www.ip-com.com.cn

User Guide

Outdoor Point to Point CPE

IP-COM

World Wide Wireless

Copyright Statement

Disclaimer

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

Preface

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

This user guide applies to CPE3 and CPE9. In the following content, we take the figures and web UI of CPE9 as examples.

Conventions

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

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

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

Symbol	Meaning
NOTE	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
Tip	This format is used to highlight a procedure that will save time or resources.

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AP	Access Point
ARP	Address Resolution Protocol
AES	Advanced Encryption Standard
CPE	Customer Premises Equipment
CCQ	Client Connection Quality
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DDNS	Dynamic Domain Name Server
GMT	Greenwich Mean Time
IP	Internet Protocol

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

Additional Information

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

Technical Support

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

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

Contents

1 Introduction

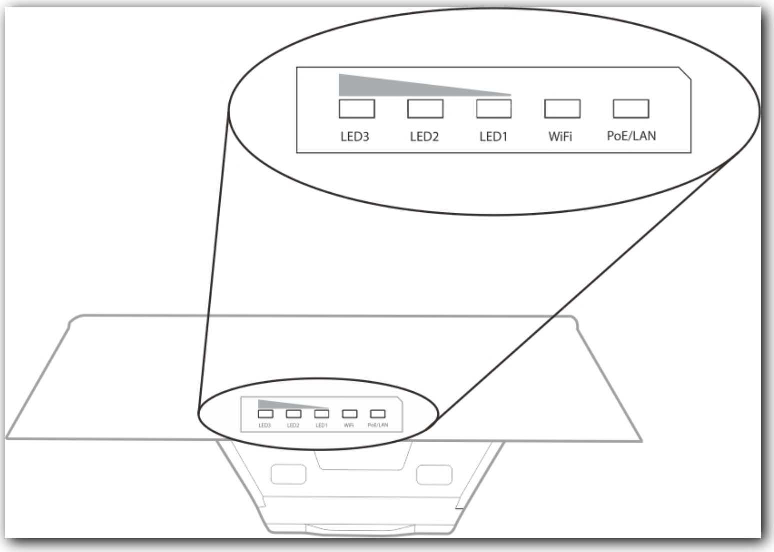
1.1 Overview

The IP-COM outdoor point to point CPE is dedicated for WISP solutions and video surveillance in elevators, tower cranes, apartments, factories, orchards, and scenic areas. Featured the built-in high-gain antennas, and the refined exterior design, the device can be installed onto walls or poles, and offers strong and stable WiFi signals. The industry grade waterproof and dustproof housing allows it to work properly even in harsh environments. With auto-bridging technology, two CPEs can connect to each other automatically to make setup a breeze.

1.2 Getting to Know Your Device

1.2.1 Appearance of CPE3

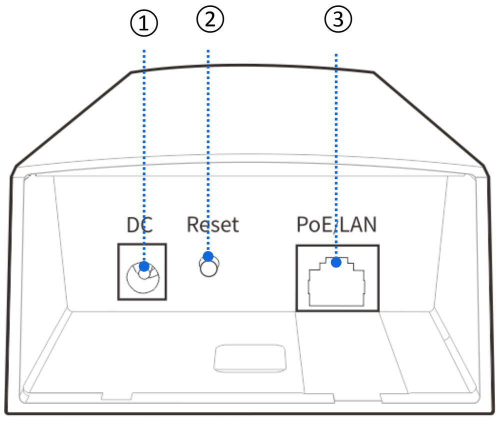
LED Indicators



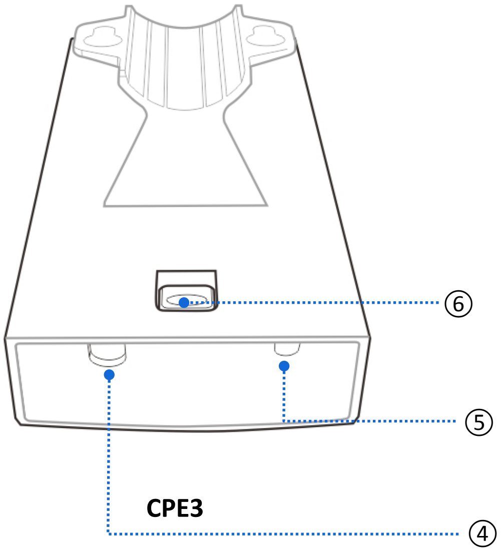
CPE3

LED Indicator	Status	Description
PoE/LAN	Solid on	The device is being powered properly, and no data is being transmitted.
	Blinking	Data is being transmitted over the port.
	Off	The device is not powered on.
WiFi	Solid on	The wireless function is enabled, but no data is being transmitted.
	Blinking	Data is being transmitted in a wireless manner.
	Off	The wireless function is disabled.
LED1, LED2, LED3 (Signal Strength LED)	Solid on	Bridged successfully, and the device works in AP mode. LED1, LED2 and LED3 are solid on: Perfect Signal LED1 and LED2 are sold on, and LED3 is off: Good signal LED1 is solid on, and LED2 and LED3 are off: Weak signal. Please adjust the direction or location of the two devices.
	Blinking	Bridged successfully, and the device works in Client mode.
	Off	The device does not bridge to another peer AP.

Button and Ports



CPE3



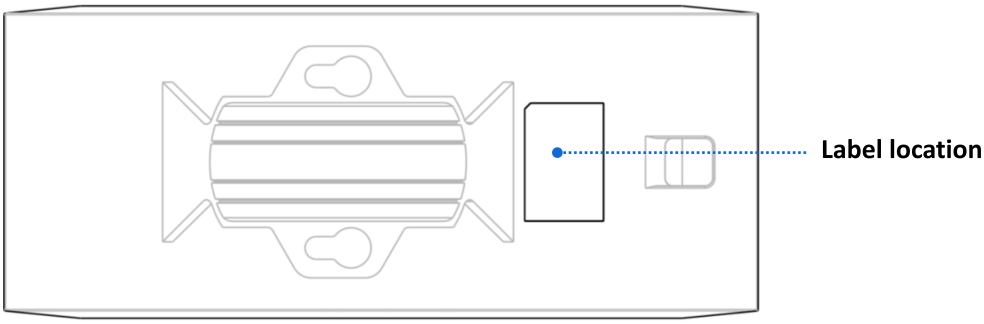
CPE3

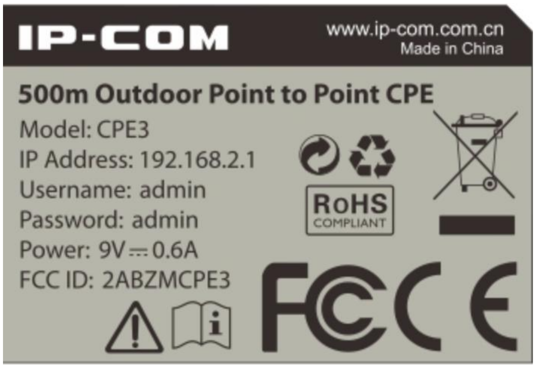
ID	Port/Button	Description
①	DC	Power Jack Connect the included power adapter to this jack to supply power to the device.
②	Reset	Reset Button After the device is powered on for 1 minute, hold down this button for about 7

ID	Port/Button	Description
		seconds. When all the LED indicators on the device light up, the device is restored factory settings.
③	PoE/LAN	It is used to supply power or transmit data. To power on the device using PoE, connect this port to the PoE port of the included PoE injector. If the device is powered on using a DC power adapter, this port can be connected to a switch.
④	/	Ethernet cable inlet.
⑤	/	Power cord inlet.
⑥	/	It is used to remove the cover.

Label

The label on the back panel of the device presents the login IP address, username and password and other information of the device.




IP-COM

www.ip-com.com.cn
Made in China

500m Outdoor Point to Point CPE

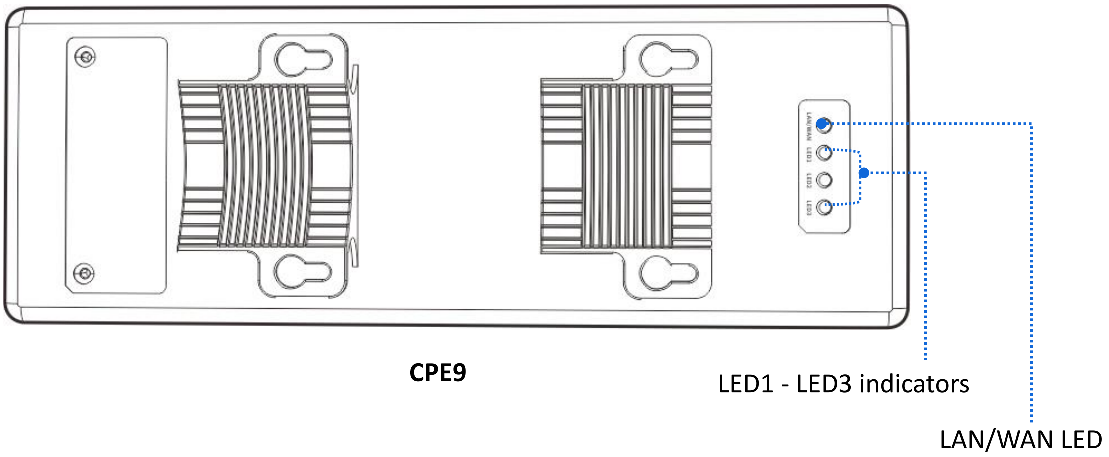
Model: CPE3
IP Address: 192.168.2.1
Username: admin
Password: admin
Power: 9V⎓0.6A
FCC ID: 2ABZMCPE3

RoHS COMPLIANT

Product label

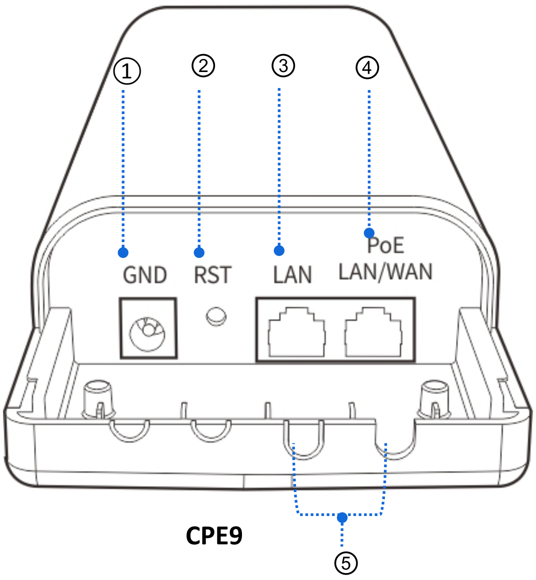
1.2.2 Appearance of CPE9

LED Indicators



LED Indicator	Status	Description
LAN/WAN	Solid on	The device is being powered properly, and no data is being transmitted.
	Blinking	Data is being transmitted over the port.
	Off	The device is not powered on.
LED1, LED2, LED3 (Signal Strength LED)	Solid on	The device has wireless clients connected to it and may work in AP, Repeater, or Router mode. If you performed auto bridging, the device is already set to AP mode. LED1, LED2 and LED3 are solid on: Perfect Signal LED1 and LED2 are sold on, and LED3 is off: Good signal LED1 is solid on, and LED2 and LED3 are off: Weak signal. Please adjust the direction or location of the two devices.
	Blinking	The device is working in Client, Universal Repeater or WISP mode, and connected to a remote AP. If the device is automatically connected to the other one, it is set to Client mode.
	Off	The device is not connected to a wireless client or a remote AP.

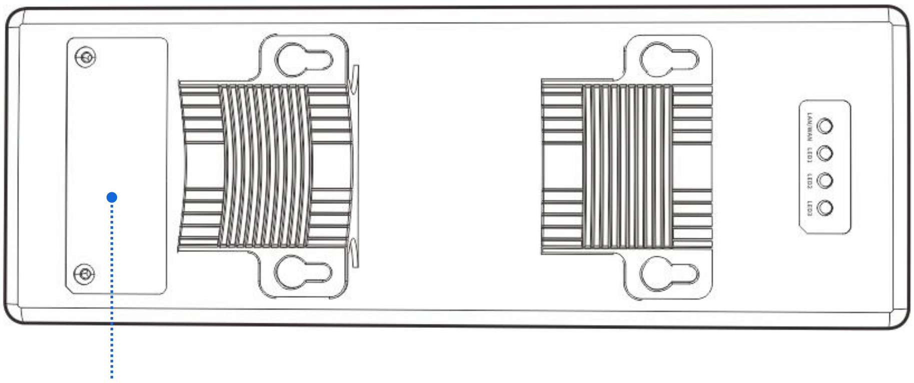
Button and Ports



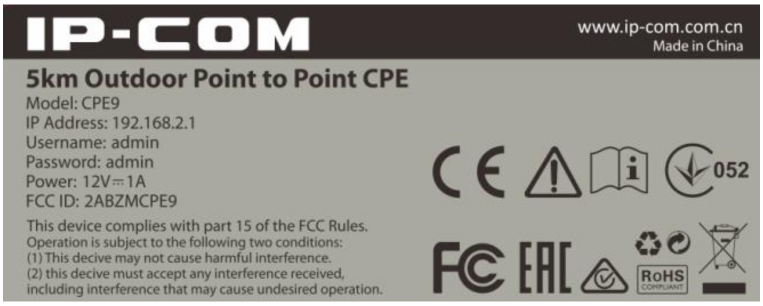
ID	Port/Button	Description
①	GND	Grounding jack Use the included grounding screw and cable to connect the device's grounding jack to a grounding terminal of building to avoid ESD and lightning damage to the device.
②	RST	Reset Button After the device is powered on for 1 minute, hold down this button for about 8 seconds. When all the LED indicators on the device light up, the device is restored factory settings.
③	LAN	10/100 Mbps automatic negotiation RJ45 port. Used to connect to a switch, computer, or other wired devices.
④	PoE LAN/WAN	It is used to supply power or transmit data. If the device works in Router mode, it is a WAN port. Otherwise, it is a LAN port. Use the included PoE injector to supply power to the device.
⑤	/	Ethernet cable inlet.

Label

The label on the back panel of the device presents the login IP address, username and password and other information of the device.



Label location



IP-COM

www.ip-com.com.cn
Made in China

5km Outdoor Point to Point CPE
Model: CPE9
IP Address: 192.168.2.1
Username: admin
Password: admin
Power: 12V⎓1A
FCC ID: 2ABZMCPE9

This device complies with part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1) This decive may not cause harmful interference.
(2) this decive must accept any interference received,
including interference that may cause undesired operation.

Product label

2 Application Scenario

2.1 ISP Hotspot Connection-WISP Mode

An apartment needs to bridge an ISP hotspot for internet access.

2.1.1 Solution

IP-COM CPE can address this requirement.

CPE9 is used as an example to illustrate the installation procedure. The installation procedure of **CPE3** is similar.

2.1.2 Setting up the CPE

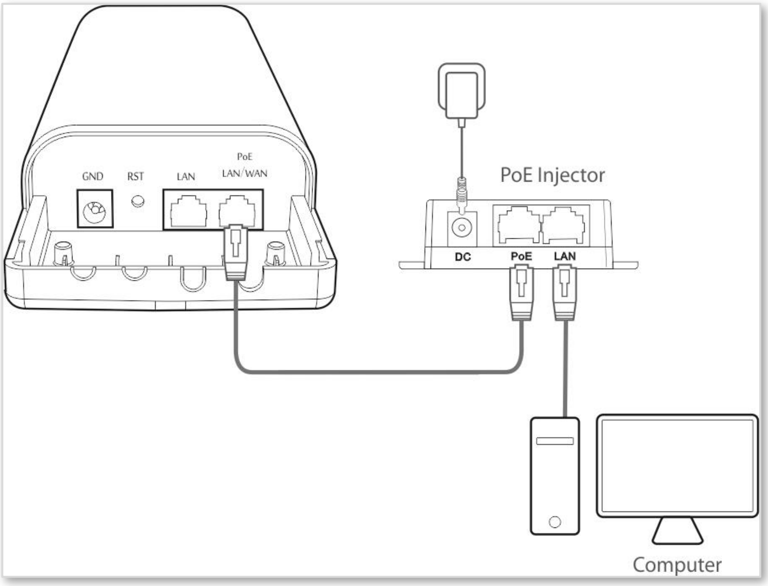
1. Connect the computer to the CPE.

   (1) Uncover the housing of the CPE.

   (2) Use an Ethernet cable to connect the **PoE/LAN/WAN** port of the device to the **PoE** port of the PoE injector.

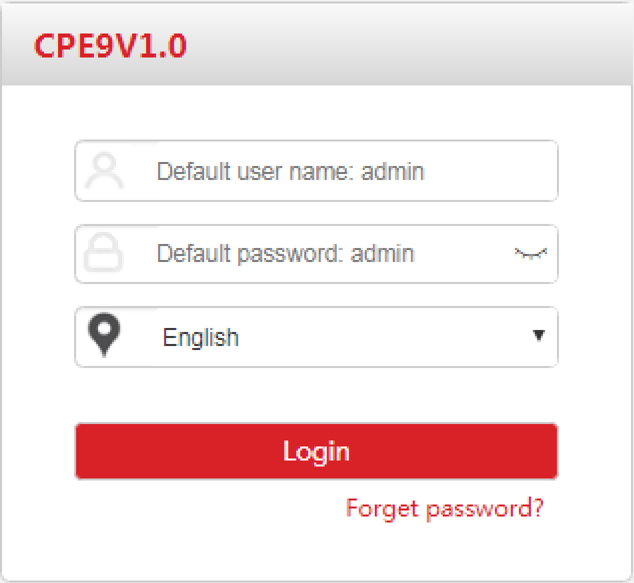
   (3) Use the included power adapter to connect the PoE injector to a power socket. The **LAN/WAN** LED indicator of the CEP lights up.

   (4) Use an Ethernet cable to connect your computer to the **LAN** port of the PoE injector.



2. Set the CPE to **WISP** mode.

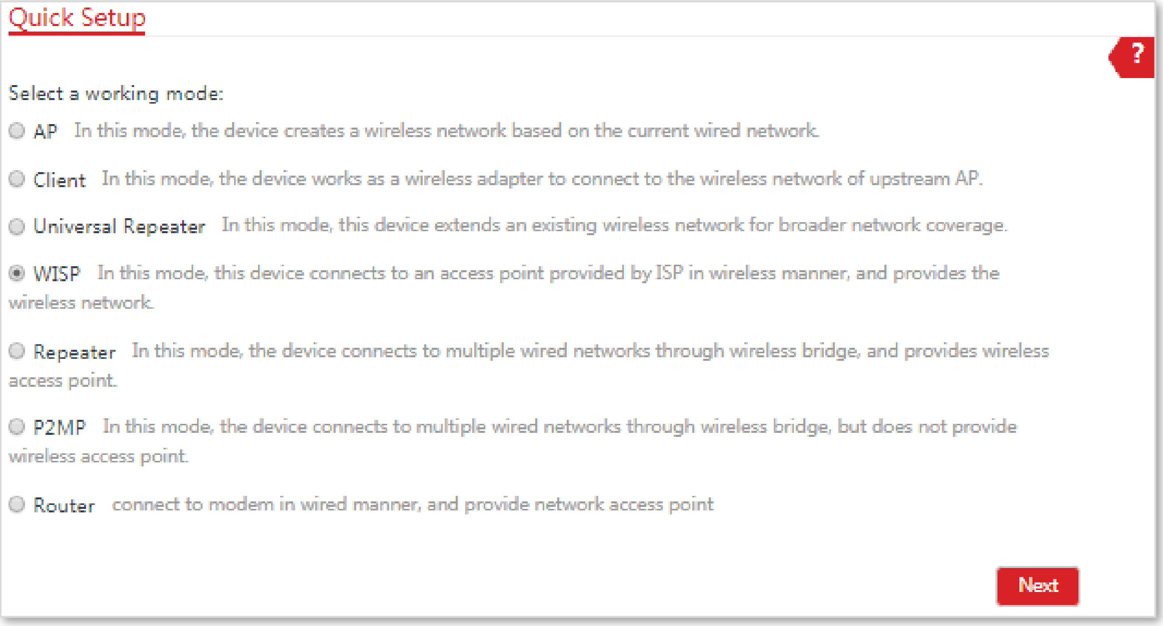
   (1) Start a web browser on your computer, and visit **192.168.2.1**. Enter your user name and password (default: **admin/admin**), and click **Login**.



Tip

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

(2) Select **WISP**, and click **Next**.



Quick Setup

Select a working mode:

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

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

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

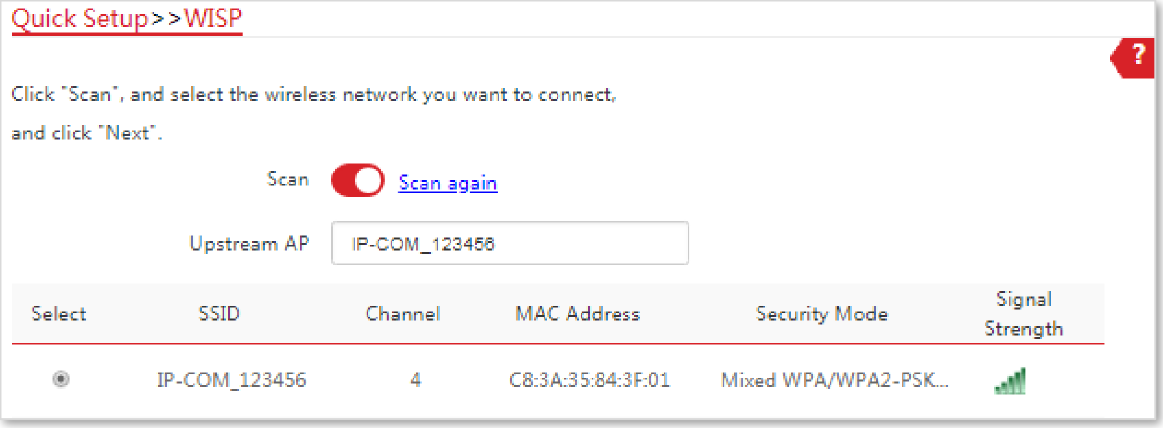
● WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

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

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

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

(3) Select the SSID of your ISP (Internet Service Provider) hotspot, which is **IP-COM_123456** in this example, and click **Next**.



Quick Setup>>WISP

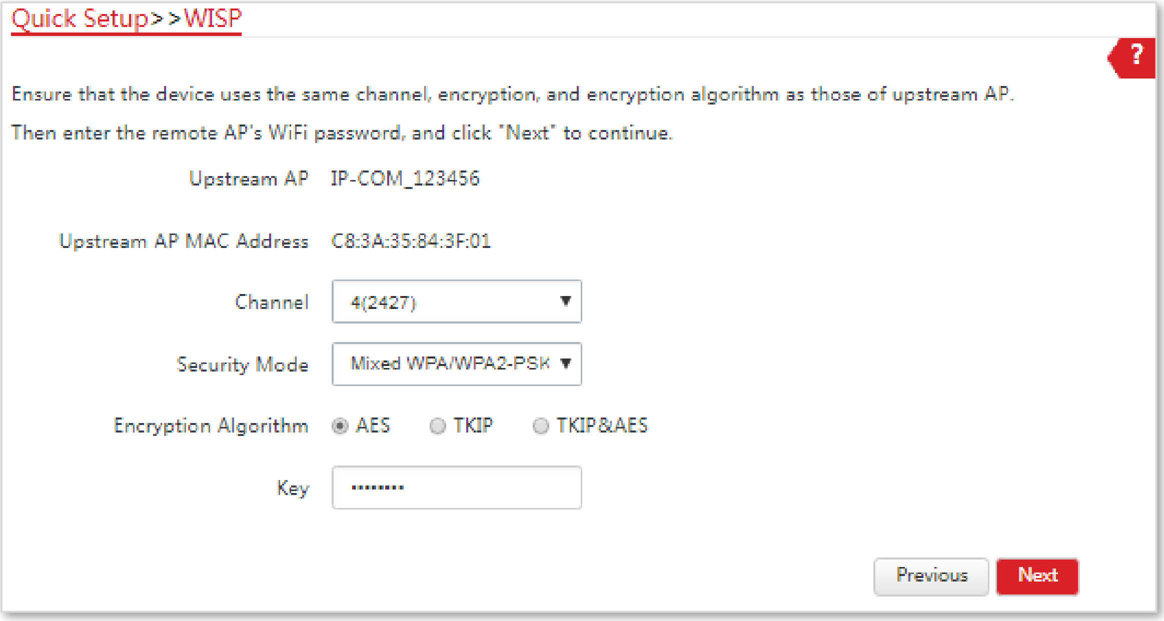
Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan: on

Upstream AP: IP-COM_123456

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	IP-COM_123456	4	C8:3A:35:84:3F:01	Mixed WPA/WPA2-PSK...	

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



Quick Setup>>WISP

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

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

Upstream AP: IP-COM_123456

Upstream AP MAC Address: C8:3A:35:84:3F:01

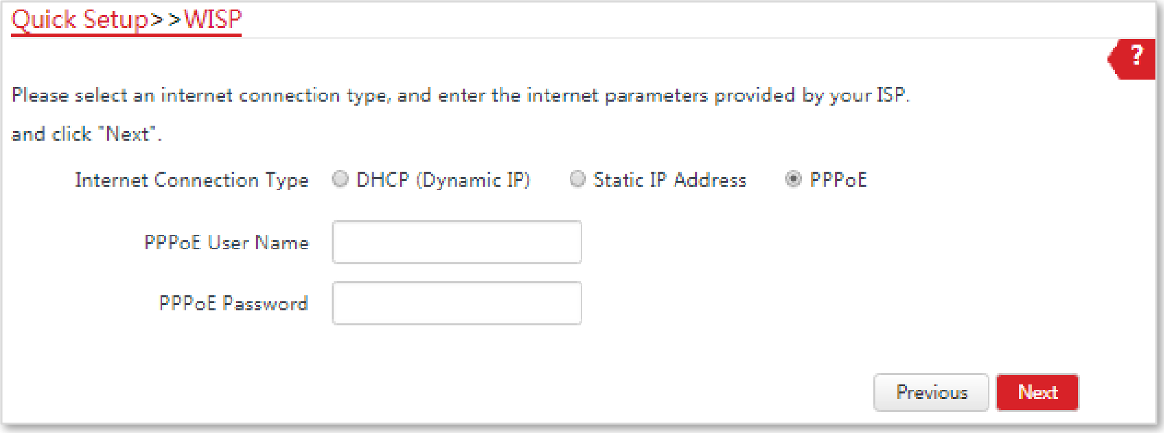
Channel: 4(2427)

Security Mode: Mixed WPA/WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

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



Quick Setup>>WISP

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

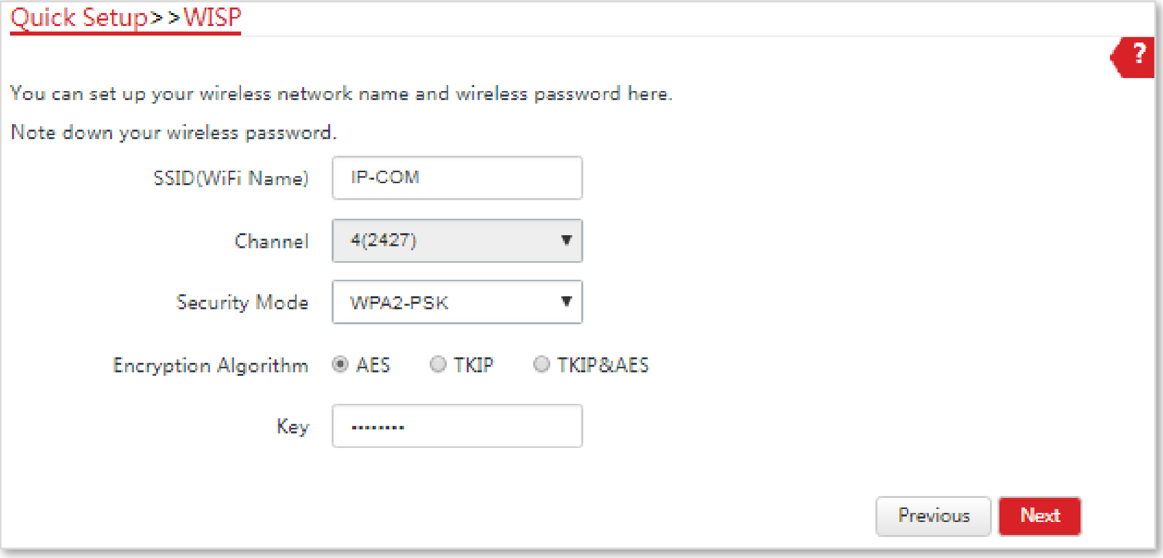
and click "Next".

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

PPPoE User Name:

PPPoE Password:

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



Quick Setup>>WISP

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

Note down your wireless password.

SSID(WiFi Name): IP-COM

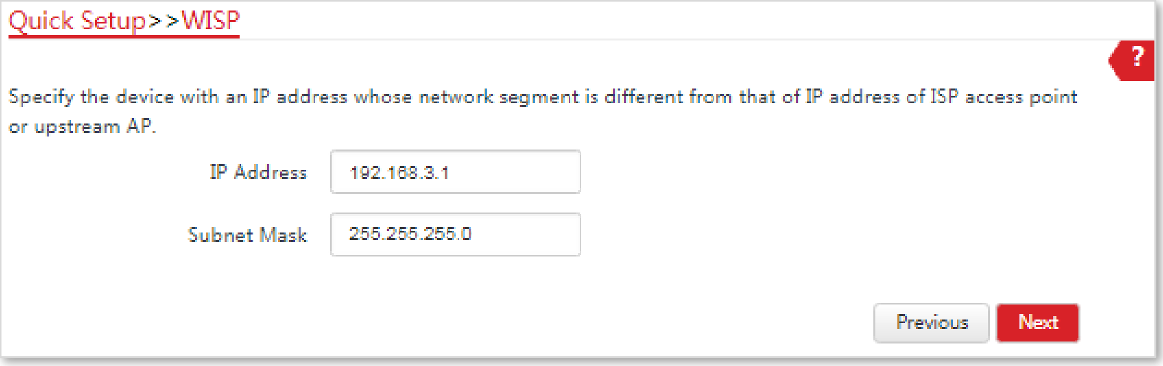
Channel: 4(2427)

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

(7) Set an IP address belonging to different network segment as that of your ISP hotspot. For example, if the IP address of your ISP hotspot is 192.168.2.1, you can set this device's IP address to 192.168.*X*.1 (*X* ranges from 0 to 254 excluding2). Then click **Next**.



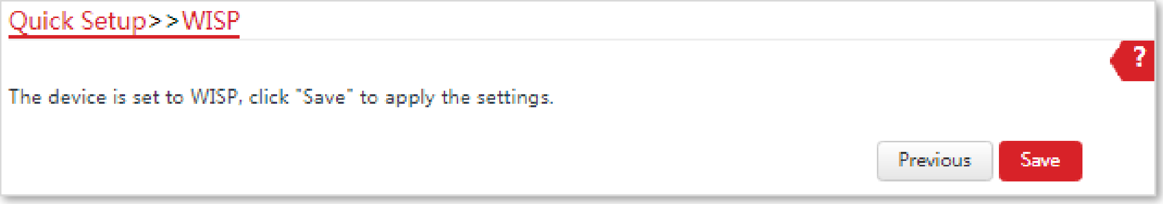
Quick Setup>>WISP

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

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

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



Quick Setup>>WISP

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

---End

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

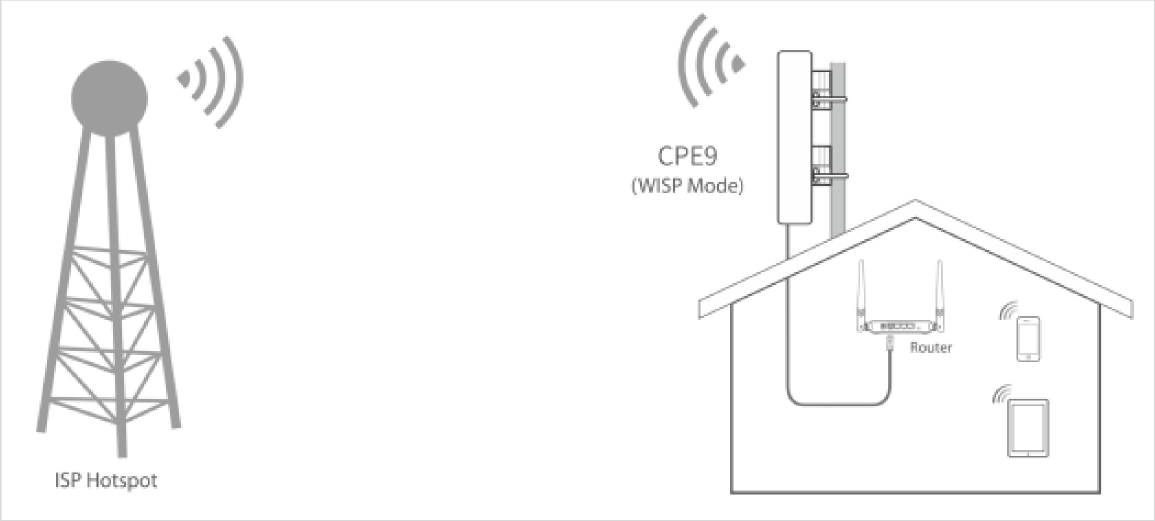
2.1.3 Installing the CPE

1. Place the device at an elevated position in the open air.

2. Uncover the housings of the device, and connect the **PoE/LAN/WAN** port of the device to the WAN port of your wireless router. The **LAN/WAN** LED indicator lights up.

3. Adjust the device's direction or location on the selected pole until the LED1, LED2 and LED3 of the device light up.

4. Use the plastic straps to attach the device to the pole.



---End

2.2 CCTV Surveillance

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

2.2.1 Solution

IP-COM CPE can address this requirement.

CPE9 is used as an example to illustrate the installation procedure. The installation procedure of **CPE3** is similar.

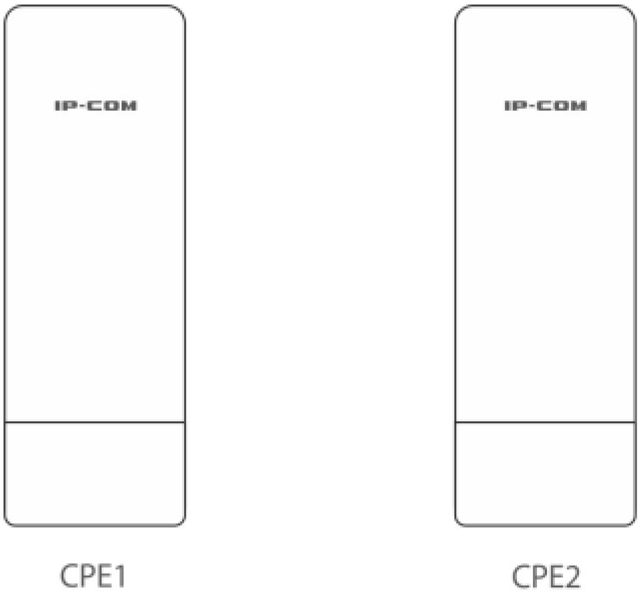
2.2.2 Setting up the CPEs

Tip

At least two CPEs are required for bridging.

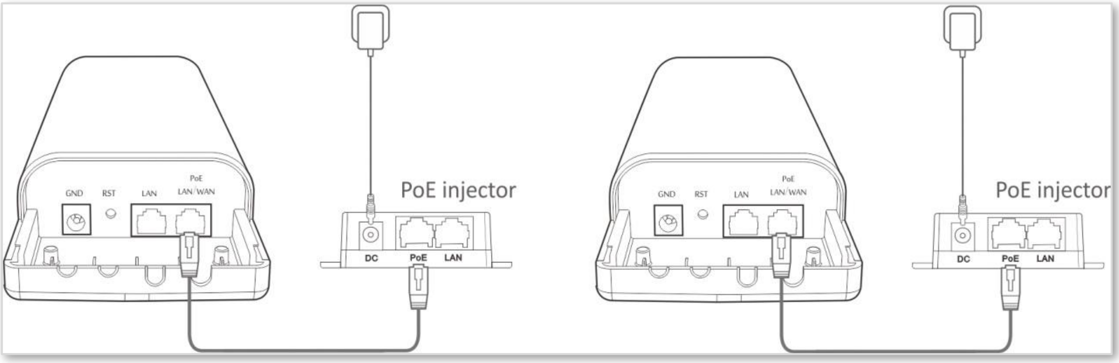
Method 1: Automatic Bridging (Recommended)

1. Place the two CPEs next to each other, see the following figure.

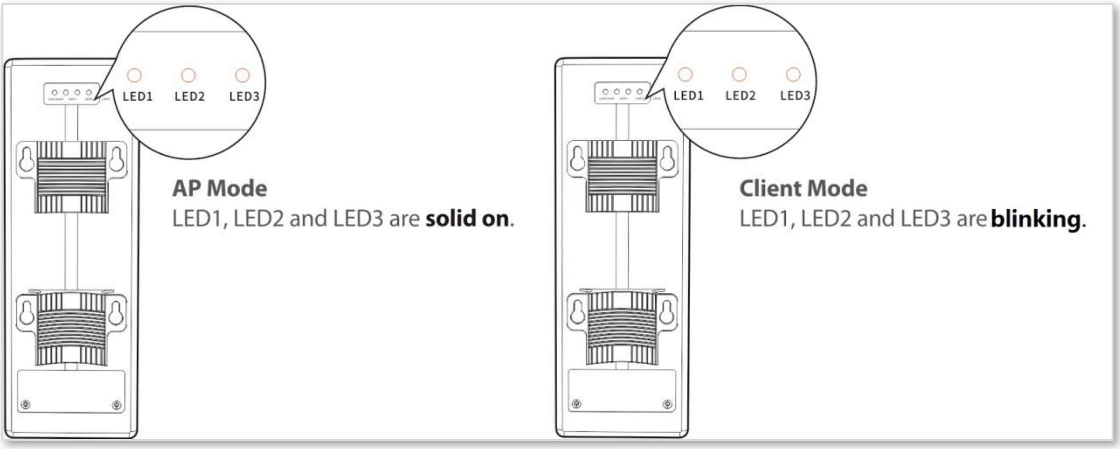


2. Remove the housing of each CPE, and use the included PoE injectors to power them on.

   Wait until the **LAN/WAN** LED indicators of the CPEs light up.



3. Wait for the two CPEs to negotiate and connect to each other automatically. The following LED indicator status indicates successful connection of the two CPEs.


LED1
LED2
LED3
AP Mode
LED1, LED2 and LED3 are **solid on**.
LED1
LED2
LED3
Client Mode
LED1, LED2 and LED3 are **blinking**.

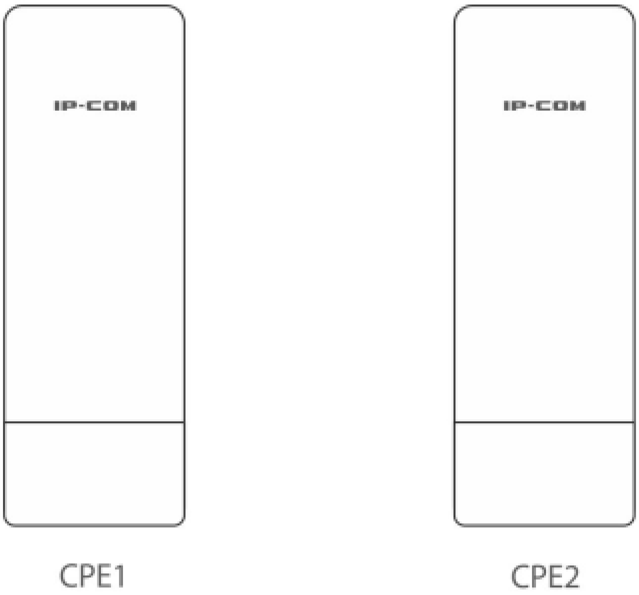
Note

- Automatic Bridging is only applicable when the CPEs are in factory settings, and the bridging process lasts less than 1 minute after the CPEs are powered on.
- Automatic Bridging is only applicable to peer-to-peer bridging. If there are three or more powered CPEs nearby, automatic bridge fails. So if you want to perform peer-to-multi peer bridging, please refer to Method 2: Set up the CPEs Using Web UI.
- If the bridging succeeds, the DHCP servers of the two CPEs are disabled, and the IP address of the CPE working in Client mode changes to 192.168.2.2.

---End

Method 2 Set up the CPEs Using Web UI

1. Place the two CPEs next to each other.



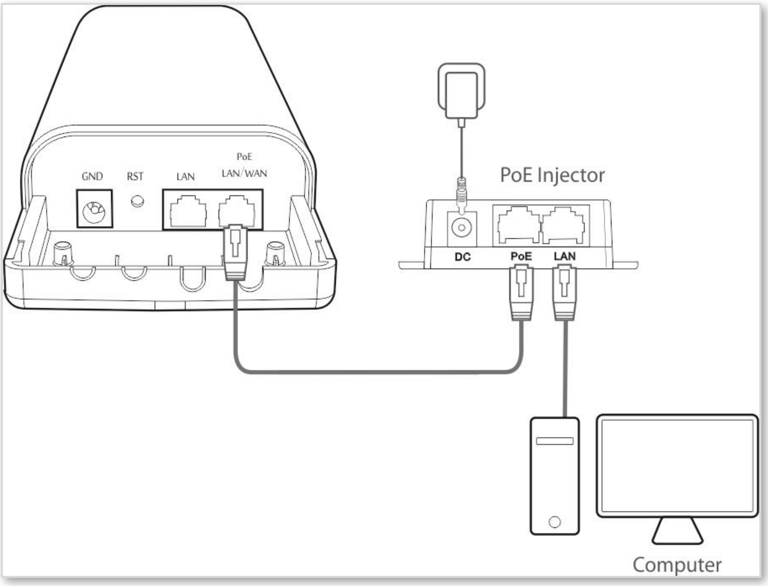
2. Connect the computer to **CPE1**.

(1) Uncover the housing of CPE1.

(2) Use an Ethernet cable to connect the PoE LAN/WAN port of CPE1 to the PoE port of the PoE injector.

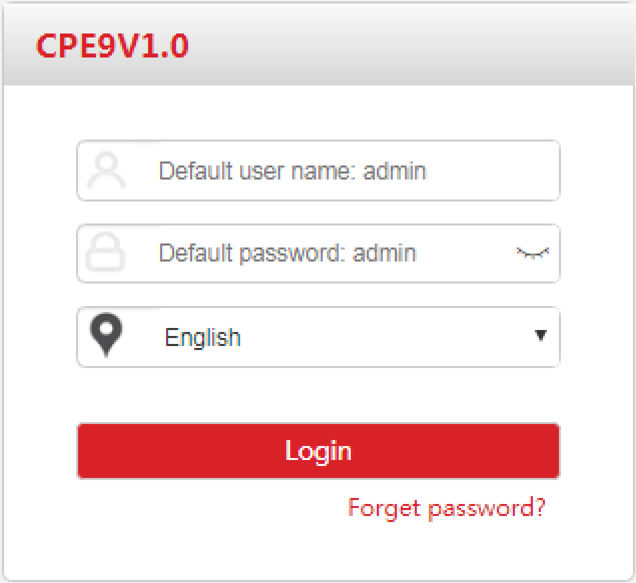
(3) Use the included power adapter to connect the PoE injector to a power socket. The **LAN/WAN** LED indicator of the **CPE1** lights up.

(4) Use an Ethernet cable to connect your computer to the **LAN** port of the PoE injector.



3. Set CPE1 to AP Mode.

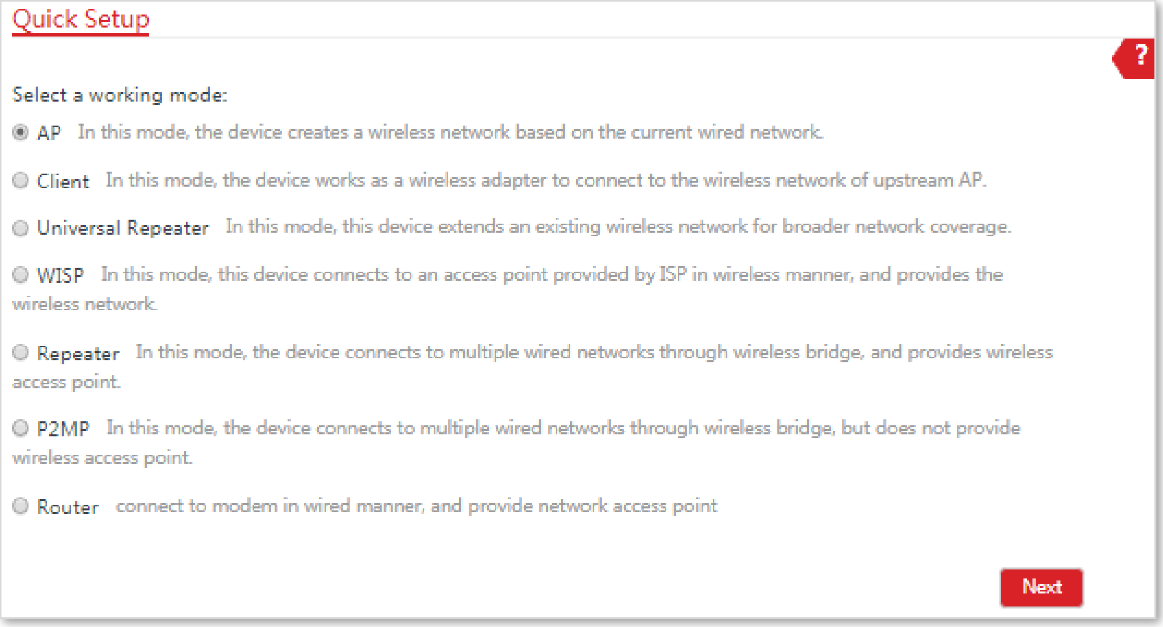
   (1) Start a web browser on the computer, and visit **192.168.2.1**. Enter your user name and password (default: **admin/admin**), and click **Login**.



Tip

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

4. Select **AP**, and click **Next**.



Select a working mode:

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

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

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

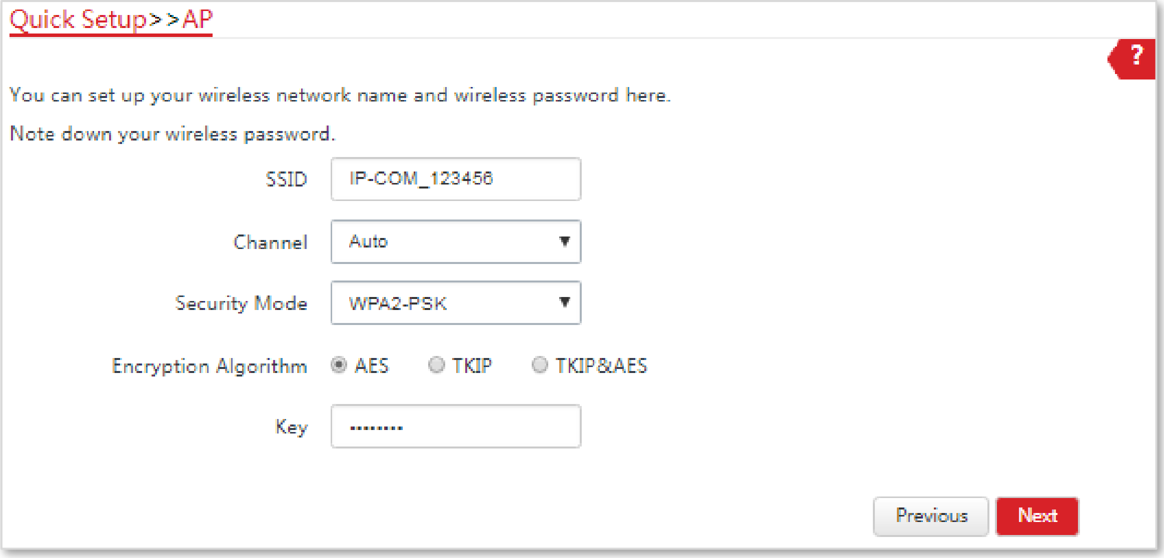
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

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

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

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

(1) Set an **SSID**, which is **IP-COM_123456** in this example, **Security Mode** (WPA2-PSK is recommended), and **Key**, and click **Next**.



Quick Setup>>AP

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

Note down your wireless password.

SSID: IP-COM_123456

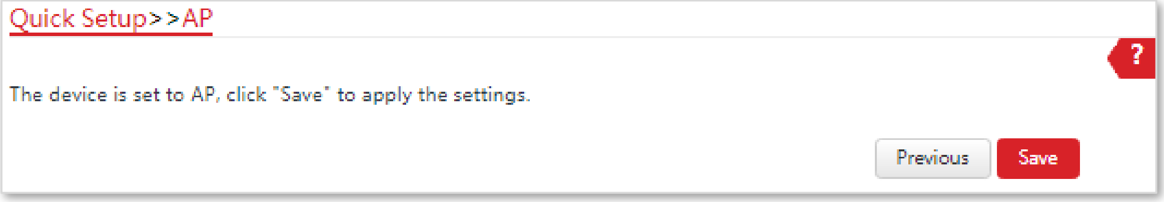
Channel: Auto

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

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



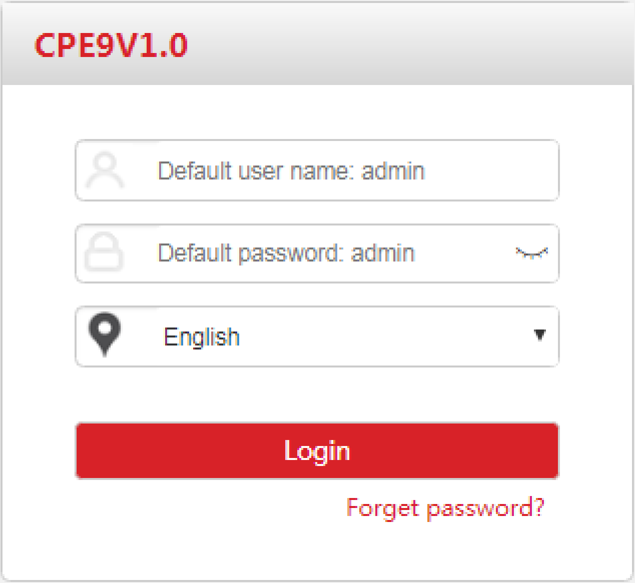
Quick Setup>>AP

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

5. Set **CPE2** to **Client Mode**.

(1) Perform the procedure in **Step 2** Connect the computer to **CPE1** to connect the computer to **CPE2**.

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



CPE9V1.0

Default user name: admin

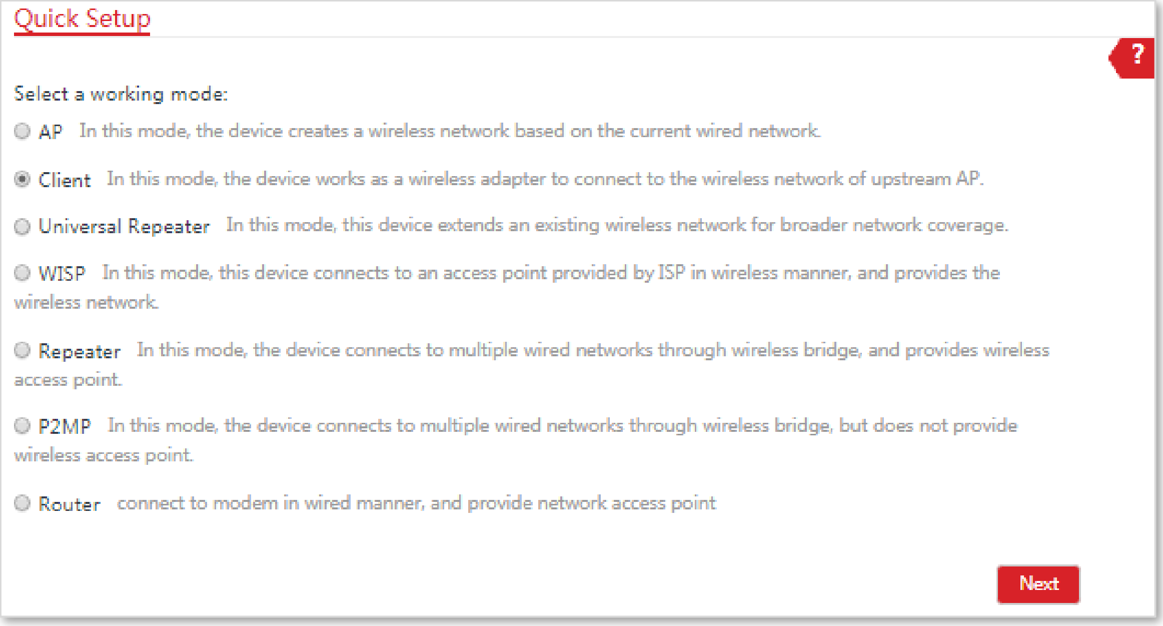
Default password: admin

English

Tip

If this page doesn't appear, please refer to Q1 in FAQ.

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



Quick Setup

Select a working mode:

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

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

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

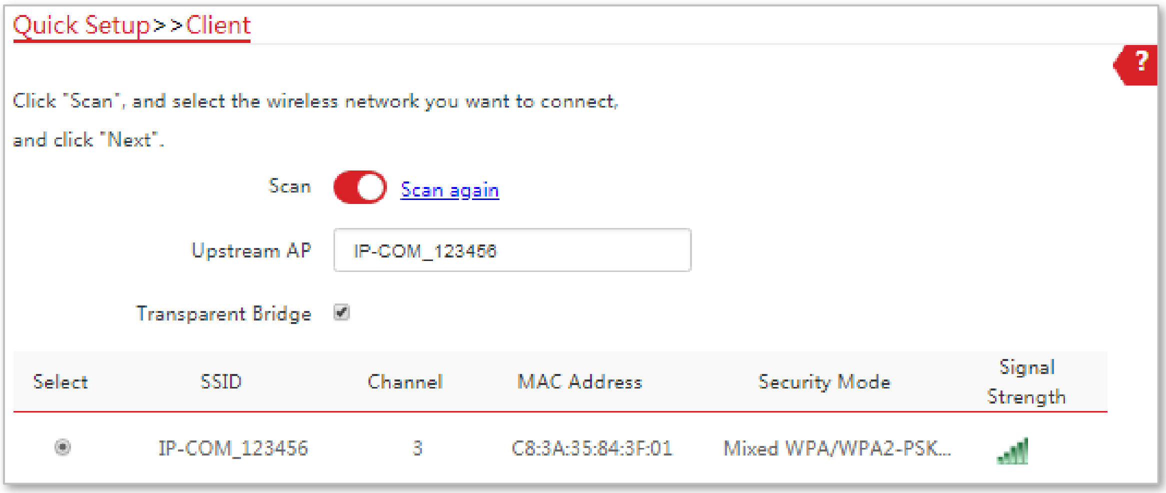
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

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

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

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

(4) Select the SSID of **CPE1** you set, which is **IP-COM_123456** in this example, and click **Next**.



Quick Setup>>Client

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

Scan: on, Scan again

Upstream AP: IP-COM_123456

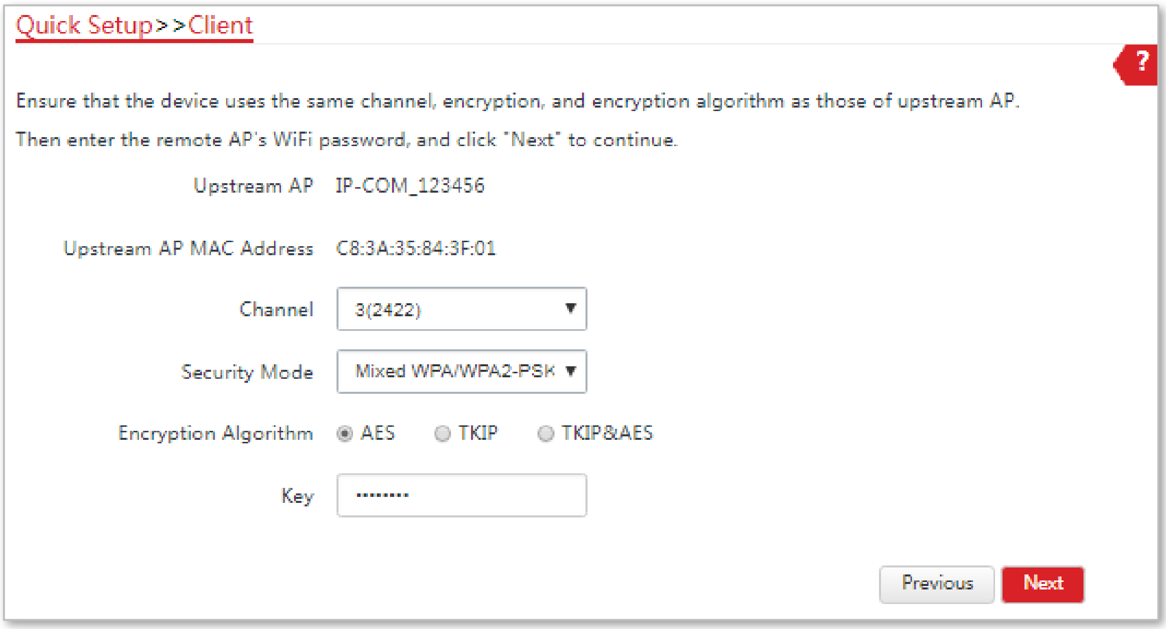
Transparent Bridge: ☑

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	IP-COM_123456	3	C8:3A:35:84:3F:01	Mixed WPA/WPA2-PSK...	📶

Tip

If there is no wireless network is scanned, choose **Wireless** > **Basic**, and ensure that the wireless function is enabled. Then try again.

