



ALL1682511

500Mbps Powerline WLAN N Access Point



User's Manual

Contents

1.	Introduction	1
2.	System Requirements	1
3.	Configuration.....	1
4.	WPS.....	9
5.	Wireless AP Settings.....	9
6.	FAQ.....	15
7.	Glossary	21

1. Introduction

The purpose of this document is to present the details on how to use the Wireless AP. There are three interfaces in the AP: Wireless, Ethernet and Powerline. As Figure 1 shows, you can use other Powerline Bridge(s) to connect the AP through power line.

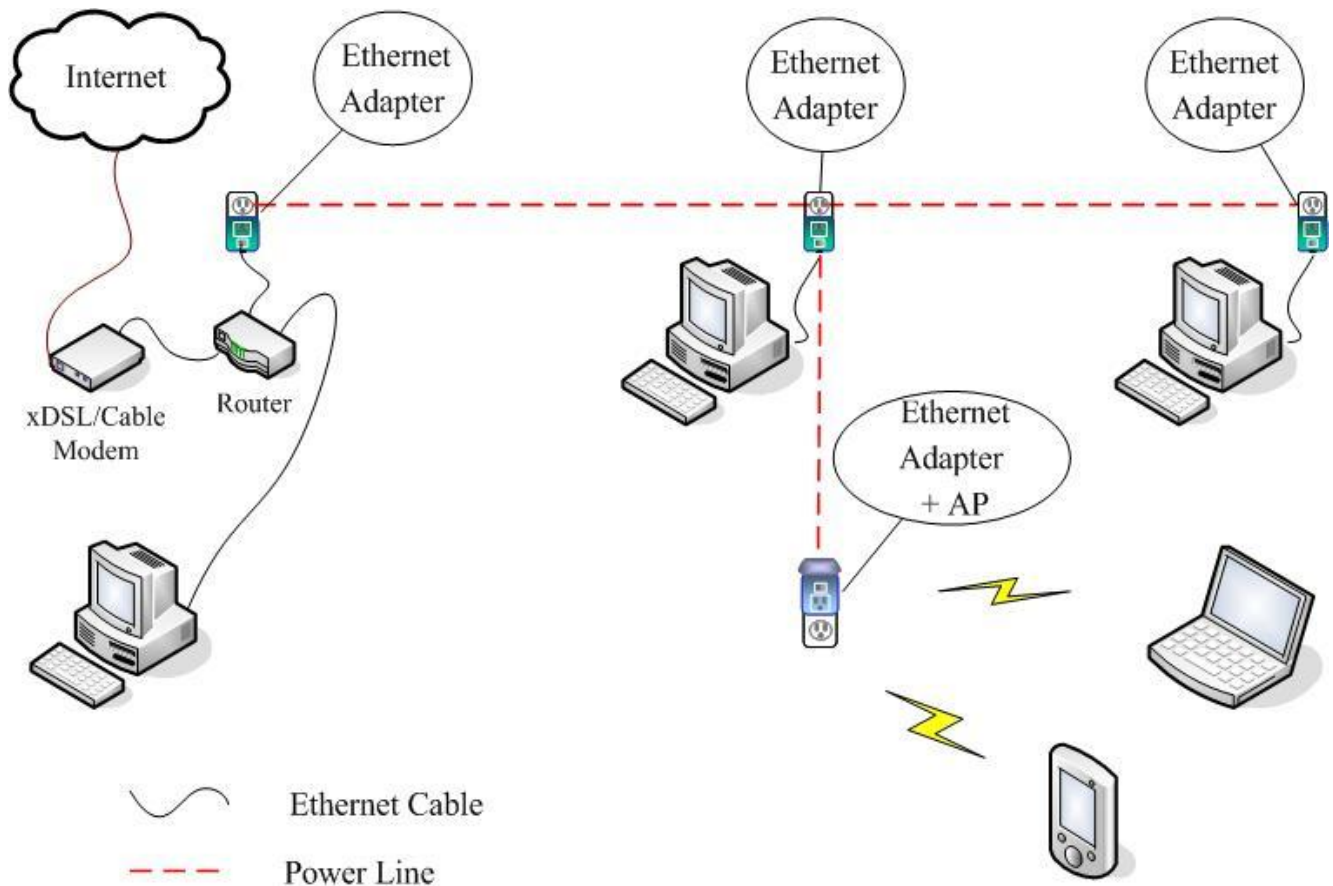


Figure 1. Powerline Access Point application example

2. System Requirements

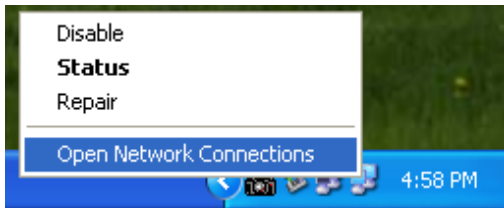
An IBM PC compatible, with :

- Processor: Pentium or higher, clock rate 2.6GHz or above recommended
- Operating System : Windows XP/Vista/7
- Memory: 128 MB or more
- Browser: Microsoft Internet Explorer 6.0 or higher version, or Firefox 1.0 .

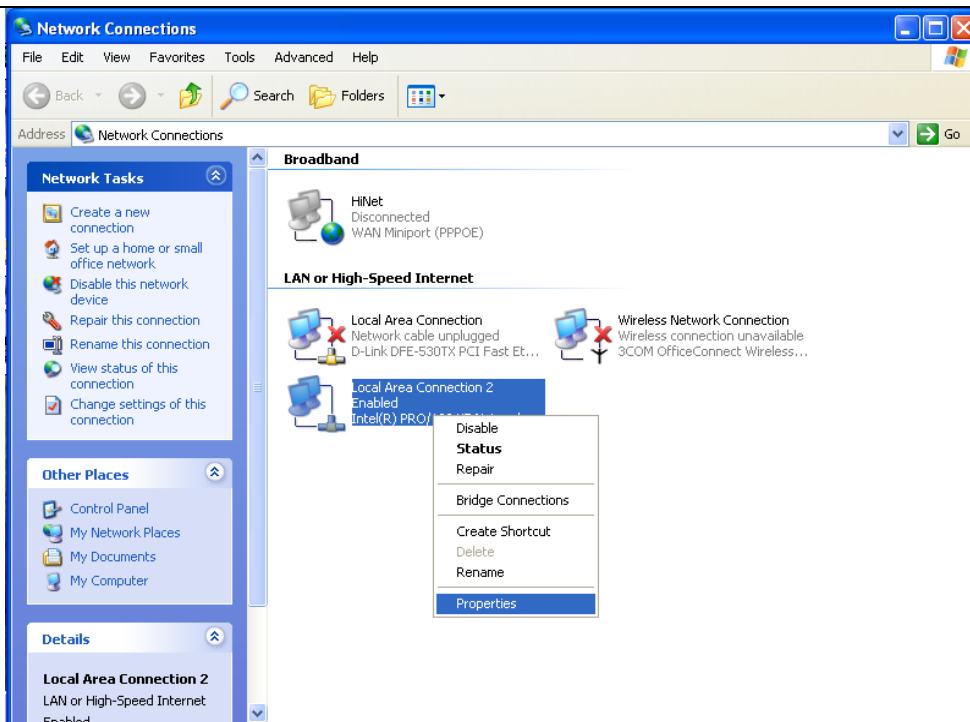
3. Configuration

In first time, please connect the AP with a PC via Ethernet port or PLC bridge. Then set your PC's IP to 192.168.1.10 or other in the same subnet 192.168.1.x except "192.168.1.2" .

