www.ip-com.com.cn

User Guide

5GHz Outdoor Point to point CPE

IP-COM

World Wide Wireless

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Conventions

If not specifically indicated, “the device”or “the AP” mentioned in this document stands for the Long Range Outdoor Point To Point CPE AP625.

Typographical conventions in this document:

Item	Presentation	Example
Menu	**Bold**	The menu "System Tool" will be simplified as **System Tool**.
Continuous Menus	>	Go to **System Tool** > **Diagnosis Tool**.

Symbols in this document:

Item	Meaning
Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
Tip	This format is used to highlight a procedure that will save time or resources.

How to download documents

Besides this document, other documents are updated on our website. To download them, please do as follows:

1. Go to our website http://www.ip-com.com.cn.
2. Search for the appropriate product model.
3. Download the correct documents.

Technical support

Tel: (86755) 2765 3089

Email: info@ip-com.com.cn

Website: http://www.ip-com.com.cn

Table of contents

1 Get to know the device

IP-COM AP625 is an advanced and high-performanced long-range wireless access point which is suitable for long-range data transmission and video surveillance, especially in WISP CPE solutions. It features with an external power amplifier and a built-in 16dBi directional antenna to provide an efficient way to pick up and maintains a stable signal for a wireless network connection range up to 10 kilometers. With waterproof cover and flexible mounting design, it applies to different harsh environments and provides reliable, secure and wide wireless coverage.

1.1 Features

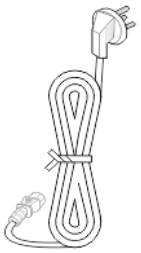
- Works at 5GHz band and the wireless rate is up to 433Mbps.
- Provide a 16dBi high power directional antenna and the transmission power is up to 400mW.
- Provide a LAN port and its transmission rate is up to 1000Mbps.
- Provide a DHCP server.
- Support WEP, WPA-PSK, WPA2-PSK, WPA-PSK&WPA2-PSK, WPA and WPA2 encryption methods.
- Support AP mode, Station mode, Universal Repeater mode, WISP mode and Router mode.
- Provide network diagnose tools, including signal scan, Ping, and traceroute.
- In router mode, the device supports extra functions, including MAC Clone, Traffic Control, Port Forwarding, MAC Filter, DDNS and Remote Web Access.
- Support IP64 dust and water proof level.

1.2 Package contents

Unpack the package. Your box should contain the following items:

Long Range Outdoor CPE * 1

Power Adapter * 1



Power Cord * 1

Ethernet Cable * 1

Plastic strap * 2

Grounding Screw * 1

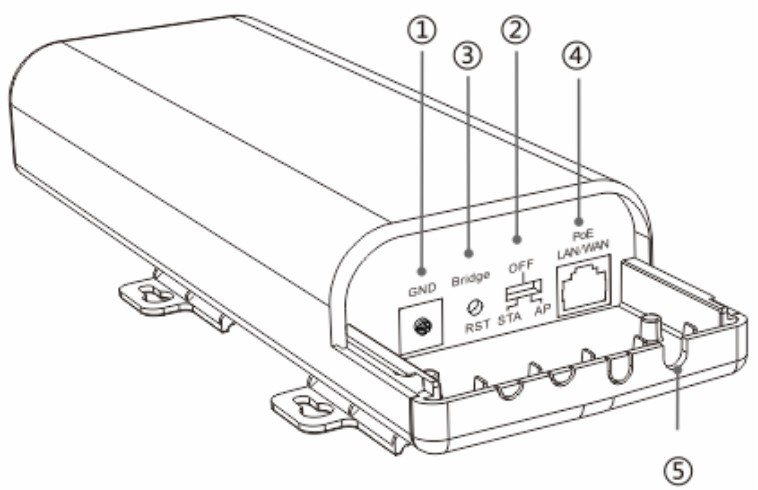
Install Guide * 1

GNU * 1

If any item is incorrect, missing, or damaged, please contact your dealer for immediate replacement.

1.3 Hardware descriptions

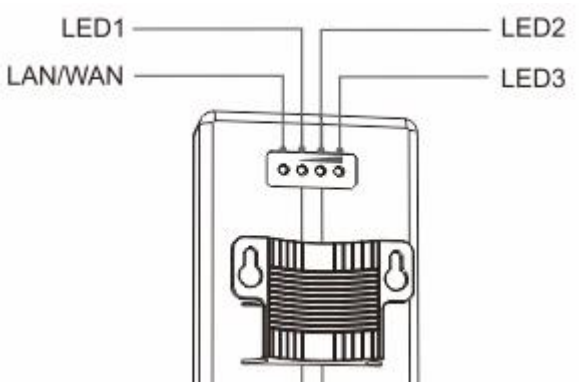
1.3.1 Front panel



Item	Port / Button	Description
①	GND	Used to protect the device from surge and lightning. To achieve that, please connect the GND port to the grounding bar of a building with a grounding cable and the included grounding screw.
②	OFF/STA/AP	Used to adjust operation mode of the device. • OFF: the default position. When it is on OFF position, you can change operation mode through web UI. • STA: When it is on STA position, the device only works at station mode and you can't change the operation mode through web UI. • AP: When it is on AP position, the device only works at AP mode and you can't change the operation mode through web UI.
③	Bridge/RST	Used to bridge two devices or reset the device. • To bridge two devices: 1. Press and hold this button for 3~7 seconds on an AP625 that works in AP mode. When you release the button, LED1/LED2/LED3 starts blinking. 2. Within two minutes, press and hold this button for 3~7 seconds on another AP625 that works in Station mode. When you release the button, LED1/LED2/LED3 starts blinking and the two devices start to bridge. LED1/LED2/LED3 of the two devices will light off and when they light and keep solid, it indicates that the two deivces bridge successfully. • To reset the device: Press and hold this button for over 15 seconds to restore the device to factory default.

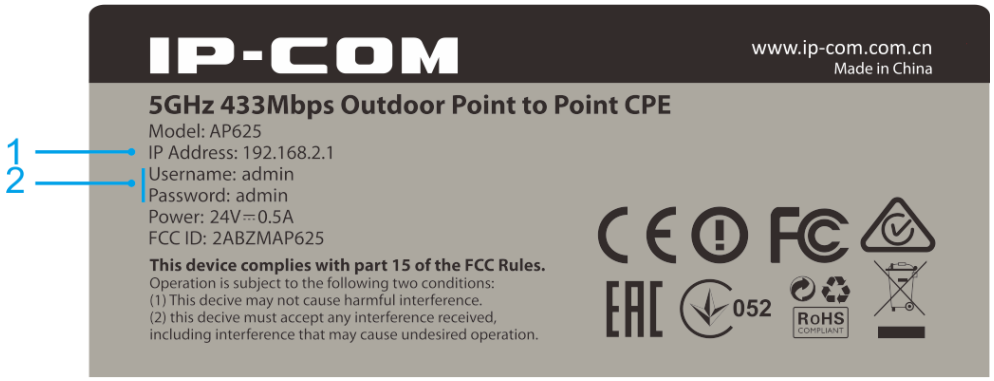
Item	Port / Button	Description
④	PoE LAN/WAN	• This port can connect to a PoE power adapter to provide power for the device and can transmit data. • It works interchangeably as a WAN port in router mode and a LAN port in other modes.
⑤	Ethernet slot	It is used for an Ethernet cable to get through so that the device cover can be firmly fixed.

1.3.2 Rear panel



LED	Status	Description
LAN/WAN (PoE LAN/WAN)	Off	The device is powered off.
	Solid	The device is powered on and is not transmitting data.
	Blinking	The device is powered on and is transmitting data.
LED1, LED2,LED3 (Signal Threshhold LED)	Off	The device does not bridge to another device.
	Blinking	The bridging between two devices is in progress.
	Solid	When two devices bridge successfully, LED1/LED2/LED3 keeps solid. The three LEDs indicate the signal strength of the other bridged device. By default, the relations between the signal strength and LEDs are shown below, and you can modify each LED's threshold on the web UI. • -90 dBm < signal strength < -80dBm: LED1 turns green. • -80 dBm < signal strength < -70dBm: LED1 and LED2 turn green. • -70 dBm < signal strength: All the three LEDs turn green.

1.3.3 Label



1 IP Address:

When the device is in factory state, this IP address is used to log in to the device's web UI.

2 Username and Password:

When the device is in factory state, both the login username and password are *admin*.

2 Device installation

2.1 Installation preparations

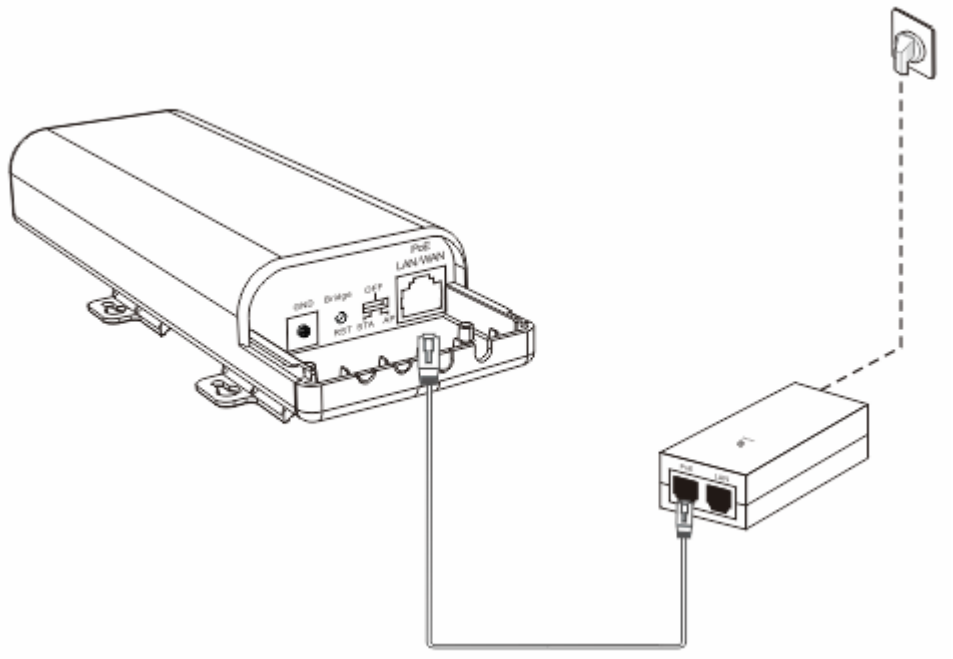
2.1.1 Environment requirements

Item	Requirement
Temperature	-30℃ ~ 55℃
Humidity	10%~90%RH (non-condensing)

2.1.2 Check your device

To check whether the device works normally or not, please do as follows:

1. Connect the device to the PoE port of the power adapter with the included Ethernet cable.
2. Plug the power adapter to a power outlet with the included power cord.



If the device works normally, when the device is powered on, the LED status should be solid or blinking.

LED	Status	Description
LAN/WAN (PoE LAN/WAN)	solid	The device is not transmitting data.
	blinking	The device is transmitting data.

2.2 Installation steps

Step 1: Install the device

1. Choose a location to install the device.

   We recommend that you install the device on a roof with a pole, or some locations like that.

2. Connect the cable to the AP.

   1) Slide the bottom cover off.

   2) Connect one end of an Ethernet cable to the PoE LAN/WAN port of the device.

      The Ethernet cable should be a cat 5 Ethernet cable (or higher).

   3) Connect one end of a grounding cable to the GND port and fix the grounding screw.

   4) Gently replace the cover by sliding it up into the place.

   5) Connect the other end of the grounding cable to the grounding bar of a building.

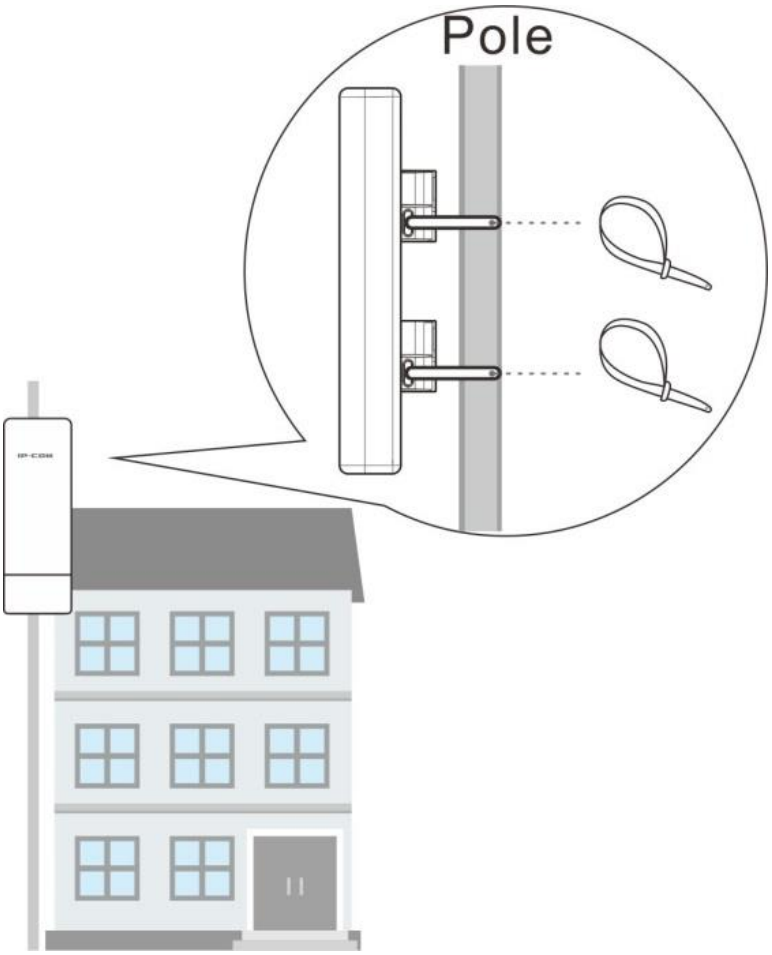
3. Mount the AP.

   1) Place the back panel of the device to a pole.

   2) Thread plastic straps through the grooves underneath the brackets.

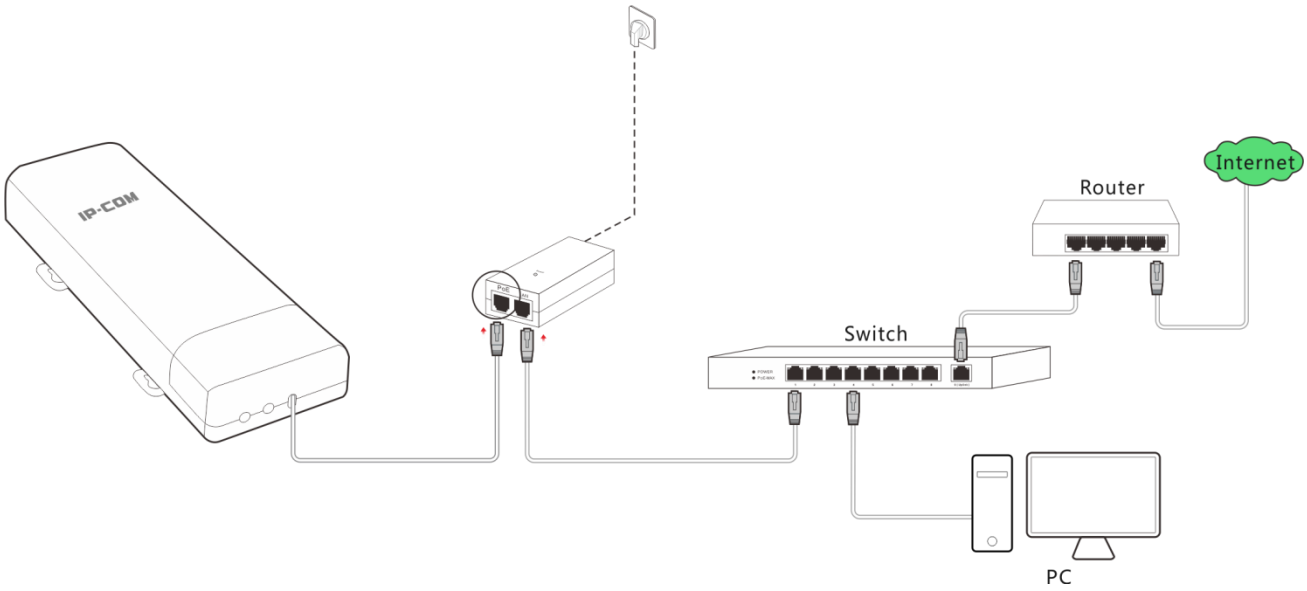
   3) Adjust the AP to get the best data transmission speed.

   4) Attach the AP to the pole firmly by pulling the plastic straps.



Step 2: Connect the device to a network

1. Connect the other end of the Ethernet cable to the PoE port of the power adapter.
2. Connect a computer, a switch or a router to the LAN port of the power adapter using an Ethernet cable.
3. Connect the power adapter to a power outlet using the power cord.



3 Web UI login

3.1 Login

When using the device for the first time, you can log in to its web UI via a browser with default login information. The default login information includes:

Item	Default Setting
IP Address	192.168.2.1
Username and Password	admin

To log in to this device:

(Assume that the AP is in factory default state and ensure that your PC is connected to the device.)

1. Set your PC's IP address to 192.168.2.X (2~254).

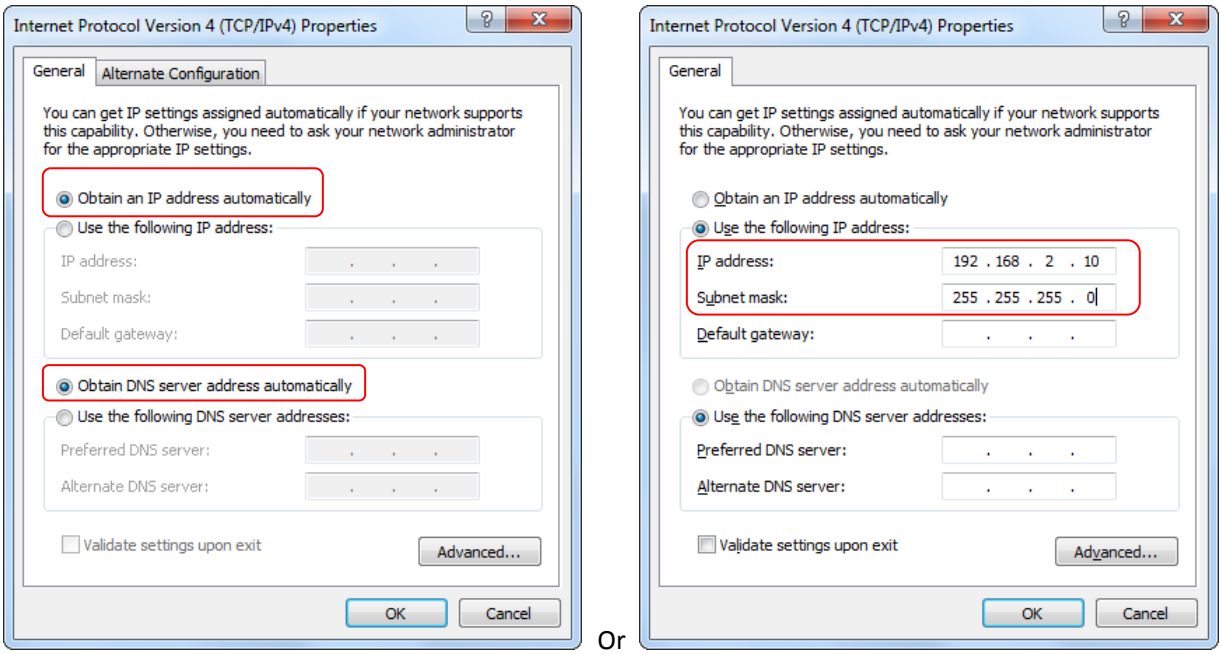
   >> Method 1: Set your PC to **Obtain an IP address automatically**.

   >> Method 2: Manually set your PC to 192.168.2.X (2~254), with a subnet mask of 255.255.255.0. (If the switch and AP are in the same IP segment, make sure that the switch, AP and PC have different IP addresses).

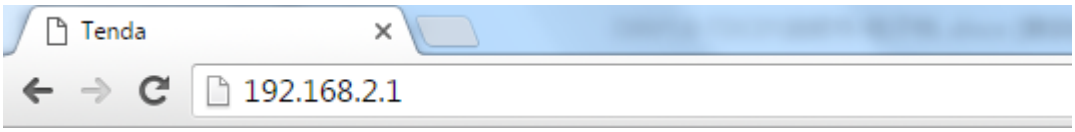
   For detailed steps, see Appendix Configure your computer.

   Tip

   The AP's DHCP server is enabled by default. Once you finished settings on **Quick Setup** page, the DHCP server will be disabled automatically.

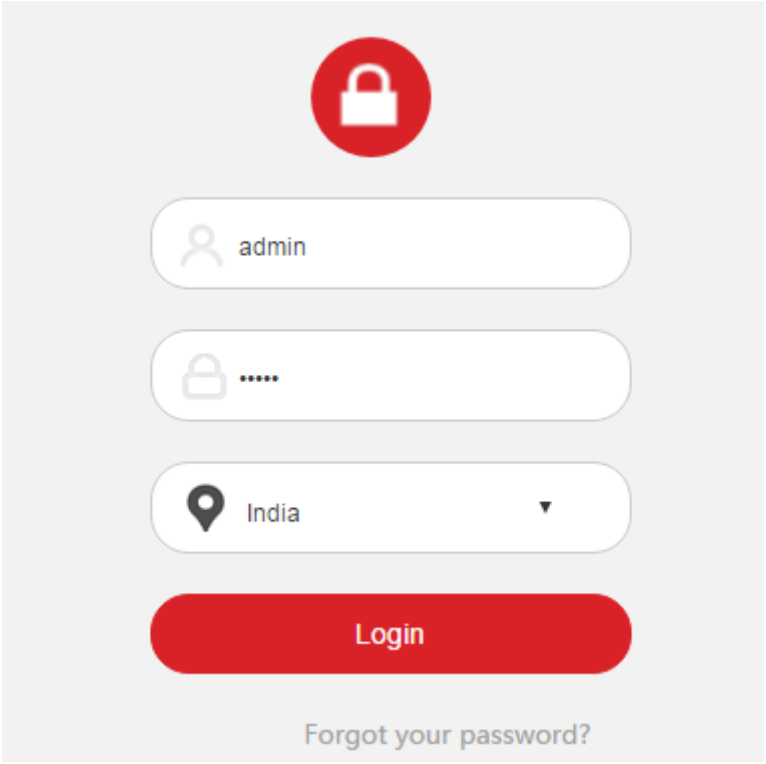


2. Launch a browser, such as Chrome , enter the AP's default IP address **192.168.2.1** in the address bar, and press **Enter**.

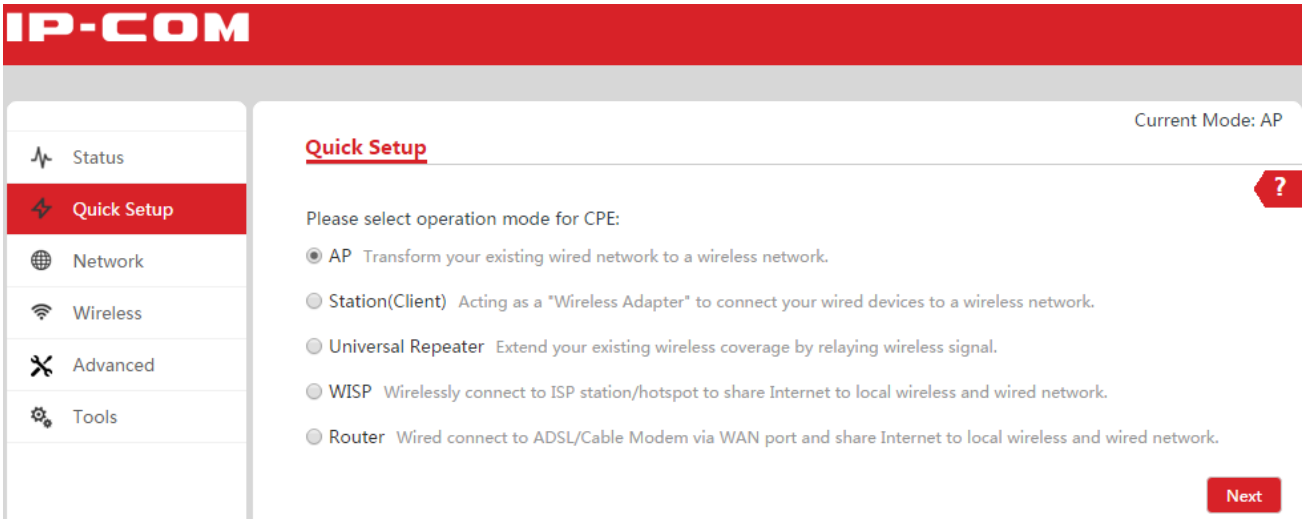


3. In the login page, enter **admin** (case sensitive) in both "Username" and "Password" box.

4. Click the dropdown list, select your country and click **Login**.

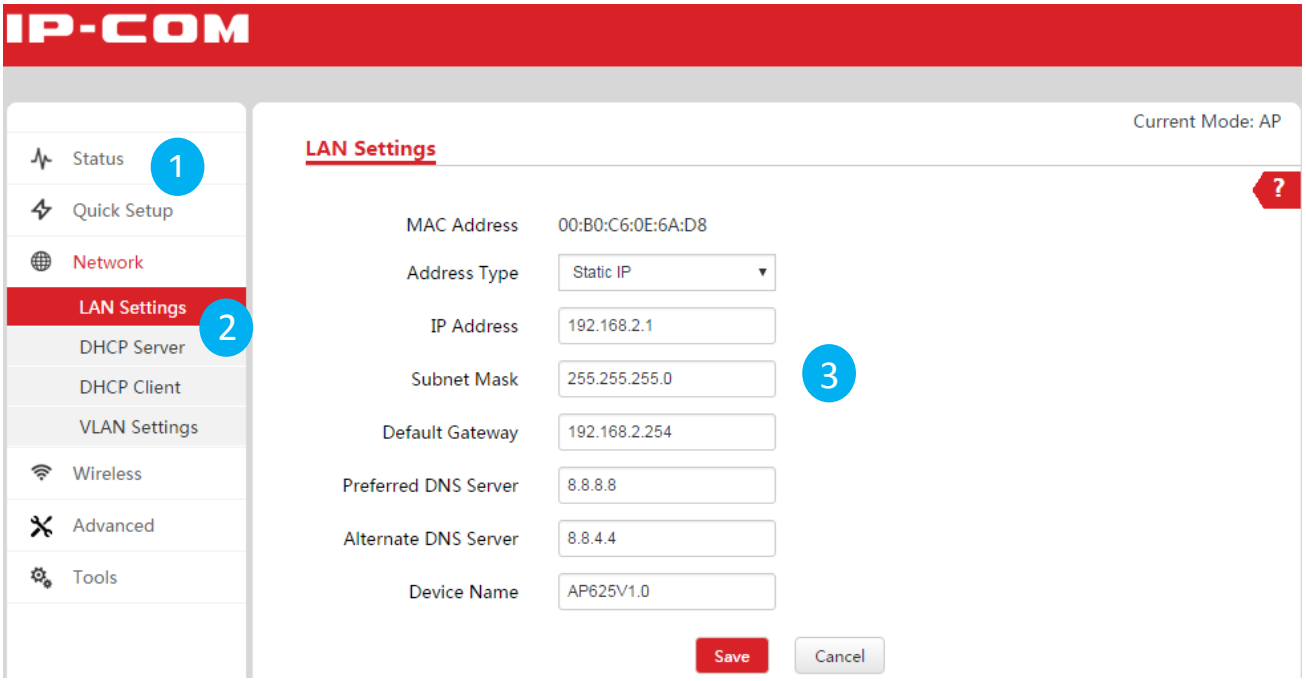


Then you come to the management page and can begin to configure the device.



3.2 Layout of web UI

This web UI is divided into three parts: primary navigation bar, secondary navigation bar and configuration area, described as follows.



Item	Name	Description
1	Primary Navigation bar	The navigation bar organizes the device's menu of all functions in the form of a navigation tree. You can choose the function menu from the navigation bar with selection result shown in the configuration area.
2	Secondary Navigation bar	
3	Configuration area	The area is used to configure and view settings.

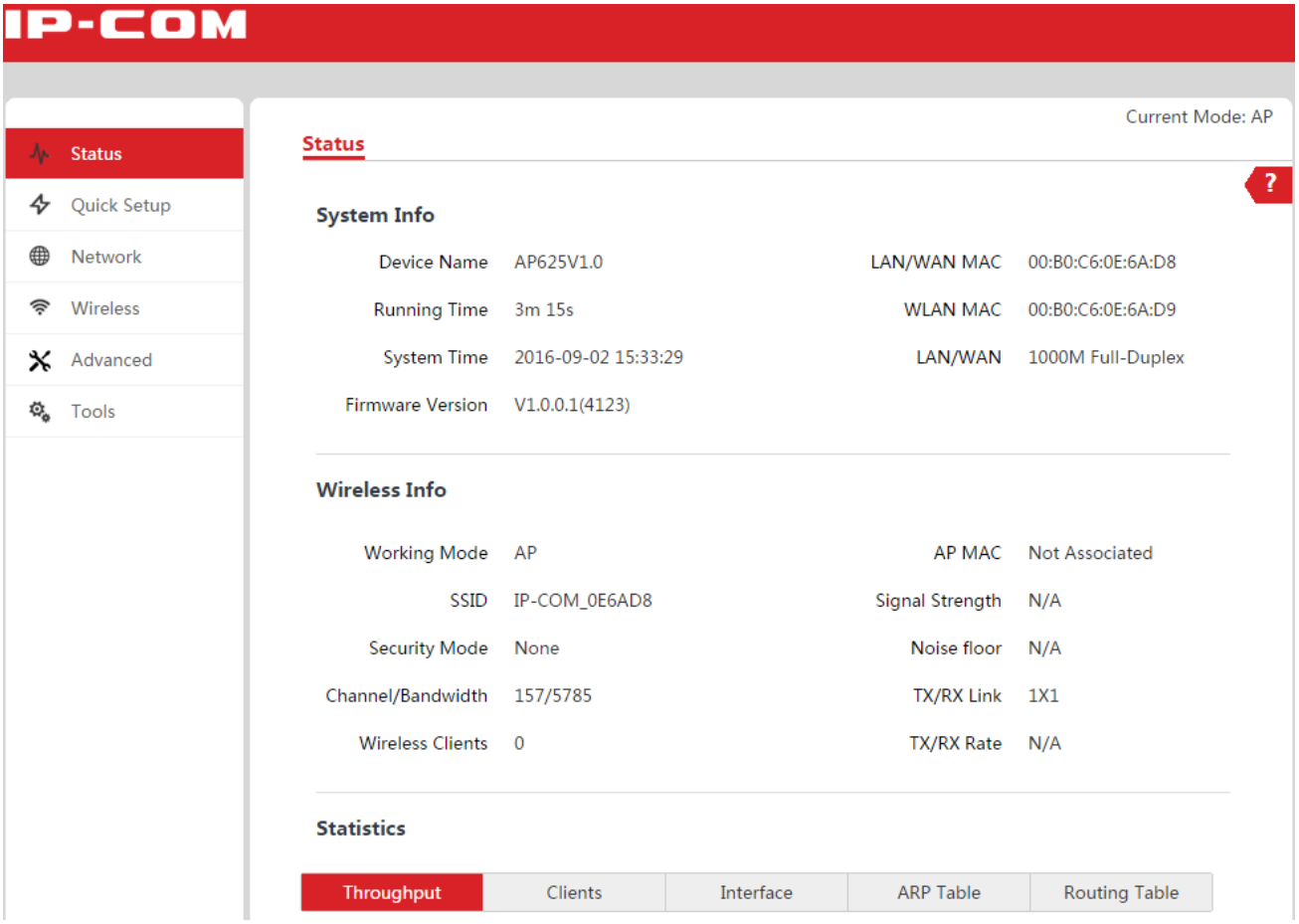
The following table shows the commonly used buttons of the web UI.

Item	Description
?	Click the button to view the help info if you meet any problems during the setup.
Save	Click the button to apply your settings.
Cancel	Click the button to clear the settings you are editing.

4 Web UI functions

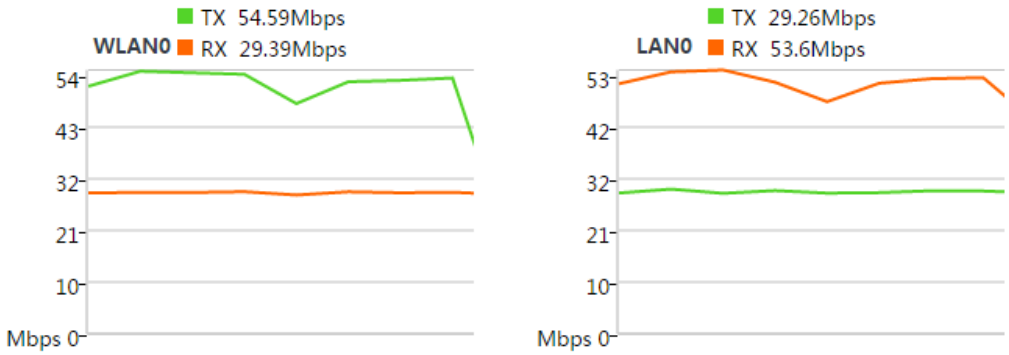
4.1 Status

This page displays system info, wireless info, and related statistics information of the device. Click **Status** to enter the setup page, and pull the scroll bar to view more information.



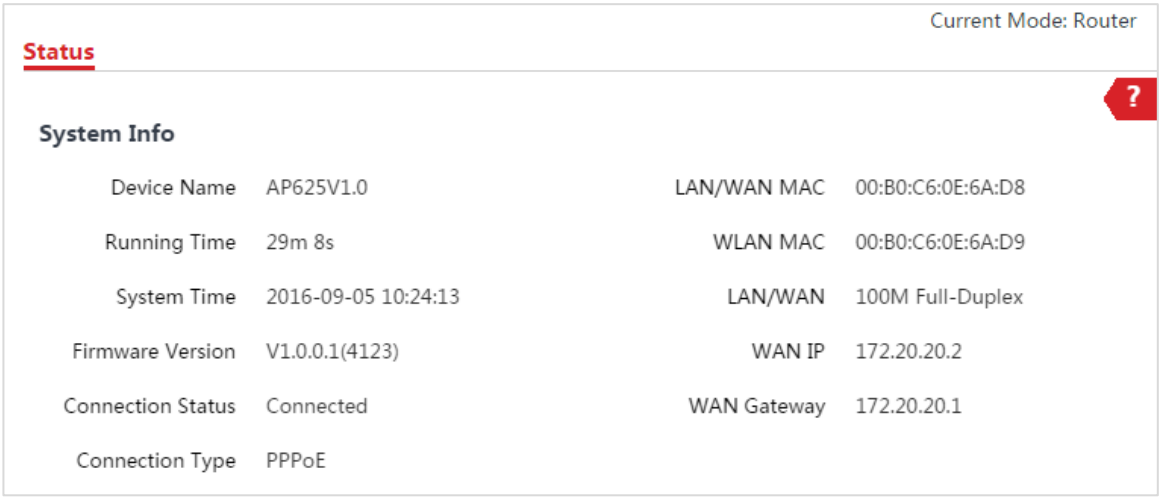
Parameter Description (part of): (You can also click ? on the upper right page to get help.)

Parameter	Description
System Info	**Running time:** The duration of time that the device has been running from last reboot. It will be reset when the device reboots.
	System Time: The device's current system time. To ensure that time-related functions work properly, go to **Tools** > **Date & Time** to set up an appropriate system time.
	LAN/WAN MAC: MAC address of *PoE LAN/WAN* port. In router mode, it is WAN MAC address and in other modes, it is LAN MAC address. If you set up MAC Clone function in router mode, you can check on this page whether it is successful.
	WLAN MAC: MAC address of the wireless interface of the device.
	LAN/WAN: Indicates the connection status of *PoE LAN/WAN* port.This can indicate that a cable is not plugged into a device, there is no active Ethernet connection, or the current rate of *PoE*

	LAN/WAN port. (In router mode, *PoE LAN/WAN* port works as a WAN port. In other modes, it works as LAN port.)
Wireless Info	**Working mode:** Current operation mode of the device. For the working modes supported by the device, please see Operation mode description.
	SSID: Current wireless network name of the device.
	Security Mode: Current wireless encryption mode of the device. For detailed encryption information, please see Encryption method description.
	Channel/Bandwidth: Current working channel and bandwidth of the device.
	Wireless Clients: Number of wireless clients currently connected to SSID of the device.
	AP MAC: Wireless MAC address of this device or a remote AP. • In AP mode and router mode, it is the wireless MAC address of this device. • In other modes, if this device is connected to another AP wirelessly, AP MAC address is the wireless MAC address of that remote AP.
	Signal strength: Wireless signal strength of the connected device. • If this device is connected to another AP wirelessly, it is the wireless signal strength of that remote AP. • In AP mode and router mode, it is the wireless signal strength of the wireless client that is first connected to this device.
	Noise Floor: Background noise of the current environment. The greater the absolute value, the less the interference.
	TX/RX link: The number of independent spatial data streams that the device is transmitting (TX) and receiving (RX). This device is Single-Input Single-Output.
	TX/RX rate: (Available in Station/Universal Repeater/WISP mode.) Displays the current 802.11 data transmission (TX) and data reception (RX) rates.
Statistics	**Throughput:** The current data traffic on wireless interface and LAN port in both graphical and numerical form.The chart scale and throughput dimension (Bps, Kbps, Mbps) change dynamically depending on the mean throughput value.The statistics are updated automatically.  **Clients:** Available in AP mode and router mode. • IP address: IP address of a wireless client.

