# User Guide

Outdoor CPE



Features available in the CPE may vary by model and software version. CPE availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual CPE experience.

## Copyright statement

© 2020-2026 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 reference 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

This guide describes how to configure each feature of the following Tenda CPEs.

- O1 V1.0
- O1-5G V2.0
- OS3 V2.0
- O4 V3.0
- O6 V3.0

NOTE

Features available in the CPE may vary by model and software version. CPE availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual CPE experience.

In this guide, unless otherwise specified, all screenshots are taken from O6 V3.0 working in AP mode.

## 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 the device. |
| TIP | This format is used to highlight a procedure that will save time or resources. |

## More information and support

Visit www.tendacn.com and search for the product model to get your questions answered and get the latest documents.

## Revision history

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the manual was released.

| Version | Date | Description |
| --- | --- | --- |
| V2.4 | 2026.08.21 | Optimized sentence expression. |
| V1.0 – V2.3 | 2020.07 – 2025.12 | Historical versions |

# Contents


**Typical usage scenarios** **1**
1.1 CCTV surveillance 1
1.2 ISP hotspot connection 8

**Log in to web UI** **12**
2.1 Login 12
2.2 Logout 17
2.3 Web UI 18
2.4 Common buttons 19

**Set up device mode** **20**
3.1 AP mode 21
3.2 Client mode 23
3.3 Universal Repeater mode 27
3.4 WISP mode 31
3.5 Router mode 37

**Get device information** **42**
4.1 System status 42
4.2 Wireless status 44
4.3 Statistics 47

**Manage network settings** **53**
5.1 LAN setup 53
5.2 Packet filter 58
5.3 MAC clone 60
5.4 DHCP server 62
5.5 DHCP client 64
5.6 VLAN settings 64
5.7 Network topology 69

**Manage wireless settings** **70**
6.1 Basic configuration 70
6.2 Advanced settings 102
6.3 Access control 105
6.4 Management RF 108

**Advanced** **111**
7.1 LAN rate 111
7.2 Diagnose 112
7.3 Bandwidth control 121
7.4 Port forwarding 124
7.5 MAC filter 127
7.6 Network service 130

**Tools** **150**
8.1 Date & time 150
8.2 Maintenance 152
8.3 Account 158
8.4 System log 159

**Appendix** **160**
A.1 Default parameters 160
A.2 Acronyms and Abbreviations 162
A.3 Assign a fixed IP address to your computer 164
A.4 How to check the gateway IP address of a computer 166

# 1 Typical usage scenarios

TIP

- At least two CPEs are required for bridging. Different application scenarios require different CPE models. For more information, visit www.tendacn.com.
- A CPE can be used with multiple cameras. The specific number of cameras can be calculated by the formula (Number of Cameras = CPE Sending/Receiving Rate * 70% ÷ Camera Stream).

## 1.1 CCTV surveillance

To ensure the personal and property safety of residents, a community needs to install surveillance cameras for real-time monitoring.

### 1.1.1 Solution

- **Method 1**: Use a 2-pack CPE to set up a monitoring network, such as O1-5G. You only need to install the CPEs to easily manage CCTV surveillance for the community.
- **Method 2**: Use two CPEs to set up a monitoring network, such as O6. To manage CCTV surveillance for the community, configure the CPEs > install the CPEs.

TIP

To quickly set up a monitoring network, it is recommended to configure the CPEs before installation.

## 1.1.2 Configure the CPEs

### Option 1: Peer-to-peer automatic bridging (recommended)

NOTE

- Automatic bridging only applies when the CPEs are in factory settings.
- When performing peer-to-peer automatic bridging, ensure that only two CPEs are powered on and near each other. Otherwise, the bridging may fail.
- After the bridging succeeds, the DHCP service of the CPE is automatically disabled. The IP address of the CPE working in AP mode remains unchanged (192.168.2.1), and the IP address of the CPE working in Client mode is changed to 192.168.2.2.

1. Place the two CPEs next to each other.
2. Power on the CPEs.

   CPEs can be powered on through a PoE injector, DC power, or standard PoE power. Different models support different power supply methods. The actual product prevails.

TIP

- If the CPE supports DC power supply, you can use the correct power adapter to power on the CPE. The power parameters can be checked on the DC power jack. If the power adapter (5.5×2.1 mm) is not included in the product package, purchase one.
- Some CPEs can be powered on by IEEE 802.3af PoE power supply devices. For more details, visit www.tendacn.com, search by a model, then check technical information on the **Specification** page.
- The maximum PoE power supply distance varies by the model. For more details, visit www.tendacn.com, search by a model, download the datasheet from the **Download** page, then check the maximum PoE power supply distance.

**---End**

After the two CPEs are powered on, they start bridging each other with their LED1, LED2 and LED3 indicators blinking fast. When the LED1, LED2 and LED3 indicators of one CPE are lit solid and the same indicators of the other CPE blink slowly, the peer-to-peer bridging succeeds.

TIP

If peer-to-peer automatic bridging fails, reset the CPEs to factory settings and try again. To reset a CPE, hold down the reset button (such as RST, RESET or Reset) for about 8 seconds, and then release it when all the indicators light up. The reset button works only after the CPE has started up.

### Option 2: Manual bridging

1. Place the two CPEs next to each other.
2. Log in to the web UI of the CPE1.

   1) Power on the CPE1.

CPEs can be powered on through a PoE injector, DC power, or standard PoE power. Different models support different power supply methods. The actual product prevails.

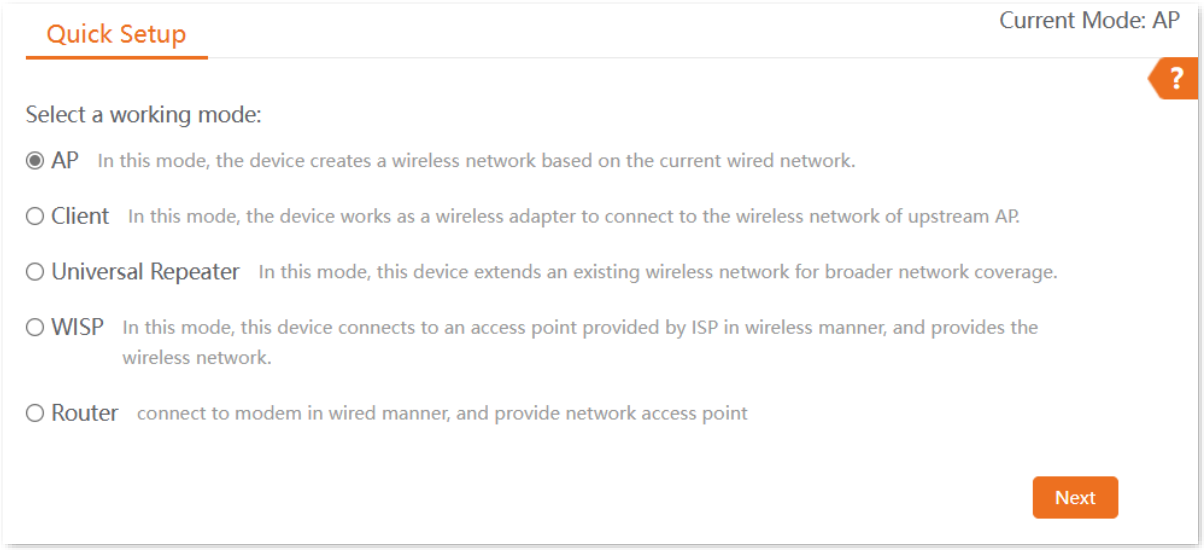
TIP

- If the CPE supports DC power supply, use the correct power adapter to power on the CPE. The power parameters can be checked on the DC power jack. If the power adapter (5.5×2.1 mm) is not included in the product package, purchase one.
- Some CPEs can be powered on by IEEE 802.3af PoE power supply devices. For more details, visit www.tendacn.com, search by a model, then check technical information on the **Specification** page.
- The maximum PoE power supply distance varies by the model. For more details, visit www.tendacn.com, search by a model, download the datasheet from the **Download** page, then check the maximum PoE power supply distance.

2) Log in to the web UI of the CPE1.

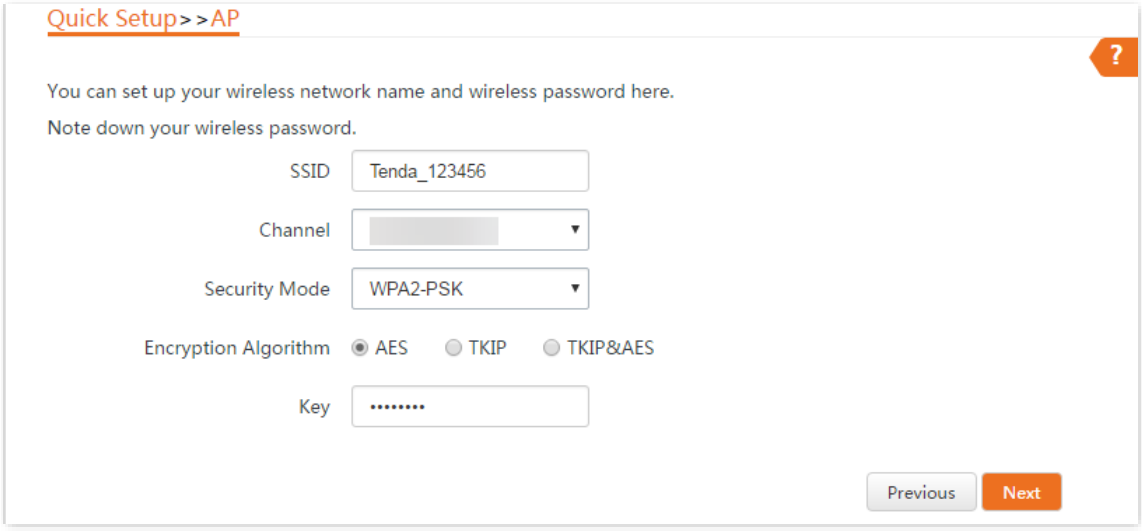
3. Set CPE1 to AP mode.

1) Navigate to **Quick Setup**. Select **AP** mode, and click **Next**.

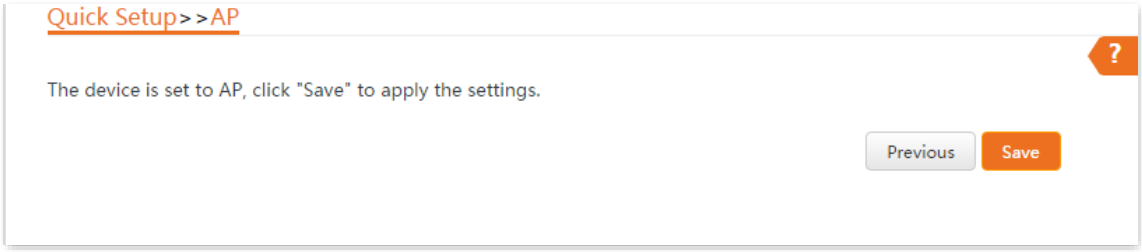



2) Set wireless network parameters and click **Next**.

- Set an **SSID** (Wi-Fi name), which is **Tenda_123456** in this example.
- Set **Security Mode**, which is **WPA2-PSK** in this example.
- Set **Encryption Algorithm**, which is **AES** in this example.
- Set **Key** (Wi-Fi password).



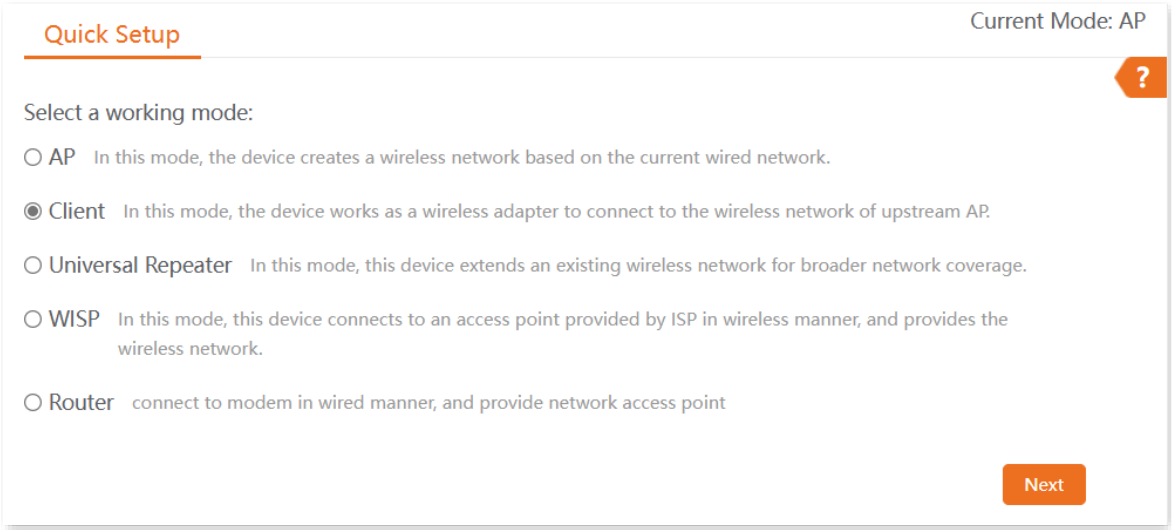

3) Click **Save**, and wait until the CPE reboots to make the settings take effect.




4. Log in to the web UI of the CPE2 and set it to Client mode.

1) Refer to step 2 to log in to the web UI of the CPE2.

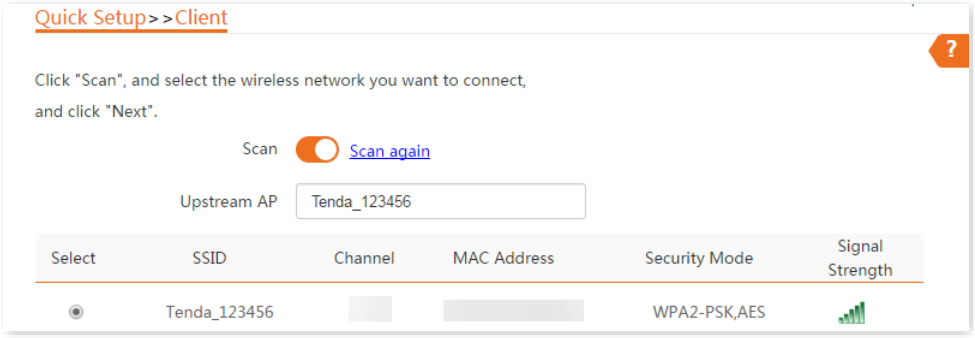
2) Navigate to **Quick Setup.** Select **Client** mode, and click **Next.**



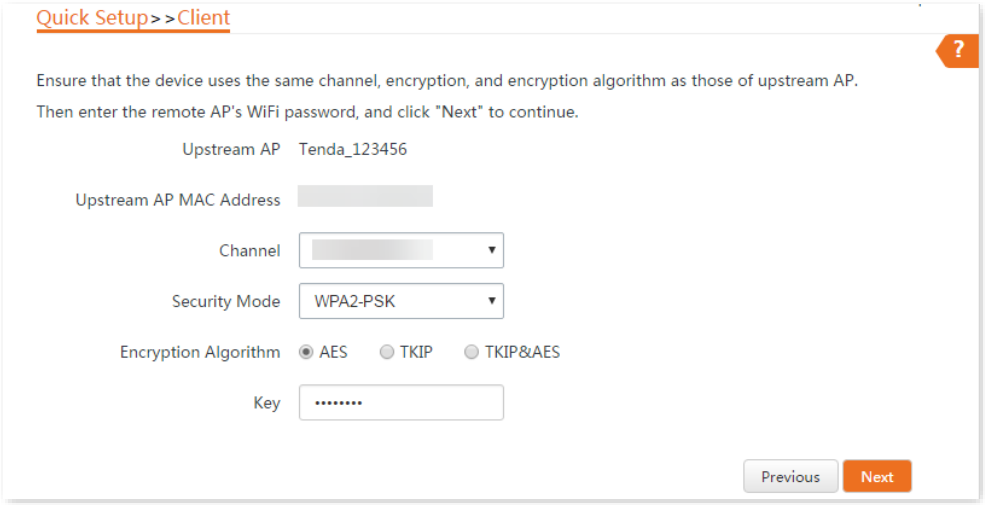

3) Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next**.

TIP

If you cannot find any wireless network from the list, navigate to **Wireless** > **Basic** and enable the wireless function. Then try again.

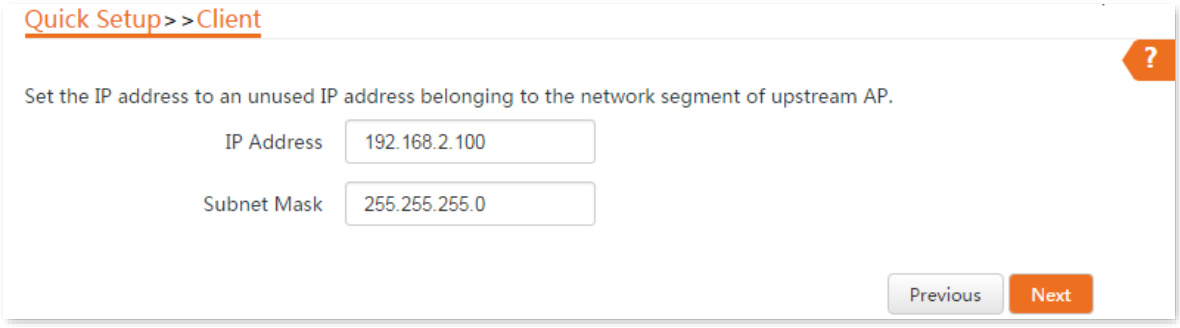



**4)** Enter the Wi-Fi password of the upstream wireless network in the **Key** field, and click **Next**.

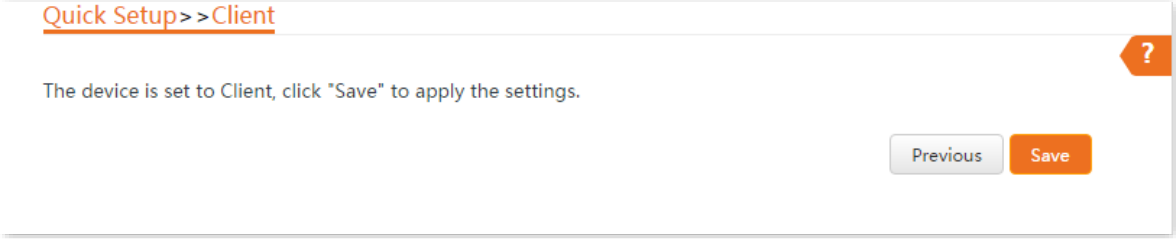



**5)** Modify the **IP address**, and click **Next**.

- Set the IP address of CPE2 to an unused IP address belonging to the same subnet as CPE1, which is **192.168.2.100** in this example.
- Set the subnet mask to the same one used by CPE1, which is **255.255.255.0** in this example.




**6)** Click **Save**, and wait until CPE2 reboots to make the settings take effect.



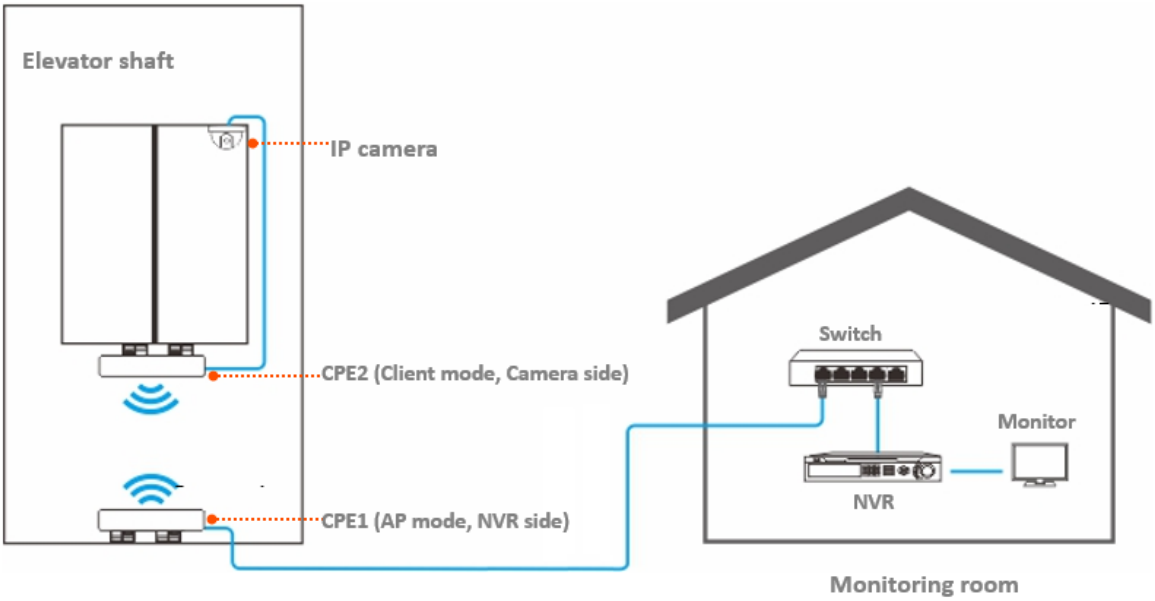

**---End**

When the two CPEs start bridging each other, all the LED1, LED2 and LED3 indicators blink fast. When the LED1, LED2 and LED3 indicators of one CPE are lit solid and the same indicators of the other CPE blink slowly, the bridging succeeds. To check the SSID and key of the CPE, you can log in to the web UI of the CPE and navigate to **Wireless** > **Basic**.

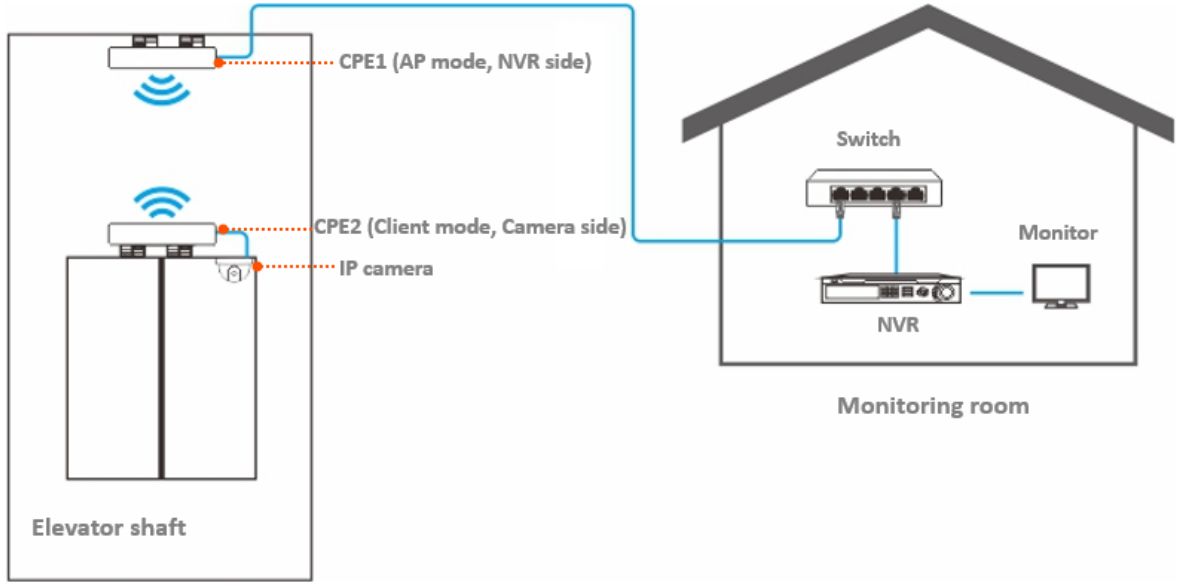
### 1.1.3 Install the CPEs

Select any of the following scenarios based on the location of the monitoring room and install the CPE accordingly.

- When the monitoring room is closer to the **bottom** of the elevator shaft, refer to **Scenario 1** for installation.
- When the monitoring room is closer to the **top** of the elevator shaft, refer to **Scenario 2** for installation.




**Scenario 1**




**Scenario 2**

Check the LED1, LED2 and LED3 indicators of the CPEs to confirm whether the positions are proper. The more indicators light up, the better the connection quality is.

O6 is used for illustration here. The table below describes signal indicators.

| Indicator | Status | Description |
|---|---|---|
| LED1, LED2, LED3<br>(signal indicators) | Solid on/Blinking | The CPE is connected to a device.<br>– Solid on: The CPE may work in AP or Router mode.<br>– Blinking: The CPE may work in Client, Universal Repeater or WISP mode.<br>The more LED indicators are on, the stronger the received signal and the better the connection quality.<br>TIP<br>– You can make changes on the **Wireless** > **Advanced** page of the web UI of the CPE.<br>– Different models of CPEs have different indicators and working modes. The actual product prevails. |
| | Off | No device is connected to the CPE, or the received signal strength is less than the RSSI threshold. |

# 1.2 ISP hotspot connection

The internet access in an apartment needs to be achieved by connecting an Internet Service Provider (ISP) hotspot.

## 1.2.1 Solution

O6 V3.0 is used as an example to illustrate the installation procedures. Procedures for other CPE models are similar.

TIP

To complete the setup more quickly, configure the CPE before installation.

## 1.2.2 Configure the CPE

1. Power on the CPE.

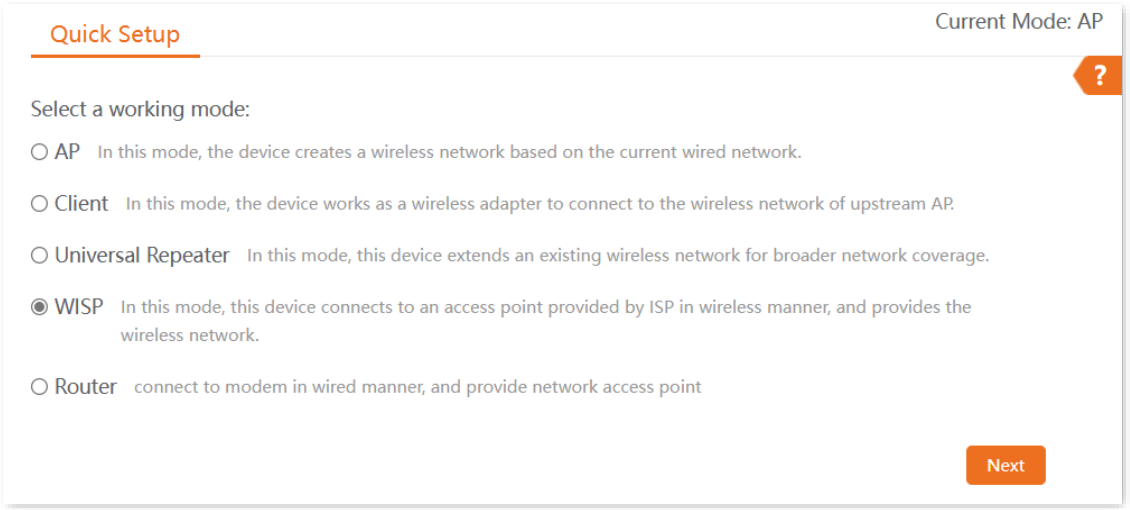
   CPEs can be powered on through a PoE injector, DC power, or standard PoE power. Different models support different power supply methods. The actual product prevails.

TIP

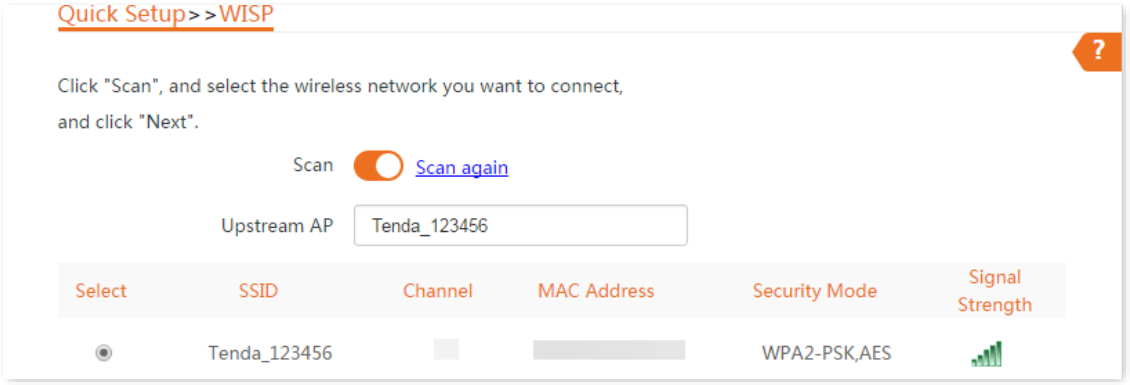
- If the CPE supports DC power supply, use the correct power adapter to power on the CPE. The power parameters can be checked on the label of the CPE. If the power adapter (5.5×2.1 mm) is not included in the product package, purchase one.
- Some CPEs can be powered on by IEEE 802.3af PoE power supply devices. For more details, visit www.tendacn.com, search by a model, then check technical information on the **Specification** page.
- The maximum PoE power supply distance varies by the model. For more details, visit www.tendacn.com, search by a model, download the datasheet from the **Download** page, then check the maximum PoE power supply distance.

2. Log in to the web UI of the CPE.
3. Set the CPE to WISP mode.

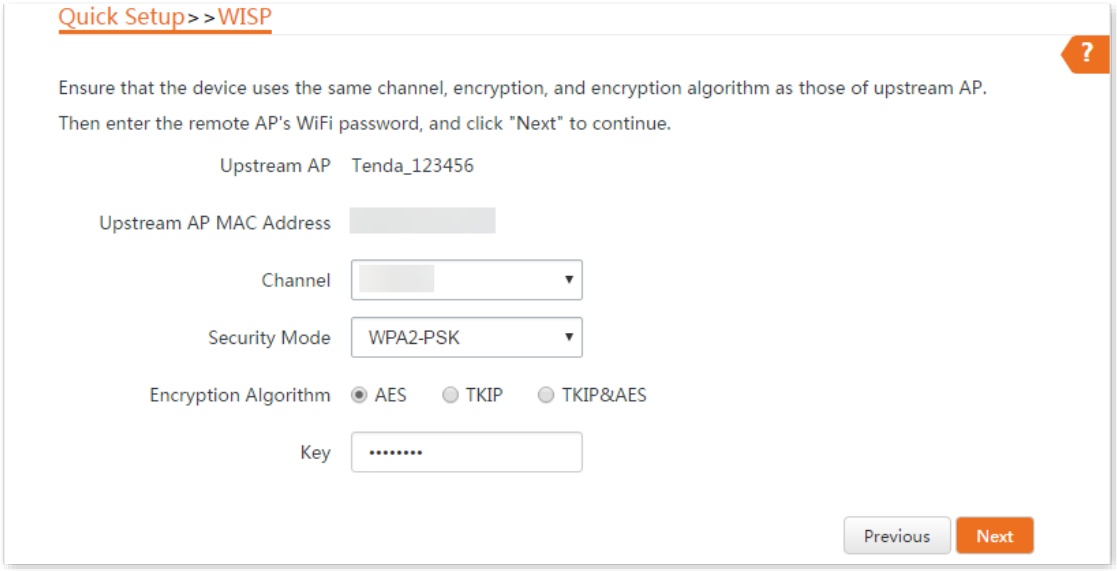
   1) Navigate to **Quick Setup**. Select **WISP** mode, and click **Next**.



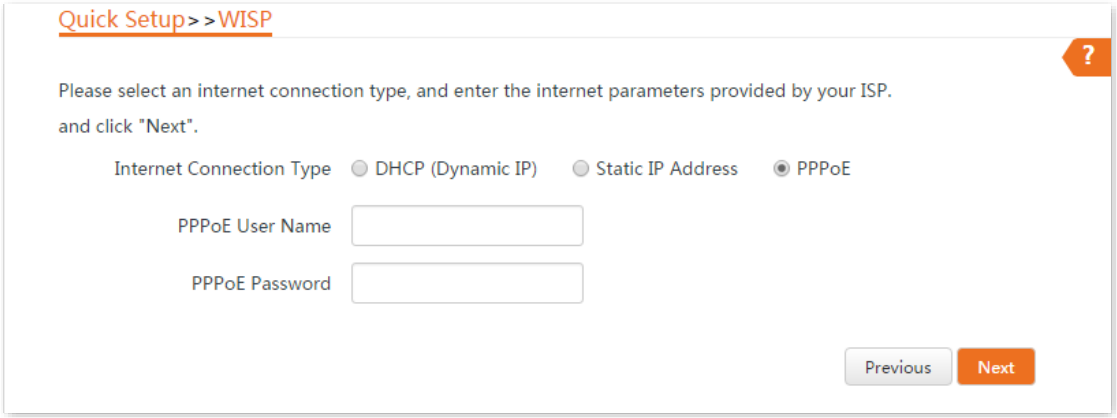

   2) Select the wireless network of your ISP hotspot, which is **Tenda_123456** in this example, and click **Next**.



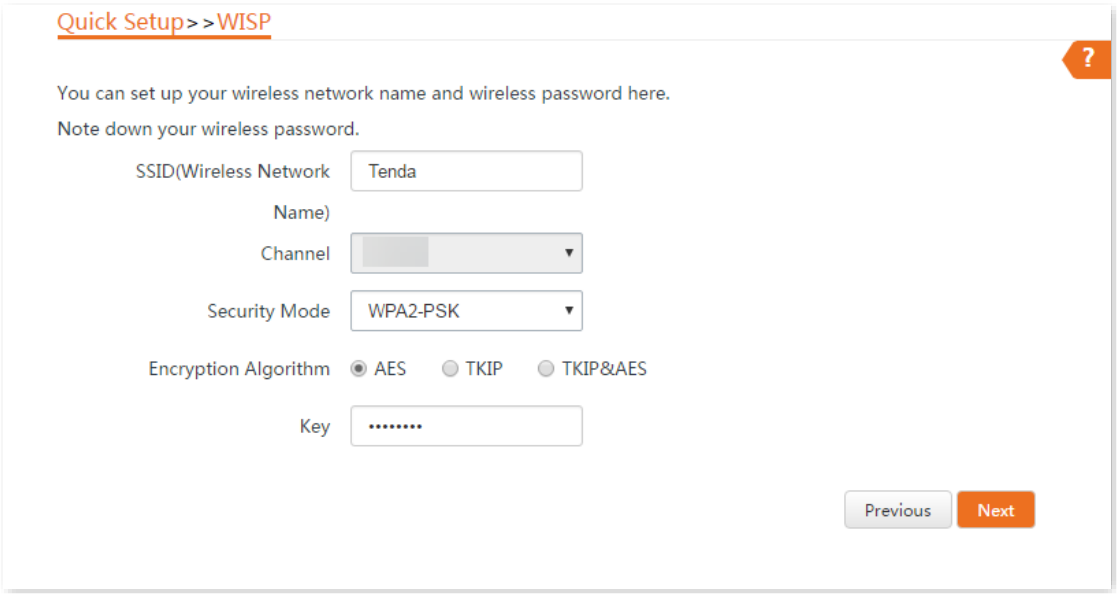

   3) Enter the Wi-Fi password of your ISP hotspot in the **Key** field, and click **Next**.




4) 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**.

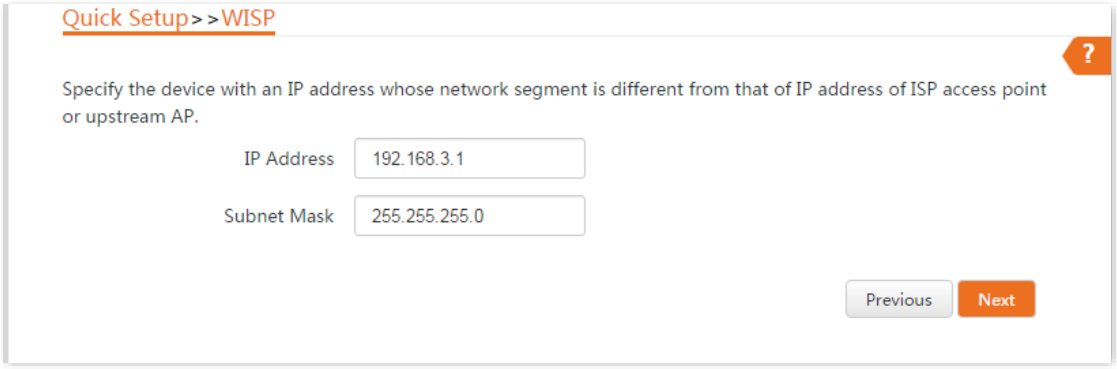



5) Customize the SSID and key, and click **Next**.

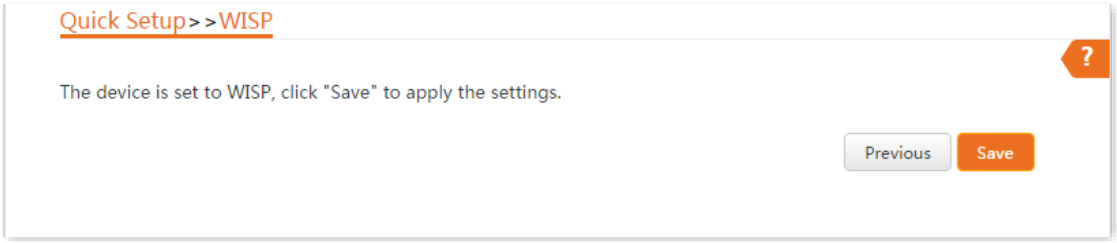


6) Modify the IP address and click **Next**.

- Set an IP address that belongs to a subnet different from your ISP hotspot, which is **192.168.3.1** in this example.
- Set a subnet mask, which is **255.255.255.0** in this example.




7) Click **Save**, and wait until the CPE reboots to make the settings take effect.




**---End**

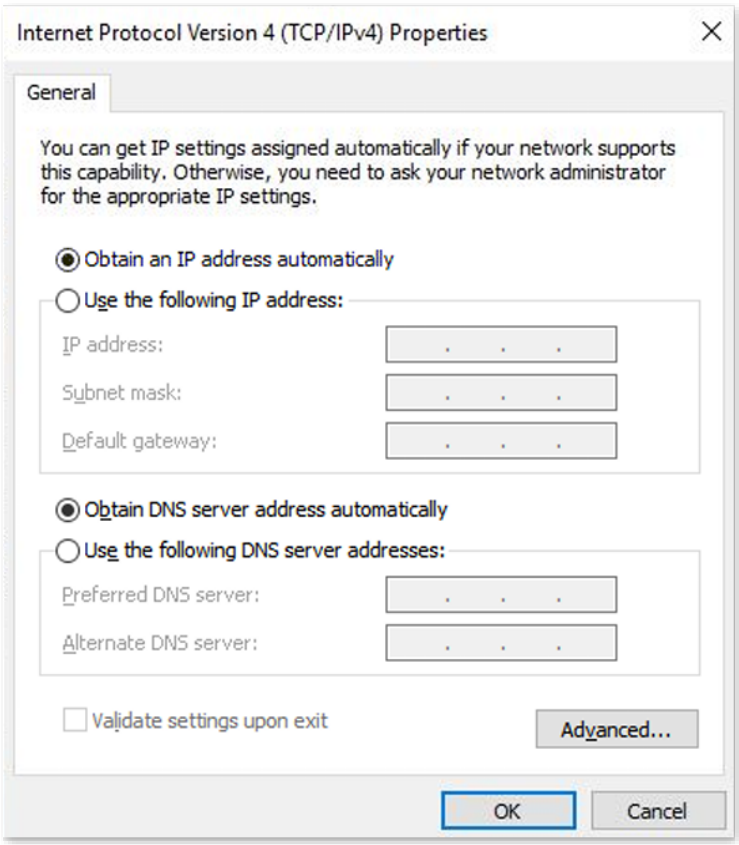
When the LED1, LED2, and LED3 indicators of the CPE are blinking, the CPE is connected to your ISP hotspot successfully.

# 2 Log in to web UI

## 2.1 Login

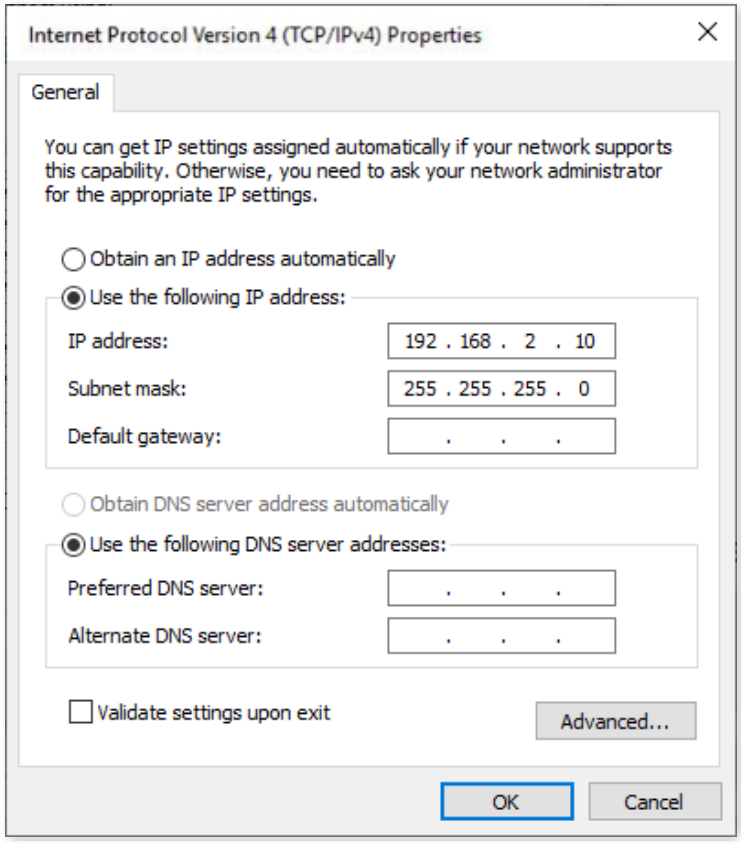
### 2.1.1 Login with computer

1. Connect the computer to the CPE or the switch connected to the CPE.
2. Set the IP address of the computer.
   - When DHCP is enabled: Set the computer to obtain an IP address automatically. The following figure is for reference only.

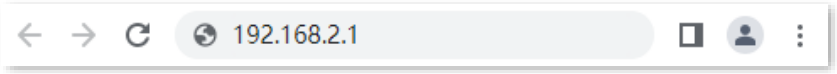



   - When DHCP is disabled: Set the computer's IP address to an unused one within the same subnet as the CPE.

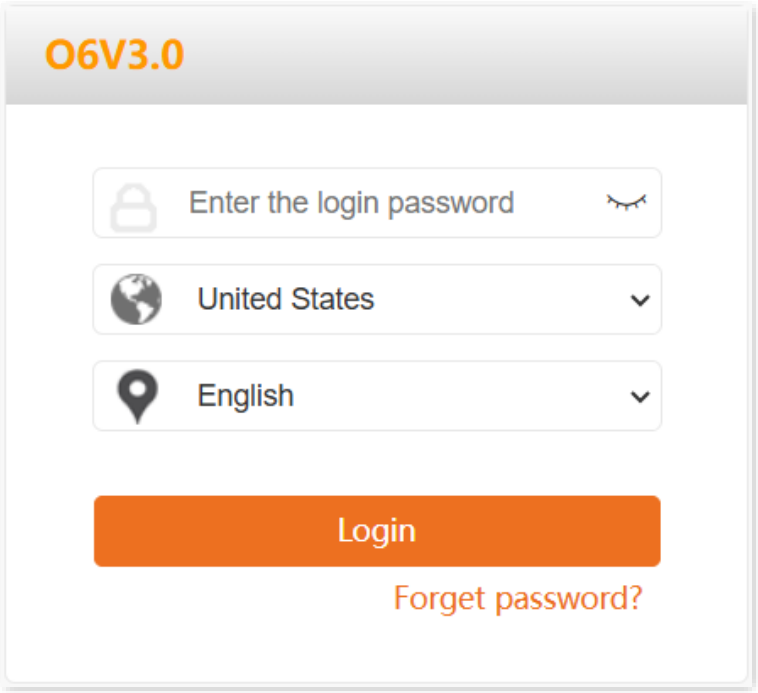
     For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.*X* (*X* ranges from 3 to 254 and is not occupied), and the subnet mask to 255.255.255.0. The following figure is for reference only.




3. Start a web browser on your computer, enter the default IP address of the CPE (AP mode: **192.168.2.1**; Client mode: **192.168.2.2**), and press the **Enter** (or **Return**) key on your keyboard.




4. Enter your password, and click **Login**. The following figure is for reference only.



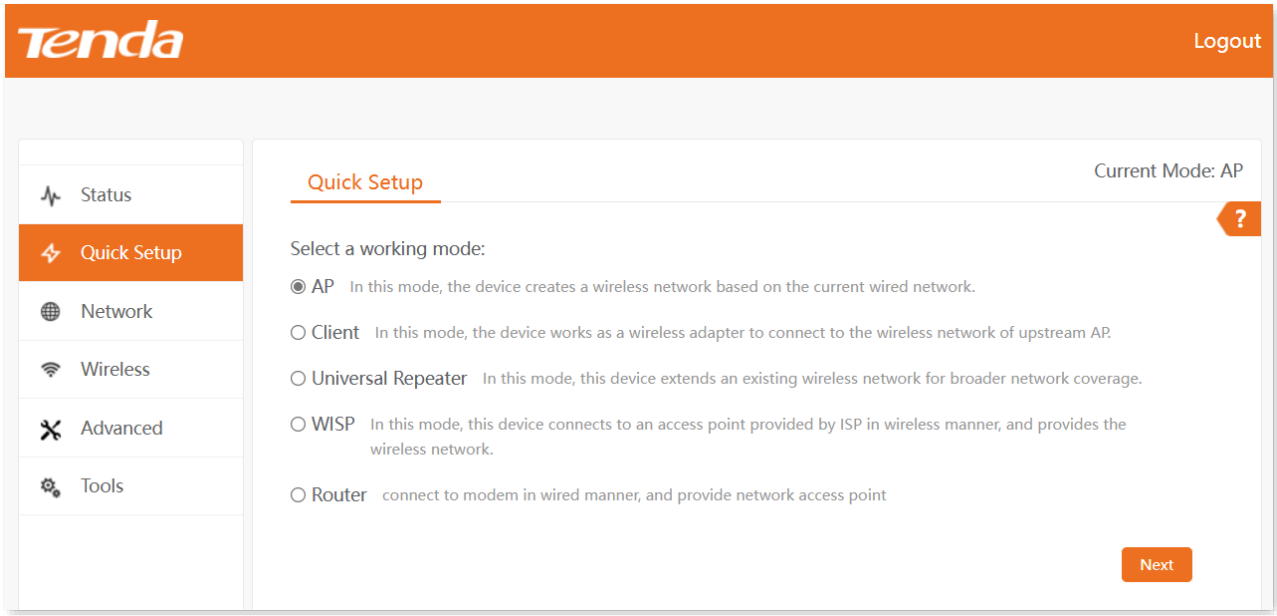
TIP

If the above page does not appear, try the following methods:

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE or the Ethernet port of the switch (which is connected to the CPE) properly.
- The CPE supports management IP address and LAN IP address. The default management IP address is 192.168.2.1 in AP mode, and 192.168.2.2 in Client mode. The LAN IP address is assigned automatically by the local DHCP server, and can be found in the server's client list. Before logging in using the IP address, ensure that the computer's IP address is in the same subnet as the CPE.
- If more than one CPE is connected, modify the IP address of each one to avoid login failure due to IP address conflict.
- Reset the CPE to factory settings. To reset the CPE, hold down the reset button (such as RST, RESET or Reset) for about 8 seconds, and then release it when all the indicators light up.

**---End**

After the successful login, you can configure the CPE.




## 2.1.2 Login with smartphone or tablet

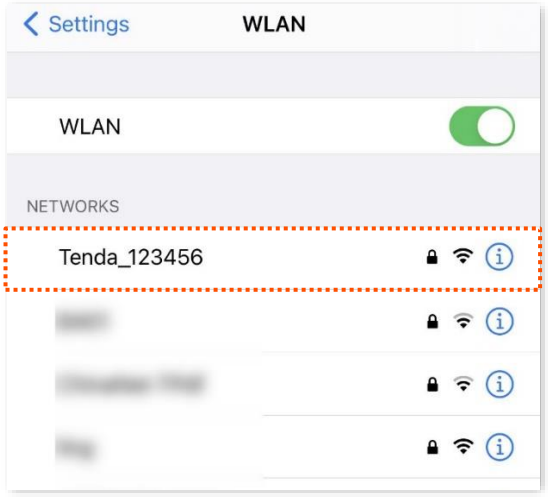
When logging in to a client-mode CPE, ensure that management RF is supported and enabled.

Take an iPhone as an example.

1. Connect the smartphone to the Wi-Fi you set for the CPE, which is **Tenda_123456** in this example.

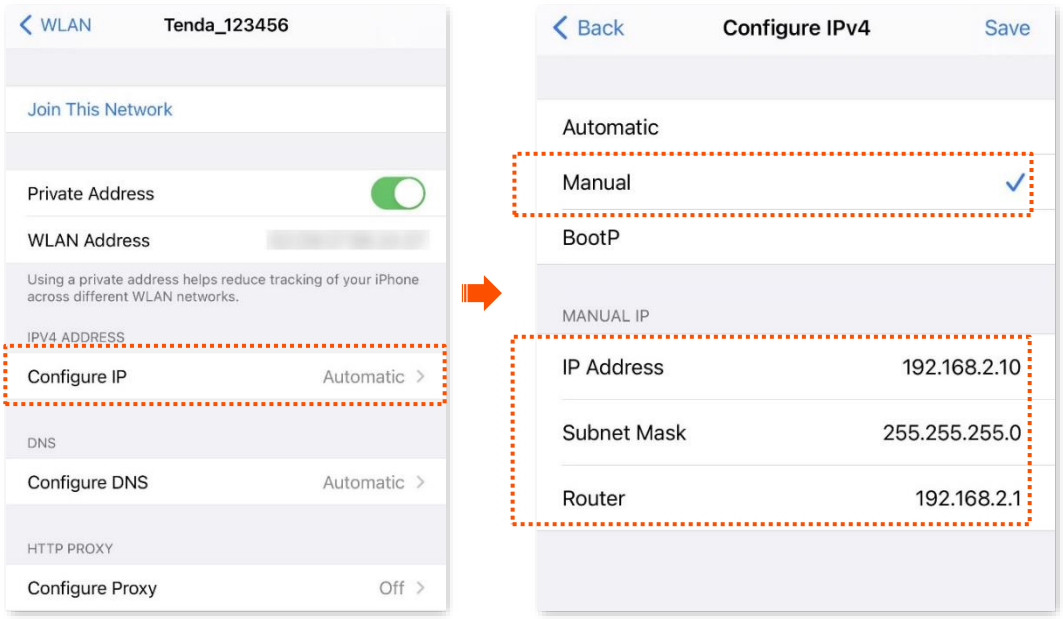
TIP

The default Wi-Fi name is Tenda_*XXXXXX* or Tenda_*XXXXXX*_MG (*XXXXXX* indicates the last six digits of the CPE MAC address). If you cannot find the Wi-Fi network, reboot the CPE and try again.

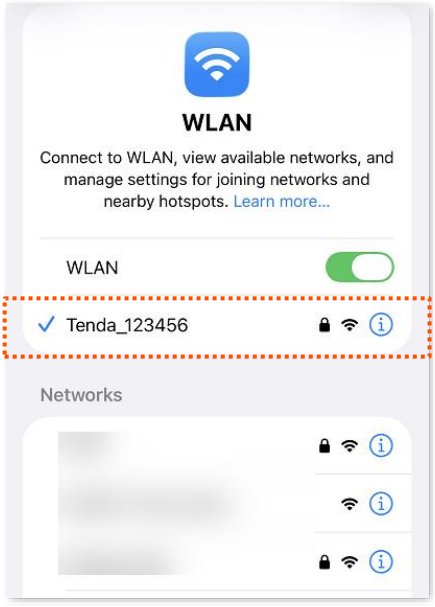



2. Set the smartphone's IP address to an unused one within the same subnet as the CPE. (If the CPE has DHCP enabled, skip this step.)

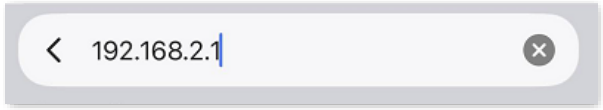
   For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the smartphone to 192.168.2.*X* (*X* ranges from 3 to 254 and is not occupied), and subnet mask to 255.255.255.0.



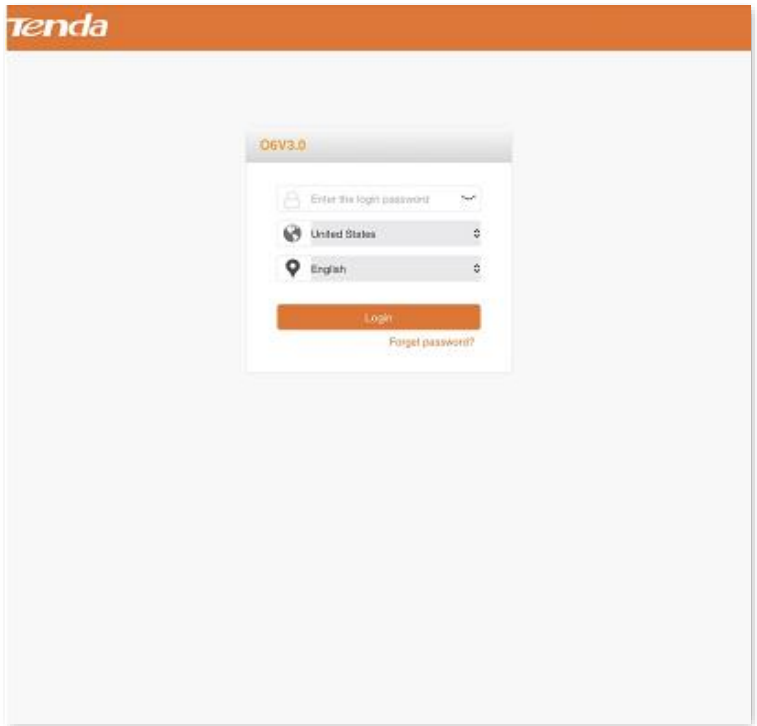
3. Ensure that the smartphone is connected to the CPE's Wi-Fi.




4. Start a browser on your smartphone, and enter the default IP address of the CPE (AP mode: **192.168.2.1**; Client mode: **192.168.2.2**).

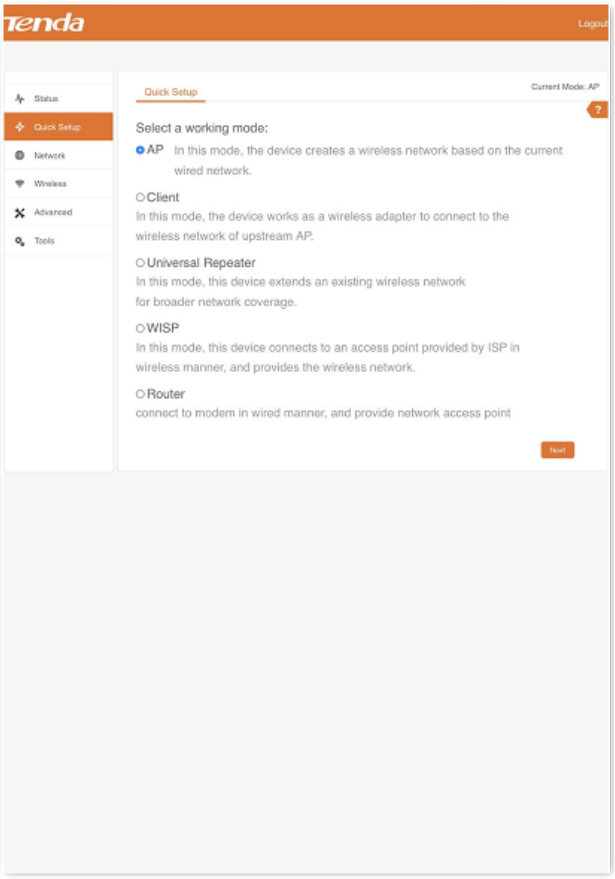



5. Enter your password, and click **Login**. The following figure is for reference only.




**---End**

After the successful login, you can configure the CPE.



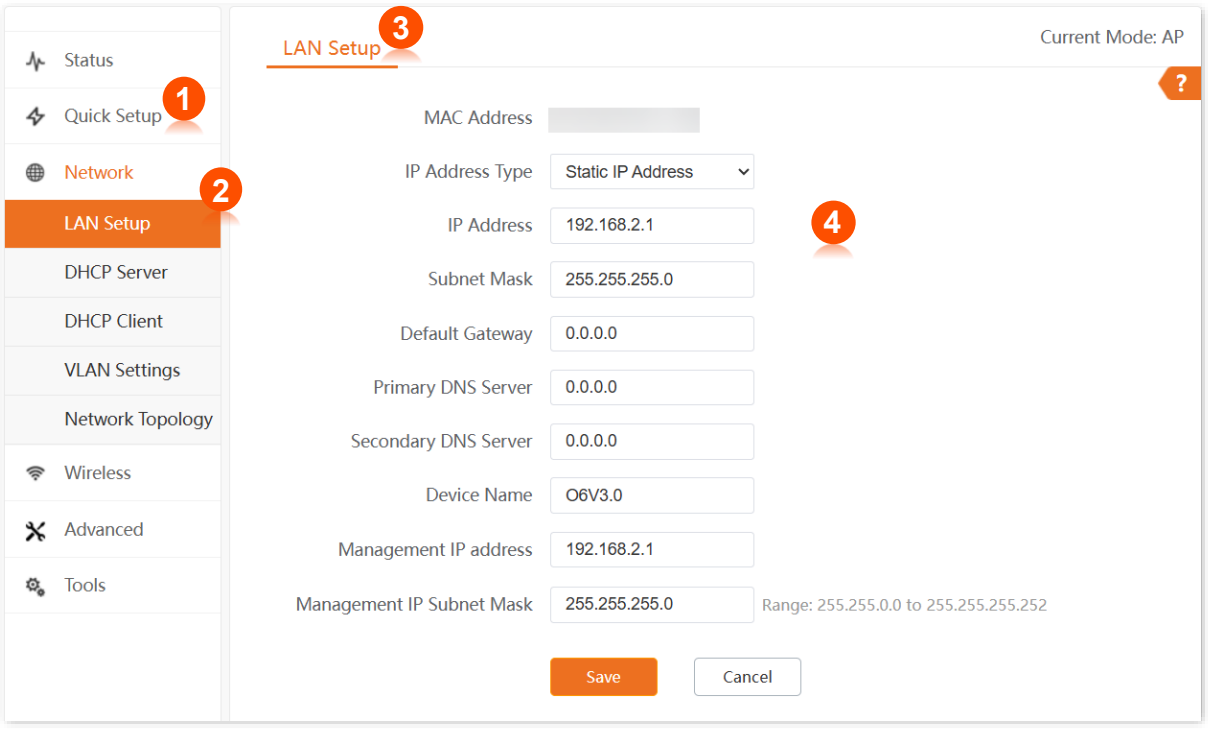

## 2.2 Logout

After you log in to the web UI of the CPE, the system will automatically log you out if there is no operation within the login timeout interval (default: 5 minutes). Alternatively, you can directly click **Logout** on the upper right corner to exit the web UI.

# 2.3 Web UI

## 2.3.1 Web layout

The web UI can be divided into four parts: level-1 navigation bar, level-2 navigation bar, tab, and configuration area.




TIP

Functions or parameters greyed out indicate they are not available or cannot be modified under the current configurations.

| No. | Name | Description |
|---|---|---|
| 1 | Level-1 navigation bar | Used to display menu items of the CPE in the form of a navigation tree that allows you to quickly access functions. |
| 2 | Level-2 navigation bar | |
| 3 | Tab | |
| 4 | Configuration area | Used to view and modify configuration. |

## 2.4 Common buttons

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

| Button | Description |
| --- | --- |
| Save | Used to save and apply the current configuration. |
| Cancel | Used to restore the original configuration without saving the current changes. |
| Refresh | Used to update the contents on the current page. |
| ? | Used to view help information for the settings on the current page. |

# 3 Set up device mode

Features available in the CPE may vary by model and software version. CPE availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual CPE experience.

