www.ip-com.com.cn

5GHz 11n 300Mbps Basestation BS6

User Guide

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 a warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM! Please read this user guide before you start.

Conventions

This user guide is applicable to the IP-COM 5GHz 11n 300Mbps Basestation BS6. The contained images and UI screenshots are subject to the actual products.

Unless otherwise specified, “base station”, "Base Station", “product”, or “the device” mentioned in this user manual indicates BS6.

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	Choose **System** > **Live Users**.
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX:XX:XX:XX:XX:XX*
UI control	Bold	On the **Policy** page, click the **OK** button.

The symbols that may be found in this document are defined as follows.

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.

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AES	Advanced Encryption Standard
AP	Access Point
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
CCQ	Client Connection Quality
CPE	Customer Premises Equipment
CTS	Clear to Send
DDNS	Dynamic Domain Name Server
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
GMT	Greenwich Mean Time
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
NMS	Network Management System
OID	Object Identifier
PoE	Power over Ethernet
PPPoE	Point-to-Point Protocol over Ethernet
PTP	Point-to-point
P2MP	Point-to-MultiPoint
P2MP	Point-to-MultiPoint
PVID	Port-based VLAN ID
RADIUS	Remote Authentication Dial In User Service

Acronym or Abbreviation	Full Spelling
RAM	Random Access Memory
RTS	Request to Send
RX	Receive Rate
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
TX	Transmit Rate
UDP	User Datagram Protocol
UI	User Interface
VLAN	Virtual Local Area Network
VID	VLAN Identifier
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	WLAN Internet Service Provider
WLAN	Wireless Local Area Networks
WMM	Wi-Fi multi-media
WPA-PSK	WiFi Protected Access-Pre-Shared Key
WPA	Wi-Fi Protected Access

Technical support

If you need more help, contact us using any of the following means. We will be glad to assist you as soon as possible.

☎	✉	🏠
+86-755-27653089	info@ip-com.com.cn	www.ip-com.com.cn

Contents

1 Application scenarios

1.1 Point to point connection between ISP control center and transit signal tower

Network requirement

You want to use two base stations to establish a Point to point (PTP) backhaul connection between ISP control center and transit signal tower.

Solution

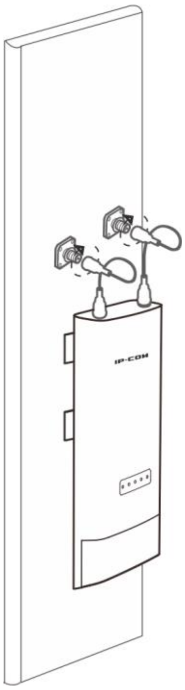
- Connect the base stations to the antennas (self-prepared)
- Set up the base stations
- Install the base stations

Tip

To establish the network quickly, you are recommended to set up the base stations before installing them.

Connect the base stations to the antennas

1. Remove the plastic screw caps on the RP-SMA connectors of a base station.
2. Connect one side of two RF coaxial cables (enclosed with the antennas) to the RP-SMA connectors of the base station.
3. Connect the other side of the RF coaxial cables to the connectors of the antenna.
4. Perform step **1** to step **3** above to connect the other base station to the antenna.



Set up the base stations

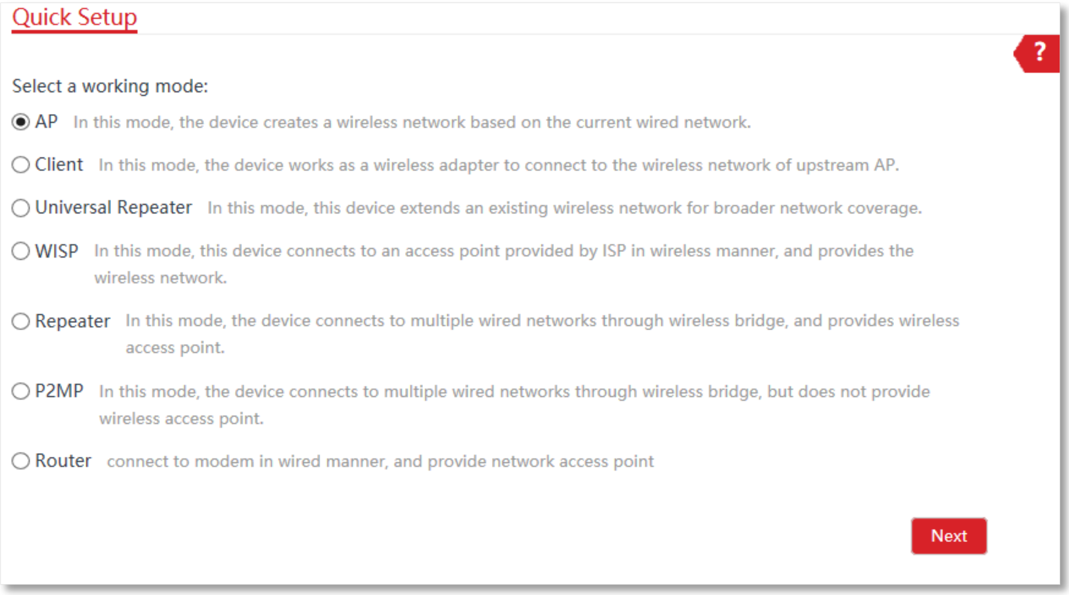
1 Put the two base stations next to each other, and power them on.

2 Set one base station (Base Station 1) to the **AP** mode.

(1) Connect a computer to the base station.

(2) Start a web browser on the computer, visit **192.168.2.1**, and choose **Quick Setup** to enter the configuration page.

(3) Select **AP** mode and click **Next**.



Quick Setup

Select a working mode:

● AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

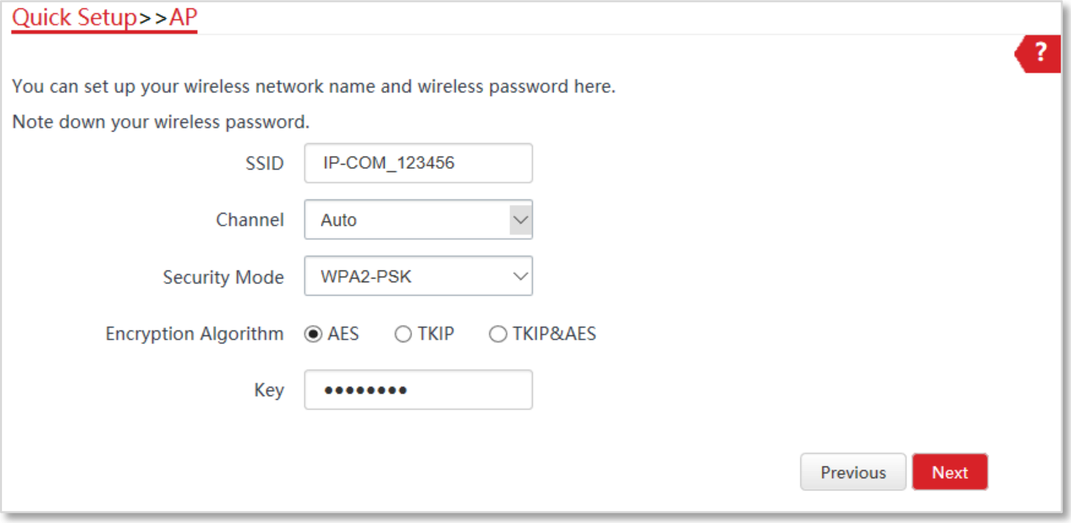
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

(4) Set an **SSID**, select a **Security Mode**, which are **IP-COM_123456** and **WPA2-PSK** in this example, customize a **Key**, and click **Next**.



Quick Setup>>AP

You can set up your wireless network name and wireless password here.

Note down your wireless password.

SSID: IP-COM_123456

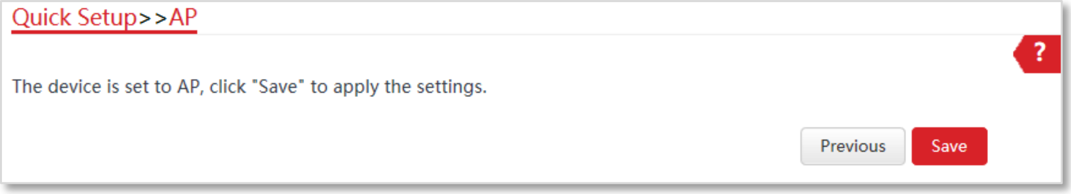
Channel: Auto

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

(5) Click **Save**, and wait until the device reboots automatically to activate the settings.



Quick Setup>>AP

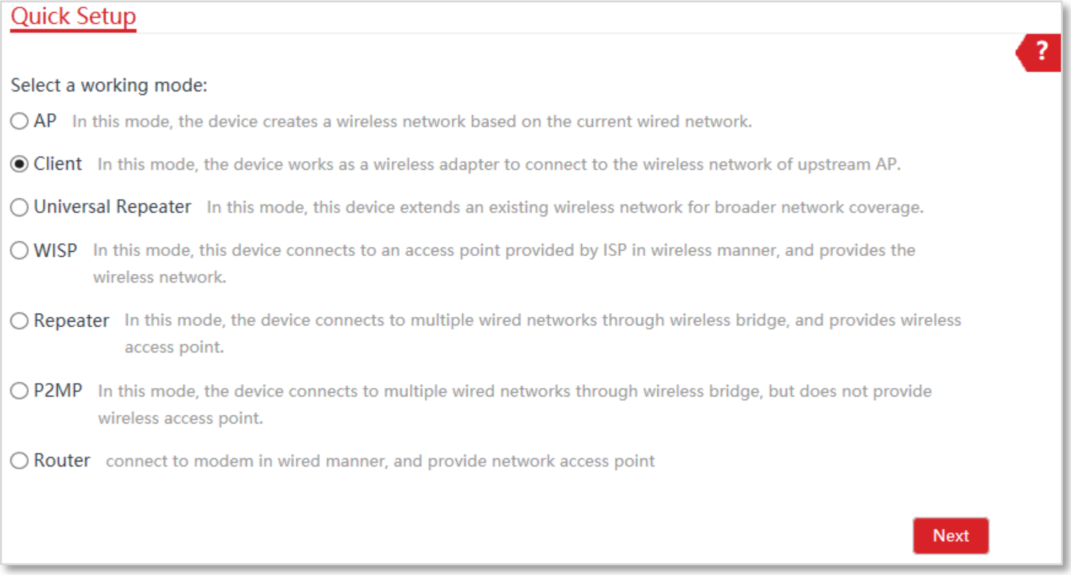
The device is set to AP, click "Save" to apply the settings.

3 Set the other base station (Base Station 2) to **Client** mode.

(1) Connect a computer to the base station.

(2) Start a web browser, visit **192.168.2.1**, and choose **Quick Setup** to enter the configuration page.

(3) Select **Client**, and click **Next**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

● Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

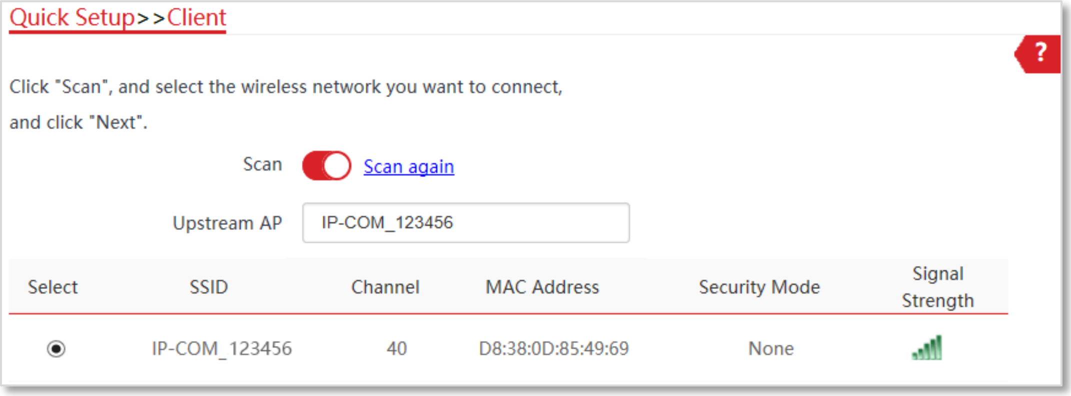
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

(4) Select the SSID of the Base Station 1, which is **IP-COM_123456** in this example, and click **Next** at the bottom of the page.



Quick Setup>>Client

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan: on — Scan again

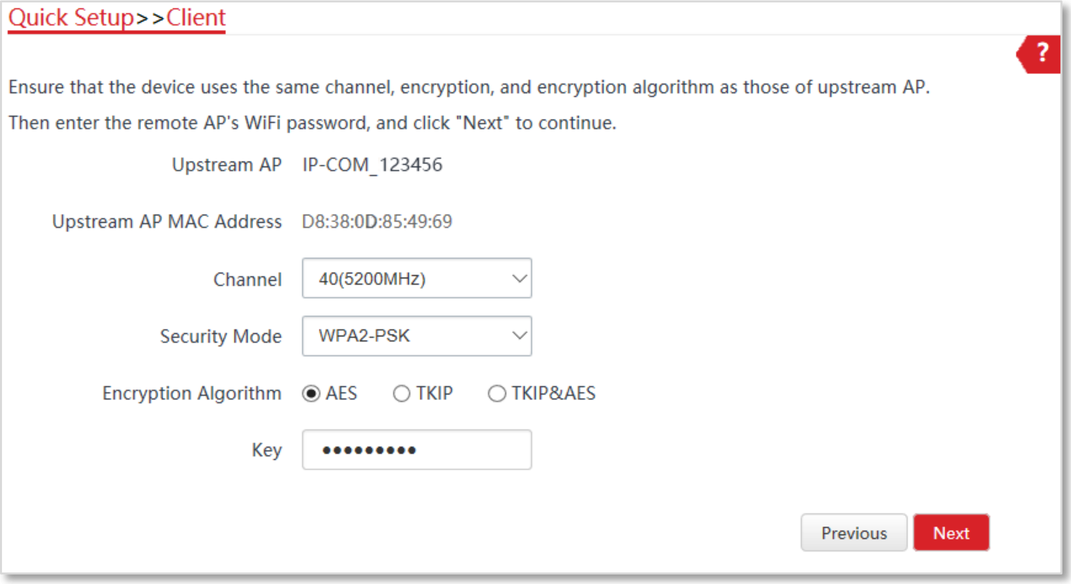
Upstream AP: IP-COM_123456

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	IP-COM_123456	40	D8:38:0D:85:49:69	None	

Tip

- If you cannot find any SSID from the list, choose Wireless > Basic and enable the wireless function. Then try again.
- If you cannot find the SSID of Base Station 1 from the list, adjust the direction of Base Station 2, and move it close to the Base Station 1.

(5) Enter the WiFi password you set on Base Station 1 in the **Key** input box, and click **Next**.



Quick Setup>>Client

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of upstream AP. Then enter the remote AP's WiFi password, and click "Next" to continue.

Upstream AP: IP-COM_123456

Upstream AP MAC Address: D8:38:0D:85:49:69

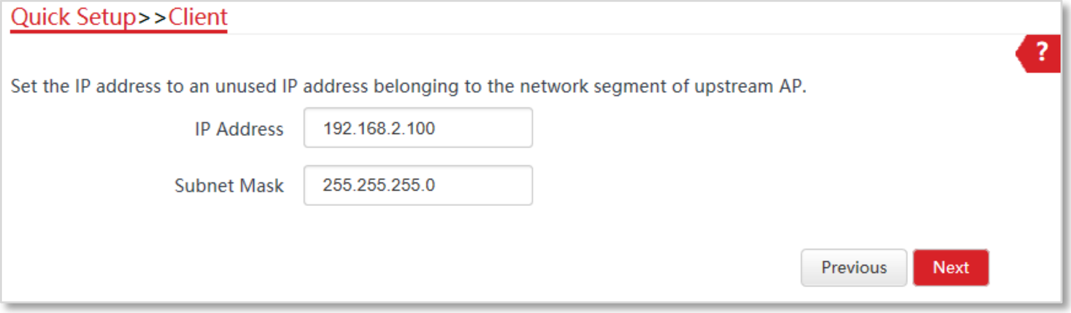
Channel: 40(5200MHz)

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••••

(6) Set the IP address to an unused one belonging to the same network segment of Base Station 1. For example, if the IP address of Base Station 1 is **192.168.2.1**, you can set the IP address of the device to 192.168.2.*X* (*X* ranges from 2 to 254). Then click **Next**.



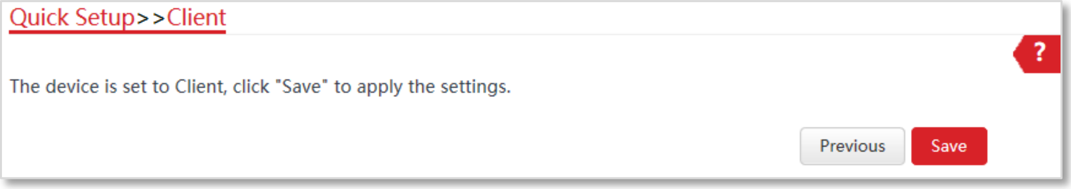
Quick Setup>>Client

Set the IP address to an unused IP address belonging to the network segment of upstream AP.

IP Address: 192.168.2.100

Subnet Mask: 255.255.255.0

(7) Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Client

The device is set to Client, click "Save" to apply the settings.

---End

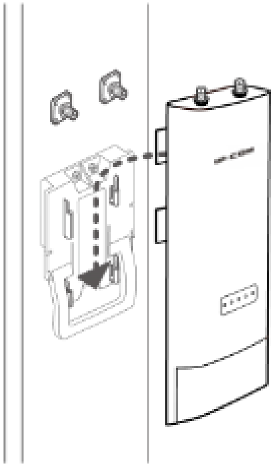
When LED1, LED2, and LED3 of Base Station 1 are solid on, and LED1, LED2, and LED3 of Base Station 2 are blinking, the bridging succeeds.

Install the base stations

Select one of the following options to install the base stations to proper positions.

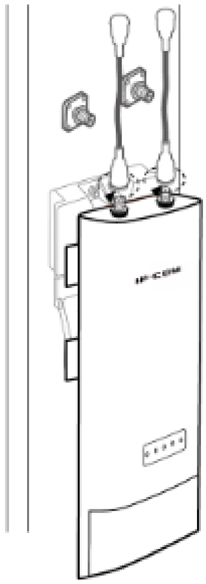
Option 1: Bracket mounting

1 Press the handle on the mount bracket, align the four hooks on the rear panel of the base station with the four slots on the bracket, and slide the base station to fix it onto the bracket

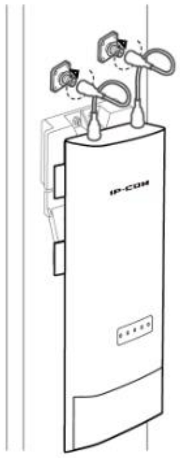


2 Remove the plastic screw caps on the RP-SMA connectors of the base station.

3 Connect one side of two RF coaxial cables (enclosed with the antennas) to the RP-SMA connectors of the base station.



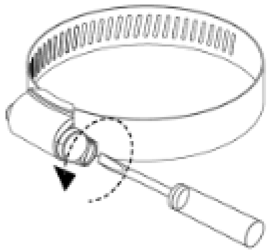
4 Connect the other side of the RF coaxial cables to the connectors of the antenna.



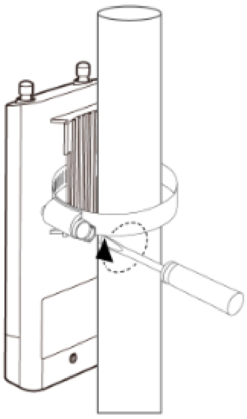
---End

Option 2: Pole mounting

1 Use a screwdriver to open the metal strap by turning the screw counter-clockwise.

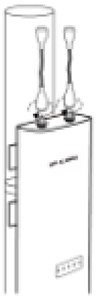


2 Straighten out the end of the metal strap, and thread it through the back of the base station, wrap the metal strap around the pole, and tighten the strap by turning the screw clockwise using the screwdriver.

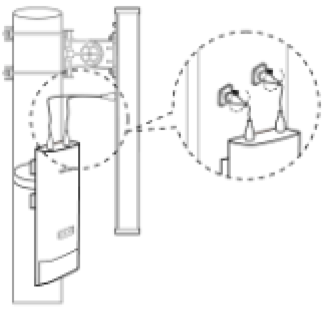


3 Remove the plastic screw caps on the RP-SMA connectors of the base station.

4 Connect one side of two RF coaxial cables (enclosed with the antennas) to the RP-SMA connectors of the base station.



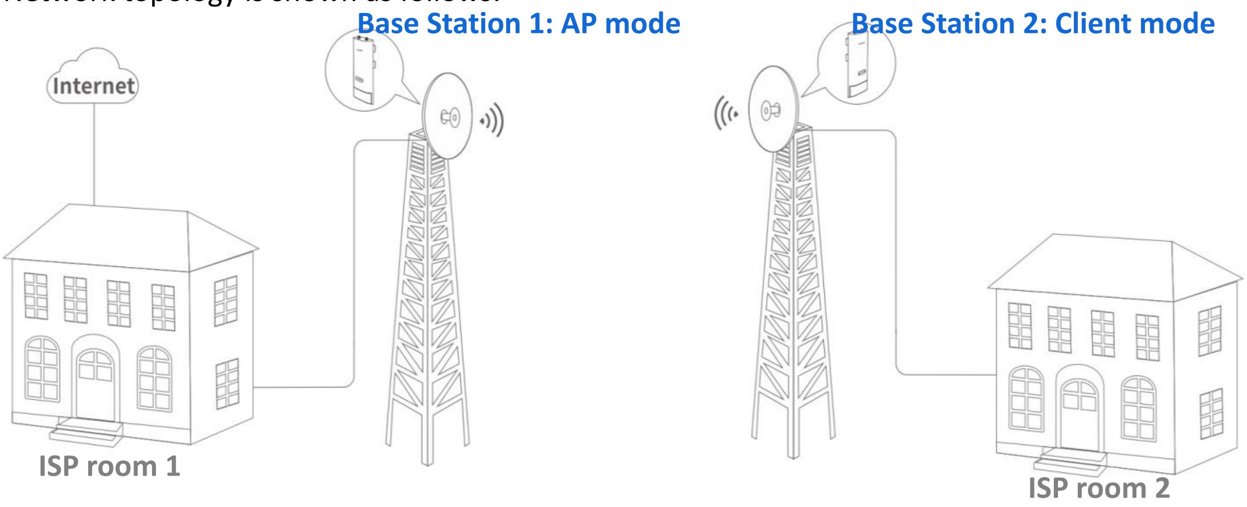
5 Connect the other side of the RF coaxial cables to the connectors of the antenna.



---End

Clients connected to the Base Station 2 can access the internet.

Network topology is shown as follows:



Check the LED1, LED2 and LED3 indicators of the base stations to confirm whether the positions are proper. The more LED indicators light up, and the better the connection quality is. The LED indicator description below is for reference.

LED indicators	Status	Description
LED1, LED2, LED3 (Received signal strength LED indicators)	Solid on/Blinking	Bridged successfully. – LED1, LED2 and LED3 are solid on/blinking: Good signal – LED1 and LED2 are solid on/blinking, and LED3 is off: Fair signal – LED1 is solid on/blinking, and LED2 and LED3 are off: Weak signal. Please adjust the direction or location of the two bridging devices. Tip – By default, the minimum signal strength of LED1, LED2 and LED3 are -90 dBm, -80 dBm and -70 dBm. You can change them on the **Wireless** > **Advanced** page of the web UI of the device. – If the LED indicators are solid on, the base station works in AP mode. If blinking, it works in Client mode.
	Off	The received signal strength does not reach the minimum RSSI threshold of the base station, or the bridging fails. Please adjust the direction or location of the two bridging devices.

1.2 Point to multiple point connections between the ISP signal tower and end users

Network requirement

You want to use the base station to work with outdoor CPEs to extend the ISP hotspot to end users. In this example, IP-COM outdoor CPE12 is used for illustration.

Solution

- Connect the base station to the antenna (self-prepared)
- Set up the base station and the CPE
- Install the base station and the CPE

Tip

To establish the network quickly, you are recommended to set up the base station and CPE before installing them.

Connect the base station to the antenna

Refer to the procedures in Connect the base stations to the antennas in **1.1 Point to point connection between ISP control center and transit signal tower**.

Set up the base station and CPE

Option 1: Automatic bridging (Recommend)

Tip

- Automatic bridging is only applicable when the base station and CPE are in factory settings.
- Ensure that only the base station and ONE CPE are powered on when performing peer-to-peer bridging. Otherwise, the peer-to-peer bridging may fail.
- If the base station and CPE are powered on using Ethernet cables, CAT5e or better Ethernet cable is recommended, and the length should not exceed 60 meters.
- For peer-to-multiple peers bridging, perform peer-to-peer bridging first, and then power on the rest CPEs within 30 minutes. Otherwise, the bridging may fail.
- A base station can bridge to 20 CPEs at most.

1 Prepare a base station and the CPEs (CPE12) which need to bridge to the base station, and put the CPEs near the base station.

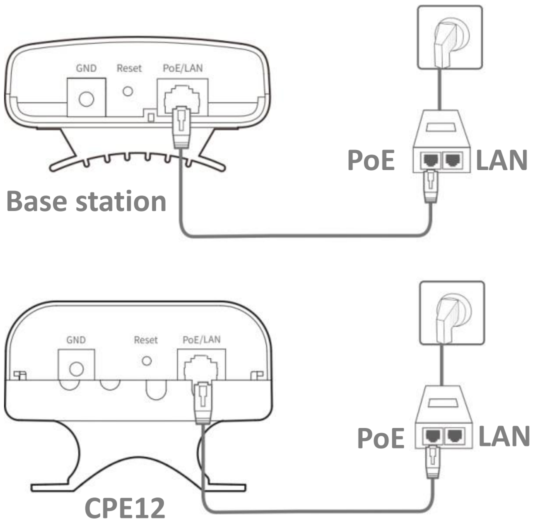
2 Choose one CPE12 to perform peer to peer bridging with the base station.

(1) Place the base station and the CPE12 next to each other.

(2) Power on the base station and CPE12.

- Remove the covers of the base station and CPE12.
- Use Ethernet cables (CAT5e or better Ethernet cable is recommended) to connect their PoE/LAN ports to the PoE ports of the included PoE adapters respectively.
- Use the power cords to connect the PoE adapters to power sources. When PoE/LAN LED indicators of the base station and CPE12 light up, they completes startup.

Within 1 minute, the base station and CPE12 perform automatic bridging. When the bridging succeeds, the DHCP servers of the base station and CPE12 are disabled. CPE12 works in **Client** mode and its IP address is changed to 192.168.2.2.



3 Within 30 minutes after the peer-to-peer bridging succeeds, power on the rest CPE12.

Wait for about 1 minute. When the LED1, LED2, and LED3 of these CPE12 are blinking, the bridging succeeds.

---End

Tip

After the bridging succeeds, all CPE12 work in Client mode, and their IP addresses are changed to 192.168.2.2.

Option 2: Setting up the base station and CPE (CPE12) using the web UI

1 Prepare a base station and the CPEs (CPE12) which need to bridge to the base station, and put the CPEs near the base station.

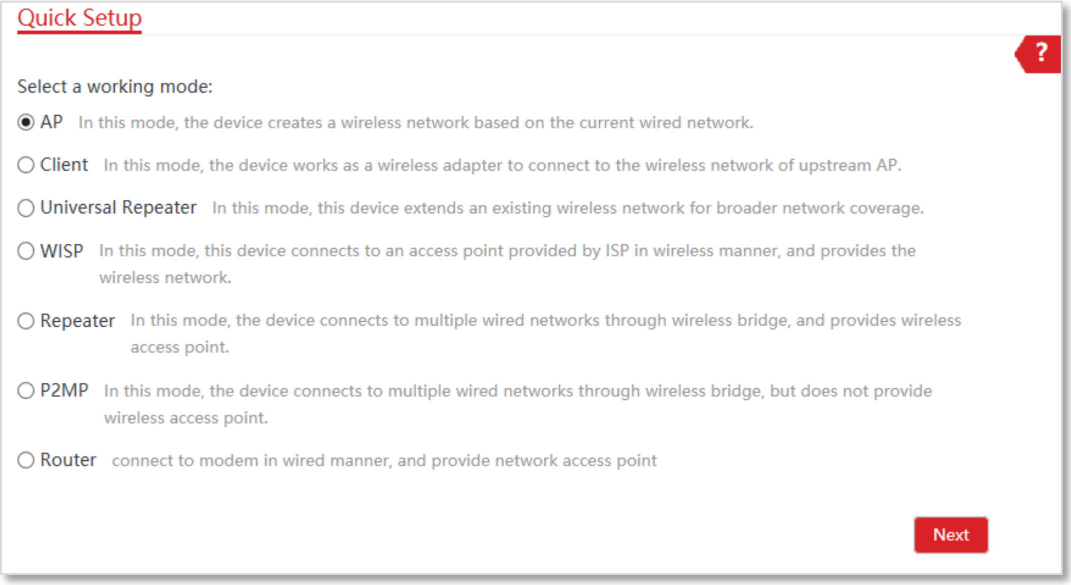
2 Power them on.

3 Set the base station to **AP** mode.

(1) Connect a computer to the base station.

(2) Start a web browser on the computer, visit **192.168.2.1**, and choose **Quick Setup** to enter the configuration page.

(3) Select **AP** mode and click **Next**.



Quick Setup

Select a working mode:

● AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

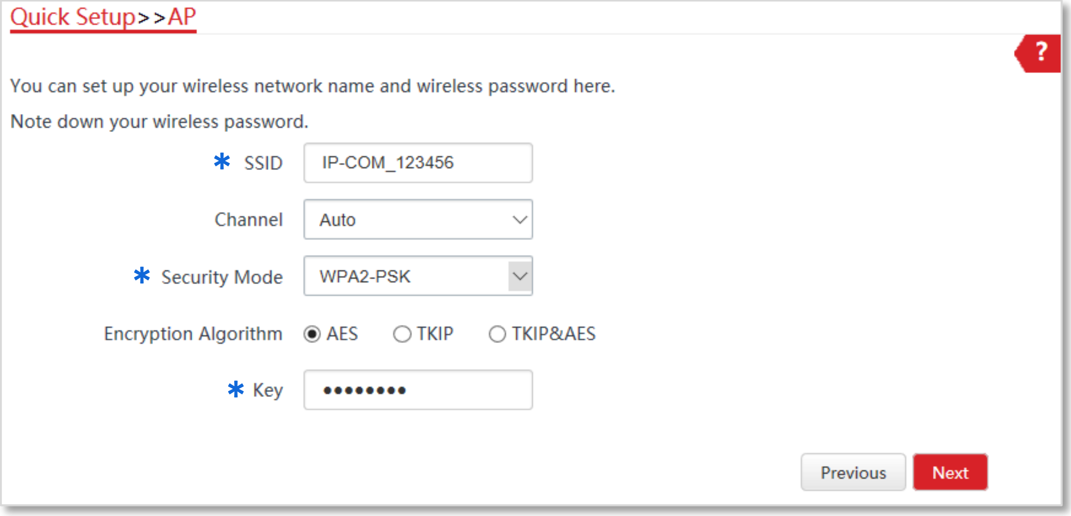
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

(4) Set an **SSID**, select a **Security Mode**, which are **IP-COM_123456** and **WPA2-PSK** in this example, customize a **Key**, and click **Next**.



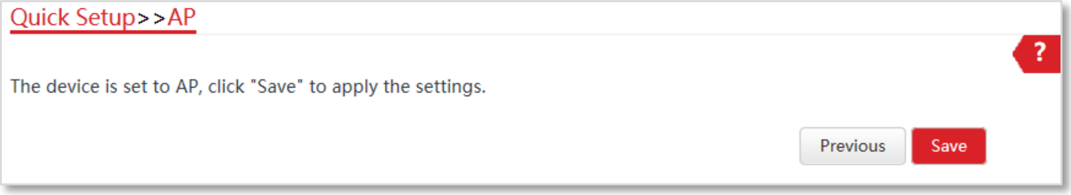
Quick Setup>>AP

You can set up your wireless network name and wireless password here.

Note down your wireless password.

* SSID	IP-COM_123456
Channel	Auto
* Security Mode	WPA2-PSK
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
* Key	••••••••

(5) Click **Save**, and wait until the device reboots automatically to activate the settings.



Quick Setup>>AP

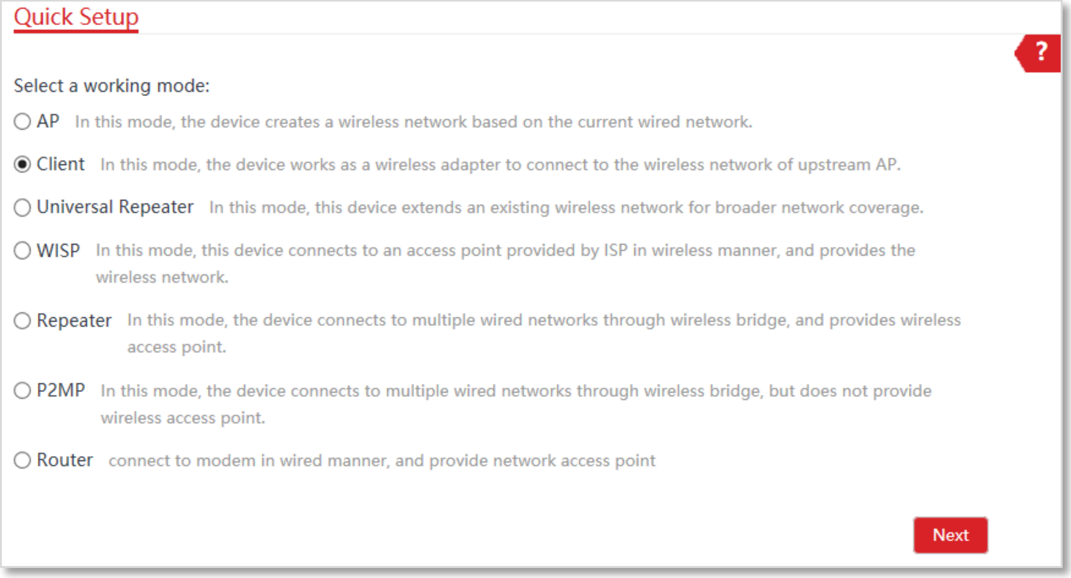
The device is set to AP, click "Save" to apply the settings.

4 Set CPE12 to **Client** mode.

(1) Connect a computer to CPE12.

(2) Start a web browser on the computer, visit **192.168.2.1**, and choose **Quick Setup** to enter the configuration page.

(3) Select **Client**, and click **Next**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

● Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

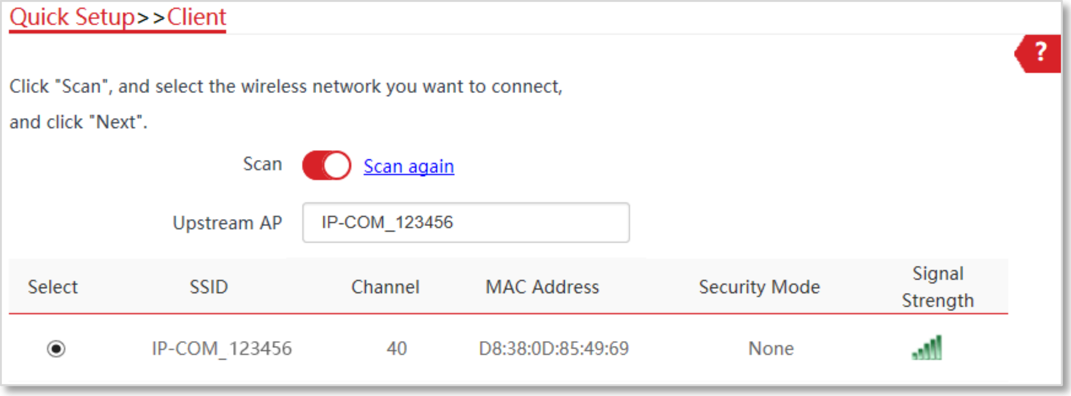
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

(4) Select the SSID of the base station, which is **IP-COM_123456** in this example, and click **Next** at the bottom of the page.



Quick Setup>>Client

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan: on, Scan again

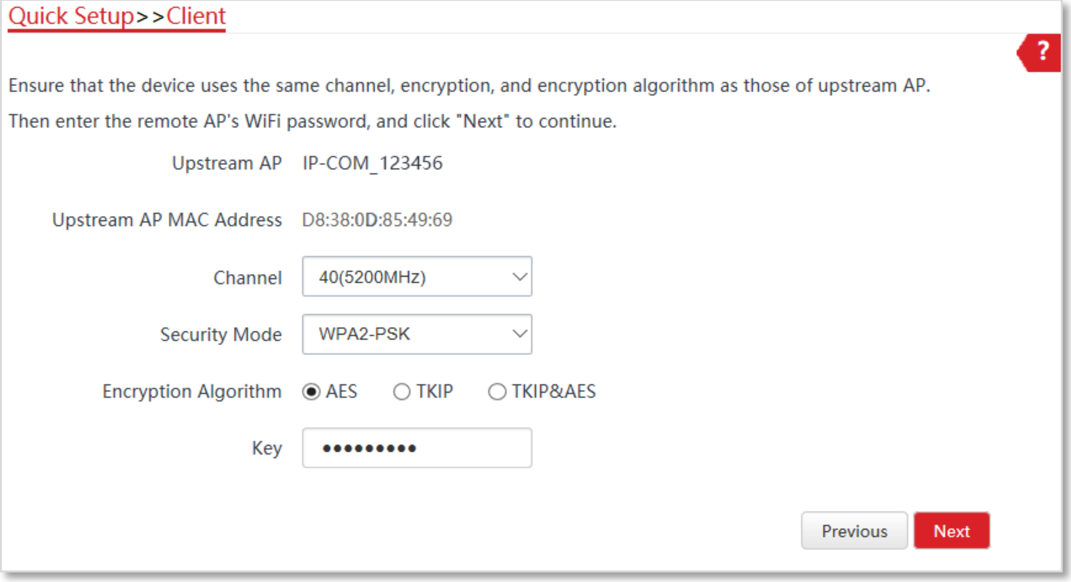
Upstream AP: IP-COM_123456

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	IP-COM_123456	40	D8:38:0D:85:49:69	None	

Tip

- If you cannot find any SSID from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.
- If you cannot find the SSID of the base station from the list, adjust the direction of CPE12, and move it close to the base station.

(5) Enter the WiFi password you set on base station in the **Key** input box, and click **Next**.



Quick Setup>>Client

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of upstream AP.

Then enter the remote AP's WiFi password, and click "Next" to continue.

Upstream AP IP-COM_123456

Upstream AP MAC Address D8:38:0D:85:49:69

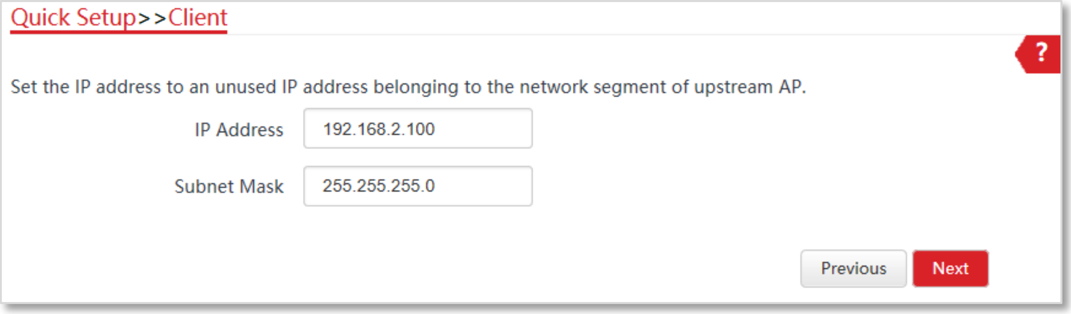
Channel 40(5200MHz)

Security Mode WPA2-PSK

Encryption Algorithm ● AES ○ TKIP ○ TKIP&AES

Key ●●●●●●●●●

(6) Set the IP address to an unused one belonging to the same network segment of the base station. For example, if the IP address of the base station is **192.168.2.1**, you can set the IP address of the device to 192.168.2.*X* (*X* ranges from 2 to 254). Then click **Next**.



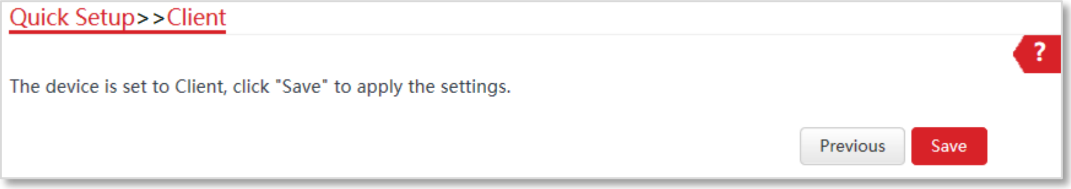
Quick Setup>>Client

Set the IP address to an unused IP address belonging to the network segment of upstream AP.

IP Address 192.168.2.100

Subnet Mask 255.255.255.0

(7) Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Client

The device is set to Client, click "Save" to apply the settings.

5 Perform step 4 to set the rest CPE12 to **Client** modes.

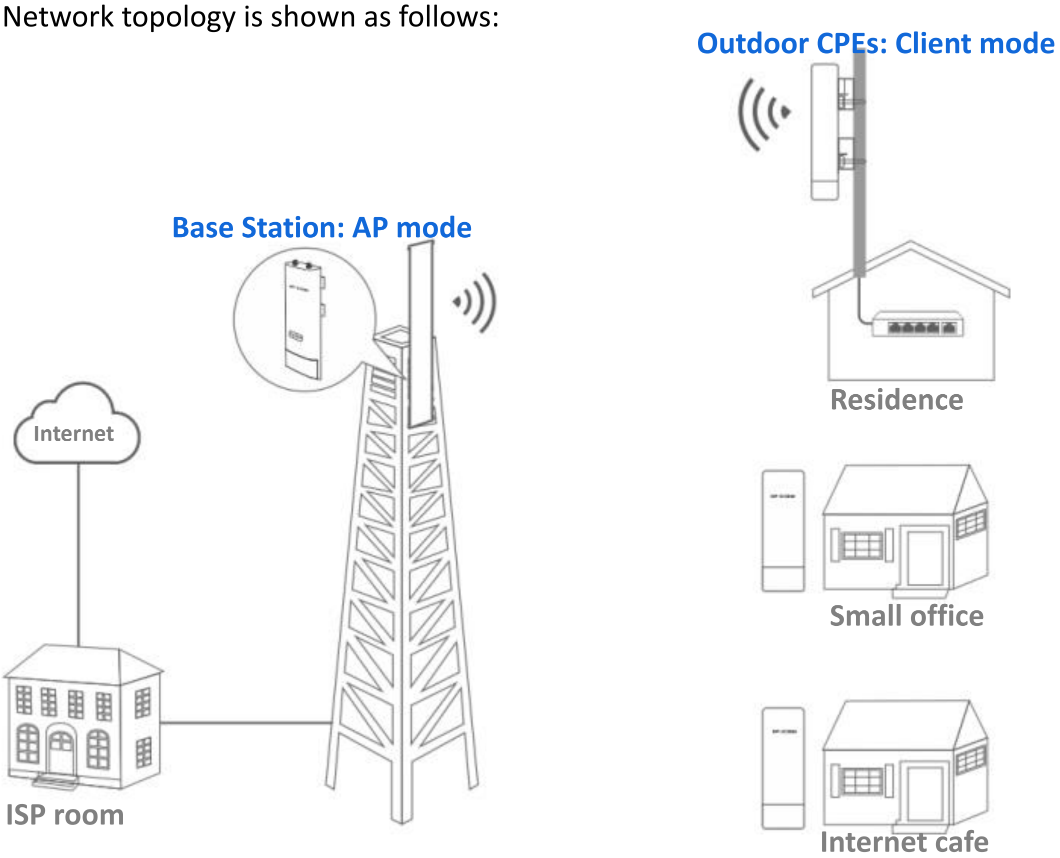
---End

When LED1, LED2, and LED3 of the base station are solid on, and LED1, LED2, and LED3 of CPE12 are blinking, the bridging succeeds.

Install the base station and CPEs

Refer to Install the base stations in **1.1 Point to point connection between ISP control center and transit signal tower** to install the base station.

Network topology is shown as follows:



Check the LED1, LED2 and LED3 indicators of the base stations and the CPEs to confirm whether the positions are proper. The more LED indicators light up, and the better the connection quality is. The LED indicator descriptions of the base station and CPEs below are for reference.

LED indicator description of the base station:

LED indicators	Status	Description
LED1, LED2, LED3 (Received signal strength LED indicators)	Solid on/Blinking	Bridged successfully. – LED1, LED2 and LED3 are solid on/blinking: Good signal – LED1 and LED2 are solid on/blinking, and LED3 is off: Fair signal – LED1 is solid on/blinking, and LED2 and LED3 are off: Weak signal. Please adjust the direction or location of the two bridging devices. Tip By default, the minimum signal strength of LED1, LED2 and LED3 are -90 dBm, -80 dBm and -70 dBm. You can change them on the **Wireless** > **Advanced** page of the web UI of the device.
	Off	The received signal strength does not reach the minimum RSSI threshold of the base station, or the bridging fails. Please adjust the direction or location of the two bridging devices.

LED indicator description of the CPEs:

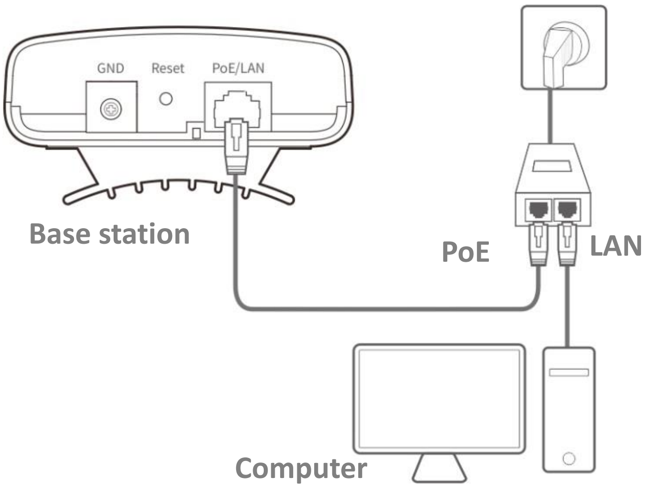
LED indicator	Status	Description
LED1, LED2, LED3 (Received signal strength LED indicators)	Solid on/Blinking	Bridged successfully. – LED1, LED2 and LED3 are solid on/blinking: Good signal – LED1 and LED2 are solid on/blinking, and LED3 is off: Fair signal – LED1 is solid on/blinking, and LED2 and LED3 are off: Weak signal. Please adjust the direction or location of your CPEs. Tip – By default, the minimum signal strength of LED1, LED2 and LED3 are -90 dBm, -80 dBm and -70 dBm. You can change them on the **Wireless** > **Advanced** page of the web UI of the CPE. – If the LED indicators are solid on, the CPE works in AP mode. If blinking, it works in Client mode.
	Off	The received signal strength does not reach the minimum RSSI threshold of the CPE, or the bridging fails. Please adjust the direction or location of your CPEs.

2 Login

2.1 Login

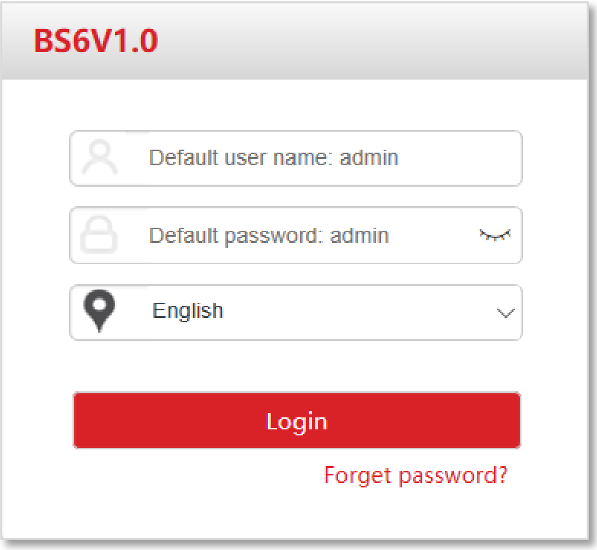
When you log in to the web UI at the first time or after the base station is reset to factory settings, follow the steps below:

1 Connect a computer to the base station as shown in the figure below.



2 Start a web browser on the computer, and visit **192.168.2.1**.

3 Enter the login user name and password (both are **admin** by default), and click **Login**.



Tip

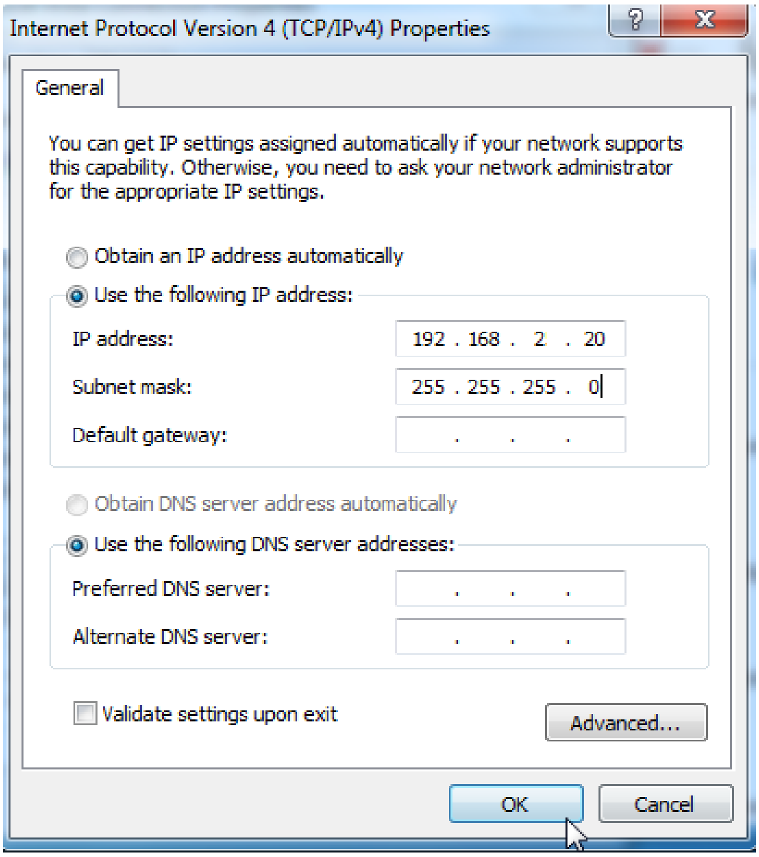
For the security of your network, you can change the login user name and password by choosing **Tools** > **Account**.

If you want to log in to the web UI after the base station is set to AP mode, Client mode, Universal Repeater mode, Repeater mode or P2MP mode, follow the steps below:

1 Connect the computer to the base station or the switch connected to the base station.

2 Set the IP address of the computer to an unused one belonging to the same network segment of the IP address of the base station.

For example, if the IP address of the base station is 192.168.2.1, you can set the IP address of the computer to 192.168.2.*X* (*X* is an unused digit ranging from 2 to 254), and subnet mask to 255.255.255.0.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

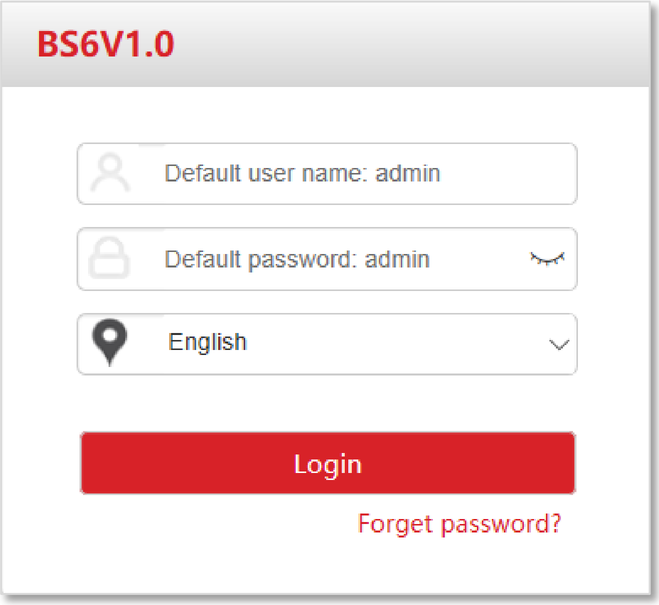
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

3 Start a web browser on your computer, and visit the IP address of the base station.

4 Enter the login user name and password, and click **Login**.



---End

Tip

- Refer to How to assign a fixed IP address to your computer in Appendix for details of step 2 above.
- If the base station is set to **AP**, **Client**, **or Universal Repeater** mode, check its IP address in the client list of the upstream device.
- If the base station is set to **Repeater** or **P2MP** mode, use the IP address you changed when you set it to these modes to log in to the web UI. If you do not change it, try 192.168.2.1.

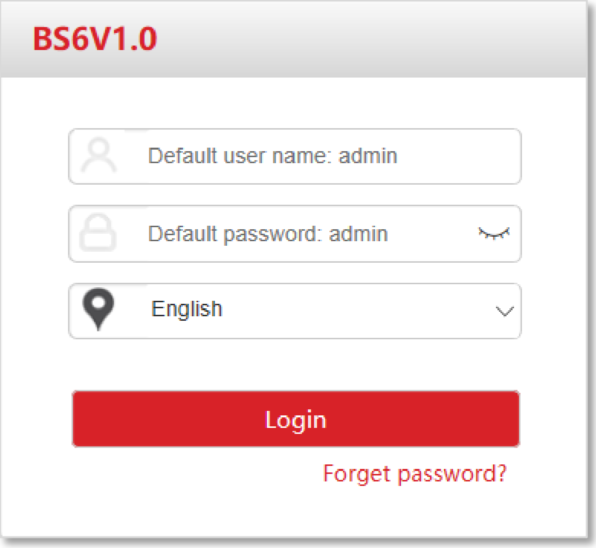
If you want to log in to the web UI after the base station is set to WISP or Router mode, follow the steps below:

1 Connect the computer to the base station or the switch connected to the base station.

2 Check the gateway IP address of the computer, and we assume that it is **192.168.0.1** in this example.

3 Start a web browser on your computer, and visit **192.168.0.1**.

4 Enter the login user name and password, and click **Login**.



BS6V1.0

Default user name: admin

Default password: admin

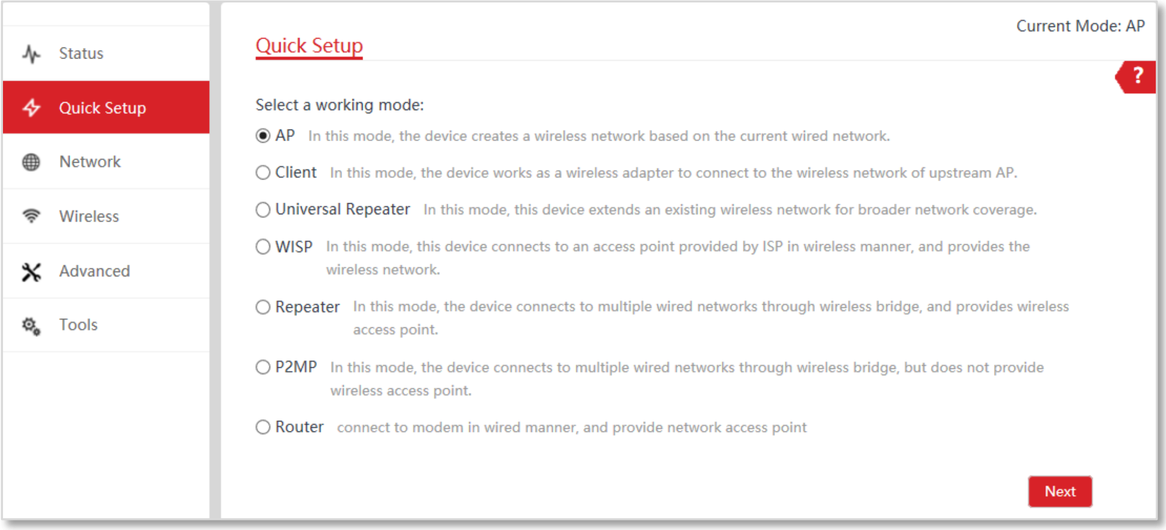
English

---End

Tip

Refer to How to check the gateway IP address of a computer in Appendix to get the gateway IP address of your computer.

After successful login, the following page appears.



Current Mode: AP

Quick Setup

Select a working mode:

● AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

2.2 Logout

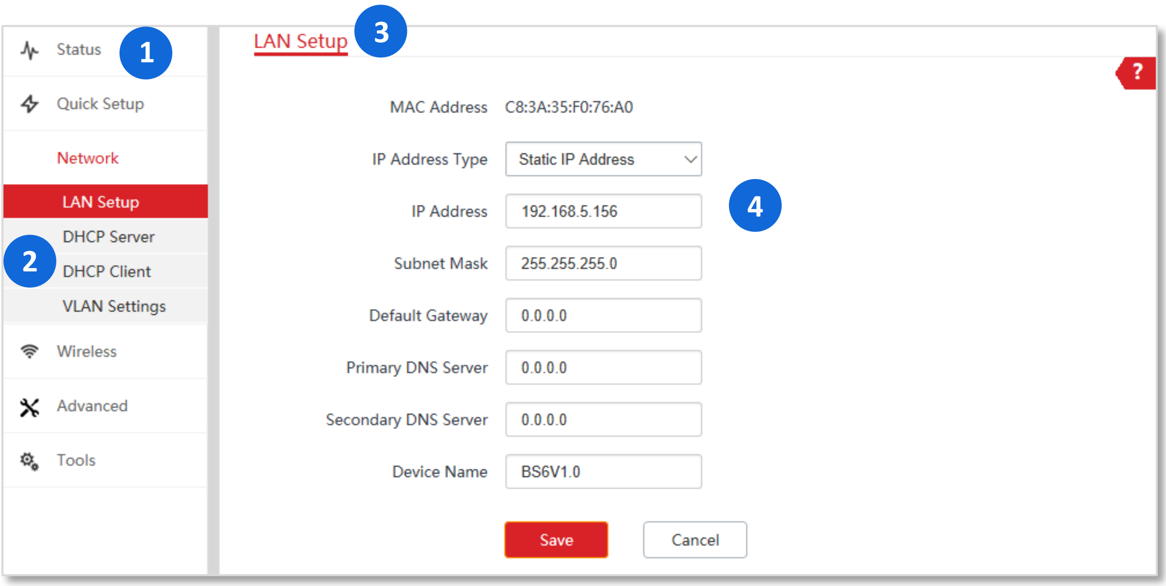
The base station logs you out when you:

- Click the **Logout** button on the upper-right corner of the web UI.
- Close the web browser.
- Perform no operation within the login timeout interval (default: 5 minutes). You can change the login timeout interval on the **Advanced** > **Network Service** page.

3 Web UI

3.1 Web UI layout

The web UI of the base station is composed of 4 parts, including the level-1 navigation tree, level-2 navigation tree, tab page area, and configuration area. See the following figure.



MAC Address C8:3A:35:F0:76:A0

IP Address Type Static IP Address

IP Address 192.168.5.156

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

Device Name BS6V1.0

SN	Area	Description
❶	Level-1 navigation bar	The navigation bars and tab pages display the function menu of the device. When you select a function in navigation bar, the configuration of the function appears in the configuration area.
❷	Level-2 navigation bar	
❸	Tab page area	
❹	Configuration area	The configuration area enables you to set or view parameters.

3.2 Common buttons

The following table describes the common buttons available on the web UI.

Button	Description
Refresh	It is used to update the content of the current page.
Save	It is used to save the configuration on the current page and enable the configuration to take effect.
Cancel	It is used to go back to the original configuration without saving the configuration on the current page.
?	It is used to view help information corresponding to the settings on the current page.

4 Quick setup

4.1 Overview

This module enables you to quickly configure the device or change the working mode of the base station to deploy your wireless network.

