TGAP-620(+)-/6620(+)-M12 Series

IEEE 802.11 a/b/g/n Access Point with Single/Dual RF

User Manual

Version 2.0

June, 2014

www.oring-networking.com

COPYRIGHT NOTICE

TRADEMARKS

ORing 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 Started

1.1 About the TGAP-620(+)-/6620(+)-M12 Series

The TGAP-620(+)-/6620(+)-M12 series are reliable outdoor WLAN access points with one (TGAP-620(+)-M12) or dual (TGAP-6620(+)-M12) 802.11 a/b/g/n wireless modules alongside two Gigabit LAN ports in M12 connectors. The two Ethernet ports allow you to form Daisy Chain structure to reduce the use of the ports. The series includes PoE models (TGAP-620+/6620+-M12) and non-PoE models (TGAP-620/6620-M12). With EN50155 compliance and M12 connectors to ensure tight and robust connections, the devices guarantee reliable operation against environmental disturbances, such as vibration and shock, and are ideal for rolling stock applications. The APs can be configured to operate in AP/Client/Bridge/AP-Client modes and support MAC filters for security control. The devices can be configured and managed via a Window utility or Web interface on LAN or WLAN networks.

1.2 Software Features

- High speed air connectivity with support up to 300Mbps
- Highly secure transmission with WEP/WPA/WPA2/Radius/TKIP supported
- Supports AP/Client/Bridge/AP-Client modes
- Supports Daisy Chain to reduce use of AP ports
- Secure management with HTTPS
- Event warning via Syslog, e-mail, SNMP traps, and relay

1.3 Hardware Features

- 2 x 10/100/1000 Base-T(X) Ethernet ports
- Supports PoE (TGAP-620+/6620+-M12 only)
- Operating temperature: -25 to 70°C
- Storage temperature: -40 to 85°C
- Operating humidity: 5% to 95%, non-condensing
- Dimensions(W x D x H): 125.6(W) x 65(D) x 196.1(H) mm

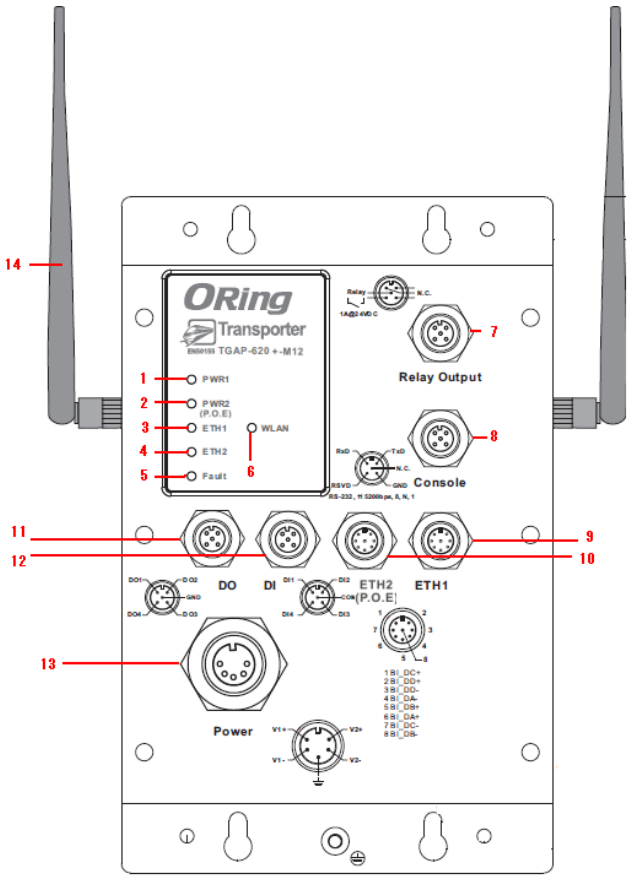
Hardware Overview

2.1 Front Panel

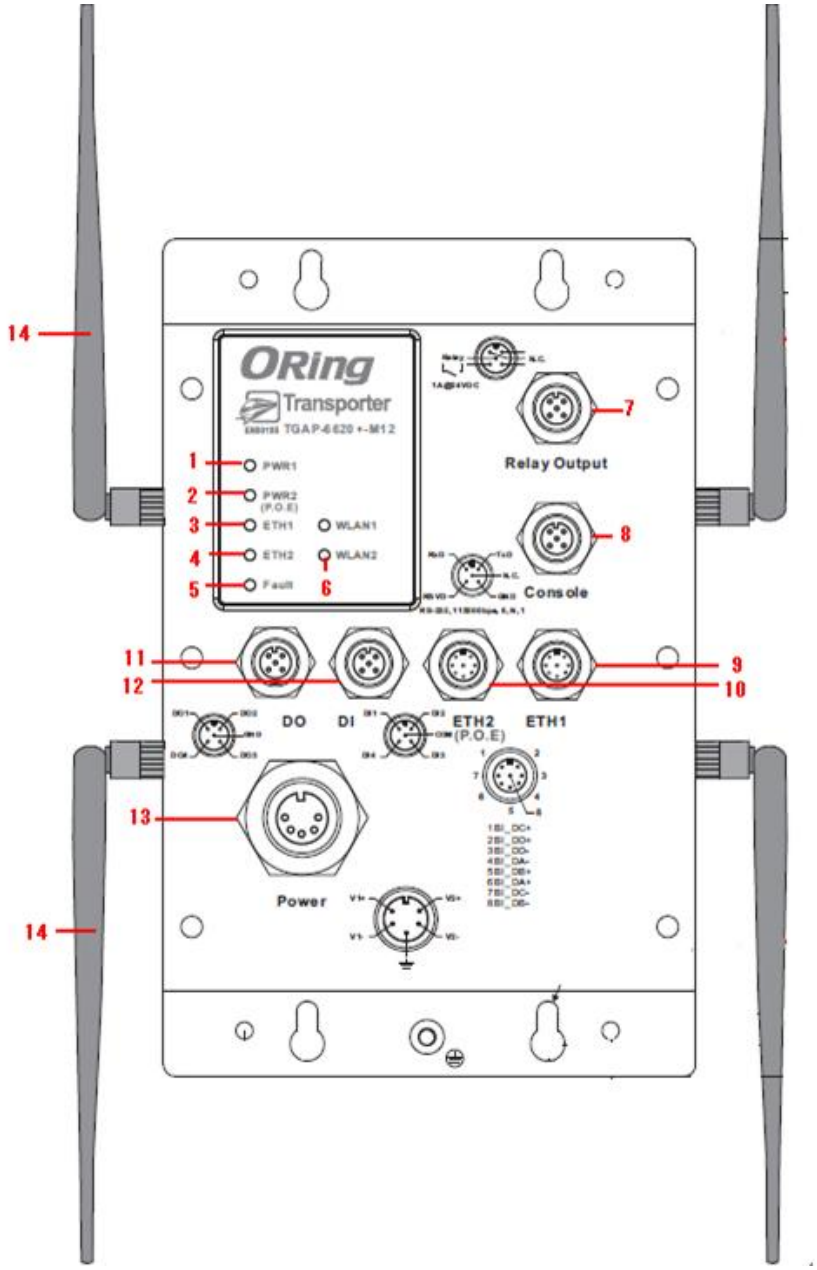
2.1.1 Ports and Connectors

The devices are equipped with the following ports and features on the front panel.

Port	Description
10/100/1000 Base-T(X) Ethernet ports with M12 connectors (A-coding)	2 x 10/100/1000 Base-T(X) ports supporting auto-negotiation.
Relay output with M12 (A-coding) connector	1 x relay output to carry capacity of 1A at 24VDC
M23 power connector with redundant power inputs	Dual power inputs for 12~48 VDC
DIDO with M12 connector (A-coding)	**4 x digital input / 4 x digital output** Dry Contact: On: short to GND, Off: open Wet Contact (DI to COM/GND): On: 0 to 3VDC, Off: 10 to 30VDC



TGAP-620+-M12



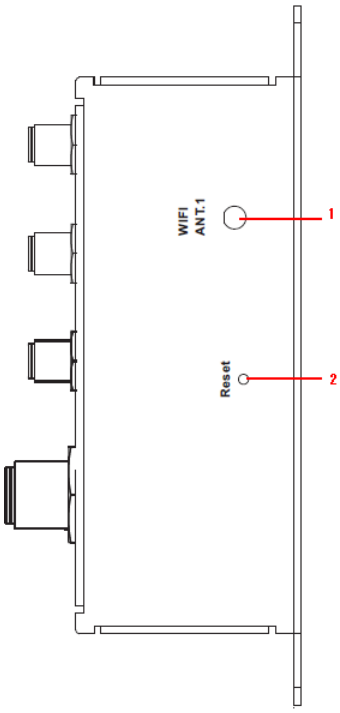
TGAP-6620+-M12

1. LED for PWR1 status
2. LED for PWR2 status (with PoE indicator)
3. LED for Ethernet port 1 status
4. LED for Ethernet port 2 status
5. LED for fault relay
6. LED for WLAN connection
8. Console port
9. Ethernet port 1
10. Ethernet port 2 (with PoE)
11. Digital output
12. Digital input
13. Power connector
14. 2.4/5GHz antenna

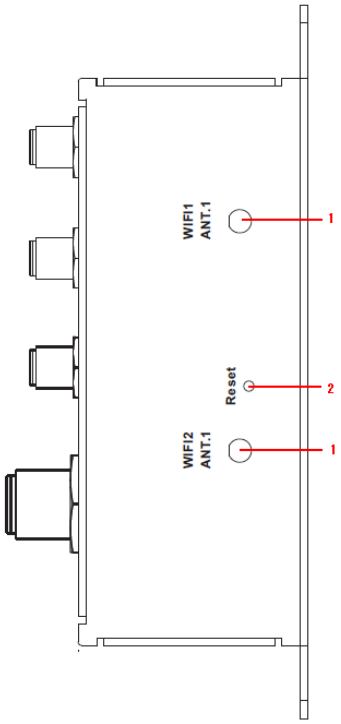
2.1.2 Front Panel LEDs

LED	Color	Status	Description
PWR1	Green	On	DC power 1 activated
PWR2 (PoE)	Green	On	DC power 2 activated or PoE enabled (when device is not connected to power supply)
ETH1	Green	On	Port is linked link
		Blinking	Transmitting data
ETH2	Green	On	Port is linked link
		Blinking	Transmitting data
WLAN (1/2)	Green	On	WLAN activated
		Blinking	Transmitting WLAN data
Fault	Red	On	Fault relay. Power failure or Port down/fail.

2.2 Side Panel



TGAP-620(+)-M12



TGAP-6620(+)-M12

1. Antenna connector
2. Reset button

Note: to restore the device configurations back to the factory defaults, press the Reset button for a few seconds. Once the power indicator starts to flash, release the button. The device will then reboot and return to factory defaults.

Hardware Installation

Before installing the devices, make sure you have all of the package contents available and a PC with Microsoft Internet Explorer 6.0 or later, for using web-based system management tools.

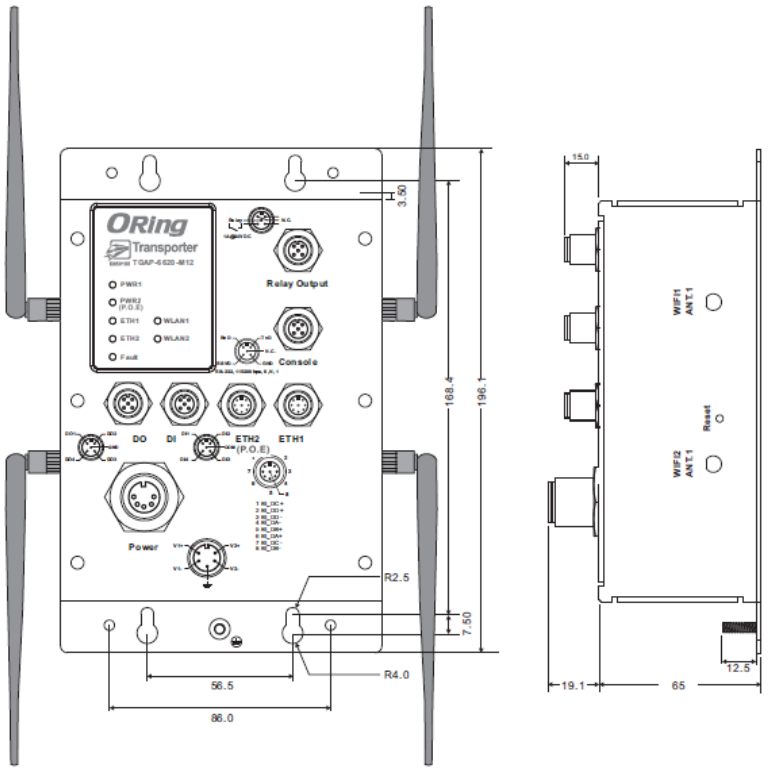
When installed outdoors, make sure the connectors on the panel are facing down to prevent water intrusion.

Do not remove the water-proof casing, and do not touch or move the device when the antennas are transmitting or receiving signals.

When installing the device, make sure to keep the radiating at a minimum distance of 20 cm (7.9 inches) from all persons to minimize the potential for human contact during normal operation.

Do not operate the device near unshielded blasting caps or in an otherwise explosive environment unless the device has been modified for such use by qualified personnel.

3.1 Wall Mounting Installation



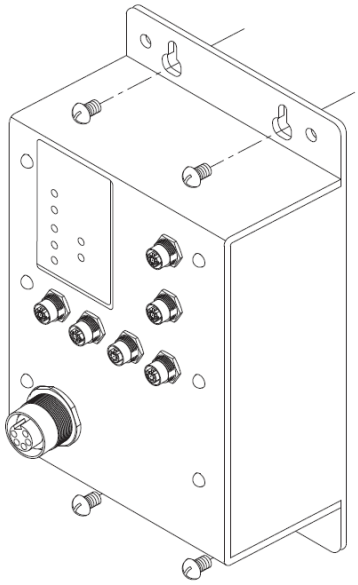
Wall-mount Measurements

The device can be fixed to the wall. Follow the steps below to install the device on the wall.

