
# IGAP-420/620 Series

# IGAP-6620 Series

## IEEE 802.11 b/g/n Access Point

## IEEE 802.11 a/b/g/n Access Point

## IEEE802.11 a/b/g/n Dual RF Access Point

www.oring-networking.com

## COPYRIGHT NOTICE



## TRADEMARKS

 is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

## REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

## WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

## DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

## CONTACT INFORMATION

**ORing Industrial Networking Corp.**

3F., No.542-2, Zhongzheng Rd., Xindian Dist., New Taipei City 23148, Taiwan (R.O.C.)
Tel: +886-2-2218-1066 // Fax: +886-2-2218-1014
Website: www.oring-networking.com

**Technical Support**

E-mail: support@oring-networking.com

**Sales Contact**

E-mail: sales@oring-networking.com (Headquarters)
sales@oring-networking.com.cn (China)

# Table of Content

# Getting to Know Your Access Point

## 1.1 About the ORing Access Point

IGAP-420/620/6620 is reliable IEEE802.11b/g/n; IEEE802.11 a/b/g/n WLAN with 2 ports LAN Access Point. It can be configured to operate in AP/Client/Bridge/AP-Client mode. You can configure IGAP-420/620/6620 by Window Utility or WEB interfaces via LAN port or WLAN interface. IGAP-420/620/6620 provides dual Ethernet ports, so you can use Daisy Chain to reduce the usage of Ethernet switch ports. Therefore, IGAP-420/620/6620 is one of the best communication solutions for wireless application.

## 1.2 Software Features

- High Speed Air Connectivity: WLAN interface support up to 300Mbps link speed connection
- Highly Security Capability: WEP/WPA/WPA2/Radius/TKIP supported
- Support AP/Client/Bridge/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

## 1.3 Hardware Features

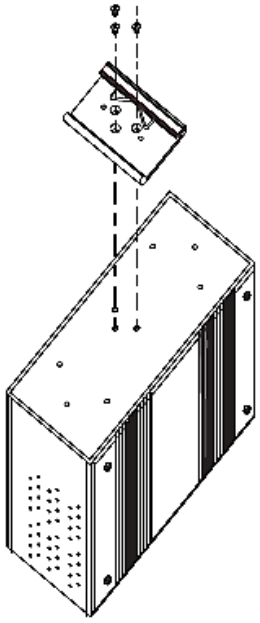
- Redundant Power Inputs: Dual 12~48 VDC
- 10/100/1000 Base-T(X) Ethernet port
- Casing: IP-30
- Dimensions(W x D x H) : 74.3(W) x 109.2(D) x 153.6(H) mm
- Operating Temperature: -10 to 60$^{o}$C
- Storage Temperature: -40 to 85$^{o}$C
- Operating Humidity: 5% to 95%, non-condensing

# Hardware Installation

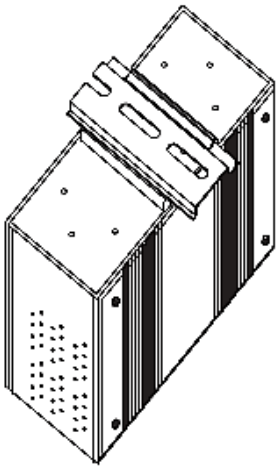
## 2.1 Installation device on Din-Rail

Each device has a DIN-Rail kit on rear panel. The DIN-Rail kit helps device to fix on the DIN-Rail.

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



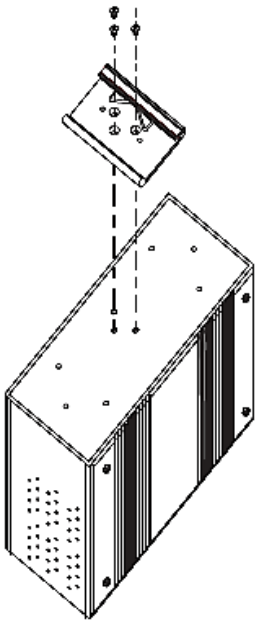
Step 2: Push the device toward the DIN-Rail until you heard a "click" sound.



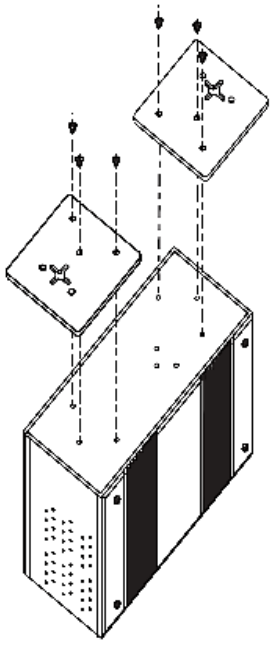
## 2.2 Wall Mounting Installation

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

Step 1: Remove DIN-Rail kit.

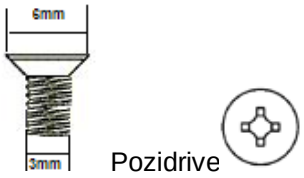


Step 2: Use 6 screws that can be found in the package to combine the wall mount panel. Just like the picture shows below:



The screws specification shows in the following two pictures. In order to prevent the

device from any damage, the screws should not larger than the size that used in it.




Step 3: Mount the combined device on the wall.

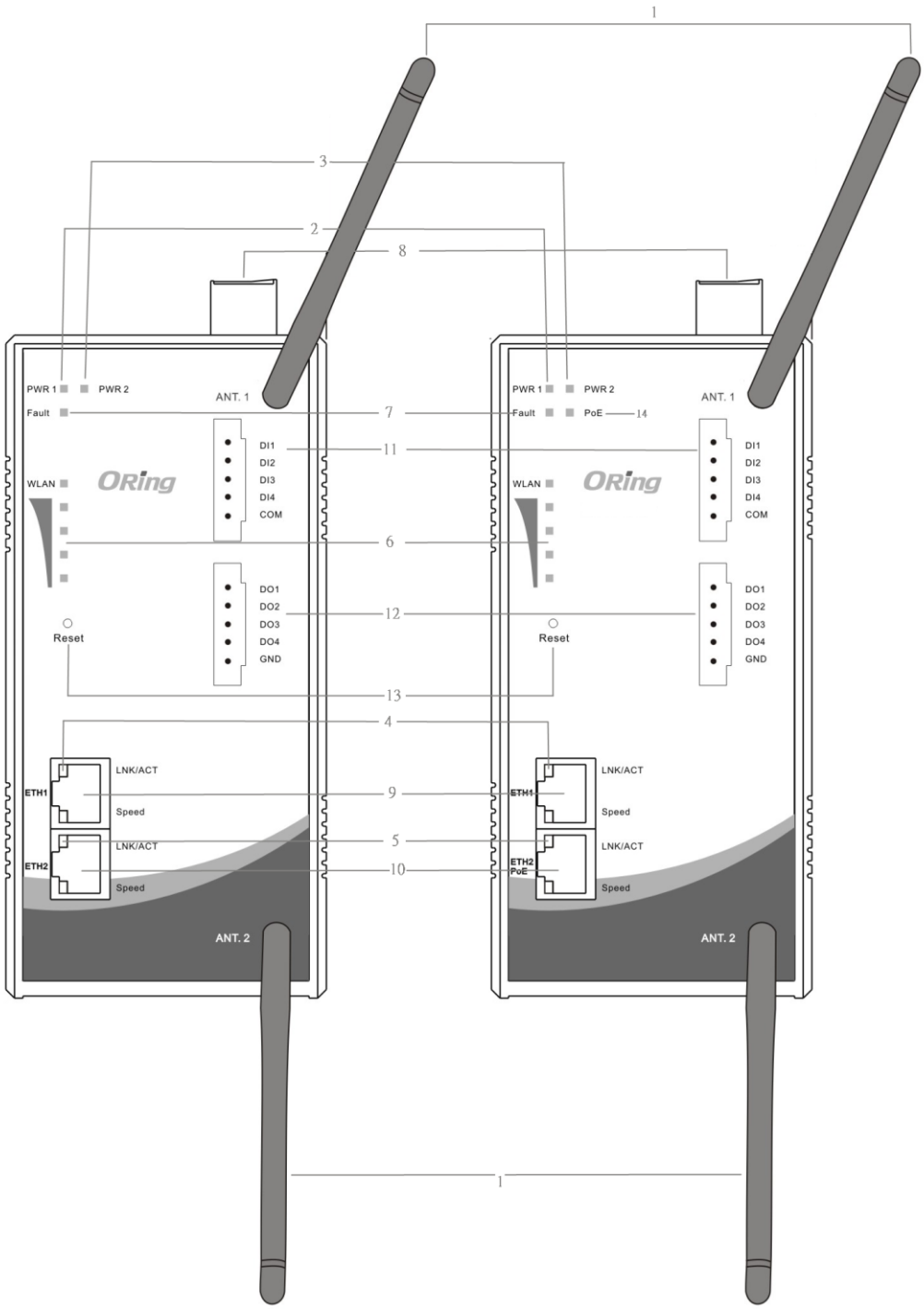
# Hardware Overview

## 3.1 Front Panel

The following table describes the labels that stick on the IGAP-420/620/6620.

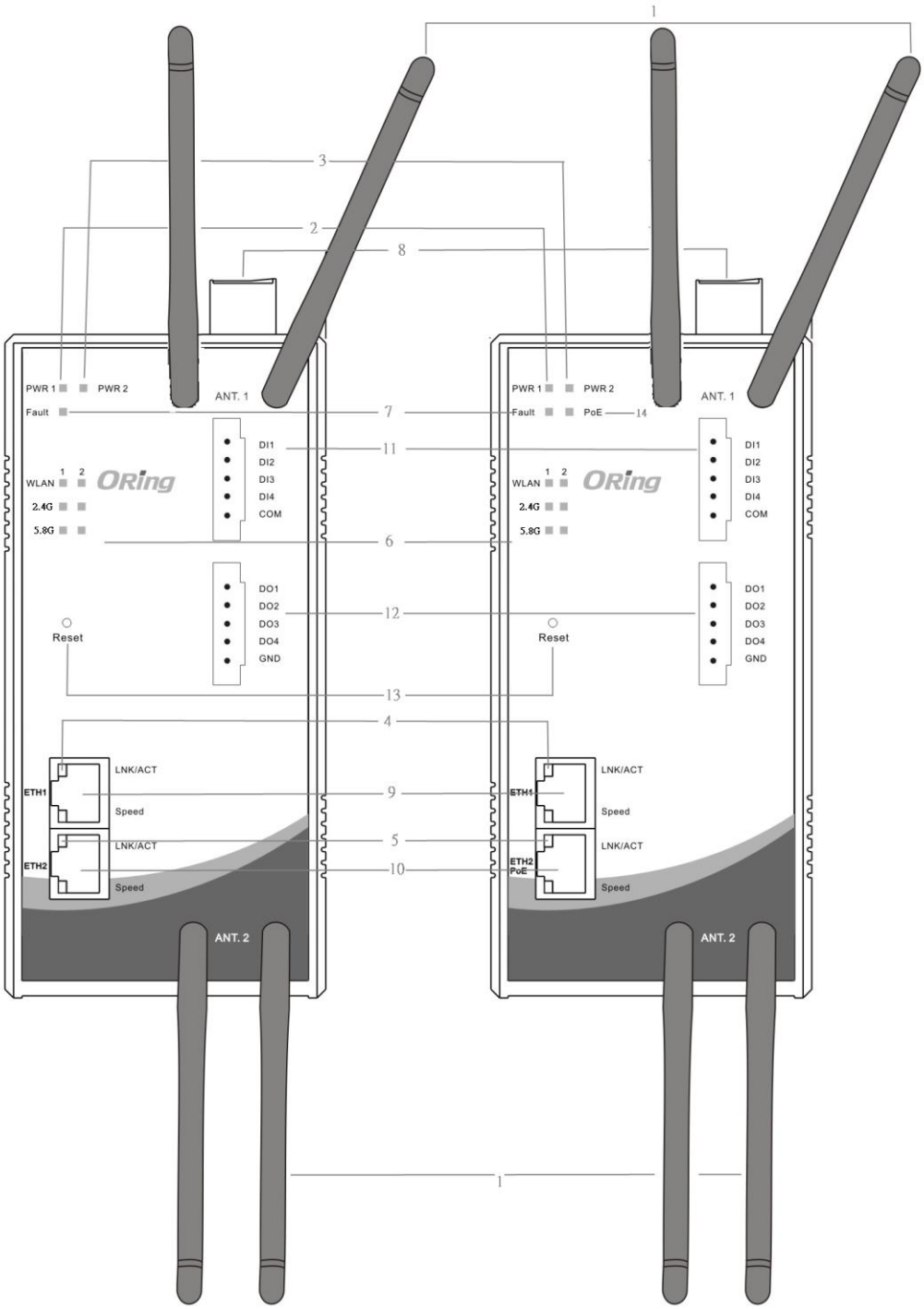
| Port | Description |
|---|---|
| **10/100/1000 Base-T(X) fast Ethernet ports** | 10/100/1000 Base-T(X) fast Ethernet ports support auto-negotiation.<br>Default Setting : auto speed |
| **Relay Output** | Relay output to carry capacity of 3A at 24VDC |
| **Redundant power inputs** | Dual Power Inputs. 12~48 VDC |
| **DIDO** | 4 digital input / 4 digital output |

# IGAP-420/620 IGAP-420+/620+



1. 2.4/5GHz antenna with typical 2 dBi antenna for 5GHz and 2.4GHz.
2. LED for PWR1 and system status. When the PWR1 links, the green LED will be light on.
3. LED for PWR2 and system status. When the PWR2 links, the green LED will be light on.
4. LED for Ethernet port1 status.
5. LED for Ethernet port2 status.
6. LED for WLAN link status.
7. LED for Fault Relay. When the fault occurs, the red LED will be light on.
8. Power Input port
9. Ethernet port1 connector
10. Ethernet port2 connector
11. Digital input
12. Digital output
13. Reset button
14. LED for P.O.E Status (IGAP-420+/620+)

# IGAP-6620 IGAP-6620+



1. 2.4/5GHz antenna with typical 2 dBi antenna for 5GHz and 2.4GHz.
2. LED for PWR1 and system status. When the PWR1 links, the green LED will be light on.
3. LED for PWR2 and system status. When the PWR2 links, the green LED will be light on.
4. LED for Ethernet port1 status.
5. LED for Ethernet port2 status.
6. LED for WLAN frequency using.
7. LED for Fault Relay. When the fault occurs, the red LED will be light on.
8. Power Input port
9. Ethernet port1 connector
10. Ethernet port2 connector
11. Digital input
12. Digital output
13. Reset button
14. LED for P.O.E Status (IGAP-6620+)

