Lantech

Industrial

Wireless Access Point

IWP-1000 User's Manual

Version 1.0

Jan, 2010.

Table of Content

Getting to Know Your Access Point

1.1 About the IWP-1000

IWP-1000 is a reliable IEEE802.11a/b/g WLAN with 2 ports LAN Access Point. It can be configured to operate in AP/Bridge/Repeater/AP-Client/Client mode. You can configure IWP-1000 by Window Utility or WEB interfaces via LAN port or WLAN interface. IWP-1000 provides dual Ethernet ports in switch mode, so you can use Daisy Chain to reduce the usage of Ethernet switch ports. It also provides P.D. feature on ETH2 which is fully compliant with IEEE802.3af PoE specification. Therefore, IWP-1000 is one of the best communication solutions for wireless application.

1.2 Software Features

- High Speed Air Connectivity: WLAN interface support up to 54Mbps link speed connection
- Highly Security Capability: WEP/WPA/WPA2/Radius/TKIP supported
- Support AP/Bridge/Repeater/AP-Client Mode
- Switch Mode Supported: Daisy Chain support to reduce usage of switch ports
- Secured Management by HTTPS
- Event Warning by Syslog, Email, SNMP Trap, Relay and Beeper

1.3 Hardware Features

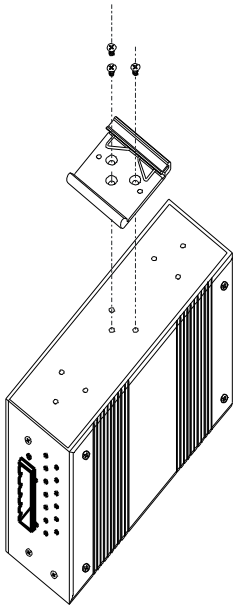
- Fully Compliant with IEEE802.3af
- Redundant Power Inputs: 12~48 VDC on terminal block
- 10/100Base-T(X) Ethernet port
- Casing: IP-30
- Dimensions(W x D x H) : 52 mm(W)x 106 mm(D)x 144 mm(H)
- Operating Temperature: -10 to 55^{o}C
- Storage Temperature: -40 to 85^{o}C
- Operating Humidity: 5% to 95%, non-condensing

Hardware Installation

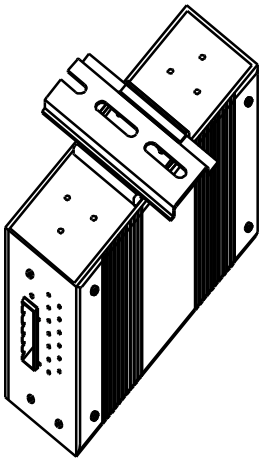
2.1 Installation AP on DIN-Rail

Each AP has a DIN-Rail kit on rear panel. The DIN-Rail kit helps AP to fix on the DIN-Rail. It is easy to install the AP on the DIN-Rail:

Step 1: Slant the AP and mount the metal spring to DIN-Rail.



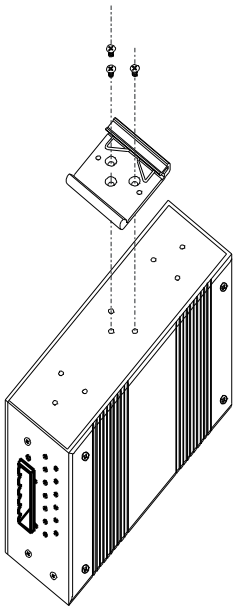
Step 2: Push the AP toward the DIN-Rail until you heard a “click” sound.



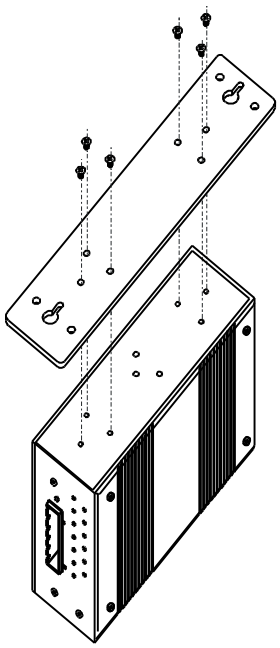
2.2 Wall Mounting Installation

Each AP has another installation method to fix the AP. A wall mount panel can be found in the package. The following steps show how to mount the AP on the wall:

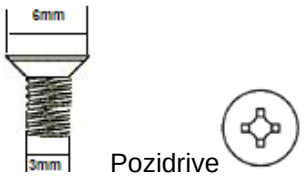
Step 1: Remove DIN-Rail kit.



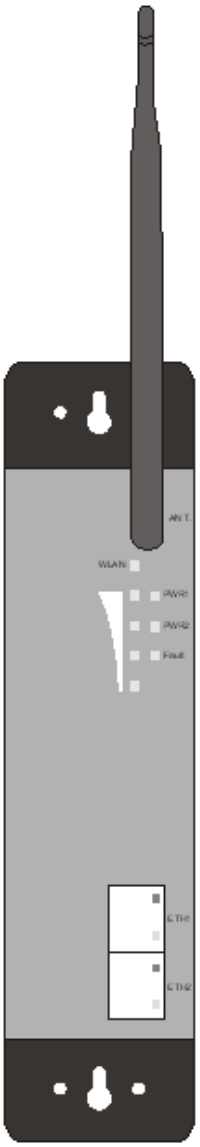
Step 2: Use 6 screws that can be found in the package to combine the wall mount panel. Just like the picture shows below:



The screws specification shows in the following two pictures. In order to prevent the AP from any damage, the screws should not larger than the size that used in IWP-1000.



Step 3: Mount the combined AP on the wall.

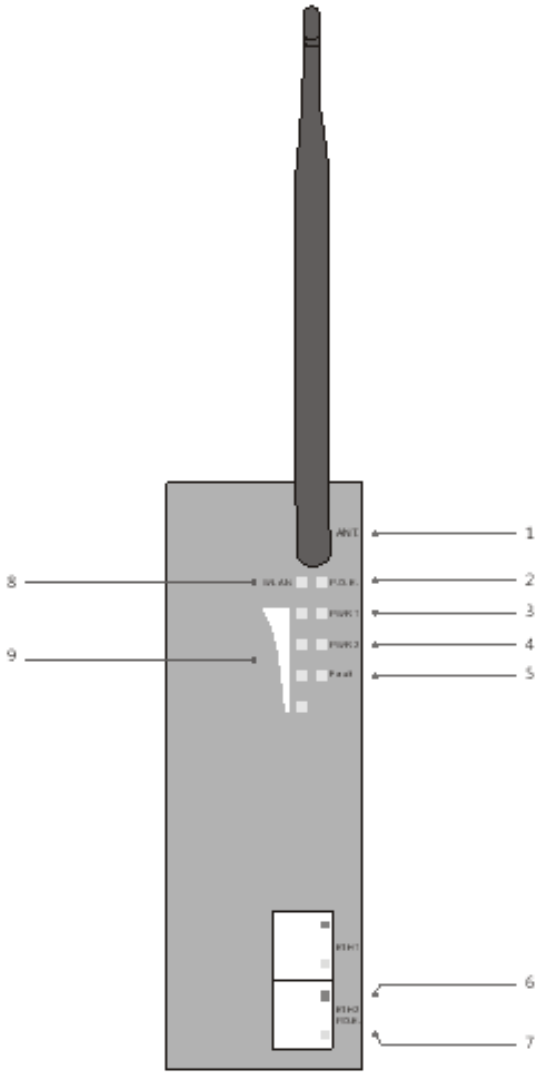


Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the IWP-1000.

Port	Description
10/100 RJ-45 fast Ethernet ports	2 10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto
PoE P.D. Port	ETH2 compliant with IEEE802.3af PoE specifications
ANT.	Reversed SMA connector for high gain external antenna.



1. 2.4GHz antenna with typical 3.0 dbi antenna.
2. LED for PoE power and system status. When the PoE power links, the green LED will be light on.
3. LED for PWR1 and system status. When the PWR1 links, the green LED will be light on.
4. LED for PWR2 and system status. When the PWR2 links, the green LED will be light on.
5. LED for Fault Relay. When the fault occurs, the amber LED will be light on.
6. 10/100Base-T(X) Ethernet ports. (contains P.D. function of PoE)
7. LED for Ethernet ports status.
8. LED for WLAN link status.
9. LED for WLAN signal strength.

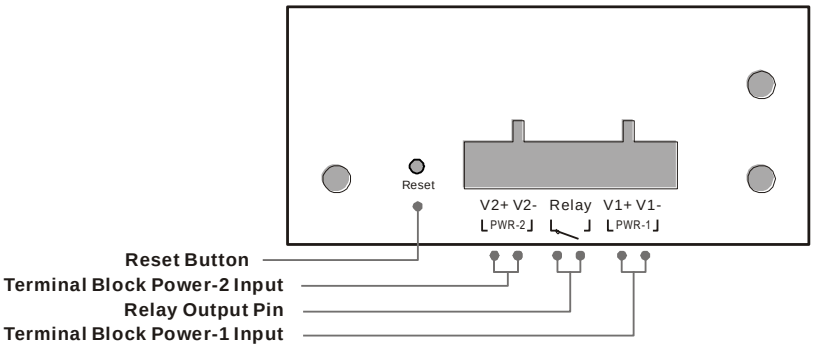
3.2 Front Panel LEDs

LED	Color	Status	Description
P.O.E.	Green/Red	Green On	PoE power connected.
		Green blinking	Device been located
		Red blinking	Indicates an IP conflict, or DHCP or BOOTP server did not respond properly
PWR1	Green/Red	Green On	DC power 1 activated.
		Green blinking	Device been located
		Red blinking	Indicates an IP conflict, or DHCP or BOOTP server did not respond properly
PWR2	Green/Red	Green On	DC power 2 activated.
		Green blinking	Device been located
		Red blinking	Indicates an IP conflict, or DHCP or BOOTP server did not respond properly
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
WLAN	Green	On	WLAN activated.
		Blinking	WLAN Data transmitted.
WLAN Strength	Green	On	WLAN signal strength. 1<25%, 2<50%, 3<75%, 4<100%
10/100Base-T(X) Fast Ethernet ports			
10Mbps LNK/ACT	Amber	On	Port link up at 10Mbps.
		Blinking	Data transmitted.
100Mbps LNK/ACT	Green	On	Port link up at 100Mbps.
		Blinking	Data transmitted.

3.3 Bottom Panel

The bottom panel components of IWP-1000 are showed as below:

1. Terminal block includes: PWR1, PWR2 (12 ~ 48V DC) and Relay output (1A@24VDC).
2. Reset bottom. Push the bottom 3 seconds for reset; 5 seconds for factory default.

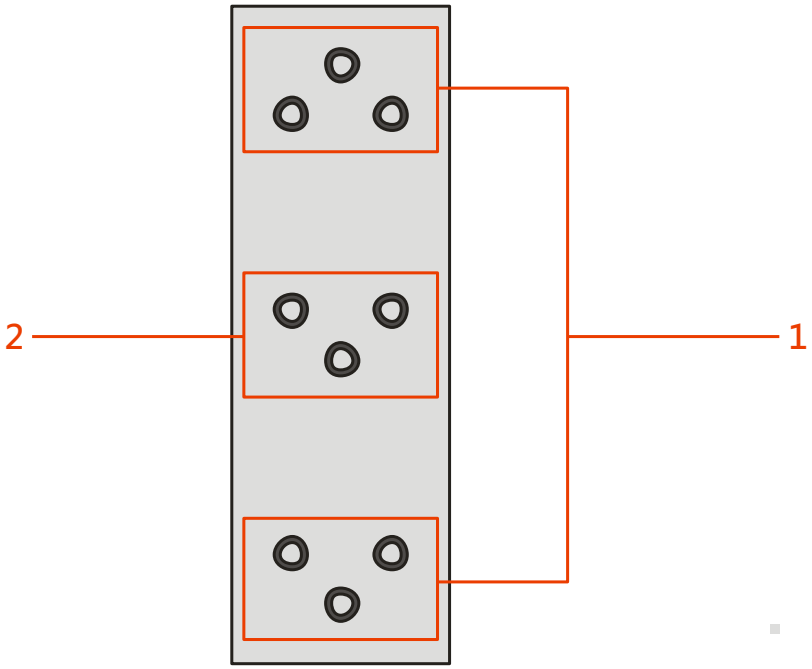


Bottom panel of IWP-1000

3.4 Rear Panel

The rear panel components of IWP-1000 are showed as below:

1. Screw holes for wall mount kit.
2. DIN-Rail kit



Rear panel of IWP-1000

Cables and Antenna

4.1 Ethernet Cables

The IWP-1000 WLAN AP has standard Ethernet ports. According to the link type, the AP use CAT 3, 4, 5,5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10Base-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100Base-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45

4.2 100Base-T(X)/10Base-T Pin Assignments

With 100Base-T(X)/10Base-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

The IWP-1000 AP supports auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and AP. The following table below shows the 10Base-T/ 100Base-T(X) MDI and MDI-X port pin outs.

MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

Note: “+” and “-” signs represent the polarity of the wires that make up each wire pair.

4.3 Wireless Antenna

A 2.4GHz antenna is used for IWP-1000 and connected with a reversed SMA connector. External antenna also can be applied with this connector.

Management Interface

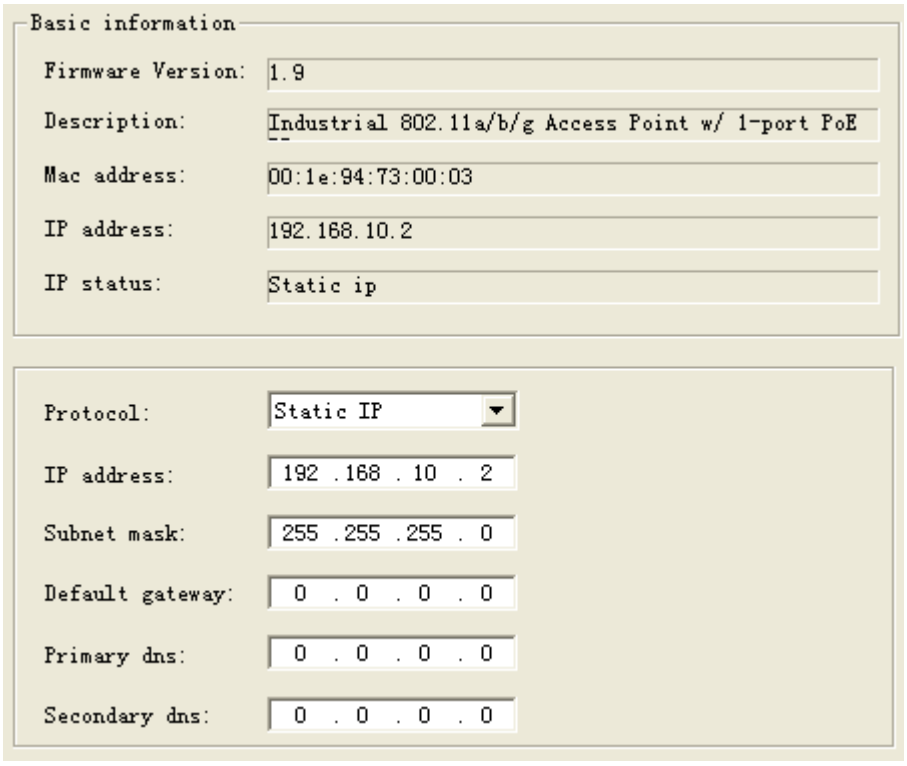
5.1 Explore IWP-1000

5.1.1 AP-Tool software

Each model contains friendly software, AP-Tool, to explore IWP-1000 on local area network.

