



Outdoor CPE

User Guide

Copyright Statement

© 2021 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

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

Disclaimer

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

Preface

Thank you for choosing Tenda! Please read this user guide before you start.



Conventions

This user guide applies to the Tenda CPEs. O4V1.0 is used for illustrations here unless otherwise specified. The contained images and UI screenshots are subject to the actual products.

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: <i>XX:XX:XX:XX:XX:XX</i>
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
	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
	This format is used to highlight a procedure that will save time or resources.




Getting more documents

If you want to get more documents of the device, visit www.tendacn.com and search for the corresponding product model. The related documents are listed as below.

Document	Description
Data Sheet	It introduces the basic information of the device, including product overview, selling points, and specifications.
Quick Installation Guide	It introduces how to set up the device quickly for internet access, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on.
User Guide	It introduces how to set up more functions of the device for more requirements, including all functions on the web UI of the device.

Technical Support

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

 <p>Hotline</p>	<p>Global: (86) 755-27657180(China Time Zone)</p> <hr/> <p>United States: 1-800-570-5892 (Toll Free: 7 x 24 hours)</p> <hr/> <p>Canada: 1-888-998-8966 (Toll Free: Mon - Fri 9 am - 6 pm PST)</p> <hr/> <p>Hong Kong: 00852-81931998</p>	 <p>Email</p> <p>support@tenda.com.cn</p>
 <p>Website</p>	<p>www.tendacn.com</p>	

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 OS3V1.0 was introduced.

Version	Date	Description
v2.0	2021-11-25	1. Add new feature description: - Transparent WDS 2. Fixed some known issues.
v1.0	2020-07-04	Original publication.

Contents

1	Application scenario	1
	1.1 ISP hotspot connection-WISP mode	1
	1.2 CCTV surveillance	6
2	Log in to web UI	14
	2.1 Login	14
	2.2 Logout	18
3	Web UI	19
	3.1 Web UI layout	19
	3.2 Common buttons	20
4	Quick setup	21
	4.1 AP mode	22
	4.2 Client mode	25
	4.3 Universal repeater mode	32
	4.4 WISP mode	35
	4.5 Repeater mode	44
	4.6 P2MP mode	55
	4.7 Router mode	68
5	Status	72
	5.1 System status	72
	5.2 Wireless status	75
	5.3 Statistics	77
6	Network	82
	6.1 LAN setup	82
	6.2 MAC clone	87
	6.3 DHCP server	89
	6.4 DHCP client	91
	6.5 VLAN settings	92
7	Wireless	96
	7.1 Basic	96
	7.2 Advanced	125
	7.3 Access control	129
8	Advanced	132

8.1 LAN rate.....	132
8.2 Diagnose.....	134
8.3 Bandwidth control	142
8.4 Port forwarding	145
8.5 MAC filter	149
8.6 Network service	152
9 Tools.....	169
9.1 Date & time	169
9.2 Maintenance	172
9.3 Account	178
9.4 System log	180
Appendix	181
A.1 Default parameters.....	181
A.2 Acronyms and Abbreviations.....	183
A.3 How to assign a fixed IP address to your computer	185
A.4 How to check the gateway IP address of a computer	187

1 Application scenario

1.1 ISP hotspot connection-WISP mode

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

1.1.1 Solution

Tenda CPE can meet this demand.

O4V1.0 is used as an example to illustrate the installation procedures. Procedures for other CPEs are similar.



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

1.1.2 Set up the CPE

Step 1 Power on the CPE.

Step 2 [Log in to the web UI of CPE.](#)

Step 3 Set the CPE to **WISP** mode.

1. Choose **Quick Setup** to enter the configuration page.
2. Select **WISP**, and click **Next**.

Quick Setup

Select a working mode:

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

Next


3. Select the SSID of your ISP hotspot, which is **WiFi_123456** in this example, and click **Next**.

Quick Setup >> WISP ?

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

Scan [Scan again](#)

Upstream AP

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="radio"/>	WiFi_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	

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

Quick Setup >> WISP ?

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

Upstream AP

Upstream AP MAC Address

Channel

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

Key

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**.

Quick Setup >> WISP ?

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

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

PPPoE User Name

PPPoE Password

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

[Quick Setup](#) >> [WISP](#) ?

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

SSID(WiFi Name)

Channel ▼

Security Mode ▼

Encryption Algorithm AES TKIP TKIP&AES

Key

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

[Quick Setup](#) >> [WISP](#) ?

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

IP Address

Subnet Mask

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

[Quick Setup](#) >> [WISP](#) ?

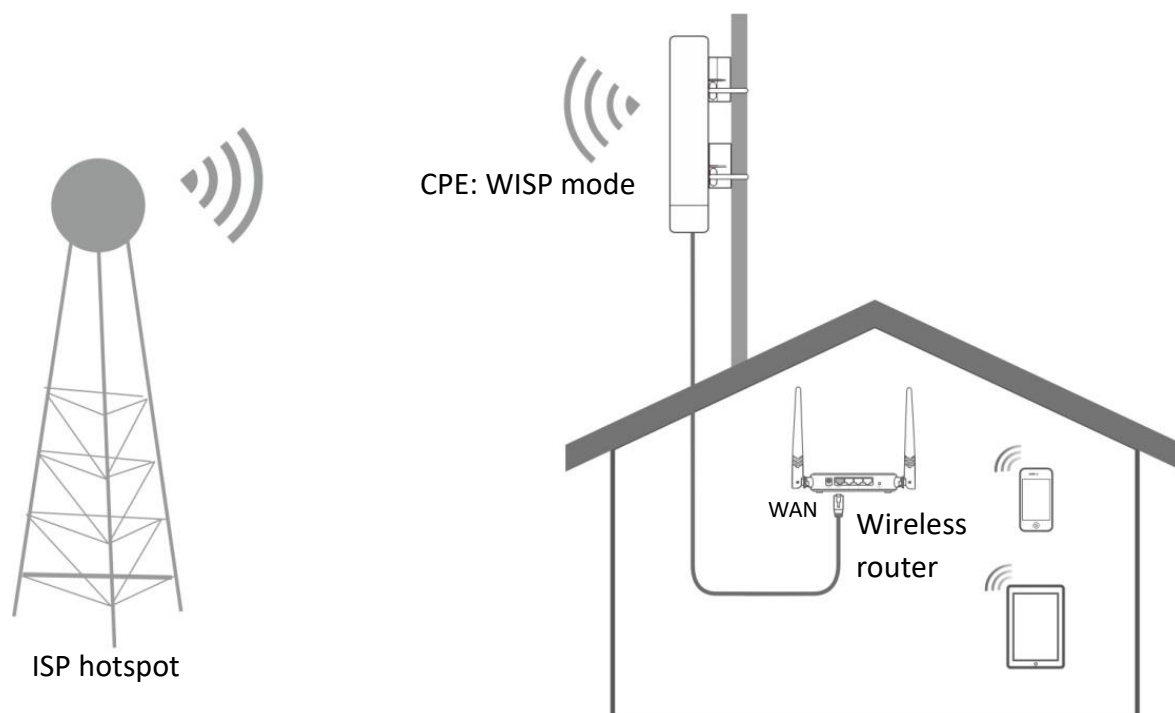
The device is set to WISP, click "Save" to apply the settings.

----End

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

1.1.3 Install the CPE

- Step 1** Place the CPE at an elevated position in the open air.
- Step 2** Power on the CPE.
- Step 3** Connect the CPE to the **WAN** port of your wireless router.
- Step 4** Adjust the CPE's direction or location on the selected pole until the LED1, LED2 and LED3 of the CPE light up.
- Step 5** Use the plastic straps to attach the CPE to the pole.



----End

Check the LED1, LED2 and LED3 indicators of the CPE to confirm whether its position is proper. The more LED indicators light up, the better the connection quality is. The LED indicator descriptions of the CPE below are for reference.

LED Indicator	Status	Description
LED1, LED2, LED3 (Received signal strength LED indicators)	Solid on/Blinking	<p>The CPE is connected to a device/devices.</p> <ul style="list-style-type: none"> • Solid on: The CPE may work in AP, Repeater, P2MP or Router mode. • Blinking: The CPE may work in Client, Universal Repeater or WISP mode. <p>Each LED indicator is set with a received signal strength value, which is the threshold for the corresponding LED indicator to light up. You can judge the connection quality through the status of these indicators.</p> <p>By default, the minimum signal strength of LED1, LED2 and LED3 are -90 dBm, -80 dBm and -70 dBm.</p> <p>You can change them on the Wireless > Advanced page of the</p>

LED Indicator	Status	Description
		web UI of the CPE.
	Off	No device is connected to the CPE, or the received signal strength is less than the RSSI threshold (default: -90 dBm).

1.2 CCTV surveillance

To ensure the safety of employees and property, a video surveillance system needs to be installed in a building site.

1.2.1 Solution

Tenda CPE can meet this demand.

O4V1.0 is used as an example to illustrate the installation procedures. Procedures for other CPEs are similar.

1.2.2 Set up the CPEs



TIP

At least two CPEs are required for bridging.

Option 1: Automatic bridging (recommended)



NOTE

- Automatic bridging is only applicable when the CPEs are in factory settings.
 - When performing peer-to-peer bridging, ensure that only two CPEs are powered on nearby. Otherwise, the peer-to-peer bridging may fail.
-

Scenario 1: Peer-to-peer bridging

Step 1 Place the two CPEs next to each other.

Step 2 Power on the CPEs.

----End

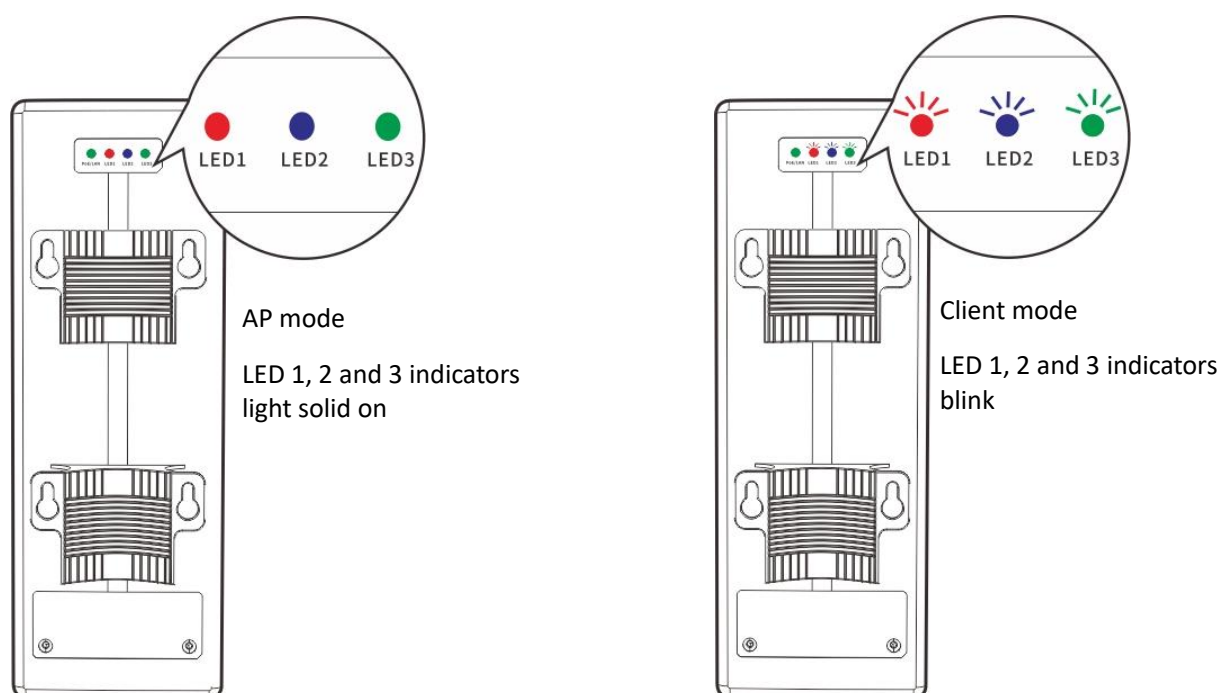
After the two CPEs are powered on, they will bridge to each other automatically, and the LED1, LED2 and LED3 indicators of the two CPEs blink rapidly. When the LED1, LED2 and LED3 indicators of a CPE light solid on while the LED1, LED2 and LED3 indicators of the other CPE blink slowly, the peer-to-peer bridging succeeds.



TIP

For earlier versions of O2 and O3, the peer-to-peer bridging procedure is as follows:

After the two CPEs are powered on, they will bridge to each other automatically. When the LED1, LED2 and LED3 indicators of a CPE light solid on while the LED1, LED2 and LED3 indicators of the other CPE keep blinking, the peer-to-peer bridging succeeds.



- After the bridging succeeds, the DHCP servers of the two CPEs are disabled. The IP address of the CPE working in AP mode remains the same (192.168.2.1), while the IP address of the CPE working in Client mode changes to 192.168.2.2.
- If the peer-to-peer automatic bridging fails, reset the two CPEs to factory settings, and try again. Reset method: After CPE completes startup, hold down the reset button for about 8 seconds, and then release it when all indicators light up. Wait for about 1 minute.

Scenario 2: Peer-to-multiple peers bridging



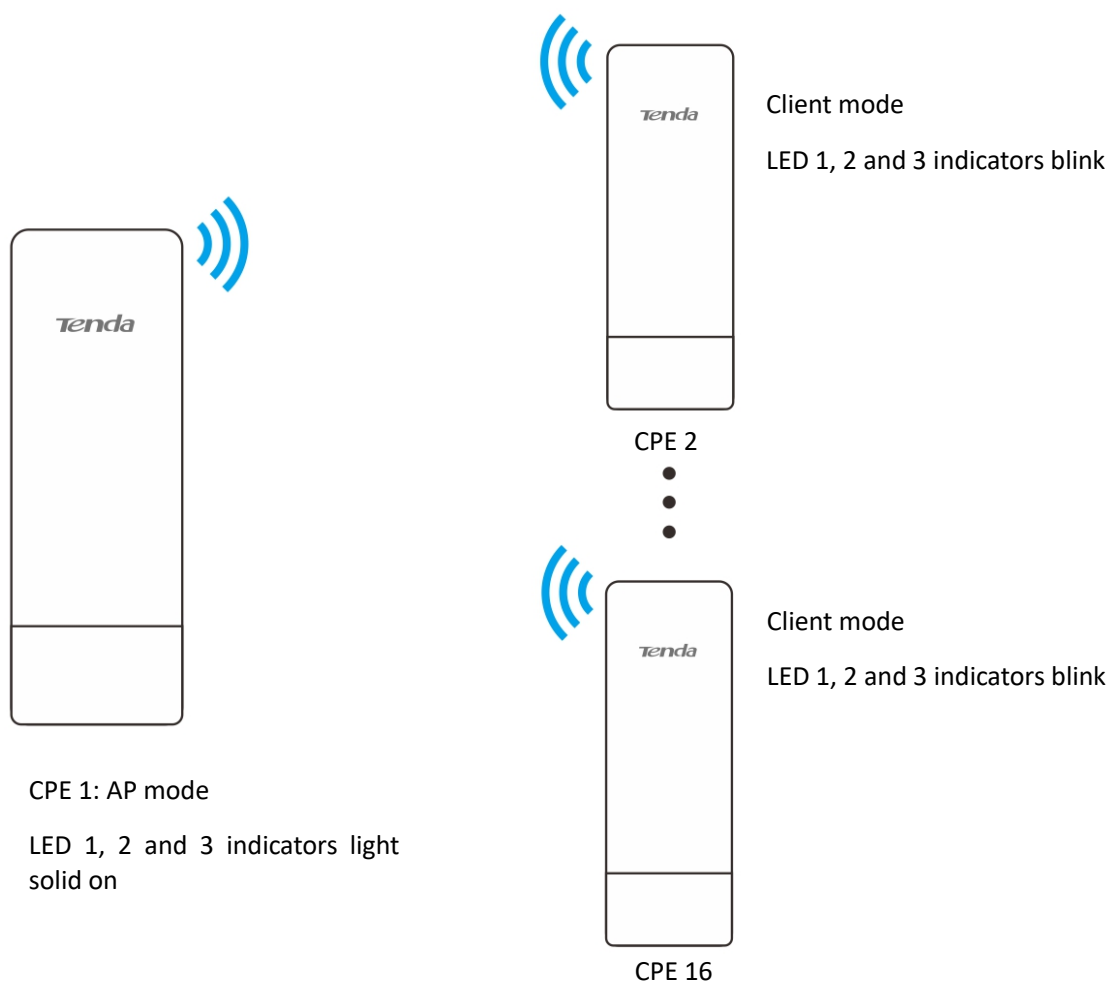
- For peer-to-multiple peers bridging, perform peer-to-peer bridging first, and then power on the rest CPEs within a certain period of time.
- A CPE can bridge 15 CPEs at most.

Step 1 Refer to [Peer-to-peer bridging](#) to make any two CPEs bridge to each other.

Step 2 Within a certain period of time (3 minutes for earlier versions of O2 while 30 minutes for other CPE models) after the peer-to-peer bridging succeeds, place the rest CPEs which are in factory settings near the CPE with the LED1, LED2, and LED3 indicators solid on and power them on.

----End

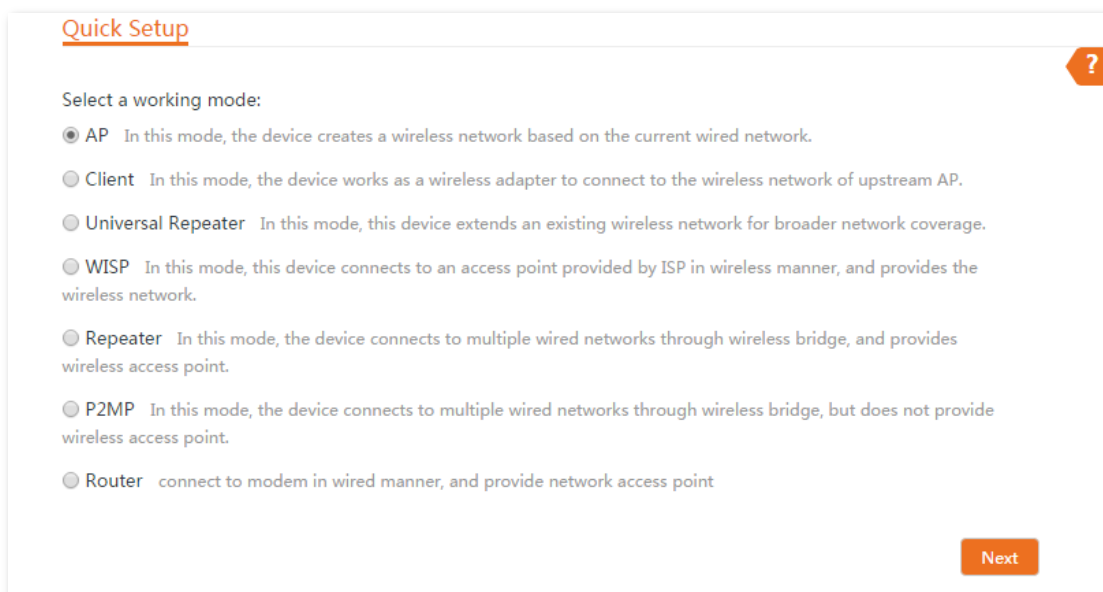
Wait about 1 minute. When the LED1, LED2, and LED3 indicators of these new-added CPEs keep blinking, the peer-to-multiple peers bridging succeeds.

**TIP**

- If the LED1, LED2 and LED3 indicators of a new-added CPE turn off after it is powered on for 1 minute, the bridging fails. Reset the CPE to factory settings, and wait until its LED1, LED2 and LED3 indicators keep blinking, which indicates that the automatic bridging succeeds.
- If the bridging still fails, try manual bridging. Refer to [Client mode](#) for details.

Option 2 Manual bridging

- Step 1** Place the two CPEs next to each other.
- Step 2** Power on the CPE1.
- Step 3** [Log in to the web UI of CPE1.](#)
- Step 4** Set CPE1 to AP Mode.
1. Choose **Quick Setup** to enter the configuration page.
 2. Select **AP**, and click **Next**.



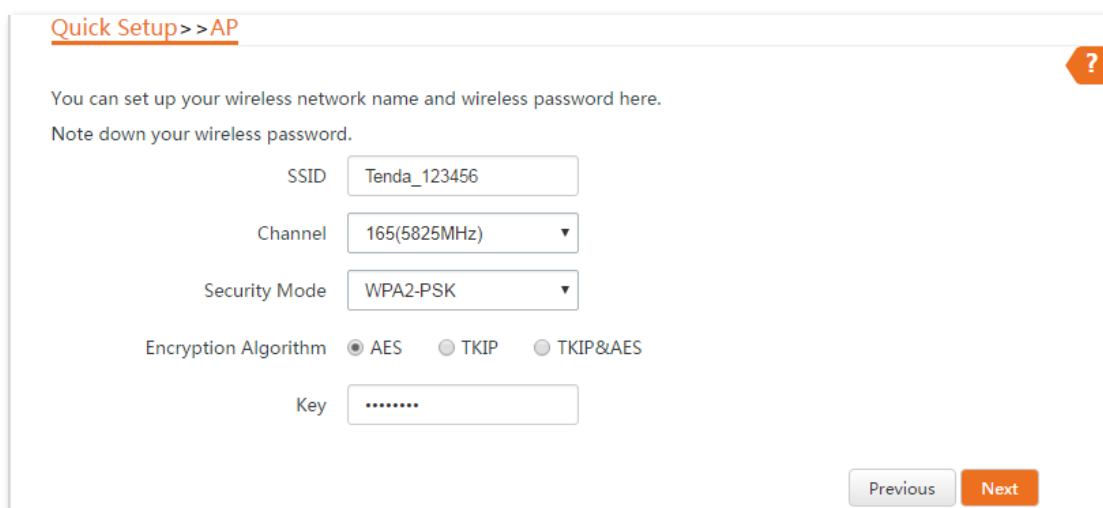
Quick Setup ?

Select a working mode:

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

Next

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



Quick Setup >> AP ?

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

SSID

Channel

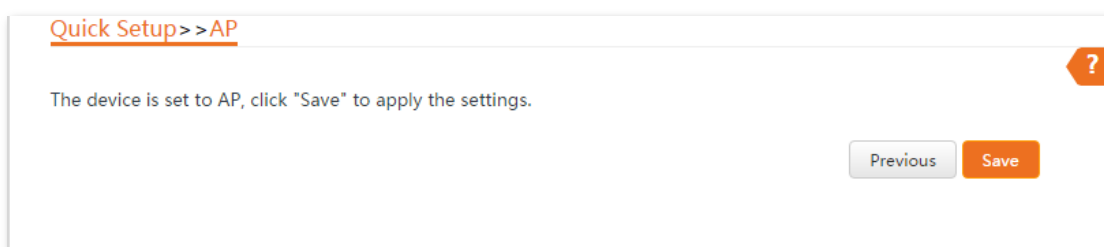
Security Mode

Encryption Algorithm AES TKIP TKIP&AES

Key

Previous **Next**

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

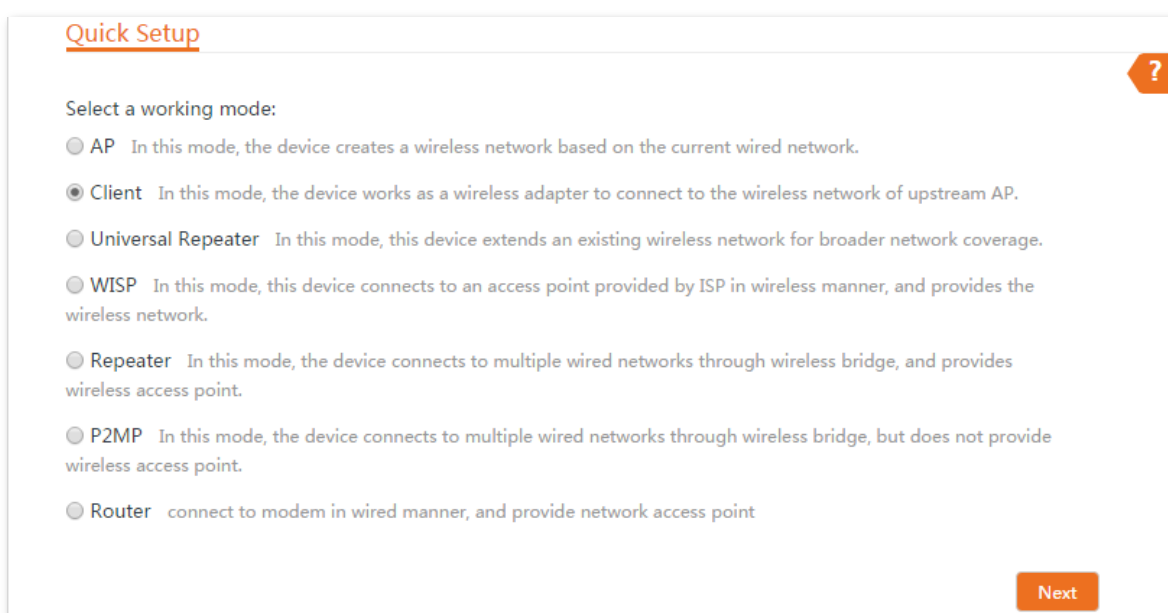


Step 5 Power on the CPE2.

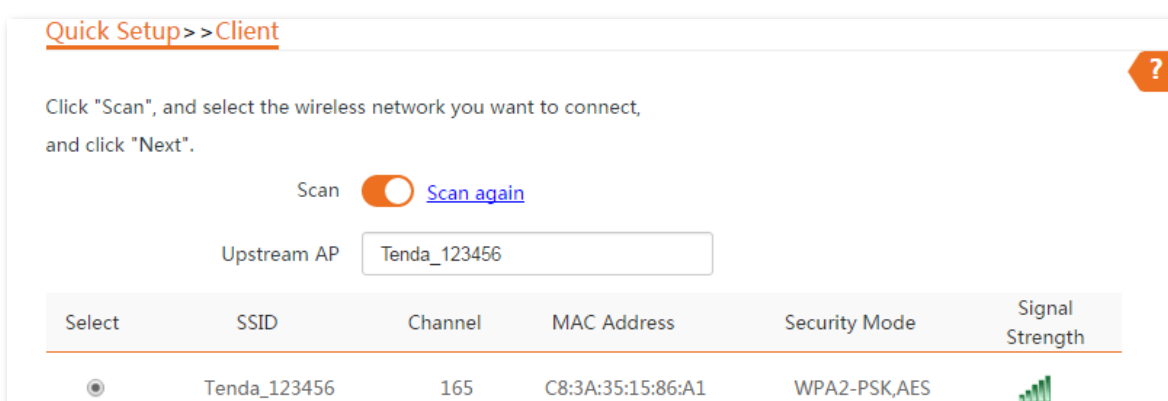
Step 6 [Log in to the web UI of CPE2.](#)

Step 7 Set **CPE2** to **Client Mode**.

1. Choose **Quick Setup** to enter the configuration page.
2. Select **Client**, and click **Next**.



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



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

Quick Setup >> Client ?

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

Upstream AP Tenda_123456

Upstream AP MAC Address C8:3A:35:15:86:A1

Channel

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

Key

5. Set the **IP address** to an unused IP address belonging to the same network segment as that of **CPE1**. For example, if the IP address of CPE1 is 192.168.2.1, you can set this CPE's IP address to 192.168.2.X (X ranges from 2 to 254). Then click **Next**.

Quick Setup >> Client ?

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

IP Address

Subnet Mask

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

Quick Setup >> Client ?

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

----End

When the two CPEs are bridging to each other, all the LED1, LED2 and LED3 indicators blink rapidly. When the LED1, LED2 and LED3 indicators of a CPE light solid on while the LED1, LED2 and LED3 indicators of the other CPE blink slowly, the bridging succeeds.



For earlier versions of O2 and O3, the bridging procedure is as follows:

When the two CPEs are bridging to each other, all the LED1, LED2 and LED3 indicators blink. When the LED1, LED2 and LED3 indicators of a CPE light solid on while the LED1, LED2 and LED3 indicators of the other CPE keep blinking, the bridging succeeds.

If you want to bridge multiple CPEs to CPE1, refer to [Step 5-7](#) to bridge them to the WiFi network of the CPE with the LED1, LED2 and LED3 indicators solid on.



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

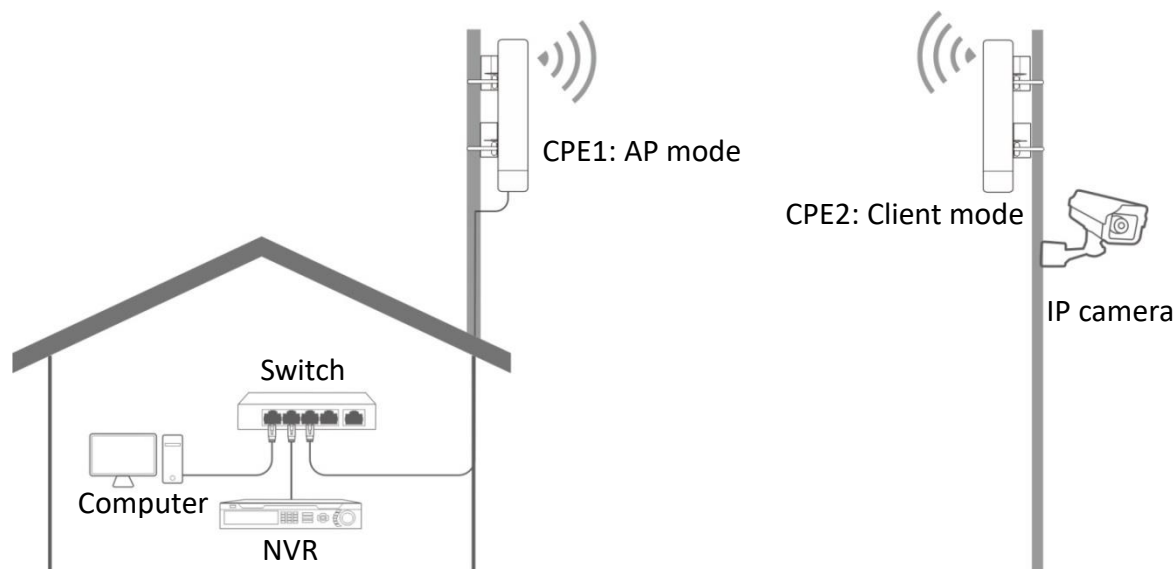
1.2.3 Install the CPEs

The CPE (transmitter in AP mode) with LED1, LED2 and LED3 solid on should be connected to the switch connecting to a network video recorder (NVR).

The CPE (receiver in Client mode) with LED1, LED2 and LED3 blinking should be connected to the IP camera or the switch connecting to IP cameras.

Detailed procedures are as follows:

- Step 1** Place the transmitter in the open air at the point where the NVR is located. Place the receiver in the open air at the point where the IP camera is located.
- Step 2** Power on the CPE.
- Step 3** Adjust the two CPEs' direction or location until the LED1, LED2 and LED3 of the two CPEs light up.
- Step 4** Use the plastic straps to attach the two CPEs to the poles respectively.



----End

Check the LED1, LED2 and LED3 indicators of the CPEs to confirm whether the positions are

proper. The more LED indicators light up, the better the connection quality is. The LED indicator descriptions of the CPEs below are for reference.

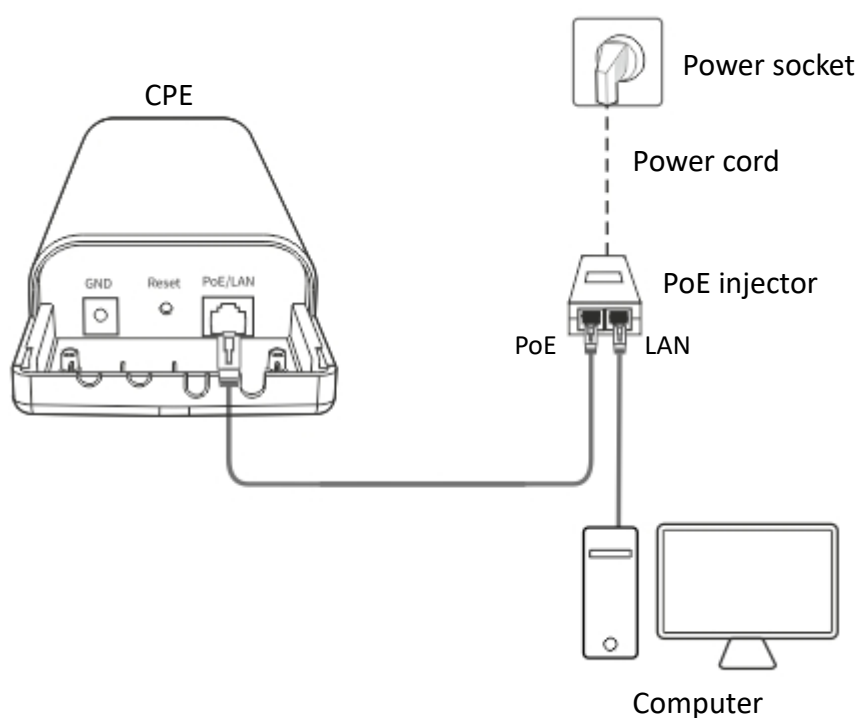
LED Indicator	Status	Description
LED1, LED2, LED3 (Received signal strength LED indicators)	Solid on/Blinking	<p>The CPE is connected to a device/devices.</p> <ul style="list-style-type: none"> • Solid on: The CPE may work in AP, Repeater, P2MP or Router mode. • Blinking: The CPE may work in Client, Universal Repeater or WISP mode. <p>Each LED indicator is set with a received signal strength value, which is the threshold for the corresponding LED indicator to light up. You can judge the connection quality through the status of these indicators.</p> <p>By default, the minimum signal strength of LED1, LED2 and LED3 are -90 dBm, -80 dBm and -70 dBm.</p> <p>You can change them on the Wireless > Advanced page of the web UI of the CPE.</p>
	Off	No device is connected to the CPE, or the received signal strength is less than the RSSI threshold (default: -90 dBm).

2 Log in to web UI

2.1 Login

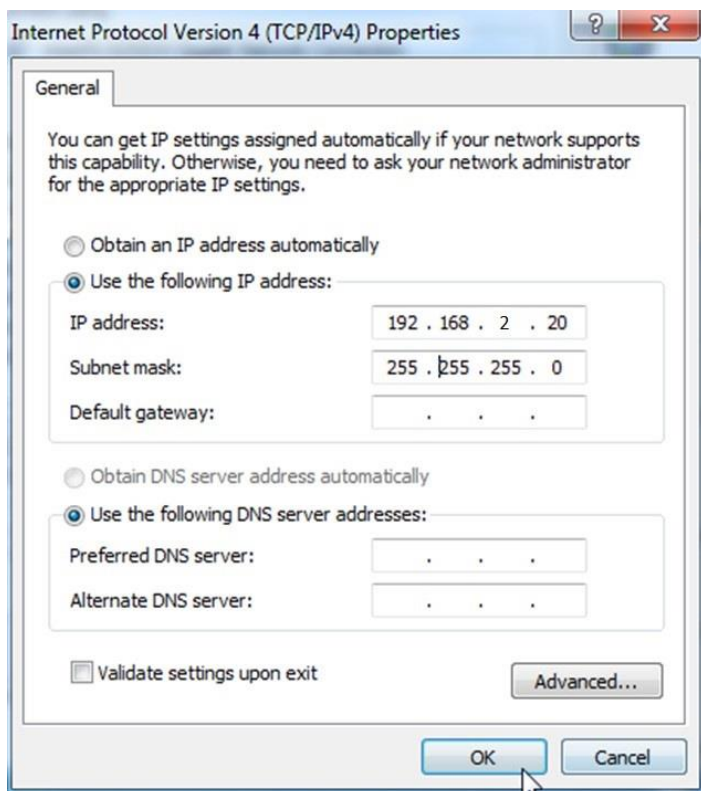
Logging in to the web UI for the first time or after the CPE is reset, or after the CPE is set to AP mode, Client mode, Universal Repeater mode, Repeater mode or P2MP mode

Step 1 Connect the computer to the CPE or the switch connected to the CPE. (powered by PoE in this example)



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

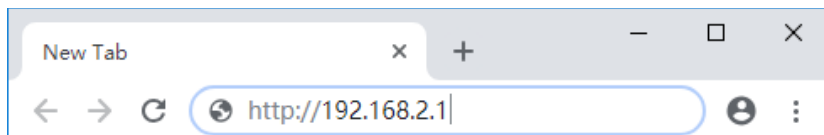
For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X is an unused digit ranging from 2 to 254), and subnet mask to 255.255.255.0.



Step 3 Start a web browser on your computer, and visit the IP address of the CPE (default: **192.168.2.1**).



If the CPE is set to **Client, Universal Repeater, Repeater** or **P2MP** mode, use the IP address you changed when you set it to these modes to log in to the web UI. If you do not change it, try 192.168.2.1.



Step 4 Enter your user name and password (default: **admin/admin**), and click **Login**.

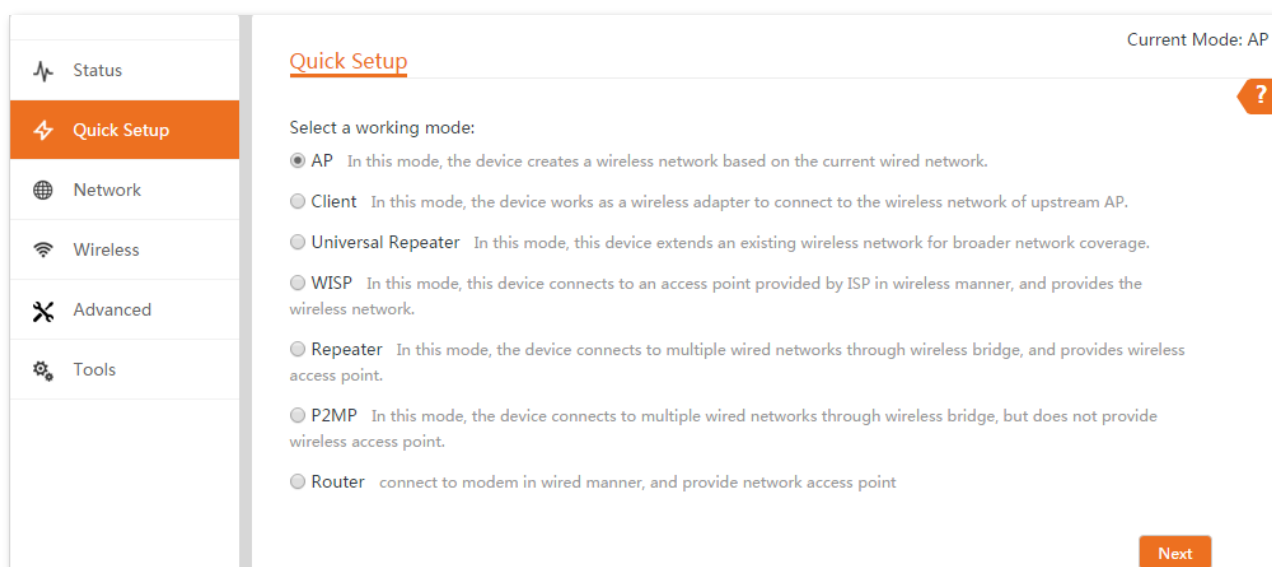


If the preceding page does not appear, please try the following methods:

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE properly.
- Ensure that the IP address of the computer is on the same network segment as that of the CPE's IP address. 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 2 to 254 and is not occupied).
- If more than one CPE is connected, please modify the IP address of each one to avoid the login failure due to IP address conflict.
- Reset the CPE to factory settings. Reset method: After CPE completes startup, hold down the reset button for about 8 seconds, and then release it when all indicators light up. Wait for about 1 minute.

----End

After successful login, the following page appears.