	• MAC address: MAC address of a wireless client. • Signal/Noise: Wireless signal strength from the device to a client and noise floor of the current environment. • TX/RX Rate: Current TX/RX rate of a client. • CCQ: Link quality of the clients. The higher the percentage, the better the network transmission quality. • Connection time: Duration of a client that is connected to the SSID of the device.
Statistics	**Upper AP:** Available in Station/Universal Repeater/WISP mode. • IP address: IP address of the upper AP. • MAC address: MAC address of the upper AP. • Signal/Noise: Wireless signal strength from this device to the upper AP and noise floor of the current environment. • TX/RX Rate: Current TX/RX rate of this device. • CCQ: Link quality of this device to the upper AP. The higher the percentage, the better the network transmission quality. • Connection time: Duration that this device is connected to the upper AP.
	Interface: The information of LAN port and bridge interface, including IP address, MAC address, RX packets, RX errors, TX packets and TX errors.
	ARP table: Current ARP table of the device. • IP address: IP address of a host in the ARP table. • MAC address: MAC address that corresponds to the IP address of a host. • Interface: Interface that is used to communicate with a host.
	Routing table: Target network the device can reach currently. • Destination Segment: IP address or IP network of the destination. • Subnet Mask: Subnet mask of the destination. • Next hop: Next hop is where the packets are forwarded to first. • Interface: Interface is where the packets are forwarded from this device.

When the device works in router mode, the system info is displayed as follows:



Parameter Description (part of): (You can also click ? on the upper right page to get help.)

Parameter	Description
System Info	**WAN IP:** WAN IP address obtained from the upper DHCP server. When the device works in router mode, the *PoE LAN/WAN* port works as WAN port.
	WAN Gateway: Gateway address of the device. When the device accesses to an external network, its data packets are forwarded by this gateway.
	Connection Status: Current network connection status of the device.
	Connection Type: Current connection type of the device. The device supports three connection types, as follows: • DHCP: WAN port of the device obtains an IP address from the upper DHCP server. • Static IP: WAN port is connected through fixed IP address, subnet mask, default gateway, and DNS server information. • PPPoE: WAN port is dialed up through user name and password.

4.2 Quick setup

This device supports the following operation modes and the default operation mode is **AP** mode.

- AP Mode
- Station (Client) Mode
- Universal Repeater Mode
- WISP Mode
- Router Mode

Operation mode description:

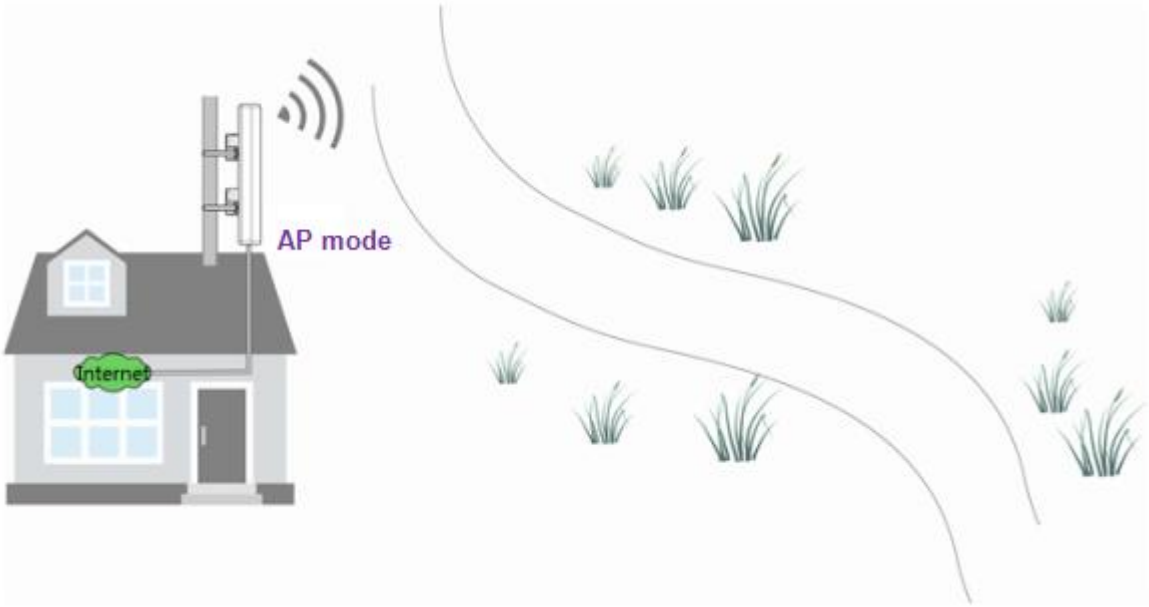
Work Mode	Description
AP	In this mode, the PoE LAN/WAN port works as a LAN port and is connected to a network, such as the internet, so that all clients can wirelessly connect to the device to access the network.
Station(Client)	In this mode, the device works as a wireless client to connect to a remote device, such as an AP, to extend the remote wireless network. On the other hand, the device's clients can only connect to the device through an Ethernet cable, for example, you can connect a switch to the device, and connect the clients to the switch. As a result, the device's wired clients can access the remote device's network.
Universal Repeater	In this mode, the device can wirelessly connect to a remote device, such as an AP, to extend the remote wireless network, and can be connected by its clients wirelessly so that the device's wireless clients can access the remote network. After the device connects to the remote device successfully, this device's SSID and WiFi password are changed to those of the remote device.
WISP	Usually, in this mode, the device wirelessly connects to a hotspot of an ISP, and of course it can connect to a wireless router. The connected wireless WAN interface obtains IP info from the hotspot or wireless router by DHCP, Static IP, or PPPoE mothod. As a result, the device's wired and wireless clients can access the hotspot or wireless router's network. **Note:** As a device's LAN and WAN IP segment cannot be the same, please make sure this device's LAN IP segment is different from that of the hotspot or wireless router's LAN IP segment. For example, if the wireless router's LAN IP segment is 192.168.2.X, please change this device's LAN IP segment to another one, such as 192.168.6.X.
Router	In this mode, the PoE LAN/WAN port works as a WAN port and is connected to an uplink router using an Ethernet cable. The WAN port obtains IP info from the router by DHCP, Static IP or PPPoE method. As a result, the device's wired and wireless clients can access the uplink router's network.

4.2.1 AP mode

In this mode, the PoE LAN/WAN port works as a LAN port and is connected to a network, such as the internet, so that all clients can wirelessly connect to the device to access the network.

Application scenario

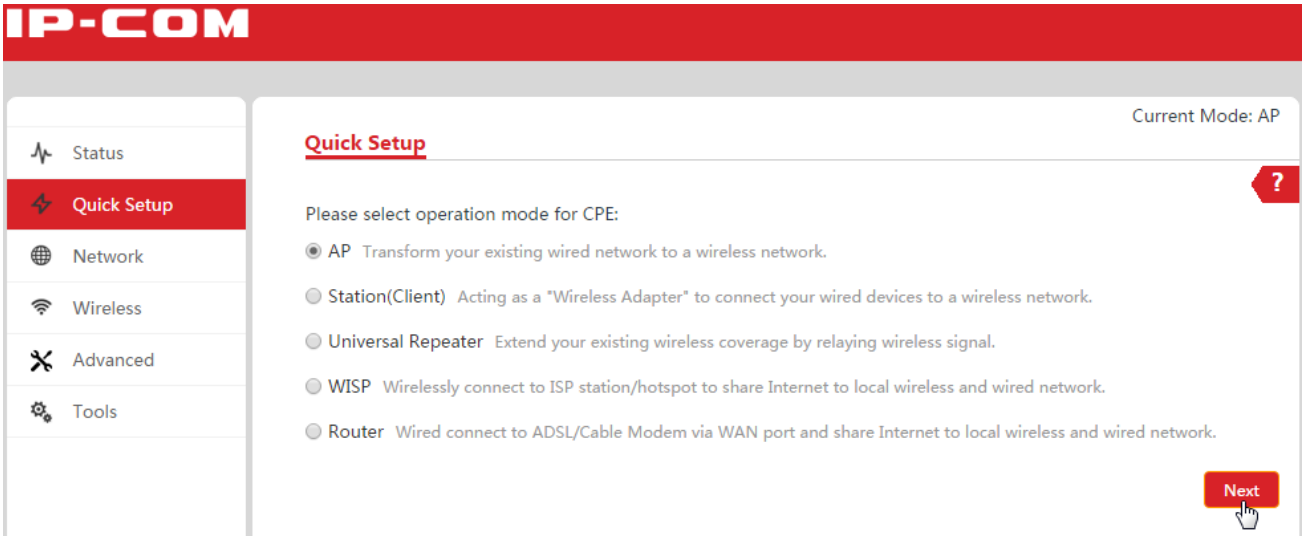
In the following application, the device connects to the internet using an Ethernet cable and transmits wireless signals so that wireless clients can connect to the device.



Configure AP mode

To configure AP mode:

1. Log in to the device's web UI.
2. Go to **Quick Setup**, select **AP** and click **Next**.



3. Set AP's basic wireless info.

   - SSID: Set up a wireless network name, such as *Local_WiFi*.

     This name is used for wireless clients to connect to the device so that they can access the internet.

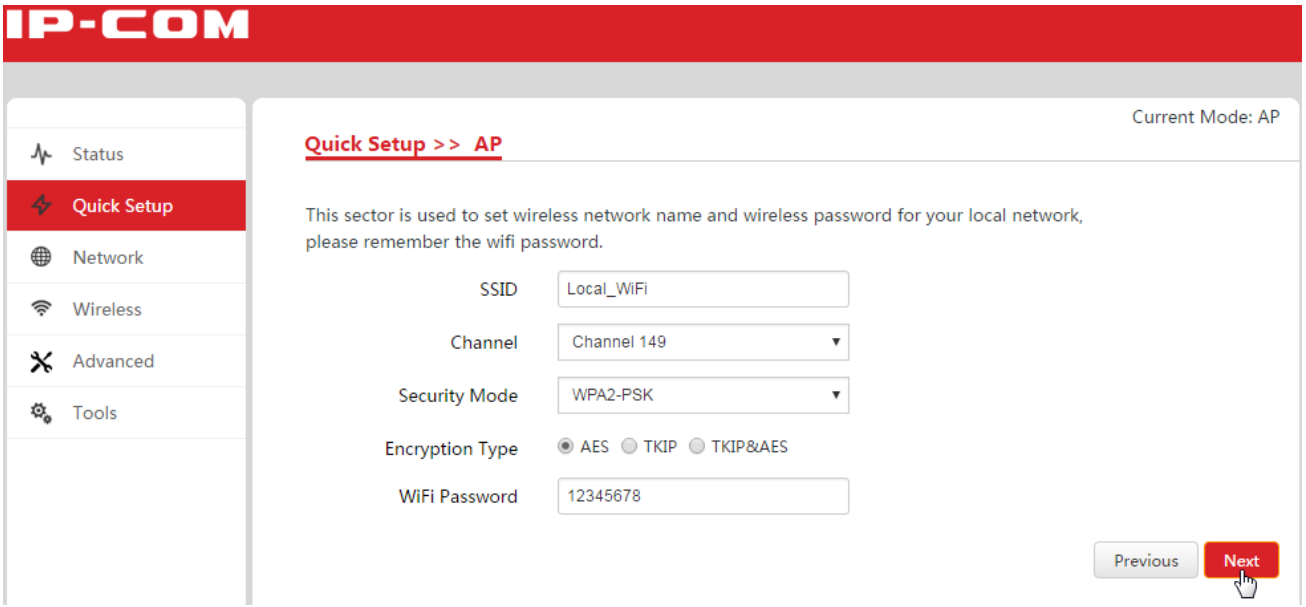
   - Channel: Select a wireless channel.

     We recommend that you select a channel that is less used in surrounding area. You can go to **Advanced > Diagnose** and select **Site Survey** to check each channel's usage.

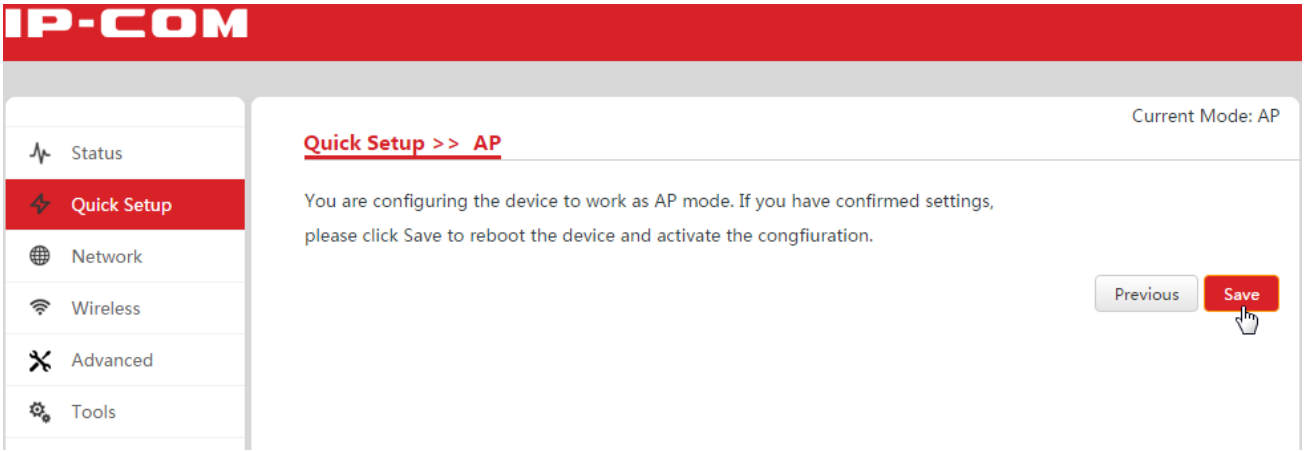
   - Security Mode, Encryption Type: We recommend that you select *WPA2-PSK, AES*.

   - WiFi Password： Set up your WiFi password, such as *12345678*.

   - Click **Next**.



4. Click **Save**. After the device reboots, the configurations takes effect.

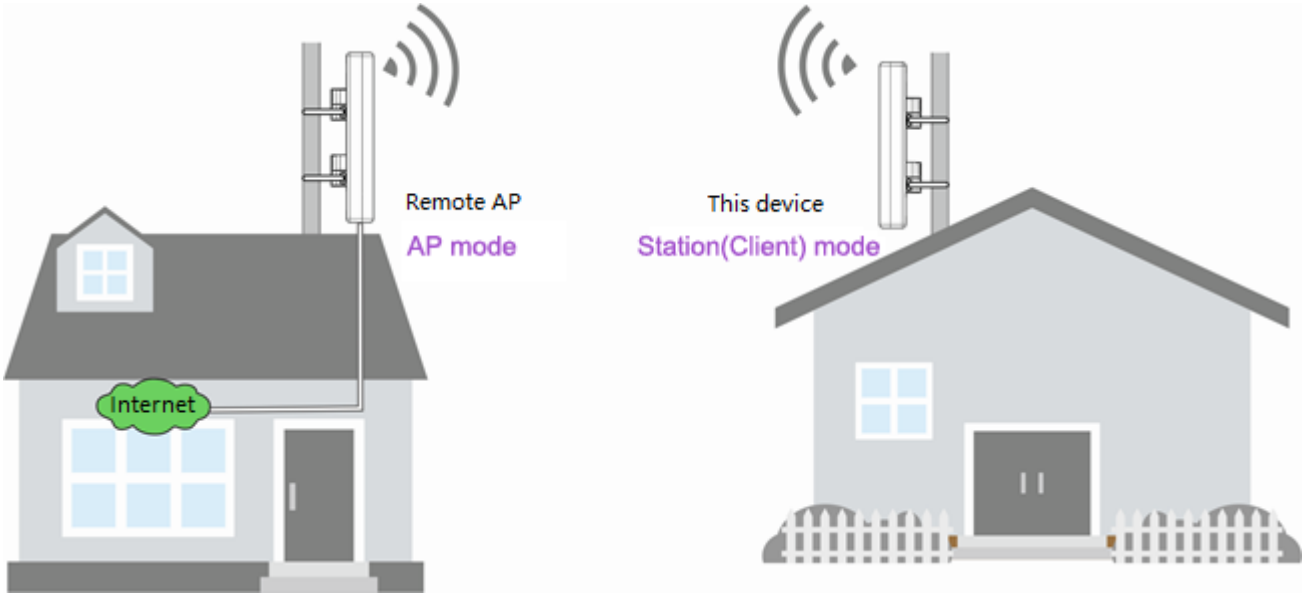


4.2.2 Station (Client) mode

In this mode, the device works as a wireless client to connect to a remote device, such as an AP, to extend the remote wireless network. On the other hand, the device's clients can only connect to the device through an Ethernet cable, for example, you can connect a switch to the device, and connect the clients to the switch. As a result, the device's wired clients can access the remote device's network.

Application scenario

In the following application, this device is a bit far away from the remote AP that connects to the internet. To help this device's clients to access the internet, this device works in station mode and wirelessly connects to the remote AP.



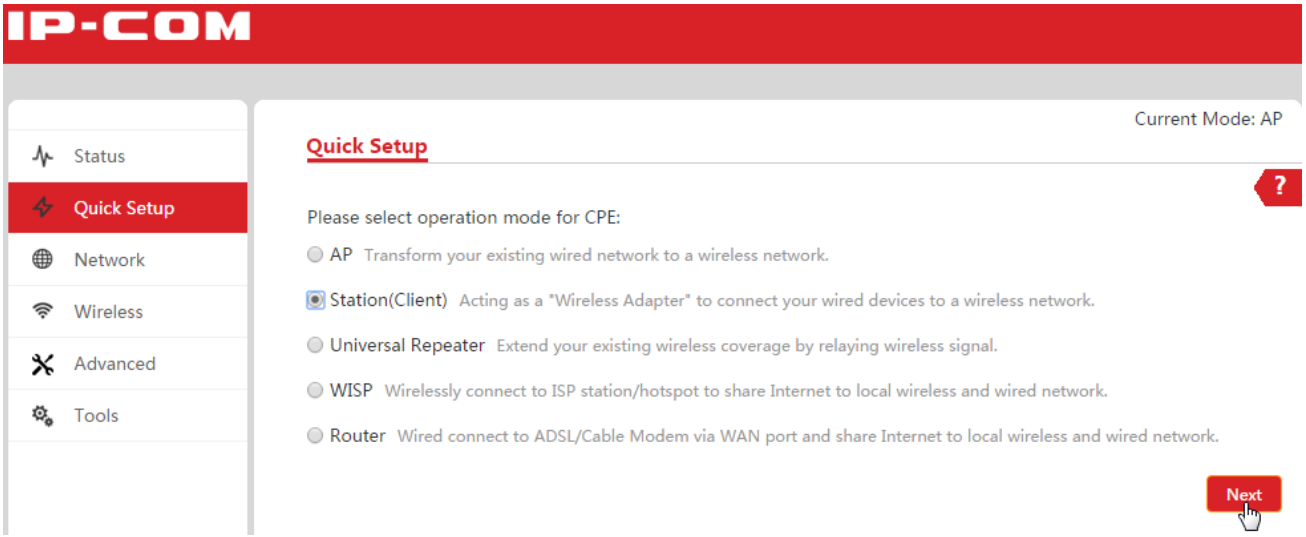
Assume that the remote AP's info is as follows:

IP Address	192.168.0.2
SSID	IP-COM_0020A0
WiFi Password	87654321

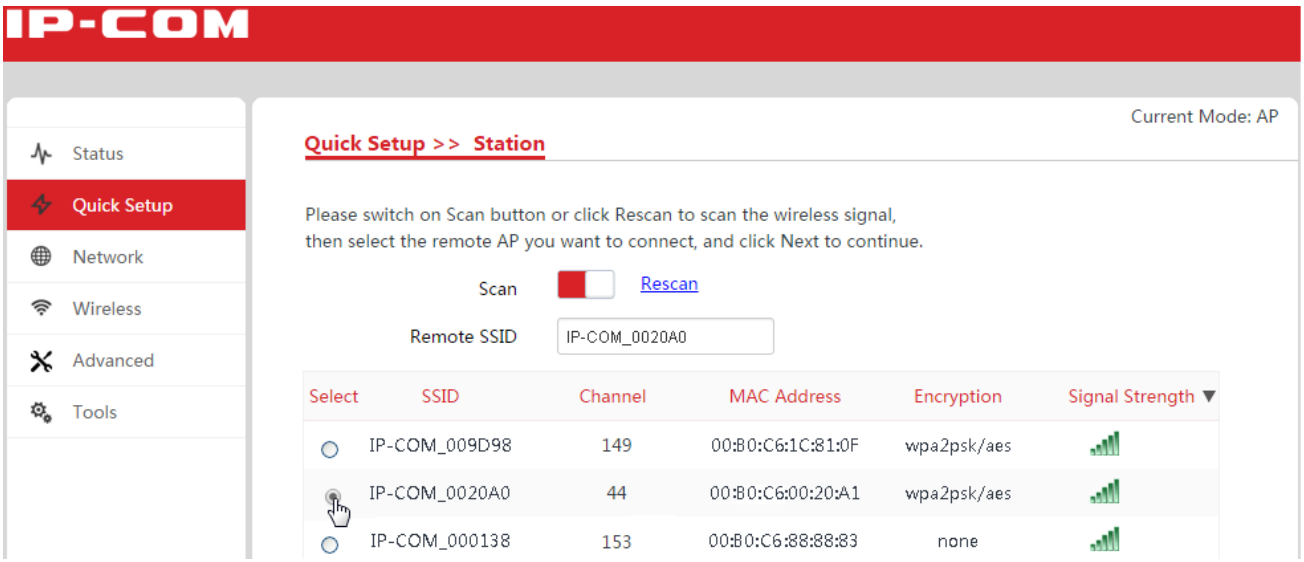
Configure station mode

To configure station mode:

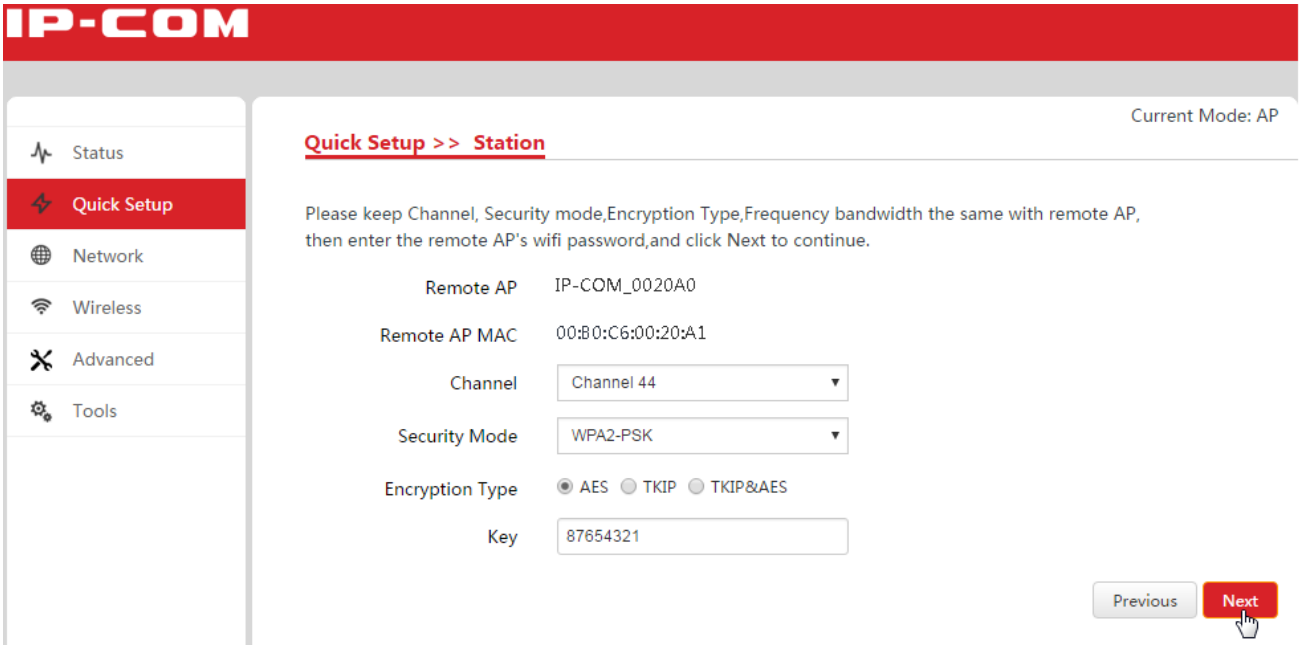
1. Log in to the device's web UI.
2. Go to **Quick Setup**, select **Station (Client)** and click **Next**.



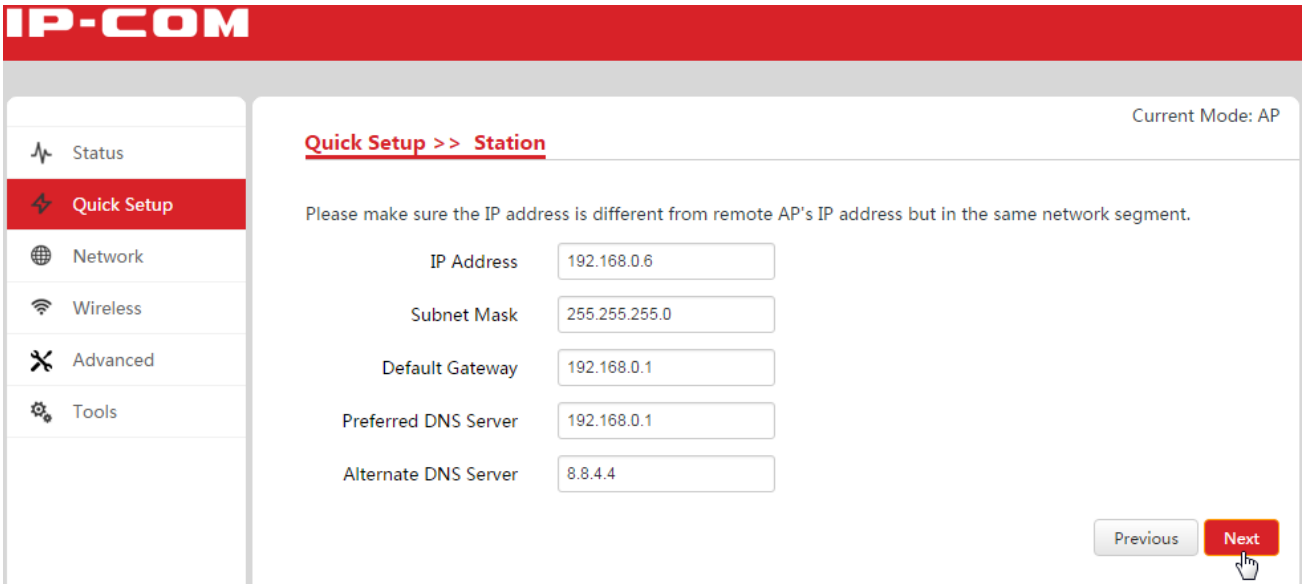
3. In the scanned wireless signal list, select the remote AP's wireless network name (SSID), here we select IP-COM_0020A0, and click **Next**.



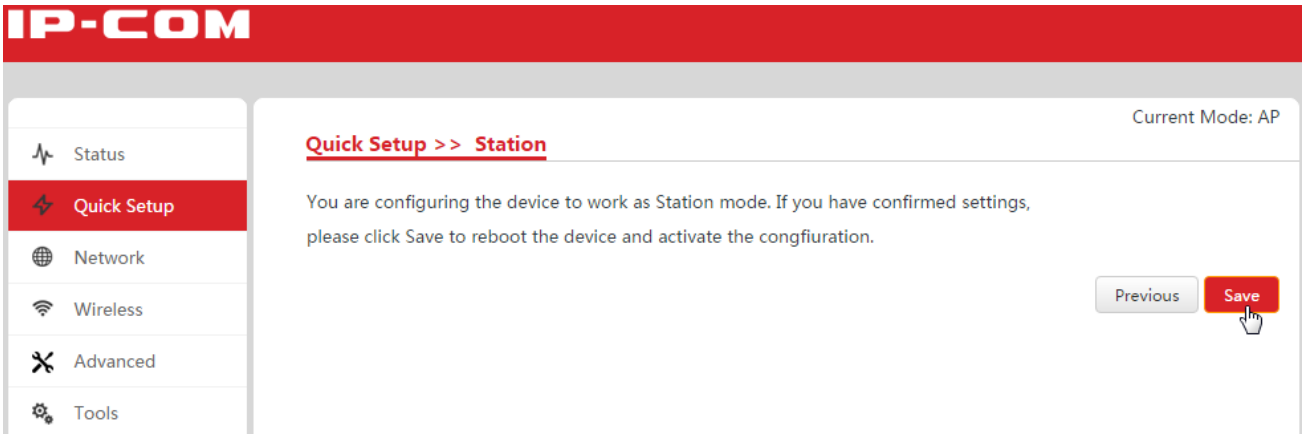
4. Enter the remote AP's WiFi password (Key), here we enter *87654321*, click **Next**.



5. Set up IP info of this device.
   - IP address: Modify this device's IP address to a different one but on the same IP segment from that of the remote AP. As the remote AP's IP address is *192.168.0.2*, we can enter *192.168.0.6* here.
   - Subnet Mask： Set up a subnet mask.
   - Default Gateway: Enter the default gateway address. We recommend that you be set to the LAN IP address of the router that is connected to the internet.
   - Preferred DNS Server: Enter DNS info.
   - Click **Next**.



6. Click **Save**. After the device reboots, the configuration takes effect.

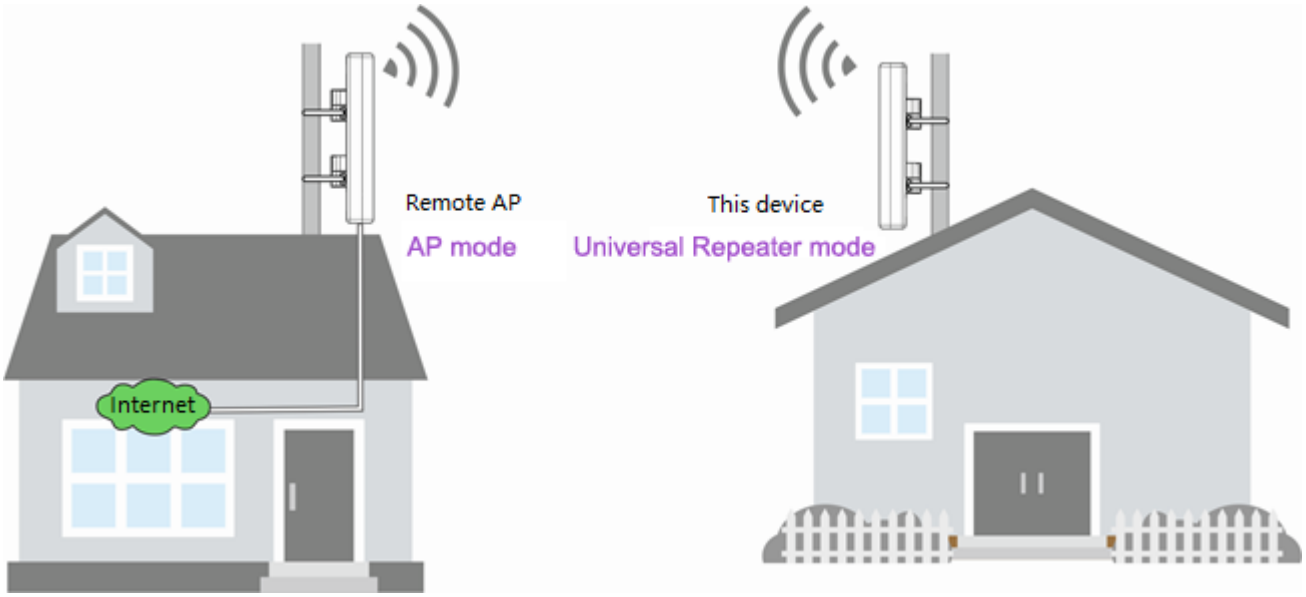


4.2.3 Universal Repeater mode

In this mode, the device can wirelessly connect to a remote device, such as an AP, to extend the remote wireless network, and can be connected by its clients wirelessly so that the device's wireless clients can access the remote network. After the device connects to the remote device successfully, this device's SSID and WiFi password are changed to those of the remote device.

Application scenario

If you want to extend your wireless coverage by point-to-point bridging to existing wireless network, you can configure your device to work in universal repeater mode, as follows.



Assume that the remote AP's info is as follows:

IP address	192.168.0.2
SSID	IP-COM_0020A0
WiFi Password	87654321

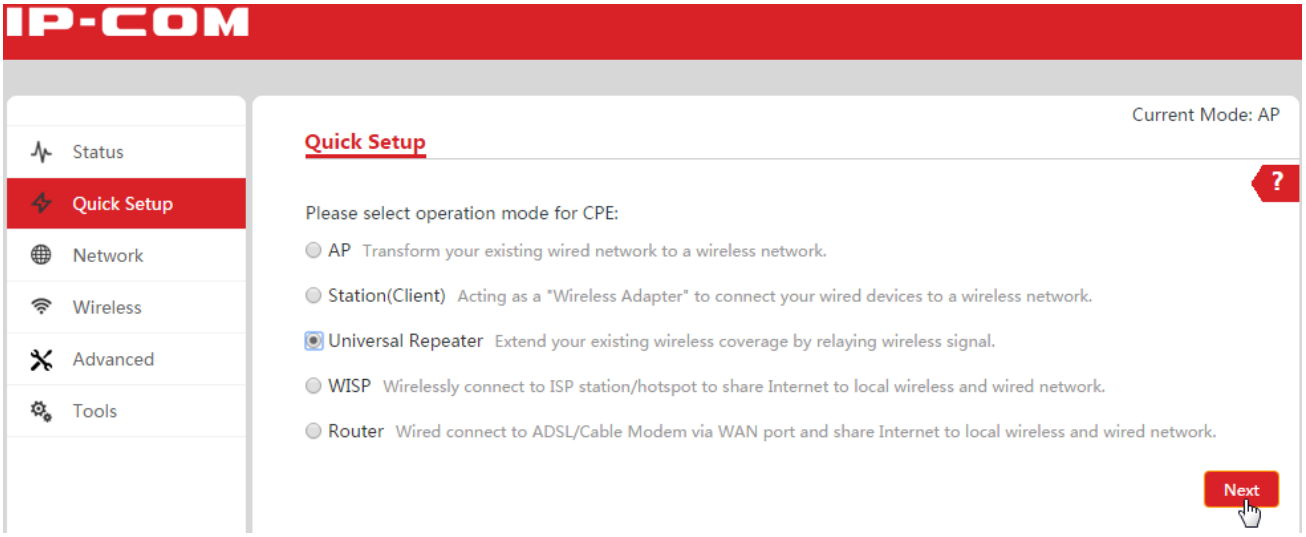
Configure universal repeater mode

Tip

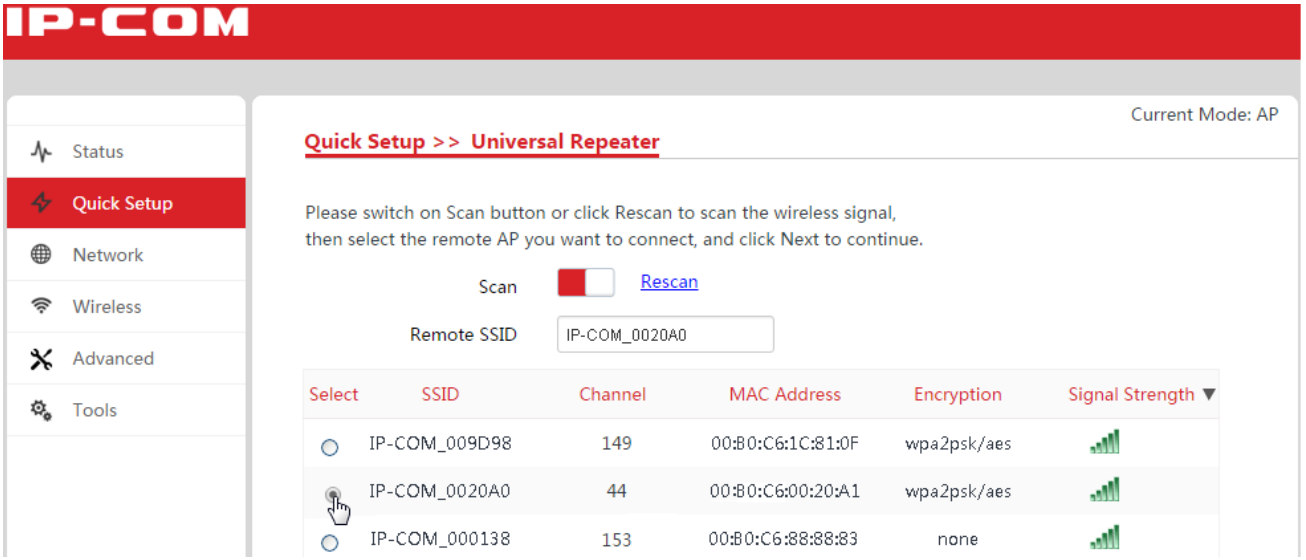
After you finish configuring universal repeater mode, this device's SSID and WiFi password are changed to those of the remote AP.