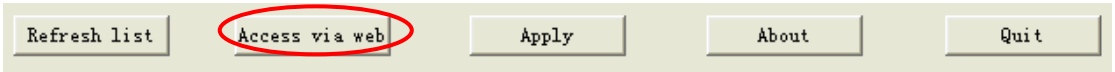
Step 1: Open the AP tool and click “Refresh list”, the AP devices will show on the list.

Step 2: Choose your access point, and it will show the AP attribute. Simultaneity, you can manual set the AP’s IP address.



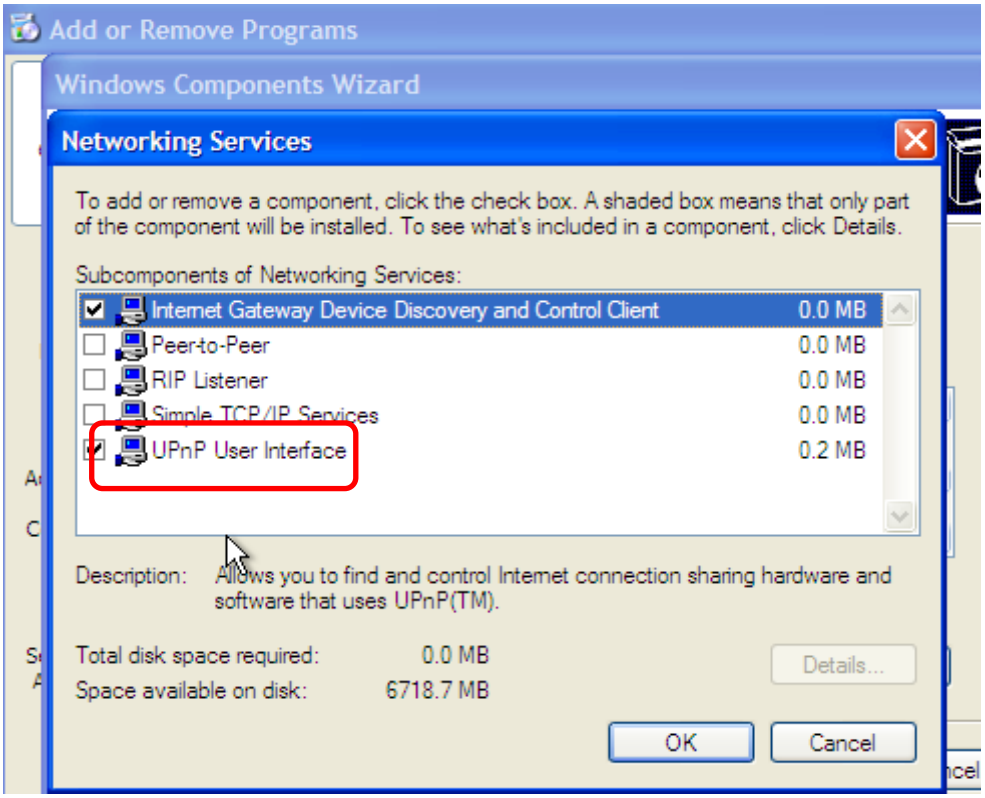
User interface of AP-Tool

Step 3: Click “Access via web” button, it will go to web page.



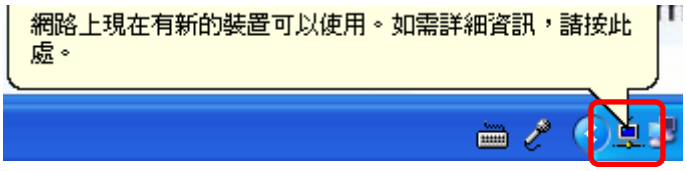
5.2 UPnP Equipment

Step 1: To check whether the UPnP UI of the computer is connected to the IWP-1000, go to **Control Panel > Add or Remove Programs > Windows Components Wizard > Networking Servers > UPnP User Interface** and pitch on the UPnP User Interface.

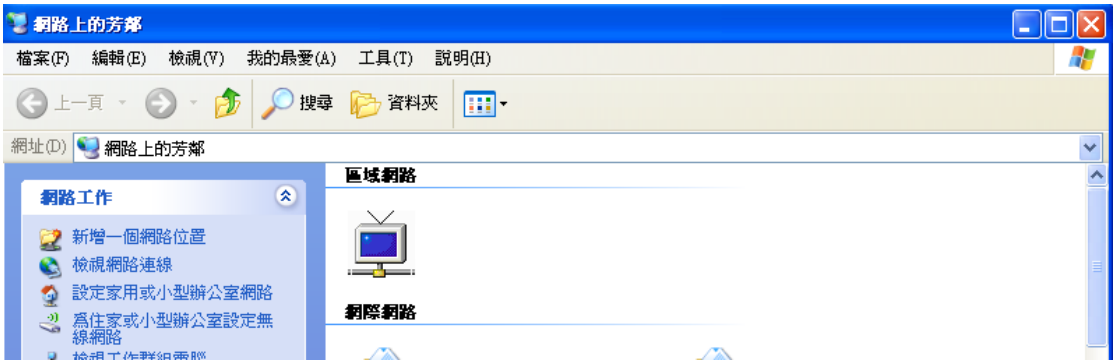


UPnP configuration page

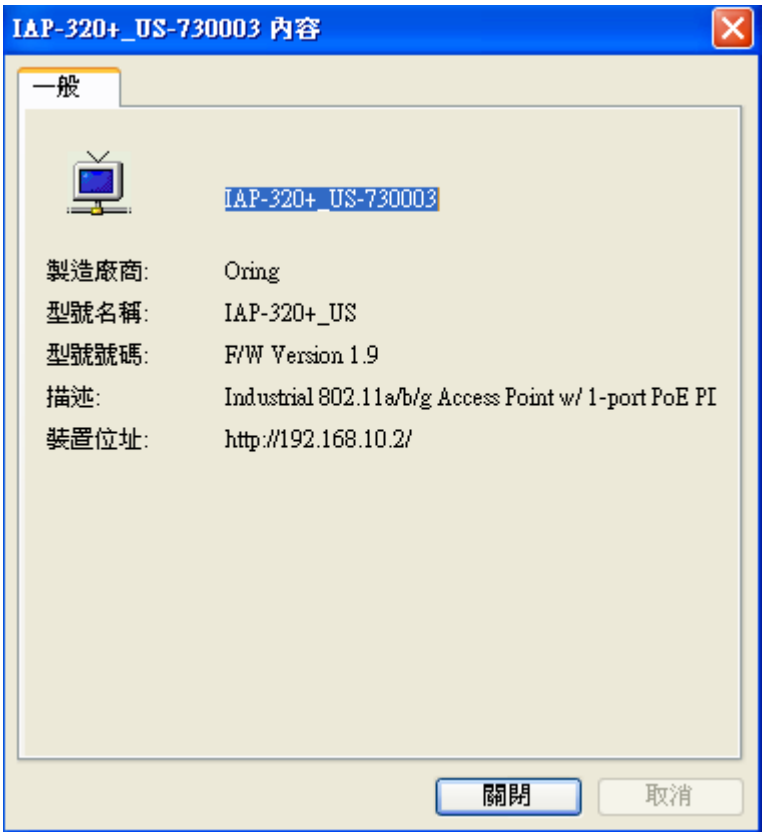
Step 2: At the right-below corner of the computer, you will find a sign of the UPnP equipment.



Step 3: Click the sign of the UPnP equipment, then you will find the UPnP equipment in the network neighborhood.



Step 4: Right click the UPnP equipment to choose “Properties”, it will show as the following pictures:



Step 5: Right click the UPnP equipment or double click the UPnP equipment to transfer; it will go to the web page.

5.3 Configuration by Web Browser

This section introduces the configuration by Web browser.

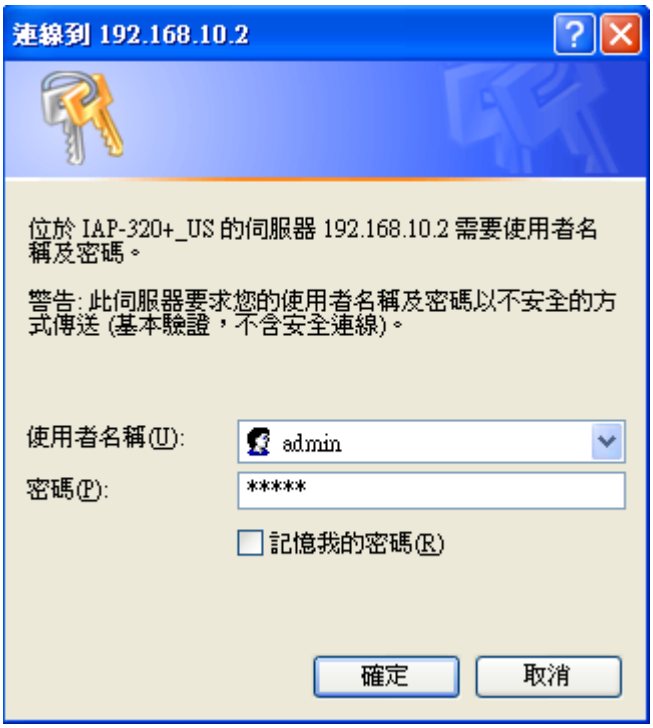
5.4 About Web-Based Management

An embedded HTML web site resides in flash memory in the system. It contains advanced management features and allows you to manage the AP from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is Based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

Through the front section's information, you will see as follows, enter your user name **(admin)** and your password **(admin)**, then click **OK** to continue.

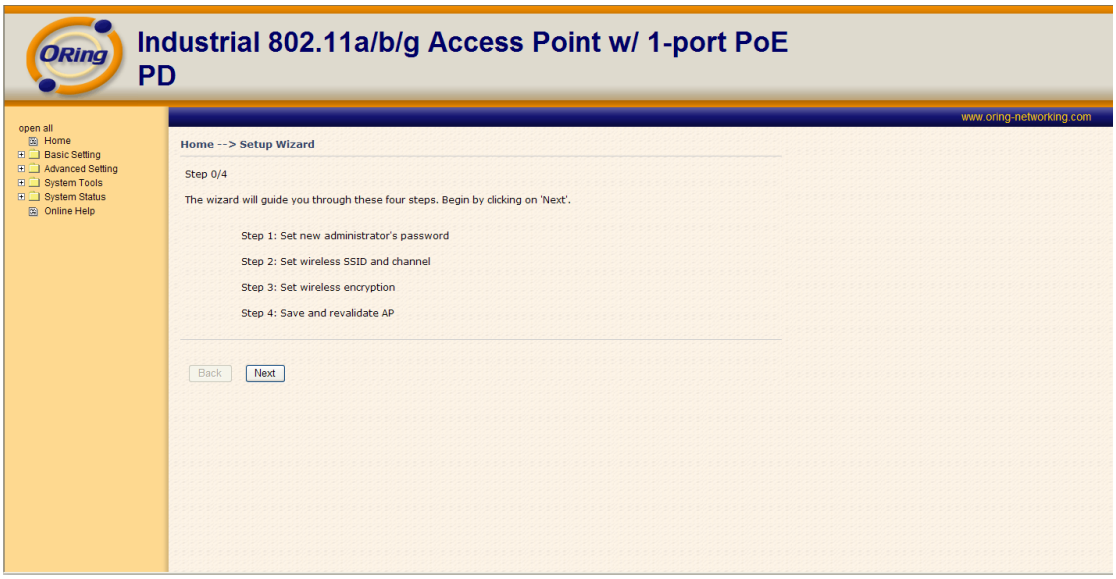


Login screen

For security reasons, we strongly suggest you change the password. Click on **System Tools > Administrator** and modify the password.

5.5 Main Interface

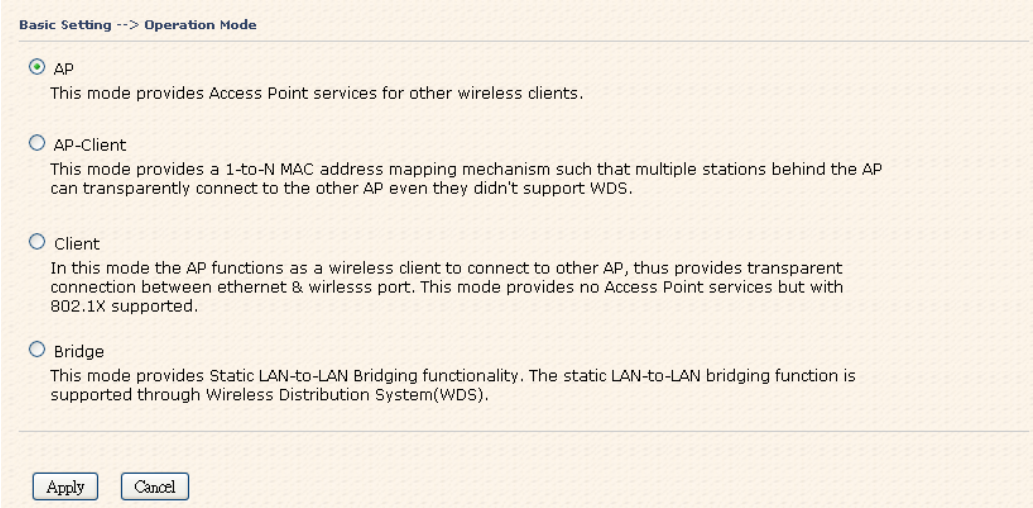
The **Home** screen will appear. Please click “Run Wizard” to go to the **Home > Setup Wizard** page to quick install the AP.



Main interface

5.5.1 Basic Setting

Setting Operation Mode



Operation mode interface

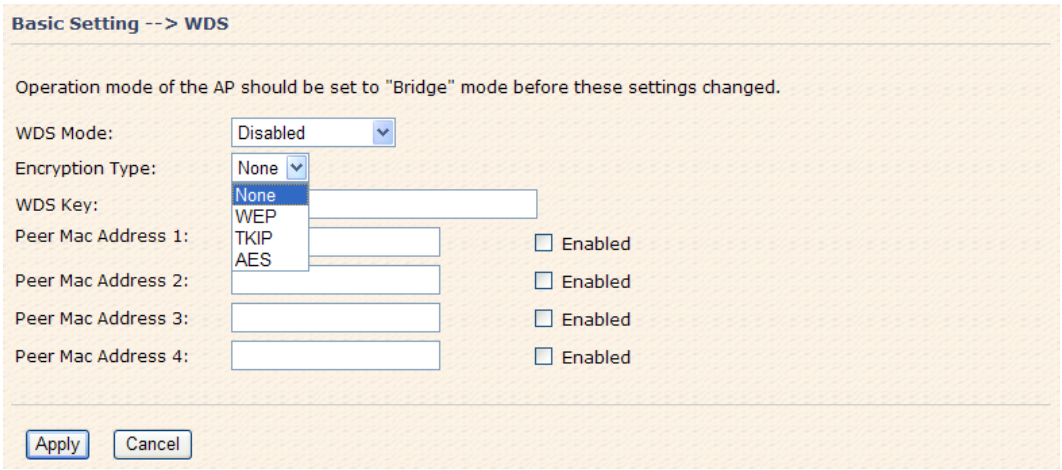
The following table describes the labels in this screen.

