# 2Km Outdoor Point to Point CPE

# User Guide

## Copyright Statement

© 2019 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Tenda is a registered trademark legally held by Shenzhen Tenda Technology Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd.

## Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product 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 Tenda! Please read this user guide before you start.

# Conventions

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

| Item | Presentation | Example |
| --- | --- | --- |
| Cascading menus | > | **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. |
| Message | “ ” | The “Success” message appears. |

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

| Symbol | 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 |
| --- | --- |
| AP | Access Point |
| ARP | Address Resolution Protocol |
| AES | Advanced Encryption Standard |
| CPE | Customer Premises Equipment |
| CCQ | Client Connection Quality |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| DDNS | Dynamic Domain Name Server |

| Acronym or Abbreviation | Full Spelling |
|---|---|
| GMT | Greenwich Mean Time |
| IP | Internet Protocol |
| ICMP | Internet Control Message Protocol |
| LAN | Local Area Network |
| MAC | Media Access Control |
| PoE | Power Over Ethernet |
| P2MP | Point-to-MultiPoint |
| PVID | Port-based VLAN ID |
| RADIUS | Remote Authentication Dial In User Service |
| SSID | Service Set Identifier |
| TCP | Transmission Control Protocol |
| TKIP | Temporal Key Integrity Protocol |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |
| WAN | Wide Area Network |
| WEP | Wired Equivalent Privacy |
| WLAN | Wireless Local Area Networks |
| WMM | Wi-Fi multi-media |
| WPA-PSK | WPA-Preshared Key |
| WPA | Wi-Fi Protected Access |

## Additional Information

For more information, search this product model on our website at http://www.tendacn.com.

## Technical Support

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

| | | | |
|---|---|---|---|
| **Hotline** | Global: (86) 755-27657180<br>Toll Free: Mon - Fri 9 am - 6 pm (China Time Zone)<br><br>United States: 1-800-570-5892<br>Toll Free: Daily-9am to 6pm EST<br><br>Canada: 1-888-998-8966<br>Toll Free: Mon - Fri 9 am - 6 pm PST<br><br>Hong Kong: 00852-81931998<br>Toll Free: Mon - Fri 9 am - 6 pm (China Time Zone) | **Email** | support@tenda.com.cn |
| **Website** | http://www.tendacn.com | | |

# Contents


1 Introduction ..... 1

1.1 Overview ..... 1

1.2 Getting to know your device ..... 1

2 Quick setup ..... 4

2.1 AP mode ..... 4

2.2 Client mode ..... 7

2.3 Example of AP mode and client mode ..... 10

2.4 Universal repeater mode ..... 16

2.5 WISP mode ..... 22

2.6 Repeater mode ..... 31

2.7 P2MP mode ..... 41

2.8 Example of repeater mode and P2MP mode ..... 45

2.9 Router mode ..... 52

3 Web UI ..... 56

3.1 Login ..... 56

3.2 Logout ..... 58

3.3 Web UI layout ..... 59

3.4 Common buttons ..... 59

4 Status ..... 60

4.1 System status ..... 60

4.2 Wireless status ..... 63

4.3 Statistics ..... 65

5 Network ..... 70

5.1 LAN setup ..... 70

5.2 MAC clone ..... 77

5.3 DHCP server ..... 79

5.4 DHCP client....81
5.5 VLAN settings....82
6 Wireless....86
6.1 Basic....86
6.2 Advanced....114
6.3 Access control....118
7 Advanced....121
7.1 LAN rate....121
7.2 Diagnose....123
7.3 Bandwidth control....130
7.4 Port forwarding....133
7.5 MAC filter....137
7.6 Network service....141
8 Tools....159
8.1 Date & time....159
8.2 Maintenance....161
8.3 Account....166
8.4 System log....169
Appendix....170
A.1 FAQ....170
A.2 Default parameters....173

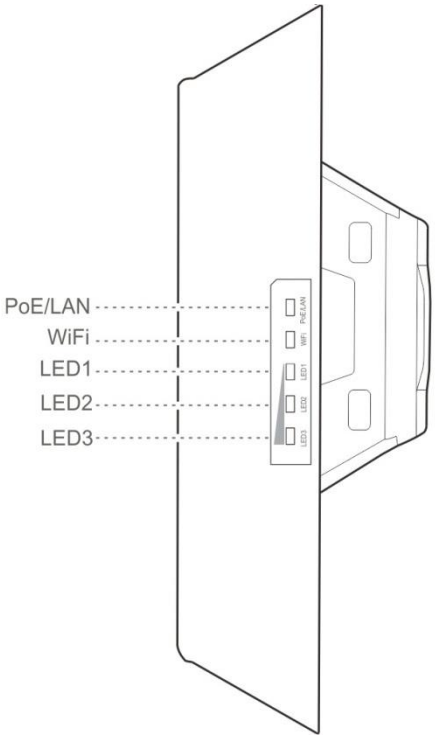
# 1 Introduction

## 1.1 Overview

The Tenda outdoor point to point CPE is dedicated for ISP and CCTV surveillance. Featured 12 dBi directional antennas, it offers strong and stable WiFi signals and a wireless connection up to 2 kilometers. The industry grade waterproof and dustproof housing allows it to work properly even in harsh environments. With auto-bridging technology, two CPEs can connect to each other automatically to make setup a breeze.

## 1.2 Getting to know your device

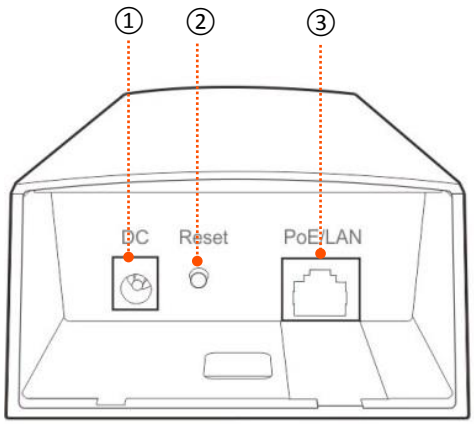
### LED indicators

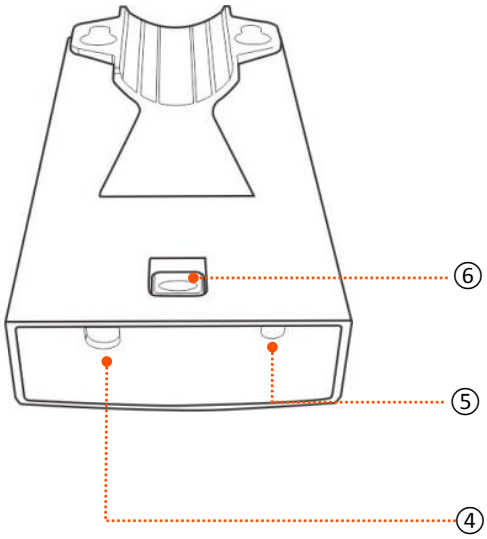



| LED Indicator | Status | Description |
|---|---|---|
| PoE/LAN | Solid on | The device is being powered properly, and no data is being transmitted. |
| | Blinking | Data is being transmitted over the port. |

| LED Indicator | Status | Description |
|---|---|---|
| | Off | The device is not powered on. |
| WiFi | Solid on | The wireless function is enabled, but no data is being transmitted. |
| | Blinking | Data is being transmitted in a wireless manner. |
| | Off | The wireless function is disabled. |
| LED1, LED2, LED3<br>(Signal strength LED) | Solid on/Blinking | Signal strength LED indicators. Solid on indicates the device works in AP, P2MP, Repeater or Router mode, while blinking indicates the device works in Client, Universal Repeater or WISP mode. The corresponding LED indicator lights up when the received signal strength reaches the threshold of the corresponding LED indicator which is set on the **Wireless** > **Advanced** page. The default threshold for LED1, LED2, and LED3 are **-90** dBm, **-80** dBm, and **-70** dBm respectively.<br>• LED1, LED2 and LED3 are solid on/blinking: Good signal<br>• LED1 and LED2 are sold on/blinking, and LED3 is off: Fair signal<br>• LED1 is solid on/blinking, and LED2 and LED3 are off: Weak signal. Please adjust the direction or location of your devices. |
| | Off | The received signal does not reach the minimum threshold of the signal strength LED indicator. |

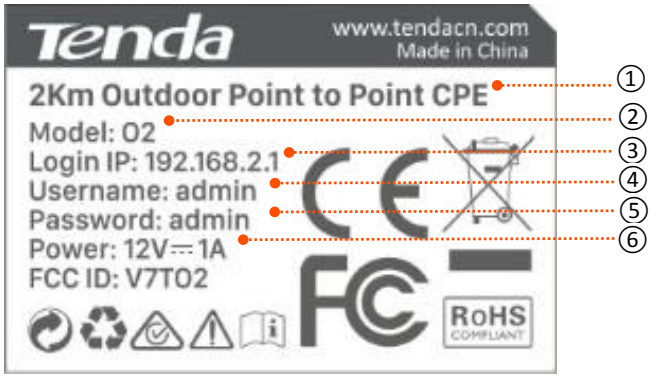
## Button and ports



| ID | Port/Button | Description |
|---|---|---|
| ① | DC | Power jack. Use the included power adapter to connect this jack to a power source for power supply. |
| ② | Reset | Reset Button. After the device is powered on for 1 minute, hold down this button for about 8 seconds. When all the LED indicators on the device light up, the device is restored factory settings. |
| ③ | PoE/LAN | This port is used to supply power or transmit data.<br>• To power on the device using PoE, connect this port to the PoE port of the included PoE injector.<br>• If the device is powered on using a DC power adapter, this port functions as a LAN port, and can be connected to a switch. |
| ④ | / | Ethernet cable inlet. |
| ⑤ | / | Power cord inlet. |
| ⑥ | / | Press this button to uncover the device. |

## Product label




①→Product name of the device

②→Product model of the device

③→Default login IP address of the device

④→Default login user name of the device

⑤→Default login password of the device

⑥→Power input standard of the device

# 2 Quick setup

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

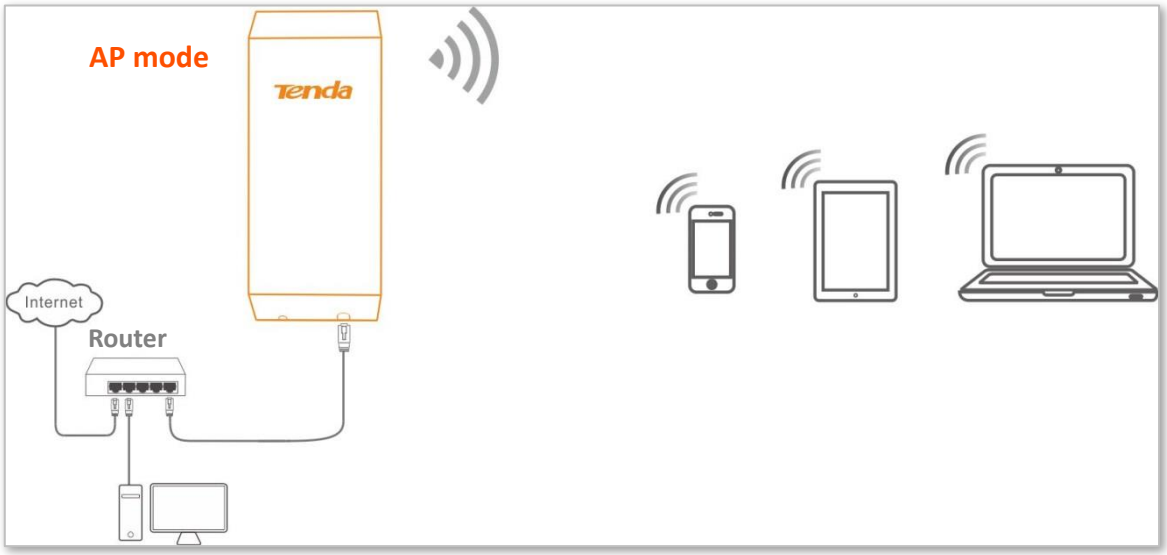
O2 supports AP, Client, Universal Repeater, WISP, Repeater, P2MP, and Router modes.

## 2.1 AP mode

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

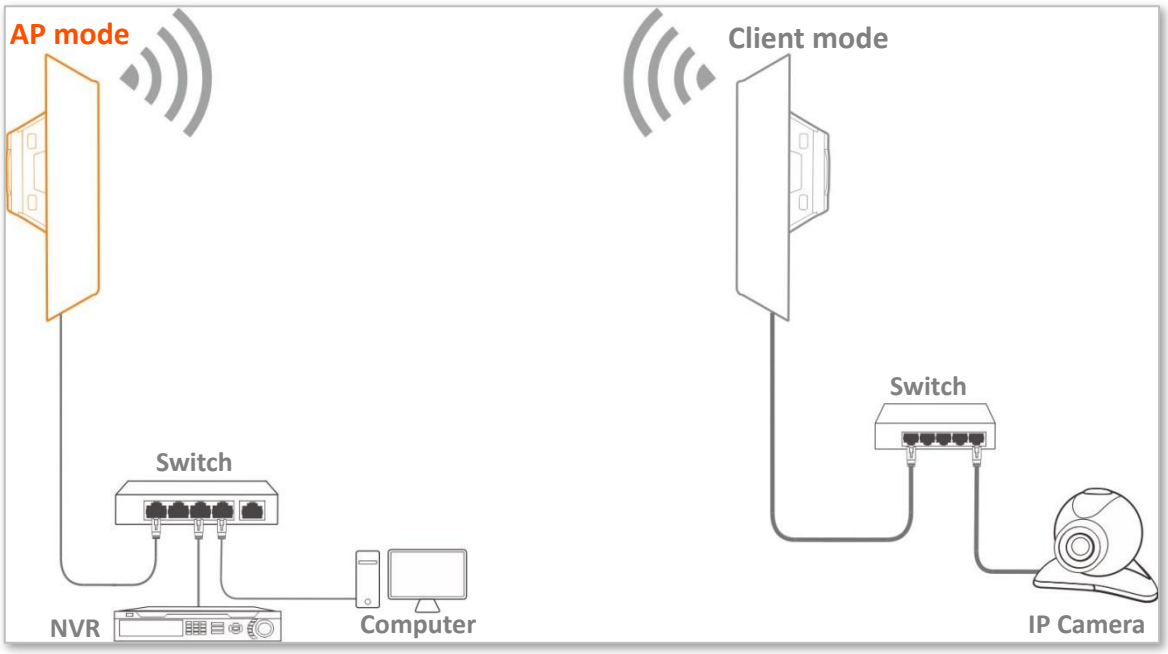
**Application scenario 1**

**Network requirement**: You want to transform your wired network to a wireless one for your wireless devices to access the internet.



### Application scenario 2

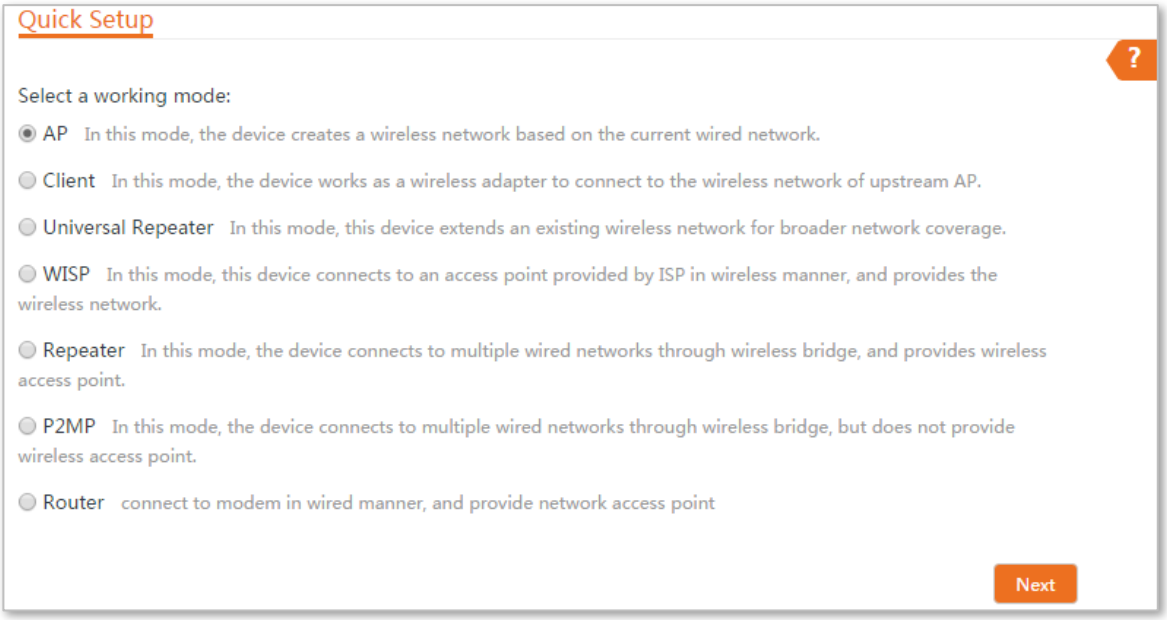
**Network requirement**: You want to establish a CCTV surveillance network, and use the CPE to connect to the NVR.



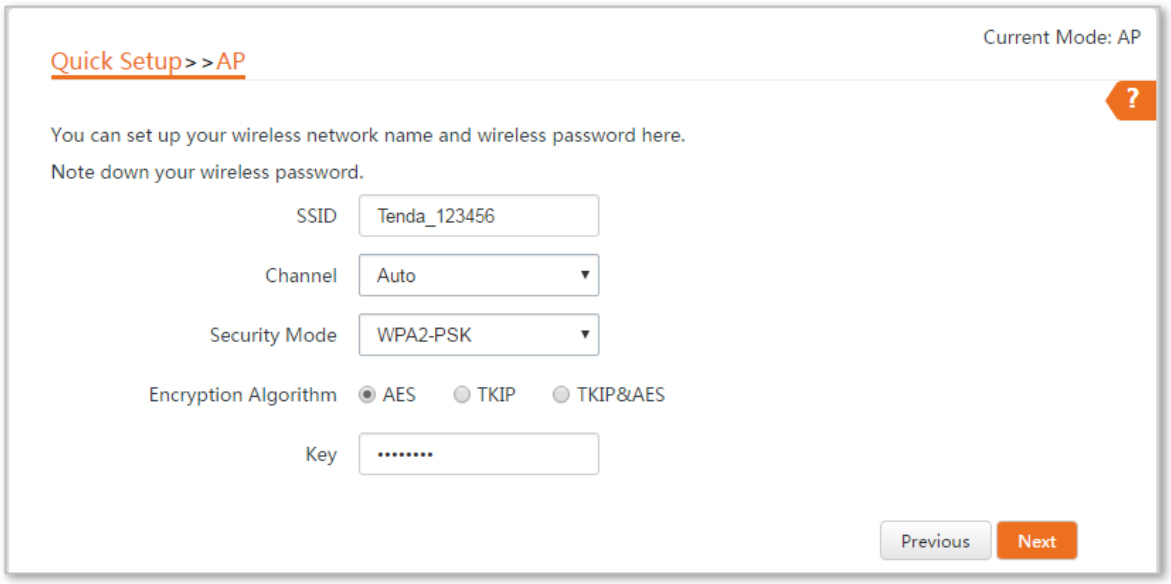

### Configuration procedure of setting AP mode

**Step 1** Log in to the web UI of the CPE and choose **Quick Setup** to enter the configuration page.

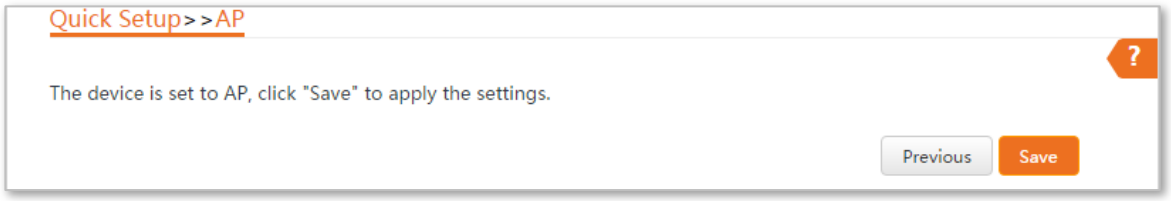
**Step 2** Select **AP** mode and click **Next**.




**Step 3** Set an SSID, **Security Mode** (WPA2-PSK is recommended) and **Key**, and click **Next**.




**Step 4** Click **Save**, and wait until the device reboots automatically to activate the settings.




**----End**

### Parameters description

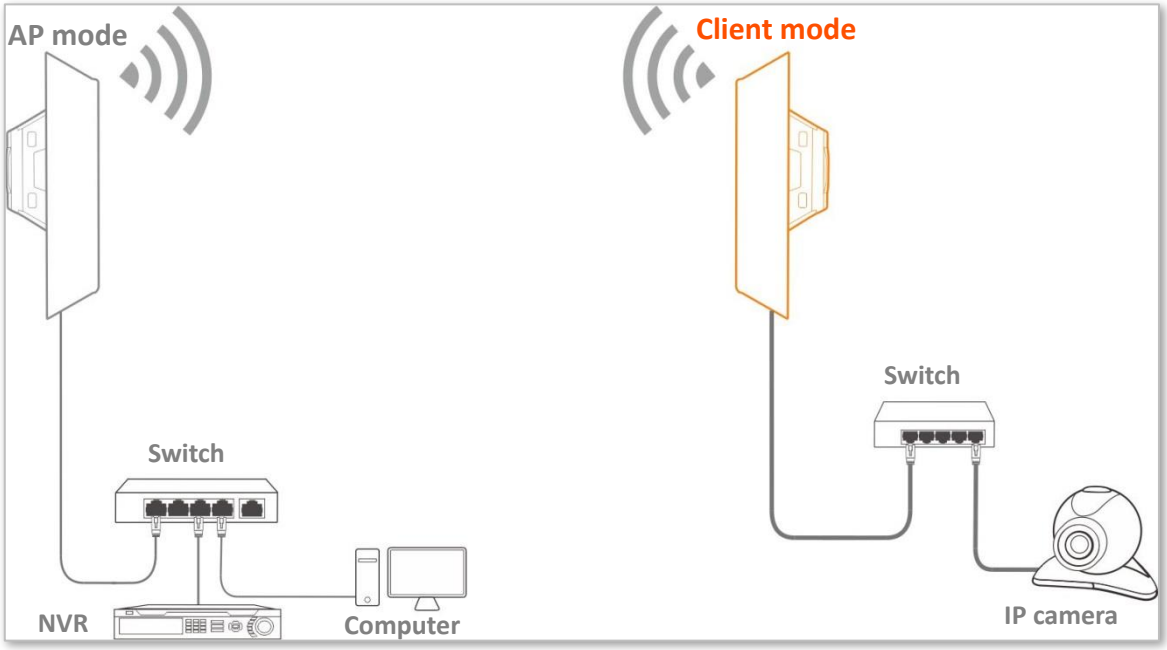
| Name | Description |
|---|---|
| Working modes | It specifies the working mode of this device.<br>**AP** mode: in this mode, the device creates a wireless network based on the current wired network. |
| SSID | It specifies the wireless network name of this device. |
| Channel | It specifies the operating channel of this device.<br>**Auto**: 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.<br>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. |
| Key | It specifies the WiFi password of the wireless network. |

# 2.2 Client mode

In Client mode, this device servers as a wireless adapter, and connects to a wireless network of upstream AP.

**Application scenario**

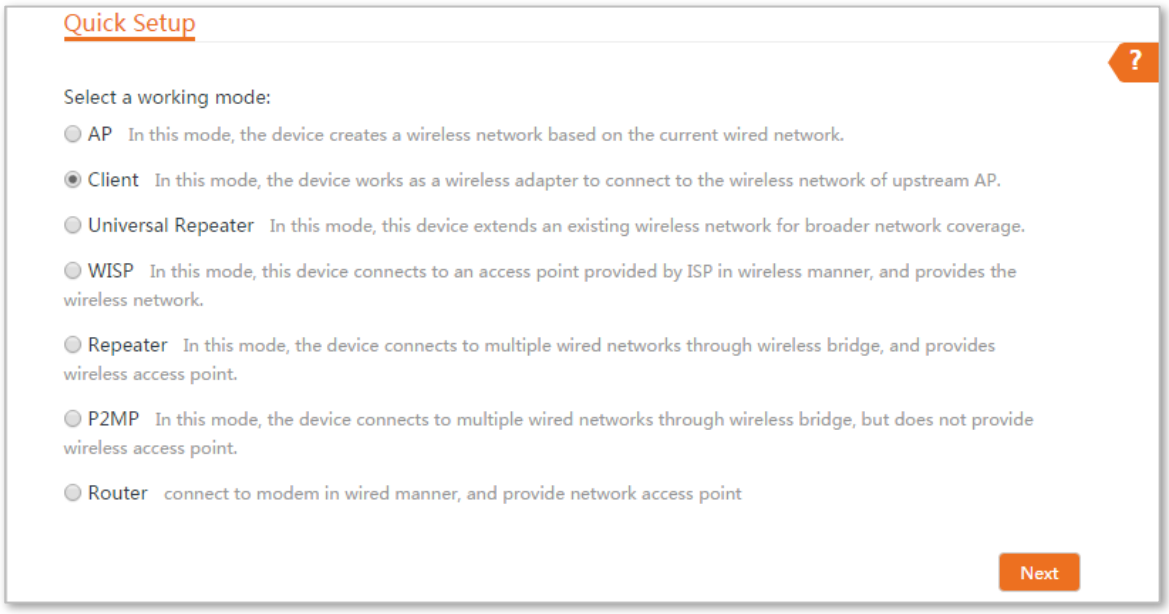
**Network requirement**: you want to establish a CCTV surveillance network, and use the CPE to connect to IP cameras.



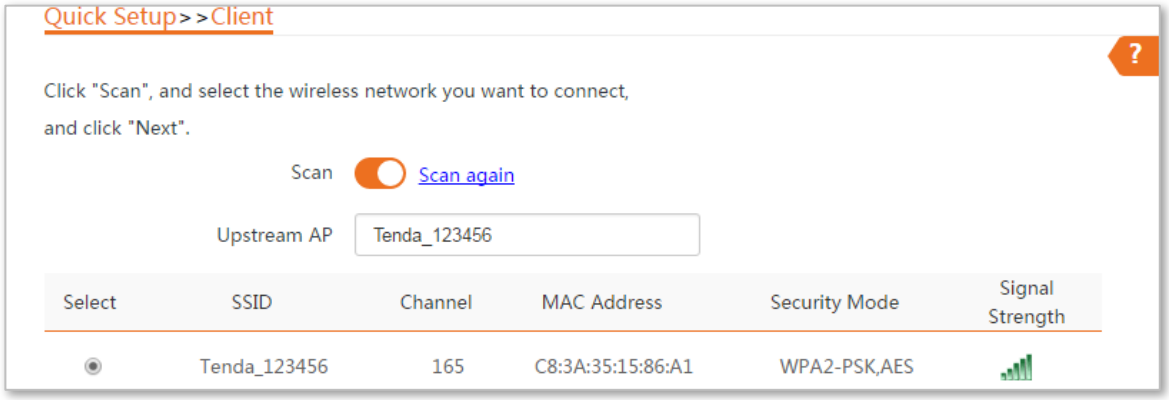

**Configuration procedure of setting Client mode**

**Step 1** Log in to the web UI of CPE and choose **Quick Setup** to enter the configuration page.

**Step 2** Select **Client**, and click **Next**.



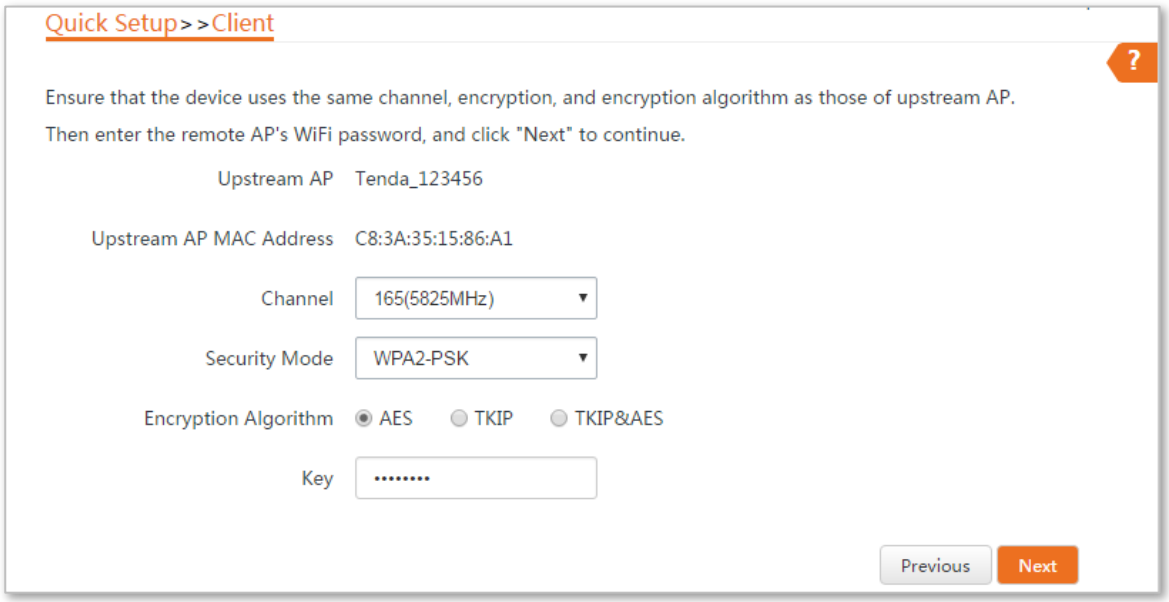

**Step 3** Select the SSID of the peer device and click **Next**.



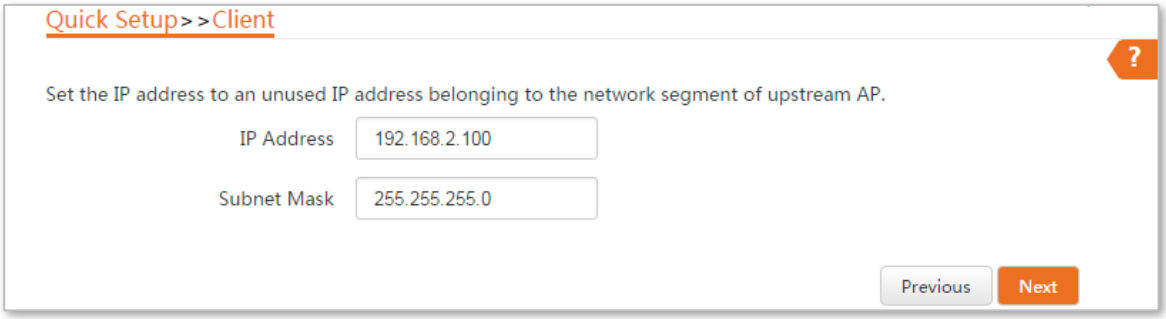

TIP

- 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 CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1.

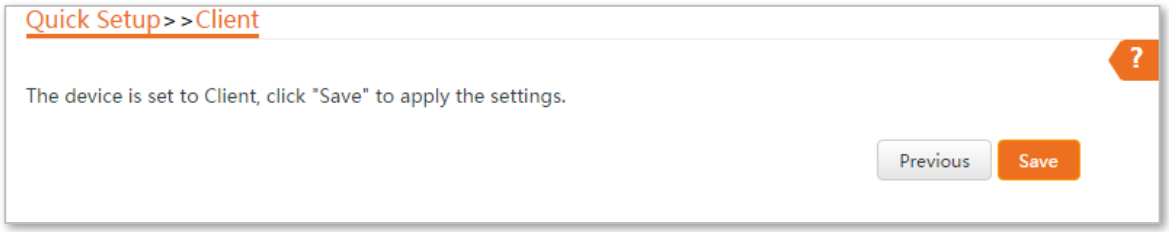
**Step 4** Enter the WiFi password you set on the peer device in the **Key** text box, and click **Next**.




**Step 5** Set the IP address to an unused IP address belonging to the same network segment as that of the peer device. For example, if the IP address of the peer device 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**.




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




**----End**

When LED1, LED2, and LED3 of the peer device are solid on, and LED1, LED2, and LED3 of the CPE are blinking, the bridging succeeds.

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 CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1

**Parameters description**

| Name | Description |
|---|---|
| Working modes | It specifies the working mode of this device.<br>**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 access point. |
| Upstream AP | It specifies the wireless network name (SSID) 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. |

# 2.3 Example of AP mode and client mode

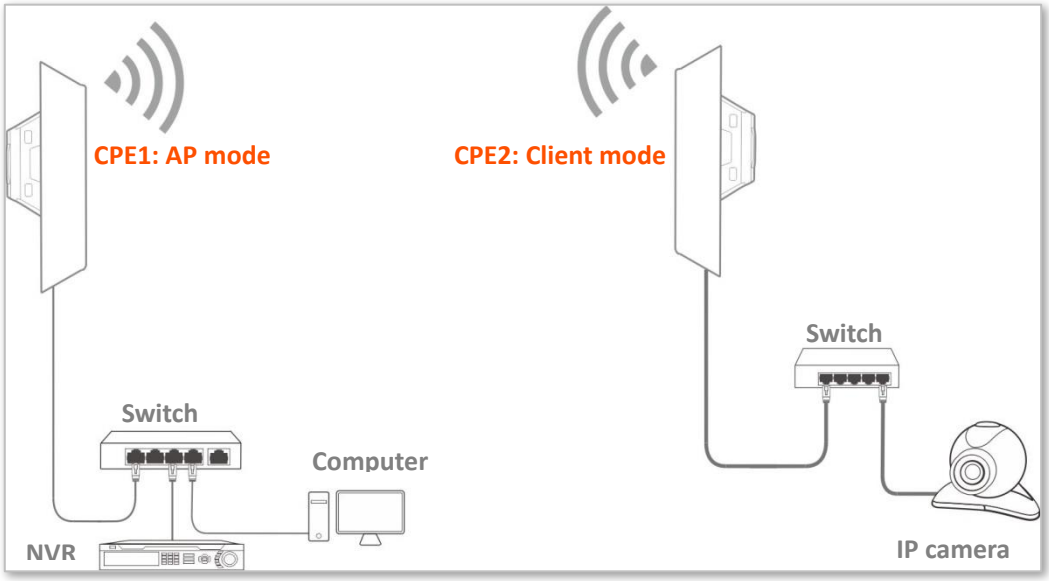
## Network requirement

You want to use two CPEs to establish a CCTV surveillance network.

## Solution

- Set CPE1 to the AP mode, and connected it to the NVR.
- Set CPE2 to the Client mode, and connected it to IP cameras.

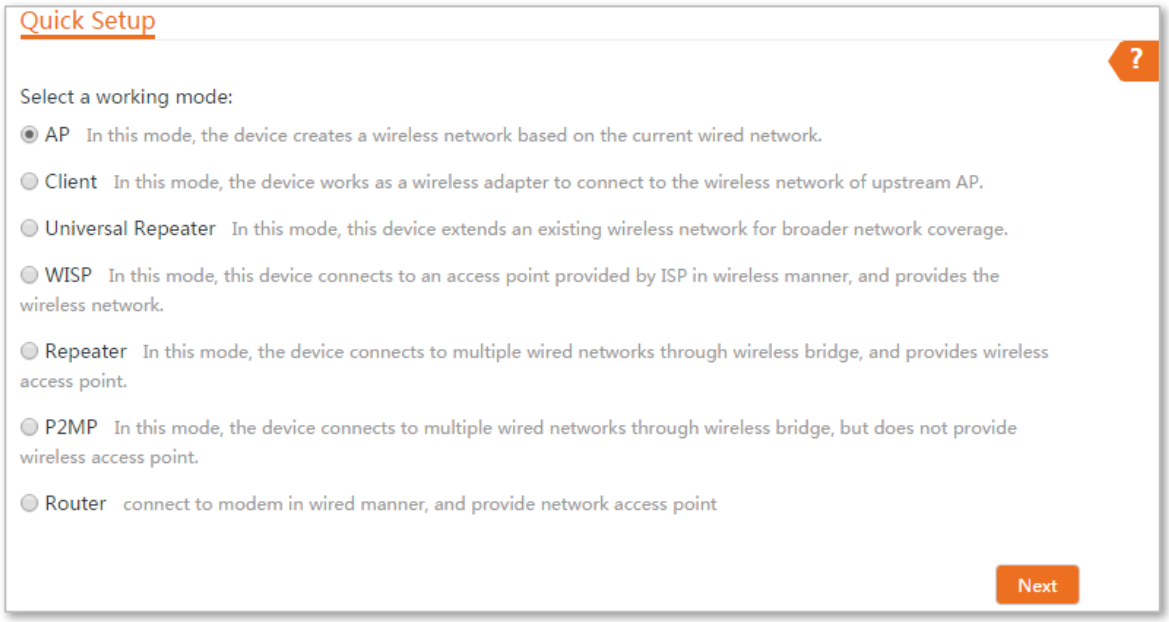
## Network topology



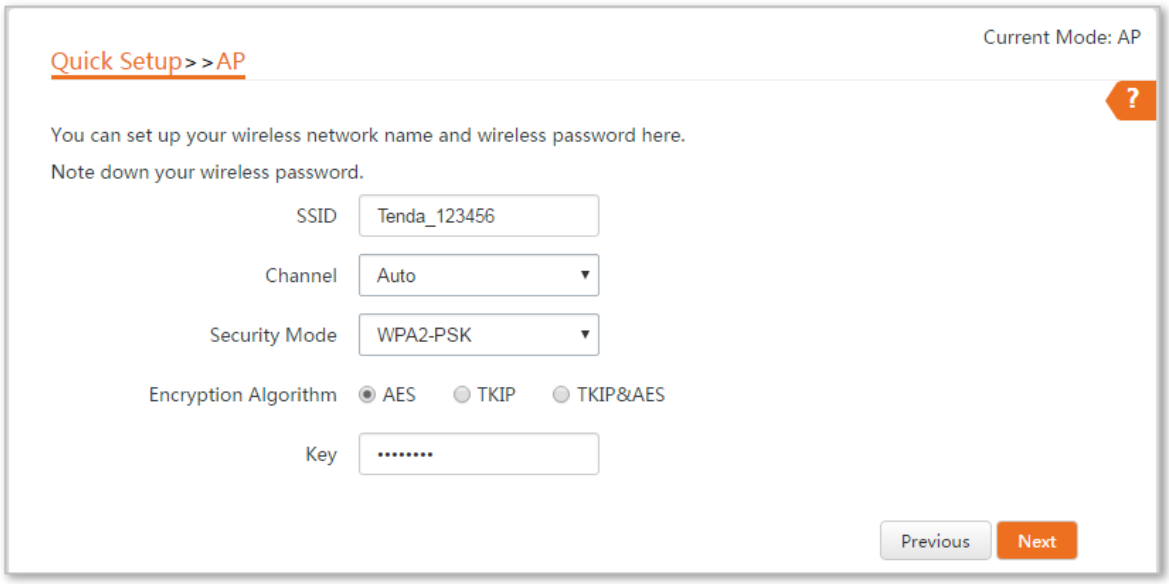

## Configuration procedure

**Step 1** Set up CPE1.

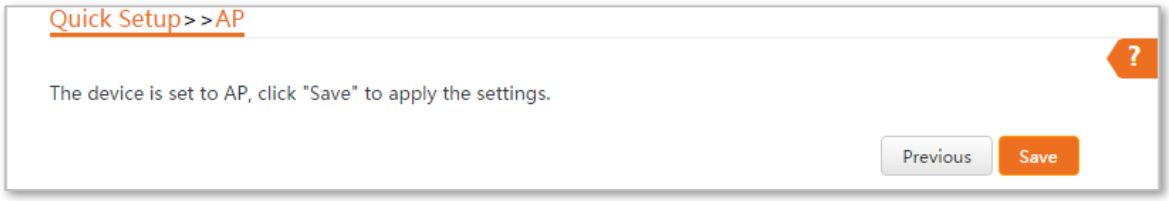
1. Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
2. Select **AP** mode and click **Next**.




3. Set an SSID, which is **Tenda_123456** in this example, **Security Mode** (WPA2-PSK is recommended) and **Key**, and click **Next**.

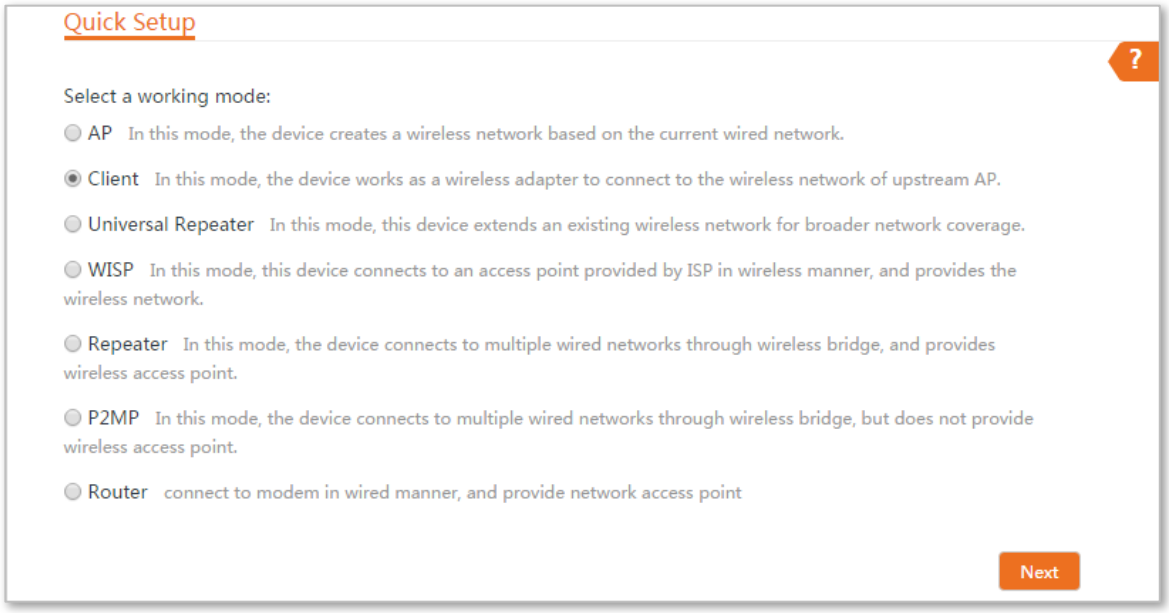



4. Click **Save**, and wait until the device reboots automatically to activate the settings.

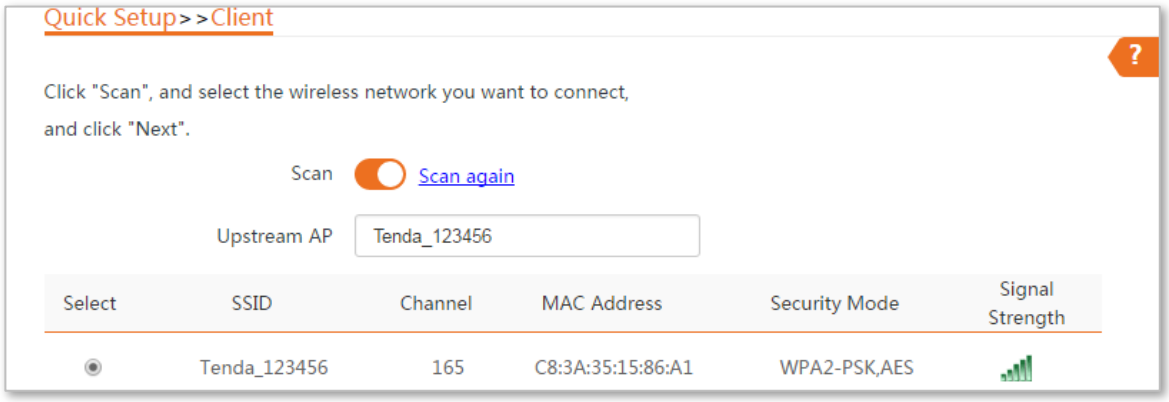



**Step 2** Set up CPE2.

1. Log in to the web UI of CPE2 and choose **Quick Setup** to enter the configuration page.
2. Select **Client**, and click **Next**.



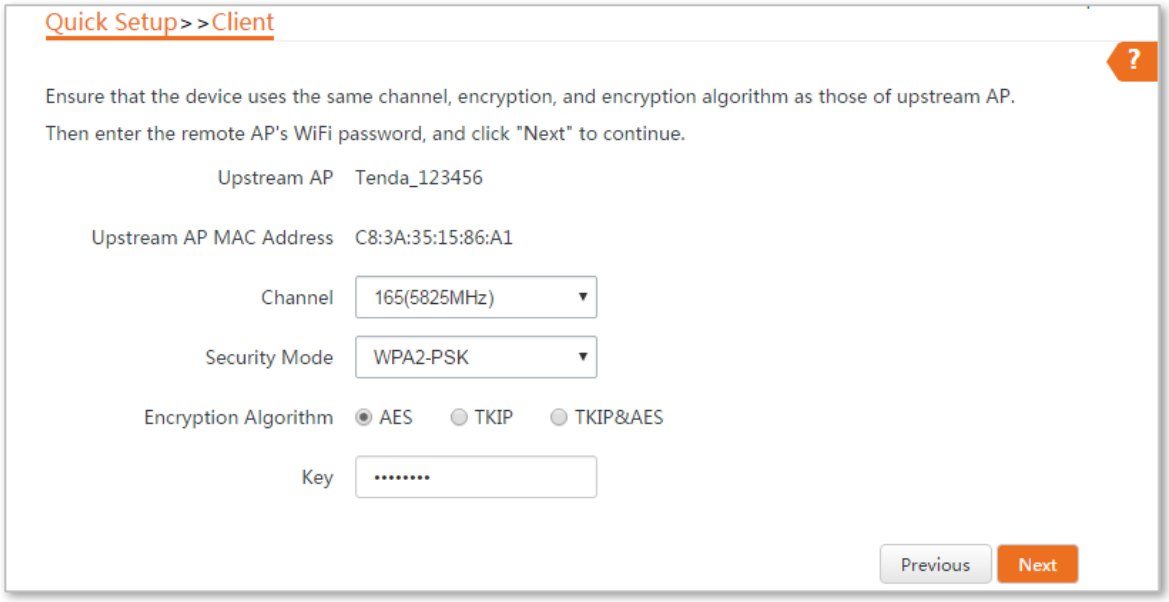

3. Select the SSID of the CPE1, which is **Tenda_123456** in this example, and click **Next**.


Quick Setup>>Client
Click "Scan", and select the wireless network you want to connect,
and click "Next".
Scan
Scan again
Upstream AP
Tenda_123456
Select
SSID
Channel
MAC Address
Security Mode
Signal Strength
Tenda_123456
165
C8:3A:35:15:86:A1
WPA2-PSK,AES

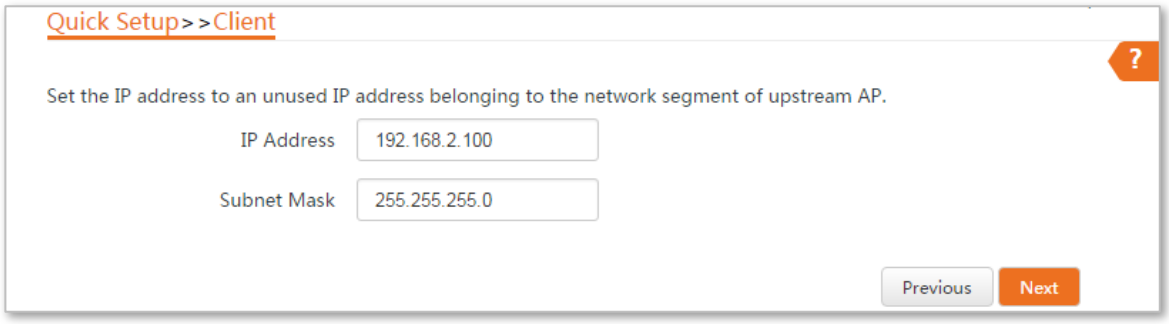
TIP

- 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 CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1.

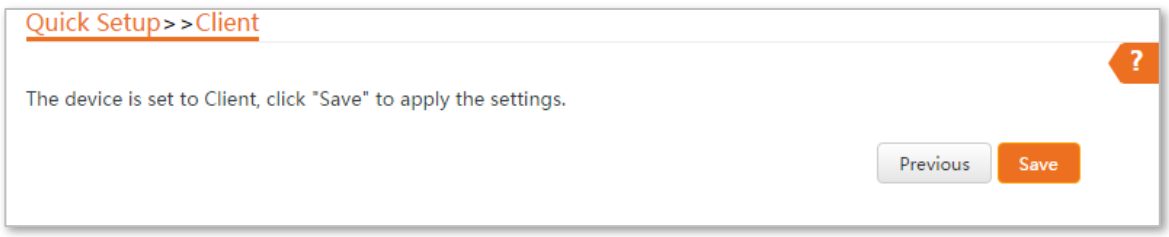
4. Enter the WiFi password you set on CPE1 in the **Key** text box, and click **Next**.




5. Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of CPE1 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**.




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




**----End**

When LED1, LED2, and LED3 of CPE1 are solid on, and LED1, LED2, and LED3 of CPE2 are blinking, the bridging succeeds.

TIP

You can check the SSID and key of CPE2 by choosing **Wireless** > **Basic** after logging in to the web UI.

## Verification

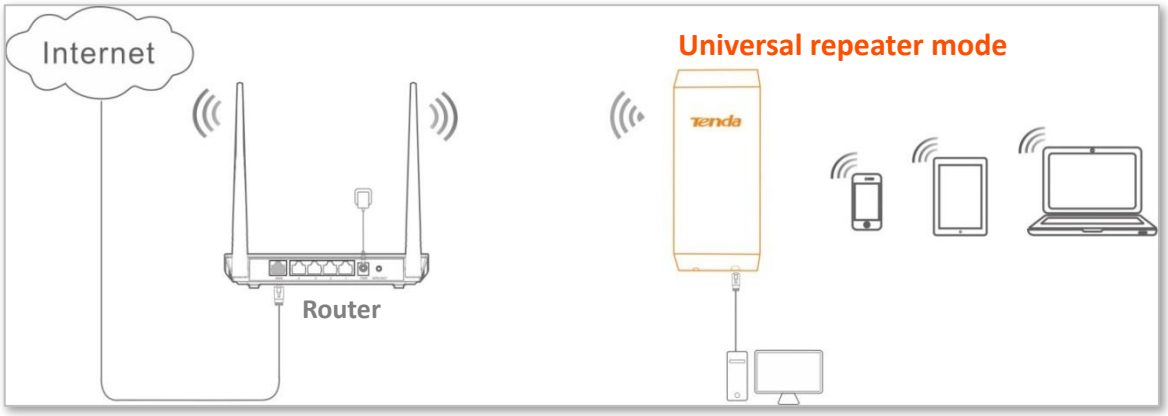
Surveillance videos can be seen on the computer in the side of CPE1.

# 2.4 Universal repeater mode

In Universal Repeater mode, this 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.

**Application scenario**

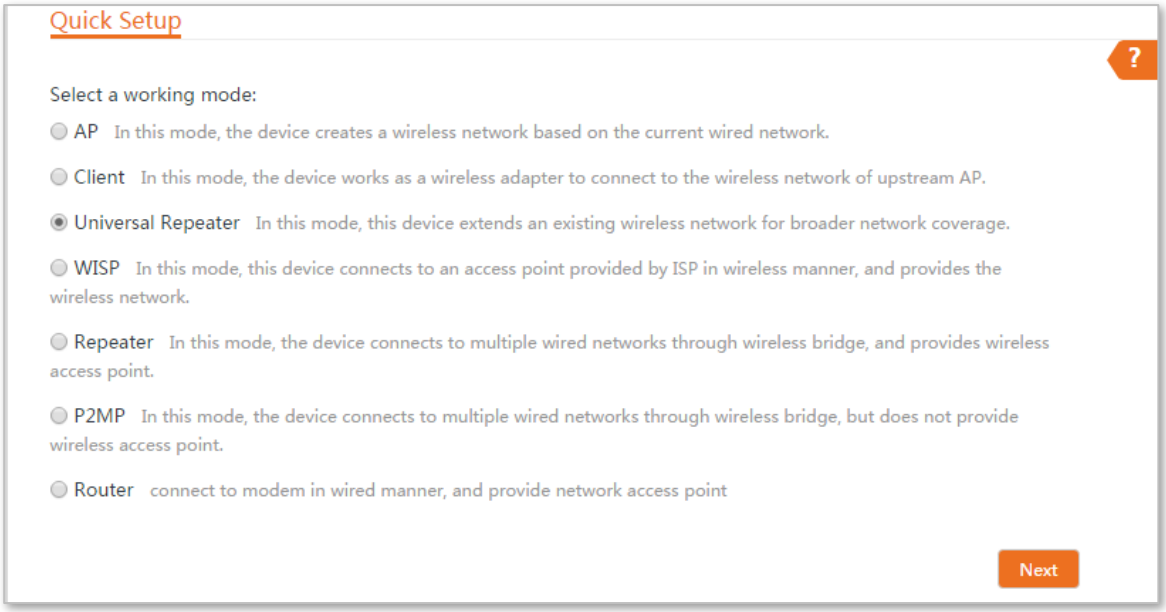
**Network requirement**: You want to use the CPE to extend your existing wireless network. And your existing router does not support WDS mode.



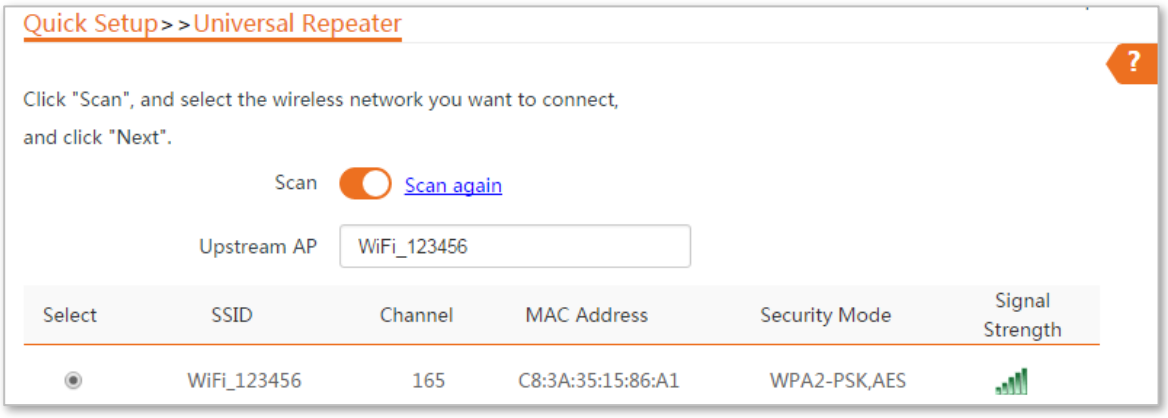

**Configuration procedure of setting Universal Repeater mode**

**Step 1** Log in to the web UI of the CPE and choose **Quick Setup** to enter the configuration page.

**Step 2** Select **Universal Repeater**, and click **Next**.



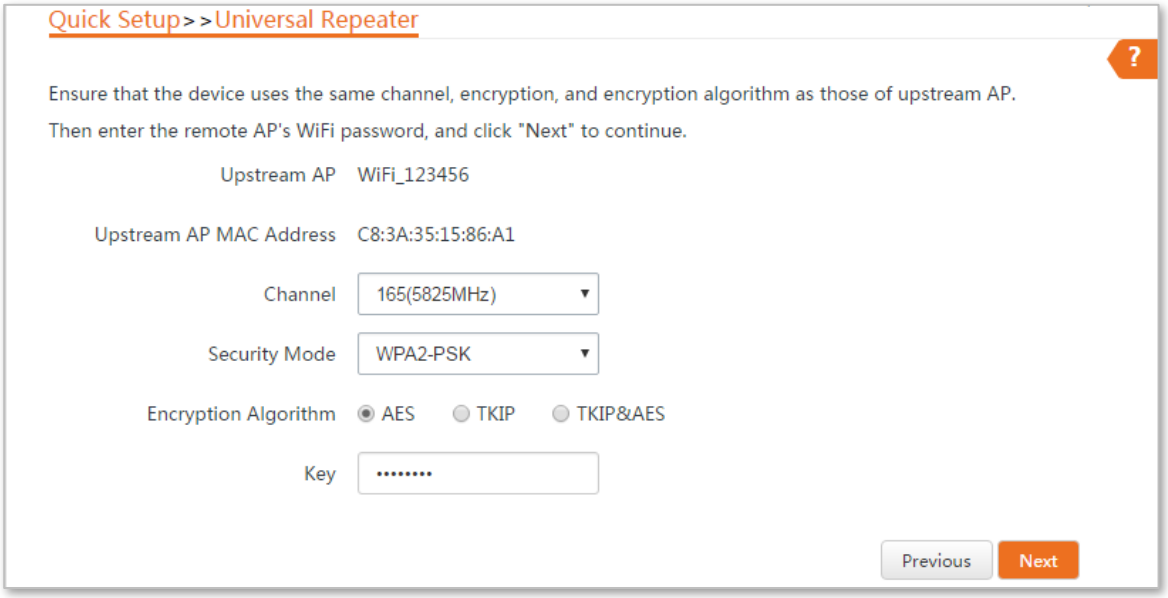
**Step 3** Select the SSID of the router and click **Next**.



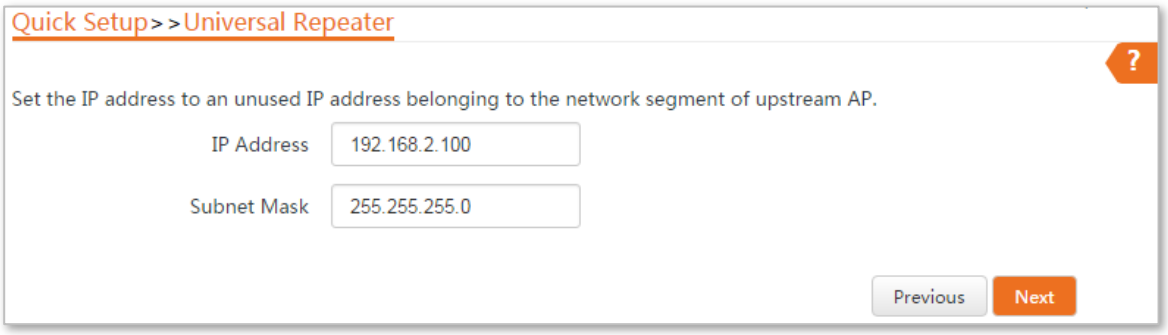

TIP

If you cannot find the SSID of the router from the list, ensure that the 5 GHz WiFi network of the router is enabled. Only the WiFi networks at 5 GHz band will be displayed in the list.

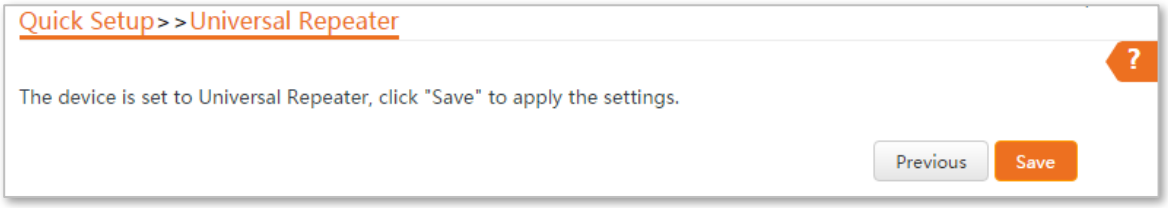
**Step 4** Enter the WiFi password of the router in the **Key** text box, and click **Next**.



**Step 5** Set the IP address to an unused IP address belonging to the same network segment as that of the router. 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**.




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




**----End**

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 CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1

### Parameters description

| Name | Description |
|---|---|
| Working modes | It specifies the working mode of this device.<br>**Universal Repeater mode**: in this mode, the device expands your WiFi network for broader network coverage.<br>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 wireless network name (SSID) 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. |

# Example of universal repeater mode

## Network requirement

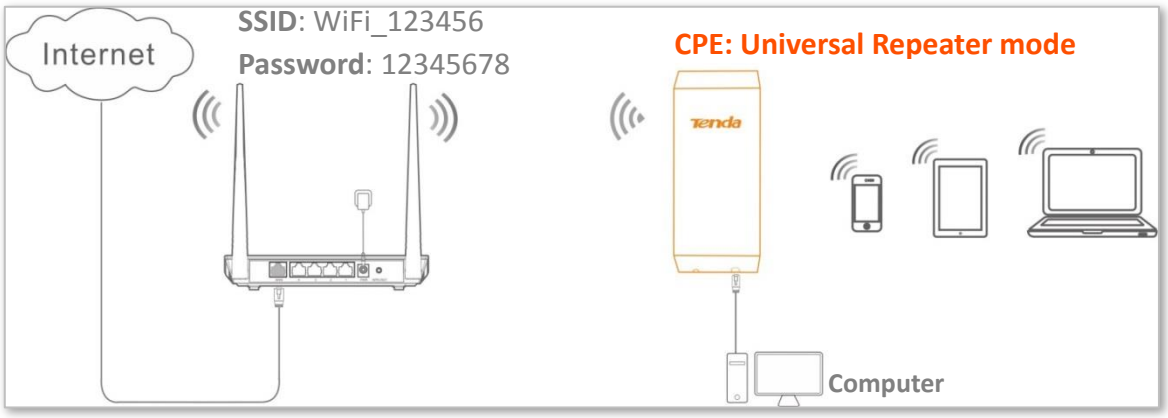
You are in a WiFi dead zone or a place with weak wireless signal, and have a wireless router that does not support WDS function. Now you want to have a larger WiFi network coverage through your home or office.