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

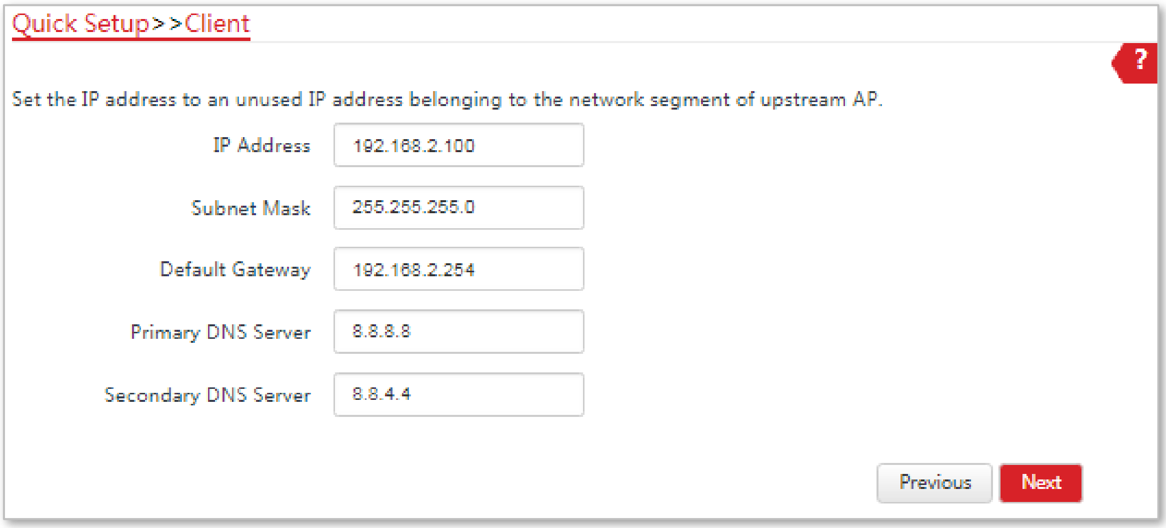


Quick Setup>>Client

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

Upstream AP	IP-COM_123456
Upstream AP MAC Address	C8:3A:35:84:3F:01
Channel	3(2422)
Security Mode	Mixed WPA/WPA2-PSK
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Key	········

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

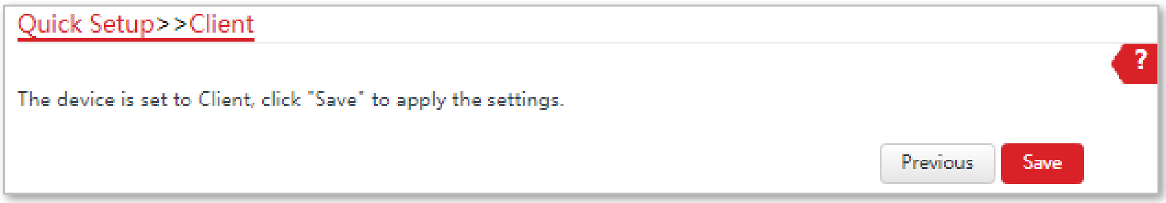


Quick Setup>>Client

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

IP Address	192.168.2.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4

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



Quick Setup>>Client

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

---End

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

Tip

You can check the SSID and key of the CPE1 or CPE2 by choosing **Wireless** > **Basic** after logging in to the web UI.

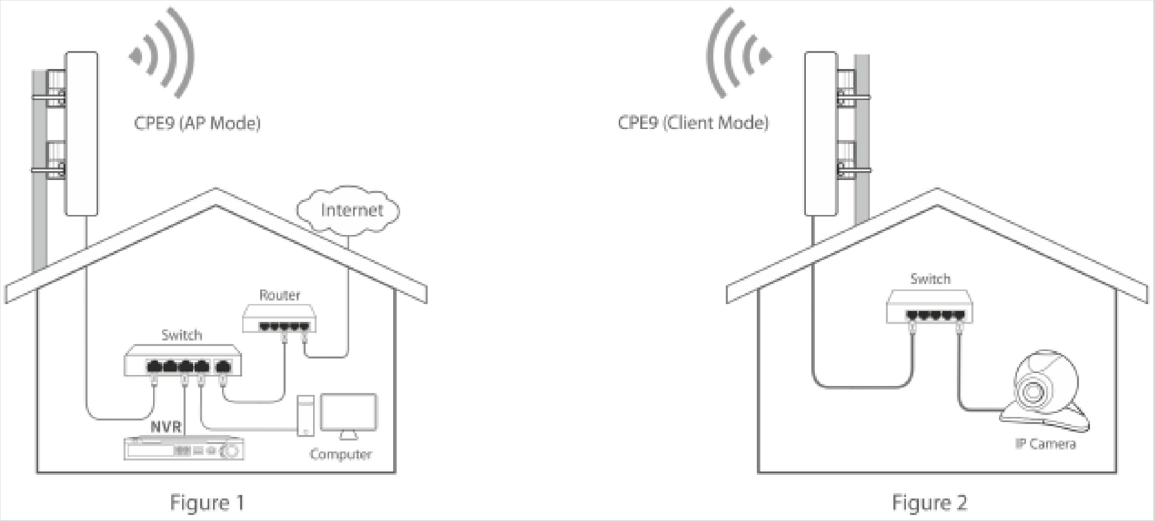
2.2.3 Installing the CPEs

The CPE (transmitter in AP mode) with LED1, LED2 and LED3 solid on should be connected to the switch connecting to a network video recorder (NVR). See **Figure 1** below.

The CPE (receiver in Client mode) with LED1, LED2 and LED3 blinking should be connected to the switch connecting to a monitoring IP camera. See **Figure 2** below.

Detailed procedures are as follows:

1. Place the transmitter in the open air at the point where the NVR is located. Place the receiver in the open air at the point where the IP camera is located.
2. Uncover the housings of the two CPEs, and connect the **PoE/LAN/WAN** ports of the CPEs to PoE injectors respectively. The **LAN/WAN** LED indicators light up.
3. Adjust the two CPEs' direction or location until the LED1, LED2 and LED3 of the two CPEs light up.
4. Use the plastic straps to attach the two CPEs to the poles respectively.



---End

3 Web UI

3.1 Login

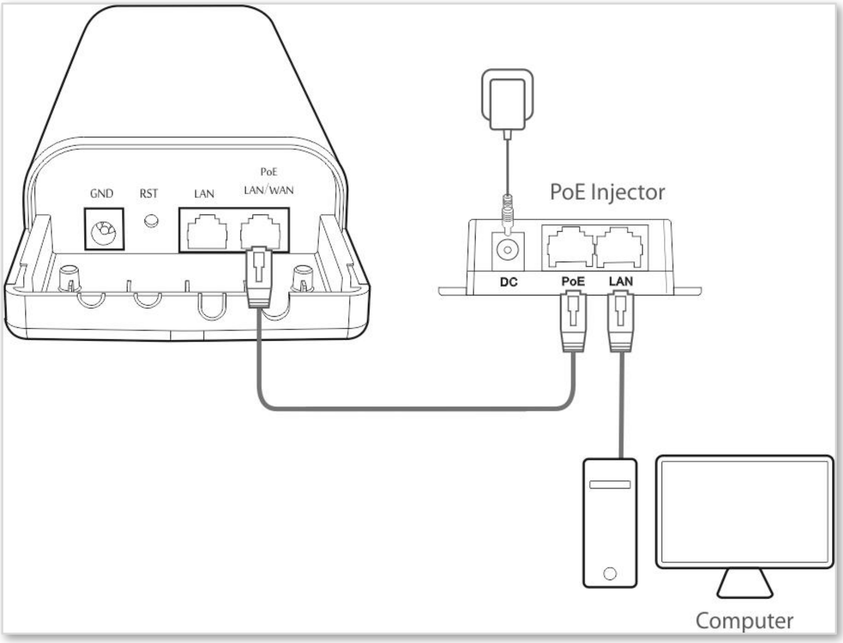
1. Connect the computer to the device.

   (1) Uncover the housing of the device.

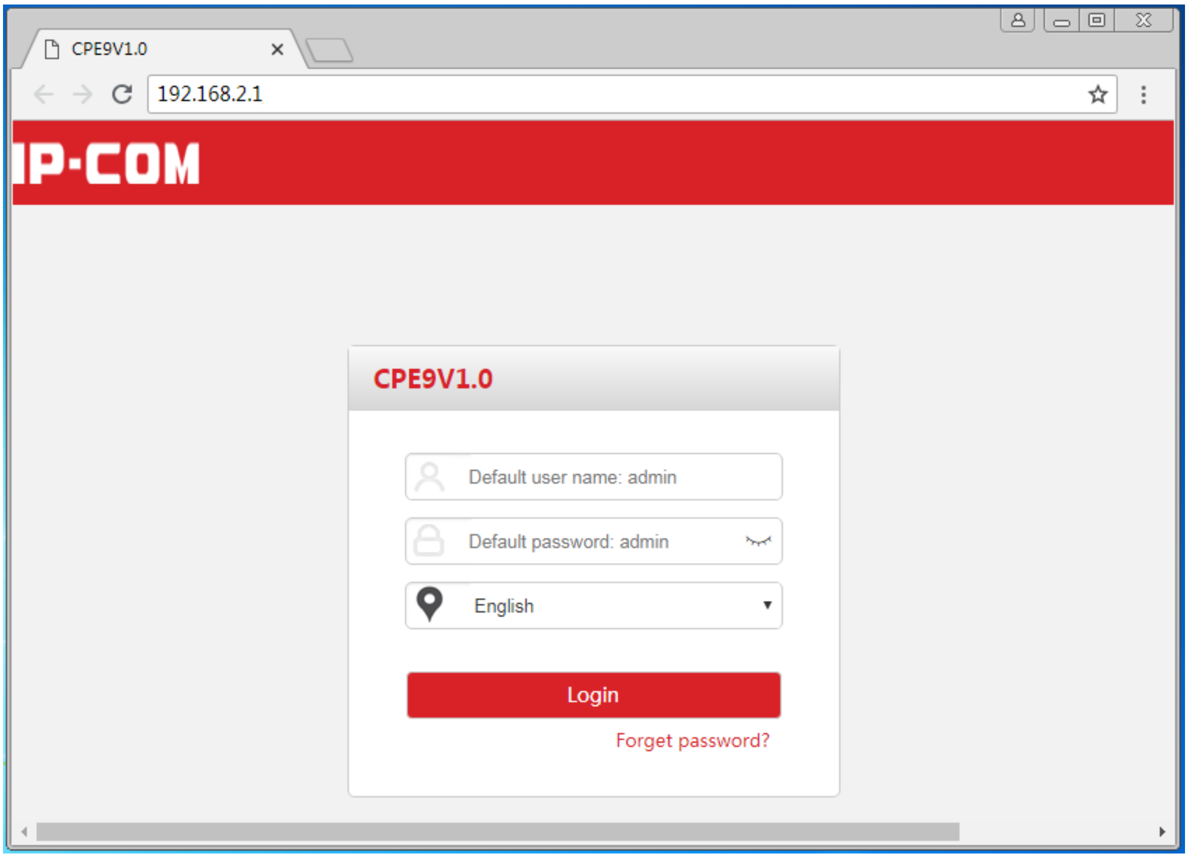
   (2) Use an Ethernet cable to connect the **PoE/LAN/WAN** port of the device to the **PoE** port of the PoE injector.

   (3) Use the included power adapter to connect the PoE injector to a power socket. The **LAN/WAN** LED indicator of the device lights up.

   (4) Use an Ethernet cable to connect your computer to the **LAN** port of the PoE injector.



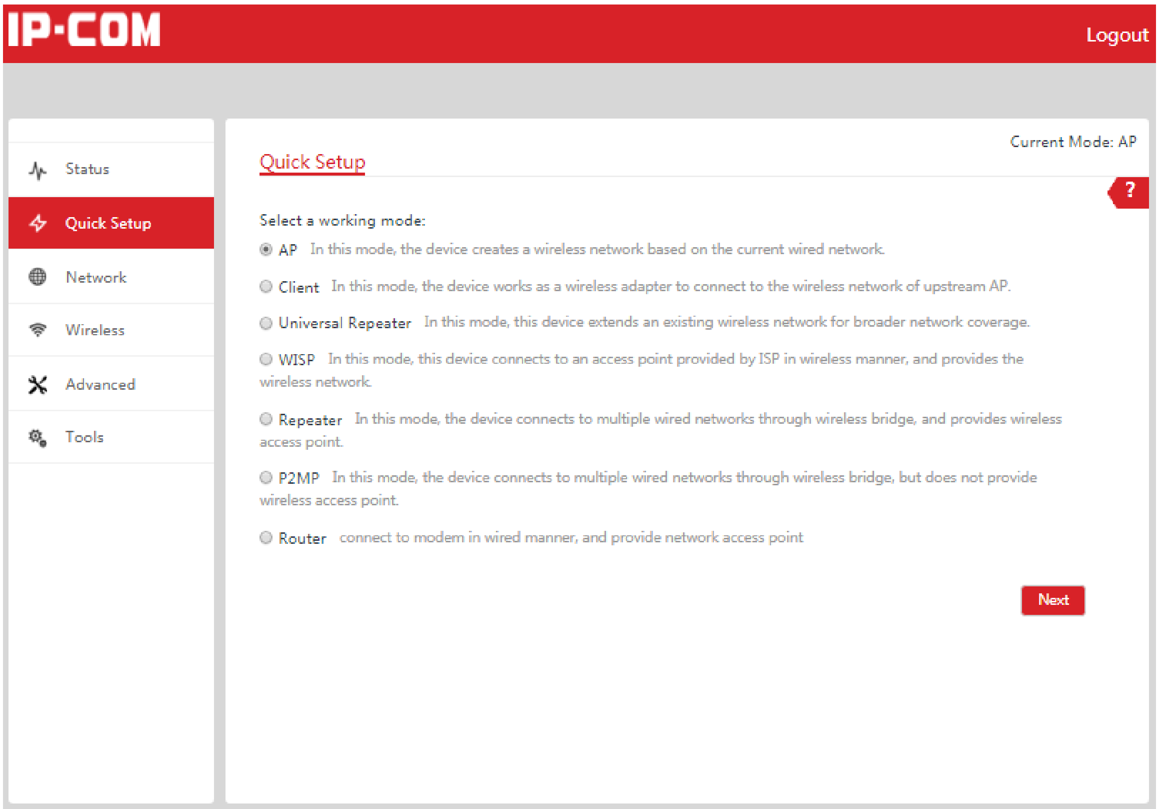
2. Start a web browser on your computer, and visit **192.168.2.1**. Enter your user name and password (default: **admin**), and click **Login**.



Tip

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

Then the following page appears.



Current Mode: AP

Quick Setup

Select a working mode:

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

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

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

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

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

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

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

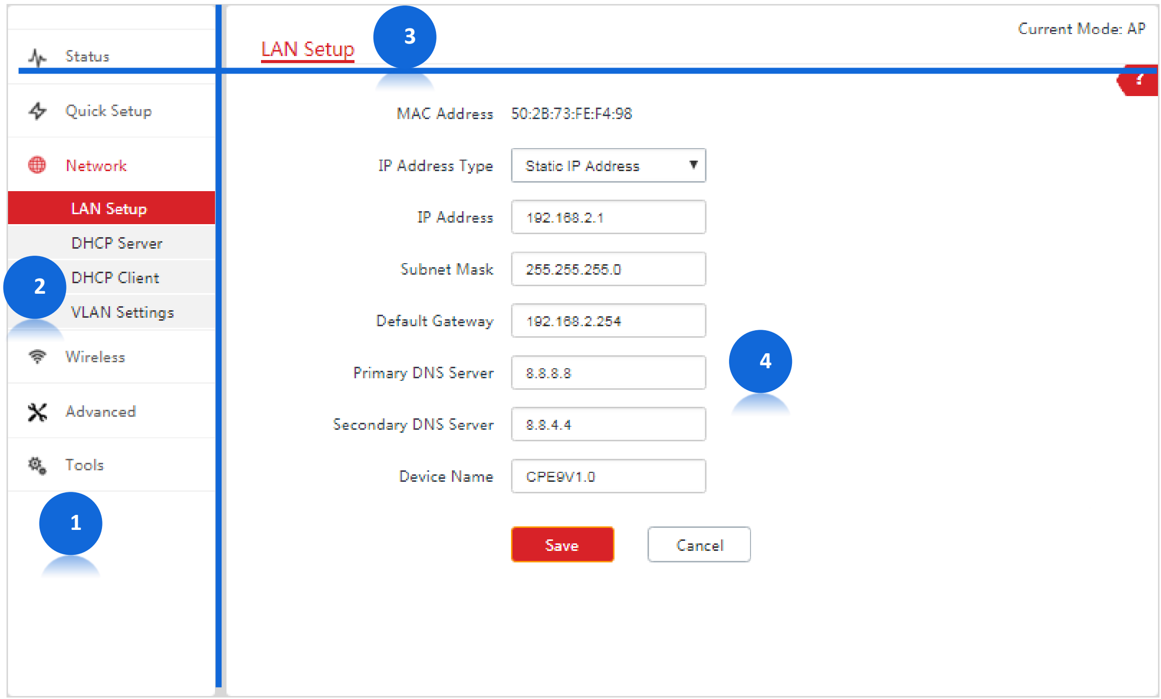
3.2 Logout

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

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

3.3 Web UI Layout

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



MAC Address 50:2B:73:FE:F4:98

IP Address Type Static IP Address

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.254

Primary DNS Server 8.8.8.8

Secondary DNS Server 8.8.4.4

Device Name CPE9V1.0

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

3.4 Common Buttons

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

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

4 Quick Setup

This module enables you to quickly configure the CPE to deploy your wireless network.

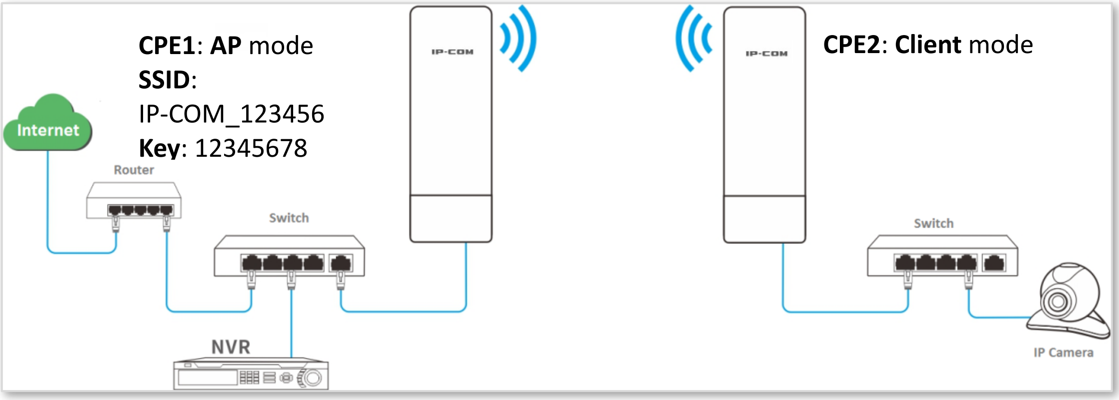
CPE3 supports AP, Client, and WISP modes. CPE9 supports AP, Client, Universal Repeater, WISP, Repeater, P2MP, and Router modes.

4.1 AP Mode

4.1.1 Overview

AP mode is the default mode of the CPE. In this mode, this CPE is connected to the internet in wired manner, and provides a WiFi network.

The CPE in AP mode can work with the CPE in Client or Universal Repeater mode. The following takes two CPEs either working in AP mode or Client mode to illustrate.

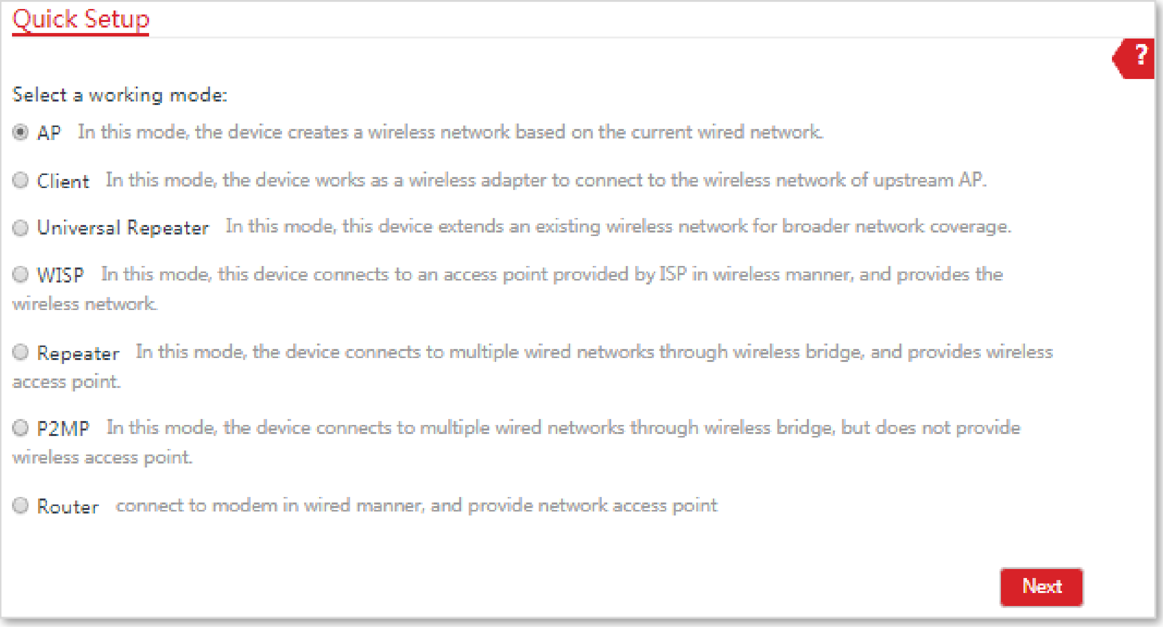


4.1.2 Setting up the AP Mode

Configuration Procedure:

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

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



Quick Setup

Select a working mode:

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

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

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

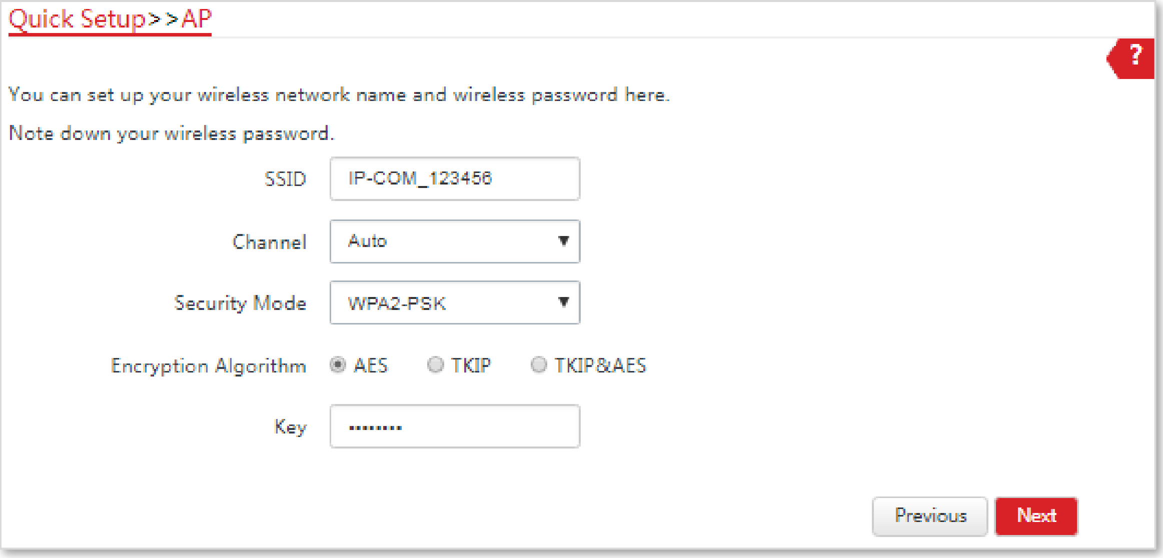
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

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

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

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

3. Set an SSID, which is **IP-COM_123456** in this example, **Security Mode** (WPA2-PSK is recommended), and **Key**, and click **Next**.



Quick Setup>>AP

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

Note down your wireless password.

SSID: IP-COM_123456

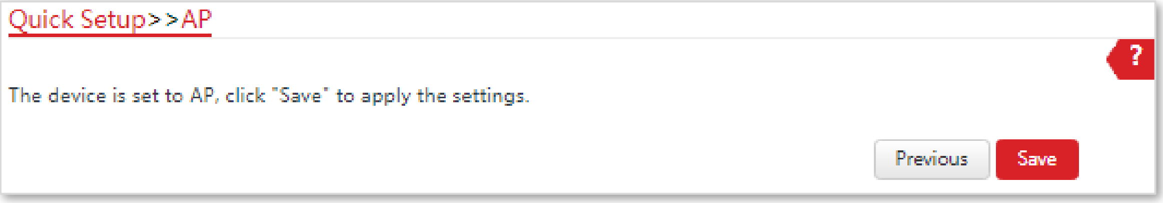
Channel: Auto

Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

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



Quick Setup>>AP

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

---End

Parameters Description

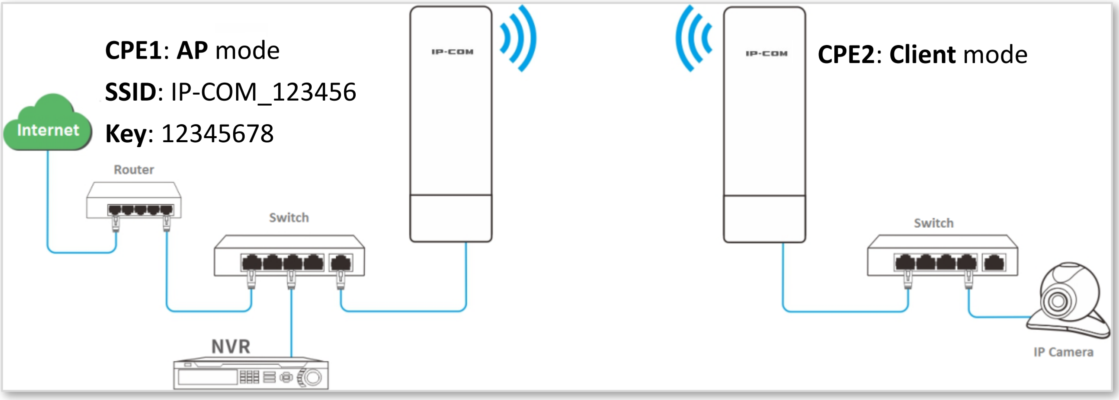
Name	Description
Working Modes	It specifies the working mode of the CPE. – **AP** mode: in this mode, the device creates a wireless network based on the current wired network. – **Client** mode: in this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point. – **Universal Repeater** mode: in this mode, this device expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function. – **WISP** mode: connect to an access point provided by ISP in wireless manner. – **Repeater** mode: the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device. – **P2MP** mode: this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city. – **Router** mode: in this mode, the **PoE LAN/WAN** port works as the WAN port and is used to connect to a modem for internet access.
SSID	It specifies the wireless network name of the CPE.
Channel	It specifies the operating channel of the CPE. **Auto**: It indicates that the CPE automatically adjusts its operating channel according to the ambient environment.
Security Mode	It specifies the security mode of the wireless network, including: None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

4.2 Client Mode

4.2.1 Overview

In Client mode, this CPE works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point.

The CPE in Client mode should work with the CPE in AP mode. See the following network topology:

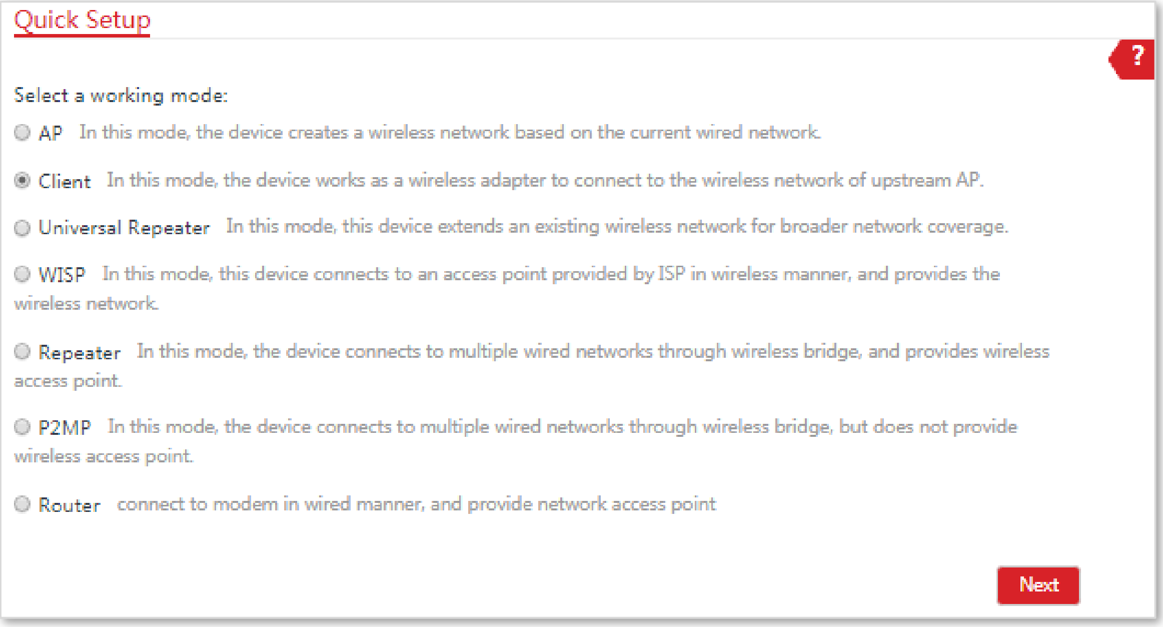


4.2.2 Setting up the Client Mode

Configuration Procedure:

Log in to the web UI of CPE2 and choose **Quick Setup** to enter the configuration page.

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



Quick Setup

Select a working mode:

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

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

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

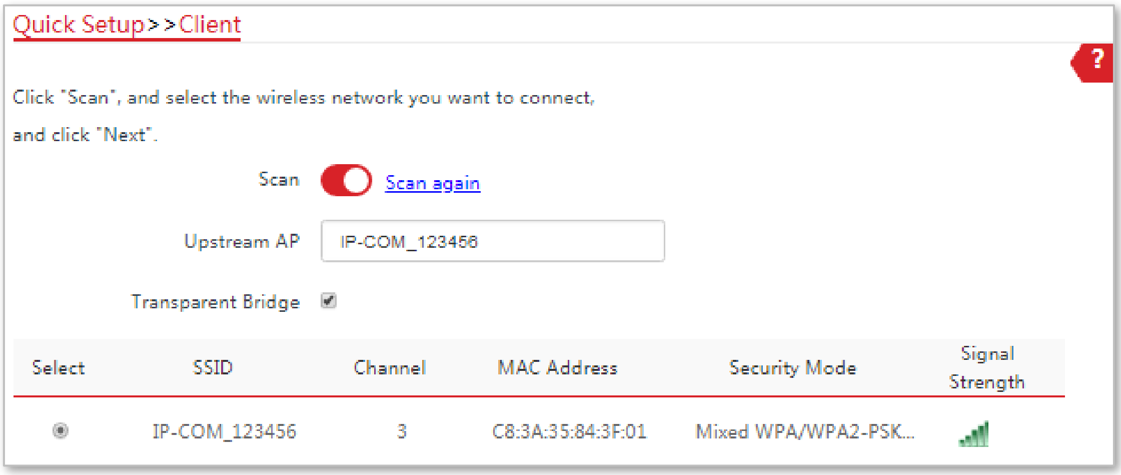
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

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

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

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

2. Select the SSID of the CPE1, which is **IP-COM_123456** in this example, and click **Next**.



Quick Setup>>Client

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

Scan: ● Scan again

Upstream AP: IP-COM_123456

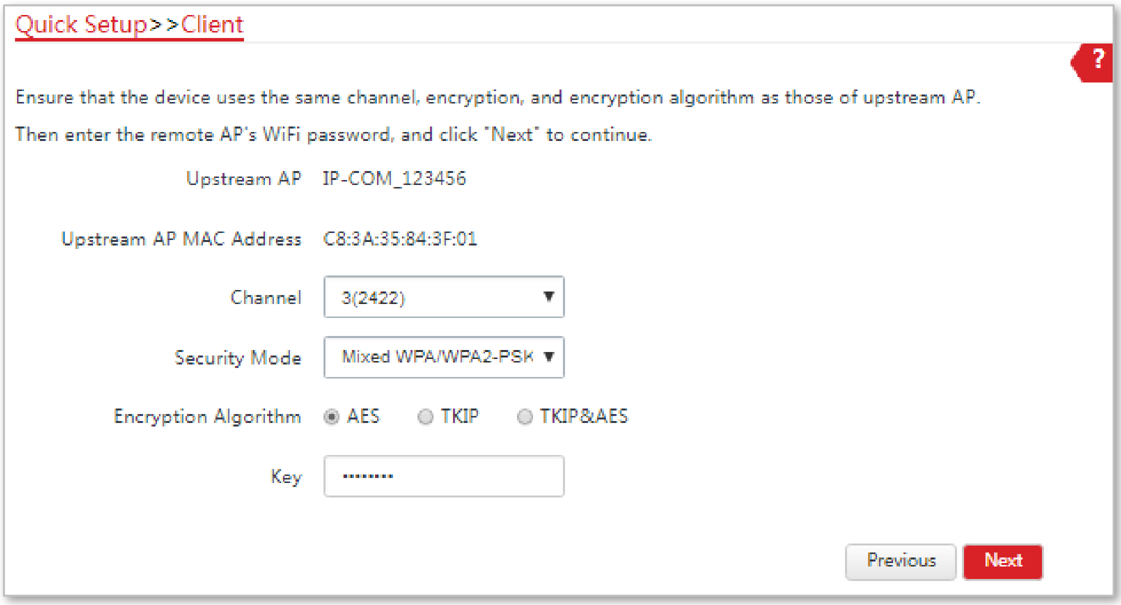
Transparent Bridge: ☑

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	IP-COM_123456	3	C8:3A:35:84:3F:01	Mixed WPA/WPA2-PSK...	

Tip

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

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



Quick Setup>>Client

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

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

Upstream AP IP-COM_123456

Upstream AP MAC Address C8:3A:35:84:3F:01

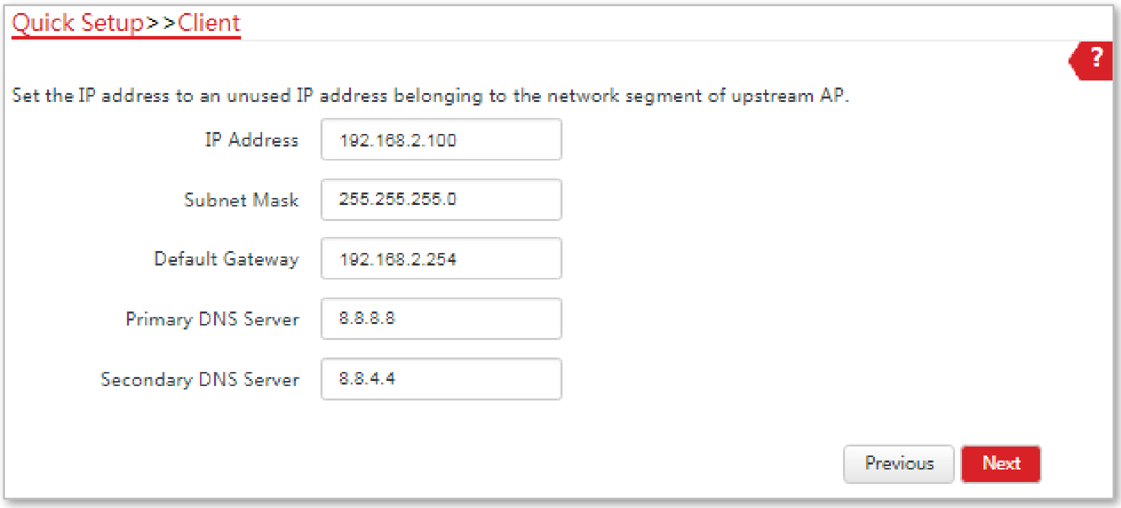
Channel 3(2422)

Security Mode Mixed WPA/WPA2-PSK

Encryption Algorithm ● AES ○ TKIP ○ TKIP&AES

Key ••••••••

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



Quick Setup>>Client

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

IP Address 192.168.2.100

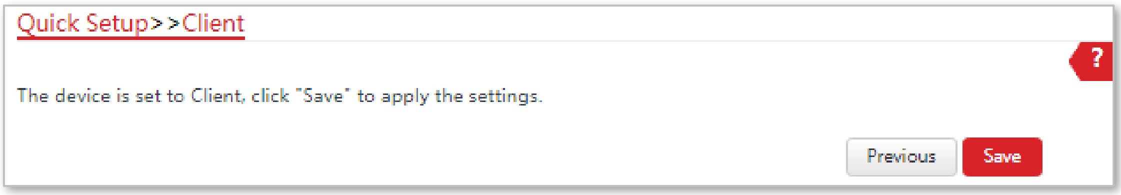
Subnet Mask 255.255.255.0

Default Gateway 192.168.2.254

Primary DNS Server 8.8.8.8

Secondary DNS Server 8.8.4.4

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



Quick Setup>>Client

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

---End

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

Tip

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

Parameters Description

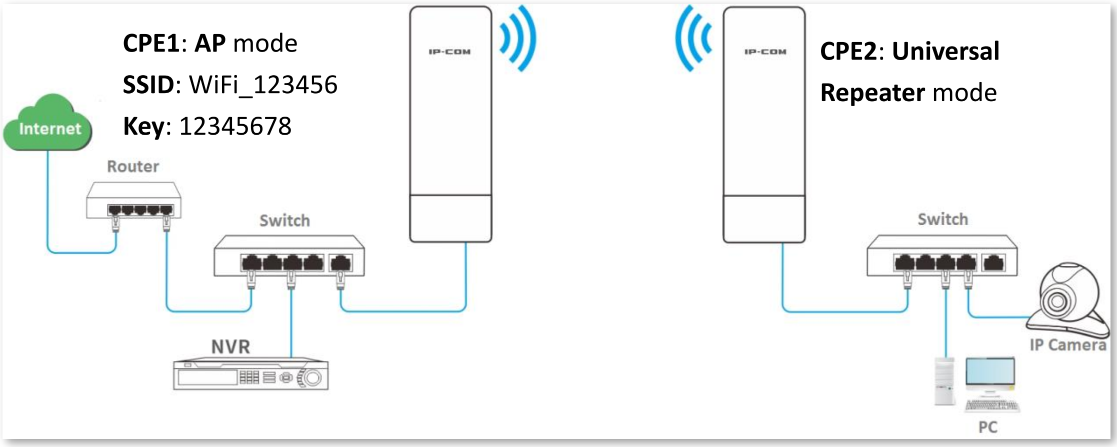
Name	Description
Working Modes	It specifies the working mode of the CPE. – **AP mode**: in this mode, the device creates a wireless network based on the current wired network. – **Client mode**: in this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point. – **Universal Repeater mode**: in this mode, this device expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function. – **WISP mode**: connect to an access point provided by ISP in wireless manner. – **Repeater** mode: the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device. – **P2MP** mode: this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city. – **Router mode**: in this mode, the PoE LAN/WAN port works as the WAN port and is used to connect to a modem for internet access.
Transparent Bridge	With the function enabled, IP cameras can be discovered by the NVR.
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

4.3 Universal Repeater Mode (Only for CPE9)

4.3.1 Overview

In Universal Repeater mode, this CPE expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function.

See the following network topology:

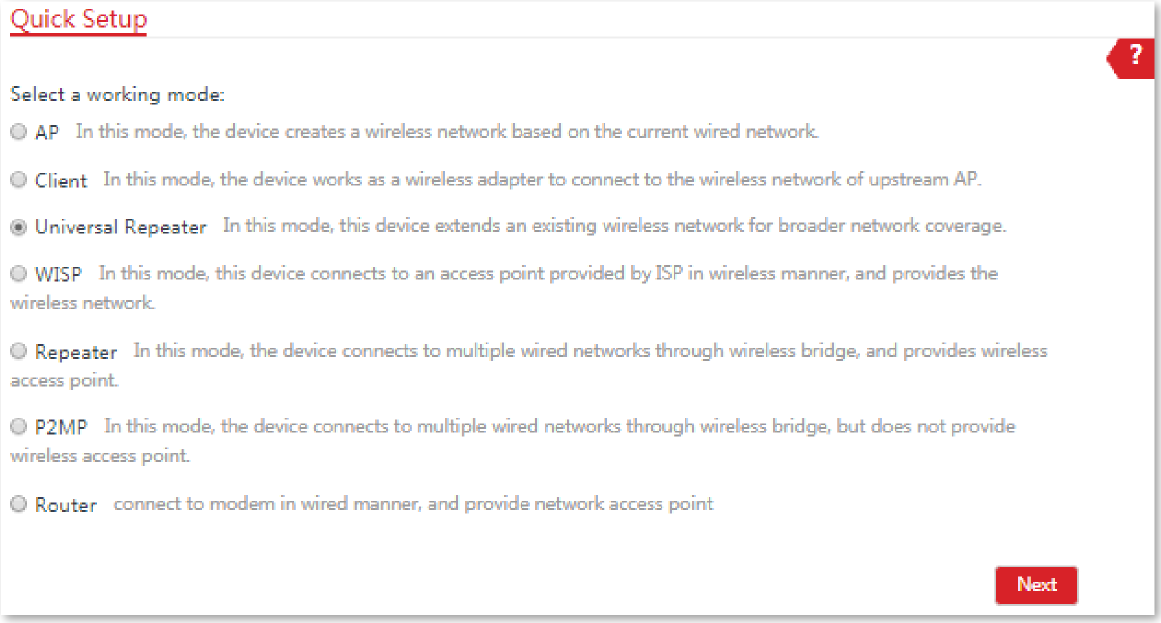


4.3.2 Setting up the Universal Repeater Mode

Configuration Procedure:

1. Log in to the web UI of the CPE2 and choose **Quick Setup** to enter the configuration page.

2. Select Universal Repeater, and click Next.



Quick Setup

Select a working mode:

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

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

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

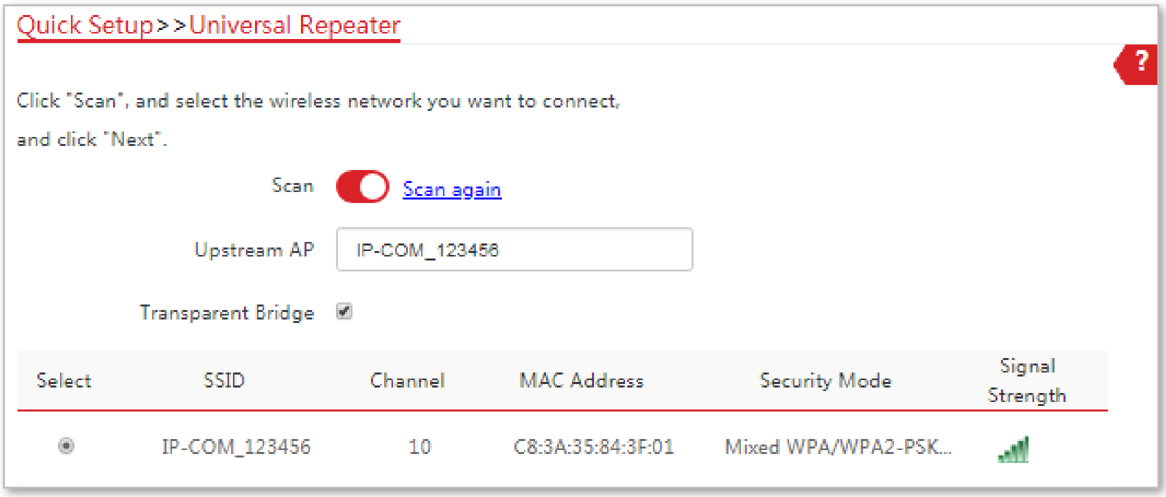
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

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

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

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

3. Select the SSID of CPE1 (the upstream AP), which is **IP-COM_123456** in this example, and click **Next**.



Quick Setup>>Universal Repeater

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

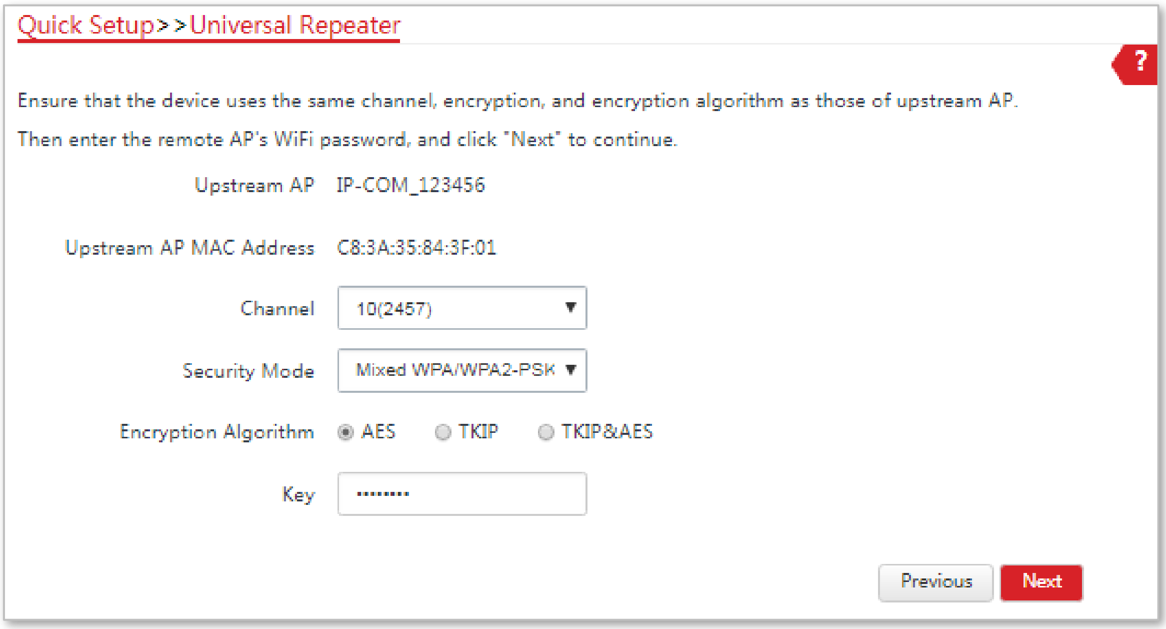
Scan: ● Scan again

Upstream AP: IP-COM_123456

Transparent Bridge: ☑

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	IP-COM_123456	10	C8:3A:35:84:3F:01	Mixed WPA/WPA2-PSK...	

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



Quick Setup>>Universal Repeater

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

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

Upstream AP: IP-COM_123456

Upstream AP MAC Address: C8:3A:35:84:3F:01

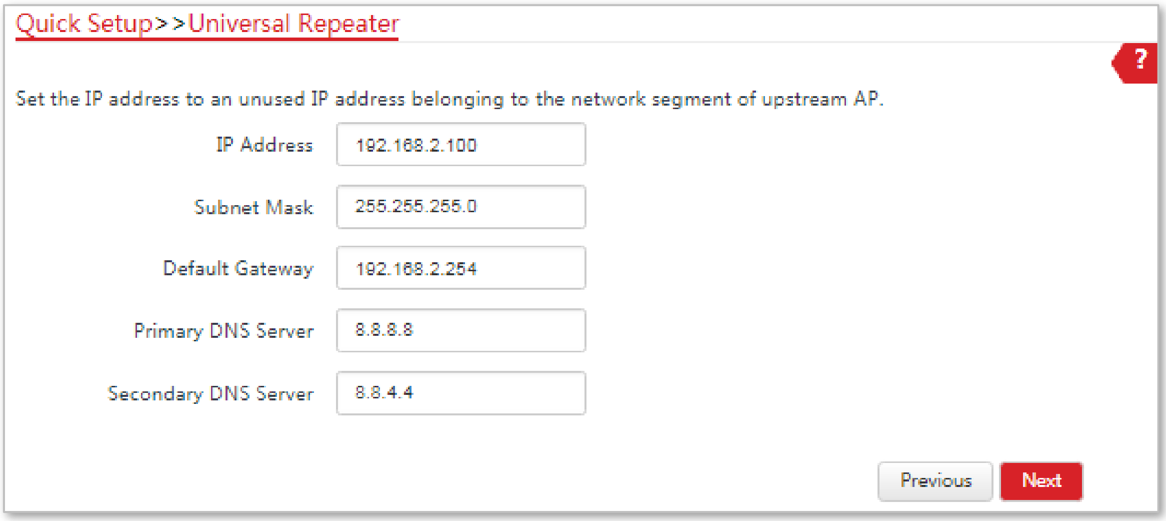
Channel: 10(2457)

Security Mode: Mixed WPA/WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ·········

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



Quick Setup>>Universal Repeater

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

IP Address: 192.168.2.100

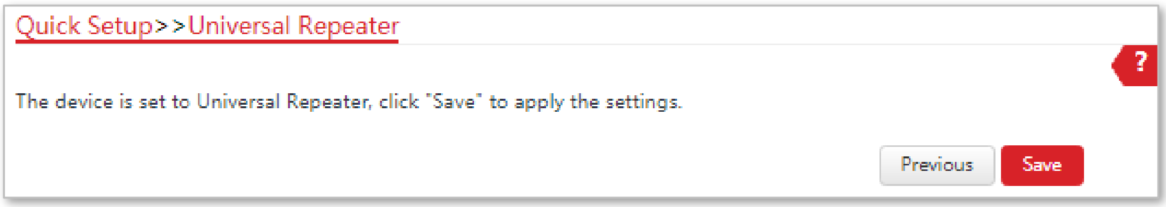
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.254

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

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



Quick Setup>>Universal Repeater

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

---End

Tip

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

Parameters Description

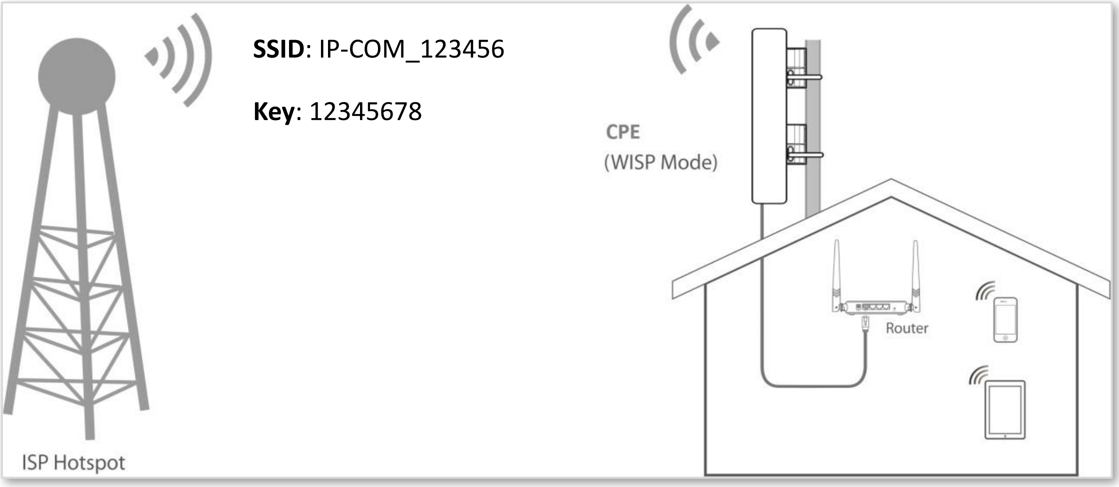
Name	Description
Working Modes	It specifies the working mode of the CPE. – **AP mode**: in this mode, the device creates a wireless network based on the current wired network. – **Client mode**: in this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point. – **Universal Repeater mode**: in this mode, this device expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function. – **WISP mode**: connect to an access point provided by ISP in wireless manner. – **Repeater** mode: the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device. – **P2MP** mode: this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city. – **Router mode**: in this mode, the PoE LAN/WAN port works as the WAN port and is used to connect to a modem for internet access.
Transparent Bridge	With the function enabled, IP cameras can be discovered by the NVR.
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

4.4 WISP Mode

4.4.1 Overview

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

See the following network topology:

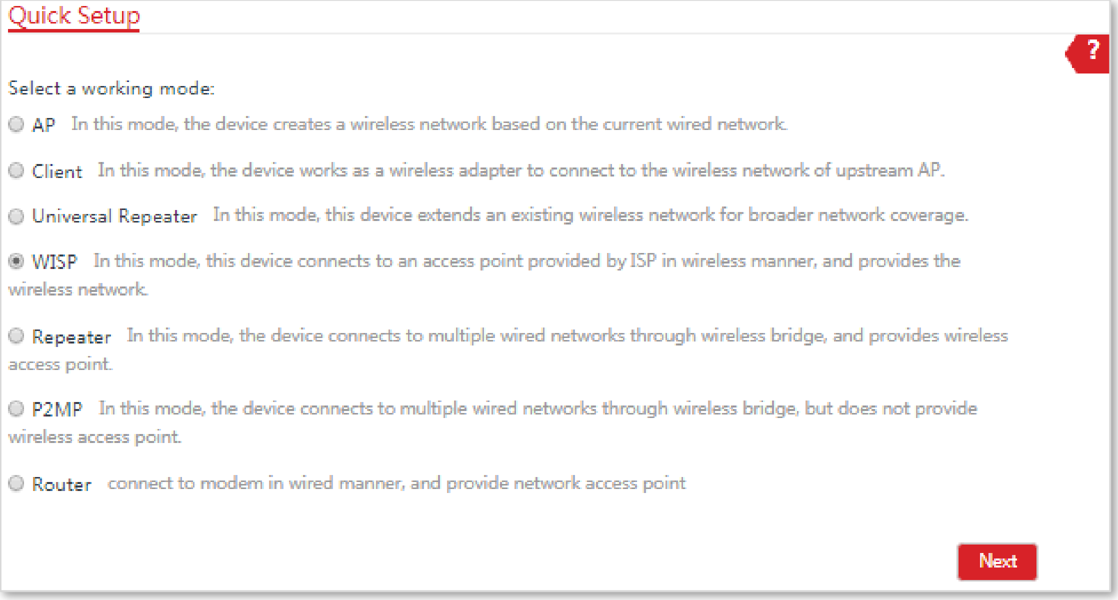


4.4.2 Setting up the WISP Mode

Configuration Procedure:

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

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



Quick Setup

Select a working mode:

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

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

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

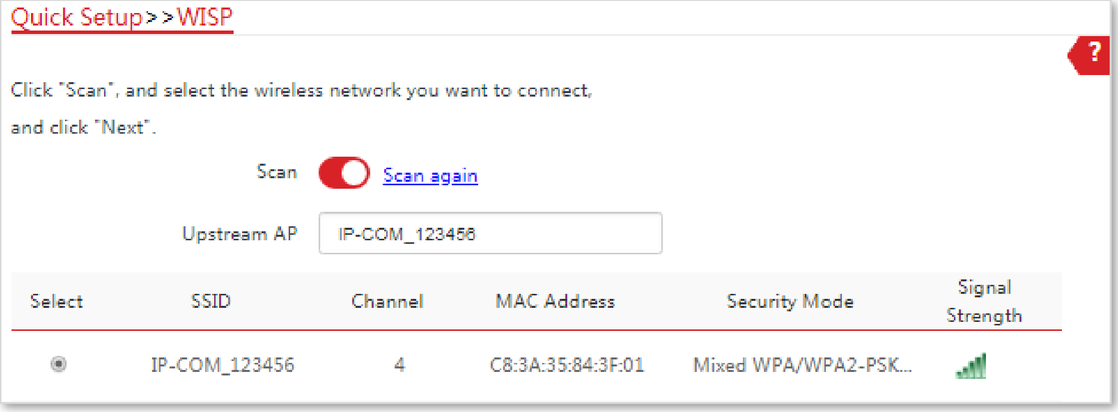
● WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

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

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

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

3. Select the SSID of your ISP (Internet Service Provider) hotspot, which is **IP-COM_123456** in this example, and click **Next**.



Quick Setup>>WISP

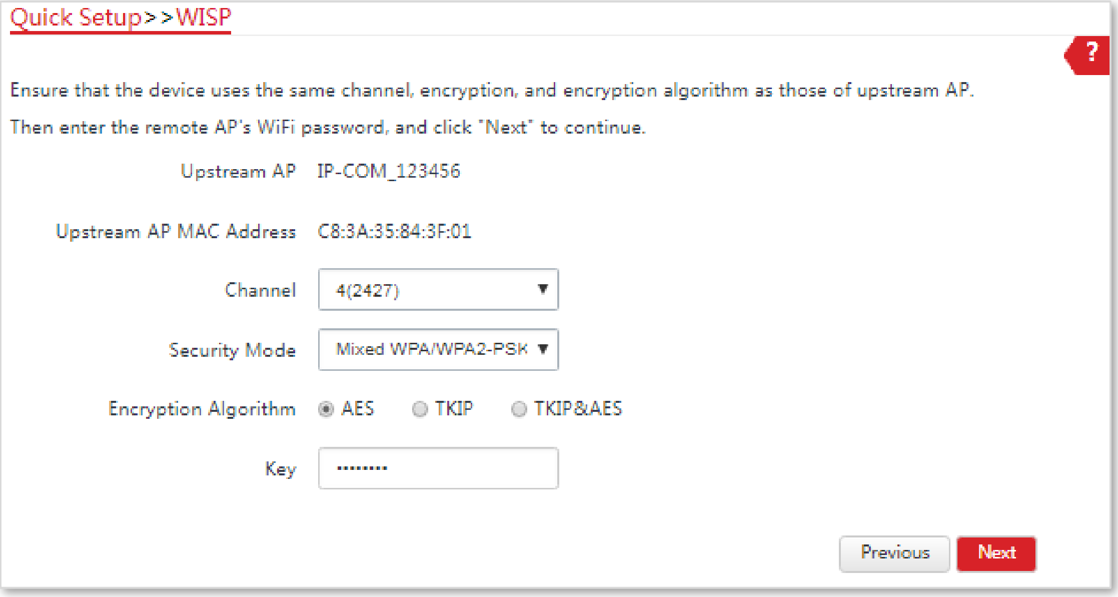
Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan ● Scan again

Upstream AP IP-COM_123456

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
●	IP-COM_123456	4	C8:3A:35:84:3F:01	Mixed WPA/WPA2-PSK...	

4. Enter the WiFi password of your ISP (Internet Service Provider) hotspot in the **Key** text box, and click **Next**.



Quick Setup>>WISP

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

Upstream AP IP-COM_123456

Upstream AP MAC Address C8:3A:35:84:3F:01

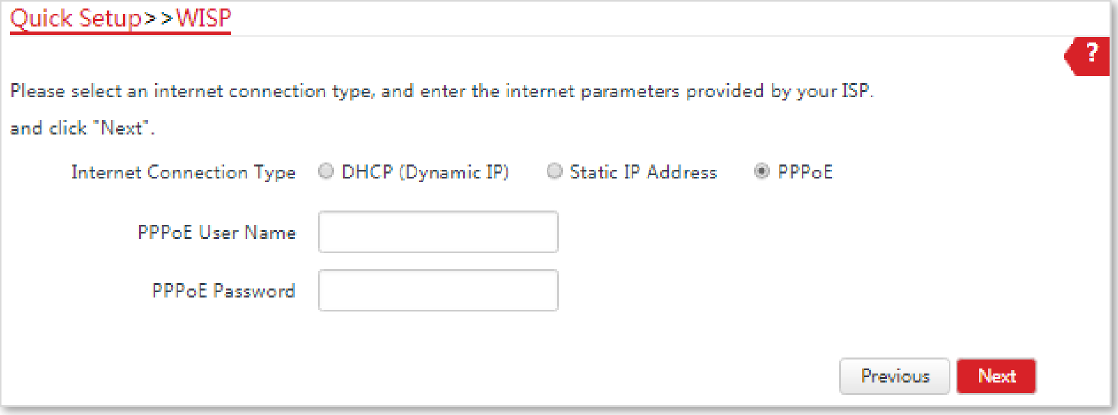
Channel 4(2427)

Security Mode Mixed WPA/WPA2-PSK

Encryption Algorithm ● AES ○ TKIP ○ TKIP&AES

Key ••••••••

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



Quick Setup>>WISP

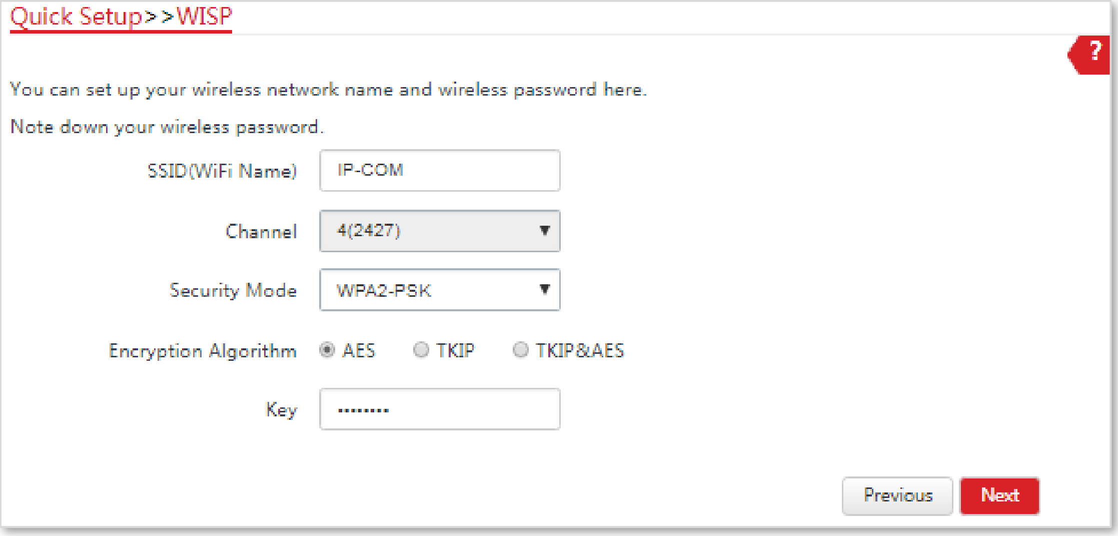
Please select an internet connection type, and enter the internet parameters provided by your ISP.
and click "Next".