TIP

In a CPE kit, the two CPEs are pre-configured and ready for installation.

This module enables you to quickly change the working mode of the CPE and deploy your wireless network.

Different working modes are described below. Select one to fit your needs:

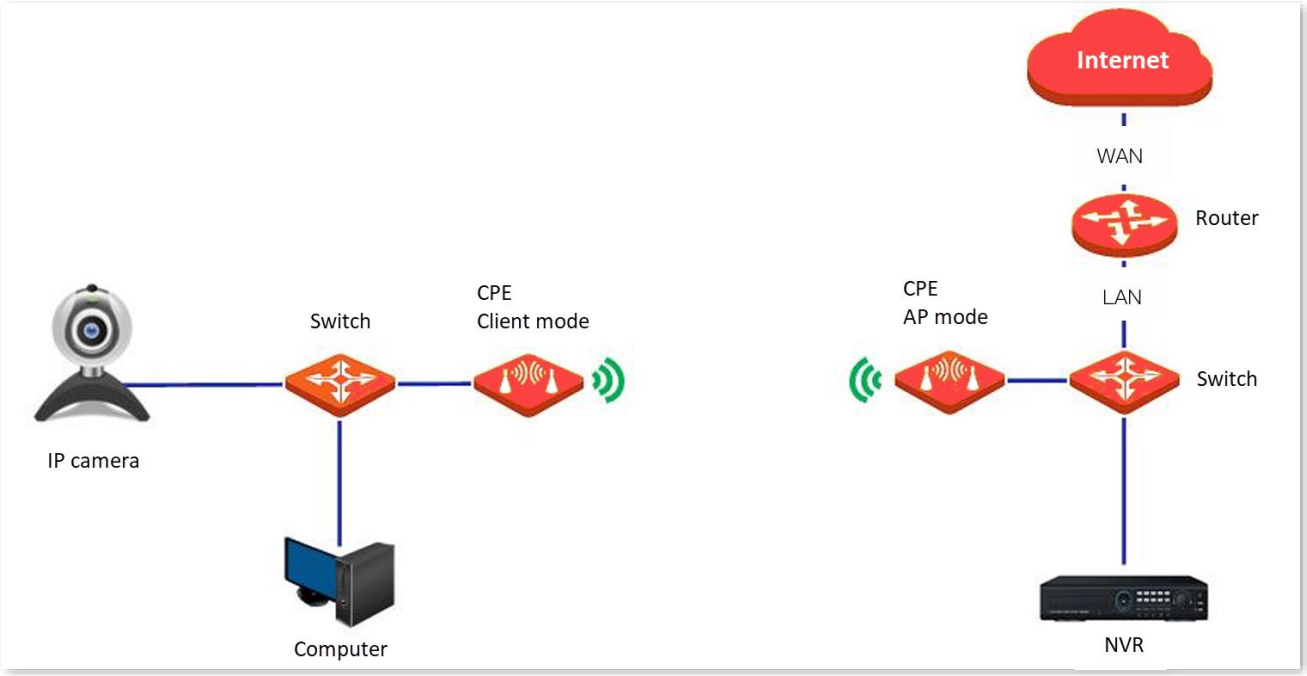
- AP: In this mode, the CPE converts a wired network into a wireless one.
- Client: In this mode, the CPE works as a wireless adapter that can connect to other wireless networks. The CPE's operating RF does not provide wireless connection, so client devices need to be connected with an Ethernet cable.
- Universal Repeater: In this mode, the CPE extends an existing wireless network for broader network coverage. The wireless information (such as SSID and password) of the new network is the same as the upstream wireless network.
- WISP: In this mode, the CPE connects wirelessly to a hotspot provided by an ISP and provides network access to connected devices. The CPE can also be connected to the LAN port of an upstream wireless router to obtain the IP address by DHCP (Dynamic IP), static IP address or PPPoE for internet access.
- Router: In this mode, the CPE connects to a modem in a wired manner to obtain the IP address by DHCP (Dynamic IP), static IP address or PPPoE for internet access.

# 3.1 AP mode

## 3.1.1 Overview

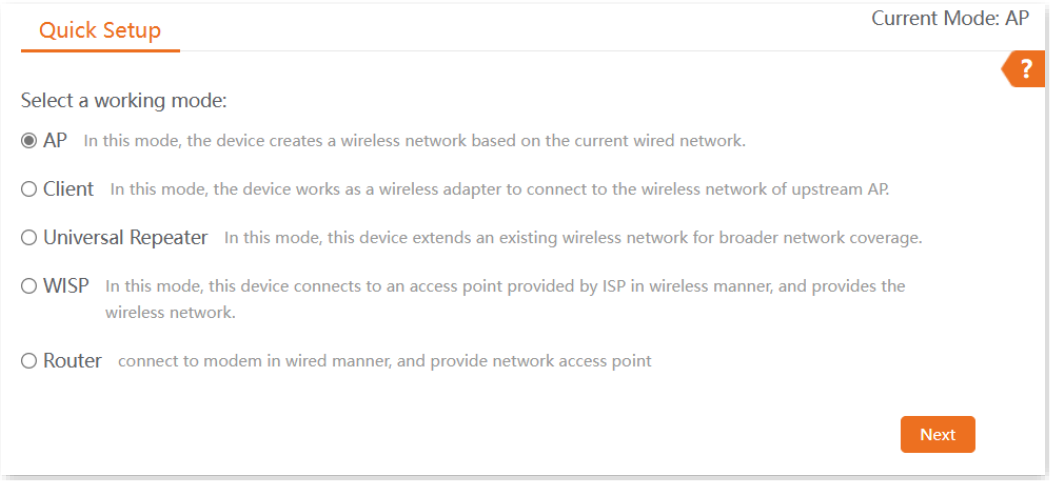
In AP mode, the CPE converts a wired network into a wireless network through an Ethernet connection.

The CPE in AP mode usually works with another CPE in Client mode or Universal Repeater mode to establish a video surveillance network. The following figure shows how the CPE in AP mode works with the one in Client mode.




## 3.1.2 Set AP mode

1. Log in to the web UI of the CPE.
2. Navigate to **Quick Setup**. Select **AP** mode and click **Next**.




3. Specify wireless network parameters and click **Next**.

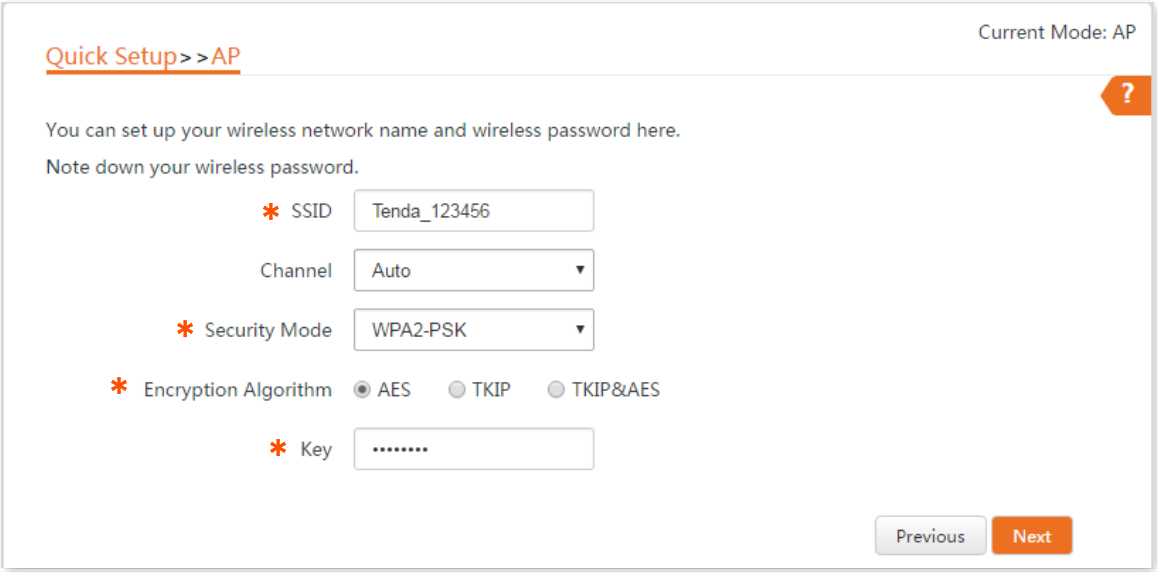
   1) Set **SSID** (Wi-Fi name), which is **Tenda_123456** in this example.

   2) Set **Channel**, which is **Auto** in this example.

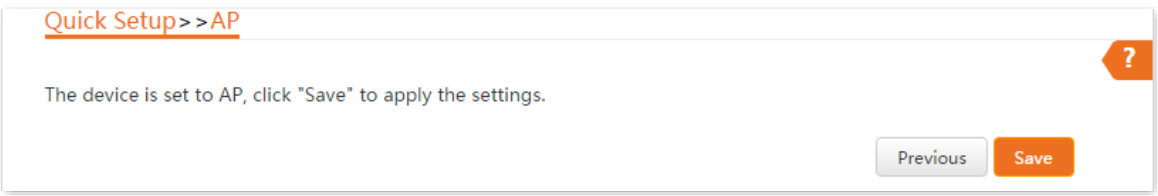
   3) Set **Security Mode**, which is **WPA2-PSK** in this example.

   4) Set **Encryption Algorithm**, which is **AES** in this example.

   5) Set **Key** (Wi-Fi password), which is **UmXmL9UK** in this example.




4. Click **Save**, and wait until the CPE reboots to make the settings take effect.




**---End**

**Parameters description**

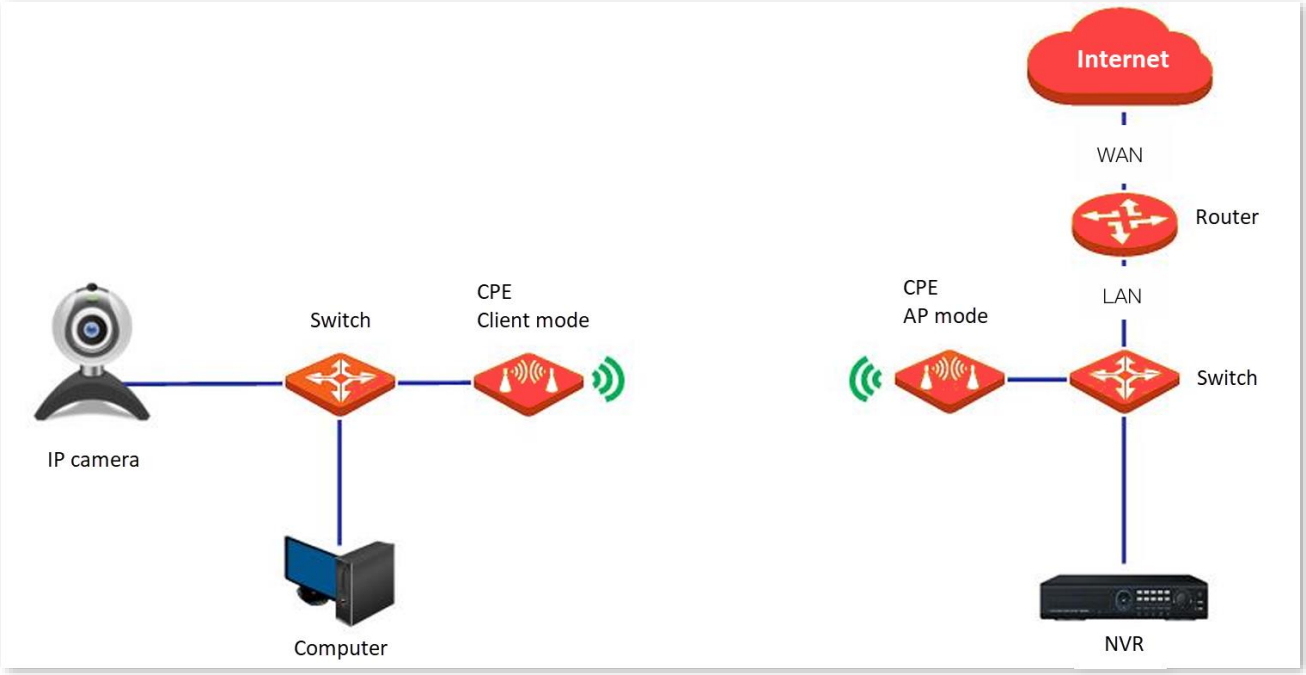
| Name | Description |
| --- | --- |
| SSID | Specifies the Wi-Fi name of this CPE. |
| Channel | Specifies the operating channel of this CPE. **Auto** indicates that the CPE automatically adjusts its operating channel according to the ambient environment.<br>If you frequently experience disconnections, lag, or slow speeds when connected to the CPE's Wi-Fi, try changing the channel to improve performance. You can use tools such as a Wi-Fi analyzer to identify channels that are less commonly used and have minimal interference. |
| Channel Bandwidth | Specifies the bandwidth of the operating channel. **Auto** indicates that the CPE automatically adjusts its operating channel according to the ambient environment.<br>With high channel bandwidth, it is easier to obtain a higher transmission rate, but the penetration is slightly worse and the transmission distance is short. If there is no special need, it is recommended to keep the default setting. |
| Security Mode | Specifies the security mode of the wireless network, including None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. |
| Encryption Algorithm | Specifies the encryption method of the wireless network.<br>- **AES**: Indicates the Advanced Encryption Standard.<br>- **TKIP**: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps.<br>- **TKIP&AES**: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. |
| Key | Specifies the Wi-Fi password of the wireless network. |

# 3.2 Client mode

## 3.2.1 Overview

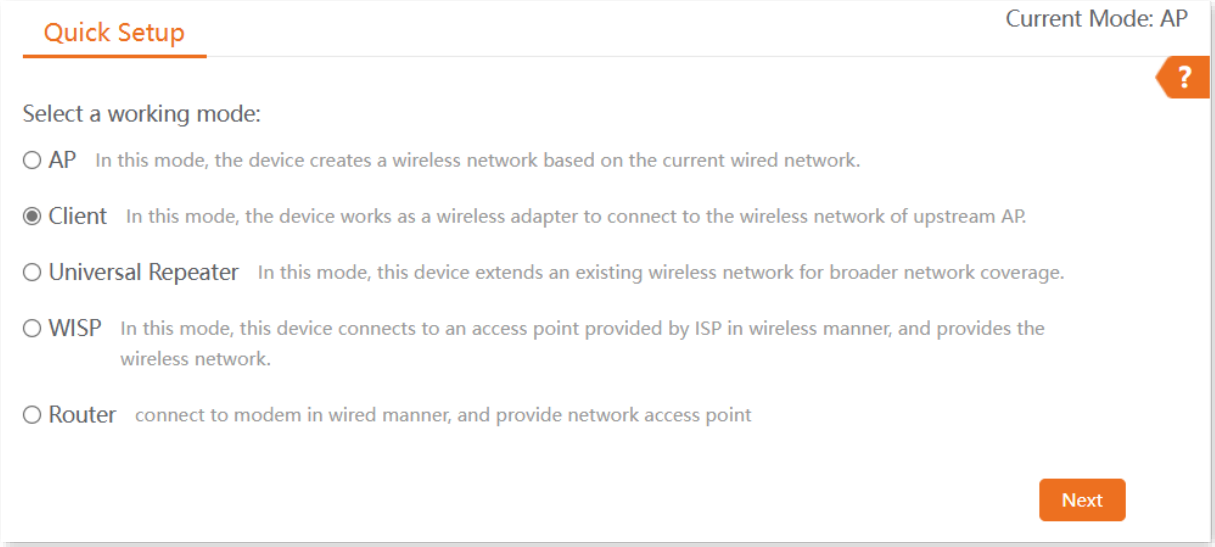
In Client mode, the CPE serves as a wireless adapter that connects to the upstream network. The CPE does not provide wireless access, so a client device needs to be connected with an Ethernet cable.

The CPE in Client mode usually works with the CPE in AP mode to create a video surveillance network. The network topology is shown below.




## 3.2.2 Set Client mode

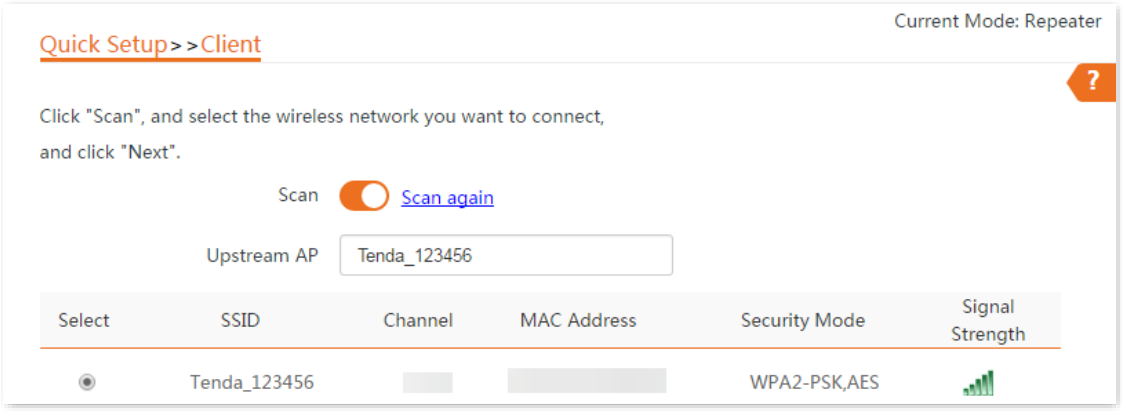
1. Log in to the web UI of the CPE.
2. Navigate to **Quick Setup**. Select **Client** mode, and click **Next**.



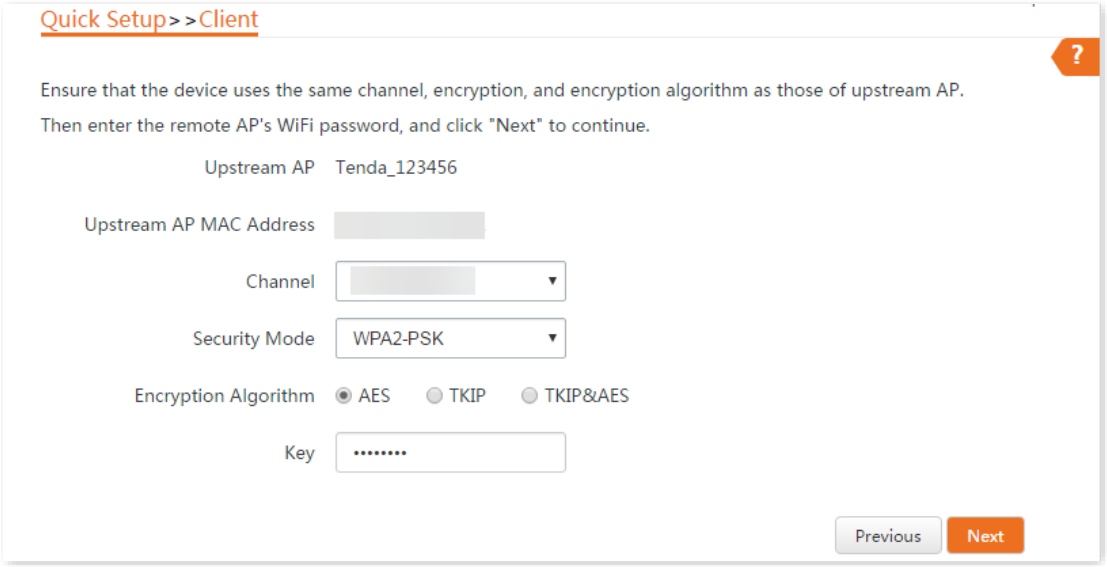

3. Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next**.

TIP

If you cannot find any wireless network from the list, navigate to **Wireless** > **Basic** and enable the wireless function. Then try again.




4. Enter the Wi-Fi password for the selected wireless network **Tenda_123456** in the **Key** field, and click **Next**.




**Parameters description**

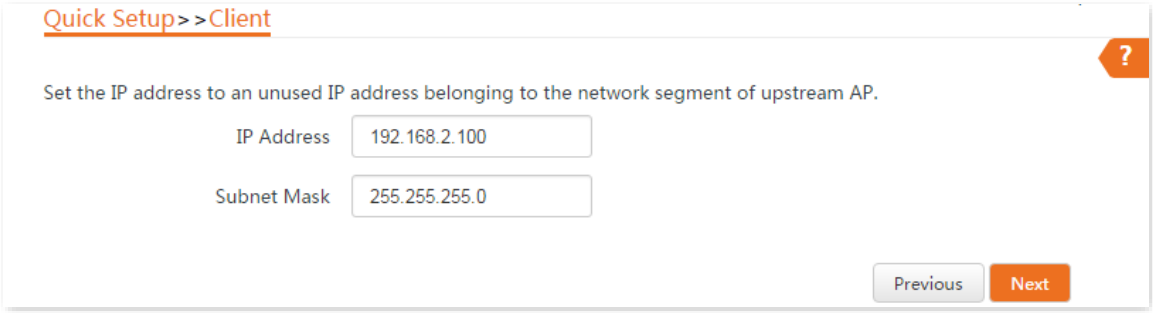
| Name | Description |
|---|---|
| Upstream AP | Specifies the Wi-Fi name (SSID) of the wireless network to be bridged. |
| Upstream AP MAC Address | Specifies the MAC address of the wireless network to be bridged. |
| Channel | Specifies the operating channel of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. |
| Security Mode | Specifies the security mode of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. If the wireless network to be bridged has a Wi-Fi password, you need to enter the password manually. |

| Name | Description |
| --- | --- |
| Encryption Algorithm | Specifies the encryption method of the wireless network.<br>- **AES**: Indicates the Advanced Encryption Standard.<br>- **TKIP**: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps.<br>- **TKIP&AES**: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. |
| Key | Specifies the Wi-Fi password of the wireless network. |

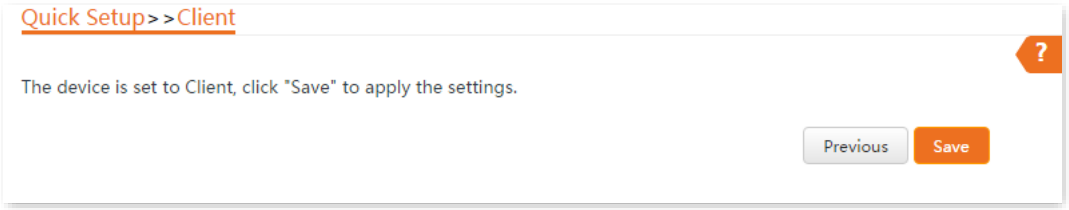
5. Specify IP address parameters and click **Next**.

   1) Enter an unused IP address within the same subnet as the peer CPE, which is **192.168.2.100** in this example.

   2) Enter the subnet mask of the peer CPE, which is **255.255.255.0** in this example.




6. Click **Save**, and wait until the CPE reboots to make the settings take effect.




**---End**

After the CPE is rebooted, verify your settings as follows.

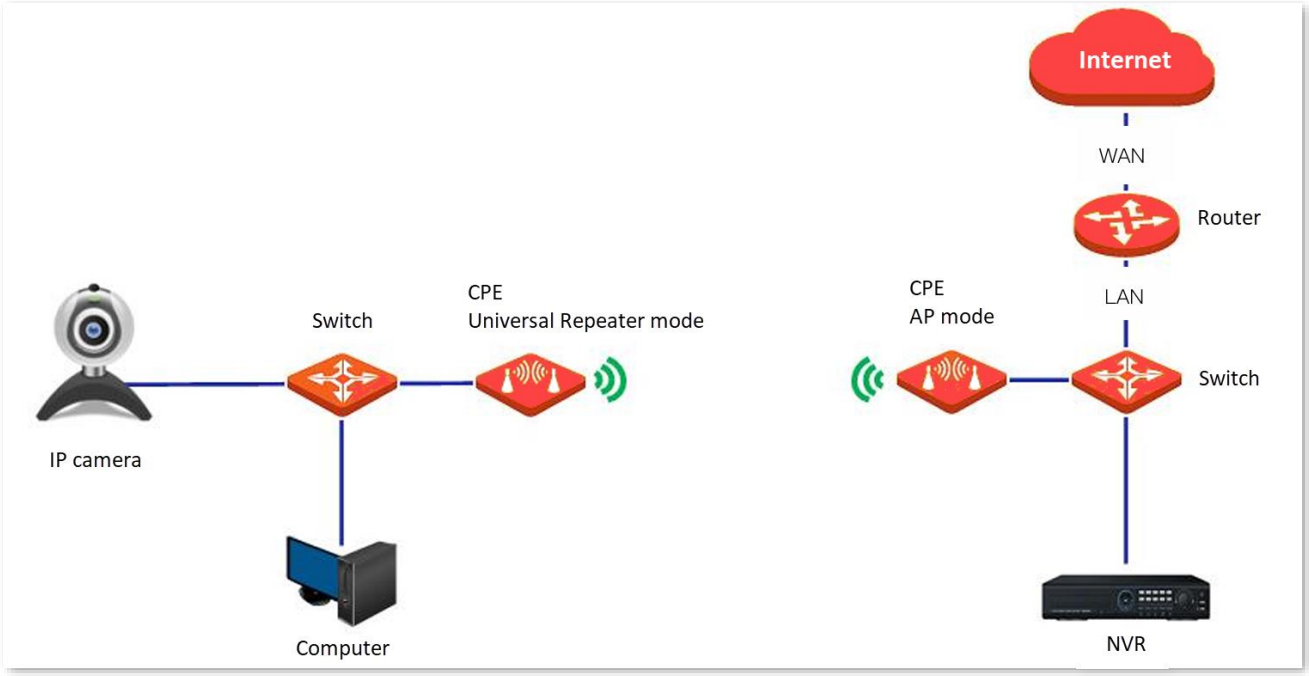
- Log in to the web UI of the CPE and navigate to **Status**.
- On the **Wireless Status** module, ensure that **Working Mode** is set to Client mode and **AP's MAC Address** changes to the same as the peer CPE's WLAN MAC address.

# 3.3 Universal Repeater mode

## 3.3.1 Overview

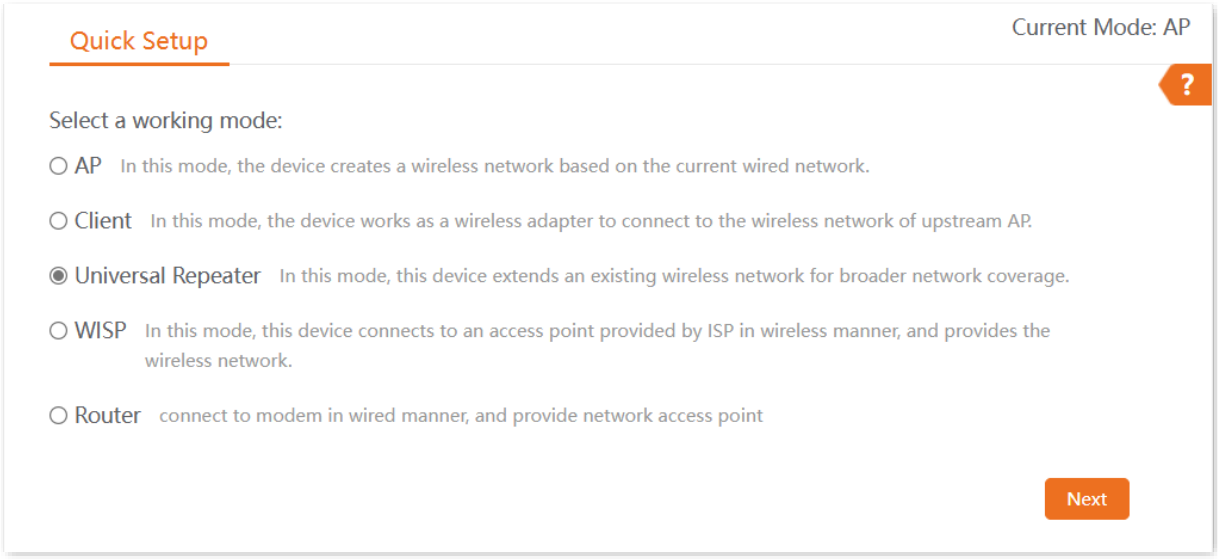
In Universal Repeater mode, the CPE expands your wireless network for broader network coverage. The wireless information (such as SSID and Wi-Fi password) of the new wireless network is the same as those of the upstream wireless network.

The CPE in Universal Repeater mode usually works with the CPE in AP mode to establish a video surveillance network. The network topology is shown below.

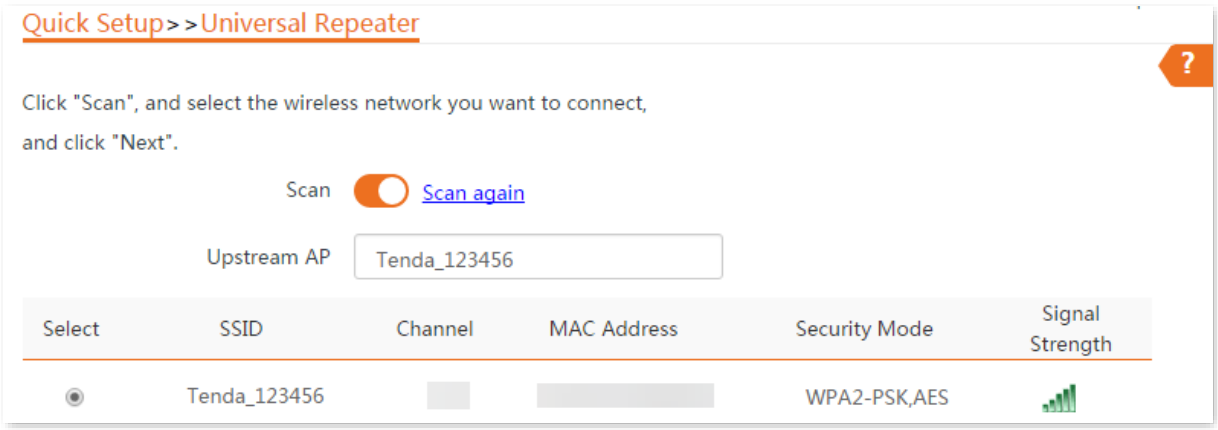



## 3.3.2 Set Universal Repeater mode

1. Log in to the web UI of the CPE.
2. Navigate to **Quick Setup**. Select **Universal Repeater**, and click **Next**.



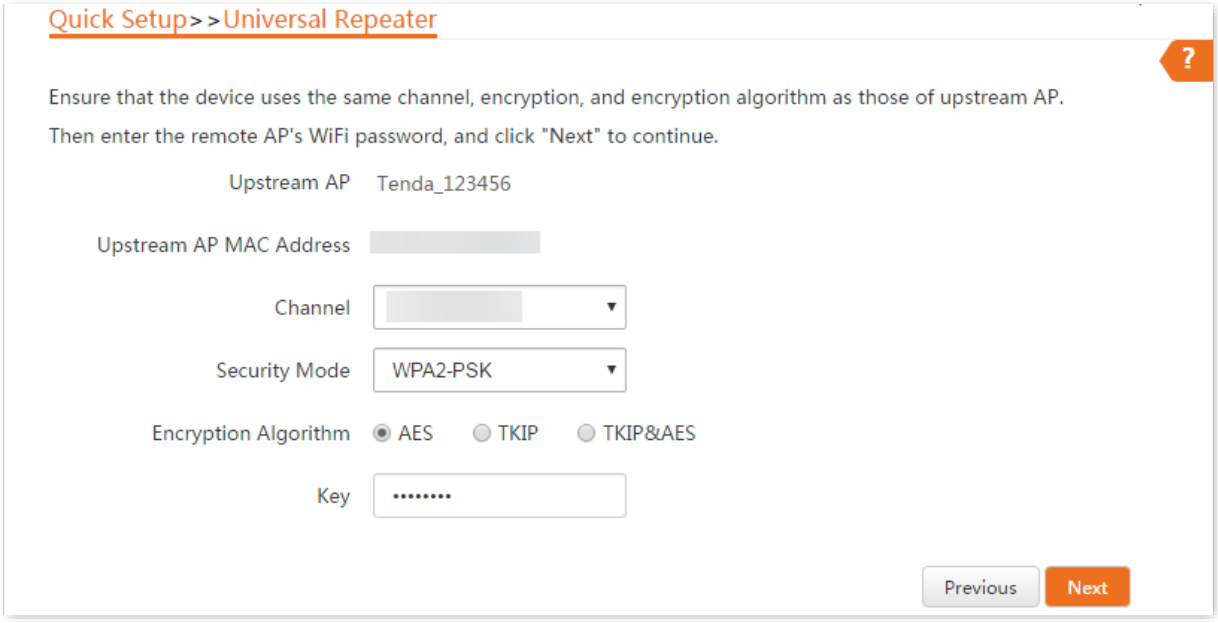

3. Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next**.




TIP

If you cannot find any wireless network from the list, navigate to **Wireless** > **Basic** and enable the wireless function. Then try again.

4. If the upstream wireless network is encrypted, enter its Wi-Fi password in the **Key** field, and click **Next**.



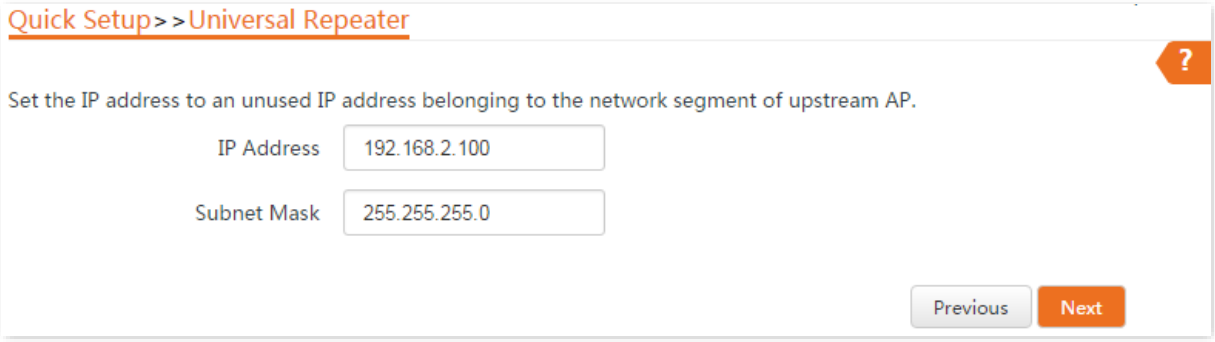

**Parameters description**

| Name | Description |
|---|---|
| Upstream AP | Specifies the Wi-Fi name (SSID) of the wireless network to be bridged. |
| Upstream AP MAC Address | Specifies the MAC address of the wireless network to be bridged. |
| Channel | Specifies the operating channel of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. |
| Security Mode | Specifies the security mode of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. If the wireless network to be bridged has a Wi-Fi password, you need to enter the password manually. |
| Encryption Algorithm | Specifies the encryption method of the wireless network.<br>- **AES**: Indicates the Advanced Encryption Standard.<br>- **TKIP:** Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps.<br>- **TKIP&AES:** Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. |
| Key | Specifies the Wi-Fi password of the wireless network. |

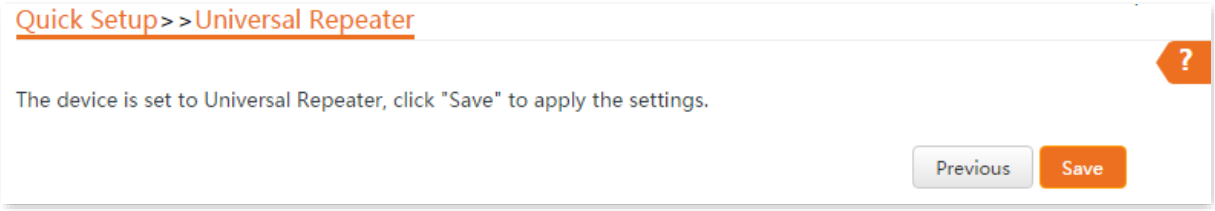
5. Specify IP address parameters and click **Next**.

   1) Enter an unused IP address within the same subnet as the peer CPE, which is **192.168.2.100** in this example.

   2) Enter the subnet mask of the peer CPE, which is **255.255.255.0** in this example.




6. Click **Save**, and wait until the CPE reboots to make the settings take effect.




**---End**

After the CPE is rebooted, verify your settings as follows.

- Log in to the web UI of the CPE and navigate to **Status**.
- On the **Wireless Status** module, when the **Working Mode** is set to Universal Repeater mode, SSID becomes the same as the peer CPE's SSID and the **AP's MAC Address** changes to the same as the peer CPE's WLAN MAC address.

TIP

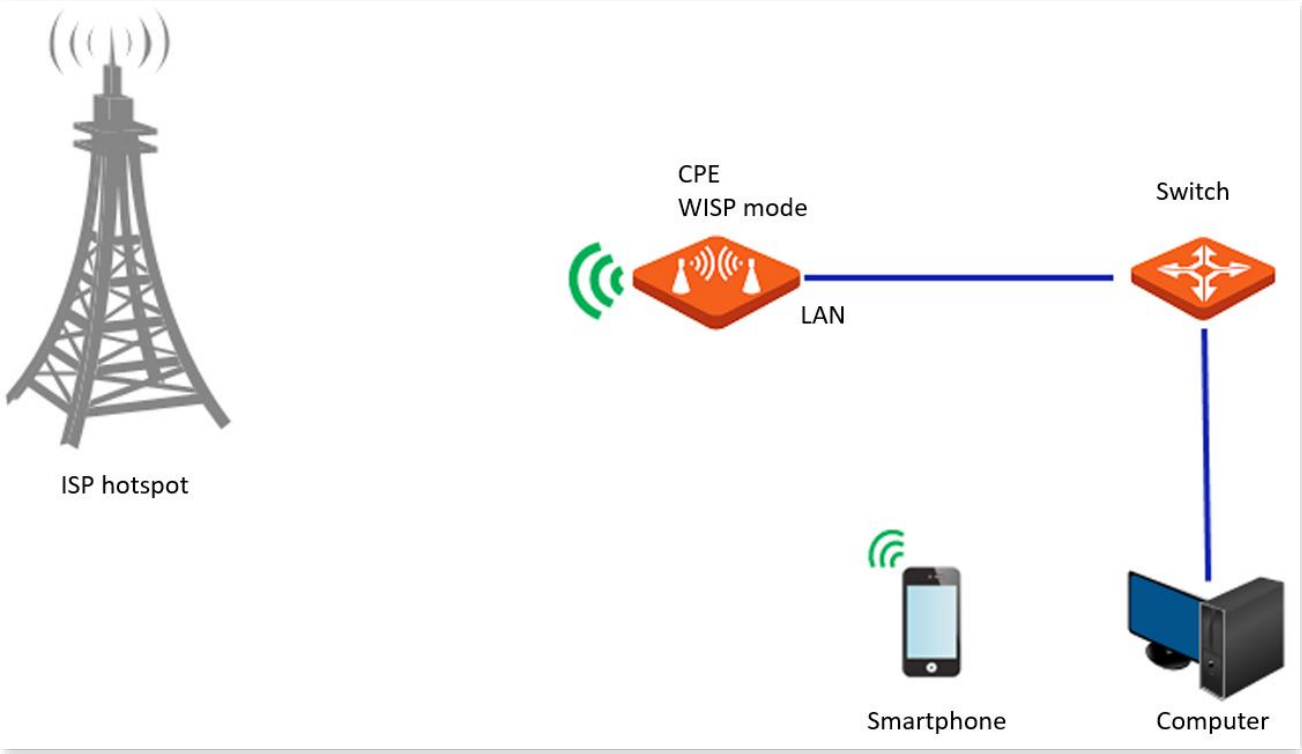
After bridging, the CPE uses the same Wi-Fi password as the peer CPE.

# 3.4 WISP mode

## 3.4.1 Overview

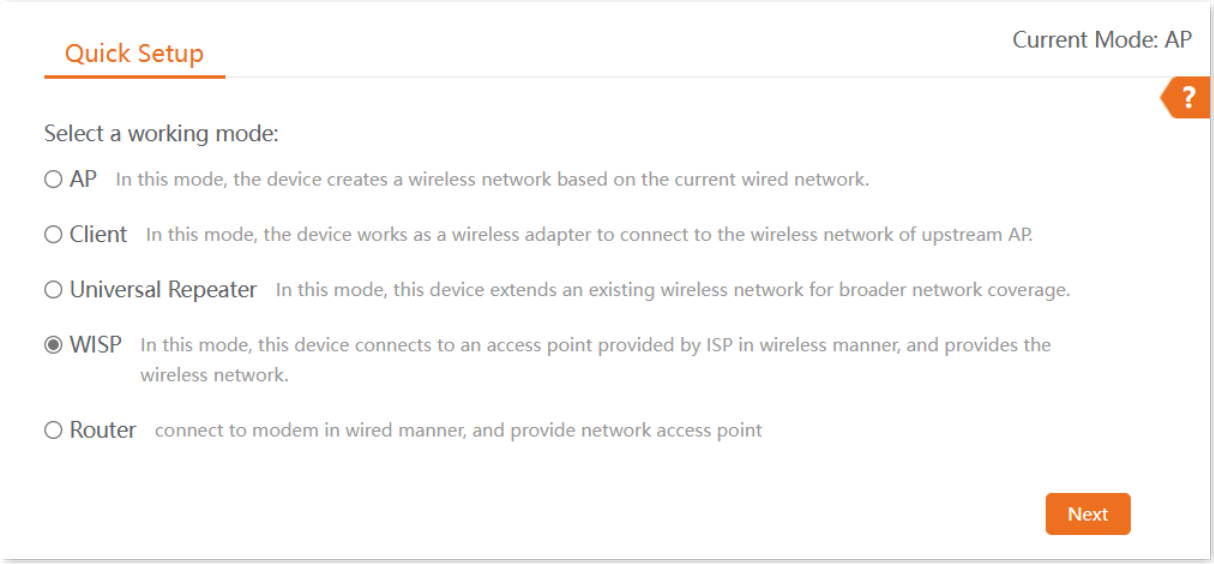
In WISP mode, the CPE connects to a hotspot provided by ISP in a wireless manner, and allows the wired and Wi-Fi-enabled devices to connect to the CPE for internet access.

The CPE is used to extend the ISP hotspot. The network topology is shown below.

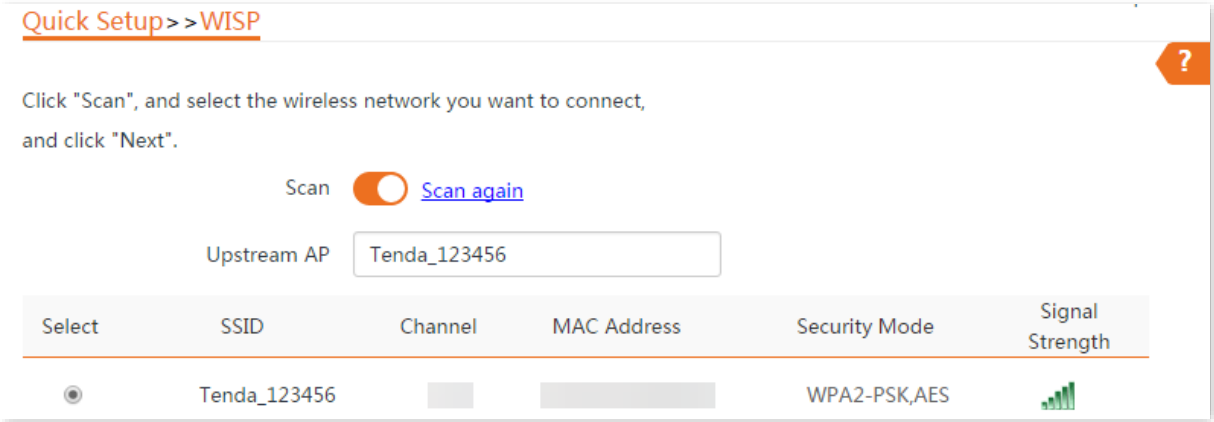



## 3.4.2 Set WISP mode

1. Log in to the web UI of the CPE.
2. Navigate to **Quick Setup**. Select **WISP** mode, and click **Next**.



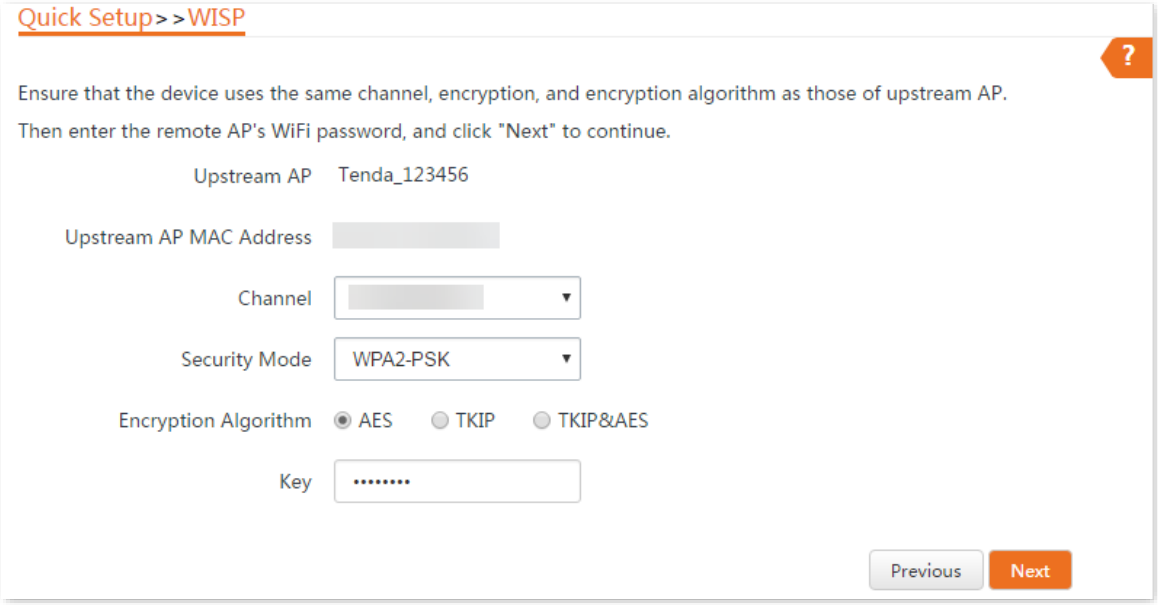

3. Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next**.




TIP

If you cannot find any wireless network from the list, navigate to **Wireless** > **Basic** and enable the wireless function. Then try again.

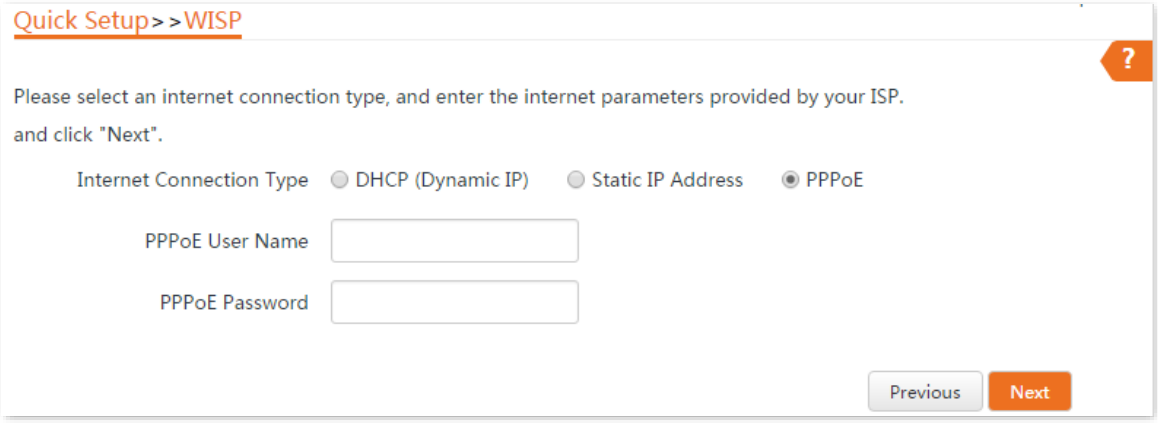
4. If the upstream wireless network is encrypted, enter its Wi-Fi password in the **Key** field, and click **Next**.




**Parameters description**

| Name | Description |
|---|---|
| Upstream AP | Specifies the Wi-Fi name (SSID) of the wireless network to be bridged. |
| Upstream AP MAC Address | Specifies the MAC address of the wireless network to be bridged. |
| Channel | Specifies the operating channel of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. |
| Security Mode | Specifies the security mode of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. If the wireless network to be bridged has a Wi-Fi password, you need to enter the password manually. |
| Encryption Algorithm | Specifies the encryption method of the wireless network.<br>- **AES**: Indicates the Advanced Encryption Standard.<br>- **TKIP**: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps.<br>- **TKIP&AES**: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. |
| Key | Specifies the Wi-Fi password of the wireless network. |

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**.




**Parameter description**

| Name | Description |
|---|---|
| Internet Connection Type | Specifies the internet connection type.<br>- **DHCP (Dynamic IP)**: The CPE obtains an IP address and other parameters from the upstream DHCP server for internet access.<br>- **Static IP Address**: The CPE accesses the internet by setting the IP address, subnet mask, default gateway and DNS server IP addresses manually.<br>- **PPPoE**: The CPE accesses the internet using the PPPoE user name and password provided by the ISP.<br>The above required internet access parameters are provided by your ISP. If you are not sure, consult your ISP for help. |

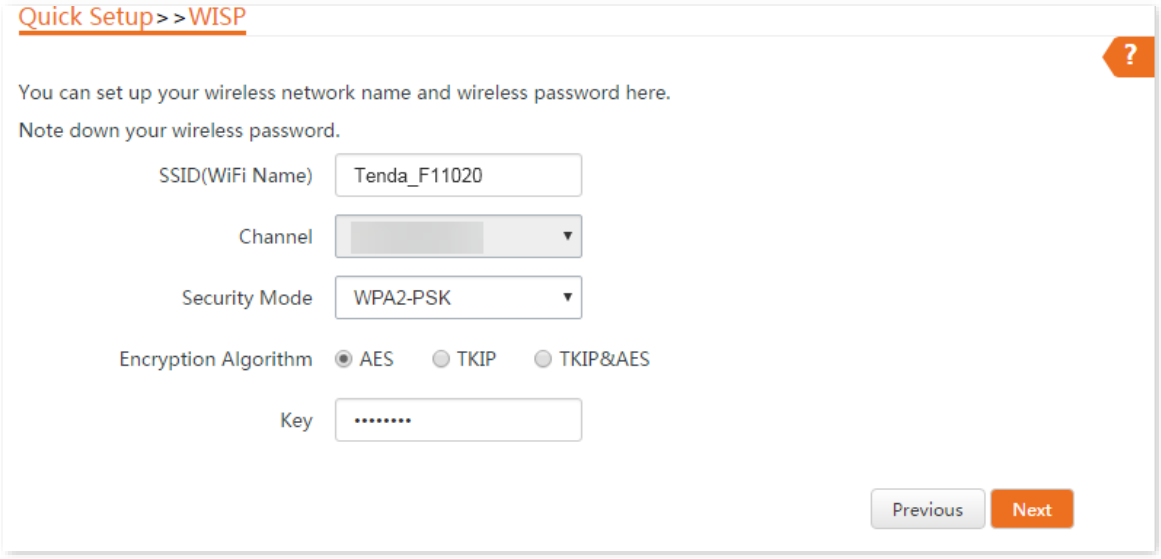
6. Specify wireless network parameters and click **Next**.

   1) Set **SSID** (Wi-Fi name).

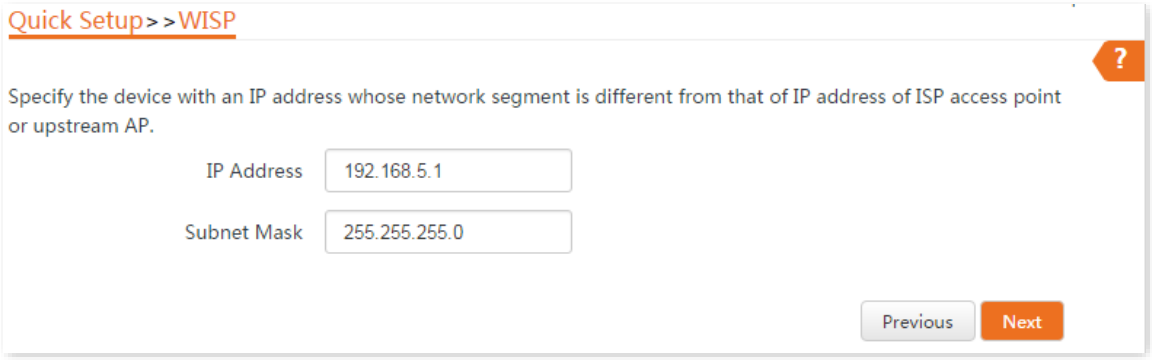
   2) Set **Security Mode**, which is **WPA2-PSK** in this example.

   3) Set **Encryption Algorithm**, which is **AES** in this example.

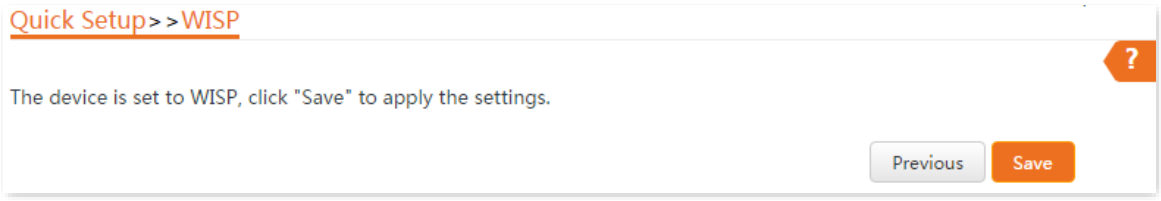
   4) Set **Key** (Wi-Fi password).




7. Set a unique LAN IP address for the CPE (default: **192.168.2.1**) and click **Next**.




8. Click **Save**, and wait until the CPE reboots to make the settings take effect.




**---End**

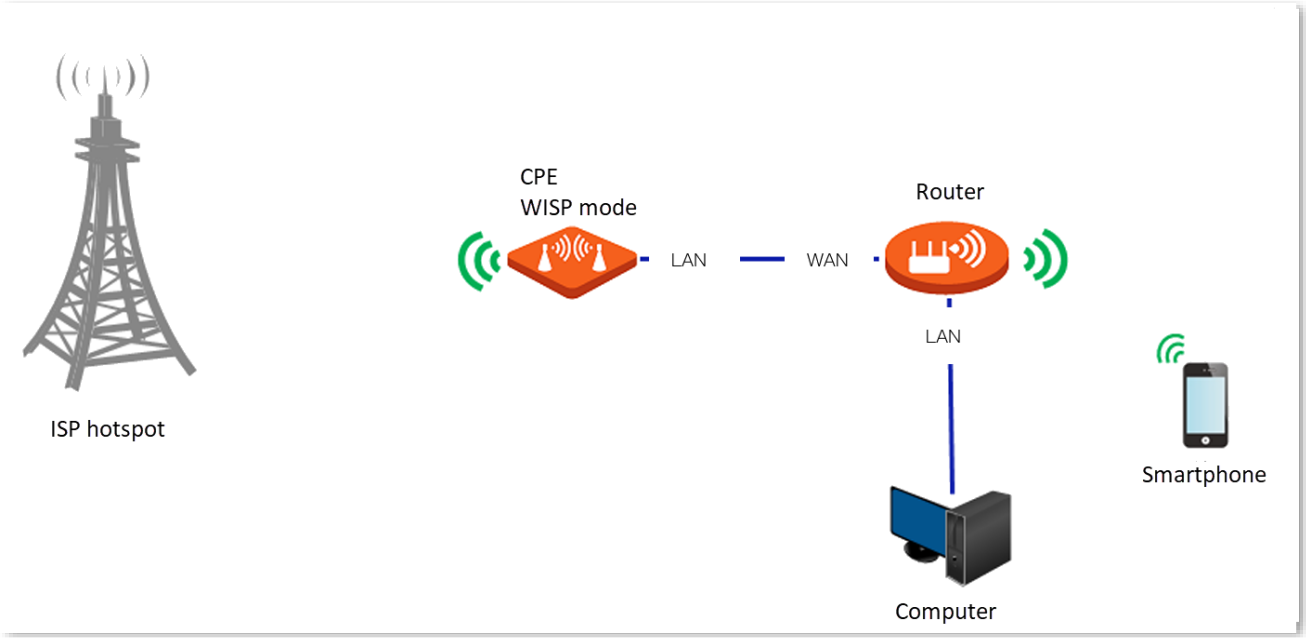
After the CPE is rebooted, verify the settings as follows.

- Log in to the web UI of the CPE and navigate to **Status**.
- On the **System Status** module, ensure that the WAN IP address, default gateway and DNS server information obtained by the WAN port are displayed.
- On the **Wireless Status** module, ensure that **Working Mode** is set to WISP mode, SSID is the Wi-Fi name you set in step 6 and the **AP's MAC Address** is the WLAN MAC address of the peer device.

After the successful configuration, devices connected to the CPE can access the internet in a wired or wireless manner. In practical environments, it is recommended to connect a wireless router to the CPE for omnidirectional wireless network coverage. The network topology is shown below.

TIP

Wi-Fi name and Wi-Fi password are **SSID** and **Key** set in step 6 above.




To access the internet, you need to configure the router as follows.

TIP

For detailed configuration of the router, refer to the user guide for your specific model.

1. Log in to the web UI of the router.
2. Select **Dynamic IP** as the **Internet Connection Type**, and save the settings.

**---End**

To access the internet with:

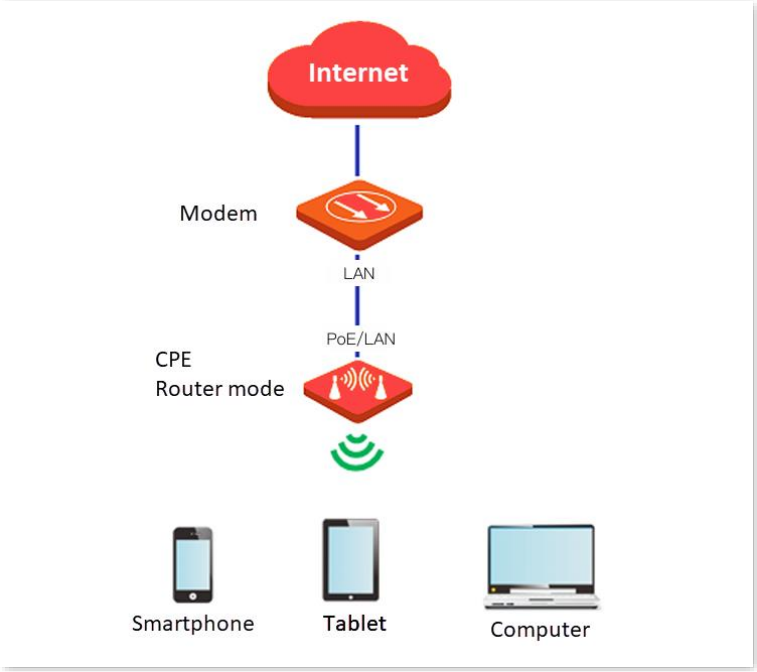
- Wi-Fi-enabled devices: Connect the Wi-Fi-enabled devices, such as a smartphone, to the router connected to the CPE over the Wi-Fi.
- Wired devices: Connect the wired devices, such as a computer, to the LAN ports of the router connected to the CPE over the Ethernet cable. Ensure that the IP address of the computer is automatically obtained.

# 3.5 Router mode

## 3.5.1 Overview

In Router mode, the CPE serves as a router to provide a wireless network.

The CPE is used to provide a wireless network and assign IP addresses to your Wi-Fi-enabled devices. The network topology is shown below.

