IGAP-W99110GP+

Industrial Dual Wi-Fi 6 Wireless Access Point

User Manual

Version 1.0

Aug, 2021

https://oringnet.com/

COPYRIGHT NOTICE

Copyright © 2021 ORing Industrial Networking Corp.
All rights reserved.
No part of this publication may be reproduced in any form without the prior written consent of ORing Industrial Networking Corp.

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, JhongJheng Rd., Sindian District, New Taipei City 231, Taiwan, R.O.C.
Tel: + 886 2 2218 1066 // Fax: + 886 2 2218 1014
Website: https://oringnet.com/
Technical Support: support@oringnet.com
Sales Contact: sales_all@oringnet.com (Headquarter)
sales@oring-china.com (China)

Table of Content

Getting Started 4
1.1 About the IGAP-W99110GP+ 4
1.2 Software Features 4
1.3 Hardware Specifications 5

Hardware Overview 6
2.1 Product Appearance 6
2.1.1 Ports and connectors 6
2.1.2 LED 6
2.2 Dimension 7

Hardware Installation 8
3.1 Grounding and Lightning Protection 8
3.2 Preparing the Installation Site 9
3.2.1 Temperature and Humidity 9
3.2.2 Outdoor Installation 9
3.2.3 Waterproof 9
3.2.4 EMI 10
3.2.5 Fiber Connection 10
3.2.6 Console Connection 10
3.2.7 Checking before Installation 10
3.3 Installing the Access Point 11
3.3.1 Installation Flowchart 11
3.3.2 Before You Begin 11
3.3.3 Precautions 12
3.3.4 Installing the AP 12
3.3.5 Cables and Pin Assignment 14
3.3.6 Connecting Cables 15

Web-based Configuration 19
4.1 Overview 19
4.2 Config Wizard 21
4.3 Monitoring 23
4.3.1 Dashboard 23

4.3.2 User Info 23
4.3.3 DHCP 24
4.4 Configuration 25
4.4.1 Wireless 25
4.4.2 AP 27
4.4.3 Network 31
4.4.4 Security 46
4.4.5 Authentication 60
4.4.6 Advanced 61
4.4.7 Rapid 62
4.5 Maintenance 63
4.5.1 Settings 63
4.5.2 System 65

Appendix 68
5.1 Product Specification 68
5.2 Antenna Patterns 69

Getting Started

1.1 About the IGAP-W99110GP+

The IGAP-W99110GP+ is a high-performance Wi-Fi 6 (IEEE802.11ax) industrial outdoor access point. The IGAP-W99110GP+ provide concurrent dual-band dual-radio with up to 2.4Gbps access rate, it offers 4 spatial streams. The interface includes one SFP port and one Gigabit Ethernet port with PoE/ local power supply. Taking the wireless network security, RF control, mobile access, QoS and other important factors into account. By the technologies implemented in IEEE802.11ax, such as OFDMA, BSS Color and MU-MIMO, it can reduce the network latency, spatial reuse and improve the network efficiency.

IGAP-W99110GP+ adopts the IP68 protection design for the enclosure, which is suitable for application in indoor and outdoor environments. It can withstand extreme weather and other environmental conditions. Equipped with built-in directional antenna, IGAP-W99110GP+ can achieve the Wi-Fi coverage in vast majority of the scenarios and greatly reduce the difficulty of installation and maintenance. Multi-hop and point-to-multipoint bridge features are supported to further enhance the deployment flexibility.

1.2 Software Features

- Highly Security Capability: WEP/ WPA/ WPA-PSK(TKIP,AES)/ WPA2/ WPA2 PSK(TKIP,AES)/ 802.1X Authentication supported
- Support wireless load balance
- Max 1024 client connections
- Supports a wide variety of QoS policies
- ARP Spoofing Protection
- Support IPv4/IPv6 address
- Support AP/Client Mode
- SSID capacity up to 32
- Wireless connecting status monitoring
- Secured Management by Telnet, SSH, TFTP, HTTP
- Event Warning by Syslog

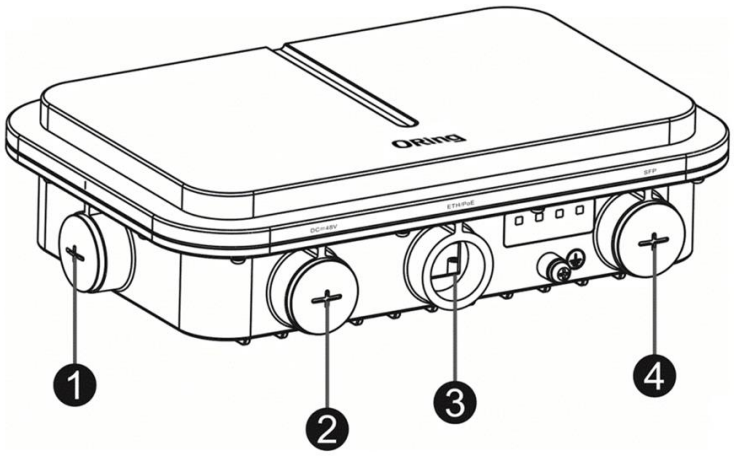
1.3 Hardware Specifications

- High Speed Air Connectivity: WLAN interface support up to 2400Mbps link speed
- Dual-Band Dual-Radio IEEE802.11ax with 4 spatial streams
- Build-in 9dBi Directional Antenna
- 1x 10/100/1000Base-T(X) port
- 1x Gigabit SFP socket
- 1x Console port
- Surge Protection +/-9kV (Common mode)
- IP68 enclosure for outdoor applications
- Operating temperature -40 to 65ºC
- Dimension 251(W) x 168(D) × 64(H) mm
- Wall/Pole-mount installation

Hardware Overview

2.1 Product Appearance

2.1.1 Ports and connectors



Note:	1. Console port and reset button 2. Port for 48VDC power supply	3. 10/100/1000 Base-T Ethernet/PoE PD port 4. SFP port

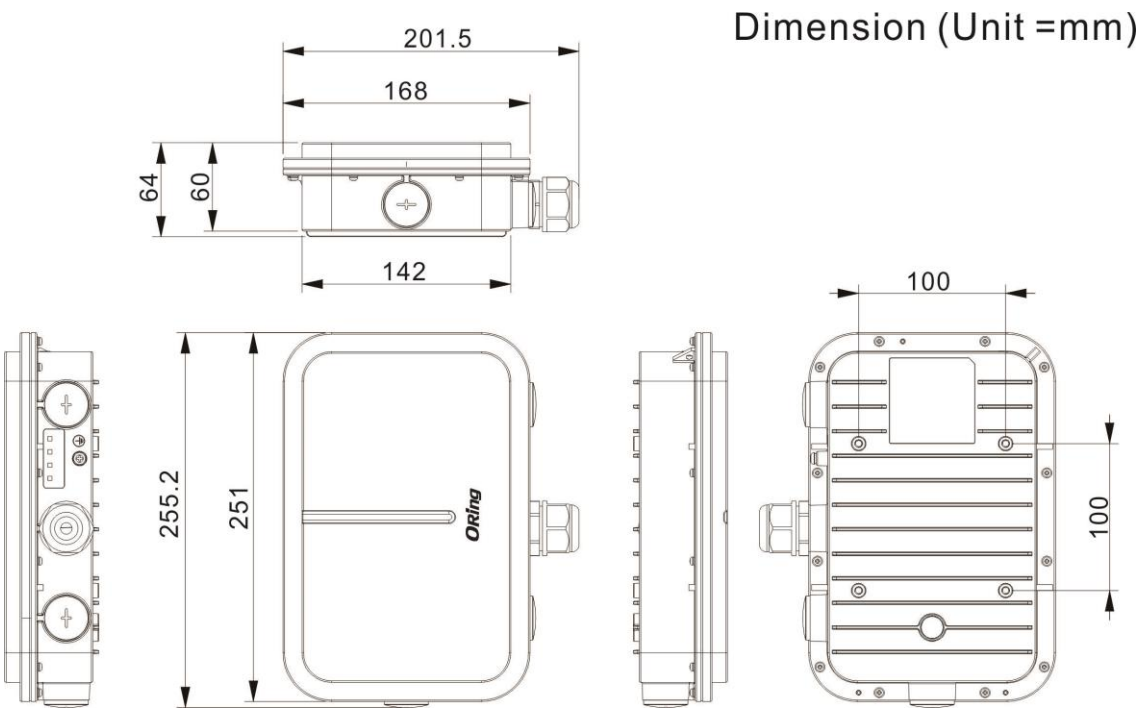
2.1.2 LED

The following table describes the function of each LED indicator.

LED	State	Meaning
System status	Blinking green	The system is booting.
	Solid green	Initialization in progress or proper operation.
	Blinking red	The uplink port is disconnected.
WDS RSSI (3 LEDs in total; available when bridging is enabled)	1 solid on	< -70dBm
	2 solid on	-70 to -50dBm
	3 solid on	> -50dBm

2.2 Dimension

IGAP-W99110GP+ dimension: 251(W) x 168(D) × 64(H) mm (Excluding the bracket)



Hardware Installation

To prevent device damage and physical injury, please read carefully the safety recommendations described in this chapter.

Recommendations do not cover all possible hazardous situations.

3.1 Grounding and Lightning Protection

- Ensure that both the power-receiving end and the power-supplying end are well-grounded.
- Keep the grounding connection within 30 m, and use a 40mm x 4mm or 50mm x 5mm ground bar of hot-dip zinc-coated flat steel sheet.
- When the connection cable between the main grounding conductor and local equipotential earthing terminal board (LEB) on each floor is shorter than 2 meters, use a stranded copper wire with a sectional area not less than 1.318 mm2 (16 AWG) for the connection cable.
- Use a shielded network cable if possible, ensure that devices connected to both ends of the shielded network cable are reliably grounded, and make sure that the sheath of the shielded network cable is also grounded if possible. If no shielded network cable is available, wire the network cable through a steel pipe and bury the steel pipe for lead-in, and properly ground both ends of the steel pipe.
- No additional lightning protector is required as a high-profile lightning protector is built in the IGAP-W99110GP+, and the power port support 6kV lightning protection. If a lightning protector of a higher profile is available, configure the lightning protector optionally. Before the configuration, connect the lightning protector to the ground cable.
- Use a power cable with the PE end to ground the power supply (AC). Ensure that the PE end is properly grounded, with a ground resistance less than 5 ohms. Do not use a two-wire power cable with only the live (L) wire and naught (N) wire. Do not connect the N wire to the protection ground cable of other communication devices, and ensure that the L wire and N wire are properly connected.
- Ensure that the ground resistance is less than 5 ohms. In areas with high soil resistivity, reduce the soil resistivity via measures such as spreading resistivity reduction mixture around the grounding conductor.

3.2 Preparing the Installation Site

- Do not expose the AP to high temperature, dust, or harmful gases.
- Do not install the AP in an area prone to fire or explosions.
- Keep the AP away from EMI sources such as large radar stations, radio stations, and substations.
- Do not subject the AP to unstable voltage, vibration, and noises.
- Keep the AP at least 500 meters away from the ocean and do not face it towards the sea breeze.
- The installation site should be protected from water and flooding, seepage, dripping, or condensation.
- The installation site should be selected according to network planning, communications equipment features and considerations such as climate, hydrology, geology, earthquake, electric power, and transportation.

3.2.1 Temperature and Humidity

The following table shows required temperature and humidity for IGAP-W99110GP+

Operating Temperature	-40°C to 65°C (-40°F to 149°F)
Operating Humidity	0% to 100% (non-condensing)

3.2.2 Outdoor Installation

The AP can be mounted on a wall or pole.

3.2.3 Waterproof

Use a seal plug to seal the unused ports.

Use a watertight adapter to connect cables to the AP. For details, see Chapter “Installing the Access Point”.

3.2.4 EMI

All interference sources (from outside or inside of the device or application system) affect the device by capacitive coupling, inductive coupling, or electromagnetic waves.
Electromagnetic interference (EMI) occurs due to electromagnetic radiation or conduction, depending on the transmission path.

Radiation interference occurs when energy (usually radio frequency energy) is emitted from a device and propagated through space to disrupt other devices. The interference source can be part of disrupted system or a fully electrically isolated unit. Conduction interference occurs when interference is transferred from one unit to another through cables, which are usually electromagnetic wires or signal cables connected between the source and the device(s) experiencing interference. Conduction interference often affects the power supply of the device. It is eliminated by using filters. Radiation interference can influence the path of any signal from the device and is difficult to shield.

- Take effective measures against interference from the power grid.
- Keep the AP far away from the grounding or lightning protection devices for power equipment.
- Keep the AP away from high-power radio stations, radar stations, and high-frequency high-current devices.
- Take electrostatic shielding measures.

3.2.5 Fiber Connection

Before connecting fiber cables, make sure the model of the optical transceiver and fiber type match the optical port. The transmit port on the local device should be connected to the receive port on the peer device and vice versa.

3.2.6 Console Connection

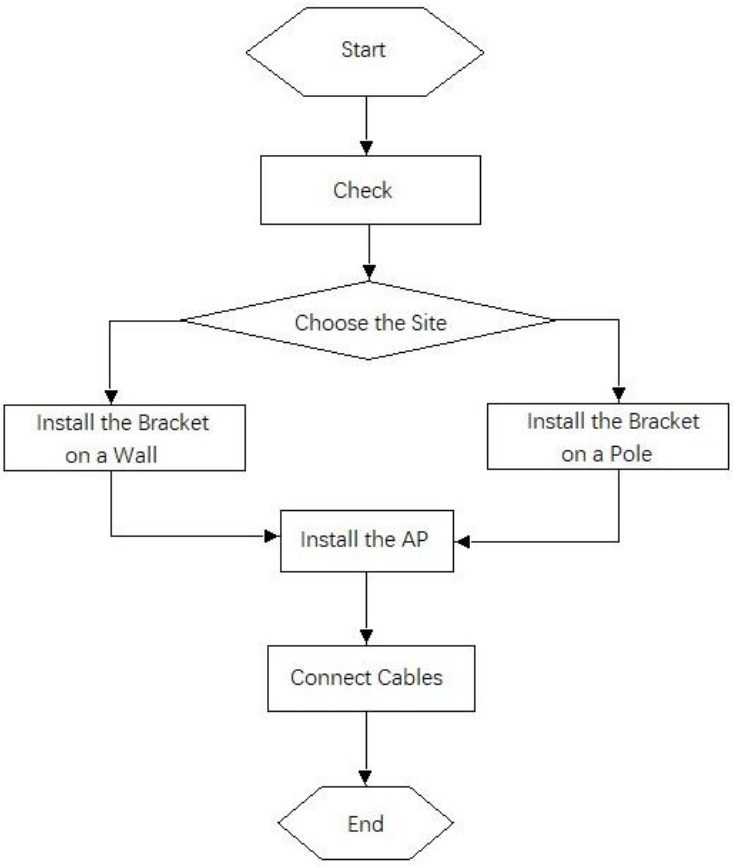
Please attach RS-232 console cable to your PC COM port, and connect the other end to the Console port of IGAP-W99110GP+, open Terminal tool and set up serial settings to 9600, N,8,1. (Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1) Then you can access CLI interface. The default username/password is admin/admin.

3.2.7 Checking before Installation

Please check your materials carefully against the package contents. If there are any errors, please contact your distributor or ORing sales representative.

3.3 Installing the Access Point

3.3.1 Installation Flowchart



3.3.2 Before You Begin

Before you install the AP, verify that all the parts in the package contents are there and make sure that:

- The installation site meets temperature and humidity requirements.
- The installation site is equipped with a proper power supply.
- Network cables are in place.

3.3.3 Precautions

IGAP-W99110GP+ can be mounted on a wall and a pole (diameter: 50mm to 140mm, thickness: ≥ 2.5mm). Otherwise, the AP could fall down and cause injuries. The installation site can vary due to on-the-spot surveys conducted by technical personnel.

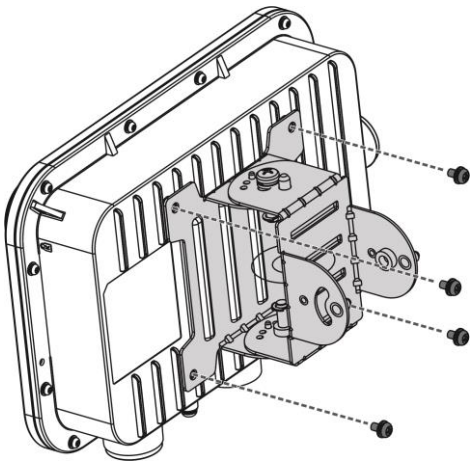
Please make full preparations as described in Chapter 2 and observe the following precautions before installing the AP.

- Before connecting the power supply, make sure the external power supply matches the power module inside the AP.
- Before connecting the power cord, make sure the power switch is in the OFF position.
- When connecting a wire to a binding post, make sure their colors are the same.
- Make sure the power supply is properly connected.

3.3.4 Installing the AP

1. Use four M5 screws to secure the AP to the mounting plate.

Figure: Securing the AP with M5 Screws

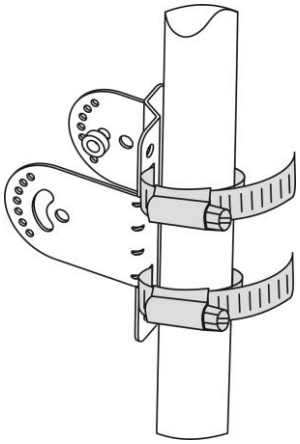


2. Install the mounting bracket to a pole or wall.

- **Pole mount**

Attach the bracket to a pole with two hose clamp and fasten the clamp with screws and nuts.

Figure: Mounting the Bracket on a Pole



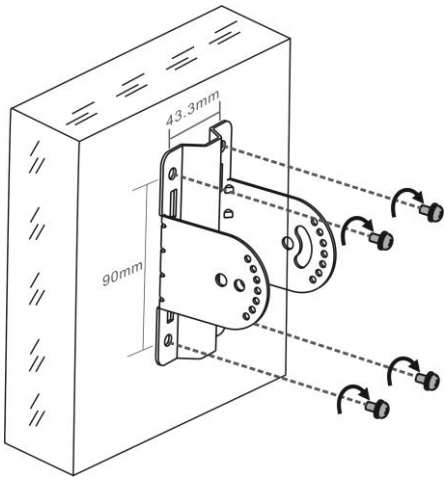
- **Wall mount**

Use four M8 x 60 screws to implement the wall mount. (The screws, made of SUS304 stainless steel, are customer-supplied.)

a. Attach the bracket to the wall and mark the screw hole locations.

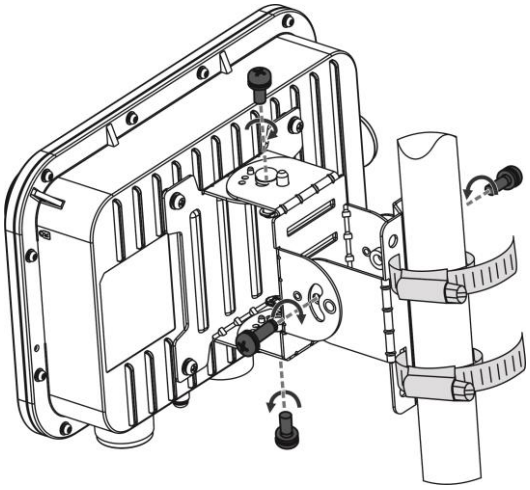
b. Align the screw holes on the bracket and those on the wall, and tighten the M8 x 40 screws to mount the bracket.

Figure: Mounting the Bracket on Wall



3. Use four M6 screws to join the mounting plate and the bracket. Adjust the angle of the device before fastening the screws.

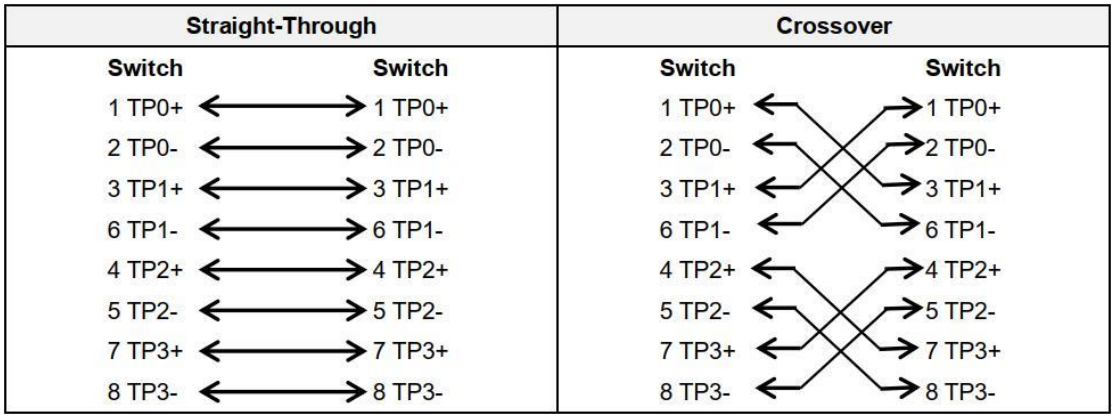
Figure: Complete the Installation



3.3.5 Cables and Pin Assignment

The 1000BASE-T/100BASE-TX/10BASE-T is a 10/100/1000 Mbps auto-negotiation port that supports auto MDI/MDIX. Compliant with IEEE 802.3ab, 1000BASE-T requires Category 5e 100-ohm UTP or STP (STP is recommended) with a maximum distance of 100 meters (328 feet). 1000BASE-T requires all four pairs of wires be connected for data transmission.

Figure: 1000BASE-T Connection

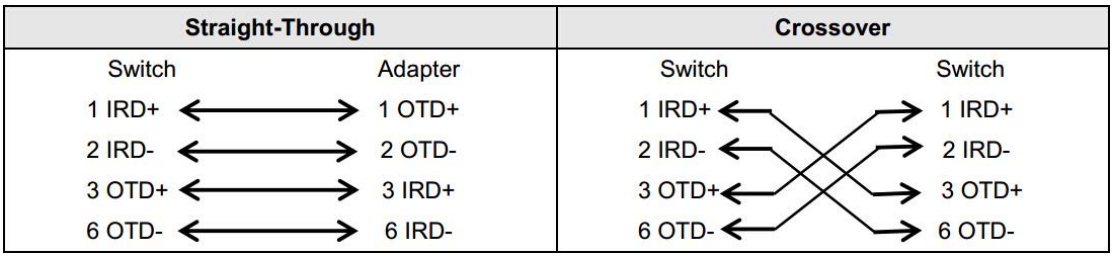


10BASE-T uses Category 3, 4, 5 100-ohm UTP/STP and 1000BASE-T uses Category 5 100-ohm UTP/STP for connections. Both support a maximum length of 100 meters.

Table: 100BASE-TX/10BASE-T Pin Assignments

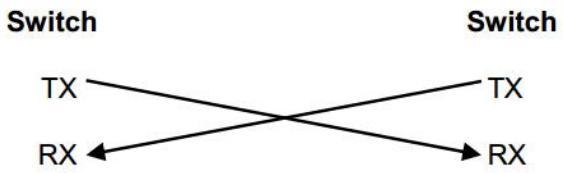
Pin	Socket	Plug
1	Input Receive Data+	Output Transmit Data+
2	Input Receive Data-	Output Transmit Data-
3	Output Transmit Data+	Input Receive Data+
6	Output Transmit Data-	Input Receive Data-
4,5,7,8	Not used	Not used

The figure below shows the wiring of straight-through and crossover cables for 100BASE-TX/10BASE-T.



Fiber Connection

You can choose to use single-mode or multi-mode fiber according to the transceiver module types. Figure below shows connection of fiber cables.