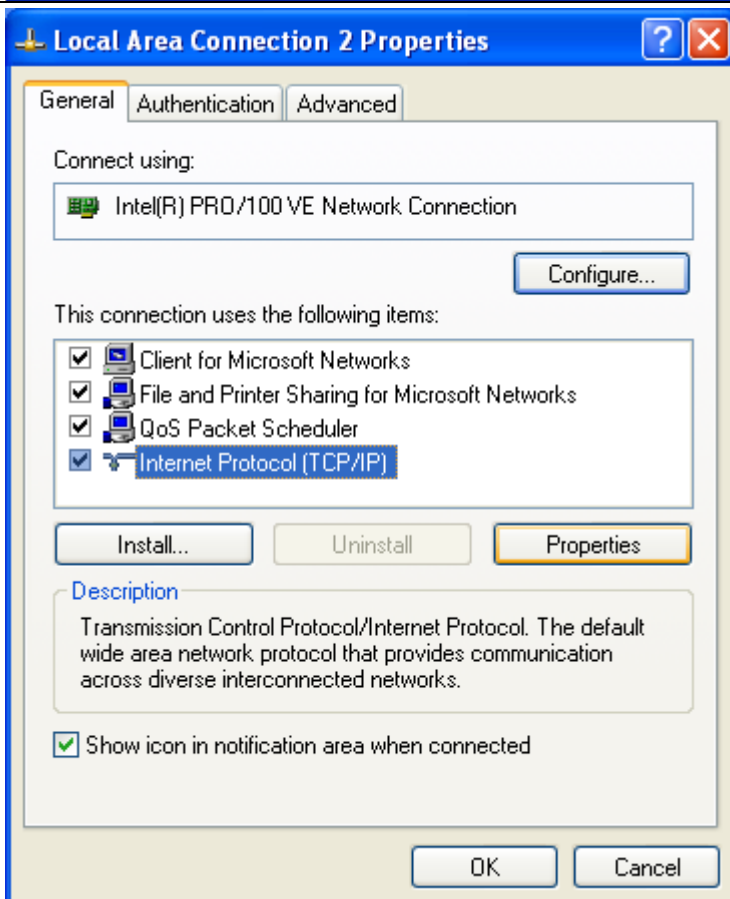
Below is an example for Windows XP:



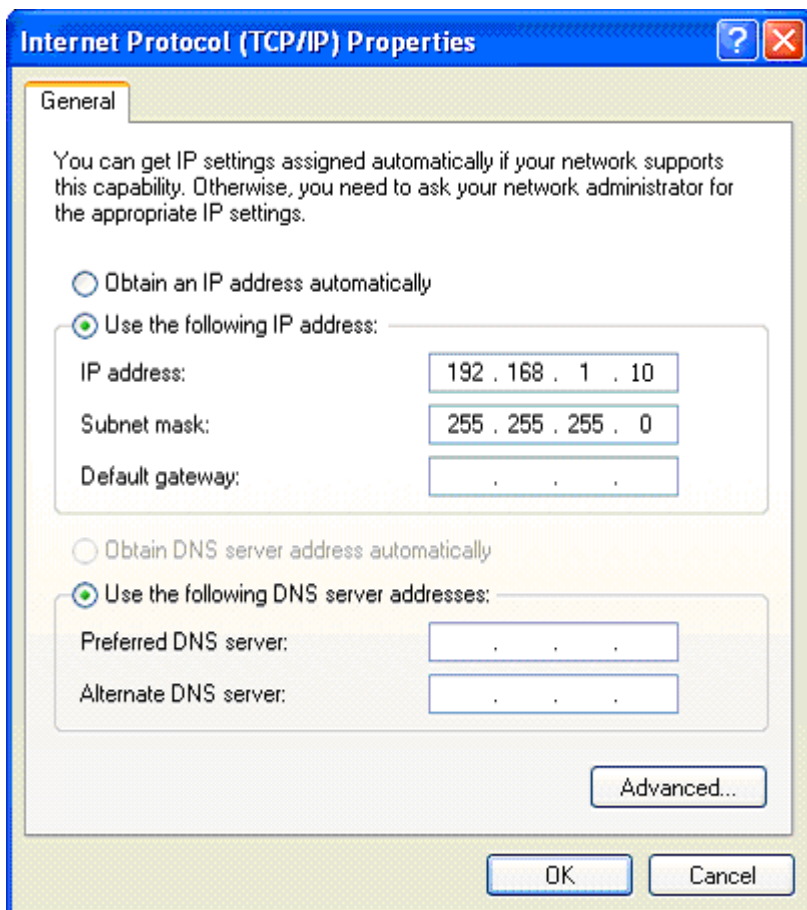
Right click on the Network icon, choose "Open Network Connections".



Right click on the "Local Area Connection" icon, choose "Properties".

