www.ip-com.com.cn

# User Guide

### Outdoor CPE



#### **Copyright Statement**

©2020 IP-COM Networks Co., Ltd. All rights reserved.

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

#### Disclaimer

Pictures, images and product specifications herein are for 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! This user guide helps you configure, manage and maintain the product.

#### Conventions

This guide applies to the following CPEs. iLBE-5AC is used for illustrations unless otherwise specified. The contained images and UI screenshots are subject to the actual products.

Product Model	Description
CPE6S	5GHz 11AC 867Mbps 12dBi Outdoor CPE
iLBE-5AC	5GHz 11AC 23dBi Gigabit Outdoor CPE

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 <b>User Name</b> to <b>Tom</b> .
Variable	Italic	Format: XX:XX:XX:XX:XX:XX
UI control	Bold	On the <b>Policy</b> page, click the <b>OK</b> button.

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

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

#### For more documents

Go to our website at <u>https://www.ip-com.com.cn</u> and search for the latest documents for this product.

#### **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) 2765 3089

info@ip-com.com.cn

https://www.ip-com.com.cn

## Contents

1 Application scenario	
1.1 ISP hotspot connection-WISP mode	1
1.1.1 Solution	
1.1.2 Set up the CPE	
1.1.3 Install the CPE	
1.2 CCTV surveillance	6
1.2.1 Solution	6
1.2.2 Set up the CPEs	6
1.2.3 Install the CPEs	
2 Login	
2.1 Login	
2.2 Logout	
3 Web UI	21
3.1 Web UI layout	
3.2 Common buttons	
4 Quick setup	
4.1 AP mode	24
4.1.1 Overview	
4.1.2 Quick setup	
4.2 Client mode	
4.2.1 Overview	
4.2.2 Quick setup	
4.2.3 Example of AP mode and client mode	
4.3 Universal repeater mode	
4.3.1 Overview	
4.3.2 Quick setup	
4.4 WISP mode	
4.4.1 Overview	
4.4.2 Quick setup	
4.4.3 Example of WISP mode	
4.5 Repeater mode	

4.5.1 Overview	
4.5.2 Quick setup	
4.6 P2MP mode	
4.6.1 Overview	
4.6.2 Quick setup	
4.7 Router mode	
4.7.1 Overview	
4.7.2 Quick setup	
5 Status	
5.1 System status	73
5.2 Wireless status	
5.3 Statistics	
5.3.1 Throughput	
5.3.2 Wireless client/Upstream AP	
5.3.3 Interface	
5.3.4 ARP table	
5.3.5 Routing table	
6 Network	
6.1 LAN setup	
6.1.1 Overview	
6.1.2 Set the LAN IP address manually	
6.1.3 Log in to the web UI after changing the LAN IP address	
6.1.4 Set the device to obtaining a LAN IP address automatically	
6.2 MAC clone	
6.2.1 Overview	
6.2.2 Clone a MAC address	
6.3 DHCP server	
6.3.1 Overview	
6.3.2 Configure the DHCP server	
6.4 DHCP client	
6.5 VLAN settings	
6.5.1 Overview	
6.5.2 Example of configuring VLAN	
7 Wireless	
7.1 Basic	
7.1.1 Overview	
7.1.2 Set up a non-encrypted wireless network	
7.1.3 Set up a wireless network encrypted using WPA2-PSK	
7.1.4 Set up a wireless network encrypted using WPA or WPA2	

7.2 Advanced	
7.3 Access control	
7.3.1 Overview	
7.3.2 Example of configuring access control	
8 Advanced	134
8.1 LAN rate	
8.2 Diagnose	
8.2.1 Site Survey	
8.2.2 Ping	
8.2.3 Traceroute	
8.2.4 Speed test	
8.2.5 Spectrum Analysis	
8.3 Bandwidth control	143
8.3.1 Overview	
8.3.2 Example of configuring bandwidth control	
8.4 Port forwarding	
8.4.1 Overview	
8.4.2 Example of configuring port forwarding	
8.5 MAC filter	
8.5.1 Overview	
8.5.2 Example of configuring MAC filter	151
8.6 Network service	
8.6.1 DDNS	
8.6.2 Remote web management	
8.6.3 Reboot schedule	
8.6.4 Login timeout interval	
8.6.5 SNMP agent	
8.6.6 Ping watch dog	
8.6.7 DMZ host	
8.6.8 Telnet service	
8.6.9 UPnP	
8.6.10 Hardware watch dog	
8.6.11 STP	
9 Tools	170
9.1 Date & time	
9.1.1 Synchronized with the Internet	
9.1.2 Manual	
9.2 Maintenance	
9.2.1 Reboot device	
9.2.2 Reset to factory settings	

9.2.3 Upgrade firmware	
9.2.4 Backup/Restore	
9.3 Account	
9.3.1 Administrator	
9.3.2 Guest	
9.4 System log	
Appendix	

## **1** Application scenario

### **1.1** ISP hotspot connection-WISP mode

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

#### 1.1.1 Solution

IP-COM CPE can meet this demand.