To configure universal repeater mode:

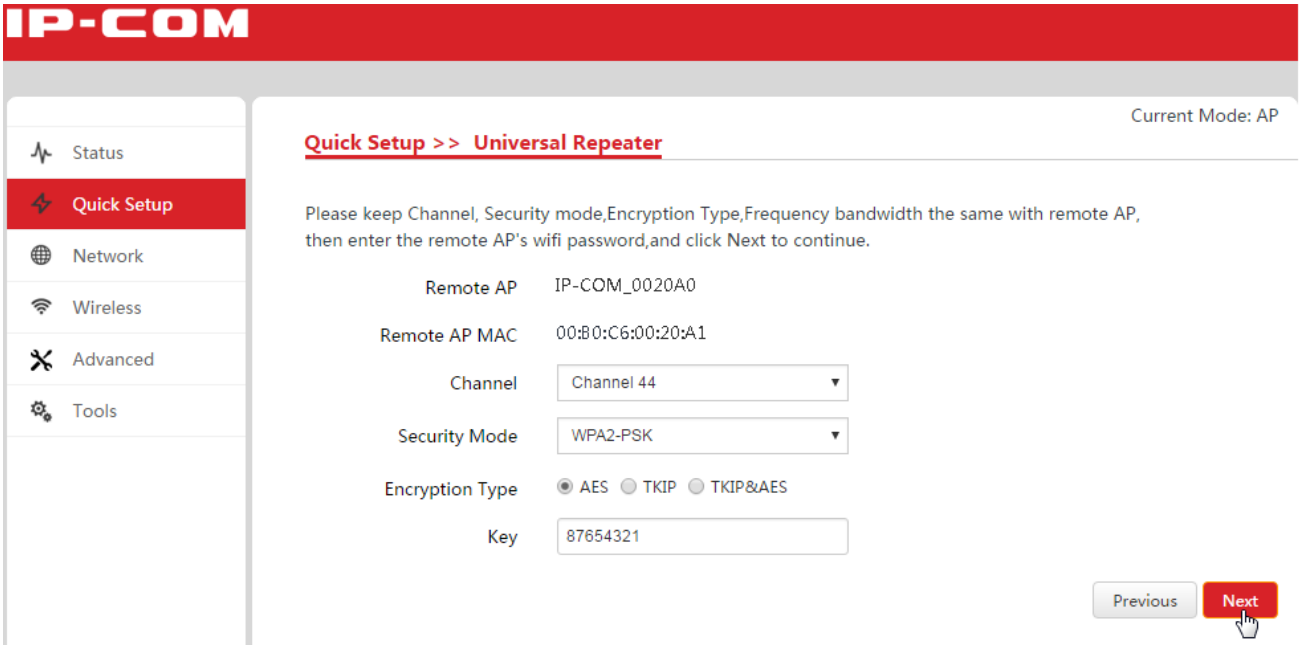
1. Log in to the device's web UI.
2. Go to **Quick Setup**, select **Universal Repeater**, and click **Next**.



3. In the scanned wireless signal list, select the remote AP's wireless network name (SSID), here we select IP-COM_0020A0, and click **Next**.

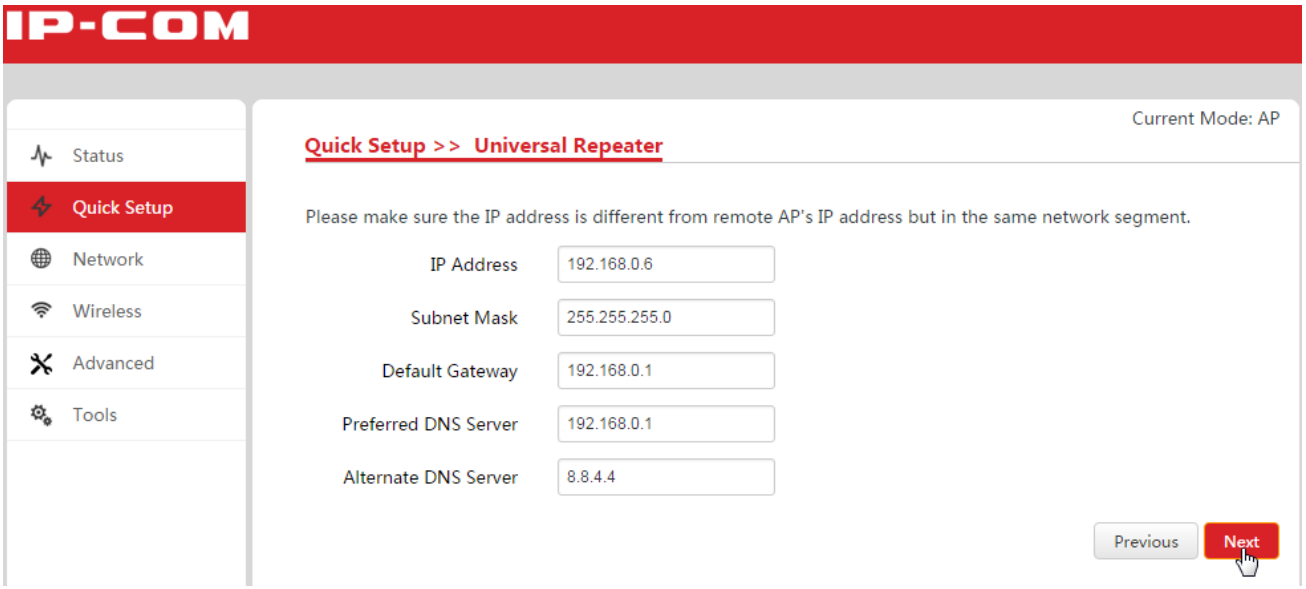


4. Enter the remote AP's WiFi password (Key), here we enter *87654321*, and click **Next**.

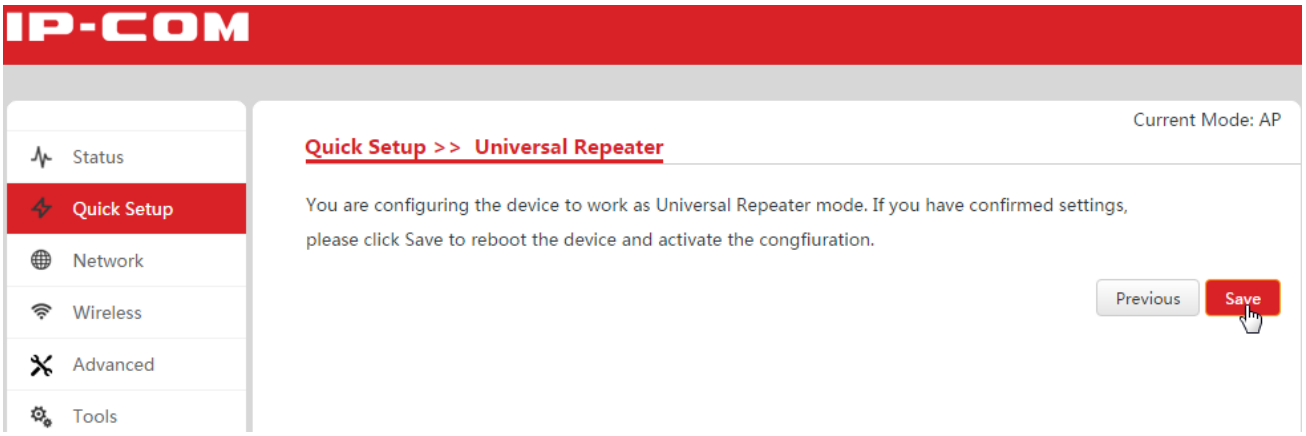


5. Set up IP info of this device.

- IP address: Modify this device's IP address to a different one but on the same IP segment from that of the remote AP. As the remote AP's IP address is *192.168.0.2*, we can enter *192.168.0.6* here.
- Subnet Mask： Set up a subnet mask.
- Default Gateway: Enter the default gateway address. We recommend that you be set to the LAN IP address of the router that is connected to the internet.
- Preferred DNS Server: Enter DNS info.
- Click **Next**.



6. Click **Save**. After the device reboot, the configuration will take effect.



Tip

After you finish configuring universal repeater mode, this device's SSID and WiFi password are changed to those of the remote AP.

4.2.4 WISP Mode

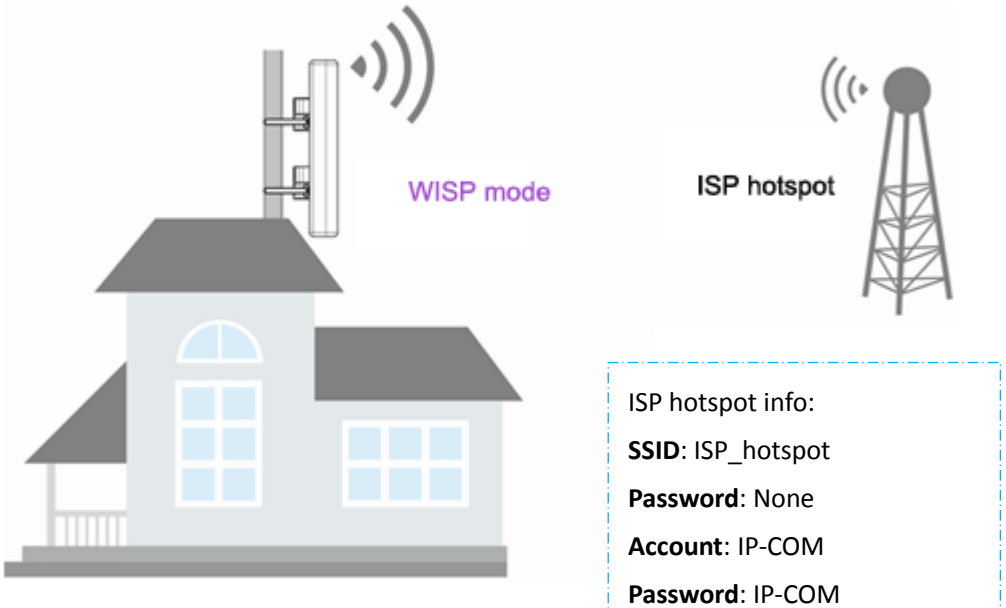
Usually, in this mode, the device wirelessly connects to a hotspot of an ISP, and of course it can connect to a wireless router. The connected wireless WAN interface obtains IP info from the hotspot or wireless router by DHCP, Static IP, or PPPoE mothod. As a result, the device's wired and wireless clients can access the hotspot or wireless router's network.

Note:

As a device's LAN and WAN IP segment cannot be the same, please make sure this device's LAN IP segment is different from that of the hotspot or wireless router's LAN IP segment. For example, if the wireless router's LAN IP segment is 192.168.2.X, please change this device's LAN IP segment to another one, such as 192.168.6.X.

Application scenario

In the following application, many wireless users want to access external network through the ISP hotspot. To achieve that, you can deploy this device in a place that the users can connect to and make the device work in WISP mode. In this way, the device can connect to the ISP hotspot wirelessly and the users that are connected to the device can access the external network.



ISP hotspot info:

SSID: ISP_hotspot

Password: None

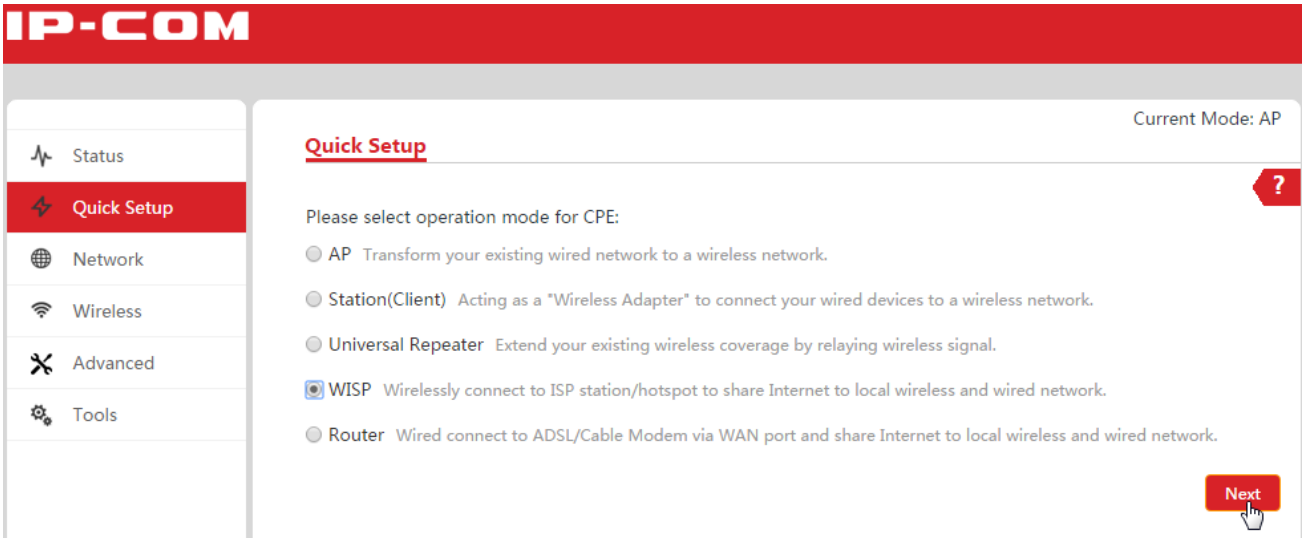
Account: IP-COM

Password: IP-COM

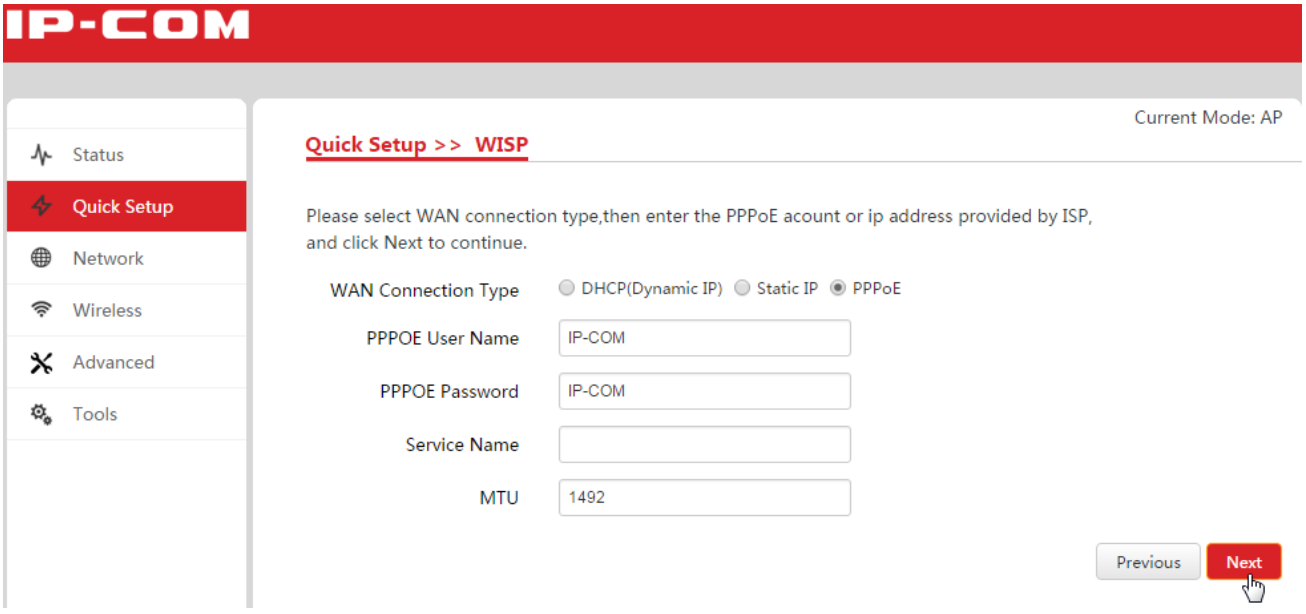
Configure WISP mode

To configure WISP mode:

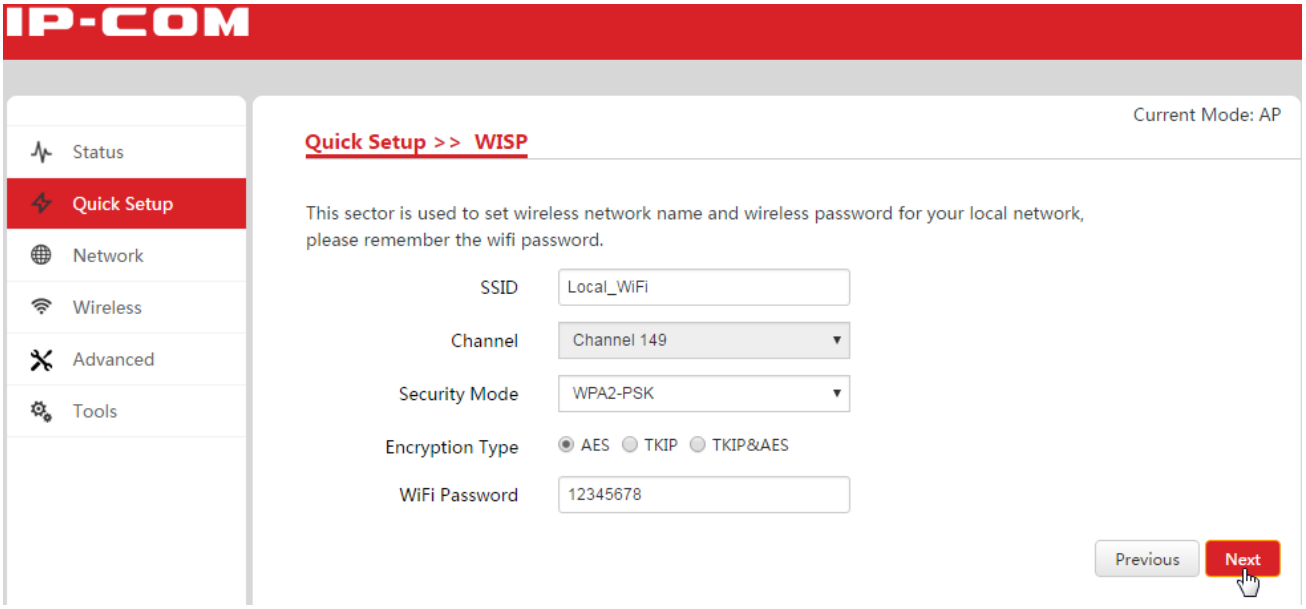
1. Log in to the device's web UI.
2. Go to **Quick Setup**, select **WISP**, and click **Next**.



3. In the scanned wireless signal list, select the ISP hotspot's SSID, here we select *hotspot*, and click **Next**.
4. In the pop-up page, click **Next**.
5. Set WAN info.
   - WAN Connection Type: Select PPPoE.
   - PPPoE User Name: Enter username provided by ISP, here we enter IP-COM.
   - PPPoE Password: Enter Password provided by ISP, here we enter IP-COM.
   - Service Name: Set up the service name, optional.
   - MTU: Set up the MTU value of this service. We recommend that you keep it default if you are not familiar.
   - Click **Next**.

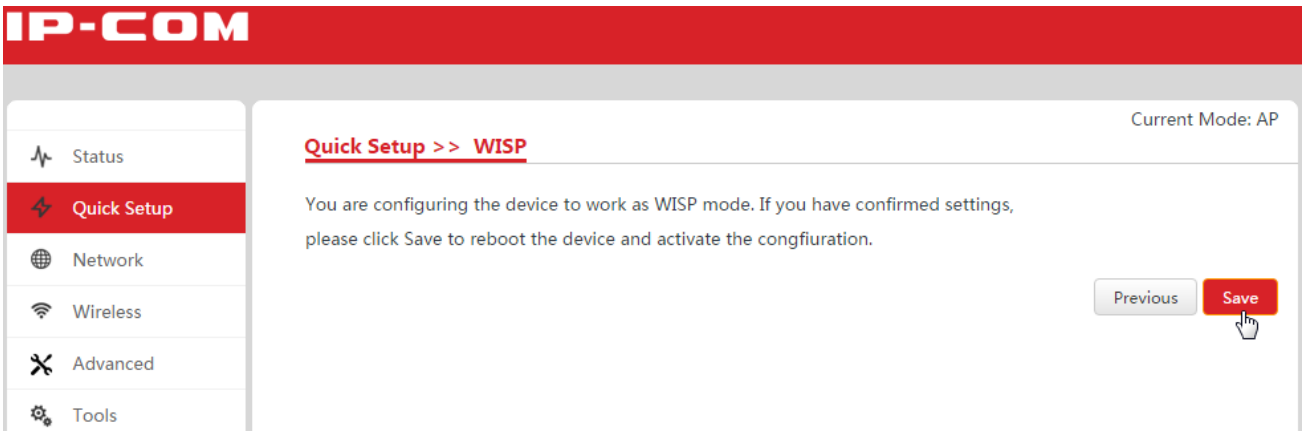


6. Set up the wireless parameters of this device.
   - SSID: Modify a SSID name, such as *Local WiFi*.
   - Security Mode, Encryption Type: We recommend that you select WPA2-PSK, AES.
   - WiFi Password: Set up wireless password, such as *12345678*.
   - Click **Next**.



7. Click **Next**.

8. Click **Save**. After the device reboots, the configurations take effect.



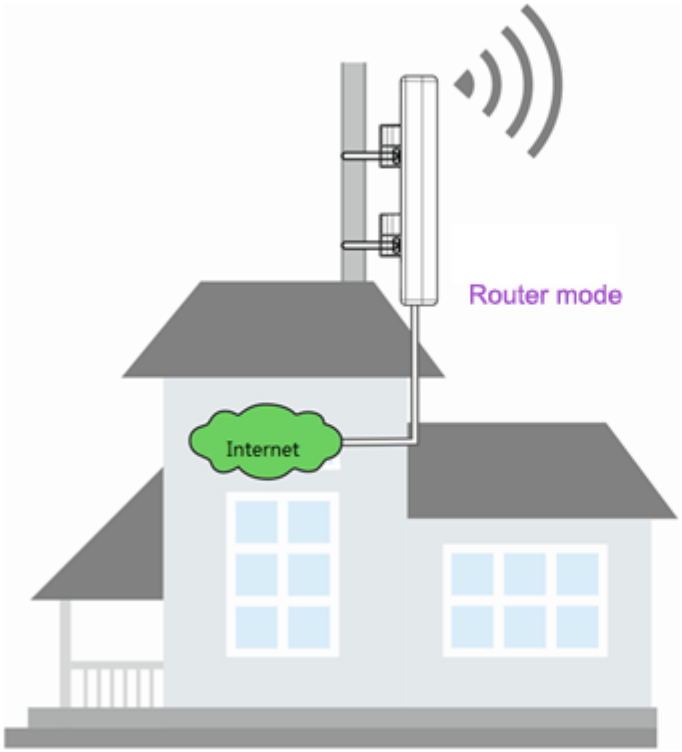
Re-enter into page **Status**, Connection Status is displayed as **Connected**. This means that the device is successfully connected to the ISP's hotspot.

4.2.5 Router Mode

In this mode, the PoE LAN/WAN port works as a WAN port and is connected to an uplink router using an Ethernet cable. The WAN port obtains IP info from the router by DHCP, Static IP or PPPoE method. As a result, the device's wired and wireless clients can access the uplink router's network.

Application scenario

A company subscribes to the ISP internet service and uses AP625 to deploy the company's network. In this case, AP625 can work in router mode to connect to the internet and provide wireless signals for users.



Internet account info provided by the ISP:

Username (PPPoE): 111

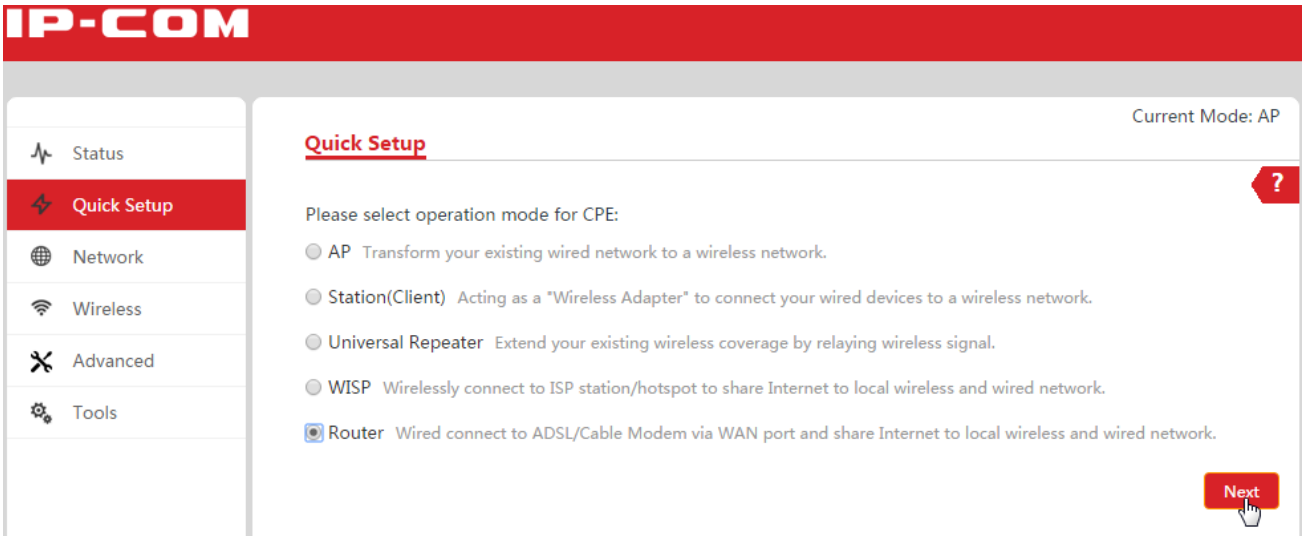
Password (PPPoE): 111

MTU: 1492

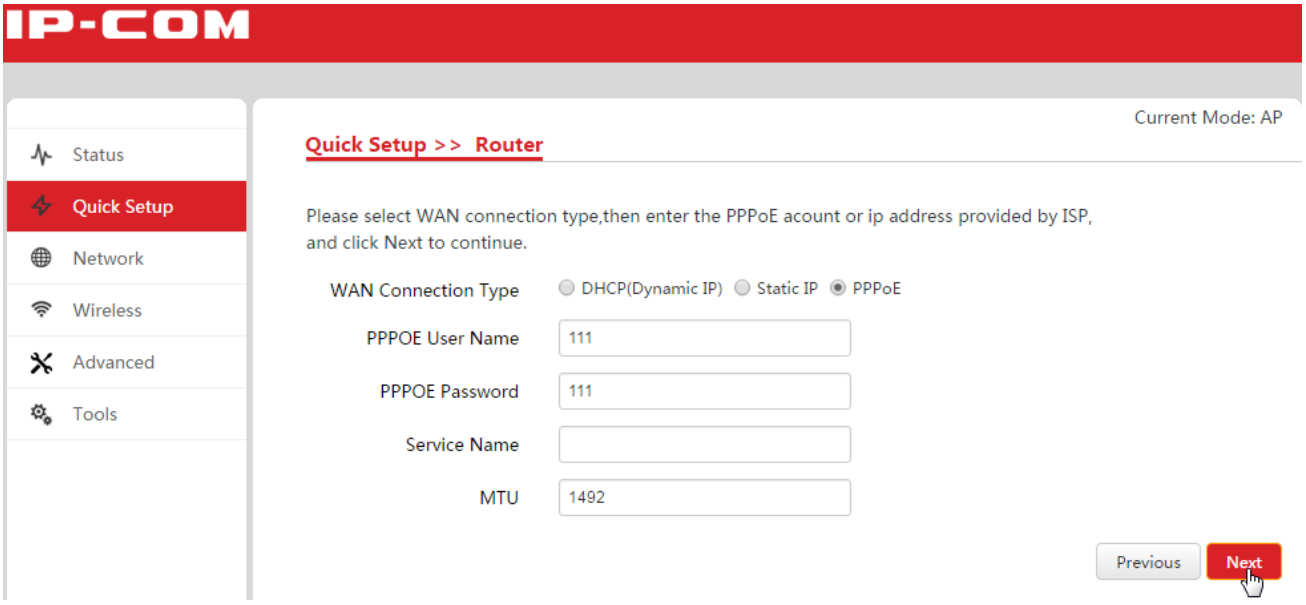
Configure router mode

To configure router mode:

1. Log in to the device's web UI.
2. Go to **Quick Setup**, select **Router**, and click **Next**.

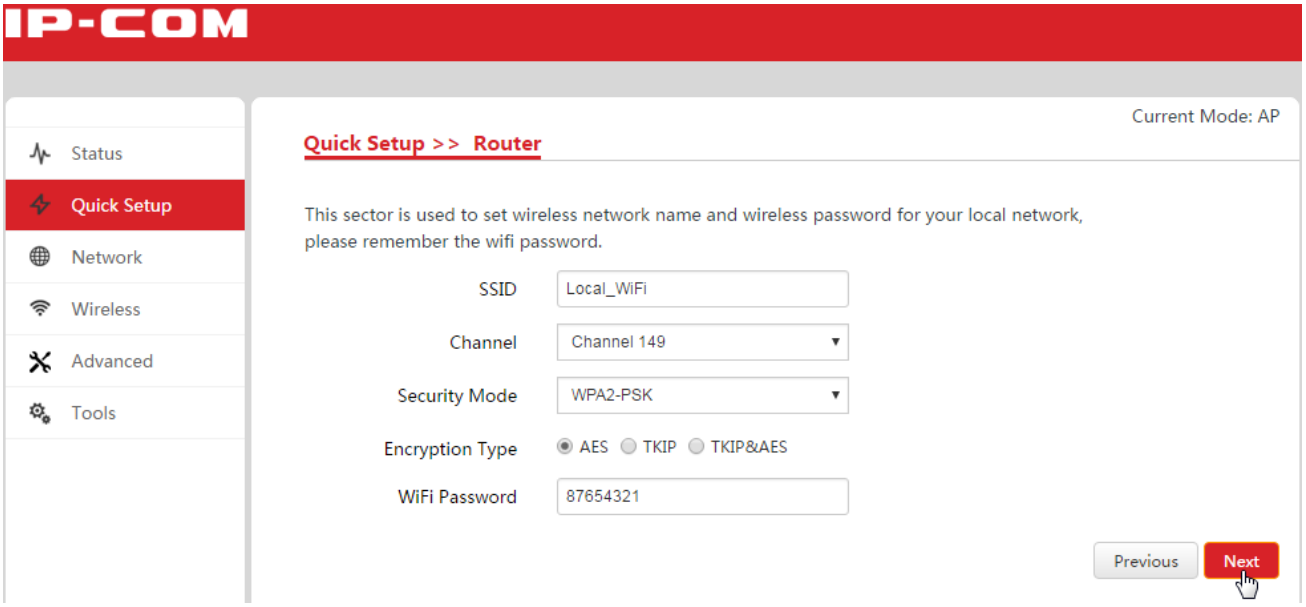


3. Set connection parameters.
   - WAN Connection Type: Select PPPoE.
   - PPPoE User Name: Enter *111*.
   - PPPoE Password: Enter *111*.
   - Service Name: Set up the service name, optional.
   - MTU: Enter *1492*.
   - Click **Next**.

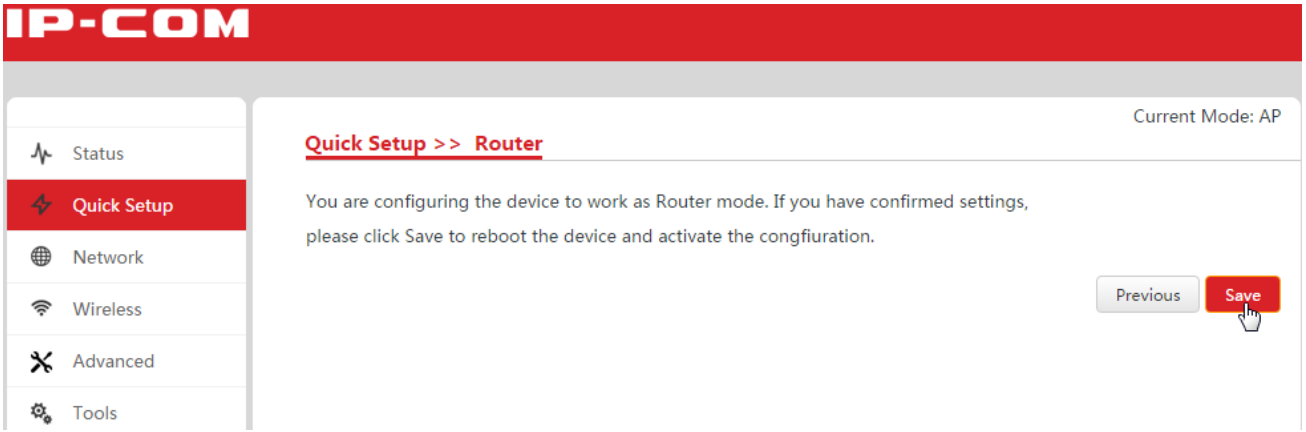


4. Set up the wireless parameters of this device.
   - SSID: Modify a SSID name, such as *Local WiFi*.
   - Security Mode, Encryption Type: We recommend that you select WPA2-PSK, AES.
   - WiFi Password: Set up wireless password, such as *12345678*.

- Click **Next**.



5. On the pop-up page, click **Save**. After the device reboots, the configurations take effect.



4.3 Network

Network settings contain the following:

- LAN Settings: On this page, you can set up LAN IP address, which is used to log in to the web UI and communicate with the local network.
- DHCP Server: On this page, you can enable/disable and set up DHCP server parameters for the device's clients.
- DHCP Client: On this page, you can check how many DHCP clients are connected and each client's IP address, MAC address and lease time.
- VLAN Settings: On this page, you can enable/disable and set up VLAN parameters.

4.3.1 LAN Settings

On this page, you can set up LAN IP address, which is used to log in to the web UI and communicate with the local network. This device supports two methods to set up your LAN IP address:

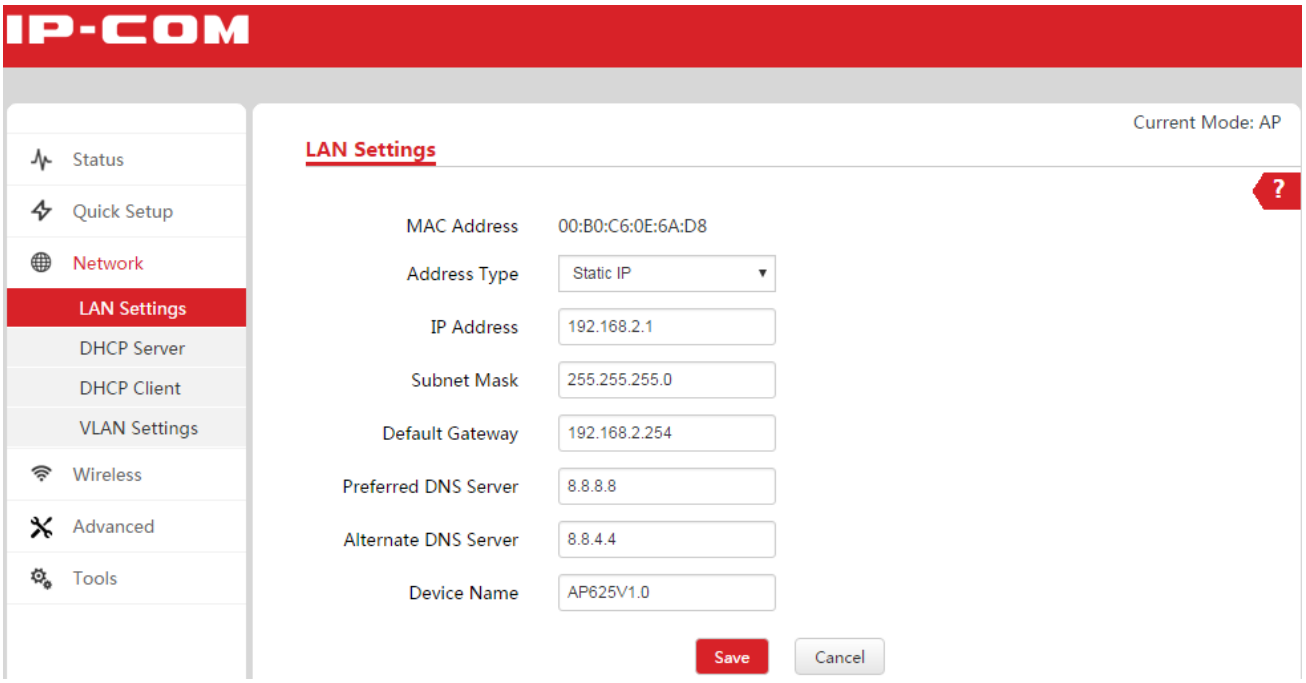
- Static IP: Set up LAN IP address manually

  In this method, you need to manually set up LAN IP address. If you modified LAN IP address, when you log in to the device's web UI, please use the new IP address. If you change LAN IP segment, please change your computer's IP segment to the new one as well.