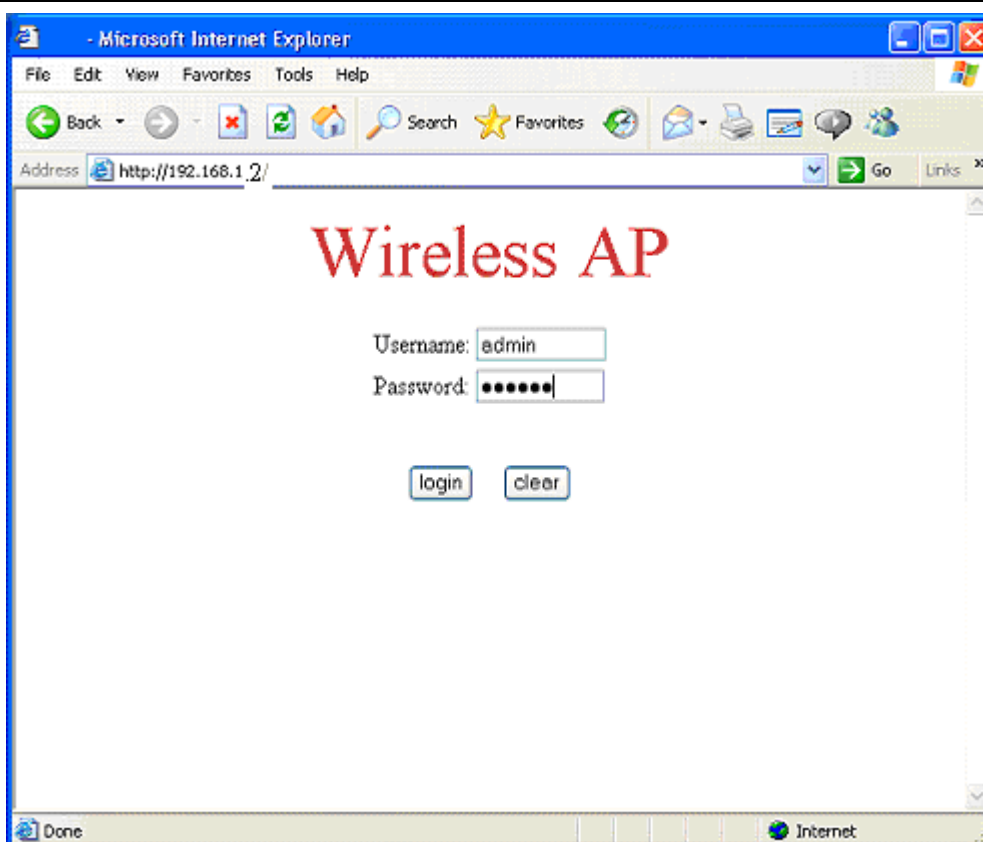


Click on the "Internet Protocol", then click "Properties".



Choose "Use the following IP address".

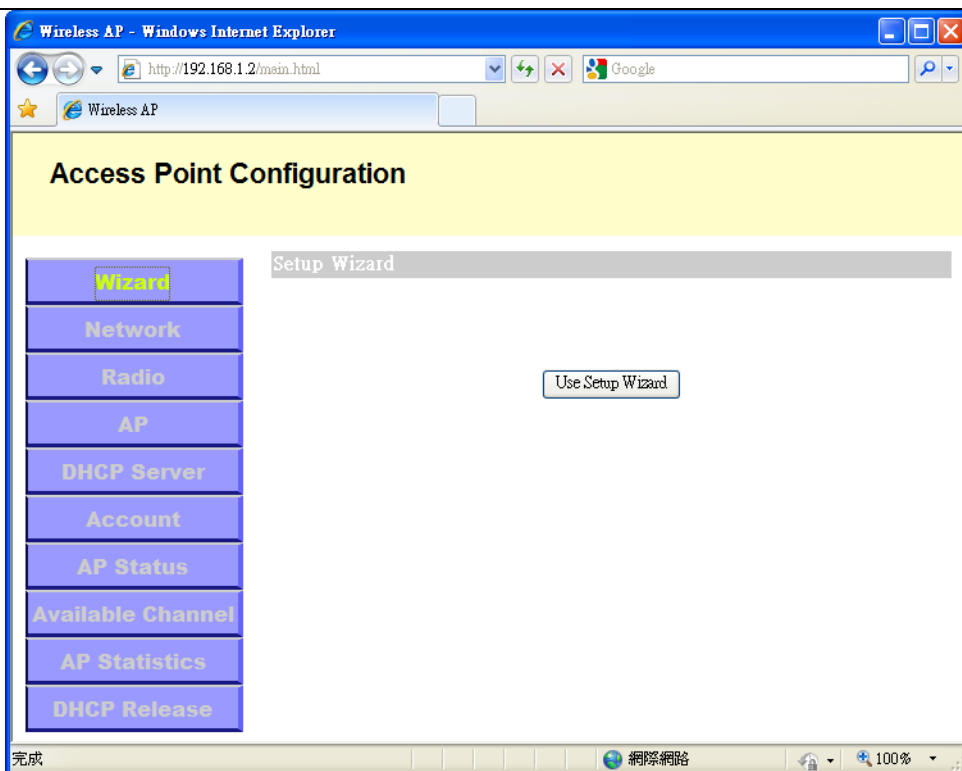
Set your PC's IP to 192.168.1.10 or other in the same subnet 192.168.1.x except "192.168.1.2".



Open the "Microsoft Internet Explorer" window, type "http://192.168.1.2" (default value, if not changed.) in the "Address" column and press Enter. Type "admin" as the Username and "12345" as the Password in the login page. (default value, if not changed.) Then click the "login" button.



If pop up a "AutoComplete" window, you can make the choice by your need.



Then you can see the setup menu.

You can click "Use Setup Wizard" to set the AP easily with security.

Wireless AP - Windows Internet Explorer

http://192.168.1.2/main.html

Google

Wireless AP

Access Point Configuration

Wizard

Network

Radio

AP

DHCP Server

Account

AP Status

Available Channel

AP Statistics

DHCP Release

Setup Wizard

Please assign a name (SSID) for the wireless AP (up to 32 characters)

Name(SSID)

Please input the security password (8 to 63 characters) for access the wireless AP

Password

Done

完成

國際網路

100%

Just assign a new name (SSID) and input the security password (8 to 63 characters, Alphanumeric). Then click “Save” button to save your settings. Then click “Reboot” button to apply your settings. The AP will reboot. Please wait about 20 sec.

Wireless AP - Windows Internet Explorer

http://192.168.1.2/main.html

Google

Wireless AP

Access Point Configuration

Wizard

Network

Radio

AP

DHCP Server

Account

AP Status

Available Channel

AP Statistics

DHCP Release

Save Reboot FactoryReset

Basic AP Configuration

Startup Mode: Standard

Local IP settings

Local IP Addr 192.168.1.2

Local Netmask 255.255.255.0

國際網路

100%

You can click on the “Network” item to set the IP settings.

Wireless AP - Windows Internet Explorer

http://192.168.1.2/main.html

Wireless AP

Access Point Configuration

Save Reboot

Virtual AP/Station Configuration for VAP

ESSID String

VLAN ID VLAN Bridge

VAP Mode ☒ Access Point ☐ Station ☐ WDS Access Point ☐ WDS Station

Root AP Mac Address

Security Settings

☐ Open No Security Applied

☐ WEP Simple WEP Security (64 or 128 bit hardware key)

MODE: ☐ Open ☐ Shared ☐ Auto

Key 1 ☐ Primary Key

Key 2 ☐ Primary Key

Key 3 ☐ Primary Key

Key 4 ☐ Primary Key

☒ WPA Enhanced Security for Personal/Enterprise

MODE: ☐ 802.1x ☐ WPA ☐ WPA 2 ☒ Auto

CYPHER: ☐ TKIP ☐ CCMP ☒ Auto

WPA Rekey Int: WPA Master Rekey:

WEP Rekey Int: (802.1x mode Only)

☒ Personal Shared Key

PSK KEY

v0.15

完成 網際網路 100%

You can click on the “AP” item to set the wireless AP settings.

