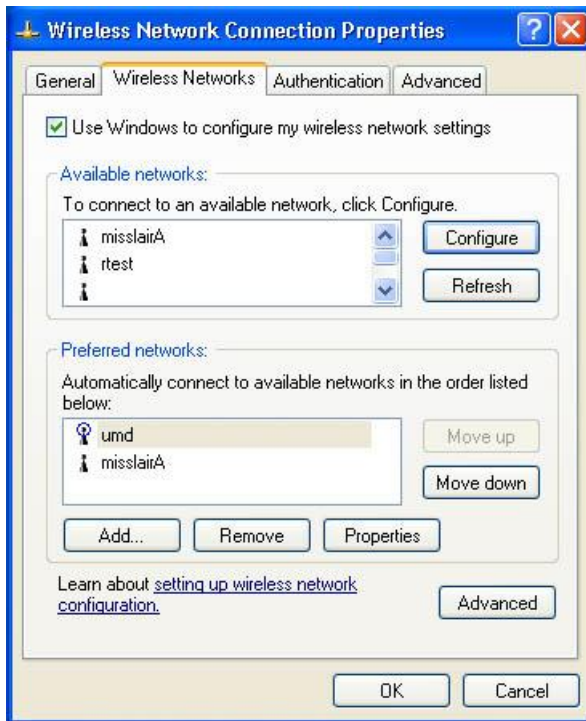
The Encryption settings must match the APs (WAP-4060PE) on the Wireless network you want to join.

- Windows XP will detect any available Wireless networks, and allow you to configure each network independently.
- Your network administrator can advise you of the correct settings for each network. 802.1x networks typically use EAP-TLS. This is a dynamic key system, so there is no need to enter key values.

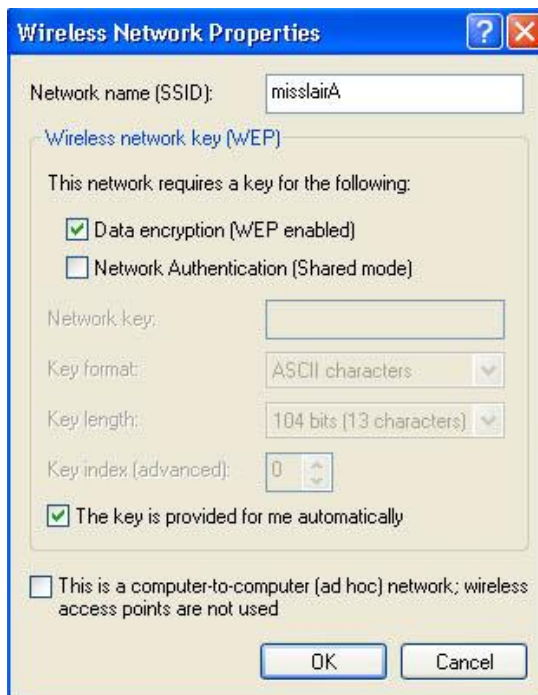
Enabling Encryption

To enable encryption for a wireless network, follow this procedure:

1. Click on the *Wireless Networks* tab.



2. Select the wireless network from the *Available Networks* list, and click *Configure*.
3. Select and enter the correct values, as advised by your Network Administrator. For example, to use EAP-TLS, you would enable *Data encryption*, and click the checkbox for the setting: *The key is provided for me automatically*, as shown below.



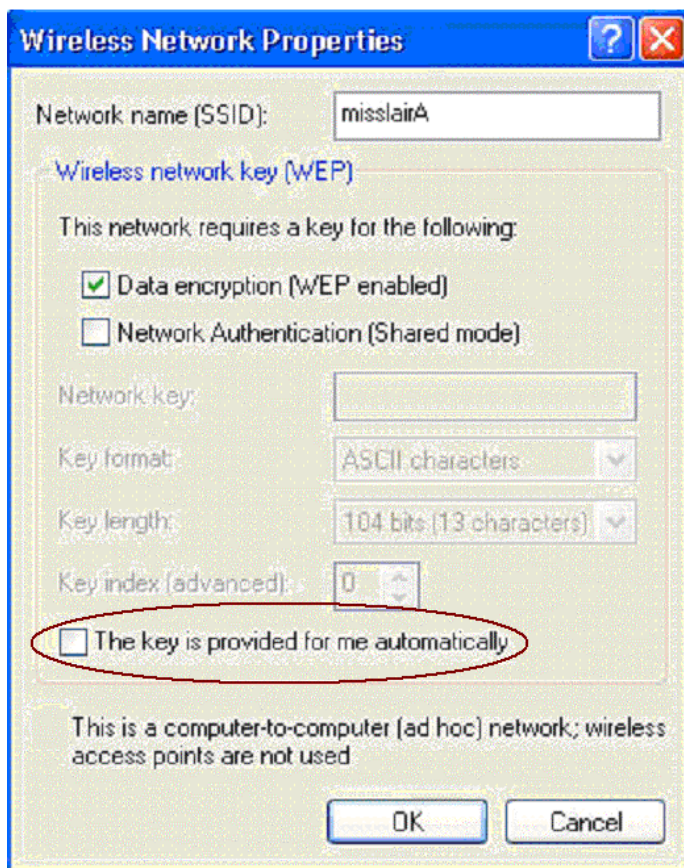
Setup for Windows XP and 802.1x client is now complete.

4.7 Using 802.1x Mode (without WPA)

The procedures are similar to using WPA-802.1x.

The only difference is that on your client, you must NOT enable the setting: *The key is provided for me automatically*.

Instead, you must enter the WEP key manually, ensuring it matches the WEP key used on the Access Point.



Note:

On some systems, the "64 bit" WEP key is shown as "40 bit" and the "128 bit" WEP key is shown as "104 bit". This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

Chapter 5

Operation and Status



5.1 Operation

Once both the WAP-4060PE and the PCs are configured, operation is automatic.

However, you may need to perform the following operations on a regular basis.

- If using the *Access Control* feature, update the *Trusted PC* database as required. (See *Access Control* in Chapter 3 for details.)
- If using 802.1x mode, update the *User Login* data on the Windows 2000 Server, and configure the client PCs, as required.

5.2 Status Screen

Use the **Status** link on the main menu to view this screen.