Label	Description
AP	This mode provides Access Point services for other wireless clients.
AP-Client	The AP-Client function provides a 1-to-N MAC address mapping mechanism such that multiple stations behind the AP can

	transparently connect to the other AP even they didn't support WDS.
Client	In this mode the AP functions as a wireless client to connect to other AP, thus provides transparent connection between Ethernet & wireless port. This mode provides no Access Point services but with 802.1X supported.
Bridge	This mode provides Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).

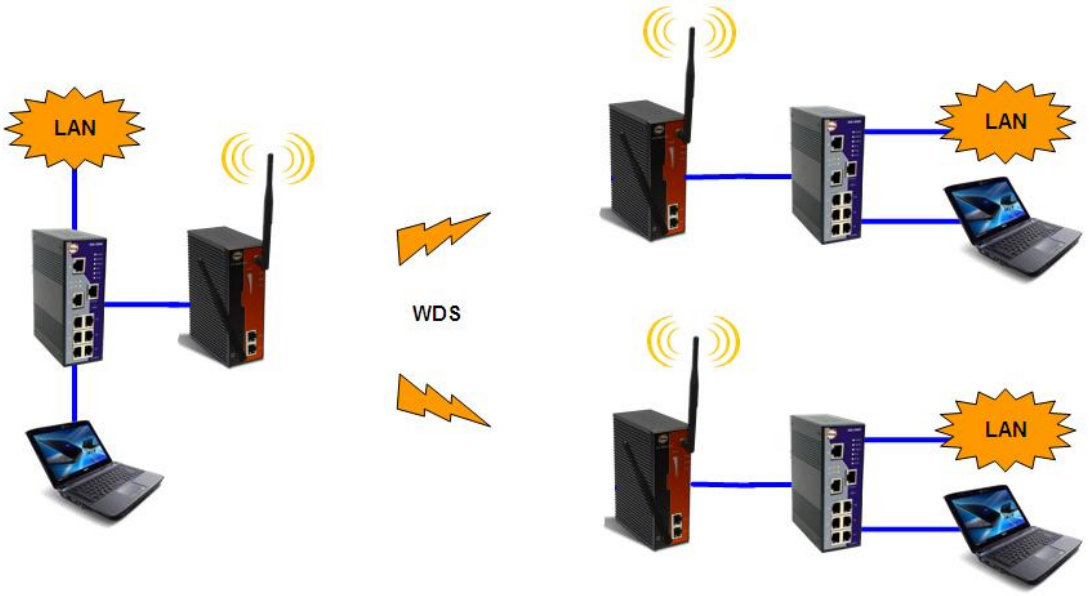
In each mode, the IWP-1000 forwards packet between its Ethernet interface and wireless interface for wired hosts on the Ethernet side, and wireless hosts on the wireless side.

Setting WDS (Bridge Mode)

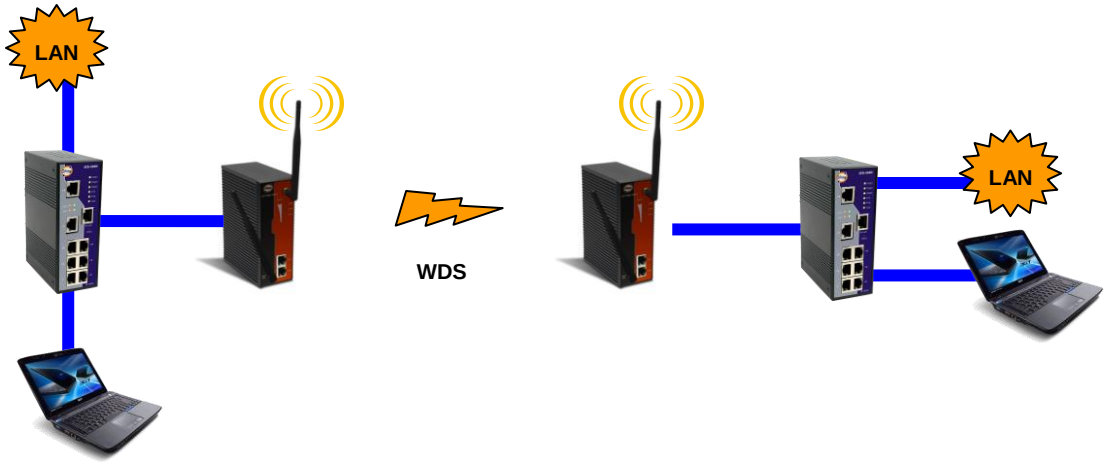


WDS setting interface

This type of wireless link is established between two IEEE 802.11 access points. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.



Point-to-Multipoint WDS Link



Point-to-Point WDS Link

The following table describes the labels in this screen.

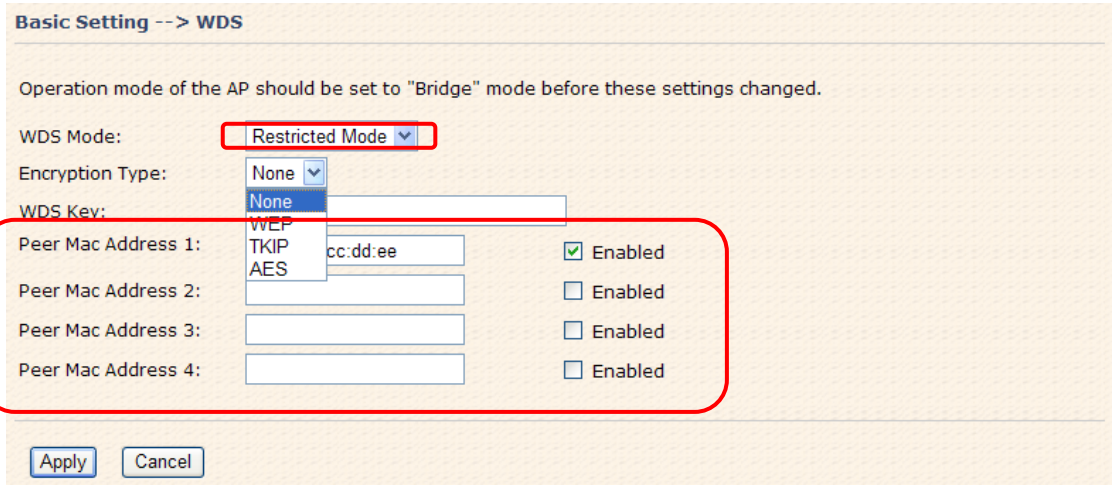
Label	Description
WDS Mode	This mode provides Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
Encryption Type	Select the type of security for your wireless network
WDS Key	Fill in the encryption key when Encryption Type is TKIP or AES.

Peer MAC Address	Set the Mac address(es) of other access point(s). Simultaneity, choose on “Enable”.

First of all, if APs link with WDS mode, it should obey the following rules:

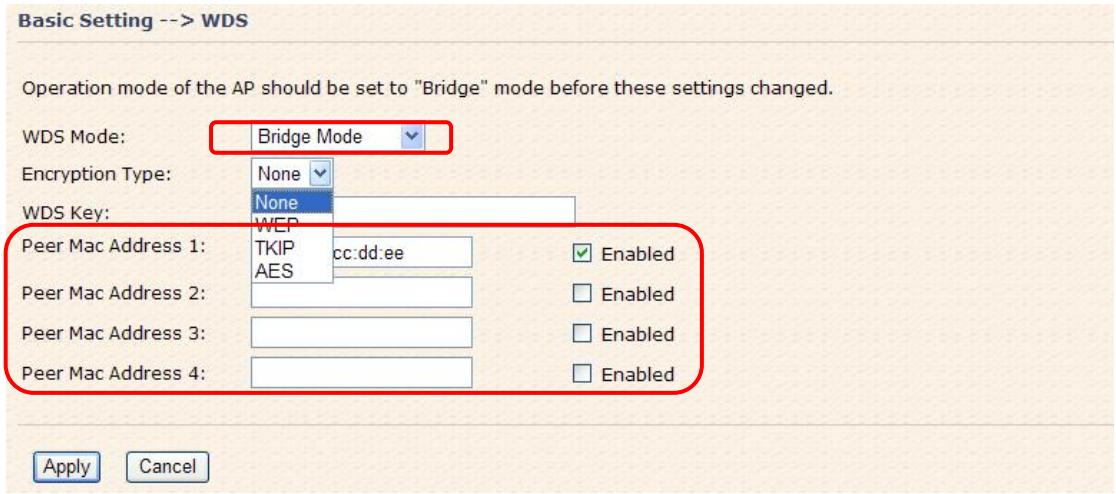
1. LAN IP Address should set different IP in the same network.
2. All AP’s DHCP Server should set shutdown.
3. WDS should set Enable.
4. Each AP should have the same setting except ‘Peer Mac Address’ set to the other’s Mac address
5. WEP Key and Channel should be the same, and each AP’s SSID should be broadcast to see in the other’s computer.
6. AP’s distance should limit to a certainty area.

WDS – Restricted Mode



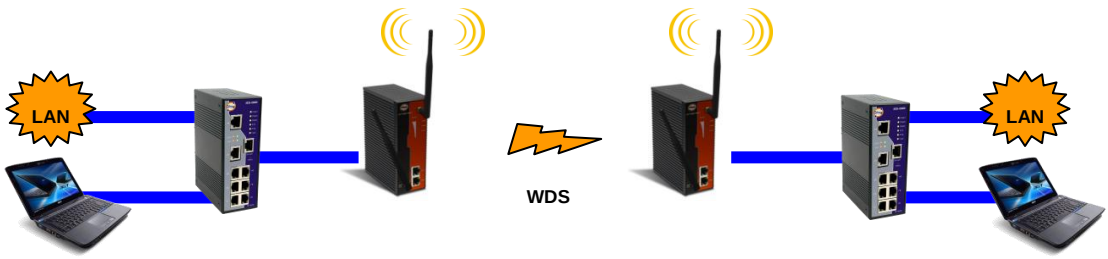
The peer WDS APs are according to the MAC address listed in "Peer Mac Address" fields.

WDS –Bridge Mode



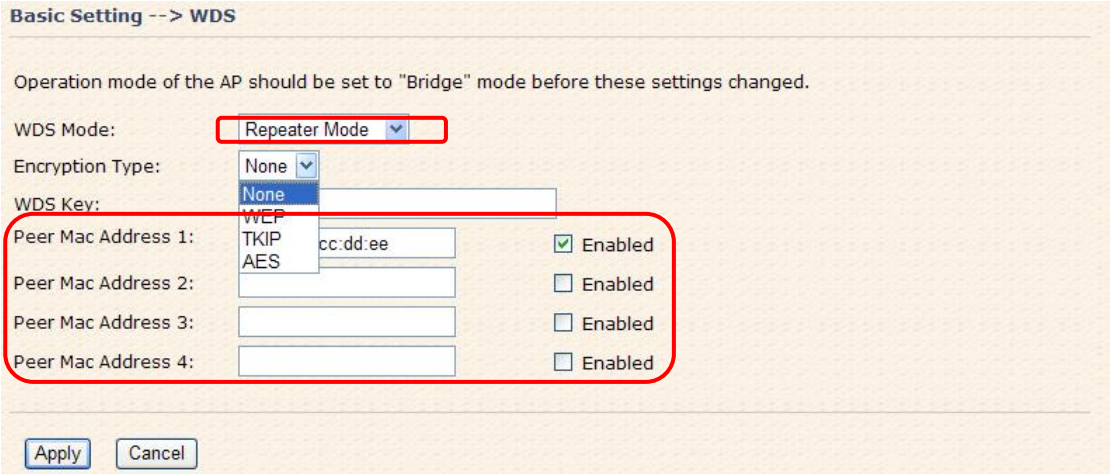
Same as Restrict mode in functionality and also one WDS link side can not set **Peer Mac Address 1-4.**

The working principle of **Bridge Mode** as follows:



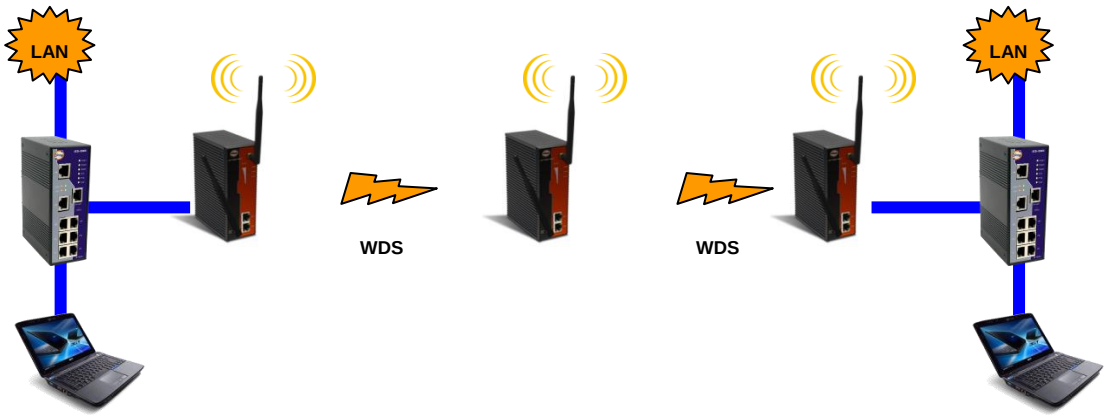
In the figure, the AP behaves as a standard bridge that forwards traffic between WDS links (links that connect to other AP/wireless bridges) and an Ethernet port. As a standard bridge, the AP learns MAC addresses of up to 64 wireless or 128 total wired and wireless network devices, which are connected to their respective Ethernet ports to limit the amount of data to be forwarded. Only data destined for stations which are known to reside on the peer Ethernet link, multicast data or data with unknown destinations need to be forwarded to the peer AP via the WDS link.

WDS –Repeater Mode



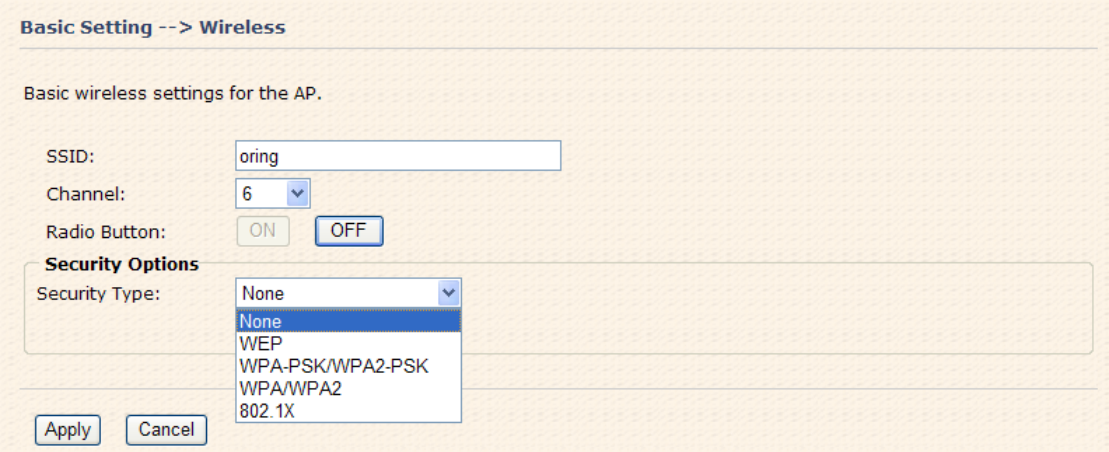
Same as Restrict mode in functionality and also one WDS link side can not set **Peer Mac Address 1-4.**

The working principle of **Repeater Mode** as follows:



In the figure, Repeater is used to extend the range of the wireless infrastructure by forwarding traffic between associated wireless stations and another repeater or AP connected to the wired LAN.

