



User Guide

Outdoor CPE

This guide is for reference only and does not imply that the product supports all functions in the guide. Functions may vary with the product model and product version. The actual product

Copyright statement

Copyright ©2024 IP-COM Networks Co., Ltd. All rights reserved.

IP-COM is the registered trademark of IP-COM Networks 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 IP-COM Networks 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 IP-COM Networks Co., Ltd.

Disclaimer

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

Preface

Thank you for choosing IP-COM. This user guide is a complement to Quick Installation Guide. Quick Installation Guide provides instructions for quick internet setup, while this user guide contains details of each function and demonstrates how to configure them.

This user guide applies to IP-COM CPEs. CPE13V2.0 working in AP mode is used for illustrations here unless otherwise specified.

This user guide is for configuration reference only and does indicate that the product supports all functions described here. Functions available may vary with the product model and product version. Please refer to the actual product.



The UI screenshots, IP addresses and other data are for illustrative purposes only and do not affect your configuration. Functions or parameters grayed out on the UI indicate that they are unavailable or cannot be modified on the product.

Conventions

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

Item	Presentation	Example
Cascading menus	>	Choose System > Live Users .
Parameter and value	Bold	Set User Name to Tom .
Variable	Italic	Format: <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
 Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to the device.
 Tip	This format is used to highlight a procedure that will save time or resources.

For more documents

Go to our website at www.ip-com.com.cn and search for the latest documents for your product.

Technical support

Contact us if you need more help. We will be glad to assist you as soon as possible.

Email address: info@ip-com.com.cn

Website: www.ip-com.com.cn

Revision history

IP-COM is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the user guide was released.

Version	Description	Date
V2.0	Modified the description of Typical applications , Login , Quick setup , and VLAN settings .	2024-07-31
V1.0	Original publication	2024-03-29

Contents

1 Typical applications	1
1.1 CCTV surveillance	1
1.1.1 Solution.....	1
1.1.2 Configure the CPEs	2
1.1.3 Install the CPEs	7
1.2 ISP hotspot connection	9
1.2.1 Solution.....	9
1.2.2 Configure the CPE.....	9
2 Login and logout.....	13
2.1 Login	13
2.1.1 Login with computer	13
2.1.2 Login with smartphone or tablet.....	15
2.2 Logout.....	17
3 Web UI.....	18
3.1 Web UI layout	18
3.2 Common buttons.....	19
4 Quick setup	20
4.1 AP mode	21
4.1.1 Overview.....	21
4.1.2 Set AP mode	22
4.2 Client mode	24
4.2.1 Overview.....	24
4.2.2 Set Client mode	24
4.3 Universal Repeater mode	28
4.3.1 Overview.....	28
4.3.2 Set Universal Repeater mode	28
4.4 WISP mode	32
4.4.1 Overview.....	32
4.4.2 Set WISP mode	32
4.5 Router mode.....	38
4.5.1 Overview.....	38

4.5.2 Set Router mode.....	38
5 Status.....	43
5.1 System status.....	43
5.2 Wireless status.....	46
5.2.1 View operating RF status.....	46
5.2.2 View management RF status.....	48
5.3 Statistics.....	49
5.3.1 Throughput.....	49
5.3.2 Wireless client.....	50
5.3.3 Upstream AP.....	51
5.3.4 Interface.....	52
5.3.5 ARP table.....	53
5.3.6 Routing table.....	54
6 Network.....	55
6.1 LAN setup.....	55
6.1.1 Overview.....	55
6.1.2 Modify LAN IP address.....	57
6.2 Packet filter.....	60
6.3 MAC clone.....	62
6.3.1 Overview.....	62
6.3.2 Clone a MAC address.....	62
6.4 DHCP server.....	64
6.4.1 Overview.....	64
6.4.2 Configure the DHCP server.....	64
6.5 DHCP client.....	66
6.6 VLAN settings.....	67
6.6.1 Overview.....	67
6.6.2 Configure VLAN (Example: CPE6SV2.0).....	67
6.6.3 Example of configuring VLAN on CPE13.....	68
7 Wireless settings.....	71
7.1 Basic configuration.....	71
7.1.1 Overview.....	71
7.1.2 Basic wireless settings.....	73
7.1.3 Set up a non-encrypted wireless network.....	81
7.1.4 Set up a wireless network encrypted using WPA2-PSK.....	83
7.1.5 Set up a wireless network encrypted using WPA or WPA2.....	85
7.2 Advanced settings.....	102
7.3 Access control.....	106
7.3.1 Overview.....	106

7.3.2 Configure access control.....	106
7.3.3 Example of configuring access control	107
7.4 Management RF	109
7.4.1 Overview.....	109
7.4.2 Extend management WiFi duration	110
8 Advanced	112
8.1 LAN rate	112
8.2 Diagnose	114
8.2.1 Site survey	114
8.2.2 Ping	115
8.2.3 Traceroute.....	116
8.2.4 Speed test	117
8.2.5 Spectrum analysis.....	120
8.3 Bandwidth control	123
8.3.1 Overview.....	123
8.3.2 Example of configuring bandwidth control	124
8.4 Port forwarding.....	125
8.4.1 Overview.....	125
8.4.2 Example of configuring port forwarding	126
8.5 MAC filter.....	129
8.5.1 Overview.....	129
8.5.2 Example of configuring MAC filter.....	130
8.6 Network service.....	132
8.6.1 DDNS.....	132
8.6.2 Remote web management	136
8.6.3 Reboot schedule	138
8.6.4 Login timeout interval	138
8.6.5 SNMP agent	139
8.6.6 Ping watch dog	143
8.6.7 DMZ host	144
8.6.8 Telnet service.....	147
8.6.9 UPnP	147
8.6.10 Hardware watch dog	147
9 Tools	148
9.1 Date & time	148
9.1.1 Sync system time with internet	148
9.1.2 Set system time manually.....	149
9.2 Maintenance.....	151
9.2.1 Reboot device.....	151

9.2.2 Restore to factory settings.....	152
9.2.3 Upgrade firmware	153
9.2.4 Backup/Restore	154
9.3 Account.....	156
9.3.1 Administrator.....	156
9.3.2 Guest.....	157
9.4 System log.....	158
Appendix	159

1 Typical applications



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

1.1 CCTV surveillance

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

1.1.1 Solution

- **Method 1:** Use the CPE kit to set up a monitoring network, such as CPE6S. You only need to [install the CPEs](#) to easily manage the CCTV surveillance for the community.
- **Method 2:** Use two CPEs to set up a monitoring network, such as CPE13. You only need to [Configure the CPEs](#) > [Install the CPEs](#) to easily manage the CCTV surveillance for the community.



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

1.1.2 Configure the CPEs

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



Note

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

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

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



Tip

- If the CPE supports DC power supply, you can use the correct power adapter to power on the CPE. The power parameters can be checked on the DC power jack. If the power adapter (5.5×2.1 mm) is not included in the product package, you can purchase it by yourself.
- Some CPEs can be powered on by IEEE 802.3af PoE power supply devices. For more details, visit www.ip-com.com.cn to search for the specific product model, and check the relevant information on the **Specification** page.
- The maximum PoE power supply distance supported by each CPE is different. For more details, visit www.ip-com.com.cn to search for the specific product model, enter the **Download** page, and download the datasheet to check the maximum PoE power supply distance.

----End

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



Tip

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

Option 2: Manual bridging

1. Place the two CPEs next to each other.
2. Power on the CPE1.

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



- If the CPE supports DC power supply, you can use the correct power adapter to power on the CPE. The power parameters can be checked on the DC power jack. If the power adapter (5.5×2.1 mm) is not included in the product package, you can purchase it by yourself.
- Some CPEs can be powered on by IEEE 802.3af PoE power supply devices. For more details, visit www.ip-com.com.cn to search for the specific product model, and check the relevant information on the **Specification** page.
- The maximum PoE power supply distance supported by each CPE is different. For more details, visit www.ip-com.com.cn to search for the specific product model, enter the **Download** page, and download the datasheet to check the maximum PoE power supply distance.

3. [Log in to the web UI](#) of CPE1.
4. Set CPE1 to AP mode.
 - 1) Navigate to **Quick Setup**. Select **AP** mode, and click **Next**.

Quick Setup Current Mode: AP

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

Next

- 2) Set wireless network parameters and click **Next**.
 - Set an **SSID** (WiFi name), which is **IP-COM_1** in this example.
 - Set **Security Mode**, which is **WPA2-PSK** in this example.
 - Set **Encryption Algorithm**, which is **AES** in this example.
 - Set **Key**.

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

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

Quick Setup >> AP ?

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

5. [Log in to the web UI](#) of CPE2 and set it to Client mode.

- 1) Refer to step [2](#) to log in to the web UI of CPE2.
- 2) Navigate to **Quick Setup**. Select **Client** mode, and click **Next**.

Quick Setup Current Mode: AP ?

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.

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

- 3) Select the wireless network to bridge from the list, which is **IP-COM_1** in this example, and click **Next**.



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

Quick Setup >> Client Current Mode: AP

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"/>	IP-COM_1			WPA2-PSK,AES	

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

Quick Setup >> Client Current Mode: AP

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

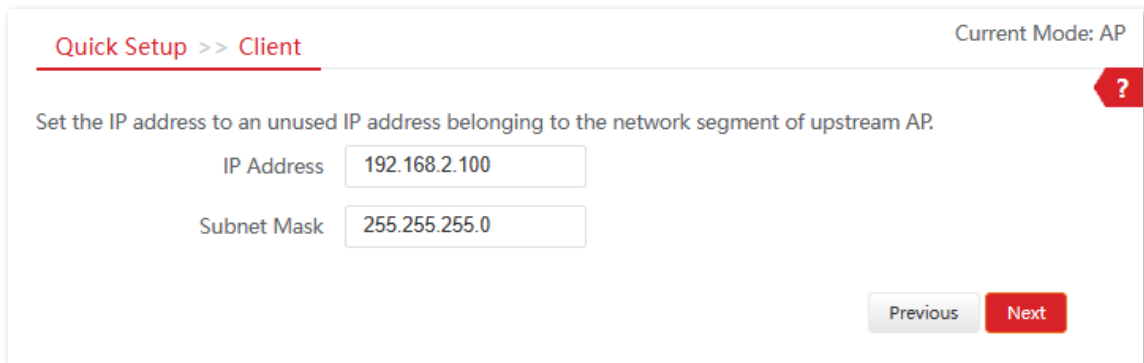
Security Mode

Encryption Algorithm AES TKIP TKIP&AES

Key

- 5) Set the IP address of this CPE to an unused IP address belonging to the same network segment as that of the first CPE. Then set the subnet mask to the same one used by the first CPE, and click **Next**.

In this example, **IP Address** is set to **192.168.2.100** and **Subnet Mask** is set to **255.255.255.0**.



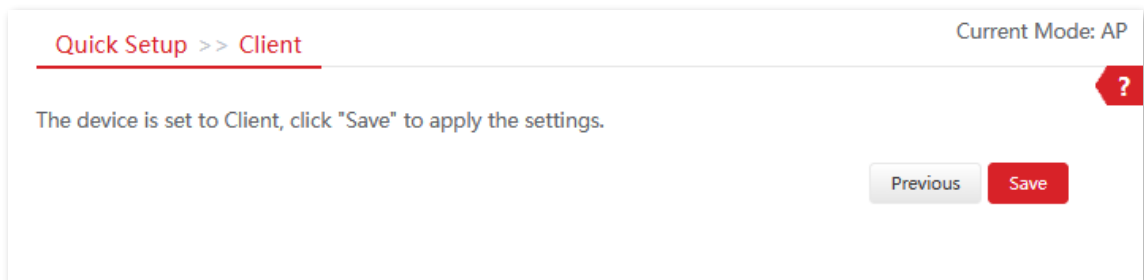
Quick Setup >> Client Current Mode: AP

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 make the settings take effect.



Quick Setup >> Client Current Mode: AP

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

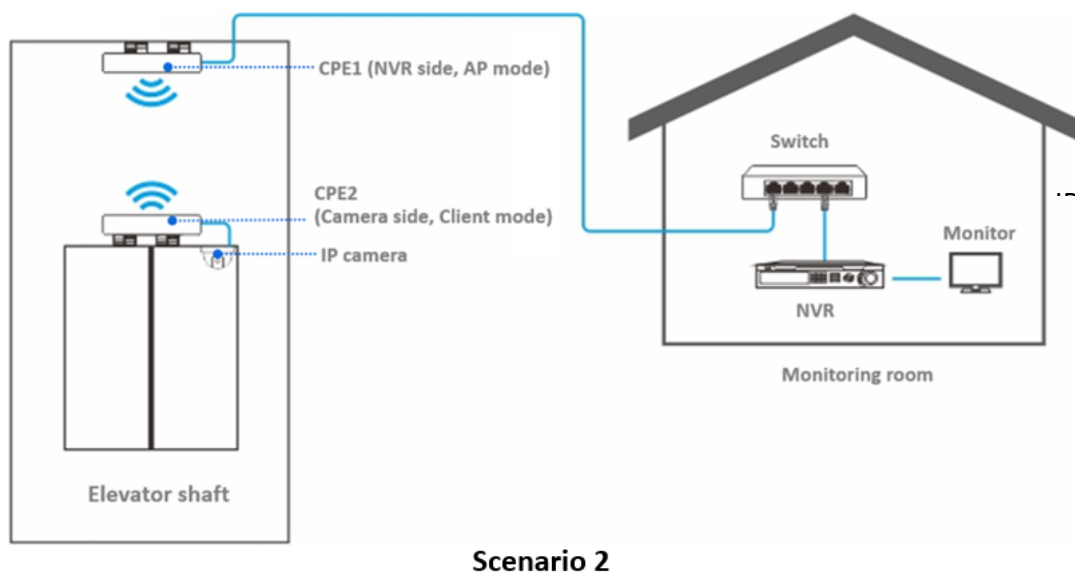
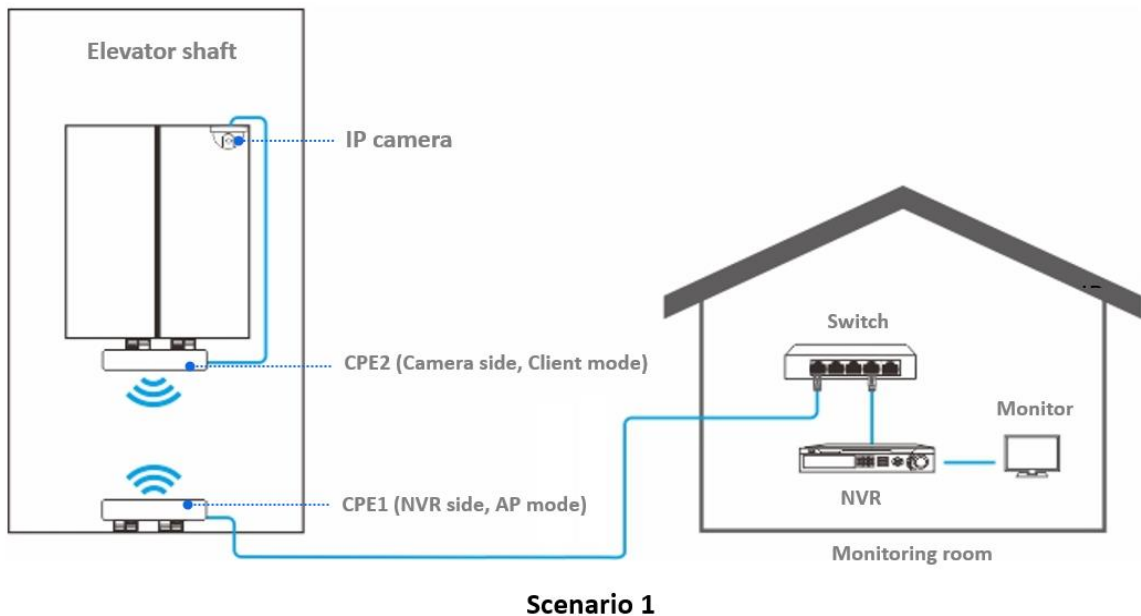
----End

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

1.1.3 Install the CPEs


Select any of the following scenarios according to the location of the monitoring room and install the CPE to the corresponding location.

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



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.

CPE13 is used for illustration here. Below describes the signal indicators.

Indicator	Status	Description
LED1, LED2, LED3 (signal indicators)	Solid on/Blinking	<p>The CPE is connected to the device.</p> <ul style="list-style-type: none"> - Solid on: The CPE may work in AP or Router mode. - Blinking: The CPE may work in Client, Universal Repeater or WISP mode. <p>The more LED indicator are on, the stronger the received signal is, and the better the connection quality is.</p> <p> Tip</p> <ul style="list-style-type: none"> - You can make changes on the Wireless > Advanced page of the web UI of the CPE. - Different models of CPEs have different LED indicators and working modes. The actual product prevails.
	Off	<p>No device is connected to the CPE, or the received signal strength is less than the RSSI threshold (default: -90 dBm).</p>

1.2 ISP hotspot connection

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

1.2.1 Solution

CPE12V3.0 is used as an example to illustrate the installation procedures. Procedures for other CPEs are similar.



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

1.2.2 Configure the CPE

1. Power on the CPE.

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



- If the CPE supports DC power supply, you can use the correct power adapter to power on the CPE. The power parameters can be checked on the DC power jack. If the power adapter (5.5×2.1 mm) is not included in the product package, you can purchase it by yourself.
 - Some CPEs can be powered on by IEEE 802.3af PoE power supply devices. For more details, visit www.ip-com.com.cn to search for the specific product model, and check the relevant information on the **Specification** page.
 - The maximum PoE power supply distance supported by each CPE is different. For more details, visit www.ip-com.com.cn to search for the specific product model, enter the **Download** page, and download the datasheet to check the maximum PoE power supply distance.
-

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

3. Set the CPE to WISP mode.

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

Quick Setup Current Mode: AP

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.

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

Next

- 2) Select the wireless network of your ISP hotspot, which is **IP-COM_ERIC** 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"/>	IP-COM_ERIC			WPA-PSK,AES	

- 3) Enter the WiFi password of your ISP hotspot in the **Key** field, 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

Previous **Next**

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

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

- 5) 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

- 6) Set an IP address that belongs to a subnet different from 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**.

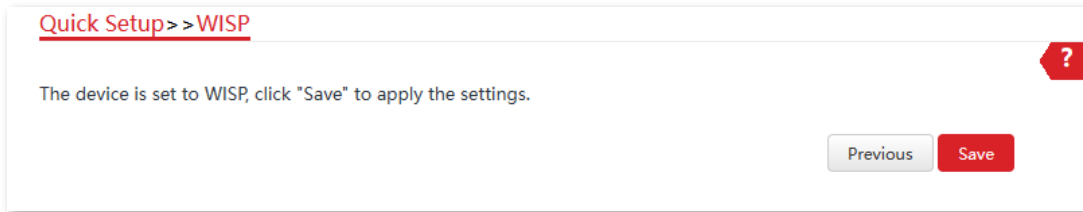
Quick Setup > > WISP ?

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

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



----End

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

2 Login and logout

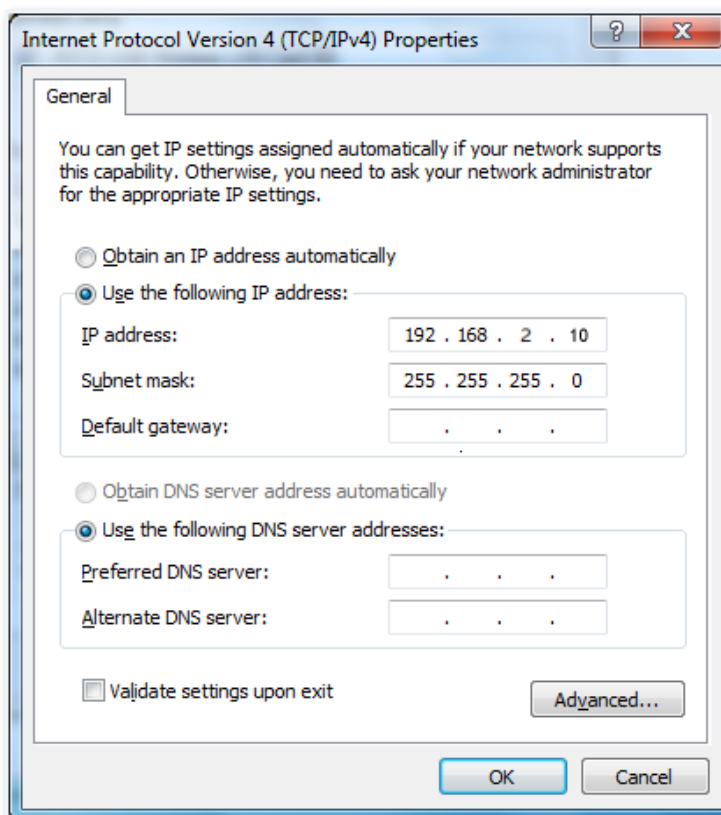
2.1 Login

For a single-unit CPE, DHCP server is enabled by default. When a single-unit CPE is bridged successfully, DHCP server is automatically disabled. For a kit-unit CPE, DHCP server is disabled by default.

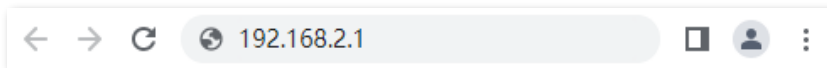
2.1.1 Login with computer

1. Connect the computer to the CPE or the switch connected to the CPE.
2. Set the IP address of the computer to an unused one within the same subnet as the CPE. (If the DHCP of the CPE is enabled, skip this step.)

For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied), and the subnet mask to 255.255.255.0. The following figure is for reference only.



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



4. Enter your user name and password, and click **Login**.

A screenshot of the login page for a device labeled "CPE12V3.0". The page has a white background with a grey header bar containing the text "CPE12V3.0" in red. Below the header, there are three input fields: the first is for the username, labeled "Default user name: admin"; the second is for the password, labeled "Default password: admin", with a toggle icon for visibility; the third is a dropdown menu for language, currently set to "English". Below these fields is a prominent red "Login" button. Underneath the button is a red link that says "Forget password?".

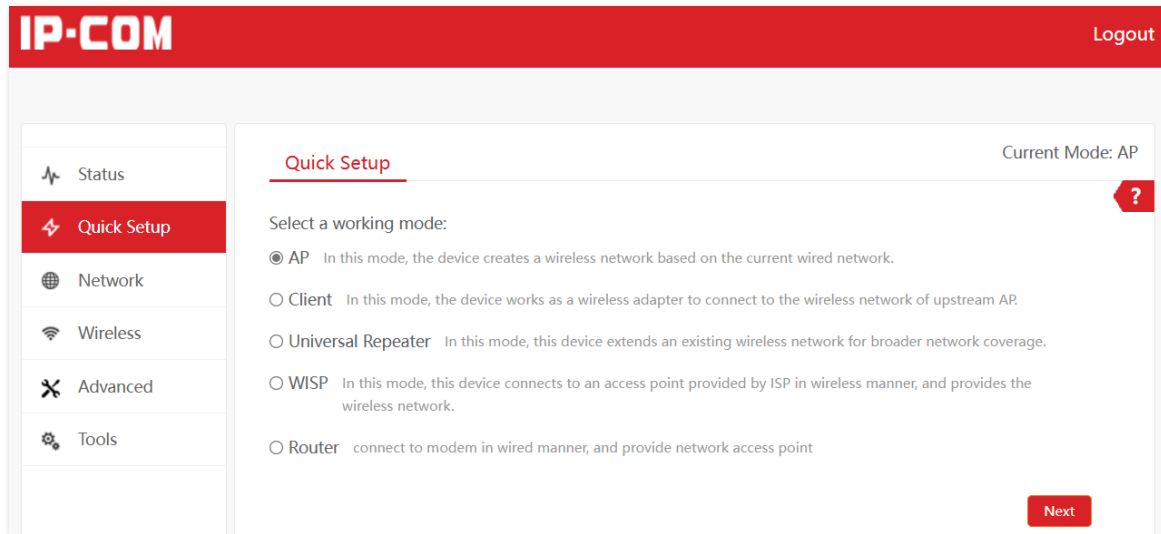
Tip

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

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE properly.
- Ensure that the IP address of the computer is on the same subnet as the CPE. For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied).
- If more than one CPE is connected, modify the IP address of each one to avoid the login failure due to IP address conflict.
- Reset the CPE to factory settings and try again. To reset the CPE, hold down the reset button (such as RST, RESET or Reset) for about 8 seconds, and then release it when all the LED indicators light up.
- The default login user name and password of the CPE are **admin**. For network security, refer to the [Account](#) and change the login user name and password.

----End

After the successful login, the following page appears.



2.1.2 Login with smartphone or tablet

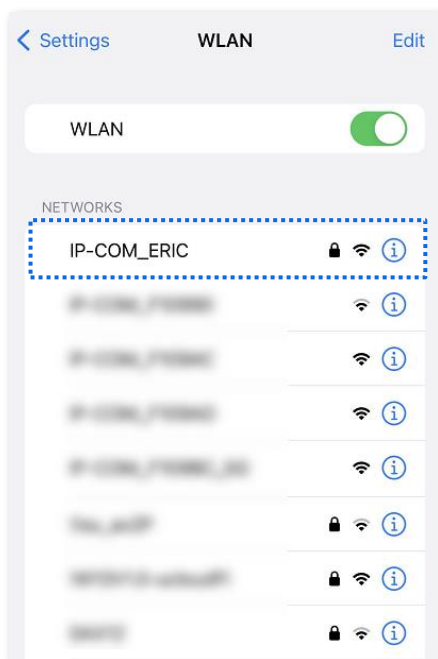
When logging in to a client-mode CPE, ensure that management RF is supported and enabled. Take iPhone as an example.

1. Connect the smartphone to the WiFi you set for the CPE, which is **IP-COM_ERIC** in this example.



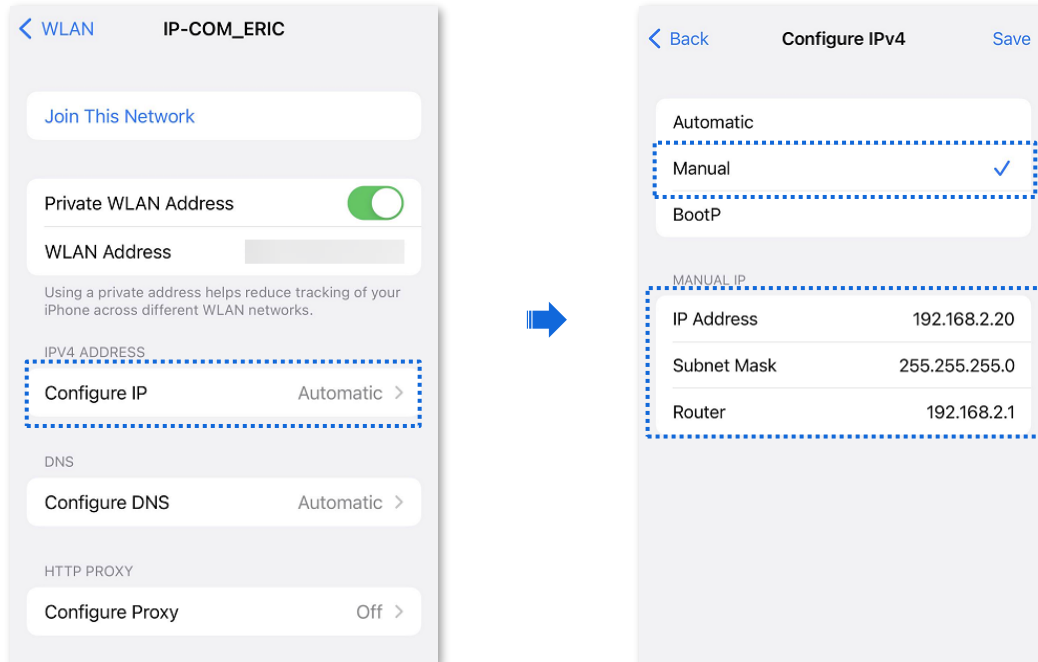
Tip

The default WiFi name is IP-COM_XXXXXX or IP-COM_XXXXXX_MG (XXXXXX indicates the last six digits of the CPE MAC address). If you cannot find the WiFi network, reboot the CPE and try again.

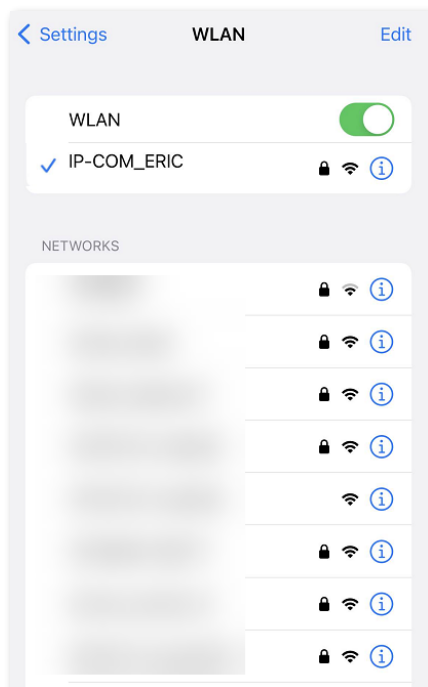


- Set the IP address of the smartphone to an unused one within the same subnet as the CPE. (If the DHCP of the CPE is enabled, skip this step.)

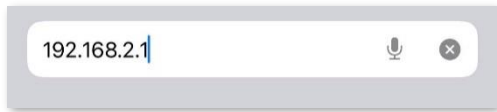
For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied), and the subnet mask to 255.255.255.0.



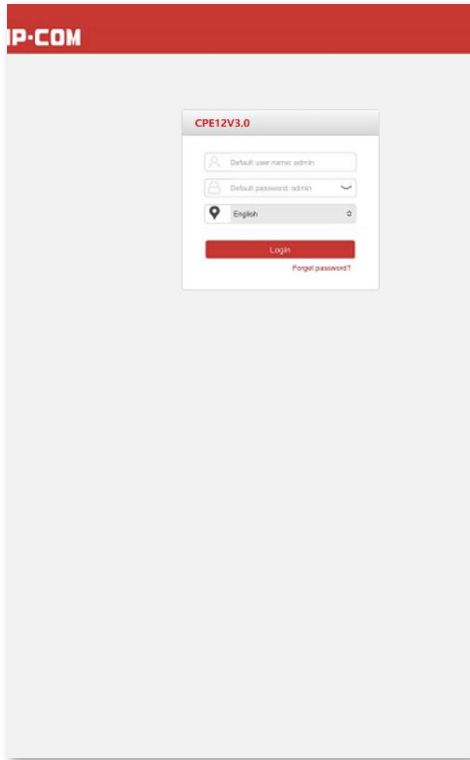
- Connect to the CPE's WiFi successfully.



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



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



----End

2.2 Logout

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

3 Web UI

3.1 Web UI layout

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

The screenshot shows the 'LAN Setup' configuration page. On the left is a navigation menu with items: Status, Quick Setup, Network (1), LAN Setup (2), DHCP Server, DHCP Client, VLAN Settings, Wireless, Advanced, and Tools. The main content area is titled 'LAN Setup' (3) and shows configuration fields: MAC Address (D8:38:0D:23:9D:A0), IP Address Type (Static IP Address), IP Address (192.168.2.2), Subnet Mask (255.255.255.0) (4), Default Gateway (0.0.0.0), Primary DNS Server (0.0.0.0), Secondary DNS Server (0.0.0.0), and Device Name (CPE12V3.0). At the bottom are 'Save' and 'Cancel' buttons. The top right indicates 'Current Mode: AP'.