Detailed settings are described at next sections.

Wireless AP - Windows Internet Explorer

http://192.168.1.2/main.html

Wireless AP

Access Point Configuration

Save Reboot

AP Radio Configuration

Channel: 2.4 GHz Auto select

Mode: WiFi 11gn HT20

Gating Index: ☒ Half ☐ Full

Aggregation: ☒ Enabled ☐ Disabled

Agg Frames: 32

Agg Size: 50000

Agg Min Size: 32768

Channel Width: ☐ HT20 ☒ HT20/40

TX ChainMask: ☐ 1 Chain ☒ 2 Chain ☐ 3 Chain ☐ EEPROM

RX ChainMask: ☐ 1 Chain ☒ 2 Chain ☐ 3 Chain ☐ EEPROM

Video Features: ☐ Enable ☐ Disable

完成

You can click on the “Radio” item to set the radio settings.

Wireless AP - Windows Internet Explorer

http://192.168.1.2/main.html

Wireless AP

Access Point Configuration

Save FactoryReset

DHCP Server Setup

DHCP Server settings

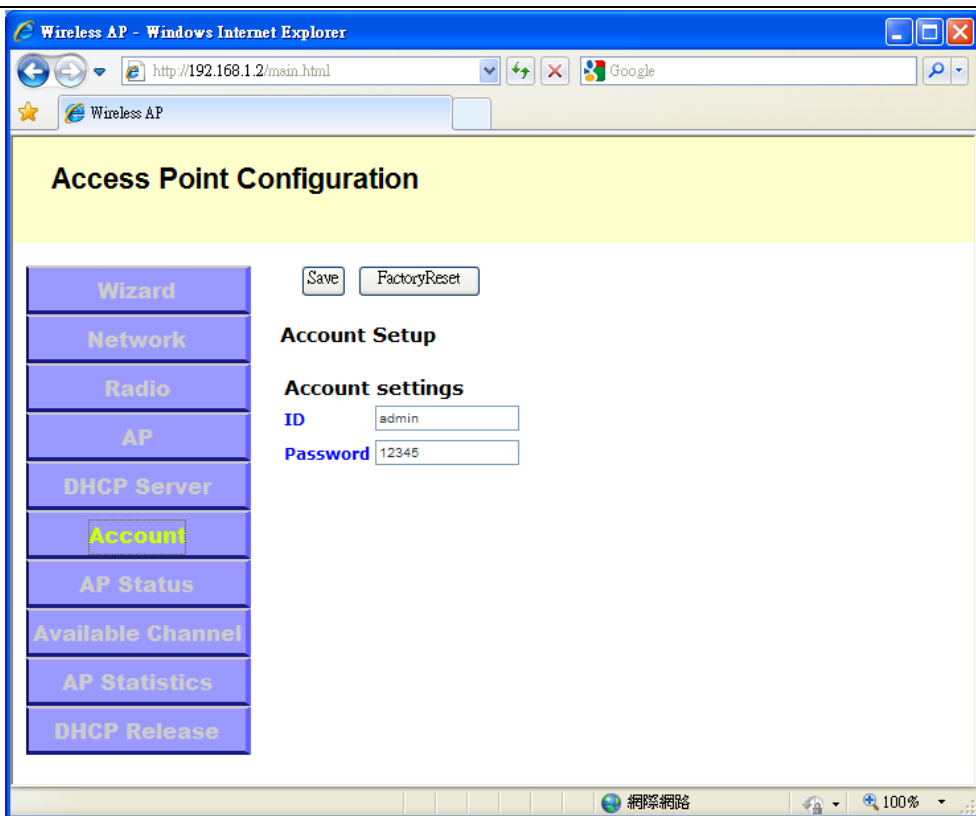
DHCP Server: ☒ Enabled ☐ Disabled

IP address Start: 192.168.1.20

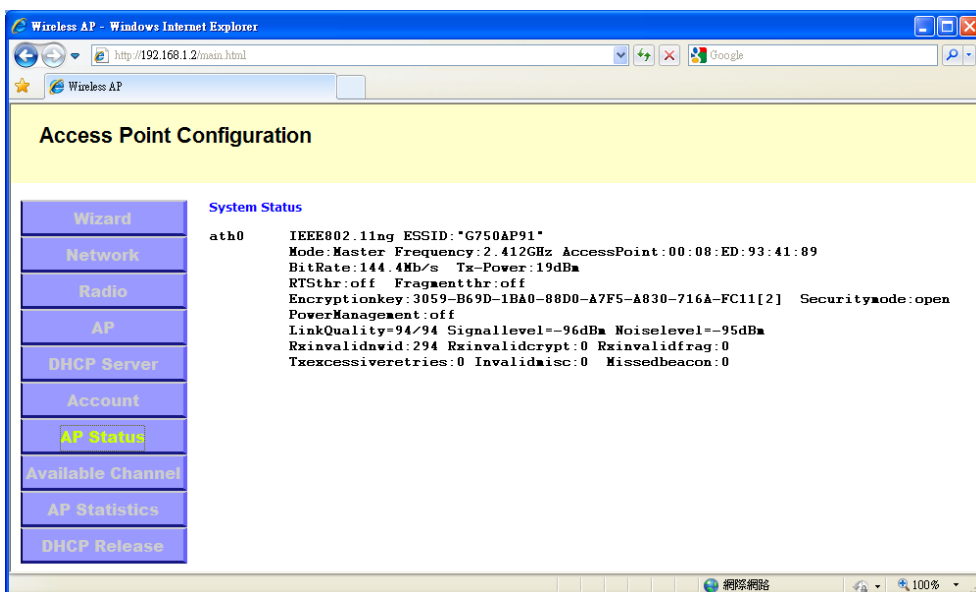
IP address End: 192.168.1.253

完成

You can click on the “DHCP Server” item to set the DHCP Server settings.



You can click on the “Account” item to set the login account and password.



You can click on the “AP Status” item to see the information of this device.

4. WPS

If your wireless device supports WPS (Wi-Fi Protected Setup) function, please click WPS button on wireless device, then press WPS button on this wireless AP device for less than 2 seconds.

5. Wireless AP Settings

At “Radio” page:

Normally, no change is needed.

Wireless AP - Windows Internet Explorer

http://192.168.1.2/main.html

Google

Wireless AP

Access Point Configuration

Wizard Network **Radio** AP DHCP Server Account AP Status Available Channel AP Statistics DHCP Release

Save Reboot

AP Radio Configuration

Channel: 2.4 GHz Auto select

Mode: WiFi 11gn HT20

Gating Index: ☒ Half ☐ Full

Aggregation: ☒ Enabled ☐ Disabled

Agg Frames: 32

Agg Size: 50000

Agg Min Size: 32768

Channel Width: ☐ HT20 ☒ HT20/40

TX ChainMask: ☐ 1 Chain ☒ 2 Chain ☐ 3 Chain ☐ EEPROM

RX ChainMask: ☐ 1 Chain ☒ 2 Chain ☐ 3 Chain ☐ EEPROM

Video Features: ☐ Enable ☒ Disable

完成 網際網路 100%

Channel

Please choose the channel for best performance. Normally, no change is needed.