Step 1: Hold the AP upright against the wall

Step 2: Insert four screws through the large opening of the keyhole-shaped apertures at the top and bottom of the unit and fasten the screw to the wall with a screwdriver.

Step 3: Slide the AP downwards and tighten the four screws for added stability.



Instead of screwing the screws in all the way, it is advised to leave a space of about 2mm to allow room for sliding the AP between the wall and the screws.

3.2 Wiring

For pin assignments of power, console and relay output ports, please refer to the following tables.

3.2.1 Grounding

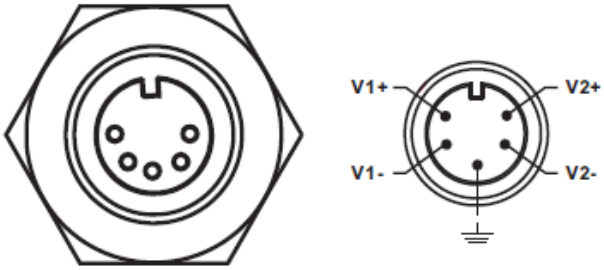
Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the grounding pin on the power connector to the grounding surface prior to connecting devices.

3.2.2 Power Port Pinouts

The device supports two sets of power supplies and uses the M23 5-pin female connector on the front panel for the dual power inputs.

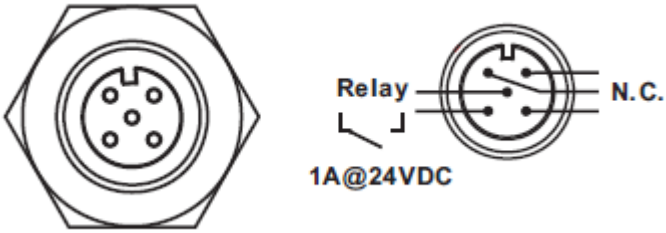
Step 1: Insert a power cable to the power connector on the device.

Step 2: Rotate the outer ring of the cable connector until a snug fit is achieved. Make sure the connection is tight.



3.2.3 Relay Output Port Pinouts

The APs use the M12 A-coded 5-pin male connector on the front panel for relay output. Use a power cord with an M12 A-coded 5-pin female connector to connect the relay. The relay contacts will detect user-configured events and form an open circuit when an event is triggered.

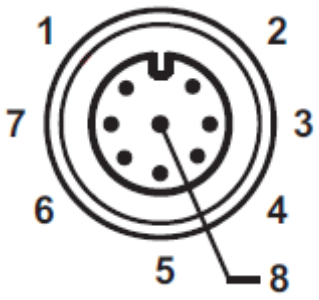


Cables and Antenna

4.1 Ethernet Pin Definition

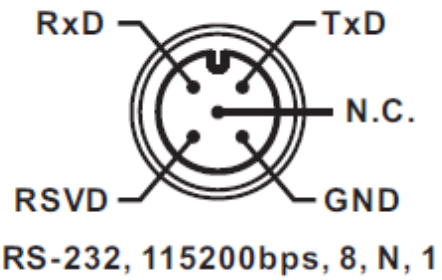
The AP has two 10/100/1000 Base-T(X) Ethernet ports. According to the link type, the AP uses CAT 3, 4, 5, 5e, UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable	Type	Max. Length	Connector
10Base-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	M12
100Base-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	M12
1000BASE-T	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	M12

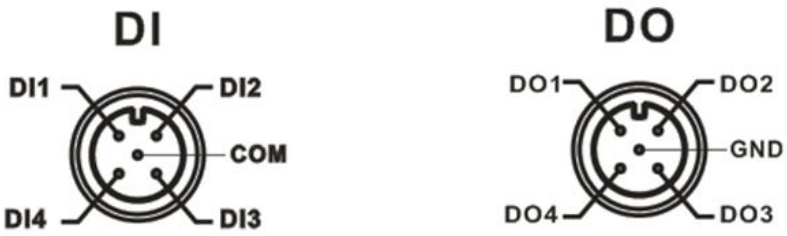


PIN	Definition
1	BI_DC+
2	BI_DD+
3	BI_DD-
4	BI_DA-
5	BI_DB+
6	BI_DA+
7	BI_DC-
8	BI_DB-

4.2 Console Port Pin Definition

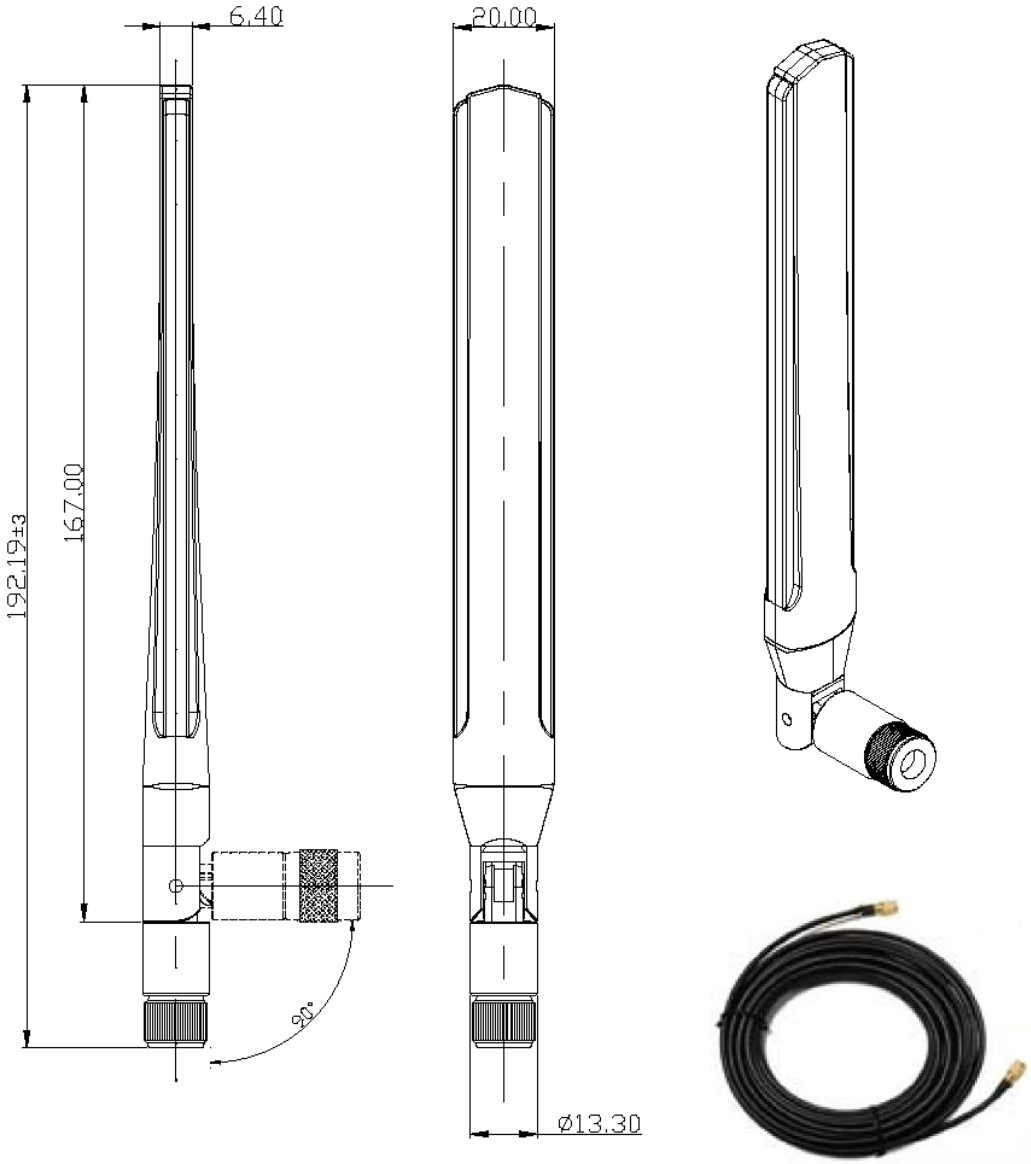


4.3 DI/DO



4.4 Wireless Antenna

The series uses 2.4GHz/5GHz antennas with reversed SMA connectors. You can also use external RF cables and antennas with the connectors.



Management

5.1 Network Connection

Before installing the device, you need to be able to access the device via a computer equipped with an Ethernet card or wireless LAN interface. To simplify the connection, it is recommended to use an Ethernet card to connect to a LAN.

Follow the steps below to install and connect the device to PCs:

Connect a computer to the device. Use either a straight-through Ethernet cable or cross-over cable to connect the LAN port of the device to a computer. Once the LED of the LAN port lights up, which indicates the connection is established, the computer will initiate a DHCP request to retrieve an IP address from the AP.

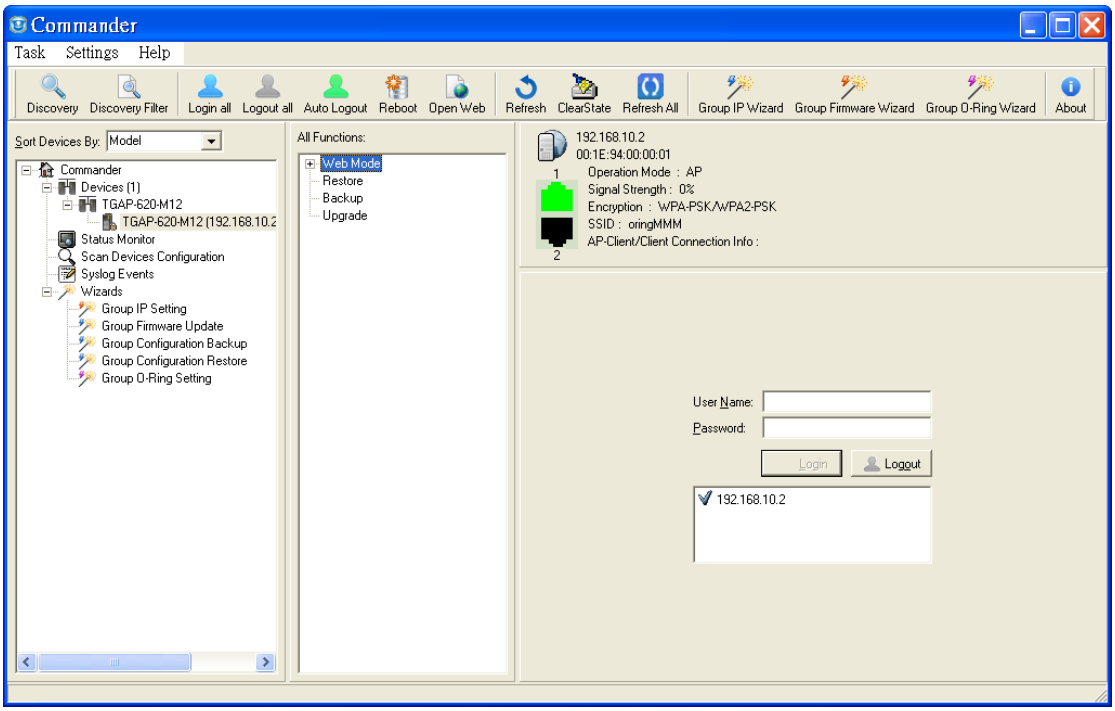
5.2 Open-Vision Configuration

The device can be configured using ORing's proprietary Windows utility Open-Vision. Follow the steps below to set up the device in Open-Vision.

Step 1: Open the commander and click **Discover**, a list of AP devices will be shown.

Step 2: Choose your access point. The functions of the AP will be shown in a tree structure.

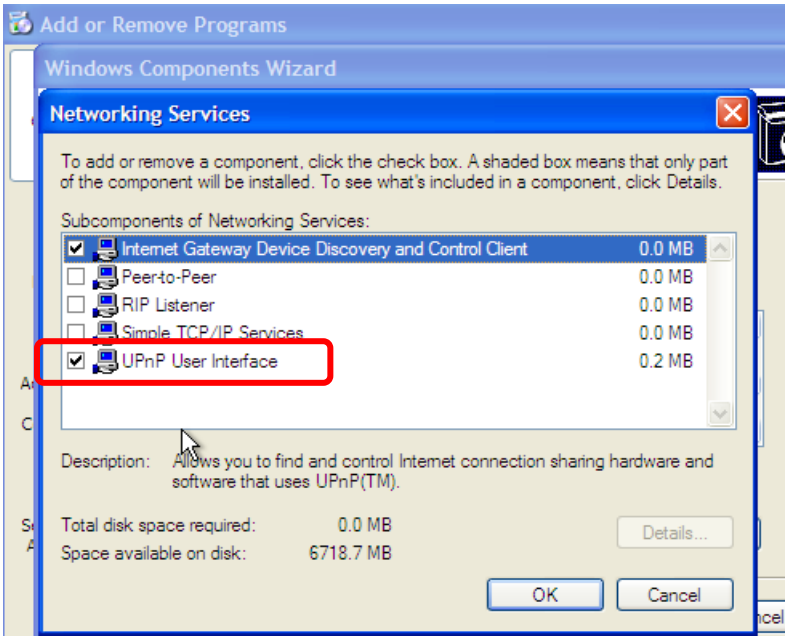
Step 3: Type in the username and password to log in to setup the AP.



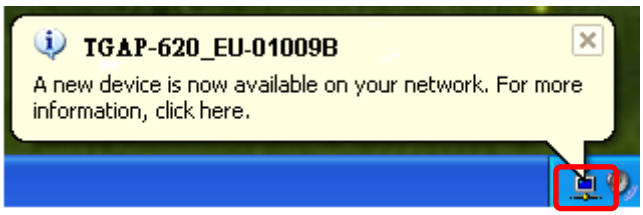
5.3 UPnP Equipment

The device supports UPnP; therefore, when you connect the device to the PC, it will discover the presence of the device automatically. To check the connection of the device to you PC, follow the steps below.