Setting Wireless



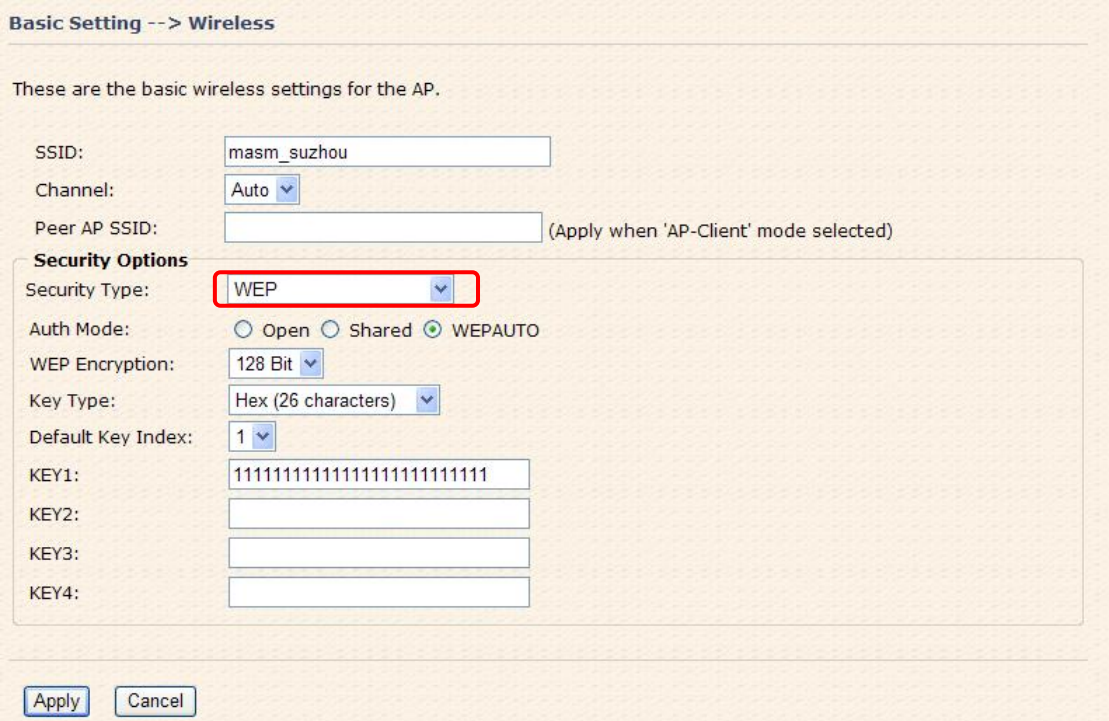
The following table describes the labels in this screen.

Label	Description
SSID	Service Set Identifier Default is the default setting. The SSID is a unique name that identifies a network. All devices on the network must share the same SSID name in order to communicate on the network. If you change the SSID from the default setting, input your new SSID name in this field.
Channel	Channel 6 is the default channel, input a new number if you want to change the default setting. All devices on the network must be set to the same channel to communicate on the network.
Peer AP SSID	Only Operation Mode selects AP-Client Mode, you should enter the peer AP SSID.
Security options	Select the type of security for your wireless network at **Security Type:** **None:** Select for no security. **WEP:** Select for security WEP. **WPA-PSK/WPA2-PSK:** Select for security WPA-PSK or WPA2-PSK without a RADIUS server. **WPA/WPA2:** Select for WPA or WPA2 (Wi-Fi Protected Access) authentication in conjunction with a RADIUS server. **802.1x:** Authentication through RADIUS server

Security Type – None

No security protection on your wireless LAN access.

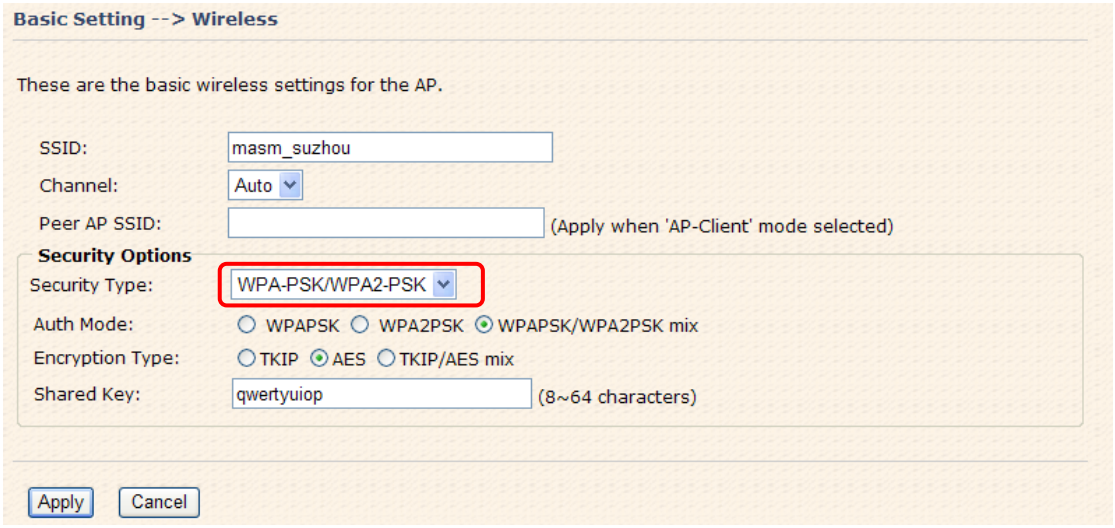
Security Type – WEP



1. Security Type: Select **WEP**
2. WEP Encryption: Select 64 Bit or 128 Bit WEP encryption.
3. Key Type: Select ASCII or Hex key type.
4. Default Key Index: Select one of the keys to be the active key.
5. Key 1-4: Input up to four encryption keys.

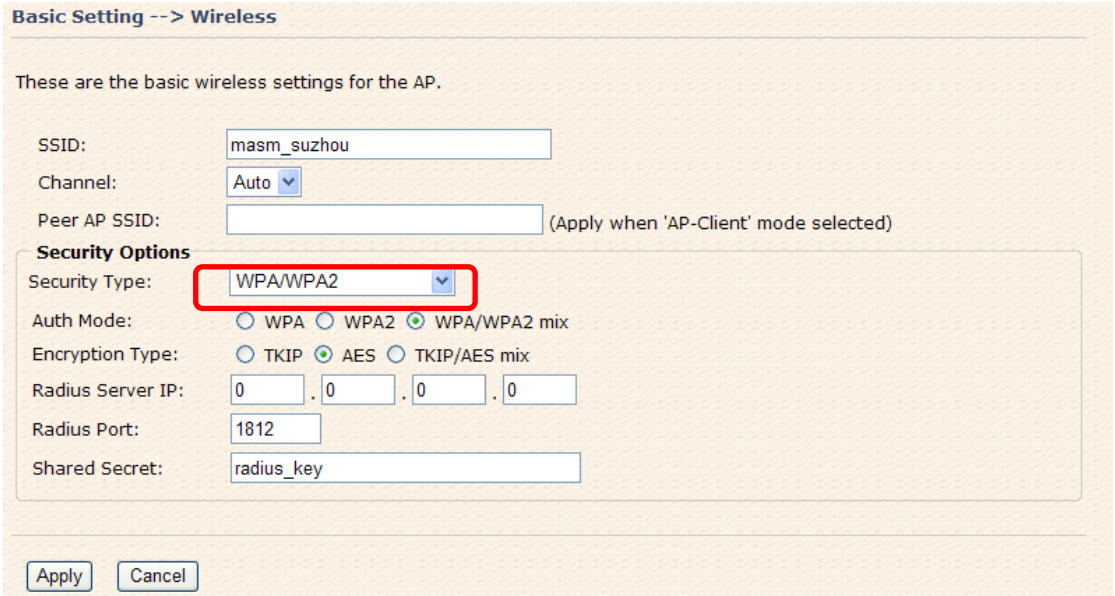
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. **Hex** digits consist of the numbers 0-9 and the letters A-F.

Security Type – WPA-PSK/WPA2-PSK



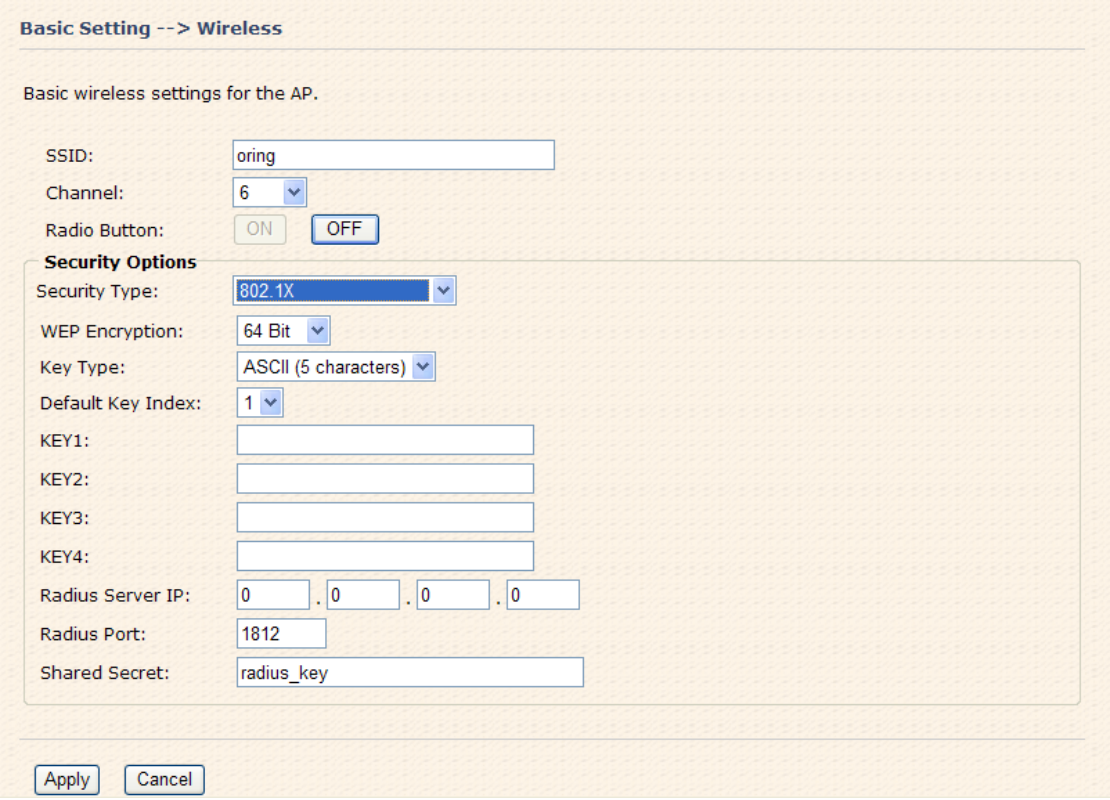
1. Security Type: Select **WPA-PSK/WPA2-PSK**.
2. Encryption Type: Select **TKIP** or **AES** encryption.
3. Share Key: Enter your password. The password can be between 8 and 64 characters.

Security Type – WPA /WPA2



1. Security Type: Select **WPA/WPA2**
2. Radius Server IP: Enter the IP address of the RADIUS Server.
3. Port: Enter the RADIUS port (1812 is default).
4. Shared Secret: Enter the RADIUS password or key.

Security Type – 802.1x

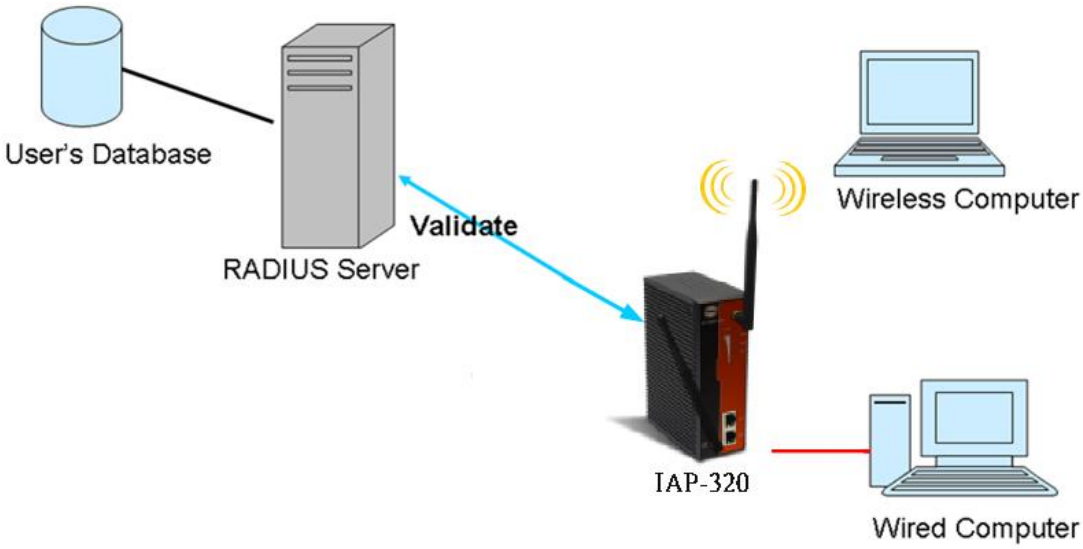


1. Security Type: Select **802.1x**
2. WEP Encryption: Select 64 Bit or 128 Bit WEP encryption.
3. Key Type: Select ASCII or Hex key type.
4. Default Key Index: Select one of the keys to be the active key.
5. Key 1-4: Input up to four encryption keys.
6. Radius Server IP: Enter the IP address of the RADIUS Server.
7. Port: Enter the RADIUS port (1812 is default).
8. Shared Secret: Enter the RADIUS password or key.

RADIUS (Remote Authentication Dial-in User Service) is the industrial standard agreement, and it is used to provide an identify verification. The Radius customer (is usually a dial-in server, VPN server or wireless point) send your proof and the conjunction parameter to the Radius server by Radius news. The Radius server validates the request of the Radius customer, and return Radius news to back.

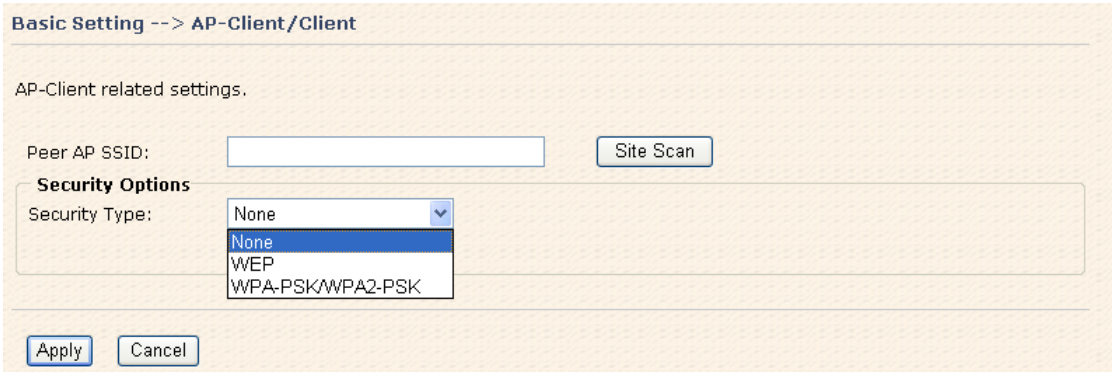
Radius server validates your proof, also carry on the authorization. So the Radius server received by ISA server responded (point out the customer carries proof to be not granted) and it means that the Radius server did not authorize you to carry. Even if the proof has already passed an identify verification, the ISA server may also refuse you to carry a claim according to the authorization strategy of the Radius server.