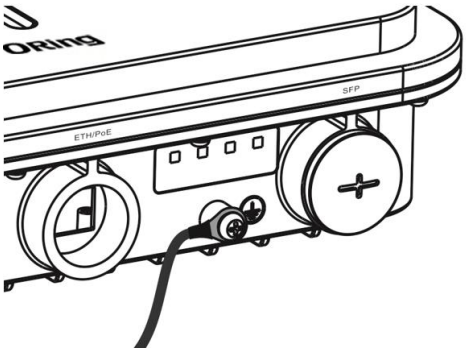


3.3.6 Connecting Cables

Connecting the grounding cable

The grounding cable is made on site. Connect the supplied grounding wire (yellow-green) to the AP grounding hole on one end and ground the wire on the other end through OT terminals. To avoid waste, adjust the cable length for actual demands.

Figure: Grounding the AP



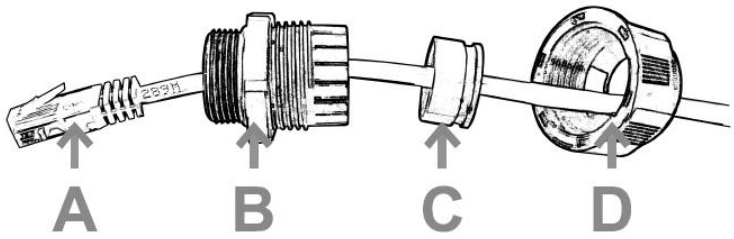
Connecting the network cable

Waterproofing material is customer-supplied.

1. Trim the network cable according to the distance between the AP and the power supply. And put the trimmed cable through the bracket.

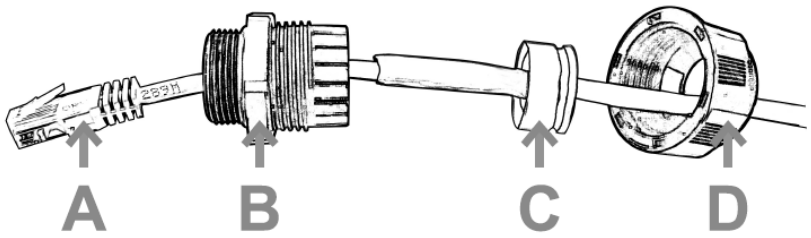
2. Thread the cable through liquid-tight adapter and add a plug to the end. See figure below.

Figure: Threading the Network Cable



3. Wrap the cable between B and C upwards with two or three layers of liquid-tight material. See figure below.

Figure: Wrapping Liquid-tight Material around Cable



4. Insert the plug into the ETH/PoE port and tighten B, C and D in order.

Make sure the plug is correctly inserted. The plug can be damaged if the liquid-tight adapter is improperly tightened.

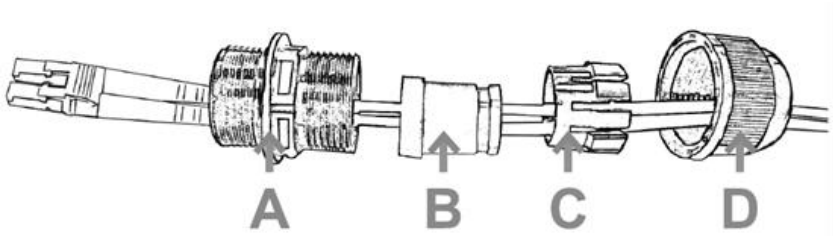
Before removing the network cable, dismantle the liquid-tight adapter first and then the plug.

Connecting the optical fiber

Waterproofing material is customer-supplied.

1. Choose an LC-LC optical fiber with the diameter of 2.7±0.2mm.
2. Thread the fiber through the liquid-tight adapter in the order as shown in figure below.

Figure: Threading the Fiber



3. Insert the plug of the fiber into the SFP port.
4. Tighten A.
5. Combine B and C and put the combination into A.
6. Tighten D before applying waterproof glue to its joint with A.

Before removing the optical fiber, dismantle the liquid-tight adapter first and then the plug.

If the diameter of LC-LC fiber is not 2.7±0.2mm, waterproofness of the adapter cannot be guaranteed.

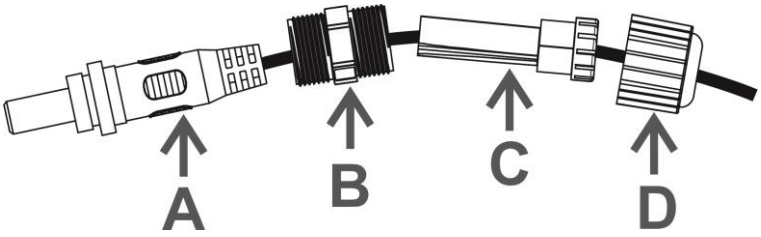
Connecting the DC Power Cord (Optional)

Waterproofing material is customer-supplied.

Please make sure the port for DC power supply face to the ground.

Thread the DC power cord through the liquid-tight adapter in the order as shown in Figure below. Use waterproof duct tape and waterproof plaster to fill in the space between the power cord and the adapter.

Figure: Threading the DC Power Cord

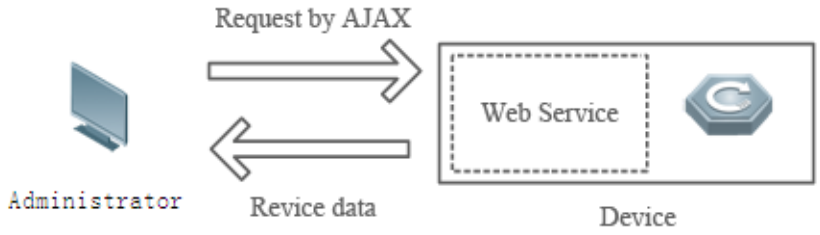


Web-based Configuration

4.1 Overview

The AP can be controlled via a built-in web server which supports Internet Explorer (Internet Explorer 7.0 or above versions) and other Web browsers such as Chrome, Firefox and some IE kernel-based browsers. Therefore, you can manage and configure the switch easily and remotely. You can also upgrade firmware via a web browser. The Web management function not only reduces network bandwidth consumption, but also enhances access speed and provides a user-friendly viewing screen.

The Web management system integrates configuration commands and sends them to the device through AJAX requests. Web service is enabled on the device to process HTTP requests to return requested data.



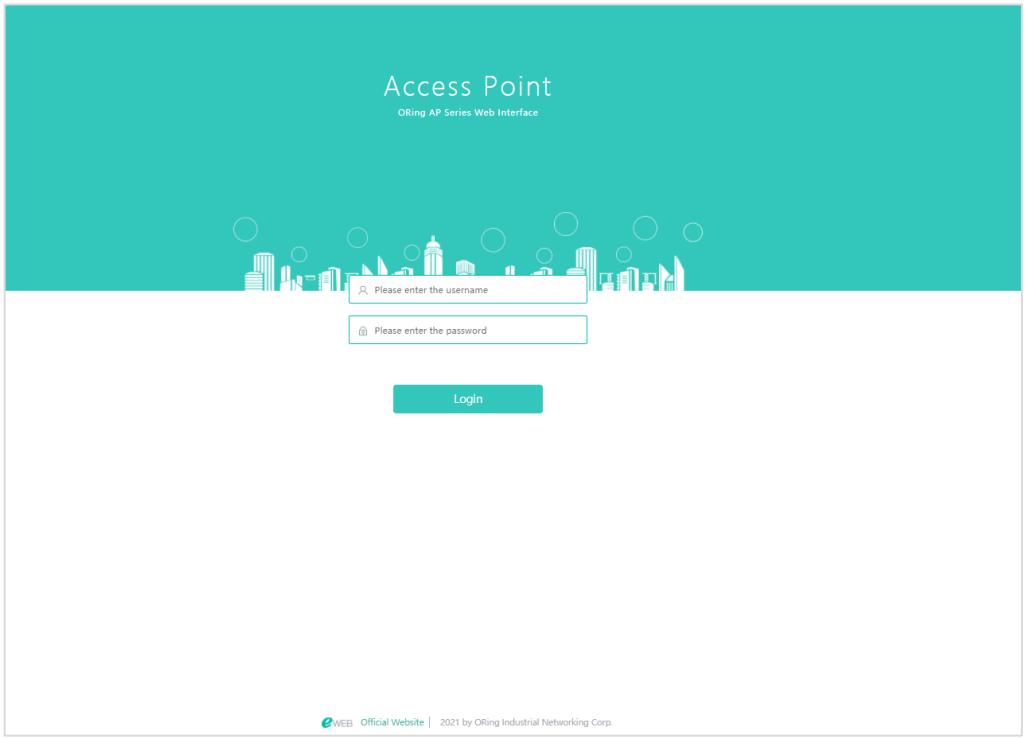
Note	It is recommended that the resolution be set to 1024 x 768, 1280 x 1024, or 1440 x 960. Exceptions such as font alignment error and format error may occur when other resolutions are selected.

The following table lists the Web management system default configuration.

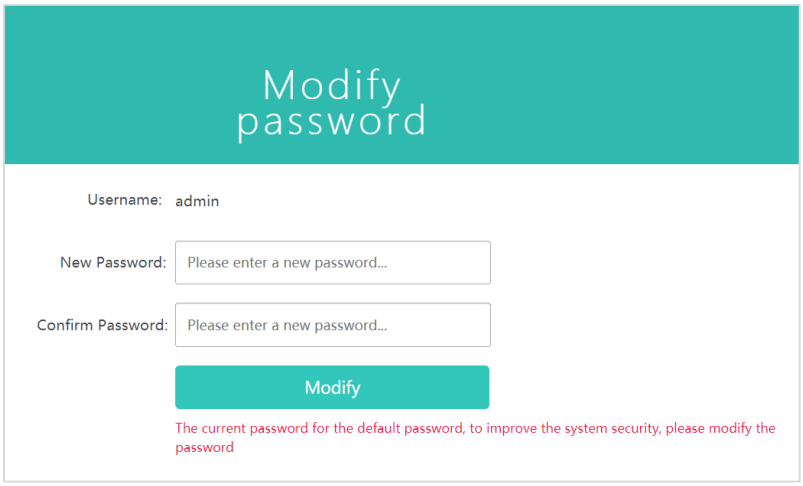
Feature	Default Settings
Web service	Enabled
Management IP	192.168.110.1
Default Username/Password	admin/admin

The default password is not saved in **show running-config**.

Type **http://X.X.X.X** (management IP address), default: http://192.168.110.1, in the address bar of a browser and press **Enter** to access the login page, as shown in the following figure.

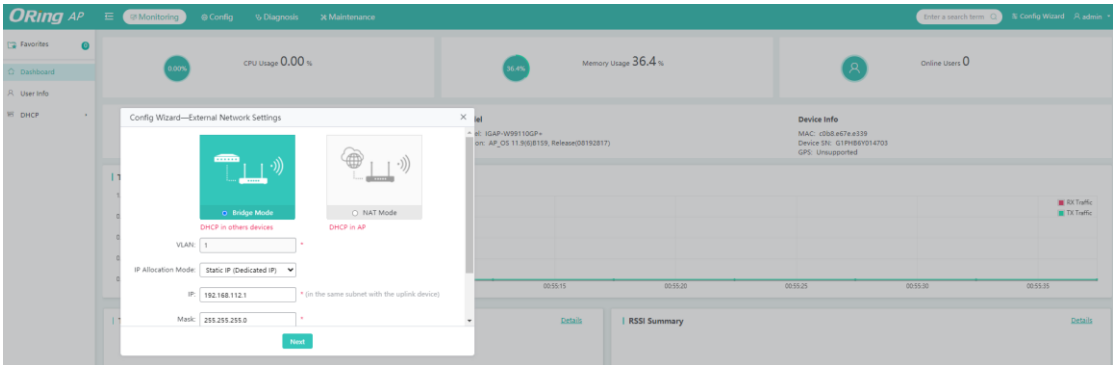


When you log in successfully for the first time, you will be prompted to change the password to increase security, please enter a new password containing at least eight characters.



4.2 Config Wizard

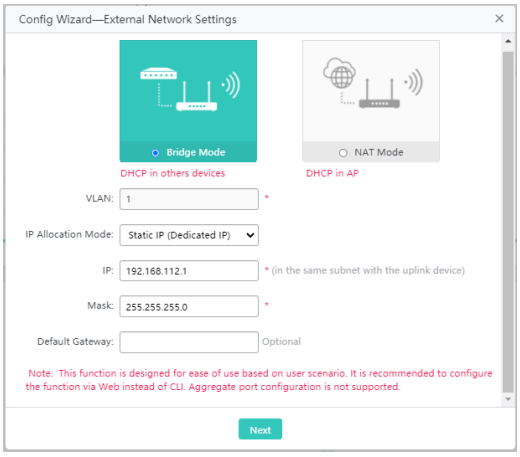
Build a WiFi network for STAs to access for Internet services.



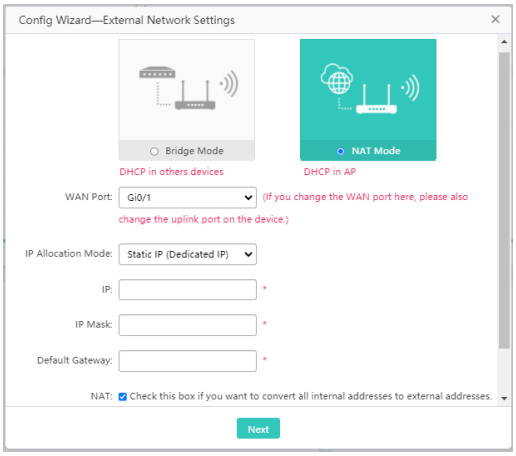
1. The **Config Wizard** page is displayed after successfully logging in to the Web if the device is in the default factory setting state, as shown in the preceding figure.

2. The **Config Wizard** page is also displayed when you click the **Config Wizard** link in the upper-right corner on the homepage.

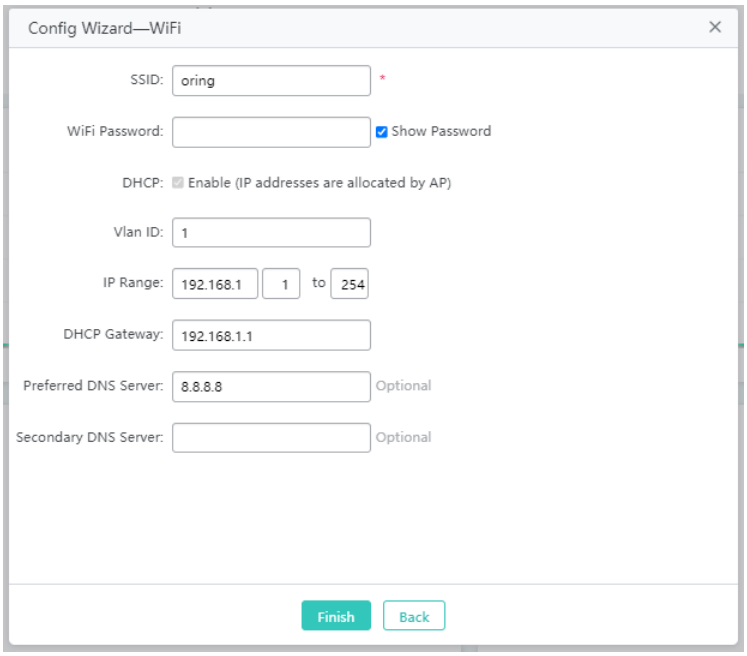
The device supporting NAT can work in Bridge mode or NAT mode.



Bridge mode



NAT mode



Configure the WiFi parameters, and click **Finish** to finish the configuration.

After the AP device is initialized, please configure the AP device through the **Config Wizard** page.

All quick settings are scenario-based settings. And some of the configuration is delivered by default. If configurations such as NAT, interface, or address pool are changed via CLI, it is recommended to not change the configuration again via Quick Settings, otherwise there could be incompatibility.

If the AP device is in access mode, it is recommended to build the gateway and address pool on the other device. If the AP device is in routing mode, it is recommended to build the gateway and address pool on the AP device and configure the NAT for it.

4.3 Monitoring

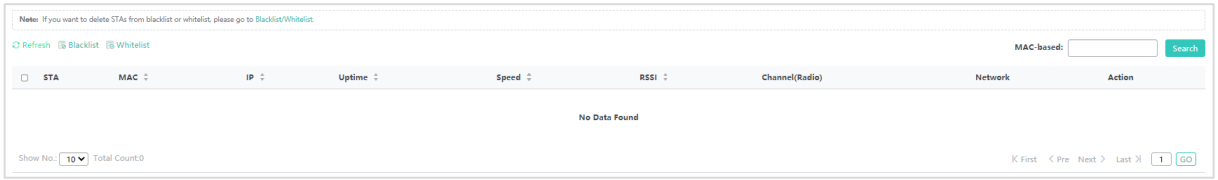
4.3.1 Dashboard

The dashboard enables viewing basic information for the AP device, including the device MAC address, device model, system alarm information, flow trends of AP device ports, latest trends of all management APs, and STA information corresponding to each management AP. In addition, it enables you to know the distribution condition of STA signal strength in real time.

Click the **Traffics** > **Details** or **RSSI Summary** > **Details** link in the lower left corner to view the STA details on the displayed page, for example, the MAC address and RSSI.

4.3.2 User Info

User information is displayed here.

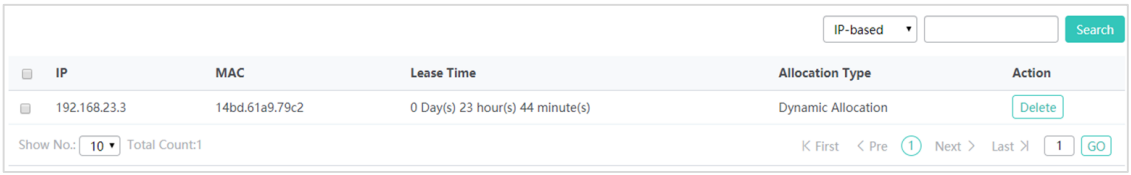


4.3.3 DHCP

DHCP includes DHCP client list and DHCP server status.

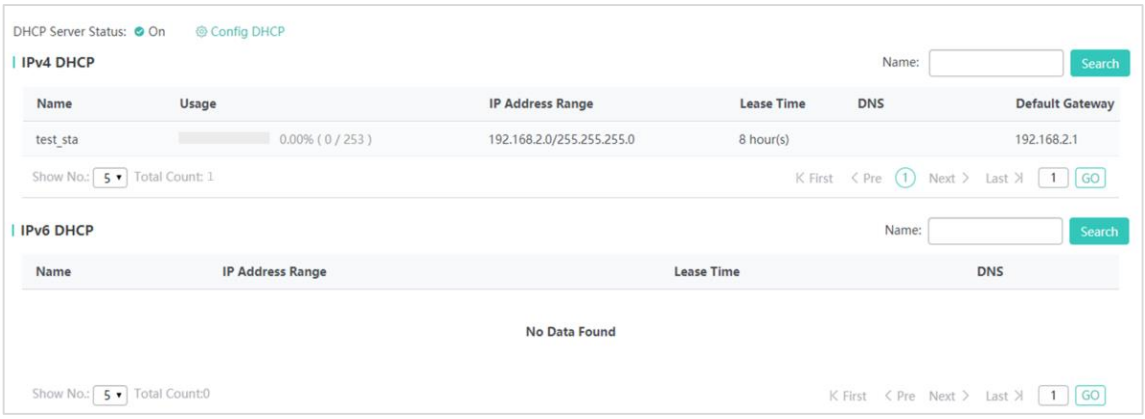
- **DHCP Client List**

  DHCP clients are displayed here.



- **DHCP Server Status**

  DHCP server status and address pool usage are displayed here.



4.4 Configuration

4.4.1 Wireless

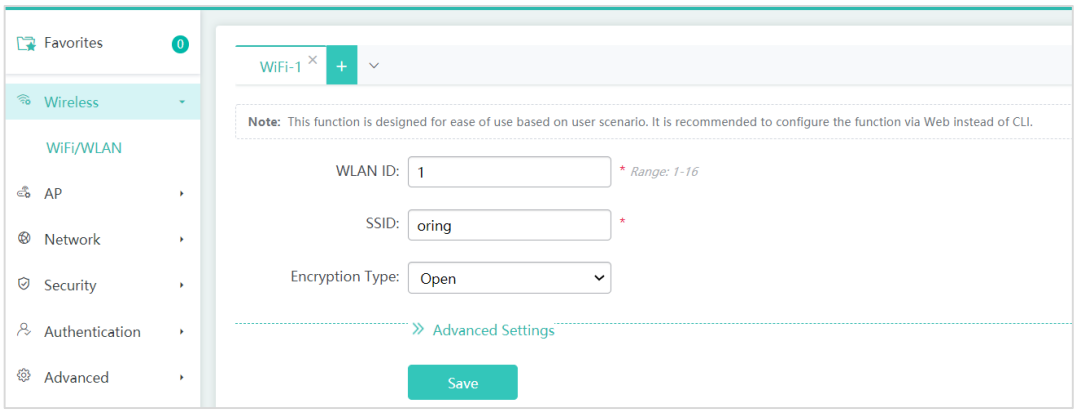
A Wireless Local Area Network (WLAN) refers to a network system that allows different PCs to communicate and share resources with each other by interconnecting different PCs through wireless communication technologies. The essence of a WLAN is that PCs are interconnected with each other in wireless rather than wired mode, thus constructing a network and allowing terminals to move more flexibly.

Wi-Fi or WiFi is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers, smart TVs, digital audio players and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.

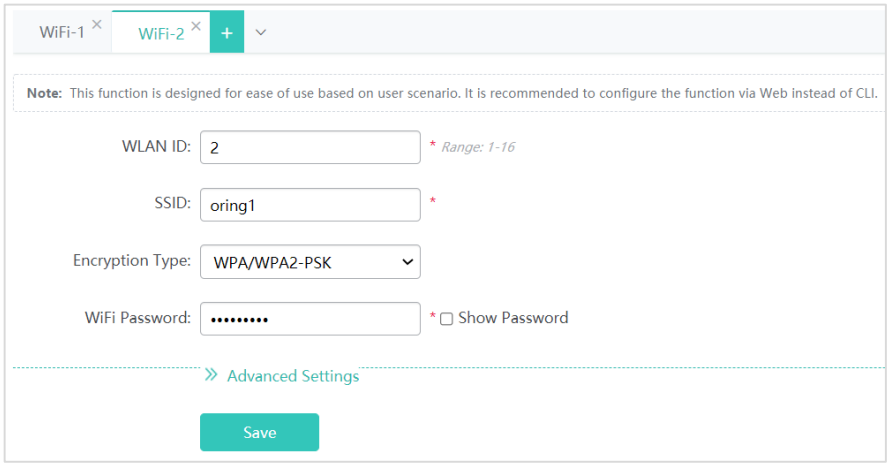
Service Set Identifier (SSID), also referred to as ESSID: It is used to distinguish different networks, that is, identifying an ESS. An SSID contains a maximum of 32 characters. A WNIC configured with different SSIDs can access different networks. SSIDs are usually broadcasted by an AP or a wireless router. To be simple, an SSID is the name of a WLAN. Only computers with the same SSID can communicate with each other. The WLAN allows wireless STAs to access the AP through WiFi for Internet services. Multiple WLANs can be added or deleted.

4.4.1.1 WiFi/WLAN

The following figure shows the page for adding a WLAN.

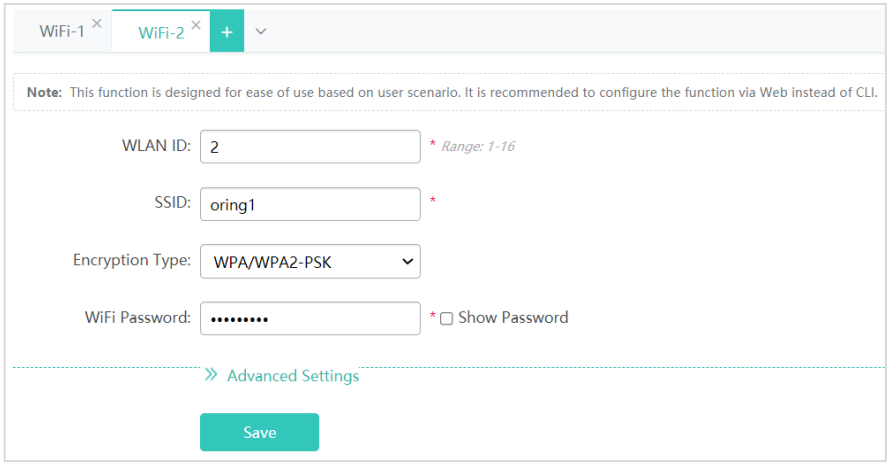


- **Adding WiFi/WLAN**



1. Click +, and a new panel for WiFi configuration is displayed.
2. Set the WiFi parameters.
3. Click **Save** to finish the configuration.