## Solution

Set the CPE to **Universal Repeater** mode, and extend the WiFi network of the router.
Assume that the SSID and password of the router are shown as follows:

- **SSID**: WiFi_123456
- **Password**: 12345678

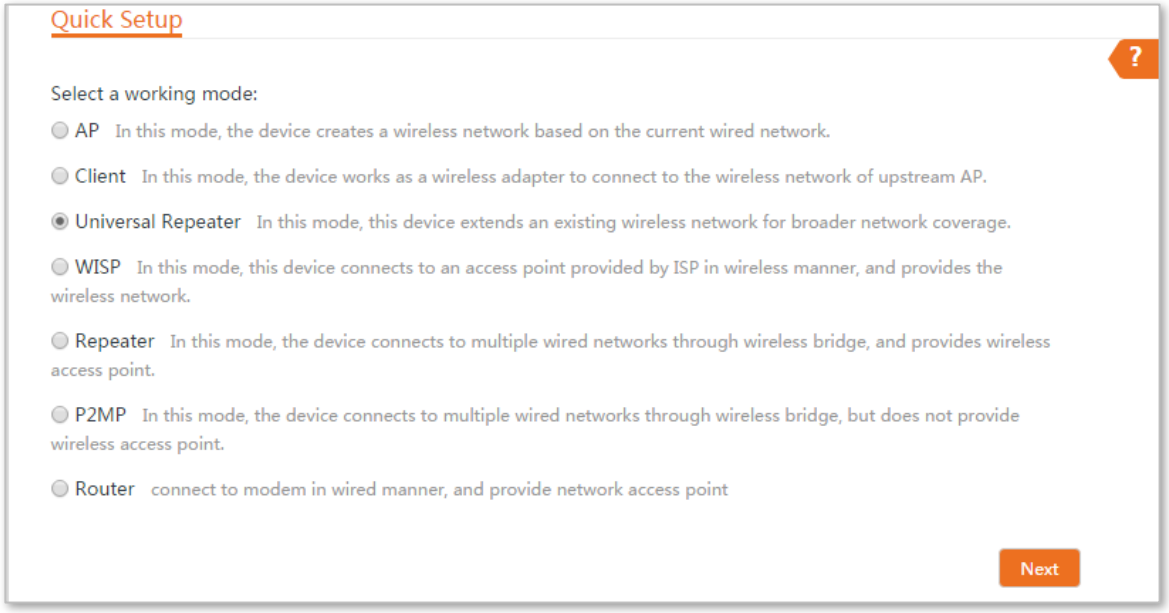
## Network topology



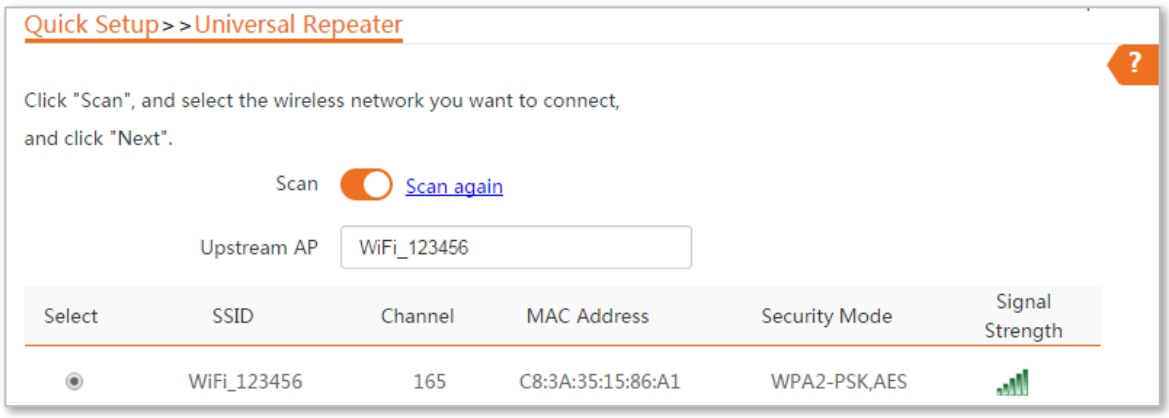
## Configuration procedure

**Step 1** Log in to the web UI of the CPE and choose **Quick Setup** to enter the configuration page.

**Step 2** Select **Universal Repeater**, and click **Next**.



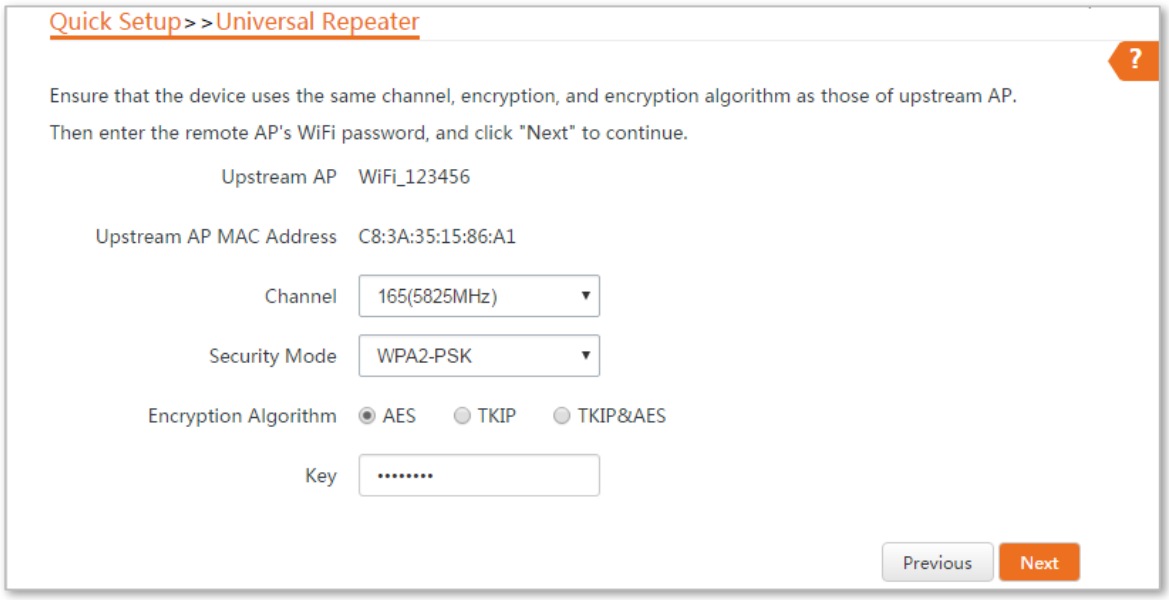

**Step 3** Select the SSID of the router, which is **WiFi_123456** in this example, and click **Next**.



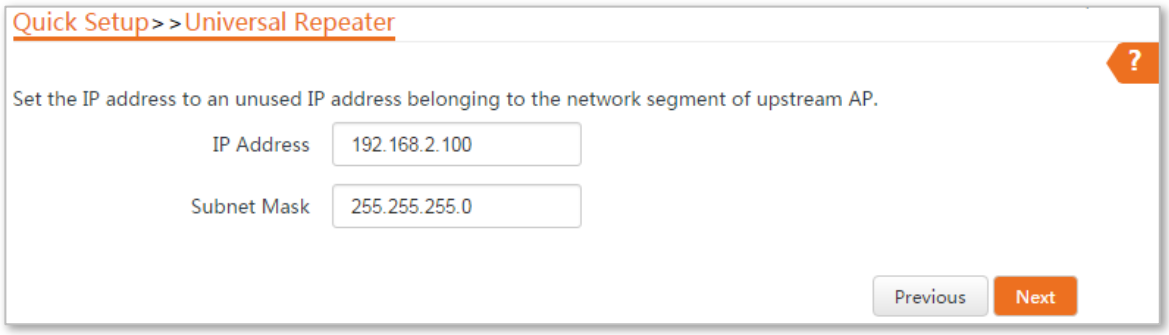

TIP

If you cannot find the SSID of the router from the list, ensure that the 5 GHz WiFi network of the router is enabled. Only the WiFi networks at 5 GHz band will be displayed in the list.

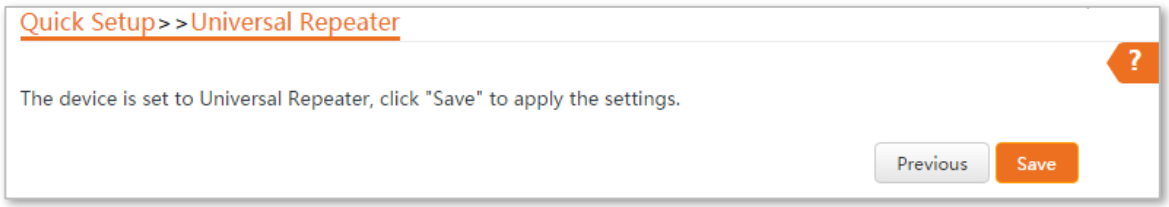
**Step 4** Enter the WiFi password of the router in the **Key** text box, and click **Next**.




**Step 5** Set the IP address to an unused IP address belonging to the same network segment as that of the router. 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**.




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




**----End**

TIP

You can check the SSID and key of the CPE by choosing **Wireless** > **Basic** after logging in to the web UI.

### Verification

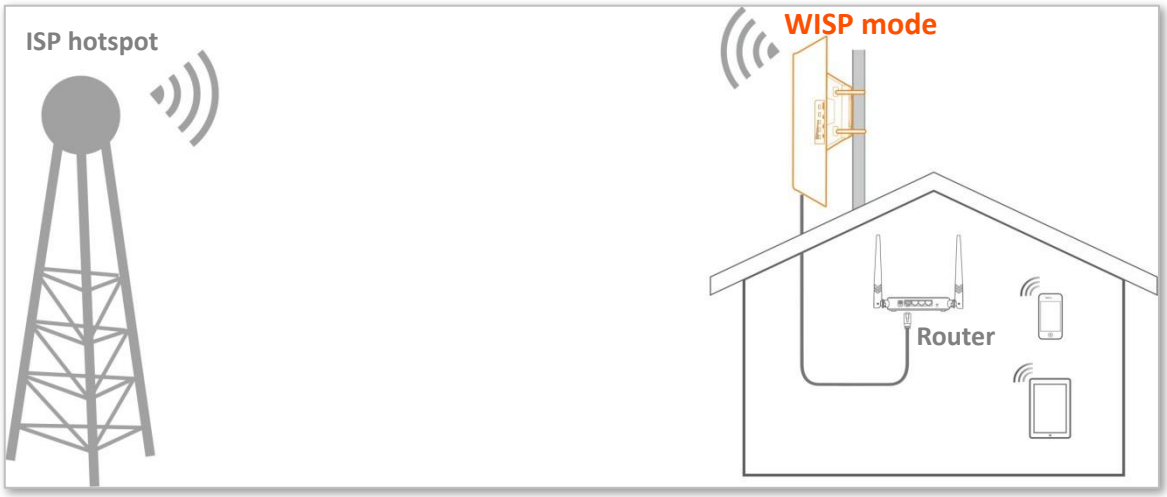
Your wireless devices can search the SSID of the CPE, and connect to its wireless network for internet access.

## 2.5 WISP mode

In WISP mode, this device connects to an access point provided by ISP in wireless manner, and allowed the wireless devices to connect to the internet.

### Application scenario

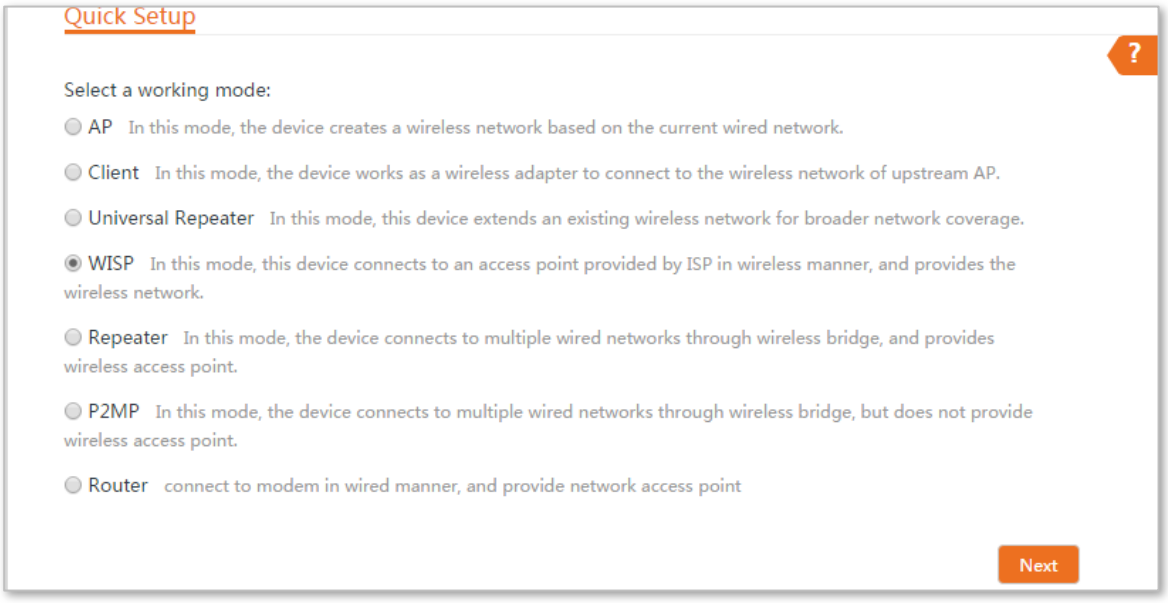
**Network requirement**: You want to use the CPE to extend the ISP hotspot to your home.



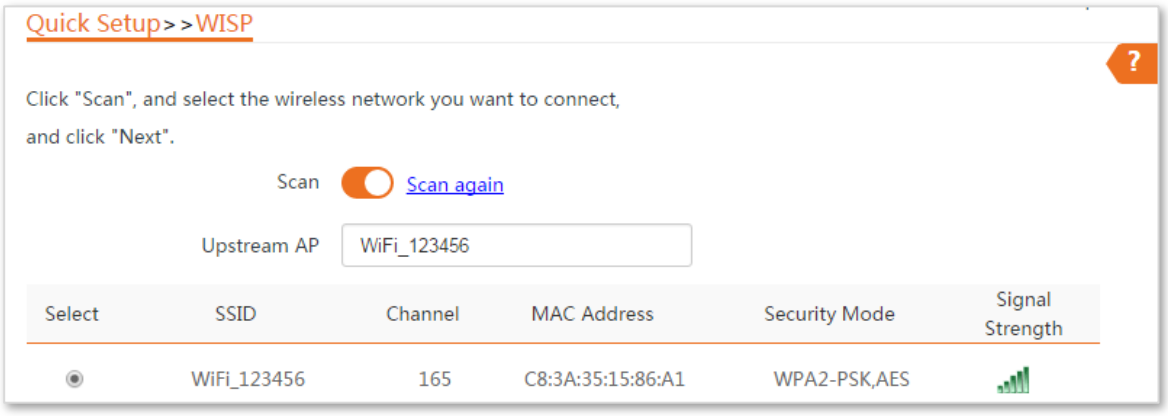

### Configuration procedure of setting WISP mode

**Step 1** Log in to the web UI of this CPE and choose **Quick Setup** to enter the configuration page.

**Step 2** Select **WISP**, and click **Next**.



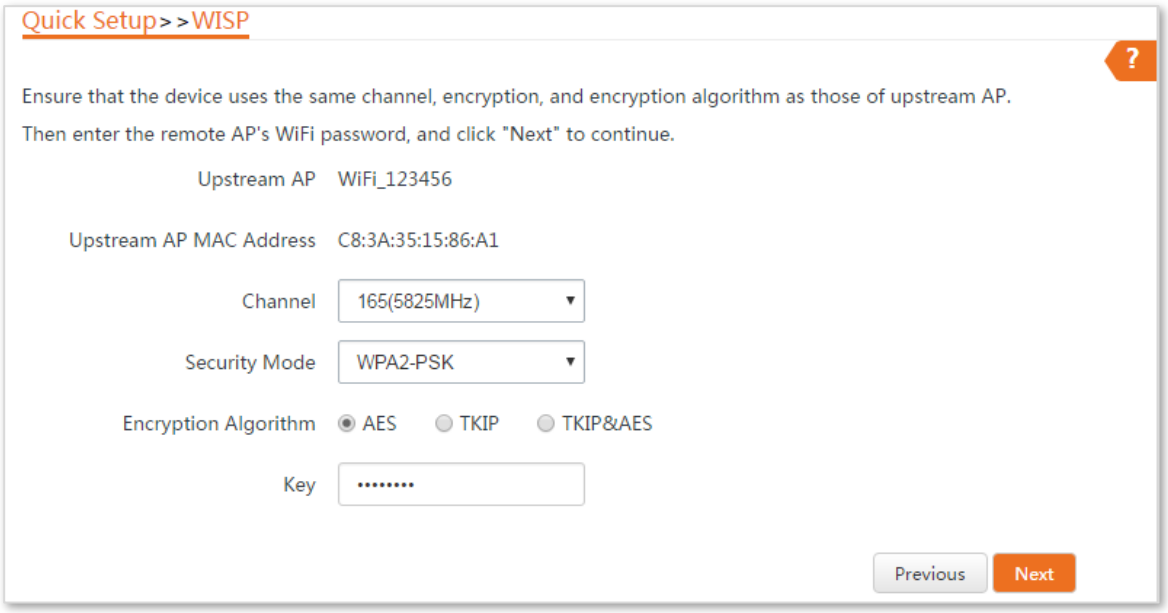
**Step 3** Select the SSID of your ISP (Internet Service Provider) hotspot and click **Next**.



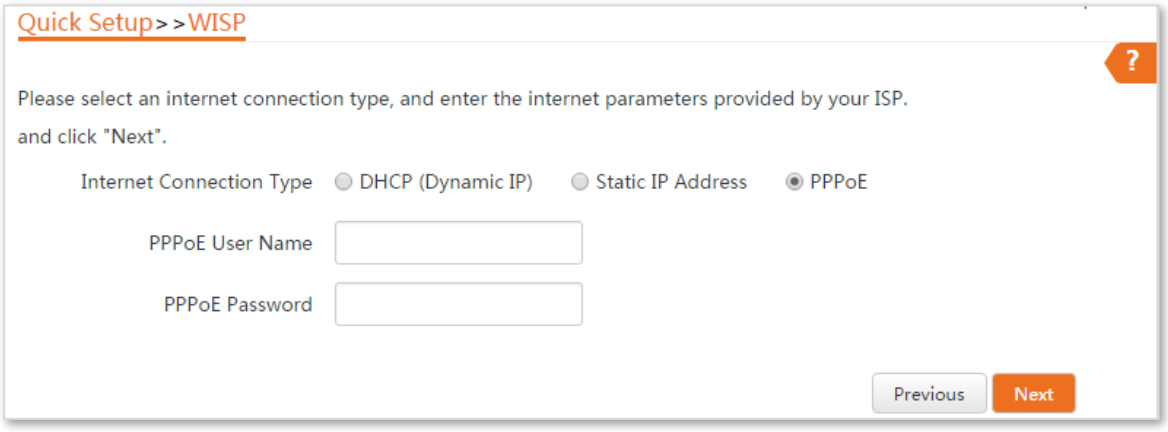

TIP

If you cannot find the ISP hotspot from the list, ensure that the hotspot is at 5 GHz. Only the WiFi networks at 5 GHz band will be displayed in the list.

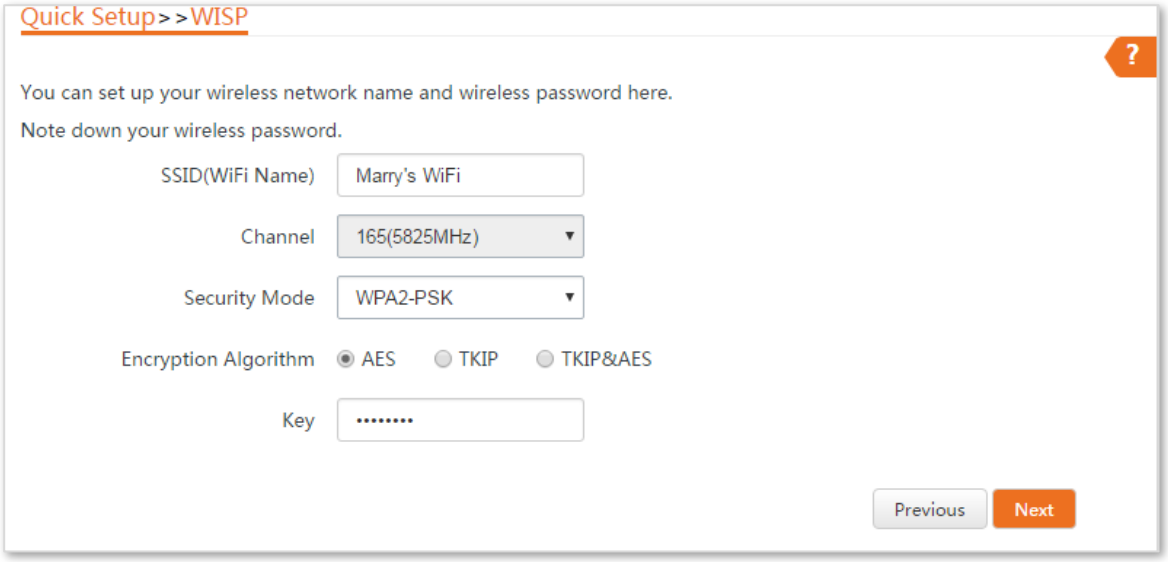
**Step 4** Enter the WiFi password of your ISP hotspot in the **Key** text box, and click **Next**.



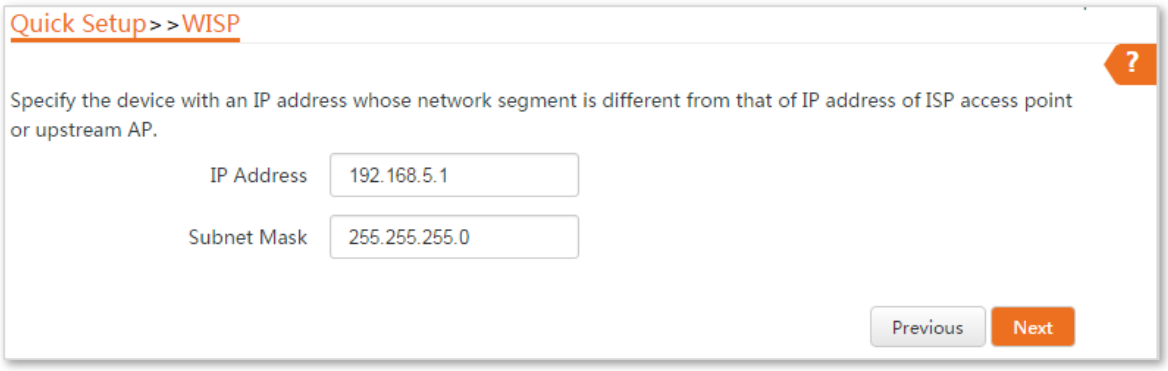
**Step 5** Select the **Internet Connection Type** of your ISP hotspot, which is **PPPoE** in this example. Enter the PPPoE user name and password provided by your ISP, and click **Next**.



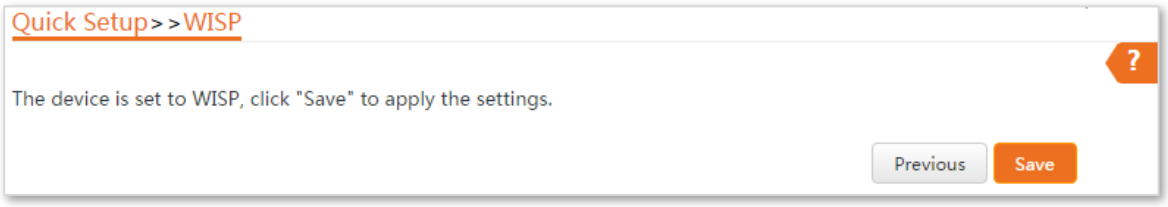

**Step 6** Customize the SSID and key, and click **Next**.




**Step 7** Set an IP address belonging to different network segment as 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 excluding2) which is also the login IP address of the CPE. Then click **Next**.



**Step 8** Click **Save**, and wait until the device reboots to activate the settings.




**----End**

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

TIP

You can check the SSID and key of the CPE by choosing **Wireless** > **Basic** after logging in to the web UI.

**Parameters description**

| Name | Description |
|---|---|
| Working modes | It specifies the working mode of this device.<br>**WISP mode**: in this mode, the device connects to an access point provided by ISP in wireless manner. |
| Upstream AP | It specifies the wireless network name (SSID) 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. |
| Internet Connection Type | **DHCP (Dynamic IP)**: The device obtains IP address and other parameters form the DHCP server of upstream device for internet access.<br>**Static IP Address**: The device access the internet by setting the IP address, subnet mask, default gateway and DNS server IP addresses manually.<br>**PPPoE**: The device access the internet using the PPPoE user name and password provided by the ISP. |

# Example of WISP mode

## Network requirement

You live in countryside, and it is not convenient for you to connect the nearest ISP base station using Ethernet cables. So you want to extend the ISP hotspot to your home in wireless manner.

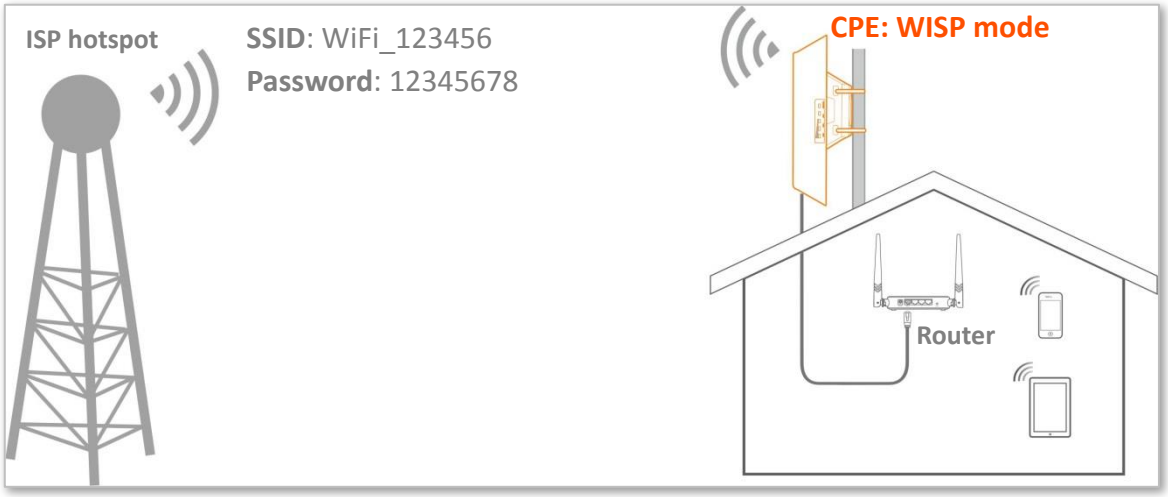
## Solution

Set the CPE to WISP mode, and bridge to the ISP hotspot.

Assume that the SSID and password of the ISP hotspot are:

- SSID: WiFi_123456
- Password: 12345678

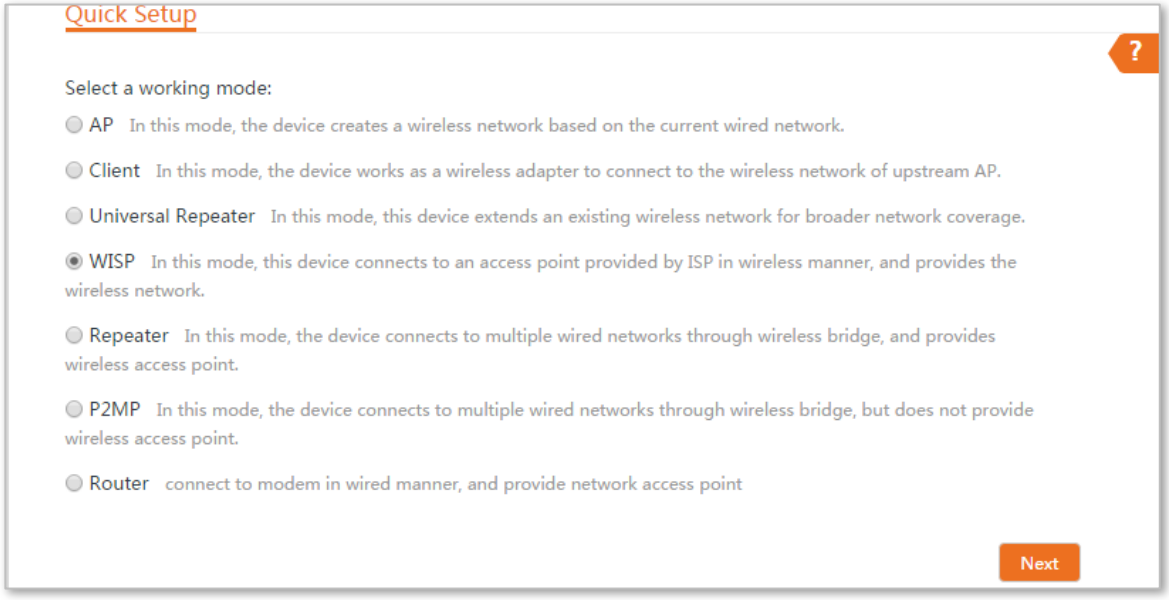
## Network topology



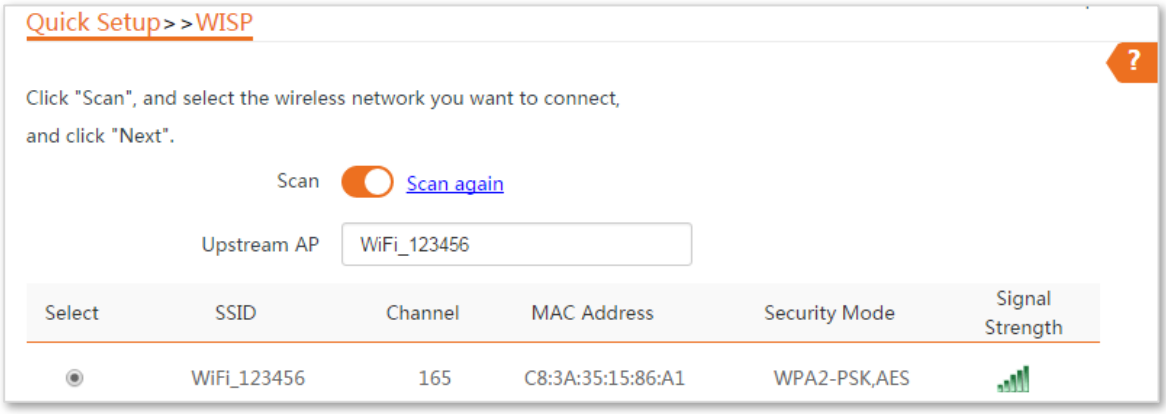
## Configuration procedure

**Step 1** Log in to the web UI of this CPE and choose **Quick Setup** to enter the configuration page.

**Step 2** Select **WISP**, and click **Next**.



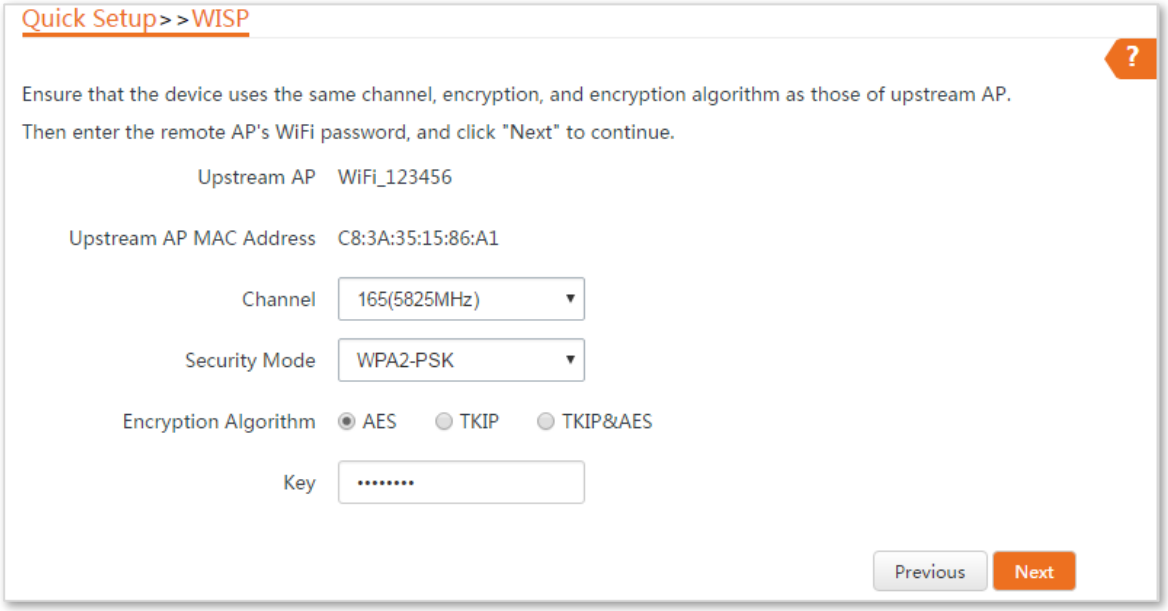

**Step 3** Select the SSID of your ISP (Internet Service Provider) hotspot, which is **WiFi_123456** in this example, and click **Next**.



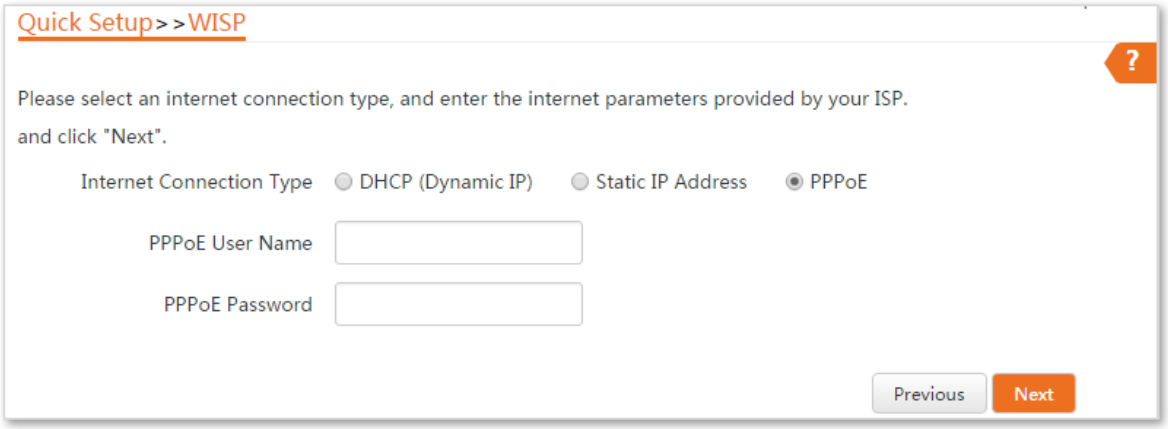

TIP

If you cannot find the ISP hotspot from the list, ensure that the hotspot is at 5 GHz. Only the WiFi networks at 5 GHz band will be displayed in the list.

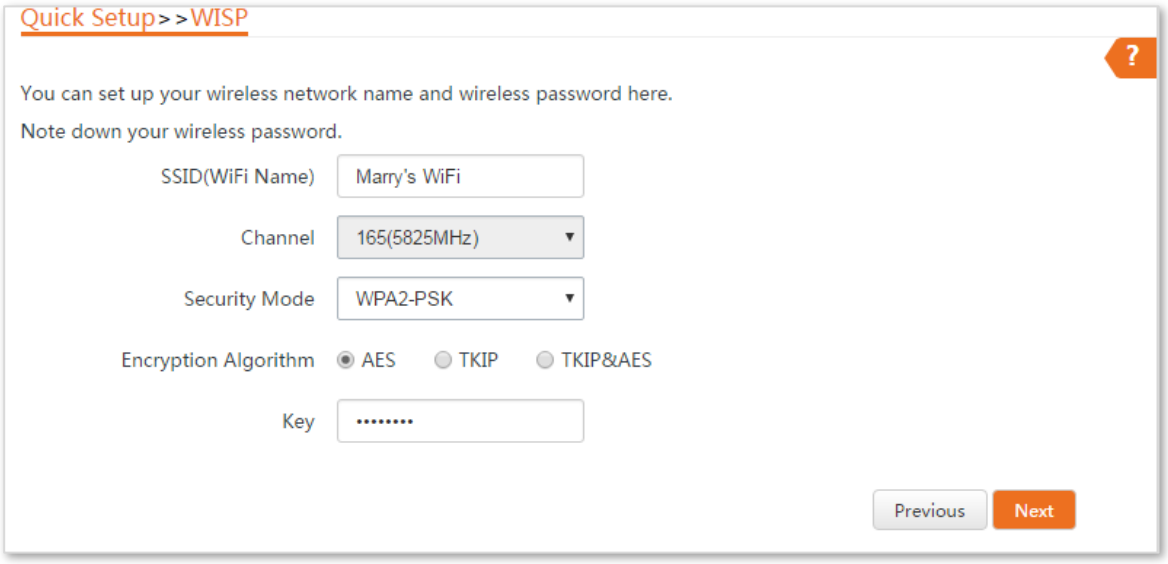
**Step 4** Enter the WiFi password of your ISP hotspot in the **Key** text box, and click **Next**.



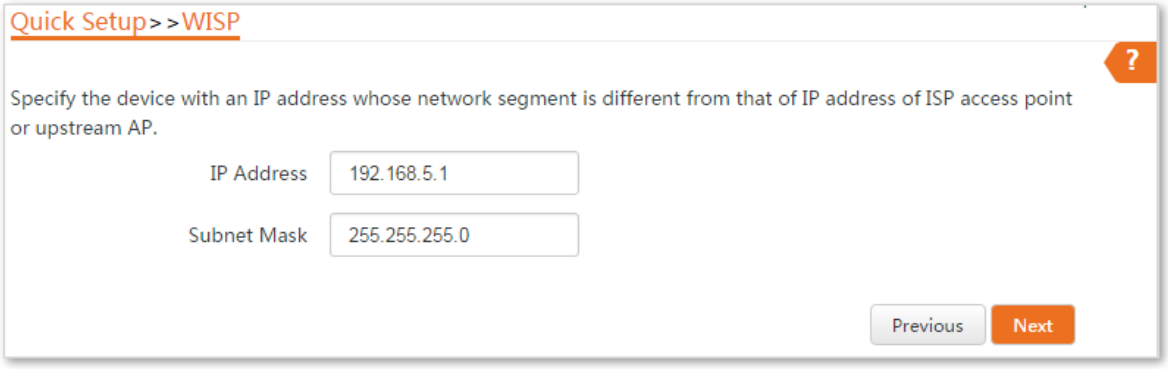

**Step 5** Select the **Internet Connection Type** of your ISP hotspot, which is **PPPoE** in this example. Enter the PPPoE user name and password provided by your ISP, and click **Next**.



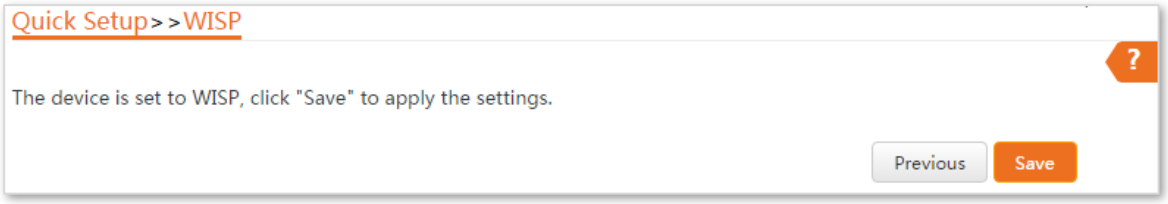
**Step 6** Customize the SSID and key, and click **Next**.




**Step 7** Set an IP address belonging to different network segment as 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 excluding2) which is also the login IP address of the CPE. Then click **Next**.




**Step 8** Click **Save**, and wait until the device reboots to activate the settings.




**----End**

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

TIP

You can check the SSID and key of the CPE by choosing **Wireless** > **Basic** after logging in to the web UI.

## Verification

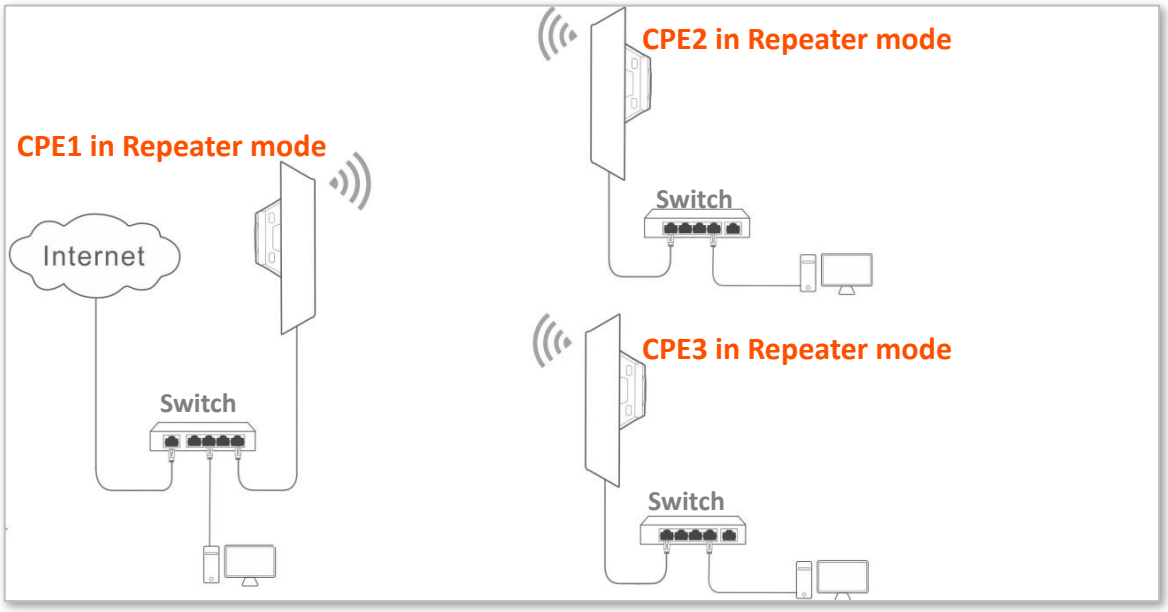
Your wired and wireless devices can connect your router which is connected to the CPE for internet access.

# 2.6 Repeater mode

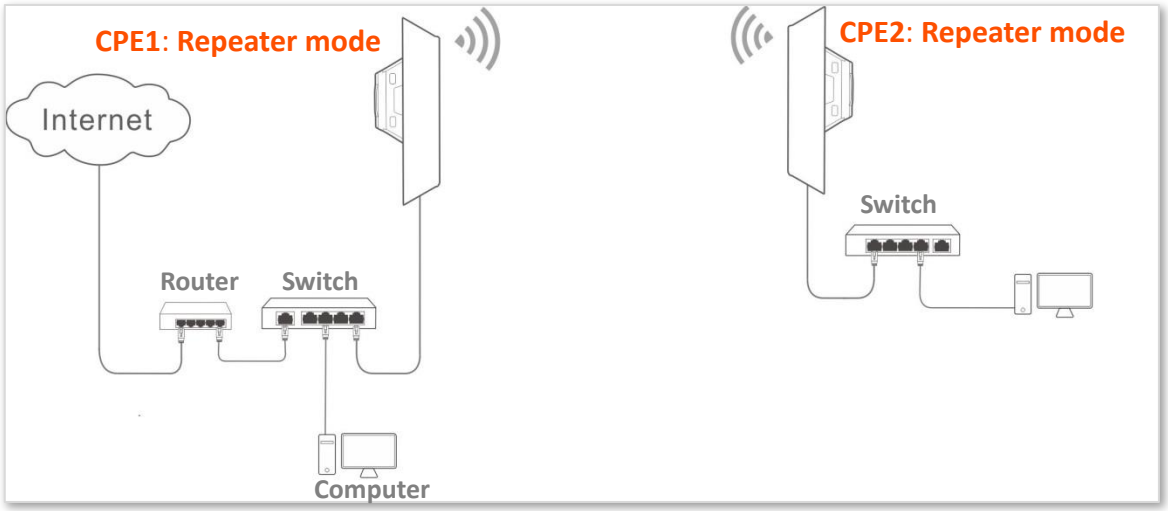
In Repeater mode, this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use this function, the peer AP is required to support WDS function.

**Application scenario**

**Network requirement**: You want to combine multiple wired networks into one in wireless manner.




## Configuration procedure of one to one bridging

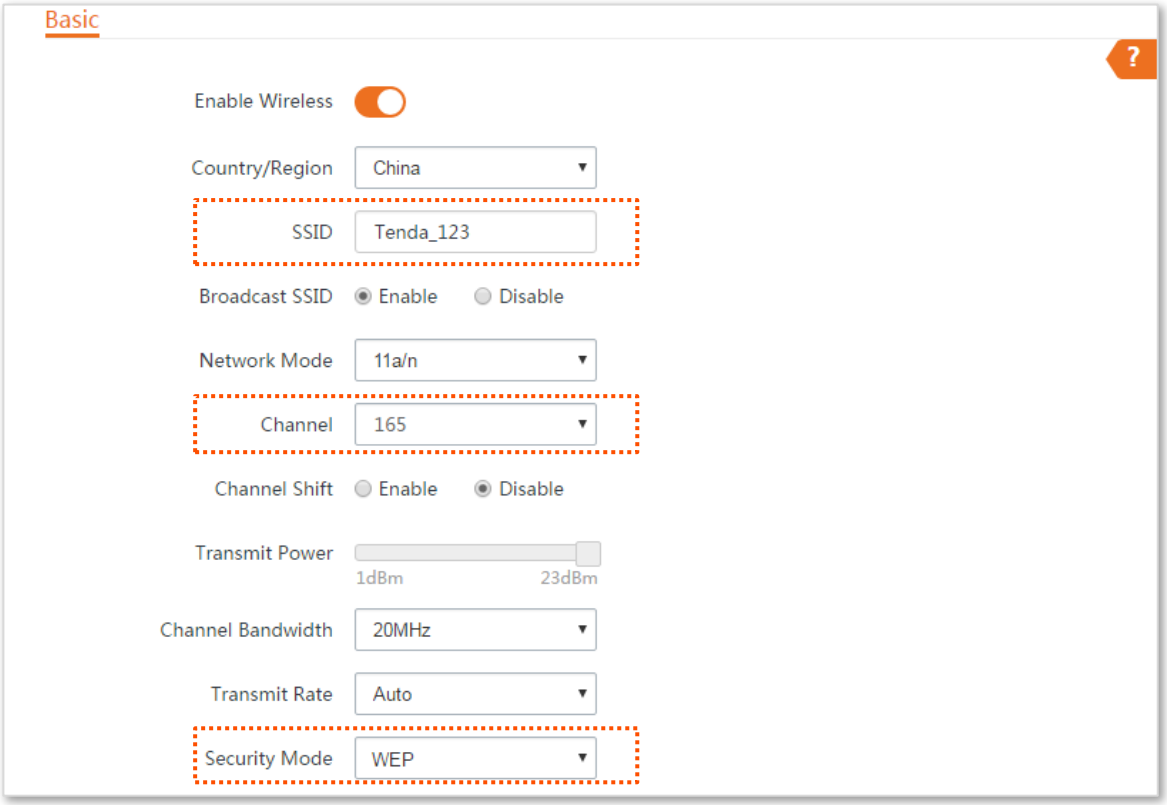



Assume that the wireless parameters of CPE1 are as follows:

- **SSID**: Tenda_123456
- **Channel**: 165
- **Security mode**: WEP
- **Authentication type**: Shared
- **Key1 to key4**: 12345

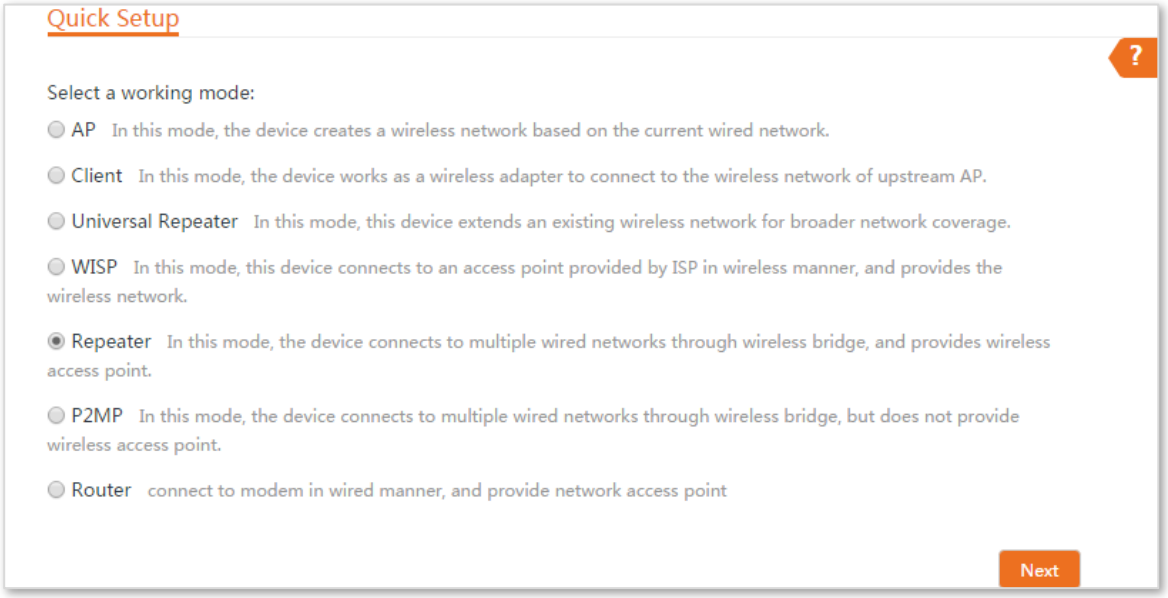
**Step 1** Configure the wireless settings of CPE2.

1. Log in to the web UI of CPE2, and choose **Wireless > Basic** to enter the configuration page.
2. Change the SSID, which is **Tenda_123** in this example.
3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
4. Set the **Security Mode** to the same as that of CPE1, which is **WEP** in this example.
5. Click **Save** to apply the settings.

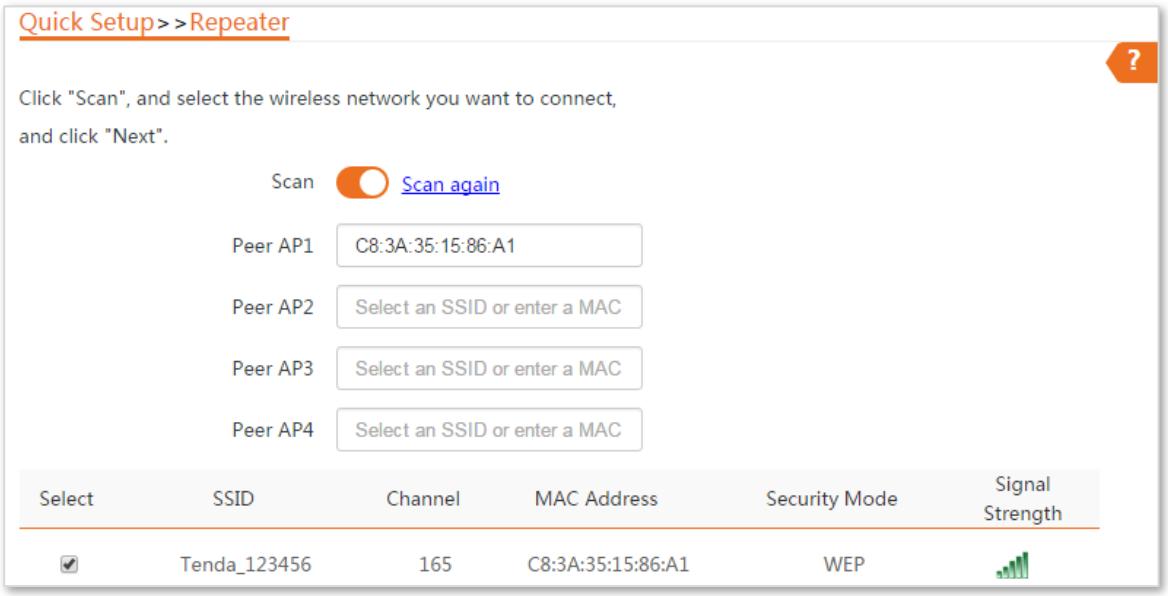



**Step 2** Set **CPE2** to the **Repeater** mode.

1. Log in to the web UI of CPE2 and choose **Quick Setup** to enter the configuration page.
2. Select the SSID of CPE1, which is **Tenda_123456** in this example, and click **Next**.



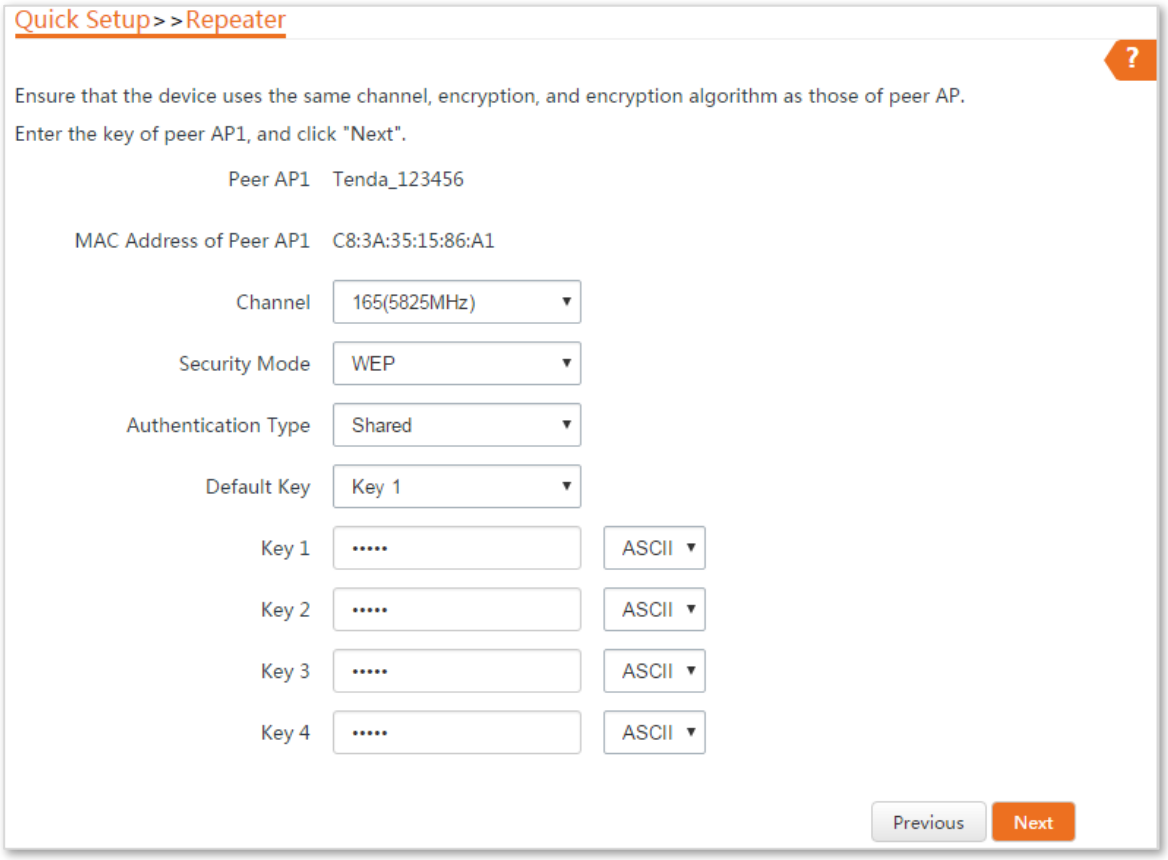

3. Select the SSID of CPE1 from the list and click **Next**.



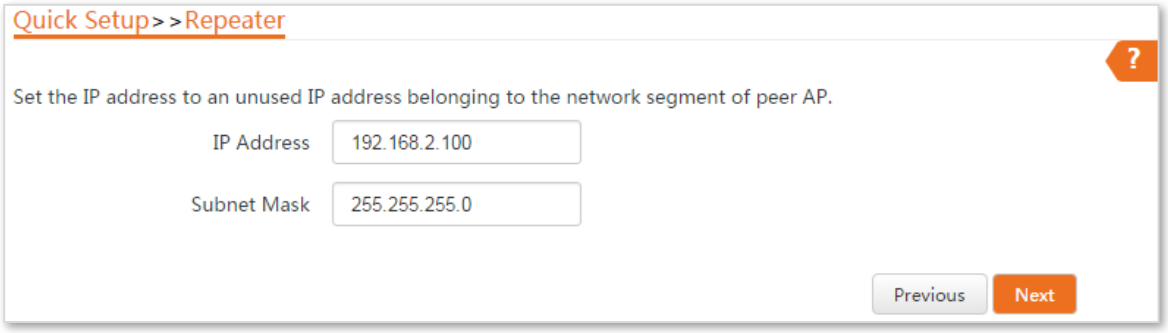

TIP

Only the WiFi networks which are not encrypted or encrypted using the WEP mode can be found on the list.

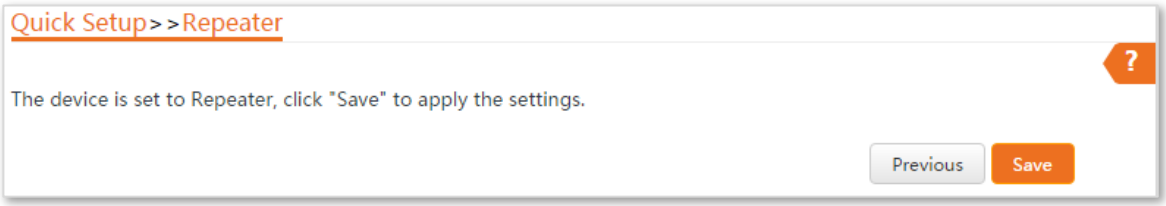
4. Set the **Authentication Type** and **Default Key** to the same as those of CPE1, enter the key 1, key2, key 3 and key4, and click **Next**.




5. Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of CPE1 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**.




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



**Step 3** Perform the procedure in Step 2 above to set **CPE1** to the **Repeater** mode.

**----End**

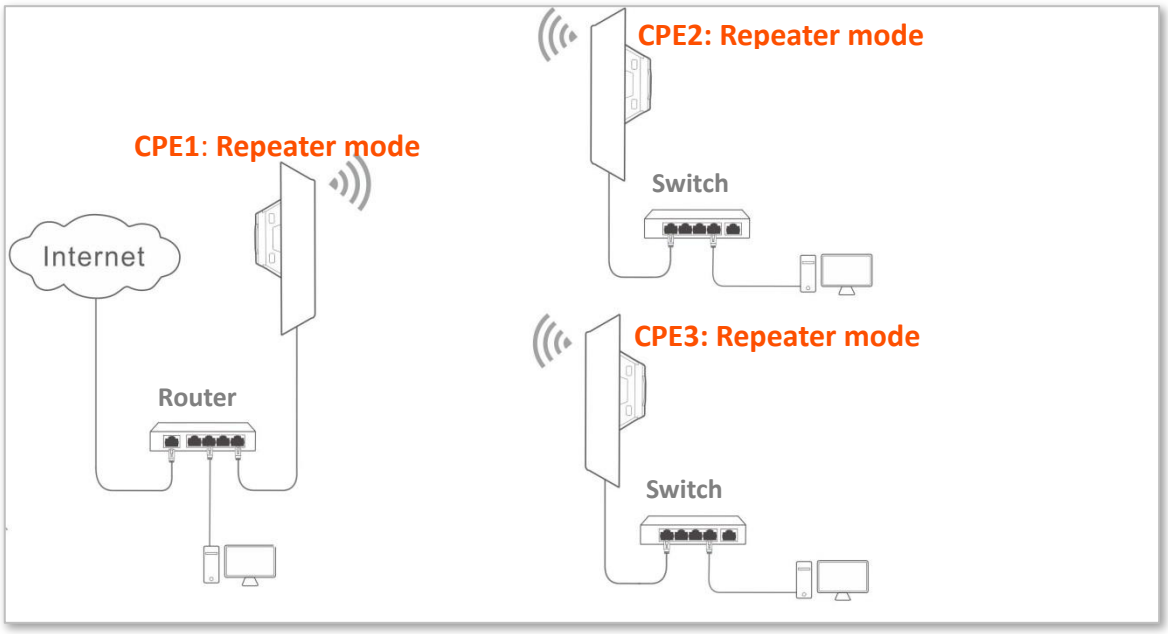
TIP

You can check the SSID and key of the CPE by choosing **Wireless** > **Basic** after logging in to the web UI.

### Parameters description

| Name | Description |
| --- | --- |
| Working modes | It specifies the working mode of this device.<br>**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 specifies the wireless network name (SSID) 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.<br>TIP<br>The Repeater mode only supports WEP and None security modes. |

## Configuration procedure of one to multiple briding

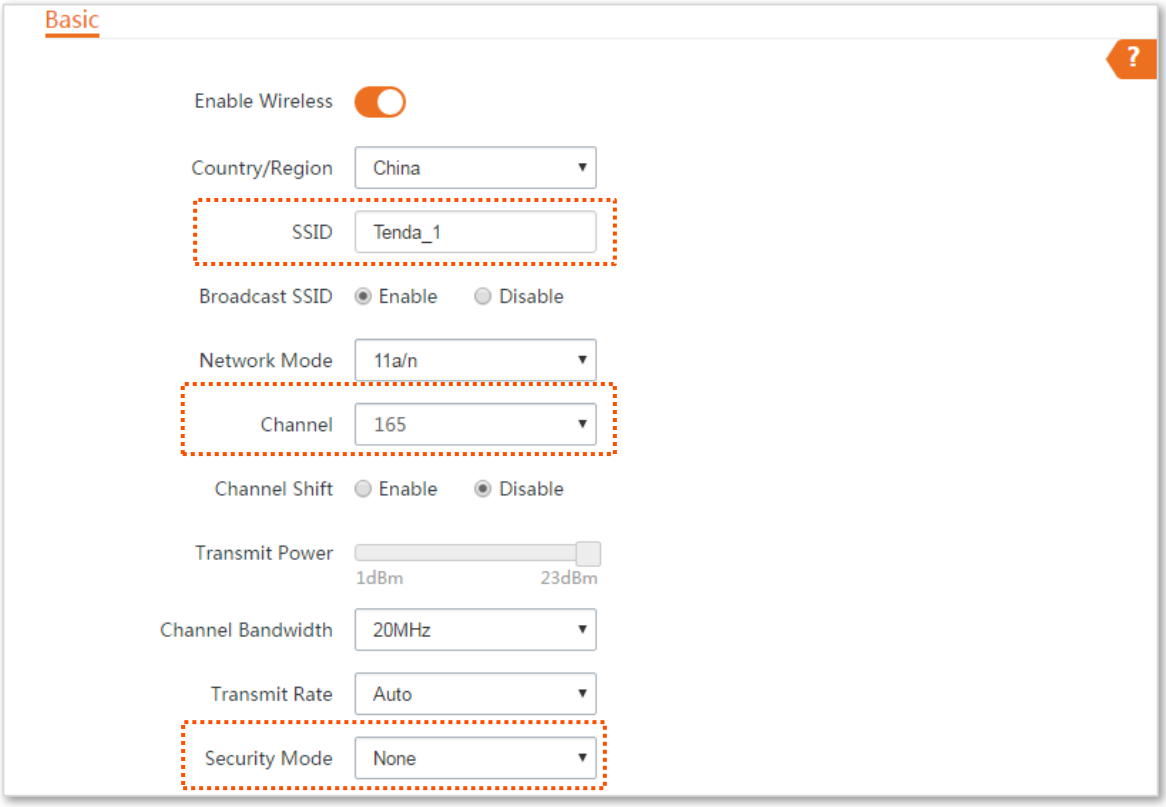



Assume that the wireless parameters of CPE1 are shown as follows:

- **IP Address**: 192.168.2.1
- **SSID**: Tenda_123456
- **Channel**: 165
- **Security mode**: None

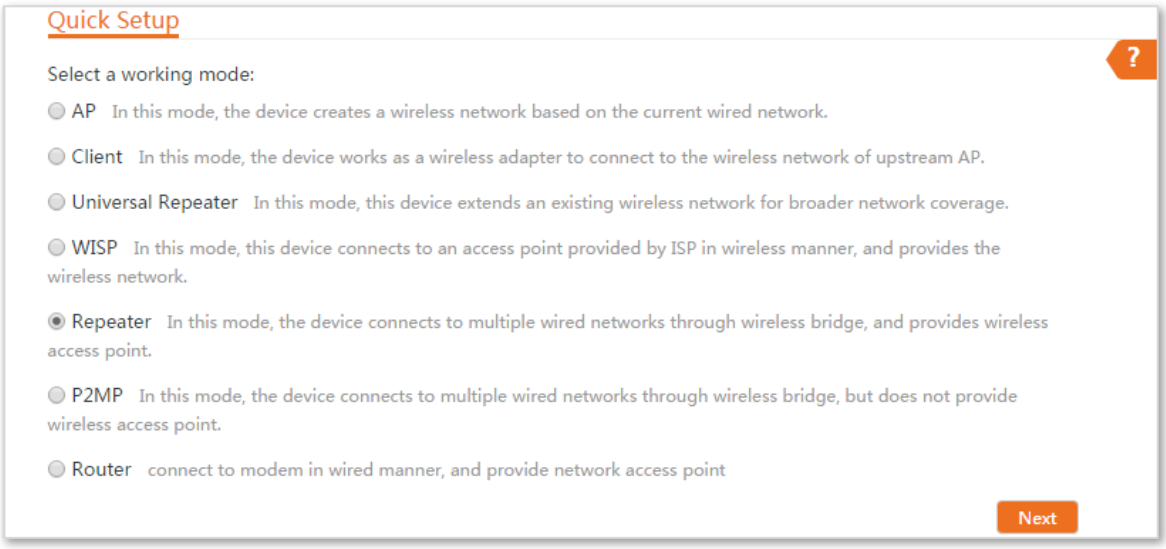
**Step 1** Configure the wireless settings of CPE2.