- DHCP: Obtain LAN IP address from another DHCP server

  In this method, the device can obtain LAN IP address from another DHCP server. In this way, it reduces IP conflict and the cost of configuring IP address manually. If your device obtains LAN IP address from a DHCP server of an uplink router and you don't know the IP address, you can log in to the uplink router's web UI to check the obtained IP address.

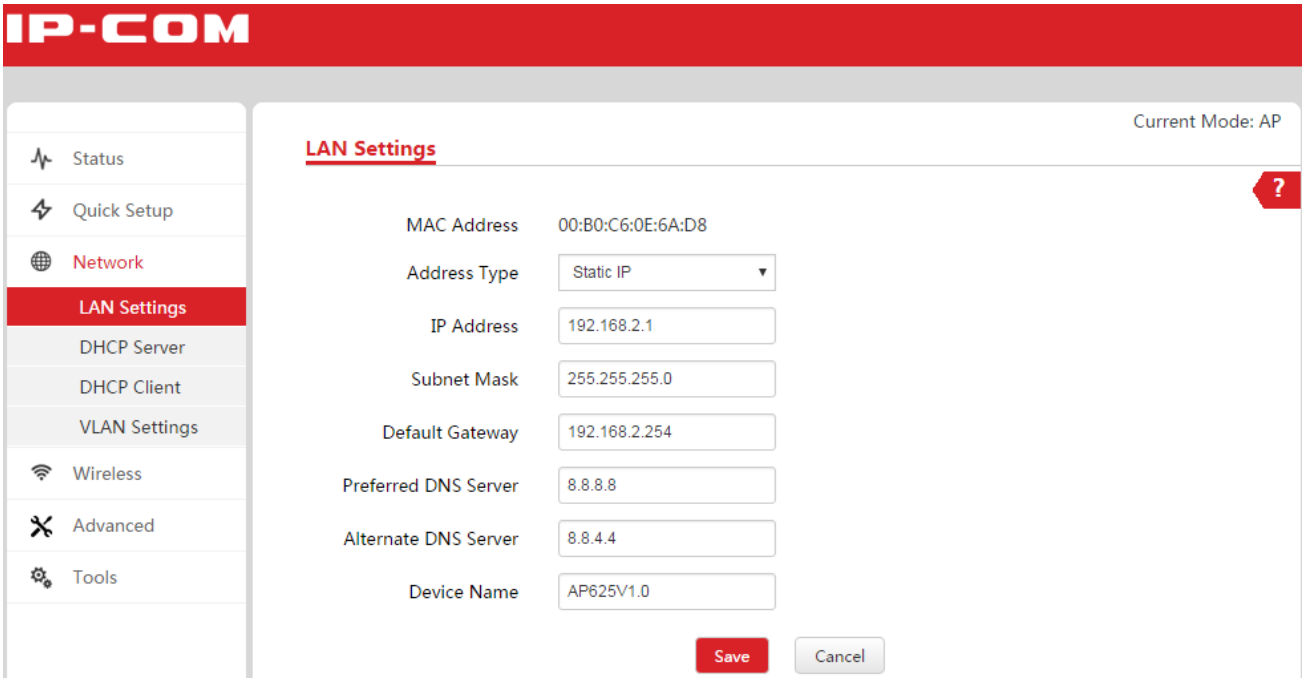
Parameter description



Parameter	Description
MAC Address	This device's MAC address of LAN port.
Address Type	Select a method to set up the LAN IP address.The default method is **Static IP**. • **Static IP:** In this method, you need to manually set up LAN IP address. If you modified LAN IP address, when you log in to the device's web UI, please use the new IP address. If you change LAN IP segment, please change your computer's IP segment to the new one as well. • **DHCP:** In this method, the device can obtain LAN IP address from another DHCP server. In this way, it reduces IP conflict and the cost of configuring IP address manually. If your device obtains LAN IP address from a DHCP server of an uplink router and you don't know the IP address, you can log in to the uplink router's web UI to check the obtained IP address.
IP Address	It is used to log in to the device's web UI and communicate with the local network. The default one is 192.168.2.1.
Subnet Mask	It is used to determine IP segment of the IP address. The default one is 255.255.255.0
Default gateway	It helps the device find a network route to connect to the internet or other networks.
Preferred DNS server	Domain names, such as *www.google.com*, are easier to remember than IP addresses, such as *93.46.8.89*. A correct DNS server allows you to access websites using their domain names instead of IP addresses.
Alternate DNS server	It is a backup DNS server address.
Device Name	Enter a distinct name for your device so that the administrator can manage the device from a remote spot if necessary.

Static IP: Set up LAN IP address manually

In this method, you need to manually set up LAN IP address. If you modified LAN IP address, when you log in to the device's web UI, please use the new IP address. If you change LAN IP segment, please change your computer's IP segment to the new one as well.



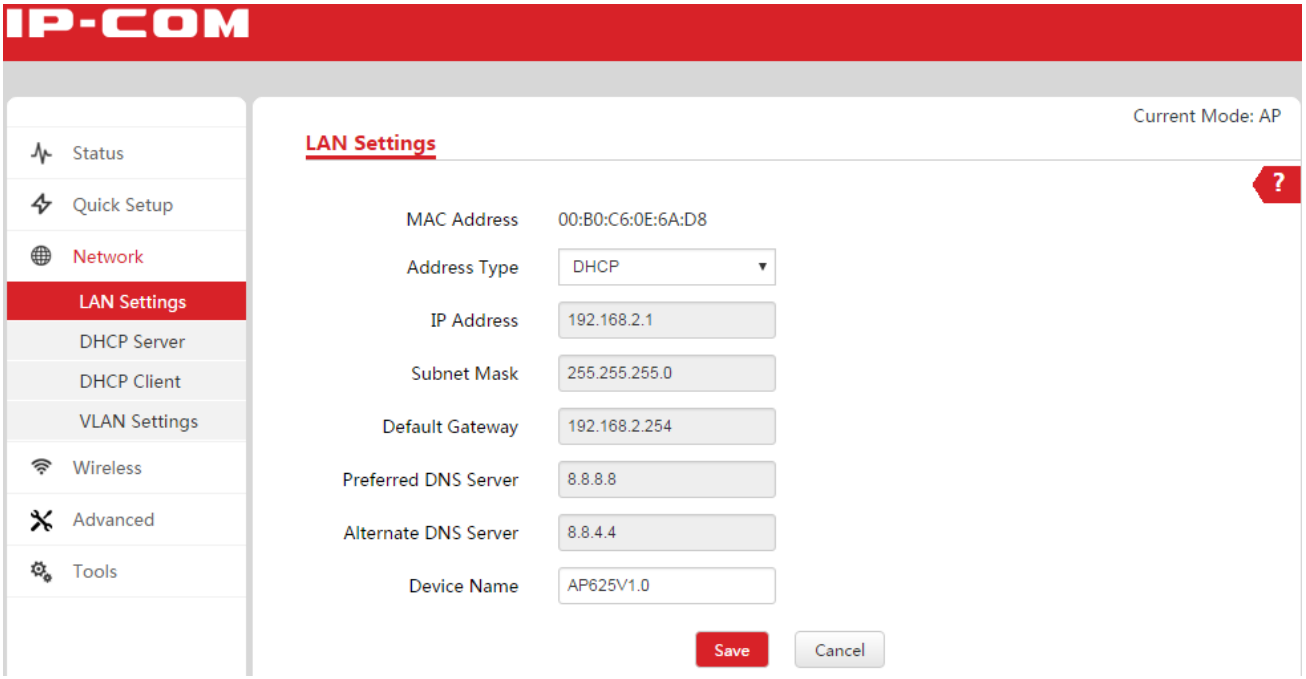
To set up LAN IP address manually:

1. Log in to the device's web UI.
2. Go to **Network > LAN Settings**.
3. Set up LAN IP parameters.
   1) Address Type: Click the dropdown list and select **Static IP**.
   2) IP Address: Enter a new IP address, such as *192.168.0.2*.
   3) Subnet Mask: Enter a subnet mask for the IP address, such as *255.255.255.0*.
   4) Default Gateway: Enter a gateway for the device so that the device can find a network route to connect to the internet or other networks. Usually it's the uplink router's LAN IP address.
   5) Preferred DNS Server: Enter the preferred DNS server address. If there is another backup DNS server, enter it into Alternate DNS Server field.

      A correct DNS server allows you to access websites using their domain names instead of IP addresses.
   6) Device Name: Enter a distinct name for your device so that the administrator can manage the device from a remote spot if necessary.
4. Click **Save** to make these settings take effect.

DHCP: Obtain LAN IP address from another DHCP server

In this method, the device can obtain LAN IP address from another DHCP server. In this way, it reduces IP conflict and the cost of configuring IP address manually. If your device obtains LAN IP address from a DHCP server of an uplink router and you don't know the IP address, you can log in to the uplink router's web UI to check the obtained IP address.

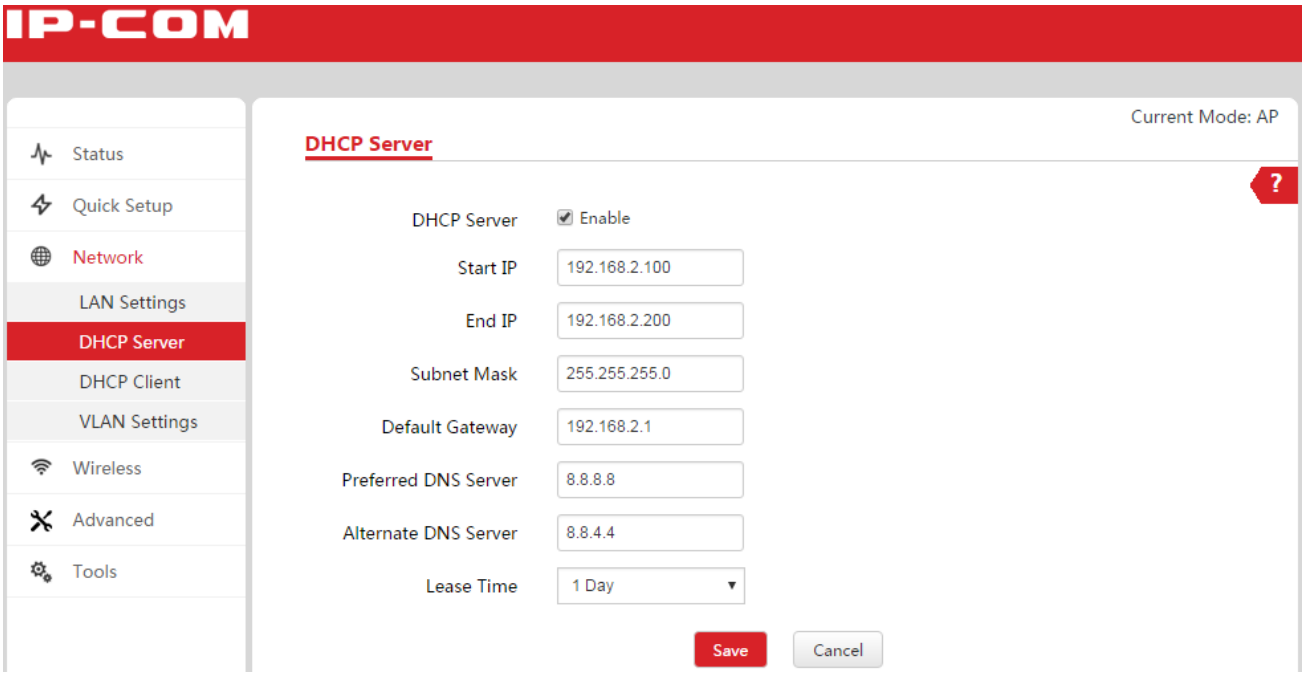


To obtain LAN IP address from another DHCP server:

1. Log in to the device's web UI.
2. Go to **Network > LAN Settings**.
3. Address Type: Click the dropdown list and select **DHCP**.
4. Click **Save** to make these settings take effect.

4.3.2 DHCP Server

On this page, you can enable/disable and set up DHCP server parameters for the device's clients. When you finish configuring AP mode, Station (Client) mode or Universal Reapter mode, DHCP server is automatically disabled and you need to manually enable this function if necessary.



Parameter description

Parameter	Description
DHCP Server	Enable/disable the device's DHCP server. By default, it is enabled.
Start IP	The first IP address that can be assigned to a DHCP client. By default, it is 192.168.2.100.
End IP	The last IP address that can be assigned to a DHCP client. By default, it is 192.168.2.200.
Subnet Mask	It is used to determine the IP segment of the DHCP server. By default, it is 255.255.255.0.
Default gateway	It is assigned to DHCP clients so that they can find a network path to access the internet or other networks. By default, it is 192.168.2.254.
Preferred DNS Server	Domain names, such as *www.google.com*, are easier to remember than IP addresses, such as *93.46.8.89*. A correct DNS server allows you to access websites using their domain names instead of IP addresses.
Alternate DNS Server	It is a backup DNS server address.
Lease Time	When a DHCP client obtains IP address, the DHCP server will assign a certain lease time to the client's IP address. If a DHCP client wants to use the IP address continuously, when the lease time goes to 50%, the DHCP client will transmit a unicast DHCP request to the DHCP server. If the DHCP client gets no response from the DHCP server, it will continue to transmit a unicast DHCP request to the DHCP server when the lease time goes to 7/8. If it fails again, when the lease time goes to 100%, the IP address will be released and might be used by other DHCP clients.

Configure DHCP server

Note

If more than one DHCP server exists in the same network, to avoid IP conflict, make sure the IP pool of each DHCP server doesn't overlap.

To configure DHCP server:

1. Log in to the device's web UI.
2. Go to **Network > DHCP Server**.
3. Set up DHCP server parameters.
    1) DHCP Server: Check the box of **Enable**.

2) Start IP/End IP: Enter the first and last IP address of the DHCP IP pool.

3) Subnet Mask: Enter a subnet mask for the DHCP server.

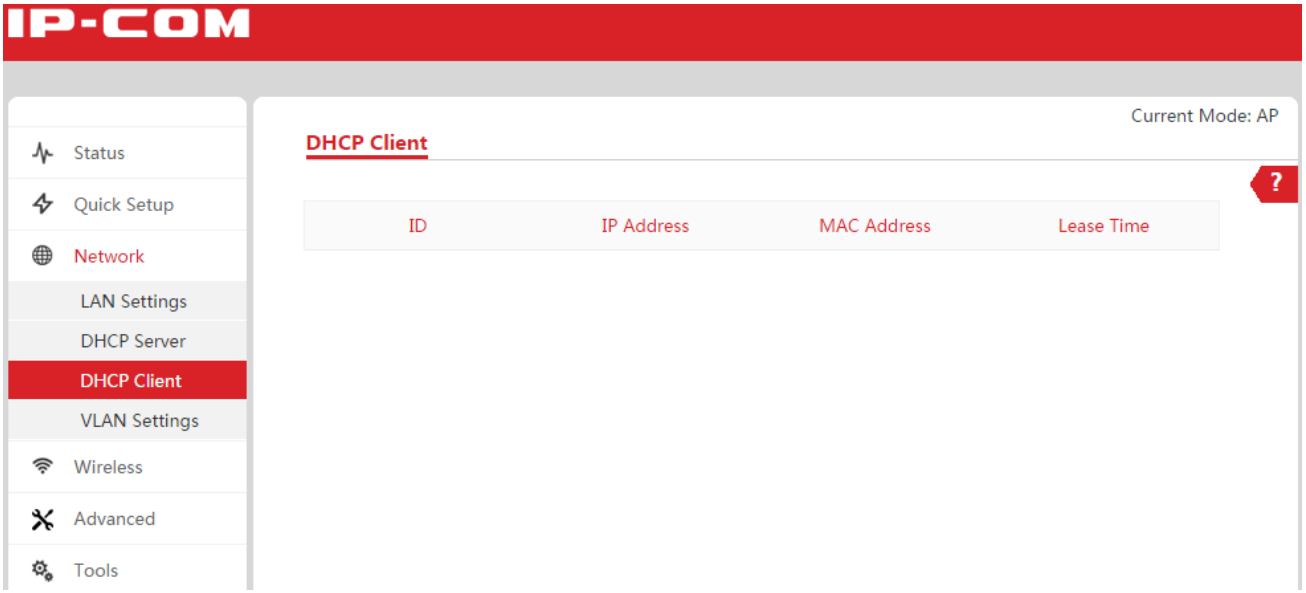
4) Default Gateway: Enter a gateway which is assigned to DHCP clients.

5) Preferred/Alternate DNS Server: Enter a preferred DNS server address for DHCP clients. If there is another DNS server, please enter it into the Alternate DNS Server field.

4. Click **Save** to make these settings take effect.

4.3.3 DHCP Client

On this page, you can check how many DHCP clients are connected and each client's IP address, MAC address and lease time.

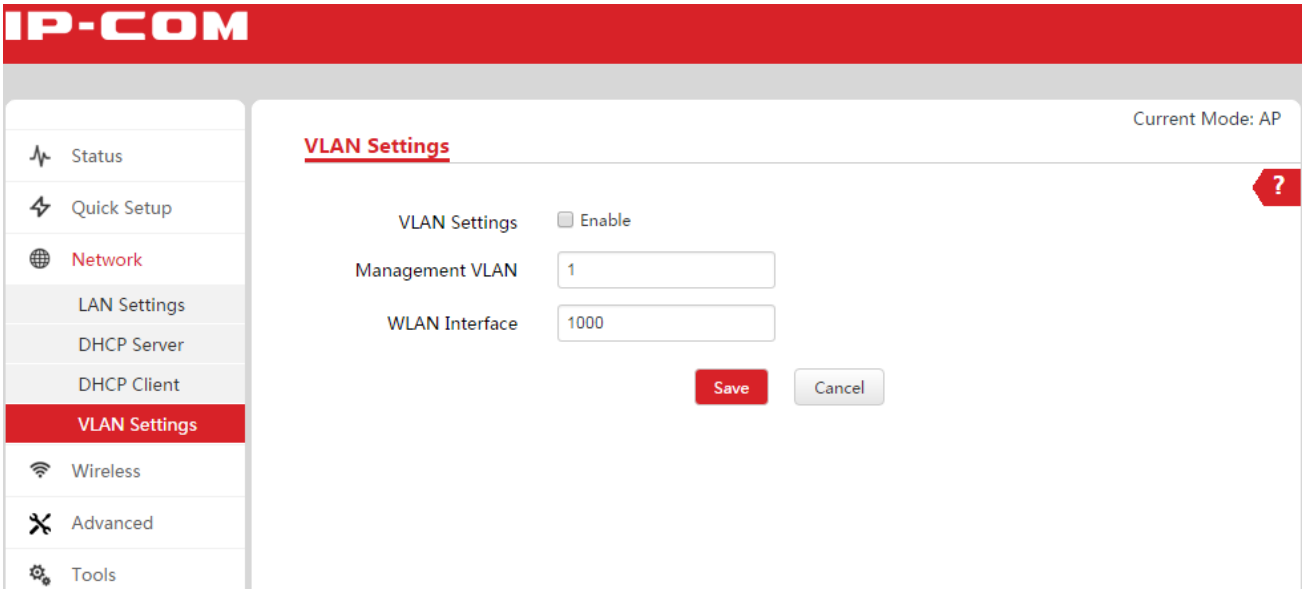


To enter DHCP Client page:

1. Log in to the device's web UI.
2. Go to **Network > DHCP Client**.

4.3.4 VLAN Settings

On this page, you can enable/disable and set up VLAN parameters. With this device and a switch with QVLAN function, you can effectively manage wireless network.



Parameter description

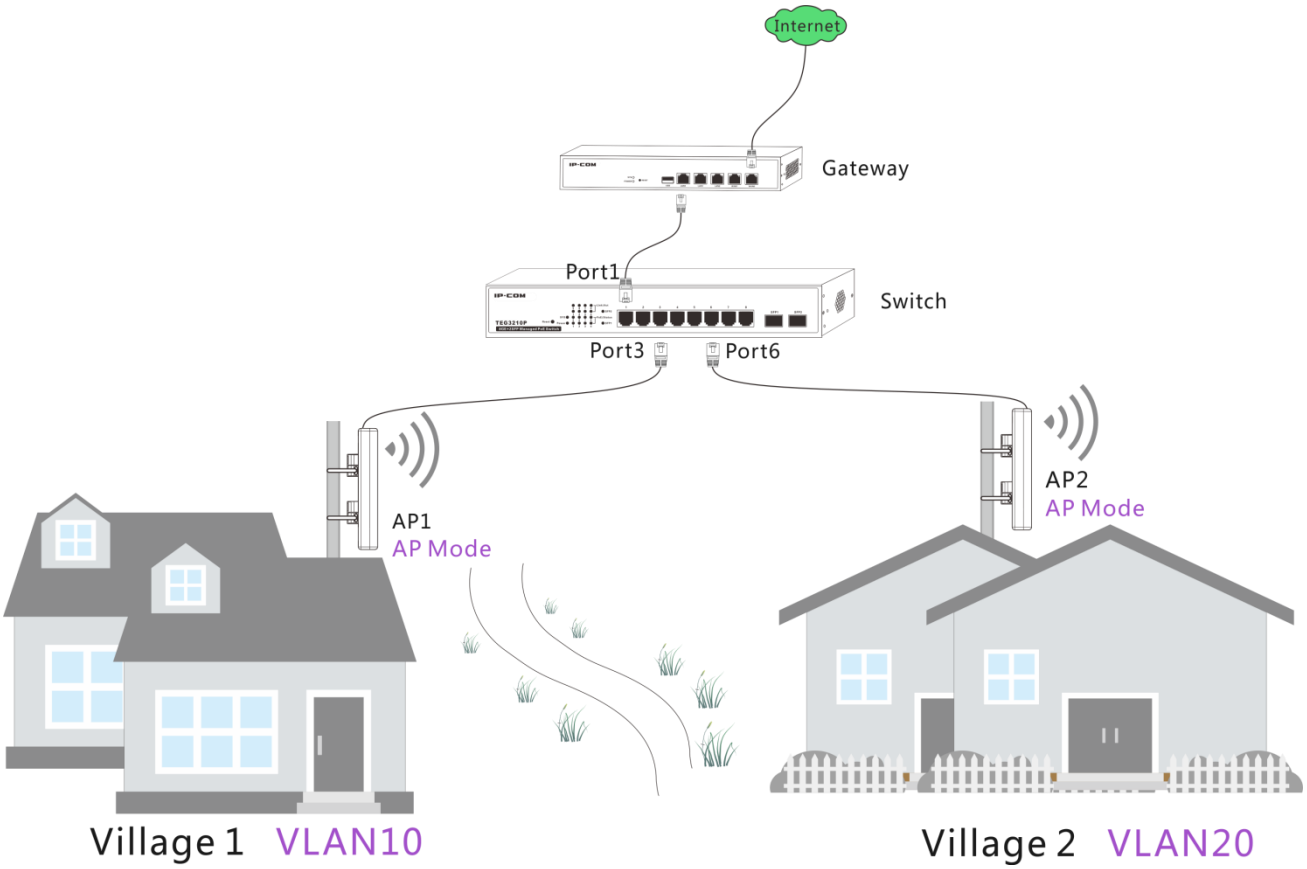
Parameter	Description
VLAN Settings	Enable of disable VLAN function of the device. After you enable VLAN function, the *PoE LAN/WAN* port becomes a trunk port, which can allow multiple VLANs to get through. By default, VLAN function is disabled.
Management VLAN	Set up this device's management VLAN ID. By default it is 1. After the management VLAN is modified, only when the management computer is in the same VLAN can it access this device's web UI.
WLAN Interface	Set up VLAN ID of this device's wireless interface. By default it is 1000. The range is 1 ~ 4094. After you set up this VLAN ID, the device's wireless interface becomes an access port, which only allows tagged packets in the same VLAN or untagged packets to get through.

The detailed receiving and sending procedures on each type of port are described as below:

Port Type	Procedures on receiving packets		Procedures on sending packets
	Tagged packets	Untagged packets	
Access port	Tagged packets are forwarded to other ports with the same VLAN ID as the tagged packets.	Untagged packets are forwarded to other ports with the same VLAN ID as the PVID of the receiving port.	Delete the packets' tag and send the packets to a network device that doesn't support VLAN function.
Trunk port			VLAN ID = PVID, delete tag and send. VLAN ID ≠PVID, keep tag and send.

Application scenario

In the following application, users in village 1 and village 2 need to access the internet. On the other hand, for network security, users in different villages can't communicate with each other. In this case, we can deploy an AP625 in village 1 and village 2 respectively, and make the two devices work in different VLANs. Assume that village 1 is in VLAN 10, and village 2 is in VLAN 20.



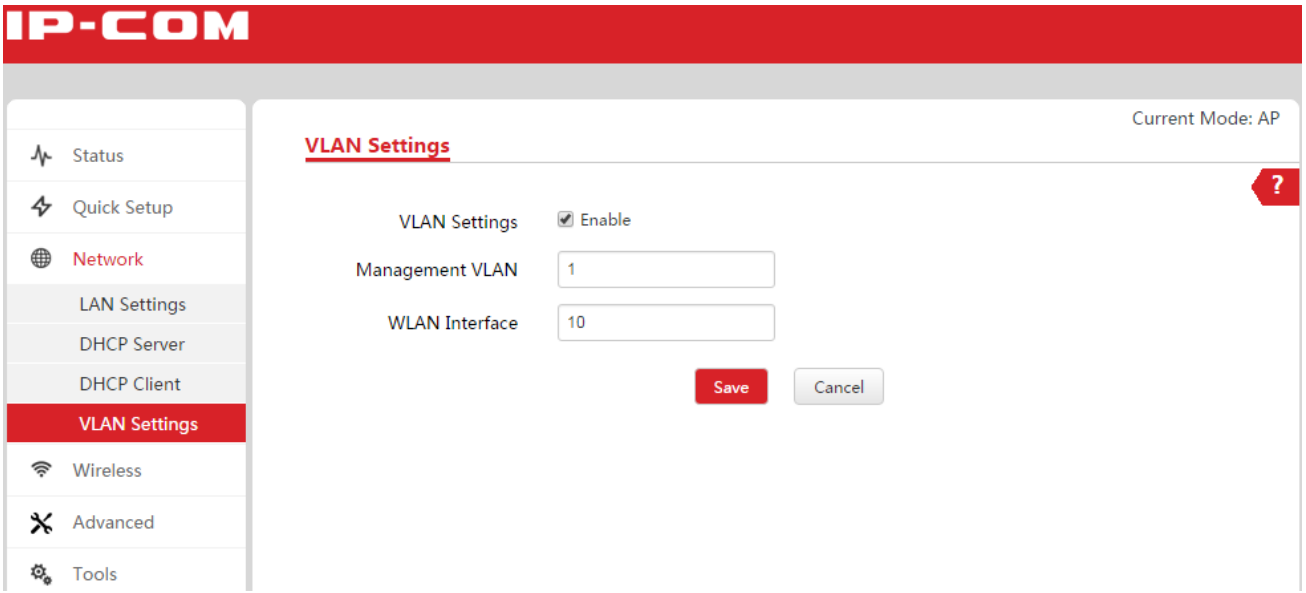
Configure VLAN function

Step1: Set up LAN IP address of the two APs

Please refer to 4.3.1 LAN Settings to finish this step. Make sure LAN IP addresses of the two devices are different but on the same IP segment.

Step 2: Set up VLAN parameters of AP1.

1. Log in to AP1's web UI and go to **Network > VLAN Settings**.
2. VLAN Settings: Check the box to enable VLAN function.
3. Management VLAN: Keep the default value.
4. WLAN Interface: Enter *10*.
5. Click **Save** to make these settings take effect.



Step 3: Set up VLAN parameters of AP2.

This step is similar to that of AP1. One difference is that enter *20* in WLAN Interface field.

Step 4: Set up VLAN parameters of the switch (Here we take IP-COM G1224T as an example.)

Switch Port	Allowed VLAN ID	Port Type	PVID
Port 1 (Connect to Gateway)	1, 10, 20	Trunk port	1
Port 3 (Connect to AP1)	1,10	Trunk port	1
Port 6 (Connect to AP2)	1,20	Trunk port	1

Step 5: Set up VLAN parameters of the gateway

The port connecting to the switch should allow VLAN 10 and VLAN 20 to get through.

4.4 Wireless

Wireless settings contain the following:

- Basic: On this page, you can set up basic wireless parameters of this device, such as SSID, broadcast SSID, encryption type, etc.
- Advanced: On this page, you can set up advanced wireless parameters of this device. You can keep the default value if you're not familiar with these parameters.
- Access Control: On this page, you can set up rules to forbid or permit specified wireless clients to access this device. The rules are based on MAC address.

4.4.1 Basic

On this page, you can set up basic wireless parameters of this device, such as SSID, broadcast SSID, encryption type, etc.

Parameter description

As the device provides lots of wireless parameters, to help you understand these parameters, we devide them into several parts, shown as below.

- Commonly used parameters description
- Parameter description of WEP
- Parameter description of WPA-PSK, WPA2-PSK and WPA-PSK&WPA2-PSK
- Parameter description of WPA and WPA2

Commonly used parameters description

Parameter	Description
WiFi	Enable/Disable the device's wireless signal.
Country	Select a country that your device is operating.
SSID	The wireless name of the device. To better recognize your wireless network, we recommend that you modify the SSID.
Broadcast SSID	Enable or disable broadcast SSID function. • Enable: the device broadcasts its SSID and the SSID is displayed in the network list of clients that support 5G. • Disable: the device does not broadcast its SSID and the SSID is not displayed in the network list of clients that support 5G. When a client want to connect to the device, the client needs to manually enter the correct SSID name.

Network Mode	Select an 802.11 network mode. By default the device works at 11ac mode. • 11a mode: Clients that support 11a network mode can connect to the device. The wireless speed can be up to 54Mbps. • 11a/n mode: Clients that support 11a or 11n network mode can connect to the device. The wireless speed can be up to 150Mbps. • 11ac mode: Clients that support 11ac network mode can connect to the device. The wireless speed can be up to 433Mbps.
Encryption Type	Set up the wireless encryption type. None means allowing any client to connect to the device. This device supports WEP, WPA-PSK, WPA2-PSK, WPA-PSK&WPA2-PSK, WPA and WPA2, for details, refer to ● Parameter description of WEP ● Parameter description of WPA-PSK, WPA2-PSK and WPA-PSK&WPA2-PSK ● Parameter description of WPA and WPA2
Channel	Click the dropdown list and select a wireless channel. To avoid channel conflict, please select a channel that is less used in surrounding area. You can go to **Advanced > Diagnose** and select Site Survey to check each channel's usage.
TX Power	Set up the device's wireless TX Power. The range is 8dBm ~ 26dBm.
Bandwidth	• 20: This device can only use 20MHz bandwidth. • 40: This device can only use 40MHz bandwidth. • 80: This device can only use 80MHz bandwidth.
Extension Channel	It is used to determine the AP's channel range when bandwidth is 40.
AP Isolation	• Enable: Wireless clients that connect to the SSID can't communicate with each other. • Disable: Wireless clients that connect to the SSID can communicate with each other.
TX Rate	Wireless transmission rate of the device. The device can automatically adjust the rate based on the network environment, so you can select **Auto** if not specified. • When you select 20 at bandwidth section, the highest wireless rate is MCS8 86Mbps. • When you select 40 at bandwidth section, the highest wireless rate is MCS9 200Mbps. • When you select 80 at bandwidth section, the highest wireless rate is MCS9 433Mbps.

Encryption mode description:

Parameter description of WEP

WEP (Wired Equivalent Privacy). A static key is used to encrypt all data, providing a security level equal to wired LAN encryption. The wireless rate can be up to 54Mbps.

Parameter	Description
Authentication Type	This device support 2 authentication methods: Open, Shared. The encryption method of the two processes is the same. • **Open**: In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate. In effect, no authentication occurs. Subsequently WEP keys can be used for encrypting data frames. At this point, the client must have the correct keys. • **Shared**: In a shared authentication, the WLAN client needs to provide its credentials to the Access Point during authentication.
Default Key	Once you select a certain key, such as key 1, wireless clients must use the same key, key 1, to connect to your device. For WEB security mode, most smart phones only support key 1, so we recommend that you select key 1 of this device.
ASCII	Enter a WEP key. The length of the character string is a 5 or 13.
HEX	Enter a WEP key. The length of the character string is 10 or 26.

Parameter description of WPA-PSK, WPA2-PSK and WPA-PSK&WPA2-PSK

It is designed for home and small office networks and doesn't require an authentication server. Each WLAN network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. If ASCII characters are used, the 256 bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1.

Parameters	Description
Security Mode	Select a security mode.
Encryption Type	Select WPA encryption type. • AES: AES is short for Advanced Encryption Standard. This encryption algorithm ensures a higher wireless rate. • TKIP: TKIP is short for Timing Key Integrity Protocol. Wireless rate can only reach 54Mbps with this algorithm.

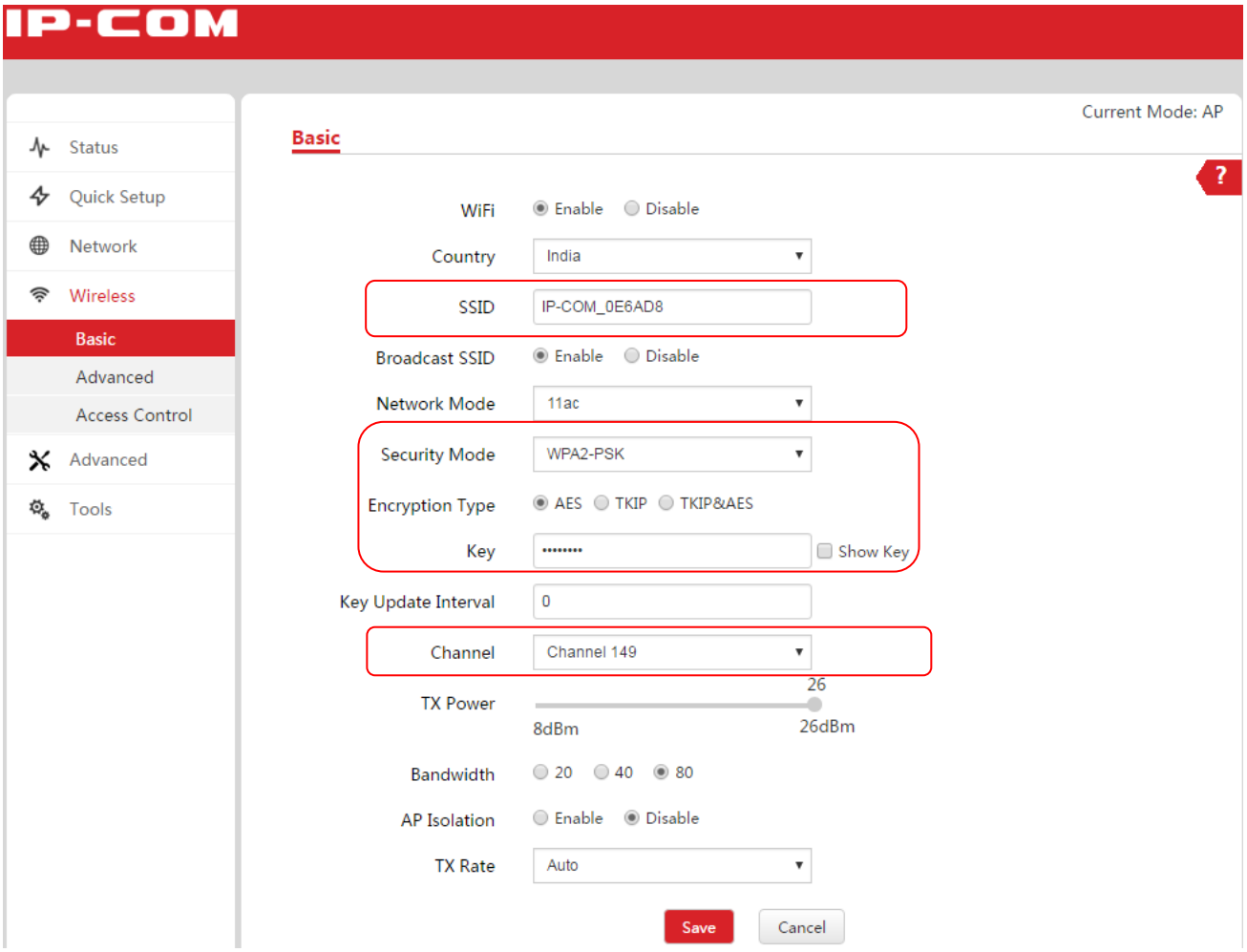
	• TKIP&AES: Compatible with TKIP and AES. The wireless client can use either AES or TKIP algorithm to connect to the WiFi.
Key	Enter a security key that is either 8 - 63 ASCII characters or 8 - 64 Hex characters.
Key Update Interval	You can configure security key's update interval here within the range from 60 to 99999 seconds. If set to 0, the key will not be updated.