- **Editing the WLAN**

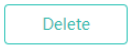


1. Click the WiFi panel you want to edit.
2. Edit the WiFi configuration.
   - **WLAN ID**: WLAN ID is used to identify a WLAN network.
   - **SSID**: An SSID is the name of a wireless local area network.
   - **Encryption Type**: Open, WPA/WPA2-PSK, WPA/WPA2-802.1X
3. Click **Save**. The **Edit succeeded** message is displayed.

- **Advanced Settings**
  - **Hide SSID:** This function is disabled by default.
  - **SSID Code**
    - UTF-8: Most terminals support UTF-8. The default code is UTF-8.
    - GBK: Some terminals and PCs support GBK.
  - **WiFi Type:** Radio1 is a 2.4GHz network and Radio2 is a 5GHz network.
  - **5G-prior Access:** Associate with the 5 GHz radio first

- **Deleting WLANs**

1. Click the WiFi panel you want to delete.

2. Click 

.

3. Click **OK** in the dialog box displayed to finish the deletion operation.

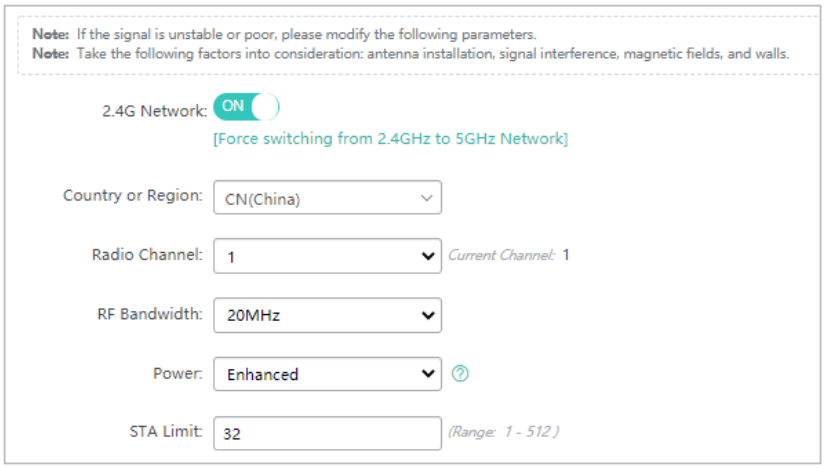
4.4.2 AP

4.4.2.1 RADIO

Wireless channels transmit RF medium between APs and wireless STAs. The use of channels varies with different countries and frequency bands. For example, the 2.4 GHz frequency band can be configured with 13 channels (channel 1 to channel 13), and the 5 GHz frequency band can be configured with five channels (channels 149, 153, 157, 161, and 165). The overlapping channels in the 2.4 GHz frequency band generate interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision. The five channels in the 5 GHz frequency band do not overlap or generate interference.

Wireless channel settings are mainly about adjusting the strength of the WiFi signal sent out by the device. Channel parameters can be set for the 2.4G and 5G networks.

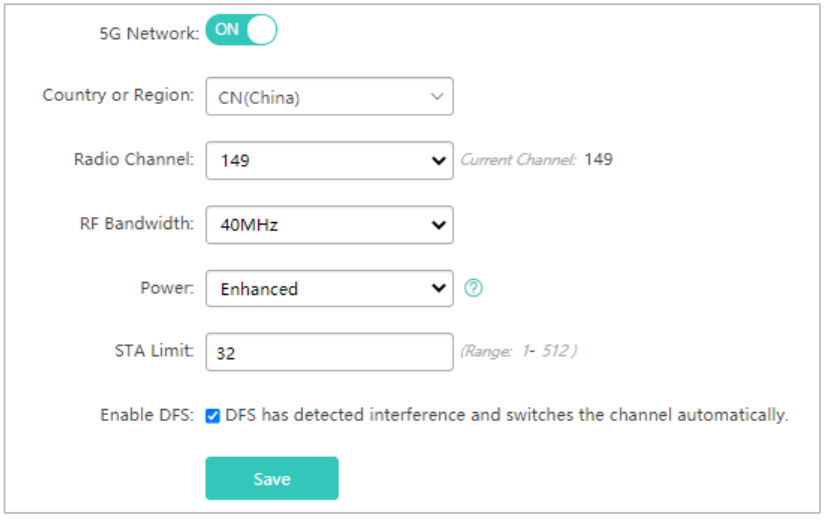
- **Enabling a 2.4G network**



1. Click ON to enable or disable the 2.4G network.

2. Click **Force switching from 2.4GHz to 5GHz Network** to forcibly switch the network type.

- **Enabling the 5G network**



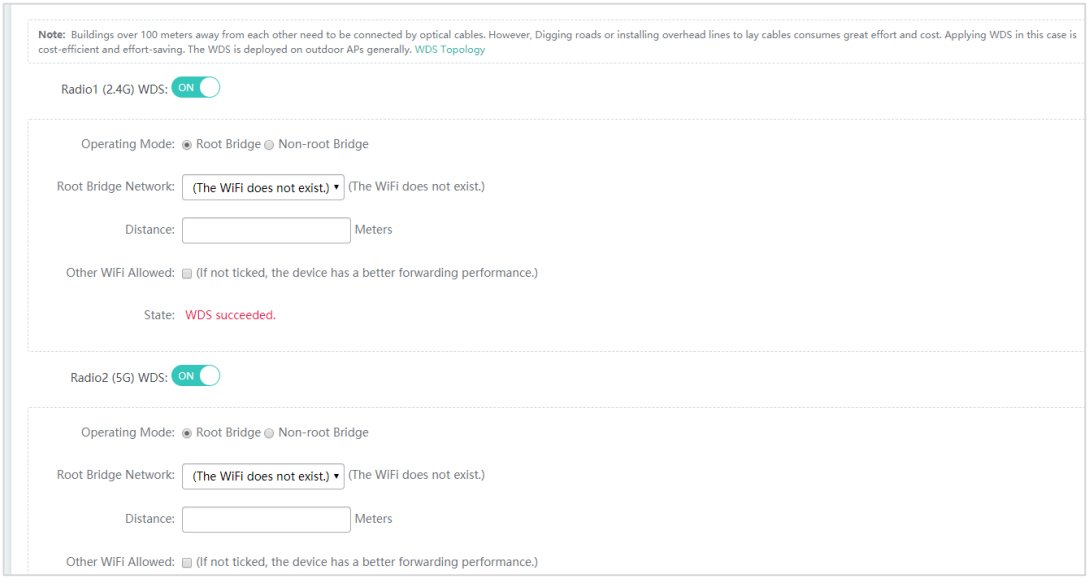
1. Click ON to enable or disable the 5G network.

2. Click **Enforce switching from 5GHz to 2.4GHz Network** to forcibly switch the network type.

4.4.2.2 WDS

Multiple APs are connected to each other in a wireless repeater or bridging mode to connect distributed networks and spread wireless signals. An AP device can be regarded as a repeater. It spreads the front-end network and elongates the WiFi transmission distance for association and connection of STAs far away. Wireless bridging supports the 2.4G network and 5G network bridging.

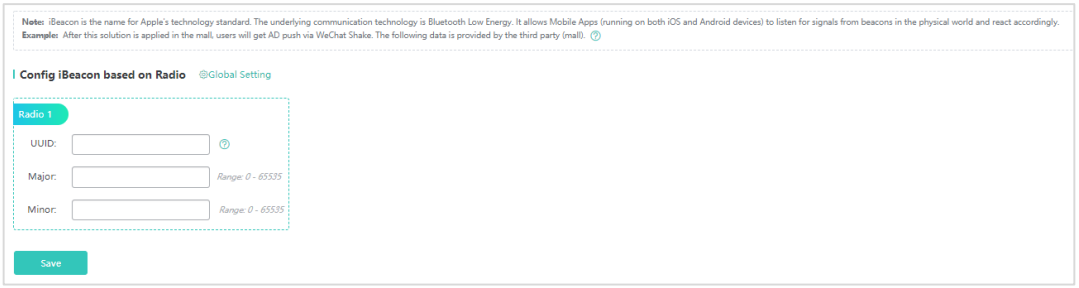
Enable the 2.4G or 5G network bridging function as required, select the **Operating Mode**, and click **Save** to finish configuration.



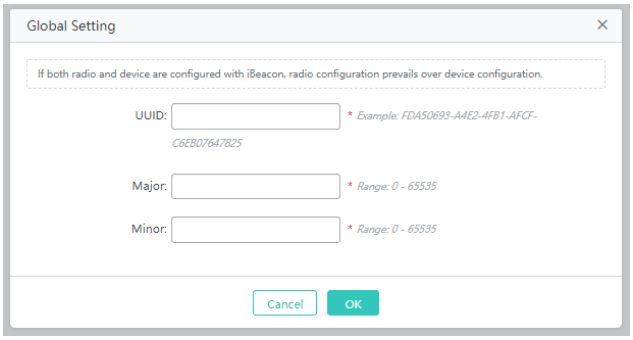
4.4.2.3 IBEACON

iBeacon uses Bluetooth low energy proximity sensing to transmit a universally unique identifier picked up by a compatible app or operating system. The identifier and several bytes sent with it can be used to determine the device's physical location, track customers, or trigger a location-based action on the device such as a check-in on social media or a push notification.

iBeacon signals are broadcast over Bluetooth, and mainly applied to WeChat Shake.

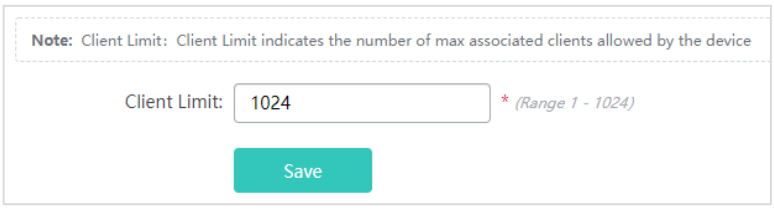


You can configure iBeacon globally or based on radio. Radio-based iBeacon settings prevail over global iBeacon settings.



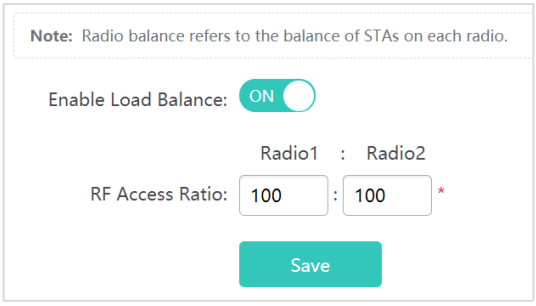
4.4.2.4 CLIENT LIMIT

Client limit refers to the maximum number of associated STAs. IGAP-W99110GP+ supports up to 1024 clients.



4.4.2.5 RADIO BALANCE

Radio balance refers to the balance of STAs on each radio.

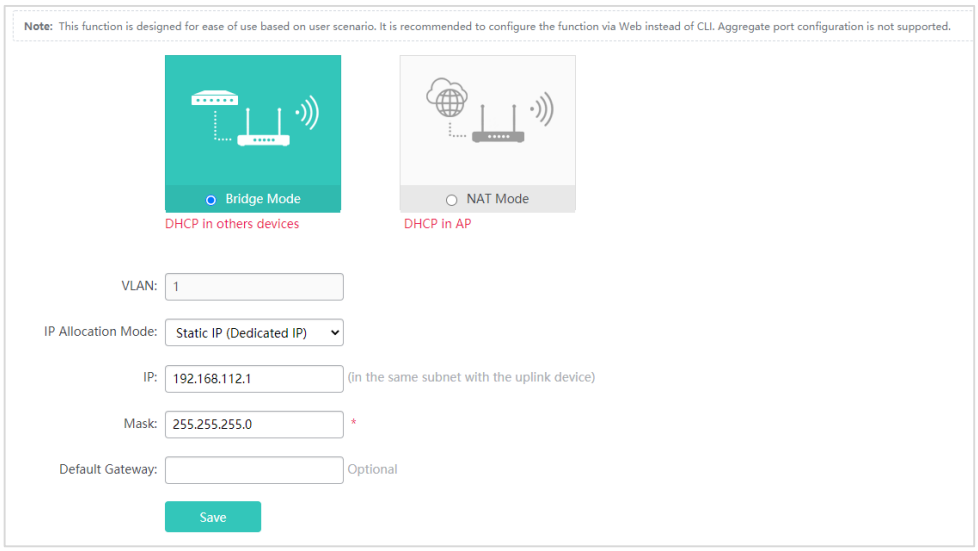


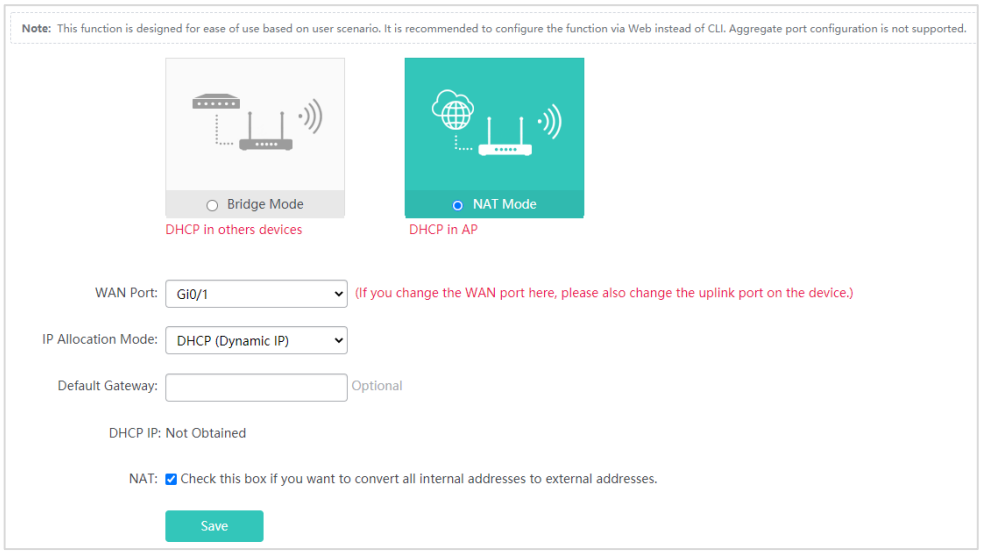
4.4.3 Network

4.4.3.1 External Network

External network settings are mainly about configuration of the communication mode between the AP and external network. Two communication modes are available: Bridge mode and NAT mode.

- **Bridge Mode**: The ORing APs act as bridges, allowing wireless clients to obtain their IP addresses from an upstream DHCP server.
- **NAT Mode**: The ORing APs run as DHCP servers to assign IP addresses to wireless clients out of a private 10.x.x.x IP address pool behind a NAT.



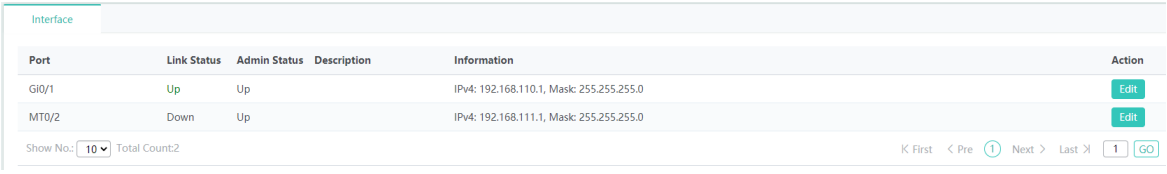


You can select the AP working mode to determine the AP role and then configure based on the corresponding working mode.

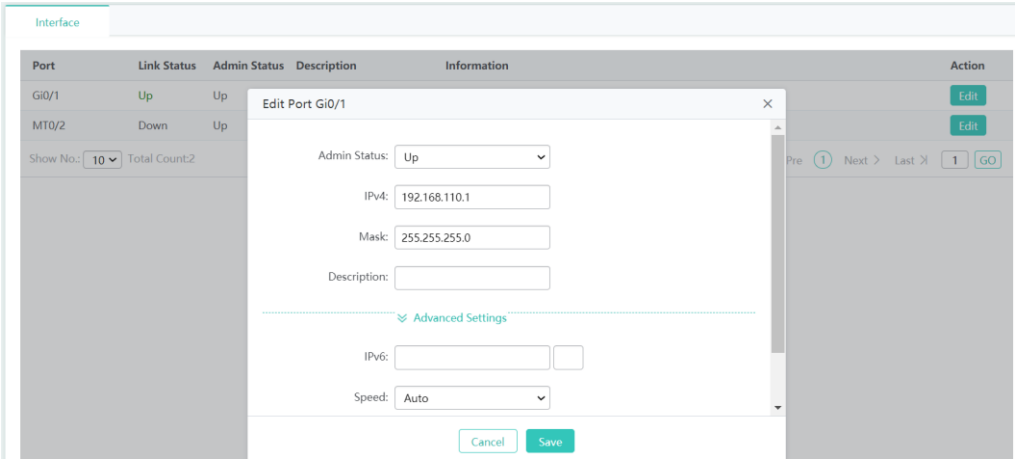
Set corresponding parameters and save the configuration.

4.4.3.2 INTERFACE

A port is a physical entity that is used for connections on the network devices. Gi0/1 is ETH/POE port, and MT0/2 is SFP port.



- **Editing port settings**



1. Click the **Edit** button for a port in the list.

- **Admin Status**

  You can configure the administrative status of an interface to disable the interface as required. If the interface is disabled, no frame will be received or sent on this interface, and the interface will loss all its functions. You can enable a disabled interface by configuring the administrative status of the interface. Two types of interface administrative status are defined: Up and Down. The administrative status of an interface is Down when the interface is disabled, and Up when the interface is enabled.

- **Description**

  You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A".

- **Speed**

  Generally, the speed of an Ethernet physical port is determined through negotiation with the peer device. The negotiated speed can be any speed within the interface capability. You can also configure any speed within the interface capability for the Ethernet physical port on the Web page.

When you configure the speed of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

2. The configuration for the port is displayed in the dialog box. Next, edit the configuration.

3. Click **Save**. The **Save operation succeeded** message is displayed.

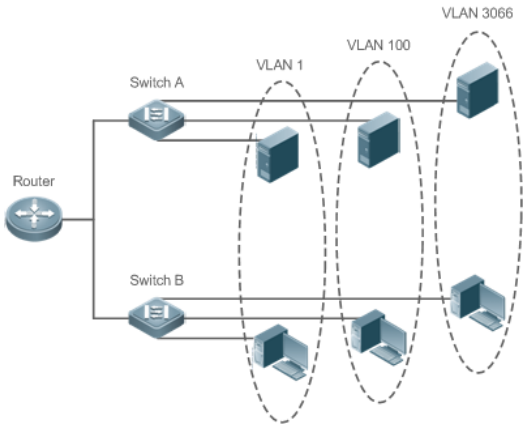
Note: The default network segments of Gi0/1 and MT0/2 are different, if you need to set the ports in the same segment, please configure in CLI or Telnet.

Command Example
ORing(config)#in gi0/1
ORing(config-if-GigabitEthernet 0/1)#no ip add
ORing(config-if-GigabitEthernet 0/1)#encapsulation dot1Q
ORing(config-if-GigabitEthernet 0/1)#in mt 0/2
ORing(config-if-MTGigabitEthernet 0/2)#no ip add
ORing(config-if-MTGigabitEthernet 0/2)#encapsulation dot1Q 1
ORing(config-if-MTGigabitEthernet 0/2)#exit
ORing(config)#i bvi 1
ORing(config-if-BVI 1)#ip add 192.168.21.1/24

4.4.3.3 VLAN

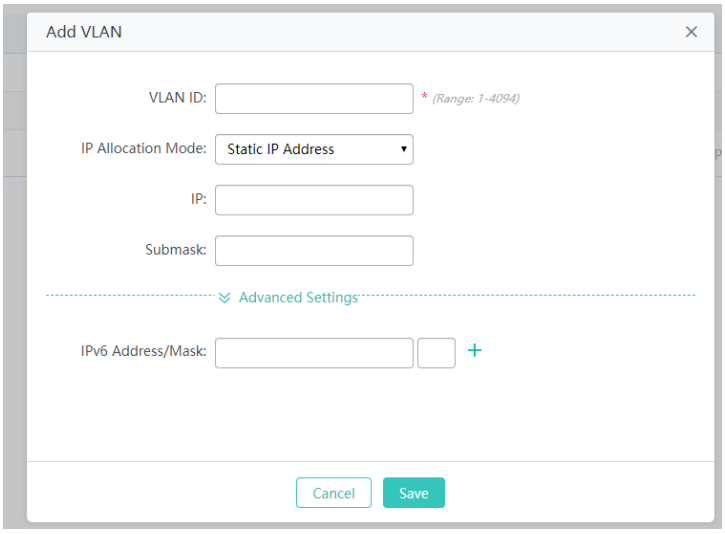
A Virtual Local Area Network (VLAN) is a logical network created based on a physical network. A VLAN can be categorized into Layer-2 networks of the OSI model. A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

We may define a port as a member of a VLAN, and all terminals connected to this port are parts of a virtual network that supports multiple VLANs. You do not need to adjust the network physically when adding, removing and modifying users. Communication among VLANs is realized through Layer-3 devices.



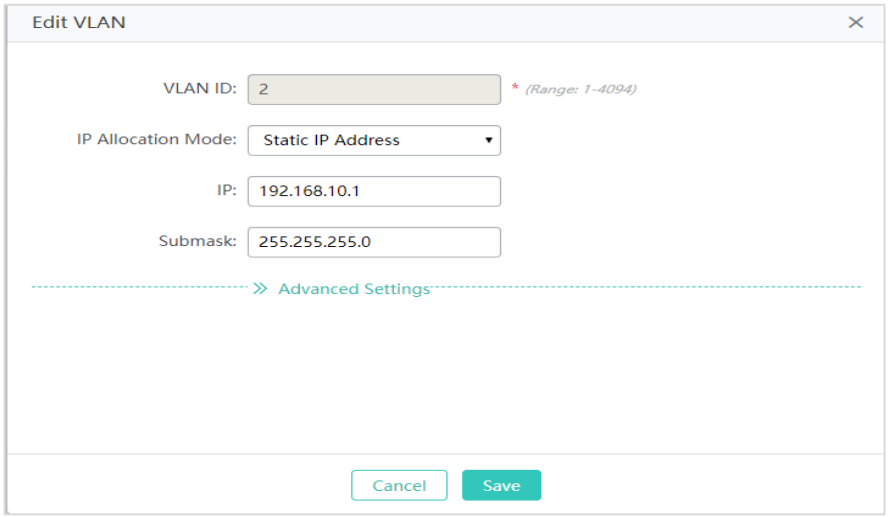
The VLANs comply with the IEEE802.1Q standard. A maximum of 4094 VLANs (VLAN ID 1-4094) are supported, among which VLAN 1 cannot be deleted.