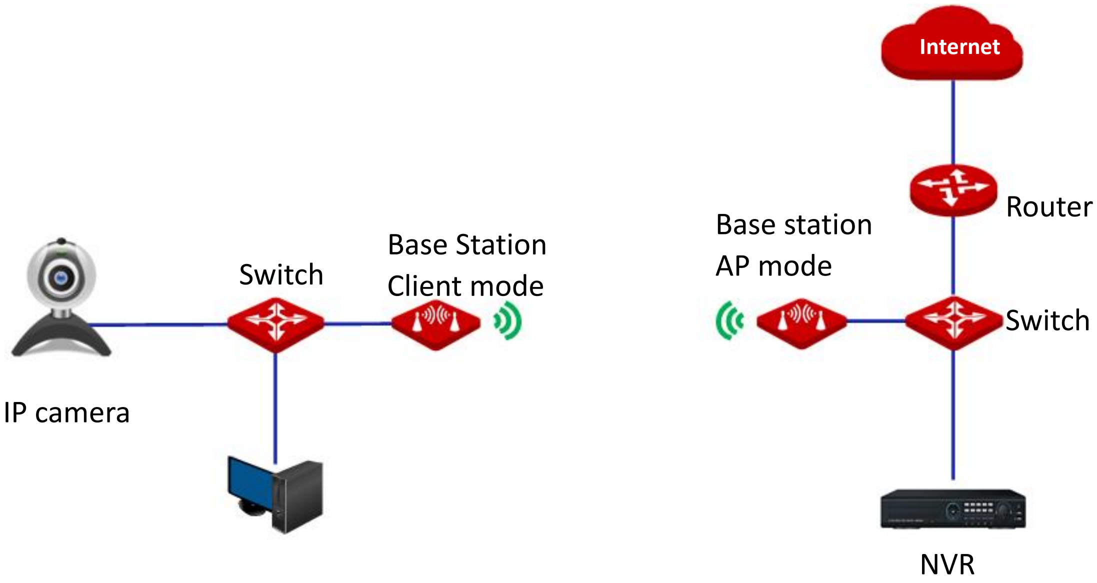
The base station supports the following working modes:

- AP: In this mode, the device creates a wireless network based on the current wired network.
- Client: In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
- Universal Repeater: In this mode, this device extends an existing wireless network for broader network coverage.
- WISP: In this mode, this device connects to a hotspot provided by ISP in wireless manner, and provides the wireless network.
- Repeater: In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
- P2MP: In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
- Router: In this mode, the device connects to a modem in wired manner, and provides a wireless network.

4.2 AP mode

In **AP** mode, this device connects to a wired network, and provides a wireless access point for wireless clients.

The base station in **AP** mode usually works with another base station in **Client** mode to establish a PTP network, such as point to point connection between ISP control center and transit signal tower. The network topology is shown as below:

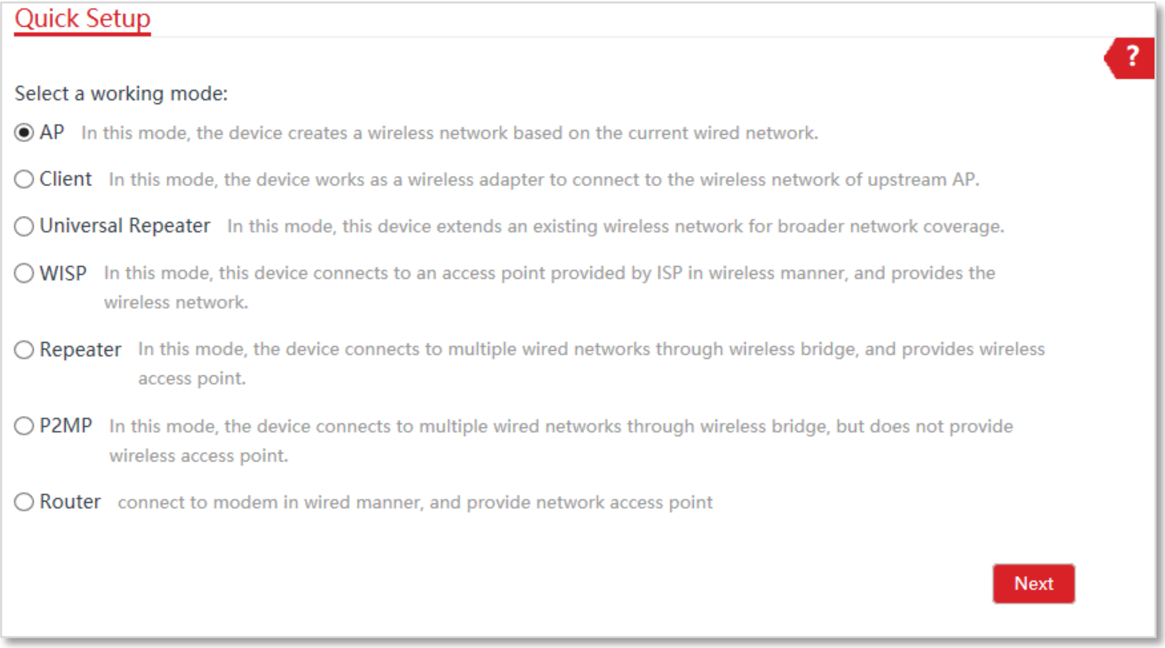


Configuration procedure

1 Start a web browser on the computer connected to Base Station 1, and visit **192.168.2.1**.

2 Choose **Quick Setup** to enter the configuration page.

3 Select **AP** mode and click **Next**.



Quick Setup

Select a working mode:

● AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

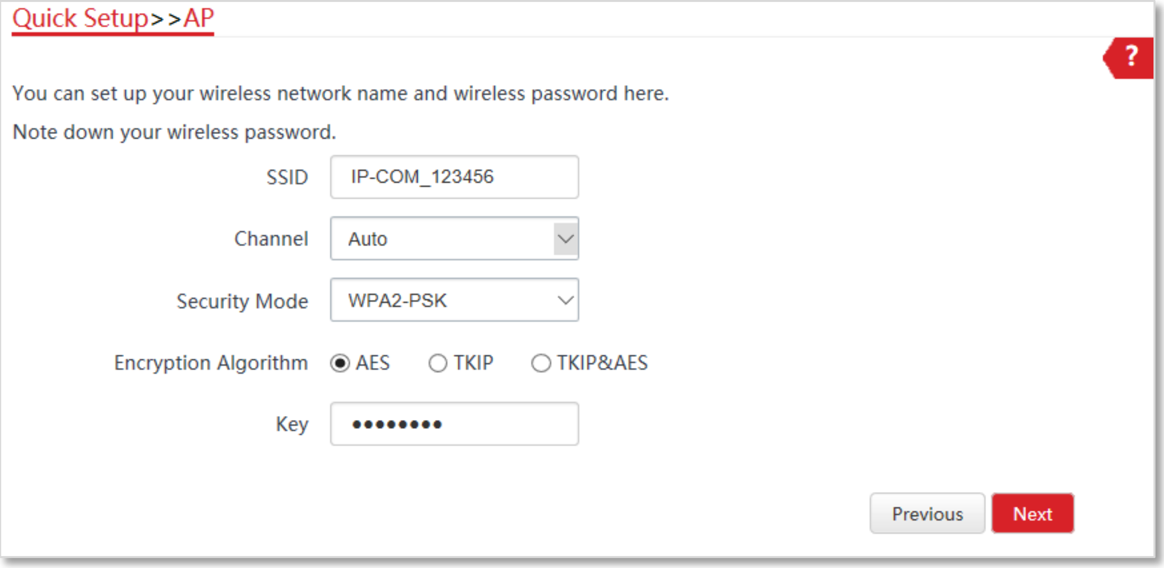
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

4 Set an **SSID**, **Security Mode**, which are **IP-COM_123456** and **WPA2-PSK** in this example, and **Key**, and click **Next**.



Quick Setup>>AP

You can set up your wireless network name and wireless password here.

Note down your wireless password.

SSID: IP-COM_123456

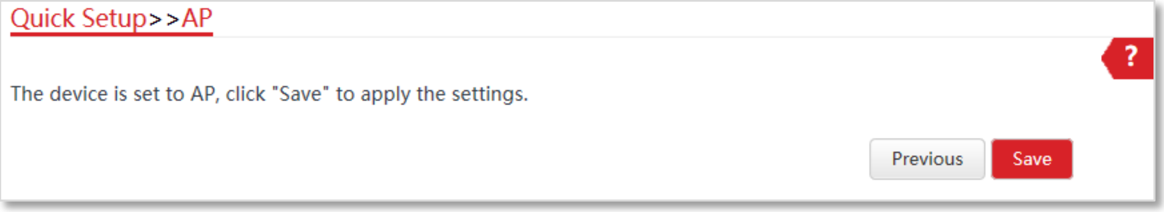
Channel: Auto

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ●●●●●●●●●

5 Click **Save**, and wait until the device reboots automatically to activate the settings.



Quick Setup>>AP

The device is set to AP, click "Save" to apply the settings.

---End

Parameters description

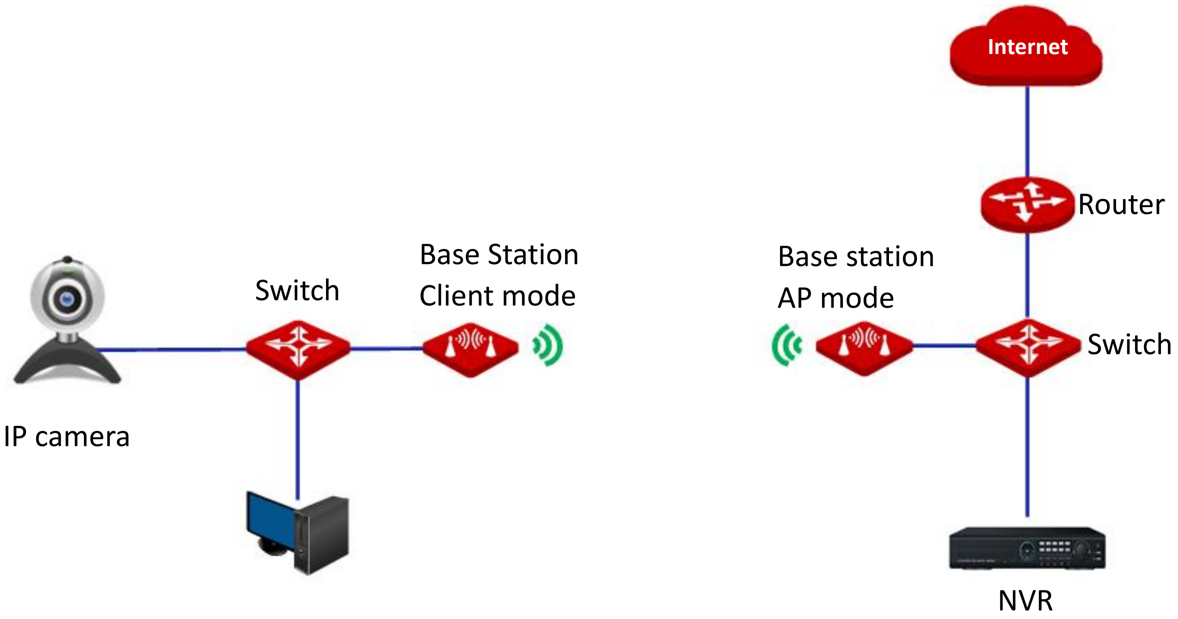
Parameter	Description
Working modes	It specifies the working mode of this device. **AP** mode: In this mode, the device creates a wireless network based on the current wired network.
SSID	It specifies the wireless network name of this device.
Channel	It specifies the operating channel of this device. Select a less used channel in the ambient environment to reduce interference. **Auto** (Default): It indicates that the device automatically adjusts its operating channel according to the ambient environment.
Security Mode	It specifies the security mode of the wireless network, including: None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.
Encryption Algorithm	It specifies the encryption method of the wireless network. **AES**: It indicates the Advanced Encryption Standard.

Parameter	Description
	TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless rate of the device is limited to 54 Mbps. **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies the WiFi password of the wireless network.

4.3 Client mode

In **Client** mode, this device serves as a wireless adapter, and connects to a wireless network of upstream AP. The base station is unable to be connected by wireless devices in this mode.

The device in **Client** mode usually works with the device in **AP** mode for PTP backhaul connection.

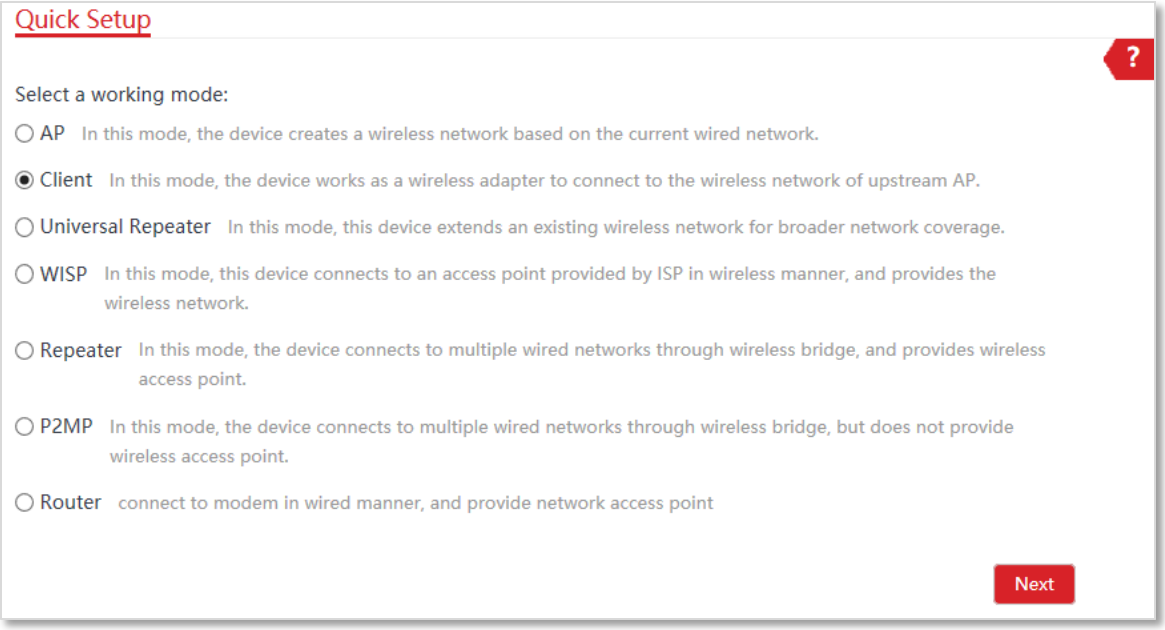


Configuration procedure

1 Start a web browser on the computer connected to Base Station 2, and visit **192.168.2.1**.

2 Choose **Quick Setup** to enter the configuration page.

3 Select **Client**, and click **Next**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

● Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

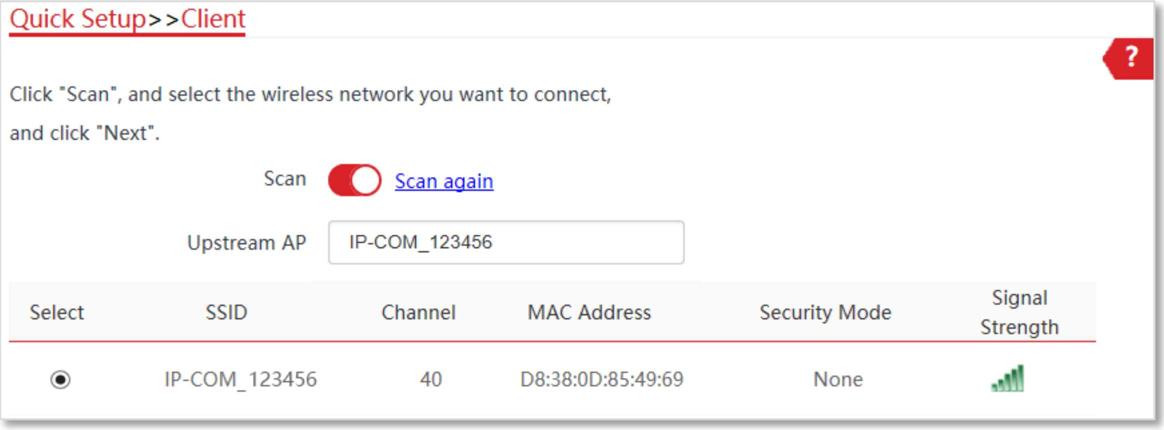
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

4 Select the SSID of the Base Station 1, which is **IP-COM_123456** in this example, and click **Next** at the bottom of the page.



Quick Setup>>Client

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan ● Scan again

Upstream AP: IP-COM_123456

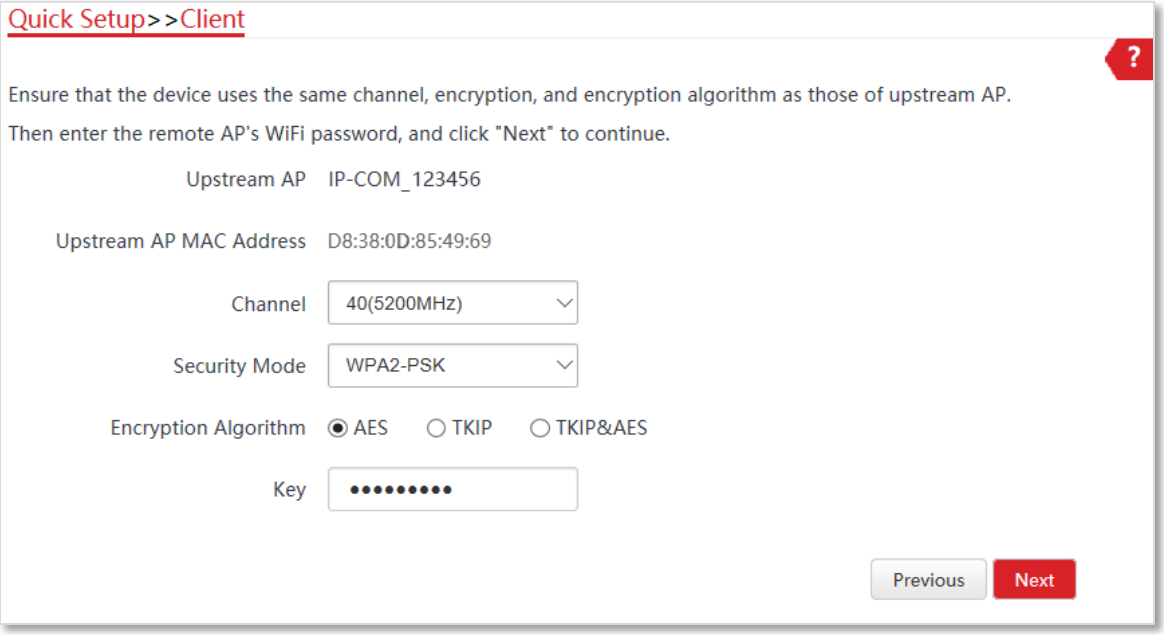
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	IP-COM_123456	40	D8:38:0D:85:49:69	None	

Tip

– If you cannot find any SSID from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.

– If you cannot find the SSID of the Base Station 1 from the list, adjust the direction of base station in **Client** mode, and move it close to the Base Station 1.

5 Enter the WiFi password you set on the Base Station 1 in the **Key** input box, and click **Next**.



Quick Setup>>Client

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of upstream AP. Then enter the remote AP's WiFi password, and click "Next" to continue.

Upstream AP: IP-COM_123456

Upstream AP MAC Address: D8:38:0D:85:49:69

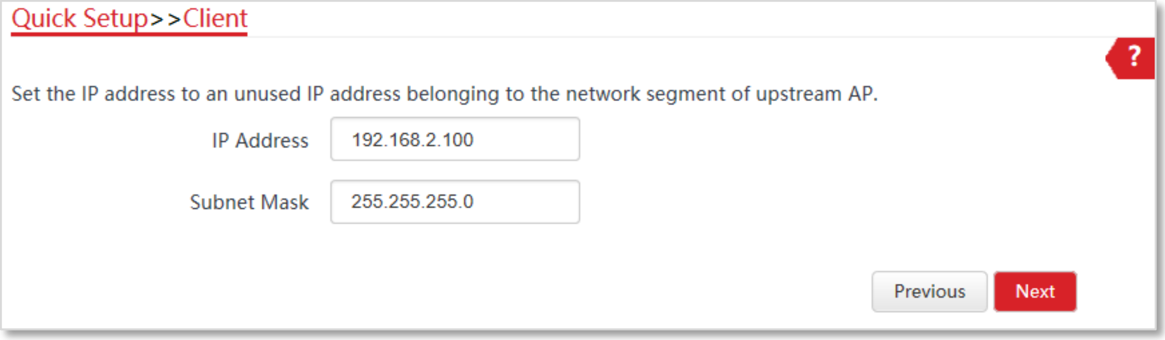
Channel: 40(5200MHz)

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••••

6 Set the IP address to an unused IP address belonging to the same network segment of the Base Station 1. For example, if the IP address of the Base Station 1 is **192.168.2.1**, you can set the IP address of this base station to 192.168.2.*X* (*X* ranges from 2 to 254). Then click **Next**.



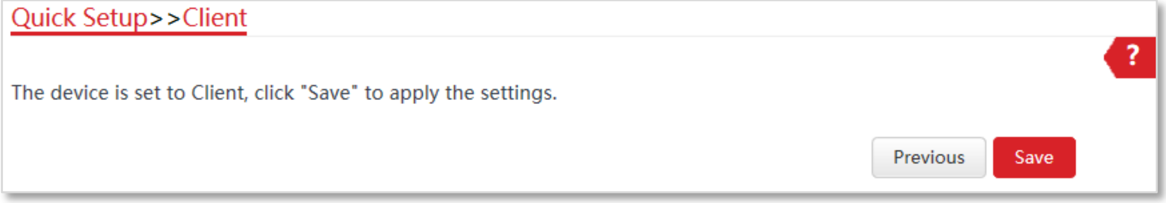
Quick Setup>>Client

Set the IP address to an unused IP address belonging to the network segment of upstream AP.

IP Address: 192.168.2.100

Subnet Mask: 255.255.255.0

7 Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Client

The device is set to Client, click "Save" to apply the settings.

----End

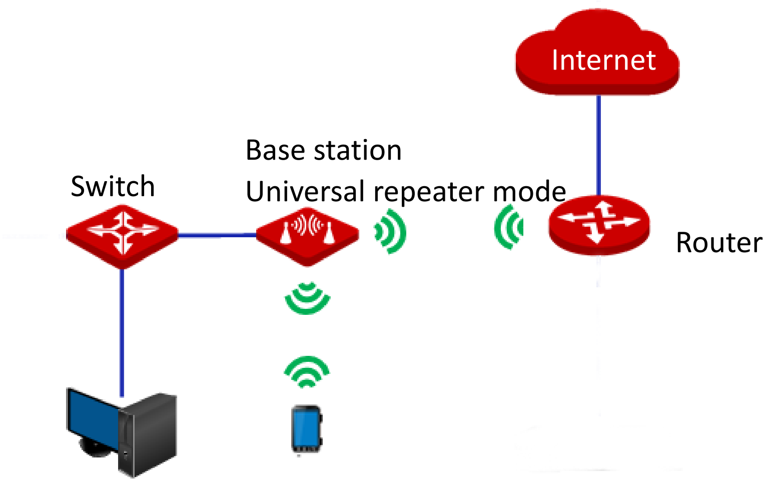
When the LED1, LED2, and LED3 of the Base Station 1 are solid on, and LED1, LED2, and LED3 of this base station are blinking, the bridging succeeds.

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **Client** mode: In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless network.
Upstream AP	It specifies the SSID (wireless network name) of the upstream AP.
Channel	It specifies the operating channel of the device, which is the same as its upstream AP to be bridged.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

4.4 Universal repeater mode

In **Universal Repeater** mode, this device bridges to an upstream AP to expand your existing WiFi network for broader network coverage.

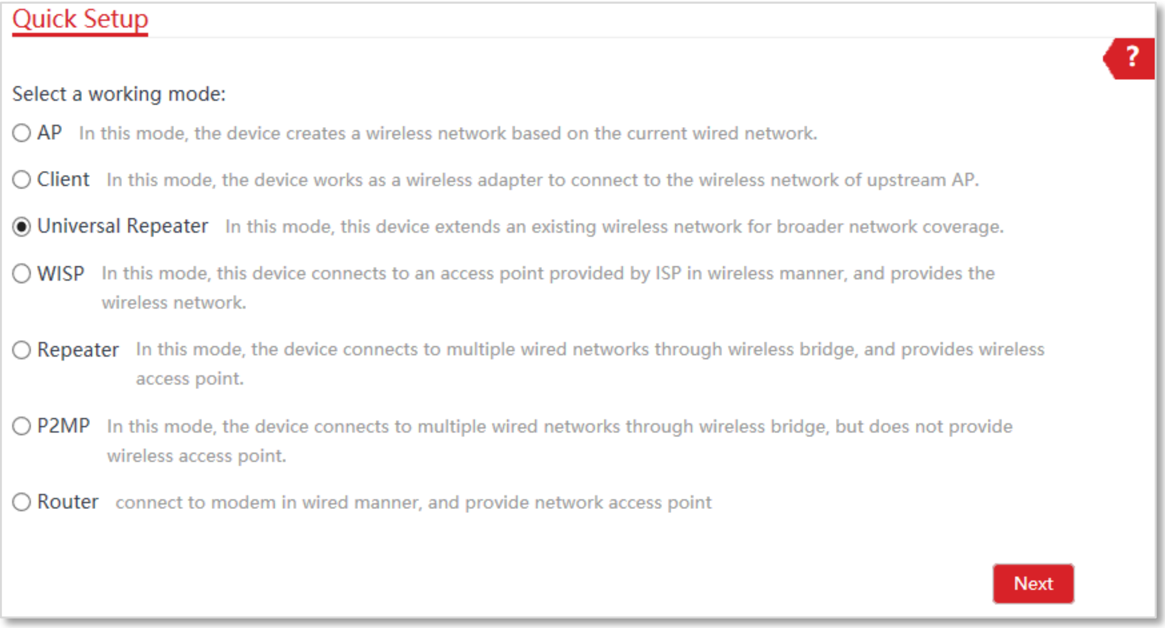


Configuration procedure

1 Start a web browser on the computer connected to the base station, and visit **192.168.2.1**.

2 Choose **Quick Setup** to enter the configuration page.

3 Select **Universal Repeater**, and click **Next**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

● Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

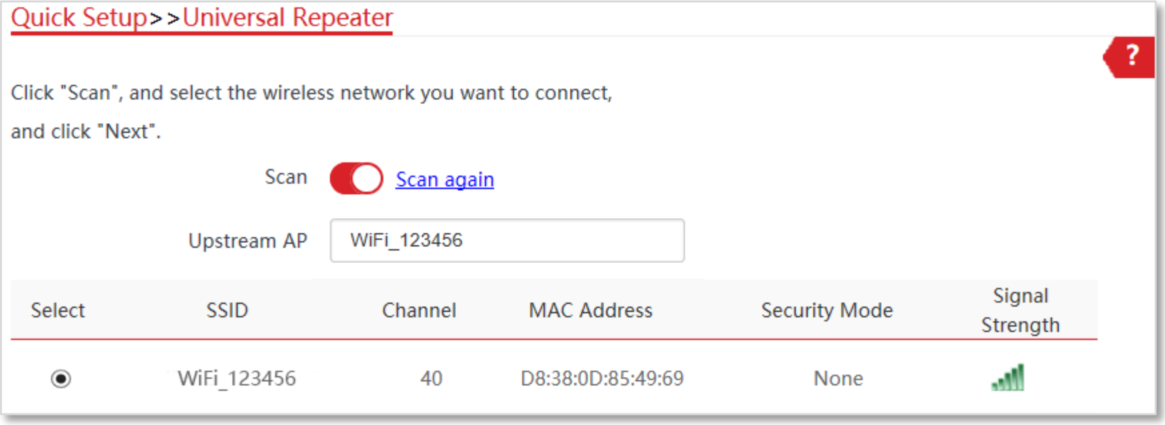
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

4 Select the SSID of the upstream AP, which is **WiFi_123456** in this example, and click **Next** at the bottom of the page.



Quick Setup>>Universal Repeater

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan ● Scan again

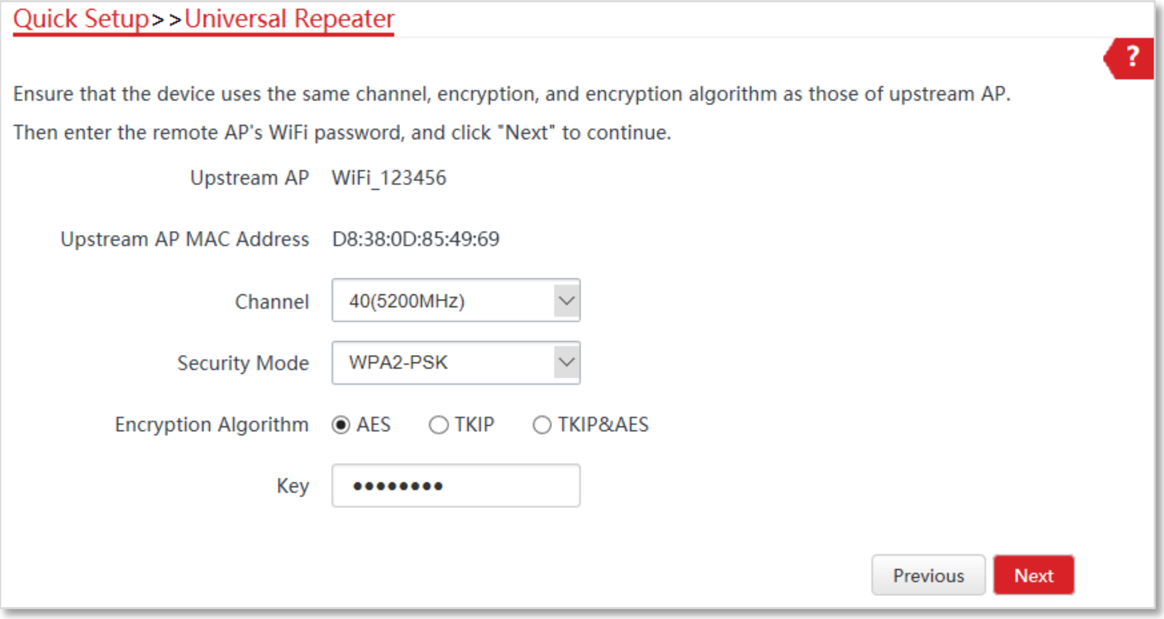
Upstream AP: WiFi_123456

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	WiFi_123456	40	D8:38:0D:85:49:69	None	

Tip

If you cannot find the SSID of your router from the list, ensure that the 5 GHz WiFi network of the router is enabled. Only the WiFi networks at 5 GHz band can be scanned by the base station.

5 Enter the WiFi password of the upstream AP in the **Key** input box, and click **Next**.



Quick Setup>>Universal Repeater

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of upstream AP. Then enter the remote AP's WiFi password, and click "Next" to continue.

Upstream AP: WiFi_123456

Upstream AP MAC Address: D8:38:0D:85:49:69

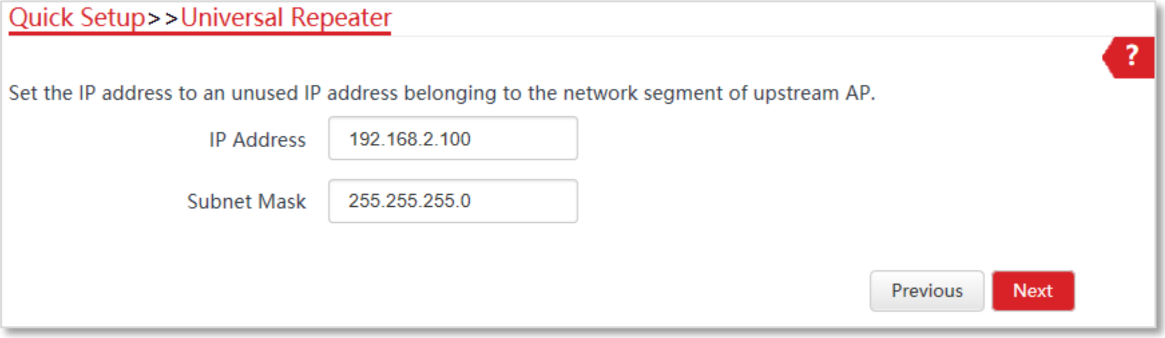
Channel: 40(5200MHz)

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

6 Set the IP address to an unused IP address belonging to the same network segment of the upstream AP. For example, if the IP address of the router is **192.168.2.1**, you can set this device's IP address to 192.168.2.*X* (*X* ranges from 2 to 254). Then click **Next**.



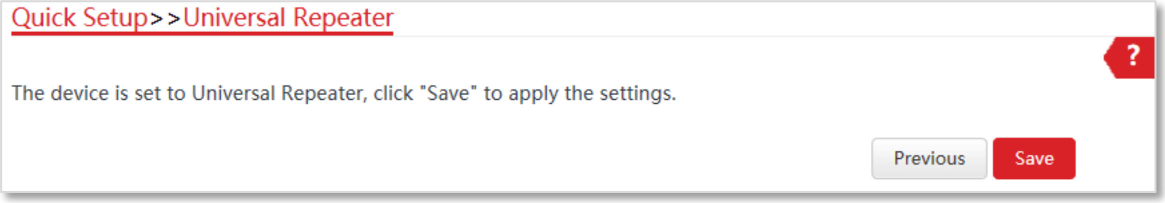
Quick Setup>>Universal Repeater

Set the IP address to an unused IP address belonging to the network segment of upstream AP.

IP Address: 192.168.2.100

Subnet Mask: 255.255.255.0

7 Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Universal Repeater

The device is set to Universal Repeater, click "Save" to apply the settings.

---End

When the LED1, LED2, and LED3 are blinking, the bridging succeeds. The WiFi name and password of the device are the same as those of the router.

To access the internet with:

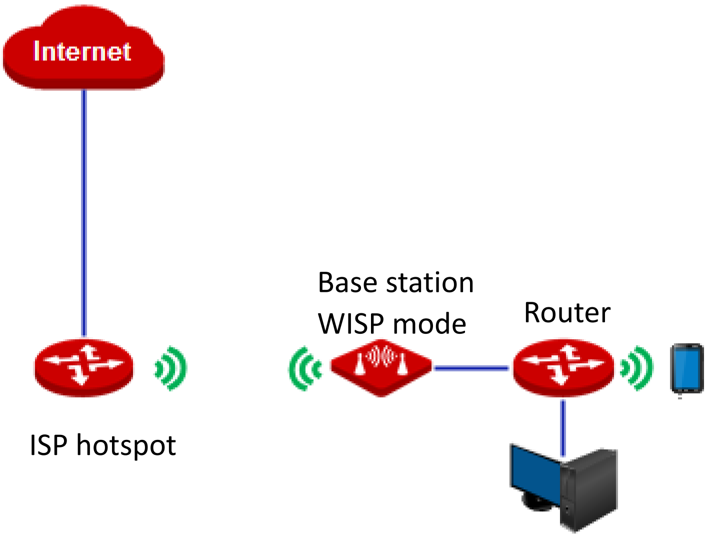
- Wireless devices: Connect the wireless devices, such as a smartphone, to the WiFi network of the base station using the SSID and key of the upstream AP.
- Wired devices: Connect the wired devices, such as a computer, to the LAN port of the power adapter, or the switch connected to the LAN port of the power adapter.

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **Universal Repeater** mode: In this mode, the device expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function.
Upstream AP	It specifies the SSID (wireless network name) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

4.5 WISP mode

In **WISP** mode, this device connects to a hotspot provided by ISP (Internet Service Provider) in wireless manner, and allows the wired and wireless devices to connect to the internet.



Configuration procedure

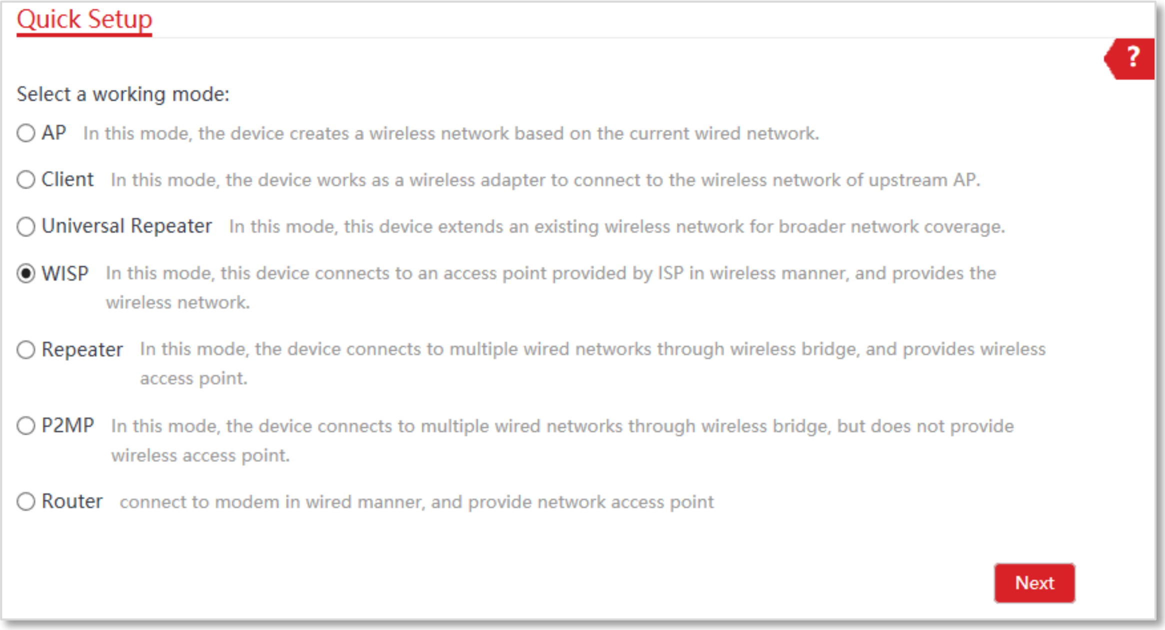
Assume that the SSID and internet parameters of the ISP hotspot are:

- **SSID**: WiFi_123456, no WiFi password
- **Internet connection type**: PPPoE
- **PPPoE user name/password**: admin/admin

1 Start a web browser on the computer connected to the base station, and visit **192.168.2.1**.

2 Choose **Quick Setup** to enter the configuration page.

3 Select **WISP**, and click **Next**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

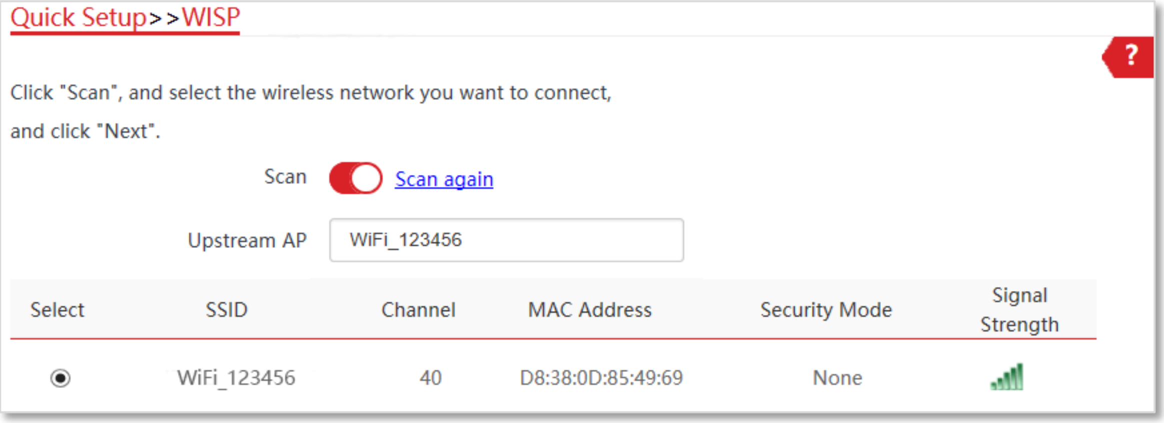
● WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

4 Select the SSID of your ISP hotspot, which is **WiFi_123456** in this example, and click **Next** at the bottom of the page.



Quick Setup>>WISP

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan: on Scan again

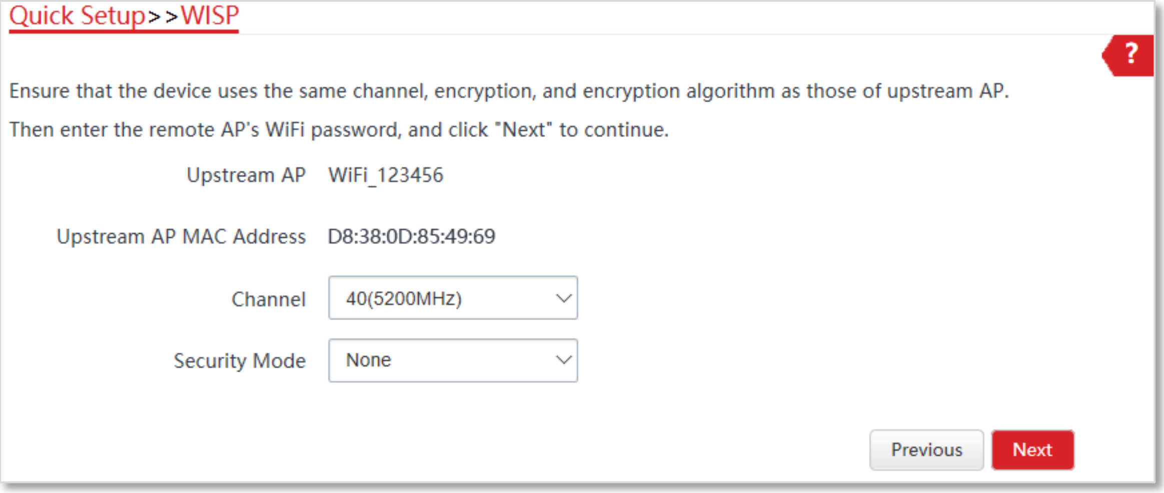
Upstream AP: WiFi_123456

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	WiFi_123456	40	D8:38:0D:85:49:69	None	

Tip

If you cannot find the ISP hotspot from the list, ensure that the hotspot is at 5 GHz band. Only the WiFi networks at 5 GHz band can be scanned by the base station.

5 Click **Next**.



Quick Setup>>WISP

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of upstream AP. Then enter the remote AP's WiFi password, and click "Next" to continue.

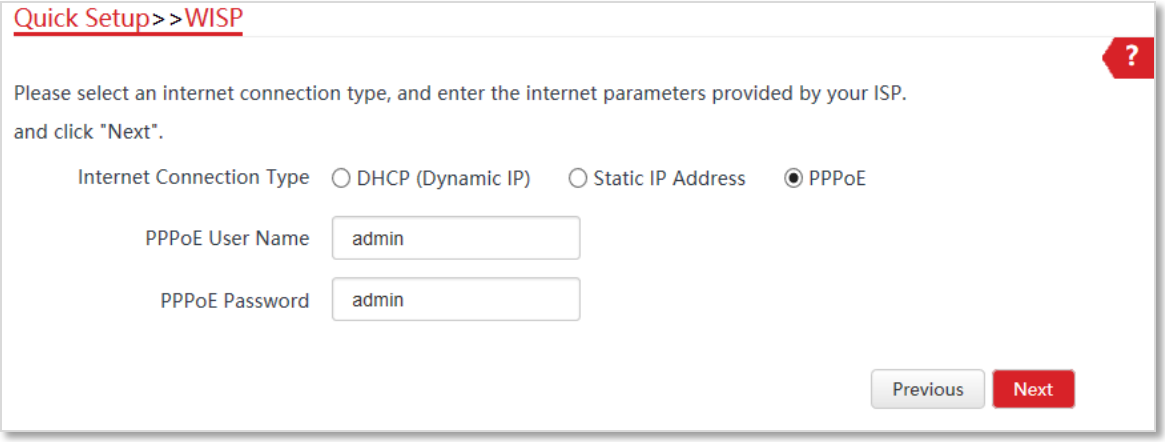
Upstream AP: WiFi_123456

Upstream AP MAC Address: D8:38:0D:85:49:69

Channel: 40(5200MHz)

Security Mode: None

6 Select **PPPoE**, enter the PPPoE user name and password provided by your ISP, both are **admin** in this example, and click **Next**.



Quick Setup>>WISP

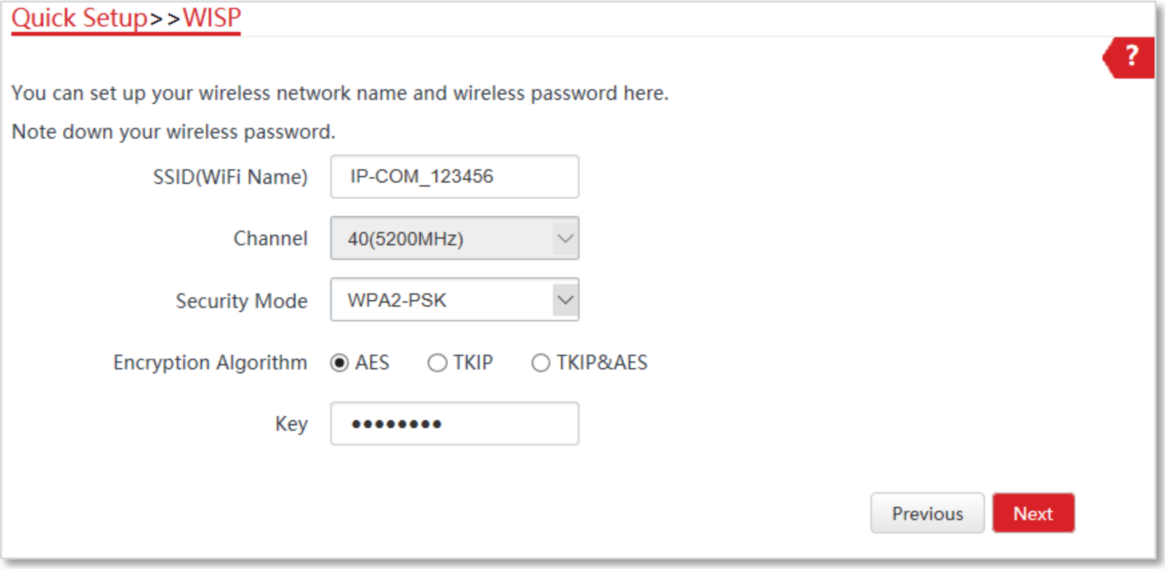
Please select an internet connection type, and enter the internet parameters provided by your ISP.
and click "Next".

Internet Connection Type ○ DHCP (Dynamic IP) ○ Static IP Address ● PPPoE

PPPoE User Name admin

PPPoE Password admin

7 Customize the **SSID** and **Key**, and click **Next**.



Quick Setup>>WISP

You can set up your wireless network name and wireless password here.
Note down your wireless password.

SSID(WiFi Name) IP-COM_123456

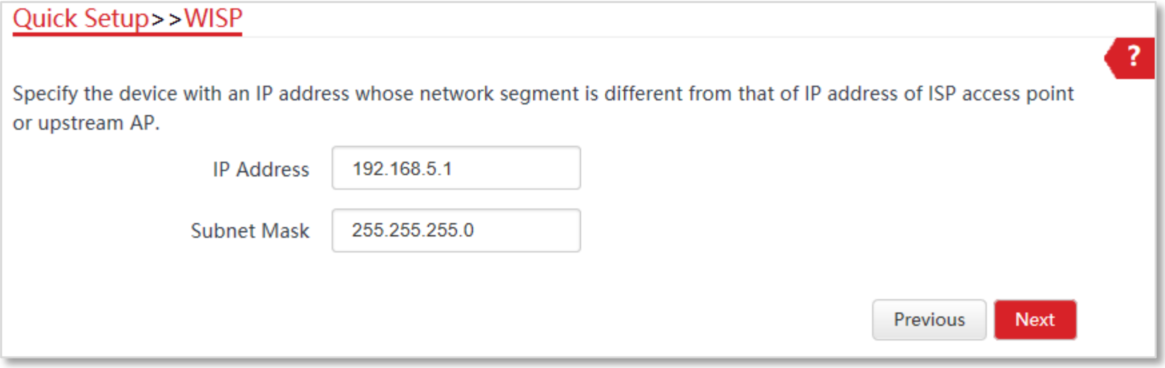
Channel 40(5200MHz)

Security Mode WPA2-PSK

Encryption Algorithm ● AES ○ TKIP ○ TKIP&AES

Key ••••••••

8 Set an IP address belonging to a different network segment from that of your ISP hotspot. For example, if the IP address of your ISP hotspot is **192.168.2.1**, you can set this device's IP address to 192.168.*X*.1 (*X* ranges from 0 to 254 excluding 2) which is also the login IP address of the base station. Then click **Next**.



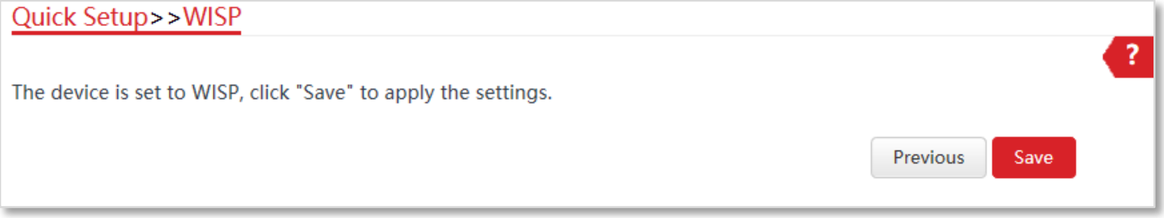
Quick Setup>>WISP

Specify the device with an IP address whose network segment is different from that of IP address of ISP access point or upstream AP.

IP Address 192.168.5.1

Subnet Mask 255.255.255.0

9 Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>WISP

The device is set to WISP, click "Save" to apply the settings.

---End

When LED1, LED2, and LED3 of the base station are blinking, the device is connected to your ISP hotspot successfully.

To access the internet with:

- Wireless devices: Connect the wireless devices, such as a smartphone, to the WiFi network of the base station using the **SSID** and **Key** you set for the base station.
- Wired devices: Connect the wired devices, such as a computer, to the LAN port of the power adapter, or the switch connected to the LAN port of the power adapter.

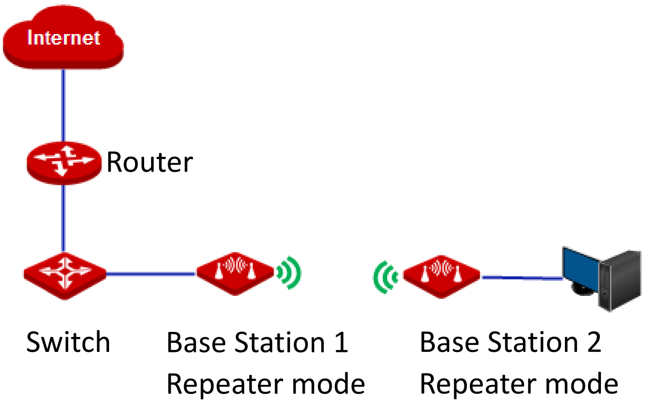
Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **WISP** mode: In this mode, the device connects to the hotspot provided by the wireless internet service provider (WISP), and offers a separate WiFi network.
Upstream AP	It specifies the SSID (wireless network name) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network of the device. It includes None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.
Internet Connection Type	− **DHCP (Dynamic IP)**: The device obtains an IP address and other parameters from the DHCP server of upstream device for internet access. − **Static IP Address**: The device accesses the internet by setting the IP address, subnet mask, default gateway and DNS server IP addresses manually. − **PPPoE**: The device accesses the internet using the PPPoE user name and password provided by the ISP.

4.6 Repeater mode

In **Repeater** mode, this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use this function, the peer AP is required to support WDS function.

Configuration procedure of peer to peer bridging



Assume that the wireless parameters are as follows:

Base Station 1

- **SSID**: IP-COM_123456
- **Channel**: 40
- **Security mode**: WEP
- **Authentication type**: Shared
- **Default key**: Key 1, 12345

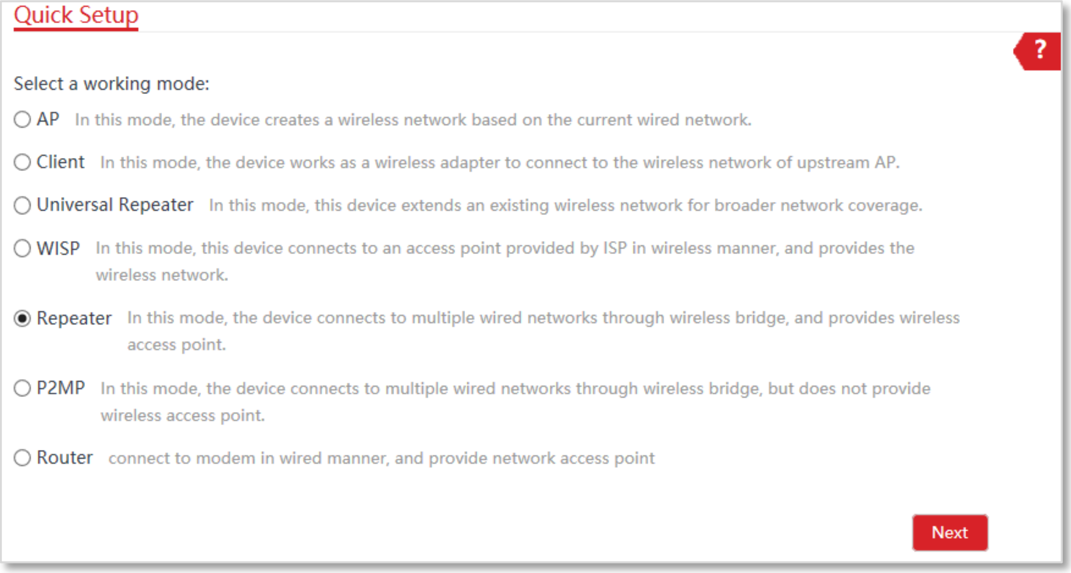
Base Station 2

- **SSID:** IP-COM_654321
- **WLAN MAC Address:** D8:38:0D:15:86:B2

1 Set Base Station 2 to the **Repeater** mode.

(1) Start a web browser on the computer connected to Base Station 2.

(2) Choose **Quick Setup** to enter the configuration page.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

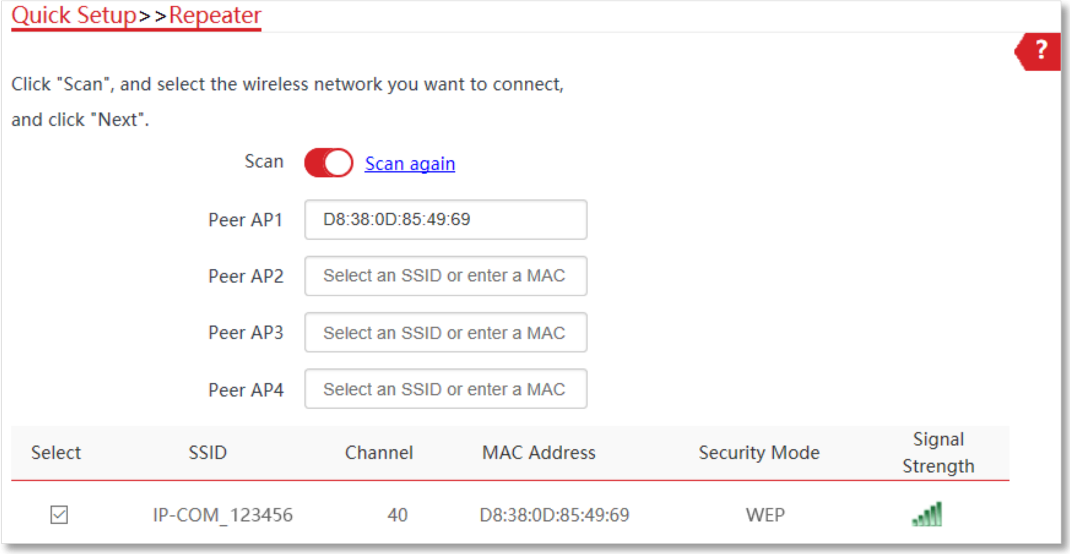
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

● Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

(3) Select the SSID of Base Station 1 from the list, which is **IP-COM_123456** in this example, and click **Next** at the bottom of the page.



Quick Setup>>Repeater

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan: ON Scan again

Peer AP1: D8:38:0D:85:49:69

Peer AP2: Select an SSID or enter a MAC

Peer AP3: Select an SSID or enter a MAC

Peer AP4: Select an SSID or enter a MAC

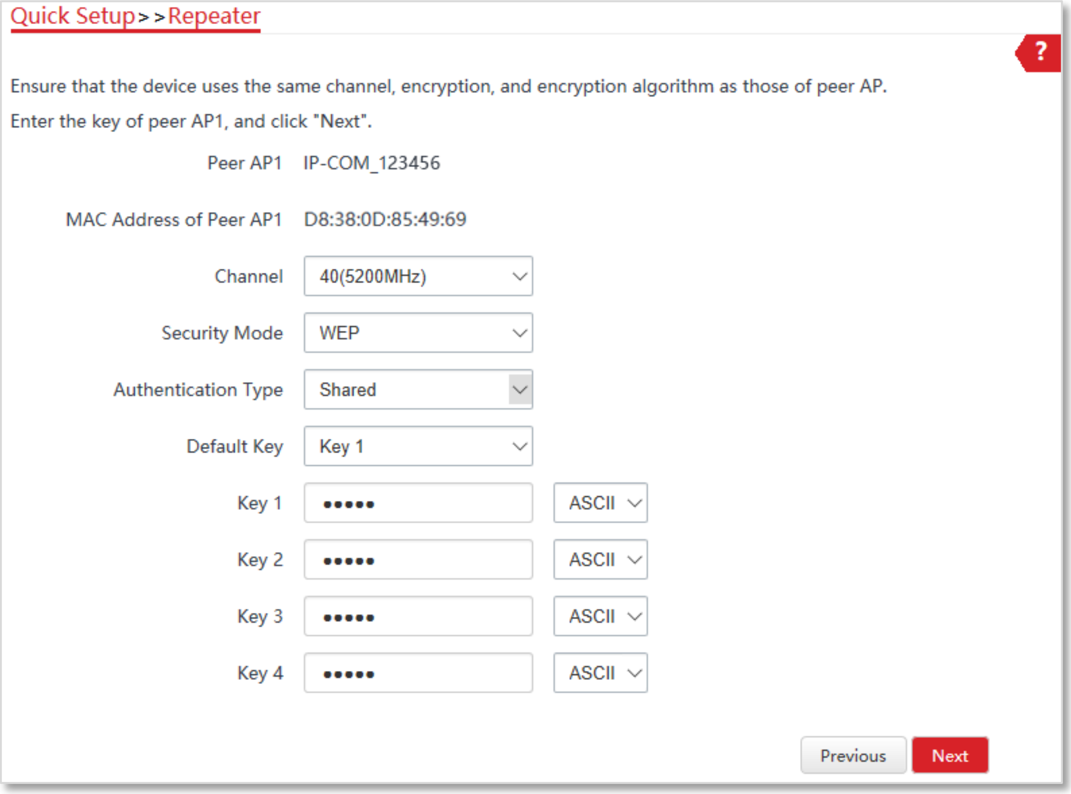
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_123456	40	D8:38:0D:85:49:69	WEP	

Tip

– If you cannot scan the SSID of Base Station 1 from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.

– Only the WiFi networks whose security modes are set to none or WEP can be displayed on the list.

(4) Set the **Authentication Type** and **Default Key** to the same as those of Base Station 1, enter the key 1, and click **Next**.



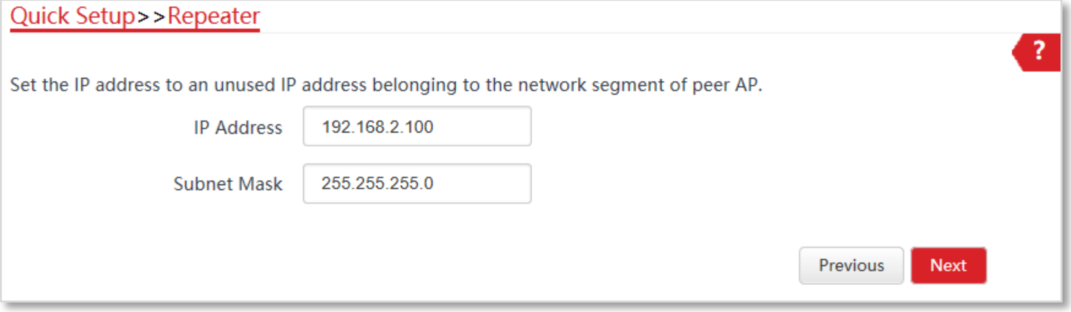
Quick Setup>>Repeater

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of peer AP.

Enter the key of peer AP1, and click "Next".

Peer AP1	IP-COM_123456	
MAC Address of Peer AP1	D8:38:0D:85:49:69	
Channel	40(5200MHz)	
Security Mode	WEP	
Authentication Type	Shared	
Default Key	Key 1	
Key 1	•••••	ASCII
Key 2	•••••	ASCII
Key 3	•••••	ASCII
Key 4	•••••	ASCII

(5) Set the IP address to an unused IP address belonging to the same network segment as that of Base Station 1. For example, if the IP address of Base Station 1 is **192.168.2.1**, you can set this device's IP address to 192.168.2.*X* (*X* ranges from 2 to 254). Then click **Next**.