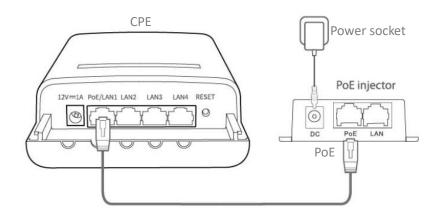
CPE6S is used as an example to illustrate the installation procedures. Procedures for other CPEs are similar.



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

#### 1.1.2 Set up the CPE

- 1. Power on the CPE (powered by PoE in this example).
  - (1) Uncover the housing of the CPE.
  - (2) Use an Ethernet cable (CAT5e or better is recommended) to connect the PoE/LAN port of the CPE to the PoE port of the PoE injector.
  - (3) Use the included power adapter to connect the PoE injector to a power socket. The Power LED indicator of the CPE lights up.

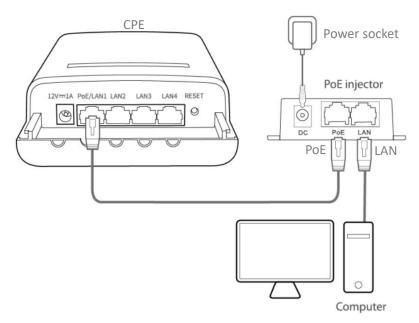




Refer to your actual product for the supported PoE power supply distance.

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

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



- (2) Log in to the web UI of CPE, and choose **Quick Setup** to enter the configuration page.
- (3) 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.
O Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
• WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
Router connect to modem in wired manner, and provide network access point
Next

(4) Select the SSID of your ISP hotspot, which is WiFi\_123456 in this example, and click Next.

Quick Setu	p>>WISP				
Click "Scan", a and click "Nex	and select the wireles	s network you wan	nt to connect,		
	Scan	C Scan again			
	Upstream AP	WiFi_123456			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	WiFi_123456	165	D8:38:0D:5A:AA:34	WPA2-PSK,AES	.all

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

Quick Setup>>WISP					
Ensure that the device uses the same channel, encryption, and encryption algorithm as those of upstream AP. Then enter the remote AP's WiFi password, and click "Next" to continue.					
Upstream AP	WiFi_123456				
Upstream AP MAC Address	D8:38:0D:5A:AA:34				
Channel	165(5825MHz) •				
Security Mode	WPA2-PSK •				
Encryption Algorithm	● AES ○ TKIP ◎ TKIP&AES				
<b>*</b> Key					
	Previous				

#### (6) 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						2
Please select an internet connecti and click "Next".	on type, and enter the int	ternet parameters provi	ded by your IS	SP.		ł
Internet Connection Type	DHCP (Dynamic IP)	Static IP Address	PPPoE			
PPPoE User Name						
PPPoE Password						
				Previous	Next	

(7) Customize the SSID and key, and click Next.

Quick Setup>>WISP				
You can set up your wireless netwo	ork name and wireless passw	ord here.		2
Note down your wireless password				
* SSID(WiFi Name)	Tom's WiFi			
Channel	165(5825MHz) •			
Security Mode	WPA2-PSK •			
Encryption Algorithm	● AES   ○ TKIP   ○ TKI	P&AES		
*Key				
			Previous	Next

(8) 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 excluding 2). Then click Next.

Quick Setup>>WISP		
Specify the device with an IP addre or upstream AP.	ss whose network segment	is different from that of IP address of ISP access point
* IP Address	192.168.8.1	
Subnet Mask	255.255.255.0	
		Previous

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

Quick Setup>>WISP			
			?
The device is set to WISP, click "Save" to apply the settings.			
	Previous	Save	

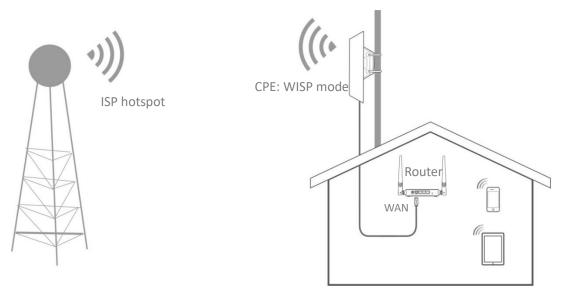
----End

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

#### **1.1.3** Install the CPE

- 1. Place the CPE at an elevated position in the open air.
- Connect the PoE/LAN port of the CPE to the WAN port of your wireless router. The Power LED indicator lights up.
- Adjust the CPE's direction or location on the selected pole until the LED1, LED2 and LED3 indicators of the CPE light up.

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



#### ----End

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

LED indicator	Status	Description
LED1, LED2, LED3 (Received signal strength LED indicators)	Solid on/Blinking	<ul> <li>There is device connected to the CPE.</li> <li>Solid on: The CPE may work in AP, Repeater, P2MP or Router mode.</li> <li>Blinking: The CPE may work in Client, Universal Repeater or WISP mode.</li> <li>Each LED indicator corresponds to a received signal strength value. When the received signal strength of the CPE reaches the RSSI threshold, the corresponding LED indicator lights up. You can judge the connection quality based on the statuses of the LED indicators.</li> <li>By default, the minimum signal strength of LED1, LED2 and LED3 are -90 dBm, -80 dBm and -70 dBm. You can change them on the Wireless &gt; Advanced page of the web UI of the CPE.</li> </ul>
	Off	No device is connected to the CPE, or the received signal strength is less than the RSSI threshold (default: -90 dBm).