Parameter description of WPA and WPA2

WPA is opposed to WPA-PSK and is also referred to as WPA-802.1X mode. It is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. WPA-Enterprise mode is available with both WPA and WPA2.

Parameters	Description
Radius Server IP	Enter the radius server IP address for authentication.
Radius Port	Enter the authentication port of the radius server.
Key	Enter the shared key of the radius server.

Configure basic wireless parameters

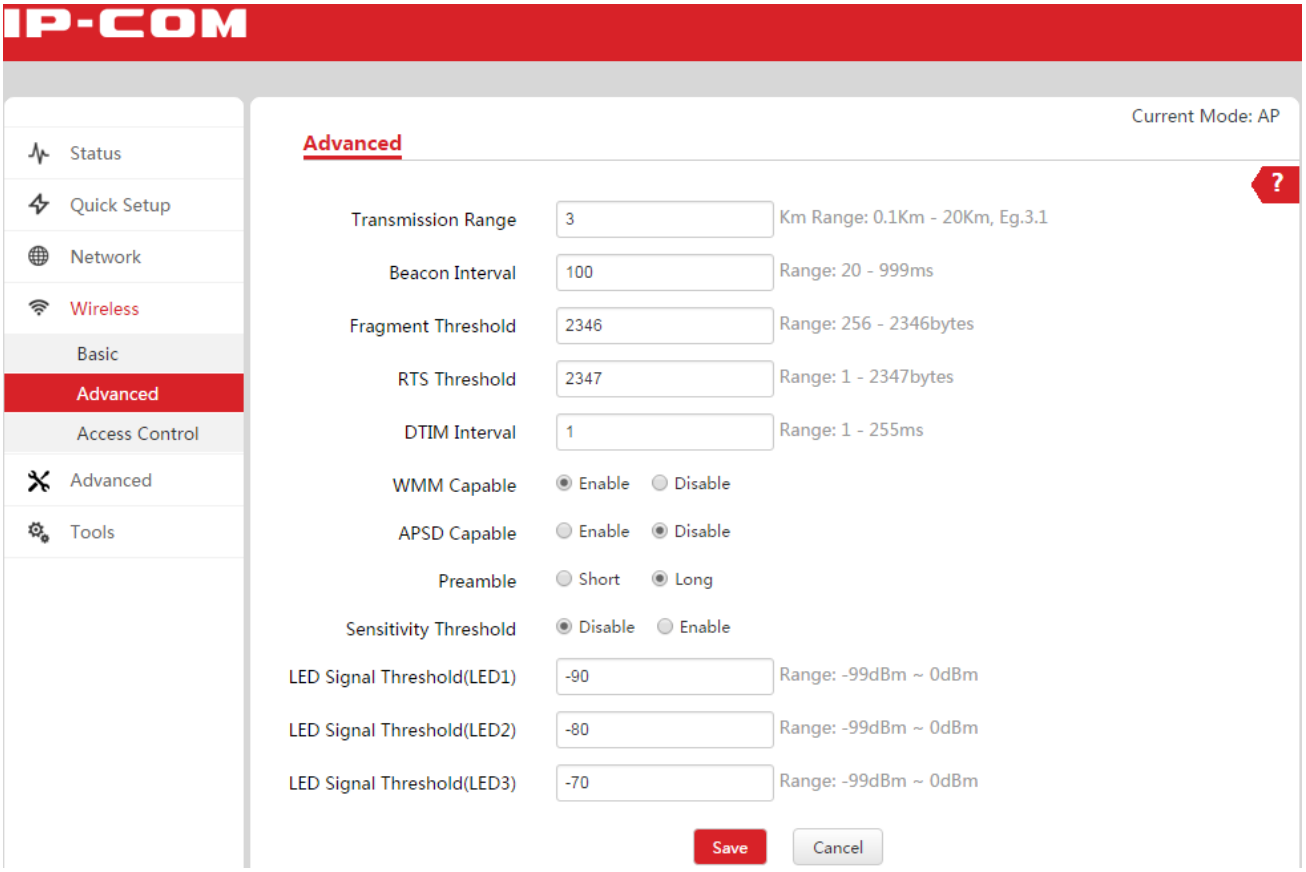


To configure basic wireless parameters:

1. Log in to the device's web UI.
2. Go to **Wireless > Basic**.
3. Set up basic wireless parameters.
   1) SSID: Modify the device's SSID.
   2) Security Mode, Encryption Type, Key: We recommend that you select WPA2-PSK and AES and set up a WiFi password (Key). For more information, please refer to Encryption Method Description.
   3) Channel: Click the dropdown list and select a wireless channel. To avoid channel conflict, please select a channel that is less used in surrounding area. You can go to **Advanced > Diagnose** and select Site Survey to check each channel's usage.
   4) Other parameters: If not specified, you can keep the default value.
4. Click **Save** to make these settings take effect.

4.4.2 Advanced

On this page, you can set up advanced wireless parameters of this device. You can keep the default value if you're not familiar with these parameters.



Parameter description

Parameter	Description
Transmission Range	This device's wireless transmission range.
Beacon Interval	Set up an interval for sending beacon frames. The range is 20~999ms. Beacon frames are transmitted at a regular interval to allow mobile clients to join the network. Beacon frames are used for a client to identify nearby APs. In general, the smaller the value is, the quicker a wireless client can connect to the AP. the larger the value is, the higher the data transmission of the WLAN network's efficiency is.

Fragment Threshold	Set up the maximum length of frames that can be transmitted without fragmentation. The range is 256~2346 bytes. Fragmentation means to fragment a large frame into small pieces, with each piece transmitted and acknowledged separately. When the length of a frame exceeds the specified fragment threshold value, it is fragmented. • A longer frame is less likely to be successfully received. Therefore, in a WLAN where there is high error rate, you can decrease the fragment threshold to increase frame transmission reliability. • In a WLAN network with no interference, we recommend that you increase the Fragment Threshold to improve the data transmission throughput by decreasing the ACK times.
RTS Threshold	Set up the threshold length for RTS/CTS mechanism. RTS/CTS frames occupy a certain network bandwidth so that only the frames larger than RTS/CTS threshold will enable RTS/CTS mechanism to avoid data sending collisions in a WLAN network. The RTS/CTS threshold range is 1~2347 bytes. You need to set up a rational value: A small value causes RTS packets to be sent more often, thus consuming more of the available bandwidth. However, the more often RTS packets are sent, the quicker the system can recover from interference or collisions. We recommend that you set up a small value in a high-density WLAN network to decrease the probability of collision.
DTIM Interval	Set up the number of beacon intervals between Delivery Traffic Indication Message (DTIM) transmissions. The range is 1~255 Beacon interval. The AP sends buffered broadcast/multicast frames with the configured DTIM interval. For example, if you set DTIM to 2, the AP will send buffered broadcast/multicast frames every two Beacon intervals.
WMM Capable	WMM is a wireless QoS protocol designed to preferentially transmit packets with high priority, thus guaranteeing better QoS services for voice and video applications in a WLAN network.
APSD Capable	APSD (Automatic Power Save Delivery) is disabled by default.
Preamble	Mainly used for preamble synchronization. It is advisable to keep the default value unchanged.
Sensitivity Threshold	Define the minimum client signal level accepted by the AP for the client to connect to. If the client signal level subsequently drops, the client remains connected to the AP.
LED Signal Threshold (LED1/LED2/LED3）	When two devices bridge successfully, LED1/LED2/LED3 keeps solid. The three LEDs indicate the signal strength of the other bridged device. By default, the relations between the signal strength and LEDs are shown below, and you can modify each LED's threshold on the web UI. • -90 dBm < signal strength < -80dBm: LED1 turns green. • -80 dBm < signal strength < -70dBm: LED1 and LED2 turn green. • -70 dBm < signal strength: All the three LEDs turn green.

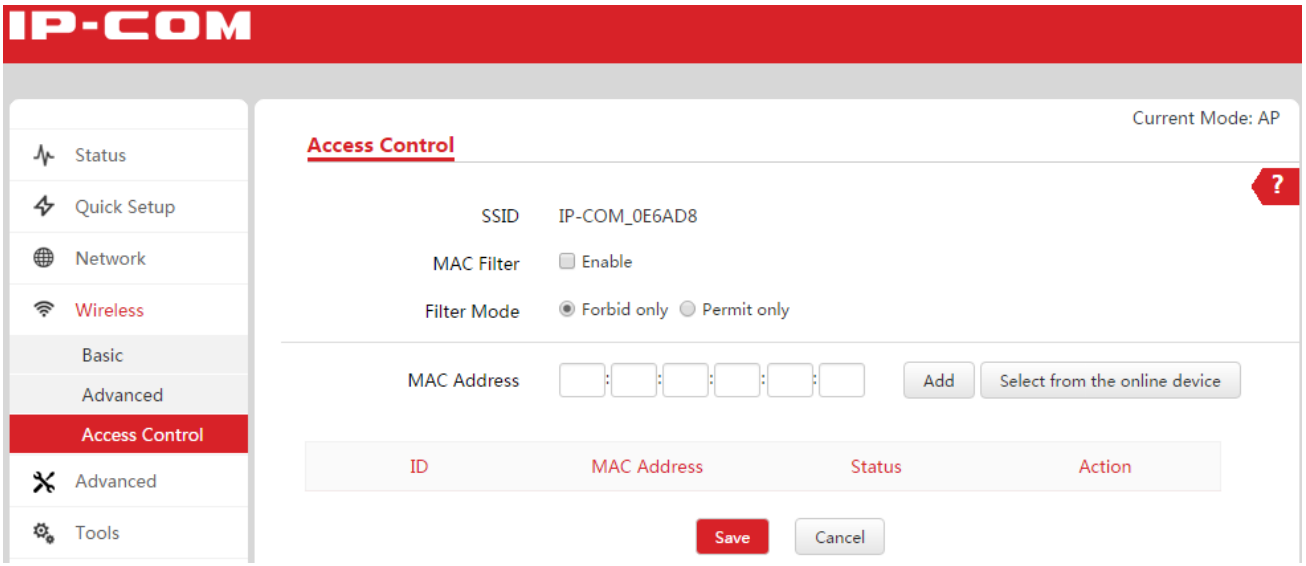
Configure advanced wireless parameters

1. Log in to the device's web UI.
2. Go to **Wireless > Advanced**.
3. Set up advanced wireless parameters.

   We recommend that you keep the default value if you are not familiar with these parameters.
4. Click **Save** to make these settings take effect.

4.4.3 Access control

On this page, you can set up rules to forbid or permit specified wireless clients to access this device. The rules are based on MAC address.



Parameter descriptions

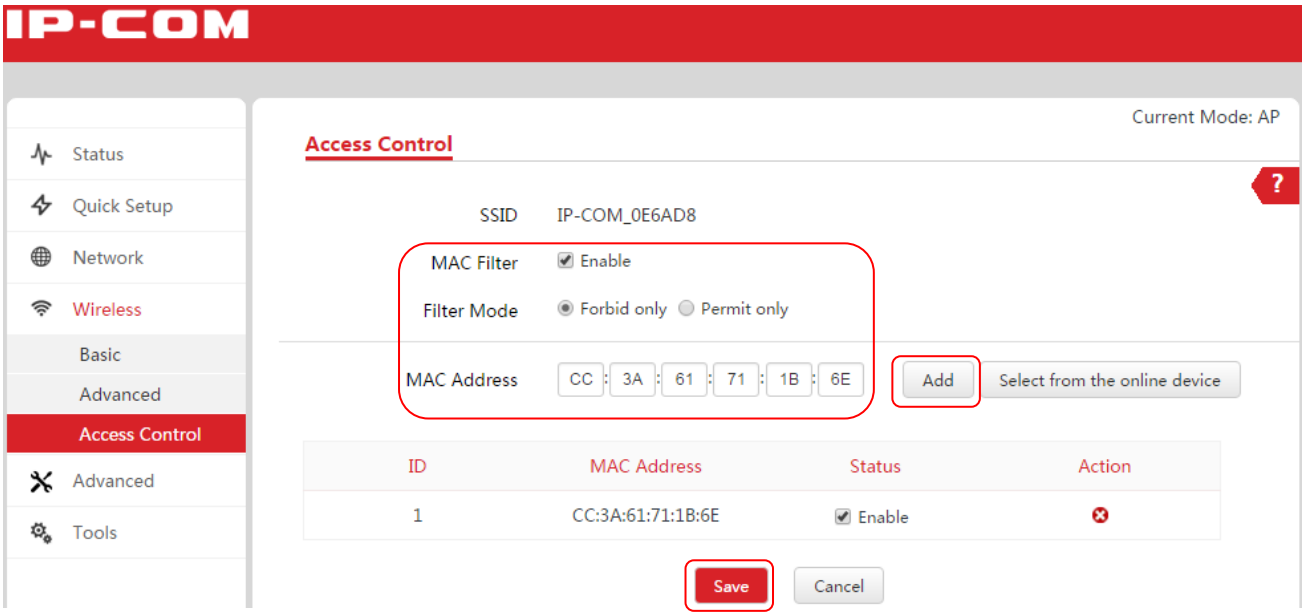
Parameter	Description
MAC Filter	Enable/Disable wireless access control function that is based on MAC address.
Filter Mode	• Forbid only: The device forbids wireless users that correspond to the added MAC addresses to connect to the device. Other users are allowed to connect. • Permit Only: The device permits wireless users that correspond to the added MAC addresses to connect to the device. Other users are not allowed to connect.

MAC address	Manually enter MAC addresses of wireless users that are forbidden or permitted to connect to the device.
Add	To make a MAC address effective to be forbidden or permitted, click this button to add the entered MAC address to the following list.
Select from the online device	If some wireless users have connected to the device, you can click this button to add them into following list.

Configure access control function

➘ When you want to forbid or permit some wireless users that are not connected to the device, do as follows:

1. Log in to the device's web UI.
2. Go to **Wireless > Access Control**.
3. Set up the access control rule.
   1) MAC Filter: Check the box to enable this function.
   2) Filter Mode: Select an option. For example, if you want to forbid certain wireless users to connect to this device, please select *Forbit only*.
   3) MAC Address: Enter a MAC address that is forbidden or permitted to connect, such as CC:3A:61:71:1B:6E.
   4) Click **Add**. The MAC address goes into the following list.
4. Click **Save** to make these settings take effect.



➘ When you want to forbid or permit some wireless users that are connected to the device, do as follows:

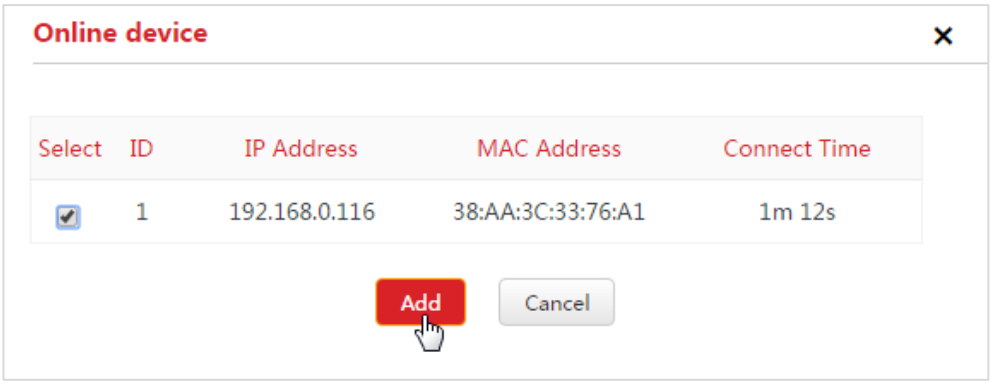
1. Log in to the device's web UI.
2. Go to **Wireless > Access Control**.
3. Set up the access control rule.

1) MAC Filter: Check the box to enable this function.

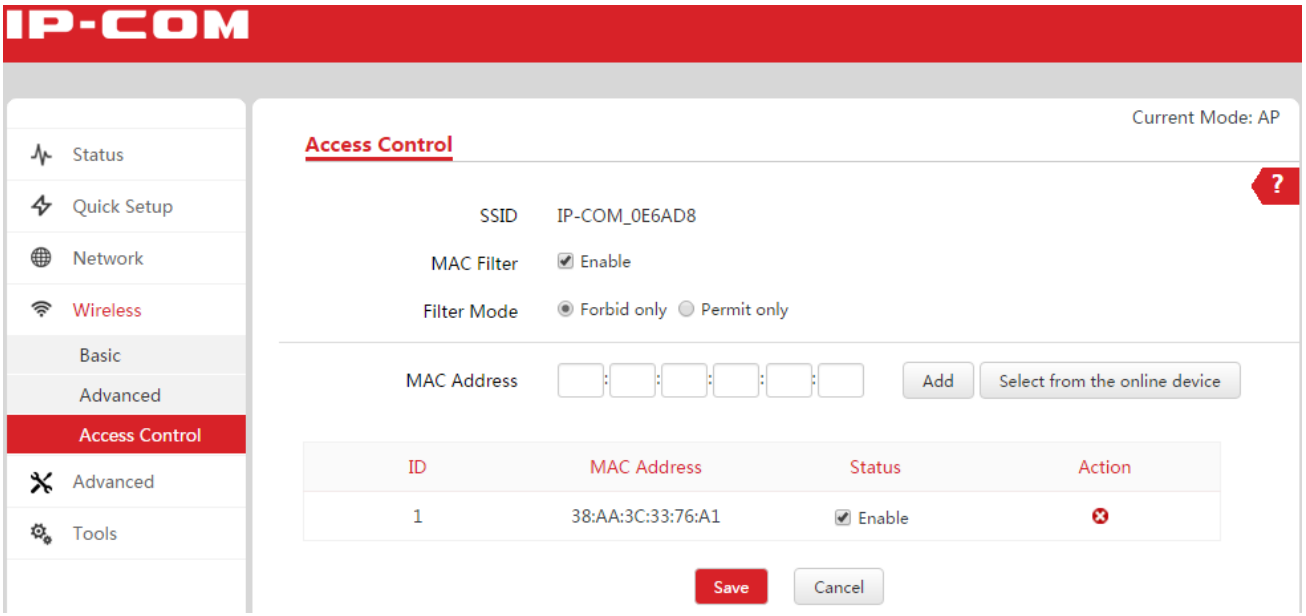
2) Filter Mode: Select an option. For example, if you want to forbid certain wireless users to connect to this device, please select *Forbit only*.

3) MAC Address: Click *Select from the online device*.

4) On the pop-up window, select the client and click **Add**.



4. Click **Save** to make these settings take effect.



↘ If you want to delete a wireless user from the access control rule, you can click ⊗ and follow on-screen instructions.

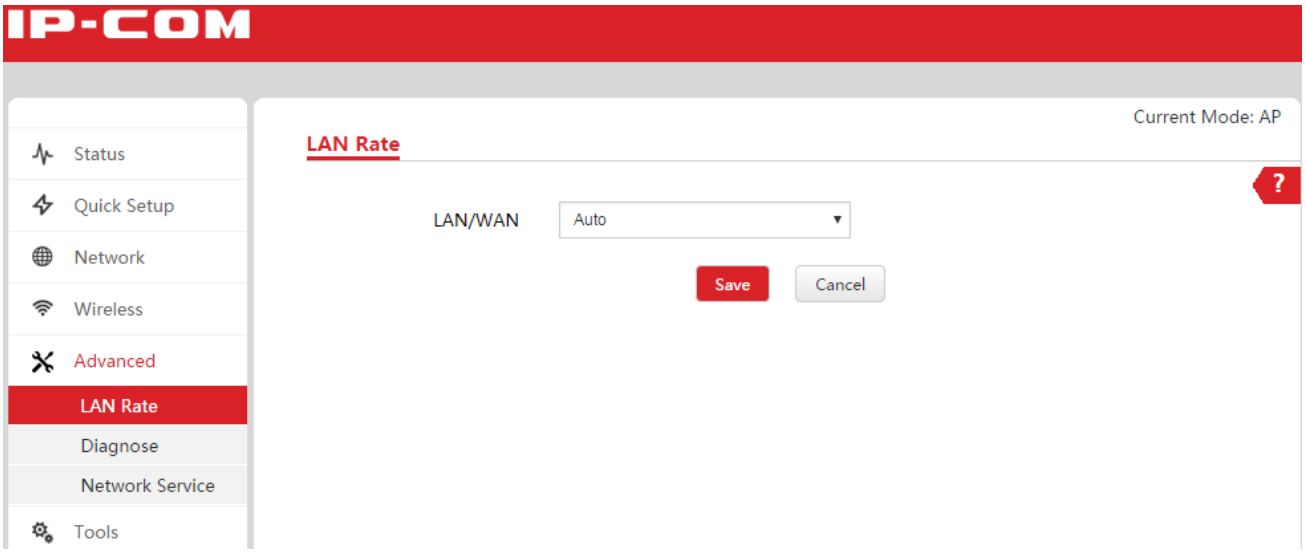
4.5 Advanced Setting

Advanced setting contains the following:

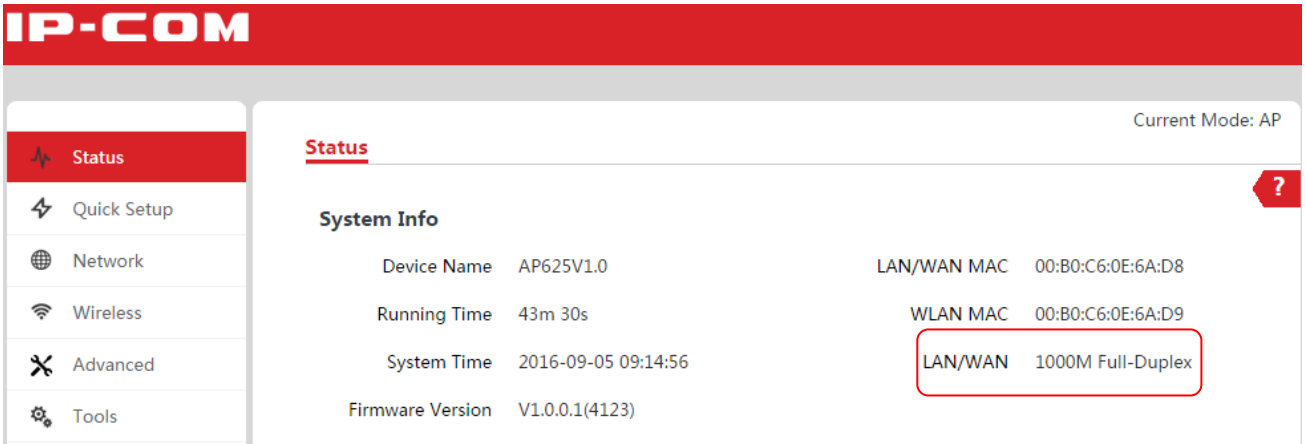
- LAN Rate: On this page, you can select a transmission rate for the *PoE LAN/WAN* port.
- Diagnose: The device provides several diagnose tools to detect the network connection, including scanning signal (site survey), ping and traceroute.
- Network Service: The device provides several network services, including regular reboot, SNMP, UPNP, etc.

4.5.1 LAN Rate

On this page, you can select a transmission rate for the *PoE LAN/WAN* port. Make sure two connected devices have the same rate. We recommend that you keep the default value, *Auto*, if you are not familiar with this parameter.



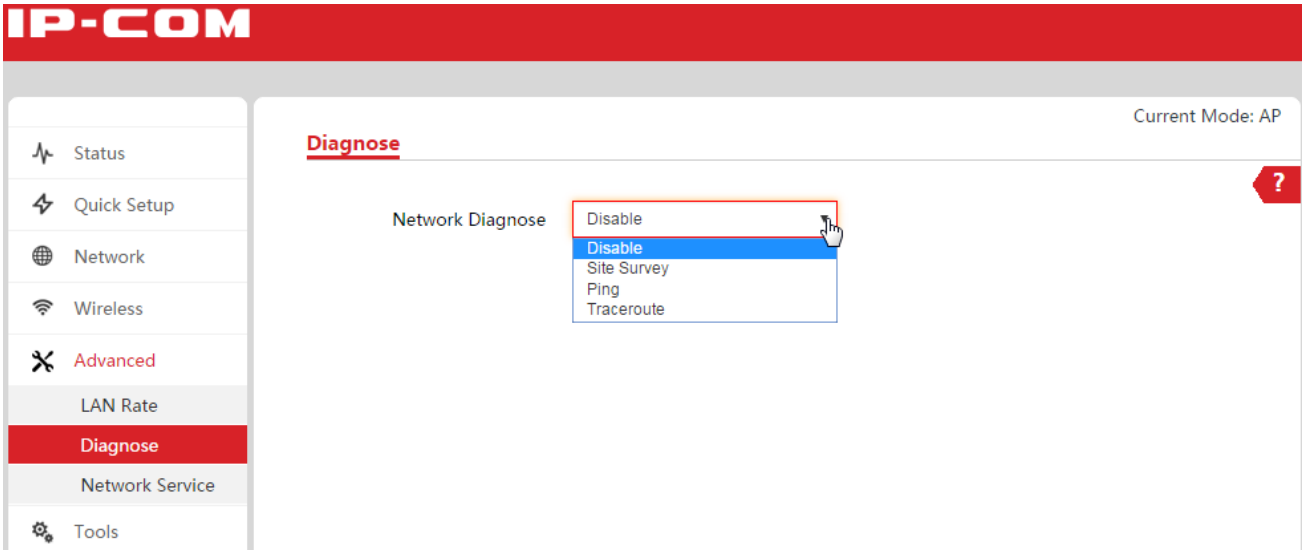
If you want to see the current rate of the *PoE LAN/WAN* port, go to page **Status** and check the *LAN/WAN* status.



4.5.2 Diagnose

The device provides several diagnose tools to detect the network connection, including scanning signal (site survey), ping and traceroute.

- Site Survey: Scanning signal
- Ping
- Traceroute



Site Survey: Scanning signal

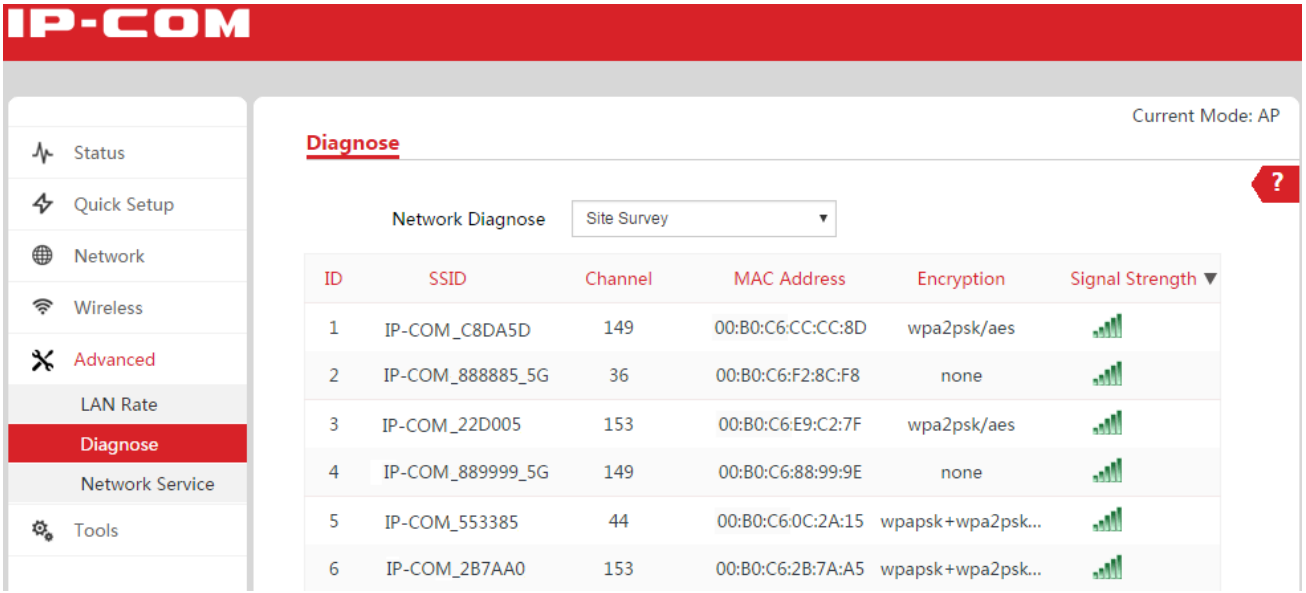
With this function, you can see wireless signals surrounding the area and some of their information.

To start scanning signals:

1. Log in to the device's web UI.
2. Go to **Advanced > Diagnose**.
3. Click the dropdown list and select *Site Survey.*

   Wait a moment and the results will be displayed on the page, as shown in the figure below. Drag the scroll bar to see more wireless signals.

According to the wireless signals, to reduce the channel interference, you can select a channel that is less used surrounding the area for your device.



Ping

Ping is a commonly used diagnosis and troubleshooting command. It can detect whether the device is reachable to a specified IP address or domain name. If it is reachable, the destination IP address returns response packets.

Parameter description:

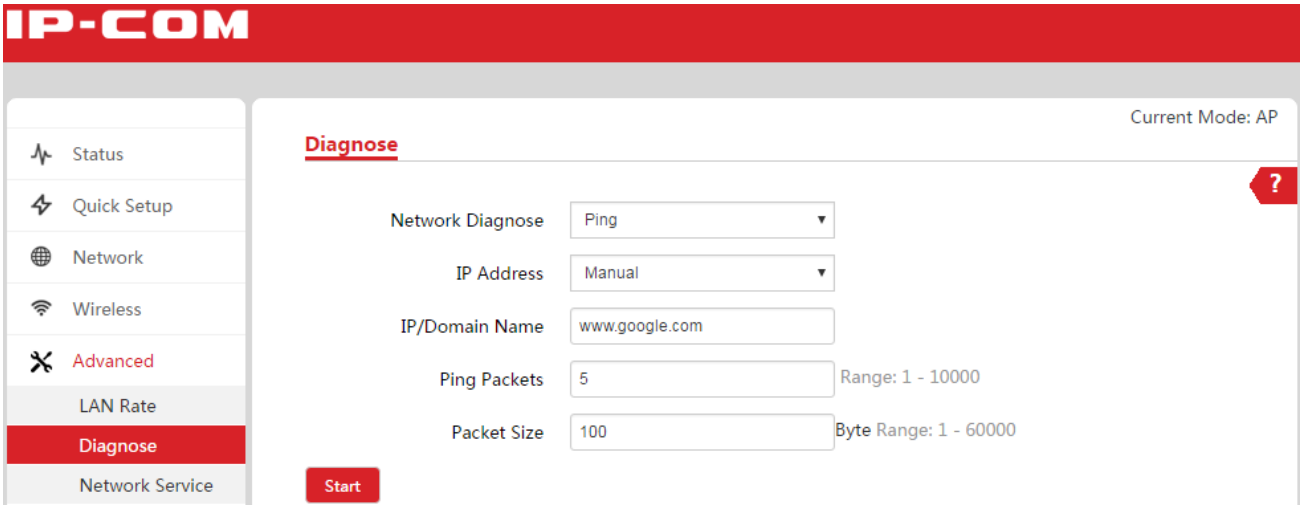
Parameter	Description
IP Address	Select an existed IP address in the drowdown list or select *Manual* to enter an IP address or domain name.
IP/Domain Name	When you select *Manual*, please enter an IP address or domain name to be detected.
Ping Packets	Set up the number of ping packets.
Packet Size	Set up the size of each ping packet.

To check whether an IP or domain name is reachable, do as follows:

1. Log in to the device's web UI.
2. Go to **Advanced > Diagnose**.
3. Set up the parameters.
    1) Click the dropdown list and select *Ping*.
    2) IP Address: Select an existed IP address in the drowdown list or select *Manual*.
    3) IP/Domain Name: When you select *Manual*, please enter an IP address or domain name to be detected, such as *www.google.com*.
    4) Ping Packets: Set up the number of ping packets.
    5) Packet Size: Set up the size of each ping packet.

4. Click **Start.**

Wait a moment and the results will be displayed on the page.



Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.

To detect a path from the device to *google*, do as follows:

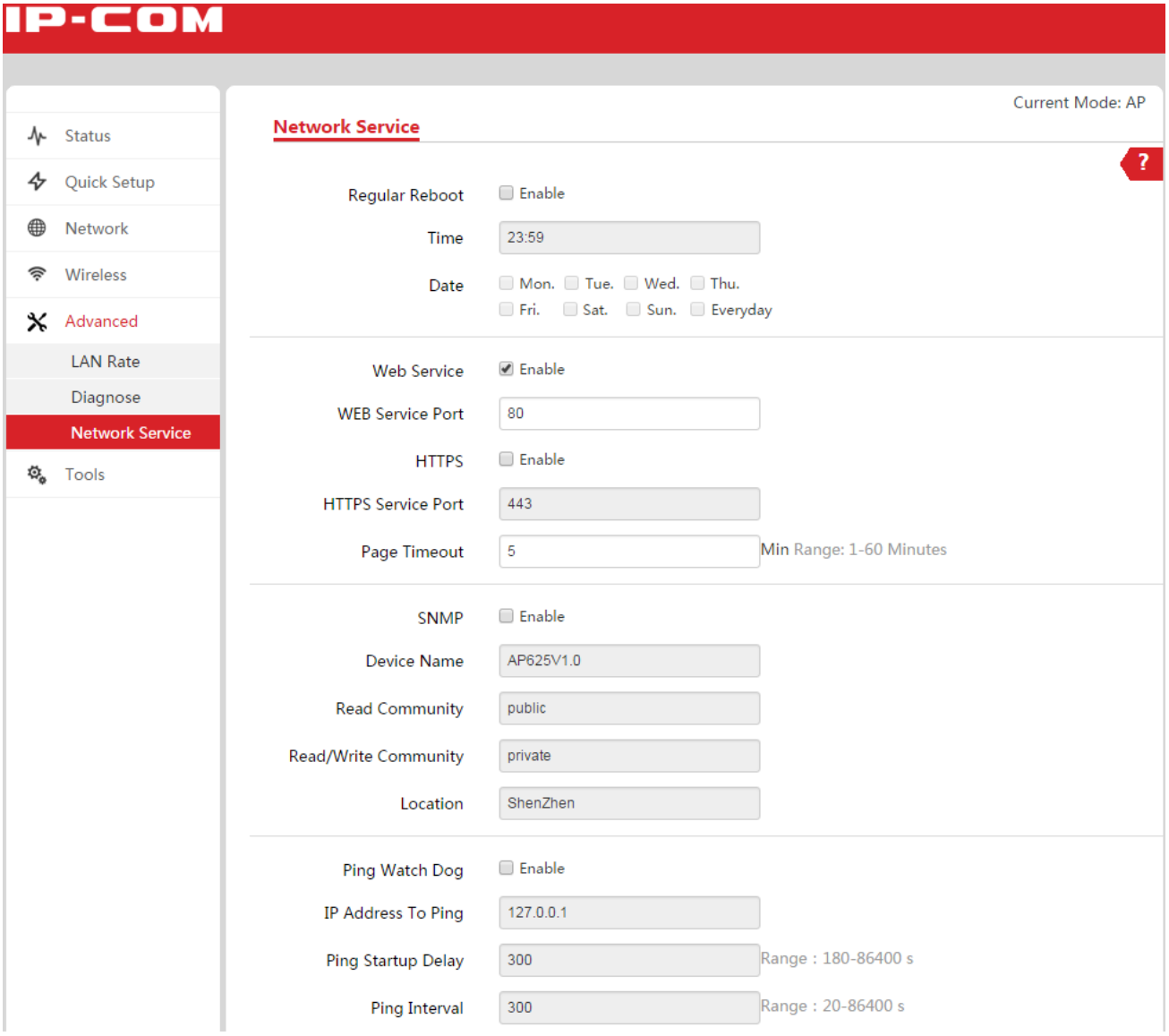
1. Log in to the device's web UI.
2. Go to **Advanced > Diagnose**.
3. Set up the parameters.
    1) Click the dropdown list and select *Traceroute*.
    2) Destination IP/Domain Name: Enter an IP address or domain name to be detected, such as *www.google.com*.
4. Click **Start**.

Wait a moment and the results will be displayed on the page.

4.5.3 Network Service

The device provides several network services, including regular reboot, SNMP, UPNP, etc.