## 3.2 Front Panel LEDs

| LED | Color | Status | Description |
|---|---|---|---|
| **PWR1** | Green | Green On | DC power 1 activated. |
| **PWR2** | Green | Green On | DC power 2 activated. |
| **ETH1** | Green/Amber | On | Port link up at 10Mbps /1000Mbps. |
| | Green | On | Port link up at 100Mbps. |
| | | Blinking | Data transmitted. |
| **ETH2** | Green/Amber | On | Port link up at 10Mbps/1000Mbps. |
| | Green | On | Port link up at 100Mbps. |
| | | Blinking | Data transmitted. |
| **WLAN** | Green | On | WLAN activated. |
| | | Blinking | WLAN Data transmitted. |
| **2.4GHz** | Green | On | In using |
| **5GHz** | Green | On | In using |
| **Fault** | Red | On | Fault relay. Power failure or Port down/fail. |

# Cables and Antenna

## 4.1 Ethernet Cables

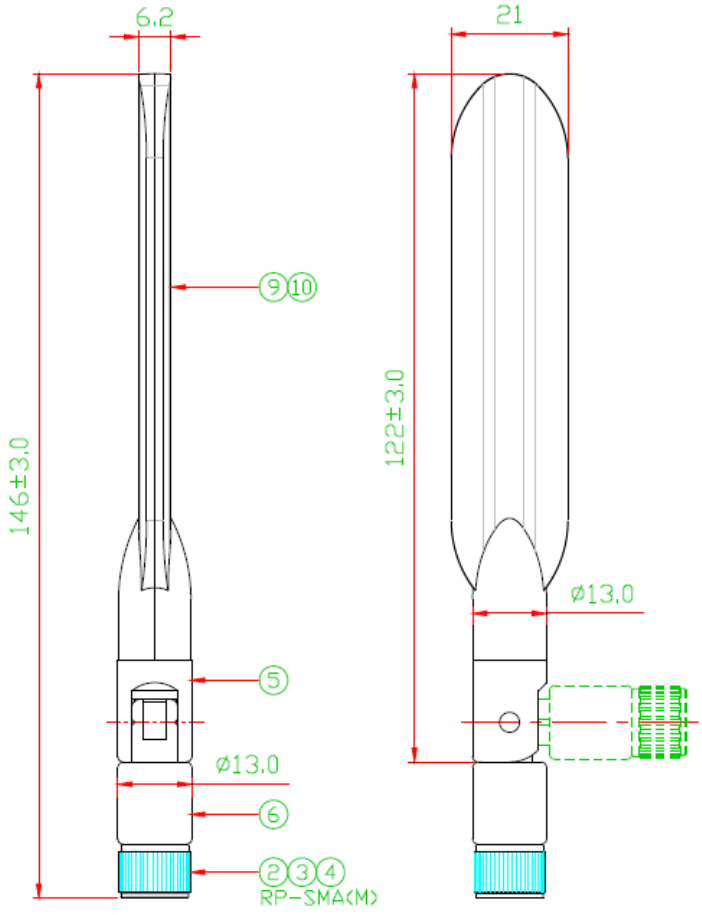
The IGAP-420/620/6620 WLAN AP has two 10/100/1000 Base-T(X) Ethernet ports. According to the link type, the AP use CAT 3, 4, 5,5e,6 UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

| Cable | Type | Max. Length | Connector |
|---|---|---|---|
| 10Base-T | Cat. 3, 4, 5 100-ohm | UTP 100 m (328 ft) | RJ45 |
| 100Base-T(X) | Cat. 5 100-ohm UTP | UTP 100 m (328 ft) | RJ45 |
| 1000Base-T(X) | Cat 5e,6 | UTP 100 m (328 ft) | RJ45 |

## 4.2 Wireless Antenna

2.4GHz/5GHz antenna is used for IGAP-420/620/6620 and connected with a reversed SMA connector. External RF cable and antenna also can be applied with this connector.



# Management Interface

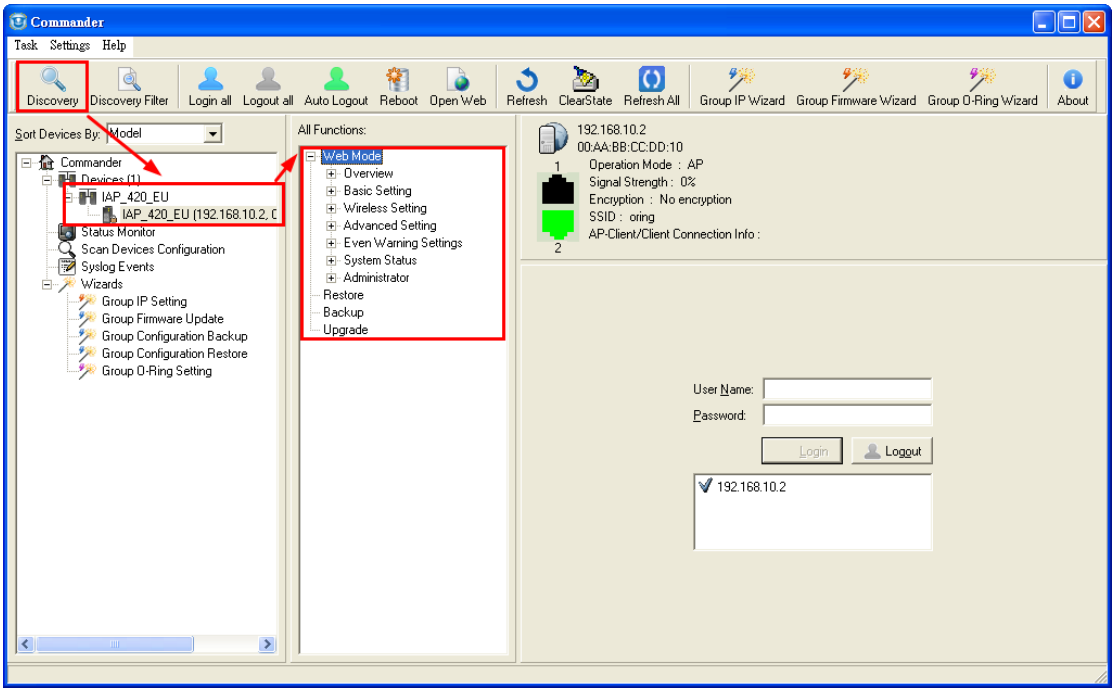
## 5.1 Explore IGAP-420/620/6620

### 5.1.1 Open-Vision_Commander

IGAP-420/620/6620 can also be configure through Oring's window utility Open-Vision

Step 1: Open the commander and click "Discover", the AP devices will show on the list.

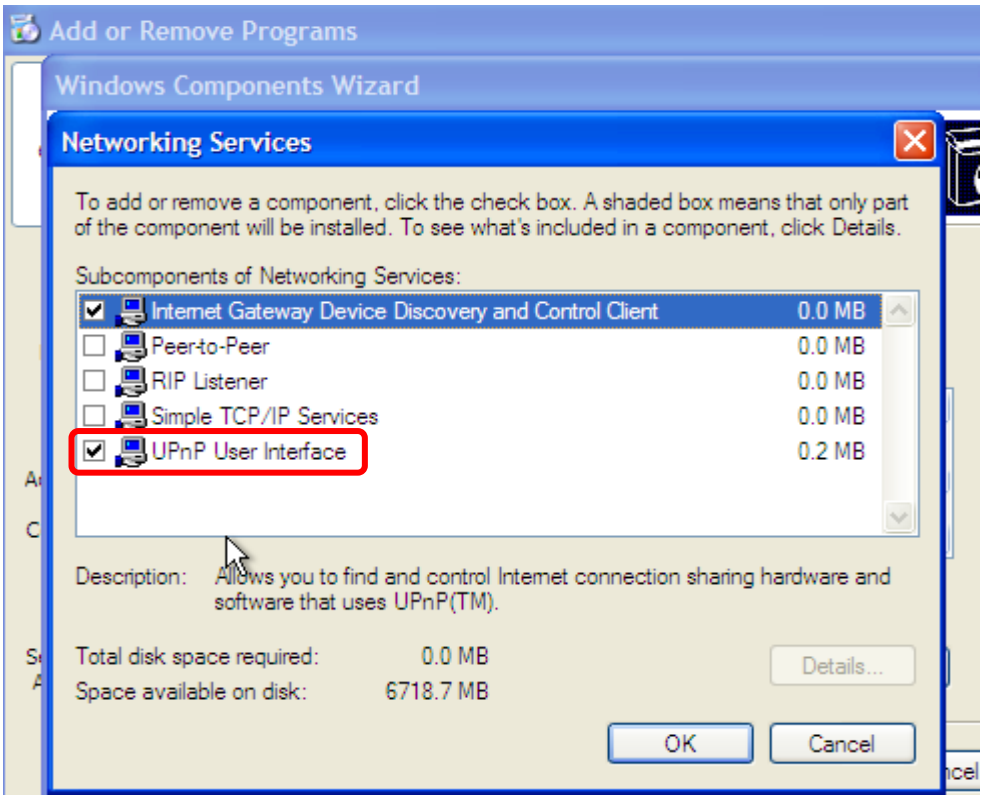
Step 2: Choose your access point, and it will show the AP function tree. Simultaneity, you can login and then set the AP.




User interface of commander

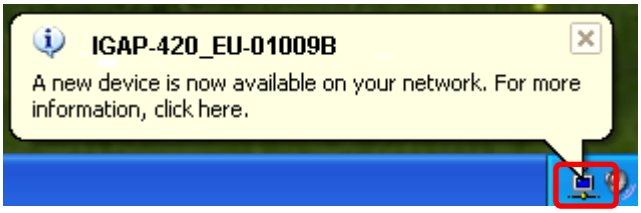
## 5.2 UPnP Equipment

Step 1: To check whether the UPnP UI of the computer is connected to the IGAP-420/620/6620, go to **Control Panel > Add or Remove Programs > Windows Components Wizard > Networking Servers > UPnP User Interface** and pitch on the UPnP User Interface.

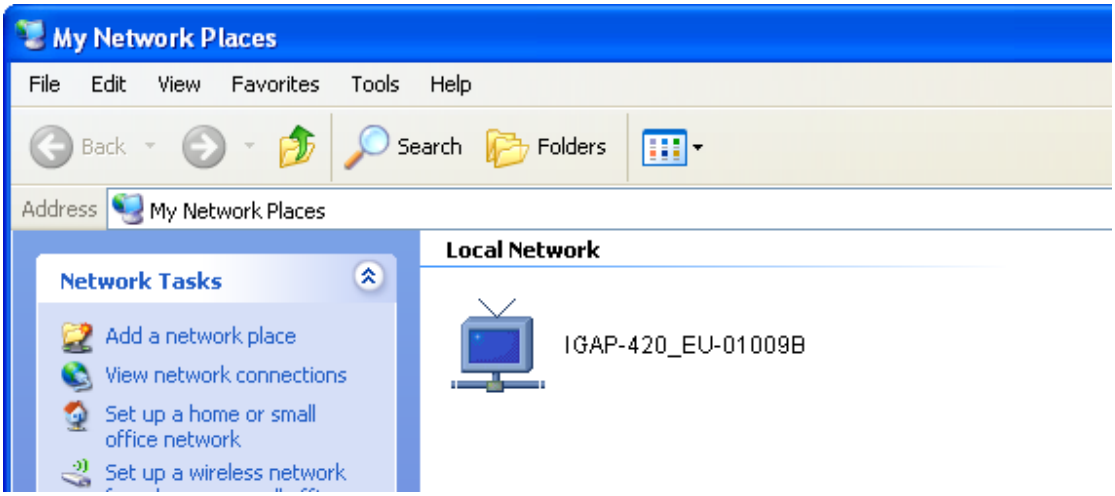



UPnP configuration page

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

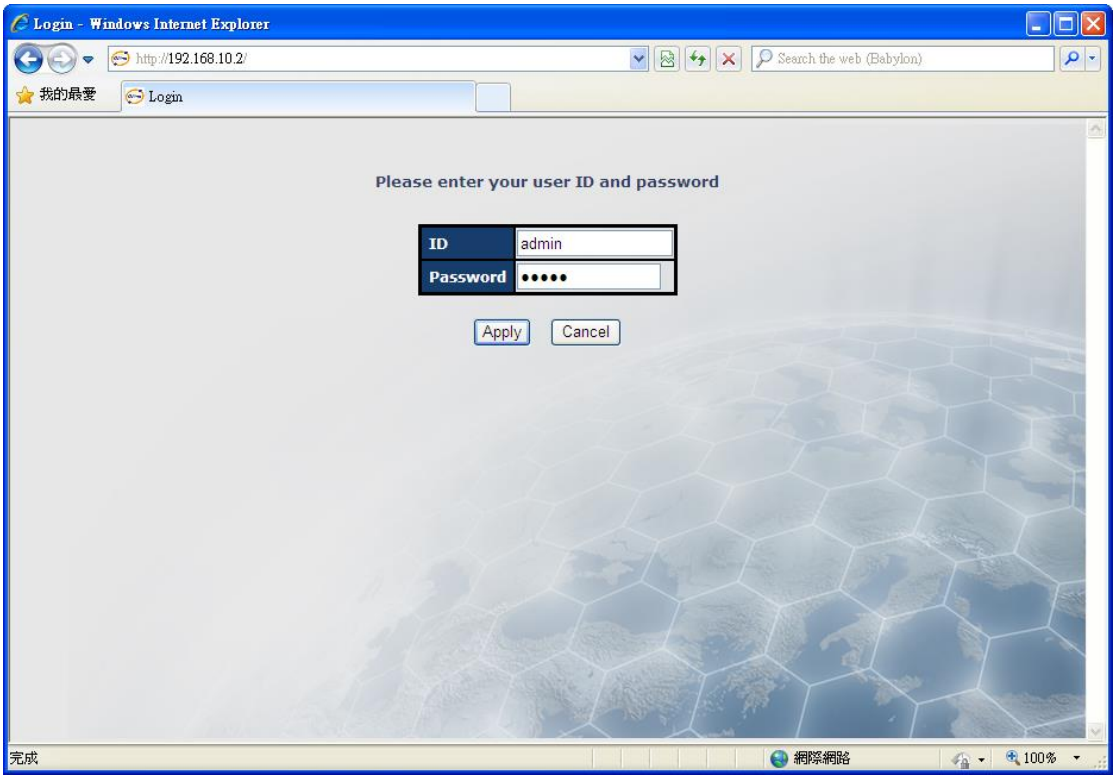
An embedded HTML web site resides in flash memory in the system. It contains advanced management features and allows you to manage the AP from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

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)**, and then click **OK** to continue.