Channels 1-11 approved for use in the United States, Canada, Latin America, and Taiwan.

Channels 1-14 approved for use in Japan.

Channels 1-13 approved for use in other countries.

Wireless Mode

There are four choice: “**WiFi 11g**”, “**WiFi 11gn HT20**” , “**WiFi 11gn HT40+**”, “**WiFi 11gn HT40-**”. The default value is “**WiFi 11gn HT20**”. Normally, no change is needed.

At “AP” page:

ESSID

ESSID is the network name of the Access Point in the wireless network. You should set the same ESSID name for all your wireless-equipped devices to allow dynamic clients to easily roam among them. The ESSID name can be up to 32 characters in length and is case sensitive.

Security Settings (Authentication Mode/ Encryption Mode)

There are four basic security types you can set up:

Open: Allows any device to connect to the network, assuming the device's ESSID matches the access point's ESSID.

WEP: Only those devices that have the same key can join the network. To limit communication to only those devices which share the same WEP settings.

Key Length:

64-bits - enter 5 ASCII characters or 10 hexadecimal digits.

128-bits - enter 13 ASCII characters or 26 hexadecimal digits.

Key Format:

Choose **HEX** or **ASCII** is up to your choice.

Hexadecimal digits consist of the numbers "0-9" and the letters "A~F".

ASCII characters consist of the letters uppercase "A~Z", lowercase "a~z", or numbers "0~9".

For example, please select MODE: "Shared", type "12345" in "Key 1" field, then click "Primary Key" after "Key 1" field. Then click "Save" button.

WPAPSK: To secure your network using a password and dynamic key changes with TKIP or AES algorithm. (No RADIUS server required). Enter a WPA Personal Shared Key, at least 8 characters, up to 63 ASCII characters.

Wireless AP - Windows Internet Explorer

http://192.168.1.2/main.html

Google

Wireless AP

Access Point Configuration

Security Settings

☐ **Open** No Security Applied

☐ **WEP** Simple WEP Security (64 or 128 bit hardware key)

MODE: ☐ Open ☐ Shared ☐ Auto

Key 1 ☐ Primary Key

Key 2 ☐ Primary Key

Key 3 ☐ Primary Key

Key 4 ☐ Primary Key

☒ **WPA** Enhanced Security for Personal/Enterprise

MODE: ☐ 802.1x ☒ WPA ☐ WPA 2 ☐ Auto

CYPHER: ☒ TKIP ☐ CCMP ☐ Auto

WPA Rekey Int: WPA Master Rekey:

WEP Rekey Int: (802.1x mode Only)

☒ **Personal Shared Key**

PSK KEY

完成 網際網路 100%

For example, please select MODE: WPA", CYPHER: "TKIP", then select "Personal Shared Key", type "12345678" in "PSK KEY" field. Then click "Save" button.

WPA (Wi-Fi Protected Access)/WPA2: To secure your network via RADIUS server, input RADIUS server's information.

Auth Server: IP of Radius server.

Port: port number of Radius server.

Shared Secret: Enter a RADIUS Key up to 32 ASCII characters.

For example, please select MODE: WPA", CYPHER: "TKIP", then select "Enterprise/RADIUS", type "192.168.1.5" in "Auth Server" field, "1812" in port field, "testing123" in "Shared Secret" field. Then click "Save" button.

6. FAQ

Q1. You set Security Settings with WEP, but you can't connect to AP.

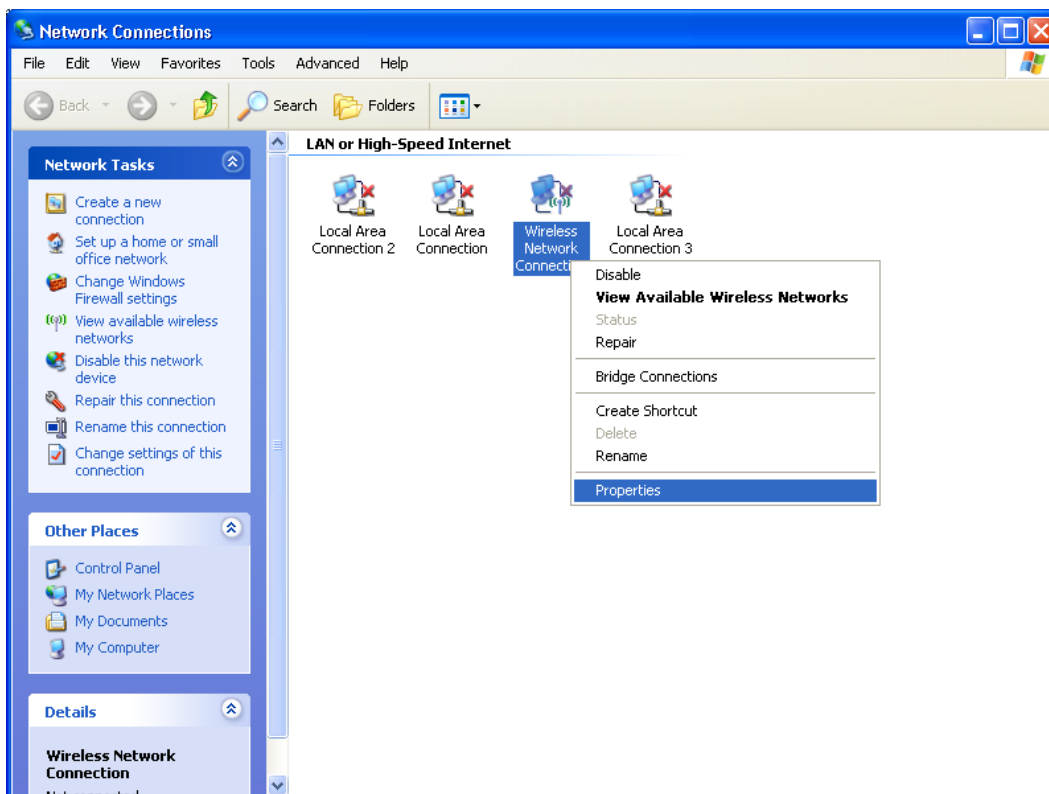
Ans. Please check the properties of "Wireless Network Connection". Below is an example for Windows XP.