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

PPPoE User Name

PPPoE Password

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



Quick Setup>>WISP

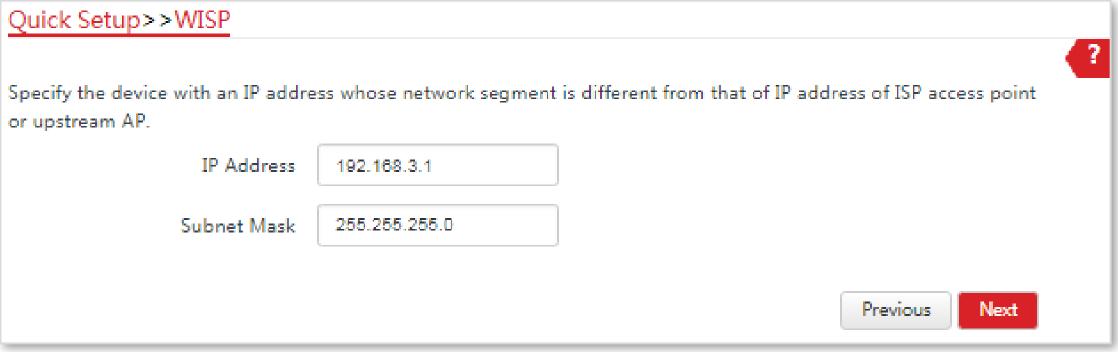
You can set up your wireless network name and wireless password here.

Note down your wireless password.

SSID(WiFi Name)	IP-COM
Channel	4(2427)
Security Mode	WPA2-PSK
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Key	••••••••

7. Set an IP address belonging to different network segment as that of your ISP hotspot. For example, if the IP address of your ISP hotspot is 192.168.2.1, you can set this device's IP address to 192.168.*X*.1 (*X* ranges from 0 to 254 excluding2). Then click **Next**.

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



Quick Setup>>WISP

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

IP Address	192.168.3.1
Subnet Mask	255.255.255.0

---End

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

Tip

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

Parameters Description

Name	Description
Working Modes	It specifies the working mode of the CPE. – **AP mode**: in this mode, the device creates a wireless network based on the current wired network. – **Client mode**: in this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point. – **Universal Repeater mode**: in this mode, this device expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function. – **WISP mode**: connect to an access point provided by ISP in wireless manner. – **Repeater** mode: the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device. – **P2MP** mode: this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city. – **Router mode**: in this mode, the PoE LAN/WAN port works as the WAN port and is used to connect to a modem for internet access.
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.
Internet Connection Type	– **DHCP (Dynamic IP)**: The CPE obtains IP address and other parameters form the DHCP server of upstream device for internet access. – **Static IP Address**: The CPE access the internet by setting the IP address, subnet mask, default gateway and DNS server IP addresses manually. – **PPPoE**: The CPE access the internet using the PPPoE user name and password provided by the ISP.

4.5 Repeater Mode (Only for CPE9)

4.5.1 Overview

In Repeater mode, the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use this function, the peer AP is required to support WDS function. Repeater mode is used to achieve communication between multiple offices of an enterprise in a city.

The CPE in Repeater mode can works with the CPE in Repeater or P2MP mode. It supports one to four bridging at most.

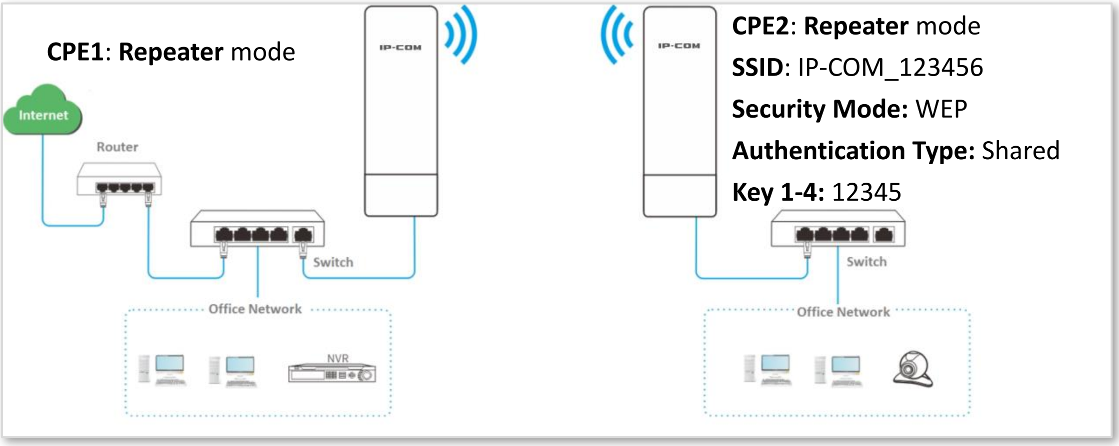
4.5.2 Setting up the Repeater Mode

One to One Bridging

Assume that CPE1 and CPE2 both work in Repeater mode and the wireless parameters of CPE2 are as follows:

- **SSID**: IP-COM_123456
- **Security mode**: WEP
- **Authentication type**: Shared
- **Key1 to key4**: 1234

See the following network topology:

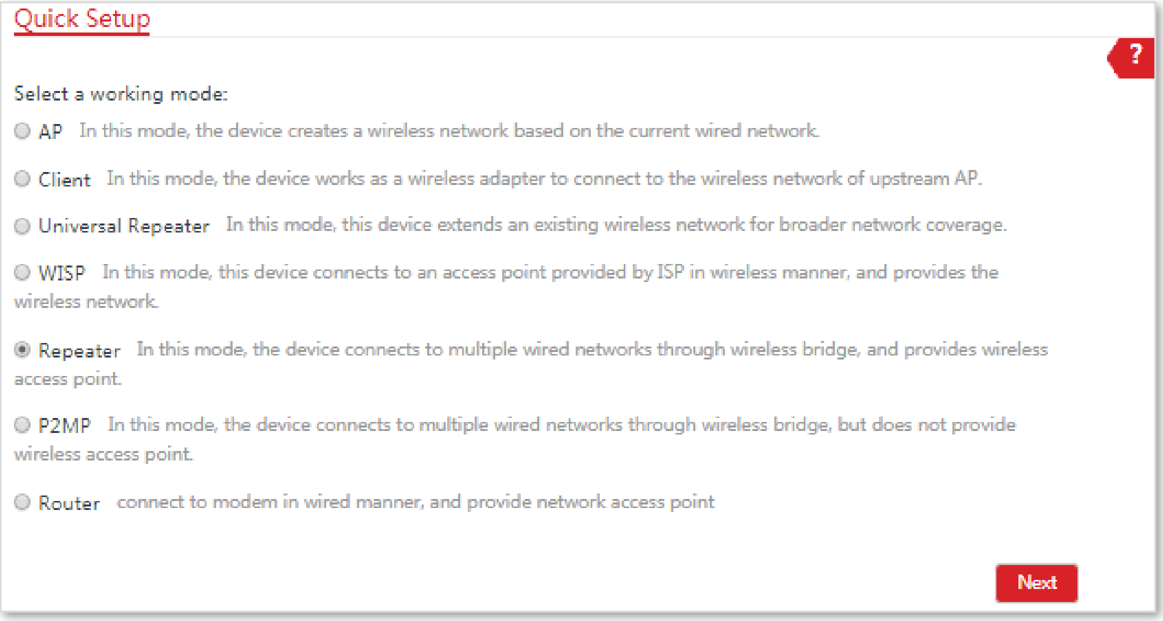


Configuration Procedure:

1. Set **CPE1** to the **Repeater** mode.

   (1) Log in to the web UI of CPE1 and choose **Quick Setup** to enter the configuration page.

(2) Select the SSID of CPE2, which is **IP-COM_123456** in this example, and click **Next**.



Quick Setup

Select a working mode:

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

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

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

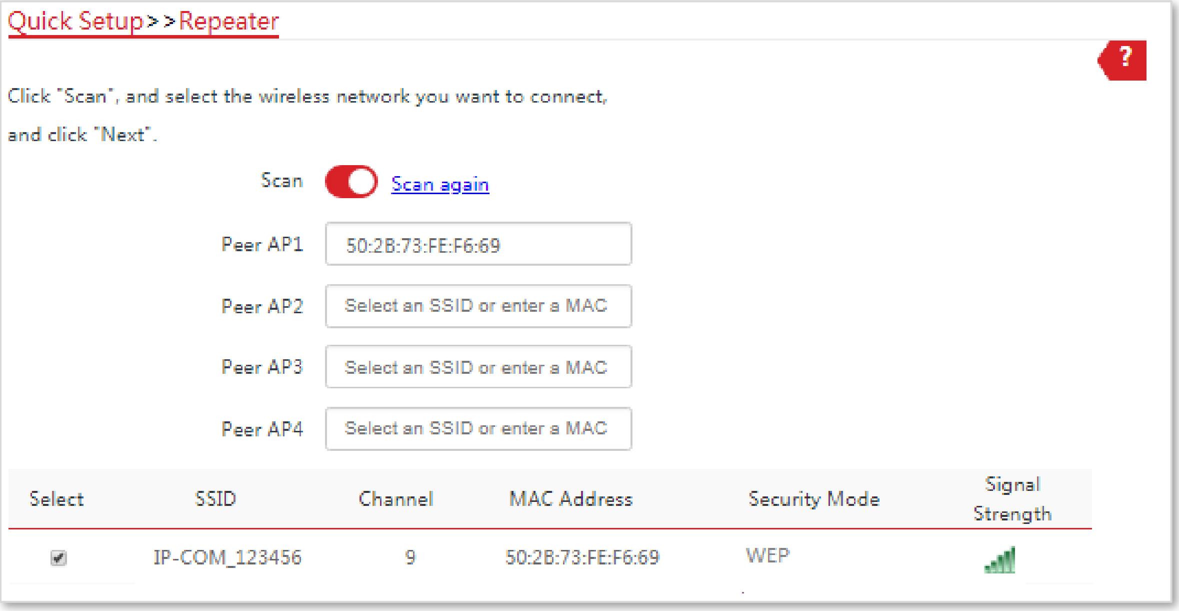
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.

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

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

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

(3) Select the SSID of CPE2 from the list and click **Next**.



Quick Setup>>Repeater

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

Scan: on — Scan again

Peer AP1: 50:2B:73:FE:F6:69

Peer AP2: Select an SSID or enter a MAC

Peer AP3: Select an SSID or enter a MAC

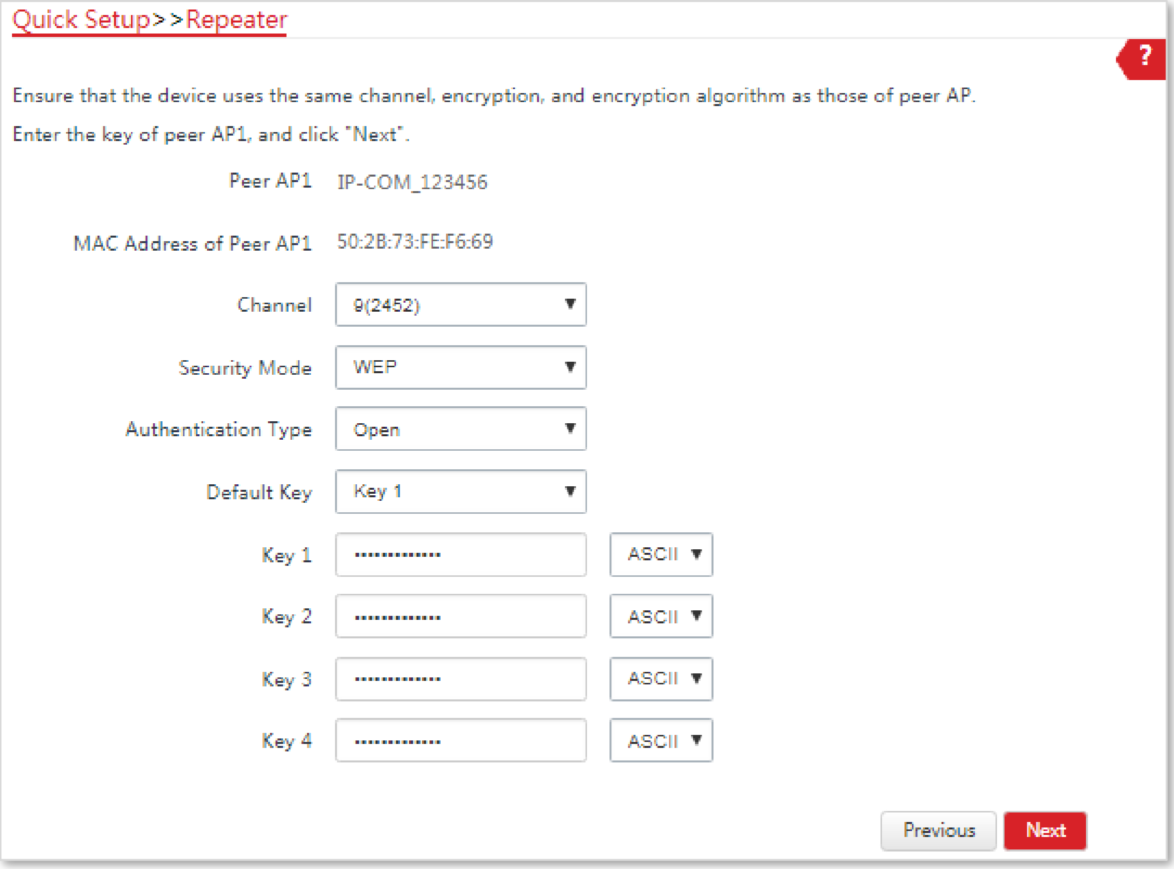
Peer AP4: Select an SSID or enter a MAC

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_123456	9	50:2B:73:FE:F6:69	WEP	

Tip

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

(4) Set the **Authentication Type** and **Default Key** to the same as those of CPE2, enter the key 1, key2, key 3 and key4, and click **Next**.



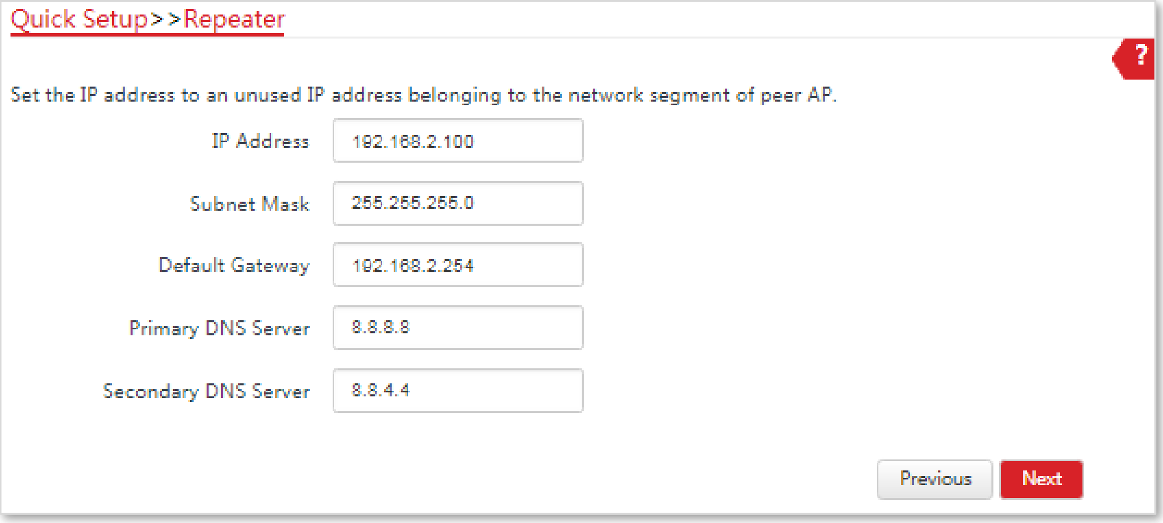
Quick Setup>>Repeater

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

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

Peer AP1	IP-COM_123456	
MAC Address of Peer AP1	50:2B:73:FE:F6:69	
Channel	9(2452)	
Security Mode	WEP	
Authentication Type	Open	
Default Key	Key 1	
Key 1	•••••••••••••	ASCII
Key 2	•••••••••••••	ASCII
Key 3	•••••••••••••	ASCII
Key 4	•••••••••••••	ASCII

(5) Set the IP address to an unused IP address belonging to the same network segment as that of CPE2. For example, if the IP address of CPE2 is 192.168.2.1, you can set this device's IP address to 192.168.2.*X* (*X* ranges from 2 to 254). Then click **Next**.

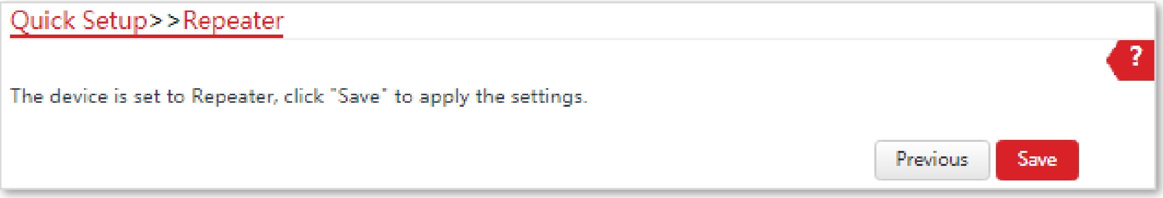


Quick Setup>>Repeater

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

IP Address	192.168.2.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4

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



Quick Setup>>Repeater

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

2. Perform the procedure in step 1 above to set **CPE2** to the **Repeater** mode.

---End

Tip

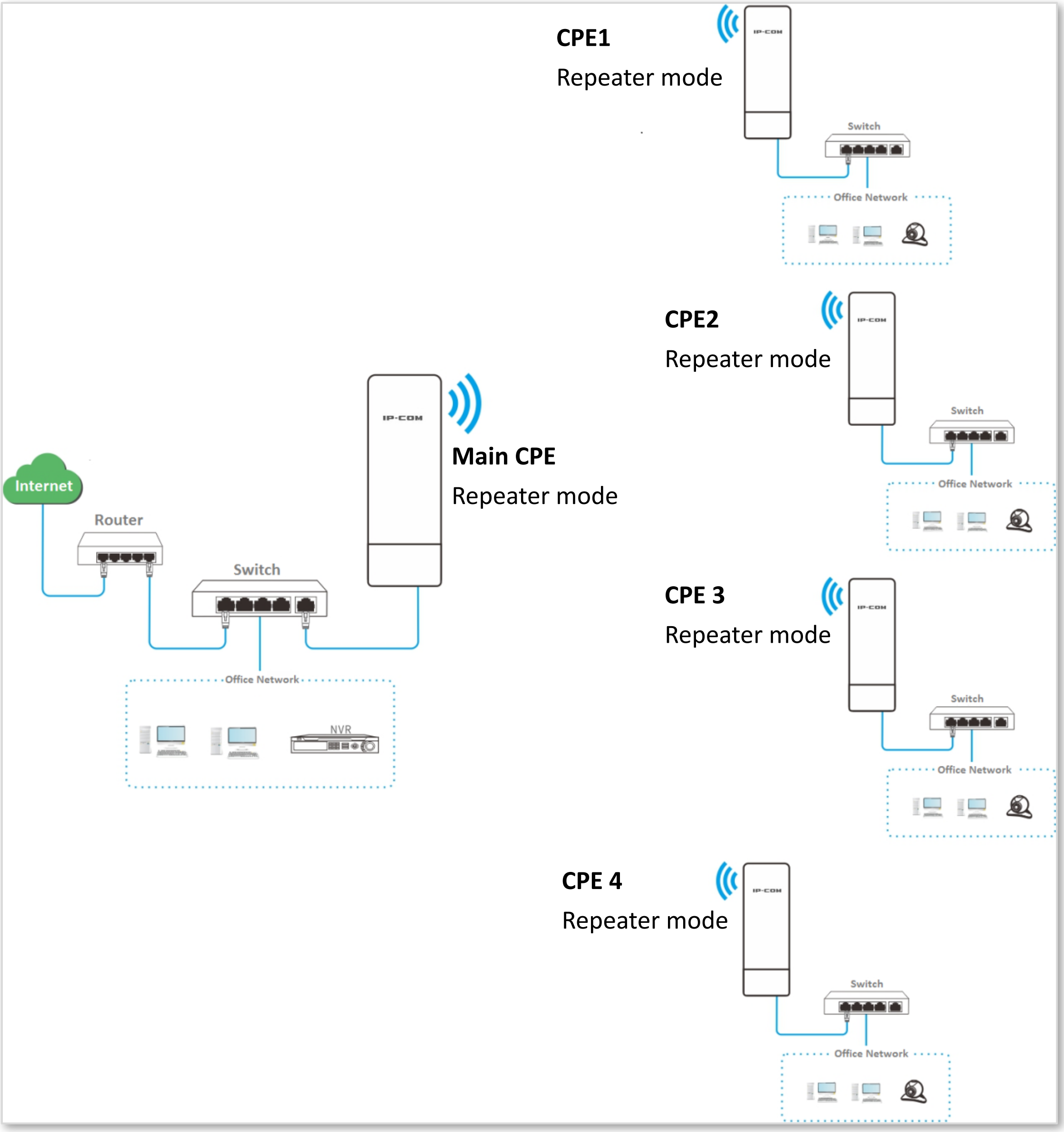
You can check the SSID and key of the CPE by choosing **Wireless** > **Basic** after logging in to the web UI.

Parameters Description

Name	Description
Working Modes	It specifies the working mode of the CPE. – **AP mode**: in this mode, the device creates a wireless network based on the current wired network. – **Client mode**: in this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point. – **Universal Repeater mode**: in this mode, this device expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function. – **WISP mode**: connect to an access point provided by ISP in wireless manner. – **Repeater** mode: the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device. – **P2MP** mode: this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city. – **Router mode**: in this mode, the PoE LAN/WAN port works as the WAN port and is used to connect to a modem for internet access.
Peer AP	It specifies the wireless network name (SSID) of the peer AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. Tip The Repeater mode only supports WEP and None security modes.

One to Four Briding

See the following network topology:



Assume that the related parameters of the main CPE is shown as follows:

- **IP address**: 192.168.2.1
- **SSID**: IP-COM_1
- **Channel**: 11
- **Security mode**: None

Configuration procedure:

1. Set CPE1 to **Repeater** mode to bridge the main CPE.

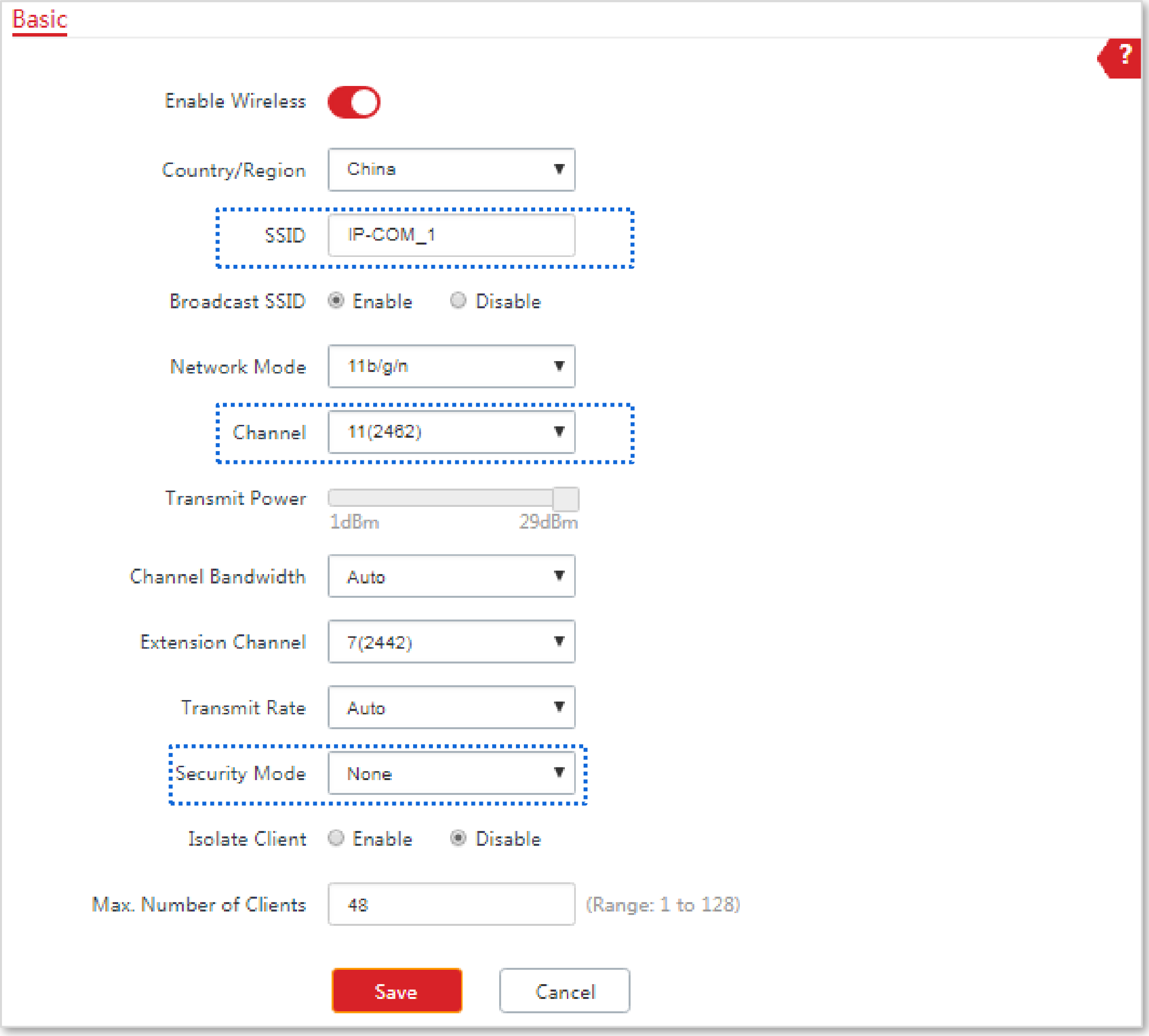
   (1) Log in to the web UI of CPE1, and choose **Wireless > Basic** to enter the configuration page.

   (2) Customize an SSID, which is **IP-COM_2** in this example.

   (3) Set the **Channel** to the same as that of the main CPE, which is **11** in this example.

(4) Set the **Security Mode** to the same as that of the main CPE, which is **None** in this example.

(5) Click **Save** to apply the settings.



Enable Wireless ●

Country/Region: China

SSID: IP-COM_1

Broadcast SSID: ● Enable ○ Disable

Network Mode: 11b/g/n

Channel: 11(2462)

Transmit Power: 1dBm 29dBm

Channel Bandwidth: Auto

Extension Channel: 7(2442)

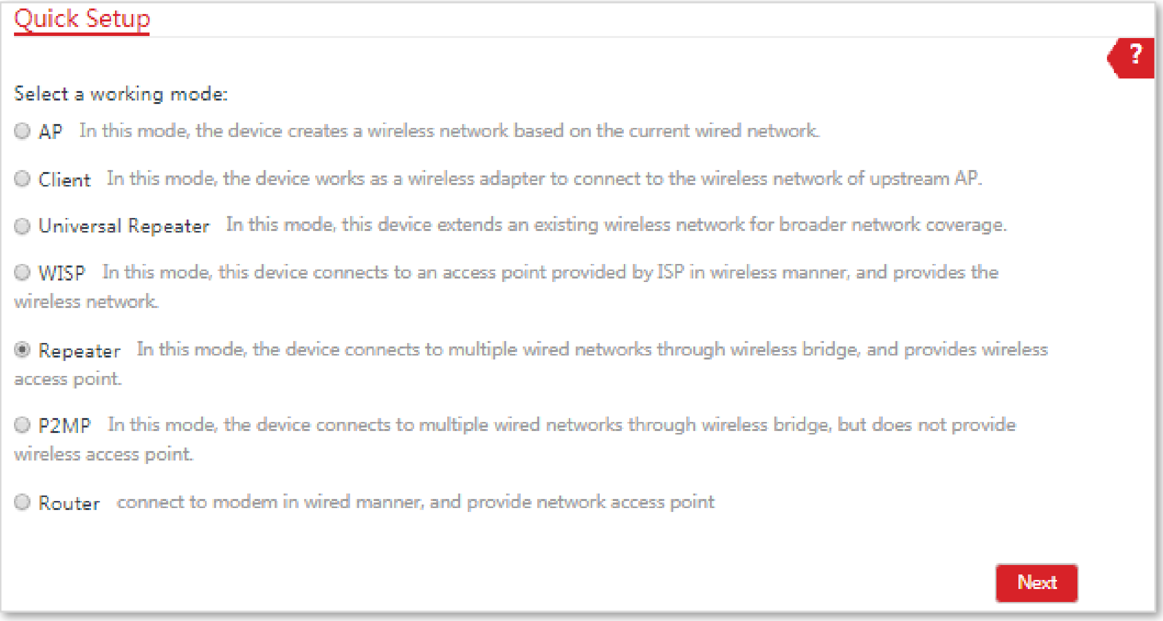
Transmit Rate: Auto

Security Mode: None

Isolate Client: ○ Enable ● Disable

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

(6) Choose **Quick Setup**, select **Repeater** mode, and click **Next**.



Quick Setup

Select a working mode:

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

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

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

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

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

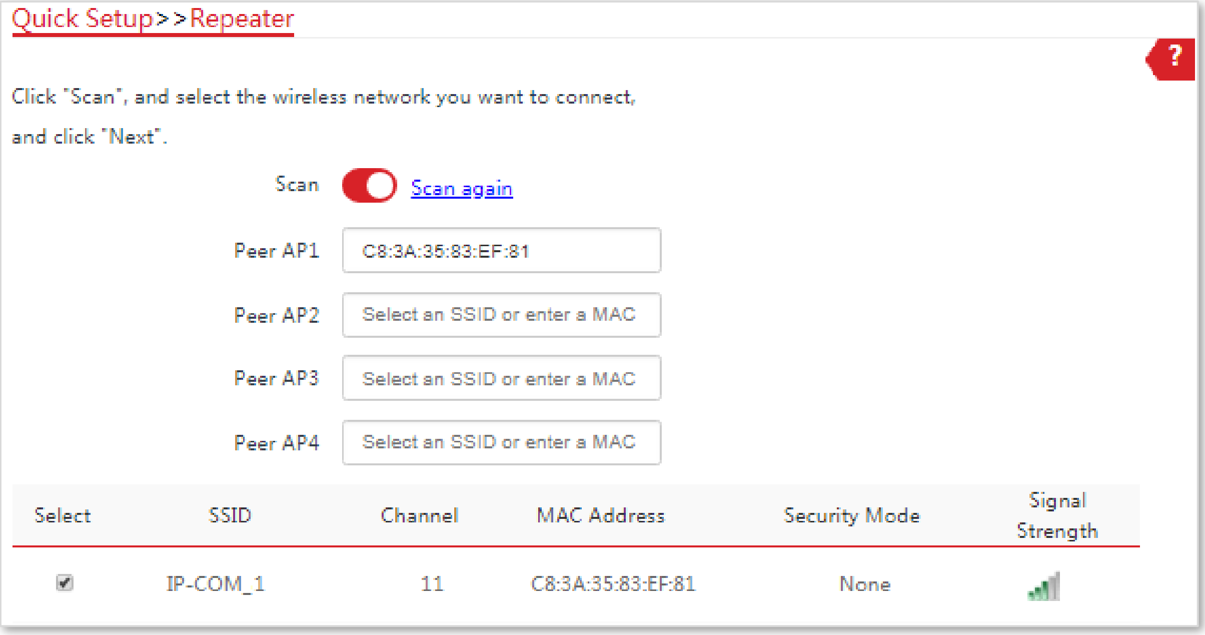
○ P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.

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

(7) Select the SSID of the main CPE from the list, which is **IP-COM_1** in this example, and click **Next**.

Tip

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



Quick Setup>>Repeater

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

Scan: ● Scan again

Peer AP1: C8:3A:35:83:EF:81

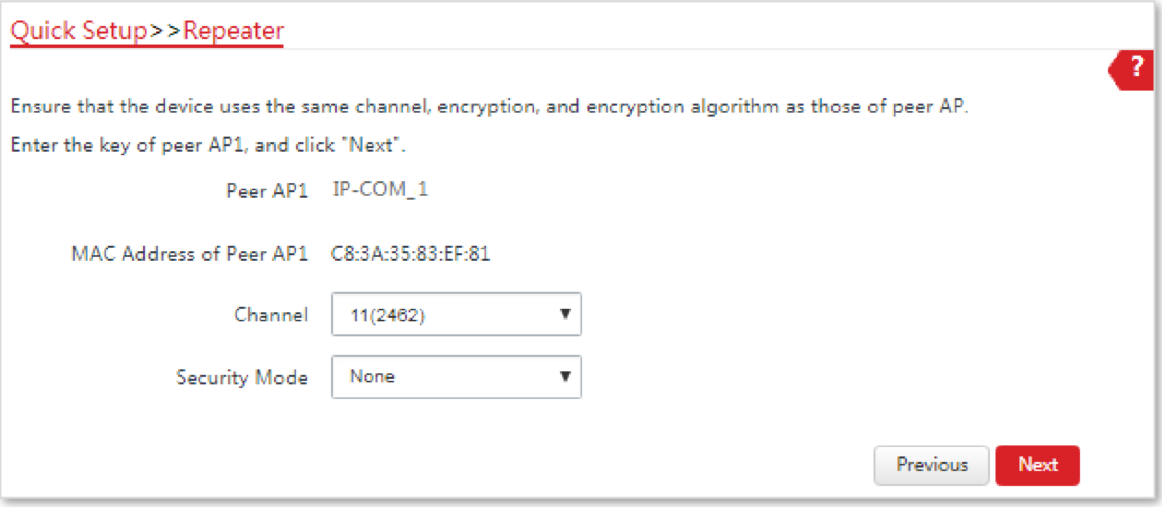
Peer AP2: Select an SSID or enter a MAC

Peer AP3: Select an SSID or enter a MAC

Peer AP4: Select an SSID or enter a MAC

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_1	11	C8:3A:35:83:EF:81	None	

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



Quick Setup>>Repeater

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

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

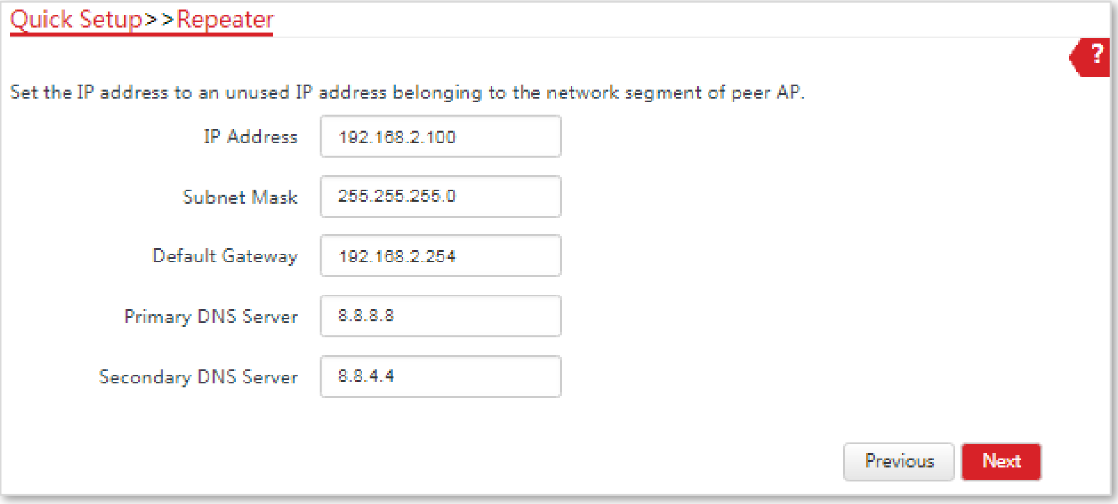
Peer AP1 IP-COM_1

MAC Address of Peer AP1 C8:3A:35:83:EF:81

Channel 11(2462)

Security Mode None

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



Quick Setup>>Repeater

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

IP Address 192.168.2.100

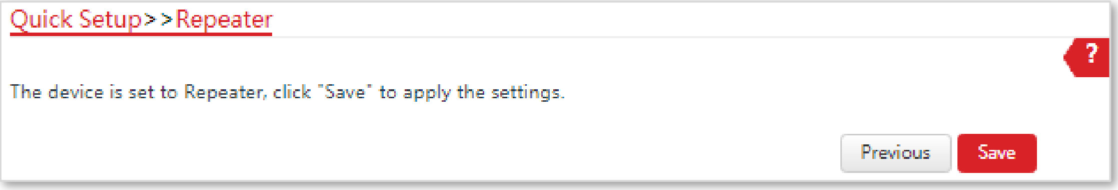
Subnet Mask 255.255.255.0

Default Gateway 192.168.2.254

Primary DNS Server 8.8.8.8

Secondary DNS Server 8.8.4.4

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



Quick Setup>>Repeater

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

2. Perform Step 1 above to set **CPE2**, **CPE3** and **CPE4** to **Repeater** mode respectively.

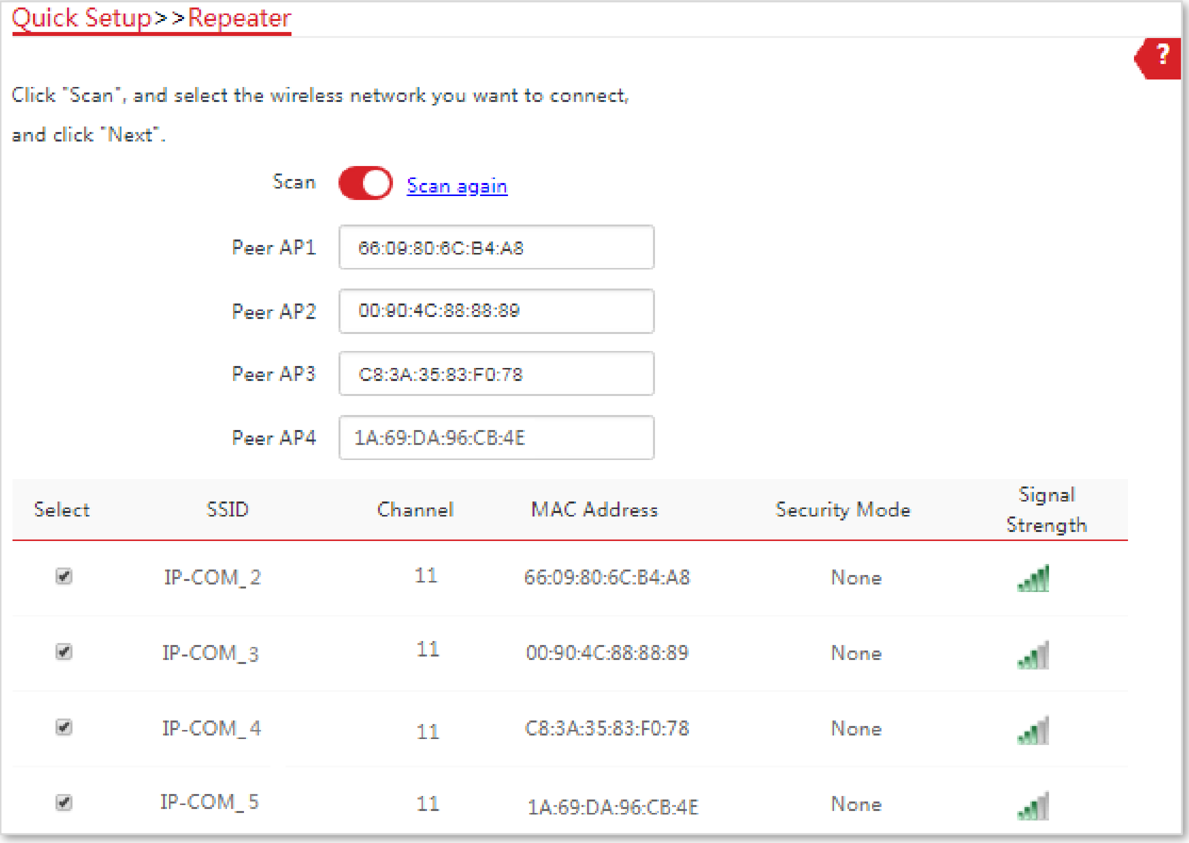
3. Set the main CPE to **Repeater** mode to bridge CPE1, CPE2, CPE3 and CPE4.

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

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

(3) Select SSIDs of CPE1, CPE2, CPE3 and CPE4 respectively, and click **Next**.

(4) Click **Next** at the bottom of the following page.



Quick Setup>>Repeater

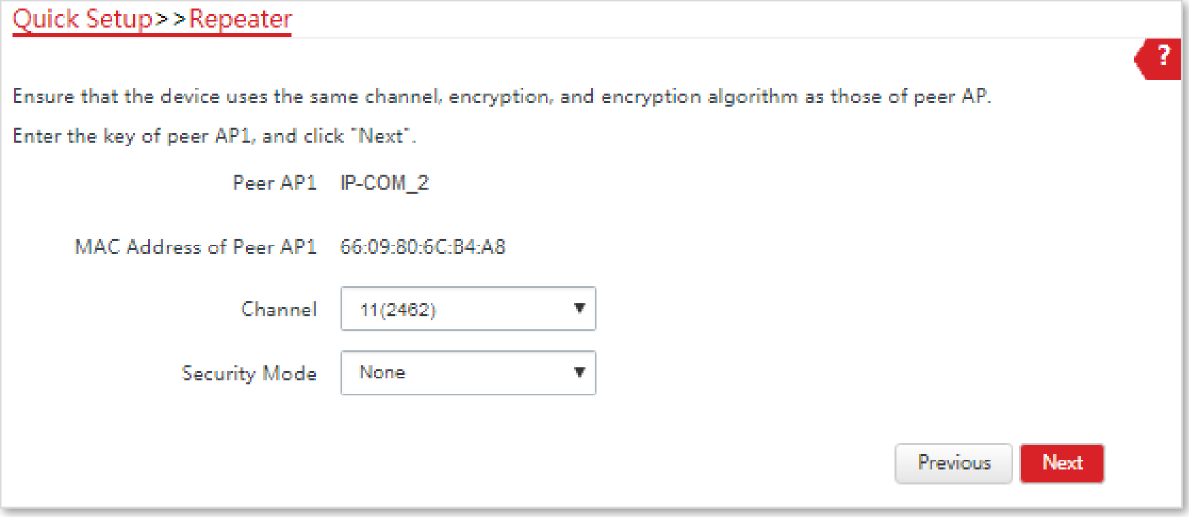
Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan: On [Scan again](#)

Peer AP1	66:09:80:6C:B4:A8
Peer AP2	00:90:4C:88:88:89
Peer AP3	C8:3A:35:83:F0:78
Peer AP4	1A:69:DA:96:CB:4E

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_2	11	66:09:80:6C:B4:A8	None	
☑	IP-COM_3	11	00:90:4C:88:88:89	None	
☑	IP-COM_4	11	C8:3A:35:83:F0:78	None	
☑	IP-COM_5	11	1A:69:DA:96:CB:4E	None	

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

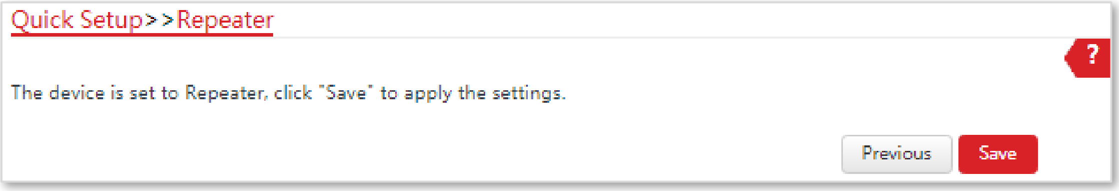


Quick Setup>>Repeater

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

Peer AP1	IP-COM_2
MAC Address of Peer AP1	66:09:80:6C:B4:A8
Channel	11(2462)
Security Mode	None

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



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

---End

4.6 P2MP Mode (Only for CPE9)

4.6.1 Overview

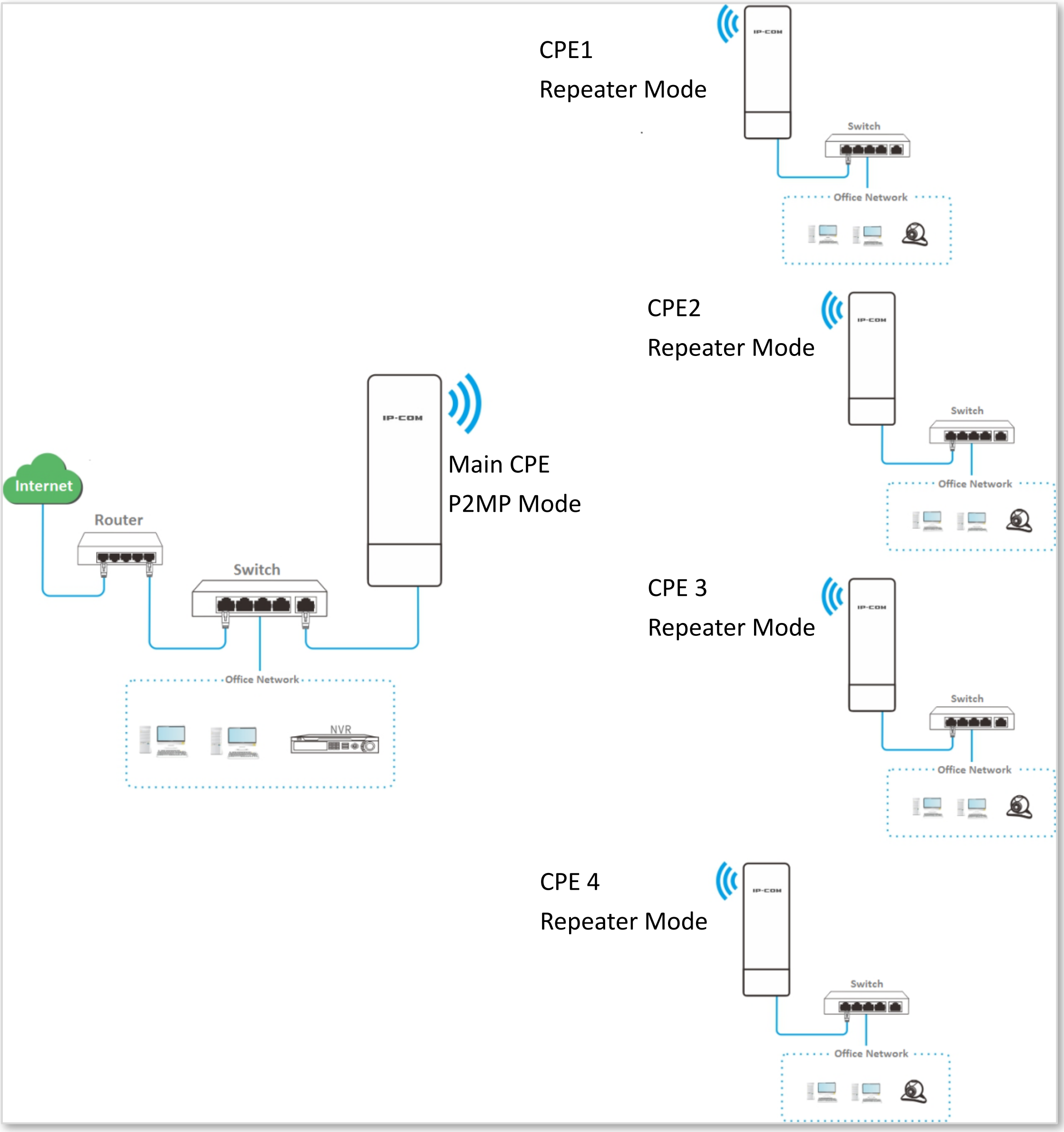
In P2MP mode, this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city.

The CPE in P2MP mode can work with the CPE in Repeater or P2MP mode. It supports one to four bridging at most.

4.6.2 Setting up P2MP Mode

The configuration procedure of P2MP mode is similar to that of Repeater mode. The following example shows that the main CPE in P2MP mode bridges to four CPEs in Repeater mode.

See the following network topology:



Assume that the related parameters of the main CPE is shown as follows:

- **IP Address**: 192.168.2.1
- **SSID**: IP-COM_1
- **Channel**: 11
- **Security Mode**: None

Configuration Procedure:

1. Set the CPE1 to **Repeater** mode to bridge the main CPE.

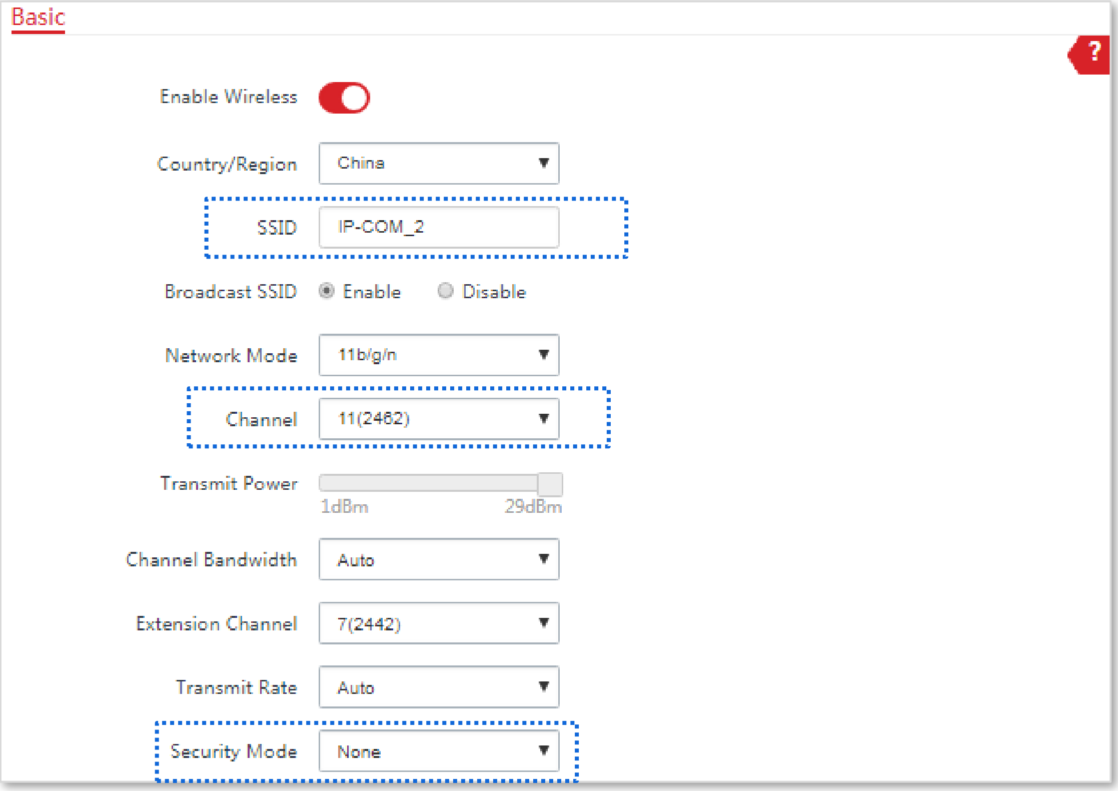
(1) Log in to the web UI of CPE1, and choose **Wireless** > **Basic** to enter the configuration page.

(2) Customize the **SSID**, which is **IP-COM_2** in this example.

(3) Set the **Channel** to the same as that of the main CPE, which is **11** in this example.

(4) Set the **Security mode** to the same as that of the main CPE, which is **None** in this example.

(5) Click **Save** to apply the settings.



Basic

Enable Wireless ●

Country/Region: China

SSID: IP-COM_2

Broadcast SSID: ● Enable ○ Disable

Network Mode: 11b/g/n

Channel: 11(2462)

Transmit Power: 1dBm 29dBm

Channel Bandwidth: Auto

Extension Channel: 7(2442)

Transmit Rate: Auto

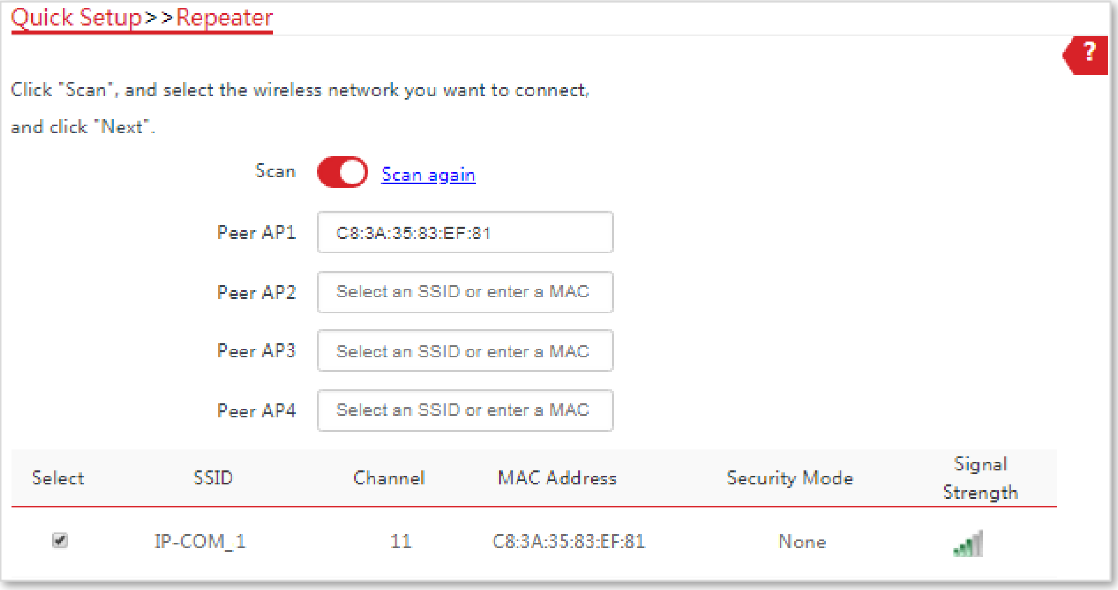
Security Mode: None

(6) Choose **Quick Setup**, select **Repeater** mode, and click **Next**.

(7) Select the SSID of the main CPE, which is **IP-COM_1** in this example, and click **Next**.

