

# QP-W0259GHP



**Outdoor High-Power 54Mbps  
Wireless Access Point**

---



---

# Table of Contents

<b>Chapter I</b>	<b>System Requirements</b>	<b>4</b>
<b>Chapter II</b>	<b>Installation</b>	<b>4</b>
	1. Hardware Installation.....	4
	1.1 Appearance and Interface Introduction .....	4
	1.2 Hardware installation steps .....	8
	2. Software Installation .....	14
	3. Resetting the AP to Factory Default Settings.....	14
<b>Chapter III</b>	<b>Software configuration</b>	<b>14</b>
	1. Connect to the WLAN Access Point.....	15
	2. Prepare your PC to configure the WLAN Access Point.....	15
<b>Chapter IV</b>	<b>Management and configuration</b>	<b>16</b>
	1. Status.....	17
	2. Setup Wizard.....	18
	3. Wireless - Basic Settings.....	19
	4. Wireless - Advanced Settings .....	21
	5. Wireless - Security Setup .....	22
	6. WEP Key Setup.....	24
	7. Wireless - Access Control.....	25
	8. WDS Settings.....	27
	8.1 WDS Security Setup .....	28
	8.1. WDS AP Table .....	29
	9. Site Survey .....	30
	10. TCP/IP Settings .....	30
	11. Log.....	32
	12. Statistics.....	33
	13. Upgrade Firmware.....	33
	14. Save / Reload Settings.....	34
	15. Password Setup .....	35
	16. Logout .....	36
<b>Chapter V</b>	<b>Troubleshooting</b>	<b>37</b>
<b>Chapter VI</b>	<b>Frequently Asked Questions (FAQ)</b>	<b>43</b>
	1. What and how to find my PC's IP and MAC address?.....	43

---

2. What is Wireless LAN?.....	44
3. What are ISM bands?.....	44
4. How does wireless networking work? .....	44
5. What is BSSID? .....	45
6. What is ESSID? .....	45
7. What are potential factors that may causes interference? .....	45
8. What are the Open System and Shared Key authentications? .....	45
9. What is WEP?.....	45
10. What is Fragment Threshold?.....	46
11. What is RTS (Request To Send) Threshold? .....	46
12. What is Beacon Interval?.....	46
13. What is Preamble Type? .....	47
14. What is SSID Broadcast? .....	47
15. What is Wi-Fi Protected Access (WPA)? .....	47
16. What is WPA2?.....	47
17. What is 802.1x Authentication?.....	48
18. What is Temporal Key Integrity Protocol (TKIP)?.....	48
19. What is Advanced Encryption Standard (AES)?.....	48
20. What is Inter-Access Point Protocol (IAPP)? .....	48
21. What is Wireless Distribution System (WDS)?.....	48
22. What is Clone MAC Address?.....	48

---

# 1 System Requirements

- Computer with Windows, Macintosh, or Linux-based operating system with an installed Ethernet adapter.
- Internet Explorer or Netscape Navigator version 6.0 or above, with JavaScript enabled.

## 2 Installation

### 2.1 Hardware Installation

#### 2.1.1 Appearance and Interface Introduction

Notes: The product shot is for reference only please refer to physical product.

**1** LED Panel    **2** Waterproof Sliding Door



**3** Pass through Ethernet cable from this cable **4** Push these button to remove upper housing

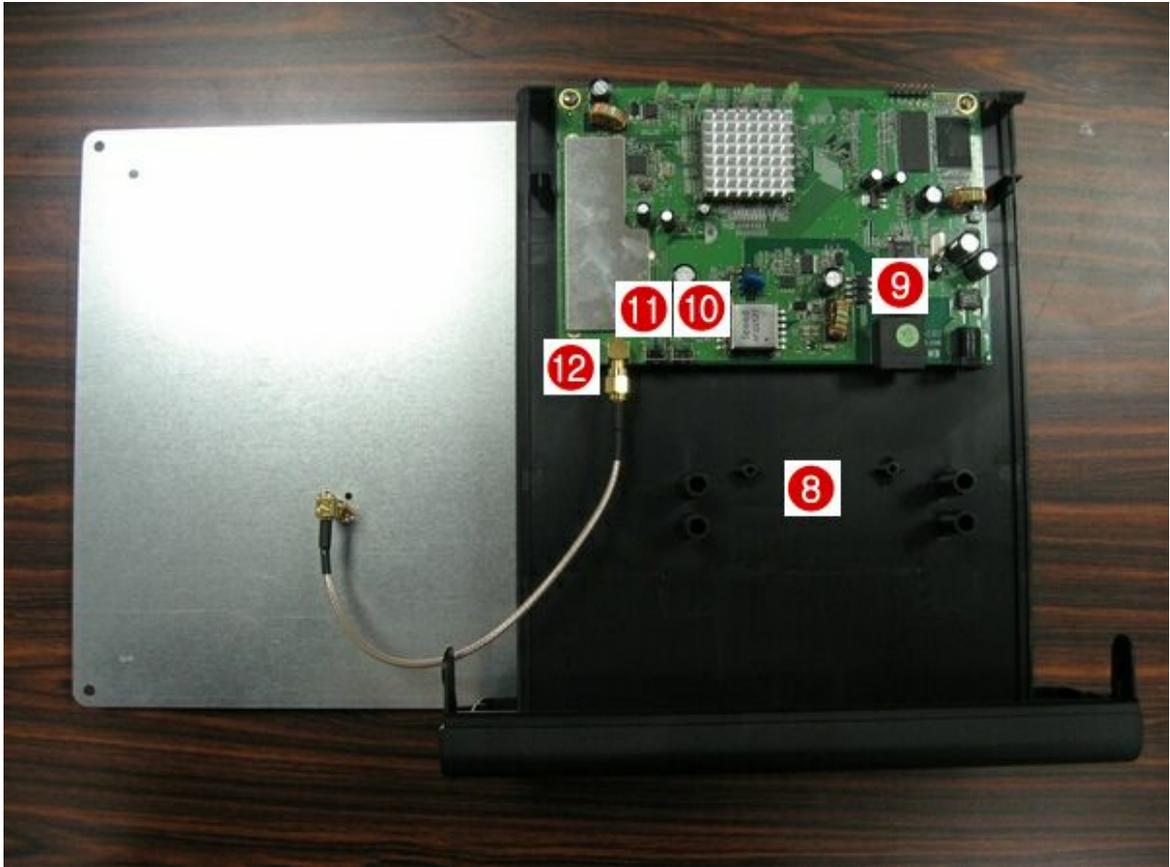


**5** Wall Mount **6** Pole Mount



- 7 Intergrated 14 dbi dual polarity antenna
- 8 Pillars to fasten cables, to avoid PCB is broken by pulling and draging cables
- 9 Lan port wih POE

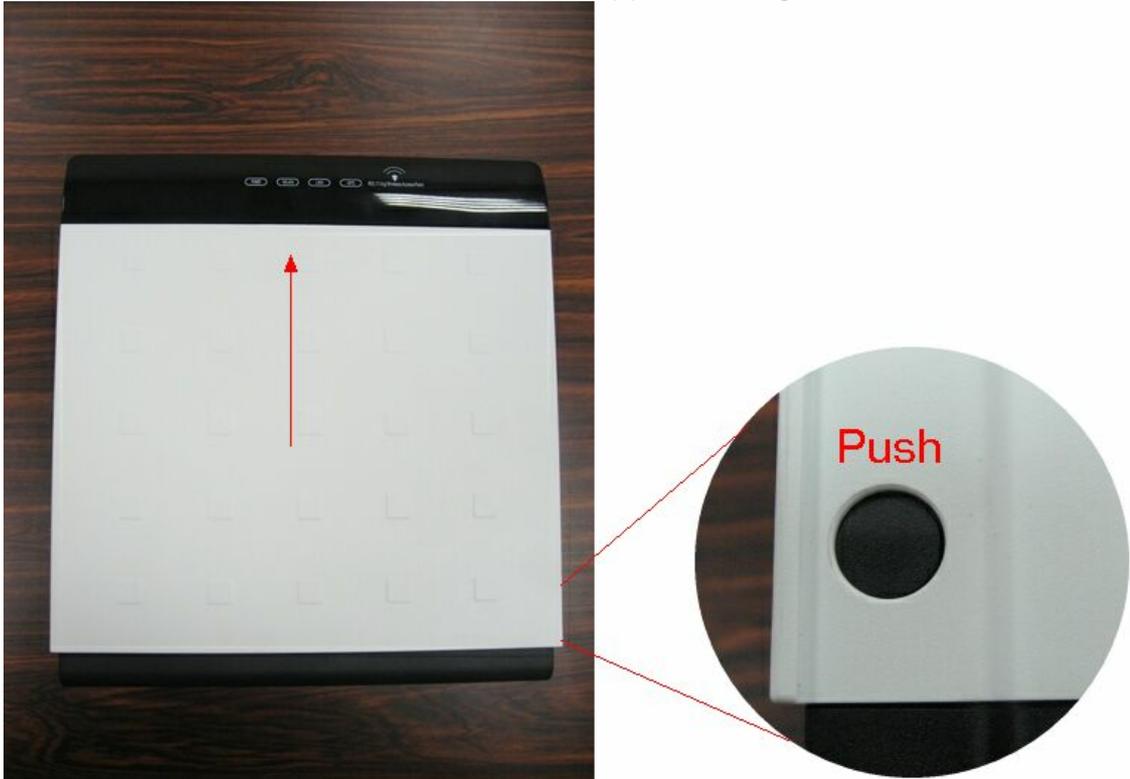
- ⑩ WPS Button
- ⑪ Reset Button
- ⑫ SMA antenna connector