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

Logging in to the web UI after the CPE is set to WISP or Router mode

Step 1 Connect the computer to the LAN port of CPE or the switch connected to the CPE.

Step 2 Start a web browser on your computer, and visit the IP address of the CPE.

In WISP or Router mode, the CPE provides a DHCP server function to assign IP addresses to clients in LAN. In this case, the gateway IP address of the computer is the IP address of the CPE.



Refer to [How to check the gateway IP address of a computer](#) in Appendix to get the gateway IP address of your computer.

Step 3 Enter the login user name and password, and click **Login**.



If the preceding page does not appear, please 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 properly.
- Ensure that the IP address of the computer is on the same network segment of the CPE's IP address. 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 2 to 254 and is not occupied).
- Reset the CPE to factory settings. Reset method: After CPE completes startup, hold down the reset button for about 8 seconds, and then release it when all indicators light up. Wait for about 1 minute.

----End

After logging in to the web UI, you can start to configure the CPE.



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

2.2 Logout

The CPE logs out when you:

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

3 Web UI

3.1 Web UI layout

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

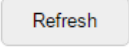

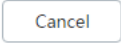



Functions or parameters in grey fields indicate that the CPE does not support it or it cannot be modified under the current configurations.

No.	Name	Description
1	Level-1 navigation tree	
2	Level-2 navigation tree	The navigation bars and tab pages display the function menu of the CPE. When you select a function in navigation bar, the configuration of the function appears in the configuration area.
3	Tab page area	
4	Configuration area	It enables you to view and modify configuration.

3.2 Common buttons

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

Common Buttons	Description
	It is used to update the contents on the current page.
	It is used to save the configuration on the current page and enable the configuration to take effect.
	It is used to go back to the original configuration without saving the configuration on the current page.
	It is used to view help information corresponding to the settings on the current page.

4 Quick setup

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

The CPE supports the following working modes:

- [AP](#): In this mode, the CPE creates a wireless network based on the current wired network.
- [Client](#): In this mode, the CPE works as a wireless adapter to connect to the wireless network of upstream AP. Working in Client mode, the CPE does not provide wireless access service, and a client needs to be connected to the CPE with an Ethernet cable.
- [Universal Repeater](#): In this mode, the CPE extends an existing wireless network for broader network coverage. The new wireless network has the same SSID, password, and related wireless information as the upstream wireless network.
- [WISP](#): In this mode, the CPE connects to a hotspot provided by ISP in a wireless manner, and provides the wireless network. 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.
- [Repeater](#): In this mode, the CPE connects multiple wired networks through wireless bridging, and provides wireless access point.
- [P2MP](#): In this mode, the CPE connects multiple wired networks through wireless bridging, but does not provide wireless access point.
- [Router](#): In this mode, the CPE connects to a modem in wired manner, and provides a wireless network.

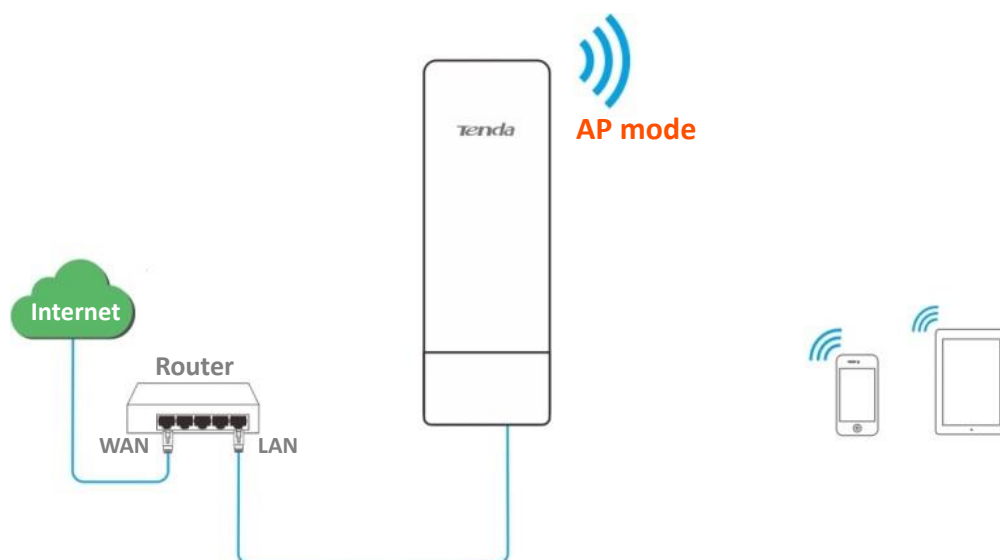
4.1 AP mode

4.1.1 Overview

In AP mode, the CPE connects to a wired network, and provides a wireless network for wireless clients.

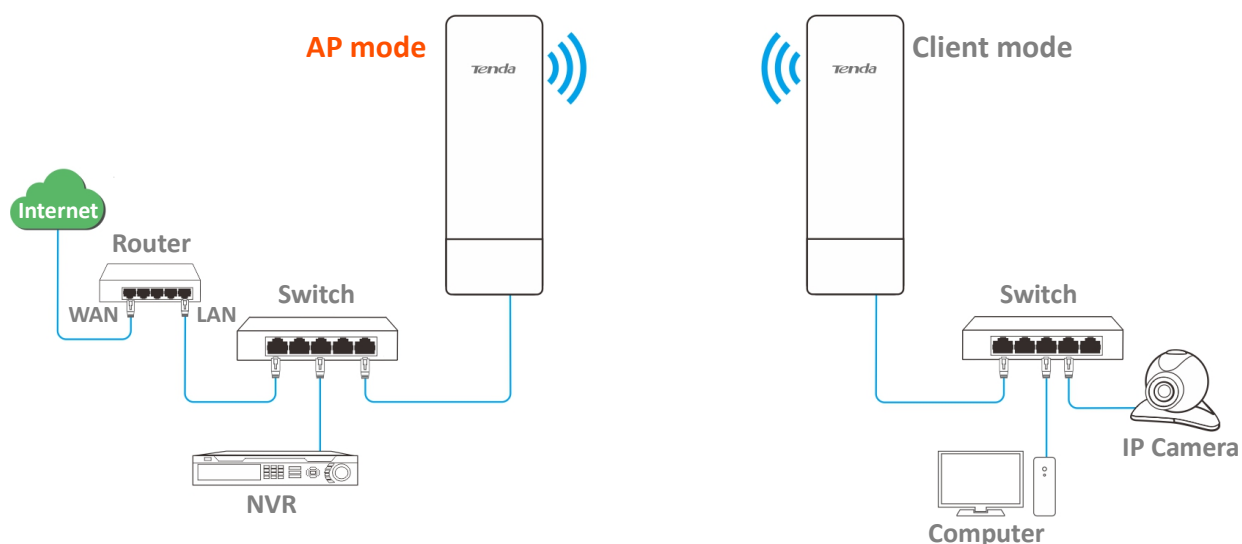
Application scenario 1

The CPE can be used to transform a wired network to a wireless one for your wireless devices to access the internet. The network topology is shown as below.



Application scenario 2

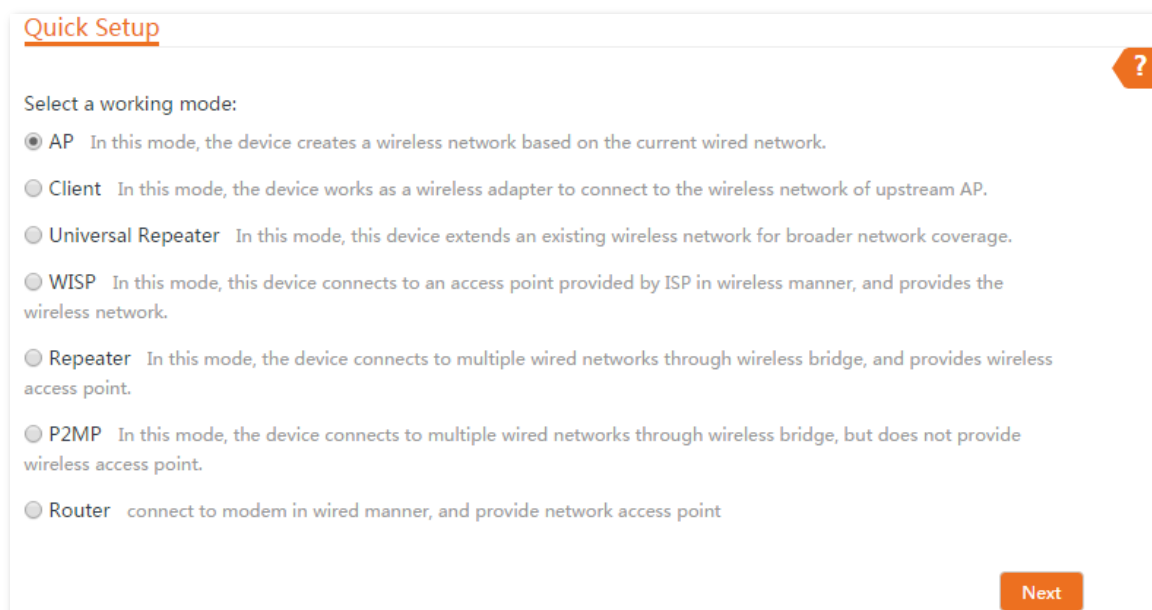
The CPE in AP mode usually works with another CPE in Client mode or Universal Repeater mode to establish a CCTV surveillance network. Client mode is used as an example here. Set one CPE to AP mode and connect it to the switch which is connected to the NVR, and the other to Client mode, and connect it to the switch which is connected to an IP camera. The network topology is shown as below.



4.1.2 Quick setup

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

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



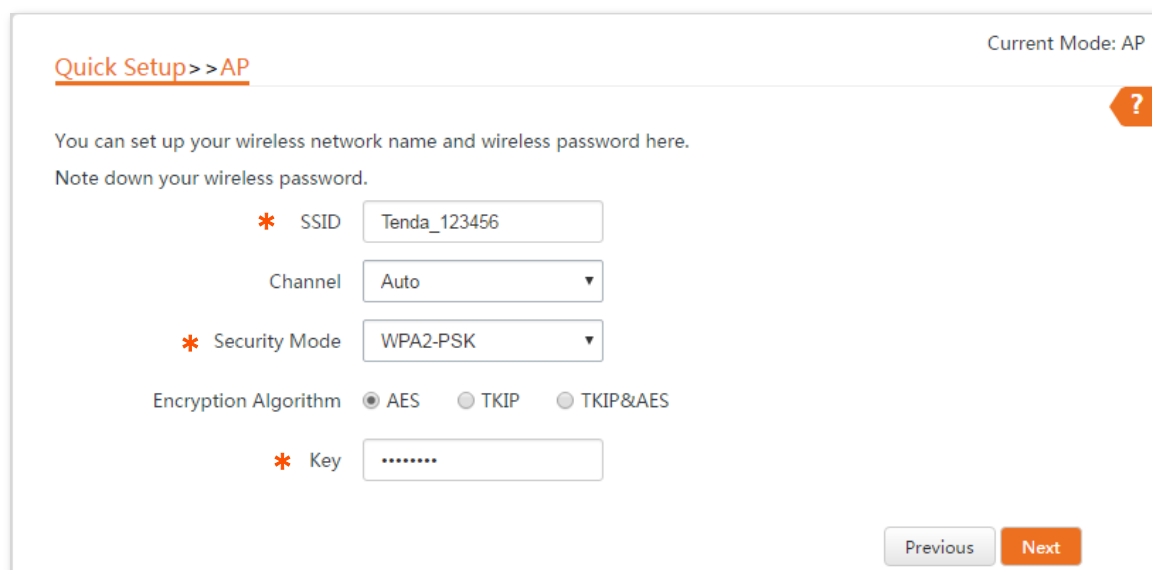
Quick Setup ?

Select a working mode:

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

Next

Step 3 Set an SSID, which is **Tenda_123456** in this example, **Security Mode**, which is WPA2-PSK in this example, **Encryption Algorithm**, which is **AES** in this example, **Key**, and click **Next**.



Quick Setup >> AP Current Mode: AP ?

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

* SSID

Channel

* Security Mode

Encryption Algorithm AES TKIP TKIP&AES

* Key

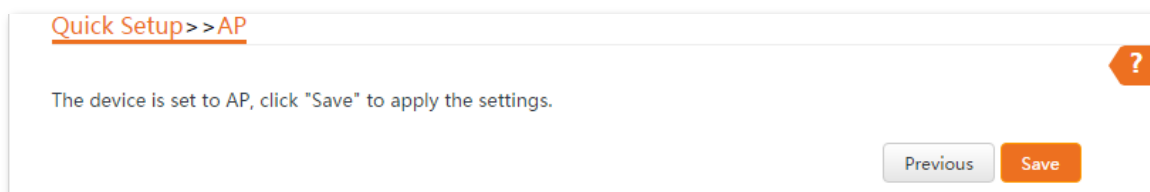
Previous **Next**

Parameters description

Name	Description
SSID	It specifies the wireless network name of this device.
Channel	It specifies the operating channel of this device. Select a less used channel in the ambient environment to reduce interference. Auto indicates that the device automatically adjusts its operating channel according to

Name	Description
	the ambient environment.
Security Mode	It specifies the security mode of the wireless network, including: None , WPA-PSK , WPA2-PSK , and Mixed WPA/WPA2-PSK .
Encryption Algorithm	<p>It specifies the encryption method of the wireless network.</p> <ul style="list-style-type: none"> • AES: It indicates the Advanced Encryption Standard. • TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. • TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies the WiFi password of the wireless network.

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



----End

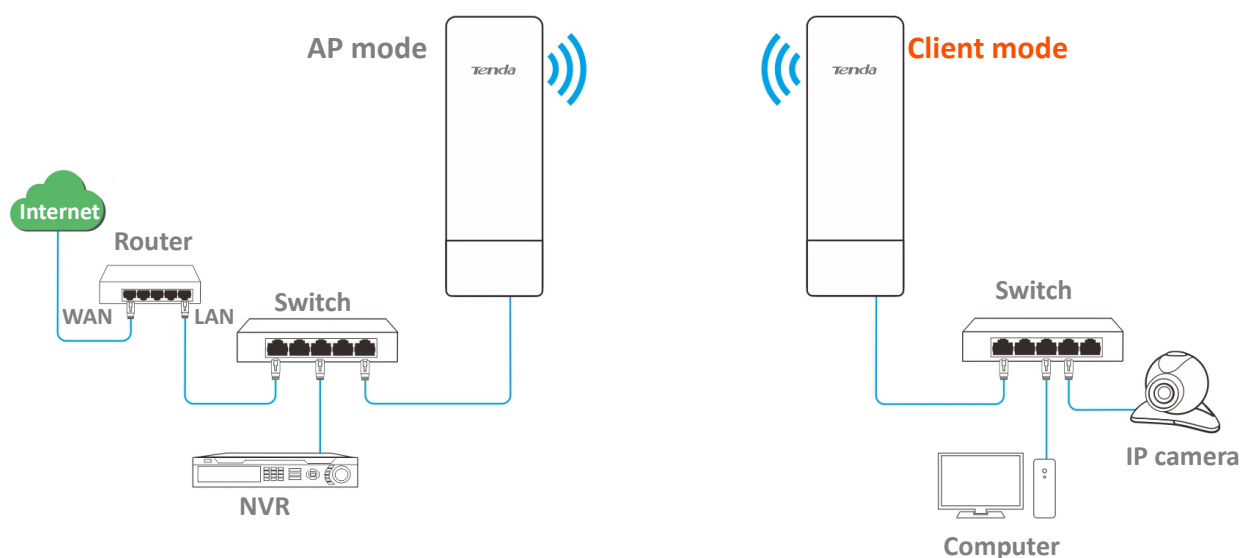
4.2 Client mode

4.2.1 Overview

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

Application scenario

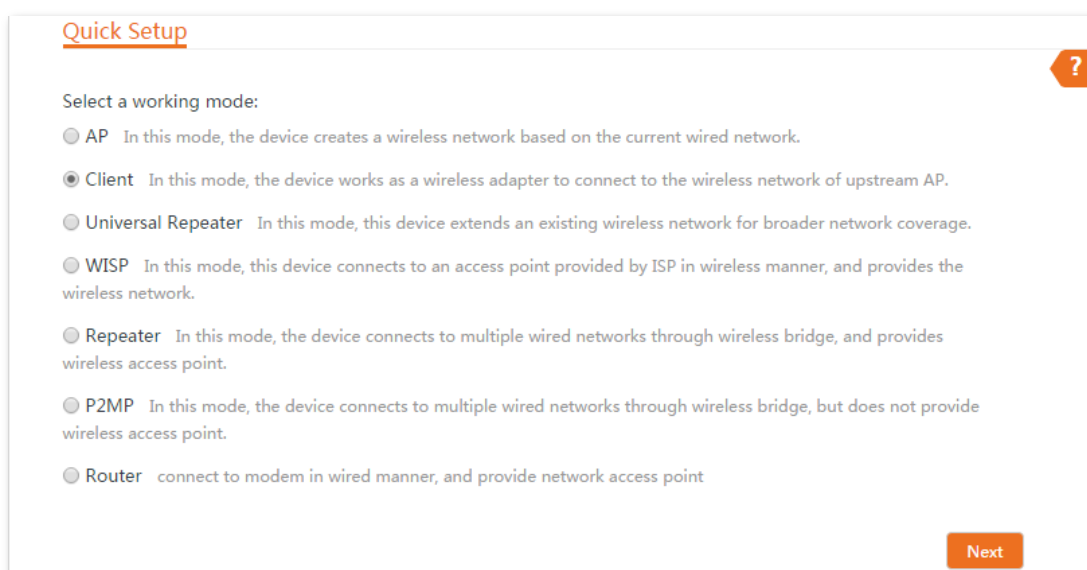
The CPE in client mode usually works with the CPE in AP mode to establish a CCTV surveillance network, and use the CPE in client mode to connect to IP cameras. The network topology is shown as below.



4.2.2 Quick setup

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

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



- Step 3** Select the SSID of the upstream AP, which is **Tenda_123456** in this example, and click **Next** at the bottom of the page.

[Quick Setup](#) >> [Client](#)

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

Scan [Scan again](#)

Upstream AP

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="radio"/>	Tenda_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	



- TIP**
- If you cannot find any SSID from the list, choose **Wireless > Basic** and enable the wireless function. Then try again.
 - If you cannot find the SSID of the upstream AP from the list:
 - Ensure that the WiFi network of the upstream AP is enabled. Only the WiFi networks at the same band as that of the CPE will be displayed in the list.
 - Adjust the direction of the CPE, and move it closer to the upstream AP.

- Step 4** Enter the WiFi password for the selected WiFi network **Tenda_123456** in the **Key** text box, and click **Next**.

[Quick Setup](#) >> [Client](#)

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

Upstream AP

Upstream AP MAC Address

Channel

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

* Key

Parameters description

Name	Description
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.

Name	Description
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

Step 5 Set the **IP address** to an unused IP address belonging to the same network segment as that of the upstream AP. Then set the **Subnet Mask** to the same one of the upstream AP, and click **Next**.

For example, if the IP address of the upstream AP is 192.168.2.1, you can set the IP address of this device to 192.168.2.X (X ranges from 2 to 254).

Quick Setup >> Client

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

IP Address

Subnet Mask

Previous Next

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

Quick Setup >> Client

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

Previous Save

----End

When the LED1, LED2, and LED3 of CPE are keep blinking, the bridging succeeds.

4.2.3 Example of establishing a CCTV surveillance network (AP mode + client mode)

Networking requirement

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



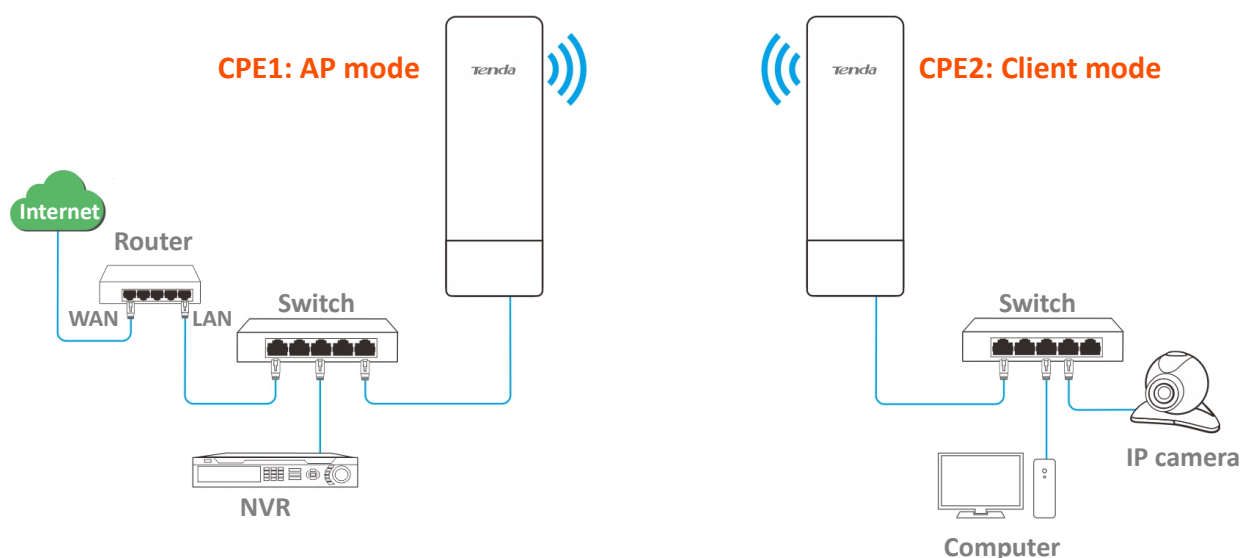
A CPE can support several IP cameras. The maximum number of IP cameras can be calculated with the following formula:

Number of IP cameras=(Transmitted/received rate of the CPE)*70% / Data rate of IP camera

Solution

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

Network topology



Configuration procedures

Step 1 Set CPE1 to AP mode.

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

Quick Setup ?

Select a working mode:

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

Next

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

Quick Setup >> AP ?

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

* SSID

Channel

* Security Mode

Encryption Algorithm AES TKIP TKIP&AES

* Key

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

Quick Setup >> AP ?

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

Step 2 Set CPE2 to Client mode.

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

Quick Setup ?

Select a working mode:

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

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

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

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

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

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

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

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

Quick Setup >> Client ?

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

Scan [Scan again](#)

Upstream AP

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="radio"/>	Tenda_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	



If you cannot find the SSID of CPE1 from the list, adjust the direction of CPE2, and move it closer to the CPE1.

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

Quick Setup >> Client ?

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

Upstream AP

Upstream AP MAC Address

Channel

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

* Key

5. Set the **IP address** to an unused IP address belonging to the same network segment as that of CPE1. Then set the **Subnet Mask** to the same one of the peer device, and click **Next**.

For example, if the IP address of CPE1 is 192.168.2.1, you can set the IP address of the device to 192.168.2.X (X ranges from 2 to 254).

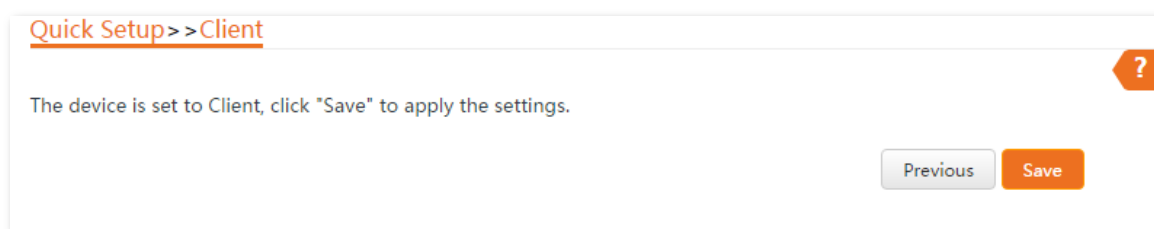
Quick Setup >> Client ?

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

IP Address

Subnet Mask

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



----End

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



TIP

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

Verification

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

4.3 Universal repeater mode

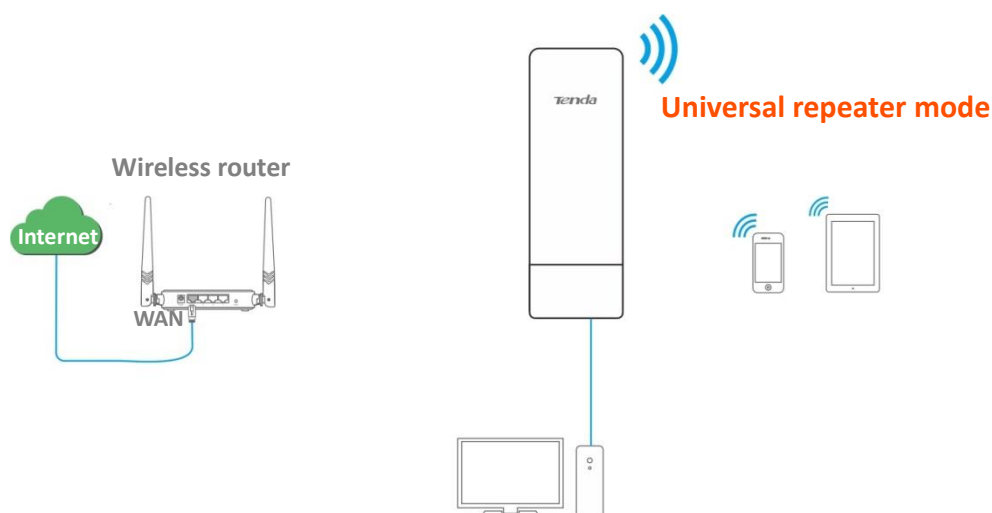
4.3.1 Overview

In Universal Repeater mode, the CPE expands your WiFi network for broader network coverage.

Advantage of Universal Repeater compared with [Repeater mode](#): This mode does not require that the upstream AP supports the WDS function.

Application scenario

The CPE is used to extend your existing wireless network. The network topology is shown as below.



4.3.2 Quick setup

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

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

Quick Setup ?

Select a working mode:

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

Next

Step 3 Select the SSID of the upstream AP, which is **WiFi_123456** in this example, and click **Next** at the bottom of the page.

Quick Setup >> Universal Repeater

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

Scan [Scan again](#)

Upstream AP

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="radio"/>	WiFi_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	



- If you cannot find any SSID from the list, choose **Wireless > Basic** and enable the wireless function. Then try again.
- If you cannot find the SSID of the upstream AP from the list:
Ensure that the WiFi network of the upstream AP is enabled. Only the WiFi networks at the same band as that of the CPE will be displayed in the list.
Adjust the direction of the CPE, and move it closer to the upstream AP.

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

Quick Setup >> Universal Repeater

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

Upstream AP

Upstream AP MAC Address

Channel

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

* Key

Parameters description

Name	Description
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.

Name	Description
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

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

[Quick Setup](#) >> [Universal Repeater](#) ?

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

IP Address

Subnet Mask

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

[Quick Setup](#) >> [Universal Repeater](#) ?

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

----End

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

To access the internet with:

- Wireless devices: Connect the wireless devices, such as a smart phone, to the WiFi network of the CPE using the WiFi name and password of the upstream AP.
- Wired devices: Connect the wired devices, such as a computer, to the LAN port of the CPE, or the switch connected to the LAN port of the PoE injector.

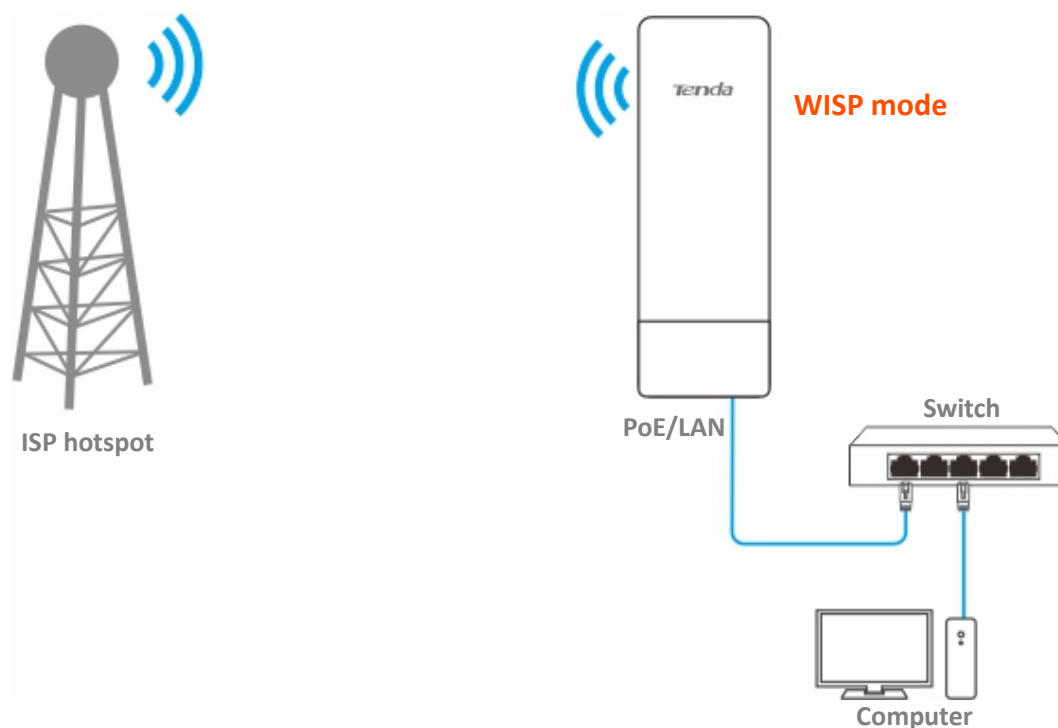
4.4 WISP mode

4.4.1 Overview

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

Application scenario

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



4.4.2 Quick setup

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

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

Quick Setup ?

Select a working mode:

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

Next


Step 3 Select the SSID of upstream AP, which is **WiFi_123456** in this example, and click **Next** at the bottom of the page.

Quick Setup > > WISP ?

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

Scan [Scan again](#)

Upstream AP

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="radio"/>	WiFi_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	



- TIP**
- If you cannot find the SSID of the wireless network from the list, choose **Wireless > Basic** to enter the page and ensure that the wireless network function is enabled.
 - If you cannot find the SSID of the upstream AP from the list:
 - Ensure that the WiFi network of the upstream AP is enabled. Only the WiFi networks at the same band as that of the CPE will be displayed in the list.
 - Adjust the direction of the CPE, and move it closer to the upstream AP.

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

[Quick Setup](#) >> [WISP](#)

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

Upstream AP WiFi_123456

Upstream AP MAC Address C8:3A:35:15:86:A1

Channel

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

* Key

Parameters description

Name	Description
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

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

[Quick Setup](#) >> [WISP](#)

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

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

PPPoE User Name

PPPoE Password

Parameter description

Name	Description
Internet Connection Type	<ul style="list-style-type: none"> DHCP (Dynamic IP): The device obtains an IP address and other parameters from the DHCP server of upstream device for internet access.

Name	Description
	<ul style="list-style-type: none"> • Static IP Address: The device accesses the internet by setting the IP address, subnet mask, default gateway and DNS server IP addresses manually. • PPPoE: The device accesses the internet using the PPPoE user name and password provided by the ISP.

Step 6 Customize the SSID (which is **Marry's WiFi** in this example) and key, and click **Next**.

Step 7 Set an IP address belonging to a different network segment as that of your ISP hotspot. For example, if the IP address of your ISP hotspot is 192.168.2.1, you can set this device's IP address to 192.168.X.1 (X ranges from 0 to 254 excluding 2) which is also the login IP address of the CPE. Then click **Next**.

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

----End

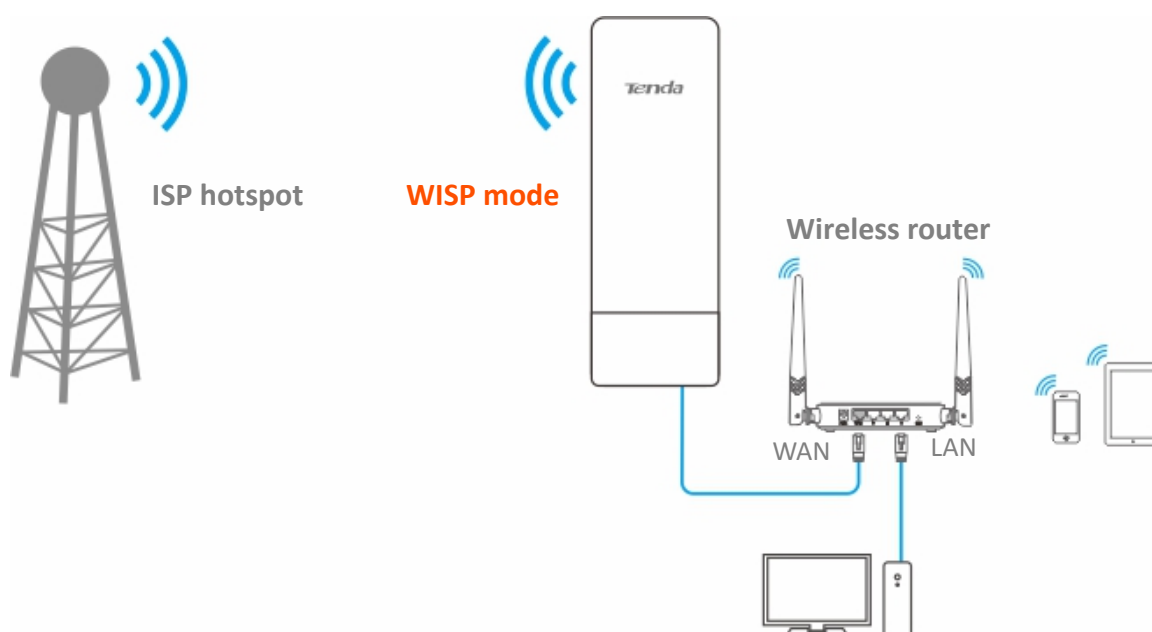
After the CPE reboots, log in to the Web UI of the device again and choose **Status** to enter the

page. If the WAN IP address, default gateway and DNS server information obtained by the WAN port are displayed on the **System Status** section, the configuration succeeds.

After successful configuration, devices connected to the CPE can access to 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 name and password of the wireless network are SSID and Key set in **Step 6** above.



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



For detailed configuration of the router, please refer to the corresponding user guide.

Step 1 Log in to the Web UI of the router.

Step 2 Select **Dynamic IP** as the **Internet Connection Type**, and save the settings.

----End

To access the internet with:

- **Wireless devices:** Connect the wireless devices, such as a smart phone, to the WiFi network of the wireless router which is connected to the CPE.
- **Wired devices:** Connect the wired devices, such as a computer, to the LAN ports of the wireless router which is connected to the CPE. Ensure that the IP address of the computer is automatically obtained.

4.4.3 Example of wireless ISP hotspot access

Networking requirement

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

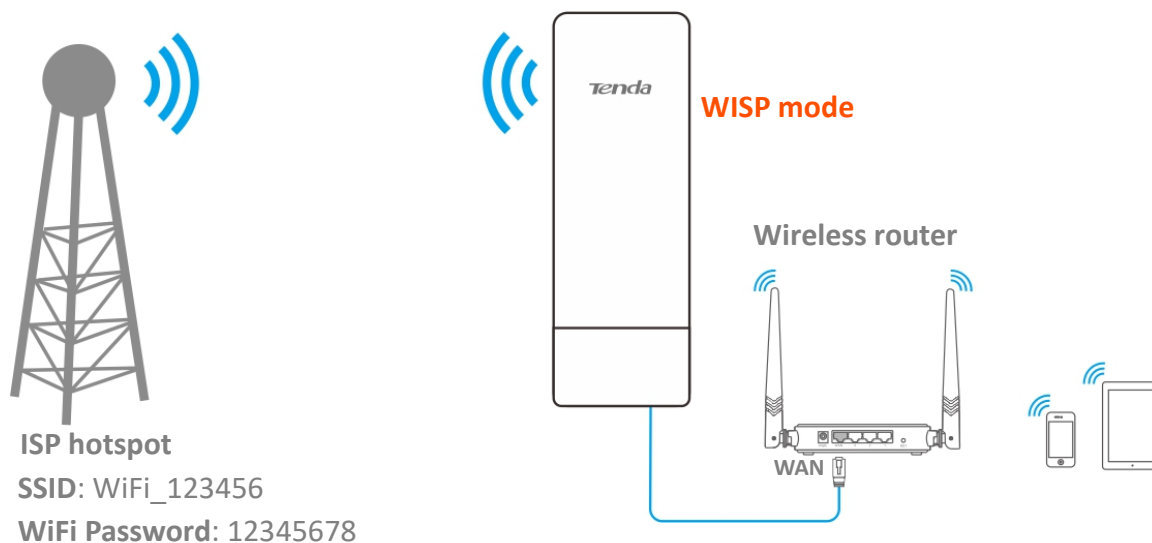
Solution

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

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

- SSID: WiFi_123456
- Password: 12345678
- Internet Connection Type: PPPoE
User name: admin
Password: admin

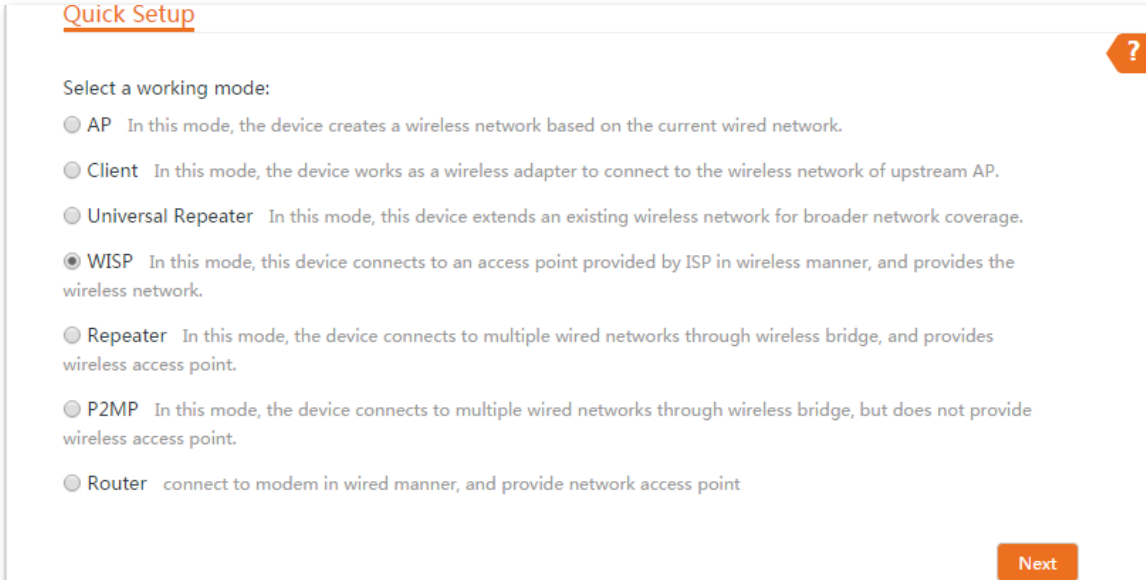
Network topology



Configuration procedures

Step 1 Set the CPE to the WISP mode.