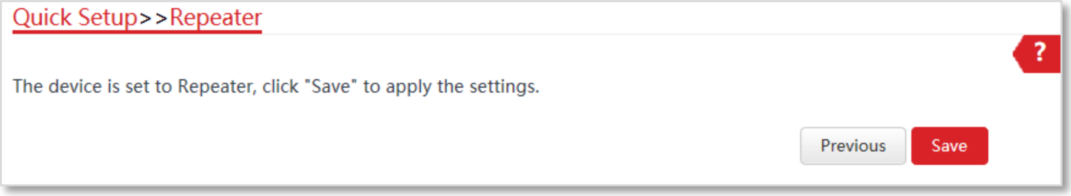


Quick Setup>>Repeater

Set the IP address to an unused IP address belonging to the network segment of peer AP.

IP Address	192.168.2.100
Subnet Mask	255.255.255.0

(6) Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Repeater

The device is set to Repeater, click "Save" to apply the settings.

2 Perform the procedure in step 1 above to set the Base Station 1 to **Repeater** mode. The differences are list below:

- Select the SSID of Base Station 2, which is **IP-COM_654321** in this example.
- Do not need to change the IP address of Base Station 1.

Tip

If there are multiple wireless networks with the same SSID, select the one with the WLAN MAC address of the Base Station 2, which is **D8:38:0D:15:86:B2** in this example.

---End

To check whether the bridging is successful:

Method 1: When the LED1, LED2, and LED3 indicators of Base Station 1 and Base Station 2 are solid on, the bridging succeeds.

Method 2:

1 Start a web browser on the computer which is connected to Base Station 1 and visit its IP address.

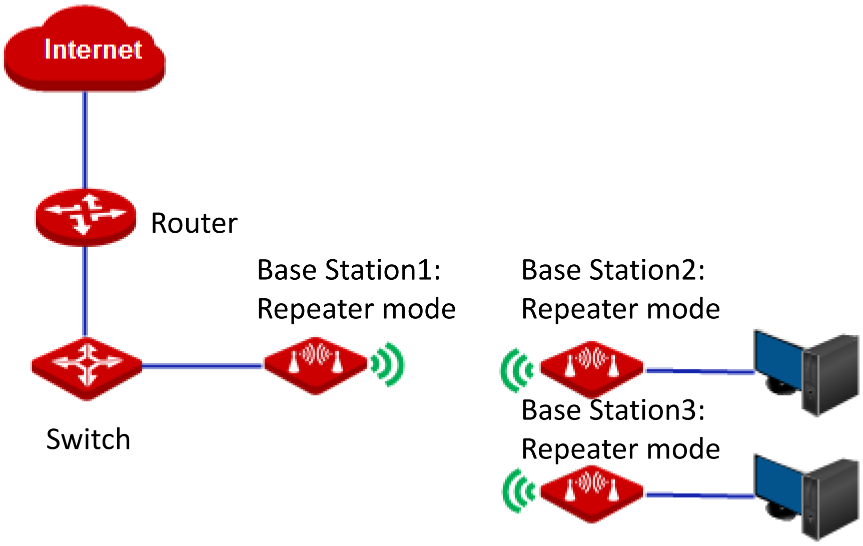
2 Choose **Advanced** > **Diagnose**, select **Ping** from the **Diagnose** drop-down list menu, enter the IP address of Base Station 2 and click **Start**.

The bridging is successful when the ping succeeds.

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **Repeater** mode: In this mode, the device can connect 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device.
Peer AP	It displays the SSID (wireless network name) of the peer AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. Tip The Repeater mode only supports WEP and None security modes.

Configuration procedure of peer to multiple peers briding



Assume that the wireless parameters are shown as follows:

Base Station 1:

- **IP Address**: 192.168.2.1
- **SSID**: IP-COM_123456
- **Channel**: 40
- **Security mode**: None

Base Station 2:

- **SSID:** IP-COM_1
- **WLAN MAC address:** D8:38:0D:7F:80:C9
- **Channel**: 40
- **Security mode**: None

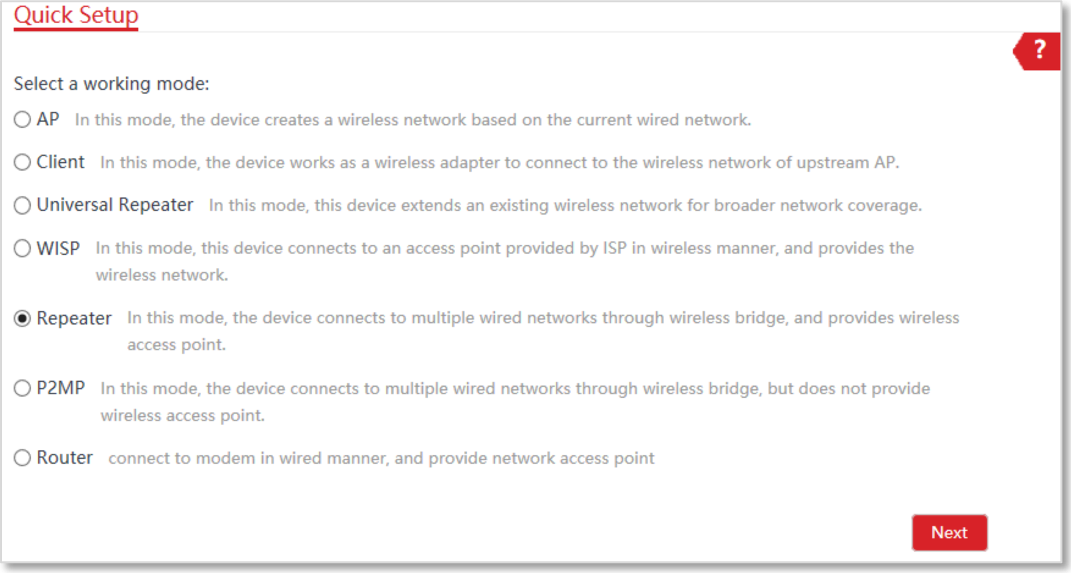
Base Station 3:

- **SSID:** IP-COM_2
- **WLAN MAC address:** D8:38:0D:85:49:29
- **Channel**: 40
- **Security mode**: None

1 Set the Base Station 2 to the **Repeater** mode.

(1) Start a web browser on the computer connected to Base Station 2, and visit **192.168.2.1**.

(2) Choose **Quick Setup**, and select **Repeater**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

● Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

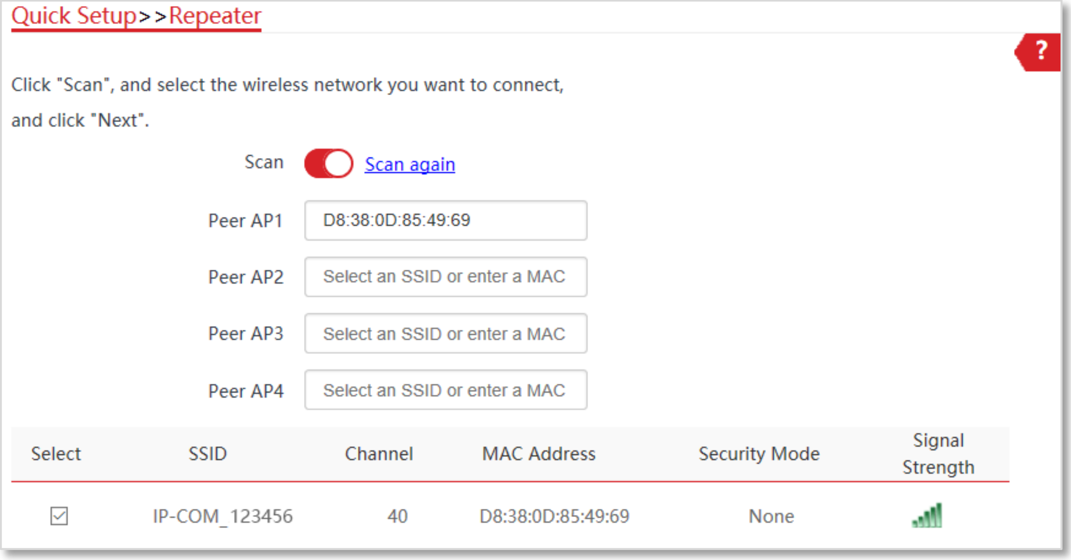
○ Router connect to modem in wired manner, and provide network access point

(3) Select the SSID of Base Station 1 from the list, which is **IP-COM_123456** in this example, and click **Next** at the bottom of the page.

Tip

– If you cannot scan the SSID of Base Station 1 from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.

– Only the WiFi networks whose security modes are set to none or WEP can be displayed on the list.



Quick Setup>>Repeater

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan: on, Scan again

Peer AP1: D8:38:0D:85:49:69

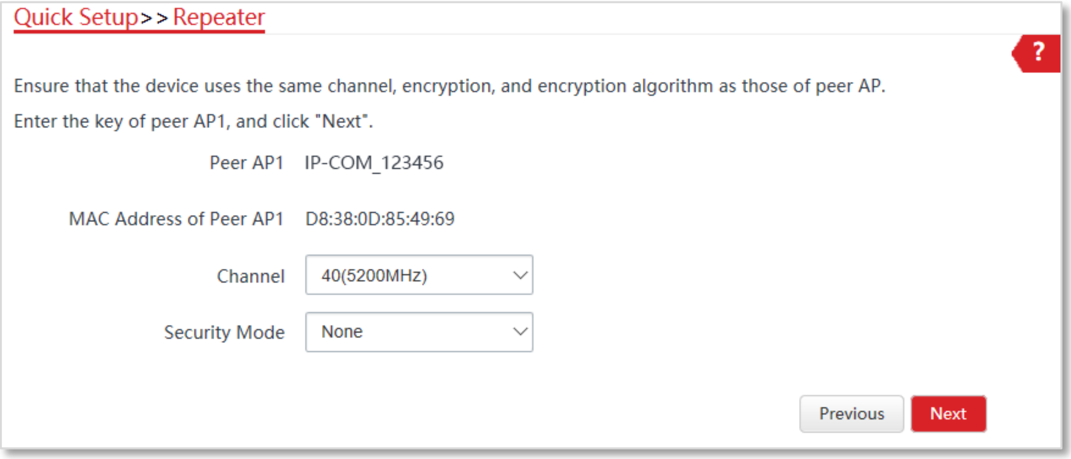
Peer AP2: Select an SSID or enter a MAC

Peer AP3: Select an SSID or enter a MAC

Peer AP4: Select an SSID or enter a MAC

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_123456	40	D8:38:0D:85:49:69	None	

(4) Click **Next** directly on the following page.



Quick Setup>>Repeater

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of peer AP.

Enter the key of peer AP1, and click "Next".

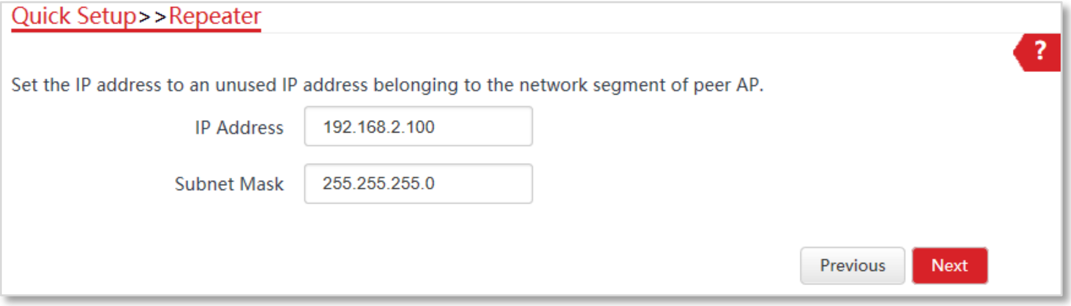
Peer AP1 IP-COM_123456

MAC Address of Peer AP1 D8:38:0D:85:49:69

Channel 40(5200MHz)

Security Mode None

(5) Set the IP address to an unused IP address belonging to the same network segment as that of Base Station 1. For example, if the IP address of the Base Station 1 is **192.168.2.1**, you can set this device's IP address to 192.168.2.*X* (*X* ranges from 2 to 254). Then click **Next**.



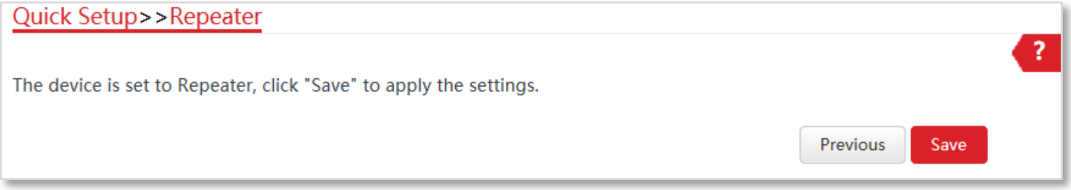
Quick Setup>>Repeater

Set the IP address to an unused IP address belonging to the network segment of peer AP.

IP Address 192.168.2.100

Subnet Mask 255.255.255.0

(6) Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Repeater

The device is set to Repeater, click "Save" to apply the settings.

2 Perform step 1 to set Base Station 3 to **Repeater** mode, and bridge to Base Station 1.

3 Set Base Station 1 to **Repeater** mode and bridge to Base Station 2 and Base Station 3.

(1) Start a web browser on the computer connected to Base Station 1, and visit **192.168.2.1**.

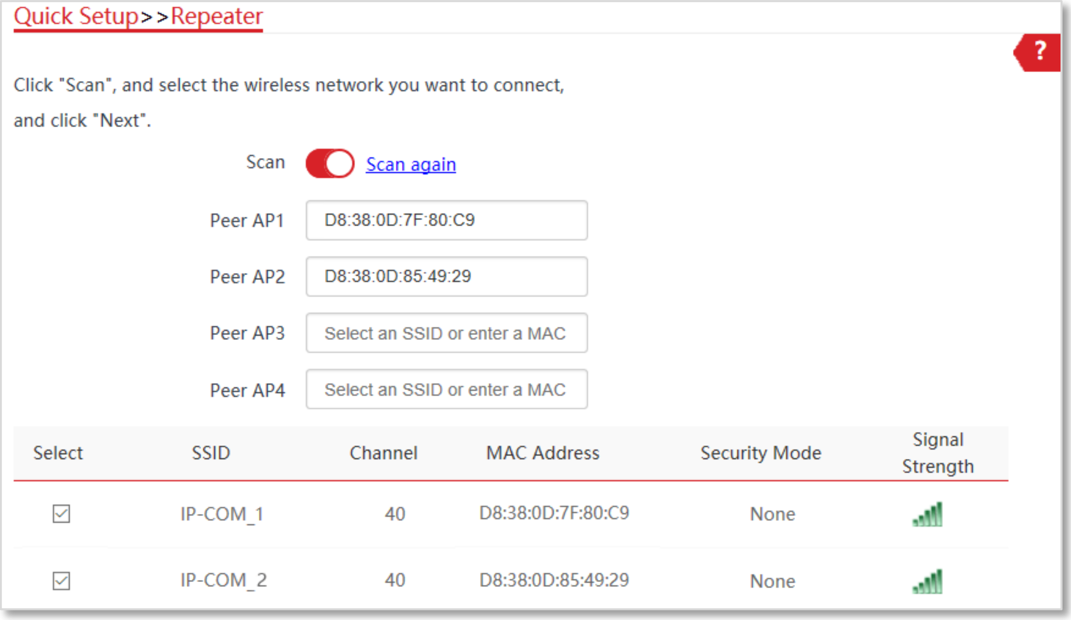
(2) Choose **Quick Setup** to enter the configuration page.

(3) Select **Repeater** mode, and click **Next**.

(4) Select SSIDs of Base Station 2 and Base Station 3, and click **Next** at the bottom of the page.

Tip

If there are multiple wireless networks with the same SSID, select the ones with the WLAN MAC addresses of the Base Station 2 and Base Station 3, which are D8:38:0D:7F:80:C9 and D8:38:0D:85:49:29 in this example.



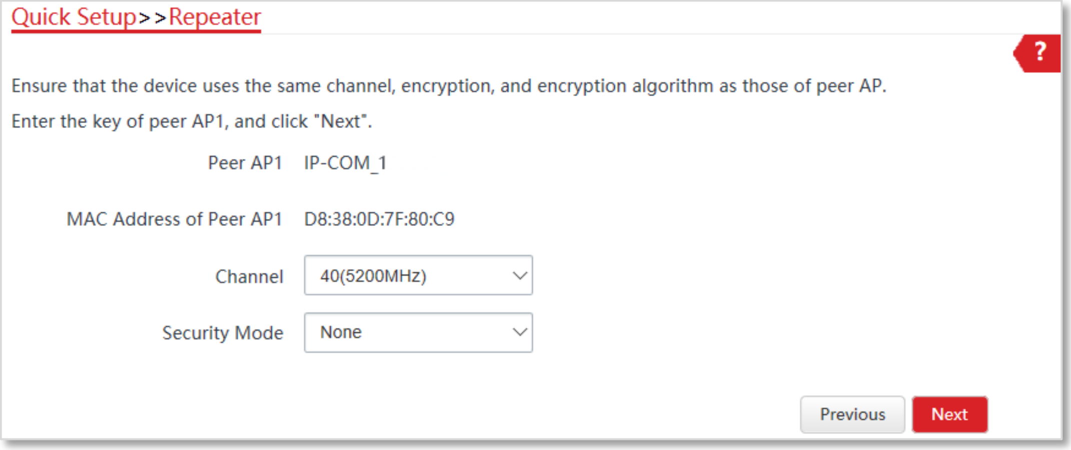
Quick Setup>>Repeater

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan	● Scan again
Peer AP1	D8:38:0D:7F:80:C9
Peer AP2	D8:38:0D:85:49:29
Peer AP3	Select an SSID or enter a MAC
Peer AP4	Select an SSID or enter a MAC

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_1	40	D8:38:0D:7F:80:C9	None	
☑	IP-COM_2	40	D8:38:0D:85:49:29	None	

(5) Click **Next** on the following page.

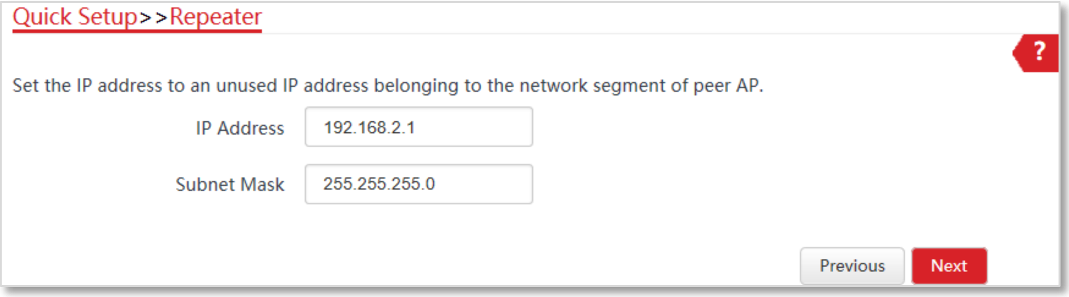


Quick Setup>>Repeater

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of peer AP. Enter the key of peer AP1, and click "Next".

Peer AP1	IP-COM_1
MAC Address of Peer AP1	D8:38:0D:7F:80:C9
Channel	40(5200MHz)
Security Mode	None

(6) Click **Next**.

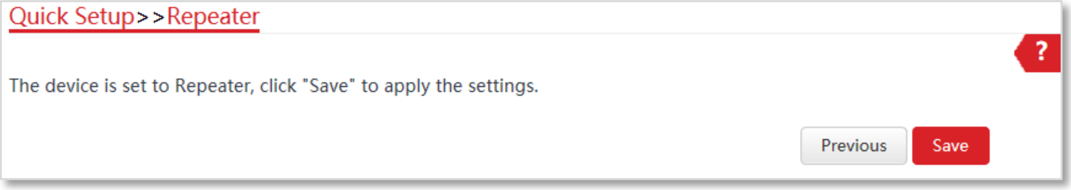


Quick Setup>>Repeater

Set the IP address to an unused IP address belonging to the network segment of peer AP.

IP Address	192.168.2.1
Subnet Mask	255.255.255.0

(7) Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Repeater

The device is set to Repeater, click "Save" to apply the settings.

---End

To check whether the bridging is successful:

Method 1: When the LED1, LED2, and LED3 indicators of Base Station 1, Base Station 2 and Base Station 3 are solid on, the bridging succeeds.

Method 2:

1 Start a web browser on the computer which is connected to Base Station 1 and visit its IP address.

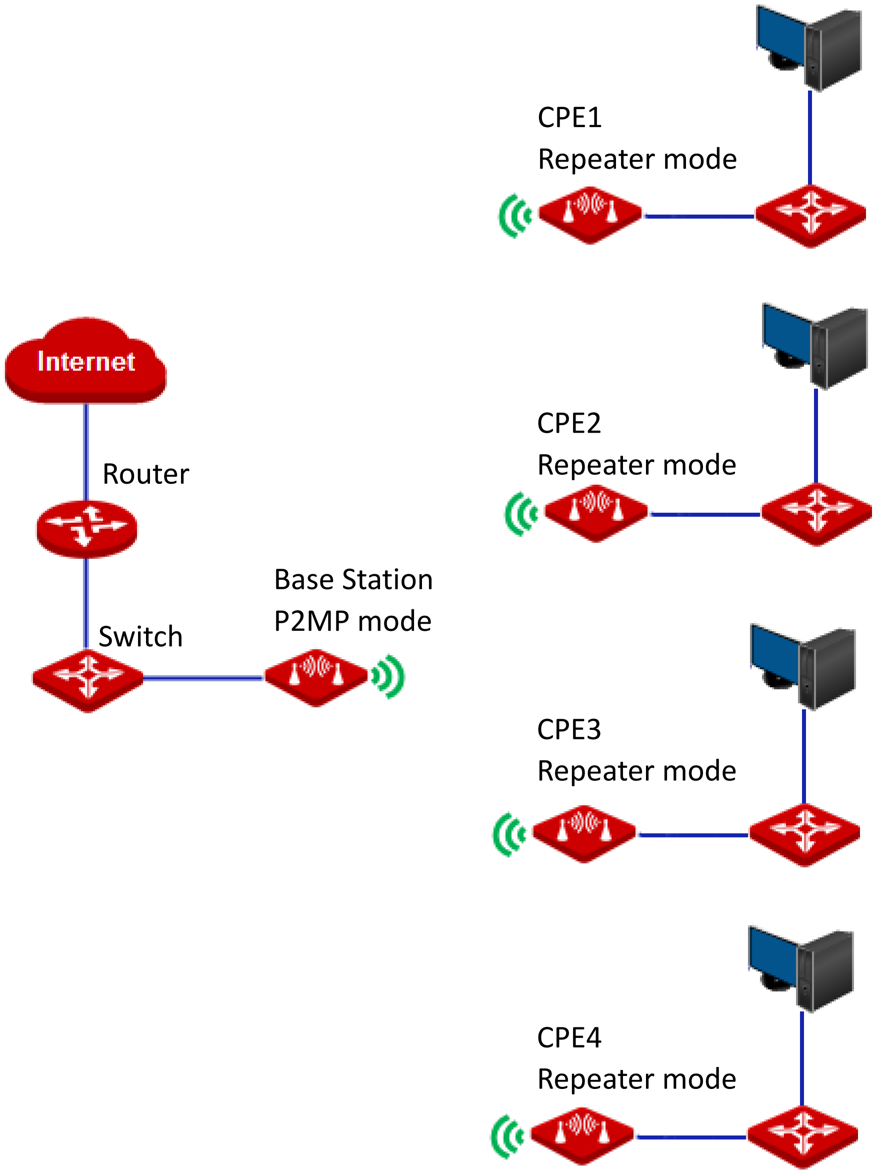
2 Choose **Advanced** > **Diagnose**, select **Ping** from the **Diagnose** drop-down list menu, enter the IP address of Base Station 2 and Base Station 3 respectively, and click **Start**.

The bridging is successful when the ping succeeds.

4.7 P2MP mode

In **P2MP** mode, this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected to wireless clients.

The configuration procedure of P2MP mode is similar with Repeater mode. In the following example, the Base Station works in P2MP mode, and bridges to four CPEs work in Repeater mode.



Assume that the related parameters are shown as follows:

Base Station:

- **IP Address**: 192.168.2.1
- **SSID**: IP-COM_1
- **Channel**: 40
- **Security Mode**: None

CPE1 to CPE4:

CPE	SSID	WLAN MAC address
CPE1	IP-COM_2	D8:38:0D:85:49:69
CPE2	IP-COM_3	D8:38:0D:7F:80:C9
CPE3	IP-COM_4	D8:38:0D:85:49:29
CPE4	IP-COM_5	D8:38:0D:7F:80:69

Configuration procedure

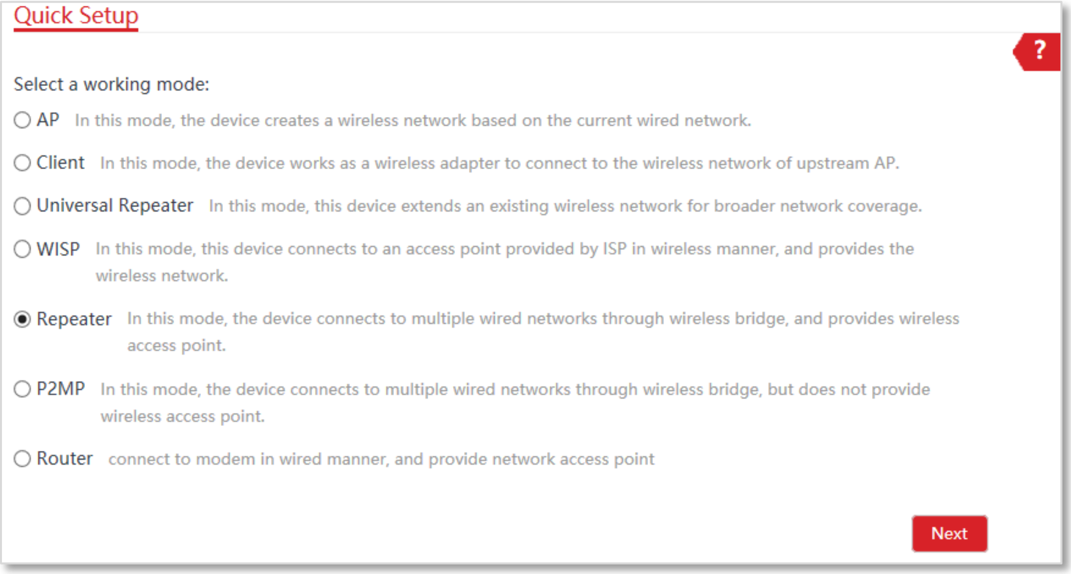
Tip

When setting the Base Station to P2MP mode, ensure that the Base Station and all CPEs operate in the same channel.

1 Set CPE1 to **Repeater** mode and bridge to the Base Station.

(1) Start a web browser on the computer connected to CPE1, and visit **192.168.2.1**.

(2) Choose **Quick Setup**, and select **Repeater**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

● Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

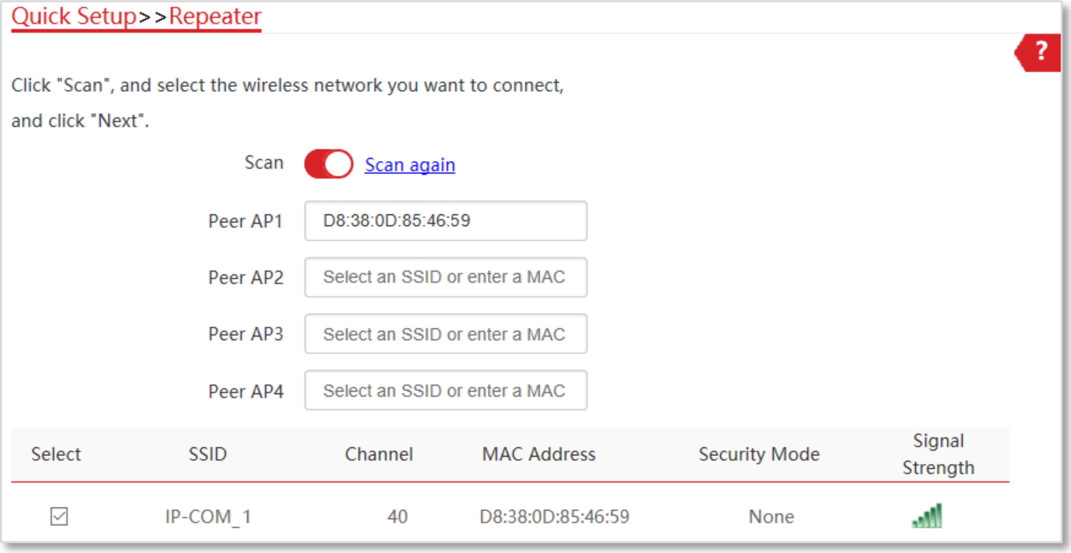
○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

(3) Select the SSID of the Base Station from the list, which is **IP-COM_1** in this example, and click **Next** at the bottom of the page.

Tip

- If you cannot scan the SSID of Base Station 1 from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.
- Only the WiFi networks whose security modes are set to none or WEP can be displayed on the list.



Quick Setup>>Repeater

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan ● Scan again

Peer AP1: D8:38:0D:85:46:59

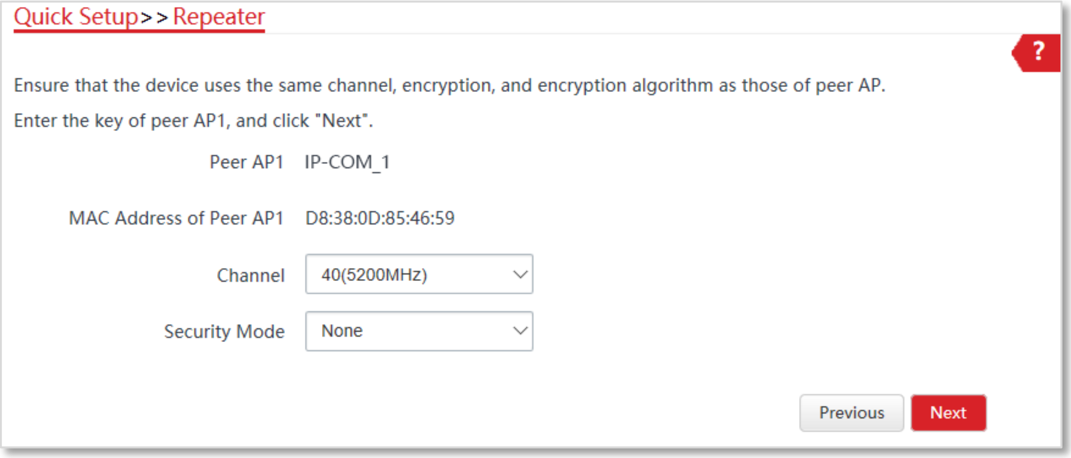
Peer AP2: Select an SSID or enter a MAC

Peer AP3: Select an SSID or enter a MAC

Peer AP4: Select an SSID or enter a MAC

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_1	40	D8:38:0D:85:46:59	None	▂▄▆█

(4) Click **Next** directly on the following page.



Quick Setup>>Repeater

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of peer AP. Enter the key of peer AP1, and click "Next".

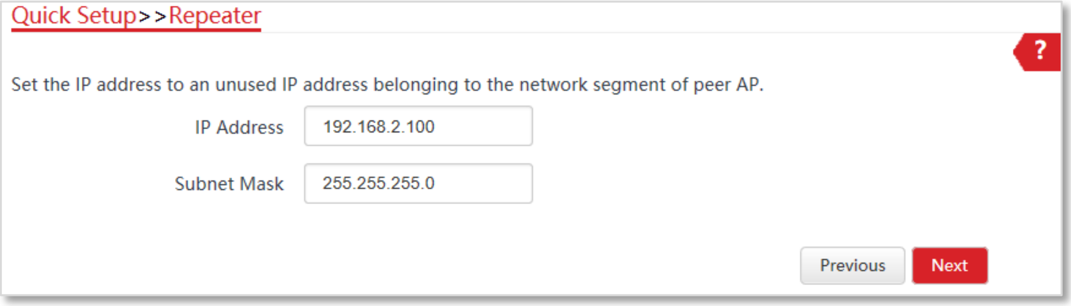
Peer AP1: IP-COM_1

MAC Address of Peer AP1: D8:38:0D:85:46:59

Channel: 40(5200MHz)

Security Mode: None

(5) Set the IP address to an unused IP address belonging to the same network segment as that of the Base Station. For example, if the IP address of the Base Station is **192.168.2.1**, you can set this device's IP address to 192.168.2.*X* (*X* ranges from 2 to 254). Then click **Next**.



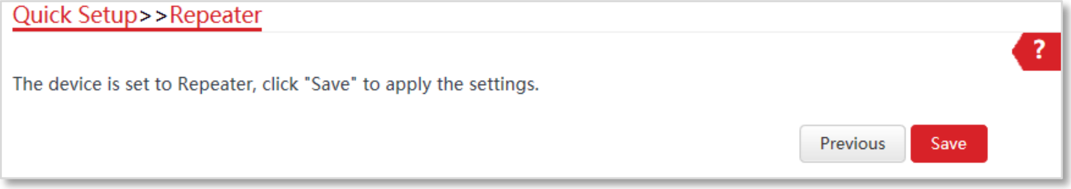
Quick Setup>>Repeater

Set the IP address to an unused IP address belonging to the network segment of peer AP.

IP Address: 192.168.2.100

Subnet Mask: 255.255.255.0

(6) Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Repeater

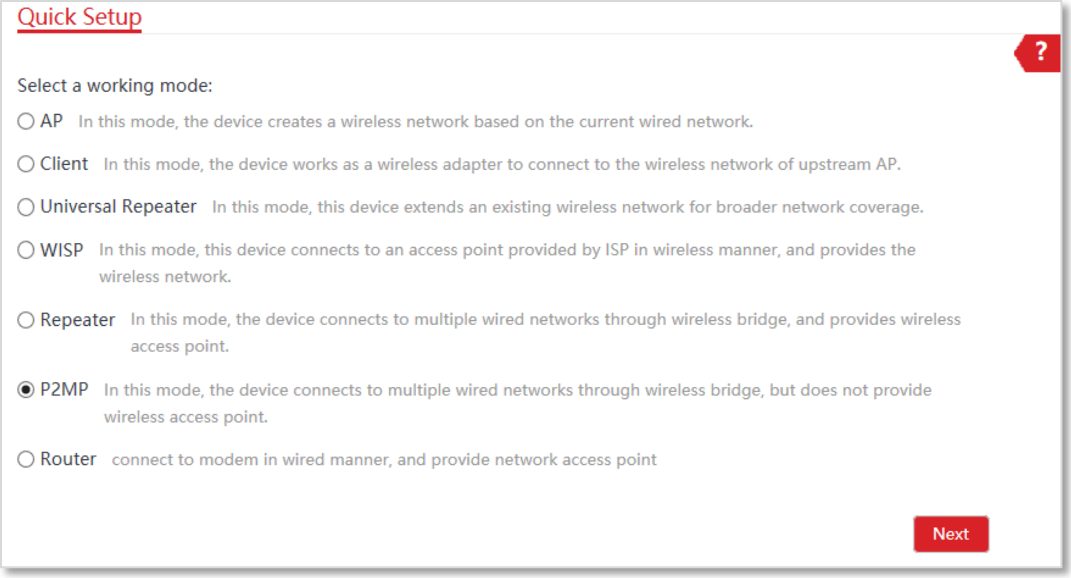
The device is set to Repeater, click "Save" to apply the settings.

2 Perform step 1 to set CPE2, CPE3, and CPE4 to **Repeater** mode, and bridge to the Base Station.

3 Set the Base Station to **P2MP** mode and bridge to the CPE1, CPE2, CPE3, and CPE4.

(1) Start a web browser on the computer connected to the Base Station, and visit **192.168.2.1**.

(2) Choose **Quick Setup**, select **P2MP** mode, and click **Next**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

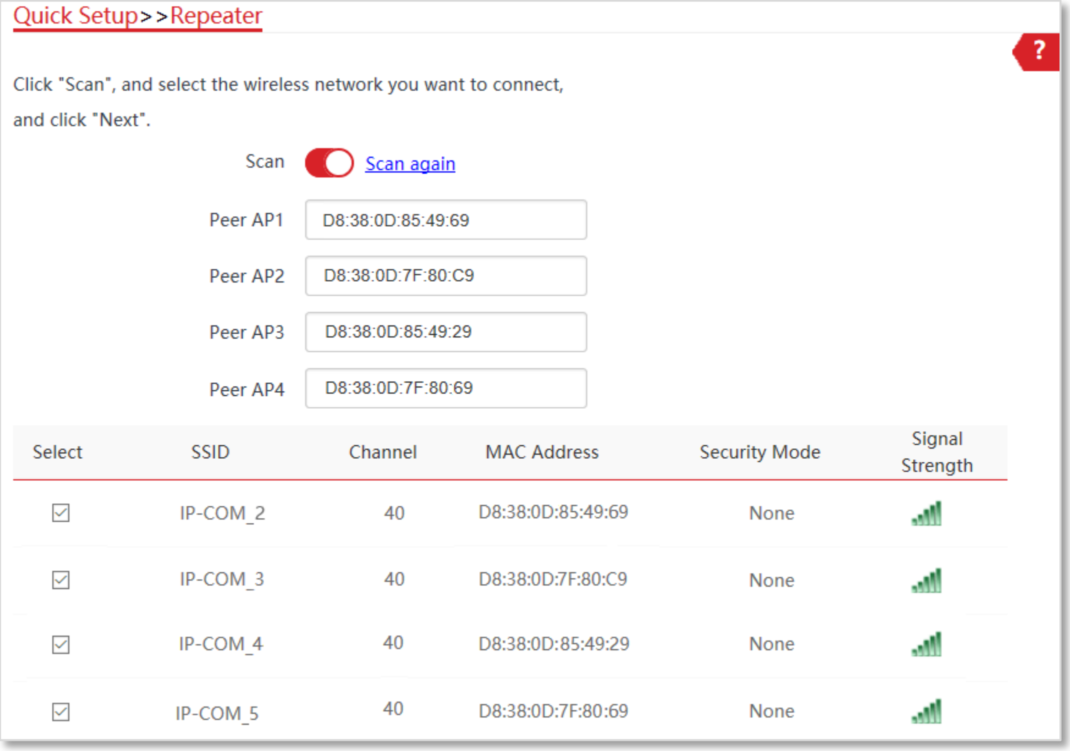
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

● P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

○ Router connect to modem in wired manner, and provide network access point

(3) Select the SSID of CPE1, CPE2, CPE3 and CPE4, which are **IP-COM_2**, **IP-COM_3, IP-COM_4** and **IP-COM_5** in this example, and click **Next** at the bottom of the page.



Quick Setup>>Repeater

Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan ● Scan again

Peer AP1 D8:38:0D:85:49:69

Peer AP2 D8:38:0D:7F:80:C9

Peer AP3 D8:38:0D:85:49:29

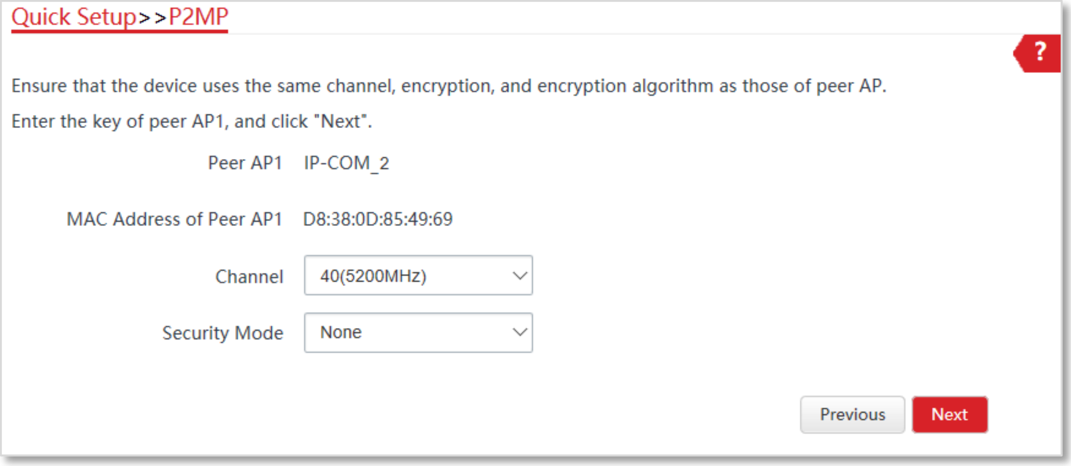
Peer AP4 D8:38:0D:7F:80:69

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_2	40	D8:38:0D:85:49:69	None	▂▄▆█
☑	IP-COM_3	40	D8:38:0D:7F:80:C9	None	▂▄▆█
☑	IP-COM_4	40	D8:38:0D:85:49:29	None	▂▄▆█
☑	IP-COM_5	40	D8:38:0D:7F:80:69	None	▂▄▆█

Tip

- If you cannot find any SSID from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.
- If you cannot find the SSID of Base Station 1 from the list, adjust the direction of Base Station 2, and move it close to the Base Station 1.

(4) Click **Next** on the following page.



Quick Setup>>P2MP

Ensure that the device uses the same channel, encryption, and encryption algorithm as those of peer AP.

Enter the key of peer AP1, and click "Next".

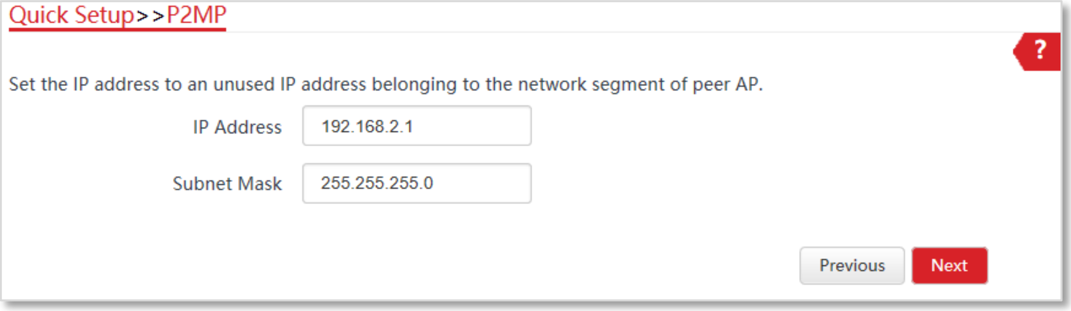
Peer AP1 IP-COM_2

MAC Address of Peer AP1 D8:38:0D:85:49:69

Channel 40(5200MHz)

Security Mode None

(5) Click **Next** on the following page.



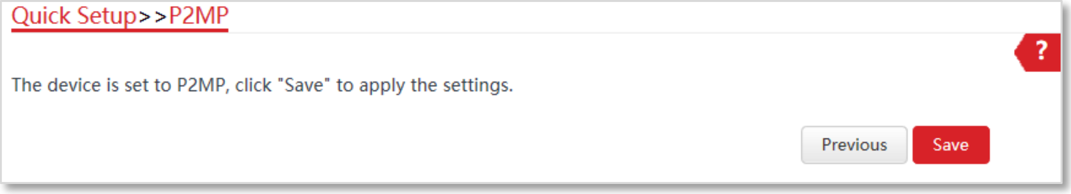
Quick Setup>>P2MP

Set the IP address to an unused IP address belonging to the network segment of peer AP.

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

(6) Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>P2MP

The device is set to P2MP, click "Save" to apply the settings.

---End

To check whether the bridging is successful:

Method 1: When the LED1, LED2, and LED3 indicators CPE1, CPE2, CPE3 and CPE4 are solid on, the bridging succeeds.

Method 2:

1 Start a web browser on the computer which is connected to the Base Station and visit its IP address.

2 Choose **Advanced** > **Diagnose**, select **Ping** from the **Diagnose** drop-down list menu, enter the IP addresses of CPE1, CPE2, CPE3 and CPE4 respectively and click **Start**.

The bridging is successful when the ping succeeds.

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **P2MP** mode: In this mode, the device can connect 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city.
Peer AP	It displays the SSID (wireless network name) of the peer AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. Tip The P2MP mode only supports WEP and None security modes.

4.8 Router mode

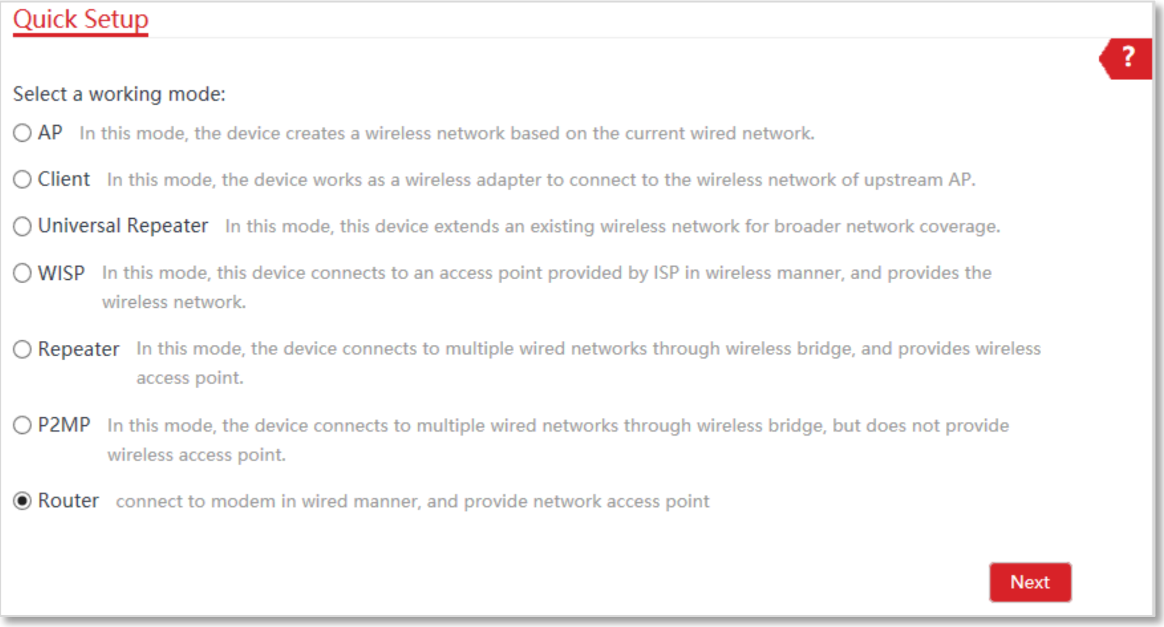
In **Router** mode, this device serves as a router to provide internet access for wired and wireless clients.

Configuration procedure

1 Start a web browser on the computer connected to the base station, and visit **192.168.2.1**.

2 Choose **Quick Setup** to enter the configuration page.

3 Select **Router** mode, and click **Next**.



Quick Setup

Select a working mode:

○ AP In this mode, the device creates a wireless network based on the current wired network.

○ Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.

○ Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.

○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

○ Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.

○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

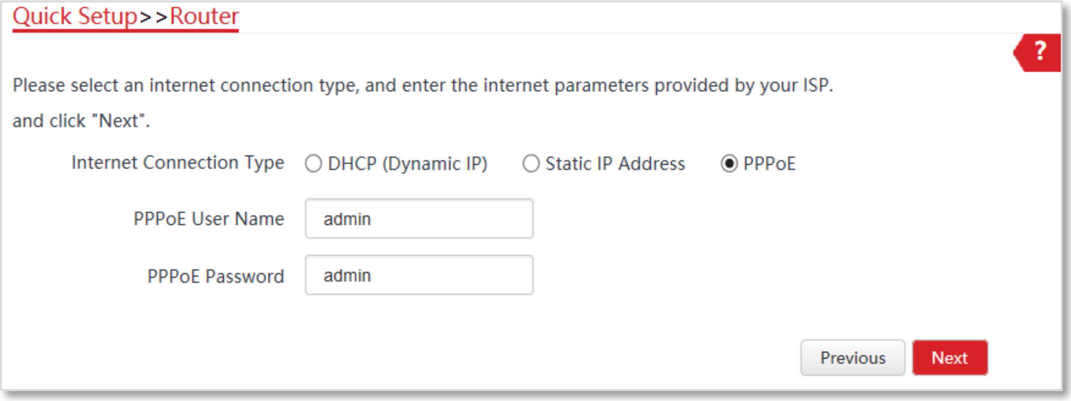
● Router connect to modem in wired manner, and provide network access point

4 Select your **Internet Connection Type**, and set the related parameters. Take **PPPoE** as an example here.

(1) Select **PPPoE**.

(2) Enter the PPPoE user name and password provided by your ISP, which are both **admin** in this example.

(3) Click **Next**.



Quick Setup>>Router

Please select an internet connection type, and enter the internet parameters provided by your ISP. and click "Next".

Internet Connection Type ○ DHCP (Dynamic IP) ○ Static IP Address ● PPPoE

PPPoE User Name admin

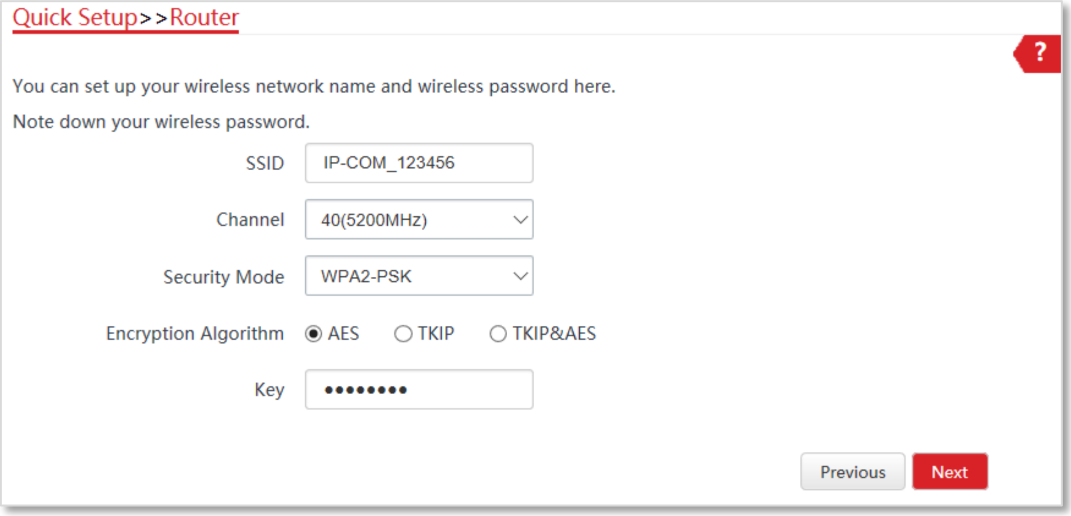
PPPoE Password admin

5 Set wireless parameters of the base station.

(1) Customize a SSID, which is **IP-COM_123456** in this example.

(2) Select a security mode, which is **WPA2-PSK** in this example.

(3) Set a **Key** for the wireless network, and click **Next**.



Quick Setup>>Router

You can set up your wireless network name and wireless password here.

Note down your wireless password.

SSID: IP-COM_123456

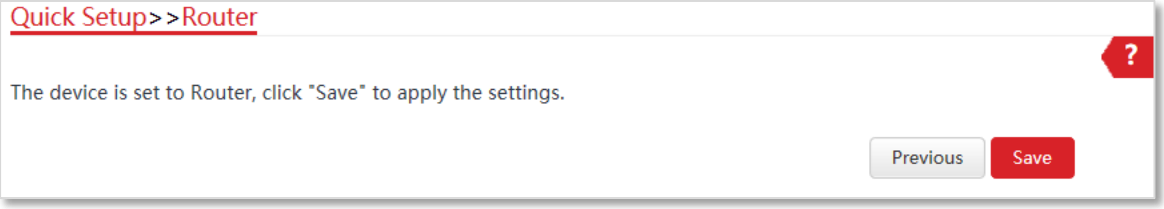
Channel: 40(5200MHz)

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

6 Click **Save**, and wait until the device reboots to activate the settings.



Quick Setup>>Router

The device is set to Router, click "Save" to apply the settings.

7 Connect the Ethernet cable with internet access to the LAN port of the PoE injector.

Note

Under **Router** mode, the LAN port of the PoE injector is converted into a WAN port.

---End

To access the internet with wireless devices: Connect the wireless devices, such as a smartphone, to the WiFi network of the base station using the WiFi name and password you set for the base station.

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **Router** mode: In this mode, this device serves as a router to provide internet access for wired and wireless clients. The PoE/LAN port functions as a WAN port used to connect to the internet.
Internet Connection Type	The device in Router mode supports three internet connection types: – **DHCP (Dynamic IP)**: The device obtains the IP address and other parameters from the DHCP server of upstream device for internet access. – **Static IP Address**: The device accesses the internet using the IP address, subnet mask, default gateway and DNS server IP addresses provided by your ISP. – **PPPoE**: The device accesses the internet using the PPPoE user name and password provided by the ISP.
SSID	It specifies the wireless network name of the device.
Channel	It specifies the channel that the WiFi network operates.
Security Mode	It specifies the security mode of the WiFi network of the device. It includes None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

5 Status

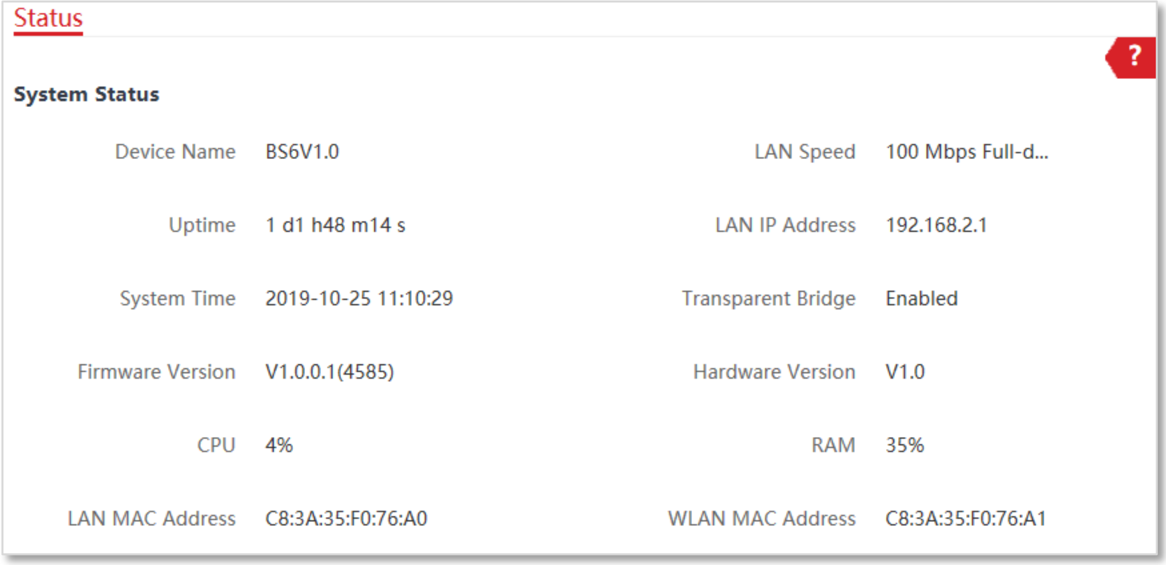
This module includes three parts: system status, wireless status, and statistics.

5.1 System status

You can view the system status here.

To access the page, start a web browser on the computer which is connected to the base station, start a web browser and visit **192.168.2.1**, then choose **Status**.

In **AP** mode, **Client** mode, **Universal Repeater** mode, **Repeater** mode and **P2MP** mode, this page is shown as follows:



System Status

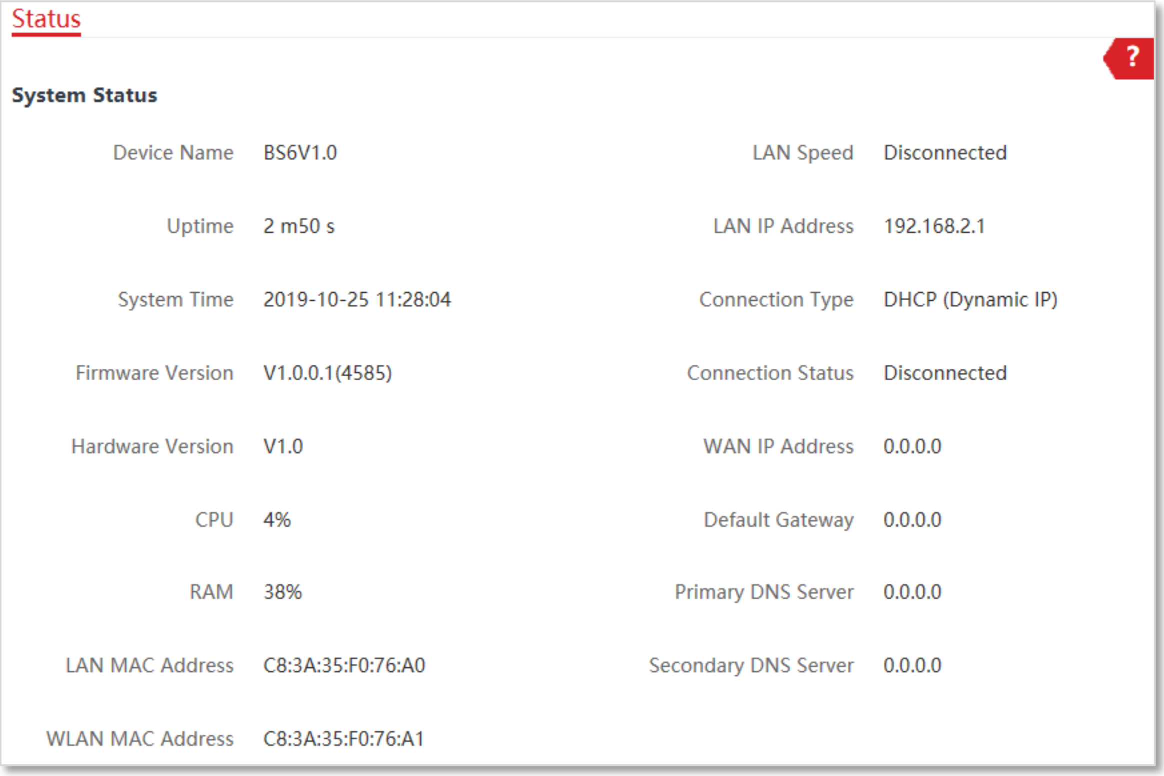
Device Name	BS6V1.0	LAN Speed	100 Mbps Full-d...
Uptime	1 d1 h48 m14 s	LAN IP Address	192.168.2.1
System Time	2019-10-25 11:10:29	Transparent Bridge	Enabled
Firmware Version	V1.0.0.1(4585)	Hardware Version	V1.0
CPU	4%	RAM	35%
LAN MAC Address	C8:3A:35:F0:76:A0	WLAN MAC Address	C8:3A:35:F0:76:A1

Parameters description

Parameter	Description
Device Name	It specifies the name of this device. A unique device name helps you manage multiple devices that are of the same model on LAN easily. To modify the device name, go to **Network** > **LAN Setup** page. You are allowed to modify only when the device works in **AP**, **Client**, **Universal Repeater**, **Repeater**, or **P2MP** mode.

Parameter	Description
Uptime	It specifies the total working time since the device was started last time.
System Time	It specifies the current system time of this device.
Firmware Version	It specifies the system software version number of this device.
CPU	Central Processing Unit. It specifies the CPU usage of this device.
LAN MAC Address	It specifies the MAC address of LAN port of this device.
LAN Speed	It specifies the connection status of LAN port. It includes connection rate and duplex mode.
LAN IP Address	It specifies the IP address (also called login IP address or management IP address) of this device. By default, it is **192.168.2.1**.
Transparent Bridge	It displays whether or not the Transparent Bridge function is enabled.
Hardware Version	It specifies the hardware version number of this device.
RAM	Random Access Memory. It specifies the memory usage of this device.
WLAN MAC Address	It specifies the MAC address of the wireless network of this device.