- **Adding a VLAN**



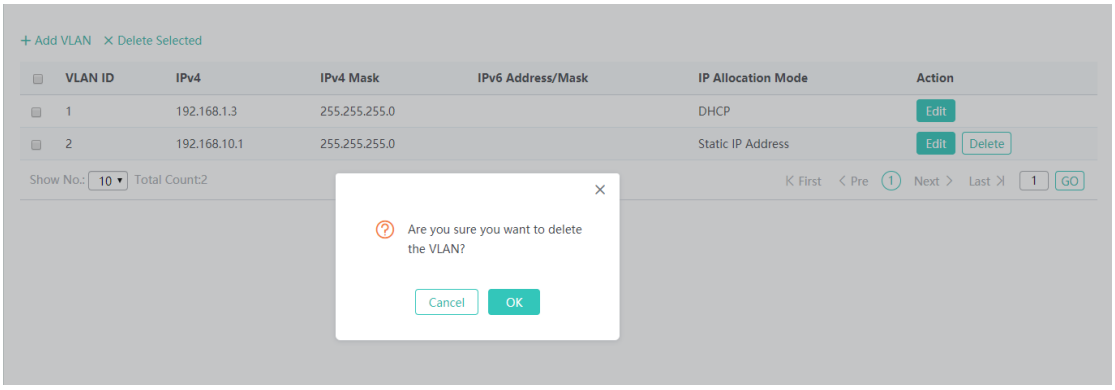
Click **Add VLAN**. A dialog box is displayed, as shown in the preceding figure. Set corresponding parameters in the dialog box and click **Save**. The newly added VLAN is displayed in the VLAN list after the **Add operation succeeded** message is displayed.

- **Editing a VLAN**



Click the **Edit** button. A dialog box is displayed, as shown in the preceding figure. Click **Save**. The **Save operation succeeded** message is displayed.

- **Deleting a VLAN**



Click the **Delete** button for a VLAN in the list and then click **OK** in the displayed dialog box to finish deleting.

- **Deleting VLANs in batches**

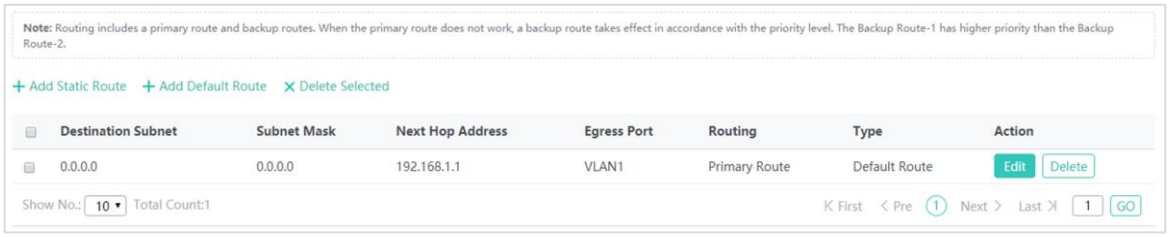
1. Select the VLAN to be deleted from the list.
2. Click Delete Selected to finish deleting.

4.4.3.4 ROUTE

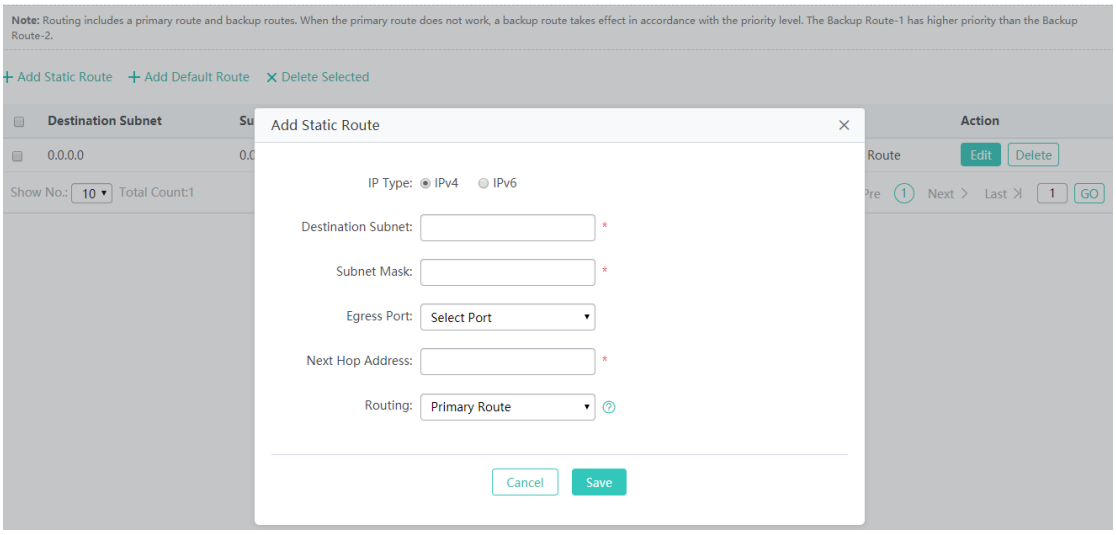
Routing is the process of selecting a path for traffic in a network, or between or across multiple networks.

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.

Default route is a setting on a computer that defines the packet forwarding rule to use when no specific route can be determined for a given Internet Protocol (IP) destination address. All packets for destinations not established in the routing table are sent via the default route.

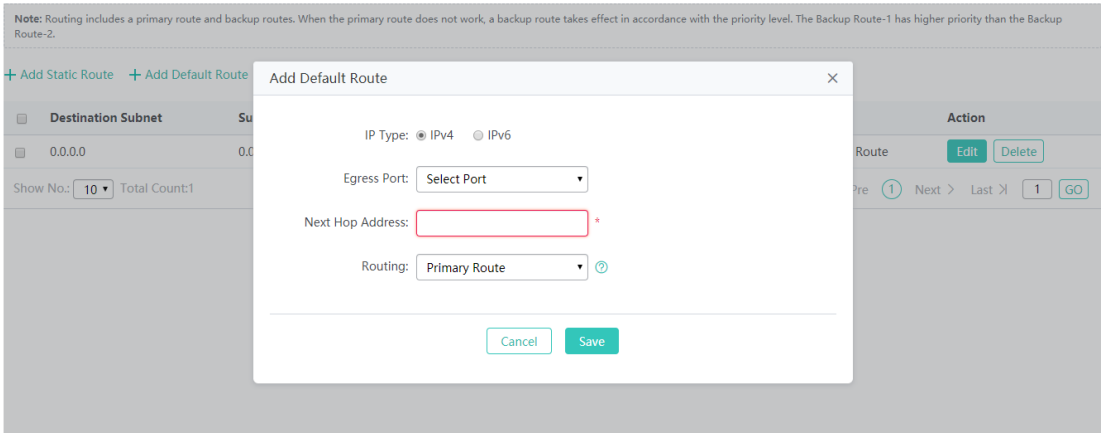


- **Adding a static route**



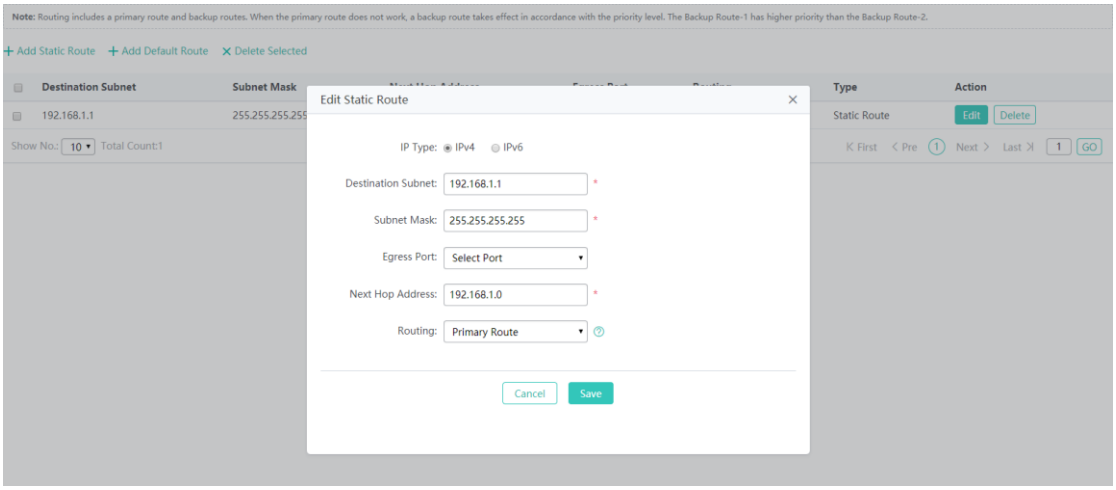
Click **Add Static Route**, set the configuration items in the dialog box displayed, and click **Save**. The newly added static route is displayed in the route list after the **Save operation succeeded** message is displayed.

- **Adding the default route**



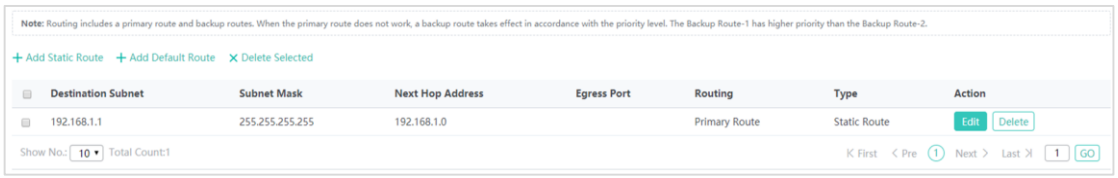
Click **Add Default Route**. Set the configuration items in the displayed dialog box, and click **Save**. The newly added route is displayed in the route list after the **Save operation succeeded** message appears.

- **Editing a route**



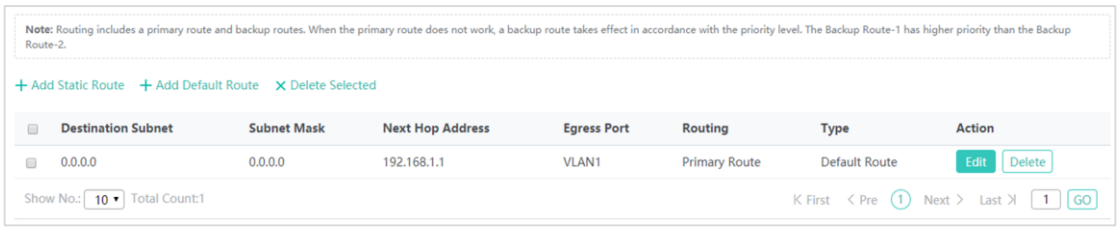
1. Click the **Edit** button for a route in the list.
2. A dialog box is displayed, as shown in the preceding figure. The configuration for the route is displayed. Next, edit the configuration.
3. Click **Save**. The **Save operation succeeded** message is displayed.

- **Deleting a route**



Click the **Delete** button for a route in the list and then click **OK** in the displayed dialog box to finish deleting.

- **Deleting routes in batches**



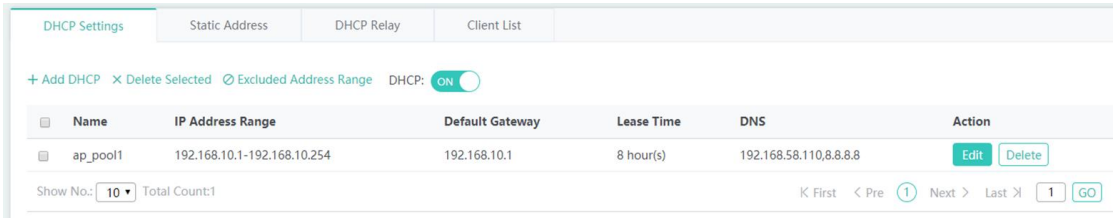
1. Select the route from the list.
2. Click **Delete Selected Route** to finish deleting.

4.4.3.5 DHCP

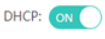
Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

DHCP supports three mechanisms for IP address allocation. In "automatic allocation", DHCP assigns a permanent IP address to a client. In "dynamic allocation", DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). In "static allocation", a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.

4.4.3.5.1 DHCP Settings

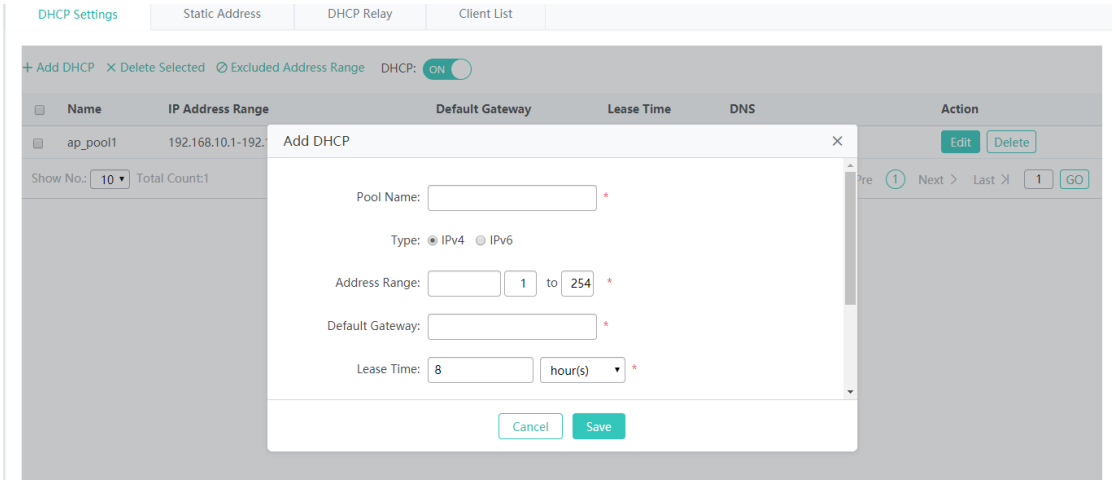


- **DHCP service**

  Click 

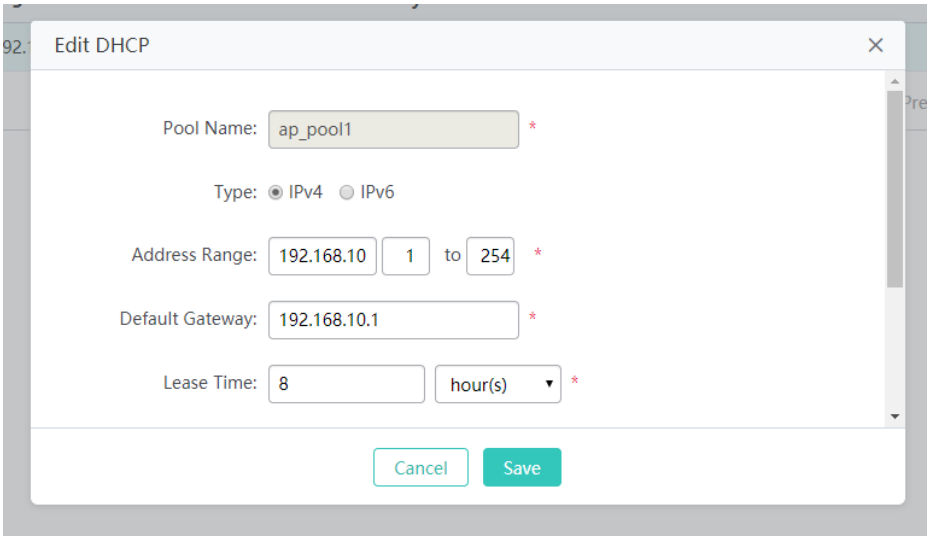
 to enable or disable the DHCP service.

- **Adding a DHCP Pool**



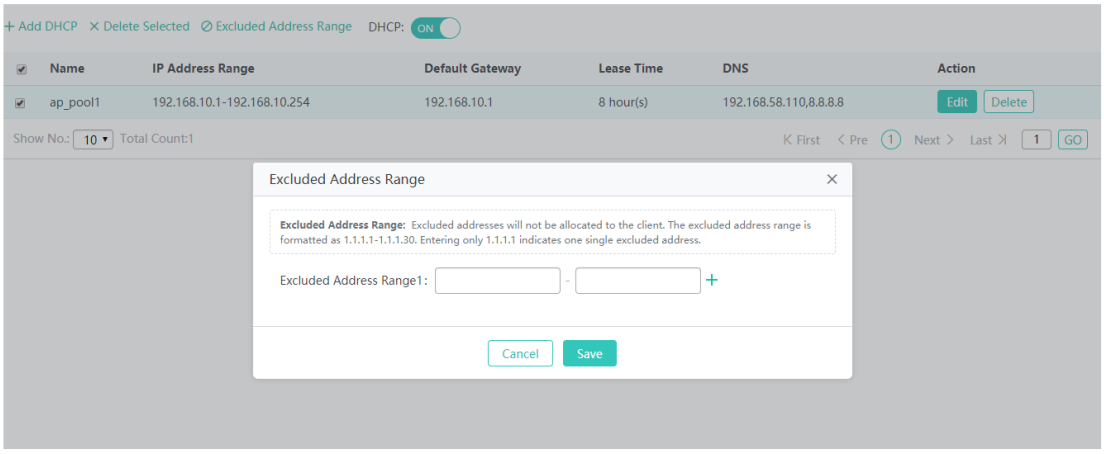
Click **Add DHCP**, set the configuration items in the dialog box displayed, and click **Save**. The newly added DHCP pool is displayed in the DHCP pool list after the **Save operation succeeded** message is displayed.

- **Editing a DHCP pool**



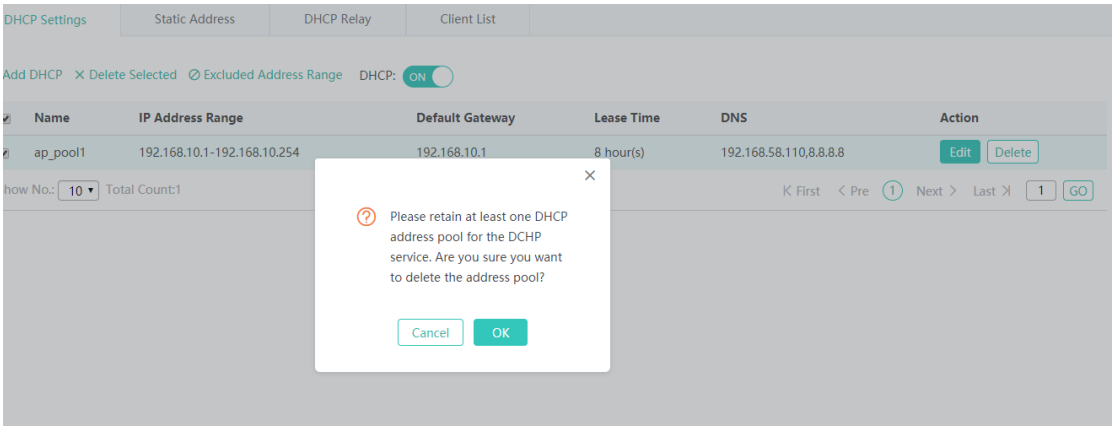
1. Click the **Edit** button for a DHCP pool in the list.
2. The configuration for the DHCP pool is displayed in the dialog box. Next, edit the configuration.
3. Click **Save**. The **Save operation succeeded** message is displayed

- **Configuring excluded address range**



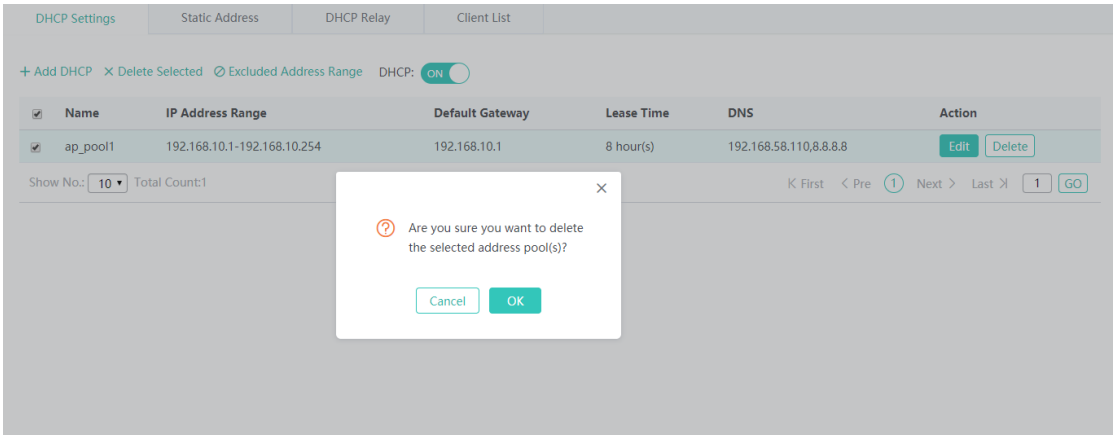
Click **Excluded Address Range**. A dialog box is displayed, as shown in the preceding figure. Set the configuration items in the displayed dialog box, and click **Save**. The newly configured address range is displayed in the DHCP pool list after the **Save operation succeeded** message is displayed.

- **Deleting a DHCP pool**



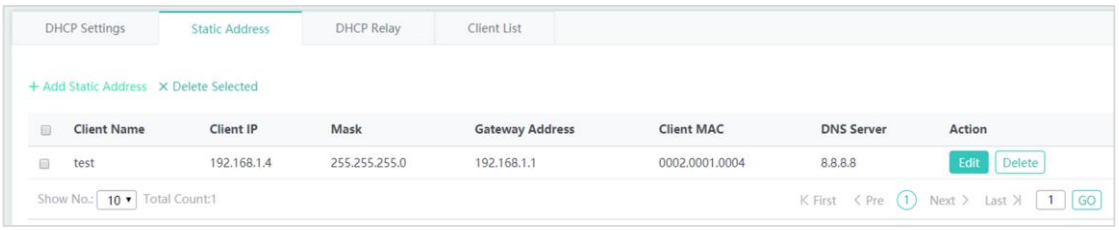
Click **Delete** to finish deleting.

- **Deleting DHCPs in batches**

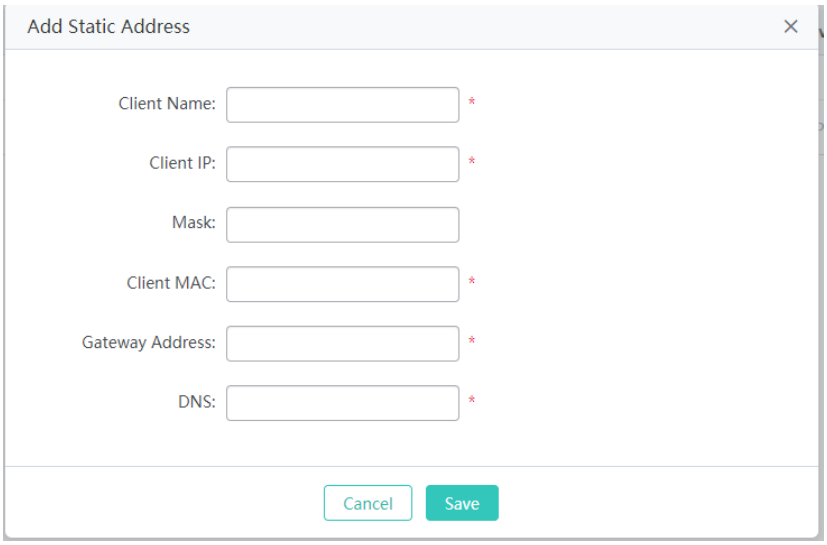


1. Select the DHCP pool from the list.
2. Click **Delete Selected DHCP** and then click **OK** in the dialog box displayed to finish deleting.