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



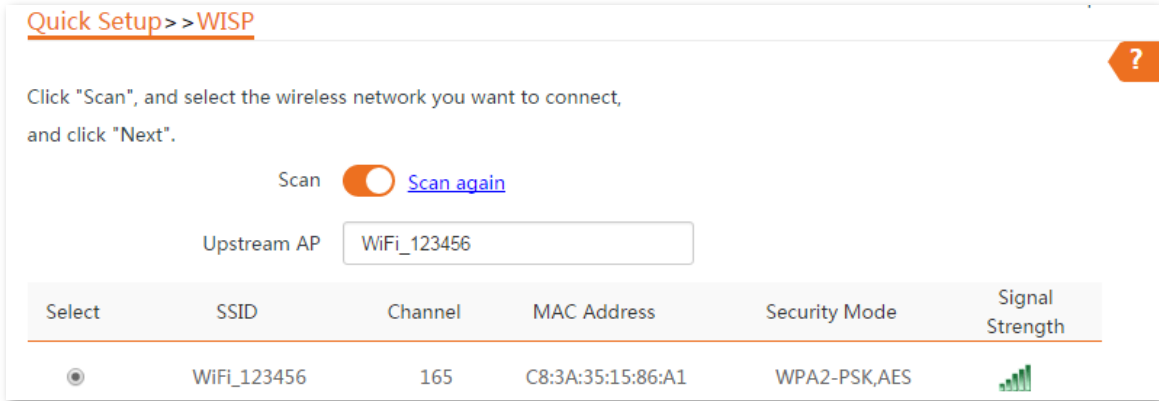
Quick Setup ?

Select a working mode:

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

Next

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




Quick Setup >> WISP ?

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

Scan [Scan again](#)

Upstream AP

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="radio"/>	WiFi_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	

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

[Quick Setup](#) > > [WISP](#)

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

Upstream AP WiFi_123456

Upstream AP MAC Address C8:3A:35:15:86:A1

Channel 165(5825MHz)

Security Mode WPA2-PSK

Encryption Algorithm AES TKIP TKIP&AES

* Key

Previous Next

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**.

[Quick Setup](#) > > [WISP](#)

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

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

PPPoE User Name

PPPoE Password

Previous Next

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

[Quick Setup](#) > > [WISP](#)

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

* SSID(WiFi Name) Mary's WiFi

Channel 165(5825MHz)

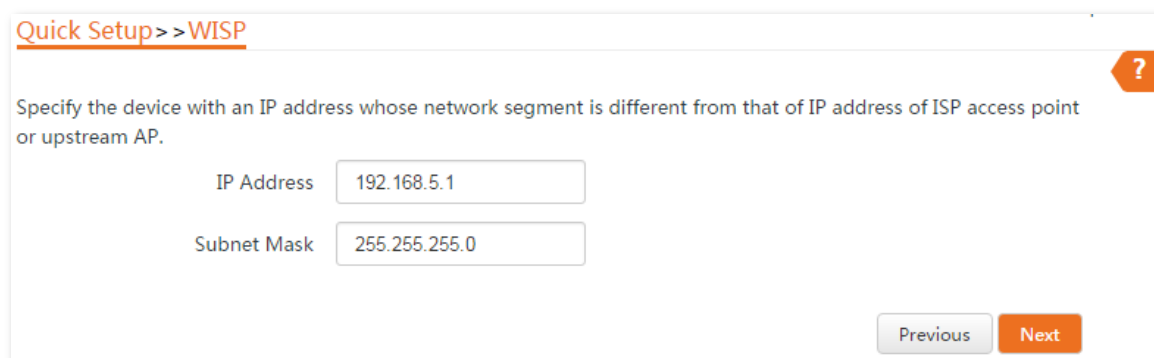
Security Mode WPA2-PSK

Encryption Algorithm AES TKIP TKIP&AES

* Key

Previous Next

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



Quick Setup >> WISP

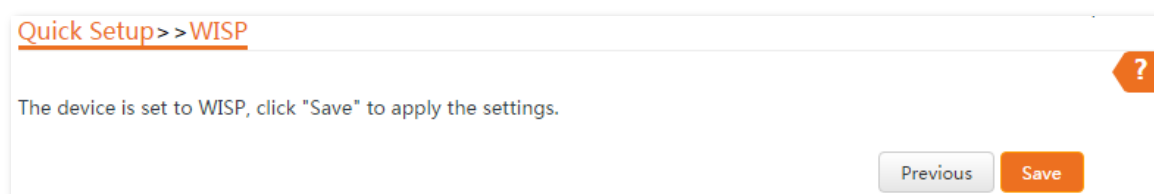
Specify the device with an IP address whose network segment is different from that of IP address of ISP access point or upstream AP.

IP Address

Subnet Mask

[Previous](#) [Next](#)

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



Quick Setup >> WISP

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

[Previous](#) [Save](#)

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

Step 2 Set the wireless router.

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

----End

Verification

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

4.5 Repeater mode

4.5.1 Overview

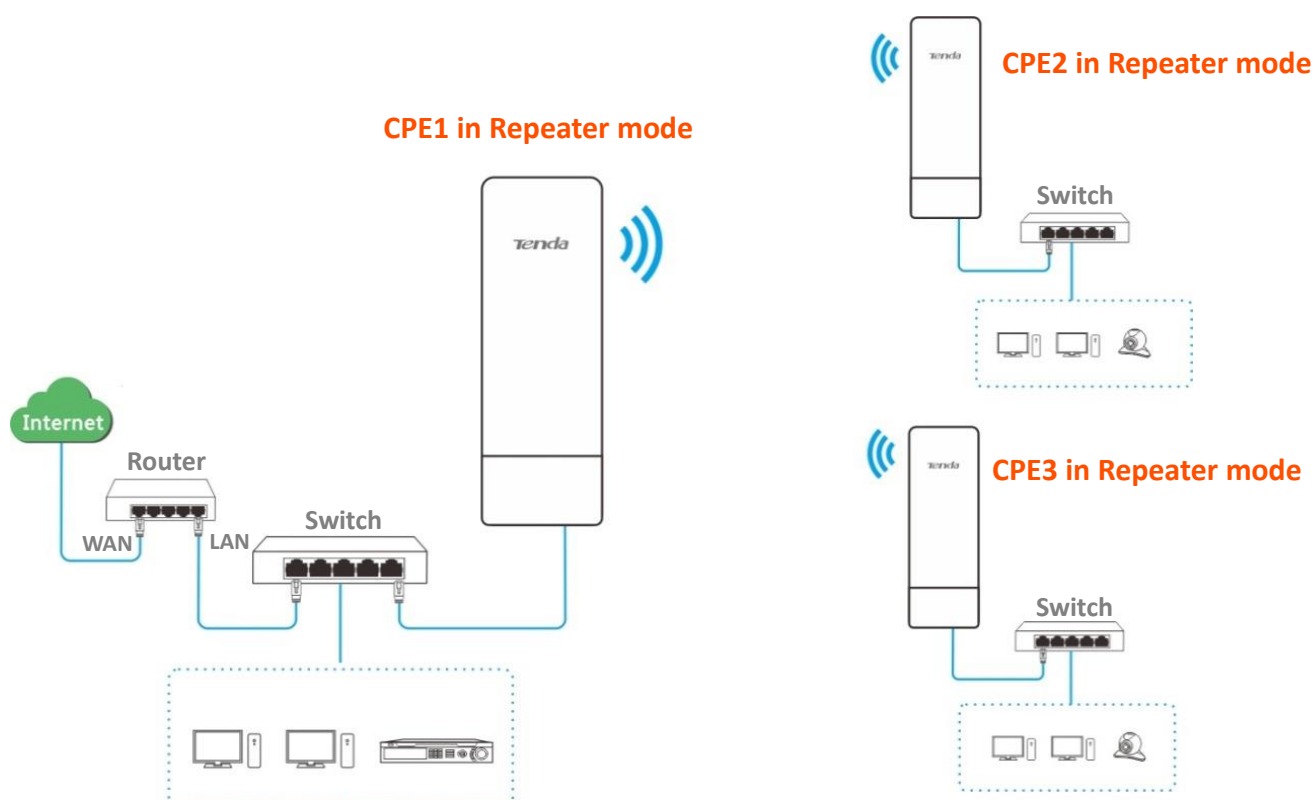
In Repeater mode, the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients.

To use this function, the peer AP is required to support WDS function. Repeater mode can be used to achieve communication between multiple office sites of an enterprise in a city.

The CPE in Repeater mode can work with the CPE in Repeater or [P2MP mode](#).

Application scenario

You want to combine multiple wired networks into one in a wireless manner. The network topology is shown as below.

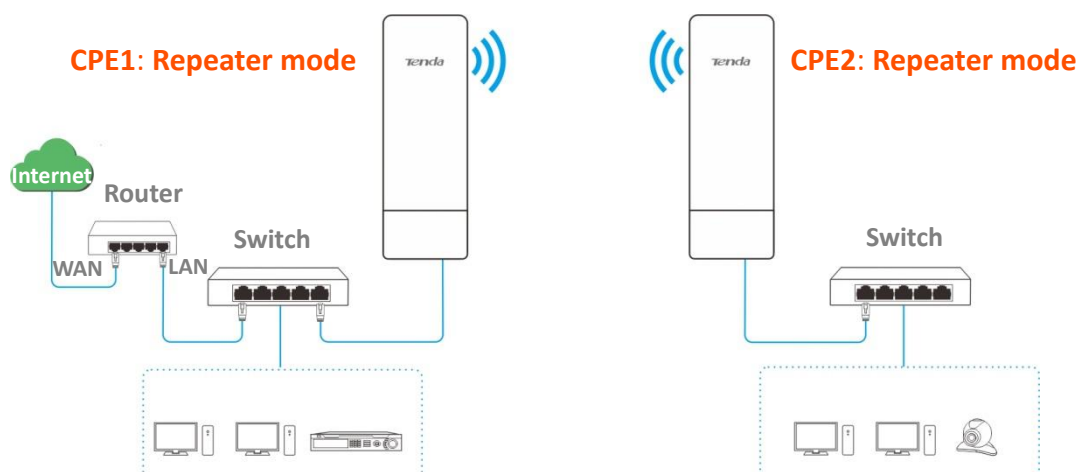


4.5.2 Quick setup



When configuring the Repeater mode, please ensure that the Channel and Channel Bandwidth of all CPEs are the same.

Peer to peer bridging



Assume that the related parameters are as follows:

CPE1

- **SSID:** Tenda_123456
- **Channel:** 165
- **Security mode:** WEP
- **Authentication type:** Shared
- **Default key:** Key 1, 12345

CPE2

- **SSID:** Tenda_654321
- **WLAN MAC Address:** C8:3A:35:15:86:B2



To check the SSID and key of the CPE, you can log in to the web UI of the CPE and choose **Wireless > Basic** to enter the page.

Step 1 Set the CPE2 to the **Repeater** mode.

1. Log in to the web UI of CPE2, and choose **Wireless > Basic** to enter the configuration page.
2. Modify the **Channel** (165 in this example) and **Channel Bandwidth** (20MHz in this example), and click **Save**.

Basic

Enable Wireless

Country/Region

SSID

Broadcast SSID Enable Disable

Network Mode

* Channel

Channel Shift Enable Disable

Transmit Power 1dBm 26dBm

* Channel Bandwidth

Transmit Rate

Security Mode

Isolate Client Enable Disable

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

3. Choose **Quick Setup** to enter the configuration page. Click **Repeater** and then **Next**.

Quick Setup ?

Select a working mode:

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

- Select the SSID of CPE1 from the list, which is **Tenda_123456** in this example, and click **Next** at the bottom of the page.

[Quick Setup](#) >> [Repeater](#)

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


Scan [Scan again](#)

Peer AP1

Peer AP2

Peer AP3

Peer AP4

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="checkbox"/>	Tenda_123456	165	C8:3A:35:15:86:A1	WEP	



- If wireless networks cannot be scanned, make sure you have toggled on **Enable Wireless** on **Wireless > Basic** page.
 - Only the WiFi networks whose security modes are set to none or WEP can be displayed on the list.
- Set the **Authentication Type** and **Default Key** to the same as those of CPE1, enter the key 1, and click **Next**.

[Quick Setup](#) >> [Repeater](#)

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

Peer AP1 Tenda_123456

MAC Address of Peer AP1 C8:3A:35:15:86:A1

Channel

Security Mode

Authentication Type

Default Key


Key 1

Key 2


Key 3

Key 4

Parameters description

Name	Description
Peer AP1	It specifies the wireless network name (SSID) of the peer AP1.
MAC Address of Peer AP1	It specifies the MAC address of the wireless network to be bridged.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	<p>It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.</p> <p> TIP</p> <p>The Repeater mode only supports WEP and None security modes.</p>

- Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of CPE1 is 192.168.2.1, you can set this device's IP address to 192.168.2.X (X ranges from 2 to 254). Then set the Subnet Mask to the same one of the CPE1, and click **Next**.


Quick Setup > > Repeater 

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

IP Address

Subnet Mask

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

Quick Setup > > Repeater 

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

Step 2 Perform the procedure in [Step 1](#) above to set the CPE1 to **Repeater** mode. The differences are listed below:

- Select the SSID of CPE2, which is **Tenda_654321** in this example.
- Do not need to change the IP address of CPE1.



If there are multiple wireless networks with the same SSID, select the one with the WLAN MAC address of the CPE2, which is **C8:3A:35:15:86:B2** in this example.

----End

To check whether the bridging is successful:

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

Method 2:

Step 1 Log in to the web UI of CPE1.

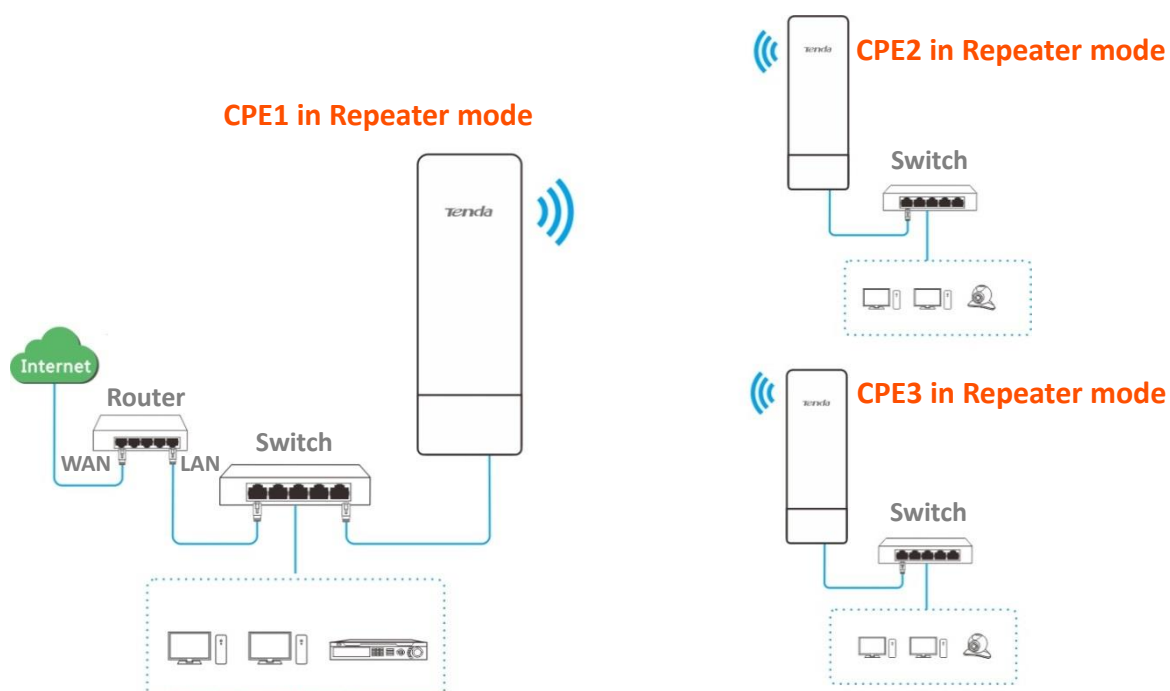
Step 2 Choose **Advanced > Diagnose**, select **Ping** from the **Diagnose** drop-down list menu, enter the IP address of CPE2 and click **Start**.

The screenshot shows the 'Diagnose' web interface with the following fields and options:

- Diagnose:** A dropdown menu set to 'Ping'.
- IP Address:** A dropdown menu set to 'Manual'.
- IP Address/Domain Name:** An empty text input field.
- Ping Packet:** A text input field containing '4', with '(Range: 1 to 10000)' to its right.
- Packet Size:** A text input field containing '32', with 'Byte (Range: 1 to 60000)' to its right.
- Start:** An orange button at the bottom center.

The bridging is successful when the ping succeeds.

Peer to multiple peers bridging



Assume that the related parameters are shown as follows:

CPE1:

- **IP Address:** 192.168.2.1
- **SSID:** Tenda_123456
- **Channel:** 165
- **Channel bandwidth:** 20MHz
- **Security mode:** None

CPE2:

- **SSID:** Tenda_1
- **WLAN MAC address:** C8:3A:35:15:86:8C

CPE3:

- **SSID:** Tenda_2
- **WLAN MAC address:** C8:3A:35:01:8C:C9

Step 1 Set the CPE2 to the **Repeater** mode.

1. Log in to the web UI of CPE2.
2. Modify the **Channel** (165 in this example) and **Channel Bandwidth** (20MHz in this example), and click **Save**.

Basic

Enable Wireless

Country/Region

SSID

Broadcast SSID Enable Disable

Network Mode

* Channel

Channel Shift Enable Disable

Transmit Power 1dBm 26dBm

* Channel Bandwidth

Transmit Rate

Security Mode

Isolate Client Enable Disable

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

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

Quick Setup ?

Select a working mode:

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

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

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

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

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

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

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

Next

4. Select the SSID of CPE1 from the list, which is **Tenda_123456** in this example, and click **Next** at the bottom of the page.



- If you cannot scan the SSID of CPE1 from the list, choose **Wireless > Basic** and enable the wireless function. Then try again.
- Only the WiFi networks whose security modes are set to none or WEP can be displayed on the list.

Quick Setup >> Repeater ?

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

Scan [Scan again](#)

Peer AP1

Peer AP2

Peer AP3

Peer AP4

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="checkbox"/>	Tenda_123456	165	C8:3A:35:15:86:A1	None	

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

[Quick Setup](#) >> [Repeater](#)

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

Peer AP1 Tenda_123456

MAC Address of Peer AP1 C8:3A:35:15:86:A1

Channel

Security Mode

6. Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of the CPE1 is **192.168.2.1**, you can set this device's IP address to 192.168.2.X (X ranges from 2 to 254). Then set the Subnet Mask to the same one of the CPE1, and click **Next**.

[Quick Setup](#) >> [Repeater](#)

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

IP Address

Subnet Mask

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

[Quick Setup](#) >> [Repeater](#)

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

Step 2 Perform [Step 1](#) above to set CPE3 to **Repeater** mode, and bridge to CPE1.

Step 3 Set CPE1 to **Repeater** mode and bridge to CPE2 and CPE3.

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



If there are multiple wireless networks with the same SSID, select the ones with the WLAN MAC addresses of the CPE2 and CPE3, which are **C8:3A:35:15:86:8C** and **C8:3A:35:01:8C:C9** in this example.

[Quick Setup](#) >> [Repeater](#)

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



Scan [Scan again](#)

Peer AP1

Peer AP2

Peer AP3

Peer AP4

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="checkbox"/>	Tenda_1	165	C8:3A:35:15:86:8C	None	
<input checked="" type="checkbox"/>	Tenda_2	165	C8:3A:35:01:8C:C9	None	

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

[Quick Setup](#) >> [Repeater](#)

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

Peer AP1 Tenda_1

MAC Address of Peer AP1 C8:3A:35:15:86:8C

Channel

Security Mode

5. Click **Next**.

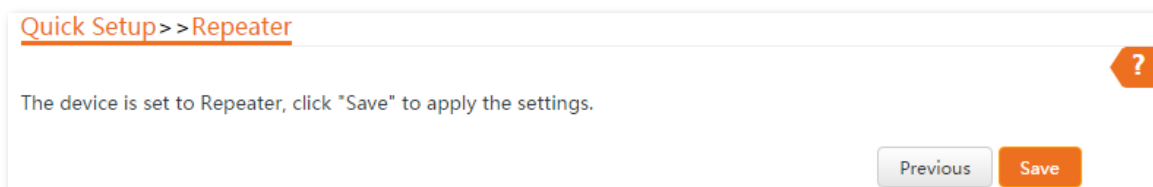
[Quick Setup](#) >> [Repeater](#)

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

IP Address

Subnet Mask

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



----End

To check whether the bridging is successful:

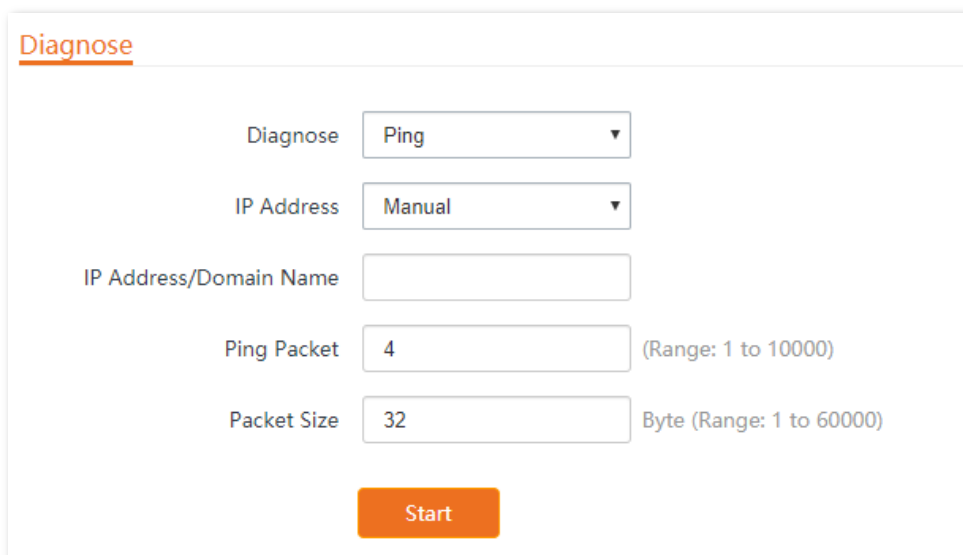
Method 1: When the LED1, LED2, and LED3 indicators of CPE1, CPE2 and CPE3 are solid on, the bridging succeeds.

Method 2:

Step 1 Log in to the web UI of CPE1.

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

The bridging is successful when the ping succeeds.



4.6 P2MP mode

4.6.1 Overview

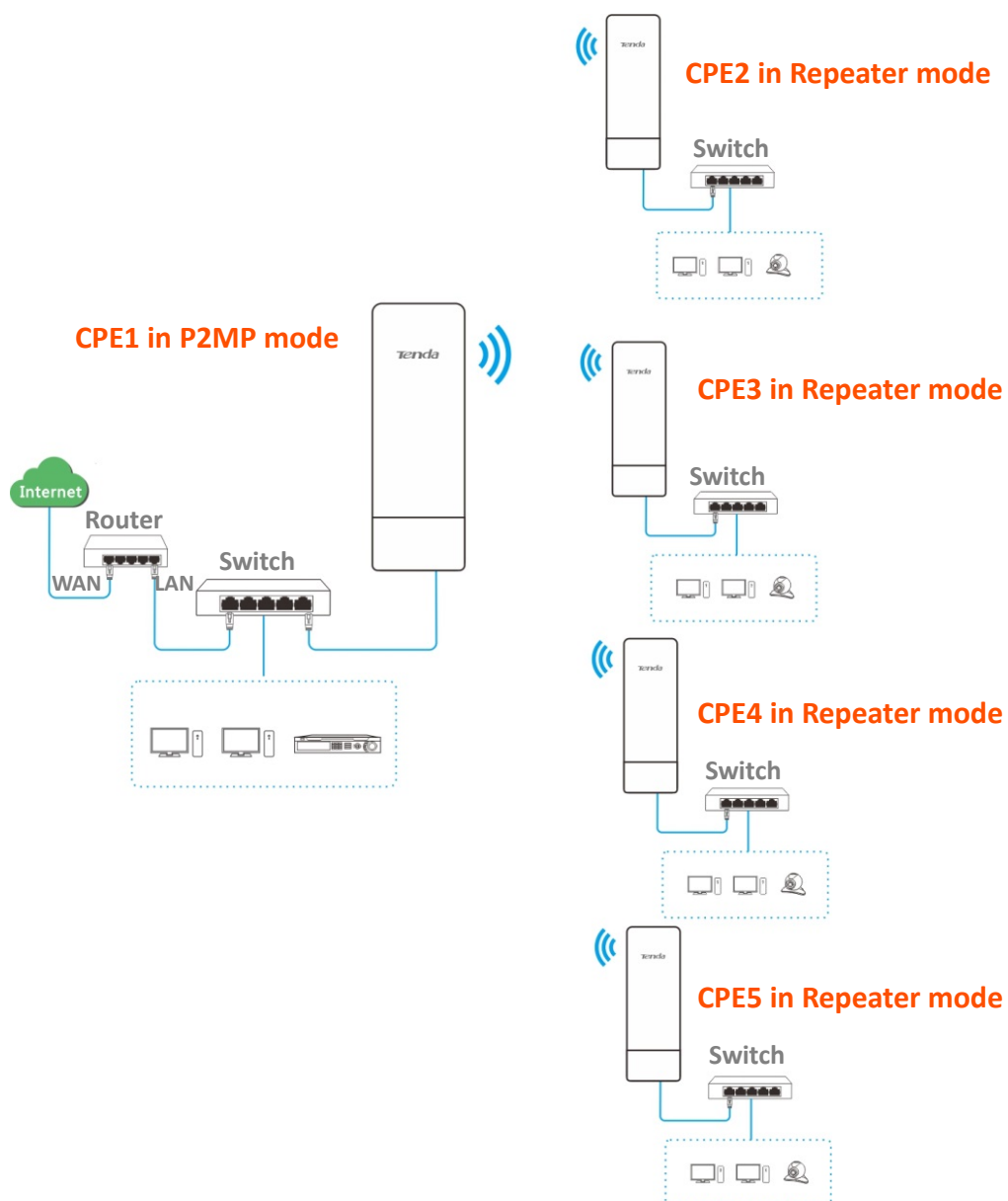
In **P2MP** mode, the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and it does not provide wireless access service.

The CPE in P2MP mode can work with the CPE in Repeater mode.

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

Application scenario

The CPE is used to combine 4 local networks into one in a wireless manner. The network topology is shown as below.



4.6.2 Quick setup

Assume that the related parameters are shown as follows:

CPE1:

- **IP Address:** 192.168.2.1
- **SSID:** Tenda_1
- **Channel:** 165
- **Channel Bandwidth:** 20MHz
- **Security Mode:** None

CPE2 to CPE5:

CPE	SSID	WLAN MAC address
CPE2	Tenda_2	C8:3A:35:01:8C:C9
CPE3	Tenda_3	C8:3A:35:35:BA:01
CPE4	Tenda_4	C8:3A:35:FD:8D:A1
CPE5	Tenda_5	C8:3A:35:09:93:51

Configuration procedures



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

Step 1 Set CPE2 to **Repeater** mode and bridge to the CPE1.

1. Log in to the web UI of CPE2
2. Choose **Wireless > Basic** to modify the channel and Channel Bandwidth of the CPE, which are 165 and 20MHz in this example.

Basic ?

Enable Wireless

Country/Region

SSID

Broadcast SSID Enable Disable

Network Mode

* Channel

Channel Shift Enable Disable

Transmit Power
1dBm 23dBm

* Channel Bandwidth

Transmit Rate

Security Mode

3. Choose **Quick Setup**, select **Repeater** mode, and click **Next**.

Quick Setup ?

Select a working mode:

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

Next

4. Select the SSID of CPE1, which is **Tenda_1** in this example, and click **Next** at the bottom of the page.

[Quick Setup](#) >> [Repeater](#)

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


Scan [Scan again](#)

Peer AP1

Peer AP2

Peer AP3

Peer AP4

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="checkbox"/>	Tenda_1	165	C8:3A:35:15:86:A1	None	



- TIP**
- If you cannot find any SSID from the list, choose **Wireless > Basic** and enable the wireless function. Then try again.
 - If you cannot find the SSID of CPE1 from the list, adjust the direction of the CPE2, and move it closer to the CPE1.
 - The repeater mode only supports **None** and **WEP** security modes.

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

[Quick Setup](#) >> [Repeater](#)

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

Peer AP1 Tenda_1

MAC Address of Peer AP1 C8:3A:35:15:86:A1

Channel

Security Mode

- Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of CPE1 is **192.168.2.1**, you can set the IP address of the device to 192.168.2.X (X ranges from 2 to 254). Then click **Next**.

[Quick Setup](#) >> [Repeater](#)

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

IP Address

Subnet Mask

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

[Quick Setup](#) >> [Repeater](#)

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

Step 2 Perform [Step 1](#) to set the CPE3, CPE4 and CPE5 to Repeater mode, and bridge to the CPE1.

Step 3 Set CPE1 to **P2MP** mode and bridge to CPE2, CPE3, CPE4 and CPE5.

- Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
- Select **P2MP** mode, and click **Next**.
- Select the SSID of CPE2, CPE3, CPE4 and CPE5, which are **Tenda_2**, **Tenda_3**, **Tenda_4** and **Tenda_5** in this example, and click **Next**.

[Quick Setup](#) >> [P2MP](#)

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





Scan [Scan again](#)

Peer AP1

Peer AP2

Peer AP3

Peer AP4

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="checkbox"/>	Tenda_2	165	C8:3A:35:01:8C:C9	None	
<input checked="" type="checkbox"/>	Tenda_3	165	C8:3A:35:35:BA:01	None	
<input checked="" type="checkbox"/>	Tenda_4	165	C8:3A:35:FD:8D:A1	None	
<input checked="" type="checkbox"/>	Tenda_5	165	C8:3A:35:09:93:51	None	

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

Quick Setup >> P2MP ?

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


Peer AP1 Tenda_2

MAC Address of Peer AP1 C8:3A:35:01:8C:C9

Channel

Security Mode

Parameters description

Name	Description
Peer AP1	It specifies the wireless network name (SSID) of the peer AP.
MAC Address of Peer AP1	It specifies the MAC address of the wireless network to be bridged.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.  TIP The P2MP mode only supports WEP and None security modes.

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

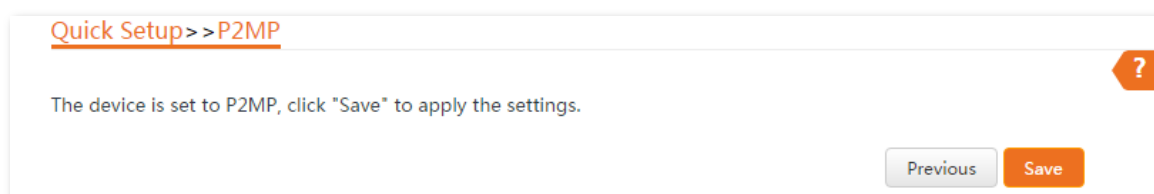
Quick Setup >> P2MP ?

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

IP Address

Subnet Mask

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



----End

To check whether the bridging is successful:

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

Method 2:

Step 1 Log in to the web UI of CPE1.

Step 2 Choose **Advanced > Diagnose**, select **Ping** from the **Diagnose** drop-down list menu, enter the IP addresses of the CPE2, CPE3, CPE4 and CPE5 respectively and click **Start**.

The bridging is successful when the ping succeeds.

4.6.3 Example of combining wired networks (repeater mode + P2MP mode)

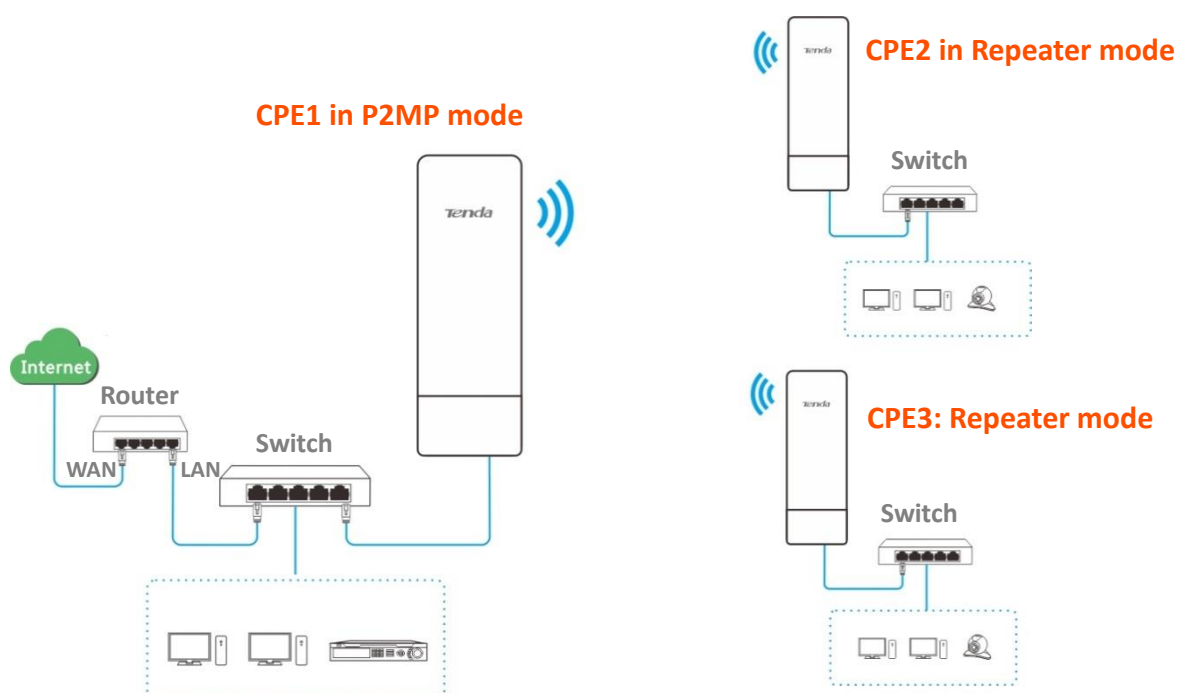
Networking requirement

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

Solution

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

Network topology



Configuration procedures

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

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

Step 1 Configure the wireless settings of CPE2.

1. Log in to the web UI of CPE2, and choose **Wireless > Basic** to enter the configuration page.
2. Change the SSID, which is **Tenda_1** in this example.

3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
4. Set the **Security Mode** to the same as that of CPE1, which is **None** in this example.
5. Click **Save** to apply the settings.

Basic

Enable Wireless

Country/Region

* SSID

Broadcast SSID Enable Disable

Network Mode

* Channel

Channel Shift Enable Disable

Transmit Power 1dBm 23dBm

Channel Bandwidth

Transmit Rate

* Security Mode

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

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

Quick Setup

Select a working mode:

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

Next

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



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

Quick Setup >> Repeater

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

Scan [Scan again](#)

Peer AP1

Peer AP2

Peer AP3

Peer AP4

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="checkbox"/>	Tenda_123456	165	C8:3A:35:15:86:A1	None	

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

Quick Setup >> Repeater

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

Peer AP1 Tenda_123456

MAC Address of Peer AP1 C8:3A:35:15:86:A1

Channel

Security Mode

- Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. For example, if the IP address of the CPE1 is **192.168.2.1**, you can set this device's IP address to 192.168.2.X (X ranges from 2 to 254). Then click **Next**.

[Quick Setup](#) >> [Repeater](#) ?

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

IP Address

Subnet Mask

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

[Quick Setup](#) >> [Repeater](#) ?

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

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

Step 4 Set CPE1 to **P2MP** mode and bridge to CPE2 and CPE3.

- Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
- Select **P2MP** mode, and click **Next**.

[Quick Setup](#) ?

Select a working mode:

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

3. Select SSIDs of CPE2 and CPE3, and click **Next** at the bottom of the following page.

Quick Setup >> P2MP

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



Scan [Scan again](#)

Peer AP1

Peer AP2

Peer AP3

Peer AP4

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
<input checked="" type="checkbox"/>	Tenda_1	165	C8:3A:35:15:86:A1	None	
<input checked="" type="checkbox"/>	Tenda_2	165	C8:3A:35:01:8C:C9	None	

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

Quick Setup >> P2MP

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

Peer AP1 Tenda_1

MAC Address of Peer AP1 C8:3A:35:15:86:A1

Channel

Security Mode

5. Click **Next**.

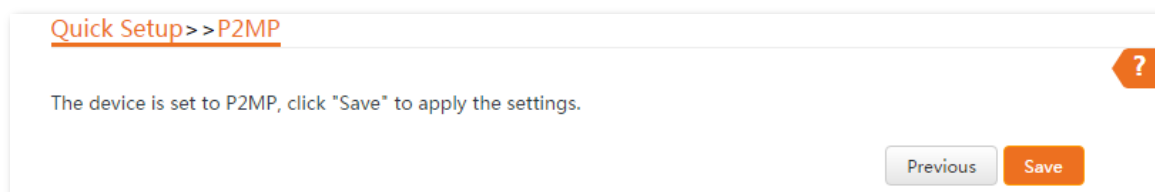
Quick Setup >> P2MP

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

IP Address

Subnet Mask

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



----End

Verification

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

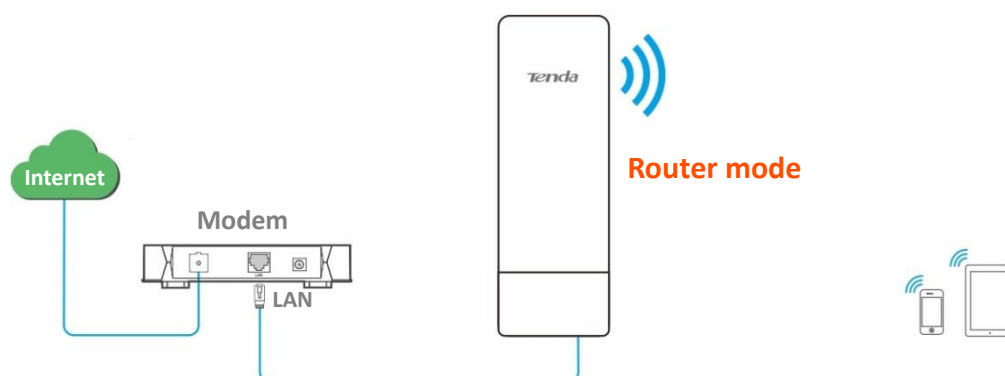
4.7 Router mode

4.7.1 Overview

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

Application scenario

The CPE is used to provide a wireless network and assign IP addresses to your wireless devices. The network topology is shown as below.



4.7.2 Quick setup



If there is only one Ethernet port on the CPE, you can 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 following configurations.

- Step 1** Log in to the web UI of the CPE, and choose **Quick Setup** to enter the configuration page.
- Step 2** Select **Router** mode, and click **Next**.

Quick Setup ?

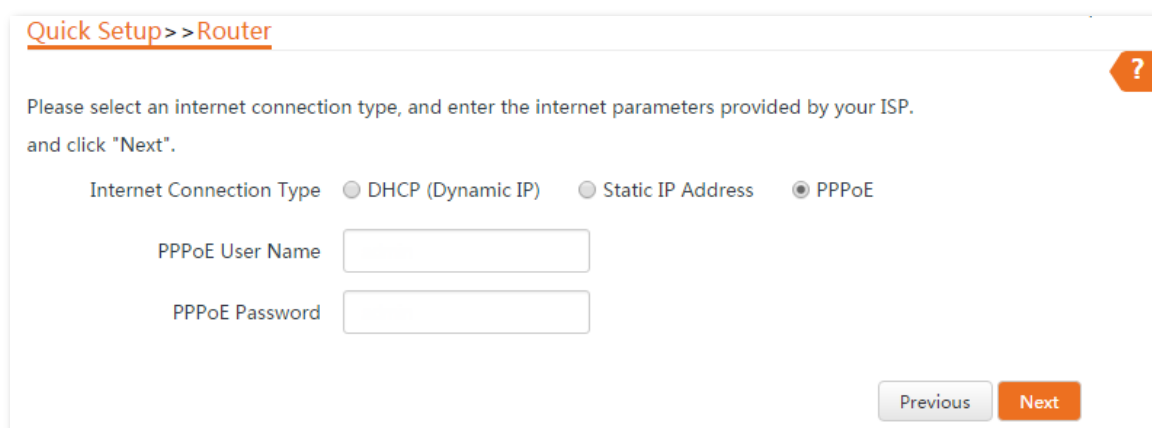
Select a working mode:

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

Next

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

1. Select **PPPoE**.
2. Enter the **PPPoE User Name** and **Password** provided by your ISP.
3. Click **Next**.



Parameters description

Name	Description
Internet Connection Type	<p>The device in Router mode supports three internet connection types:</p> <ul style="list-style-type: none"> • DHCP (Dynamic IP): The device obtains the IP address and other parameters from the DHCP server of upstream device for internet access. • Static IP Address: The device accesses the internet using the IP address, subnet mask, default gateway and DNS server IP addresses provided by your ISP. • PPPoE: The device accesses the internet using the PPPoE user name and password provided by the ISP.