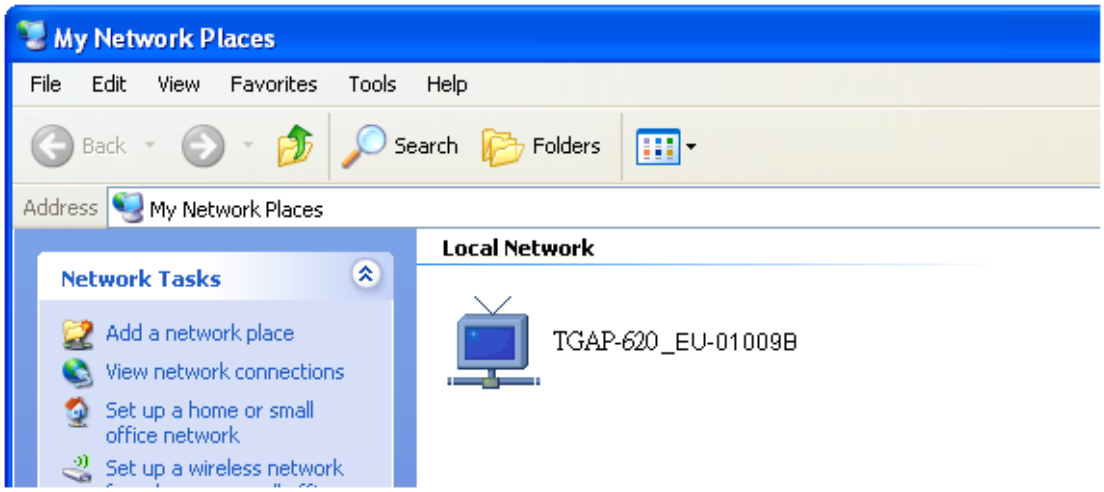
Step 1: Go to **Control Panel > Add or Remove Programs > Windows Components Wizard > Networking Servers > UPnP User Interface** and pitch on the UPnP User Interface.



Step 2: At the right-below corner of the computer, you will find an UPnP icon of the device.



Step 3: Click on the icon and you will find the UPnP device in **My Network Places**.



Step 4: Right click the UPnP device and choose **Properties**, the following picture will be shown.

Step 5: Double click the device icon will lead you to the management web page.

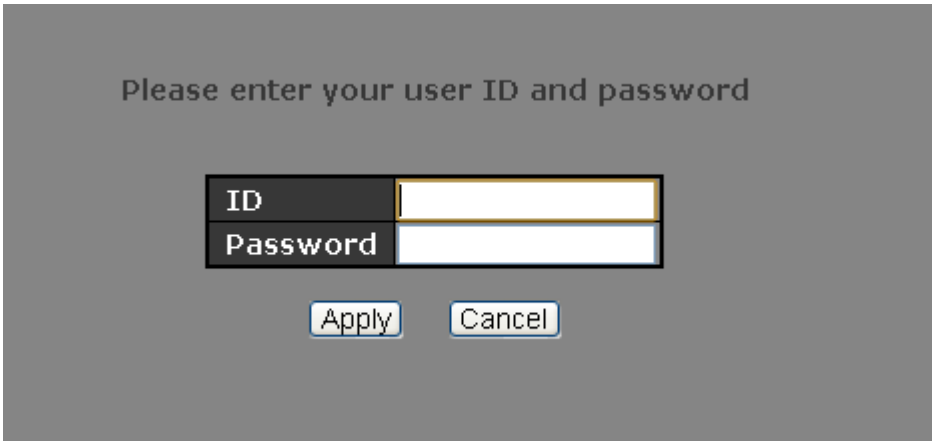
5.4 Web Browser Management

An embedded HTML web site resides in the flash memory of the device. It contains advanced management features which you can manage from anywhere on the network through a standard web browser such as Microsoft Internet Explorer (Internet Explorer 5.0 or later versions). It is based on Java Applets which can reduce network bandwidth consumption, enhance access speed, and provide user-friendly viewing windows.

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

Open a web browser on your computer and type http://192.168.10.2 (default gateway IP of the device) in the address box to access the webpage. A login window will pop up where you can enter the default login name admin and password **admin**. For security reasons, we strongly recommend you to change the password. Click on **Administrator > Password** after

logging in to change the password.



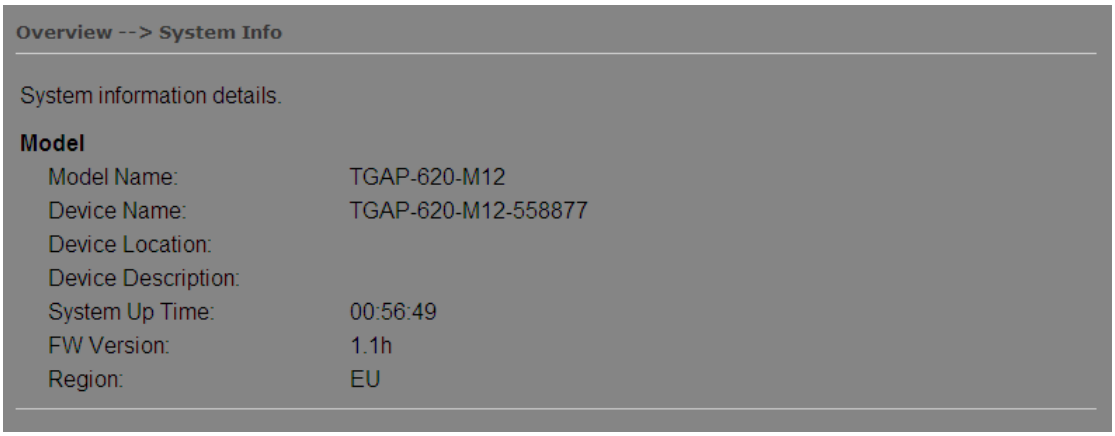
5.5 Configurations

The **Home** screen will appear with a short description of the device. You can lick **Run Wizard** on the page for quick configurations of a new password, wireless SSID and channel, and encryption.

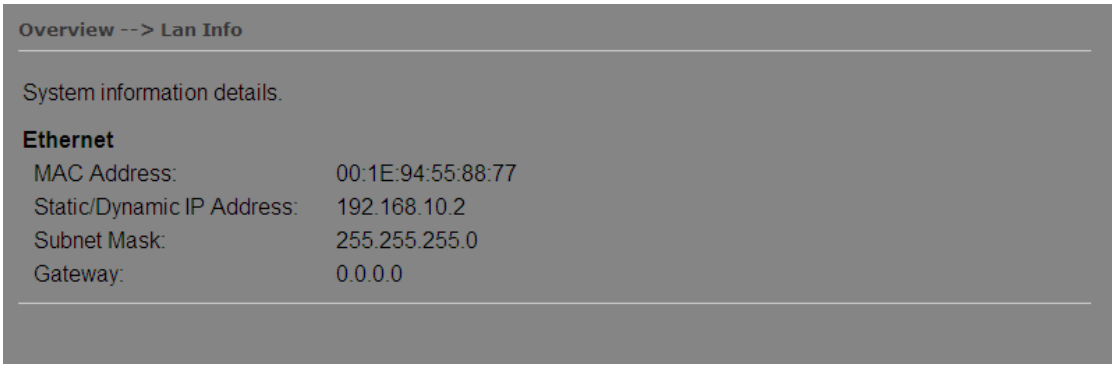
5.5.1 Overview

This setting will show the general information with regard to the device, including system information, LAN network information, and wireless network information.

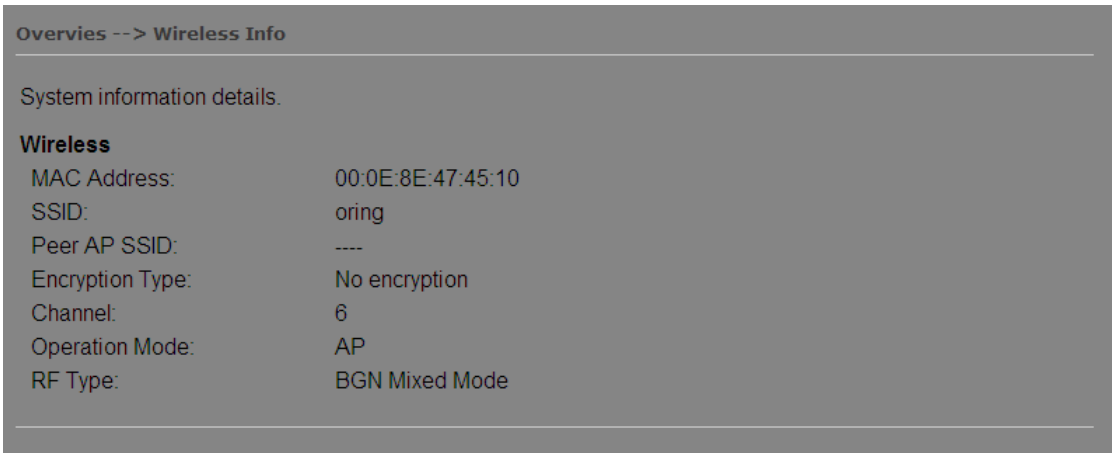
System Info



LAN Info



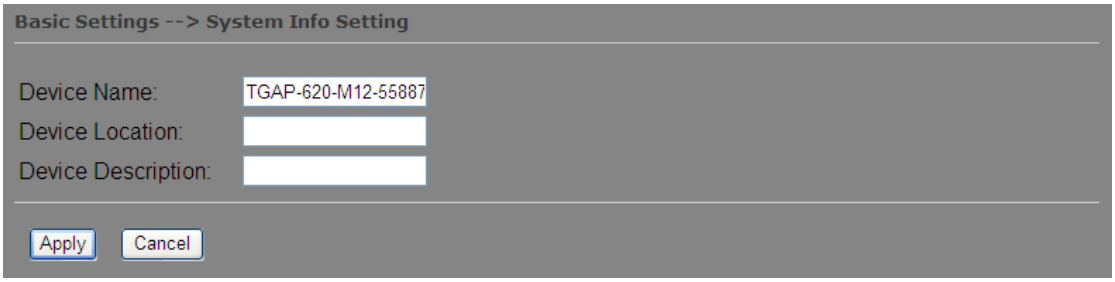
Wireless Info



5.5.2 Basic Setting

This section will allow you to configure the general settings for the device.

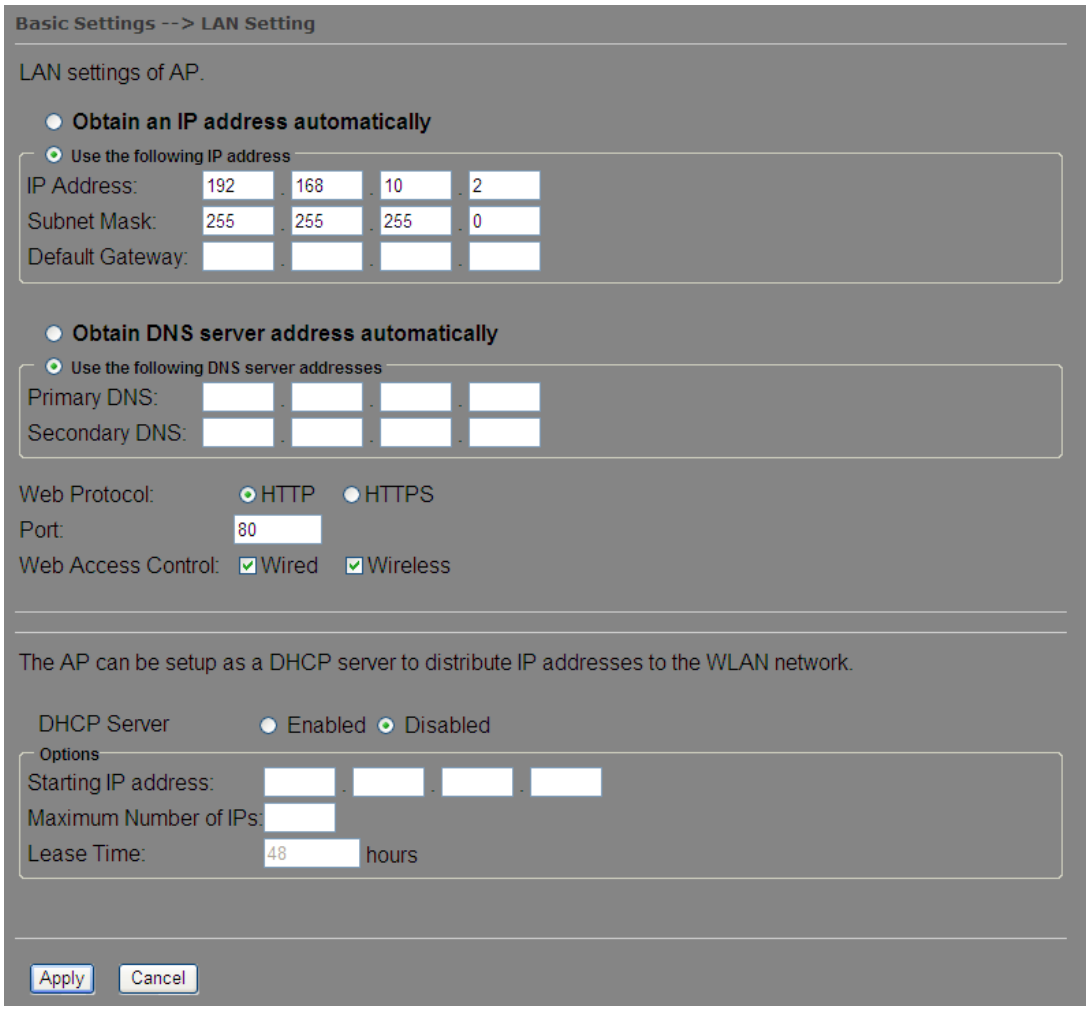
System Info Setting



Label	Description
Device Name	Define the name of the device
Device Location	Enter the location of the device
Device Description	Enter a description for the device

LAN Setting

This page allows you to configure the IP settings of the LAN port for the device.