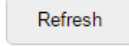

Tip

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

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

3.2 Common buttons

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

Button	Description
	Used to save the configuration on the current page and enable the configuration to take effect.
	Used to go back to the original configuration without saving the configuration on the current page.
	Used to update the content on the current page.
	Used to view help information for the settings on the current page.

4 Quick setup

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and product version. Please refer to the actual product.



In a CPE kit, the two CPEs are pre-configured and can be installed directly.

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

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

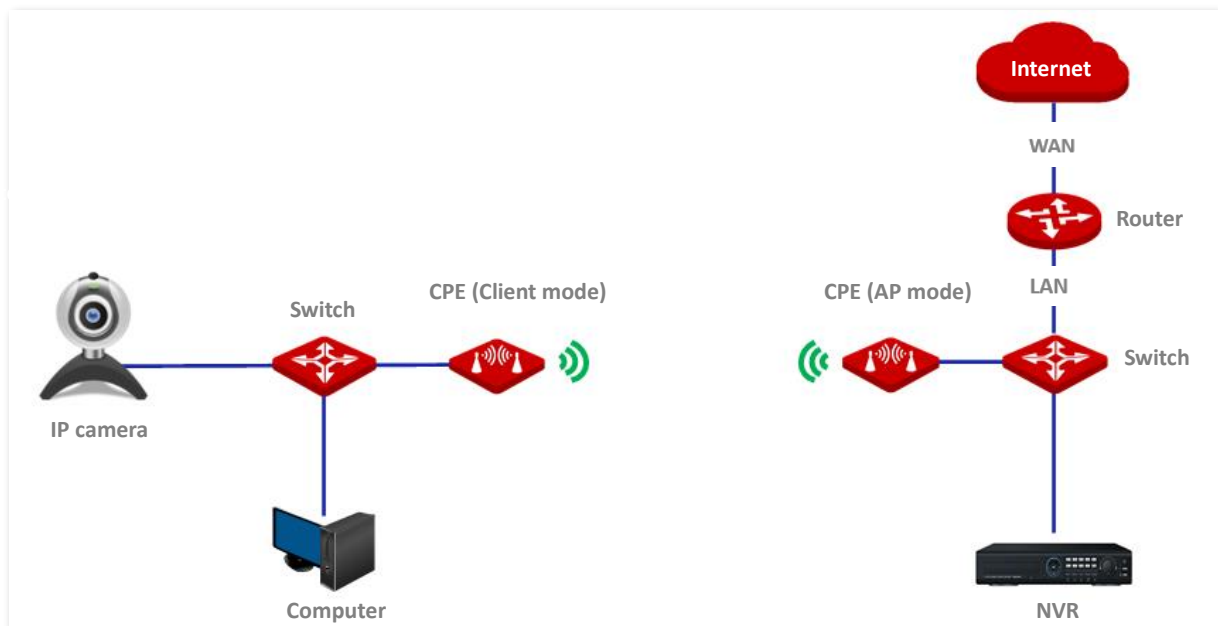
- [AP](#): In this mode, the CPE converts a wired network into a wireless one.
- [Client](#): In this mode, the CPE works as a wireless adapter that can connect to other wireless networks. The CPE's operating RF does not provide wireless connection, so client devices need to be connected with an Ethernet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

4.1 AP mode

4.1.1 Overview

In AP mode, the CPE converts a wired network into a wireless one by connecting to the internet through an Ethernet cable.

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



4.1.2 Set AP mode

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

The screenshot shows the 'Quick Setup' page with the current mode set to 'AP'. The page title is 'Quick Setup' and the current mode is 'AP'. There is a red question mark icon in the top right corner. The main content area says 'Select a working mode:' and lists five options with radio buttons:

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

 A red 'Next' button is located at the bottom right of the form.

3. Specify wireless network parameters and click **Next**.
 - Set **SSID**, which is **IP-COM_1** in this example.
 - Set **Channel**, which is **Auto** in this example.
 - Set **Security Mode**, which is **WPA2-PSK** in this example.
 - Set **Encryption Algorithm**, which is **AES** in this example.
 - Set **Key**, which is **UmXmL9UK** in this example.

The screenshot shows the 'Quick Setup >> AP' page. The page title is 'Quick Setup >> AP' and there is a red question mark icon in the top right corner. The main content area says 'You can set up your wireless network name and wireless password here. Note down your wireless password.' and lists the following parameters:

- *SSID: IP-COM_1
- Channel: Auto
- *Security Mode: WPA2-PSK
- *Encryption Algorithm: AES TKIP TKIP&AES
- *Key:

 At the bottom right, there are 'Previous' and 'Next' buttons.

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

The screenshot shows the 'Quick Setup >> AP' page. The page title is 'Quick Setup >> AP' and there is a red question mark icon in the top right corner. The main content area says 'The device is set to AP, click "Save" to apply the settings.' At the bottom right, there are 'Previous' and 'Save' buttons.

----End

Parameters description

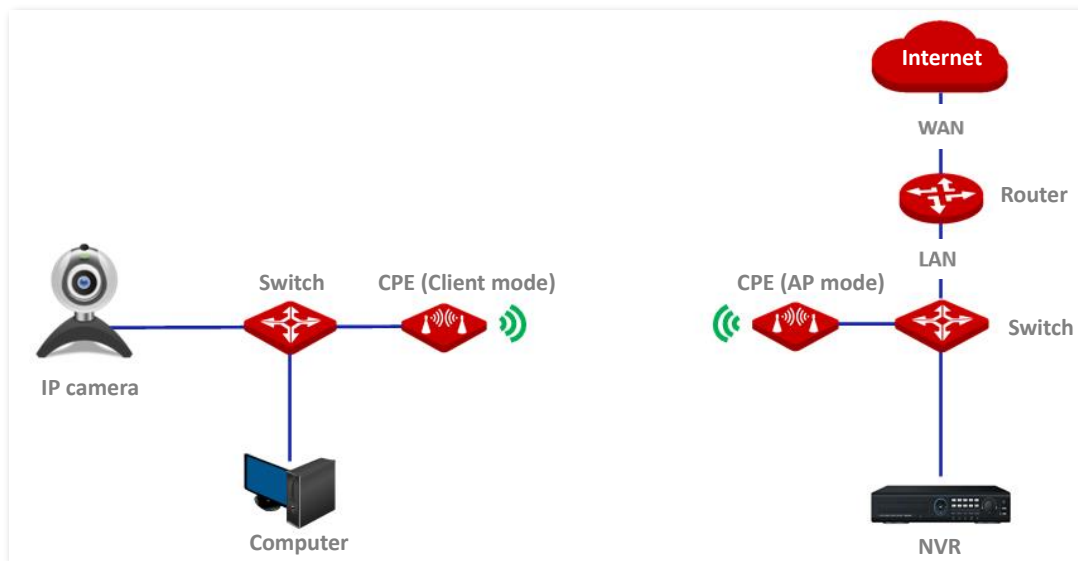
Name	Description
SSID	Specifies the WiFi name of the CPE.
Channel	<p>Specifies the operating channel of the CPE. To reduce interference, it is recommended to use the least used channel in the current area.</p> <p>Auto indicates that the CPE automatically adjusts its operating channel according to the ambient environment.</p>
Channel Bandwidth	<p>Specifies the bandwidth of the operating channel. Take CPE5 as an example.</p> <p>Auto indicates that the CPE automatically adjusts its operating channel according to the ambient environment.</p> <p>With high channel bandwidth, it is easier to obtain a higher transmission rate, but the penetration is slightly worse and the transmission distance is short. If there is no special need, it is recommended to keep the default setting.</p>
Security Mode	<p>Specifies the security mode of the wireless network.</p> <p>For more details, see Security Mode.</p>
Encryption Algorithm	<p>Specifies the encryption method of the wireless network.</p> <ul style="list-style-type: none"> – AES: Indicates the Advanced Encryption Standard. – TKIP: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. – TKIP&AES: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	Specifies the WiFi password of the wireless network.

4.2 Client mode

4.2.1 Overview

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

The CPE in Client mode usually works with the CPE in [AP mode](#) to establish a video surveillance network. The network topology is shown as below.



4.2.2 Set Client mode

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

Quick Setup
Current Mode: AP

?

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.

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

3. Select the wireless network to bridge from the list, which is **IP-COM_1** in this example, and click **Next**.



Tip

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

Quick Setup >> Client Current Mode: AP

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"/>	IP-COM_1			WPA-PSK,AES	

4. Enter the WiFi password for the selected wireless network **IP-COM_1** in the **Key** field, and click **Next**.

Quick Setup >> Client Current Mode: AP

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	Specifies the WiFi name (SSID) of the wireless network to be bridged.
Upstream AP MAC Address	Specifies the MAC address of the wireless network to be bridged.
Channel	Specifies the operating channel of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	Specifies the security mode of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. If the wireless network to be bridged has a WiFi password, you need to enter the password manually.
Encryption Algorithm	<p>Specifies the encryption method of the wireless network.</p> <ul style="list-style-type: none"> - AES: Indicates the Advanced Encryption Standard. - TKIP: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. - TKIP&AES: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	Specifies the WiFi password of the wireless network.

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

- For **IP Address**, enter an unused IP address that belongs to the same subnet as the peer CPE.
- For **Subnet Mask**, enter the subnet mask of the peer CPE.

Here, the IP address of the peer CPE is 192.168.2.1 and the subnet mask is 255.255.255.0. So this CPE's IP address can be set to **192.168.2.10** and its subnet mask is set to **255.255.255.0**.

Current Mode: AP

[Quick Setup >> Client](#)

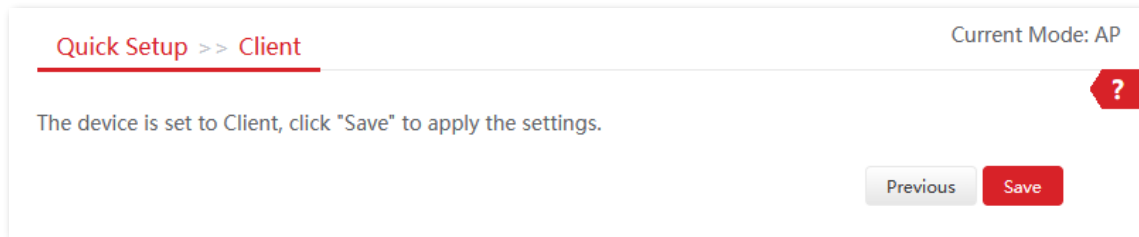
?

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 make the settings take effect.



----End

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

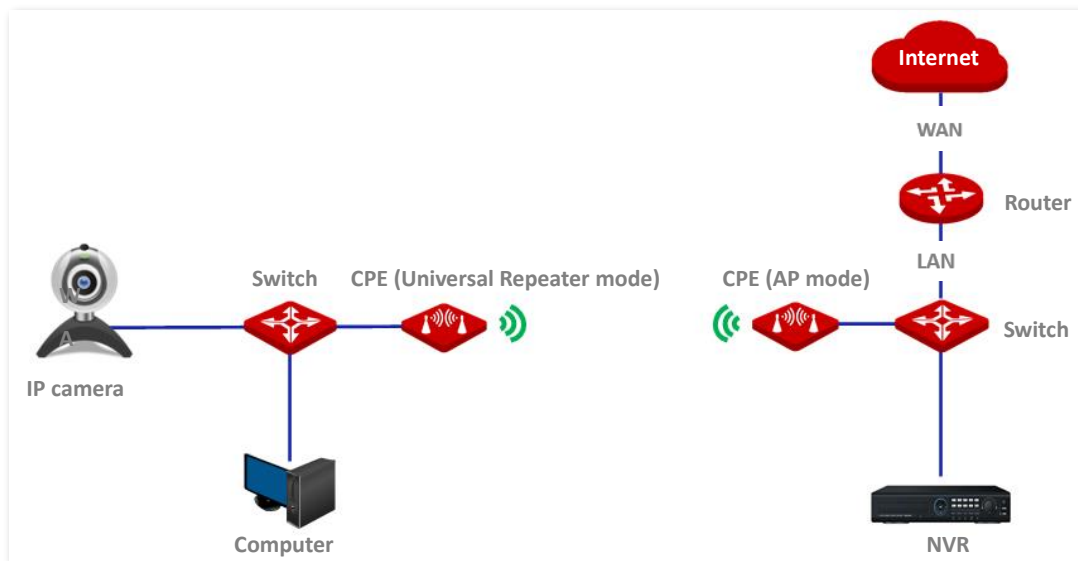
- [Log in to the web UI](#) of the CPE and navigate to **Status**.
- On the **Wireless Status** module, ensure that **Working Mode** is set to Client mode and **AP's MAC Address** changes to the peer CPE's WLAN MAC address.

4.3 Universal Repeater mode

4.3.1 Overview

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

The CPE in Universal Repeater mode usually works with the CPE in [AP mode](#) to establish a video surveillance network. The network topology is shown as below.



4.3.2 Set Universal Repeater mode

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Quick Setup**. Select **Universal Repeater** mode, and click **Next**.

Quick Setup
Current Mode: AP

?

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.

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

3. Select the wireless network to bridge from the list, which is **IP-COM_1** in this example, and click **Next**.

Quick Setup >> Universal Repeater Current Mode: Station

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"/>	IP-COM_1			WPA-PSK,AES	



Tip

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

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

Quick Setup >> Universal Repeater Current Mode: Station

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	Specifies the WiFi name (SSID) of the wireless network to be bridged.
Upstream AP MAC Address	Specifies the MAC address of the wireless network to be bridged.
Channel	Specifies the operating channel of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	Specifies the security mode of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. If the wireless network to be bridged is encrypted, you need to enter its WiFi password manually.
Encryption Algorithm	<p>Specifies the encryption method of the wireless network.</p> <ul style="list-style-type: none"> - AES: Indicates the Advanced Encryption Standard. - TKIP: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. - TKIP&AES: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	Specifies the WiFi password of the wireless network.

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

- For **IP Address**, enter an unused IP address that belongs to the same subnet as the peer CPE.
- For **Subnet Mask**, enter the subnet mask of the peer CPE.

Here, the IP address of the peer CPE is 192.168.2.1 and the subnet mask is 255.255.255.0. So this CPE's IP address can be set to **192.168.2.10** and its subnet mask is set to **255.255.255.0**.

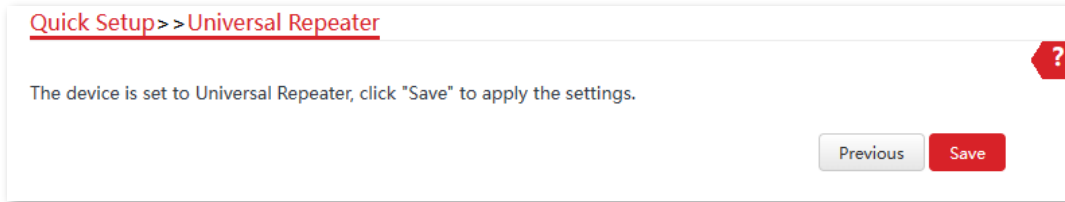
[Quick Setup](#) > > [Universal Repeater](#) ?

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

IP Address

Subnet Mask

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



----End

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

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



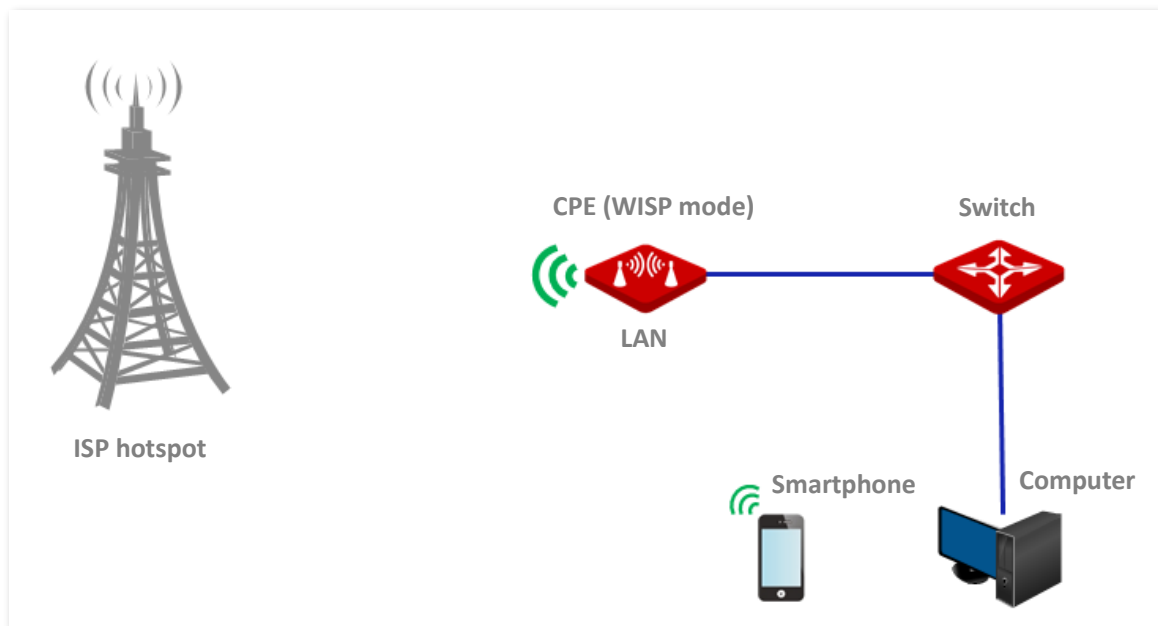
After the CPE is bridged, it uses the same key for the peer CPE.

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 WiFi-enabled devices to connect the CPE for internet access.

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



4.4.2 Set WISP mode

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

Quick Setup
Current Mode: AP

?

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

Next

3. Select the wireless network to bridge from the list, which is **IP-COM_1** in this example, and click **Next**.

Quick Setup >> WISP Current Mode: 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"/>	IP-COM_1			WPA2-PSK,AES	



Tip

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

- Enter the WiFi password of the upstream wireless network in the **Key** field, and click **Next**.

Quick Setup >> WISP Current Mode: 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	Specifies the WiFi name (SSID) of the wireless network to be bridged.
Upstream AP MAC Address	Specifies the MAC address of the wireless network to be bridged.
Channel	Specifies the operating channel of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge.

Name	Description
Security Mode	Specifies the security mode of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. If the wireless network to be bridged is encrypted, you need to enter the password manually.
Encryption Algorithm	<p>Specifies the encryption method of the wireless network.</p> <ul style="list-style-type: none"> - AES: Indicates the Advanced Encryption Standard. - TKIP: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. - TKIP&AES: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	Specifies the WiFi password of the wireless network.

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

Parameter description

Name	Description
Internet Connection Type	<p>Specifies the internet connection type.</p> <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. - 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. <p>The above required internet access parameters are provided by your ISP. If you are not sure, consult your ISP for help.</p>

6. Specify wireless network parameters and click **Next**.
 - Set **SSID** (WiFi name).
 - Set **Security Mode**, which is **WPA2-PSK** in this example
 - Set **Encryption Algorithm**, which is **AES** in this example.
 - Set **Key** (WiFi password).

Quick Setup >> WISP Current Mode: Universal Repeater

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

Quick Setup >> WISP Current Mode: Universal Repeater

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 make the settings take effect.

Quick Setup >> WISP Current Mode: Universal Repeater

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

----End

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

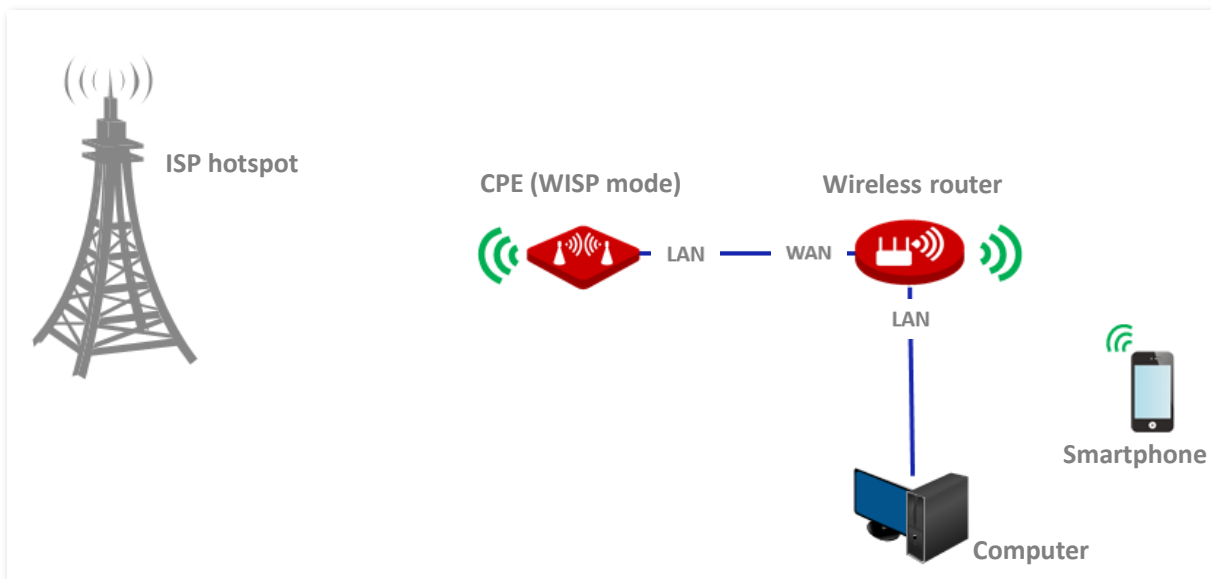
- [Log in to the web UI](#) of the CPE and navigate to **Status**.
- On the **System Status** module, ensure that the WAN IP address, default gateway and DNS server information obtained by the WAN port are displayed.
- On the **Wireless Status** module, ensure that **Working Mode** is set to WISP mode,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

After the successful configuration, devices connected to the CPE can access 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 network topology is shown as below.



Tip

WiFi name and WiFi password are **SSID** and **Key** set in step [6](#) above.



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

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

----End

To access the internet with:

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



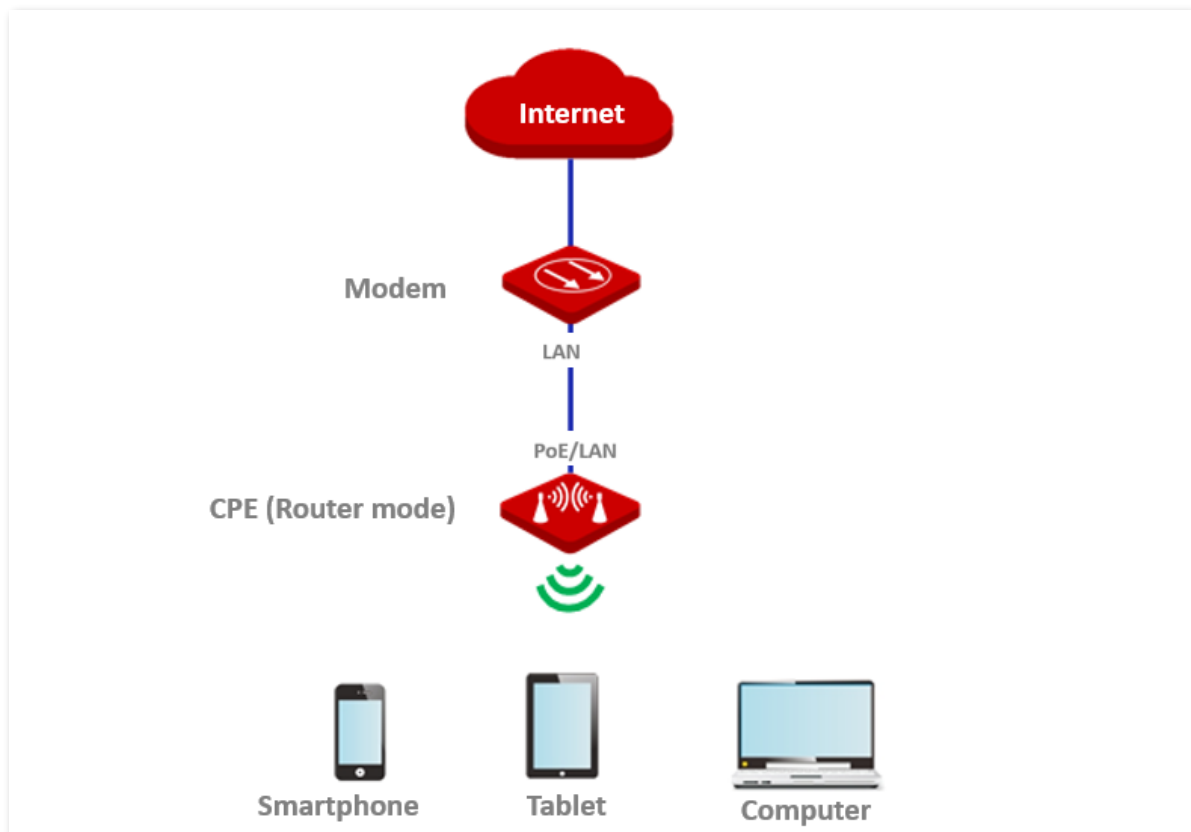
For detailed configuration of the router, refer to the user guide.

4.5 Router mode

4.5.1 Overview

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

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



4.5.2 Set Router mode



Tip

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 the following configurations.

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

Quick Setup Current Mode: AP

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

Next

3. 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 >> Router Current Mode: AP

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**

Parameters description

Name	Description
Internet Connection Type	<p>Refer to the following instructions to select the appropriate 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.

4. Set wireless network parameters of the CPE, and click **Next**.
 - 1) Customize an SSID, which is **IP-COM_AS1DF3** in this example.
 - 2) Set **Channel**.
 - 3) Set **Security Mode**, which is **WPA2-PSK** in this example.
 - 4) Set **Encryption Algorithm**, which is **AES** in this example.
 - 5) Set **Key** (WiFi password) for the wireless network.

Current Mode: AP

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

?

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

SSID

Channel ▼

Security Mode ▼

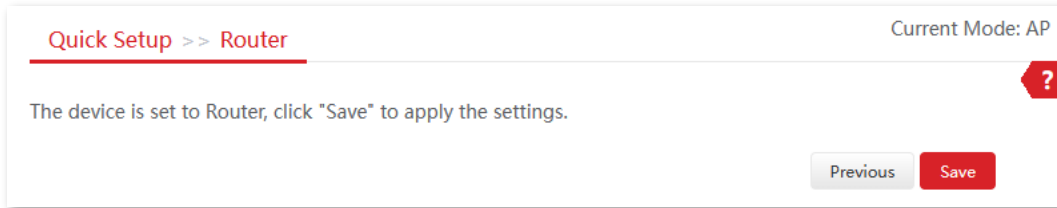
Encryption Algorithm AES TKIP TKIP&AES

Key

Parameters description

Name	Description
SSID	Specifies the WiFi name of the CPE.
Channel	Specifies the channel that the wireless network operates. Auto indicates that the device automatically adjusts its operating channel according to the ambient environment.
Security Mode	Specifies the security mode of the wireless network of the device. For more details, see Security Mode .
Encryption Algorithm	Specifies the encryption method of the wireless network. <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 available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	Specifies the WiFi password of the wireless network.

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



----End

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

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

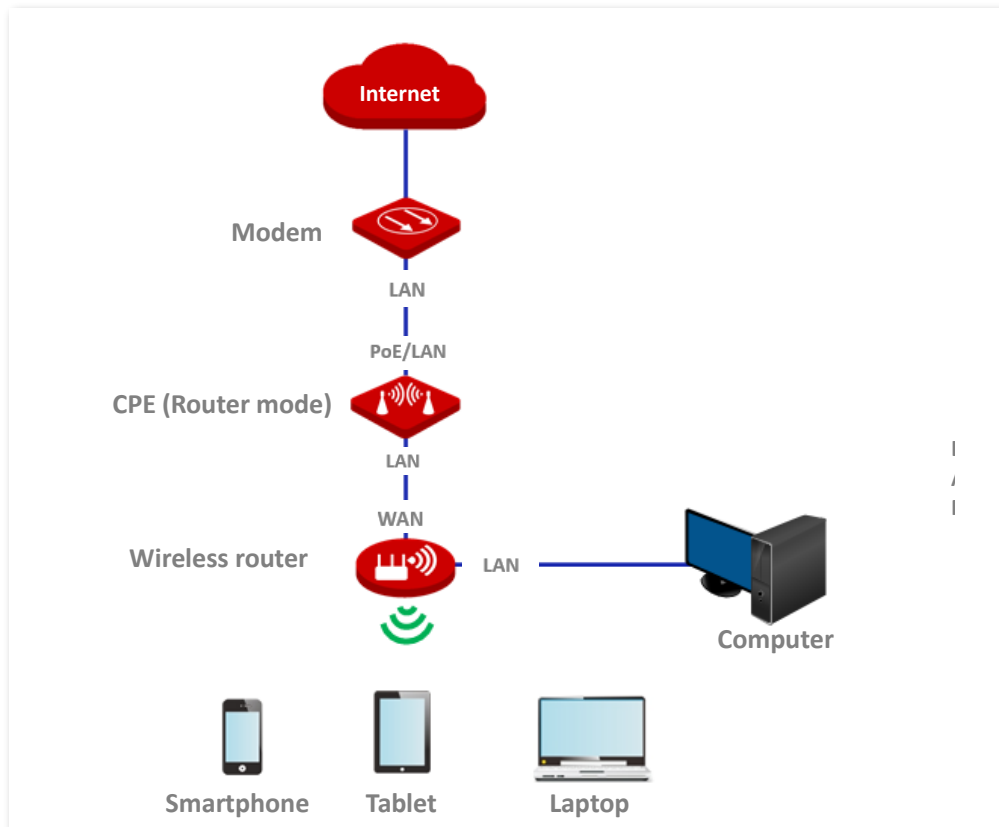
After the successful configuration, devices connected to the CPE can access to the internet in a wired or wireless manner.



Tip

- If there is only 1 LAN port on the CPE, you can connect your WiFi-enabled devices to the wireless network of the CPE to access the internet.
 - The name and password of the wireless network are **SSID** and **Key** set in step [4](#).
-

If the CPE has more than one LAN port, 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.

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

----End

To access the internet with:

- WiFi-enabled devices: Connect the WiFi-enabled devices, such as a smartphone, to the wireless 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.



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

5 Status

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and product version. Please refer to the actual product.