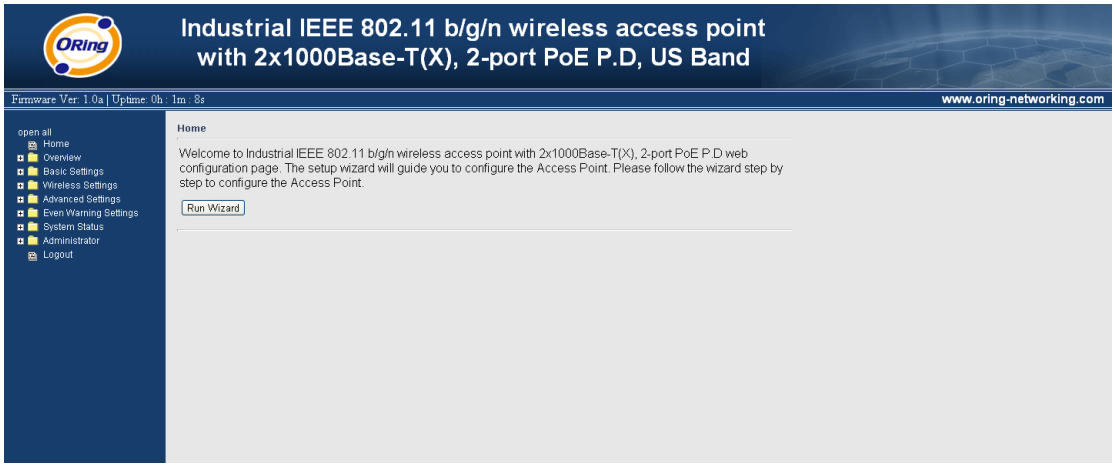



Login screen

For security reasons, we strongly suggest you change the password. Click on **Administrator → Password** 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.



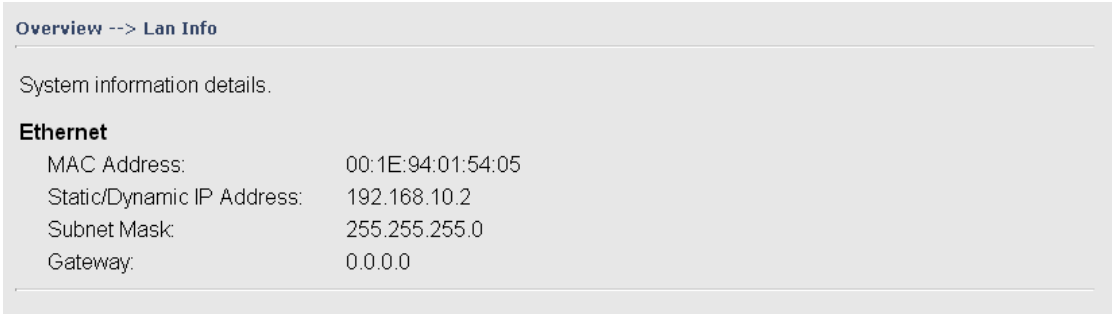

Main interface

## 5.5.1 Overview

### System Info


System Info

### Lan Info



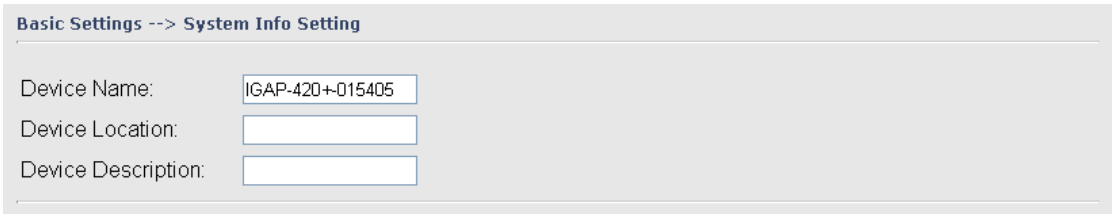

Lan Info

### Wireless Info


Wireless Info

## 5.5.2 Basic Setting

### System Info Setting

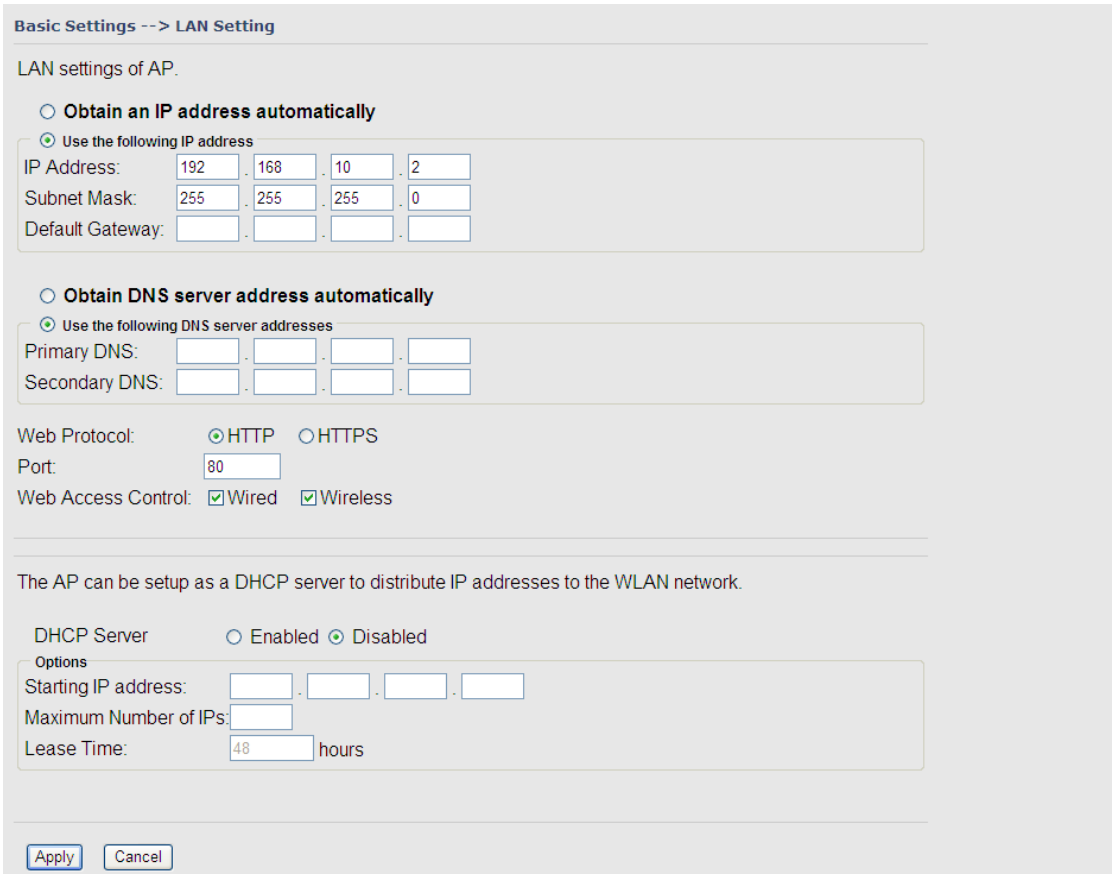



System Info Setting interface

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| **Device Name** | Define Device Name |
| **Device Location** | Define Device Location |
| **Device Description** | Define Device Description |

## Lan Setting



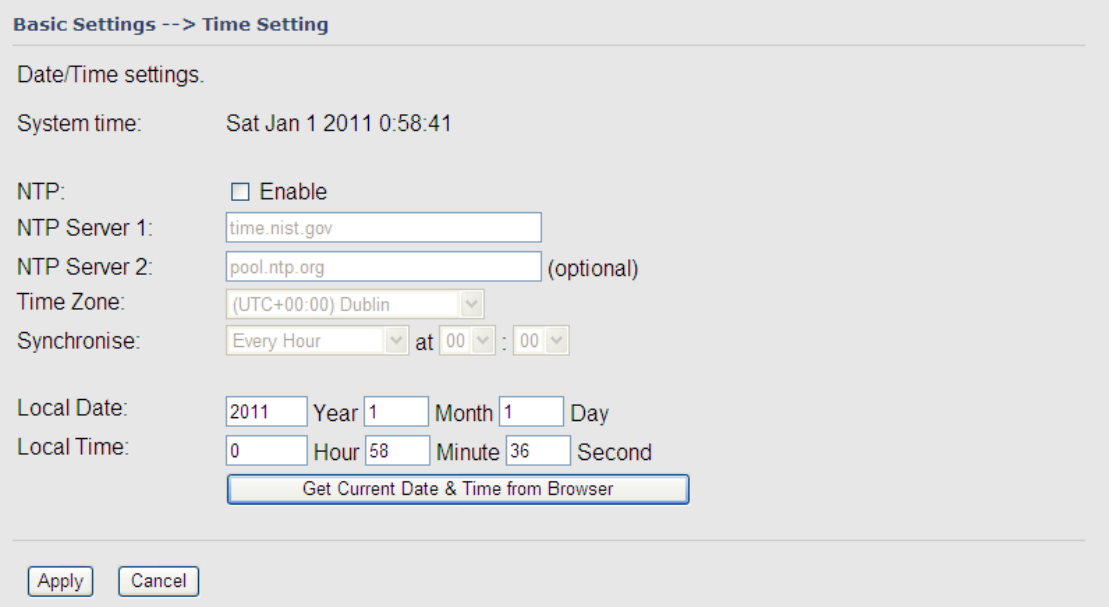

Lan Setting interface

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| **Obtain an IP address automatically** | Select this option if you would like to obtain an IP address automatically assigned by DHCP server in your network |
| **Use the following IP address** | Select this option if you are manually assigning an IP address.<br><br>**IP Address:** There is a default IP address in the AP, and you can input a new IP address.<br><br>**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.<br><br>**Default Gateway:** Enter the IP address of the router in your network. |
| **Obtain DNS server address** | This option is selected by DHCP server. |

| | |
|---|---|
| **automatically** | |
| **Use the following DNS server addresses** | This option is selected by manually set<br><br>**Preferred DNS:** There is a default DNS server, and you can input another new DNS server.<br><br>**Alternate DNS:** There is a default DNS server, and you can input another new DNS server. |
| **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. |
| **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 IPs** | The dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. **100** will be entering 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. |

## Time Setting

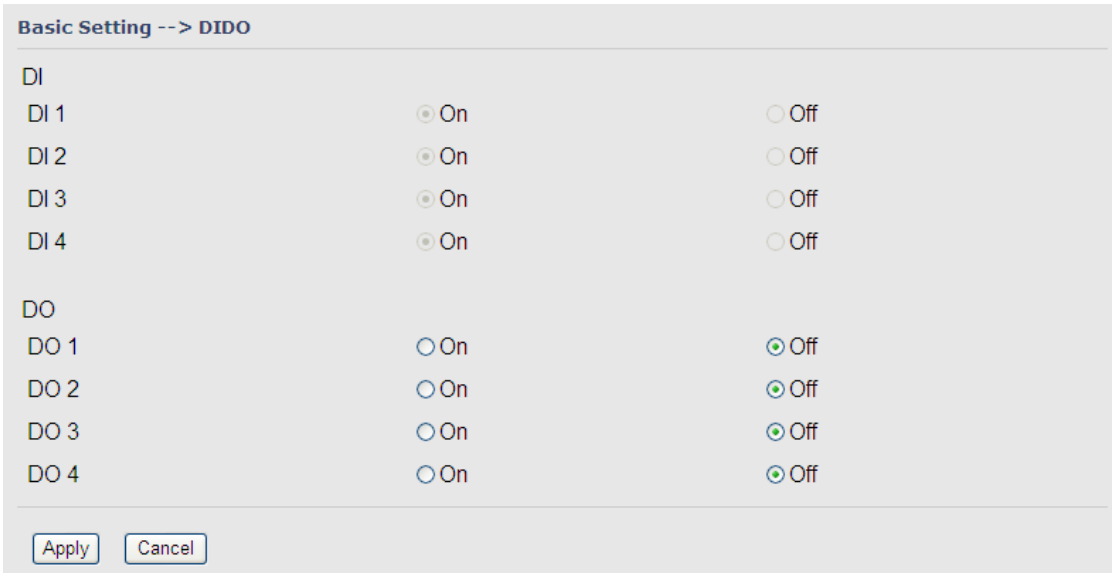



Time setting interface

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| **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. |
| **Time Zone** | Select the time zone manually |
| **Synchronize** | Set the time, and the AP's time synchronize with the NTP Server at the time |
| **Local Date** | Set local date manually. |
| **Local Time** | Set local time manually. |
| **Get Current Date & Time from Browser** | Click this button, you can set the time from browser. |

### DIDO

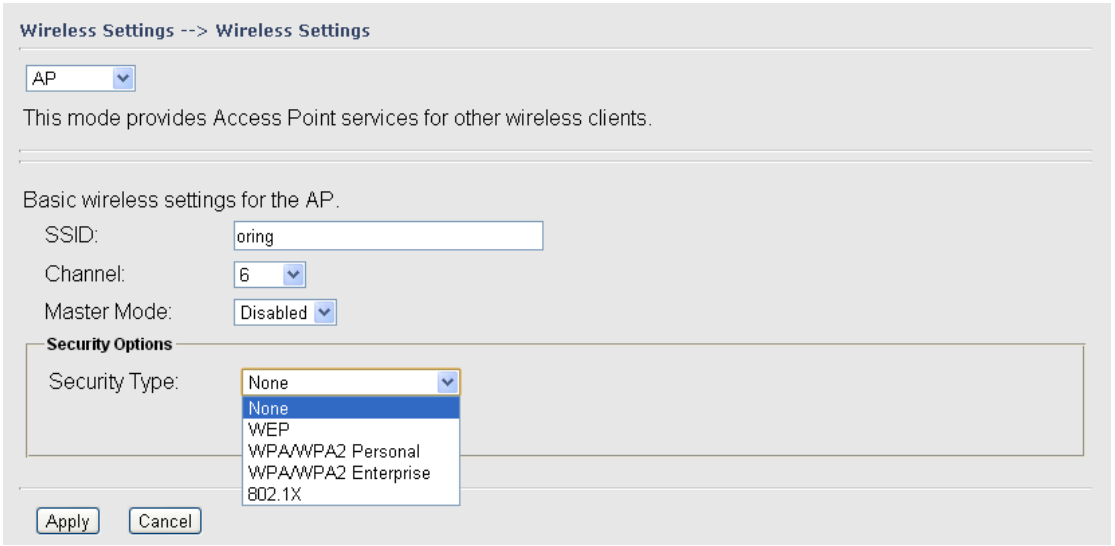



DIDO setting interface

## 5.5.3 Wireless Setting

### AP Mode

This mode provides Access Point services for other wireless clients.