### **1.2** CCTV surveillance

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

#### 1.2.1 Solution

IP-COM CPE can meet this demand.

CPE6S is used as an example to illustrate the installation procedures. Procedures for other CPEs are similar.

#### 1.2.2 Set up the CPEs

-) - Tip

At least two CPEs are required for bridging.

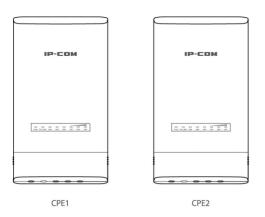
#### **Option 1: Automatic bridging (recommended)**



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

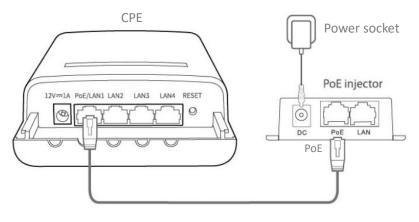
#### Scenario 1: Peer-to-peer bridging

1. Place the two CPEs next to each other.



- 2. Power on the CPEs (powered by PoE in this example).
  - (1) Remove the housing of each CPE.
  - (2) Use the Ethernet cables (CAT5e or better is recommended) to connect the **PoE/LAN** ports of the CPEs to the **PoE** ports of the included PoE injectors to power them on.

(3) Connect the PoE injectors to power sockets. The **Power** LED indicators of the CPEs light up.



### · 🍯 - Tip

Refer to your actual product for the supported PoE power supply distance.

#### ----End

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



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

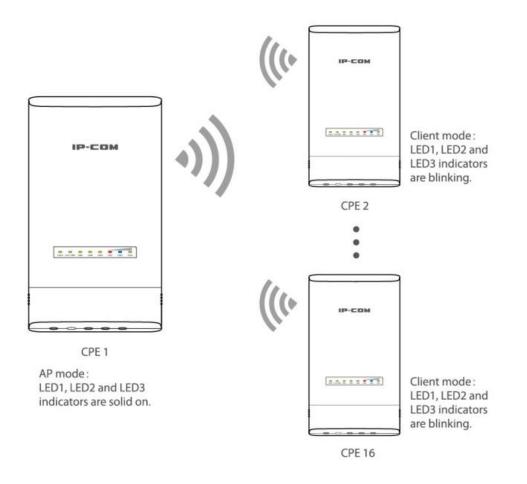
#### Scenario 2: Peer-to-multiple peers bridging



- For peer-to-multiple peers bridging, perform peer-to-peer bridging first, and then power on the rest CPEs within 30 minutes.
- A CPE can bridge to 15 CPEs at most.
- 1. Refer to <u>Peer-to-peer bridging</u> to make any two CPEs bridge to each other.
- 2. Within 30 minutes after the peer-to-peer bridging succeeds, place the rest CPEs which are in factory settings near the CPE with the LED1, LED2, and LED3 indicators solid on and power them on.

----End

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

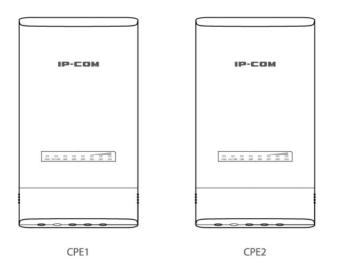


### - Тір

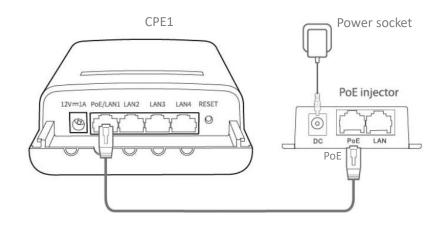
- If the LED1, LED2 and LED3 indicators of a new-added CPE turn off after it is powered on for 1 minute, the bridging fails. Reset the CPE to factory settings, and wait until its LED1, LED2 and LED3 indicators keep blinking, which indicates that the automatic bridging succeeds.
- If the bridging still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

#### **Option 2 Manual bridging**

1. Place the two CPEs next to each other.



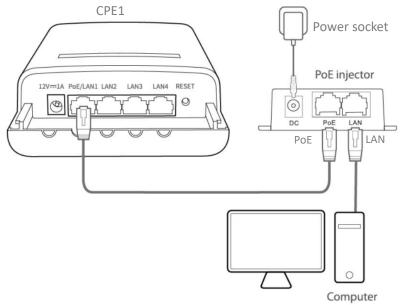
- 2. Power on the CPE1 (powered by PoE in this example).
  - (1) Uncover the housing of CPE1.
  - (2) Use an Ethernet cable (CAT5e or better is recommended) to connect the **PoE/LAN** port of CPE1 to the **PoE** port of the included PoE injector to power it on.
  - (3) Use the included power adaptor to connect the PoE injector to a power socket. The **Power** LED indicator of the **CPE1** lights up.