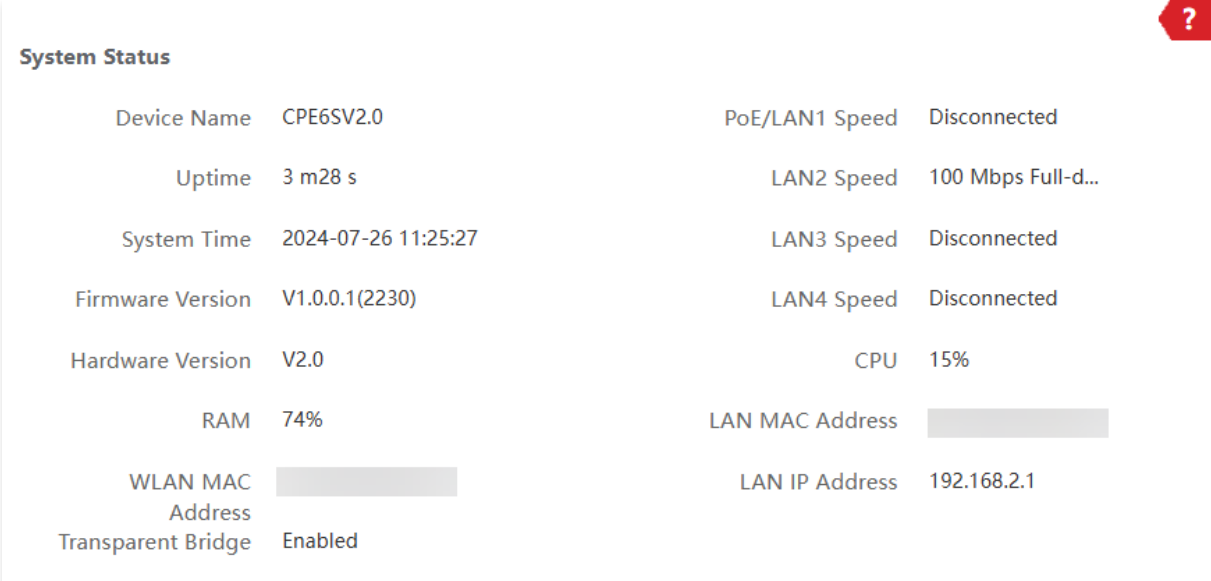
This module allows you to view the information of system and wireless network, including [system status](#), [wireless status](#), and [statistics](#).

5.1 System status

To access the page, [log in to the web UI](#) of the CPE and navigate to **Status**.

You can view the system status here. CPE6SV2.0 is used for illustration.

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



System Status			
Device Name	CPE6SV2.0	PoE/LAN1 Speed	Disconnected
Uptime	3 m28 s	LAN2 Speed	100 Mbps Full-d...
System Time	2024-07-26 11:25:27	LAN3 Speed	Disconnected
Firmware Version	V1.0.0.1(2230)	LAN4 Speed	Disconnected
Hardware Version	V2.0	CPU	15%
RAM	74%	LAN MAC Address	[Redacted]
WLAN MAC Address	[Redacted]	LAN IP Address	192.168.2.1
Transparent Bridge	Enabled		

If the CPE is set to WISP or Router mode, the system status is shown below. The following figure is for reference only.



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

System Status			
Device Name	CPE6SV2.0	PoE/LAN1 Speed	Disconnected
Uptime	7 m23 s	LAN2 Speed	100 Mbps Full-d...
System Time	2024-07-31 11:34:24	LAN3 Speed	Disconnected
Firmware Version	V1.0.0.1(2230)	LAN4 Speed	Disconnected
Hardware Version	V2.0	Connection Type	DHCP (Dynamic IP)
CPU	12%	Connection Status	Connected
RAM	80%	WAN IP Address	
LAN MAC Address		Default Gateway	
WLAN MAC Address		Primary DNS Server	
LAN IP Address	192.168.2.1	Secondary DNS Server	

Parameters description

Name	Description
Device Name	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 LAN Setup page.
Uptime	Specifies the time that has elapsed since the CPE was started last time.
System Time	Specifies the current system time of the CPE.
Firmware Version	Specifies the system firmware version number of the CPE.
Hardware Version	Specifies the hardware version number of the CPE.
CPU	Specifies the Central Processing Unit (CPU) usage of the CPE.
RAM	Specifies the memory usage of the CPE.
LAN MAC Address	Specifies the MAC address of LAN port of the CPE.

Name	Description
WLAN MAC Address	Specifies the MAC address of the wireless interface of the CPE.
Transparent Bridge	Specifies the status of transparent bridge of the CPE in AP mode, Client mode or Universal Repeater mode.
LAN Speed	Specifies the PoE/LAN or LAN port speed and duplex mode of the CPE.
LAN IP Address	<p>Specifies the IP address of the CPE, which is also the management IP address of this CPE.</p> <p>A LAN user can access the web UI of this device using this IP address. You can modify this IP address on the LAN Setup page.</p>
Connection Type	<p>Specifies the internet connection type of the CPE 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	Specifies the connection status of WAN port of the CPE in WISP or Router mode.
WAN IP Address	Specifies the IP address of WAN port of the CPE in WISP or Router mode.
Default Gateway	Specifies the default gateway address of the CPE in WISP or Router mode.
Primary DNS Server	Specifies the IP address of primary DNS server of the CPE in WISP or Router mode.
Secondary DNS Server	Specifies the IP address of secondary DNS server of the CPE in WISP or Router mode.

5.2 Wireless status

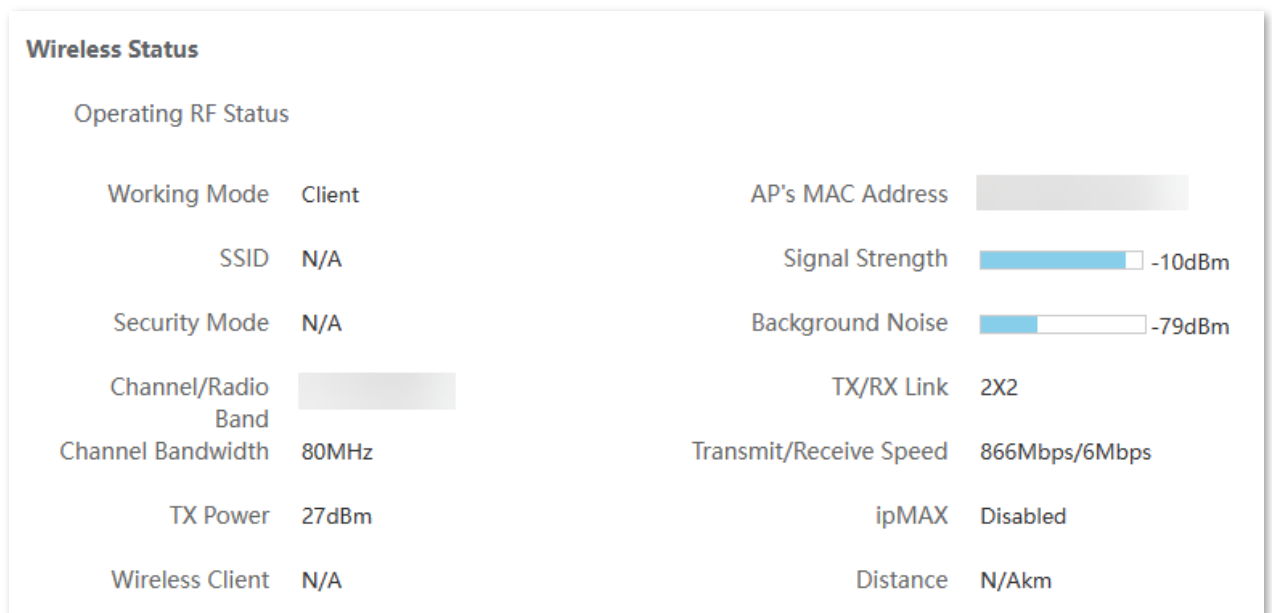
To access the page, [log in to the web UI](#) of the CPE and navigate to **Status**.

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

5.2.1 View operating RF status

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

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



Parameters description

Name	Description
Working Mode	Specifies the working mode in which the CPE operates.
SSID	Specifies the WiFi name of the operating RF.
Security Mode	Specifies the security mode of the wireless network of the operating RF.
Channel/Radio Band	Specifies the channel and radio band used by this device to transmit radio signals.
Channel Bandwidth	Specifies the channel bandwidth of the operating RF.
TX Power	Specifies the transmitted power of the operating RF.

Name	Description
Wireless Client	Specifies the number of wireless clients connected to the wireless network of the CPE's operating RF.
AP's MAC Address	<p>Specifies the MAC address of the upstream device.</p> <ul style="list-style-type: none"> - In AP or Router mode, it displays the WLAN MAC address of the 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>Specifies 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 to the wireless network of this CPE. - In Client, Universal Repeater or WISP mode, it displays the received signal strength of the peer CPE.
Background Noise	Specifies the strength of radio interference signals in the ambient environment that interferes with the wireless signal of this device in the same channel. Larger absolute value indicates less interference. For example, -95 dBm indicates less interference than that of -75 dBm.
TX/RX Link	Specifies the number of spatial streams of wireless data the device is transmitting or receiving. The more links indicates the more traffic.
Transmit/Receive Speed	<p>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 CPE. - In Client, Universal Repeater or WISP mode, it displays transmitting/receiving rate of this CPE.
ipMAX	Specifies the status of the ipMAX function. For details, refer to ipMAX .
Distance	<p>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>

5.2.2 View management RF status

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

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

Management RF Status

Status	Disable	Enabled upon Power on	Enable
SSID	IP-COM_03CB00_M...	Duration	15mins
Channel/Frequency Band			

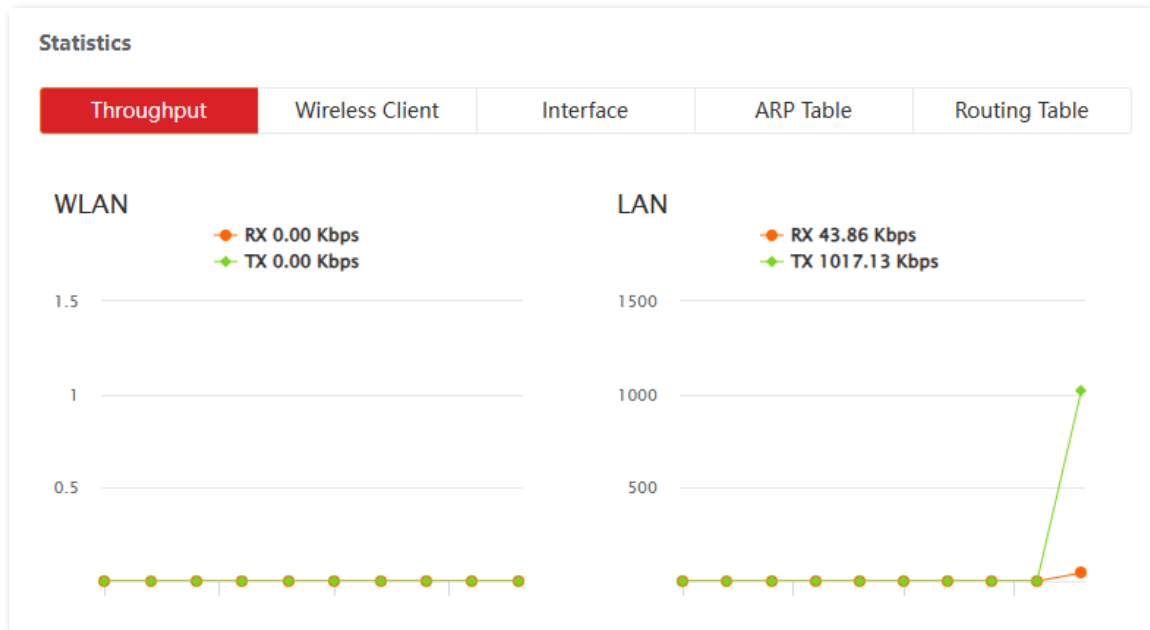
Parameters description

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

5.3 Statistics

To access the page, [log in to the web UI](#) of the CPE and navigate to **Status**.

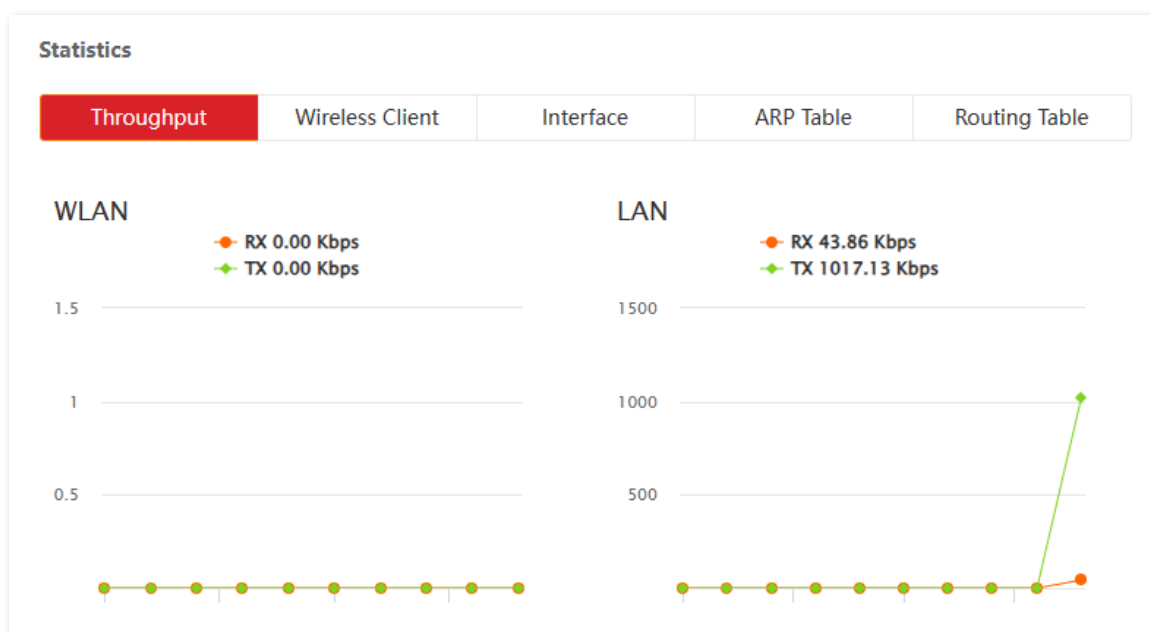
You can learn statistics information about [throughput](#), [wireless client](#), [interface](#), [ARP table](#) and [routing table](#) here. The following figure is for reference only.



5.3.1 Throughput

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

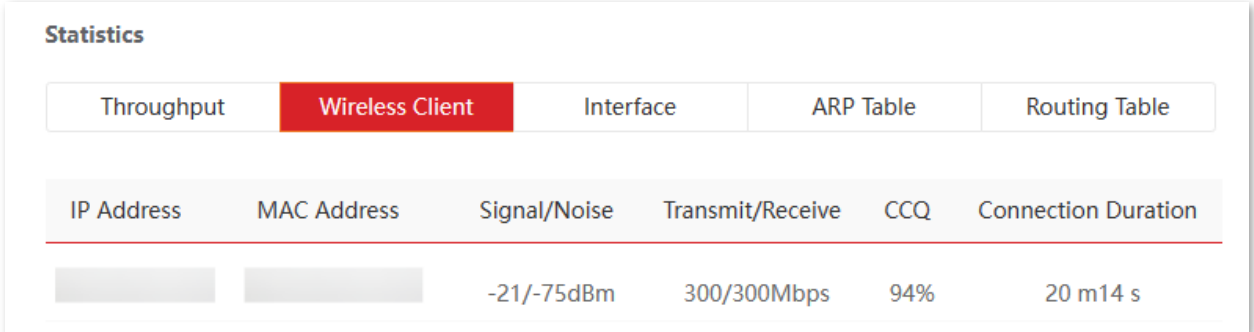
The line charts visually show the real-time transmitting and receiving traffic of WLAN and LAN port of the CPE. The following figure is for reference only.



5.3.2 Wireless client

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

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



Statistics					
Throughput	Wireless Client	Interface	ARP Table	Routing Table	
IP Address	MAC Address	Signal/Noise	Transmit/Receive	CCQ	Connection Duration
		-21/-75dBm	300/300Mbps	94%	20 m14 s

Parameters description

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

5.3.3 Upstream AP

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

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

Statistics					
Throughput	Upstream AP	Interface	ARP Table	Routing Table	
IP Address	MAC Address	Signal/Noise	Transmit/Receive	CCQ	Connection Duration
0.0.0.0		-43/-113dBm	300/270Mbps	100%	33 m33 s

Parameters description

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

5.3.4 Interface

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

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

Statistics						
Throughput		Wireless Client		Interface	ARP Table	Routing Table
Interface	IP Address	MAC Address	Received Packets	Receive Error	Transmitted Packets	Transmit Error
LAN	0.0.0.0		2187	0	3511	0
Bridge	192.168.2.10		2274	0	1468	0
WLAN	0.0.0.0		110	0	4819	0

Parameters description

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

5.3.5 ARP table

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

Address Resolution Protocol (ARP) 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 MAC address the device visits. The following figure is for reference only.

Statistics		
Throughput	Wireless Client	Interface
ARP Table		Routing Table
IP Address	MAC Address	Interface
192.168.2.100		Bridge

Parameters description

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

5.3.6 Routing table

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

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

Statistics				
Throughput	Wireless Client	Interface	ARP Table	Routing Table
Destination Network	Subnet Mask	Next Hop	Interface	
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	Specifies the destination network address of the IP packet.
Subnet Mask	Specifies the subnet mask of the destination network.
Next Hop	Specifies the IP address of entrance of the next hop route when the packets egress from the interface of the device.
Interface	Specifies the interface that the packets egress.

6 Network

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and product version. Please refer to the actual product.

6.1 LAN setup

6.1.1 Overview

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


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. The following figure is for reference only.

The screenshot displays the 'LAN Setup' configuration page. At the top left, the title 'LAN Setup' is underlined in red. At the top right, it says 'Current Mode: AP' with a red question mark icon. The form contains the following fields:

- MAC Address: A greyed-out text input field.
- IP Address Type: A dropdown menu set to 'Static IP Address'.
- IP Address: A text input field containing '192.168.2.2'.
- Subnet Mask: A text input field containing '255.255.255.0'.
- Default Gateway: A text input field containing '0.0.0.0'.
- Primary DNS Server: A text input field containing '0.0.0.0'.
- Secondary DNS Server: A text input field containing '0.0.0.0'.
- Device Name: A text input field containing 'CPE13V2.0'.

At the bottom, there are two buttons: a red 'Save' button and a white 'Cancel' button with a grey border.

Parameters description

Name	Description
MAC Address	Specifies the MAC address of LAN port.
IP Address Type	<p>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 CPE obtains an IP address, subnet mask, default gateway and DNS server IP address from the 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 CPE'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 CPE.</p>
IP Address	<p>Specifies the IP address of the CPE. A LAN user can use this IP address to log in to the web UI of the CPE.</p> <p>To access the internet, change this IP address to the same network segment of the LAN IP address of the egress router.</p>
Subnet Mask	Specifies the subnet mask of the CPE. The default is 255.255.255.0 .
Default Gateway	<p>Specifies the default gateway of the CPE.</p> <p>You can set it to the LAN IP address of the egress router to enable the CPE to access the internet.</p>
Primary DNS Server	<p>Specifies the primary DNS server IP address of the CPE.</p> <p>If the egress router has the DNS proxy function, it can be set to the LAN IP address of the egress router. Otherwise, specify a DNS server IP address manually.</p> <p>If there is only one DNS server IP address, enter it in this box.</p>
Secondary DNS Server	<p>Specifies the secondary DNS server IP address of the CPE.</p> <p>If there are two DNS server IP addresses, enter one in this box.</p>
Device Name	<p>Specifies the name of the CPE. The default name is the product model and version.</p> <p>You are recommended to change the name to indicate the location of the CPE, so that you can easily identify the CPE when there are multiple CPEs in the network.</p>

6.1.2 Modify LAN IP address

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 procedure

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Network > LAN Setup**.
3. Set **IP Address Type** to **Static IP Address**.
4. Set **IP Address** and **Subnet Mask**. If you want to connect the CPE to the internet, you need to configure **Default Gateway** and **Primary/Secondary DNS Server**.
5. Click **Save**.

LAN Setup

MAC Address

*IP Address Type

*IP Address

*Subnet Mask

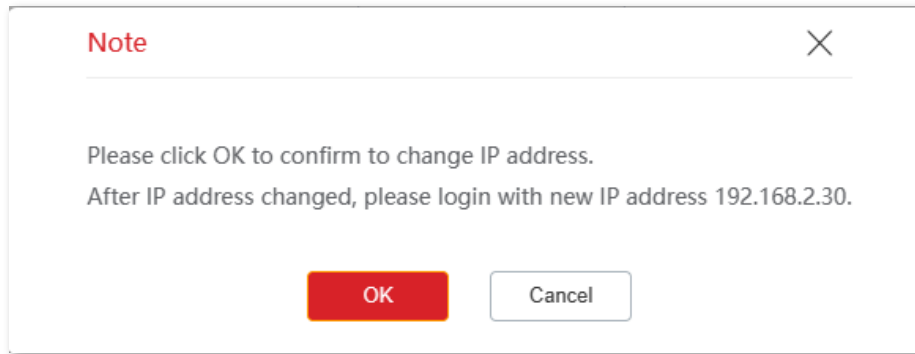
Default Gateway

Primary DNS Server

Secondary DNS Server

Device Name

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



----End

After changing the LAN IP address of the CPE:

- If the new and original IP addresses belong to the same subnet, you will be directed to the web UI of the device.
- If the new and original IP address belong to different subnets, assign your computer an IP address that falls in the same subnet as the new IP address before login with the new IP address. Refer to [Assign a fixed IP address to your computer](#) in **Appendix** for details.

Set the device to obtain a LAN IP address automatically

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 procedure

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Network > LAN Setup**.
3. Set **IP Address Type** to **DHCP (Dynamic IP Address)**.
4. Click **Save**.

LAN Setup

MAC Address	<input type="text"/>
IP Address Type	DHCP (Dynamic IP Ad ▾)
IP Address	192.168.2.30
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	CPE13V2.0

----End

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

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

6.2 Packet filter

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

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

On this page, you can set packet filtering parameters of the wired Ethernet port. Below takes CPE3V1.0 as an example.

Packet Filter ?

Wired port network packet filtering Enable

Filter Rule Indicates the packet filtering mode Enable Disable

Adding a filtering policy

ID	Filter rule	Rule details	Regular switch state	Filter mode	Operation
1	UDP protocol	Destination IP 255.255.255.255:5050	Enable	Prohibit	Delete Edit
2	UDP protocol	Destination IP 239.255.255.251:37810	Enable	Prohibit	Delete Edit
3	ARP&MAC address	ARP packet Destination MAC FF:FF:FF:FF:FF:FF	Enable	Prohibit	Delete Edit

Save
Cancel

Parameters description

Name	Description
Wired port network packet filtering	Specifies whether to enable the wired port network packet filtering function.
Filter Rule Indicates the packet filtering mode	Specifies whether to allow packets without filtering rules configured to pass through.
Adding a filtering policy	Used to add a rule for filtering packets.

Name	Description
Filter rule	<p>Specifies the filter rule of packets that need to be filtered.</p> <ul style="list-style-type: none"> - MAC address: Used to configure the packets corresponding to the MAC address to be filtered. - IP: Packets whose protocol type is IP protocol will be filtered. - VLAN: Packets whose protocol type is IEEE 802.1q protocol will be filtered. - ARP: Packets whose protocol type is ARP protocol will be filtered. - Port No.: Used to configure the packets corresponding to the port number to be filtered. - Custom: Used to customize the protocol type field of the packets to be filtered.
Rule details	Specifies the parameter settings required for filtering rules to filter the packets.
Regular switch state	Specifies the status of the filter rule. Values: Enable and Disable .
Filter mode	Specifies whether to filter the packets. Values: Permit and Prohibit .
Operation	<p>Used to edit or delete the packet filter policy.</p> <ul style="list-style-type: none"> - Edit: Used to edit the packet filter policy. - Delete: Used to delete the packet filter policy.
Source MAC	Specifies the data frames originating from this MAC address will be filtered.
Destination MAC	Specifies the data frames going to this MAC address will be filtered.
Source IP	Specifies the packets originating from this IP address will be filtered.
Destination IP	Specifies the packets going to this IP address will be filtered.
IP protocol type	Specifies the type of transport layer protocol used by the data segments that need to be filtered. All means filtering both TCP and UDP protocols.
VLAN ID	Specifies the VLAN ID of the packets to be filtered.
Source port	Specifies the packets corresponding to the source port number will be filtered.
Destination port	Specifies the packets corresponding to the destination port number will be filtered.
Custom	Used to customize the protocol type field of the packets that need to be filtered (2 bytes, hexadecimal, such as 0x8010).

6.3 MAC clone

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

6.3.1 Overview

If the CPE cannot access the internet after you configure the internet settings, your ISP may have associated your internet service account with a device's MAC address.

In this case, MAC cloning can generally fix this problem.



Note

Before you clone the MAC address, ensure that the device (such as a computer and router) you used previously can access the internet.

6.3.2 Clone a MAC address

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

Method 1

1. Connect the computer to the CPE.
2. [Log in to the web UI](#) of the CPE, and navigate to **Network > MAC Clone**.
3. Click **Clone Local MAC Address**.
4. Click **Save**.

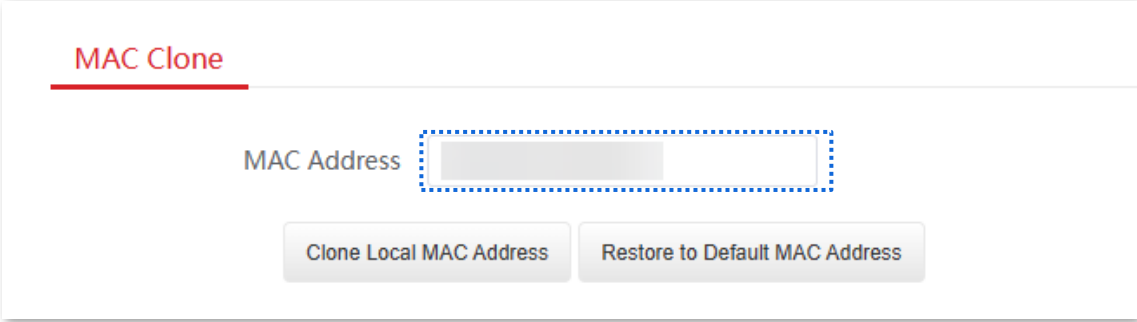
MAC Clone

MAC Address

----End

Method 2

1. Log in to the web UI of the router, and record the MAC address.
2. [Log in to the web UI](#) of the CPE, and navigate to **Network > MAC Clone**.
3. Enter the MAC address of the router in the **MAC Address** field.
4. Click **Save**.



MAC Clone

MAC Address

Clone Local MAC Address Restore to Default MAC Address

----End



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

6.4 DHCP server

6.4.1 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.



Tip

If you [change the LAN IP address of the CPE](#) and the new and original IP addresses belong to different subnet, the system automatically changes the IP address pool of the DHCP server to be in the same subnet as the new IP address of the LAN port.

6.4.2 Configure the DHCP server

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Network > DHCP Server**.
3. Enable the **DHCP Server** function.
4. Set the parameters. Generally, you need to set only **Gateway Address** and **Primary DNS Server**.
5. Click **Save**.

DHCP Server Current Mode: AP

* DHCP Server

Start IP Address

End IP Address

Subnet Mask

* Gateway Address

* Primary DNS Server

Secondary DNS Server

Lease Time




----End



Note

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	Specifies whether to enable the DHCP server function of the CPE.
Start IP Address	Specifies the start IP address of the IP address pool of the DHCP server. The default value is 192.168.2.100 .
End IP Address	<p>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 subnet as the LAN port of the CPE.</p>
Subnet Mask	Specifies the subnet mask assigned by the DHCP server to clients. The default value is 255.255.255.0 .
Gateway Address	<p>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 servers or hosts outside the local network only through a gateway.</p>
Primary DNS Server	<p>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	(Optional) Specifies the secondary DNS server IP address assigned by the DHCP server to clients.
Lease Time	<p>Specifies the validity period that a client holds an IP address assigned by the DHCP server.</p> <p>When the IP address expires:</p> <ul style="list-style-type: none"> - If the client is still connected to the CPE, the client will automatically renew and continue to occupy the IP address. - If the client is not connected to the CPE (due to shut-down or wireless disconnection), the CPE will release the IP address. If other clients send a request for an IP address, the CPE can assign this IP address to other clients. <p>You are recommended to keep the default value.</p>

6.5 DHCP client

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

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

DHCP Client				
ID	Host Name	IP Address	MAC Address	Lease Time
1	DESKTOP-2PAVGKC	192.168.2.147		23h 58m 33s
2	DESKTOP-0RMLE69	192.168.2.198		23h 24m 5s
3	DESKTOP-OE85T2C	192.168.2.100		22h 7m 48s
4	linux-c83a359c6c40	192.168.2.114		2h 6m 53s
5		192.168.2.173		1h 33m 50s

10 Datas/Page 5 data in total

Parameters description

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

6.6 VLAN settings

6.6.1 Overview

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

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

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

Port Type	Received Packets		Transmitted Packets
	Tagged Packets	Untagged Packets	
Access			Strip the tag in the packet and then forward it
Trunk	Forward data to the ports of the corresponding VLAN based on the tag's VID	Forward data to the ports of the corresponding VLAN based on the PVID	VID = Port PVID, strip the tag in the packet and then forward it
			VID \neq Port PVID, retain the tag in the packet and then forward it

6.6.2 Configure VLAN (Example: CPE6SV2.0)

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

VLAN Settings ?

VLAN Settings

PVID (Range: 1 to 4094)

Management VLAN (Range: 1 to 4094)

WLAN VLAN ID (Range: 1 to 4094)

LAN2 (Range: 1 to 4094)

LAN3 (Range: 1 to 4094)

LAN4 (Range: 1 to 4094)

Parameters description

Name	Description
VLAN Settings	Specifies whether to enable the 802.1Q VLAN function of this CPE. By default, it is disabled. After the VLAN function is enabled, the LAN port with PoE power supply function (such as PoE/LAN) is used as a trunk port.
PVID	Specifies the default native VLAN ID of the trunk port. The default is 1.
Management VLAN	Specifies the 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.
Trunk port	A wired LAN port that serves as a trunk port. A trunk port allows all VLANs to pass through. Here takes CPE12V3.0 as an example.
WLAN VLAN ID	Used to set a VLAN ID for the wireless network of the CPE. By default, it is set to 1000. After the VLAN function is enabled, the WLAN interface functions is equivalent to an access port, whose PVID is the same as VLAN ID.
LAN2	Used to set a VLAN ID of the Ethernet port of the CPE. By default, it is set to 1.
LAN3	After the VLAN function is enabled, the Ethernet port is equivalent to an access port, whose PVID is the same as VLAN ID.
LAN4	

6.6.3 Example of configuring VLAN on CPE13

Networking requirements

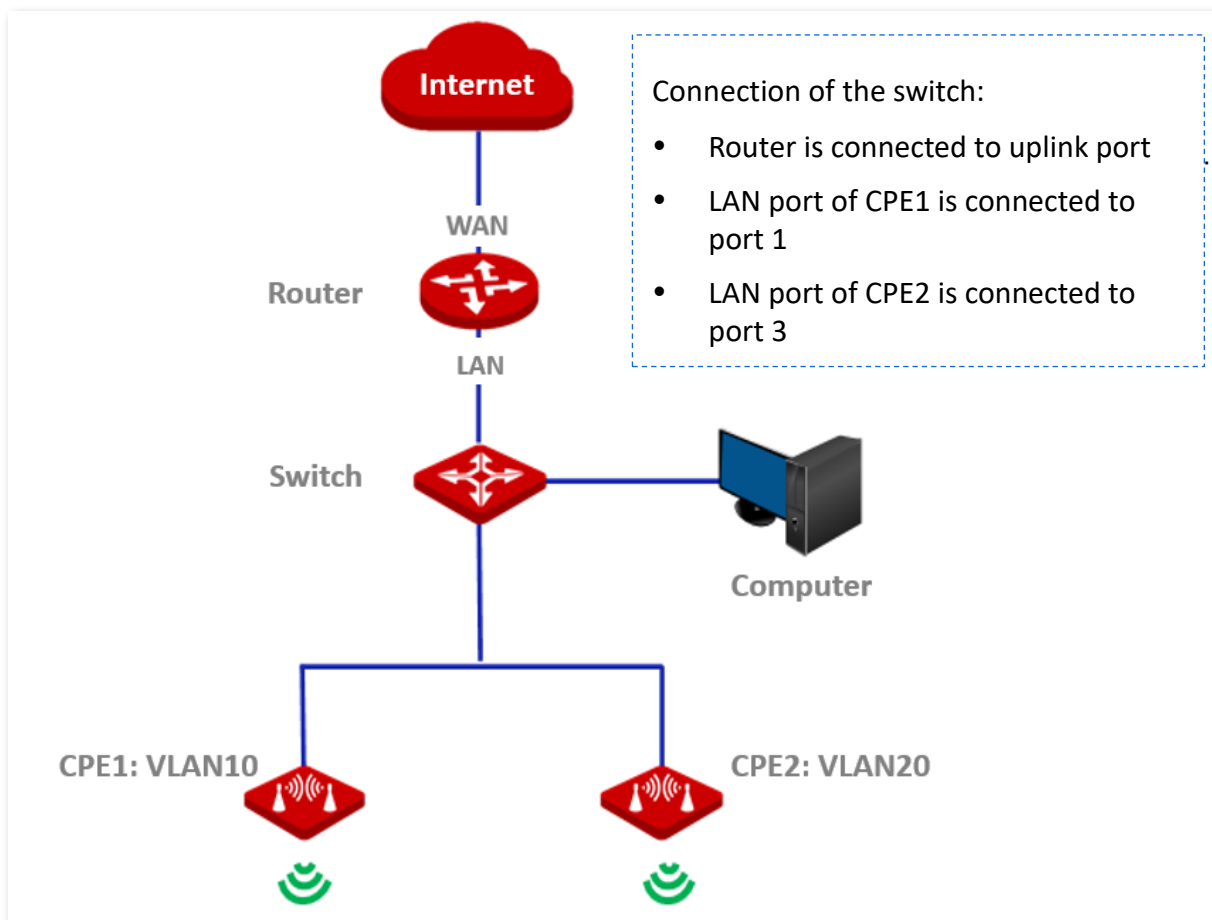
Two communities want to create an isolated network with two CPEs and connect to the internet through the same router.