Status

Access Point

Access Point Name	PLE0046A
MAC Address	00:C0:02:E0:04:6A
Domain	United States
Firmware Version	Version 2.0 Release 35

TCP/IP

IP Address	210.66.155.66
Subnet Mask	255.255.255.224
Gateway	210.66.155.94
DHCP Client	Disabled

Wireless

Channel/Frequency	10 (Automatic)
Wireless Mode	802.11b and 802.11g
AP Mode	Access Point
Bridge Mode	None (disable)

2.4 GHz Statistics

Security Profiles

Name	SSID	Status
wireless	wireless	Enabled
Profile02	wireless	Disabled
Profile03	wireless	Disabled
Profile04	wireless	Disabled
Profile05	wireless	Disabled
Profile06	wireless	Disabled
Profile07	wireless	Disabled
Profile08	wireless	Disabled

Profile Status

Log **Stations** **Help**

Data - Status Screen

Access Point	
Access Point Name	The current name will be displayed.
MAC Address	The MAC (physical) address of the WAP-4060PE.
Domain	The region or domain, as selected on the System screen.
Firmware Version	The version of the firmware currently installed.
TCP/IP	
IP Address	The IP Address of the WAP-4060PE.
Subnet Mask	The Network Mask (Subnet Mask) for the IP Address above.
Gateway	Enter the Gateway for the LAN segment to which the WAP-4060PE is attached (the same value as the PCs on that LAN segment).
DHCP Client	This indicates whether the current IP address was obtained from a DHCP Server on your network. It will display "Enabled" or "Disabled".
Wireless	
Channel/Frequency	The Channel currently in use is displayed.
Wireless Mode	The current mode (e.g. 802.11g) is displayed.
AP Mode	The current Access Point mode is displayed.
Bridge Mode	The current Bridge mode is displayed.
Security Profiles	
Name	This displays the current name of each security profile.
SSID	This displays the SSID associated with the profile.
Status	This indicates whether or not the profile is enabled.
Buttons	
Statistics	Click this to open a sub-window where you can view Statistics on data transmitted or received by the WAP-4060PE.
Profile Status	Click this to open a sub-window which displays further details about each security profile.
Log	Click this to open a sub-window where you can view the activity log.
Stations	Click this to open a sub-window where you can view the list of all current Wireless Stations using the WAP-4060PE.

5.3.1 Statistics Screen

This screen is displayed when the *2.4GHz Statistics* button on the *Status* screen is clicked. It shows details of the traffic flowing through the WAP-4060PE.

Statistics				
Up Time:		00:07:39		
2.4GHz Wireless				
Authentication	Deauthentication	Association	Disassociation	Reassociation
0	0	0	0	0
		Received	Transmitted	
MSDU	0	3418		
Data	0	3050		
Multicast	0	3061		
Management	46154	485		
Control	0	0		
<input type="button" value="Refresh"/>				

Data - Statistics Screen

System Up Time	
System Up Time	This indicates the time period which the system has been running since the last restart or reboot.
2.4GHz Wireless	
Authentication	The number of "Authentication" packets received. Authentication is the process of identification between the AP and the client.
Deauthentication	The number of "Deauthentication" packets received. Deauthentication is the process of ending an existing authentication relationship.
Association	The number of "Association" packets received. Association creates a connection between the AP and the client. Usually, clients associate with only one AP at any time.
Disassociation	The number of "Disassociation" packets received. Disassociation breaks the existing connection between the AP and the client.
Reassociation	The number of "Reassociation" packets received. Reassociation is the service that enables an established association (between AP and client) to be transferred from one AP to another (or the same) AP.
Wireless	
MSDU	Number of valid Data packets transmitted to or received from Wireless Stations, at application level.
Data	Number of valid Data packets transmitted to or received from Wireless Stations, at driver level.

Multicast Packets	Number of Broadcast packets transmitted to or received from Wireless Stations, using Multicast transmission.
Management	Number of Management packets transmitted to or received from Wireless Stations.
Control	Number of Control packets transmitted to or received from Wireless Stations.

5.3.2 Profile Status

The **Profile Status** screen is displayed when the *Profile Status* button on the Status screen is clicked.

Profile Status						
Name	SSID	Broadcast SSID	Security	Band	Status	Clients
wireless	wireless	Enable	None	2.4 GHz	Enabled	1
Profile02	wireless	Disable	None	2.4 GHz	Disabled	0
Profile03	wireless	Disable	None	2.4 GHz	Disabled	0
Profile04	wireless	Disable	None	2.4 GHz	Disabled	0
Profile05	wireless	Disable	None	2.4 GHz	Disabled	0
Profile06	wireless	Disable	None	2.4 GHz	Disabled	0
Profile07	wireless	Disable	None	2.4 GHz	Disabled	0
Profile08	wireless	Disable	None	2.4 GHz	Disabled	0

For each profile, the following data is displayed:

Name	The name you gave to this profile; if you didn't change the name, the default name is used.
SSID	The SSID assigned to this profile.
Broadcast SSID	Indicates whether or not the SSID is broadcast.
Band	The Wireless band used by this profile.
Status	Indicates whether or not this profile is enabled.
Clients	The number of wireless stations currently using accessing this WAP-4060PE using this profile. If the profile is disabled, this will always be zero.

5.3.3 Activity Log

This screen is displayed when the *Log* button on the *Status* screen is clicked.