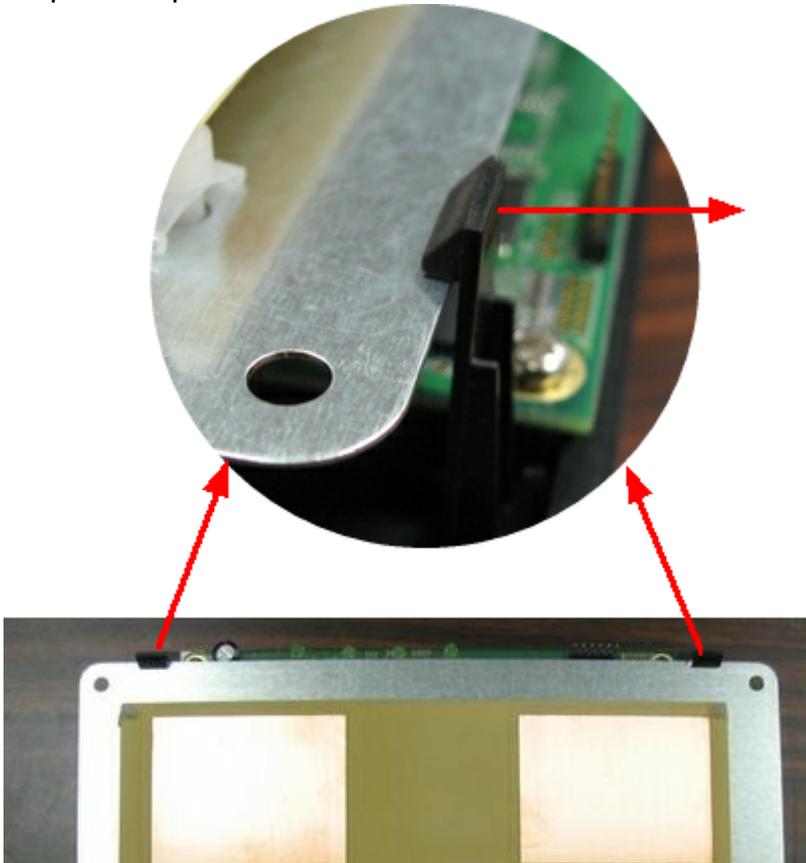
---

## 2.1.2 Hardware installation steps

Step1: push buttons in the sides to remove upper housing.

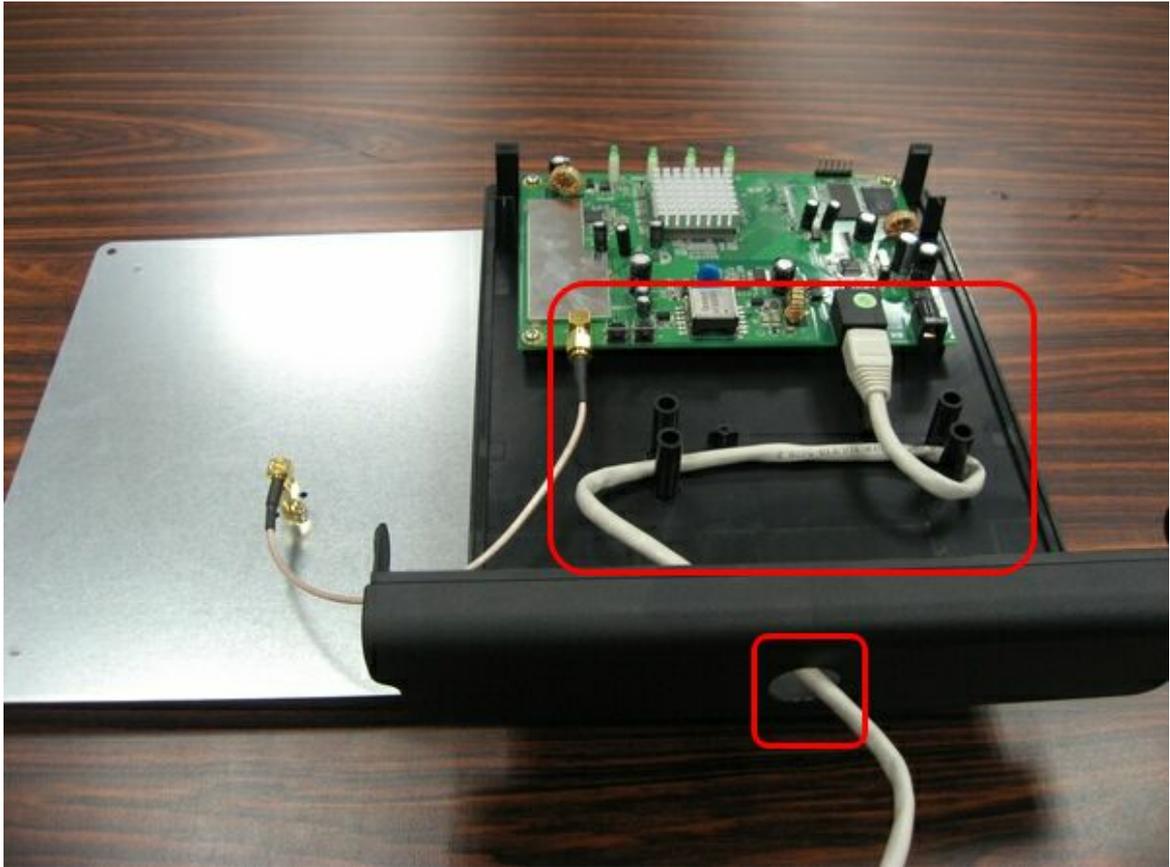


Step2: Pull open the click and dismantle the antenna board

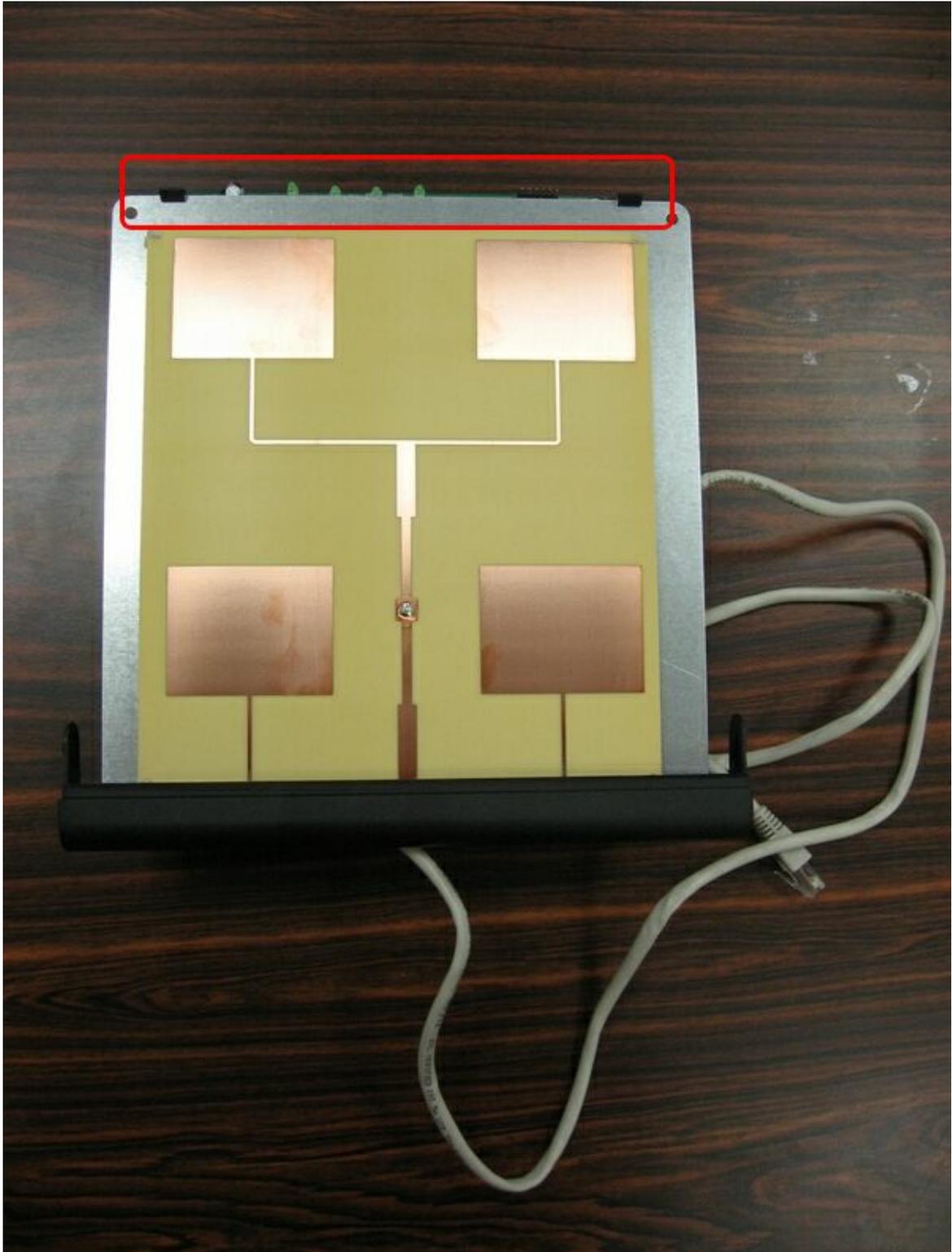


Step3: Pass through Ethernet cable from the hole, insert the cable to LAN port.