AP mode setting interface

The following table describes the labels in this screen.

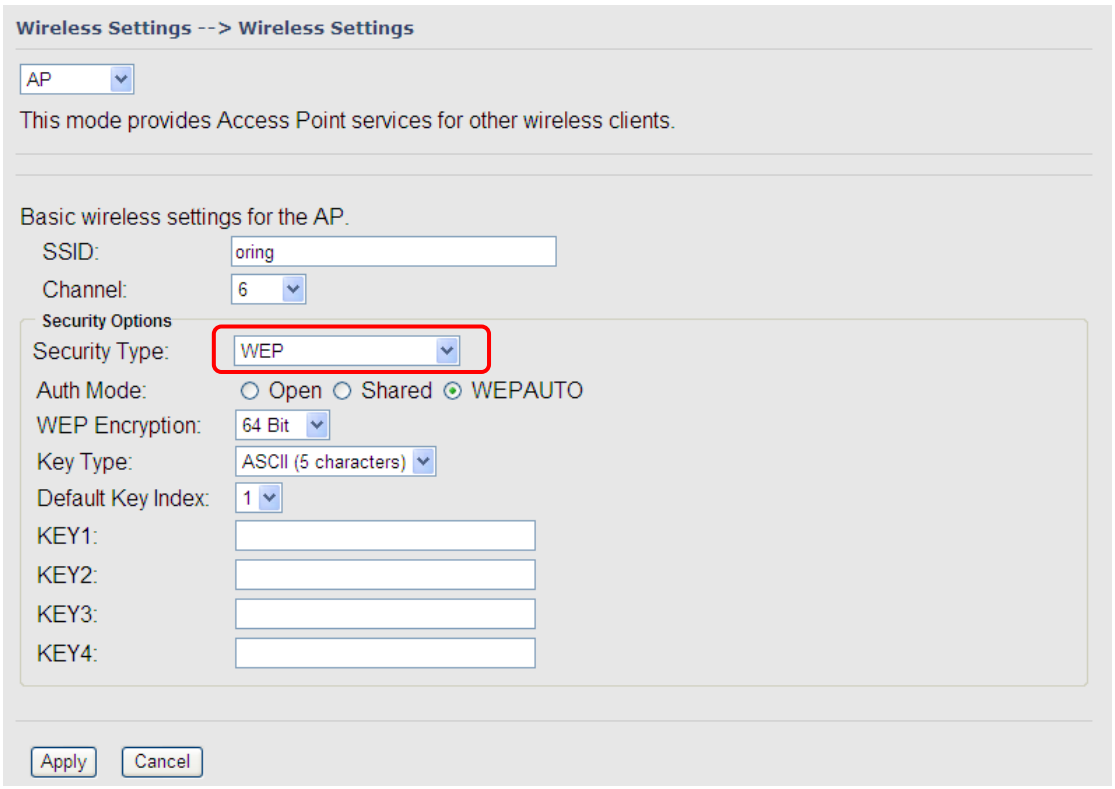
| Label | Description |
|---|---|
| **SSID** | Service Set Identifier Default is the default setting. The SSID is a unique name that identifies a network. All devices on the network must share the same SSID name in order to communicate on the network. If you change the SSID from the |

| | |
|---|---|
| | 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. |
| **Master Mode** | Enable / disable Master mode |
| **Security options** | Select the type of security for your wireless network at **Security Type:**<br><br>**None:** Select for no security.<br><br>**WEP:** Select for security WEP.<br><br>**WPA/WPA2-Personal (per share key):** Select for security WPA-PSK or WPA2-PSK without a RADIUS server.<br><br>**WPA/WPA2-Enterprice:** Select for WPA or WPA2 (Wi-Fi Protected Access) authentication in conjunction with a RADIUS server.<br><br>**802.1x:** Authentication through RADIUS server |

**Security Type – None**

No security protection on your wireless LAN access.

**Security Type – WEP**

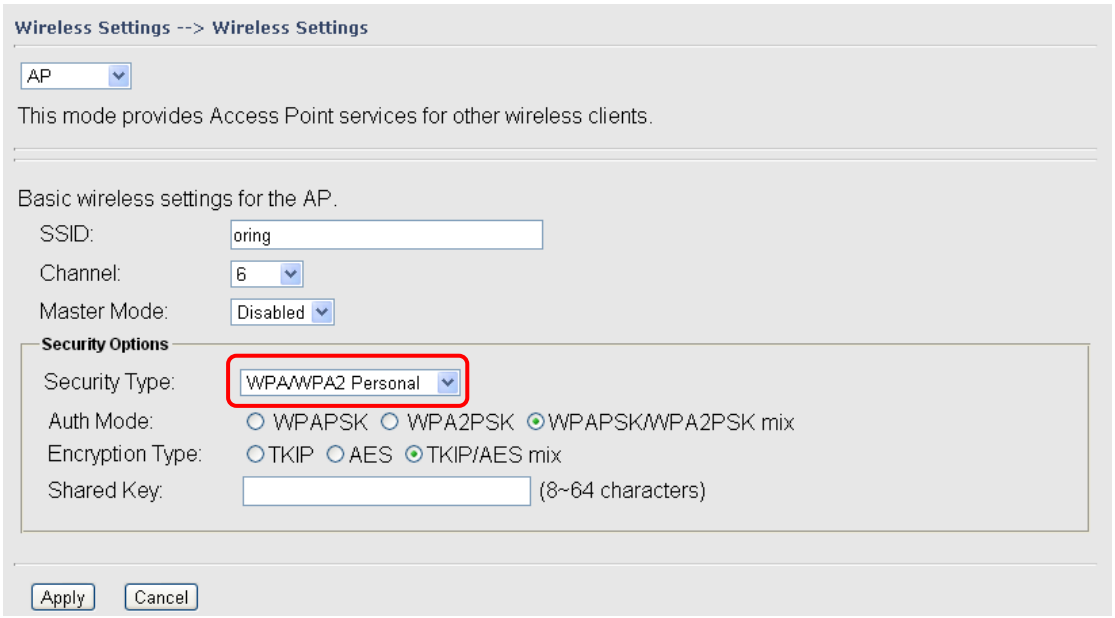



WEP setting interface

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.

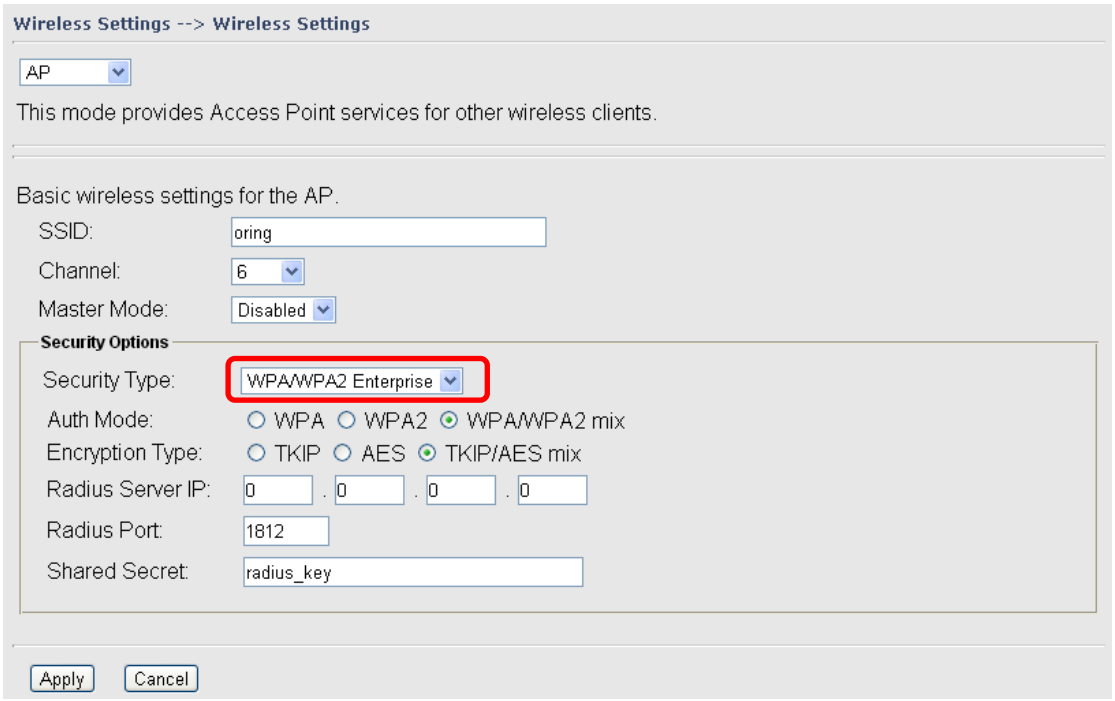
**Security Type –WPA/WPA2-Personal (per share key)**