Details as follow:

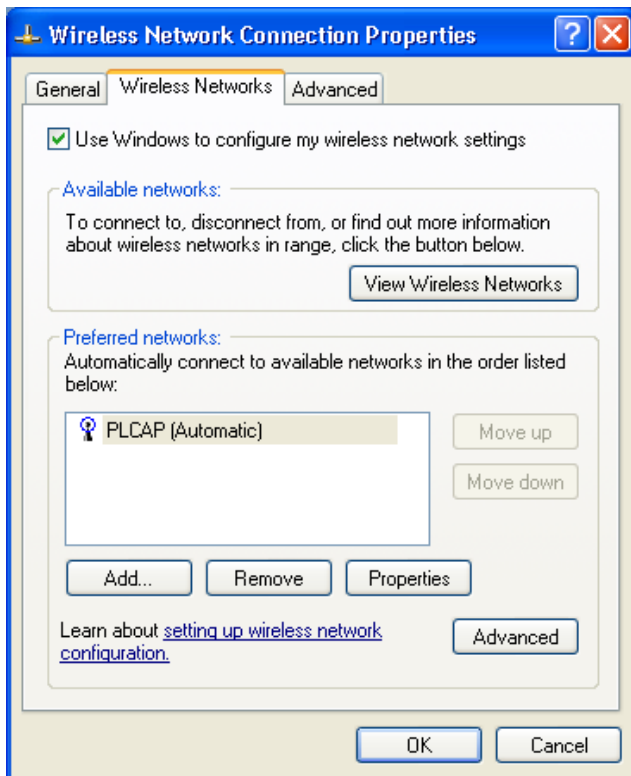
1.1 Right click on the "Network Connection" icon and choose "Open Network Connections".



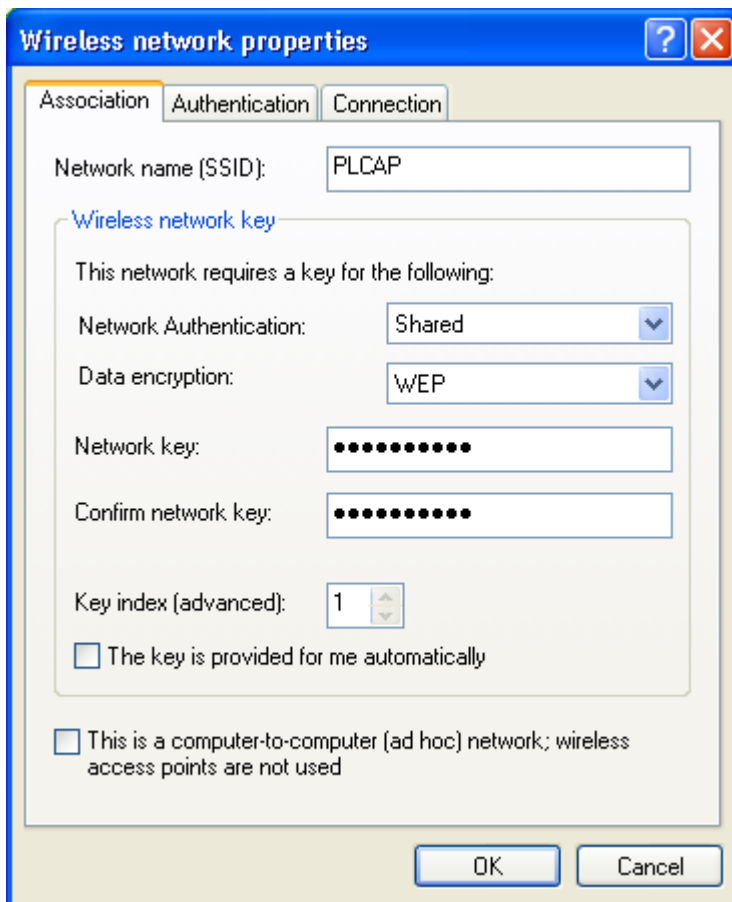
1.2 Right click on the "Wireless Network Connection" and choose "Properties".



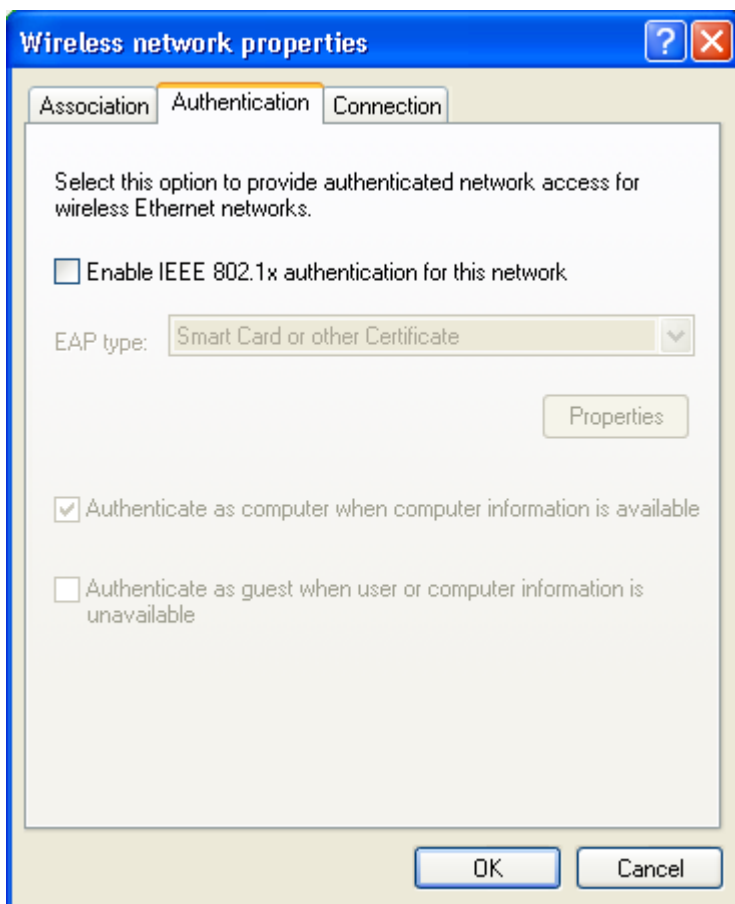
1.3 On the "Wireless Networks" tab, choose the preferred network and click "Properties" button.