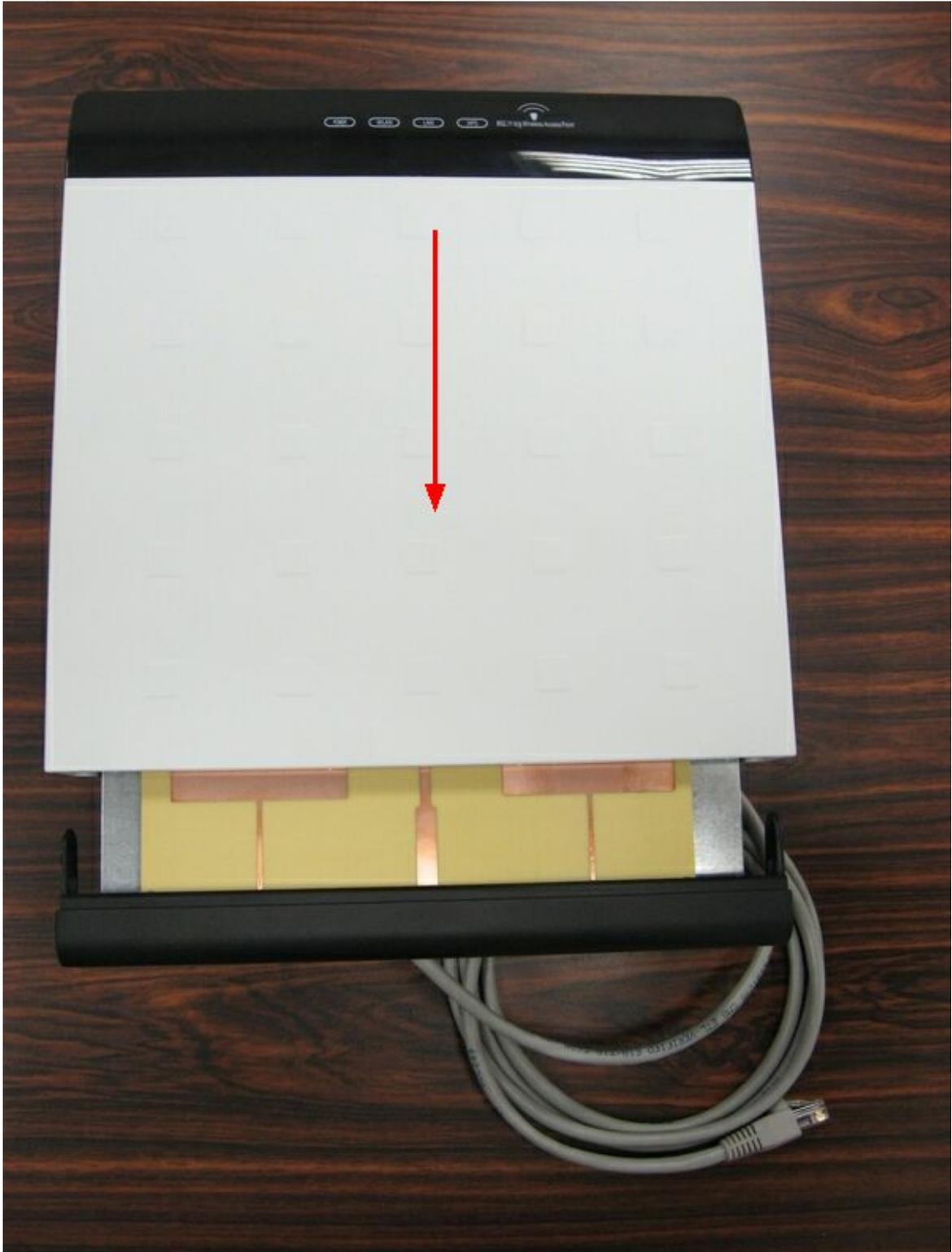
**Notes: RJ-45 8P8C Ethernet cable is required**



Step4: Install the antenna.  
Make sure the Antenna is well installed.



Step5:Install the upper housing  
Make sure the housing is well installed.



Step6:Fasten cables by the black ring.  
Move and fasten cables to the hole with that black ring.



Step7:Install POE Injector  
DC:Insert adapter

POE:this hole is linked to Outdoor AP with RJ-45

LAN:this hole is linked to Hub/router/ADSL modem devies with RJ-45



Step7:Complete diagram



---

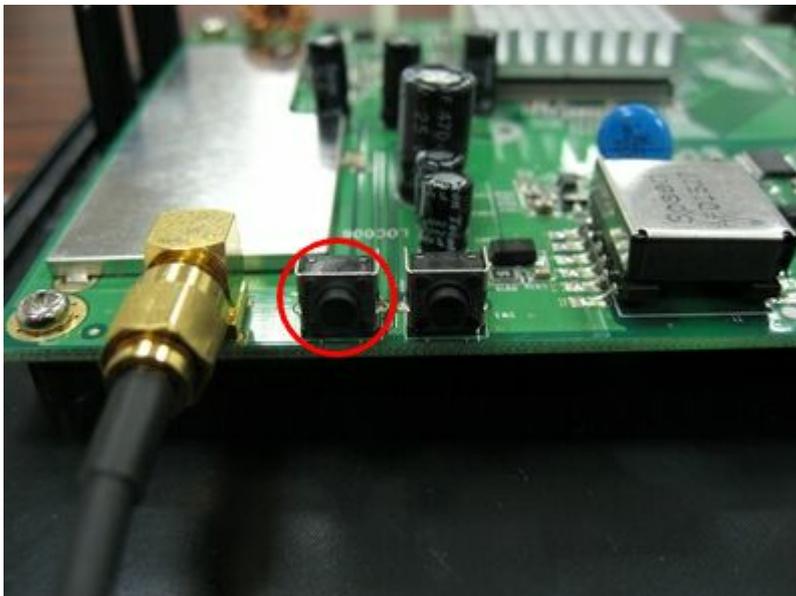
## 2.2 Software Installation

There are no software drivers, patches or utilities installation needed, but only the configuration setting.

**Notice:** It will take about 55 seconds to complete the boot up sequence after powered on the WLAN Access Point; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.

## 2.3 Resetting the AP to Factory Default Settings

After you have tried other methods for troubleshooting your network, you may choose to Reset the Access Point to the factory default settings.



To hard-reset the Access Point to Factory Default Settings, please do the following:

**Notes:** Access Point status: Power on

- Locate the Reset button on the back of the Access Point PCB
- Press the Reset button
- Hold for about 5 seconds and then release
- After the Access Point reboots (this may take a few minutes) it will be reset to the factory default settings.

## 3 Software configuration

There are web based management and configuration functions allowing you to have the jobs done easily.

The WLAN Access Point is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: **192.168.1.254**  
Default IP subnet mask: **255.255.255.0**  
WEB login User Name: **<empty>**  
WEB login Password: **<empty>**

### 3.1 Connect to the WLAN Access Point

**This product can be set up using any current web browser, i.e., Internet Explorer 6 or Netscape Navigator 6.2.3.**

Open a WEB browser, i.e. Microsoft Internet Explore, then enter **192.168.1.254** on the URL to connect the WLAN Access Point.



### 3.2 Prepare your PC to configure the WLAN Access Point

#### **For OS of Microsoft Windows 95/ 98/ Me:**

1. Click the Start button and select Settings, then click Control Panel. The Control Panel window will appear.

Note: Windows Me users may not see the Network control panel. If so, select View all Control Panel options on the left side of the window

2. Move mouse and double-click the right button on Network icon. The Network window will appear.

3. Check the installed list of Network Components. If TCP/IP is not installed, click the Add button to install it; otherwise go to step 6.

4. Select Protocol in the Network Component Type dialog box and click Add button.

5. Select TCP/IP in Microsoft of Select Network Protocol dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to Network dialog box after the TCP/IP installation.

6. Select TCP/IP and click the properties button on the Network dialog box.

7. Select Specify an IP address and type in values as following example.

- IP Address: 192.168.1.1, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
- IP Subnet Mask: 255.255.255.0

8. Click OK and reboot your PC after completes the IP parameters setting.

#### **For OS of Microsoft Windows 2000, XP:**

1. Click the Start button and select Settings, then click Control Panel. The Control Panel window will appear.

2. Move mouse and double-click the right button on Network and Dial-up Connections icon. Move mouse and double-click the Local Area Connection icon. The Local Area Connection window will appear. Click Properties button in the Local Area Connection window.