In **WISP** or **Router** mode, the base station as follows:



System Status

Device Name	BS6V1.0	LAN Speed	Disconnected
Uptime	2 m50 s	LAN IP Address	192.168.2.1
System Time	2019-10-25 11:28:04	Connection Type	DHCP (Dynamic IP)
Firmware Version	V1.0.0.1(4585)	Connection Status	Disconnected
Hardware Version	V1.0	WAN IP Address	0.0.0.0
CPU	4%	Default Gateway	0.0.0.0
RAM	38%	Primary DNS Server	0.0.0.0
LAN MAC Address	C8:3A:35:F0:76:A0	Secondary DNS Server	0.0.0.0
WLAN MAC Address	C8:3A:35:F0:76:A1		

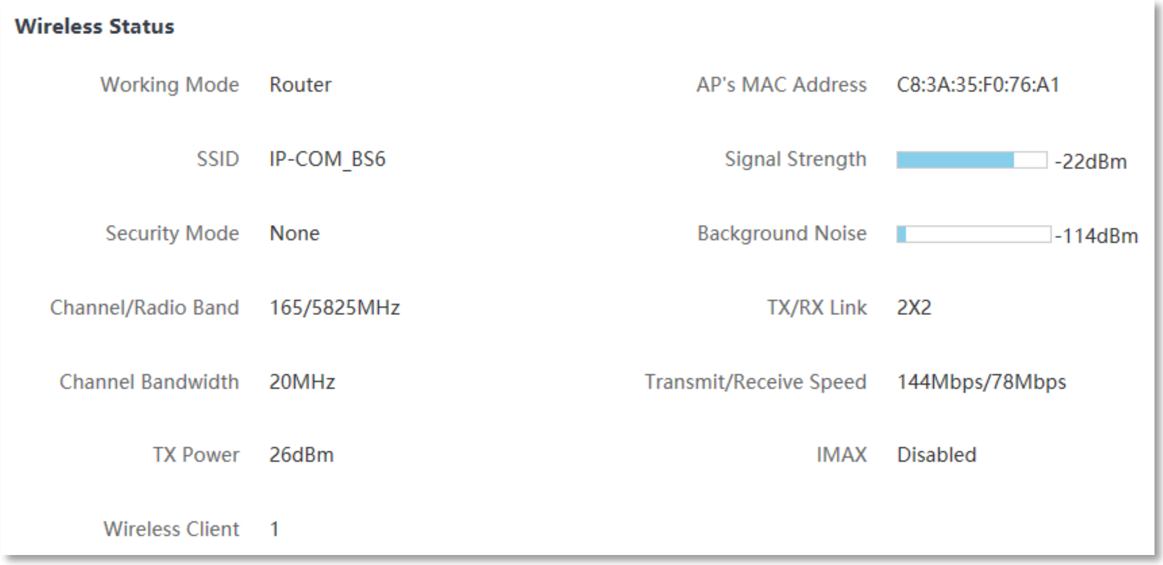
Parameters description

Parameter	Description
Device Name	It specifies the name of this device. Different device names help you manage multiple devices on LAN easily. You can change the name of this device on the **Network** > **LAN Setup** page when the device works in **AP**, **Client**, **Universal Repeater**, **Repeater**, and **P2MP** modes. When the device works in **WISP** or **Router** mode, it displays the model of the device, and cannot be changed.
Uptime	It specifies the total working time since the device was started last time.
System Time	It specifies the current system time of this device.
Firmware Version	It specifies the system software version number of this device.
Hardware Version	It specifies the hardware version of this device.
CPU	Central Processing Unit. It specifies the CPU usage of this device.
RAM	Random Access Memory. It specifies the memory usage of this device.
LAN MAC Address	It specifies the MAC address of LAN port of this device.
WLAN MAC Address	It specifies the MAC address of the wireless network of this device.
LAN Speed	It specifies the PoE/LAN port speed and duplex mode of this device.
LAN IP Address	It specifies the IP address (also named management IP address) of this device. By default, it is **192.168.2.1**. You can access the web UI of this device using this IP address.
Connection Type	It specifies the internet connection type of this device.
Connection Status	It specifies the connection status of WAN port of this device.
WAN IP Address	It specifies the IP address of WAN port of this device.
Default Gateway	It specifies the default gateway address of this device.
Primary DNS Server	It specifies the IP address of primary DNS server of this device.
Secondary DNS Server	It specifies the IP address of secondary DNS server of this device.

5.2 Wireless status

You can view wireless status here, including working mode, SSID, security mode, and so on.

To access the page, log in to the web UI of the device and choose **Status**.



Wireless Status

Working Mode	Router	AP's MAC Address	C8:3A:35:F0:76:A1
SSID	IP-COM_BS6	Signal Strength	-22dBm
Security Mode	None	Background Noise	-114dBm
Channel/Radio Band	165/5825MHz	TX/RX Link	2X2
Channel Bandwidth	20MHz	Transmit/Receive Speed	144Mbps/78Mbps
TX Power	26dBm	IMAX	Disabled
Wireless Client	1		

Parameters description

Parameter	Description
Working Mode	It specifies the current working mode the device operates.
SSID	It specifies the wireless network name of this device. In **Client** mode, it displays **N/A**.
Security Mode	It specifies the security mode of the wireless network of this device.
Channel/Radio Band	It specifies the channel and frequency band the device operates.
Channel Bandwidth	It specifies the channel bandwidth of this device.
TX Power	It specifies the transmit power of this device.
Wireless Client	It specifies the number of wireless clients connected to this device.
AP's MAC Address	In **Client**, **Universal Repeater**, **WISP**, **P2MP** or **Repeater** mode, it displays the MAC address of peer AP to which this device bridged. In **AP** or **Router** mode, it displays **No Peer AP** if the device works.
Signal Strength	In **AP** or **Router** mode, it displays the signal strength of the first device connected to the WiFi network of the device. In **Client**, **Universal Repeater**, **WISP**, **P2MP** or **Repeater** mode, it displays the received signal strength from peer AP.
Background Noise	It specifies the strength of ambient radio interference. Larger absolute value indicates less interference. For example, -95 dBm indicates less interference than that of -75 dBm.
TX/RX Link	It specifies the number of spatial streams the device is transmitting or receiving.
Transmit/Receive	It specifies the wireless transmitting/receiving rate.

Parameter	Description
Speed	In **AP** or **Router** mode, it displays the transmitting/receiving rate of the first device connected to the wireless network of this device. In **Client**, **Universal Repeater**, **WISP**, **Repeater**, or **P2MP** mode, it displays transmitting/receiving rate of this device.
TD-MAX	It specifies the status of the TD-MAX function.

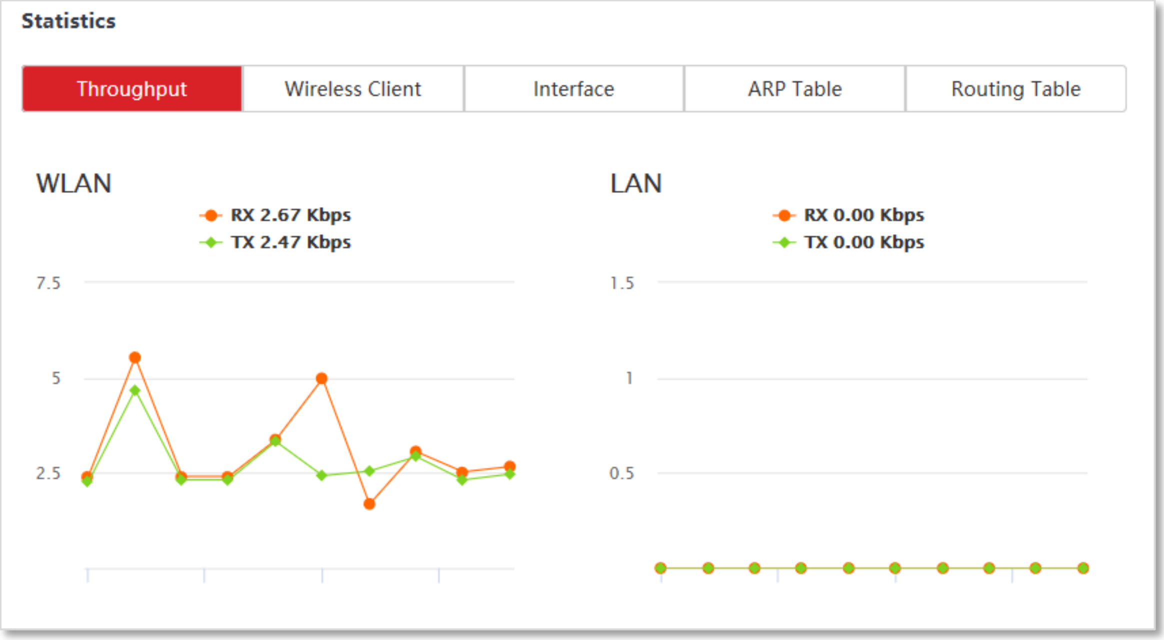
5.3 Statistics

On the **Status** page, you can learn statistics information about throughput, wireless client, interface, ARP table and routing table.

To access the page, log in to the web UI of the device and choose **Status**.

5.3.1 Throughput

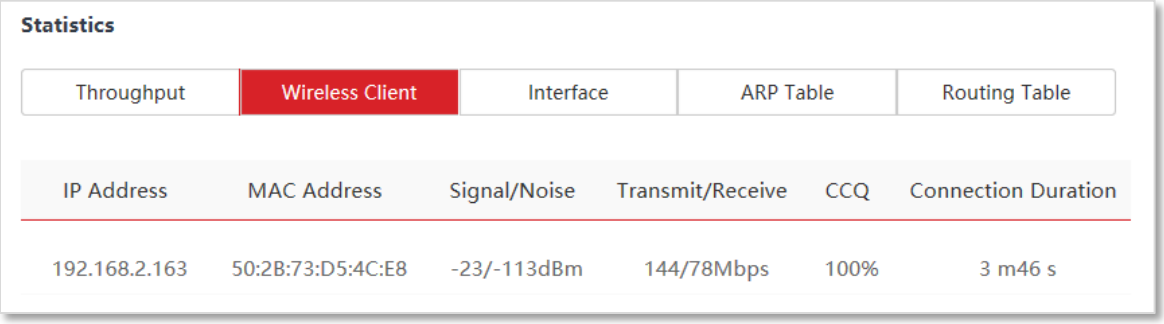
The line charts visually show the real-time transmitting and receiving traffic of WLAN and LAN ports of the device.



5.3.2 Wireless client/Upstream AP

This module differs depending on the working mode of the device.

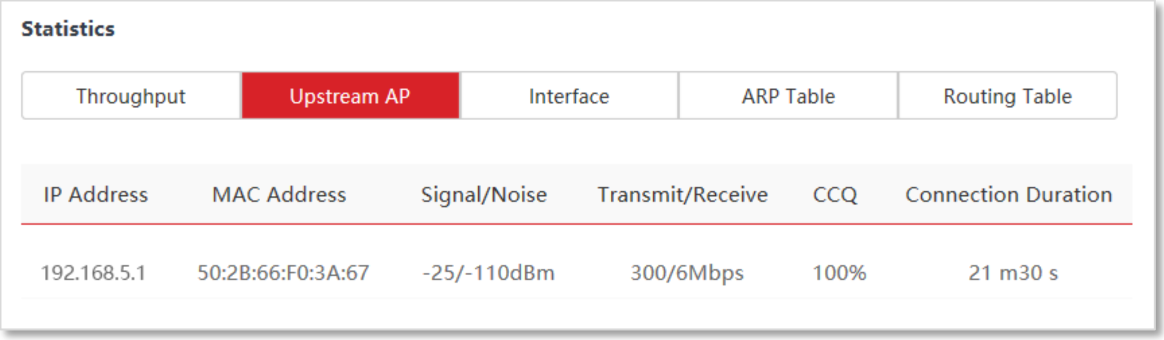
- In **AP** or **Router** mode, it displays information of connected wireless clients.
- In **Client**, **Universal Repeater**, **WISP**, **P2MP** or **Repeater** mode, it displays information of upstream AP.



IP Address	MAC Address	Signal/Noise	Transmit/Receive	CCQ	Connection Duration
192.168.2.163	50:2B:73:D5:4C:E8	-23/-113dBm	144/78Mbps	100%	3 m46 s

Parameters description

Parameter	Description
IP Address	It specifies the IP address of the corresponding wireless client.
MAC Address	It specifies the MAC address of the corresponding wireless client.
Signal/Noise	– **Signal**: It specifies the WiFi signal strength of the corresponding wireless client. – **Noise**: It specifies the ambitus interference signal and electromagnetic interference strength.
Transmit/Receive	It specifies the transmitting and receiving rate of a client.
CCQ	It specifies the connection quality of the corresponding client. A higher percentage indicates a better connection quality.
Connection Duration	It specifies the time that has elapsed since the wireless client is connected to the wireless network of the device.


Statistics

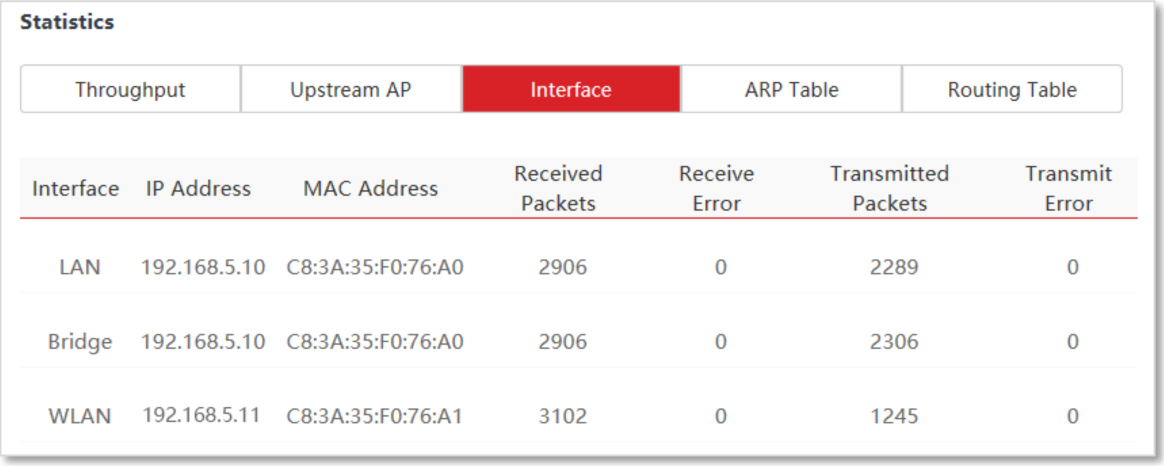
IP Address	MAC Address	Signal/Noise	Transmit/Receive	CCQ	Connection Duration
192.168.5.1	50:2B:66:F0:3A:67	-25/-110dBm	300/6Mbps	100%	21 m30 s

Parameters description

Parameter	Description
IP Address	It specifies the IP address of the upstream device.
MAC Address	It specifies the MAC address of the upstream device.
Signal/Noise	– **Signal**: It specifies the WiFi signal strength of the corresponding upstream AP. – **Noise**: It specifies the ambitus interference signal and electromagnetic interference strength.
Transmit/Receive	It specifies the transmitting and receiving rate of the upstream device.
CCQ	It specifies the connection quality of the upstream device. A higher percentage indicates a better connection quality.
Connection Duration	It specifies the time that has elapsed since this device connects to the upstream device.

5.3.3 Interface

It displays the IP address, MAC address and traffic information of the interfaces of the device.



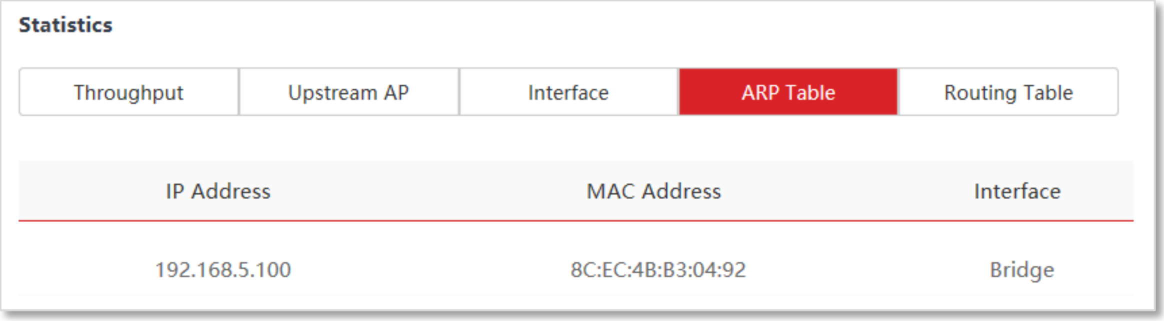
Interface	IP Address	MAC Address	Received Packets	Receive Error	Transmitted Packets	Transmit Error
LAN	192.168.5.10	C8:3A:35:F0:76:A0	2906	0	2289	0
Bridge	192.168.5.10	C8:3A:35:F0:76:A0	2906	0	2306	0
WLAN	192.168.5.11	C8:3A:35:F0:76:A1	3102	0	1245	0

Parameters description

Parameter	Description
Interface	It specifies the interface type that a host passes through, including **LAN**, **Bridge**, and **WLAN**.
IP Address	It displays the IP addresses of wired interface, bridge interface, and WLAN interface.
MAC Address	It displays the MAC addresses of an interface.
Received Packets	It displays the received and transmitted packets of the interface.
Transmitted Packets	
Receive Error	It displays the received and transmitted error packets of the interface.
Transmit Error	

5.3.4 ARP table

ARP (Address Resolution Protocol) is a network layer protocol used to convert an IP address into a physical address. The ARP table displays the IP address and its corresponding MAC address the device visits, and the interface the packets pass through.



IP Address	MAC Address	Interface
192.168.5.100	8C:EC:4B:B3:04:92	Bridge

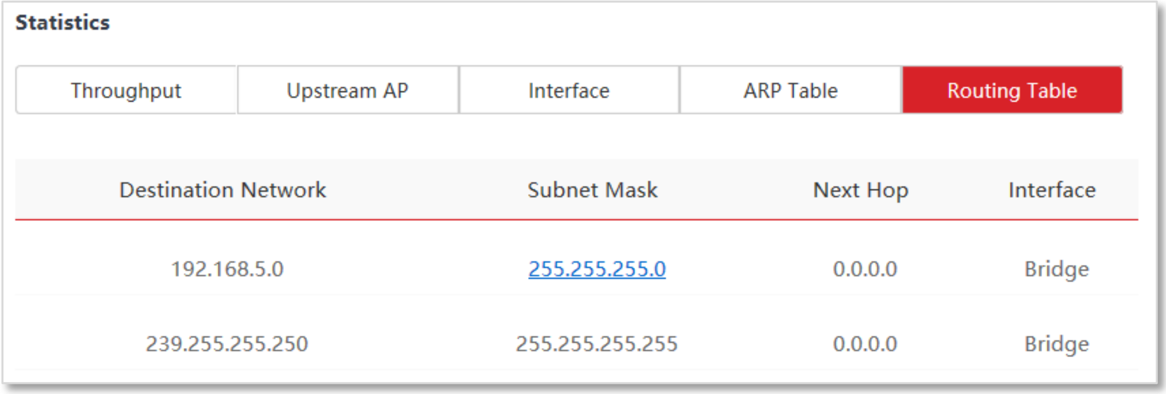
Parameters description

Parameter	Description
IP Address	It specifies the IP address of the host in the APR table.
MAC Address	It specifies the MAC address corresponding to the IP address.
Interface	It specifies the interface used to communicate with the host, including LAN, WLAN and bridge interfaces.

5.3.5 Routing table

It specifies the destination networks that the device can access.

To access the page, log in to the web UI of the device, and choose **Status**, then **Routing Table** in **Statistics** part.



Destination Network	Subnet Mask	Next Hop	Interface
192.168.5.0	255.255.255.0	0.0.0.0	Bridge
239.255.255.250	255.255.255.255	0.0.0.0	Bridge

Parameters description

Parameter	Description
Destination Network	It specifies the IP address of the destination network.
Subnet Mask	It specifies the subnet mask of the destination network.
Next Hop	It specifies the IP address of entrance of the next hop route when the packets egress from the interface of the device. 0.0.0.0 indicates that the destination network is the network which is directly connected to the interface.
Interface	It specifies the interface that the packets egress.

6 Network

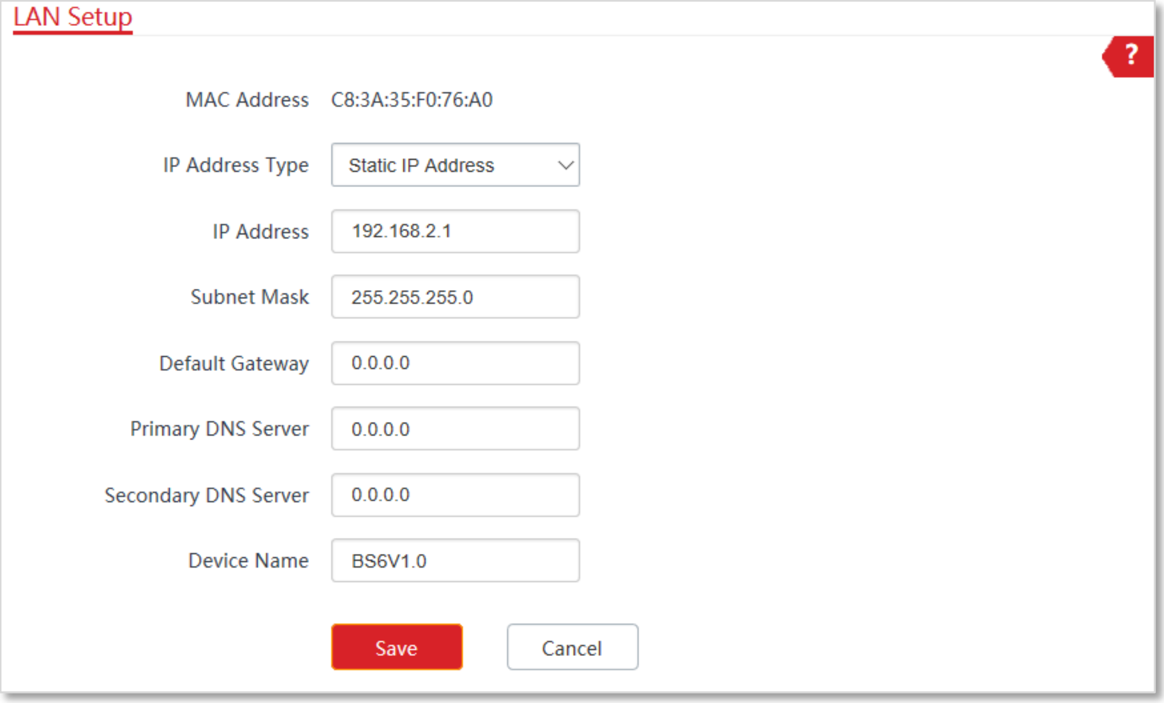
6.1 LAN setup

6.1.1 Overview

On the **LAN Setup** page, you can view the MAC address of the LAN port, configure the device name, and type of obtaining an IP address and related parameters.

To access the page, choose **Network** > **LAN Setup**.

In **AP**, **Client**, **Universal Repeater**, **Repeater**, and **P2MP** modes, the page displays:



MAC Address C8:3A:35:F0:76:A0

IP Address Type Static IP Address

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

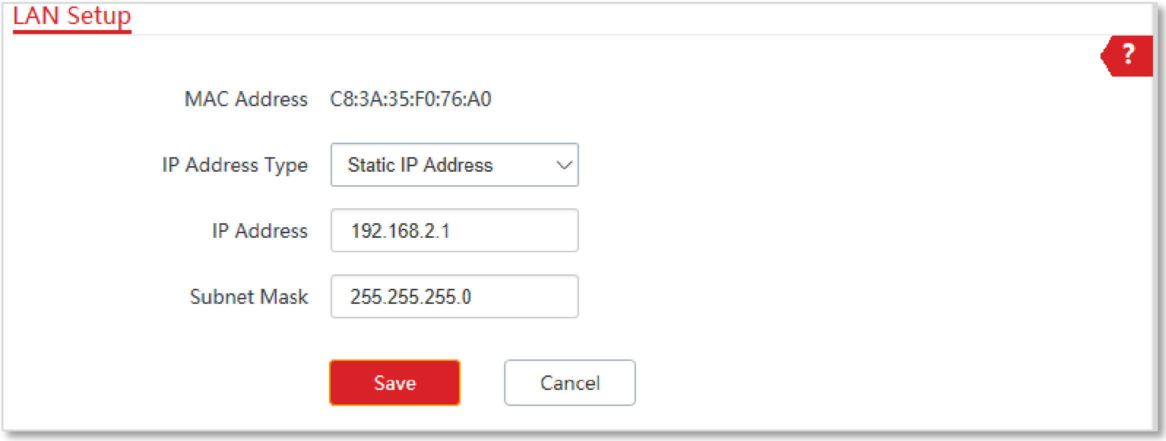
Device Name BS6V1.0

Parameters description

Parameter	Description
MAC Address	It specifies the MAC address of LAN port.
IP Address Type	It specifies the type of obtaining an IP address. The default is **Static IP Address**. **Static IP Address**: Specify the IP address, subnet mask, default gateway, and DNS

Parameter	Description
	server IP addresses manually. **DHCP (Dynamic IP Address)**: The device obtains an IP address, subnet mask, default gateway and DNS server IP address from the DHCP server to which it connects. Tip If the **IP Address Type** is set to **DHCP (Dynamic IP Address)**, you need to check the device's IP address on the clients list of the DHCP server to which it connects, and use this IP address to log in.
IP Address	It specifies the LAN IP address of the device. The default is **192.168.2.1**.
Subnet Mask	It specifies the subnet mask of the device. The default is **255.255.255.0**.
Default Gateway	It specifies the default gateway of the device. You can set it to the IP address of the egress router to enable the device to access the internet.
Primary DNS Server	It specifies the primary DNS server IP address of the device. If the egress router has the DNS agent function, You can manually set this parameter to the LAN IP address of the egress router.
Secondary DNS Server	Optional. It specifies the secondary DNS server IP address of the device.
Device Name	It specifies the name of the device. The default name indicates the product model and version. A unique device name helps you manage multiple devices that are of the same model on LAN easily. You are allowed to modify only when the device works in **AP**, **Client**, **Universal Repeater**, **Repeater** or **P2MP** mode.

In **WISP** and **Router** modes, the page displays:



MAC Address	C8:3A:35:F0:76:A0
IP Address Type	Static IP Address
IP Address	192.168.2.1
Subnet Mask	255.255.255.0

Parameters description

Parameter	Description
MAC Address	It specifies the MAC address of LAN port.
IP Address Type	It specifies the type of obtaining an IP address. The default is **Static IP Address**. **Static IP Address**: Specify the IP address and subnet mask manually. **DHCP (Dynamic IP Address)**: The device obtains an IP address and subnet mask from the upstream DHCP server in the network. Tip If the IP Address Type is set to DHCP (Dynamic IP Address), you need to check the device's IP address on the clients list of the DHCP server of the upstream device, and use this IP address to log in.
IP Address	It specifies the LAN IP address of the device. The default is **192.168.2.1**.
Subnet Mask	It specifies the subnet mask corresponding to the LAN IP address of the device. The default is **255.255.255.0**.

6.1.2 Set the LAN IP address manually

This method applies to a small LAN network with a few base stations. With this method, you need manually set the IP address, subnet mask, gateway IP address, and DNS server IP addresses of the device. Therefore, this mode is recommended if you need to deploy only a few devices.

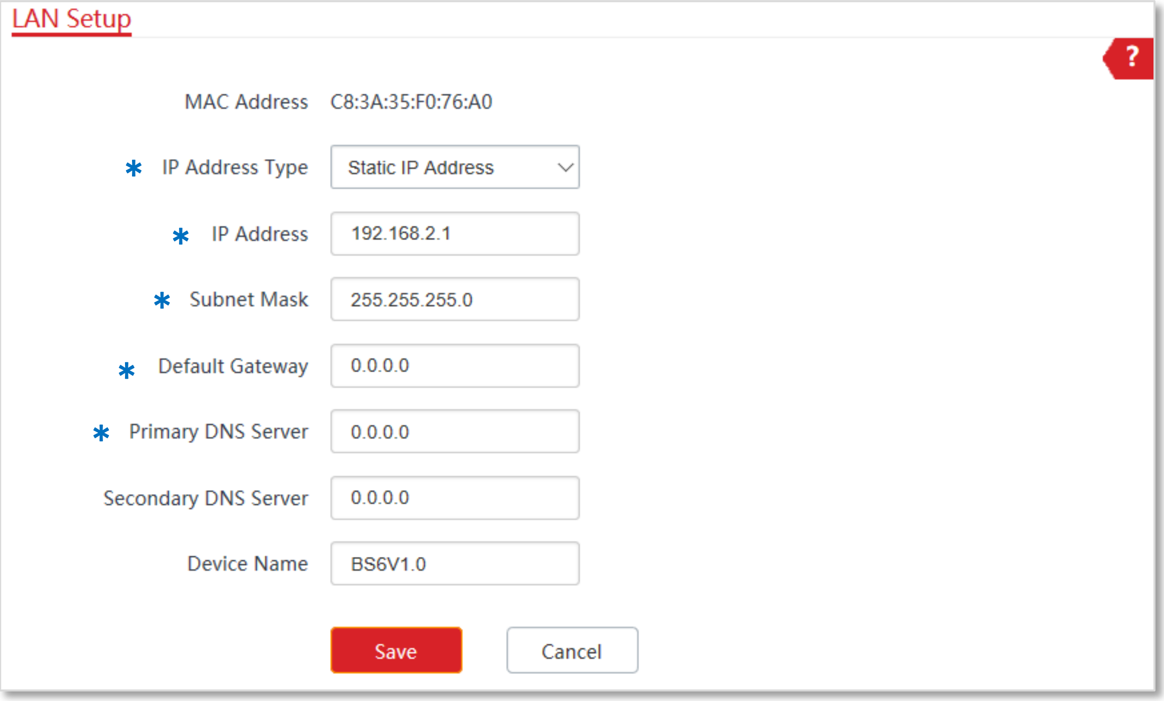
Configuration procedure:

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Network** > **LAN Setup** to enter the configuration page.

2 Select **Static IP Address** from the **IP Address Type** drop-down list.

3 Set **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**.

4 Click **Save**.



LAN Setup

MAC Address C8:3A:35:F0:76:A0

* IP Address Type: Static IP Address

* IP Address: 192.168.2.1

* Subnet Mask: 255.255.255.0

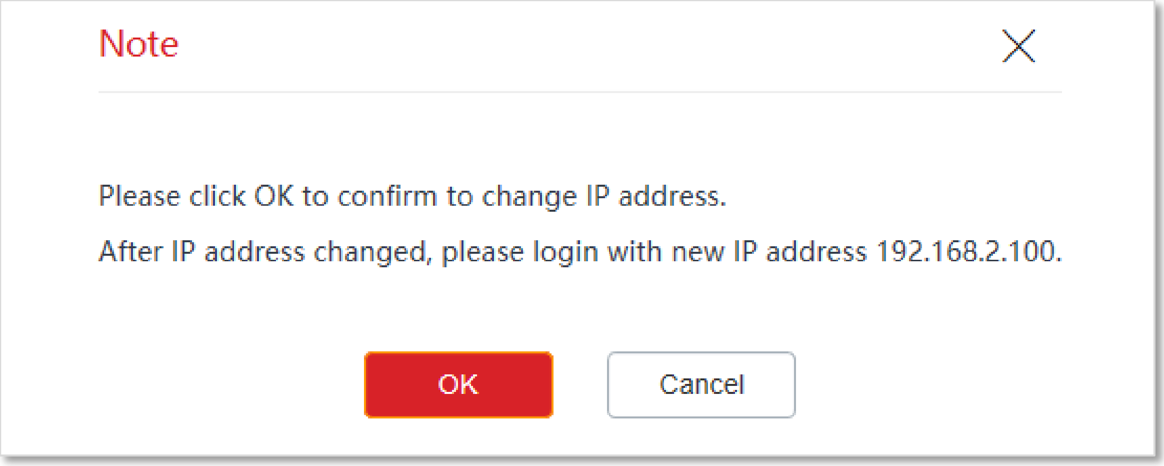
* Default Gateway: 0.0.0.0

* Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Device Name: BS6V1.0

5 Click **OK** on the pop-up window.



Note

Please click OK to confirm to change IP address.

After IP address changed, please login with new IP address 192.168.2.100.

---End

6.1.3 Log in to the web UI after changing the LAN IP address

After the configuration, if the new and original IP addresses belong to the same network segment, you can log in to the web UI of the device by accessing the new IP address.

Otherwise, assign your computer an IP address that belongs to the same network segment as the new IP address of the device before login with the new IP address. Refer to How to assign a fixed IP address to your computer in Appendix for details.

6.1.4 Set the device to obtaining an LAN IP address automatically

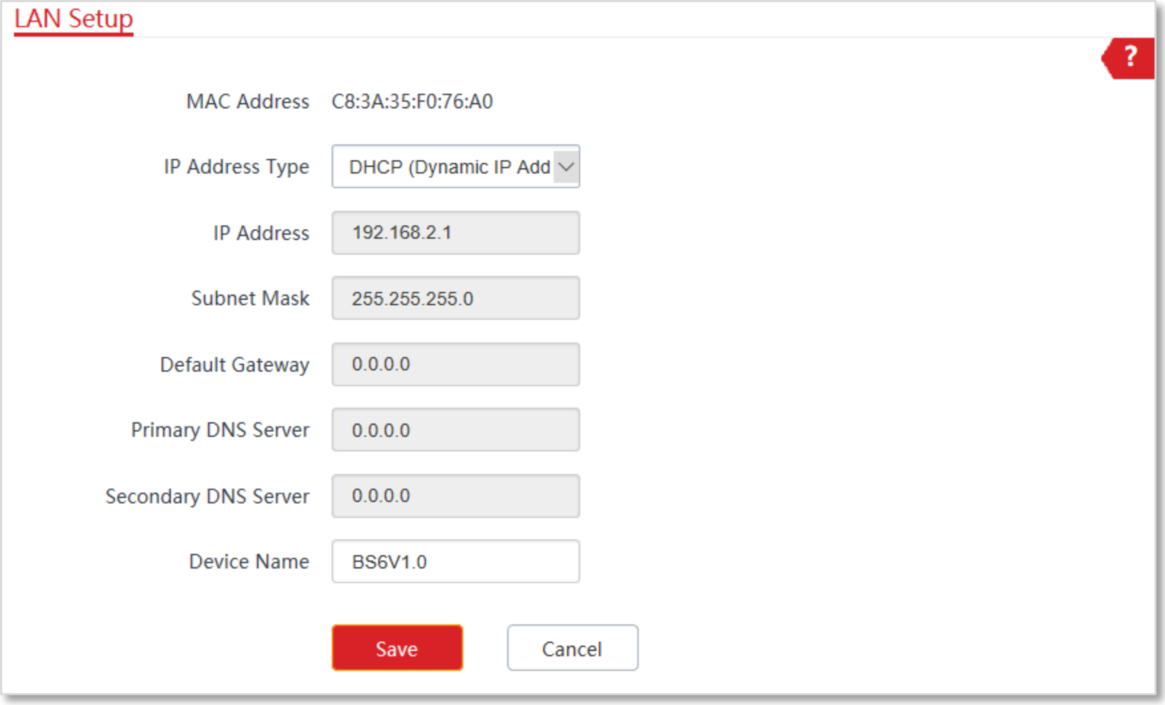
This method applies to a large LAN network with a large number of base stations. With this method, the device automatically obtains an IP address, a subnet mask, a gateway IP address, DNS server IP addresses assigned by the DHCP server of the upstream device.

Configuration procedure:

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Network** > **LAN Setup** to enter the configuration page.

2 Select **DHCP (Dynamic IP Address)** from the **IP Address Type** drop-down list.

3 Click **Save**.



LAN Setup

MAC Address	C8:3A:35:F0:76:A0
IP Address Type	DHCP (Dynamic IP Add
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Device Name	BS6V1.0

---End

After changing the configuration, if you want to re-log in to the web UI of the device, check the new IP address on the web UI of the upstream device which assigns the IP address to this device. Ensure that the IP address of the management computer and the IP address of the device belong to the same network segment, and access the IP address of the device. Refer to How to assign a fixed IP address to your computer in Appendix to assign an IP address to the computer manually.

6.2 MAC clone

This function is available only when the device works in **WISP** or **Router** mode.

6.2.1 Overview

If the base station cannot access the internet after configuring internet settings, your ISP may have bound your internet service account with the MAC address of your computer that was used to verify the internet connectivity after you subscribed to the internet service. Therefore, only this computer can access the internet with the account.

In this case, you need to clone the MAC address of this computer to the WAN port of the base station for internet access.

6.2.2 Clone a MAC address

Select one of the following methods to clone the MAC address according to your networking scenario.

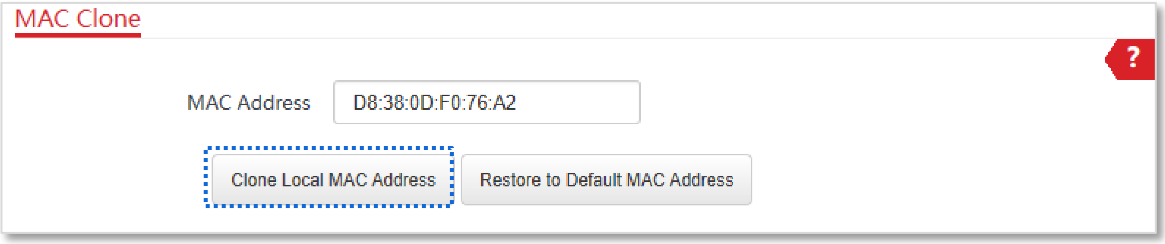
Use the computer with the MAC address bound to your internet service for setup

1 Connect the computer to the device.

2 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Network** > **MAC Clone** to enter the configuration page.

3 Click **Clone Local MAC Address**.

4 Click **Save**.



MAC Address: D8:38:0D:F0:76:A2

---End

Use a device without the MAC address bound your internet service for setup

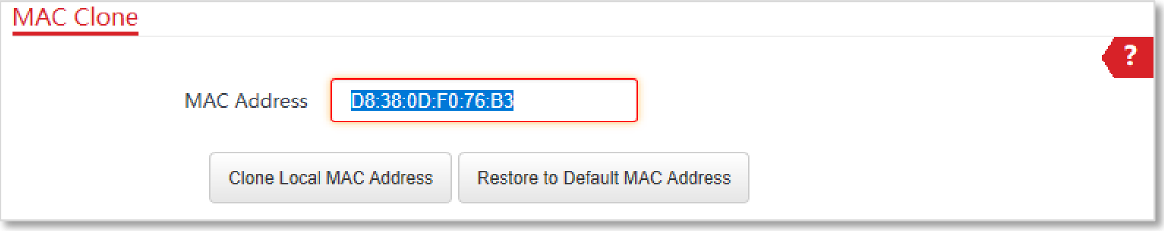
If you use a device whose MAC address is not bound to your internet service to set up the function, perform the following steps:

1 Connect the device (such as a smart phone or tablet) to the base station.

2 Start a web browser the device, visit **192.168.2.1** and choose **Network** > **MAC Clone** to enter the configuration page.

3 Enter the MAC address of the computer that can access the internet in the **MAC Address** input box.

4 Click **Save**.


MAC Clone

MAC Address: D8:38:0D:F0:76:B3

----End

Tip

If you want to restore the MAC address to factory settings, choose **Network** > **MAC Clone**, click **Restore to Default MAC Address**, and click **Save**.

6.3 DHCP server

6.3.1 Overview

The device provides a DHCP server function to assign IP addresses to clients in the LAN. By default, the DHCP server function is enabled.

Tip

If the network segment of the device's LAN port changes, the network segment of the device's DHCP server pool changes accordingly.

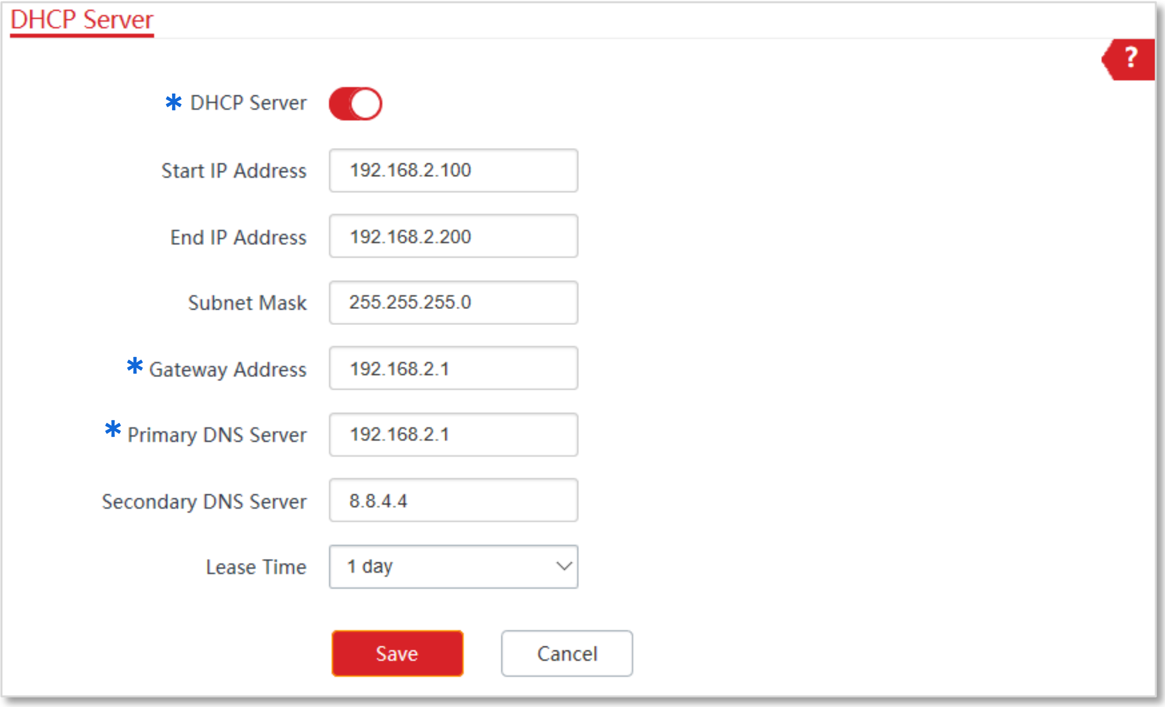
6.3.2 Configure the DHCP server

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1**, and choose **Network** > **DHCP Server** to enter the configuration page.

2 Set the **DHCP server** to ●.

3 Set the parameters. Generally, you only need to set **Gateway Address** and **Primary DNS Server**.

4 Click **Save**.


DHCP Server

* DHCP Server	●
Start IP Address	192.168.2.100
End IP Address	192.168.2.200
Subnet Mask	255.255.255.0
* Gateway Address	192.168.2.1
* Primary DNS Server	192.168.2.1
Secondary DNS Server	8.8.4.4
Lease Time	1 day

---End

Tip

If another DHCP server is available on your LAN, ensure that the IP address pool of the device does not overlap with the IP address pool of that DHCP server. Otherwise, IP address conflicts may occur.

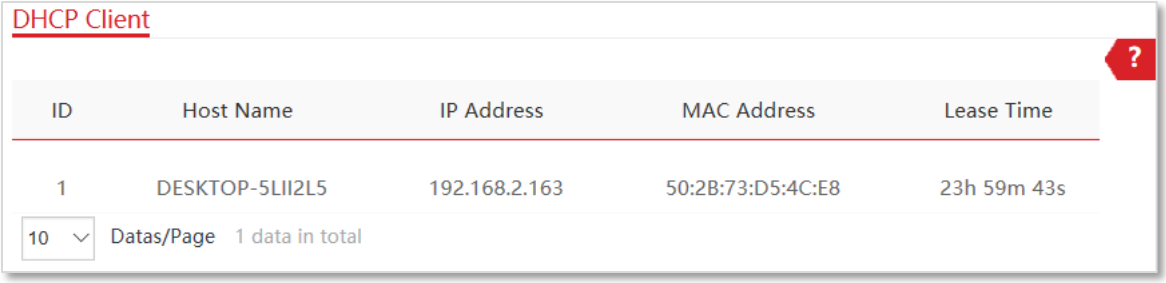
Parameters description

Parameter	Description
DHCP Server	It specifies whether to enable the DHCP server function of the device. By default, it is enabled.
Start IP Address	It specifies the start IP address of the IP address pool of the DHCP server. The default value is **192.168.2.100**.
End IP Address	It specifies the end IP address of the IP address pool of the DHCP server. The default value is **192.168.2.200**. Tip The start and end IP addresses must belong to the same network segment as the IP address of the LAN port of the device.
Subnet Mask	It specifies the subnet mask assigned by the DHCP server. The default value is **255.255.255.0**.
Gateway Address	It specifies the default IP address gateway assigned by the DHCP server. Generally, it is the IP address of the LAN port of a router on the LAN. The default value is **192.168.2.254**. Tip A client can access a server or host not in the local network segment only through a gateway.
Primary DNS Server	It specifies the primary DNS server IP address assigned by the DHCP server. The default value is **8.8.8.8**. Tip To enable clients to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server	Optional. It specifies the secondary DNS server IP address assigned by the DHCP server. The default value is **8.8.4.4**.
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client. When half of the lease time has elapsed, the client sends a DHCP request to the DHCP server to renew the lease time. If the request succeeds, the lease time is extended according to the request. Otherwise, the client sends the request again when 7/8 of the lease time has elapsed. If the request succeeds, the lease time is extended according to the request. Otherwise, the client must request an IP address from the DHCP server after the lease time expires. It is recommended that you retain the default value **1 day**.

6.4 DHCP client

If the device functions as a DHCP server, you can view the DHCP client list to understand the details about the clients that obtain IP addresses from the DHCP server.

To access the page, choose **Network** > **DHCP Client**.



DHCP Client

ID	Host Name	IP Address	MAC Address	Lease Time
1	DESKTOP-5LII2L5	192.168.2.163	50:2B:73:D5:4C:E8	23h 59m 43s

10 Datas/Page 1 data in total

Parameters description

Parameter	Description
ID	It specifies the serial number.
Host Name	It specifies the name of the host whose IP address is assigned by the DHCP server of the device.
IP Address	It specifies the IP address that the DHCP server assigns to the host.
MAC Address	It specifies the MAC address of the host.
Lease Time	It specifies the validity period of the IP address assigned by the DHCP server to the host.

6.5 VLAN settings

6.5.1 Overview

The device supports the IEEE 802.1q VLAN function, so that it can be used in networks with QVLAN. By default, the function is disabled.

After the VLAN settings take effect, packet with tag will be forwarded to the ports of the corresponding VLAN according to the VID of the packet, and packet without tag will be forwarded to the ports of the corresponding VLAN according to the PVID of the port.

The following form shows the details about how different link type ports address received packets:

Type of the Port	Type of Received Packets		Transmitted Packets
	Packet with Tag	Packet without Tag	
Access	Forward the data to the ports of the corresponding VLAN based on the VID in the tag.	Forward the data to the ports of the corresponding VLAN based on the PVID of ports	Strip the tag in the packet and then forward it
Trunk			VID ＝ PVID of the port, strip the tag in the packet and then forward it VID ≠ PVID of the port, retain the tag in the packet and then forward it

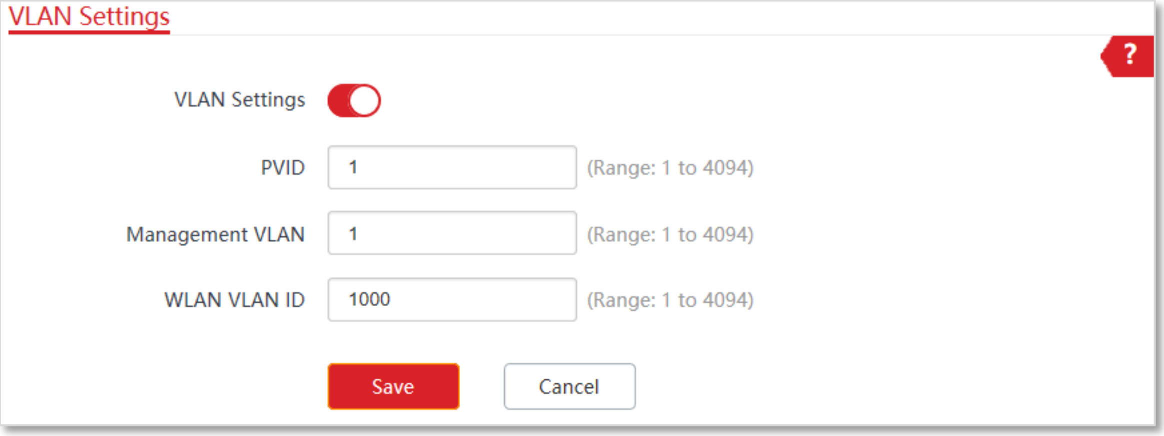
6.5.2 Set up VLAN

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Network** > **VLAN Settings** to enter the configuration page.

2 Set the **VLAN Settings** to ●.

3 Set the parameters as needed.

4 Click **Save**.


VLAN Settings

VLAN Settings ●

PVID 1 (Range: 1 to 4094)

Management VLAN 1 (Range: 1 to 4094)

WLAN VLAN ID 1000 (Range: 1 to 4094)

---End

Parameters description

Parameter	Description
VLAN Settings	It specifies whether to enable the VLAN function of this device. By default, it is disabled.
PVID	It specifies the ID of the default native VLAN ID of the trunk port. The default ID is **1**.
Management VLAN	It specifies the ID of the management VLAN of this device. The default ID is **1**. After changing the management VLAN, you can manage this device only after connecting your computer to the new management VLAN.
WLAN VLAN ID	It allows you to set a VLAN ID for the wireless network of this device. By default, it is set to **1000**. After the VLAN function is enabled, the WLAN interface functions as an access port, whose PVID is the same as VLAN ID.

6.5.3 Example of configuring VLAN settings

Networking requirement

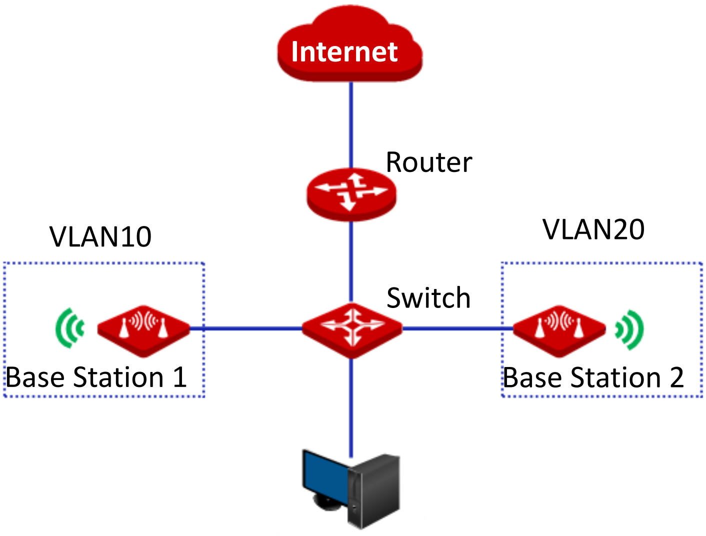
You use Base Station 1 and Base Station 2 to set up networks in two residential communities. To secure the data transmission, you want the two base stations to be isolated from each other.

You can assign Base Station 1 and Base Station 2 to different VLANs.

Assume that:

- Base Station 1 is assigned to VLAN10, and Base Station 2 is assigned to VLAN20.
- The router in the network supports IEEE 802.1q VLAN and enables two DHCP servers which belong to VLAN10 and VLAN 20 respectively.

Network Topology



The connections of the switch:

- The router is connected to the uplink port
- Base Station 1 is connected to port 1
- Base Station 2 is connected to port 2

Configuration procedure

1 Set up Base Station 1.

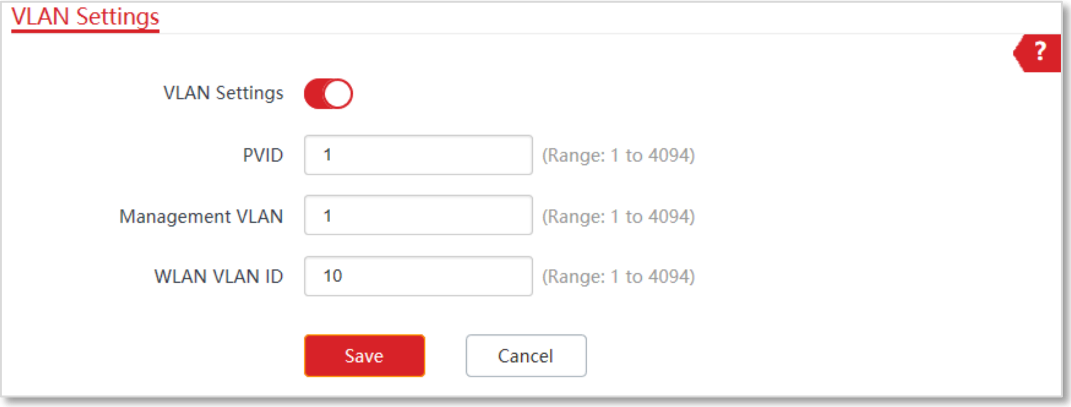
(1) Start a web browser on the computer connected to Base Station 1, visit **192.168.2.1** and choose **Network** > **VLAN Settings**.

(2) Set the **VLAN Settings** to ●.

(3) Set **Management VLAN** to **1**.

(4) Set **WLAN VLAN ID** to **10**.

(5) Click **Save**.



VLAN Settings

VLAN Settings ●

PVID 1 (Range: 1 to 4094)

Management VLAN 1 (Range: 1 to 4094)

WLAN VLAN ID 10 (Range: 1 to 4094)

(6) Click **OK** on the pop-up window, and wait until the Base Station 1 completes reboot.

2 Set the **WLAN VLAN ID** of Base Station 2 to **20** according to the steps in step 1.

3 Set up the switch as shown in the following table.

Ports of the Switch	VLAN ID (Allow the packets belonging to the following VLANs to access)	Type of Port	PVID
Uplink port (Connected to a router)	1,10,20	Trunk	1
Port 1 (Connected to Base Station 1)	1,10	Trunk	1
Port 2 (Connected to Base Station 2)	1,20	Trunk	1

Keep the default settings for the parameters which are not mentioned here. Refer to the user guide of the switch for details.

4 Set up the router as shown in the following table.

Enables two DHCP servers on the router, and assign them to VLAN10 and VLAN20 respectively.

Port of the router is connected to	VLAN ID (Allow the packets belonging to the following VLANs to access)	Type of Port	PVID
The switch	10, 20	Trunk	1

Refer to the user guide of the router for details.

---End

Verification

If the router enables two DHCP servers which belong to VLAN10 and VLAN20 respectively, the device connected to the Base Station 1 obtains an IP address and related parameters from the DHCP server belonging to VLAN10, and the device connected to Base Station 2 obtains these parameters from the DHCP sever belonging to VLAN20.

7 Wireless

7.1 Basic

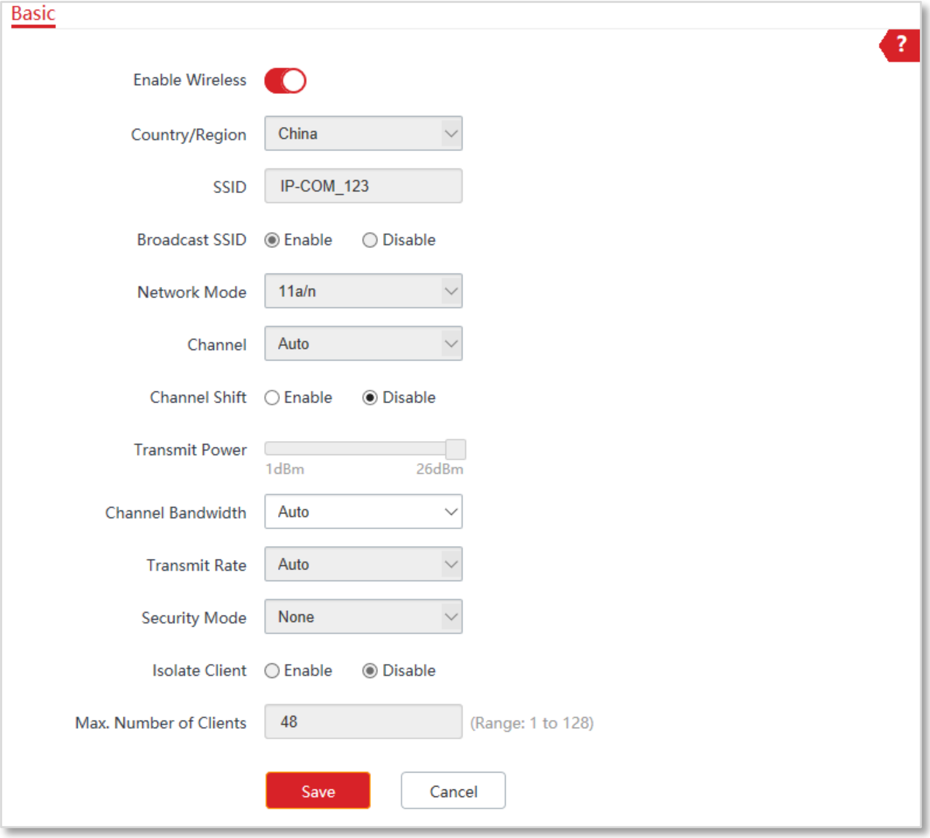
This module enables you to set basic wireless settings of the device, including SSID-related parameters, network mode, channel, transmit power and so on. This module is not available when the device works in **Client** or **Universal Repeater** mode.

7.1.1 Change the basic settings

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Wireless** > **Basic**.

2 Change the parameters as required.

3 Click **Save**.



Basic

Enable Wireless: ●

Country/Region: China

SSID: IP-COM_123

Broadcast SSID: ● Enable ○ Disable

Network Mode: 11a/n

Channel: Auto

Channel Shift: ○ Enable ● Disable

Transmit Power: 1dBm 26dBm

Channel Bandwidth: Auto

Transmit Rate: Auto

Security Mode: None

Isolate Client: ○ Enable ● Disable

Max. Number of Clients: 48 (Range: 1 to 128)

---End

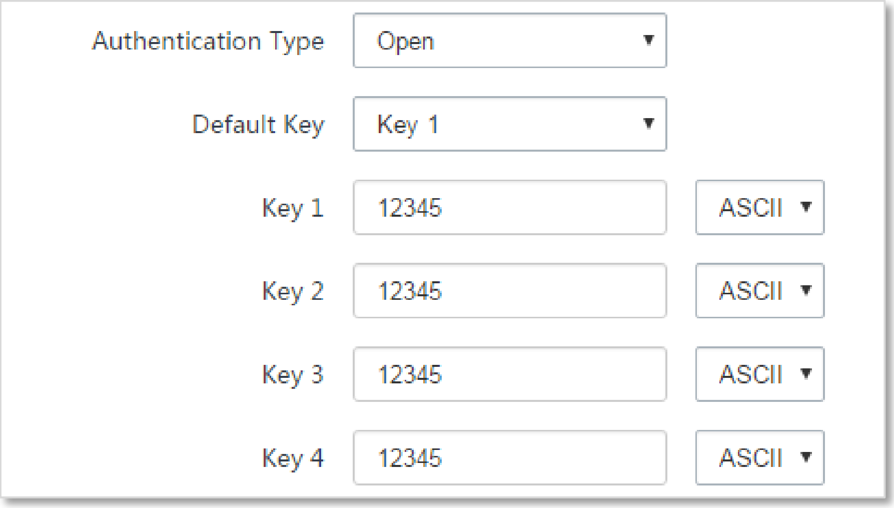
Parameters description

Parameter	Description
Enable Wireless	It specifies whether to enable the wireless function. By default, it is enabled.
Country/Region	It specifies country or region where this device is located. You can select the country or region to ensure that this device complies with the channel regulations of the country or region.
SSID	It specifies the wireless network name.
Broadcast SSID	It specifies whether to broadcast the SSID. When the device broadcasts an SSID, wireless clients can detect the SSID. When this parameter is set to **Disable**, the device does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This to some extent enhances the security of the wireless network.
Network Mode	It specifies the wireless network mode of this device. The available options include **11a**, **11n**, and **11 a/n**. – **11a**: It indicates that clients compliant with the 802.11a protocol can connect to the device. – **11n**: It indicates that clients working at 5 GHz and compliant with 802.11n can connect to the device. – **11 a/n**: It indicates that all clients working at 5 GHz and compliant with the 802.11a or 802.11n protocol can connect to the device.
Channel	It specifies channel in which this device operates. **Auto** indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.
Channel Shift	It specifies the shift of the channel center frequency. With this function enabled, the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the device can exchange data on less interference channels.
Transmit Power	It specifies the transmit power of this device. Higher number indicates wider WiFi coverage. Setting a proper transmit power helps improve the performance and security of the wireless network.
Channel Bandwidth	It specifies the bandwidth of the operating channel of a wireless network. Change the default setting only when necessary. – **10MHz**: The device can only use 10 MHz channel bandwidth. – **20MHz**: The device can only use 20 MHz channel bandwidth. – **30MHz**: The device can only use 30 MHz channel bandwidth. – **40MHz**: The device can only use 40 MHz channel bandwidth. – **Auto**: It specifies that the device can switch its channel bandwidth among 10MHz, 20 MHz, 30MHz and 40 MHz based on the ambient environment.
Transmit Rate	It specifies wireless transmit rate of the device. – When the channel bandwidth is set to **10 MHz**, the rate automatically reduces, and the maximum rate is 72.2 Mbps. – When the channel bandwidth is set to **20 MHz**, the rate automatically reduces, and the maximum rate is 144.4 Mbps. – When the channel bandwidth is set to **30 MHz**, the rate automatically reduces, and the maximum rate is 216.6 Mbps.