Solution

You can perform as follows:

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

Network topology



Configuration procedure

1. Set up the CPE1.
 - 1) [Log in to the web UI](#) of CPE1, and navigate to **Network > VLAN Settings**.
 - 2) Enable the **VLAN Settings** function.
 - 3) Configure **WLAN VLAN ID**, which is **10** in this example.
 - 4) Click **Save**.

VLAN Settings

VLAN Settings

PVID (Range: 1 to 4094)

Management VLAN (Range: 1 to 4094)

WLAN VLAN ID (Range: 1 to 4094)

- 5) Click **OK**, and wait until the CPE1 completes reboot.
2. Set the WLAN VLAN ID of CPE2 to 20 by step [1](#).
3. Set up the switch as shown in the following table.

Port	Type	VLAN ID (Allowed Packets)	PVID
Uplink port (Connected to router)	Trunk	1, 10, 20	1
Port 1 (Connected to CPE1)	Trunk	1, 10	1
Port 3 (Connected to CPE2)	Trunk	1, 20	1

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

4. Set up the router.
 - 1) Enable two DHCP servers on the router, and assign them to VLAN10 and VLAN20 respectively.
 - 2) Configure the QVLAN on the router as shown in the following table.

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

For details, see the user guide for the router.

----End

Verification

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

7 Wireless settings

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and product version. Please refer to the actual product.

7.1 Basic configuration

7.1.1 Overview

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

Broadcast SSID

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

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

Isolate client

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

Max. number of clients

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

Security mode

A wireless network uses radio, which is open to the public, as its data transmission medium. If a wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network.

To ensure communication security, transmission links of wireless networks must be encrypted for protection.

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

■ None

The CPE does not encrypt its wireless network. When users connect to the wireless network, they can access the internet without entering a password. This option is not recommended because it affects network security.

■ WEP

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

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

WPA-PSK, WPA2-PSK and Mixed WPA/WPA2-PSK (compatible with WPA-PSK and WPA2-PSK) use a pre-shared key or personal key for authentication only. Data encryption keys are generated by the CPE. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks.

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

■ WPA and WPA2

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

WPA and WPA2 use 802.1x to authenticate clients and the login information of a client is managed by the client. This effectively reduces the probability of information leakage.

In addition, each time a client connects to a wireless network that adopts the WPA or WPA2 security mode, the RADIUS server generates a dynamic 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.

7.1.2 Basic wireless settings

To access the page, [log in to the web UI](#) of the CPE and navigate to **Wireless > Basic**.

On this page, you can modify the basic wireless settings of the CPE.

When the CPE works in AP, WISP or Router mode, the basic wireless settings page is displayed as below. The following figure is for reference only.

Basic

Enable Wireless

Country/Region

SSID

Transparent WDS Enable Disable

Broadcast SSID Enable Disable

Network Mode

Channel Bandwidth

Channel

Channel Shift Enable Disable

DFS Function Enable Disable

Transmit Power 1dBm 8dBm

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)

Parameters description

Name	Description
Enable Wireless	Specifies whether to enable the wireless function.
Country/Region	<p>Specifies the country or region where this CPE is located.</p> <p>You can select the country or region to ensure that this CPE complies with the channel regulations of the country or region. By default, it is set to China.</p>
SSID	<p>Specifies the name of the wireless network (SSID). You can modify it as required.</p> <ul style="list-style-type: none"> For single-unit CPEs, it defaults to IP-COM_XXXXXX (XXXXXX indicates the last six digits of the LAN MAC address). For kit-unit CPEs, it defaults to IP-COM_XXXXXX (XXXXXX indicates random six digits).
Transparent WDS	<p>It is available when the CPE works in AP mode or Client mode.</p> <p>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.</p> <p> Tip</p> <p>Transparent WDS and Transparent Bridge cannot be enabled at the same time.</p>
Broadcast SSID	<p>Specifies whether to broadcast the SSID.</p> <ul style="list-style-type: none"> Enable: When an SSID is broadcast, wireless clients can detect the SSID. Disable: When an SSID is not broadcast, you need to manually enter the SSID to connect to the wireless network.
Network Mode	Specifies the wireless network mode of the CPE. Only wireless clients supporting the listed network mode can connect to the CPE.
Channel Bandwidth	<p>Specifies the bandwidth of the operating channel of a wireless network.</p> <p>The channel bandwidth varies with different network modes. Select it based on your actual operating environment. Auto indicates that the CPE can switch its channel bandwidth based on the ambient environment.</p>
Channel	<p>Specifies the channel in which the CPE operates.</p> <p>Auto indicates that the CPE automatically changes to a channel rarely used in the ambient environment to prevent interference.</p>

Name	Description
Channel Shift	<p>Specifies the shift of the channel center frequency.</p> <p>With this function enabled, the channel center frequency will shift based on the frequency defined by the IEEE 802.11 standard, so that the CPE can exchange data on less interference channels.</p> <p> Note</p> <p>When the Channel Shift function is enabled, other CPEs that bridge with it should also enable this function, and the offset value must be consistent. Otherwise the bridge will fail.</p>
Offset Value	<p>Specifies the offset value of the channel center frequency. The parameter is available only when the Channel Shift function is enabled.</p>
DFS Function	<p>Specifies the Dynamic Frequency Selection (DFS).</p> <p>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.</p>
Transmit Power	<p>Specifies the transmit power of the CPE.</p> <p>Higher number indicates wider WiFi coverage. Setting a proper transmit power helps improve the performance and security of the wireless network.</p>
Transmit Rate	<p>Specifies wireless transmission rate of the CPE. Auto is recommended.</p> <p>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.</p>
Security Mode	<p>There are various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, Mixed-WPA/WPA2-PSK, WPA and WPA2.</p>
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. It is set to Disable by default.
Max. Number of Clients	<p>Specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID.</p> <p>If the number is reached, the wireless network rejects new connection requests from clients.</p>

- **None**

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

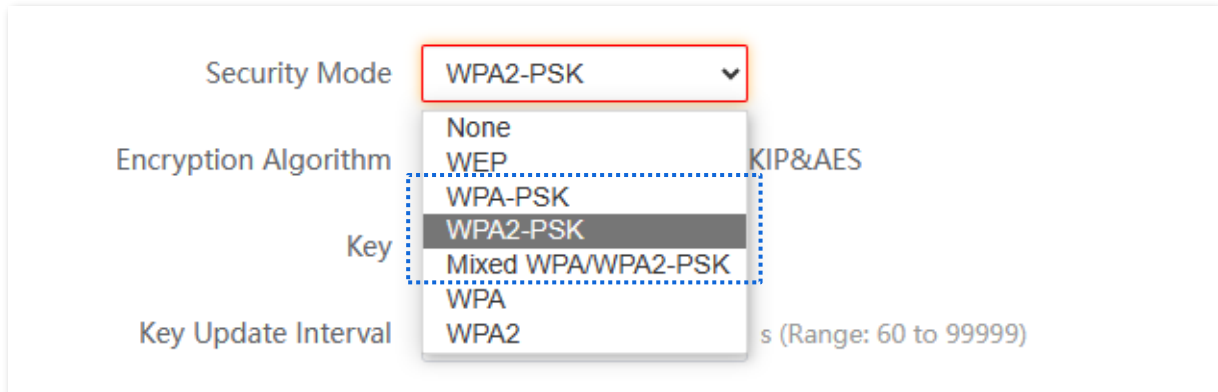
- **WEP**

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
Encryption Type	<p>Specifies the encryption type for the WEP security mode. Values:</p> <ul style="list-style-type: none"> – Open: A wireless client can connect to the wireless network of the selected SSID without being authenticated, and data exchanged between the client and the network is encrypted using WEP. – Shared: A shared key is used for authentication and data is encrypted using WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network of the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key.
Default Key	<p>Specifies the WEP key for the Open or Shared encryption type.</p> <p>For example, if Default Key is set to Key 2, a wireless client can connect to the wireless network of the selected SSID only with the password specified by Key 2.</p>
Key 1/2/3/4	<p>Specifies the WEP key. You can enter four keys, but only the one specified as Default Key takes effect.</p> <p>Supported formats:</p> <ul style="list-style-type: none"> – ASCII: Enter 5 or 13 ASCII characters for the key. – Hex: Enter 10 or 26 hexadecimal characters (0-9, a-f, and A-F) for the key.


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



The screenshot shows a configuration window with the following fields and values:

- Security Mode:** WPA2-PSK (selected in a dropdown menu)
- Encryption Algorithm:** TKIP&AES
- Key:** (empty field)
- Key Update Interval:** (empty field, with a note: s (Range: 60 to 99999))

Parameters description

Name	Description
Security Mode	<p>Specifies the security mechanism that protects the wireless network. Values:</p> <ul style="list-style-type: none"> – WPA-PSK: The wireless network of the selected SSID is encrypted using WPA-PSK. – WPA2-PSK: The wireless network of the selected SSID is encrypted using WPA2-PSK. – Mixed WPA/WPA2-PSK: Wireless clients can connect to the wireless network of the selected SSID using either WPA-PSK or WPA2-PSK.
Encryption Algorithm	<p>Specifies the encryption algorithm corresponding to the selected security mode. Values:</p> <ul style="list-style-type: none"> – AES: Advanced Encryption Standard. – TKIP: Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. – TKIP&AES: Both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network of the selected SSID using TKIP or AES. <p> Tip</p> <p>If Security Mode is set to WPA-PSK, this parameter can be set to AES or TKIP. If it is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter can be set to AES, TKIP, or TKIP&AES.</p>
Key	<p>Specifies a pre-shared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.</p>
Key Update Interval	<p>Specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p>The value 0 indicates that a WAP key is not updated.</p>

■ WPA, WPA2

The screenshot shows a configuration window with the following fields and values:

- Security Mode:** WPA (dropdown menu)
- RADIUS Server:** (empty text field)
- RADIUS Port:** (empty text field)
- Encryption Algorithm:** WPA2 (dropdown menu, with options: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, WPA2)
- RADIUS Password:** (password field with a visibility icon)
- Key Update Interval:** 0 (text field) s (Range: 60 to 99999)

Parameters description

Name	Description
	The WPA and WPA2 options are available for network protection with a RADIUS server.
Security Mode	<ul style="list-style-type: none"> – WPA: The wireless network of the selected SSID is encrypted using WPA. – WPA2: The wireless network of the selected SSID is encrypted using WPA2.
RADIUS Server	Specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	Specifies the port number of the RADIUS server for client authentication.
RADIUS Password	Specifies the shared key of the RADIUS server for client authentication.
Encryption Algorithm	<p>Specifies the encryption algorithm corresponding to the selected security mode. Values:</p> <ul style="list-style-type: none"> – AES: Advanced Encryption Standard. – TKIP: Temporal Key Integrity Protocol. – TKIP&AES: Both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network of the selected SSID using TKIP or AES.
Key Update Interval	<p>Specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p>The value 0 indicates that a WAP key is not updated.</p>

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

Basic

Enable Wireless

Country/Region

Broadcast SSID Enable Disable

Network Mode

Channel Bandwidth

Channel

Channel Shift Enable Disable

DFS Function Enable Disable

Transmit Power (1dBm to 8dBm)

Transmit Rate

Primary Upstream SSID

Primary AP BSSID Lock

Transparent WDS Enable Disable

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

Key

Key Update Interval s (Range: 60 to 99999)

Secondary Upstream SSID Enable Disable

Secondary Upstream SSID

Secondary Upstream BSSID Lock

Transparent WDS Enable Disable

Security Mode

Reconnect Primary Upstream SSID Enable Disable

Reconnection Interval (Range: 1~720minutes)


Isolate Client Enable Disable

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

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

The following only describes main parameters. For other parameters, refer to [Parameter description](#) for AP mode.

Parameters description

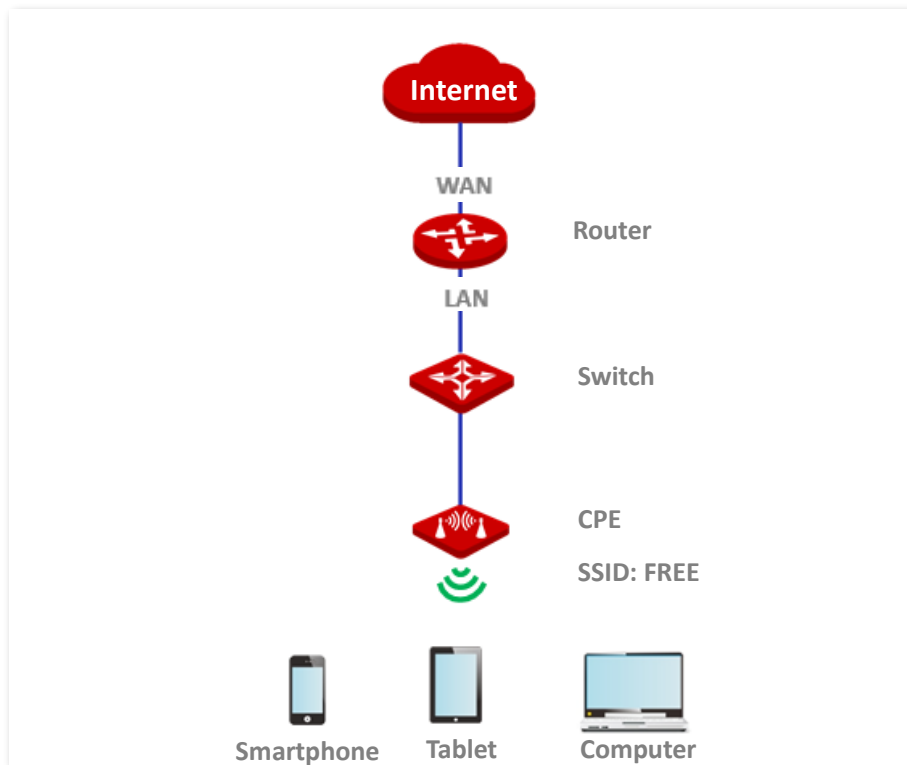
Name	Description
Primary Upstream SSID	<p>Specifies the SSID of the primary upstream wireless network that the CPE connects to.</p> <p>After bridging succeeds, the SSID of the primary upstream wireless network will automatically populate.</p>
Primary AP BSSID	<p>Specifies the MAC address of the primary upstream wireless network.</p> <p>After bridging succeeds, the MAC address of the primary upstream wireless network will automatically populate.</p>
Lock	<p>Used to lock the upstream wireless network.</p> <p>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 WiFi name.</p>
Secondary Upstream SSID	<p>Specifies the SSID of the secondary upstream wireless network that the CPE connects to.</p> <p>With this function enabled, if the CPE fails to connect to the primary upstream SSID, it will automatically connect to the secondary upstream SSID.</p>
Secondary Upstream BSSID	<p>Specifies the wireless MAC address of the secondary upstream wireless network.</p>
Reconnect Primary Upstream SSID	<p>Used to reconnect to the primary upstream wireless network.</p> <p>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.</p>
Reconnection Interval	<p>Specifies the interval at which the CPE tries to reconnect to the primary upstream SSID when it is connected to the secondary upstream SSID.</p>
	<p>Used to refresh the available wireless networks and select the one for connection.</p>

7.1.3 Set up a non-encrypted wireless network

Networking requirements

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

Network topology



Configuration procedure

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

Basic

Enable Wireless

Country/Region

*SSID

Transparent WDS Enable Disable

Broadcast SSID Enable Disable

Network Mode

Channel Bandwidth

Channel

Channel Shift Enable Disable

DFS Function Enable Disable

Transmit Power 1dBm 27dBm

Transmit Rate

*Security Mode

Isolate Client Enable Disable

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

----End

Verification

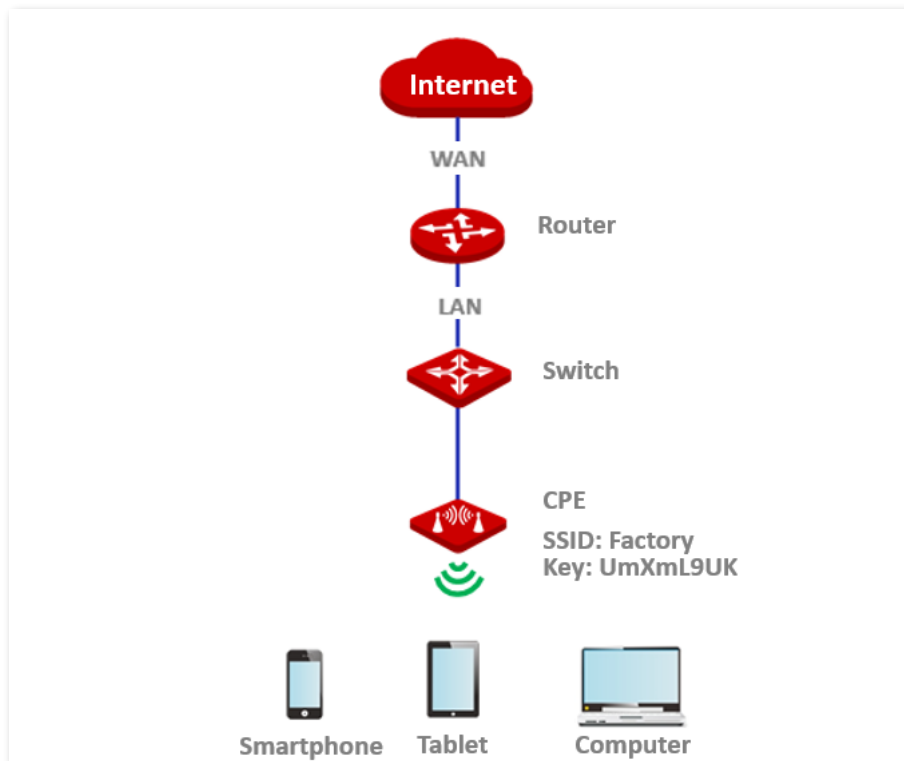
WiFi-enabled devices can connect to the wireless network whose SSID is **FREE** without a password.

7.1.4 Set up a wireless network encrypted using WPA2-PSK

Networking requirements

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

Network topology



Configuration procedure

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

Basic

Enable Wireless

Country/Region

* SSID

Transparent WDS Enable Disable

Broadcast SSID Enable Disable

Network Mode

Channel Bandwidth

Channel

Channel Shift Enable Disable

DFS Function Enable Disable

Transmit Power 1dBm 27dBm

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

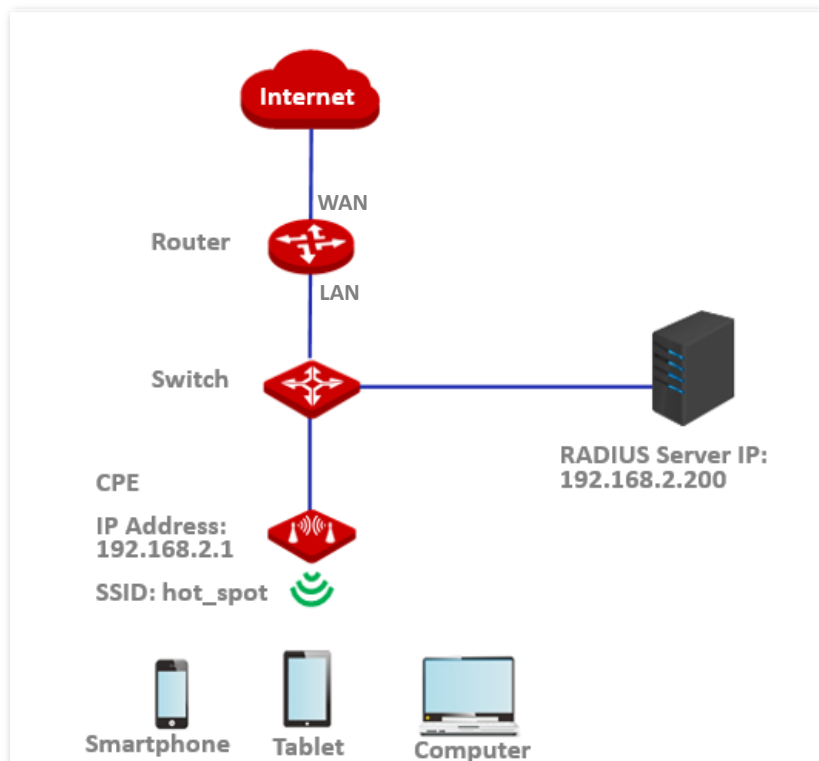
WiFi-enabled devices can connect to the WiFi named **Factory** with the password **UmXmL9UK**.

7.1.5 Set up a wireless network encrypted using WPA or WPA2

Networking requirements

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

Network topology



Configuration procedure

I. Configure the CPE

Assume that:

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

1. [Log in to the web UI](#) of the CPE, and navigate to **Wireless > Basic**.
2. Set **SSID** to **hot_spot**.

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

Basic Current Mode: AP

Enable Wireless

Country/Region

* SSID

Transparent WDS Enable Disable

Broadcast SSID Enable Disable

Network Mode

Channel Bandwidth

Channel

Channel Shift Enable Disable

DFS Function Enable Disable

Transmit Power 1dBm 27dBm

Transmit Rate

* Security Mode

* RADIUS Server

* RADIUS Port

* Encryption Algorithm AES TKIP TKIP&AES

* RADIUS Password

Key Update Interval s (Range: 60 to 99999)

Isolate Client Enable Disable


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

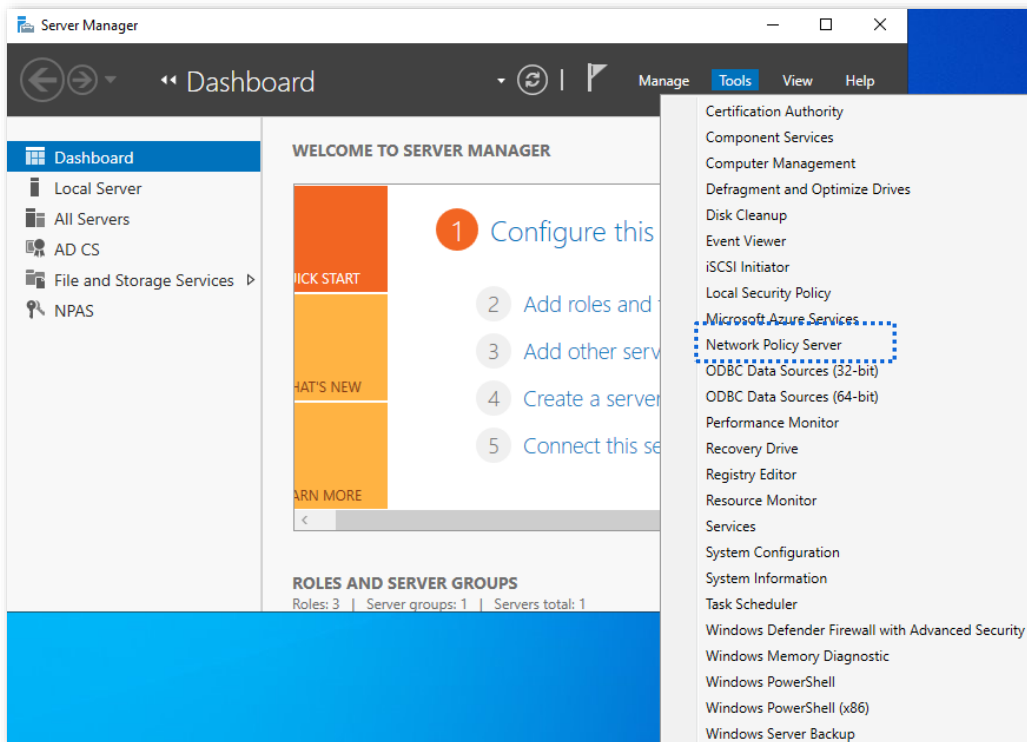
----End

II. Configure the RADIUS server

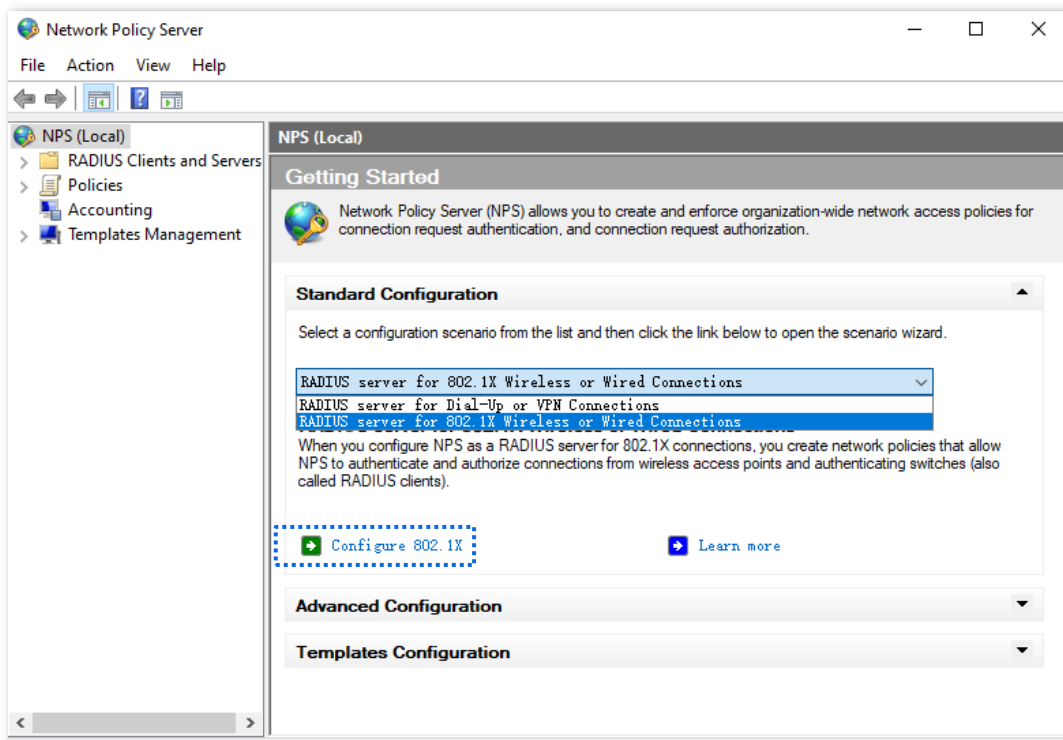


Windows 2016 is used as an example to describe how to configure the RADIUS server.

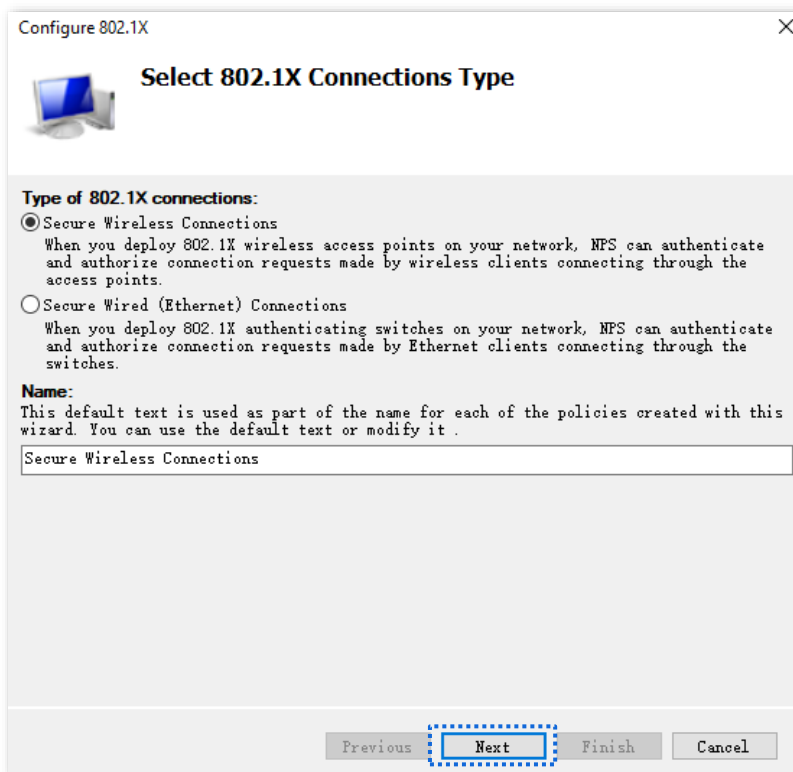
1. Install **Active Directory Certificate Services** and **Network Policy and Access Services**, and deploy the certificate.
 - 1) On the **Start > Server Manager > Dashboard** page, navigate to **Add roles and features > Server Selection > Server Roles**, and tick the **Active Directory Certificate Services**.
 - 2) According to the operation wizard, install the **Certification Authority of Active Directory Certificate Services** and **Network Policy and Access Services**.
 - 3) After the service installation is completed, click  in the upper right corner and follow the prompts to deploy the certificate.
2. Configure 802.1X.
 - 1) Navigate to **Start > Server Manager > Dashboard**, click **Tools** in the upper right corner, and click **Network Policy Server**.