3. Check the installed list of Network Components. If TCP/IP is not installed, click the Add button to install it; otherwise go to step 6.

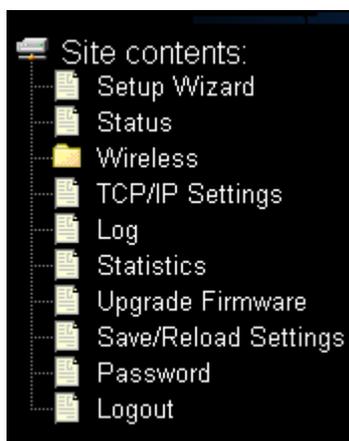
4. Select Protocol in the Network Component Type dialog box and click Add button.

- 
5. Select TCP/IP in Microsoft of Select Network Protocol dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to Network dialog box after the TCP/IP installation.
  6. Select TCP/IP and click the properties button on the Network dialog box.
  7. Select Specify an IP address and type in values as following example.
    - IP Address: 192.168.1.1, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
    - IP Subnet Mask: 255.255.255.0
  8. Click OK to completes the IP parameters setting.

**For OS of Microsoft Windows NT:**

1. Click the Start button and select Settings, then click Control Panel. The Control Panel window will appear.
2. Move mouse and double-click the right button on Network icon. The Network window will appear. Click Protocol tab from the Network window.
3. Check the installed list of Network Protocol window. If TCP/IP is not installed, click the Add button to install it; otherwise go to step 6.
4. Select Protocol in the Network Component Type dialog box and click Add button.
5. Select TCP/IP in Microsoft of Select Network Protocol dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to Network dialog box after the TCP/IP installation.
6. Select TCP/IP and click the properties button on the Network dialog box.
7. Select Specify an IP address and type in values as following example.
  - IP Address: 192.168.1.1, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
  - IP Subnet Mask: 255.255.255.0
8. Click OK to complete the IP parameters setting.

## 4 Management and configuration



## 4.1 Status

This page shows the current status and some basic settings of the device, includes system, wireless, and Ethernet LAN configuration information.

<b>Access Point Status</b>	
This page shows the current status and some basic settings of the device.	
System	
<b>Uptime</b>	0day:0h:9m:18s
<b>Firmware Version</b>	v1.4b
Wireless Configuration	
<b>Mode</b>	AP
<b>Band</b>	2.4 GHz (B+G)
<b>SSID</b>	Access Point
<b>Channel Number</b>	1
<b>Encryption</b>	Disabled
<b>BSSID</b>	00:1a:ef:02:56:8e
<b>Associated Clients</b>	1
TCP/IP Configuration	
<b>Attain IP Protocol</b>	Fixed IP
<b>IP Address</b>	192.168.1.254
<b>Subnet Mask</b>	255.255.255.0
<b>Default Gateway</b>	192.168.1.254
<b>MAC Address</b>	00:1a:ef:02:56:8e

### System

#### [Uptime]

It shows the duration since WLAN Access Point is powered on.

#### [Firmware version]

It shows the firmware version of WLAN Access Point.

### Wireless configuration

#### [Mode]

It shows wireless operation mode

#### [Band]

It shows the current wireless operating frequency.

#### [SSID]

It shows the SSID of this WLAN Access Point.

The SSID is the unique name of WLAN Access Point and shared among its service area, so all devices attempts to join the same wireless network can identify

it.

[Channel Number]

It shows the wireless channel connected currently.

[Encryption]

It shows the status of encryption function.

[Associated Clients]

It shows the number of connected clients (or stations, PCs).

[BSSID]

It shows the BSSID address of the WLAN Access Point. BSSID is a six-byte address.

[Associated Clients]

It shows total numbers of WLAN clients connected,

### TCP/IP Configuration

[Attain IP Protocol]

It shows how the WLAN Access Point gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server.

[IP Address]

It shows the IP address of WAN interface of WLAN Access Point.

[Subnet Mask]

It shows the IP subnet mask of LAN interface of WLAN Access Point.

[Default Gateway]

It shows the default gateway setting for outgoing data packets.

[MAC Address]

It shows the MAC address of WLAN Access Point.

## 4.2 Setup Wizard

This page guides you to configure wireless Access Point for first time. Enter topic text here.

### 1. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

---

**IP Address:**

**Subnet Mask:**

### 1. LAN Interface Setup

This page is used to configure local area network IP address and subnet mask

## 2. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

**Band:**

**Mode:**

**Network Type:**

**SSID:**

**Channel Number:**

**Enable Mac Clone (Single Ethernet Client)**

### 2. Wireless Basic Settings

This page is used to configure basic wireless parameters like Band, Mode, Network Type SSID, Channel Number, Enable Mac Clone(Single Ethernet Client)

## 3. Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

**Encryption:**

### 3. Wireless Security Setup

This page is used to configure wireless security

## 4.3 Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

## Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

**Disable Wireless LAN Interface**

**Band:**

**Mode:**

**Network Type:**

**SSID:**

**Channel Number:**

**Associated Clients:**

**Enable Mac Clone (Single Ethernet Client)**

**Enable Universal Repeater Mode (Acting as AP and client simultaneously)**

**SSID of Extended Interface:**

### **Disable Wireless LAN Interface**

*Click on to disable the wireless LAN data transmission.*

### **Band**

*Click to select 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(B+G)*

### **Mode**

*Click to select the WLAN AP / Client / WDS / AP+WDS wireless mode.*

### **Site Survey**

*The Site Survey button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.*

### **SSID**

*It is the wireless network name. The SSID can be 32 bytes long.*

### **Channel Number**

*Select the wireless communication channel from pull-down menu.*

### **Associated Clients**

*Click the **Show Active Clients** button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client.*

### **Enable Mac Clone (Single Ethernet Client)**

*Take Laptop NIC MAC address as wireless client MAC address. [Client Mode*

only]

### Enable Universal Repeater Mode

Click to enable Universal Repeater Mode

### SSID of Extended Interface

Assign SSID when enables Universal Repeater Mode.

### Apply Changes

Click the Apply Changes button to complete the new configuration setting.

### Reset

Click the Reset button to abort change and recover the previous configuration setting.

## 4.4 Wireless - Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your WLAN Access Point.

### Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

---

**Authentication Type:**  Open System  Shared Key  Auto

**Fragment Threshold:**  (256-2346)

**RTS Threshold:**  (0-2347)

**Beacon Interval:**  (20-1024 ms)

**Data Rate:**

**Preamble Type:**  Long Preamble  Short Preamble

**Broadcast SSID:**  Enabled  Disabled

**IAPP:**  Enabled  Disabled

**802.11g Protection:**  Enabled  Disabled

**RF Output Power:**  100%  50%  25%  10%  5%

**Turbo Mode:**  Auto  Always  Off

Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

### Authentication Type

Click to select the authentication type in Open System, Shared Key or Auto

---

*selection.*

**Fragment Threshold**

*Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes.*

**RTS Threshold**

*Set the RTS Threshold, value can be written between 0 and 2347 bytes.*

**Beacon Interval**

*Set the Beacon Interval, value can be written between 20 and 1024 ms.*

**Data Rate**

*Select the transmission data rate from pull-down menu. Data rate can be auto-select, 11M, 5.5M, 2M or 1Mbps.*

**Preamble Type**

*Click to select the Long Preamble or Short Preamble support on the wireless data packet transmission.*

**Broadcast SSID**

*Click to enable or disable the SSID broadcast function.*

**IAPP**

*Click to enable or disable the IAPP function.*

**802.11g Protection**

*Protect 802.11b user.*

**RF Output Power**

*To adjust transmission power level.*

**Turbo Mode**

*Click to enable/disable turbo mode. (Only apply to WLAN IC of Realtek).*

**Apply Changes**

*Click the Apply Changes button to complete the new configuration setting.*

**Reset**

*Click the Reset button to abort change and recover the previous configuration setting.*

## **4.5 Wireless - Security Setup**

This page allows you setup the wireless security. Turn on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.

## Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

**Encryption:**

**Use 802.1x Authentication**  WEP 64bits  WEP 128bits

**WPA Authentication Mode:**  Enterprise (RADIUS)  Personal (Pre-Shared Key)

**WPA Cipher Suite:**  TKIP  AES

**WPA2 Cipher Suite:**  TKIP  AES

**Pre-Shared Key Format:**

**Pre-Shared Key:**

**Enable Pre-Authentication**

**Authentication RADIUS Server:** Port  IP address  Password

*Note: When encryption WEP is selected, you must set WEP key value.*



### Encryption

Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA(TKIP), WPA2 or WPA2 Mixed

### Use 802.1x Authentication

While Encryption is selected to be WEP.

Click the check box to enable IEEE 802.1x authentication function.

### WPA Authentication Mode

While Encryption is selected to be WPA.

Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key).