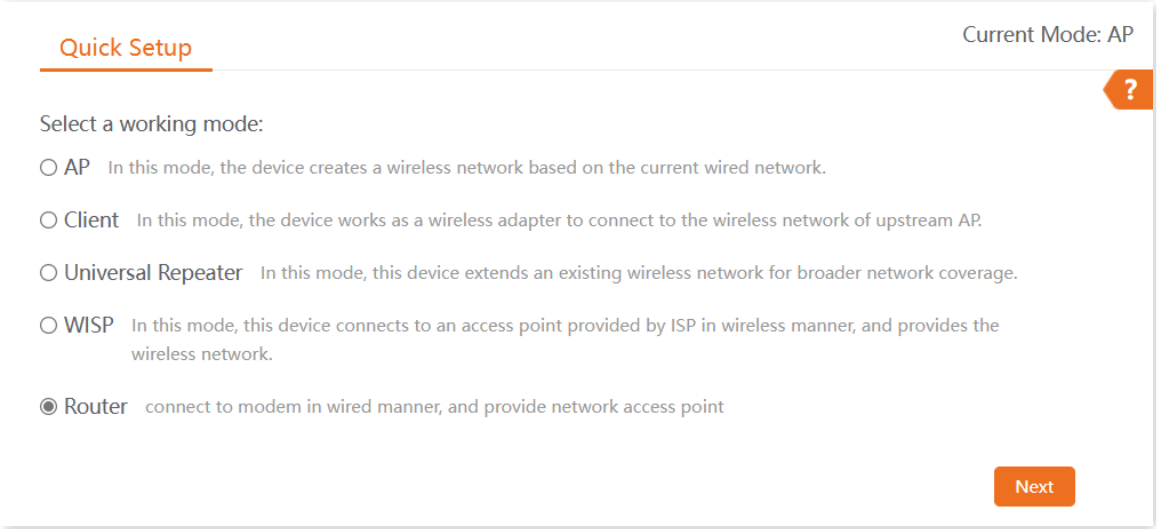



## 3.5.2 Set Router mode

TIP

If there is only one Ethernet port on the CPE, connect a wireless device (such as a laptop) to the wireless network of the CPE and log in to the web UI of the CPE to perform the following configurations.

1. Log in to the web UI of the CPE.
2. Navigate to **Quick Setup**. Select **Router** mode, and click **Next**.

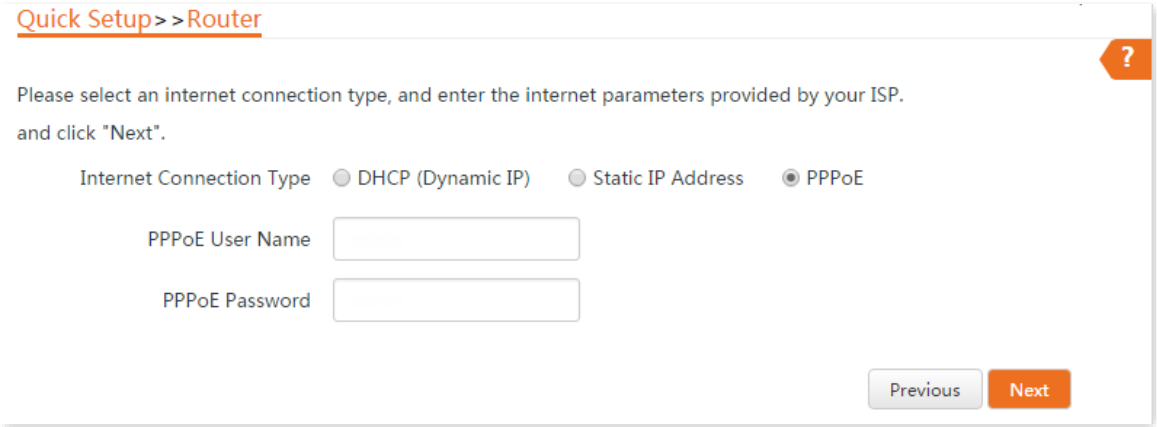



3. Select the internet connection type and configure the required parameters provided by your ISP. **PPPoE** is used as an example.

   1) Select **PPPoE**.

   2) Enter the **PPPoE User Name** and **Password** provided by your ISP.

   3) Click **Next**.



**Parameters description**

| Name | Description |
| --- | --- |
| Internet Connection Type | Select the appropriate internet connection type.<br>- **DHCP (Dynamic IP)**: The CPE obtains the IP address and other parameters from the DHCP server of the upstream device for internet access.<br>- **Static IP Address**: The CPE accesses the internet using the IP address, subnet mask, default gateway and DNS server IP addresses provided by the ISP.<br>- **PPPoE**: The CPE accesses the internet using the PPPoE user name and password provided by the ISP. |

4. Set wireless parameters of the CPE, and click **Next**.

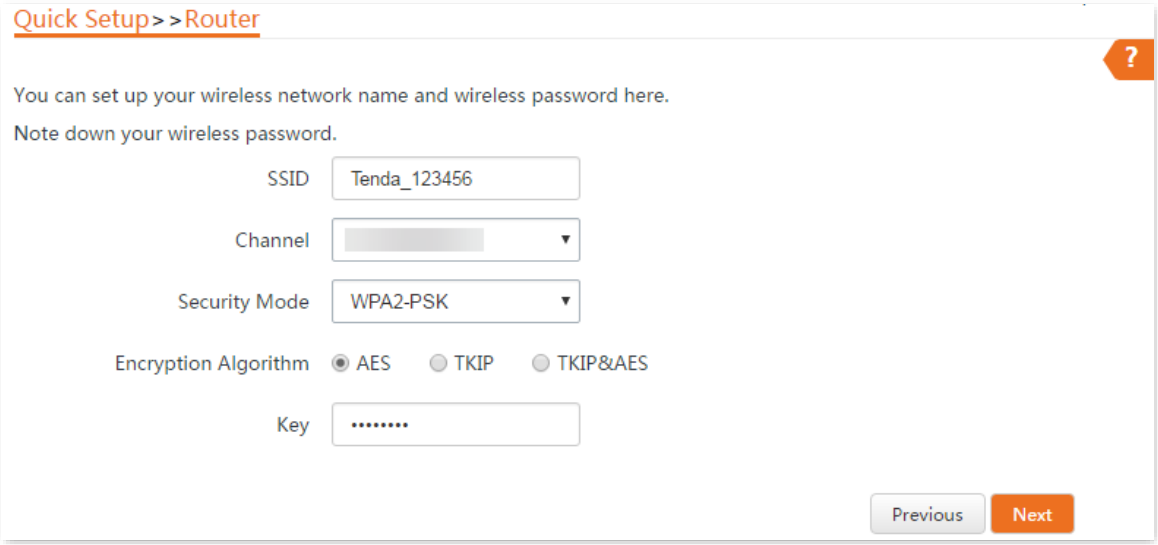
   1) Customize an **SSID** (Wi-Fi name), which is **Tenda_123456** in this example.

   2) Set **Channel**.

   3) Set **Security Mode**, which is **WPA2-PSK** in this example.

   4) Set **Encryption Algorithm**, which is **AES** in this example.

   5) Set **Key** (Wi-Fi password) for the wireless network.

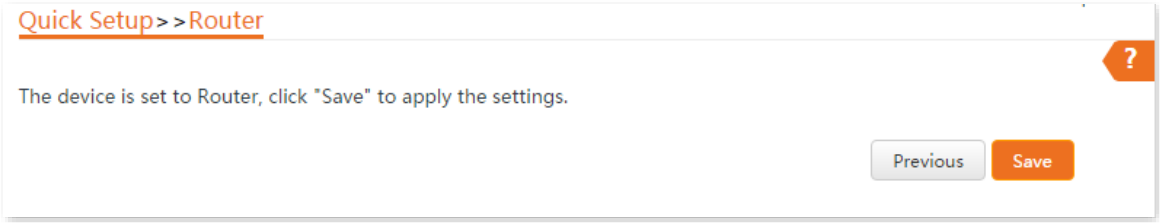



**Parameters description**

| Name | Description |
| --- | --- |
| SSID | Specifies the Wi-Fi name of the CPE. |
| Channel | Specifies the channel that the wireless network operates.<br>Auto indicates that the CPE automatically adjusts its operating channel based on the ambient environment. |
| Security Mode | Specifies the security mode of the wireless network of the CPE, including None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. |

| Name | Description |
| --- | --- |
| Encryption Algorithm | Specifies the encryption method of the wireless network.<br>- **AES**: It indicates the Advanced Encryption Standard.<br>- **TKIP**: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps.<br>- **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. |
| Key | Specifies the Wi-Fi password of the wireless network. |

5. Click **Save**, and wait until the CPE reboots to make the settings take effect.




**---End**

After the CPE is rebooted, verify the settings as follows.

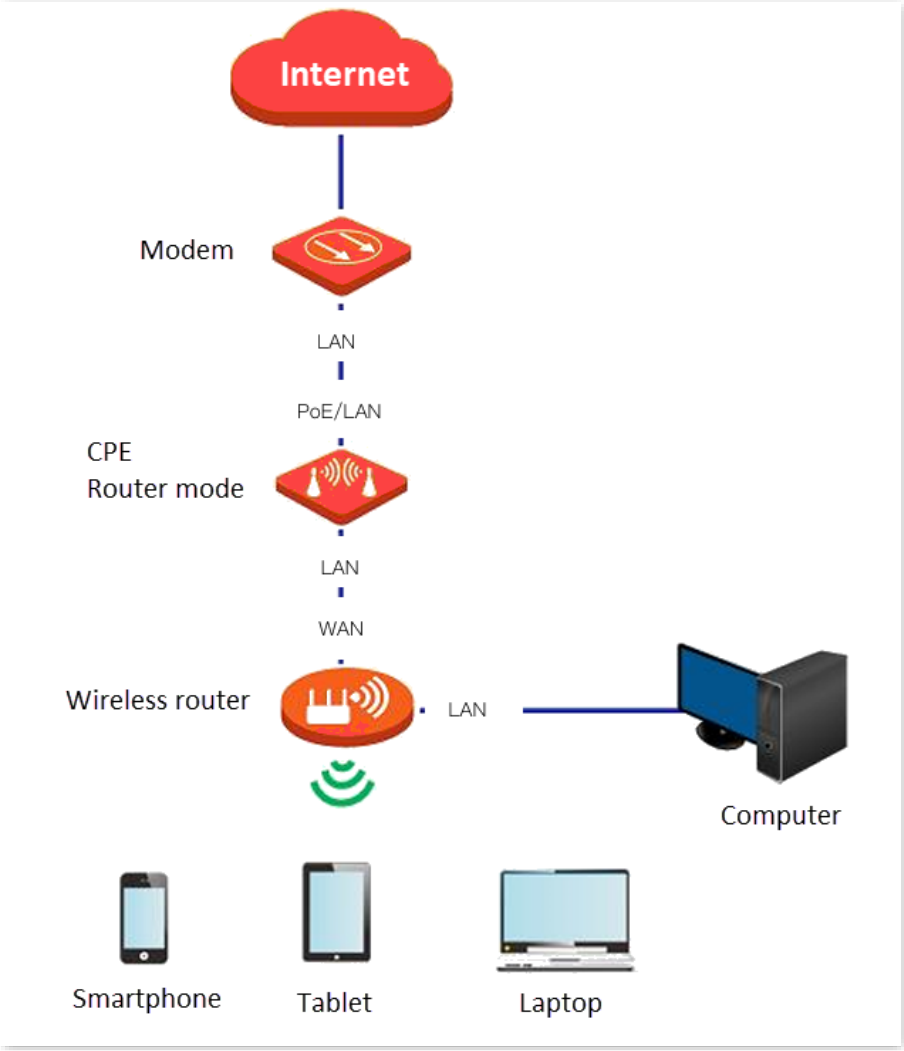
- Log in to the web UI of the CPE and navigate to Status.
- On the System Status module, ensure that the WAN IP address, default gateway and DNS server information obtained by the WAN port are displayed.

After the successful configuration, devices connected to the CPE can access the internet in a wired or wireless manner.

TIP

- If there is only one LAN port on the CPE, connect your Wi-Fi-enabled devices to the wireless network of the CPE to access the internet.
- The name and password of the wireless network are **SSID** and **Key** set in step 4.

If the CPE has more than one LAN port, connect a wireless router to the CPE for omnidirectional wireless network coverage. The network topology is shown below.




To access the internet, you need to configure the router as follows.

TIP

For detailed configuration of the router, refer to the user guide for your specific model.

1. Log in to the web UI of the router.
2. Select **Dynamic IP** as the **Connection Type**, and save the settings.

**---End**

To access the internet with:

- Wi-Fi-enabled devices: Connect the Wi-Fi-enabled devices, such as a smartphone, to the router connected to the CPE over the Wi-Fi.
- Wired devices: Connect the wired devices, such as a computer, to the LAN ports of the router connected to the CPE over the Ethernet cable. Ensure that the IP address of the computer is automatically obtained.

# 4 Get device information

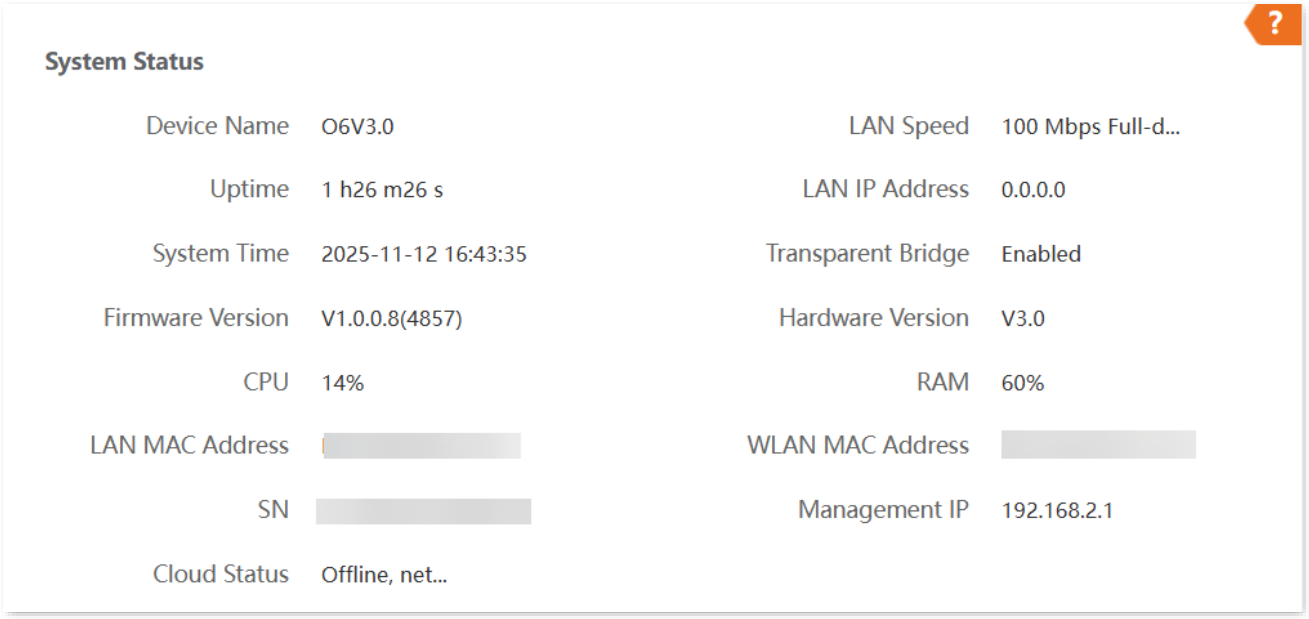
Features available in the CPE may vary by model and software version. CPE availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual CPE experience.

## 4.1 System status

To access the page, log in to the web UI of the CPE and navigate to **Status**.

You can view the system status here. O6 V3.0 is used for illustration.

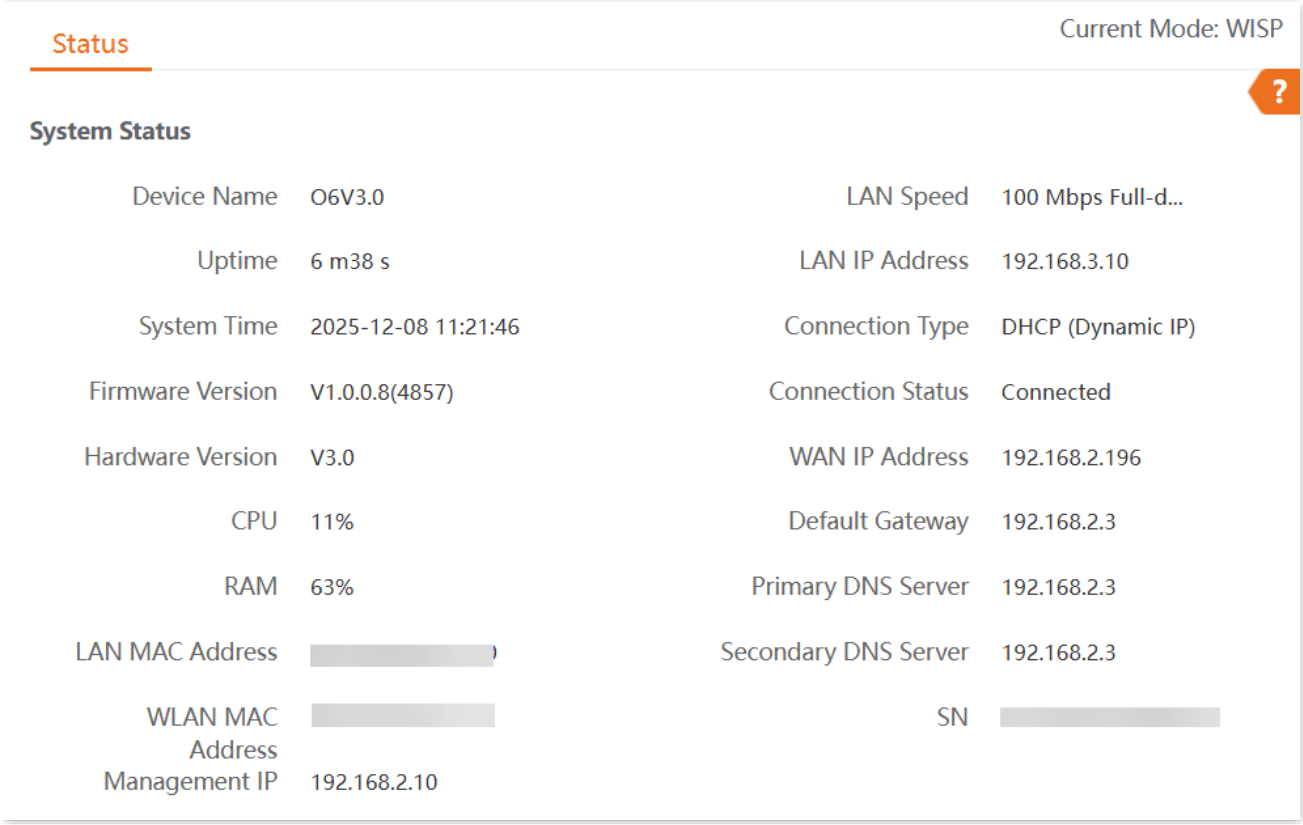
If the CPE is set to AP mode, Client mode, or Universal Repeater mode, the system status is shown as follows. If the CPE has multiple Ethernet ports, this page displays the current connection rate of each LAN port. The following figure is for reference only.




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

TIP

When the CPE works in Router mode, the PoE port serves as a WAN port.




### Parameters description

| Name | Description |
|---|---|
| Device Name | Specifies the name of this CPE. Different device names help you easily identify CPEs on the LAN.<br>You can change the name of this CPE on the LAN Setup page. |
| Uptime | Specifies the time that has elapsed since the CPE was last started. |
| System Time | Specifies the current system time of this CPE. |
| Firmware Version | Specifies the system firmware version number of this CPE. |
| Hardware Version | Specifies the hardware version number of this CPE. |
| CPU | Specifies the Central Processing Unit (CPU) usage of this CPE. |
| RAM | Specifies the memory usage of this CPE. |
| LAN MAC Address | Specifies the MAC address of the LAN port of this CPE. |
| WLAN MAC Address | Specifies the MAC address of the wireless interface of this CPE. |
| Transparent Bridge | Specifies the status of transparent bridge of the CPE in AP mode, Client mode or Universal Repeater mode. |

| Name | Description |
| --- | --- |
| Management IP | Specifies the management IP address of the CPE.<br>A LAN user can access the web UI using this IP address. You can modify this IP address on the LAN Setup page. |
| LAN Speed | Specifies the PoE/LAN or LAN port speed and duplex mode of the CPE. |
| LAN IP Address | Specifies the IP address of the CPE's LAN port, which is also the management IP address of this CPE.<br>A LAN user can access the web UI of this CPE using this IP address. You can modify this IP address on the LAN Setup page. |
| Connection Type | Specifies the internet connection type of this CPE in WISP or Router mode.<br>- **DHCP (Dynamic IP)**: The CPE obtains an IP address from the upstream DHCP server for internet access.<br>- **Static IP Address**: The CPE uses a fixed IP address, subnet mask, default gateway, and DNS server info for internet access.<br>- **PPPoE**: The CPE uses a user name and password for internet access. |
| Connection Status | Specifies the connection status of the WAN port of this CPE in WISP or Router mode. |
| WAN IP Address | Specifies the IP address of the WAN port of this CPE in WISP or Router mode. |
| Default Gateway | Specifies the default gateway address of this CPE in WISP or Router mode. |
| Primary DNS Server | Specifies the IP address of the primary DNS server of this CPE in WISP or Router mode. |
| Secondary DNS Server | Specifies the IP address of secondary DNS server of this CPE in WISP or Router mode. |
| SN | Specifies the serial number of the CPE. |
| Cloud Status | Specifies the connection status between the CPE and Tenda CloudFi Cloud platform. |

# 4.2 Wireless status

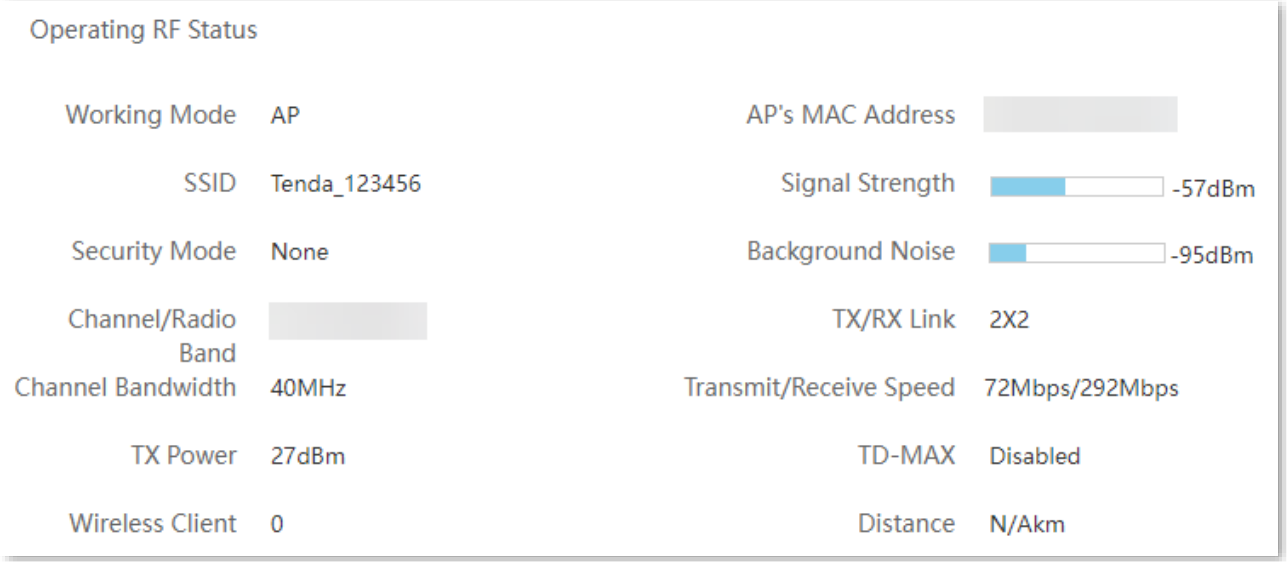
To access the page, log in to the web UI of the CPE and navigate to **Status**.

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

## 4.2.1 View operating RF status

The operating RF (such as 5 GHz) is mainly used to bridge the wireless network of another CPE.

On the **Operating RF Status** module, you can view the wireless status information of the CPE's operating RF, including working mode, SSID, security mode, and so on. The following figure is for reference only.




**Parameters description**

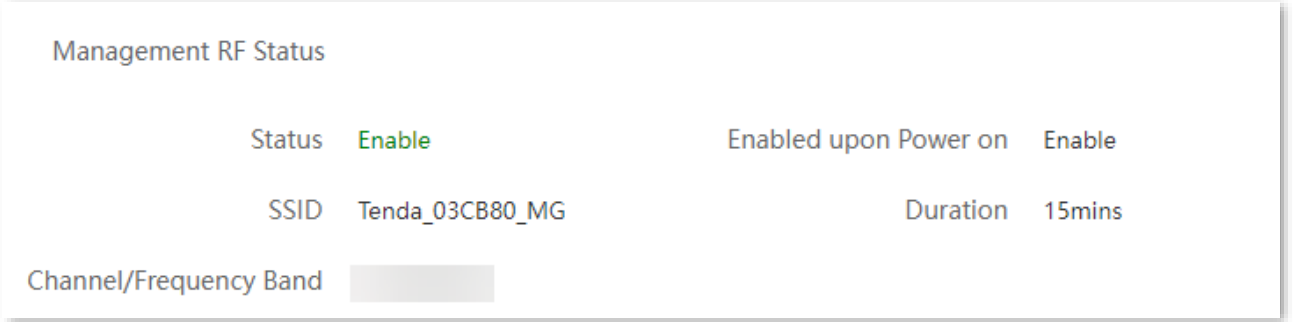
| Name | Description |
|---|---|
| Working Mode | Specifies the working mode in which the CPE operates. |
| SSID | Specifies the Wi-Fi name of the operating RF.<br>N/A means the feature is not supported. |
| Security Mode | Specifies the security mode of the wireless network of the CPE's operating RF. |
| Channel/Radio Band | Specifies the channel and radio band used by this device to transmit radio signals. |
| Channel Bandwidth | Specifies the channel bandwidth of the CPE's operating RF. |
| TX Power | Specifies the transmitted power of the CPE's operating RF. |
| Wireless Client | Specifies the number of wireless clients connected to the wireless network of the CPE's operating RF. |
| AP's MAC Address | Specifies the MAC address of the upstream device.<br>- In AP or Router mode, it displays the WLAN MAC address of the CPE.<br>- In Client, Universal Repeater or WISP mode, when the bridging succeeds, it displays the WLAN MAC address of the upstream AP. When the bridging fails, it displays N/A. |

| Name | Description |
| --- | --- |
| Signal Strength | Specifies the wireless signal strength of the peer device.<br>- In AP or Router mode, it displays the signal strength of the first device connected to the wireless network of this CPE.<br>- In Client, Universal Repeater or WISP mode, it displays the received signal strength of the peer CPE. |
| Background Noise | Specifies the strength of radio interference signals in the ambient environment that interferes with the wireless signal of this CPE in the same channel. A larger absolute value indicates less interference. |
| TX/RX Link | Specifies the number of spatial streams of wireless data the CPE is transmitting or receiving. The more links indicate the more traffic. A larger number of spatial streams indicates a higher link capacity. |
| Transmit/Receive Speed | 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 CPE.<br>- In Client, Universal Repeater or WISP mode, it displays transmitting/receiving rate of this CPE. |
| TD-MAX | Specifies the status of the TD-MAX function. For details, refer to TD-MAX. |
| Distance | Specifies the distance between the two CPEs after the bridging succeeds.<br>If there are more than two CPEs, it specifies the bridging distance between this CPE and the farthest CPE. |

## 4.2.2 View management RF status

The management RF (2.4 GHz) is mainly used to allow users to connect to the CPE's wireless network and manage the CPE under special circumstances. For example: When the CPE is working in Client mode, you can log in to the web UI of the CPE by connecting to the wireless network of the CPE's management RF.

On the **Management RF Status** module, you can view the wireless status information of the CPE's management RF, including working status, SSID, status of management RF enabled upon power on, and so on. Relevant configurations can be set on the Management RF page. The following figure is for reference only.



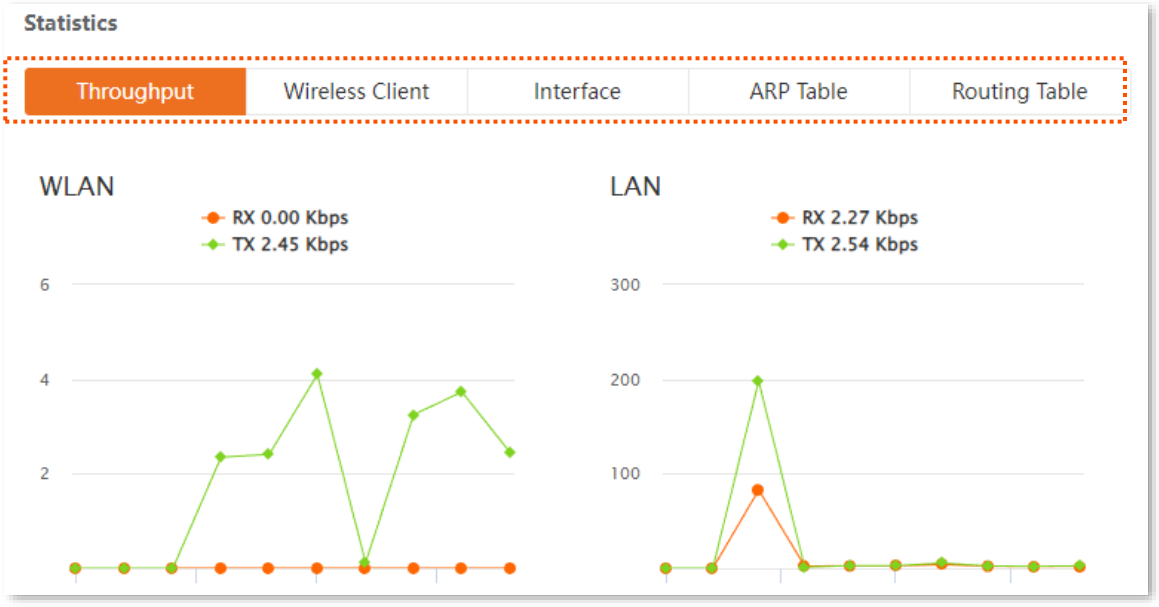
**Parameters description**

| Name | Description |
|---|---|
| Status | Specifies the working status of the CPE's management RF. |
| SSID | Specifies the Wi-Fi name sent by the CPE's management RF. |
| Channel/Frequency Band | Specifies the channel and frequency band of the CPE's management RF. |
| Enabled upon Power on | Specifies the status of the CPE's management RF auto-start function. With this function enabled, the management RF will be automatically enabled after the CPE is powered off and then powered on again. |
| Duration | Specifies how long the CPE's management RF remains enabled. If you do not extend duration of management RF's wireless network, the management RF will be automatically disabled after the auto-start duration is exceeded. |

# 4.3 Statistics

To access the page, log in to the web UI of the CPE and navigate to **Status**.

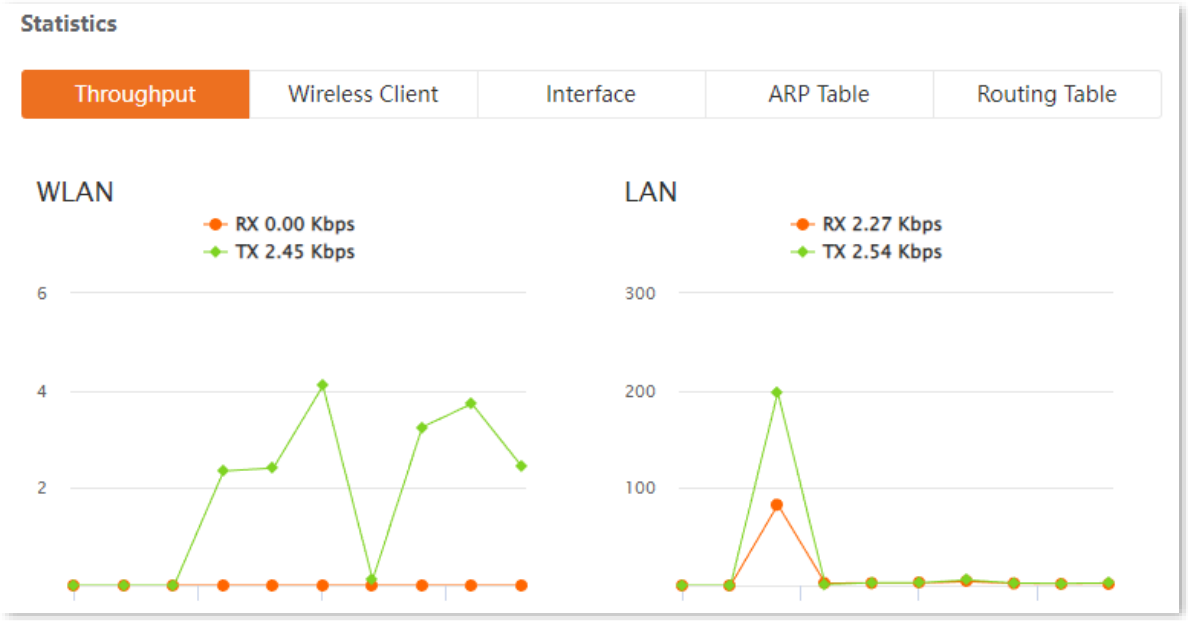
You can view statistics for throughput, wireless client, interface, ARP table and routing table here. The following figure is for reference only.




## 4.3.1 Throughput

On the **Statistics** module, click **Throughput** to access the page.

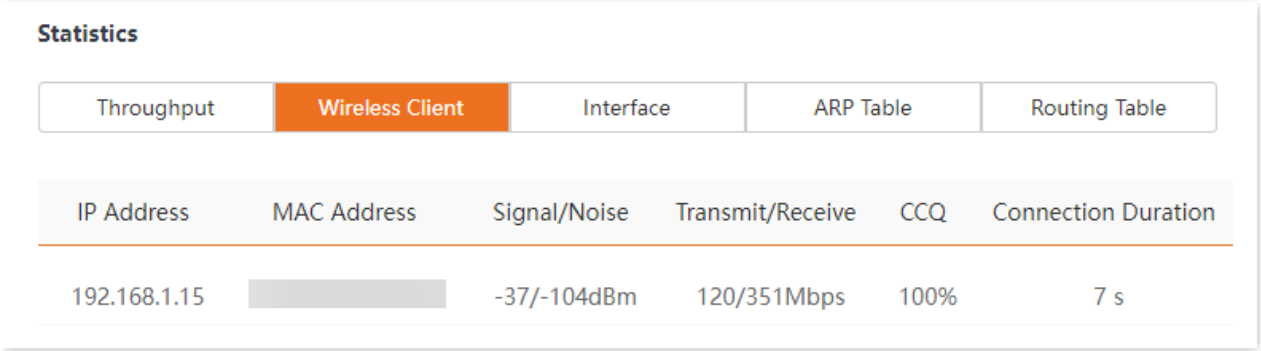
The line charts visually show the real-time transmitting and receiving traffic of WLAN and LAN port of the CPE. RX indicates the receive rate, and TX indicates the transmit rate. The following figure is for reference only.




## 4.3.2 Wireless client

On the **Statistics** module, click **Wireless Client** to access the page.

In AP or Router mode, it displays information of connected wireless clients. The following figure is for reference only.




**Parameters description**

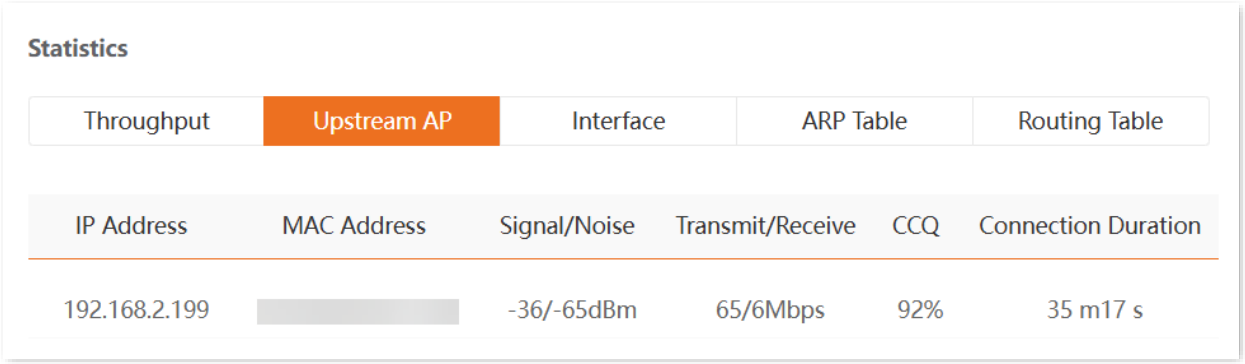
| Name | Description |
|---|---|
| IP Address | Specifies the IP address of the wireless client. |
| MAC Address | Specifies the MAC address of the wireless client. |

| Name | Description |
| --- | --- |
| Signal/Noise | **Signal**: Specifies the Wi-Fi signal strength of the wireless client.<br>**Noise**: Specifies the ambient interference signal strength and electromagnetic interference signal strength of the wireless client. |
| Transmit/Receive | Specifies the transmitting and receiving rate of the wireless client. |
| CCQ | Specifies the connection quality of the wireless client. A higher percentage indicates better connection quality. |
| Connection Duration | Specifies the time that has elapsed since the wireless client connected to the wireless network of the CPE. |

## 4.3.3 Upstream AP

On the **Statistics** module, click **Upstream AP** to access the page.

In Client, Universal Repeater or WISP mode, it displays information of the upstream AP. The following figure is for reference only.



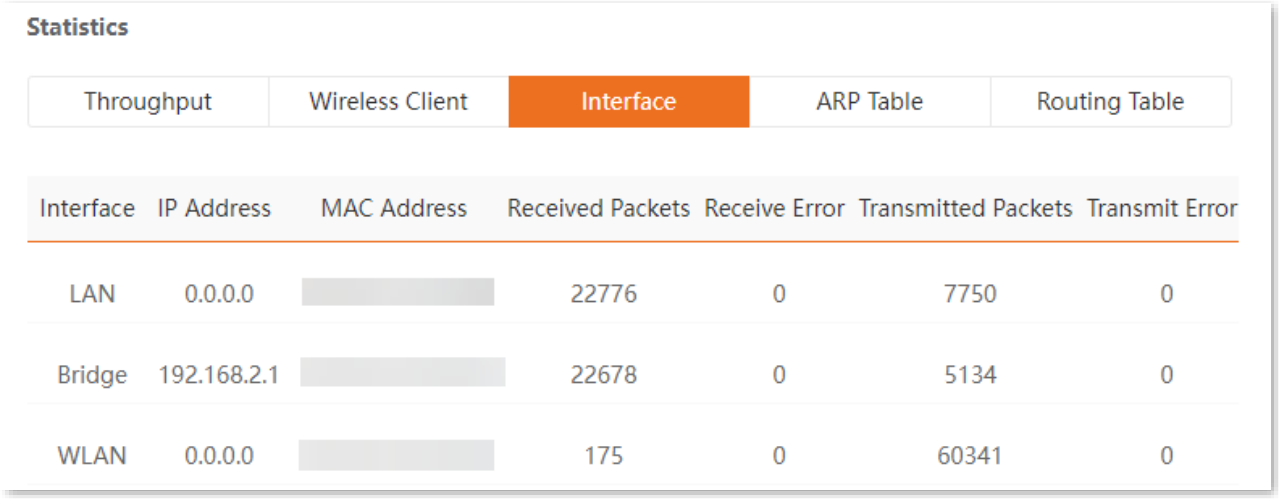

**Parameters description**

| Name | Description |
| --- | --- |
| IP Address | Specifies the IP address of the upstream device. |
| MAC Address | Specifies the MAC address of the upstream device. |
| Signal/Noise | **Signal**: Specifies the Wi-Fi signal strength of the upstream device.<br>**Noise**: Specifies the ambient interference signal strength and electromagnetic interference signal strength of the upstream device. |
| Transmit/Receive | Specifies the transmitting and receiving rate of the upstream device. |
| CCQ | Specifies the connection quality between this CPE and the upstream device. A higher percentage indicates better connection quality. |
| Connection Duration | Specifies the time that has elapsed since this CPE established a bridge connection to the upstream device. |

## 4.3.4 Interface

On the **Statistics** module, click **Interface** to access the page.

It displays the IP address, MAC address and traffic information of the interfaces of the CPE. The following figure is for reference only.



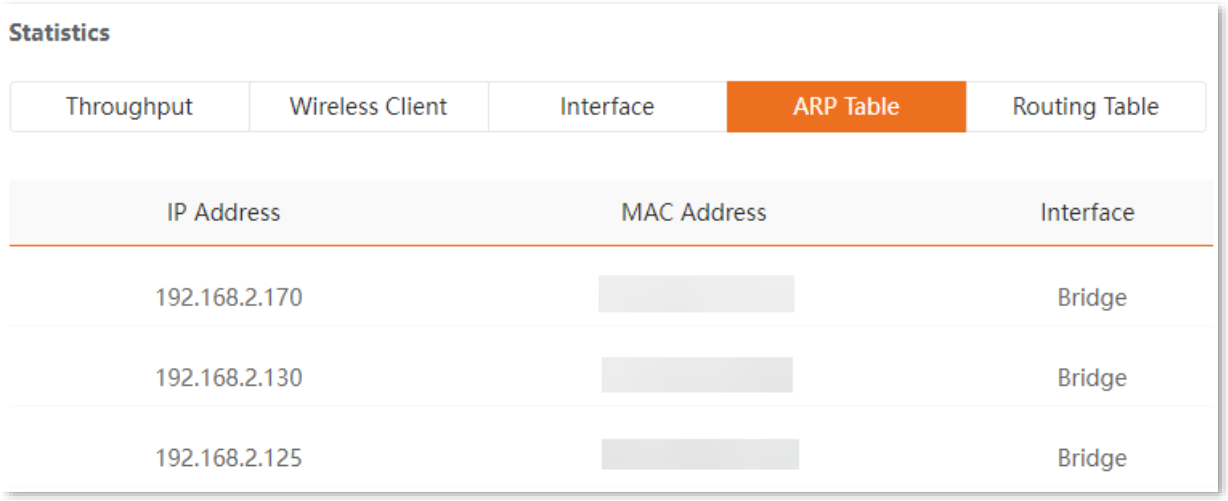

**Parameters description**

| Name | Description |
|---|---|
| Interface | Specifies the wired interface, bridge interface, and WLAN interface of the CPE. |
| IP Address | Specifies the IP addresses of the wired interface, bridge interface, and WLAN interface. |
| MAC Address | Specifies the MAC addresses of the wired interface, bridge interface, and WLAN interface. |
| Received Packets | Specify the number of received or transmitted packets of the interface. |
| Transmitted Packets | |
| Receive Error | Specify the number of received or transmitted error packets of the interface. |
| Transmit Error | |

## 4.3.5 ARP table

On the **Statistics** module, click **ARP Table** to access the page.

ARP, short for Address Resolution Protocol, obtains the MAC address of a target device based on its IP address, thereby ensuring smooth communication. The ARP table displays the mappings between IP addresses and their corresponding MAC addresses. The following figure is for reference only.



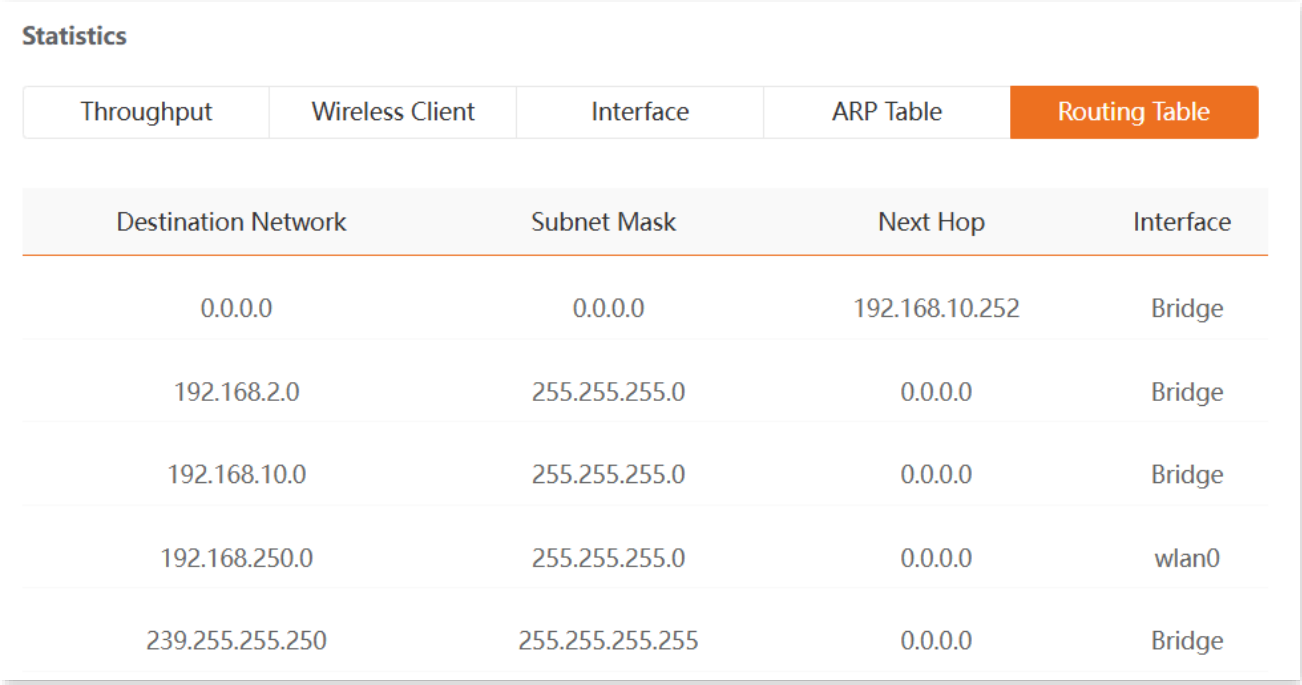

**Parameters description**

| Name | Description |
|---|---|
| IP Address | Specifies the IP address of the host in the ARP table. |
| MAC Address | Specifies the MAC address corresponding to the IP address of the host. |
| Interface | Specifies the interface used to communicate with the host. |

## 4.3.6 Routing table

On the **Statistics** module, click **Routing Table** to access the page.

The routing table displays the destination networks that the CPE can access. The following figure is for reference only.



### Parameters description

| Name | Description |
| --- | --- |
| Destination Network | Specifies the destination network address of the IP packet. |
| Subnet Mask | Specifies the subnet mask of the destination network. |
| Next Hop | Specifies the ingress IP address of the next-hop router after packets egress from the interface of the CPE. |
| Interface | Specifies the interface through which the packets egress. |

# 5 Manage network settings

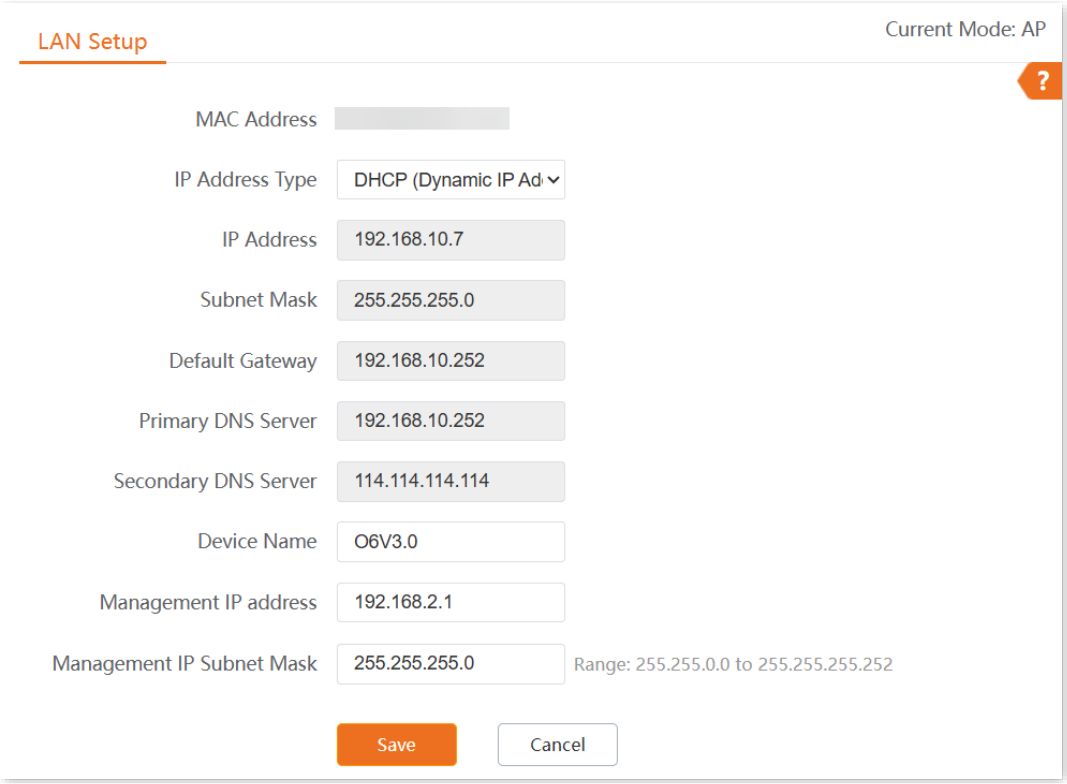
Features available in the CPE may vary by model and software version. CPE availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual CPE experience.

## 5.1 LAN setup

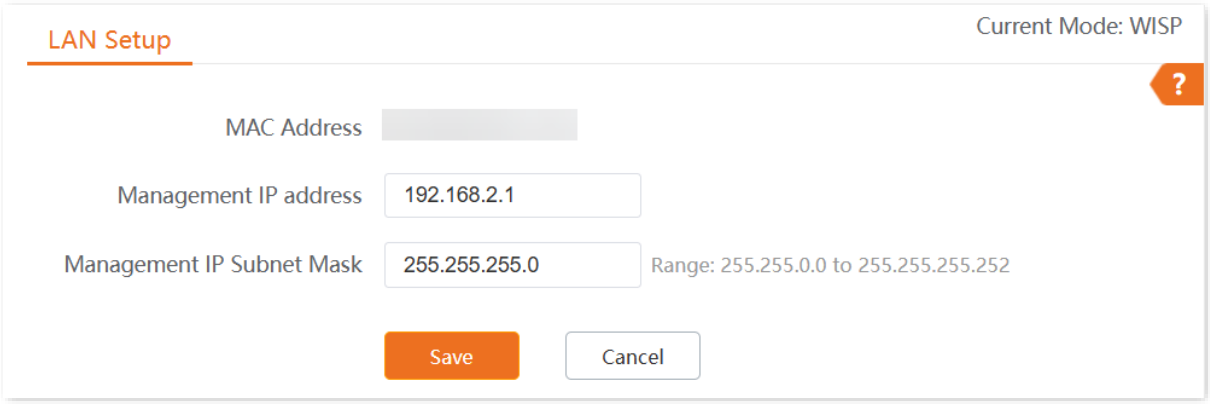
### 5.1.1 Overview

To access the page, log in to the web UI of the CPE and navigate to **Network** > **LAN Setup**.

In AP or Client mode, you can view the MAC address of the LAN port, configure the device name and method used to obtain an IP address and related parameters for the CPE. The following figure is for reference only.



In WISP or Router mode, you can view the MAC address of the LAN port, management IP address (also LAN IP address), and subnet mask. The following figure is for reference only.




### Parameters description

| Name | Description |
|---|---|
| MAC Address | Specifies the MAC address of LAN port. |
| IP Address Type | Specifies how the CPE obtains 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 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 CPE's IP address on the client list of the upstream DHCP server, and use this IP address to log in to the web UI of the CPE. |
| IP Address | Specifies the IP address of the CPE. A LAN user can use this IP address to log in to the web UI of the CPE.<br>To connect the CPE to the internet, change this IP address to the same subnet as the LAN IP address of the egress router. |
| Subnet Mask | Specifies the subnet mask of the CPE. The default is **255.255.255.0**. |
| Default Gateway | Specifies the default gateway of the CPE.<br>You can set it to the LAN IP address of the egress router to enable the CPE to access the internet. |
| Primary DNS Server | Specifies the primary DNS server IP address of the CPE.<br>If the egress router has the DNS proxy function, it can be set to the LAN IP address of the egress router. Otherwise, specify a DNS server IP address manually.<br>If there is only one DNS server IP address, enter it in this box. |

| Name | Description |
| --- | --- |
| Secondary DNS Server | Specifies the secondary DNS server IP address of the CPE.<br>If two DNS server IP addresses are available, enter the secondary DNS server IP address in this box. |
| Device Name | Specifies the name of the CPE. The default name is the product model and version.<br>You are recommended to change the name to indicate the location of the CPE, so that you can easily identify the target CPE in the network. |
| Management IP address | Specifies the management IP address of the CPE.<br>When the device's IP address and the management IP address are in the same subnet within the local network, you can log in to the web UI via the management IP address. |
| Management IP Subnet Mask | Specifies the subnet mask of the management IP address for the CPE. |

## 5.1.2 Modify LAN IP address

### Set a manual LAN IP address

If you need to deploy only a few CPEs as a network administrator, you can manually set the IP address, subnet mask, gateway IP address and DNS server IP addresses of the CPEs.

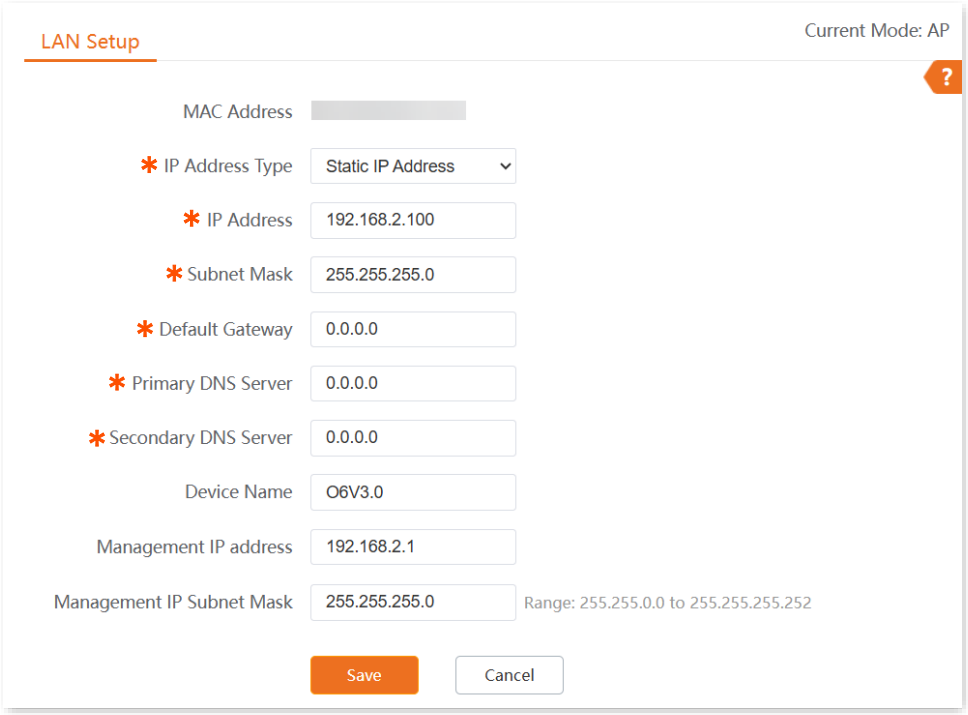
**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Network** > **LAN Setup**.
3. Set **IP Address Type** to **Static IP Address**.
4. Configure **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary/Secondary DNS Server**.

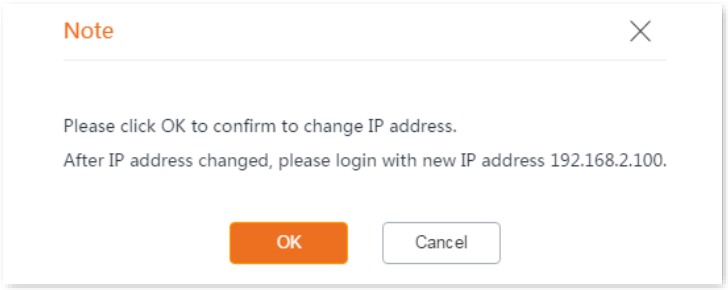
TIP

To configure the CPE to access the internet, ensure its IP address is unique and within the same subnet as the LAN IP address of the upstream device. Then, set the default gateway to the LAN IP address of the upstream device, and enter a valid DNS server address.

5. Click **Save**. The following figure is for reference only.




6. Confirm the prompt information, and click **OK**.




**---End**

To re-access the web UI of the CPE using the LAN IP address:

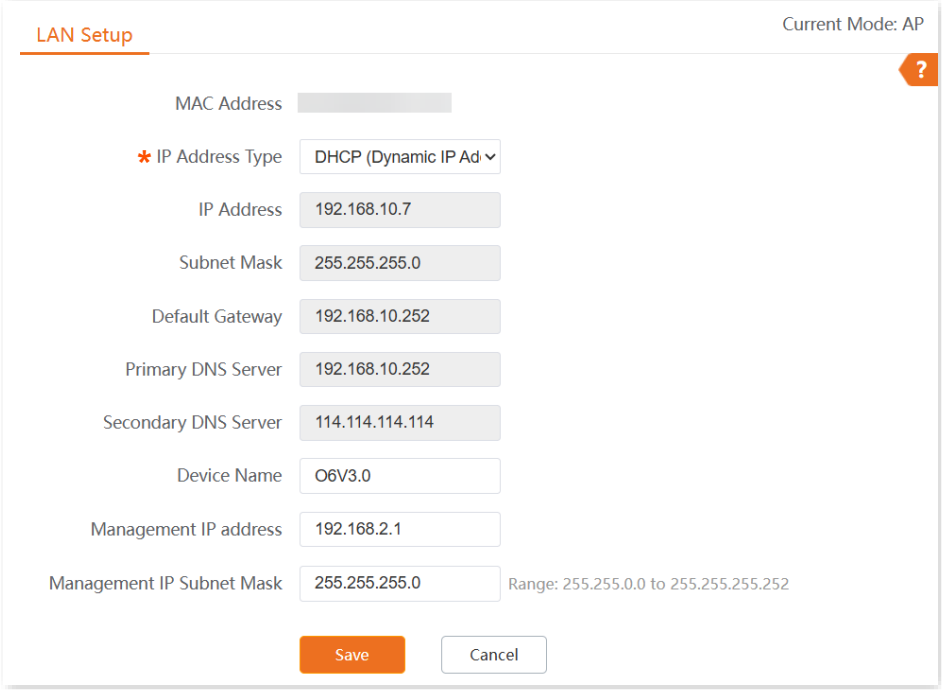
- If the new IP address is in the same subnet as the original one, use the new IP address to log in to the web UI again.
- If the new and original IP addresses belong to different subnets, assign your computer an IP address that falls in the same subnet as the new IP address before logging in with the new IP address. Refer to Assign a fixed IP address to your computer in **Appendix** for details.

## Obtain a LAN IP address automatically

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

**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Network** > **LAN Setup**.
3. Set **IP Address Type** to **DHCP (Dynamic IP Address)**.
4. Click **Save**. The following figure is for reference only.




**---End**

If you want to re-access the web UI of the CPE, check the new IP address in the DHCP client list of the upstream device. Ensure that the management computer and the CPE belong to the same subnet before accessing the IP address of the CPE.

Refer to steps in Assign a fixed IP address to your computer to assign an IP address to the computer manually.