Tip

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



Quick Setup>>Repeater

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

Scan ● Scan again

Peer AP1: C8:3A:35:83:EF:81

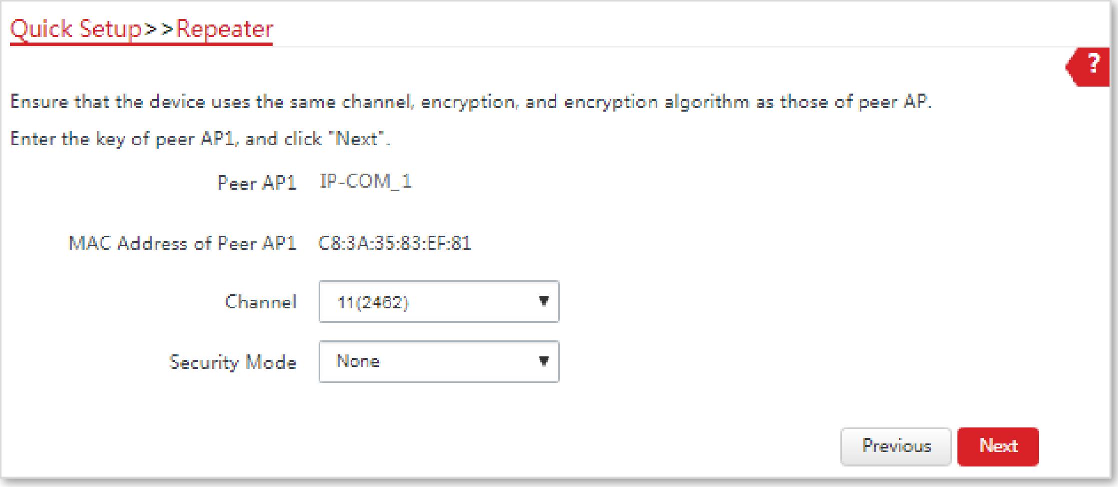
Peer AP2: Select an SSID or enter a MAC

Peer AP3: Select an SSID or enter a MAC

Peer AP4: Select an SSID or enter a MAC

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_1	11	C8:3A:35:83:EF:81	None	

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



Quick Setup>>Repeater

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

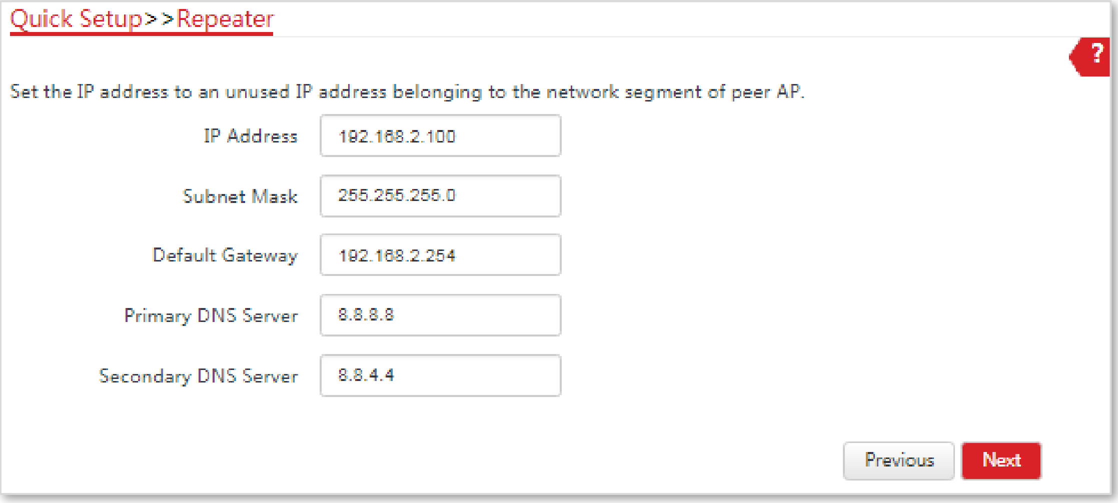
Peer AP1: IP-COM_1

MAC Address of Peer AP1: C8:3A:35:83:EF:81

Channel: 11(2462)

Security Mode: None

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



Quick Setup>>Repeater

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

IP Address: 192.168.2.100

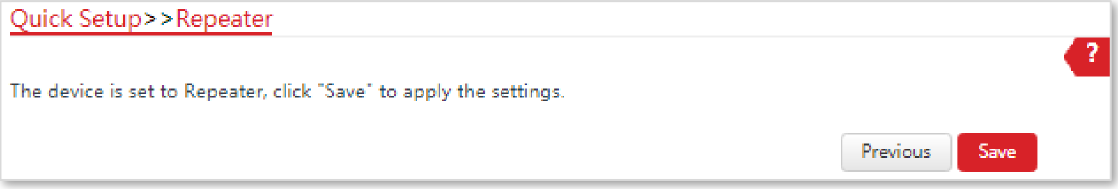
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.254

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

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



Quick Setup>>Repeater

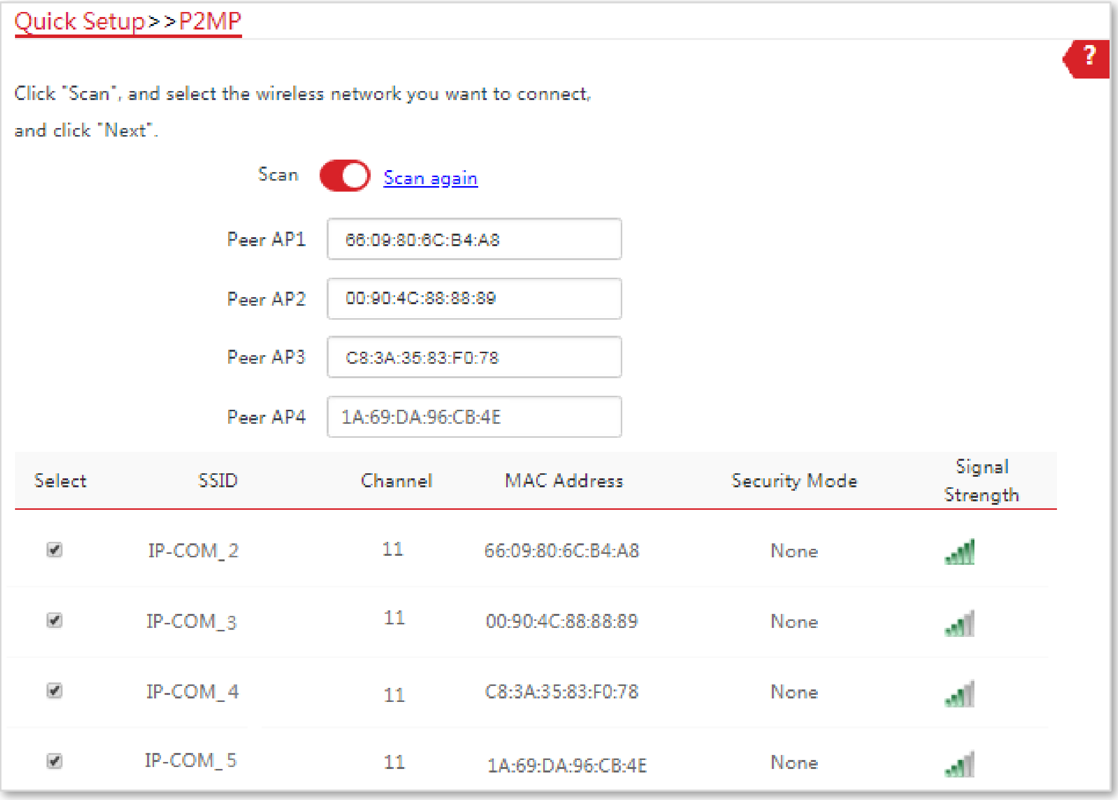
The device is set to Repeater, click "Save" to apply the settings.

2. Perform Step 1 above to set **CPE2**, **CPE3**, and **CPE4** to **Repeater** modes respectively.

3. Set the main CPE to P2MP mode to bridge CPE1, CPE2, CPE3 and CPE4.

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

(2) Select the SSIDs of CPE1, CPE2, CPE3 and CPE4 respectively, and click **Next**.



Quick Setup>>P2MP

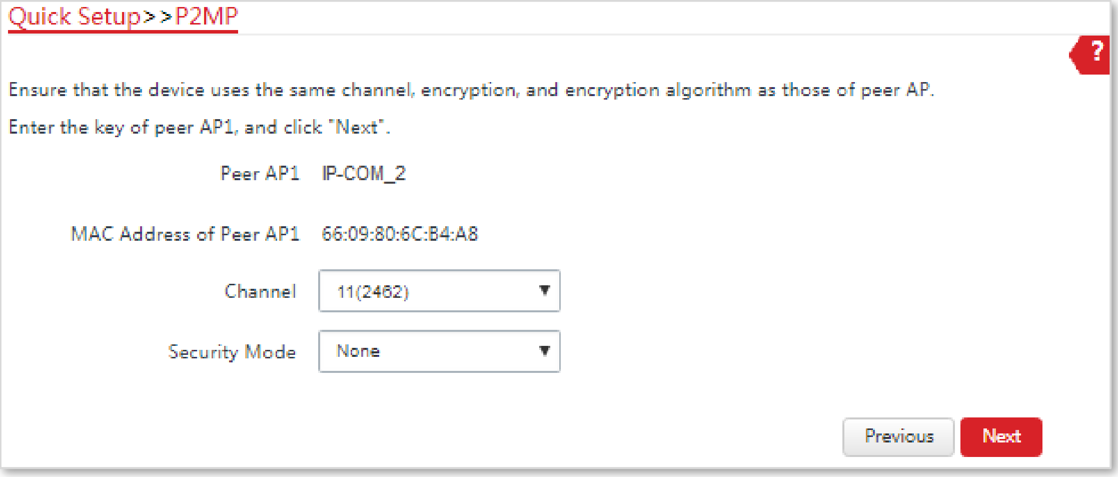
Click "Scan", and select the wireless network you want to connect, and click "Next".

Scan ● Scan again

Peer AP1	66:09:80:6C:B4:A8
Peer AP2	00:90:4C:88:88:89
Peer AP3	C8:3A:35:83:F0:78
Peer AP4	1A:69:DA:96:CB:4E

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
☑	IP-COM_2	11	66:09:80:6C:B4:A8	None	
☑	IP-COM_3	11	00:90:4C:88:88:89	None	
☑	IP-COM_4	11	C8:3A:35:83:F0:78	None	
☑	IP-COM_5	11	1A:69:DA:96:CB:4E	None	

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

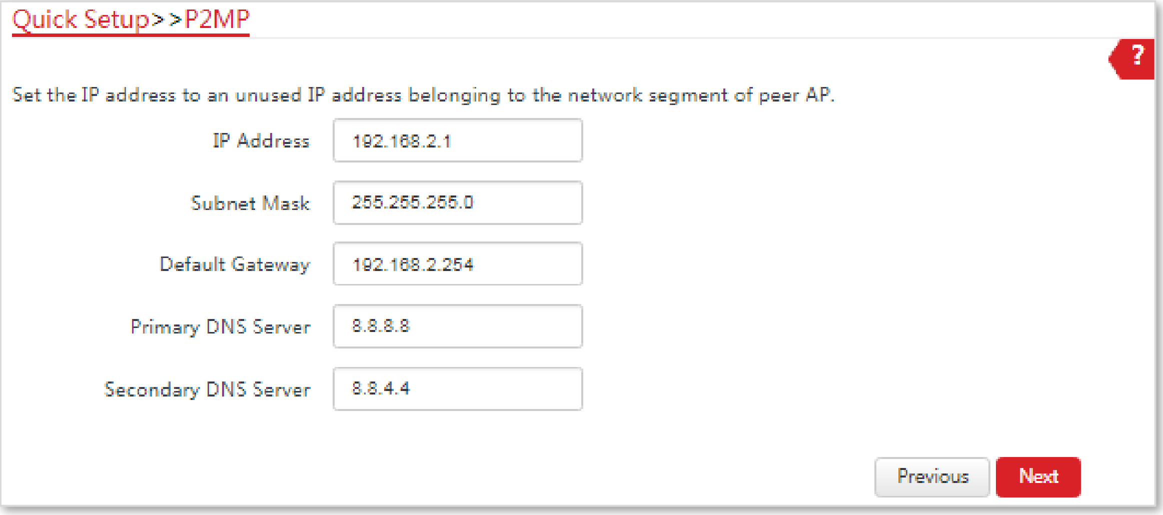


Quick Setup>>P2MP

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

Peer AP1	IP-COM_2
MAC Address of Peer AP1	66:09:80:6C:B4:A8
Channel	11(2462)
Security Mode	None

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

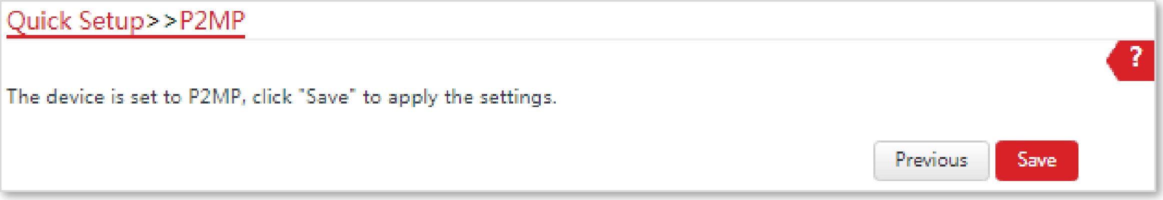


Quick Setup>>P2MP

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

IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4

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



Quick Setup>>P2MP

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

---End

Parameters Description

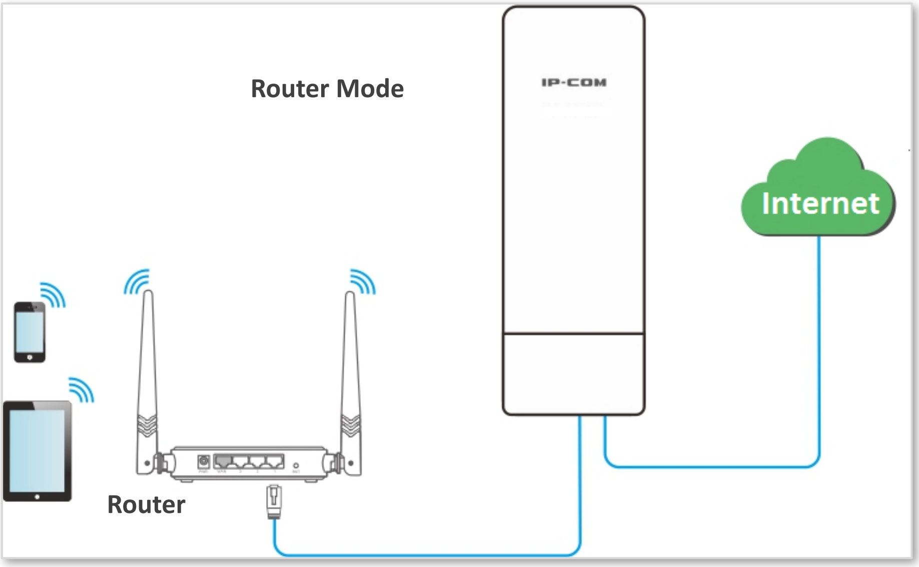
Name	Description
Working Modes	It specifies the working mode of the CPE. – **AP mode**: in this mode, the device creates a wireless network based on the current wired network. – **Client mode**: in this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point. – **Universal Repeater mode**: in this mode, this device expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function. – **WISP mode**: connect to an access point provided by ISP in wireless manner. – **Repeater** mode: the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device. – **P2MP** mode: this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city. – **Router mode**: in this mode, the PoE LAN/WAN port works as the WAN port and is used to connect to a modem for internet access.
Peer AP	It specifies the wireless network name (SSID) of the peer AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. Tip The P2MP mode only supports WEP and None security modes.

4.7 Router Mode (Only for CPE9)

4.7.1 Overview

If this device works in Router mode, the PoE LAN/WAN port works as WAN port and is used to connect to a modem for internet access.

See the following network topology:

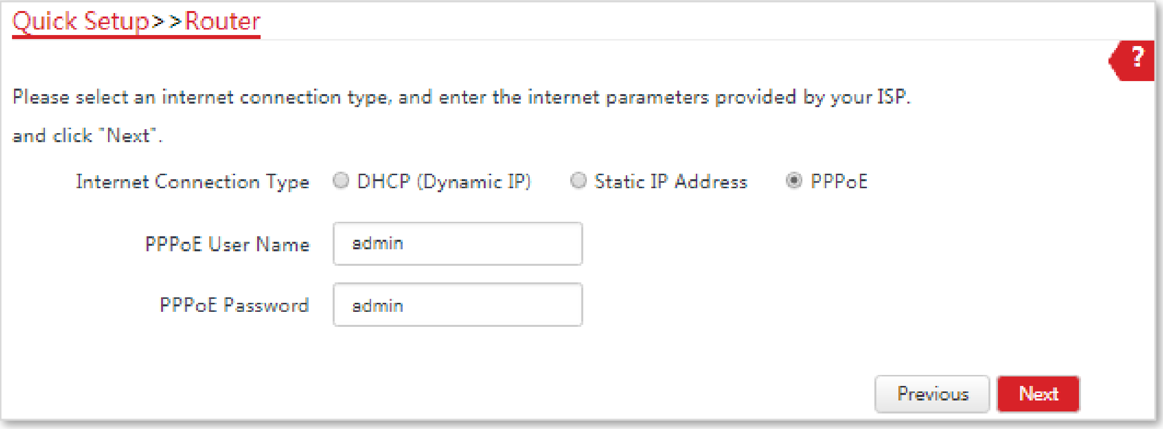


4.7.2 Setting up the Router Mode

Configuration Procedure:

1. Log in to the web UI of the CPE, and choose **Quick Setup** to enter the configuration page.
2. Select **Router** mode, and click **Next**.
3. Select your internet connection type, and set the related parameters. Take PPPoE as an example here.
   (1) Select **PPPoE**.
   (2) Enter the PPPoE user name and password provided by your internet service provider, which are both **admin** in this example.

(3) Click **Next**.



Quick Setup>>Router

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

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

PPPoE User Name: admin

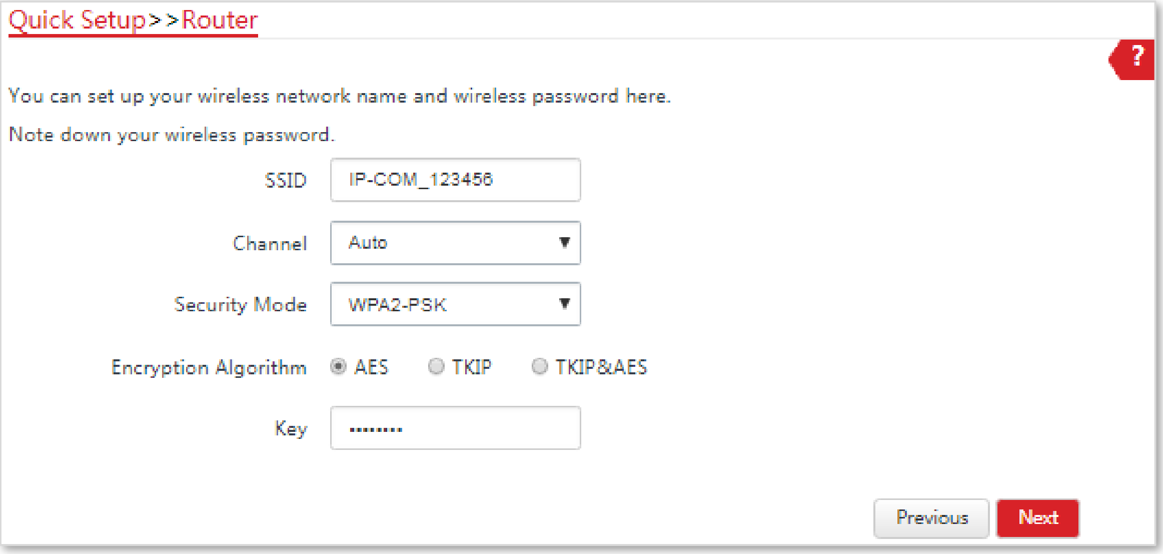
PPPoE Password: admin

4. Set wireless parameters of the CPE.

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

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

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



Quick Setup>>Router

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

SSID: IP-COM_123456

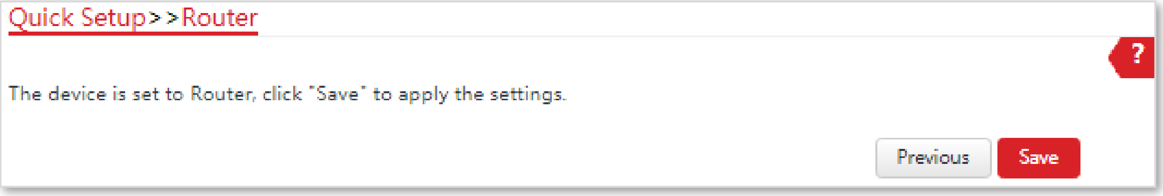
Channel: Auto

Security Mode: WPA2-PSK

Encryption Algorithm ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

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



Quick Setup>>Router

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

---End

Parameters Description

Name	Description
Working Modes	It specifies the working mode of the CPE. – **AP mode**: in this mode, the device creates a wireless network based on the current wired network. – **Client mode**: in this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point. – **Universal Repeater mode**: in this mode, this device expands your WiFi network for broader network coverage. Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function. – **WISP mode**: connect to an access point provided by ISP in wireless manner. – **Repeater** mode: the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device. – **P2MP** mode: this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city. – **Router mode**: in this mode, the PoE LAN/WAN port works as the WAN port and is used to connect to a modem for internet access.
Internet Connection Type	The CPE in Router mode supports three internet connection types: – **DHCP (Dynamic IP)**: The CPE obtains the IP address and other parameters from the DHCP server of upstream device for internet access. – **Static IP Address**: The CPE accesses the internet using the IP address, subnet mask, default gateway and DNS server IP addresses you manually entered. – **PPPoE**: The CPE accesses the internet using the PPPoE user name and password provided by the ISP.
SSID	It specifies the wireless network name of the CPE.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network of the CPE. It includes None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

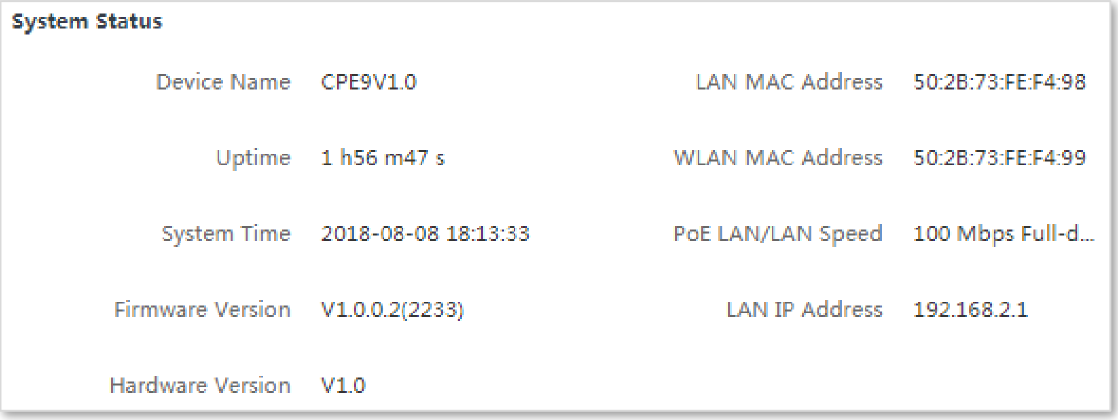
5 Status

This module allows you to view the information of system and wireless network.

5.1 System Status

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

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



System Status

Device Name CPE9V1.0

Uptime 1 h56 m47 s

System Time 2018-08-08 18:13:33

Firmware Version V1.0.0.2(2233)

Hardware Version V1.0

LAN MAC Address 50:2B:73:FE:F4:98

WLAN MAC Address 50:2B:73:FE:F4:99

PoE LAN/LAN Speed 100 Mbps Full-d...

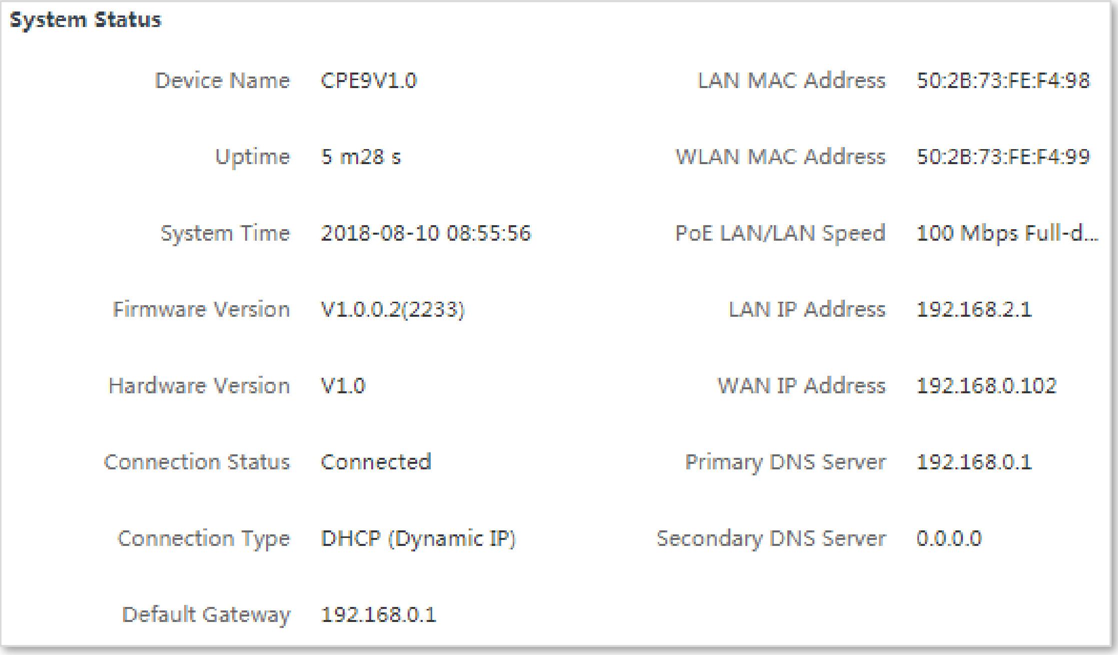
LAN IP Address 192.168.2.1

Parameters Description

Name	Description
Device Name	It specifies the name of this device. If this device is not the only one of its kind in the network, this name helps you identify the device. You can change the name of this device on the **Network** > **LAN Setup** page.
Uptime	It specifies time during which this device is operating.
System Time	It specifies the current system time of this device.
Firmware Version	It specifies the system software version number of this device.
Hardware Version	It specifies the hardware version of this device.
LAN MAC Address	It specifies the MAC address of LAN port of this device. When connecting to another device using an Ethernet cable, the CPE uses this MAC address to communicate with the device.
WLAN MAC Address	It specifies the MAC address of the wireless network of this device.

Name	Description
PoE LAN/LAN Speed	It specifies the connection status of PoE LAN/WAN and LAN ports. It includes connection rate and duplex mode.
LAN IP Address	It specifies the IP address (also named management IP address) of this device. By default, it is 192.168.2.1. You can access the web UI of this device using this IP address.

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



System Status

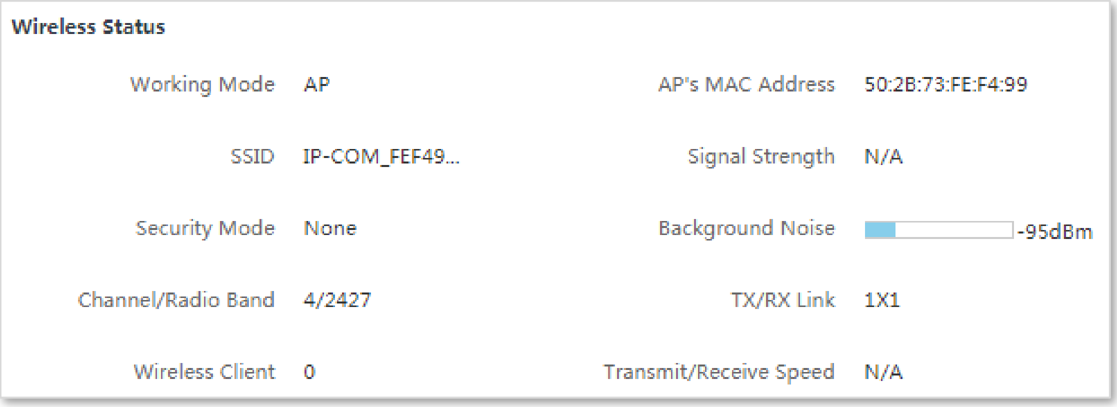
Device Name	CPE9V1.0	LAN MAC Address	50:2B:73:FE:F4:98
Uptime	5 m28 s	WLAN MAC Address	50:2B:73:FE:F4:99
System Time	2018-08-10 08:55:56	PoE LAN/LAN Speed	100 Mbps Full-d...
Firmware Version	V1.0.0.2(2233)	LAN IP Address	192.168.2.1
Hardware Version	V1.0	WAN IP Address	192.168.0.102
Connection Status	Connected	Primary DNS Server	192.168.0.1
Connection Type	DHCP (Dynamic IP)	Secondary DNS Server	0.0.0.0
Default Gateway	192.168.0.1		

Parameters Description

Name	Description
Connection Status	It specifies the connection status of WAN port of this device in WISP or Router mode.
Connection Type	It specifies the internet connection type of this device in WISP or Router mode.
WAN IP Address	It specifies the IP address of WAN port of this device in WISP or Router mode.
Default Gateway	It specifies the default gateway address of this device in WISP or Router mode.
Primary DNS Server	It specifies the IP address of primary DNS server of this device in WISP or Router mode.
Secondary DNS Server	It specifies the IP address of secondary DNS server of this device in WISP or Router mode.

5.2 Wireless Status

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



Wireless Status

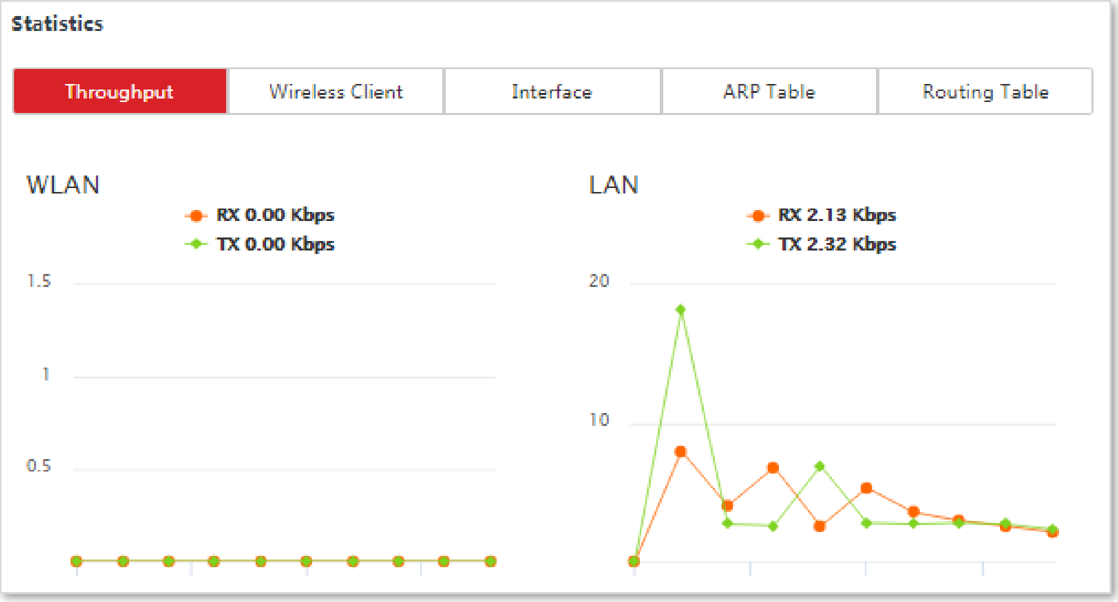
Working Mode	AP	AP's MAC Address	50:2B:73:FE:F4:99
SSID	IP-COM_FEF49...	Signal Strength	N/A
Security Mode	None	Background Noise	-95dBm
Channel/Radio Band	4/2427	TX/RX Link	1X1
Wireless Client	0	Transmit/Receive Speed	N/A

Parameters Description

Name	Description
Working Mode	It specifies the working mode the device operates.
SSID	It specifies the wireless network name of this device.
Security Mode	It specifies the security mode of the wireless network of this device.
Channel/Radio Band	It specifies the channel and radio band used by this device to transmit radio signals.
Wireless Client	It specifies the number of wireless clients connected to this device.
AP's MAC Address	It displays "No Peer AP" if the device works in AP or Router mode. And in other modes, it displays the MAC address of peer AP to which this device bridged.
Signal Strength	It displays the signal strength of the first device connected to the wireless network of the device when it works in AP or Router mode. It displays the received signal strength from peer AP when the device works in Client, Universal Repeater, WISP, Repeater or P2MP mode.
Background Noise	It specifies the strength of radio interference signals in the ambient environment that interfere with the channel of this device. Larger absolute value indicates less interference.
TX/TR Link	It specifies the number of spatial streams the device is transmitting or receiving.
Transmit/Receive Speed	It specifies the wireless transmitting/receiving rate. – In AP or Router mode: it displays the transmitting/receiving rate of the first device connected to the wireless network of this device. – In Client, Universal Repeater, WISP, Repeater, or P2MP mode: it displays transmitting/receiving rate of this device.

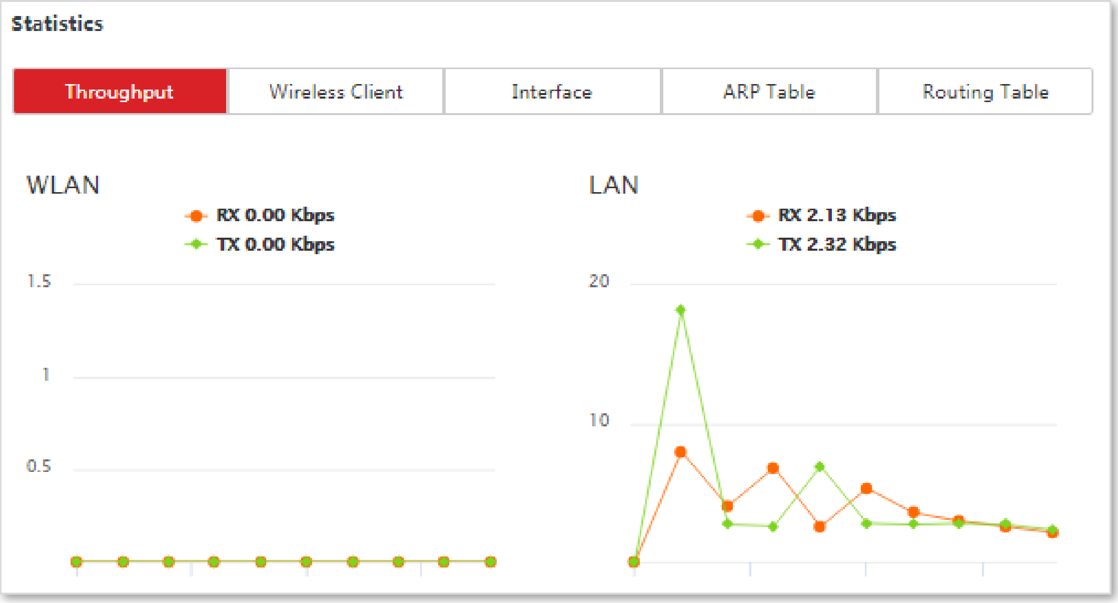
5.3 Statistics

Log in to the web UI of the CPE, and choose **Status**. You can view statistics information here, including throughput, wireless client, interface and so on.



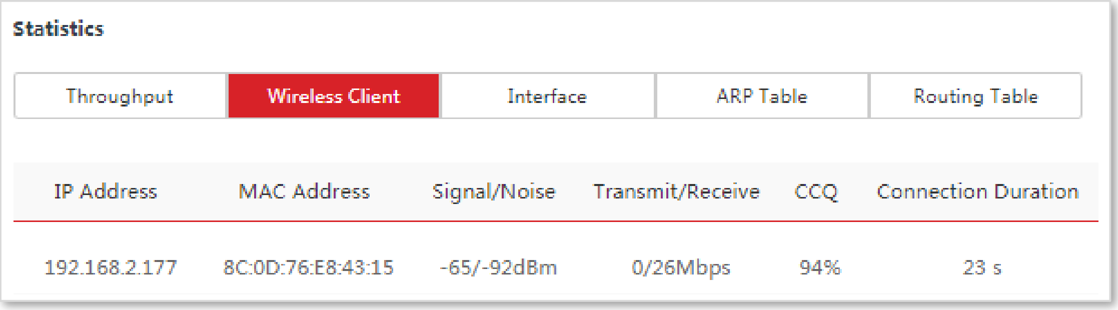
5.3.1 Throughput

It displays the throughput of WLAN and LAN ports here.



5.3.2 Wireless Client

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



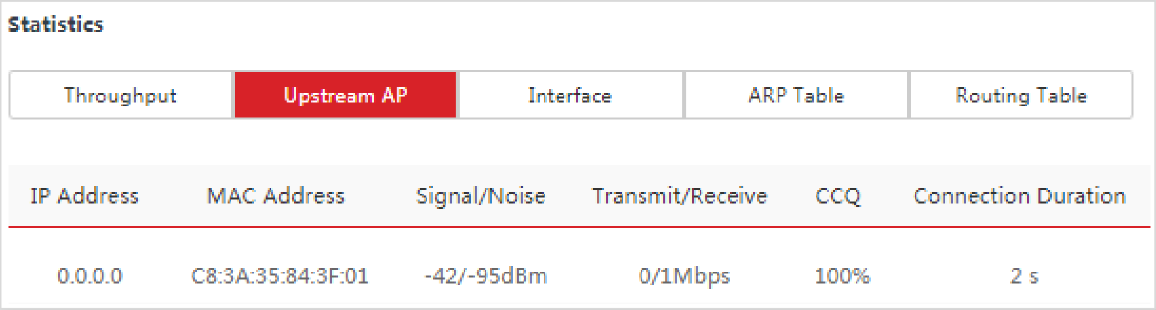
IP Address	MAC Address	Signal/Noise	Transmit/Receive	CCQ	Connection Duration
192.168.2.177	8C:0D:76:E8:43:15	-65/-92dBm	0/26Mbps	94%	23 s

Parameters Description

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

5.3.3 Upstream AP

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



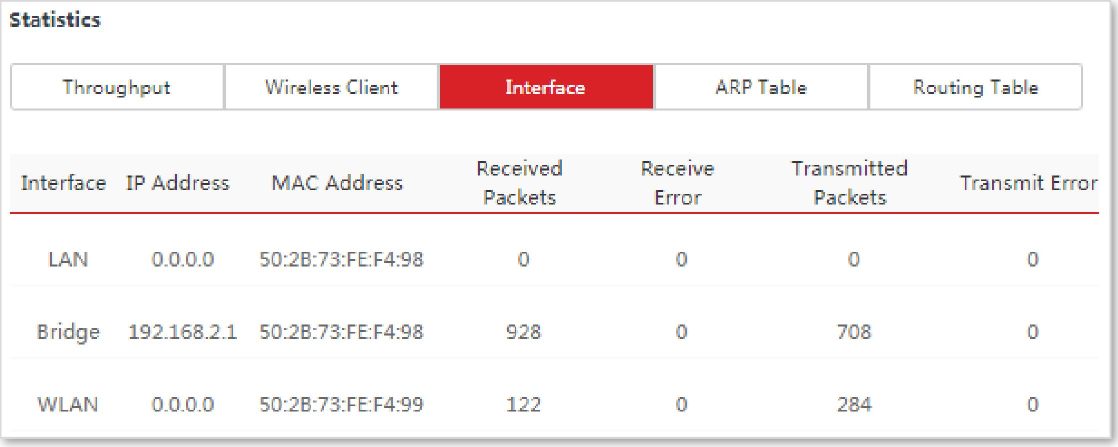
IP Address	MAC Address	Signal/Noise	Transmit/Receive	CCQ	Connection Duration
0.0.0.0	C8:3A:35:84:3F:01	-42/-95dBm	0/1Mbps	100%	2 s

Parameters Description

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

5.3.4 Interface

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



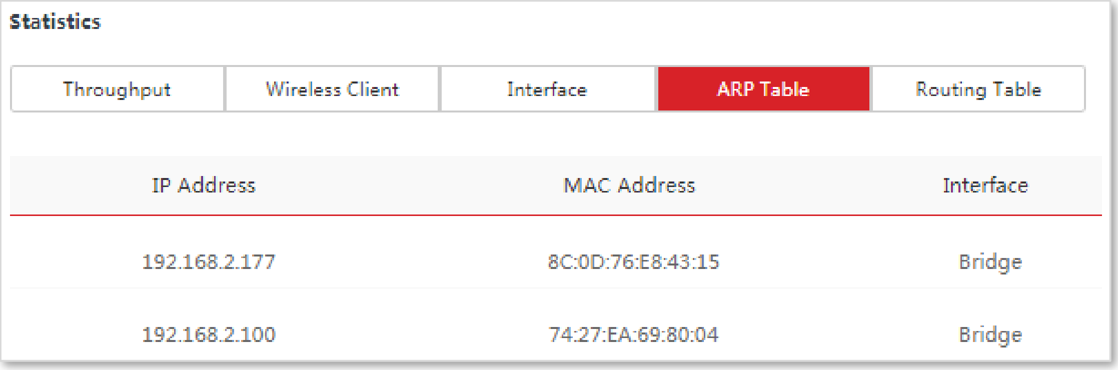
Interface	IP Address	MAC Address	Received Packets	Receive Error	Transmitted Packets	Transmit Error
LAN	0.0.0.0	50:2B:73:FE:F4:98	0	0	0	0
Bridge	192.168.2.1	50:2B:73:FE:F4:98	928	0	708	0
WLAN	0.0.0.0	50:2B:73:FE:F4:99	122	0	284	0

Parameters Description

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

5.3.5 ARP Table

It specifies the current ARP table of the CPE.



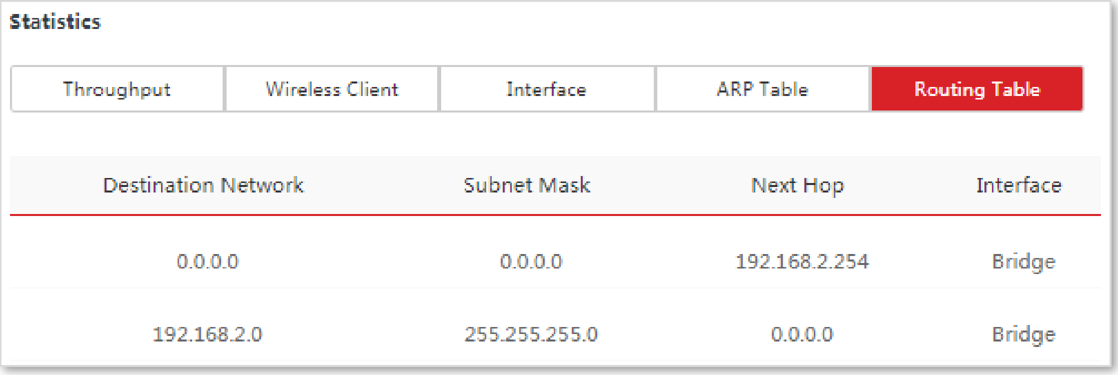
IP Address	MAC Address	Interface
192.168.2.177	8C:0D:76:E8:43:15	Bridge
192.168.2.100	74:27:EA:69:80:04	Bridge

Parameters Description

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

5.3.6 Routing Table

It specifies the destination networks that the CPE can access.



Destination Network	Subnet Mask	Next Hop	Interface
0.0.0.0	0.0.0.0	192.168.2.254	Bridge
192.168.2.0	255.255.255.0	0.0.0.0	Bridge

Parameters Description

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

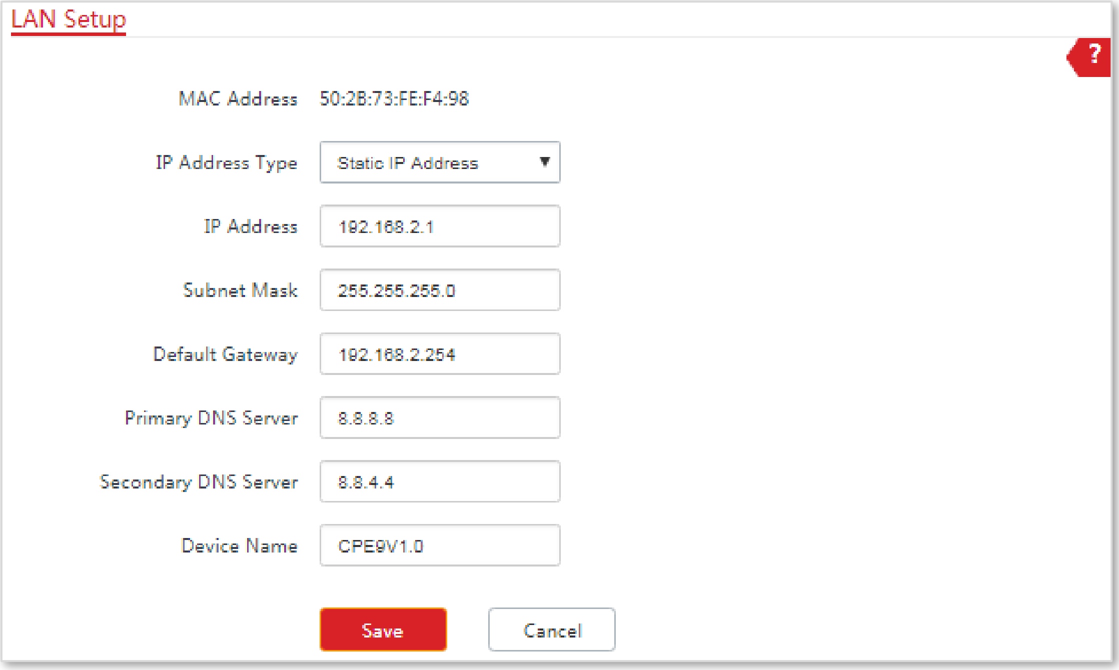
6 Network

6.1 LAN Setup

6.1.1 Overview

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

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



LAN Setup

MAC Address	50:2B:73:FE:F4:98
IP Address Type	Static IP Address
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Device Name	CPE9V1.0

Parameters Description

Name	Description
MAC Address	It specifies the MAC address of LAN port. The default SSID of the CPE is **IP-COM_XXXXXX**, and XXXXXX is the last six characters of this MAC address.
IP Address Type	It specifies the type of obtaining an IP address. The default is **Static IP Address**. Static IP Address: Specify the IP address, subnet mask, default gateway, and DNS server IP

Name	Description
	addresses manually.
IP Address	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. Tip 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.
Subnet Mask	It specifies the subnet mask of the CPE's IP address. The default is **255.255.255.0**.
Default Gateway	It specifies the default gateway of the CPE. You can set it to the IP address of the egress router to enable the CPE to access the internet.
Primary DNS Server	It specifies the primary DNS server IP address of the CPE. If the egress router has the DNS agency function, it can be set to the LAN IP address the egress router. Otherwise, specify a DNS server IP address manually.
Secondary DNS Server	It specifies the secondary DNS server IP address of the CPE. If there are two DNS server IP addresses, enter one in this box.
Device Name	It specifies the name of the CPE. The default name indicates the CPE's model and version. You are recommended to change the name of the CPE to indicate the location of the CPE, so that you can easily identify the CPE when there are multiple CPEs in the network.

6.1.2 Changing the LAN IP Address

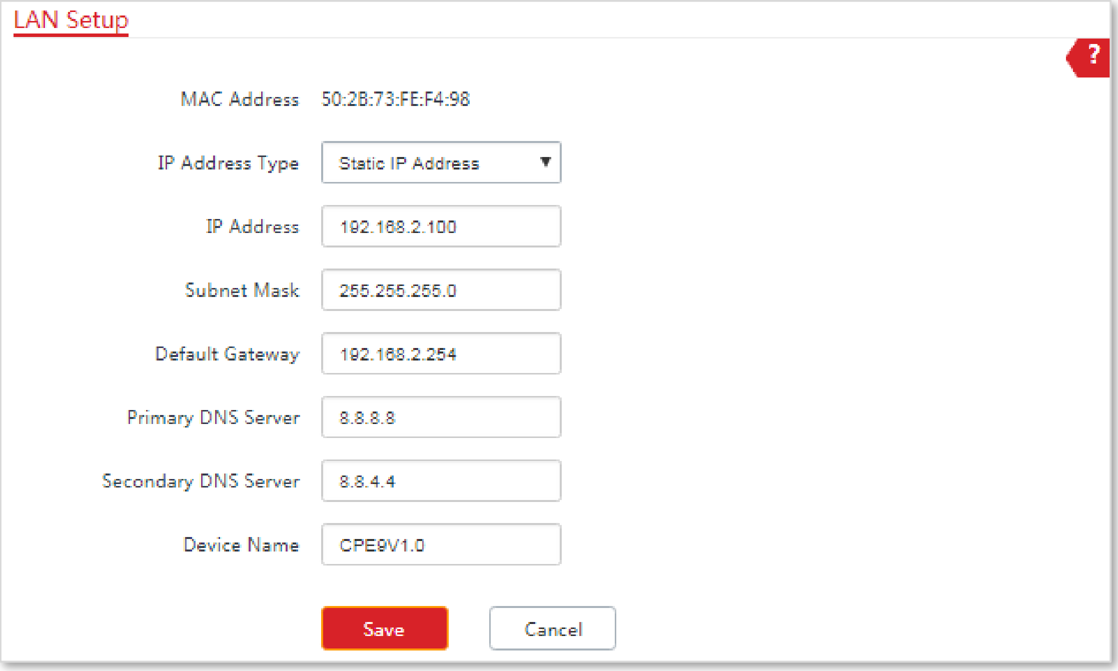
Manually Setting the IP Address

In this mode, you must manually set the IP address, subnet mask, gateway IP address, and DNS server IP addresses of the CPE. Therefore, this mode is recommended if you need to deploy only a few CPEs.

Configuration Procedure:

1. Choose **Network** > **LAN Setup** to enter the configuration page.
2. Set **IP Address Type** to **Static IP Address**.
3. Set **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**. If another DNS server is available, set **Secondary DNS Server** to the IP address of the additional DNS server.

4. Click **Save**.



LAN Setup

MAC Address 50:2B:73:FE:F4:98

IP Address Type: Static IP Address

IP Address: 192.168.2.100

Subnet Mask: 255.255.255.0

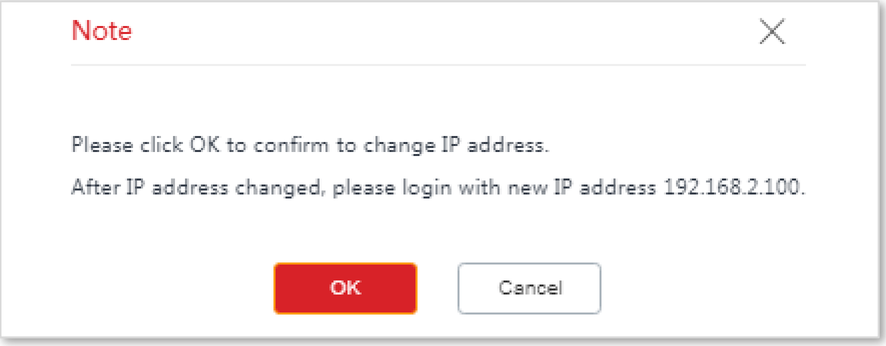
Default Gateway: 192.168.2.254

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

Device Name: CPE9V1.0

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



Note

Please click OK to confirm to change IP address.

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

---End

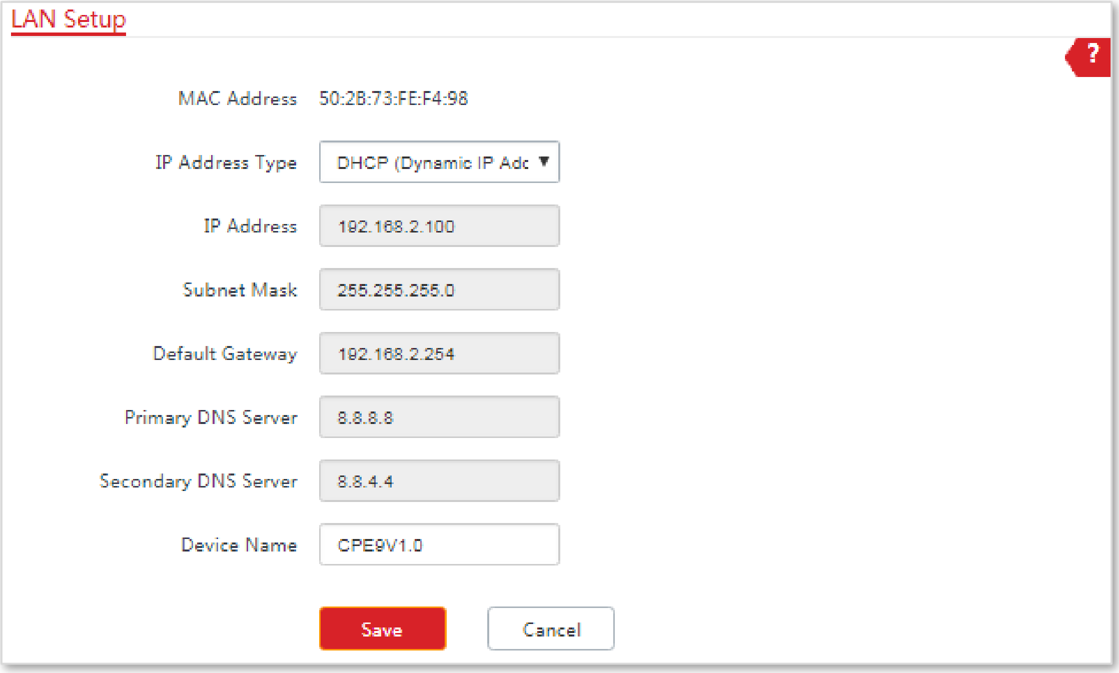
After the configuration, if the new and original IP addresses belong to the same network segment, you can log in to the web UI of the CPE by accessing the new IP address. Otherwise, assign your computer an IP address that belongs to the same network segment as the new IP address of the CPE before login.

Automatically Obtaining an IP Address

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

Configuration Procedure:

1. Choose **Network** > **LAN Setup** to enter the configuration page.
2. Set IP Address Type to DHCP (Dynamic IP Address).
3. Click **Save**.



LAN Setup

MAC Address	50:2B:73:FE:F4:98
IP Address Type	DHCP (Dynamic IP Adc ▼
IP Address	192.168.2.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Device Name	CPE9V1.0

---End

After the configuration, if you want to re-log in to the web UI of the CPE, check the client list of the DHCP server for the IP address assigned to the CPE, ensure that the IP address of the management computer and the IP address of the CPE belong to the same network segment, and access the IP address of the CPE.

6.2 MAC Clone

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

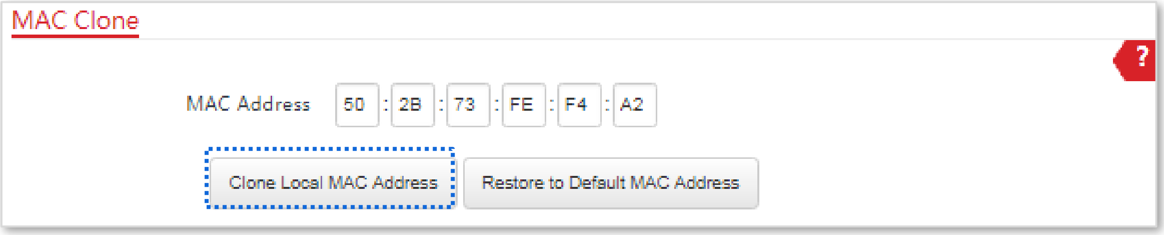
6.2.1 Overview

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

In this case, you can try either of the following methods to address the issue.

Method 1

1. Connect the computer to the device.
2. Log in to the device's web UI.
3. Choose **Network** > **MAC Clone** to enter the configuration page.
4. Click **Clone Local MAC Address**.
5. Click **Save**.



MAC Clone

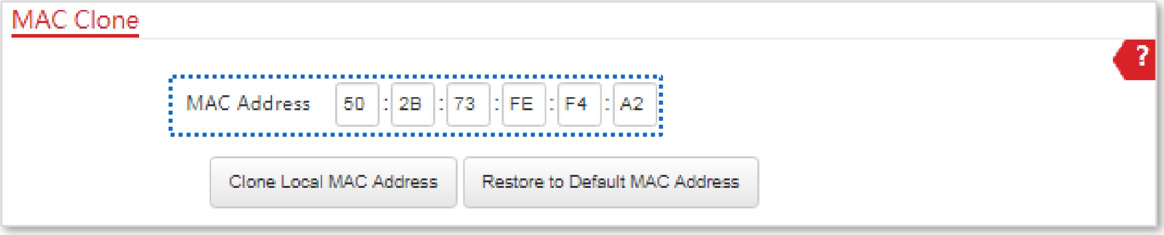
MAC Address 50 : 2B : 73 : FE : F4 : A2

---End

Method 2

Connect another device (such as a smart phone or tablet) to the device

1. Log in to the device's web UI.
2. Choose **Network** > **MAC Clone**.
3. Enter the MAC address of the computer that can access the internet in the **MAC Address** boxes.
4. Click **Save**.



MAC Address 50 : 2B : 73 : FE : F4 : A2

---End

Tip

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

6.3 DHCP Server

6.3.1 Overview

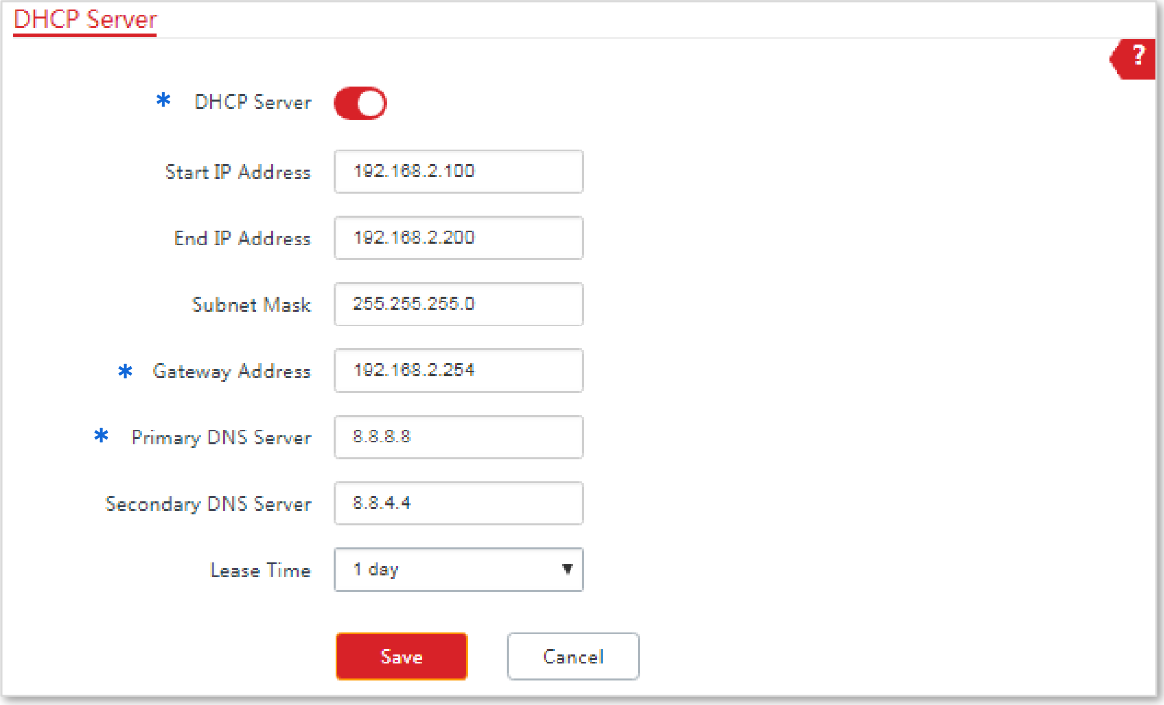
The CPE provides a DHCP server function to assign IP addresses to clients on the LAN. By default, the DHCP server function is disabled.

Tip

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

6.3.2 Configuring the DHCP Server

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


DHCP Server

* DHCP Server	● (enabled)
Start IP Address	192.168.2.100
End IP Address	192.168.2.200
Subnet Mask	255.255.255.0
* Gateway Address	192.168.2.254
* Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Lease Time	1 day ▼

---End

Tip

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

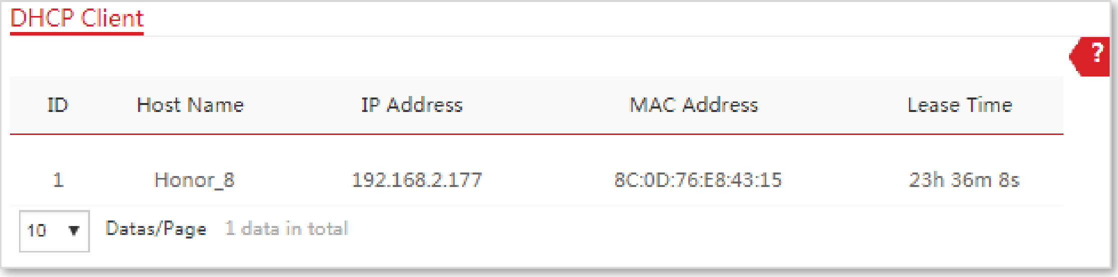
Parameters Description

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

6.4 DHCP Client

If the CPE functions as a DHCP server, you can view the DHCP client list to understand the details about the clients that obtain IP addresses from the DHCP server. The details include host names, IP addresses, MAC addresses, and lease times.