### WPA Cipher Suite

Enable TKIP or AES. Depends on which encryption you set.

### WPA2 Cipher Suite

Enable TKIP or AES. Depends on which encryption you set.

### Pre-Shared Key Format

While Encryption is selected to be WPA.

Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). [WPA, Personal(Pre-Shared Key) only]

### Pre-Shared Key

---

Fill in the key value. [WPA, Personal(Pre-Shared Key) only]

**Enable Pre-Authentication**

Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only]

**Authentication RADIUS Server**

Set the IP address, port and login password information of authentication RADIUS sever.

**Apply Changes**

Click the Apply Changes button to complete the new configuration setting.

**Reset**

Click the Reset button to abort change and recover the previous configuration setting.

## 4.6 WEP Key Setup

### Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

---

**Key Length:**

**Key Format:**

**Default Tx Key:**

**Encryption Key 1:**

**Encryption Key 2:**

**Encryption Key 3:**

**Encryption Key 4:**

**Key Length**

Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as "WEP2") keys.

The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit).

**Key Format**

Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.

**Default Tx Key**

Set the default secret key for WEP security function.

Value can be chose between 1 and 4.

**Encryption Key 1**

*Secret key 1 of WEP security encryption function.*

**Encryption Key 2**

*Secret key 2 of WEP security encryption function.*

**Encryption Key 3**

*Secret key 3 of WEP security encryption function.*

**Encryption Key 4**

*Secret key 4 of WEP security encryption function.*

**Apply Changes**

*Click the Apply Changes button to complete the new configuration setting.*

**Close**

*Click to close this WEP Key setup window.*

**Reset**

*Click the Reset button to abort change and recover the previous configuration setting.*

WEP encryption key (secret key) length:			
	Length	64-bit	128-bit
Format			
	ASCII	5 characters	13 characters
	HEX	10 hexadecimal codes	26 hexadecimal codes

## 4.7 Wireless - Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.

## Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

**Wireless Access Control Mode:**

**MAC Address:**  **Comment:**

**Current Access Control List:**

MAC Address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>		

### **Wireless Access Control Mode**

Click the Disabled, Allow Listed or Deny Listed of drop down menu choose wireless access control mode.

This is a security control function; only those clients registered in the access control list can link to this WLAN Access Point.

### **MAC Address**

Fill in the MAC address of client to register this WLAN Access Point access capability.

### **Comment**

Fill in the comment tag for the registered client.

### **Apply Changes**

Click the Apply Changes button to register the client to new configuration setting.

### **Reset**

Click the Reset button to abort change and recover the previous configuration setting.

### **Current Access Control List**

It shows the registered clients that are allowed to link to this WLAN Access Point.

### **Delete Selected**

Click to delete the selected clients that will be access right removed from this WLAN Access Point.

### **Delete All**

Click to delete all the registered clients from the access allowed list.

### **Reset**

Click the Reset button to abort change and recover the previous configuration setting.

## 4.8 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.]

**Requirement:** Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS

### WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

---

**Enable WDS**

**Add WDS AP:**    **MAC Address**     **Comment**

**Current WDS AP List:**

MAC Address	Comment	Select
00:00:00:00:00:00	AP-1	<input type="checkbox"/>
11:11:11:11:11:11	AP-2	<input type="checkbox"/>

### **Enable WDS**

Click the check box to enable wireless distribution system. Refer to 4.21 What is Wireless Distribution System (WDS)?

### **MAC Address**

Fill in the MAC address of AP to register the wireless distribution system access capability.

### **Comment**

Fill in the comment tag for the registered AP.

### **Apply Changes**

Click the Apply Changes button to register the AP to new configuration setting.

---

**Reset**

Click the Reset button to abort change and recover the previous configuration setting.

**Set Security**

Click button to configure wireless security like WEP(64bits), WEP(128bits), WPA (TKIP), WPA2(AES) or None

**Show Statistics**

It shows the TX, RX packets, rate statistics

**Delete Selected**

Click to delete the selected clients that will be removed from the wireless distribution system.

**Delete All**

Click to delete all the registered APs from the wireless distribution system allowed list.

**Reset**

Click the Reset button to abort change and recover the previous configuration setting.

#### 4.8.1 WDS Security Setup

**Requirement: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS**

This page is used to configure the wireless security between APs.

## WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

---

Encryption:	<input type="text" value="None"/>
WEP Key Format:	<input type="text" value="ASCII (5 characters)"/>
WEP Key:	<input type="text"/>
Pre-Shared Key Format:	<input type="text" value="Passphrase"/>
Pre-Shared Key:	<input type="text"/>

## 4.8.1.1 WDS AP Table

This page is used to show WDS statistics

## WDS AP Table

This table shows the MAC address, transmission, reception packet counters and state information for each configured WDS AP.

---

MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)
00:00:00:00:00:00	238	238	0	1
11:11:11:11:11:11	238	0	0	54

**MAC Address**

*It shows the MAC Address within WDS.*

**Tx Packets**

*It shows the statistic count of sent packets on the wireless LAN interface.*

**Tx Errors**

*It shows the statistic count of error sent packets on the Wireless LAN interface.*

**Rx Packets**

*It shows the statistic count of received packets on the wireless LAN interface.*

**Tx Rare (Mbps)**

*It shows the wireless link rate within WDS.*

**Refresh**

*Click to refresh the statistic counters on the screen.*

**Close**

*Click to close the current window.*

## 4.9 Site Survey

This page is used to view or configure other APs near yours.

### Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
Computer Room AP Router	00:1a:ef:04:f1:66	6 (B+G)	AP	WPA2-PSK	32	<input checked="" type="radio"/>
Living Room Ap Router	00:1a:ef:02:57:94	1 (B+G)	AP	WPA2-PSK	13	<input type="radio"/>

### **SSID**

*It shows the SSID of AP.*

### **BSSID**

*It shows BSSID of AP.*

### **Channel**

*It show the current channel of AP occupied.*

### **Type**

*It show which type AP acts.*

### **Encrypt**

*It shows the encryption status.*

### **Signal**

*It shows the power level of current AP.*

### **Select**

*Click to select AP or client you'd like to connect.*

### **Refresh**

*Click the Refresh button to re-scan site survey on the screen.*

### **Connect**

*Click the Connect button to establish connection.*

**Requirement: Set**

**[Wireless]->[Basic Settings]->[Mode]->client**

## 4.10 TCP/IP Settings

This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc.

## LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

<b>IP Address:</b>	<input type="text" value="192.168.1.254"/>
<b>Subnet Mask:</b>	<input type="text" value="255.255.255.0"/>
<b>Default Gateway:</b>	<input type="text" value="0.0.0.0"/>
<b>DHCP:</b>	<input type="text" value="Server"/> <input type="button" value="v"/>
<b>DHCP Client Range:</b>	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
<b>DNS Server:</b>	<input type="text"/>
<b>Domain Name:</b>	<input type="text"/>
<b>802.1d Spanning Tree:</b>	<input type="text" value="Disabled"/> <input type="button" value="v"/>
<b>Clone MAC Address:</b>	<input type="text" value="000000000000"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

### IP Address

Fill in the IP address of LAN interfaces of this WLAN Access Point.

### Subnet Mask

Fill in the subnet mask of LAN interfaces of this WLAN Access Point.

### Default Gateway

Fill in the default gateway for LAN interfaces out going data packets.

### DHCP

Click to select Disabled, Client or Server in different operation mode of wireless Access Point.

### DHCP Client Range

Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.

### Show Client

Click to open the Active DHCP Client Table window that shows the active clients with their assigned IP address, MAC address and time expired information.

[Server mode only]

### DNS Server

Manual setup DNS server IP address.

### Domain Name

Assign Domain Name and dispatch to DHCP clients. It is optional field.

### 802.1d Spanning Tree

Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.

## Clone MAC Address

Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?

## Apply Changes

Click the Apply Changes button to complete the new configuration setting.

## Reset

Click the Reset button to abort change and recover the previous configuration setting.

## 4.11 Log

This page is used to configure the remote log server and shown the current log.

### System Log

This page can be used to set remote log server and show the system log.

**Enable Log**

**system all**       **wireless**

**Enable Remote Log**      **Log Server IP Address:**

```
Oday 00:45:48 br0: port 4(wlan0-wds1) entering forwarding state
Oday 00:45:48 br0: topology change detected, propagating
Oday 00:45:48 br0: port 2(wlan0) entering listening state
Oday 00:45:48 br0: port 3(wlan0-wds0) entering learning state
Oday 00:45:48 br0: port 3(wlan0-wds0) entering forwarding state
Oday 00:45:48 br0: topology change detected, propagating
Oday 00:45:48 br0: port 1(eth0) entering listening state
Oday 00:45:48 br0: port 2(wlan0) entering learning state
Oday 00:45:48 br0: port 2(wlan0) entering forwarding state
Oday 00:45:48 br0: topology change detected, propagating
Oday 00:45:48 br0: port 1(eth0) entering learning state
Oday 00:45:48 br0: port 1(eth0) entering forwarding state
Oday 00:45:48 br0: topology change detected, propagating
Oday 00:45:48 wlan0: A wireless client is associated - 00:1A:EF:01:00:E5
```

### Enable Log

*System all*

### Wireless only

*Click the checkbox to enable log.*

### Show all log of wireless Access Point.

*Only show wireless log.*

### Enable Remote Log

Click the checkbox to enable remote log service.