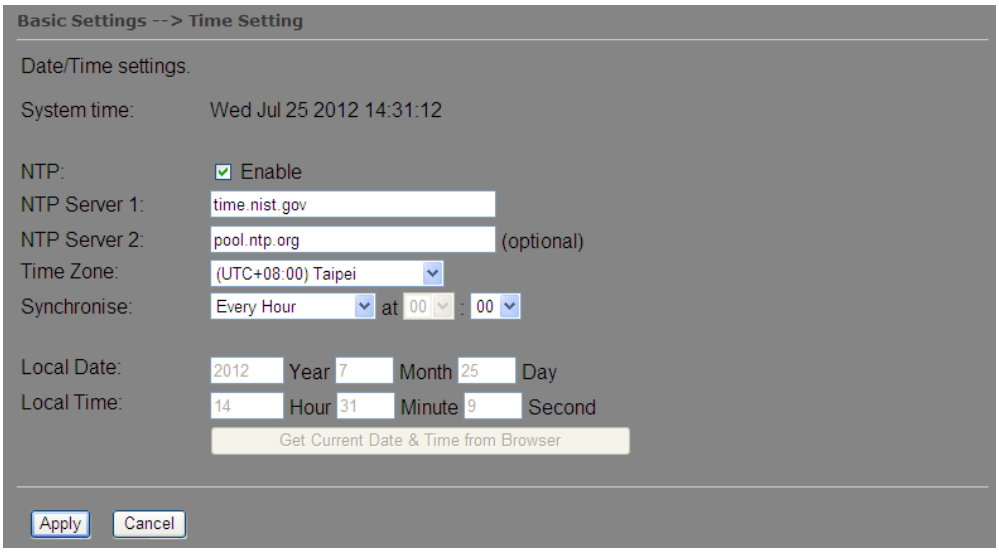


Label	Description
Obtain an IP address automatically	Select this option if you want the IP address to be assigned automatically by the DHCP server in your network.
Use the following IP address	Select this option if you want to assign an IP address to the device manually. You should set up IP address, subnet mask, and default gateway for the device. **IP Address:** The device comes with default IP address, but you can also input a new IP address. **Subnet Mask: 255.255.255.0** is the default value. All devices on the network must have the same subnet mask to communicate on the network.

	Default Gateway: Enter the IP address of the device in your network.
Obtain DNS server address automatically	Obtains a DNS server address from a DHCP server. If you have chosen to obtain an IP address automatically, this option will be selected accordingly.
Use the following DNS server addresses	Specifies a DNS server address manually. You can enter two addresses as the primary and secondary options.
Web Protocol	Choose a Web protocol for the device. The default value is **HTTP**. For higher security, choose **HTTPS**.
Port	Each Web protocol has a default port (HTTP is 80 and HTTPS is 443). You can also enter a value from 1 to 65535.
Web Access Control	You can choose to access the web page via wired or wireless connections.
DHCP Server	Enables or disables the DHCP server function. When enabled, the device will become the DHCP server on your local network.
Start IP Address	The starting IP address of the IP range assigned by the DHCP server. The start IP address is usually the lowest figures. For example, in a dynamic IP range from 192.168.1.100 to 192.168.1.200, 192.168.1.100 will be the start IP address.
Maximum Number of IPs	You can specify the number of IPs allowed to access the device. For example, if the dynamic IP range is from 192.168.1.100 to 192.168.1.200, you should enter **100** in this box.
Lease Time (Hour)	The period of time for an IP address to be leased. During the lease time, the DHCP server cannot assign that IP address to any other clients. Once the lease time ends, the system will reassign the IP address.

Time Setting

In this page, you can set the date & time of the device. A correct date and time will help the system log events. You can set up a NTP (Network Time Protocol) client to synchronize date & time to a NTP server on the Internet.



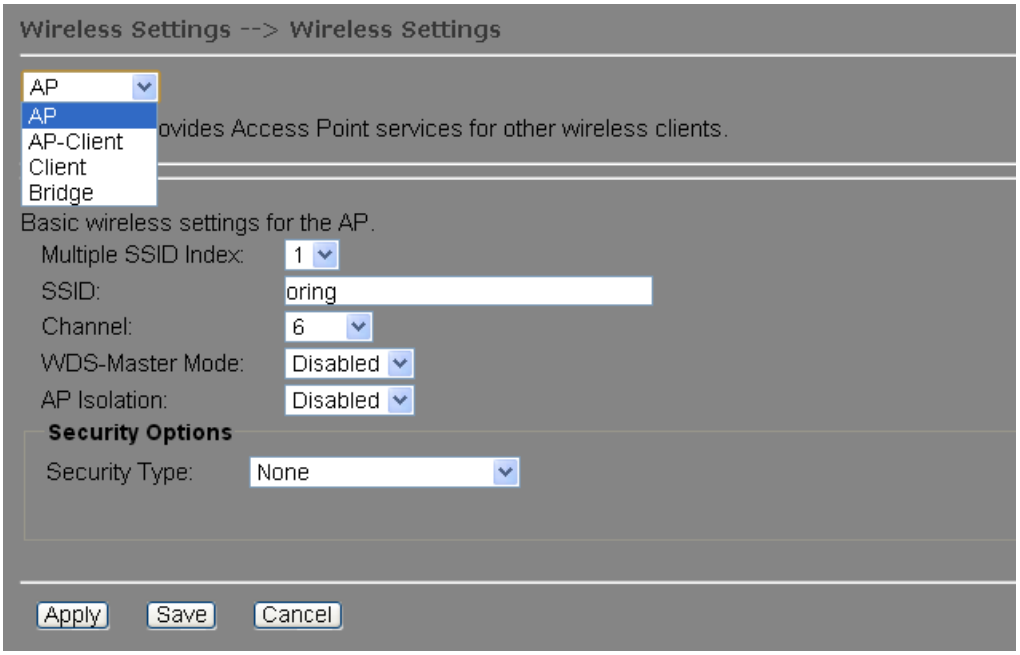
Label	Description
NTP	Enables or disables NTP function
NTP Server 1	The primary NTP server
NTP Server 2	The secondary NTP server
Time Zone	Select the time zone you are located in
Synchronize	Specify the scheduled time for synchronization
Local Date	Set a local date manually
Local Time	Set a local time manually
Get Current Date & Time from Browser	Click to set the time from your browser

DIDO

This page allows you to set up digital input/output for the device. Simply click on the radio button to activate or deactivate the function.

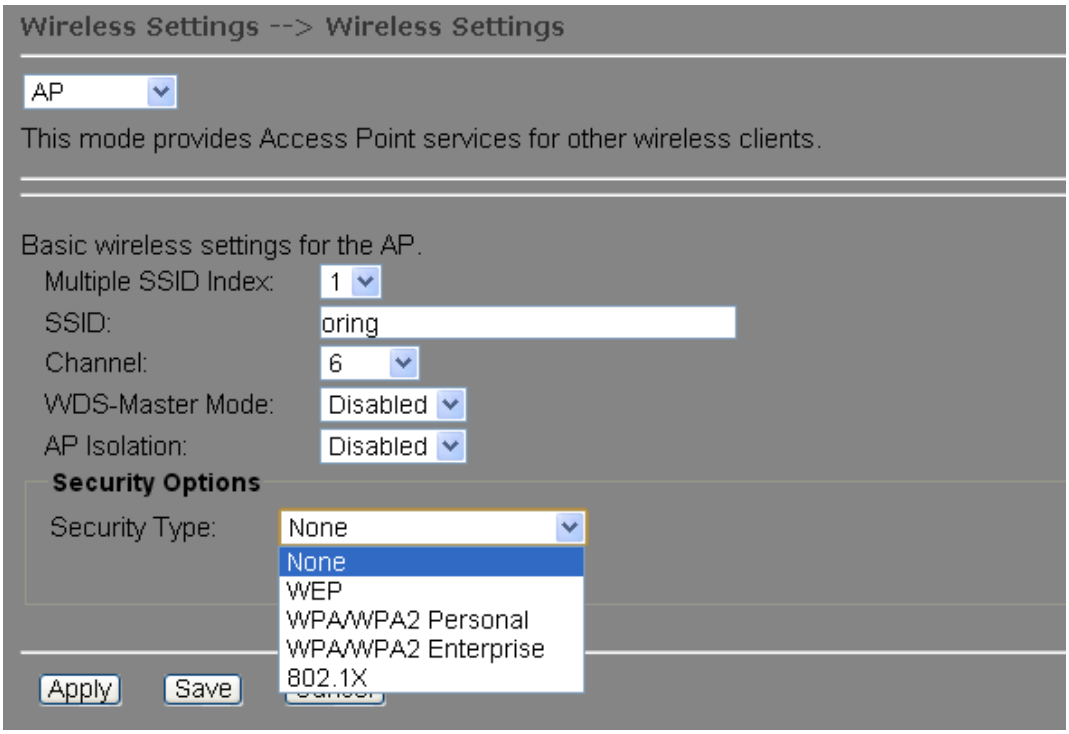
5.5.3 Wireless Setting

This section allows you to configure the wireless settings of the device when operating in different modes.



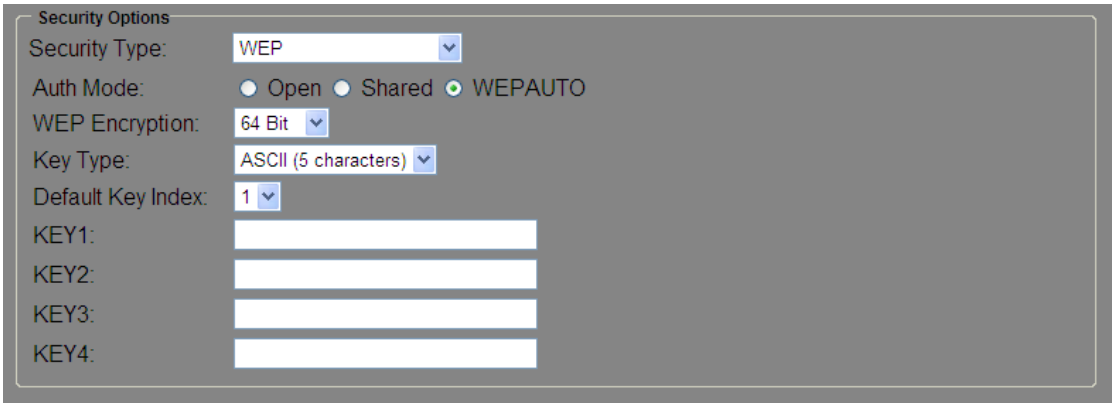
AP Mode

You can set the device to work in AP mode. This is the most common mode for all wireless APs. In this mode, the AP will act as a central connection point which other wireless clients can connect to.



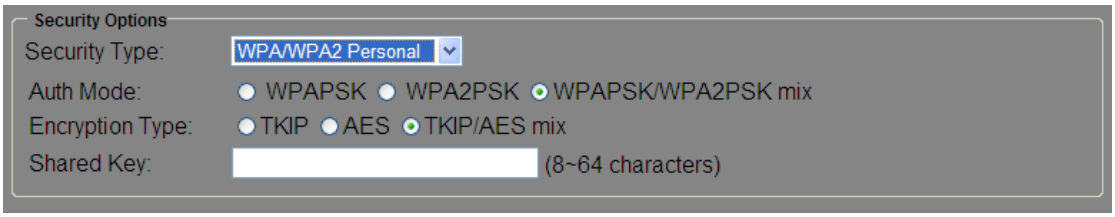
Label	Description
Multiple SSID index	The index of the SSID
SSID	SSID (Service Set Identifier) is a unique name that identifies a network. All devices on the network must be set with the same SSID in order to communicate with each other. Fill in a new SSID in this field if you do not want to use the default value.
Channel	Specify a channel to be used. **Channel 6** is the default channel. You can also select a new number from the dropdown list. All devices on the network must be set to use the same channel to communicate on the network.
WDS-Master Mode	A WDS master is the central control point for authenticating wireless clients, caching client key material, distributing MFP key material, reporting radio management information to an upstream network management station, and updating other APs participating in WDS. You can set the device as the WDS-master by selecting from the list.
AP Isolation	This function prevents devices connected to an AP from communicating directly with each other. This function is useful when many wireless clients request your network frequently.
Security options	You can choose the security type for your WLAN connection from the following options: **None**: no encryption **WEP**: WEP (Wired Equivalent Privacy) is a wireless security protocol for WLAN. WEP will encrypt data transmitted on the WLAN. **WPA/WPA2 Personal**: uses a pre-shared key for authentication. This pre-shared key is then dynamically sent between the AP and clients. Each authorized computer is given the same pass phrase. **WPA/WPA2 Enterprise**: this type includes all of the features of WPA/WPA2 Personal plus support for 802.1x RADIUS authentication. **802.1x**: authentication through a RADIUS server

When you set security type as **WEP**, the following fields will appear to allow you to configure individual settings.



Label	Description
Auth Mode	Available values include **Open**, **Shared**, and **WEPAUTO**. When choosing **Open** or **Shared**, all of the clients must select the same authentication to associate this AP. If select **WEPAUTO**, the clients do not have to use the same **Open** or **Shared** authentication. They can choose any one to authenticate.
WEP Encryption	You can select **64 Bit** or **128 Bit**.
Key Type	Available values include **ASCII** and **Hex Key Type**. ASCII (American Standard Code for Information Interchange) is a code for representing English characters as numbers in the range from 0 to 127. Hex digits uses 0–9 to represent values zero to nine, and characters A-F to represent values ten to fifteen.
Default Key Index	Select one of the keys to be the active key
Key 1 to 4	You can input up to four encryption keys.

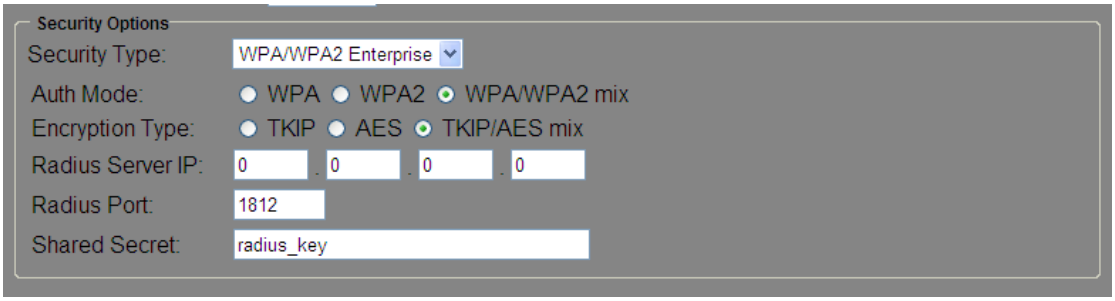
When you set security type as **WPA/WPA2-Personal**, the following fields will appear to allow you to configure individual settings.