1. Log in to the web UI of CPE2, and choose **Wireless > Basic** to enter the configuration page.
2. Change the SSID, which is **Tenda_1** in this example.
3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
4. Set the **Security Mode** to the same as that of CPE1, which is **None** in this example.
5. Click **Save** to apply the settings.




**Step 2** Set CPE2 to the **Repeater** mode.

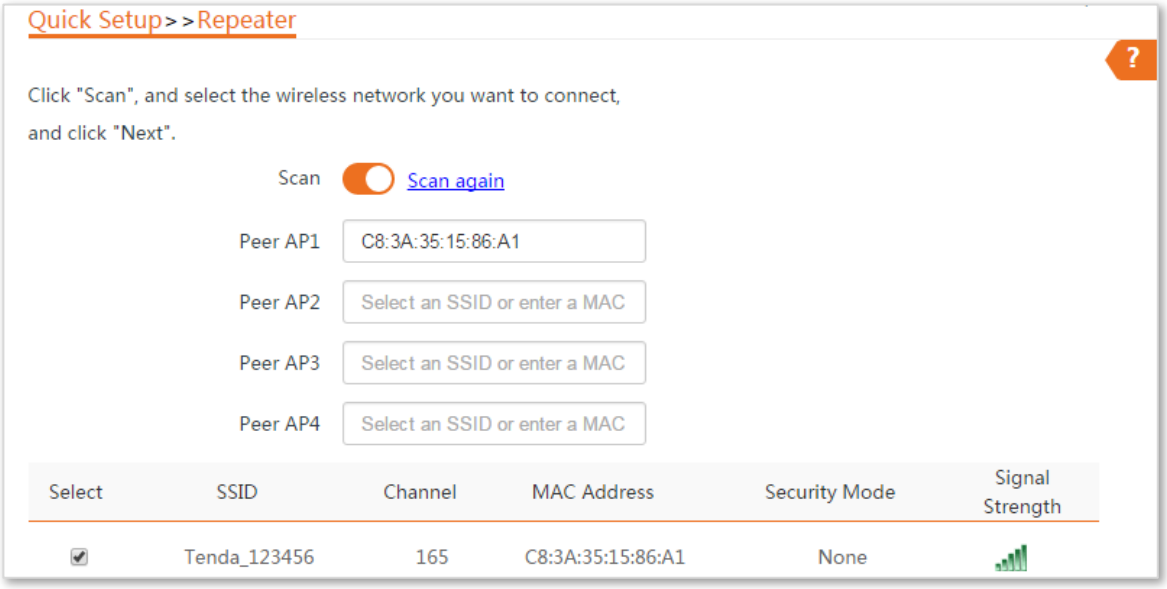
1. Choose **Quick Setup**, and select **Repeater**.



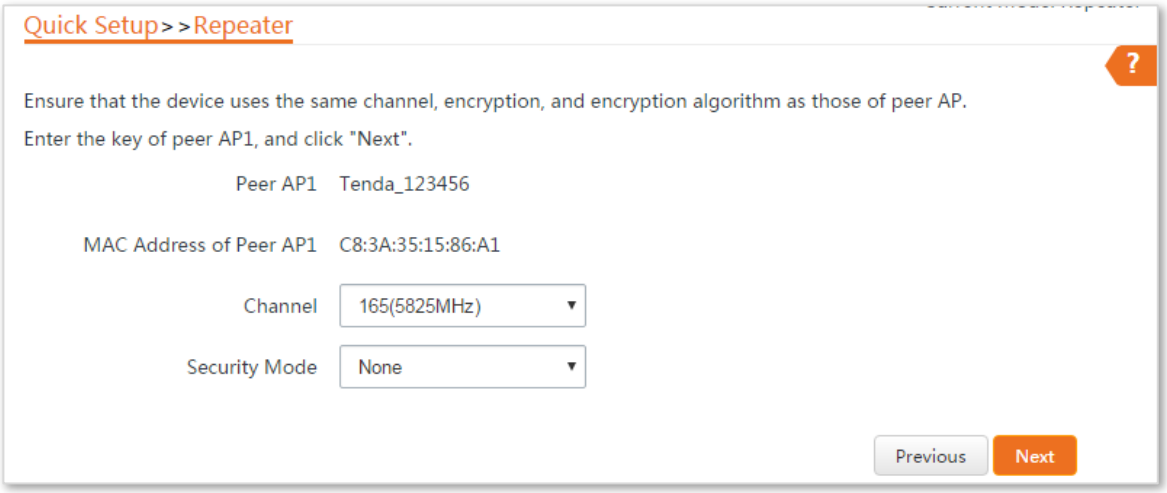

2. Select the SSID of CPE1 from the list, which is **Tenda_123456** in this example, and click **Next**.

TIP

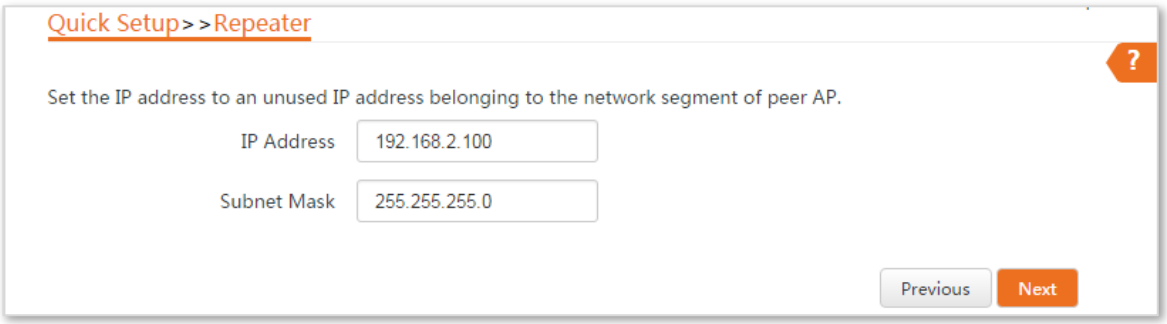
If you cannot scan the SSID of CPE1 from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.



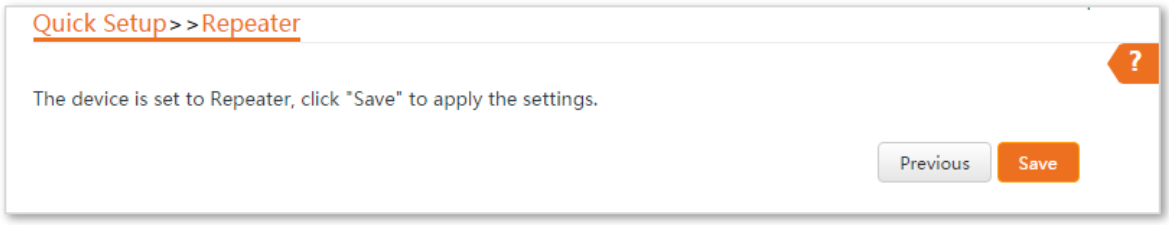

3. Click **Next** directly on the following page.




4. Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of the CPE1 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**.



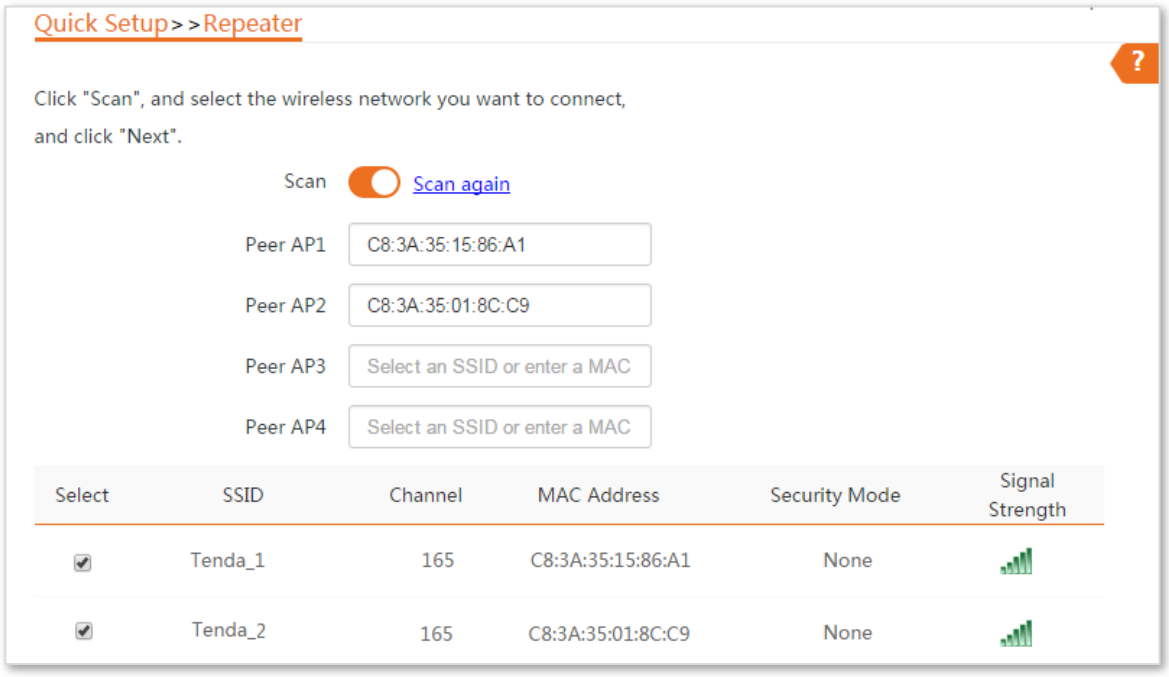
5. Click **Save**, and wait until the device reboots to activate the settings.



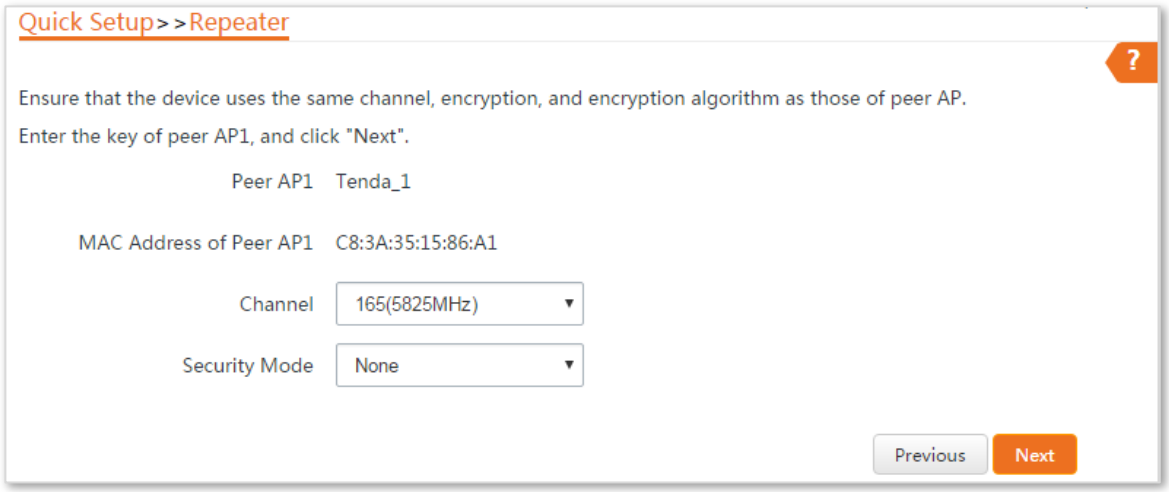

**Step 3** Perform **Step 1** and **Step 2** above to change the wireless settings of **CPE3**, whose SSID is **Tenda_2** in this example, set it to **Repeater** mode, and bridge to CPE1.

**Step 4** Set CPE1 to **Repeater** mode and bridge to CPE2 and CPE3.

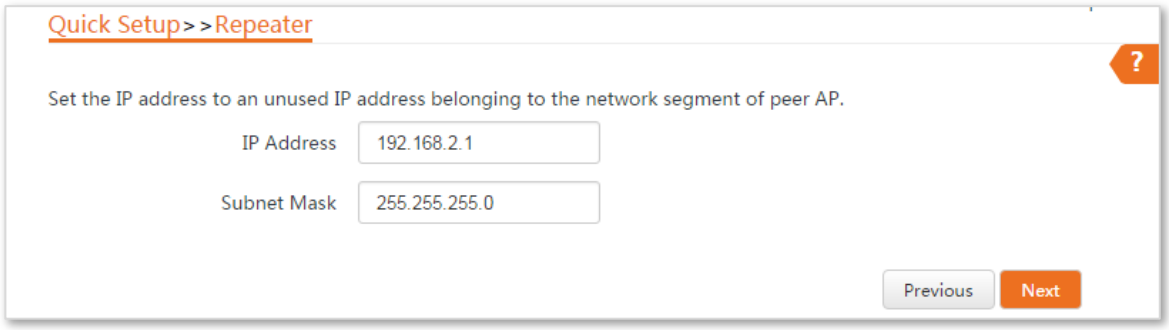
1. Log in to the web UI of CPE1, and choose Quick Setup to enter the configuration page.
2. Select **Repeater** mode, and click **Next**.
3. Select SSIDs of CPE2 and CPE3, and click **Next**.
4. Click **Next** at the bottom of the following page.



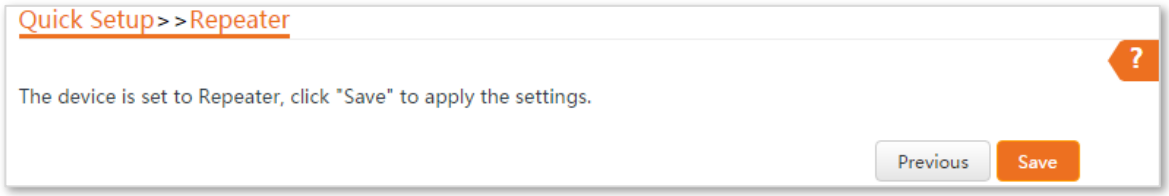
5. Click **Next** on the following page.




6. Click **Next**.




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




**----End**

# 2.7 P2MP mode

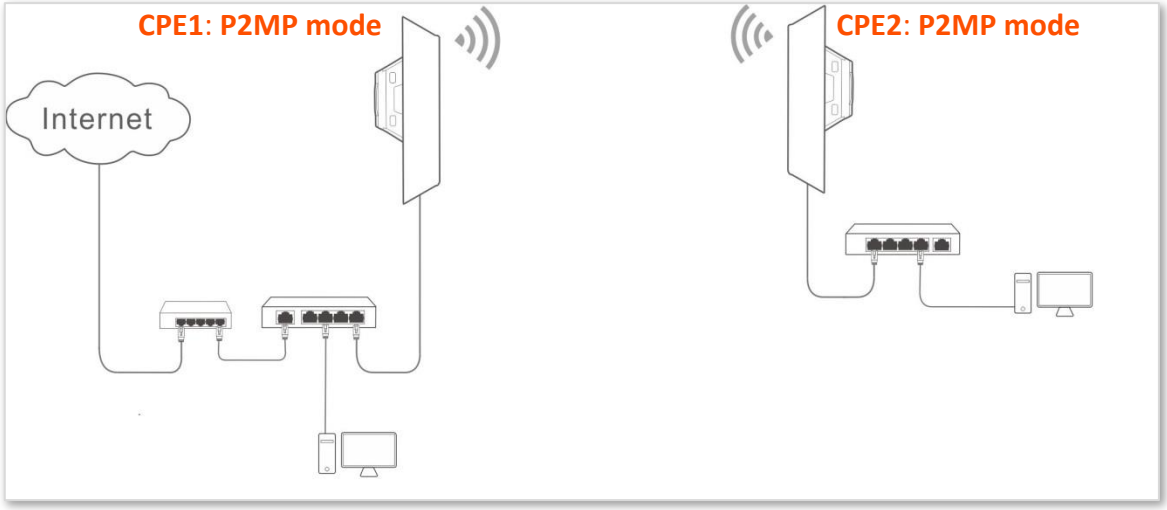
In P2MP mode, this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients.

TIP

The device in P2MP mode can work with the device in Repeater or P2MP mode.

**Application scenario**

**Network requirement**: You want to combine two local networks into one in wireless manner.



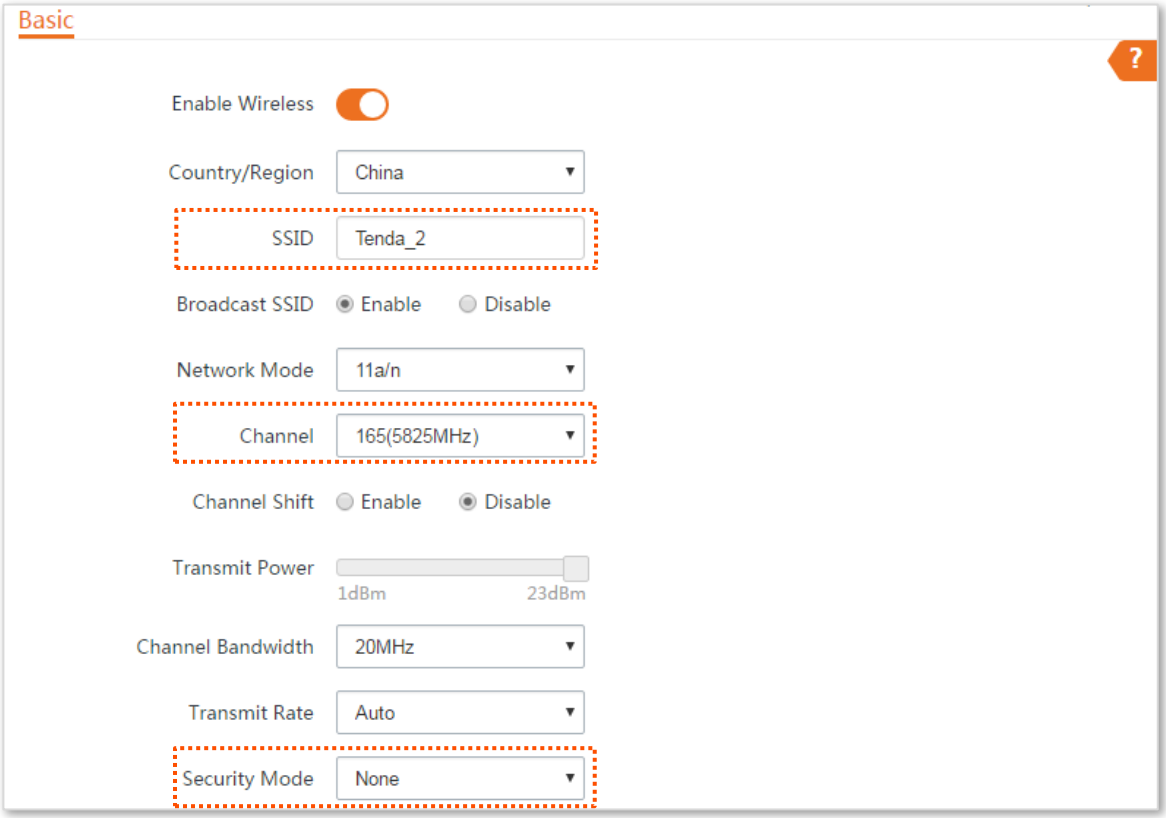

## Configuration procedure

Assume that the related parameters of CPE1 are shown as follows:

- **IP Address**: 192.168.2.1
- **SSID**: Tenda_1
- **Channel**: 165
- **Security Mode**: None

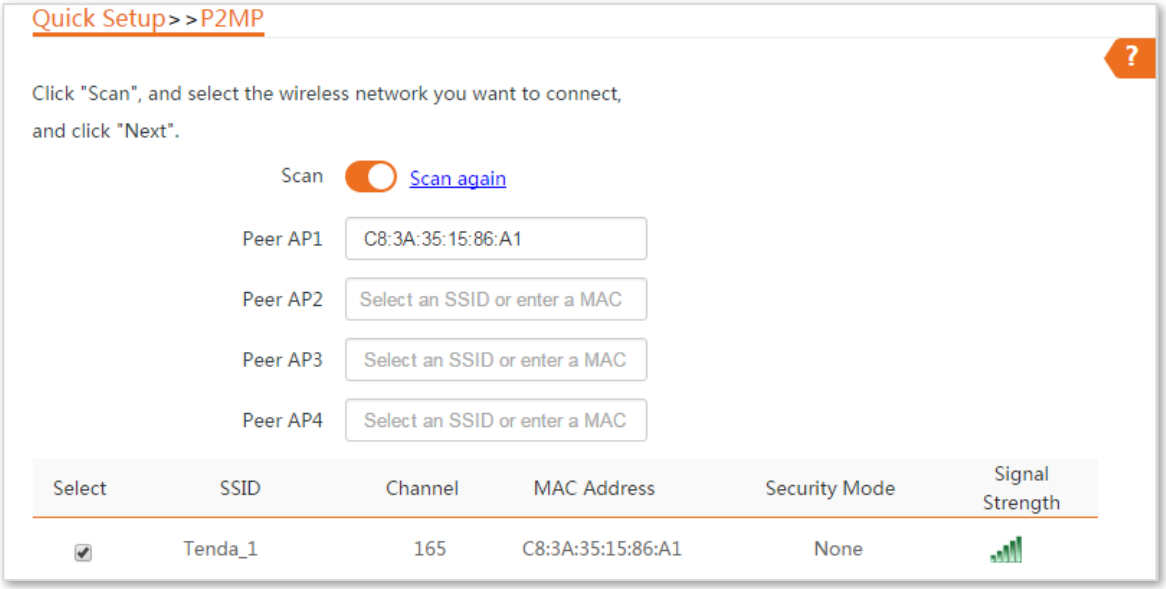
**Step 1** Change the wireless settings of CPE2.

1. Log in to the web UI of CPE2, and choose **Wireless** > **Basic** to enter the configuration page.
2. Change the **SSID**, which is **Tenda_2** in this example.
3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
4. Set the **Security mode** to the same as that of CPE1, which is **None** in this example.
5. Click **Save** to apply the settings.




**Step 2** Set CPE2 to **P2MP** mode and bridge to CPE1.

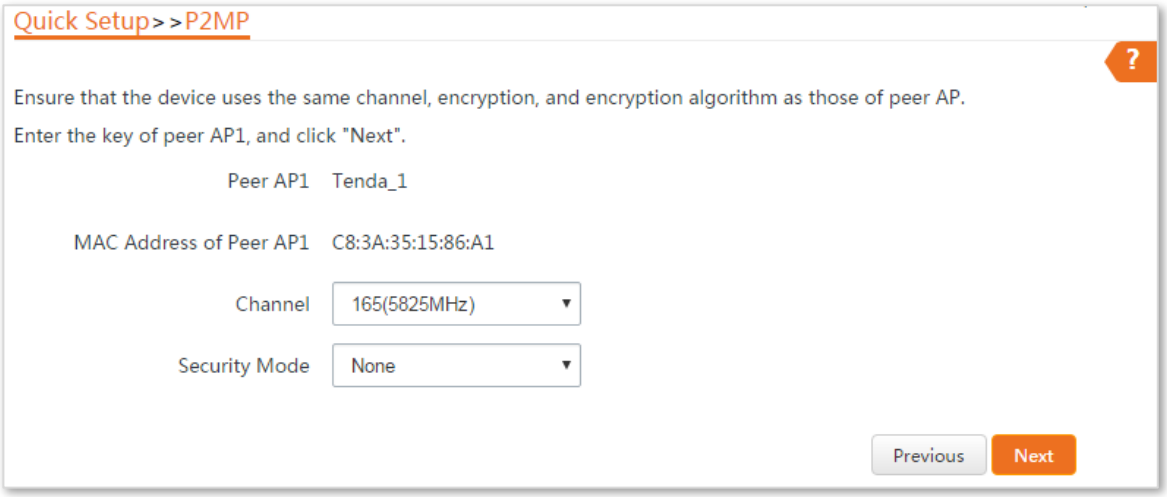
1. Choose **Quick Setup**, select **P2MP**mode, and click **Next**.
2. Select the SSID of CPE1, which is **Tenda_1** in this example, and click **Next**.



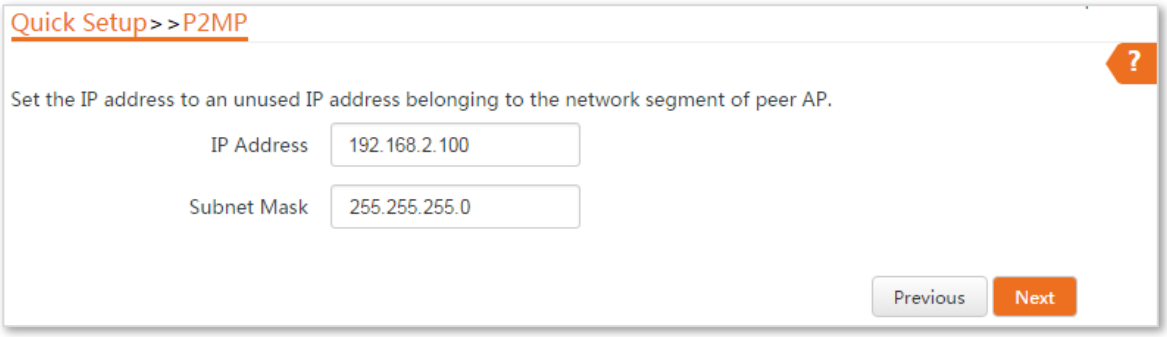
TIP

- 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 CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1.

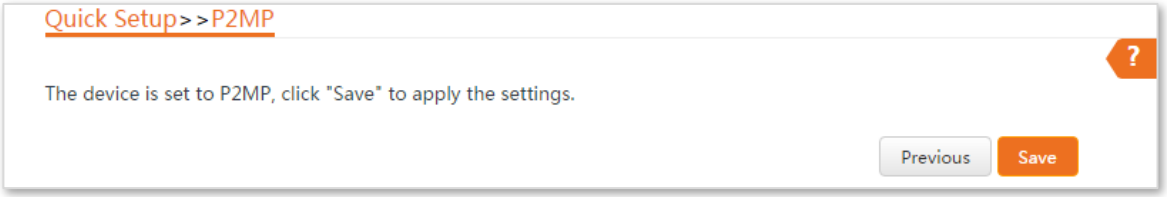
3. Click **Next** on the following page.




4. Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of CPE1 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**.

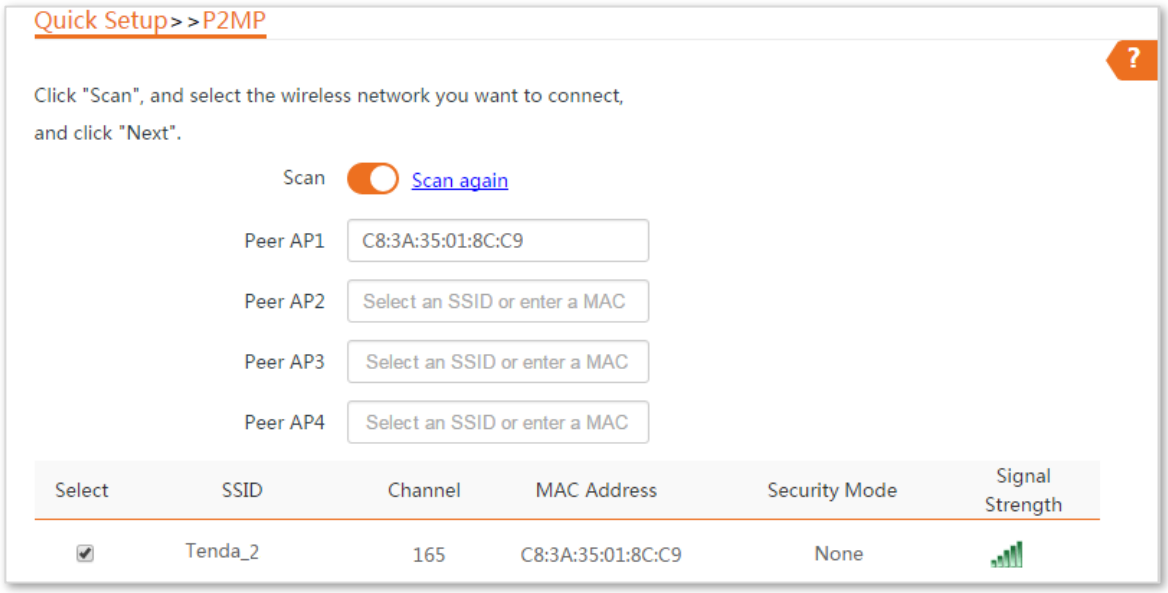



5. Click **Save**, and wait until the device reboots to activate the settings.

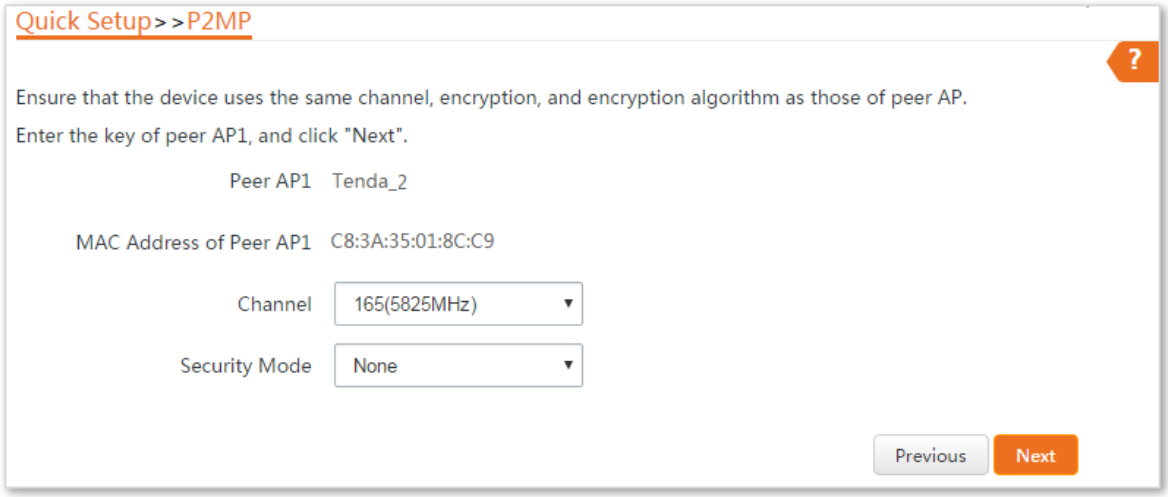



**Step 3** Set CPE1 to **P2MP** mode and bridge to CPE2.

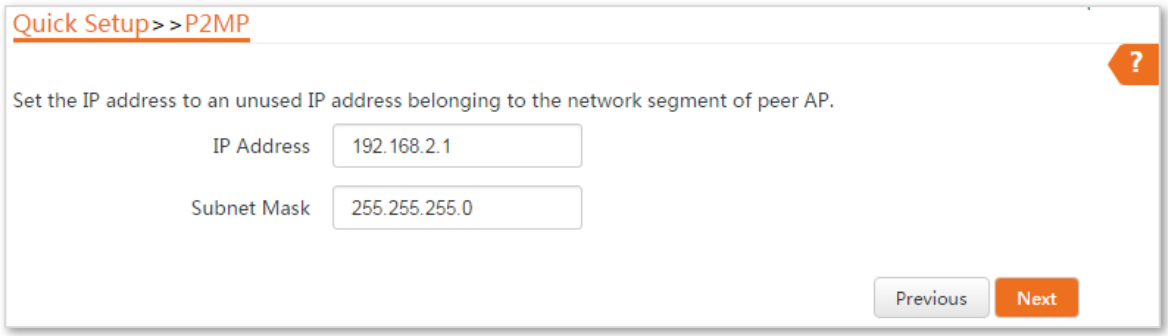
1. Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
2. Select the SSID of CPE2, which is **Tenda_2** in this example, and click **Next**.



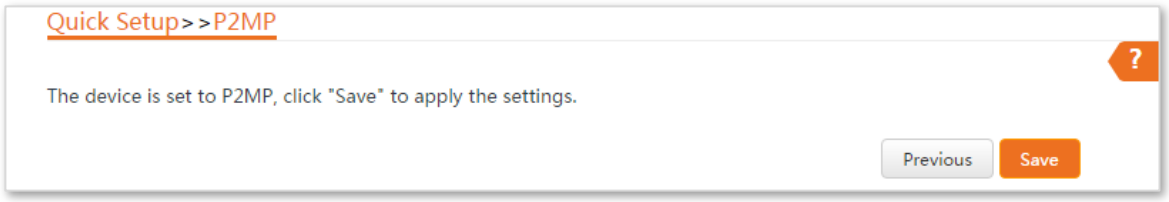

3. Click **Next** on the following page.




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



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




**----End**

**Parameters description**

| Name | Description |
|---|---|
| Working modes | It specifies the working mode of this device.<br>**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 specifies the wireless network name (SSID) 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.<br>TIP<br>The P2MP mode only supports WEP and None security modes. |

# 2.8 Example of repeater mode and P2MP mode

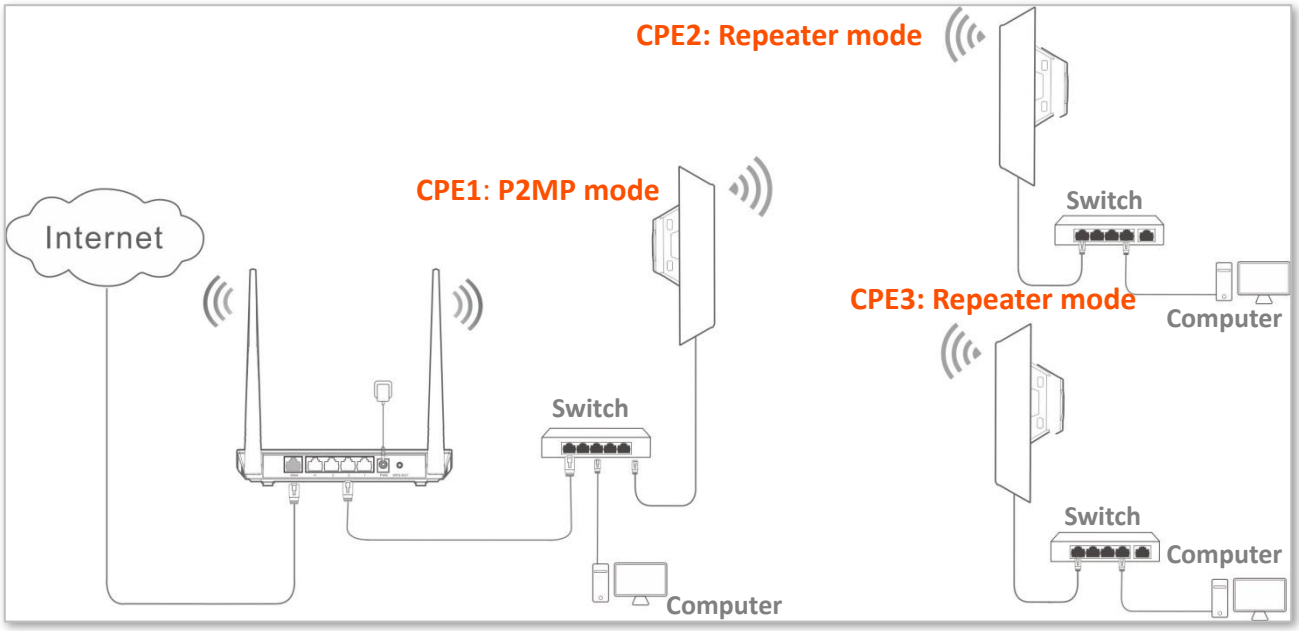
## Network requirement

You have three offices which are not far away from each other, and only one office has internet service. Now you want to combine the networks in three offices into one, and provide wireless networks to wireless devices in the offices without internet service.

## Solution

Set CPE1 to P2MP mode, and set CPE2 and CPE3 to Repeater mode.

## Network typology



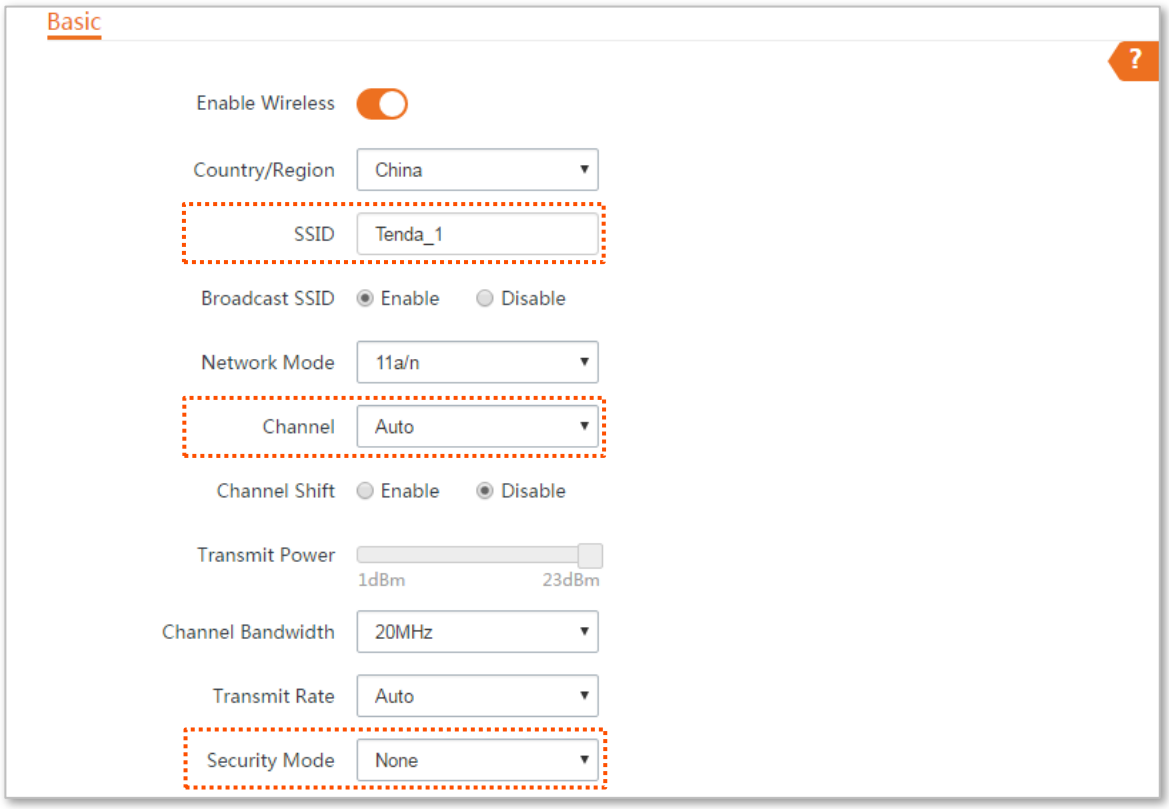

## Configuration procedure

Assume that the wireless parameters of CPE1 are shown as follows:

- **IP Address**: 192.168.2.1
- **SSID**: Tenda_123456
- **Channel**: 165
- **Security mode**: None

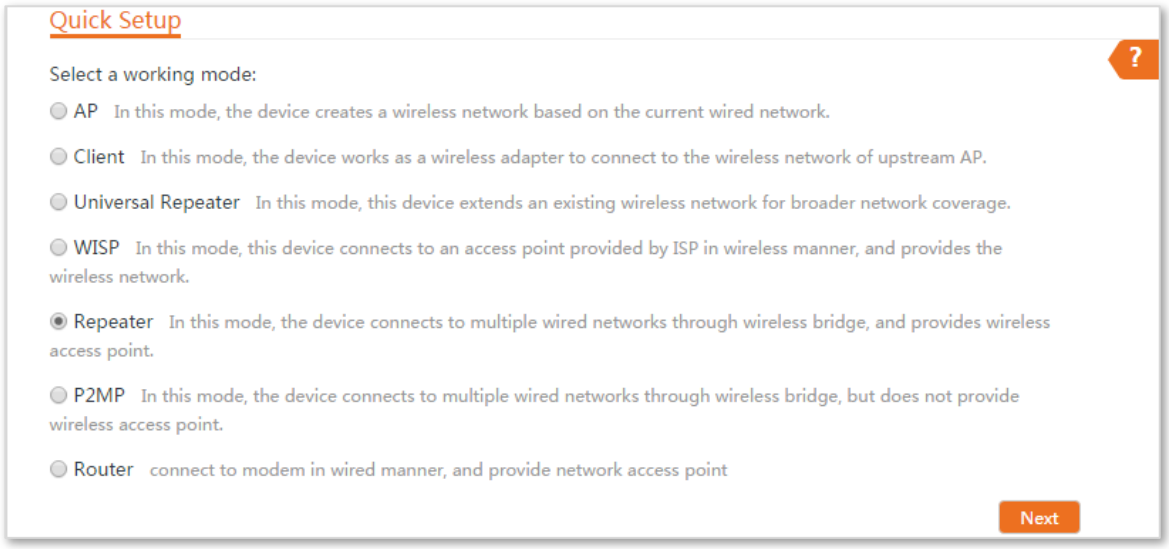
**Step 1** Configure the wireless settings of CPE2.

1. Log in to the web UI of CPE2, and choose **Wireless > Basic** to enter the configuration page.
2. Change the SSID, which is **Tenda_1** in this example.
3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
4. Set the **Security Mode** to the same as that of CPE1, which is **None** in this example.
5. Click **Save** to apply the settings.




**Step 2** Set CPE2 to the **Repeater** mode.

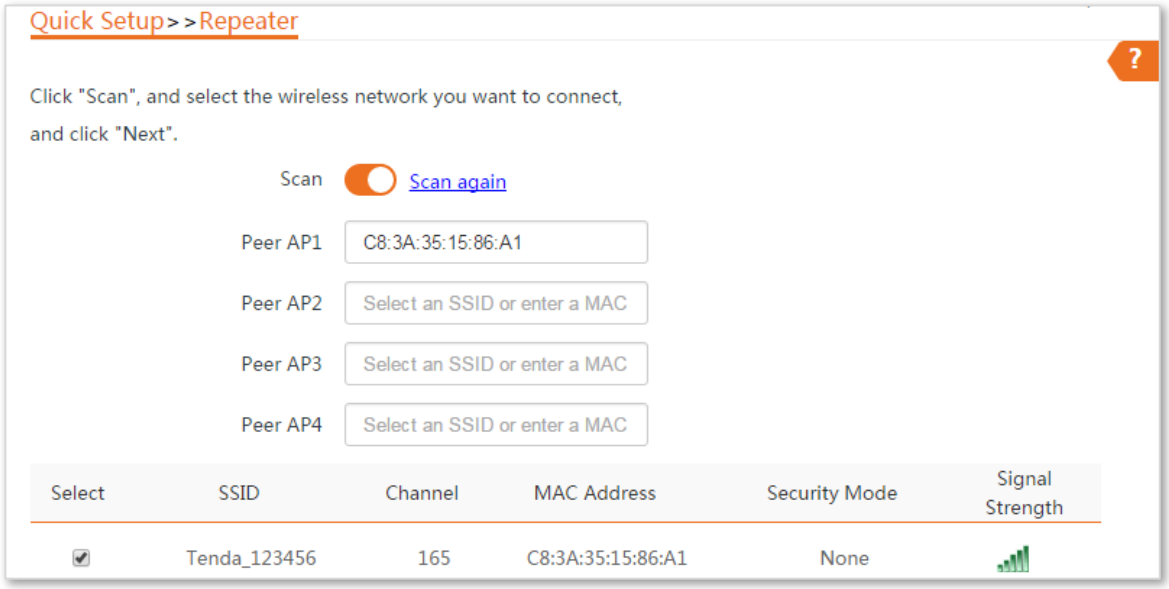
1. Choose **Quick Setup**, and select **Repeater**.



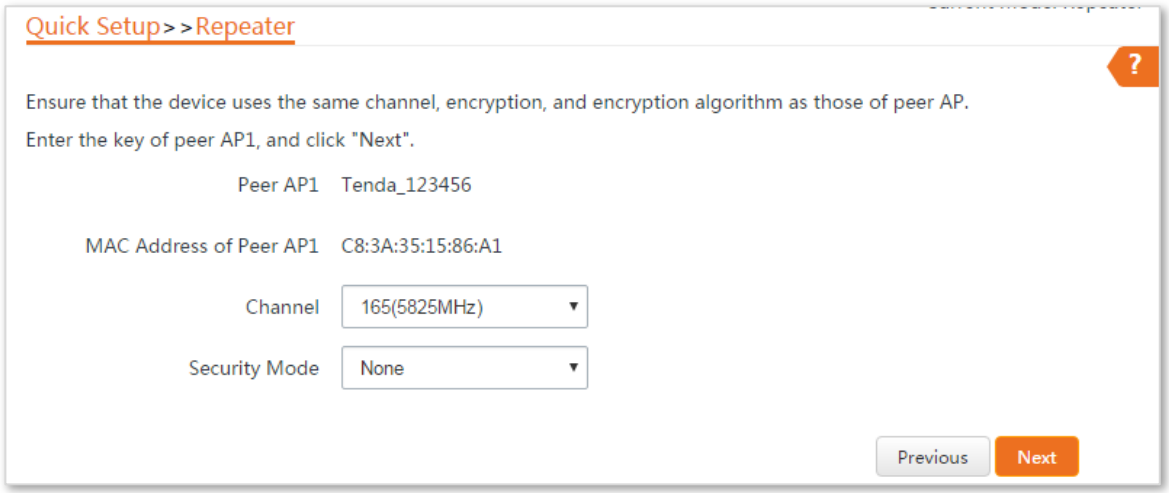

2. Select the SSID of CPE1 from the list, which is **Tenda_123456** in this example, and click **Next**.

TIP

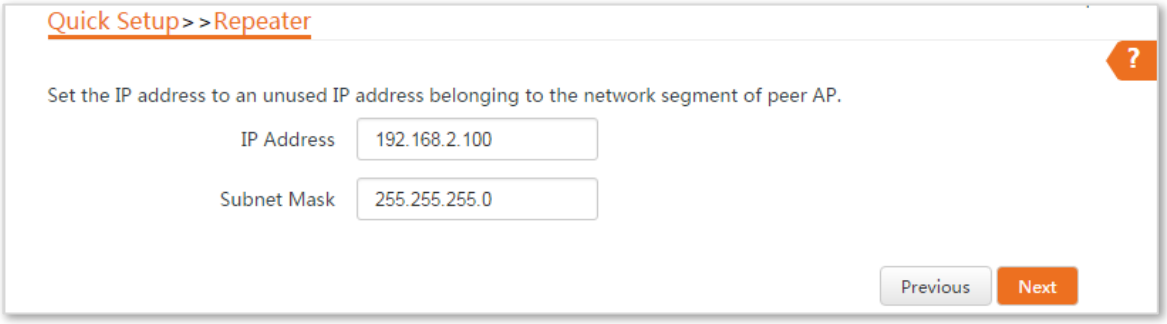
- If you cannot find any SSID from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.
- If you cannot find the SSID of CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1.



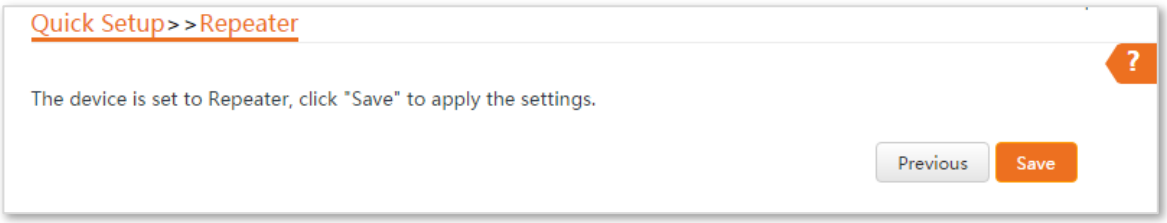

3. Click **Next** directly on the following page.



4. Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of the CPE1 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**.



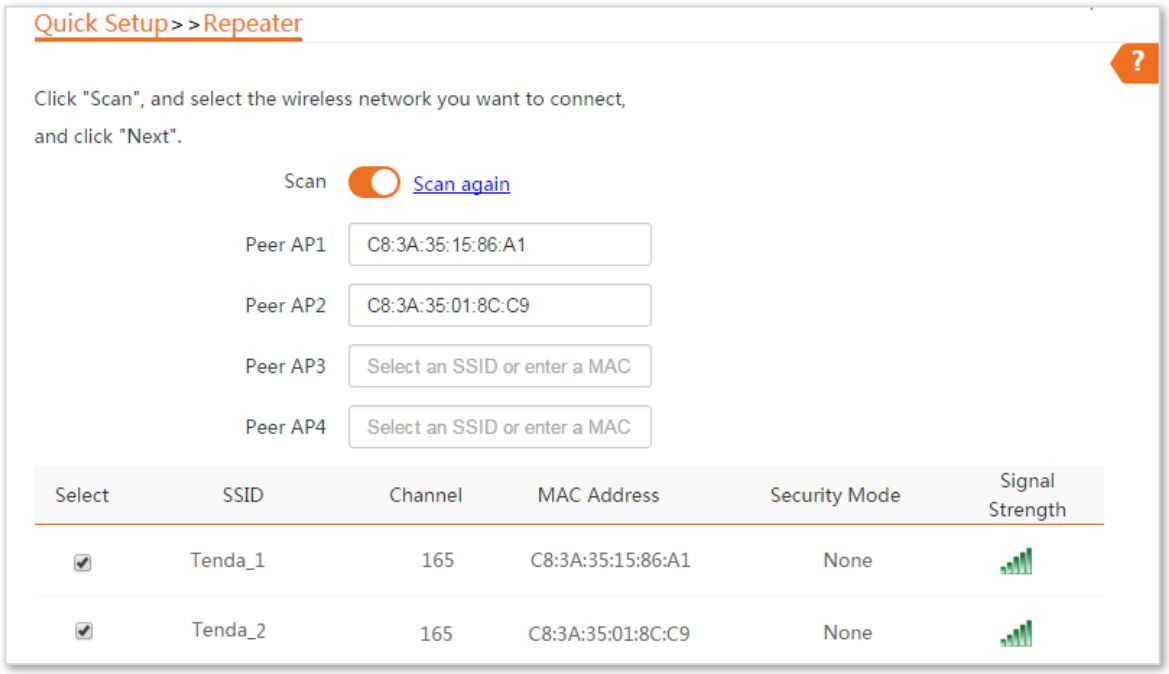

5. Click **Save**, and wait until the device reboots to activate the settings.



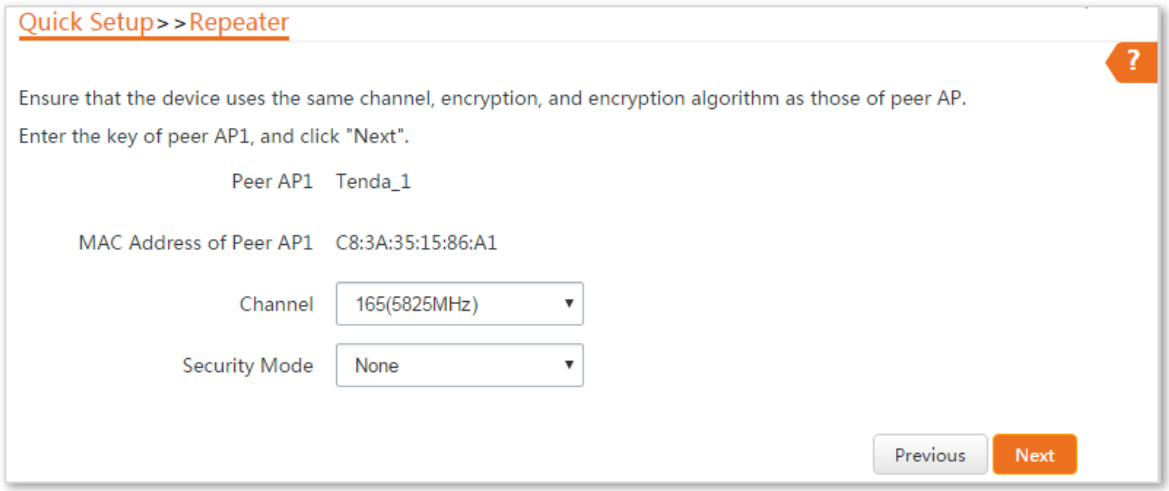

**Step 3** Perform Step 1 and Step 2 above to change the wireless settings of **CPE3**, whose SSID is **Tenda_2** in this example, set it to **Repeater** mode, and bridge to CPE1.

**Step 4** Set CPE1 to **Repeater** mode and bridge to CPE2 and CPE3.

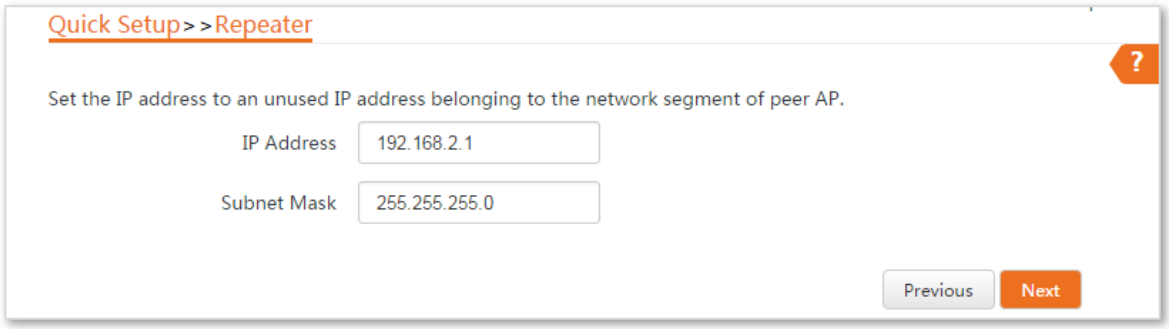
1. Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
2. Select **Repeater** mode, and click **Next**.
3. Select SSIDs of CPE2 and CPE3, and click **Next**.
4. Click **Next** at the bottom of the following page.



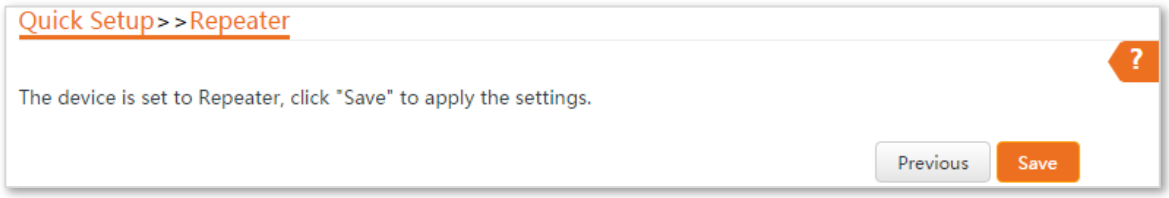

5. Click **Next** on the following page.




6. Click **Next**.




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




**----End**

## Verification

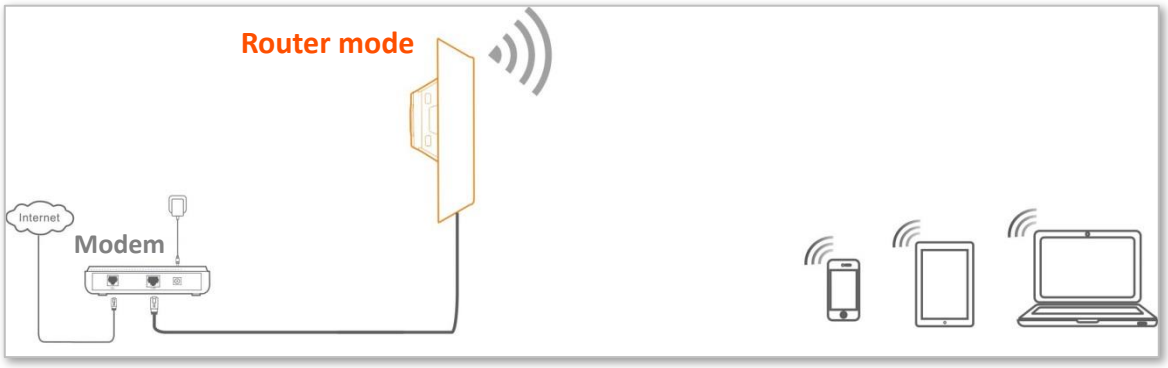
Wired or wireless devices connected to CPE2 and CPE3 can access the internet.

# 2.9 Router mode

In Router mode, this device serves as a router to provide a wireless network.

**Application scenario**

**Network requirement**: You want to use the CPE to provide a wireless network and assign IP addresses to your wireless devices.



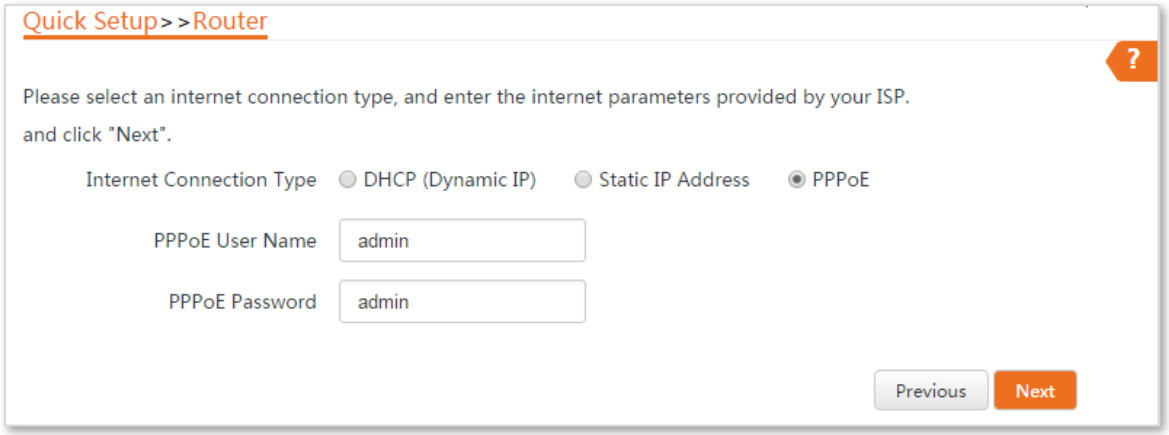

**Configuration procedure of setting Router mode**

**Step 1** Log in to the web UI of the CPE, and choose **Quick Setup** to enter the configuration page.

**Step 2** Select **Router** mode, and click **Next**.

**Step 3** Select your internet connection type, and set the related parameters. Take **PPPoE** as an example here.

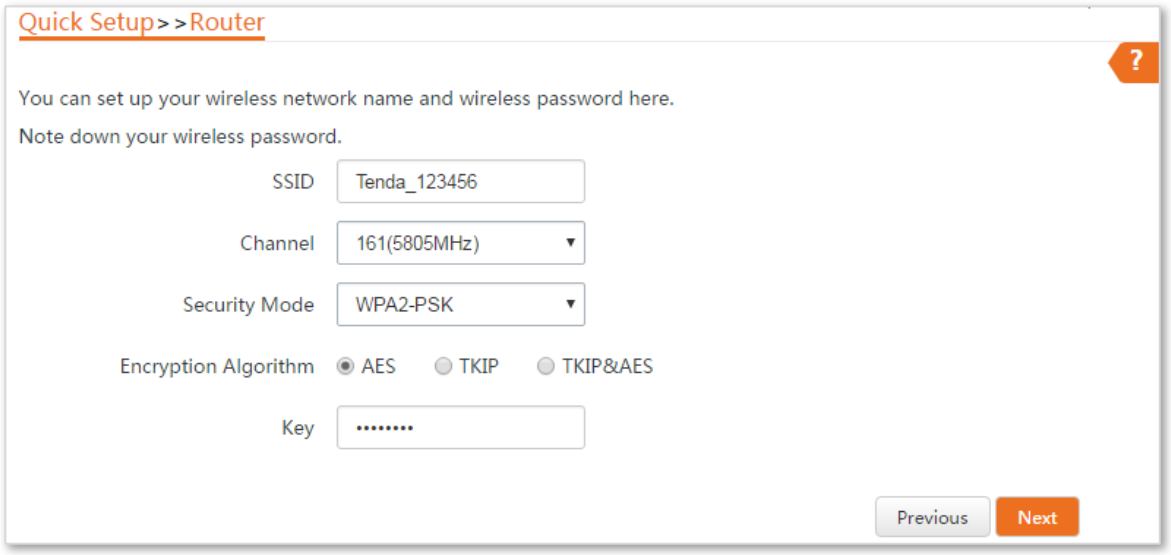
1. Select **PPPoE**.
2. Enter the PPPoE user name and password provided by your internet service provider, which are both **admin** in this example.
3. Click **Next**.