4.4.3.5.2 Static Address

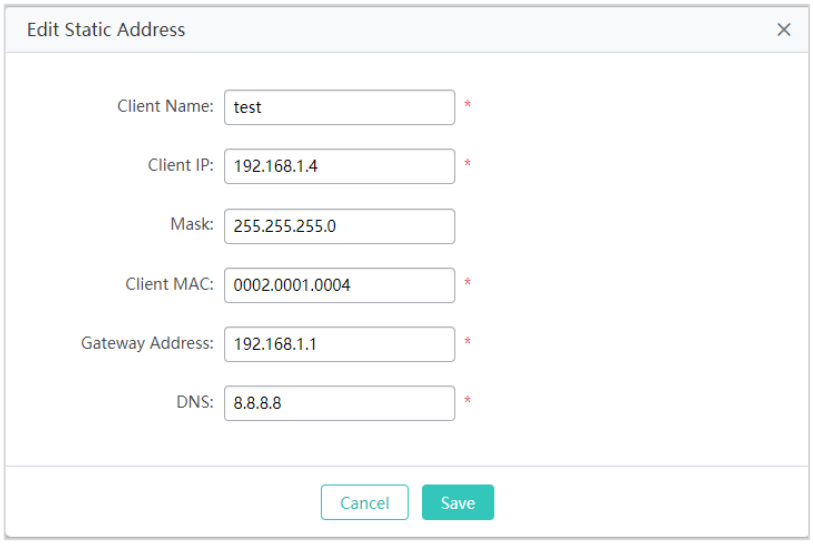


- **Adding a static address**



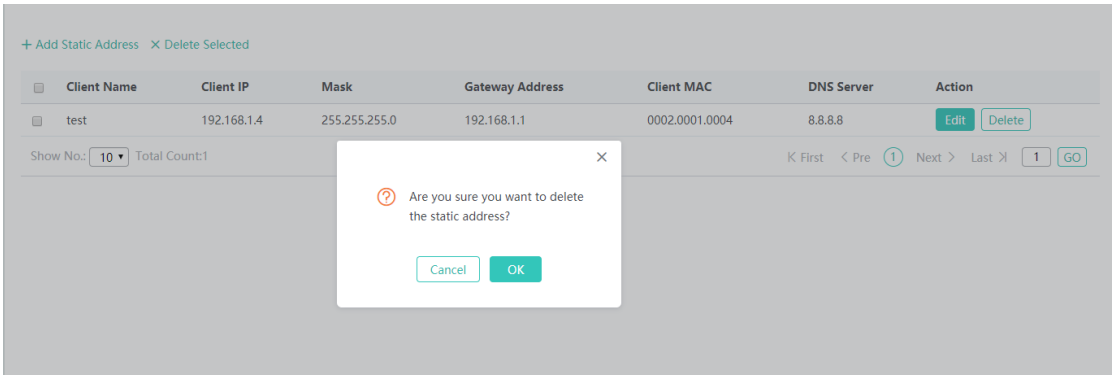
Click **Add Static Address**, set the configuration items in the displayed dialog box, and then click **Save**. The newly added static address is displayed in the list after the **Save operation succeeded** message is displayed.

- **Editing a static address**



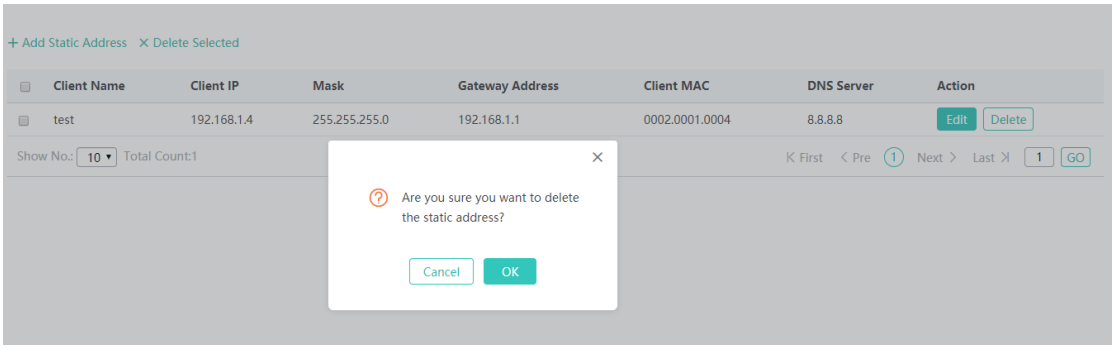
1. Click the **Edit** button for a static address in the list. A dialog box is displayed.
2. The configuration for the static address is displayed in the dialog box. Next, edit the configuration.
3. Click **Save**. The **Save operation succeeded** message is displayed.

- **Deleting a static address**



Click the **Delete** button for a static address in the list to finish deleting.

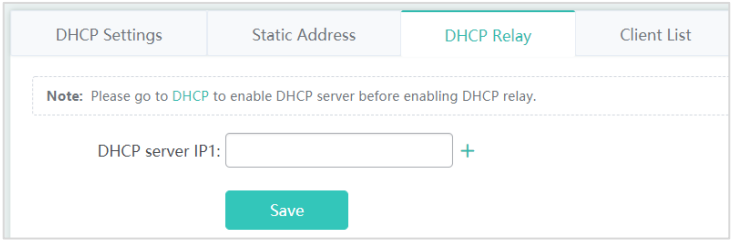
- **Deleting static addresses in batches**



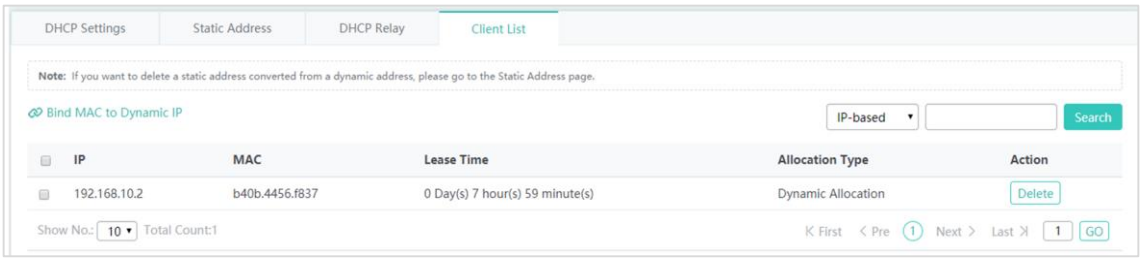
1. Select the static address from the list.
2. Click **Delete Selected Address** and then click **OK** in the dialog box displayed to finish deleting.

4.4.3.5.3 DHCP Relay

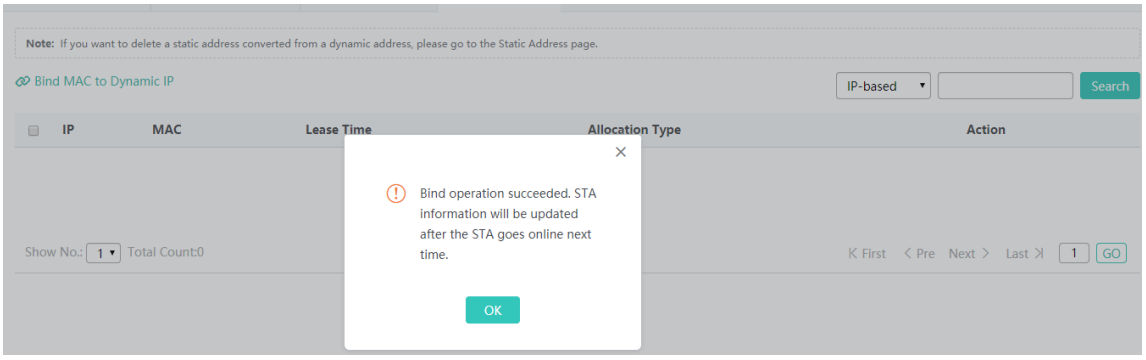
A DHCP relay agent is any host that forwards DHCP packets between clients and servers. You need to enable DHCP server before configuring DHCP relay, and then fill the DHCP server's IP address in the DHCP Relay page.



4.4.3.5.4 Client List

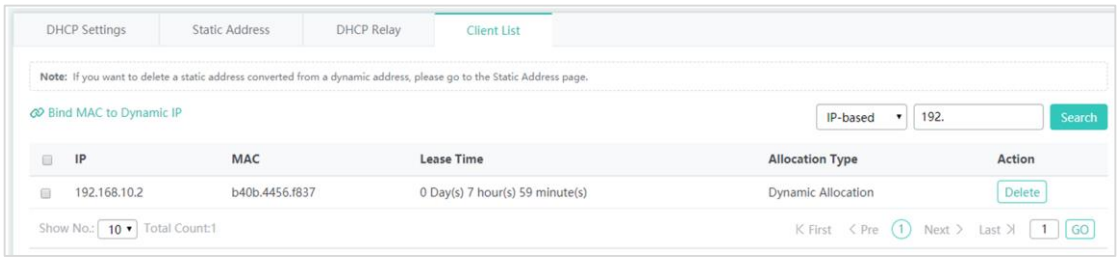


- **Binding a MAC address to a dynamic IP address**



1. Select the static address from the list.
2. Click **Bind MAC to Dynamic IP** and then click **OK** in the displayed dialog box to finish deleting.

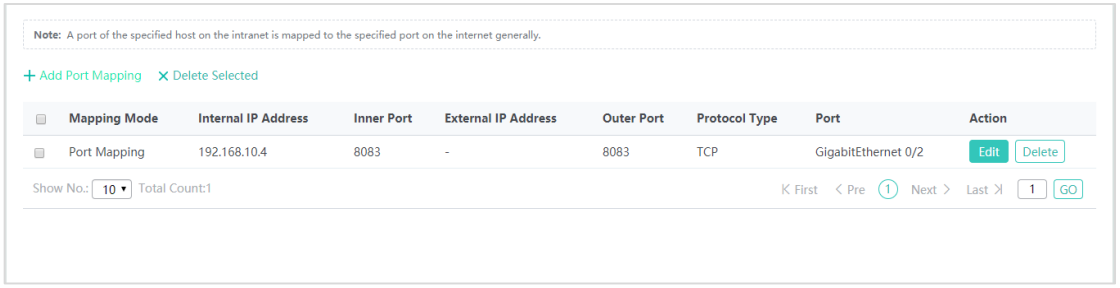
- **Querying clients based on IP address**



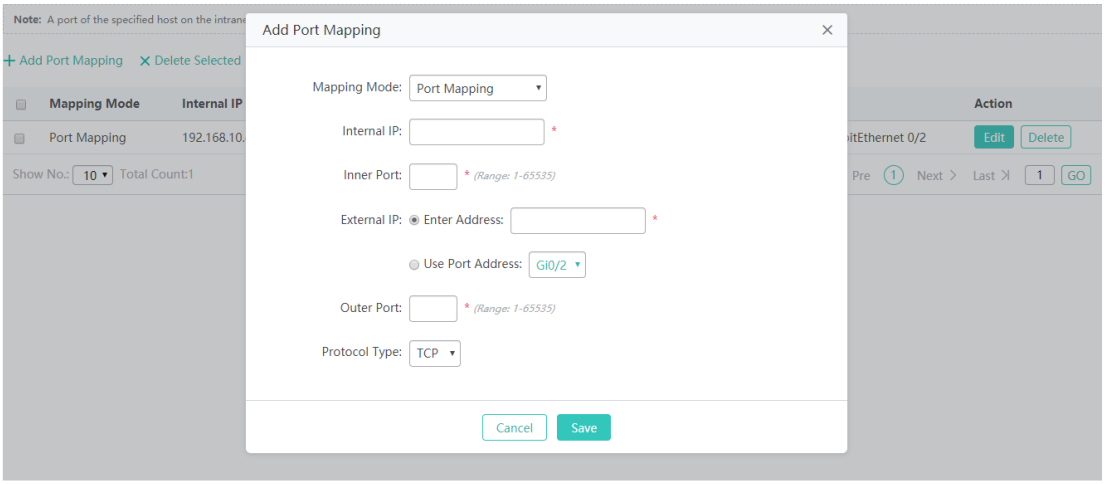
Input the IP address in the text box. Click **Search**. The search results meeting the criterion are displayed in the list.

4.4.3.5.5 Port Mapping

Generally, this function is used to map a specified port of a specified host in the internal network to a specified port of an external network address.



- **Adding port mapping**



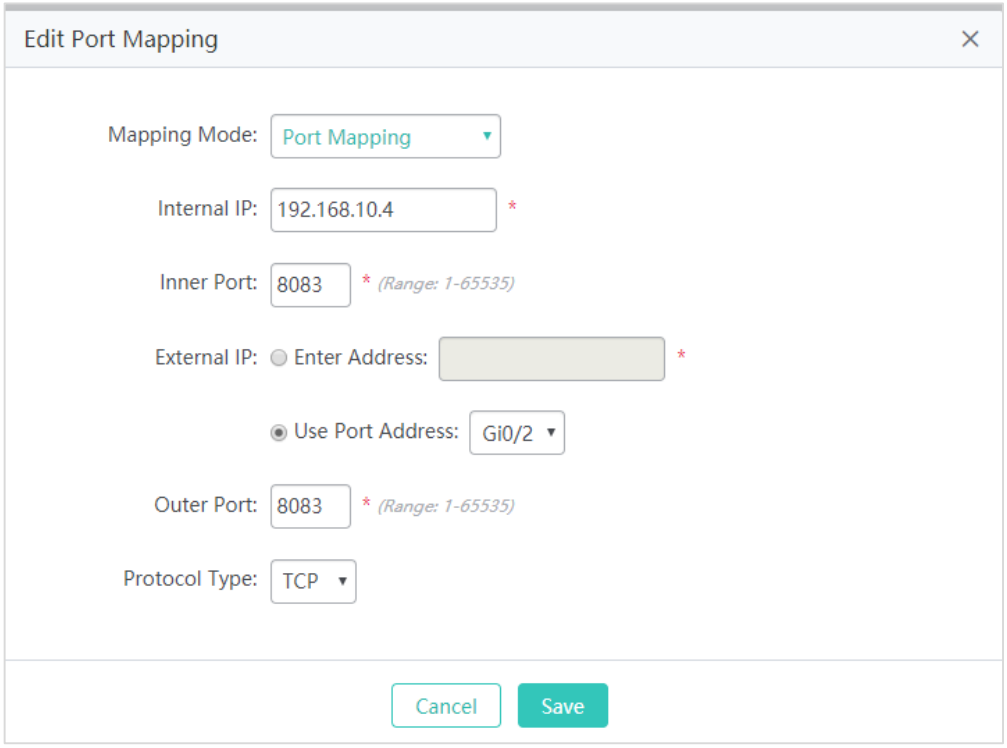
Click **Add Port Mapping**, set the configuration items in the dialog box displayed, and then click **Save**. The newly added port mapping is displayed in the list after the **Save operation succeeded** message is displayed.

- **Batch deleting port mapping entries**

1. Select the port mapping from the list.

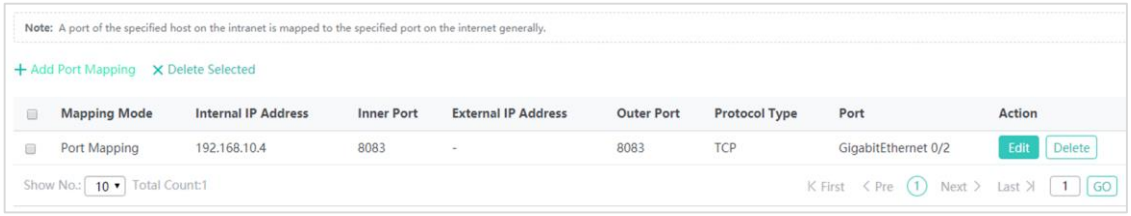
2. Click **Delete Selected Port Mapping** and then click **OK** in the displayed dialog box to finish deleting.

- **Editing port mapping**



1. Click the **Edit** button for a port mapping in the list.
2. The configuration for port mapping is displayed in the dialog box. Next, edit the configuration.
3. Click **Save**. The **Save operation succeeded** message is displayed.

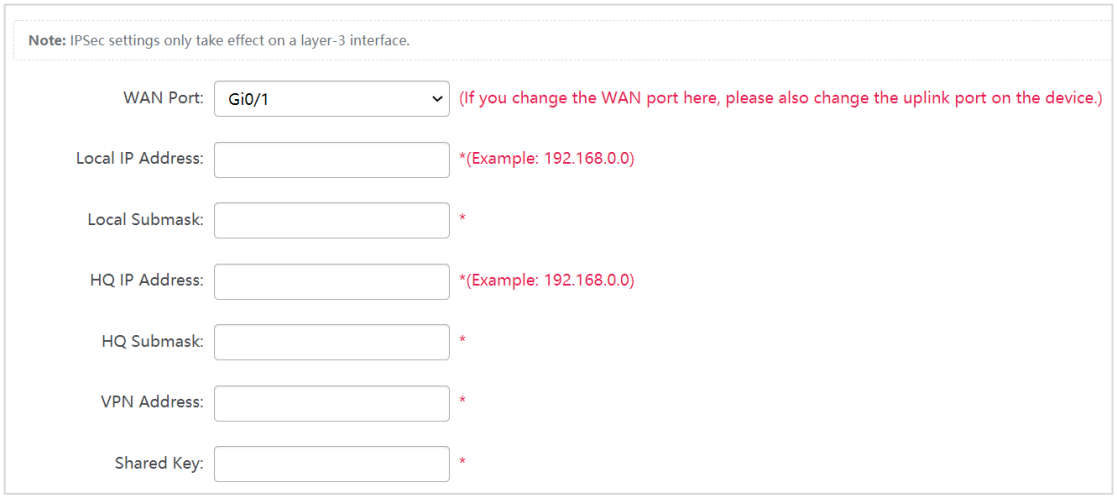
- **Deleting port mapping**



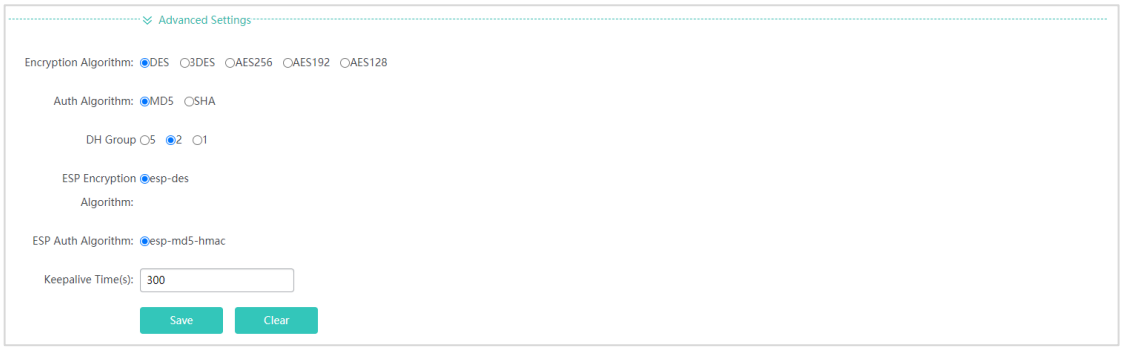
Click the **Delete** button for a port mapping entry in the list to finish deleting.

4.4.3.5.6 VPN

It is only allowed to configure VPN settings on a WAN port.



The **Advanced Settings** include some algorithm settings. It is recommended to use the default settings.

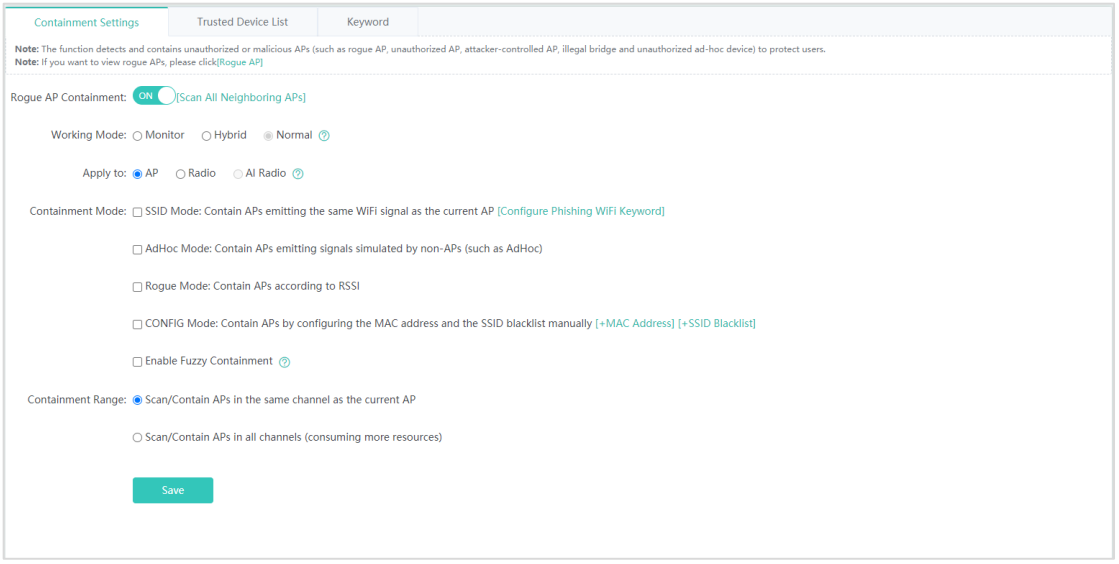


4.4.4 Security

Rogue APs may exist in a WLAN. Rogue APs may have security vulnerabilities and can be manipulated by attackers to seriously threaten and endanger network security. The containment function can be enabled on the AP to attack rogue devices and prevent other wireless STAs from being associated with rogue devices.

4.4.4.1 CONTAINMENT

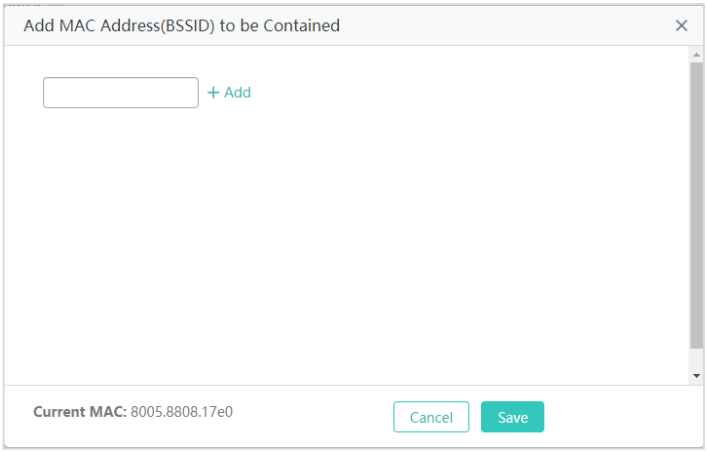
4.4.4.1.1Containment Settings



Click to enable or disable rogue AP containment for the device.

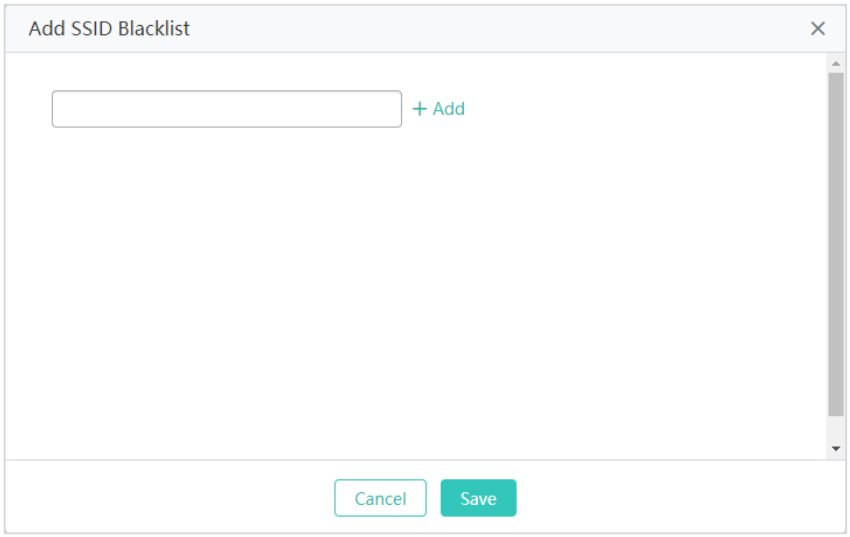
- **Adding a MAC address**

You can add the MAC address to be contained here.