1.4 Make sure the Network Authentication is “Shared” and the Data encryption is “WEP”.



1.5 Don’t select the “Enable IEEE 802.1x authentication for this network”.

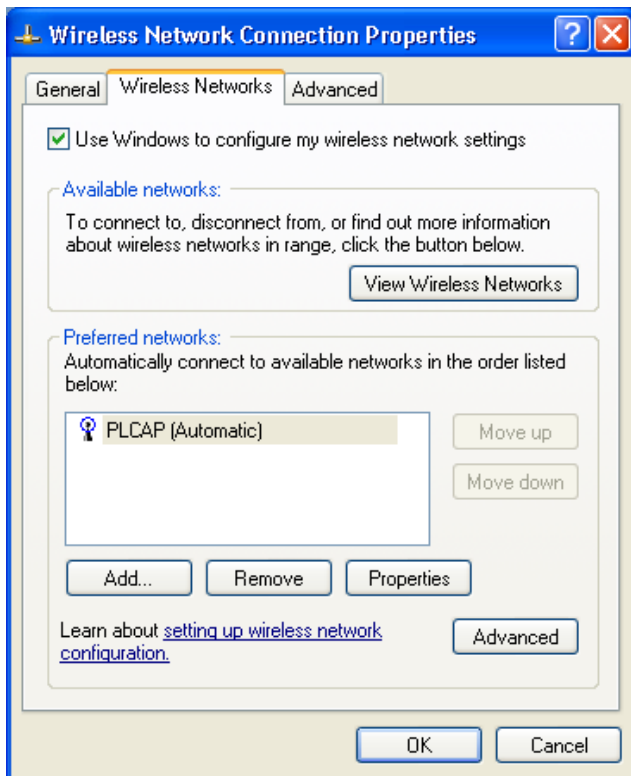


Q3. How to use WPA with RADIUS?

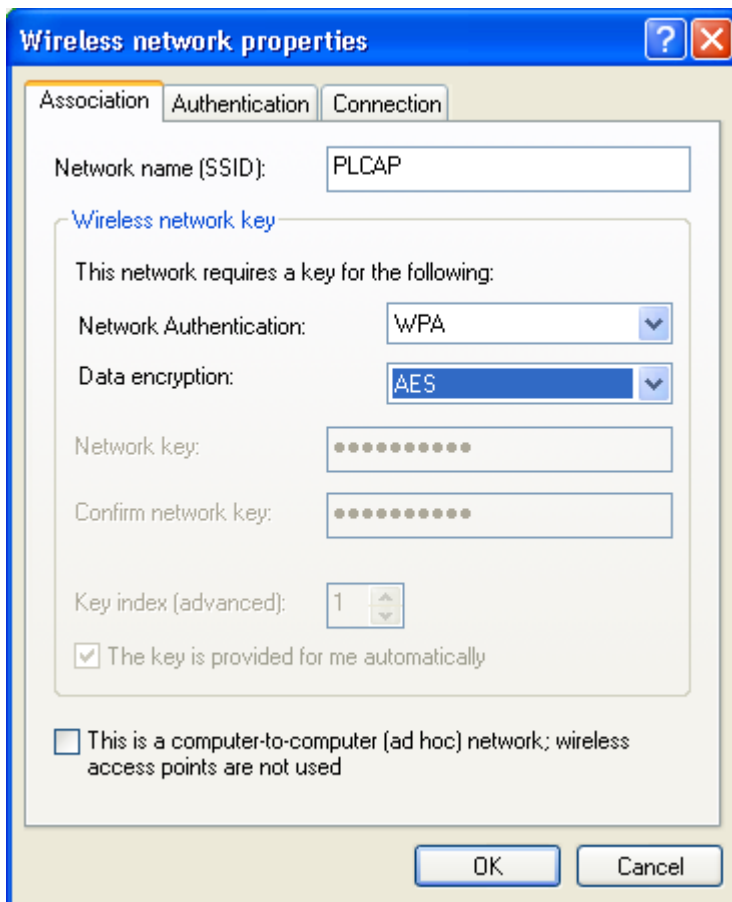
Ans. You can download the win32 distribution of FreeRADIUS (FreeRADIUS.net) from <http://www.freeradius.net/>.

Below are some configurations for Windows XP client connected to the RADIUS with Files authentication mode.

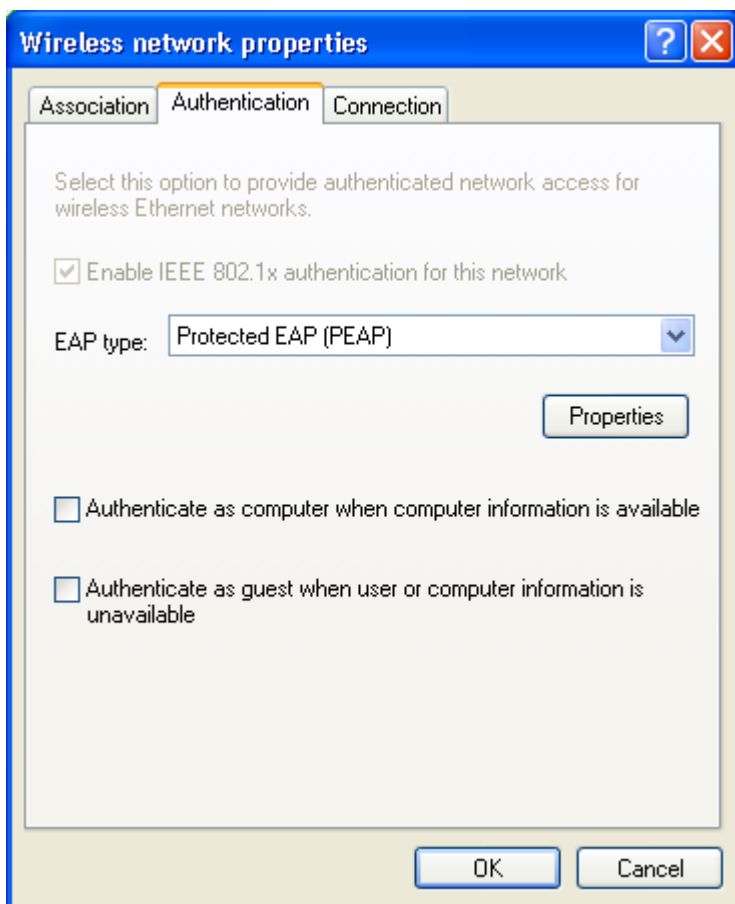
3.1 On the "Wireless Networks" tab, choose the preferred network and click "Properties" button.