- 🍎 - Tip

Refer to your actual product for the supported PoE power supply distance.

- **3.** Set CPE1 to AP Mode.
  - (1) Use an Ethernet cable to connect your computer to the LAN port of the PoE injector.



- (2) Log in to the web UI of CPE1, and choose Quick Setup to enter the configuration page.
- (3) Select **AP**, and click **Next**.

$\mathbf{v}$	Status	Quick Setup Current Mode: AP
4	Quick Setup	Select a working mode:
	Network	<ul> <li>AP In this mode, the device creates a wireless network based on the current wired network.</li> <li>Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.</li> </ul>
((¢	Wireless	Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
*	Advanced	WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
۵,	Tools	Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
		P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
		Router connect to modem in wired manner, and provide network access point
_		Next

(4) Set an SSID, which is IP-COM\_158808 in this example, Security Mode, which is WPA2-PSK in this example, and Key, and click Next.

Quick Setup>>AP		
You can set up your wireless netwo Note down your wireless password	ork name and wireless password here.	<b>4</b> 2
* SSID	IP-COM_158808	
Channel	Auto •	
* Security Mode	WPA2-PSK •	
Encryption Algorithm	● AES	
<b>*</b> Key		
		Previous

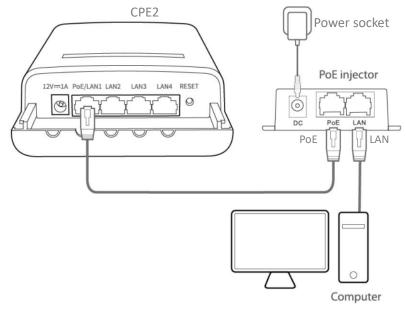
(5) Click **Save**, and wait until the CPE reboots automatically to activate the settings.

Quick Setup>>AP		
		?
The device is set to AP, click "Save" to apply the settings.		
	Previous	
	Previous	

4. Perform the procedure in <u>2 Power on the CPE1</u> to power on the CPE2.

#### 5. Set CPE2 to Client Mode.

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



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

Quick Setup
2
Select a working mode:
○ AP In this mode, the device creates a wireless network based on the current wired network.
Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
Router connect to modem in wired manner, and provide network access point
Next

(4) Select the SSID of CPE1 you set, which is **IP-COM\_158808** in this example, and click **Next**.

Quick Setup>>Client					
Click "Scan", and click "Ne	and select the wireless ext".	network you wa	nt to connect,		
	Scan	Scan agair	<u>1</u>		
	Upstream AP	IP-COM_158808	3		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	IP-COM_158808	165	D8:38:0D:5A:AA:34	WPA2-PSK,AES	line.

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

Quick Setup>>Client	
	ame channel, encryption, and encryption algorithm as those of upstream AP.
	password, and click "Next" to continue. IP-COM_158808
Upstream AP MAC Address	D8:38:0D:5A:AA:34
Channel	165(5825MHz) •
Security Mode	WPA2-PSK V
Encryption Algorithm	● AES
* Key	
	Previous Next

(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 r	etwork segment of upstream AF	».
* IP Address	192.168.2.10		
Subnet Mask	255.255.255.0	]	
			Previous Next
			Previous

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

Quick Setup>>Client	
	2
The device is set to Client, click "Save" to apply the settings.	
	Previous Save

#### ----End

When the LED1, LED2 and LED3 indicators of a CPE light solid on while the LED1, LED2 and LED3 indicators of the other CPE blink, the bridging succeeds.

If you want to perform peer-to-multiple peers bridging, refer to **Step 4-5** to bridge them to the CPE with the LED1, LED2 and LED3 indicators solid on.

### -`@\_- Tip

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

#### **1.2.3** Install the CPEs

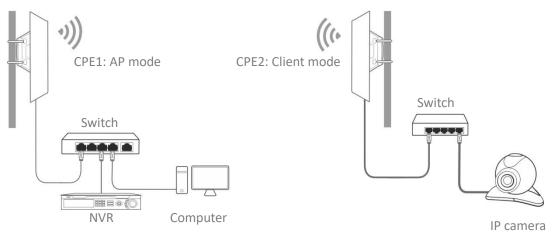
The CPE (transmitter in AP mode) with LED1, LED2 and LED3 solid on should be connected to the switch connecting to a network video recorder (NVR).

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

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.
- Uncover the housings of the two CPEs, and connect the PoE/LAN ports of the CPEs to PoE injectors respectively. The Power LED indicators light up.

- 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.