The principle of the Radius server shows in the following pictures:

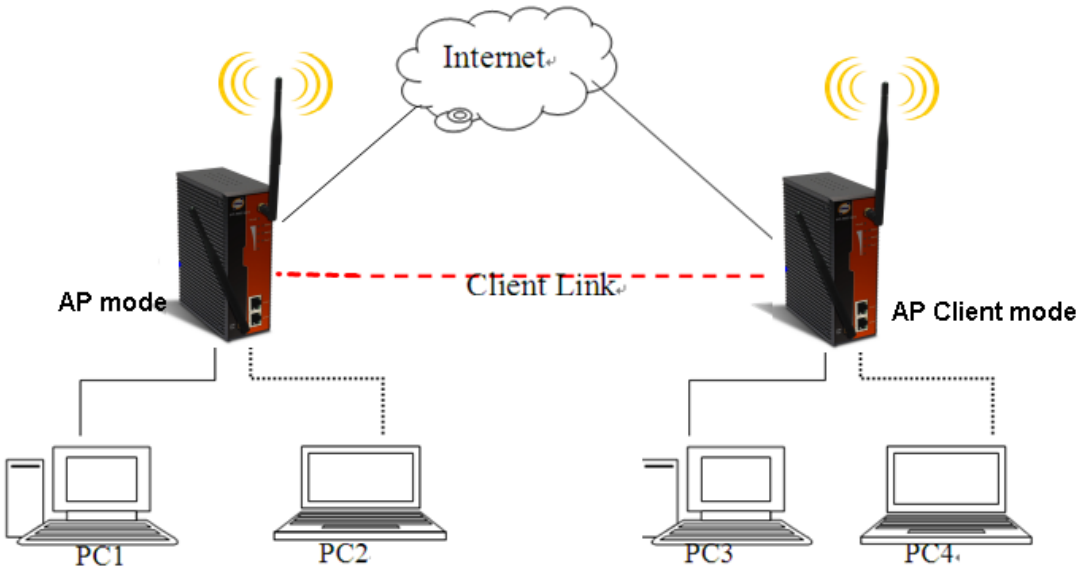


AP-Client/Client

The **Basic setting—>AP-Client/Client** page is mainly set the client which through the SSID and Security to connect to other AP. In this mode, the Security Type should be the same with the AP Server.



The principle of the AP-Client/Client mode shows in the following pictures:



Result:

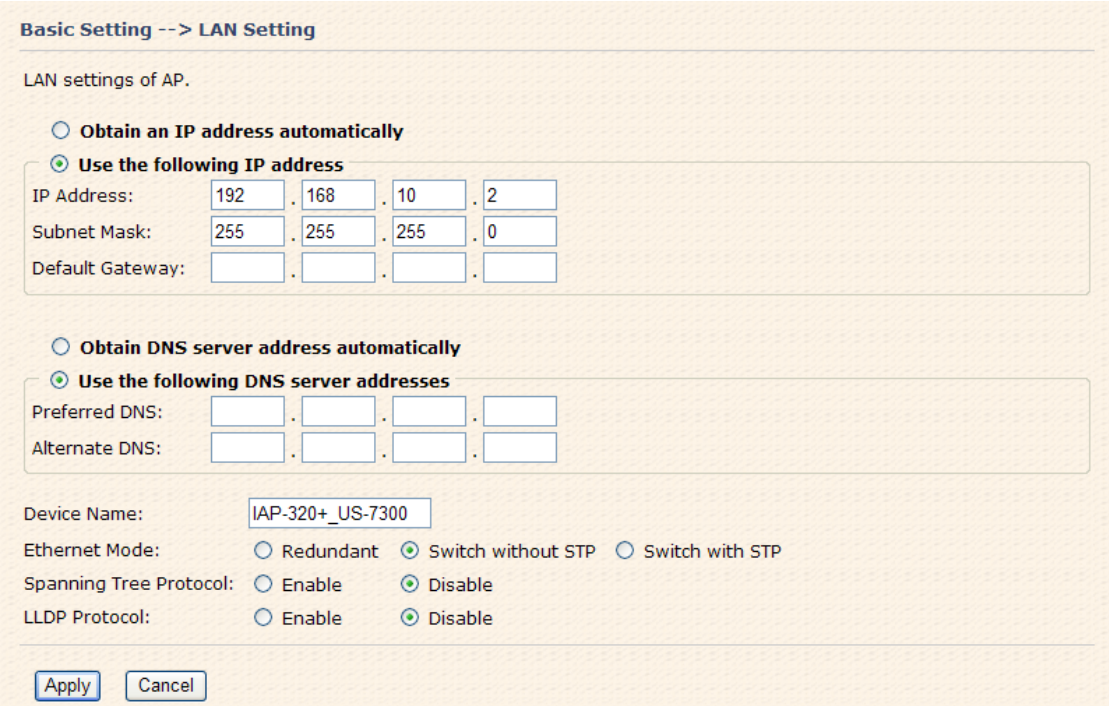
1. PC1, PC2 can visit PC3, PC4 and AP Client
2. PC3, PC4 can visit PC1, PC2 and AP
3. AP Client can visit AP

The following table describes the labels in this screen.

Label	Description
Peer AP SSID	Enter the other AP which used for AP mode.
Site Scan	You can scan the APs which used for AP mode in the certainty area
Security Type	Set the same security with the AP which you want to connect.

LAN Setting

The **Basic Setting > LAN Setting** page is mainly set IP address for LAN interface. To access the AP normally, a valid IP address of your LAN should be specified to the LAN interface. The default IP setting is DHCP server (Obtain an IP address automatically).

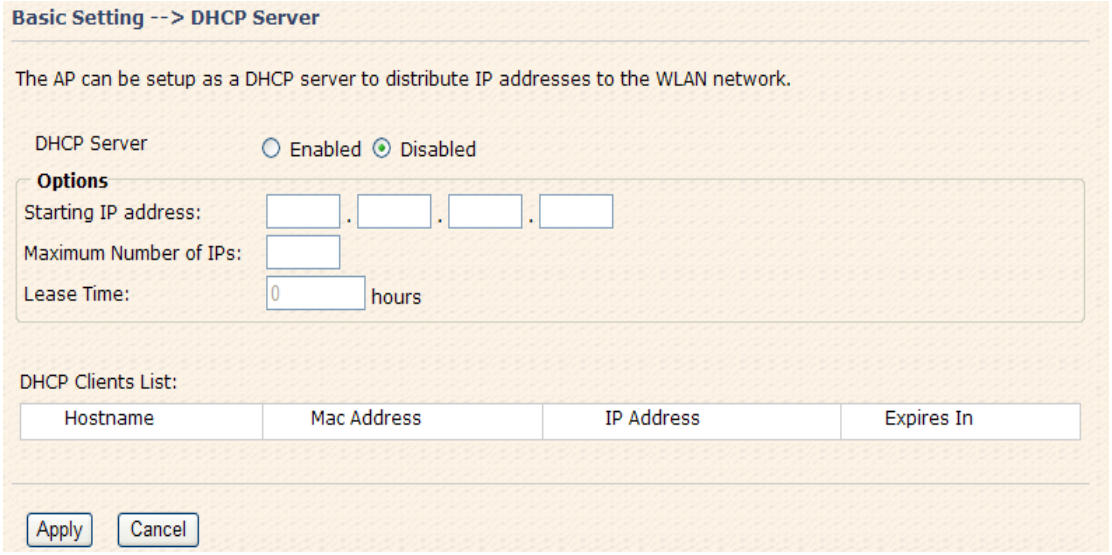


The following table describes the labels in this screen.

Label	Description
Obtain an IP address automatically	Select this option if you would like to have an IP address automatically assigned to the IWP-1000 by DHCP server in your network
Use the following IP address	Select this option if you are manually assigning an IP address. **IP Address:** There is a default IP address in the AP, and you can input a new IP address. **Subnet Mask:** 255.255.255.0 is the default Subnet Mask. All

	devices on the network must have the same subnet mask to communicate on the network. **Default Gateway:** Enter the IP address of the router in your network.
Obtain DNS server address automatically	This option is selected by DHCP server.
Use the following DNS server addresses	This option is selected by manually set **Preferred DNS:** There is a default DNS server, and you can input another new DNS server. **Alternate DNS:** There is a default DNS server, and you can input another new DNS server.

Setting DHCP Server

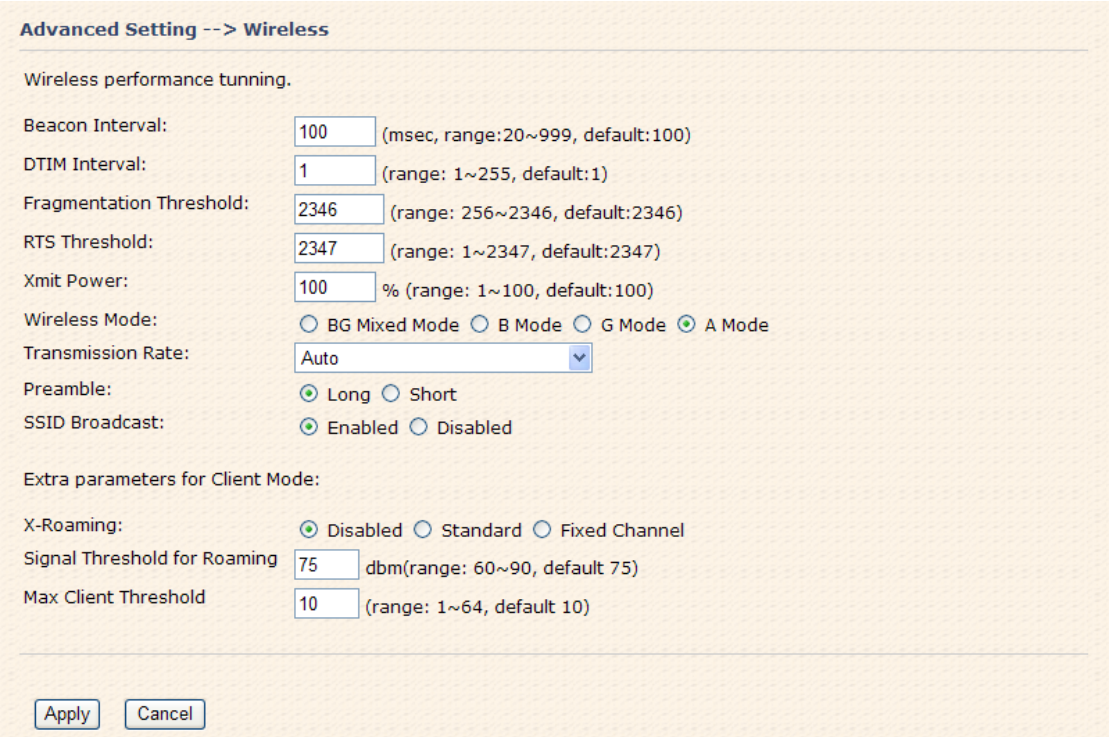


The following table describes the labels in this screen.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. Enable – the AP will be the DHCP server on your local network
Start IP Address	The dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. 192.168.1.100 will be the Start IP address.
Maximum Number of	The dynamic IP assign range. High IP address is the end of the

IPs	dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. **100** will be enter into textbox.
Lease Time (Hour)	It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
DHCP Clients List	List the devices on your network that are receiving dynamic IP addresses from the IWP-1000.

5.5.2 Advanced Setting
Wireless



The following table describes the labels in this screen.

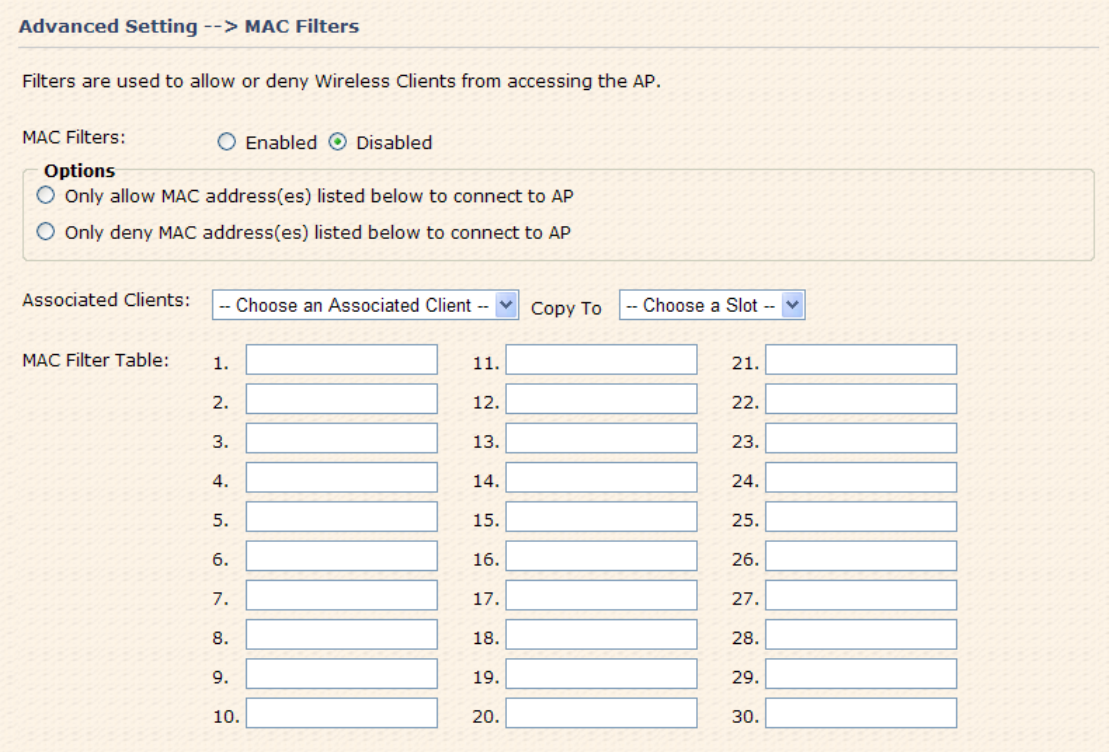
Label	Description
Beacon Interval	The default value is 100. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network. 50 is recommended in poor reception.
DTIM Interval	The default value is 1. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and

	multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
Fragmentation Threshold	This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The AP sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
Xmit Power	This value ranges from 1 - 100 percent, default value is 100 percent. A safe increase of up to 60 percent would be suitable for most users. Higher power settings are not recommended for users due to excess heat generated by the radio chipset, which can affect the life of the AP.
Wireless Network Mode	If you have Wireless-G and 802.11b devices in your network, then keep the default setting, BG Mixed mode. If you have only Wireless-G devices, select G Mode. If you would like to limit your network to only 802.11b devices, then select B Mode. If you would like to use 802.11a devices then select A only mode.
Transmission Rate	The default setting is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, Auto, to have the AP automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client.