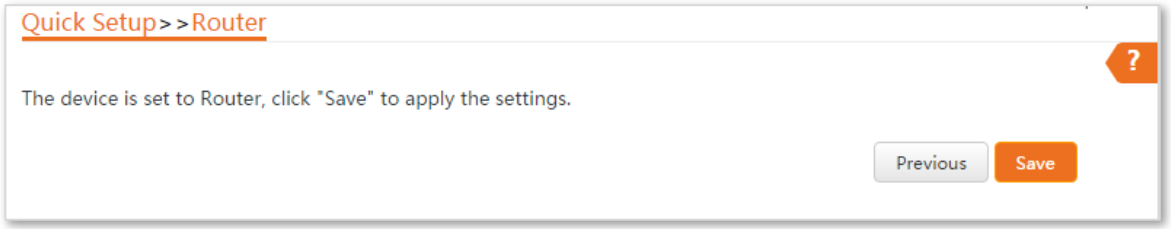

**Step 4** Set wireless parameters of the CPE.

1. Customize a SSID, which is **Tenda_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**.




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




**----End**

### Parameters description

| Name | Description |
|---|---|
| Working modes | It specifies the working mode of this device.<br>**Router mode**: in this mode, the PoE/LAN port works as the WAN port and is used to connect to a modem for internet access. |
| Internet Connection Type | The device in Router mode supports three internet connection types:<br>**DHCP (Dynamic IP)**: The device obtains the IP address and other parameters from the DHCP server of upstream device for internet access.<br>**Static IP Address**: The device accesses the internet using the IP address, subnet mask, default gateway and DNS server IP addresses you manually entered.<br>**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 operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. |

| Name | Description |
| --- | --- |
| 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.<br>Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode. |

## 2.9.2 Example of router mode

### Network requirement

You want to use the CPE to server as a wireless router.

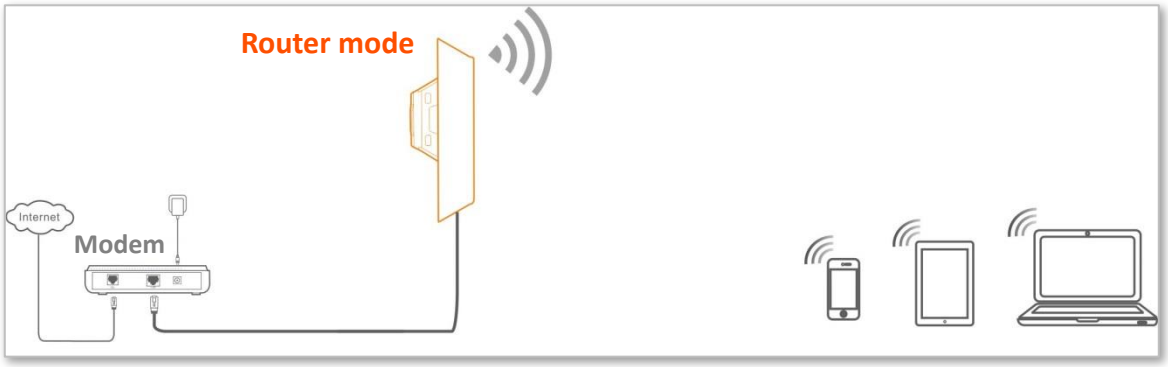
### Solution

Set the CPE to Router mode.

Assume that:

- Your internet connection type: **PPPoE**
- User name: **admin**
- Password: **admin**

### Network typology

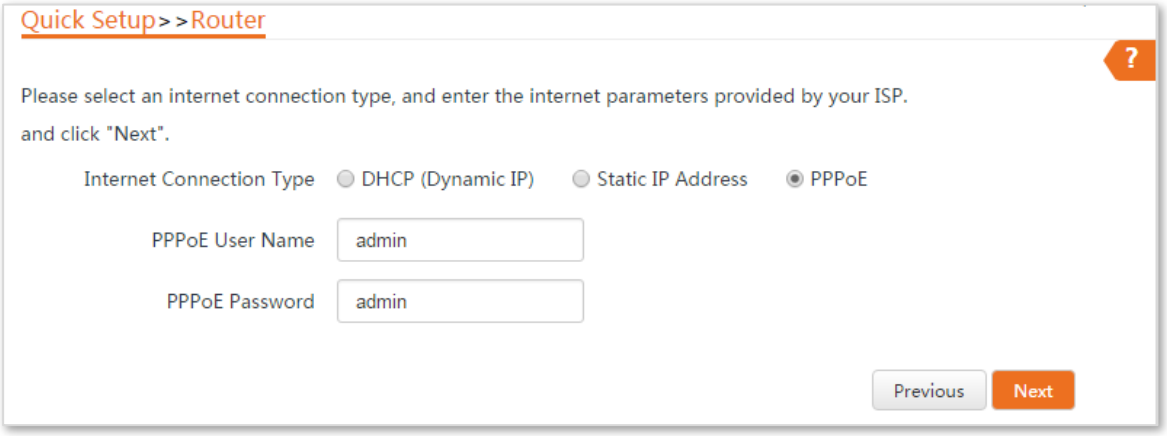



### Configuration procedure

**Step 1** Log in to the web UI of the CPE, and choose **Quick Setup** to enter the configuration page.

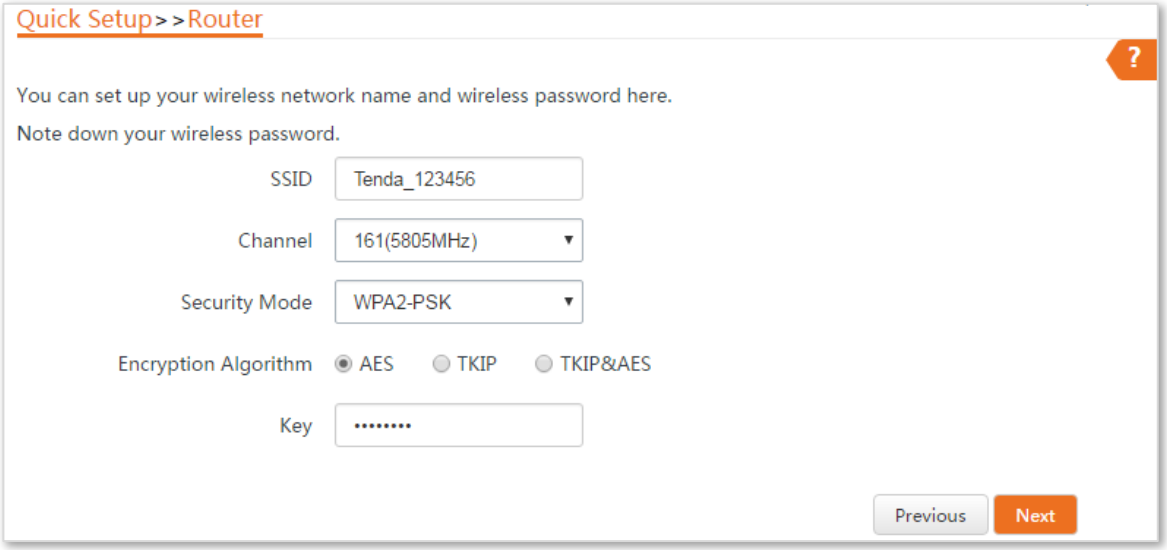
**Step 2** Select **Router** mode, and click **Next**.

**Step 3** Select **PPPoE**, enter **admin** in both **PPPoE User Name** and **PPPoE Password** boxes, and click **Next**.

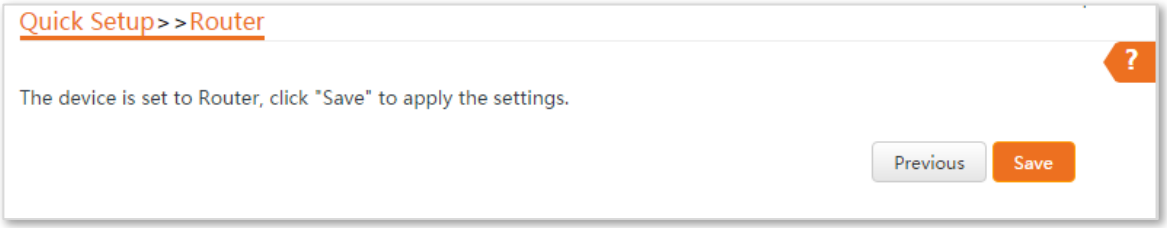



**Step 4** Set wireless parameters of the CPE.

1. Customize a SSID, which is **Tenda_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**.




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




**----End**

## Verification

Wireless devices connected to the wireless network of the CPE can access the internet.

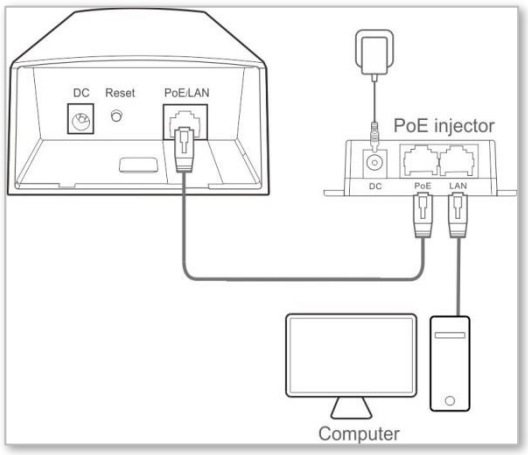
# 3 Web UI

## 3.1 Login

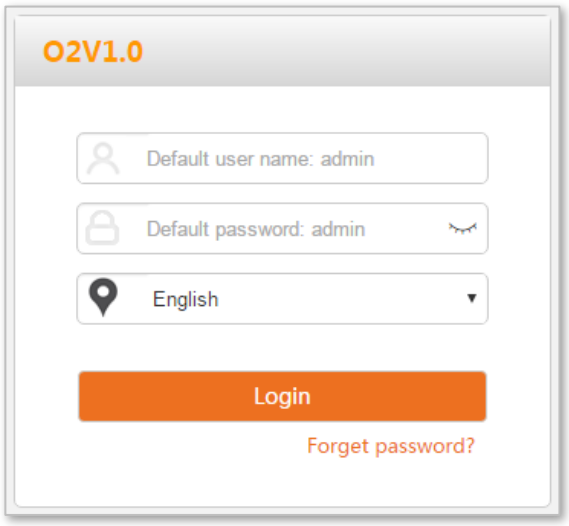
**When you log in to the web UI at the first time, follow the steps below:**

**Step 1** Connect the computer to the device.

1. Uncover the housing of the device.
2. Use an Ethernet cable to connect the **PoE/LAN** port of the device to the **PoE** port of the included PoE injector.
3. Use the included power adapter to connect the PoE injector to a power source. The **LAN/WAN** LED indicator of the device lights up.
4. Use an Ethernet cable to connect your computer to the **LAN** port of the PoE injector.




**Step 2** Start a web browser on your computer, and visit **192.168.2.1**. Enter your user name and password (default: **admin**), and click **Login**.

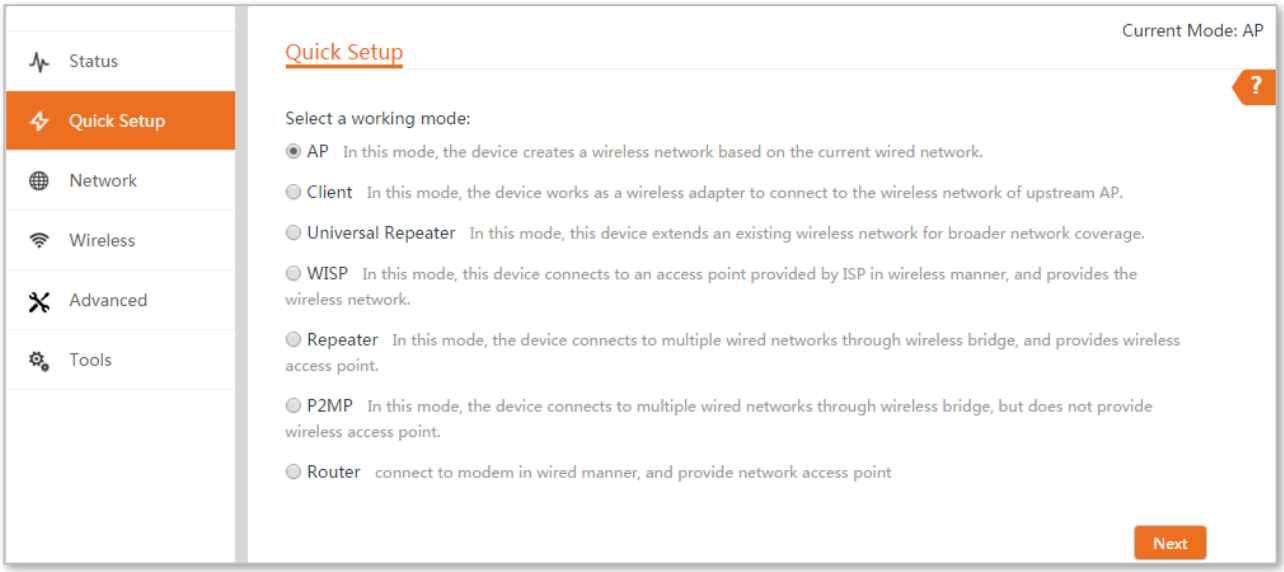



**----End**

TIP

If this page does not appear, please refer to Q1 in FAQ.

Then the following page appears.




**When you log in to the web UI after the device is configured, select one of the following situations to perform.**

- If you want to log in to the CPE in Client mode (LED1, LED2, and LED3 are blinking) after one-to-one auto-bridge, perform the following procedure.

**Step 1** Connect the computer to the **PoE/LAN** port of one of the CPEs, or connect to the wireless network using the SSID and password set on the CPE in AP mode.

**Step 2** Start a web browser on your computer, and visit **192.168.2.2**. Enter your user name and password you set (default: **admin**), and click **Login**.

TIP

If you want to log in to the CPEs in client mode (LED1, LED2, and LED3 are blinking) after one-to-multiple bridge, connect the computer to the **PoE/LAN** port of the corresponding CPE you want to log in one by one using an Ethernet cable, and visit **192.168.2.2**.

**----End**

- If you want to log in to the CPE in Router mode, perform the following procedure.

**Step 1** Connect the computer to the wireless network using the SSID and password set on the CPE.

**Step 2** Visit the LAN IP address you set for the CPE.

**----End**

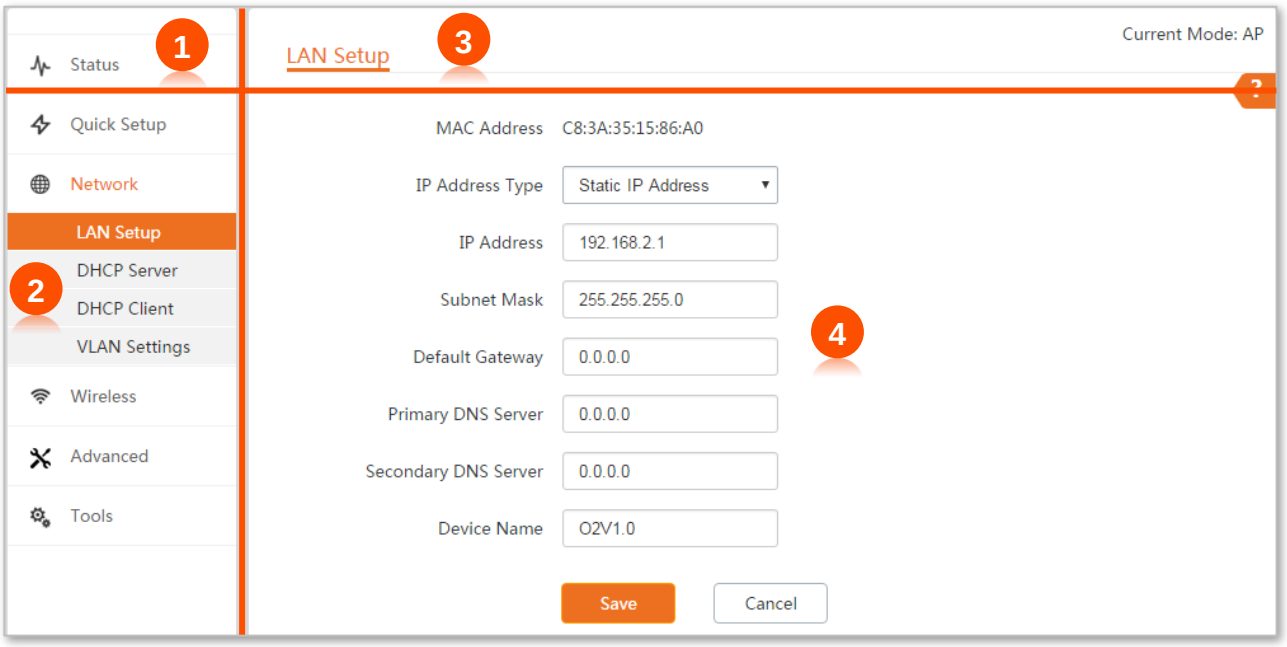
# 3.2 Logout

You can click **Logout** on the upper-right corner of the web UI to logout. When you close the web browser, the system logs you out as well.

If you log in to the web UI of the device and perform no operation within the login timeout interval (default: 5 minutes), the device logs you out.

# 3.3 Web UI layout

The web UI of the device 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.




| No. | Name | Description |
|---|---|---|
| 1 | Level-1 navigation tree | 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. |
| 2 | Level-2 navigation tree | |
| 3 | Tab page area | |
| 4 | Configuration area | It enables you to view and modify configuration. |

# 3.4 Common buttons

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

| Common Buttons | 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. |

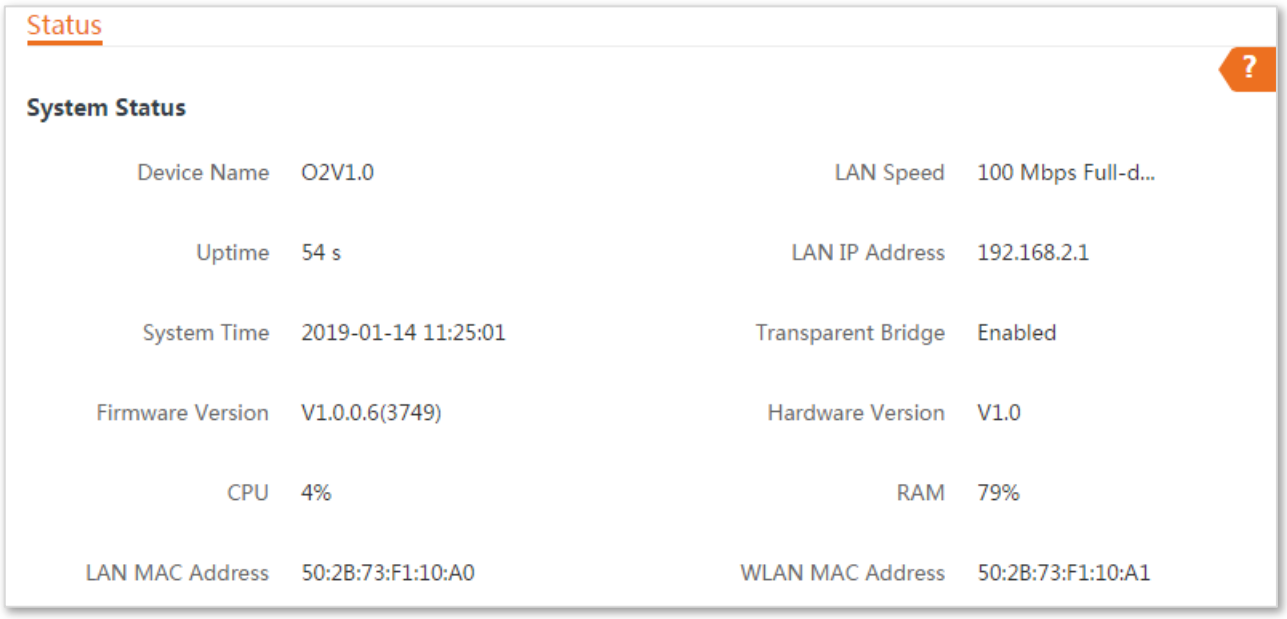
# 4 Status

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

## 4.1 System status

Log in to the web UI of the device, and choose **Status**. You can view the system status here.

If this device is set to **AP** mode, **Client** mode, **Universal Repeater** mode, **Repeater** mode or **P2MP** mode, the system status is shown as follows:

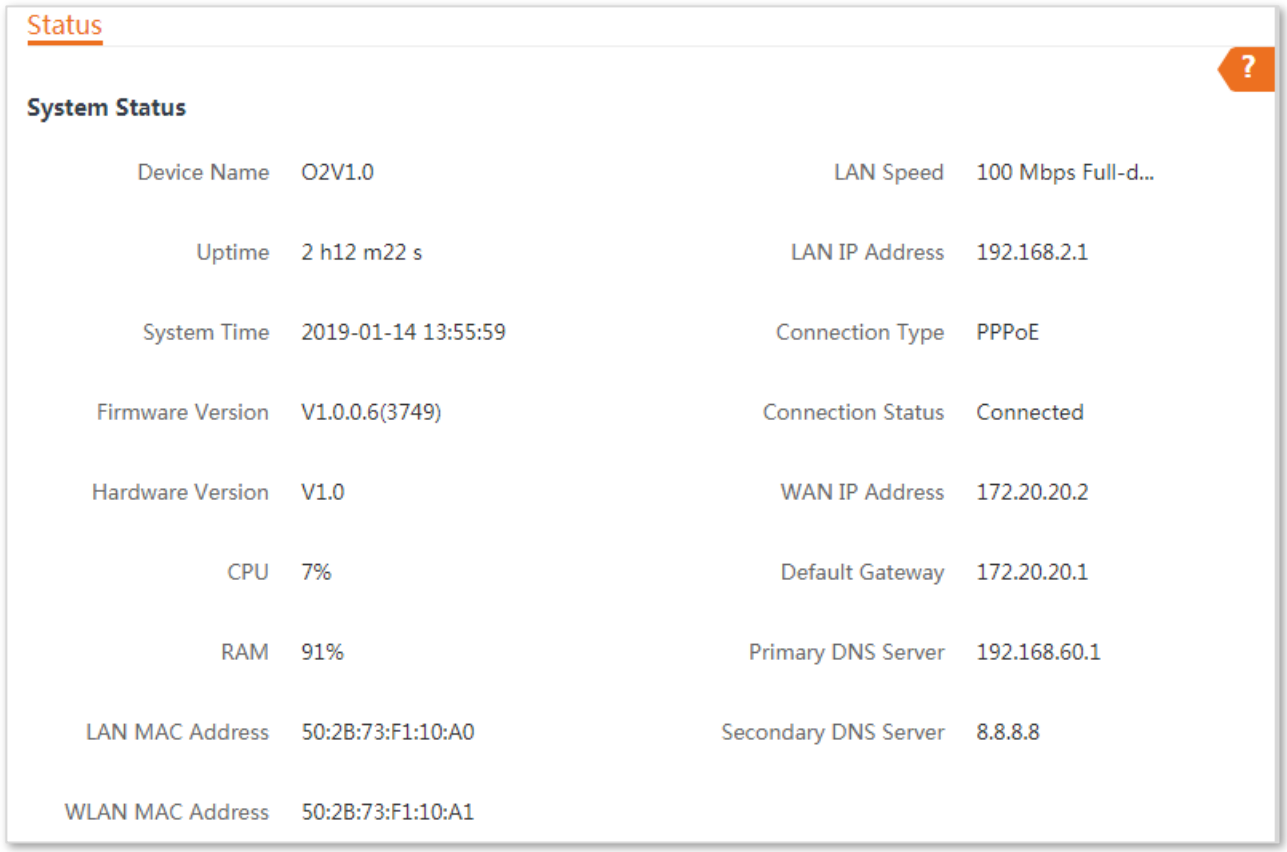



**Parameters description**

| Name | 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 time that has elapsed since the device was started last time. |
| System Time | It specifies the current system time of this device. |
| Hardware Version | It specifies the hardware version of this device. |
| RAM | Random Access Memory. It specifies the memory usage of this device. |

| Name | Description |
| --- | --- |
| 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. |
| 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. When connecting to another device using an Ethernet cable, the device uses this MAC address to communicate with the device. |

If the device is set to **WISP** or **Router** mode, the system status is shown as follows:



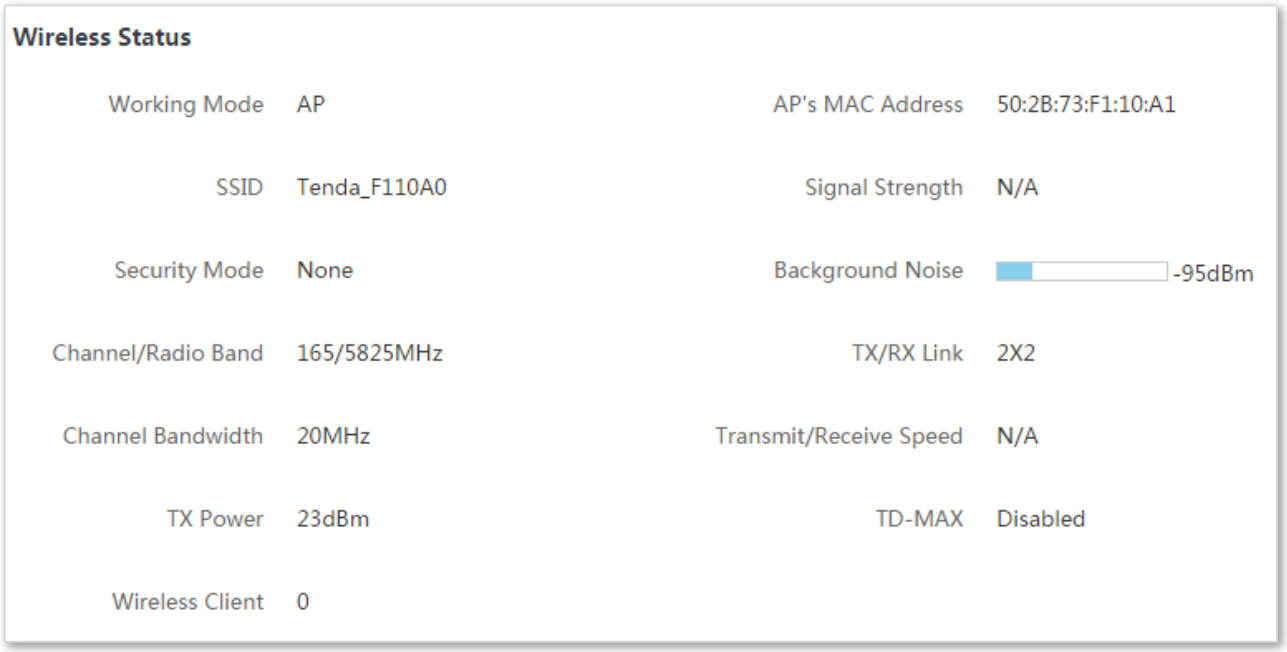

### Parameters description

| Name | Description |
| --- | --- |
| Connection Type | It specifies the internet connection type of this device in **WISP** or **Router** mode. |
| Connection Status | It specifies the connection status of WAN port of this device in **WISP** or **Router** |

| Name | Description |
| --- | --- |
| | mode. |
| WAN IP Address | It specifies the IP address of WAN port of this device in **WISP** or **Router** mode. |
| Default Gateway | It specifies the default gateway address of this device in **WISP** or **Router** mode. |
| Primary DNS Server | It specifies the IP address of primary DNS server of this device in **WISP** or **Router** mode. |
| Secondary DNS Server | It specifies the IP address of secondary DNS server of this device in **WISP** or **Router** mode. |

# 4.2 Wireless status

Log in to the web UI of the device, and choose **Status**. You can view wireless status here, including working mode, SSID, security mode, and so on.



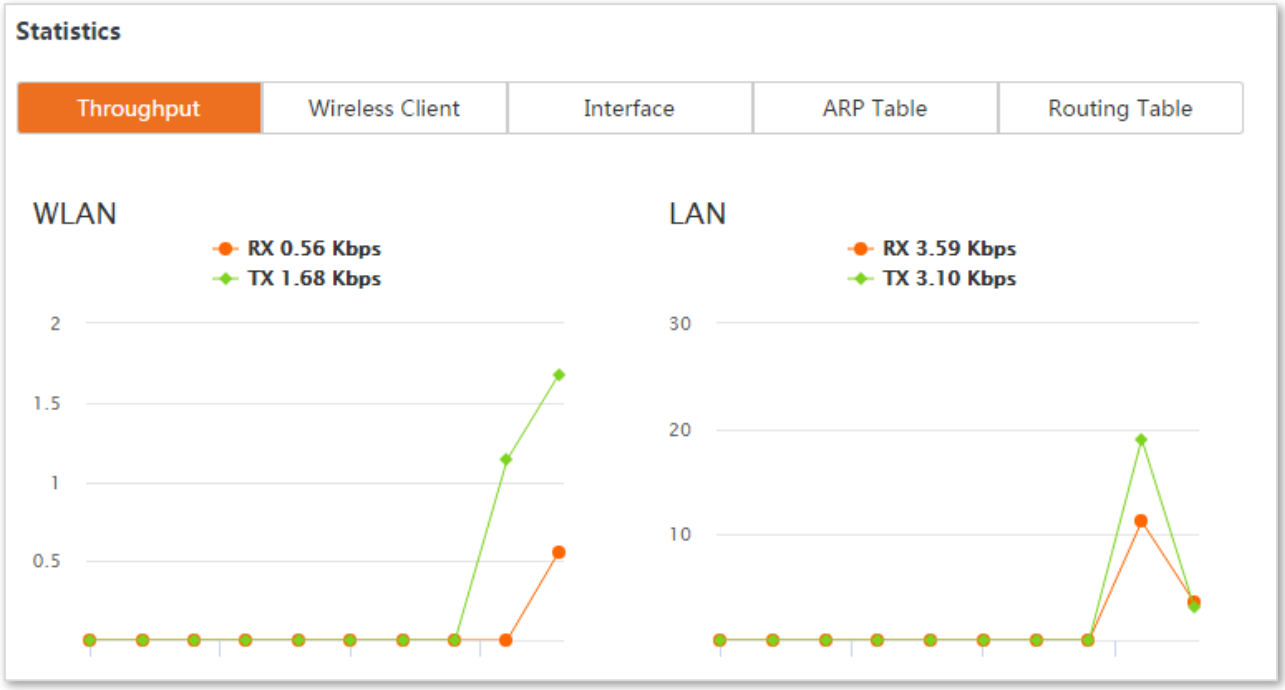

### Parameters description

| Name | Description |
|---|---|
| Working Mode | It specifies the working mode the device operates. |
| SSID | It specifies the wireless network name of this device. |
| Security Mode | It specifies the security mode of the wireless network of this device. |
| Channel/Radio Band | It specifies the channel and radio band used by this device to transmit radio signals. |
| Channel Bandwidth | It specifies the channel bandwidth of this device. |
| TX Power | It specifies the transmitted power of this device. |
| Wireless Client | It specifies the number of wireless clients connected to this device. |
| AP's MAC Address | It displays **No Peer AP** if the device works in **AP** or **Router** mode. And in other modes, it displays the MAC address of peer AP to which this device bridged. |
| Signal Strength | It displays the signal strength of the first device connected to the wireless network of the device when it works in AP or Router mode. It displays the received signal strength from peer AP when the device works in Client, Universal Repeater, WISP, Repeater or P2MP mode. |
| Background Noise | It specifies the strength of radio interference signals in the ambient environment that interfere with the channel of this device. Larger absolute value indicates less |

| Name | Description |
| --- | --- |
| | interference. For example, -95 dBm indicates less interference than -75 dBm. |
| TX/RX Link | It specifies the number of spatial streams the device is transmitting or receiving. |
| Transmit/Receive Speed | It specifies the wireless transmitting/receiving rate.<br>In AP or Router mode: it displays the transmitting/receiving rate of the first device connected to the wireless network of this device.<br>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. |

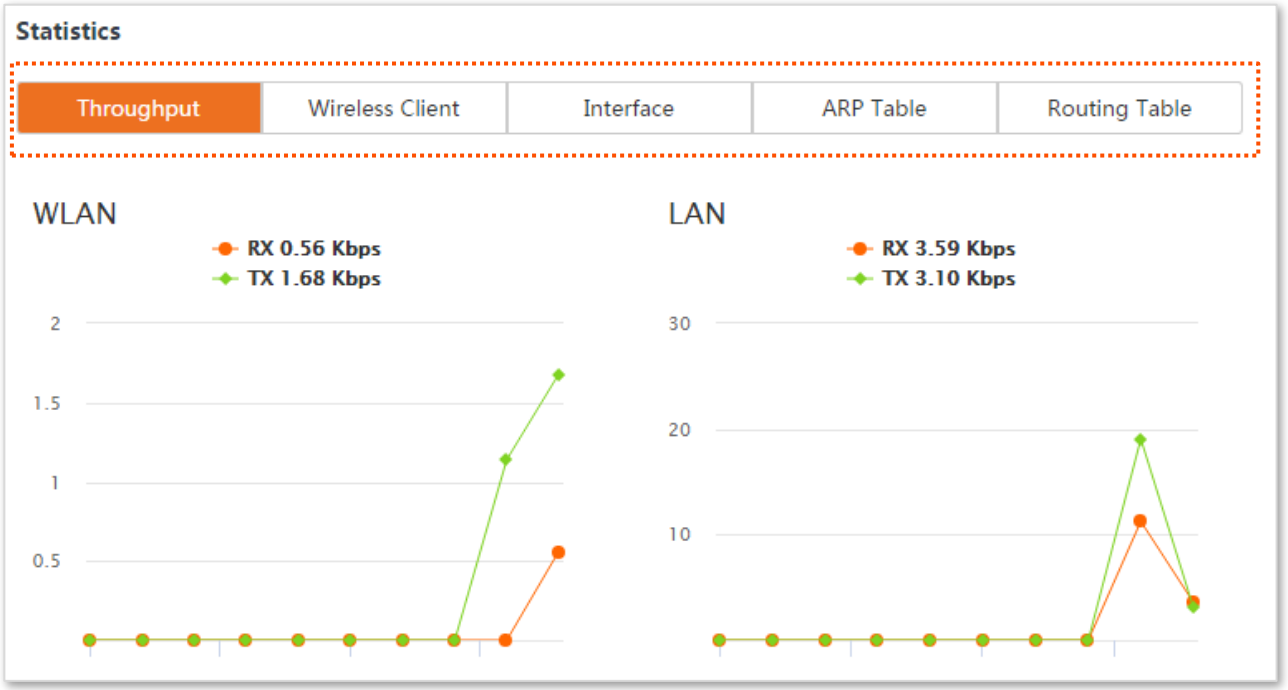
# 4.3 Statistics

Log in to the web UI of the device, and choose **Status**. You can view statistics information here, including throughput, wireless client, interface, ARP table and routing table.



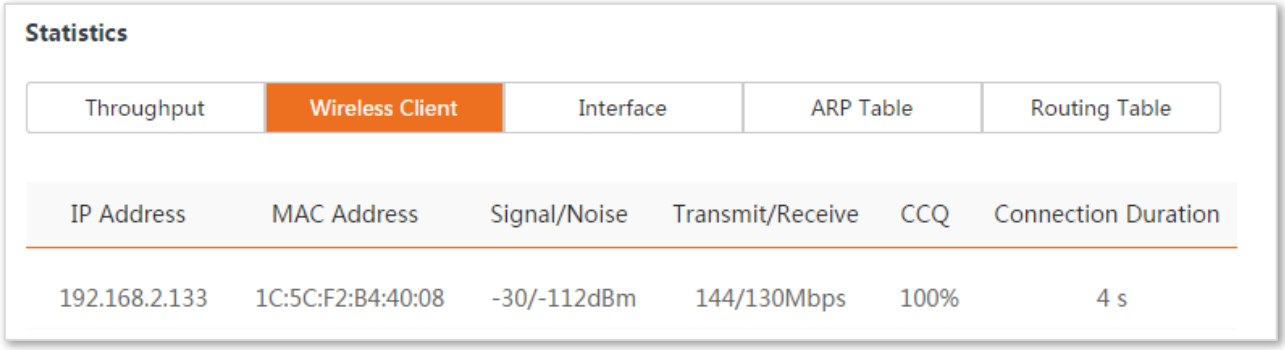

## 4.3.1 Throughput

It displays the throughput of WLAN and LAN ports here.



## 4.3.2 Wireless client

It displays the information of wireless clients when the device works in **AP**, **Repeater**, **P2MP**, or **Router** mode.

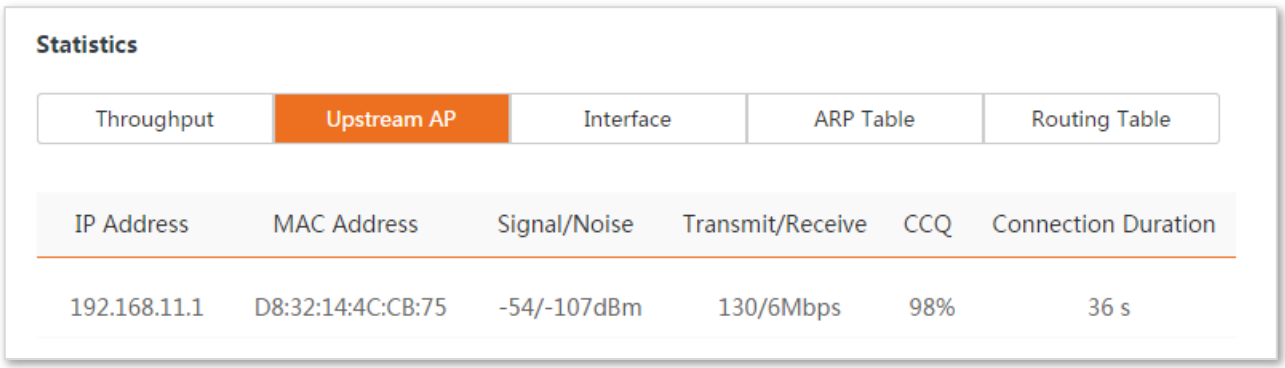



**Parameters description**

| Name | 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 | It specifies the WiFi signal strength and electromagnet interference signal strength of the corresponding wireless client. |
| Transmit/Receive | It specifies the transmitting and receiving rate of the corresponding client. |
| CCQ | It specifies the connection quality of the corresponding client. Higher percentage indicates 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. |

## 4.3.3 Upstream AP

This function is available only when the device works in Client, Universal Repeater, or WISP mode.

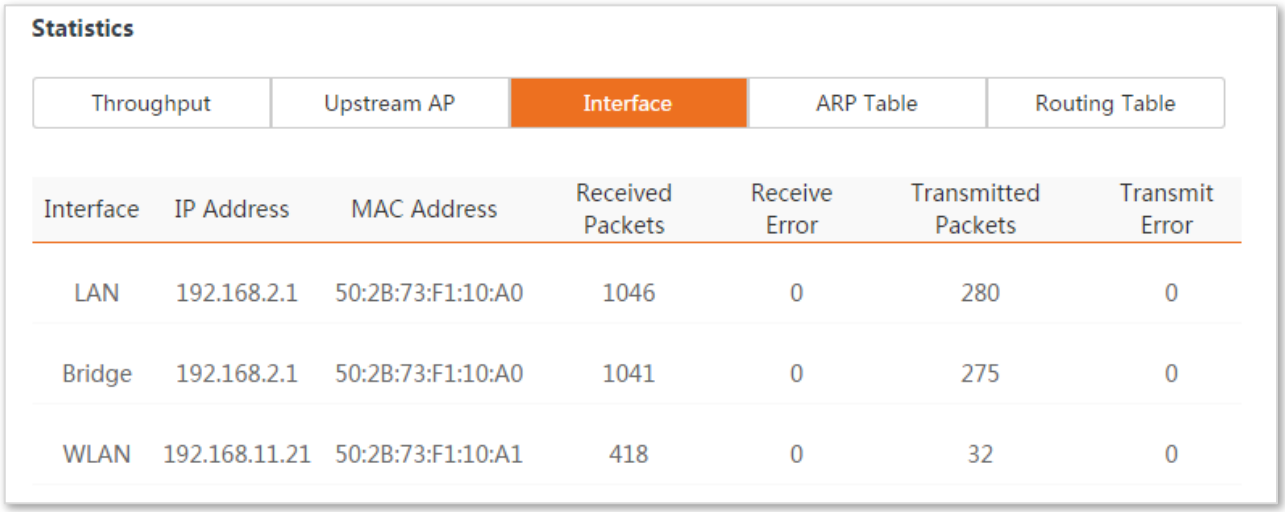


### Parameters description

| Name | 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 | It specifies the WiFi signal strength and electromagnet interference signal strength of the upstream device. |
| Transmit/Receive | It specifies the transmitting and receiving rate of the upstream device. |
| CCQ | It specifies the connection quality of the upstream device. Higher percentage indicates better connection quality. |
| Connection Duration | It specifies the time that has elapsed since this device bridges to the upstream device. |

## 4.3.4 Interface

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



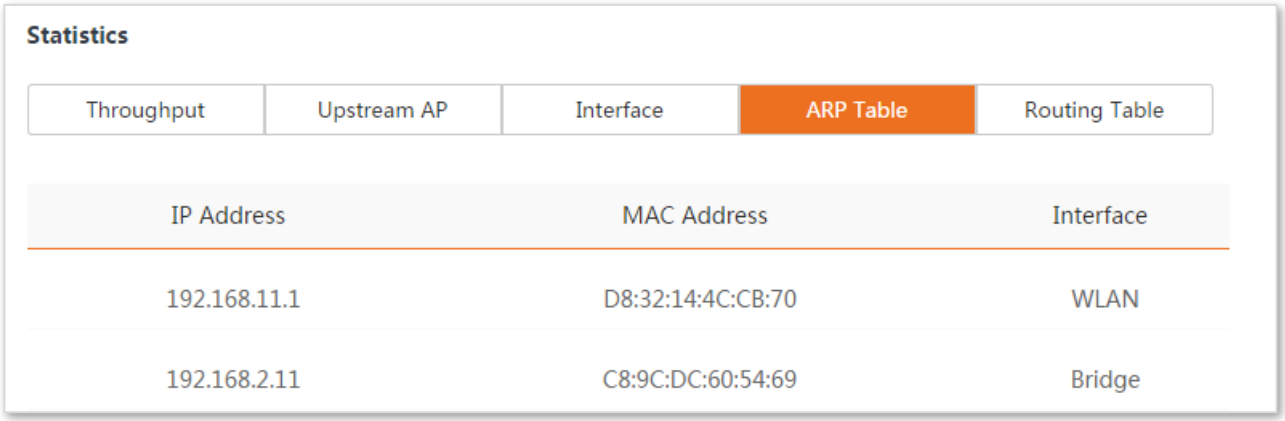

### Parameters description

| Name | Description |
|---|---|
| Interface | It displays the wired interface, bridge interface, and WLAN interface of the device. |
| IP Address | It displays the IP addresses of wired interface, bridge interface, and WLAN interface. |
| MAC Address | It displays the MAC addresses of wired interface, bridge interface, and WLAN 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 | |

## 4.3.5 ARP table

It specifies the current ARP table of the device.

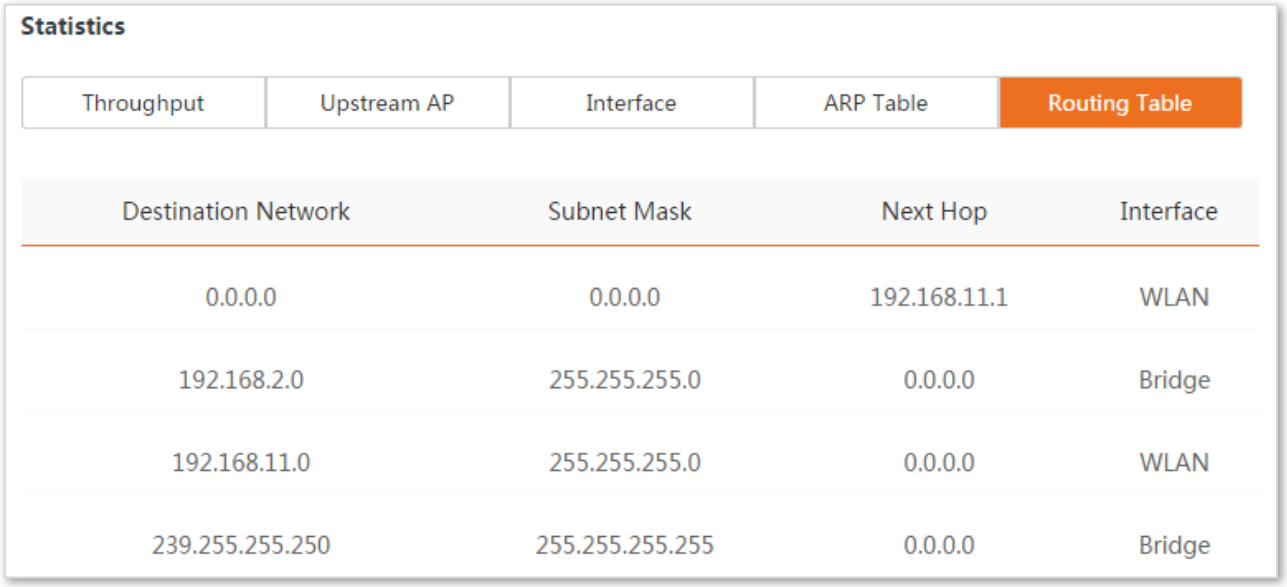



**Parameters description**

| Name | 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. |

## 4.3.6 Routing table

It specifies the destination networks that the device can access.




**Parameters description**

| Name | 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. |
| Interface | It specifies the interface that the packets egress. |

# 5 Network

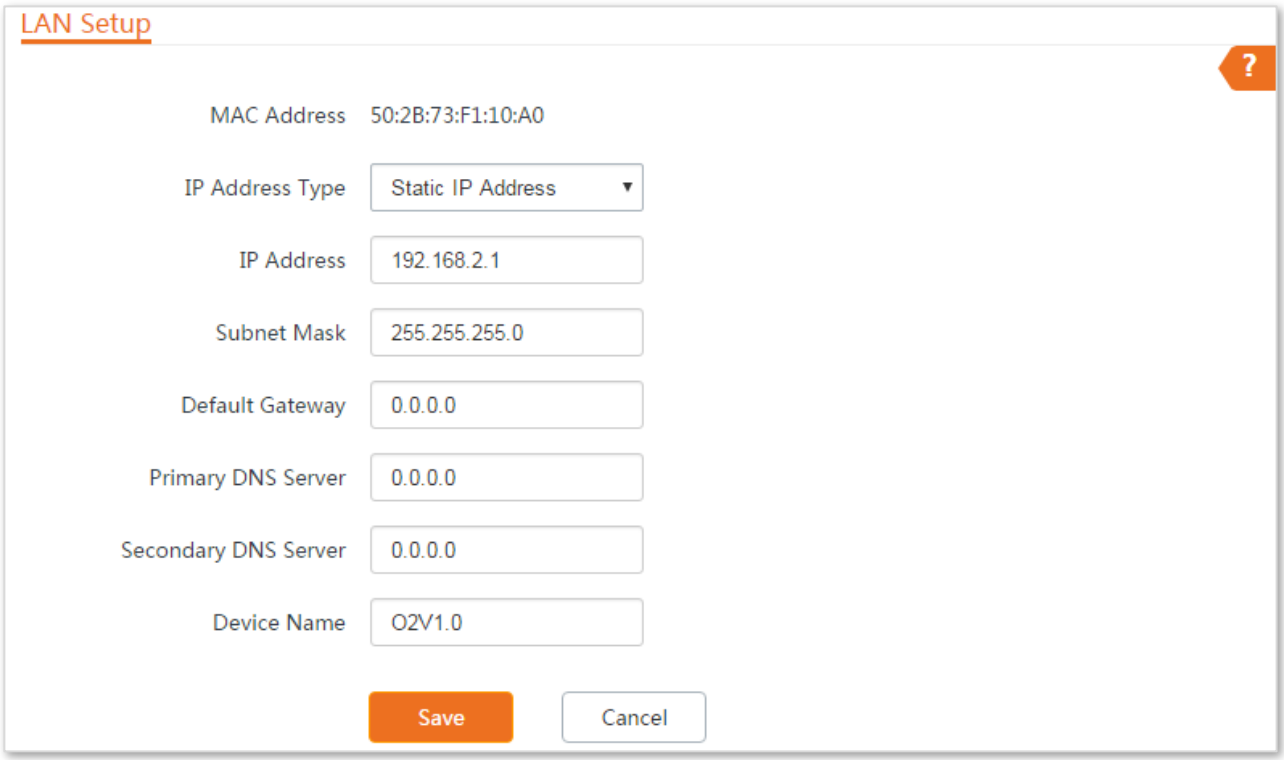
## 5.1 LAN setup

### 5.1.1 Overview

Log in to the web UI of the device, and choose **Network** > **LAN Setup** to enter the page.

This page enables you to view the MAC address of the LAN port, set up the device name, and type of obtaining an IP address and related parameters.

When the CPE is in **AP**, **Client**, **Universal Repeater**, **Repeater**, and **P2MP** modes, the page displays:

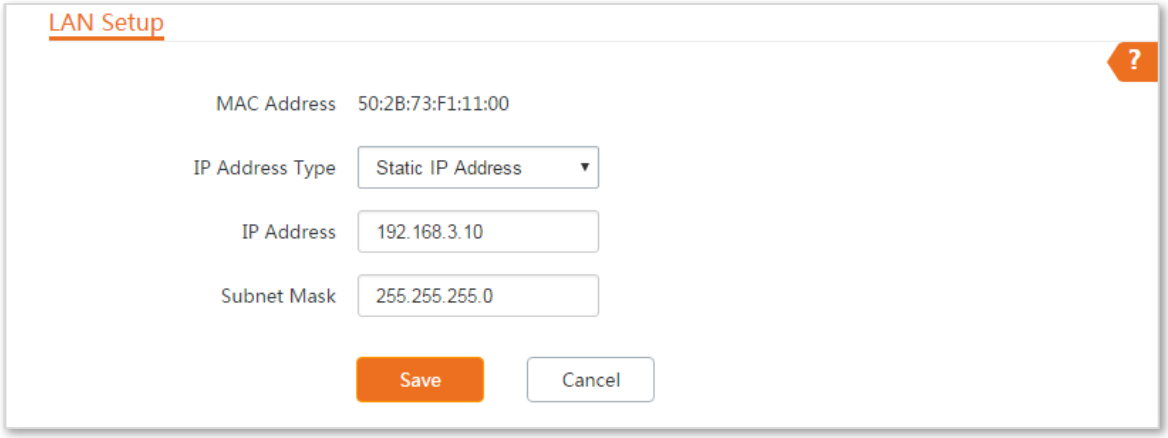



**Parameters description**

| Name | 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**.<br>**Static IP Address**: Specify the IP address, subnet mask, default gateway, and DNS server IP addresses manually.<br>**DHCP (Dynamic IP Address)**: The device obtains an IP address, subnet mask, default |

| Name | Description |
| --- | --- |
| | gateway and DNS server IP address from the DHCP server in the network.<br>TIP<br>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 in the network, and use this IP address to log in. |
| IP Address | It specifies the LAN IP address of the device. |
| Subnet Mask | It specifies the subnet mask corresponding to the LAN IP address of the device. The default is **255.255.255.0**. |
| Default Gateway | It specifies the default gateway of the device.<br>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.<br>If the egress router has the DNS agency function, it can be set to the LAN IP address the egress router. Otherwise, specify a DNS server IP address manually. |
| Secondary DNS Server | It specifies the secondary DNS server IP address of the device.<br>If there are two DNS server IP addresses, enter one in this box. |
| Device Name | It specifies the name of the device. The default name indicates the product model and version.<br>You are recommended to change the name to indicate the location of the device, so that you can easily identify the device when there are multiple devices in the network. |

When the CPE is in **WISP** and **Router** modes, the page displays:




| Name | 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**. |

| Name | Description |
| --- | --- |
| | **Static IP Address**: Specify the IP address and subnet mask manually.<br><br>**DHCP (Dynamic IP Address)**: The device obtains an IP address and subnet mask from the upstream DHCP server in the network.<br><br>TIP<br><br>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. |
| Subnet Mask | It specifies the subnet mask corresponding to the LAN IP address of the device. The default is **255.255.255.0**. |

## 5.1.2 Changing the LAN IP address

### Manually setting the IP address

In this mode, you must 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.

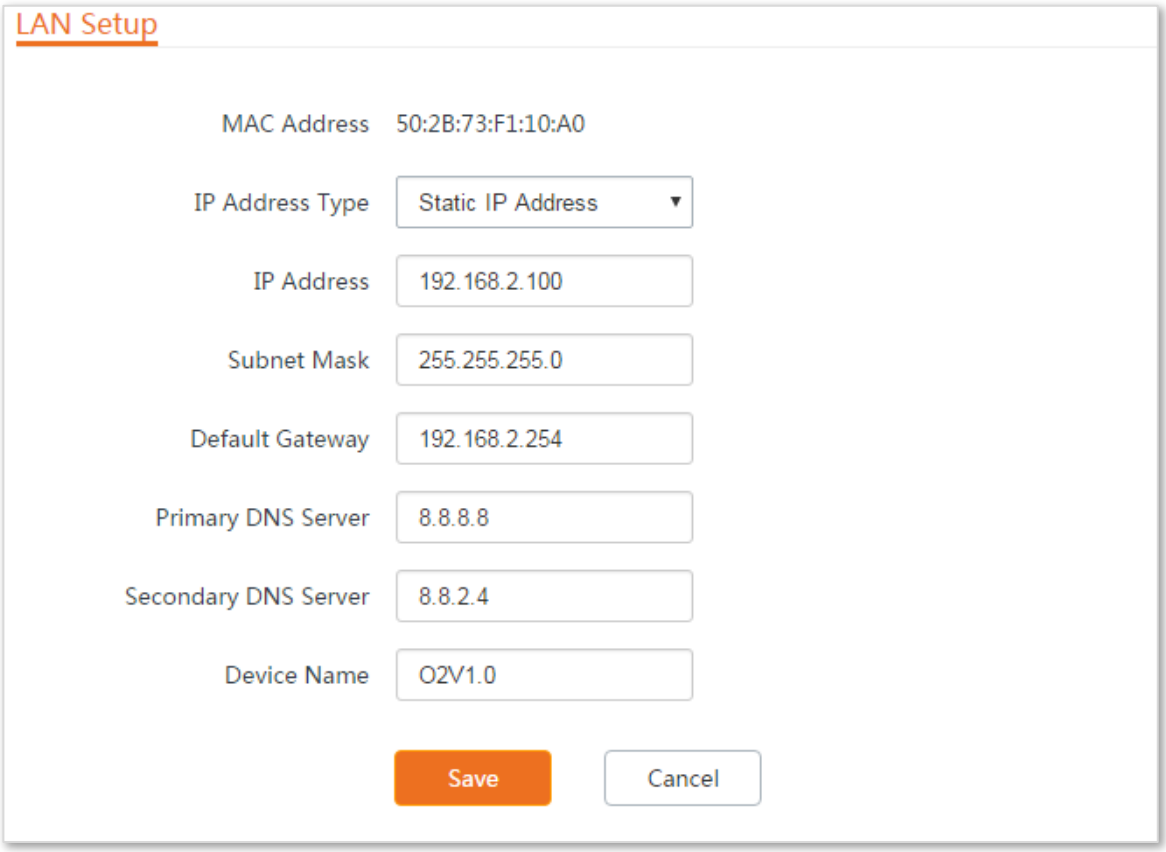
**Configuration procedure:**

**Step 1** Choose **Network** > **LAN Setup** to enter the configuration page.

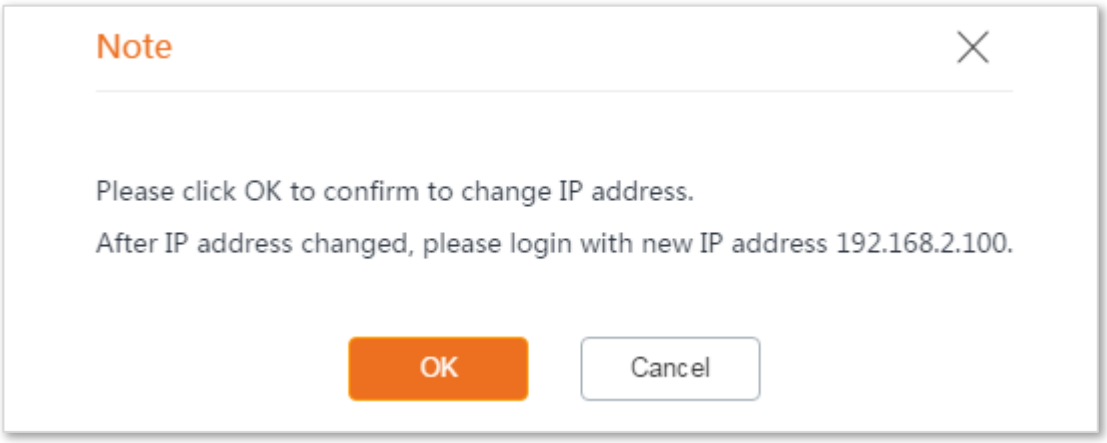
**Step 2** Set **IP Address Type** to **Static IP Address**.

**Step 3** Set **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**. If another DNS server is available, set **Secondary DNS Server** to the IP address of the additional DNS server.

**Step 4** Click **Save**.




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




**----End**

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.

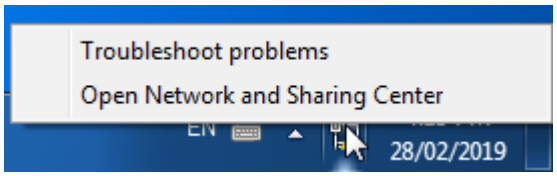
Otherwise, assign your computer an IP address that belongs to the same network segment as the new IP address of the device before login with the new IP address.

**Assume that**: the new IP address of the device is **192.168.1.1**, and subnet mask is **255.255.255.0**, then assign an IP address belonging to the same segment.

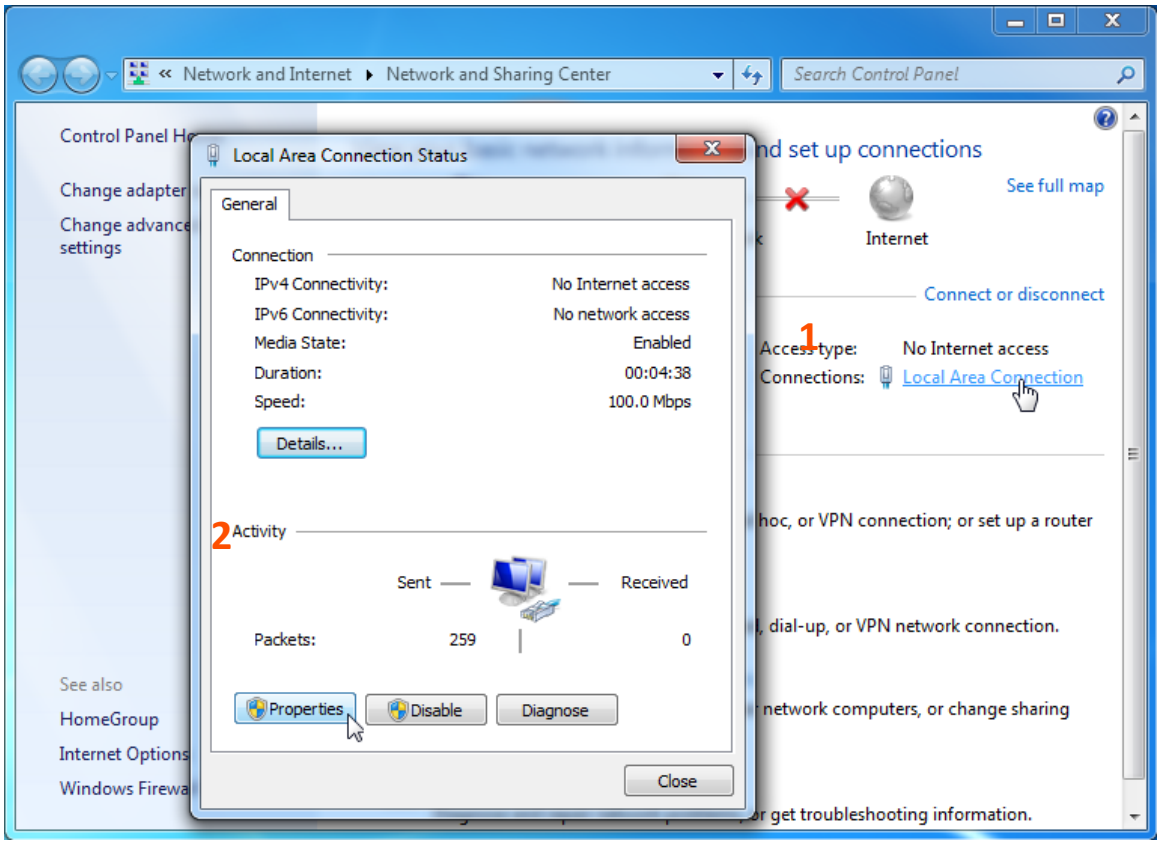
**Configuration procedure** (OS example: Windows 7)**:**

**Step 1** Right-click the icon on the bottom-right corner of the desktop.

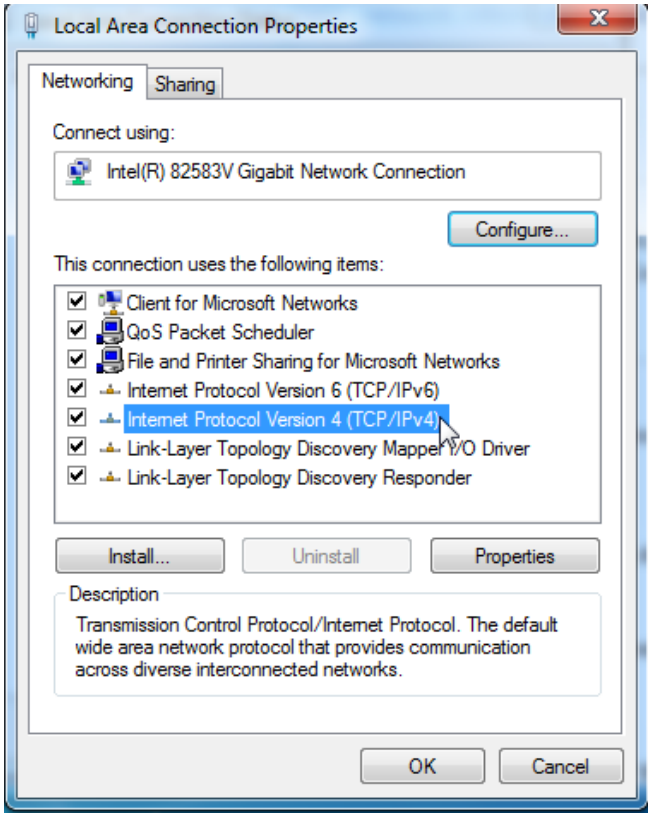
**Step 2** Click **Open Network and Sharing Center**.