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

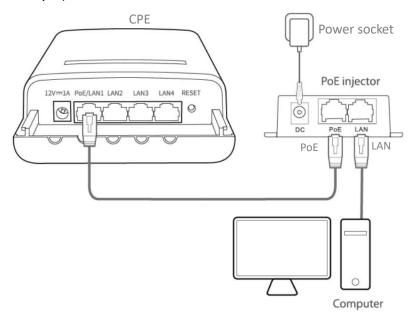
LED indicator	Status	Description
LED1, LED2, LED3 (Received signal strength LED indicators)	Solid on/Blinking	<ul> <li>The CPE is connected to a device/devices.</li> <li>Solid on: The CPE may work in AP, Repeater, P2MP or Router mode.</li> <li>Blinking: The CPE may work in Client, Universal Repeater or WISP mode.</li> <li>Each LED indicator corresponds to a received signal strength value. When the received signal strength of the CPE reaches the RSSI threshold, the corresponding LED indicator lights up. You can judge the connection quality based on the statuses of the LED indicators.</li> <li>By default, the minimum signal strength of LED1, LED2 and LED3 are -90 dBm, -80 dBm and -70 dBm. You can change them on the Wireless &gt; Advanced page of the web UI of the CPE.</li> </ul>
	Off	No device is connected to the CPE, or the received signal strength is less than the RSSI threshold (default: -90 dBm).

## 2 Login

### 2.1 Login

CPE6S is used for illustration here.

- Logging in to the web UI for the first time or after the CPE is reset
- 1. Connect the computer to the CPE or the switch connected to the CPE (powered by PoE in this example).



2. 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**.



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

New Tab	× +	-		×
$\ \in \ \rightarrow \ G$	S http://192.168.2.1		0	:

A Default user na	me: admin
Default passwo	rd: admin 🛛 😽
<b>Q</b> English	
Log	gin

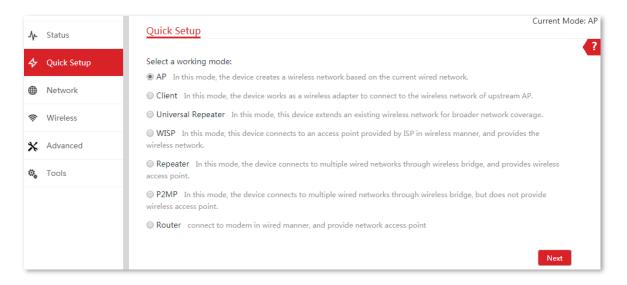
### - Tip

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

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE properly.
- Ensure that the IP address of the computer is in the same network segment of the CPE's IP address. For example, if the default IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied).
- If more than one CPE is connected, please modify the IP address of each one to avoid the failure to log
  in to the web UI of the CPE due to IP address conflict.
- Reset the CPE to factory settings. Reset method: With the CPE powered on, hold down the reset button for about 8 seconds, and then release it when all indicators light up and then turn off. The CPE is restored to factory settings successfully.

#### ----End

After successful login, the following page appears.



- Logging in to the web UI after the CPE is set to AP mode, Client mode, Universal Repeater mode, Repeater mode or P2MP mode
- 1. Connect the computer to the CPE or the switch connected to the CPE.
- 2. Set the IP address of the computer to an unused one belonging to the same network segment of the IP address of the CPE.

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

Internet Protocol Version 4 (TCP/IPv4) Properties					
General					
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.					
Obtain an IP address automatically					
Use the following IP address:	Ouse the following IP address:				
IP address:	192 . 168 . 2 . 20				
Subnet mask:	255 . 255 . 255 . 0				
Default gateway:	· · ·				
Obtain DNS server address automatically					
Use the following DNS server addresses:					
Preferred DNS server:					
Alternate DNS server:	· · ·				
Validate settings upon exit	Advanced				
	OK Cancel				



Refer to Assign a fixed IP address to your computer in Appendix for details of step 2 above.

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

### - 🍎 - Tip

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

Enter the login user name and password you set (default: admin/admin), and click Login.

A Default user nar	me: admin
Default passwo	rd: admin 😽
English	
Loç	gin

### - 🧊 - Тір

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

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE properly.
- Ensure that the IP address of the computer is in the same network segment of the CPE's IP address. For example, if the default IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied).
- If more than one CPE is connected, please modify the IP address of each one to avoid the failure to log
  in the web UI of the CPE due to IP address conflict.
- Reset the CPE to factory settings. Reset method: With the CPE powered on, hold down the reset button for about 8 seconds, and then release it when all indicators light up and then turn off. The CPE is restored to factory settings successfully.

----End

- Logging in to the web UI after the CPE is set to WISP or Router mode
- **1.** Connect the computer to the CPE or the switch connected to the CPE.
- 2. Start a web browser on your computer, and visit the IP address of the CPE.

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



Refer to <u>Check the gateway IP address of a computer</u> in Appendix to get the gateway IP address of your computer.

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

A Defaul	t user name:	admin	
Defaul	t password: ;	admin	¥
<b>Q</b> Englis	sh		2
	Login		

### - Tip

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

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE properly.
- Ensure that the IP address of the computer is in the same network segment of the CPE's IP address. For example, if the default IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied).
- If more than one CPE is connected, please modify the IP address of each one to avoid the failure to log in the web UI of the CPE due to IP address conflict.
- Reset the CPE to factory settings. Reset method: With the CPE powered on, hold down the reset button for about 8 seconds, and then release it when all indicators light up and then turn off. The CPE is restored to factory settings successfully.