### Log Server IP Address

Input the remote log IP address

### Apply Changes

Click the Apply Changes button to save above settings.

### Refresh

Click the refresh the log shown on the screen.

### Clear

Clear log display screen

## 4.12 Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet LAN networks.

### Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

---

<b>Wireless LAN</b>	<i>Sent Packets</i>	210
	<i>Received Packets</i>	65
<b>Ethernet LAN</b>	<i>Sent Packets</i>	519
	<i>Received Packets</i>	0

### Wireless LAN Sent Packets

*It shows the statistic count of sent packets on the wireless LAN interface.*

### Wireless LAN Received Packets

*It shows the statistic count of received packets on the wireless LAN interface.*

### Ethernet LAN Sent Packets

*It shows the statistic count of sent packets on the Ethernet LAN interface.*

### Ethernet LAN Received Packets

*It shows the statistic count of received packets on the Ethernet LAN interface.*

### Refresh

Click the refresh the statistic counters on the screen.

## 4.13 Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

---

## Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

### Select File

Click the Browse button to select the new version of web firmware image file.

### Upload

Click the Upload button to update the selected web firmware image to the WLAN Access Point.

### Reset

Click the Reset button to abort change and recover the previous configuration setting.

## 4.14 Save / Reload Settings

This page allows you save current settings to a file or reload the settings from the file that was saved previously. Besides, you could reset the current configuration to factory default.

## Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

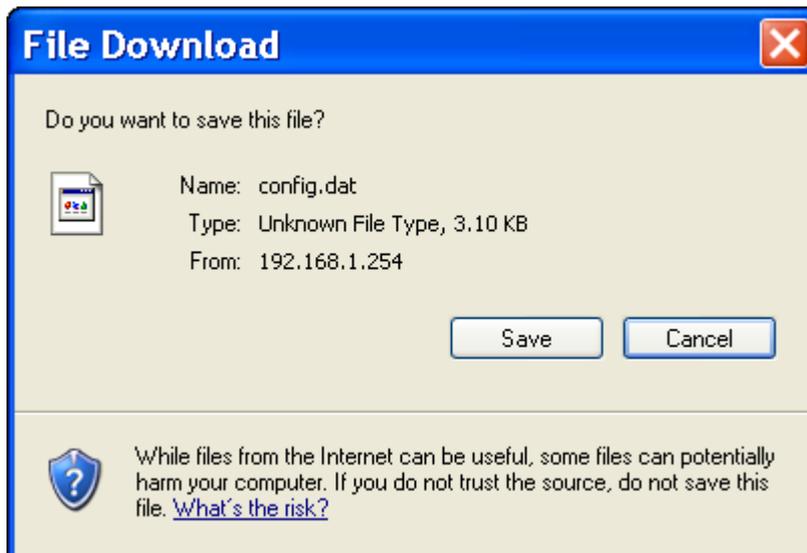
Save Settings to File:

Load Settings from File:

Reset Settings to Default:

### Save Settings to File

Click the Save button to download the configuration parameters to your personal computer.



### Load Settings from File

Click the *Browse* button to select the configuration files then click the *Upload* button to update the selected configuration to the WLAN Access Point.

### Reset Settings to Default

Click the *Reset* button to reset the configuration parameter to factory defaults.

## 4.15 Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

### Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

---

**User Name:**

**New Password:**

**Confirmed Password:**

### User Name

Fill in the user name for web management login control.

### New Password

Fill in the password for web management login control.

### Confirmed Password

Because the password input is invisible, so please fill in the password again for confirmation purpose.

---

## Apply Changes

Clear the User Name and Password fields to empty, means to apply no web management login control.

Click the Apply Changes button to complete the new configuration setting.

## Reset

Click the Reset button to abort change and recover the previous configuration setting.

## After set password finish.

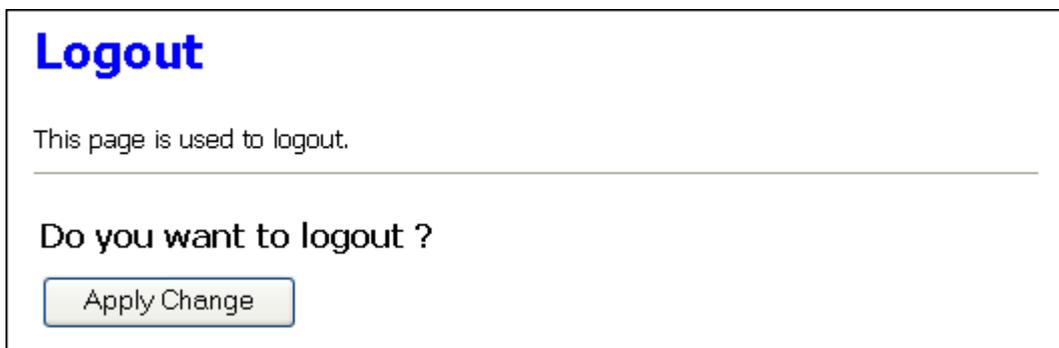
Open a WEB browser, i.e. Microsoft Internet Explore, then enter **192.168.1.254** on the URL to connect the WLAN Access Point.



Type admin for the username and type the password click ok to login.

## 4.16 Logout

This page is used to logout web management page. This item will be activated next time you login after you define user account and password.





### Apply Change

Click the Apply Change button, Then click OK button to logout.

## 5 Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the Access Point. We cover various aspects of the network including network adapters. (The examples below are illustrated in Windows XP. If you have another operating system, these solutions will still apply, although the appearance on your computer screen may differ.)

**Note:** It is recommended that you use an Ethernet connection to configure the Access Point.

1. The computer used to configure the Access Point can not access the configuration menu.

- Check that the LAN LED on the Access Point is ON. If the LED is not ON, check that the cable for the Ethernet connection is securely inserted.
- Check that the Ethernet adapter is working properly. Please see item 3 (Check that the drivers for the network adapters are installed properly) in this Troubleshooting section to check that the drivers are loaded properly.
- Check that the IP address is in the same range and subnet as the Access Point. Please see Checking the IP Address in Windows XP in the Networking Basics section of this manual.

**Note:** The IP address of the Access Point is 192.168.1.254. All the computers on the network must have a unique IP address in the same range, e.g., 192.168.1.x. Any computers that have identical IP addresses will not be visible on the network. They must all have the same subnet mask, e.g., 255.255.255.0

- Do a **Ping test** to make sure that the Access Point is responding. Go to **Start>Run>Type Command>Type** ping 192.168.1.254 A successful ping will show four replies.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dip>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=20ms TTL=255
Reply from 192.168.1.254: bytes=32 time=6ms TTL=255
Reply from 192.168.1.254: bytes=32 time=5ms TTL=255
Reply from 192.168.1.254: bytes=32 time=28ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 28ms, Average = 14ms

C:\Documents and Settings\dip>
```

Ping fail

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dip>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

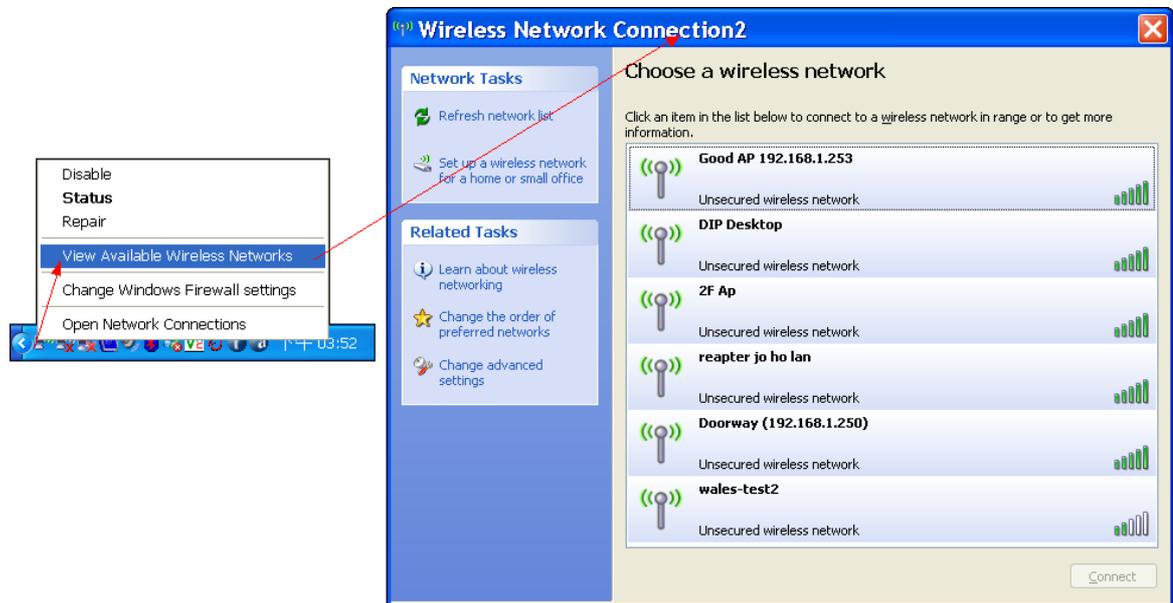
C:\Documents and Settings\dip>
```

**2. The wireless client cannot access the Internet in the Infrastructure mode.**

Make sure the wireless client is associated and joined with the correct access point (Access Point). To check this connection: Right-click on the Local Area Connection icon in the taskbar> select View Available Wireless Networks.