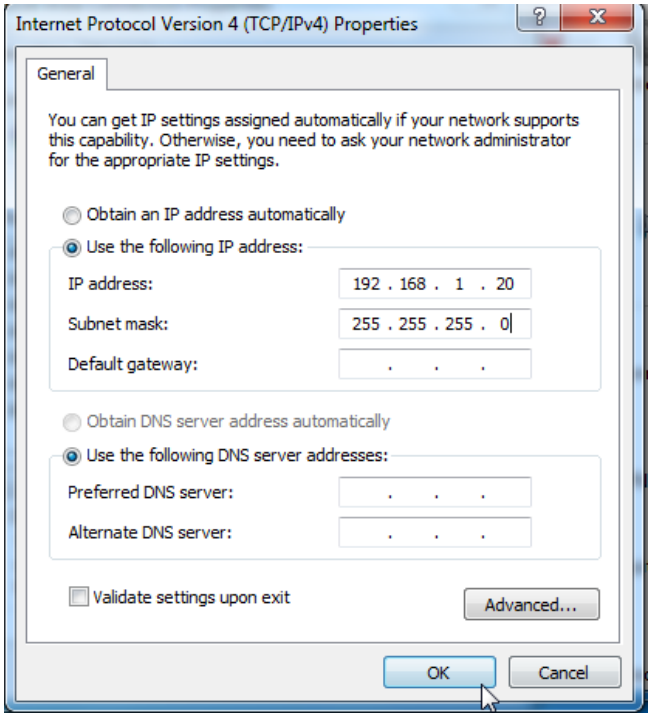

**Step 3** Click **Local Area Connection**, then click **Properties**.



**Step 4** Double-click **Internet Protocol Version 4 (TCP/IPv4)**.




**Step 5** Select **Use the following IP address**, set the **IP address** to **192.168.1.*X*** (*X* ranges from 2 to 253), the **Subnet mask** to **255.255.255.0**, and click **OK**.




6. Click **OK** on the **Local Area Connection Properties** window, and close the other windows.

**----End**

## Automatically obtaining an IP address

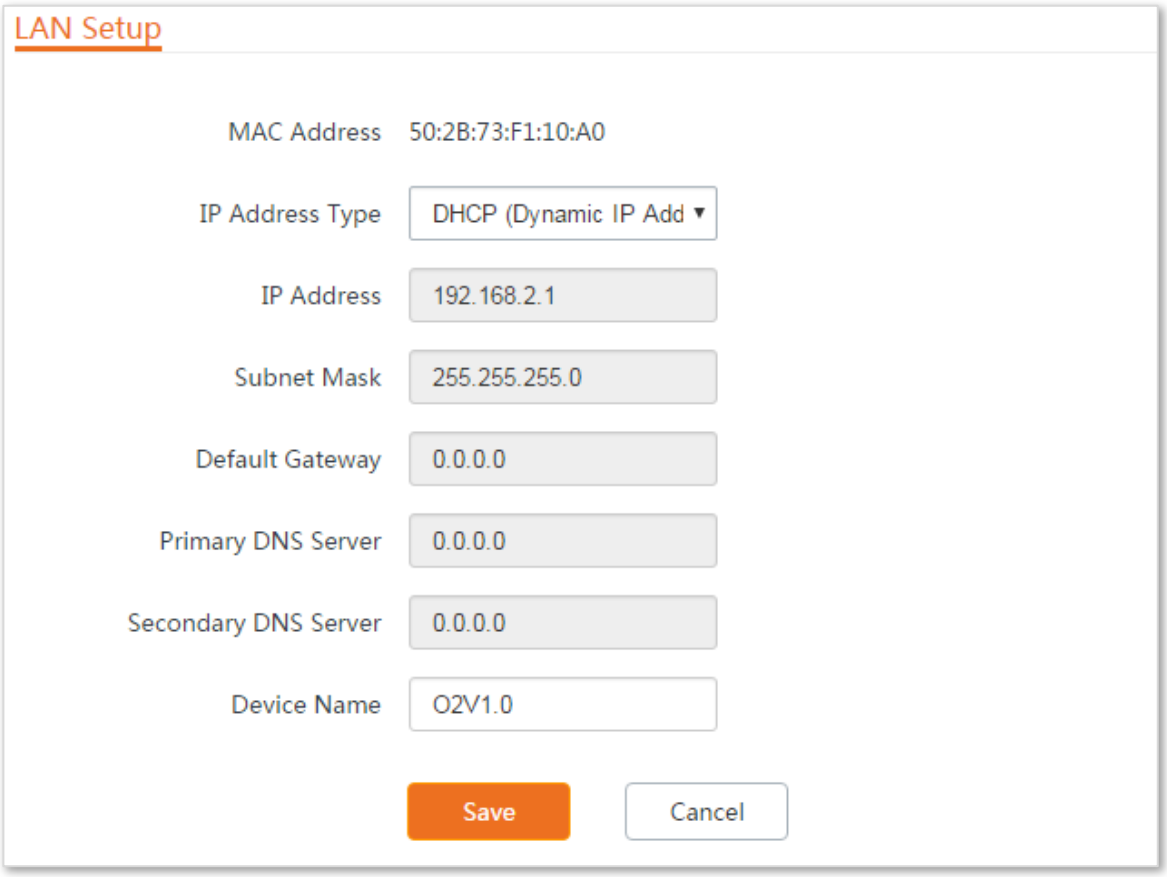
This mode enables the device to automatically obtain an IP address, a subnet mask, a gateway IP address, DNS server IP addresses assigned by the DHCP server of the upstream device. If a large number of devices are deployed, you can adopt this mode to prevent IP address conflicts and effectively reduce your workload.

**Configuration procedure:**

**Step 1** Choose **Network** > **LAN Setup** to enter the configuration page.

**Step 2** Set **IP Address Type** to **DHCP (Dynamic IP Address)**.

**Step 3** Click **Save**.




**----End**

After 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 steps in the **Manually setting the IP address** part to assign an IP address to the computer manually.

# 5.2 MAC clone

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

## 5.2.1 Overview

If the device 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 this device for internet access.

## 5.2.2 Cloning a MAC address

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

### Method 1

If you can find the computer that can access the internet after it connects to the modem directly, perform the following steps:

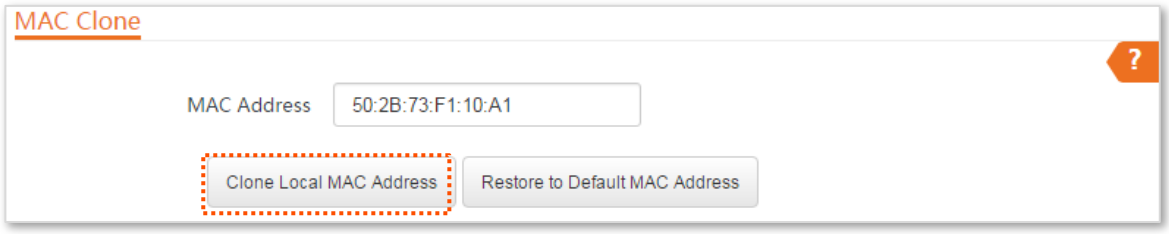
**Step 1** Connect the computer to the device.

**Step 2** Log in to the web UI.

**Step 3** Choose **Network** > **MAC Clone** to enter the configuration page.

**Step 4** Click **Clone Local MAC Address**.

**Step 5** Click **Save**.




**----End**

### Method 2

If you cannot find the computer that can access the internet after it connects to the modem directly, but you know the MAC address of this computer, perform the following steps:

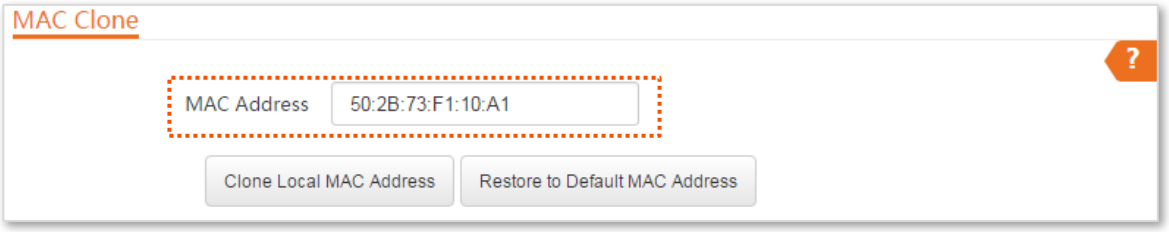
**Step 1** Connect another device (such as a smart phone or tablet) to the device.

**Step 2** Log in to the web UI.

**Step 3** Choose **Network** > **MAC Clone**.

**Step 4** Enter the MAC address of the computer that can access the internet in the **MAC Address** box.

**Step 5** Click **Save**.




**----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**.

# 5.3 DHCP server

## 5.3.1 Overview

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

TIP

If the new and original IP addresses of the LAN port belong to different network segment, the system changes the IP address pool of the DHCP server of the device, so that the IP address pool and the new IP address of the LAN port belong to the same network segment.

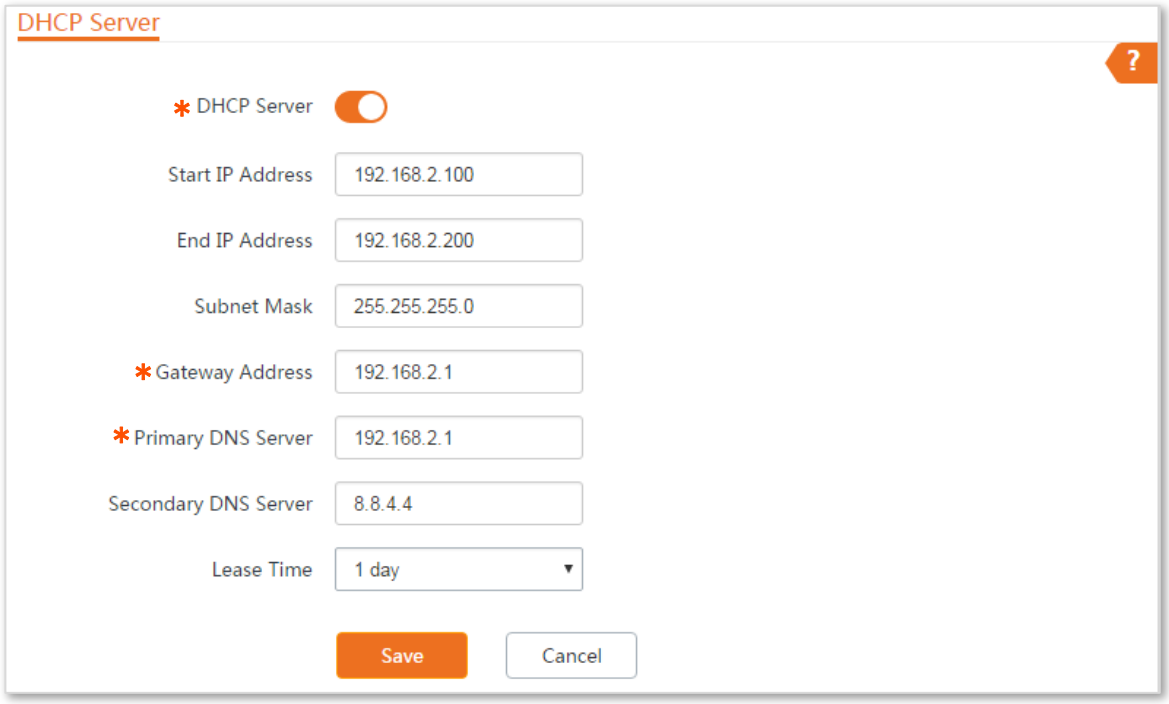
## 5.3.2 Configuring the DHCP server

**Step 1** Choose **Network** > **DHCP Server** to enter the configuration page.

**Step 2** Enable the **DHCP server**.

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

**Step 4** Click **Save**.




**----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.

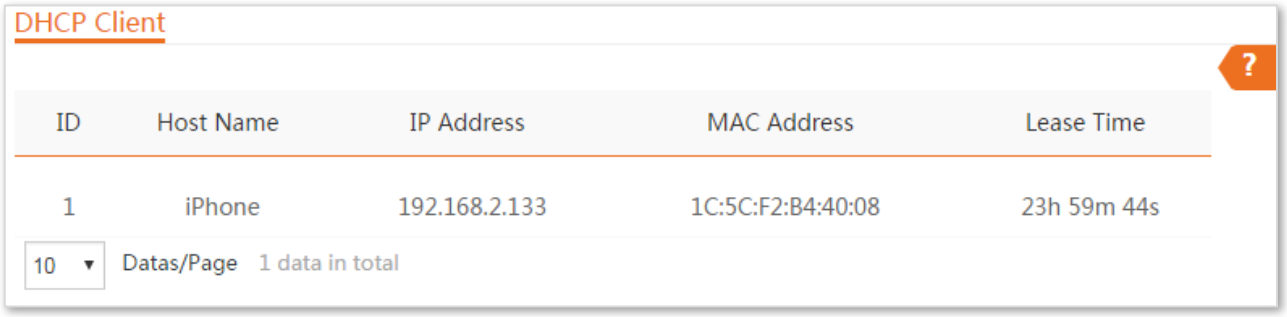
### Parameters description

| Name | Description |
| --- | --- |
| DHCP Server | It specifies whether to enable the DHCP server function of the device. By default, it is disabled. |
| 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**.<br> <br>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 to clients. The default value is **255.255.255.0**. |
| Gateway Address | It specifies the default IP address gateway assigned by the DHCP server to clients. Generally, it is the IP address of the LAN port of a router on the LAN. The default value is **192.168.2.254**.<br> <br>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 to clients. The default value is **8.8.8.8**.<br> <br>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 | It specifies the secondary DNS server IP address assigned by the DHCP server to clients. This parameter is optional. |
| Lease Time | It specifies the validity period of an IP address assigned by the DHCP server to a client.<br>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.<br>It is recommended that you retain the default value. |

# 5.4 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. The details include host names, IP addresses, MAC addresses, and lease time.

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



# 5.5 VLAN settings

## 5.5.1 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.

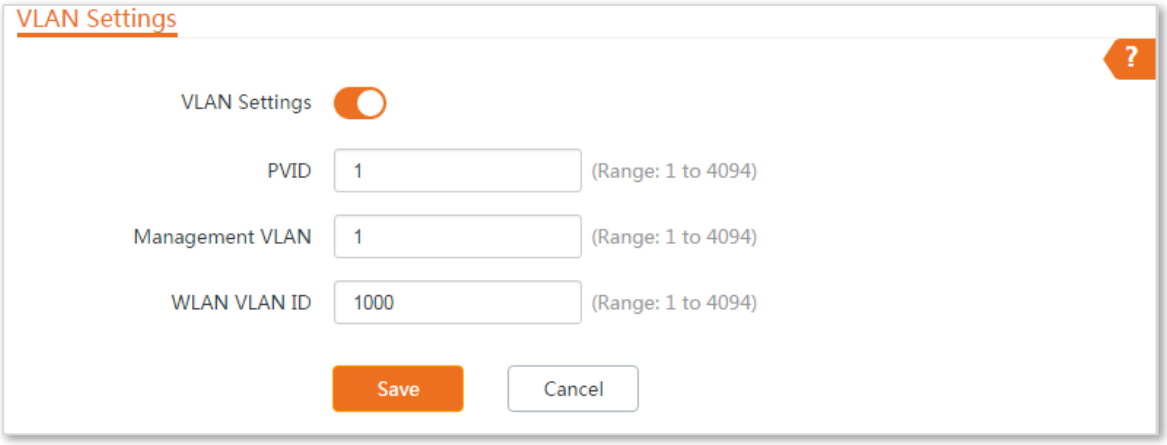
## 5.5.2 Setting up VLAN

**Step 1** Choose **Network** > **VLAN Settings** to enter the configuration page.

**Step 2** Enable the function.

**Step 3** Set the parameters as needed.

**Step 4** Click **Save**.




**----End**

**Parameters description**

| Name | Description |
|---|---|
| VLAN Settings | It specifies whether to enable the VLAN function of this device. By default, it is disabled. After the VLAN function is enabled, the PoE/LAN port is used as trunk port. |
| PVID | It specifies the ID of the default native VLAN of the trunk port. The default ID is **1**. After the VLAN function is enabled, the PoE/LAN port is used as trunk port. |
| 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**.<br><br>After the VLAN function is enabled, the WLAN interface functions as an access port, whose PVID is the same as VLAN ID. |

After the IEEE 802.1Q VLAN settings take effect, packet with tag will be forwards to the ports of the corresponding VLAN according to the VID of the packet, and packet without tag will be forwards 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:

| Link 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<br>VID ≠ PVID of the port, retain the tag in the packet and then forward it |

## 5.5.3 Example of configuring VLAN settings

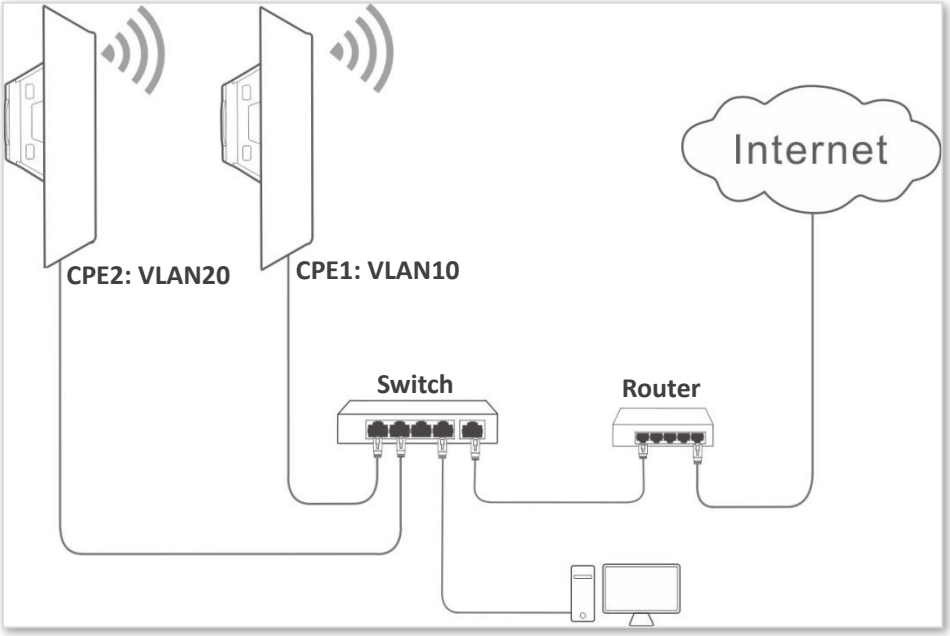
### Networking requirement

The devices connected to the same switch should belong to different VLANs.

**Assumption:**

CPE1 belongs to VLAN10, and CPE2 belongs to VLAN20.

### Network Topology



The connections of the switch:

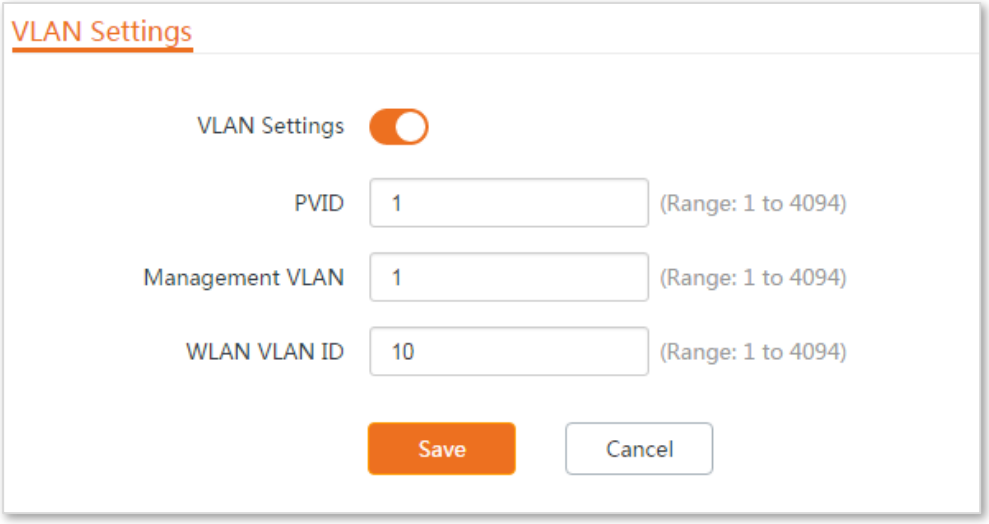
The router is connected to the uplink port.

- CPE1 is connected to port 1
- CPE2 is connected to port 2

## Configuration procedure

**Step 1** Set up CPE1.

1. Log in to the web UI of CPE1, and choose **Network** > **VLAN Settings**.
2. Enable the function.
3. Set **Management VLAN** to **1**.
4. Set **WLAN VLAN ID** to **10**.
5. Click **Save**.




6. Click **OK** on the pop-up window, and wait until the CPE1 completes reboot.

**Step 2** Set up CPE2 according to the steps in step 1.

**Step 3** Set up the switch.

**The following table shows the configuration on the switch:**

| 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 CPE1) | 1,10 | Trunk | 1 |

| | | | |
|---|---|---|---|
| Port 2 (Connected to CPE2) | 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.

**The following form shows the configuration on the router:**

| 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 first client connected to the CPE obtains an IP address and related parameters from the DHCP server belonging to VLAN10, and the second client obtains these parameters from the DHCP sever belonging to VLAN20.

# 6 Wireless

## 6.1 Basic

### 6.1.1 Overview

This module enables you to set basic wireless settings of the device, including SSID-related parameters, network mode, channel, transmit power and so on.

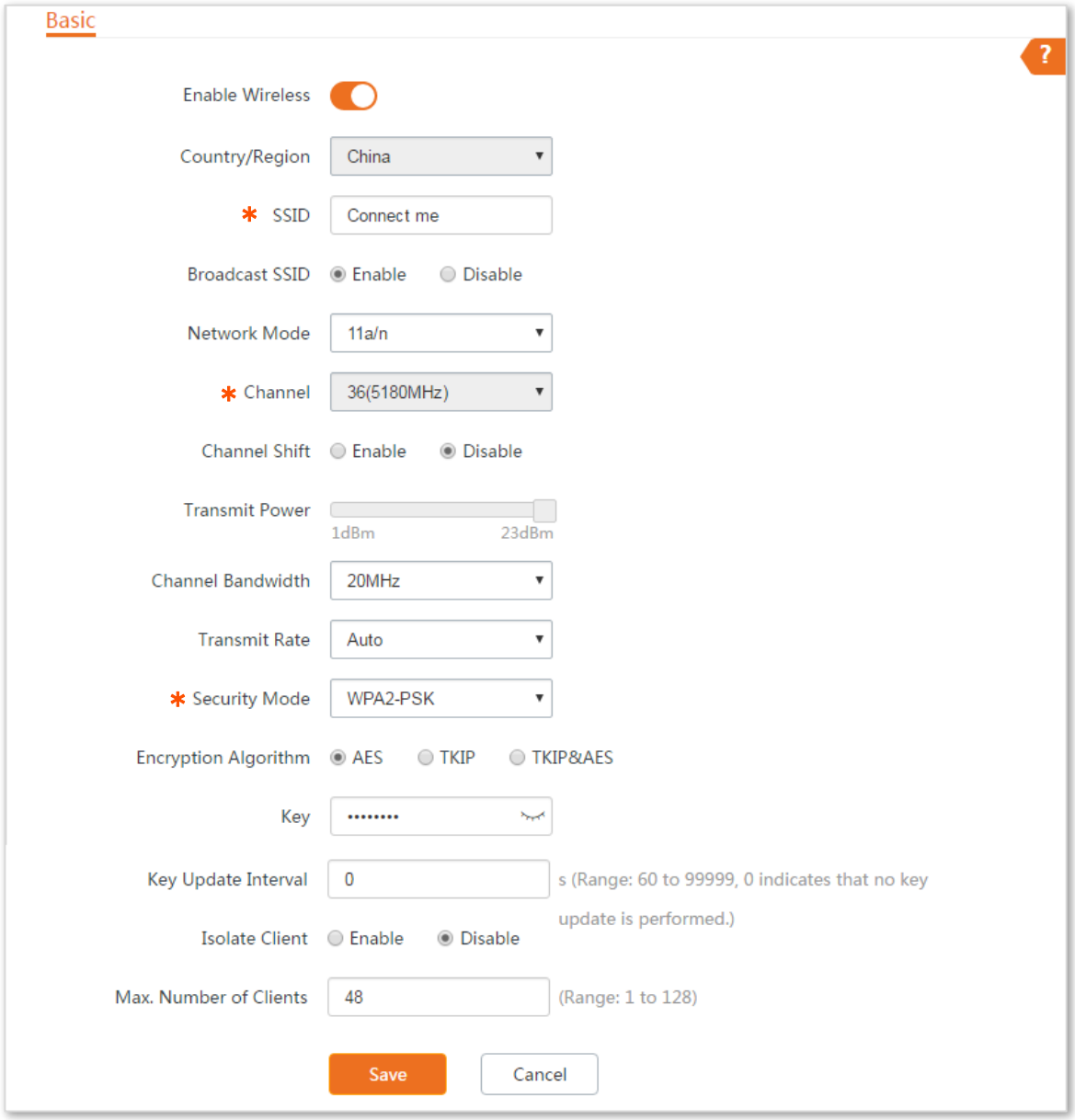
### 6.1.2 Changing the basic settings

To change the basic settings of an SSID, perform the following procedure:

**Step 1** Choose **Wireless** > **Basic**.

**Step 2** Change the parameters as required. Generally, you only need to enable the wireless function, and change **SSID**, **Channel** and **Security Mode** settings.

**Step 3** Click **Save**.




**----End**

## Parameters description

| Name | 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.<br>When the device broadcasts an SSID, nearby 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 |

| Name | Description |
| --- | --- |
| | 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.<br><br>It is worth noting that after Broadcast SSID is set to Disable, a hacker can still connect to the corresponding wireless network if he/she manages to obtain the SSID by other means. |
| Network Mode | It specifies the wireless network mode of this device. The available options include 11a, 11n, and 11 a/n.<br><br>**11a**: It indicates that clients compliant with the 802.11a protocol can connect to the device.<br><br>**11n**: It indicates that clients working at 5 GHz and compliant with 802.11n can connect to the device.<br><br>**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.<br><br>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.<br><br>**10MHz**: It indicates that the channel bandwidth of the device is 10 MHz.<br><br>**20MHz**: It indicates that the channel bandwidth of the device is 20 MHz.<br><br>**30MHz**: It indicates that the channel bandwidth of the device is 30 MHz.<br><br>**40MHz**: It indicates that the channel bandwidth of the device is 40 MHz.<br><br>**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 transmission rate of the device.<br><br>When the channel bandwidth is set to 10 MHz, the rate automatically reduces, and the maximum rate is 72.2 Mbps.<br><br>When the channel bandwidth is set to 20 MHz, the rate automatically reduces, and the maximum rate is 144.4 Mbps.<br><br>When the channel bandwidth is set to 30 MHz, the rate automatically reduces, and the maximum rate is 216.6 Mbps. |

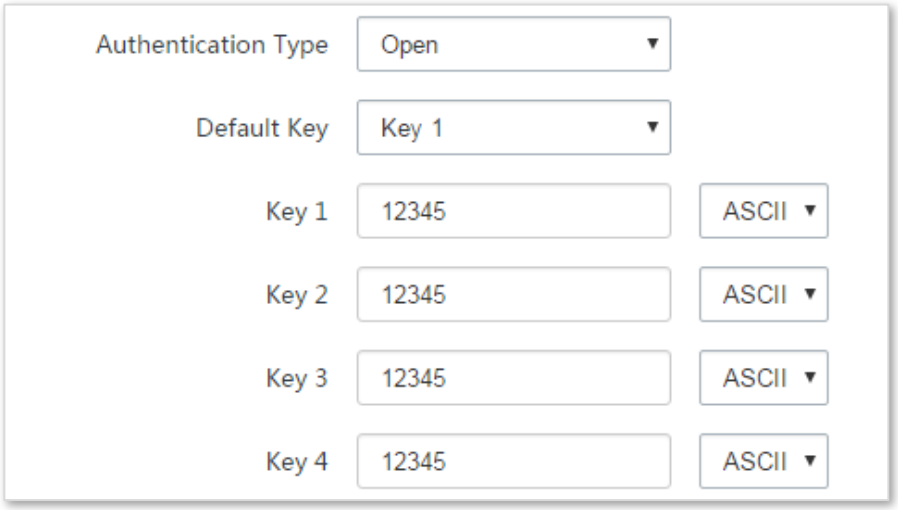
| Name | Description |
| --- | --- |
| | When the channel bandwidth is set to 40 MHz, the maximum rate is 300 Mbps.<br><br>When the channel bandwidth is set to Auto, the maximum rate is 300 Mbps. |
| Security Mode | A wireless network uses radio, which is open to the public, as its data transmission 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.<br><br>The device supports various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2.<br><br>**None**: It indicates that any wireless client can connect to the wireless network. This option is not recommended because it affects network security.<br><br>**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.<br><br>**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.<br><br>WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK adopt a pre-shared key for authentication, while the AP 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 AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.<br><br>To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use 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.<br><br>**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 the AES, TKIP, and TKIP&AES values.<br><br>**AES**: It indicates the Advanced Encryption Standard.<br><br>**TKIP**: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum |

| Name | Description |
| --- | --- |
| | wireless throughput of the AP is limited to 54 Mbps.<br><br>**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. The value **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. |

## None

It indicates that any wireless client can connect to the wireless network. Choose this option only when necessary.

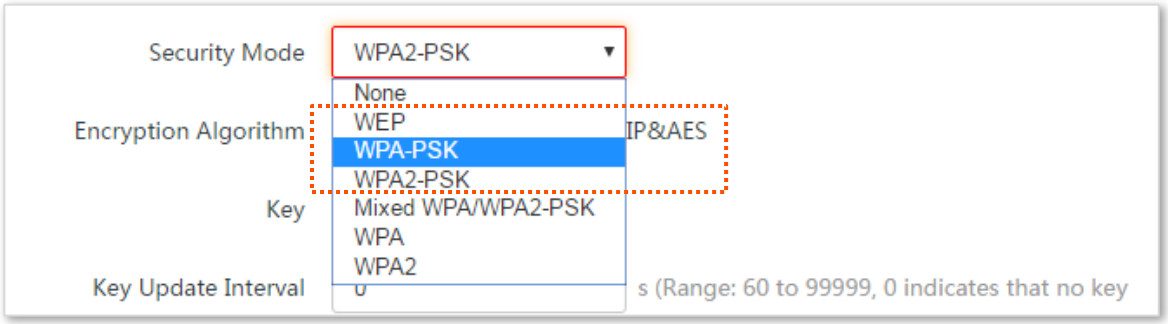
## WEP




**Parameters description**

| Name | 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.<br><br>**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.<br><br>**Shared**: It specifies that a shared key is used for authentication and data 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.<br><br>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 hexadecimal characters.<br><br>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.<br><br>10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key. |

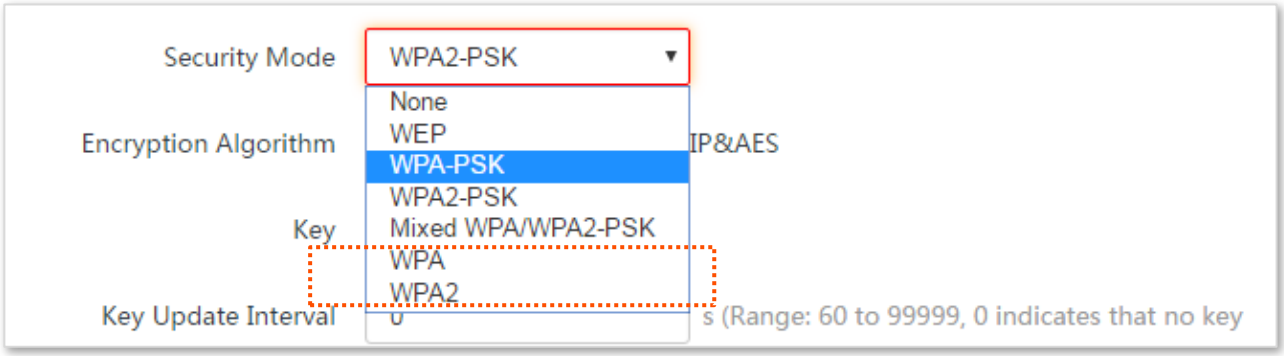
## WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK

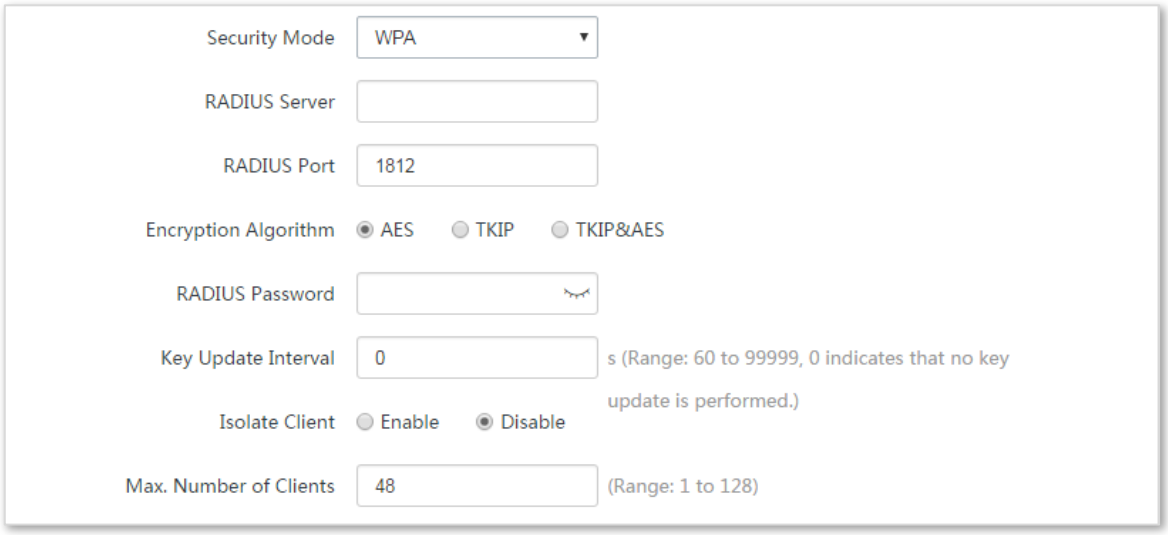


### Parameters description

| Name | Description |
|---|---|
| Security Mode | It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK.<br><br>**WPA-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA-PSK.<br><br>**WPA2-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2-PSK.<br><br>**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.<br><br>**AES**: It indicates the Advanced Encryption Standard.<br><br>**TKIP**: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps.<br><br>**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.<br><br>The value 0 indicates that a WAP key is not updated. |

## WPA and WPA2






## Parameters description

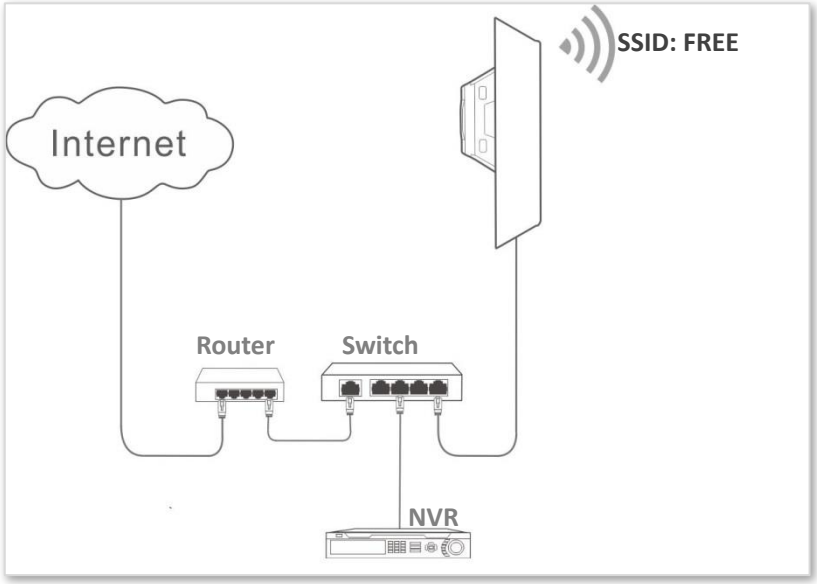
| Name | Description |
|---|---|
| Security Mode | The **WPA** and **WPA2** options are available for network protection with a RADIUS server.<br>**WPA**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA.<br>**WPA**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA. |
| 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**.<br>**AES**: It indicates the Advanced Encryption Standard.<br>**TKIP**: It indicates the Temporal Key Integrity Protocol.<br>**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 Update Interval | It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.<br>The value 0 indicates that a WAP key is not updated. |

## 6.1.3 Example of configuring basic settings

### Setting up a non-encrypted wireless network

#### Networking requirement

A residential community uses the devices to deploy its network for video surveillance. It requires that the SSID is FREE and there is no WiFi password.




#### Configuration procedure

Assume that the second SSID of the AP, the WPA2-PSK security mode, and AES encryption algorithm are used.

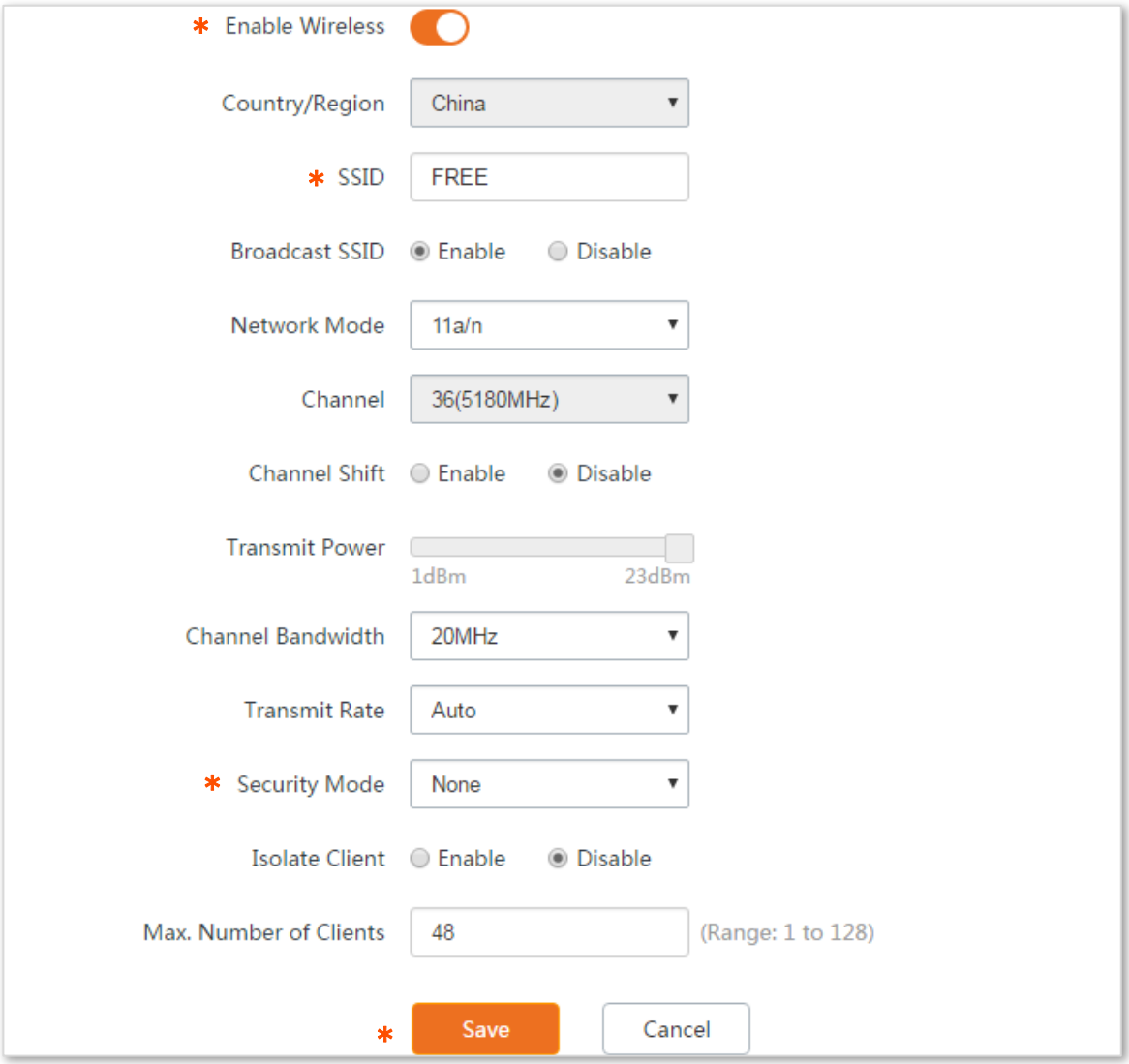
**Step 1** Choose **Wireless** > **Basic**.

**Step 2** Enable the wireless function.

**Step 3** Change the value of the **SSID** text box to **FREE**.

**Step 4** Set **Security Mode** to **None**.

**Step 5** Click **Save**.




**----End**

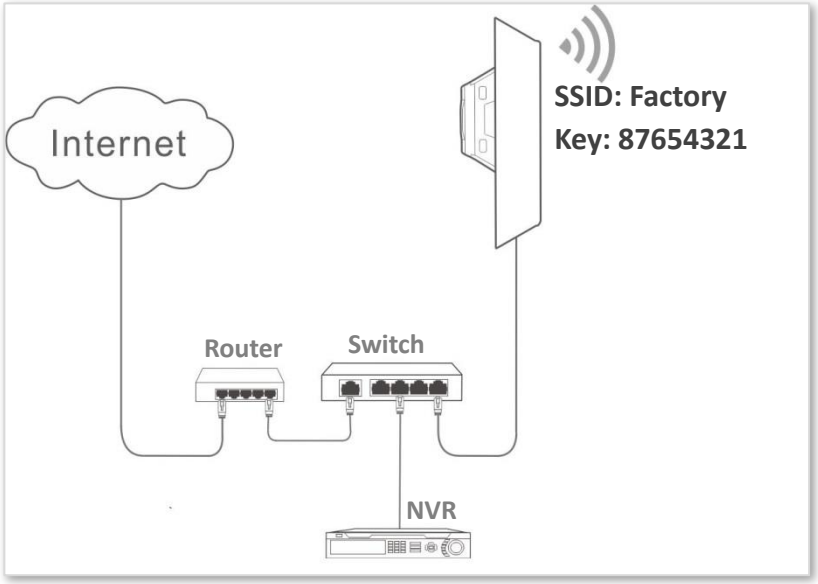
**Verification**

Verify that wireless devices can connect to the wireless network whose SSID is FREE without a password.

## Setting up a wireless network encrypted using WPA2-PSK

### Networking requirement

A factory's surveillance network with a certain level of security must be set up through a simply procedure. In this case, WPA2-PSK mode is recommended. See the following figure.




### Configuration procedure

Assume that the second SSID of the AP, the WPA2-PSK security mode, and AES encryption algorithm are used.

**Step 1** Choose **Wireless** > **Basic**.

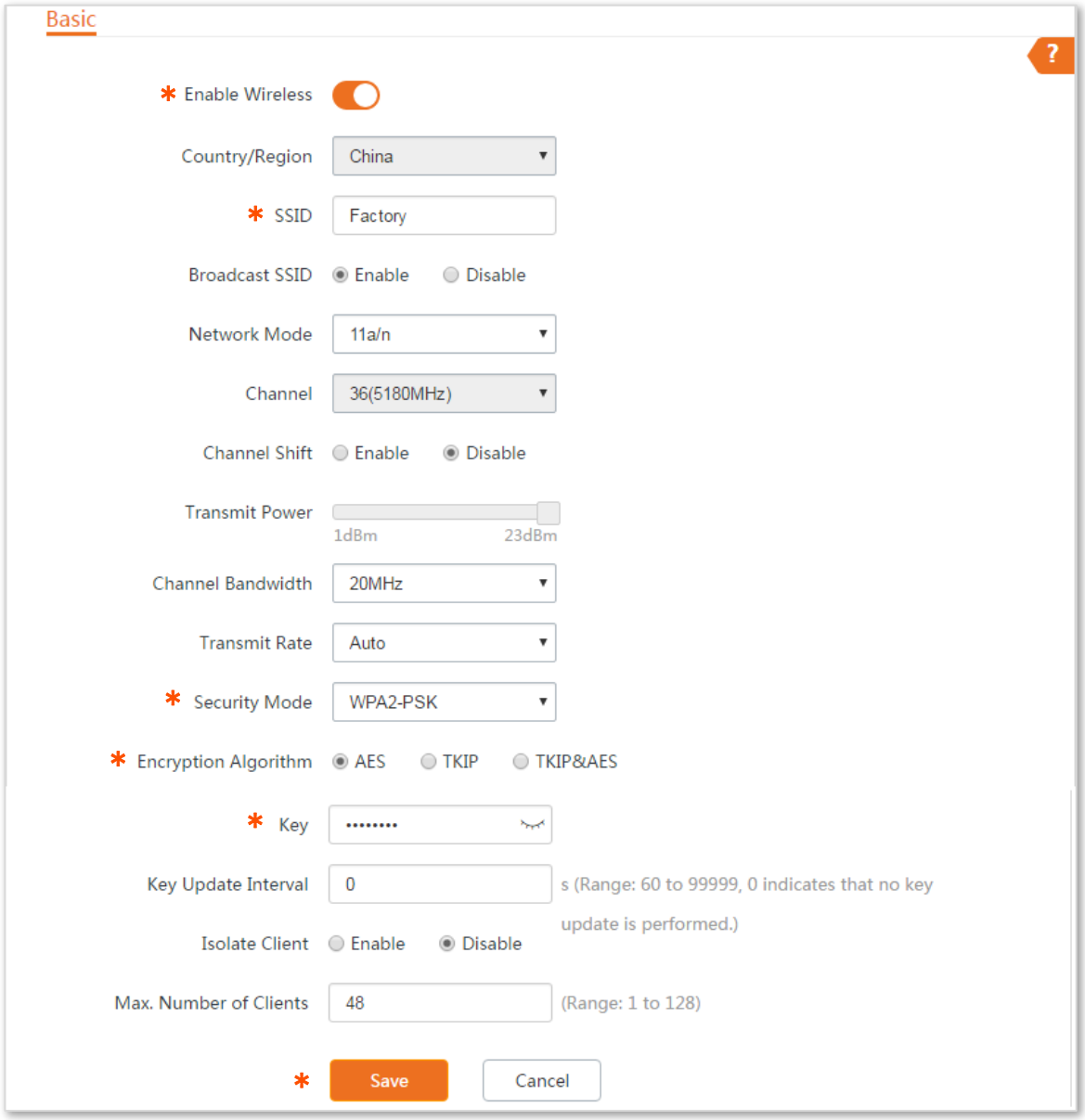
**Step 2** Enable the wireless function.

**Step 3** Change the value of the SSID text box to **Factory**.

**Step 4** Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.

**Step 5** Set **Key** to **87654321**.

**Step 6** Click **Save**.




**----End**

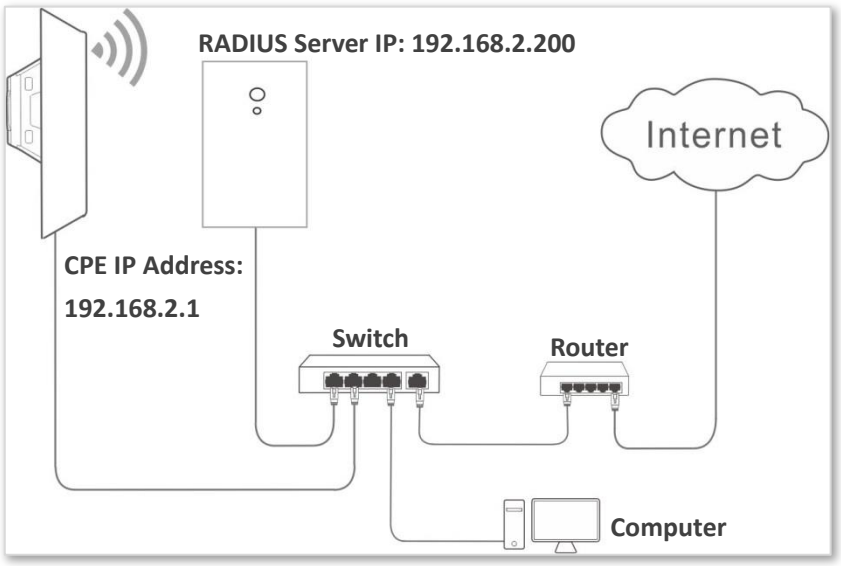
## Verification

Verify that wireless devices can connect to the wireless network named **Factory** with the password **87654321**.

## Setting up a wireless network encrypted using WPA or WPA2

### Networking requirement

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




### Configuration procedure

#### Configure the device

Assume that the IP address of the RADIUS server is 192.168.0.200, the Key is 12345678, and the port number for authentication is 1812.

Assume that the second SSID of the AP is used.

**Step 1** Choose **Wireless** > **Basic**, and enable the wireless function.

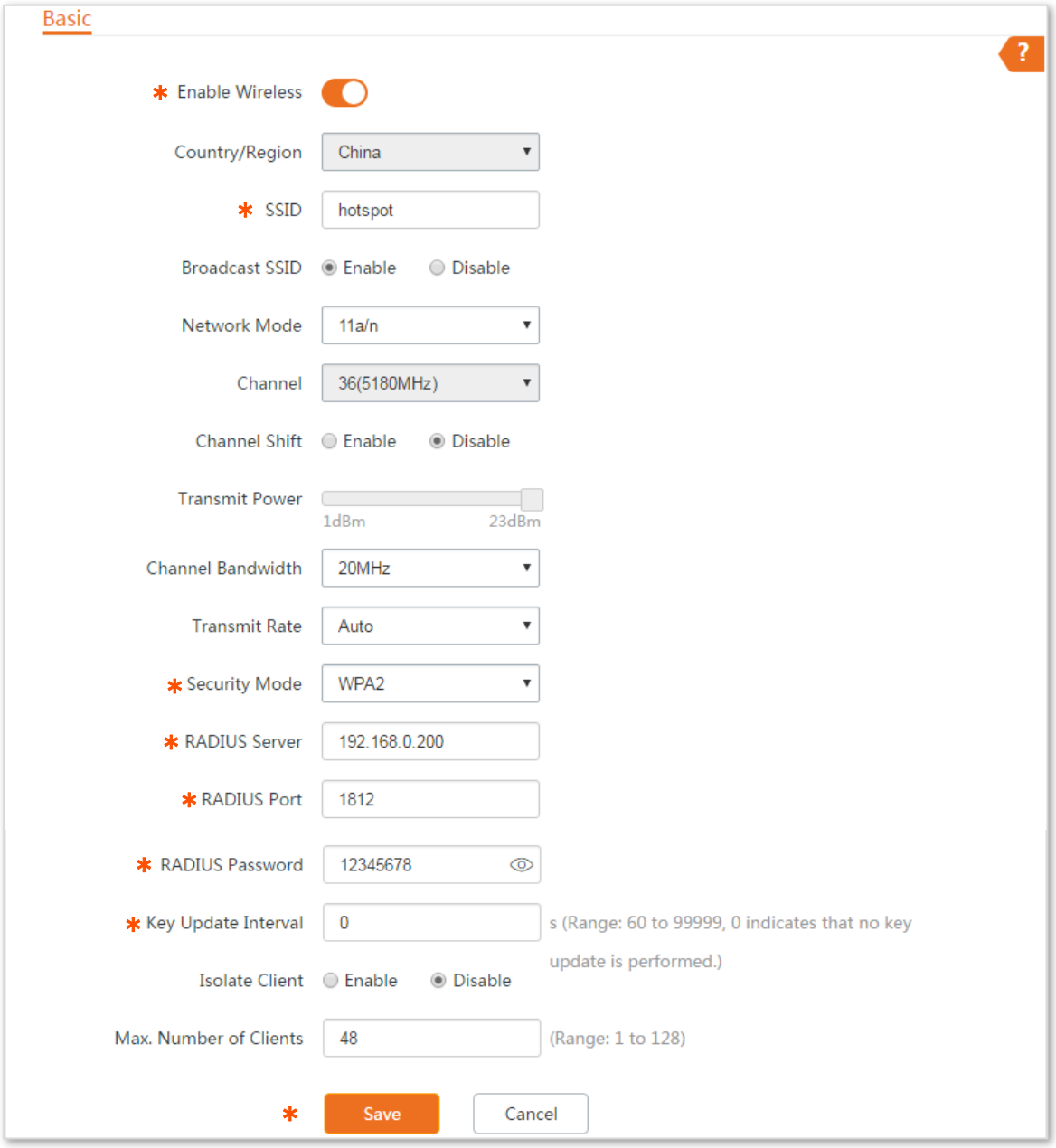
**Step 2** Change the value of the SSID text box to **hotspot**.

**Step 3** Set **Security Mode** to **WPA2**.

**Step 4** Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Password** to **192.168.0.200**, **1812**, and **12345678** respectively.

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

**Step 6** Click **Save**.




**----End**

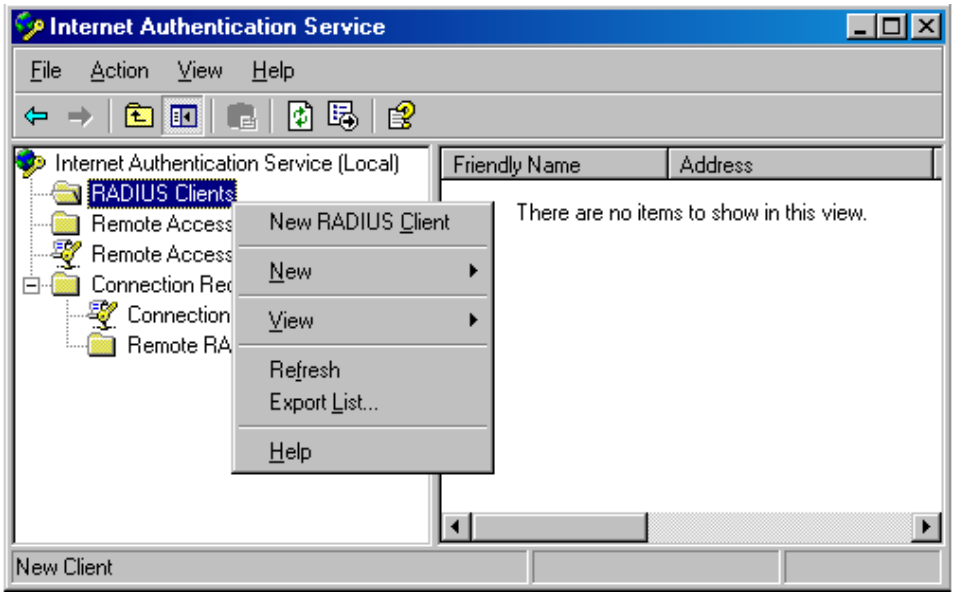
### Configure the RADIUS server

TIP

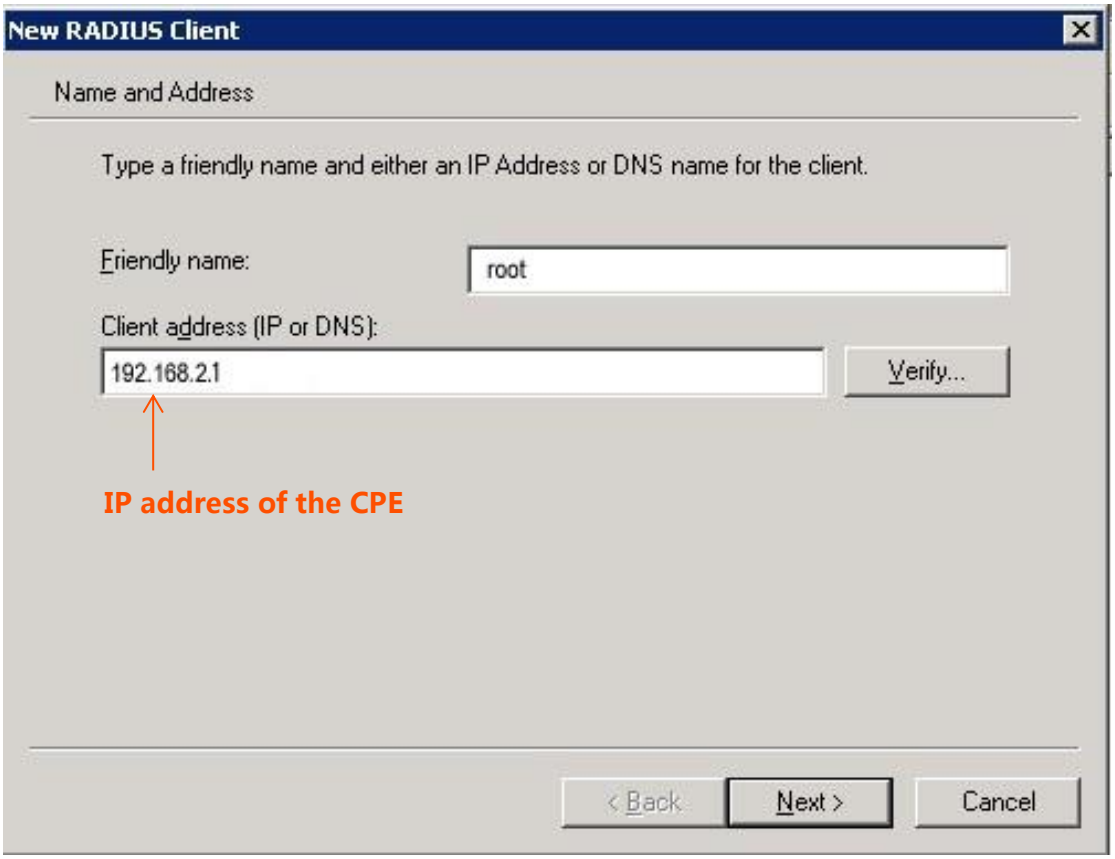
Windows 2003 is used as an example to describe how to configure the RADIUS server.

**Step 1** Configure a RADIUS client.

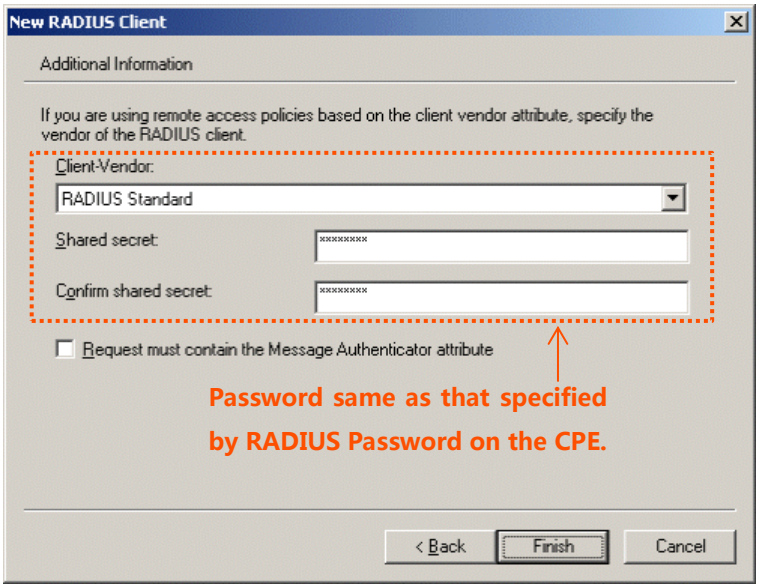
1. In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.