## 5.1.3 Modify management IP address

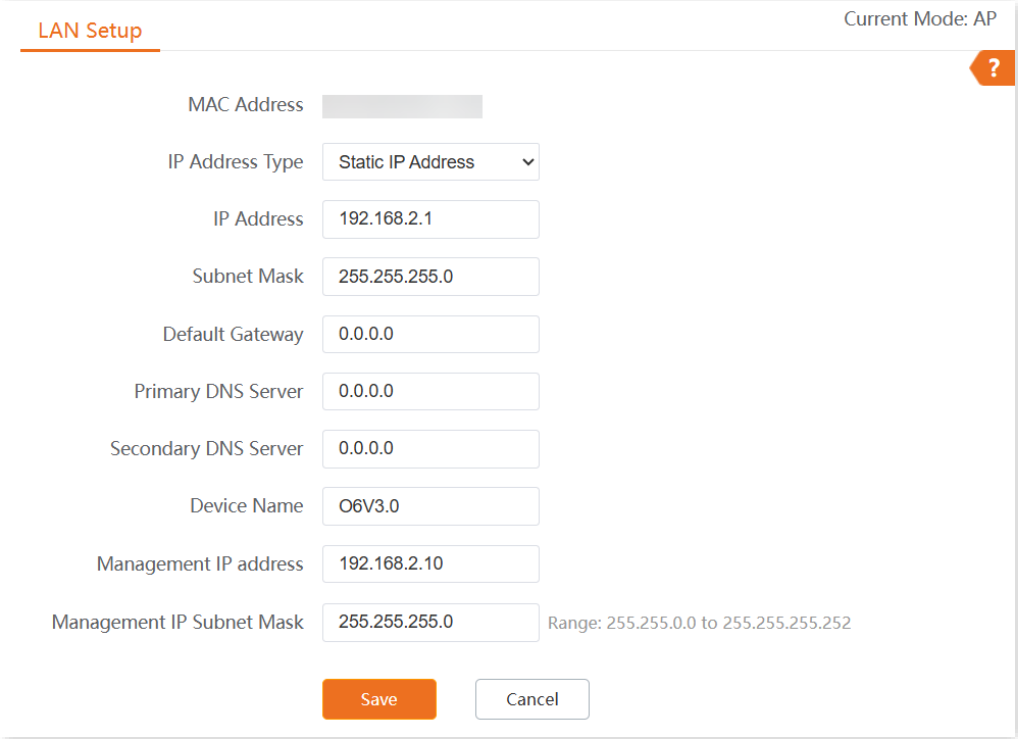
LAN users can access the CPE's web UI page using either the LAN IP address or the management IP address. If you're unsure of the CPE's LAN IP when logging in, try the management IP (default: 192.168.2.1 in AP mode, 192.168.2.2 in Client mode).

Suppose you want to change the CPE's management IP address to 192.168.2.10.

**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Network** > **LAN Setup**.

3. Change the management IP address to 192.168.2.10.
4. Click **Save**. The following figure is for reference only.




**---End**

To re-access the web UI of the CPE using the management IP address:

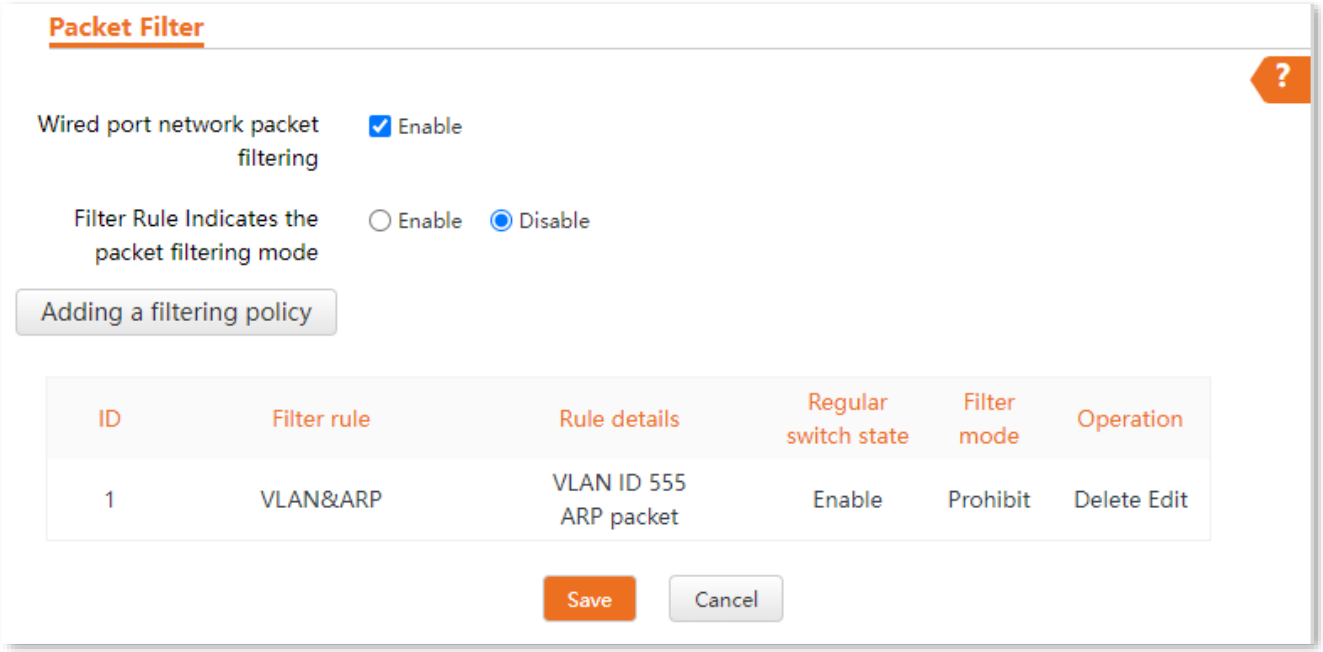
- If the new IP address is in the same subnet as the original one, use the new IP address to log in to the web UI again.
- If the new and original IP address belong to different subnets, assign your computer an IP address that falls in the same subnet as the new IP address before logging in with the new IP address. Refer to Assign a fixed IP address to your computer in **Appendix** for details.

# 5.2 Packet filter

If there are a large number of broadcast packets in the LAN, processing these broadcast packets by the CPE will occupy a large amount of CPU resources, thus affecting the data transmission of the CPE. After the packet filtering function is configured, when the packets received by the CPE's wired Ethernet port meet the preset features, these packets will be filtered out, reducing the number of broadcast packets that the CPE needs to process and ensuring the CPE's data transmission.

To access the page, log in to the web UI of the CPE and navigate to **Network** > **Packet Filter**.

On this page, you can set packet filtering parameters of the wired Ethernet port. The 2-pack CPE O1 V1.0 is used for illustration.




### Parameters description

| Name | Description |
|---|---|
| Wired port network packet filtering | Specifies whether to enable the wired port network packet filtering function. |
| Filter Rule Indicates the packet filtering mode | Specifies whether to allow packets without filtering rules configured to pass through. |
| Adding a filtering policy | Used to add a rule for filtering packets. |
| Filter rule | Specifies the filtering rule of packets that need to be filtered.<br>- **MAC address**: Used to configure the packets corresponding to the MAC address to be filtered.<br>- **IP**: Packets whose protocol type is IP protocol will be filtered.<br>- **VLAN**: Packets whose protocol type is IEEE 802.1Q protocol will be filtered.<br>- **ARP**: Packets whose protocol type is ARP protocol will be filtered.<br>- **Port No.**: Used to configure the packets corresponding to the port number to be filtered.<br>- **Custom**: Customize the protocol type field of the packets to be filtered. |
| Rule details | Specifies the parameter settings required for filtering rules to filter the packets. |
| Regular switch state | Specifies the status of the filtering rule. Values: **Enable** and **Disable**. |
| Filter mode | Specifies whether to filter the packets. Values: **Permit** and **Prohibit**. |

| Name | Description |
| --- | --- |
| Operation | Used to edit or delete the packet filter policy.<br>- **Edit**: Used to edit the packet filter policy.<br>- **Delete**: Used to delete the packet filter policy. |
| Source MAC | Specifies the data frames from this MAC address to be filtered. |
| Destination MAC | Specifies the data frames with this MAC address as the destination address to be filtered. |
| Source IP | Specifies the packets from this IP address to be filtered. |
| Destination IP | Specifies the packets with this IP address as the destination address to be filtered. |
| IP protocol type | Specifies the type of transport layer protocol used by the data segments that need to be filtered. **All** means filtering both TCP and UDP protocols. |
| VLAN ID | Specifies the VLAN ID of the packets to be filtered. |
| Source port | Specifies the packets corresponding to the source port number to be filtered. |
| Destination port | Specifies the packets corresponding to the destination port number to be filtered. |
| Custom | Used to customize the protocol type field of the packets that need to be filtered (2 bytes, hexadecimal, such as 0x8010). |

# 5.3 MAC clone

## 5.3.1 Overview

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

If the CPE cannot access the internet after you configure the internet settings, your ISP may have associated your internet service account with a device's MAC address. In this case, MAC cloning can generally fix this problem.

NOTE

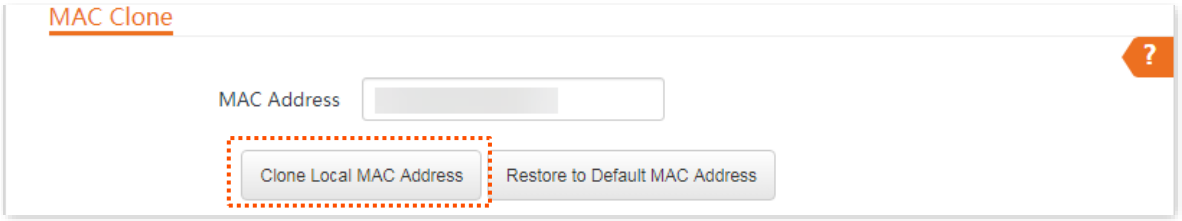
Clone the MAC address of a computer that can access the internet, or the MAC address of the WAN port of the CPE that can access the internet.

## 5.3.2 Clone a MAC address

If you can access the internet through your previous computer, perform the steps in Method 1. If you can access the internet through your previous router, see Method 2.

## Method 1

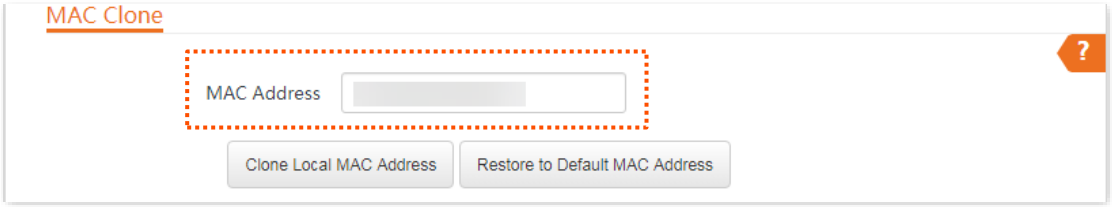
1. Connect the computer to the CPE.
2. Log in to the web UI of the CPE.
3. Navigate to **Network** > **MAC Clone.**
4. Click **Clone Local MAC Address**.
5. Click **Save**.




**---End**

## Method 2

1. Record the correct MAC address.
2. Log in to the web UI of the CPE.
3. Navigate to **Network** > **MAC Clone.**
4. Enter the MAC address in the **MAC Address** field.
5. Click **Save**.




**---End**

TIP

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

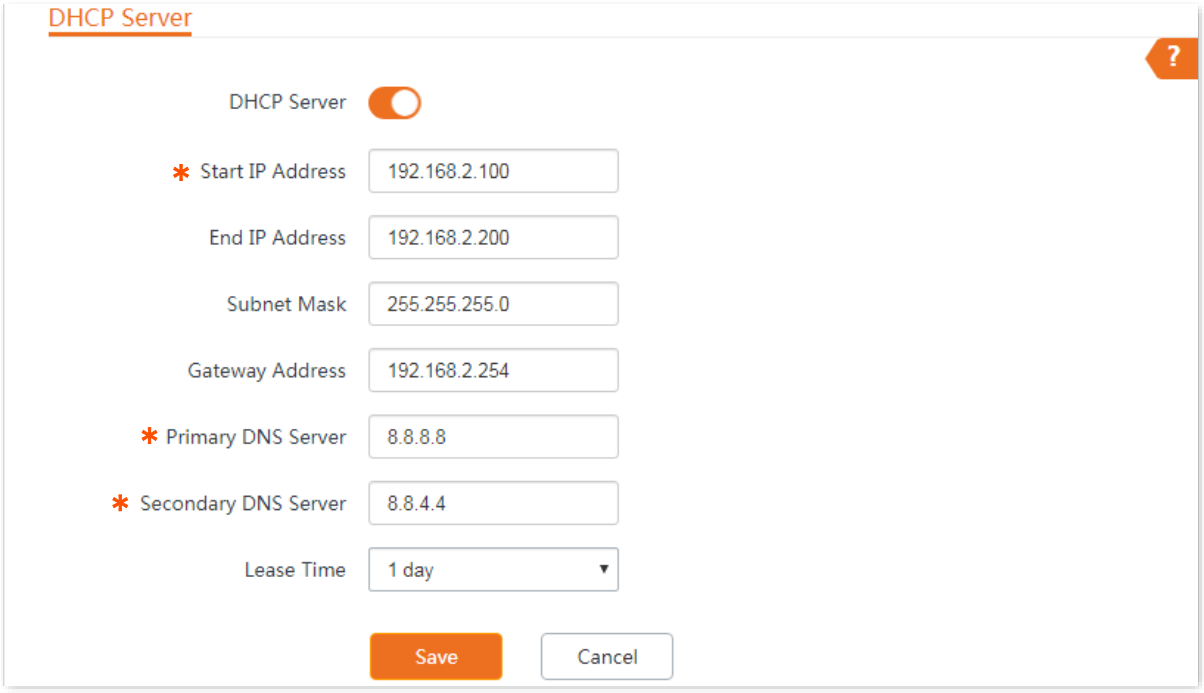
# 5.4 DHCP server

## 5.4.1 Overview

The CPE provides the DHCP server function to automatically assign IP addresses to clients in the local network. In AP, Client, or Universal Repeater mode, if the CPE obtains an IP address from the DHCP server in the local network, the CPE will disable its DHCP server automatically.

## 5.4.2 Configure the DHCP server

1. Log in to the web UI of the CPE.
2. Navigate to **Network** > **DHCP Server**.
3. Enable the **DHCP Server** function, then set parameters.
4. Click **Save**.




**---End**

NOTE

If the CPE obtains an IP address from the DHCP server in the local network, the CPE will disable its DHCP server automatically upon any change in the IP address.

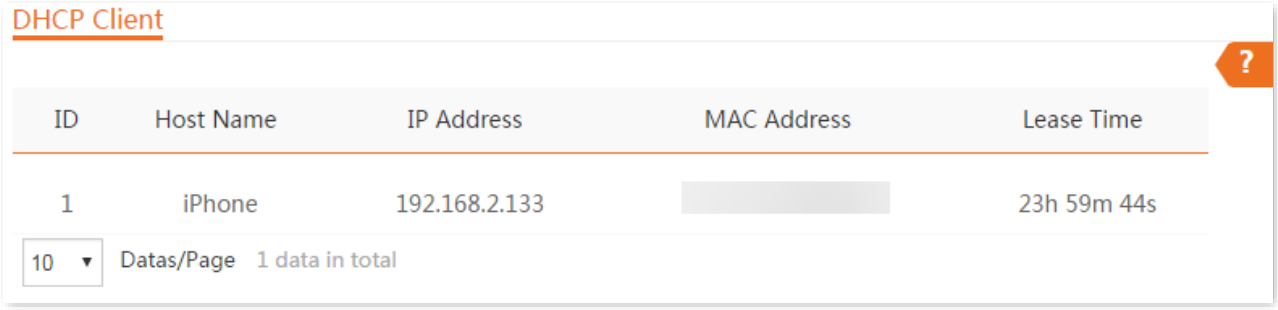
### Parameters description

| Name | Description |
| --- | --- |
| DHCP Server | Specifies whether to enable the DHCP server function of the CPE. |
| Start IP Address | 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 | Specifies the end IP address of the IP address pool of the DHCP server. The default value is **192.168.2.200**.<br>TIP<br>The start and end IP addresses must belong to the same subnet as the LAN IP address of the CPE. |
| Subnet Mask | Specifies the subnet mask assigned by the DHCP server to clients. The default value is **255.255.255.0**. |
| Gateway Address | Specifies the IP address of default gateway assigned by the DHCP server to clients. Generally, it is the IP address of the LAN port of the router in LAN. The default value is **192.168.2.254**.<br>TIP<br>A client can access a server or host not in the local network segment only through a gateway. |
| Primary DNS Server | Specifies the primary DNS server IP address assigned by the DHCP server to clients. The default value is **8.8.8.8**.<br>TIP<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 | (Optional) Specifies the secondary DNS server IP address assigned by the DHCP server to clients. |
| Lease Time | Specifies the validity period that a client holds an IP address assigned by the DHCP server.<br>When the IP address expires:<br>- If the client is still connected to the CPE, the client will automatically renew and continue to occupy the IP address.<br>- If the client is not connected to the CPE (due to shut-down or wireless disconnection), the CPE will release the IP address. If other clients send a request for an IP address, the CPE can assign this IP address to other clients.<br>You are recommended to keep the default value. |

# 5.5 DHCP client

To access the page, log in to the web UI of the CPE and navigate to **Network** > **DHCP Client**.

With the DHCP server enabled on the CPE, you can view details about the clients that obtain IP addresses from the DHCP server, including host names, IP addresses, MAC addresses and lease time. The following figure is for reference only.




**Parameters description**

| Name | Description |
|---|---|
| Host Name | Specifies the name of the DHCP client. |
| IP Address | Specifies the IP address assigned by the DHCP server to clients. |
| MAC Address | Specifies the MAC address of the DHCP client. |
| Lease Time | Specifies the validity period that a client holds an IP address assigned by the DHCP server. |

# 5.6 VLAN settings

## 5.6.1 Overview

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

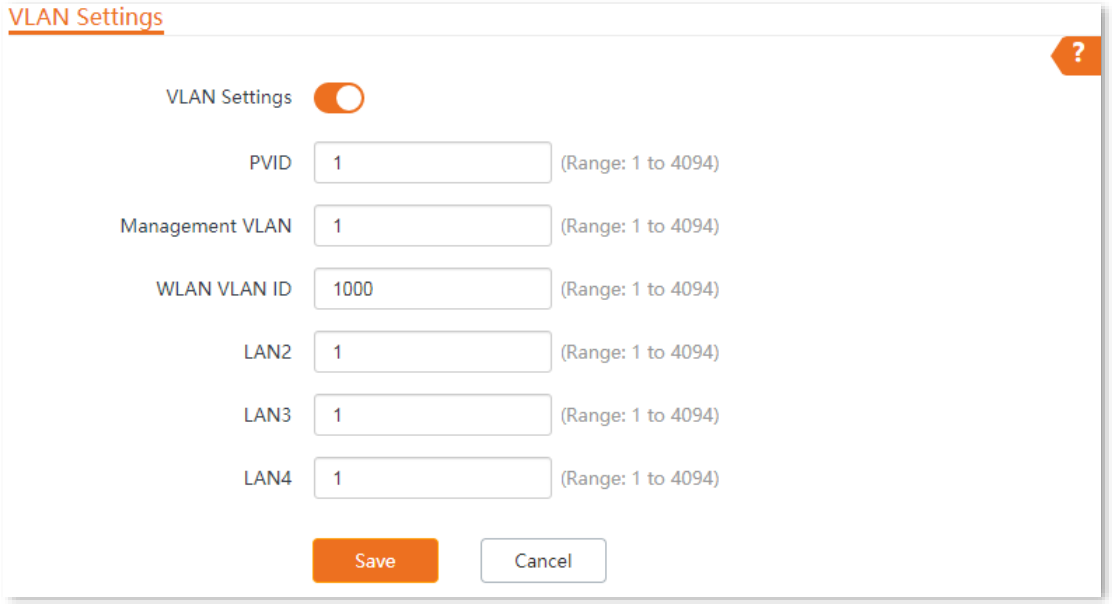
After the IEEE 802.1Q VLAN settings take effect, tagged packets will be forwarded to the ports of the corresponding VLAN according to the VID of the packet, and untagged packets will be forwarded to the ports of the corresponding VLAN according to the PVID of the port.

The following table shows how different link ports process received packets and transmitted packets:

| Port Type | Received Packets | | Transmitted Packets |
|---|---|---|---|
| | Tagged Packets | Untagged Packets | |
| Access | Forward data to the ports of the corresponding VLAN based on the tag's VID | Forward data to the ports of the corresponding VLAN based on the PVID | Strip the tag in the packet and then forward it |
| Trunk | | | VID = Port PVID, strip the tag in the packet and then forward it<br>VID ≠ port PVID, retain the tag in the packet and then forward it |

## 5.6.2 Configure VLAN (Example: OS3 V2.0)

To access the page, log in to the web UI of the CPE and navigate to **Network** > **VLAN Settings**. Enable the **VLAN Settings** function. Set the parameters as required and click **Save**.




**Parameters description**

| Name | Description |
|---|---|
| VLAN Settings | Specifies whether to enable the 802.1Q VLAN function of this CPE. By default, it is disabled. After the VLAN function is enabled, the LAN port with PoE power supply function (such as PoE/LAN) is used as a trunk port. |
| PVID | Specifies the default native VLAN ID of the trunk port. The default is **1**. |
| Management VLAN | Specifies the management VLAN ID of this CPE. The default ID is **1**.<br>After changing the management VLAN, you can manage this CPE only after connecting your computer to the new management VLAN. |
| Trunk Port | A wired LAN port that serves as a trunk port. A trunk port allows all VLANs to pass through. The default trunk port is **PoE/LAN**. |

| Name | Description |
| --- | --- |
| WLAN VLAN ID | Used to set a VLAN ID for the wireless network of this CPE. By default, it is set to **1000**.<br>After the VLAN function is enabled, the WLAN interface is equivalent to an access port, whose PVID is the same as VLAN ID. |
| LAN2 | Used to set a VLAN ID of the Ethernet port of this CPE. By default, it is set to **1**.<br>After the VLAN function is enabled, the Ethernet port is equivalent to an access port, whose PVID is the same as VLAN ID. |
| LAN3 | |
| LAN4 | |

## 5.6.3 Example of configuring VLAN on O6 V3.0

### Networking requirements

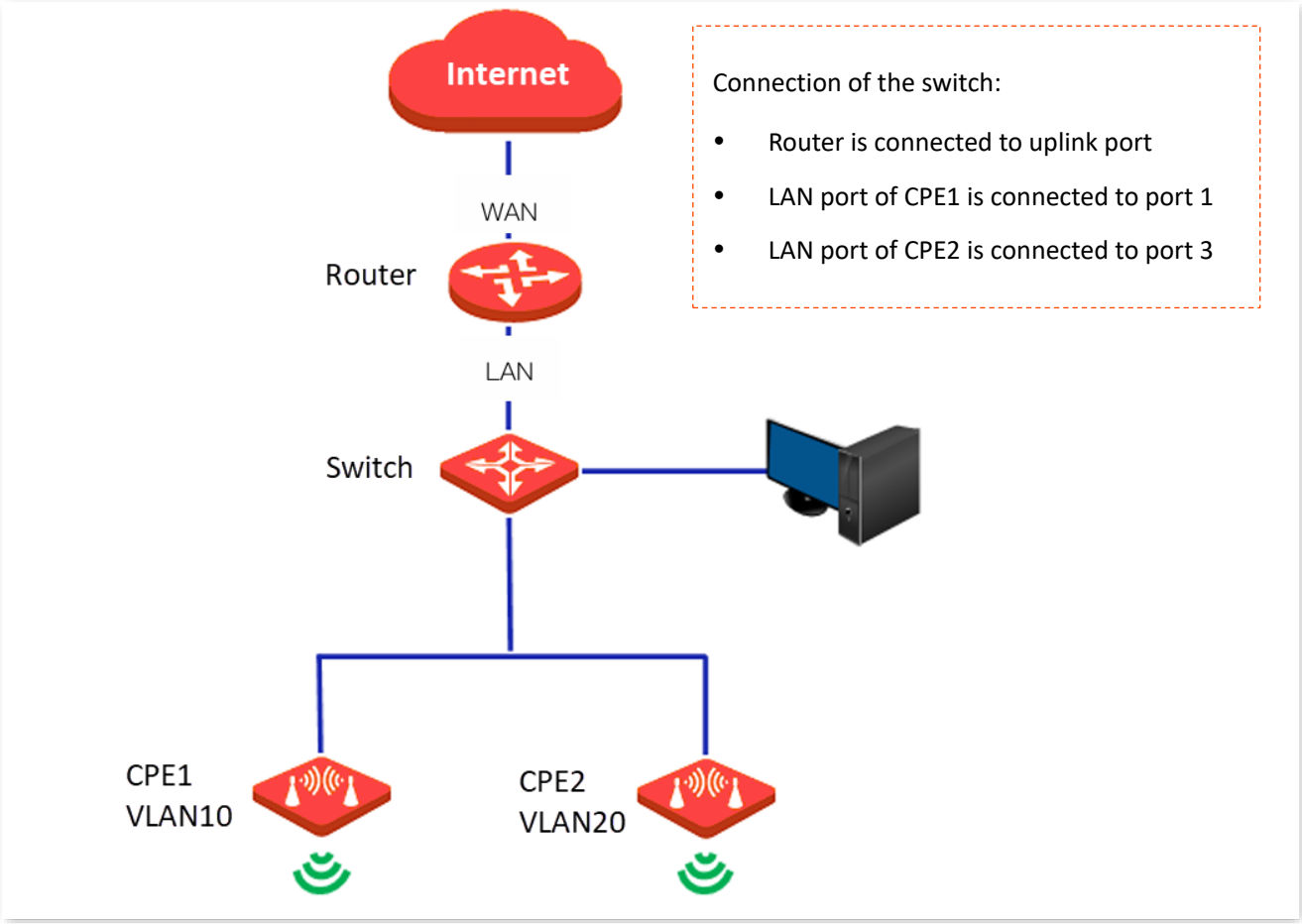
Two communities want to create a separate network with two CPEs and connect to the internet through the same router.

### Solution

Perform the following steps:

- Assign CPE1 to VLAN10, and CPE2 to VLAN20.
- Configure two separate DHCP servers for VLAN10 and VLAN20 on the router that supports IEEE 802.1Q VLAN.

## Network topology




## Configuration procedure

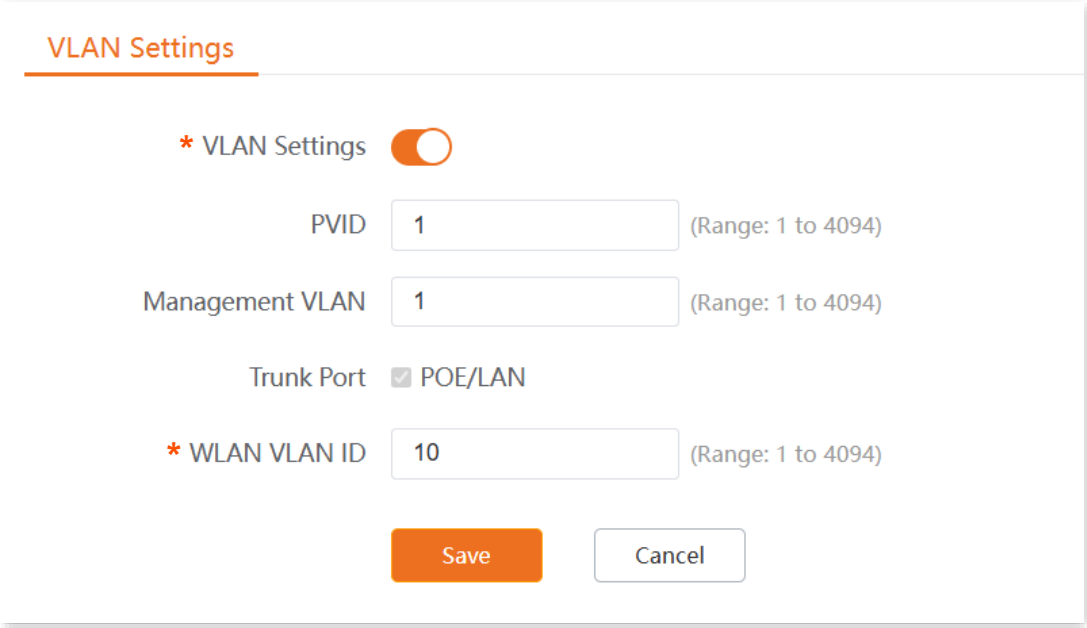
1. Set up the CPE1.

   1) Log in to the web UI of the CPE1, and navigate to **Network** > **VLAN Settings**.

   2) Enable the **VLAN Settings** function.

   3) Configure **WLAN VLAN ID**, which is **10** in this example.

   4) Click **Save**.




5) Click **OK**, and wait until CPE1 completes reboot.

2. Repeat step 1 for CPE2 and set its **WLAN VLAN ID** to **20**.

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

| Port | Type | VLAN ID (Allow Packets) | PVID |
|---|---|---|---|
| Uplink port<br>(Connected to the router) | Trunk | 1, 10, 20 | 1 |
| Port 1<br>(Connected to CPE1) | Trunk | 1, 10 | 1 |
| Port 3<br>(Connected to CPE2) | Trunk | 1, 20 | 1 |

Keep the default settings for other ports not mentioned here. For details, see the user guide for the switch.

4. Set up the router.

1) Enable two DHCP servers on the router, and assign them to VLAN10 and VLAN20 respectively.

2) Configure the QVLAN on the router as shown in the following table.

| Port Connected To | Type | VLAN ID (Allow Packets) | PVID |
|---|---|---|---|
| Switch | Trunk | 10, 20 | 1 |

For details, see the user guide for the router.

**---End**

### Verification

If the router enables two DHCP servers for VLAN10 and VLAN20 respectively, the client connected to the CPE1 obtains an IP address and related parameters from the DHCP server belonging to VLAN10, and the client connected to CPE2 obtains these parameters from the DHCP server belonging to VLAN20.

## 5.7 Network topology

To access the page, log in to the web UI of the CPE and navigate to **Network** > **Network Topology**. Here you can turn network topology on or off. By default, the function is disabled.

After adding the CPE to the project on the Tenda CloudFi Cloud platform, enter the project, navigate to **Network** > **Visualization** > **Network Topology**. If the network topology function is enabled on the CPE, you can see the topology composed of various network devices and CPEs in the project on the page.

# 6 Manage wireless settings

Features available in the CPE may vary by model and software version. CPE availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual CPE experience.

## 6.1 Basic configuration

### 6.1.1 Overview

This module enables you to set basic wireless settings of the CPE, including SSID parameters, network mode, channel, and transmitted power.

#### Broadcast SSID

If broadcast SSID is enabled, nearby wireless clients can detect the SSID. If the function is disabled, the CPE does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network of the SSID. This enhances wireless security to some extent.

However, hackers may still find ways to obtain SSIDs and gain access to target networks.

#### Isolate client

Similar to a VLAN on a wired network, the isolate client function completely isolates all wireless clients connected to the same SSID. Only the wired network connected to the CPE can be accessed. It is suitable for the establishment of public hotspots such as hotels and airports, so that the wireless clients connected can be kept isolated and the wireless network security can be improved.

#### Max. number of clients

You can set the maximum number of clients that can connect to the wireless network corresponding to an SSID. When the number of wireless clients connected to the SSID reaches this value, the wireless network rejects new connection requests from clients. This limit helps balance load among devices.

## Security mode

A wireless network uses radio, which is open to the public, as its data transmission medium. If a 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.

There are various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2.

- **None**

In this mode, any wireless client can connect to the CPE's wireless network. This is not a secure option.

- **WEP**

Wired Equivalent Privacy (WEP) uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. Data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum wireless network throughput of only 54 Mbps. Therefore, this security mode is not recommended.

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

WPA-PSK, WPA2-PSK and Mixed WPA/WPA2-PSK (compatible with WPA-PSK and WPA2-PSK) use a pre-shared key or personal key for authentication only. Data encryption keys are generated by the CPE. 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 CPE, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.

- **WPA and WPA2**

To address the key management weakness of WPA-PSK and WPA2-PSK, the Wi-Fi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate clients and generate root keys to encrypt data, instead of using pre-shared keys that are set manually. The encryption process is the same as WPA-PSK and WPA2-PSK.

WPA and WPA2 use 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.

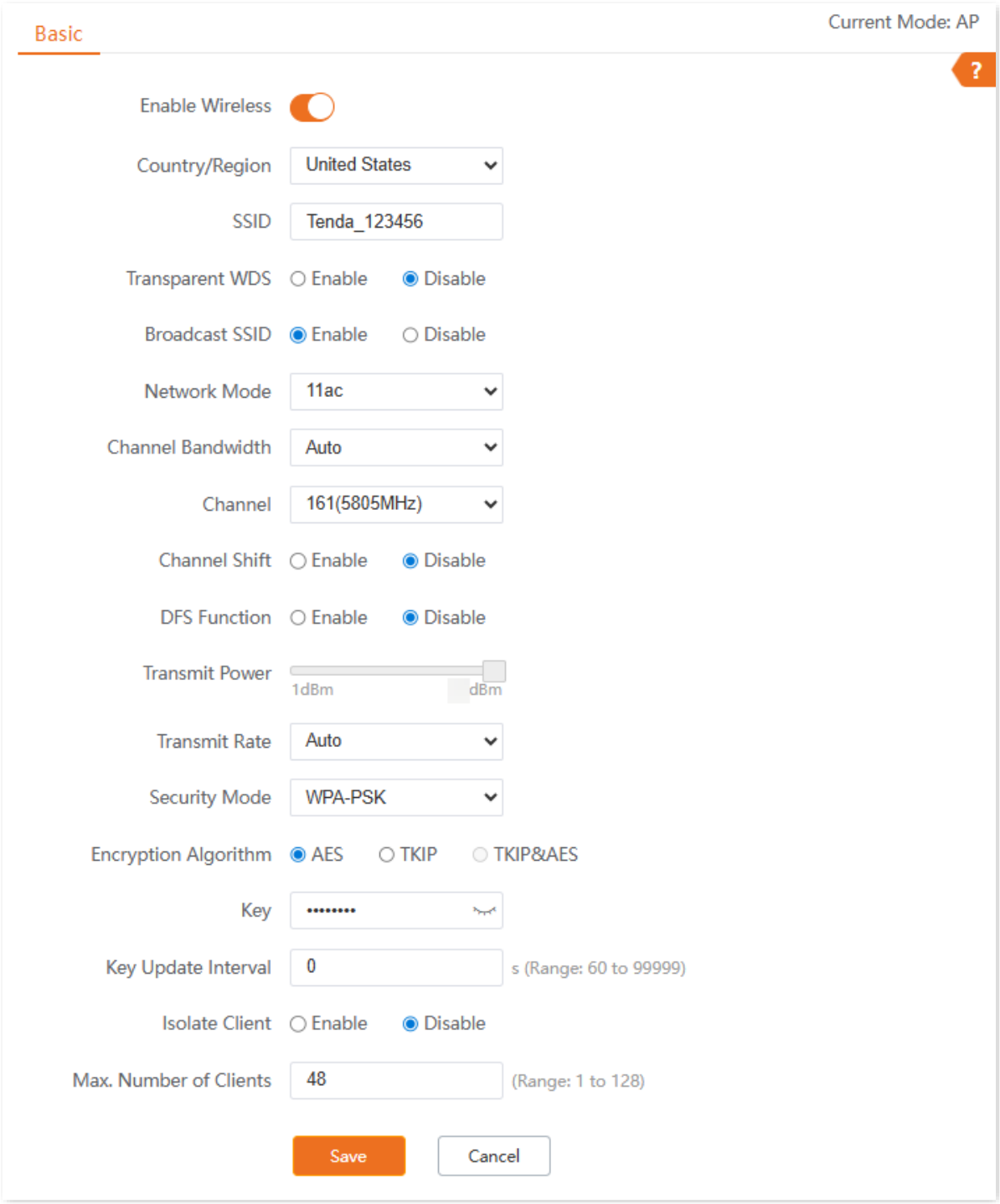
In addition, each time a client connects to an AP that adopts the WPA or WPA2 security mode, the RADIUS server generates a data encryption key and assigns it to the client. This makes it difficult for attackers to obtain the key.

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.

## 6.1.2 Basic wireless settings

To access the page, log in to the web UI of the CPE and navigate to **Wireless** > **Basic**. On this page, you can modify the basic wireless settings of the CPE.

When the CPE works in AP, WISP, or Router mode, the basic wireless settings page is displayed as below.



### Parameters description

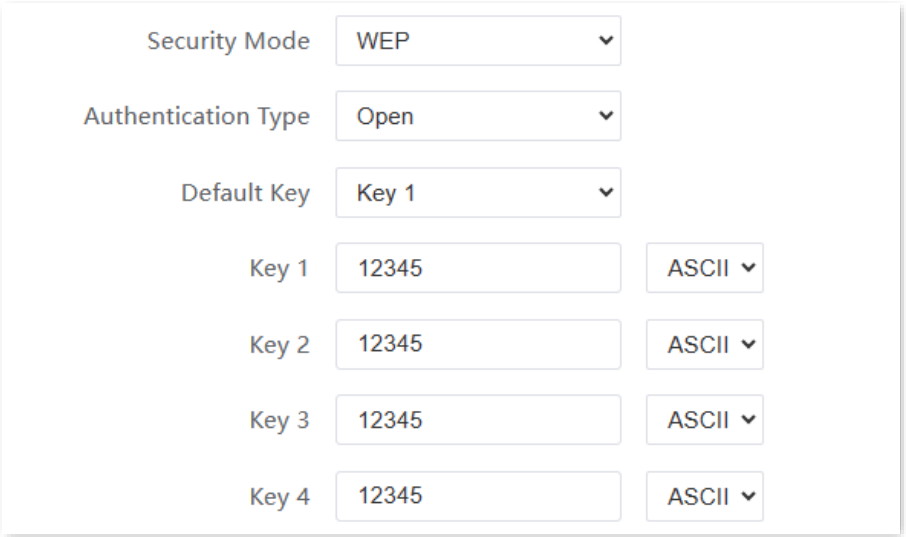
| Name | Description |
| --- | --- |
| Enable Wireless | Specifies whether to enable the wireless function. |
| Country/Region | Specifies the country or region where this CPE is located.<br>You can select the country or region to ensure that this CPE complies with the channel regulations of the country or region. By default, it is set to **China**. |
| SSID | Specifies the name of the wireless network (SSID). You can modify it as required.<br>- For single CPEs, it defaults to **Tenda_*XXXXXX*** (***XXXXXX*** indicates the last six digits of the LAN MAC address).<br>- For CPE kits, it defaults to **Tenda_*XXXXXX*** (*XXXXXX* indicates six random digits). |
| Transparent WDS | It is available when the CPE works in AP mode or Client mode.<br>With this function enabled, the CPE can bridge to CPEs from other manufacturers. Devices connected to the CPE working in Client mode will be displayed on the ARP table of the CPE working in AP mode.<br>TIP<br>Transparent WDS and Transparent Bridge cannot be enabled at the same time. |
| Broadcast SSID | Specifies whether to broadcast the SSID.<br>- **Enable**: When an SSID is broadcast, wireless clients can detect the SSID.<br>- **Disable**: When an SSID is not broadcast, you need to manually enter the SSID to connect to the wireless network of the CPE. |
| Network Mode | Specifies the wireless network mode of the CPE. Only wireless clients supporting the listed network mode can connect to the CPE. |
| Channel Bandwidth | Specifies the bandwidth of the operating channel of the CPE's wireless network.<br>The channel bandwidth varies with different network modes. Select it based on your actual operating environment. **Auto** indicates that the CPE can switch its channel bandwidth based on the ambient environment. |
| Channel | Specifies the channel in which the CPE operates.<br>**Auto** indicates that the CPE automatically changes to the least used channel in the ambient environment to prevent interference. |
| Channel Shift | Specifies whether to enable or disable Channel Shift.<br>With this function enabled, the channel center frequency will shift based on the frequency defined by the IEEE 802.11 standard, so that the CPE can exchange data on channels with less interference.<br>NOTE<br>When the Channel Shift function is enabled, other CPEs that bridge with it should also enable this function, and the offset value must be consistent. Otherwise, the bridging will fail. |

| Name | Description |
| --- | --- |
| Offset Value | Specifies the offset value of the channel center frequency. This parameter is available only when the Channel Shift function is enabled. |
| DFS Function | Specifies whether to enable or disable Dynamic Frequency Selection (DFS).<br>With this function enabled, the CPE automatically detects radar signals. When the CPE detects radar signals in the same frequency as the CPE itself, the CPE will automatically switch to another frequency to avoid interference with the radar system. |
| Transmit Power | Specifies the transmit power of the CPE.<br>A higher number indicates wider Wi-Fi coverage. Setting a proper transmit power helps improve the performance and security of the wireless network. |
| Transmit Rate | Specifies wireless transmission rate of the CPE. **Auto** is recommended.<br>The maximum negotiation rate varies with different channel bandwidths and network modes. When **Auto** is selected, the CPE will be adjusted to the maximum transmit rate under the corresponding network mode. |
| Security Mode | There are various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2. |
| Isolate Client | - **Enable**: Clients connected to this wireless network cannot communicate with each other, which improves the wireless network security.<br>- **Disable**: Clients connected to this wireless network can communicate with each other. It is set to **Disable** by default. |
| Max. Number of Clients | Specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID.<br>If the number is reached, the wireless network rejects new connection requests from clients. |

- **None**

In this mode, the wireless network is not protected by password. This is not a secure option.

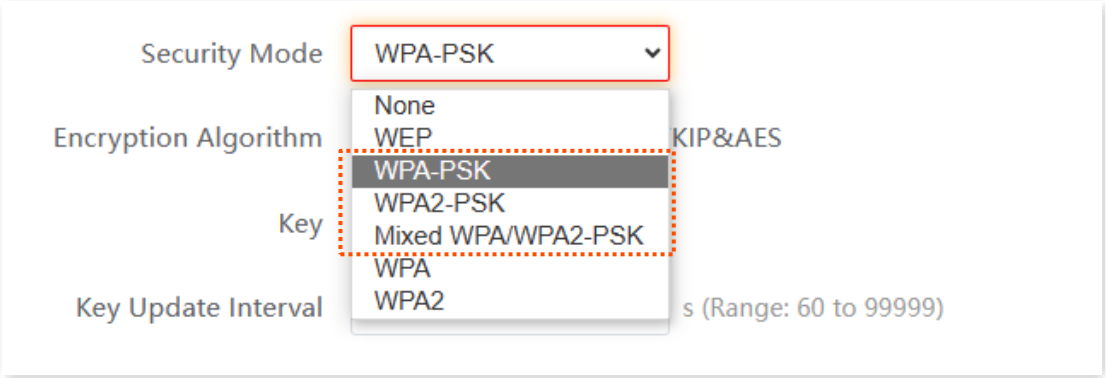
- **WEP**




**Parameters description**

| Name | Description |
|---|---|
| Encryption Type | Specifies the encryption type for the WEP security mode. Values:<br>- **Open**: A wireless client can connect to the wireless network of the selected SSID without being authenticated, and data exchanged between the client and the network is encrypted using WEP.<br>- **Shared**: A shared key is used for authentication and data is encrypted using WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network of the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key. |
| Default Key | Specifies the WEP key for the Open or Shared encryption type.<br>For example, if **Default Key** is set to **Key 2**, a wireless client can connect to the wireless network of the selected SSID only with the password specified by **Key 2**. |
| Key 1/2/3/4 | Specifies the WEP key. You can enter four keys, but only the one specified as Default Key takes effect.<br>Supported formats:<br>- **ASCII**: Enter 5 or 13 ASCII characters for the key.<br>- **Hex**: Enter 10 or 26 hexadecimal characters (0-9, a-f, and A-F) for the key. |

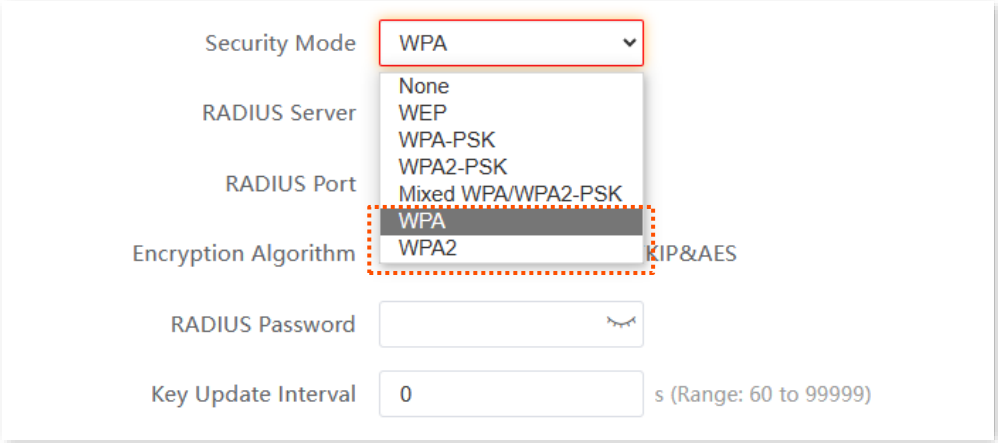
- **WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK**




### Parameters description

| Name | Description |
|---|---|
| Security Mode | Specifies the security mechanism that protects the wireless network. Values:<br>– **WPA-PSK**: The wireless network of the selected SSID is encrypted using WPA-PSK.<br>– **WPA2-PSK**: The wireless network of the selected SSID is encrypted using WPA2-PSK.<br>– **Mixed WPA/WPA2-PSK**: Wireless clients can connect to the wireless network of the selected SSID using either WPA-PSK or WPA2-PSK. |
| Encryption Algorithm | Specifies the encryption algorithm corresponding to the selected security mode. Values:<br>– **AES**: Advanced Encryption Standard.<br>– **TKIP**: Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless speed of the CPE is limited to 54 Mbps.<br>– **TKIP&AES**: Both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network of the selected SSID using TKIP or AES.<br>TIP<br>If **Security Mode** is set to **WPA-PSK**, this parameter can be set to **AES** or **TKIP**. If it is set to **WPA2-PSK** or **Mixed WPA/WPA2-PSK**, this parameter can be set to **AES**, **TKIP**, or **TKIP&AES**. |
| Key | Specifies a pre-shared WPA key. |
| Key Update Interval | 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 WPA key is not updated. |

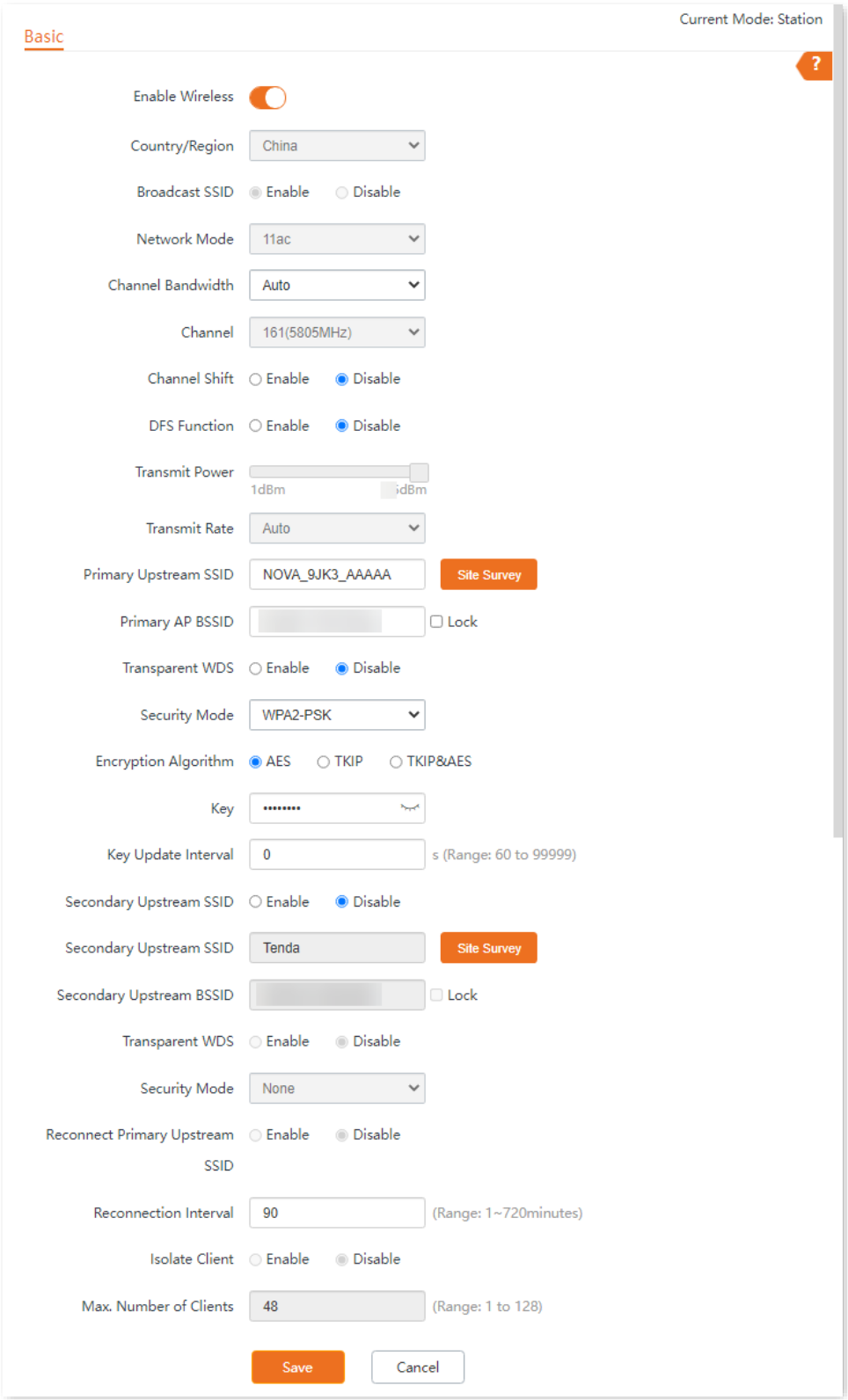
- **WPA, WPA2**




**Parameters description**

| Name | Description |
|---|---|
| Security Mode | Specifies the security mechanism that protects the wireless network. Values:<br>– **WPA**: The wireless network of the selected SSID is encrypted using WPA.<br>– **WPA2**: The wireless network of the selected SSID is encrypted using WPA2. |
| RADIUS Server | Specifies the IP address of the RADIUS server for client authentication. |
| RADIUS Port | Specifies the port number of the RADIUS server for client authentication. |
| RADIUS Password | Specifies the shared key of the RADIUS server for client authentication. |
| Encryption Algorithm | Specifies the encryption algorithm corresponding to the selected security mode. Values:<br>– **AES**: Advanced Encryption Standard.<br>– **TKIP**: Temporal Key Integrity Protocol.<br>– **TKIP&AES**: Both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network of the selected SSID using TKIP or AES. |
| Key Update Interval | 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 WPA key is not updated. |

When the CPE works in Client or Universal Repeater mode, the basic wireless settings page is displayed as below.




Parameters on the **Basic** page vary with different modes. Refer to the actual web UI.

The following table describes parameters for the CPE working in Client mode. For other parameters, see Parameter description of AP mode.

### Parameters and buttons description

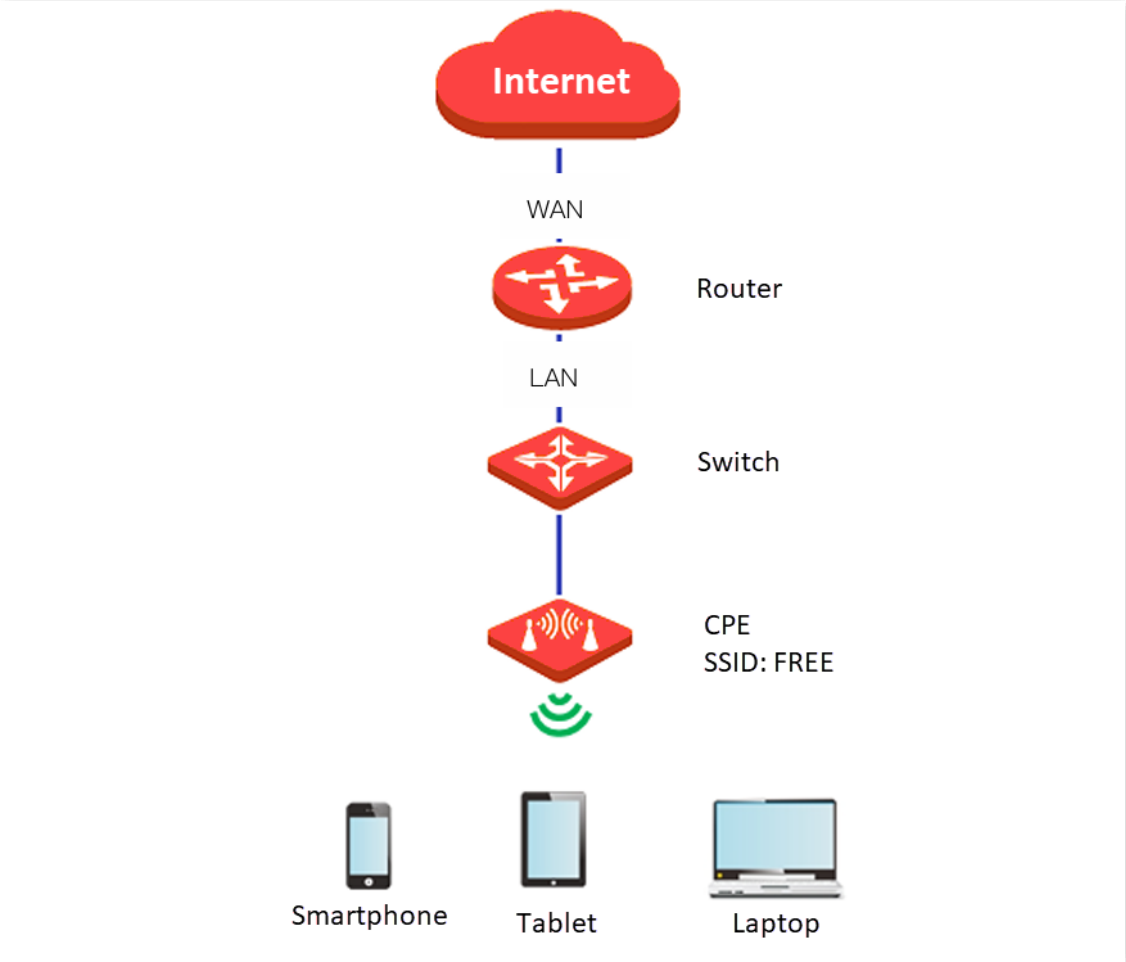
| Name | Description |
| --- | --- |
| Primary Upstream SSID | Specifies the SSID of the primary upstream wireless network that the CPE connects to.<br>After bridging succeeds, the SSID of the primary upstream wireless network will automatically populate. |
| Primary AP BSSID | Specifies the MAC address of the primary upstream wireless network.<br>After bridging succeeds, the MAC address of the primary upstream wireless network will automatically populate. |
| Lock | Used to lock the upstream wireless network.<br>With this function enabled, the CPE can only connect to the wireless network with the current MAC address, and cannot connect to other upstream APs with the same Wi-Fi name. |
| Secondary Upstream SSID | Specifies the SSID of the secondary upstream wireless network that the CPE connects to.<br>With this function enabled, if the CPE fails to connect to the primary upstream SSID, it will automatically connect to the secondary upstream SSID. |
| Secondary Upstream BSSID | Specifies the wireless MAC address of the secondary upstream wireless network. |
| Reconnect Primary Upstream SSID | Used to reconnect to the primary upstream wireless network.<br>With this function enabled, after connecting the secondary upstream SSID, the CPE tries to reconnect to the primary upstream SSID at intervals of the reconnection interval that you configure. |
| Reconnection Interval | Specifies the interval at which the CPE tries to reconnect to the primary upstream SSID when it is connected to the secondary upstream SSID. |
| Site Survey | Used to refresh the available wireless networks and select the one for connection. |

## 6.1.3 Set up a non-encrypted wireless network

### Networking requirements

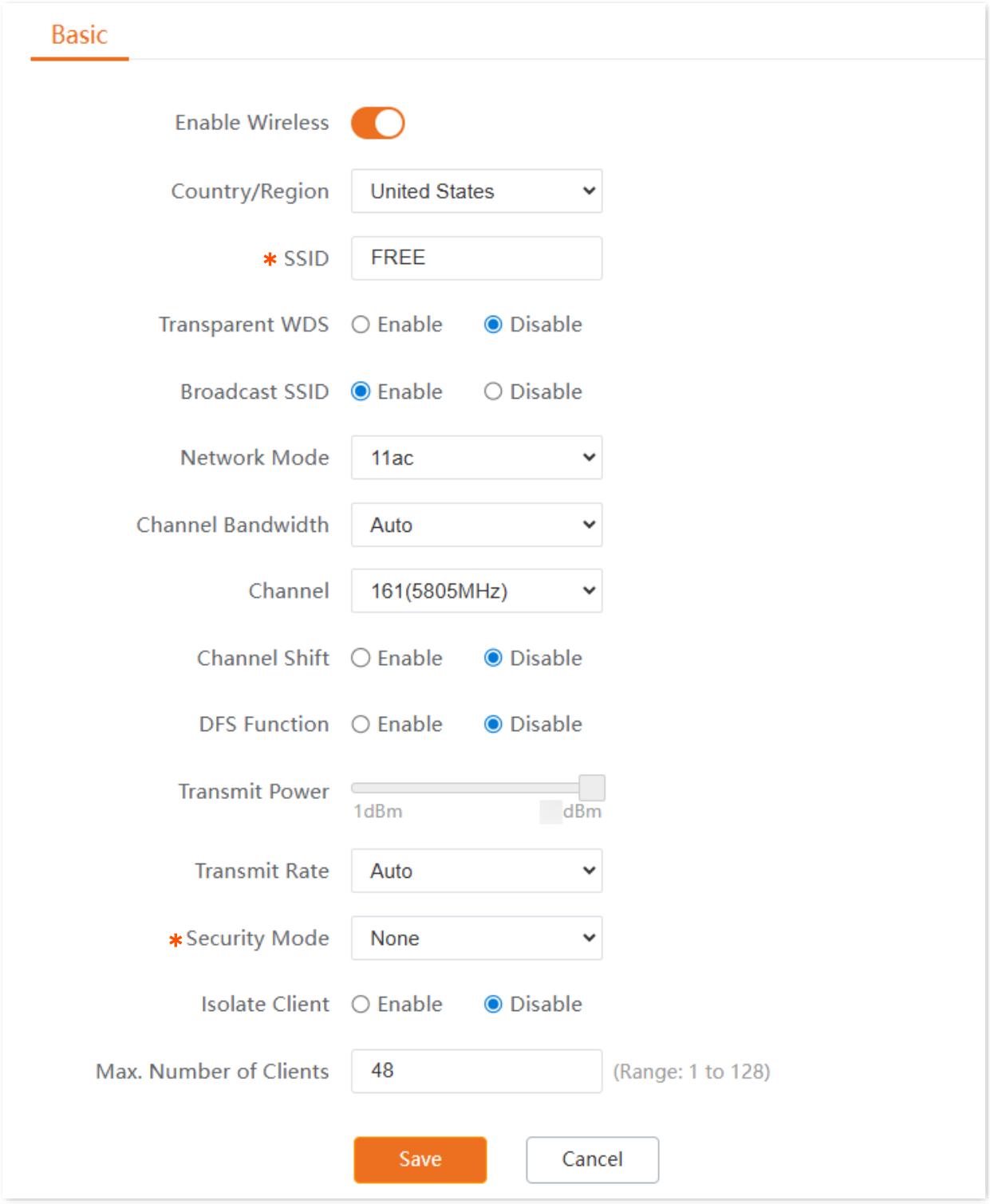
A community uses the CPE to deploy its network for CCTV surveillance. It requires that the SSID is FREE and there is no Wi-Fi password.

### Network topology




### Configuration procedure

1. Log in to the web UI of the CPE.
2. Navigate to **Wireless** > **Basic**.
3. Set **SSID** to **FREE**.
4. Set **Security Mode** to **None**.
5. Click **Save**.