Activity Log

Current time: 2004 Jan 1 04:54:36 GMT

```
[2004 Jan 1 00:00:00 GMT] AP activated
[2004 Jan 1 00:21:01 GMT] 00:04:23:73:19:61 authenticated
[2004 Jan 1 00:21:01 GMT] 00:04:23:73:19:61 associated
[2004 Jan 1 00:27:32 GMT] 00:C0:02:03:05:66 authenticated
[2004 Jan 1 00:27:32 GMT] 00:C0:02:03:05:66 associated
[2004 Jan 1 00:38:35 GMT] 00:04:23:73:19:61 disconnected(Idle Timeout)
[2004 Jan 1 00:38:35 GMT] 00:04:23:73:19:61 disassociated
[2004 Jan 1 00:38:36 GMT] 00:04:23:73:19:61 authenticated
[2004 Jan 1 00:38:36 GMT] 00:04:23:73:19:61 associated
[2004 Jan 1 04:07:30 GMT] 00:04:23:73:19:61 disassociated
[2004 Jan 1 04:07:49 GMT] 00:04:23:73:19:61 authenticated
[2004 Jan 1 04:07:49 GMT] 00:04:23:73:19:61 associated
[2004 Jan 1 04:28:22 GMT] 00:0C:43:71:01:12 authenticated
[2004 Jan 1 04:28:22 GMT] 00:0C:43:71:01:12 associated
[2004 Jan 1 04:28:45 GMT] 00:0C:43:71:01:12 disassociated
[2004 Jan 1 04:31:23 GMT] 00:0E:35:09:4D:65 authenticated
[2004 Jan 1 04:31:23 GMT] 00:0E:35:09:4D:65 associated
[2004 Jan 1 04:36:34 GMT] 00:0E:35:09:4D:65 disconnected(Idle Timeout)
[2004 Jan 1 04:36:34 GMT] 00:0E:35:09:4D:65 disassociated
[2004 Jan 1 04:47:26 GMT] 00:04:23:73:19:61 disconnected(Idle Timeout)
[2004 Jan 1 04:47:26 GMT] 00:04:23:73:19:61 disassociated
[2004 Jan 1 04:47:26 GMT] 00:04:23:73:19:61 authenticated
[2004 Jan 1 04:47:26 GMT] 00:04:23:73:19:61 associated
```

Data - Activity Log

Data	
Current Time	The system date and time is displayed.
Log	The Log shows details of the connections to the WAP-4060PE.
Buttons	
Refresh	Update the data on screen.
Save to file	Save the log to a file on your pc.
Clear Log	This will delete all data currently in the Log. This will make it easier to read new messages.

5.3.4 Station List

This screen is displayed when the *Stations* button on the *Status* screen is clicked.



Data - Station List Screen

Station List	
Name	The name of each Wireless Station is displayed. If the name is not known, "unknown" is displayed for the name.
MAC Address	The MAC (physical) address of each Wireless Station is displayed.
Mode	The mode of each Wireless Station.
SSID	This displays the SSID used the Wireless station. Because the WAP-4060PE supports multiple SSIDs, different PCs could connect using different SSIDs.
Status	This indicates the current status of each Wireless Station.
Refresh Button	Update the data on screen.

Chapter 6 Management



6.1 Overview

This Chapter covers the following features, available on the WAP-4060PE's **Management** menu.

- Admin Login
- Auto Config/Update
- Config File
- Log Settings
- Rogue APs
- SNMP
- Upgrade Firmware

6.2 Admin Login Screen

The Admin Login screen allows you to assign a password to the WAP-4060PE. This password limits access to the configuration interface. The default password is *password*. It is recommended to change it for security consideration.

Admin Login

Login

User Name

Change Admin Password

New Password

Repeat New Password

Admin Connections

Allow Admin connections via wired Ethernet only

Enable HTTP Admin connections

HTTP Port Number:

Enable HTTPS (secure HTTP) Admin connections

HTTPS Port Number:

Enable Management via Telnet

Data - Admin Login Screen

Login	
User Name	Enter the login name for the Administrator.

Change Admin Password	If you wish to change the Admin password, check this field and enter the new login password in the fields below.
New Password	Enter the desired login password.
Repeat New Password	Re-enter the desired login password.
Admin Connections	
Allow Admin connections via wired Ethernet only	If checked, then Admin connections via the Wireless interface will not be accepted.
Enable HTTP	Enable this to allow admin connections via HTTP. If enabled, you must provide a port number in the field below. Either HTTP or HTTPS must be enabled.
HTTP Port Number	Enter the port number to be used for HTTP connections to this device. The default value is 80.
Enable HTTPS	Enable this to allow admin connections via HTTPS (secure HTTP). If enabled, you must provide a port number in the field below. Either HTTP or HTTPS must be enabled.
HTTPS Port Number	Enter the port number to be used for HTTPS connections to this device. The default value is 443.
Enable Telnet	If desired, you can enable this option. If enabled, you will be able to connect to this AP using a Telnet client. You will have to provide the same login data (user name, password) as for a HTTP (Web) connection.

6.3 Auto Config/Update

The Auto Config/Update screen provides two features:

- **Auto Config** - The Access Point will configure itself by copying data from another (compatible) Access Point.
- **Auto Update** - The Access Point will update its Firmware by downloading the Firmware file from your FTP Server.

Auto Config/Auto Update

Auto Config	<input type="checkbox"/> Perform Auto Configuration on this AP next restart <input type="checkbox"/> Respond to Auto-configuration request by other AP <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Provide admin login name and password <input type="checkbox"/> Provide "Respond to Auto-configuration" setting
Auto Update	<input type="checkbox"/> Check for Firmware upgrade every <input type="text" value="1"/> days <input checked="" type="radio"/> Install FW if different version found <input checked="" type="radio"/> Install later version only FTP Server address: <input type="text"/> Firmware pathname: <input type="text"/> FTP Login Name: <input type="text"/> FTP Password: <input type="text"/>

Data - Auto Config/Update Screen

Admin Connections	
Perform Auto Configuration on this AP next restart	<p>If checked, this AP will perform Auto Configuration the next time it restarts.</p> <ul style="list-style-type: none"> The wired LAN (NOT the Wireless LAN) will be searched for compatible APs. If a compatible AP is found, its configuration is copied. If more than one compatible AP exists, the first one found is used. Some data cannot be copied: <ul style="list-style-type: none"> The IP address is not copied, and will not change. The operating mode (Repeater, Bridge, etc) is not copied, and will not change. <p>Note: This checkbox is automatically disabled, so the Auto-configuration is only performed once.</p>
Respond to Auto-configuration request by other AP	<p>If checked, this AP will respond to "Auto Configuration" requests it receives. If not checked, "Auto Configuration" requests will be ignored.</p>
Provide login name and password	<p>If enabled, the login name and password on this AP is supplied to the AP making the Auto-configuration request. If disabled, the AP making the Auto-configuration request will keep its existing login name and password.</p>