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

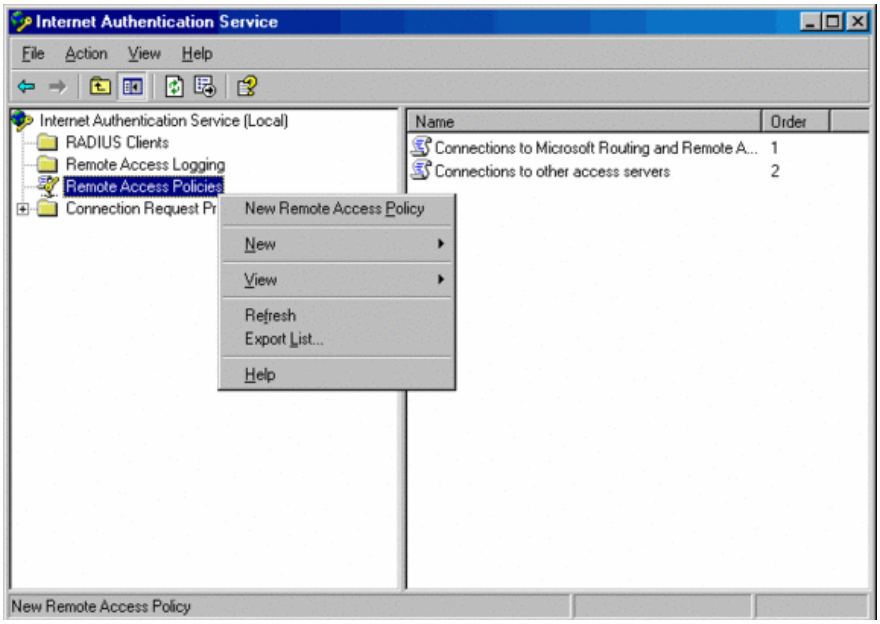



3. Enter **12345678** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.

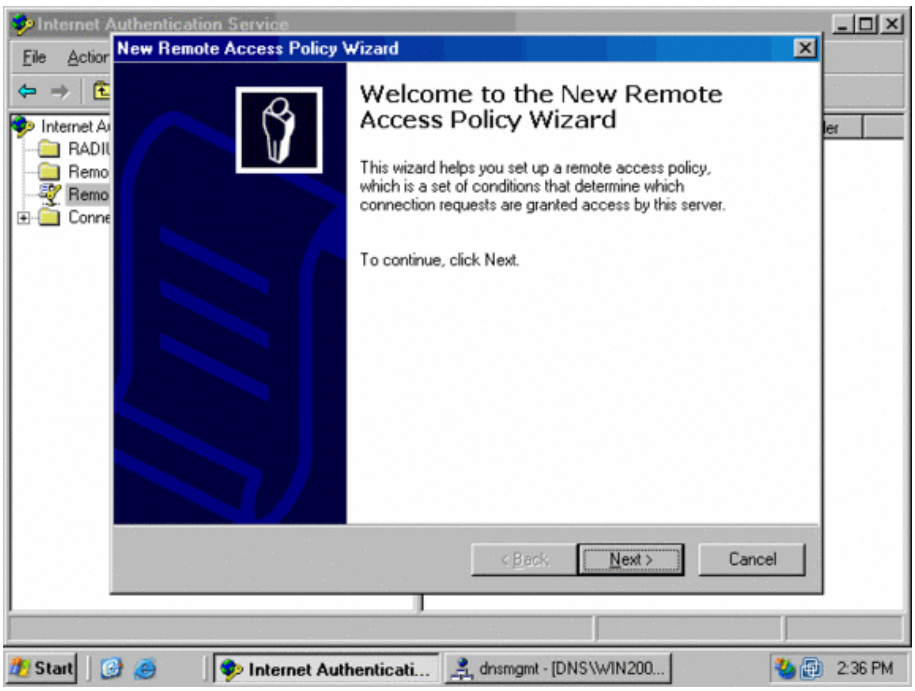



**Step 2** Configure a remote access policy.

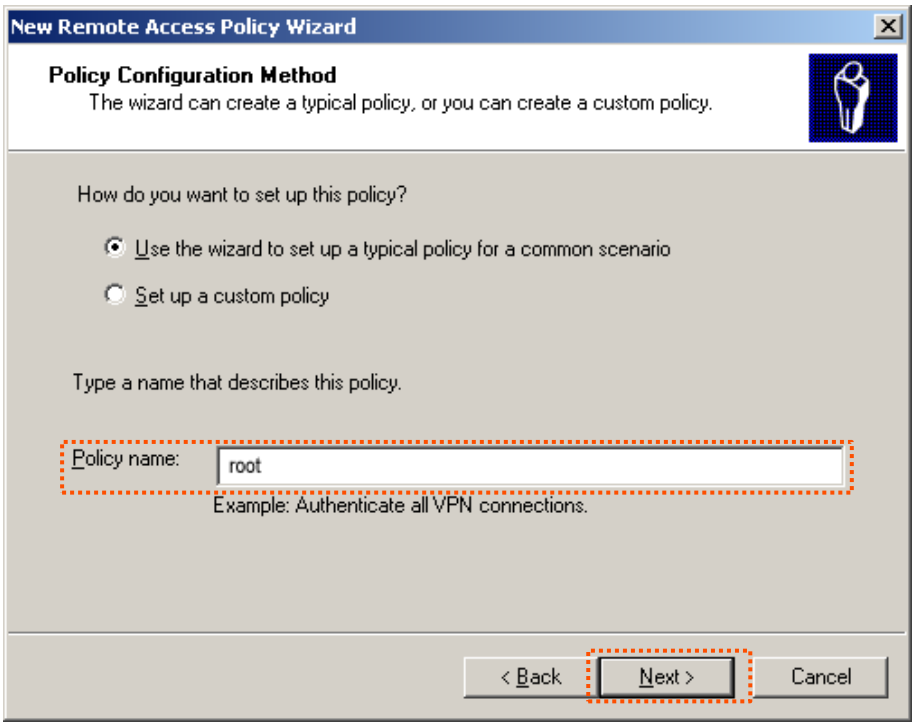
Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



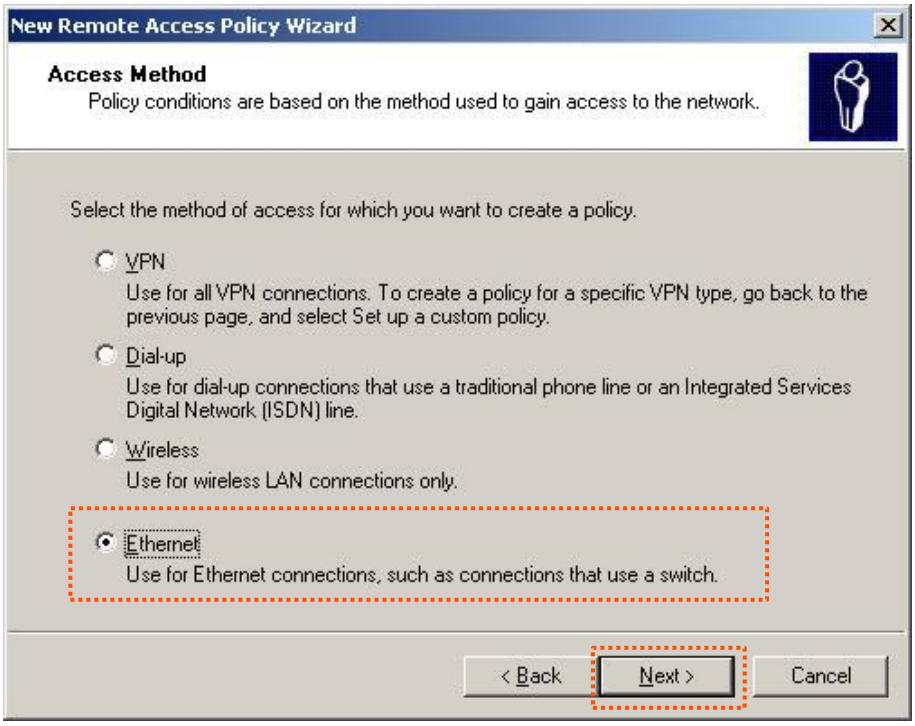

4. In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.



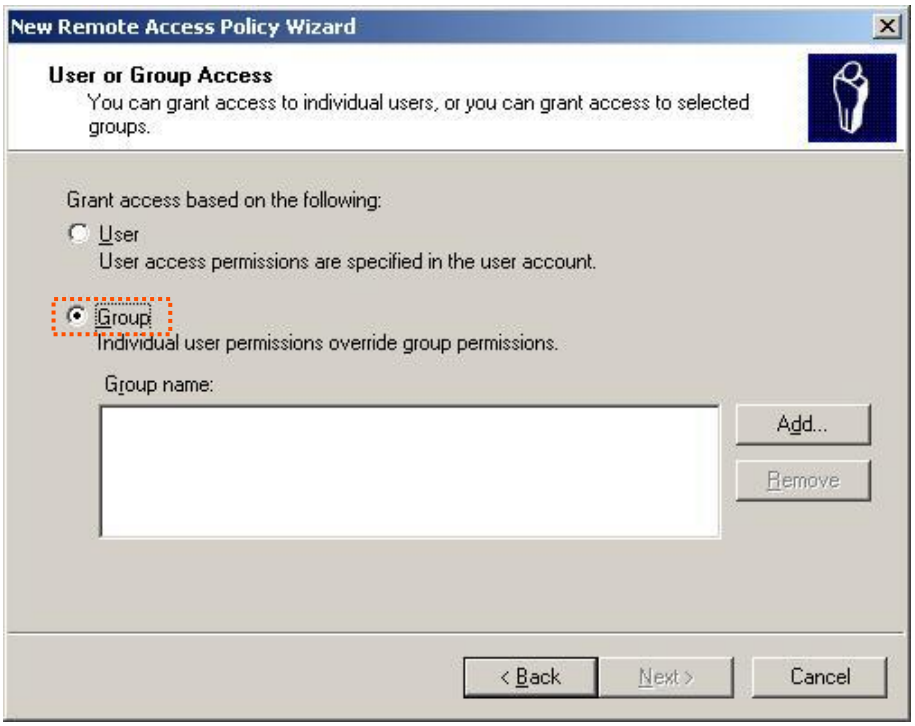

5. Enter a policy name and click **Next**.



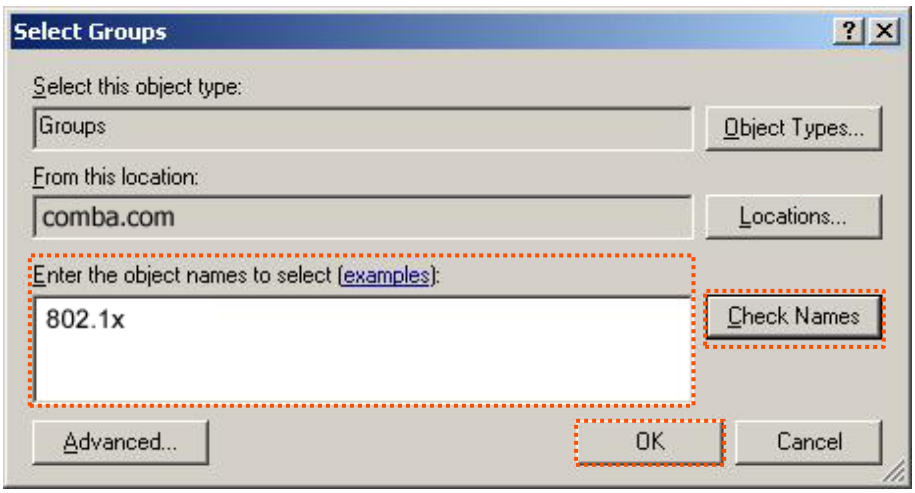
6. Select **Ethernet** and click **Next**.



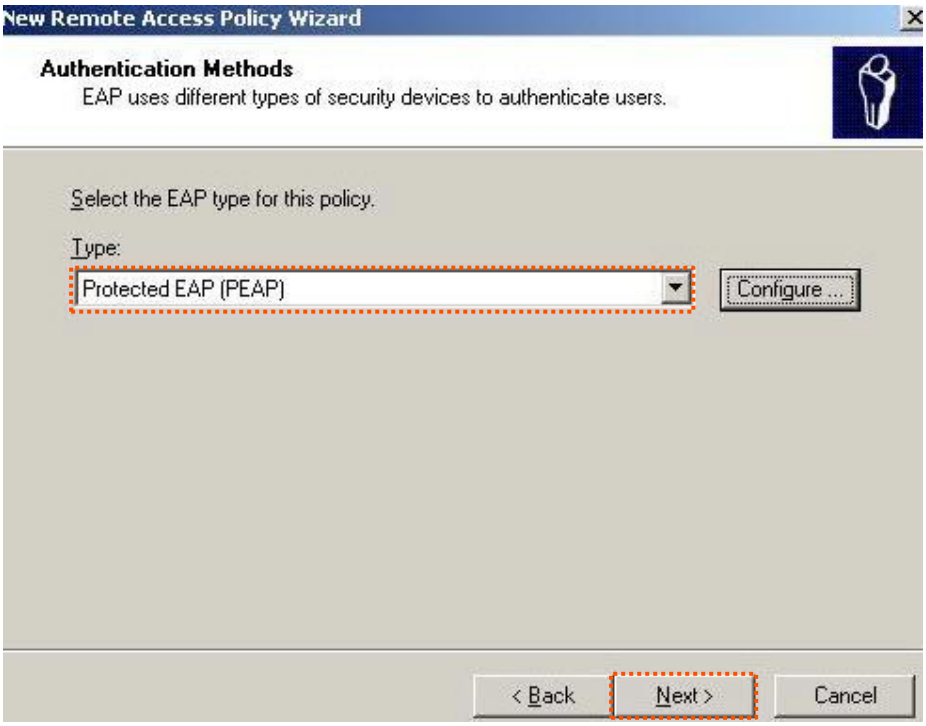

7. Select **Group** and click **Add**.



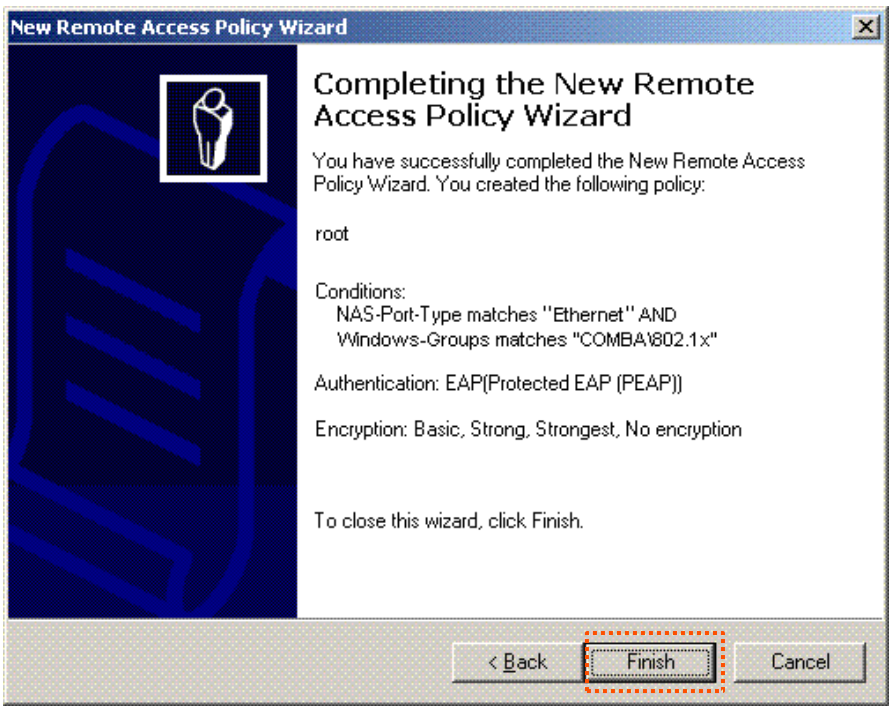

8. Enter **802.1x** in the **Ente**r the object names to select text box, click **Check Names**, and click **OK**.



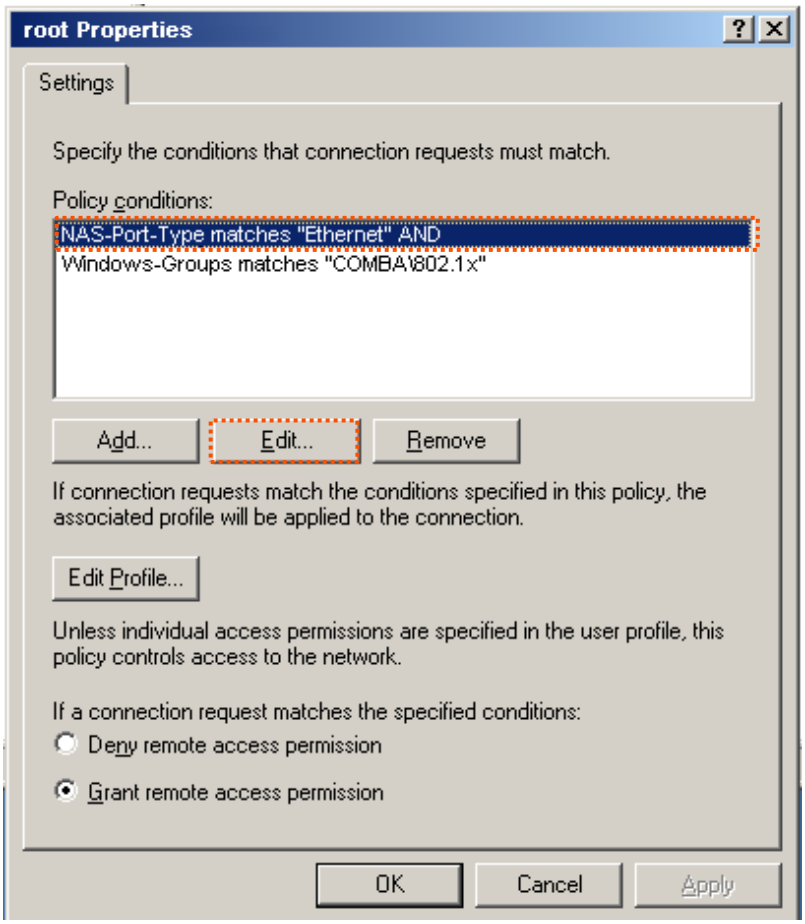

9. Select **Protected EAP (PEAP)** and click **Next**.



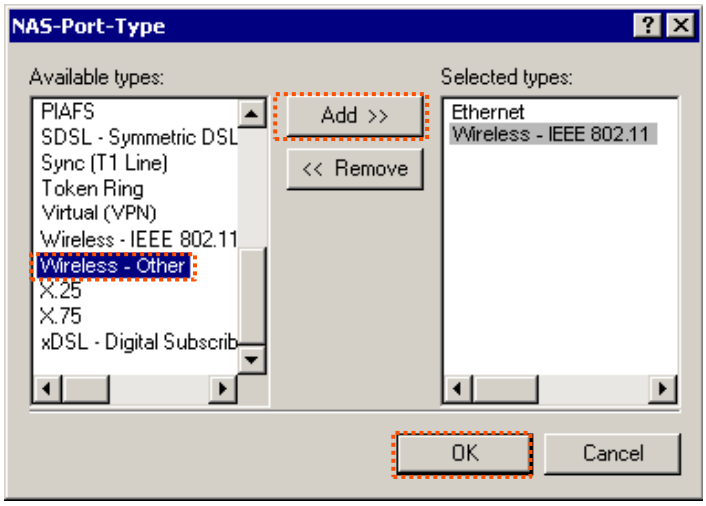

10. Click **Finish**. The remote access policy is created.



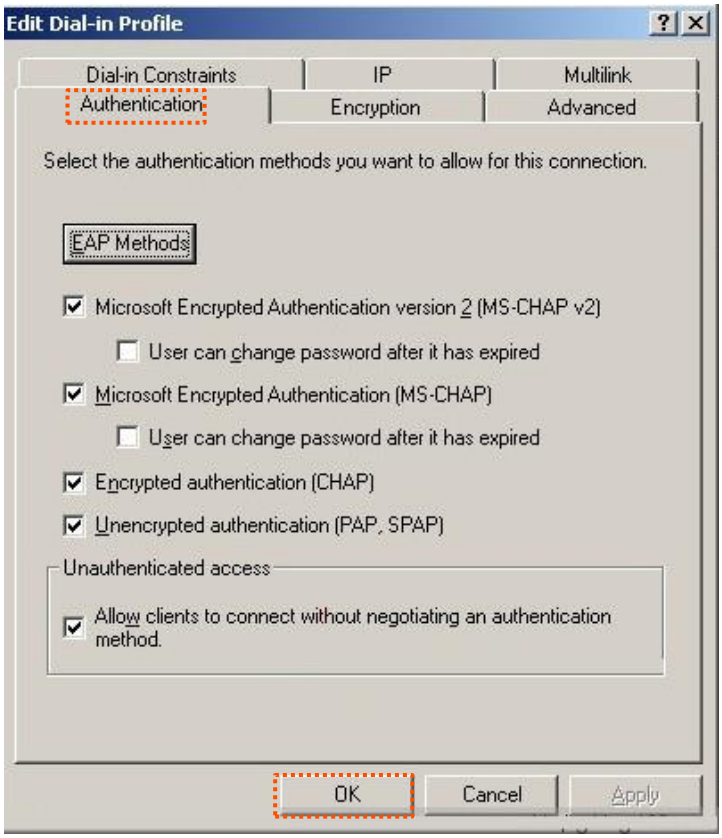

**11.** Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



12. Select **Wireless – Other**, click **Add**, and click **OK**.




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




14. When a message appears, click **No**.

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

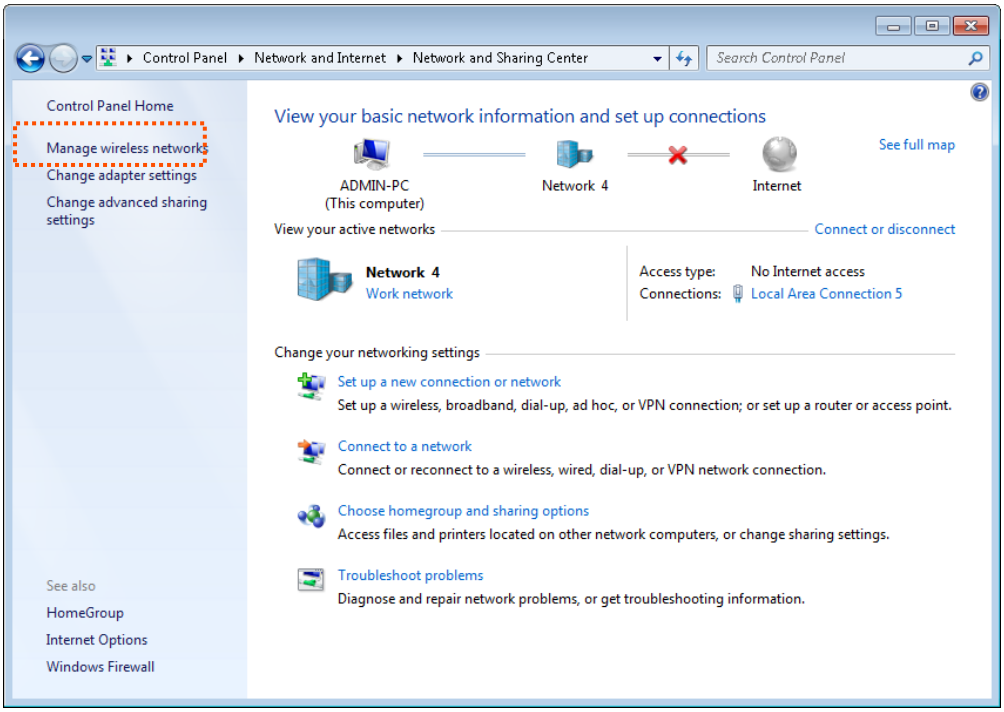
**----End**

## Configure your wireless device

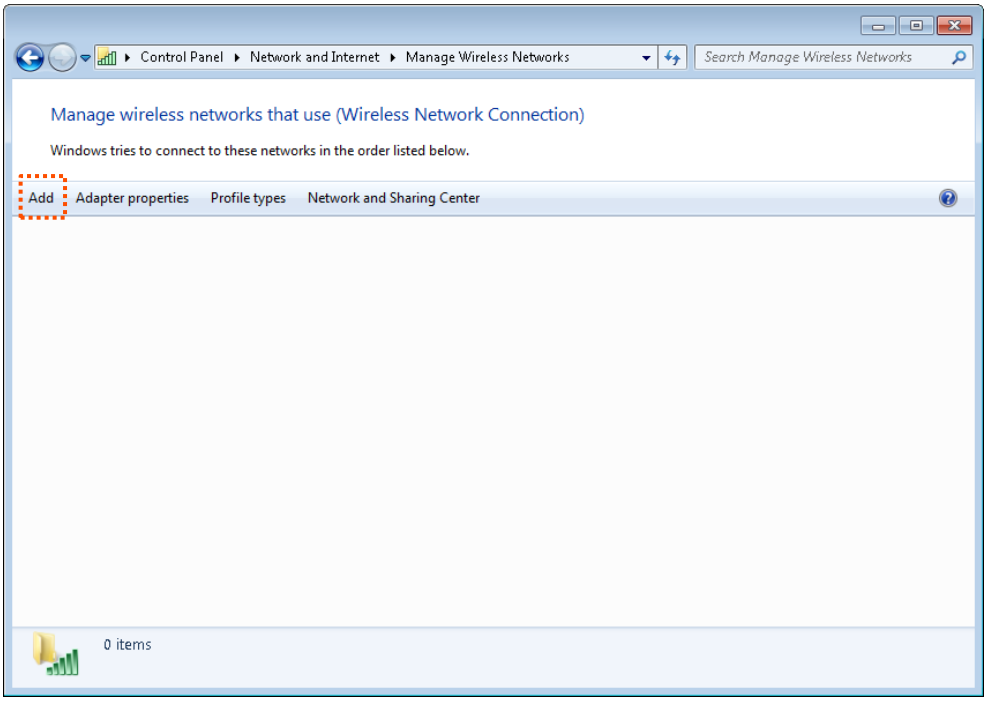
TIP

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

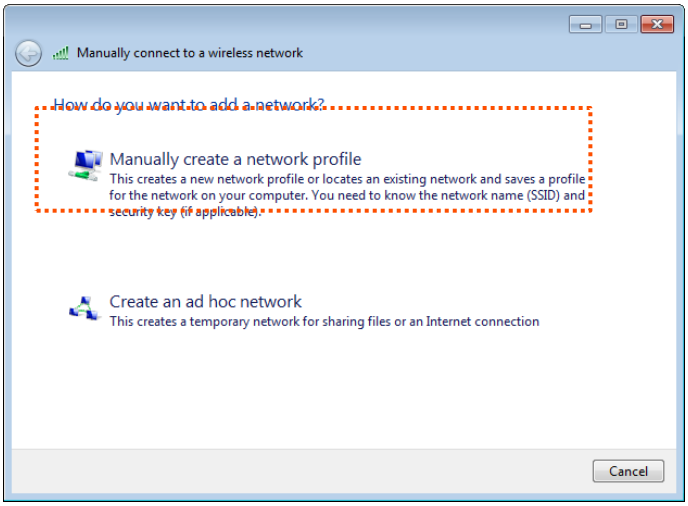
**Step 1** Choose **Start** > **Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



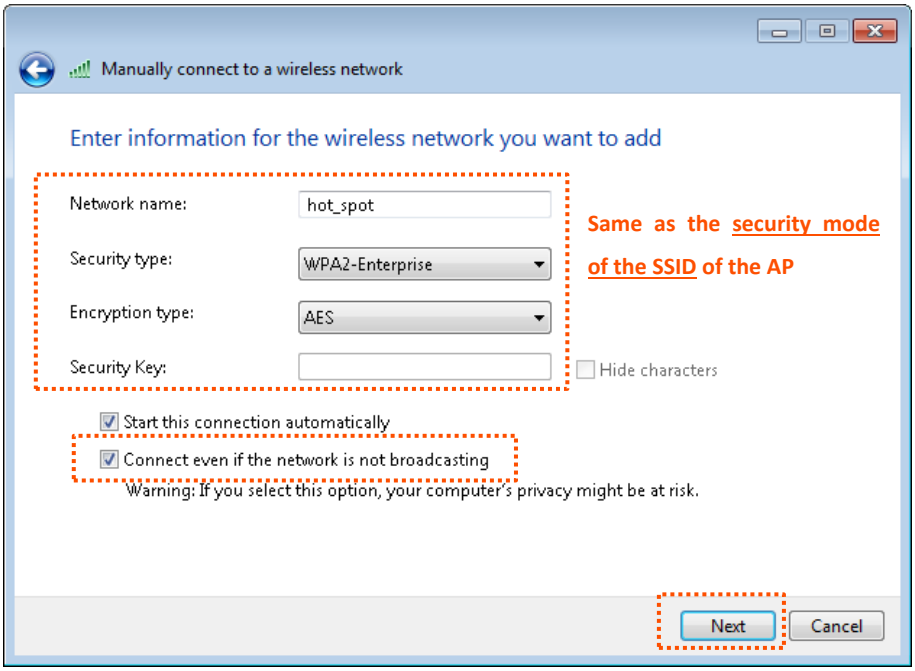

**Step 2** Click **Add**.



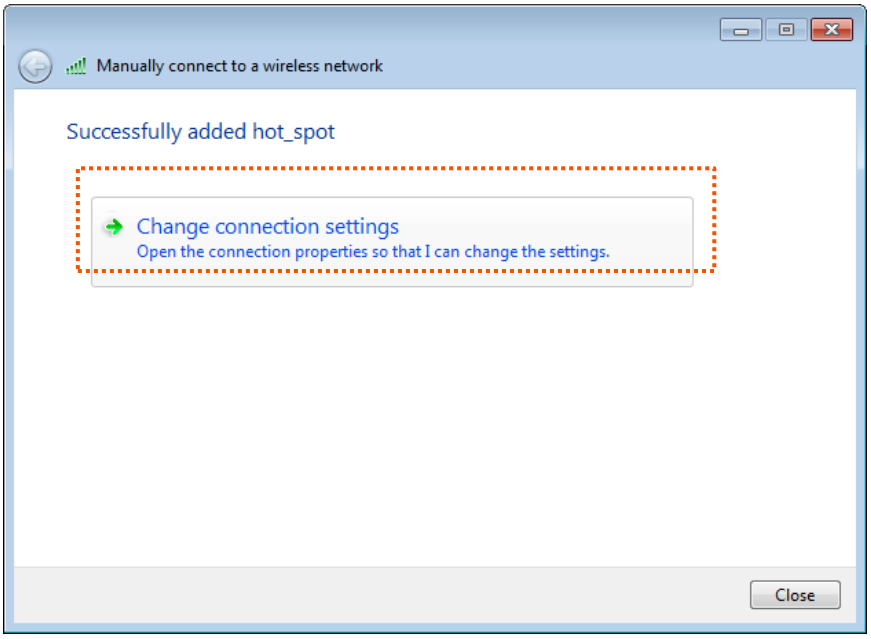
**Step 3** Click **Manually create a network profile**.



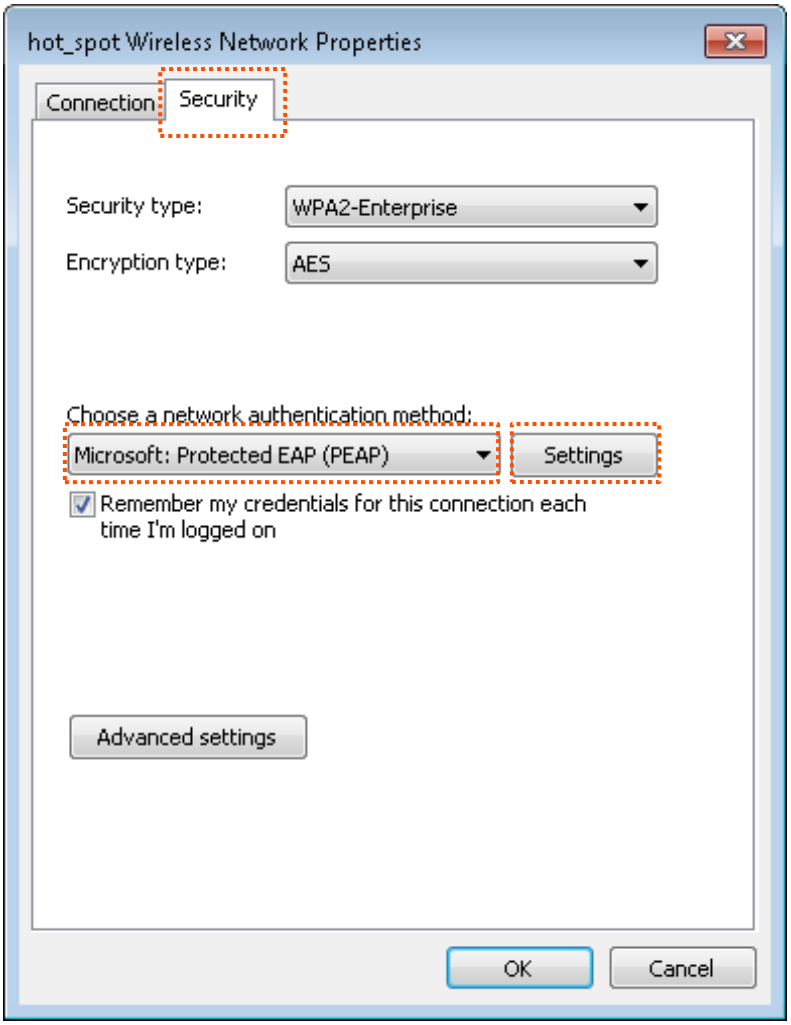

**Step 4** Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.



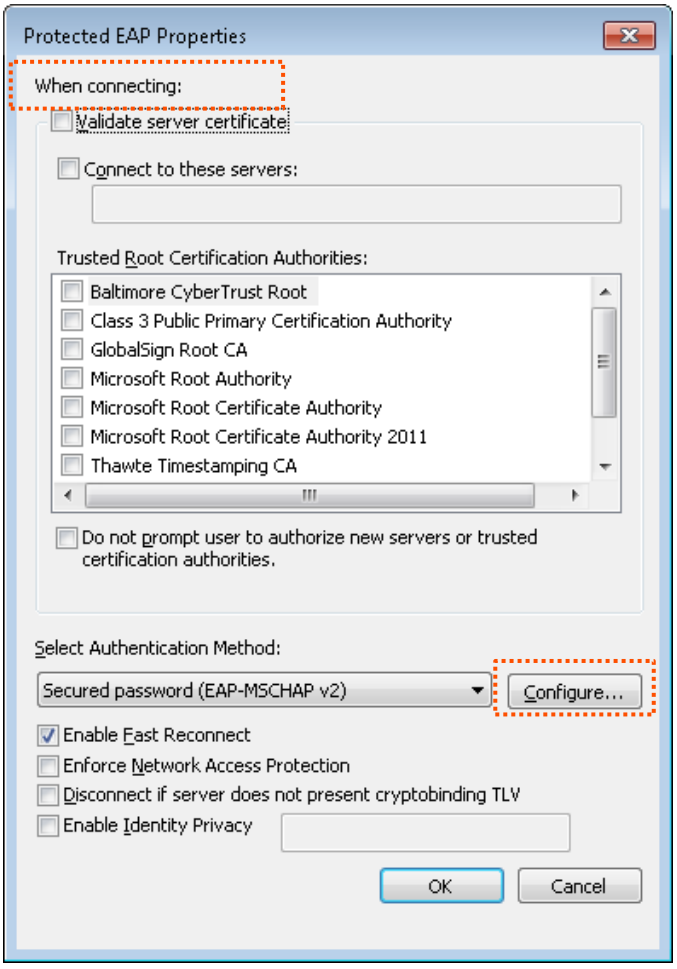
**Step 5** Click **Change connection settings**.



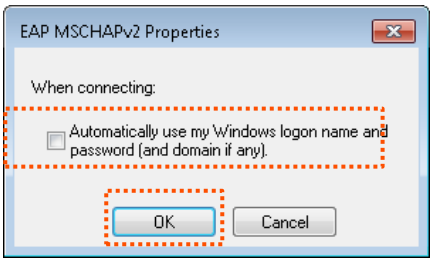

**Step 6** Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



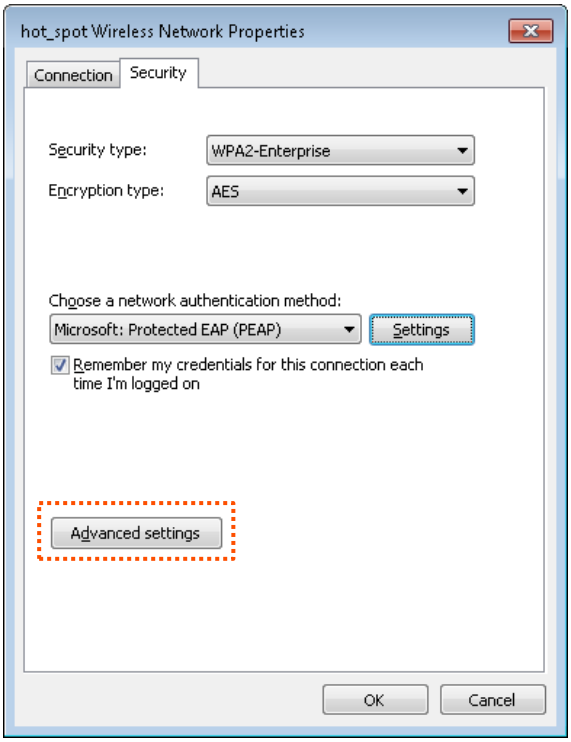
**Step 7** Deselect **Validate server certificate** and click **Configure**.



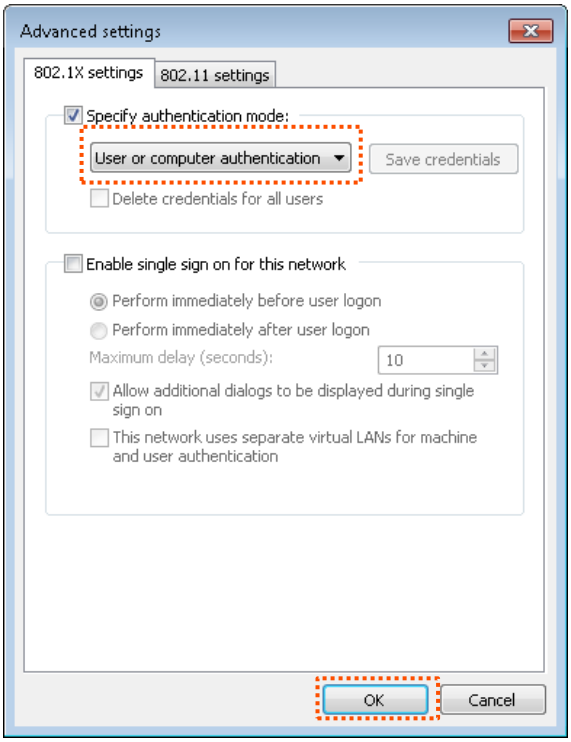

**Step 8** Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



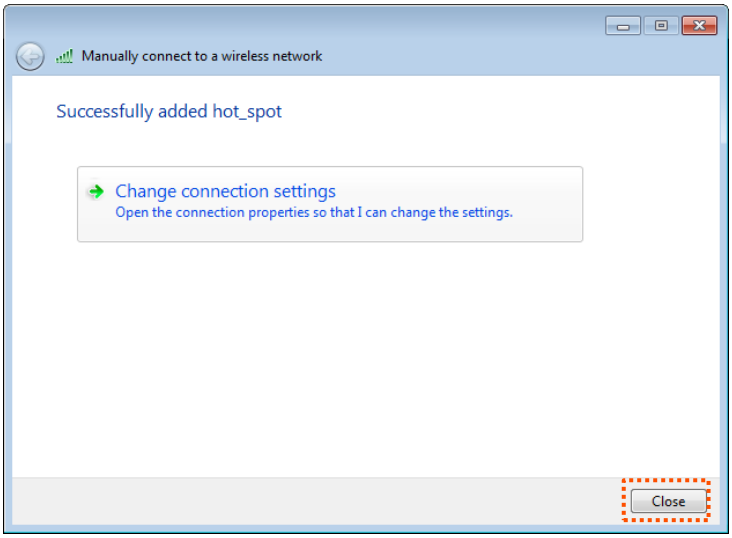
**Step 9** Click **Advanced settings**.

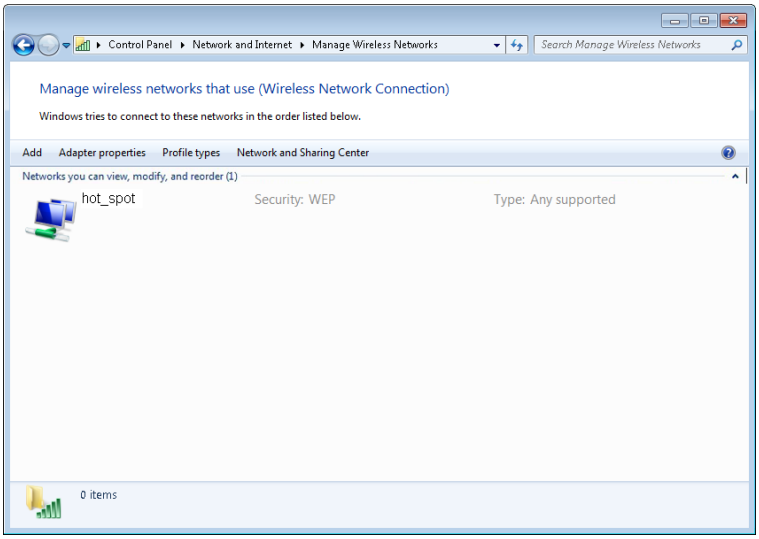



**Step 10** Select **User or computer authentication** and click **OK**.

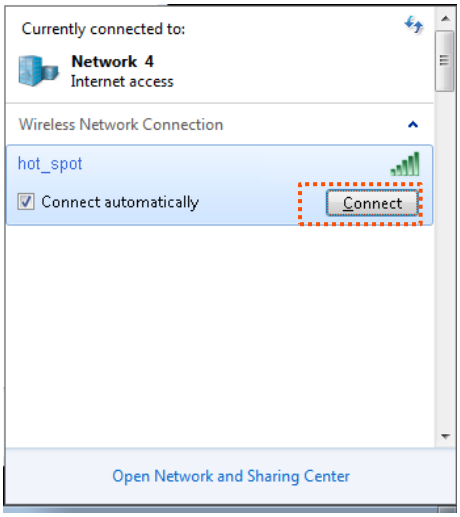


**Step 11** Click **Close**.



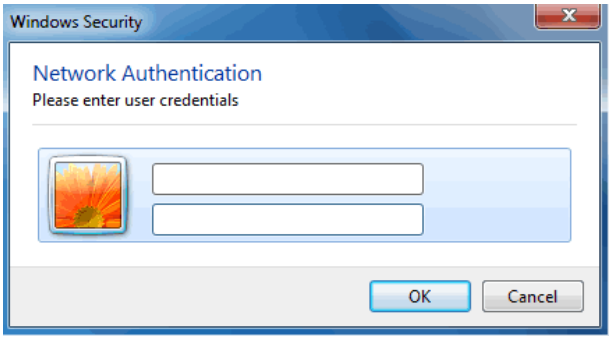




**Step 12** Click the network icon in the lower-right corner of the desktop and choose the wireless network of the CPE such as **hotspot** in this example.




**Step 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 **hotspot**.

# 6.2 Advanced

## 6.2.1 Overview

This module enables you to adjust the wireless performance. You are recommended to configure it under the guide of a professional.

## 6.2.2 Changing advanced settings

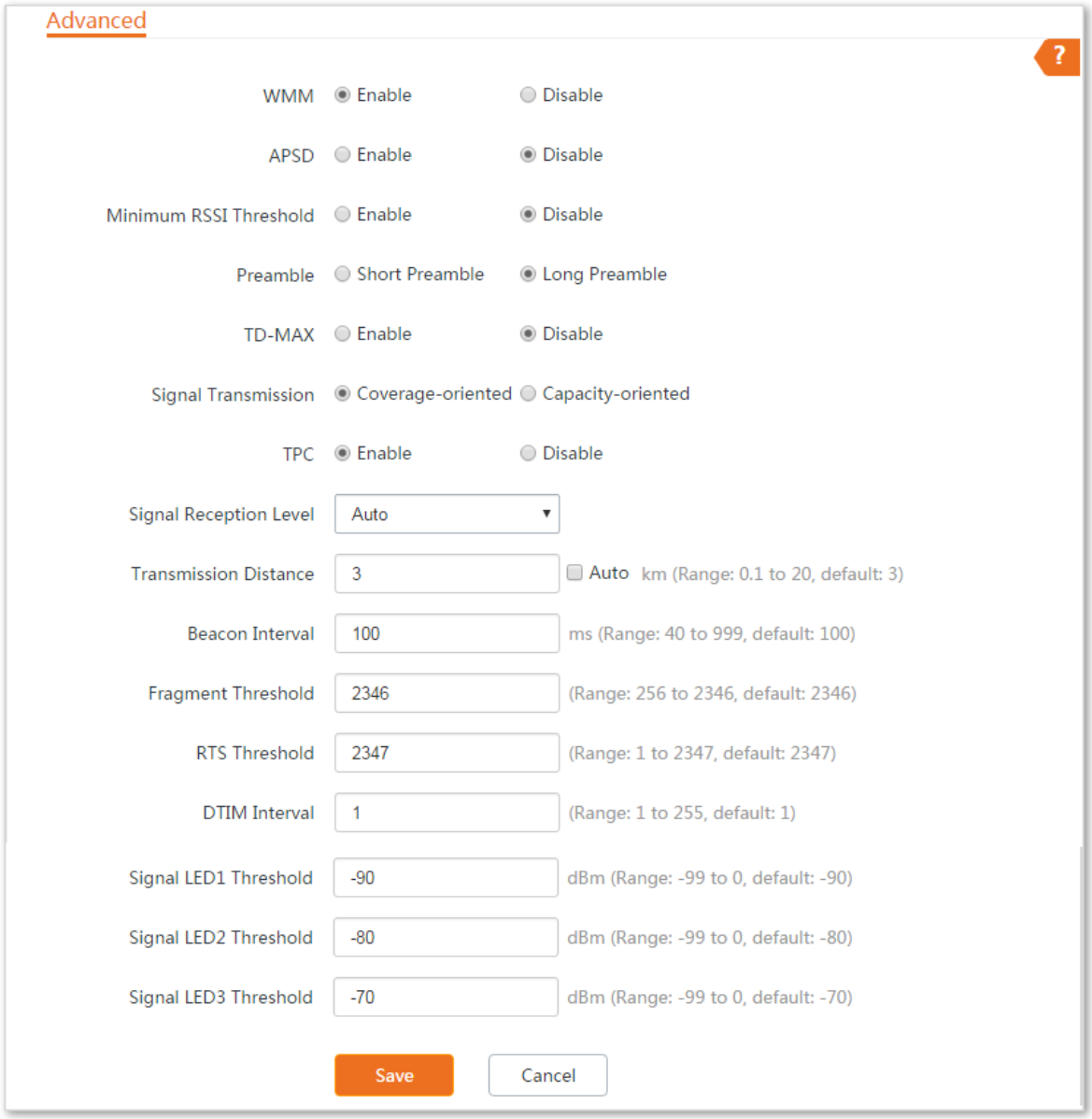
TIP

It is recommended that you change the settings only under the instruction of professional personnel, so as to prevent decreasing the wireless performance of the device.

**Step 1** Choose **Wireless** > **Advanced**.

**Step 2** Change the parameter settings as required.

**Step 3** Click **Save**.




**----End**

## Parameters description

| Name | 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. You are recommended to configure the advanced setting instructed by professional. |
| APSD | It specifies whether to enable the Automatic Power Save Delivery (APSD) mode. 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 |

| Name | Description |
| --- | --- |
| | 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. By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the Short Preamble option. |
| TD-MAX | TD-MAX is Tenda's proprietary Time Division Multiple Access (TDMA) polling technology. It assigns time slots for each device communication to avoid 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.<br>TD-MAX improves overall performance in Point-to-MultiPoint (PtMP) installations and noisy environments, because it reduces latency, and offers better tolerance against interference. Because of its advantages, TD-MAX also increases the maximum possible number of users that can associate with an AP that uses TD-MAX.<br>NOTE<br>If 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 CPE. |
| Signal Transmission | It specifies the wall penetrating capability of the device.<br>**Coverage-oriented**: With less interference nearby, this mode enables the device to cover wider area.<br>**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<br>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 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 |

| Name | Description |
| --- | --- |
| | 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. 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. |
| 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. |

# 6.3 Access control

## 6.3.1 Overview

It specifies, based on MAC address filter rules, the wireless devices that can or cannot access the wireless networks of the device. The device supports the following MAC address filter rules:

- **Disallow**: It indicates that only the wireless devices with the specified MAC addresses cannot access the wireless networks of the device.
- **Allow**: It indicates that only the wireless devices with the specified MAC addresses can access the wireless networks of the device.

## 6.3.2 Configuring access control

### Configuration procedure

**Step 1** Choose **Wireless** > **Access Control**.

**Step 2** Enable the **Access Control** function.

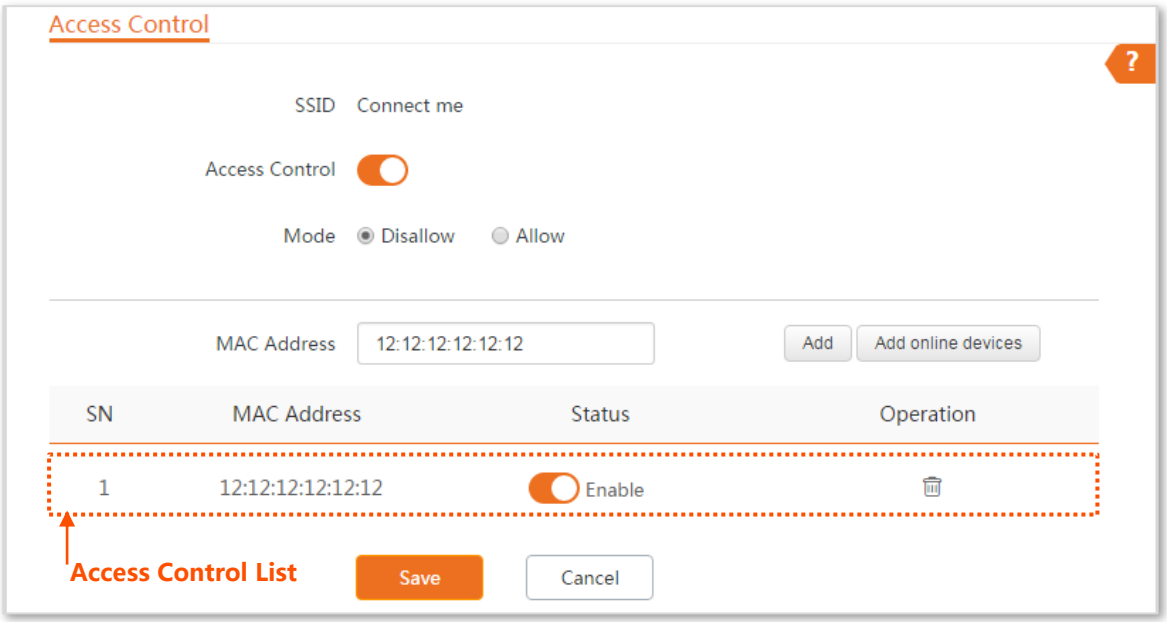
**Step 3** Select a MAC address filter mode, **Disallow** or **Allow**.

**Step 4** Enter the MAC addresses and click **Add**.

TIP

If the wireless devices to be controlled are connected to the CPE, click **Add online devices** to add them to the access control list quickly.

**Step 5** Click **Save**.



**----End**

**Parameters description**

| Name | 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 Access Control function. |
| Mode | It specifies the mode for filtering MAC addresses.<br>**Allow**: It indicates that only the wireless clients on the access control list can connect to the WiFi network of the device.<br>**Disallow**: It indicates that only the wireless clients on the access control list cannot connect to the WiFi network of the device. |

## 6.3.3 Example of configuring access control

### Networking requirement

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

The Access Control function of the CPE is recommended. Assume that the users have three wireless devices whose MAC addresses are C8:3A:35:00:00:01, C8:3A:35:00:00:02, and C8:3A:35:00:00:03.

### Configuration procedure

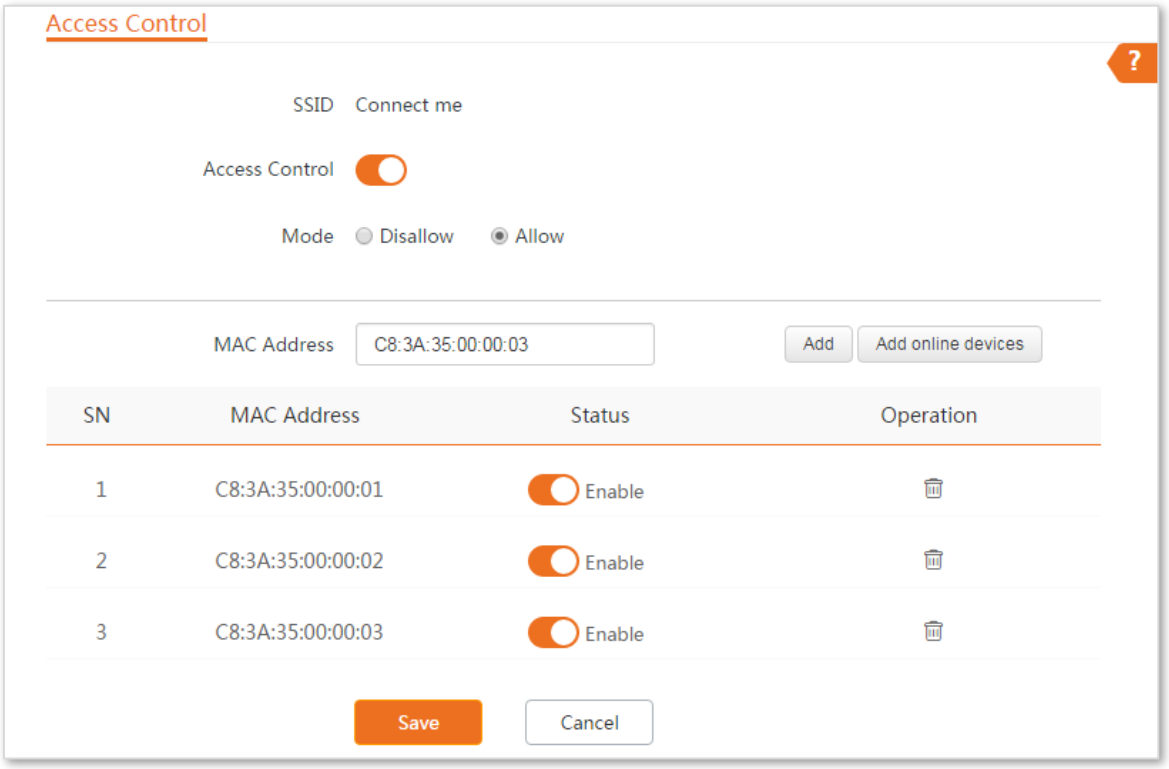
**Step 1** Choose **Wireless** > **Access Control**, and enable the **Access Control** function.

**Step 2** Set the **Mode** to **Allow**.

**Step 3** Enter the MAC address, which is C8:3A:35:00:00:01 is this example, and click **Add**.

**Step 4** Perform **Step 3** to add the other two MAC addresses.

**Step 5** Click **Save**.




**----End**

## Verification

Only above-mentioned wireless devices can connect to the WiFi network of the device.

# 7 Advanced

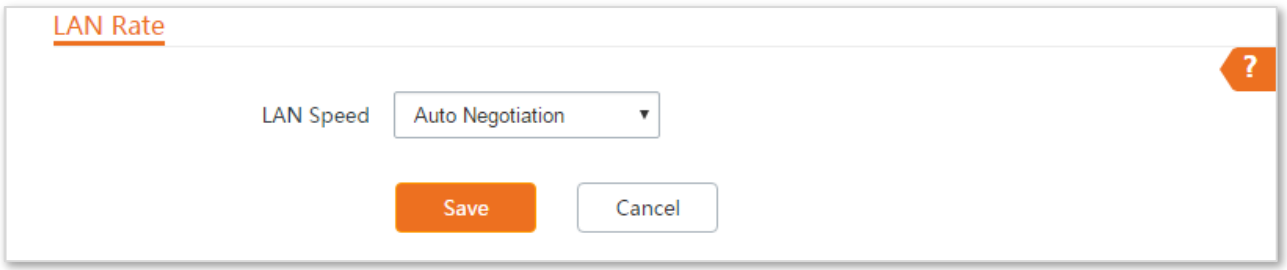
## 7.1 LAN rate

### 7.1.1 Overview

Choose **Advanced** > **LAN Rate** to enter the page.

This module enables you to change LAN speed and duplex mode settings.

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 the peer device. By default, the LAN speed settings of the LAN port is **Auto Negotiation**.



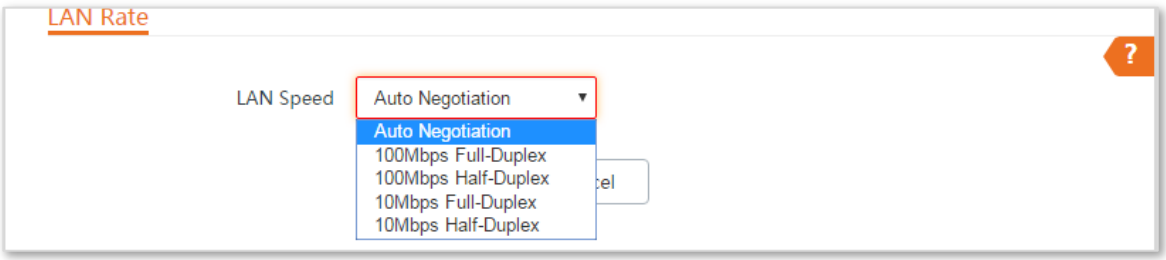

### 7.1.2 Changing the LAN speed and duplex mode

#### Configuration procedure

**Step 1** Choose **Advanced** > **LAN Rate**.

**Step 2** Select a LAN speed and duplex mode for each LAN port.

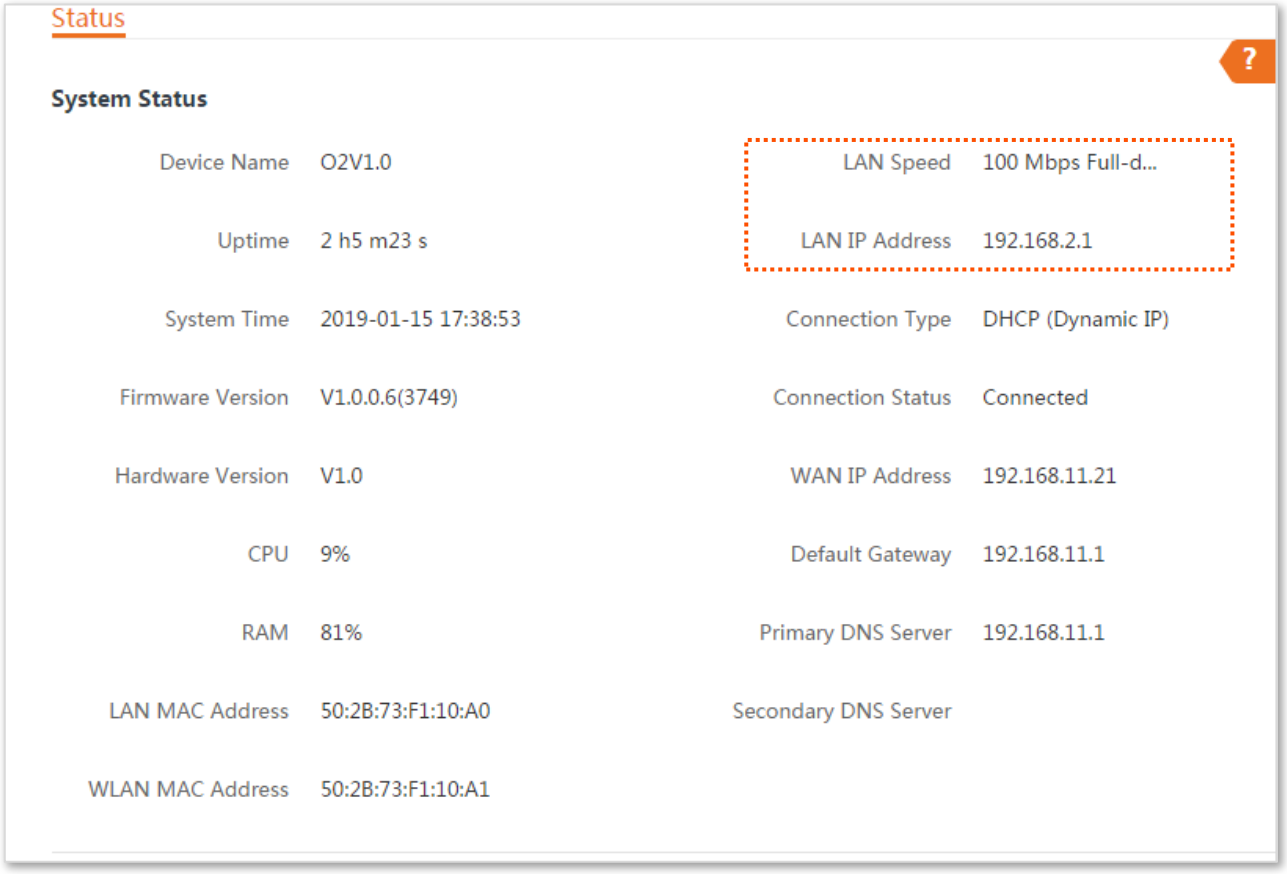
**Step 3** Click **Save**.




**----End**

## Verification

Choose **Status** and check the changes in **System Status** part.



# 7.2 Diagnose

## 7.2.1 Overview

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

If the network connection fails, you can use the diagnosis tools for troubleshooting. The device supports the following four tools:

- **Site Survey**: used to check nearby wireless signals.
- **Ping**: used to check the network connectivity and routes.
- **Traceroute**: used to check the network routes.
- **Speed Test**: used to check the connection speed between two devices in a same network.

## 7.2.2 Site Survey

Site survey gives you an insight into the information of nearby wireless signals.

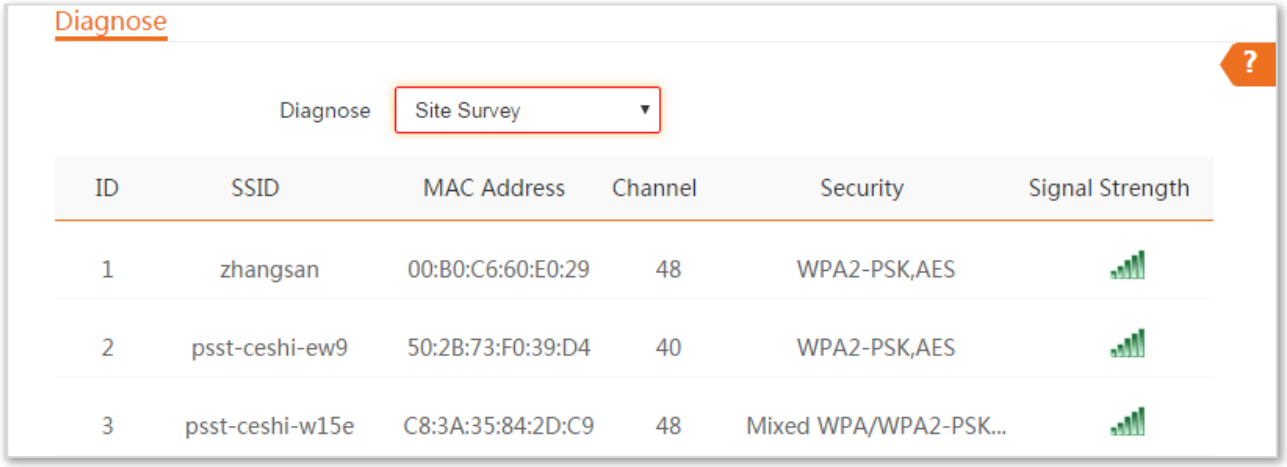
### Configuration pocedure

**Step 1** Choose **Advanced** > **Diagnose**.

**Step 2** Select **Site Survey** in the **Diagnose** drop-down list menu.

**----End**

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




According to the diagnosis result, you can select a less interference channel (used by few devices) for the wireless network of the device to improve the transmission efficiency.