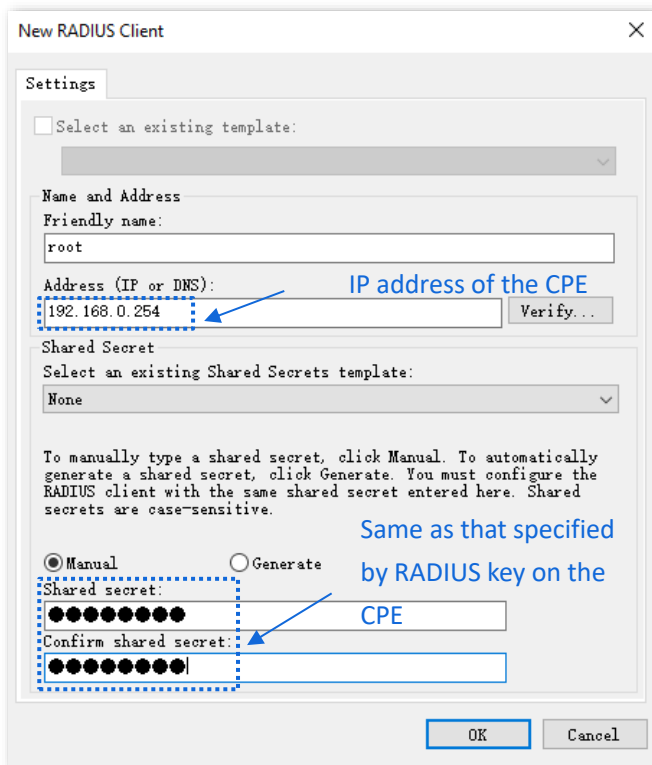
- 2) Select **RADIUS server for 802.1X Wireless or Wired Connection from Standard Configuration** and click **Configure 802.1X**.



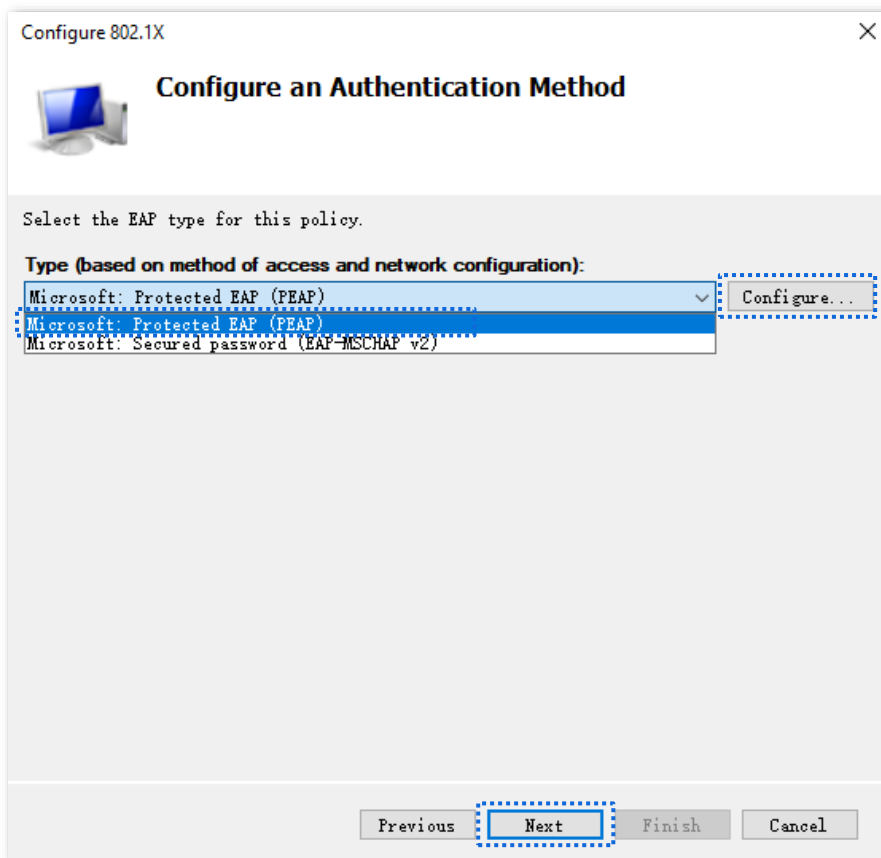
- 3) Select **Secure Wireless Connections for Type of 802.1X connections**. Modify the name as required, which is **Secure Wireless Connections** in this example, and click **Next**.

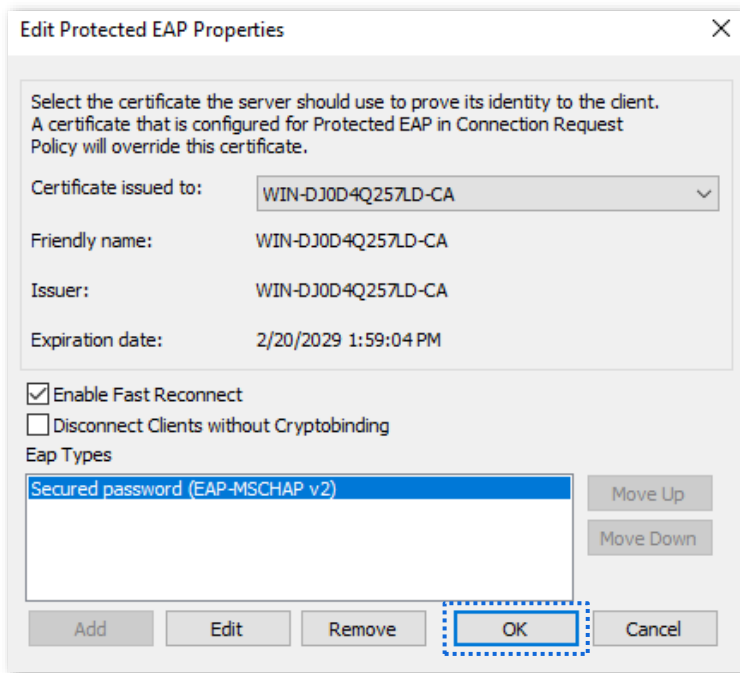


- 4) On the **Specify 802.1X Switches** page, click **Add**.
- 5) Set a RADIUS client name (which can be the name of the CPE) and the IP address of the CPE. Enter **UmXml9UK** in the **Shared secret** and **Confirm shared secret** text boxes, and click **OK**.

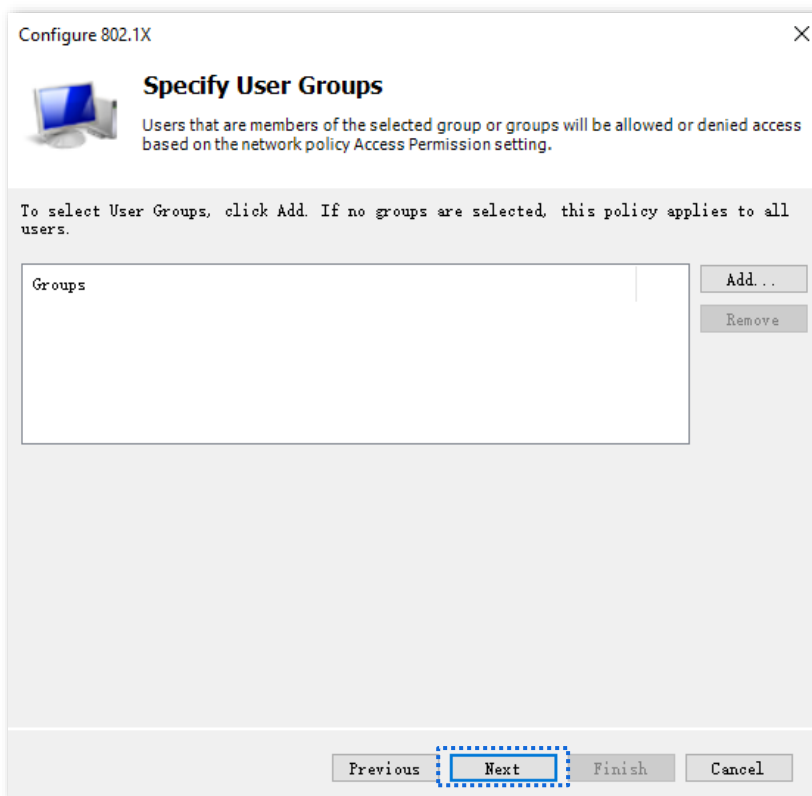


- 6) Select **Microsoft: Protected EAP (PEAP)** from **Type**, and click **Configure**. Select the certificate deployed in the certificate authority in the previous step, click **OK**, and click **Next** after the configuration is completed.

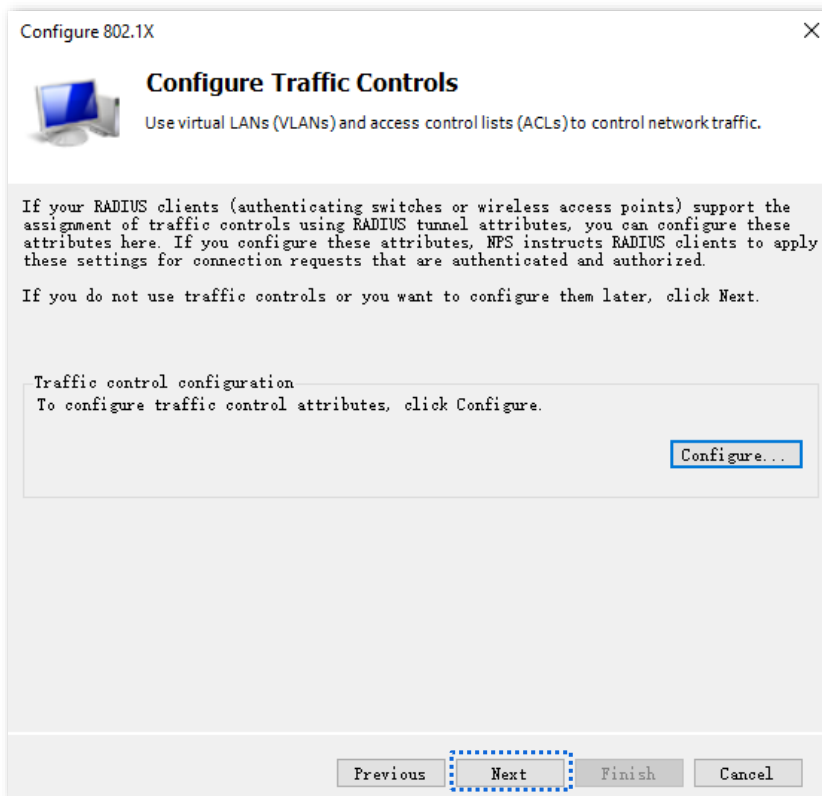




- 7) Click **Next** on the **Specify User Groups** page.



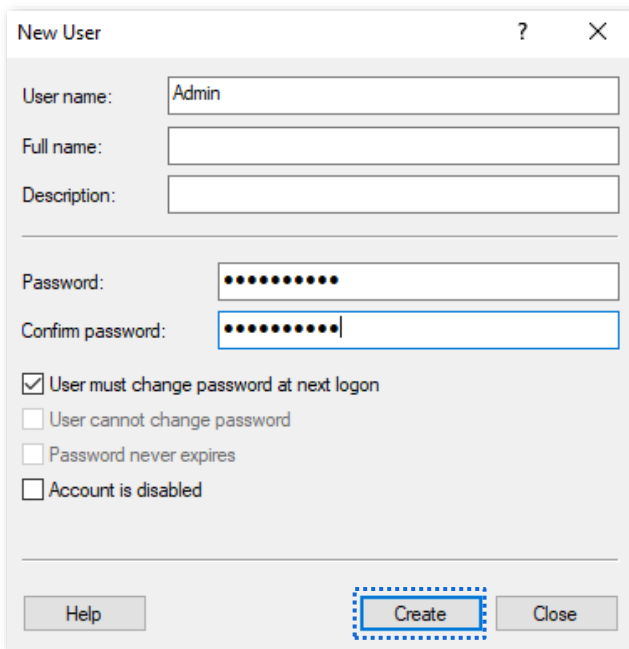
- 8) On the **Configure Traffic Controls** page, configure the parameters as required, click **Next**, and click **Finish**.



3. Configure the user and user group.
 - 1) Create a user.

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

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



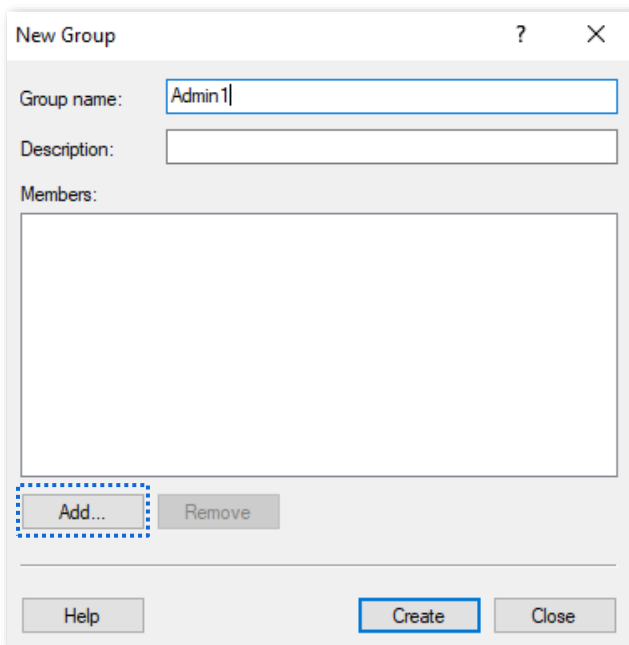
The 'New User' dialog box is shown with the following fields and options:

- User name: Admin
- Full name: (empty)
- Description: (empty)
- Password: (masked with dots)
- Confirm password: (masked with dots)
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

Buttons: Help, Create (highlighted), Close.

2) Create a user group.

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

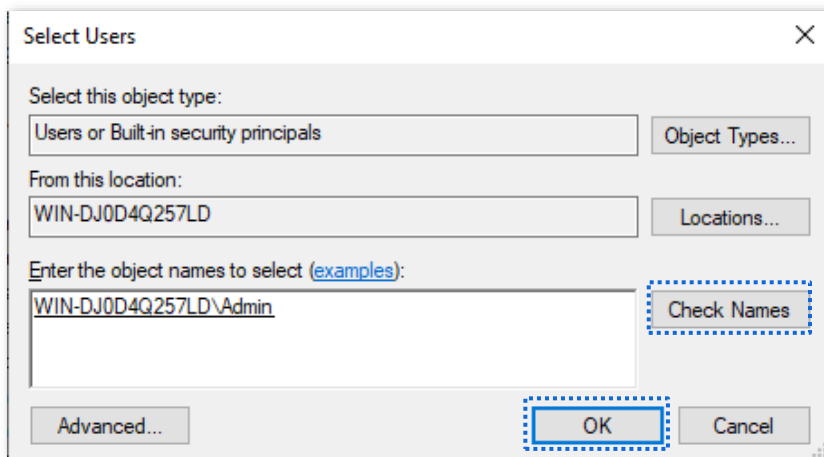


The 'New Group' dialog box is shown with the following fields and options:

- Group name: Admin1
- Description: (empty)
- Members: (empty list)

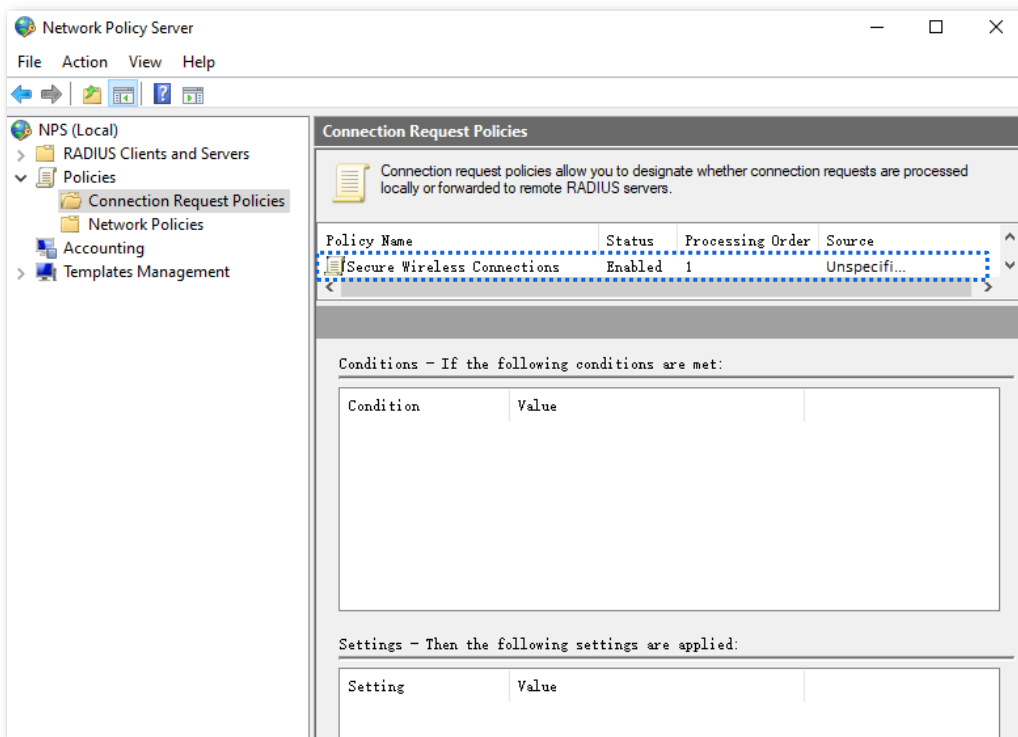
Buttons: Add... (highlighted), Remove, Help, Create, Close.

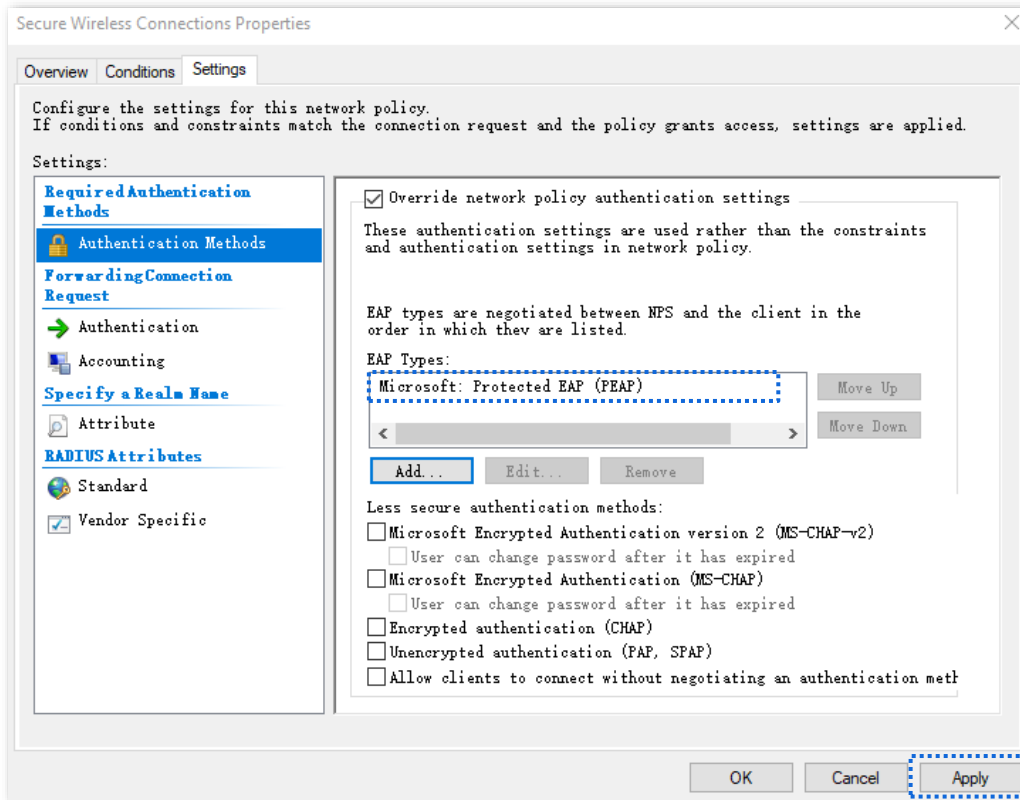




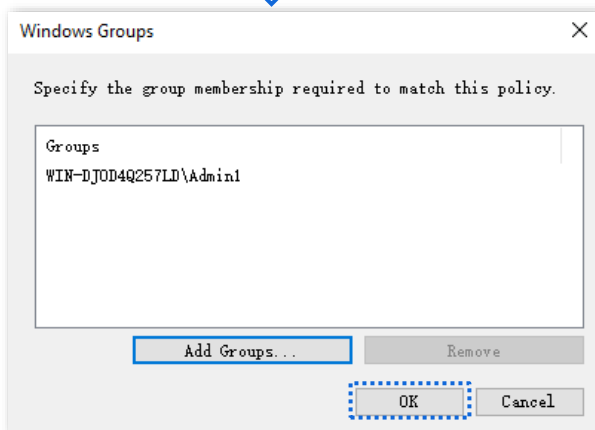
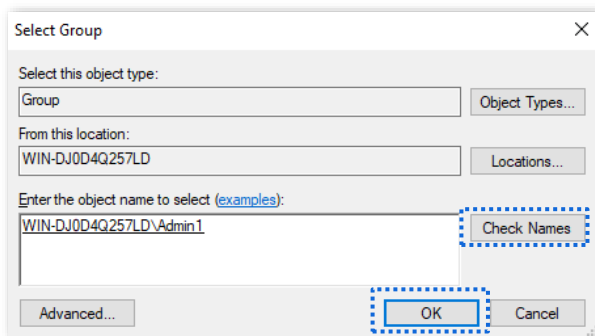
4. Configure the policies.

- 1) Navigate to **Start > Server Manager > Dashboard**, click **Tools** in the upper right corner, click **Network Policy Server**, and double-click **Policies**.
- 2) Click **Connection Request Policies** and double-click **Secure Wireless Connections**. On the **Secure Wireless Connections Properties** window, click **Settings** and tick **Override network policy authentication settings**. Click **Add**, add **Microsoft: Protected EAP (PEAP)** as **EAP Types**, and click **Apply**.





- 3) Click **Network Policies** and double-click **Secure Wireless Connections**. On the **Secure Wireless Connections Properties** window, click **Conditions**, and click **Add**.
 Add the **Windows Groups**, enter the created [user group](#), click **Check Names**, click **OK**, then click **OK**, and click **Apply**.



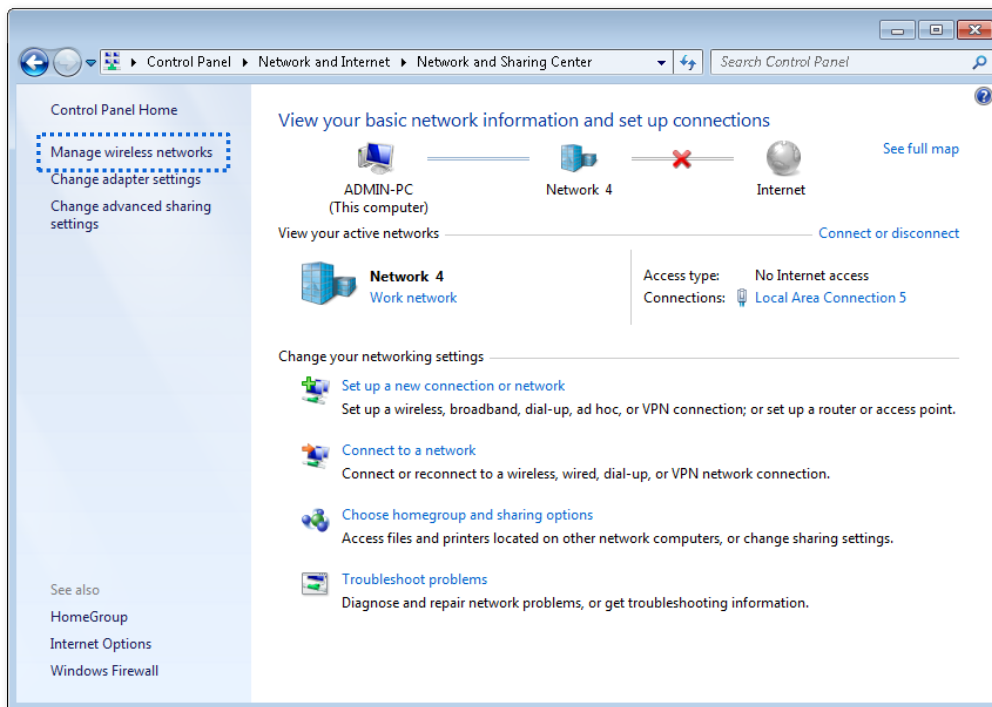
----End

III. Configure your wireless device

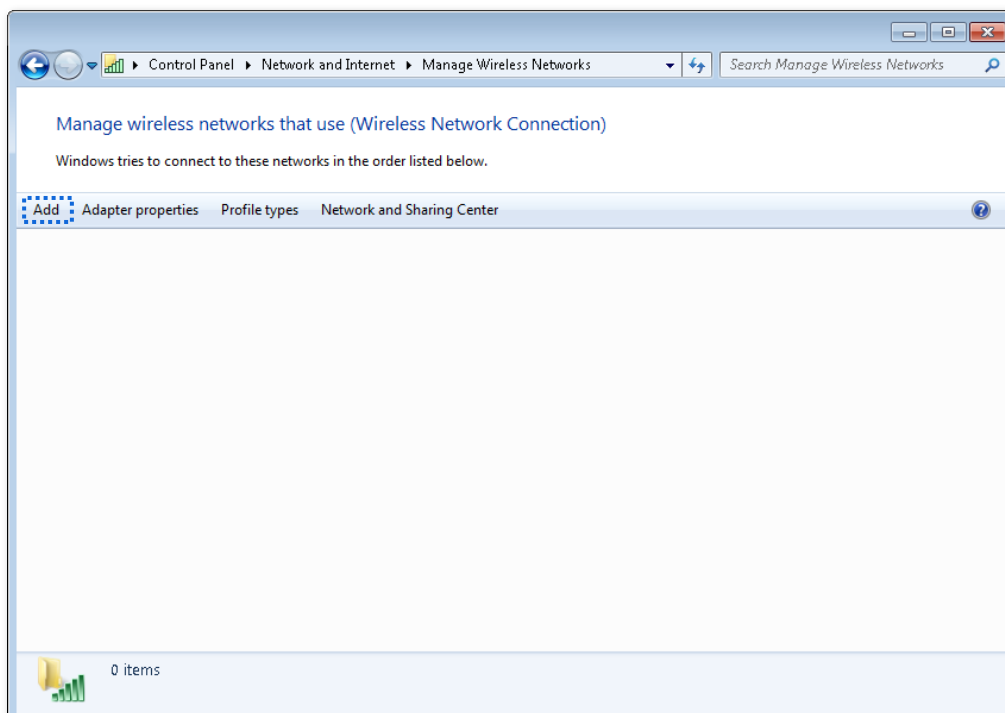


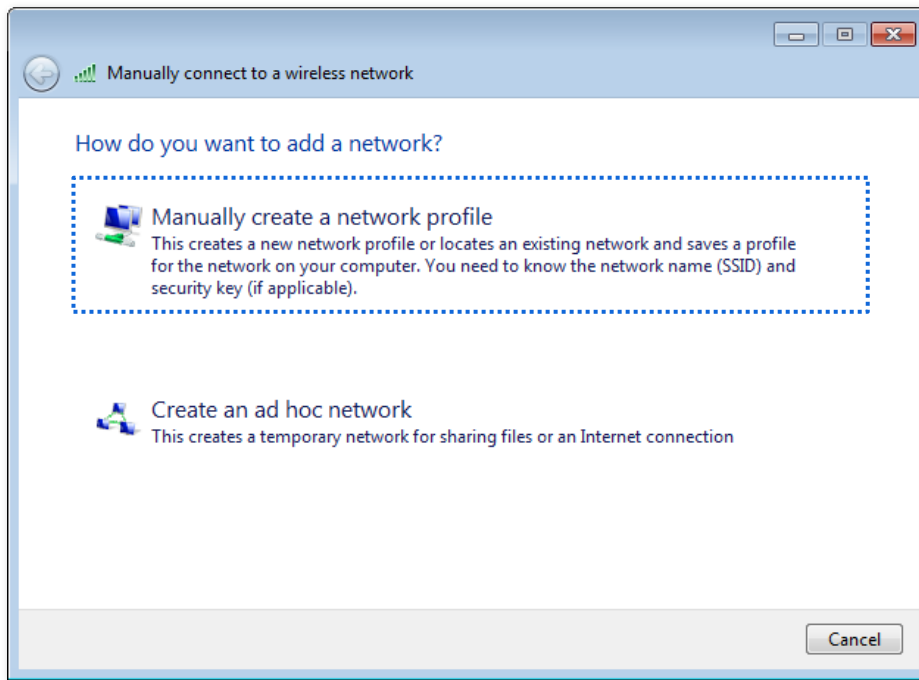
Windows 7 is taken as an example to describe the procedures.