Parameter	Description
	– When the channel bandwidth is set to **40 MHz**, the maximum rate is 300 Mbps. – When the channel bandwidth is set to **Auto**, the maximum rate is 300 Mbps.
Security Mode	A wireless network uses radio, which is open to the public, as its data transmission medium. If the wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network. To ensure communication security, transmission links of wireless networks must be encrypted for protection. The device supports various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2. – **None**: It indicates that the WiFi network allows any wireless client to connect to it. This option is not recommended because it affects network security. – **WEP**: It uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. Data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum wireless network throughput of only 54 Mbps. Therefore, this security mode is not recommended. – **WPA-PSK/WPA2-PSK/Mixed WPA/WPA2-PSK**: They belong to pre-shared key or personal key modes, where Mixed WPA/WPA2-PSK supports both WPA-PSK and WPA2-PSK. – **WPA-PSK, WPA2-PSK**, and **Mixed WPA/WPA2-PSK** adopt a pre-shared key for authentication, while the base station generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all clients use the same key to connect to the same base station, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required. To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use IEEE 802.1x to authenticate clients and generate data encryption–oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK. – **WPA/WPA2**: WPA and WPA2 uses 802.1x to authenticate clients and the login information of a client is managed by the client. This effectively reduces the probability of information leakage. In addition, each time a client connects to an AP that adopts the WPA or WPA2 security mode, the RADIUS server generates a data encryption key and assigns it to the client. This makes it difficult for attackers to obtain the key. These features of WPA and WPA2 help significantly increase network security, making WPA and WPA2 the preferred security modes of wireless networks that require high security.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK, this parameter has the AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter has

Parameter	Description
	the AES, TKIP, and TKIP&AES values. – **AES**: It indicates the Advanced Encryption Standard. – **TKIP**: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the base station is limited to 54 Mbps. – **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key. It consists of 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies interval at which a WPA key is updated. A shorter interval leads to higher security. **0** indicates that no key update is performed.
Isolate Client	This parameter implements a function similar to the VLAN function for wired networks. It isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can access only the wired network connected to the device. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.
Max. Number of Clients	This parameter specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID. If the number is reached, the wireless network rejects new connection requests from clients. This limit helps balance load among devices.

WEP



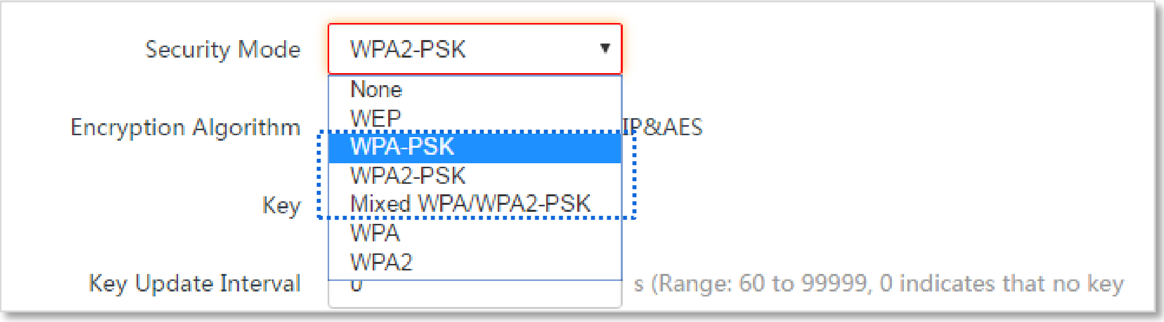
Authentication Type	Open ▾	
Default Key	Key 1 ▾	
Key 1	12345	ASCII ▾
Key 2	12345	ASCII ▾
Key 3	12345	ASCII ▾
Key 4	12345	ASCII ▾

Parameters description

Parameter	Description
Authentication Type	It specifies the authentication type for the WEP security mode. The options include **Open** and **Shared**. The options share the same encryption process. – **Open**: It specifies that authentication is not required and data exchanged is encrypted using WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. – **Shared**: It specifies that a shared key is used for authentication and data

Parameter	Description
	exchanged is encrypted using WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key.
Default Key	It specifies the WEP key for the **Open** or **Shared** encryption type. For example, if Default Key is set to Security Key 2, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Security Key 2.
Key 1/2/3/4	Enter WEP key. You can enter four keys, but only the key specified in the Default Key takes effect.
ASCII	It indicates that a key selected for the **Open** or **Shared** authentication type contains ASCII characters. 5 or 13 ASCII characters are allowed in the key.
Hex	It indicates that a key selected for the **Open** or **Shared** authentication type contains hexadecimal characters. 10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK



Security Mode: WPA2-PSK

Encryption Algorithm: IP&AES

Key

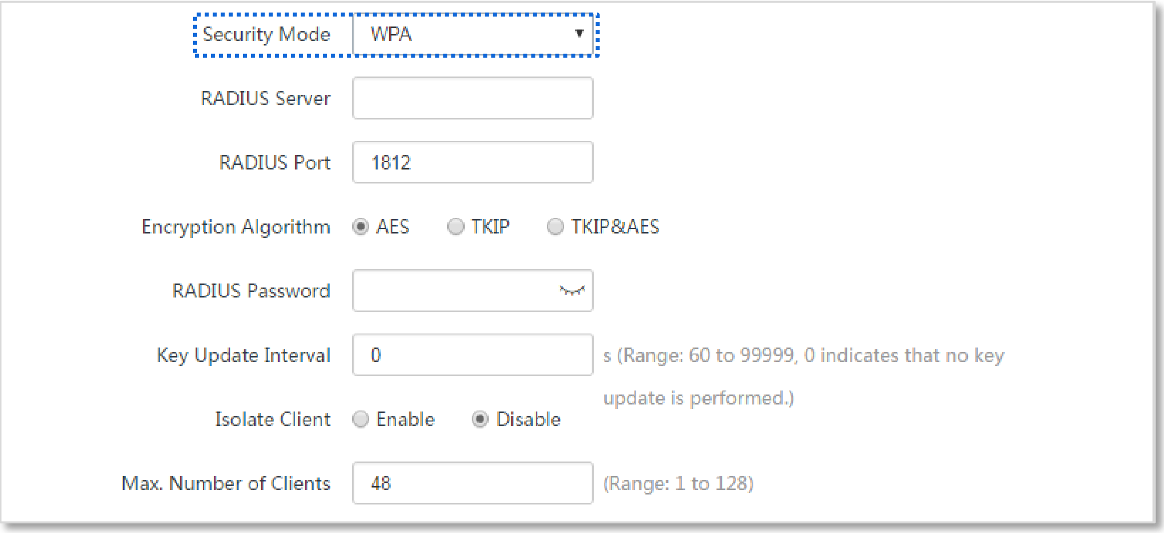
Key Update Interval: 0 s (Range: 60 to 99999, 0 indicates that no key

Parameters description

Parameter	Description
Security Mode	It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. – **WPA-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA-PSK. – **WPA2-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2-PSK. – **Mixed WPA/WPA2-PSK**: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK, this parameter has the AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter has the AES, TKIP, and TKIP&AES values. – **AES**: It indicates the Advanced Encryption Standard. – **TKIP**: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the

Parameter	Description
	maximum wireless throughput of the AP is limited to 54 Mbps. – **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value 0 indicates that a WAP key is not updated.

WPA and WPA2



Security Mode	WPA ▾
RADIUS Server	
RADIUS Port	1812
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
RADIUS Password	
Key Update Interval	0 s (Range: 60 to 99999, 0 indicates that no key update is performed.)
Isolate Client	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)

Parameters description

Parameter	Description
Security Mode	The **WPA** and **WPA2** options are available for network protection with a RADIUS server. – **WPA**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA. – **WPA2**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2.
RADIUS Server	It specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	It specifies the port number of the RADIUS server for client authentication.
RADIUS Password	It specifies the shared password of the RADIUS server.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. The available options include **AES**, **TKIP**, and **TKIP&AES**. – **AES**: It indicates the Advanced Encryption Standard. – **TKIP**: It indicates the Temporal Key Integrity Protocol. – **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network

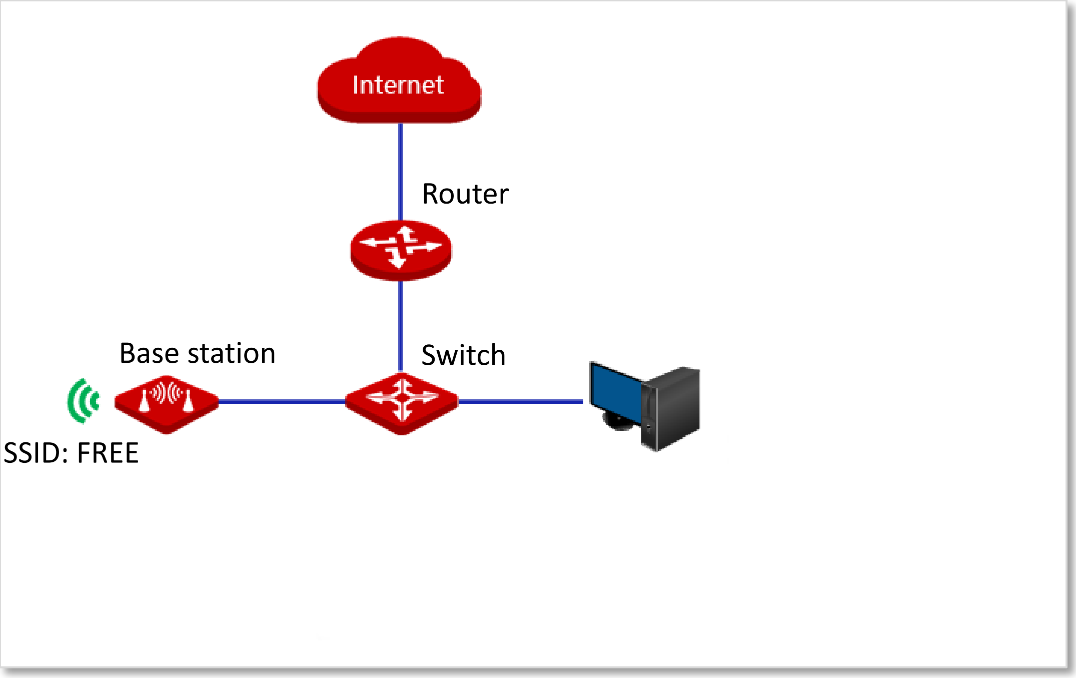
Parameter	Description
	corresponding to the selected SSID using TKIP or AES.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value 0 indicates that a WAP key is not updated.

7.1.2 Set up a non-encrypted wireless network

Networking requirement

A residential community uses the base station to deploy its network. It requires that the SSID is FREE and there is no WiFi password.

Network topology



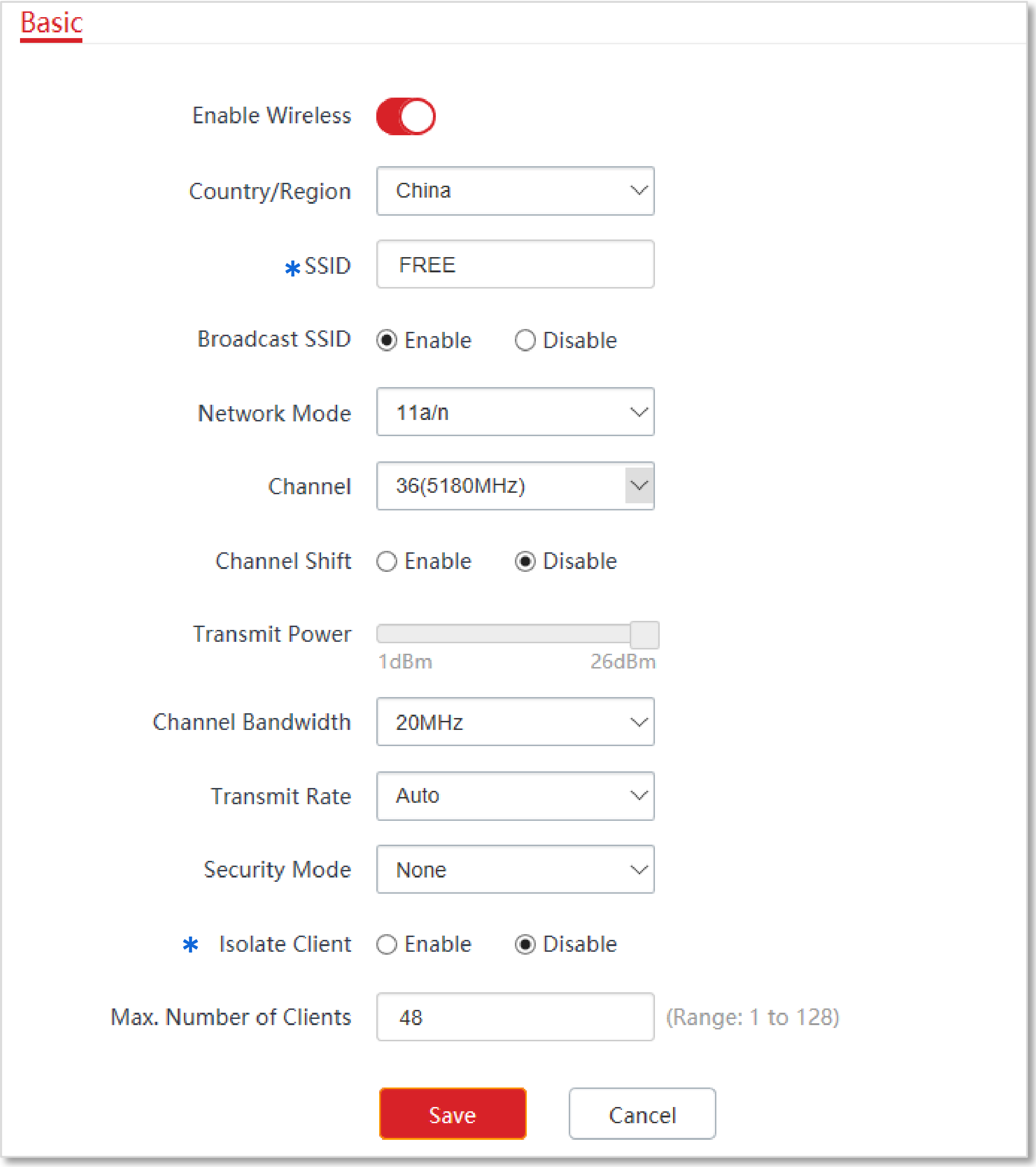
Configuration procedure

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Wireless** > **Basic**.

2 Change the value of the **SSID** input box to **FREE**.

3 Set **Security Mode** to **None**.

4 Click **Save**.



Basic

Enable Wireless	●
Country/Region	China
*SSID	FREE
Broadcast SSID	● Enable ○ Disable
Network Mode	11a/n
Channel	36(5180MHz)
Channel Shift	○ Enable ● Disable
Transmit Power	1dBm 26dBm
Channel Bandwidth	20MHz
Transmit Rate	Auto
Security Mode	None
* Isolate Client	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)

---End

Verification

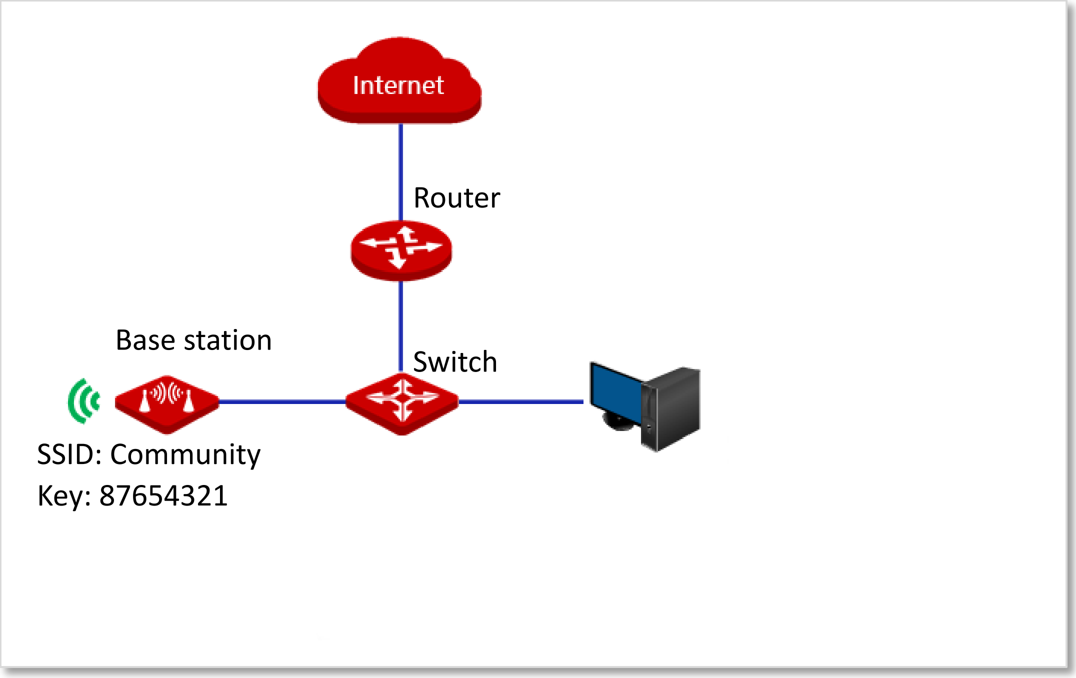
Wireless devices can connect to the wireless network whose SSID is **FREE** without a password.

7.1.3 Set up a wireless network encrypted using WPA2-PSK

Networking requirement

A residential community uses the base station to set up a wireless network. It requires that the wireless network has a certain level of security. In this case, WPA2-PSK mode is recommended. See the following figure.

Network topology



Configuration procedure

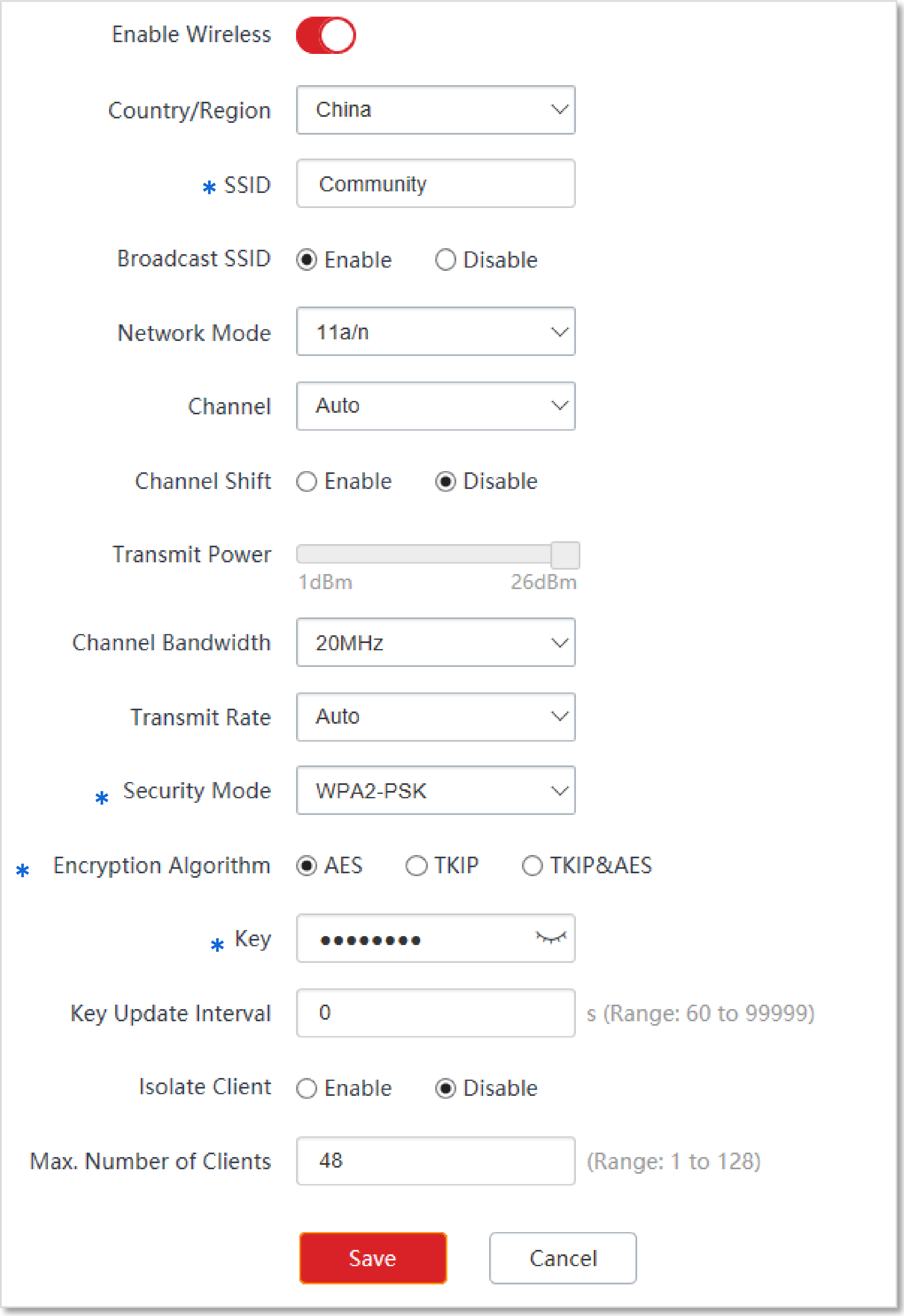
1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Wireless** > **Basic**.

2 Change the value of the SSID input box to **Community**.

3 Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.

4 Set **Key** to **87654321**.

5 Click **Save**.



Enable Wireless	●
Country/Region	China
* SSID	Community
Broadcast SSID	● Enable ○ Disable
Network Mode	11a/n
Channel	Auto
Channel Shift	○ Enable ● Disable
Transmit Power	1dBm 26dBm
Channel Bandwidth	20MHz
Transmit Rate	Auto
* Security Mode	WPA2-PSK
* Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
* Key	••••••••
Key Update Interval	0 s (Range: 60 to 99999)
Isolate Client	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)

---End

Verification

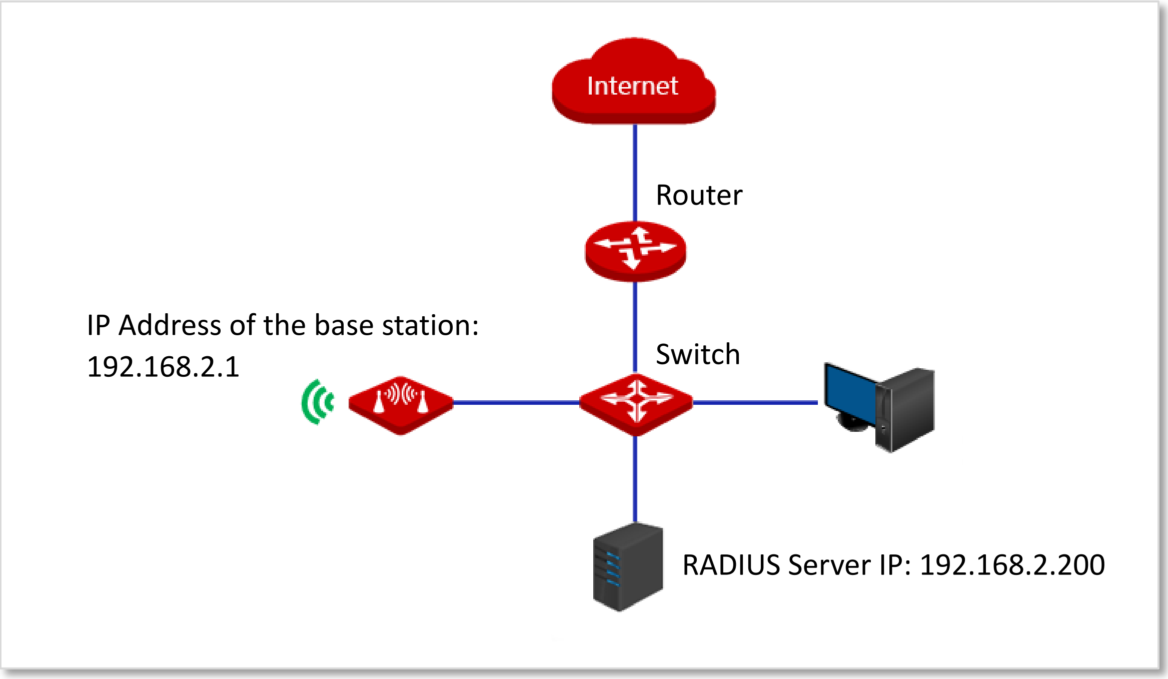
Wireless devices can connect to the wireless network named **Community** with the password **87654321**.

7.1.4 Set up a wireless network encrypted using WPA or WPA2

Networking requirement

A high secure wireless network is required and a RADIUS server is available. In this case, WPA or WPA2 mode is recommended. See the following figure.

Network topology


Internet
Router
Switch
IP Address of the base station:
192.168.2.1
RADIUS Server IP: 192.168.2.200

Configuration procedure

To configure the base station:

Assume that:

The IP address of the RADIUS server is **192.168.2.200**, the Key is **12345678**, and the port number for authentication is **1812**.

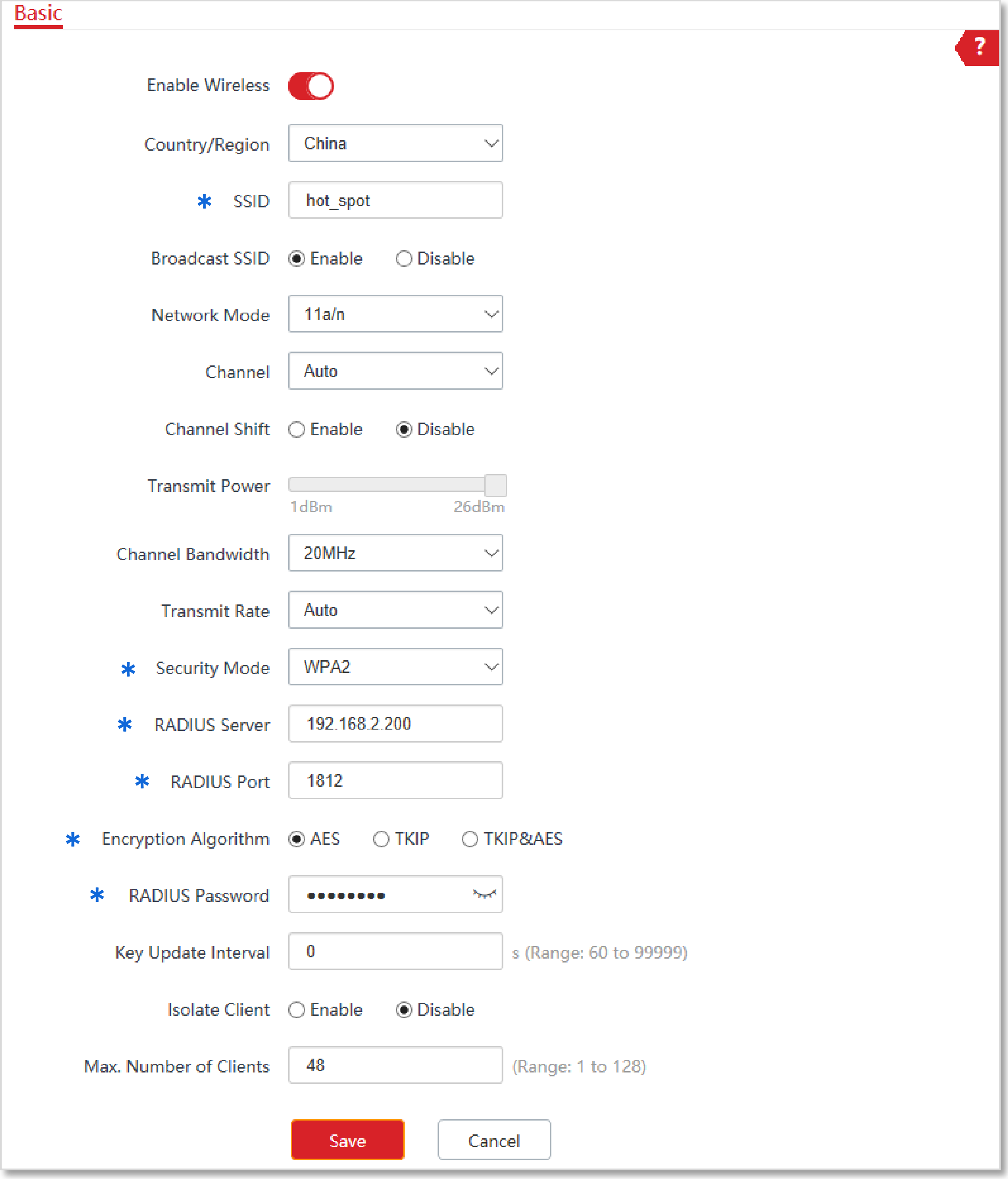
The SSID of the base station is **hot_spot**, security mode is **WPA2**, and the encryption algorithm is **AES**.

1. Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Wireless** > **Basic**.
2. Change the value of the SSID input box to **hot_spot**.
3. Set **Security Mode** to **WPA2**.

4 Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Password** to **192.168.2.200**, **1812**, and **12345678** respectively.

5 Set **Encryption Algorithm** to **AES**.

6 Click **Save**.



Basic

Enable Wireless	●
Country/Region	China
* SSID	hot_spot
Broadcast SSID	● Enable ○ Disable
Network Mode	11a/n
Channel	Auto
Channel Shift	○ Enable ● Disable
Transmit Power	1dBm 26dBm
Channel Bandwidth	20MHz
Transmit Rate	Auto
* Security Mode	WPA2
* RADIUS Server	192.168.2.200
* RADIUS Port	1812
* Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
* RADIUS Password	••••••••
Key Update Interval	0 s (Range: 60 to 99999)
Isolate Client	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)

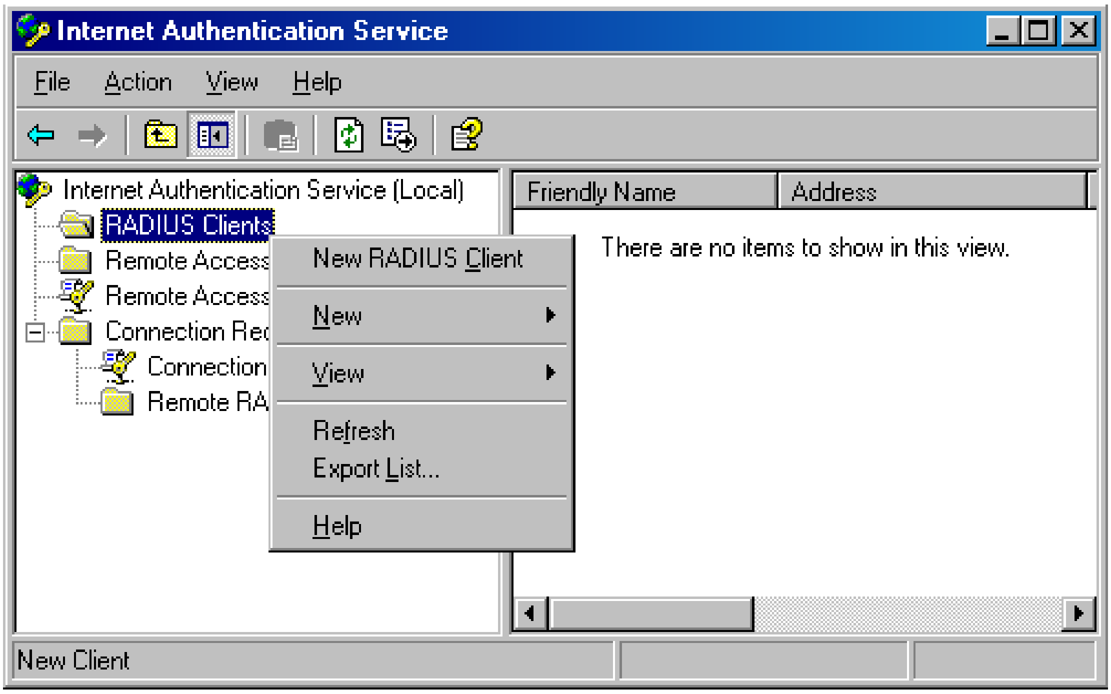
To configure the RADIUS server:

Tip

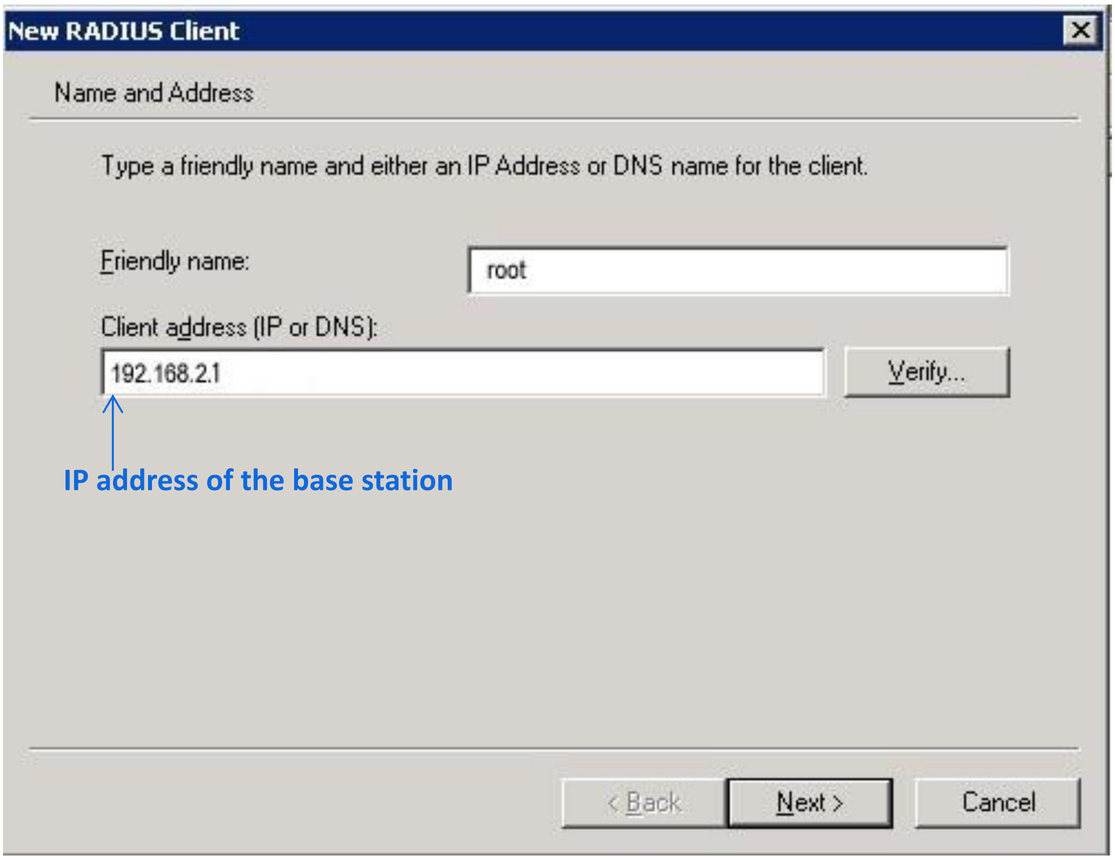
Windows 2003 is used as an example to describe how to configure the RADIUS server.

1 Configure a RADIUS client.

(1) In the Computer Management dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



(2) Enter a RADIUS client name (which can be the name of the base station) and the IP address of the base station, and click **Next**.



New RADIUS Client

Name and Address

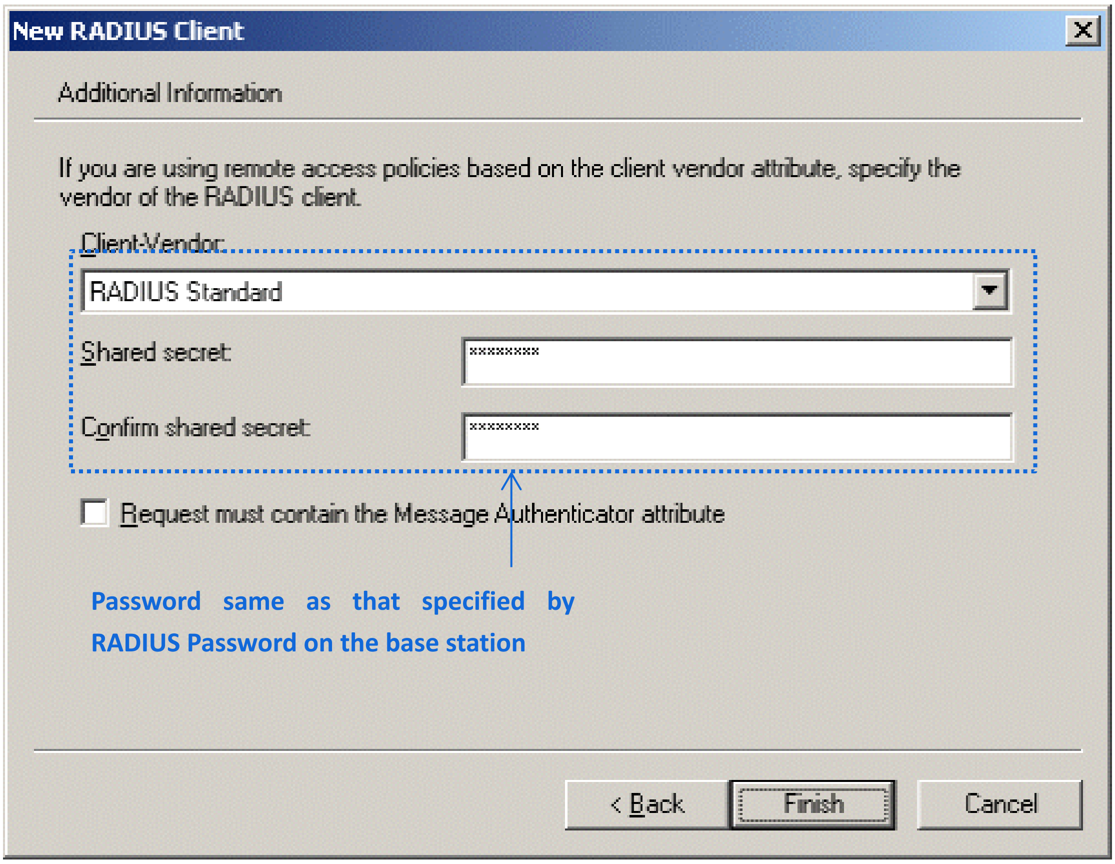
Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: root

Client address (IP or DNS): 192.168.2.1

IP address of the base station

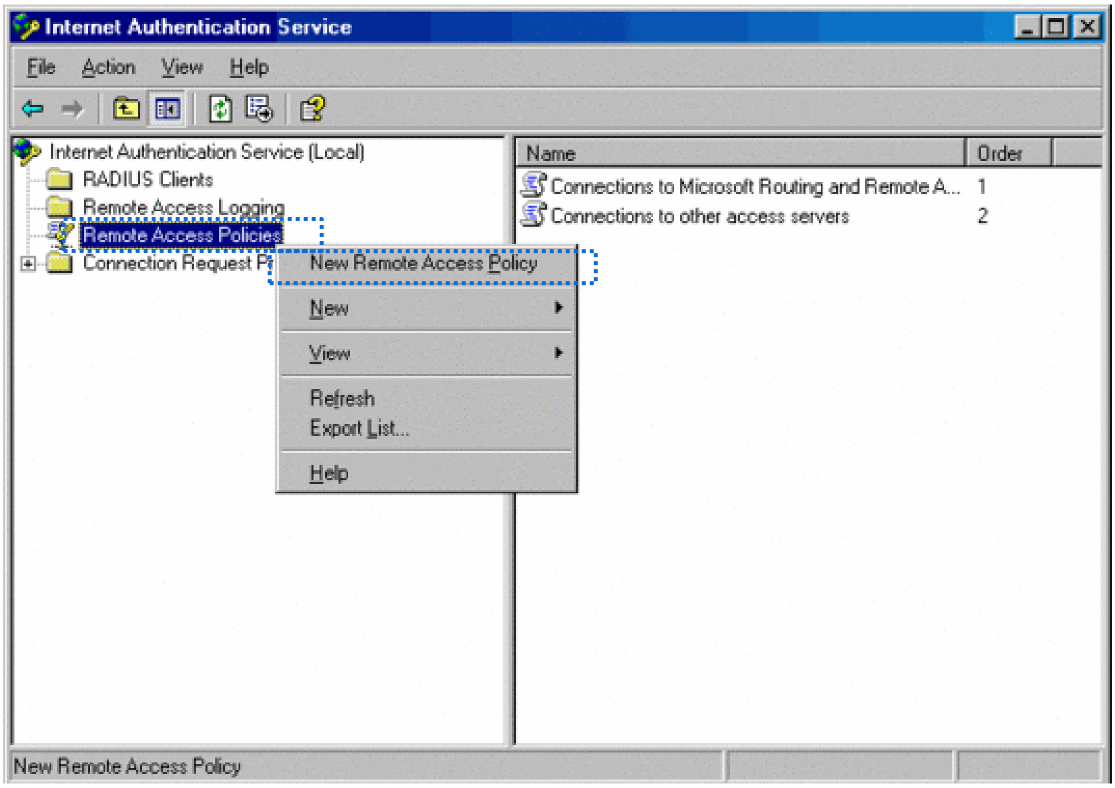
(3) Enter 12345678 in the Shared secret and Confirm shared secret input boxes, and click Finish.


New RADIUS Client
Additional Information
If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.
Client-Vendor:
RADIUS Standard
Shared secret:
****
Confirm shared secret:
****
□ Request must contain the Message Authenticator attribute
< Back
Finish
Cancel

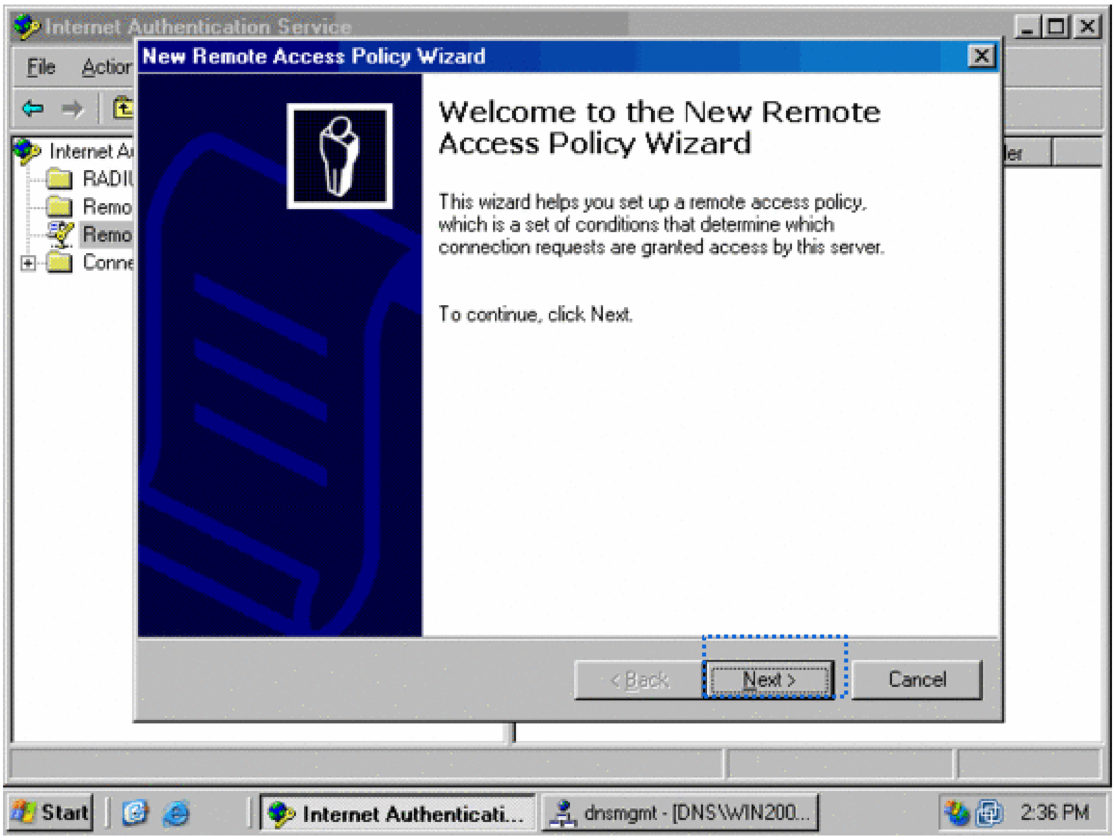
Password same as that specified by RADIUS Password on the base station

2 Configure a remote access policy.

(1) Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



(2) In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.

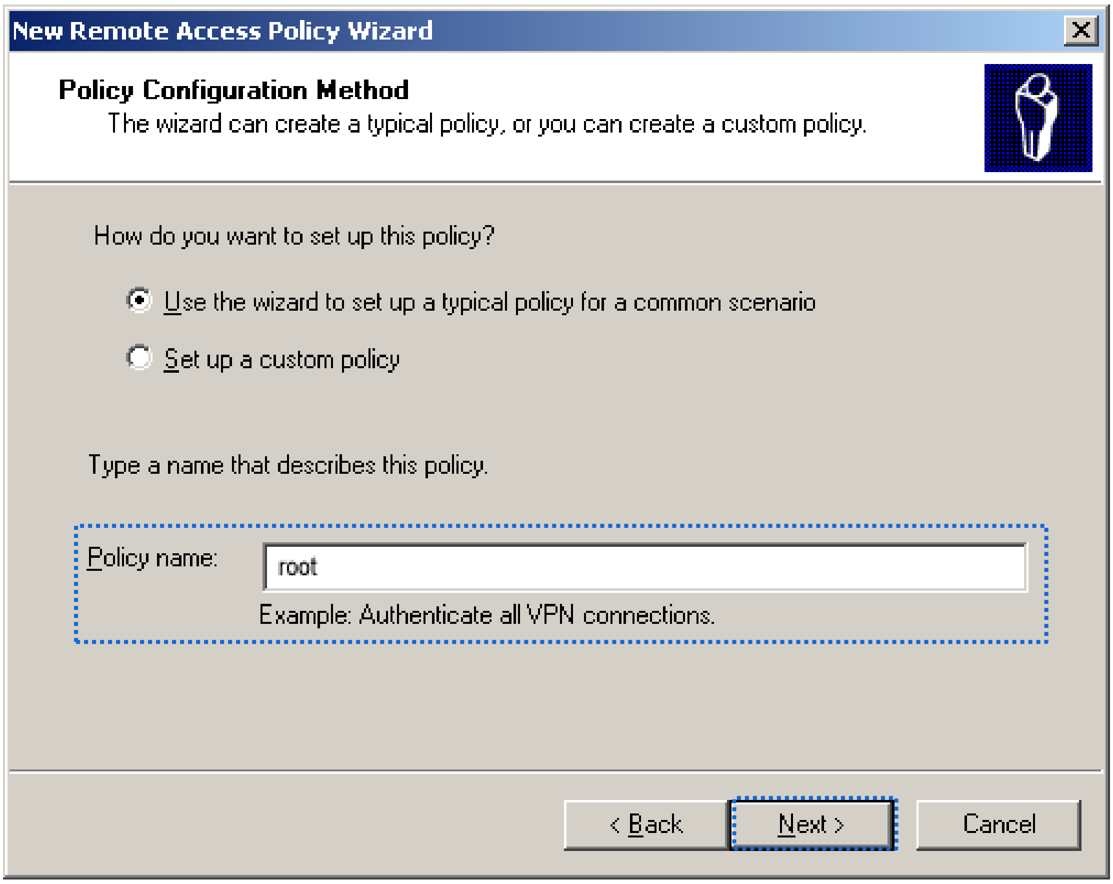


Welcome to the New Remote Access Policy Wizard

This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.

To continue, click Next.

(3) Enter a policy name and click **Next**.



New Remote Access Policy Wizard

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

● Use the wizard to set up a typical policy for a common scenario

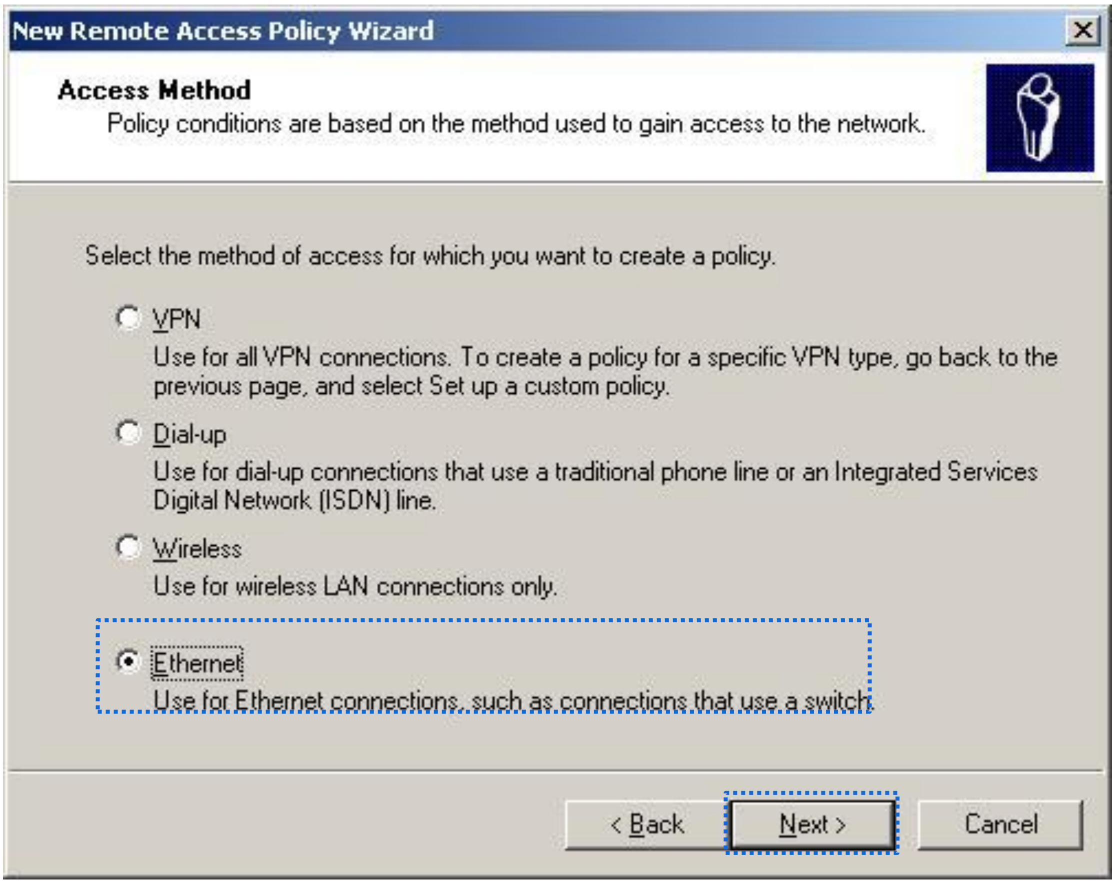
○ Set up a custom policy

Type a name that describes this policy.

Policy name: root

Example: Authenticate all VPN connections.

(4) Select **Ethernet** and click **Next**.



New Remote Access Policy Wizard

Access Method

Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

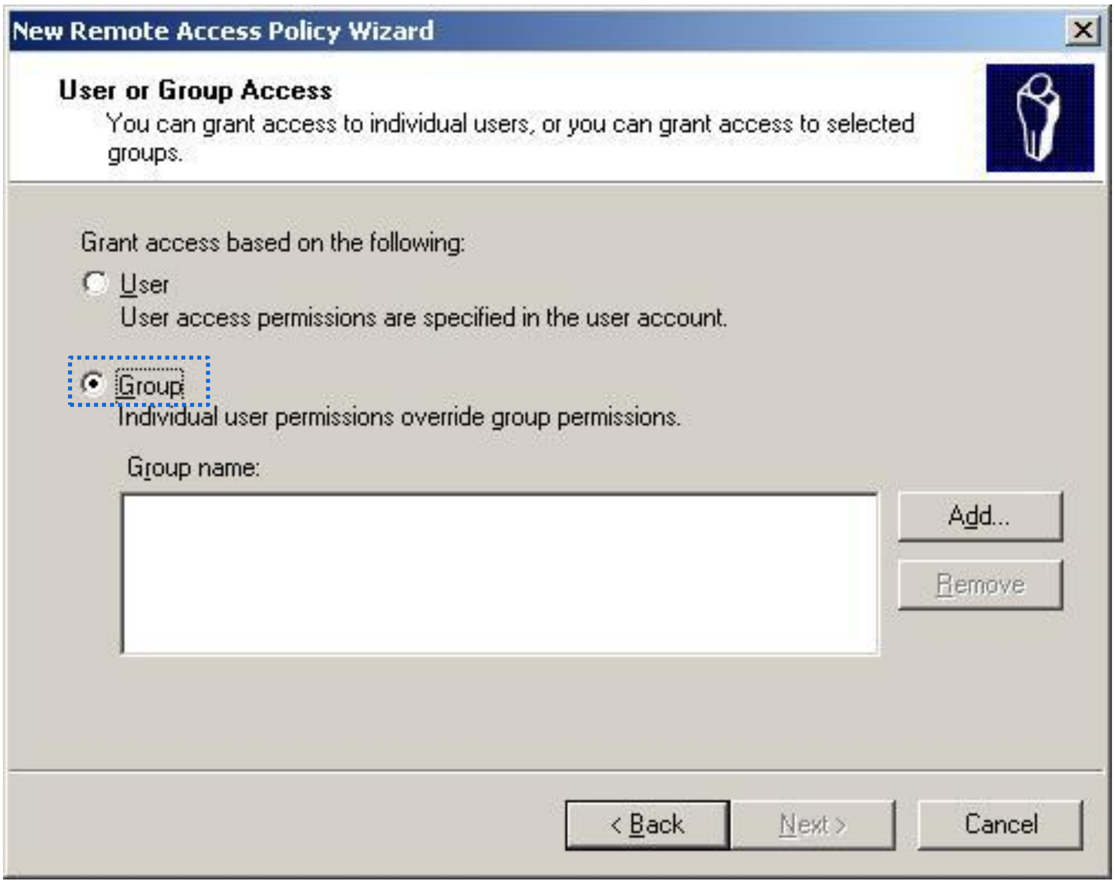
○ VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

○ Dial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

○ Wireless
Use for wireless LAN connections only.

● Ethernet
Use for Ethernet connections, such as connections that use a switch.

(5) Select **Group** and click **Add**.



New Remote Access Policy Wizard

User or Group Access

You can grant access to individual users, or you can grant access to selected groups.

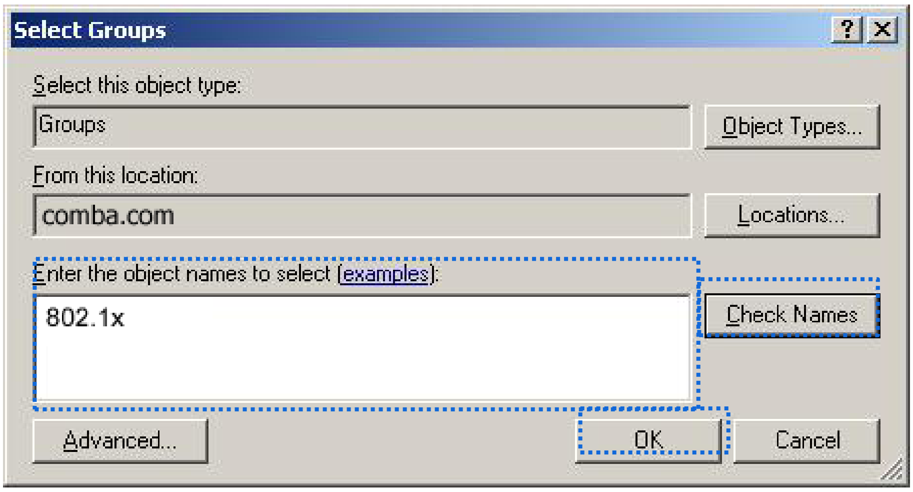
Grant access based on the following:

○ User
User access permissions are specified in the user account.

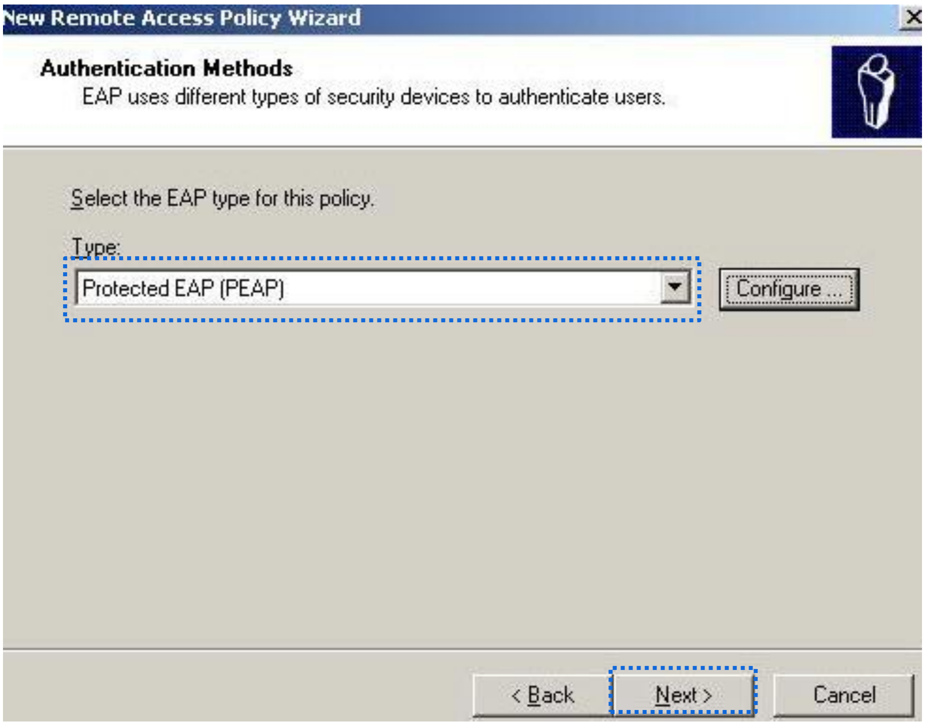
● Group
Individual user permissions override group permissions.

Group name:

(6) Enter **802.1x** in the **Ente**r the object names to select input box, click **Check Names**, and click **OK**.

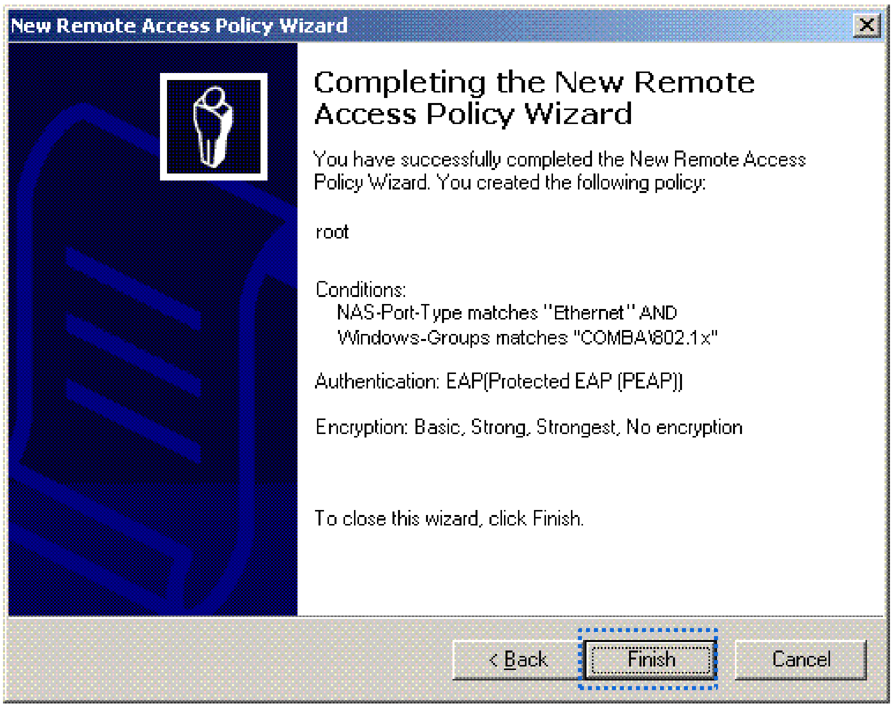


(7) Select **Protected EAP (PEAP)** and click **Next**.