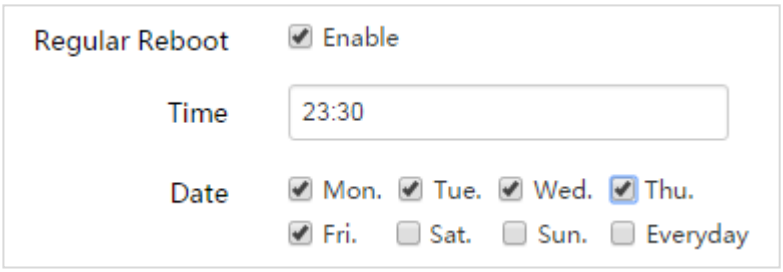
- Regular Reboot
- Web Service
- SNMP
- Ping Watch Dog
- UPNP



Regular Reboot

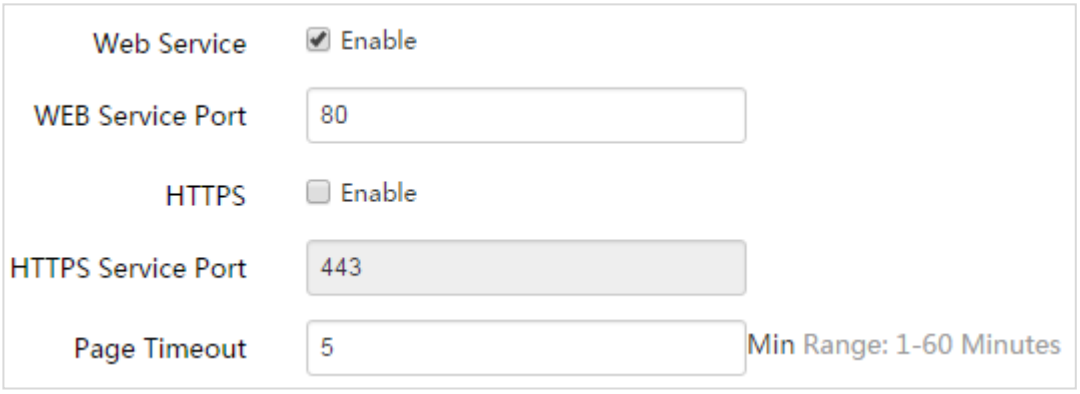
An AP can be set to automatically reboot periodically at a specified point in time so that the administrator can flexibly select a point in time for AP reboot according to the busy degree of the network.

To enable an AP to automatically reboot at 23:30 on Monday to Friday, perform configurations as follows:



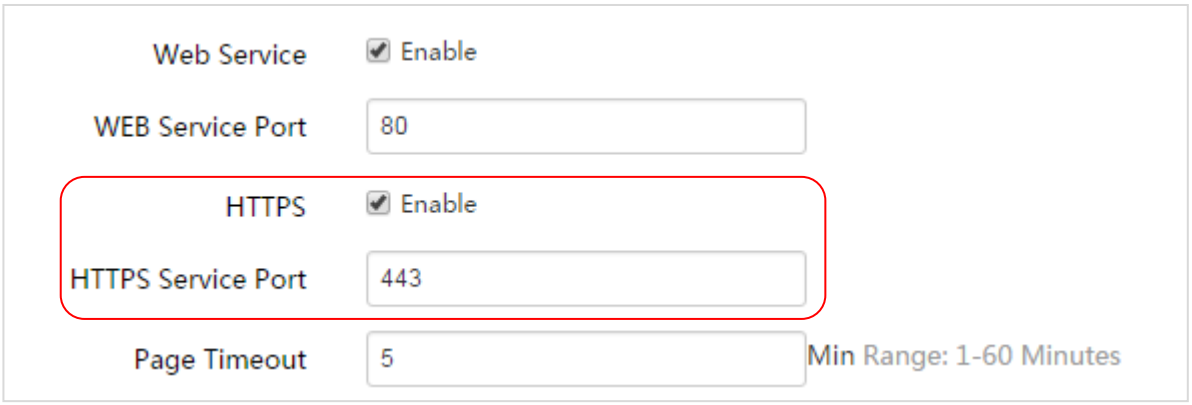
Web Service

The AP Web page access mode and page timeout time can be set through Web Service. This AP supports HTTP and HTTPS access.By default, HTTP access is enabled. We recommend that you the default Web port number in the absence of exceptional circumstances.



Steps for Enabling HTTPS Access:

In the HTTPS service option, click the **Enable** checkbox and then **Save** at the bottom of the page to enable the HTTPS function.



After finishing settings, you can access the Web page in the form of "https://LAN IP:port number" (in this example, https://192.168.2.1:443).

SNMP

This AP supports the SNMP agent function. SNMP management software can be used to manage the AP.

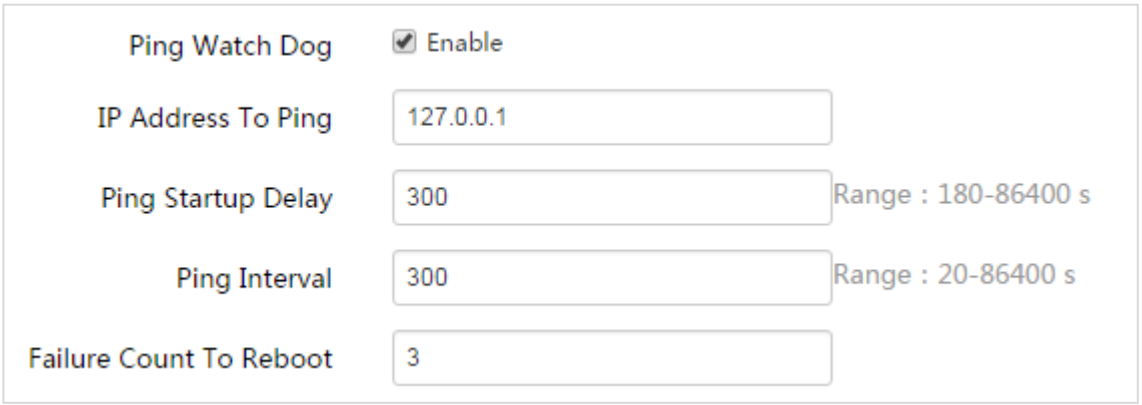
By default, the AP disables the SNMP agent function. If you want to enable SNMP agent, check the **Enable** checkbox to enable SNMP and then click **Save** at the bottom of the page.

Parameter description:

Parameter	Description
SNMP	Enable/Disable the AP SNMP agent function. The default is Disable.
Device Name	AP device name. The default is AP625V1.0.
Read Community	Select a read operation password between SNMP management software and SNMP agent. The default is public. This SNMP agent allows SNMP management software to perform the read operation on variables in AP MIB using Read Community.
Read/Write Community	Select a read and write operation command between SNMP management software and SNMP agent. The default is private. This SNMP agent allows SNMP management software to perform the read and write operation on variables in AP MIB using Read/Write Community.
Location	AP installation location. The default is ShenZhen.

Ping Watch Dog

The Ping Watch Dog function is a function that the AP detects network connectivity. After ping packets are sent periodically to a destination IP address, if a reply is normally received, it indicates that the network is unobstructed. If no response is obtained within Maximum Discard Packets, the AP will automatically reboot. After reboot, it will continue to detect until the network is restored to normal.

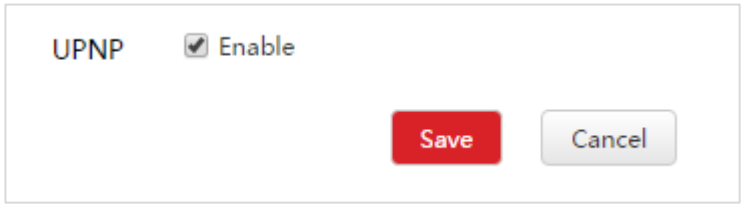


Parameter description:

Parameter	Description
Ping Watch Dog	Enable/Disable the Ping Watch Dog function. After the function is enabled, ping packets are sent periodically to detect network connectivity between this device and a destination IP address, judging whether the link fails. If yes, the AP will automatically reboot to ensure that the network is in good condition.
IP Address To Ping	A destination IP address to which the AP sends Ping packets, i.e. a host IP address whose connectivity to the AP will be detected.
Ping Startup Delay	Delay time from AP startup to enabling the Ping Watch Dog function. This can avoid triggering the Ping Watch Dog function in the system startup process, causing the AP to be continuously restarted so that the user cannot log in to the management interface to modify configurations.
Ping Interval	A time interval at which the AP sends Ping packets.
Failure Count to Reboot	Once the failed ping packets of the AP reach this value, the AP will reboot. The range is 1-65,535. The default is 3. For example, Failure Count to Reboot is N. When the AP continuously sends N Ping packets to a destination IP address and no reply is received, the AP will automatically reboot.

UPNP

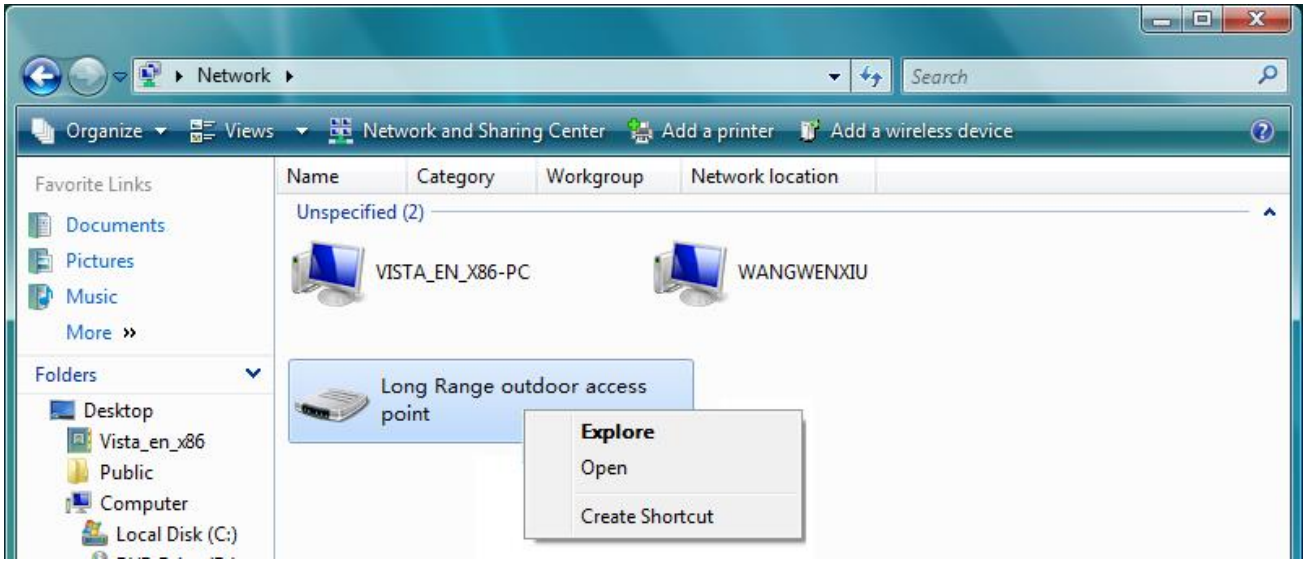
UPNP is shor for Universal Plug and Play. After UPNP is enabled, interworking between devices can be performed via the UPNP protocol. For example, you can view AP information through the AP icon or log in to the AP management page on the client that supports UPNP. This function is valid only in router mode.



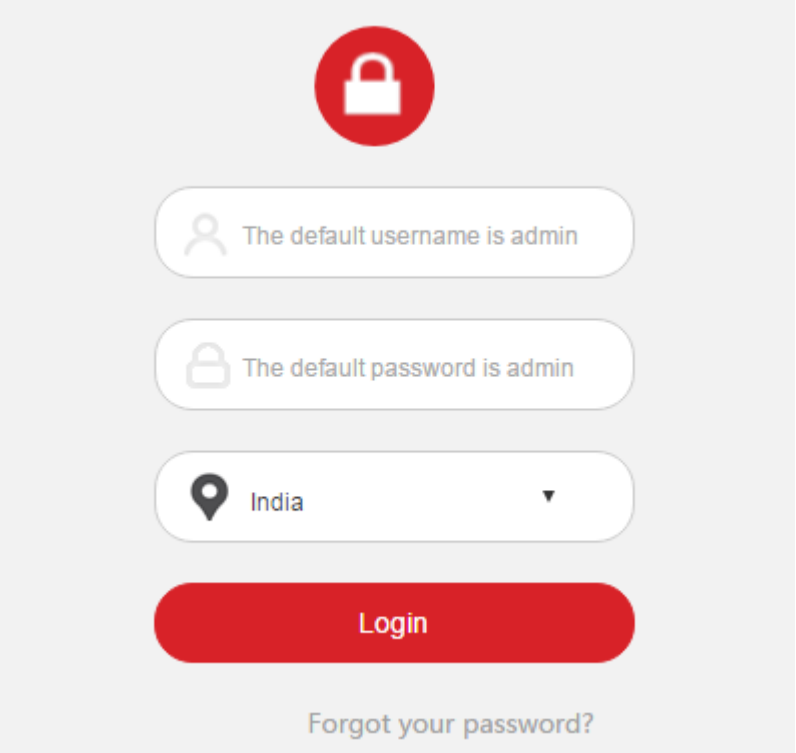
The steps to log in to the AP management page are as follows (take Windows 7 as an example):

1. Double-click the network icon.

2. Right-click the AP description icon and select **Explore**.



The system will go to the AP login page. Enter a user name and password to log in to the AP management page.



4.6 Tools

System tools contain the following contents:

- Date & Time: Set AP system time.
- Maintenance: AP maintenance operations including Reboot Device, Reset to Factory Defaults, Upgrade Firmware, and Backup/Restore.
- Administrator: Modify an Administrator's and visitor's user name and password to prevent any unauthorized users from entering the management page.
- System Log: View AP system logs.

4.6.1 Date & Time

Calibrate AP system time to ensure that time for functions such as logs and timed reboot is executed correctly. Click System Tools to enter the Date & Time configuration page. You can set AP system time by the following methods.

- Synchronize system time with the internet
- Manually set up system time

Note

Time information will be lost after power failure of the AP. If Synchronized with the Internet is enabled, after the AP is started and connected to the Internet, it will resynchronize correct time from the Internet. Time to execute System Log and Reboot Device is correct only after this.

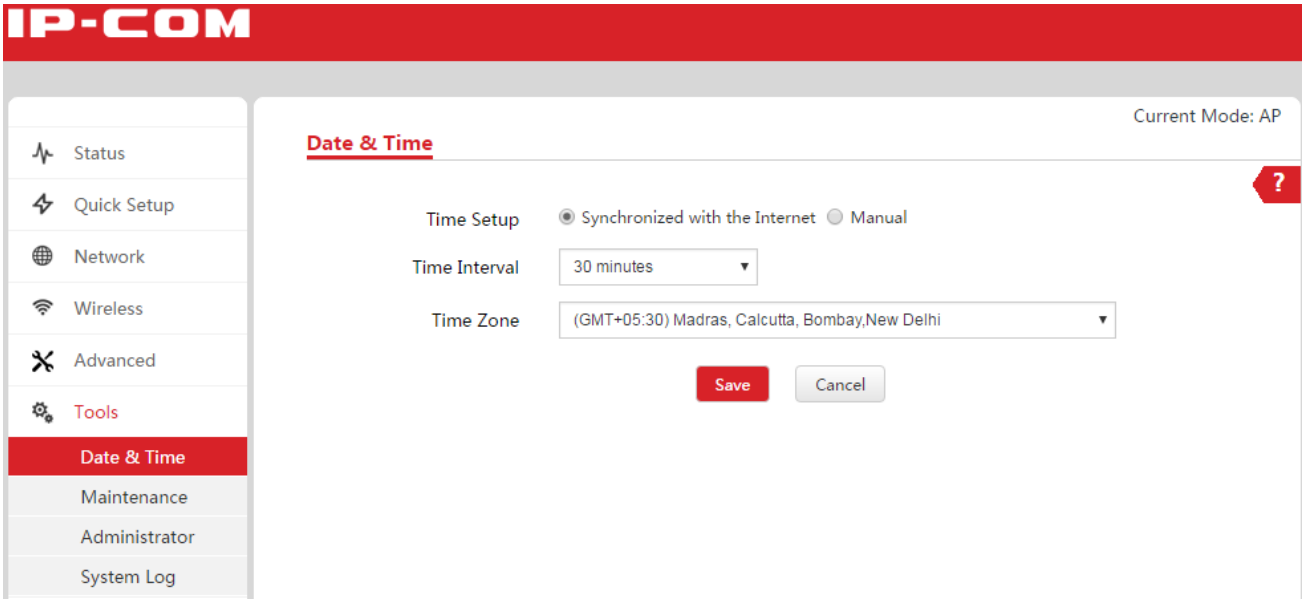
Synchronize system time with the internet

The method for getting AP system time is synchronized with the Internet by default. To ensure correct system time, the AP will automatically calibrate its system time towards the time server on the Internet every time slot set in Time Interval.

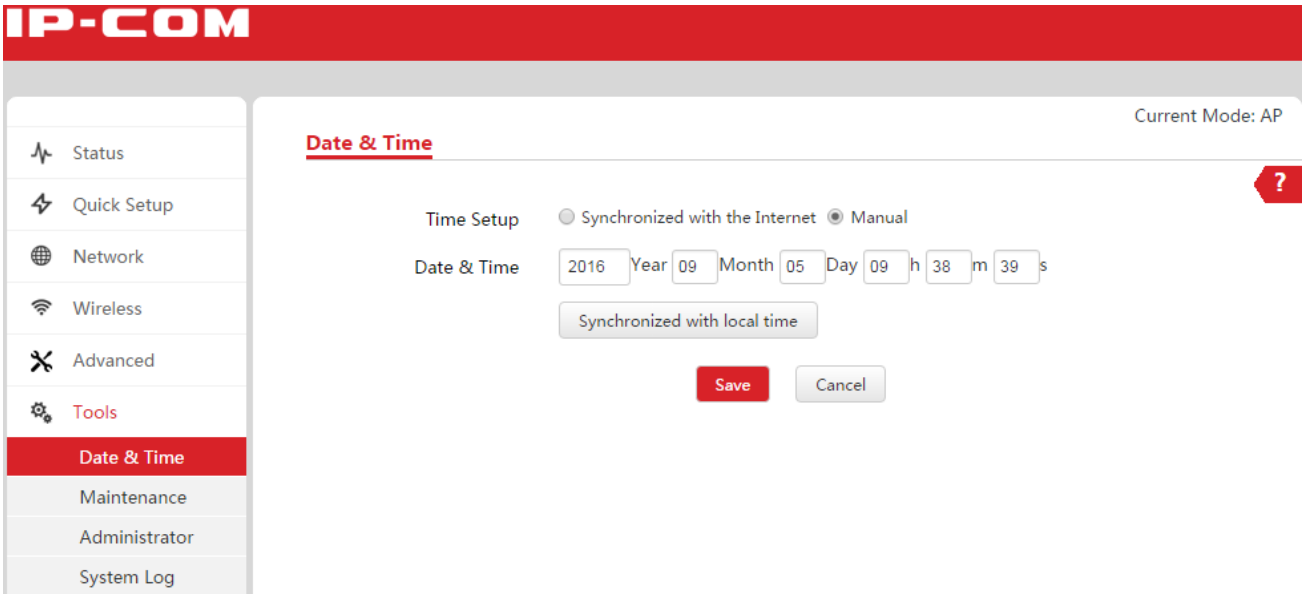
To synchronize system time with the internet:

1. Log in to the device's web UI.
2. Go to **Tools > Date & Time**.
3. Time Setup: Check the *Synchronized with the Internet* checkbox.
4. Select a time interval that is recommended to be 30 minutes.
5. Time Zone: Select a time zone in your region. For example, in China, you can select (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumchi, Taipei.
6. Click **Save** to finish settings.

After the AP is successfully connected to the Internet, the system will get standard GMT time from the Internet.



Manually set up system time



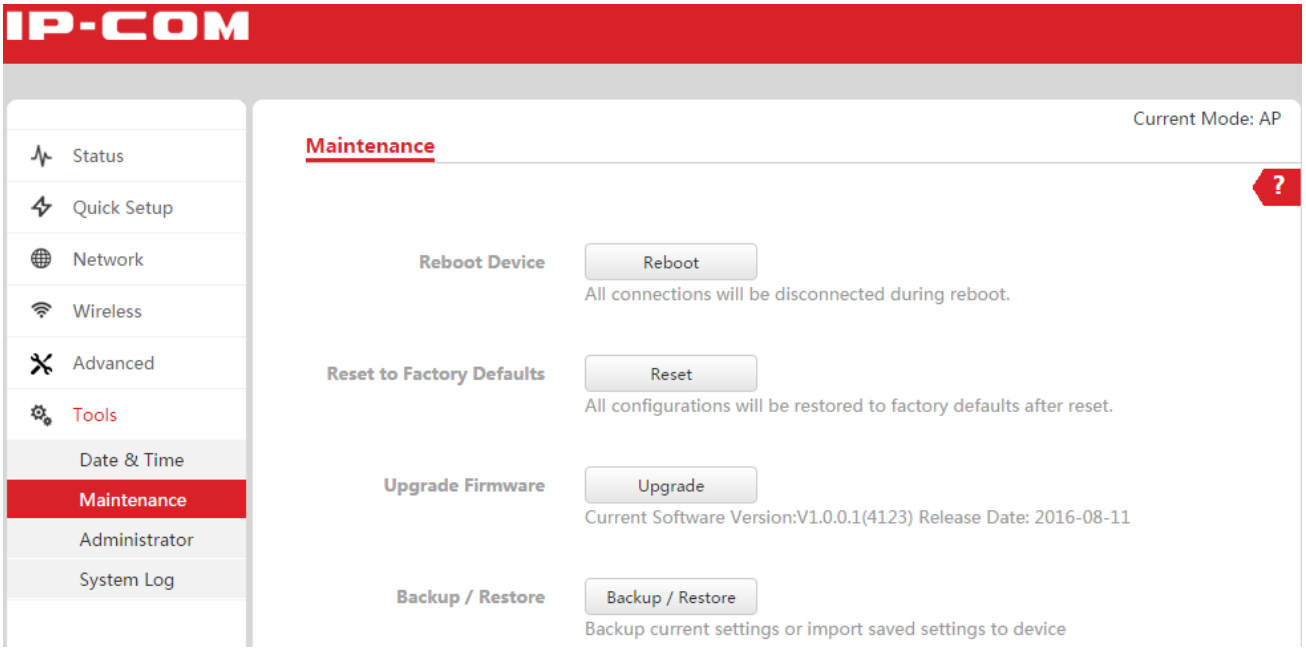
To manually set up system time:

1. Log in to the device's web UI.
2. Go to **Tools > Date & Time**.
3. Time Setup: Check the Manual checkbox.
4. Date & Time: Click Synchronized with local time to synchronize to the AP the time of the current computer that is managing the AP (Ensure that this computer's time is correct).
5. Click **Save** to finish settings.

4.6.2 Maintenance

You can use the following ways to maintain your device:

- Reboot device
- Reset to factory defaults
- Upgrade firmware
- Backup/Restore



Reboot device

All wireless connections will be automatically disconnected during AP reboot. Perform reboot when the network is relatively idle.

Reboot the AP by clicking **Reboot** and performing operations according to the prompt on the page.

Reset to factory defaults

If you encounter a problem in surfing the Internet but cannot find this problem, you are recommended to reset the AP to factory defaults and then reset it.

Note

- Reset to Factory Defaults means that all previous settings will be lost and the AP must be reset.
- Ensure the device power supply is normal in the process of Reset to Factory Defaults.

You can reset the device to factory defaults by the following methods:

Method 1: Click **Reset** and perform operations according to the prompt on the page.

Method 2: In power-up state, open the device protective cover, continuously press and hold the button for 15s and then release it.

Method 3: In power-up state, continuously press and hold the RESET button of the PoE injector with a needle for 15s and then release it.

All configuration data of the AP will be cleared after it is reset to factory defaults. Basic default parameters are as follows:

- Default login IP address: 192.168.2.1
- Default user name and password: admin

Upgrade firmware

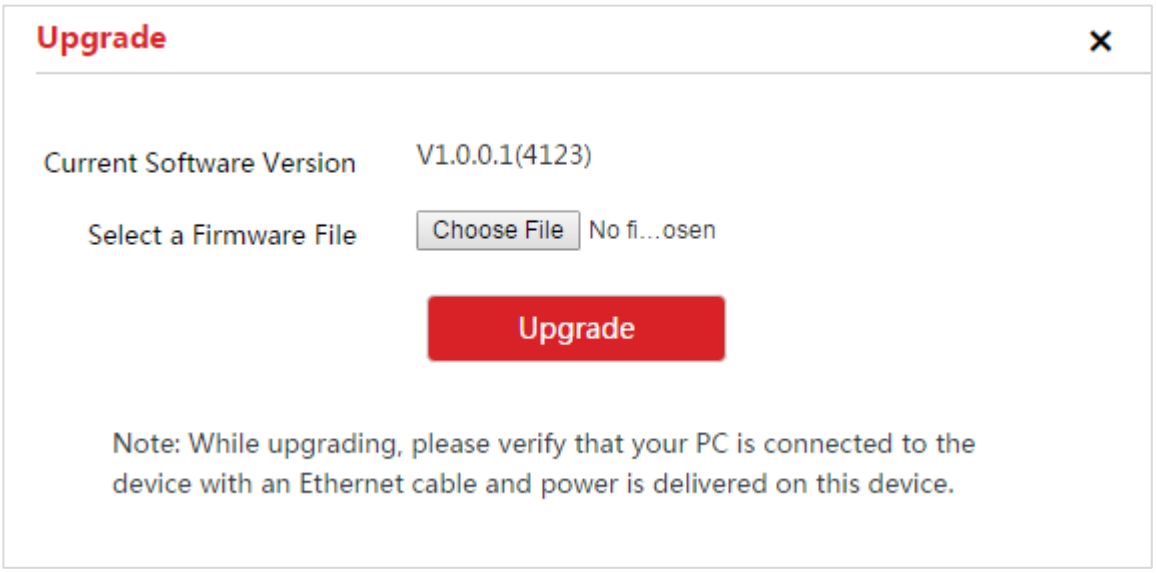
Upgrade firmware may enable the device to obtain a higher firmware version. If the device runs normally, it is not recommended to perform firmware upgrade. If it is really necessary to upgrade firmware, enter the Maintenance page to do so.

To upgrade a firmware for the device:

Note

Do not disconnect the AP power supply during the upgrade process, otherwise it may cause damage to the AP! In case of sudden power failure, re-upgrade firmware. If you cannot enter the management page after sudden power failure, contact the after-sales department.

1. Go to http://www.ip-com.com.cn to download the latest version of the firmware of the device.
2. Decompress the downloaded file using a decompress firmware and place it in a corresponding directory.
3. Log in to the device's web UI.
4. Go to **Tools > Maintenance > Upgrade Firmware**.
5. Click **Upgrade**.
6. In the dialog box that appears, click **Choose File** (different characters may be displayed for different browses) to load the decompressed upgraded firmware.
7. Click **Upgrade** and perform operations according to the prompt on the page.



After the progress bar is over, enter this page to view the displayed Current Software Version, judging that AP firmware is successfully upgraded.

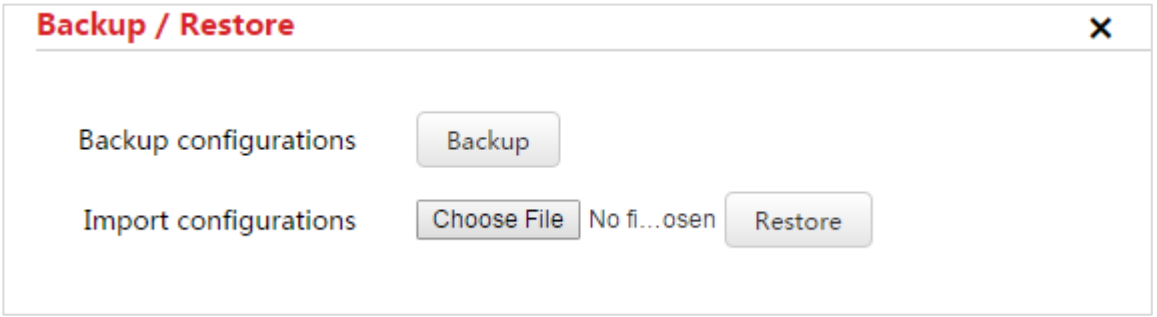
Backup/Restore

After AP settings are finished, the existing AP configuration information can be backed up. The system will export a configuration file after backup. If the device is reset to factory defaults, the previous configurations can be restored by importing the configuration file.

- Backup: Back up the existing AP configuration information.
- Restore: Restore the previous configurations by importing the AP backup file.

To backup configurations:

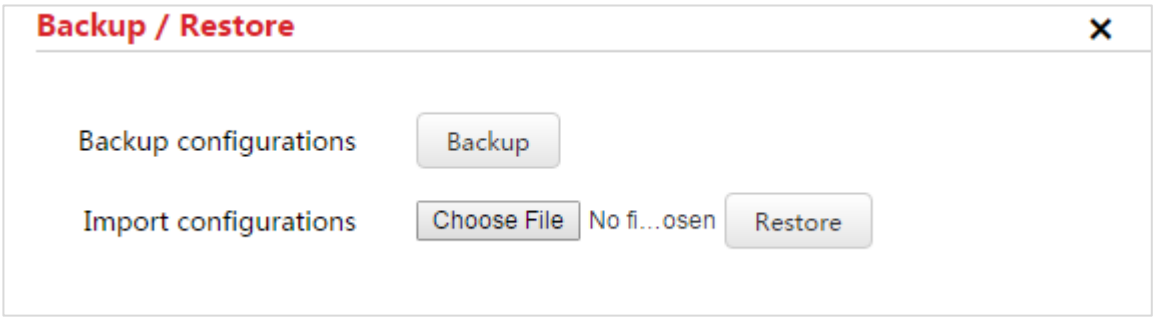
1. Log in to the device's web UI.
2. Go to **Tools > Maintenance > Backup/Restore**.
3. Click **Backup/Restore**.
4. In the dialog box that appears, click **Backup**.
5. Choose a storage path of the backup file by referring to the prompt in the computer.



To restore configurations:

1. Log in to the device's web UI.
2. Go to **Tools > Maintenance > Backup/Restore**.

3. Click **Backup/Restore**.
4. In the dialog box that appears, click **Choose Flie** and choose and load the device backup file.
5. Click **Restore**, and perform operations by referring to the prompt in the computer, and wait until the progress bar is over.



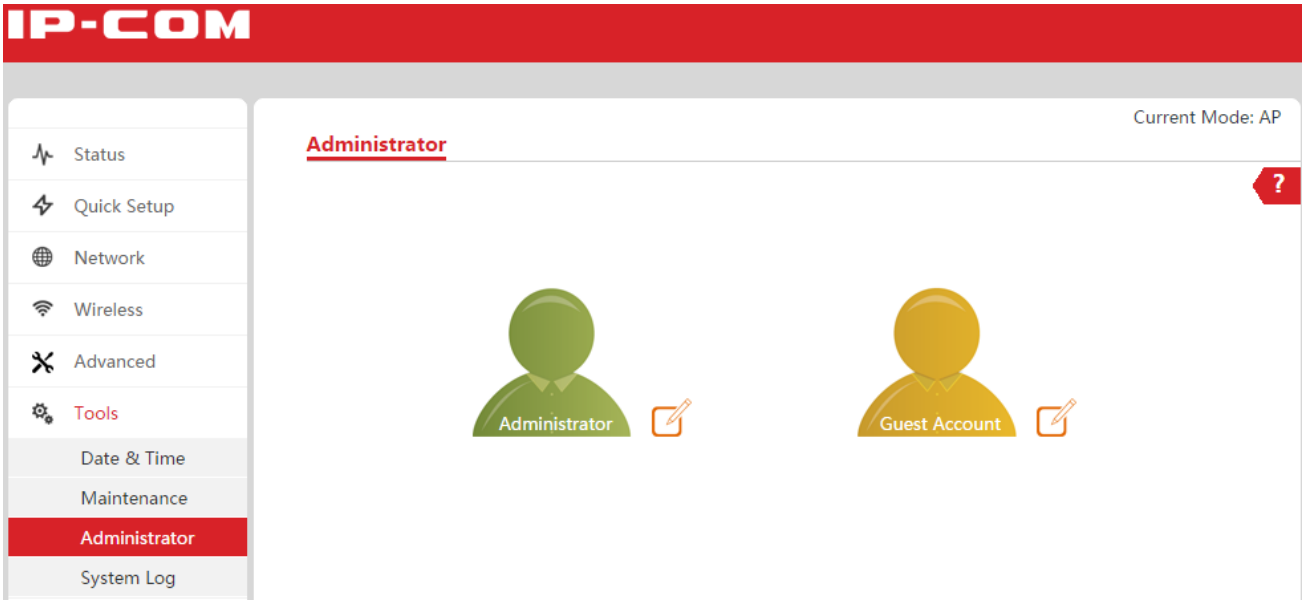
4.6.3 Administrator

To prevent others from using the default login information to enter the AP management page to modify AP configurations, it is strongly recommended to modify the user name and password in the login page.

This AP supports two account types: administrator and guest account.

- Administrator: Have all authorities to manage the AP. Both the user name and password are admin.
- Guest Account: View the AP configuration information only and cannot modify any configurations. Both the user name and password are **user**.

Modify the user name and password by clicking of a corresponding account.

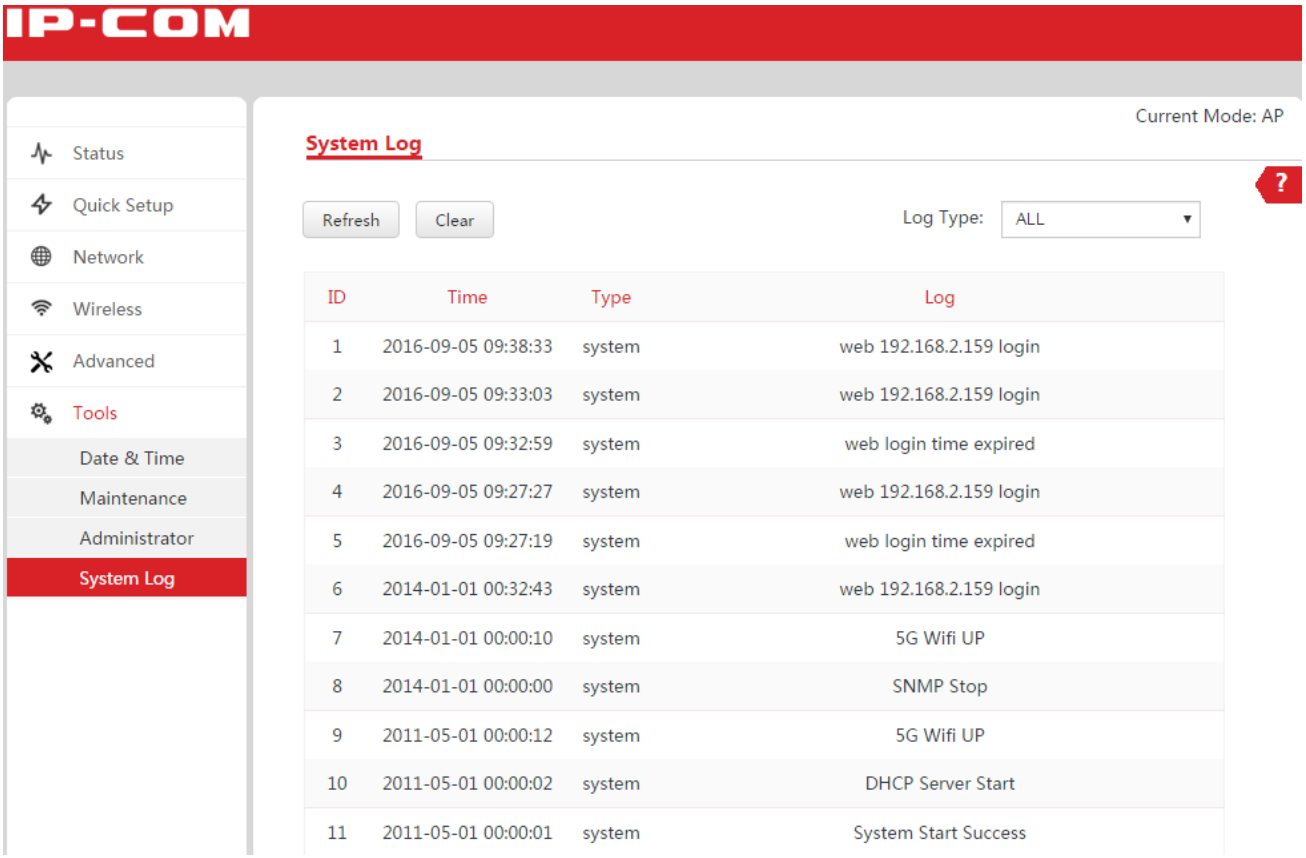


4.6.4 System Log

To view various situations appearing after the startup of the AP system as well as the user's operation records on the AP, click Tools>System Log to enter the configuration page.

To facilitate real-time monitoring on network running and diagnosis on network faults, we recommend that you enter the **Tools** > **Date & Time** page to calibrate AP system time to ensure that log time is correct.