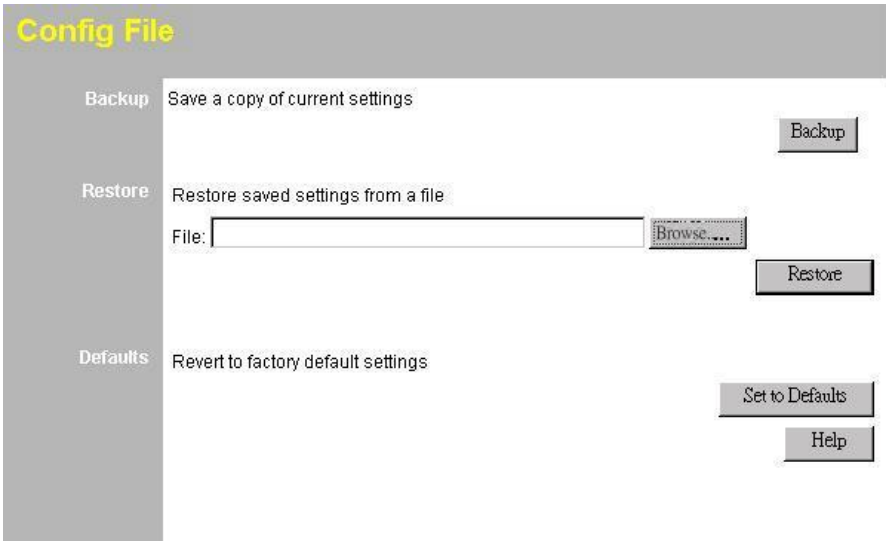
Provide "Respond to Auto-configuration" setting	If enabled, the "Respond to Auto-configuration" setting on this AP is supplied to the AP making the Auto-configuration request. If disabled, the AP making the Auto-configuration request will keep its existing setting.
Auto Update	
Check for Firmware upgrade	<p>If enabled, this AP will check to see if a Firmware (FW) upgrade is available on the specified FTP Server. If enabled:</p> <ul style="list-style-type: none"> • Enter the desired time interval (in days) between checks. • Select the desired option for installation (see next item). • Provide the FTP server information.
Install...	<p>Select the desired option:</p> <ul style="list-style-type: none"> • Install FW if different version found If selected, and the firmware file at the specified location is different to the current installed version, the FW will be installed. This allows "Downgrades" - installing an older version of the FW to replace the current version. • Install later version only If selected, the firmware file at the specified location will only be installed if it is a later version.
FTP Server address	Enter the address (domain name or IP address) of the FTP Server.
Firmware pathname	Enter the full path (including the FW filename) to the FW file on the FTP Server.
FTP Login Name	Enter the login name required to gain access to the FTP Server.
FTP Password	Enter the password for the login name above.

6.4 Config File

This screen allows you to Backup (download) the configuration file, and to restore (upload) a previously saved configuration file.

You can also set the WAP-4060PE back to its factory default settings.

To reach this screen, select *Config File* in the **Management** section of the menu.



Data - Config File Screen

Backup	
<p>Save a copy of current settings</p>	<p>Once you have the WAP-4060PE working properly, you should back up the settings to a file on your computer. You can later restore the settings from this file, if necessary.</p> <p>To create a backup file of the current settings:</p> <ul style="list-style-type: none"> • Click Back Up. • If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click Save.
Restore	
<p>Restore saved settings from a file</p>	<p>To restore settings from a backup file:</p> <ol style="list-style-type: none"> 1. Click Browse. 2. Locate and select the previously saved backup file. 3. Click Restore
Defaults	
<p>Revert to factory default settings</p>	<p>To erase the current settings and restore the original factory default settings, click Set to Defaults button.</p> <p>Note:</p> <ul style="list-style-type: none"> • This will terminate the current connection. The WAP-4060PE will be unavailable until it has restarted. • By default, the WAP-4060PE will act as a DHCP client, and automatically obtain an IP address. You will need to determine its new IP address in order to re-connect.

6.5 Log Settings (Syslog)

If you have a log server on your LAN, this screen allows you to configure the WAP-4060PE to send log data to your log server.

Syslog

Syslog Server

Disable

Broadcast

Send to specified Syslog Server

Syslog Server Address:
(Name/IP address)

Minimum Severity Level:

Save Cancel Help

Data - Log Settings Screen

Syslog Server	Select the desired Option: <ul style="list-style-type: none">• Disable - Syslog server is not used.• Broadcast - Syslog data is broadcast. Use this option if different PCs act as the Syslog server at different times.• Send to specified Syslog Server - Select this if the same PC is always used as the Syslog server. If selected, you must enter the server address in the field provided.
Syslog Server Address	Enter the name or IP address of your Syslog Server.
Minimum Severity Level	Select the desired severity level. Events with a severity level equal to or higher (i.e. lower number) than the selected level will be logged.

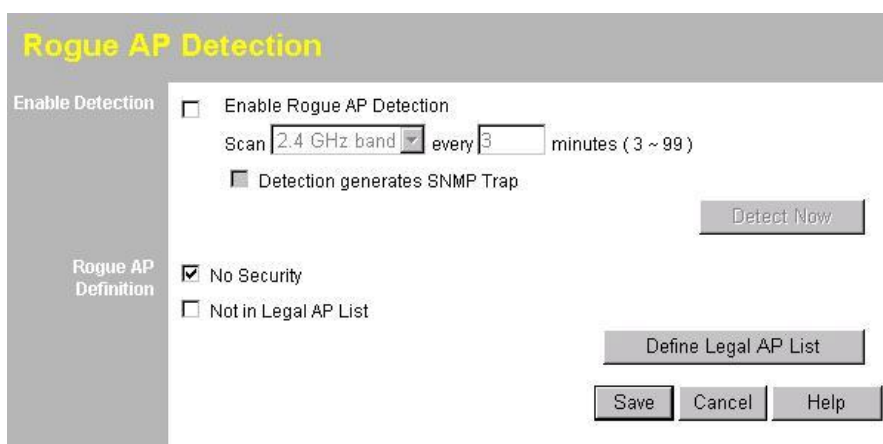
6.6 Rogue APs

A "Rogue AP" is an Access Point which should not be in use, and so can be considered to be providing unauthorized access to your LAN.

This WAP-4060PE can assist to locate 2 types of Rogue APs:

- APs which have Wireless security disabled.
- APs which are not in the list of valid APs which you have entered.

When a Rogue AP is located, it is recorded in the log. If using SNMP, you can also choose to have detection of a Rogue AP generate an SNMP trap.