Label	Description
Auth Mode	Available values include **WPAPSK**, **WPA2PSK**, and **WPAPSK/WPA2PSK mix.** WPAPSK and WPA2PSK will

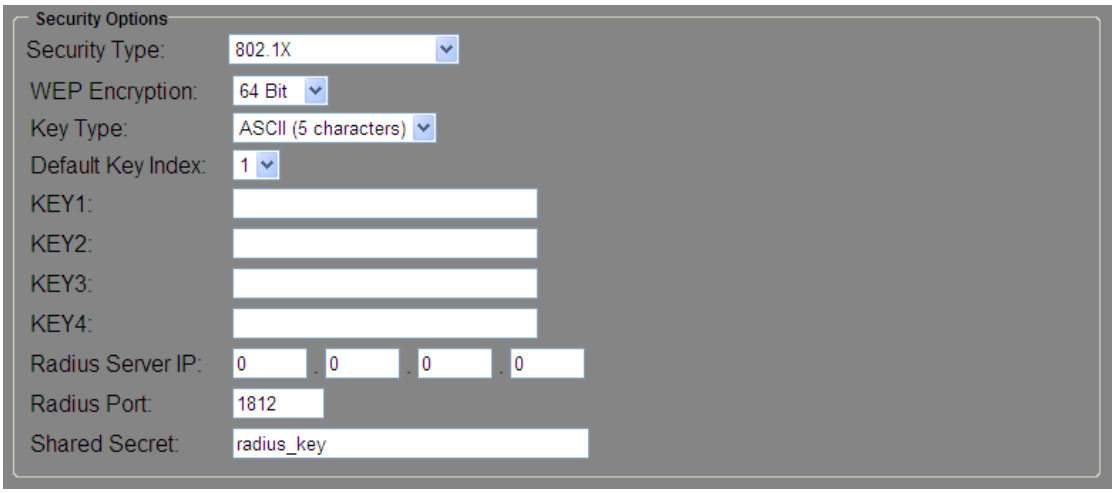
	encrypt the link without additional RADIUS server, only an access point and client station that supports WPA-PSK is required. For WPA/WPA2, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.
Encryption Type	Available values include **TKIP**, **AES**, and **TKIP/AES mix**. WPA-PSK uses TKIP encryption, and WPA2-PSK uses AES encryption. TKIP/AES provides the most reliable security, and is easiest to implement.
Shared Key	Enter a pass phrase in this field. The value must be within 8 to 64 characters

When you set security type as **WPA /WPA2 Enterprise**, the following screen will appear to allow you to configure individual settings.



Label	Description
Auth Mode	Available values include **WPAPSK**, **WPA2PSK**, and **WPAPSK/WPA2PSK mix.** WPAPSK and WPA2PSK will encrypt the link without additional RADIUS server, only an access point and client station that supports WPA-PSK is required. For WPA/WPA2, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.
Encryption Type	Available values include **TKIP**, **AES**, and **TKIP/AES mix**. WPA-PSK uses TKIP encryption, and WPA2-PSK uses AES encryption. TKIP/AES provides the most reliable security, and is easiest to implement.
Radius Server IP	Enter the IP address of the RADIUS server
Radius Port	Enter the RADIUS port (default is 1812)
Shared Secret	Enter the RADIUS password or key

When you set security type as **802.1x**, the following fields will appear to allow you to configure individual settings.

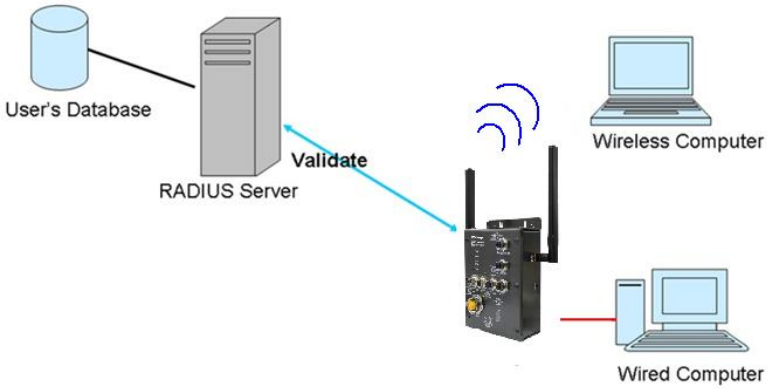


Label	Description
WEP Encryption	You can select **64 Bit** or **128 Bit**.
Key Type	Available values include **ASCII** and **Hex Key Type**. ASCII (American Standard Code for Information Interchange) is a code for representing English characters as numbers in the range from 0 to 127. Hex digits uses 0–9 to represent values zero to nine, and characters A-F to represent values ten to fifteen.
Default Key Index	Select one of the keys to be the active key
Key 1 to 4	Input up to four encryption keys
Radius Server IP	Enter the IP address of the RADIUS server
Radius Port	Enter the RADIUS port (default is **1812**)
Shared Secret	Enter the RADIUS password or key

RADIUS (Remote Authentication Dial-In User Service) is a widely deployed protocol that enables companies to authenticate and authorize remote users' access to a system or service from a central network server.

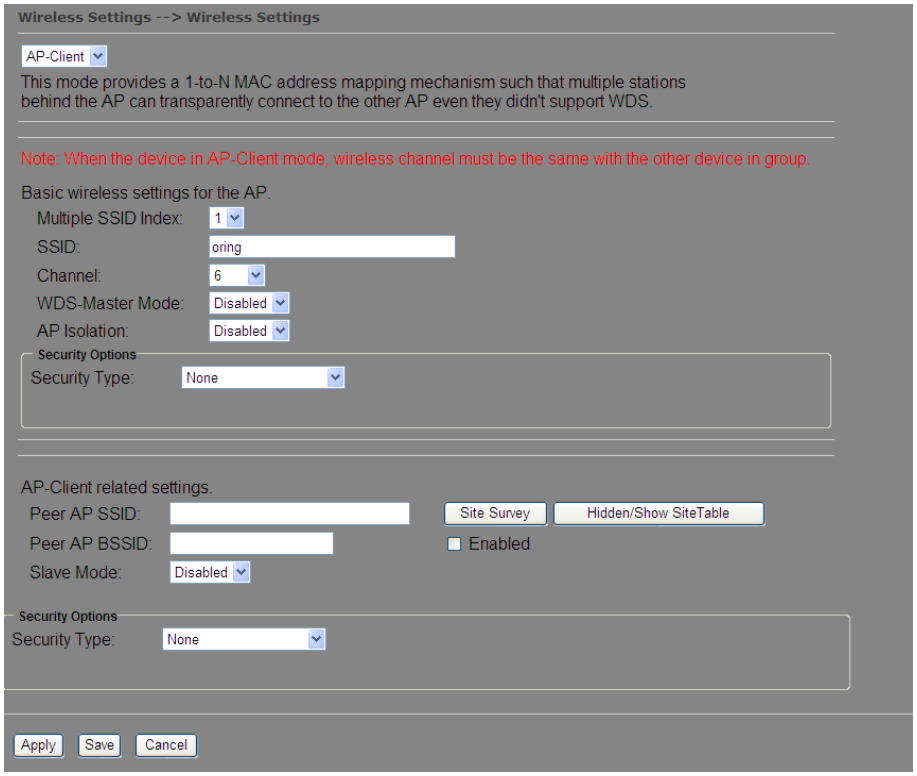
When you configure the remote access server for RADIUS authentication, the credentials of the connection request are passed to the RADIUS server for authentication and authorization. If the request is both authenticated and authorized, the RADIUS server sends an accept message back to the remote access server and the connection attempt is accepted. If the request is either not authenticated or not authorized, the RADIUS server sends a reject message back to the remote access server and the connection attempt is rejected.

The principle of the Radius server is shown 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 if they don't support WDS.

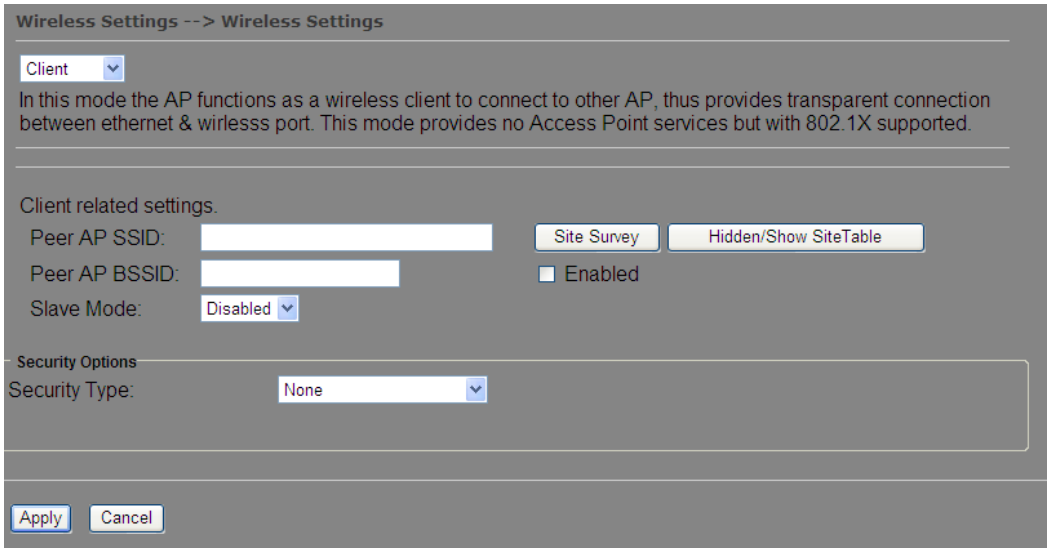


Label	Description
SSID	SSID (Service Set Identifier) is a unique name that identifies a network. All devices on the network must be set with the same SSID in order to communicate with each other. Fill in a new SSID in this field if you do not want to use the default value.
Channel	Specify a channel to be used. Channel 6 is the default channel. You can also select a new number from the dropdown list. All devices on

	the network must be set to the same channel to communicate on the network. (**Wireless channel must be the same as the other device in the group**)
WDS-Master Mode	A WDS master is the central control point for authenticating wireless clients, caching client key material, distributing MFP key material, reporting radio management information to an upstream network management station, and updating other APs participating in WDS. You can set the device as the WDS-master by selecting from the list.
Security options	You can choose the security type for your WLAN connection from the following options: **None**: no encryption **WEP**: WEP (Wired Equivalent Privacy) is a wireless security protocol for WLAN. WEP will encrypt data transmitted on the WLAN. **WPA/WPA2 Personal**: uses a pre-shared key for authentication. This pre-shared key is then dynamically sent between the AP and clients. Each authorized computer is given the same pass phrase.
Peer AP SSID	Enter the SSID of the AP you want to connect as a client
Peer AP BSSID	Enter the BSSID (Wireless MAC address) to limit client target
Slave Mode	Enables or disables slave mode
Site Scan	You can scan APs on the network using this mode.
Security Type	Select the security type used by the client you want to connect

Client Mode

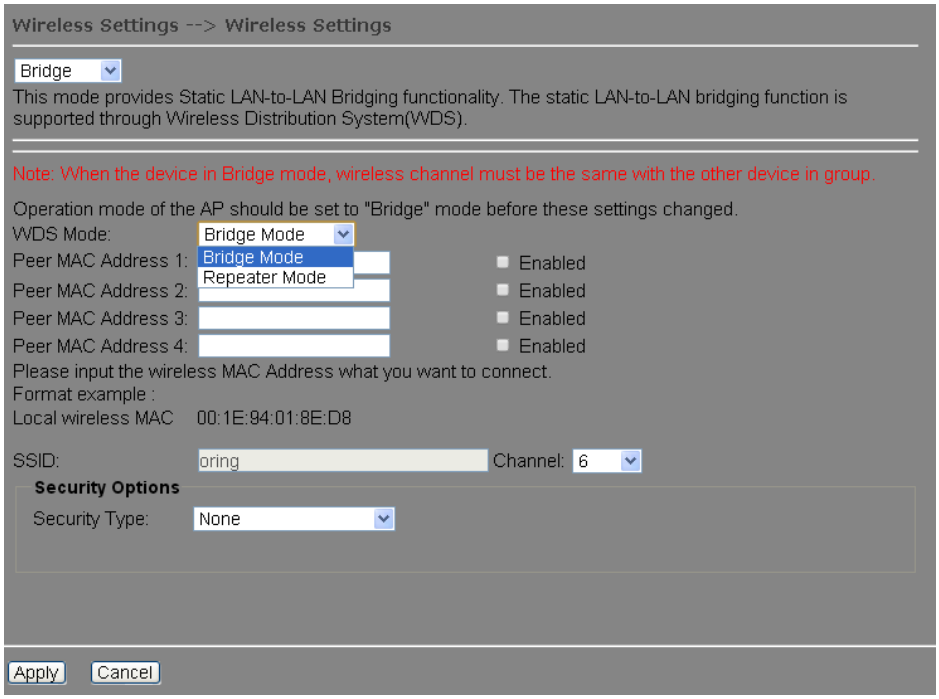
In this mode, the AP functions as a wireless client to connect your wired devices to a wireless network. This mode provides no access point services but supports 802.1X.



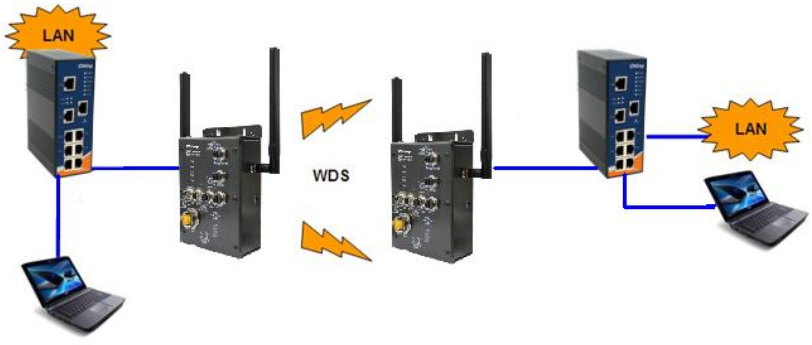
Label	Description
Peer AP SSID	Enter the SSID of the AP you want to connect as a client
Peer AP BSSID	Enter the BSSID (Wireless MAC address) to limit client target
Site Scan	Enables or disables slave mode
WDS-Slave Mode	You can scan APs on the network using this mode.
Security Type	Select the security type used by the client you want to connect

Bridge Mode

Select this option if the device is connected to a local network downstream from another router. In this mode, the device functions as a bridge between the network on its WAN port and the devices on its LAN port and those connected to it wirelessly.