WPA/WPA2-Personal setting interface

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

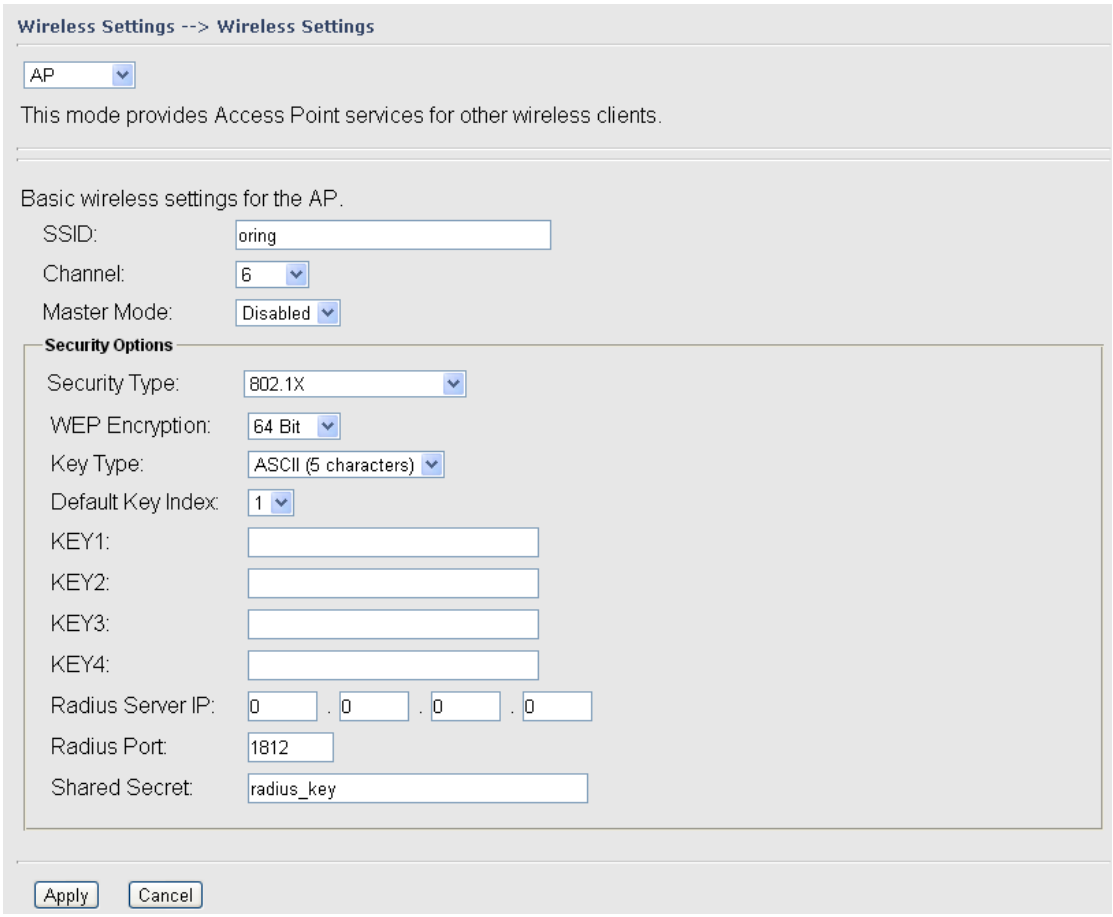
**Security Type –WPA/WPA2-Enterprice**




WPA/WPA2-Enterprice setting interface

1. Security Type: Select **WPA/WPA2-Enterprice**
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**



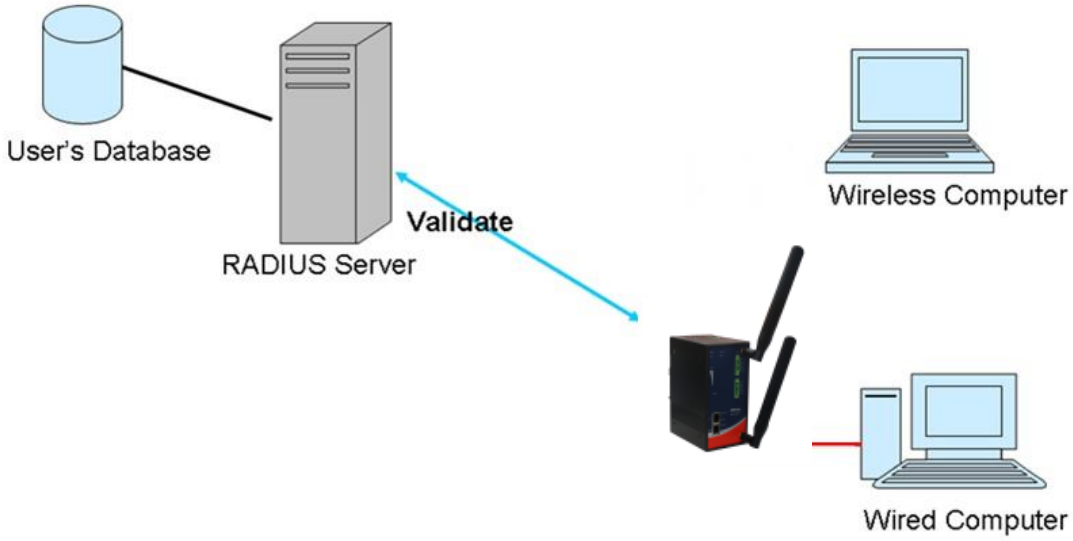

802.1x setting interface

1. Security Type: Select **802.1x**
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.

**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.

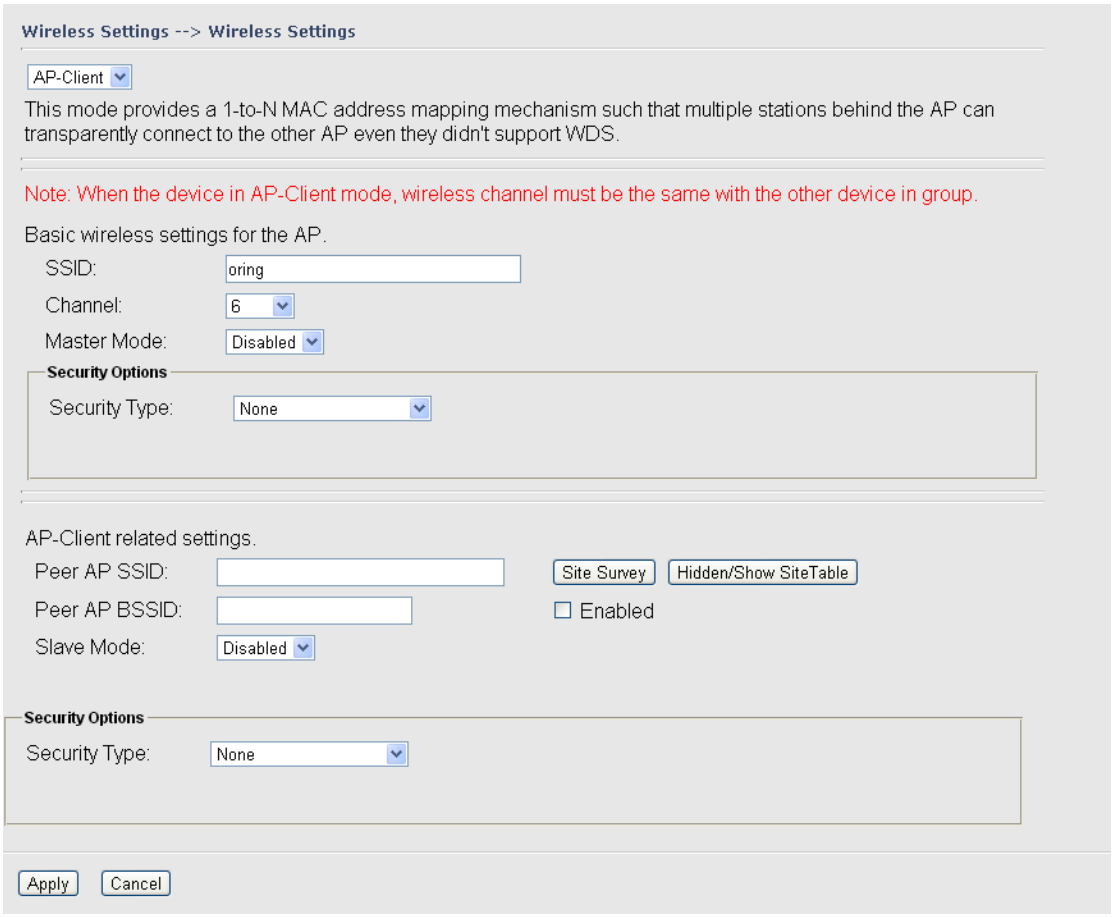
Radius server validates your proof, also carry on the authorization. So the Radius server received by ISA server responded (point out the customer carries proof to be not granted) and it means that the Radius server did not authorize you to carry. Even if the proof has already passed an identify verification,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

This mode 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.




AP-Client setting interface

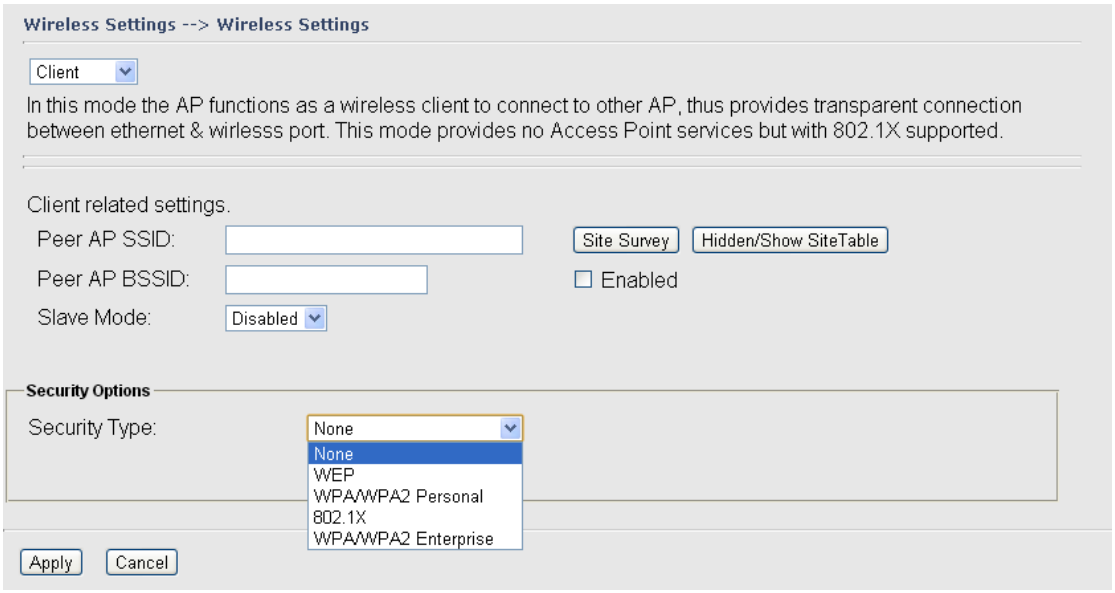
The following table describes the labels in this screen.

| 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.( **wireless channel must be the same with the other device in group**) |
| **Master Mode** | Enable / disable master mode |
| **Security options** | Select the type of security for your wireless network at **Security** |

| | |
|---|---|
| | **Type:**<br>**None:** Select for no security.<br><br>**WEP:** Select for security WEP.<br><br>**WPA/WPA2-Personal (per share key):** Select for security WPA-PSK or WPA2-PSK without a RADIUS server. |
| **Peer AP SSID** | Enter the other AP which used for AP mode. |
| **Peer AP BSSID** | Fill the Peer AP BSSID (Wireless MAC address) limit client target |
| **Slave Mode** | Enable / disable Slave 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, AP-client mode only supports WEP and WPA/WPA2 Personal. |

## Client Mode

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.



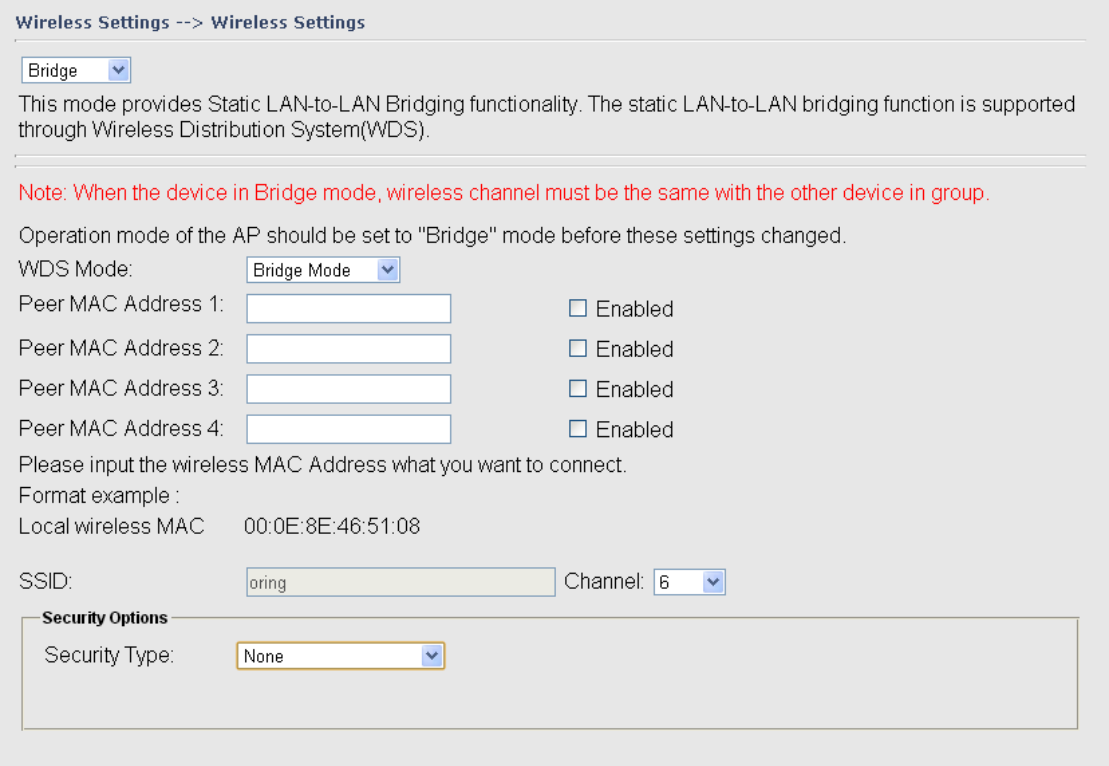

Client mode setting interface

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| **Peer AP SSID** | Enter the other AP which used for AP mode. |
| **Peer AP BSSID** | Fill the Peer AP BSSID (Wireless MAC address) limit client target |
| **Site Scan** | You can scan the APs which used for AP mode in the certainty area |
| **Slave Mode** | Enable / disable Slave mode |
| **Security Type** | Set the same security with the AP which you want to connect. |

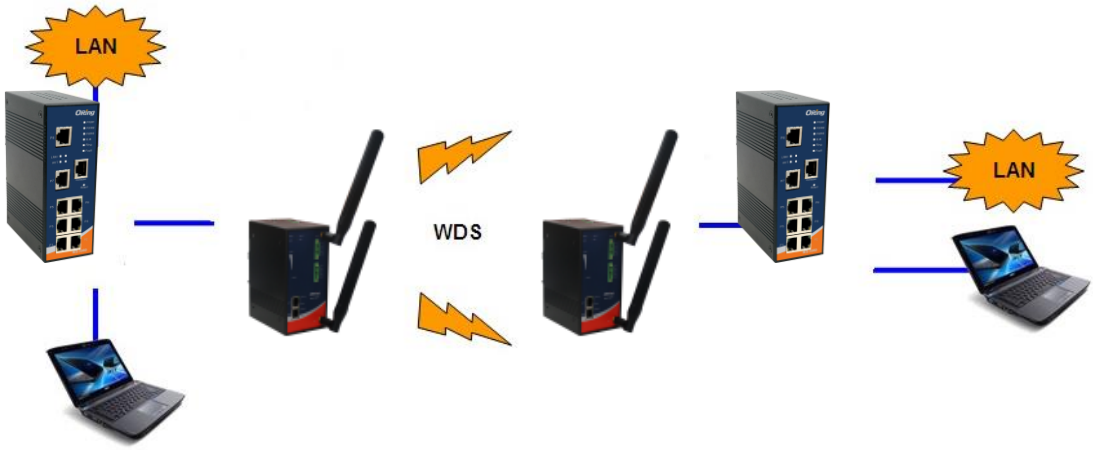
## Bridge Mode

This mode provides Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS), this mode only support 802.11b/g.




Bridge mode 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-Point WDS Link

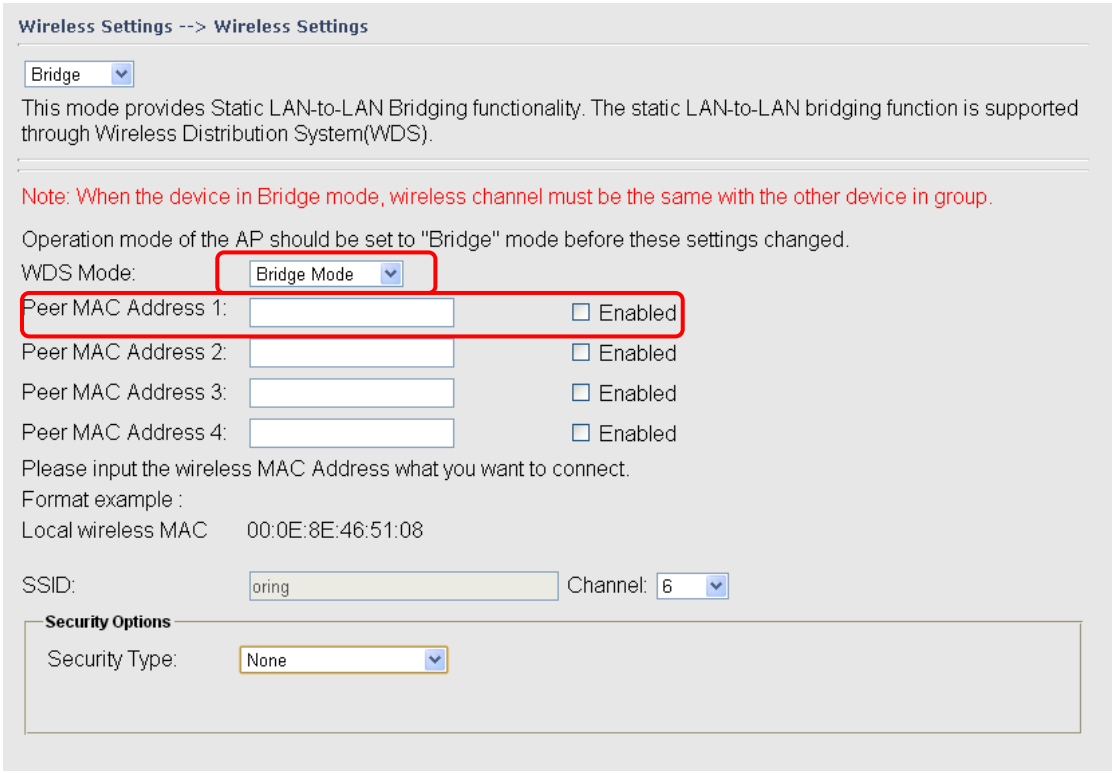
The following table describes the labels in this screen.

| 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). |
| **Peer MAC Address** | Set the Mac address of other access point(s). Simultaneity, choose on "Enable". |
| **SSID(only Repeater mode support)** | 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. ( **wireless channel must be the same with the other device in group**) |
| **Security options** | Select the type of security for your wireless network at **Security Type:**<br><br>**None:** Select for no security.<br><br>**WEP:** Select for security WEP.<br><br>**WPA/WPA2-Personal (per share key):** Select for security WPA-PSK or WPA2-PSK without a RADIUS server. |

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. At wireless web setting Security and Channel should be the same,
6. AP's distance should be limited within a certainty area.