Preamble	Values are Long and Short, default value is Long. If your wireless device supports the short preamble and you are having trouble getting it to communicate with other 802.11b devices, make sure that it is set to use the long preamble
SSID Broadcast	When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the AP. To broadcast the AP SSID, keep the default setting, Enable. If you do not want to broadcast the AP SSID, then select Disable.
X-Roaming	**Disable:** Disable X-Roaming protocol. **Standard:** Roaming group does not require the same wireless channel, but slower to switch than the “fixed channel” mode **Fixed channel:** Roaming group must be required the same wireless channel, but faster to switch than the “Standard” mode
Signal Threshold for Roaming	Roaming signal threshold setting. When signal below this value AP will roaming to another client target which the same SSID, security option and signal strongest within the environment.(This value just effect on client-mode equipment)
Max Client Threshold	Max number of client equipment setting. When client number over this value AP will reject roaming equipment connection.(This value just effect on AP-mode equipment)

MAC Filter

Use **Advanced Setting > MAC Filters** to allow or deny wireless clients, by their MAC addresses, from accessing the IWP-1000. You can manually add a MAC address or select the MAC address from **Connected Clients** that are currently connected to the AP.

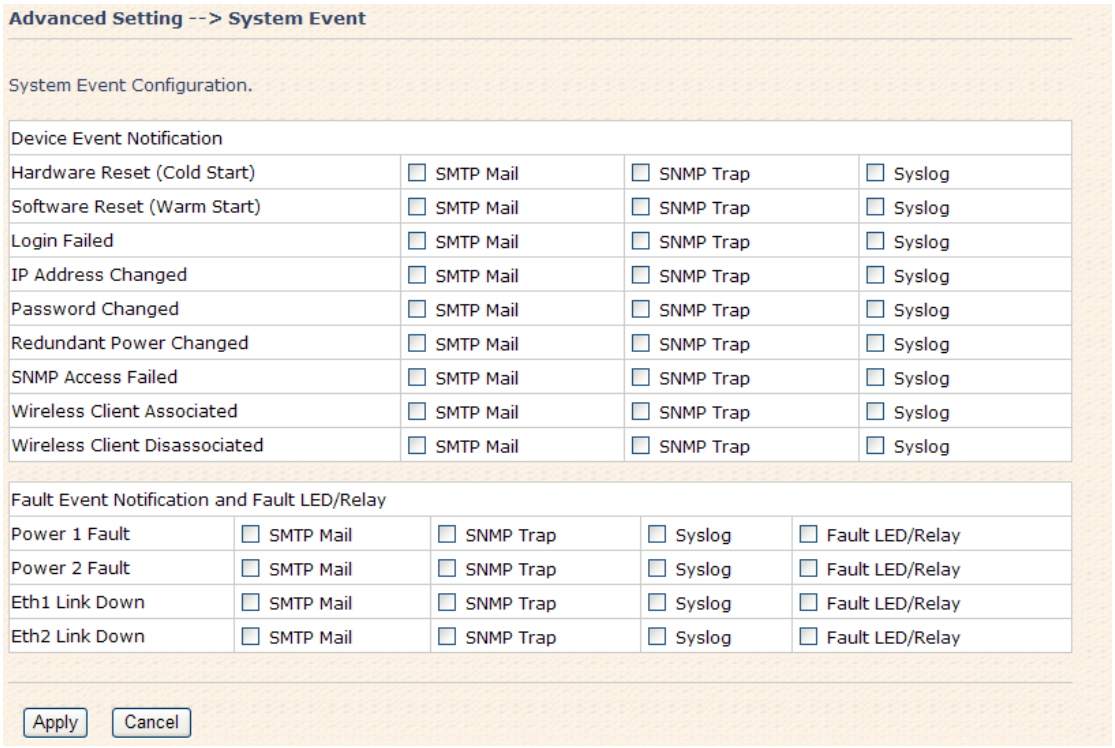


The following table describes the labels in this screen.

Label	Description
MAC Filter	Enable or disable the function of MAC filter. MAC address allowed or denied option is selected by you.
MAC Filter List	This list will display the MAC addresses that are in the selected filter.
Connected Clients	This list will display the wireless MAC addresses that linked with AP.
MAC Address	MAC addresses need to be added to or clear from MAC filter list.
Apply	Click Apply to set the configurations.

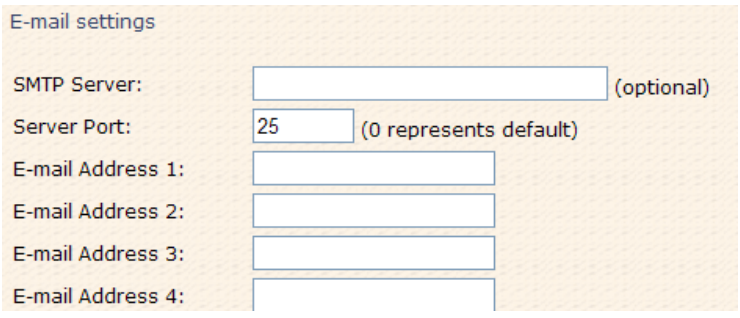
System Event

When the AP event triggered, the notification procedure will be performed according to the type of the event. Which notification would be performed depends on the selection of corresponding option in the **Advanced Setting > System Event** page.



System events record the activities of the AP system. When the setting changes or action performs, the event will be sent to administrator by email. A trap will also be sent to SNMP server. The Syslog will record the event locally and may send the log remotely to a Syslog server. If serious event occurred, such as the power failure or link down, the fault LED will be switched on as warning.

Email Settings

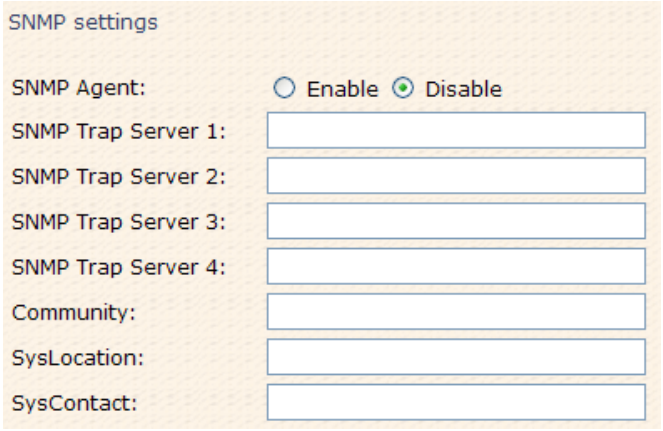


The following table describes the labels in this screen.

Label	Description
SMTP Server	Simple Message Transfer Protocol, enter the backup host to use if primary host is unavailable while sending mail by SMTP server.

Server Port	Specify the port where MTA can be contacted via SMTP server.
E-mail Address 1-4	Inputs specify the destination mail address.

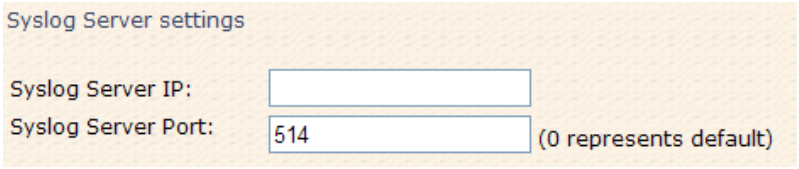
SNMP Settings



The following table describes the labels in this screen.

Label	Description
SNMP Agent	SNMP (Simple Network Management Protocol) Agent is a service program that runs on the access point. The agent provides management information to the NMS by keeping track of various operational aspects of the AP system. Turn on to open this service and off to shutdown it.
SNMP Trap Server 1-4	Specify the IP of trap server, which is the address to which it will send traps AP generates.
Community	Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-write community.
SysLocation	Specify sysLocation string.
SysContact	Specify sysContact string.

Syslog Server Settings



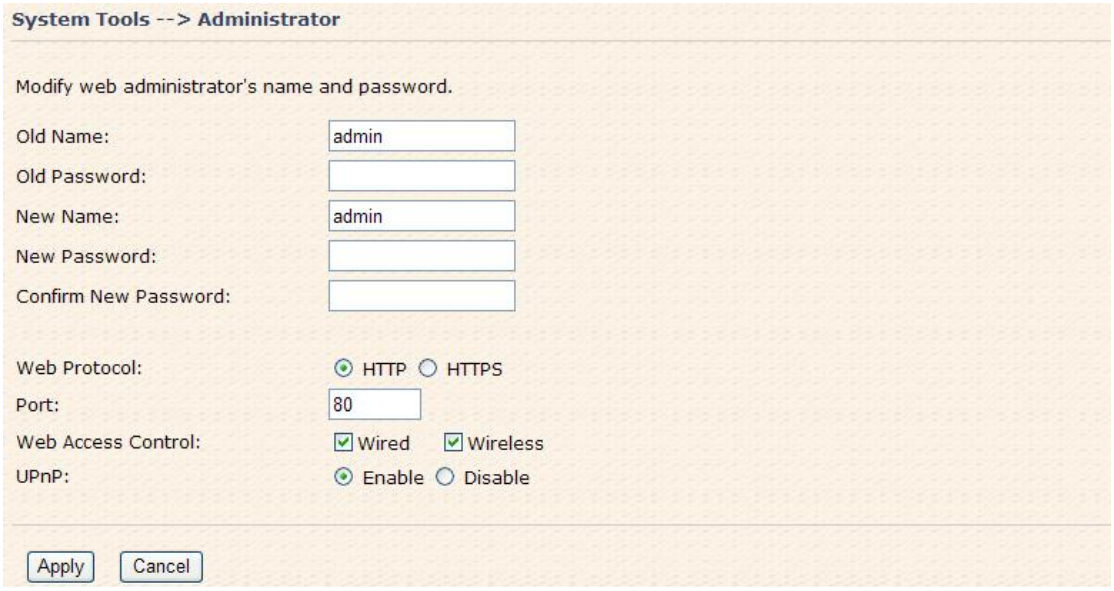
The following table describes the labels in this screen.

Label	Description
Syslog Server IP	Not only the syslog keeps the logs locally, it can also log to remote server. Specify the IP of remote server. Leave it blank to disable logging remotely.
Syslog Server Port	Specify the port of remote logging. Default port is 514.

5.5.3 System Tools

Administrator

In this page, you can change the username and password. The new password must be typed twice to confirm (the default Name and Password is "**admin**" and "").



The following table describes the labels in this screen.

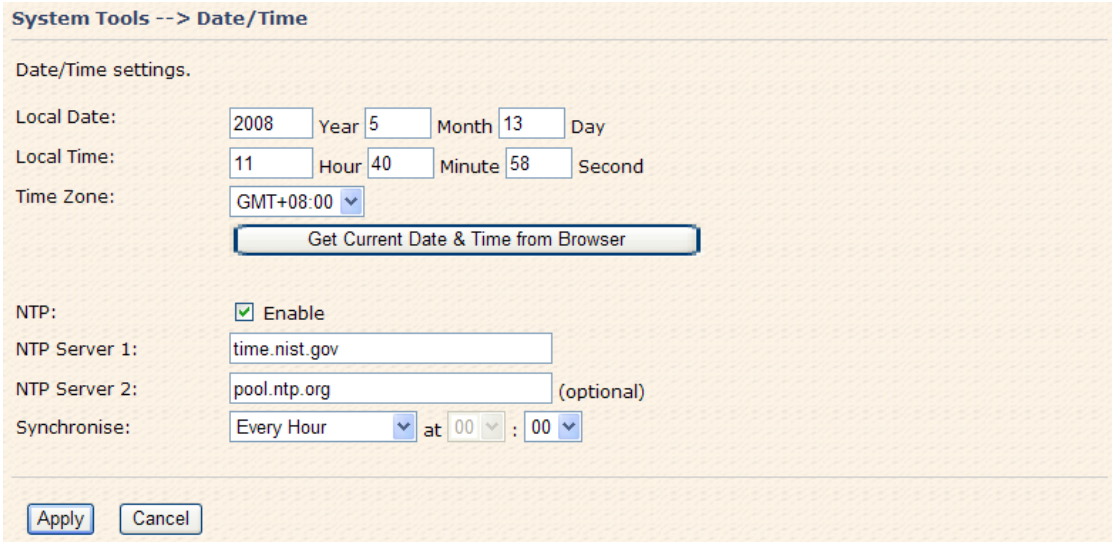
Label	Description
Old Name	This field displays the old login name. It's read only. The default value of login name is "admin".
Old Password	Before making a new setting, you should provide the old password for a verify check. Acceptable inputs of this field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length. The factory default value of login password is null.
New Name	Enter a new login name. Acceptable inputs of this field contains

	'0-9', 'a-z', 'A-Z' and must be between 1 to 15 characters in length. This field can not accept null input.
New Password	Enter a new login password. Acceptable inputs of this field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length.
Confirm New Password	Retype the password to confirm it. Acceptable inputs of this field contains '0-9', 'a-z', 'A-Z' and must be between 0 to 15 characters in length.
Web Protocol	Choose on the protocol for web. The default value is **HTTP**, if you want the web pages' security is better, choose the **HTTPS** protocol.
Port	Corresponding to the Web protocol, there is a default port (HTTP: 80, HTTPS: 443). And you can enter another number which should be in range of 1-65535.
Web Access Control	Choose the checkbox of the Wired and Wireless; you can visit the web page through the mode you choose.
UPnP	Pitch on "Enable", and the UPnP will display in the right-behind corner.

HTTPS (HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

Date & Time

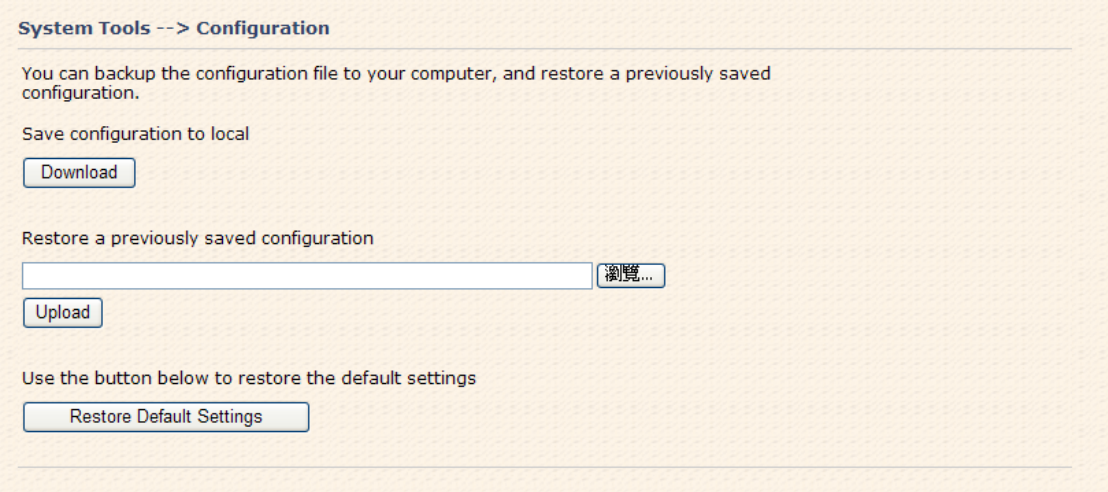
In this page, set the date & time of the device. The correct date & time will be helpful for logging of system events. A NTP (Network Time Protocol) client can be used to synchronize date & time with NTP server.



The following table describes the labels in this screen.