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

1. Customize an SSID, which is **Tenda_123456** in this example.
2. Select a channel, which is **161** in this example.
3. Select a security mode, which is **WPA2-PSK** in this example.
4. Select an encryption algorithm, which is **AES** in this example.
5. Set a **Key** (WiFi password) for the wireless network.

[Quick Setup](#) > > [Router](#)

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

SSID

Channel

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

Key

Parameters description

Name	Description
SSID	It specifies the wireless network name of the device.
Channel	It specifies the channel that the WiFi network operates.
Security Mode	It specifies the security mode of the WiFi network of the device. It includes None , WPA-PSK , WPA2-PSK , and Mixed WPA/WPA2-PSK .
Encryption Algorithm	<p>It specifies the encryption method of the wireless network.</p> <ul style="list-style-type: none"> • AES: It indicates the Advanced Encryption Standard. • TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. • TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.

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

[Quick Setup](#) > > [Router](#)

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

----End

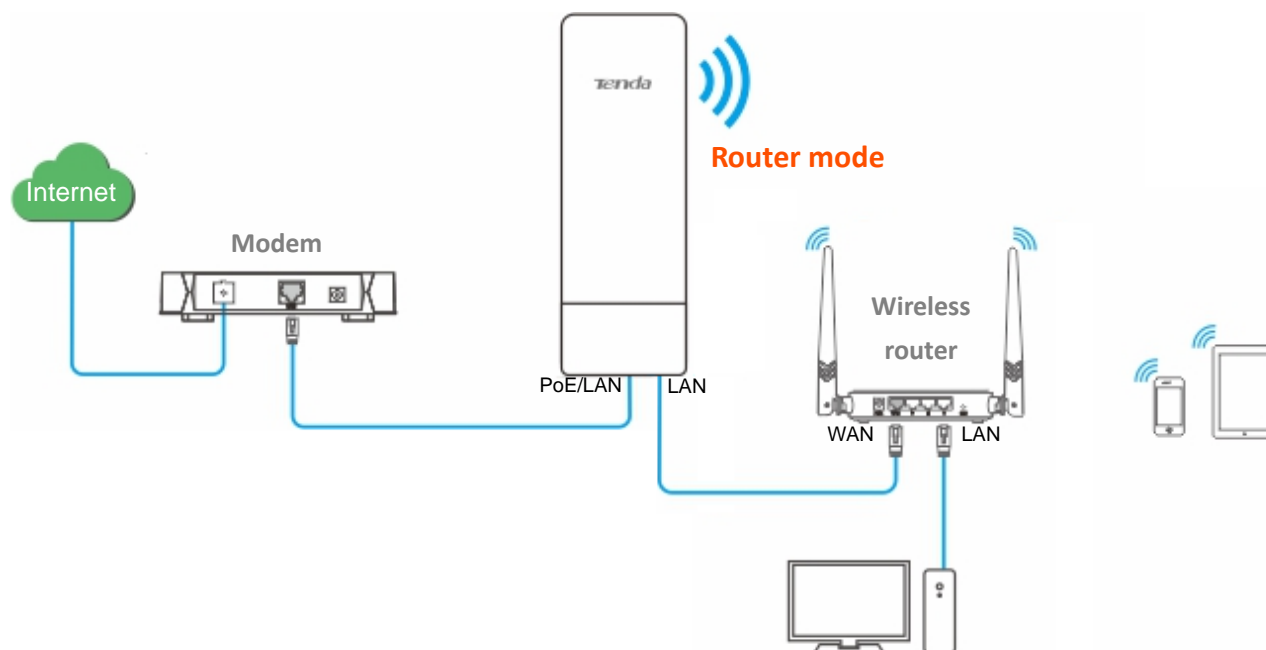
After the CPE reboots, log in to the Web UI of the CPE again and choose **Status** to enter the page. If the WAN IP address, default gateway and DNS server information obtained by the WAN port are displayed on the **System Status** section, the configuration succeeds.

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



- If there is only 1 LAN port on the CPE, you can connect your wireless 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](#) above.

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



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



For detailed configuration of the router, please refer to the corresponding user guide.

Step 6 Log in to the web UI of the router.

Step 7 Select **Dynamic IP** as the **Connection Type**, and save the settings.

----End

To access the internet with:

Wireless devices: Connect the wireless devices, such as a smart phone, to the WiFi network of the wireless router which is connected to the CPE.

Wired devices: Connect the wired devices, such as a computer, to the LAN ports of the wireless router which is connected to the CPE. Ensure that the IP address of the computer is automatically obtained.

5 Status

This module allows you to view the information of system and wireless network, including three parts: [system status](#), [wireless status](#), and [statistics](#).

To access the page, choose **Status**.

5.1 System status

You can view the system status here. O8V1.0 is used for illustration.

If the CPE is set to **AP** mode, **Client** mode, **Universal Repeater** mode, **Repeater** mode or **P2MP** 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.

System Status			
Device Name	O8V1.0	LAN Speed	100 Mbps Full-d...
Uptime	2 d17 m33 s	LAN IP Address	192.168.2.1
System Time	2021-11-11 10:23:35	Transparent Bridge	Disabled
Firmware Version	V1.0.0.10(7975)	Hardware Version	V1.0
CPU	4%	RAM	54%
LAN MAC Address	C8:3A:35:F8:CD:00	WLAN MAC Address	C8:3A:35:F8:CD:01

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 is changed to WAN port from LAN port.

Status		Current Mode: WISP	
System Status			
Device Name	O8V1.0	LAN Speed	100 Mbps Full-d...
Uptime	2 m41 s	LAN IP Address	192.168.2.1
System Time	2021-11-11 10:47:03	Connection Type	DHCP (Dynamic IP)
Firmware Version	V1.0.0.10(7975)	Connection Status	Connected
Hardware Version	V1.0	WAN IP Address	192.168.0.177
CPU	9%	Default Gateway	192.168.0.1
RAM	53%	Primary DNS Server	192.168.0.1
LAN MAC Address	C8:3A:35:F8:CD:00	Secondary DNS Server	
WLAN MAC Address	C8:3A:35:F8:CD:01		



Parameters description

Name	Description
Device Name	It specifies the name of this device. Different device names help you identify CPEs on LAN easily. You can change the name of this CPE on the Network > LAN Setup page when the device works in AP, Client, Universal Repeater, Repeater, and P2MP modes. When the device works in WISP or Router mode, it displays the model of the device, and cannot be changed.
Uptime	It specifies the time that has elapsed since the device was started last time.
System Time	It specifies the current system time of this device.
Firmware Version	It specifies the system firmware version number of this device.
Hardware Version	It specifies the hardware version number of this device.
CPU	Central Processing Unit. It specifies the CPU usage of this device.
RAM	Random Access Memory. It specifies the memory usage of this device.
LAN MAC Address	It specifies the MAC address of LAN port of this device.
WLAN MAC Address	It specifies the MAC address of the wireless network of this device.
Transparent Bridge	It displays the status of transparent bridge.

Name	Description
LAN Speed	It specifies the PoE/LAN or LAN port speed and duplex mode of this device.
LAN IP Address	<p>It specifies the IP address of this device, which is also the management IP address of this device.</p> <p>By default, it is 192.168.2.1. A LAN user can access the web UI of this device using this IP address. You can modify this IP address on Network > LAN Setup.</p>
Connection Type	<p>It specifies the internet connection type of this device in WISP or Router mode.</p> <ul style="list-style-type: none"> • DHCP (Dynamic IP): The CPE obtains IP address from the upstream DHCP server for internet access. • Static IP Address: The CPE uses a fixed IP address, subnet mask, default gateway, and DNS server info for internet access. • PPPoE: The CPE uses a user name and password for internet access.
Connection Status	It specifies the connection status of WAN port of this device in WISP or Router mode.
WAN IP Address	It specifies the IP address of WAN port of this device in WISP or Router mode.
Default Gateway	It specifies the default gateway address of this device in WISP or Router mode.
Primary DNS Server	It specifies the IP address of primary DNS server of this device in WISP or Router mode.
Secondary DNS Server	It specifies the IP address of secondary DNS server of this device in WISP or Router mode.

5.2 Wireless status

You can view wireless status here, including working mode, SSID, security mode, and so on. O6 is used for illustration here.

Wireless Status			
Working Mode	WISP	AP's MAC Address	50:2B:73:F8:F9:8A
SSID	Tenda_F8CD00	Signal Strength	 -57dBm
Security Mode	None	Background Noise	 -103dBm
Channel/Radio Band	161/5805MHz	TX/RX Link	1X1
Channel Bandwidth	80MHz	Transmit/Receive Speed	72Mbps/292Mbps
TX Power	25dBm	TD-MAX	Disabled
Wireless Client	0	Distance	N/Akm

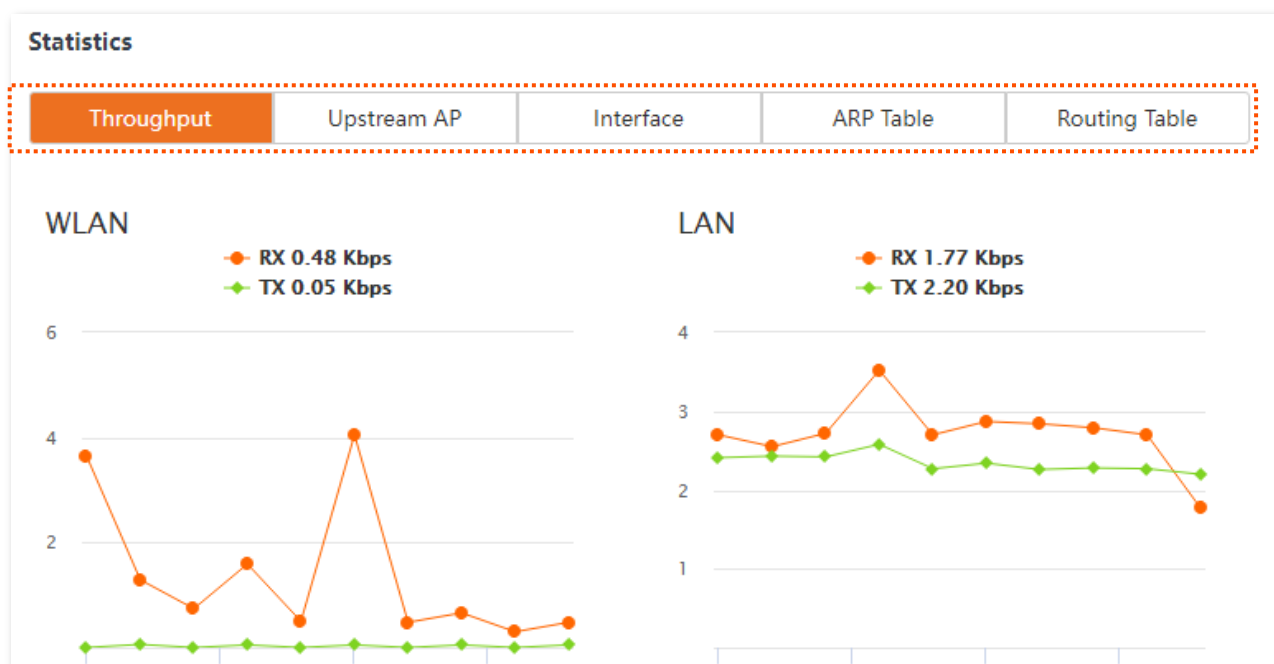
Parameters description

Name	Description
Working Mode	It specifies the working mode in which the device operates.
SSID	It specifies the wireless network name of this device.
Security Mode	It specifies the security mode of the wireless network of this device.
Channel/Radio Band	It specifies the channel and radio band used by this device to transmit radio signals.
Channel Bandwidth	It specifies the channel bandwidth of this device.
TX Power	It specifies the transmitted power of this device.
Wireless Client	It specifies the number of wireless clients connected to this device.
AP's MAC Address	<p>It displays the MAC address of the upstream device.</p> <ul style="list-style-type: none"> In AP, Router, Repeater, or P2MP mode, it displays the WLAN MAC address of this CPE. 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.
Signal Strength	<p>It displays the wireless signal strength of the peer device.</p> <ul style="list-style-type: none"> In AP or Router mode, it displays the signal strength of the first device connected

Name	Description
	<p>to the wireless network of this device.</p> <ul style="list-style-type: none"> In Client, Universal Repeater, WISP, Repeater or P2MP mode, it displays the received signal strength of the peer AP.
Background Noise	<p>It specifies the strength of radio interference signals in the ambient environment that interferes with the wireless signal of this device in the same channel. Larger absolute value indicates less interference. For example, -95 dBm indicates less interference than that of -75 dBm.</p>
TX/RX Link	<p>It specifies the number of spatial streams of wireless data the device is transmitting or receiving. The more links indicates the more traffic.</p>
Transmit/Receive Speed	<p>It specifies the wireless transmitting/receiving rate.</p> <ul style="list-style-type: none"> In AP or Router mode: it displays the transmitting/receiving rate of the first device connected to the wireless network of this device. In Client, Universal Repeater, WISP, Repeater, or P2MP mode: it displays transmitting/receiving rate of this device.
TD-MAX	<p>It specifies the status of the TD-MAX function. For details, please refer to TD-MAX.</p>
Distance	<p>It specifies the distance between the two CPEs after the bridging succeeds.</p> <p>If there are more than two CPEs, it specifies the bridging distance between this CPE and the farthest CPE.</p>

5.3 Statistics

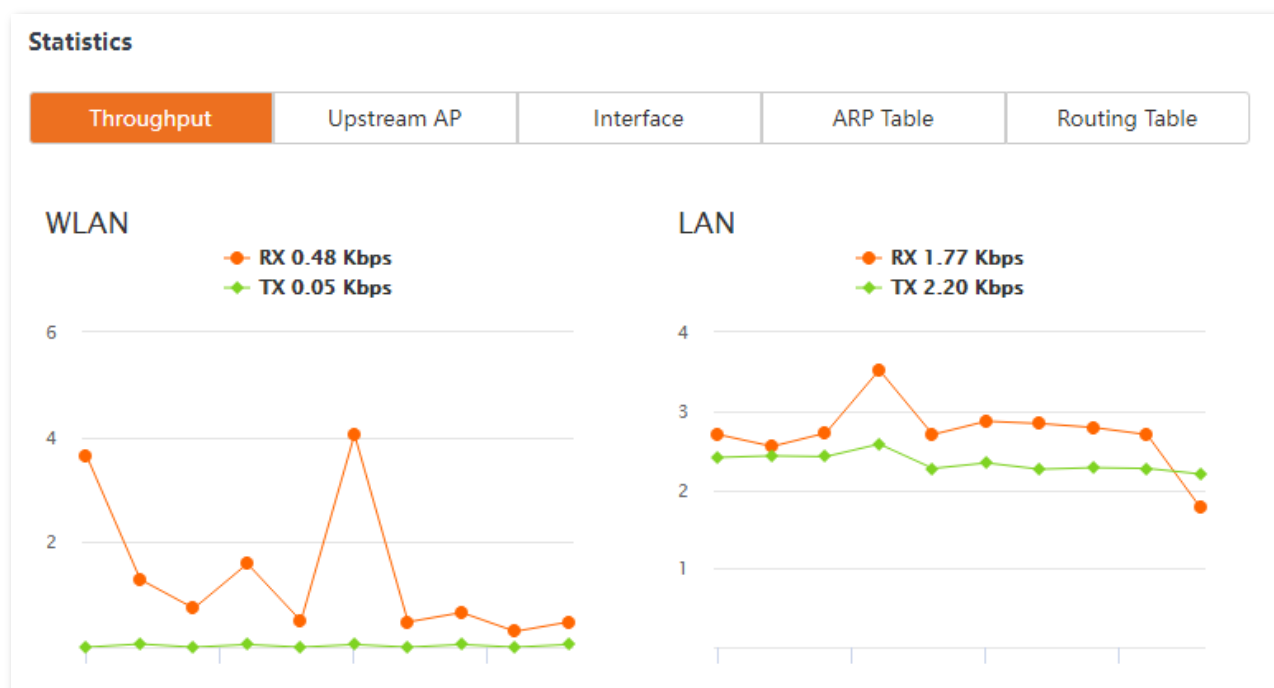
You can learn statistics information about [throughput](#), [wireless client](#), [interface](#), [ARP table](#) and [routing table](#) here.



5.3.1 Throughput

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

To access the page, choose **Status**, then click **Throughput** in **Statistics** part.



5.3.2 Wireless client

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

In **AP**, **Router**, **P2MP** or **Repeater** mode, it displays information of connected wireless clients.

To access the page, choose **Status**, then click **Wireless Client** in **Statistics** part.

Statistics					
Throughput	Wireless Client	Interface	ARP Table	Routing Table	
IP Address	MAC Address	Signal/Noise	Transmit/Receive	CCQ	Connection Duration
192.168.1.15	██████████	-37/-104dBm	120/351Mbps	100%	7 s

Parameters description

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

5.3.3 Upstream AP

In **Client**, **Universal Repeater** or **WISP** mode, it displays information of the upstream AP.

To access the page, choose **Status**, then click **Upstream AP** in **Statistics** part.

Statistics					
Throughput	Upstream AP	Interface	ARP Table	Routing Table	
IP Address	MAC Address	Signal/Noise	Transmit/Receive	CCQ	Connection Duration
N/A	50:2B:73:F8:F9:8A	-56/-103dBm	292/325Mbps	97%	19 m13 s

Parameters description

Name	Description
IP Address	It specifies the IP address of the upstream device.
MAC Address	It specifies the MAC address of the upstream device.
Signal/Noise	<ul style="list-style-type: none"> • Signal: It specifies the WiFi signal strength of the corresponding upstream AP. • Noise: It specifies the ambient interference signal and electromagnetic interference strength.
Transmit/Receive	It specifies the transmitting and receiving rate of the upstream device.
CCQ	It specifies the connection quality of the upstream device. A higher percentage indicates better connection quality.
Connection Duration	It specifies the time that has elapsed since this device bridges to the upstream device.

5.3.4 Interface

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

To access the page, choose **Status**, then click **Interface** in **Statistics** part.

Statistics						
Throughput		Upstream AP		Interface	ARP Table	Routing Table
Interface	IP Address	MAC Address	Received Packets	Receive Error	Transmitted Packets	Transmit Error
LAN	192.168.2.1	C8:3A:35:F8:CD:00	3251	0	1536	0
Bridge	192.168.2.1	C8:3A:35:F8:CD:00	3251	0	1536	0
WLAN	192.168.0.177	C8:3A:35:F8:CD:01	4	0	145	0

Parameters description

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

Name	Description
Received Packets	It displays the number of received/transmitted packets of the interface.
Transmitted Packets	
Receive Error	It displays the number of received/transmitted error packets of the interface.
Transmit Error	

5.3.5 ARP table

ARP (Address Resolution Protocol) is a network layer protocol used to convert the IP address of the destination device into a physical address. The ARP table displays the IP address and its corresponding MAC address the device visits.

To access the page, choose **Status**, then click **ARP Table** in **Statistics** part.

Statistics				
Throughput	Upstream AP	Interface	ARP Table	Routing Table
IP Address	MAC Address	Interface		
192.168.2.50	44:37:E6:4F:37:3B	Bridge		
192.168.0.1	50:2B:73:F8:F9:80	WLAN		

Parameters description

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

5.3.6 Routing table

It specifies the destination networks that the CPE can access.

To access the page, choose **Status**, then click **Routing Table** in **Statistics** part.

Statistics				
Throughput	Upstream AP	Interface	ARP Table	Routing Table
Destination Network	Subnet Mask	Next Hop	Interface	
0.0.0.0	0.0.0.0	192.168.0.1	WLAN	
192.168.0.0	255.255.255.0	0.0.0.0	WLAN	
192.168.2.0	255.255.255.0	0.0.0.0	Bridge	
239.255.255.250	255.255.255.255	0.0.0.0	Bridge	

Parameters description

Name	Description
Destination Network	It specifies the IP address of the destination network.
Subnet Mask	It specifies the subnet mask of the destination network.
Next Hop	It specifies the IP address of entrance of the next hop route when the packets egress from the interface of the device.
Interface	It specifies the interface that the packets egress.

6 Network

6.1 LAN setup

6.1.1 Overview

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

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

In **AP, Client, Universal Repeater, Repeater, and P2MP** modes, the page is displayed as below.

LAN Setup ?

MAC Address C8:3A:35:15:87:50

IP Address Type

IP Address

Subnet Mask

Default Gateway


Primary DNS Server

Secondary DNS Server

Device Name

Parameters description

Name	Description
MAC Address	It specifies the MAC address of LAN port.
IP Address Type	<p>It specifies the type of obtaining an IP address. The default is Static IP Address.</p> <ul style="list-style-type: none"> • Static IP Address: Specify the IP address, subnet mask, default gateway, and DNS server IP addresses manually. • DHCP (Dynamic IP Address): The device obtains an IP address, subnet mask, default gateway and DNS server IP address from the DHCP server in the network.

Name	Description
	 TIP If the IP Address Type is set to DHCP (Dynamic IP Address) , you need to check the device's IP address on the clients list of the DHCP server in the network, and use this IP address to log in to the web UI of the device.
IP Address	It specifies the IP address of the device. A LAN user can visit this address to enter the web UI of the device. The default is 192.168.2.1 . To access the internet, change this IP address to the same network segment of the LAN IP address of the egress router.
Subnet Mask	It specifies the subnet mask of the device. The default is 255.255.255.0 .
Default Gateway	It specifies the default gateway of the device. You can set it to the LAN IP address of the egress router to enable the device to access the internet.
Primary DNS Server	It specifies the primary DNS server IP address of the device. If the egress router has the DNS agency function, it can be set to the LAN IP address of the egress router. Otherwise, specify a DNS server IP address manually. If there is only one DNS server IP address, enter it in this box.
Secondary DNS Server	It specifies the secondary DNS server IP address of the device. If there are two DNS server IP addresses, enter one in this box.
Device Name	It specifies the name of the device. The default name indicates the product model and version. You are recommended to change the name to indicate the location of the device, so that you can easily identify the device when there are multiple devices in the network.

When the CPE is in **WISP** and **Router** modes, the page is displayed as below.

LAN Setup ?


MAC Address C8:3A:35:15:87:50

IP Address Type

IP Address

Subnet Mask

Parameters description

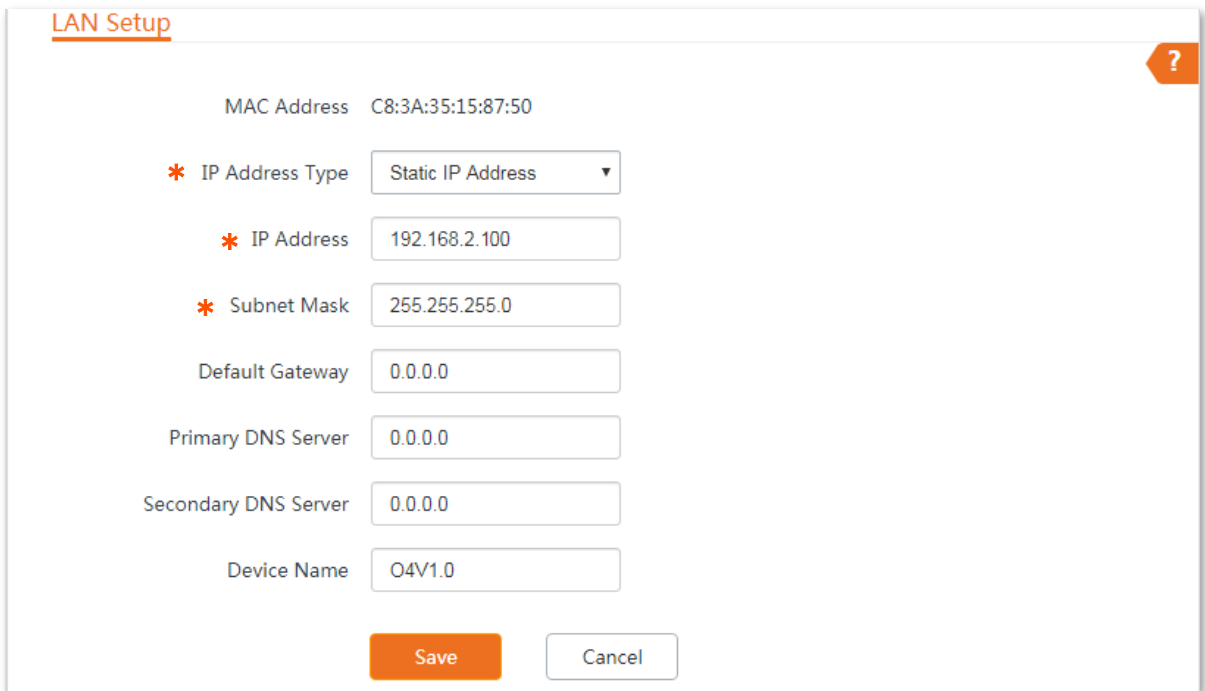
Name	Description
MAC Address	It specifies the MAC address of LAN port.
IP Address Type	<p>It specifies the type of obtaining an IP address. The default is Static IP Address.</p> <ul style="list-style-type: none"> • Static IP Address: Specify the IP address and subnet mask manually. • DHCP (Dynamic IP Address): The device obtains an IP address and subnet mask from the upstream DHCP server in the network. <p> TIP</p> <p>If the IP Address Type is set to DHCP (Dynamic IP Address), you need to check the device's IP address on the clients list of the DHCP server of the upstream device, and use this IP address to log in to the web UI of the device.</p>
IP Address	It specifies the LAN IP address of the device. A LAN user can visit this address to enter the web UI of the device. The default is 192.168.2.1 .
Subnet Mask	It specifies the subnet mask corresponding to the LAN IP address of the device. The default is 255.255.255.0 .

6.1.2 Set the LAN IP address manually

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

Configuration procedures

- Step 1** Choose **Network > LAN Setup** to enter the configuration page.
- Step 2** Set **IP Address Type** to **Static IP Address**.
- Step 3** Set **IP Address, Subnet Mask**. If you want to connect the CPE to the internet, you need to configure **Default Gateway, DNS Server**.
- Step 4** Click **Save**.



LAN Setup

MAC Address C8:3A:35:15:87:50

* IP Address Type Static IP Address

* IP Address 192.168.2.100

* Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

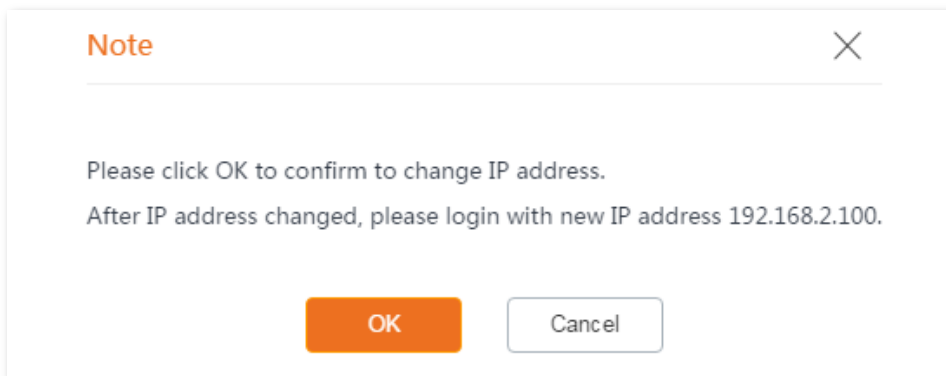
Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

Device Name O4V1.0

Save Cancel

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



Note

Please click OK to confirm to change IP address.
After IP address changed, please login with new IP address 192.168.2.100.

OK Cancel

----End

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

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

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

6.1.3 Set the device to obtain a LAN IP address automatically

DHCP (Dynamic IP Address) enables the device to automatically obtain an IP address, a subnet mask, a gateway IP address, DNS server IP addresses assigned by the DHCP server of the upstream device. If a large number of devices are deployed, you can adopt this mode to prevent IP address

conflicts and effectively reduce your workload.

Configuration procedures:

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

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

Step 3 Click **Save**.

LAN Setup

MAC Address C8:3A:35:15:87:50

* IP Address Type DHCP (Dynamic IP Add ▾)

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

Device Name O4V1.0

Save Cancel

----End

After completing the configuration, if you want to re-log in to the web UI of the CPE, check the new IP address on the web UI of the upstream device which assigns the IP address to this device. Ensure that the IP address of the management computer and the IP address of the CPE belong to the same network segment, and access the IP address of the CPE.

Refer to steps in the [How to assign a fixed IP address to your computer](#) part to assign an IP address to the computer manually.

6.2 MAC clone

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

6.2.1 Overview

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

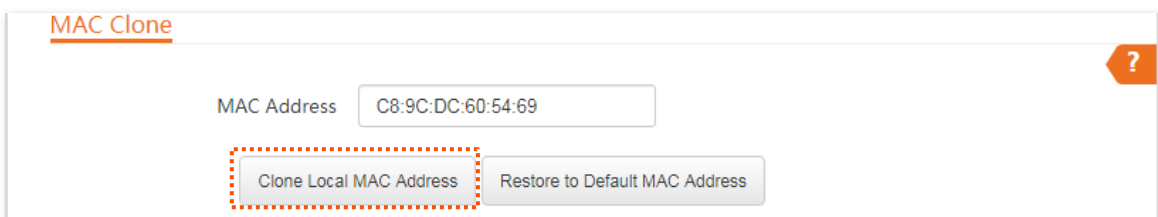
In this case, you need to clone the MAC address of this computer to the WAN port of the CPE for internet access.

6.2.2 Clone a MAC address

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

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

- Step 1** Connect the computer to the CPE.
- Step 2** Start a web browser on the computer and log in to the web UI of the CPE. Choose **Network > MAC Clone** to enter the configuration page.
- Step 3** Click **Clone Local MAC Address**.
- Step 4** Click **Save**.



----End

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

If you do NOT use the computer that can access the internet after it connects to the modem directly to configure the CPE, but you know the MAC address of this computer, perform the following steps:

- Step 1** Start a web browser on the computer and log in to the web UI of the CPE. Choose **Network > MAC Clone** to enter the configuration page.
- Step 2** Enter the MAC address of the computer in the **MAC Address** box.
- Step 3** Click **Save**.

MAC Clone ?

MAC Address

----End



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

6.3 DHCP server

6.3.1 Overview

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



If you change the LAN IP address of the CPE and the new and original IP addresses belong to different network segments, the system automatically changes the IP address pool of the DHCP server to make the IP address pool and the new IP address of the LAN port belong to the same network segment.

6.3.2 Configure the DHCP server

- Step 1** Choose **Network > DHCP Server** to enter the configuration page.
- Step 2** Enable the **DHCP server**.
- Step 3** Set the parameters. Generally, you need to set only **Gateway Address** and **Primary DNS Server**.
- Step 4** Click **Save**.

DHCP Server ?

* DHCP Server

Start IP Address

End IP Address

Subnet Mask

* Gateway Address

* Primary DNS Server

Secondary DNS Server




Lease Time

----End



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

Parameters description

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

6.4 DHCP client

With the DHCP server enabled, 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.

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

DHCP Client ?

ID	Host Name	IP Address	MAC Address	Lease Time
1	iPhone	192.168.2.133	1C:5C:F2:B4:40:08	23h 59m 44s

10 ▾ Datas/Page 1 data in total

6.5 VLAN settings

6.5.1 Overview

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

After the IEEE 802.1q VLAN settings take effect, packet with tag will be forwarded to the ports of the corresponding VLAN according to the VID of the packet, and packet without tag will be forwarded to the ports of the corresponding VLAN according to the PVID of the port.

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

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

To access the page, choose **Network > VLAN Settings**.

VLAN Settings ?

VLAN Settings

PVID (Range: 1 to 4094)

Management VLAN (Range: 1 to 4094)

WLAN VLAN ID (Range: 1 to 4094)

Parameters description

Name	Description
VLAN Settings	It is used to enable or disable the 802.1Q VLAN function of this CPE. By default, it is disabled. After the VLAN function is enabled, the PoE/LAN port is used as a trunk port.
PVID	It specifies the default native VLAN ID of the trunk port. The default is 1 . After the VLAN function is enabled, the PoE/LAN port is used as a trunk port.
Management VLAN	It specifies the ID of the management VLAN of this CPE. The default ID is 1 . After changing the management VLAN, you can manage this CPE only after connecting your computer to the new management VLAN.

Name	Description
WLAN VLAN ID	It allows you to set a VLAN ID for the wireless network of this device. By default, it is set to 1000 .
	After the VLAN function is enabled, the WLAN interface functions as an access port, whose PVID is the same as VLAN ID.

6.5.2 Example of configuring VLAN

Networking requirement

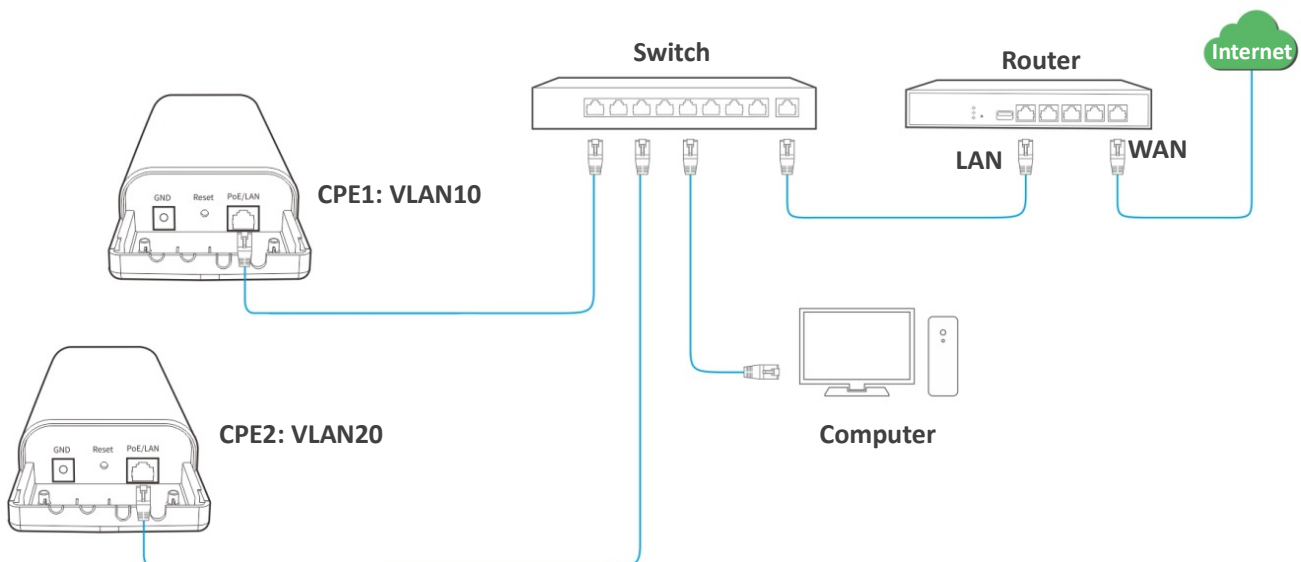
You use CPEs to set up CCTV surveillance networks. CPE1 and CPE2 are used to connect to IP cameras in different places and cannot communicate with each other.

You can assign CPE1 and CPE2 to different VLANs.

Assume that:

- CPE1 is assigned to VLAN10, and CPE2 is assigned to VLAN20.
- The router in the network supports IEEE 802.1q VLAN and enables two DHCP servers which belong to VLAN10 and VLAN20 respectively.

Network topology



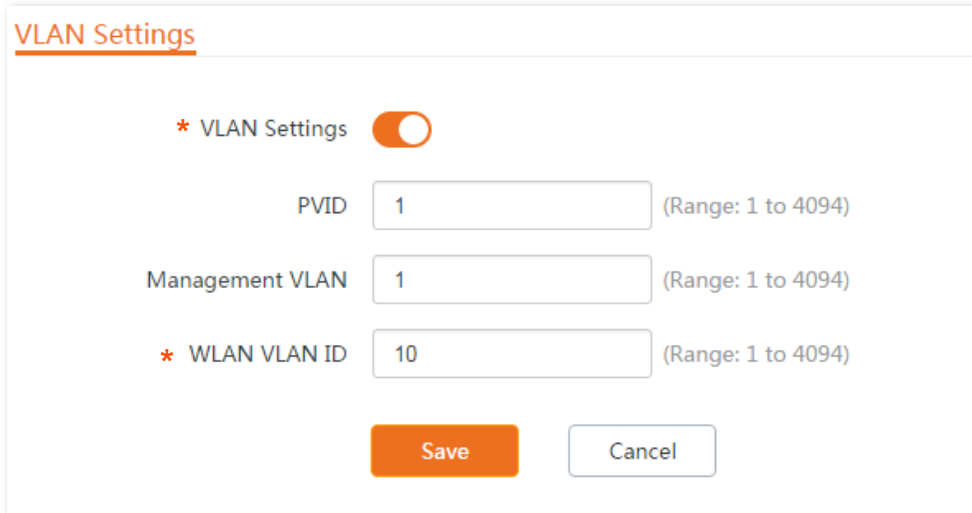
The connections of the switch:

- The router is connected to the uplink port
- CPE1 is connected to port 1
- CPE2 is connected to port 2

Configuration procedures

Step 1 Set up CPE1.

1. Log in to the web UI of CPE1, and choose **Network > VLAN Settings**.
2. Enable the function.
3. Configure **WLAN VLAN ID**, which is **10** in this example.
4. Click **Save**.



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

Step 2 Set the **WLAN VLAN ID** of CPE2 to **20** according to the steps in [Step 1](#).

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

Ports of the Switch	VLAN ID (Allow the packets belonging to the following VLANs to access)	Type of Port	PVID
Uplink port (Connected to a router)	1, 10, 20	Trunk	1
Port 1 (Connected to CPE1)	1, 10	Trunk	1
Port 2 (Connected to CPE2)	1, 20	Trunk	1

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

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

Refer to the user guide of the router for details.