Data - Rogue AP Screen

Enable Detection	
Enable Detection	To use this feature, enable the "Enable Rogue AP Detection" checkbox, and select the desired wireless band and time interval.
Scan	Select the desired Wireless band to scan to Rogue APs and enter the desired time interval between each scan.
Detection generates SNMP Trap	If using SNMP, checking this option will generate a SNMP trap whenever a Rogue AP is detected. If not using SNMP, do not enable this option.
Rogue Detection	
No Security	If checked, any AP operating with security disabled is considered to be a Rogue AP.
Not in Legal AP List	If checked, any AP not listed in the "Legal AP List" is considered to be a Rogue AP. If checked, you must maintain the Legal AP List.
Define Legal AP List	Click this button to open a sub-screen where you can modify the "Legal AP List". This list must contain all known APs, so must be kept up to date.

6.7 SNMP

SNMP (Simple Network Management Protocol) is only useful if you have a SNMP program on your PC. To reach this screen, select *SNMP* in the **Management** section of the menu.

SNMP

General

Enable SNMP

Community:

Access Rights:

Managers

Managers: Any Station

Only this Station: ...

Traps

Disable

Broadcast

Send to: ...

Trap Version:

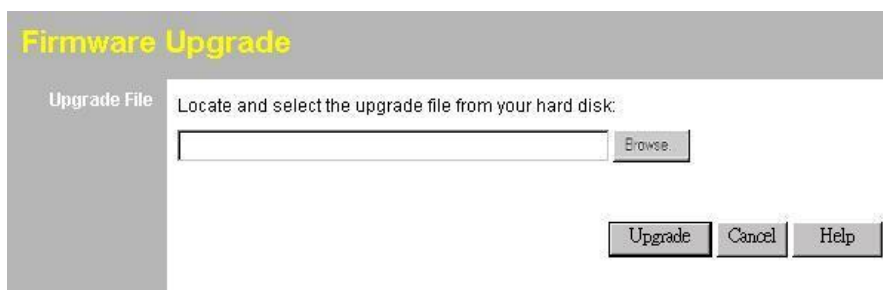
Data - SNMP Screen

General	
Enable SNMP	Use this to enable or disable SNMP as required
Community	Enter the community string, usually either "Public" or "Private".
Access Rights	Select the desired option: <ul style="list-style-type: none"> Read-only - Data can be read, but not changed. Read/Write - Data can be read, and setting changed.
Managers	
Any Station	The IP address of the manager station is not checked.
Only this station	The IP address is checked, and must match the address you enter in the IP address field provided. If selected, you must enter the IP address of the required station.
Traps	
Disable	Traps are not used.
Broadcast	Select this to have Traps broadcast on your network. This makes them available to any PC.
Send to	Select this to have Trap messages sent to the specified PC only. If selected, you must enter the IP Address of the desired PC.
Trap version	Select the desired option, as supported by your SNMP Management program.

6.8 Upgrade Firmware

The firmware (software) in the Wireless Access Point can be upgraded using your Web Browser.

You must first download the upgrade file, and then select *Upgrade Firmware* in the **Management** section of the menu. You will see a screen like the following.



The screenshot shows a web interface titled "Firmware Upgrade". On the left, there is a vertical label "Upgrade File". To the right, the text "Locate and select the upgrade file from your hard disk:" is displayed above a text input field. A "Browse..." button is positioned to the right of the input field. At the bottom right of the form, there are three buttons: "Upgrade", "Cancel", and "Help".

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the *Upgrade* button to commence the firmware upgrade.

Note: The WAP-4060PE is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the WAP-4060PE will be lost.

Appendix A

Specifications



Model	WAP-4060PE	
Standard	IEEE 802.11b, 802.11g	
Signal Type	DSSS (Direct Sequence Spread Spectrum)	
Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK	
Port	10/100Mbps RJ-45 port * 1, 802.3af compliant	
Antenna Connector	Reverse SMA male * 1	
Output Power	18dBm	
Sensitivity	802.11b	11 Mbps (CCK): -85dBm 5.5 Mbps (QPSK): - 89dBm 1, 2 Mbps (BPSK): - 90dBm (typically @PER < 8% packet size 1024 and @25°C ± 5°C)
	802.11g	54 Mbps: -72dBm 48 Mbps: - 72dBm 36 Mbps: -76dBm 24 Mbps: -79dBm 18 Mbps: -82dBm 12 Mbps: -86dBm 9 Mbps: -89dBm 6 Mbps: -90dBm (typically @PER < 8% packet size 1024 and @25°C + 5°C)
Operating Mode	AP, AP Client, Wireless Bridge, Multiple Bridge, Repeater	
Security	Open, shared, WPA, and WPA-PSK authentication 802.1x support EAP-TLS, EAP-TTLS, PEAP Block inter-wireless station communication Block SSID broadcast	

Management	Web based configuration RADIUS Accounting RADIUS-On feature RADIUS Accounting update CLI Message Log Access Control list file support Configuration file Backup/Restore Statistics support Device discovery program Windows Utility	
Data Rate	Super G mode	Up to 108Mbps
	802.11g	Up to 54Mbps (6/9/12/18/24/36/48/54)
	802.11b	Up to 11Mbps (1/2/5.5/11)
Dimensions (L x W x H)	150 x 102 x 30mm	
Weight	210g	
Environmental Specification	Operating temperature: 0 – 40 degree C Storage temperature: -20 – 70 degree C Relative humidity: 0% – 90% (non-condensing)	
Power Requirement	24V DC, 0.5A	
Electromagnetic Compatibility	FCC, CE	

Appendix B

Troubleshooting



Problem 1: Can't connect to the WAP-4060PE to configure it.

Solution 1: Check the following:

- The WAP-4060PE is properly installed, LAN connections are OK, and it is powered ON. Check the LEDs for port status.
- Ensure that your PC and the WAP-4060PE are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- You can use the following method to determine the IP address of the WAP-4060PE, and then try to connect using the IP address, instead of the name.

To Find the Access Point's IP Address

1. Open a MS-DOS Prompt or Command Prompt Window.
2. Use the Ping command to "ping" the WAP-4060PE. Enter ping followed by the Default Name of the WAP-4060PE.
e.g.

```
ping PL003318
```
3. Check the output of the ping command to determine the IP address of the WAP-4060PE.