Label	Description
Local Date	Set local date manually.
Local Time	Set local time manually.
Time Zone	Select the time zone manually
Get Current Date & Time from Browser	Click this button; you can set the time from browser.
NTP	Enable or disable NTP function to get the time from the NTP server.
NTP Server 1	The initial choice about NTP Server.
NTP Server 2	The second choice about NTP Server.
Synchronize	Set the time, and the AP's time synchronize with the NTP Server at the time

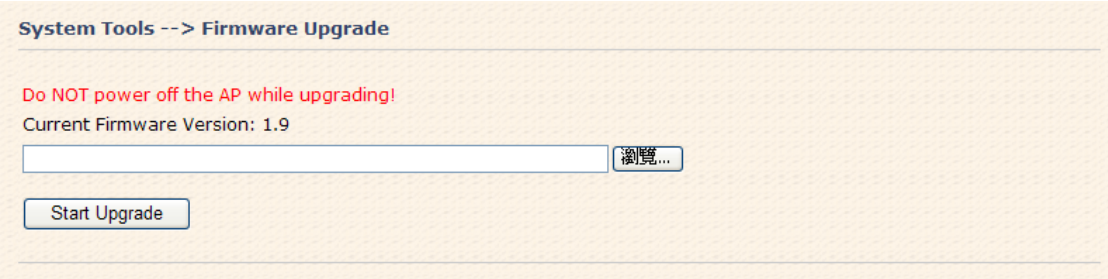
Configuration



The following table describes the labels in this screen.

Label	Description
Download configuration	The current system settings can be saved as a file onto the local hard drive.
Upload configuration	The saved file or any other saved setting file can be uploaded back on the AP. To reload a system settings file, click on **Browse** to browse the local hard drive and locate the system file to be used. Click **Upload** when you have selected the file to be loaded back onto the AP.
Restore Default Settings	You may also reset the IWP-1000 back to factory settings by clicking on **Restore Default Settings**. Make sure to save the unit's settings before clicking on this button. You will lose your current settings when you click this button.

Firmware Upgrade



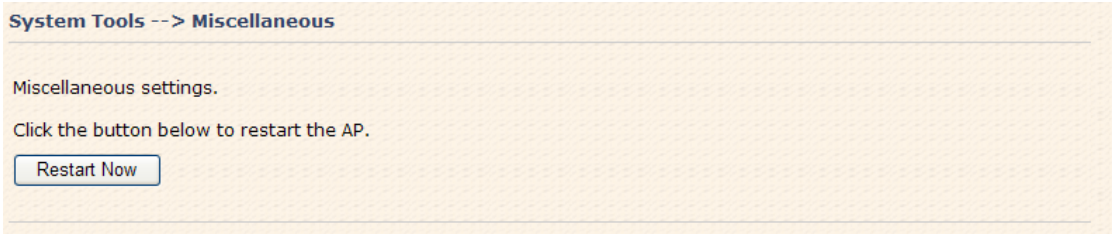
New firmware may provide better performance, bug fixes or more functions. To upgrade, you need a firmware file correspond to this AP model. It will take several

minutes to upload and upgrade the firmware. After the upgrade is done successfully, the access point will reboot and get revalidated.

Notice: DO NOT POWER OFF THE AP OR PRESS THE RESET BUTTON WHILE THE FIRMWARE IS BEING UPGRADED.

Miscellaneous

If you want restart the access point through the **Warm Reset**, click **Restart Now** to restart the AP.

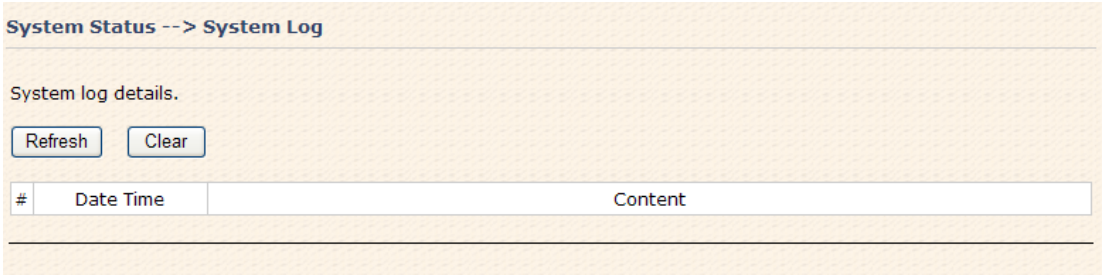


5.5.4 System Status

System Info

This page displays the current information for the IWP-1000. It will display model name, as well as firmware version, Ethernet, Wireless info and device time.

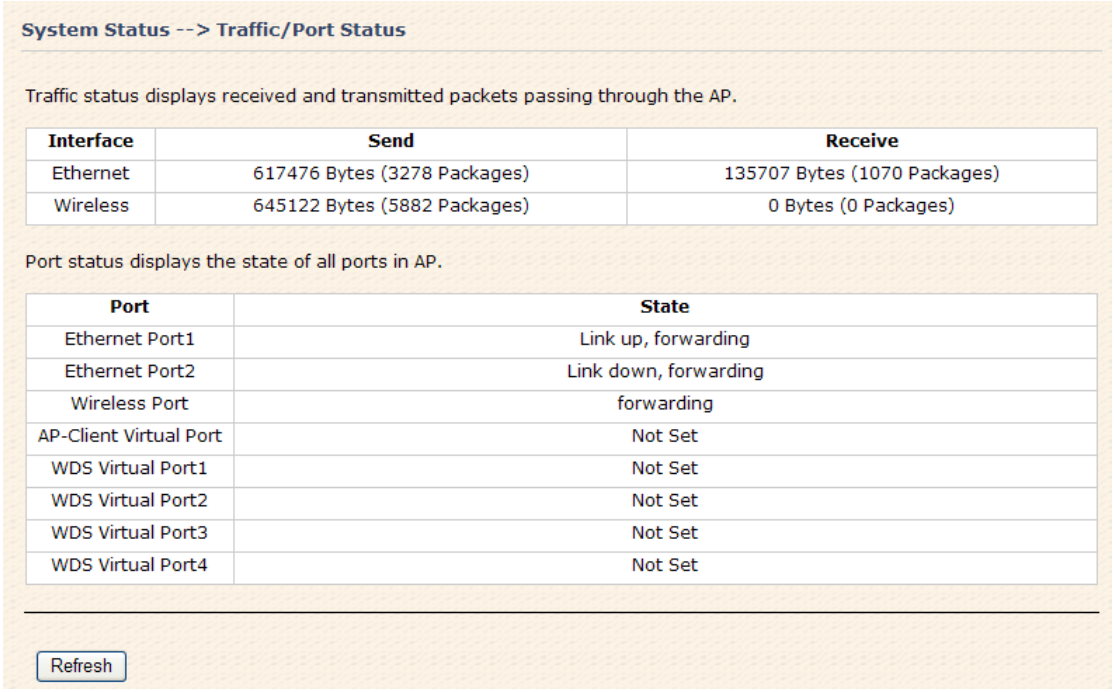
System Log



The system log tracks the important events and setting changes of the AP. If the AP is rebooted, the logs are automatically cleared.

Click the button '**Refresh**' to refresh the page; Click the button '**Clear**' to clear log entries.

Traffic Statistics



System Status --> Traffic/Port Status

Traffic status displays received and transmitted packets passing through the AP.

Interface	Send	Receive
Ethernet	617476 Bytes (3278 Packages)	135707 Bytes (1070 Packages)
Wireless	645122 Bytes (5882 Packages)	0 Bytes (0 Packages)

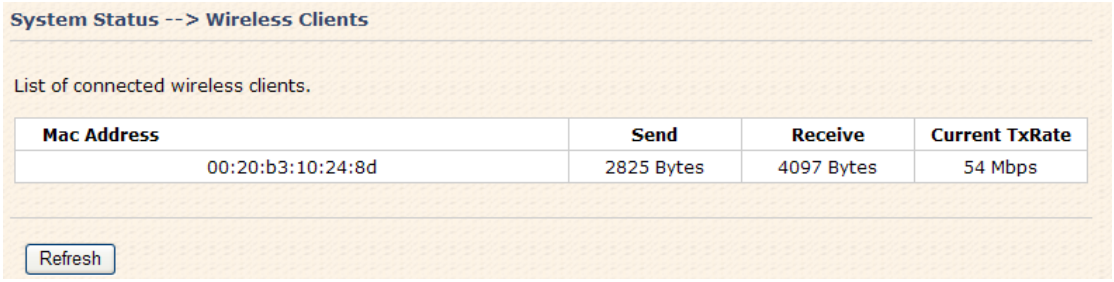
Port status displays the state of all ports in AP.

Port	State
Ethernet Port1	Link up, forwarding
Ethernet Port2	Link down, forwarding
Wireless Port	forwarding
AP-Client Virtual Port	Not Set
WDS Virtual Port1	Not Set
WDS Virtual Port2	Not Set
WDS Virtual Port3	Not Set
WDS Virtual Port4	Not Set

Refresh

This page displays the network traffic statistics for both received and transmitted packets through the Ethernet port and wireless connections associated with the AP. Simultaneity, the traffic counter will reset by the device rebooting.

Wireless Clients



System Status --> Wireless Clients

List of connected wireless clients.

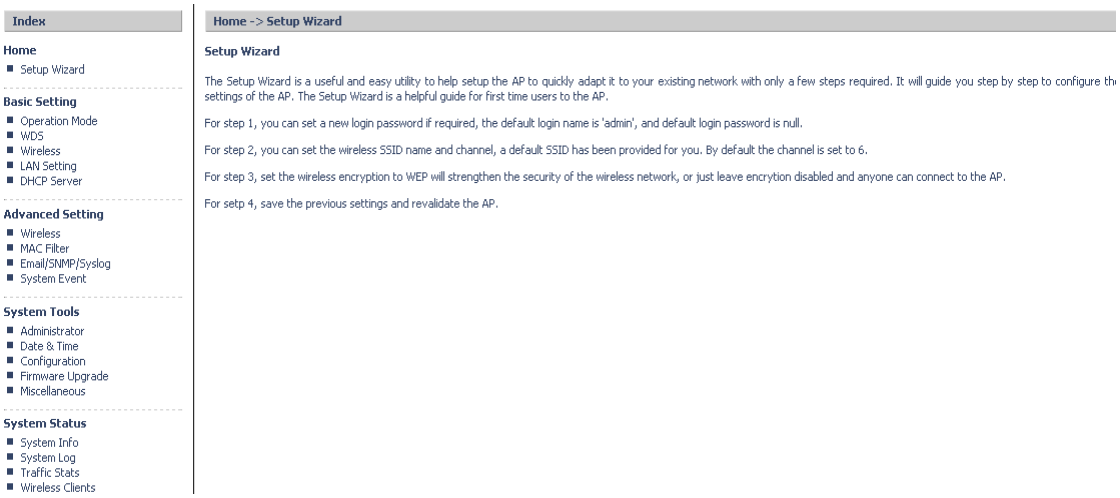
Mac Address	Send	Receive	Current TxRate
00:20:b3:10:24:8d	2825 Bytes	4097 Bytes	54 Mbps

Refresh

This page of the list displays the **Mac Address** of the wireless clients connected. **Current TX Rate** is corresponding to the **Transmission Rate** in the **Advanced Setting > Wireless** pages.

5.5.5 Online Help

Click on any item in the **Online Help** screen for more information.



Technical Specifications

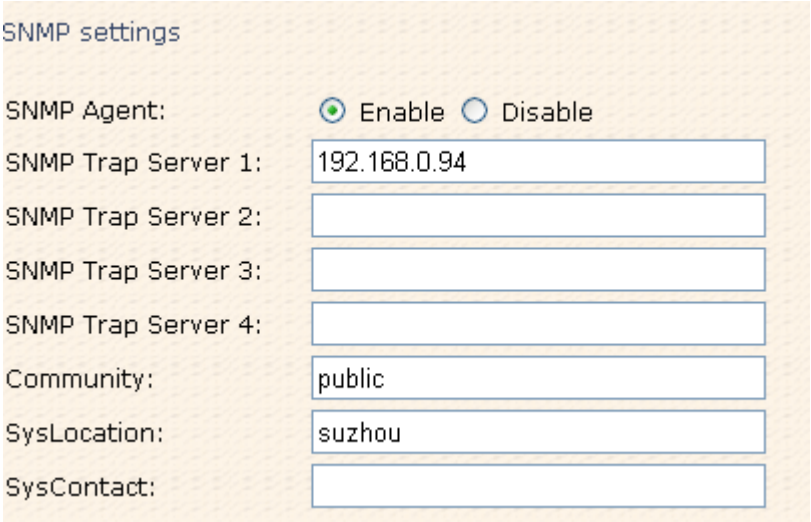
LAN Interface	
RJ45 Ports	2 x 10/100Base-T(X), Auto MDI/MDI-X
PoE P.D. (Power Device)	Present at ETH2 of IAP-320+ ETH2 act as Power Device (IEEE802.3af): IEEE 802.3af compliant input interface Power consumption: 8Watts max. Over load & short circuit protection Isolation Voltage: 1000 VDC min. Isolation Resistance: 10^8 ohms min
Protocols	IP, TCP, UDP, DHCP, BOOTP, ARP/RARP, DNS, SNMP MIB II, HTTPS, SNMPV1/V2, Trap, Private MIB
WLAN Interface	
Operating Mode	AP/Bridge/Repeater/AP-Client/Client
Antenna Connector	Reverse SMA
Radio Frequency Type	DSSS
Modulation	IEEE802.11b: CCK, DQPSK, DBPSK IEEE802.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM
Frequency Band	(US)America/FCC: 2.412~2.462 GHz (11channels) (EU)Europe CE/ETSI: 2.412~2.472 GHz (13channels) (JP)Japan:2.412~2.484 GHz (13Channels)
Transmission Rate	IEEE802.11b: 1/2/5.5/11 Mbps IEEE802.11g: 6/9/12/18/24/36/48/54 Mbps
Transmit Power	IEEE802.11b/g: 20dBm
Receiver Sensitivity	-81dBm@11Mbps, PER< 8%; -64dBm@54Mbps, PER< 10%
Encryption Security	WEP: (64-bit, 128-bit key supported) WPA: WPA2:802.11i (WEP and AES encryption) PSK (256-bit key pre-shared key supported) TKIP encryption
Wireless Security	SSID broadcast disable

LED Indicators	PWR 1(2) (PoE, IAP-320+) / Ready: 1) Red On: Power is on and booting up. 2) Green On: Power is on and functioning normally. ETH1 (2) Link / ACT: Orange ON/Blinking: 10 Mbps Ethernet Green ON/Blinking: 100 Mbps Ethernet WLAN Link/ACT: Green WLAN Strength:1<25%, 2<50%, 3<75%, 4<100% Fault: Power or LAN link down (Red)
Power Requirements	
Power Input Voltage	Dual power inputs PWR1/2: 12 ~ 48VDC in 6-pin Terminal Block
Reverse Polarity Protection	Present
Power Consumption	6 Watts
Environmental	
Operating Temperature	-10 to 55^{o}C
Storage Temperature	-40 to 85^{o}C
Operating Humidity	5% to 95%, non-condensing
Mechanical	
Dimensions(W x D x H)	52 mm(W)x 106 mm(D)x 144 mm(H)
Casing	IP-30 protection
Regulatory Approvals	
Regulatory Approvals	FCC Part 15, CISPER (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS)
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Warranty	3 years

APPENDIX A

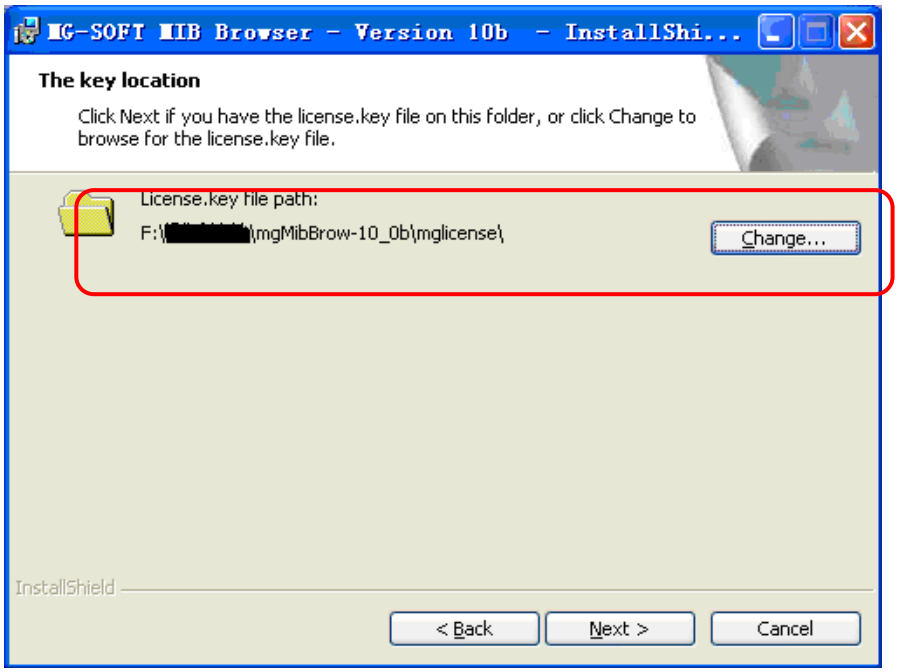
How to configure SNMP MIB and use SNMP in the PCs?