Click **Refresh** to view the latest log information about the AP. Click **Clear** to clear log information displayed on the page. After the device is restarted, previous log information will be lost.



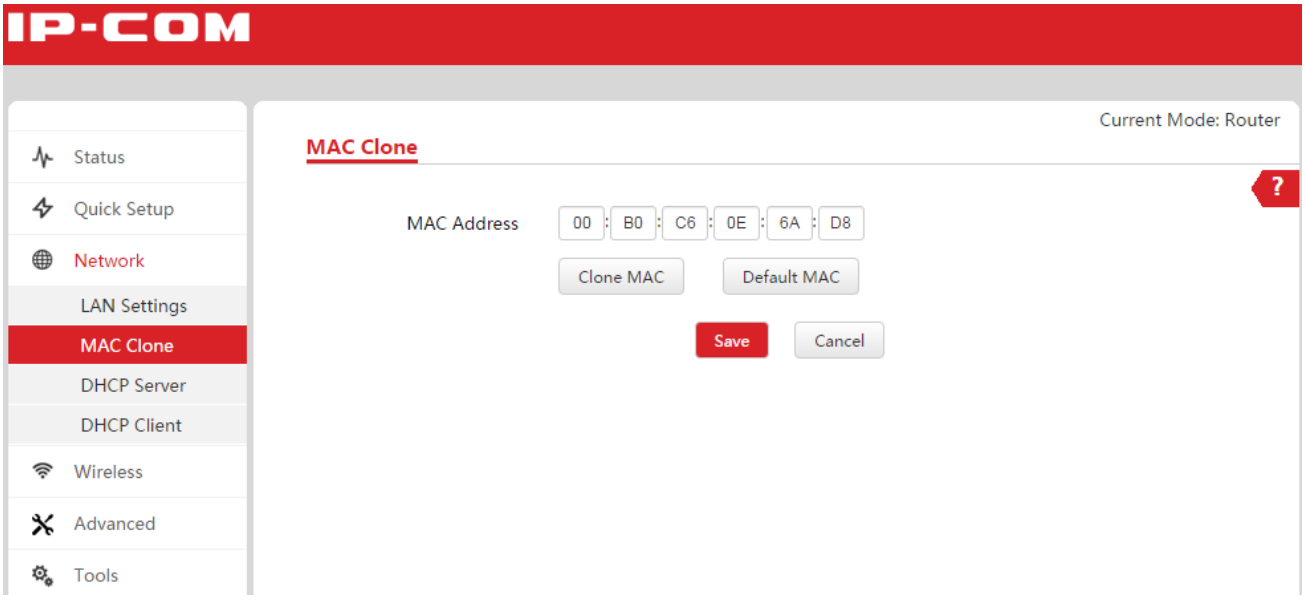
4.7 Other Functions in Router Mode

Other functions in router mode contain the following contents:

- MAC Clone: Modify AP WAN MAC address.
- Traffic Control: Set the user's minimum uploading rate and maximum downloading rate in a specified LAN.
- Port Forwarding: Set port forwarding to enable Internet users to access intranet resources.
- DMZ: Enable a host in the intranet to implement bidirectional unlimited communication with the Internet.
- MAC Filter: Set limitations on a specified client from surfing the Internet.
- DDNS: Establish a mapping relation between a changed WAN IP address of the device and a fixed domain name. You need only to access this domain name during remote access.
- Remote Web Access: Set Internet users' authority to access the device.

4.7.1 MAC Clone

You can try to clone the MAC address if you cannot access the Internet after performing settings on router mode.



Parameter description

Parameter	Description
MAC address	Current AP WAN MAC address. Manually enter a correct MAC address and click **Save**.
Clone MAC	Clone to the AP WAN the MAC address of the current computer managing the AP.
Default MAC	Set the AP WAN MAC address to the default.

Configure MAC clone function

Tip

Please use a correct MAC address to perform the clone operation! A correct MAC address is a MAC address of a computer on which a technician performs commissioning to surf the Internet during broadband installation.

To Configure MAC clone function:

1. Log in to the device's web UI.
2. Go to **Network > MAC Clone**.

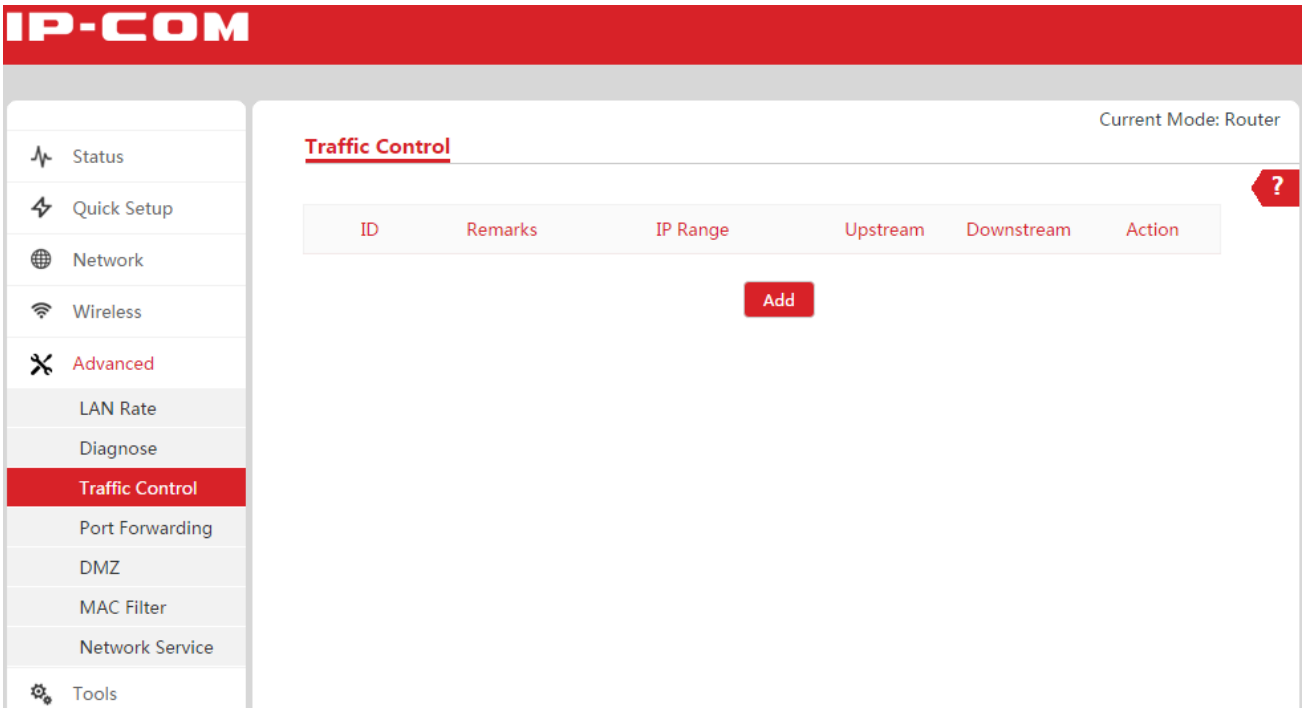
3. Click **Clone MAC** to copy the MAC address of the current management computer to the current MAC address bar.
4. Click **Save** to finish settings.s

4.7.2 Traffic Control

Traffic Control enables you to set bandwidth control on a LAN IP address according to actual need. By setting corresponding restriction rules, traffic control on data transmission is realized so that limited bandwidth resources are reasonably distributed to achieve the objective of effectively utilizing the existing bandwidth.

Tip

1. In the computer network or network operator, broadband rate is generally in bps (or b/s).
2. 1 B = 8 b 1 B/s = 8 b/s (or 1 Bps = 8 bps) 1 KB = 1,024 B 1 KB/s = 1,024 B/s 1 MB = 1,024 KB 1 MB/s = 1,024 KB/s



Parameter description

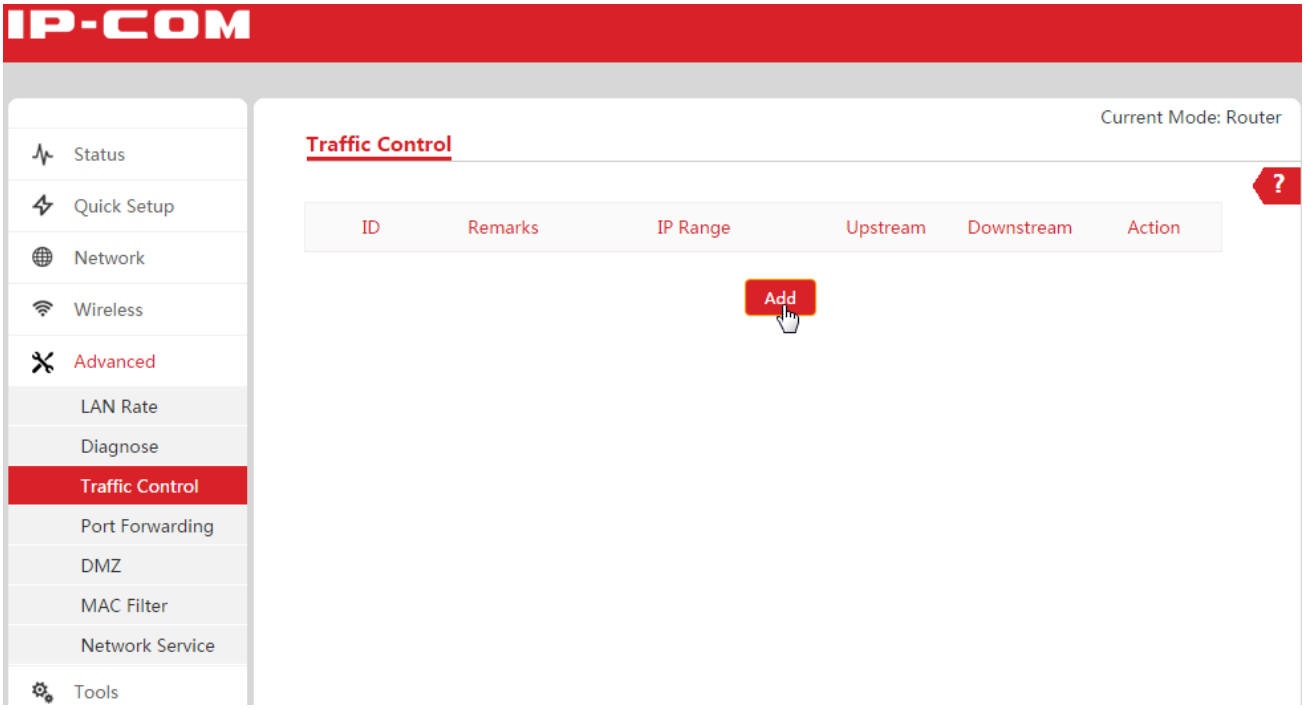
Parameter	Description
Remarks	Information about remarks of the rule.
IP Range	IP address range of clients where the rule is effective.
Upstream	Minimum upstream rate of clients in the rule in KB/s and MB/s.
Downstream	Maximum downstream rate of clients in the rule in KB/s and MB/s.
Operation	Click to delete a corresponding rule.

Application scenario

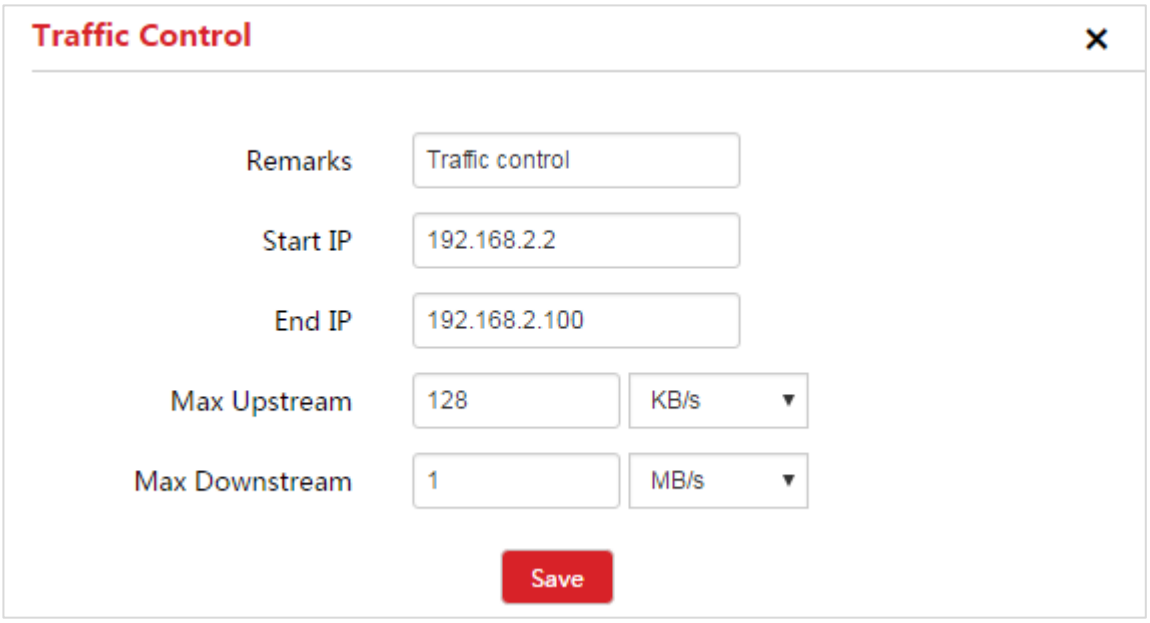
Assume that you want to restrict the network speed of clients with an IP address range of 192.168.2.2 to 192.168.2.100 in the LAN. The minimum upstream rate is 128 KB/s. The maximum downstream rate is 8 Mbps, i.e. 1 MB/s.

Configure traffic control

1. Log in to the device's web UI.
2. Go to **Advanced > Traffic Control**.
3. Click **Add.**

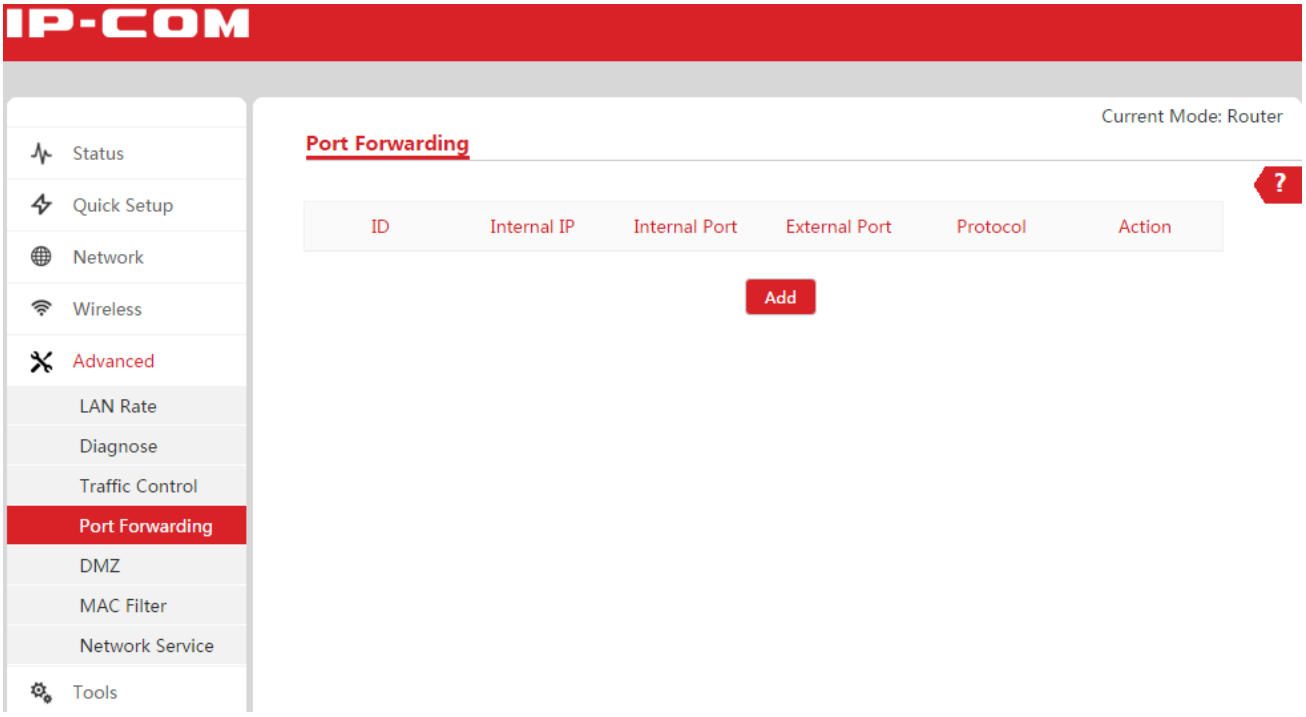


4. On the pop-up window, set up the parameters.
   1) Remarks: Set information about remarks of this rule.
   2) Start/End Address: Enter IP addresses where traffic control must be set (including an address field or a single address) (in this example, 192.168.2.2 to 192.168.2.100).
   3) Minimum Upstream Rate: Set a minimum value that restricts the client's uploading rate.
   4) Maximum Downstream Rate: Set a maximum value that restricts the client's downloading rate.
5. Click **Save** to make these settings take effect.



4.7.3 Port Forwarding

By default, a WAN host cannot actively access a LAN host. Port Forwarding enables WAN users to access a LAN host and protects the interior of the LAN against invasion. Port Forwarding defines a service port and specifies its corresponding LAN server using an IP address. The device locates to this server any service request on this port from the WAN.



Parameter description

Parameter	Description
Internal IP	IP address of intranet server.
Internal Port	Service port of intranet server. During settings, automatic filling is performed after Public Service is selected.
External Port	Port that is open to the user to access. During settings, automatic filling is performed after Public Service is selected.
Protocol	Protocol type of a corresponding service. If you are not sure about protocol type of a service during settings, you are recommended to select **TCP/UDP**.
Operation	After successfully setting rules, click to delete corresponding rules.

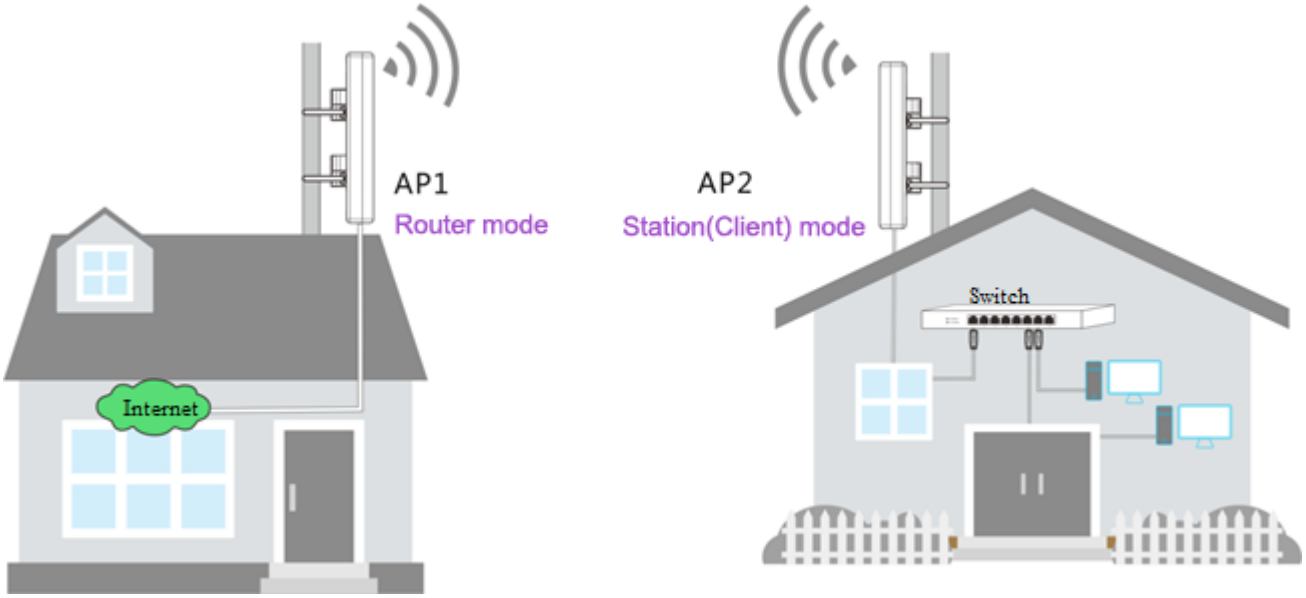
Application scenario

A community uses 06 to perform networking. AP1 works in router mode and is connected to the Internet. AP2 is bridged to AP1 wireless signals in station (client) mode. The AP1 WAN IP address is 202.105.106.55. The network administrator needs to access resources on the intranet computer during business trip. This can be achieved through the port forwarding function. Establish and enable an FTP server on the intranet computer. Store resources to be accessed on the server. Set the port forwarding function on 06.

Assume that basic information about the FTP server is as follows:

IP address	192.168.2.100
User Name and Password	admin
Port	21

The reference topological graph is as follows:

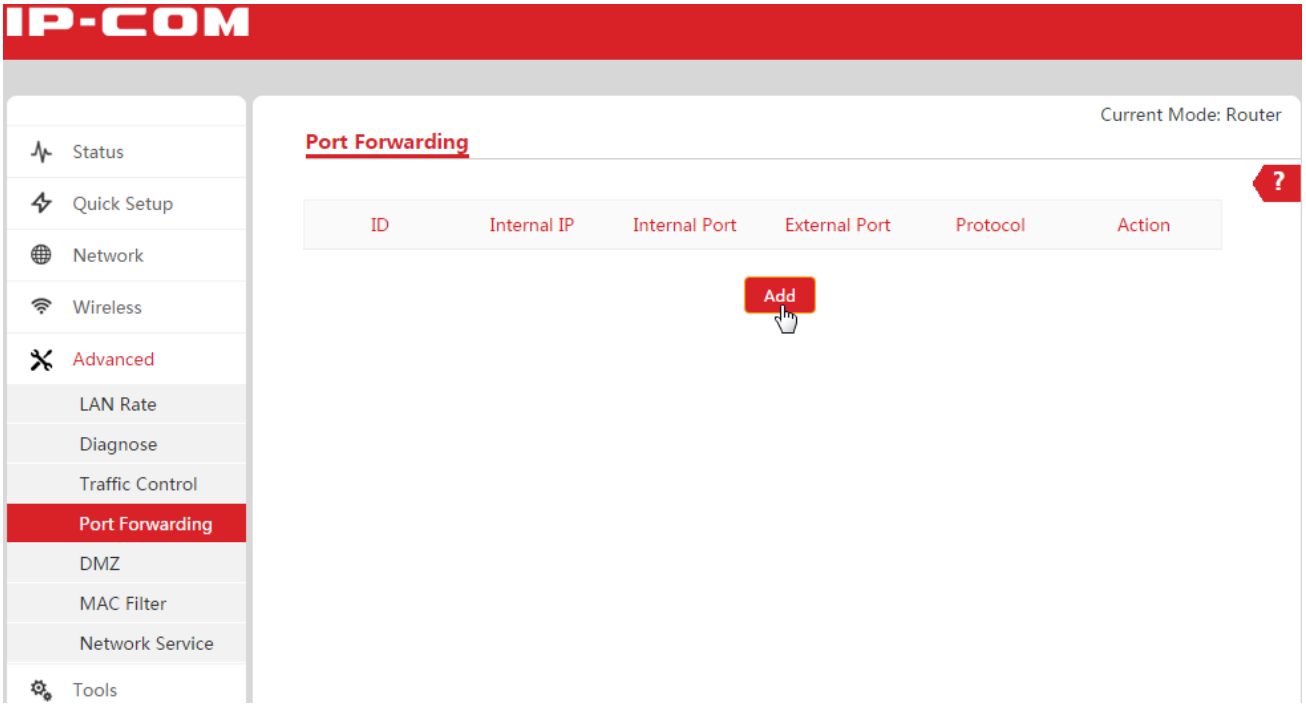


Tip

- Ensure that the AP WAN port has obtained a public network IP address.
- If the AP WAN IP address is dynamically changed, refer to relevant contents of DDNS.
- An intranet computer IP address must be manually configured to avoid service interruption due to automatic change of IP address.
- System firewall, some pieces of antivirus software, and security software may prevent other computers from accessing the server on the computer. You are recommended to disable them temporarily when using this function.

Configure port forwarding

1. Log in to the device's web UI.
2. Go to **Advanced > Port Forwarding**.
3. Click **Add.**

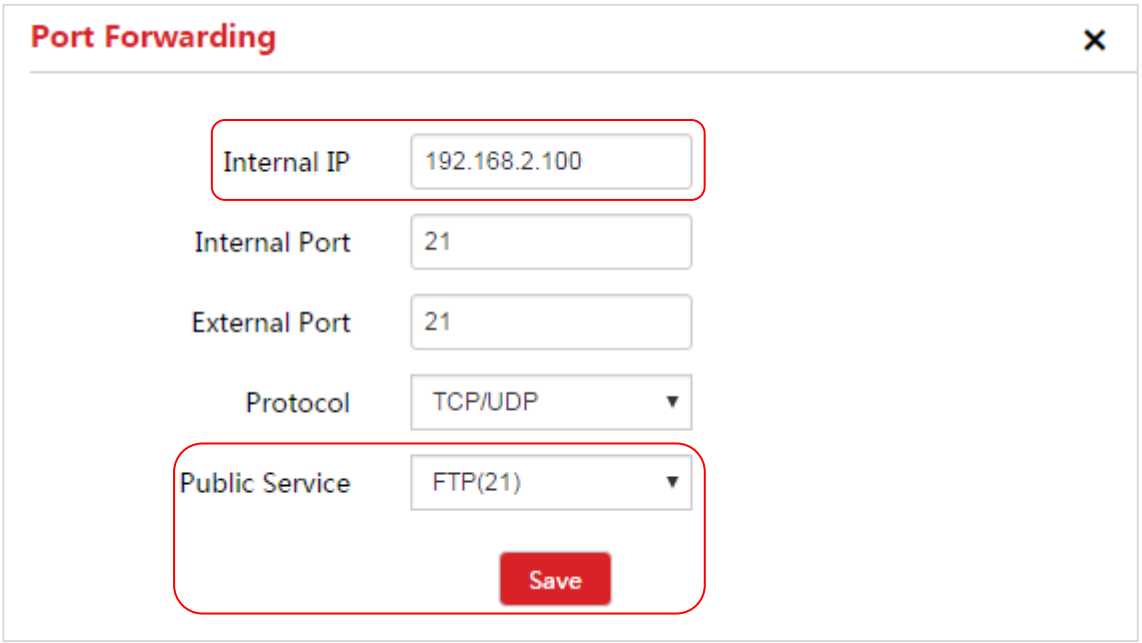


4. In the pop-up window, set up the parameters.

   1) Internal IP: Enter an intranet server IP address, here we enter *192.168.2.100*.

   2) Public Service: Click the dropdown list and select a service enabled in the intranet, here we select *FTP*.

5. Click **Save** to finish settings.



Verify the configuration

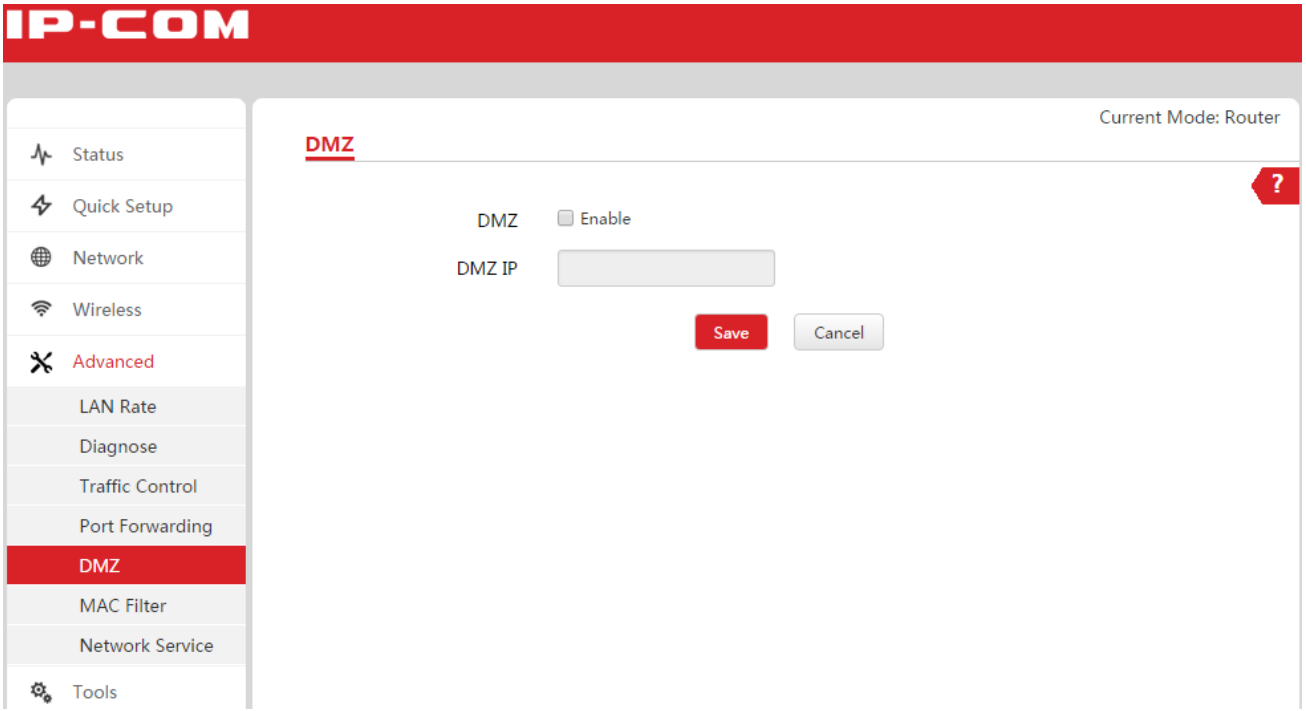
When extranet users access intranet resources, they need to access *ftp://202.105.106.55* on a computer that has obtained a public network IP address.

Note

- External Port of the port forwarding rule shall not be the same as Port number of remote web access, otherwise a conflict will occur so that port forwarding cannot be used.
- After the rule is set, Internet users can access a corresponding server erected in the LAN in the form of "Protocol name://Current WAN IP address: External port".

4.7.4 DMZ

After a LAN computer is set to a DMZ host, this computer is not restricted when it communicates with the Internet. For example, for some video conferences and online games, you can set computers under these applications to DMZ hosts so that the video conferences and online games function more smoothly.

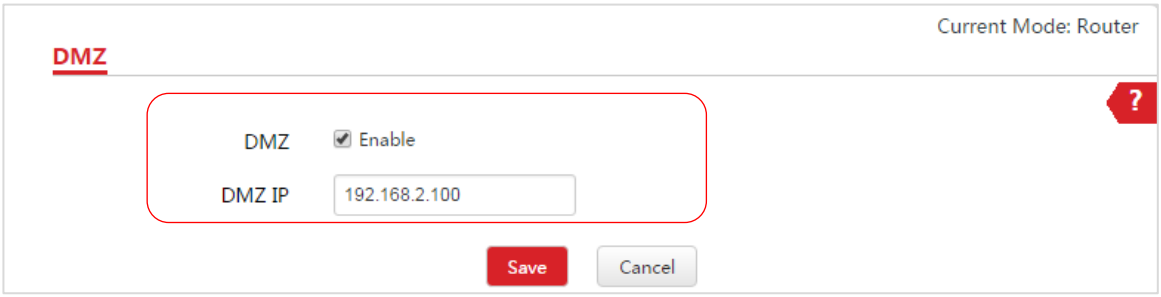


Note

- When a computer is set to a DMZ host, this computer is fully exposed to the extranet and the router firewall does act on this host any more. Hackers may use the DMZ host to attack the local network. Do not use the DMZ host function carelessly.
- It is necessary to set the DMZ host IP address to a static IP address to avoid failure of the DMZ function due to dynamic acquisition.
- Security software, antivirus software, and system firewall may affect the DMZ host function. Disable them temporarily when using this function. When you do not use the DMZ host function, you are recommended to cancel DMZ settings and enable firewall, security software, and antivirus software.

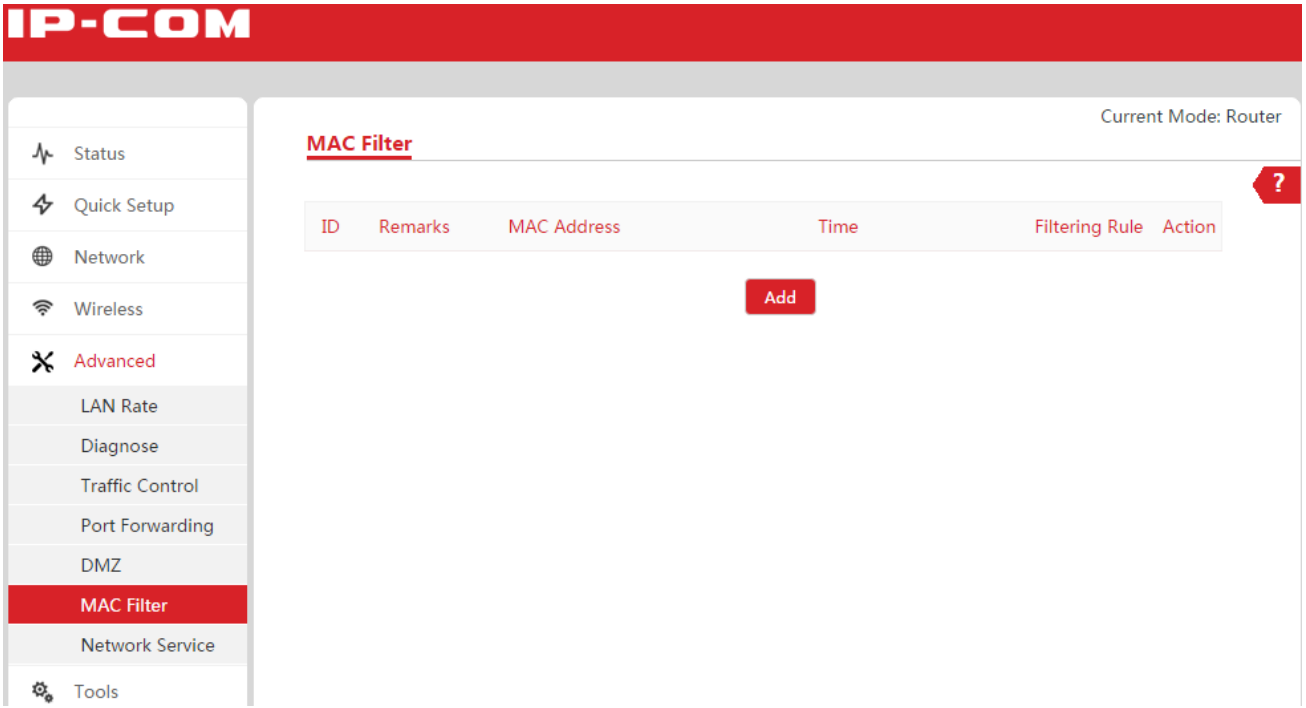
To add a DMZ host:

1. Log in to the device's web UI.
2. Go to **Advanced > DMZ**.
3. Click *Enable* in the DMZ option.
4. In the DMZ IP option, enter an IP address of DMZ host, and then click **Save**.



4.7.5 MAC Filter

Computers, laptops, tablet PCs, and smartphones that people often use have respective MAC addresses. You can control LAN clients' access to the Internet through the MAC Filter function. MAC Filter has two access control modes: Allow_Internet and Forbid_Internet.