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



DHCP Client

ID	Host Name	IP Address	MAC Address	Lease Time
1	Honor_8	192.168.2.177	8C:0D:76:E8:43:15	23h 36m 8s

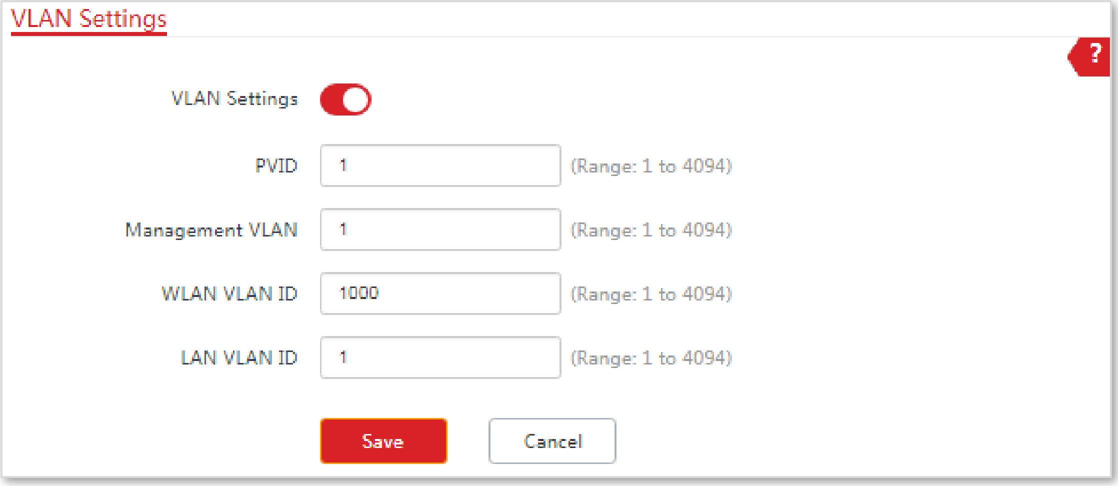
6.5 VLAN Settings

6.5.1 Overview

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

6.5.2 Setting up VLAN

1. Choose **Network** > **VLAN Settings** to enter the configuration page.
2. Enable the function.
3. Set the parameters as needed.
4. Click **Save**.



VLAN Settings

VLAN Settings	●	
PVID	1	(Range: 1 to 4094)
Management VLAN	1	(Range: 1 to 4094)
WLAN VLAN ID	1000	(Range: 1 to 4094)
LAN VLAN ID	1	(Range: 1 to 4094)

---End

Parameters Description

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

Name	Description
LAN VLAN ID	It allows you to set a VLAN ID for the LAN port (wired network) of this device. By default, it is set to **1**. After the VLAN function is enabled, the WLAN interface functions as an access port, whose PVID is the same as VLAN ID.

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

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

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

6.5.3 Examples of Configuring VLAN Settings

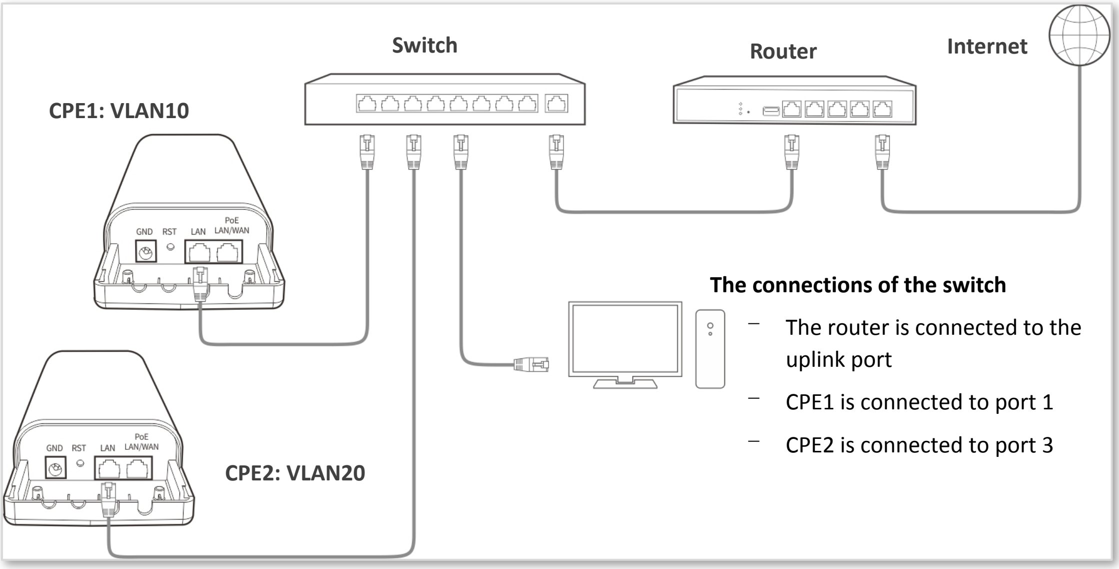
Networking Requirement

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

Assumption:

CPE1 belongs to VLAN10, and CPE2 belongs to VLAN20.

Network Topology



The connections of the switch

- The router is connected to the uplink port
- CPE1 is connected to port 1
- CPE2 is connected to port 3

Configuration Procedure

1. Set up CPE1.

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

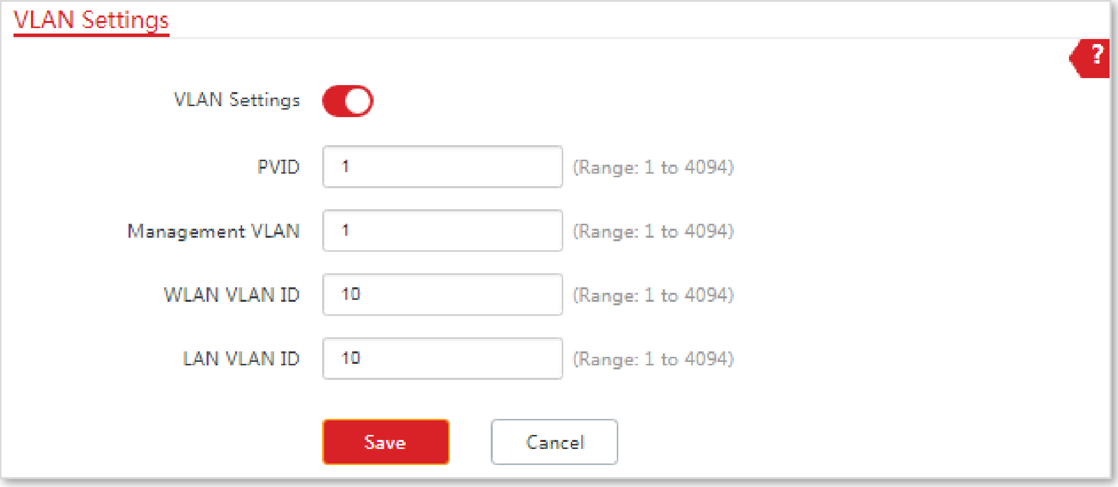
   (2) Enable the function.

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

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

   (5) Set **LAN VLAN ID** to **10**.

   (6) Click **Save**.



VLAN Settings

VLAN Settings: On

PVID: 1 (Range: 1 to 4094)

Management VLAN: 1 (Range: 1 to 4094)

WLAN VLAN ID: 10 (Range: 1 to 4094)

LAN VLAN ID: 10 (Range: 1 to 4094)

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

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

3. Set up the switch.

The following form shows the configuration on the switch:

Ports of the Switch	VLAN ID (Allow the packets belonging to the following VLANs to access)	Type of Port	PVID
Uplink port (Connected to a router)	1,10,20	Trunk	1
Port 1 (Connected to CPE1)	1,10	Trunk	1
Port 3 (Connected to CPE2)	1,20	Trunk	1

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

The following form shows the configuration on the router:

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

Refer to the user guide of the router for details.

---End

Verification

If the router enables two DHCP servers which belong to VLAN10 and VLAN20 respectively, the first device connected to the CPE obtains an IP address and related parameters from the DHCP server belonging to VLAN10, and the second device obtains these parameters from the DHCO sever belonging to VLAN20.

7 Wireless

7.1 Basic

7.1.1 Overview

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

Broadcast SSID

When the CPE broadcasts an SSID, nearby wireless clients can detect the SSID. When this parameter is set to **Disable**, 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 corresponding to the SSID. This to some extent enhances the security of the wireless network.

It is worth noting that after **Broadcast SSID** is set to **Disable**, a hacker can still connect to the corresponding wireless network if he/she manages to obtain the SSID by other means.

Isolate Client

This parameter implements a function similar to the VLAN function for wired networks. It isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can access only the wired network connected to the CPE. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.

Max. Number of Clients

This parameter specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID. If the number is reached, the wireless network rejects new connection requests from clients. This limit helps balance load among CPEs.

Security Mode

A wireless network uses radio, which is open to the public, as its data transmission medium. If the wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network. To ensure communication security, transmission links of wireless networks must be encrypted for protection.

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

None

It indicates that any wireless client can connect to the wireless network. This option is not recommended because it affects network security.

WEP

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

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

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

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK adopt a pre-shared key for authentication, while the AP generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.

WPA and WPA2

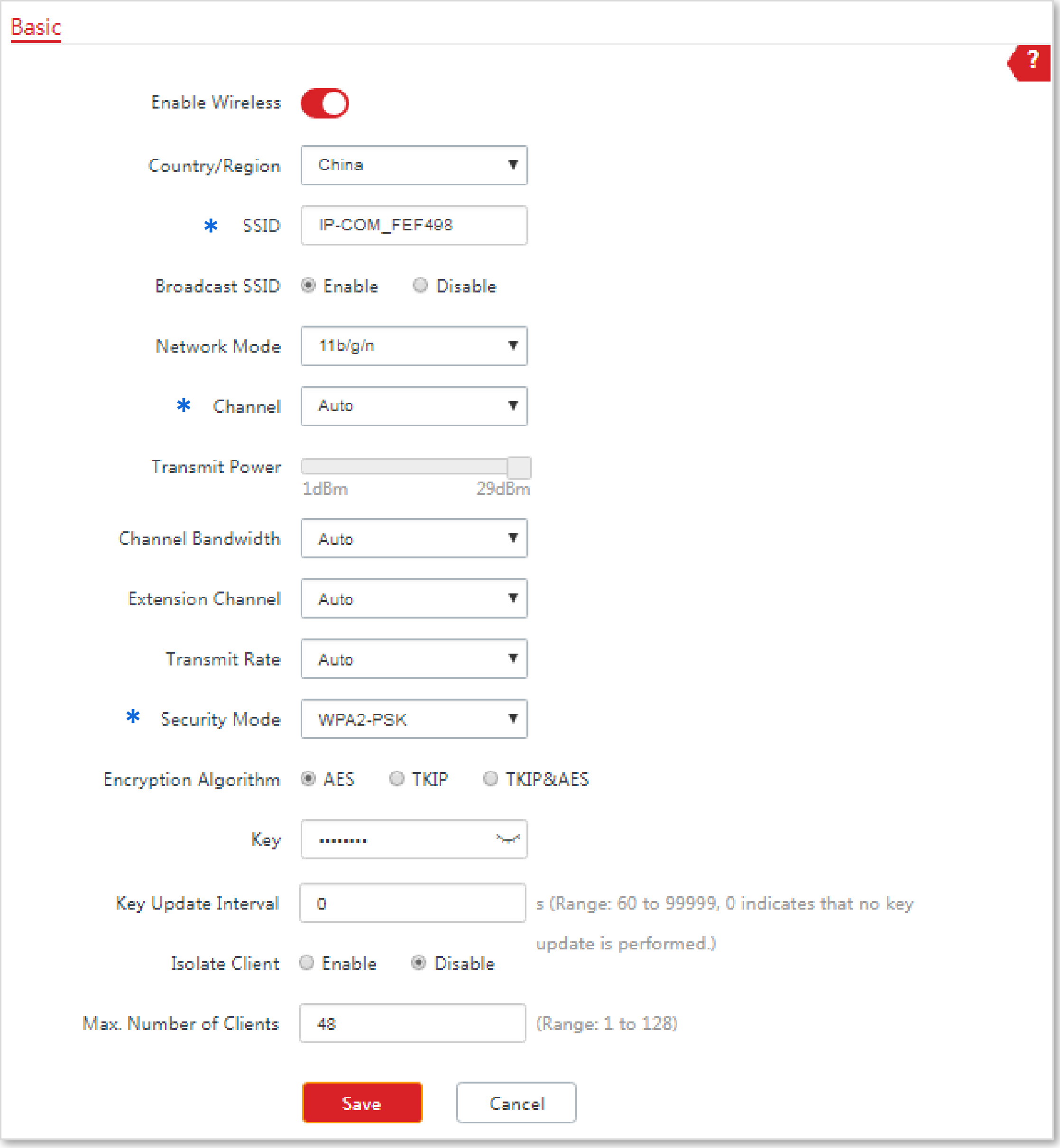
To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate clients and generate data encryption–oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys that set manually, but adopt the same encryption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

WPA and WPA2 uses 802.1x to authenticate clients and the login information of a client is managed by the client. This effectively reduces the probability of information leakage. In addition, each time a client connects to an AP that adopts the WPA or WPA2 security mode, the RADIUS server generates a data encryption key and assigns it to the client. This makes it difficult for attackers to obtain the key. These features of WPA and WPA2 help significantly increase network security, making WPA and WPA2 the preferred security modes of wireless networks that require high security.

7.1.2 Changing the Basic Settings

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

1. Choose Wireless > Basic.
2. Change the parameters as required. Generally, you only need to enable the wireless function, and change **SSID**, **Channel** and **Security Mode** settings.
3. Click **Save**.



Basic

Enable Wireless: On

Country/Region: China

* SSID: IP-COM_FEF498

Broadcast SSID: ● Enable ○ Disable

Network Mode: 11b/g/n

* Channel: Auto

Transmit Power: 1dBm – 29dBm

Channel Bandwidth: Auto

Extension Channel: Auto

Transmit Rate: Auto

* Security Mode: WPA2-PSK

Encryption Algorithm: ● AES ○ TKIP ○ TKIP&AES

Key: ••••••••

Key Update Interval: 0 s (Range: 60 to 99999, 0 indicates that no key update is performed.)

Isolate Client: ○ Enable ● Disable

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

---End

Parameters Description

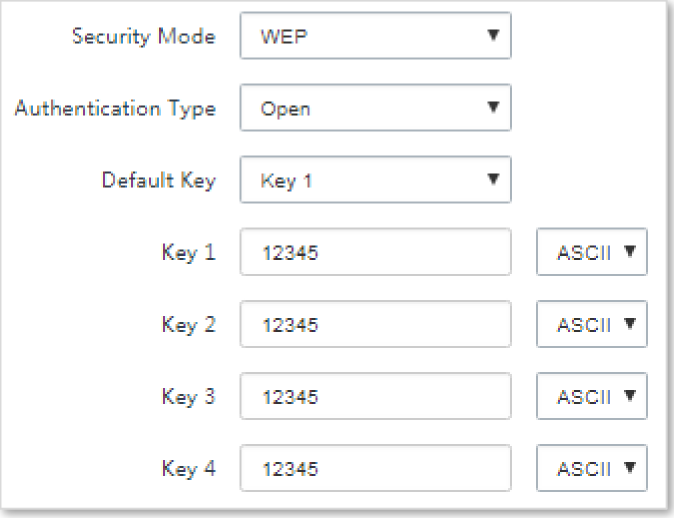
Name	Description
Enable Wireless	It specifies whether to enable the wireless function. By default, it is enabled.
Country/Region	It specifies country or region where this device is located. You can select the country or region to ensure that this device complies with the channel regulations of the country or region.
SSID	It specifies the wireless network name.
Broadcast SSID	It specifies whether to broadcast the SSID. – **Enable** indicates that the SSID is broadcast and nearby wireless devices can find the SSID. – **Disable** indicates that the SSID is not broadcast and nearby wireless devices cannot find the SSID.
Network Mode	It specifies the network mode of this device. The available options include 11b/g, 11b, 11g, and 11 b/g/n. – **11b/g**: It indicates that clients compliant with the 802.11b or 802.11g protocol can connect to the CPE. – **11g**: It indicates that clients working at 2.4 GHz and compliant with 802.11g can connect to the CPE. – **11n**: It indicates that clients working at 2.4 GHz and compliant with 802.11n can connect to the CPE. – **11b/g/n**: It indicates that all clients working at 2.4 GHz and compliant with the 802.11b, 802.11g, or 802.11n protocol can connect to the CPE.
Channel	It specifies channel in which this device operates. **Auto** indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.
Transmit Power	It specifies the transmit power of this device. Higher number indicates wider WiFi coverage. Setting a proper transmit power helps improve the performance and security of the wireless network.
Channel Bandwidth	It specifies the bandwidth of the operating channel of a wireless network. Change the default setting only when necessary. – **20**: It indicates that the channel bandwidth of a CPE is 20 MHz. – **40**: It indicates that the channel bandwidth of a CPE is 40 MHz. – **Auto**: It specifies that a CPE can switch its channel bandwidth between 20 MHz and 40 MHz based on the ambient environment.
Extension Channel	It is used to determine the operating frequency band of this device when it uses the 40 MHz channel bandwidth in 11n mode.
Transmit Rate	It specifies wireless transmission rate of the device. If the channel bandwidth is set to 40 MHz, the maximum transmission rate is MCS7 (135 Mbps). If the channel bandwidth is set to 20 MHz, this device uses lower transmission rate. And the maximum transmission rate is MCS7 (65 Mbps).
Security Mode	It specifies security mode of the wireless network of this device. The available modes include None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA and WPA2.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK, this parameter has the AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter has the AES, TKIP, and TKIP&AES values. – **AES**: It indicates the Advanced Encryption Standard. – **TKIP**: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps.

Name	Description
	– **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key. It consists of 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies interval at which a WPA key is updated. A shorter interval leads to higher security. The value 0 indicates that no key update is performed.
Isolate Client	– **Enable**: It indicates that the wireless clients connected to the CPE with the selected SSID cannot communicate with each other. This improves wireless network security. – **Disable**: It indicates that the wireless clients connected to the CPE with the selected SSID can communicate with each other. By default, it is disabled.
Max. Number of Clients	It specifies the maximum number of wireless clients that can be connected to the wireless network with the SSID. After this upper limit is reached, the CPE rejects new requests from clients for connecting to the wireless network.

None

It indicates that any wireless client can connect to the wireless network. This option is not recommended because it affects network security.

WEP



Security Mode: WEP ▼

Authentication Type: Open ▼

Default Key: Key 1 ▼

Key 1: 12345 ASCII ▼

Key 2: 12345 ASCII ▼

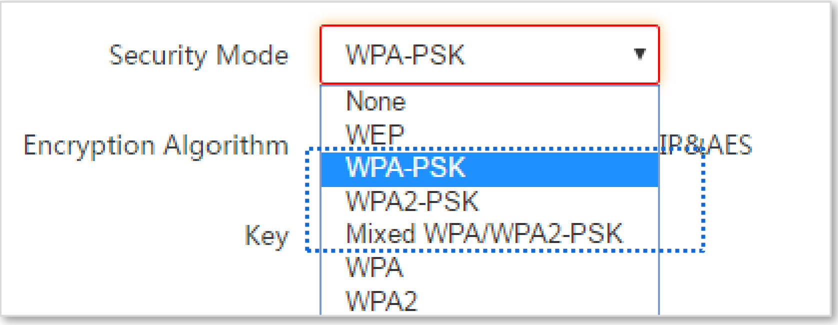
Key 3: 12345 ASCII ▼

Key 4: 12345 ASCII ▼

Parameters Description

Name	Description
Authentication Type	It specifies the authentication type for the WEP security mode. The options include Open and Shared. The options share the same encryption process. – **Open**: It specifies that authentication is not required and data exchanged is encrypted using WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. – **Shared**: It specifies that a shared key is used for authentication and data exchanged is encrypted using WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key.
Default Key	It specifies the WEP key for the Open or Shared encryption type. For example, if Default Key is set to Security Key 2, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Security Key 2.
Key 1/2/3/4	Enter WEP key. You can enter four keys, but only the key specified in the Default Key takes effect.
ASCII	It indicates that a key selected for the Open or Shared authentication type contains hexadecimal characters. 5 or 13 ASCII characters are allowed in the key.
Hex	It indicates that a key selected for the Open or Shared authentication type contains hexadecimal characters. 10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.

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



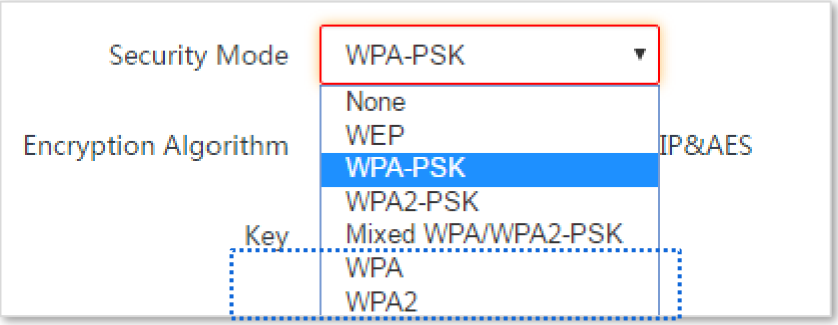
Security Mode: WPA-PSK

Parameters Description

Name	Description
Security Mode	It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. – **WPA-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA-PSK. – **WPA2-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2-PSK. – **Mixed WPA/WPA2-PSK**: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK.

Name	Description
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK, this parameter has the AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter has the AES, TKIP, and TKIP&AES values. – **AES**: It indicates the Advanced Encryption Standard. – **TKIP**: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. – **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value 0 indicates that a WAP key is not updated.

WPA and WPA2



Security Mode: WPA-PSK

Encryption Algorithm: IP&AES

Key

Parameters Description

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

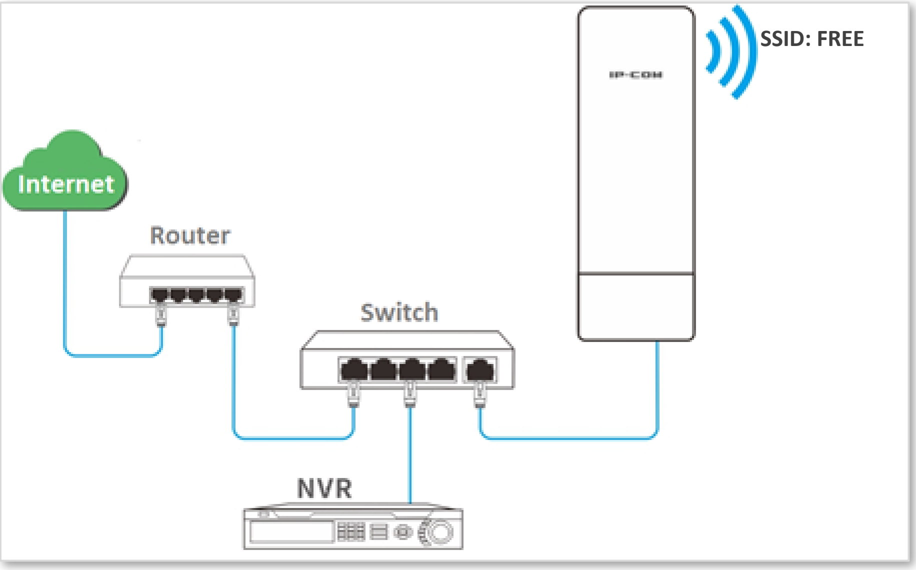
Name	Description
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value 0 indicates that a WAP key is not updated.

7.1.3 Examples of Configuring Basic Settings

Setting up a Non-encrypted Wireless Network

Networking Requirement

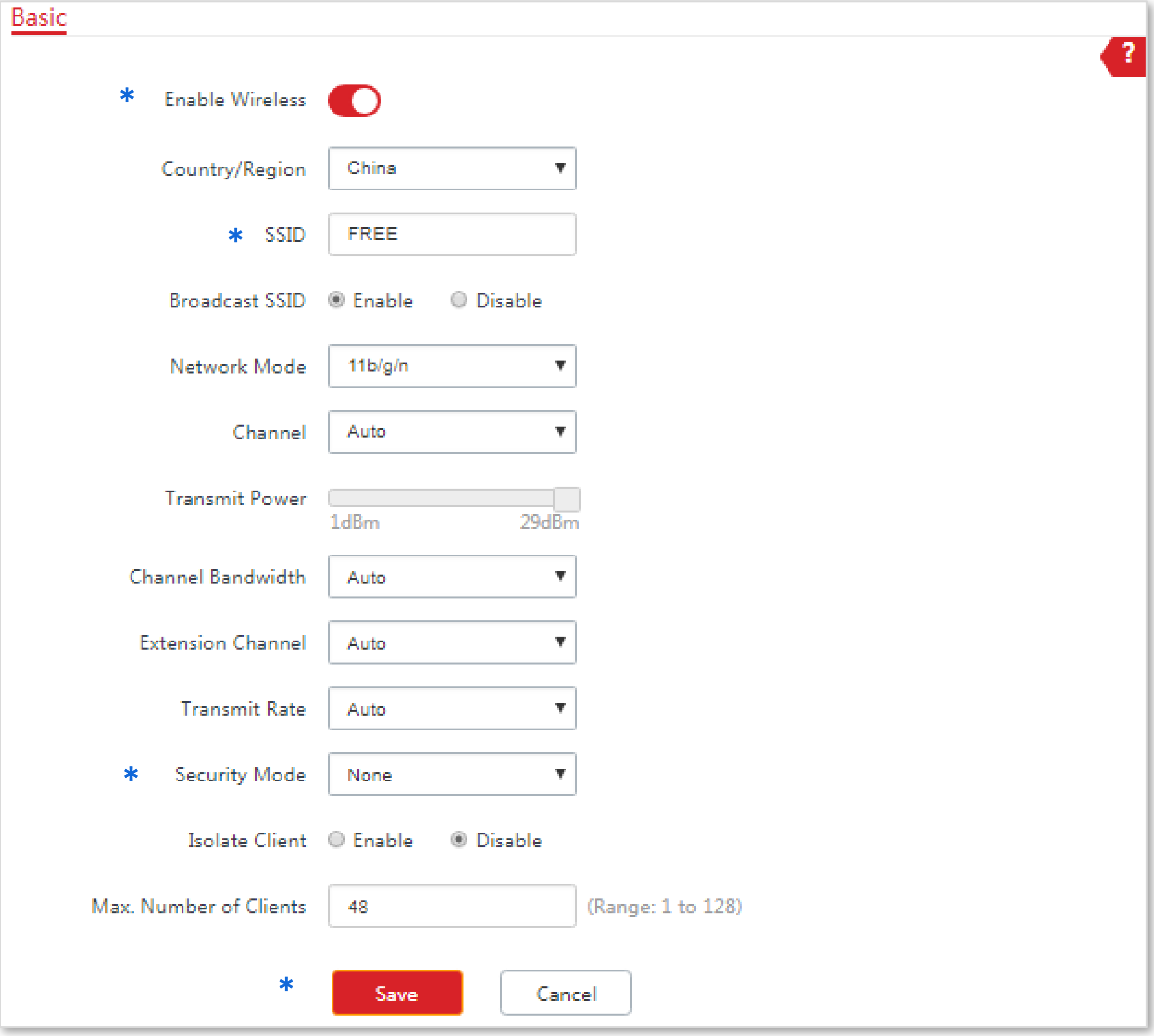
A residential community uses the CPEs to deploy its network for video surveillance. It requires that the SSID is FREE and there is no WiFi password.



Configuration Procedure

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

1. Choose Wireless > Basic.
2. Enable the wireless function.
3. Change the value of the **SSID** text box to **FREE**.
4. Set **Security Mode** to **None**.
5. Click **Save**.



Basic

* Enable Wireless	● (on)
Country/Region	China ▼
* SSID	FREE
Broadcast SSID	● Enable ○ Disable
Network Mode	11b/g/n ▼
Channel	Auto ▼
Transmit Power	1dBm – 29dBm
Channel Bandwidth	Auto ▼
Extension Channel	Auto ▼
Transmit Rate	Auto ▼
* Security Mode	None ▼
Isolate Client	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)

---End

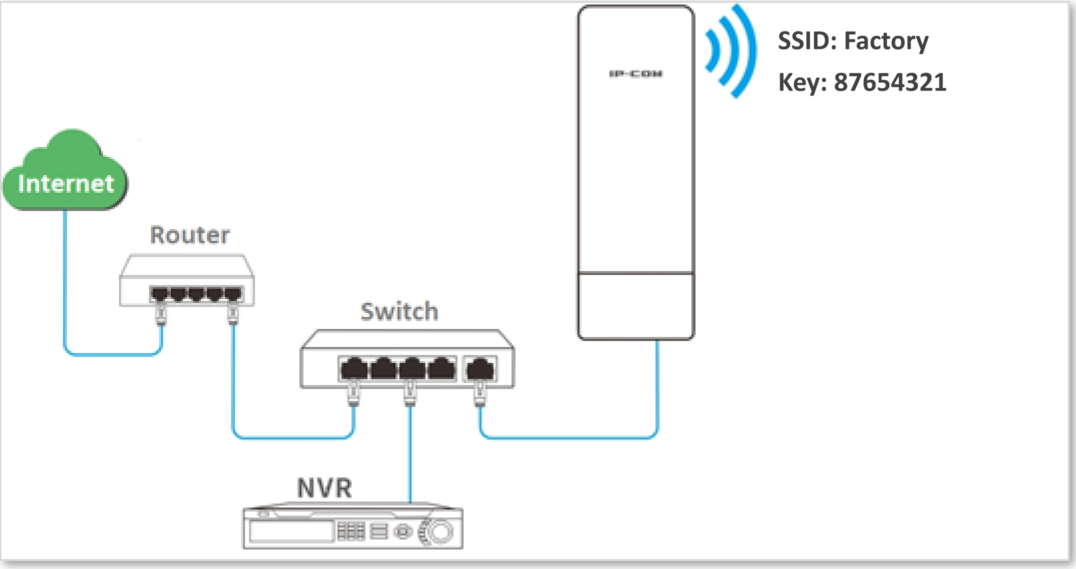
Verification

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

Setting up a Wireless Network Encrypted Using WPA2-PSK

Networking requirement

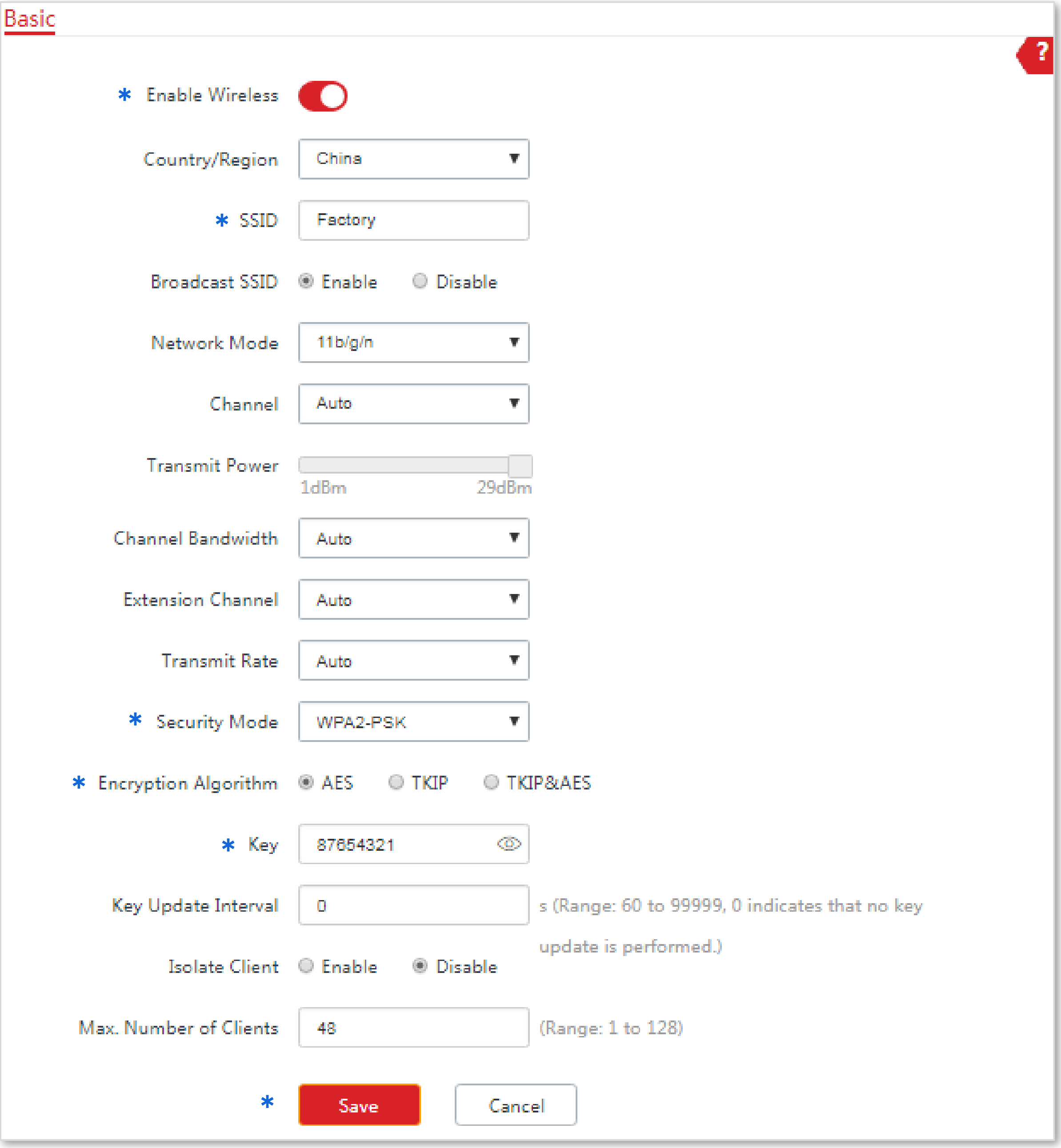
A factory's surveillance network with a certain level of security must be set up through a simply procedure. In this case, WPA2-PSK mode is recommended. See the following figure.



Configuration procedure

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

1. Choose Wireless > Basic.
2. Enable the wireless function.
3. Change the value of the SSID text box to **Factory**.
4. Set Security Mode to WPA2-PSK and Encryption Algorithm to AES.
5. Set Key to 87654321.
6. Click **Save**.



Basic

* Enable Wireless	● (on)
Country/Region	China
* SSID	Factory
Broadcast SSID	● Enable ○ Disable
Network Mode	11b/g/n
Channel	Auto
Transmit Power	1dBm – 29dBm
Channel Bandwidth	Auto
Extension Channel	Auto
Transmit Rate	Auto
* Security Mode	WPA2-PSK
* Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
* Key	87654321
Key Update Interval	0 s (Range: 60 to 99999, 0 indicates that no key update is performed.)
Isolate Client	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)

---End

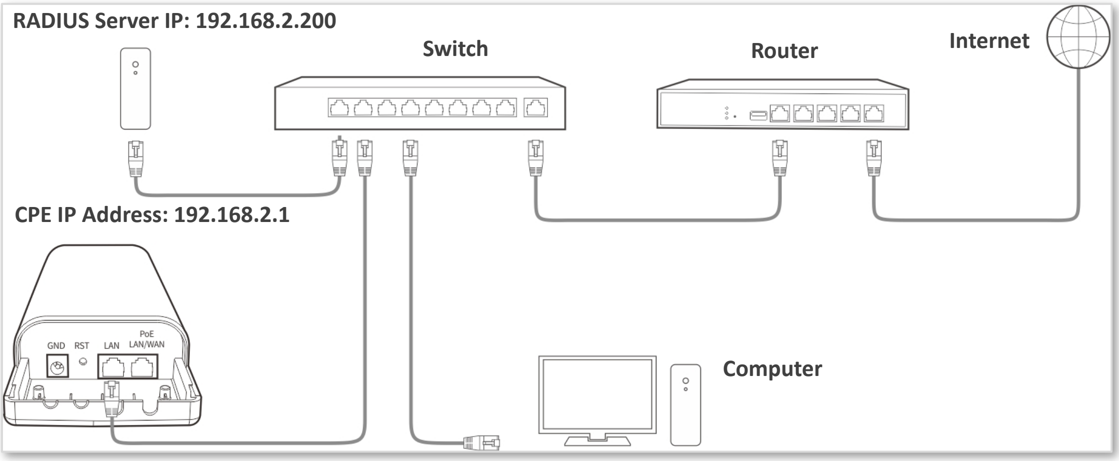
Verification

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

Setting up a Wireless Network Encrypted Using WPA or WPA2

Networking requirement

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



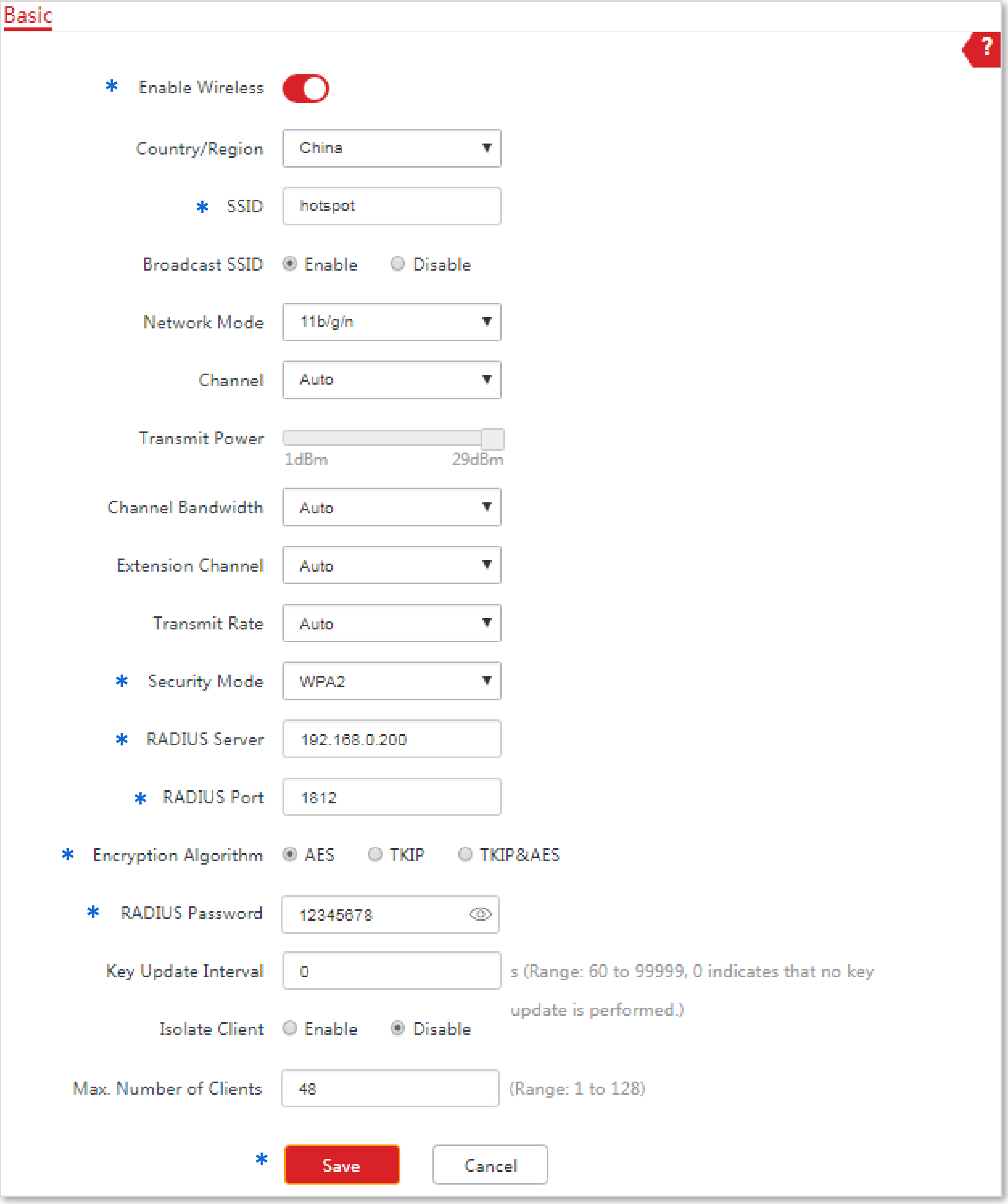
Configuration procedure

Configure the CPE

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

Assume that the second SSID of the AP is used.

1. Choose Wireless > Basic.
2. Enable the wireless function.
3. Change the value of the SSID text box to **hotspot**.
4. Set Security Mode to WPA2.
5. Set RADIUS Server, RADIUS Port, and RADIUS Password to 192.168.0.200, 1812, and 12345678 respectively.
6. Set Encryption Algorithm to AES.
7. Click **Save**.



Basic

* Enable Wireless	●
Country/Region	China ▼
* SSID	hotspot
Broadcast SSID	● Enable ○ Disable
Network Mode	11b/g/n ▼
Channel	Auto ▼
Transmit Power	1dBm – 29dBm
Channel Bandwidth	Auto ▼
Extension Channel	Auto ▼
Transmit Rate	Auto ▼
* Security Mode	WPA2 ▼
* RADIUS Server	192.168.0.200
* RADIUS Port	1812
* Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
* RADIUS Password	12345678
Key Update Interval	0 s (Range: 60 to 99999, 0 indicates that no key update is performed.)
Isolate Client	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)

---End

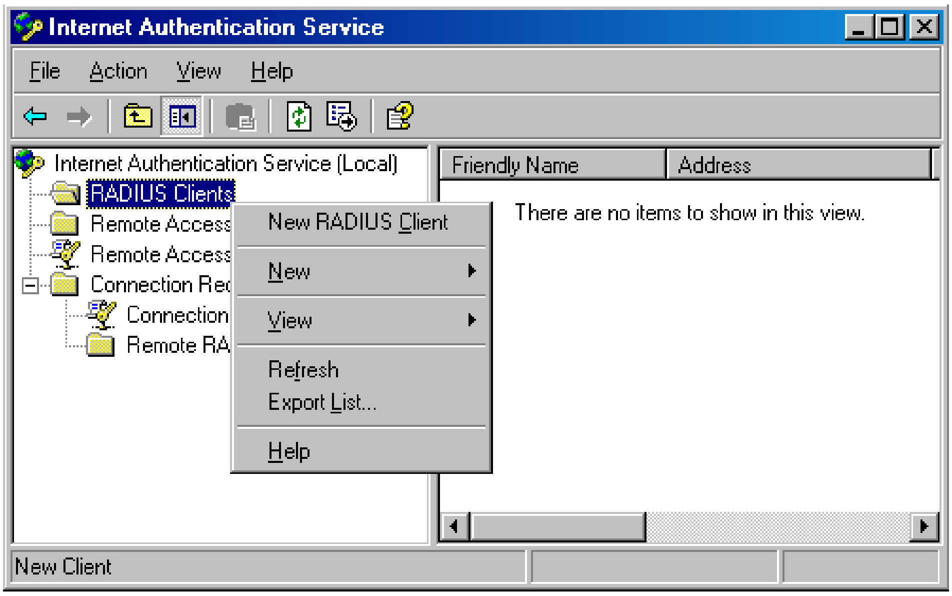
Configure the RADIUS server

Tip

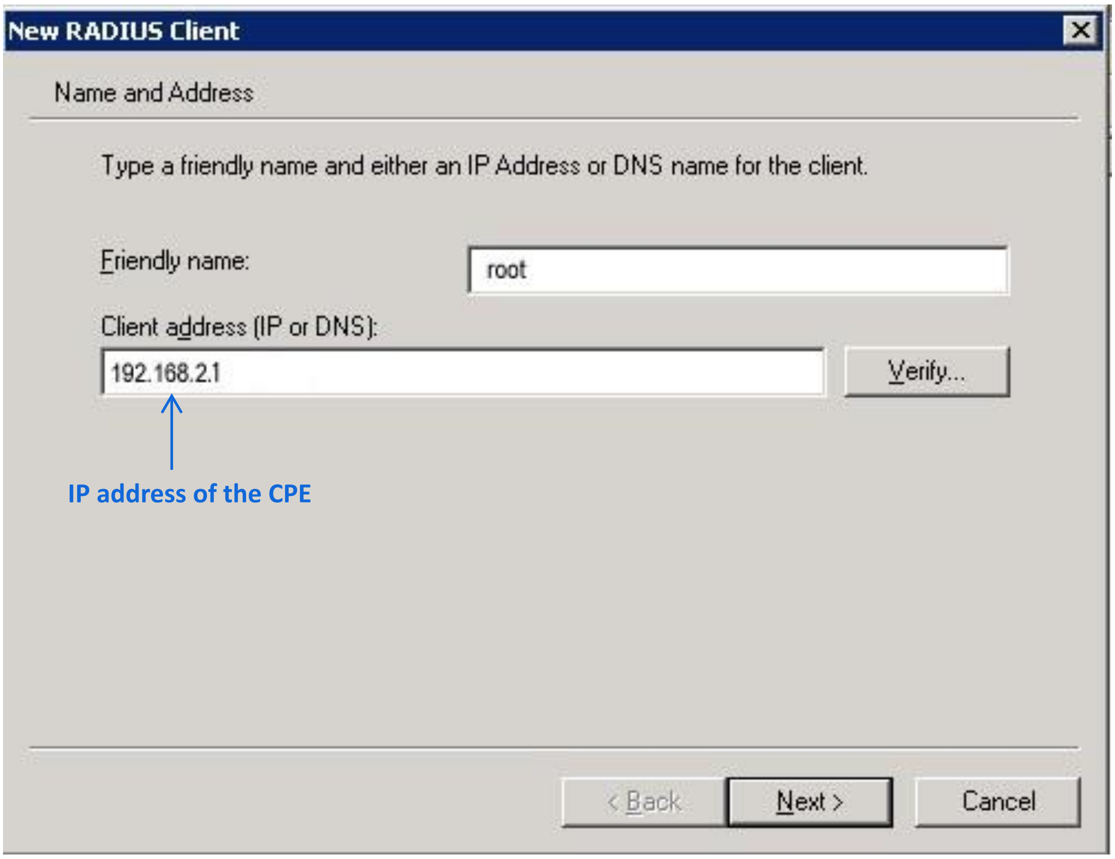
Windows 2003 is used as an example to describe how to configure the RADIUS server.

1. Configure a RADIUS client.

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



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


New RADIUS Client

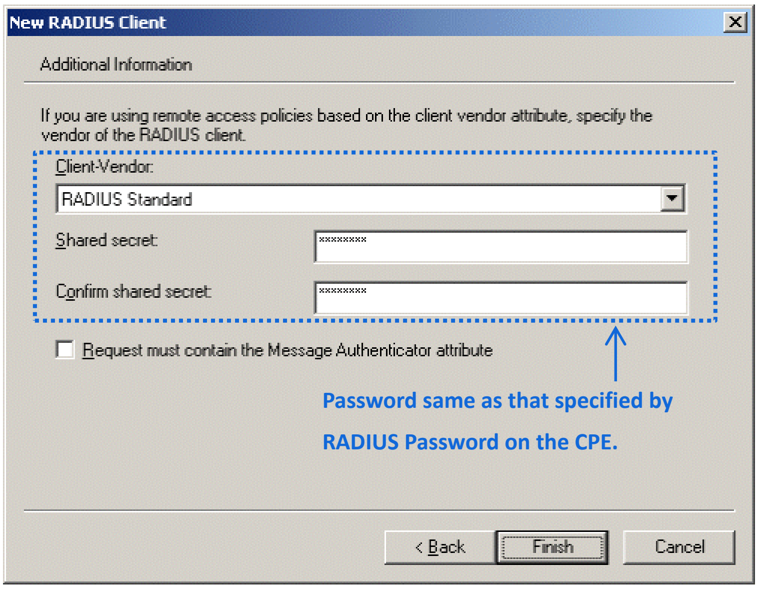
Name and Address

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

Friendly name: root

Client address (IP or DNS): 192.168.2.1

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



New RADIUS Client

Additional Information

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

Client-Vendor: RADIUS Standard

Shared secret: ********

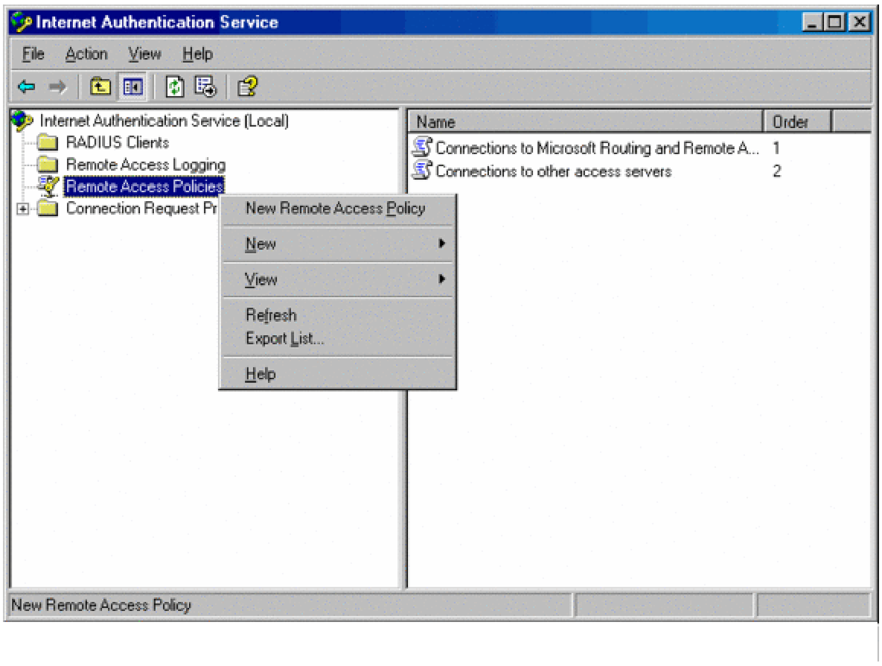
Confirm shared secret: ********

□ Request must contain the Message Authenticator attribute

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

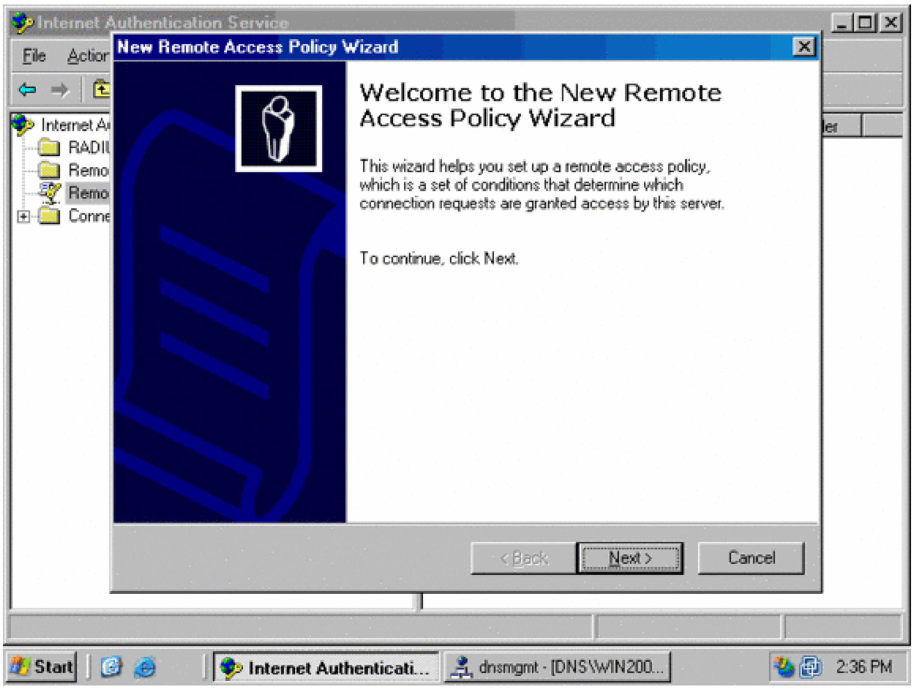
2. Configure a remote access policy.

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



Name	Order
Connections to Microsoft Routing and Remote A...	1
Connections to other access servers	2

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

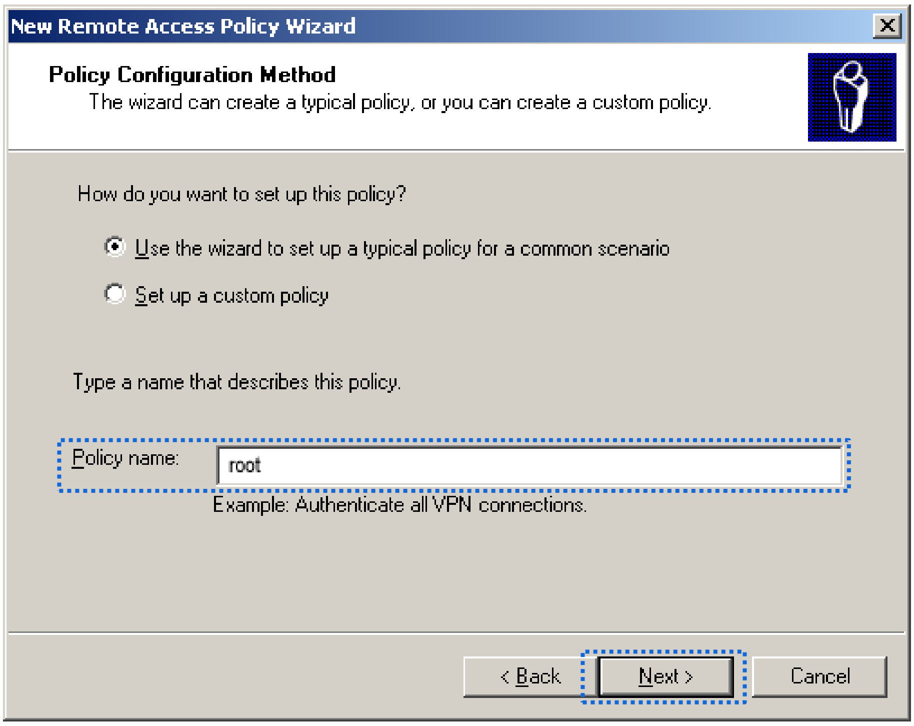


Welcome to the New Remote Access Policy Wizard

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

To continue, click Next.

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



Policy Configuration Method

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

How do you want to set up this policy?

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

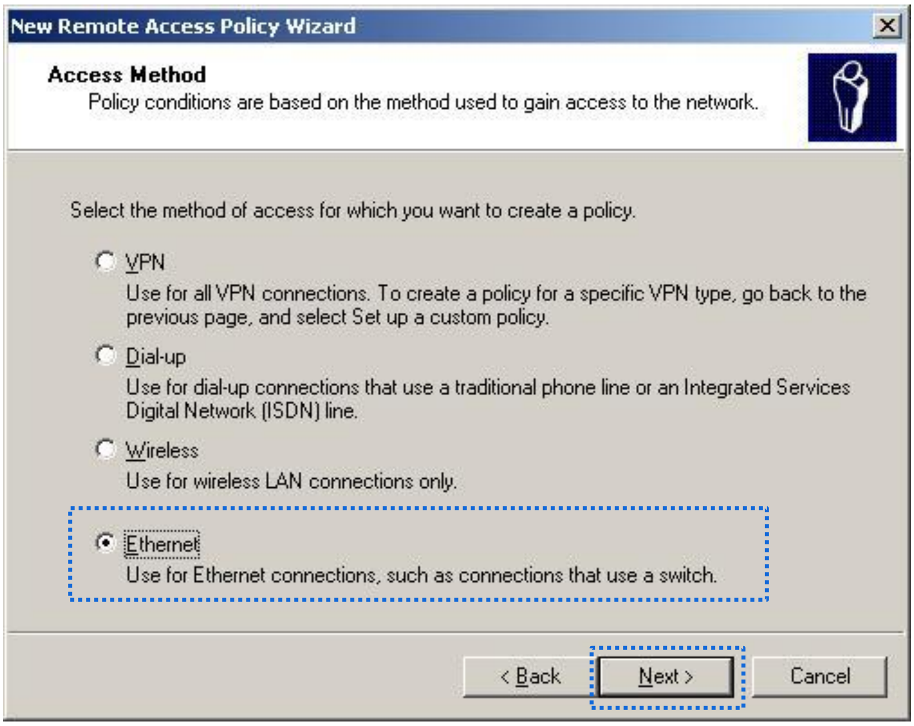
○ Set up a custom policy

Type a name that describes this policy.

Policy name: root

Example: Authenticate all VPN connections.

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



New Remote Access Policy Wizard

Access Method

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

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

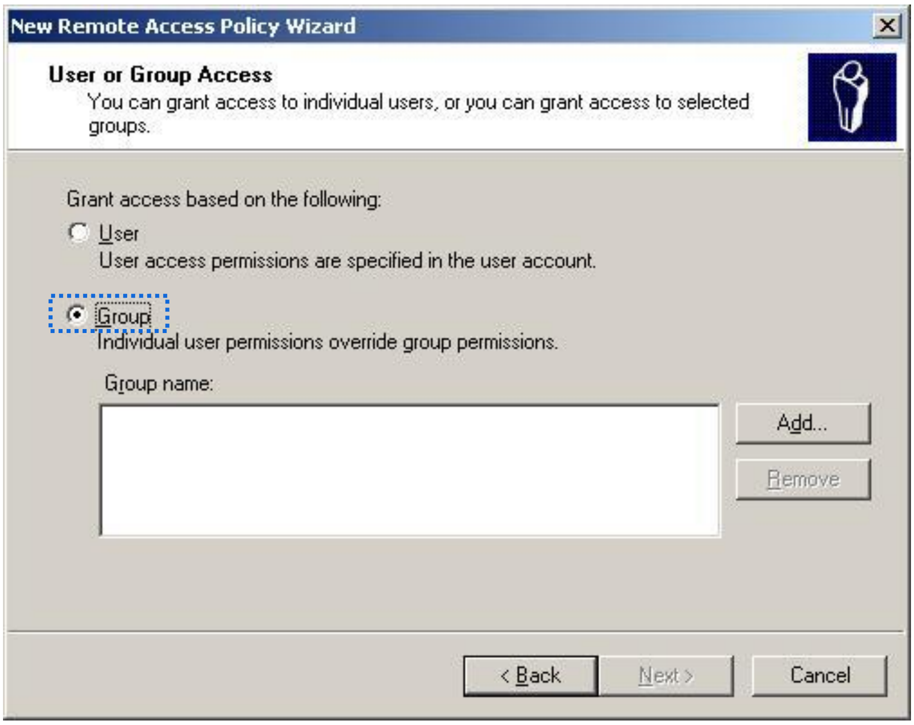
○ VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

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

○ Wireless
Use for wireless LAN connections only.

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

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



New Remote Access Policy Wizard

User or Group Access

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

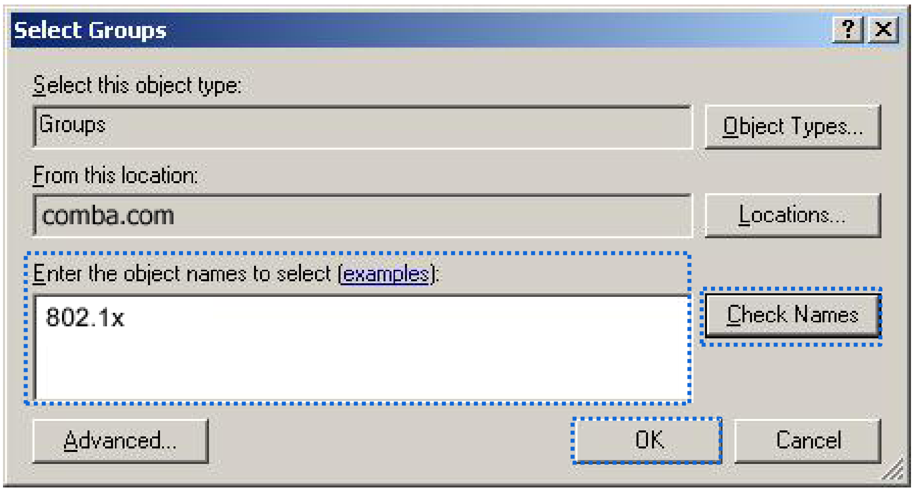
Grant access based on the following:

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

● Group
Individual user permissions override group permissions.