New Remote Access Policy Wizard
Authentication Methods
EAP uses different types of security devices to authenticate users.
Select the EAP type for this policy.
Type:
Protected EAP (PEAP)
Configure ...
< Back
Next >
Cancel

(8) Click **Finish**. The remote access policy is created.



New Remote Access Policy Wizard

Completing the New Remote Access Policy Wizard

You have successfully completed the New Remote Access Policy Wizard. You created the following policy:

root

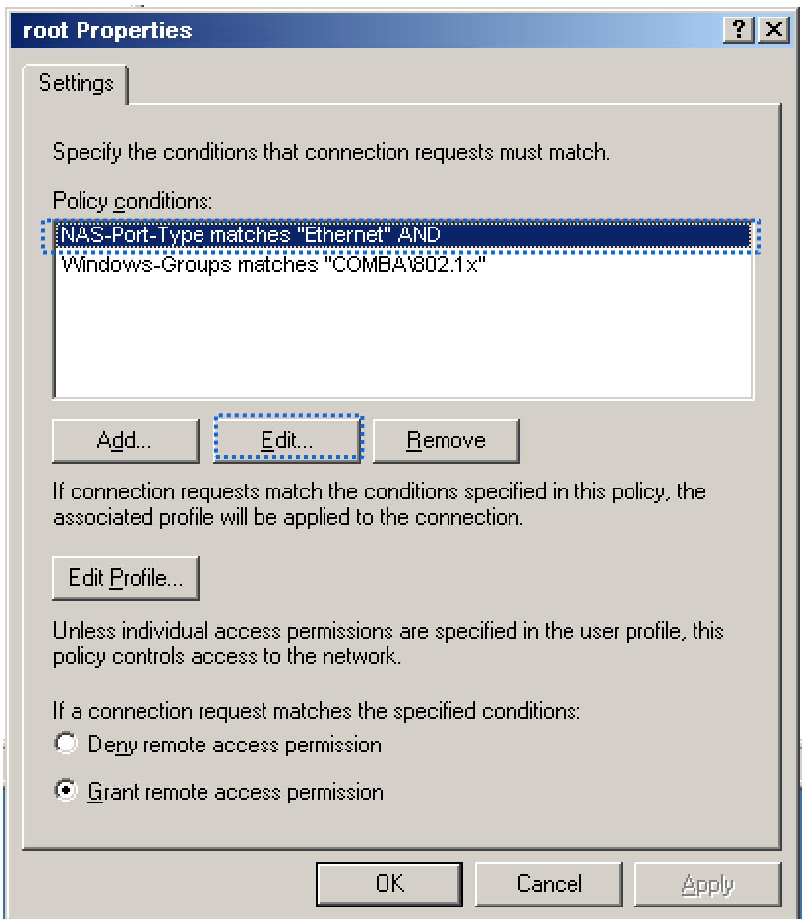
Conditions:
NAS-Port-Type matches "Ethernet" AND
Windows-Groups matches "COMBA\802.1x"

Authentication: EAP(Protected EAP (PEAP))

Encryption: Basic, Strong, Strongest, No encryption

To close this wizard, click Finish.

(9) Right-click root and choose Properties. Select Grant remote access permission, select NAS-Port-Type matches "Ethernet" AND, and click Edit.



root Properties

Settings

Specify the conditions that connection requests must match.

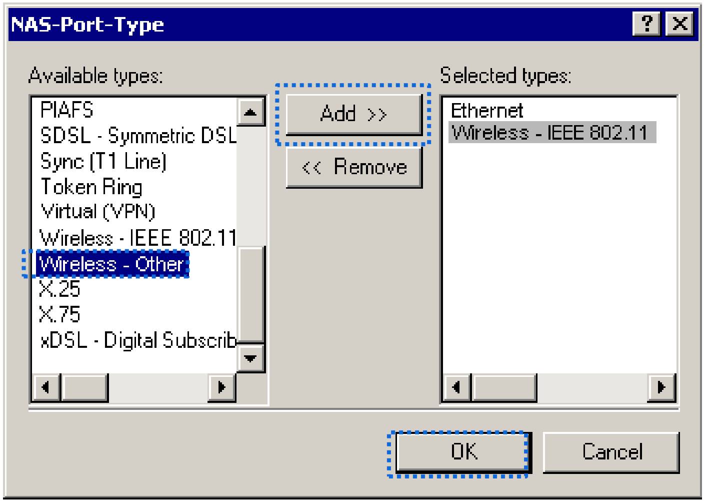
Policy conditions:
NAS-Port-Type matches "Ethernet" AND
Windows-Groups matches "COMBA\802.1x"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:
○ Deny remote access permission
● Grant remote access permission

(10) Select **Wireless – Other**, click **Add**, and click **OK**.



NAS-Port-Type

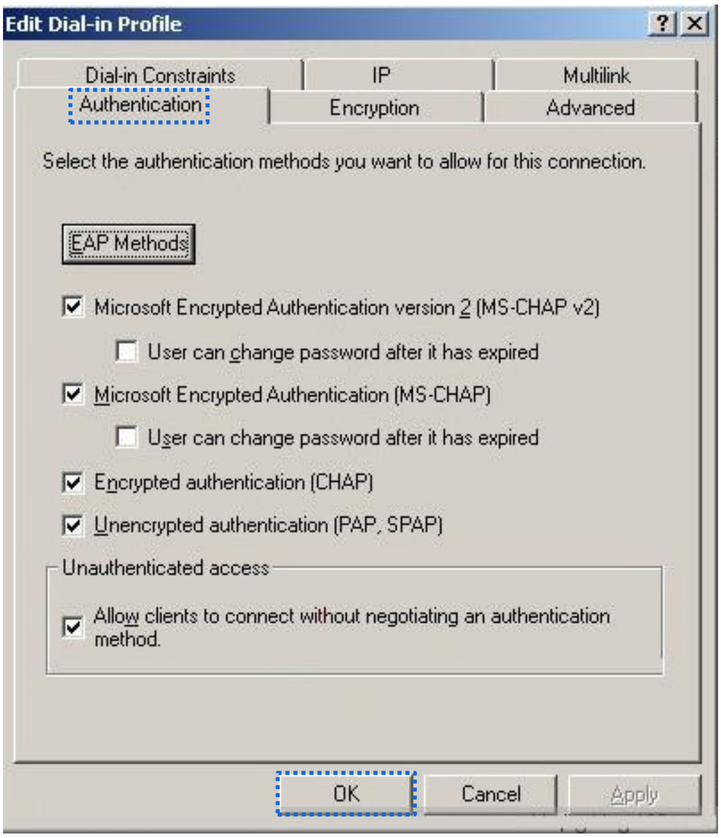
Available types:

PIAFS
SDSL - Symmetric DSL
Sync (T1 Line)
Token Ring
Virtual (VPN)
Wireless - IEEE 802.11
Wireless - Other
X.25
X.75
xDSL - Digital Subscrib

Selected types:

Ethernet
Wireless - IEEE 802.11

(11) Click **Edit Profile**, click the **Authentication** tab, configure settings as shown in the following figure, and click **OK**.



Edit Dial-in Profile

Select the authentication methods you want to allow for this connection.

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☐ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

☑ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☑ Allow clients to connect without negotiating an authentication method.

(12) When a message appears, click **No**.

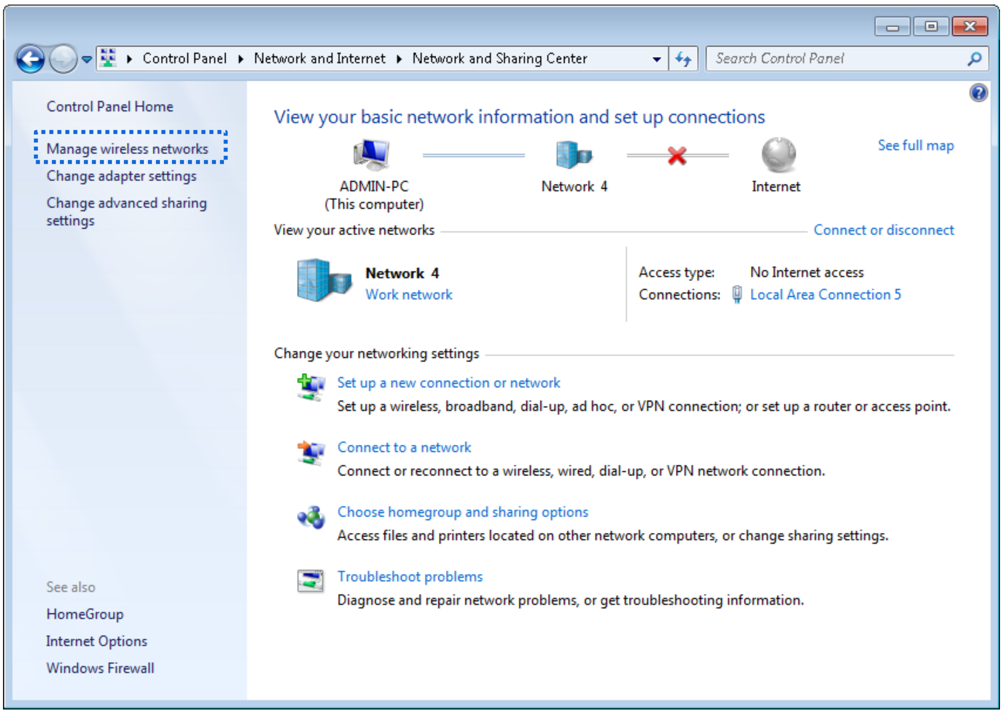
3 Configure user information. Create a user and add the user to group **802.1x**.

To configure your wireless device:

Tip

Windows 7 is taken as an example to describe the procedure.

1 Choose **Start** > **Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



Control Panel ▸ Network and Internet ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Manage wireless networks

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

View your active networks — Connect or disconnect

Network 4
Work network

Access type: No Internet access

Connections: Local Area Connection 5

Change your networking settings

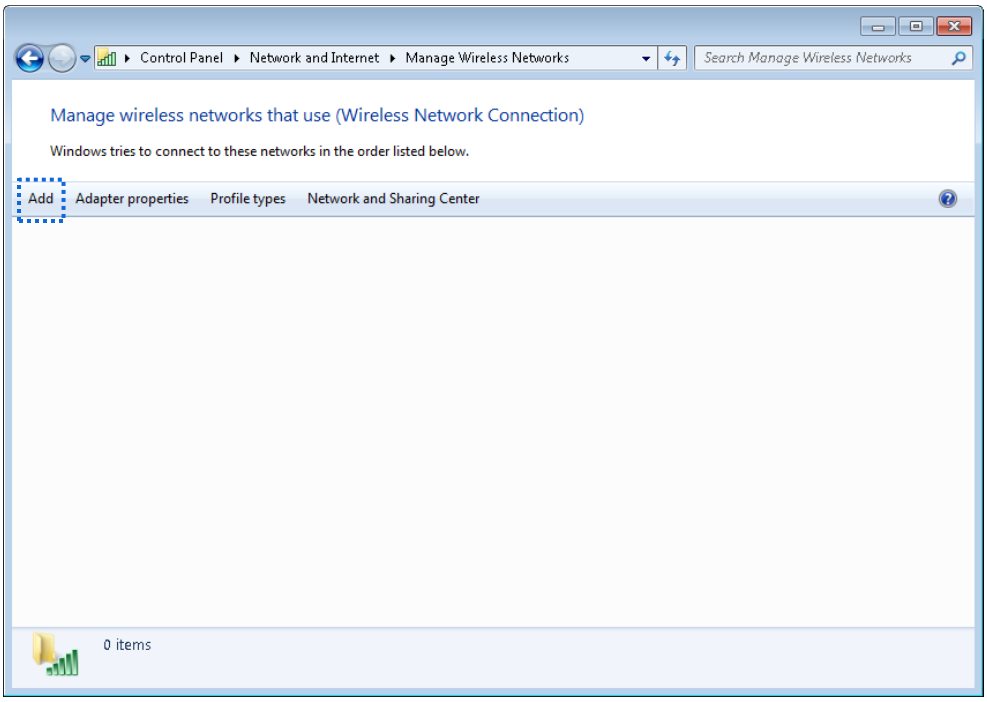
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

2 Click **Add**.



Control Panel ▸ Network and Internet ▸ Manage Wireless Networks

Search Manage Wireless Networks

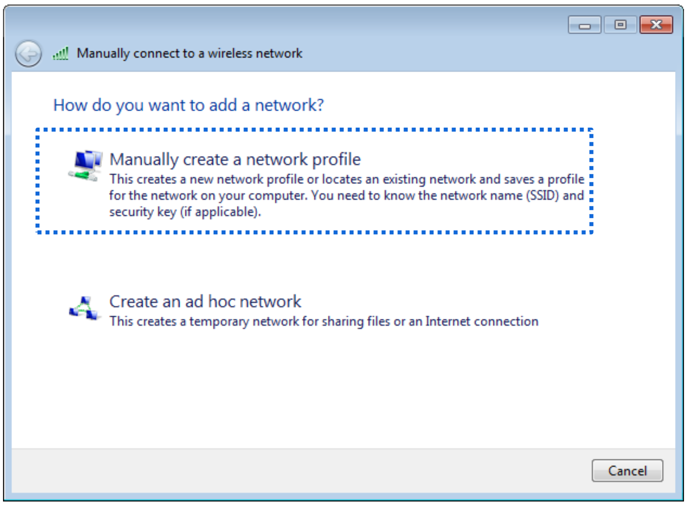
Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

Add | Adapter properties | Profile types | Network and Sharing Center

0 items

3 Click **Manually create a network profile**.



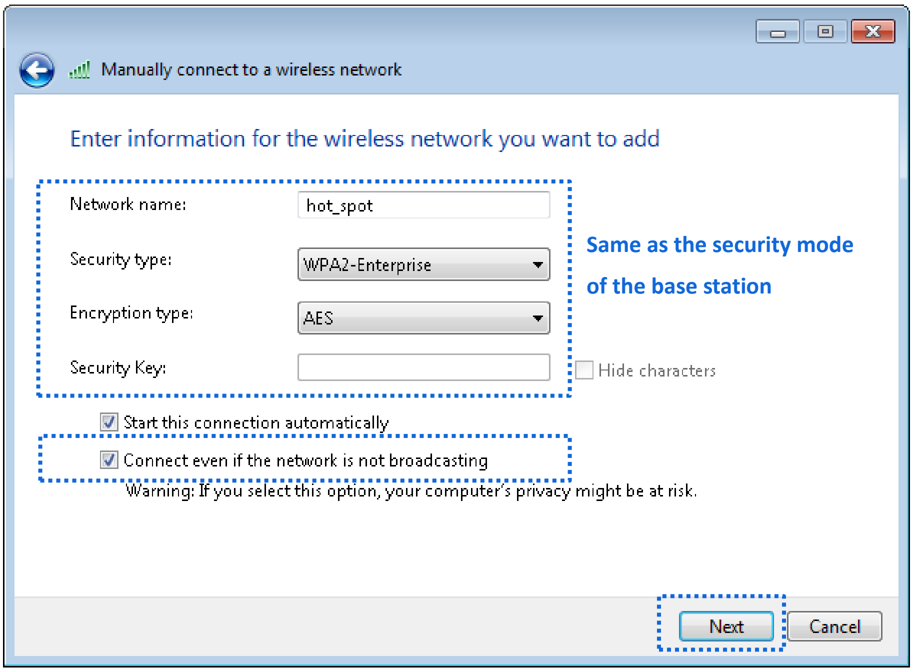
Manually connect to a wireless network

How do you want to add a network?

Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).

Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection

4 Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: hot_spot

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

□ Hide characters

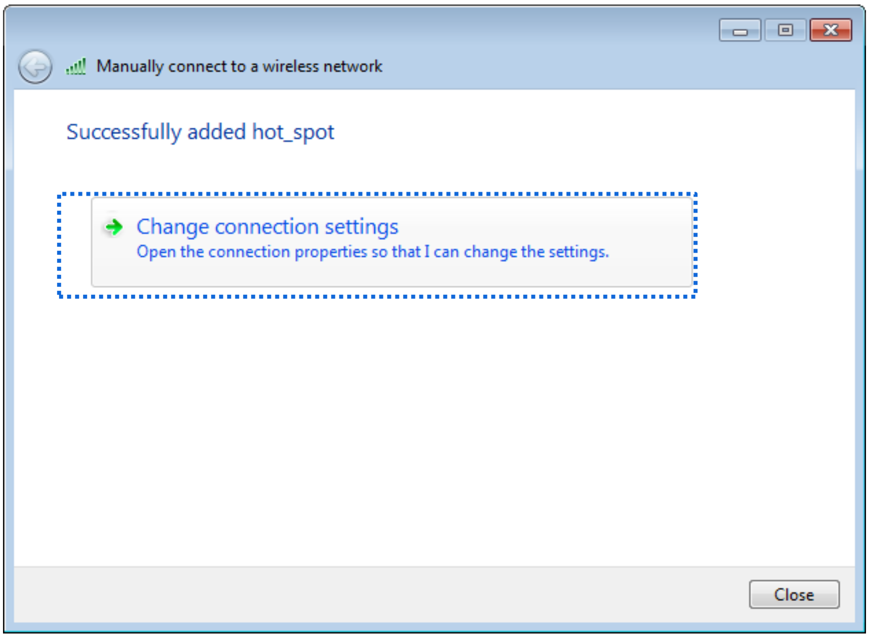
☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Same as the security mode of the base station

5 Click **Change connection settings**.

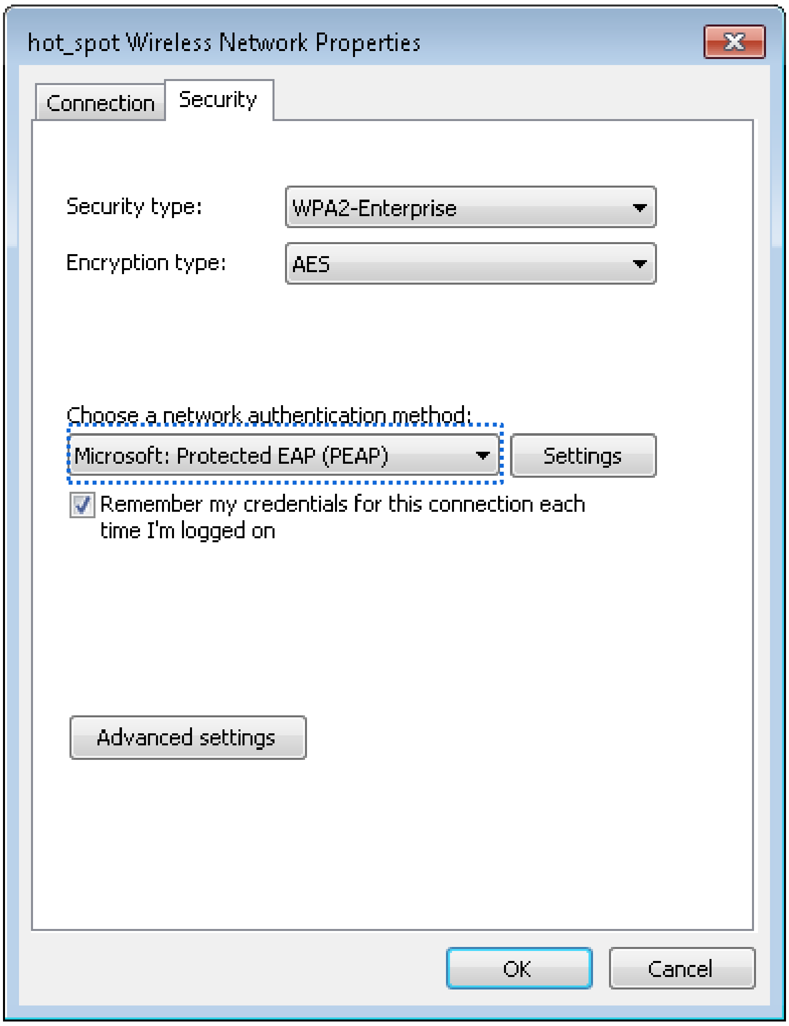


Manually connect to a wireless network

Successfully added hot_spot

Change connection settings
Open the connection properties so that I can change the settings.

6 Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



hot_spot Wireless Network Properties

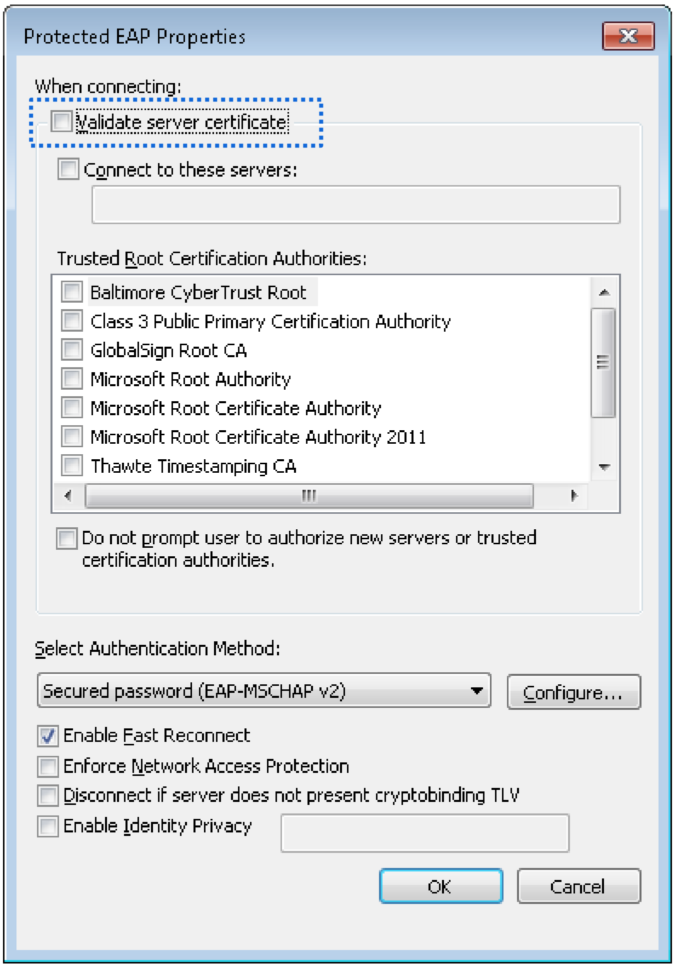
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:
Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

7 Deselect **Validate server certificate** and click **Configure**.



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ Baltimore CyberTrust Root
□ Class 3 Public Primary Certification Authority
□ GlobalSign Root CA
□ Microsoft Root Authority
□ Microsoft Root Certificate Authority
□ Microsoft Root Certificate Authority 2011
□ Thawte Timestamping CA

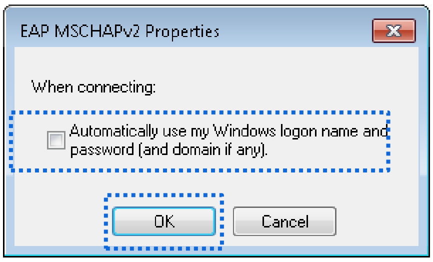
□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

8 Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.

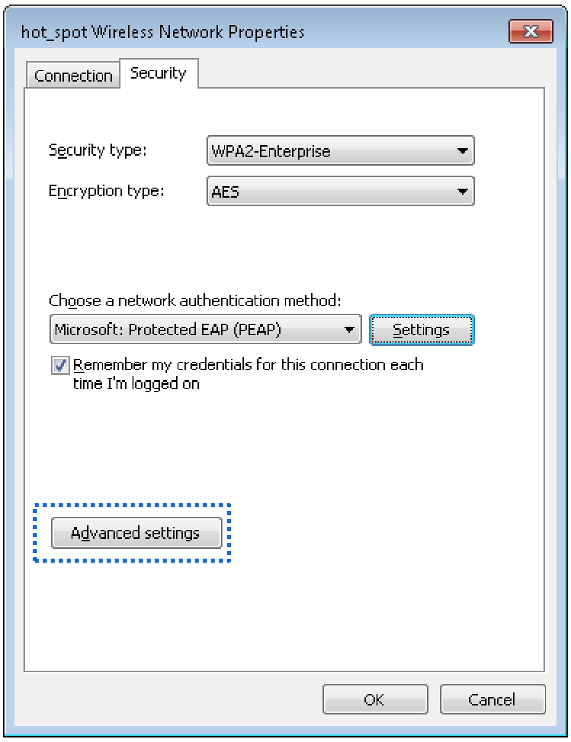


EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

9 Click **Advanced settings**.



Security type: WPA2-Enterprise

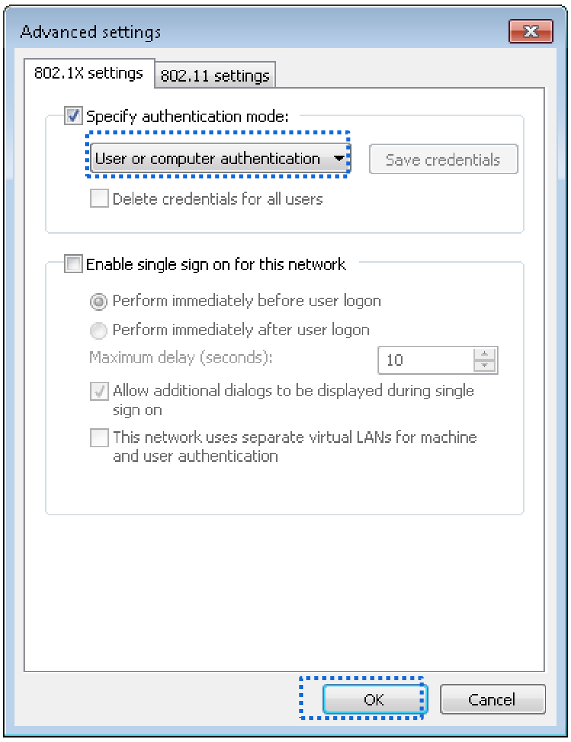
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

10 Select **User or computer authentication** and click **OK**.



☑ Specify authentication mode:

User or computer authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

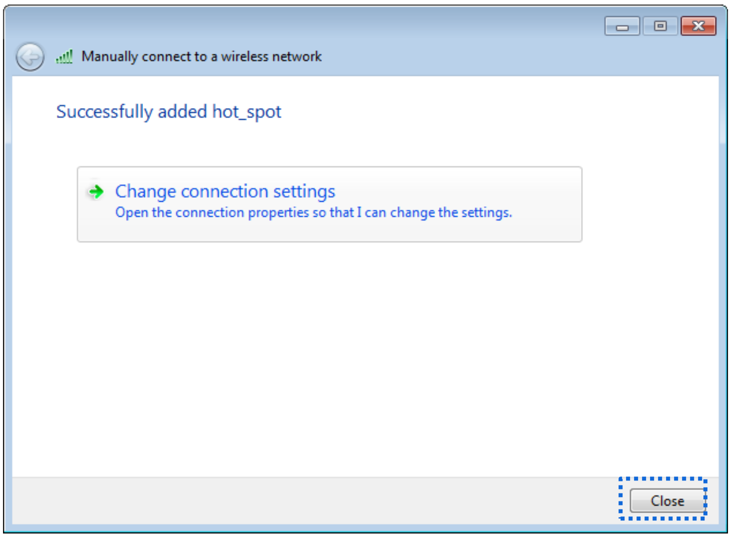
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

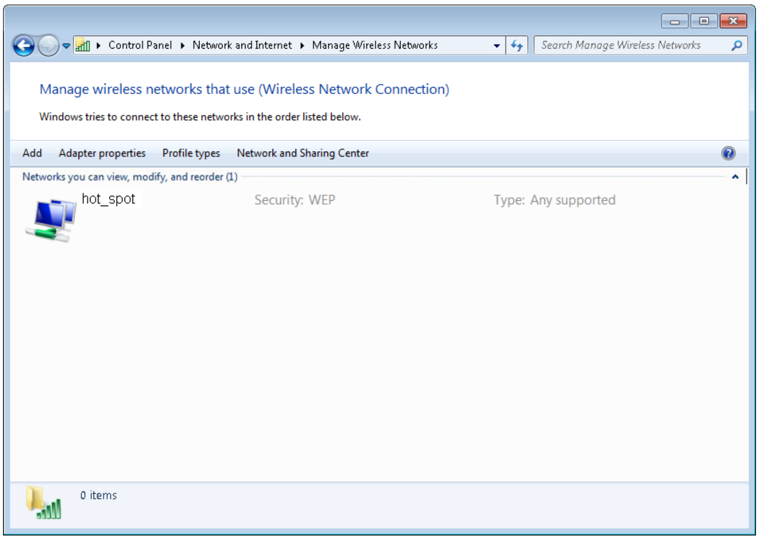
11 Click **Close**.



Manually connect to a wireless network
Change connection settings
Close

Successfully added hot_spot

Open the connection properties so that I can change the settings.



Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Networks
Add
Adapter properties
Profile types
Network and Sharing Center
0 items

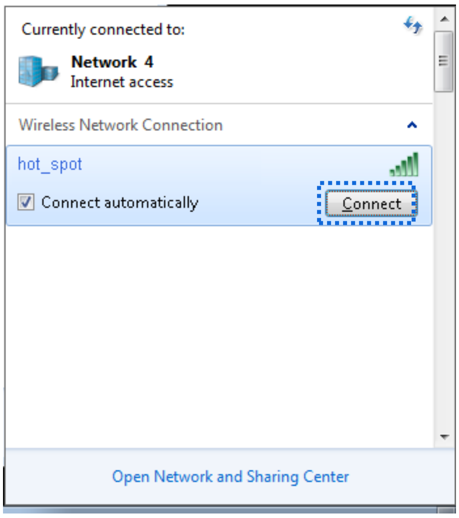
Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

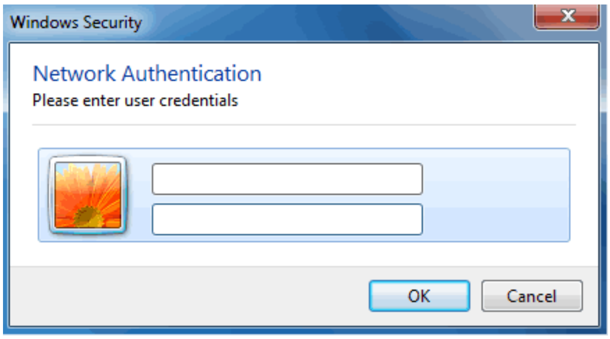
Networks you can view, modify, and reorder (1)

hot_spot Security: WEP Type: Any supported

12 Click the network icon in the lower-right corner of the desktop and choose the wireless network of the base station such as **hot_spot** in this example.



13 In the Windows Security dialog box that appears, enter the user name and password set on the RADIUS server and click **OK**.



---End

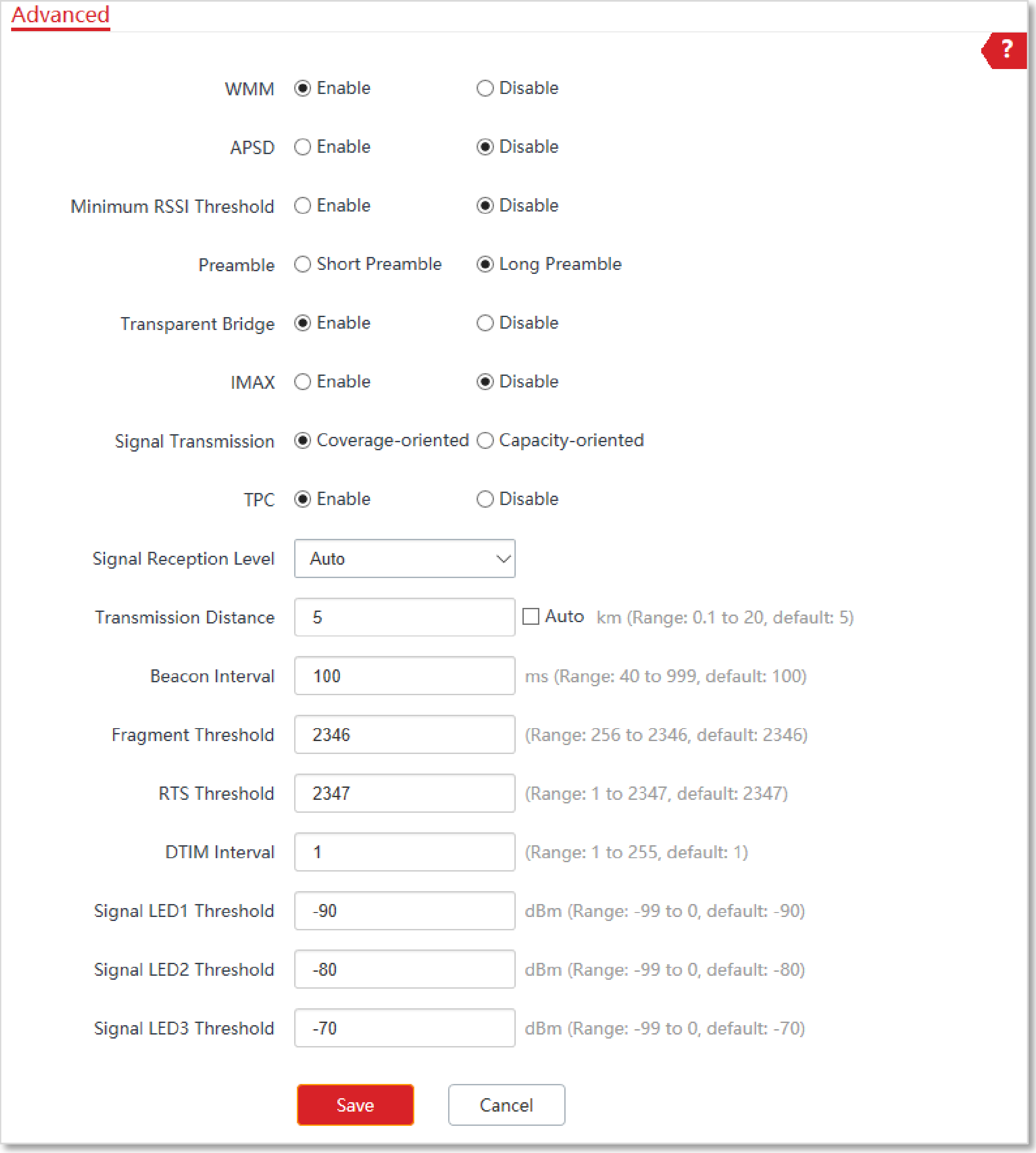
Verification

Wireless devices can connect to the wireless network **hot_spot**.

7.2 Advanced

This module enables you to adjust the wireless performance. You are recommended to configure it under the Professional guidance.

Choose **Wireless** > **Advanced** to enter the page.



Advanced

WMM	● Enable	○ Disable
APSD	○ Enable	● Disable
Minimum RSSI Threshold	○ Enable	● Disable
Preamble	○ Short Preamble	● Long Preamble
Transparent Bridge	● Enable	○ Disable
IMAX	○ Enable	● Disable
Signal Transmission	● Coverage-oriented	○ Capacity-oriented
TPC	● Enable	○ Disable
Signal Reception Level	Auto	
Transmission Distance	5	□ Auto km (Range: 0.1 to 20, default: 5)
Beacon Interval	100	ms (Range: 40 to 999, default: 100)
Fragment Threshold	2346	(Range: 256 to 2346, default: 2346)
RTS Threshold	2347	(Range: 1 to 2347, default: 2347)
DTIM Interval	1	(Range: 1 to 255, default: 1)
Signal LED1 Threshold	-90	dBm (Range: -99 to 0, default: -90)
Signal LED2 Threshold	-80	dBm (Range: -99 to 0, default: -80)
Signal LED3 Threshold	-70	dBm (Range: -99 to 0, default: -70)

Parameters description

Parameter	Description
WMM	WMM (Wi-Fi Multi-media) is a wireless QoS protocol making packets with higher priorities are transmitted earlier. This ensures better QoS of voice and video applications over wireless networks.
APSD	It specifies whether to enable the Automatic Power Save Delivery (APSD) mode.

Parameter	Description
	APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
Minimum RSSI Threshold	It specifies the minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device. If there are multiple devices in a network, setting a proper value helps wireless devices connect to WiFi network with better WiFi signal.
Preamble	It specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. **Long Preamble (default)**: Applies to a large area with less interference nearby. **Short Preamble**: Applies to an area with strong interference nearby. This mode improves the device's anti-interference capability.
Transparent Bridge	With this function enabled, the base station can achieve bidirectional transparent transmission, solving the problem that the NVR cannot detect IP cameras. Tip Only available in **AP**, **Client**, and **Universal Repeater** modes.
TD-MAX	TD-MAX is IP-COM's proprietary Time Division Multiple Access (TDMA) polling technology. It allows multiple clients to share the same channel for accessing to a network. With the TD-MAX enabled, the base station assigns time slots to each client, and transmits data according to the assigned time slots, achieving Point-to-MultiPoint (P2MP) connections. – After the TD-MAX is enabled, the base station: – Avoids the "hidden node" problem, which occurs when a node is visible from a wireless AP, but not from other nodes communicating with the originating AP. – Reduces latency. – Improves throughput and anti-interference performance. – Improves overall performance in Point-to-MultiPoint (PtMP) installations, and increases the maximum possible number of users that can associate with an AP that uses TD-MAX. Tip If the TD-MAX is enabled, the device operates in TD-MAX mode and only accepts connections from TD-MAX devices. And you cannot connect standard Wi-Fi devices, such as laptops, tablets, or smart phones, to the base station.
Signal Transmission	It specifies the wall penetrating capability of the device. – **Coverage-oriented**: With less interference nearby, this mode enables the device to cover wider area. – **Capacity-oriented**: With strong interference nearby, this mode improves the device's anti-interference capability.
TPC	The Transmit Power Control (TPC) function decreases the TX power of this device automatically to improve the negotiation rate when the two devices are too close By default, when the received signal strength is greater than -25 dBm, the device decreases its TX power. The received signal strength can be checked on

Parameter	Description
	the **Status** > **Wireless Status** page.
Signal Reception Level	It is used to adjust the signal reception level. A higher level leads to better signal reception capability, but lower throughput. Adjust the level based on your actual situation.
Transmission Distance	It specifies the wireless transmission distance of this device. You can set it based on the actual installation distance.
Beacon Interval	It specifies the interval at which this device sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.
Fragment Threshold	It specifies the threshold of a fragment. The unit is byte. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold to enable this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput.
RTS Threshold	It specifies the frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	It specifies the countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval. For example, if DTIM Interval is set to 1, this device transmits all cached frames at one Beacon interval.
Signal LED1/2/3 Threshold	The device uses three signal LED indicators to indicate the received signal strength in an intuitive way, and allows you to customize the threshold for triggering each signal LED indicator to light up. The default threshold for LED1, LED2, and LED3 are **-90**, **-80**, and **-70** respectively.

7.3 Access control

7.3.1 Overview

The device allows you to set whitelist (allow to access the internet) or blacklist (disallow to access the internet) based on wireless clients’ MAC addresses.

7.3.2 Configure access control

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Wireless** > **Access Control**.

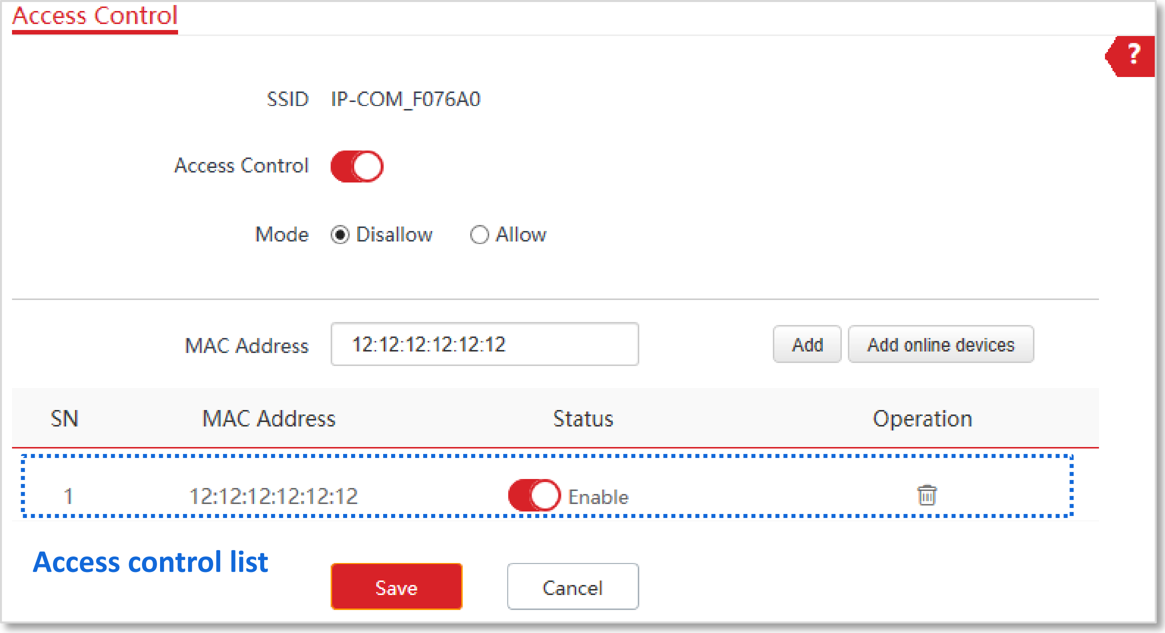
2 Set the **Access Control** to ●.

3 Select a MAC address filter mode, **Disallow** or **Allow**.

4 Add the client to be controlled.

- Manual enter: Enter the MAC address of the client in the **MAC Address** input box, and click **Add**.
- Quick add: Click **Add online devices** to add all connected clients to the access control list quickly.

5 Click **Save**.



Access Control

SSID IP-COM_F076A0

Access Control ●

Mode ● Disallow ○ Allow

MAC Address 12:12:12:12:12:12

SN	MAC Address	Status	Operation
1	12:12:12:12:12:12	● Enable	🗑

Access control list

---End

Parameters description

Parameter	Description
SSID	It specifies the SSID of this device. With the rule enabled, clients connected to the network with this SSID will be controlled by the rule.
Access Control	It specifies whether to enable the function.
Mode	It specifies the mode for filtering MAC addresses. – **Allow**: It indicates that only the wireless clients on the access control list can connect to the WiFi network of the device. – **Disallow**: It indicates that only the wireless clients on the access control list cannot connect to the WiFi network of the device.

7.3.3 Example of configuring access control

Networking requirement

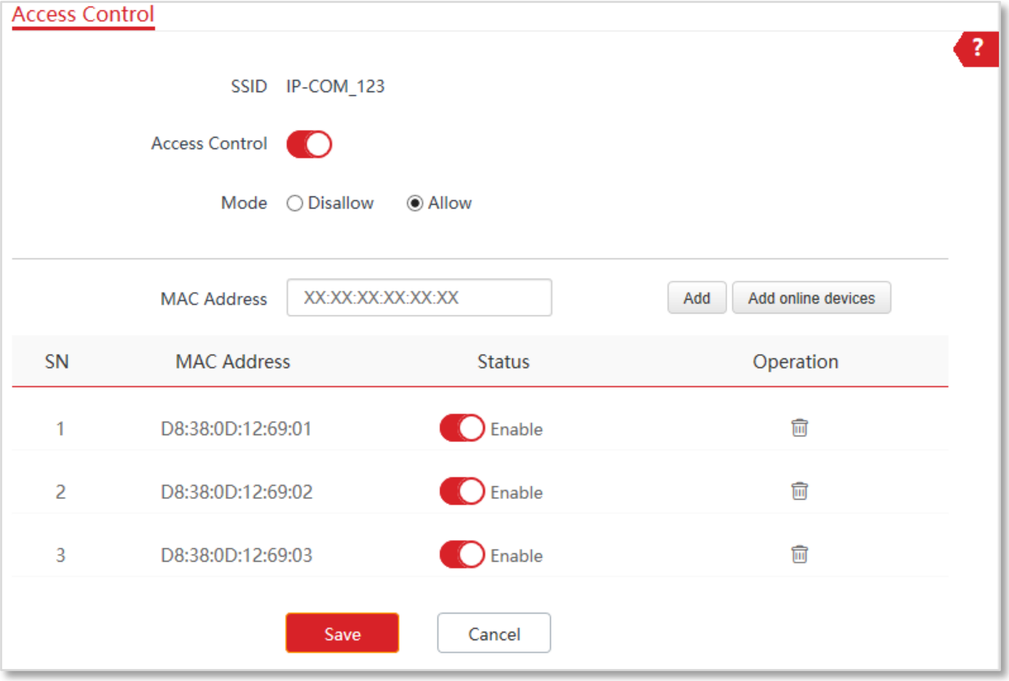
A wireless network named **Connect me** has been set up in a residential community. Only the community members are allowed to connect to the wireless network.

Solution

The **Access Control** function of the base station is recommended. Assume that the users have three wireless devices whose MAC addresses are D8:38:0D:12:69:01, D8:38:0D:12:69:02, and D8:38:0D:12:69:03.

Configuration procedure

1. Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Wireless** > **Access Control**.
2. Enable the **Access Control** function.
3. Set the **Mode** to **Allow**.
4. Enter the MAC addresses one by one and click **Add**.
5. Click **Save**.



Access Control

SSID IP-COM_123

Access Control

Mode ○ Disallow ● Allow

MAC Address XX:XX:XX:XX:XX:XX

SN	MAC Address	Status	Operation
1	D8:38:0D:12:69:01	Enable	
2	D8:38:0D:12:69:02	Enable	
3	D8:38:0D:12:69:03	Enable	

---End

Verification

Only wireless devices with the MAC addresses included in the rules can connect to the WiFi network named **Connect Me**.

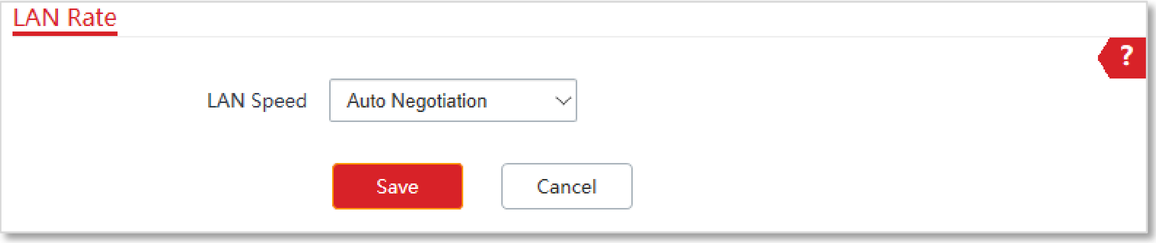
8 Advanced

8.1 LAN rate

This module enables you to change LAN speed and duplex mode settings. If the transmission distance between the ports of the base station and peer device is too long, you can reduce the port speed of the base station and peer device to increase the driving distance.

When you change the settings, ensure that the LAN speed and duplex mode of the port of the device is the same as that of peer device. By default, the LAN speed settings of the LAN port is **Auto Negotiation**.

To access the page, choose **Advanced** > **LAN Rate**.



LAN Rate

LAN Speed: Auto Negotiation

8.2 Diagnose

8.2.1 Overview

You can use the diagnosis tools for troubleshooting. The device supports the following tools:

- **Site Survey**: used to check nearby wireless signals.
- **Ping**: used to check the network connectivity.
- **Traceroute**: used to check the network routes.
- **Speed Test**: used to check the connection speed between two devices in a same network.
- **Spectrum Analysis**: used to check the nearby wireless noise of each channel, then select a frequency band with less wireless noise for the base station.

To access the page, choose **Advanced** > **Diagnose**.

8.2.2 Site Survey

Site survey gives you an insight into the information of nearby wireless signals. According to the diagnosis result, you can select a less interference channel (used by few devices) for the WiFi network of the device to improve the transmission efficiency.

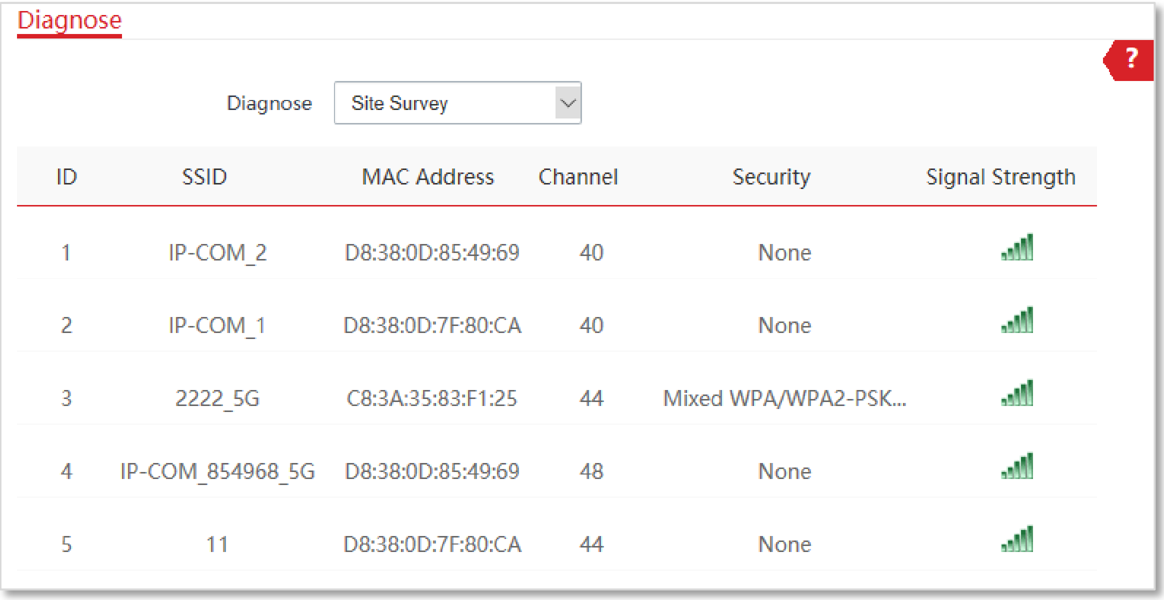
Configuration procedure

1 Start a web browser on the computer connected to the base station, visit 192.168.2.1 and choose **Advanced** > **Diagnose**.

2 Select Site Survey from the Diagnose drop-down list menu.

---End

The diagnosis result will be displayed in a few seconds below the **Diagnose** input box. See the following figure:



Diagnose: Site Survey

ID	SSID	MAC Address	Channel	Security	Signal Strength
1	IP-COM_2	D8:38:0D:85:49:69	40	None	📶
2	IP-COM_1	D8:38:0D:7F:80:CA	40	None	📶
3	2222_5G	C8:3A:35:83:F1:25	44	Mixed WPA/WPA2-PSK...	📶
4	IP-COM_854968_5G	D8:38:0D:85:49:69	48	None	📶
5	11	D8:38:0D:7F:80:CA	44	None	📶

8.2.3 Ping

You can use ping to detect the connectivity and quality of network connection.

Assume that you want to know whether the device can access **Bing**.

Configuration procedure

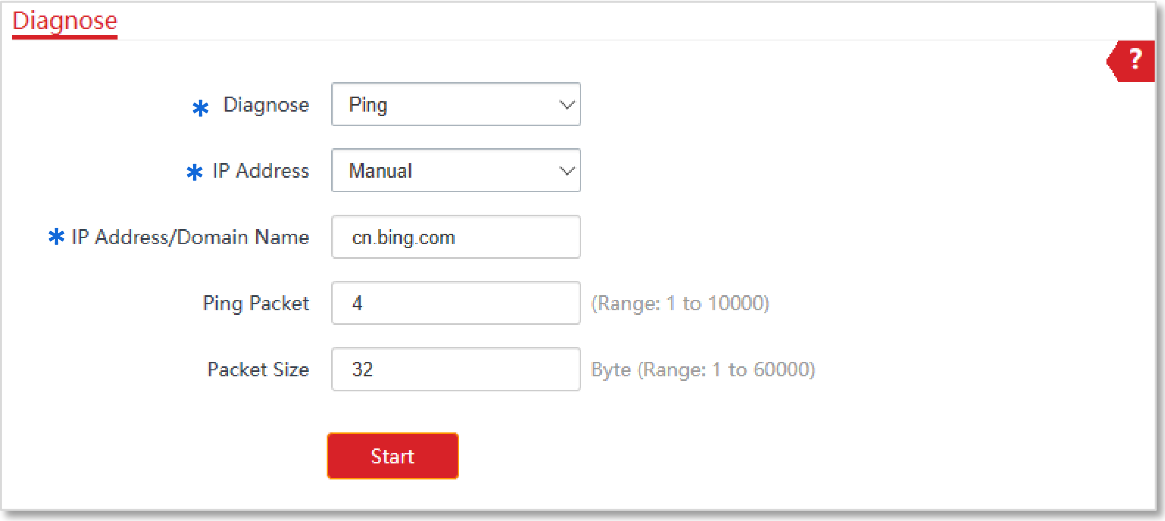
1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Diagnose**.

2 Select **Ping** from the **Diagnose** drop-down list menu.

3 Set **IP Address** to **Manual**.

4 Enter the target IP address or a domain name, which is **cn.bing.com** in this example.

5 Click **Start**.



Diagnose

* Diagnose: Ping

* IP Address: Manual

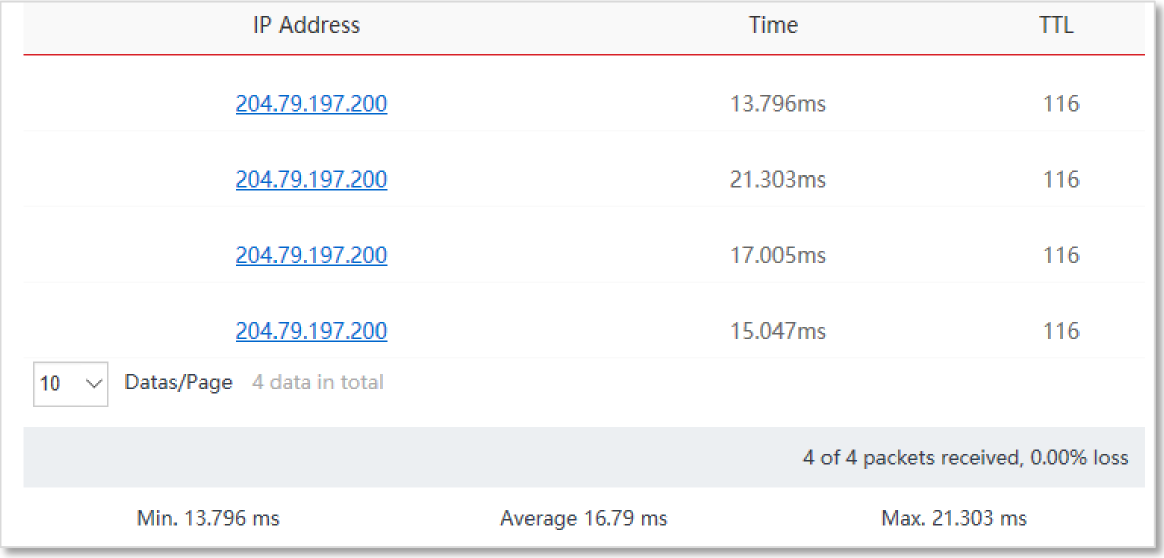
* IP Address/Domain Name: cn.bing.com

Ping Packet: 4 (Range: 1 to 10000)

Packet Size: 32 Byte (Range: 1 to 60000)

---End

The diagnosis result will be displayed in a few seconds below **Start** button. See the following figure:



IP Address	Time	TTL
204.79.197.200	13.796ms	116
204.79.197.200	21.303ms	116
204.79.197.200	17.005ms	116
204.79.197.200	15.047ms	116

10 Datas/Page 4 data in total

4 of 4 packets received, 0.00% loss

Min. 13.796 ms Average 16.79 ms Max. 21.303 ms

8.2.4 Traceroute

You can use the Traceroute tool to detect the routes that the packets pass by from the device to destination host.

Assume that you want to detect the routes that the packets pass by from the device to **cn.bing.com**.

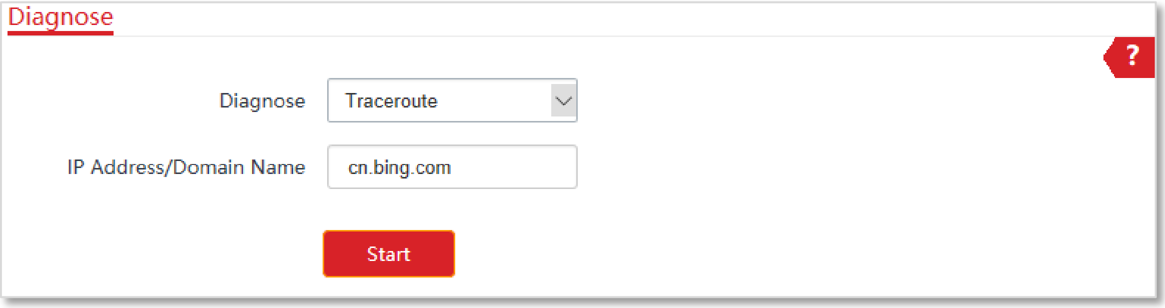
Configuration procedure

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Diagnose**.