## 7.2.3 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

**Step 1** Choose **Advanced** > **Diagnose**.

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

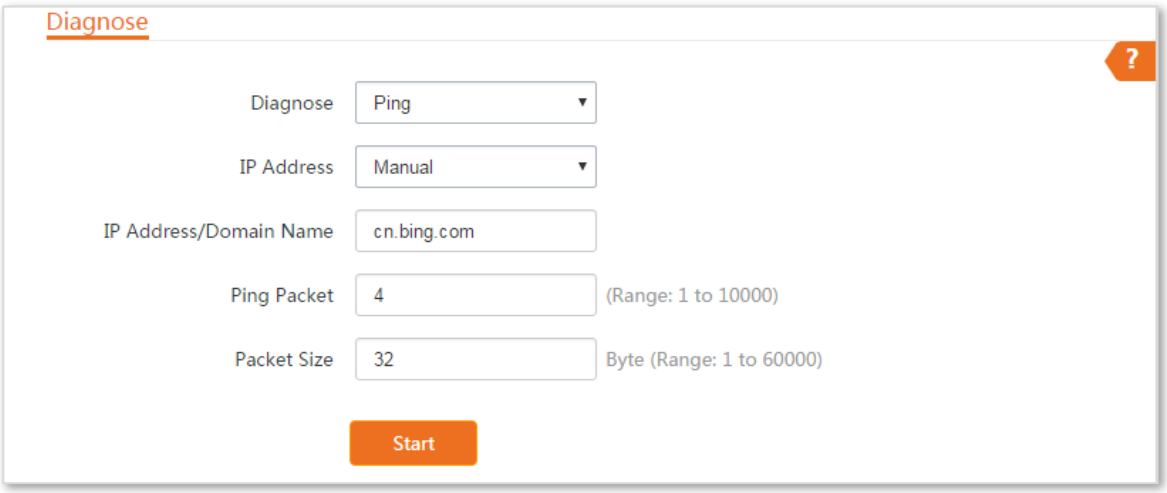
**Step 3** Set **IP Address** to **Manual**.

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

**Step 5** Enter a number of packets transmitted by ping.

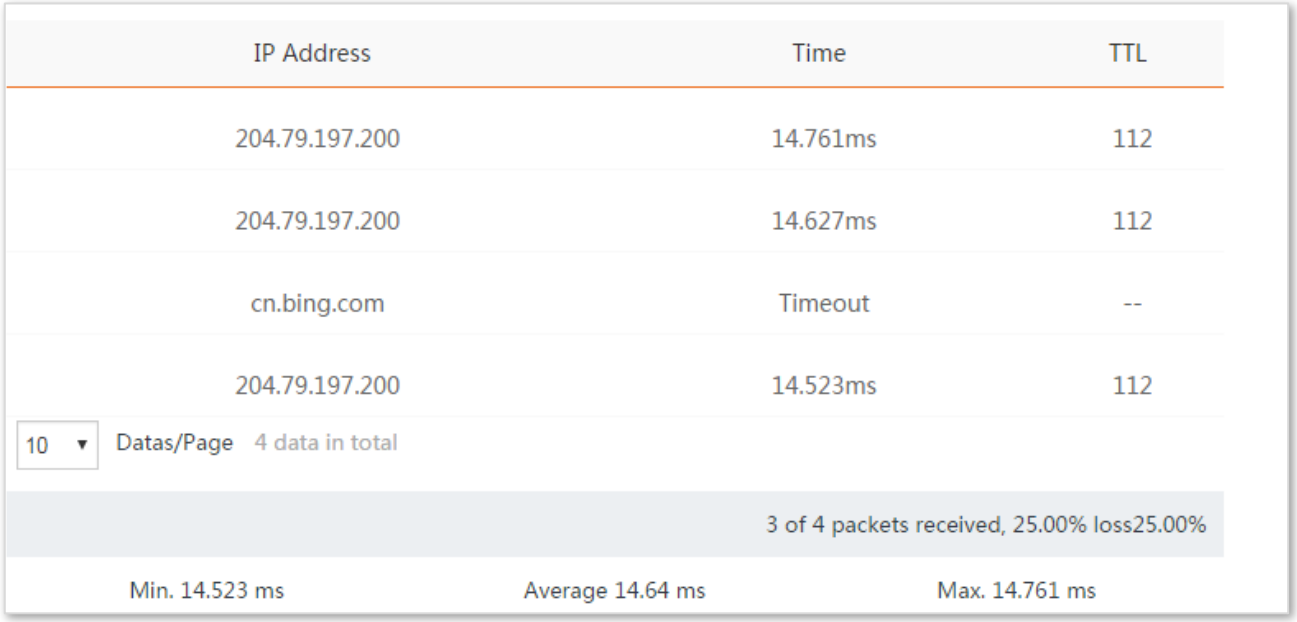
**Step 6** Enter the size of packet transmitted by ping.

**Step 7** Click **Start**.




**----End**

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




## 7.2.4 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**.

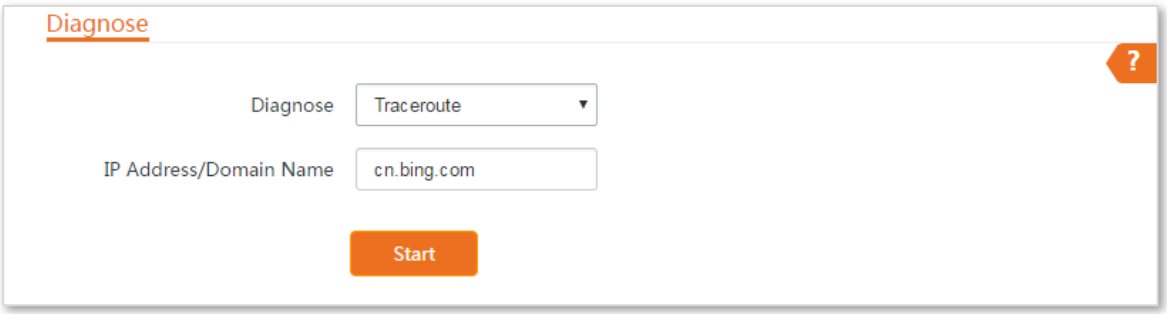
### Configuration procedure

**Step 1** Choose **Advanced** > **Diagnose**.

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

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

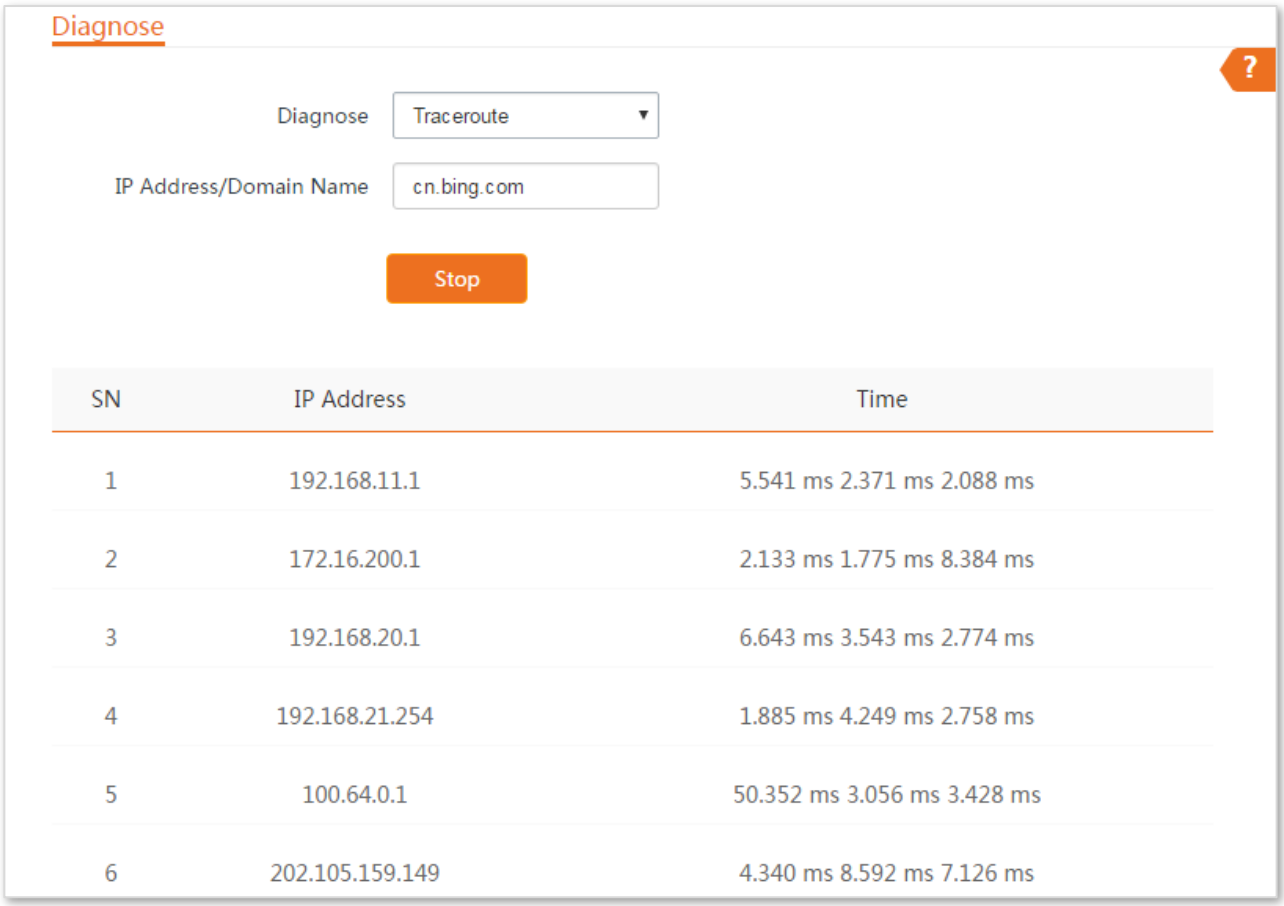
**Step 4** Click **Start**.




**----End**

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

following figure:




## 7.2.5 Speed test

It is used to test the throughput between two Tenda CPEs in the same network. The test requires one of the two devices to be set as a server and the other as a client. The client launches the test request to the server and the server responds to it.

**Step 1** Choose **Advanced** > **Diagnose** to enter the page.

**Step 2** Set **Diagnose** to **Speed Test**.

**Step 3** Set **IP Address of Peer AP** to **Manual**, and enter an IP address in the **IP Address** box. Or select an IP address from the drop-down list. All IP addresses of the devices connected to the CPE are displayed in the list.

**Step 4** Specify a HTTP port.

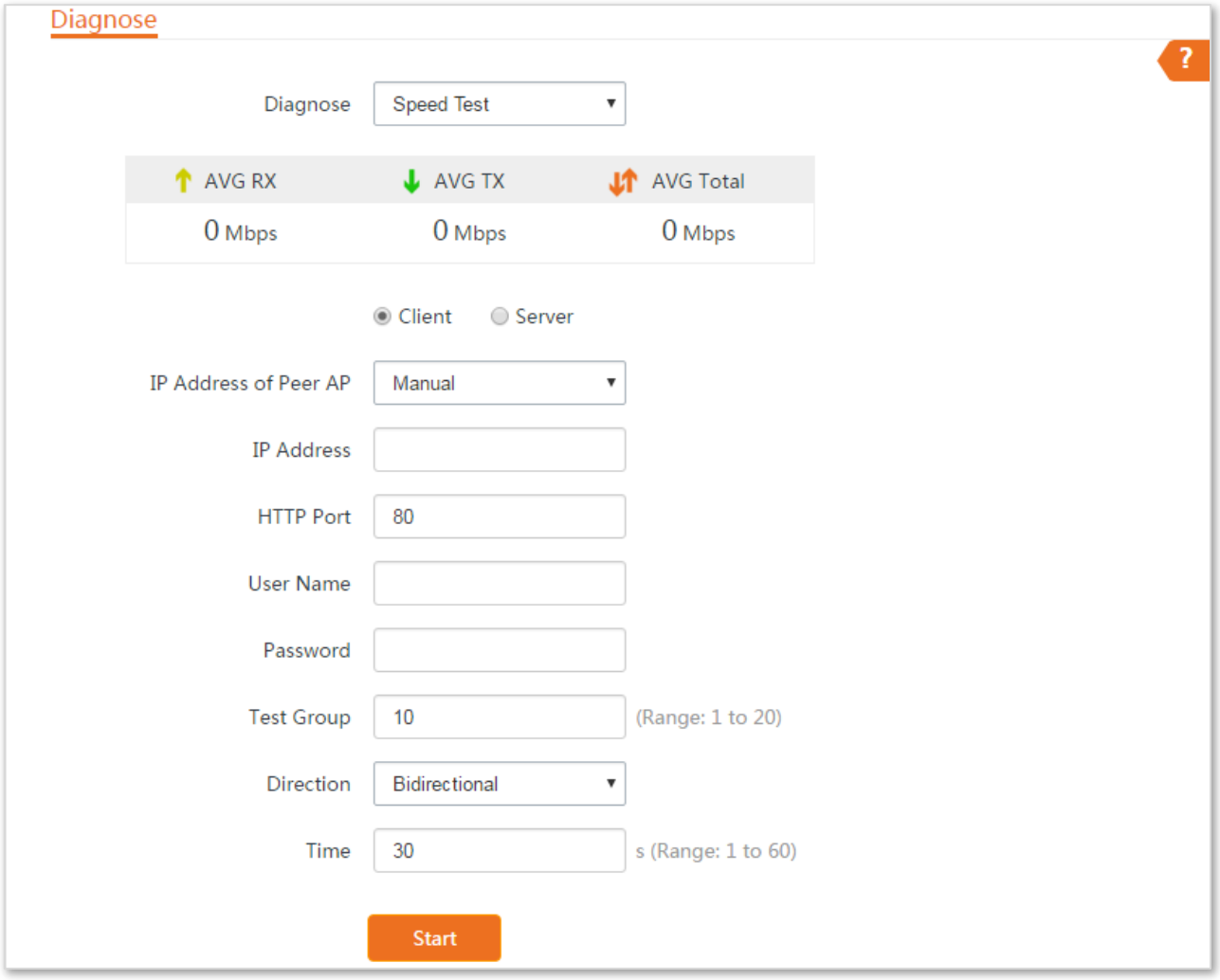
**Step 5** Enter a user name and password of peer CPE.

**Step 6** Specify the test group.

**Step 7** Select the test speed direction.

**Step 8** Specify the time of speed test.

**----End**




## Parameters description

| Name | Description |
|---|---|
| IP Address of Peer AP | It specifies the LAN IP address of peer CPE. You can enter it manually or select an IP address from the drop-down list if there are devices connected to the CPE. |
| IP Address | If the **IP Address of Peer AP** is set to **Manual**, you need to enter the LAN IP address of peer CPE in the box manually. |
| HTTP Port | It specifies the port number of HTTP service. Default: **80**. You are recommended to keep the default value. |
| User Name | It specifies the login user name of peer CPE. |
| Password | It specifies the login password of peer CPE. |
| Test Group | It specifies the number of test connection launched by the client. |
| Direction | It specifies the test speed direction.<br>**RX** (Receive): only test the speed that the peer device transmits data to this device. |

| Name | Description |
| --- | --- |
| | **TX** (Transmit): only test the speed that this device transmits data to peer device.<br>**Bidirectional**: test both transmit and receive speed between the two CPEs |
| Time | It specifies the period of speed test. |

## Example of configuring the speed test

Assume that CPE1 working in AP mode and CPE2 working in client mode have bridged successfully. Then test the wireless speed between them.

### Configuration procedure

**Step 1** Log in to the web UI of CPE2.

**Step 2** Choose **Advanced** > **Diagnose**.

**Step 3** Set **Diagnose** to **Speed Test**.

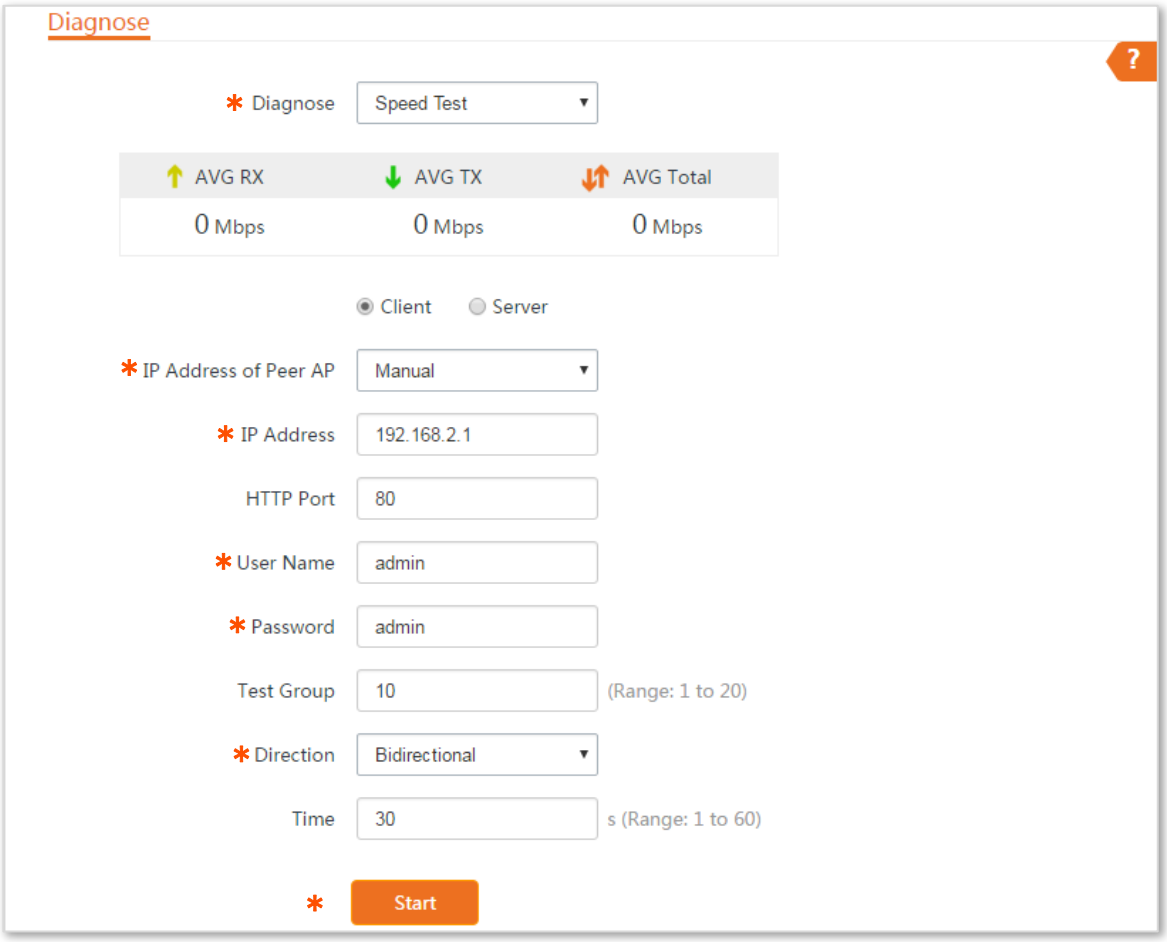
**Step 4** Set **IP Address of Peer AP** to **Manual**.

**Step 5** Enter the IP address of CPE1 to the **IP Address** box, which is **192.168.2.1** in this example.

**Step 6** Enter the login user name and password of the web UI of CPE1 in the **User name** and **Password** boxes, which are both **admin** in this example.

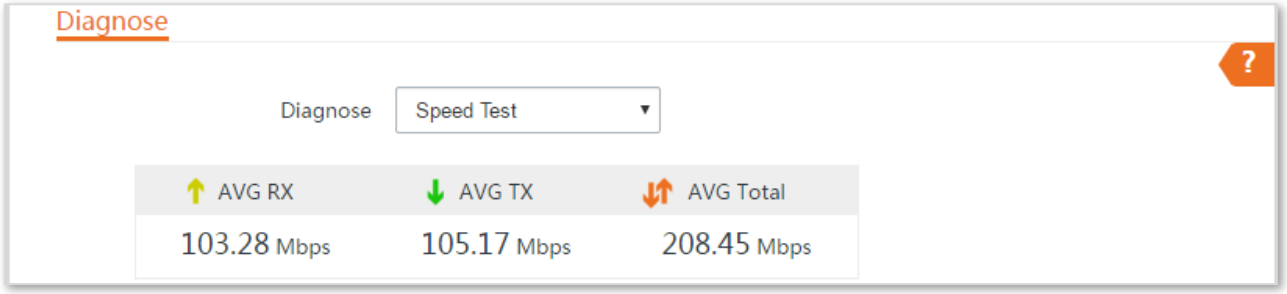
**Step 7** Set **Direction** to **Bidirectional**.

**Step 8** Click **Start**.




**----End**

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



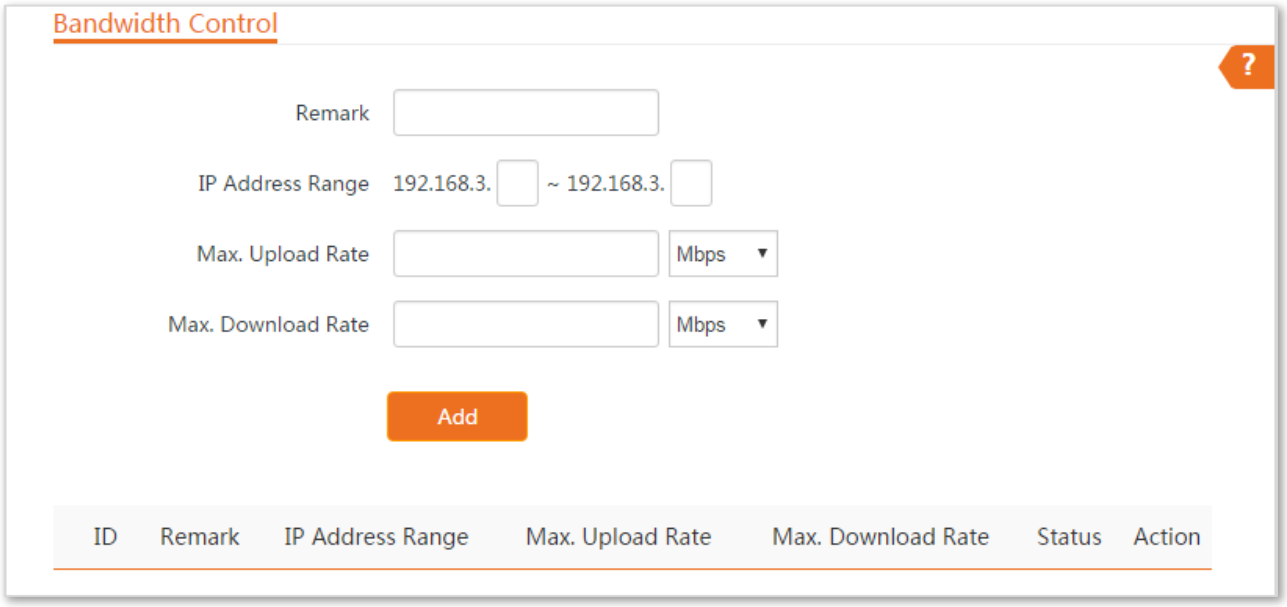
# 7.3 Bandwidth control

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

## 7.3.1 Overview

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

Choose **Advanced** > **Bandwidth Control** to enter the page.

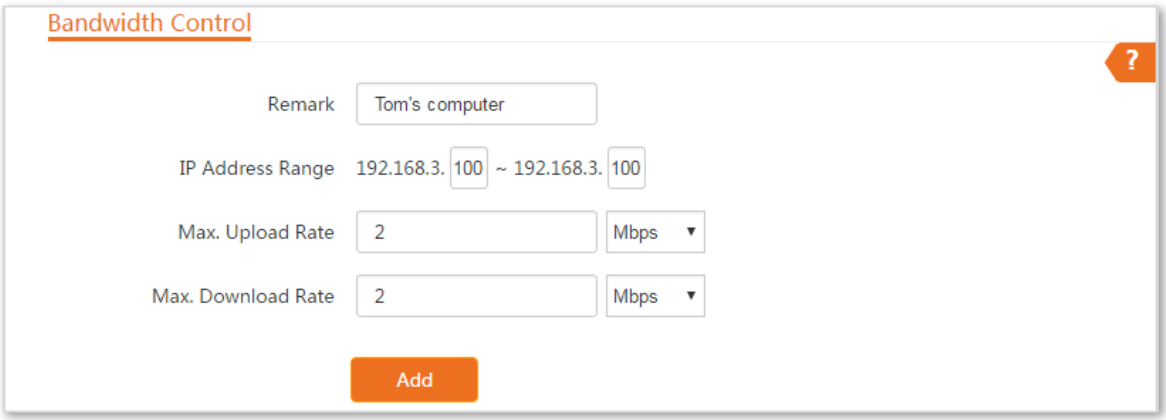



### Configuring bandwidth control

**Step 1** Choose **Advanced** >**Bandwidth Control**.

**Step 2** Set related parameters.

**Step 3** Click **Add**.



----End

**Parameters description**

| Name | Description |
| --- | --- |
| Remark | 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.<br>If you want to control only one device, enter the same IP address in the two boxes. If you want 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 the device whose IP address is within the IP Address Range. |
| 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. |

## 7.3.2 Example of configuring bandwidth control

### Networking requirement

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode. To ensure that every device can access the internet smoothly, you want to specify a maximum upload/download for each device.

**Assumption**: The maximum upload rate of each device connected to the WiFi network of the device is **5 Mbps**, and download rate is **10 Mbps**. And the IP address range of the devices connected to the WiFi network is **192.168.3.100** to **192.168.3.200**.

### Configuration procedure

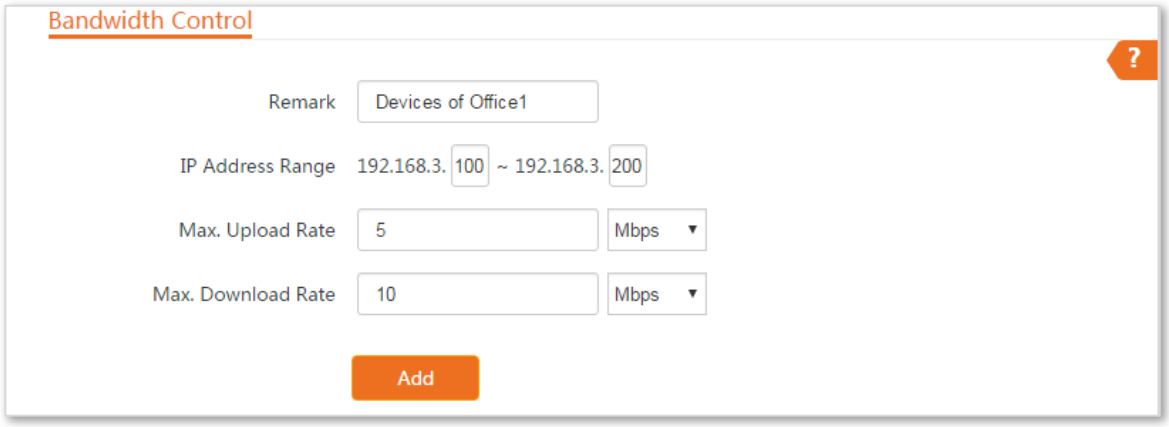
**Step 1** Choose **Advanced** > **Bandwidth Control**.

**Step 2** Enter a remark, such as **Devices of Office1**.

**Step 3** Specify an IP address range, which are **100** and **200** in this example.

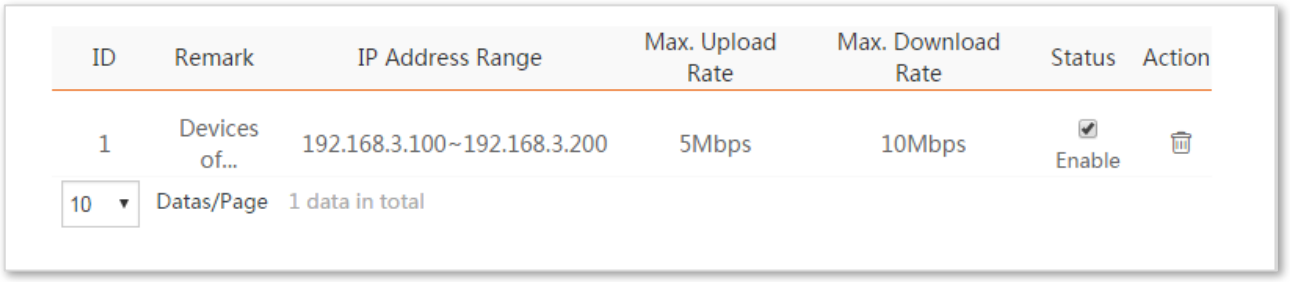
**Step 4** Specify the maximum upload rate and download rate respectively, which are **5** and **10** in this example.

**Step 5** Click **Add**.




**----End**

If the rule is added successfully, it is displayed in the list below the **Add** button. See the following figure:




## Verification

For a device whose IP address is within the range of 192.168.3.100 to 192.168.3.200, its maximum upload rate is 5 Mbps and its maximum download rate is 10 Mbps.

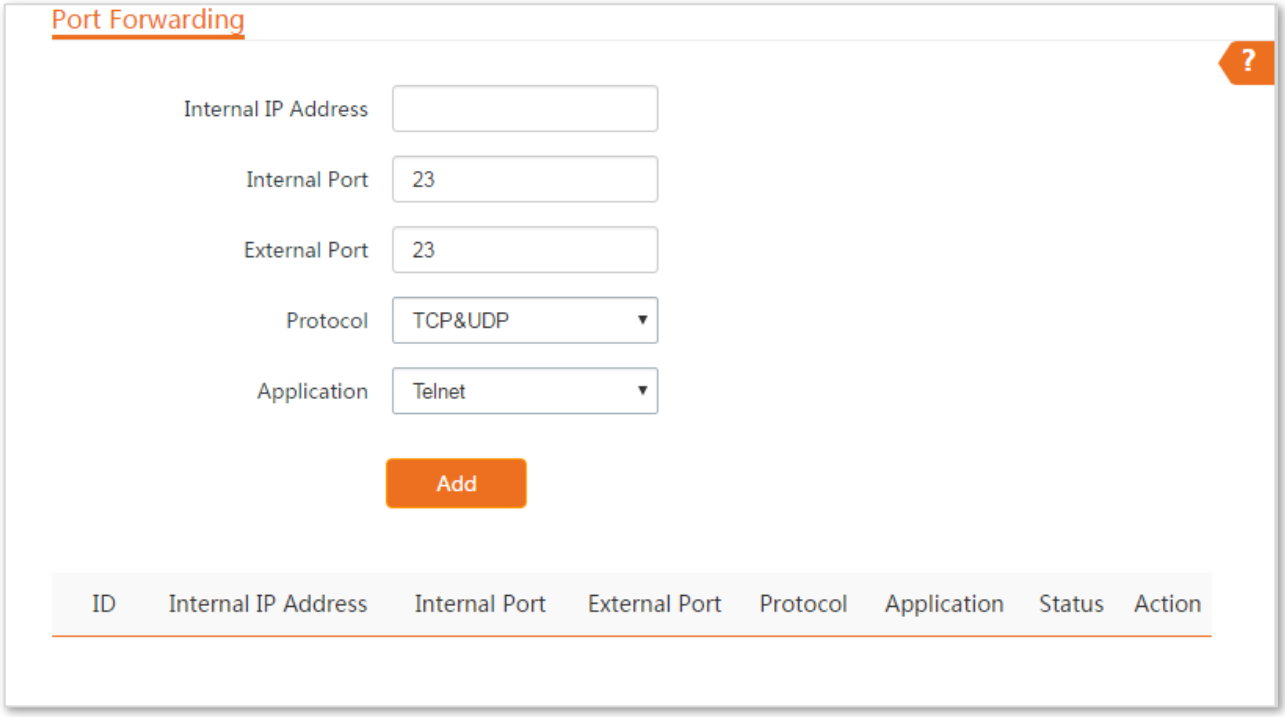
# 7.4 Port forwarding

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

## 7.4.1 Overview

If computers are connected to the router to form a LAN and access the internet through the router, 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 router, and map one service port to the IP address of the LAN server. This enables the router to forward the requests arriving at the port from the internet to the LAN server, and avoid the attacks from the WAN.

Choose **Advanced** > **Port Forwarding** to enter the page.




## 7.4.2 Configuring port forwarding

### Configuration procedure

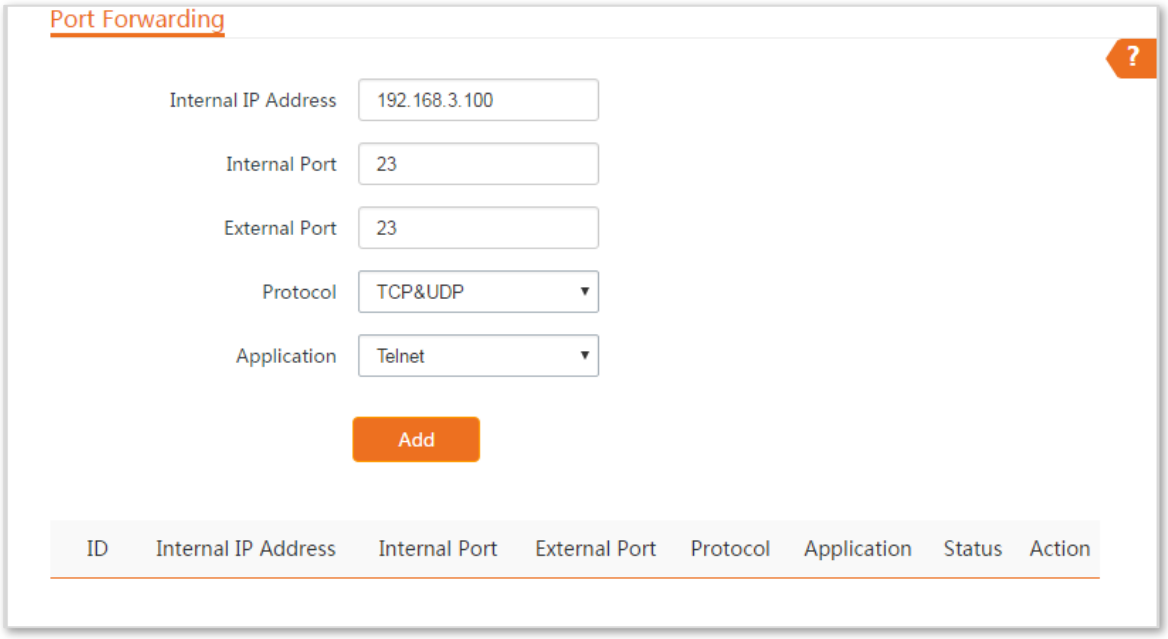
**Step 1** Choose **Advanced** > **Port Forwarding**.

**Step 2** Enter an IP address in LAN.

**Step 3** Select an **Application**, and the internal and external ports will be automatically populated.

**Step 4** Select a protocol.

**Step 5** Click **Add**.




**----End**

**Parameters description**

| Name | 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. A single port is supported. |
| External Port | It specifies the ports enabled for WAN users by this device. |
| 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. After you select an application, the internal and external ports will be populated. |
| Action | Click to delete the rule. |

## 7.4.3 Example of configuring port forwarding

### Networking requirement

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode.

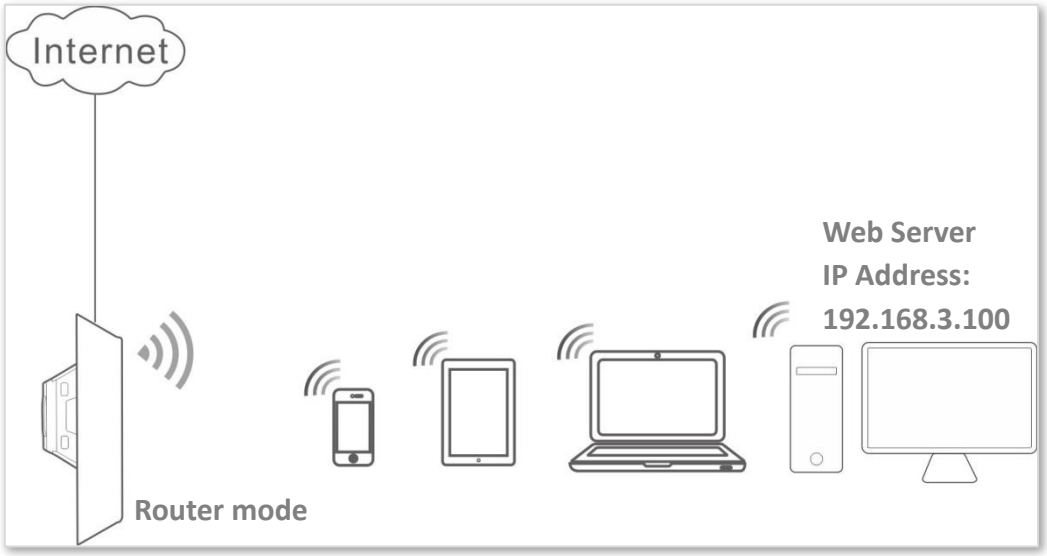
**Requirement**: Families who are not at home can visit the resources on the web server in LAN over the internet.

You are recommended to use port forwarding function to solve the problem.

**Assumption:**

- IP Address of the web server: 192.168.3.100
- Service port (internal port) of the web server in LAN: 80
- External port that this device enables for internet devices: 80
- WAN IP Address of the device: 202.105.11.22

## Network topology




## Configuration procedure

**Prerequisite**: manually set static an IP address and related parameters for the web server to avoid the service disconnection caused by the dynamic IP address.

**Step 1** Log in to the web UI of the device which works in **Router** mode.

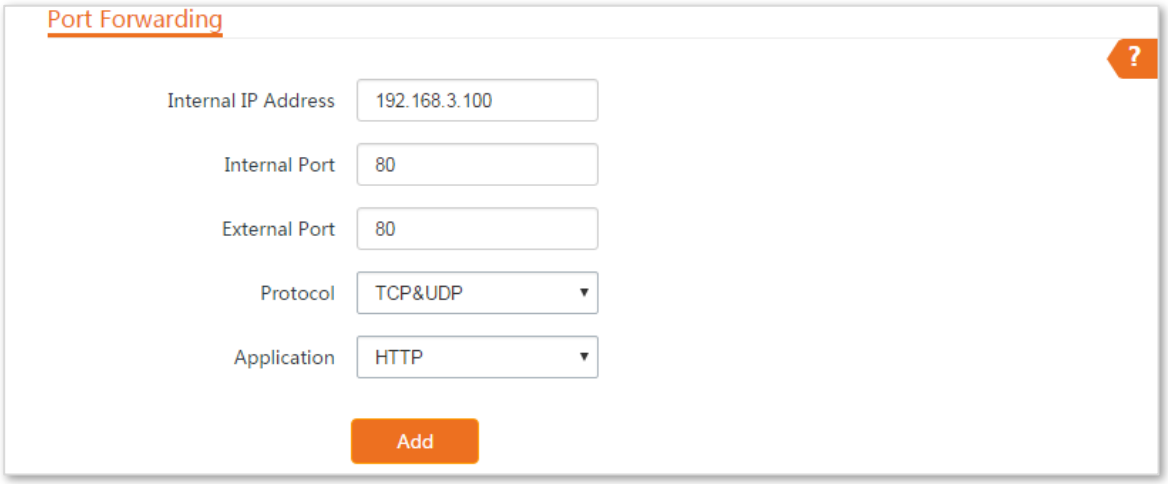
**Step 2** Choose **Advanced** > **Port Forwarding**.

**Step 3** Enter the IP address of the web server in the **Internal IP Address** box, which is **192.168.3.100** in this example.

**Step 4** Select **HTTP** from the drop-down list of **Application**, and the **Internal Port** and **External Port** boxes will be automatically populated.

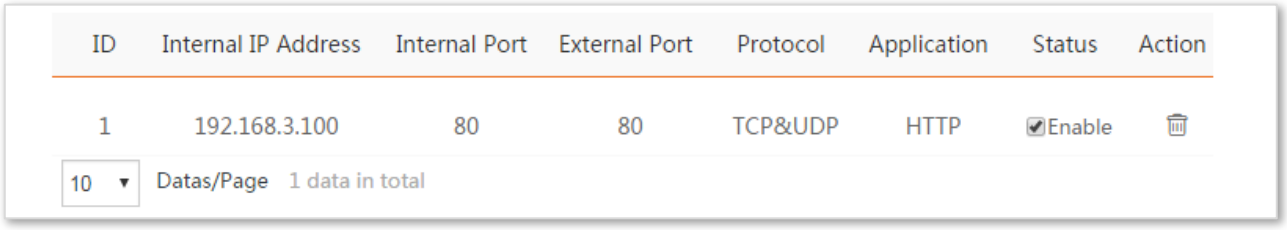
**Step 5** Select **TCP&UDP** from the drop-down list of **Protocol**.

**Step 6** Click **Add**.




**----End**

If the rule is added successfully, it is displayed in the list below the **Add** button. See the following figure:




## Verification

Enter **Protocol name**://**WAN port IP address**:**External port** in the address bar of a web browser on a computer over the internet to access the resources on the web server. In this example, enter **http://202.105.11.22:80**.

TIP

If internet users still cannot visit the web server 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 may cause port forwarding function failures. Disable them and try again.

# 7.5 MAC filter

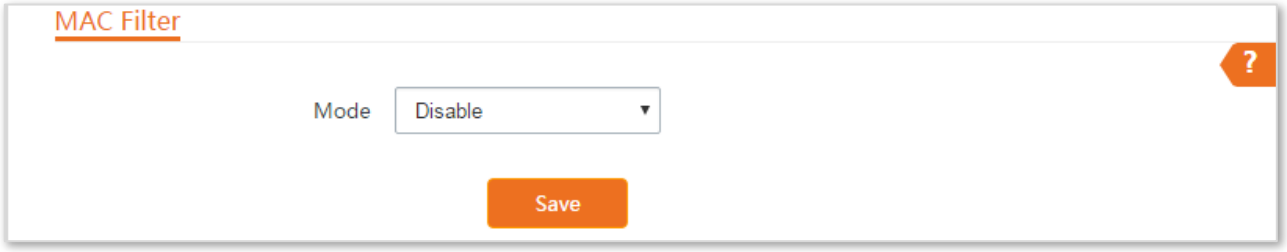
This function is available only when the device works in **WISP** or **Router** mode.

## 7.5.1 Overview

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 based on their MAC addresses.

Choose **Advanced** > **MAC Filter** to enter the page.

The function is disabled by default.




## 7.5.2 Configuring MAC filter

### Configuration procedure

**Step 1** Choose **Advanced** > **MAC Filter**.

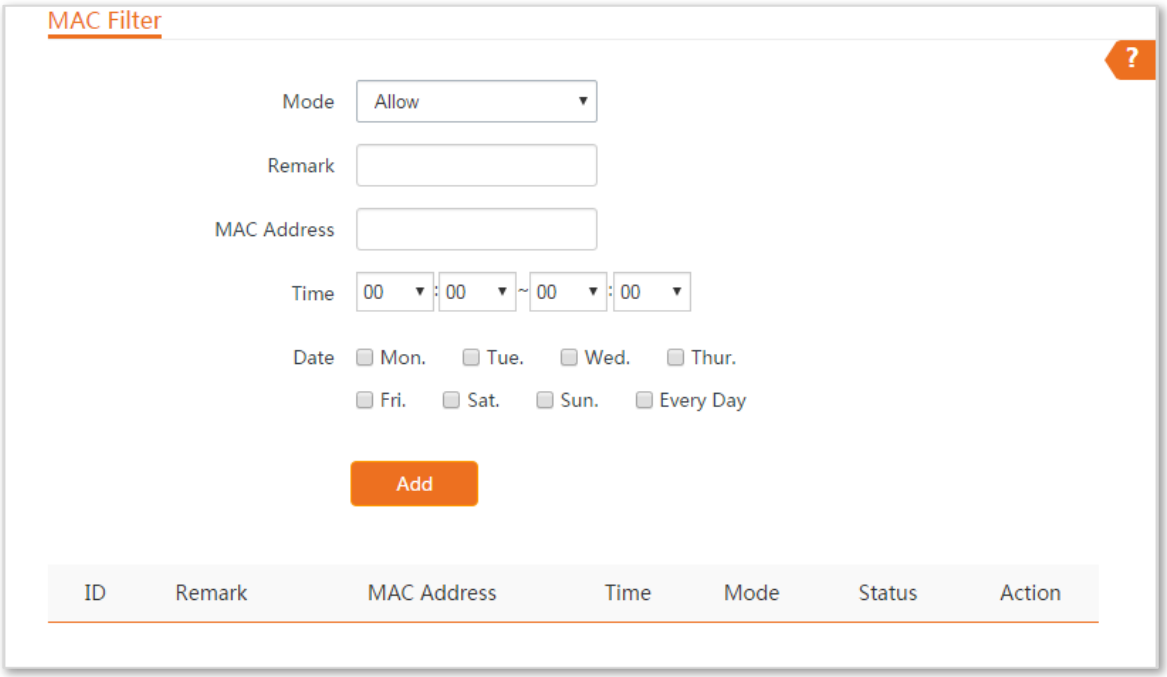
**Step 2** Select a MAC filter mode, **Disallow** or **Allow**.

**Step 3** Enter a remark for the rule, such as somebody's device.

**Step 4** Specify a period at which the rule takes effect.

**Step 5** Tick the dates on which the rule takes effect.

**Step 6** Click **Add**.




**----End**

## Parameters description

| Name | Description |
|---|---|
| Mode | It specifies the mode of MAC filter rule.<br>**Disable**: Disable the MAC Filter function.<br>**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.<br>**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 dates on which the rule takes effect. |
| Status | It specifies the status of the rule. |
| Action | Click to delete the rule. |

## 7.5.3 Example of configuring MAC filter

### Network topology

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode.

**Requirements**: Only allow the parents' devices to access the internet during 9:00 to 17:00, Monday to Friday).

You are recommended to use the MAC Filter function to solve the problem.

**Assumption:**

The MAC addresses of the parents' devices are **CC:3A:61:71:1B:6E** and **CC:3A:61:75:1F:3E**.

### Configuration procedure

**Step 1** Log in to the web UI of the device which is working in WISP mode, and choose **Advanced** > **MAC Filter**.

**Step 2** Select a mode, which is **Allow** in this example.

**Step 3** Enter a remark in the **Remark** box, which is **Dad's smartphone** in this example.

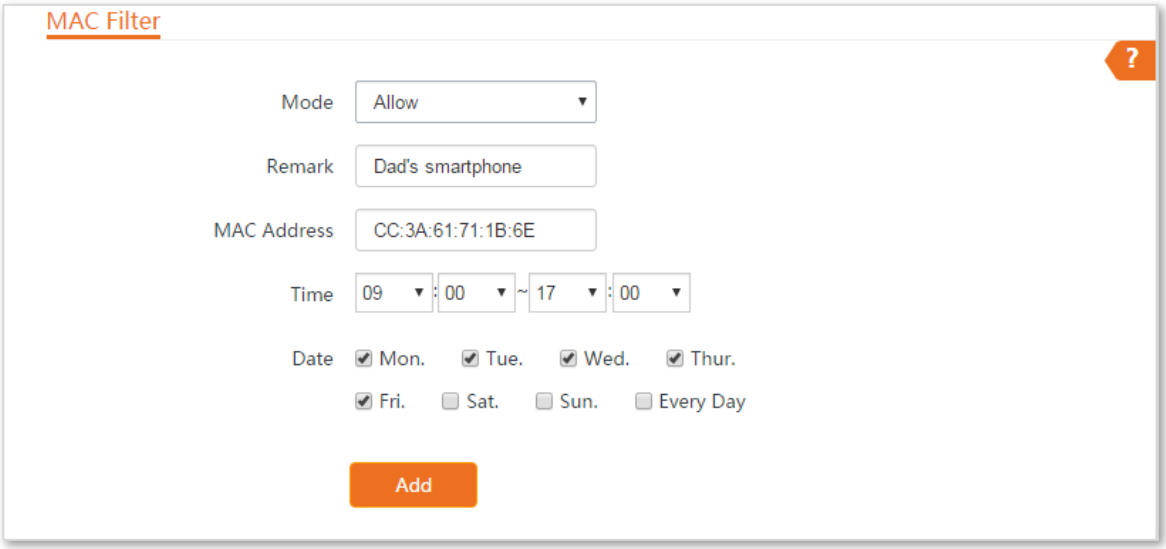
**Step 4** Enter the MAC address of the device, which is **CC:3A:61:71:1B:6E** in this example.

**Step 5** Specify a period, which is **9:00** to **17:00** in this example.

**Step 6** Tick the dates, which are **Monday to Friday** in this example.

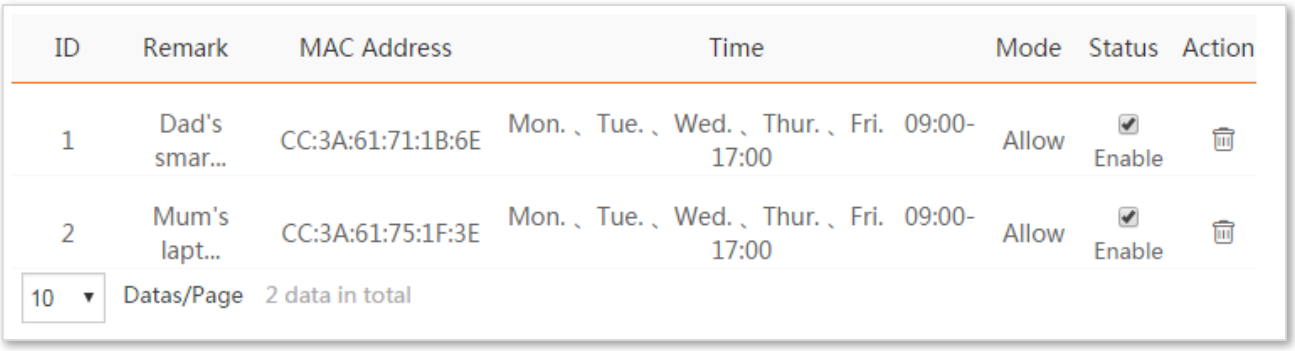
**Step 7** Click **Add**.

**Step 8** Perform **Step2** to **Step7** to add the rule with the other MAC address.




**----End**

If the rule is added successfully, it is displayed in the list below the **Add** button. See the following figure:



| ID | Remark | MAC Address | Time | Mode | Status | Action |
|---|---|---|---|---|---|---|
| 1 | Dad's smar... | CC:3A:61:71:1B:6E | Mon. 、Tue. 、Wed. 、Thur. 、Fri. 09:00-17:00 | Allow | Enable | |
| 2 | Mum's lapt... | CC:3A:61:75:1F:3E | Mon. 、Tue. 、Wed. 、Thur. 、Fri. 09:00-17:00 | Allow | Enable | |

10 ▾ Datas/Page 2 data in total

## Verification

Only the devices with the MAC addresses of CC:3A:61:71:1B:6E and CC:3A:61:75:1F:3E can access the internet at 9:00 to 17:00 from Monday to Friday. All of other devices cannot access the internet during this period.

# 7.6 Network service

## 7.6.1 DDNS

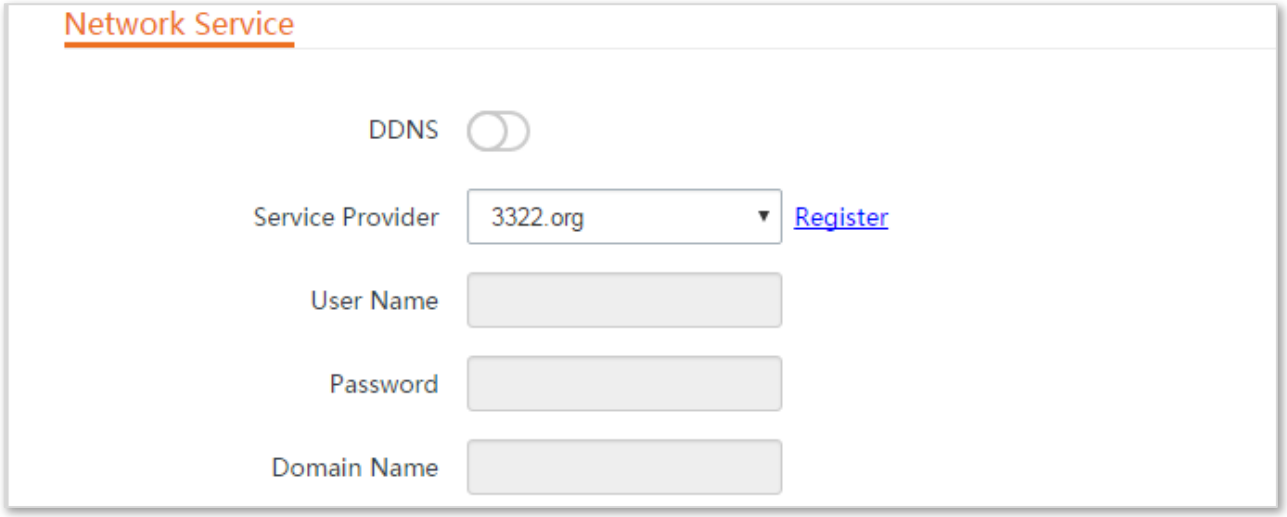
This function is available only when the device works in **WISP** or **Router** mode.

### Overview

DDNS, dynamic domain name service, 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.

The DDNS function maps a dynamic WAN IP address to a domain name. 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.

Choose **Advanced** > **Network Service** to enter the page.




### Configuring DDNS

#### Configuration procedure

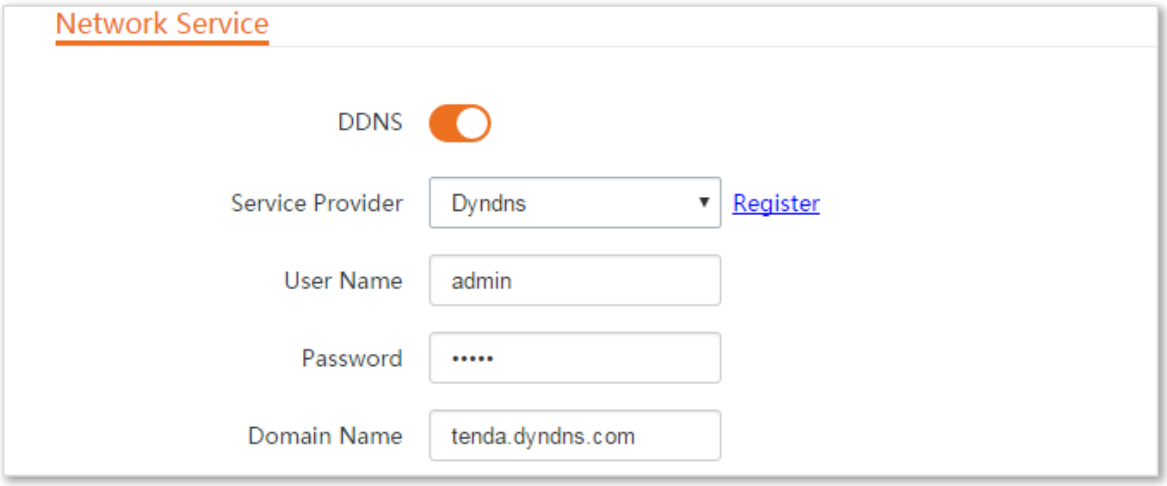
**Step 1** Choose **Advanced** > **Network Service**.

**Step 2** Enable the **DDNS** function.

**Step 3** Select a dynamic DNS provider from the drop-down list.

**Step 4** Enter the user name, password, and domain name you registered with DDNS service provider.

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




**----End**

**Parameters description**

| Name | 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 you registered on the website of the service provider. |
| Password | It specifies the password used to log in to the dynamic DNS service, as well as the login password you registered on the website of the service provider. |
| Domain Name | It specifies the domain name information obtained from the dynamic DNS server. You need to enter the domain name which you registered on the website manually. |

## Example of configuring DDNS

### Networking requirement

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode. The WAN IP address of the device is dynamic.

**Requirement:** The administrator on business can visit the resources on web server in LAN.
You are recommended to use the DDNS and port forwarding functions to solve the problem.

**Assumption:**

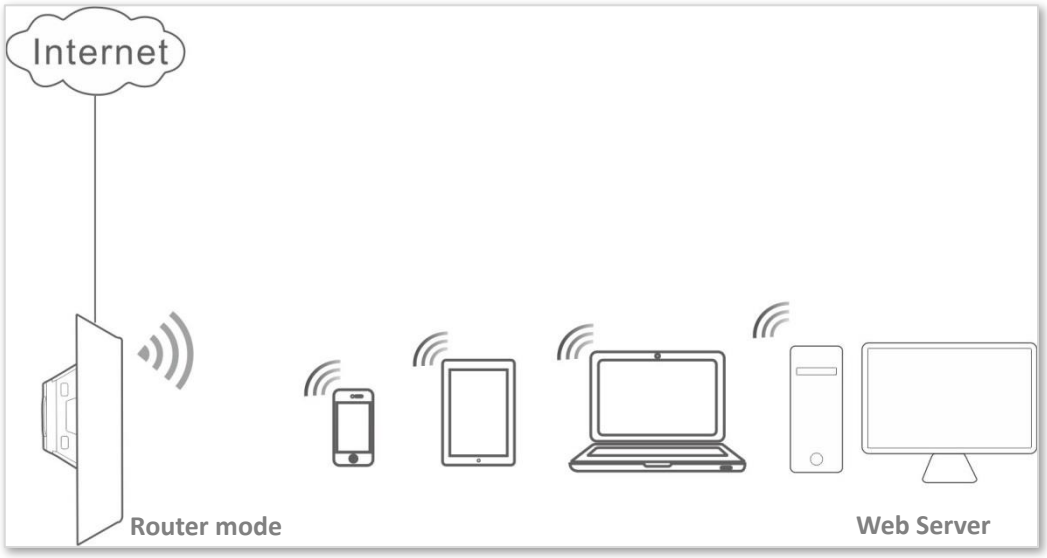
The information of the web server in LAN is shown as follows:

- **IP Address**: 192.168.3.100
- **Service Port of the Web Server**: 80

The registered domain name information is shown as follows:

- **Service Provider**: Dyndns
- **User Name**: tenda
- **Password**: tenda
- **Domain Name**: tenda.dyndns.com

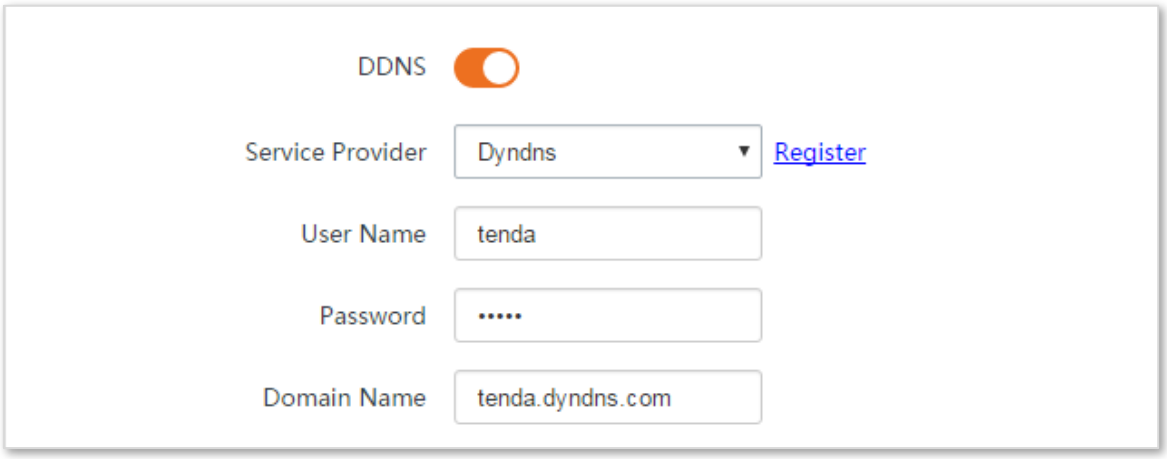
## Network topology




## Configuration procedure

**Step 1** Set up the DDNS function.

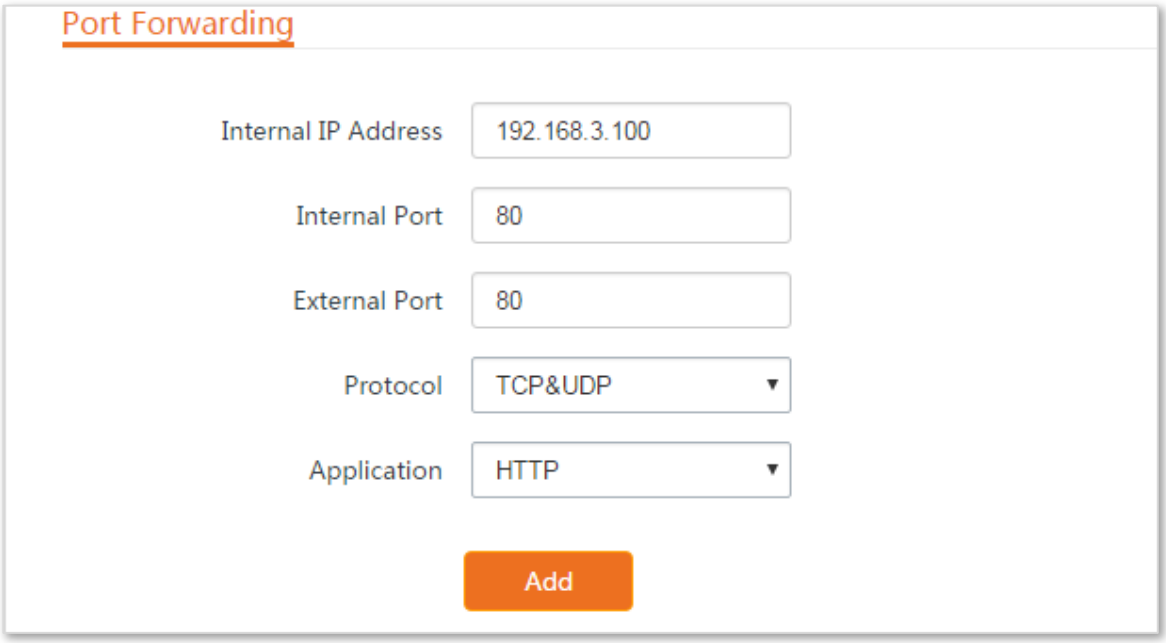
1. Log in to the web UI of the device which works in Router mode.
2. Choose **Advanced** > **Network Service**.
3. Enable the **DDNS** function.
4. Select a service provider, which is **Dyndns** in this example.
5. Enter the user name and password you registered with DDNS service provider, which are **tenda** and **tenda** in this example.
6. Enter the domain name you registered, which is **tenda.dyndns.com**.
7. Click **Save** on the bottom of this page.




**Step 2** Set up the port forwarding function.

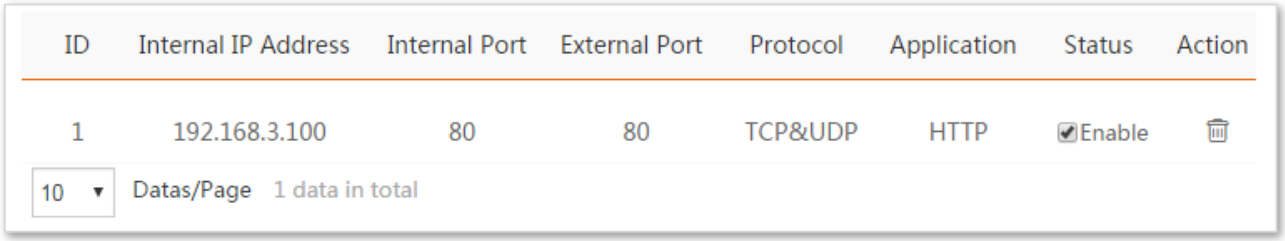
**Prerequisite**: manually set static an IP address and related parameters for the web server to avoid the service disconnection caused by the dynamic IP address.