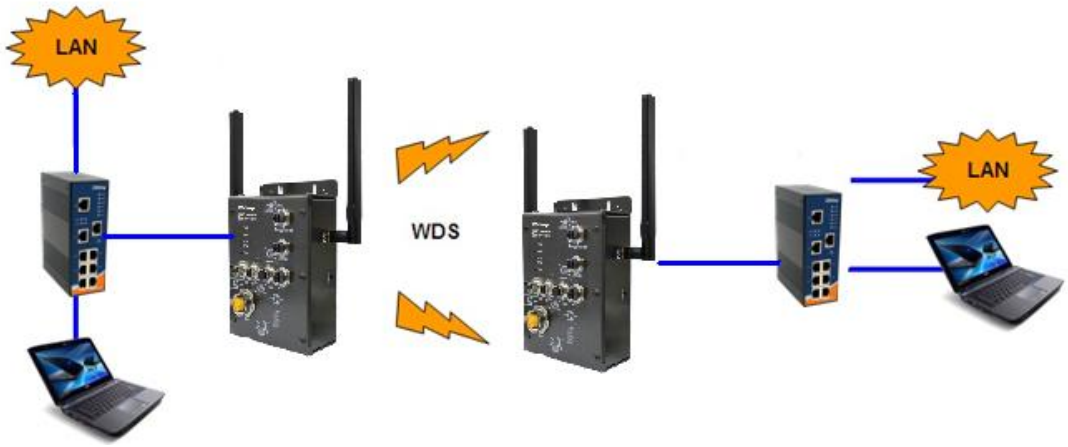
This type of wireless link is established between two IEEE 802.11 access points. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.



Label	Description
WDS Mode	This mode provides static LAN-to-LAN bridging functionality, which is supported through WDS. WDS enables access points or routers to be wirelessly connected to one another. This function is usually used in large, open areas such as warehouses where wiring is restricted or costly, and in some larger home environments.
Peer MAC Address	Enter the Mac address of other access point(s) and check the **Enable** box.
SSID (only Repeater mode support)	SSID (Service Set Identifier) is a unique name that identifies a network. All devices on the network must be set with the same SSID in order to communicate with each other. Fill in a new SSID in this field if you do not want to use the default value.
Channel	Specify a channel to be used. Channel 6 is the default channel. You can also select a new number from the dropdown list. All devices on the network must be set to the same channel to communicate on the network. (**Wireless channel must be the same as the other device in the group**)
Security options	You can choose the security type for your WLAN connection from the following options: **None**: no encryption **WEP**: WEP (Wired Equivalent Privacy) is a wireless security protocol for WLAN. WEP will encrypt data transmitted on the WLAN. **WPA/WPA2 Personal**: uses a pre-shared key for authentication. This pre-shared key is then dynamically sent between the AP and clients. Each authorized computer is given the same pass phrase.

Set WDS as Bridge Mode

In the mode, the AP acts as a standard bridge that forwards traffic between WDS links (links connected 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 wired and wireless network devices, which are connected to their respective Ethernet ports to limit the amount of forwarded data. 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. The peer WDS APs are based on the MAC addresses listed in **Peer Mac Address**.



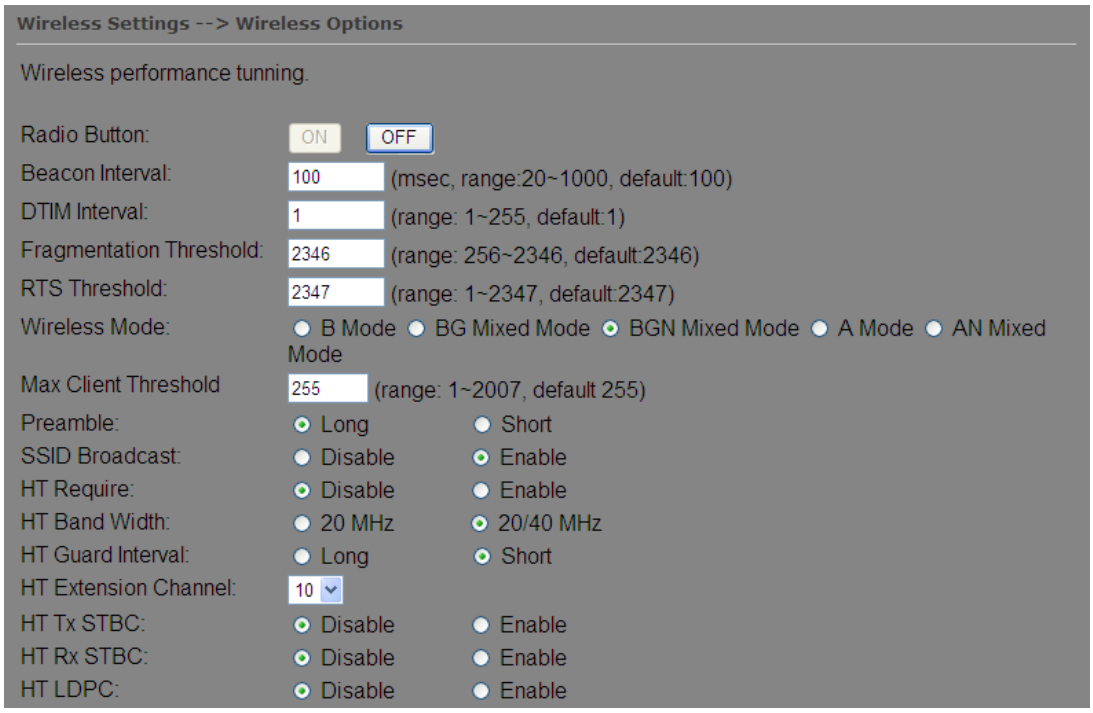
Bear in mind the following principles when setting the WDS mode to bridge mode:

1. LAN IP address should use a different IP in the same network.
2. Shut down all DHCP server functions of the AP.
3. Enable WDS.
4. Each AP should have the same setting, except **Peer Mac Address** should be set to the other's Mac address.
5. The settings of security and channel must be the same.
6. The distance of the AP should be limited within a certainty area.

Set WDS as Repeater Mode

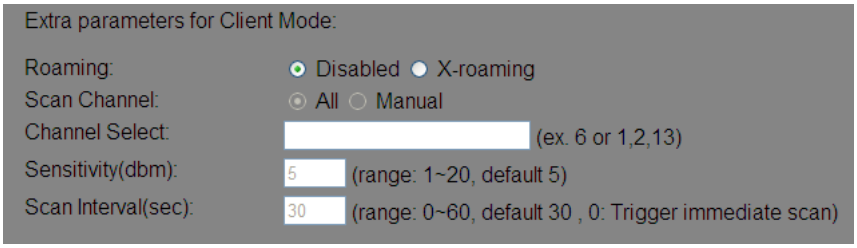
In this mode, repeater is used to extend the range of the wireless infrastructure by forwarding traffic between associated wireless stations and another repeater or AP connected to the wired LAN. The peer WDS APs are based on the MAC addresses listed in **Peer Mac Address**.

Wireless Options



Label	Description
Radio Button	Enables or disables wireless functions
Beacon Interval	A beacon is a packet sent by a wireless access point to synchronize wireless devices. The beacon interval value indicates the frequency interval of the beacon. Increasing the beacon interval reduces the number of beacons and the overhead associated with them. The default value is **100**, but **50** is recommended when reception is poor.
DTIM Interval	The value specifies the maximum size for a packet before data is fragmented into multiple packets. The value should remain at the default **2346** (the range is 256 - 2346 bytes). If you experience a high packet error rate, you may slightly increase the value. Setting the value too low may result in poor network performance. Only minor modifications of this value are recommended.
Fragmentation Threshold	The RTS (Request to Send) Threshold is the amount of time a wireless device, attempting to send, will wait for a recipient to acknowledge that it is ready. Normally, the AP sends a RTS frame to a station and negotiates the sending of data. After receiving the RTS, the station responds with a CTS (Clear to Send) frame to acknowledge the right to begin transmission. To ensure communication, the maximum value should be used, which is the

	default value **2347** (the range is 0-2347 bytes). If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled.
RTS Threshold	You can select 802.11 b, b/g, or b/g/n mode.
Wireless Network Mode	Available values include **Long** and **Short**, with **Long** as the default value. If all clients and access points in your wireless network support short preamble, then enabling it can boost overall throughput. However, if any wireless device does not support short preamble, then it will not be able to communicate with your network. If you are not sure whether your radio supports the short RF preamble, you must disable this feature.
Preamble	The value specifies the maximum size for a packet before data is fragmented into multiple packets. The value should remain at the default **2346** (the range is 256 - 2346 bytes). If you experience a high packet error rate, you may slightly increase the value. Setting the value too low may result in poor network performance. Only minor modifications of this value are recommended.



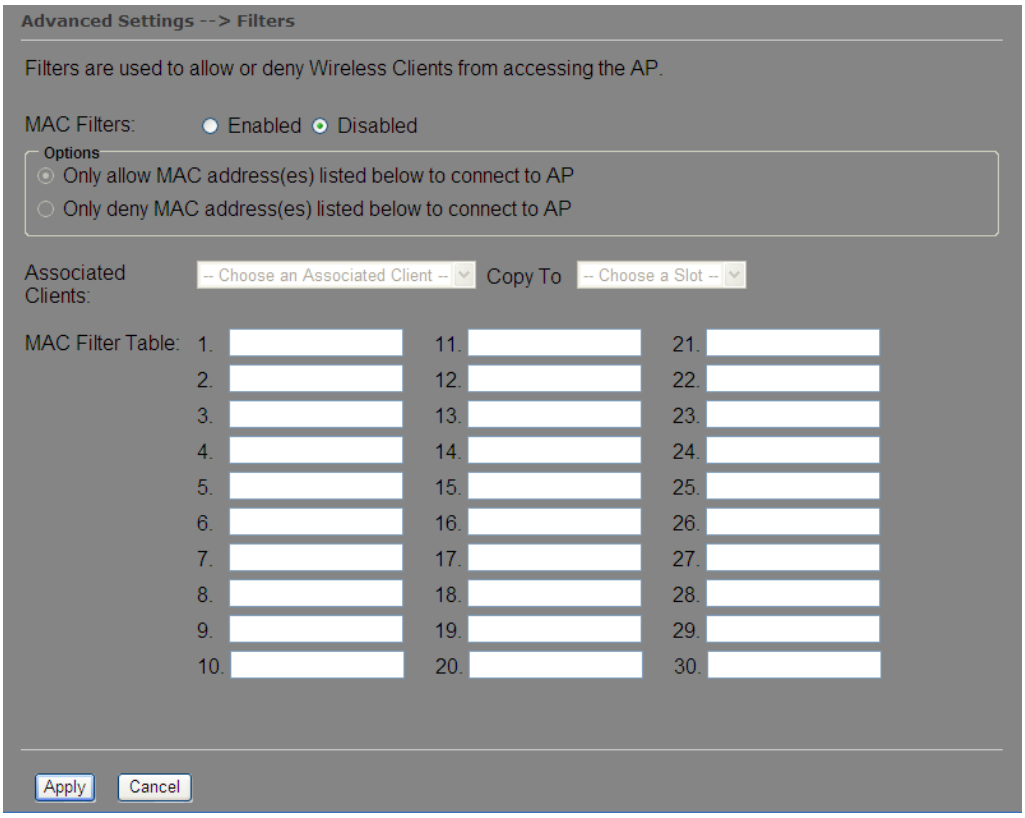
Label	Description
Roaming	Select **Disabled** to disable X-Roaming protocol or select **X-roaming** to enable X-Roaming protocol
Scan channel	Select **All** to scan all supported channels or **Manual** to scan only selected channels specified in Channel Select**.**
Channel Select	Assign the value roaming channels
Sensitivity	Configures signal sensitivity
Scan interval	Configures scan interval

5.5.4 Advanced Setting

Filters

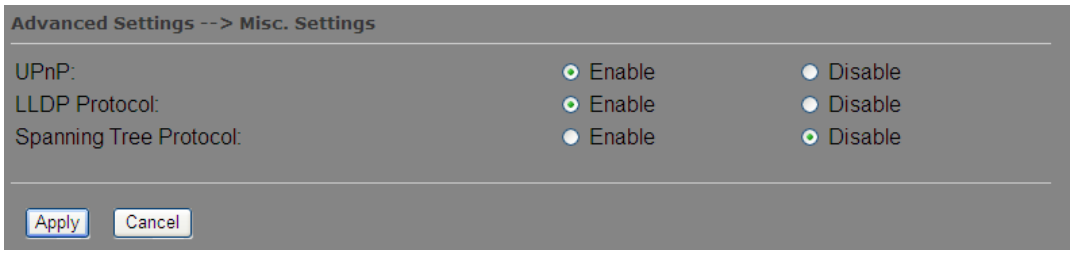
This page allows you to set up MAC filters to allow or deny wireless clients to connect to the AP. You can manually add a MAC address or select a MAC address from the Associated

Clients list currently associated with the AP.