If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address which is compatible with the WAP-4060PE. (If no DHCP Server is found, the WAP-4060PE will default to an IP Address and Mask of 192.168.0.228 and 255.255.255.0.) On Windows PCs, you can use *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Problem 2: My PC can't connect to the LAN via the WAP-4060PE.

Solution 2 Check the following:

- The SSID and WEP settings on the PC match the settings on the WAP-4060PE.
- On the PC, the wireless mode is set to "Infrastructure"
- If using the *Access Control* feature, the PC's name and address is in the *Trusted Stations* list.
- If using 802.1x mode, ensure the PC's 802.1x software is configured correctly.

Appendix C



Command Line Interface

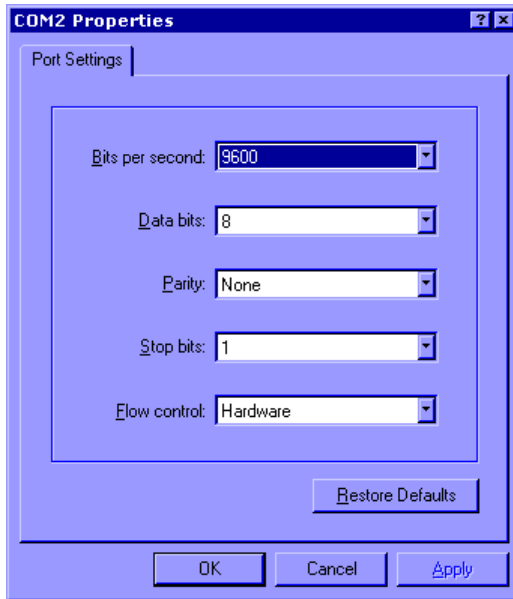
If desired, the Command Line Interface (CLI) can be used for configuration. This creates the possibility of creating scripts to perform common configuration changes. The CLI requires either a Telnet connection or a physical connection from your PC to the serial port (RS232 port) on the WAP-4060PE.

C.1 Using the CLI - Telnet

1. Start your Telnet client, and establish a connection to the WAP-4060PE.
e.g.
Telnet 192.168.0.228
2. You will be prompted for the user name and password. Enter the same login name and password as used for the HTTP (Web) interface.
The default values are **admin** for the User Name, and **password** for the Password.
3. Once connected, you can use any of the commands listed in the following **Command Reference**.

C.2 Using the CLI - Serial Port

1. Use a standard serial port cable to connect your PC to the serial (RS232) port on the WAP-4060PE.
2. Start your communications program. For example, in Windows, use HyperTerminal. (This program may not be installed. If so, you can install it using *Start - Settings - Control Panel - Add or Remove Programs*. Then select *Windows Setup* or *Add/Remove Windows Components*, depending on your version of Windows.)
3. Configure the connection properties:
 - **Name** - use a suitable name, such as "AP"
 - **"Port" or "Connect Using"** - Select the Serial Port that the cable is connected to. (Do not select your modem.)
 - **Port Settings** - Use 9600, N, 8, 1, with hardware flow control, as shown below.



4. Use the “Connect” command to start the connection.
5. You will be prompted for a user name and password.
Enter the current user name and password for the AP you are connecting to.
The default values are **admin** for the User Name, and **password** for the Password.
6. You will then see the prompt, and can use any of the commands listed in the following **Command Reference**.

C.3 Command Reference

The following commands are available.

?	Display CLI Command List
admin	Temporary factory admin
config wlan	config wlanX
config profile	config profile
del acl	Delete Access Control List
del key	Delete Encryption key
find bss	Find BSS
find channel	Find Available Channel
find all	Find All BSS
format	Format flash filesystem
bootrom	Update boot rom image
ftp	Software update via FTP

get 11gonly	Display 11g Only Allowed
get 11goptimize	Display 11g Optimization Level
get 11goverlapbss	Display Overlapping BSS Protection
get acl	Display Access Control List
get aging	Display Aging Interval
get antenna	Display Antenna Diversity
get association	Display Association Table
get authentication	Display Authentication Type
get autochannelselect	Display Auto Channel Select
get basic11b	Display Basic 11b Rates
get basic11g	Display Basic 11g Rates
get beaconinterval	Display Beacon Interval
get burstSeqThreshold	Display Max Number of frames in a Burst
get burstTime	Display Burst Time
get calibration	Display Noise And Offset Calibration Mode
get cckTrigHigh	Display Higher Trigger Threshold for CCK Phy Errors for ANI Control
get cckTrigLow	Display Lower Trigger Threshold for CCK Phy Errors for ANI Control
get cckWeakSigThr	Display ANI Parameter for CCK Weak Signal Detection Threshold
get channel	Display Radio Channel
get cipher	Display Encryption cipher
get compproc	Display Compression scheme
get compwsize	Display Compression Window Size
get config	Display Current AP Configuration
get countrycode	Display Country Code
get ctsmode	Display CTS mode
get ctsrate	Display CTS rate

get ctstype	Display CTS type
get domainsuffix	Display Domain Name Server suffix
get dtim	Display Data Beacon Rate (DTIM)
get enableANI	Display Adaptive Noise Immunity Control On/Off
get encryption	Display Encryption Mode
get extendedchan-mode	Display Extended Channel Mode
get firStepLvl	Display ANI Parameter for FirStepLevel
get fragmentthresh-old	Display Fragment Threshold
get frequency	Display Radio Frequency (MHz)
get gateway	Display Gateway IP Address
get gbeaconrate	Display 11g Beacon Rate
get gdraft5	Display 11g Draft 5.0 compatibility
get groupkeyupdate	Display Group Key Update Interval (in Seconds)
get hardware	Display Hardware Revisions
get hostipaddr	Display Host IP Address
get ipaddr	Display IP Address
get ipmask	Display IP Subnet Mask
get keyentrymethod	Display Encryption Key Entry Method
get keysource	Display Source Of Encryption Keys
get login	Display Login User Name
get minimumrate	Display Minimum Rate
get nameaddr	Display IP address of name server
get nf	Display Noise Floor
get noiseImmunityLvl	Display ANI Parameter for Noise Immunity Level
get ofdmTrigHigh	Display Higher Trigger Threshold for OFDM Phy Errors for ANI Control
get ofdmTrigLow	Display Lower Trigger Threshold for OFDM Phy Errors for ANI Control
get ofdmWeakSigDet	Display ANI Parameter for OFDM Weak Signal Detection