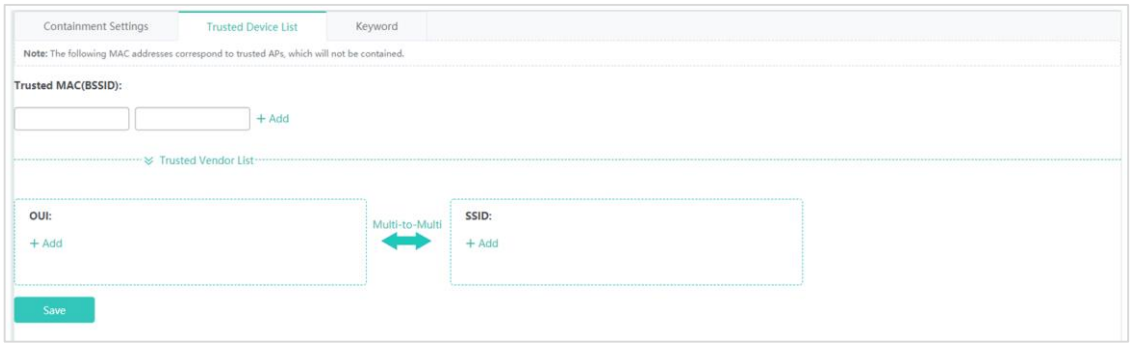
- **Adding an SSID blacklist**

You can add the MAC address to be contained here.



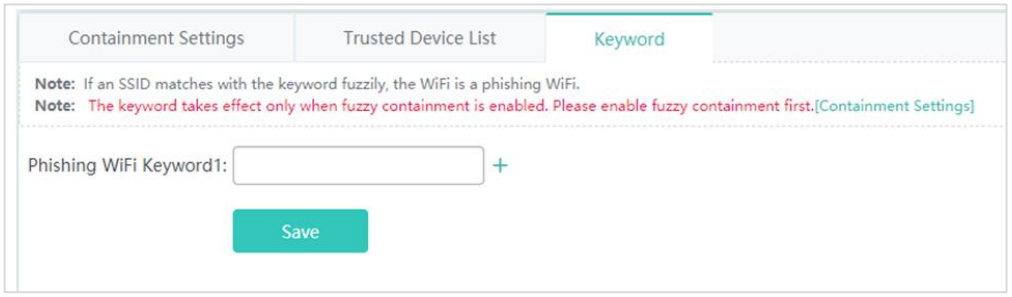
4.4.4.1.2 Trusted Device List

When the rogue AP containment function is enabled, the APs not authorized will be contained. However, some APs are trusted devices and special processing is required. You can configure the MAC addresses of trusted devices.



4.4.4.1.3 Phishing WiFi Keyword

If an SSID matches with the keyword fuzzily, the WiFi is a phishing WiFi.

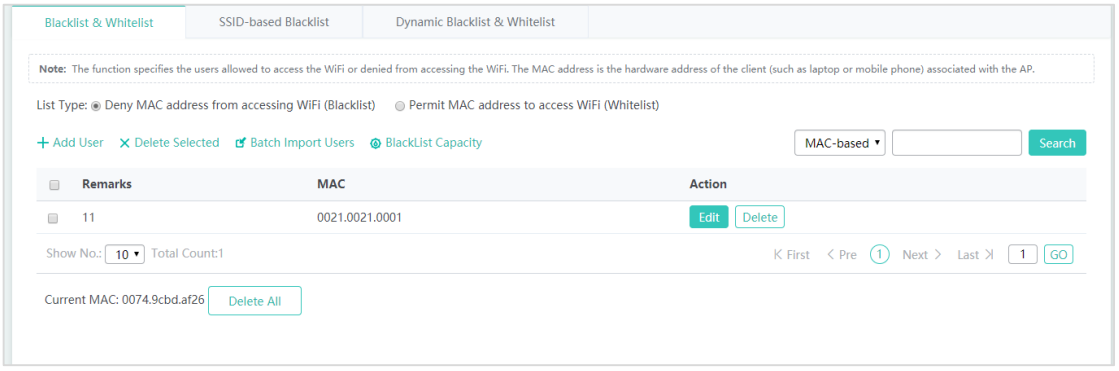


4.4.4.2 BLACKLIST & WHITELIST

4.4.4.2.1 Blacklist & Whitelist

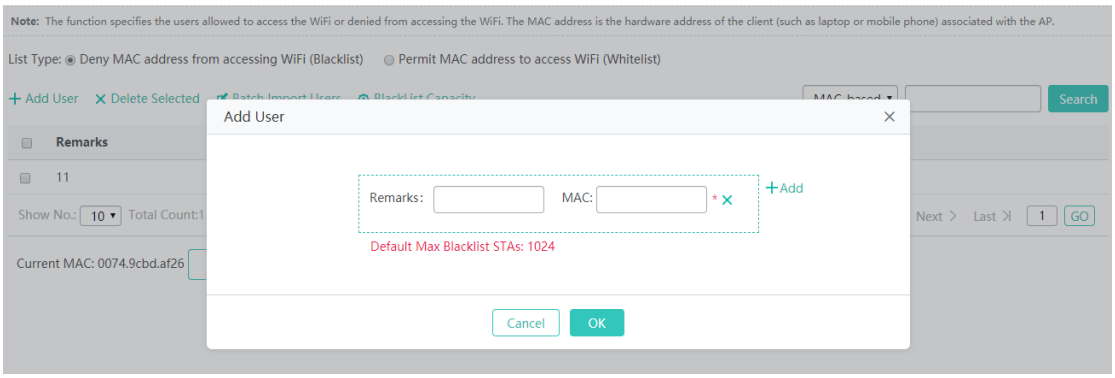
This function allows or blocks specified users from accessing the WiFi. The whitelist/blacklist capacity is 1024 by default.

Add the blacklist or whitelist user by adding the MAC address.

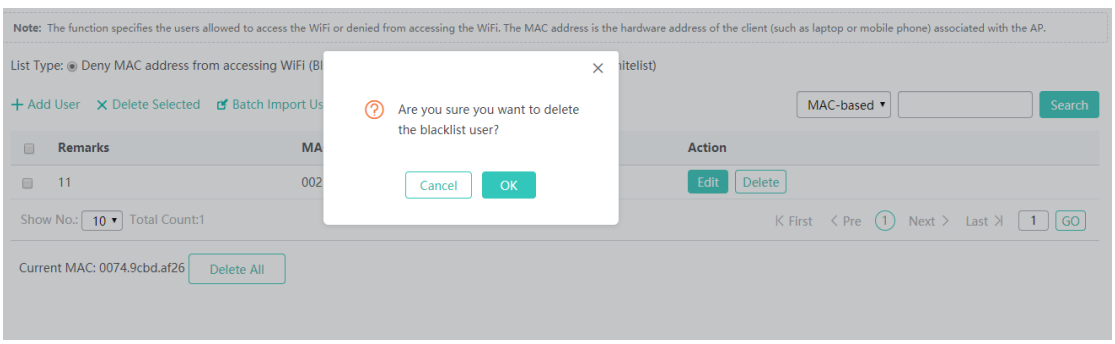


Click + Add User to add a MAC address for a user. You can add multiple MAC addresses.

Click the **SSID-based Access Control** link to configure the blacklist and whitelist for each WiFi.

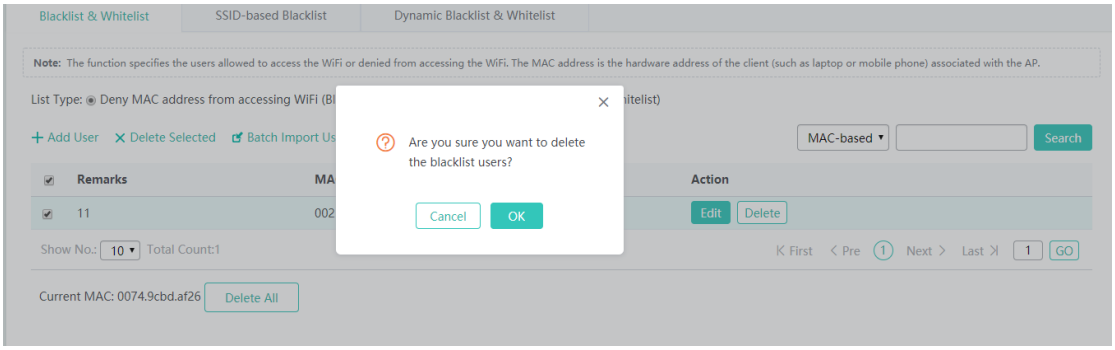


- **Deleting a blacklist user**



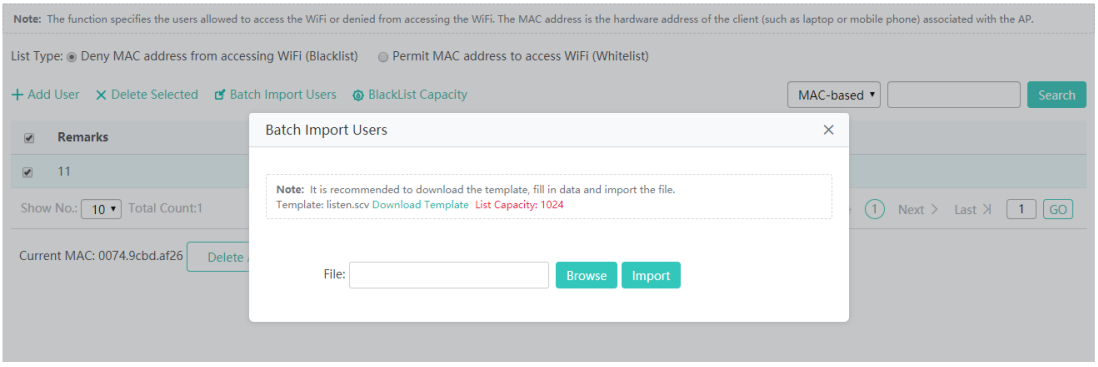
- **Deleting blacklist users in batches**

1. Select one or more records from the list.
2. Click **Delete Selected**.



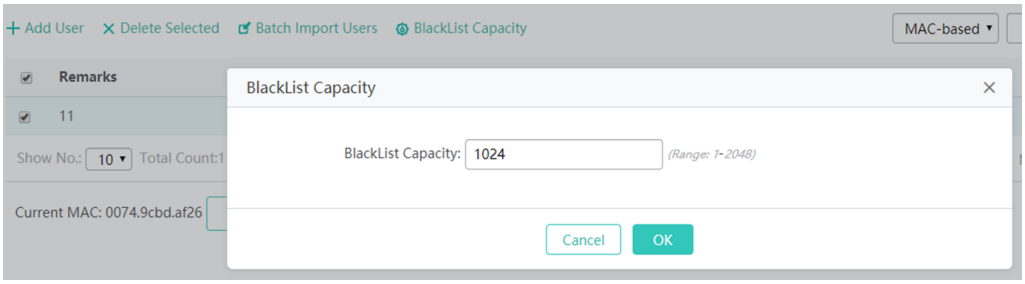
- **Importing blacklist users**

1. Click **Batch Import Users**.
2. Download the template file and enter the data.
3. Import the file.

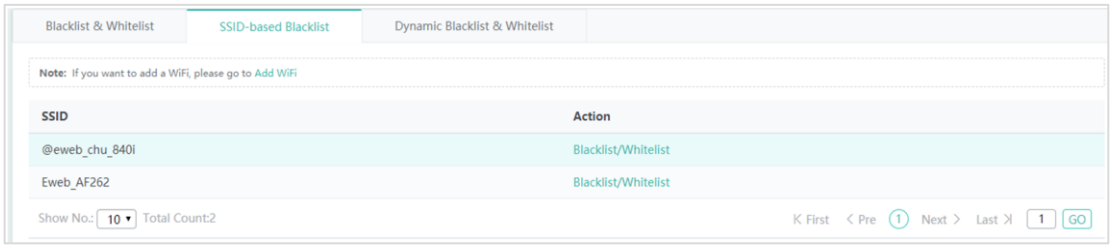


- **Setting blacklist capacity**

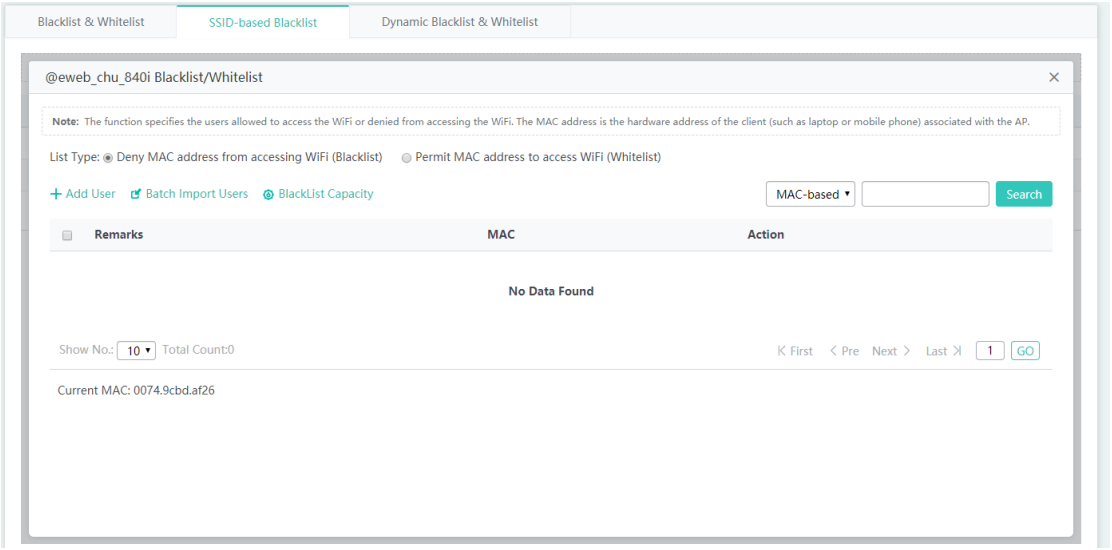
1. Click BlackList Capacity .
2. Enter a value.
3. Click **OK**. The message “Configuration succeeded.” will be displayed.



4.4.4.2.2 SSID-based Blacklist



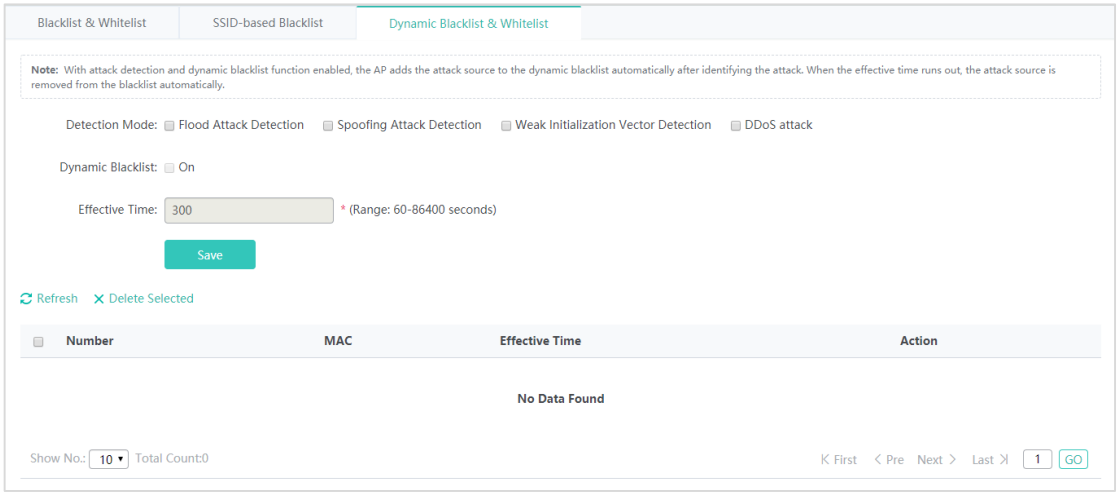
Click Blacklist/Whitelist in the list and configure the whitelist/blacklist for the specified SSID.



You can select the blacklist/whitelist type, add blacklist/whitelist users, import blacklist/whitelist users and set blacklist/whitelist capacity.

4.4.4.2.3 Dynamic Blacklist & Whitelist

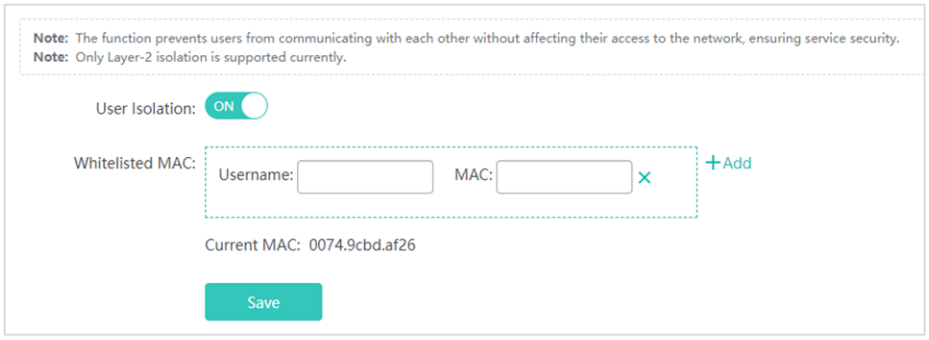
Add malicious attack sources to the dynamic blacklist to prohibit access.



1. Set the parameters and then save the configuration.
2. Select the blacklist from the list.
3. Click **Delete Selected** and then click **OK** in the displayed dialog box to finish deleting.

4.4.4.3 User Isolation

To ensure network security and prevent unwitting information transfer, you can prohibit communication between internal network users by means of configuration. Some special users (users who can access each other) can be identified based on the user name and MAC address.

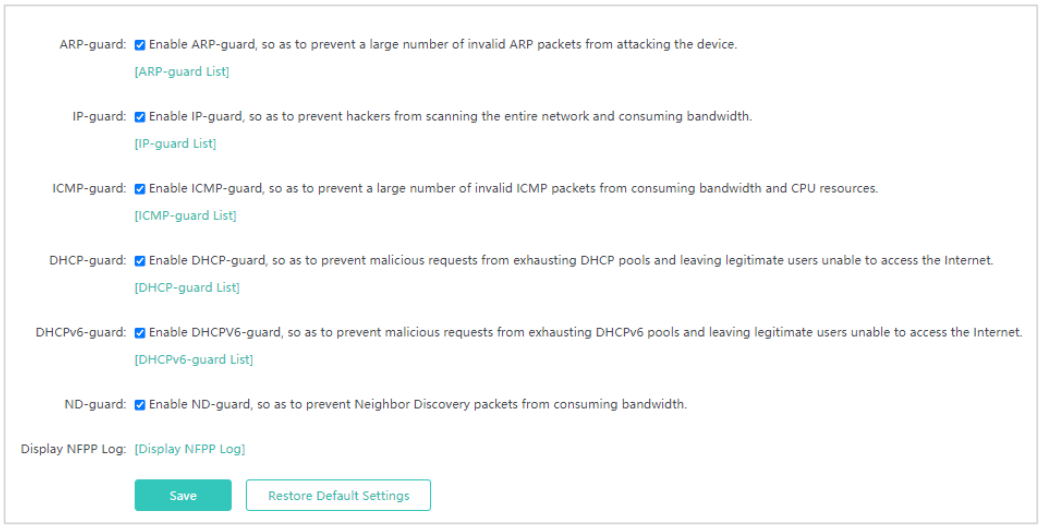


1. Click

to enable or disable mutual access for internal network users.
2. Click to delete the MAC address of the user.
3. Click the **Add** icon to add a MAC address for a mutual-access user. You can add multiple MAC addresses.
4. Click **Save** to finish the configuration.

4.4.4.4 ATTACK PROTECTION

Some malicious attacks are always found in the network environment. These attacks may bring about an extremely heavy burden for the switch, resulting in the switch using an excessive amount of CPU power and giving rise to a potential operational failure.



1. ARP-guard: Enables ARP-guard configuration. Click the **ARP-guard List** link to view the host where ARP attack is detected.

2. IP-guard: Enables IP-guard configuration. Click the **IP-guard List** link to view the host where IP scanning is detected.

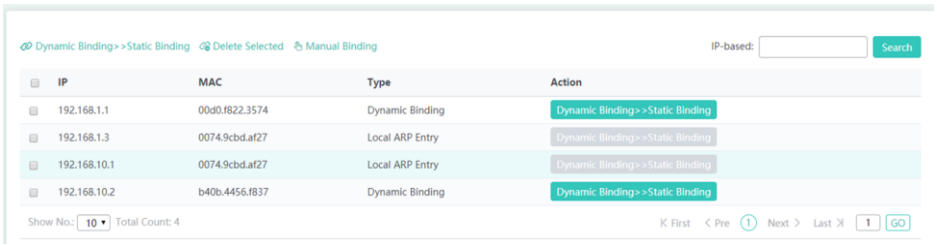
3. ICMP-guard: Enables ICMP-guard configuration. Click the **ICMP-guard List** link to view the host where an ICMP attack is detected.

4. DHCP-guard: Enables DHCP-guard configuration. Click the **DHCP-guard List** link to view the host where a DHCPv4 attack is detected.

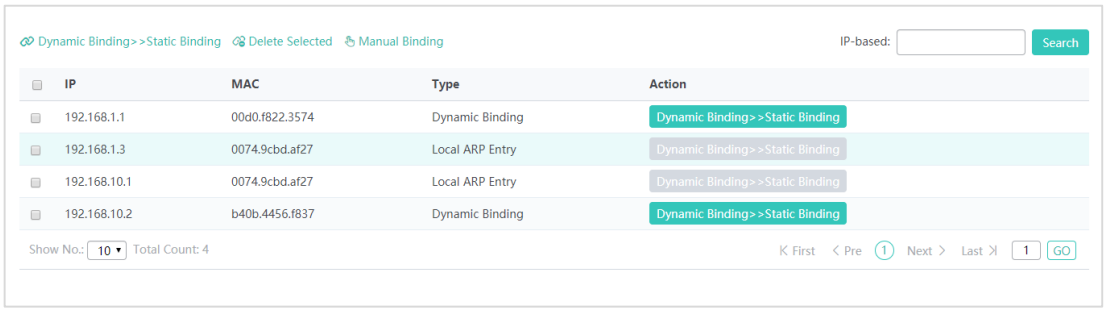
5. DHCPv6-guard: Enables DHCPv6-guard configuration. Click the **DHCPv6-guard List** link to view the host where a DHCPv6 attack is detected.

6. ND-guard: Enables ND-guard configuration.

4.4.4.5 ARP



- **Dynamic Binding>>Static Binding**



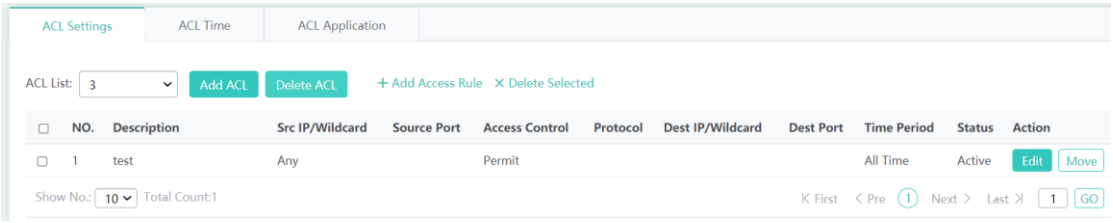
1. Select one or multiple records from the ARP list.
2. Click the **Dynamic Binding>>Static Binding** icon to switch from dynamic binding to static binding in batches.