----End

### 2.2 Logout

The CPE logs out when you:

- Click the **Logout** button on the upper-right corner of the web UI.
- Close the web browser.
- Perform no operation within the <u>login timeout interval</u> (default: 5 minutes).

You can change the login timeout interval on the **Advanced** > **Network Service** page.

## 3 Web UI

### 3.1 Web UI layout

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

Net	uick Setup 1 etwork AN Setup HCP Server HCP Client	MAC Address IP Address Type IP Address Subnet Mask	00:80:C6:15:87:70 Static IP Address • 192.168.2.1	
LAI DH 2 DH	AN Setup HCP Server	IP Address		
DH 2 DH	HCP Server		192.168.2.1	
2 DH		C. based March		
VII		Subhet Mask	255.255.255.0	4
VL/	LAN Settings	Default Gateway	0.0.0.0	
🔶 Wire	ireless	Primary DNS Server	0.0.0.0	
🗙 Adv	lvanced	Secondary DNS Server	0.0.0.0	
ο, Τοο	ols	Device Name	CPE15V1.0	

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

### **3.2** Common buttons

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

Common Buttons	Description
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 or change the working mode of the CPE to deploy your wireless network.

The CPE supports the following operating modes:

- <u>AP</u>: In this mode, the CPE creates a wireless network based on the current wired network.
- <u>Client</u>: In this mode, the CPE works as a wireless adapter to connect to the wireless network of upstream AP. Working in the Client mode, the CPE does not provide wireless access service, and a client device needs to be connected to the CPE with an Ethernet cable.
- <u>Universal Repeater</u>: In this mode, the CPE extends an existing wireless network for broader network coverage. The new wireless network has the same SSID, password, and related wireless information as the upstream wireless network.
- <u>WISP</u>: In this mode, the CPE connects to a hotspot provided by ISP in a wireless manner, and provides the wireless network. The CPE can also be connected to the wireless network of the upstream wireless router to obtain the IP address by DHCP (Dynamic IP), static IP address or PPPoE for internet access.
- <u>Repeater</u>: In this mode, the CPE connects multiple wired networks through wireless bridge, and provides wireless access point.
- <u>P2MP</u>: In this mode, the CPE connects multiple wired networks through wireless bridge, but does not provide wireless access point.
- <u>Router</u>: In this mode, the CPE connects to a modem in a wired manner, and provides a wireless network.

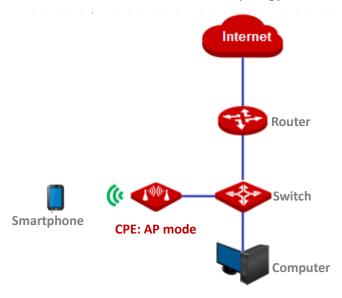
### 4.1 AP mode

#### 4.1.1 Overview

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

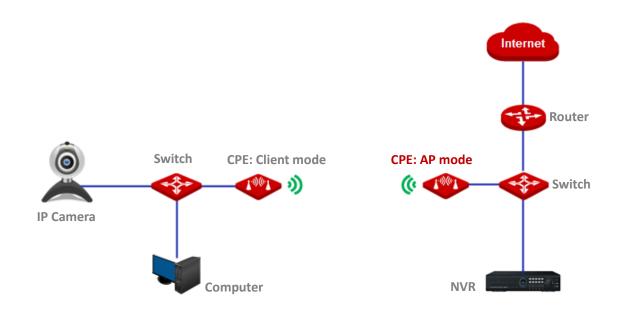
#### **Application scenario 1**

You want to transform your wired network to a wireless one for your wireless devices to access the internet. The network topology is shown as below.



#### **Application scenario 2**

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



#### 4.1.2 Quick setup

- **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	Current Mode: AP
Select a working mode:	?
AP In this mode, the device creates a wireless network based on the current wired network.	
Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP	
O Universal Repeater In this mode, this device extends an existing wireless network for broader network covera	ige.
● WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides t wireless network.	he
<b>Repeater</b> In this mode, the device connects to multiple wired networks through wireless bridge, and provides access point.	wireless
P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.	wide
Router connect to modem in wired manner, and provide network access point	
	Next

**3.** Set an SSID, which is **IP-COM\_158808** in this example, **Security Mode**, which is WPA2-PSK in this example, **Encryption Algorithm**, which is **AES** in this example, and **Key**, and click **Next**.

Quick Setup>>AP		
You can set up your wireless netwo	ork name and wireless password here.	
Note down your wireless password	l.	
* SSID	IP-COM_158808	
Channel	Auto	
* Security Mode	WPA2-PSK •	
* Encryption Algorithm	● AES   ◎ TKIP   ◎ TKIP&AES	
* Key	••••••	
		Previous Next

#### **Parameters description**

Name	Description	
SSID	It specifies the wireless network name of this CPE.	
Channel	It specifies the operating channel of this CPE. <b>Auto</b> : It indicates that the device automatically adjusts its operating channel according to the ambient environment.	
Security Mode	It specifies the security mode of the wireless network, including: <u>None</u> , <u>WPA-PSK</u> , <u>WPA2-PSK</u> , and <u>Mixed WPA/WPA2-PSK</u> .	
Encryption Algorithm	<ul> <li>It specifies the encryption method of the wireless network.</li> <li>AES: It indicates the Advanced Encryption Standard.</li> <li>TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the CPE is limited to 54 Mbps.</li> <li>TKIP&amp;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.</li> </ul>	
Кеу	It specifies the WiFi password of the wireless network.	