----End

Verification

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

7 Wireless

7.1 Basic

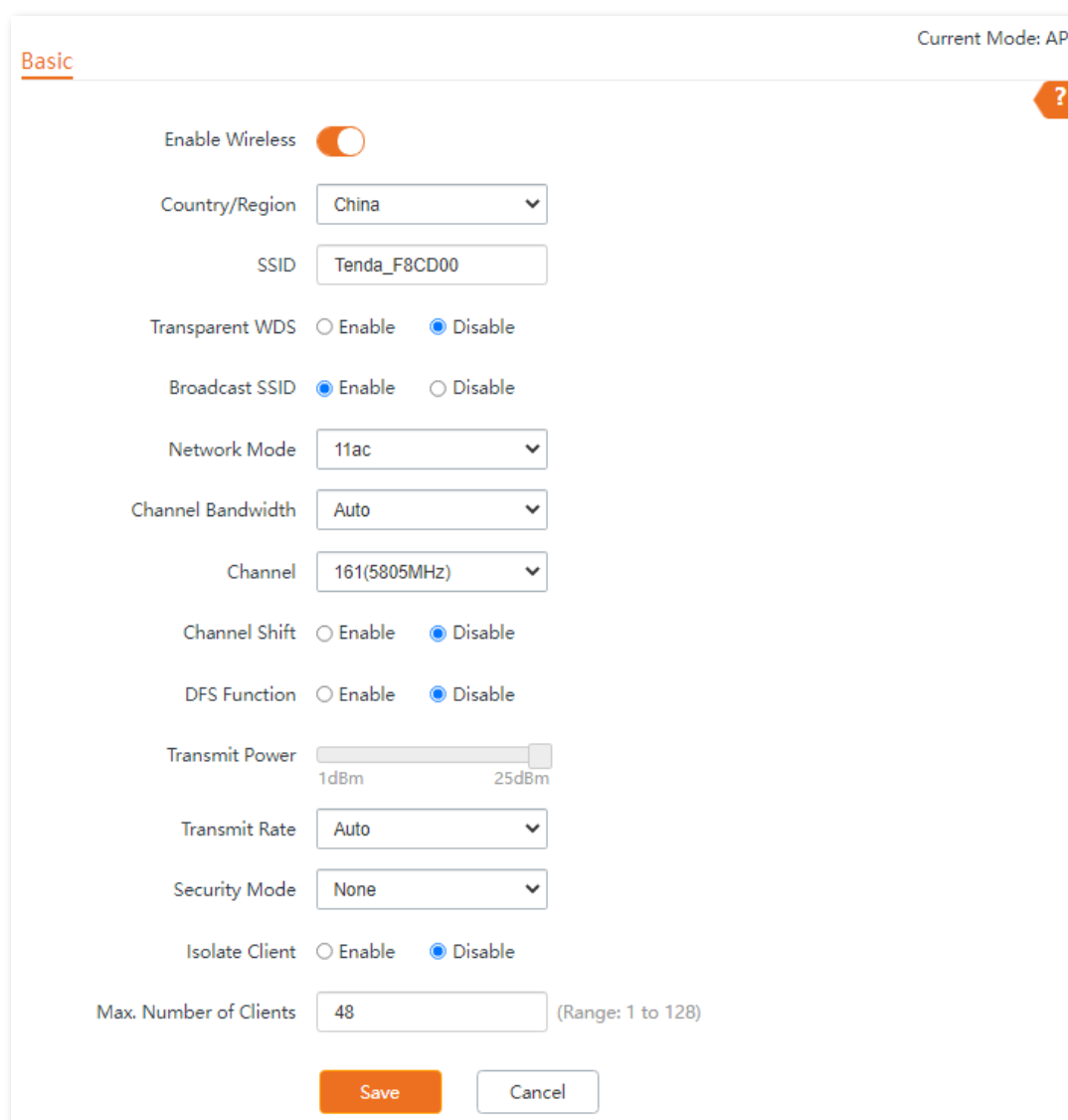
7.1.1 Overview

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

To access the page, choose **Wireless > Basic**.

In AP, WISP, Repeater, P2MP and Router modes

The page is displayed as below. O8V1.0 is used as an example for illustration here.




The screenshot shows the 'Basic' configuration page for wireless settings. The current mode is 'AP'. The page includes the following settings:

- Enable Wireless:** Toggled on.
- Country/Region:** China (dropdown menu).
- SSID:** Tenda_F8CD00 (text input).
- Transparent WDS:** Disabled (radio button).
- Broadcast SSID:** Enabled (radio button).
- Network Mode:** 11ac (dropdown menu).
- Channel Bandwidth:** Auto (dropdown menu).
- Channel:** 161(5805MHz) (dropdown menu).
- Channel Shift:** Disabled (radio button).
- DFS Function:** Disabled (radio button).
- Transmit Power:** Slider set to 25dBm (range 1dBm to 25dBm).
- Transmit Rate:** Auto (dropdown menu).
- Security Mode:** None (dropdown menu).
- Isolate Client:** Disabled (radio button).
- Max. Number of Clients:** 48 (text input, range 1 to 128).

Buttons for 'Save' and 'Cancel' are located at the bottom of the page.

Parameters description

Name	Description
Enable Wireless	It specifies whether to enable the wireless function. By default, it is enabled.
Country/Region	It specifies the country or region where this CPE is located. You can select the country or region to ensure that this CPE complies with the channel regulations of the country or region.
SSID	It specifies the wireless network name. You can modify it by yourself.
Transparent WDS	It is available when the CPE works in AP mode or Client mode. 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.  TIP Transparent WDS and Transparent Bridge cannot be enabled at the same time.
Broadcast SSID	It specifies whether to broadcast the SSID. When the device broadcasts an SSID, wireless clients can detect the SSID. When this function is set to Disable , the device does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This to some extent enhances the security of the wireless network.
Network Mode	It specifies the wireless network mode of the CPE. Only wireless clients supporting the listed network mode can connect to the CPE.
Channel Bandwidth	It specifies the bandwidth of the operating channel of a wireless network. The channel bandwidth varies with different network modes. Please select it based on your actual operating environment. Auto indicates that the CPE can switch its channel bandwidth based on the ambient environment.
Channel	It specifies the channel in which the CPE operates. Auto indicates that the CPE automatically changes to a channel rarely used in the ambient environment to prevent interference.
Channel Shift	It specifies the shift of the channel center frequency. With this function enabled, the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the CPE can exchange data on less interference channels.
DFS Function	Dynamic Frequency Selection. With this function enabled, the CPE automatically detects the frequency of the radar system. When the CPE detects radar signals in the same frequency with the CPE itself, the CPE will automatically switch to another frequency to avoid interference with the radar system.
Transmit Power	It specifies the transmit power of the CPE.

Name	Description
	Higher number indicates wider WiFi coverage. Setting a proper transmit power helps improve the performance and security of the wireless network.
Transmit Rate	It specifies wireless transmission rate of the CPE. Auto is recommended. The maximum negotiation rate varies with different channel bandwidths and network modes. Refer to the web UI of the CPE for details. When Auto is selected, the CPE will be adjusted to the maximum transmit rate under the corresponding network mode.
Security Mode	The CPE supports various security modes for network encryption, including None , WEP , WPA-PSK , WPA2-PSK , Mixed WPA/WPA2-PSK , WPA , and WPA2 .
Isolate Client	<ul style="list-style-type: none"> • Enable: Clients connected to this wireless network cannot communicate with each other, which improves the wireless network security. • Disable: Clients connected to this wireless network can communicate with each other. The default is Disable.
Max. Number of Clients	It specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID. If the number is reached, the wireless network rejects new connection requests from clients. This limit helps balance load among devices.

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.

The CPE supports various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2.

■ None

The CPE does not encrypt its wireless network. This option is not recommended because it affects network security.

■ WEP

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

When the security mode is set to **WEP**, the page is shown as follows.

Security Mode	WEP ▼	
Authentication Type	Open ▼	
Default Key	Key 1 ▼	
Key 1	12345	ASCII ▼
Key 2	12345	ASCII ▼
Key 3	12345	ASCII ▼
Key 4	12345	ASCII ▼

Parameters description

Name	Description
Authentication Type	<p>It specifies the authentication type for the WEP security mode. The options include Open and Shared. The options share the same encryption process.</p> <ul style="list-style-type: none"> • Open: It specifies that authentication is not required and data exchange is encrypted using WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. • Shared: It specifies that a shared key is used for authentication and data exchanged is encrypted using WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key.
Default Key	<p>It specifies the WEP key for the Open or Shared encryption type.</p> <p>For example, if Default Key is set to Security Key 2, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Security Key 2.</p>
Key 1/2/3/4	<p>Enter WEP key. You can enter four keys, but only the key specified in the Default Key takes effect.</p>
ASCII	<p>It indicates that a key selected for the Open or Shared authentication type contains ASCII characters.</p> <p>5 or 13 ASCII characters are allowed in the key.</p>
Hex	<p>It indicates that a key selected for the Open or Shared authentication type contains hexadecimal characters.</p> <p>10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.</p>

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

They belong to pre-shared key or personal key modes, where Mixed WPA/WPA2-PSK supports both WPA-PSK and WPA2-PSK.

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK adopt a pre-shared key for authentication, while

the CPE generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks.

Nevertheless, because the initial pre-shared key for authentication is manually set and all clients use the same key to connect to the same CPE, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.

To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate clients and generate data encryption-oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.

When the security mode is set to WPA-PSK, WPA2-PSK, or Mixed WPA/WPA2-PSK, the page is shown as follows.

The screenshot shows a configuration interface with a dropdown menu for 'Security Mode'. The dropdown is open, displaying the following options: 'None', 'WEP', 'WPA-PSK' (which is highlighted in blue), 'WPA2-PSK', 'Mixed WPA/WPA2-PSK', 'WPA', and 'WPA2'. To the right of the dropdown, the text 'IP&AES' is visible. Below the dropdown, there are fields for 'Encryption Algorithm', 'Key', and 'Key Update Interval'. The 'Key Update Interval' field has a value of '0' and a note: 's (Range: 60 to 99999, 0 indicates that no key'.

Parameters description

Name	Description
Security Mode	<p>It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK.</p> <ul style="list-style-type: none"> • WPA-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA-PSK. • WPA2-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2-PSK. • Mixed WPA/WPA2-PSK: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK.
Encryption Algorithm	<p>It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK, this parameter has the AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter has the AES, TKIP, and TKIP&AES values.</p> <ul style="list-style-type: none"> • AES: It indicates the Advanced Encryption Standard. • TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. • TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.

Name	Description
Key	It specifies a pre-shared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value 0 indicates that a WAP key is not updated.

■ WPA and WPA2

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.

When the security mode is set to WPA or WPA2, the page is shown as follows.

Parameters description

Name	Description
Security Mode	The WPA and WPA2 options are available for network protection with a RADIUS server. <ul style="list-style-type: none"> • WPA: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA. • WPA2: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2.
RADIUS Server	It specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	It specifies the port number of the RADIUS server for client authentication.
RADIUS Password	It specifies the shared password of the RADIUS server.

Name	Description
Encryption Algorithm	<p data-bbox="459 230 1401 297">It specifies the encryption algorithm corresponding to the selected security mode. The available options include AES, TKIP, and TKIP&AES.</p> <ul data-bbox="459 320 1420 533" style="list-style-type: none"><li data-bbox="459 320 1077 353">• AES: It indicates the Advanced Encryption Standard.<li data-bbox="459 376 1098 409">• TKIP: It indicates the Temporal Key Integrity Protocol.<li data-bbox="459 432 1420 533">• TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key Update Interval	<p data-bbox="459 566 1348 633">It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p data-bbox="459 656 1061 689">The value 0 indicates that a WAP key is not updated.</p>

In Client and Universal Repeater modes

In Client and Universal Repeater modes, the configurations in **Basic** page are similar. Take **Client** mode and O8V1.0 as an example here.

Basic
Current Mode: Station

?

Enable Wireless

Country/Region China ▼

Broadcast SSID Enable Disable

Network Mode 11ac ▼

Channel Bandwidth Auto ▼

Channel 161(5805MHz) ▼

Channel Shift Enable Disable

DFS Function Enable Disable

Transmit Power 1dBm 25dBm

Transmit Rate Auto ▼

Primary Upstream SSID NOVA_9JK3_AAAAA Site Survey

Primary AP BSSID 50:2B:73:F8:F9:8A Lock

Transparent WDS Enable Disable

Security Mode WPA2-PSK ▼

Encryption Algorithm AES TKIP TKIP&AES

Key *****

Key Update Interval 0 s (Range: 60 to 99999)

Secondary Upstream SSID Enable Disable

Secondary Upstream SSID Tenda Site Survey

Secondary Upstream BSSID 00:90:4C:88:88:88 Lock

Transparent WDS Enable Disable

Security Mode None ▼

Reconnect Primary Upstream SSID Enable Disable

Reconnection Interval 90 (Range: 1~720minutes)

Isolate Client Enable Disable

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

Save
Cancel

Parameters on the **Basic** page vary with different modes. Please refer to the actual web UI. Followings are descriptions of some main parameters. For other parameters, please refer to [Parameter description](#) of AP mode.

Parameters description

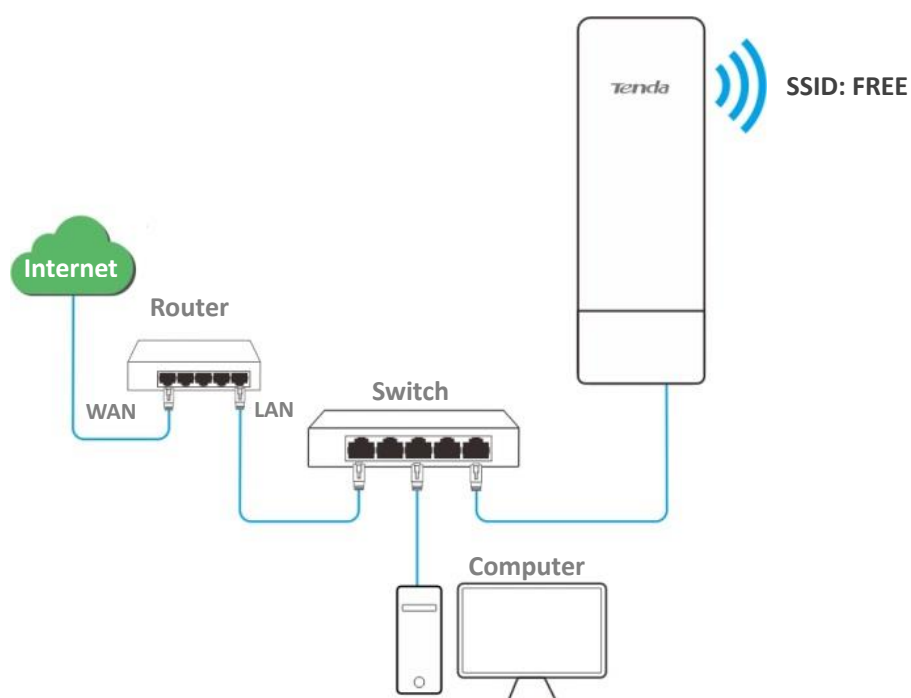
Name	Description
Primary Upstream SSID	It specifies the SSID of the primary upstream wireless network that the CPE connects to. After bridging succeeds, the SSID of the primary upstream wireless network will automatically populate.
Primary AP BSSID	It specifies the MAC address of the primary upstream wireless network. After bridging succeeds, the MAC address of the primary upstream wireless network will automatically populate.
Lock	It is used to lock the upstream wireless network. 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 wireless network name.
Secondary Upstream SSID	It specifies the SSID of the secondary upstream wireless network that the CPE connects to. 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	It specifies the wireless MAC address of the secondary upstream wireless network.
Reconnect Primary Upstream SSID	It is used to reconnect to the primary upstream wireless network. 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	It 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	It is used to refresh the available wireless networks and select the one for connection.

7.1.2 Set up a non-encrypted wireless network

Networking requirement

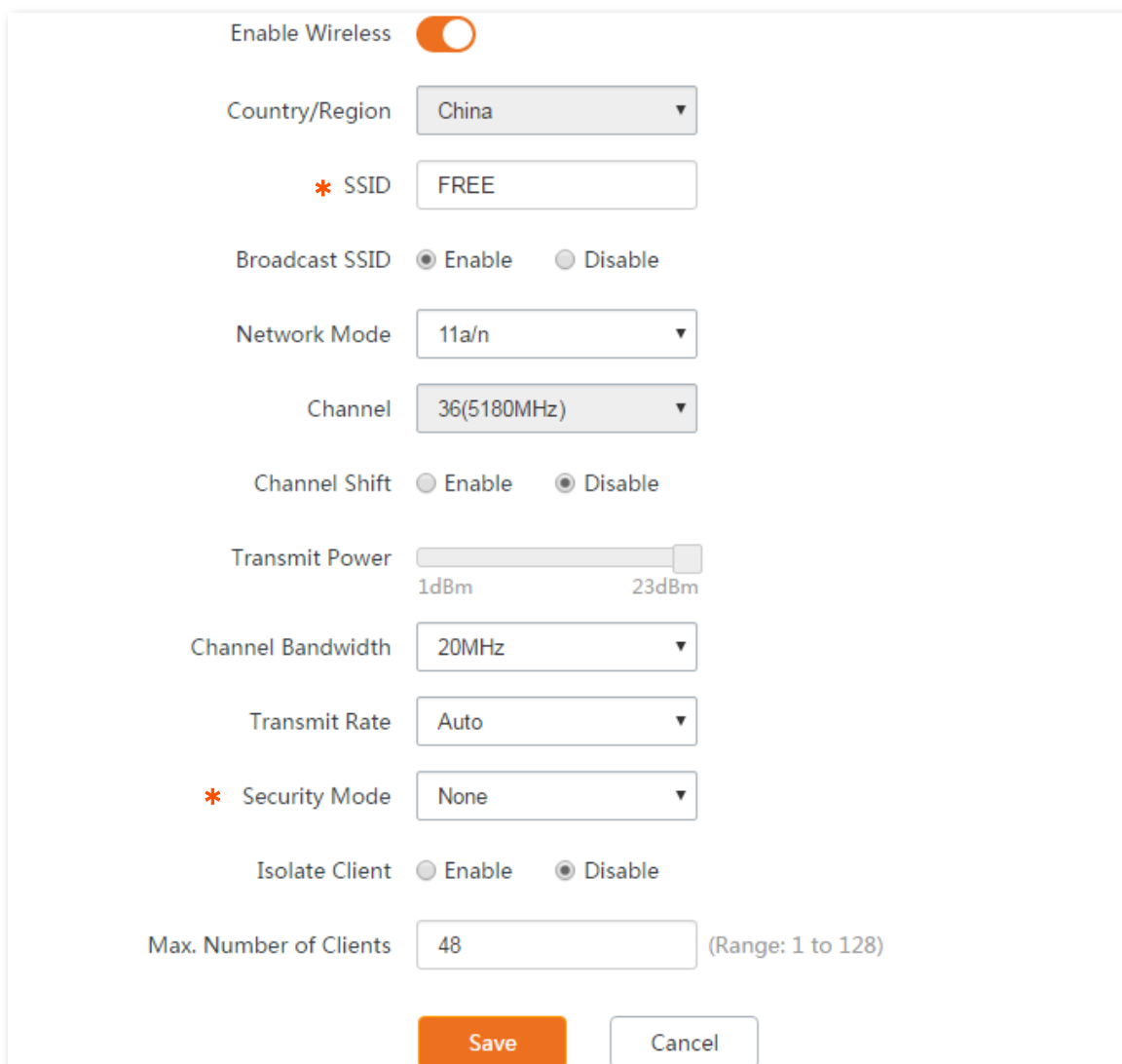
An estate uses the CPE to deploy its network for video surveillance. It requires that the SSID is FREE and there is no WiFi password.

Network topology



Configuration procedures

- Step 1** Choose **Wireless > Basic** to enter the configuration page.
- Step 2** Set **SSID** to **FREE**.
- Step 3** Set **Security Mode** to **None**.
- Step 4** Click **Save**.



The image shows a wireless network configuration interface. At the top, there is a toggle switch for 'Enable Wireless' which is turned on. Below this, there are several configuration options: 'Country/Region' is set to 'China'; '* SSID' is set to 'FREE'; 'Broadcast SSID' has 'Enable' selected; 'Network Mode' is set to '11a/n'; 'Channel' is set to '36(5180MHz)'; 'Channel Shift' has 'Disable' selected; 'Transmit Power' is shown as a slider between 1dBm and 23dBm; 'Channel Bandwidth' is set to '20MHz'; 'Transmit Rate' is set to 'Auto'; '* Security Mode' is set to 'None'; 'Isolate Client' has 'Disable' selected; and 'Max. Number of Clients' is set to '48' with a range of 1 to 128. At the bottom, there are 'Save' and 'Cancel' buttons.

Enable Wireless

Country/Region

* SSID

Broadcast SSID Enable Disable

Network Mode

Channel

Channel Shift Enable Disable

Transmit Power 1dBm 23dBm

Channel Bandwidth

Transmit Rate

* Security Mode

Isolate Client Enable Disable

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

----End

Verification

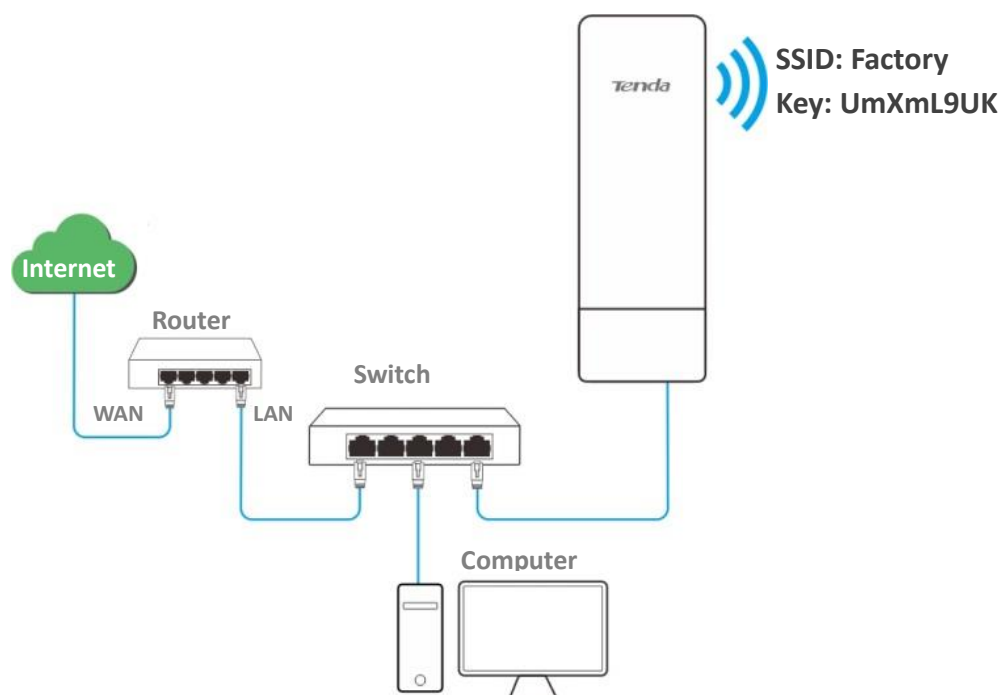
Wireless devices can connect to the wireless network whose SSID is FREE without a password.

7.1.3 Set up a wireless network encrypted using WPA2-PSK

Networking requirement

A 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. See the following figure.

Network topology



Configuration procedures

- Step 1** Choose **Wireless > Basic** to enter the configuration page.
- Step 2** Set **SSID** to **Factory**.
- Step 3** Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.
- Step 4** Set **Key** to **UmXmL9UK**.
- Step 5** Click **Save**.

Basic ?

Enable Wireless

Country/Region

* SSID

Broadcast SSID Enable Disable

Network Mode

Channel

Channel Shift Enable Disable

Transmit Power 1dBm 23dBm

Channel Bandwidth

Transmit Rate

* Security Mode

* Encryption Algorithm AES TKIP TKIP&AES

* Key

Key Update Interval s (Range: 60 to 99999)

Isolate Client Enable Disable

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

----End

Verification

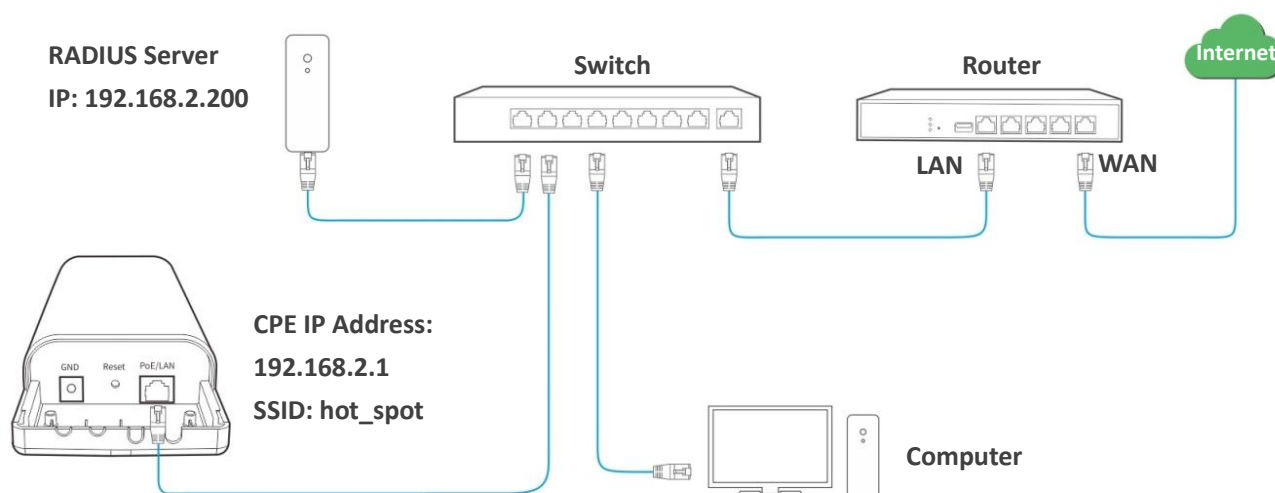
Wireless devices can connect to the wireless network named **Factory** with the password **UmXmL9UK**.

7.1.4 Set up a wireless network encrypted using WPA or WPA2

Networking requirement

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

Network topology



Configuration procedures

Configure the CPE

Assume that:

- IP address of the RADIUS server: **192.168.2.200**
- RADIUS Password: **12345678**
- Authentication port: **1812**
- SSID of the CPE: **hot_spot**
- Security mode: **WPA2**
- Encryption algorithm: **AES**

Step 1 Log in to the web UI of CPE, choose **Wireless > Basic** to enter the configuration page.

Step 2 Set **SSID** to **hot_spot**.

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

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

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

Step 6 Click **Save**.

Basic ?

Enable Wireless

Country/Region China

* SSID hot_spot

Broadcast SSID Enable Disable

Network Mode 11a/n

Channel Auto

Channel Shift Enable Disable

Transmit Power
1dBm
26dBm

Channel Bandwidth 20MHz

Transmit Rate Auto

* Security Mode WPA2

* RADIUS Server 192.168.2.200

* RADIUS Port 1812

* Encryption Algorithm AES TKIP TKIP&AES

* RADIUS Password

Key Update Interval 0 s (Range: 60 to 99999)

Isolate Client Enable Disable

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

Save
Cancel

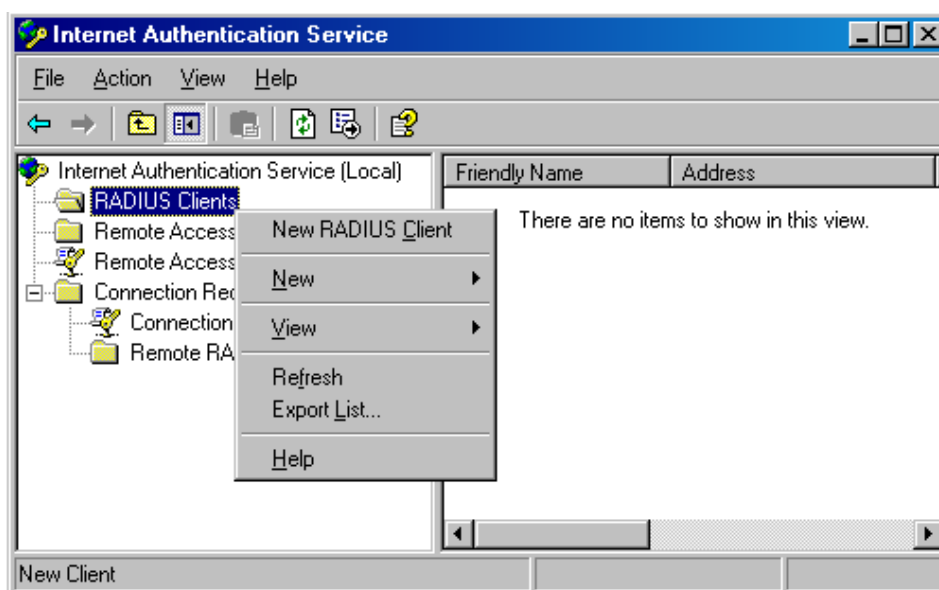
Configure the RADIUS server



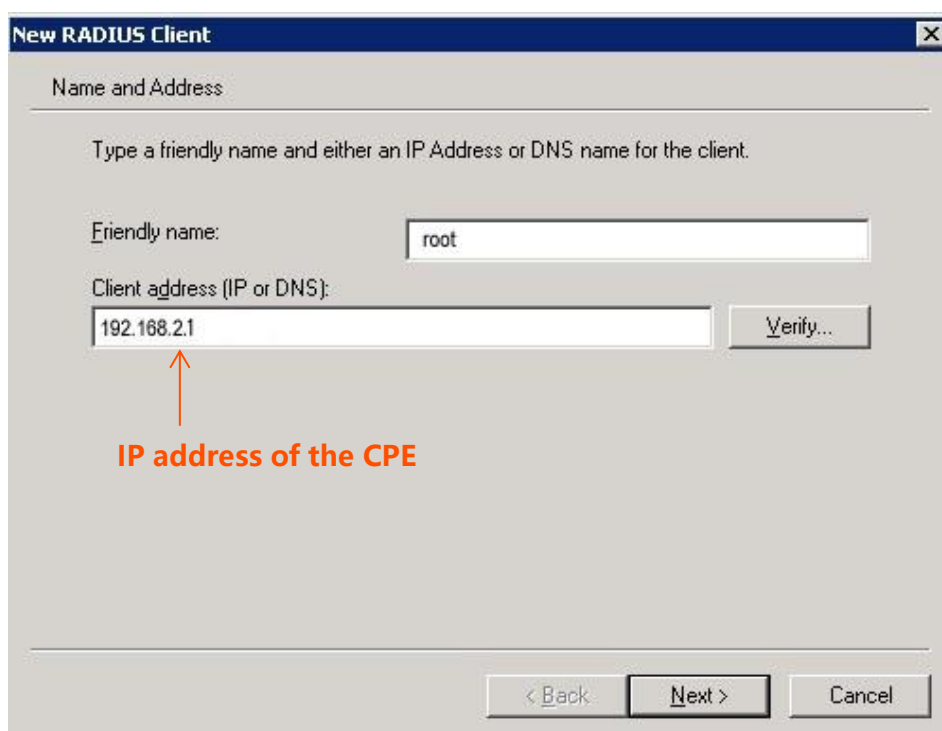
Windows 2003 is used as an example to describe how to configure the RADIUS server.

Step 1 Configure a RADIUS client.

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



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



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

New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor:
RADIUS Standard

Shared secret: [XXXXXXXXXX]

Confirm shared secret: [XXXXXXXXXX]

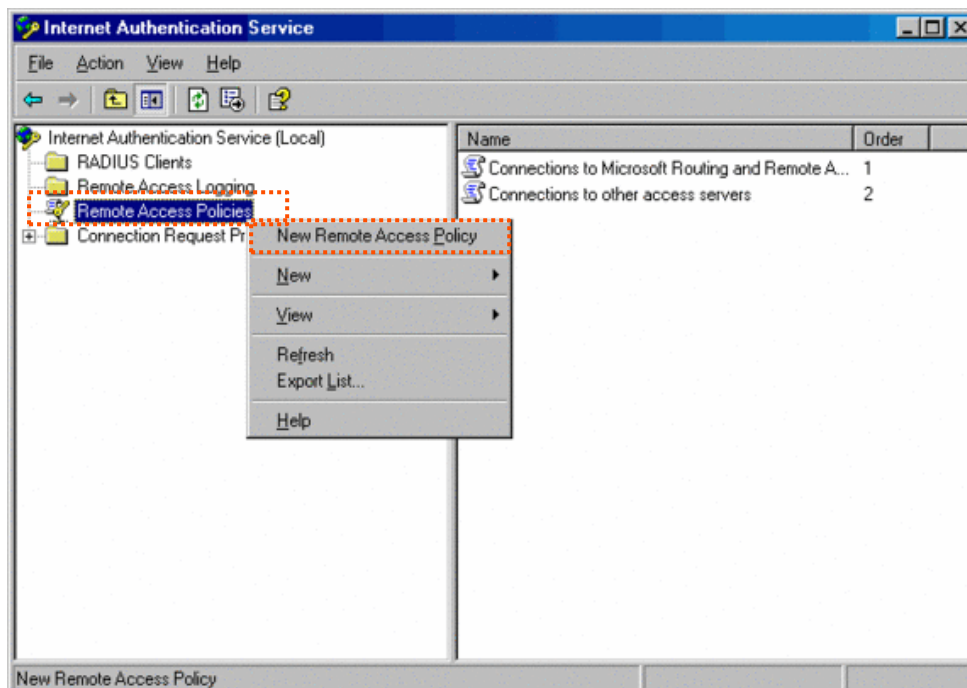
Request must contain the Message Authenticator attribute

Password same as that specified by RADIUS Password on the CPE.

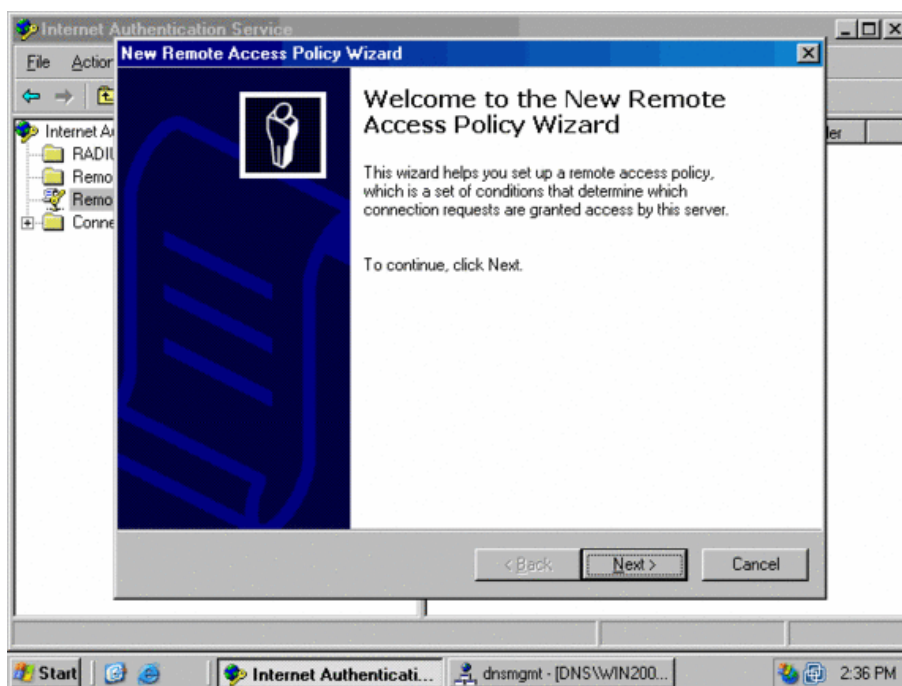
< Back Finish Cancel

Step 2 Configure a remote access policy.

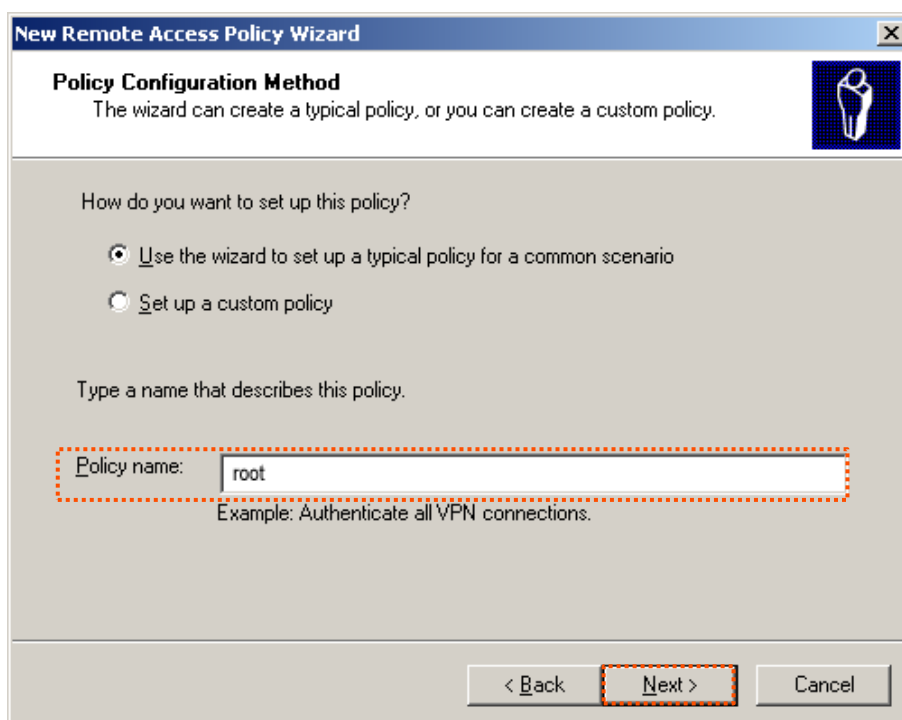
1. Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



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



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



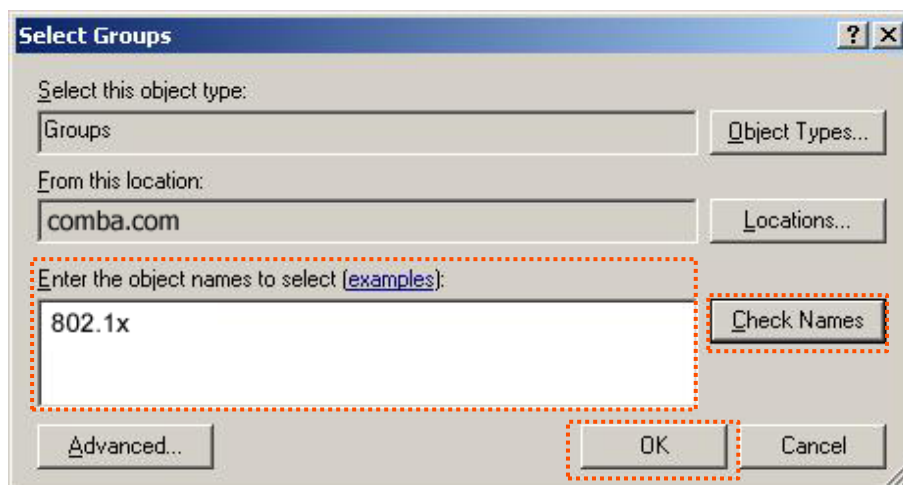
4. Select **Ethernet** and click **Next**.

The screenshot shows the 'New Remote Access Policy Wizard' dialog box. The title bar reads 'New Remote Access Policy Wizard'. The main heading is 'Access Method' with a sub-heading 'Policy conditions are based on the method used to gain access to the network.' Below this, there is a text box: 'Select the method of access for which you want to create a policy.' There are four radio button options: 'VPN' (with sub-text 'Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.'), 'Dial-up' (with sub-text 'Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.'), 'Wireless' (with sub-text 'Use for wireless LAN connections only.'), and 'Ethernet' (with sub-text 'Use for Ethernet connections, such as connections that use a switch.'). The 'Ethernet' option is selected and highlighted with a red dashed border. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

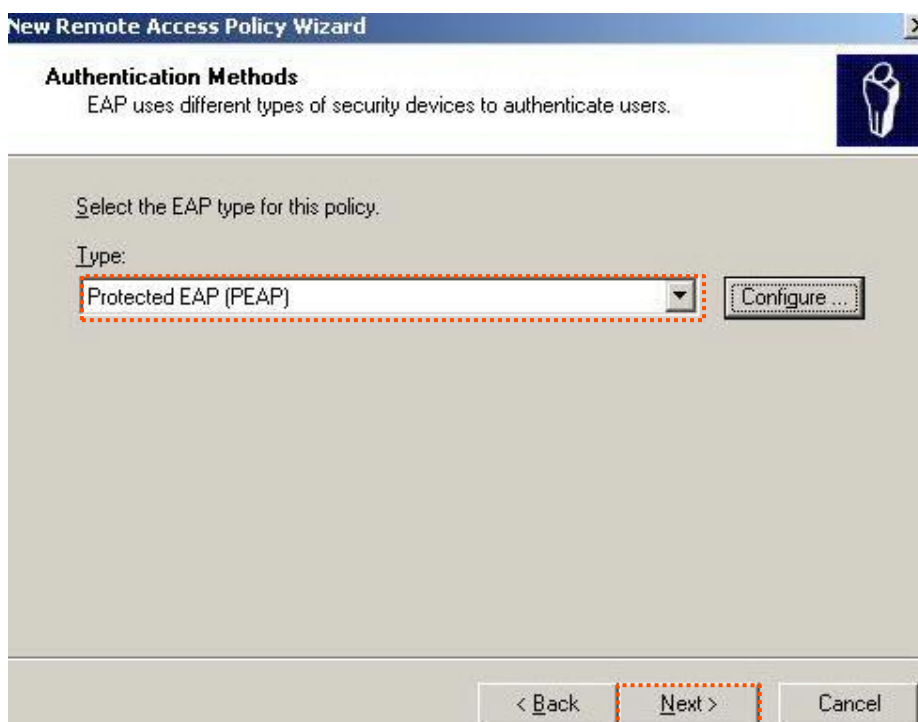
5. Select **Group** and click **Add**.