**---End**

## Verification

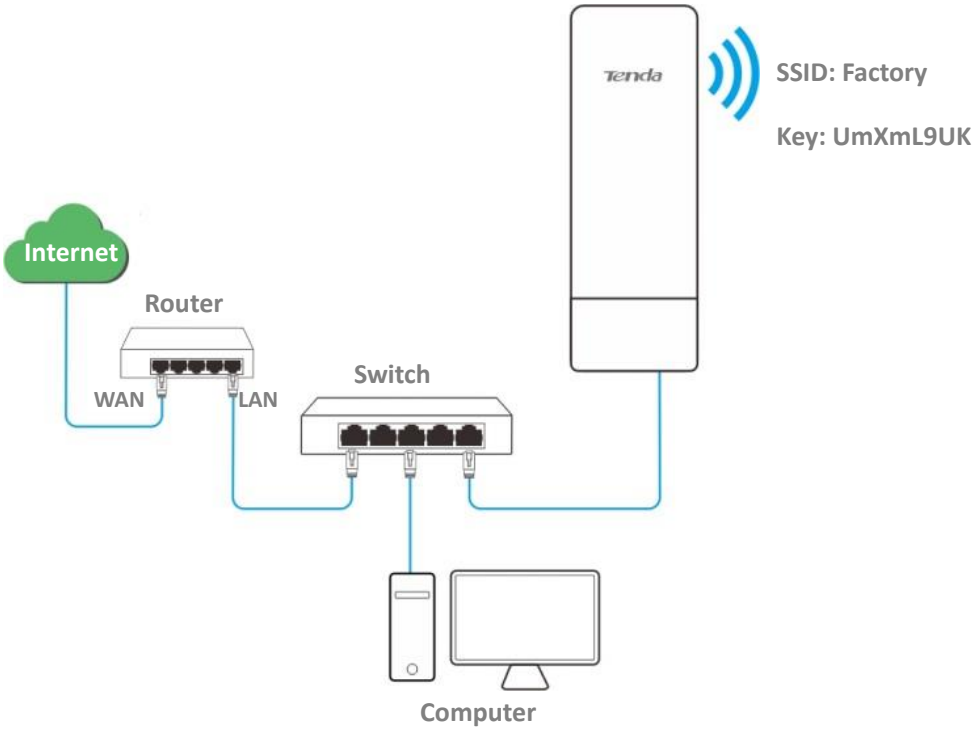
Wi-Fi-enabled devices can connect to the wireless network whose SSID is **FREE** without a password.

## 6.1.4 Set up a wireless network encrypted using WPA2-PSK

### Networking requirements

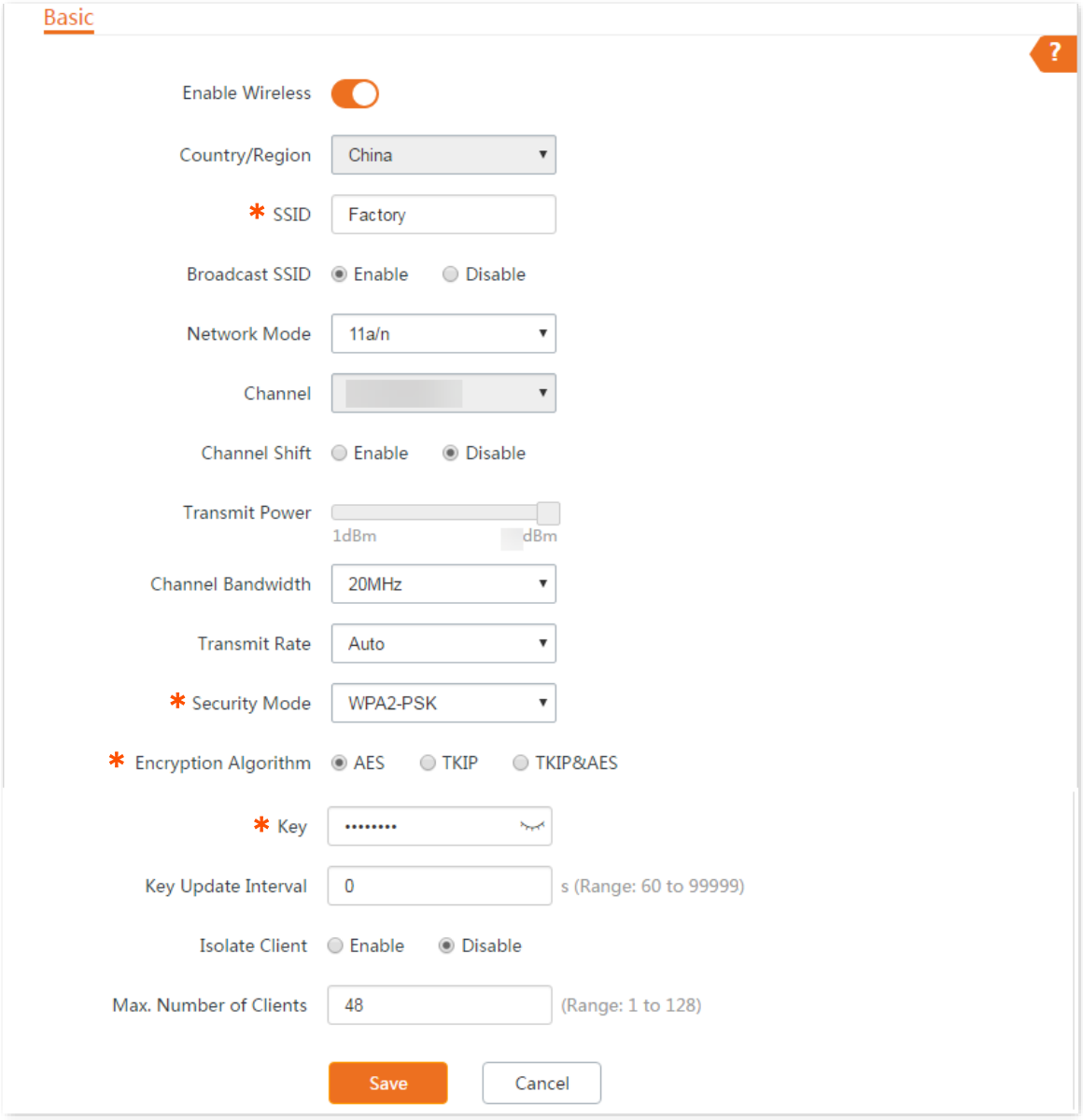
A factory uses CPEs to set up a wireless network. It requires that the wireless network has a certain level of security. In this case, WPA2-PSK mode is recommended.

### Network topology




### Configuration procedure

1. Log in to the web UI of the CPE.
2. Navigate to **Wireless** > **Basic**.
3. Set **SSID** to **Factory**.
4. Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.
5. Set **Key** to **UmXmL9UK**.
6. Click **Save**.




**---End**

## Verification

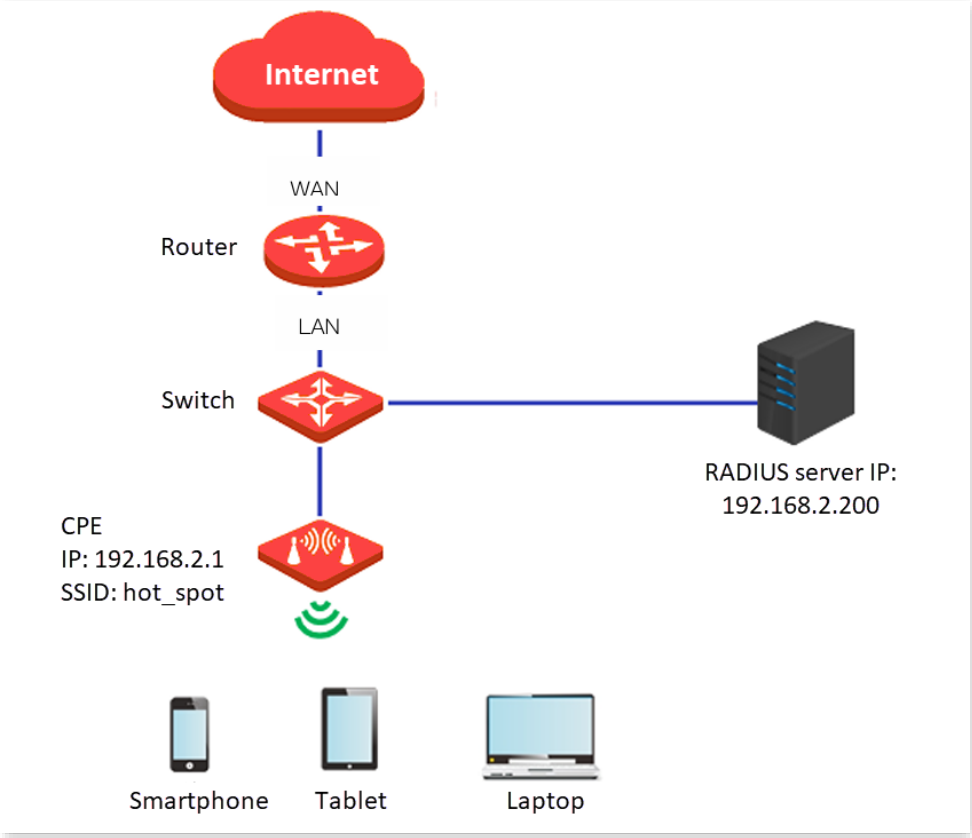
Wi-Fi-enabled devices can connect to the Wi-Fi named **Factory** with the password **UmXmL9UK**.

## 6.1.5 Set up a wireless network encrypted using WPA or WPA2

### Networking requirements

A highly secure wireless network is required and a RADIUS server is available. In this case, WPA or WPA2 mode is recommended.

### Network topology




### Configuration procedure

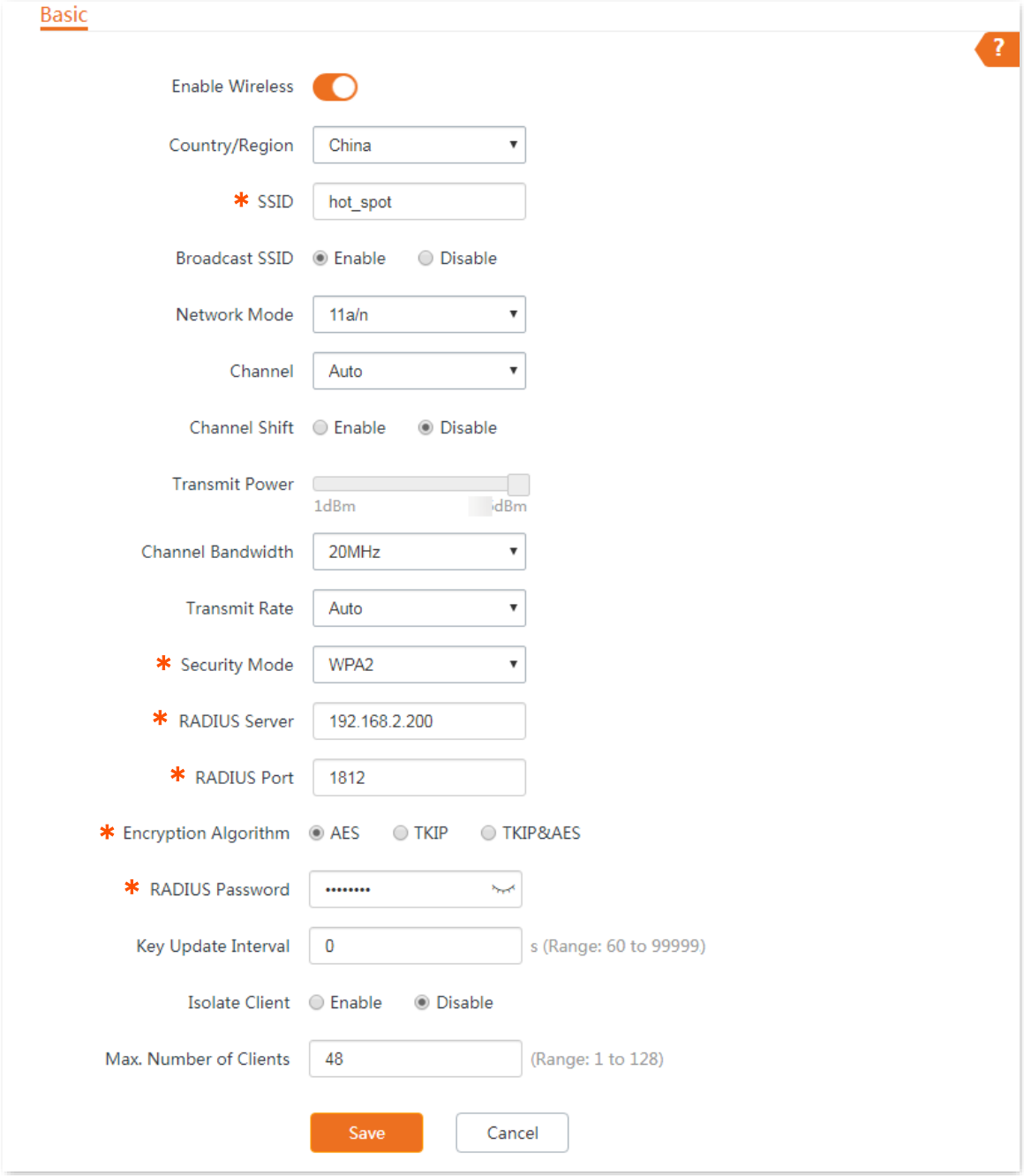
#### I. Configure the CPE

Assume that:

- IP address of the RADIUS server: **192.168.2.200**
- RADIUS Password: **UmXmL9UK**
- Authentication port: **1812**
- SSID of the CPE: **hot_spot**
- Security mode: **WPA2**
- Encryption algorithm: **AES**

1. Log in to the web UI of the CPE, and navigate to **Wireless** > **Basic**.

2. Set **SSID** to **hot_spot**.
3. Set **Security Mode** to **WPA2**.
4. Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Password** to **192.168.2.200**, **1812**, and **UmXmL9UK** respectively.
5. Set **Encryption Algorithm** to **AES**.
6. Click **Save**.




**---End**

## II. Configure the RADIUS server

Windows 2016 is used as an example to describe how to configure the RADIUS server.

1. Install **Active Directory Certificate Services** and **Network Policy and Access Services**, and deploy the certificate.

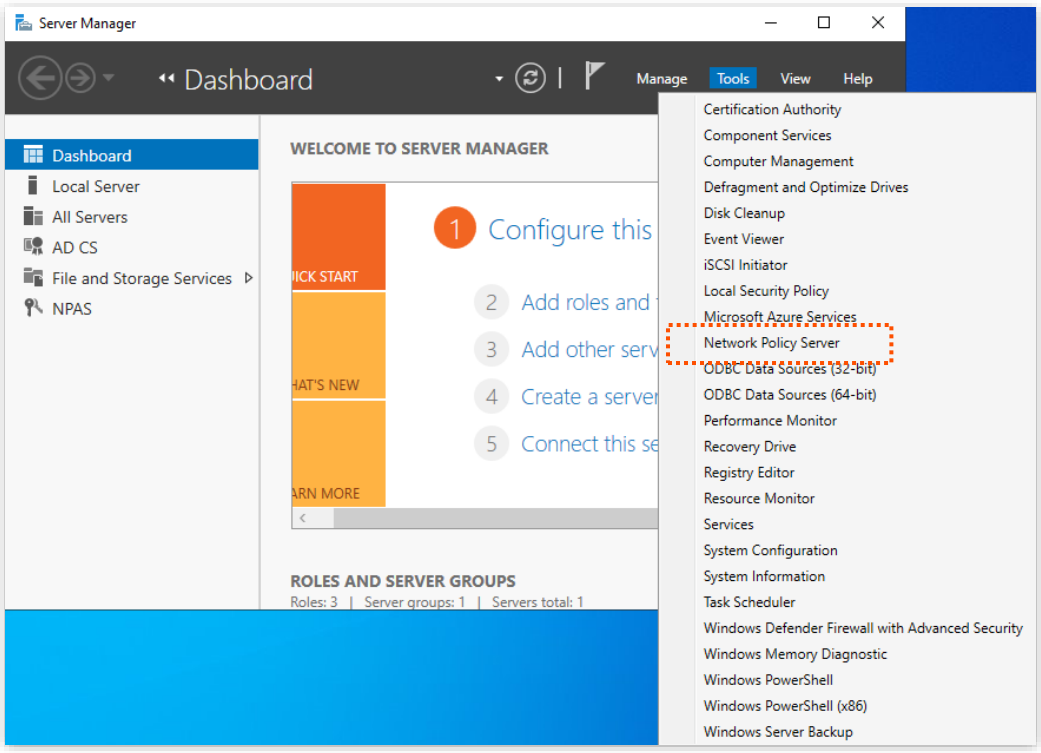
   1) On the **Start** > **Server Manager** > **Dashboard** page, navigate to **Add roles and features** > **Server Selection** > **Server Roles**, and tick the **Active Directory Certificate Services**.

   2) According to the operation wizard, install the **Certification Authority** of **Active Directory Certificate Services** and **Network Policy and Access Services**.

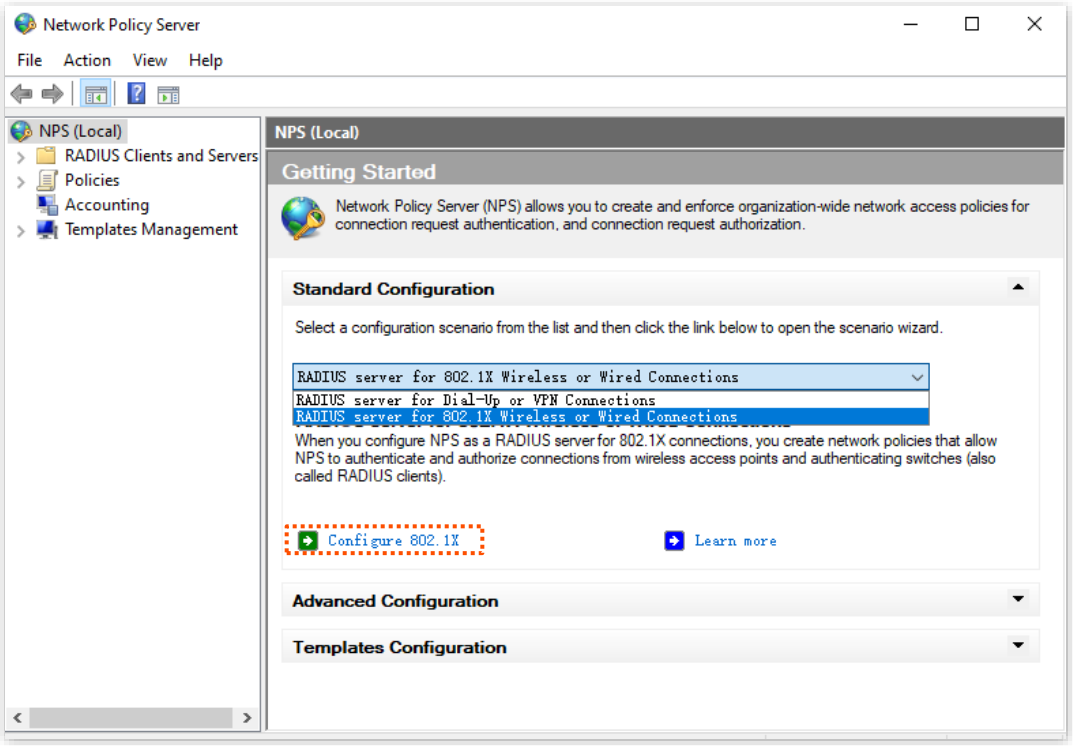
   3) After the service installation is completed, click  in the upper right corner and follow the prompts to deploy the certificate.

2. Configure 802.1X.

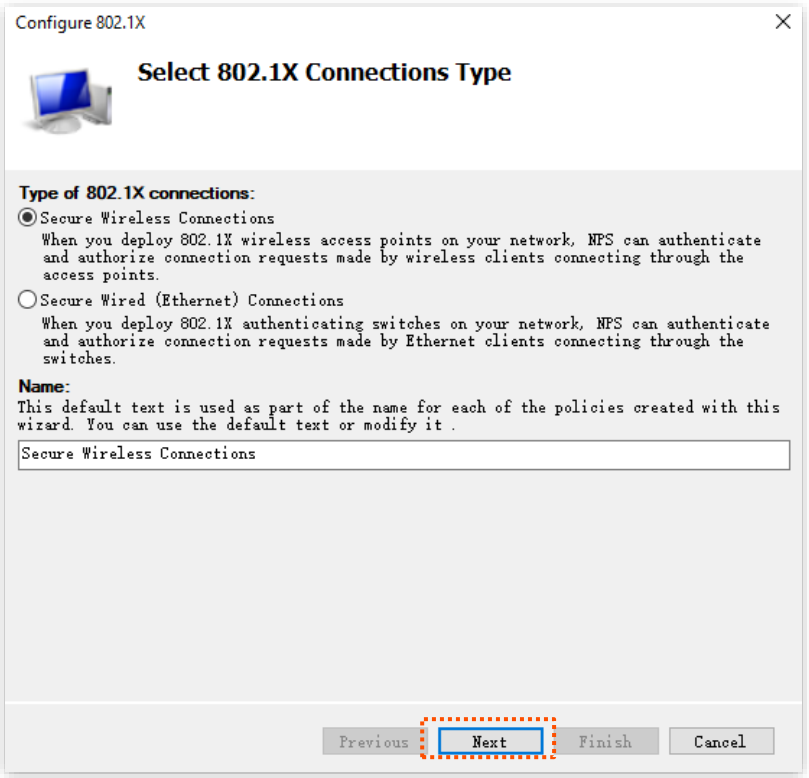
   1) Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, and click **Network Policy Server**.




   2) Select **RADIUS server for 802.1X Wireless or Wired Connection** from **Standard Configuration** and click **Configure 802.1X**.

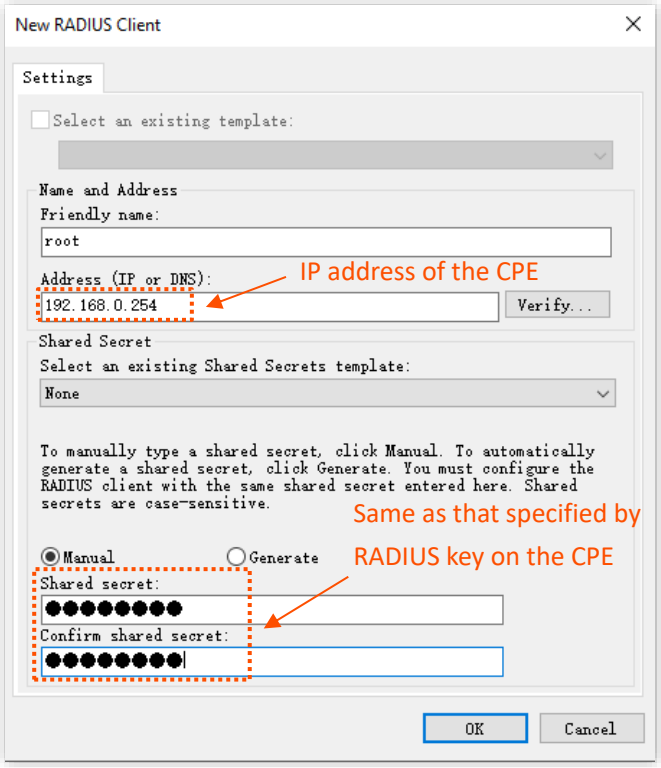



**3)** Select **Secure Wireless Connections** for **Type of 802.1X connections**. Modify the name as required, which is **Secure Wireless Connections** in this example, and click **Next**.

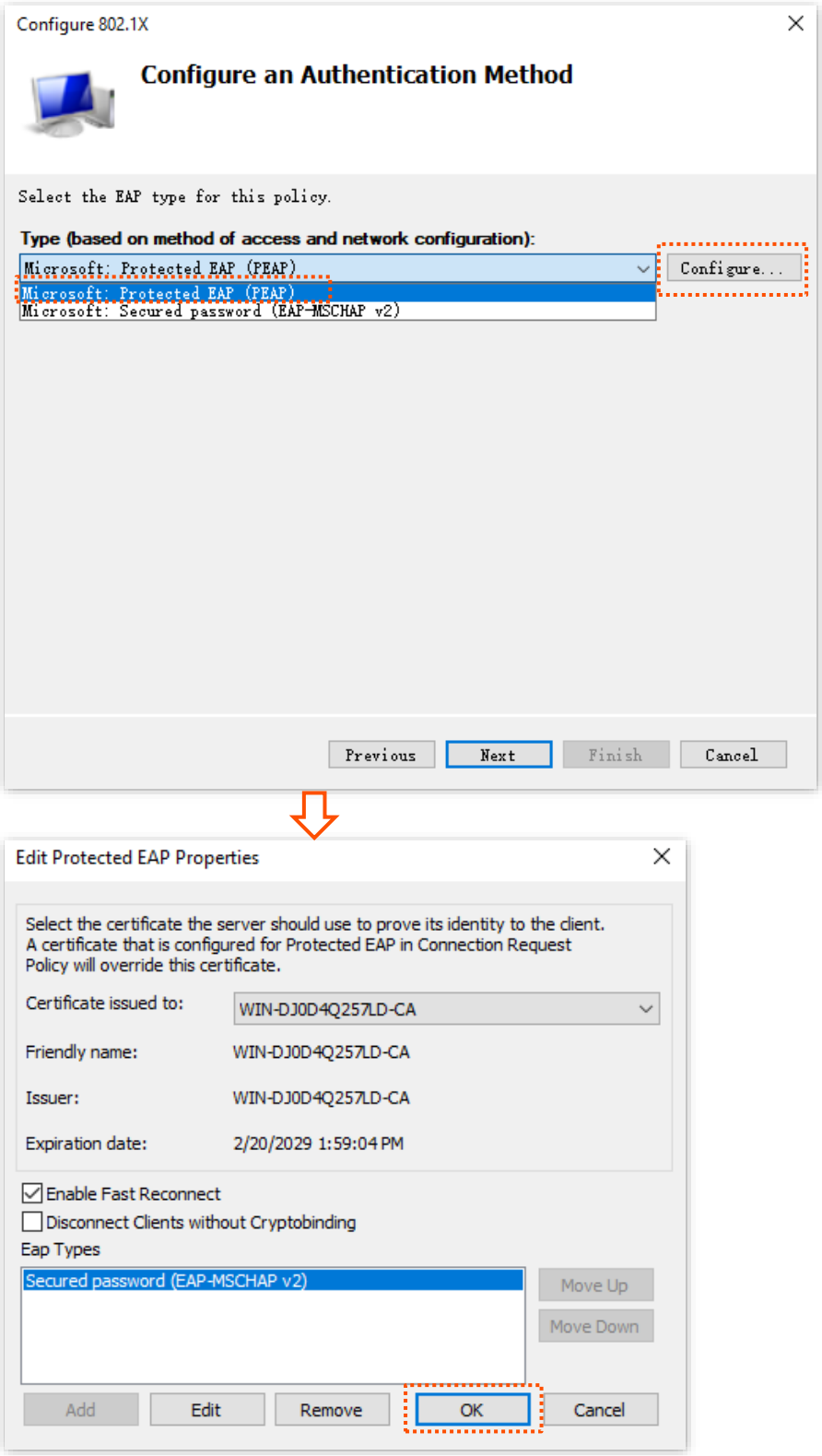



**4)** On the **Specify 802.1X Switches** page, click **Add**.

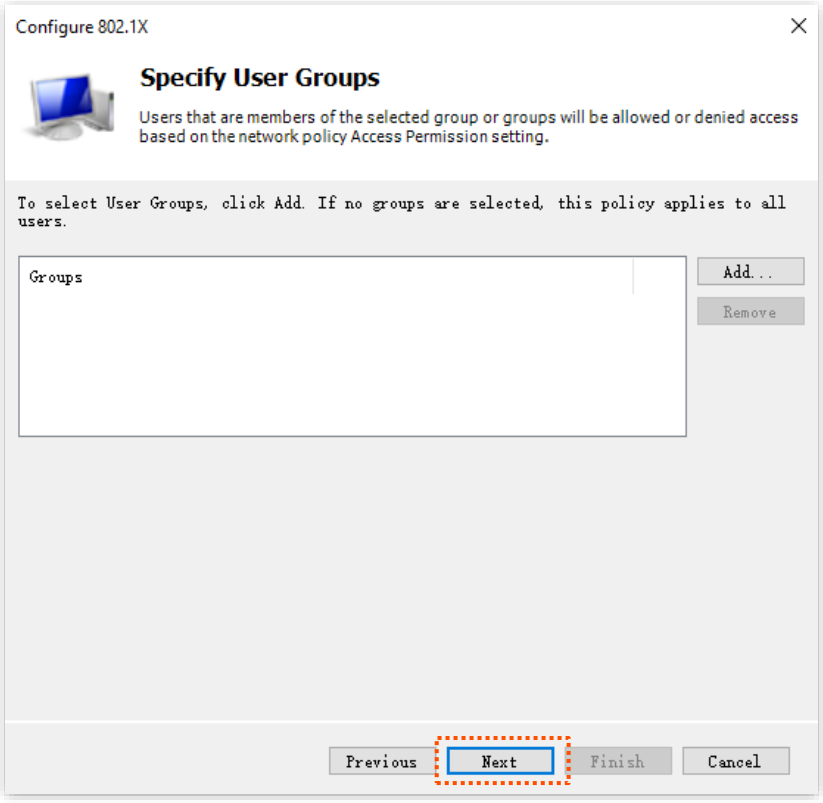
5) Set a RADIUS client name (which can be the name of the CPE) and the IP address of the CPE. Enter **UmXmL9UK** in the **Shared secret** and **Confirm shared secret** text boxes, and click **OK**.



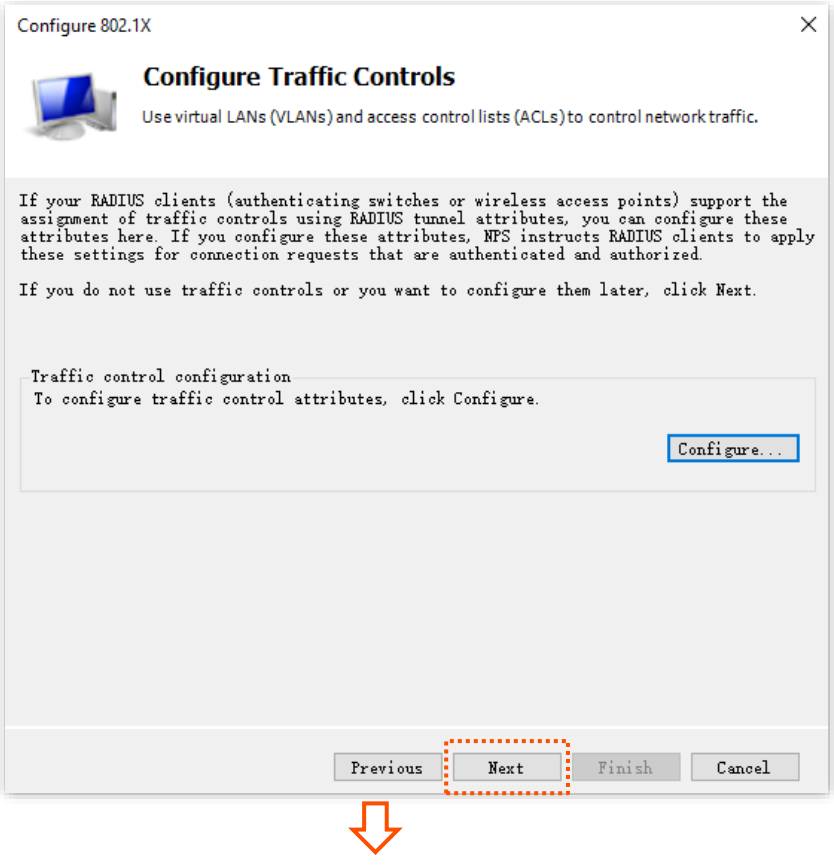

6) Select **Microsoft: Protected EAP (PEAP)** from **Type**, and click **Configure**. Select the certificate deployed in the certificate authority in the previous step, click **OK**, and click **Next** after the configuration is completed.

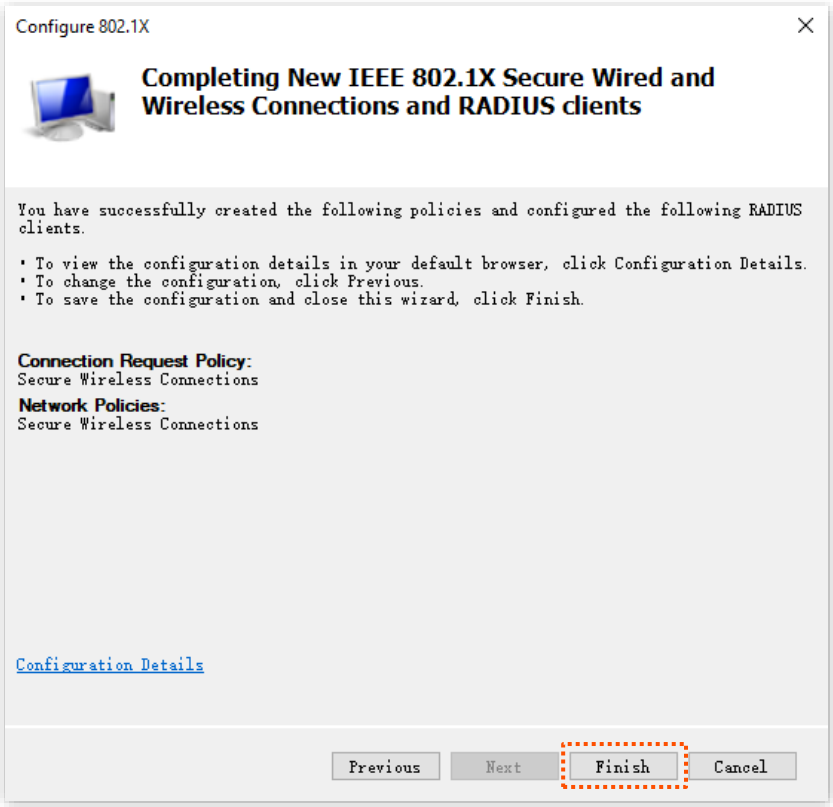

Configure 802.1X
Configure an Authentication Method
Select the EAP type for this policy.
Type (based on method of access and network configuration):
Microsoft: Protected EAP (PEAP)
Configure...
Microsoft: Protected EAP (PEAP)
Microsoft: Secured password (EAP-MSCHAP v2)
Previous
Next
Finish
Cancel
Edit Protected EAP Properties
Select the certificate the server should use to prove its identity to the client.
A certificate that is configured for Protected EAP in Connection Request
Policy will override this certificate.
Certificate issued to:
WIN-DJ0D4Q257LD-CA
Friendly name:
WIN-DJ0D4Q257LD-CA
Issuer:
WIN-DJ0D4Q257LD-CA
Expiration date:
2/20/2029 1:59:04 PM
Enable Fast Reconnect
Disconnect Clients without Cryptobinding
Eap Types
Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add
Edit
Remove
OK
Cancel

7) Click **Next** on the **Specify User Groups** page.




8) On the **Configure Traffic Controls** page, configure the parameters as required, click **Next**, and click **Finish**.



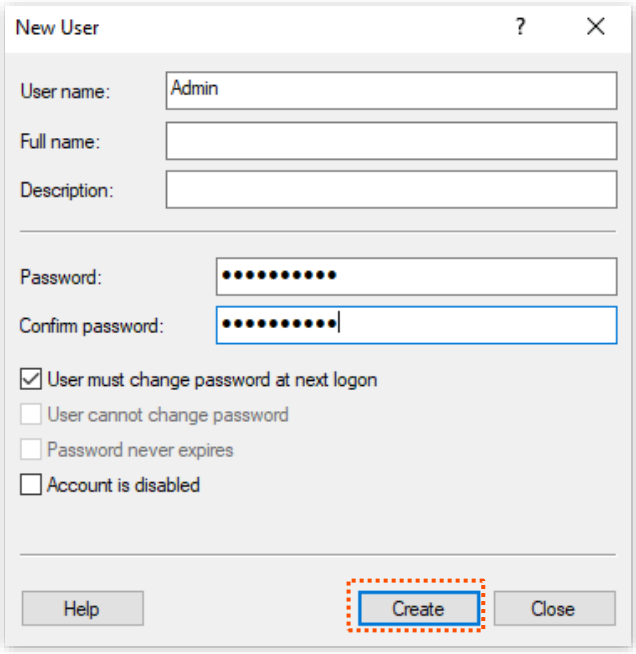



3. Configure the user and user group.

   1) Create a user.

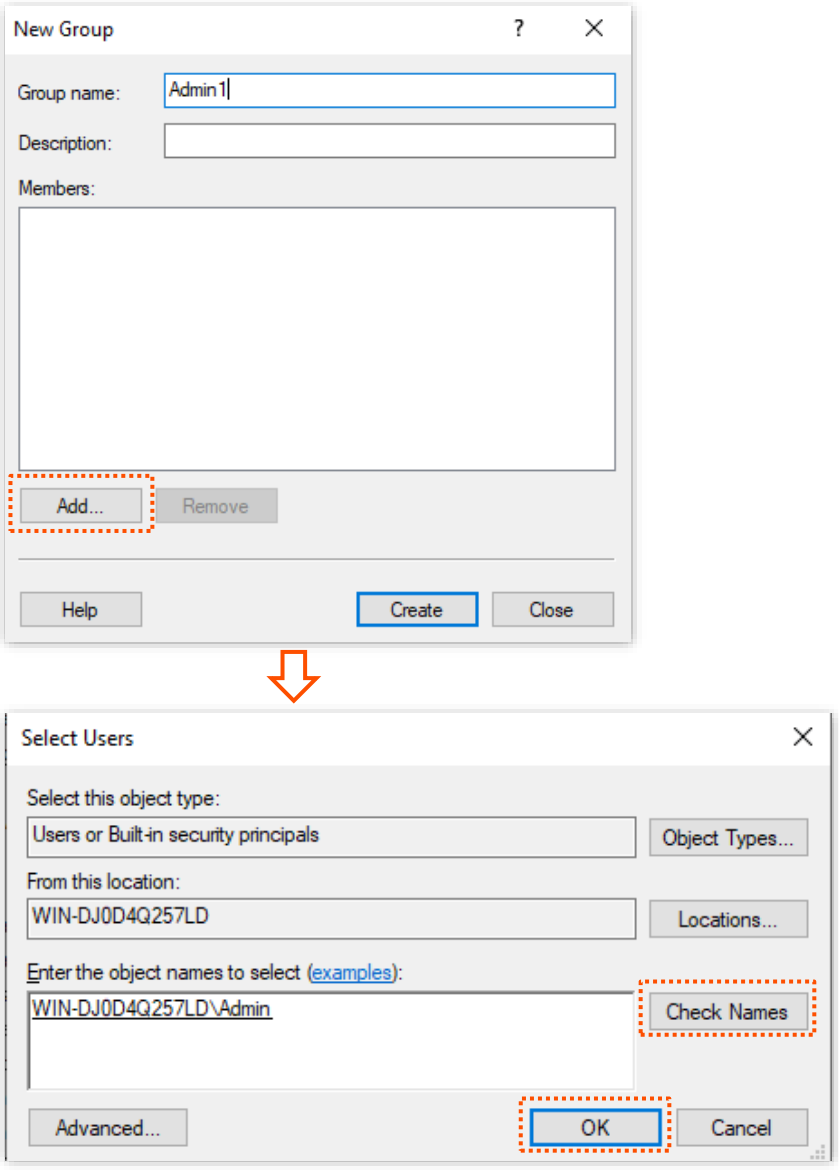
      Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, click **Computer Management**, and double-click **Local Users and Groups**.

      Right-click **Users**, and select **New User**. Enter the user name and password, which are **Admin** (user name) and **JohnDoe123** (password) in this example. And click **Create**.



2) Create a user group.

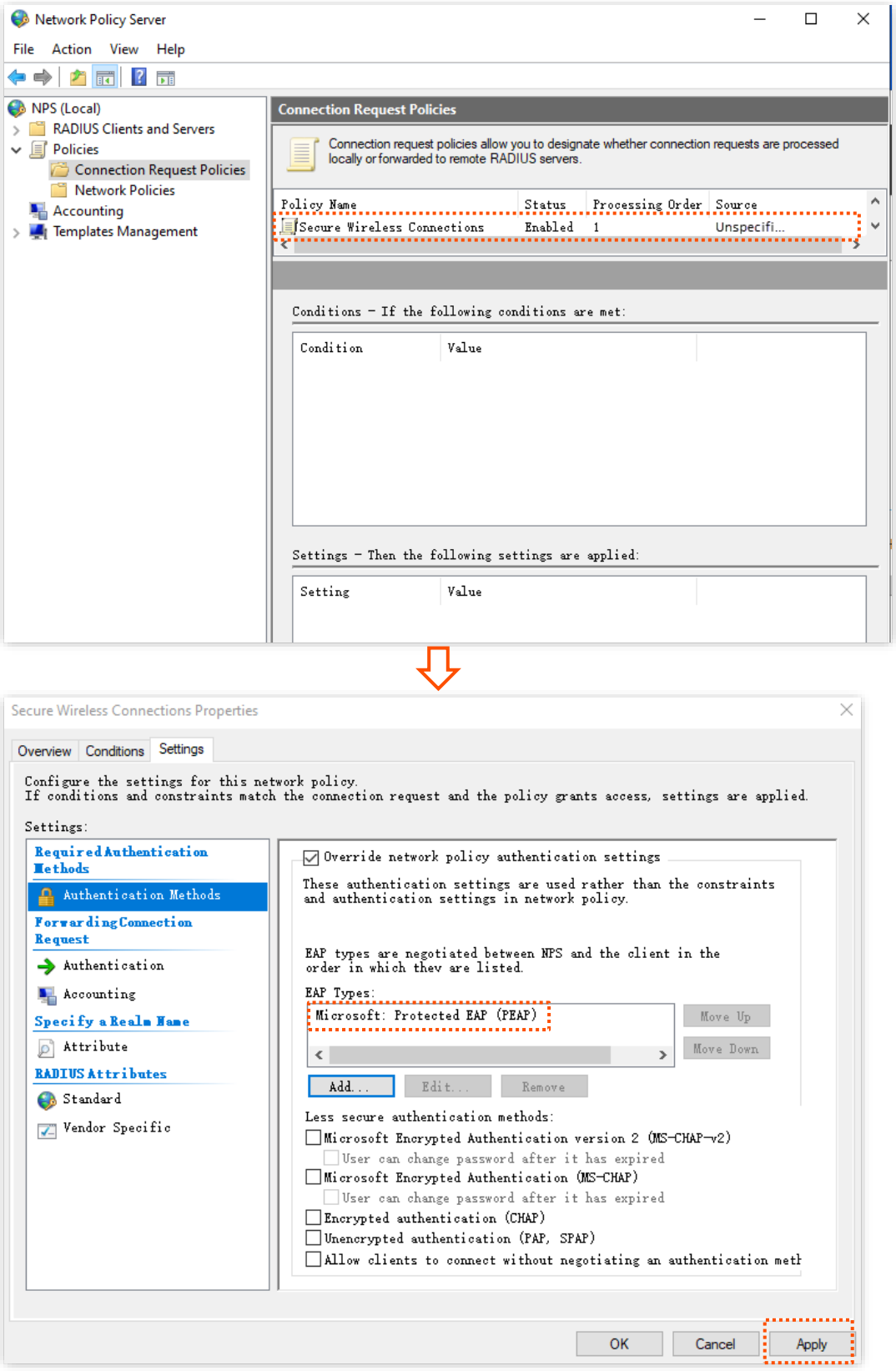
Right-click **Groups**, and select **New Group**. Set **Group name**, which is **Admin1** in this example, and click **Add**. In the **Enter the object names to select** column, enter the created user name, click **Check Names**, and click **OK**. In the **New Group** window, click **Create**.




4. Configure the policies.

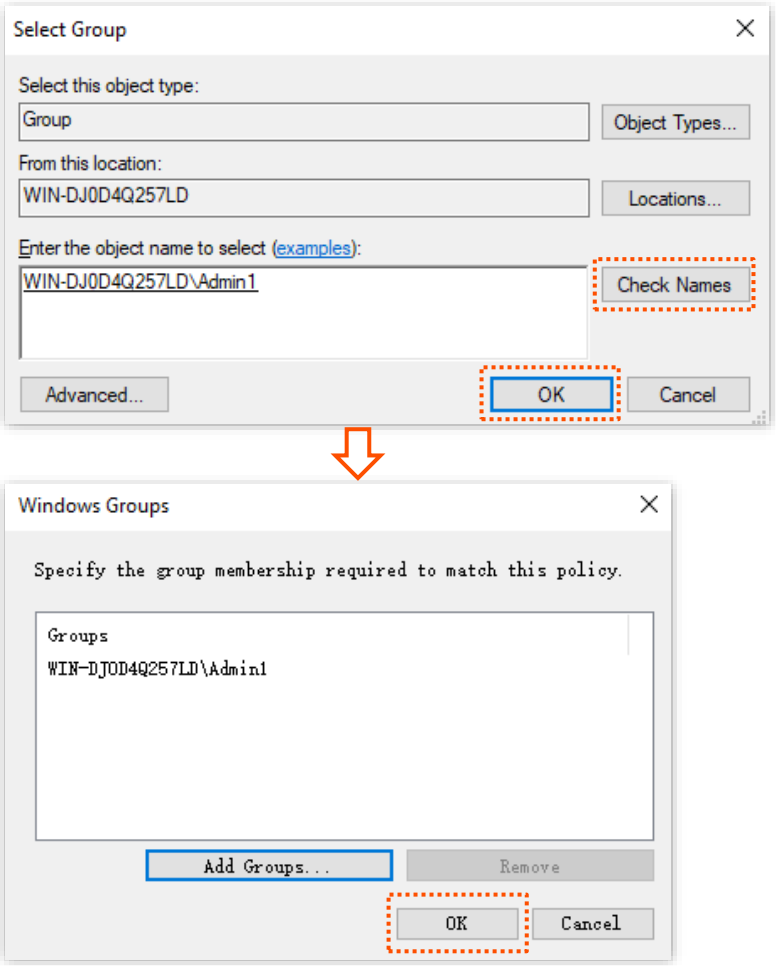
1) Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, click **Network Policy Server**, and double-click **Policies**.

2) Click **Connection Request Policies** and double-click **Secure Wireless Connections**. On the **Secure Wireless Connections Properties** window, click **Settings** and tick **Override network policy authentication settings**. Click **Add**, add **Microsoft: Protected EAP (PEAP)** as **EAP Types**, and click **Apply**.




**3)** Click **Network Policies** and double-click **Secure Wireless Connections**. On the **Secure Wireless Connections Properties** window, click **Conditions**, and click **Add**.

Add the **Windows Groups**, enter the created user group, click **Check Names**, click **OK**, then click **OK**, and click **Apply**.



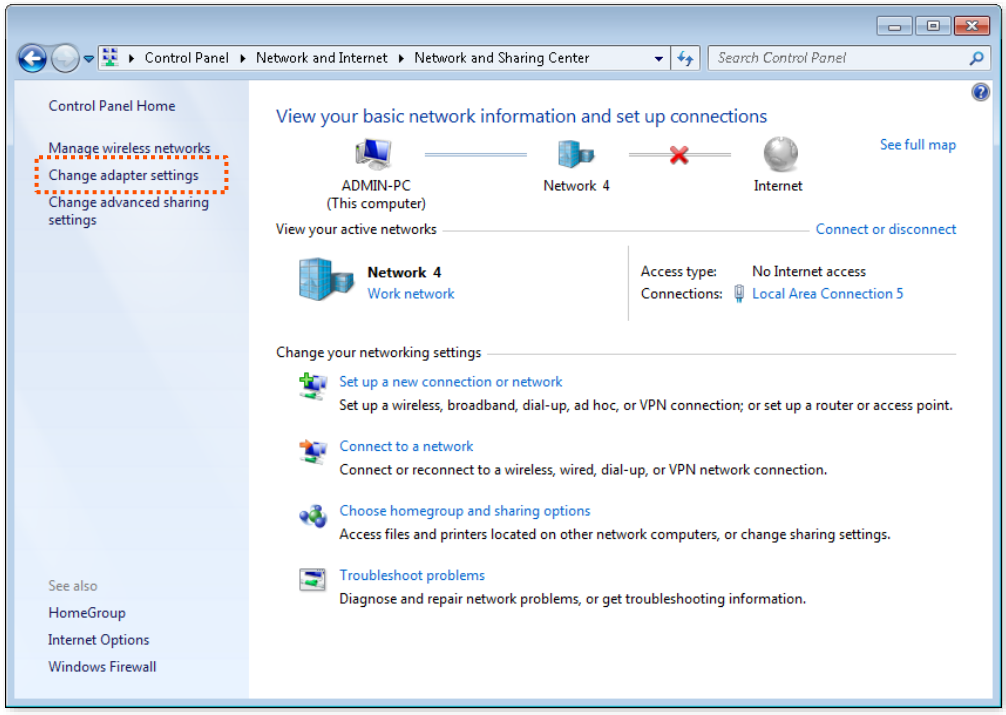

**---End**

## III. Configure your wireless device

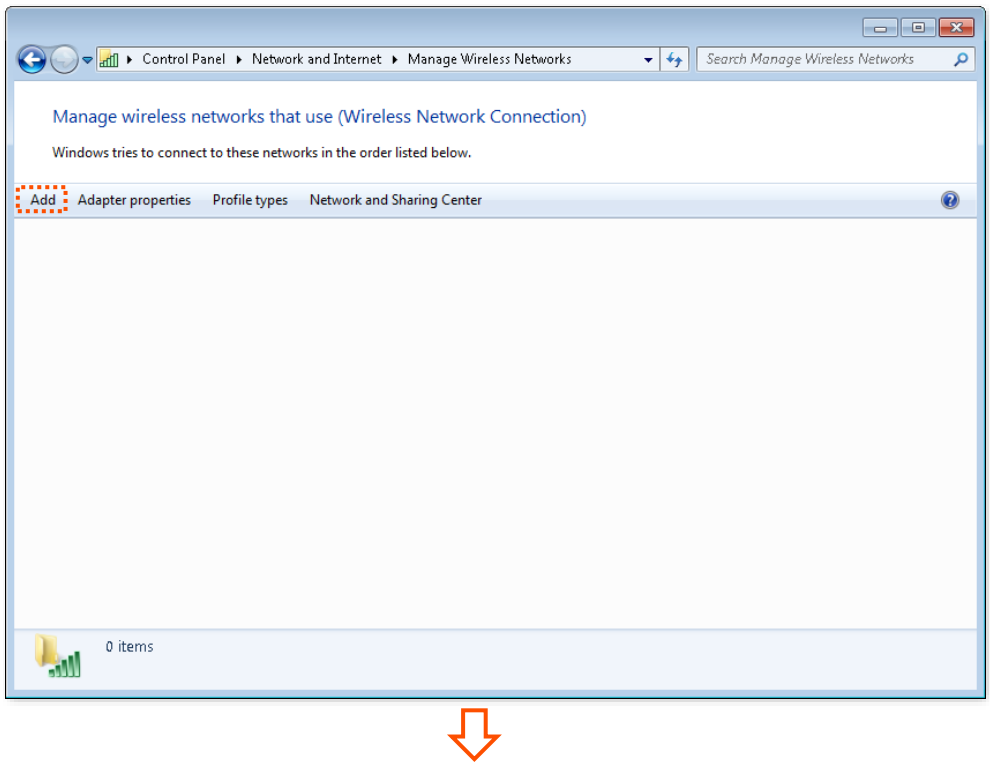
TIP

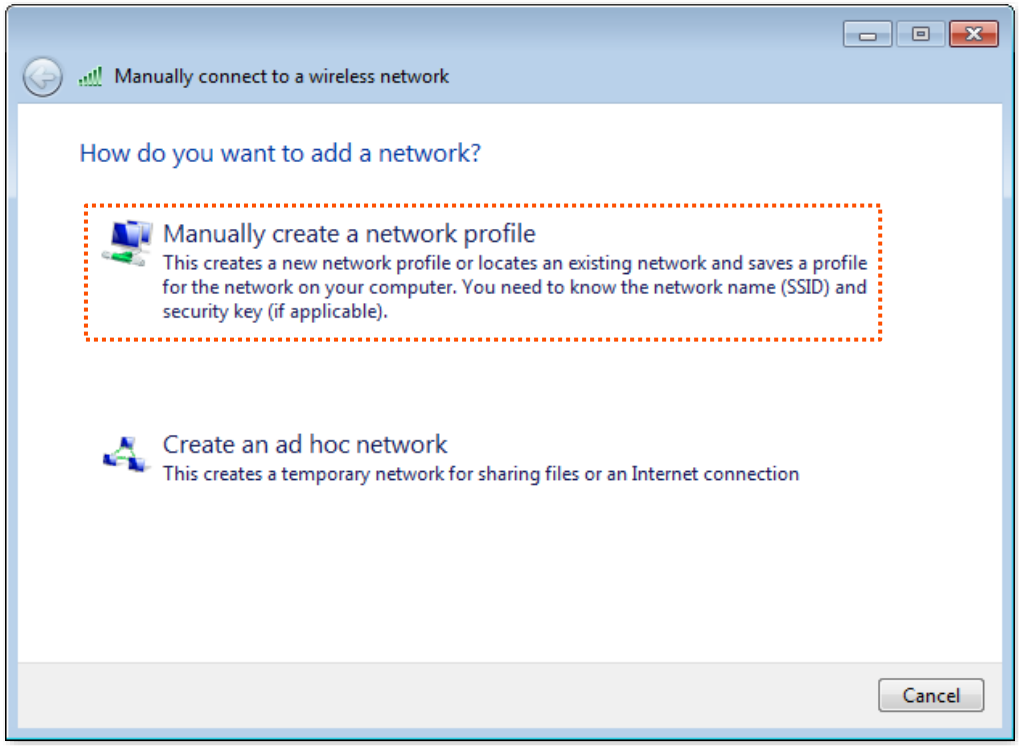
Windows 7 is taken as an example to describe the procedures.

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

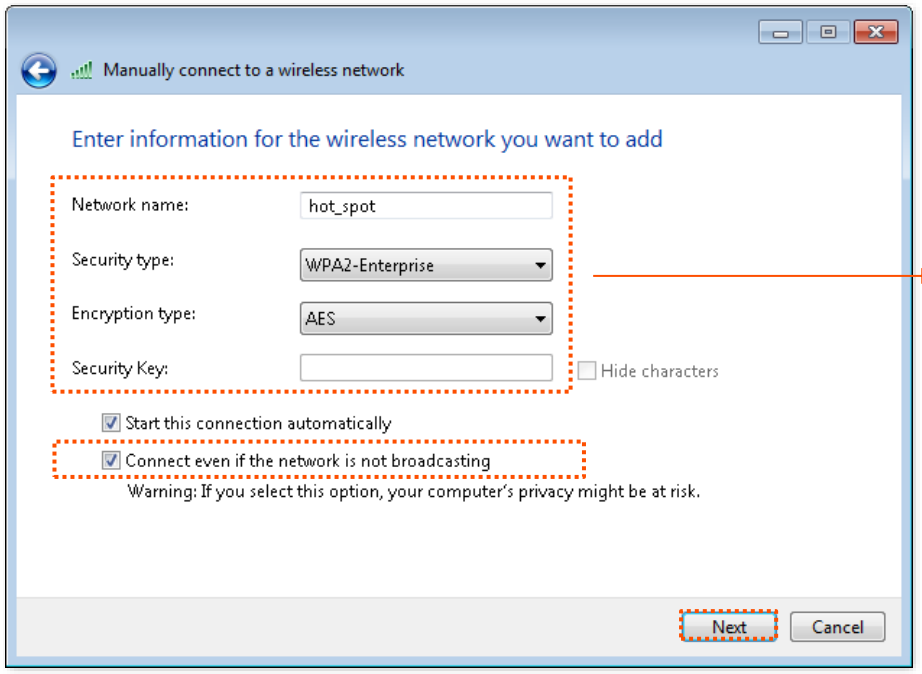



2. Click **Add**, and click **Manually create a network profile**.

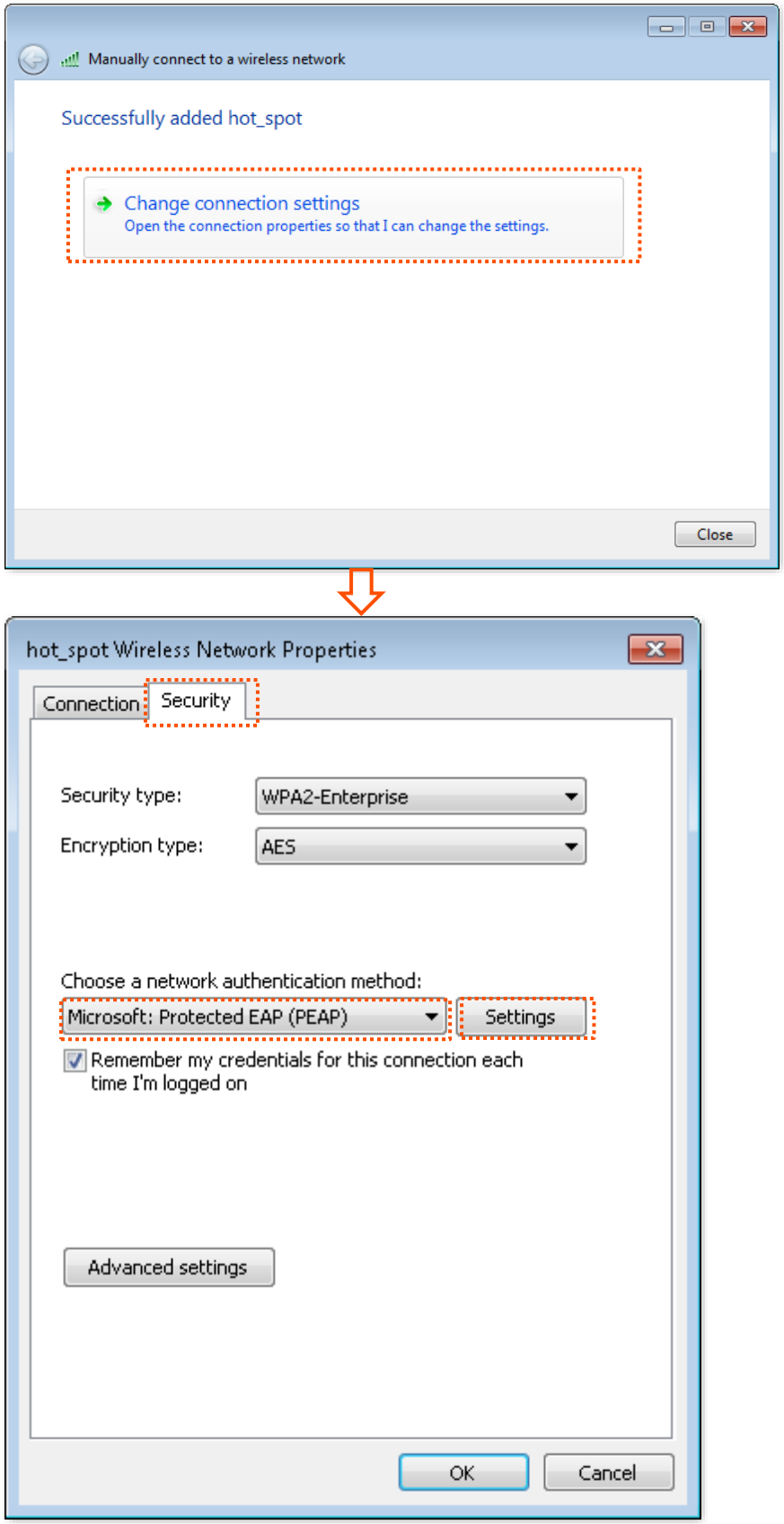




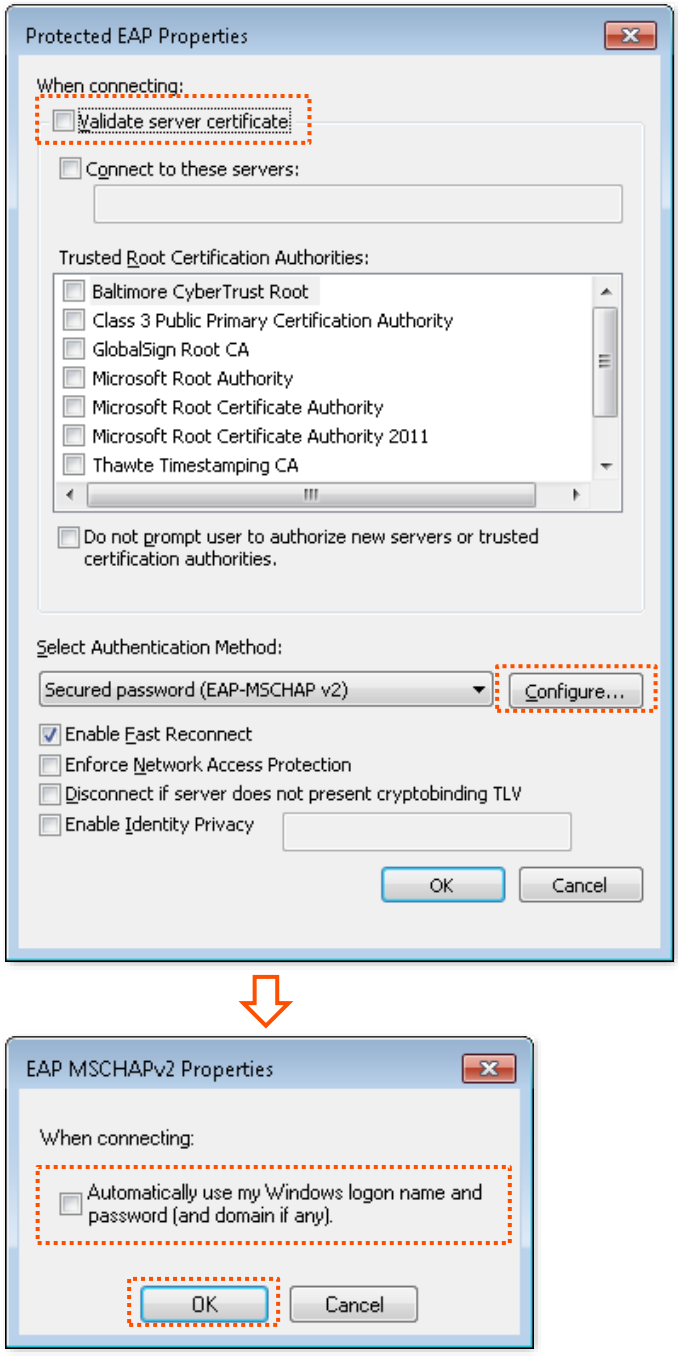

3. Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.