get overRidetxtpower	Display Tx power override
get operationMode	Display Operation Mode
get power	Display Transmit Power Setting
get quietAckCtsAllow	Display if Ack/Cts frames are allowed during quiet period
get quietDuration	Display Duration of quiet period
get quietOffset	Display Offset of quiet period into the beacon period
get radiusname	Display RADIUS server name or IP address
get radiusport	Display RADIUS port number
get rate	Display Data Rate
get remoteAp	Display Remote Ap's Mac Address
get hwtxretries	Display HW Transmit Retry Limit
get swtxretries	Display SW Transmit Retry Limit
get rtsthreshold	Display RTS/CTS Threshold
get shortpreamble	Display Short Preamble Usage
get shortslottime	Display Short Slot Time Usage
get sntpserver	Display SNTP/NTP Server IP Address
get softwareretry	Display Software Retry
get spurImmunityLvl	Display ANI Parameter for Spur Immunity Level
get ssid	Display Service Set ID
get ssidsuppress	Display SSID Suppress Mode
get station	Display Station Status
get SuperG	Display SuperG Feature Status
get systemname	Display Access Point System Name
get telnet	Display Telnet Mode
get timeout	Display Telnet Timeout
get tzone	Display Time Zone Setting
get updateparam	Display Vendor Default Firmware Update Params
get uptime	Display UpTime
get watchdog	Display Watchdog Mode

get wds	Display WDS Mode
get wep	Display Encryption Mode
get wirelessmode	Display Wireless LAN Mode
get 80211d	Display 802.11d mode
get http	Display http Enable/Disable
get HttpPort	Display http port number
get https	Display https Enable/Disable
get HttpsPort	Display https port number
get syslog	Display syslog Disable/Broadcast/Unicast
get syslogSeverity	Display syslog Severity level
get syslogServer	Display unicast syslog server IP/name
get manageOnlyLan	Display Management only via LAN Enable/Disable
get roguedetect	Display Rogue AP Detection Enable/Disable
get rogueinterval	Display Minutes of every Rogue AP Detection(Range: 3 ~ 99)
get rogueband	Display Rogue AP Detection band(s)
get roguetype	Display Rogue AP definition
get roguesnmp	Display Rogue AP Detection SNMP Trap Enable/Disable
get roguelegal	Display Legal AP List of Rogue AP
get autoConfig	Display Auto Config Enable/Disable
get autoResponse	Display Respond to Auto Config request Enable/Disable
get autoChangeName	Display Provide admin login name and password Enable/Disable
get autoSetResp	Display Provide respond to Auto Config request Enable/Disable
get autoUpdate	Display Auto Update Enable/Disable
get autoUpgradeOnly	Display Install later version only Enable/Disable
get autoUpdateInterval	Display Auto Update Interval(1~31days)
get ftpServer	Display FTP Server address
get fwPathname	Display Firmware Pathname

get ftpLogin	Display FTP Login Name
get ftpPassword	Display FTP Password
get activeCurrentProfile	Display active Current Profile
get profileName	Display Profile Name
get profileVlanId	Display Profile VLAN ID
get APPrimaryProfile	Display AP Primary Profile
get WDSPrimaryProfile	Display WDS Primary Profile
get securityMode	Display Security Mode
get Accounting	Display Accounting Enable/Disable
get Accountingport	Display Accounting port number
get keyValue	Display Encryption Key Value
get keyLength	Display Encryption Key Length
get keyIndex	Display Encryption Key Index
get UAM	Display UAM Authentication Enable/Disable
get UAMMethod	Display UAM Authentication Method
get UAMLoginURL	Display UAM Authentication Login URL
get UAMLogin-FailURL	Display UAM Authentication Login Fail URL
get macAuth	Display Mac Authentication Enable/Disable
get snmpMode	Display SNMP Mode
get snmpCommunity	Display SNMP Community Name
get snmpAccess-Right	Display SNMP Access Right
get snmpAnySta-Mode	Display SNMP Any Station Mode
get snmpStation-IPAddr	Display SNMP Station Addr
get trapMode	Display Trap Mode
get trapVersion	Display Trap Version
get trapSendMode	Display Trap Send Mode

get trapRecvIp	Display Trap Receiver IP
get wdsMacList	Display WDS Mac Address List
get enableWireless-Client	Display Wireless Client Enable/Disable
get isolationType	Display Isolation Type
get winsEnable	Display WINS Server Enable/Disable
get winsserveraddr	Display IP address of WINS server
get wirelessSeparate	Display wireless separate Mode
get description	Display Access Point Description
get dhcpmode	Display dhcp mode
get wlanstate	Display wlan state
help	Display CLI Command List
Lebradeb	Disable reboot during radar detection
ls	list directory
mem	system memory statistics
np	Network Performance
ns	Network Performance Server
ping	Ping
radar!	Simulate radar detection on current channel
reboot	Reboot Access Point
rm	Remove file
run	Run command file
quit	Logoff
set 11gonly	Set 11g Only Allowed
set 11goptimize	Set 11g Optimization Level
set 11goverlapbss	Set Overlapping BSS Protection
set acl	Set Access Control List
set aging	Set Aging Interval
set antenna	Set Antenna

set authentication	Set Authentication Type
set autochannelselect	Set Auto Channel Selection
set basic11b	Set Use of Basic 11b Rates
set basic11g	Set Use of Basic 11g Rates
set beaconinterval	Modify Beacon Interval
set burstSeqThreshold	Set Max Number of frames in a Burst
set burstTime	Set Burst Time
set calibration	Set Calibration Period
set cckTrigHigh	Set Higher Trigger Threshold for CCK Phy Errors For ANI Control
set cckTrigLow	Set Lower Trigger Threshold for CCK Phy Errors For ANI Control
set cckWeakSigThr	Set ANI Parameter for CCK Weak Signal Detection Threshold
set channel	Set Radio Channel
set cipher	Set Cipher
set compproc	Set Compression Scheme
set compwinsize	Set Compression Window Size
set countrycode	Set Country Code
set ctsmode	Set CTS Mode
set ctsrate	Set CTS Rate
set ctstype	Set CTS Type
set domainsuffix	Set Domain Name Server Suffix
set dtim	Set Data Beacon Rate (DTIM)
set enableANI	Turn Adaptive Noise Immunity Control On/Off
set encryption	Set Encryption Mode
set extendedchanmode	Set Extended Channel Mode
set factorydefault	Restore to Default Factory Settings
set firStepLvl	Set ANI Parameter for FirStepLevel