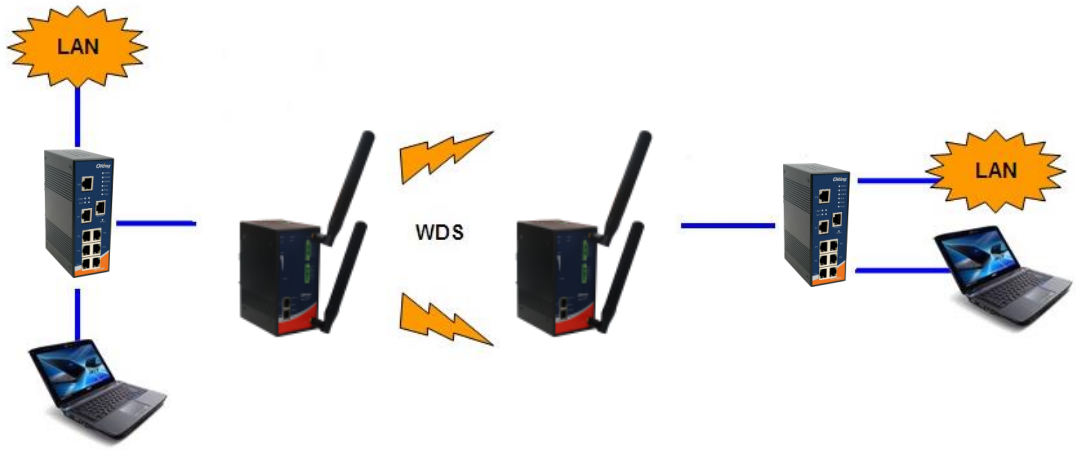
**WDS –Bridge Mode**




WDS-Bridge mode setting interface

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

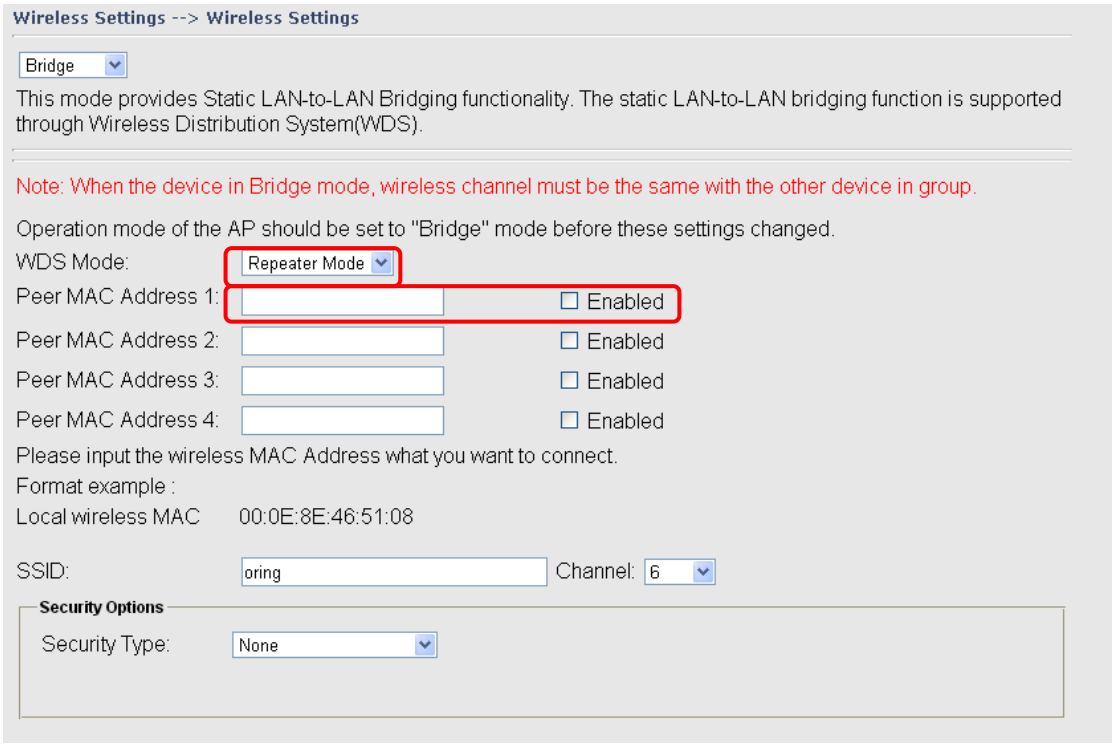
The working principle of **Bridge Mode** as follows:




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**




WDS-Repeater mode setting interface

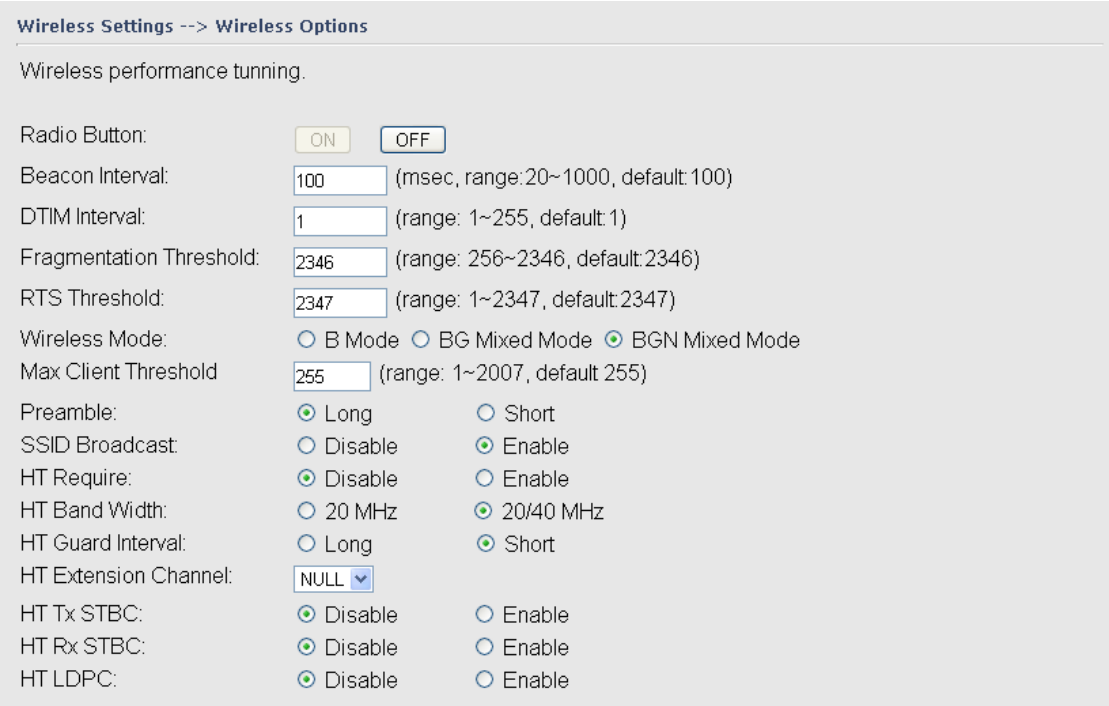
The peer WDS APs are according to the MAC address listed in "Peer Mac Address" fields.

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.

## Wireless Options



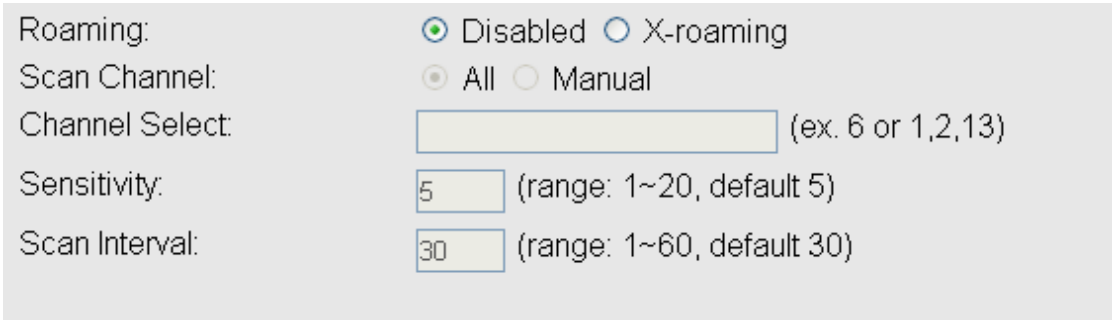

Wireless options interface

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| **Radio Button** | Enable or Disable Wireless function |
| **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. |
| **Wireless Network Mode** | You can select 802.11 b/g/n wireless mode mix or single |
| **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 |

## Extra parameters for Client Mode(X-Roaming)



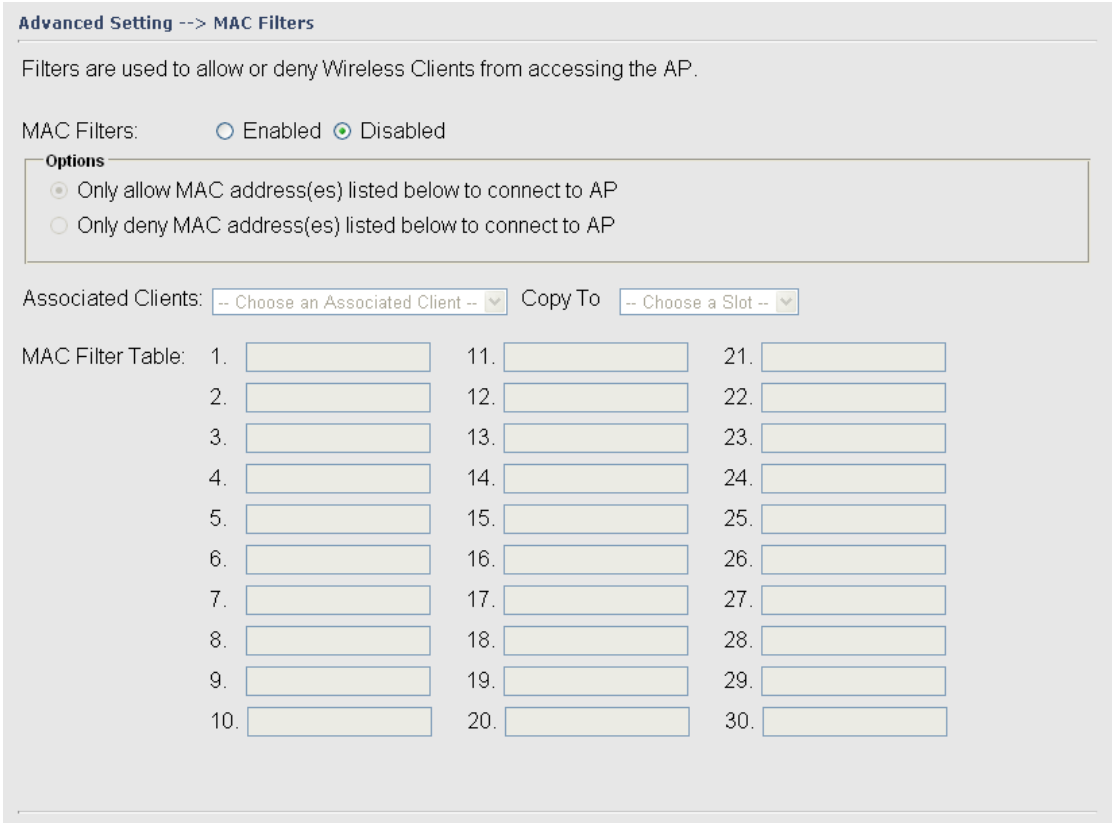

X-Roaming setting interface

The following table describes the labels in this screen

| Label | Description |
|---|---|
| **Roaming** | **Disable:** Disable X-Roaming protocol.<br>**X-roaming:** Enable X-Roaming protocol |
| **Scan channel** | **All:** scan all support channel<br>**Manual:** only scan "channel select" value |
| **Channel Select** | Assign the roaming channel value |
| **Sensitivity** | Set the signal sensitivity |
| **Scan interval** | Set the scan interval |

## 5.5.4 Advanced Setting
## Filters

Use **Advanced Setting > MAC Filters** to allow or deny wireless clients, by their MAC addresses, from accessing the IGAP-420/620. You can manually add a MAC address or select the MAC address from **Connected Clients** that are currently connected to the AP.