3.2 Make sure the Network Authentication is “WPA” and the Data encryption is “AES” or “TKIP”.

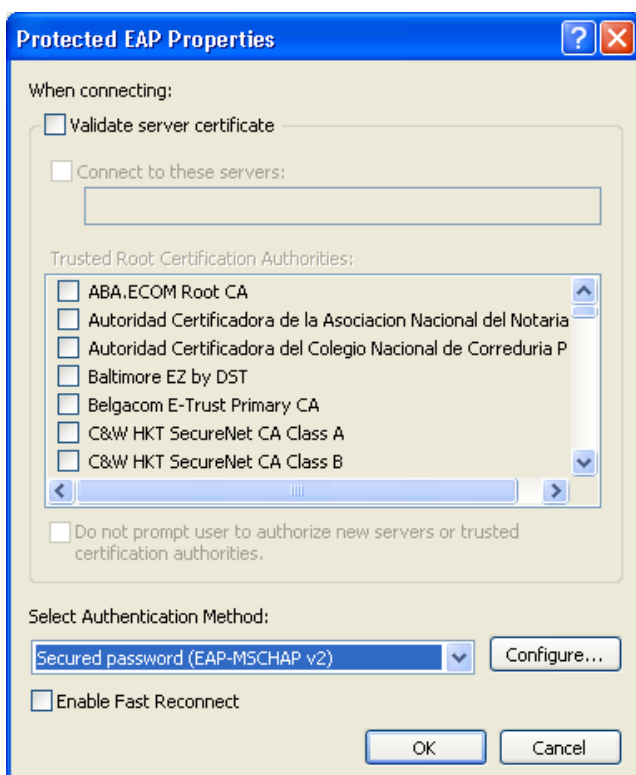


3.3 On the “Authentication” tab, select “Protected EAP (PEAP)” on the drop-down list, then click “Properties”.

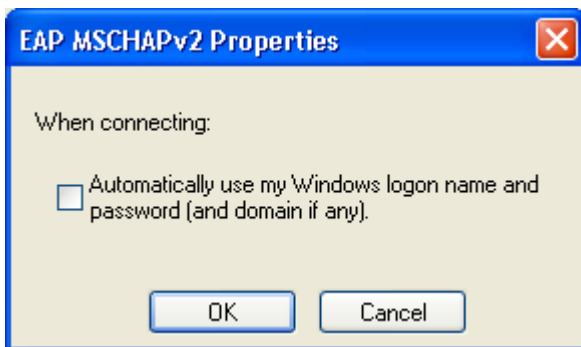


3.4 Disable "Validate server certificate".

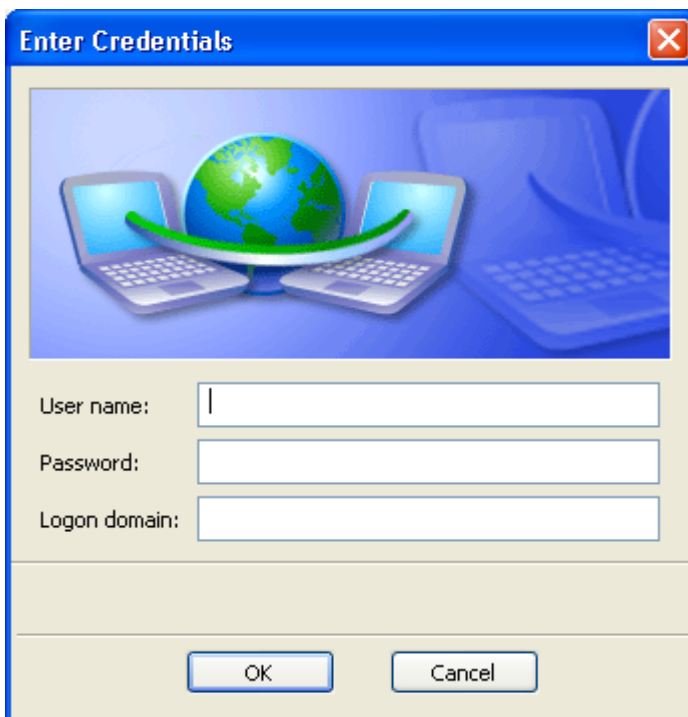
In Select Authentication Method, select "Secured password (EAP-MSCHAPv2)", then click "Configure..." button.



3.5 Disable "Automatically use my Windows logon name and password".



3.6 Then you can key in your "User name" and "Password" in the "Enter Credentials" dialog.



7. Glossary

AES

AES stands for **A**dvanced **E**ncryption **S**tandard. It is a preferred standard for the encryption of commercial and government data using a symmetric block data encryption technique.

TKIP

TKIP stands for **T**emporal **K**ey Integrity **P**rotocol. It is a wireless security encryption mechanism in Wi-Fi Protected Access. TKIP uses a key hierarchy and key management methodology that removes the predictability that intruder relied upon to exploit the WEP key. It increases the size of the key from 40 to 128 bits and replaces WEP's single static key with keys that are dynamically generated and distributed by an authentication server, providing some 500 trillion possible keys that can be used on a given data packet. It also includes a Message Integrity Check (MIC), designed to prevent an attacker from capturing data packets, altering them and resending them. By greatly expanding the size of keys, the number of keys in use, and by creating an integrity checking mechanism, TKIP magnifies the complexity and difficulty involved in decoding data on a Wi-Fi network. TKIP greatly increases the strength and complexity of wireless encryption, making it far more difficult—if not impossible—for a would-be intruder to break into a Wi-Fi network.

WEP

WEP stands for **W**ired **E**quivalent **P**rivacy. It is a data privacy mechanism based on a 64/128-bit shared key algorithm, defined in the IEEE 802.11 standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

WPA

WPA stands for **W**i-Fi **P**rotected **A**ccess. It is a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology includes two improvements over WEP:

- Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

It should be noted that WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion.

WPA2

WPA2 stands for **Wi-Fi Protected Access 2**, the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication. *[Adapted from Wi-Fi.org]* There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

RADIUS

RADIUS stands for **Remote Access Dial-Up User Service**. It is a standard technology used by many major corporations to protect access to wireless networks. RADIUS is a user name and password scheme that enables only approved users to access the network; it does not affect or encrypt data. The first time a user access to the network, he must input name and password and submit it over the network to the RADIUS server. The server then verifies that the individual has an account and, if so, ensures that the person uses the correct password before he can get on the network.

WMM

WMM stands for **Wi-Fi Multimedia**. It is a standard created to define quality of service (QoS) in Wi-Fi networks. It is a precursor to the upcoming IEEE 802.11e WLAN QoS draft standard, which is meant to improve audio, video and voice applications transmitted over Wi-Fi. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources.



CE-Declaration of Conformity

For the following equipment:

Germering, 1st of March, 2013

500Mbps Powerline WLAN N Access Point

ALL1682511



The safety advice in the documentation accompanying the products shall be obeyed.

The conformity to the above directive is indicated by the CE sign on the device.

The Allnet ALL1682511 conforms to the Council Directives of 2004/108/EC.

This equipment meets the following conformance standards:

EN 55022:2010

CISPR11/257/CD:2008

EN 61000-3-2:2006+A2:2009

EN 61000-3-3:2008

EN 50412-2-1: 2005

IEC 61000-4-2:2008

IEC 61000-4-3:2010

IEC 61000-4-4:2012

IEC 61000-4-5:2005

IEC 61000-4-6:2008

IEC 61000-4-8:2009

IEC 61000-4-11:2004

This equipment is intended to be operated in all countries.

This declaration is made by

ALLNET Computersysteme GmbH

Maistraße 2

82110 Germering

Germany

Germering, 01.03.2013



Wolfgang Marcus Bauer
CEO