4. Click **Change connection settings**. Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.

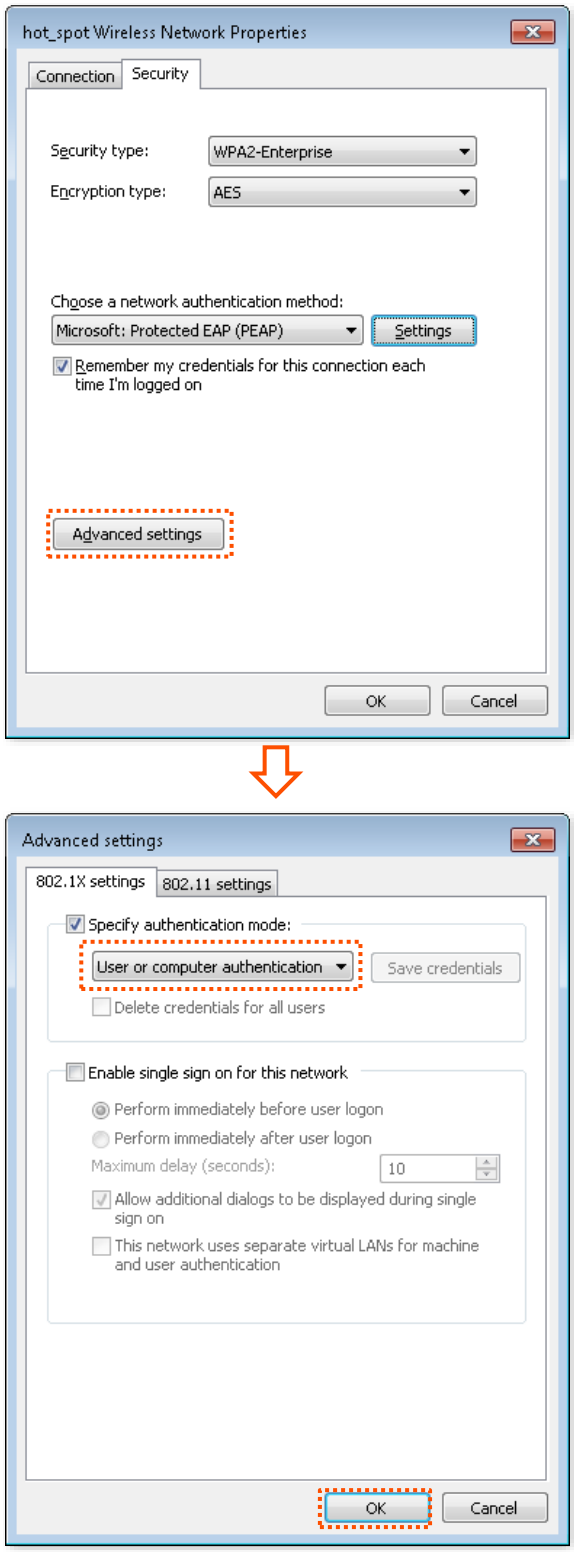



5. Deselect **Validate server certificate** and click **Configure**. Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.

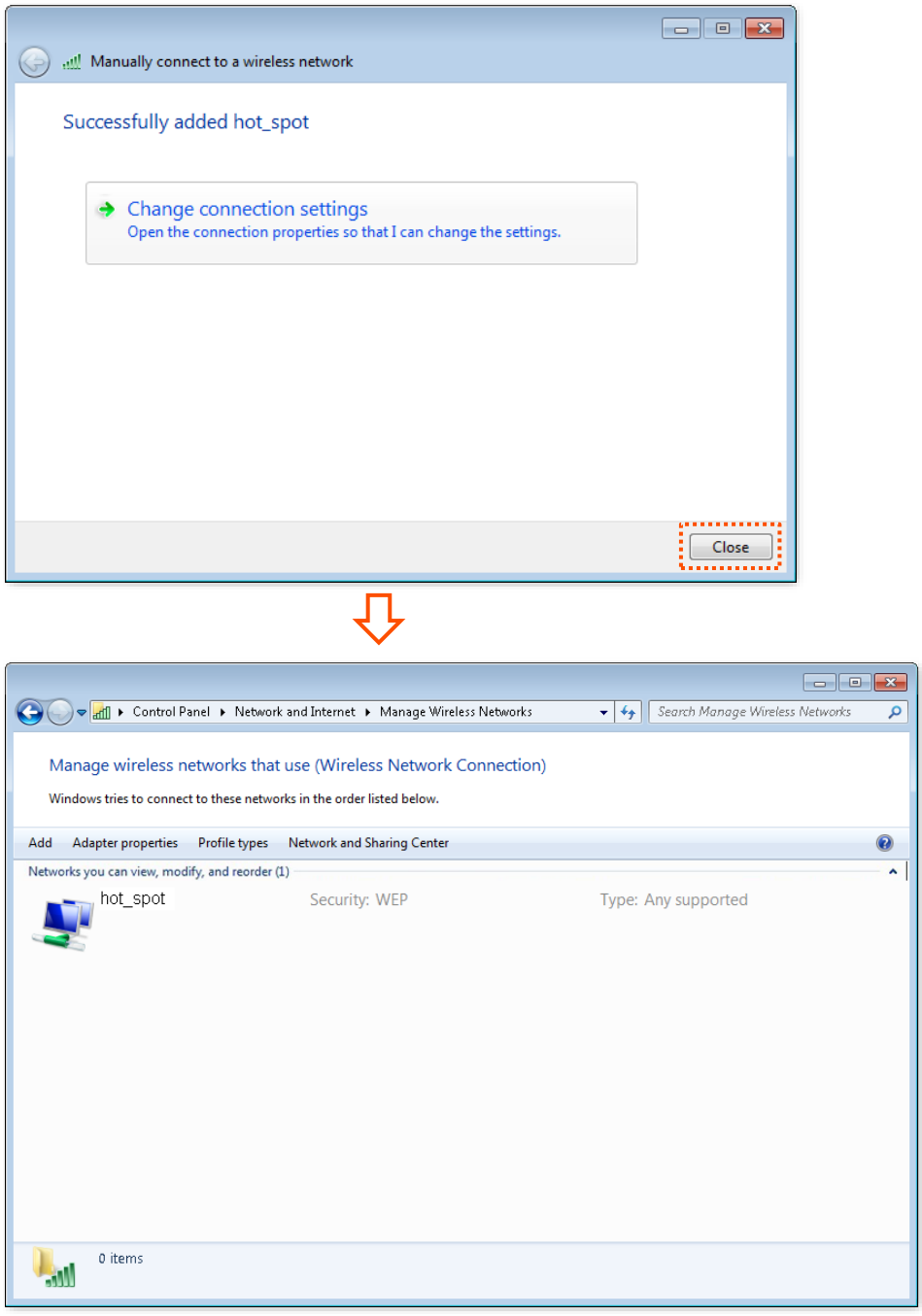

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
GlobalSign Root CA
Microsoft Root Authority
Microsoft Root Certificate Authority
Microsoft Root Certificate Authority 2011
Thawte Timestamping CA
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel


EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel

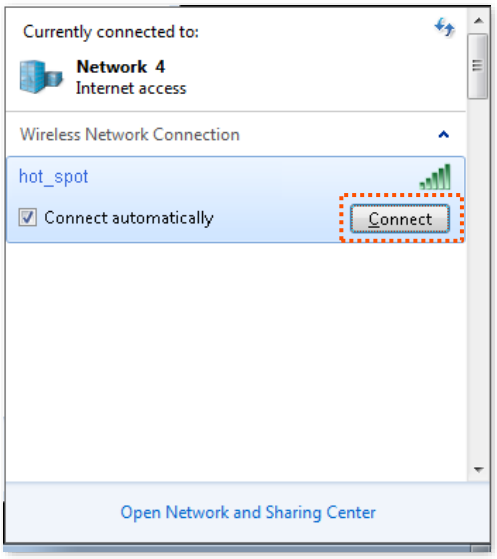
6. Click **Advanced settings**. Select **User or computer authentication** and click **OK**.



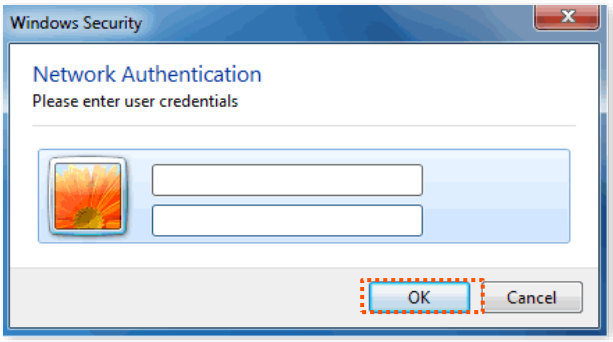
7. Click **Close**.



8. Click the network icon in the lower-right corner of the desktop and choose the wireless network of the CPE such as **hot_spot** in this example. Click **Connect**.




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




**---End**

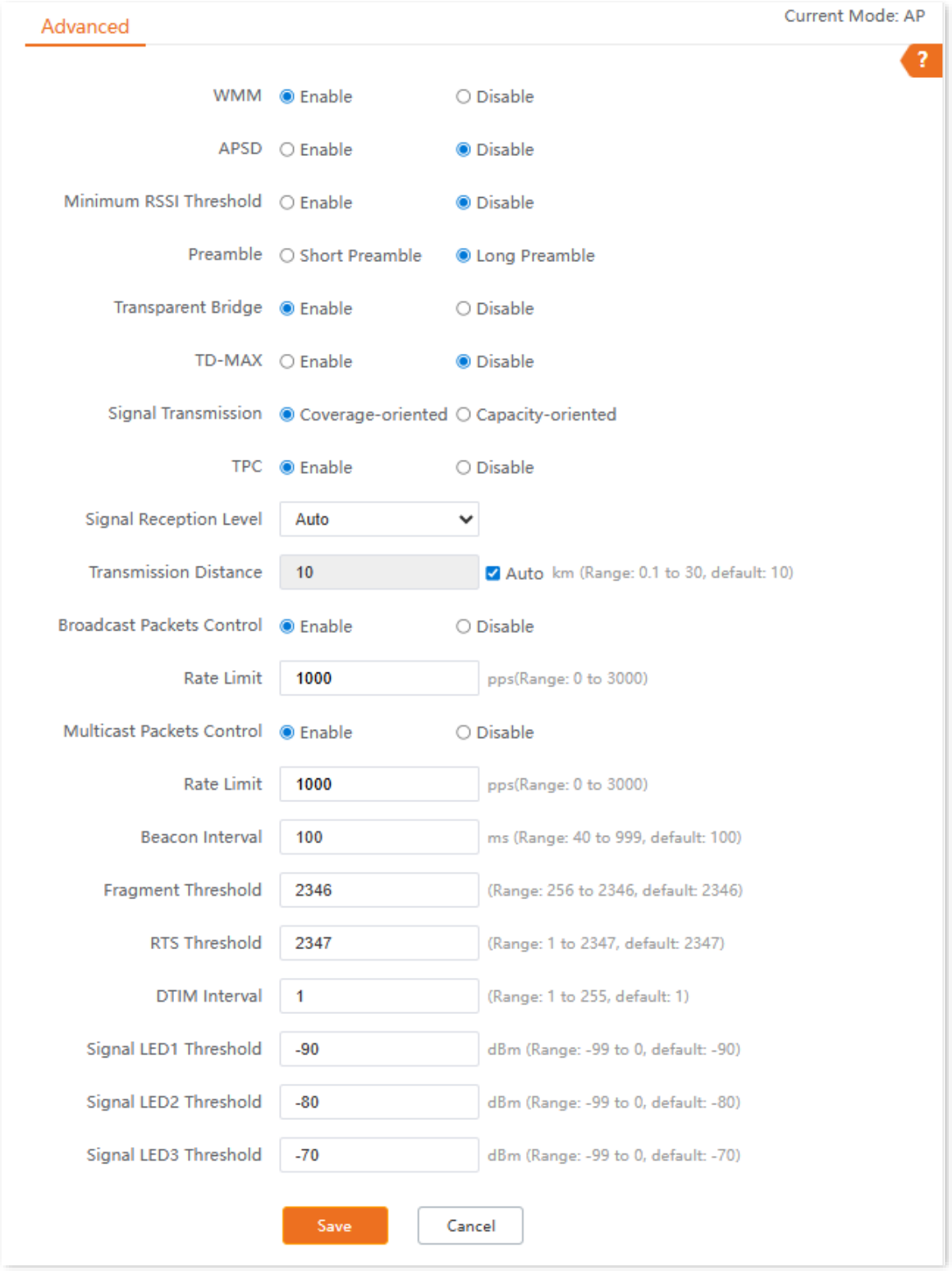
## Verification

Wi-Fi-enabled devices can connect to the wireless network **hot_spot**.

# 6.2 Advanced settings

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

To access the page, log in to the web UI of the CPE and navigate to **Wireless** > **Advanced**.



### Parameters description

| Name | Description |
| --- | --- |
| WMM | Wi-Fi Multimedia (WMM) is a wireless Quality of Service (QoS) protocol that allows higher-priority packets to be transmitted first. This ensures better QoS of voice and video applications over wireless networks. |
| APSD | Automatic Power Save Delivery (APSD) is a WMM power saving protocol created by Wi-Fi Alliance.<br>Enabling APSD helps reduce power consumption. By default, this mode is disabled. |
| Minimum RSSI Threshold | Specifies the minimum strength of received signals acceptable to this CPE.<br>If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this CPE.<br>If there are multiple CPEs in a network, setting a proper value helps Wi-Fi-enabled devices connect to a wireless network with a better wireless signal. |
| Preamble | 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.<br>By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients.<br>To achieve better synchronization performance of networks, you can select the Short Preamble option. |
| Transparent Bridge | The Transparent Bridge function enables the WLAN interface of this CPE to forward all packets. It is used to solve the problem that some NVRs cannot detect IP cameras, or cannot change the IP addresses of cameras in different networks.<br>TIP<br>- This function is applicable only when the CPE works in AP, Client or Universal Repeater mode.<br>- Transparent WDS and Transparent Bridge cannot be enabled at the same time. |

| Name | Description |
| --- | --- |
| TD-MAX | TD-MAX is Tenda's proprietary Time Division Multiple Access (TDMA) polling technology. It allows multiple clients to share the same channel for accessing a network. With the TD-MAX enabled, the CPE assigns time slots to each client, and transmits data according to the assigned time slots, achieving Point-to-MultiPoint (PtMP) connections.<br>After the TD-MAX is enabled, the CPE:<br>- Avoids the “hidden node” problem, which occurs when a node is visible from a wireless AP, but not from other nodes communicating with the originating AP.<br>- Reduces latency.<br>- Improves throughput and anti-interference performance.<br>- Improves overall performance in Point-to-MultiPoint (PtMP) installations, and increases the maximum possible number of users that can associate with an AP that uses TD-MAX.<br>TIP<br>If TD-MAX is enabled, the device operates in TD-MAX mode and only accepts connections from TD-MAX Wi-Fi-enabled devices (such as laptops, tablets, or smartphones). |
| Signal Transmission | Specifies the CPE's wall-penetration capability.<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 CPE 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 CPE decreases its TX power. |
| Signal Reception Level | Used to adjust the signal reception level of this CPE. A higher level leads to better signal reception capability and more wireless networks can be searched, but lower throughput. Adjust the level based on your actual situation. |
| Transmission Distance | Specifies the wireless transmission distance of this CPE. You can set it based on the actual installation distance.<br>TIP<br>Modifying this distance will affect wireless transmission performance, and it is recommended to keep the default setting. If you want to set it manually, you should enter a value that is greater than the actual distance between the two CPEs. |
| Broadcast Packets Control | Enabled by default. Specifies the rate limit for broadcast traffic that can be forwarded per second. Default: 1000 pps. |
| Multicast Packets Control | Enabled by default. Specifies the rate limit for multicast traffic that can be forwarded per second. Default: 1000 pps. |

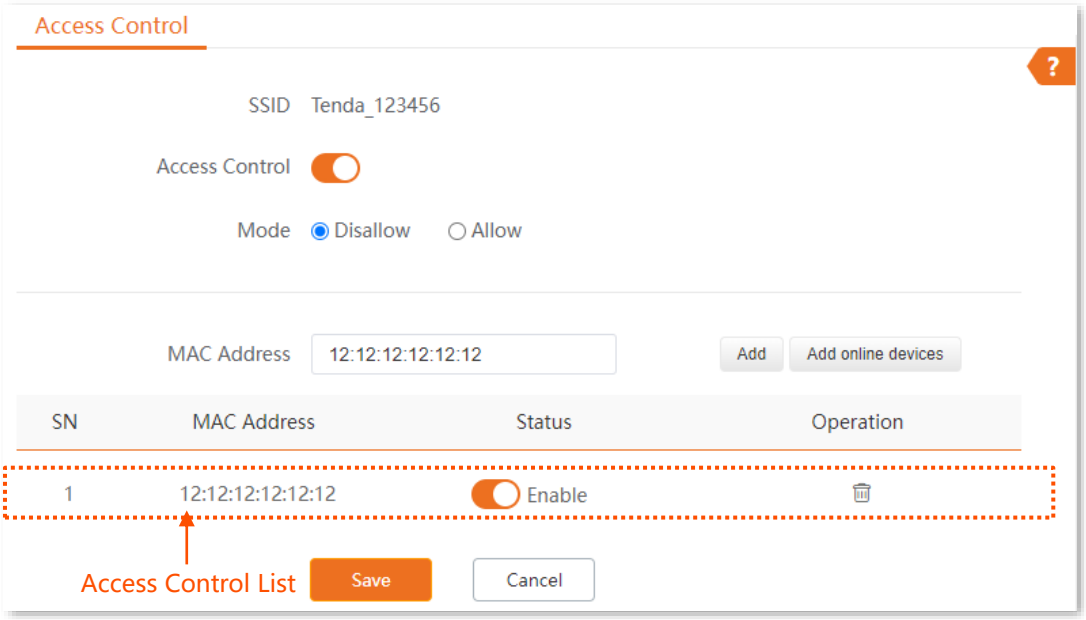
| Name | Description |
| --- | --- |
| Beacon Interval | Specifies the interval at which this CPE sends Beacon frames.<br>Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this CPE sooner, while a larger interval allows the wireless network to transmit data more quickly. |
| Fragment Threshold | Specifies the threshold of a fragment. The unit is bytes.<br>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.<br>In case of a high error rate, you can reduce the threshold. If the transmission fails, this device resends only the fragments that have not been sent successfully, so as to increase the frame throughput.<br>In an environment with little interference, you can increase the threshold to reduce the number of fragments, so as to increase the frame throughput. |
| RTS Threshold | 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 bytes.<br>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 more quickly. For a wireless network with high user density, you can reduce this threshold to reduce conflicts.<br>The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold. |
| DTIM Interval | Specifies the countdown before this device transmits broadcast and multicast frames in its cache. The unit is beacon intervals.<br>For example, if Delivery Traffic Indication Map (DTIM) Interval is set to 1, this CPE transmits all cached frames at one Beacon interval. |
| Signal LED1 Threshold | Specifies the received signal strength of this CPE's LED indicators. You can customize the threshold for triggering each signal LED indicator to light up.<br>The default thresholds for LED1, LED2, and LED3 are **-90** dBm, **-80** dBm, and **-70** dBm respectively. |
| Signal LED2 Threshold | |
| Signal LED3 Threshold | |

# 6.3 Access control

## 6.3.1 Overview

The Access Control function enables you to allow or disallow the Wi-Fi-enabled devices to access the wireless network based on their MAC addresses.

To access the page, log in to the web UI of the CPE and navigate to **Wireless** > **Access Control**. This function is disabled by default. After it is enabled, the page is shown as follows.




**Parameters description**

| Name | Description |
| --- | --- |
| SSID | 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 | Specifies whether to enable or disable the Access Control function. |
| Mode | Specifies the mode for filtering MAC addresses.<br>- **Allow**: Indicates that only the wireless clients on the access control list can connect to the wireless network of the CPE.<br>- **Disallow**: Indicates that only the wireless clients on the access control list are blocked from connecting to the wireless network of the CPE. |

## 6.3.2 Example of configuring access control

### Networking requirements

A community uses the CPE for wireless networking. Now, only specific members in this community are allowed to connect to the wireless network.

### Solution

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

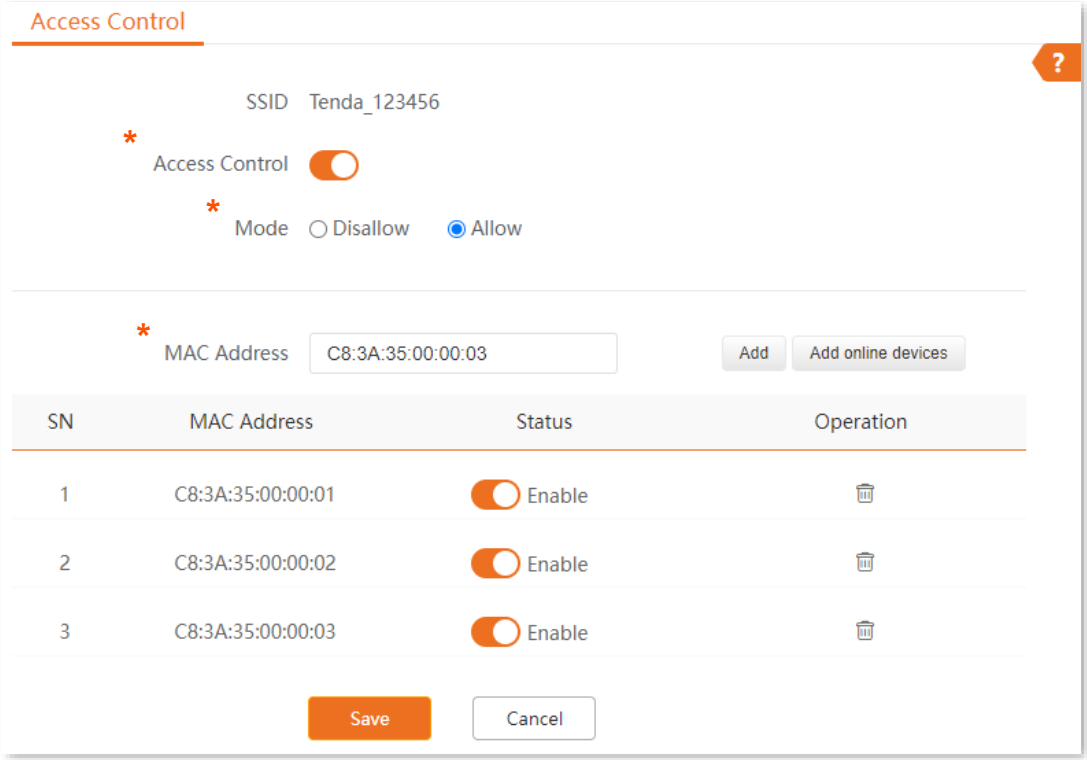
## Configuration procedure

1. Log in to the web UI of the CPE.
2. Navigate to **Wireless** > **Access Control**.
3. Enable the **Access Control** function.
4. Set **Mode** to **Allow**.
5. Enter the MAC address, which is **C8:3A:35:00:00:01** in this example, and click **Add**.

TIP

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

6. Refer to step 5 to add the other two MAC addresses.
7. Click **Save**.




**---End**

## Verification

Only Wi-Fi-enabled devices mentioned above can connect to the wireless network of the CPE.

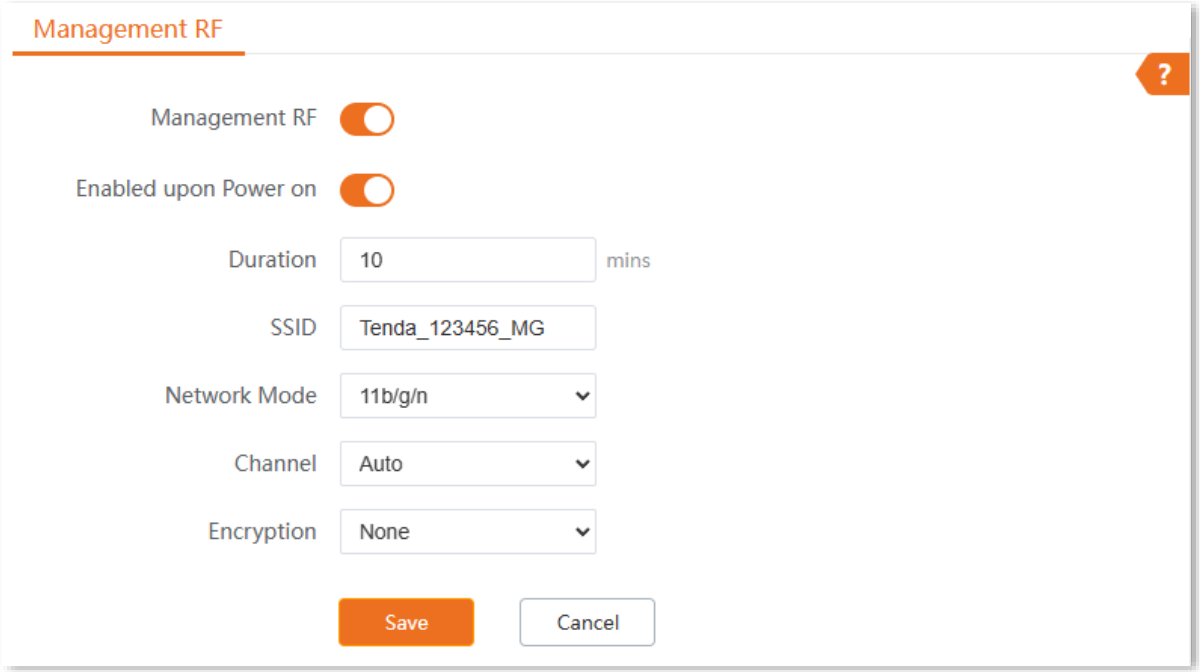
# 6.4 Management RF

## 6.4.1 Overview

Management RF (2.4 GHz) is mainly used to facilitate users to connect to the wireless network of the CPE to manage the CPE under special circumstances. For example, when the CPE is working in Client mode, you can log in to the web UI of the CPE by connecting to the wireless network of the CPE's Management RF.

To access the page, log in to the web UI of the CPE and navigate to **Wireless** > **Management RF**.

On this page, you can set the basic information of the CPE's management RF wireless network. It is recommended to only set the **SSID** and **Encryption**, and keep the other default settings.




**Parameters description**

| Name | Description |
| --- | --- |
| Management RF | Specifies whether to enable management Wi-Fi of the CPE.<br>TIP<br>Management RF is not automatically disabled when it is enabled manually. The management Wi-Fi is unprotected and should be used only when necessary. |
| Enabled upon Power on | Specifies whether to enable the Enabled upon Power on function of the management RF.<br>With this function enabled, the CPE's management RF will be automatically enabled when the CPE is powered off and on again or rebooted from the web UI. |

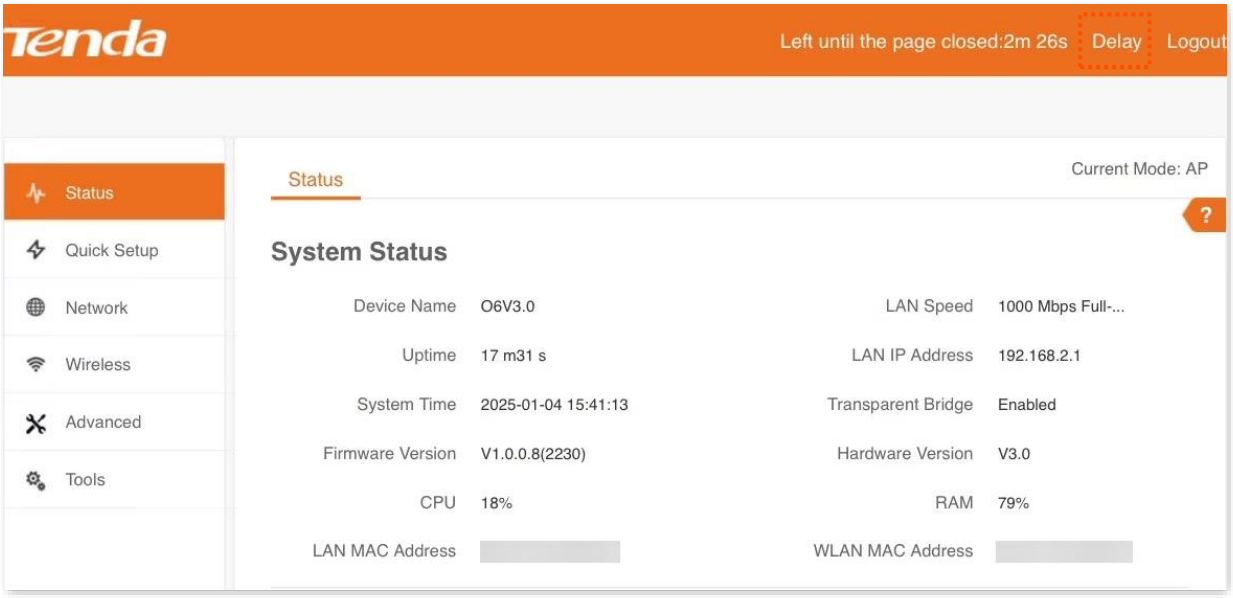
| Name | Description |
| --- | --- |
| Duration | Specifies how long management Wi-Fi remains enabled after it is enabled by a reboot.<br>With management RF enabled, if the **Duration** is exceeded and the available time for management Wi-Fi is not extended, the management Wi-Fi will be automatically disabled.<br>TIP<br>If management RF is enabled through a reboot, you can extend the available time for the management Wi-Fi from the web UI of the CPE on your wireless device. |
| SSID | Specifies the name of the management Wi-Fi. You can modify it as required. |
| Network Mode | Specifies the wireless network mode of the CPE. Only wireless devices supporting the listed network mode can connect to the CPE. |
| Channel | Specifies the operating channel of the management Wi-Fi. When **Auto** is selected, the CPE will automatically adjust its operating channel depending on the surrounding environment. |
| Encryption | Specifies the security mode of the management Wi-Fi. See Security Mode for details. |

## 6.4.2 Extend management Wi-Fi duration

With management RF enabled through a reboot, if the Duration is exceeded and the available time for management Wi-Fi is not extended, the management Wi-Fi will be automatically disabled. To extend the available time for management Wi-Fi, perform the following procedure.

**Configuration procedure**

1. Connect the wireless client to the management RF's wireless network.
2. Start a browser on your wireless client, visit the CPE's management IP address (By default, AP mode: **192.168.2.1**, Client mode: **192.168.2.2**), and log in to the web UI of the CPE.
3. Click **Delay** in the upper right corner of the page. The following figure is for reference only.




**---End**

TIP

- To extend the available time of the management RF's wireless network, you must enable the Management RF function. Extend the available time before the management Wi-Fi is automatically disabled to continue using the management Wi-Fi.
- Each time you click **Delay**, the maximum delay time is 5 minutes.
- The total delay time cannot exceed the Duration. For example, if the **Duration** is 10 minutes, it means you can extend the duration by up to 10 minutes.

# 7 Advanced

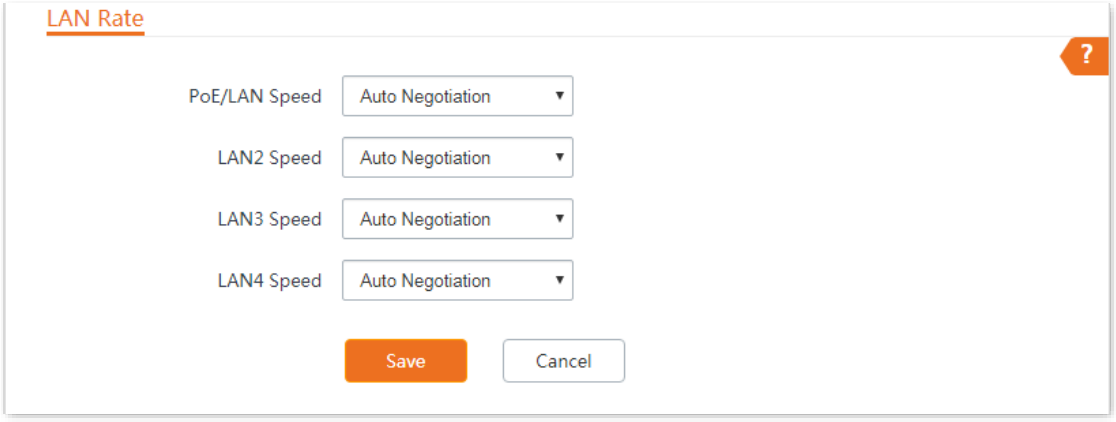
Features available in the CPE may vary by model and software version. CPE availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual CPE experience.

## 7.1 LAN rate

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **LAN Rate**.

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

When you change the settings, ensure that the LAN speed and duplex mode of the CPE port are the same as those of the peer device. By default, the LAN speed setting of the LAN port is **Auto Negotiation**. OS3 V2.0 is used for illustration.




After the LAN speed and duplex mode settings are changed, you can check on the System Status page.

**Parameters description**

| Name | Description |
|---|---|
| Auto Negotiation | Specifies that the speed and duplex mode of the port are determined through auto-negotiation between the CPE and the peer CPE. |

| Name | Description |
| --- | --- |
| 1000Mbps Full Duplex | Specifies the port working at 1000 Mbps, and can transmit and receive packets at the same time. |
| 100Mbps Full Duplex | Specifies the port working at 100 Mbps, and can transmit and receive packets at the same time. |
| 100Mbps Half Duplex | Specifies the port working at 100 Mbps, and can only transmit or receive packets. |
| 10Mbps Full Duplex | Specifies the port working at 10 Mbps, and can transmit and receive packets at the same time. |
| 10Mbps Half Duplex | Specifies the port working at 10 Mbps, and can only transmit or receive packets. |

TIP

- If you set the speed and duplex mode of the port manually, ensure that the speed and duplex mode of the peer port are set to **Auto Negotiation** or the same as this port.
- Lower speed mode can improve the transmission distance of the port. If you want to extend the PoE power supply distance, you can change the speed to a low speed mode, such as 10 Mbps full-duplex. Ensure that the speed mode of the peer port is also **10 Mbps Full Duplex** or **Auto Negotiation**.

# 7.2 Diagnose

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Diagnose**.

You can use the diagnosis tools for troubleshooting.

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

## 7.2.1 Site survey

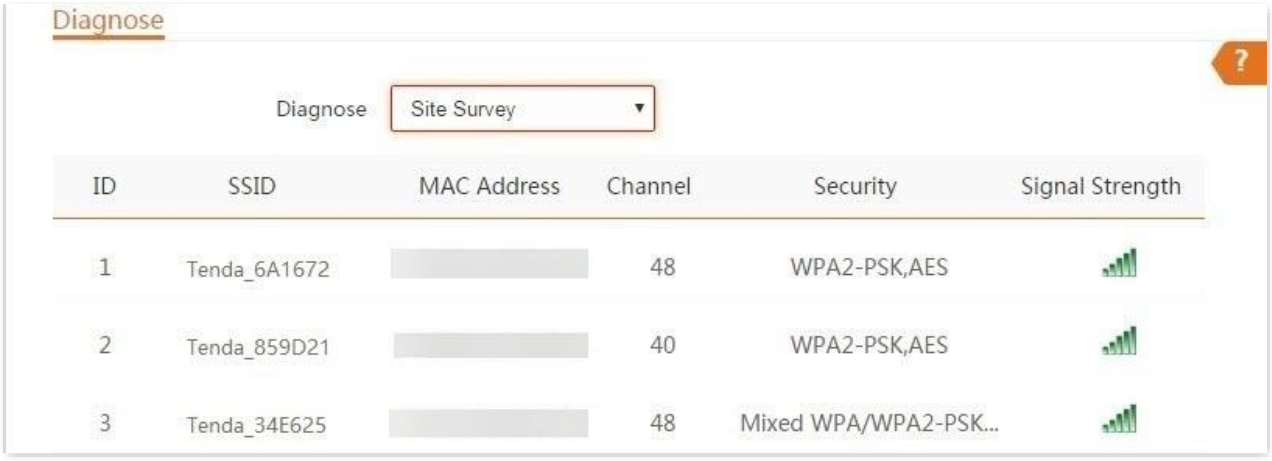
Site survey gives you an insight into the information of nearby wireless signals. According to the diagnosis result, you can select a channel that is least used for the CPE to improve the transmission efficiency.

**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Advanced** > **Diagnose**.
3. Select **Site Survey** in the **Diagnose** drop-down list.

**---End**

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



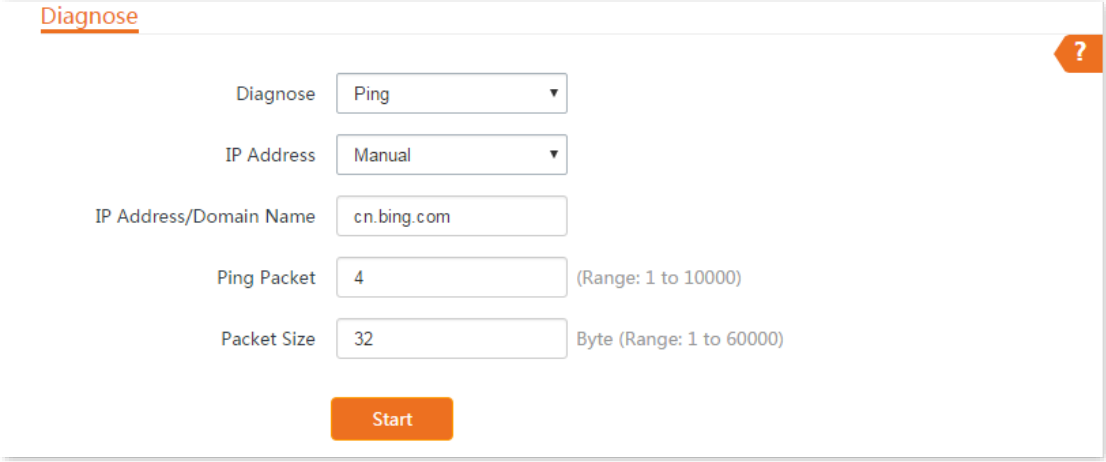

## 7.2.2 Ping

You can use ping to check network connectivity and connection quality.

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

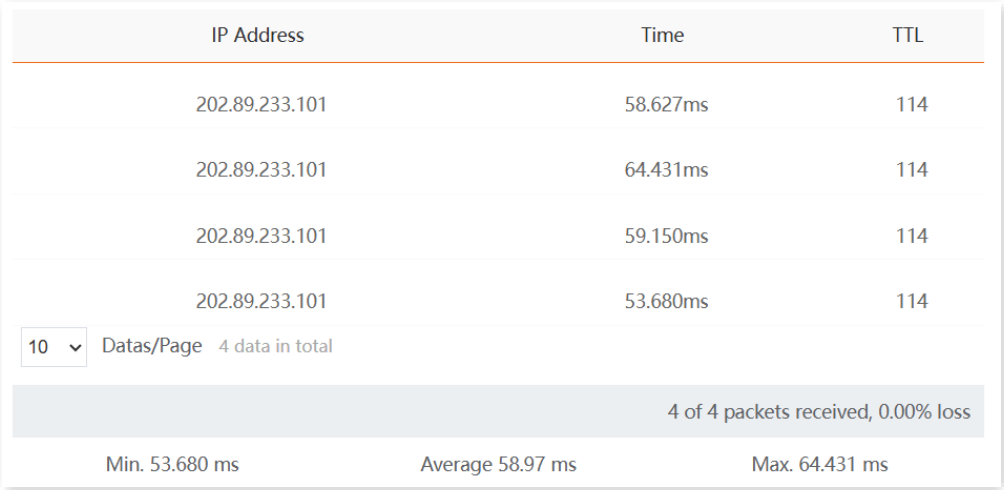
**Configuration procedure**

1. Log in to the web UI of the CPE, then navigate to **Advanced** > **Diagnose**.
2. Select **Ping** in the **Diagnose** drop-down list.
3. Set **IP Address** to **Manual**.
4. Enter the target IP address or a domain name, which is **cn.bing.com** in this example.
5. Set **Ping Packet** and **Ping Size**. The default setting is recommended.
6. Click **Start**.




**---End**

The diagnosis result will be displayed in a few seconds. The following figure is for reference only.



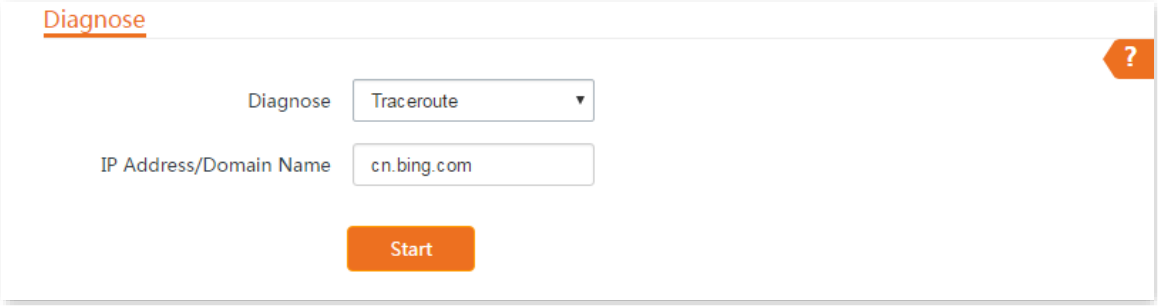

## 7.2.3 Traceroute

You can use the Traceroute tool to detect the routes that packets take from the CPE to the destination host.

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

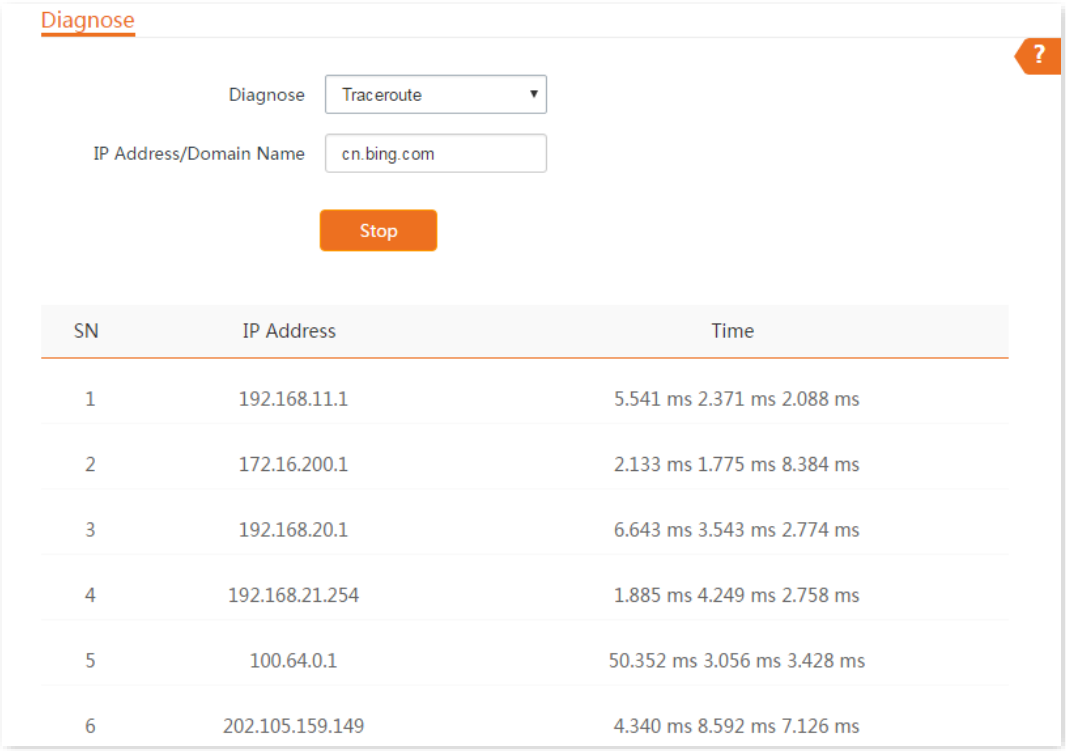
**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Advanced** > **Diagnose**.
3. Select **Traceroute** in the **Diagnose** drop-down list.
4. Enter the target IP address or a domain name, which is **cn.bing.com** in this example.
5. Click **Start**.




**---End**

The diagnosis result will be displayed in a few seconds in the list below. The following figure is for reference only.

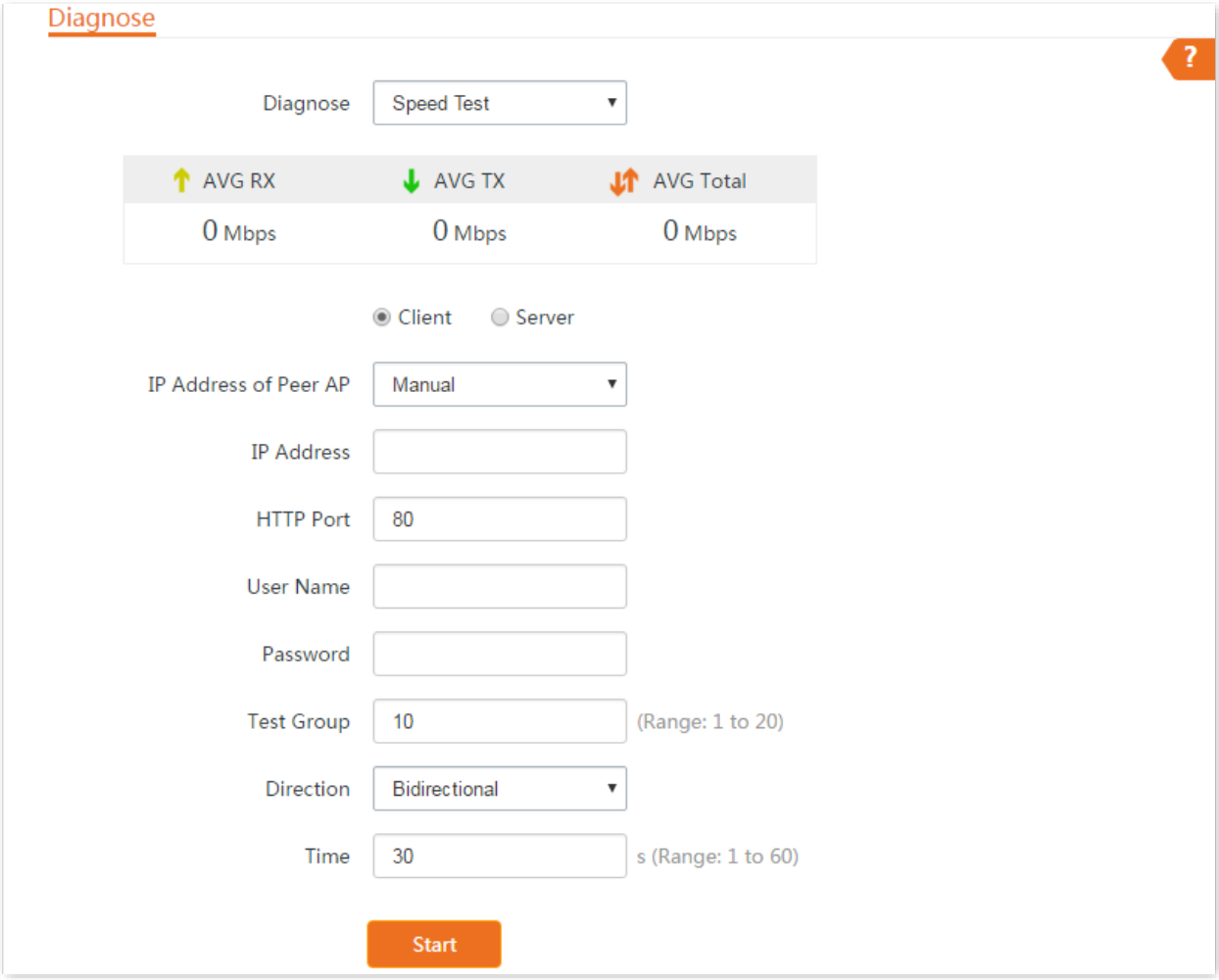



## 7.2.4 Speed test

### Overview

You can use the **Speed Test** to test the connection speed between two bridging CPEs, which helps estimate the throughput between the two CPEs. The test requires that both sides can use the **Speed Test** function. O4 V3.0 is used for illustration.

Log in to the web UI of the CPE, navigate to **Advanced** > **Diagnose**, and select **Speed Test** from the **Diagnose** drop-down list.




**Parameters description**

| Name | Description |
|---|---|
| Client | Specifies the speed test mode of the local end. Settings cannot be the same as Server. |
| Server | Specifies the speed test mode of the remote end. Settings cannot be the same as Client. |
| AVG RX | Specifies the average receive rate. |
| AVG TX | Specifies the average transmit rate. |
| AVG Total | Specifies the average total rate. |

| Name | Description |
| --- | --- |
| IP Address of Peer AP | Specifies the LAN IP address of the peer CPE. You can enter it manually or select the IP address of the peer AP from the drop-down list if there are peer CPEs 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 here. |
| HTTP Port | Specifies the HTTP service port number of peer CPE, which is used to establish speed test connections based on TCP/IP. The default value is **80**. You are recommended to keep the default value. |
| User Name | Specify the login user name and password of the peer CPE. |
| Password | |
| Test Group | Specifies the number of test connections established. |
| Direction | Specifies the test direction.<br>- **RX**: Only test the speed that this device receives data from the peer CPE.<br>- **TX**: Only test the speed that this device transmits data to the peer CPE.<br>- **Bidirectional**: Test both transmit and receive speed between the two CPEs. |
| Time | Specifies the duration of the speed test, which is 30s by default. |

## Example of configuring the speed test

Assume that CPE1 working in AP mode and CPE2 working in Client mode have bridged successfully. Basic information about the two CPEs is shown below:

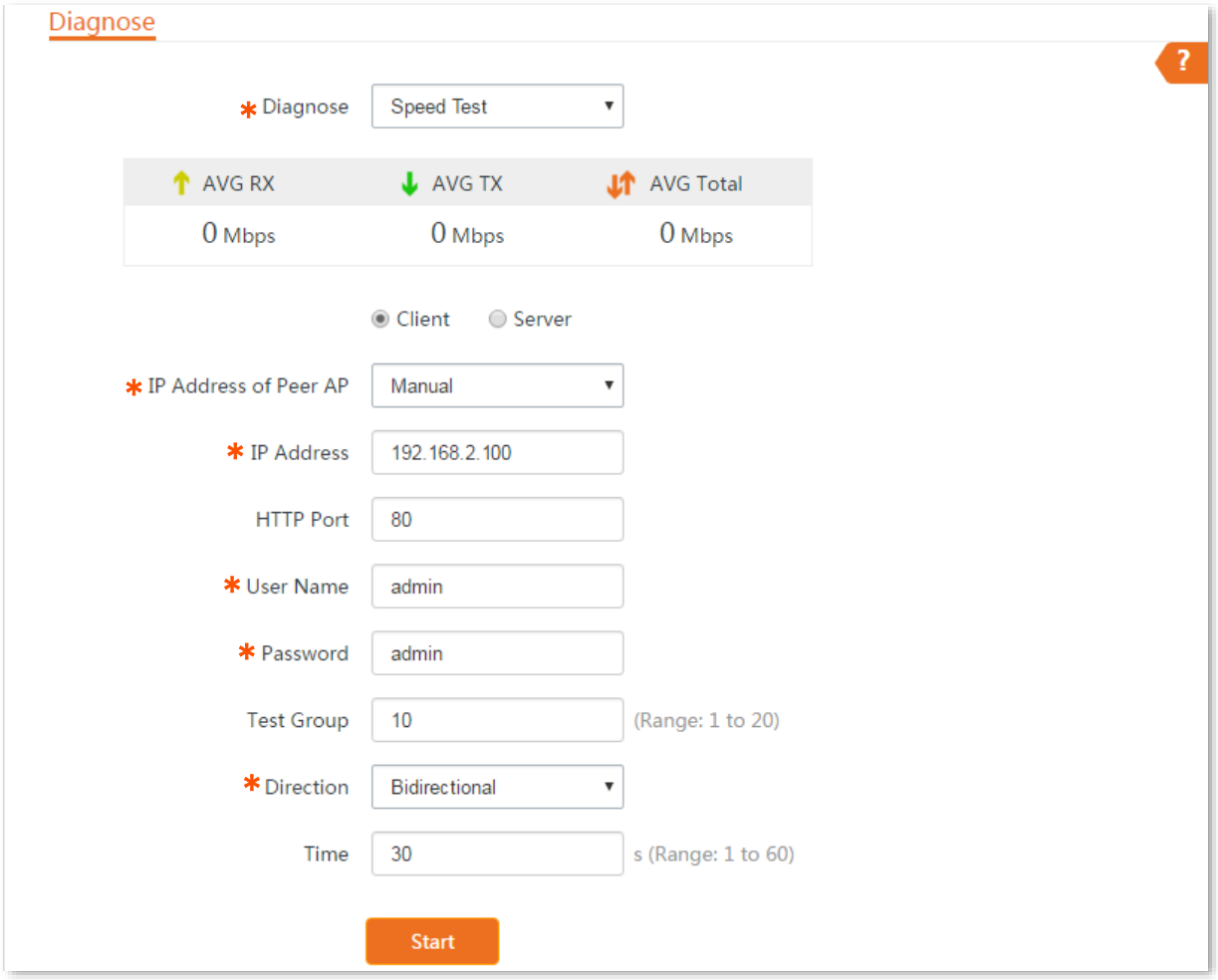
- IP address of CPE1: **192.168.2.100**
- IP address of CPE2: **192.168.2.1**
- Login user names/passwords of the two CPEs: **admin**

To test the wireless speed between them, perform the following procedure either on CPE1 or CPE2.

**Configuration procedure**

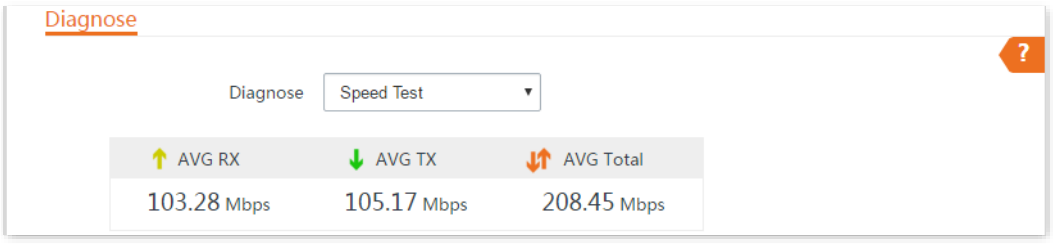
1. Log in to the web UI of the CPE2, then navigate to **Advanced** > **Diagnose**.
2. Select **Speed Test** in the **Diagnose** drop-down list.
3. Set **IP Address of Peer AP** to **Manual**.
4. Enter the IP address of CPE1 in the **IP Address** field, which is **192.168.2.100** in this example.
5. Enter the login user name and password of the web UI of CPE1 in the **User Name** and **Password** fields, which are both **admin** in this example.
6. Set **Direction** to **Bidirectional**.

7. Click **Start**.




**---End**

The test result will be displayed in a few seconds in the list below. The following figure is for reference only.



## 7.2.5 Spectrum analysis

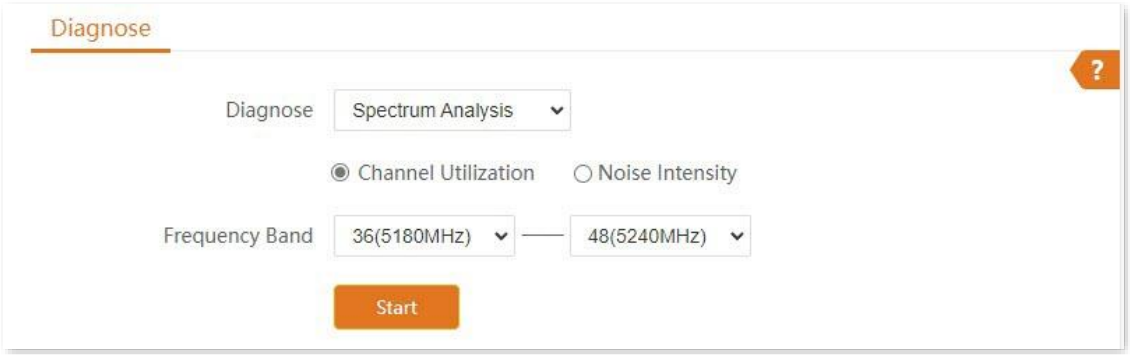
The **Spectrum Analysis** function allows you to check the channel utilization and wireless noise of each channel, so that you can select a channel with minimum channel utilization and wireless noise for the CPE based on the diagnosis result.

TIP

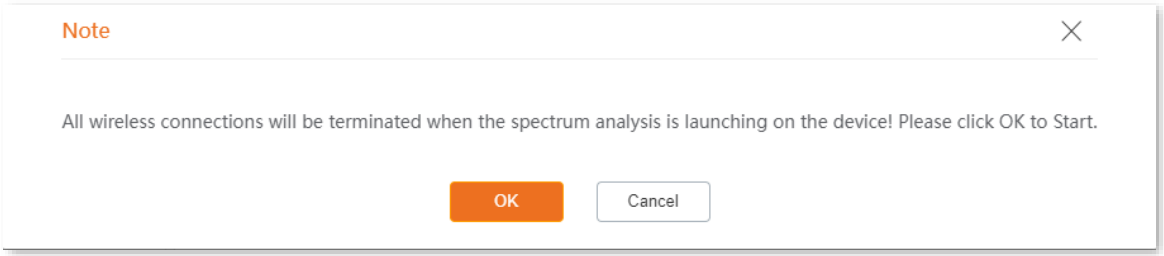
- CPEs to be bridged must operate on the same channel.
- All wireless connections are disconnected during a spectrum analysis. Perform this operation when the network is idle.

### Measure channel utilization

1. Log in to the web UI of the CPE, then navigate to **Advanced** > **Diagnose**.
2. Select **Spectrum Analysis** from the **Diagnose** drop-down list.
3. Select **Channel Utilization**.
4. Select the frequency band range you want to test, which is **36(5180 MHz)** to **48(5240MHz)** in this example.
5. Click **Start**.