1. Choose **Advanced** > **Port Forwarding**.
2. Enter the IP address of the web server, which is **192.168.3.100** in this example.
3. Select an application, which is **HTTP** in this example, and the Internal Port and External Port will be populated automatically.
4. Select the protocol of the service. **TCP&UDP** is recommended if you are not sure.
5. Click **Add**.




**----End**

If the rule is added successfully, it is displayed in the list below the **Add** button. See the following figure:



| ID | Internal IP Address | Internal Port | External Port | Protocol | Application | Status | Action |
|---|---|---|---|---|---|---|---|
| 1 | 192.168.3.100 | 80 | 80 | TCP&UDP | HTTP | Enable | |

10 Datas/Page 1 data in total

## Verification

Enter **Protocol name://WAN port domain name:External port** in the address bar of a web browser on a computer over the internet to access the resources on the web server. In this example, enter **http://tenda.dyndns.com:80**.

TIP

If internet users still cannot visit the web server 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 may cause port forwarding function failures. Disable them and try again.

## 7.6.2 Remote web management

### Overview

Generally, only the devices connected to the LAN ports of the device can access its web UI.

The remote web management function enables you to access the web UI of the device on WAN if it is required.

### Configuring remote web management

#### Configuration procedure

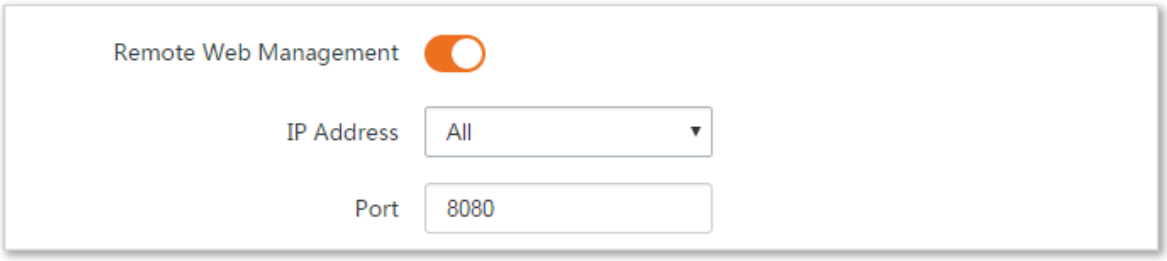
**Step 1** Log in to the web UI of the device.

**Step 2** Choose **Advanced** > **Network Service**.

**Step 3** 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.

**Step 4** Enter a port number.

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




**----End**

#### Parameters description

| Name | 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.<br>**All**: It indicates that any computer in WAN can manage this device remotely. Select this option only when necessary.<br>**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. |

| Name | Description |
| --- | --- |
| | 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**. |

## Example of configuring remote web management

### Networking requirement

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode.

**Requirement**: The host needs to troubleshoot the network when he is on business. So he needs to access the device's web UI on WAN.

You are recommended to use the remote web management function to solve the problem.

**Assumption**:

- The WAN IP address of the device is **202.105.106.55**
- The IP address of the computer which is allowed to access the device on WAN is **202.105.88.77**
- Port number is **8080**

### Configuration procedure

**Step 1** Log in to the web UI of the device, and choose **Advanced** > **Network Service**.

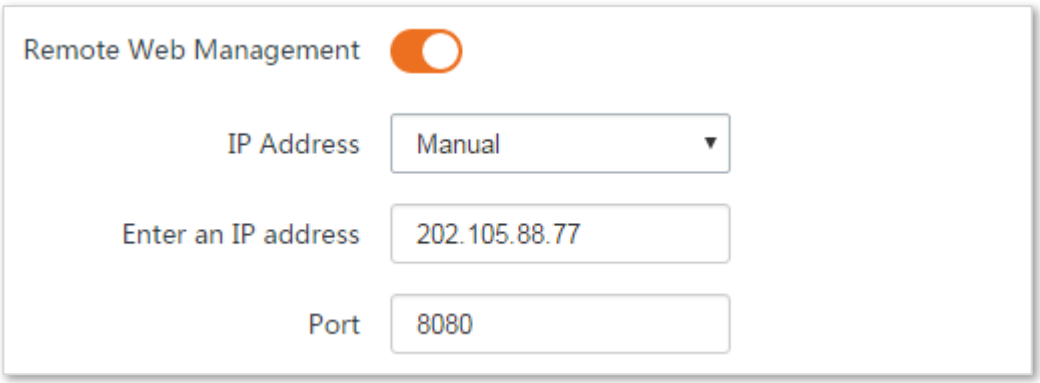
**Step 2** Enable the **Remote Web Management** function.

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

**Step 4** Enter the IP address of the computer which is allowed to access the device on WAN, which is **202.105.88.77** in this example.

**Step 5** Enter the port number, which is **8080** in this example.

**Step 6** Click **Save** in the bottom of this page.




**----End**

### Verification

The host can use his computer to log in to the web UI of the device by access **http://202.105.106.55:8080**.

## 7.6.3 Reboot schedule

### Overview

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

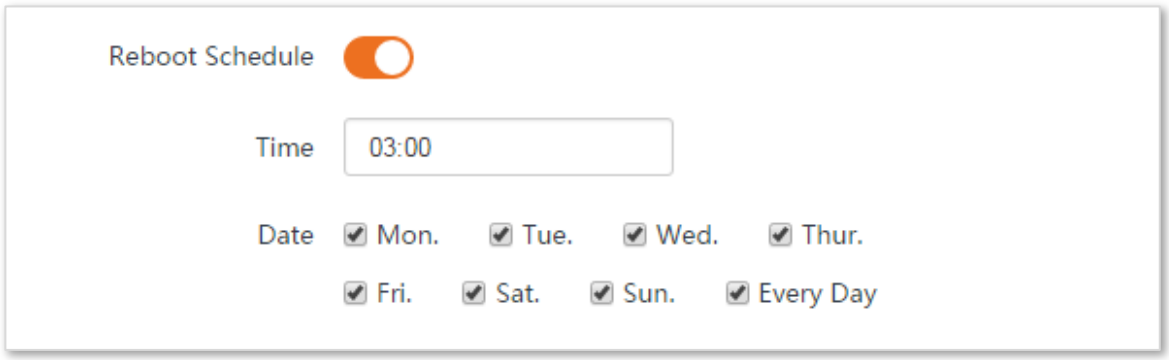
**Step 1** Choose **Advanced** > **Network Service**.

**Step 2** Enable the **Reboot Schedule** function.

**Step 3** Specify a time at which the device reboots.

**Step 4** Specify the dates on which the device reboots.

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

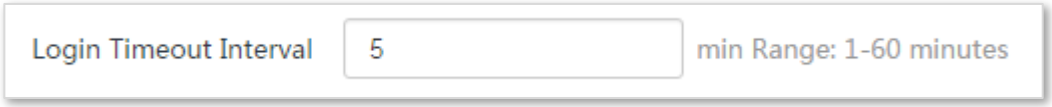



**----End**

## 7.6.4 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.

Choose **Advanced** > **Network Service** to enter the page.



## 7.6.5 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.

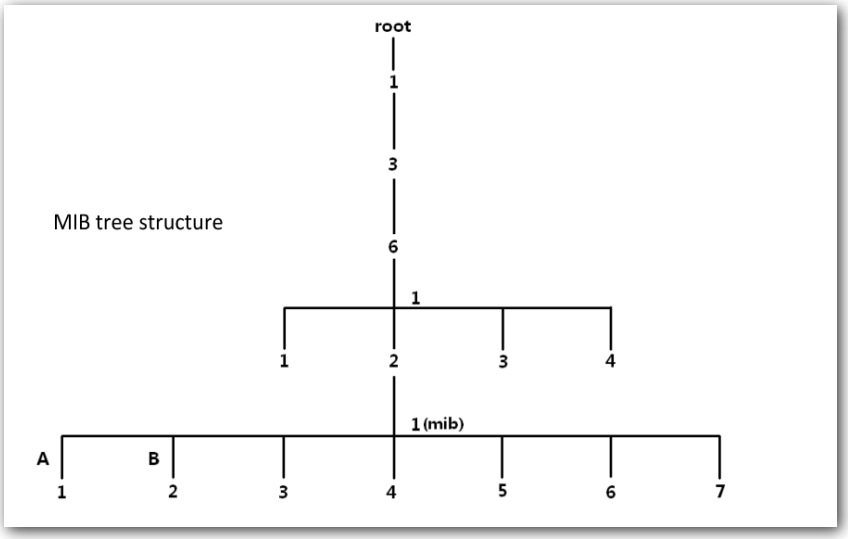
## SNMP Protocol Version

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.



MIB tree structure

## Configuring the SNMP agent function

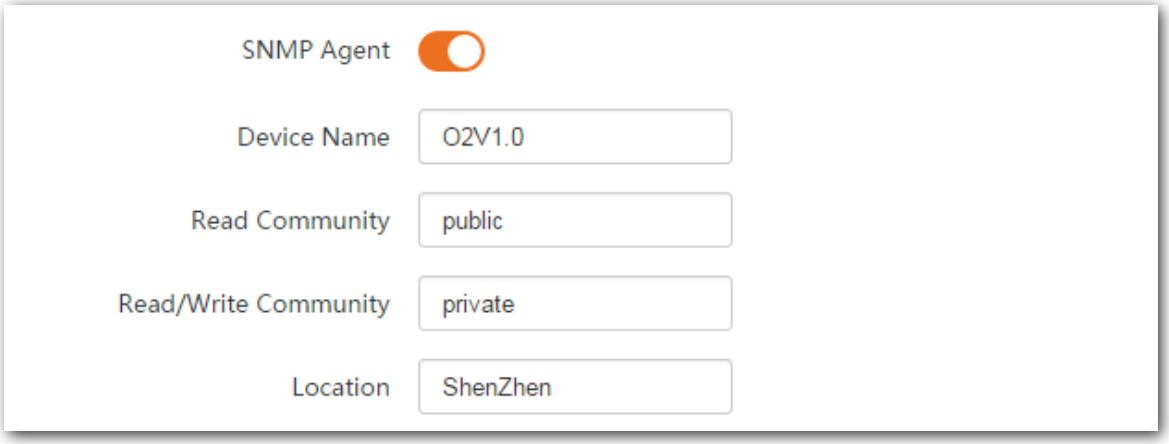
### Configuration procedure

**Step 1** Choose **Advanced** > **Network Service**.

**Step 2** Enable the **SNMP Agent** function.

**Step 3** Set the related SNMP parameters.

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




**----End**

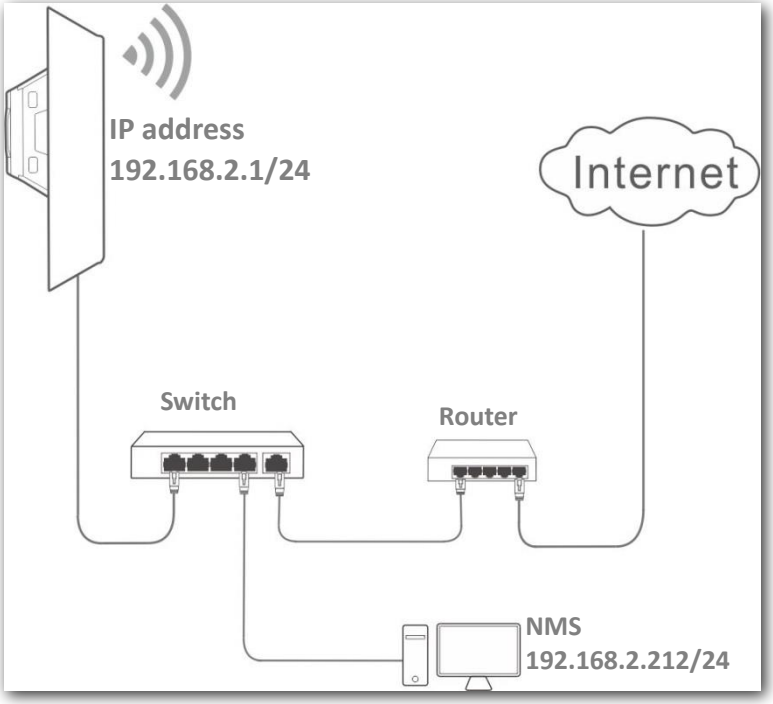
## Parameters description

| Name | Description |
|---|---|
| SNMP Agent | It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled.<br>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 O2V1.0<br>TIP<br>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.<br>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.<br>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.

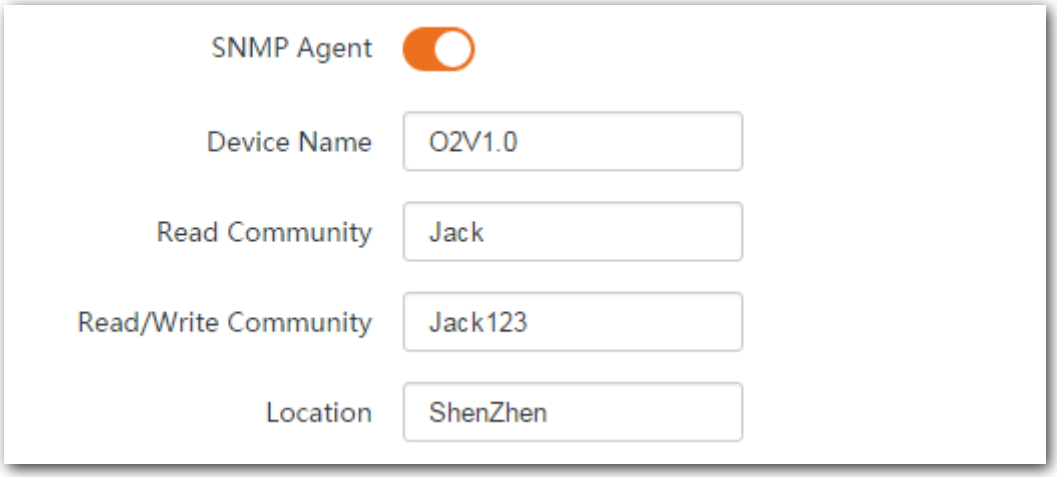



### Configuration procedure

**Step 1** Set up the device.

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

1. 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.




**Step 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.

## 7.6.6 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.

### Configuring ping watch dog

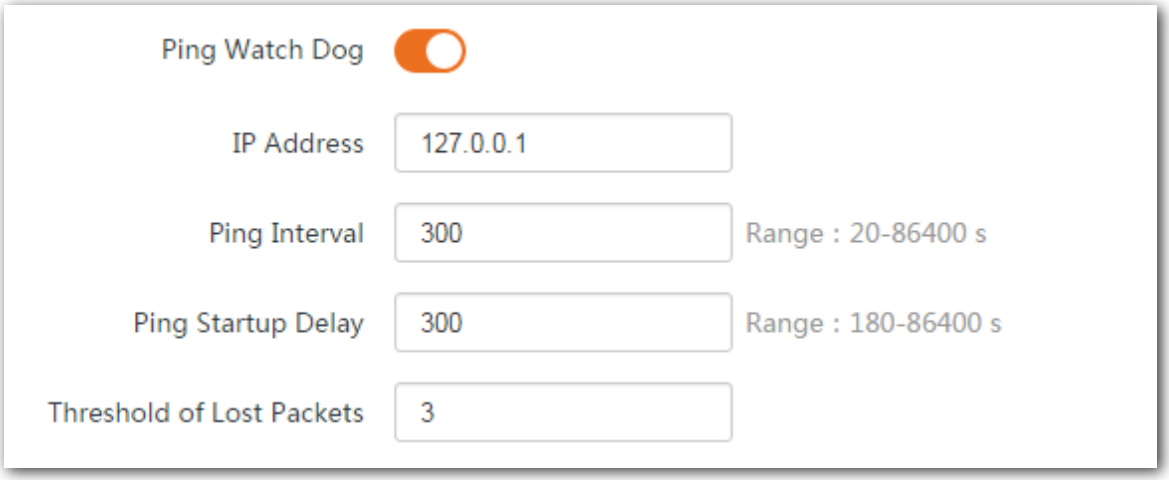
**Configuration procedure**

**Step 1** Choose **Advanced** > **Network Service**.

**Step 2** Enable the **Ping Watch Dog** function.

**Step 3** Set the related parameters.

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




**----End**

**Parameters description**

| Name | 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. |
| Threshold of Lost Packets | It specifies the threshold of lost packet that triggers reboot. Range: 1 to 65535, default: 3.<br>For example, if 5 is set, the device will reboot automatically when it sends 5 Ping packets to target IP address/domain name, and does not receive response. |

## 7.6.7 DMZ host

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

### Overview

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.

## Configuring DMZ host

### Configuration procedure

**Step 1** Choose **Advanced** > **Network Service**.

**Step 2** Enable the **DMZ Host** function.

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

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

**----End**

## Example of configuring DMZ host

### Networking requirement

The device is used in a company to deploy its network, and it is set to Router mode.

**Requirement**: The administrator on business can visit the resources on web server in LAN. You can use DMZ Host function to solve the problem.

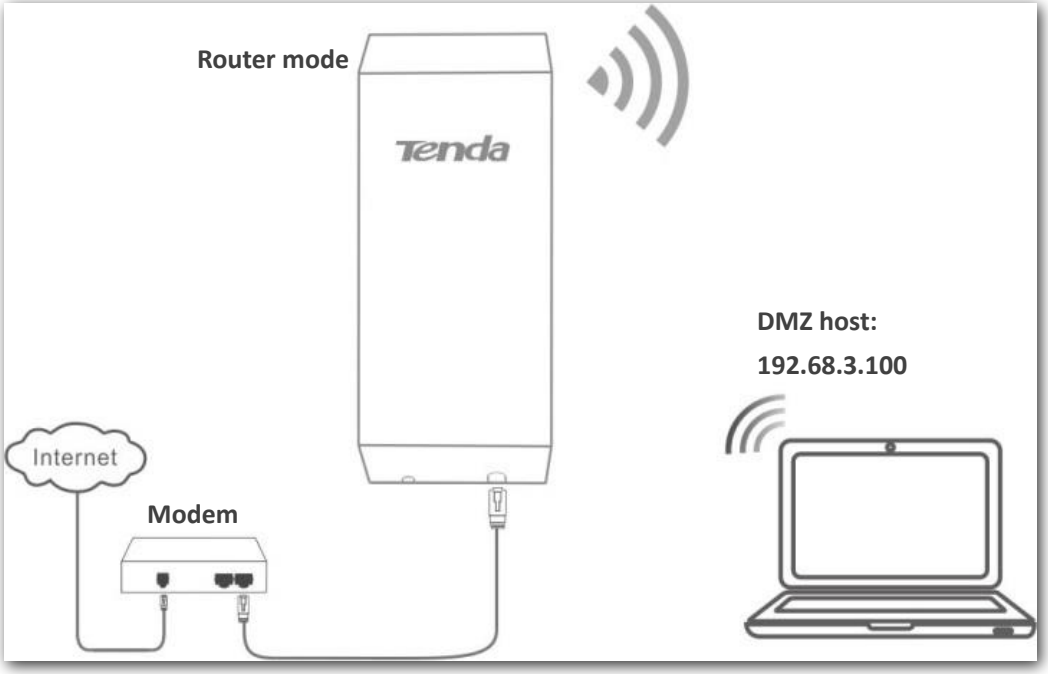
**Assumption:**

The WAN IP address of the device is **202.105.106.55**.
The information of the internal web server is shown as follows:

**IP Address**: 192.168.3.100

**Service Port of the Web Server**: 80

**Network topology**




**Configuration procedure**

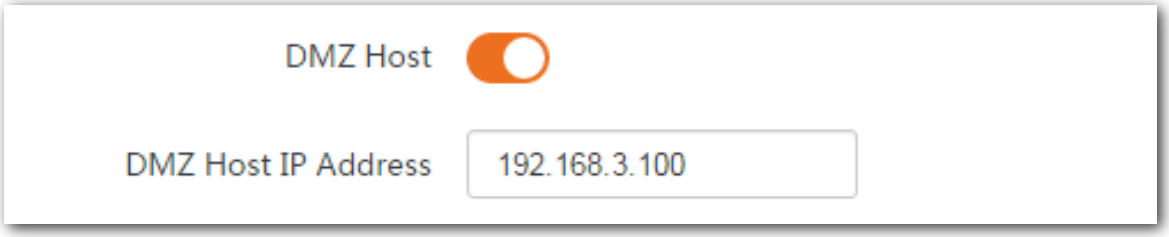
**Prerequisite**: manually set static an IP address and related parameters for the web server to avoid the service disconnection caused by the dynamic IP address.

**Step 1** Choose **Advanced** > **Network Service**.

**Step 2** Enable the **DMZ Host** function.

**Step 3** Enter the IP address of the computer to be set to DMZ host, which is **192.168.3.100** in this example.

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




**----End**

**Verification**

Enter **Protocol name**://**WAN port IP address**:**port number** in the address bar of a web browser on a computer over the internet to access the resources on the web server. In this example, enter **http://202.105.106.55:80**.

If the DDNS function is enabled, you can visit an address in the form of **Protocol name**://**domain name**:**port number.**

TIP

If internet users still cannot visit the web server in LAN after the configuration, try the following solutions:

- Ensure that the WAN IP address of the device is a public IP address.
- Security software, antivirus software, and the built-in OS firewall of the computer may cause the function failures. Disable them and try again.

## 7.6.8 Telnet service

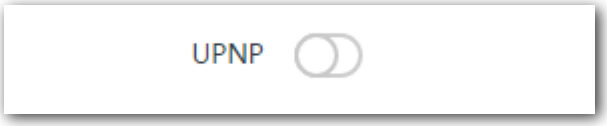
With this function enabled, you can check the information of the device via Telnet.

Choose **Advanced** > **Network Service** to enter the page. By default, the function is enabled.

## 7.6.9 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.

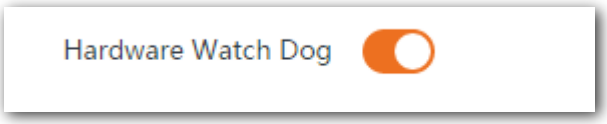
Choose **Advanced** > **Network Service** to enter this page. By default, the function is disabled.




## 7.6.10 Hardware watch dog

This function uses an embedded watchdog timer to detect the operation condition of the device's main program at scheduled time. During normal operation, the device regularly resets the watchdog timer to prevent it from elapsing, or "timing out". If, due to a hardware fault or program error, the device fails to reset the watchdog timer, the timer will elapse and generate a timeout signal. The timeout signal is used to reboot the device to make it recover from malfunctions.

Choose **Advanced** > **Network Service** to enter the page. By default, the function is enabled.



### 7.6.11 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 inability of processing packets caused by receiving duplicate packets.

Choose **Advanced** > **Network Service** to enter the page. By default, the function is disabled.

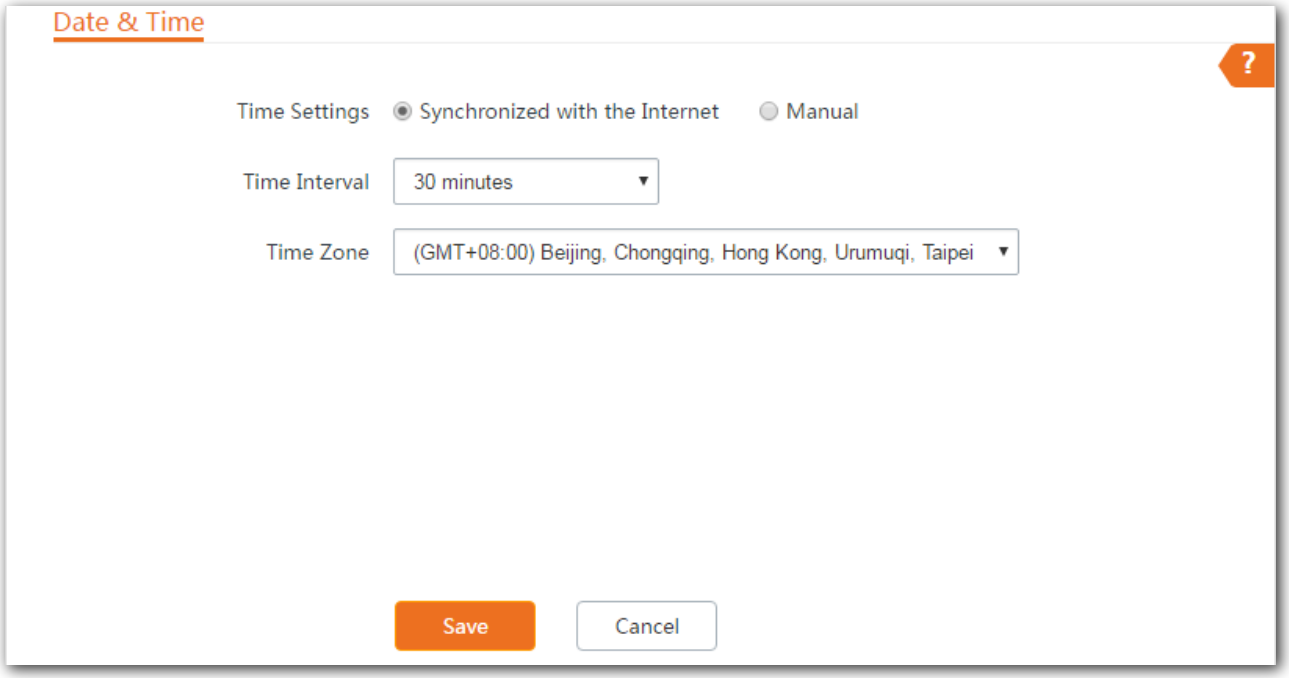
# 8 Tools

## 8.1 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 logs can be recorded correctly and the reboot schedule can be executed correctly.

Choose **Tools** > **Date & Time** to enter the page.




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.

### Synchronized with the Internet

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 device to the internet, refer to LAN Setup.

### Configuration procedure

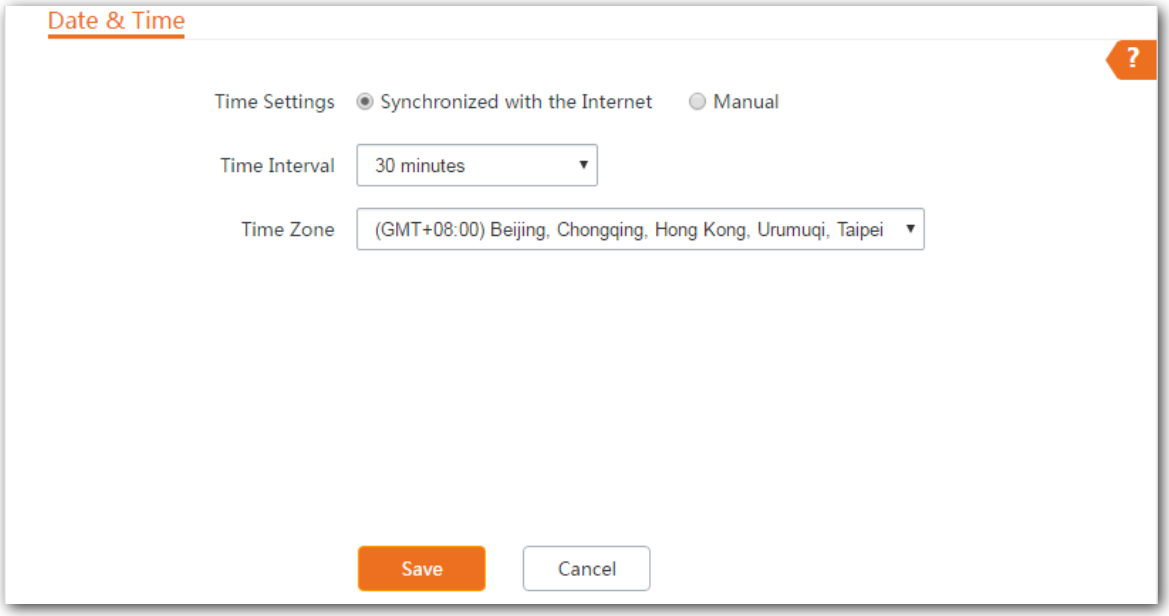
**Step 1** Choose **Tools** > **Date & Time**.

**Step 2** Set **Time settings** to **Synchronized with the Internet**.

**Step 3** Specify a time interval. The default value **30 minutes** is recommended.

**Step 4** Set **Time Zone** to your time zone.

**Step 5** Click **Save**.




**----End**

## Manual

You can manually set the system time of the device. If you choose this option, you need to set the system time each time after the device reboots.

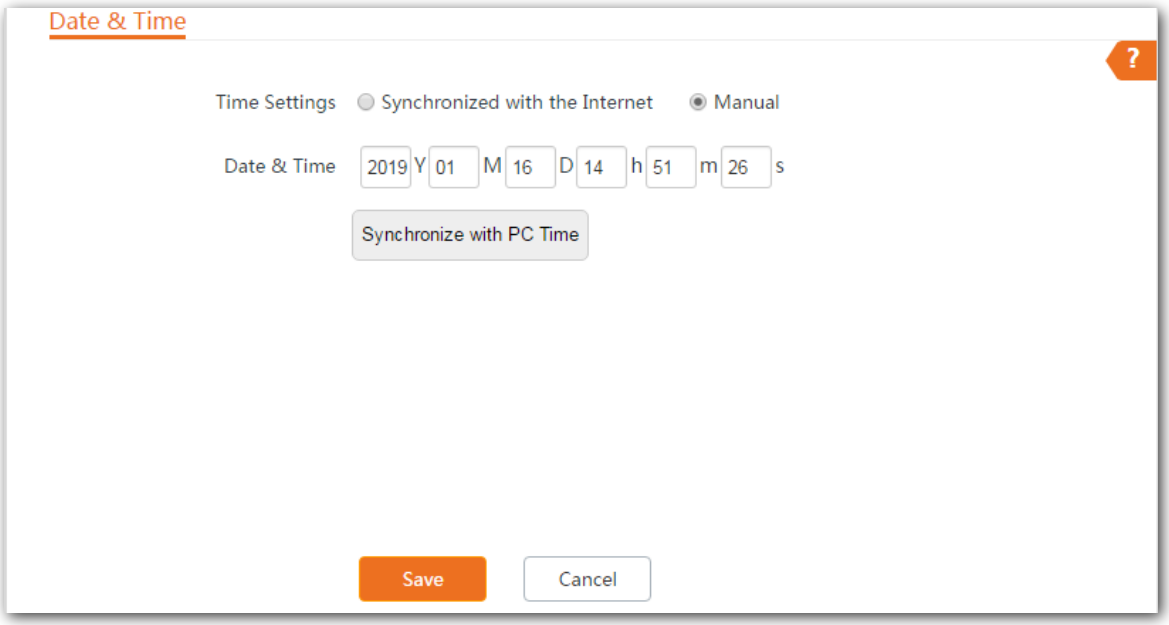
### Configuration procedure

**Step 1** Choose **Tools** > **Date & Time**.

**Step 2** Set the **Time Settings** to **Manual**.

**Step 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 (ensure that it is correct) of the computer being used to manage the device.

**Step 4** Click **Save**.




**----End**

# 8.2 Maintenance

## 8.2.1 Reboot device

If a setting does not take effect or the device works improperly, you can try rebooting the device to resolve the problem.

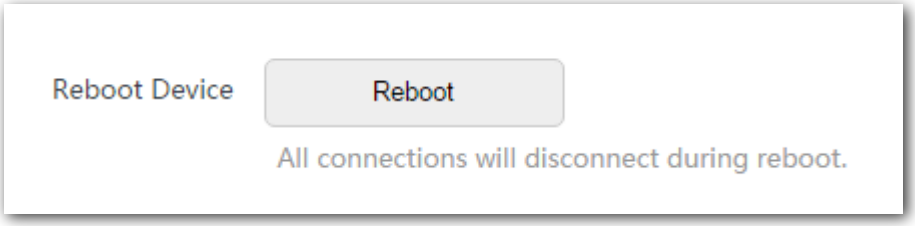
TIP

When the device reboots, the current connections will be disconnected. Perform this operation when the device does not work busy.

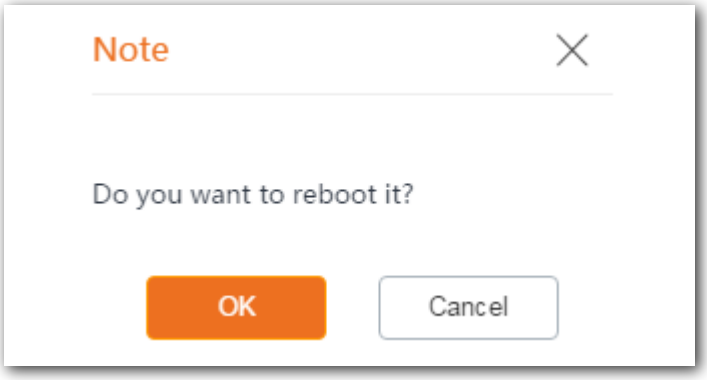
### Configuration procedure

**Step 1** Choose **Tools** > **Maintenance**.

**Step 2** Click **Reboot**.




**Step 3** Click **OK** on the pop-up window.




**----End**

A progress bar is displayed on the page. Wait for it to elapse.

## 8.2.2 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.

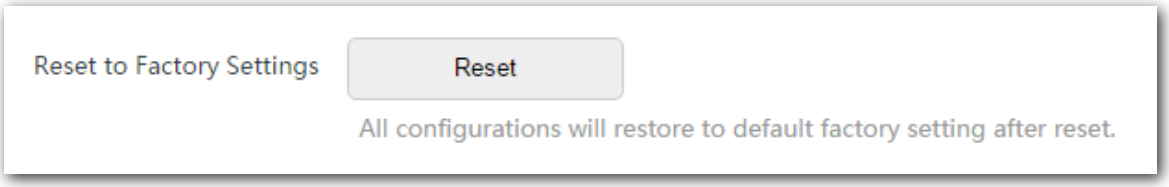
NOTE

- When the factory settings are restored, the configuration of the device is lost. Therefore, you need to reconfigure the device to connect to the internet. Restore the factory settings of the device only when necessary.
- To prevent device damages, ensure that the power supply of the device is normal when the device is reset.
- When the factory settings are restored, the login IP address is 192.168.2.1, and both login user name and password are **admin**.

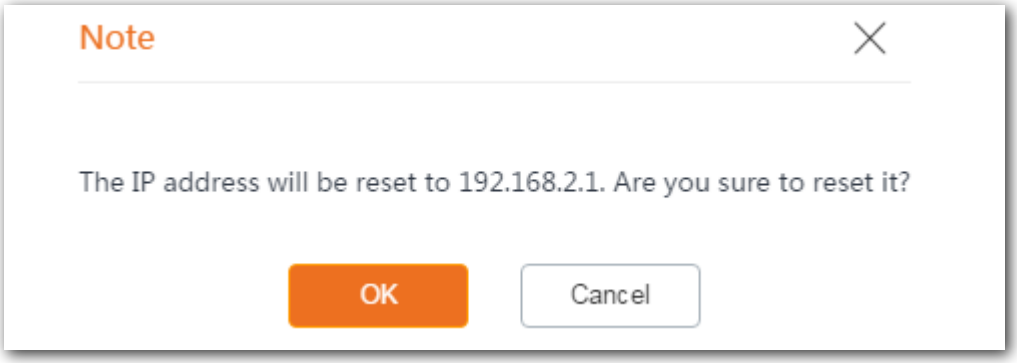
### Configuration procedure

**Step 1** Choose **Tools** > **Maintenance**.

**Step 2** Click **Reset**.




**Step 3** Click **OK** on the pop-up window.




**----End**

A progress bar is displayed on the page. Wait for it to elapse.

## 8.2.3 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

**Step 1** Download the package of a later firmware version for the device from http://www.tendacn.com to your local computer, and decompress the package.

**Step 2** Log in to the web UI of the device and choose **Tools** > **Maintenance**.

**Step 3** Click **Upgrade**.

**Step 4** Select the file from your local computer for upgrading the firmware.

After the firmware is upgraded, you are recommended to restore the factory settings of the device and configure it again, so as to ensure stability of the device and proper operation of new functions.

**----End**

A progress bar is displayed on the page. Wait for it to elapse. Then Log in to the web UI of the device, and check the **Firmware Version** on the **Status** page, and ensure that the version displayed here is the same as the firmware you upgrade.

## 8.2.4 Backup/restore

The backup function enables you to back up the current configuration of the device to a local computer. The restoration function enables you to restore the device to a previous configuration.

If the device enters the optimal condition after you greatly change the configuration of the device, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the device.

NOTE

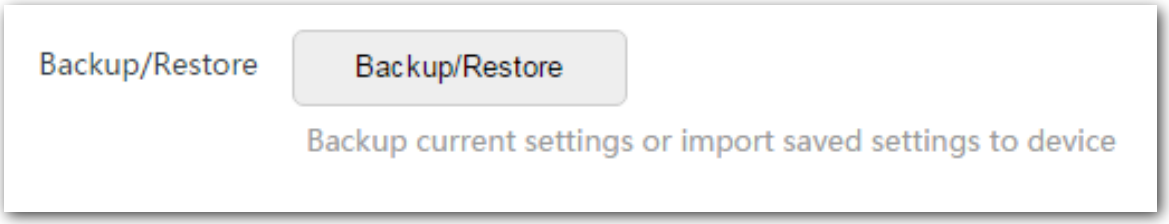
If you need to apply same or similar configurations to many devices, you can configure one of the devices, back up the configuration of the device, and use the backup to restore the configuration on the other devices. This improves configuration efficiency.

### Backup

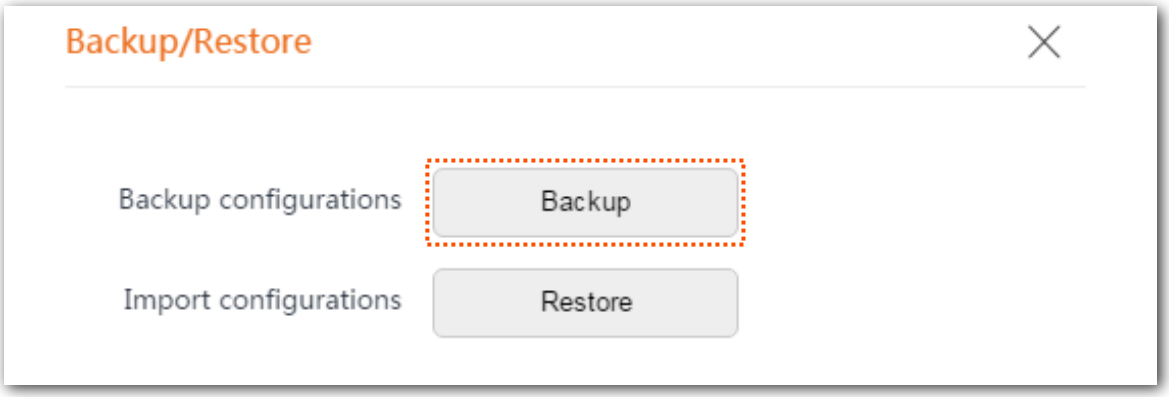
#### Configuration Proceudre

**Step 1** Choose **Tools** > **Maintenance**.

**Step 2** Click **Backup/Restore**.




**Step 3** Then click **Backup** on the pop-up window.




**----End**

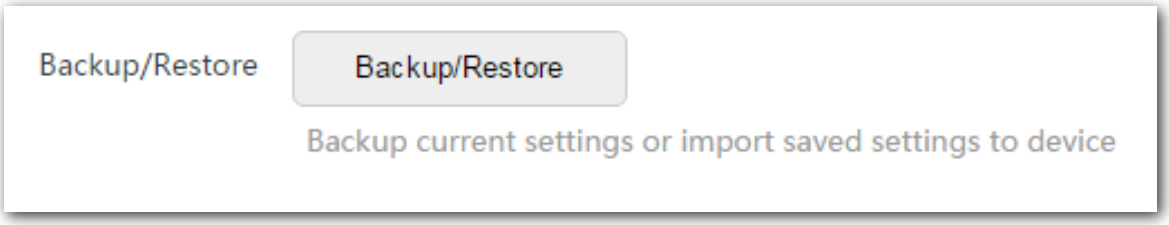
A file named **APCfm.cfg** is downloaded to your local computer.

## Restore

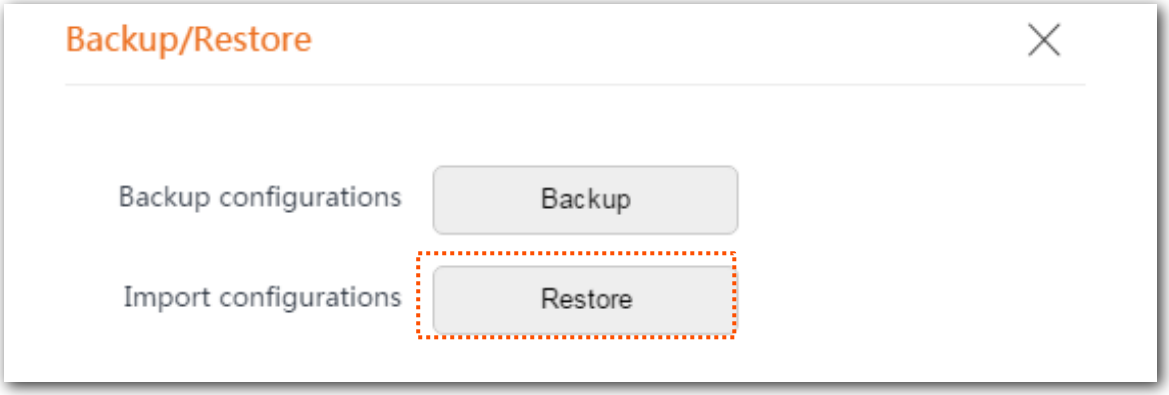
### Configuration procedure

**Step 1** Choose **Tools** > **Maintenance**.

**Step 2** Click **Backup/Restore**.



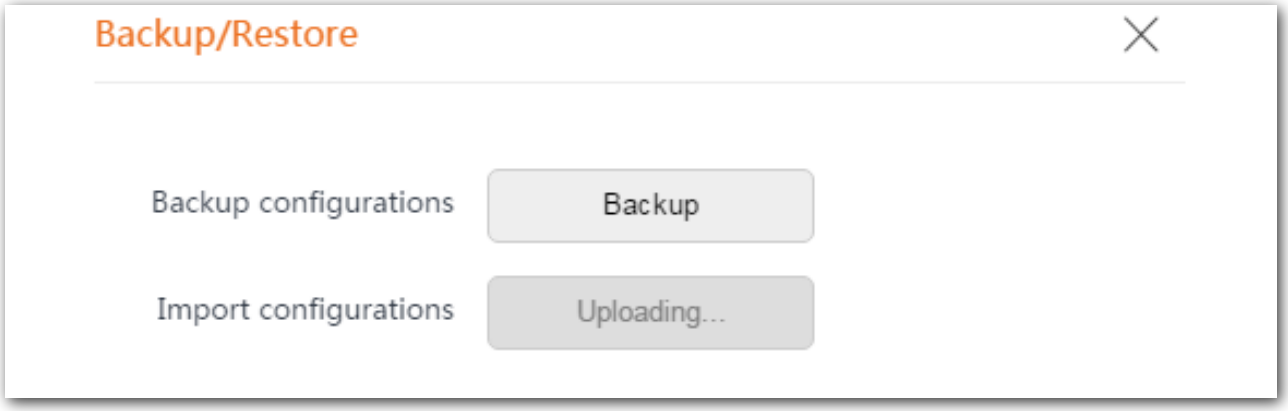

**Step 3** Click **Restore** on the pop-up window.




**Step 4** Select and upload the file you back up before.

**----End**

The file is being uploaded.



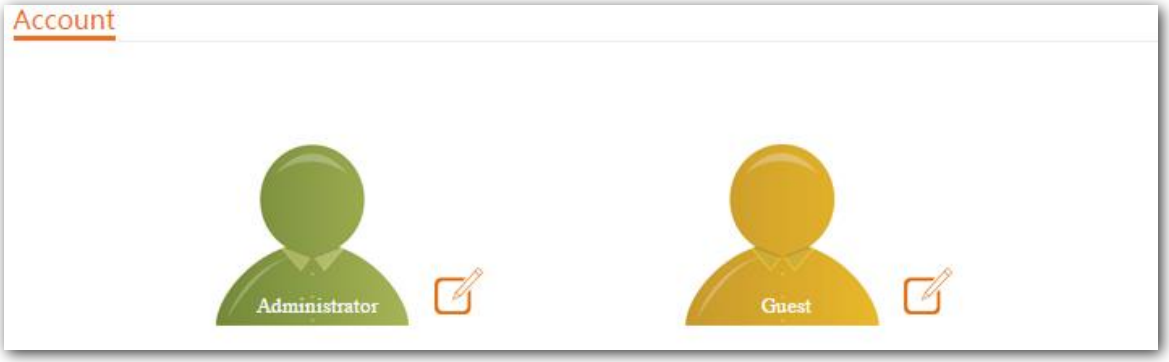

A progress bar is displayed on the page. Wait for it to elapse. Then the device is restored the settings successfully.

# 8.3 Account

To access the page, choose **Tools** > **Account**.

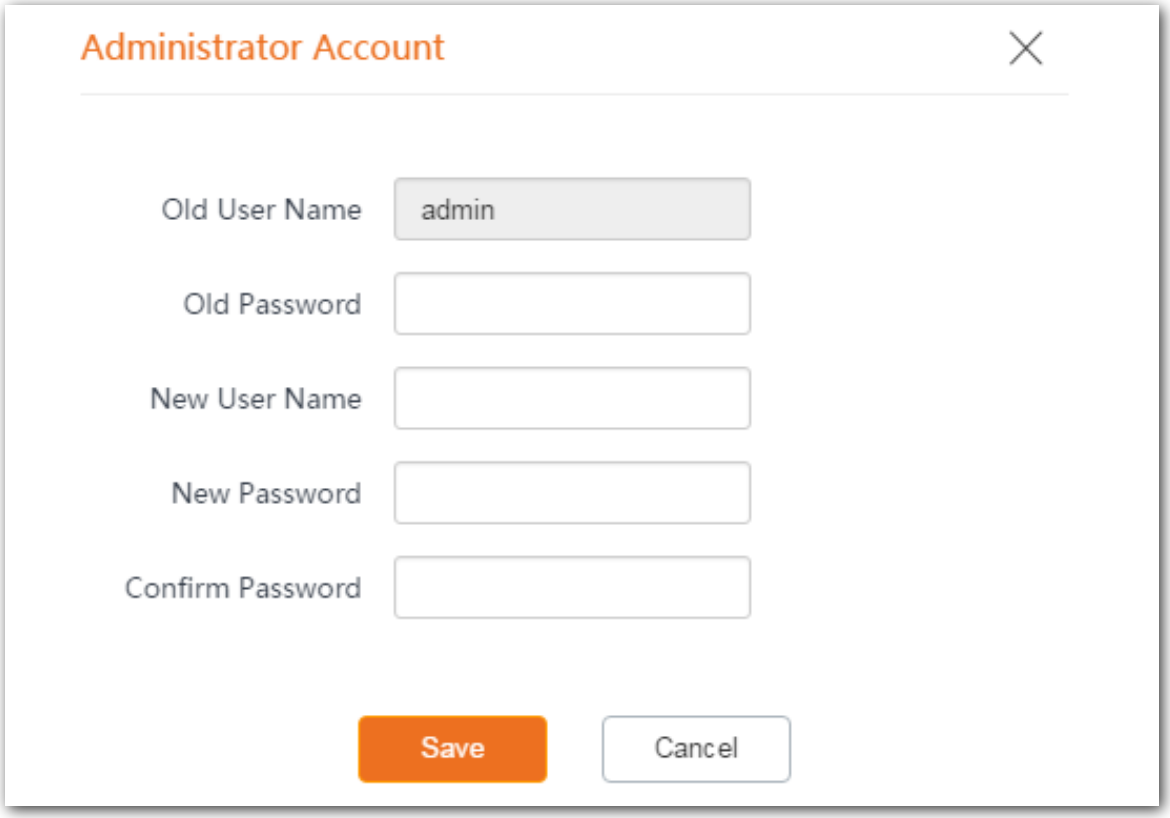
On this page, you can change the login account information of the device to prevent unauthorized login. By default, the device has one administrator account and one guest account. With the administrator account, you can modify and view the settings of the device while with the guest account, you can only view the settings.

Click to change the account information.



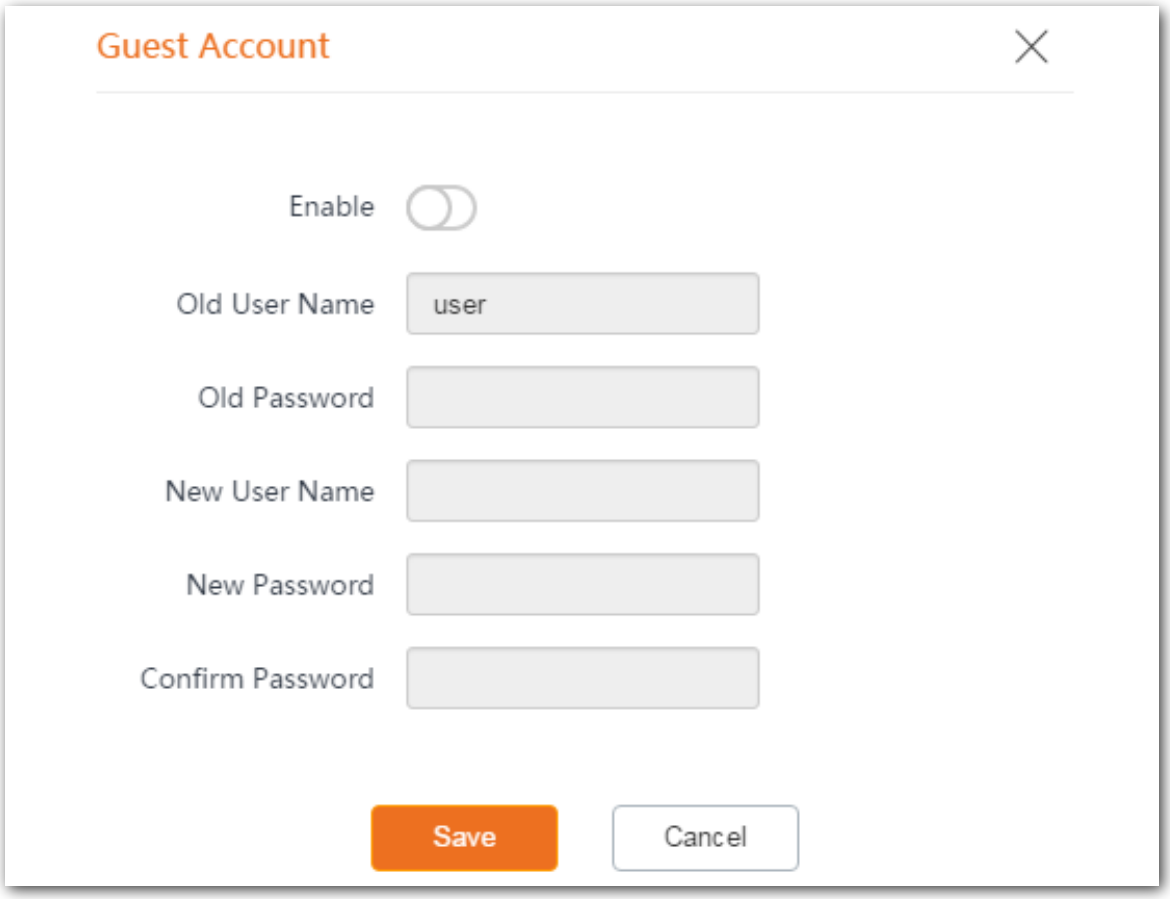

## 8.3.1 Administrator

You can modify and view the settings with the administrator account.




### 8.3.2 Guest

This account only allows you to view the settings. By default, this account is disabled.



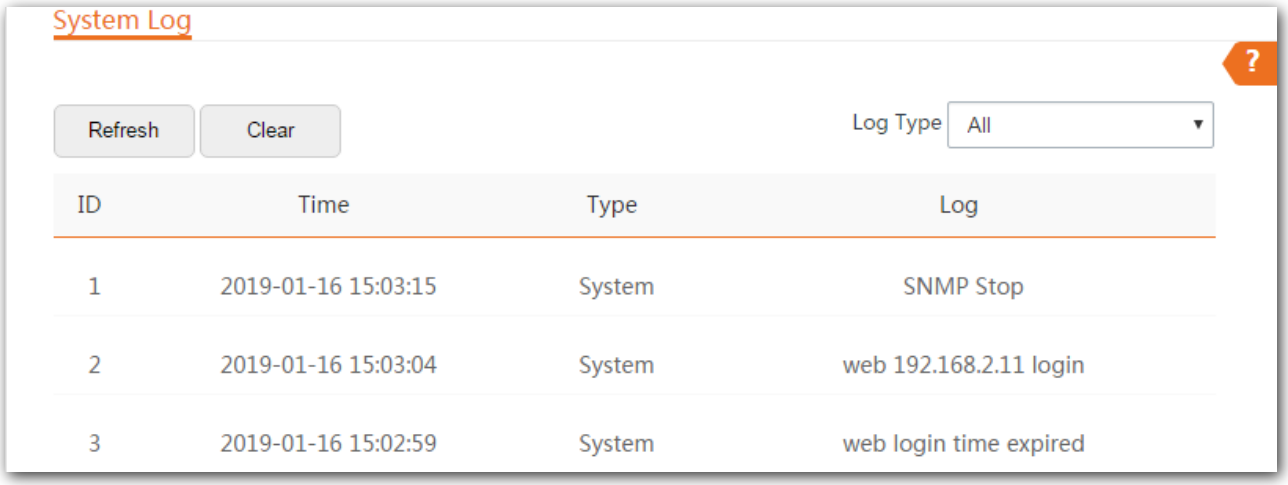

### Parameters description

| Name | Description |
|---|---|
| Old User Name | It specifies the user name of the current login account.<br>By default, the device has one administrator account and one guest account.<br>Administrator user name/password: admin/admin (all lowercase)<br>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 new login password again. |

# 8.4 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.




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 lost.
- 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 FAQ

**Q1: I cannot log in to the web UI of the device by entering 192.168.2.1. What should I do?**

Try the following methods:

- Ensure that the device has been connected to the power supply and the computer properly.
- Ensure that the IP address of the login computer is 192.168.2.*X* (*X* ranges from 2 to 254).
- If the CPE has performed one-to-one bridge, its IP address is changed to 192.168.2.2. Visit the new IP address for login.
- If the CPE is set to Router mode, the PoE/LAN port is changed to a WAN port. You need to connect to the wireless network of the CPE, and visit its LAN IP address for login.
- Restore the device to factory settings.

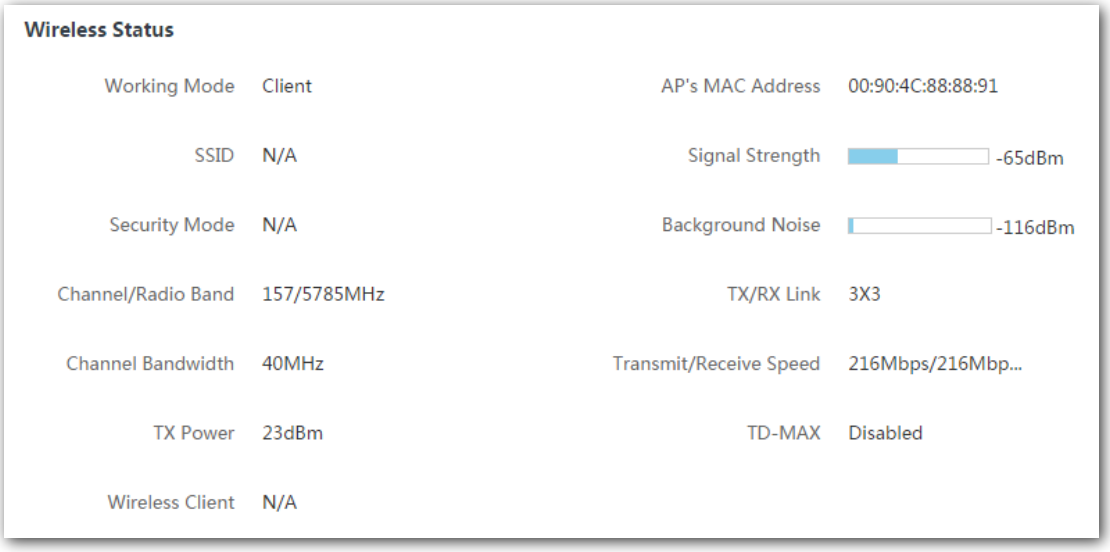
**Q2: How to reset the device to factory settings?**

**Note: Resetting the device clears all settings, and you need to configure it again.**

- **Method One**: 1 minute after the device is powered on, remove the cover of the device, and hold down the **Reset** button for about 8 seconds. When all LED indicators light up once, the device is restored to factory settings.
- **Method Two**: Log in to the web UI of the device, choose **Tools** > **Maintenance**, and click the **Reset** button.

**Q3: How to determine whether the signal strength LED indicators are optimal when the devices are used for CCTV surveillance?**

- **Option One**: Observe the LED indicators of the devices. The bridging signal is optimum when all of the LED1, LED2 and LED3 indicators are solid on or blinking.
- **Option Two**: Log in to the web UI of one device, choose **Status**, and check the **Wireless Status** on the following page:

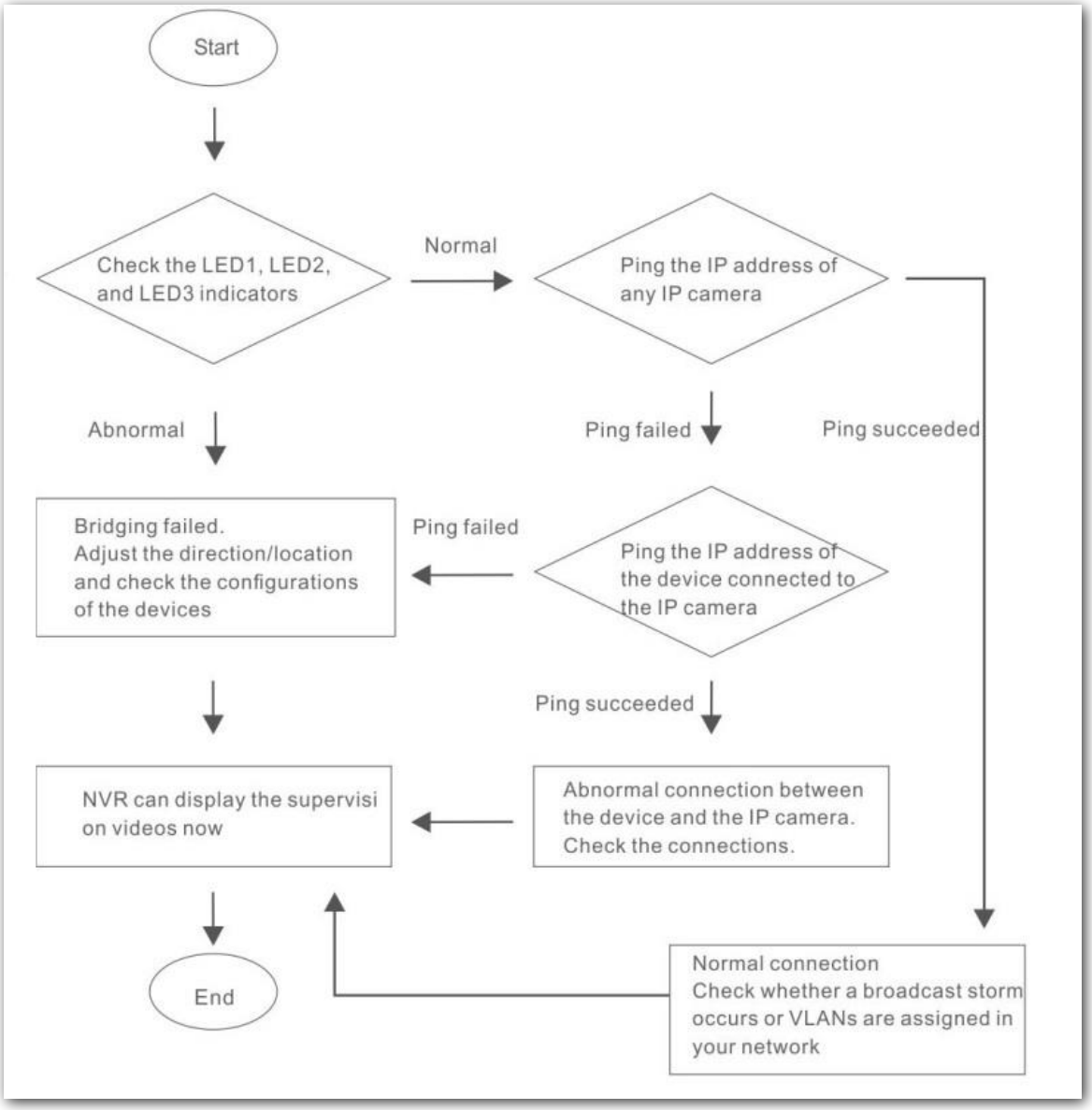



Stronger signal strength (-60 is better than -70) and less background noise (-100 is better than -90) lead to better bridging signal.

**Q4: After the installation succeeds, the IP cameras connected to the NVR cannot display the surveillance videos. What should I do?**

Try the following solutions:

- Ensure that all devices are working normally, and connected properly.
- Refer to the following figure to find the problem. Ensure that the IP addresses of computer, NVR, and IP cameras are in the same network segment.


Start
Check the LED1, LED2, and LED3 indicators
Normal
Ping the IP address of any IP camera
Abnormal
Ping failed
Ping succeeded
Bridging failed. Adjust the direction/location and check the configurations of the devices
Ping failed
Ping the IP address of the device connected to the IP camera
Ping succeeded
NVR can display the supervisi on videos now
Abnormal connection between the device and the IP camera. Check the connections.
End
Normal connection
Check whether a broadcast storm occurs or VLANs are assigned in your network

# A.2 Default parameters

By default, the parameters are shown in the following table:

| Parameters | | | O2 |
|---|---|---|---|
| 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 | | O2V1.0 |
| 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 | | O2 | |
|---|---|---|---|
| | Country/Region | China | |
| | SSID | Tenda_XXXXXX, and 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 | 23 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 | 3 km | |
| | Beacon Interval | 100ms | |
| | Fragment Threshold | 2346 | |
| | RTS Threshold | 2347 | |
| | DTIM Interval | 1 | 1 |

| Parameters | | O2 |
|---|---|---|
| | 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 |
| | 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<br>(GTM+8:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei<br>Time Interval: 30 minutes |