2 Select **Traceroute** from the **Diagnose** drop-down list menu.

3 Enter the target IP address or a domain name, which is **cn.bing.com** in this example.

4 Click **Start**.



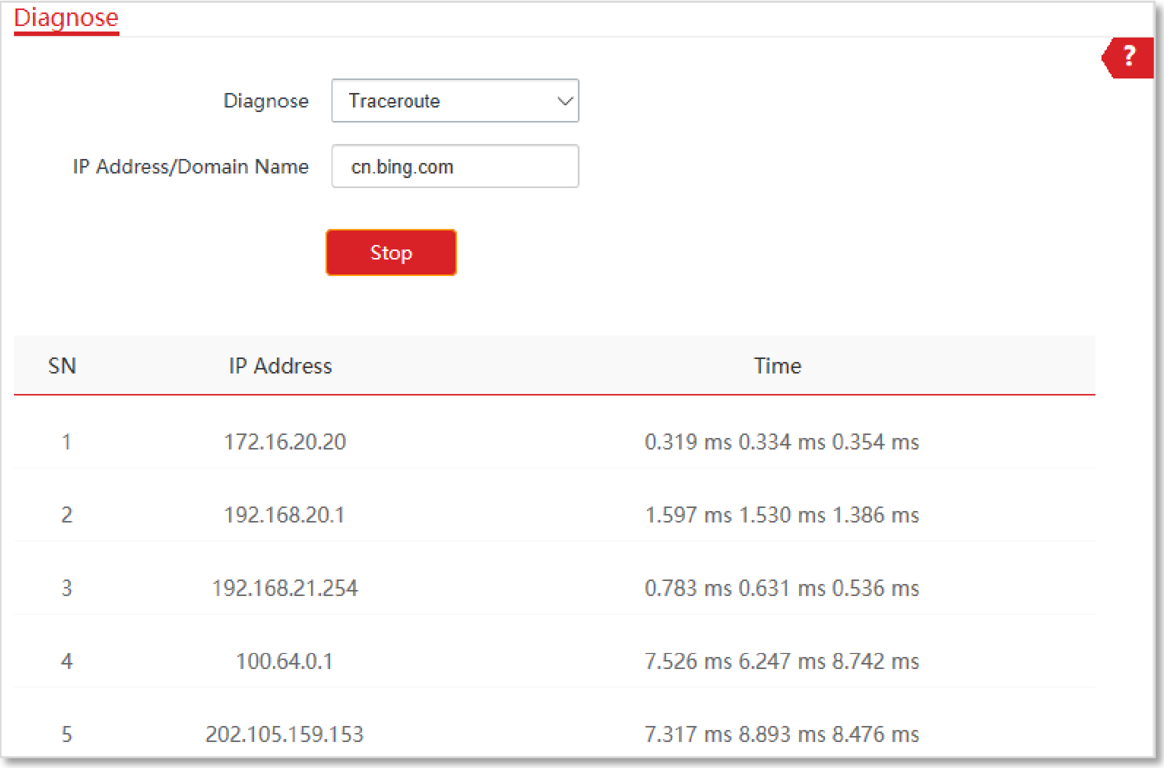
Diagnose

Diagnose: Traceroute

IP Address/Domain Name: cn.bing.com

---End

The diagnosis result will be displayed in a few seconds below **Start** button. See the following figure:



Diagnose: Traceroute

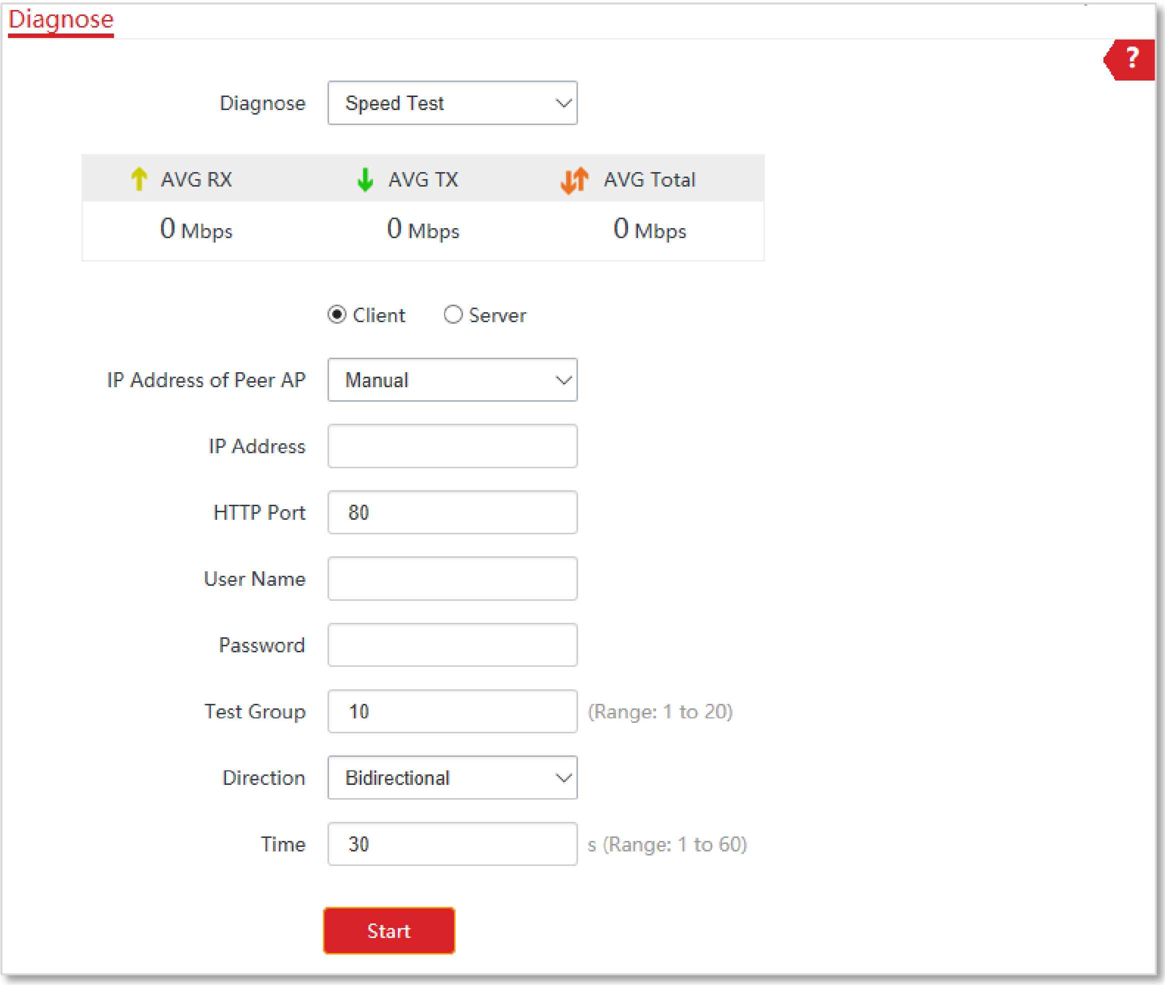
IP Address/Domain Name: cn.bing.com

SN	IP Address	Time
1	172.16.20.20	0.319 ms 0.334 ms 0.354 ms
2	192.168.20.1	1.597 ms 1.530 ms 1.386 ms
3	192.168.21.254	0.783 ms 0.631 ms 0.536 ms
4	100.64.0.1	7.526 ms 6.247 ms 8.742 ms
5	202.105.159.153	7.317 ms 8.893 ms 8.476 ms

8.2.5 Speed test

You can use the **Speed Test** to test the throughput between two IP-COM base stations or a base station and an outdoor CPE in the same network. The test requires that both sides support the **Speed Test** function.

Choose **Advanced** > **Diagnose**, and select **Speed Test** from the **Diagnose** drop-down list menu to enter the page.



Diagnose

Diagnose	Speed Test

AVG RX	AVG TX	AVG Total
0 Mbps	0 Mbps	0 Mbps

● Client ○ Server

IP Address of Peer AP	Manual	
IP Address		
HTTP Port	80	
User Name		
Password		
Test Group	10	(Range: 1 to 20)
Direction	Bidirectional	
Time	30	s (Range: 1 to 60)

Parameters description

Parameter	Description
Client	This two options are not available in this version.
Server	
IP Address of Peer AP	It specifies the LAN IP address of peer device. You can enter it manually or select an IP address from the drop-down list if there are devices connected to the base station.
IP Address	If the **IP Address of Peer AP** is set to **Manual**, you need to enter the LAN IP address of peer device in the input box manually.
HTTP Port	It specifies the HTTP service port number of peer device, which is used to establish speed test connection based on TCP/IP. Default: **80**. You are

Parameter	Description
	recommended to keep the default value.
User Name	It specifies the login user name and password of peer device.
Password	
Test Group	It specifies the number of test connection.
Direction	It specifies the test speed direction. – **RX** (Receive): only test the speed that the peer device transmits data to this device. – **TX** (Transmit): only test the speed that this device transmits data to peer device. – **Bidirectional**: test both transmit and receive speed between the two devices
Time	It specifies the duration of speed test.
AVG RX	It displays the average received rate.
AVG TX	It displays the average transmitted rate.
AVG Total	It displays the average total rate.

Example of configuring the speed test

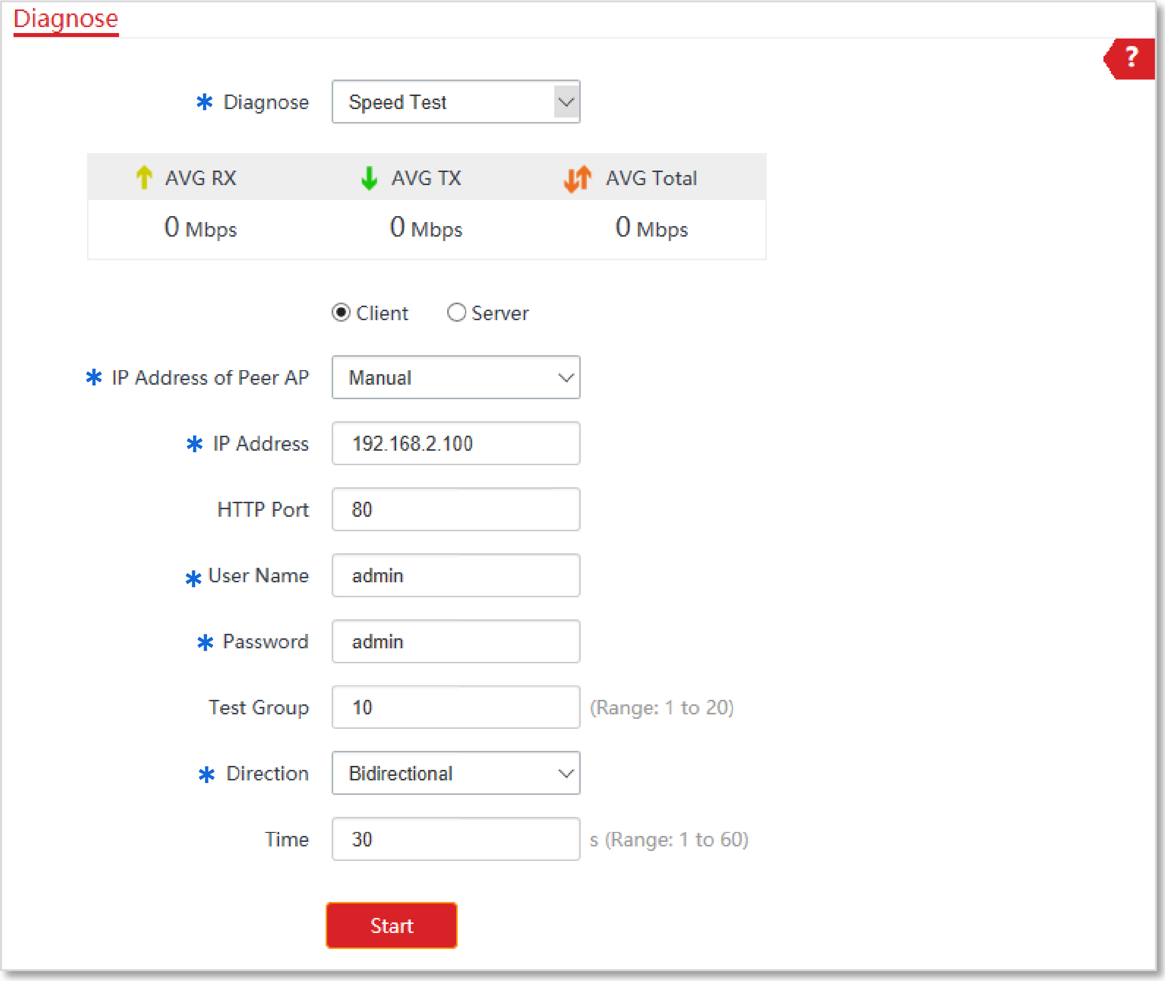
Assume that a base station working in **AP** mode and an outdoor CPE working in **Client** mode have bridged successfully. Then test the wireless speed between them.

The procedure can be performed both on the web UI of the base station and that of the CPE. The base station is used for illustration.

Assume that the IP address of peer CPE is **192.168.2.100**, and the login user name and password of peer CPE are both **admin**.

Configuration procedure

1. Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Diagnose**.
2. Set **Diagnose** to **Speed Test**.
3. Set **IP Address of Peer AP** to **Manual**.
4. Enter the IP address of peer CPE in the **IP Address** input box, which is **192.168.2.100** in this example.
5. Enter the login user name and password of the web UI of peer CPE in the **User name** and **Password** input boxes, which are both **admin** in this example.
6. Set **Direction** to **Bidirectional**.
7. Click **Start**.



Diagnose

✱ Diagnose	Speed Test

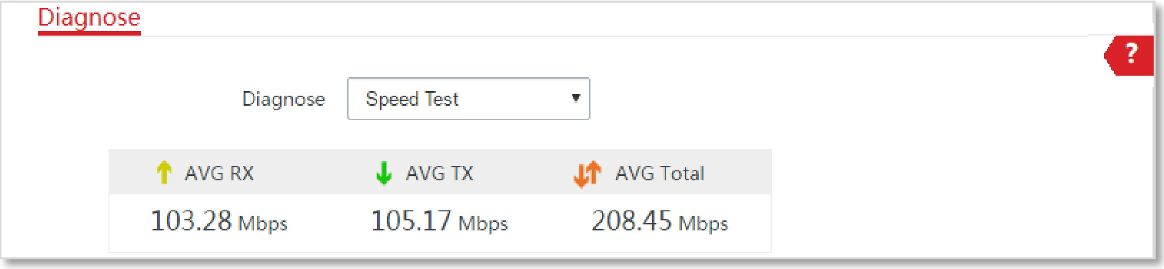
↑ AVG RX	↓ AVG TX	⇅ AVG Total
0 Mbps	0 Mbps	0 Mbps

● Client ○ Server

✱ IP Address of Peer AP	Manual
✱ IP Address	192.168.2.100
HTTP Port	80
✱ User Name	admin
✱ Password	admin
Test Group	10 (Range: 1 to 20)
✱ Direction	Bidirectional
Time	30 s (Range: 1 to 60)

---End

The test result will be displayed in a few seconds in the list below the **Diagnose** input box. See the following figure:



Diagnose

Diagnose	Speed Test

↑ AVG RX	↓ AVG TX	⇅ AVG Total
103.28 Mbps	105.17 Mbps	208.45 Mbps

8.2.6 Spectrum Analysis

You can use the **Spectrum Analysis** to check the wireless noise of each channel, then select a frequency band with less wireless noise for the base station according to the diagnose result.

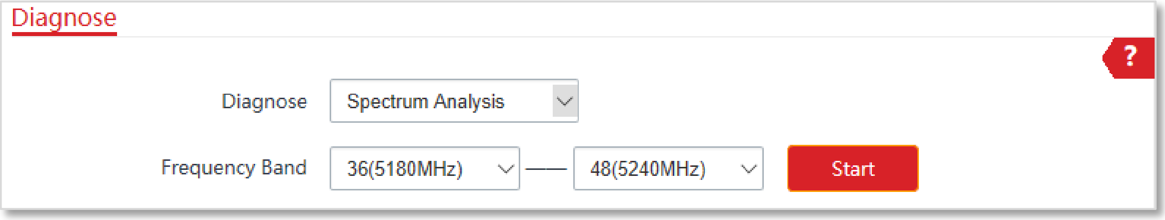
Configuration procedure

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Diagnose**.

2 Select **Spectrum Analysis** from the **Diagnose** drop-down list menu.

3 Select the frequency band range you want to test from the drop-down list.

4 Click **Start**.

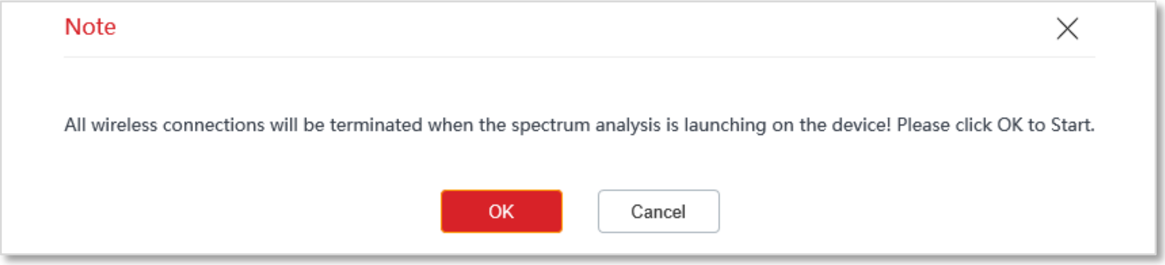


Diagnose

Diagnose: Spectrum Analysis

Frequency Band: 36(5180MHz) —— 48(5240MHz)

5 Confirm the message on the pop-up window, and click **OK**.

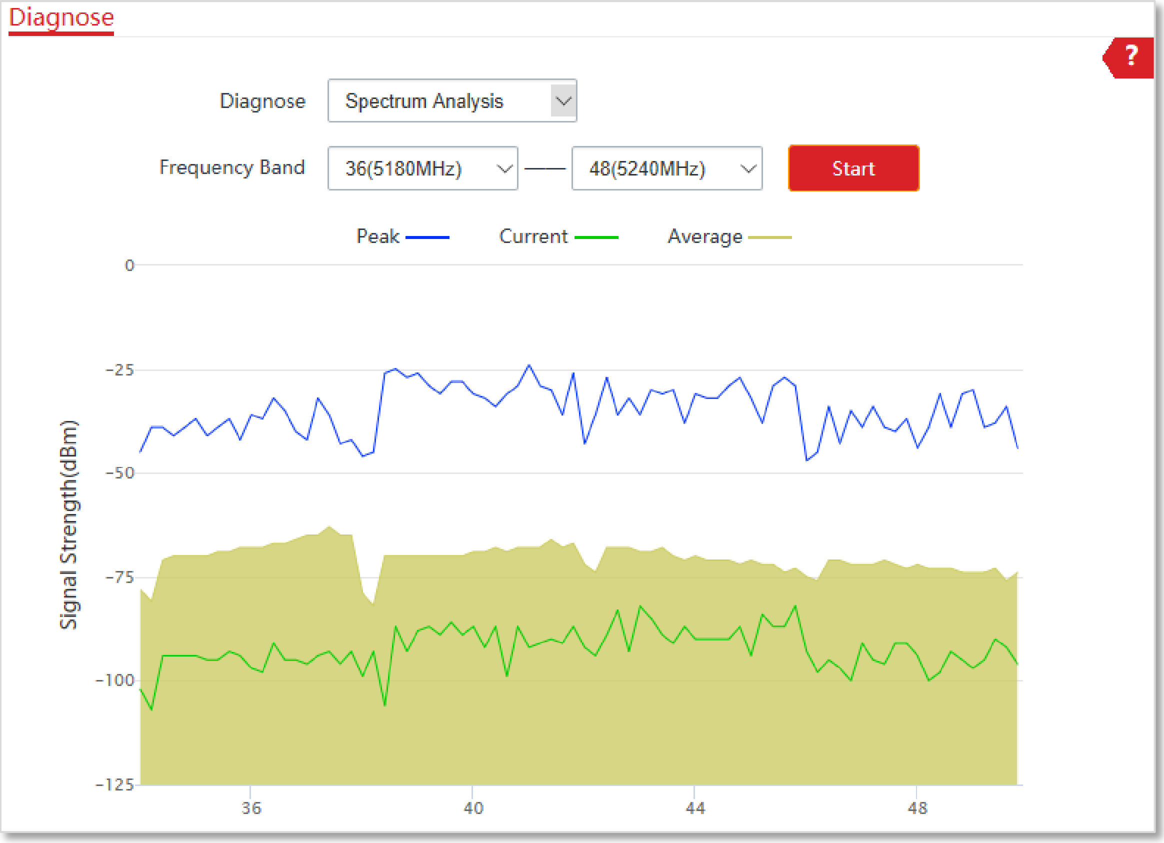


Note

All wireless connections will be terminated when the spectrum analysis is launching on the device! Please click OK to Start.

----End

The diagnosis result will be displayed in a few seconds. See the following figure.



Diagnose

Diagnose: Spectrum Analysis

Frequency Band: 36(5180MHz) —— 48(5240MHz)

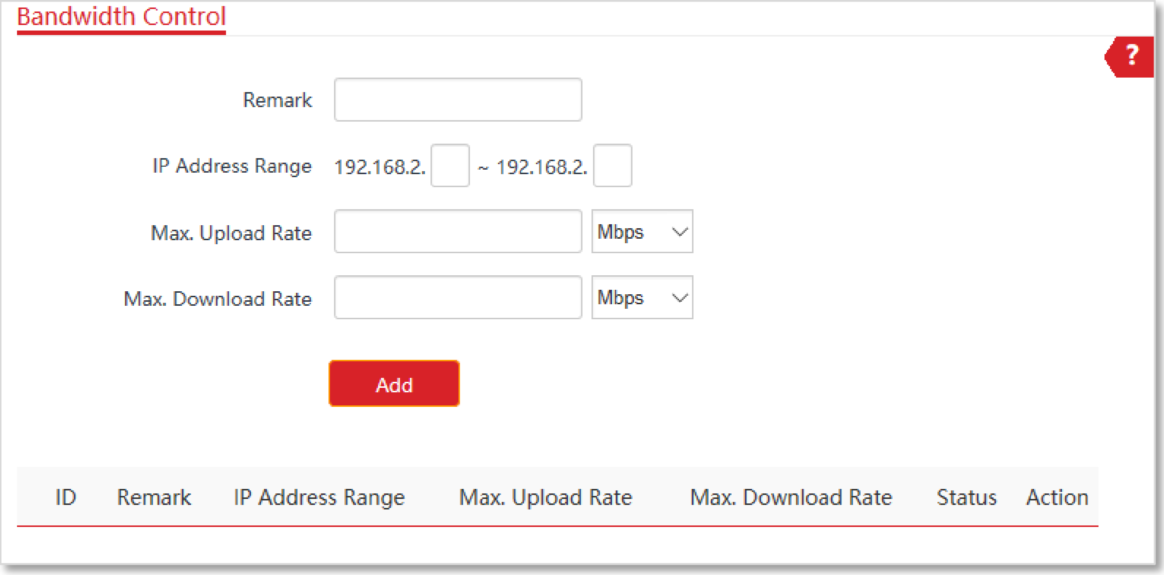
8.3 Bandwidth control

8.3.1 Overview

The **Bandwidth Control** function is only available in **WISP** or **Router** mode.

If multiple clients access the internet through the base station, bandwidth control is recommended, so that high-speed file download by a client does not reduce the internet access speed of the other clients.

To access the page, choose **Advanced** > **Bandwidth Control**.



Bandwidth Control

Remark

IP Address Range 192.168.2. ~ 192.168.2.

Max. Upload Rate Mbps

Max. Download Rate Mbps

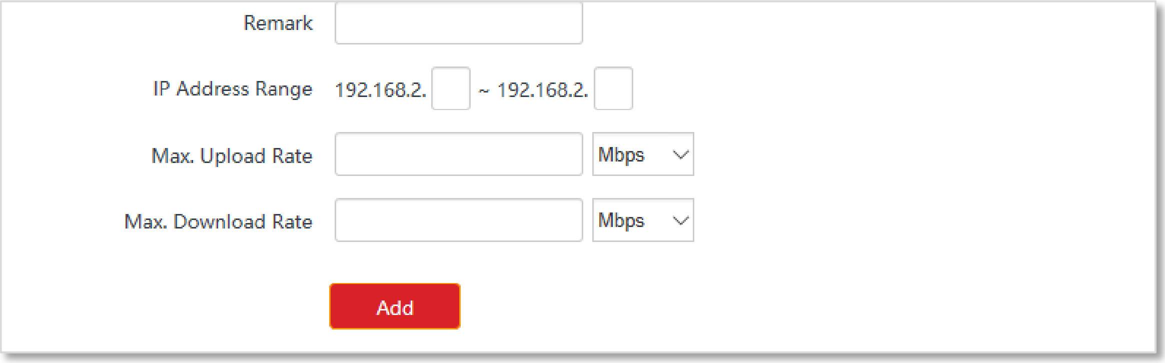
ID	Remark	IP Address Range	Max. Upload Rate	Max. Download Rate	Status	Action

8.3.2 Configure bandwidth control

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** >**Bandwidth Control**.

2 Set related parameters.

3 Click **Add**.



Remark

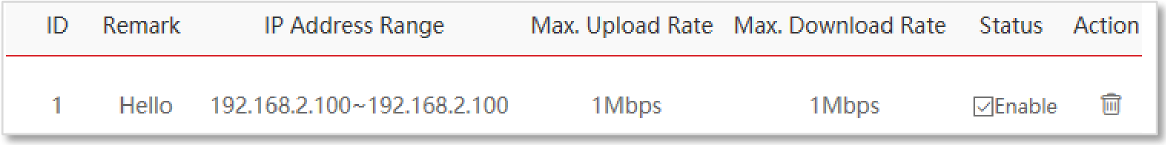
IP Address Range 192.168.2. ~ 192.168.2.

Max. Upload Rate Mbps

Max. Download Rate Mbps

---End

The added rule displays in the bandwidth control list. The parameters on the picture below are used for examples.



ID	Remark	IP Address Range	Max. Upload Rate	Max. Download Rate	Status	Action
1	Hello	192.168.2.100~192.168.2.100	1Mbps	1Mbps	☑Enable	🗑

Parameters description

Parameter	Description
Remark	Mandatory. It specifies the additional information of the bandwidth control rule. This field is required. For convenient management, you'd better specify different remarks for different rules.
IP Address Range	It specifies the IP address or IP address range of devices that this rule applies to. – **To control a single device**: Enter the same IP address in the two input boxes. – **To control multiple devices**: Enter an IP address range including start IP address and end IP address. The end IP address should be greater than the start IP address.
Max. Upload Rate	It specifies the maximum upload/download rate of clients controlled by the rule.
Max. Download Rate	
Status	It specifies the current status of the rule. You can enable or disable it as required.
Action	Click 🗑 to delete the rule.

8.4 Port forwarding

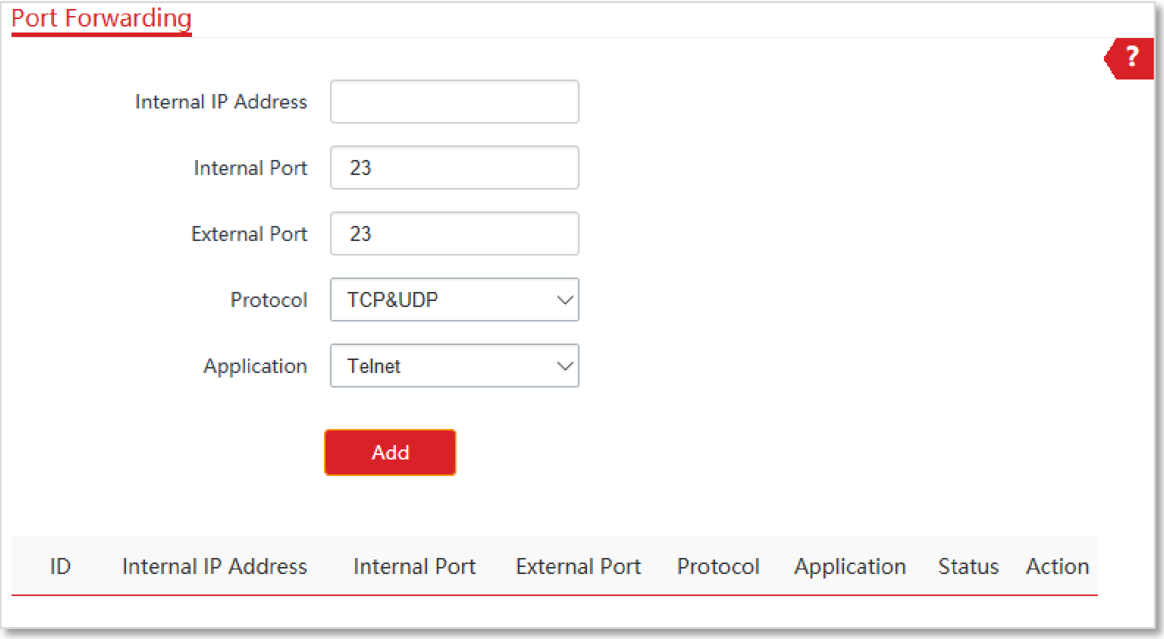
8.4.1 Overview

The **Port Forwarding** function is only available in **WISP** or **Router** mode.

If computers are connected to the base station to form a LAN and access the internet through the base station, internet users cannot access the hosts on the LAN. Therefore, the servers, such as web servers, email servers, and FTP servers, on the LAN are inaccessible to internet users.

To enable internet users to access a LAN server, enable the port forwarding function of the base station, and map one service port to the IP address of the LAN server. This enables the base station to forward the requests arriving at the port from the internet to the LAN server, and avoid the attacks from the WAN.

To access the page, choose **Advanced** > **Port Forwarding**.



Port Forwarding

Internal IP Address	
Internal Port	23
External Port	23
Protocol	TCP&UDP
Application	Telnet

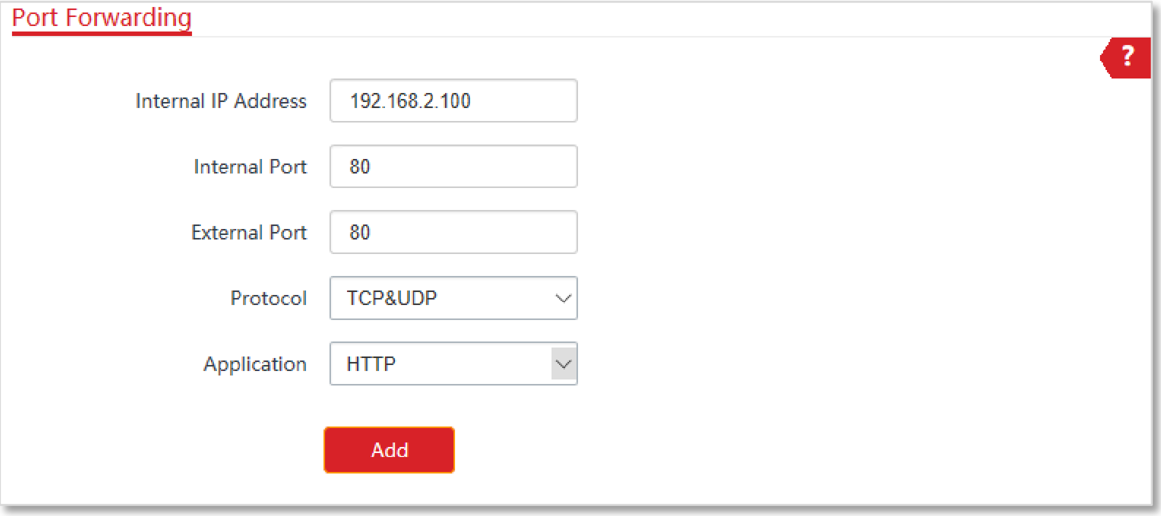
ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action

8.4.2 Configure port forwarding

1. Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Port Forwarding**.
2. Enter the IP address of a server established in LAN.
3. Enter the internal and external ports you enable for the service.

   If you are uncertain about them, select an **Application** and the internal and external ports will be populated automatically.
4. Select the protocol of the selected applications.

5 Click **Add**.



Port Forwarding

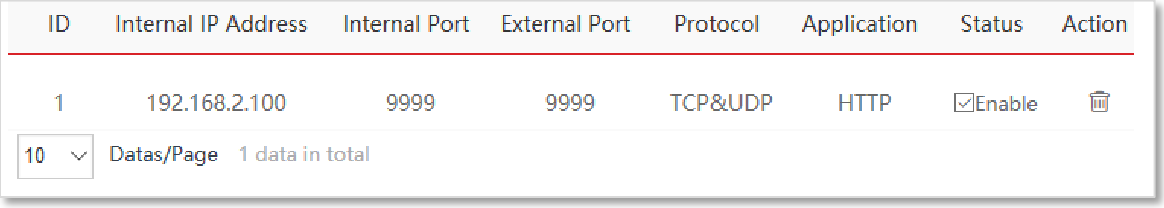
Internal IP Address	192.168.2.100
Internal Port	80
External Port	80
Protocol	TCP&UDP
Application	HTTP

---End

Tip

- If internet users still cannot visit servers in LAN after the configuration, try the following solutions:
- Ensure that the WAN IP address of the device is a public IP address, and the internal port you entered is correct.
- Security software, antivirus software, and the built-in OS firewall of the computer that establishes a server may cause port forwarding function failures. Disable them and try again.

The added rule displays in the port forwarding list. The parameters on the picture below are used for examples.



ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	9999	9999	TCP&UDP	HTTP	☑Enable	🗑

10 Datas/Page 1 data in total

After the port forwarding rule takes effect, to access the LAN server:

Enter **Protocol name**://**WAN port IP address**:**External port** in the address bar of a web browser on a computer over the internet.

Parameters description

Parameter	Description
Internal IP Address	It specifies the IP address of the host that establishes a server in LAN.
Internal Port	It specifies the service port of the server in LAN. After you select an **Application**, this option will be auto populated. You can also customize it.
External Port	It specifies the ports which are enabled for WAN users to visit the corresponding

Parameter	Description
	servers in LAN. After you select an **Application**, this option will be auto populated. You can also customize it.
Protocol	It specifies the protocol type of the selected applications. Select **TCP&UDP** when you are not sure.
Application	It specifies the application services established in LAN. The device provides some common services. If you are uncertain about the internal and external port number, you can select an application, the internal and external port number will be auto populated.
Action	Click 🗑 to delete the rule.

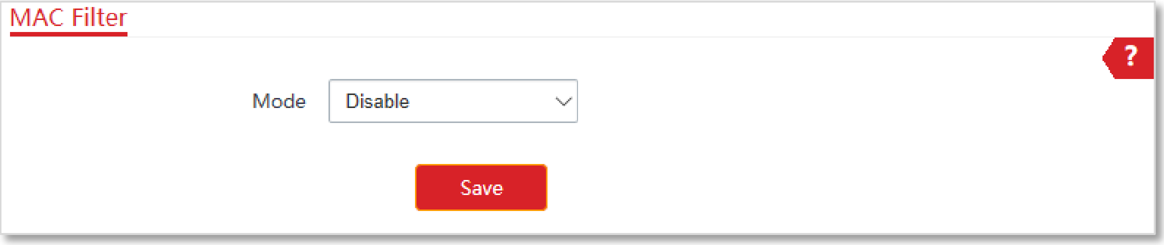
8.5 MAC filter

8.5.1 Overview

The **MAC Filter** function is only available in **WISP** or **Router** mode.

The MAC Filter function enables you to allow or disallow the devices, such as computers, laptops, tablets, and smart phones, to access the internet via the device at what time and on what days based on their MAC addresses.

To access the page, choose **Advanced** > **MAC Filter**. The function is disabled by default.


MAC Filter

Mode: Disable

8.5.2 Configure MAC filter

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **MAC Filter**.

2 Select a MAC filter mode, **Disallow** or **Allow**.

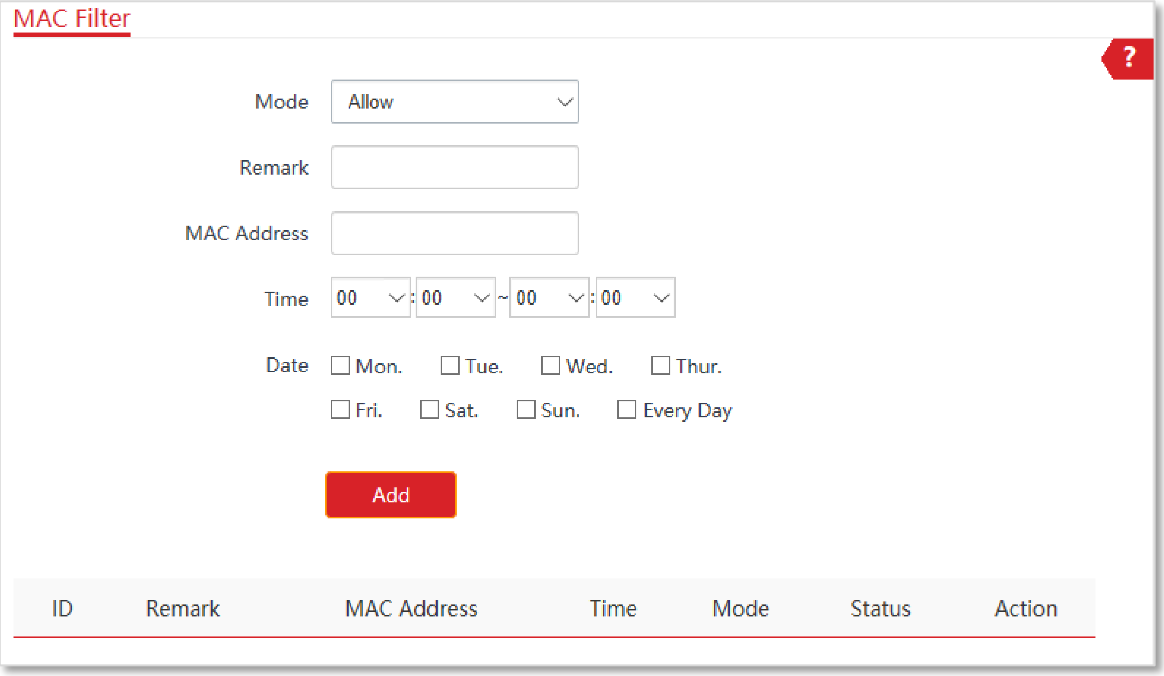
3 Optional. Enter a **Remark** for the rule, such as somebody's device.

4 Enter the **MAC Address** of the client to which this rule applies.

5 Specify a period at which the rule takes effect.

6 Tick the dates on which the rule takes effect.

7 Click **Add**.



MAC Filter

Mode: Allow

Remark:

MAC Address:

Time: 00 : 00 ~ 00 : 00

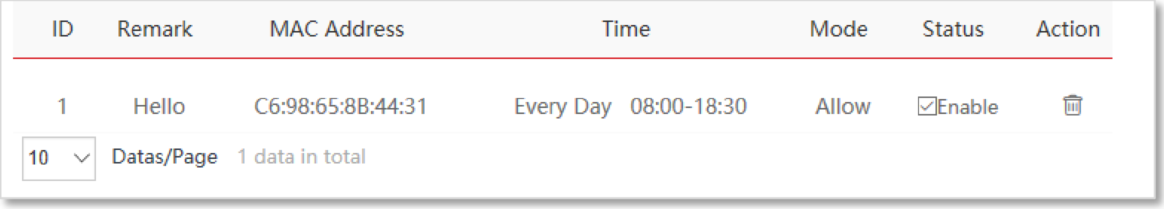
Date: □ Mon. □ Tue. □ Wed. □ Thur. □ Fri. □ Sat. □ Sun. □ Every Day

Add

ID	Remark	MAC Address	Time	Mode	Status	Action

---End

The added rule displays in the MAC filter list. The parameters on the picture below are used for examples.



ID	Remark	MAC Address	Time	Mode	Status	Action
1	Hello	C6:98:65:8B:44:31	Every Day 08:00-18:30	Allow	☑Enable	🗑

10 Datas/Page 1 data in total

Parameters description

Parameter	Description
Mode	It specifies the mode of MAC filter rule. – **Disable**: Disable the MAC Filter function. – **Allow**: Allow the devices with the MAC addresses in the list to access the internet via this device, and disallow the other devices to access the internet via this device. – **Disallow**: Disallow the devices with the MAC addresses in the list to access the internet via this device, and allow the other devices to access the internet via this device.
Remark	It specifies the additional information of the rule.
MAC Address	It specifies the MAC address of the device to which the rule applies.
Time	It specifies the period at which the rule takes effect.
Date	It specifies the period on which the rule takes effect.
Status	It specifies the status of the rule. You can tick or untick the **Enable** option to enable or disable the rule.
Action	Click 🗑 to delete the rule.

8.6 Network service

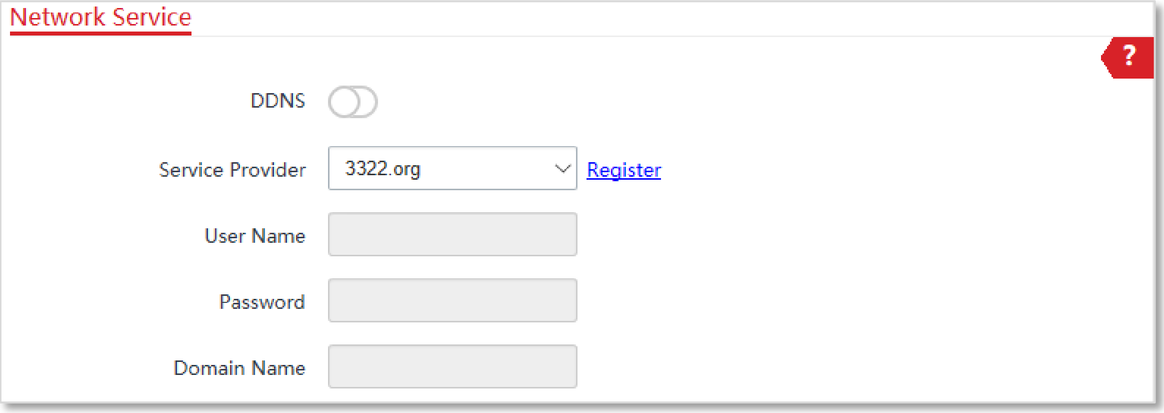
8.6.1 DDNS

The **DDNS** function is only available in **WISP** or **Router** mode.

DDNS, dynamic domain name server, enables the dynamic DNS client on the device to deliver the current WAN IP address to the DNS server. Then the server maps the WAN IP address to a domain name for dynamic domain name resolution.

This function often works with the port forwarding, DMZ host, and remote web management functions. Then users can visit an address with a domain name instead of a dynamic WAN IP address, which makes the visit easier.

To access the page, choose **Advanced** > **Network Service**.



Network Service

DDNS ○

Service Provider: 3322.org

Configuration procedure

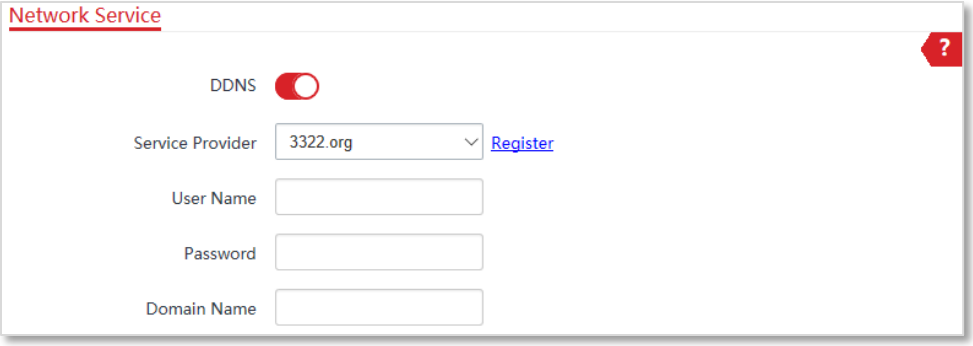
1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Network Service**.

2 Enable the **DDNS** function.

3 Select a DDNS **Service Provider** from the drop-down list menu.

4 Enter the **User Name**, **Password**, and **Domain Name** you registered with DDNS service provider.

5 Click **Save** on the bottom of this page.



Network Service

DDNS ●

Service Provider: 3322.org

---End

Parameters description

Parameter	Description
DDNS	It specifies whether to enable the DDNS function.
Service Provider	It specifies Dynamic Domain Name Service provider. The device supports Dyndns, No-ip.com, and 3322.org.
User Name	It specifies the user name used to log in to the dynamic DNS service, as well as the login user name and password you registered on the website of the service provider.
Password	
Domain Name	It specifies the domain name information obtained from the dynamic DNS server.

8.6.2 Remote web management

The **Remote Web Management** function is only available in **WISP** or **Router** mode.
Generally, only the clients connected to the base station can access its web UI.
The remote web management function enables you to access the web UI of the base station on WAN if it is required.

Configuration procedure

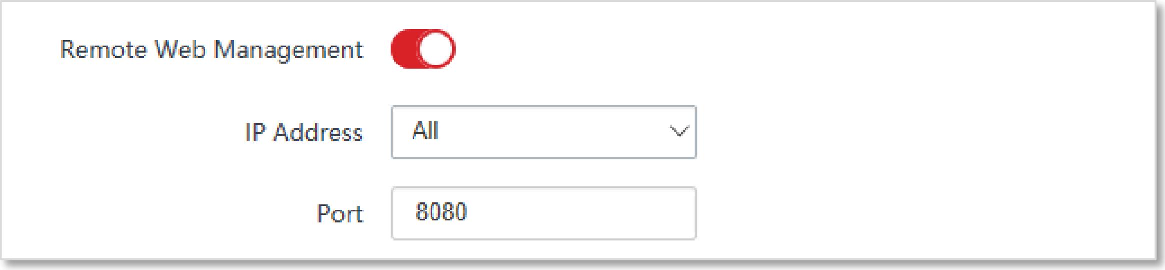
1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Network Service**.

2 Set the **Remote Web Management** to ●.

3 Select **Manual** from the **IP Address** drop-down list, enter the IP address of a device which is allowed to access the web UI of the device remotely, or select **All** to allow any device on WAN to access.

4 Optional. Enter a port number.

5 Click **Save** on the bottom of this page.



Remote Web Management ●

IP Address All

Port 8080

---End

Parameters description

Parameter	Description
Remote Web Management	It specifies whether to enable the remote web management function.
IP Address	It specifies the IP address of a device which is allowed to access the web UI of the device. – **All**: It indicates that any computer in WAN can manage this device remotely. For security, this option is not recommended. – **Manual**: It indicates that only the device with specified IP address can manage this device remotely. If this device belongs to a LAN, the gateway address (a public IP address) of the device should be entered.
Port	It specifies the port number used for remote management of device. Default: **8080**. You can change it if necessary. Ports 1 to 1024 have been used by well-known services. To avoid port conflicts, you can set the port number to one between 1025 and 65535. Then you can access the device from WAN by visiting an address in the form of **http://WAN IP address:port number**. If the DDNS function is enabled on the device, you can access the device by visiting an address in the form of **http://Domain name of WAN port:port number**.

8.6.3 Reboot schedule

This function enables the device to automatically reboot as scheduled. You can use this function to prevent wireless performance degradation or network instability that occurs after a long device uptime.

Configuration procedure

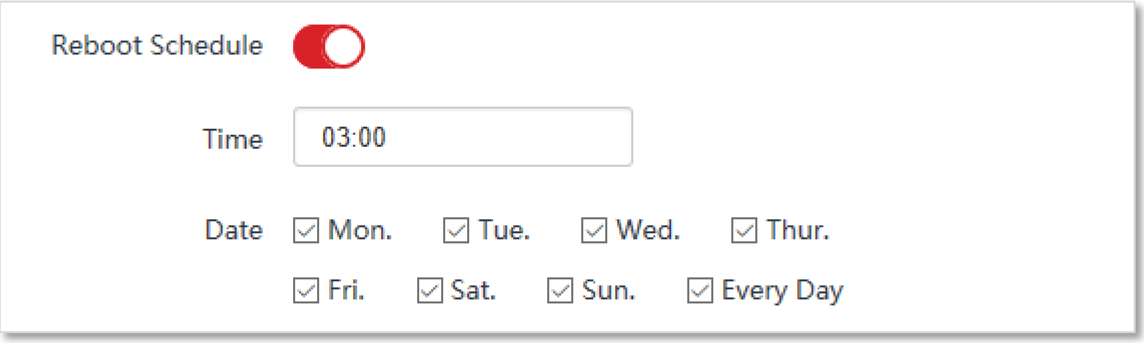
1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Network Service**.

2 Set the **Reboot Schedule** to ●.

3 Specify a time at which the device reboots.

4 Specify the dates on which the device reboots.

5 Click **Save** on the bottom of this page.



Reboot Schedule ●

Time 03:00

Date ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thur.
☑ Fri. ☑ Sat. ☑ Sun. ☑ Every Day

---End

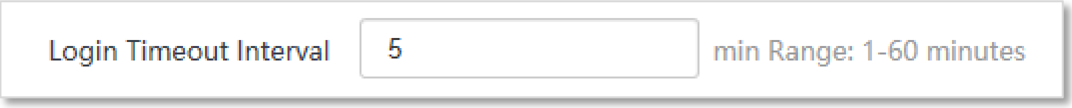
The device reboots every day at 3:00.

8.6.4 Login timeout interval

If you log in to the web UI of the device and perform no operation within the login timeout interval, the device logs you out for network security. The default login timeout interval is 5 minutes.

To access the page, start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Network Service**.

You can change the login timeout interval as required.



Login Timeout Interval 5 min Range: 1-60 minutes

8.6.5 SNMP agent

Overview

The Simple Network Management Protocol (SNMP) is the most widely used network management protocol in TCP/IP networks. SNMP enables you to remotely manage all your network devices compliant with this protocol, such as monitoring the network status, changing network device settings, and receive network event alarms.

SNMP allows automatic management of devices from various vendors regardless of physical differences among the devices.

SNMP Management Framework

The SNMP management framework consists of SNMP manager, SNMP agent, and Management Information Base (MIB).

- SNMP manager: It is a system that controls and monitors network nodes using the SNMP protocol. The SNMP manager most widely used in network environments is Network Management System (NMS). An NMS can be a dedicated network management server, or an application that implements management functions in a network device.

- SNMP agent: It is a software module in a managed device. The module is used to manage data about the device and report the management data to an SNMP manager.

- MIB: It is a collection of managed objects. It defines a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its MIB. An SNMP manager can read and/or write objects in the MIB based on the permissions assigned to the SNMP manager.

An SNMP manager manages SNMP agents in an SNMP network. The SNMP manager exchanges management information with the SNMP agents using the SNMP protocol.

Basic SNMP Operations

The device allows the following basic SNMP operations:

- Get: An SNMP manager performs this operation to query the SNMP agent of the device for values of one or more objects.

- Set: An SNMP manager performs this operation to set values of one or more objects in the MIB of the SNMP agent of the device.

SNMP Protocol Version

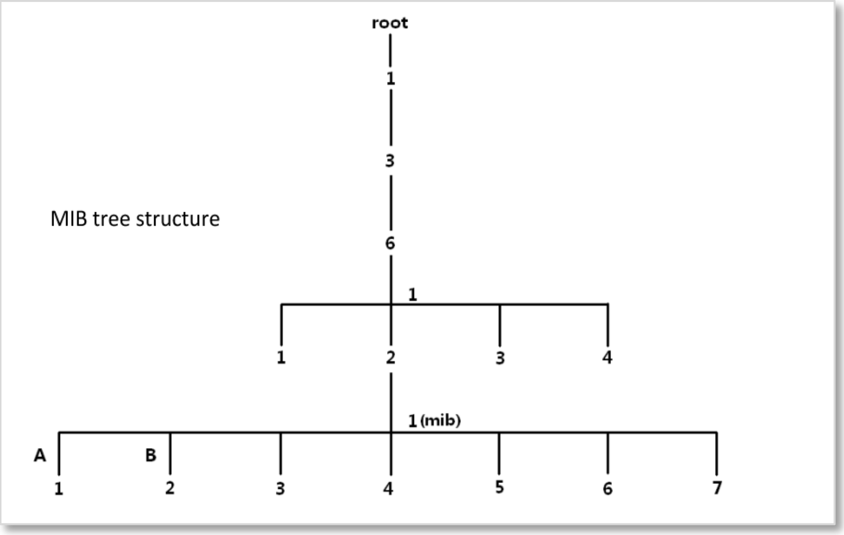
The device is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. Community name is used to define the relationship between an SNMP agent and an SNMP manager.

If the community name contained in an SNMP packet is rejected by a device, the packet is discarded. A community name functions as a password to control SNMP agent access attempts of SNMP managers.

SNMP V2C is compatible with SNMP V1 and provides more functions than SNMP V1. Compared with SNMP V1, SNMP V2C supports more operations (GetBulk and InformRequest) and data types (such as Counter64), and provides more error codes for better distinguishing errors.

MIB Introduction

An MIB adopts a tree structure. The nodes of the tree indicate managed objects. A path consisting of digits and starting from the root can be used to uniquely identify a node. This path is calling an object identifier (OID).The following figure shows the structure of an MIB. In the figure, the OID of A is 1.3.6.1.2.1.1, whereas the OID of B is 1.3.6.1.2.1.2.



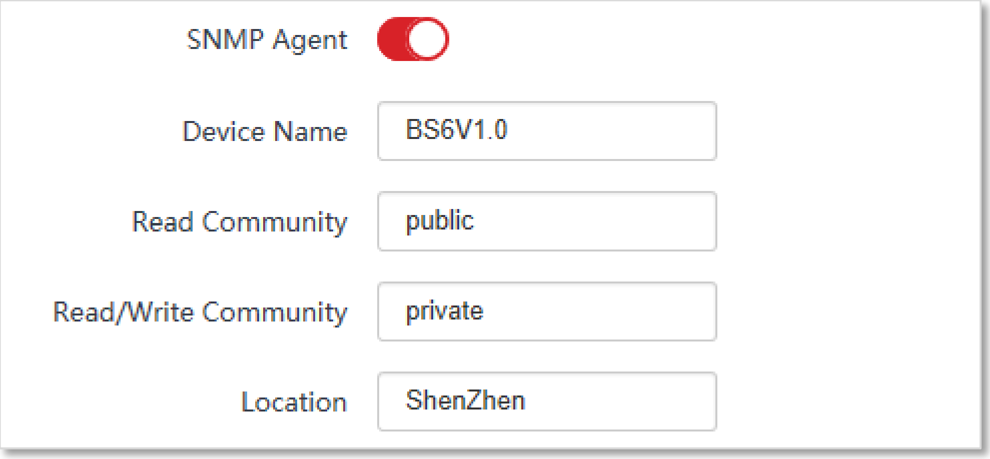
Configuring the SNMP agent function

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Network Service**.

2 Set the **SNMP Agent** to ●.

3 Set the related SNMP parameters.

4 Click **Save** on the bottom of this page.



SNMP Agent ●

Device Name: BS6V1.0

Read Community: public

Read/Write Community: private

Location: ShenZhen

---End

Parameters description

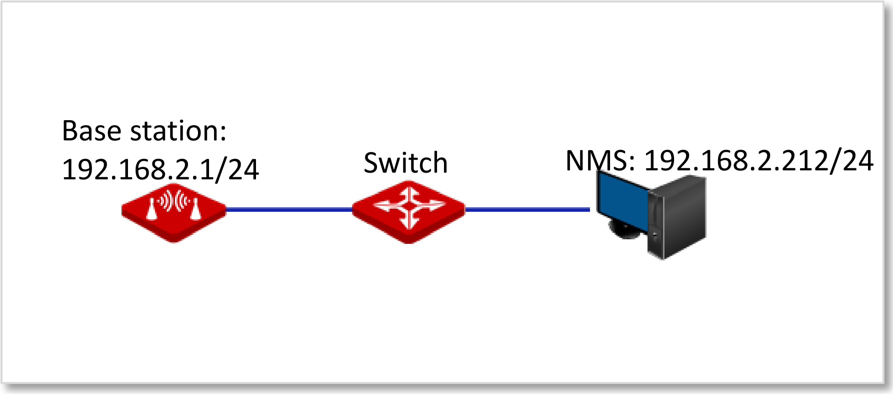
Parameter	**Description**
SNMP Agent	It specifies whether to enable the SNMP agent function of the base station. By default, it is disabled. An SNMP manager and the SNMP agent can communicate with each other only if their SNMP versions are the same. Currently, the SNMP agent function of the device supports SNMP V1 and SNMP V2C.
Device Name	It specifies the device name of the device. The default device name is the model and version number of the device. For example, the default name of this device is BS6V1.0 Tip It is recommended that you change the device name so that you can easily identify the device when managing it using SNMP.
Read Community	It specifies the read password shared between SNMP managers and this SNMP agent. The default password is public. The SNMP agent function of the device allows an SNMP manager to use the password to read variables in the MIB of the device.
Read/Write Community	It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is private. The SNMP agent function of the device allows an SNMP manager to use the password to read/write variables in the MIB of the device.
Location	It specifies the location where the device is used. You can change the location as required.

Example of configuring the SNMP function

Networking requirement

- The device connects to an NMS over an LAN. This network address of the device is 192.168.2.1/24 and the network IP address of the NMS is 192.168.2.212/24.
- The NMS use SNMP V1 or SNMP V2C to monitor and manage the device.

Assume that Read Community is Jack, and Read/Write Community is Jack123.



Configuration procedure

1 Set up the base station.

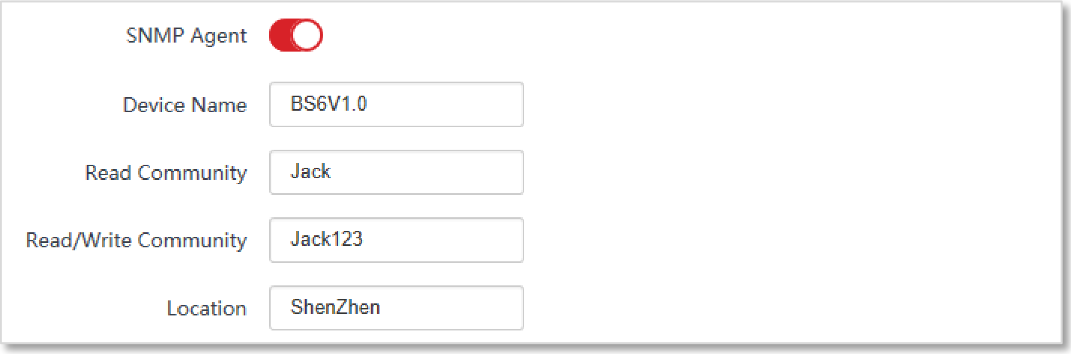
(1) Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Network Service**.

(2) Enable the **SNMP Agent** function.

(3) Set the **Read Community**, which is **Jack** in this example.

(4) Set **Read/Write Community**, which is **Jack123** in this example.

(5) Click **Save** on the bottom of this page.



SNMP Agent	●
Device Name	BS6V1.0
Read Community	Jack
Read/Write Community	Jack123
Location	ShenZhen

2 Set up the NMS.

On an NMS that uses SNMP V1 or SNMP V2C, set the read community to **Jack** and read/write community to **Jack123**. For details about how to configure the NMS, refer to the configuration guide for the NMS.

---End

Verification

After the configuration, the NMS can connect to the SNMP agent of the device and can query and set some parameters on the SNMP agent through the MIB.

8.6.6 Ping watch dog

With this function enabled, the device periodically pings target IP address to check the network connectivity and identify whether the device malfunctions. If it malfunctions, the device will reboot automatically to ensure the network performance.

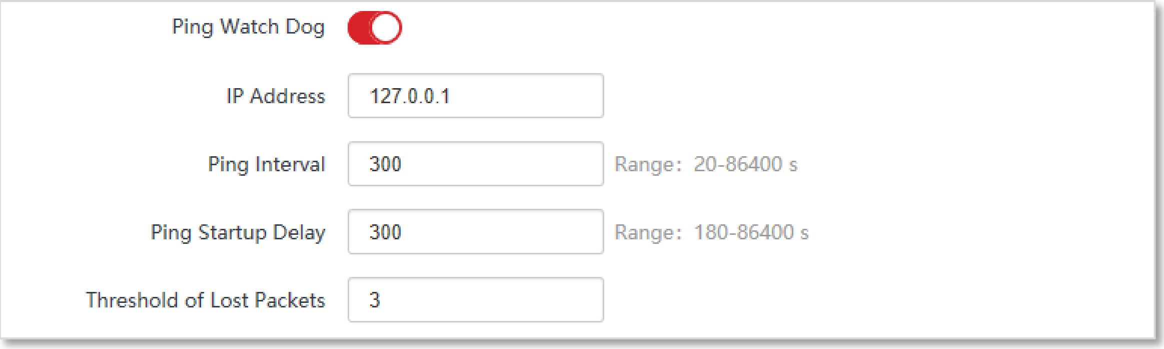
Configuration procedure

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Network Service**.

2 Set the **Ping Watch Dog** to ●.

3 Set the related parameters.

4 Click **Save** on the bottom of this page.



Ping Watch Dog ●

IP Address 127.0.0.1

Ping Interval 300 Range: 20-86400 s

Ping Startup Delay 300 Range: 180-86400 s

Threshold of Lost Packets 3

---End

Parameters description

Parameter	Description
Ping Watch Dog	It specifies whether to enable the **Ping Watch Dog** function.
IP Address	It specifies the target IP address that the device pings.
Ping Interval	It specifies the interval at which the device transmits packets to ping the target IP address.
Ping Startup Delay	It specifies the delay time for the device to enable the **Ping Watch Dog** function after the device completes startup. Setting a proper Ping Startup Delay time can stop the **Ping Watch Dog** function from being triggered during the startup of the base station. Such triggering leads to failure of accessing the web UI to modify the settings, causing the base station to start up continuously.
Threshold of Lost Packets	It specifies the threshold of lost packet that triggers reboot. Range: 1 to 65535, default: 3. For example, if 5 is set, the device will reboot automatically when it does not

Parameter	Description
	receive response after sending 5 Ping packets to target IP address/domain name.

8.6.7 DMZ host

The **DMZ** function is only available in **WISP** or **Router** mode.

A DMZ host on a LAN can communicate with the internet without limit. You can set a computer that require higher internet connection throughput, such as a computer used for video conferencing or online gaming, as a DMZ host for better user experience.

Note

- A computer set to DMZ host is not protected by the firewall of the device.
- A hacker may leverage the DMZ host to attack your LAN. Therefore, enable the DMZ function only when necessary.

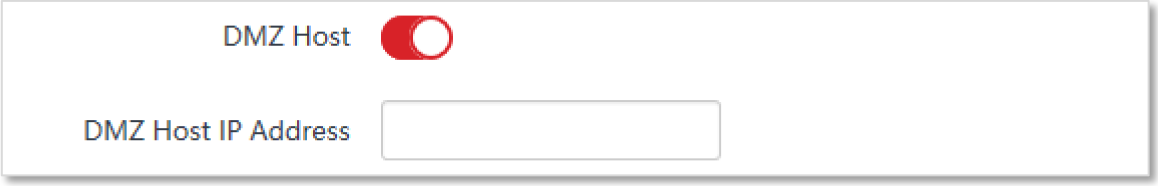
Configuration procedure

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Advanced** > **Network Service**.

2 Set the **DMZ Host** to ●.

3 Enter the IP address of the device to be set to DMZ host.

4 Click **Save** on the bottom of this page.



DMZ Host ●

DMZ Host IP Address

---End

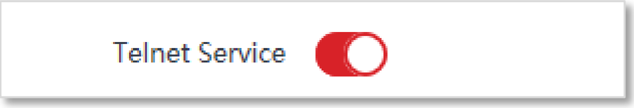
Tip

Security software, antivirus software, and the built-in OS firewall of the host may cause the function failures. Disable them and try again if the function fails.

8.6.8 Telnet service

With this function enabled, the device can be managed via Telnet. Generally this function is used to maintain the device by technical professional.

To access the page, choose **Advanced** > **Network Service**. By default, the function is enabled.