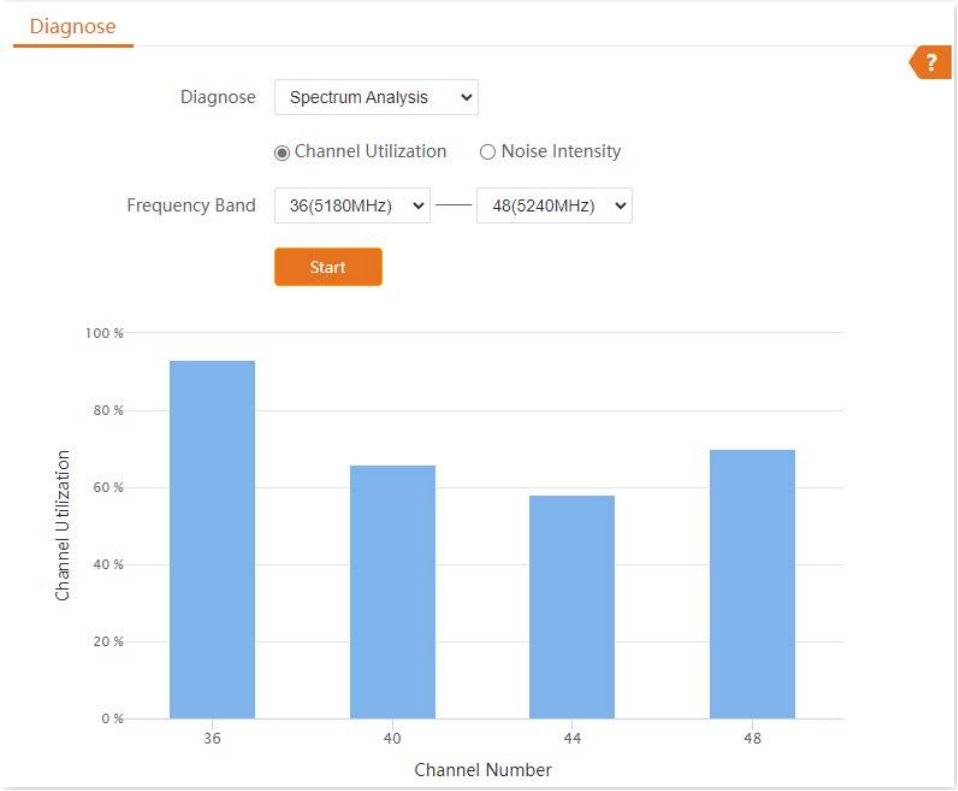

6. Confirm the prompt information, and click **OK**.




**---End**

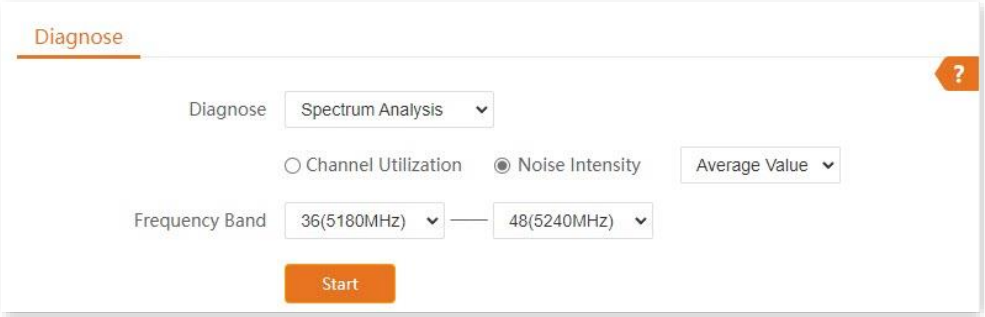
The diagnosis result will be displayed in a few seconds in the list below. The following figure is for reference only.

Based on the diagnosis result, the CPE can be set to channel 44 for optimal transmission.

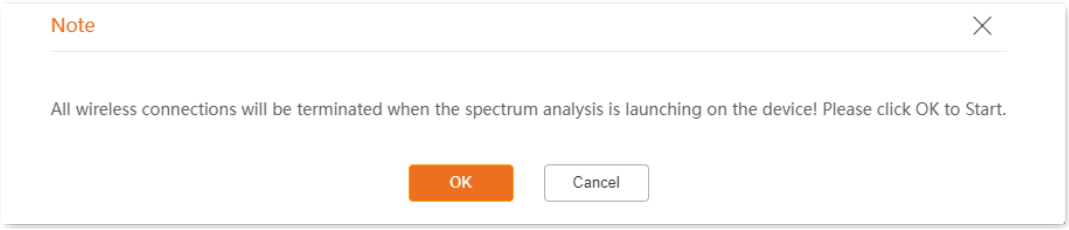



## Measure noise intensity

1. Log in to the web UI of the CPE, then navigate to **Advanced** > **Diagnose**.
2. Select **Spectrum Analysis** from the **Diagnose** drop-down list.
3. Select **Noise Intensity.**
4. Select the value to be tested, which is **Average Value** in this example.
5. Select the frequency band range you want to test, which is **36(5180 MHz)** to **48(5240MHz)** in this example.
6. Click **Start**.



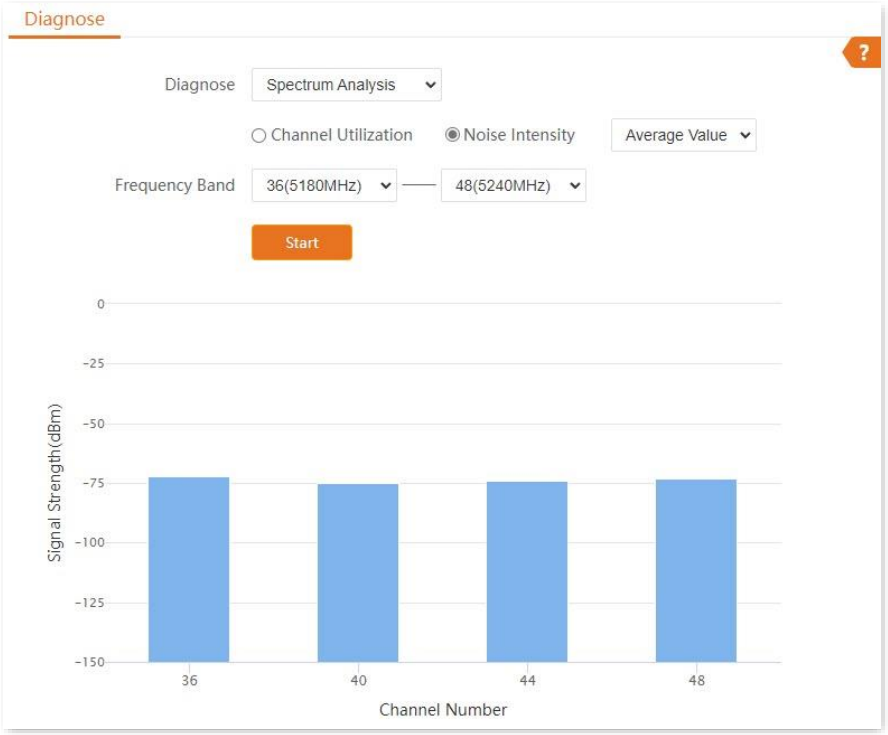

7. Confirm the prompt information, and click **OK**.




**---End**

The diagnosis result will be displayed in a few seconds in the list below. The following figure is for reference only.

Based on the diagnosis result, the CPE can be set to channel 40, 44 or 48 for optimal transmission.



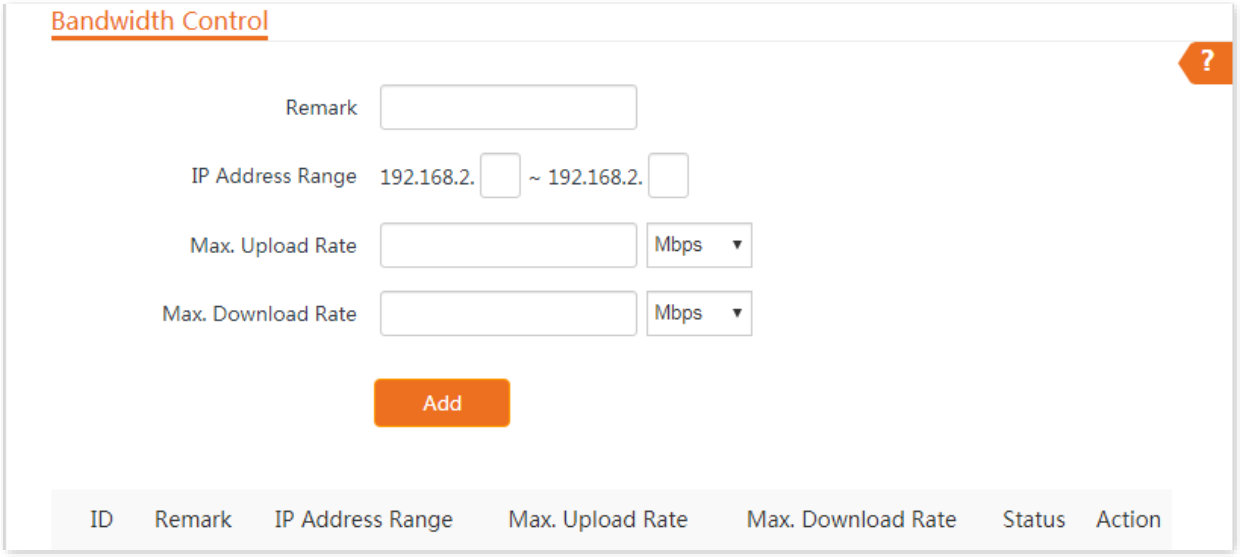

# 7.3 Bandwidth control

## 7.3.1 Overview

The Bandwidth Control function is available only when the CPE works in WISP or Router mode.

If multiple clients access the internet through the CPE, bandwidth control is recommended, so that a client downloading files at a high speed does not reduce the internet access speed of the other clients.

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Bandwidth Control**. The following figure is for reference only.




**Parameters description**

| Name | Description |
|---|---|
| Remark | Specifies the description of the bandwidth control rule.<br>This field is optional. For convenient management, it is recommended to specify different remarks for different rules. |
| IP Address Range | Specifies the IP address or IP address range of clients that this rule applies to.<br>If you want to control only one client, enter the same IP address in the two boxes.<br>If you want to control multiple clients, 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 | Specify the maximum upload or download rate of a client whose IP address is within the specified IP address range. |
| Max. Download Rate | |
| Status | 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

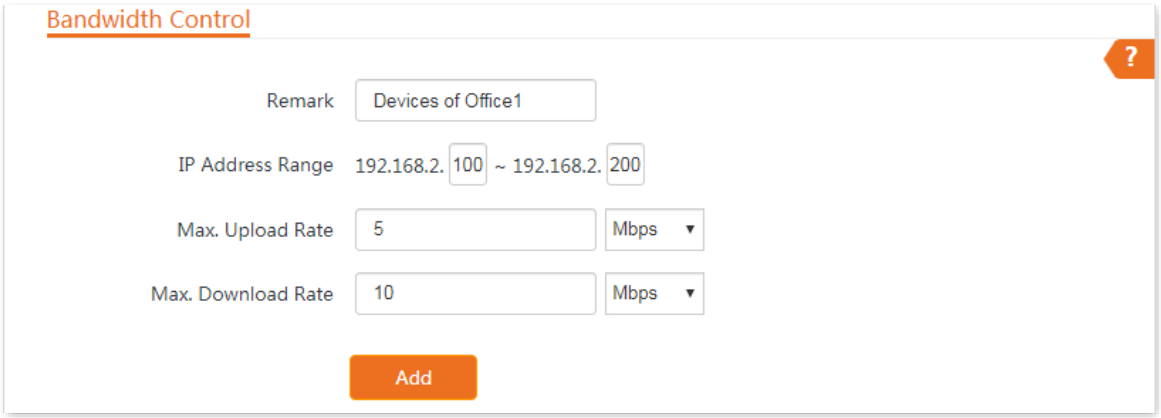
### Networking requirements

An enterprise uses the CPE to set up a network. The CPE is in WISP mode and has connected to the internet. To ensure that every device can access the internet smoothly, you want to specify the maximum upload and download rates for each device.

Assume that the maximum upload rate of each device connected to the wireless network is 5 Mbps, the maximum download rate is 10 Mbps, and the IP address range is 192.168.2.100 to 192.168.2.200.

## Configuration procedure

1. Log in to the web UI of the CPE.
2. Navigate to **Advanced** > **Bandwidth Control**.
3. (Optional) Enter a remark, which is **Devices of Office1** in this example.
4. Set **IP Address Range**, which is **192.168.2.100 ~ 192.168.2.200** in this example.
5. Set the maximum upload and download rates, which are **5 Mbps** and **10 Mbps** in this example.
6. Click **Add**.




**---End**

If the rule is added successfully, it is displayed as shown below.

| ID | Remark | IP Address Range | Max. Upload Rate | Max. Download Rate | Status | Action |
|---|---|---|---|---|---|---|
| 1 | Devices of... | 192.168.2.100~192.168.2.200 | 5Mbps | 10Mbps | Enable | |
| 10 Datas/Page | 1 data in total | | | | | |

## Verification

For a client whose IP address is within the range of 192.168.2.100 to 192.168.2.200, its maximum upload rate is 5 Mbps and its maximum download rate is 10 Mbps.

# 7.4 Port forwarding

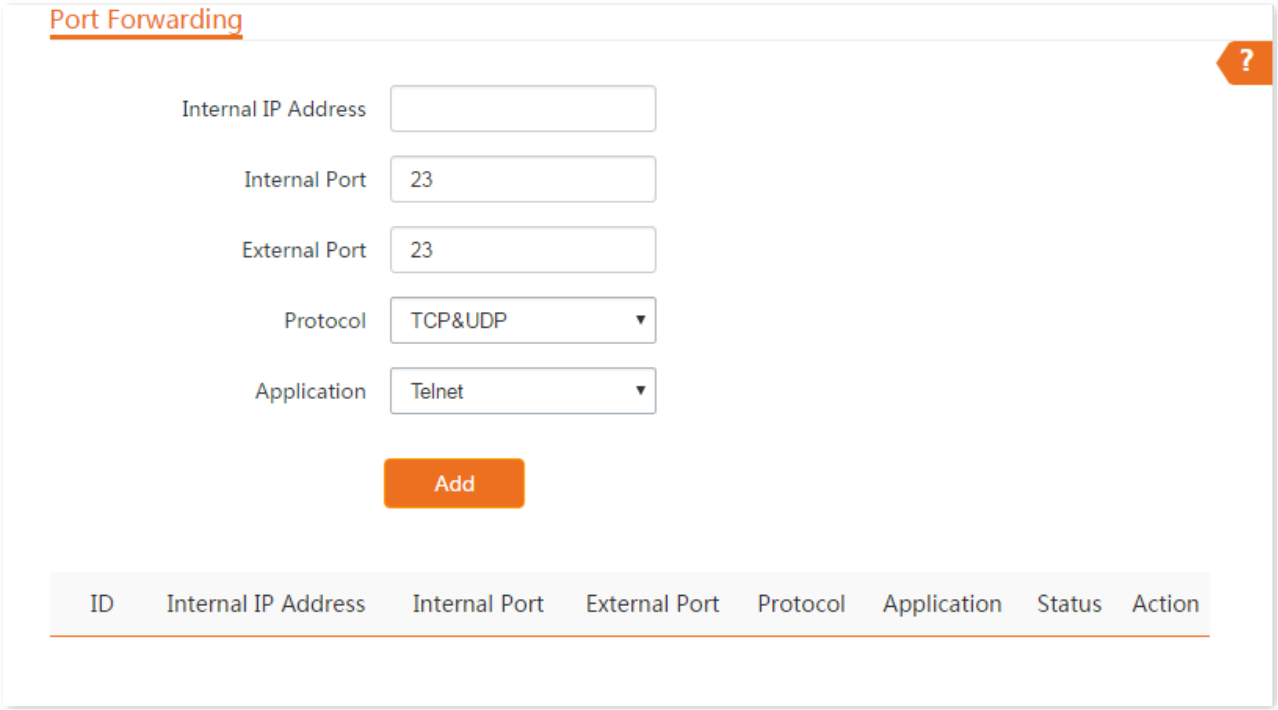
## 7.4.1 Overview

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

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

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Port Forwarding**. The following figure is for reference only.




**Parameters description**

| Name | Description |
|---|---|
| Internal IP Address | Specifies the IP address of the host that establishes a server in LAN. |
| Internal Port | Specifies the service port of the server in LAN.<br>After you select an **Application**, this option will be populated automatically. You can also customize it. |

| Name | Description |
| --- | --- |
| External Port | Specifies the ports through which WAN users can access the corresponding servers on the LAN.<br>After you select an **Application**, this option will be populated automatically. You can also customize it. |
| Protocol | Specifies the protocol type of the selected applications. Select **TCP&UDP** when you are not sure. |
| Application | Specifies the application services established in LAN. After you select an application, the internal and external ports will be populated. |
| Status | Specifies the status of the rule. You can enable or disable it according to your need. |
| Action | Click to delete the rule. |

## 7.4.2 Example of configuring port forwarding

### Networking requirements

An enterprise uses the CPE to set up a network. The CPE is in WISP mode and has connected to the internet. Now the intranet web server is required to be open to internet users to enable staff to access the intranet even when they are outside the enterprise.

### Solution

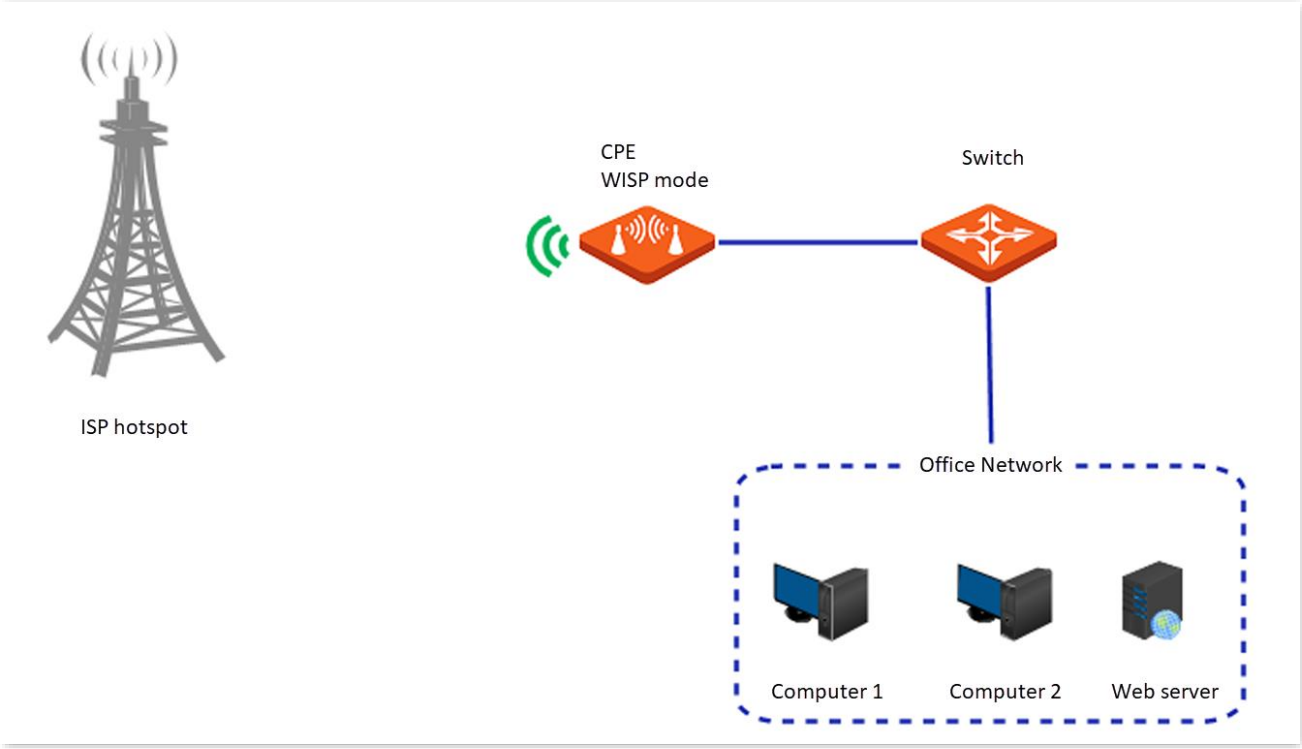
You can use the port forwarding function to enable internet users to access the intranet web server.

Assume that:

- WAN IP Address of the CPE: **202.105.11.22**
- IP Address of the web server: **192.168.2.100**
- Service port: **9999**

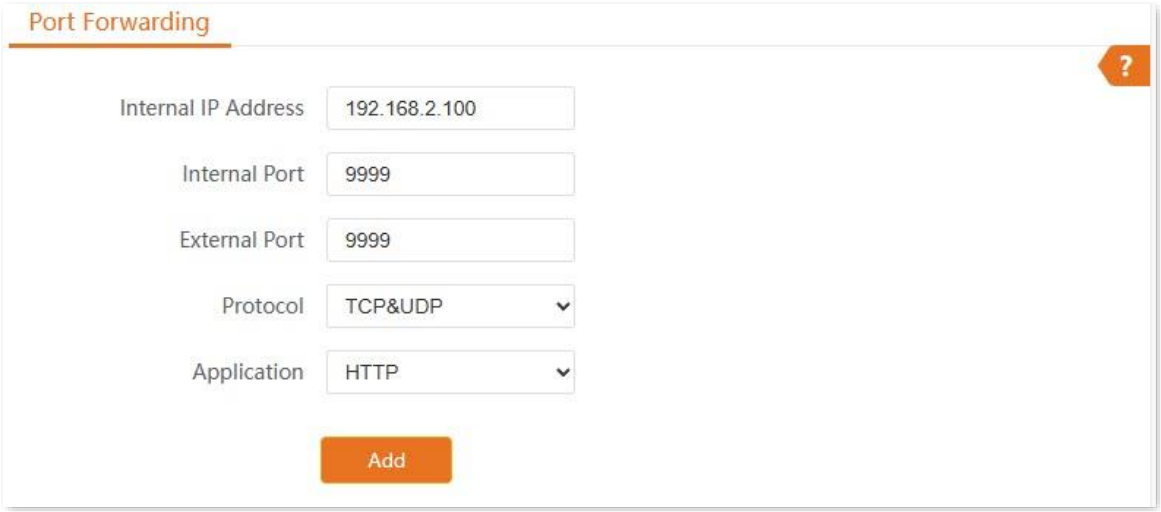
TIP

- Before configuration, ensure that the WAN port of the CPE obtains a public IP address. If the WAN port obtains a private IP address or an intranet IP address assigned by the ISP, the function may not take effect. Common IPv4 addresses can be class A, class B and class C. The private IP address ranges: Class A: 10.0.0.0-10.255.255.255, Class B: 172.16.0.0-172.31.255.255, Class C: 192.168.0.0-192.168.255.255.
- ISPs may not support unreported web service accessed using the default port number 80. When setting port mapping, you are recommended to set the external port as an uncommon port (1024 to 65535), such as 9999, to ensure normal access.
- Internal and external ports can be different.




## Configuration procedure

1. Log in to the web UI of the CPE, then navigate to **Advanced** > **Port Forwarding**.
2. Set **Internal IP Address**, which is **192.168.2.100** in this example.
3. Set **Internal Port** and **External Port**, which are **9999** in this example.
4. Set **Protocol**, which is **TCP&UDP** in this example.
5. Set **Application**, which is **HTTP** in this example.
6. Click **Add**.




**---End**

If the rule is added successfully, it is displayed as shown below.




### Verification

Internet users can successfully access the intranet server by using the **Intranet service application layer protocol name**://**WAN port IP address**. If the intranet service port is not the default port number, the access address is **Intranet service application layer protocol name**://**WAN port IP address**:**External port**.

In this example, the access address is http://202.105.11.22:9999.

You can find the current WAN port IP address in System Status.

If DDNS is enabled on the WAN port, internet users can also access the intranet server by using **Intranet service application layer protocol name://WAN port domain name:External port**.

TIP

If internet users cannot access the server on the LAN after configuration, try the following solutions:

- Ensure that the WAN IP address of the CPE 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 server may cause port forwarding function failures. Disable them and try again.
- Manually set an IP address and related parameters for the server to avoid the service disconnection caused by the dynamic IP address.

## 7.5 MAC filter

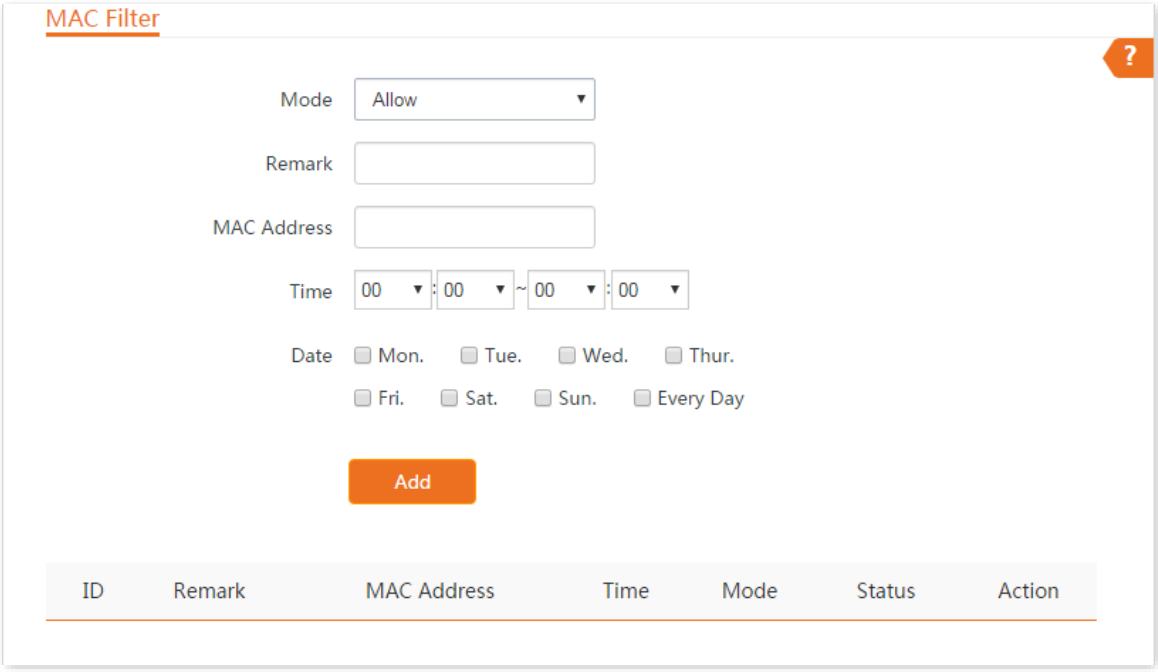
This function is available only when the CPE works in WISP or Router mode.

### 7.5.1 Overview

The MAC Filter function enables you to restrict access to devices by their MAC addresses at specific times.

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **MAC Filter**.

The function is disabled by default. Set the mode to **Allow**, and the page is shown below. The following figure is for reference only.




### Parameters description

| Name | Description |
|---|---|
| Mode | Specifies the mode of MAC filter rule.<br>- **Disable**: Disable the MAC Filter function.<br>- **Allow**: Only allow devices with the MAC addresses in the list to access the internet with the CPE during a specified period.<br>- **Disallow**: Only disallow devices with the MAC addresses in the list to access the internet with the CPE during a specified period. |
| Remark | Specifies the description of the rule. |
| MAC Address | Specifies the MAC address of the client to which the rule applies. |
| Time | Specifies the period at which the rule takes effect. |
| Date | Specifies the dates on which the rule takes effect. |
| Status | Specifies the status of the rule. You can enable or disable the rule according to your needs. |
| Action | Click to delete the rule. |

## 7.5.2 Example of configuring MAC filter

### Networking requirements

An enterprise uses the CPE to set up a network. The CPE is in WISP mode and has connected to the internet.

**Requirements**: Allow internet access to a purchasing employee from 8:00 to 18:00, Monday to Friday.

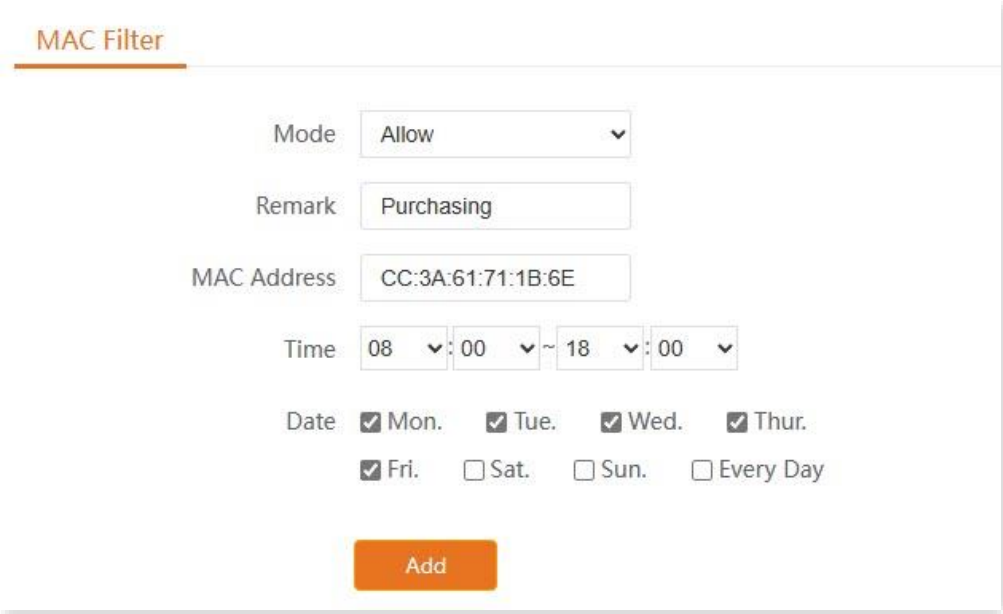
### Solution

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

Assume that the MAC address of the purchasing employee's computer is **CC:3A:61:71:1B:6E**.

### Configuration procedure

1. Log in to the web UI of the CPE, then navigate to **Advanced** > **MAC Filter**.
2. Select a mode, which is **Allow** in this example.
3. (Optional) Set **Remark**, which is **Purchasing** in this example.
4. Set the **MAC Address** of the device, which is **CC:3A:61:71:1B:6E** in this example.
5. Specify a period, which is **8:00** to **18:00** in this example.
6. Tick the dates, which are **Mon.** to **Fri.** in this example.
7. Click **Add**.




**---End**

If the rule is added successfully, it is displayed as shown below.




### Verification

Only the computer with the MAC address CC:3A:61:71:1B:6E can access the internet from 8:00 to 18:00, Monday to Friday. Other computers are blocked during this period.

# 7.6 Network service

## 7.6.1 DDNS

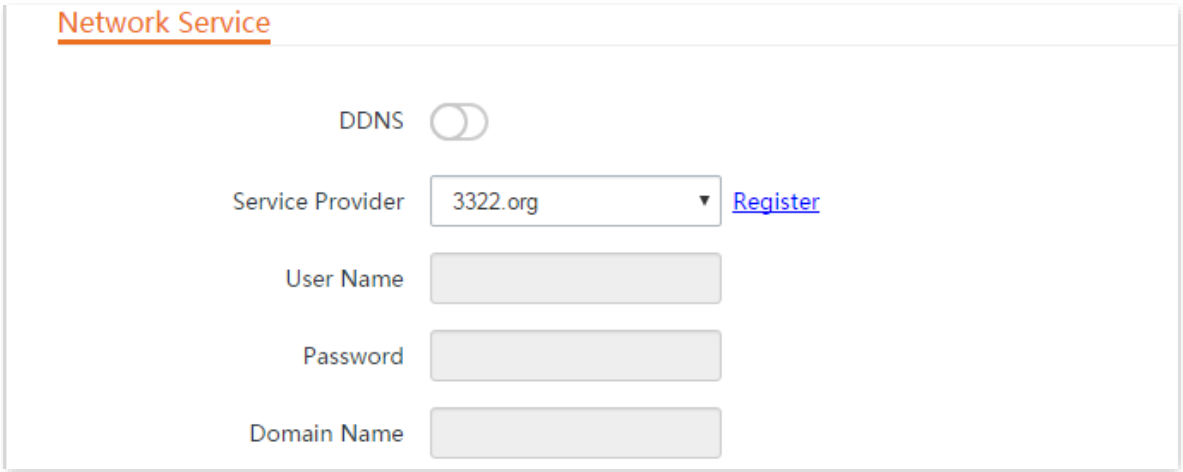
### Overview

The DDNS function is available only when the CPE works in WISP or Router mode.

DDNS, short for Dynamic DNS, enables the dynamic DNS client on the CPE 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.

On this page, you can map the dynamic WAN IP address of the CPE (public IP address) to a fixed domain name. The DDNS function is generally used with such functions as port forwarding and DMZ host to enable internet users to access the LAN server or the web UI of the CPE through a domain name without needing to track changes to the WAN IP address.

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**.



**Parameters description**

| Name | Description |
| --- | --- |
| DDNS | Specifies whether to enable the DDNS function. |
| Service Provider | Specifies Dynamic Domain Name Service (DDNS) provider. |
| User Name | Specify the user name and password used to log in to the dynamic DNS service, which are the login user name and password you registered on the website of the service provider. |
| Password | |
| Domain Name | Specifies the domain name information obtained from the dynamic DNS server. You need to enter the domain name you registered on the website. |

## Example of configuring DDNS

**Networking requirements**

An enterprise uses the CPE to set up a network. The CPE is in WISP mode and has connected to the internet.

**Requirement:** The intranet web server is open to internet users to enable staff to access the intranet even when they are outside the enterprise.

**Solution**

- You can use the Port Forwarding function to enable internet users to access the intranet web server.
- You can use the DDNS function to enable internet users to access the intranet web server through a fixed domain name, avoiding access failures caused by WAN IP address change.

Assume that:

The information of the web server in LAN is shown below:

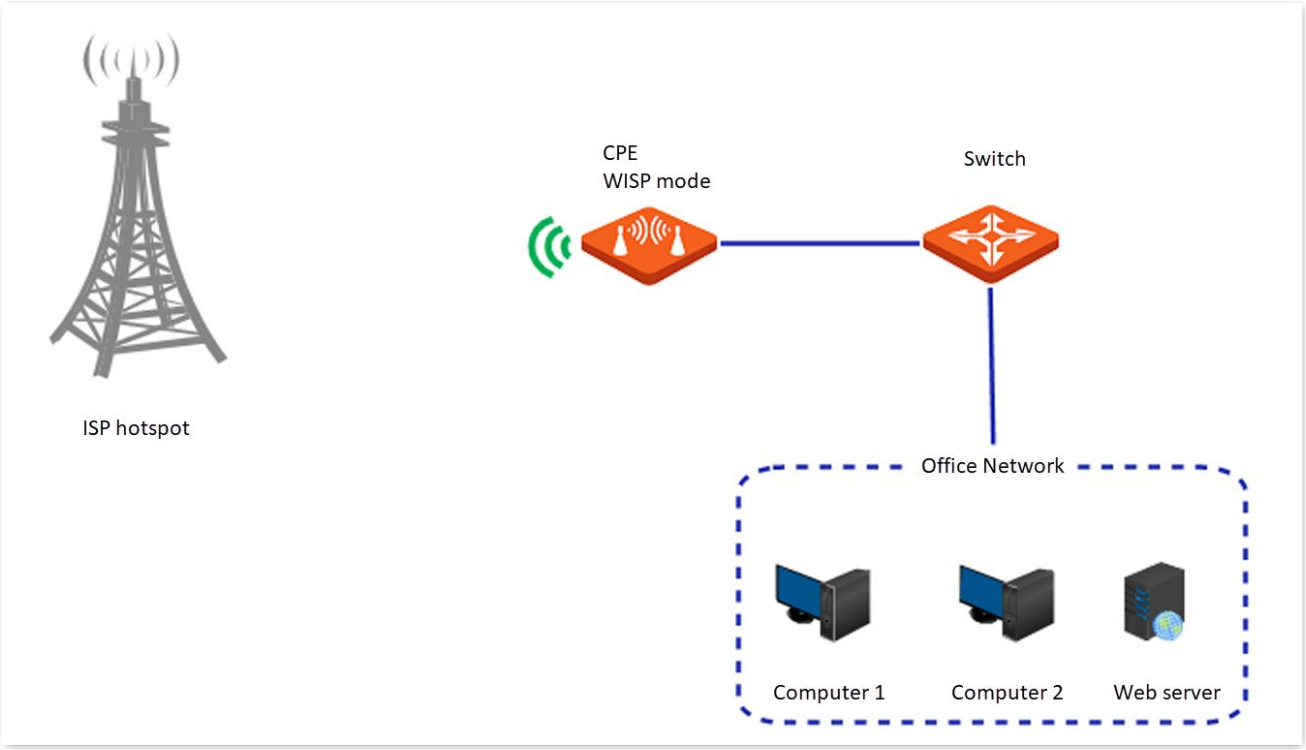
- IP Address: **192.168.2.100**
- Service Port of the Web Server: **9999**

The registered domain name information is shown below:

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

TIP

- Before configuration, ensure that the WAN port of the CPE obtains a public IP address. If the WAN port obtains a private IP address or an intranet IP address assigned by the ISP, the function may not take effect. Common IPv4 addresses can be class A, class B and class C. The private IP address ranges: Class A: 10.0.0.0-10.255.255.255, Class B: 172.16.0.0-172.31.255.255, Class C: 192.168.0.0-192.168.255.255.
- ISPs may not support unreported web service accessed using the default port number 80. Therefore, when setting port mapping, you are recommended to set the external port as an uncommon port (1024 to 65535), such as 9999, to ensure normal access.
- Internal and external ports can be different.




**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Set up the **DDNS** function.
   1) Navigate to **Advanced** > **Network Service**.
   2) Enable the **DDNS** function.
   3) Set **Service Provider** (the DDNS service provider with which you registered the domain name), which is **Dyndns** in this example.
   4) Set **User Name** and **Password** (registered with DDNS service provider), both of which are **JohnDoe** in this example.
   5) Set **Domain Name**, which is **JohnDoe.dyndns.com** in this example.
   6) Click **Save** at the bottom of this page.




3. Set up the port forwarding function.

   1) Navigate to **Advanced** > **Port Forwarding**.

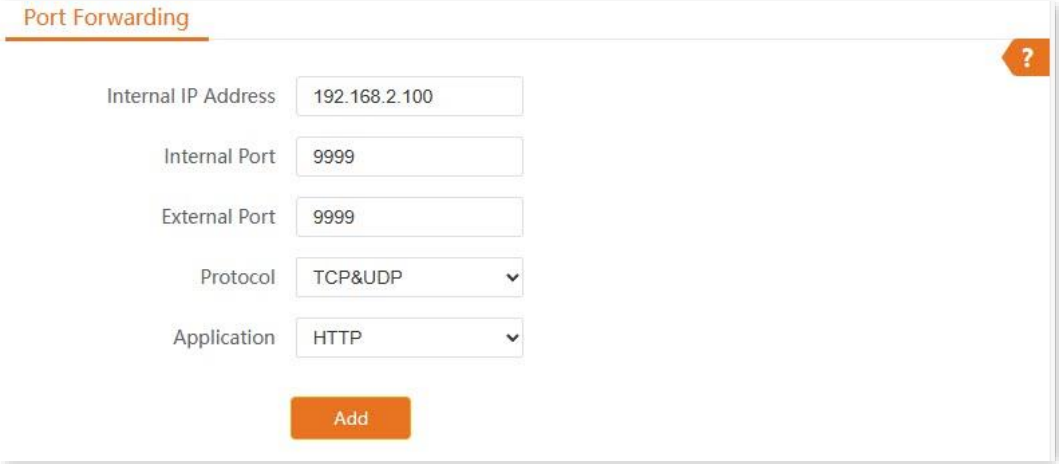
   2) Set **Internal IP Address**, which is **192.168.2.100** in this example.

   3) Set **Internal Port** and **External Port**, which are **9999** in this example.

   4) Set **Protocol**, which is **TCP&UDP** in this example.

   5) Set **Application**, which is **HTTP** in this example.

   6) Click **Add**.




**---End**

If the rule is added successfully, it is displayed as below.



**Verification**

Internet users can successfully access the intranet server by using the **Intranet service application layer protocol name**://**WAN port IP address**. If the intranet service port is not the default port number, the access address is **Intranet service application layer protocol name**://**WAN port IP address**:**External port**.

In this example, the access address is http://202.105.11.22:9999.

TIP

If internet users cannot access the server on the LAN after configuration, try the following solutions:

- Ensure that the WAN IP address of the CPE 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 server may cause port forwarding function failures. Disable them and try again.
- Manually set an IP address and related parameters for the server to avoid the service disconnection caused by the dynamic IP address.

## 7.6.2 Remote web management

### Overview

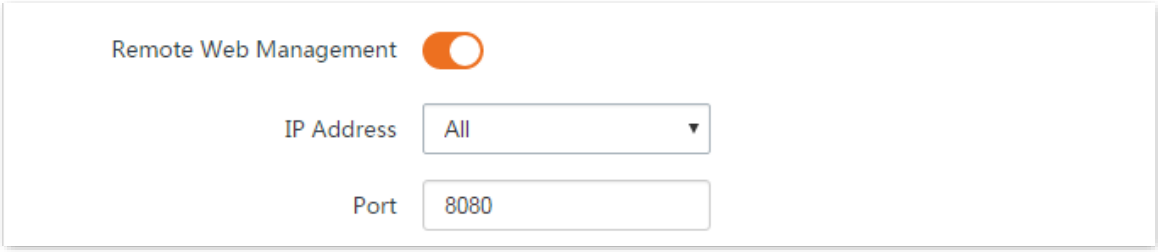
The Remote Web Management function is available only when the CPE works in WISP or Router mode.

Generally, you can log in to the web UI of the CPE only when you connect to the LAN port or the wireless network of the CPE. However, this function enables access to the web UI remotely through the WAN port in special cases (like when you need remote technical support).

You can access the CPE remotely by visiting an address in the form of **http://WAN port IP address:Port number**. If the DDNS function is enabled on the CPE, you can access the CPE by visiting an address in the form of **http://Domain name of WAN port:Port number**.

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**.

This function is disabled by default. After it is enabled, the page is shown as follows.



**Parameters description**

| Name | Description |
| --- | --- |
| Remote Web Management | Specifies whether to enable or disable the remote web management function. |
| IP Address | Specifies the IP address of a computer allowed to access the web UI of the CPE.<br>- **All**: It indicates that any computer in WAN can manage the CPE remotely. For security, this option is not recommended.<br>- **Manual**: It indicates that only the device with specified IP address can manage the CPE remotely. If the computer belongs to a LAN, enter the gateway address (a public IP address) of the computer. |
| Port | Specifies the port number used for remote management of CPE. Default: **8080**. You can change it as required.<br>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. |

## Example of configuring remote web management

**Networking requirements**

An enterprise uses the CPE to set up a network. The CPE is in WISP mode and has connected to the internet. The network administrator encountered a problem during network setup and needs the Tenda technical support to remotely log in to the web UI of the CPE to perform analysis and troubleshooting.

**Solution**

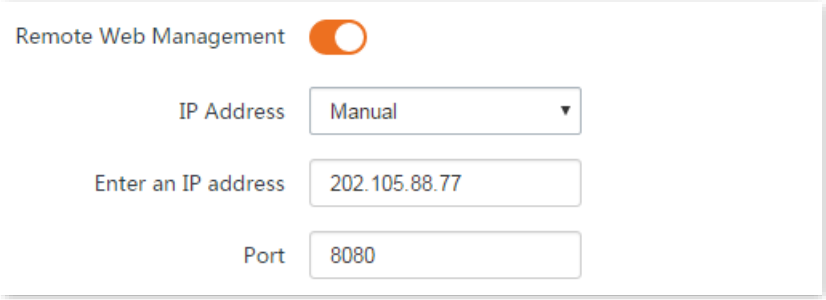
You can use the remote web management function to solve the problem.

Assume that:

- WAN IP address of the CPE: **202.105.106.55**
- IP address of the computer allowed to access the CPE: **202.105.88.77**
- Port number: **8080**

**Configuration procedure**

1. Log in to the web UI of the CPE, then navigate to **Advanced** > **Network Service**.
2. Enable the **Remote Web Management** function.
3. Set **IP Address** to **Manual**, then enter the IP address of the computer used by Tenda technical support, which is **202.105.88.77** in this example.
4. Set **Port**, which is **8080** in this example.
5. Click **Save** on the bottom of this page.




**---End**

**Verification**

The host can log in to the web UI of the CPE by visiting **http://202.105.106.55:8080** on the computer (the IP address of the computer is 202.105.88.77). If the DDNS function is enabled on the CPE, you can access the CPE by visiting an address in the form of **http://Domain name of WAN port:8080**.

## 7.6.3 Reboot schedule

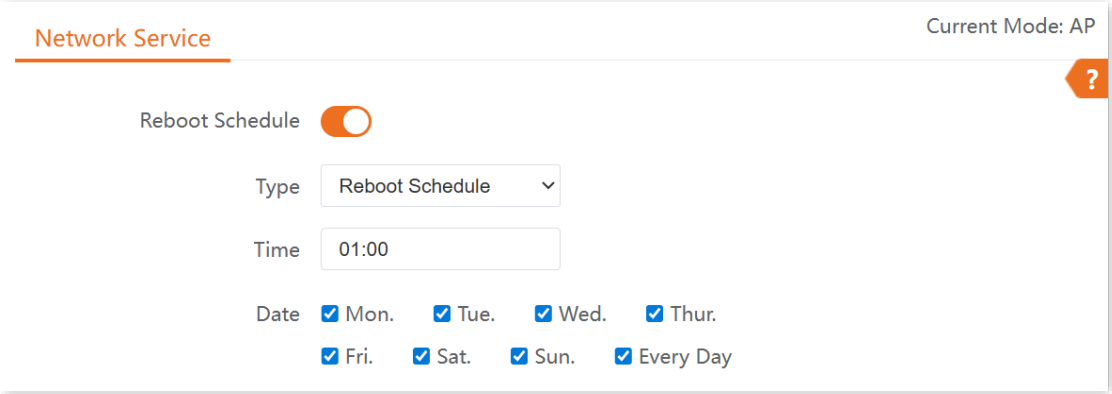
### Overview

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**.

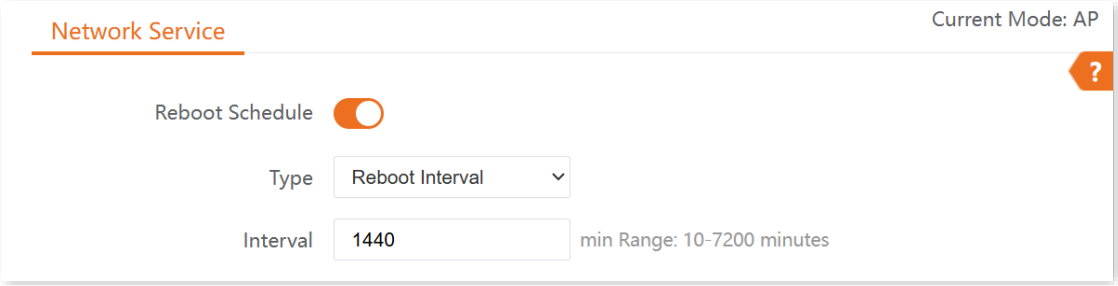
This function enables the CPE to automatically reboot as scheduled. You can use this function to prevent wireless performance degradation or network instability due to prolonged operation.

### Configuration procedure

1. Log in to the web UI of the CPE.
2. Navigate to **Advanced** > **Network Service**.
3. Enable the **Reboot Schedule** function.
4. Choose one reboot type.
   - **Reboot Schedule**: Set **Time** and **Date**, which is **01:00** and **Every Day** in this example.



- **Reboot Interval**: Set **Interval**, which is **1440** in this example.




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

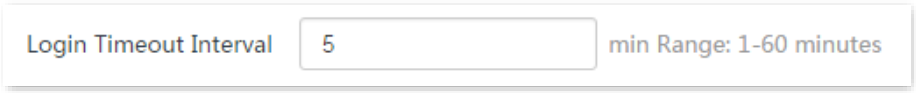
**---End**

When a reboot schedule is configured, the CPE will automatically reboot at 1 a.m. every day. When a reboot interval is configured, the CPE will automatically reboot every 1440 minutes.

## 7.6.4 Login timeout interval

If you log in to the web UI of the CPE and perform no operation within the login timeout interval, the CPE logs you out for network security. The default login timeout interval is 5 minutes. You can modify it as required.

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**.




## 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 receiving 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 an SNMP manager, an SNMP agent, and a 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 CPE 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.

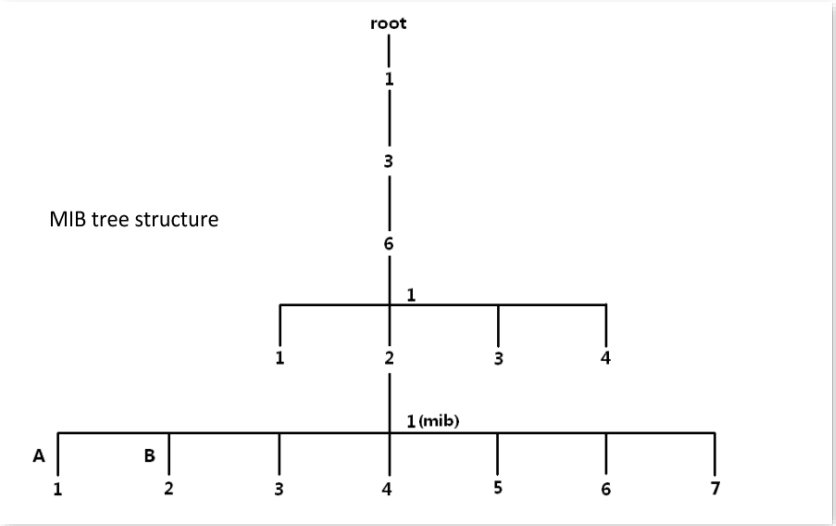
**SNMP protocol version**

The CPE is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. A 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.

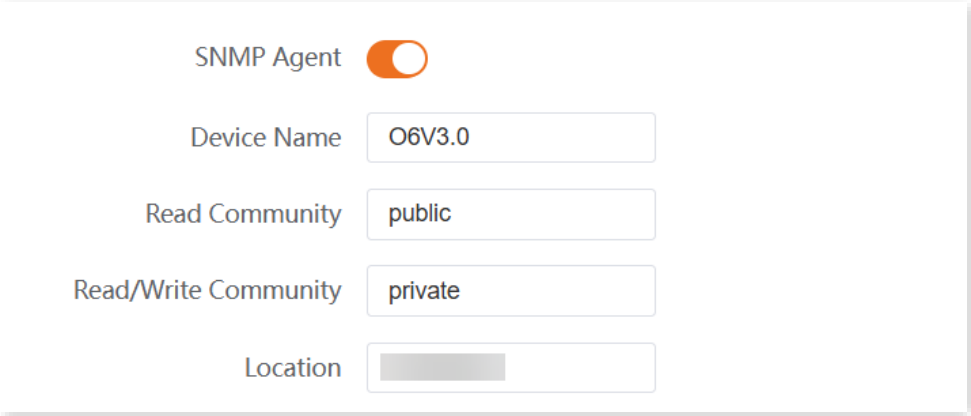
**MIB introduction**

A 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 called 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.




### SNMP agent basic configuration

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**.




### Parameter description

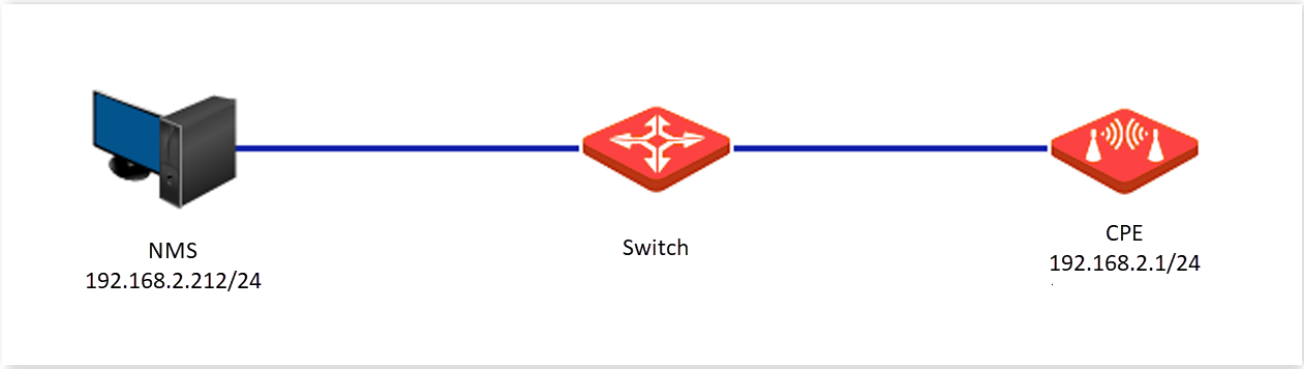
| Name | Description |
|---|---|
| SNMP Agent | Specifies whether to enable or disable the SNMP agent function of the CPE. By default, it is disabled.<br>An SNMP manager and the SNMP agent can communicate with each other only if their SNMP versions are the same. Currently, the SNMP agent function of the CPE supports SNMP V1 and SNMP V2C. |
| Device Name | Specifies the device name of the CPE. The default device name is assigned based on the model and version number of the CPE.<br>TIP<br>It is recommended that you change the device name so that you can easily identify the target CPE when managing it using SNMP. |

| Name | Description |
| --- | --- |
| Read Community | Specifies the read password shared between SNMP managers and this SNMP agent. The default password is **public**.<br>The SNMP agent function allows an SNMP manager to use the **Read Community** to read variables in the MIB of the CPE. |
| Read/Write Community | Specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is **private**.<br>The SNMP agent function allows an SNMP manager to use the **Read/Write Community** to read/write variables in the MIB of the CPE. |
| Location | Specifies the location where the CPE is used. You can change the location as required. |

## Example of configuring the SNMP function

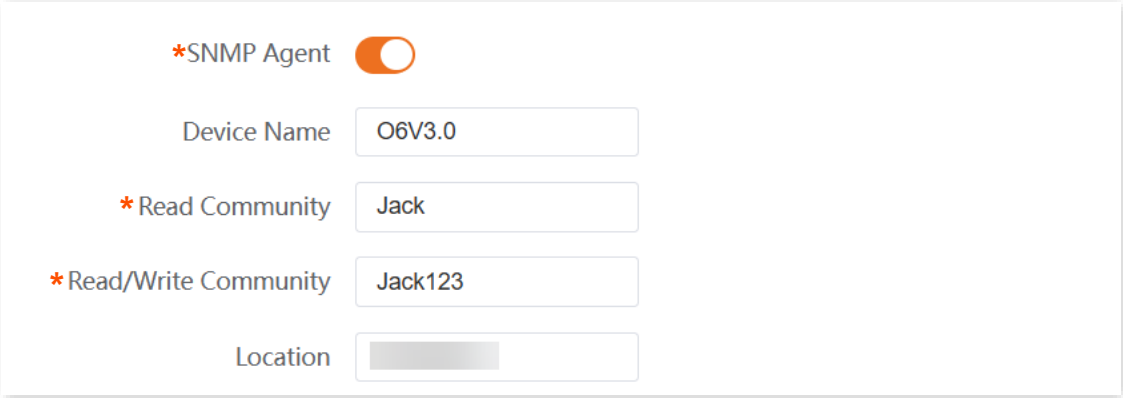
### Networking requirements

- The CPE connects to an NMS over a LAN. The IP address of the CPE is 192.168.2.1/24 and the IP address of the NMS is 192.168.2.212/24.
- The NMS uses SNMP V1 or SNMP V2C to monitor and manage the CPE.
- Assume that **Read Community** is **Jack**, and **Read/Write Community** is **Jack123**.




### Configuration procedure

1. Set up the CPE.
   1) Log in to the web UI of the CPE.
   2) Navigate to **Advanced** > **Network Service**.
   3) Enable the **SNMP Agent** function.
   4) Set **Read Community**, which is **Jack** in this example.
   5) Set **Read/Write Community**, which is **Jack123** in this example.
   6) Click **Save**.




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 user guide for the NMS.

   **---End**

**Verification**

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

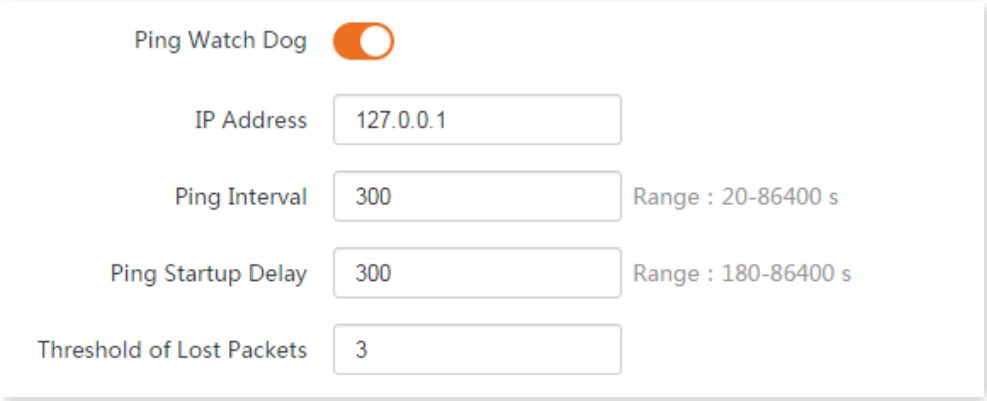
## 7.6.6 Ping watch dog

The Ping watch dog is a fail-proof for the CPE, which is dedicated to continuously monitoring the specific connection mechanism between the CPE and the remote host using the Ping tool.

With this function enabled, the CPE periodically pings a target IP address to check connectivity. If the target does not respond for the configured number of attempts, the CPE reboots automatically to try to restore connectivity.

**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Advanced** > **Network Service**.
3. Enable the **Ping Watch Dog** function.
4. Set parameters as required.
5. Click **Save** on the bottom of this page.




**---End**

**Parameters description**

| Name | Description |
|---|---|
| Ping Watch Dog | Specifies whether to enable or disable the Ping Watch Dog function. |
| IP Address | Specifies the target IP address that the CPE pings. |
| Ping Interval | Specifies the interval at which the CPE transmits packets to ping the target IP address. The default value is 300 s. |
| Ping Startup Delay | Specifies the delay time for the CPE to enable the Ping Watch Dog function after the CPE startup completes. The default value is 300s.<br>Setting a proper Ping startup delay time can stop the Ping Watch Dog function from being triggered during the startup of the CPE. Such triggering leads to failure of accessing the web UI to modify the settings, causing the CPE to start up continuously. |
| Threshold of Lost Packets | Specifies the threshold of lost packets that triggers a reboot. The value range is 1 to 65535. The default value is 3.<br>For example, if 5 is set, the CPE will reboot automatically when it does not receive a response after sending five ping requests to the target IP address or domain name. |

## 7.6.7 DMZ host

### Overview

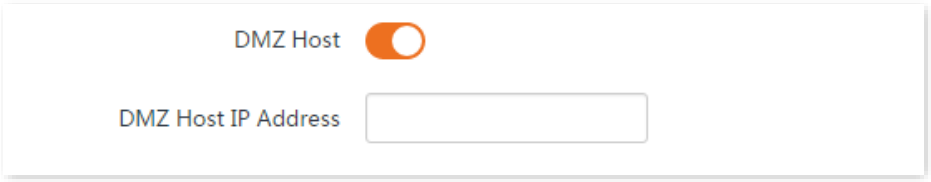
The DMZ function is available only when the CPE works in WISP or Router mode.

After a device in the LAN is set as the DMZ host, the device enjoys no limitations when communicating with the internet. For example, if video meeting or online games are underway on a computer, you can set that computer as the DMZ host to make the video meeting and online games go smoother.