Label	Description
MAC Filter	Select **Enabled** or **Disabled** to activate or deactivate MAC filters
Options	Select one of the options to allow or deny the MAC address in the list
Associated Clients	Shows the wireless MAC addresses associated with the device
MAC Filter Table	You can edit up to MAC addresses in these fields
Apply	Click to activate the configurations

Misc. Settings



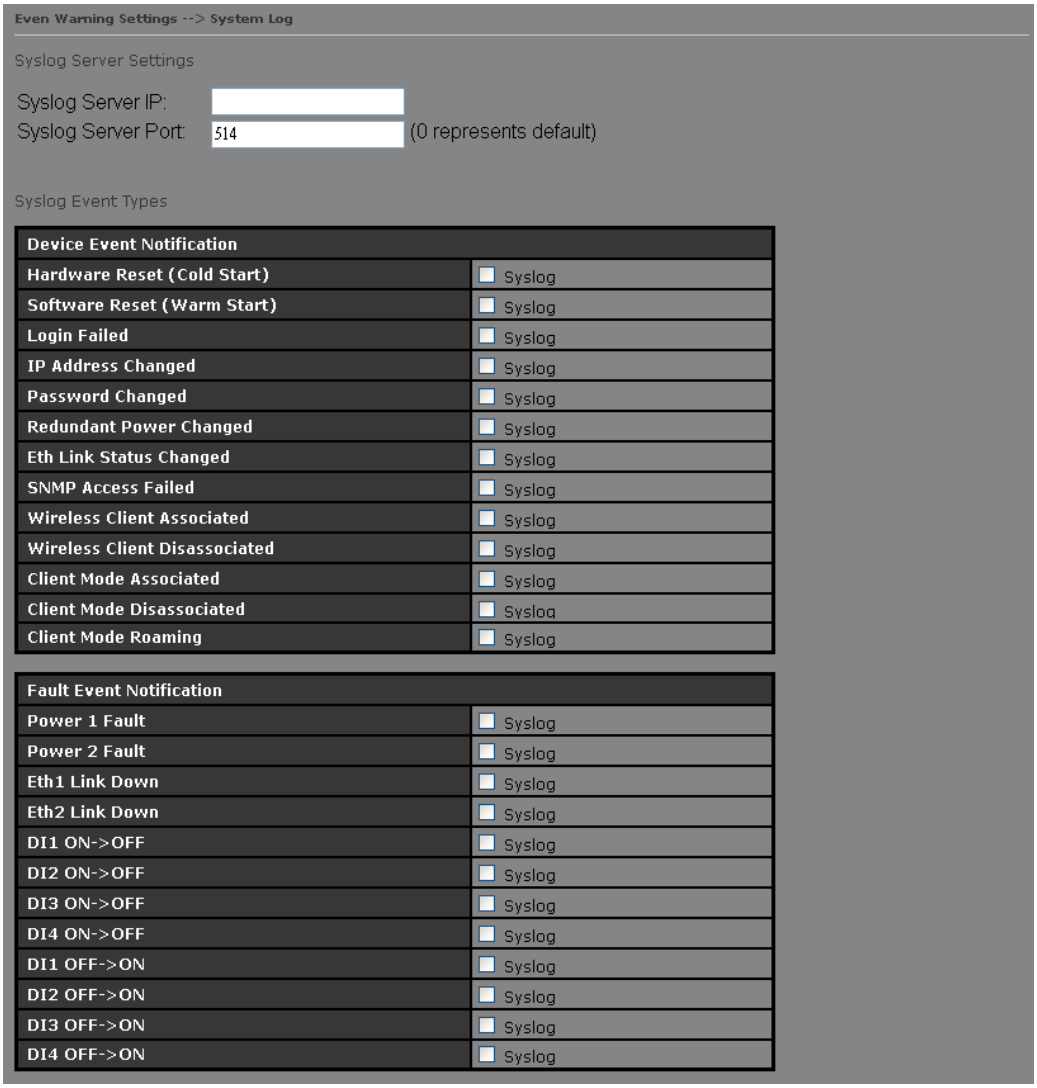
Label	Description
UPnP	Enables or disables UPnP function

LLDP Protocol	Enables or disables LLDP protocol
Spanning Tree Protocol	Enables or disables STP function

5.5.5 Event Warning Settings

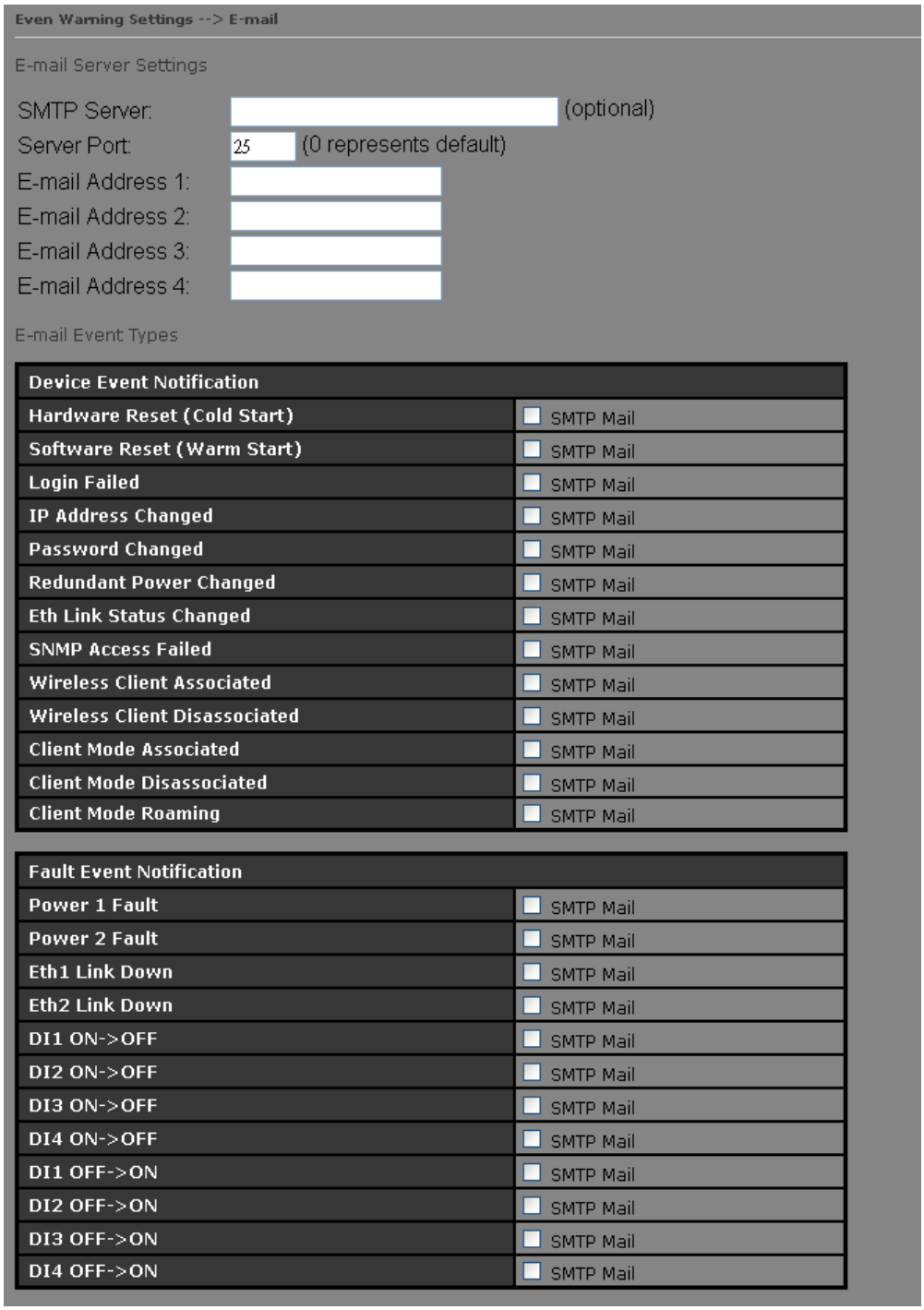
When an error occurs, the device will notify you through system log, e-mail, SNMP, and relay. You can choose the system to issue a notification when specific events occur by checking the box next to the event.

System Log



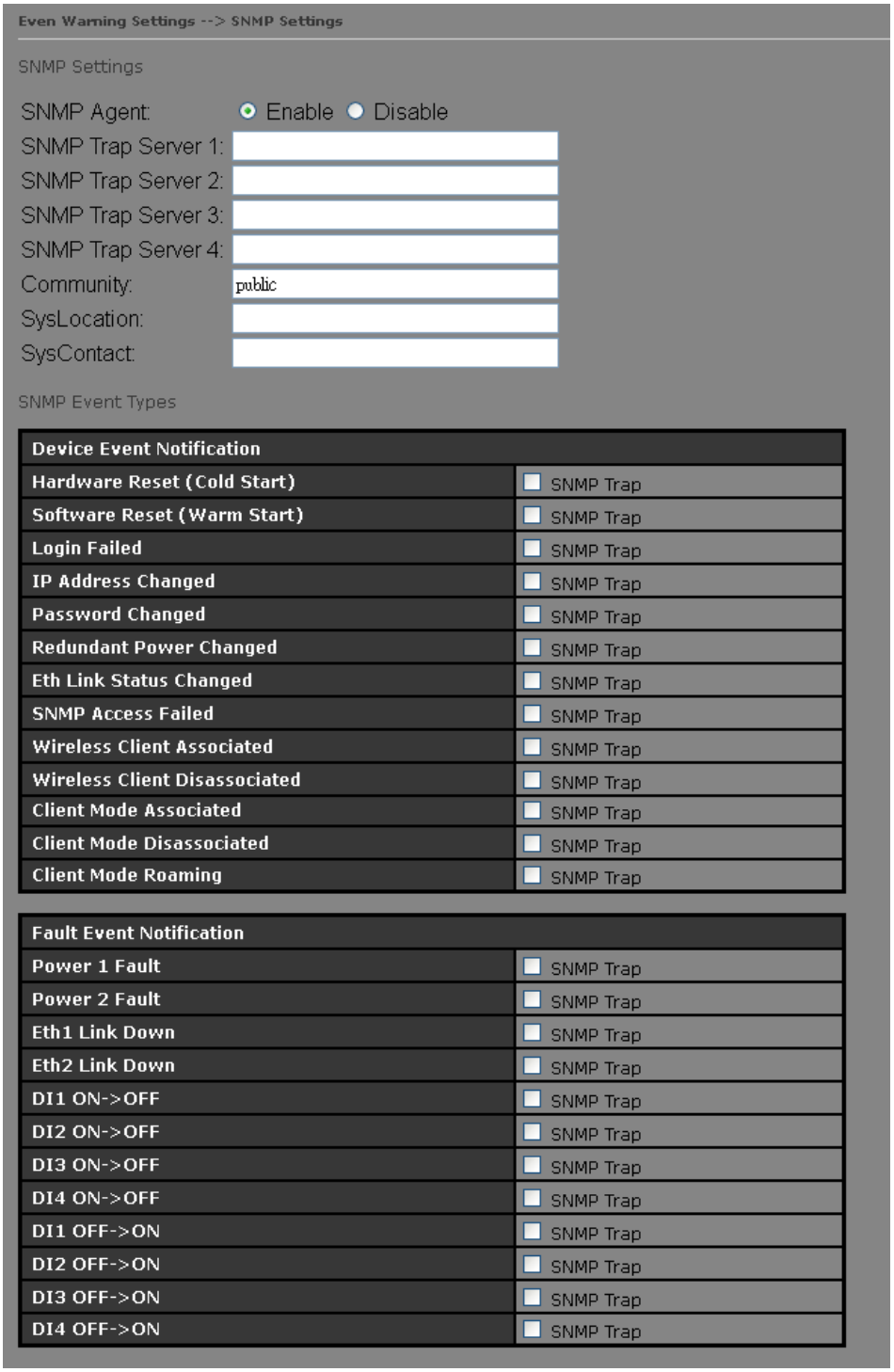
Label	Description
Syslog Server IP	Enter the IP address of a remote server if you want the logs to be stored remotely. Leave it blank will disable remote syslog.
Syslog Server Port	Specifies the port to be logged remotely. Default port is 514.

E-Mail



Label	Description
SMTP Server	Enter a backup host to be used when the primary host is unavailable.
Server Port	Specifies the port where MTA can be contacted via SMTP server
E-mail Address 1-4	Enter the mail address that will receive notifications

SNMP

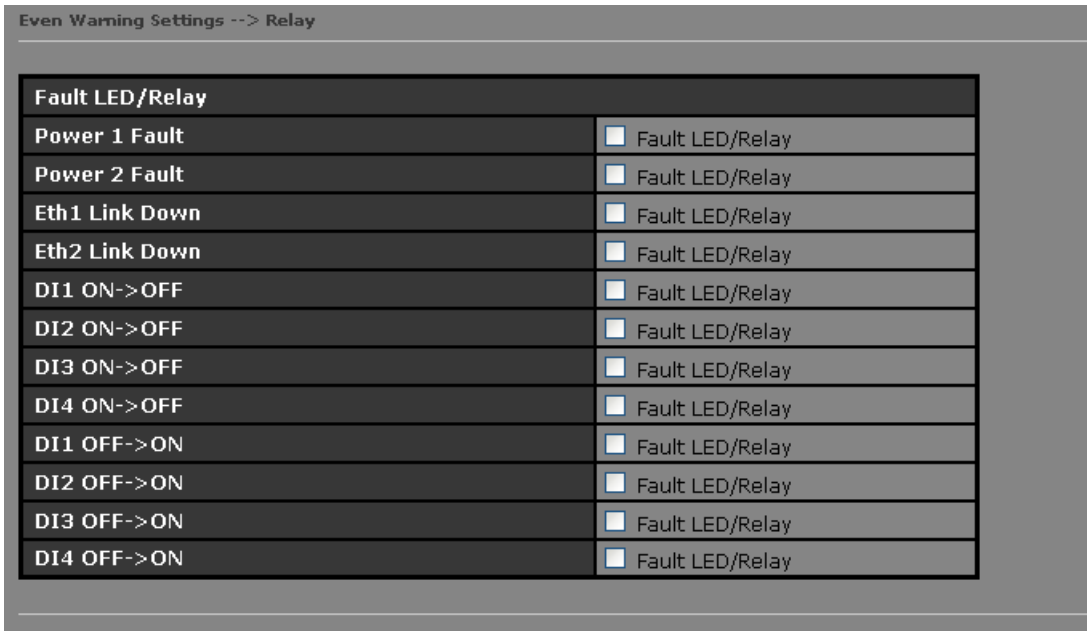


Label	Description
SNMP Agent	SNMP (Simple Network Management Protocol) Agent is a service program that runs on the access point. The agent provides management information to the NMS by keeping track of various

	operational aspects of the AP system. You can enable or disable the function.
SNMP Trap Server 1-4	Enter the IP address of the SNMP server which will send out traps generated by the AP.
Community	Community is a password to establish trust between managers and agents. Normally, **public** is used for read-write community.
SysLocation	Specifies sysLocation string
SysContact	Specifies sysContact string

Relay

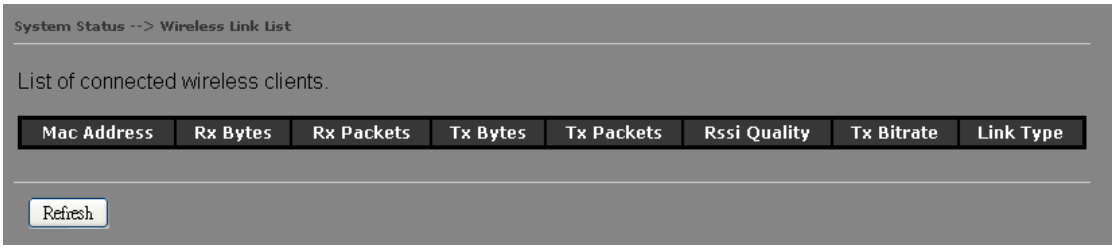
This page allows you to enable faulty relay function for the device by check the individual boxes.