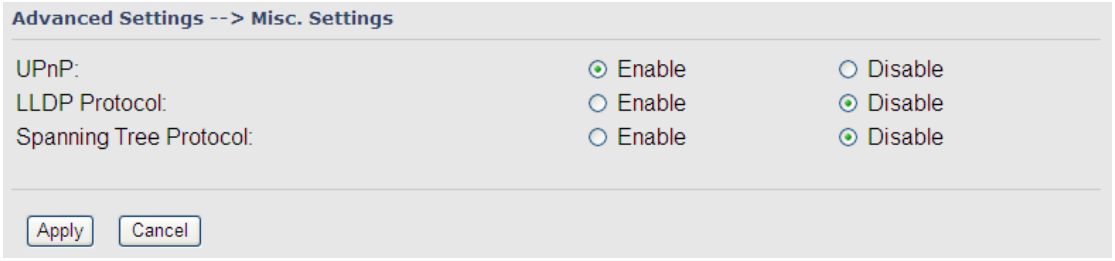



Filters setting interface

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. |

## Misc. Settings




Misc. setting interface

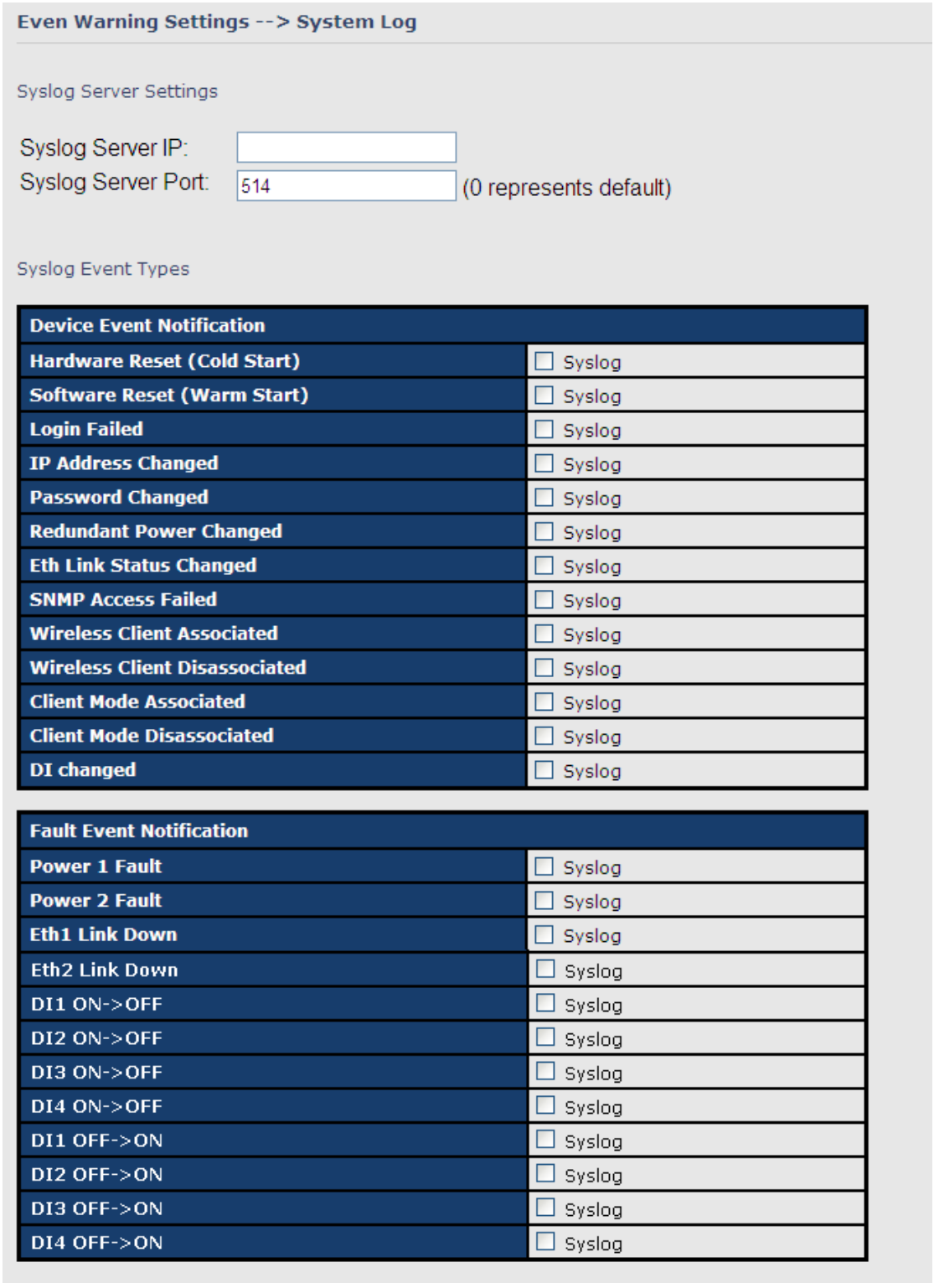
The following table describes the labels in this screen.

| Label | Description |
|---|---|
| **UPnP** | Enable or disable UPnP function |
| **LLDP Protocol** | Enable or disable LLDP function |
| **Spanning Tree Protocol** | Enable or disable STP function |

### 5.5.5 Even Warning Settings

When the AP event triggered, the notification procedure will be performed according to the type of the event.