4.4.4.6 ACL

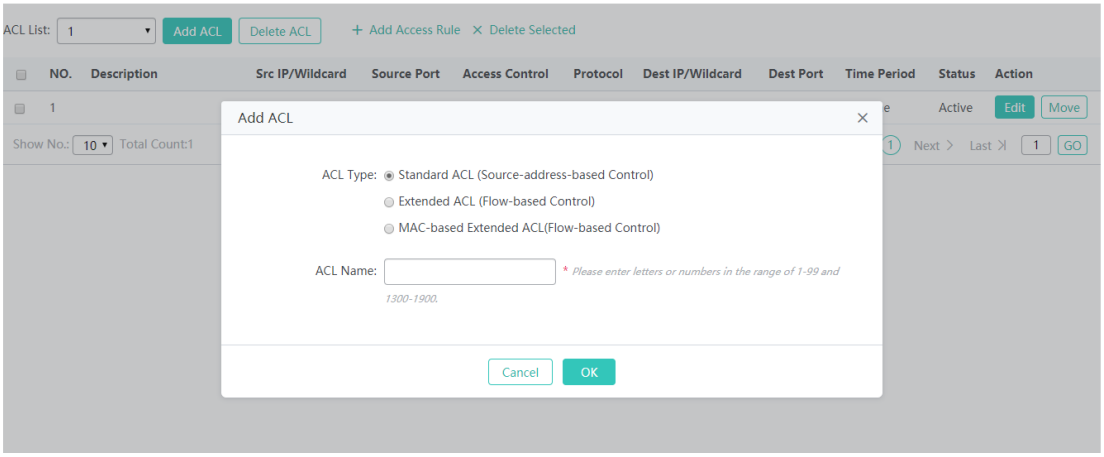
When receiving a packet on a port, the input ACL checks whether the packet matches the ACE entry for this port. When the device intends to output a packet through a port, the output ACL checks whether the packet matches the ACE entry for this port.

When there are different filtration rules, multiple rules may be applied simultaneously and only several of them can be applied. If a packet matches an ACE entry, this packet is processed (permitted or denied) according to the action policy defined by this ACE.

4.4.4.6.1 ACL Settings

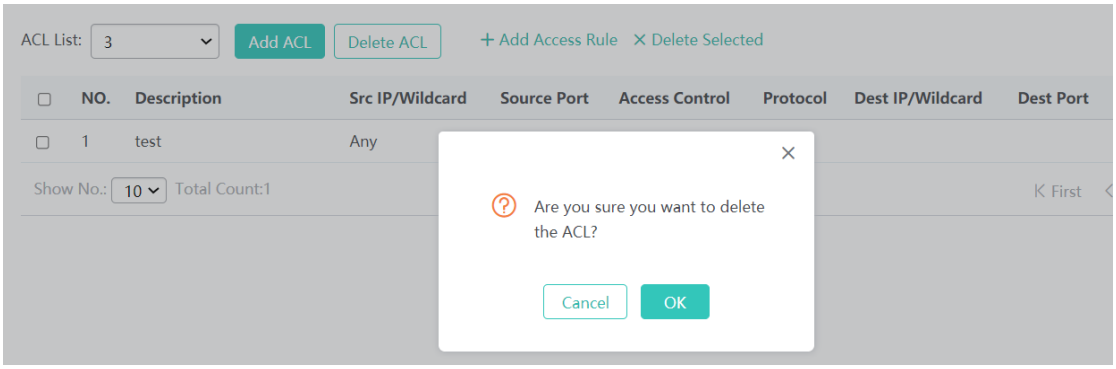


- **Adding an ACL**



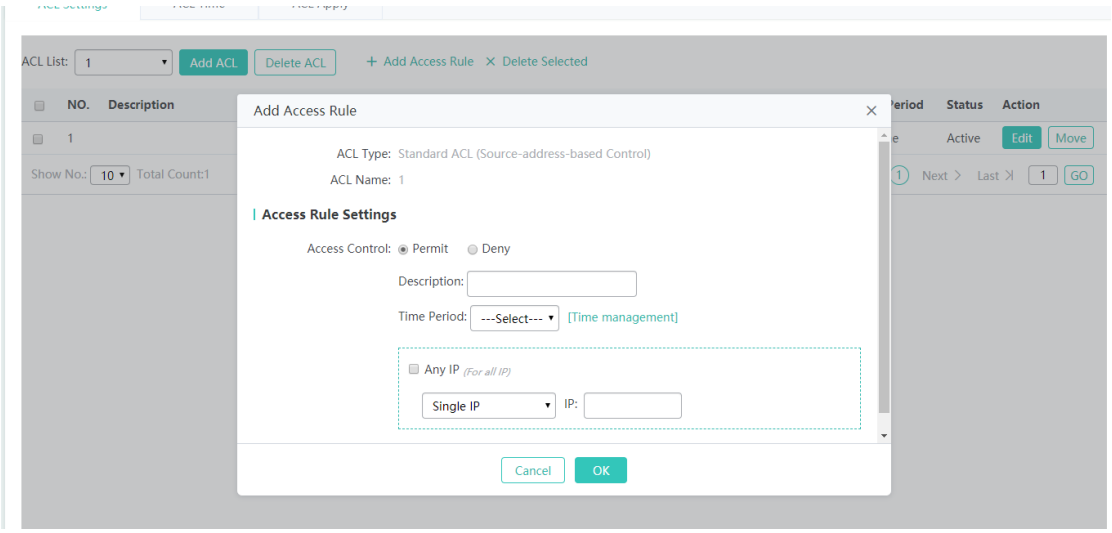
Click **Add ACL** and set the configuration items in the dialog box displayed. Click **OK**. The newly added ACL is displayed in the **ACL List** drop-down list on the left after the **Save operation succeeded** message is displayed.

- **Deleting an ACL**



1. Select the ACL from the **ACL List** drop-down list.
2. Click **Delete ACL** to finish deleting.

- **Adding an access rule**

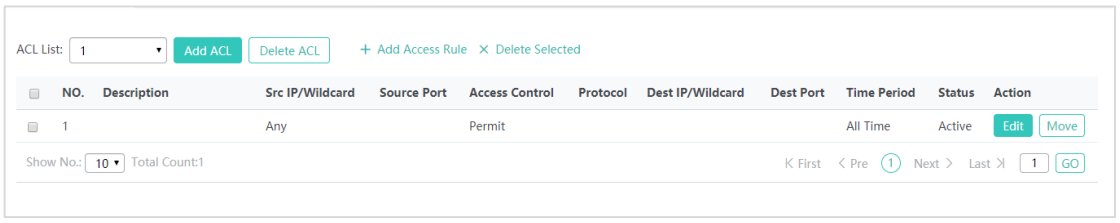


1. Click **Add Access Rule**.
2. Set the configuration items in the dialog box displayed.
3. Click **OK**. The newly added access rule is displayed in the access rule list after the Save operation succeeded message is displayed.

- **Editing an access rule**

1. Click the Edit button for an access rule in the access rule list.
2. The configuration for the access rule is displayed in the dialog box and it can be edited.
3. Click OK. The Save operation succeeded message is displayed.

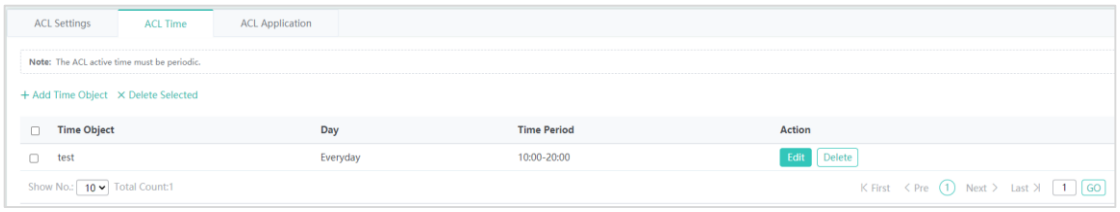
- **Deleting an access rule**



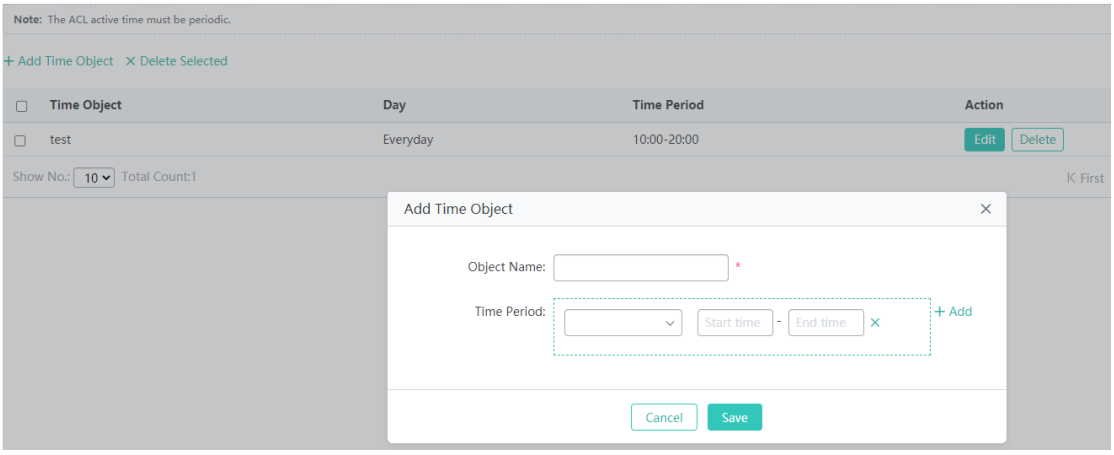
1. Select one or multiple records from the access rule list.
2. Click **Delete Selected** and then click **OK** in the displayed dialog box to finish deleting

4.4.4.6.2 ACL Time

ACLs based on time can be enabled. For example, you can set ACLs to take effect in different time segments for a week, but first a time object must be configured.

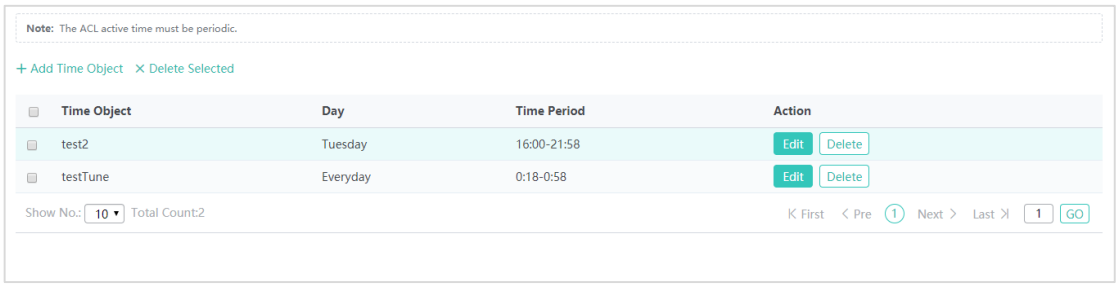


- **Adding a time object**



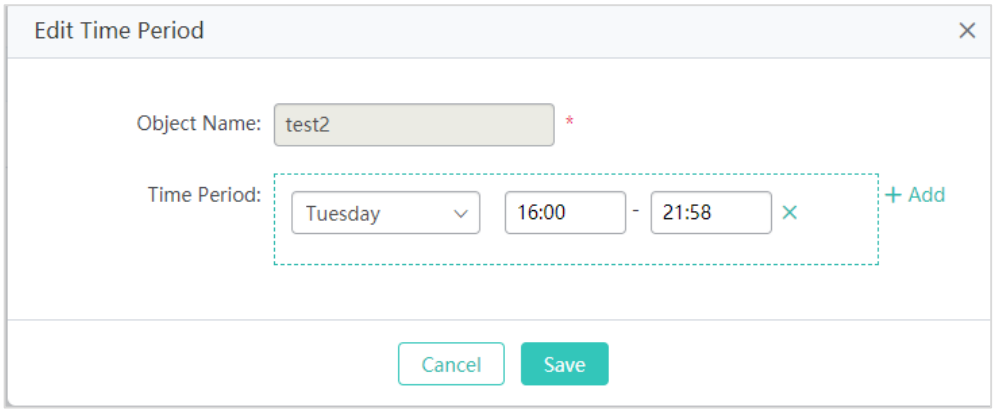
Click **Add Time Object**, then set the configuration items in the dialog box displayed, and click **Save**. The newly added time object is displayed in the time object list after the **Save operation succeeded** message is displayed.

- **Deleting time objects in batches**



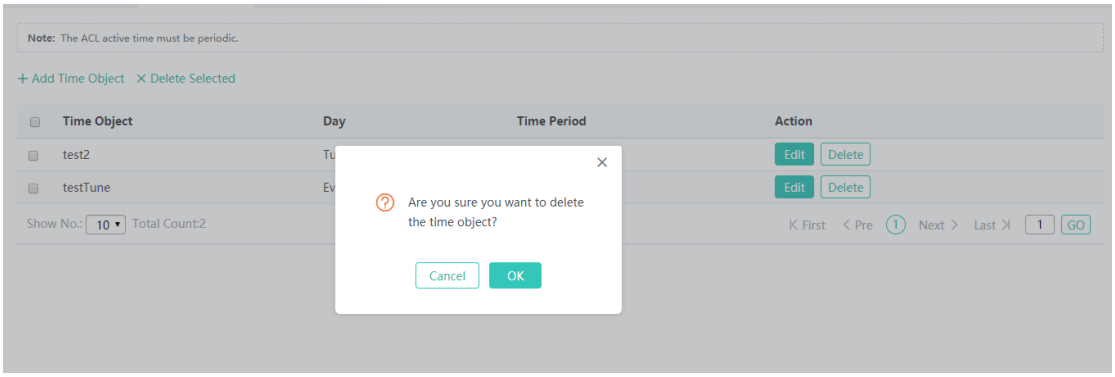
1. Select one or multiple records from the time object list.
2. Click **Delete Selected** and then click **OK** in the dialog box displayed to finish deleting.

- **Editing a time object**



1. Click the **Edit** button for a time object in the list.
2. The configuration about the time object is displayed in the dialog box. Then edit the configuration.
3. Click **Save**. The **Save operation succeeded** message is displayed.

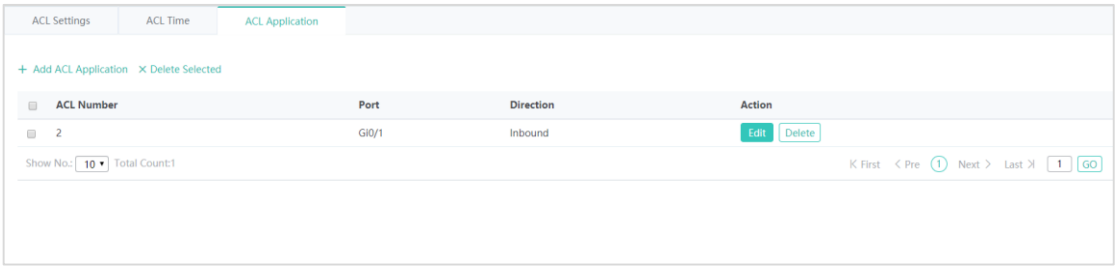
- **Deleting a time object**



Click the **Delete** button for a time object in the list.

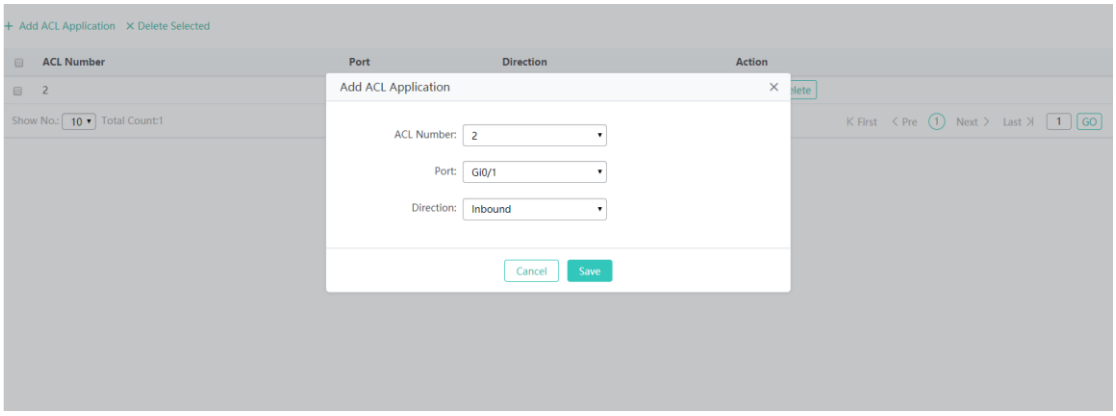
4.4.4.6.3 ACL Application

Apply an ACL to a port or a WiFi to limit user access.

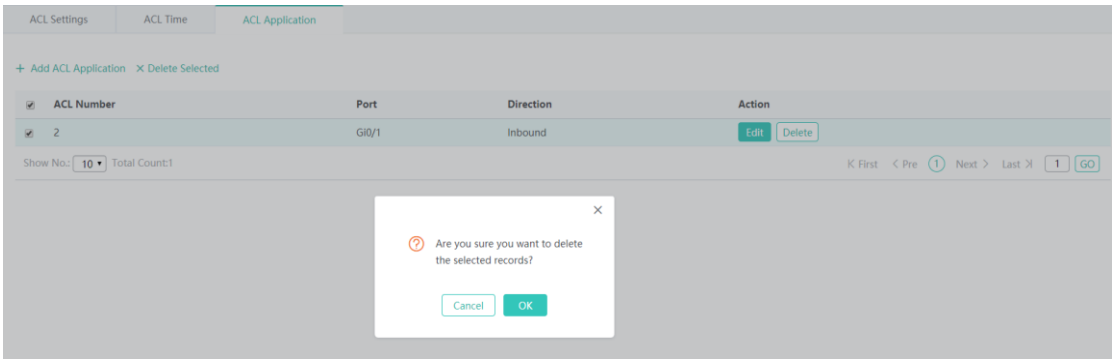


- **Adding an ACL application**

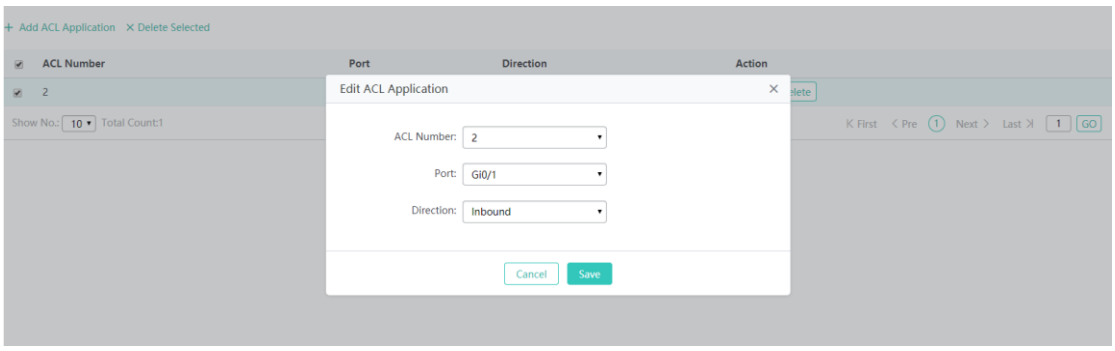
1. Click + Add ACL Application .
2. Select ACL number, port and direction in the popup window.
3. Click **Save**. After the message “Configuration succeeded.” is displayed, the ACL will appear in the list.



- **Deleting selected ACL applications**



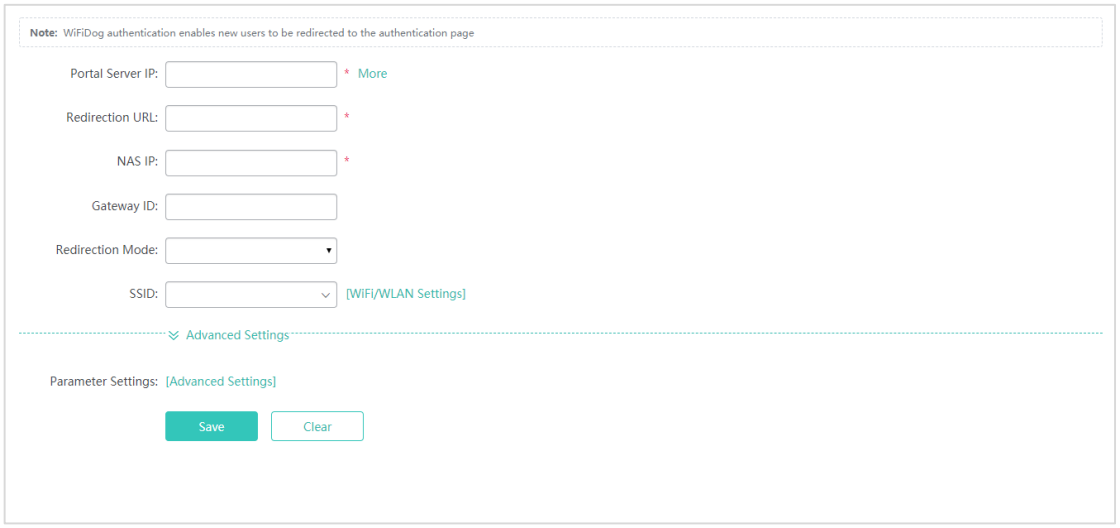
- **Editing an ACL application**



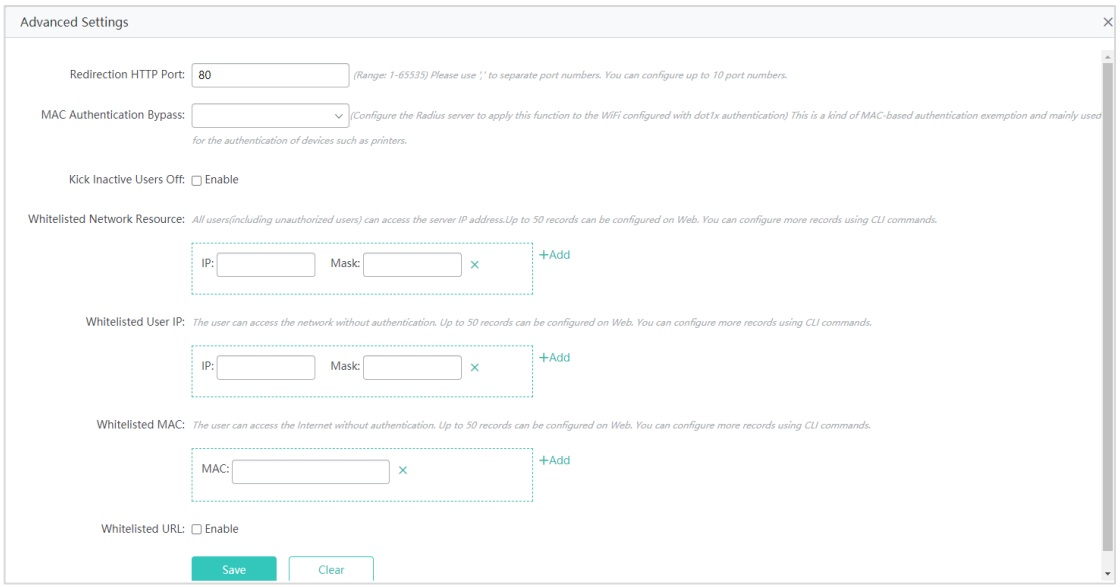
4.4.5 Authentication

4.4.5.1 WiFiDog Authentication

WiFiDog Authentication enables new users to be redirected to the authentication page.



Advanced Settings provide some optional features applicable to both Web authentication V1 and Web authentication V2.