5.5.6 System status

Wireless Link List

This page displays the information of the wireless clients connected to the device, including their MAC address, data rate, and link types.

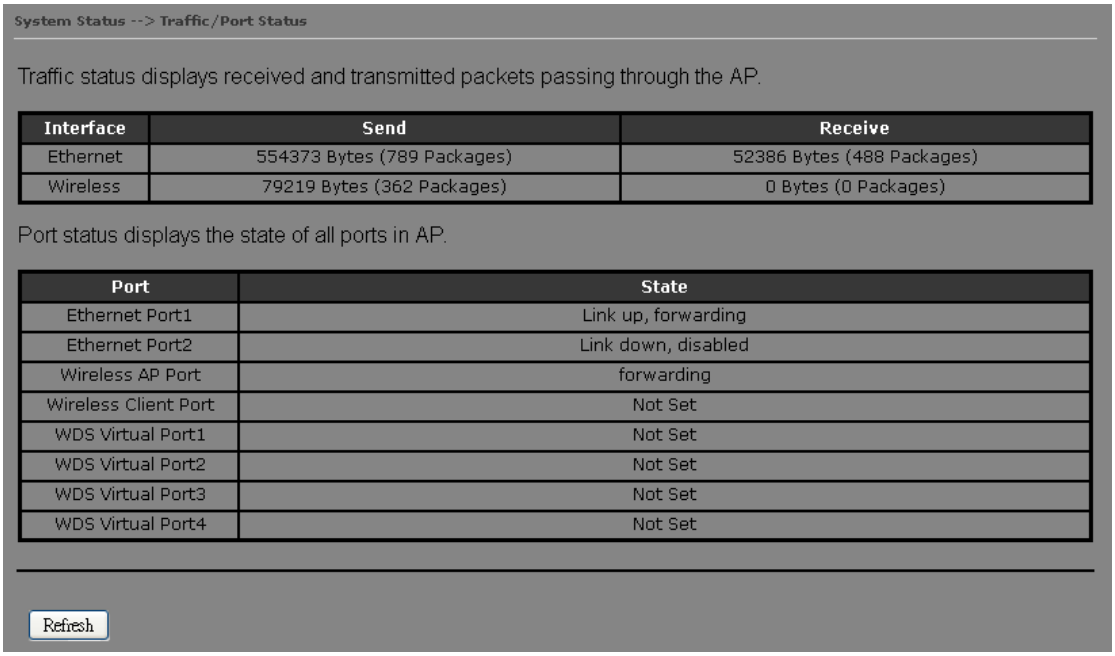


DHCP Clients List

This page lists the devices on your network that are receiving dynamic IP addresses from the device.

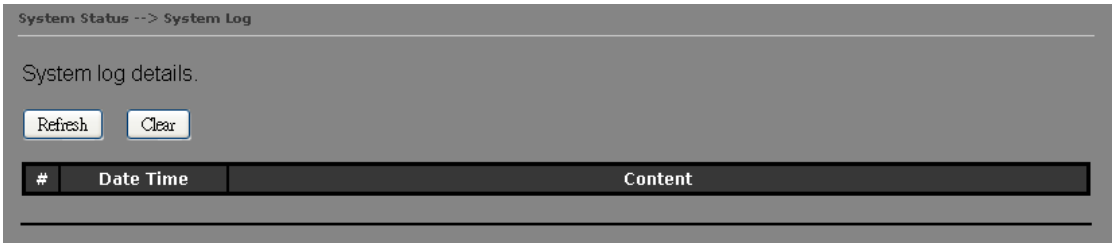
Traffic/Port Status

This page displays the network traffic statistics for both received and transmitted packets through the Ethernet port and wireless connections associated with the AP. Note that the traffic counter will reset when the device is rebooted.



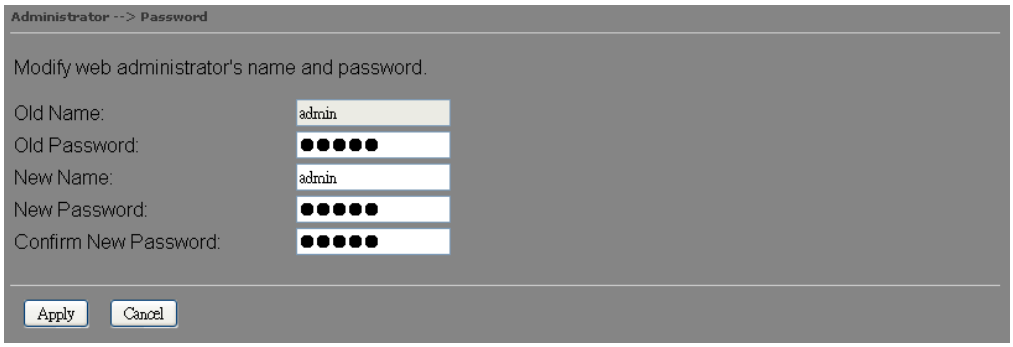
System Log

The device will constantly log events and activities in System Log and provide the file for you to review. You can click **Refresh** to renew the page or **Clear** to clear all or certain log entries.



5.5.7 Administrator Setting Password

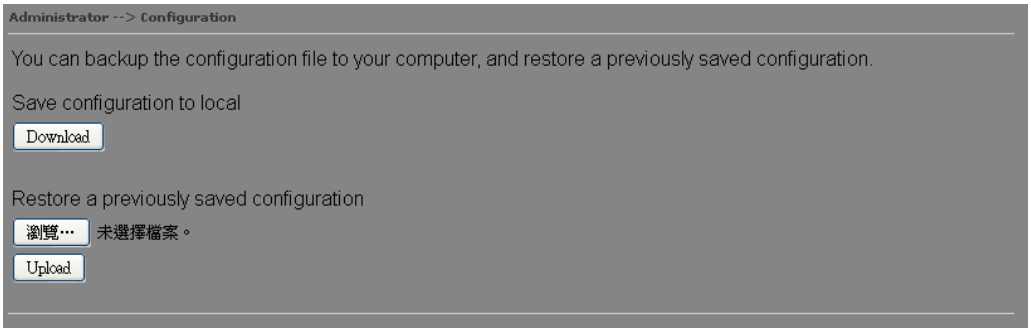
This page allows you to change the username and password. You must type in the new password twice to confirm (the default username and password are **admin**).



Label	Description
Old Name	Type in current login name
Old Password	Type in current password
New Name	Enter a new login name. Acceptable characters contain '0-9', 'a-z', 'A-Z' and the length must be 1 to 15 characters. An empty name is not acceptable.
New Password	Enter a new login password. Acceptable characters contain '0-9', 'a-z', 'A-Z' and the length must be 0 to 15 characters.
Confirm New Password	Retype the new password to confirm it.

Saving Configurations

This page allows you to save existing configurations as a backup file or return the device to previous settings.



Label	Description
Download	Click to save the current system settings as a file stored in the local hard drive.
Upload	You can restore configurations to previous status by installing a

	previous configuration file. To do this, click on **Browse** to locate the file you want to upload in the local hard drive and click **Upload**.
Restore Default Settings	Click to reset the device to the factory settings. The device will reboot to validate the default settings.

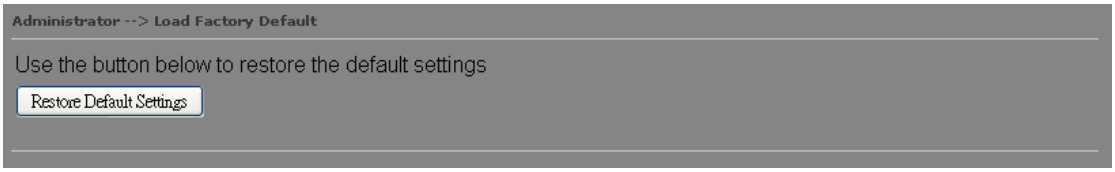
Firmware Upgrade

ORing launches new firmware constantly to enhance performance and functions. To upgrade firmware, download new firmware from ORing's website to your PC and install it via Web upgrade. Make sure the firmware file matches the model of your device. It will take several minutes to upload and update the firmware. After upgrade completes successfully, reboot the device.

During firmware upgrading, do not turn off the power of the device or press the reset button.

Load Factory Default

You can use this page to restore the device to factory default settings. Make sure to save the device settings before clicking on this button. All current settings will be lost after you click this button.



Restart

Click the button in this page to restart the device through warm reset.

Technical Specifications

ORing WLAN Access Point Model	TGAP-6620(+)-M12	TGAP-620(+)-M12
Physical Ports		
10/100/1000Base-T(X) Ports in M12 Auto MDI/MDIX (8-pin A-coding)	**2** (Present at ETH2 Fully compliant with IEEE 802.3af PoE P.D)	
DI/DO port in M12 (5-pin A-coding)	**2(DI x 4 and DO x 4)** Dry Contact: On: short to GND, Off: open Wet Contact (DI to COM/GND): On: 0 to 3VDC, Off: 10 to 30VDC	
RS-232 Console port in M12 (5-pin A-coding)	**115200, 8 ,N ,1**	
Relay port in M12 (5-pin A-coding)	**1A@24VDC**	
WLAN interface		
Operating Mode	Dual AP/Dual Client /Bridge /AP-Client Mode	AP/Bridge/Client/AP-Client
Antenna Connector	4 x External reverse SMA antenna connector	2 x External reverse SMA antenna connector
Radio Frequency Type	DSSS, OFDM	
Modulation	IEEE802.11a : OFDM with BPSK, QPSK, QAM, 64QAM IEEE802.11b: CCK, DQPSK, DBPSK IEEE802.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM IEEE802.11n : BPSK, QPSK, 16-QAM, 64-QAM	
Frequency Band	America / FCC : 2.412~2.462 GHz (11 channels) 5.180~5.240 GHz & 5.745~5.825 GHz (9 channels) Europe CE / ETSI : 2.412~2.472 Ghz (13 channels) 5.180~5.240 GHz (4 channels)	
Transmission Rate	IEEE802.11b: 1 / 2 / 5.5 / 11 Mbps IEEE802.11a/g: 6 / 9 / 12 / 18 / 24 / 36 / 48 / 54 Mbps IEEE801.11n: up to 300Mbps	
Transmit Power	802.11a: 12dBm ± 1.5dBm 802.11b: 18dBm ± 1.5dBm 802.11g: 15dBm ± 1.5dBm 802.11gn HT20: 13dBm ± 1.5dBm@150Mbps 802.11gn HT40: 12dBm ± 1.5dBm@300Mbps 802.11an HT20: 12dBm ± 1.5dBm@150Mbps 802.11an HT40: 12dBm ± 1.5dBm@300Mbps	
Receiver Sensitivity	802.11a: -68dBm ±2dBm@54Mbps 802.11b: -85dBm ±2dBm@11Mbps 802.11g: -68dBm ±2dBm@54Mbps 802.11gn HT20: -68dBm ±2dBm@150Mbps 802.11gn HT40: -68dBm ±2dBm@300Mbps 802.11an HT20: -68dBm ±2dBm@150Mbps 802.11an HT40: -68dBm ±2dBm@300Mbps	
Encryption Security	WEP: (64-bit ,128-bit key supported) WPA/WPA2 :802.11i(WEP and AES encryption) WPAPSK (256-bit key pre-shared key supported) 802.1X Authentication supported TKIP encryption	
Wireless Security	SSID broadcast disable and enable	
Protocol Support		
Protocol	ARP,BOOTP, DHCP, DNS, HTTP, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, STP, RSTP,	
LED indicators		
Power indicator	2 x LEDs, PW1:Green for DC Power on PW2:Green for DC Power on or power by PoE	

10/100/1000Base-T(X) indicator	2 x LEDs, Green for port Link/Act	
WLAN LED	2 x LEDs, Green for WLAN Link /Act	1 x LED, Green for WLAN Link/Act
Fault	1 x LED, Red for Ethernet link down or power down indicator	
Fault contact		
Relay	Relay output to carry capacity of 1A at 24VDC(5-pin M12 A-coding)	
Power		
Input power	Dual Power Inputs. 12~48 VDC	
Power consumption (Typ.)	11Watts	8W
Physical Characteristic		
Enclosure	IP-40	
Dimension (W x D x H)	125.6(W) x 65(D) x 196.1(H) mm (4.94 x 2.55 x 7.72 inch.)	
Weight (g)	965g	955g
Environmental		
Storage Temperature	-40 to 85°C (-40 to 185°F)	
Operating Temperature	-25 to 70°C (-13 to 158°F)	
Operating Humidity	5 to 95% Non-condensing	
Regulatory approvals		
EMI	FCC Part 15, CISPR (EN55022) class A, EN50155 (EN50121-3-2, EN55011, EN50121-4)	
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, EN61373	
Free Fall	IEC60068-2-31	
Vibration	IEC60068-2-6	
Safety	EN60950-1	
Warranty	5 years	

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.