Step 1, Set Enable about the SNMP inn the web of Advanced Setting→Email/SNMP/Syslog, and input the IP address of the PC used for SNMP trap server.

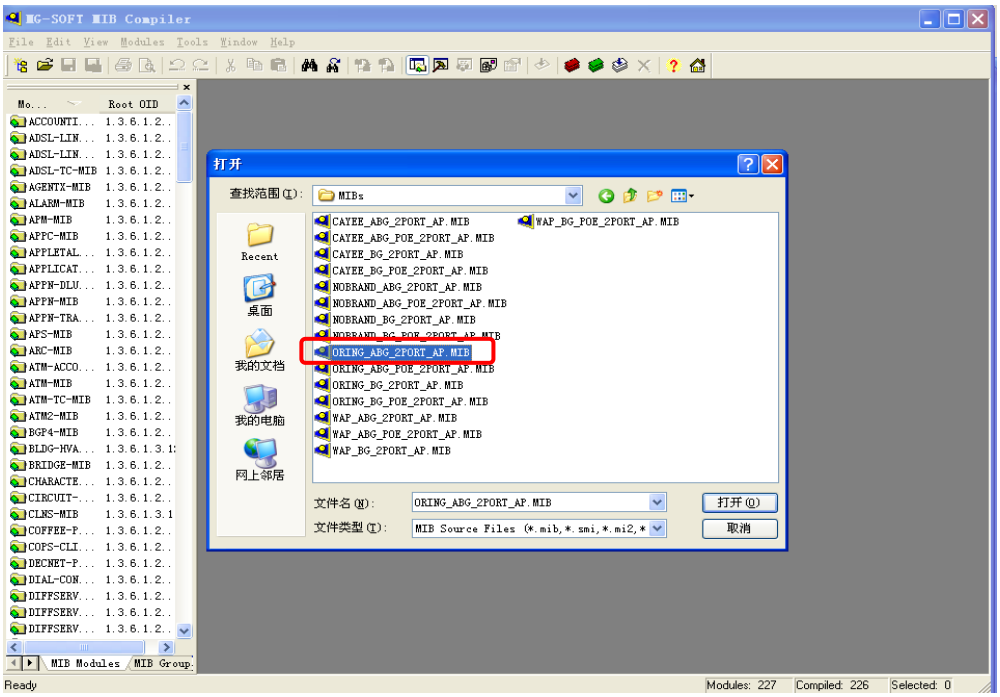


Step 2, In the PC, you should setup the SNMP trap server. This here, we use MG-SOFT for example.

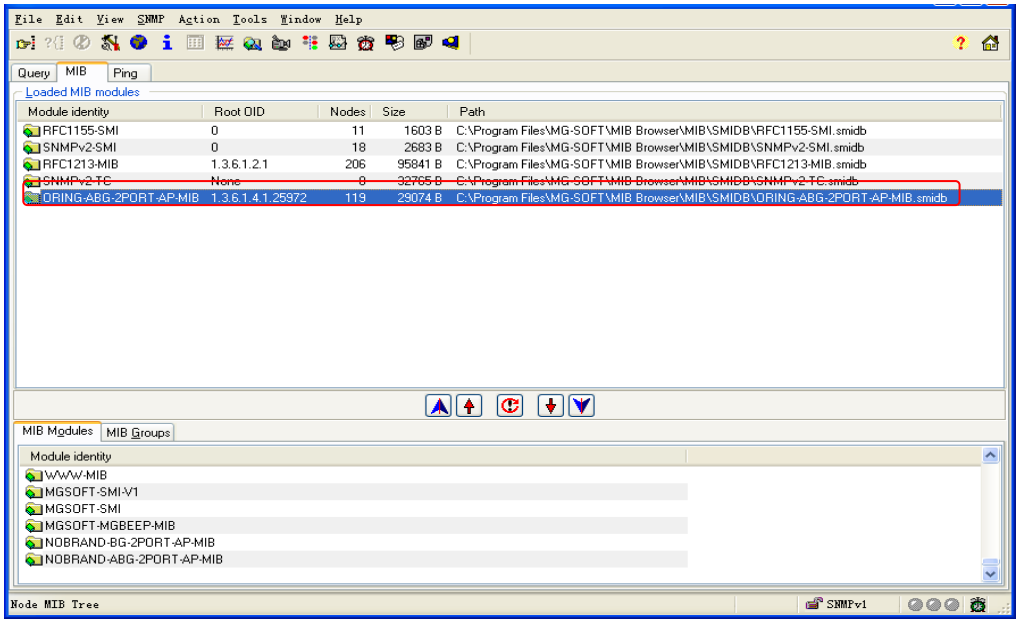
1. The location of the License should configure right during the process of the installation.



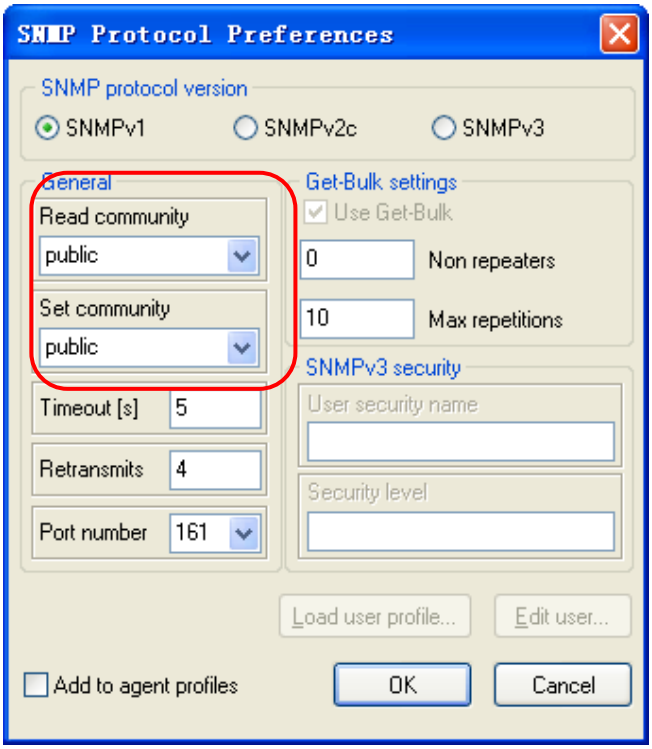
2. After the installation, click into MIB Compile to add the MIB files(for example, the Oring 802.11a/b/g and no PoE FW), and save the configuration.



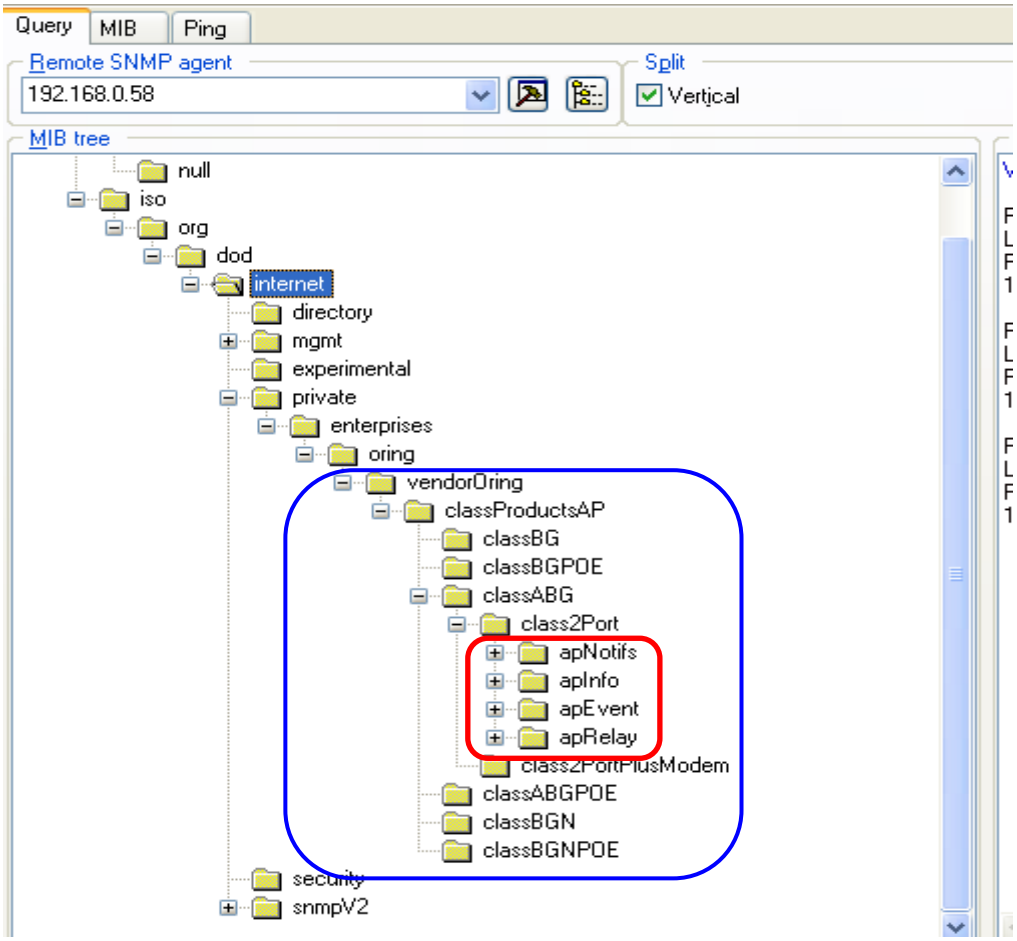
3. Open MIB Brower and select the list of MIB, then select the ORING-ABG-2Port-AP-MIB which in the MIB Modules to add in the Loaded MIB modules.



4. Click into Query list in the MIB Brower, and input the IP address of the AP in the Remote SNMP agent→ click “Apply”, there is an alarm box which let you enter the right community.

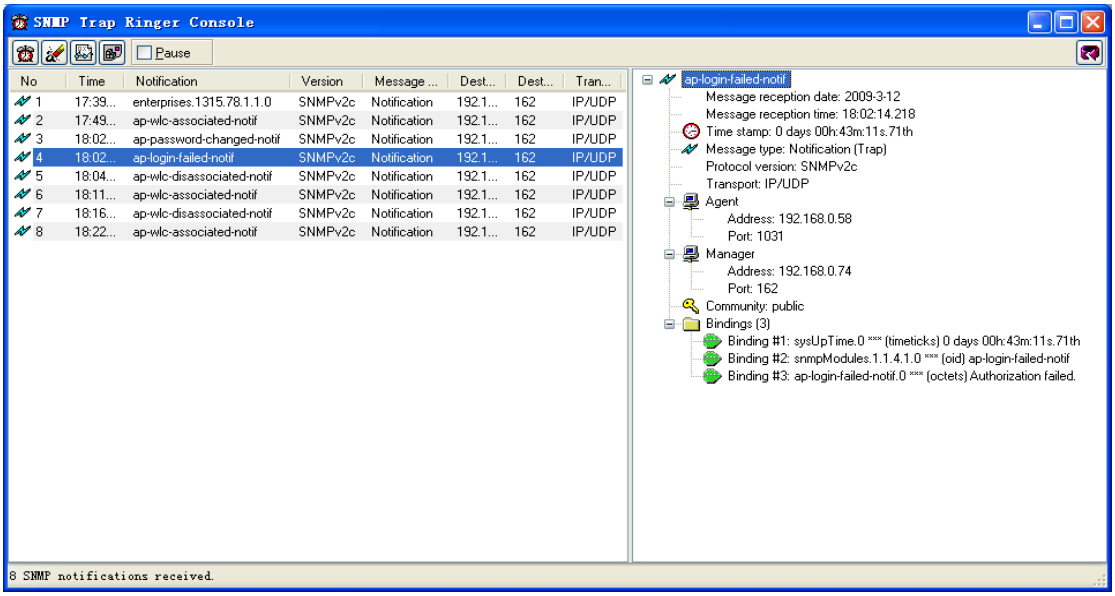


5. After all the settings, you can see the information about the Oring AP in the MIB Tree.



Step 3, Be familiar with SNMP information

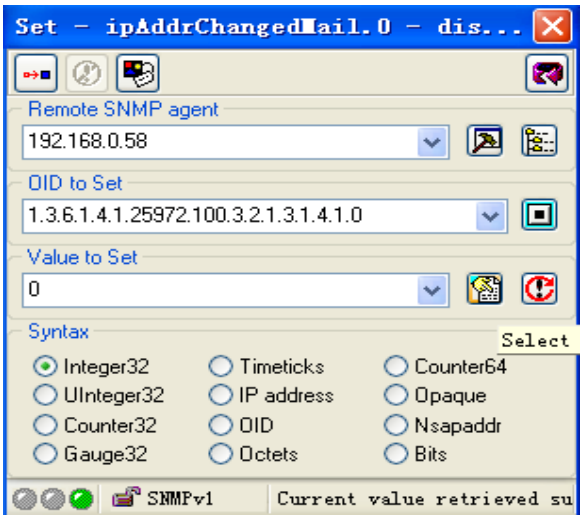
1. The **apNotifs** list will show the trap box. To modify password as an example→ select the SNMP Trap option in the **Advanced Setting→System Event** page→ modify the password in the page of Administrator→ it will be have trap box in the SNMP.



2. The apInfo shows the basic information of the AP. To apSignalStrengthInfo as an example, right-click select "Get" on access to the Signal Strength information.

Shows in SNMP：	Shows in the web page
Response binding: 1: apSignalStrengthInfo.0 (octet string) 100 [31.30.30 (hex)]	Signal Strength: 100%

3. The apEvent shows the same content with the page of the System Event and you can also configure the options. To PAddrChangedMail in the ipAddrChanged for example→now. status is in selected and the SNMP value is 1→ Set the SNMP value to 0, then the web page will be not selected.



4. Also have the relevant information, you can right-click “Properties” to view a specific property features.