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

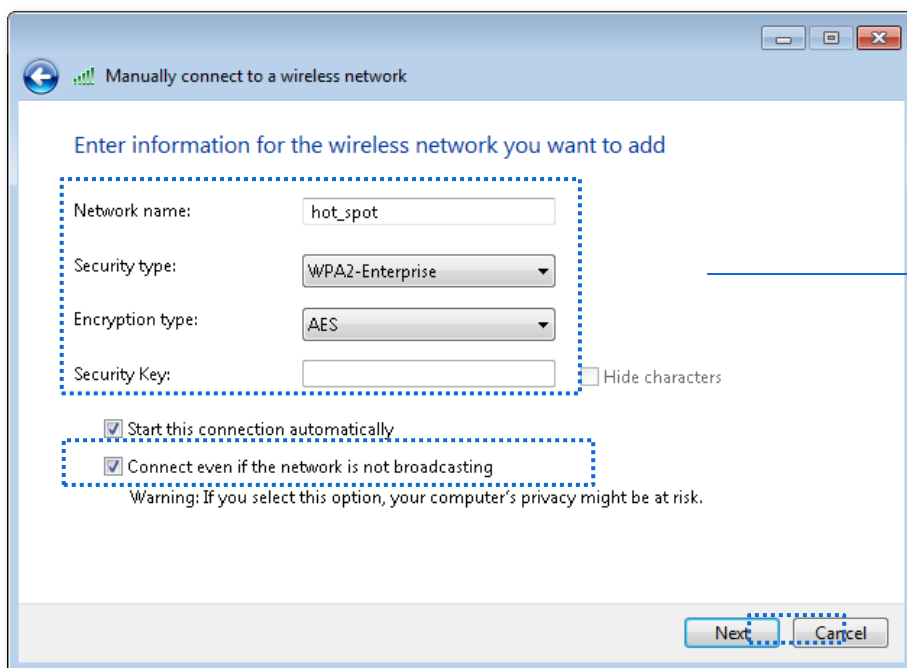


2. Click **Add**, and Click **Manually create a network profile**.



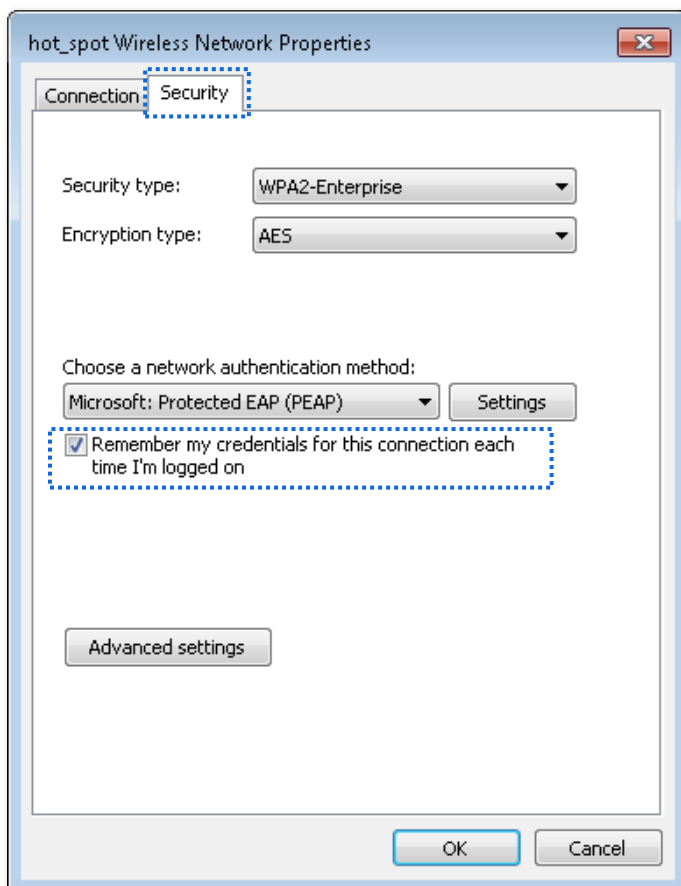
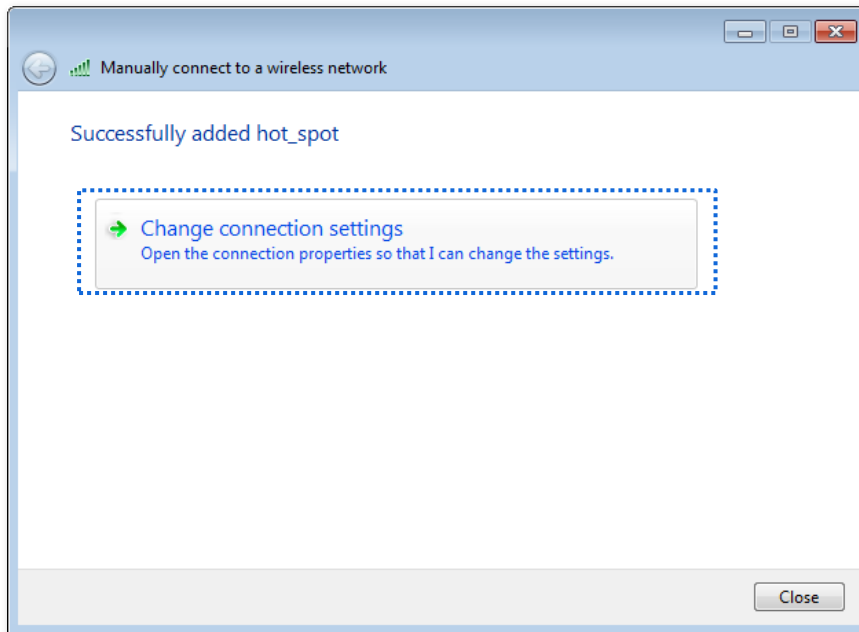


3. Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.

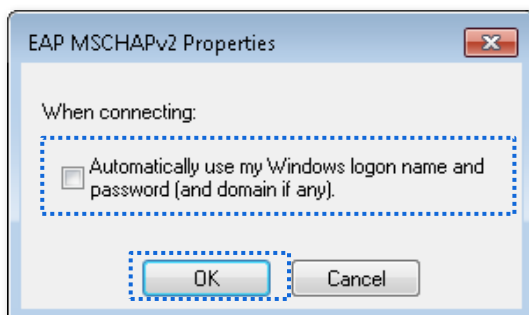
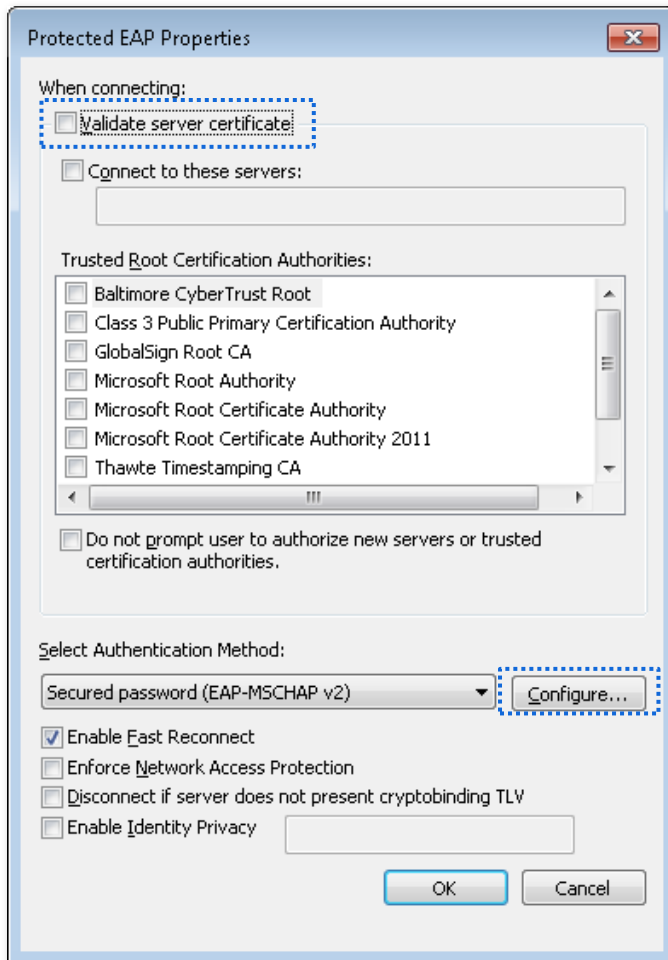


Must be the same as the security mode for the SSID specified on the CPE

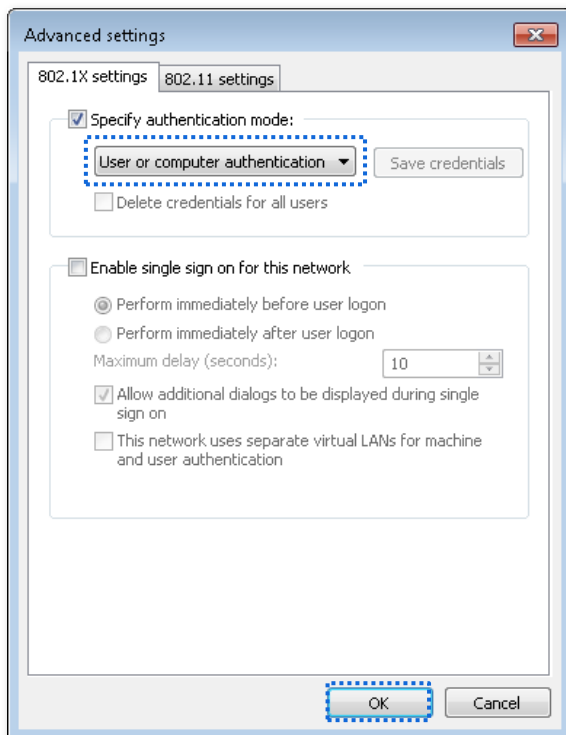
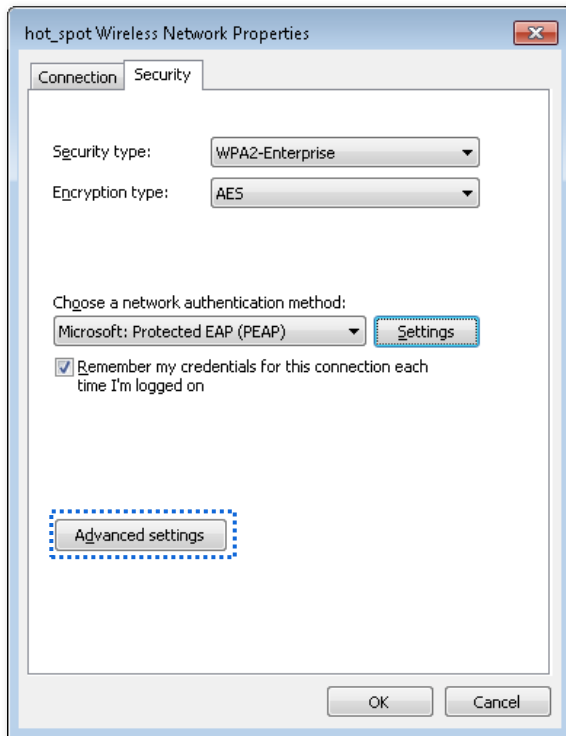
4. Click **Change connection settings**. Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



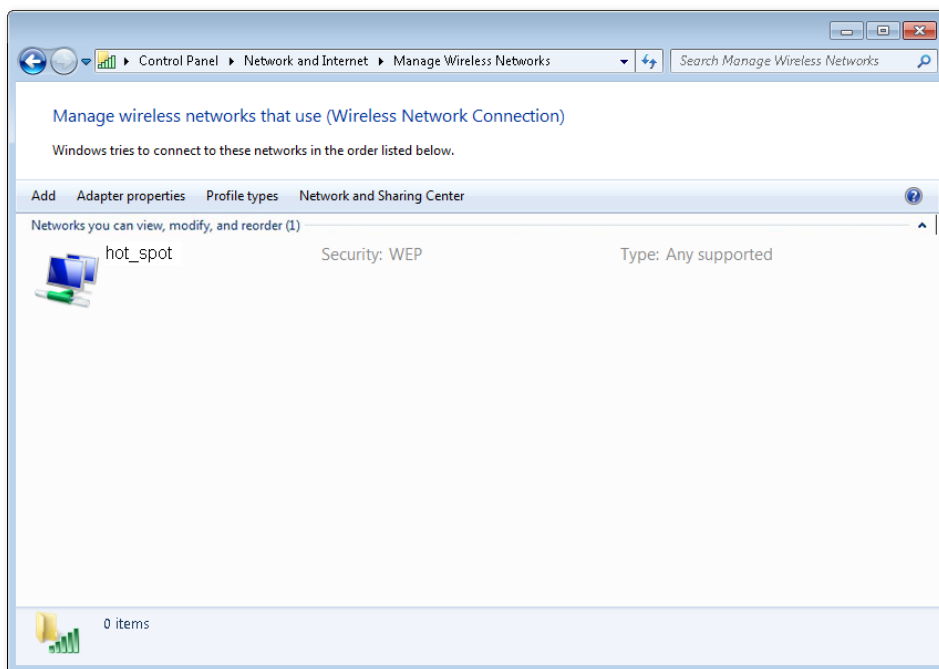
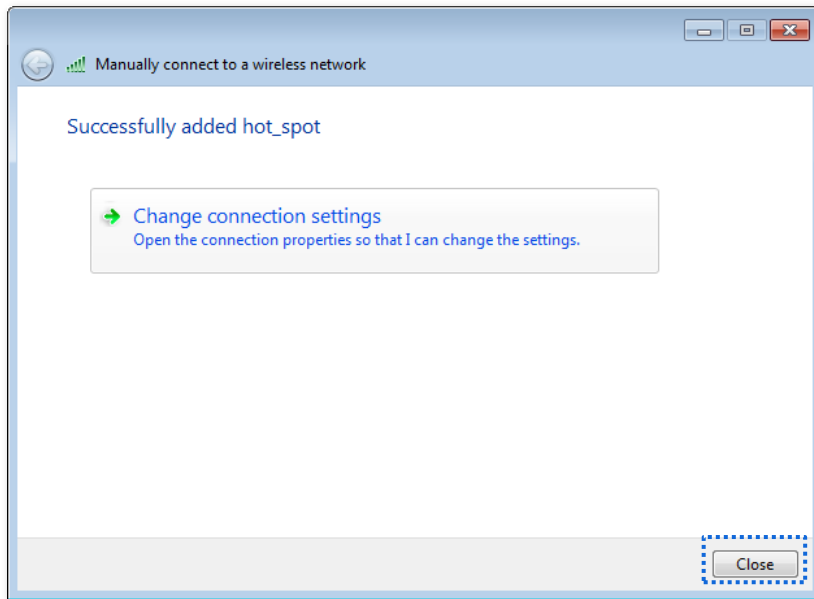
5. Deselect **Validate server certificate** and click **Configure**. Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



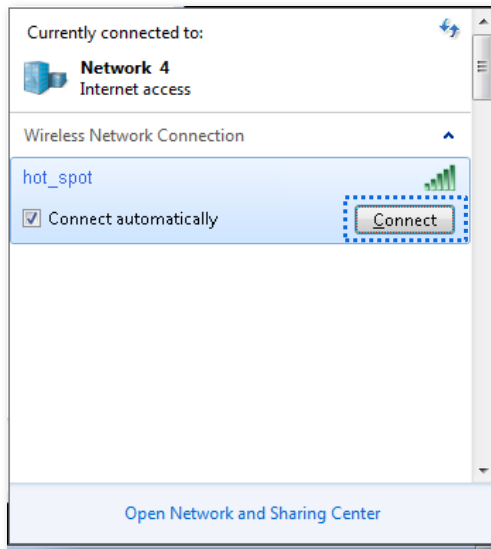
- Click **Advanced settings**. Select **User or computer authentication** and click **OK**.



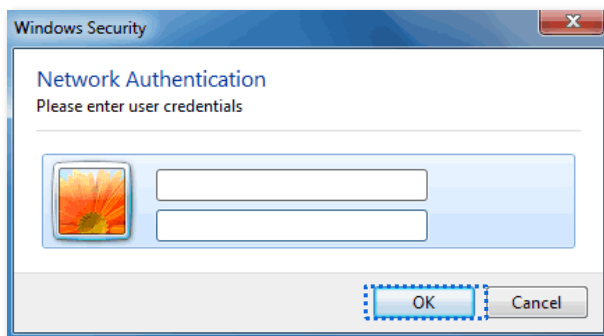
7. Click **Close**.



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



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



----End

Verification

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

7.2 Advanced settings

To access the page, [log in to the web UI](#) of the CPE and navigate to **Wireless > Advanced**.

This module enables you to adjust the wireless performance of the CPE. You are recommended to configure it under the guidance of a professional. The following figure is for reference only.

Advanced

WMM Enable Disable

APSD Enable Disable

Minimum RSSI Threshold Enable Disable

Preamble Short Preamble Long Preamble

ipMAX Enable Disable

Signal Transmission Coverage-oriented Capacity-oriented

TPC Enable Disable

Signal Reception Level ▼

Transmission Distance Auto km (Range: 0.1 to 30, 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	WiFi Multi-media (WMM) is a wireless Quality of Service (QoS) protocol making packets with higher priorities to be transmitted earlier. This ensures better QoS of voice and video applications over wireless networks.
APSD	<p>Automatic Power Save Delivery (APSD) is a WMM power saving protocol created by WiFi Alliance.</p> <p>Enabling APSD helps reduce power consumption. By default, this mode is disabled.</p>
Minimum RSSI Threshold	<p>Specifies the minimum strength of received signals acceptable to this CPE.</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 CPE.</p> <p>If there are multiple CPEs in a network, setting a proper value helps WiFi-enabled devices connect to a wireless network with better wireless signal.</p>
Preamble	<p>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 CPE to forward all packets. It is used to solve the problem that some NVRs cannot detect IP cameras, or cannot change the IP addresses of cameras in different networks.</p> <p> Tip</p> <ul style="list-style-type: none"> - This function is only applicable when the CPE works in AP, Client or Universal Repeater mode. - Transparent WDS and Transparent Bridge cannot be enabled at the same time.

Name	Description
ipMAX	<p>ipMAX is IP-COM's proprietary Time Division Multiple Access (TDMA) polling technology. It allows multiple clients to share the same channel for accessing to a network. With the ipMAX 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 ipMAX 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. - 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 ipMAX. <p> Tip</p> <p>If ipMAX is enabled, the CPE operates in ipMAX mode and only accepts connections from ipMAX WiFi-enabled devices (such as laptops, tablets, or smartphones).</p>
Signal Transmission	<p>Specifies the CPE's signal travel through wall capability.</p> <ul style="list-style-type: none"> - Coverage-oriented: With less interference nearby, this mode enables the device to cover wider area. - Capacity-oriented: With strong interference nearby, this mode improves the device's anti-interference capability.
TPC	<p>The Transmit Power Control (TPC) function decreases the TX power of this CPE automatically to improve the negotiation rate when the two CPEs are too close.</p> <p>By default, when the received signal strength is greater than -25 dBm, the CPE decreases its TX power.</p>
Signal Reception Level	<p>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>Specifies the wireless transmission distance of this CPE. You can set it based on the actual installation distance.</p> <p> Tip</p> <p>Modifying this distance will affect wireless transmission performance, and it is recommended to keep the default setting. If you want to set it manually, you should enter a value that is greater than the actual distance between the two CPEs.</p>

Name	Description
Beacon Interval	<p>Specifies the interval at which this CPE 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 CPE sooner, while a larger interval allows the wireless network to transmit data quicker.</p>
Fragment Threshold	<p>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 CPE 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>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>Specifies the countdown before this CPE transmits broadcast and multicast frames in its cache. The unit is Beacon interval.</p> <p>For example, if Delivery Traffic Indication Map (DTIM) Interval is set to 1, this CPE transmits all cached frames at one Beacon interval.</p>
Signal LED1/2/3 Threshold	<p>The CPE uses three signal LED indicators to indicate the received signal strength in an intuitive way, and allows you to customize the threshold for triggering each signal LED indicator to light up.</p> <p>The default threshold for LED1, LED2, and LED3 are -90, -80, and -70 respectively.</p>

7.3 Access control

7.3.1 Overview

The Access Control function enables you to allow or disallow the WiFi-enabled devices to access the wireless network based on their MAC addresses. This function is disabled by default.

7.3.2 Configure access control

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Wireless > Access Control**.
3. Enable the **Access Control** function.
4. Set the access control mode to **Allow** or **Disallow**.
5. Enter the target MAC address.
6. Click **Add**.



Tip

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

7. Click **Save**.

Access Control

SSID IP-COM_FAG37I

Access Control

Mode Disallow Allow

MAC Address Add Add online devices

SN	MAC Address	Status	Operation
1	12:12:12:12:12:12	<input checked="" type="checkbox"/> Enable	

Access Control List Save Cancel

----End

Parameters description

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

7.3.3 Example of configuring access control

Networking requirements

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

Solution

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

Configuration procedure

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Wireless > Access Control**.
3. Enable the **Access Control** function.
4. Set **Mode** to **Allow**.
5. Enter the MAC address, which is **C8:3A:35:00:00:01** in this example, and click **Add**.
6. Refer to step [5](#) to add the other two MAC addresses.
7. Click **Save**.

Access Control

SSID IP-COM_FAG37I

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 WiFi-enabled devices can connect to the wireless network of the CPE.

7.4 Management RF

7.4.1 Overview

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

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

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

Management RF
Current Mode: AP

?

Management RF

Enabled upon Power on

Duration mins

SSID

Network Mode


Channel


Encryption

Save

Cancel

Parameters description

Name	Description
Management RF	<p>Specifies whether to enable management WiFi of the CPE.</p> <p> Tip Management RF cannot turn itself off if it is enabled manually. The management WiFi is unprotected, so you'd better use it when necessary.</p>

Name	Description
Enabled upon Power on	<p>Specifies whether to enable the Enabled upon Power on function of the management RF.</p> <p>With this function enabled, the CPE's management RF will be automatically enabled when the CPE is powered off and on again or rebooted from the web UI.</p>
Duration	<p>Specifies the duration of management WiFi when it is enabled through a reboot.</p> <p>With management RF enabled, if the Duration is exceeded and the available time for management WiFi is not extended, the management WiFi will be automatically disabled.</p> <p> Tip</p> <p>If management RF is enabled through a reboot, you can extend the available time for management WiFi from the web UI of the CPE on your wireless device.</p>
SSID	Specifies the name of the management WiFi. You can modify it as required.
Network Mode	Specifies the wireless network mode of the CPE. Only wireless devices supporting the listed network mode can connect to the CPE.
Channel	Specifies the operating channel of the management WiFi. When Auto is selected, the CPE will automatically adjust its operating channel depending on the surrounding environment.
Encryption	Specifies the security mode of the management WiFi. See Security Mode for details.

7.4.2 Extend management WiFi duration

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

Configuration procedure

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

IP-COM Left until the page closed:4m 41s **Delay** Logout

Status Current Mode: AP

System Status

Device Name	CPE12V3.0	LAN Speed	1000 Mbps Full-...
Uptime	10 m17 s	LAN IP Address	192.168.2.1
System Time	2024-07-27 12:02:17	Transparent Bridge	Enabled
Firmware Version	V1.0.0.10(2547)	Hardware Version	V2.0
CPU	16%	RAM	78%
LAN MAC Address	[REDACTED]	WLAN MAC Address	[REDACTED]

----End



Tip

- To extend the available time of the management RF's wireless network, you must enable the Management RF function. As long as you extend the available time of wireless network before the wireless network of the management RF is automatically disabled, that is, you can normally use the wireless network of the management RF.
- Each time you click **Delay**, the maximum delay time is 5 minutes.
- The total delay time cannot exceed the [Duration](#). For example, if the **Duration** is 10 minutes, it means you can only delay to a maximum of 10 minutes.

8 Advanced

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and product version. Please refer to the actual product.

8.1 LAN rate

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

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

When you change the settings, ensure that the LAN speed and duplex mode of the 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**. CPE6SV2.0 is used for illustration.

The screenshot shows the 'LAN Rate' configuration page. It features four dropdown menus for setting the speed of different LAN ports: PoE/LAN Speed, LAN2 Speed, LAN3 Speed, and LAN4 Speed. All dropdowns are currently set to 'Auto Negotiation'. Below the dropdowns are two buttons: a red 'Save' button and a white 'Cancel' button. A red question mark icon is visible in the top right corner of the configuration area.

After the LAN speed and duplex mode settings are changed, you can check on the [System status](#) page.

Parameters description

Name	Description
Auto Negotiation	Specifies 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.
1000Mbps Full-Duplex	Specifies the port working at 1000 Mbps, and can transmit and receive packets at the same time.

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



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

8.2 Diagnose

To access the page, [log in to the web UI](#) of the CPE and navigate to **Advanced > Diagnose**.

You can use the diagnosis tools for troubleshooting.

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

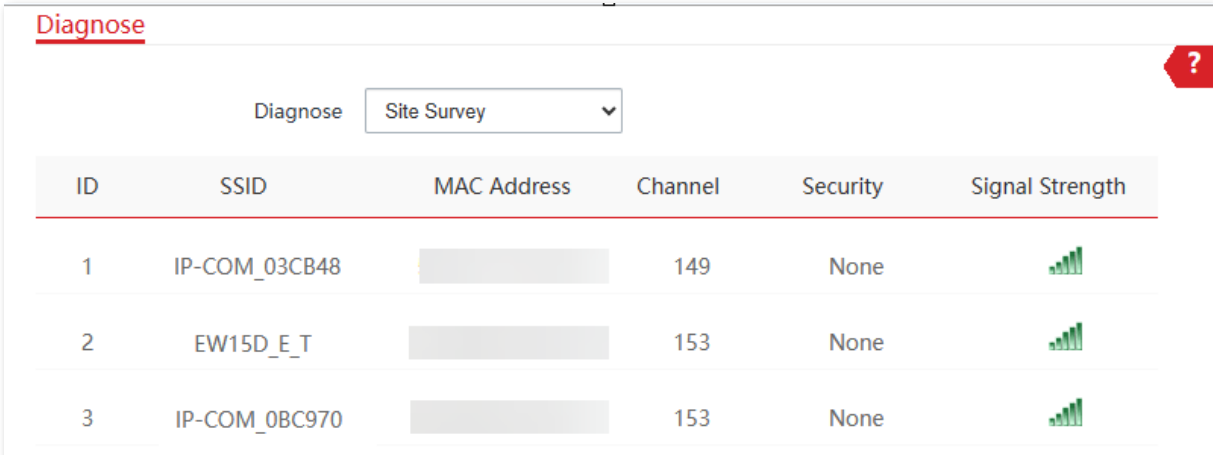
Site survey gives you an insight into the information of nearby wireless signals. According to the diagnosis result, you can select a channel that is least used for the CPE to improve the transmission efficiency.




Configuration procedure

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

----End

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



ID	SSID	MAC Address	Channel	Security	Signal Strength
1	IP-COM_03CB48	[REDACTED]	149	None	
2	EW15D_E_T	[REDACTED]	153	None	
3	IP-COM_0BC970	[REDACTED]	153	None	

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 CPE can access **Bing**.

Configuration procedure

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

The screenshot shows the 'Diagnose' configuration page. At the top left, the word 'Diagnose' is underlined in red. In the top right corner, there is a red question mark icon. The configuration fields are as follows:

- Diagnose:** A dropdown menu with 'Ping' selected.
- IP Address:** A dropdown menu with 'Manual' selected.
- IP Address/Domain Name:** A text input field containing 'cn.bing.com'.
- Ping Packet:** A text input field containing '4', with '(Range: 1 to 10000)' displayed to its right.
- Packet Size:** A text input field containing '32', with 'Byte (Range: 1 to 60000)' displayed to its right.
- Start:** A red button located at the bottom center of the form.

----End

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

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 CPE to destination host.

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

Configuration procedure

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

The screenshot shows the 'Diagnose' section of a web interface. At the top left, the word 'Diagnose' is underlined in red. On the right side, there is a red question mark icon. Below the title, there is a 'Diagnose' label followed by a dropdown menu currently set to 'Traceroute'. Underneath, there is a label 'IP Address/Domain Name' followed by a text input field containing 'cn.bing.com'. At the bottom center, there is a red 'Start' button.

----End

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

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

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 can use the **Speed Test** function.

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

The screenshot shows the 'Diagnose' web interface. At the top, there is a 'Diagnose' dropdown menu set to 'Speed Test'. Below this, a summary bar displays three metrics: 'AVG RX' (0 Mbps), 'AVG TX' (0 Mbps), and 'AVG Total' (0 Mbps). Underneath, there are radio buttons for 'Client' (selected) and 'Server'. The 'IP Address of Peer AP' is set to 'Manual'. Below that are input fields for 'IP Address', 'HTTP Port' (80), 'User Name', and 'Password'. The 'Test Group' is set to '10' with a range of 1 to 20. The 'Direction' is set to 'Bidirectional'. The 'Time' is set to '30' seconds with a range of 1 to 60. A red 'Start' button is at the bottom.

Parameters description

Name	Description
AVG RX	Specifies the average receive rate.
AVG TX	Specifies the average transmit rate.
AVG Total	Specifies the average total rate.
Client	This version is not supported yet.
Server	

Name	Description
IP Address of Peer AP	Specifies the LAN IP address of the peer CPE. You can enter it manually or select the IP address of the peer AP from the drop-down list if there are peer CPEs connected to the CPE.
IP Address	If the IP Address of Peer AP is set to Manual , you need to manually enter the LAN IP address of peer CPE here.
HTTP Port	Specifies the HTTP service port number of peer CPE, which is used to establish speed test connection based on TCP/IP. The default value is 80 . You are recommended to keep the default value.
User Name	Specify the login user name and password of the peer CPE.
Password	
Test Group	Specifies the number of test connections established.
Direction	<p>Specifies the test direction.</p> <ul style="list-style-type: none"> - RX: Only test the speed that this device receives data from the peer CPE. - TX: Only test the speed that this device transmits data to the peer CPE. - Bidirectional: Test both transmit and receive speed between the two CPEs.
Time	Specifies the duration of speed test, which is 30s by default.

Example of configuring the speed test

Assume that CPE1 works in AP mode and CPE2 works in Client mode have bridged successfully. Below shows basic information about two CPEs:

- IP address of the CPE1: **192.168.2.1**
- IP address of CPE2: **192.168.2.10**
- Login user names/passwords of the two CPEs: **admin**

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

Configuration procedure

1. [Log in to the web UI](#) of the CPE2.
2. Navigate to **Advanced > Diagnose**.
3. Select **Speed Test** in the **Diagnose** drop-down list.

4. Set **IP Address of Peer AP** to **Manual**.
5. Enter the IP address of CPE1 in the **IP Address** field, which is **192.168.2.1** in this example.
6. Enter the login user name and password of the web UI of the CPE1 in the **User name** and **Password** fields, which are both **admin** in this example.
7. Set **Direction** to **Bidirectional**.
8. Click **Start**.

Diagnose

Diagnose Speed Test

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

Client Server

IP Address of Peer AP Manual

IP Address 192.168.2.1

HTTP Port 80

User Name admin

Password admin

Test Group 10 (Range: 1 to 20)

Direction Bidirectional

Time 30 s (Range: 1 to 60)

Start

----End

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

Diagnose

Diagnose Speed Test

↑ AVG RX	↓ AVG TX	↕ AVG Total
8.83 Mbps	0 Mbps	4.86 Mbps

8.2.5 Spectrum analysis

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



- CPEs to bridge must operate in the same channel.
- All wireless connections are disconnected during a spectrum analysis. Operate when the network is idle.

Measure channel utilization

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

The screenshot shows the 'Diagnose' section of a web interface. Under the 'Diagnose' heading, there is a dropdown menu set to 'Spectrum Analysis'. Below this, there are two radio buttons: 'Channel Utilization' (which is selected) and 'Noise Intensity'. At the bottom, there are two dropdown menus for 'Frequency Band', with the first set to '36(5180MHz)' and the second to '48(5240MHz)'. A red 'Start' button is positioned below the frequency band dropdowns.

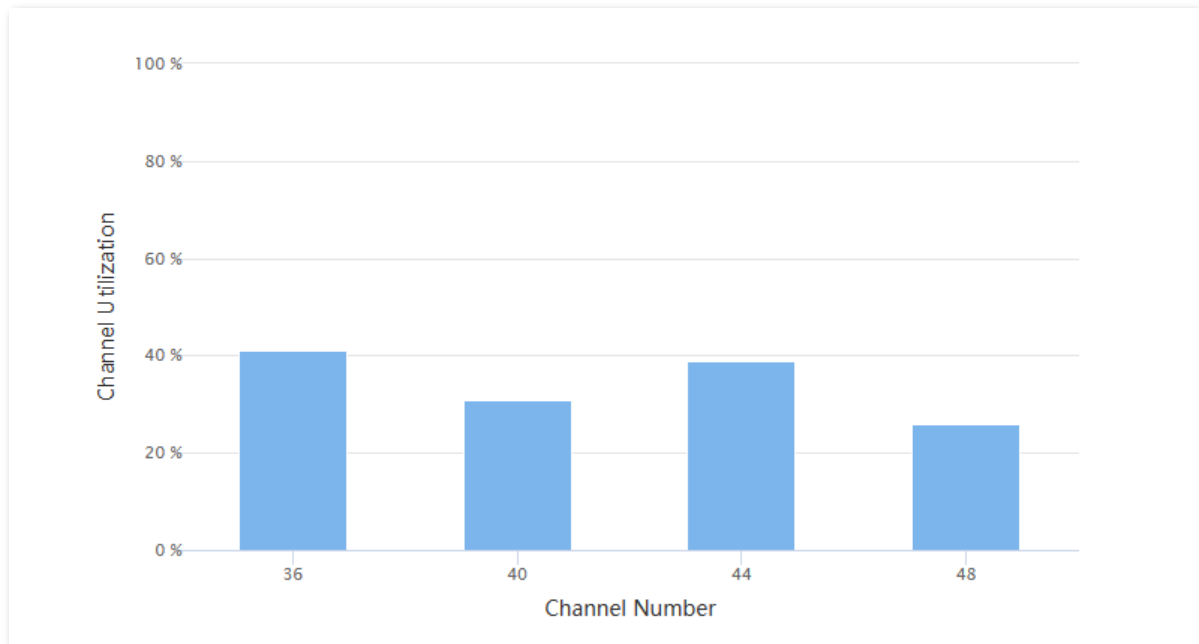
7. Confirm the prompt information, and click **OK**.