set fragmentthresh-old	Set Fragment Threshold
set frequency	Set Radio Frequency (MHz)
set gateway	Set Gateway IP Address
set gbeaconrate	Set 11g Beacon Rate
set groupkeyupdate	Set Group Key Update Interval (in Seconds)
set gdraft5	Set 11g Draft 5.0 compatibility
set hostipaddr	Set Host IP address
set ipaddr	Set IP Address
set ipmask	Set IP Subnet Mask
set keyentrymethod	Select Encryption Key Entry Method
set keysource	Select Source Of Encryption Keys
set login	Modify Login User Name
set minimumrate	Set Minimum Rate
set nameaddress	Set Name Server IP address
set noiseImmunityLvl	Set ANI Parameter for Noise Immunity Level
set ofdmTrigHigh	Set Higher Trigger Threshold for OFDM Phy Errors for ANI Control
set ofdmTrigLow	Set Lower Trigger Threshold for OFDM Phy Errors for ANI Control
set ofdmWeakSigDet	Set ANI Parameter for OFDM Weak Signal Detection
set overRidetxpower	Set Tx power override
set operationMode	Set operation Mode
set password	Modify Password
set passphrase	Modify Passphrase
set power	Set Transmit Power
set quietAckCtsAllow	Allow Ack/Cts frames during quiet period
set quietDuration	Duration of quiet period
set quietOffset	Offset of quiet period into the beacon period
set radiusname	Set RADIUS name or IP address

set radiusport	Set RADIUS port number
set radiussecret	Set RADIUS shared secret
set rate	Set Data Rate
set rate	Set Data Rate
set rate	Set Data Rate
set rate	Set Data Rate
set rate	Set Data Rate
set regulatorydomain	Set Regulatory Domain
set remoteAP	Set Remote AP's Mac Address
set hwtxretries	Set HW Transmit Retry Limit
set swtxretries	Set SW Transmit Retry Limit
set rtsthreshold	Set RTS/CTS Threshold
set shortpreamble	Set Short Preamble
set shortslottime	Set Short Slot Time
set sntpserver	Set SNTP/NTP Server IP Address
set softwareretry	Set Software Retry
set spurImmunityLvl	Set ANI Parameter for Spur Immunity Level
set ssid	Set Service Set ID
set ssidsuppress	Set SSID Suppress Mode
set SuperG	Super G Features
set systemname	Set Access Point System Name
set telnet	Set Telnet Mode
set timeout	Set Telnet Timeout
set tzone	Set Time Zone Setting
set updateparam	Set Vendor Default Firmware Update Parameters
set watchdog	Set Watchdog Mode
set wds	Set WDS Mode
set wep	Set Encryption Mode
set wlanstate	Set wlan state

set wirelessmode	Set Wireless LAN Mode
set 80211d	Set 802.11d mode
set http	Set http Enable/Disable
set HttpPort	Set http port number
set https	Set https Enable/Disable
set HttpsPort	Set https port number
set syslog	Set syslog Disable/Broadcast/Unicast
set syslogSeverity	Set syslog Severity level
set syslogServer	Set unicast syslog server IP/name
set manageOnlyLan	Set Management only via LAN Enable/Disable
set roguedetect	Set Rogue AP Detection Enable/Disable
set rogueteval	Set Minutes of every Rogue AP Detection(Range: 3 ~ 99)
set roguiband	Set Rogue AP Detection band(s)
set roguetype	Set Rogue AP definition
set roguesnmp	Set Rogue AP Detection SNMP Trap Enable/Disable
set roguelegal	Add/Delete one AP MAC/OUI into/from Rogue AP Legal List
set autoConfig	Set Auto Config Enable/Disable
set autoResponse	Set Respond to Auto Config request Enable/Disable
set autoChangeName	Set provide admin login name and password Enable/Disable
set autoSetResp	Set Provide respond to Auto Config request Enable/Disable
set autoUpdate	Set Auto Update Enable/Disable
set autoUpgradeOnly	Set Install later version only Enable/Disable
set autoUpdateInterval	Set Auto Update Interval(1~31days)
set ftpServer	Set FTP Server address
set fwPathname	Set Firmware Pathname
set ftpLogin	Set FTP Login Name
set ftpPassword	Set FTP Password

set activeCurrentProfile	Set active Current Profile
set profileName	Set Profile Name
set profileVlanId	Set Profile Vlan Id
set APPrimaryProfile	Set AP's Primary Profile
set WDSPrimaryProfile	Set WDS's Primary Profile
set securityMode	Set Security Mode
set Accounting	Set Accounting Enable/Disable
set Accountingport	Set Accounting port number
set keyValue	Set Encryption Key Value
set keyLength	Set Encryption Key Length
set keyIndex	Set Encryption Key Index
set UAM	Set UAM Authentication Enable/Disable
set UAMMethod	Set UAM Authentication Method
set UAMLoginURL	Set UAM Authentication Login URL
set UAMLogin-FailURL	Set UAM Authentication Login Fail URL
set macAuth	Set Mac Authentication Enable/Disable
set snmpMode	Set SNMP Mode
set snmpCommunity	Set SNMP Community Name
set snmpAccess-Right	Set SNMP Access Right
set snmpAnySta-Mode	Set SNMP Any Station Mode
set snmpStationI-PAddr	Set SNMP Station Address
set trapMode	Set Trap Mode
set trapVersion	Set Trap Version
set trapSendMode	Set Trap Send Mode
set trapRecvIp	Set Trap Receiver IP
set description	Set Access Point Description

set dhcpMode	Set Dhcp Mode
set wdsMacList	Set WDS Mac Address List
set enableWireless-Client	Set Wireless Client Enable/Disable
set isolationType	Set Isolation Type
set winsEnable	Set WINS Server Enable/Disable
set winsServerAddr	Set WINS Server IP address
set wirelessSeparate	Set wireless separate Mode
set sdSet	Set debug level
set sdAdd	Add debug level
set sdDel	Del debug level
start wlan	Start the current wlan
stop wlan	Stop the current wlan
timeofday	Display Current Time of Day
version	Software version

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>