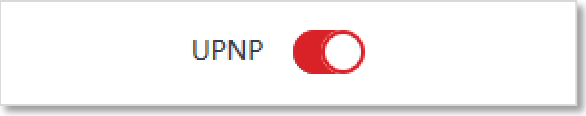
Telnet Service

8.6.9 UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that makes automatic port forwarding possible. It can identify devices and enable ports for certain applications, such as Thunder. To use this function, it requires that the operating system support UPnP, or application software supporting UPnP is installed.

To access the page, choose **Advanced** > **Network Service**. By default, the function is disabled.

You can enable it as required.

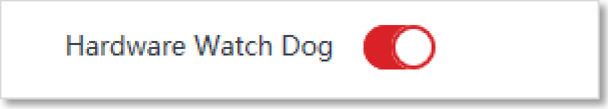


UPNP

8.6.10 Hardware watch dog

This function uses an embedded watchdog timer to detect the operation condition of the device’s main program regularly. During normal operation, the device regularly resets the watchdog timer to prevent it from elapsing, or "timing out". If the device fails to reset the watchdog timer, due to a hardware fault or program error, the timer will elapse and generate a timeout signal. The timeout signal is used to reboot the device to make it recover from malfunctions.

To access the page, choose **Advanced** > **Network Service**. By default, the function is enabled.

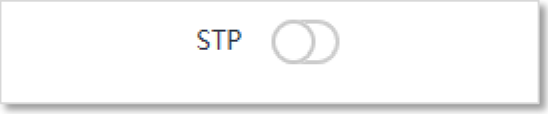


Hardware Watch Dog

8.6.11 STP

Spanning Tree Protocol (STP) is a network protocol standardized by IEEE 802.1D. It helps establish a loop-free logical topology for Ethernet network, and allows a network design to include backup links to provide fault tolerance if an active link fails. The STP-enabled device creates a spanning tree within a network of connected layer-2 bridges, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. So that it prevents packets from continued proliferation and endless loop in a loop network to avoid reducing the capability of processing packets caused by receiving duplicate packets.

To access the page, choose **Advanced** > **Network Service**. By default, the function is disabled.



STP ○

9 Tools

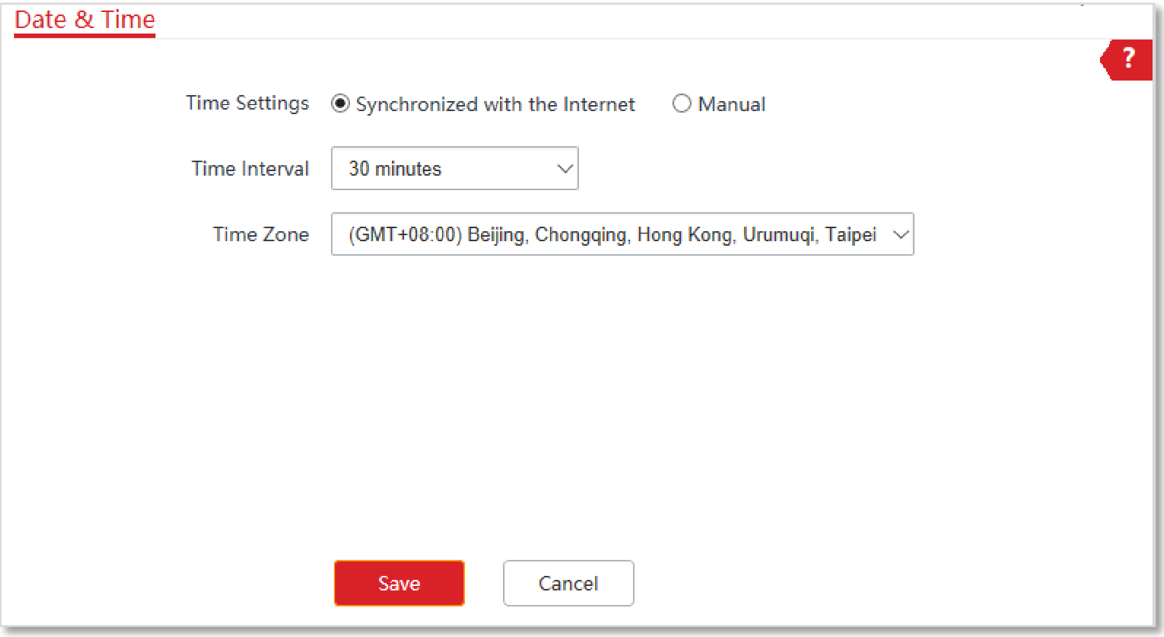
9.1 Date & time

This module enables you to set the system time of the device.

Ensure that the system time of the device is correct, so that time-based functions can be executed correctly.

The device allows you to set the system time by synchronizing the time with the internet or manually setting the time. By default, it is configured to synchronize the system time with the internet.

To access the page, choose **Tools** > **Date & Time**.



Date & Time

Time Settings ● Synchronized with the Internet ○ Manual

Time Interval: 30 minutes

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei

9.1.1 Synchronize the system time with the Internet automatically

The device automatically synchronizes its system time with a time server of the internet. This enables the device to automatically correct its system time after being connected to the internet.

For details about how to connect the base station to the internet, refer to the configuration procedure of corresponding mode in Quick Setup.

Configuration procedure

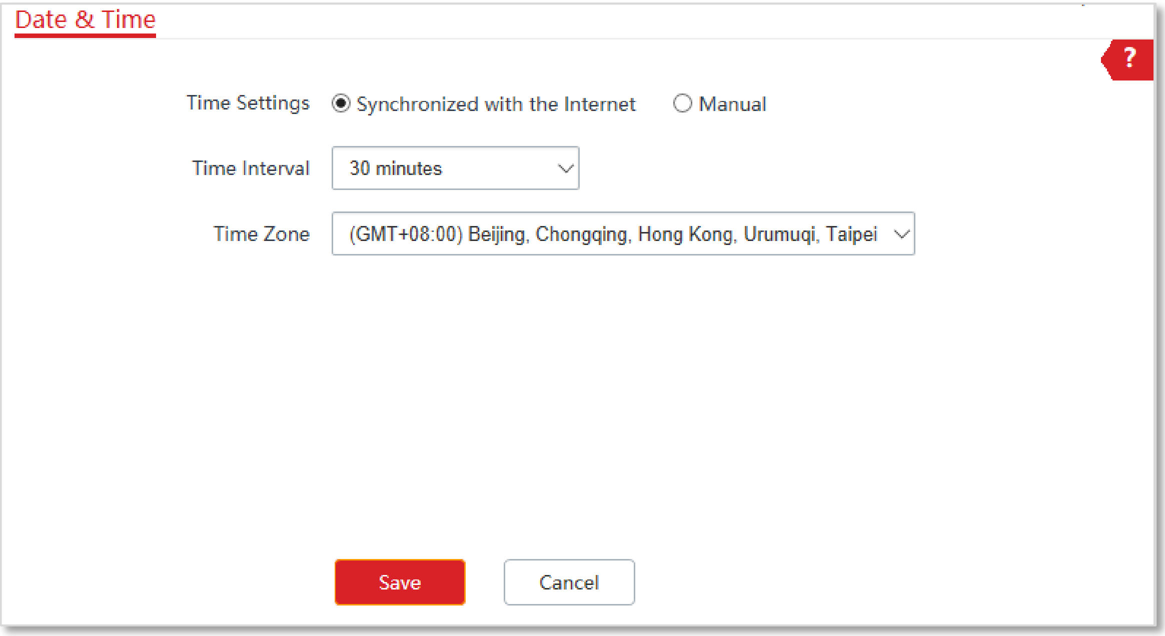
1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Tools** > **Date & Time**.

2 Set **Time Settings** to **Synchronized with the Internet**.

3 Specify a **Time Interval**. The default value **30 minutes** is recommended.

4 Set **Time Zone** to your time zone.

5 Click **Save**.



Date & Time

Time Settings ● Synchronized with the Internet ○ Manual

Time Interval 30 minutes

Time Zone (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei

---End

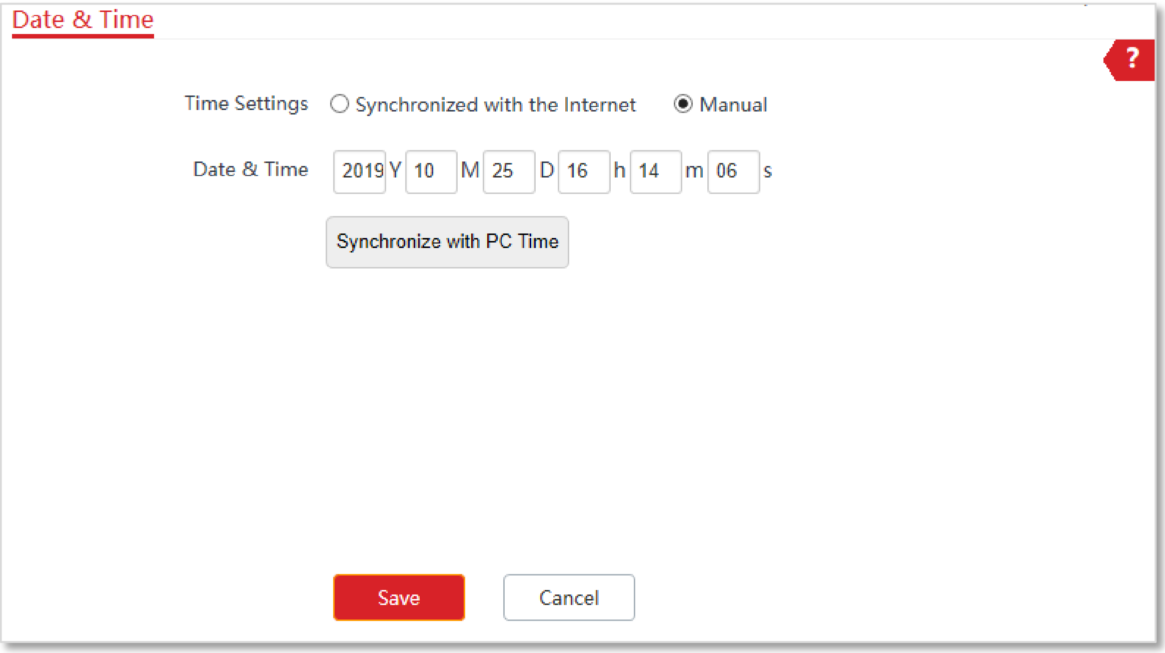
9.1.2 Set the system time manually

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Tools** > **Date & Time**.

2 Set the **Time Settings** to **Manual**.

3 Enter a correct date and time, or click **Synchronize with PC Time** to synchronize the system time of the device with the system time of the management computer.

4 Click **Save**.



Date & Time

Time Settings ○ Synchronized with the Internet ● Manual

Date & Time 2019 Y 10 M 25 D 16 h 14 m 06 s

---End

9.2 Maintenance

9.2.1 Reboot device

If a setting does not take effect or the device works improperly, you can try rebooting the device to resolve the problem.

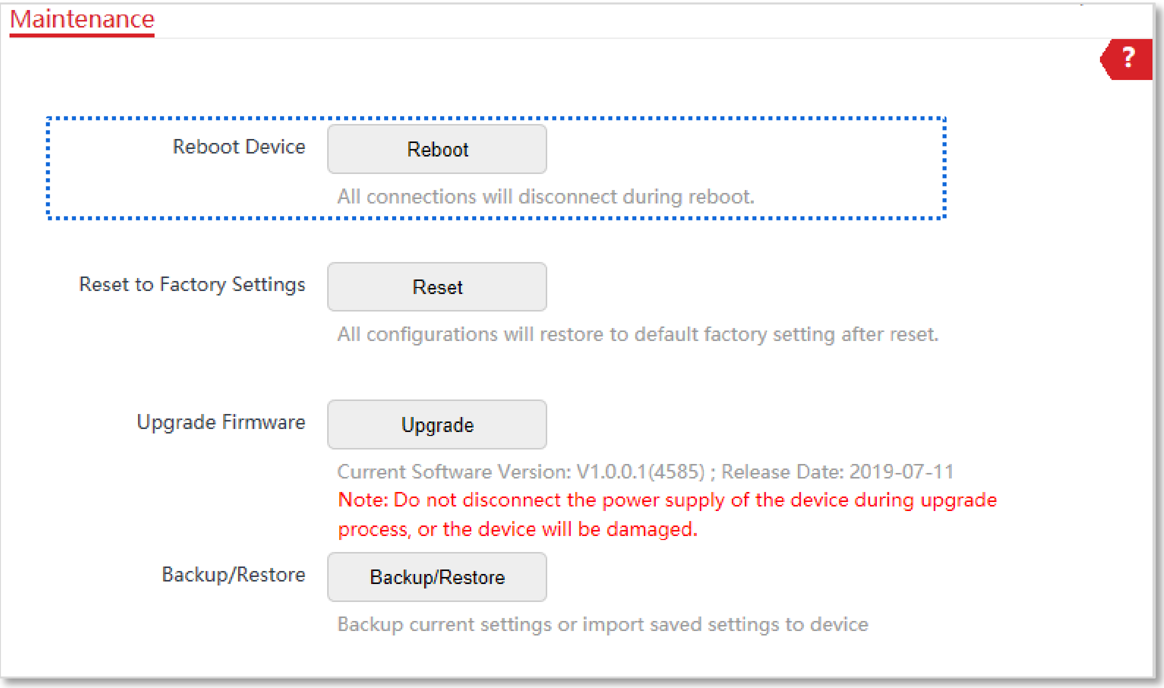
Tip

When the device reboots, the current connections will be disconnected. Perform this operation when the device is NOT busily.

Configuration procedure

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Tools** > **Maintenance**.

2 Click **Reboot**.



Maintenance

Reboot Device: Reboot

All connections will disconnect during reboot.

Reset to Factory Settings: Reset

All configurations will restore to default factory setting after reset.

Upgrade Firmware: Upgrade

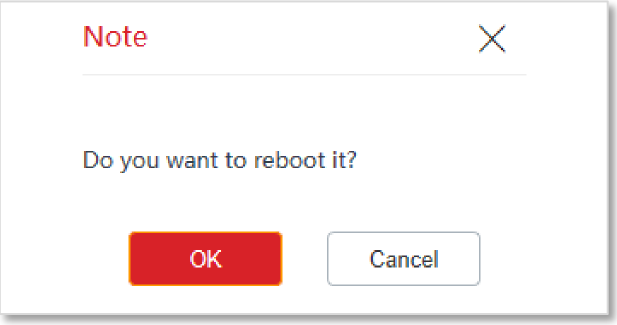
Current Software Version: V1.0.0.1(4585) ; Release Date: 2019-07-11

Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.

Backup/Restore: Backup/Restore

Backup current settings or import saved settings to device

3 Click **OK** on the pop-up window.



Note

Do you want to reboot it?

OK Cancel

---End

A progress bar is displayed on the page. Wait for it to elapse.

9.2.2 Reset to factory settings

If you cannot locate a fault of the device or forget the login password of the web UI, you can reset the device to restore its factory settings and then configure it again.

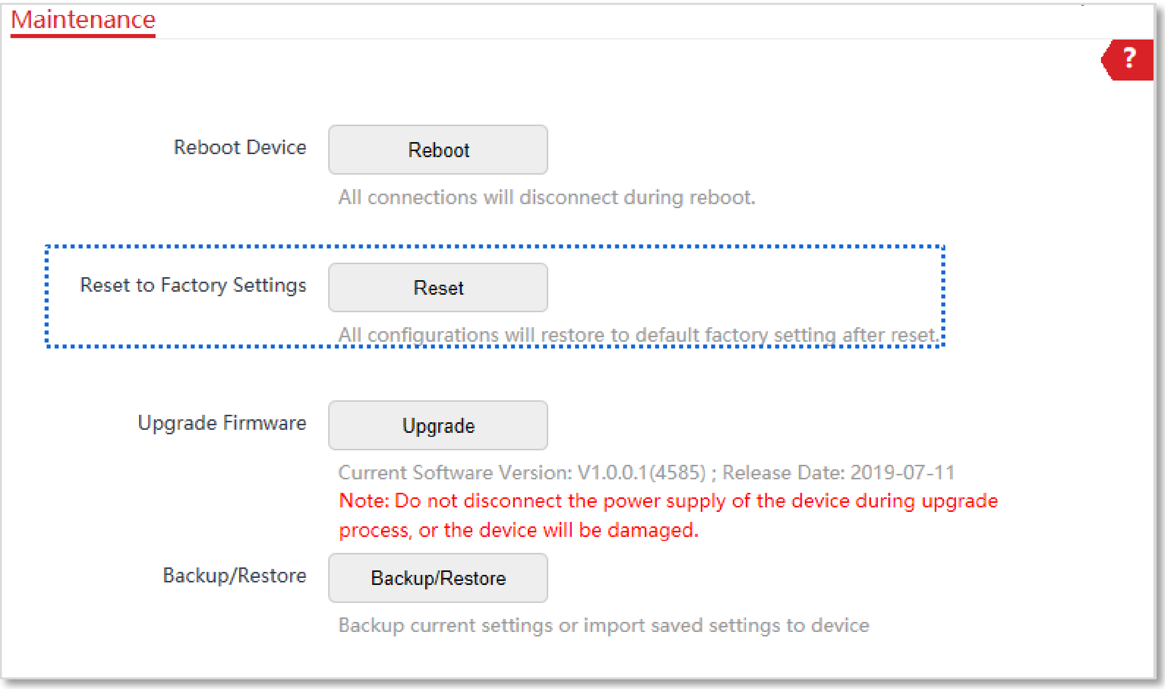
Note

- When the factory settings are restored, the configuration of the device is cleared.
- To prevent device damages, do not power off the device during resetting.
- When the factory settings are restored, the login IP address is 192.168.2.1, and both login user name and password are admin.

Option 1: Reset the base station using the web UI

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Tools** > **Maintenance**.

2 Click **Reset**.



Maintenance

Reboot Device: Reboot

All connections will disconnect during reboot.

Reset to Factory Settings: Reset

All configurations will restore to default factory setting after reset.

Upgrade Firmware: Upgrade

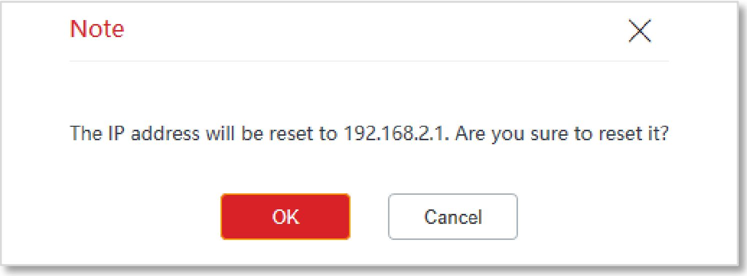
Current Software Version: V1.0.0.1(4585) ; Release Date: 2019-07-11

Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.

Backup/Restore: Backup/Restore

Backup current settings or import saved settings to device

3 Click **OK** on the pop-up window.



Note

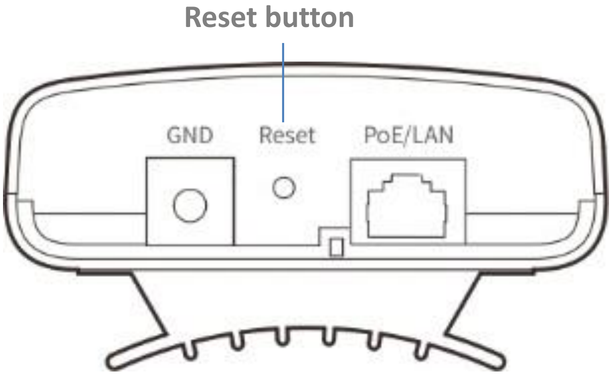
The IP address will be reset to 192.168.2.1. Are you sure to reset it?

---End

A progress bar is displayed on the page. Wait for it to elapse.

Option 2: Reset the base station using the Reset button

When the **Power** LED indicator lights solid on, hold down the **Reset** button for about 8 seconds, then release it. When all the LED indicators light up and then turn off, the base station is restored to factory settings.



9.2.3 Upgrade firmware

This function upgrades the firmware of the device for more functions and higher stability.

Note

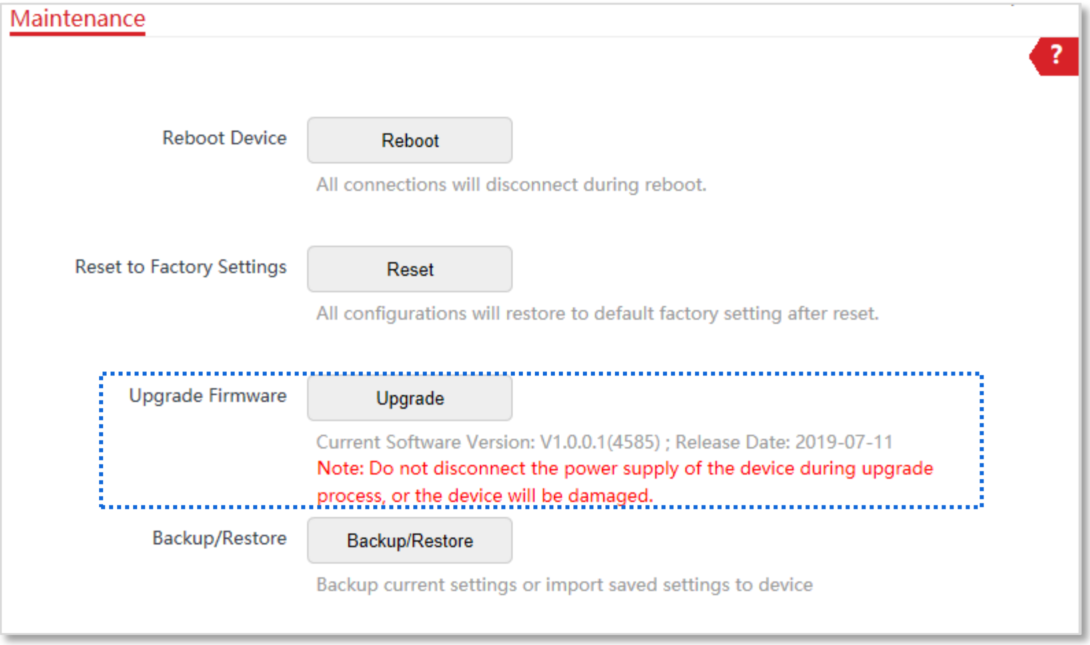
To prevent damaging the device, verify that the new firmware version is applicable to the device before upgrading the firmware and keep the power supply of the device connected during an upgrade.

Configuration procedure

1 Download the file of the latest firmware version for the device from www.ip-com.com.cn to your local computer, and unzip it.

2 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Tools** > **Maintenance**.

3 Click **Upgrade**.



Reboot Device Reboot

All connections will disconnect during reboot.

Reset to Factory Settings Reset

All configurations will restore to default factory setting after reset.

Upgrade Firmware Upgrade

Current Software Version: V1.0.0.1(4585) ; Release Date: 2019-07-11

Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.

Backup/Restore Backup/Restore

Backup current settings or import saved settings to device

4 Select the correct upgrade file from your local computer.

---End

Wait for the progress bar completes. Then log in to the web UI of the device. On the Status page, check if the current Firmware Version is consistent with the firmware version you selected for upgrade.

Tip

After the device is upgraded, you are recommended to restore the factory settings of the device and configure it again to get the best experience.

9.2.4 Backup/restore

The **Backup/Restore** function enables you to export the current configuration of the device to a local computer, and import the configuration file you export before.

You are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the device, or import the configuration to other devices of the same product model.

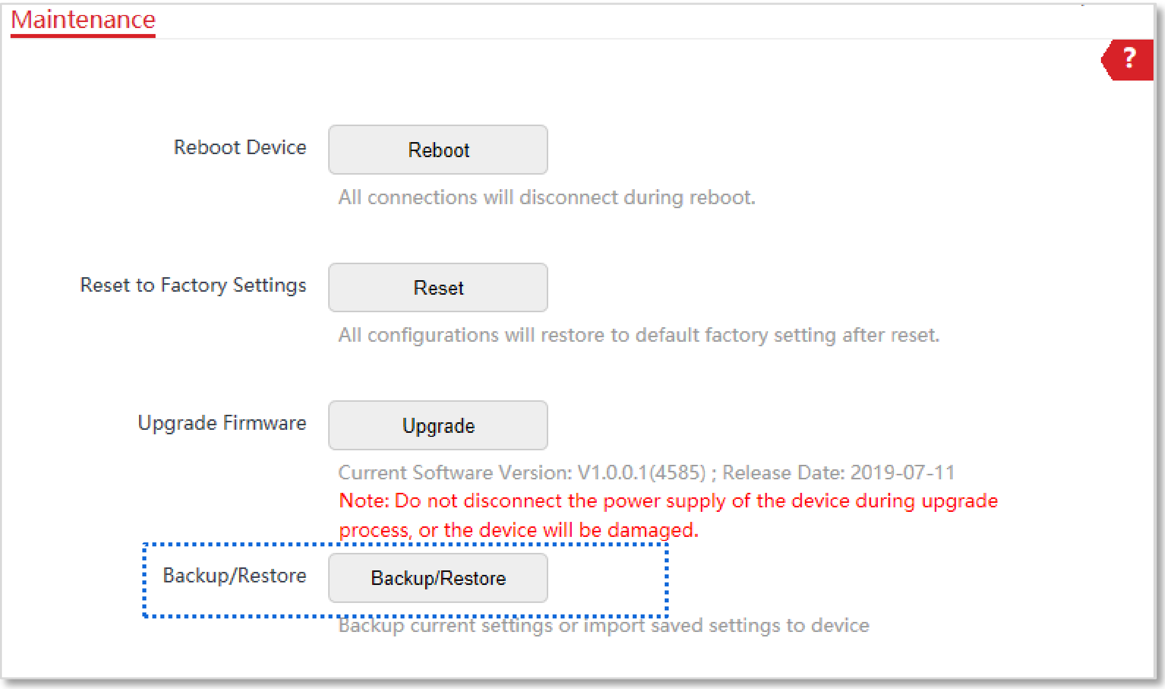
Note

If you need to apply same or similar configurations to many devices, you can configure one of the devices, back up the configuration of the device, and import the configuration file to the other devices. This improves configuration efficiency.

Export the configuration

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Tools** > **Maintenance**.

2 Click **Backup/Restore**.



All connections will disconnect during reboot.

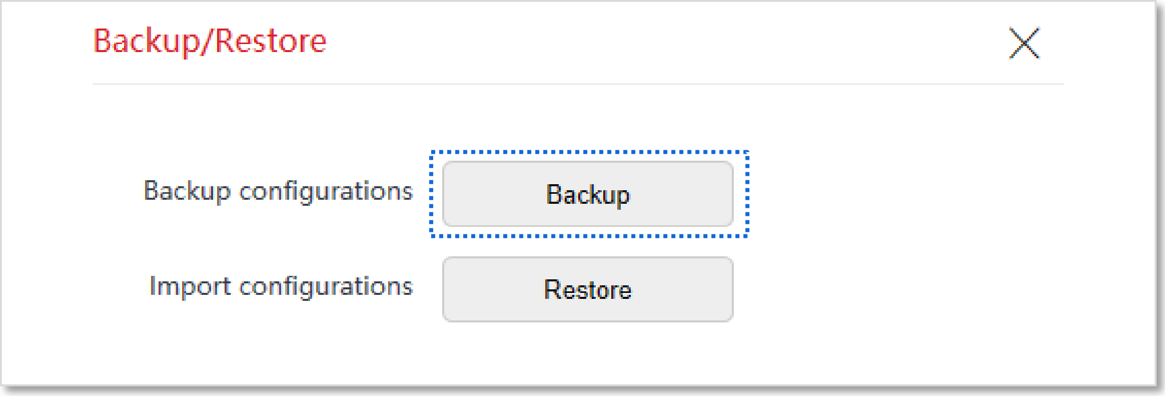
All configurations will restore to default factory setting after reset.

Current Software Version: V1.0.0.1(4585) ; Release Date: 2019-07-11

Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.

Backup current settings or import saved settings to device

3 Then click **Backup** on the pop-up window.



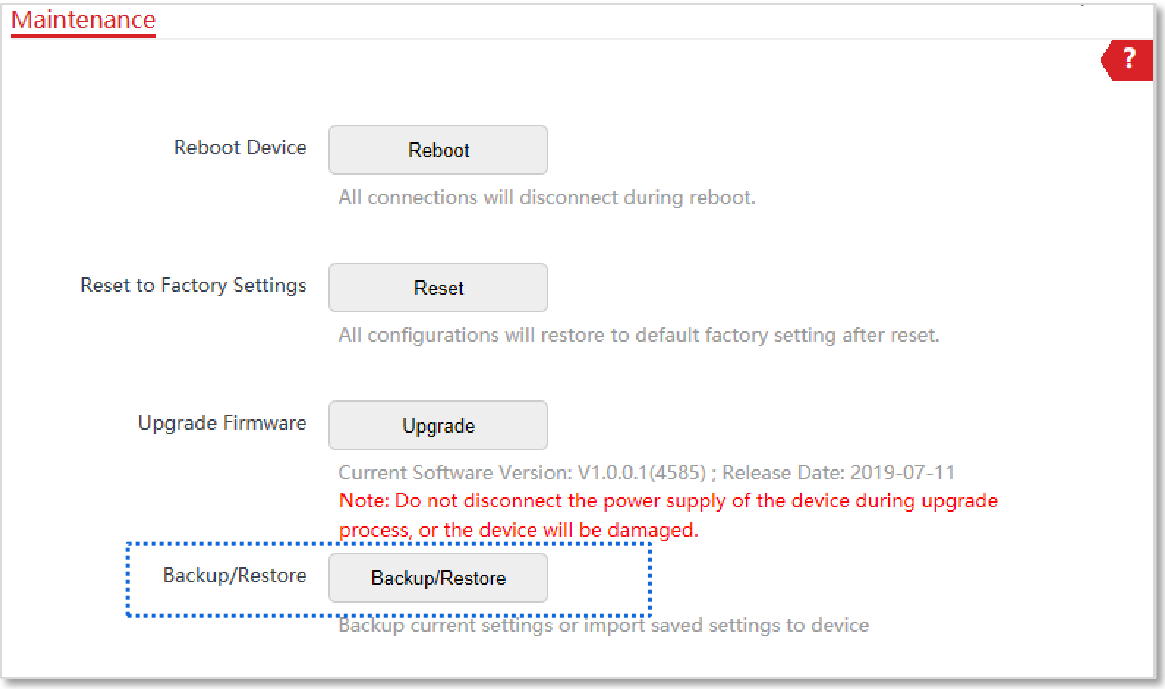
---End

A file named **APCfm.cfg** is downloaded to your local computer.

Import the configuration

1 Start a web browser on the computer connected to the base station, visit **192.168.2.1** and choose **Tools** > **Maintenance**.

2 Click **Backup/Restore**.



All connections will disconnect during reboot.

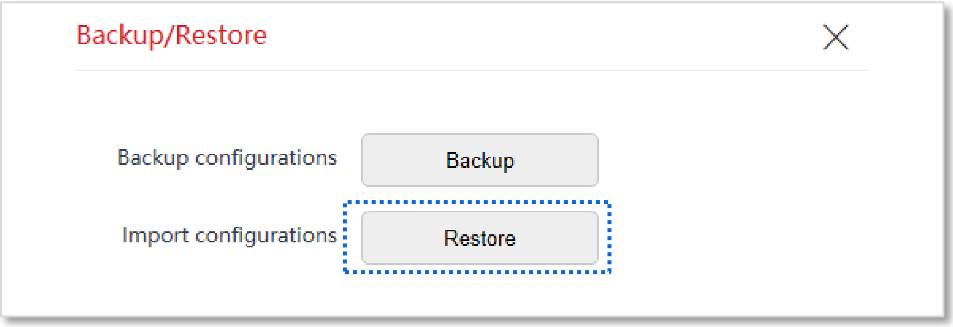
All configurations will restore to default factory setting after reset.

Current Software Version: V1.0.0.1(4585) ; Release Date: 2019-07-11

Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.

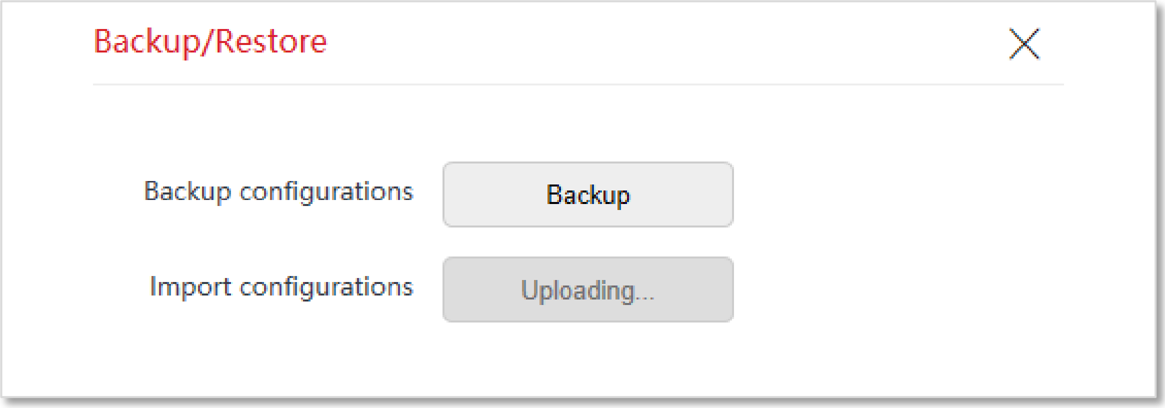
Backup current settings or import saved settings to device

3 Click **Restore** on the pop-up window.



4 Select and upload the file you export before.

---End



Backup/Restore

Backup configurations Backup

Import configurations Uploading...

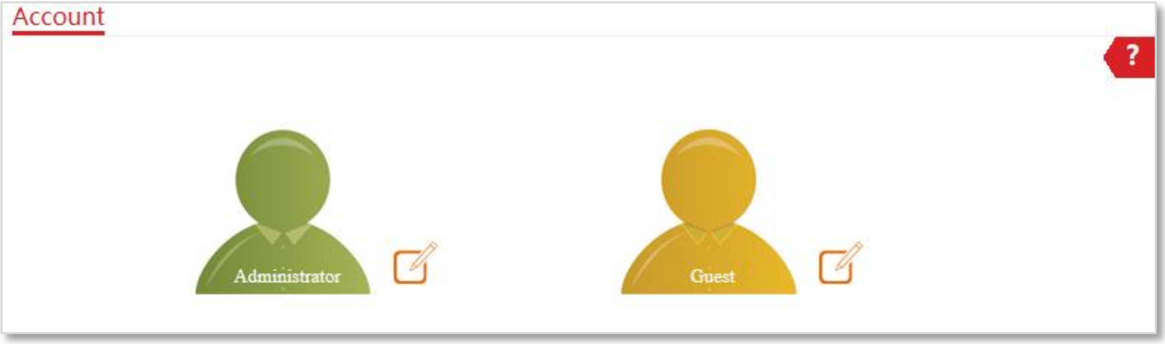
Wait for the progress bar completes. Then the device is restored the settings successfully.

9.3 Account

On this page, you can change the login account information of the device to prevent unauthorized login. By default, the device has one administrator account and one guest account. With the administrator account, you can modify and view the settings of the device while with the guest account, you can only view the settings.

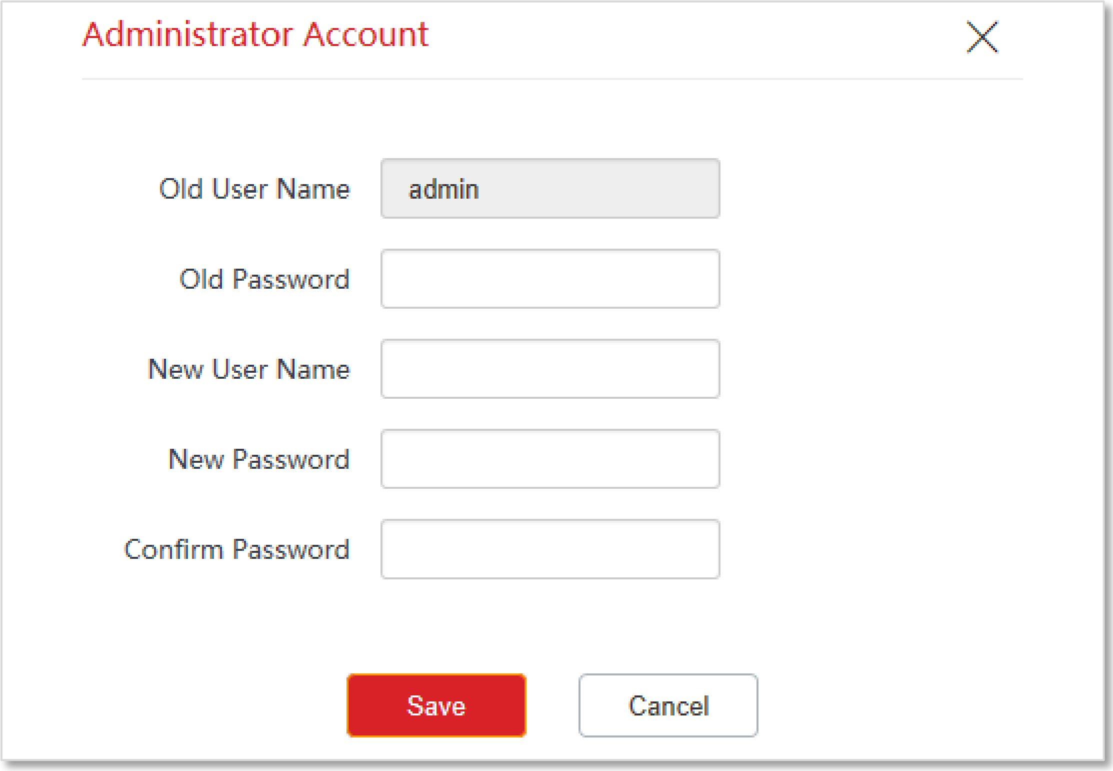
To access the page, choose **Tools** > **Account**.

Click ✎ to change the account information.



9.3.1 Administrator

You can modify and view the settings with the administrator account. Both the default user name and password of the administrator account are **admin**.



Administrator Account

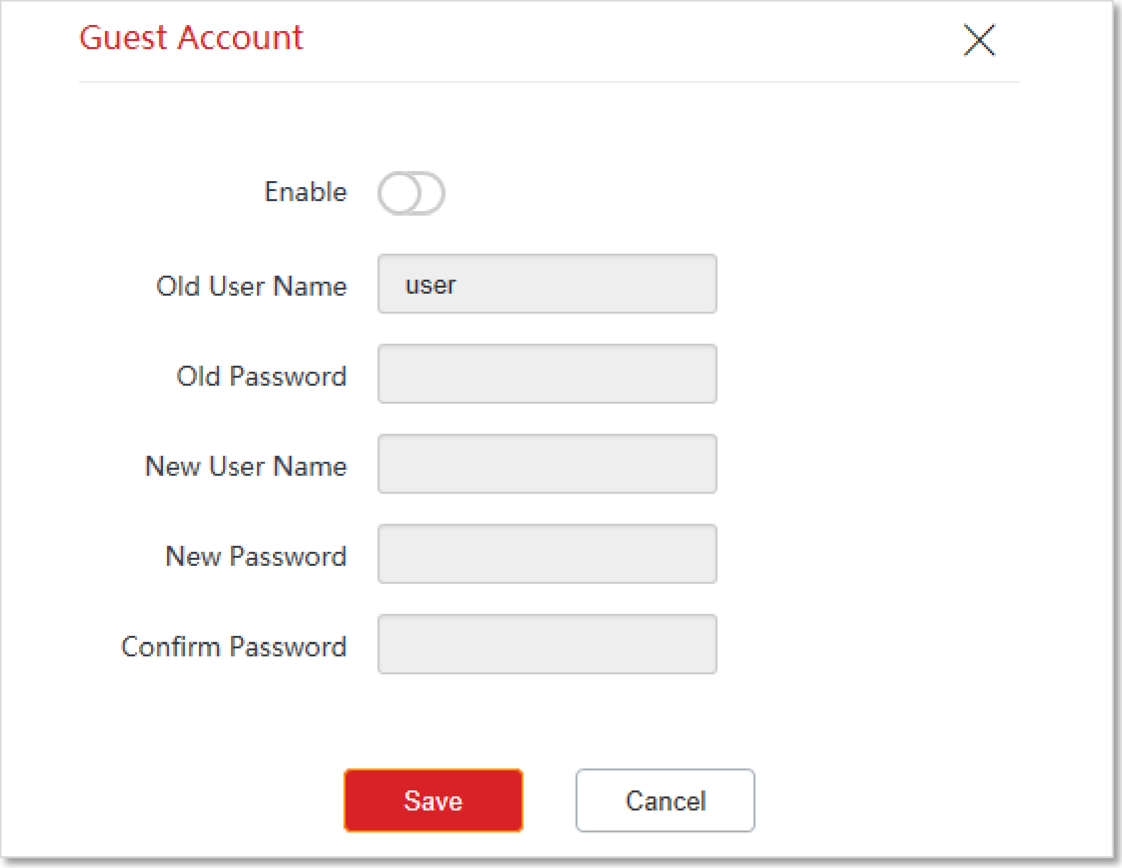
Old User Name	admin
Old Password	
New User Name	
New Password	
Confirm Password	

Parameters description

Parameter	Description
Old User Name	It specifies the user name of the current login account. By default, the device has one administrator account and one guest account. Administrator user name/password: admin/admin (all lowercase) Guest user name/password: user/user (all lowercase)
Old Password	It specifies the current login password.
New User Name	Specify a new login user name.
New Password	Specify a new login password.
Confirm Password	Enter the login password again to confirm the new login password.

9.3.2 Guest

This account only allows you to view the settings. By default, this account is disabled. Both the default user name and password are **user**.



Guest Account

Enable ○

Old User Name: user

Old Password:

New User Name:

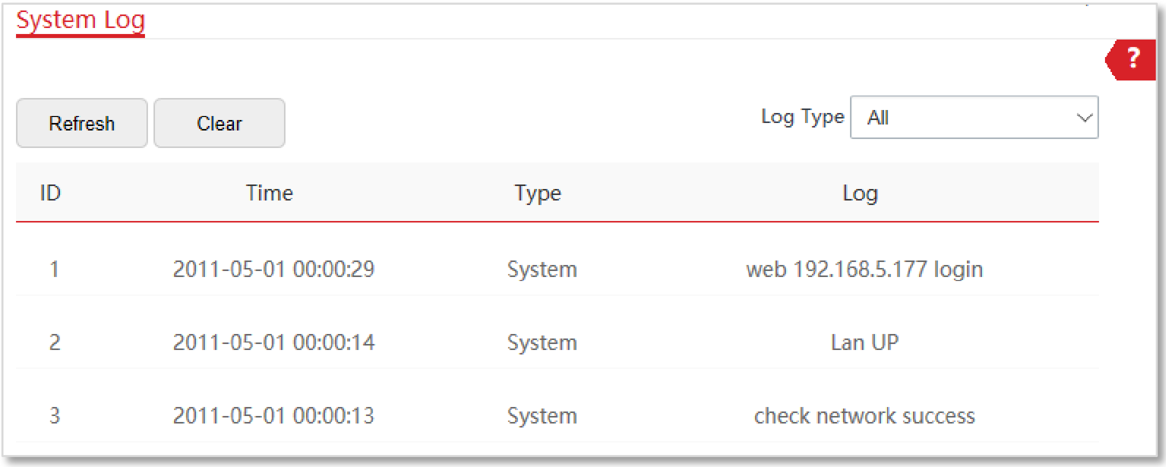
New Password:

Confirm Password:

9.4 System log

To access the page, choose **Tools** > **System Log**. The maximum of 300 items can be saved. After the total log items exceed the maximum number, the previous logs will be cleared.

The logs of the device record various events that occur and the operations that users perform after the device starts. In case of a system fault, you can refer to the logs during troubleshooting.



Log Type: All

ID	Time	Type	Log
1	2011-05-01 00:00:29	System	web 192.168.5.177 login
2	2011-05-01 00:00:14	System	Lan UP
3	2011-05-01 00:00:13	System	check network success

To ensure that the logs are recorded correctly, verify the system time of the device. You can correct the system time of the device by choosing **Tools** > **Date & Time**.

To view the latest logs of the device, click **Refresh**. To clear the existing logs, click **Clear**.

Note

- When the device reboots, the previous logs are cleared.
- The device reboots when one of the following situations occurs: the device is powered on after a power failure, the VLAN function is configured, the firmware is upgraded, the configuration of the device is backed up or restored or the factory settings are restored.

Appendix

A.1 Default parameters

The default parameters are shown in the following table:

Parameters			BS6
Login	Login IP Address		192.168.2.1
	Account	Administrator	admin/admin
		Guest	Disabled
Quick Setup	Working Mode		AP mode
LAN Setup	IP Address Type		Static IP address
	IP Address		192.168.2.1
	Subnet Mask		255.255.255.0
	Default Gateway		0.0.0.0
	Primary DNS Server		0.0.0.0
	Secondary DNS Server		0.0.0.0
	Device Name		BS6V1.0
DHCP Server	DHCP Server		Enable
	Start IP Address		192.168.2.100
	End IP Address		192.168.2.200
	Subnet Mask		255.255.255.0
	Gateway Address		192.168.2.254
	Primary DNS Server		8.8.8.8
	Secondary DNS Server		8.8.4.4
	Lease Time		1 day
VLAN Settings	VLAN Settings		Disable
	PVID		1
	Management VLAN		1
	WLAN		1000
Wireless-Basic	Wireless Network		Enable

Parameters		BS6
	Country/Region	China
	SSID	IP-COM_*XXXXXX*. *XXXXXX* is the last six characters of the LAN MAC address of the device.
	Broadcast SSID	Enable
	Network Mode	11a/n
	Channel	Auto
	Channel Shift	Disable
	Transmit Power	26 dBm
	Channel Bandwidth	20 MHz
	Transmit Rate	Auto
	Security Mode	None
	Isolate Client	Disable
	Max. Number of Clients	48
Wireless-Advanced	WMM	Enable
	APSD	Disable
	Minimum RSSI Threshold	Disable
	Preamble	Long Preamble
	Transparent Bridge	Enable
	TD-MAX	Disable
	Signal Transmission	Coverage-oriented
	TPC	Enable
	Signal Reception Level	Auto
	Transmission Distance	5 km
	Beacon Interval	100ms
	Fragment Threshold	2346
	RTS Threshold	2347
	DTIM Interval	1
	Signal LED1 Threshold	-90 dBm
	Signal LED2 Threshold	-80 dBm
	Signal LED3 Threshold	-70 dBm
Wireless – Access Control		Disable
LAN Rate		Auto Negotiation
Diagnose		Disable
Network Service	Reboot Schedule	Disable

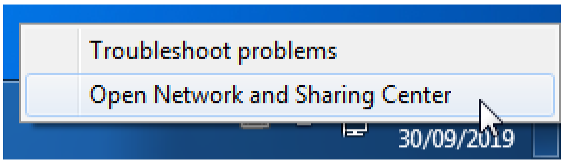
Parameters		**BS6**
	Login Timeout Interval	5 min
	SNMP Agent	Disable
	Ping Watch Dog	Disable
	Telnet Service	Enable
	UPnP	Disable
	Hardware Watch Dog	Enable
	STP	Disable
Tools	Date & Time	Synchronized with the Internet (GTM+8:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei Time Interval: 30 minutes

A.2 How to assign a fixed IP address to your computer

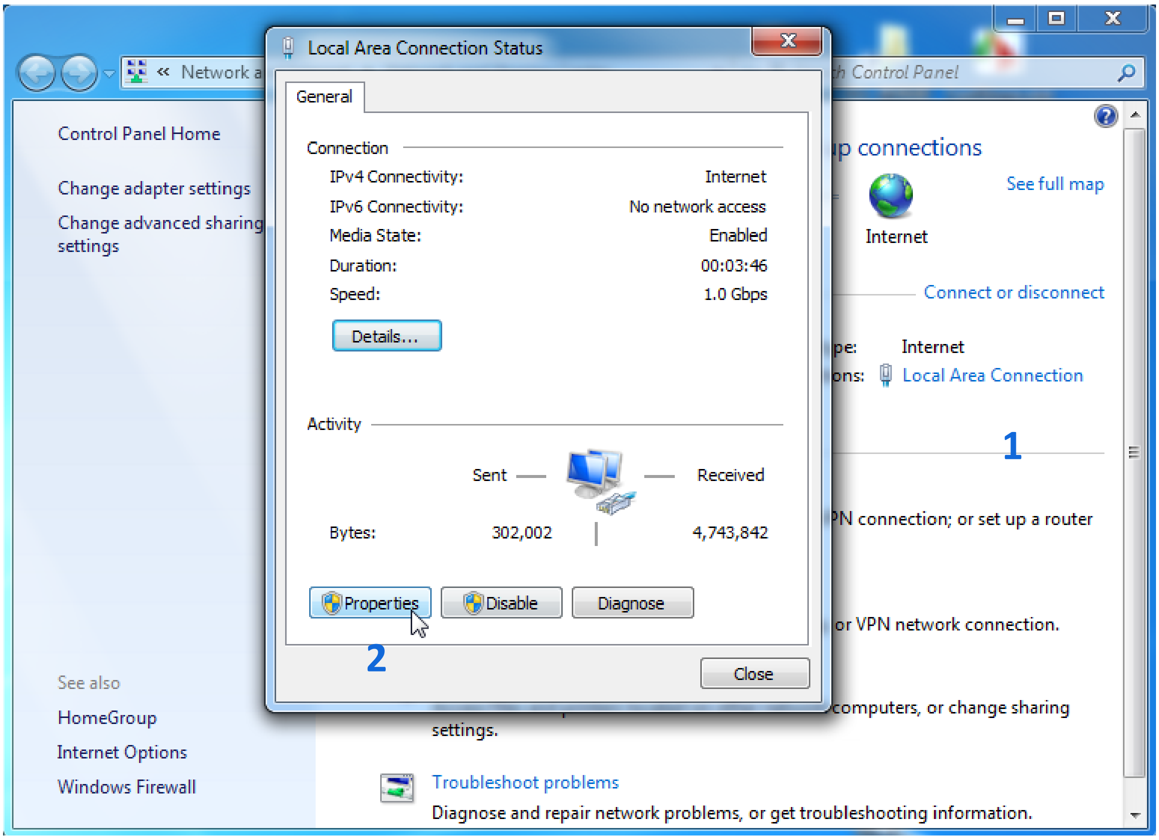
OS example: Windows 7

1 Right-click the icon on the bottom-right corner of the desktop.

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



3 Click **Local Area Connection**, then click **Properties**.



Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 00:03:46

Speed: 1.0 Gbps

Activity

	Sent	Received
Bytes:	302,002	4,743,842

pe: Internet

ons: Local Area Connection

PN connection; or set up a router

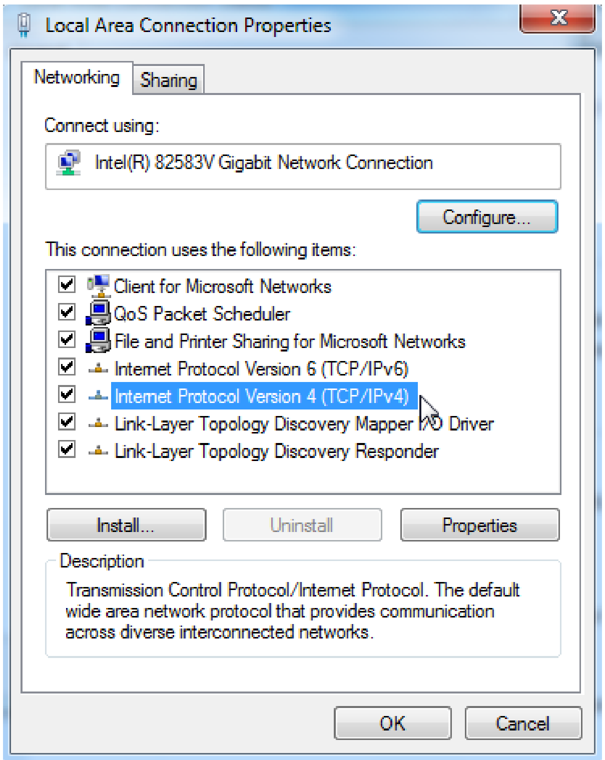
or VPN network connection.

computers, or change sharing settings.

Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

4 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Intel(R) 82583V Gigabit Network Connection

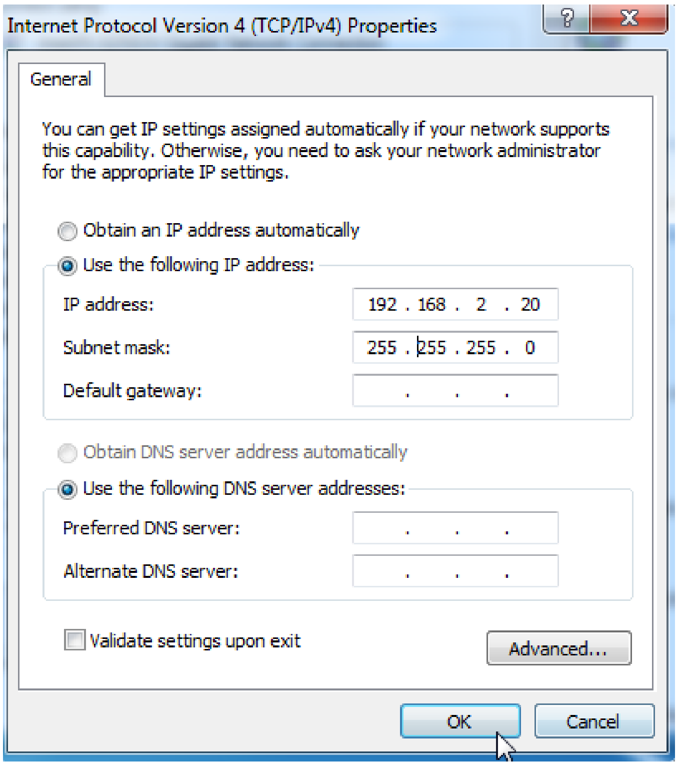
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5 Select **Use the following IP address**, set the **IP address** to **192.168.2.*X*** (*X* ranges from 2 to 253), the **Subnet mask** to **255.255.255.0**, and click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

6 Click **OK** on the **Local Area Connection Properties** window, and close the other windows.

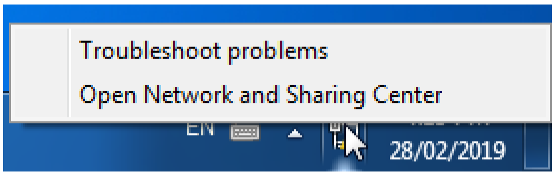
---End

A.3 How to check the gateway IP address of a computer

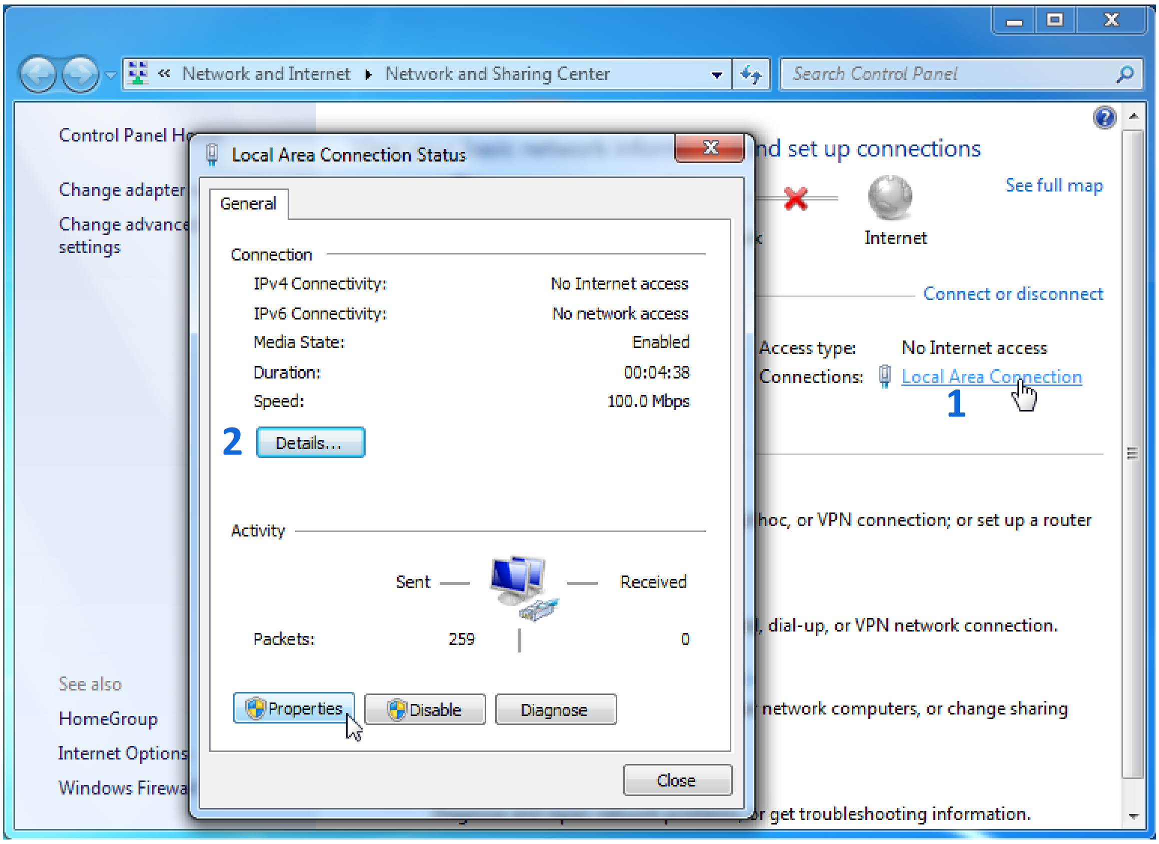
OS example: Windows 7

1 Right-click the icon on the bottom-right corner of the desktop.

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



3 Click **Local Area Connection**, then click **Details...**



Connection

IPv4 Connectivity: No Internet access

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 00:04:38

Speed: 100.0 Mbps

Activity

Sent — Received

Packets: 259 | 0

Access type: No Internet access

Connections: Local Area Connection

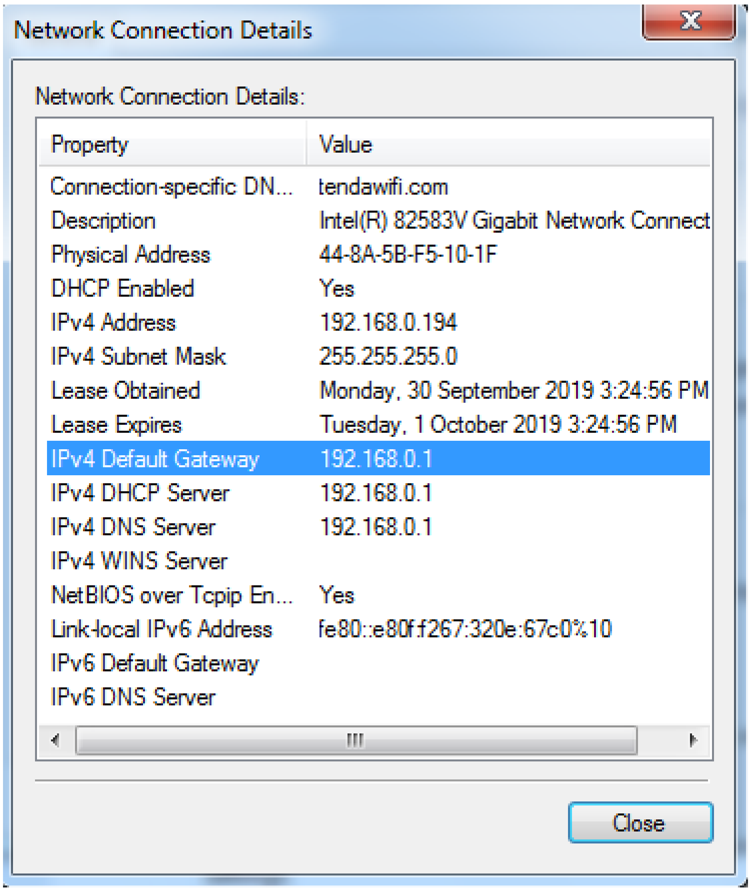
hoc, or VPN connection; or set up a router

, dial-up, or VPN network connection.

network computers, or change sharing

r get troubleshooting information.

Then you can check the default gateway address on the following page.



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	tendawifi.com
Description	Intel(R) 82583V Gigabit Network Connect
Physical Address	44-8A-5B-F5-10-1F
DHCP Enabled	Yes
IPv4 Address	192.168.0.194
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Monday, 30 September 2019 3:24:56 PM
Lease Expires	Tuesday, 1 October 2019 3:24:56 PM
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::e80f:f267:320e:67c0%10
IPv6 Default Gateway	
IPv6 DNS Server	