The screenshot shows a 'Note' dialog box with a close button (X) in the top right corner. The text inside the dialog reads: 'All wireless connections will be terminated when the spectrum analysis is launching on the device! Please click OK to Start.' At the bottom of the dialog, there are two buttons: a red 'OK' button and a white 'Cancel' button.

----End

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

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



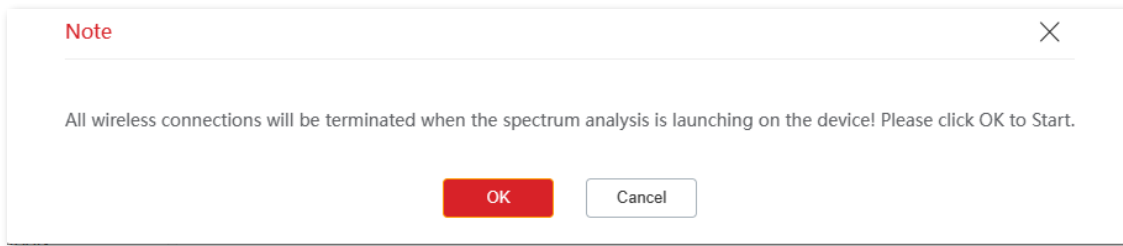
Measure noise intensity

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

The screenshot shows the 'Diagnose' interface with the following settings:

- Diagnose: Spectrum Analysis
- Channel Utilization:
- Noise Intensity:
- Average Value:
- Frequency Band: 36(5180MHz) to 48(5240MHz)
- Start:

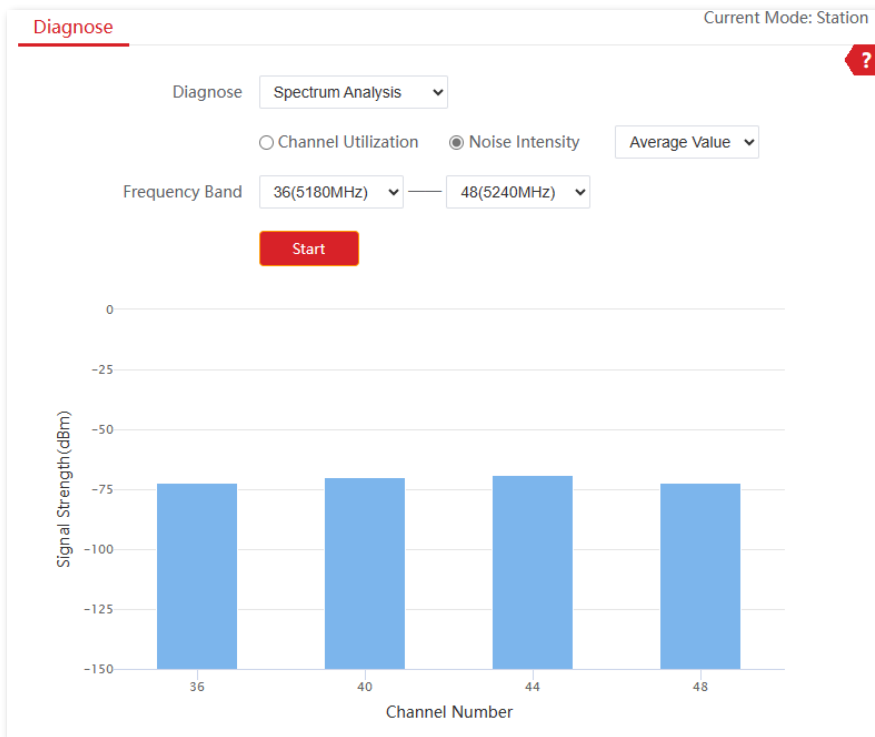
8. Confirm the prompt information, and click **OK**.



----End

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

Based on the diagnosis result, the CPE can be set to channel 36 or 48 for optimal transmission.



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, [log in to the web UI](#) of the CPE and navigate to **Advanced > Bandwidth Control**. The following figure is for reference only.

The screenshot shows the 'Bandwidth Control' configuration page in 'Router' mode. It features a form with the following fields:

- Remark:** A text input field.
- IP Address Range:** Two input boxes with a tilde (~) between them, showing '192.168.2.' as an example.
- Max. Upload Rate:** A text input field with a 'Mbps' dropdown menu.
- Max. Download Rate:** A text input field with a 'Mbps' dropdown menu.

Below the form is a red 'Add' button. At the bottom of the page, there is a table with the following columns: ID, Remark, IP Address Range, Max. Upload Rate, Max. Download Rate, Status, and Action.

Parameters description

Name	Description
Remark	Specifies the description of the bandwidth control rule. This field is optional. For convenient management, you'd better specify different remarks for different rules.
IP Address Range	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	Specify the maximum upload/download rate of a device whose IP address is within the specified IP Address Range.
Max. Download Rate	
Status	Specifies the current status of the rule. You can enable or disable it as required.
Action	Click  to delete the rule.

8.3.2 Example of configuring bandwidth control

Networking requirements

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

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

Configuration procedure

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Advanced > Bandwidth Control**.
3. (Optional) Enter a remark, which is **Office_1** in this example.
4. Set **IP Address Range**, which is **192.168.2.100 ~ 192.168.2.200** in this example.
5. Set the maximum upload and download rates, which are **5 Mbps** and **10 Mbps** in this example.
6. Click **Add**.

The screenshot shows the 'Bandwidth Control' configuration interface. At the top right, it indicates 'Current Mode: WISP'. The form contains the following fields:

- Remark:** Office_1
- IP Address Range:** 192.168.2.100 ~ 192.168.2.100
- Max. Upload Rate:** 5 Mbps
- Max. Download Rate:** 10 Mbps

An 'Add' button is located at the bottom center of the form.

----End

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

ID	Remark	IP Address Range	Max. Upload Rate	Max. Download Rate	Status	Action
1	Offic_1	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.

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


The screenshot shows the 'Port Forwarding' configuration page. At the top right, it says 'Current Mode: Router'. The form contains the following fields:

- Internal IP Address: [Empty text box]
- Internal Port: [23]
- External Port: [23]
- Protocol: [TCP&UDP]
- Application: [Telnet]

At the bottom of the form is a red 'Add' button. There is also a red question mark icon in the top right corner of the form area.

Parameters description

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

Name	Description
External Port	Specifies the ports which are enabled for WAN users to visit the corresponding servers in LAN. After you select an Application , this option will be auto populated. You can also customize it.
Protocol	Specifies the protocol type of the selected applications. Select TCP&UDP when you are not sure.
Application	Specifies the application services established in LAN. The device provides some common services. After you select an application, the internal and external ports will be populated.
Status	Specifies the status of the rule. You can enable or disable it according to your need.
Action	Click  to delete the rule.

8.4.2 Example of configuring port forwarding

Networking requirements

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

The intranet web server is open to internet users to enable staff to access the intranet even when they are not physically in the enterprise.

Solution

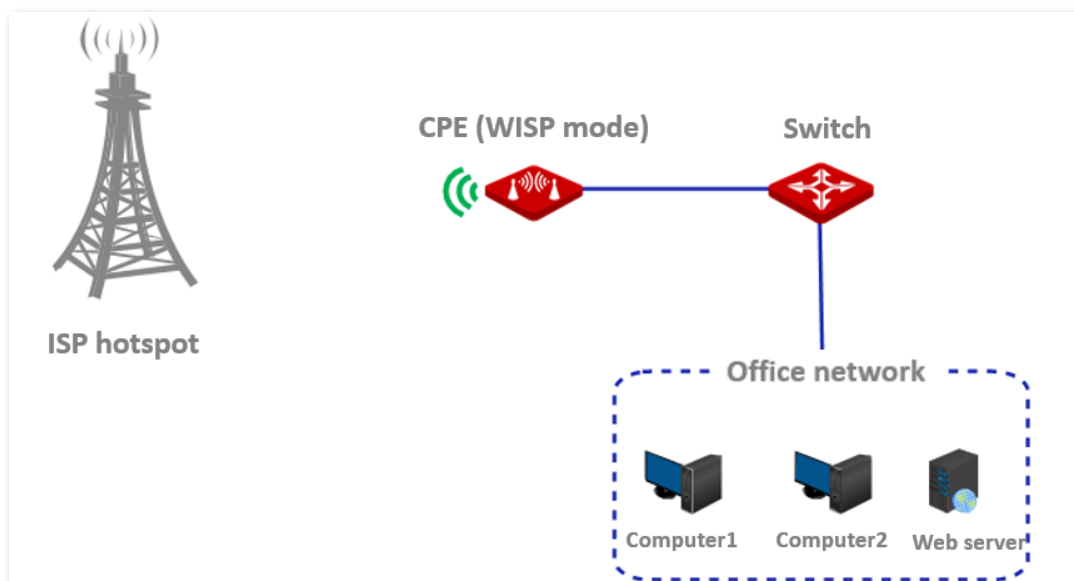
You can use the port forwarding function to enable internet users to access the intranet web server.

Assume that:

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



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



Configuration procedure

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

Port Forwarding
Current Mode: Router

Internal IP Address

Internal Port

External Port

Protocol

Application

Add

----End

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

ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	9999	9999	TCP&UDP	HTTP	<input checked="" type="checkbox"/> Enable	

10 Datas/Page 1 data in total

Verification

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

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

You can find the current WAN port IP address in [System status](#).

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



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 restrict access to devices by their MAC addresses at specific times.

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

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

Parameters description

Name	Description
Mode	<p>Specifies the mode of MAC filter rule.</p> <ul style="list-style-type: none"> - Disable: Disable the MAC Filter function. - Allow: Only allow devices with the MAC addresses in the list to access the internet with the CPE. - Disallow: Only disallow devices with the MAC addresses in the list to access the internet with the CPE.
Remark	Specifies the additional information of the rule.
MAC Address	Specifies the MAC address of the device to which the rule applies.

Name	Description
Time	Specifies the period at which the rule takes effect.
Date	Specifies the dates on which the rule takes effect.
Status	Specifies the status of the rule. You can enable or disable the rule according to your need.
Action	Click  to delete the rule.

8.5.2 Example of configuring MAC filter

Networking requirements

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

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

Solution

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

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

Configuration procedure

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

MAC Filter

Mode:

Remark:

MAC Address:

Time: : ~ :

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

----End

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

ID	Remark	MAC Address	Time	Mode	Status	Action
1	Purchasing	CC:3A:61:71:1B:6E	Mon. , Tue. , Wed. , Thur. , Fri. 00:00-00:00	Allow	<input checked="" type="checkbox"/> Enable	

10 Datas/Page 1 data in total

Verification

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

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

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

The screenshot shows the 'Network Service' configuration page in 'Router' mode. At the top right, it says 'Current Mode: Router'. The main heading is 'Network Service'. Below it, there is a 'DDNS' toggle switch which is currently turned off. Underneath, there are several fields: 'Service Provider' is a dropdown menu showing '3322.org' with a 'Register' link to its right; 'User Name', 'Password', and 'Domain Name' are all empty text input fields.

Parameters description

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

Example of configuring DDNS

Networking requirements

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

Requirements: The intranet web server is open to internet users to enable staff to access the intranet even when they are not in the enterprise.

Solution

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

Assume that:

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

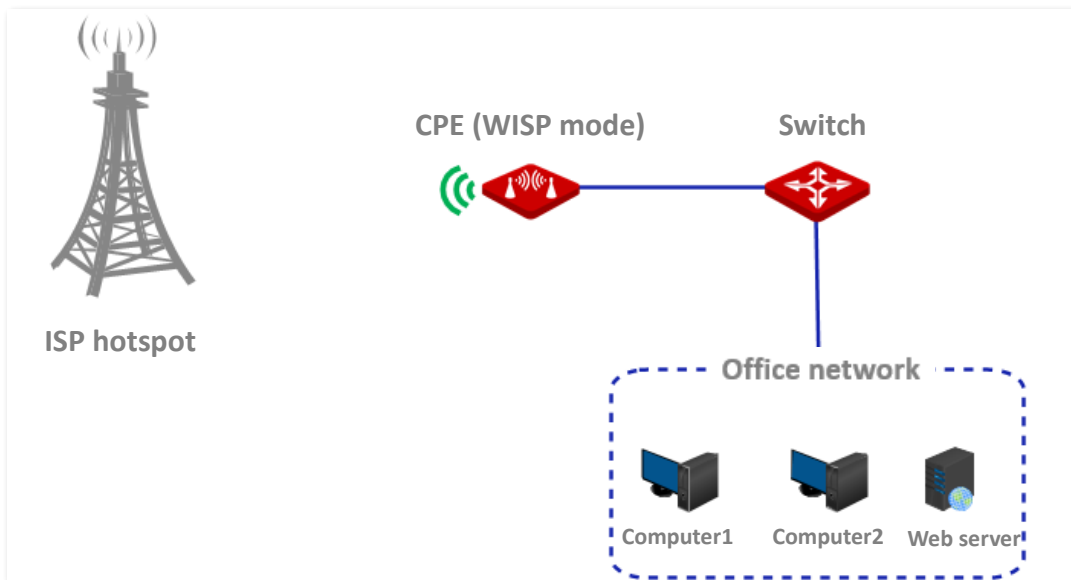
- IP Address: **192.168.2.100**
- Service Port of the Web Server: **9999**

The registered domain name information is shown as below:

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



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



Configuration procedure

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

DDNS

Service Provider [Register](#)

User Name

Password

Domain Name

3. Set up the port forwarding function.
 - 1) Navigate to **Advanced > Port Forwarding**.
 - 2) Set **Internal IP Address**, which is **192.168.2.100** in this example.
 - 3) Set **Internal Port** and **External Port**, which are **9999** in this example.
 - 4) Set **Protocol**, which is **TCP&UDP** in this example

- 5) Set **Application**, which is **HTTP** in this example.
- 6) Click **Add**.

Port Forwarding
Current Mode: Router

Internal IP Address

Internal Port

External Port

Protocol

Application

Add

----End

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

ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	9999	9999	TCP&UDP	HTTP	<input checked="" type="checkbox"/> Enable	

10 Datas/Page 1 data in total

Verification

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

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



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

You can access the CPE remotely by visiting an address in the form of **http://WAN port's 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://WAN port's domain name:Port number**.

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

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

Parameters description

Name	Description
Remote Web Management	Specifies whether to enable the remote web management function.
IP Address	<p>Specifies the IP address of a computer 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 computer belongs to a LAN, enter the gateway address (a public IP address) of the computer.
Port	<p>Specifies the port number used for remote management of CPE. Default: 8080. You can change it as required.</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.</p>

Example of configuring remote web management

Networking requirements

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

The network administrator encountered a problem during network setup and needs the IP-COM technical support to remotely log in to the web UI of the CPE to perform analysis and troubleshooting.

Solution

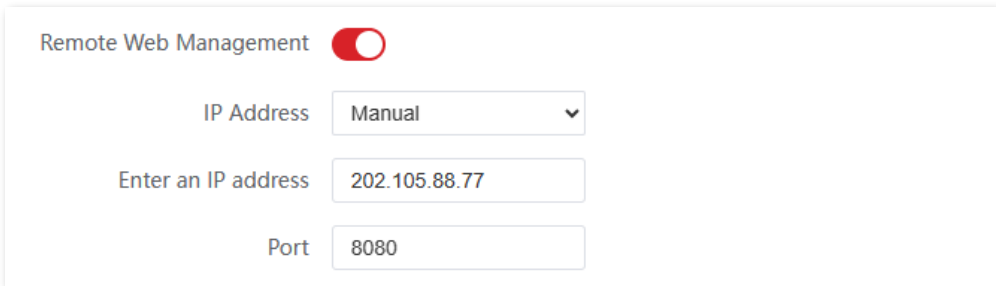
You can use the remote web management function to solve the problem.

Assume that:

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

Configuration procedure

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Advanced > Network Service**.
3. Enable the **Remote Web Management** function.
4. Set **IP Address** to **Manual**.
5. Enter the IP address of the computer supported by IP-COM technology, which is **202.105.88.77** in this example.
6. Set **Port**, which is **8080** in this example.
7. Click **Save** in the bottom of this page.



Remote Web Management

IP Address

Enter an IP address

Port

----End

Verification

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

8.6.3 Reboot schedule

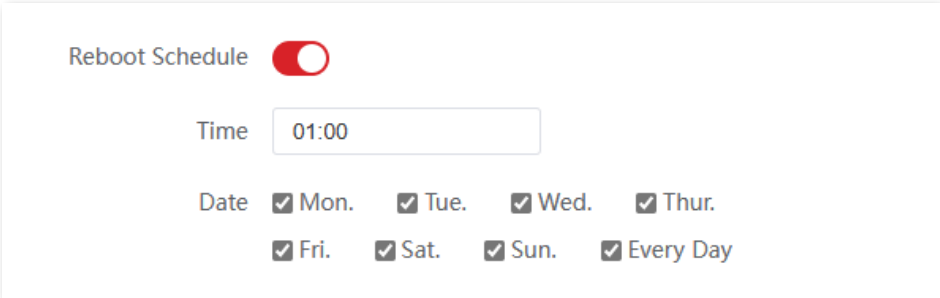
Overview

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

This function enables the CPE to automatically reboot as scheduled. You can use this function to prevent wireless performance degradation or network instability due to long-time running.

Configuration procedure

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Advanced > Network Service**.
3. Enable the **Reboot Schedule** function.
4. Set **Time** at which the CPE reboots, which is **01:00** in this example.
5. Set **Date** on which the CPE reboots, which is **Every Day** in this example.
6. Click **Save** on the bottom of this page.



Reboot Schedule

Time

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

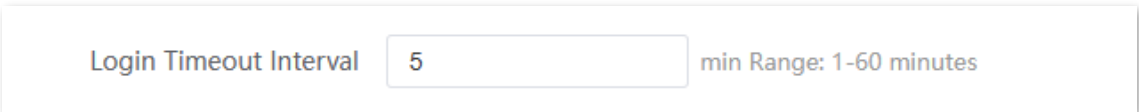
----End

After successfully configured, the CPE will automatically reboot at 1 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. You can modify it as required.

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



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.

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

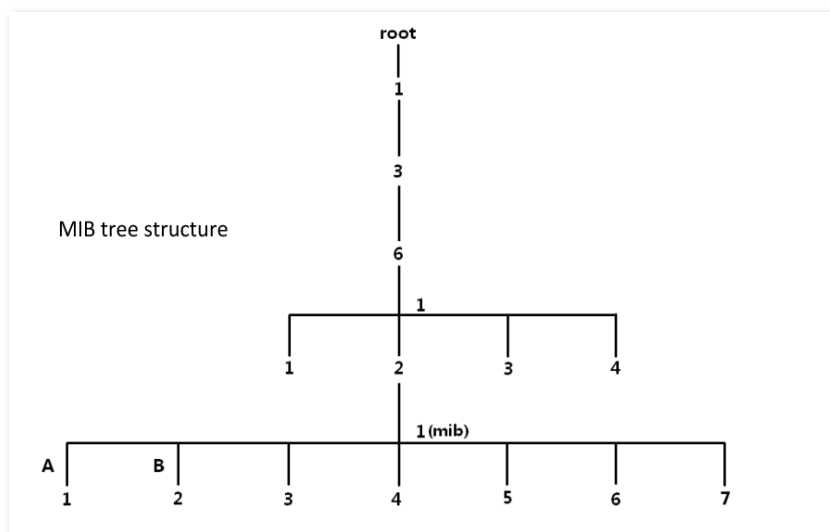
The device is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. Community name is used to define the relationship between an SNMP agent and an SNMP manager. If the community name contained in an SNMP packet is

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 error identification.

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.



SNMP agent basic configuration

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

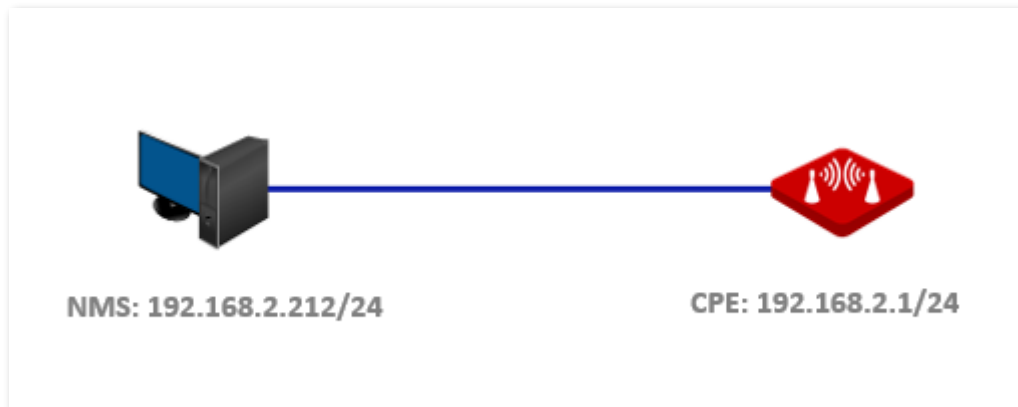
SNMP Agent	<input checked="" type="checkbox"/>
Device Name	<input type="text" value="CPE12V3.0"/>
Read Community	<input type="text" value="public"/>
Read/Write Community	<input type="text" value="private"/>
Location	<input type="text" value="ShenZhen"/>

Name	Description
SNMP Agent	<p>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>Specifies the device name of the CPE. The default device name is assigned based on 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>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 Read Community to read variables in the MIB of the device.</p>
Read/Write Community	<p>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 Read/Write Community to read/write variables in the MIB of the device.</p>
Location	<p>Specifies the location where the CPE is used. You can change the location as required.</p>

Example of configuring the SNMP function

Networking requirements

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



Configuration procedure

1. Set up the CPE.
 - 1) [Log in to the web UI](#) of the CPE.
 - 2) Navigate to **Advanced > Network Service**.
 - 3) Enable the **SNMP Agent** function.
 - 4) Set **Read Community**, which is **FLASH** in this example.
 - 5) Set **Read/Write Community**, which is **FLASH-11** in this example.
 - 6) Click **Save** on the bottom of this page.

SNMP Agent	<input checked="" type="checkbox"/>
Device Name	<input type="text" value="CPE12V3.0"/>
Read Community	<input type="text" value="FLASH"/>
Read/Write Community	<input type="text" value="FLASH_1"/>
Location	<input type="text" value="ShenZhen"/>

2. Set up the NMS.

On an NMS that uses SNMP V1 or SNMP V2C, set the read community to **FLASH** and read/write community to **FLASH-11**. For details about how to configure the NMS, refer to the user guide for the NMS.

----End

Verification

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

8.6.6 Ping watch dog

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

With this function enabled, the CPE periodically pings 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 procedure

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

Ping Watch Dog

IP Address

Ping Interval Range: 20-86400 s

Ping Startup Delay Range: 180-86400 s

Threshold of Lost Packets

----End

Parameters description

Name	Description
Ping Watch Dog	Specifies whether to enable the Ping Watch Dog function.

Name	Description
IP Address	Specifies the target IP address that the CPE pings.
Ping Interval	Specifies the interval at which the CPE transmits packets to ping the target IP address. The default value is 300s.
Ping Startup Delay	Specifies the delay time for the CPE to enable the Ping Watch Dog function after the CPE startup completes. The default value is 300s. Setting a proper Ping startup delay time can stop the Ping Watch Dog function from being triggered during the startup of the CPE. Such triggering leads to failure of accessing the web UI to modify the settings, causing the CPE to start up continuously.
Threshold of Lost Packets	Specifies the threshold of lost packets to reboot the CPE. The value range is 1 to 65535. The default value is 3. For example, if the threshold is set to 5, the CPE 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.

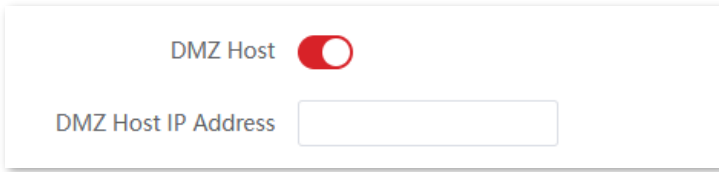
After a device in the LAN is set as the DMZ host, the device enjoys no limitations when communicating with the internet. For example, if video meeting or online games are underway on a computer, you can set that computer as the DMZ host to make the video meeting and online games go smoother.



Tip

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

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



Parameters description

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

Example of configuring DMZ host

Networking requirements

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

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

Solution

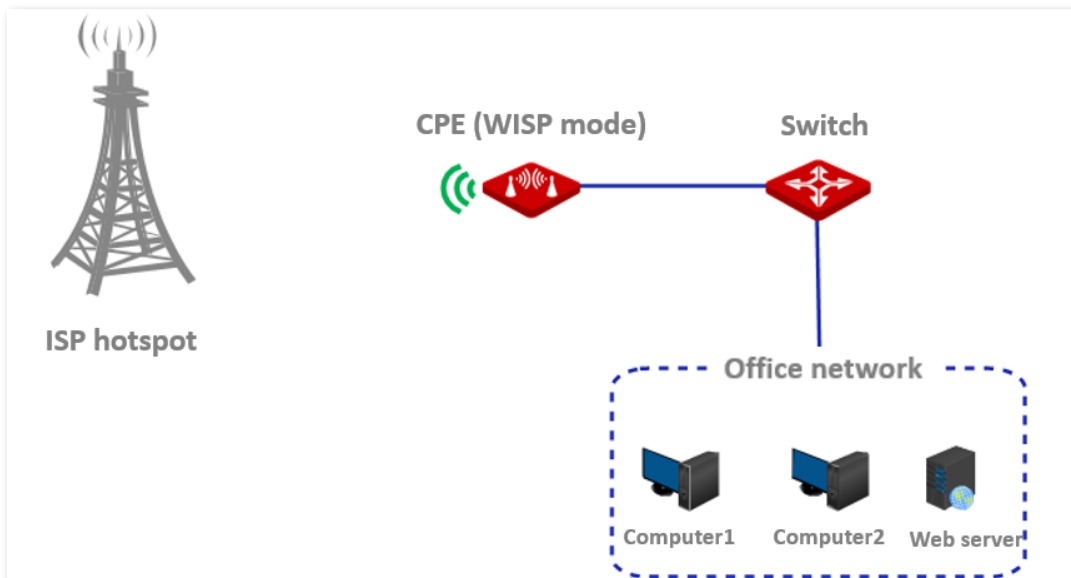
You can use DMZ Host function to solve the problem.

Assume that:

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



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



Configuration procedure

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

DMZ Host

DMZ Host IP Address

----End

Verification

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

In this example, the access address is <http://202.105.11.22:9999>. You can find the current WAN port's IP address in [System status](#).

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



Tip

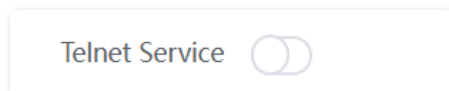
If internet users cannot visit the server in LAN after the configuration, try the following solutions:

- Ensure that the WAN IP address of the CPE is a public IP address.
- 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 through the Telnet. Generally, this function is used to maintain the CPE by technical professional.

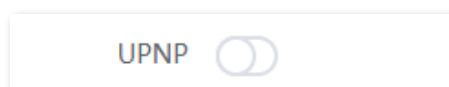
To access the page, [log in to the web UI](#) of the CPE and navigate to **Advanced** > **Network Service**.



8.6.9 UPnP

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

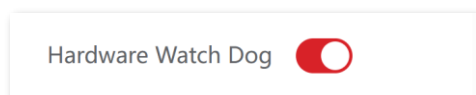
To access the page, [log in to the web UI](#) of the CPE and navigate to **Advanced** > **Network Service**. By default, the function is disabled. You can enable it as required.



8.6.10 Hardware watch dog

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

To access the page, [log in to the web UI](#) of the CPE and navigate to **Advanced** > **Network Service**. By default, the function is enabled.



9 Tools

This user guide is for configuration reference only and does not indicate that the product supports all functions described here. Functions available may vary with the product model and product version. Please refer to the actual product.

9.1 Date & time

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

This module enables you to set the system time of the CPE. To ensure that the time-based functions of the CPE are effective, it is necessary to ensure that the system time of the CPE is accurate.

The system time of the CPE can be [synchronized with the internet](#) or [set manually](#). 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 Sync system time with internet

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

For details about how to connect the CPE to the internet, refer to [LAN setup](#).

Configuration Procedure

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

----End

After the configuration is completed, you can navigate to [Status](#) page to check whether the system time of the CPE is correct.

Parameters description

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

9.1.2 Set system time manually

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

Configuration procedure

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

Date & Time
Current Mode: AP

?

Time Settings Synchronized with the Internet Manual

Date & Time Y M D h m s

----End

After the configuration is completed, you can navigate to [Status](#) page to check whether the system time of the CPE is correct.

Parameters description

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

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.

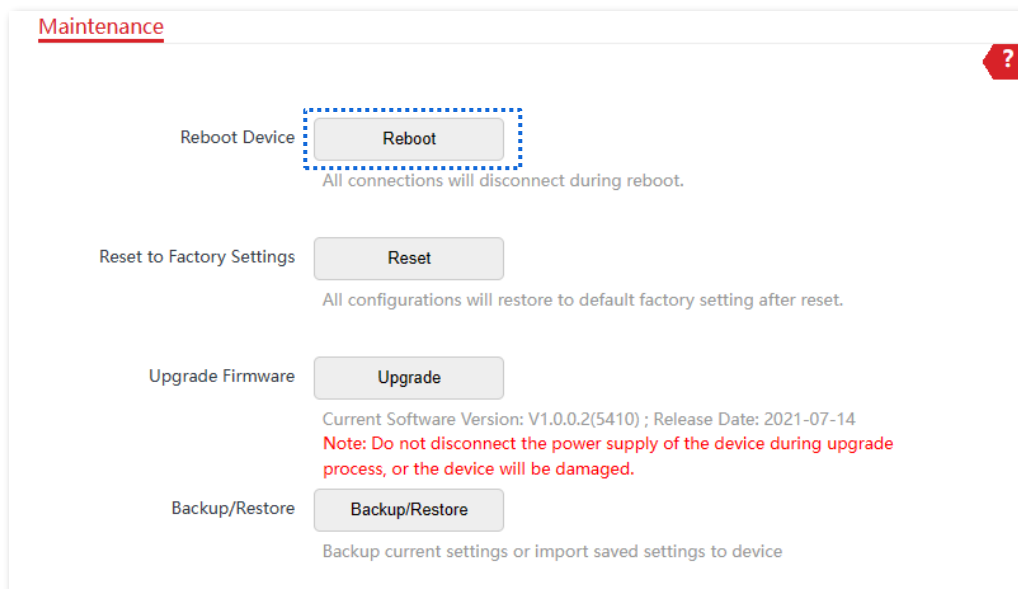


Tip

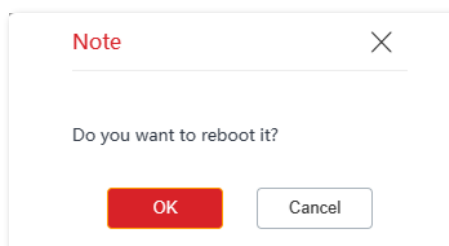
When the device reboots, the current connections will be disconnected. Perform this operation when the device is idle.