Group name:

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



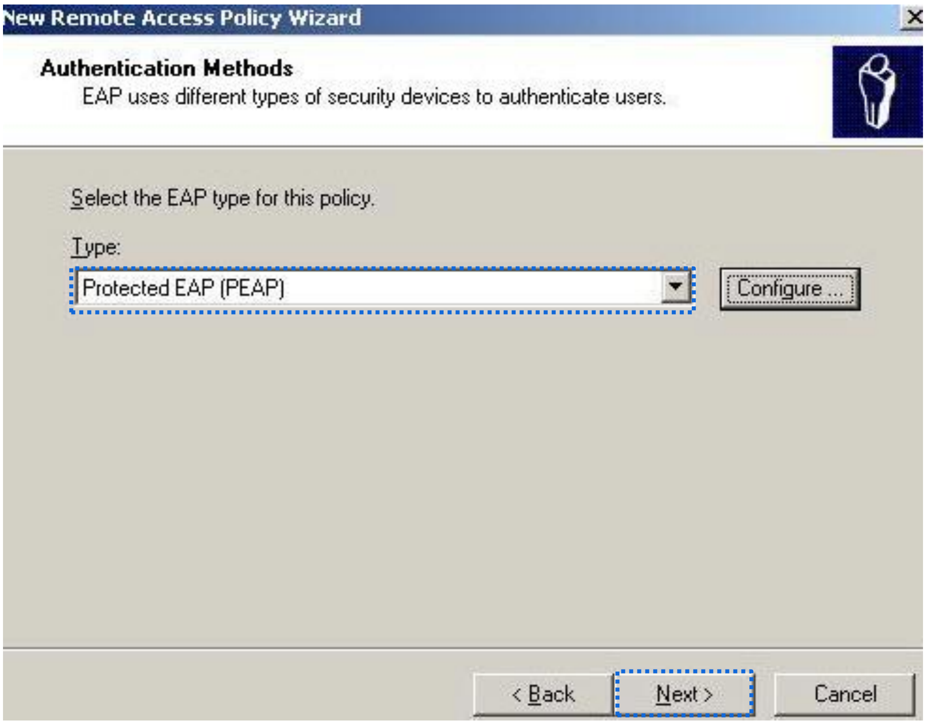
Select Groups

Select this object type: Groups

From this location: comba.com

Enter the object names to select (examples): 802.1x

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



New Remote Access Policy Wizard

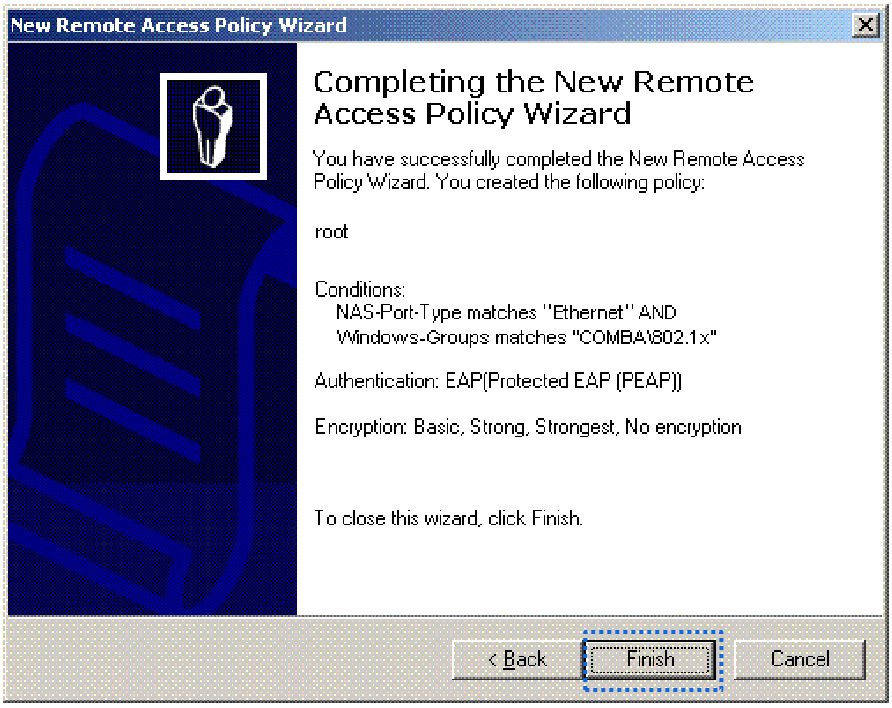
Authentication Methods

EAP uses different types of security devices to authenticate users.

Select the EAP type for this policy.

Type: Protected EAP (PEAP)

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



New Remote Access Policy Wizard

Completing the New Remote Access Policy Wizard

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

root

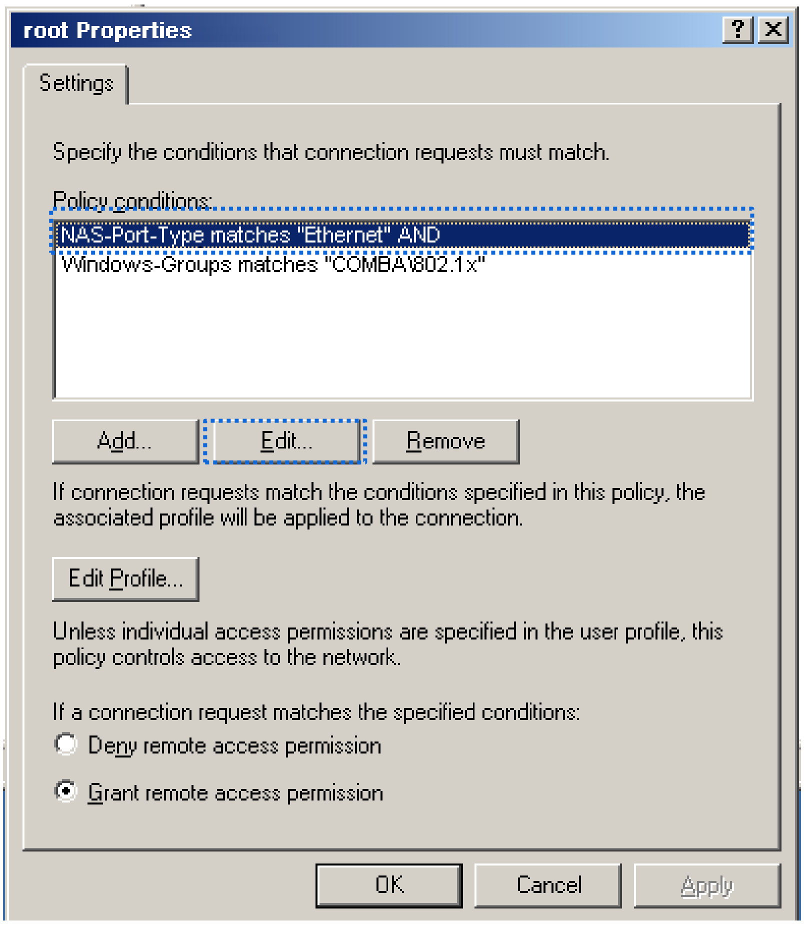
Conditions:
NAS-Port-Type matches "Ethernet" AND
Windows-Groups matches "COMBA\802.1x"

Authentication: EAP(Protected EAP (PEAP))

Encryption: Basic, Strong, Strongest, No encryption

To close this wizard, click Finish.

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



root Properties

Settings

Specify the conditions that connection requests must match.

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

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

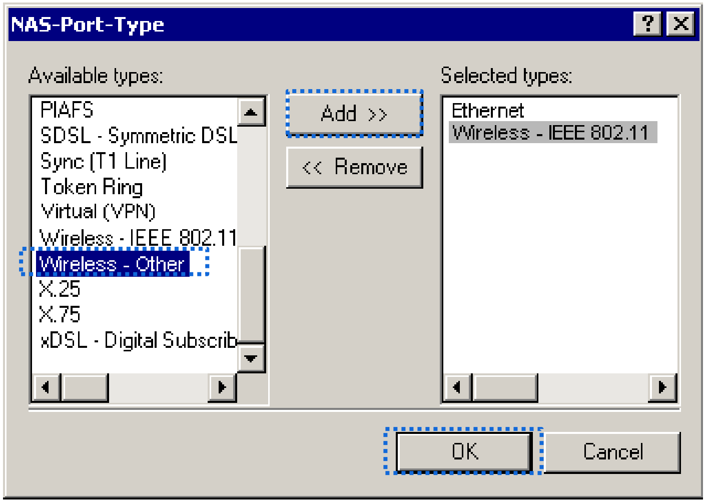
Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

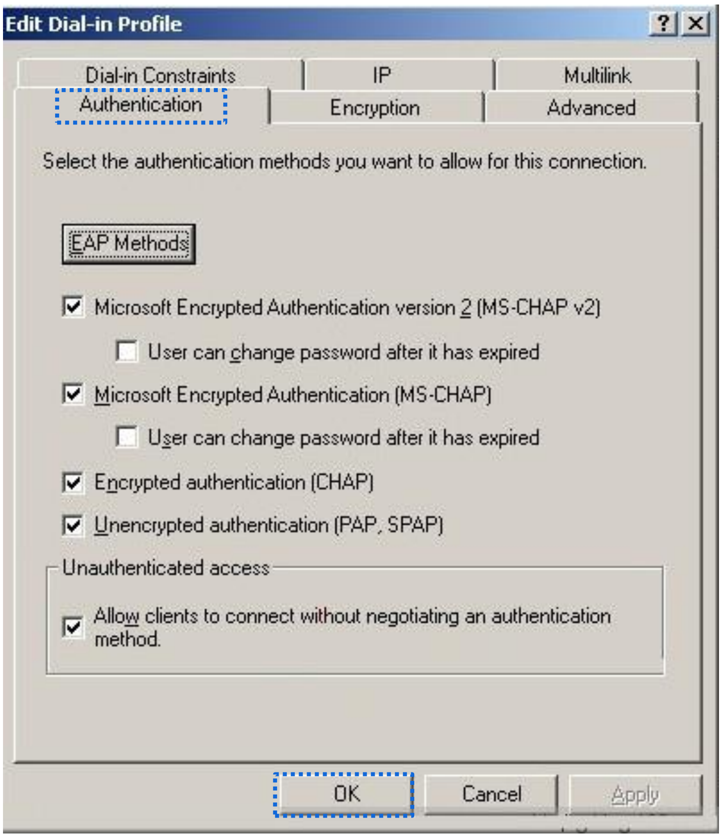
○ Deny remote access permission

● Grant remote access permission

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



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



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

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

☐ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

☑ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☑ Allow clients to connect without negotiating an authentication method.

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

3. Configure user information.

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

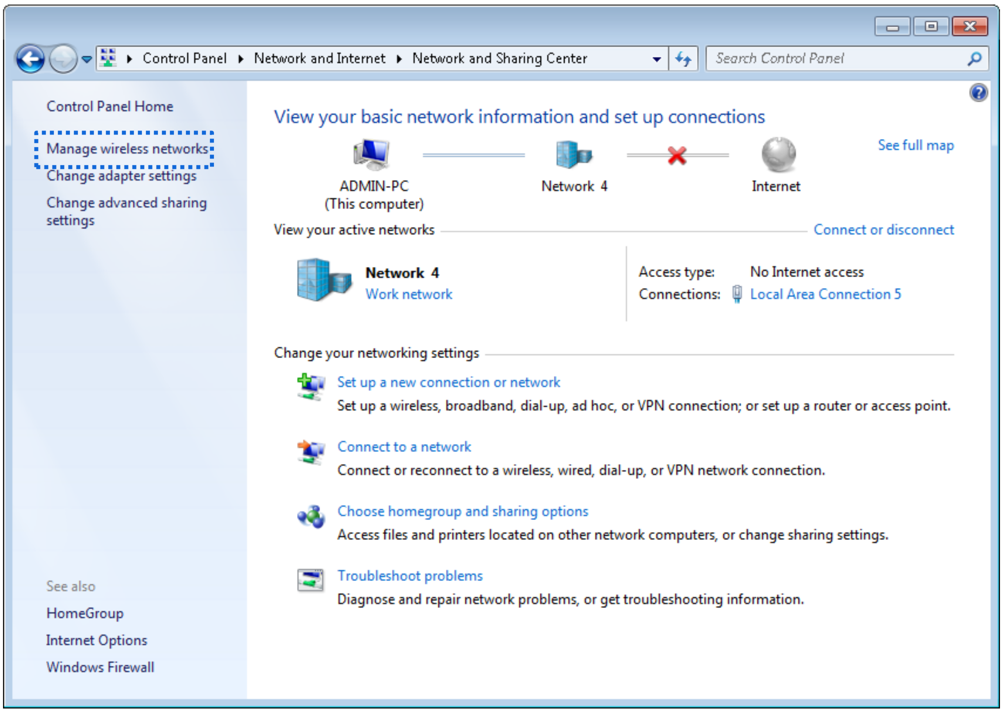
---End

Configure your wireless device

Tip

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

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



View your basic network information and set up connections

View your active networks

Network 4
Work network

Access type: No Internet access
Connections: Local Area Connection 5

Change your networking settings

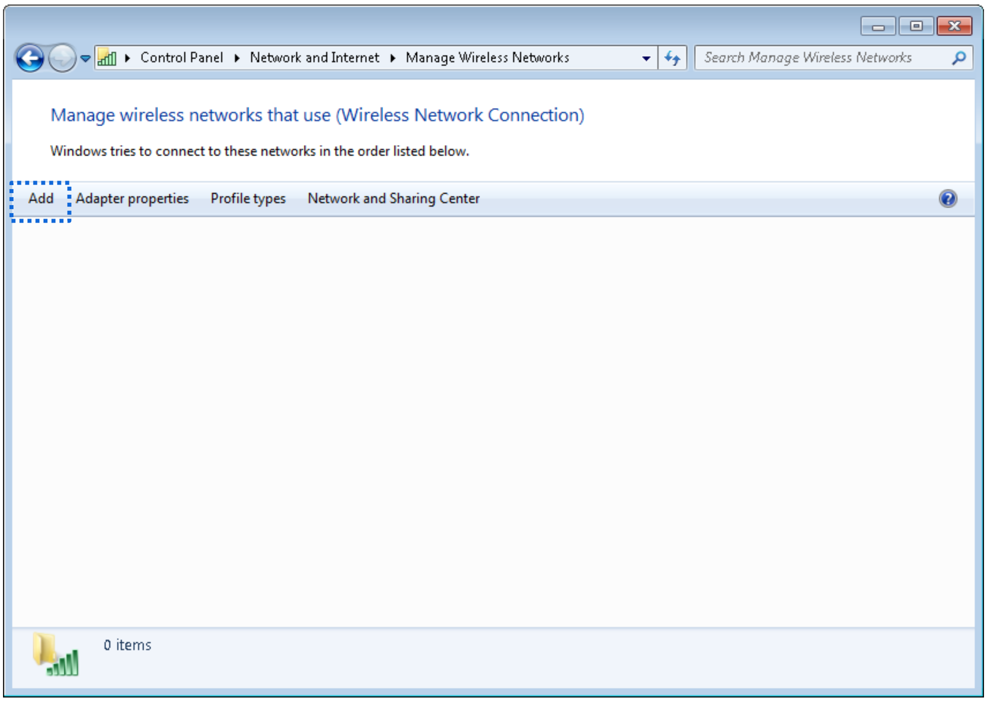
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

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

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

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

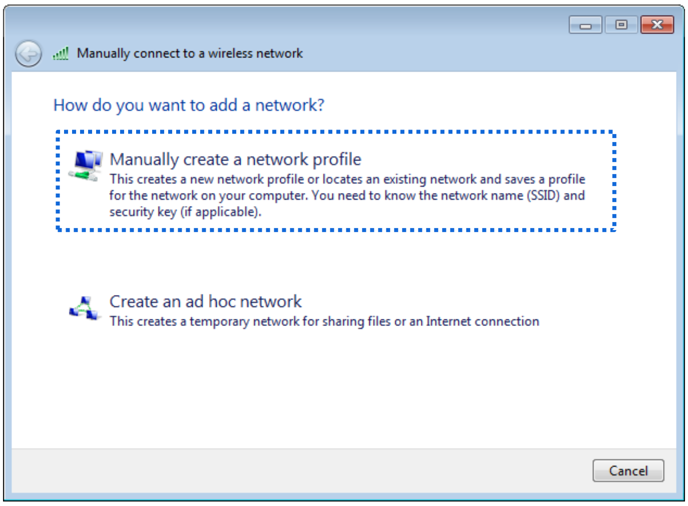
2. Click **Add**.


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

Manage wireless networks that use (Wireless Network Connection)

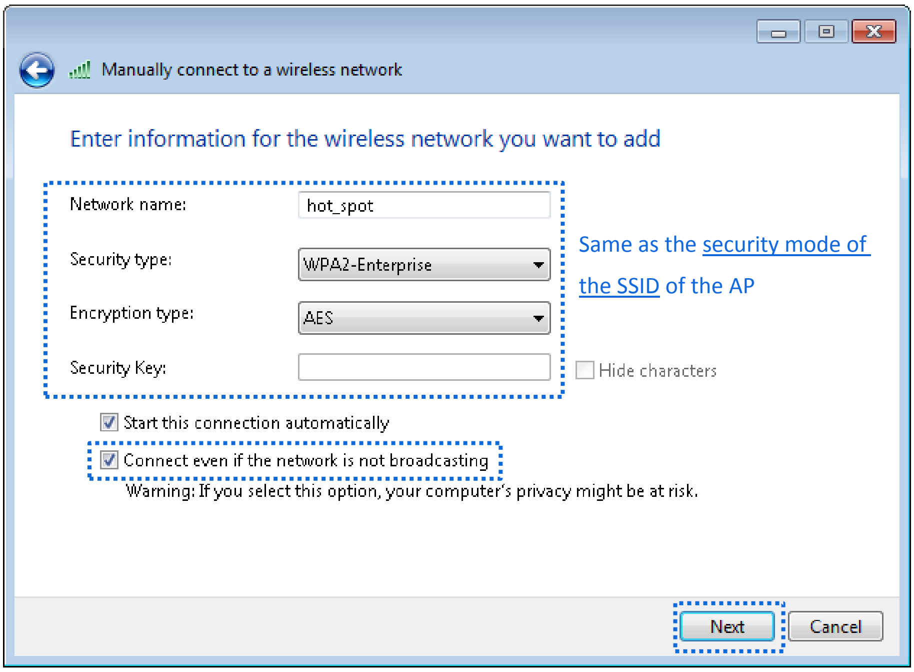
Windows tries to connect to these networks in the order listed below.

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



Manually connect to a wireless network
How do you want to add a network?
Manually create a network profile
This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).
Create an ad hoc network
This creates a temporary network for sharing files or an Internet connection
Cancel

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



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:	hot_spot
Security type:	WPA2-Enterprise
Encryption type:	AES
Security Key:	

□ Hide characters

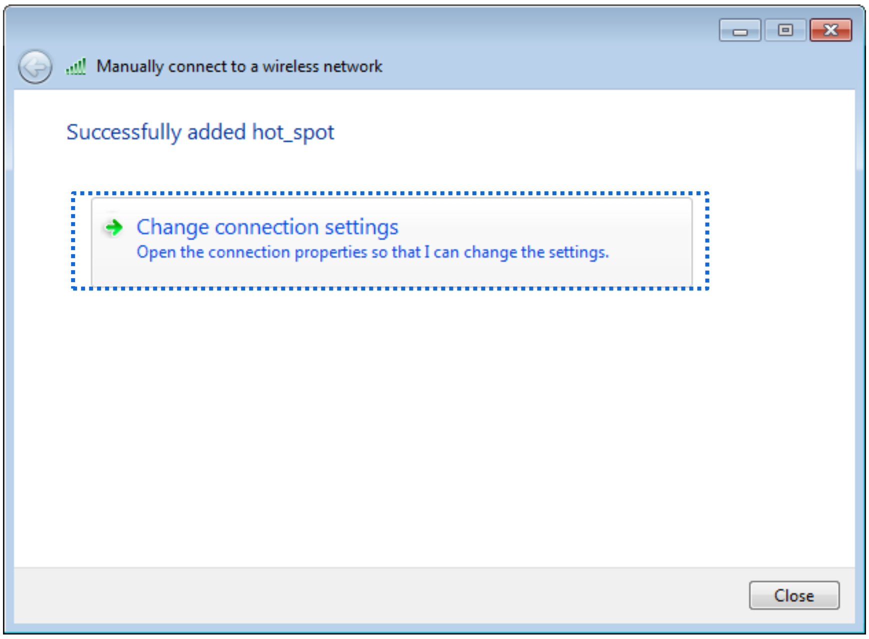
☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

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

Same as the security mode of the SSID of the AP

5. Click **Change connection settings**.

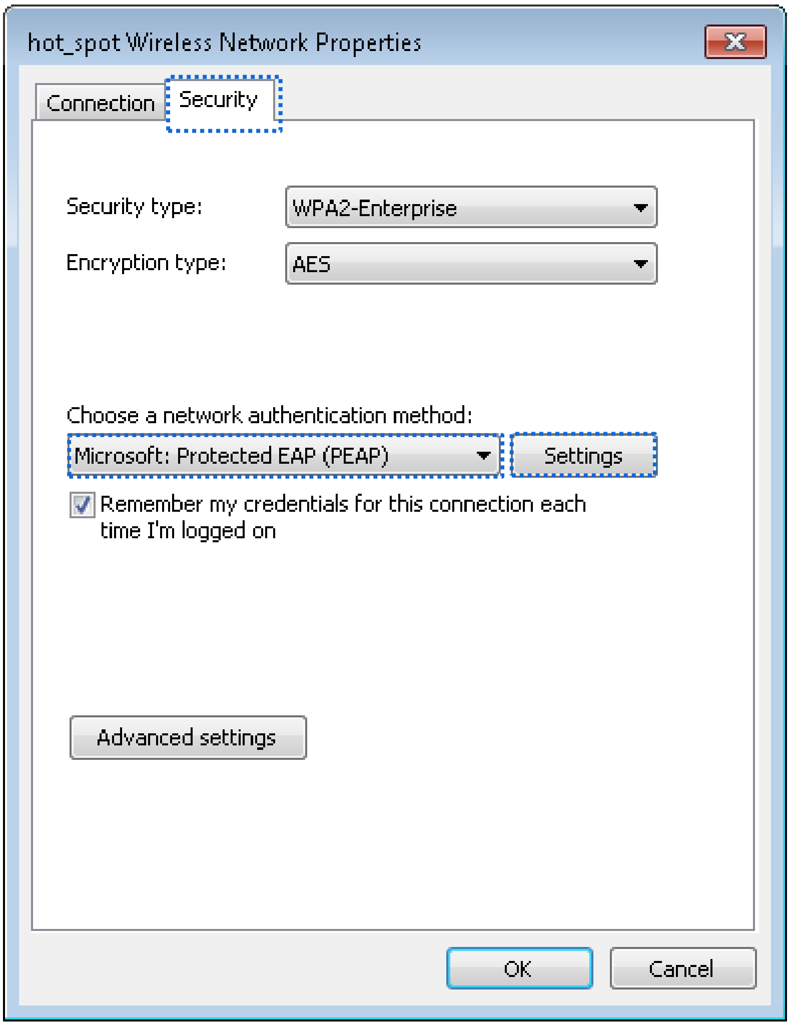


Manually connect to a wireless network

Successfully added hot_spot

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

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



hot_spot Wireless Network Properties

Security type: WPA2-Enterprise

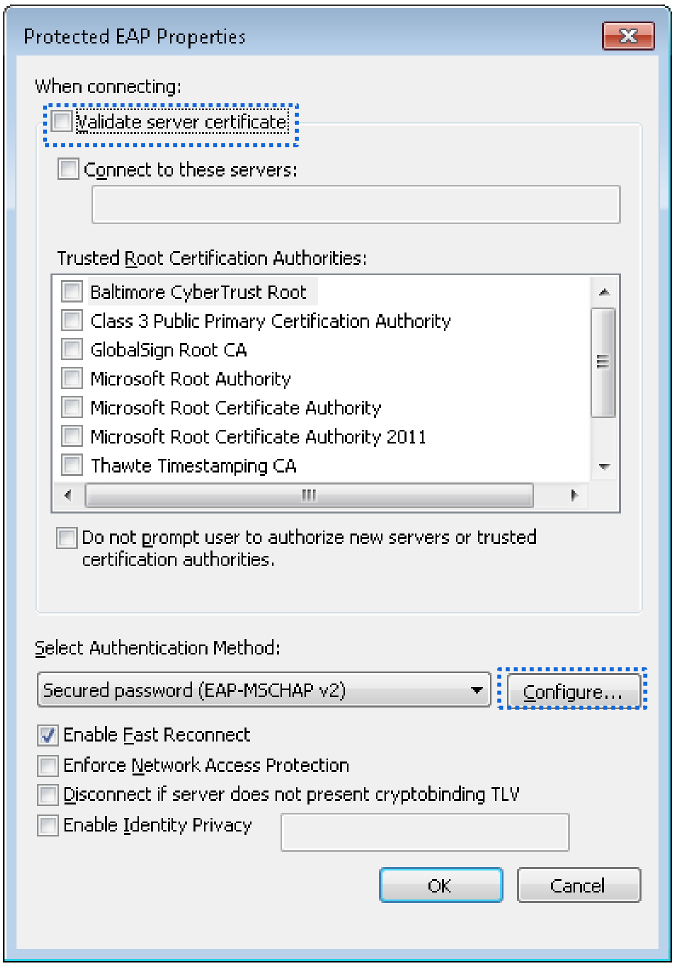
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

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

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



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

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

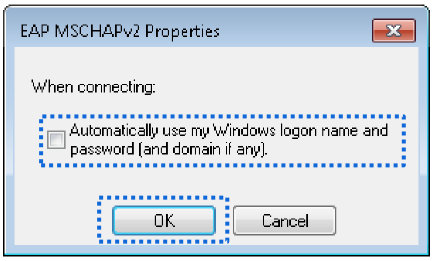
□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

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

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

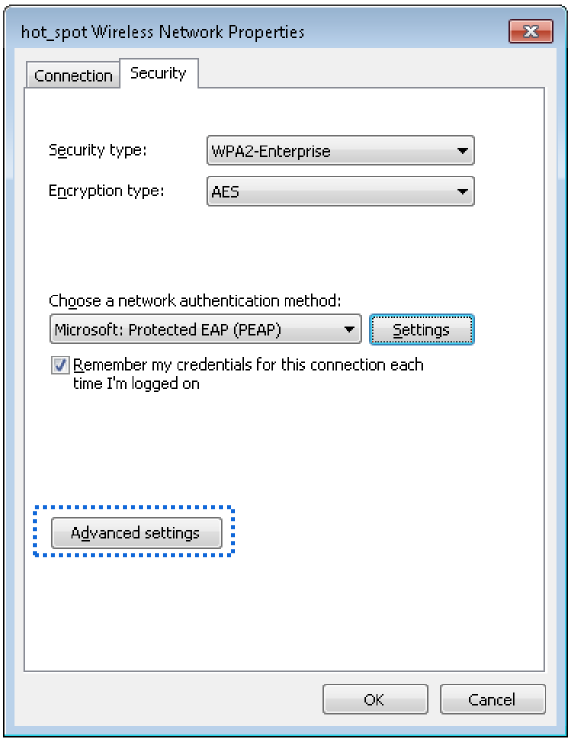


EAP MSCHAPv2 Properties

When connecting:

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

9. Click **Advanced settings**.



hot_spot Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

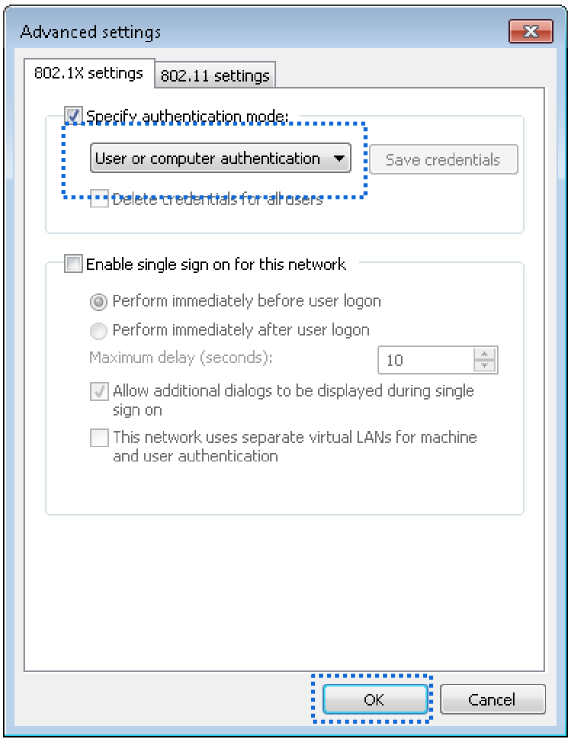
Microsoft: Protected EAP (PEAP) | Settings

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

Advanced settings

OK | Cancel

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



Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User or computer authentication | Save credentials

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

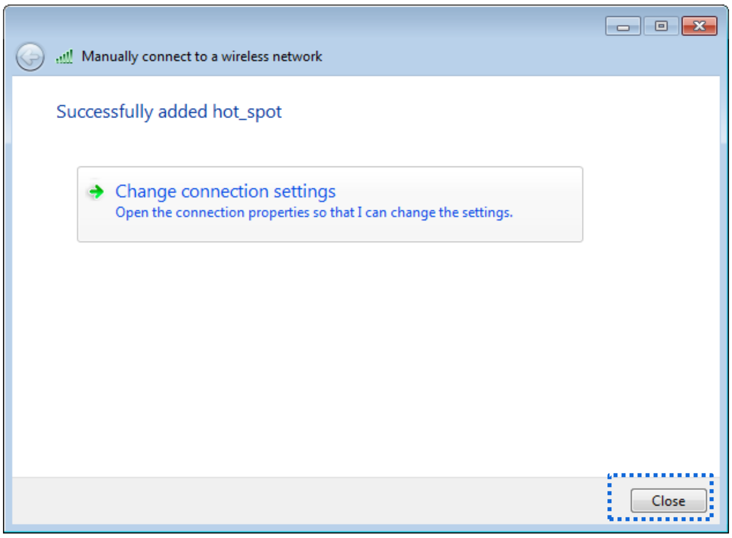
Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

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

OK | Cancel

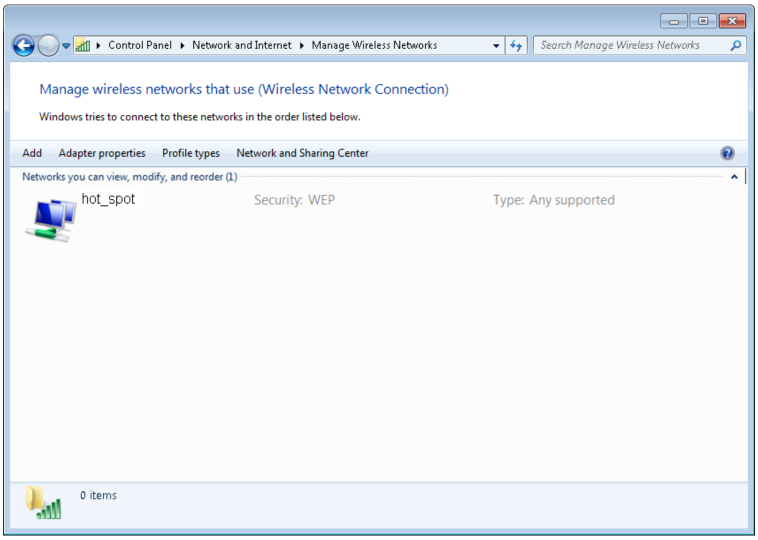
11. Click **Close**.



Manually connect to a wireless network

Successfully added hot_spot

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



Control Panel ▸ Network and Internet ▸ Manage Wireless Networks

Manage wireless networks that use (Wireless Network Connection)

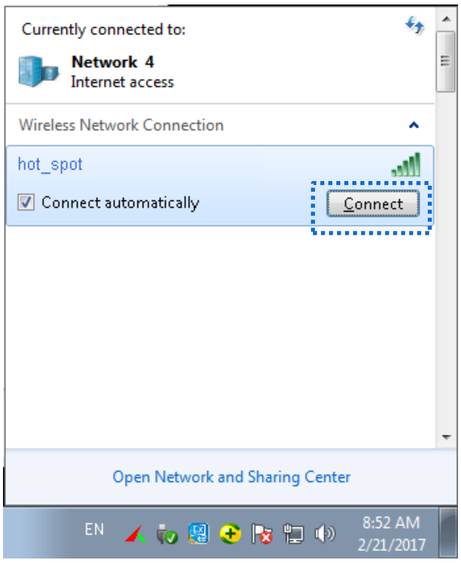
Windows tries to connect to these networks in the order listed below.

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

hot_spot Security: WEP Type: Any supported

0 items

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



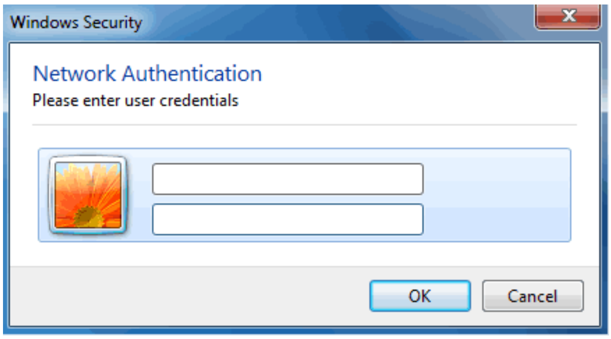
Currently connected to:
Network 4
Internet access

Wireless Network Connection

hot_spot

☑ Connect automatically

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



Windows Security

Network Authentication

Please enter user credentials

Verification

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

7.2 Advanced

7.2.1 Overview

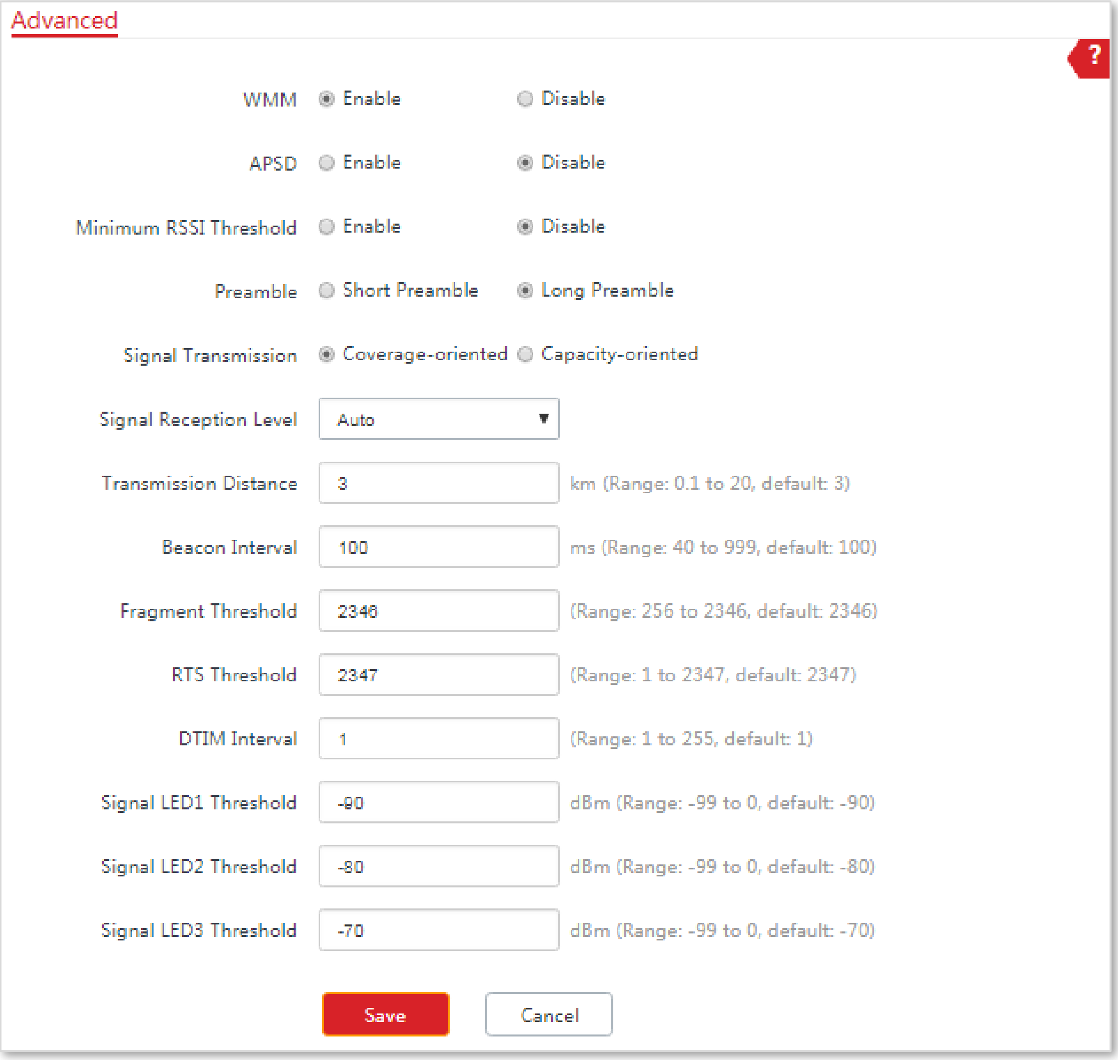
This module enables you to adjust the wireless performance. You are recommended to configure it under the guide of a professional.

Changing Advanced Settings

Tip

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

1. Choose Wireless > Advanced.
2. Change the parameter settings as required.
3. Click **Save**.



Advanced

WMM ● Enable ○ Disable

APSD ○ Enable ● Disable

Minimum RSSI Threshold ○ Enable ● Disable

Preamble ○ Short Preamble ● Long Preamble

Signal Transmission ● Coverage-oriented ○ Capacity-oriented

Signal Reception Level: Auto

Transmission Distance: 3 km (Range: 0.1 to 20, default: 3)

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

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

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

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

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

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

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

---End

Parameters Description

Name	Description
WMM	WMM is a wireless QoS protocol ensuring that packets with higher priorities are transmitted earlier. This ensures better QoS of voice and video applications over wireless networks. You are recommended to enable it.
APSD	Automatic Power Save Delivery. If it is enabled, the power consumption of this device is reduced after a specified period during which no traffic is transmitted or received. By default, it is disabled.
Minimum RSSI Threshold	It specifies the minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device. If there are multiple CPEs in a network, setting a proper value helps wireless devices connect to WiFi network with better WiFi signal.
Preamble	It specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the Short Preamble option.
Signal Transmission	It specifies the wall penetrating capability of the CPE. Coverage-oriented: With less interference nearby, this mode enables the CPE to cover wider

Name	Description
	area. Capacity-oriented: With strong interference nearby, this mode improves the CPE's anti-interference capability.
Signal Reception Level	It is used to adjust the signal reception level. A higher level leads to better signal reception capability, but lower throughput.
Transmission Distance	It specifies the wireless transmission distance of this device. You can set it based on the actual installation distance.
Beacon Interval	It specifies the interval at which this device sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.
Fragment Threshold	It specifies the threshold of a fragment. The unit is byte. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold to enable this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput. Frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
RTS Threshold	It specifies the frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	It specifies the countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval. For example, if DTIM Interval is set to 1, this device transmits all cached frames at one Beacon interval.
Signal LED1/2/3 Threshold	It is used to edit the threshold value determining whether WiFi signal LEDs light up. Corresponding LED will be triggered to light up when the received WiFi signal strength reaches the threshold.

7.3 Access Control

7.3.1 Overview

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

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

7.3.2 Configuring Access Control

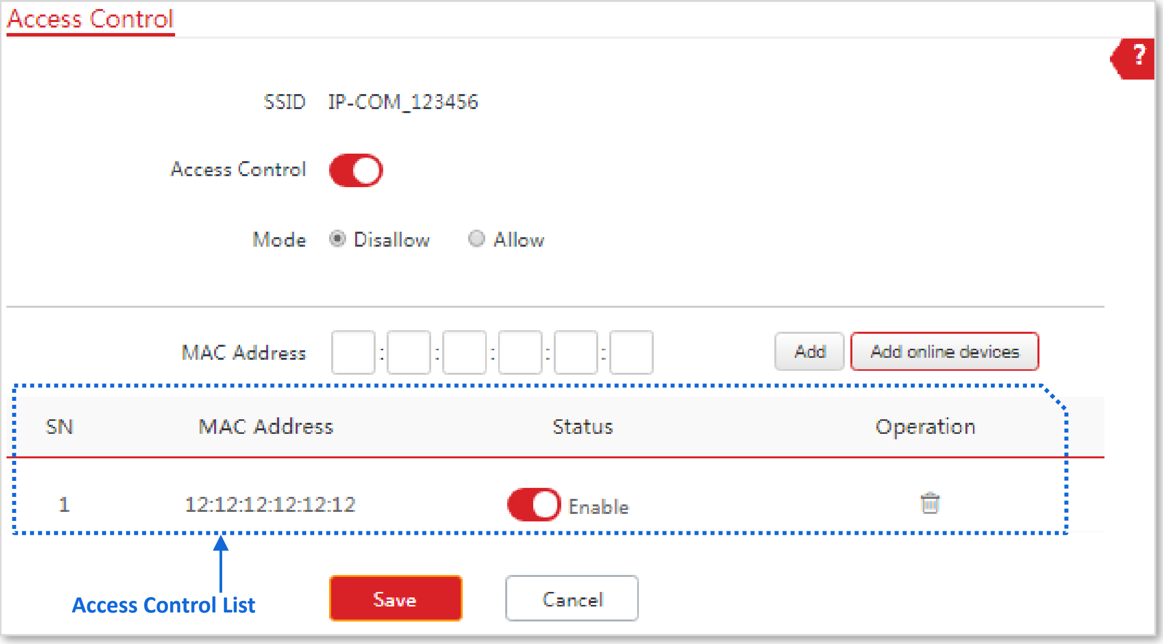
Configuration Procedure

1. Choose Wireless > Access Control.
2. Enable the **Access Control** function.
3. Select a MAC address filter mode, **Disallow** or **Allow**.
4. Enter the MAC addresses to control in the access control list and click **Add**.

Tip

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

5. Click **Save**.



Access Control

SSID IP-COM_123456

Access Control ●

Mode ● Disallow ○ Allow

MAC Address □:□:□:□:□:□

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

---End

Parameters Description

Name	Description
SSID	It specifies the SSID that requires wireless client access control.
Access Control	It specifies whether to enable the Access Control function.
Mode	It specifies the mode for filtering MAC addresses. – **Allow**: It indicates that only the wireless clients on the access control list can connect to the WiFi network of the CPE. – **Disallow**: It indicates that only the wireless clients on the access control list cannot connect to the WiFi network of the CPE.

7.3.3 Example of Configuring Access Control

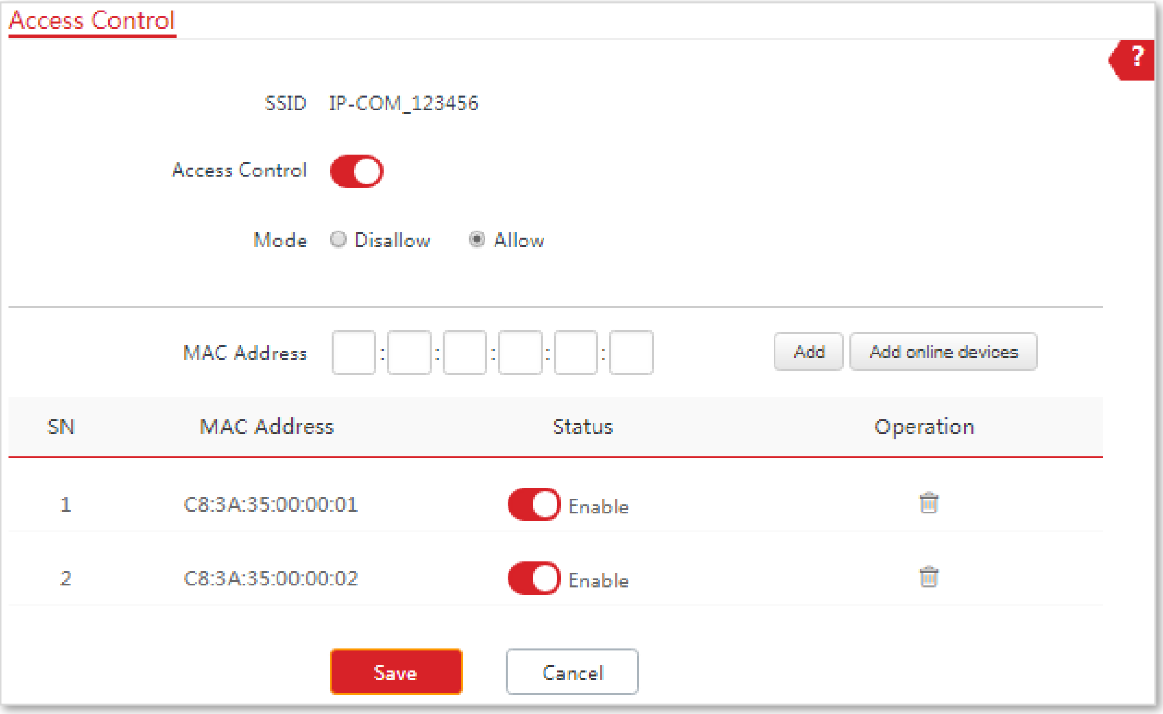
Networking Requirement

A wireless network whose SSID is IP-COM_123456 has been set up in a residential community. Only several users are allowed to connect to the wireless network.

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

Configuration Procedure:

1. Choose Wireless > Access Control.
2. Enable the **Access Control** function.
3. Set the **Mode** to **Allow**.
4. Enter the MAC address, which is C8:3A:35:00:00:01 is this example, and click **Add**.
5. Perform step 4 to add the other two MAC addresses.
6. Click **Save**.



Access Control

SSID IP-COM_123456

Access Control

Mode ○ Disallow ● Allow

MAC Address □:□:□:□:□:□

SN	MAC Address	Status	Operation
1	C8:3A:35:00:00:01	Enable	
2	C8:3A:35:00:00:02	Enable	

---End

Verification

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

8 Advanced

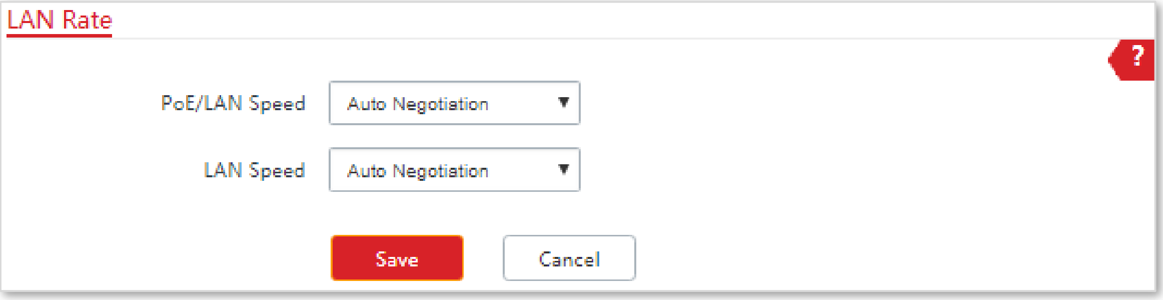
8.1 LAN Rate

8.1.1 Overview

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

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

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



LAN Rate

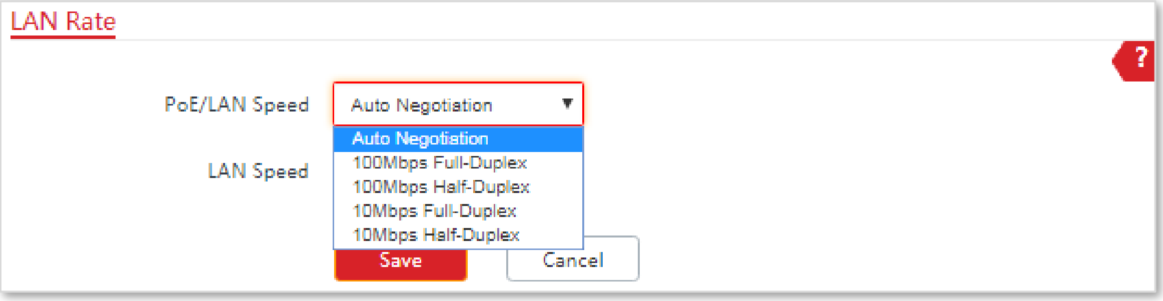
PoE/LAN Speed: Auto Negotiation

LAN Speed: Auto Negotiation

8.1.2 Changing the LAN Speed and Duplex Mode

Configuration Procedure

1. Choose **Advanced** > **LAN Rate**.
2. Select a LAN speed and duplex mode for each LAN port.
3. Click **Save**.



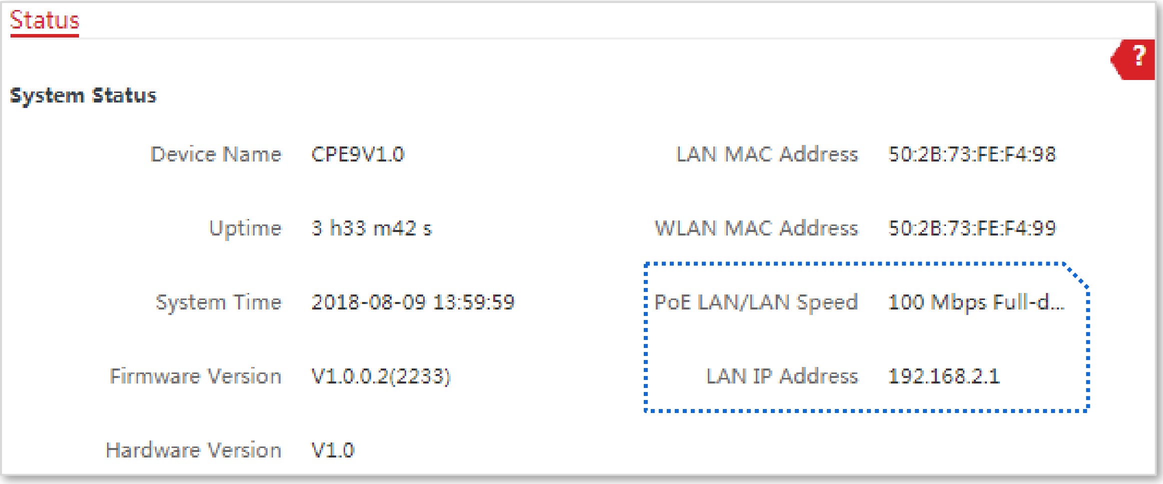
PoE/LAN Speed Auto Negotiation

LAN Speed

---End

Verification

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



System Status

Device Name	CPE9V1.0	LAN MAC Address	50:2B:73:FE:F4:98
Uptime	3 h33 m42 s	WLAN MAC Address	50:2B:73:FE:F4:99
System Time	2018-08-09 13:59:59	PoE LAN/LAN Speed	100 Mbps Full-d...
Firmware Version	V1.0.0.2(2233)	LAN IP Address	192.168.2.1
Hardware Version	V1.0		

8.2 Diagnose

8.2.1 Overview

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

If the network connection fails, you can use the diagnosis tools included with the CPE to locate the faulty node.

8.2.2 Site Survey

It is used to scan WiFi signals nearby for analysis with SSIDs, MAC addresses, channels and signal strength marked.

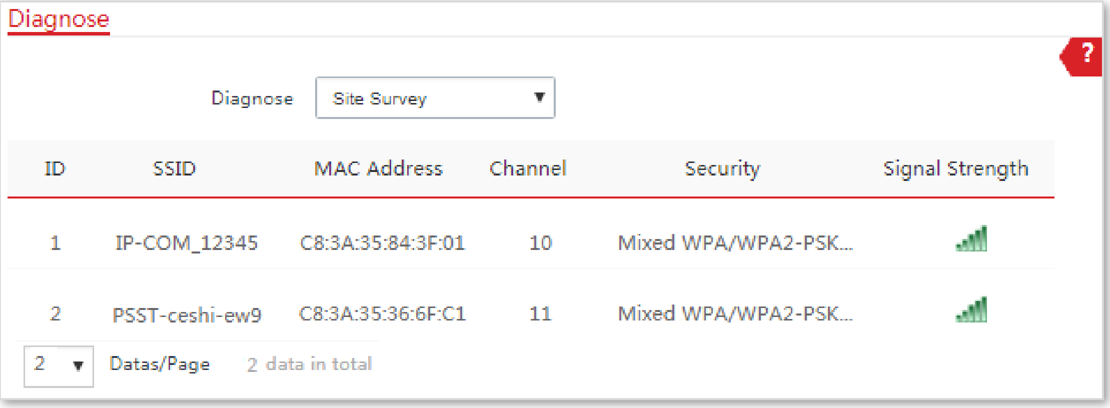
Assume that you want to know the WiFi networks nearby.

Configuration Pocedure

1. Choose **Advanced** > **Diagnose**.
2. Select **Site Survey** in the **Diagnose** list.

---End

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



Diagnose

Diagnose: Site Survey

ID	SSID	MAC Address	Channel	Security	Signal Strength
1	IP-COM_12345	C8:3A:35:84:3F:01	10	Mixed WPA/WPA2-PSK...	📶
2	PSST-ceshi-ew9	C8:3A:35:36:6F:C1	11	Mixed WPA/WPA2-PSK...	📶

2 Datas/Page 2 data in total

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

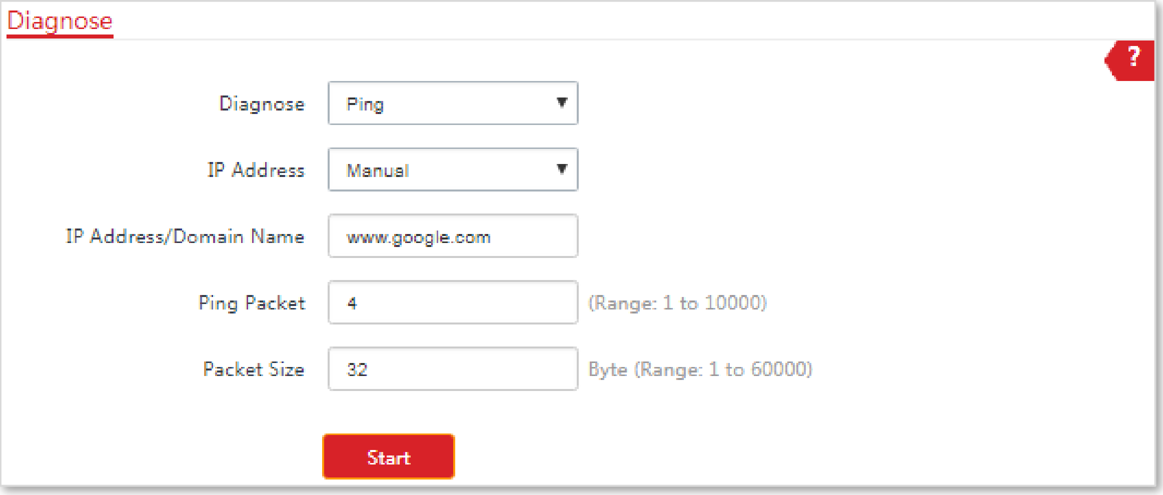
8.2.3 Ping

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

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

Configuration Procedure

1. Choose **Advanced** > **Diagnose**.
2. Select **Ping** in the Diagnose list.
3. Set **IP Address** to **Manual**.
4. Enter an IP address or a domain name, which is **www.google.com** in this example.
5. Enter a number of packets transmitted by ping.
6. Enter the size of packet transmitted by ping.
7. Click **Start**.