The screenshot shows the 'New Remote Access Policy Wizard' dialog box. The title bar reads 'New Remote Access Policy Wizard'. The main heading is 'User or Group Access' with a sub-heading 'You can grant access to individual users, or you can grant access to selected groups.' Below this, there is a text box: 'Grant access based on the following:'. There are two radio button options: 'User' (with sub-text 'User access permissions are specified in the user account.') and 'Group' (with sub-text 'Individual user permissions override group permissions.'). The 'Group' option is selected and highlighted with a red dashed border. Below the 'Group' option, there is a text box labeled 'Group name:' and an empty text input field. To the right of the input field are two buttons: 'Add...' and 'Remove'. The 'Add...' button is highlighted with a red dashed border. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

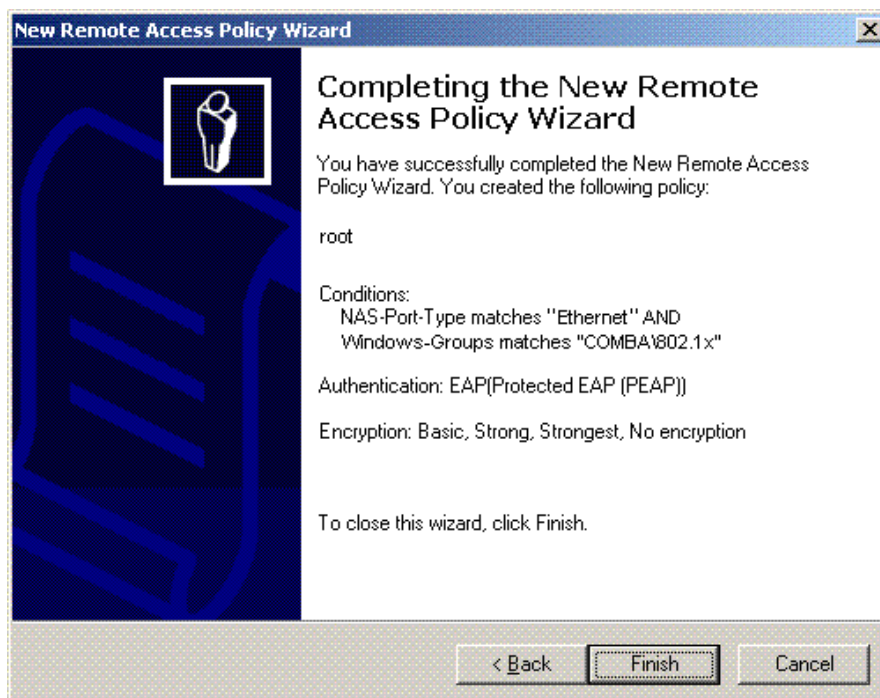
6. Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



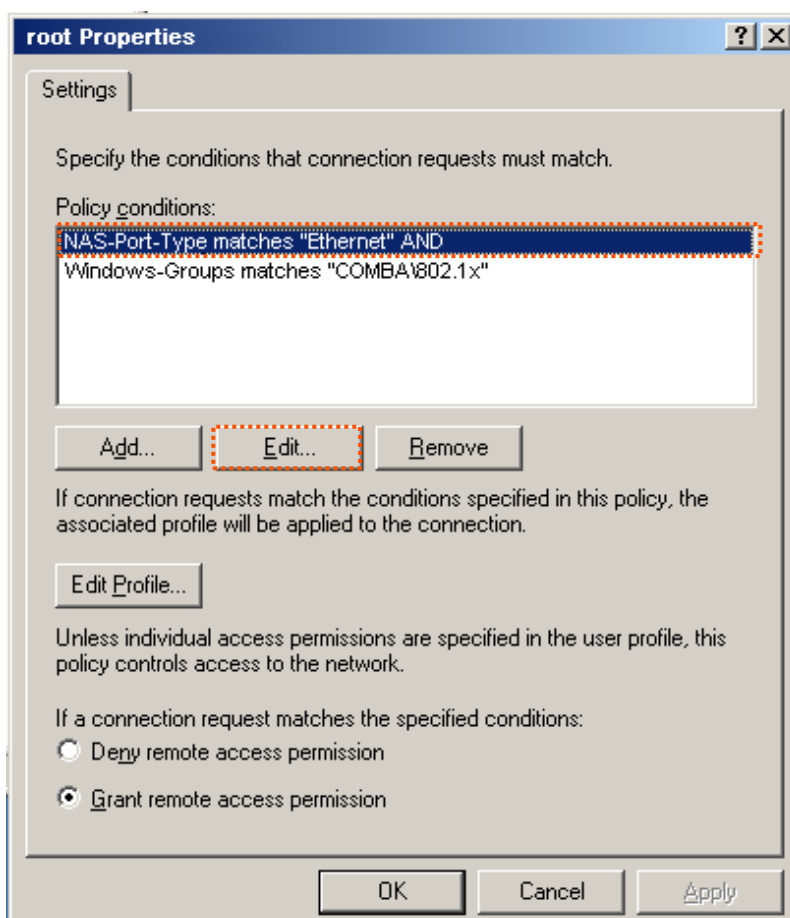
7. Select Protected EAP (PEAP) and click Next.



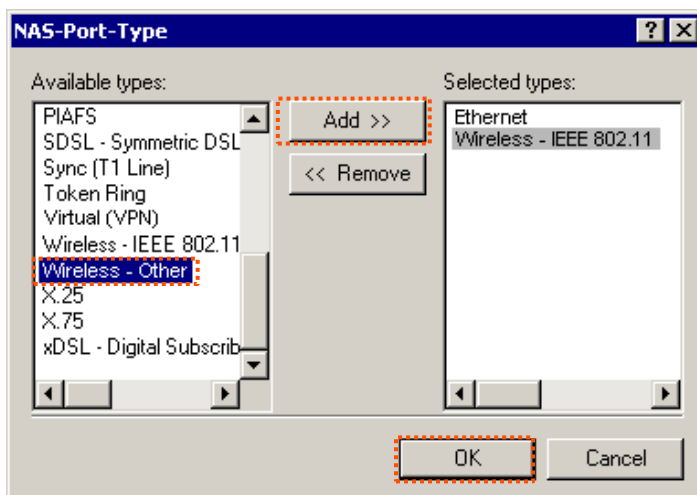
- Click **Finish**. The remote access policy is created.



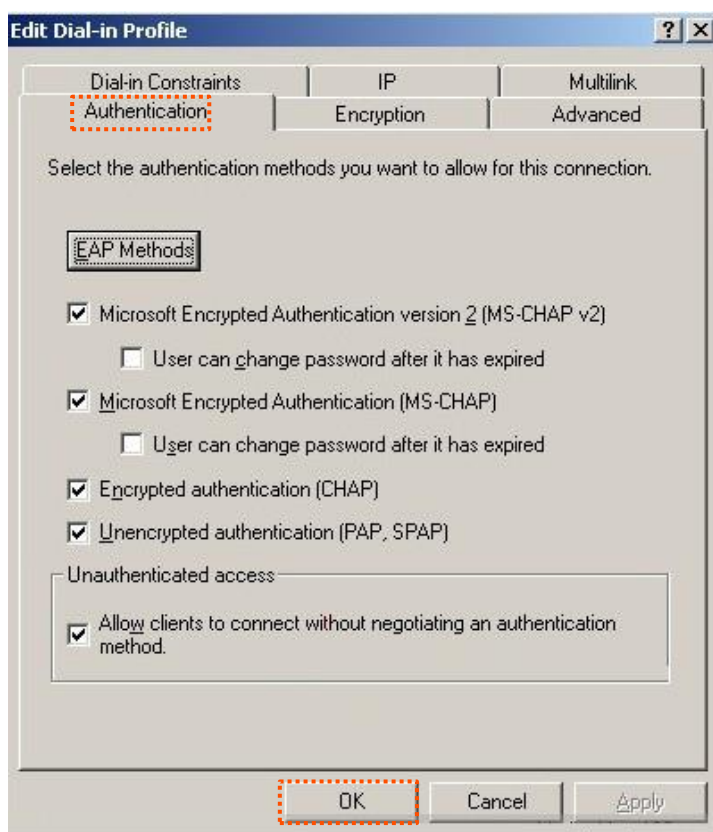
- Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



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



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



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

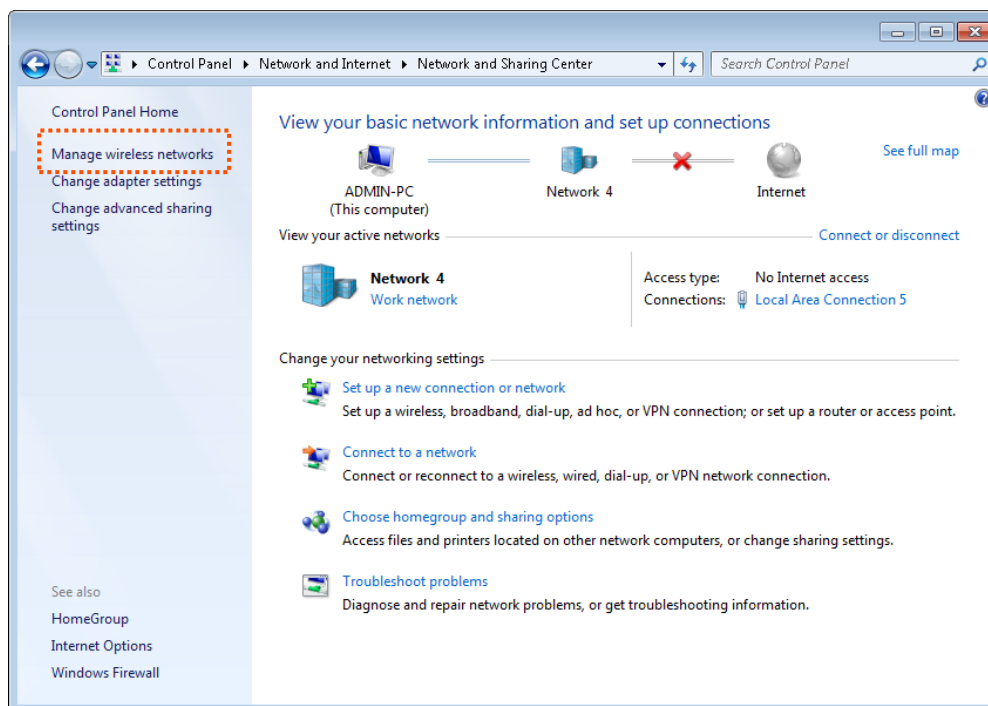
Step 3 Configure user information. Create a user and add the user to group **802.1x**.

Configure your wireless device

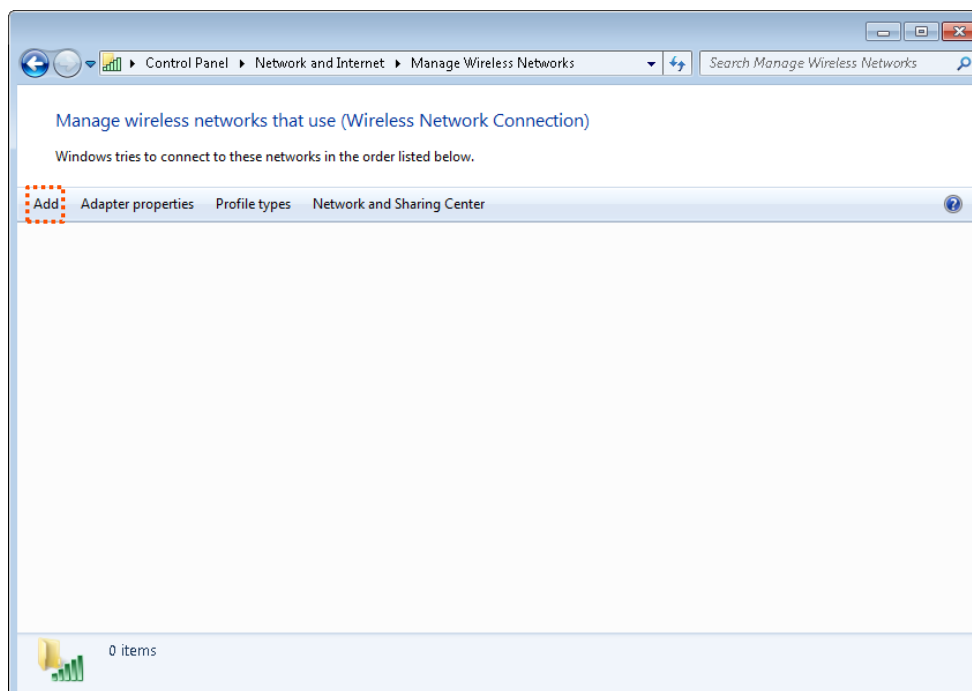


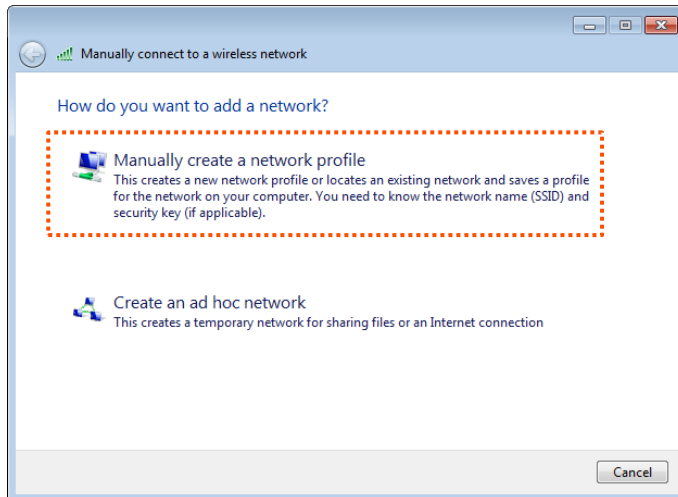
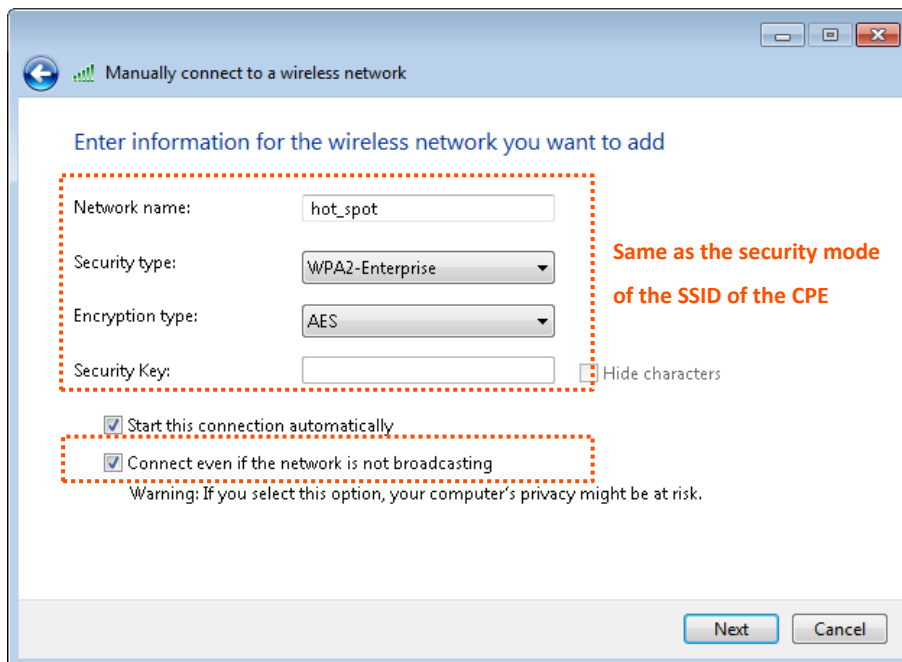
Windows 7 is taken as an example to describe the procedures.

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

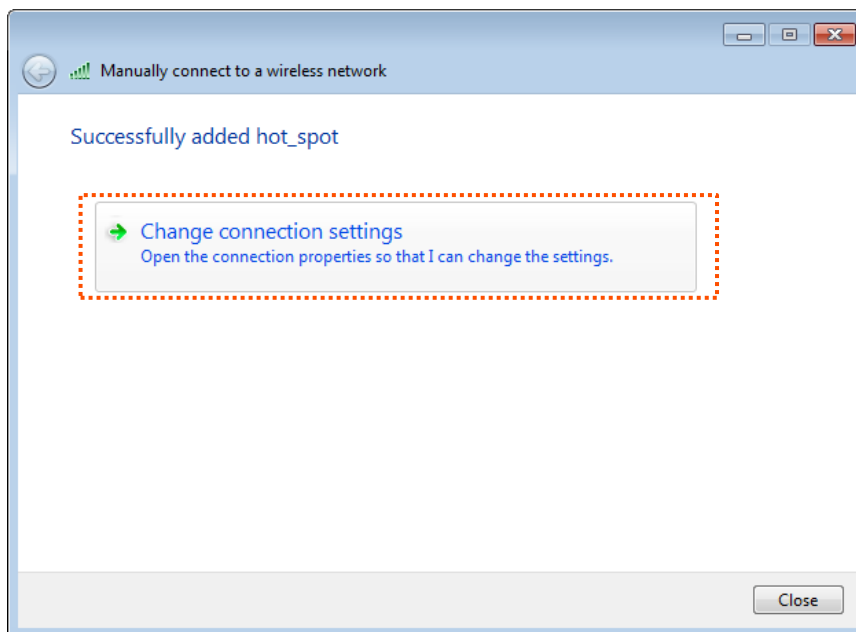


Step 2 Click **Add**.

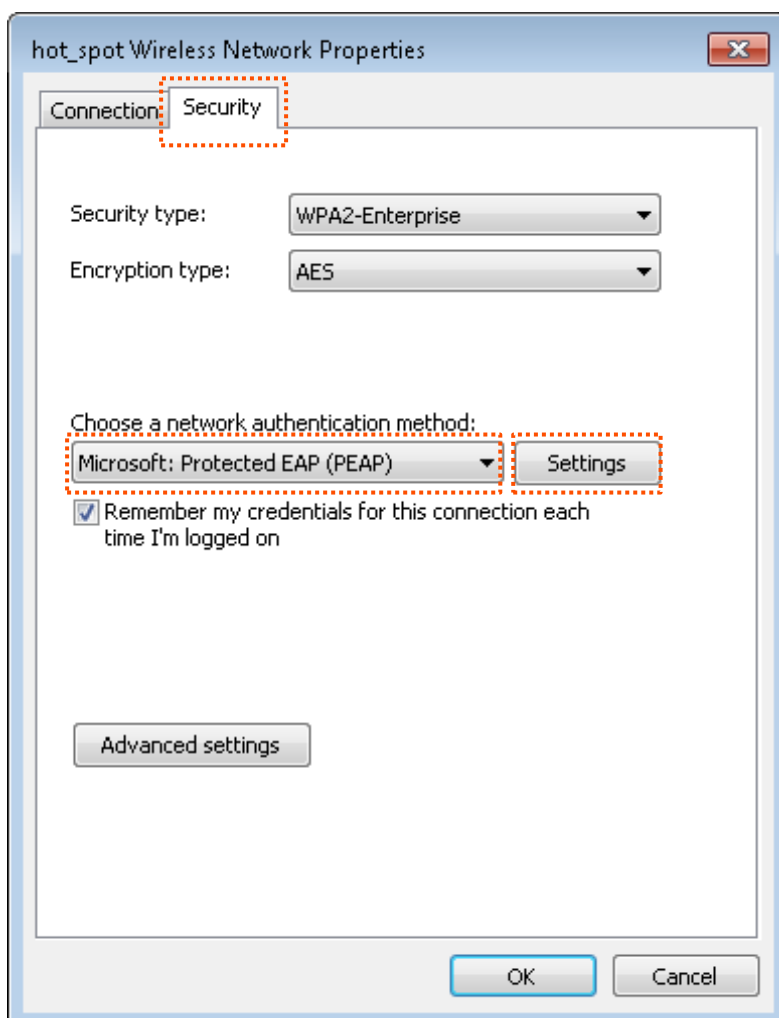


Step 3 Click **Manually create a network profile**.**Step 4** Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.

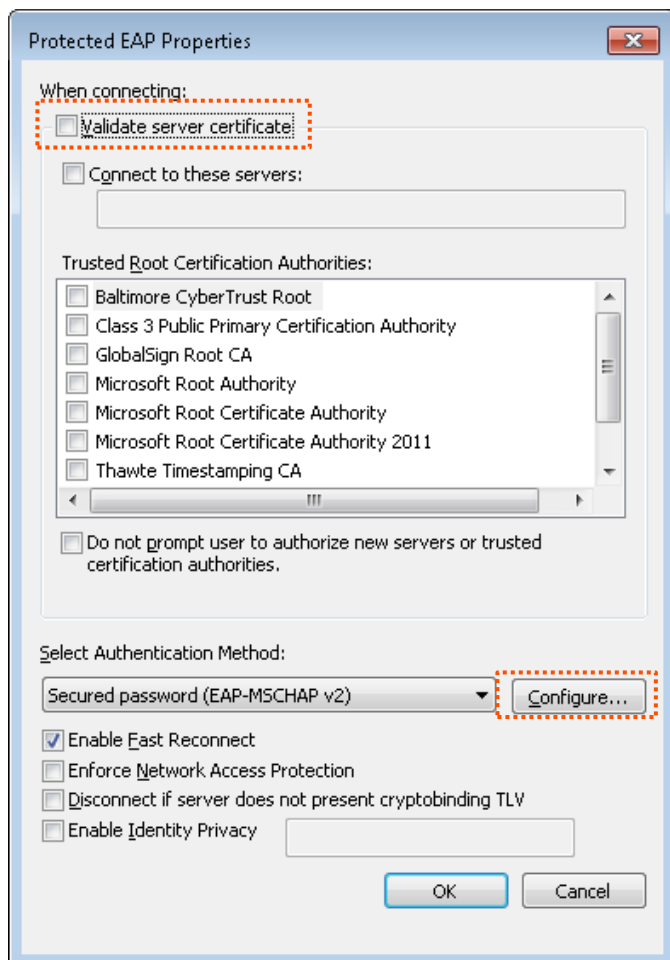
Step 5 Click **Change connection settings**.



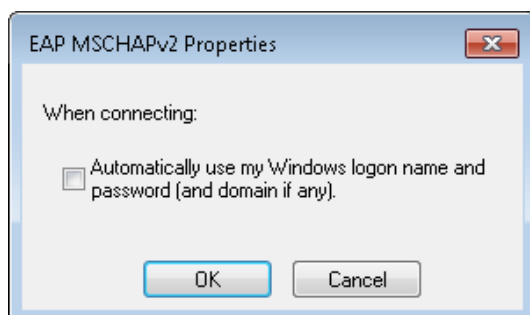
Step 6 Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.

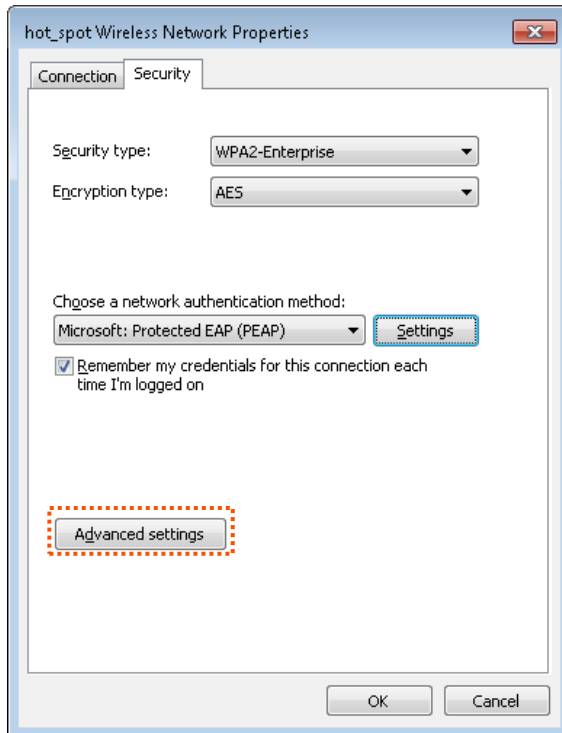
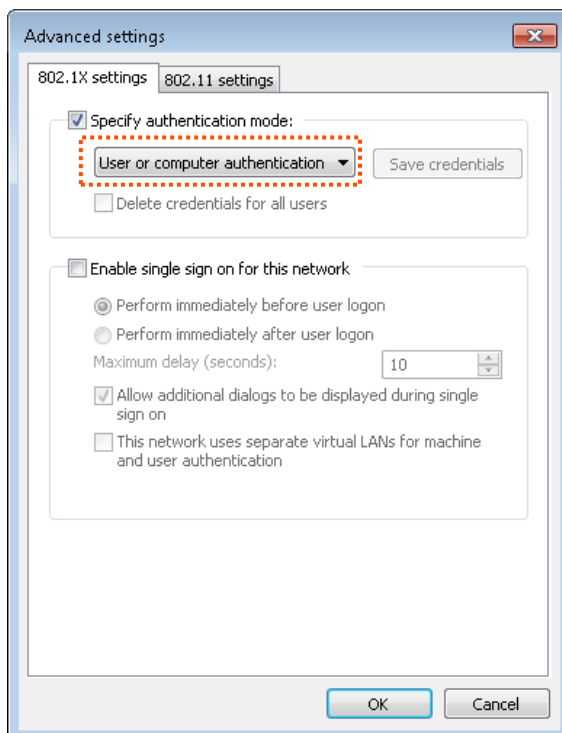


Step 7 Deselect **Validate server certificate** and click **Configure**.

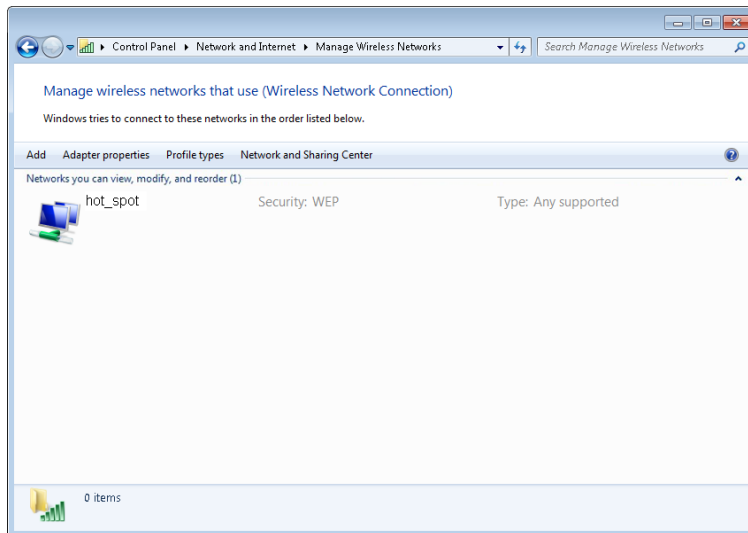
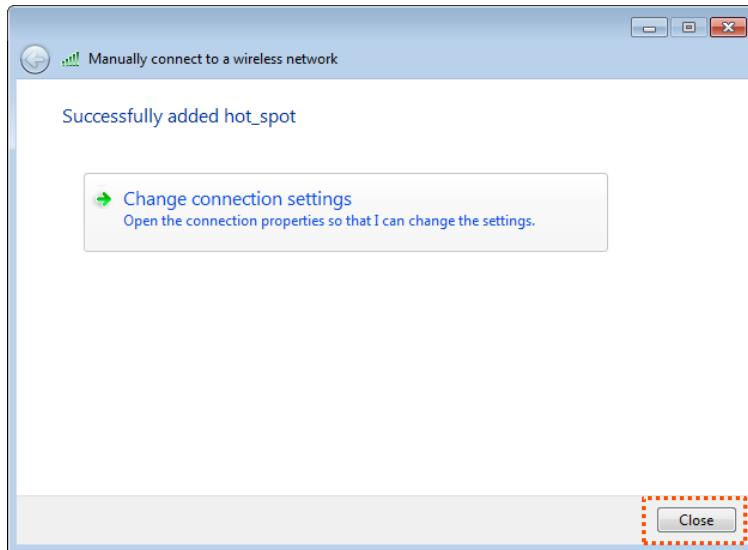


Step 8 Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.

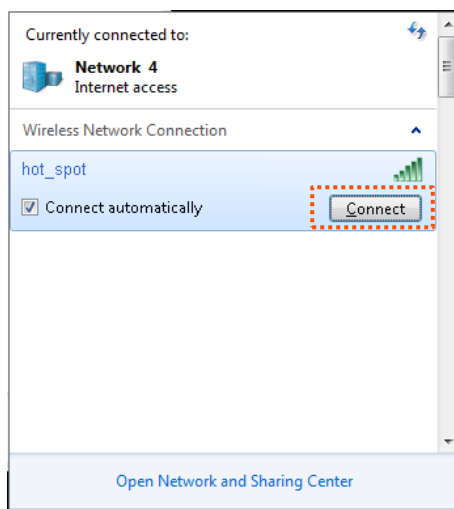


Step 9 Click **Advanced settings**.**Step 10** Select **User or computer authentication** and click **OK**.

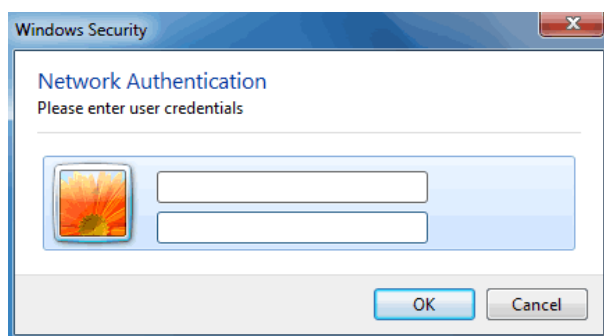
Step 11 Click **Close**.



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



Step 13 In the Windows Security dialog box that appears, enter the [user name and password](#) set on the RADIUS server and click **OK**.



----End

Verification

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

7.2 Advanced

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

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

Advanced ?

WMM Enable Disable

APSD Enable Disable

Minimum RSSI Threshold Enable Disable

Preamble Short Preamble Long Preamble

Transparent Bridge Enable Disable

TD-MAX Enable Disable

Signal Transmission Coverage-oriented Capacity-oriented

TPC Enable Disable

Signal Reception Level

Transmission Distance Auto km (Range: 0.1 to 20, default: 5)

Beacon Interval ms (Range: 40 to 999, default: 100)

Fragment Threshold (Range: 256 to 2346, default: 2346)

RTS Threshold (Range: 1 to 2347, default: 2347)

DTIM Interval (Range: 1 to 255, default: 1)



Signal LED1 Threshold dBm (Range: -99 to 0, default: -90)

Signal LED2 Threshold dBm (Range: -99 to 0, default: -80)

Signal LED3 Threshold dBm (Range: -99 to 0, default: -70)

Parameters description

Name	Description
WMM	WMM (Wi-Fi Multi-media) is a wireless QoS (Quality of Service) protocol making packets with higher priorities to be transmitted earlier. This ensures better QoS of voice and video applications over wireless networks.

Name	Description
APSD	<p>APSD (Automatic Power Save Delivery) is a WMM power saving protocol created by Wi-Fi Alliance.</p> <p>Enabling APSD helps reduce power consumption. By default, this mode is disabled.</p>
Minimum RSSI Threshold	<p>It specifies the minimum strength of received signals acceptable to this device.</p> <p>If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device.</p> <p>If there are multiple CPEs in a network, setting a proper value helps wireless devices connect to WiFi network with better WiFi signal.</p>
Preamble	<p>It specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data.</p> <p>By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients.</p> <p>To achieve better synchronization performance of networks, you can select the Short Preamble option.</p>
Transparent Bridge	<p>The Transparent Bridge function enables the WLAN interface of this device 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.</p> <p> TIP</p> <p>This function is only applicable when the CPE works in AP, Client or Universal Repeater mode.</p>
TD-MAX	<p>TD-MAX is Tenda's proprietary Time Division Multiple Access (TDMA) polling technology. It allows multiple clients to share the same channel for accessing to a network. With the TD-MAX enabled, the CPE assigns time slots to each client, and transmits data according to the assigned time slots, achieving Point-to-MultiPoint (P2MP) connections.</p> <p>After the TD-MAX is enabled, the CPE:</p> <ul style="list-style-type: none"> • Avoids the “hidden node” problem, which occurs when a node is visible from a wireless AP, but not from other nodes communicating with the originating AP. • Reduces latency. • Improves throughput and anti-interference performance. <p>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.</p> <p> NOTE</p> <p>If TD-MAX is enabled, the device operates in TD-MAX mode and only accepts connections from TD-MAX devices. And you cannot connect standard Wi-Fi devices, such as laptops, tablets, or smart phones, to the CPE.</p>
Signal Transmission	<p>It specifies the wall penetrating capability of the CPE.</p> <ul style="list-style-type: none"> • Coverage-oriented: With less interference nearby, this mode enables the device to cover wider area.

Name	Description
	<ul style="list-style-type: none"> • Capacity-oriented: With strong interference nearby, this mode improves the device's anti-interference capability.
TPC	<p>The Transmit Power Control (TPC) function decreases the TX power of this device automatically to improve the negotiation rate when the two devices are too close.</p> <p>By default, when the received signal strength is greater than -25 dBm, the CPE decreases its TX power. The received signal strength can be checked on the Status > Wireless Status page.</p>
Signal Reception Level	<p>It is used to adjust the signal reception level. 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.</p>
Transmission Distance	<p>It specifies the wireless transmission distance of this device. You can set it based on the actual installation distance.</p>
Beacon Interval	<p>It specifies the interval at which this device sends Beacon frames.</p> <p>Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.</p>
Fragment Threshold	<p>It specifies the threshold of a fragment. The unit is byte.</p> <p>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.</p> <p>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.</p> <p>In an environment with little interference, you can increase the threshold to reduce the number of fragments, so as to increase the frame throughput.</p>
RTS Threshold	<p>It specifies the frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte.</p> <p>Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts.</p> <p>The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.</p>
DTIM Interval	<p>It specifies the countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval.</p> <p>For example, if DTIM Interval is set to 1, this device transmits all cached frames at one Beacon interval.</p>
Signal LED1/2/3	<p>The device uses three signal LED indicators to indicate the received signal strength in an intuitive way, and allows you to customize the threshold for triggering each</p>

Name	Description
Threshold	signal LED indicator to light up. The default threshold for LED1, LED2, and LED3 are -90 , -80 , and -70 respectively.

7.3 Access control

7.3.1 Overview

The Access Control function enables you to allow or disallow the wireless devices to access the wireless network based on their MAC addresses. The CPE supports the following MAC address filter rules.

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

To access the page, choose **Wireless > Access Control**.

The screenshot shows the 'Access Control' configuration interface. At the top, the SSID is set to 'Connect me'. The 'Access Control' toggle is turned on. The 'Mode' is set to 'Disallow'. Below this, there is a 'MAC Address' input field containing '12:12:12:12:12:12' and two buttons: 'Add' and 'Add online devices'. A table below lists the 'Access Control List' with columns for SN, MAC Address, Status, and Operation. The first row is highlighted with a dashed orange border and contains SN '1', MAC Address '12:12:12:12:12:12', Status 'Enable' (with a toggle switch), and a trash icon. At the bottom of the form are 'Save' and 'Cancel' buttons. An orange arrow points from the text 'Access Control List' to the first row of the table.

Parameters description

Name	Description
SSID	It specifies the SSID of this device. With the rule enabled, clients connected to the network with this SSID will be controlled by the rule.
Access Control	It specifies whether to enable the Access Control function.
Mode	It specifies the mode for filtering MAC addresses. <ul style="list-style-type: none"> • Allow: It indicates that only the wireless clients on the access control list can connect to the WiFi network of the CPE. • Disallow: It indicates that only the wireless clients on the access control list cannot connect to the WiFi network of the CPE.

7.3.2 Example of configuring access control

Networking requirement

A wireless network whose SSID is **Connect me** has been set up in an estate. Only specific members in this estate are allowed to connect to the wireless network.

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

Configuration procedures

- Step 1** Choose **Wireless > Access Control** to enter the configuration page.
- Step 2** Enable the **Access Control** function.
- Step 3** Set the **Mode** to **Allow**.
- Step 4** Enter the MAC address, which is **C8:3A:35:00:00:01** in this example, and click **Add**.



TIP

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

- Step 5** Perform **Step 4** to add the other two MAC addresses.
- Step 6** Click **Save**.

Access Control ?

SSID Connect me

* Access Control

* Mode Disallow Allow

* MAC Address

SN	MAC Address	Status	Operation
1	C8:3A:35:00:00:01	<input checked="" type="checkbox"/> Enable	
2	C8:3A:35:00:00:02	<input checked="" type="checkbox"/> Enable	
3	C8:3A:35:00:00:03	<input checked="" type="checkbox"/> Enable	

----End

Verification

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

8 Advanced

8.1 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 port of the CPE is the same as that of peer device. By default, the LAN speed settings of the LAN port is **Auto Negotiation**. OS3V1.0 is used for illustration.

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

The screenshot shows a configuration window titled "LAN Rate" with a question mark icon in the top right corner. It contains four dropdown menus for "PoE/LAN Speed", "LAN2 Speed", "LAN3 Speed", and "LAN4 Speed", all of which are currently set to "Auto Negotiation". At the bottom of the window are two buttons: "Save" (in orange) and "Cancel" (in white with a grey border).

Parameters description

Name	Description
Auto Negotiation	The speed and duplex mode of the port is determined by the negotiation between the port of the CPE and the port of the peer device.
100Mbps Full-Duplex	The port is under 100 Mbps, and can transmit and receive packets at the same time.
100Mbps Half-Duplex	The port is under 100 Mbps, and can only transmit or receive packets at the same time.
10Mbps Full-Duplex	The port is under 10 Mbps, and can transmit and receive packets at the same time.
10Mbps Half-Duplex	The port is under 10 Mbps, and can only transmit or receive packets at the same time.



- If you set the speed and duplex mode of the port manually, please 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. And ensure that the speed mode for peer port is also 10 Mbps full duplex or auto negotiation.
-

8.2 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 a 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.