Parameter description

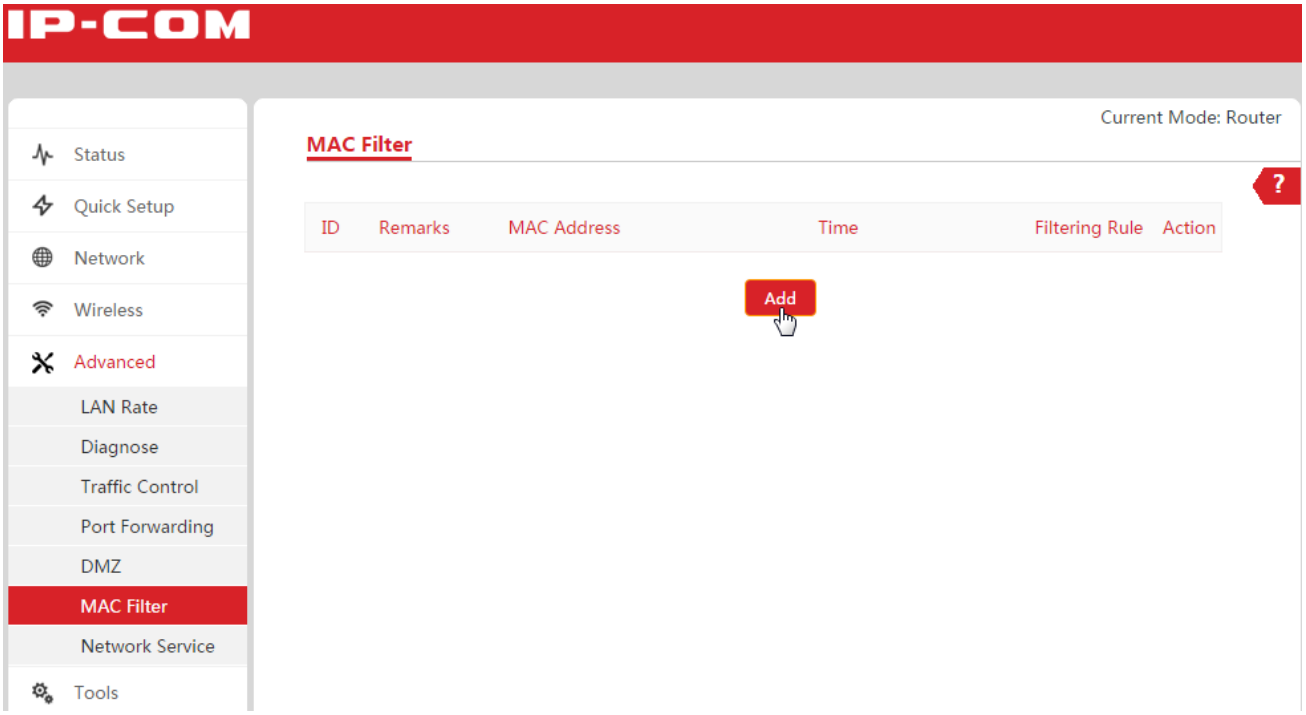
Parameter	Description
Remarks	Information about remarks of the MAC filter rule.
MAC Address	MAC address of client device.
Time	Time to forbid or allow a corresponding device in the rule to access the Internet.
Filtering Rule	• Allow only: Allow only the device with this MAC address to access the Internet. Other devices cannot access the Internet. • Forbid only: Forbid only the device with this MAC address from accessing the Internet. Other devices can access the Internet.
Operation	After successfully setting rules, click to delete corresponding rules.

Configure MAC filter

Assume that you want to forbid a client with MAC address C8:3A:35:03:11:79 from accessing the Internet at 18:00 to 20:00 on Monday to Friday. The Setup steps are as follows:

To configure MAC filter function:

1. Log in to the device's web UI.
2. Go to **Advanced > MAC Filter**.
3. Click **Add.**



4. In the pop-up window, set up the parameters.

   1) Filtering Rule: Click the dropdown list and select Forbid only.

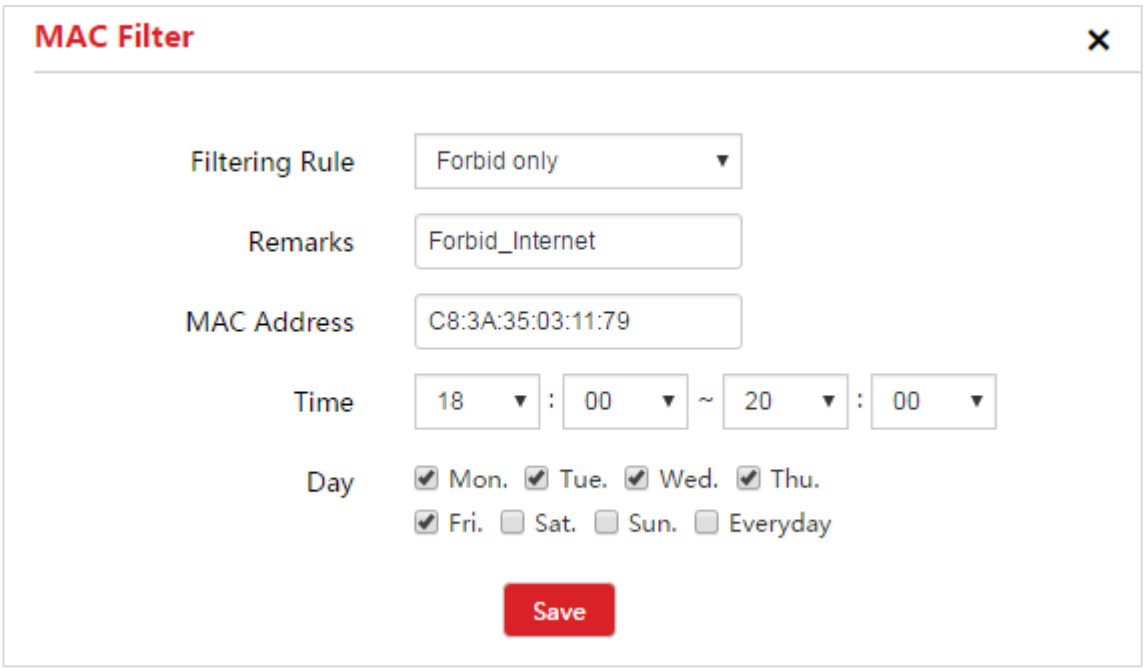
   2) Remarks: Description of setting a rule, for example, forbid accessing the Internet.

   3) MAC Address: Enter a MAC address of a client that is forbidden from being connecting to the AP (in this example, C8:3A:35:03:11:79).

   4) Time: Click the dropdown list and select a point in time when the rule is effective (in this example, 18:00~20:00).

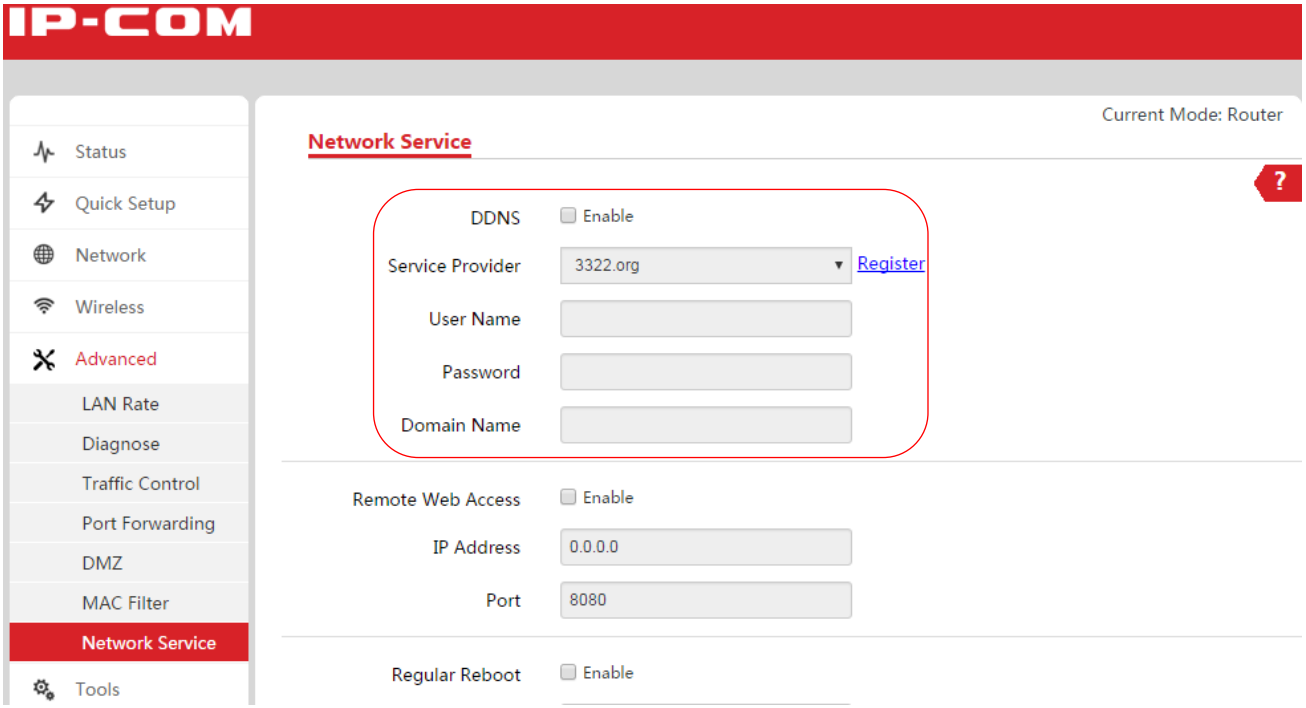
   5) Day: Click the dropdown list and select a date when the rule is effective (in this example, Monday to Friday).

5. Click **Save** to finish settings.



4.7.6 DDNS

DDNS (Dynamic Domain Name Service) is to map the device's dynamic WAN IP address (public network IP address) to a fixed domain name. When the service runs, the DDNS client sends this host's current WAN IP address to the DDNS server through information transmission. The server updates the mapping relation between the domain name and the IP address in the database to achieve dynamic domain name resolution.



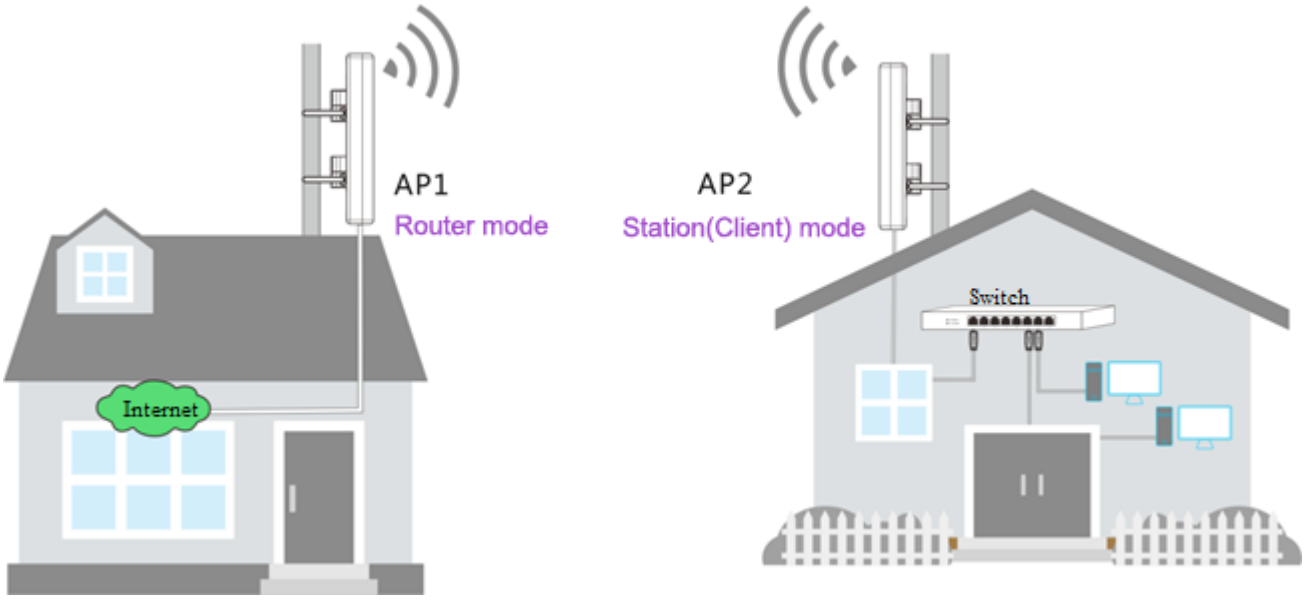
Parameter description

Parameter	Description
DDNS	Enable/Disable the DDNS function. The default is Disable.
Service Provider	Service provider who provides DDNS. This device supports 3322.org, dyndns.com, and noip.com.
User Name	User name to log in to DDNS, i.e. user name registered on the Service Provider website.
Password	Password to log in to DDNS, i.e. password registered on the Service Provider's website.
Domain Name	Domain name information obtained from the DDNS Service Provider website.

Application Scenario

A community uses 06 to perform networking. AP1 works in router mode and is connected to the Internet. The WAN IP address is dynamically changed. AP2 is bridged to AP1 wireless signals in station (client) mode. The network administrator needs to access resources on the intranet computer during business trip. This can be achieved through the DDNS function. Establish and enable an FTP server on the intranet computer. Store resources to be accessed on the server. Set the DDNS and port forwarding function on 06.

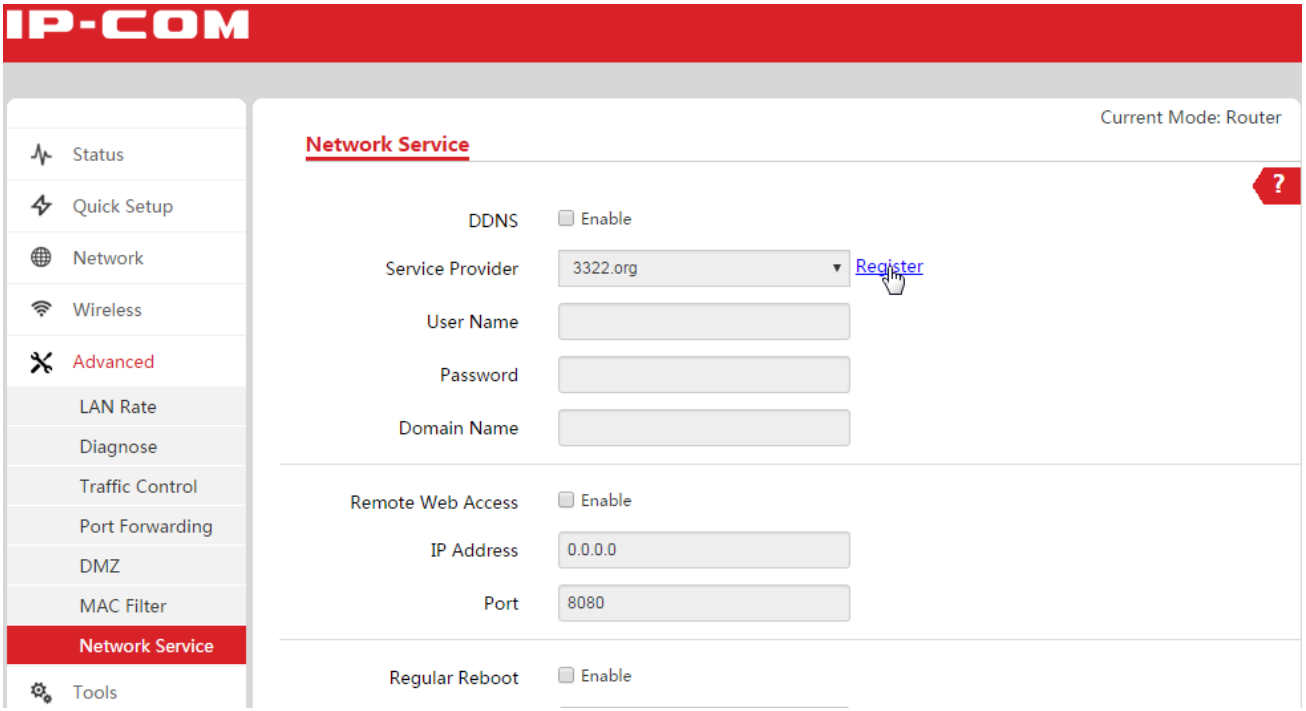
The reference topological graph is as follows:



Configure DDNS function

Step 1: Register a domain name.

1. Log in to the device's web UI.
2. Go to **Advanced > Network Service > DDNS**.
3. Go to the DDNS configuration page and click **Regiser**. (In case of noip.com or dyndns.com, check the Enable checkbox of DDNS, select a corresponding service provider, and click **Regiser**.)
4. Register a domain name by referring to prompt messages in the website.



Assume that registered basic information is as follows:

Service Provider	3322.org
User Name、Password	abc
Domain Name	abc.3322.org

Step 2: Set up a DDNS rule.

1. Re-enter the DDNS page and perform operations by referring to the following contents.

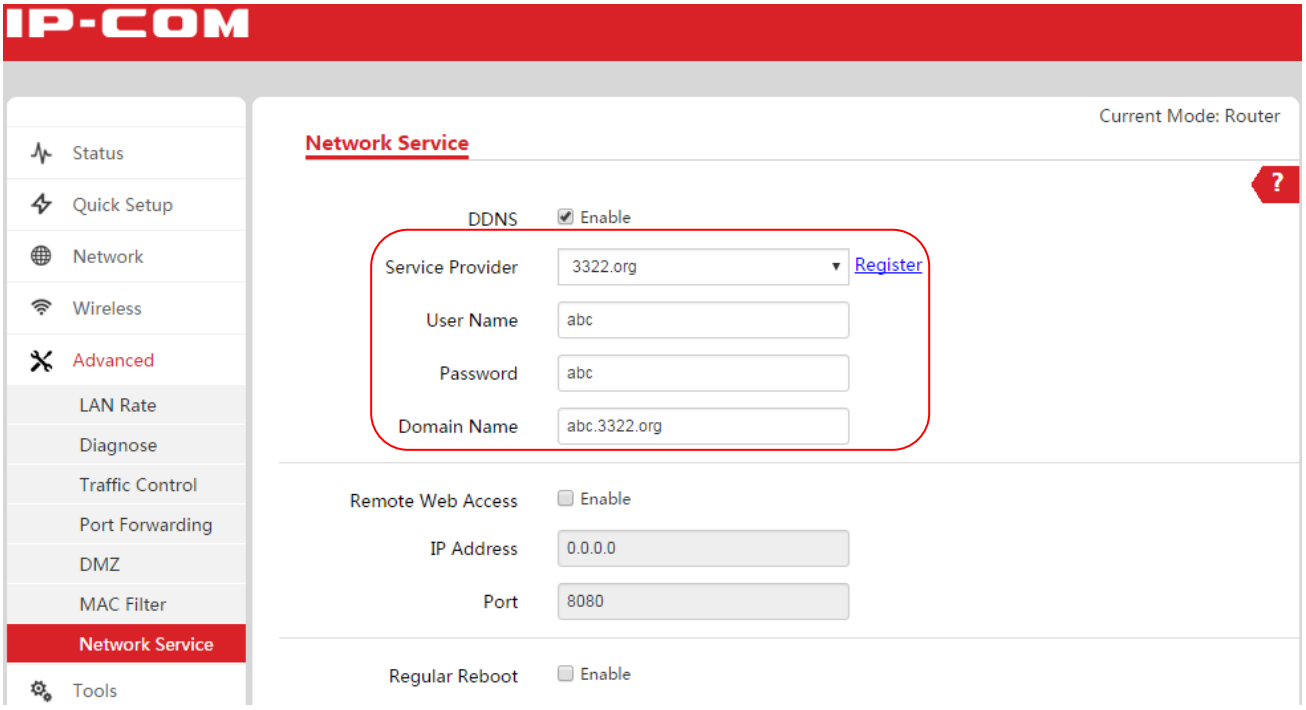
   1) DDNS: Click the Enable checkbox to enable this function.

   2) Service Provider: Click the dropdown box and select a corresponding DDNS Service Provider (in this example, 3322.org).

   3) User Name and Password: Enter the user name and password registered in the Service Provider website (in this example, abc).

   4) Domain Name: Enter the domain name created in the Service Provider website (in this example, abc.3322.org).

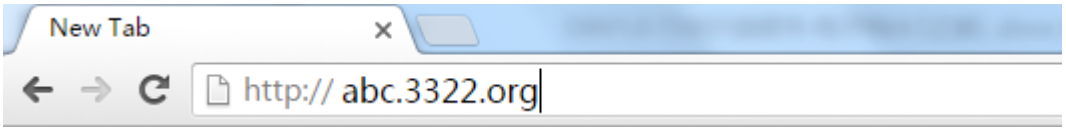
2. Click **Save** at the bottom of the page.



Step 3: Set the port forwarding function. For details of setup steps, refer to Port Forwarding.

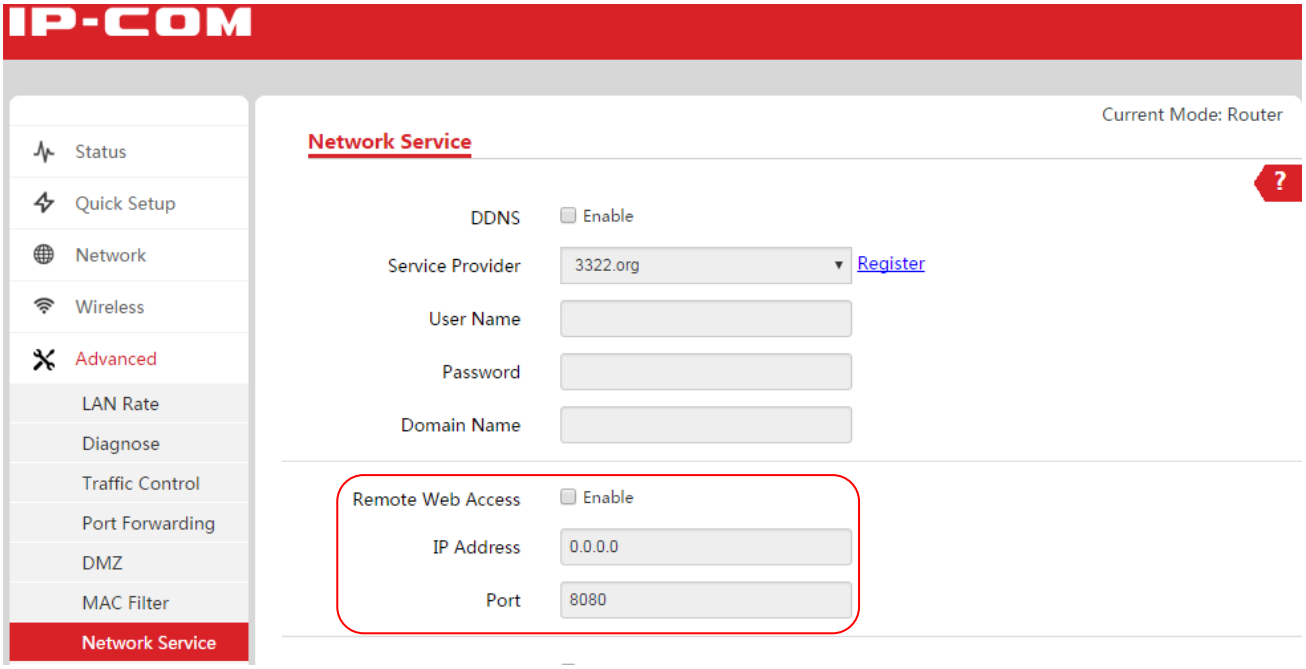
Verify the configuration

When extranet users access intranet resources, they need only to access http://abc.3322.org on a computer that has obtained a public network IP address.



4.7.7 Remote Web Access

As a general rule, only the client that is connected to the device with a network cable or wireless device can log in to its web UI. If necessary, you can remotely access the web UI of the device via the WAN interface.



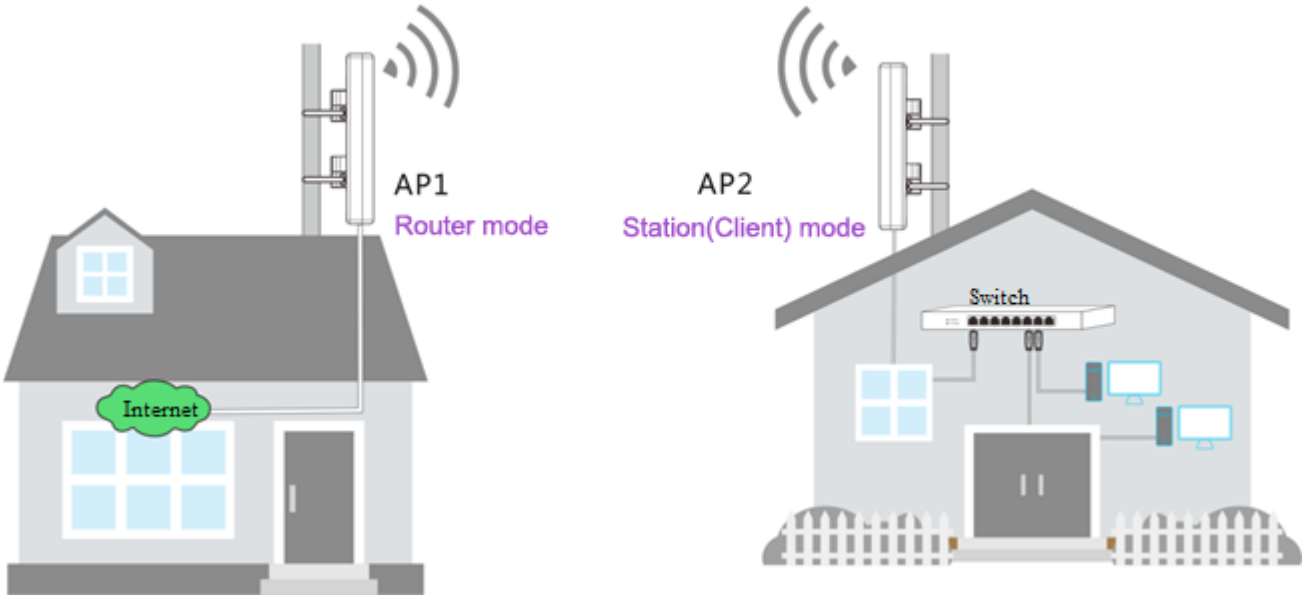
Parameter description

Parameter	Description
Remote Web Access	Enable/Disable the remote web management function. The default is Disable.
IP Address	IP address that remotely accesses the device. If no IP address is entered, it indicates that all computers on the Internet can log in to the web UI of the device.
Port Number	Port number used during remote management on the device. The default is 8080 and can be modified as needed. **Tip** Ports 1-1,024 have been occupied by known services. To avoid port conflict, it is strongly recommended to modify these ports to Ports 1,025-65,535.

Application Scenario

A community uses 06 to perform networking. AP1 works in router mode and is connected to the Internet. AP2 is bridged to AP1 wireless signals in Client mode. The AP1 WAN IP address is 202.105.106.55. The network administrator may want to maintain the network during business trip and needs to log in to the web UI of the device. This can be achieved through the Remote Web Access function.

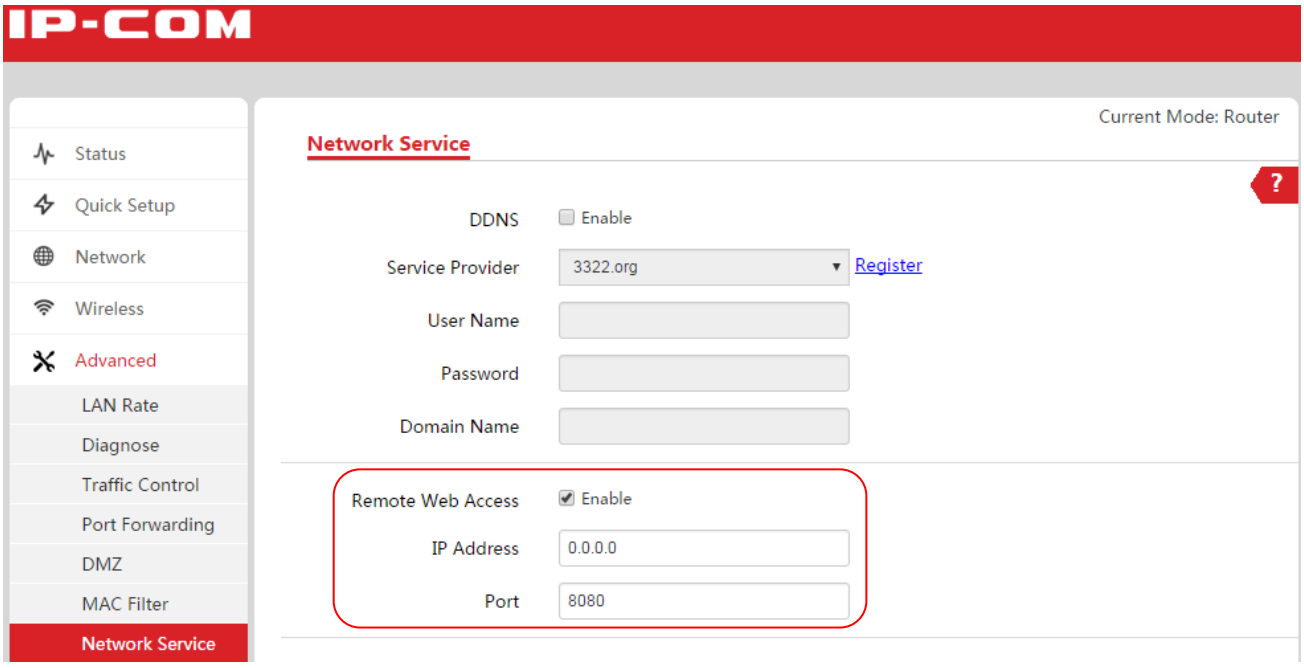
The reference topological graph is as follows:



Configure remote web access function

Step 1: Enable the Remote Web Access function of the device.

1. Log in to the device's web UI.
2. Go to **Advanced > Network Service**.
3. Check the **Enable** checkbox of the **Remote Web Access** option and click **Save** at the bottom of the page.



Verify the configuration

Log in to and manage the device by accessing http://202.106.105.55:8080 on the browser of a remote computer that has been connected to the Internet and has obtained a public network IP address.

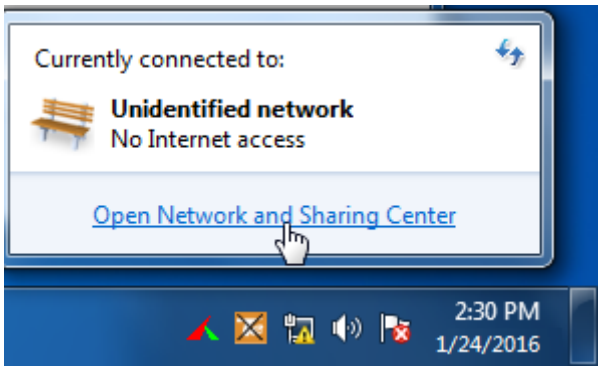
Appendix

Configure your computer

Here we take Windows 7 as an example.

Step 1: Click the icon  on the bottom right corner of your desktop.

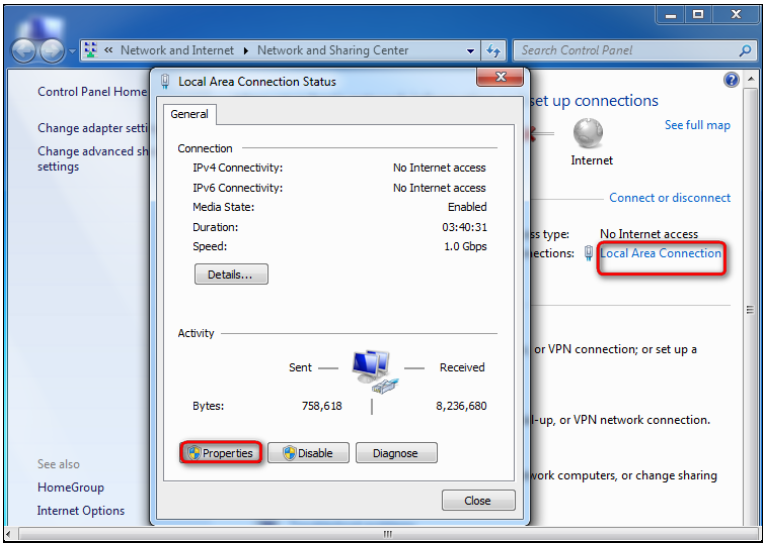
Step 2: Click **Open Network and Sharing Center**.



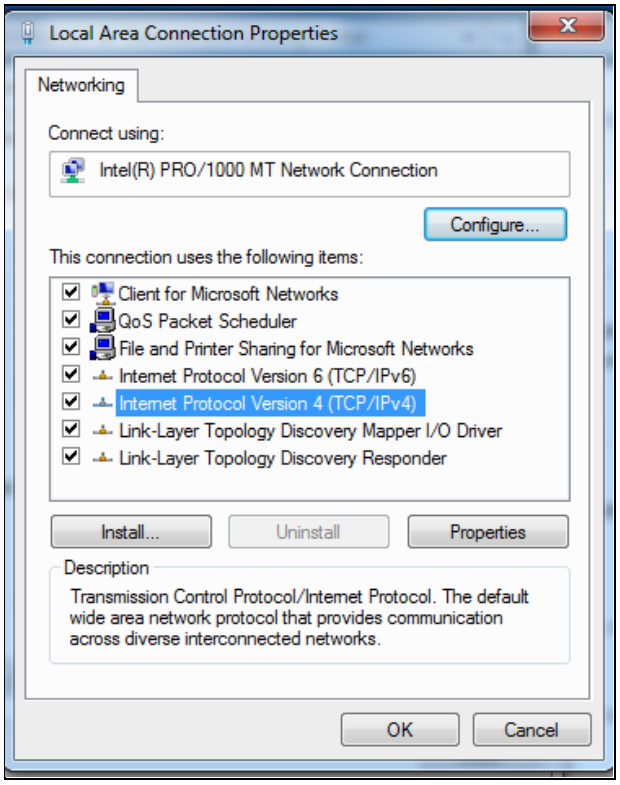
Tips

If you cannot find the icon  on the bottom right corner of your desktop, follow steps below: Click **Start > Control Panel > Network and Internet > Network and Sharing Center**.

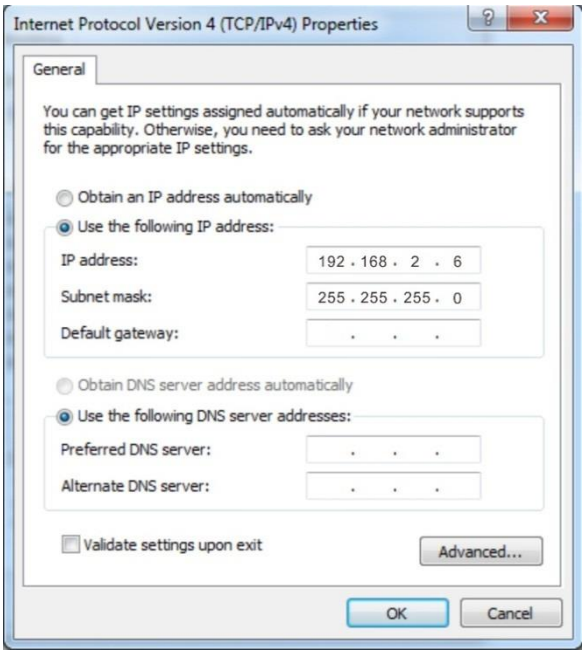
Step 3: Click **Local Area Connection > Properties**.



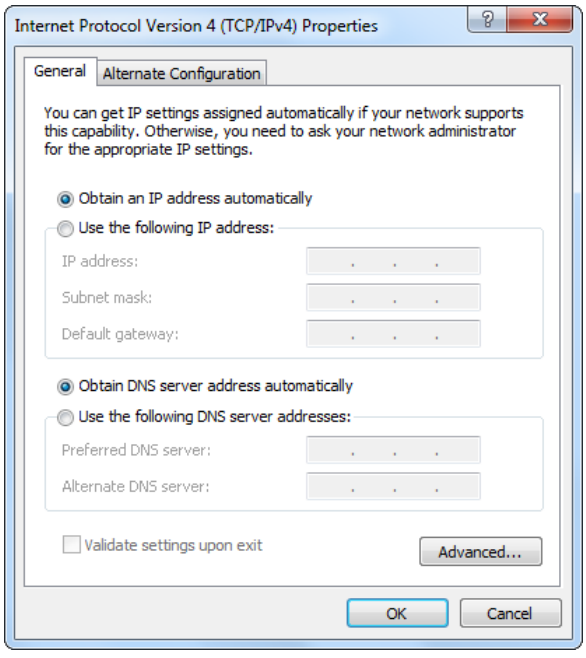
Step 4: Find and double click **Internet Protocol Version 4(TCP/IPv4)**.



Step 5: Select **Use the following IP address**, type in the IP address: **192.168.2.x** (2~253), Subnet mask: **255.255.255.0** and click **OK**. Or you can select **Obtain an IP address automatically**.



or



Step 6: Click **OK** on the **Local Area Connection Properties** window (see **Step 4** for the screenshot).

Safety and emission statement

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, we recommend that you use a shielded RJ45 cable.

Declaration of Conformity

Hereby, IP-COM NETWORKS Co., LTD. declares that the radio equipment type AP625 is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: http://www.ip-com.com.cn/en/ce.html

Operate Frequency: 5150-5250MHz (CH36-CH48)

EIRP Power (Max.): 22.8dBm

Software Version: V1.0.0.2

 Caution：

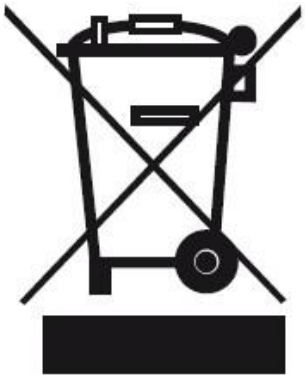
Adapter Model: BN060-P12024

Manufacture: SHENZHEN HEWEISHUN NETWORK TECHNOLOGY CO., LTD.

Input: 100-240V~50/60HZ 0.3A

Output: 24V 0.5A

 ：DC Voltage



RECYCLING

This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.

User has the choice to give his product to a competent recycling organization or to the retailer when he buys an new electrical or electronic equipment.

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.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, we recommend that you use a shielded RJ45 cable.