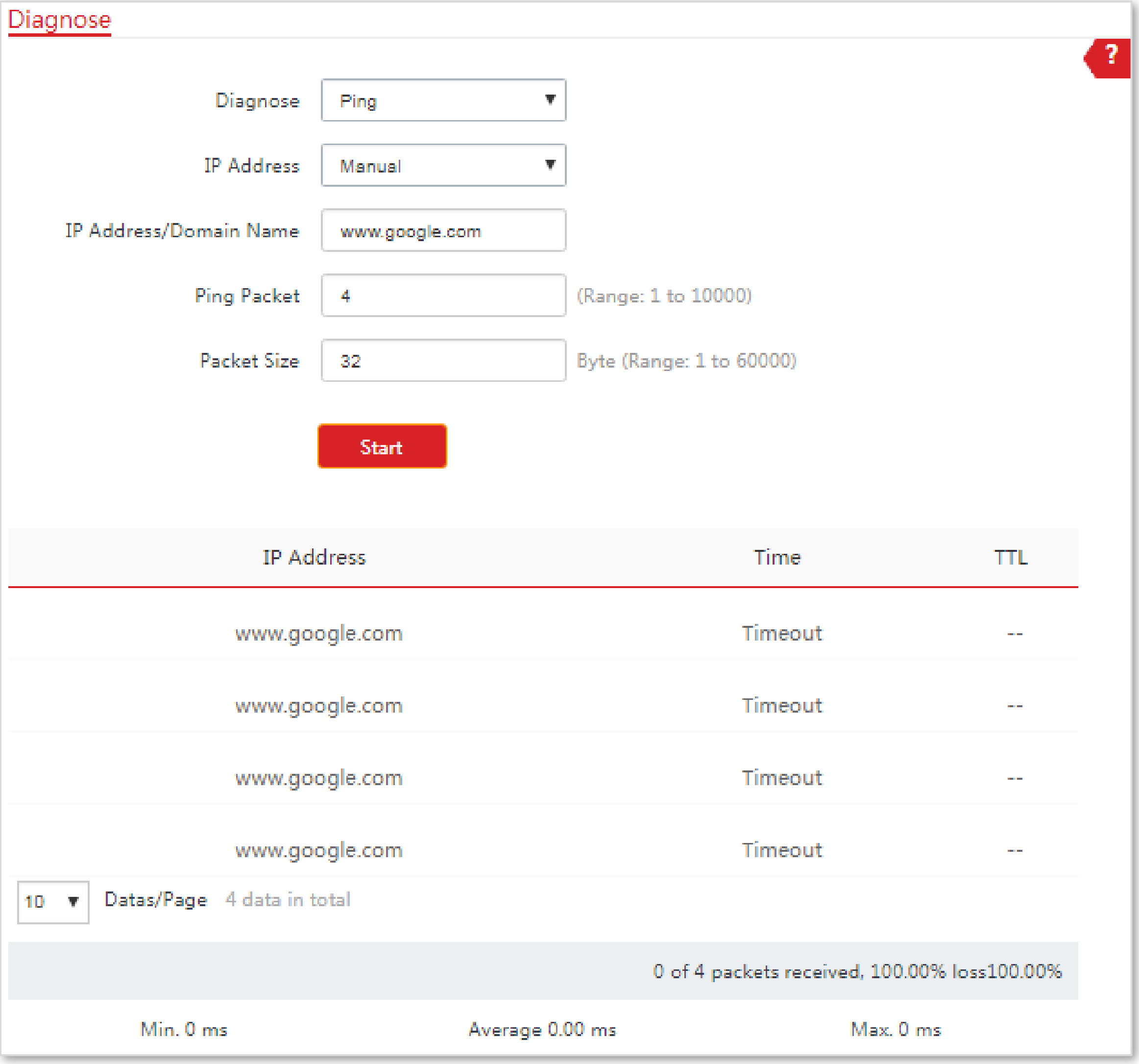


Diagnose

Diagnose	Ping ▼	
IP Address	Manual ▼	
IP Address/Domain Name	www.google.com	
Ping Packet	4	(Range: 1 to 10000)
Packet Size	32	Byte (Range: 1 to 60000)

---End

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



Diagnose

Diagnose	Ping
IP Address	Manual
IP Address/Domain Name	www.google.com
Ping Packet	4 (Range: 1 to 10000)
Packet Size	32 Byte (Range: 1 to 60000)

IP Address	Time	TTL
www.google.com	Timeout	--
www.google.com	Timeout	--
www.google.com	Timeout	--
www.google.com	Timeout	--

10 Datas/Page 4 data in total

0 of 4 packets received, 100.00% loss100.00%

Min. 0 ms Average 0.00 ms Max. 0 ms

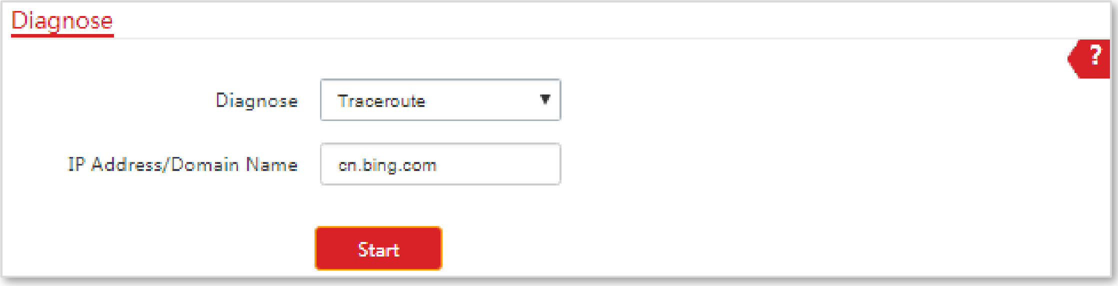
8.2.4 Traceroute

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

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

Configuration Procedure

1. Choose **Advanced** > **Diagnose**.
2. Select **Traceroute** in the Diagnose list.
3. Enter an IP address or a domain name, which is **cn.bing.com** in this example.
4. Click **Start**.

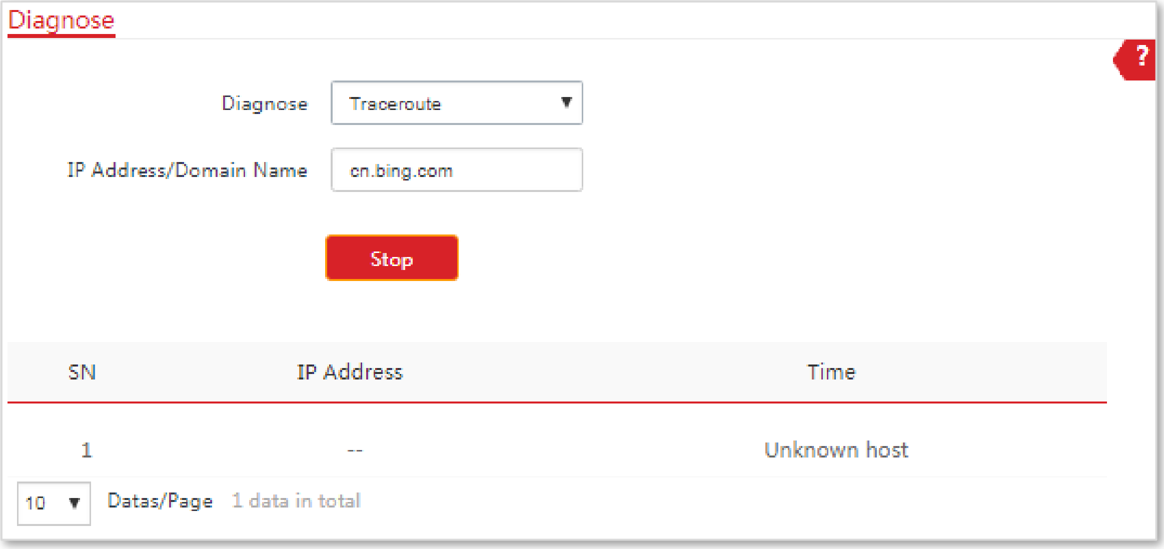


Diagnose: Traceroute

IP Address/Domain Name: cn.bing.com

---End

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



Diagnose: Traceroute

IP Address/Domain Name: cn.bing.com

SN	IP Address	Time
1	--	Unknown host

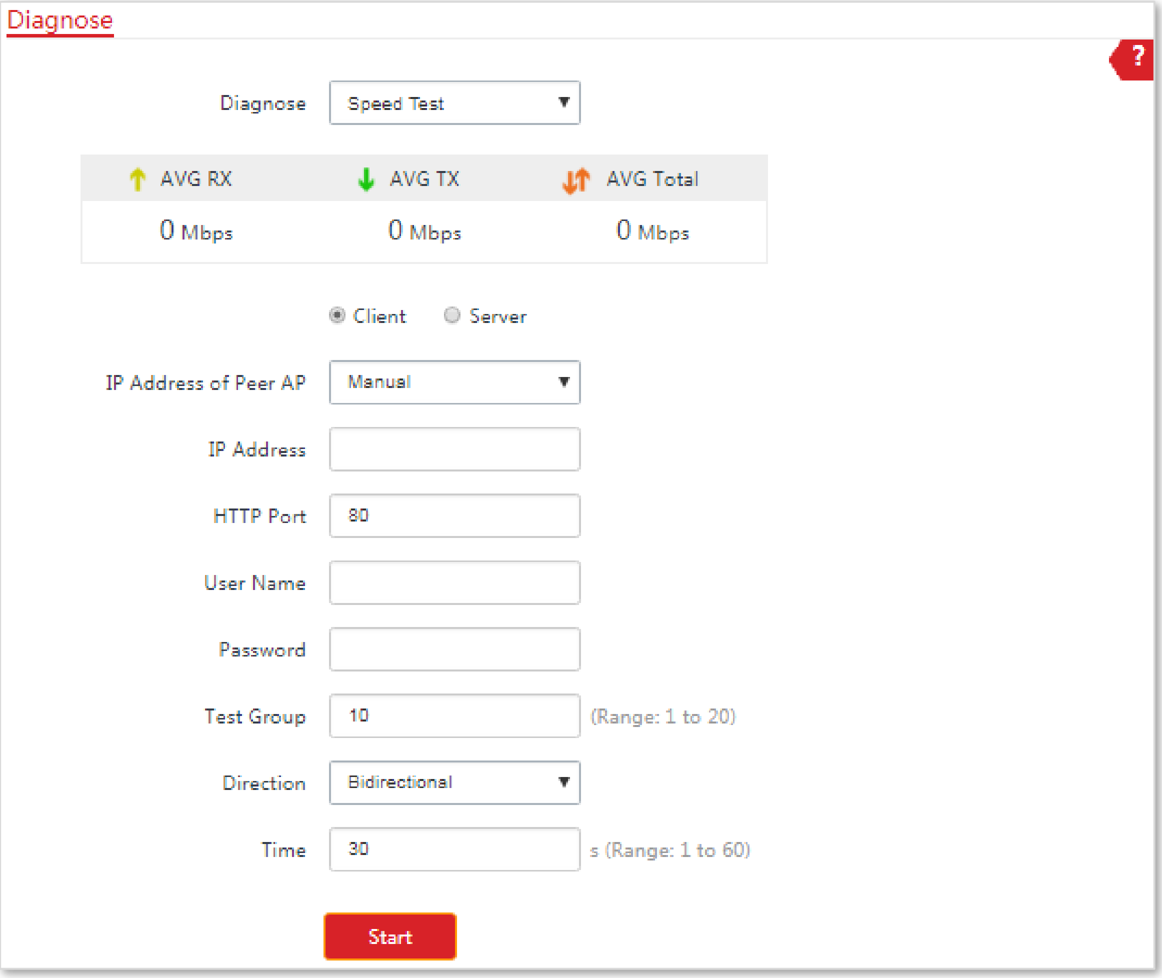
10 Datas/Page 1 data in total

8.2.5 Speed Test

It is used to test the throughput between two IP-COM CPE in the same network. The test requires one of the two devices to be set as a server and the other as a client. The client launches the test request to the server and the server responds to it. The test result displays on the Speed Test page of the client.

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

Set Diagnose to **Speed Test**.



Diagnose

Diagnose: Speed Test

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

● Client ○ Server

IP Address of Peer AP: Manual

IP Address:

HTTP Port: 80

User Name:

Password:

Test Group: 10 (Range: 1 to 20)

Direction: Bidirectional

Time: 30 s (Range: 1 to 60)

Parameters Description

Name	Description
IP Address of Peer AP	It specifies the LAN IP address of peer CPE. You can enter one manually.
IP Address	If the **IP Address of Peer AP** is set to **Manual**, you need to enter the LAN IP address of peer CPE in the box manually.
HTTP Port	It specifies the port number of HTTP service. Default: **80**. You are recommended to keep the default value.
User Name	It specifies the user name of web UI of peer CPE.
Password	It specifies the password of web UI of peer CPE.

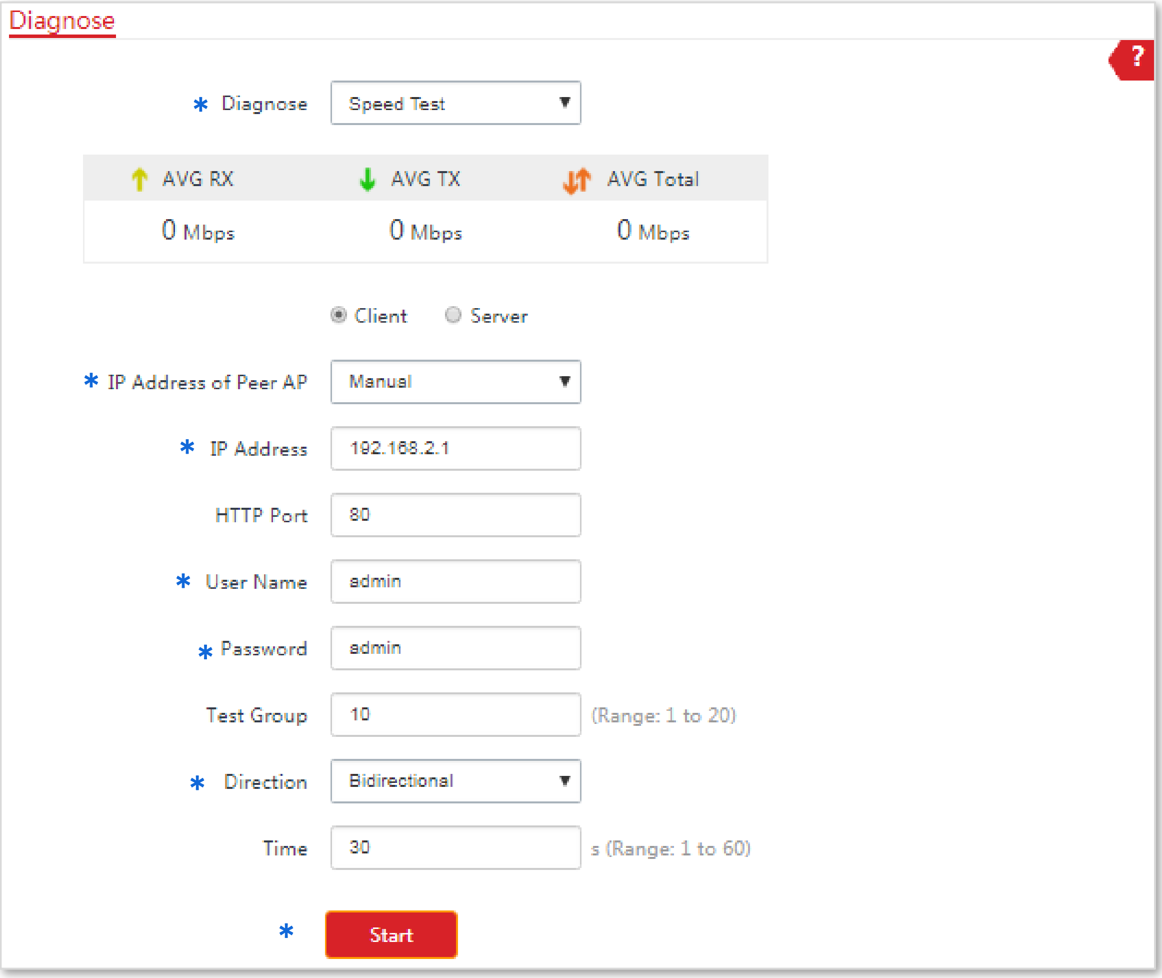
Name	Description
Test Group	It specifies the number of test connection launched by the client. Range: 1 to 20.
Direction	It specifies the test speed direction. – **RX** (Receive): only test the speed that the peer device transmits data to this device. – **TX** (Transit): only test the speed that this device transmits data to peer device. – **Bidirectional**: test the speed that this device transmits data to peer device and the peer device transmits data to this device.
Time	It specifies the period of speed test.
Test Progress	It specifies the process of speed test.
Test Result	It displays the test result. – **AVG RX**: It specifies the average of received speed. – **AVG TX**: It specifies the average of transmitted speed. – **AVG Total**: It specifies the average of the total connection speed.

Examples of Configuring the Speed Test

Assume that CPE1 works in AP mode, and CPE2 works in Client mode and bridges to the WiFi network of CPE1. Then test the wireless speed between them.

Configuration Procedure

1. Log in to the web UI of CPE2.
2. Choose **Advanced** > **Diagnose**.
3. Set **Diagnose** to **Speed Test**.
4. Set **IP Address of Peer AP** to **Manual**.
5. Enter the IP address of CPE1 to the **IP Address** box, which is **192.168.2.1** in this example.
6. Enter the login user name and password of the web UI of CPE1 in the **User name** and **Password** boxes, which are both **admin** in this example.
7. Set **Direction** to **Bidirectional**.
8. Click **Start**.



Diagnose

* Diagnose	Speed Test ▼

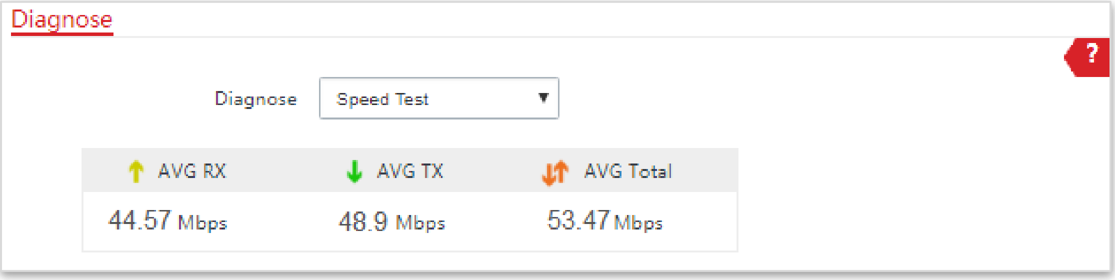
↑ AVG RX	↓ AVG TX	⇅ AVG Total
0 Mbps	0 Mbps	0 Mbps

● 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)

---End

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



Diagnose

Diagnose	Speed Test ▼

↑ AVG RX	↓ AVG TX	⇅ AVG Total
44.57 Mbps	48.9 Mbps	53.47 Mbps

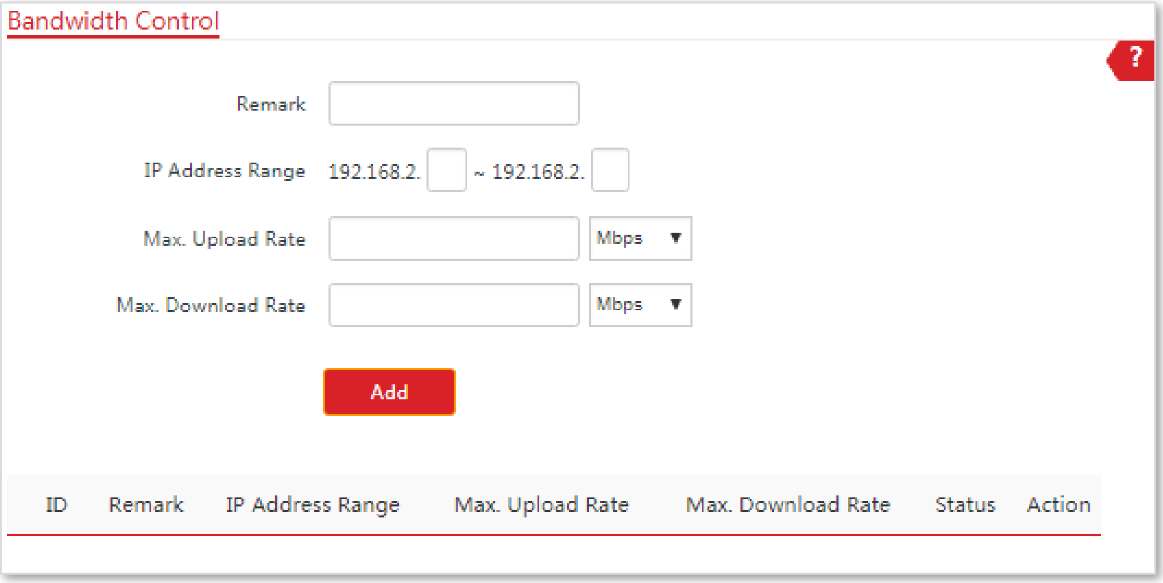
8.3 Bandwidth Control (Only for CPE9)

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

8.3.1 Overview

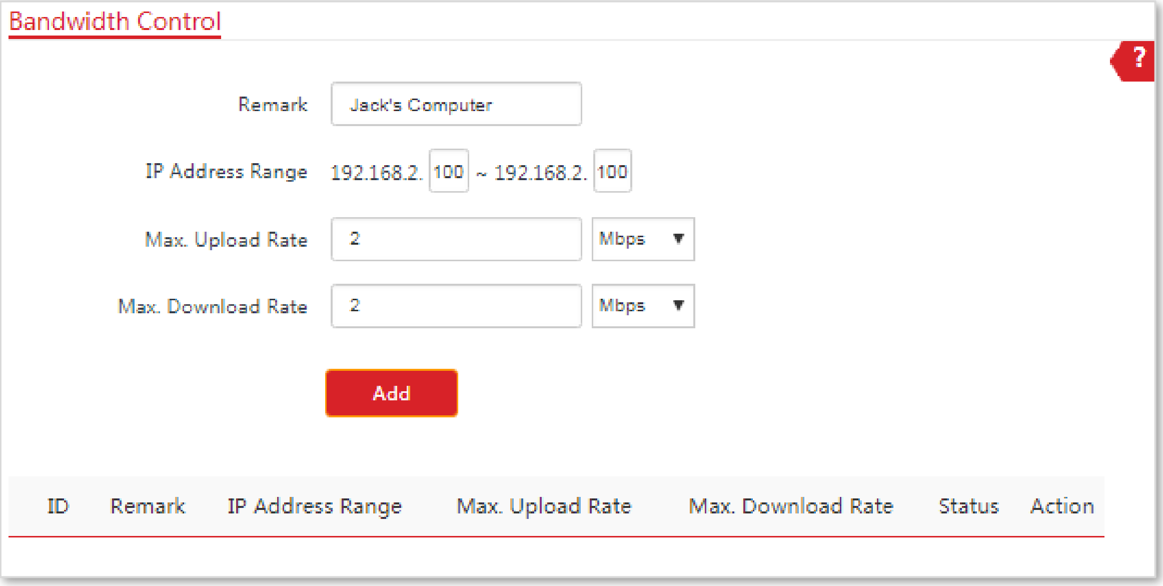
If multiple devices access the internet through the CPE, bandwidth control is recommended, so that high-speed file download by a device does not reduce the internet access speed of the other devices.

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



Configuring Bandwidth Control

1. Choose **Advanced** > **Bandwidth Control**.
2. Set up the related parameters.
3. Click **Add**.



Bandwidth Control

Remark: Jack's Computer

IP Address Range: 192.168.2. 100 ~ 192.168.2. 100

Max. Upload Rate: 2 Mbps

Max. Download Rate: 2 Mbps

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

---End

Parameters Description

Name	Description
Remark	It specifies the additional information of the bandwidth control rule.
IP Address Range	It specifies the IP addresses or range of devices that this rule applies to.
Max. Upload Rate	It specifies the maximum upload/download rate of the each device whose IP address is within the IP Address Range.
Max. Download Rate	
Status	It specifies the current status of the rule. You can enable or disable it as required.
Action	Click 🗑 to delete the rule.

8.3.2 Examples of Configuring Bandwidth Control

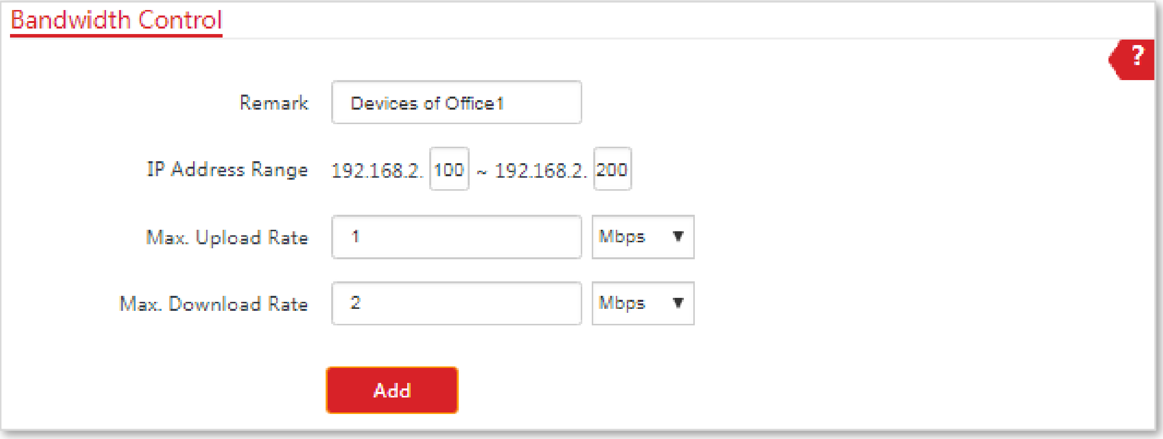
Networking Requirement

The CPE is used in a company to deploy its network, and the device is set to Router mode. To ensure that every device can access the internet smoothly, you want to specify a maximum upload/download for each device.

Assumption: The maximum upload rate of each device connected to the WiFi network of the CPE is **1 Mbps**, and download rate is **2 Mbps**. And the IP address range of the devices connected to the WiFi network is **192.168.2.100** to **192.168.2.200**.

Configuration Procedure

1. Choose **Advanced** > **Bandwidth Control**.
2. Enter a remark, such as **Devices of Office1**.
3. Specify an IP address range, which are **100** and **200** in this example.
4. Specify the maximum upload rate and download rate respectively, which are **1** and **2** in this example.
5. Click **Add**.



Bandwidth Control

Remark: Devices of Office1

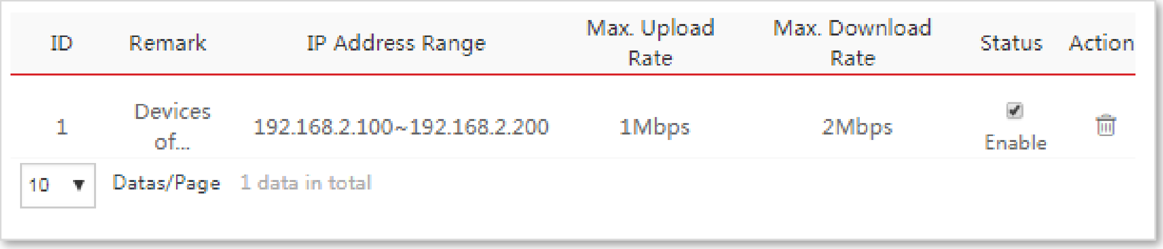
IP Address Range: 192.168.2. 100 ~ 192.168.2. 200

Max. Upload Rate: 1 Mbps ▼

Max. Download Rate: 2 Mbps ▼

---End

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



ID	Remark	IP Address Range	Max. Upload Rate	Max. Download Rate	Status	Action
1	Devices of...	192.168.2.100~192.168.2.200	1Mbps	2Mbps	☑ Enable	🗑

10 ▼ Datas/Page 1 data in total

Verification

A device whose IP address is within the range of 192.168.2.100 to 192.168.2.200, its maximum upload rate is 1 Mbps and its maximum download rate is 2 Mbps.

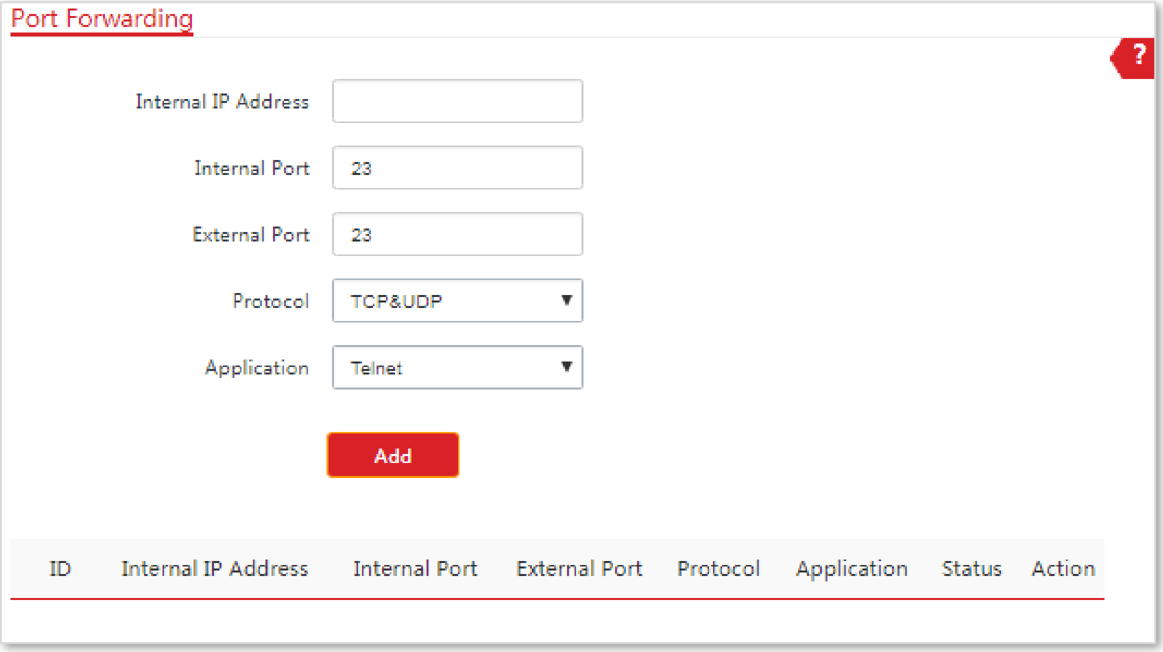
8.4 Port Forwarding (Only for CPE9)

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

8.4.1 Overview

If computers are connected to the router to form a LAN and access the internet through the router, internet users cannot access the hosts on the LAN. Therefore, the servers, such as web servers, email servers, and FTP servers, on the LAN are inaccessible to internet users. To enable internet users to access a LAN server, enable the port forwarding function of the router, and map one service port to the IP address of the LAN server. This enables the router to forward the requests arriving at the port from the internet to the LAN server, and avoid the attacks from the WAN.

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



Port Forwarding

Internal IP Address

Internal Port: 23

External Port: 23

Protocol: TCP&UDP

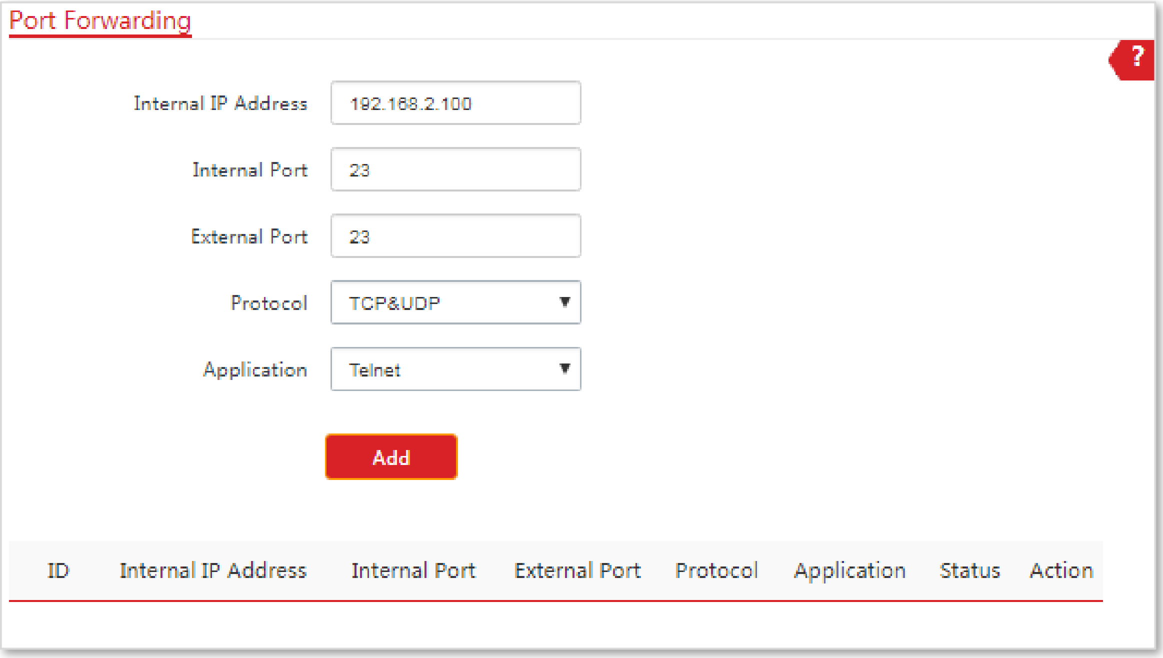
Application: Telnet

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

8.4.2 Configuring Port Forwarding

Configuration Procedure

1. Choose **Advanced** > **Port Forwarding**.
2. Set the related parameters.
3. Click **Add**.



Port Forwarding

Internal IP Address: 192.168.2.100

Internal Port: 23

External Port: 23

Protocol: TCP&UDP

Application: Telnet

---End

Parameters Description

Name	Description
Internal IP Address	It specifies the IP address of the host which establishes a server in LAN.
Internal Port	It specifies the service port of the server in LAN. A single port is supported.
External Port	It specifies the ports enabled for WAN users by this device.
Protocol	It specifies the protocol type of the selected applications. Select TCP&UDP when you are not sure.
Application	It specifies the application services established in LAN.
Action	Click 🗑 to delete the rule.

8.4.3 Example of Configuring Port Forwarding

Networking Requirement

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

Requirement: The employees of the company who are on business can visit the resources on the web server in LAN over the internet.

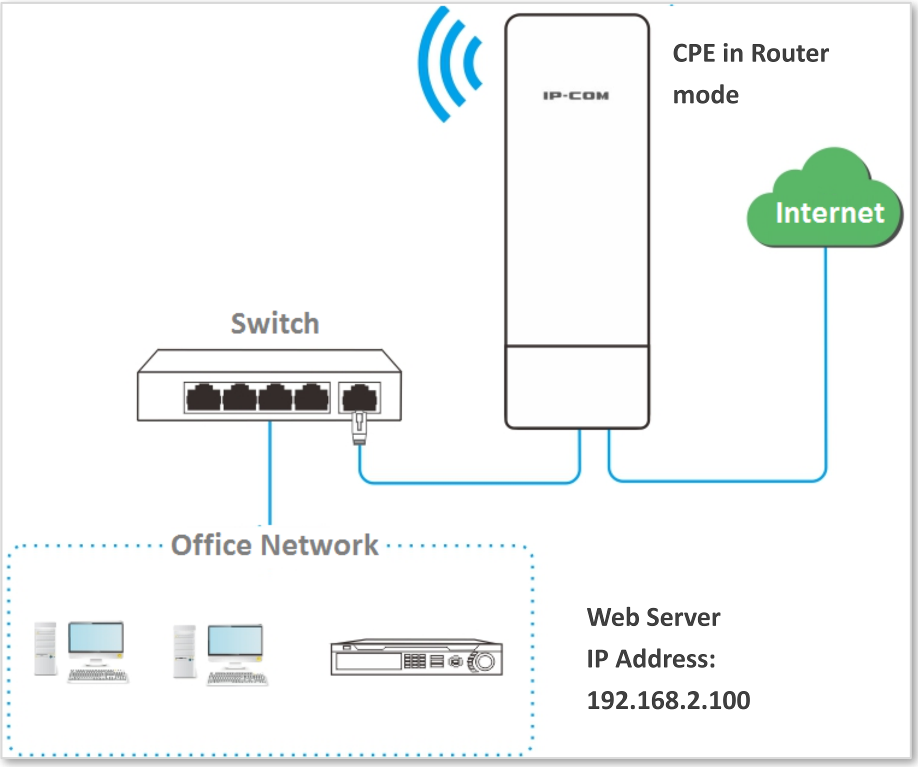
You are recommended to use port forwarding function to solve the problem.

Assumption:

- IP Address of the web server: 192.168.2.100

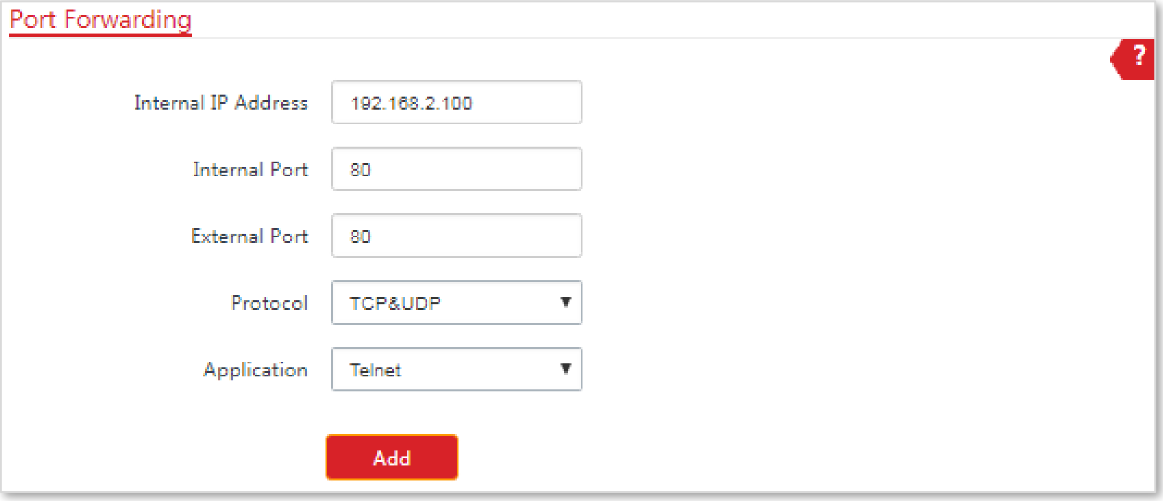
- Service port (internal port) of the web server in LAN:80
- External port that this device enables for internet devices: 80
- WAN IP Address of the CPE: 202.105.11.22

Network Topology



Configuration Procedure

1. Log in to the web UI of the CPE which works in **Router** mode.
2. Choose **Advanced** > **Port Forwarding**.
3. Enter the IP address of the web server in the **Internal IP Address** box, which is **192.168.2.100** in this example.
4. Enter **80** and **80** on the **Internal Port** and **External Port** boxes respectively.
5. Select **TCP&UDP** from the dropdown list of **Protocol**.
6. Select **HTTP** from the dropdown list of **Application**.
7. Click **Add**.

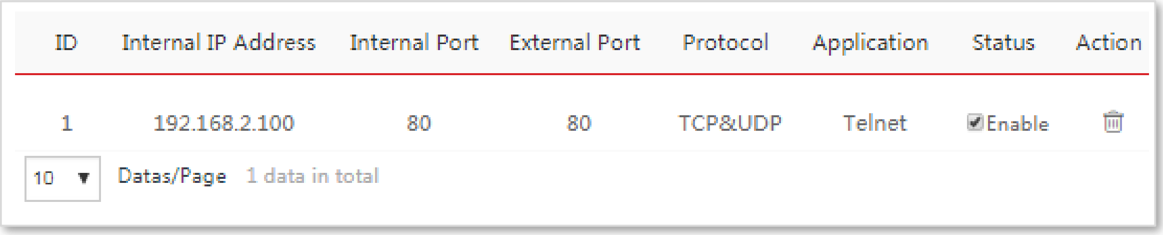


Port Forwarding

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

---End

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



ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	80	80	TCP&UDP	Telnet	☑Enable	🗑

10 ▼ Datas/Page 1 data in total

Verification

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

Tip

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

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

8.5 MAC Filter (Only for CPE9)

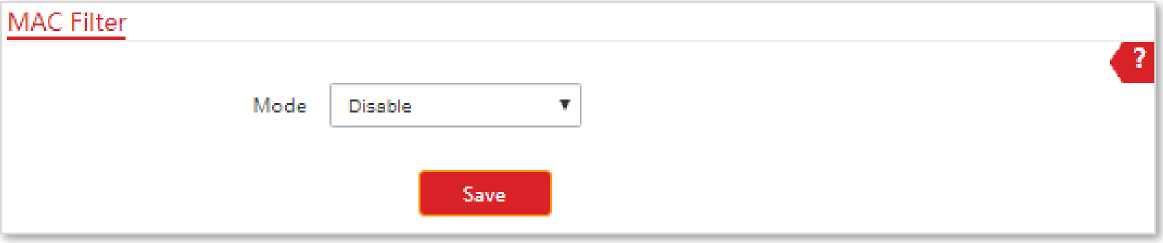
This function is available only when the CPE works in **WISP** or **Router** mode.

8.5.1 Overview

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

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

The function is disabled by default.



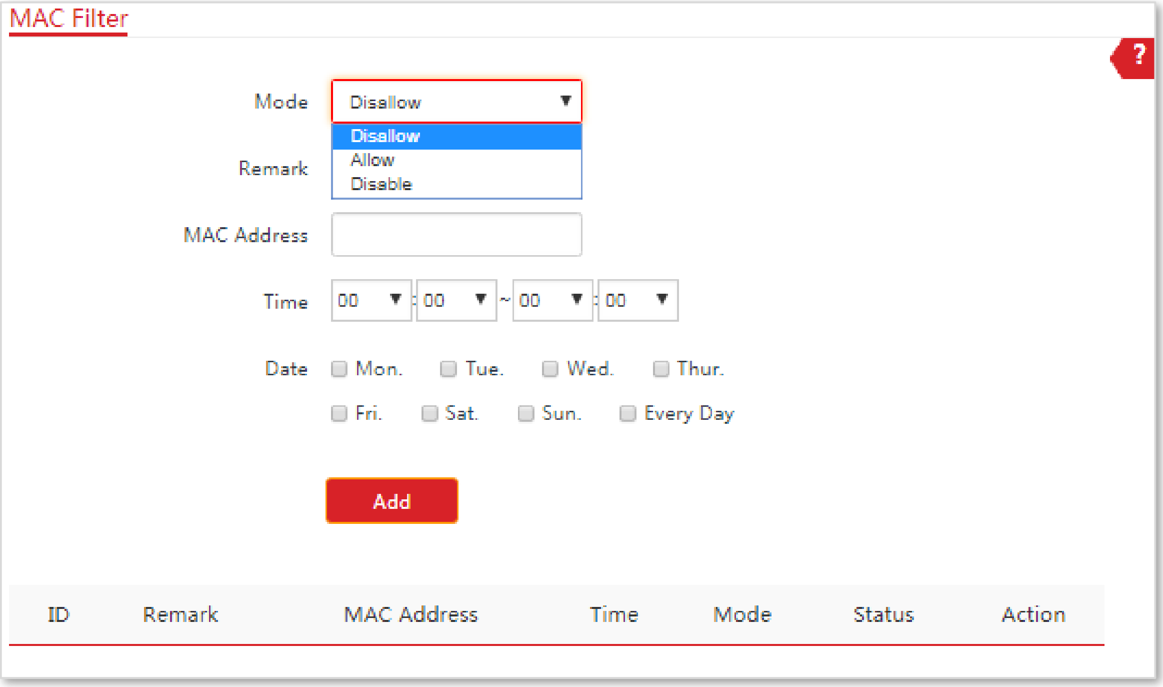
MAC Filter

Mode: Disable

8.5.2 Configuring MAC Filter

Configuration Procedure

1. Choose **Advanced** > **MAC Filter**.
2. Select a MAC filter mode, Disallow or Allow.
3. Enter a remark for the rule, such as somebody's device.
4. Specify a period at which the rule takes effect.
5. Tick the dates on which the rule takes effect.
6. Click **Add**.


MAC Filter

Mode: Disallow ▼

Disallow
Allow
Disable

Remark

MAC Address

Time: 00 ▼ : 00 ▼ ~ 00 ▼ : 00 ▼

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

Add

ID	Remark	MAC Address	Time	Mode	Status	Action

---End

Parameters Description

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

8.5.3 Examples of Configuring MAC Filter

Network Topology

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

Requirements: Only allow the procurement staff to access the internet during working hours (9:00 to 17:00, Monday to Friday).

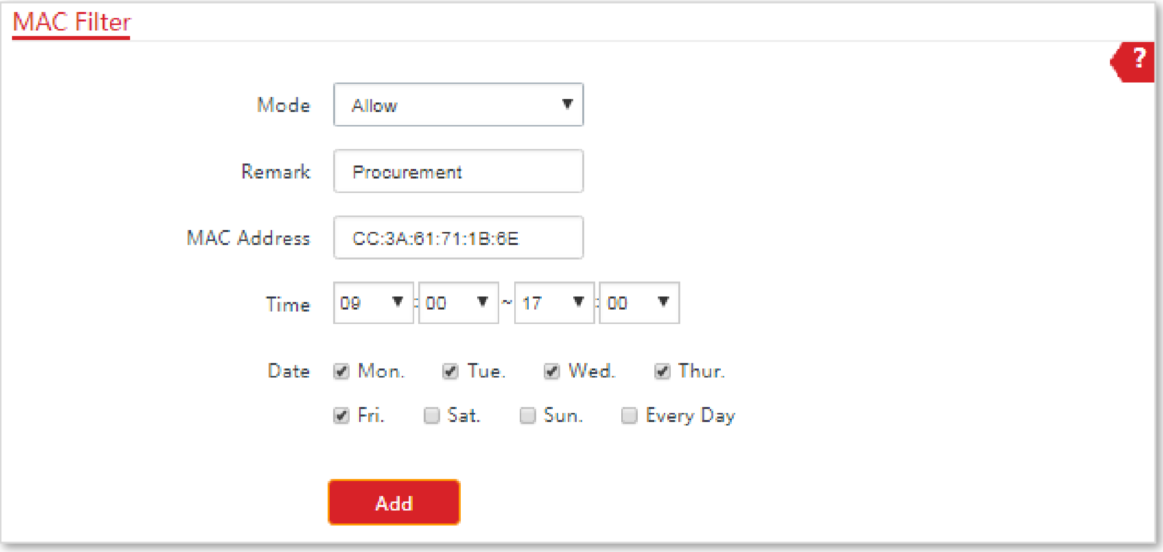
You are recommended to use the MAC Filter function to solve the problem.

Assumption:

The MAC address of the procurement staff's device is **CC:3A:61:71:1B:6E**.

Configuration Procedure

1. Log in to the web UI of the CPE which is working in Router mode.
2. Choose **Advanced** > **MAC Filter**.
3. Select a mode, which is **Allow** in this example.
4. Enter a remark in the **Remark** box, which is **Procurement** in this example.
5. Enter the MAC address of the device, which is **CC:3A:61:71:1B:6E** in this example.
6. Specify a period, which is **9:00** to **17:00** in this example.
7. Tick the dates, which are **Monday to Friday** in this example.
8. Click **Add**.



MAC Filter

Mode: Allow

Remark: Procurement

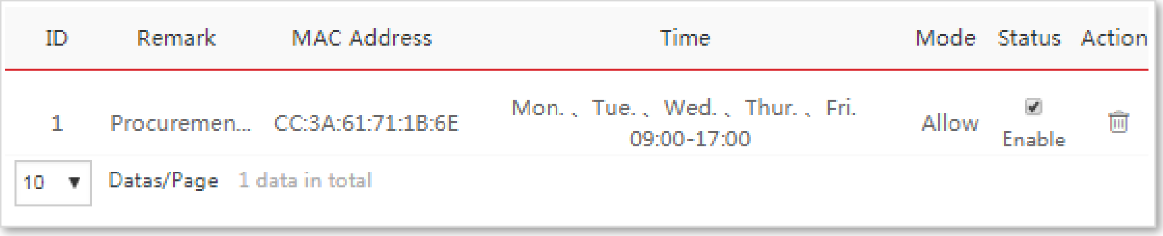
MAC Address: CC:3A:61:71:1B:6E

Time: 09 : 00 ~ 17 : 00

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

---End

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



ID	Remark	MAC Address	Time	Mode	Status	Action
1	Procuremen...	CC:3A:61:71:1B:6E	Mon.、Tue.、Wed.、Thur.、Fri. 09:00-17:00	Allow	☑ Enable	🗑

10 ▼ Datas/Page 1 data in total

8.5.4 Verification

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

8.6 Network Service

8.6.1 DDNS

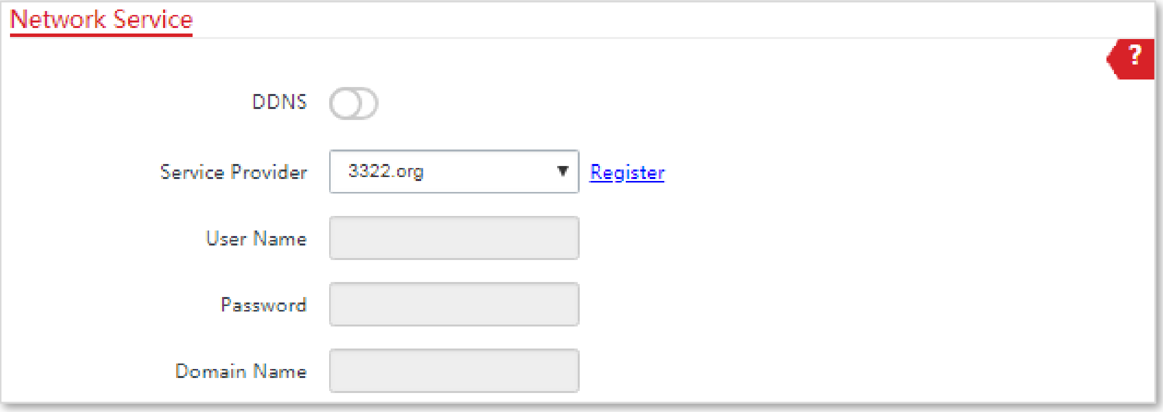
This function is available only when the CPE works in **WISP** or **Router** mode.

Overview

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

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

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



Network Service

DDNS ○

Service Provider 3322.org

User Name

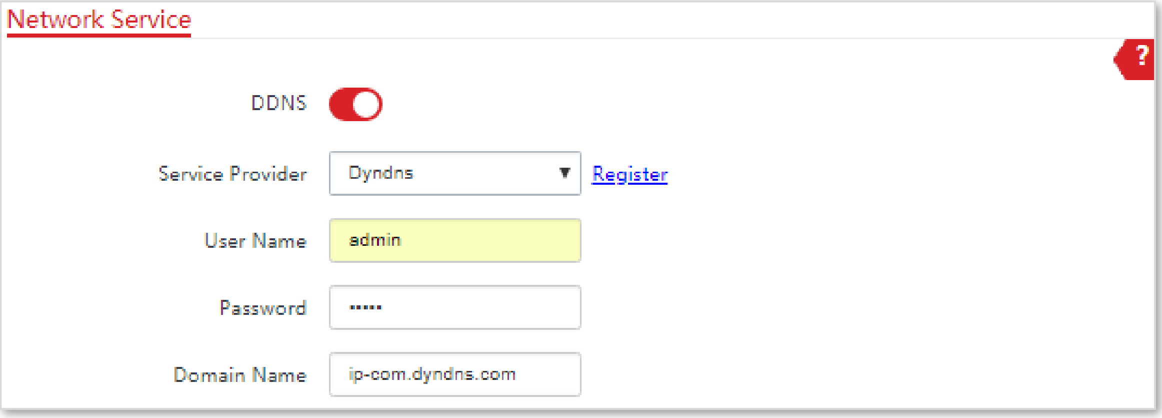
Password

Domain Name

Configuring DDNS

Configuration Procedure

1. Choose **Advanced** > **Network Service**.
2. Enable the **DDNS** function.
3. Select a dynamic DNS provider from the dropdown list.
4. Enter the user name, password, and domain name you registered with DDNS service provider.
5. Click **Save** on the bottom of this page.



Network Service

DDNS ●

Service Provider: Dyndns ▼ Register

User Name: admin

Password: ·····

Domain Name: ip-com.dyndns.com

---End

Parameters Description

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

Examples of Configuring DDNS

Networking Requirement

The CPE is used in a company to deploy its network, and it is set to Router mode. The WAN IP address of the CPE is dynamic.

Requirement: The administrator on business can visit the resources on web server in LAN.

You are recommended to use the DDNS and port forwarding functions to solve the problem.

Assumption:

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

IP Address: 192.168.2.100

Service Port of the Web Server: 80

The registered domain name information is shown as follows:

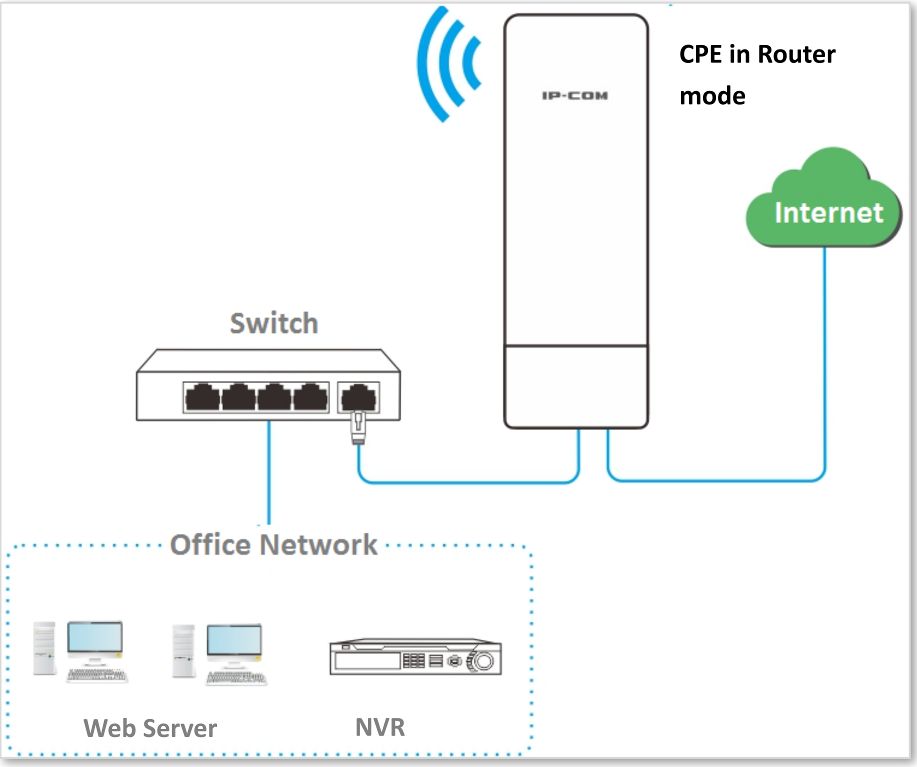
Service Provider: Dyndns

User Name: ip-com

Password: ip-com

Domain Name: ip-com.dyndns.com

Network Topology



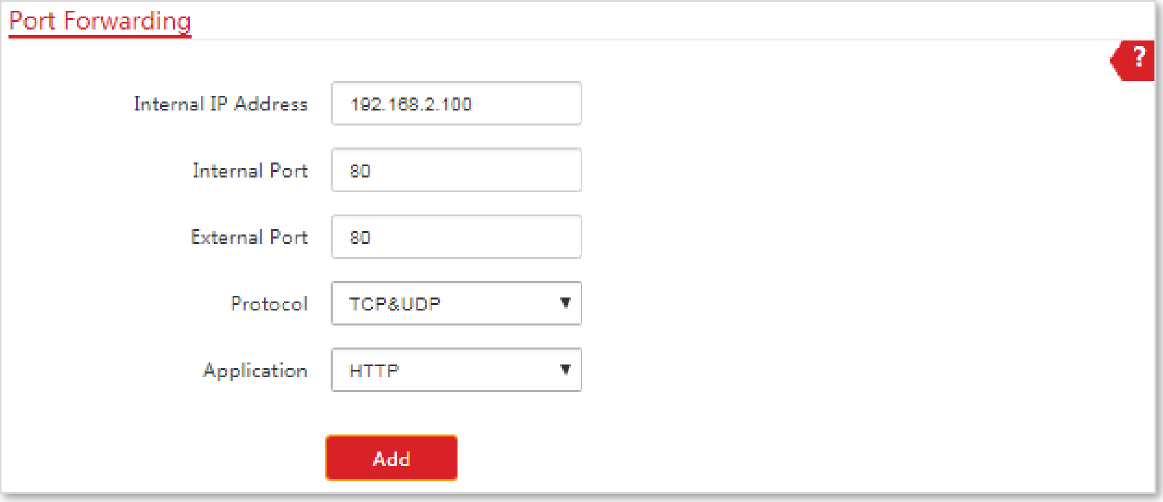
Configuration Procedure

1. Set up the DDNS function.
   (1) Log in to the web UI of the CPE which works in Router mode.
   (2) Choose **Advanced** > **Network Service**.
   (3) Enable the **DDNS** function.
   (4) Select a service provider, which is **Dyndns** in this example.
   (5) Enter the user name and password you registered, which are **ip-com** and **ip-com** in this example.
   (6) Enter the domain name you registered, which is **ip-com.dyndns.com**.
   (7) Click **Save** on the bottom of this page.
2. Set up the port forwarding function.
   (1) Choose Advanced > Port Forwarding.
   (2) Enter the IP address of the web server, which is **192.168.2.100** in this example.

(3) Select an application, which is **HTTP** in this example.

(4) Select the protocol of the service. **TCP&UDP** is recommended if you are not sure.

(5) Click **Add**.

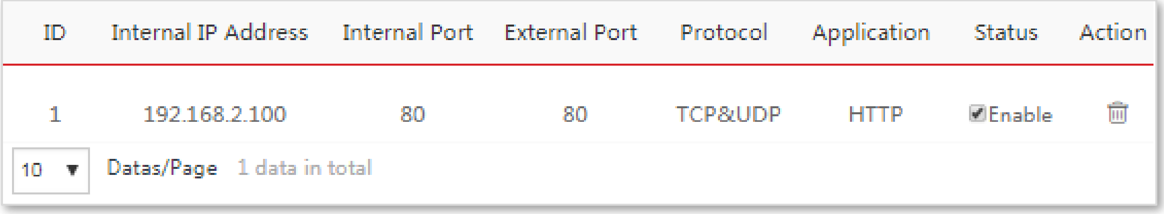


Port Forwarding

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

---End

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



ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	80	80	TCP&UDP	HTTP	☑Enable	🗑

10 ▼ Datas/Page 1 data in total

Verification

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

Tip

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

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

8.6.2 Remote Web Management

Overview

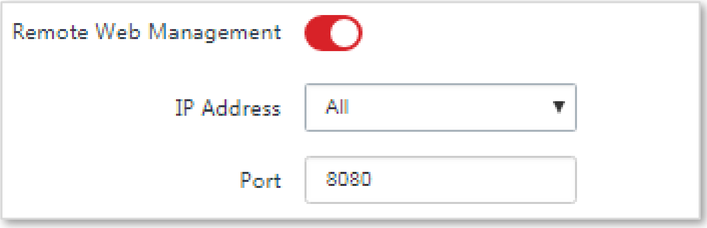
Generally, only the devices connected to the LAN ports of the device can access its web UI.

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

Configuring Remote Web Management

Configuration procedure

1. Log in to the web UI of the CPE.
2. Choose **Advanced** > **Network Service**.
3. Enter the IP address of a device which is allowed to access the web UI of the CPE remotely, or select **All** to allow any device on WAN to access.
4. Enter a port number.
5. Click **Save** on the bottom of this page.



Remote Web Management

IP Address: All

Port: 8080

---End

Parameters Description

Name	Description
Remote Web Management	It specifies whether to enable the remote web management function.
IP Address	It specifies the IP address of a device which is allowed to access the web UI of the CPE. – **All**: It indicates that any computer in WAN can manage this device remotely. For security, it is not recommended. – **Manual**: It indicates that only the device with specified IP address can manage this device remotely. If this device belongs to a LAN, the gateway address (a public IP address) of the device should be entered.
Port	It specifies the port number used for remote management of device. Default: 8080. You can change it if necessary. Port s1 to 1024 have been used by well-known services. To avoid port conflict, you can set the port number to one between 1025 and 65535. Then you can access the device from WAN by

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

Examples of Configuring Remote Web Management

Networking Requirement

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

Requirement: The administrator needs to maintenance the network when he is on business. So he needs to access the device’s web UI on WAN.

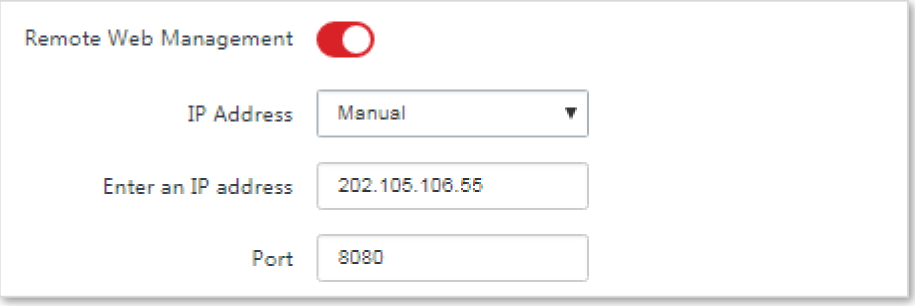
You are recommended to use the remote web management function to solve the problem.