## System Log

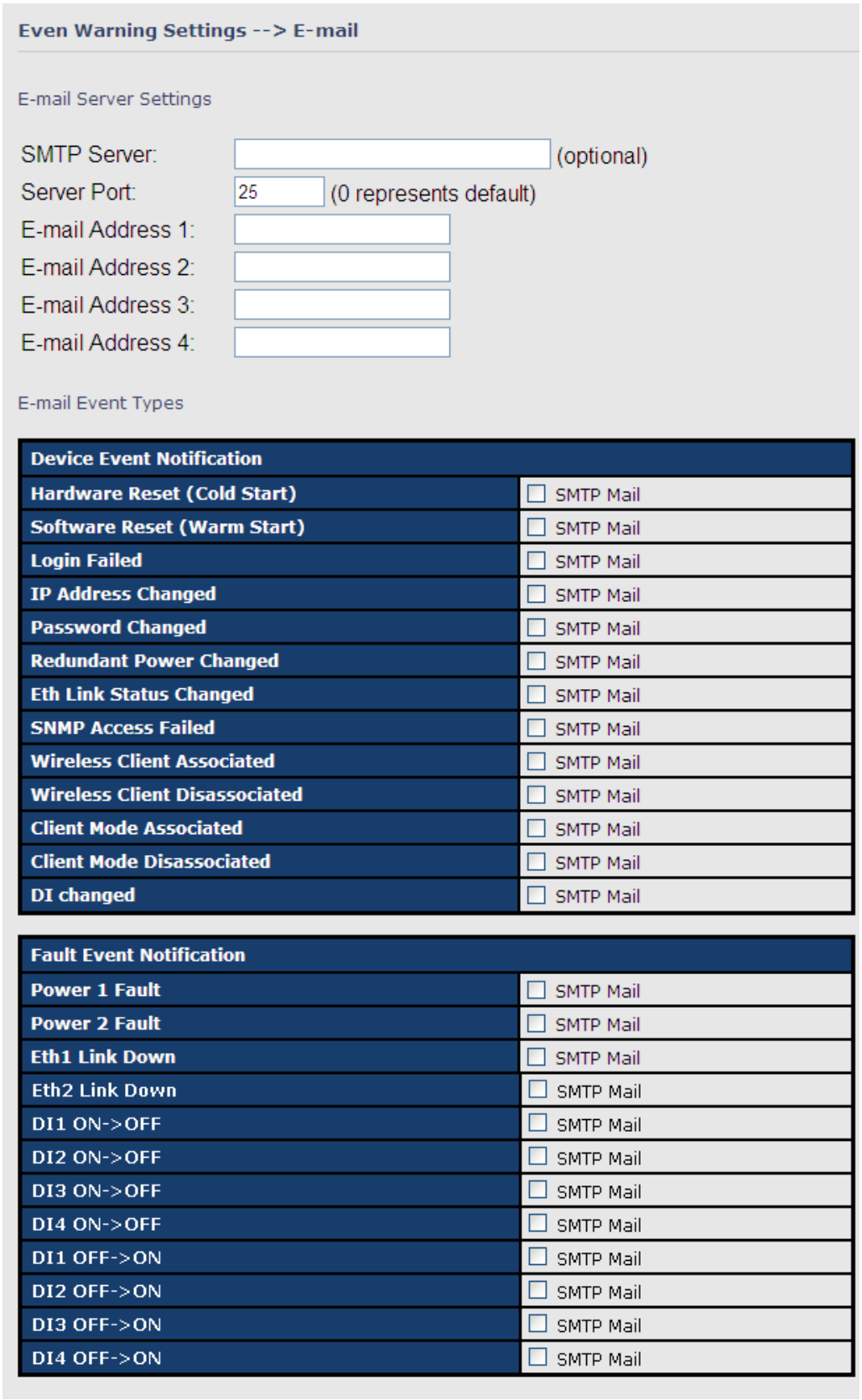



System Log setting interface

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. |

## E-Mail

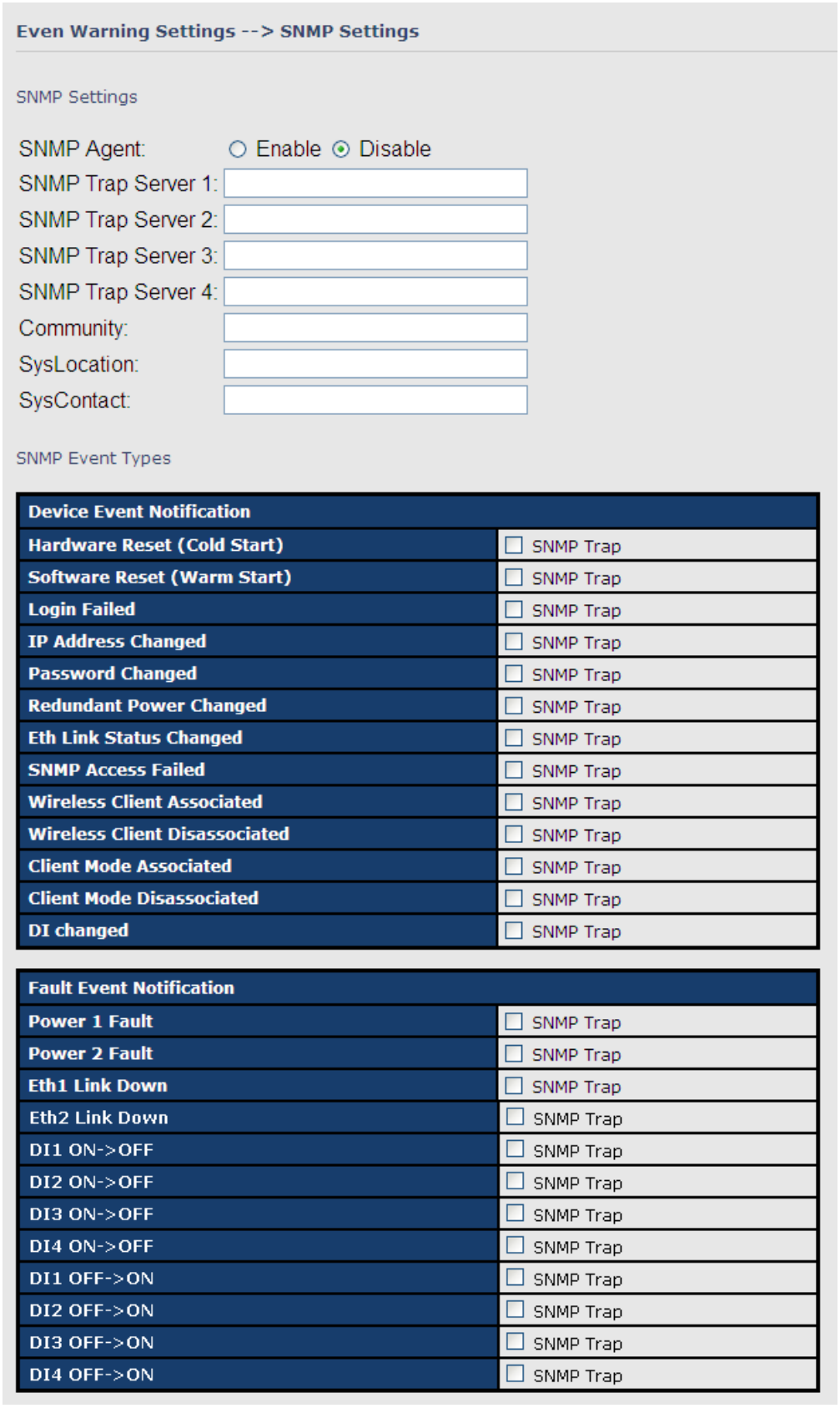



E-Mail setting interface

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

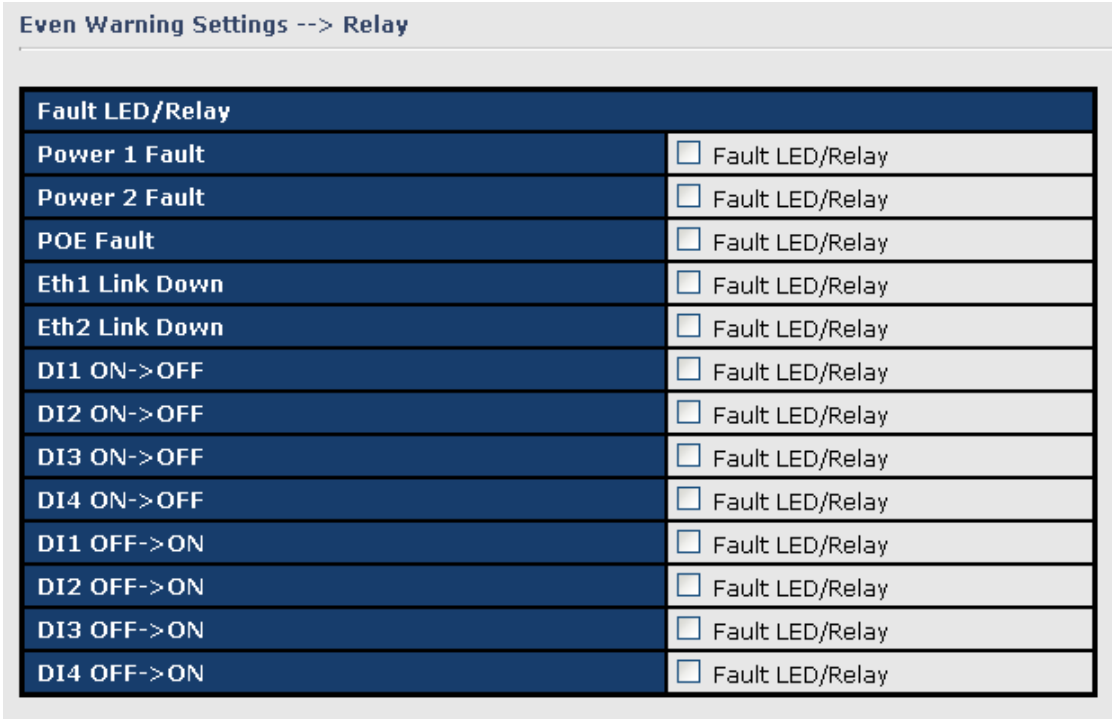



SNMP setting interface

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. |

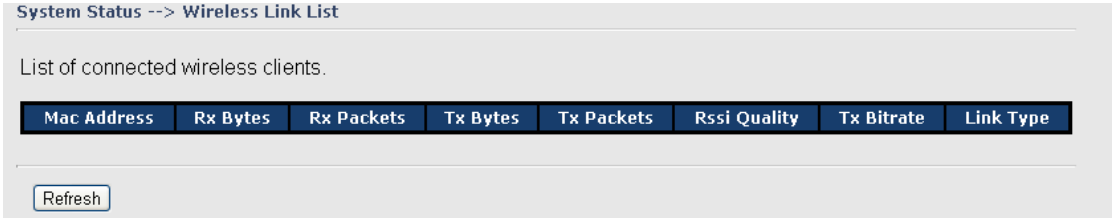
## Relay




Relay setting interface

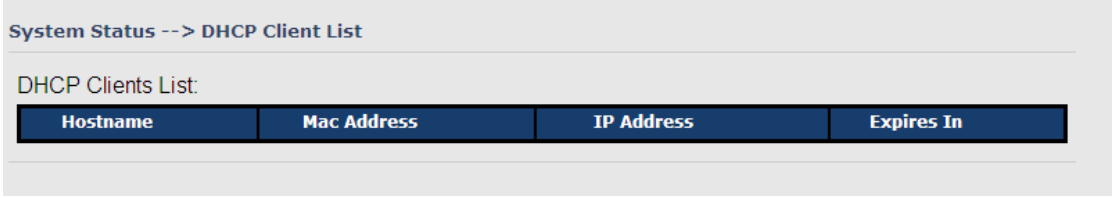
## 5.5.6 System status

### Client status



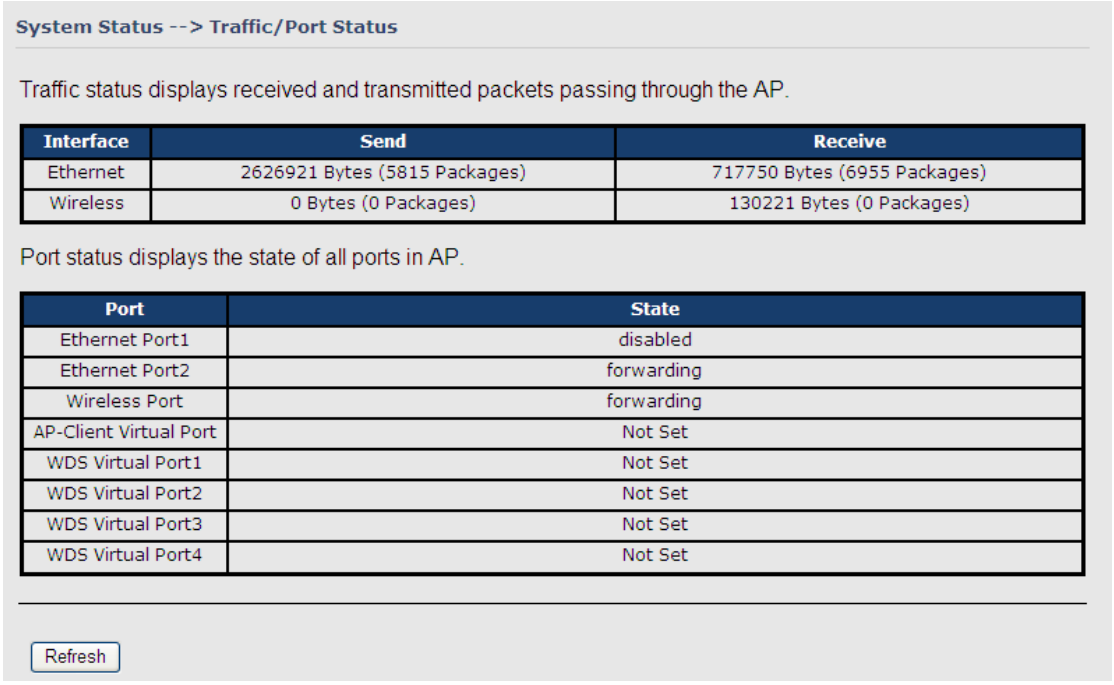

This page of the list displays the **Mac Address** of the wireless clients connected.

### DHCP Clients List




List the devices on your network that are receiving dynamic IP addresses from the IGAP-420/620.

### Traffic/Port Status




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.

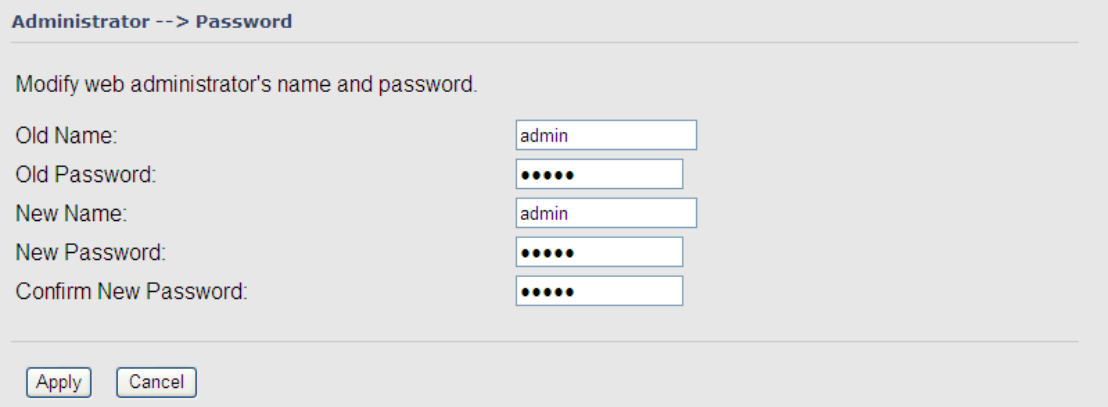
## System Log


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.

## 5.5.7 Administrator Password

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 "").



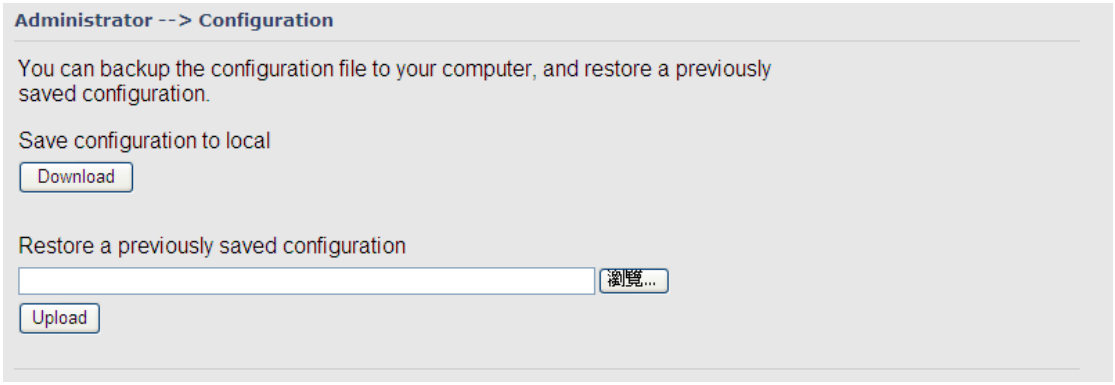

Password setting interface

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 cannot 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. |

## 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 IGAP-420 / 420+ ; IGAP-620/620+ 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. |

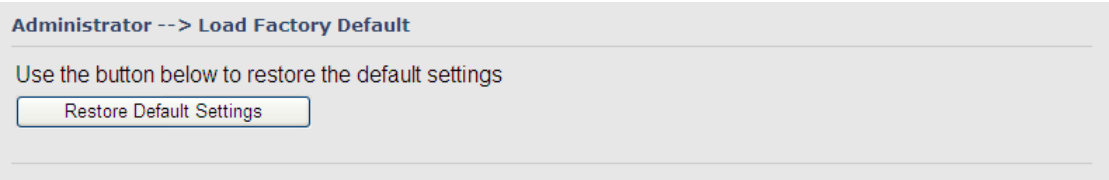
## Firmware Upgrade


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.

---

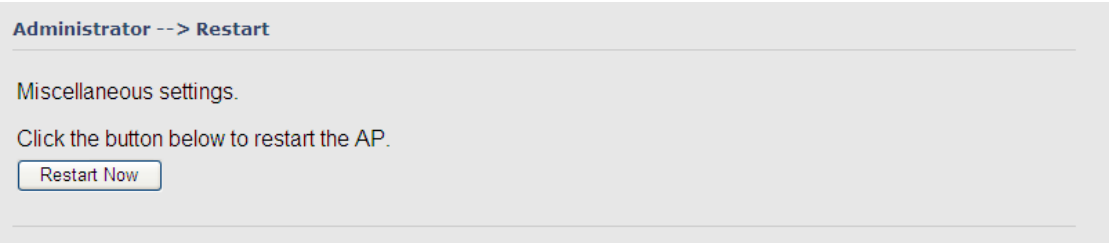
**Notice: DO NOT POWER OFF THE AP OR PRESS THE RESET BUTTON WHILE THE FIRMWARE IS BEING UPGRADED.**

## Load Factory Default




You may also reset the IGAP-420/620 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.

## Restart




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

# Technical Specifications

| | |
|---|---|
| **LAN Interface** | |
| Ethernet Ports | 2 x 10/100/1000Base-T(X), Auto MDI/MDI-X |
| Protocols | IP, TCP, UDP, DHCP, BOOTP, ARP/RARP, DNS, SNMP MIB II, HTTPS, SNMPV1/V2, Trap, Private MIB |
| **WLAN Interface** | |
| Operating Mode | AP/ Client /Bridge/ AP-Client |
| Antenna and Connector | 2 antennas with 2dBi for 5GHz and 2.4GHz in reverse SMA connector |
| Radio Frequency Type | DSSS, OFDM |
| Modulation | IEEE802.11b: CCK/DQPSK/DBPSK<br>IEEE802.11a/g: OFDM<br>IEEE802.11n: BPSK, QPSK, 16-QAM, 64-QAM |
| Frequency Band | America / FCC : 2.412~2.462 GHz (11 channels)<br>5.180~5.240 GHz & 5.745~5.825 GHz ( 9 channels )<br>Europe CE / ETSI : 2.412~2.472 Ghz (13 channels)<br>5.180~5.240 GHz (4 channels) |
| Transmission Rate | 802.11b: 1/2/5.5/11 Mbps<br>802.11a/g: 6/9/12/18/24/36/48/54 Mbps<br>802.11n(40MHz): UP to 300 Mbps |
| Transmit Power | 802.11a: 12dBm ± 1.5dBm@54Mbps(IGAP-620/6620)<br>802.11b: 17dBm ± 1.5dBm@11Mbps<br>802.11g: 16dBm ± 1.5dBm@54Mbps<br>802.11gn HT20: 15dBm ± 1.5dBm @MCS7<br>802.11gn HT40: 14dBm ± 1.5dBm @MCS7<br>802.11an HT20: 12dBm ± 1.5dBm @MCS7(IGAP-620/6620)<br>802.11an HT40: 11dBm ± 1.5dBm @MCS7(IGAP-620/6620) |
| Receiver Sensitivity | 802.11a : -76dBm ± 2dBm@54Mbps(IGAP-620)<br>802.11b : -85dBm ± 2dBm@11Mbps<br>802.11g : -76dBm ± 2dBm@54Mbps<br>802.11gn HT20:-75dBm ± 2dBm@MCS7<br>802.11gn HT40:-72dBm ± 2dBm@MCS7<br>802.11an HT20:-74dBm ± 2dBm@MCS7(IGAP-620)<br>802.11an HT40:-71dBm ± 2dBm@MCS7(IGAP-620) |
| Encryption Security | WEP: (64-bit, 128-bit key supported)<br>WPA/WPA2:802.11i (WEP and AES encryption) |

| | |
|---|---|
| | WPA-PSK (256-bit key pre-shared key supported)<br>TKIP encryption |
| Wireless Security | SSID broadcast disable |
| LED Indicators | 3 x LEDs, PWR1(2)(PoE) / Ready:<br>1) Red On: Power is on and booting up.<br>2) Green On: Power is on and functioning normally.<br>2 x LEDs, ETH1(2)<br>Speed: Green for port Link at 1000Mbps<br>Amber for port Link at 100Mbps.<br>Off for port Link at 10Mbps<br>WLAN Link/ACT:<br>Green for WLAN<br>Fault indicator:<br>Red On: Ethernet link down or power down |
| **Power Requirements** | |
| Power Input Voltage | Dual DC inputs. 12~48VDC on 6-pin terminal block |
| Reverse Polarity Protection | Present |
| Power Consumption | 8.3 Watts |
| **Environmental** | |
| Operating Temperature | -10 to 60°C |
| Storage Temperature | -40 to 85°C |
| Operating Humidity | 5% to 95%, non-condensing |
| **Mechanical** | |
| Dimensions(W x D x H) | 74.3(W) x 109.2(D) x 153.6(H) mm<br>(2.93 x 4.3 x 6.05 inch.) |
| Casing | IP-30 protection |
| **Regulatory Approvals** | |
| EMI | FCC Part 15, CISPR (EN55022) class A |
| EMS | EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11 |
| Shock | IEC60068-2-27 |
| Free Fall | IEC60068-2-32 |
| Vibration | IEC60068-2-6 |
| Rail Traffic | EN60950-1 |

# Compliance

## FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

RF exposure warning: The equipment complies with RF exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment. This device should be operated with minimum distance 20cm between the device and all persons. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

## Industry Canada Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

*Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

Industry Canada - Class B This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

*Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matérial brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie.*

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

*L'opération est soumise aux deux conditions suivantes: (1) cet appareil ne peut causer d'interférences,et (2) cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer fonctionnement du dispositif.*

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

*Afin de réduire les interférences radio potentielles pour les autres utilisateurs, le type d'antenne et son gain doivent être choisie que la puissance isotrope rayonnée équivalente (PIRE) est pas plus que celle premise pour une communication réussie*

RF exposure warning: The equipment complies with RF exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

*Avertissement d'exposition RF: L'équipement est conforme aux limites d'exposition aux RF établies pour un incontrôlés environnement. L'antenne (s) utilisée pour ce transmetteur ne doit pas être co-localisés ou fonctionner en conjonction avec toute autre antenne ou transmetteur.*