The Connect to Wireless Network screen will appear. Please make sure you have selected the correct available network, as shown in the illustrations below.

**Note:** Screen shots were taken using Windows XP. Your screens may differ.

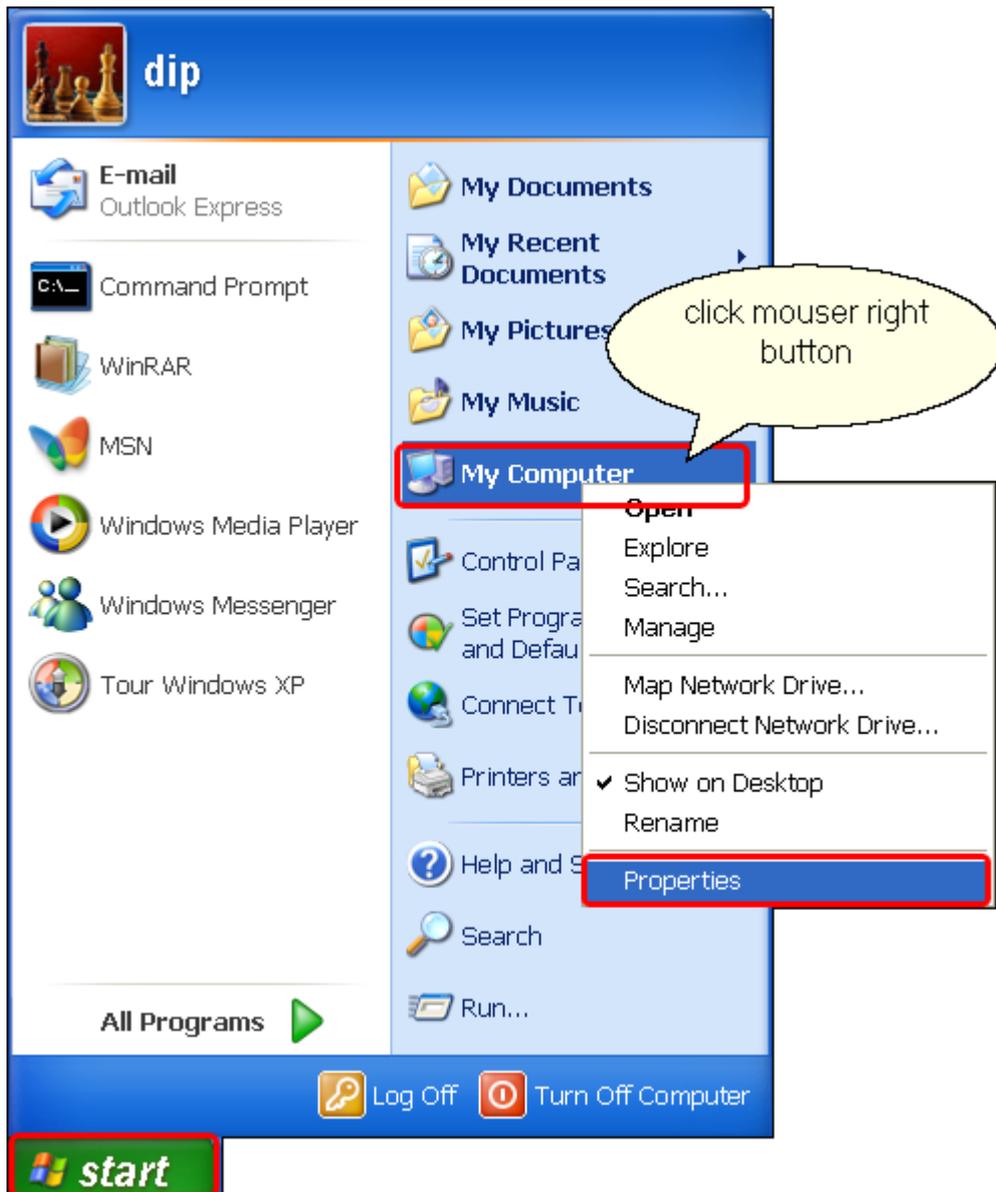


- Check that the **IP address** assigned to the wireless adapter is within the same **IP address range** as the access point and gateway. Since the Access Point has an IP address of **192.168.1.254**, wireless adapters must have an IP address in the same range, e.g., **192.168.1.x**. Each device must have a unique IP address; no two devices may have the same IP address. The subnet mask must be the same for all the computers on the network. To check the **IP address** assigned to the wireless adapter, **double-click** on the **Local Area Connection** icon in the taskbar > select the **Support** tab and the **IP address** will be displayed. (Please refer to **Checking the IP Address** in the **Networking Basics** section of this manual.)
- If it is necessary to assign a **static IP address** to the wireless adapter, please refer to the appropriate section in **Networking Basics**. If you are entering a **DNS Server address** you must also enter the **Default Gateway Address**. (Remember that if you have a DHCP-capable router, you will not need to assign a static IP address. See **Networking Basics: Assigning a Static IP Address**.)

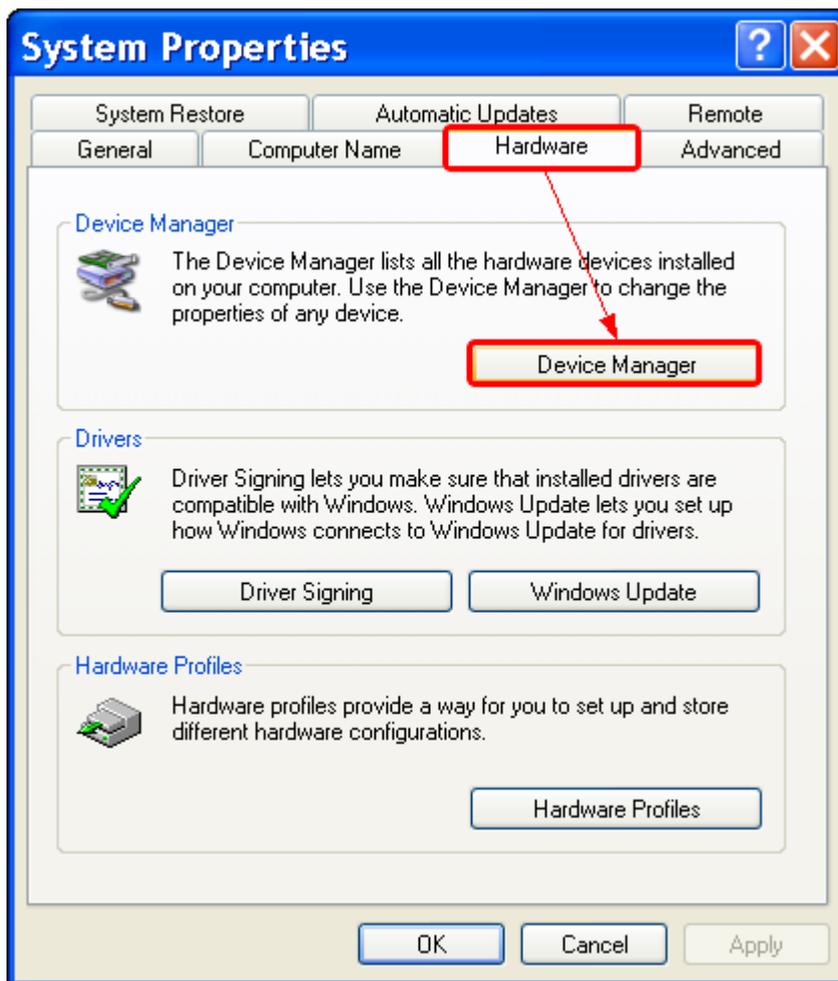
**3. Check that the drivers for the network adapters are installed properly.**

You may be using different network adapters than those illustrated here, but this procedure will remain the same, regardless of the type of network adapters you are using.