8.2.1 Site Survey

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

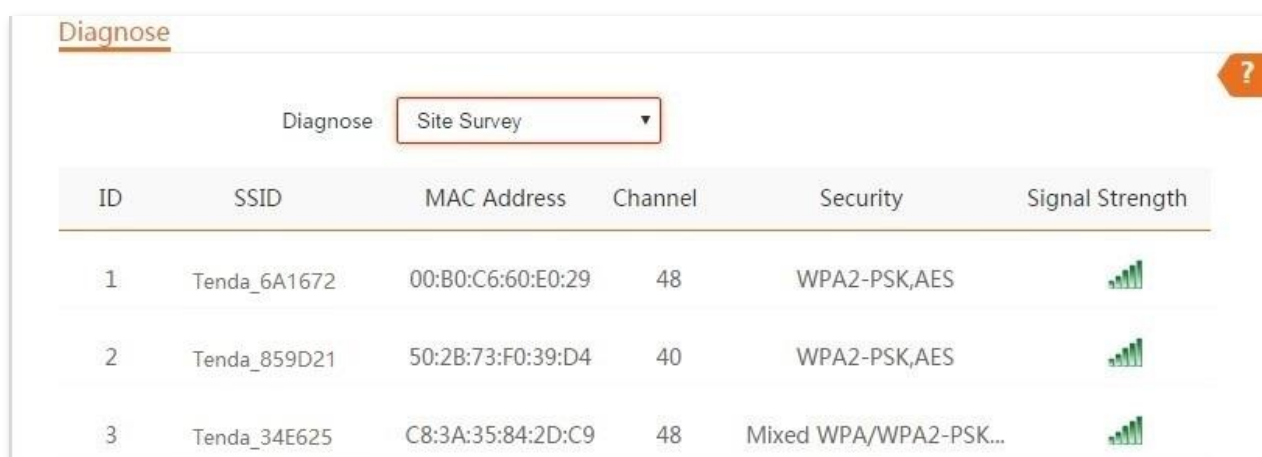
Configuration procedures:

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

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

----End

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



The screenshot shows the 'Diagnose' configuration page. A dropdown menu labeled 'Diagnose' is set to 'Site Survey'. Below it is a table with the following data:

ID	SSID	MAC Address	Channel	Security	Signal Strength
1	Tenda_6A1672	00:B0:C6:60:E0:29	48	WPA2-PSK,AES	
2	Tenda_859D21	50:2B:73:F0:39:D4	40	WPA2-PSK,AES	
3	Tenda_34E625	C8:3A:35:84:2D:C9	48	Mixed WPA/WPA2-PSK...	

8.2.2 Ping

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

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

Configuration procedures:

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

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

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

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

Step 5 Click **Start**.

The screenshot shows a web interface for a network diagnostic tool. At the top left, the word "Diagnose" is underlined. On the top right, there is an orange button with a white question mark. Below this, there are five input fields and a "Start" button. The "Diagnose" field is a dropdown menu with "Ping" selected. The "IP Address" field is a dropdown menu with "Manual" selected. The "IP Address/Domain Name" field is a text input containing "cn.bing.com". The "Ping Packet" field is a text input containing "4", with "(Range: 1 to 10000)" written to its right. The "Packet Size" field is a text input containing "32", with "Byte (Range: 1 to 60000)" written to its right. At the bottom center, there is an orange "Start" button.

----End

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

IP Address	Time	TTL
204.79.197.200	14.761ms	112
204.79.197.200	14.627ms	112
cn.bing.com	Timeout	--
204.79.197.200	14.523ms	112

10 Datas/Page 4 data in total

3 of 4 packets received, 25.00% loss25.00%

Min. 14.523 ms Average 14.64 ms Max. 14.761 ms

8.2.3 Traceroute

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

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

Configuration procedures:

- Step 1** Choose **Advanced** > **Diagnose** to enter the configuration page.
- Step 2** Select **Traceroute** in the **Diagnose** drop-down list menu.
- Step 3** Enter the target IP address or a domain name, which is **cn.bing.com** in this example.
- Step 4** Click **Start**.

The screenshot shows the 'Diagnose' configuration page. At the top left is the title 'Diagnose' with a question mark icon on the right. Below the title, there is a 'Diagnose' label followed by a dropdown menu set to 'Traceroute'. Underneath is an input field labeled 'IP Address/Domain Name' containing the text 'cn.bing.com'. At the bottom center is an orange 'Start' button.

----End

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

The screenshot shows the 'Diagnose' configuration page after the test is completed. The 'Diagnose' dropdown is still set to 'Traceroute' and the 'IP Address/Domain Name' field still contains 'cn.bing.com'. The 'Start' button has been replaced by an orange 'Stop' button. Below the form is a table displaying the traceroute results.

SN	IP Address	Time
1	192.168.11.1	5.541 ms 2.371 ms 2.088 ms
2	172.16.200.1	2.133 ms 1.775 ms 8.384 ms
3	192.168.20.1	6.643 ms 3.543 ms 2.774 ms
4	192.168.21.254	1.885 ms 4.249 ms 2.758 ms
5	100.64.0.1	50.352 ms 3.056 ms 3.428 ms
6	202.105.159.149	4.340 ms 8.592 ms 7.126 ms

8.2.4 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 support the **Speed Test** function.

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

Diagnose ?

Diagnose Speed Test ▼

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

Client Server

IP Address of Peer AP Manual ▼

IP Address

HTTP Port 80

User Name

Password

Test Group 10 (Range: 1 to 20)

Direction Bidirectional ▼

Time 30 s (Range: 1 to 60)

Start

Parameters description

Name	Description
Client	It specifies that the client side launches the test request. You need to set the parameters of speed test on client side.
Server	It specifies that the server launches the test request.
IP Address of Peer AP	It specifies the LAN IP address of 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 in the box manually.
HTTP Port	It specifies the HTTP service port number of peer device, which is used to establish speed test connection based on TCP/IP. Default: 80 . You are recommended to keep the default value.
User Name	It specifies the login user name and password of the peer device.

Name	Description
Password	
Test Group	It specifies the number of test connections launched.
Direction	<p>It specifies the test direction.</p> <ul style="list-style-type: none"> • RX (Receive): Only test the speed that the peer device transmits data to this device. • TX (Transmit): Only test the speed that this device transmits data to peer device. • Bidirectional: test both transmit and receive speed between the two CPEs.
Time	It specifies the duration of speed test, which is 30s by default.
AVG RX	It displays the average receive rate.
AVG TX	It displays the average transmit rate.
AVG Total	It displays the average total rate.

Example of configuring the speed test

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

The procedure can be performed both on the web UI of the CPE1 or CPE2. The CPE2 is used for illustration here.

Assume that:

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

Configuration procedures:

Step 1 Log in to the web UI of CPE2, and choose **Advanced > Diagnose** to enter the configuration page.

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

Step 3 Set **IP Address of Peer AP** to **Manual**.

Step 4 Enter the IP address of CPE1 to the **IP Address** box, which is **192.168.2.100** in this example.

Step 5 Enter the login user name and password of the web UI of CPE1 in the **User name** and **Password** boxes, which are both **admin** in this example.

Step 6 Set **Direction** to **Bidirectional**.

Step 7 Click **Start**.

Diagnose ?

* Diagnose Speed Test

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

Client Server

* IP Address of Peer AP Manual

* IP Address

HTTP Port

* User Name

* Password

Test Group (Range: 1 to 20)

* Direction Bidirectional

Time s (Range: 1 to 60)

Start

----End

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

Diagnose ?

Diagnose Speed Test

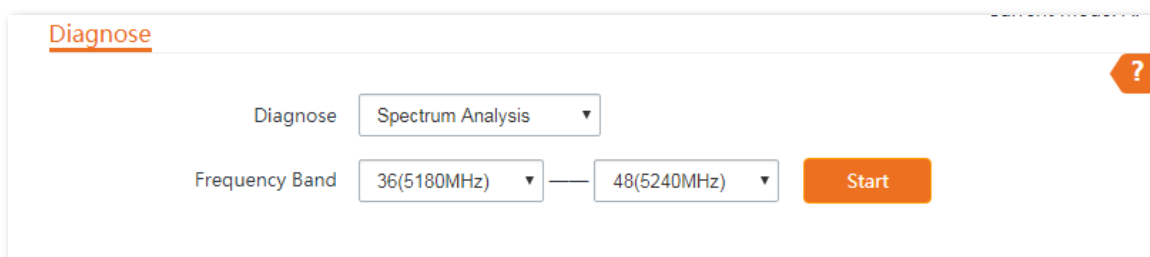
↑ AVG RX	↓ AVG TX	↕ AVG Total
103.28 Mbps	105.17 Mbps	208.45 Mbps

8.2.5 Spectrum Analysis

You can use the Spectrum Analysis to check the wireless noise of each channel, then select a frequency band with less wireless noise for the CPE based on the diagnose result.

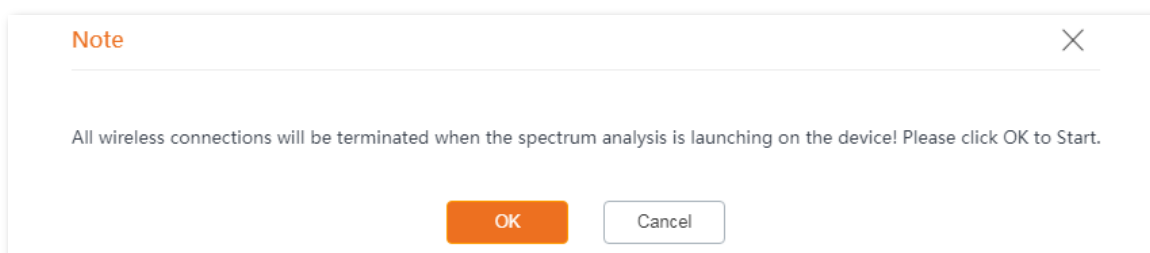
Configuration procedures:

- Step 1** Choose **Advanced** > **Diagnose** to enter the configuration page.
- Step 2** Select **Spectrum Analysis** from the **Diagnose** drop-down list menu.
- Step 3** Select the frequency band range you want to test from the drop-down lists.
- Step 4** Click **Start**.



The screenshot shows a configuration window titled "Diagnose" with a question mark icon in the top right corner. It features two dropdown menus: "Diagnose" set to "Spectrum Analysis" and "Frequency Band" with two sub-selectors set to "36(5180MHz)" and "48(5240MHz)". An orange "Start" button is located to the right of the frequency band selectors.

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



The screenshot shows a "Note" pop-up window with a close button (X) in the top right corner. The text inside reads: "All wireless connections will be terminated when the spectrum analysis is launching on the device! Please click OK to Start." At the bottom, there are two buttons: "OK" (orange) and "Cancel" (white with grey border).

----End

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

Diagnose

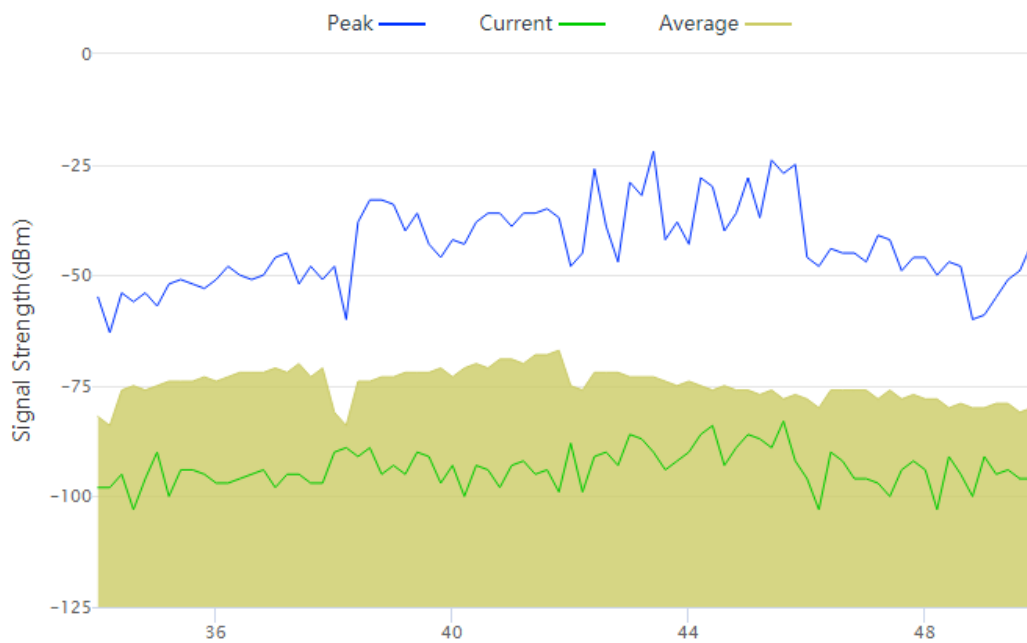


Diagnose Spectrum Analysis

Frequency Band 36(5180MHz)

48(5240MHz)

Start



8.3 Bandwidth control

8.3.1 Overview

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

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

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

Bandwidth Control ?

Remark

IP Address Range 192.168.2. ~ 192.168.2.

Max. Upload Rate Mbps ▼

Max. Download Rate Mbps ▼

Add

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

Parameters description

Name	Description
Remark	It specifies the additional information of the bandwidth control rule. This field is optional. For convenient management, you'd better specify different remarks for different rules.
IP Address Range	It specifies the IP address or IP address range of devices that this rule applies to. If you want to control only one device, enter the same IP address in the two boxes. If you want to control multiple devices, enter an IP address range including start IP address and end IP address. The end IP address should be greater than the start IP address.
Max. Upload Rate	It specifies the maximum upload/download rate of a device whose IP address is within the specified IP Address Range.
Max. Download Rate	
Status	It specifies the current status of the rule. You can enable or disable it as required.
Action	Click to delete the rule.

8.3.2 Example of configuring bandwidth control

Networking requirement

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

Assume that: The maximum upload rate of each device connected to the WiFi network of the device is **5 Mbps**, and download rate is **10 Mbps**. And the IP address range of the devices connected to the WiFi network is **192.168.2.100** to **192.168.2.200**.

Configuration procedures

- Step 1** Choose **Advanced** > **Bandwidth Control** to enter the configuration page.
- Step 2** Enter a remark (optional), such as **Devices of Office1**.
- Step 3** Specify an IP address range, which is **192.168.2.100 ~ 192.168.2.200** in this example.
- Step 4** Specify the maximum upload rate and download rate respectively, which are **5** and **10** in this example.
- Step 5** Click **Add**.

----End

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

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	<input checked="" type="checkbox"/> Enable	

10 ▾ Datas/Page 1 data in total

Verification

For a device 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.

8.4 Port forwarding

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

8.4.1 Overview

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, and avoid the attacks from the WAN.

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

Port Forwarding ?

Internal IP Address

Internal Port

External Port

Protocol


Application

Add

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

Parameters description

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

Name	Description
	After you select an Application , this option will be auto populated. You can also customize it.
Protocol	It specifies the protocol type of the selected applications. Select TCP&UDP when you are not sure.
Application	It specifies the application services established in LAN. The device provides some common services. After you select an application, the internal and external ports will be populated.
Status	It specifies the status of the rule. You can enable or disable it based on your need.
Action	Click  to delete the rule.

8.4.2 Example of configuring port forwarding

Networking requirement

The CPE is in WISP mode and has connected to the ISP hotspot to provide internet access for a remote household.

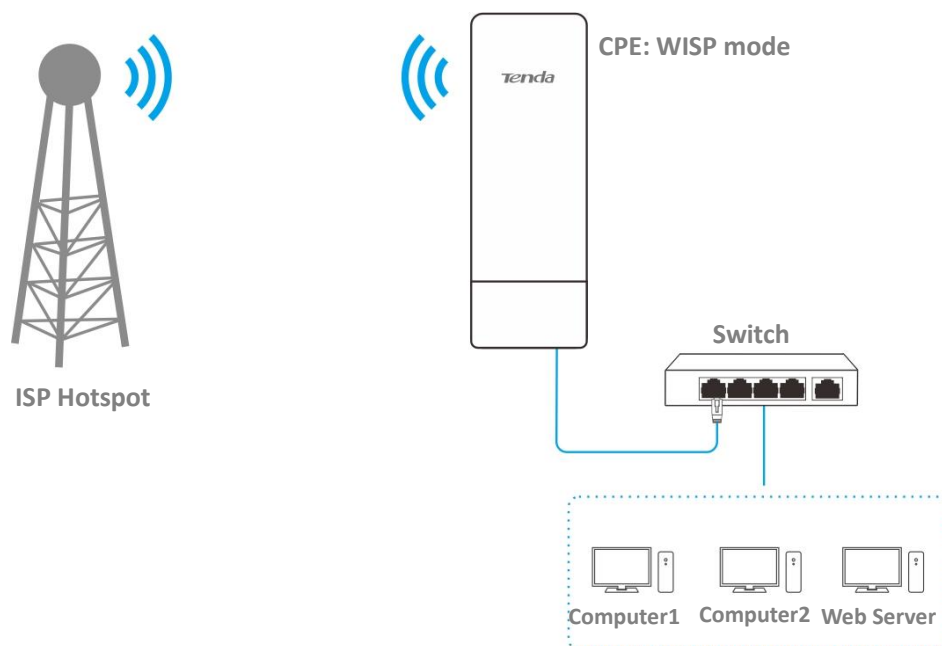
Requirement: Family members who are not at home can visit the resources on the web server in LAN over the internet.

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

Assume that:

- IP Address of the web server: **192.168.2.100**
- Service port (internal port) of the web server in LAN: **80**
- External port that this device enables for internet devices: **80**
- WAN IP Address of the device: **202.105.11.22**

Network topology



Configuration procedures

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


- Step 1** Choose **Advanced > Port Forwarding** to enter the configuration page.
- Step 2** Enter the IP address of the web server in the **Internal IP Address** box, which is **192.168.2.100** in this example.
- Step 3** Select an application from the drop-down list of **Application**, which is **HTTP** in this example, and the **Internal Port** and **External Port** boxes will be automatically populated.
- Step 4** Select the protocol used for web server from the drop-down list of **Protocol**, which is **TCP&UDP** in this example.
- Step 5** Click **Add**.

Port Forwarding ?

Internal IP Address	<input type="text" value="192.168.2.100"/>
Internal Port	<input type="text" value="80"/>
External Port	<input type="text" value="80"/>
Protocol	<input type="text" value="TCP&UDP"/>
Application	<input type="text" value="HTTP"/>

----End

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

ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	80	80	TCP&UDP	HTTP	<input checked="" type="checkbox"/> Enable	

10 Datas/Page 1 data in total

Verification

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



TIP

If internet users cannot visit the server in LAN after the 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.

8.5 MAC filter

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

8.5.1 Overview


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

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

The function is disabled by default. Set the mode to **Allow**, and the page is shown as below.

Parameters description

Name	Description
Mode	<p>It specifies the mode of MAC filter rule.</p> <ul style="list-style-type: none"> • Disable: Disable the MAC Filter function. • Allow: Allow the devices with the MAC addresses in the list to access the internet via the CPE, and disallow the other devices to access the internet via the CPE. • Disallow: Disallow the devices with the MAC addresses in the list to access the internet via the CPE, and allow the other devices to access the internet via the CPE.
Remark	It specifies the additional information of the rule.
MAC Address	It specifies the MAC address of the device to which the rule applies.
Time	It specifies the period at which the rule takes effect.

Name	Description
Date	It specifies the dates on which the rule takes effect.
Status	It specifies the status of the rule. You can enable or disable the rule based on your need.
Action	Click  to delete the rule.

8.5.2 Example of configuring MAC filter

Networking requirement

The CPE is in WISP mode and has connected to the ISP hotspot to provide internet access for a remote household.

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

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

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

Configuration procedures

- Step 1** Choose **Advanced > MAC Filter** to enter the configuration page.
- Step 2** Select a mode, which is **Allow** in this example.
- Step 3** (Optional) Enter a remark in the **Remark** box, which is **Dad's smartphone** in this example.
- Step 4** Enter the MAC address of the device, which is **CC:3A:61:71:1B:6E** in this example.
- Step 5** Specify a period, which is **9:00 to 17:00** in this example.
- Step 6** Tick the dates, which are Monday to Friday in this example.
- Step 7** Click **Add**.
- Step 8** Perform **Step2** to **Step7** to add the rule with the other MAC address.

MAC Filter ?

Mode Allow

Remark Dad's smartphone

MAC Address CC:3A:61:71:1B:6E



Time 09 : 00 ~ 17 : 00

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

Add

----End

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

ID	Remark	MAC Address	Time	Mode	Status	Action
1	Dad's smar...	CC:3A:61:71:1B:6E	Mon. , Tue. , Wed. , Thur. , Fri. 09:00-17:00	Allow	<input checked="" type="checkbox"/> Enable	
2	Mum's lapt...	CC:3A:61:75:1F:3E	Mon. , Tue. , Wed. , Thur. , Fri. 09:00-17:00	Allow	<input checked="" type="checkbox"/> Enable	

10 v Datas/Page 2 data in total

Verification

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

8.6 Network service

8.6.1 DDNS

Overview

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

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

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

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

The screenshot shows the 'Network Service' configuration page. At the top, there is a section titled 'Network Service' with a red underline. Below this, the 'DDNS' function is shown as a toggle switch, currently turned off. Underneath, there are four input fields: 'Service Provider' (a dropdown menu with '3322.org' selected and a 'Register' link to its right), 'User Name', 'Password', and 'Domain Name'.

Parameters description

Name	Description
DDNS	It specifies whether to enable the DDNS function.
Service Provider	It specifies Dynamic Domain Name Service provider. The CPE supports Dyn dns, No-ip.com, and 3322.org.
User Name	It specifies the user name/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	It specifies the domain name information obtained from the dynamic DNS server. You need to enter the domain name which you registered on the website manually.

Example of configuring DDNS

Networking requirement

The CPE is in WISP mode and has connected to the ISP hotspot to provide internet access for a remote household. The WAN IP address of the CPE is dynamic.

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

Assume that:

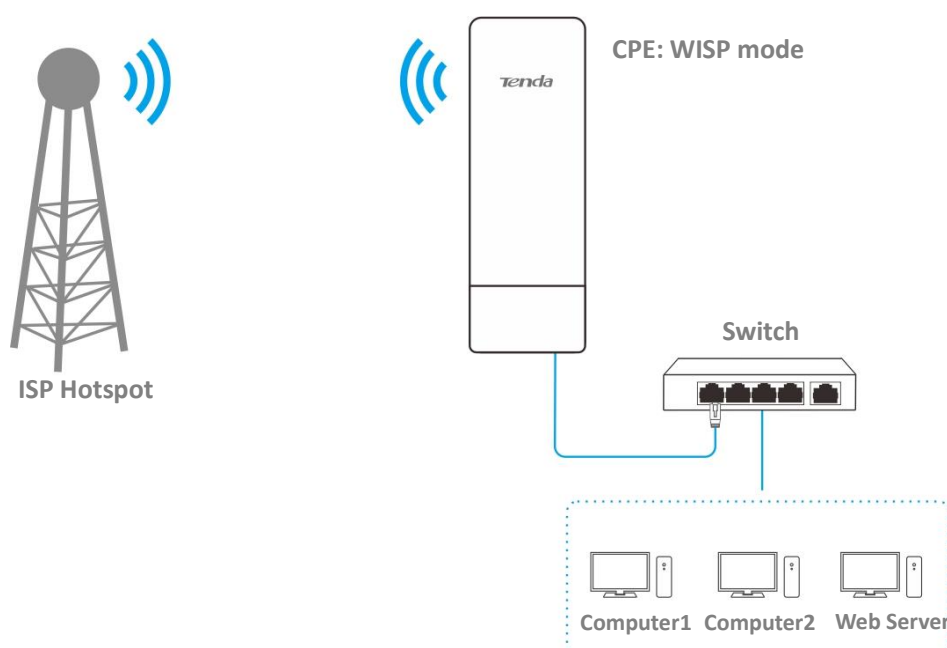
The information of the web server in LAN is shown as follows:

- **IP Address:** 192.168.2.100
- **Service Port of the Web Server:** 80

The registered domain name information is shown as follows:

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

Network topology

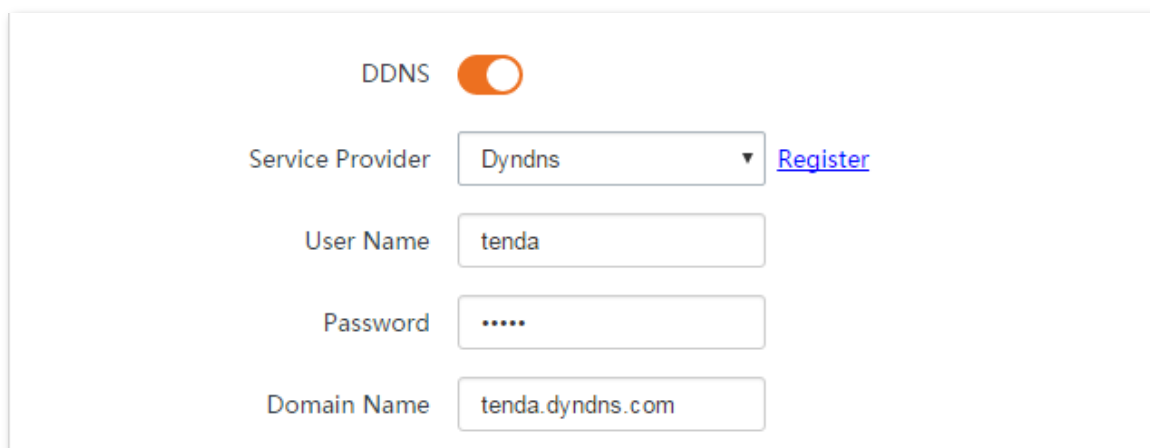


Configuration procedures

Step 1 Set up the DDNS function.

1. Choose **Advanced > Network Service** to enter the configuration page.
2. Enable the **DDNS** function.
3. Select a service provider, which is **Dyndns** in this example.

4. Enter the user name and password you registered with DDNS service provider, which are **tenda** and **tenda** in this example.
5. Enter the domain name you registered, which is **tenda.dyndns.com**.
6. Click **Save** on the bottom of this page.



DDNS

Service Provider [Register](#)

User Name

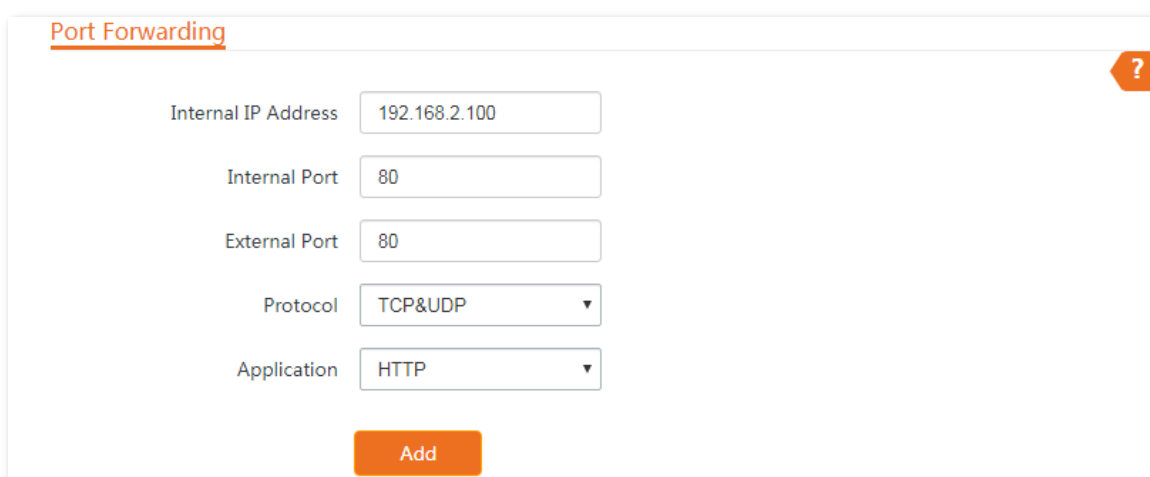
Password

Domain Name

Step 2 Set up the port forwarding function.

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

1. Choose **Advanced > Port Forwarding** to enter the configuration page.
2. Enter the IP address of the web server, which is **192.168.2.100** in this example.
3. Select an application, which is **HTTP** in this example, and the Internal Port and External Port will be populated automatically.
4. Select the protocol of the service. **TCP&UDP** is recommended if you are not sure.
5. Click **Add**.



Port Forwarding ?

Internal IP Address

Internal Port


External Port

Protocol

Application

----End

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

ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	80	80	TCP&UDP	HTTP	<input checked="" type="checkbox"/> Enable	

10 Datas/Page 1 data in total

Verification

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



TIP

If internet users cannot visit the server in LAN after the 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.

8.6.2 Remote web management

Overview

The **Remote Web Management** function is only available in **WISP** or **Router** mode.

Generally, only the clients connected to the CPE can access its web UI.

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

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

Parameters description

Name	Description
Remote Web Management	It specifies whether to enable the remote web management function.
IP Address	<p>It specifies the IP address of a device which is allowed to access the web UI of the CPE.</p> <ul style="list-style-type: none"> • All: It indicates that any computer in WAN can manage the CPE remotely. For security, this option is not recommended. • Manual: It indicates that only the device with specified IP address can manage the CPE remotely. If the CPE belongs to a LAN, the gateway address (a public IP address) of the CPE should be entered.
Port	<p>It specifies the port number used for remote management of CPE. Default: 8080. You can change it if necessary.</p> <p>Ports 1 to 1024 have been used by well-known services. To avoid port conflicts, you can set the port number to one between 1025 and 65535. Then you can access the CPE from WAN by visiting an address in the form of http://WAN 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.</p>

Example of configuring remote web management

The CPE is in WISP mode and has connected to the ISP hotspot to provide internet access for a remote household.

Networking requirement

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

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

Assume that:

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

Configuration procedures

Step 1 Choose **Advanced > Network Service** to enter the configuration page.

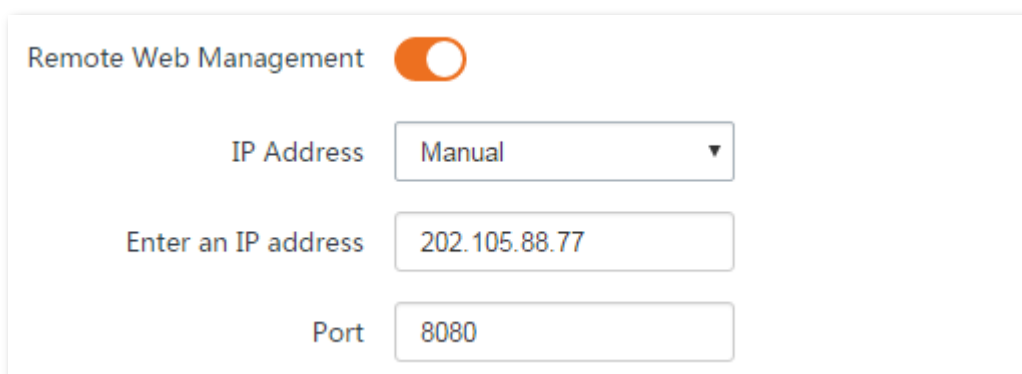
Step 2 Enable the **Remote Web Management** function.

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

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

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

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



Remote Web Management

IP Address

Enter an IP address

Port

----End

Verification

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

8.6.3 Reboot schedule

Overview

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 long-time running.

Configuration procedures

- Step 1** Choose **Advanced > Network Service** to enter the configuration page.
- Step 2** Enable the **Reboot Schedule** function.
- Step 3** Specify a time at which the device reboots, which is 3:00 in this example.
- Step 4** Specify the dates on which the CPE reboots, which is every day in this example.
- Step 5** Click **Save** on the bottom of this page.

Reboot Schedule

Time

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

----End

After successfully configured, the CPE will automatically reboot at 3 a.m. every day.

8.6.4 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.

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

Login Timeout Interval min Range: 1-60 minutes

8.6.5 SNMP agent

Overview

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

- **SNMP manager:** It is a system that controls and monitors network nodes using the SNMP protocol. The SNMP manager most widely used in network environments is Network Management System (NMS). An NMS can be a dedicated network management server, or an application that implements management functions in a network device.
- **SNMP agent:** It is a software module in a managed device. The module is used to manage data about the device and report the management data to an SNMP manager.
- **MIB:** It is a collection of managed objects. It defines a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its MIB. An SNMP manager can read and/or write objects in the MIB based on the permissions assigned to the SNMP manager.

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

Basic SNMP Operations

The device allows the following basic SNMP operations:

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

SNMP Protocol Version

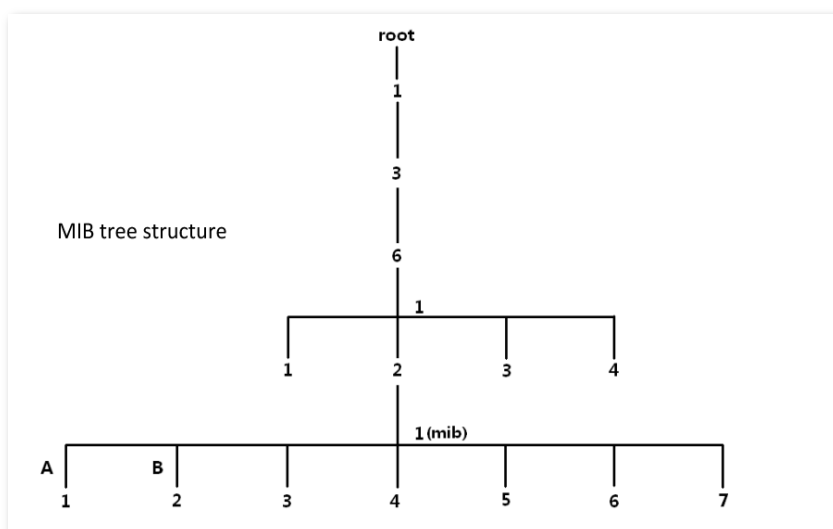
The device is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. Community name is used to define the relationship between an SNMP agent and an SNMP manager. If the community name contained in an SNMP packet is rejected by a device, the

packet is discarded. A community name functions as a password to control SNMP agent access attempts of SNMP managers.

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

MIB Introduction


An MIB adopts a tree structure. The nodes of the tree indicate managed objects. A path consisting of digits and starting from the root can be used to uniquely identify a node. This path is 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.



Parameters description

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

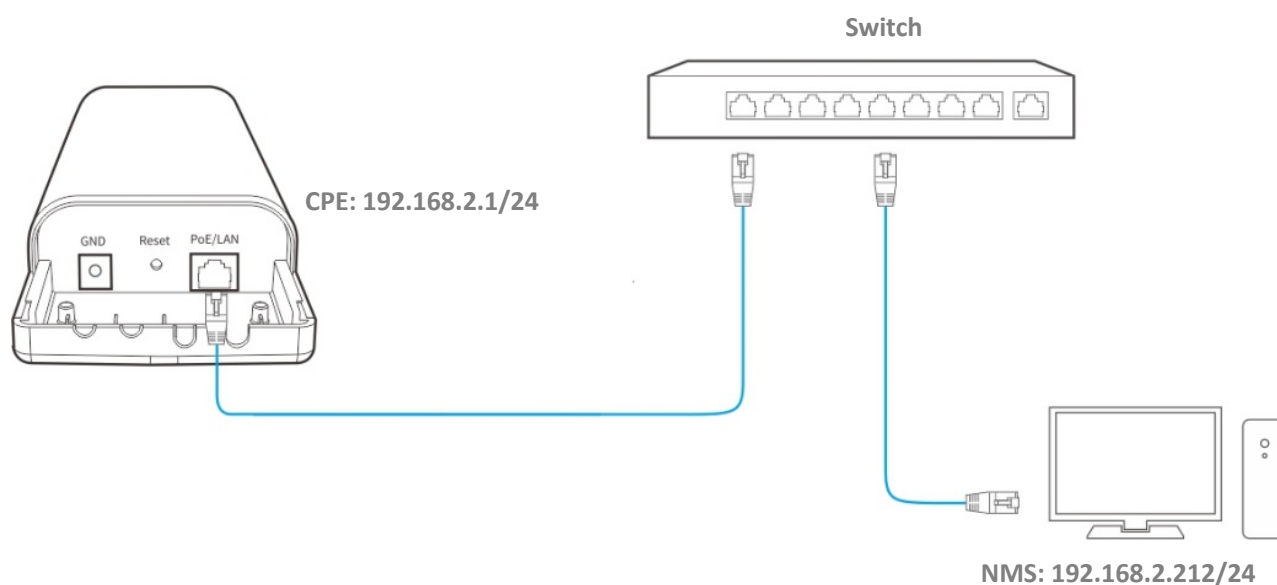
SNMP Agent	<input checked="" type="checkbox"/>
Device Name	<input type="text" value="O4V1.0"/>
Read Community	<input type="text" value="public"/>
Read/Write Community	<input type="text" value="private"/>
Location	<input type="text" value="ShenZhen"/>

Name	Description
SNMP Agent	<p>It specifies whether to enable the SNMP agent function of the CPE. By default, it is disabled.</p> <p>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.</p>
Device Name	<p>It specifies the device name of the CPE. The default device name is the model and version number of the CPE.</p> <p> TIP</p> <p>It is recommended that you change the device name so that you can easily identify the CPE when managing it using SNMP.</p>
Read Community	<p>It specifies the read password shared between SNMP managers and this SNMP agent. The default password is public.</p> <p>The SNMP agent function of the device allows an SNMP manager to use the password to read variables in the MIB of the device.</p>
Read/Write Community	<p>It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is private.</p> <p>The SNMP agent function of the device allows an SNMP manager to use the password to read/write variables in the MIB of the device.</p>
Location	<p>It specifies the location where the CPE is used. You can change the location as required.</p>

Example of configuring the SNMP function

Networking requirement

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



Configuration procedures

Step 1 Set up the CPE.

1. Log in to the web UI of CPE, choose **Advanced** > **Network Service** to enter the configuration page.
2. Enable the **SNMP Agent** function.
3. Set the **Read Community**, which is **Jack** in this example.
4. Set **Read/Write Community**, which is **Jack123** in this example.
5. Click **Save** on the bottom of this page.

* SNMP Agent

Device Name

* Read Community

* Read/Write Community

Location

Step 2 Set up the NMS.

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

----End

Verification

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

8.6.6 Ping watch dog

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

Configuration procedures:

Step 1 Choose **Advanced > Network Service** to enter the configuration page.

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

Step 3 Set the related parameters.

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

The screenshot shows a configuration panel for 'Ping Watch Dog'. At the top, there is a toggle switch labeled 'Ping Watch Dog' which is turned on (orange). Below this are four input fields:

- IP Address:** A text box containing '127.0.0.1'.
- Ping Interval:** A text box containing '300', with a range indicator 'Range : 20-86400 s' to its right.
- Ping Startup Delay:** A text box containing '300', with a range indicator 'Range : 180-86400 s' to its right.
- Threshold of Lost Packets:** A text box containing '3'.

----End

Parameters description

Name	Description
Ping Watch Dog	It specifies whether to enable the Ping Watch Dog function.
IP Address	It specifies the target IP address that the CPE pings.
Ping Interval	It specifies the interval at which the CPE transmits packets to ping the target IP address.
Ping Startup Delay	It specifies the delay time for the CPE to enable the Ping Watch Dog function after the CPE startup completes. Default: 300 s. 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	It specifies the threshold of lost packet that triggers reboot. Range: 1 to 65535, default: 3. For example, if 5 is set, the device will reboot automatically when it does not receive response after sending 5 Ping packets to target IP address/domain name.