NOTE

- After you set a LAN device as a DMZ host, the device will be completely exposed to the internet and the firewall of the CPE does not take effect on this device.
- Hackers may attack the local network by using the DMZ host. Use the DMZ host function with caution.
- Security software, antivirus software, and the system firewall on the DMZ host may affect the DMZ function. Disable them when using this function. When you are not using the DMZ function, you are recommended to disable the function and enable the firewall, security guard and anti-virus software on the DMZ host.

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**.




**Parameters description**

| Name | Description |
|---|---|
| DMZ Host | Specifies whether to enable the DMZ host function of the CPE. By default, it is disabled. |
| DMZ Host IP Address | Specifies the IP address of the LAN device to be set to DMZ host. |

## Example of configuring DMZ host

**Networking requirements**

An enterprise uses the CPE to set up a network. The CPE is in WISP mode and has connected to the internet.

The intranet web server needs to be accessible to staff even when they are outside the enterprise.

**Solution**

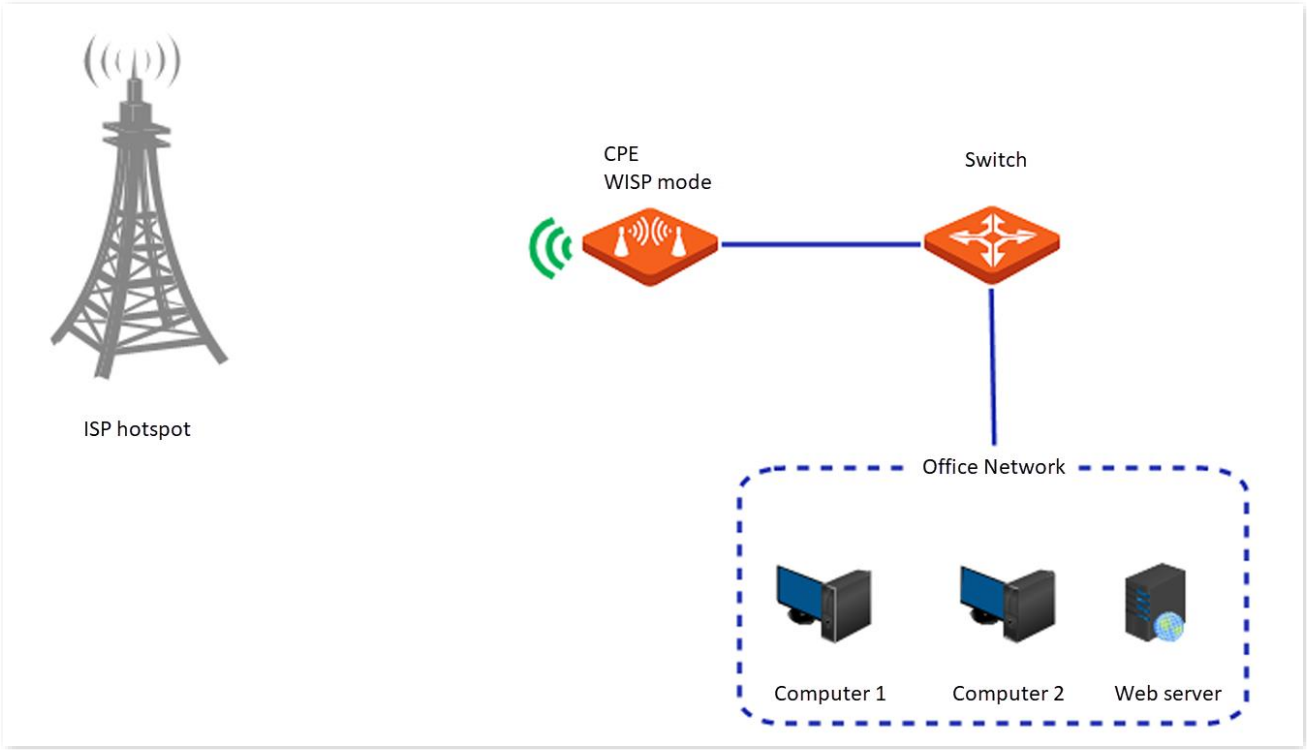
You can use DMZ Host function to solve the problem.

Assume that:

- WAN IP address of the CPE: **202.105.106.55**
- Internal web server IP Address: **192.168.2.100**
- Port number: **9999**

TIP

- Before the configuration, ensure that the WAN port of the CPE obtains a public IP address. If the WAN port obtains a private IP address or an intranet IP address assigned by the ISP, the function may not take effect. Common IPv4 addresses can be class A, class B and class C. Private IP address ranges: Class A: 10.0.0.0-10.255.255.255, Class B: 172.16.0.0-172.31.255.255, Class C: 192.168.0.0-192.168.255.255.
- ISPs may not support unreported web service accessed using the default port number 80. Therefore, when setting the DMZ host, you are recommended to set the internal port as an uncommon port (1024 to 65535), such as 9999, to ensure normal access.




**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Advanced** > **Network Service**.
3. Enable the **DMZ Host** function.
4. Set **DMZ Host IP Address**, which is **192.168.2.100** in this example.
5. Click **Save** on the bottom of this page.




**---End**

**Verification**

Internet users can successfully access the intranet server by using the **Intranet service application layer protocol name**://**WAN port IP address**. If the intranet service port is not the default port number, the access address is **Intranet service application layer protocol name**://**WAN port IP address**:**Intranet service port**.

In this example, the access address is http://202.105.106.55:9999.

You can find the current WAN port IP address in System status.

If DDNS is enabled on the WAN port, internet users can also access the intranet server by using **Intranet service application layer protocol name://WAN port domain name: Intranet service port**.

TIP

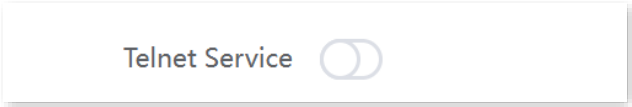
If internet users cannot access the server on the LAN after configuration, try the following solutions:

- Ensure that the WAN IP address of the CPE is a public IP address.
- Security software, antivirus software, and the built-in OS firewall of the server may cause the function to fail. Disable them and try again.
- Manually set an IP address and related parameters for the server to avoid the service disconnection caused by the dynamic IP address.

## 7.6.8 Telnet service

With this function enabled, the CPE can be managed through Telnet. Generally, this function is used to maintain the CPE by technical professionals.

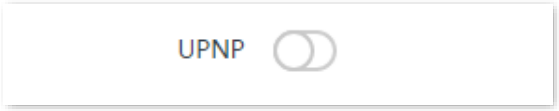
To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**. By default, the function is disabled. You can enable it as required.




## 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 BitComet. To use this function, ensure that the operating system supports UPnP, or application software supporting UPnP is installed.

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**. By default, the function is disabled. You can enable it as required.

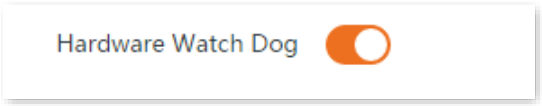



## 7.6.10 Hardware watch dog

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

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Network Service**.

By default, the function is enabled.



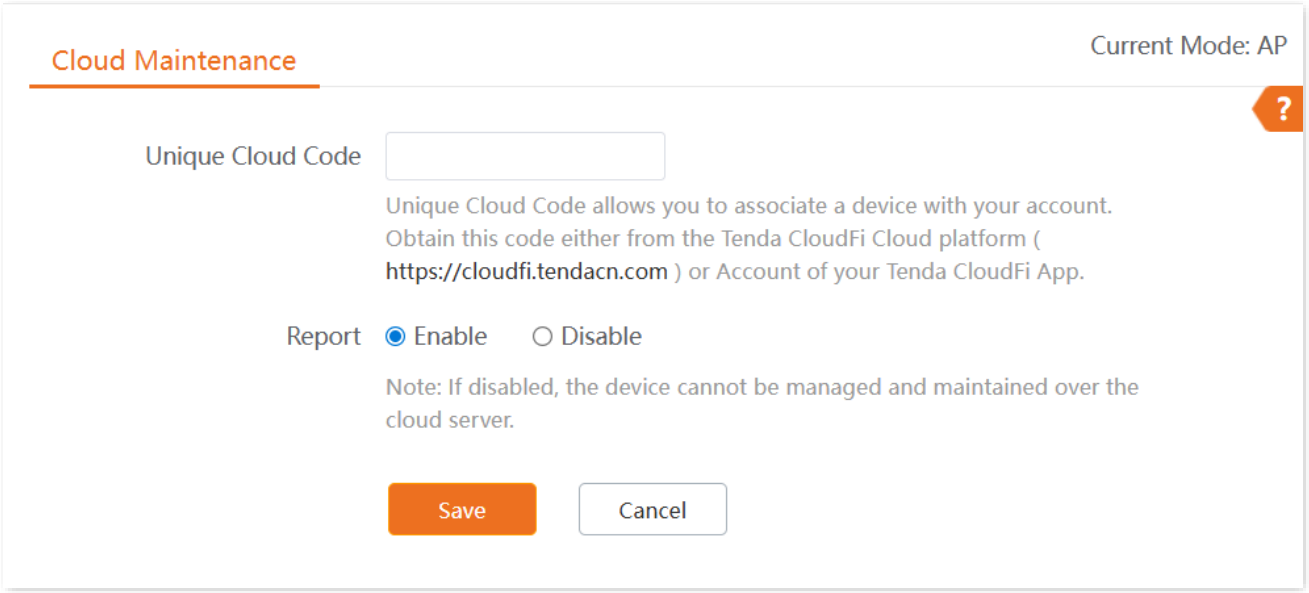

## 7.6.11 Cloud maintenance

### Overview

The Tenda CloudFi Cloud management system is a cloud platform for centrally managing Tenda devices.

You can remotely manage your CPE after adding the device to the cloud via the Tenda CloudFi Cloud web portal (https://cloudfi.tendacn.com) or the Tenda CloudFi App.

To access the page, log in to the web UI of the CPE and navigate to **Advanced** > **Cloud Maintenance**.



### Parameters description

| Name | Description |
| --- | --- |
| Unique Cloud Code | Specifies the Unique Cloud Code used to associate the device with a Tenda CloudFi Cloud account or project. You can obtain the code from the Tenda CloudFi Cloud web portal (https://cloudfi.tendacn.com) or the Tenda CloudFi App. |
| Report | CPEs can be managed via the Tenda CloudFi Cloud platform only after the report function is enabled. The device configuration data will then be reported to the platform. |

## Example of configuring cloud maintenance

### Networking requirements

CPEs can be managed through the Tenda CloudFi App or the Tenda CloudFi Cloud web portal (https://cloudfi.tendacn.com), with all settings delivered by the cloud.

### Configuration procedure

TIP

- Before configuring cloud maintenance, ensure that the CPE can access the network.
- Data are synced automatically between the Tenda CloudFi App and Tenda CloudFi Cloud web portal.

or

GET IT ON Google Play

Download on the App Store

### Option 1: Use Tenda CloudFi App

1. Download the Tenda CloudFi App to your phone by scanning the QR code or searching for **Tenda CloudFi** in Google Play or App Store.

   TIP

   If the Tenda CloudFi App is already installed, ensure it is updated to the latest version.

2. Connect your phone to the CPE's Wi-Fi network.
3. Open your Tenda CloudFi App, then add the CPE.
   1) Create a new project (skip this step if projects exist).

2) Enter the project.

3) Tap the pop-up window that shows the CPE is detected, then add the device to the project.

For more details, see the help guide in the Tenda CloudFi App's Help Center.

**---End**

**Option 2: Use Tenda CloudFi Cloud web portal**

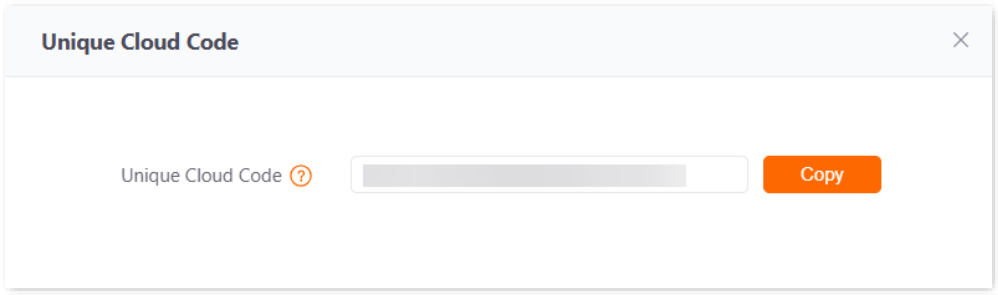
TIP

Tenda CloudFi Cloud web portal V0.8.80 is used for illustration here. The actual operations and interface are subject to the version in use.

1. Obtain the Unique Cloud Code.

   1) On the computer connected to the internet, visit https://cloudfi.tendacn.com via the browser and log in to the Tenda CloudFi Cloud web portal.

   2) Click **Add** > **Unique Cloud Code**, then copy the code.




2. Enable and configure cloud maintenance on the CPE.

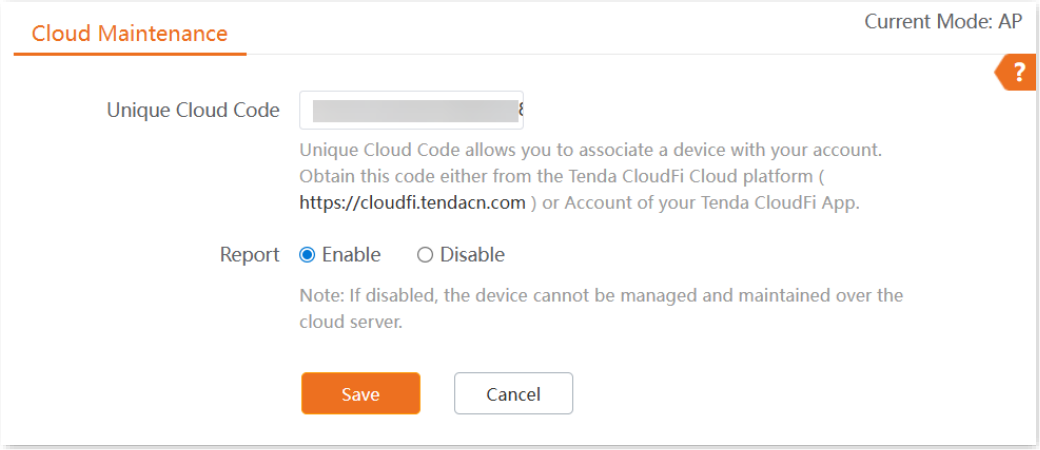
   1) Log in to the web UI of the CPE and navigate to **Advanced** > **Cloud Maintenance**.

   2) Set cloud maintenance parameters.

   3) Paste the code in step 1, substep 2) into the field.

   4) Enable the **Report** function.

   5) Click **Save**.




3. Add the CPE to the project.

   1) On the computer connected to the internet, visit https://cloudfi.tendacn.com via the browser and log in to the Tenda CloudFi Cloud web portal.

   2) Click **Add** > **Device-joining Alert**.

   3) Locate the CPE and add it to the project.

   **---End**

**Verification**

After the setup is completed, the CPE can be managed through the Tenda CloudFi App and its web portal, with all configuration data delivered via the cloud.

# 8 Tools

Features available in the CPE may vary by model and software version. CPE availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual CPE experience.

## 8.1 Date & time

To access the page, log in to the web UI of the CPE and navigate to **Tools** > **Date & Time**.

This module enables you to set the system time of the CPE. Ensure that the CPE's system time is accurate so that time-based functions work correctly.

The system time of the CPE can be synchronized with the internet or manually configured. By default, it is configured to synchronize the system time with the internet.

TIP

When you log in to the web UI of the CPE, the system time will be synchronized with the management host automatically no matter which time setting method you choose.

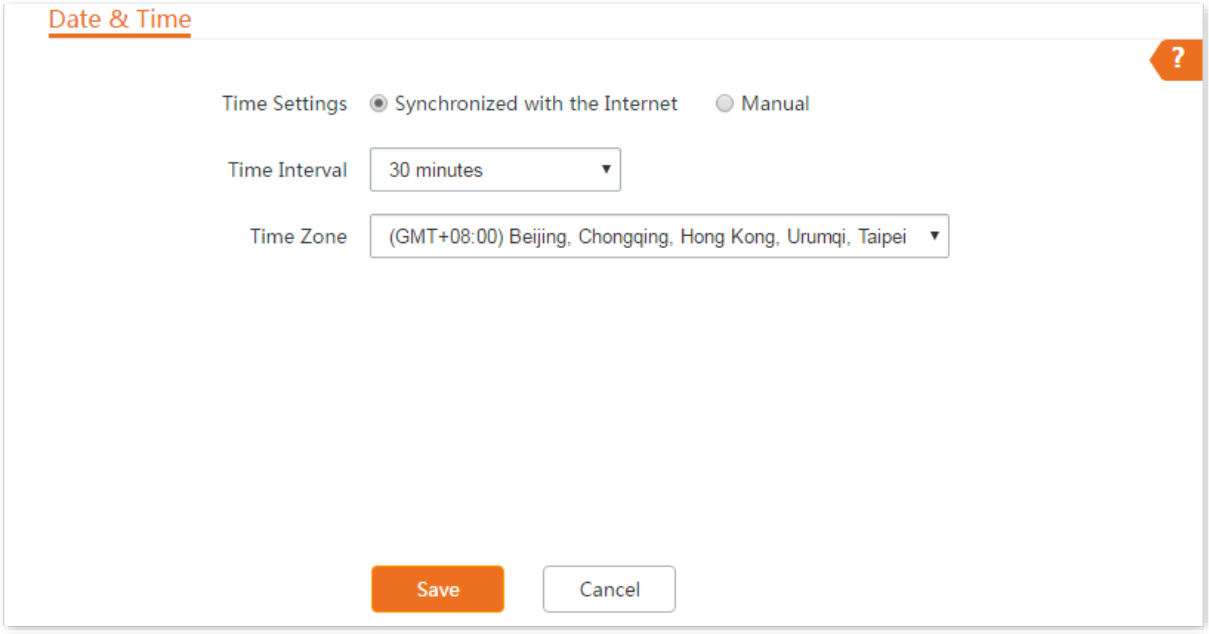
### 8.1.1 Sync system time with internet

The CPE automatically synchronizes its system time with a time server on the internet. This enables the CPE to automatically correct its system time after being connected to the internet.

For details about how to connect the CPE to the internet, refer to LAN setup.

**Configuration Procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Tools** > **Date & Time**.
3. Set Time Settings to Synchronized with the Internet.
4. Set **Time Interval**. The default value of **30 minutes** is recommended.
5. Set **Time Zone** to your time zone.
6. Click **Save**.




**---End**

After the configuration is successful, you can navigate to Status page to check whether the system time of the CPE is correct. The following figure is for reference only.

**Parameters description**

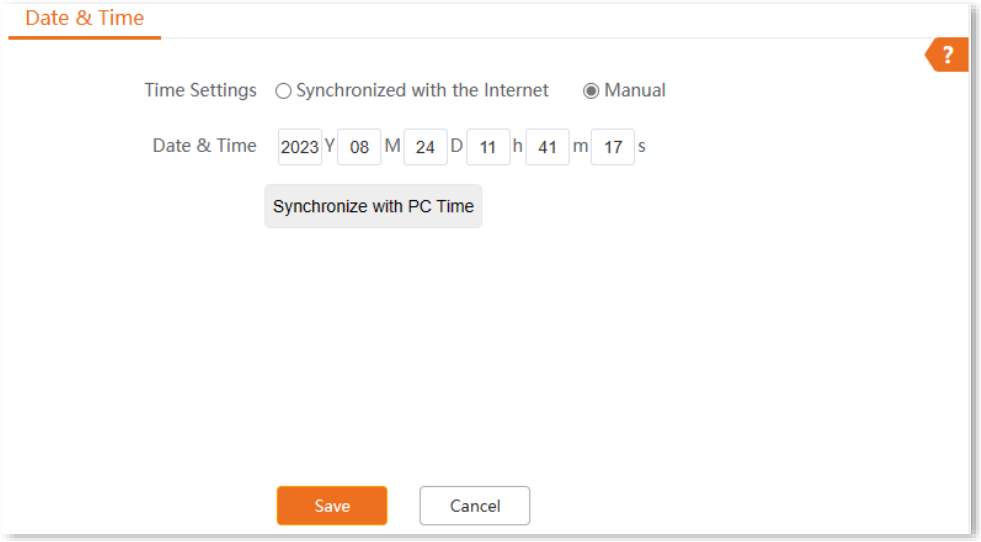
| Name | Description |
|---|---|
| Time Settings | Specifies the method to set the system time of the CPE. |
| Time Interval | Specifies the interval to synchronize the system time of the CPE with the time server on the internet. |
| Time Zone | Specifies the standard time zone where the CPE is located. |

## 8.1.2 Set system time manually

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

**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Tools** > **Date & Time**.
3. Set **Time Settings** to **Manual**.
4. Set **Date & Time**, or click **Synchronize with PC Time** to synchronize the system time of the CPE with the system time of the computer being used to manage the CPE.
5. Click **Save**.




**---End**

After the configuration is successful, you can navigate to Status page to check whether the system time of the CPE is correct. The following figure is for reference only.

**Parameters description**

| Name | Description |
|---|---|
| Time Settings | Specifies the method to set the system time of the CPE. |
| Date & Time | You can either enter the accurate time in this field, or click **Synchronize with PC Time** to synchronize the system time of the CPE with the management computer. |

# 8.2 Maintenance

## 8.2.1 Reboot device

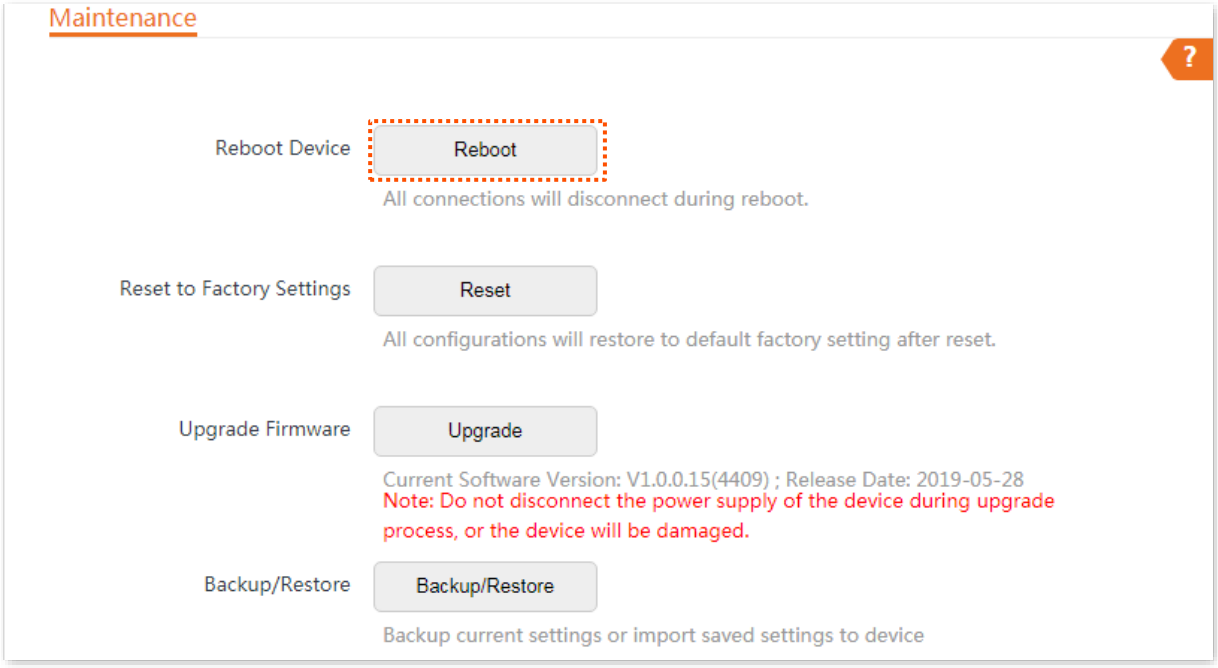
If your settings do not take effect or the CPE works improperly, you can try rebooting the CPE to resolve the problem.

TIP

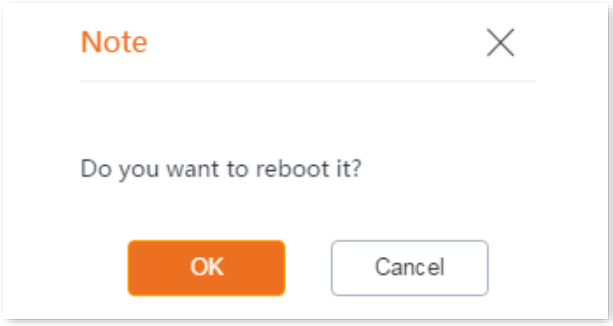
When the CPE reboots, the current connections will be disconnected. Perform this operation when the CPE is idle.

**Configuration procedure**

1. Log in to the web UI of the CPE.
2. Navigate to **Tools** > **Maintenance**.
3. Click **Reboot**.




4. Confirm the prompt information, and click **OK**.




**---End**

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

## 8.2.2 Restore to factory settings

If you forget the login password of the web UI, you can reset the CPE to restore its factory settings and then configure it again.

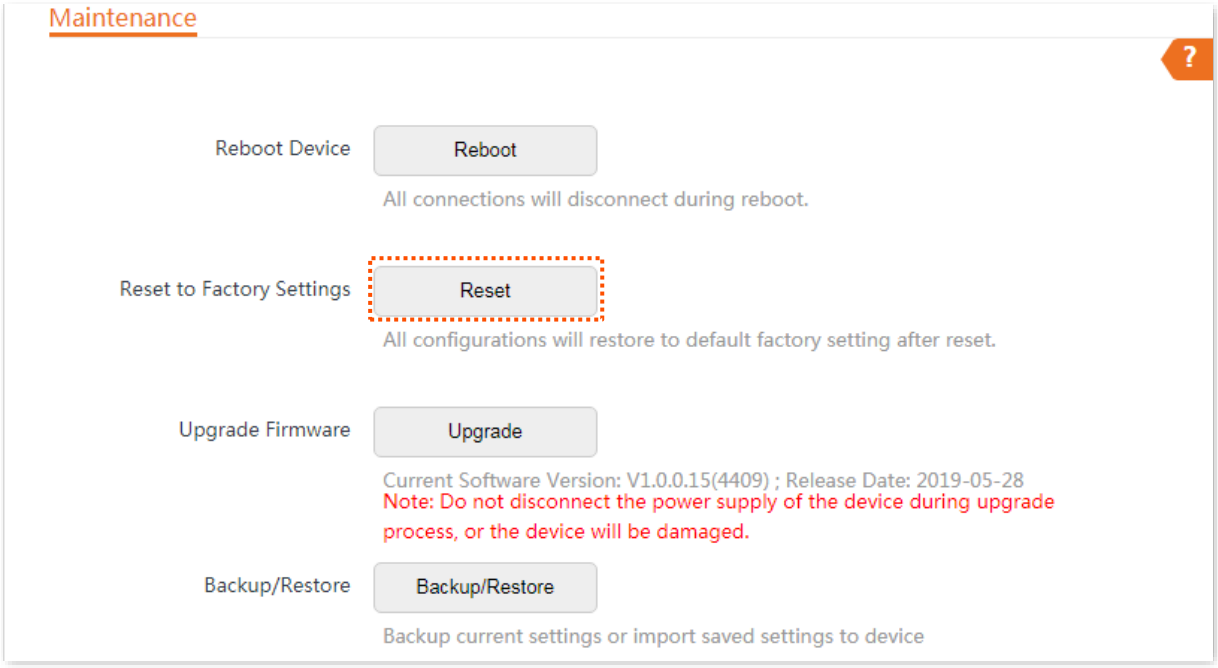
NOTE

- Restoring factory settings removes all user-configured settings and restores the defaults. Perform this operation only when necessary.
- To prevent damage to the CPE, do not power off the CPE during the factory reset.

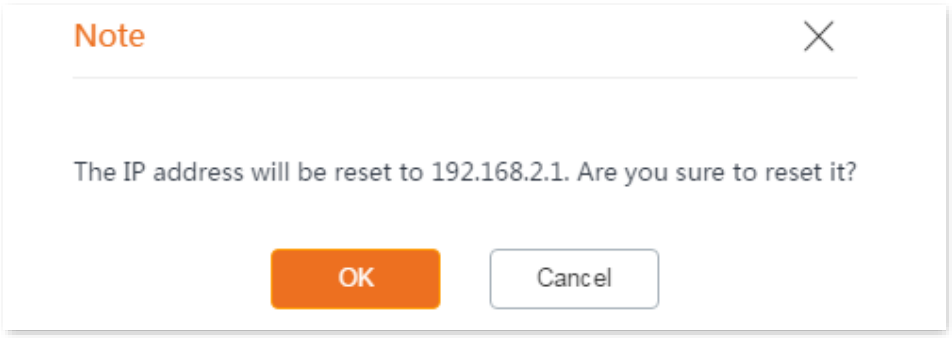
### Option 1: Reset the CPE through the web UI

1. Log in to the web UI of the CPE.

2. Navigate to **Tools** > **Maintenance**.
3. Click **Reset**.




4. Confirm the prompt information, and click **OK**.




**---End**

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

### Option 2: Reset the CPE through the Reset button

After the CPE completes startup, hold down the reset button (RST, RESET or Reset) for about 8 seconds, then release it when all the indicators light up. The CPE will be reset.

## 8.2.3 Upgrade firmware

This function upgrades the firmware of the CPE for more functions and higher stability.

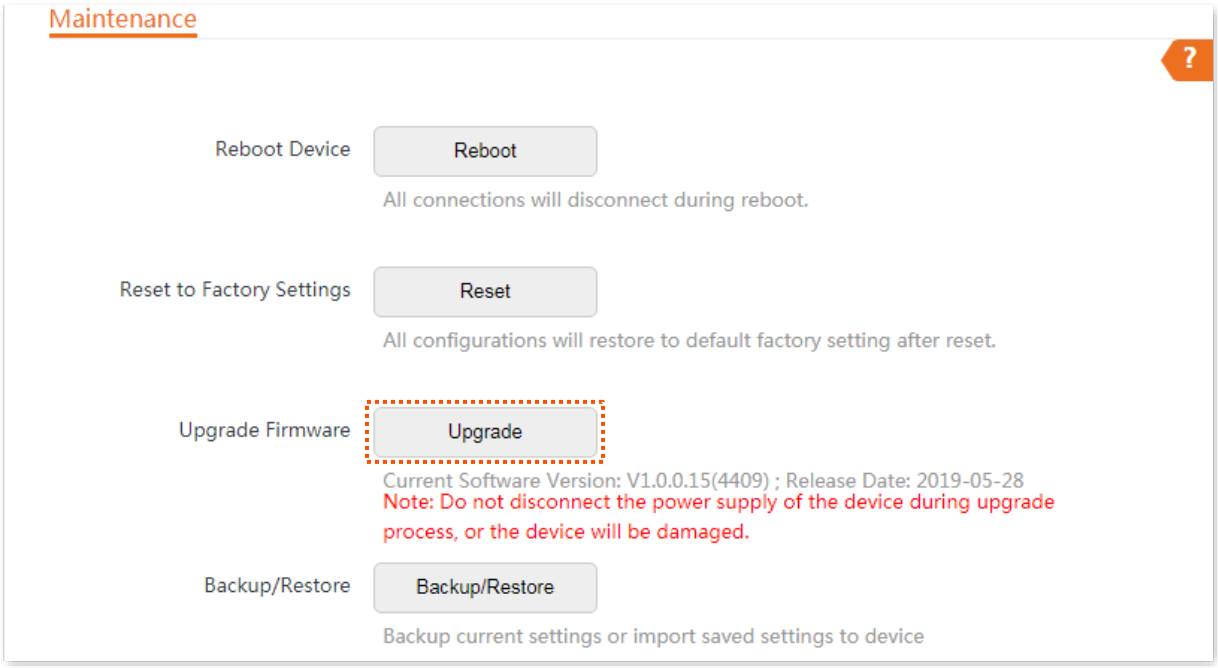
NOTE

To prevent damage to the CPE, ensure that:

- Ensure that the firmware file is compatible with the CPE before upgrading. Generally, the suffix of the firmware file is **.bin**.
- Keep the CPE powered on during the upgrade.

**Configuration procedure**

1. Download the firmware file for the CPE from www.tendacn.com to your local computer, and unzip it.
2. Log in to the web UI of the CPE, then navigate to **Tools** > **Maintenance**.
3. Click **Upgrade**.




4. Select the correct upgrade file (extension: .bin) from your local computer and the system will upgrade automatically.

**---End**

Wait for the progress bar to complete. Then log in to the web UI of the CPE. To verify your upgrade, log in to the web UI of the CPE, and go to the Status page to check the current firmware version.

## 8.2.4 Backup/Restore

The **Backup** function can save the current configuration of the CPE to your computer. The **Restore** function can restore the CPE configuration from the previous backup.

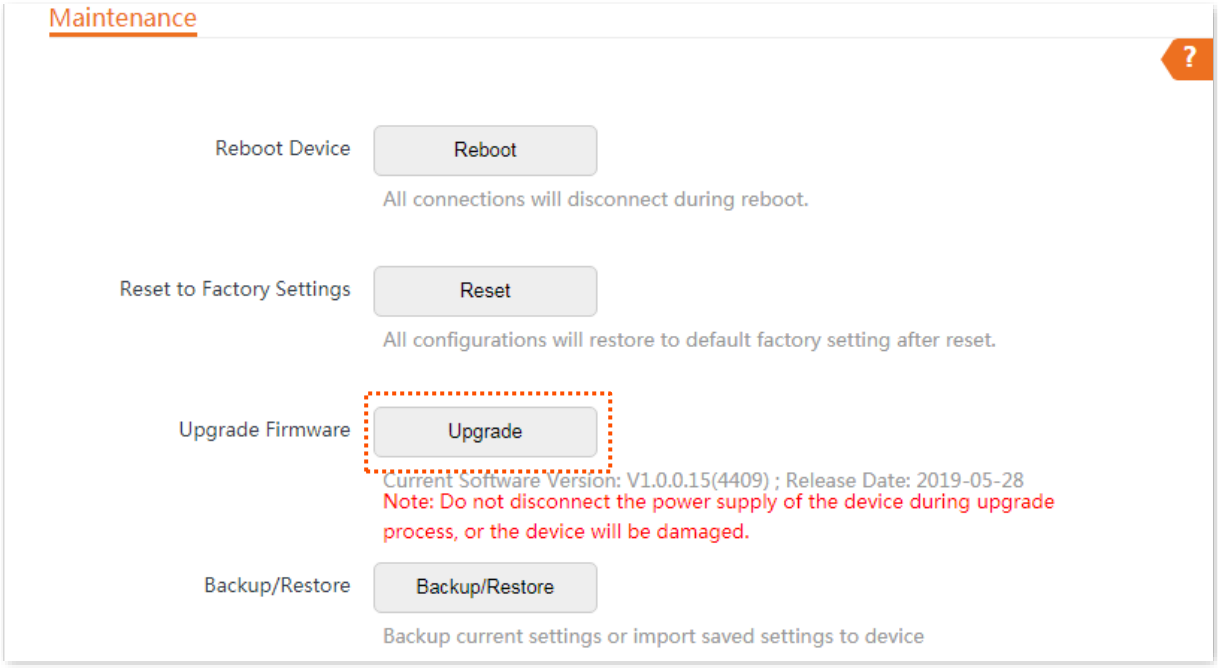
When you have made a lot of configurations to the CPE for operating conditions and environmental requirements, it is recommended to back up the configuration. After upgrading the firmware or restoring the CPE to factory settings, you can restore the previous configuration.

NOTE

To apply the same configuration to multiple CPEs with minimal effort, configure one CPE, back up its configuration, and import the backup file to the rest.

## Backup

1. Log in to the web UI of the CPE.
2. Navigate to **Tools** > **Maintenance**.
3. Click **Backup/Restore**.




4. Click **Backup** on the pop-up window.



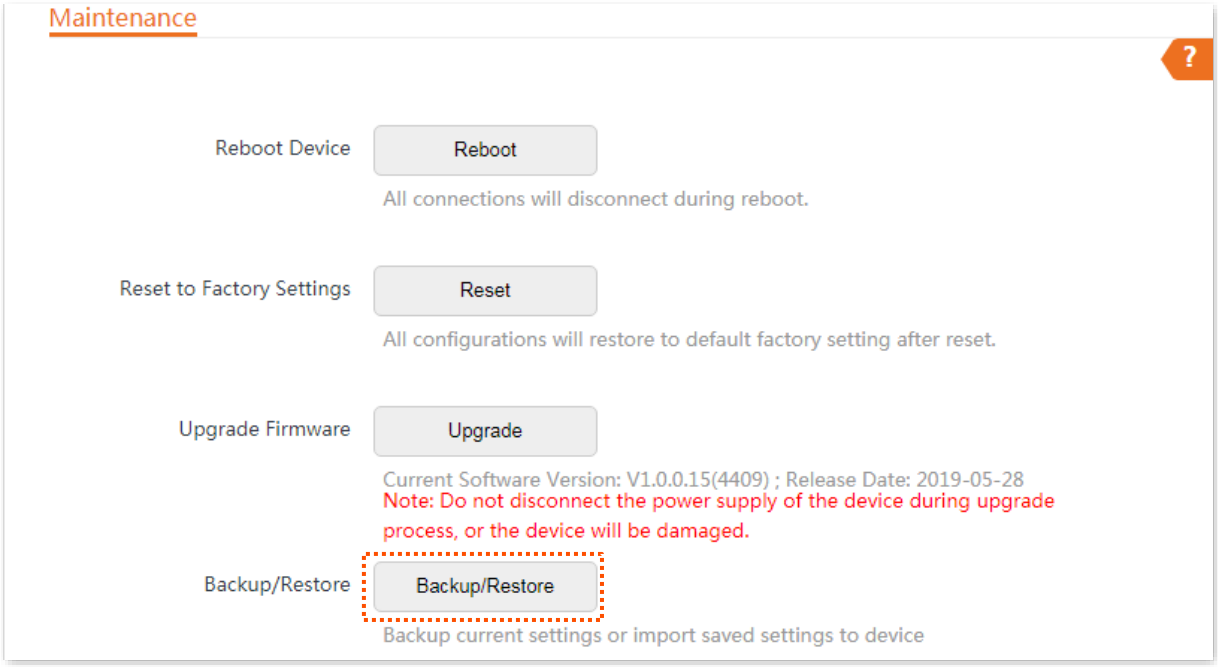

5. Confirm the prompt information, and click **Save**.

**---End**

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

## Restore

1. Log in to the web UI of the CPE.
2. Navigate to **Tools** > **Maintenance**.
3. Click **Backup/Restore**.




4. Click **Restore** on the pop-up window.




5. Select and upload the backup file (extension: **.cfg**).

**---End**

After the file is uploaded, the CPE reboots automatically.

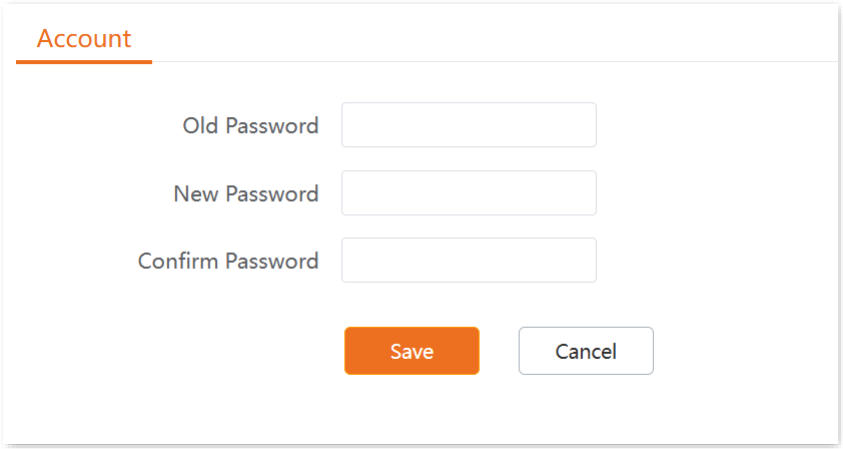
Wait for the progress bar to complete. The CPE is successfully restored to the previous settings.

# 8.3 Account

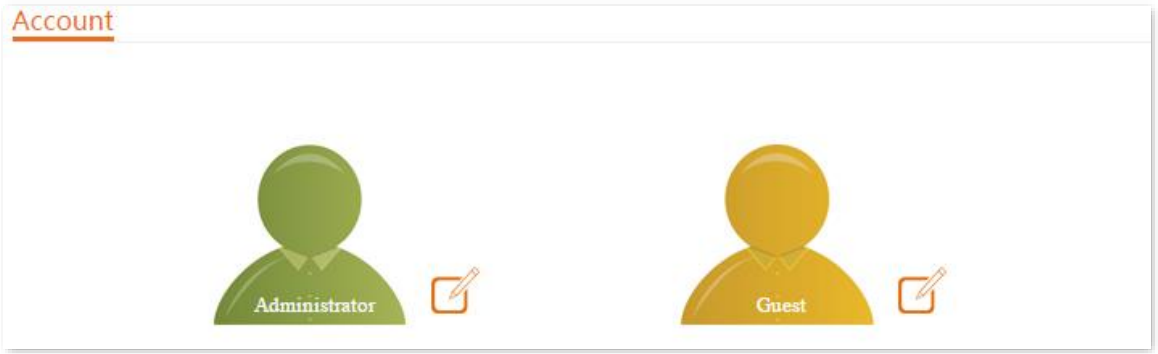
To access the page, log in to the web UI of the CPE and navigate to **Tools** > **Account**.

On this page, you can change the login account information of the CPE to prevent unauthorized login.

O6 V3.0 is used as an example. Enter the old password and a new password, confirm the new password by entering it again, then click **Save**.




O4 V3.0 is used as an example. Click to change the account information.




By default, the CPE has one administrator account and one guest account.

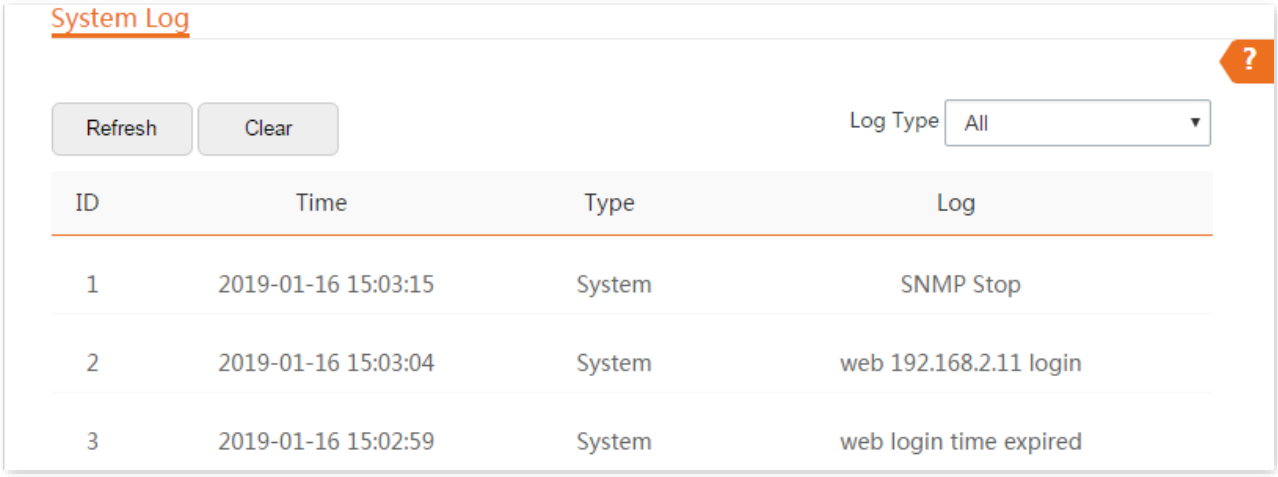
- Administrator account: When logging in with this account, you can view and modify the device settings. Both the default user name and password are **admin**.
- Guest account: When logging in with this account, you can only view the device settings. Both the default user name and password are **user**.

# 8.4 System log

To access the page, log in to the web UI of the CPE and navigate to **Tools** > **System Log**.

The logs of the CPE record various events that occur and the operations that users perform after the CPE starts. In case of a system fault, you can refer to the logs during troubleshooting.

To view the latest logs of the CPE, click **Refresh**. To clear the existing logs, click **Clear**.




To ensure that the logs are recorded correctly, verify the system time of the CPE. You can correct the system time of the CPE on the Date & Time page.

NOTE

- When the CPE reboots, the previous logs are removed.
- The CPE reboots in case of the following situations: the CPE is powered on after a power failure, the VLAN function is configured, the firmware is upgraded, the configuration of the CPE is restored to the factory settings.

# Appendix

## A.1 Default parameters

The main default parameters are shown in the following table.

| Parameters | | | Default settings |
|---|---|---|---|
| Login | Login IP Address | Single | 192.168.2.1 |
| | | Kit | AP mode: 192.168.2.1<br>Client mode: 192.168.2.2 |
| | Administrator | User name | admin |
| | | Password | admin |
| | Guest | | Disable |
| Quick Setup | Working Mode | Single | AP mode |
| | | Kit | AP mode or Client mode |
| LAN Setup | IP Address Type | | Static IP address |
| | IP Address | Single | 192.168.2.1 |
| | | Kit | AP mode: 192.168.2.1<br>Client mode: 192.168.2.2 |
| | Subnet Mask | | 255.255.255.0 |
| DHCP Server | DHCP Server | Single | Enable |
| | | Kit | Disable |
| | Start IP Address | | 192.168.2.100 |
| | End IP Address | | 192.168.2.200 |

| Parameters | | | Default settings |
|---|---|---|---|
| | Subnet Mask | | 255.255.255.0 |
| | Gateway Address | | 192.168.2.254 |
| | Primary DNS Server | | 8.8.8.8 |
| | Lease Time | | 1 day |
| VLAN Settings | VLAN Settings | | Disable |
| | PVID | | 1 |
| | Management VLAN | | 1 |
| | WLAN | | 1000 |
| Wireless | Wireless Network | | Enable |
| | SSID | | Operating RF: Tenda_*XXXXXX* (*XXXXXX* is the last six digits of the LAN MAC address of the CPE)<br>Management RF: Tenda_*XXXXXX*_MG (*XXXXXX* is the last six digits of the LAN MAC address of the CPE)<br>TIP<br>The management RF is not available for some CPEs. |
| | Security Mode | Single | None |
| | | Kit | Encrypted |
| | Transparent Bridge | | Enable |
| | TD-MAX | | Disable |
| | TPC | | Enable |
| Network Service | Login Timeout Interval | | 5 min |
| | Ping Watch Dog | | Disable |
| | Telnet Service | | Disable |
| | UPnP | | Disable |
| | Hardware Watch Dog | | Enable |

| Parameters | | Default settings |
|---|---|---|
| Tools | Date & Time | Synchronized with the internet |

# A.2 Acronyms and Abbreviations

| Acronym or Abbreviation | Full Spelling |
|---|---|
| AES | Advanced Encryption Standard |
| AP | Access Point |
| ARP | Address Resolution Protocol |
| ASCII | American Standard Code for Information Interchange |
| BSSID | Basic Service Set Identifier |
| CAT5e | Category 5 Enhanced |
| CCQ | Client Connection Quality |
| CPE | Customer Premises Equipment |
| CPU | Central Processing Unit |
| DFS | Dynamic Frequency Selection |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| DDNS | Dynamic Domain Name System |
| DTIM | Delivery Traffic Indication Map |
| DMZ | Demilitarized Zone |
| FTP | File Transfer Protocol |
| GMT | Greenwich Mean Time |
| HTTP | Hypertext Transfer Protocol |
| IP | Internet Protocol |
| ICMP | Internet Control Message Protocol |
| IPv4 | Internet Protocol Version 4 |
| ISP | Internet Service Provider |

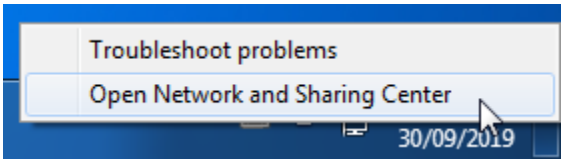
| Acronym or Abbreviation | Full Spelling |
|---|---|
| LAN | Local Area Network |
| MAC | Media Access Control |
| MIB | Management Information Base |
| NMS | Network Management System |
| NVR | Network Video Recorder |
| OID | Object Identifier |
| PoE | Power over Ethernet |
| PPPoE | Point-to-Point Protocol over Ethernet |
| PSK | Pre-Shared Key |
| P2MP | Point-to-Multi-Point |
| PVID | Port-based VLAN ID |
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial-In User Service |
| RAM | Random Access Memory |
| RF | Radio Frequency |
| RSSI | Received Signal Strength Indicator |
| RTS | Request to Send |
| RX | Receive |
| SSID | Service Set Identifier |
| SNMP | Simple Network Management Protocol |
| TCP | Transmission Control Protocol |
| TDMA | Time Division Multiple Access |
| TPC | Transmit Power Control |
| TKIP | Temporal Key Integrity Protocol |
| TX | Transmit |
| UDP | User Datagram Protocol |
| UI | User Interface |
| UPnP | Universal Plug and Play |

| Acronym or Abbreviation | Full Spelling |
|---|---|
| VID | VLAN Identifier |
| VLAN | Virtual Local Area Network |
| WAN | Wide Area Network |
| WDS | Wireless Distribution System |
| WEP | Wired Equivalent Privacy |
| WISP | Wireless Internet Service Provider |
| WLAN | Wireless Local Area Network |
| WMM | Wi-Fi Multimedia |
| WPA | Wi-Fi Protected Access |
| WPA-PSK | Wi-Fi Protected Access Pre-Shared Key |

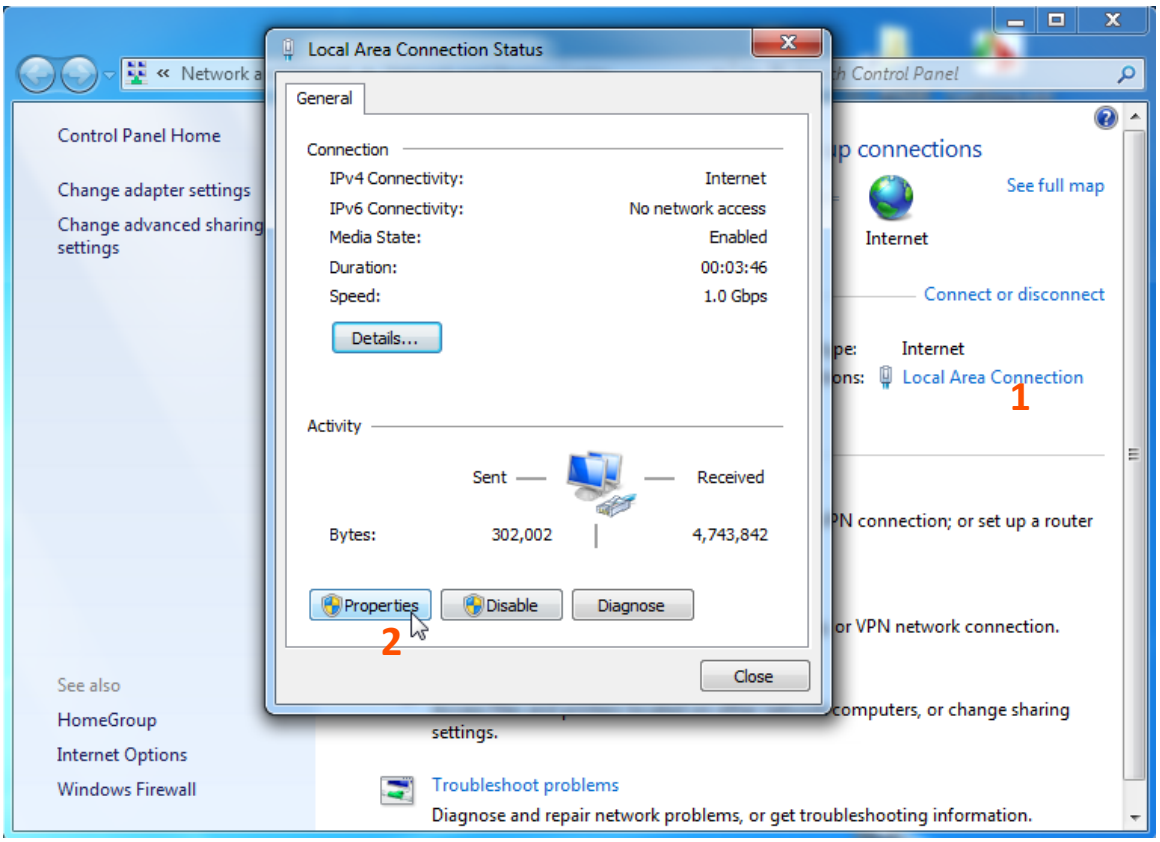
# A.3 Assign a fixed IP address to your computer

OS example: Windows 7

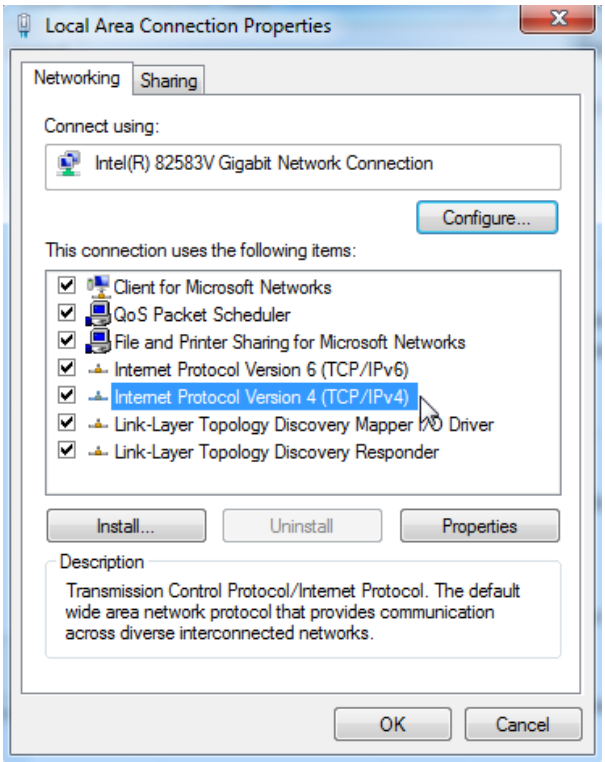
1. Right-click the  icon on the bottom-right corner of the desktop.
2. Click **Open Network and Sharing Center**.



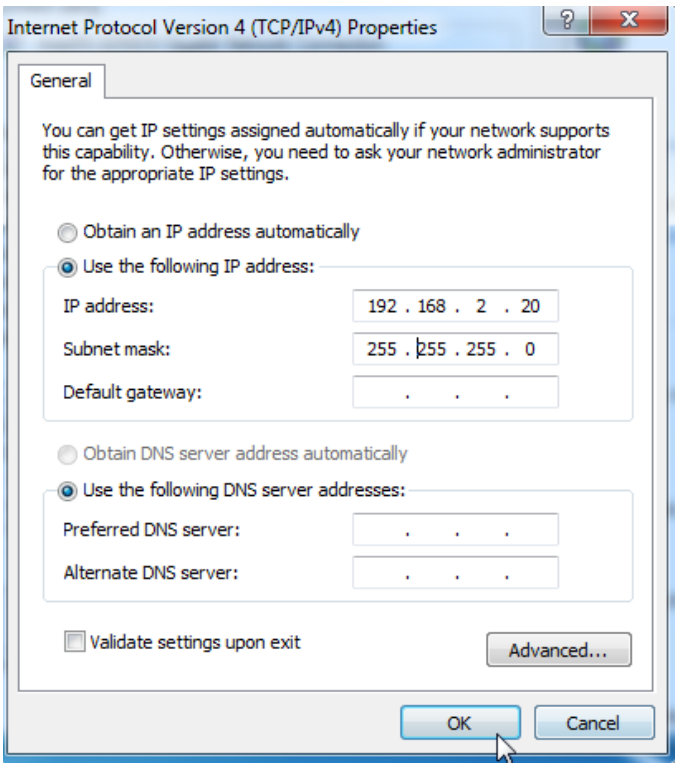

3. Click **Local Area Connection**, then click **Properties**.




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




5. Select **Use the following IP address**, set the **IP address** to **192.168.2.*X*** (*X* ranges from 2 to 253), the **Subnet mask** to **255.255.255.0**, and click **OK**.



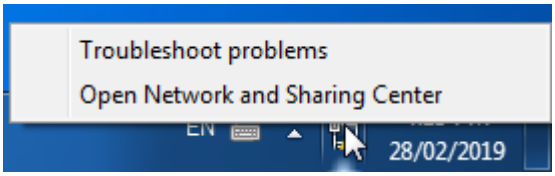

6. Click **OK** on the **Local Area Connection Properties** window, and close the other windows.

**---End**

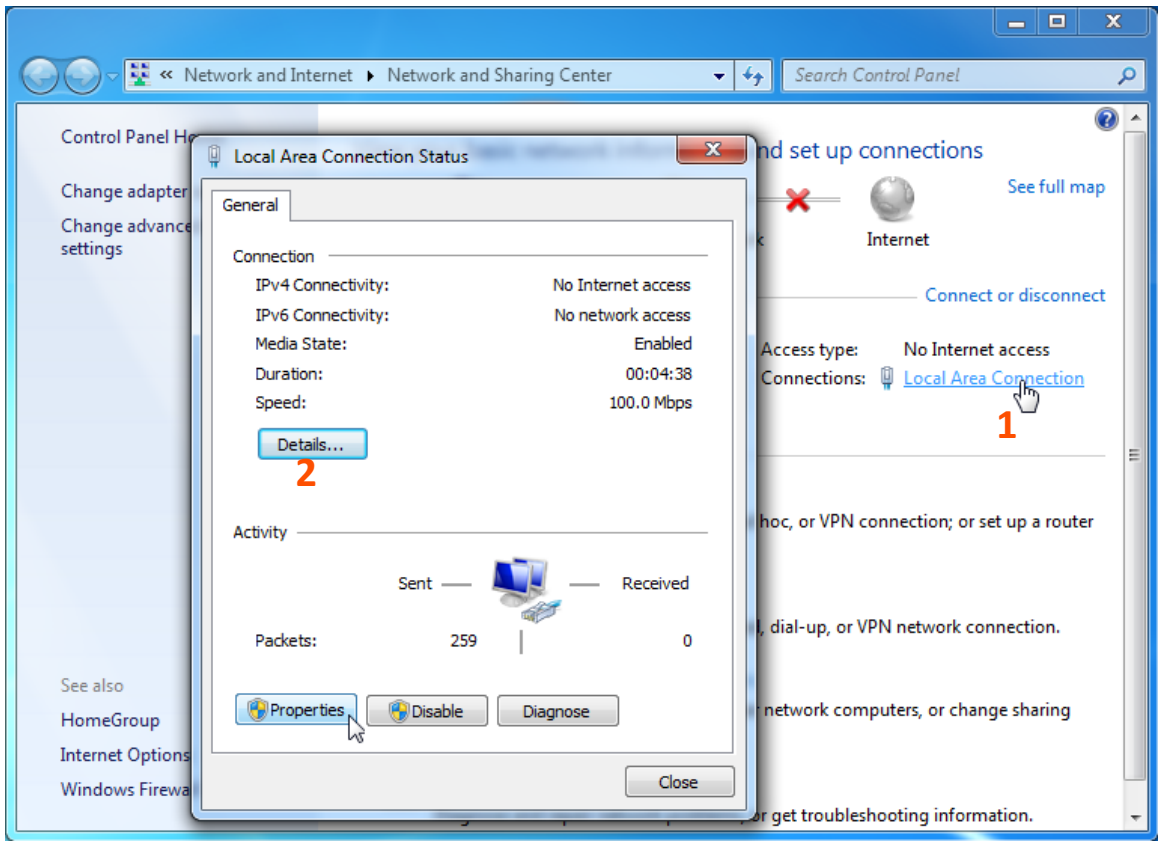
# A.4 How to check the gateway IP address of a computer

OS example: Windows 7

1. Right-click the icon on the bottom-right corner of the desktop.
2. Click **Open Network and Sharing Center**.




3. Click **Local Area Connection**, then click **Details…**




**---End**

Then you can check the default gateway address on the following page.