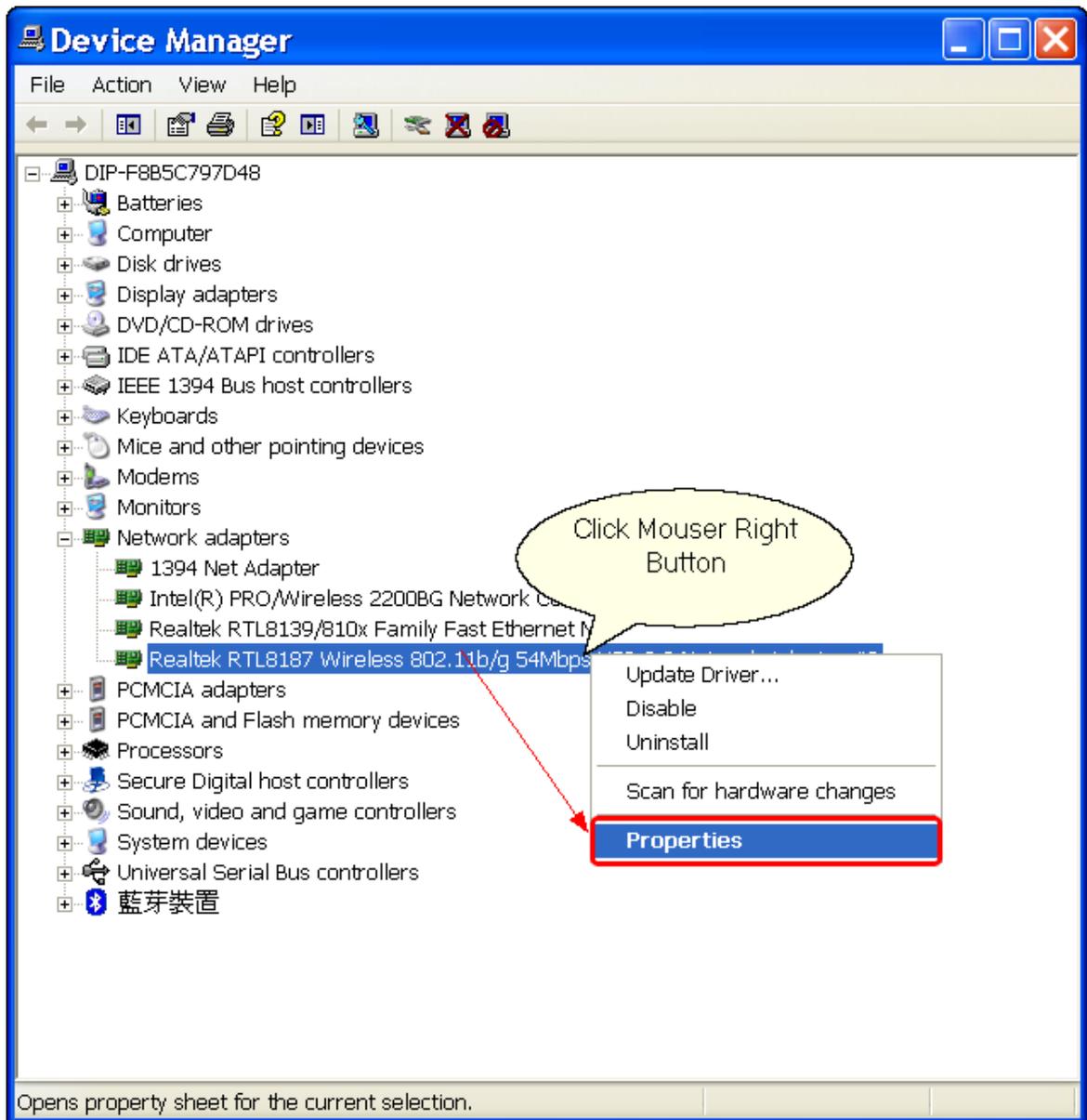
- Go to **Start**
- Right-click on **My Computer**
- Click **Properties**



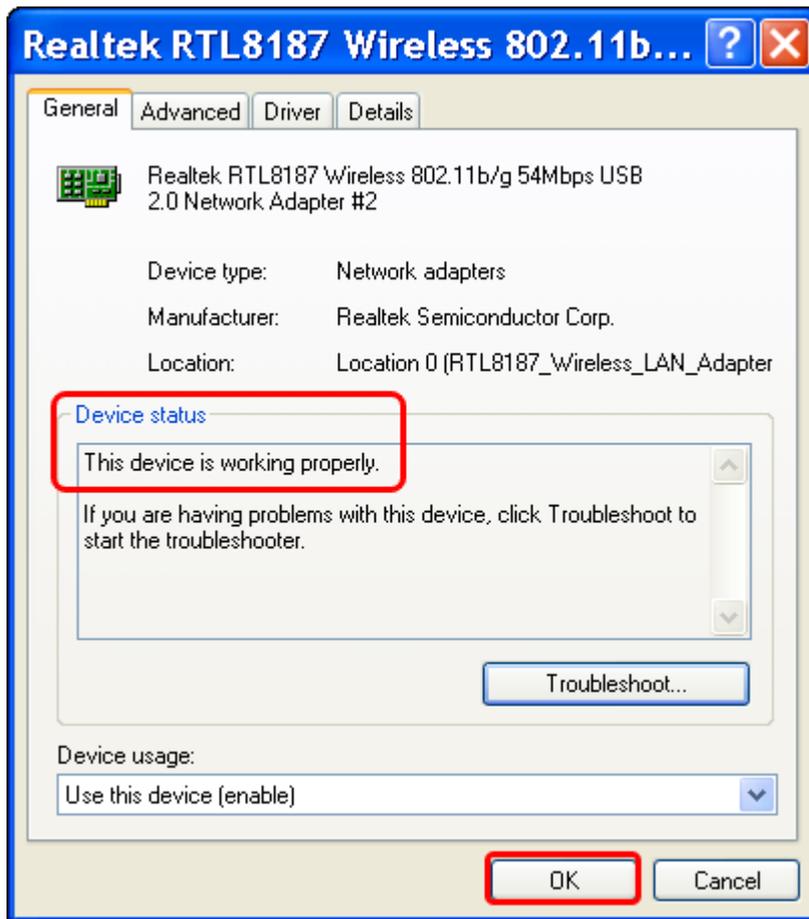
- Select the **Hardware** Tab
- Click **Device Manager**



- Double-click on **Network Adapters**
- **Right-click** on **Realtek RTL8187 Wireless Adapter** (or whatever network adapter you are using)
- Select **Properties** to check that the drivers are installed properly



- Look under **Device Status** to check that the device is working properly.
- Click **OK**



## 6 Frequently Asked Questions (FAQ)

### 6.1 What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, **191.168.1.254** could be an IP address.

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- Open the Command program in the Microsoft Windows.
- Type in ipconfig /all then press the Enter button.
- Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

---

## 6.2 What is Wireless LAN?

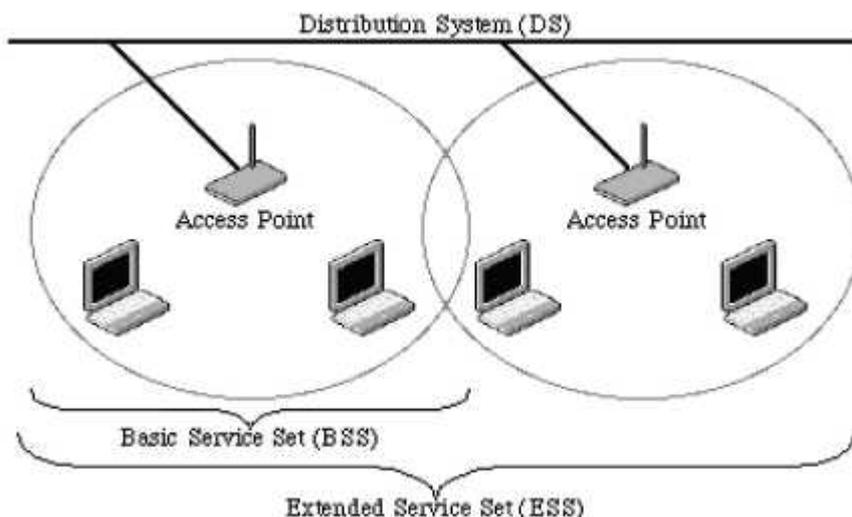
A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

## 6.3 What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

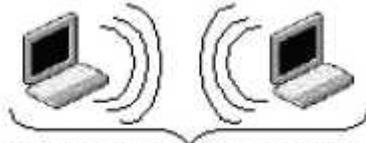
## 6.4 How does wireless networking work?

The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Independent Basic Service Set (IBSS)  
Example 2: wireless Ad Hoc Mode

## 6.5 What is BSSID?

A six-byte address that distinguishes a particular access point from others. Also known as just SSID. Serves as a network ID or name.

## 6.6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

## 6.7 What are potential factors that may cause interference?

Factors of interference:

- Obstacles: walls, ceilings, furniture... etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- Minimizing the number of walls and ceilings.
- Position the WLAN antenna for best reception.
- Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors, ... etc.
- Add additional WLAN Access Points if necessary.

## 6.8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

## 6.9 What is WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to encrypt frame bits to avoid disclosure to eavesdroppers.

---

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

## 6.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

## 6.11 What is RTS (Request To Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

## 6.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN,

enabling stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

### **6.13 What is Preamble Type?**

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

### **6.14 What is SSID Broadcast?**

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

### **6.15 What is Wi-Fi Protected Access (WPA)?**

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the Wi-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

### **6.16 What is WPA2?**

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

---

## 6.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

## 6.18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

## 6.19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

## 6.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet. IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

## 6.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

## 6.22 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address. Since that all the clients will communicate outside world through the WLAN Access Point, so have the cloned MAC address set on the WLAN Access Point will solve the issue.