Configuration procedure

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Tools > Maintenance**.
3. Click **Reboot**.



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



----End

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

9.2.2 Restore to factory settings

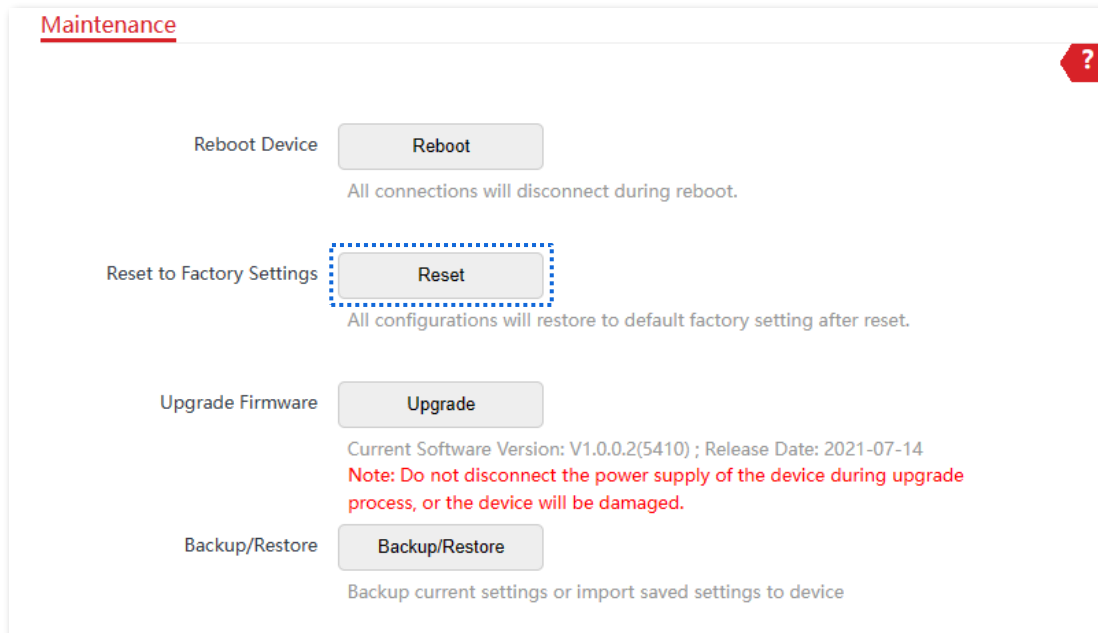
If you forget the login password of the web UI, you can reset the CPE to restore its factory settings and then configure it again.

Note

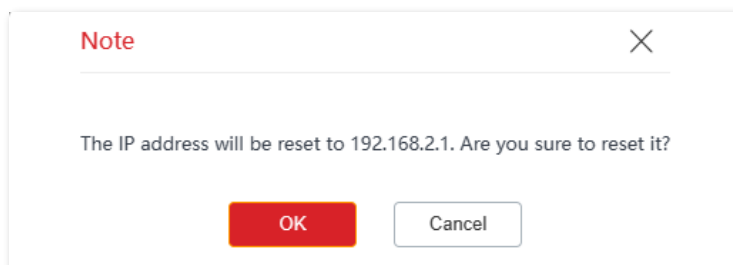
- When the factory settings are restored, the user configuration of the CPE is cleared, and you need to re-configure the CPE. Reset the CPE with caution.
- To prevent damages to the device, do not power off the CPE during resetting.

Option 1: Reset the CPE through the web UI

1. [Log in to the web UI](#) of the CPE.
2. Navigate to **Tools > Maintenance**.
3. Click **Reset**.



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



----End

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

Option 2: Reset the CPE through the Reset button

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

9.2.3 Upgrade firmware

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



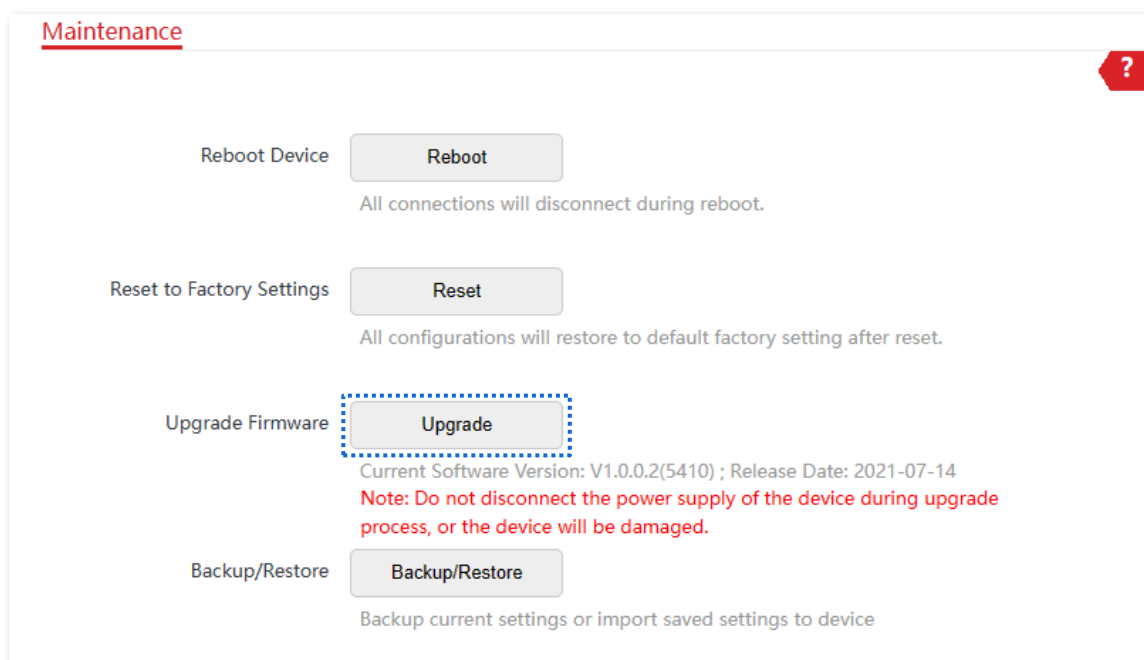
Note

To prevent damaging the device, 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 procedure

1. Download the firmware upgrade package for the CPE from www.ip-com.com.cn to your local computer, and decompress the package.
2. [Log in to the web UI](#) of CPE, and navigate to **Tools > Maintenance**.
3. Click **Upgrade**.



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

----End

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



After the CPE is upgraded, you are recommended to restore the factory settings of the CPE and configure it again to get the better experience.

9.2.4 Backup/Restore

The **Backup** function enables you to export the current configuration of the CPE to a local computer. The **Restore** function enables you to import the configuration file you export before.

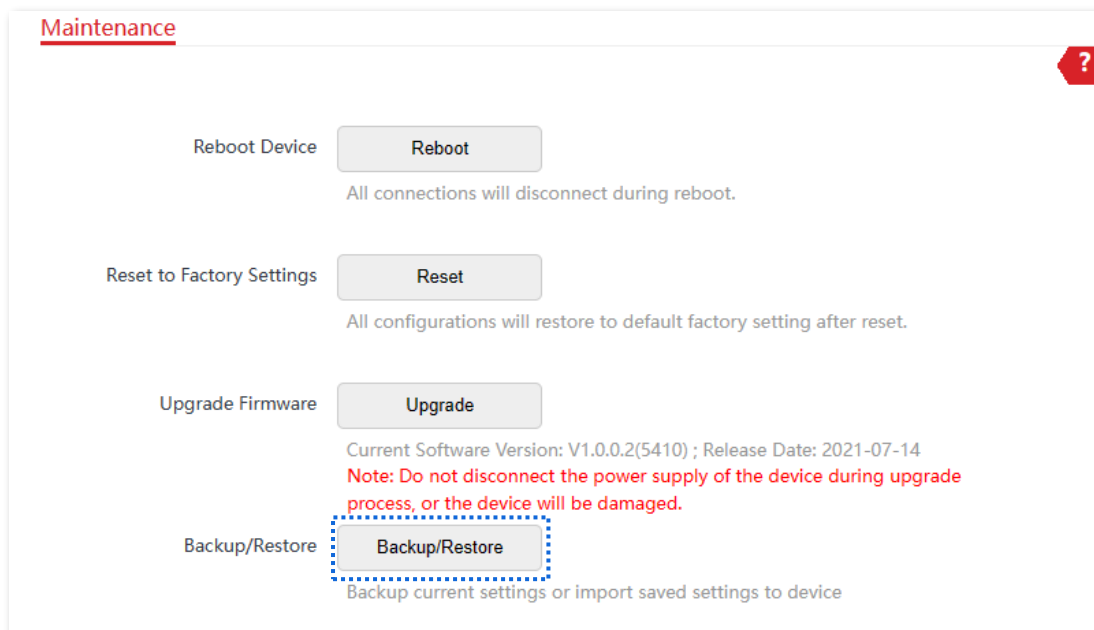
You are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the CPE, or import the configuration to other devices of the same product model.



If you need to apply configurations to multiple devices, you can configure one device, back up its configuration, and import the backup file to restore the configuration on the other devices. This improves configuration efficiency.

Backup

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



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



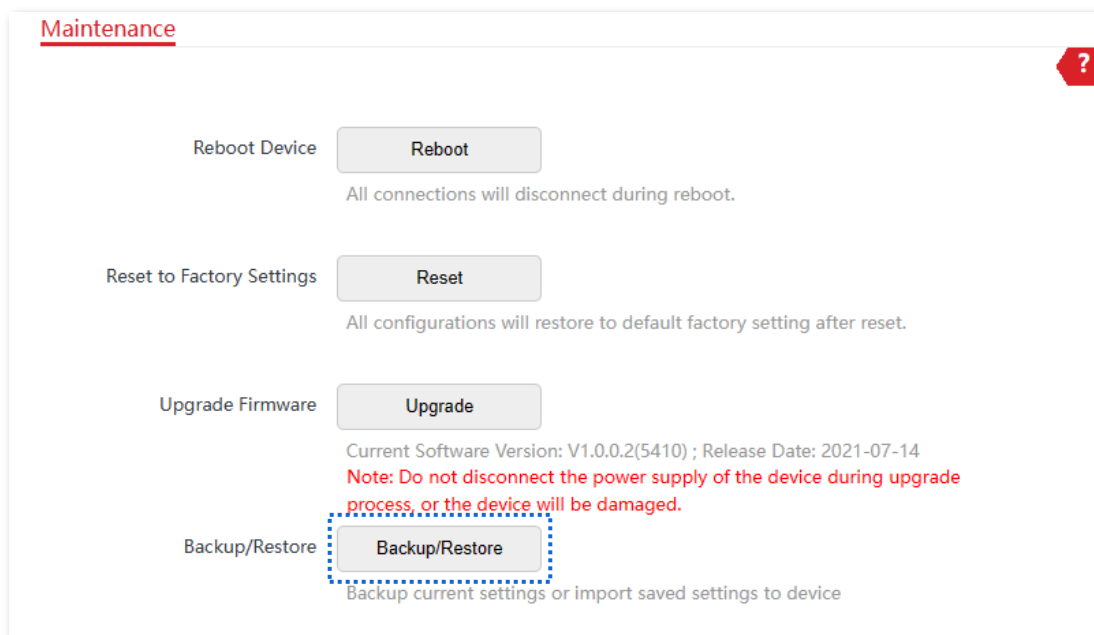
5. Confirm the prompt information, and click **Save**.

----End

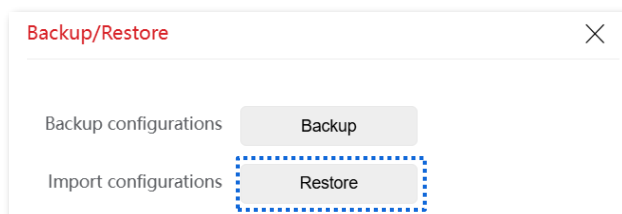
A file named **APCfm.cfg** is downloaded to your local computer.

Restore

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



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



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


----End

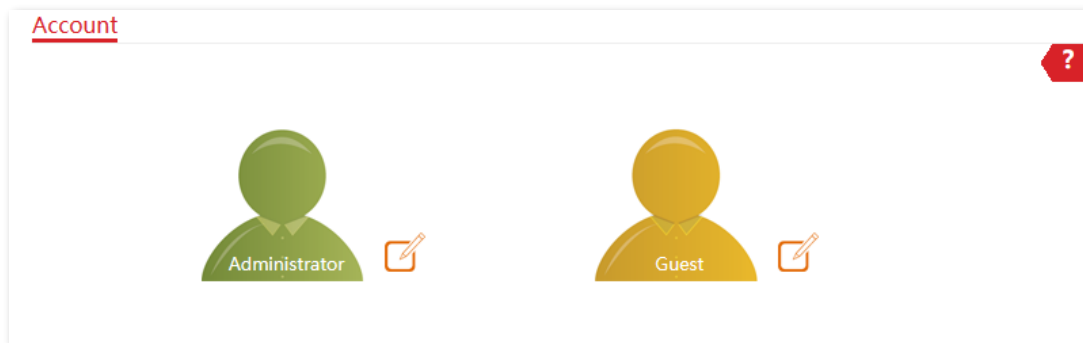
After the file is uploaded, the CPE reboots automatically. Wait for the progress bar to complete. Then the CPE is restored to the settings successfully.

9.3 Account

To access the page, [log in to the web UI](#) of the CPE and navigate to **Tools > Account**.

On this page, you can change the login account information of the CPE to prevent unauthorized login. 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 CPE while with the guest account, you can only view the settings.

Click  to change the account information.

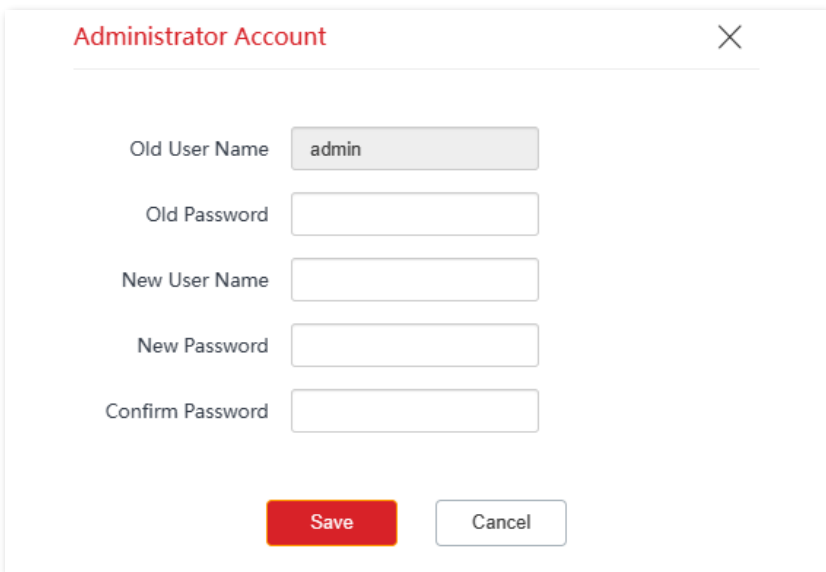


9.3.1 Administrator

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 strong password is preferred, such as a combination of lower-case letters, capital letters and numbers.


 A dialog box titled 'Administrator Account' with a close button (X) in the top right. 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: a red 'Save' button and a white 'Cancel' button.

Parameters description

Name	Description
Old User Name	Specifies the user name and password of the current login account. By default, the CPE has one administrator account and one guest account.
Old Password	Administrator user name/password: admin Guest user name/password: user
New User Name	Specifies a new login user name.
New Password	Specifies a new login password.
Confirm Password	Enter the new login password again.

9.3.2 Guest

Guest 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

Save

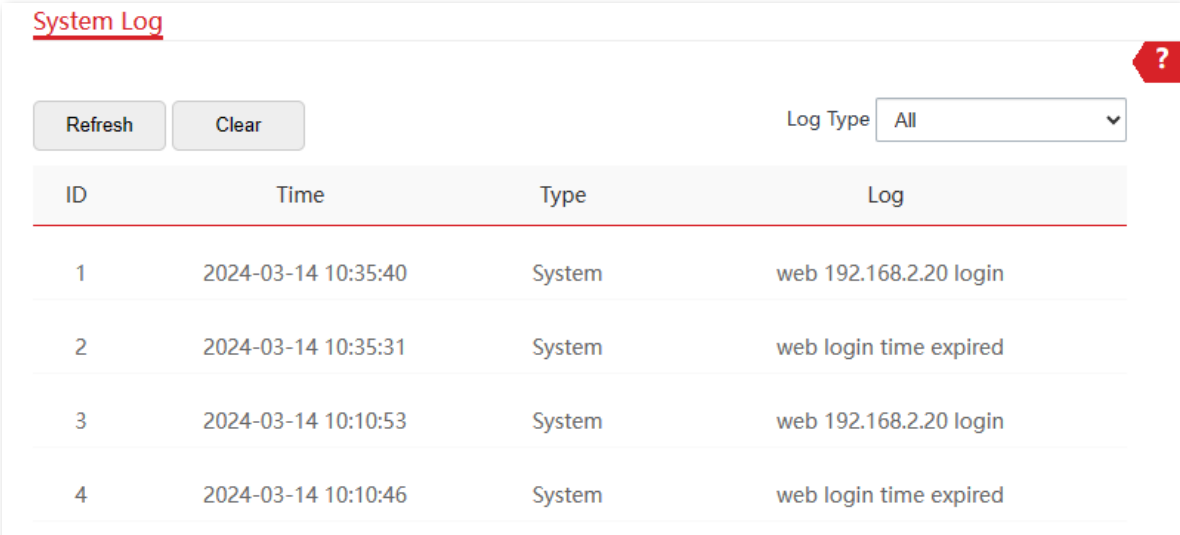
Cancel

9.4 System log

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

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

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



ID	Time	Type	Log
1	2024-03-14 10:35:40	System	web 192.168.2.20 login
2	2024-03-14 10:35:31	System	web login time expired
3	2024-03-14 10:10:53	System	web 192.168.2.20 login
4	2024-03-14 10:10:46	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 on the [Date & Time](#) page.

Note



- When the CPE reboots, the previous logs are removed.
- The CPE reboots when one of the following situations occurs: the CPE is powered on after a power failure, the VLAN function is configured, the firmware is upgraded, the configuration of the CPE 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	Single	192.168.2.1
		Kit	AP mode: 192.168.2.1 Client mode: 192.168.2.2
	Administrator	User name	admin
		Password	admin
Guest		Disable	
Quick Setup	Working Mode	Single	AP mode
		Kit	AP mode or Client mode
	IP Address Type		Static IP address
LAN Setup	IP Address	Single	192.168.2.1
		Kit	AP mode: 192.168.2.1 Client mode: 192.168.2.2
	Subnet Mask		255.255.255.0
DHCP Server	DHCP Server	Single	Enable
		Kit	Disable
	Start IP Address		192.168.2.100
	End IP Address		192.168.2.200
	Subnet Mask		255.255.255.0
	Gateway Address		192.168.2.254

Parameters		Default settings	
	Primary DNS Server	8.8.8.8	
	Lease Time	1 day	
VLAN Settings	VLAN Settings	Disable	
	PVID	1	
	Management VLAN	1	
	WLAN	1000	
	Wireless Network	Enable	
Wireless	SSID	Single <p>Operating RF: IP-COM_XXXXXX (XXXXXX is the last six digits of the LAN MAC address of the CPE)</p> <p>Management RF: IP-COM_XXXXXX_MG (XXXXXX is the last six digits of the LAN MAC address of the CPE)</p>  Tip Management RF is not available for some CPEs.	
		Kit <p>Operating RF: IP-COM_XXXXXX (XXXXXX is the random six digits)</p> <p>Management RF: IP-COM_XXXXXX_MG (XXXXXX is the last six digits of the LAN MAC address of the CPE)</p>  Tip Management RF is not available for some CPEs.	
	Security Mode	Single	None
		Kit	Encrypted
		Transparent Bridge	Enable
		ipMAX	Disable
	TPC	Enable	
Network Service	Login Timeout Interval	5 min	
	Ping Watch Dog	Disable	
	Telnet Service	Disable	

Parameters	Default settings
UPnP	Disable
Hardware Watch Dog	Enable
Tools	Date & Time
	Synchronized with the internet

A.2 Acronyms and Abbreviations


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

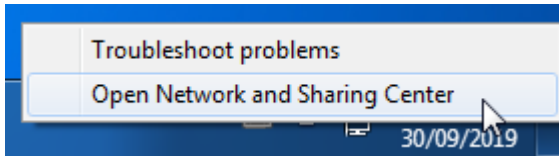
Acronym or Abbreviation	Full Spelling
IP	Internet Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
NMS	Network Management System
NVR	Network Video Recorder
OID	Object Identifier
PoE	Power over Ethernet
PPPoE	Point-to-Point Protocol over Ethernet
PSK	Preshared Key
P2MP	Point-to-Multi-Point
PVID	Port-based VLAN ID
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTS	Request to Send
RX	Receive
SSID	Service Set Identifier

Acronym or Abbreviation	Full Spelling
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	WiFi Multi-Media
WPA	WiFi Protected Access
WPA-PSK	WPA-Preshared Key

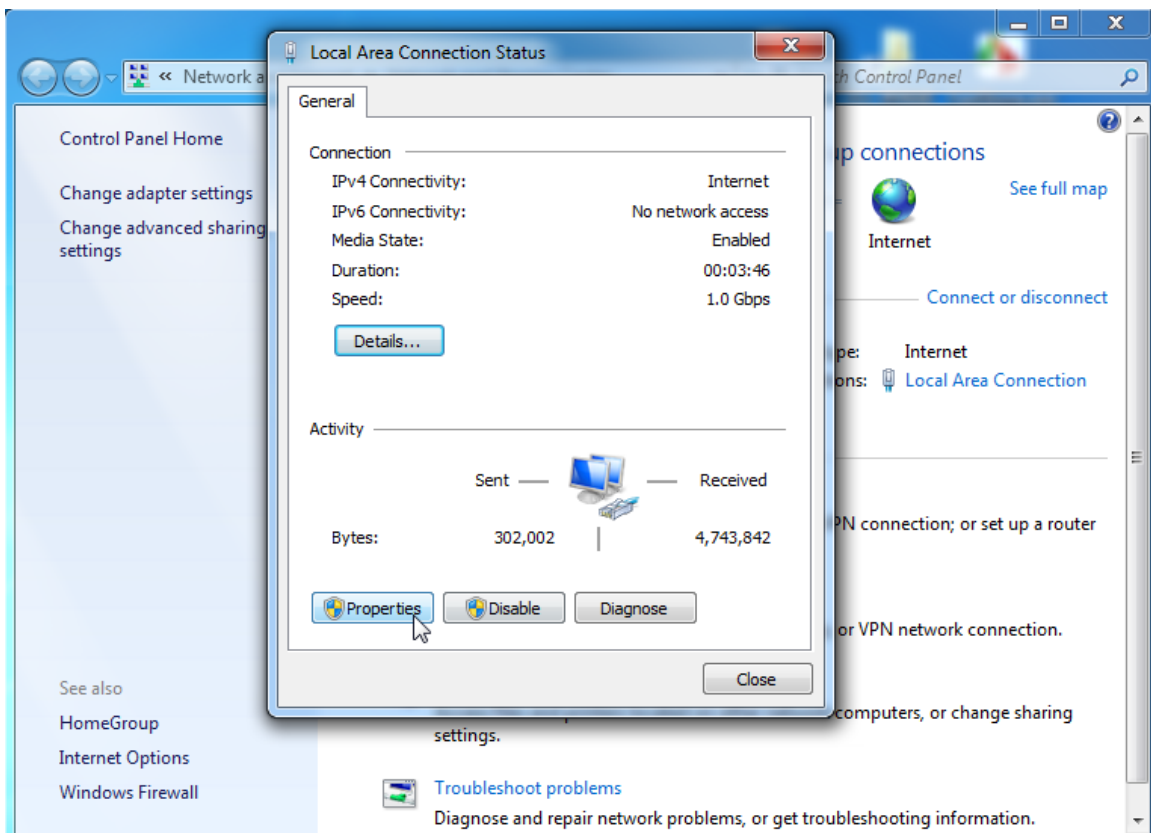
A.3 Assign a fixed IP address to your computer

OS example: Windows 7

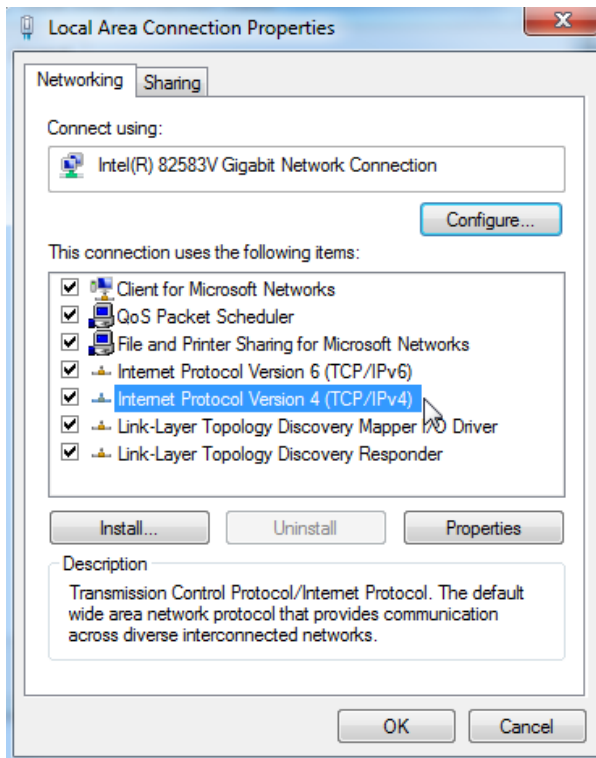
1. Right-click the  icon on the bottom-right corner of the desktop.
2. Click **Open Network and Sharing Center**.



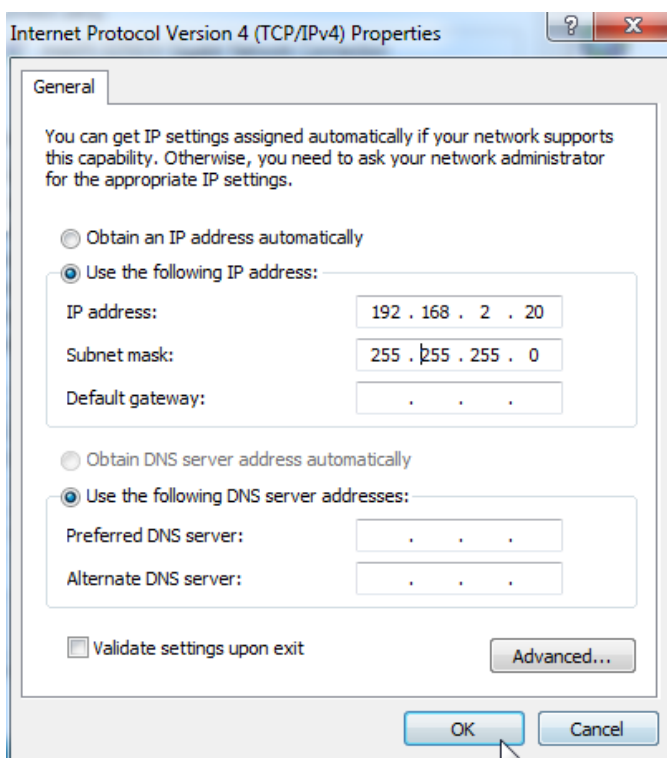
3. Click **Local Area Connection**, then click **Properties**.



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



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




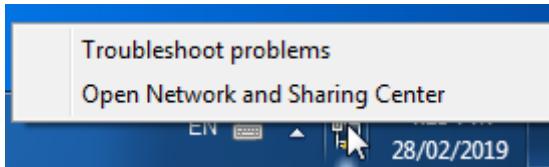
6. Click **OK** on the **Local Area Connection Properties** window, and close the other windows.

----End

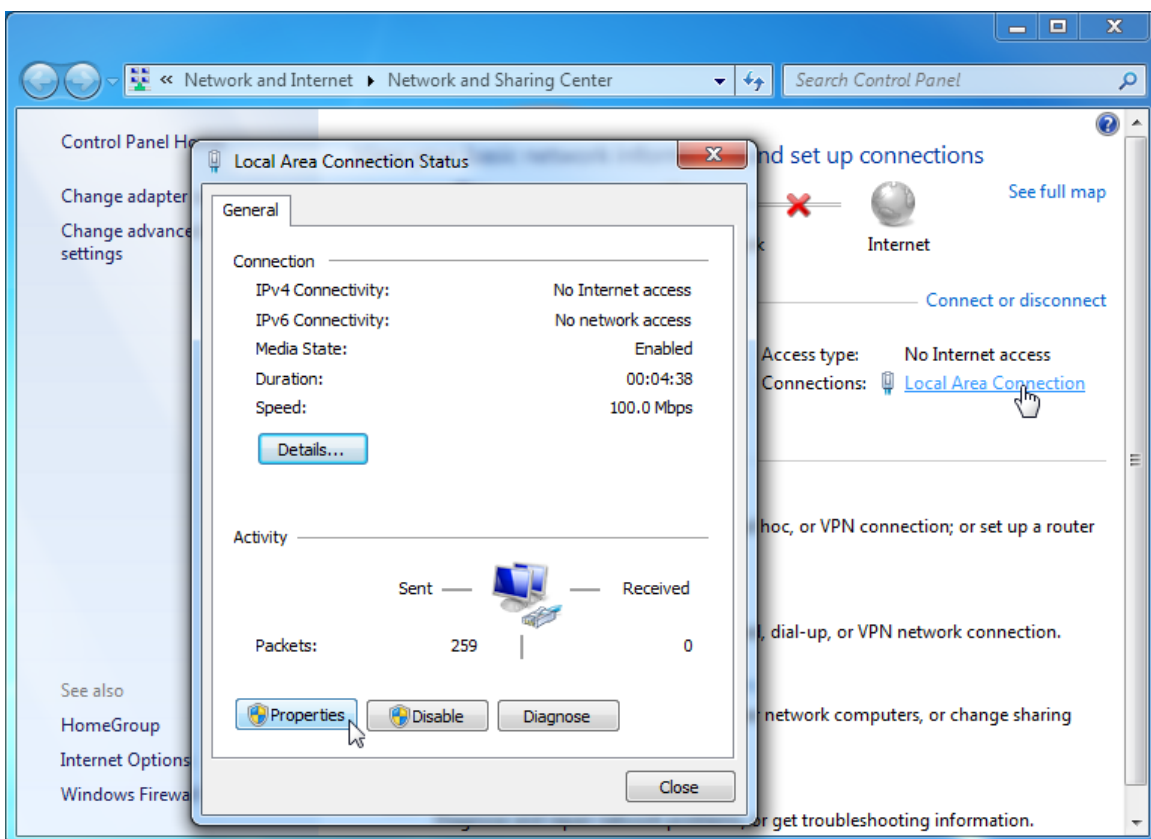
A.4 Check the gateway IP address of a computer

OS example: Windows 7

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



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



----End

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