8.6.7 DMZ host

Overview

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

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



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

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

Parameters description

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

Example of configuring DMZ host

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

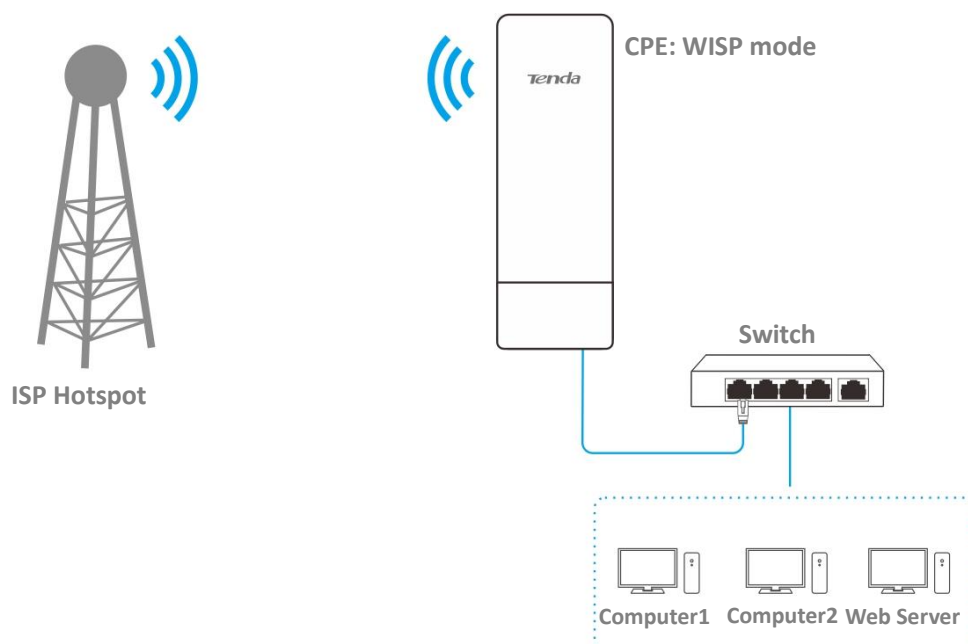
Networking requirement

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

Assume that:

- The WAN IP address of the device is **202.105.106.55**.
- The internal web server IP Address: **192.168.2.100**.
- The port number is: **9999**.

Network topology



Configuration procedures:

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

- Step 1** Choose **Advanced > Network Service** to enter the configuration page.
- Step 2** Enable the **DMZ Host** function.
- Step 3** Enter the IP address of the computer to be set to DMZ host, which is **192.168.2.100** in this example.
- Step 4** Click **Save** on the bottom of this page.

DMZ Host

DMZ Host IP Address

----End

Verification

Enter **Protocol name://WAN port IP address: Port number** in the address bar of a web browser on a computer over the internet to access the resources on the web server. In this example, enter **http://202.105.106.55:9999**.

If the [DDNS](#) function is enabled, you can visit an address in the form of **Protocol name://domain name:9999**.



If internet users cannot visit the server in LAN after the 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 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.

8.6.8 Telnet service

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

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



8.6.9 UPnP

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

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

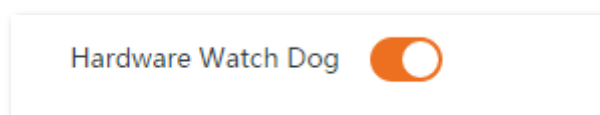
You can enable it as required.



8.6.10 Hardware watch dog

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

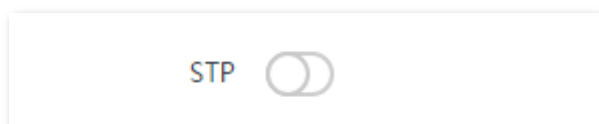
Choose **Advanced > Network Service** to enter the page. By default, the function is enabled.



8.6.11 STP

Spanning Tree Protocol (STP) is a network protocol standardized by IEEE 802.1d. It helps establish a loop-free logical topology for Ethernet network, and allows a network design to include backup links to provide fault tolerance if an active link fails. The STP-enabled device creates a spanning tree within a network of connected layer-2 bridges, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. So that it prevents packets from continued proliferation and endless loop in a loop network to avoid reducing the capability of processing packets caused by receiving duplicate packets.

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



9 Tools

9.1 Date & time

This module enables you to set the system time of the CPE.

Ensure that the system time of the CPE is correct, so that logs can be recorded correctly and the reboot schedule can be executed correctly.

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

The CPE allows you to set the system time by synchronizing the time with the internet or manually setting the time. By default, it is configured to synchronize the system time with the internet.



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

9.1.1 Synchronized with the Internet

The CPE automatically synchronizes its system time with a time server of 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 the configuration procedure of corresponding mode in [Quick Setup](#).

Configuration procedures:

- Step 1** Choose **Tools > Date & Time** to enter the configuration page.
- Step 2** Set **Time settings** to **Synchronized with the Internet**.
- Step 3** Specify a time interval. The default value **30 minutes** is recommended.
- Step 4** Set **Time Zone** to your time zone.
- Step 5** Click **Save**.

----End

Parameters description

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

9.1.2 Manual

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 procedures:

- Step 1** Choose **Tools > Date & Time** to enter the configuration page.
- Step 2** Set the **Time Settings** to **Manual**.
- Step 3** Enter a correct date and time, or click **Synchronize with PC Time** to synchronize the system time of the CPE with the system time (ensure that it is correct) of the computer being used to manage the CPE.
- Step 4** Click **Save**.

Date & Time ?

Time Settings Synchronized with the Internet Manual

Date & Time Y M D h m s

----End

Parameters description

Name	Description
Time Settings	It 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.

9.2 Maintenance

9.2.1 Reboot device

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

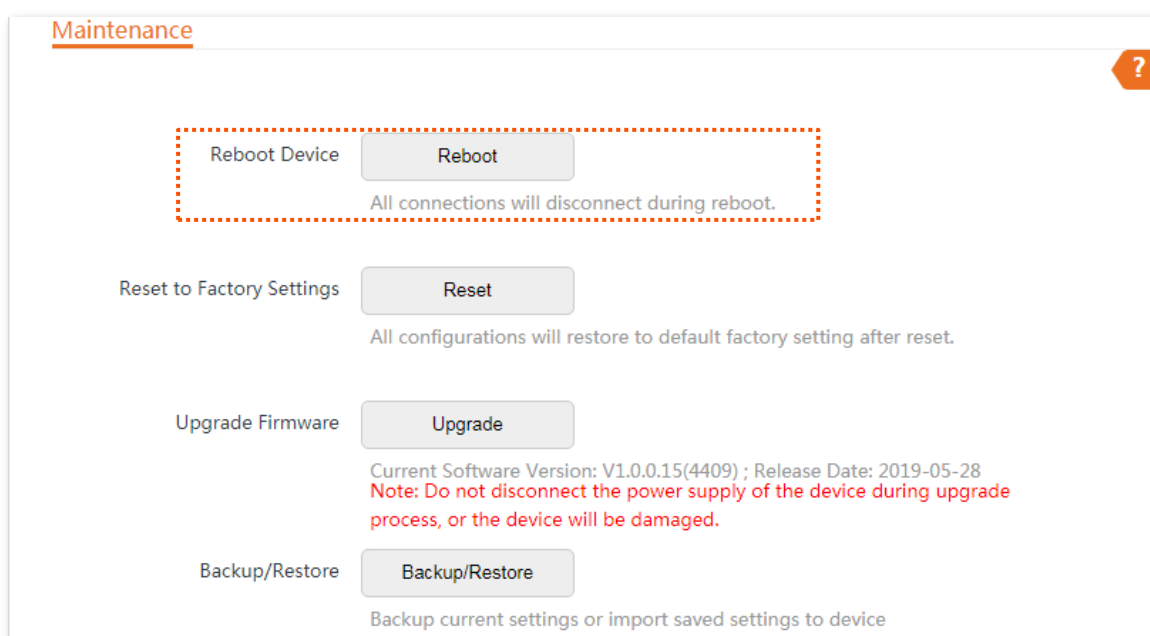


When the device reboots, the current connections will be disconnected. Perform this operation when the device is NOT busy.

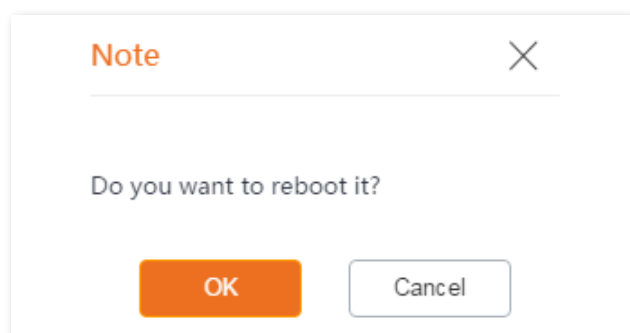
Configuration procedures:

Step 1 Choose **Tools > Maintenance** to enter the configuration page.

Step 2 Click **Reboot**.



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



----End

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

9.2.2 Reset to factory settings

If you cannot locate a fault of the CPE or forget the login password of the web UI, you can reset the CPE to restore its factory settings and then configure it again.

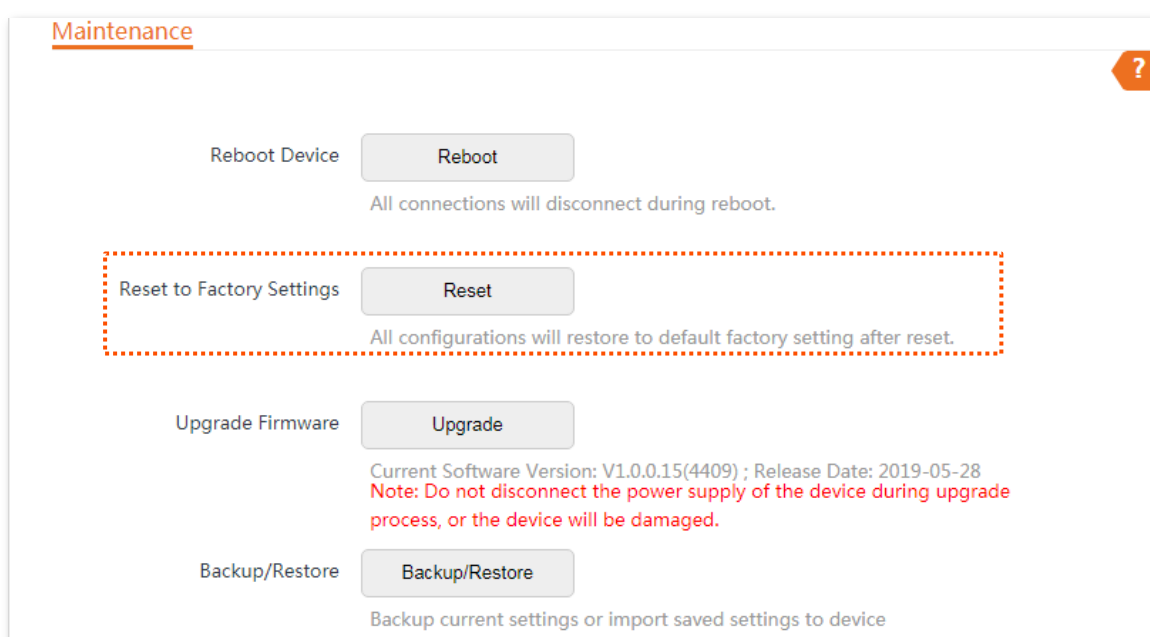


- When the factory settings are restored, the configuration of the device is cleared, and you need to re-configure the device.
- To prevent device damages, do not power off the device during resetting.
- When the factory settings are restored, the login IP address is 192.168.2.1, and both login user name and password are **admin**.

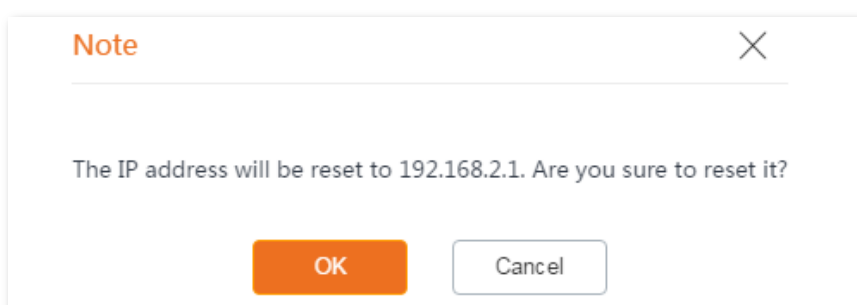
Option 1: Reset the CPE using the web UI

Step 1 Choose **Tools > Maintenance** to enter the configuration page.

Step 2 Click **Reset**.



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



----End

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

Option 2: Reset the CPE using the Reset button

After CPE completes startup, hold down the **Reset** button for about 8 seconds, then release it when all the LED indicators light up. Wait for about 1 minute.

9.2.3 Upgrade firmware

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



To prevent damaging the device, please:

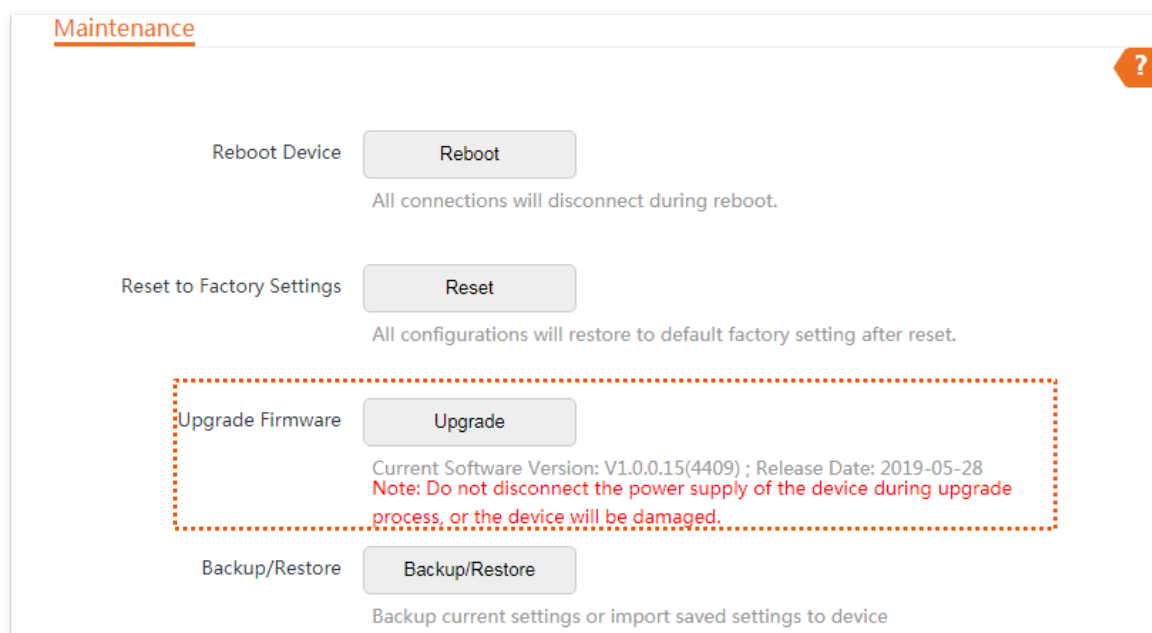
- Ensure that the new firmware version is applicable to the device before upgrading the firmware. Generally, the suffix of the upgrade file is **.bin**.
- Keep the power supply of the CPE connected during an upgrade.

Configuration procedures:

Step 1 Download the package of a later firmware version for the CPE from www.tendacn.com to your local computer, and decompress the package.

Step 2 Log in to the web UI of CPE, and choose **Tools > Maintenance** to enter the configuration page.

Step 3 Click **Upgrade**.



Step 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. On the Status page, check if the current Firmware Version is consistent with the firmware version you selected for

upgrade.



After the device is upgraded, you are recommended to restore the factory settings of the device and configure it again to get the best experience.

9.2.4 Backup/restore

The **Backup/Restore** function enables you to export the current configuration of the CPE to a local computer, and import the configuration file you export before.

You are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the CPE, or import the configuration to other devices of the same product model.

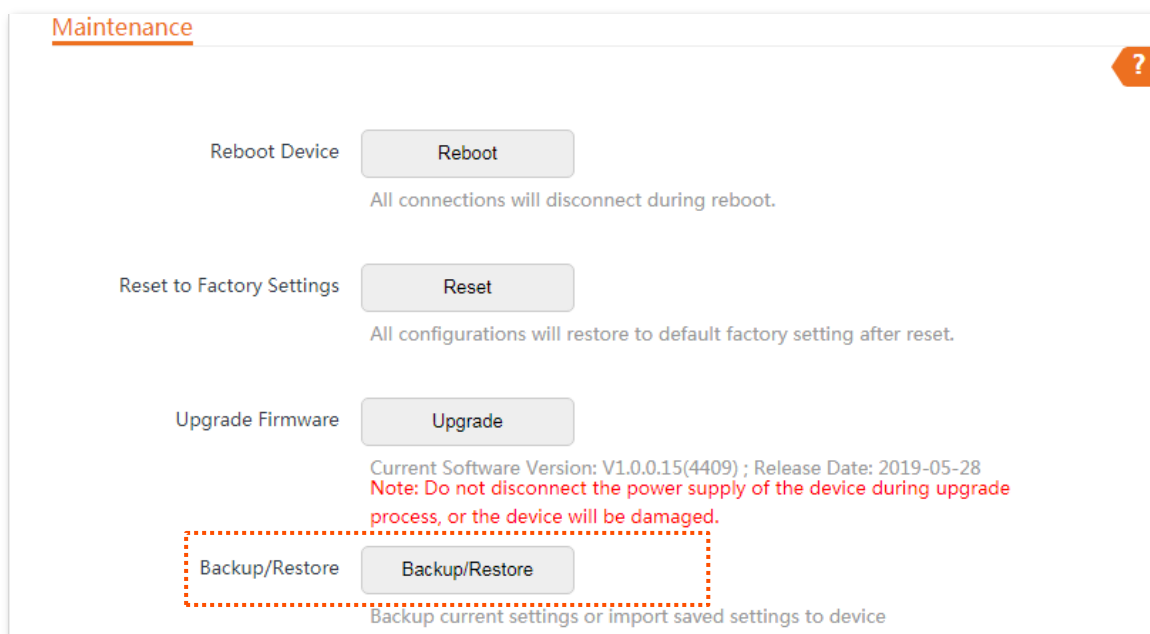


If you need to apply same or similar configurations to many devices, you can configure one of the devices, back up the configuration of the device, and use the backup to restore the configuration on the other devices. This improves configuration efficiency.

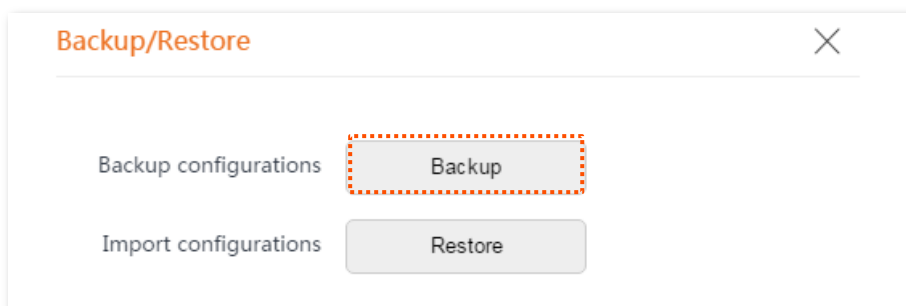
Export the configuration

Step 1 Choose **Tools > Maintenance** to enter the configuration page.

Step 2 Click **Backup/Restore**.



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



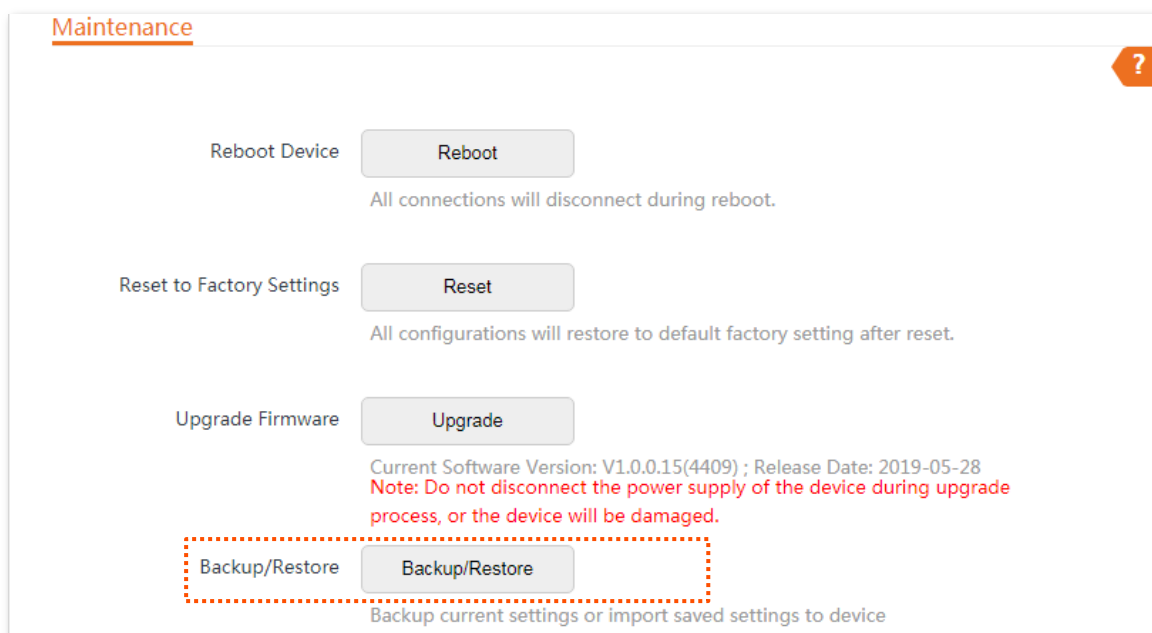
----End

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

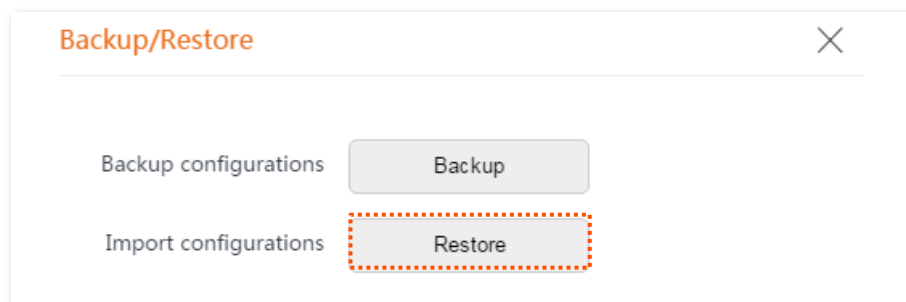
Import the configuration

Step 1 Choose **Tools > Maintenance** to enter the configuration page.

Step 2 Click **Backup/Restore**.



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



Step 4 Select and upload the file you back up before (the suffix of the backup file: .cfg).

----End


After the file is uploaded, the CPE reboots automatically.

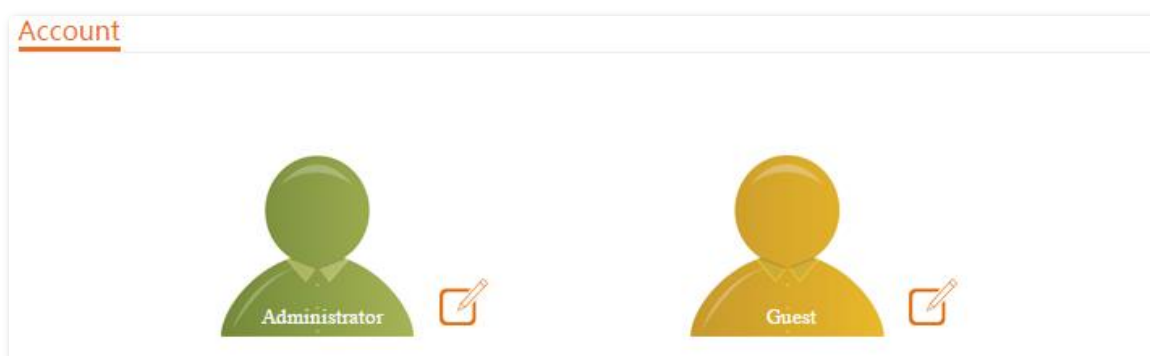
Wait for the progress bar to complete. Then the CPE is restored to the settings successfully.

9.3 Account

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

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

Click  to change the account information.

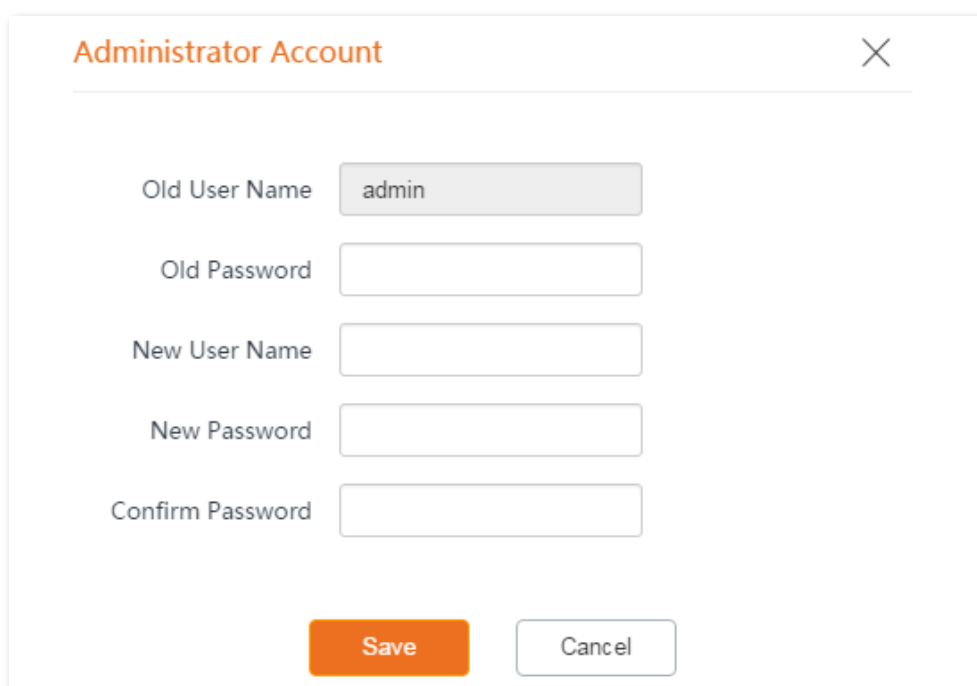


9.3.1 Administrator

You can modify and view the settings with the administrator account. Both the default user name and password of the administrator account are **admin**.



For network security, it is recommended to modify your login password regularly. A password of high security is preferred, such as a combination of lower-case letters, capital letters and numbers.

The dialog box is titled "Administrator Account" and has a close button (X) in the top right corner. It contains five input fields: "Old User Name" (pre-filled with "admin"), "Old Password", "New User Name", "New Password", and "Confirm Password". At the bottom, there are two buttons: "Save" (orange) and "Cancel" (white with grey border).

Parameters description

Name	Description
	It specifies the user name/password of the current login account.
Old User Name/Old Password	By default, the CPE has one administrator account and one guest account. Administrator user name/password: admin/admin (all lowercase) Guest user name/password: user/user (all lowercase)
New User Name	It specifies a new login user name.
New Password	It specifies a new login password.
Confirm Password	Enter the new login password again.

9.3.2 Guest

This account only allows you to view the settings. By default, this account is disabled. Both the default user name and password are **user**.

Guest Account
✕

Enable

Old User Name

Old Password

New User Name

New Password

Confirm Password

9.4 System log

To access the page, choose **Tools > System Log**. The maximum of 300 items can be saved. After the total log items exceed the maximum number, the previous logs will be cleared.

The logs of the 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.

System Log ?

Log Type

ID	Time	Type	Log
1	2019-01-16 15:03:15	System	SNMP Stop
2	2019-01-16 15:03:04	System	web 192.168.2.11 login
3	2019-01-16 15:02:59	System	web login time expired

To ensure that the logs are recorded correctly, verify the system time of the CPE. You can correct the system time of the CPE by choosing **Tools > Date & Time**.

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

NOTE

- When the device reboots, the previous logs are lost.
- The device reboots when one of the following situations occurs: the device is powered on after a power failure, the VLAN function is configured, the firmware is upgraded, the configuration of the device is backed up or restored or the factory settings are restored.

Appendix

A.1 Default parameters

The main default parameters are shown in the following table.

Parameters	Default settings		
Login	Login IP Address	192.168.2.1	
	Administrator	User name	admin
		Password	admin
	Guest	Disable	
Quick Setup	Working Mode	AP mode	
LAN Setup	IP Address Type	Static IP address	
	IP Address	192.168.2.1	
	Subnet Mask	255.255.255.0	
DHCP Server	DHCP Server	Enable	
	Start IP Address	192.168.2.100	
	End IP Address	192.168.2.200	
	Subnet Mask	255.255.255.0	
	Gateway Address	192.168.2.254	
	Primary DNS Server	8.8.8.8	
	Lease Time	1 day	
VLAN Settings	VLAN Settings	Disable	
	PVID	1	
	Management VLAN	1	
	WLAN	1000	
Wireless	Wireless Network	Enable	
	SSID	Tenda_XXXXXX, and XXXXXX is the last six characters of the LAN MAC address of the device	
	Security Mode	None	
	Transparent Bridge	Enable	
	TD-MAX	Disable	

Parameters	Default settings	
	TPC	Enable
	Signal LED1 Threshold	-90 dBm
	Signal LED2 Threshold	-80 dBm
	Signal LED3 Threshold	-70 dBm
Network Service	Login Timeout Interval	5 min
	Ping Watch Dog	Disable
	Telnet Service	Enable
	UPnP	Disable
	Hardware Watch Dog	Enable
	STP	Disable
Tools	Date & Time	Synchronized with the Internet


A.2 Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AP	Access Point
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
AES	Advanced Encryption Standard
CAT5e	Category 5 Enhanced
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CCQ	Client Connection Quality
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DDNS	Dynamic Domain Name Server
DTIM	Delivery Traffic Indication Map
DMZ	Demilitarized Zone
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISP	Internet Service Provider
ICMP	Internet Control Message Protocol
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
P2MP	Point-to-Multi-Point
PVID	Port-based VLAN ID
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RSSI	Received Signal Strength Indicator

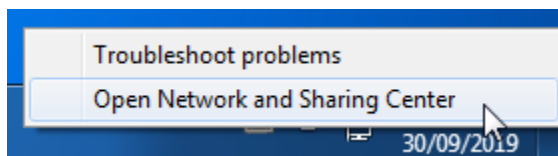
Acronym or Abbreviation	Full Spelling
RTS	Request to Send
RX	Receive
SSID	Service Set Identifier
STP	Spanning Tree Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TPC	Transmit Power Control
TKIP	Temporal Key Integrity Protocol
TX	Transmit
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
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 Networks
WMM	Wi-Fi Multi-Media
WPA-PSK	WPA-Preshared Key
WPA	Wi-Fi Protected Access

A.3 How to assign a fixed IP address to your computer

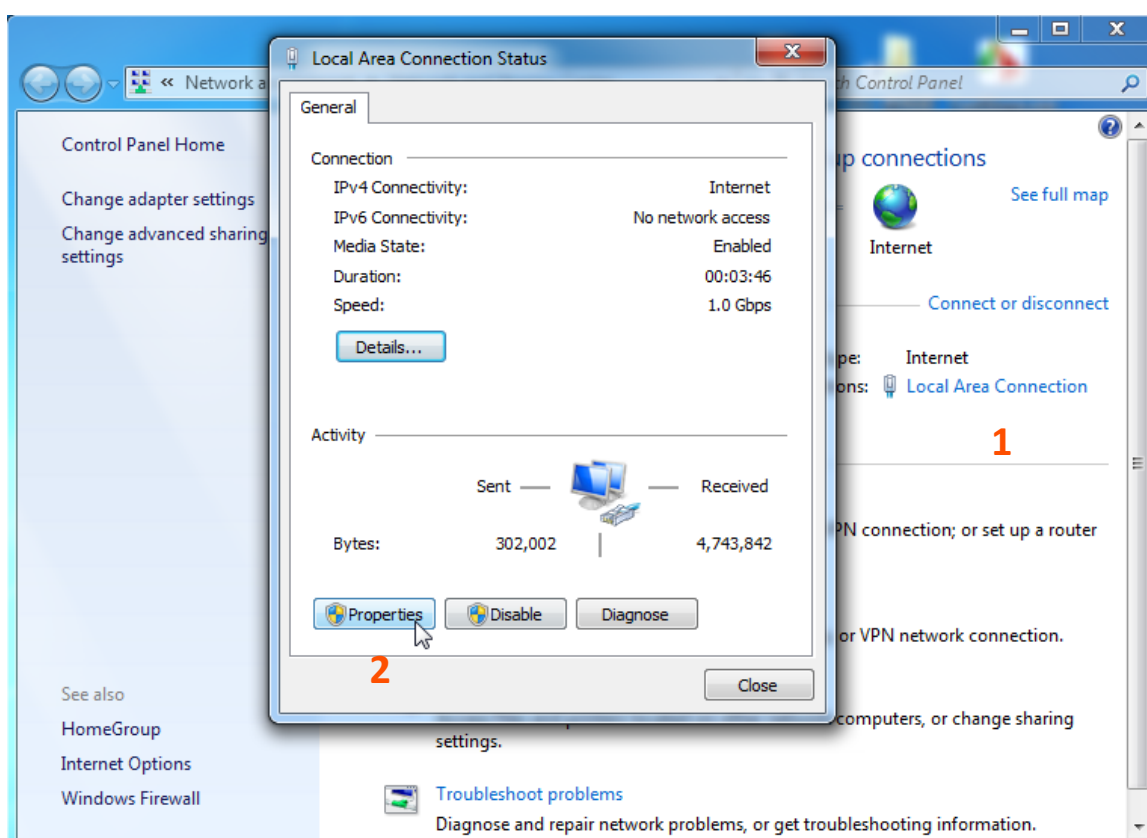
OS example: Windows 7

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

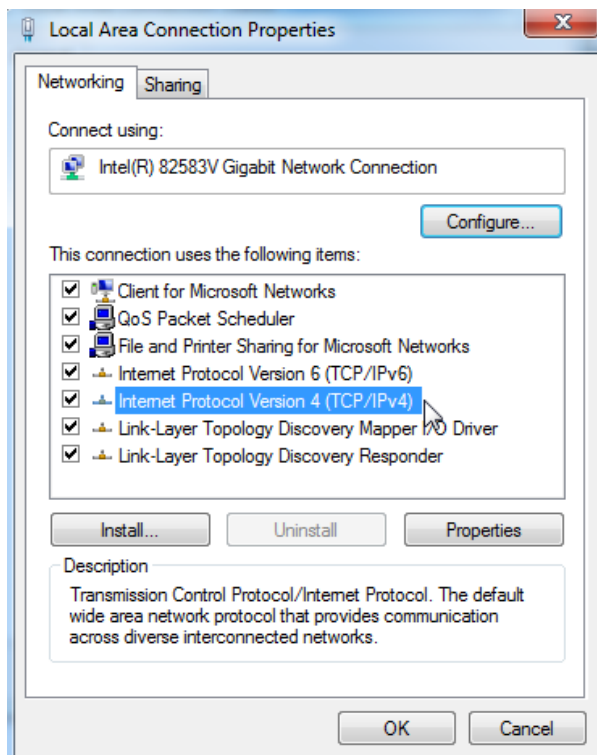
Step 2 Click **Open Network and Sharing Center**.



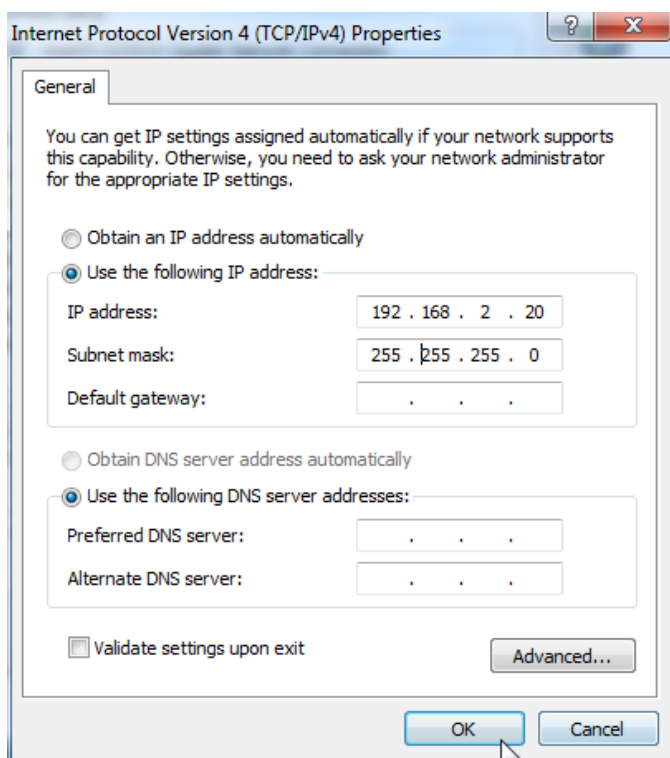
Step 3 Click **Local Area Connection**, then click **Properties**.



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



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




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

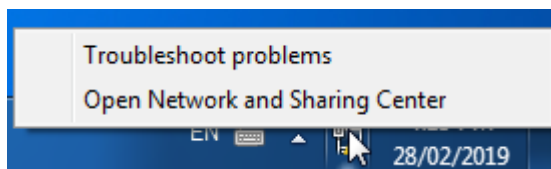
----End

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

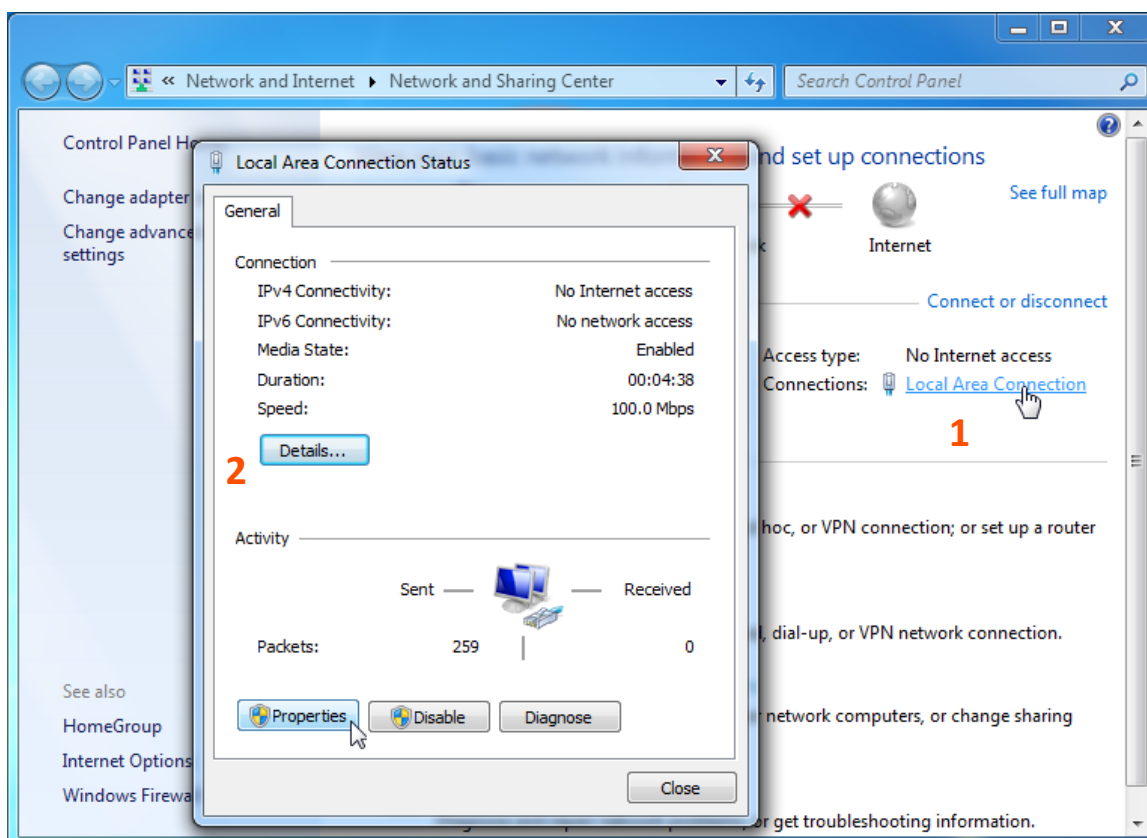
OS example: Windows 7

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

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



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



----End

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