Assumption:

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

Configuration Procedure

1. Log in to the web UI of the CPE.
2. Choose **Advanced** > **Network Service**.
3. Enable the **Remote Web Management** function.
4. Set **IP Address** to **Manual**.
5. Enter the IP address of the computer which is allowed to access the CPE on WAN, which is **202.105.106.55** in this example.
6. Enter the port number, which is **8080** in this example.
7. Click **Save** in the bottom of this page.



Remote Web Management

IP Address: Manual

Enter an IP address: 202.105.106.55

Port: 8080

---End

Verification

On the computer with the IP address of **202.105.106.55**, start a browser and visit **http://202.105.106.55:8080**. Then you can log in to the web UI of the CPE and configure the settings.

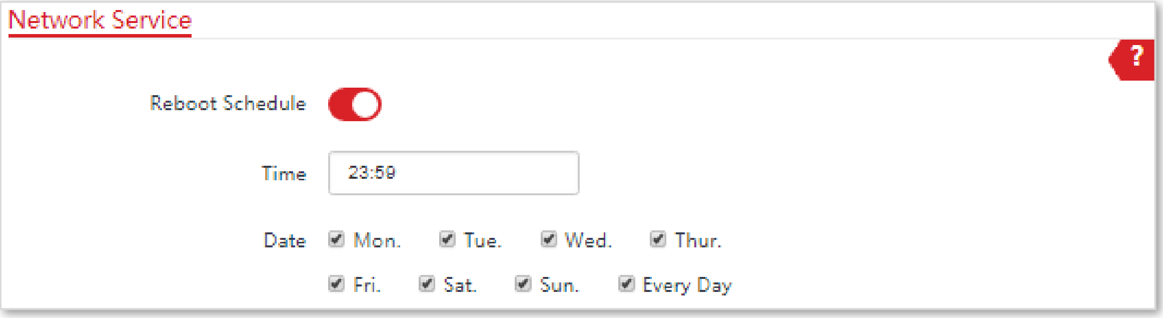
8.6.3 Reboot Schedule

Overview

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

Configuration Procedure

1. Choose **Advanced** > **Network Service**.
2. Enable the **Reboot Schedule** function.
3. Specify a time at which the device reboots.
4. Specify the dates on which the device reboots.
5. Click **Save** on the bottom of this page.



Network Service

Reboot Schedule: ●

Time: 23:59

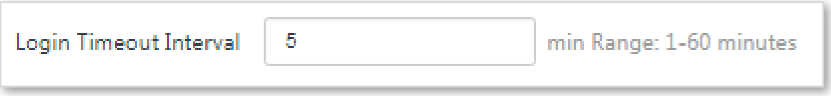
Date: ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thur.
☑ Fri. ☑ Sat. ☑ Sun. ☑ Every Day

---End

8.6.4 Login Timeout Interval

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

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



Login Timeout Interval: 5 min Range: 1-60 minutes

8.6.5 SNMP Agent

Overview

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

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

SNMP Management Framework

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

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

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

Basic SNMP Operations

The CPE allows the following basic SNMP operations:

- Get: An SNMP manager performs this operation to query the SNMP agent of the CPE 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 CPE.

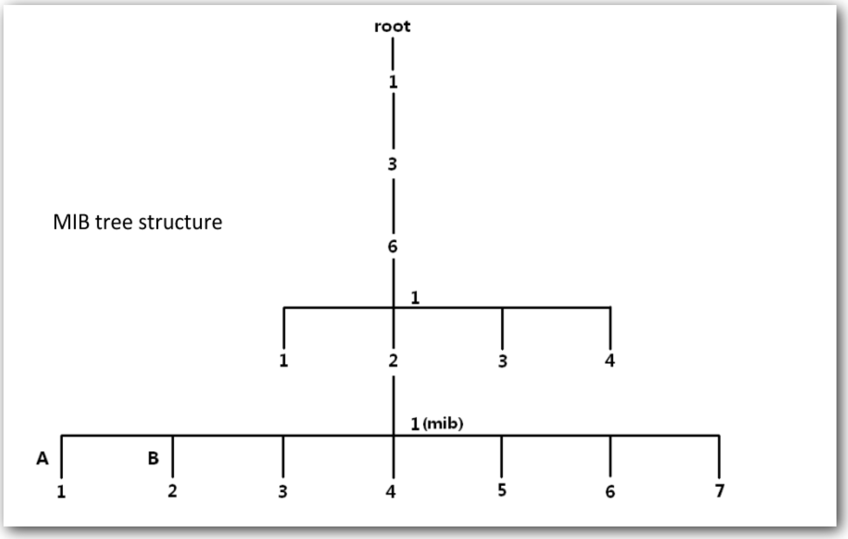
SNMP Protocol Version

The CPE is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. Community name is used to define the relationship between an SNMP agent and an SNMP manager. If the community name contained in an SNMP packet is rejected by a device, the packet is discarded. A community name functions as a password to control SNMP agent access attempts of SNMP managers.

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

MIB Introduction

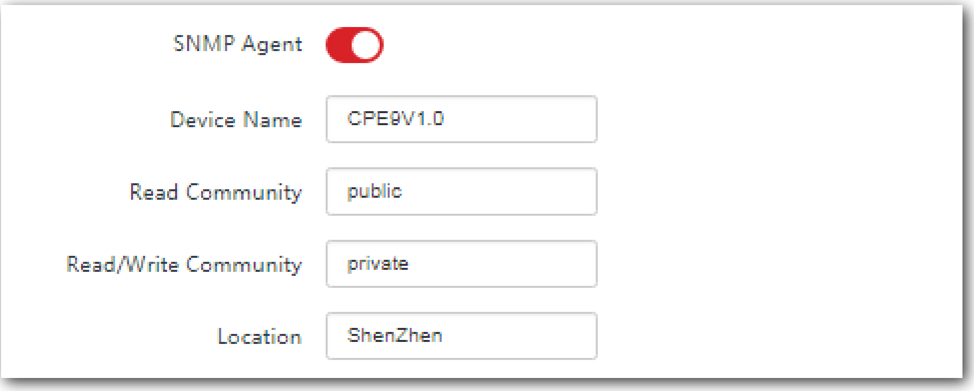
An MIB adopts a tree structure. The nodes of the tree indicate managed objects. A path consisting of digits and starting from the root can be used to uniquely identify a node. This path is calling an object identifier (OID).The following figure shows the structure of an MIB. In the figure, the OID of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



Configuring the SNMP Function

Configuration Procedure

1. Choose **Advanced** > **Network Service**.
2. Enable the **SNMP Agent** function.
3. Set the related SNMP parameters.
4. Click **Save** on the bottom of this page.



SNMP Agent ●

Device Name: CPE9V1.0

Read Community: public

Read/Write Community: private

Location: ShenZhen

---End

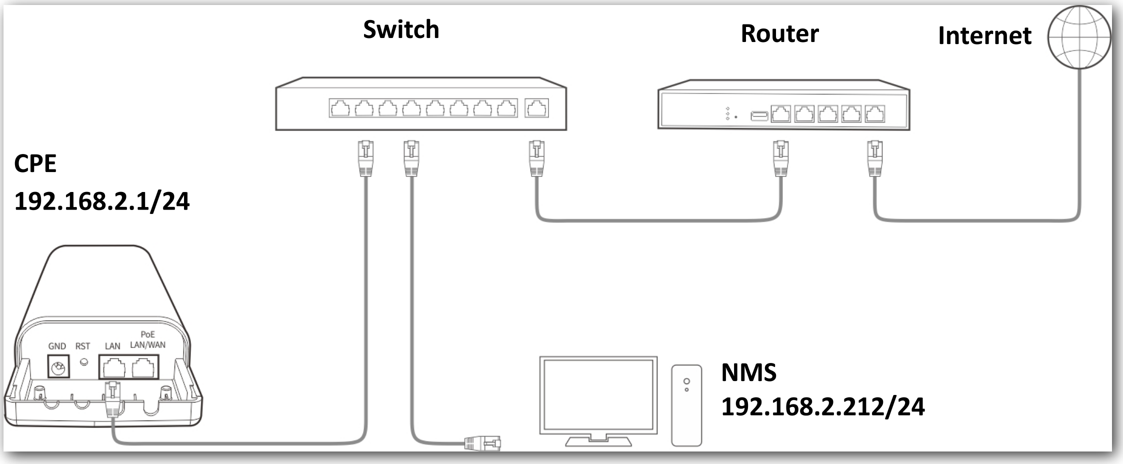
Parameters Description

Name	Description
SNMP Agent	It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled. An SNMP manager and the SNMP agent can communicate with each other only if their SNMP versions are the same. Currently, the SNMP agent function of the CPE supports SNMP V1 and SNMP V2C.
Device Name	It specifies the device name of the CPE. The default device name is the model and version number of the CPE. For example, the default name of this device is CPE9V2.0 Tip It is recommended that you change the CPE name so that you can easily identify the CPE when managing the CPE using SNMP.
Read Community	It specifies the read password shared between SNMP managers and this SNMP agent. The default password is public. The SNMP agent function of the CPE allows an SNMP manager to use the password to read variables in the MIB of the CPE.
Read/Write Community	It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is private. The SNMP agent function of the CPE allows an SNMP manager to use the password to read/write variables in the MIB of the CPE.
Location	It specifies the location where the AP is used. You can change the location as required.

Example of Configuring the SNMP Function

Networking Requirement

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



Configuration Procedure

1. Set up the CPE.

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

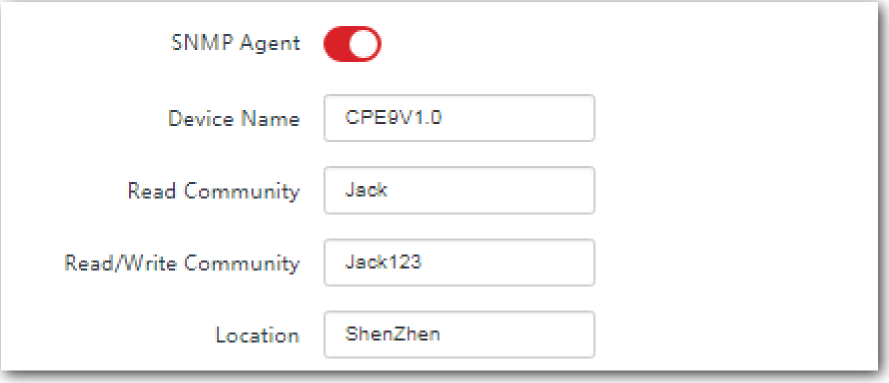
(1) Choose **Advanced** > **Network Service**.

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

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

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

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



SNMP Agent: on

Device Name: CPE9V1.0

Read Community: Jack

Read/Write Community: Jack123

Location: ShenZhen

2. Set up the NMS.

On an NMS that uses SNMP V1 or SNMP V2C, set the read community to **Jack** and read/write community to

Jack123.For details about how to configure the NMS, refer to the configuration guide for the NMS.

---End

Verification

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

8.6.6 Ping Watch Dog

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

Configuring Ping Watch Dog

Configuration Procedure

1. Choose **Advanced** > **Network Service**.
2. Enable the **Ping Watch Dog** function.
3. Set the related parameters.
4. Click **Save** on the bottom of this page.

---End

Parameters Description

Name	Description
Ping Watch Dog	It specifies whether to enable the Ping Watch Dog function.
IP Address	It specifies the target IP address that the device pings.
Ping Interval	It specifies the interval at which the device transmits packets to ping the target IP address.
Ping Startup Delay	It specifies the interval at which the device enables the Ping Watch Dog function after the device reboots. You can set this parameter to keep the device from rebooting repeatedly on account that the system triggers Ping Watch Dog during rebooting while users cannot log in to the web UI of the device to change the settings.
Threshold of Lost Packets	It specifies the threshold of lost packet that triggers reboot. Range: 1 to 65535, default: 3. If N is set, the device will reboot automatically when it sends N Ping packets to target IP address/domain name, and does not receive response.

8.6.7 DMZ Host

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

Overview

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

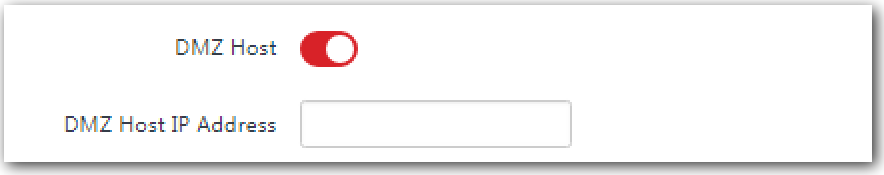
Note

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

Configuring DMZ Host

Configuration Procedure

1. Choose **Advanced** > **Network Service**.
2. Enable the **DMZ Host** function.
3. Enter the IP address of the device to be set to DMZ host.
4. Click **Save** on the bottom of this page.



---End

Examples of Configuring DMZ Host

Networking Requirement

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

Requirement: The administrator on business can visit the resources on web server in LAN.

You can use DMZ Host function to solve the problem.

Assumption:

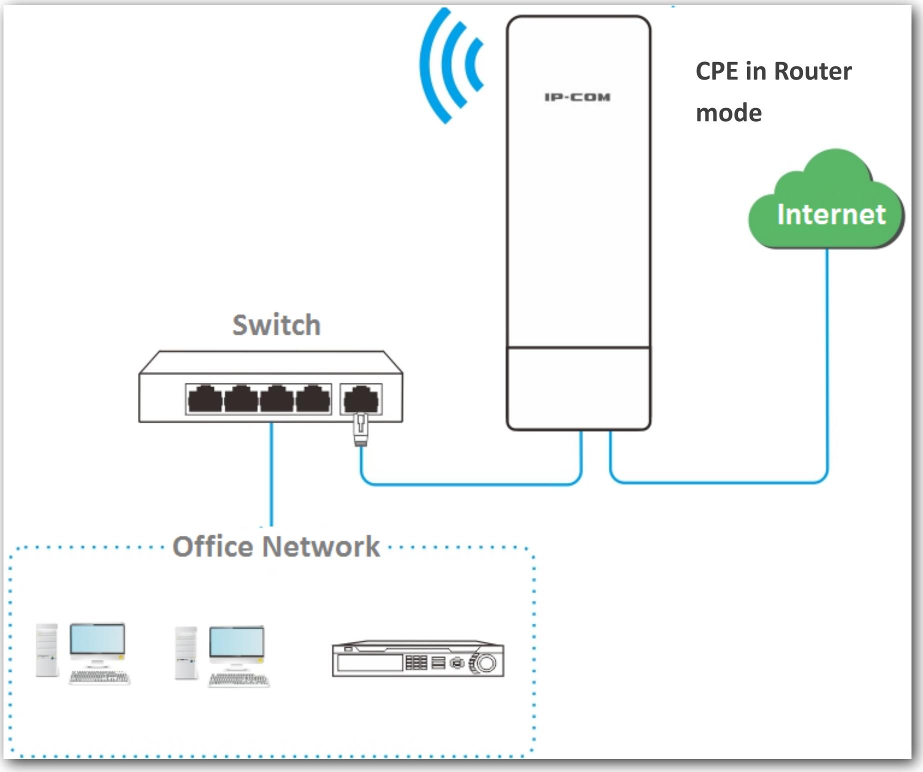
The WAN IP address of the CPE is **202.105.106.55**.

The information of the internal web server is shown as follows:

IP Address: 192.168.2.100

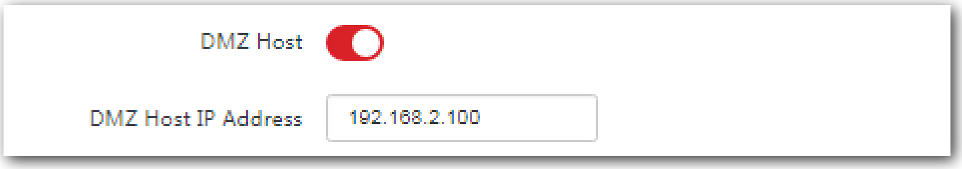
Service Port of the Web Server: 80

Network Topology



Configuration Procedure

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


DMZ Host ●

DMZ Host IP Address 192.168.2.100

---End

Verification

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

http://202.105.106.55:80.

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

Tip

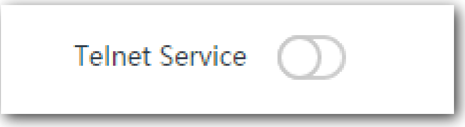
If internet users still cannot visit the web server in LAN after the configuration, try the following solutions:

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

8.6.8 Telnet Service

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

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

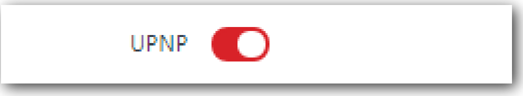


Telnet Service ○

8.6.9 UPnP

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

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

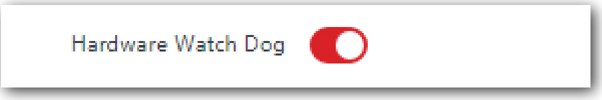


UPNP ●

8.6.10 Hardware Watch Dog (Only for CPE9)

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

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



Hardware Watch Dog ●

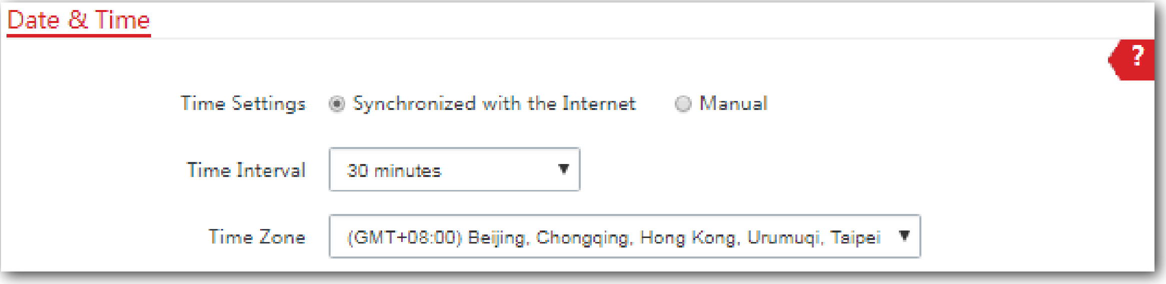
9 Tools

9.1 Date & Time

This module enables you to set the system time of the CPE.

Ensure that the system time of the CPE is correct, so that logs can be recorded correctly and the reboot schedule can be executed correctly.

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



Date & Time

Time Settings ● Synchronized with the Internet ○ Manual

Time Interval 30 minutes

Time Zone (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei

The CPE allows you to set the system time by synchronizing the time with the internet or manually setting the time. By default, it is configured to synchronize the system time with the internet.

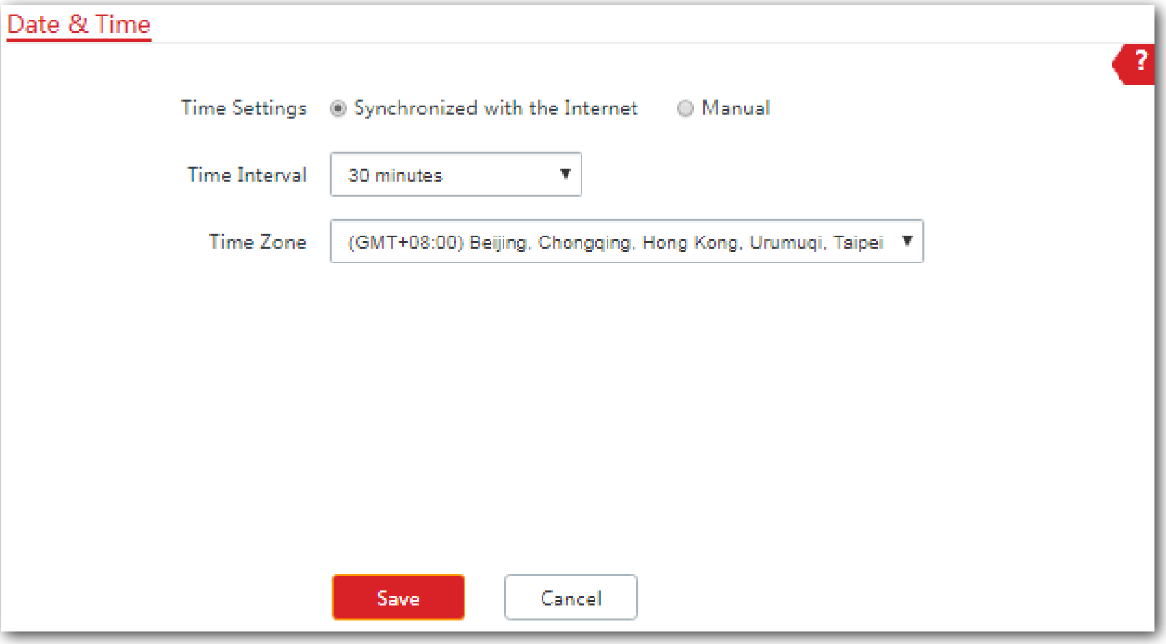
9.1.1 Synchronized with the Internet

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

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

Configuration Procedure

1. Choose **Tools** > **Date & Time**.
2. Set **Time settings** to **Synchronized with the Internet**.
3. Specify a time interval. The default value **30 minutes** is recommended.
4. Set **Time Zone** to your time zone.
5. Click **Save**.



Date & Time

Time Settings ● Synchronized with the Internet ○ Manual

Time Interval 30 minutes

Time Zone (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei

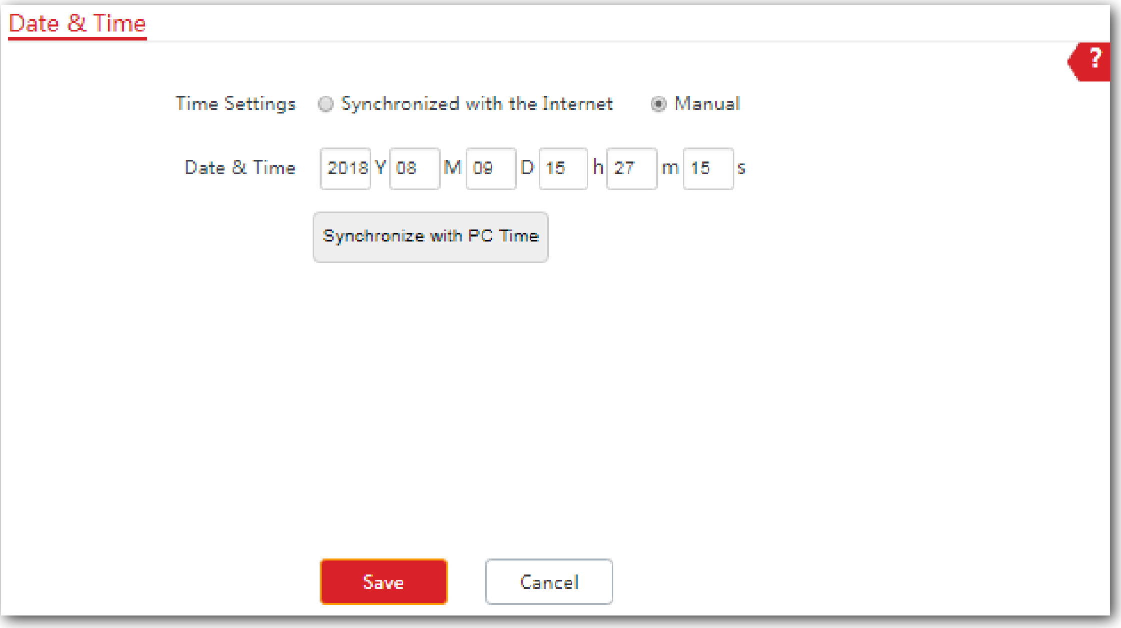
---End

9.1.2 Manual

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

Configuration Procedure

1. Choose **Tools** > **Date & Time**.
2. Set the **Time Settings** to **Manual**.
3. Enter a correct date and time, or click **Synchronize with PC Time** to synchronize the system time of the CPE with the system time (ensure that it is correct) of the computer being used to manage the CPE.
4. Click **Save**.



Date & Time

Time Settings ○ Synchronized with the Internet ● Manual

Date & Time 2018 Y 08 M 09 D 15 h 27 m 15 s

---End

9.2 Maintenance

9.2.1 Reboot Device

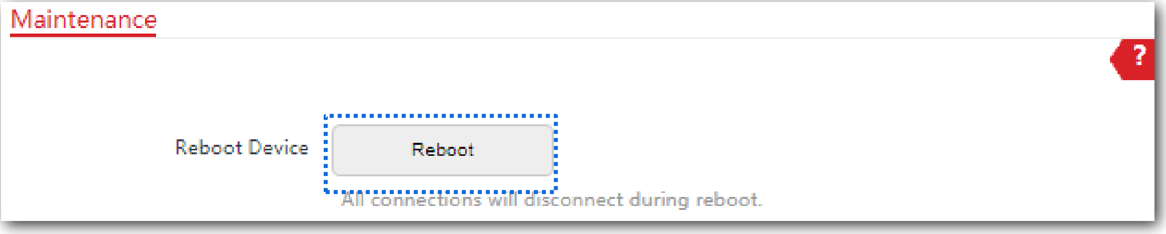
If a setting does not take effect or the CPE works improperly, you can try rebooting the CPE to resolve the problem.

Tip

When the CPE reboots, the current connections disconnect. Perform this operation when the CPE does not work busy.

Configuration Procedure

1. Choose **Tools** > **Maintenance**.
2. Click **Reboot**.

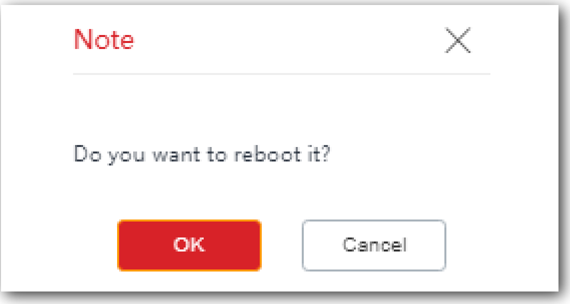


Maintenance

Reboot Device

All connections will disconnect during reboot.

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



---End

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

9.2.2 Reset to Factory Settings

If you cannot locate a fault of the CPE or forget the login password of the web UI of the CPE, you can reset the CPE to restore its factory settings and then configure it again.

Note

– When the factory settings are restored, the configuration of the CPE is lost. Therefore, you need to reconfigure the CPE to connect to the internet. Restore the factory settings of the CPE only when necessary.

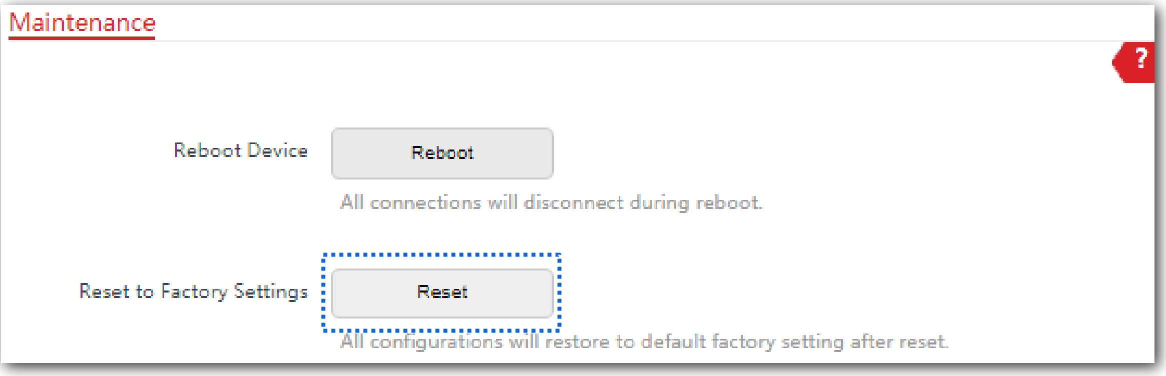
– To prevent CPE damages, ensure that the power supply of the CPE is normal when the CPE is reset.

– When the factory settings are restored, the login IP address is 192.168.2.1, and both login user name and password are **admin**.

Configuration Procedure

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

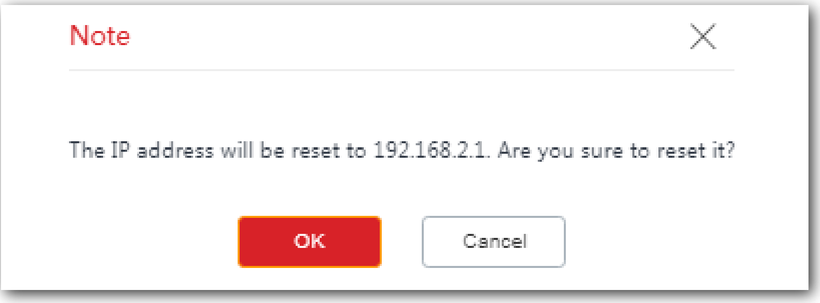
2. Click **Reset**.



All connections will disconnect during reboot.

All configurations will restore to default factory setting after reset.

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



Note

The IP address will be reset to 192.168.2.1. Are you sure to reset it?

---End

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

9.2.3 Upgrade Firmware

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

Note

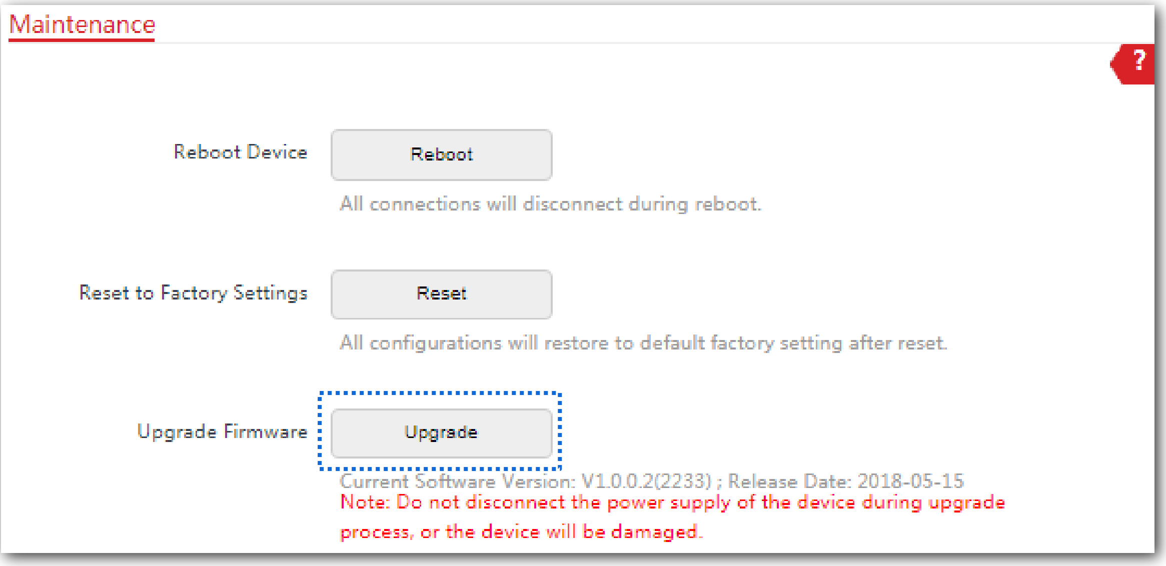
To prevent damaging the CPE, verify that the new firmware version is applicable to the CPE before upgrading the firmware and keep the power supply of the CPE connected during an upgrade.

Configuration Procedure

1. Download the package of a later firmware version for the CPE from http://www.ip-com.com.cn to your local computer, and decompress the package.

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

   Click **Upgrade**.



Maintenance

Reboot Device

All connections will disconnect during reboot.

Reset to Factory Settings

All configurations will restore to default factory setting after reset.

Upgrade Firmware

Current Software Version: V1.0.0.2(2233) ; Release Date: 2018-05-15
Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.

3. Select the file from your local computer for upgrading the firmware.

   ---End

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

Tip

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

9.2.4 Backup/Restore

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

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

Note

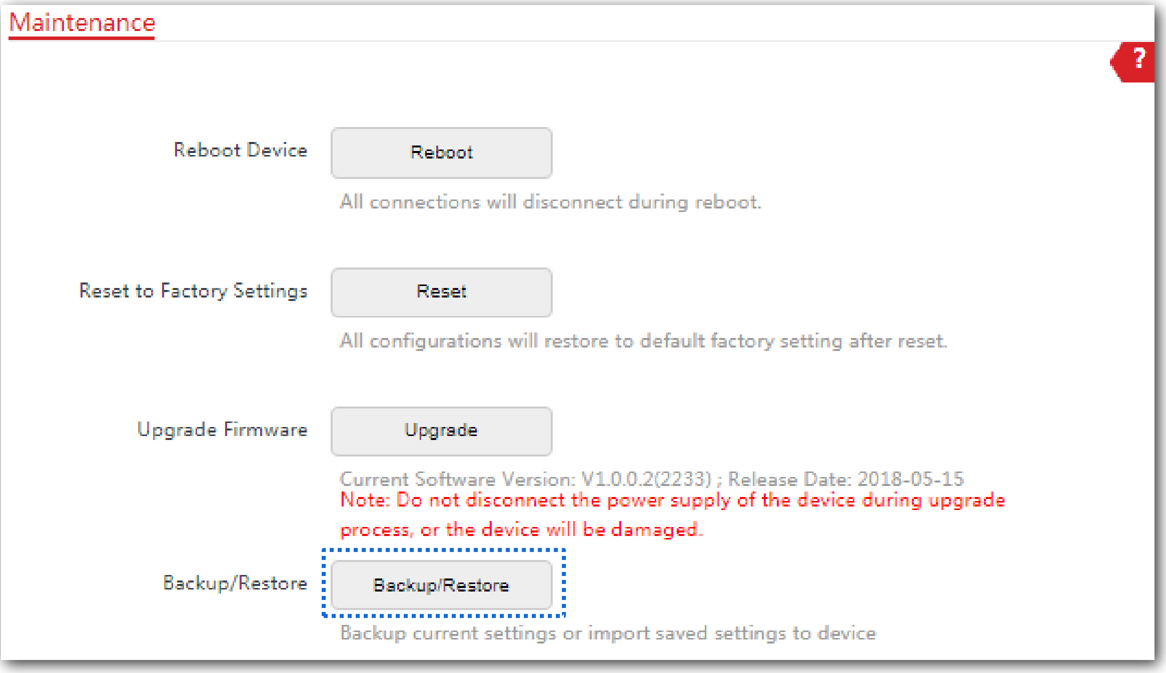
If you need to apply same or similar configurations to many CPEs, you can configure one of the CPEs, back up the configuration of the CPE, and use the backup to restore the configuration on the other CPEs. This improves configuration efficiency.

Backup

Configuration Proceudre

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

2. Click **Backup/Restore**.



Maintenance

Reboot Device

All connections will disconnect during reboot.

Reset to Factory Settings

All configurations will restore to default factory setting after reset.

Upgrade Firmware

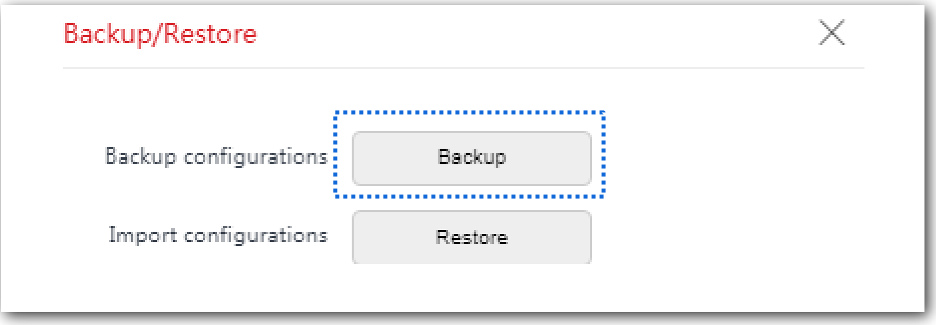
Current Software Version: V1.0.0.2(2233) ; Release Date: 2018-05-15

Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.

Backup/Restore

Backup current settings or import saved settings to device

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



Backup/Restore

Backup configurations

Import configurations

---End

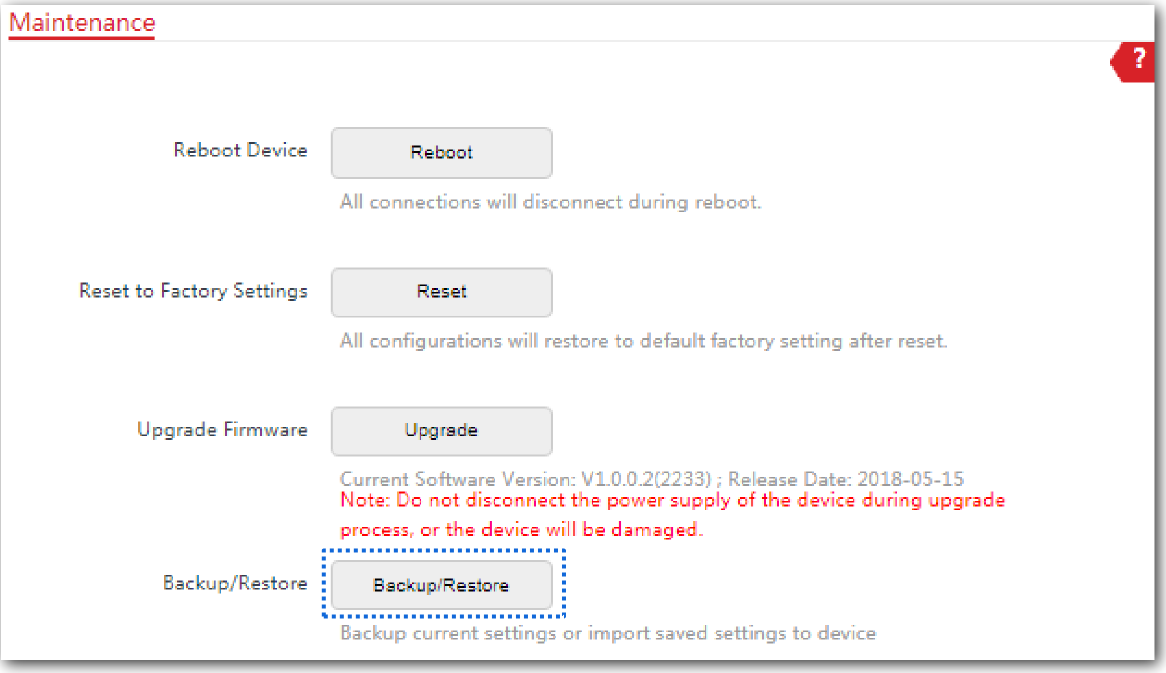
A file named **APCfm.cfg** is downloaded to your local computer.

Restore

Configuration Procedure

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

2. Click **Backup/Restore**.



Maintenance

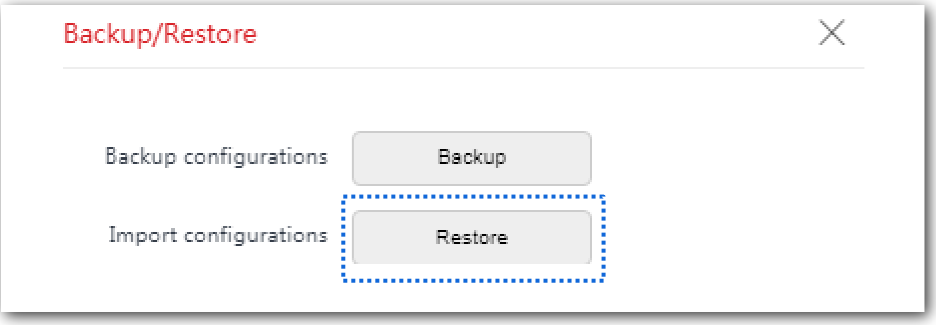
Reboot Device
Reboot
All connections will disconnect during reboot.

Reset to Factory Settings
Reset
All configurations will restore to default factory setting after reset.

Upgrade Firmware
Upgrade
Current Software Version: V1.0.0.2(2233) ; Release Date: 2018-05-15
Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.

Backup/Restore
Backup/Restore
Backup current settings or import saved settings to device

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



Backup/Restore

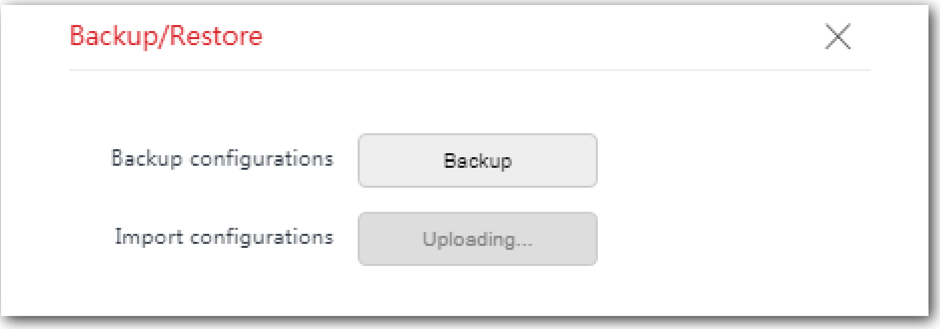
Backup configurations
Backup

Import configurations
Restore

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

---End

The file is being uploaded.



Backup/Restore

Backup configurations
Backup

Import configurations
Uploading...

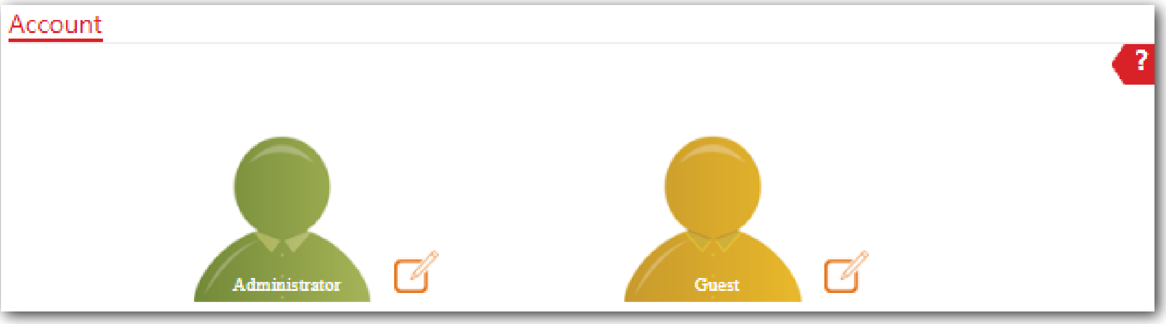
A progress bar is displayed on the page. Wait for it to elapse. Then the CPE is restored the settings successfully.

9.3 Account

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

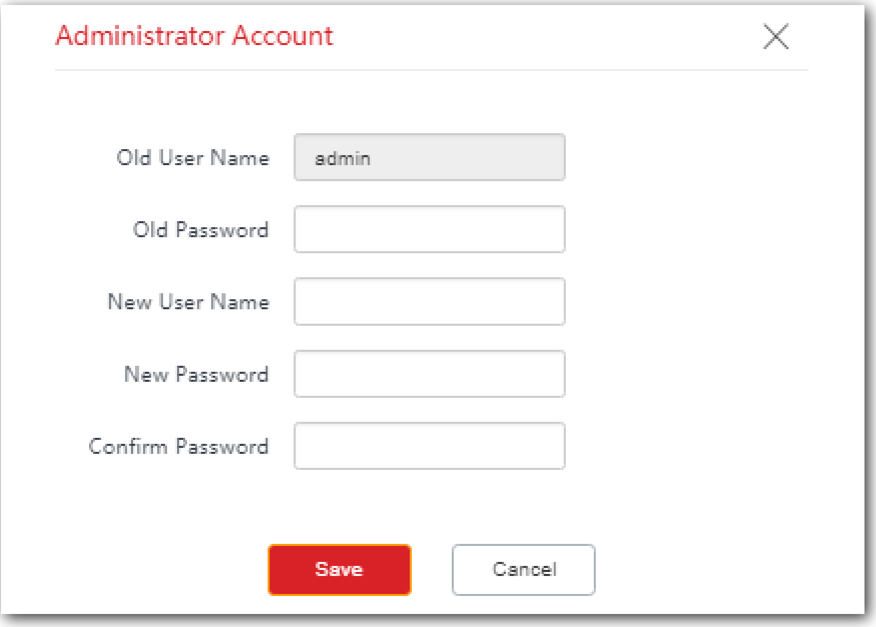
On this page, you can change the login account information of the CPE to prevent unauthorized login.

Click ✎ to change the account information.



9.3.1 Administrator

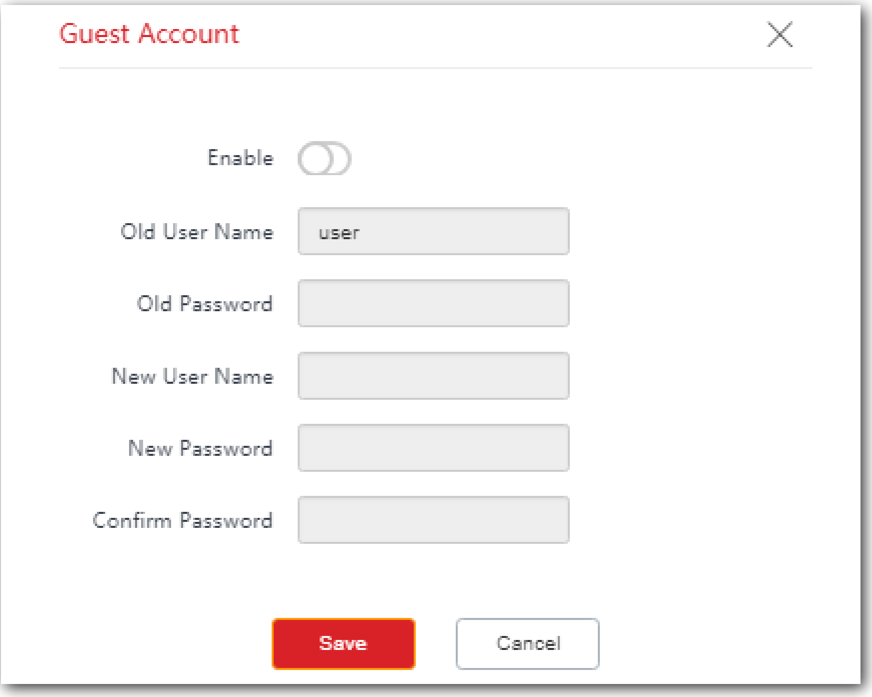
You can modify and view the settings with the administrator account.


Administrator Account

Old User Name	admin
Old Password	
New User Name	
New Password	
Confirm Password	

9.3.2 Guest

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



Guest Account

Enable	○
Old User Name	user
Old Password	
New User Name	
New Password	
Confirm Password	

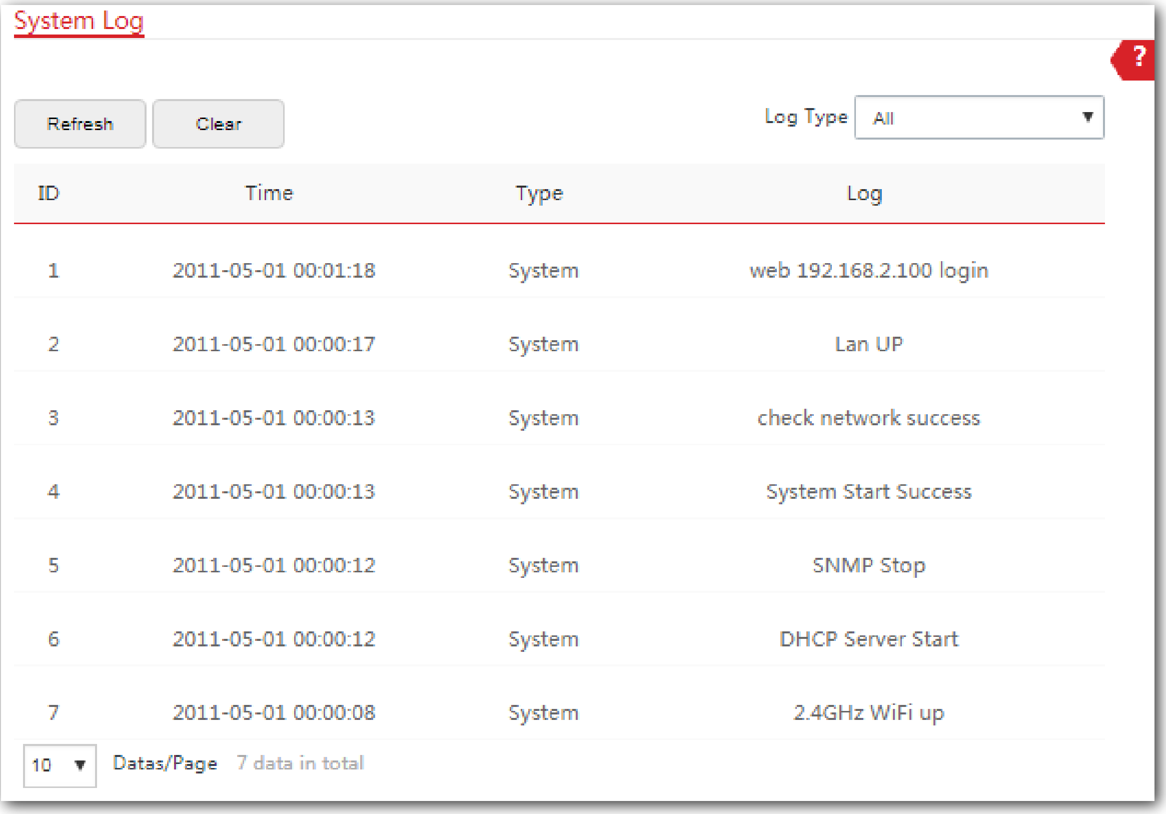
Parameters Description

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

9.4 System Log

To access the page, choose **Tools** > **System Log**.

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



Log Type: All

ID	Time	Type	Log
1	2011-05-01 00:01:18	System	web 192.168.2.100 login
2	2011-05-01 00:00:17	System	Lan UP
3	2011-05-01 00:00:13	System	check network success
4	2011-05-01 00:00:13	System	System Start Success
5	2011-05-01 00:00:12	System	SNMP Stop
6	2011-05-01 00:00:12	System	DHCP Server Start
7	2011-05-01 00:00:08	System	2.4GHz WiFi up

10 Datas/Page 7 data in total

To ensure that the logs are recorded correctly, verify the system time of the CPE. You can correct the system time of the CPE by choosing **Tools** > **Date & Time**.

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

Note

– - When the CPE reboots, the previous logs are lost.

– -The CPE reboots when the CPE is powered on after a power failure, the VLAN function is configured, the firmware is upgraded, a CPE configuration is backed up or restored or the factory settings are restored.

Appendix

A.1 FAQ

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

A1: Try the following methods and try again:

- Ensure that the device has been connected to the power supply and the computer properly.
- Ensure that the IP address of the login computer is 192.168.2.*X* (*X* ranges from 2 to 254).
- Reset the device to factory settings.

Q2: How to reset the device to factory settings?

A2: Note: Resetting the device will clear all settings, and you need to configure it again.

Method One: 1 minute after the device is powered on, uncover the device, and hold down the reset button for about 8 seconds.

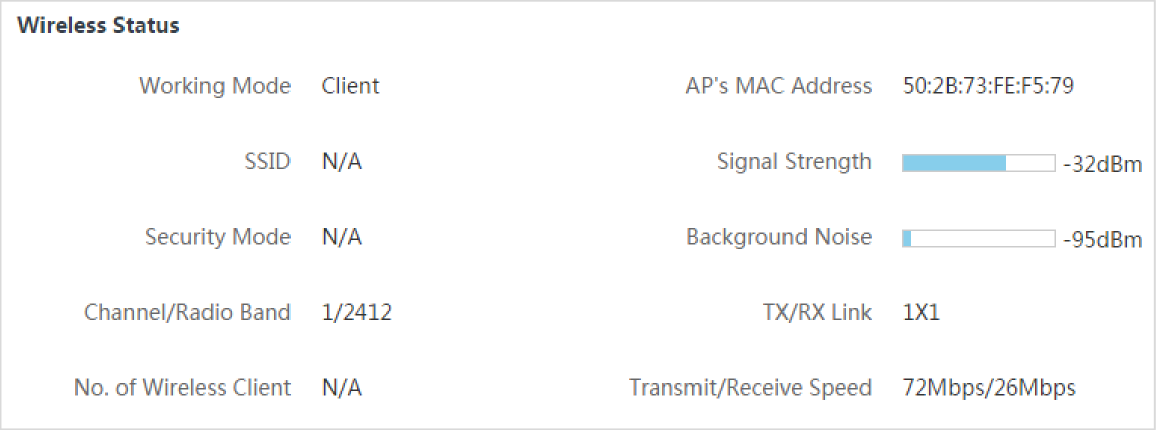
Method Two: Log in to the web UI of the device, choose **Tools** > **Maintenance**, and click the **Reset** button.

Q3: How to judge whether the bridging signal is optimal when the devices are used for CCTV surveillance?

A3:

Method One: Observe the LED indicators of the two devices. The bridging signal is optimum when the LED1, LED2 and LED3 indicators are solid on or flashing.

Method Two: Log in to the web UI of one device (default login address: 192.168.2.1), choose **Status**, and check the wireless status on the following page:



Wireless Status

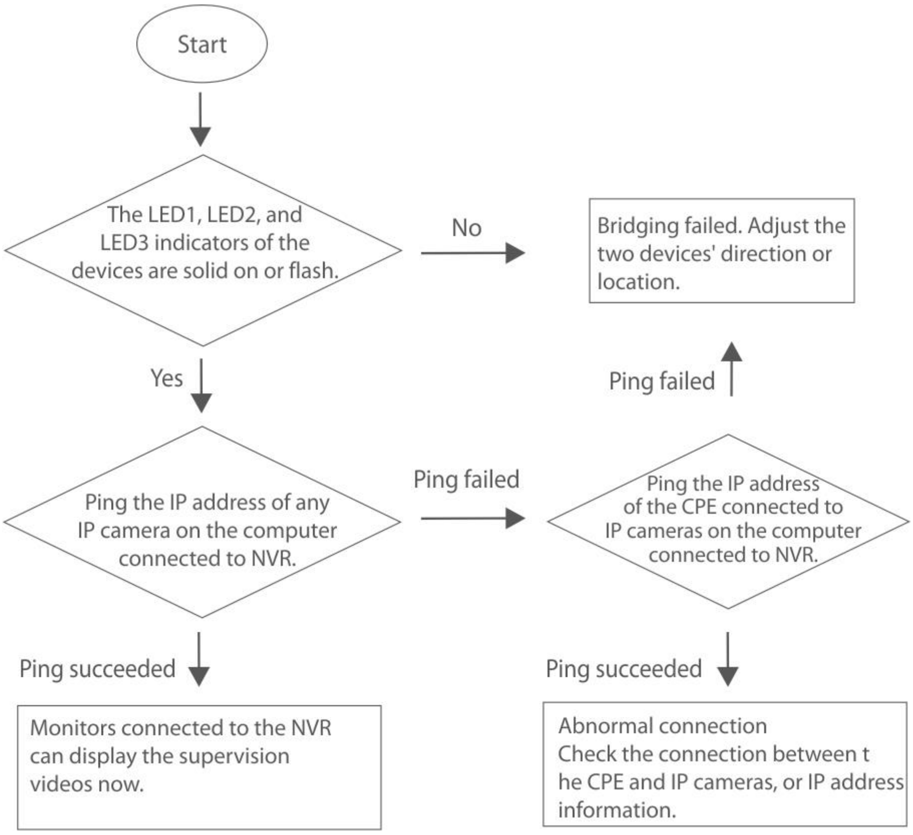
Working Mode	Client	AP's MAC Address	50:2B:73:FE:F5:79
SSID	N/A	Signal Strength	-32dBm
Security Mode	N/A	Background Noise	-95dBm
Channel/Radio Band	1/2412	TX/RX Link	1X1
No. of Wireless Client	N/A	Transmit/Receive Speed	72Mbps/26Mbps

Stronger signal strength (-90 is better than -100) and less background noise (-100 is better than -90) indicates better bridging signal.

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

A4: Try the following solutions:

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


Start
The LED1, LED2, and LED3 indicators of the devices are solid on or flash.
No
Bridging failed. Adjust the two devices' direction or location.
Yes
Ping failed
Ping the IP address of any IP camera on the computer connected to NVR.
Ping failed
Ping the IP address of the CPE connected to IP cameras on the computer connected to NVR.
Ping succeeded
Monitors connected to the NVR can display the supervision videos now.
Ping succeeded
Abnormal connection Check the connection between t he CPE and IP cameras, or IP address information.

- If the preceding check is normal, it indicates the connections are properly. Please check the configuration information, including the configuration information of NVR, and IP cameras.

A.2 Default Parameters

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

Parameters			**CPE3**	**CPE9**
Login	Login IP Address		192.168.2.1	
	Account	Administrator	admin/admin	
		Guest	Disabled	
Quick Setup	Working Mode		AP mode	
LAN Setup	IP Address Type		Static IP address	
	IP Address		192.168.2.1	
	Subnet Mask		255.255.255.0	
	Default Gateway		192.168.2.254	
	Primary DNS Server		8.8.8.8	
	Secondary DNS Server		8.8.4.4	
	Device Name		CPE3V1.0	CPE9V2.0
DHCP Server	DHCP Server		Enable	
	Start IP Address		192.168.2.100	
	End IP Address		192.168.2.200	
	Subnet Mask		255.255.255.0	
	Gateway Address		192.168.2.254	
	Primary DNS Server		8.8.8.8	
	Secondary DNS Server		8.8.4.4	
	Lease Time		1 day	
VLAN Settings	VLAN Settings		Disable	
	PVID		/	1
	Management VLAN		1	1
	WLAN		1000	1000
	LAN		/	1
Wireless-Basic	Wireless Network		Enable	
	Country/Region		China	
	SSID		IP-COM_XXXXXX, and XXXXXX is the last six characters of the LAN MAC address of the CPE	
	Broadcast SSID		Enable	
	Network Mode		11b/g/n	
	Channel		Auto	

Parameters		CPE3	CPE9
	Transmit Power	20 dBm	29 dBm
	Channel Bandwidth	20 MHz	Auto
	Extension Channel	/	Auto
	Transmit Rate	Auto	Auto
	Security Mode	None	
	Isolate Client	Disable	
	Max. Number of Clients	16	48
Wireless-Advanced	WMM	Enable	
	APSD	Disable	
	Minimum RSSI Threshold	Disable	
	Preamble	Long Preamble	
	Signal Transmission	/	Coverage-oriented
	Signal Reception Level	Level 4	Auto
	Transmission Distance	/	3 km
	Beacon Interval	100ms	
	Fragment Threshold	2346	
	RTS Threshold	2347	
	DTIM Interval	1	1
	Signal LED1 Threshold	-90 dBm	-90 dBm
	Signal LED2 Threshold	-80 dBm	-80 dBm
	Signal LED3 Threshold	-70 dBm	-70 dBm
Wireless –Access Control		Disable	
PoE/LAN Speed		/	Auto Negotiation
LAN Speed		Auto Negotiation	
Diagnose		Disable	
Network Service	Reboot Schedule	Disable	
	Login Timeout Interval	5 min	
	SNMP Agent	Disable	
	Ping Watch Dog	Disable	
	Telnet Service	Disable	
	UPnP	Enable	
	Hardware Watch Dog	/	Enable

Parameters		CPE3	CPE9
Tools	Date & Time	Synchronized with the Internet (GTM+8:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei Time Interval: 30 minutes	