4. 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.	
	Previous Save

----End

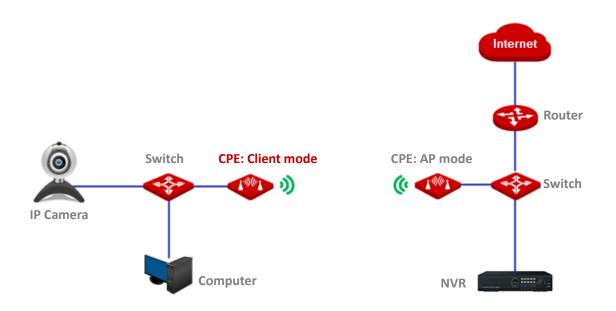
### 4.2 Client mode

#### 4.2.1 Overview

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

#### **Application scenario**

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



#### 4.2.2 Quick setup

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

Select a working mo	
select a working mi	pde:
OAP In this mode,	the device creates a wireless network based on the current wired network.
Client In this mo	de, the device works as a wireless adapter to connect to the wireless network of upstream AP.
Universal Repeat	er In this mode, this device extends an existing wireless network for broader network coverage.
• WISP In this mod wireless network.	de, this device connects to an access point provided by ISP in wireless manner, and provides the
Repeater In this access point.	mode, the device connects to multiple wired networks through wireless bridge, and provides wireless
P2MP In this mo wireless access point.	de, the device connects to multiple wired networks through wireless bridge, but does not provide
Router connect	to modem in wired manner, and provide network access point

3. Select the SSID of the upstream AP, which is **IP-COM\_158808** in this example. and click **Next** at the bottom of the page.

Quick Setu	ip>>Client						
Click "Scan", and select the wireless network you want to connect, and click "Next".							
	Scan 💽 <u>Scan again</u>						
	Upstream AP IP-COM_158808						
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength		
۲	IP-COM_158808	165	D8:38:0D:5A:AA:34	WPA2-PSK,AES	lin-		

#### -) - Tip

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

If you cannot find the SSID of the upstream AP from the list:

- Ensure that the WiFi network of the upstream AP is enabled. Only the WiFi networks at the same band as that of the CPE will be displayed in the list.
- Adjust the direction of the CPE, and move it closer to the upstream AP.
- Enter the WiFi password for the selected WiFi network IP-COM\_158808 in the Key text box, and click Next.

Quick Setup>>Client	?
Ensure that the device uses the sa	me 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_158808
Upstream AP MAC Address	D8:38:0D:5A:AA:34
Channel	165(5825MHz) •
Security Mode	WPA2-PSK V
Encryption Algorithm	● AES   ○ TKIP   ○ TKIP&AES
<b>∗</b> Key	
	Previous

#### **Parameters description**

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

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

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

Quick Setup>>Client				
Set the IP address to an unused IP a	address belonging to the	network segment of upstream	AP.	
* IP Address	192.168.2.10			
Subnet Mask	255.255.255.0			
			Previous	Next

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

Quick Setup>>Client			
The device is set to Client, click "Save" to apply the settings.			
	Previous	Save	

### ----End

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

# 4.2.3 Example of AP mode and client mode

### **Network requirement**

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

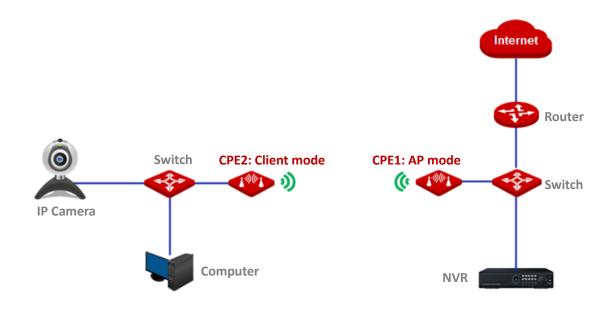


- A CPE can support several IP cameras. The maximum number of IP cameras can be calculated with the following formula:
- Number of IP cameras=Transmitted/received rate of the CPE / Data rate of IP camera

### Solution

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

### **Network topology**



### **Configuration procedure**

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

Quick Setup	Current Mode: AF
Select a working mode:	•
$\textcircled{\sc online 0}$ AP $% (AB)$ 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	k of upstream AP.
Universal Repeater In this mode, this device extends an existing wireless network for broade	er network coverage.
WISP In this mode, this device connects to an access point provided by ISP in wireless manne wireless network.	er, and provides the
Repeater In this mode, the device connects to multiple wired networks through wireless brid access point.	lge, and provides wireless
P2MP In this mode, the device connects to multiple wired networks through wireless bridge, wireless access point.	but does not provide
Router connect to modem in wired manner, and provide network access point	

(3) Set an SSID, which is **IP-COM\_158808** in this example, select a **Security Mode** (WPA2-PSK is recommended), customize **Key**, and click **Next**.