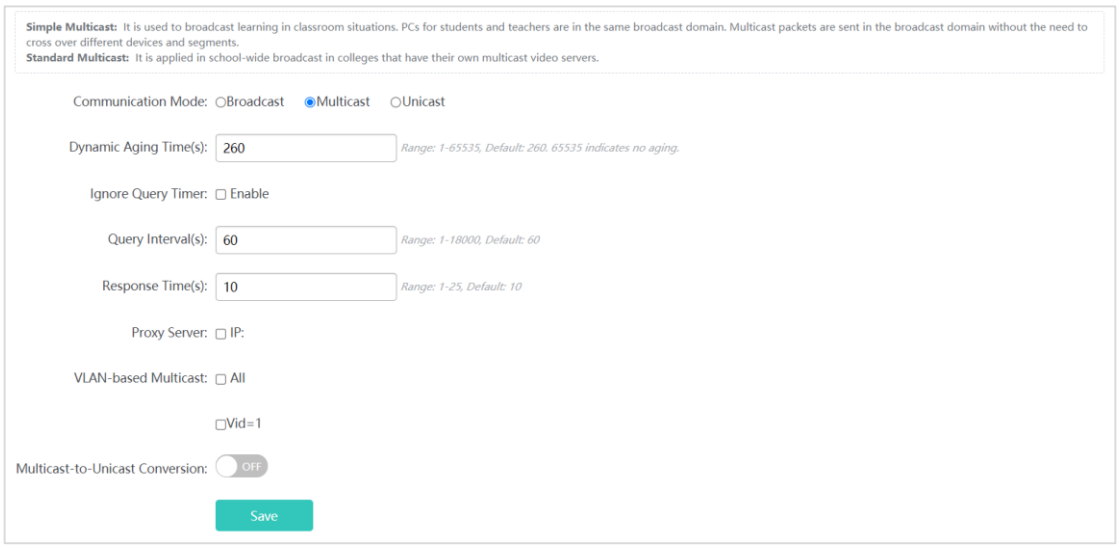


4.4.6 Advanced

4.4.6.1 MULTICAST/UNICAST

Unicast refers to a one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a network address.

Multicast is group communication where information is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.

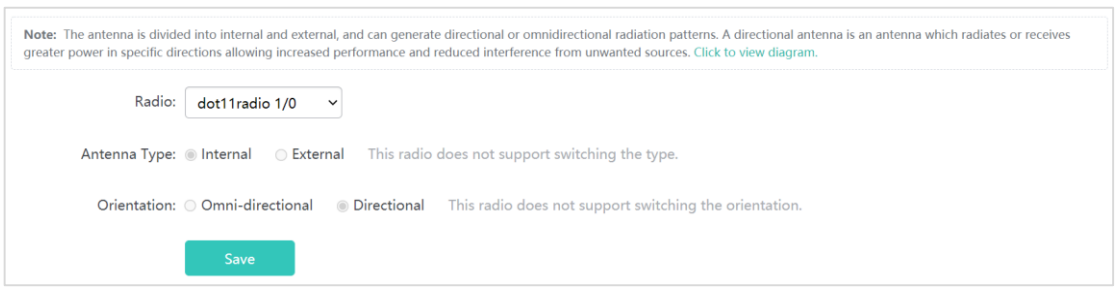


Set parameters as required, and then click **Save**.

4.4.6.2 ANTENNA

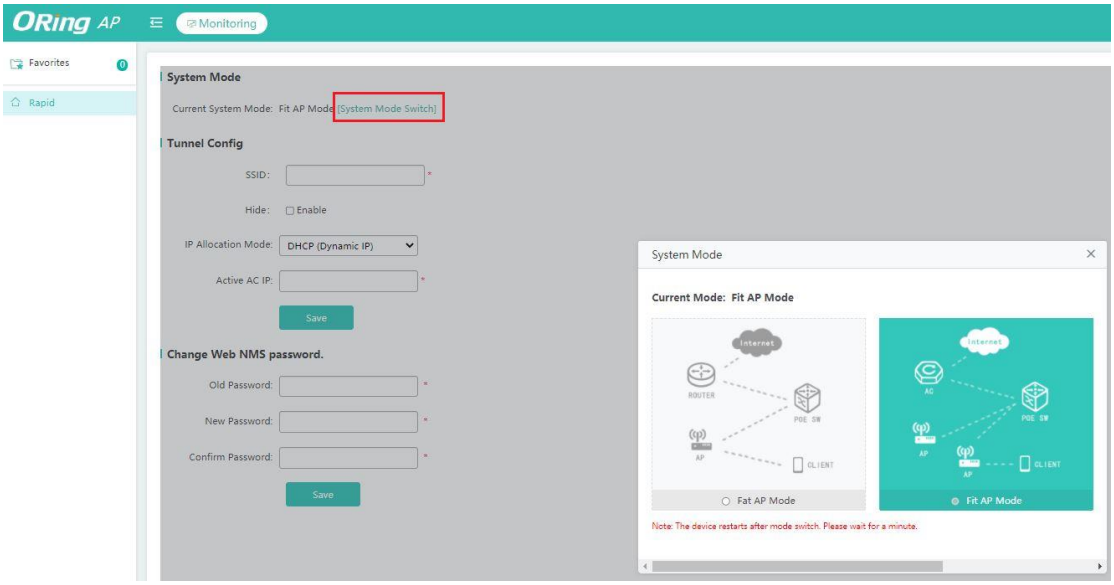
The antenna is divided into internal and external, and can generate directional or omnidirectional radiation patterns. Whether antenna type switchover and orientation switchover are supported depends on the radio capacity, which is displayed on the page.

IGAP-W99110GP+ built-in internal directional antenna, and it cannot switch to another antenna type and orientation.



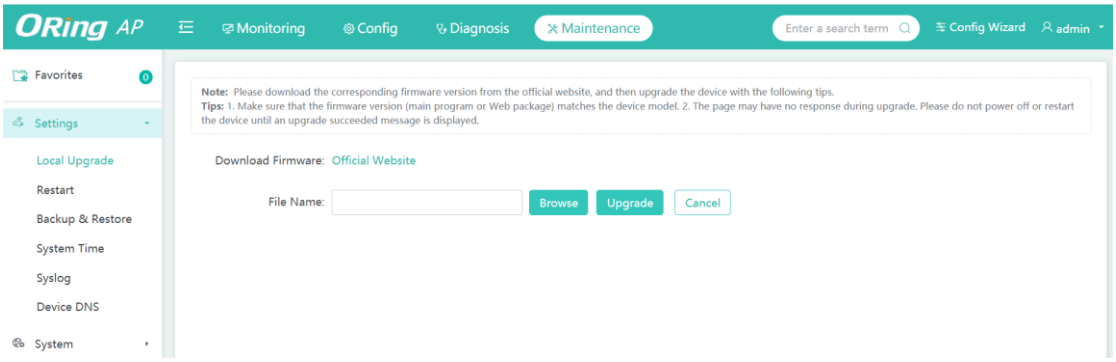
4.4.7 Rapid

After press the hardware reset button and then access to web interface, it will show **Rapid** page for configuration. System mode will be turned to Fit AP mode after system resetting. In order to use full function normally, please press **System Mode Switch** for switching to **Fat AP mode**.



Fat AP mode: System mode for IGAP-W99110GP+
Fit AP mode: Reserve for further use. NOT support at the current stage.

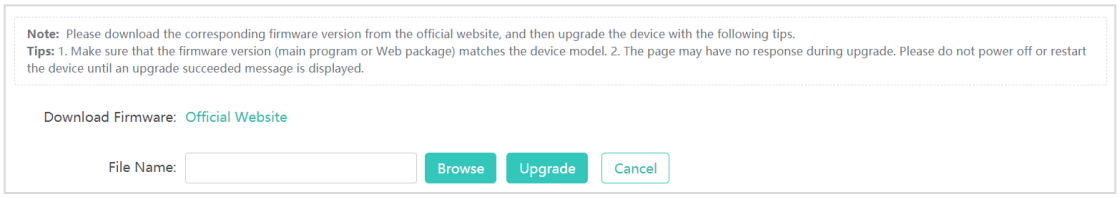
4.5 Maintenance



4.5.1 Settings

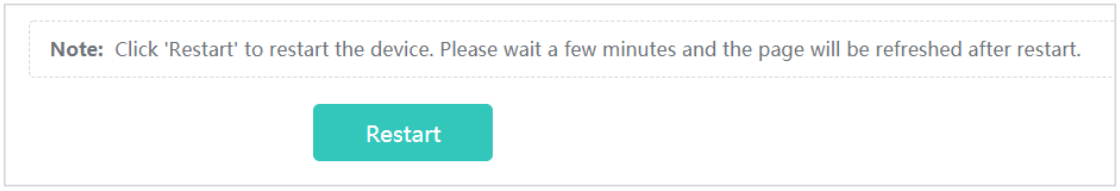
4.5.1.1 Local Upgrade

This page allows you to upgrade firmware. We suggest to use the latest firmware before installing the switch to the customer site. Please download the latest firmware from ORing website.



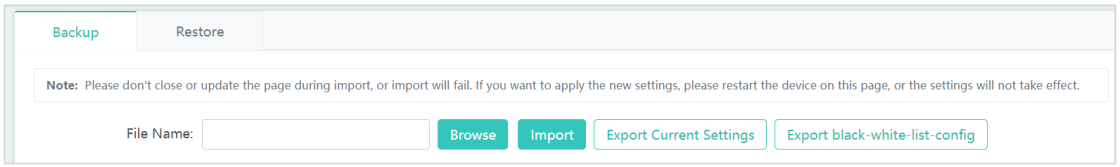
4.5.1.2 Restart

Click the Restart button to restart the system.



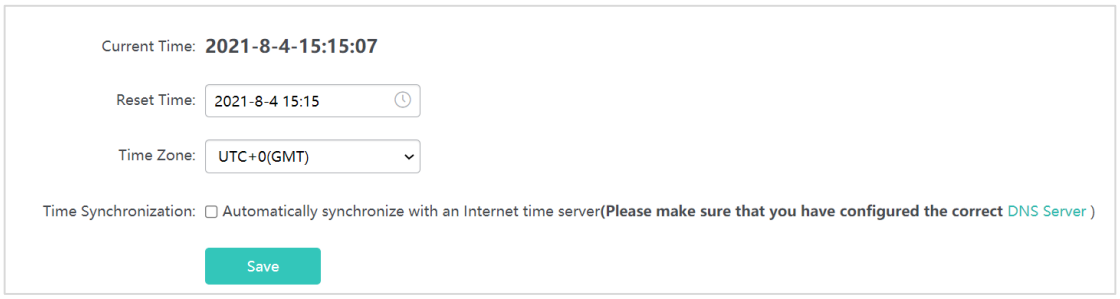
4.5.1.3 Backup & Restore

This item allows you to import or export the configuration file. You can also click on Restore page to **Restore Factory Settings**.



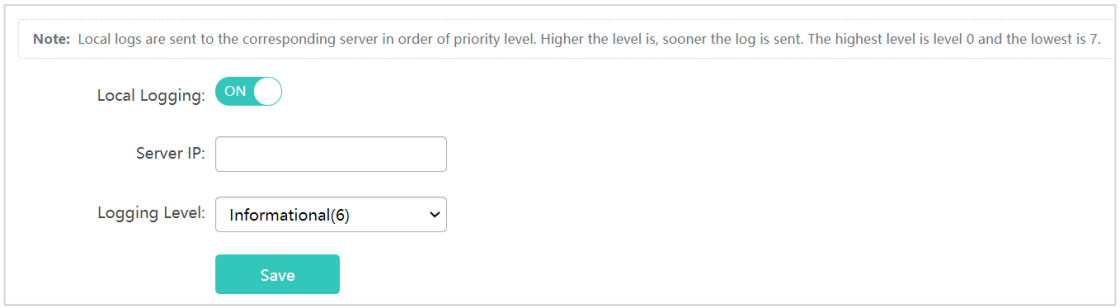
4.5.1.4 SYSTEM TIME

This page allows you to reset the system time or synchronize the time from an Internet time server



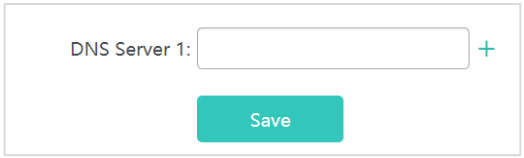
4.5.1.5 SYSLOG

System Log is useful to provide system administrator locally or remotely monitor switch events history. Please type the server IP address and select the logging level.



4.5.1.6 DEVICE DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates much information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. You could and one or more DNS servers in this page.

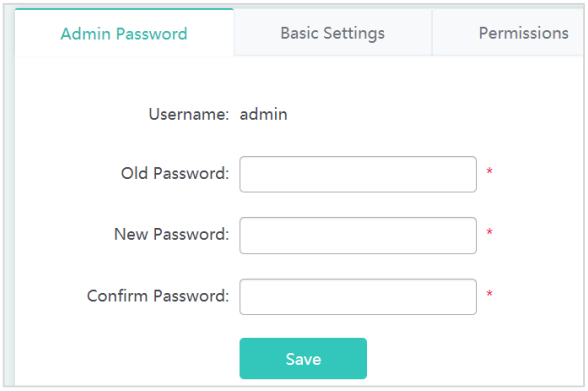


4.5.2 System

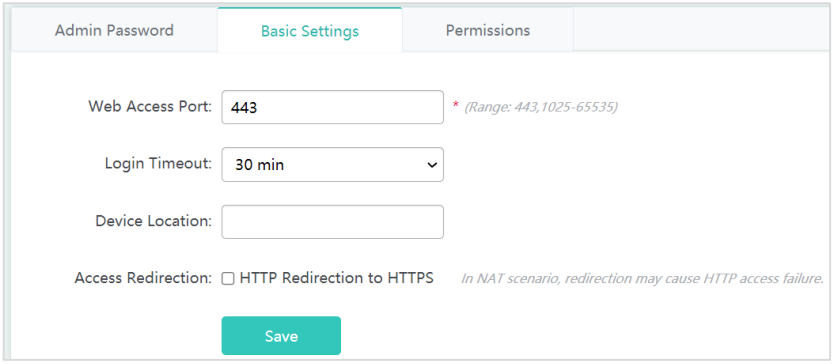
4.5.2.1 WEB

- **Admin Password**

  Change the password of admin.

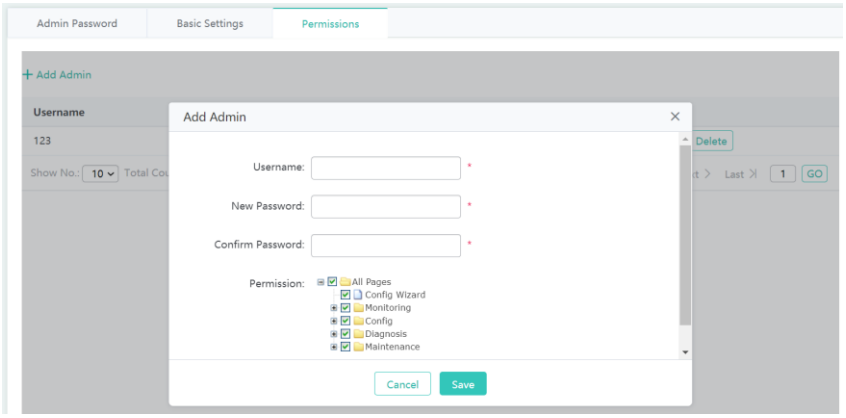


- **Basic Settings**



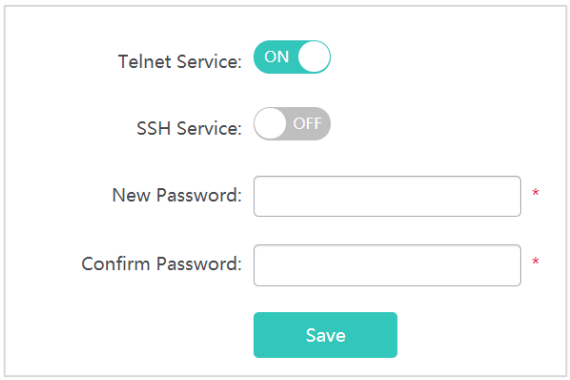
- **Permissions**

  Add more user accounts with different permission.



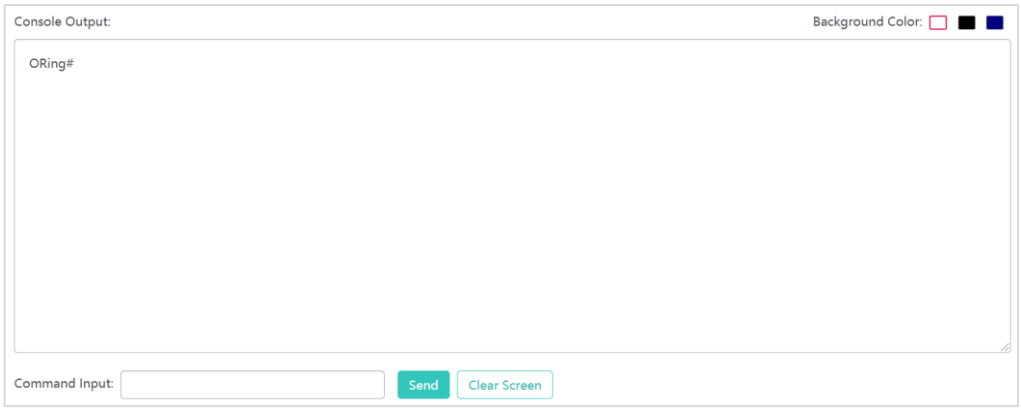
4.5.2.2 TELNET

Enable or disable the Telnet and SSH service, and setup the new password.



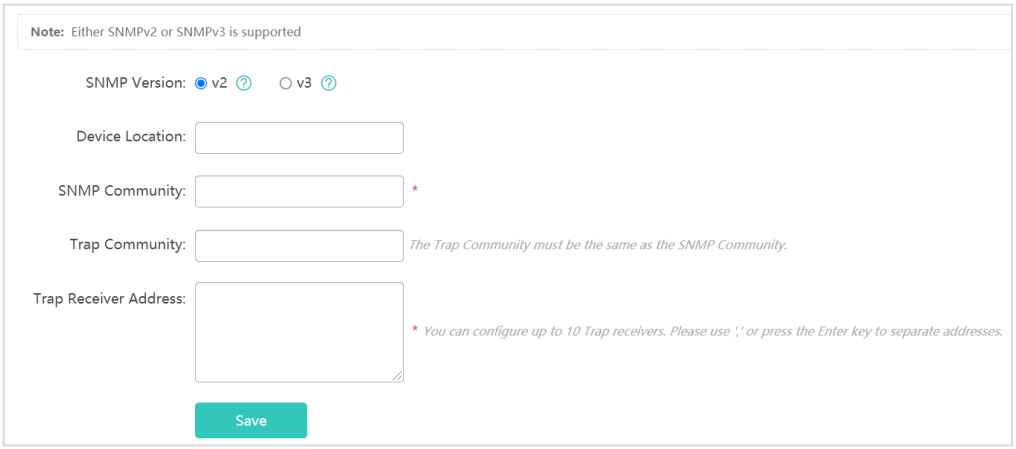
4.5.2.3 WEB CLI

Extensible web-based command line interface.



4.5.2.4 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. IGAP-W99110GP+ supports SNMP v2 and v3.



The SNMP Community cannot be set to “public” in the webUI, if you need to configure the community as public, please set commands in CLI.

Appendix

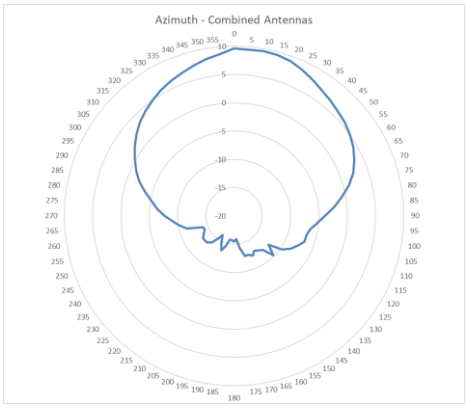
5.1 Product Specification

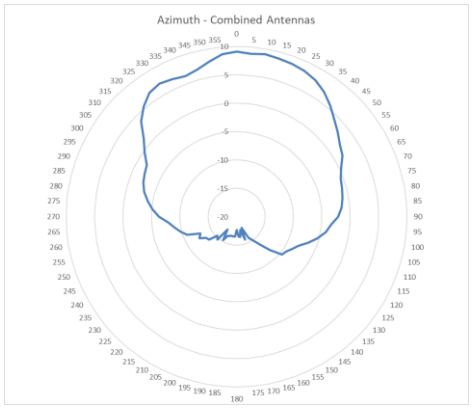
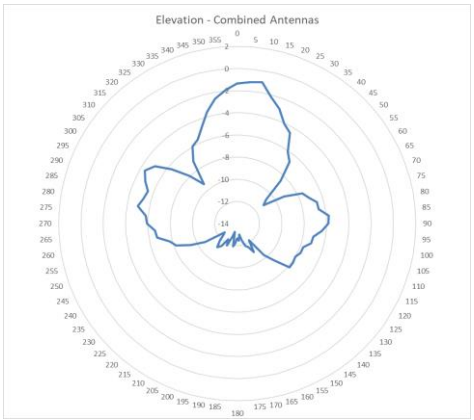
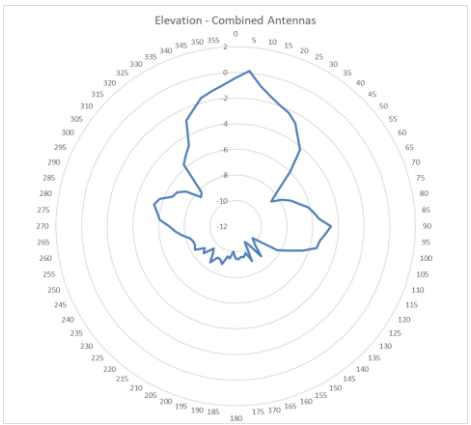
Model Name	IGAP-W99110GP+
Physical Ports	
10/100/1000Base-T(X) Ports in RJ45	1
Gigabit SFP	1
Console	1
Reset	Reset AP/Factory default by press time
WLAN interface	
Operating Mode	AP/Client
Antenna	Build-in 9dBi Directional Antenna, 60° total
Spatial Streams	4 spatial streams, MU-MIMO
WIFI Standard	IEEE802.11a: OFDM IEEE802.11b: CCK/DQPSK/DBPSK IEEE802.11g: OFDM IEEE802.11n: BPSK, QPSK, 16-QAM, 64-QAM IEEE802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM IEEE802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
Frequency Band	2.412~2.472 GHz 5.180~5.240 GHz, 5.745~5.825 GHz
Transmission Rate	Up to 0.575Gbps@2.4G Up to 1.2Gbps@5G Up to 2.4Gbps per AP 2.4G+5G is recommended with 1.775Gbps access rate
Transmit Power	28dBm (Note: The actual transmit power varies according to different countries and regions)
Receiver Sensitivity	802.11a : -71dBm ± 2dBm@54Mbps 802.11b : -85dBm ± 2dBm@11Mbps 802.11g : -71dBm ± 2dBm@54Mbps 802.11n : -83dBm ± 2dBm@MCS0 802.11ac HT20 :-83dBm ± 2dBm@MCS0 802.11ac HT40 :-79dBm ± 2dBm@MCS0 802.11ac HT80 :-76dBm ± 2dBm@MCS0 802.11ax HT80 :-76dBm ± 2dBm@MCS0
Encryption Security	WEP: (64-bit ,128-bit key) WPA/WPA2 PSK :TKIP and AES encryption (802.11i) 802.1X/RADIUS Authentication supported
Wireless Security	SSID broadcast disable and enable
LED Indicators	
System Indicator	Green Blinking:System booting Green Solid:Initialization in progres or proper operation. Orange Blinking:Initialization is complete Red Blinking:uplink port is disconnected.
RSSI	Green 1 Solid : <-70dBm, 2 Solid : -70 ~ -50dBm, 3 Solid : > -50dBm
Power	
Input Power	PoE (802.3af / 802.3at) or 44~57VDC power supply
Power Consumption (Typ.)	<12.95W
Surge Protection	Common mode +/-9kV

Physical Characteristic	
Enclosure	IP-68
Dimension (W x D x H)	251 x 168 × 64 mm (Excluding the bracket)
Weight	<1.5kg
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 65°C (-40 to 149°F)
Operating Humidity	0% to 100% Non-condensing
Regulatory Approvals	
EMC	EN55032, EN55035, EN301 489, GB9254
RF	EN300 328, EN301 893, SRRC
Safety	EN60950-1, GB4943
Warranty	3 years

5.2 Antenna Patterns

Horizontal planes (top view)





Vertical (elevation) planes (side view, AP facing down)