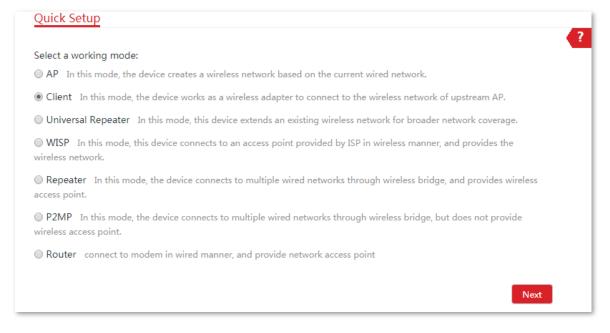
Quick Setup>>AP	
You can set up your wireless netwo	rk name and wireless password here.
Note down your wireless password	
* SSID	IP-COM_158808
Channel	Auto 🔻
* Security Mode	WPA2-PSK
Encryption Algorithm	● AES   ○ TKIP   ○ TKIP&AES
* Key	•••••
	Previous

(4) 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.			
	Previous	Save	

#### 2. Set CPE2 to Client mode.

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



# (3) Select the SSID of the CPE1, which is **IP-COM\_158808** in this example, and click **Next** at the bottom of the page.

Quick Set	up>>Client				
Click "Scan", and click "N	, and select the wireless ext".	network you wa	int to connect,		
	Scan	Scan agai	n		
	Upstream AP	IP-COM_15880	8		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	IP-COM_158808	165	D8:38:0D:5A:AA:34	WPA2-PSK,AES	.atl

### -) - Tip

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

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

Quick Setup>>Client	
	ame channel, encryption, and encryption algorithm as those of upstream AP.
Upstream AP	IP-COM_158808
Upstream AP MAC Address	D8:38:0D:5A:AA:34
Channel	165(5825MHz) •
Security Mode	WPA2-PSK V
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
* Key	
	Previous

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

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

Quick Setup>>Client		
Set the IP address to an unused IP	address belonging to the	network segment of upstream AP.
* IP Address	192.168.2.10	
Subnet Mask	255.255.255.0	
		Previous Next

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

Quick Setup>>Client	
	?
The device is set to Client, click "Save" to apply the settings.	
	Previous

#### ----End

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



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

### Verification

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

# 4.3 Universal repeater mode

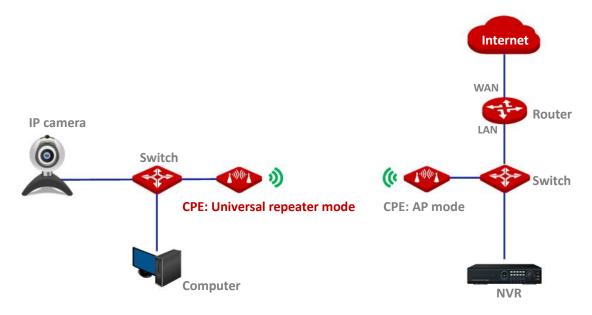
## 4.3.1 Overview

In Universal Repeater mode, the CPE expands your WiFi network for broader network coverage. The new wireless network has the same SSID, password, and related wireless information as the upstream wireless network.

Advantage of Universal Repeater compared with <u>Repeater mode</u>: The Universal Repeater mode does not require that the upstream AP supports WDS function.

### **Application scenario**

The CPE in Universal Repeater mode used to extend your existing wireless network, usually working with the CPE in AP mode. The network topology is shown as below.



## 4.3.2 Quick setup

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

Qu	lick Setup
~ .	
Sele	ect a working mode:
0/	AP In this mode, the device creates a wireless network based on the current wired network.
0	Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
•	Jniversal 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 eless network.
	Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless ess point.
	P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide eless access point.
O F	Router connect to modem in wired manner, and provide network access point
	Next

3. Select the SSID of the upstream AP, which is **IP-COM\_158808** in this example, and click **Next** at the bottom of this page.

-	Quick Setu	ıp>>Universal Rep	eater			
	Click "Scan", and click "Ne	and select the wireless	network you war	nt to connect,		
	and click the	Scan	Scan again	1		
		Upstream AP	IP-COM_158808			
	Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
	۲	IP-COM_158808	165	D8:38:0D:5A:AA:34	WPA2-PSK,AES	.atl

# - Ťip

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

If you cannot find the SSID of the upstream AP from the list:

- Ensure that the WiFi network of the upstream AP is enabled. Only the WiFi networks at the same band as that of the CPE will be displayed in the list.
- Adjust the direction of the CPE, and move it closer to the upstream AP.
- 4. Enter the WiFi password of the upstream AP in the Key text box, and click Next.

Quick Setup>>Universal Re	
Ensure that the device uses the sa	ame 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_158808
Upstream AP MAC Address	D8:38:0D:5A:AA:34
Channel	165(5825MHz) •
Security Mode	WPA2-PSK
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
<b>*</b> Key	••••••
	Previous Next

#### **Parameters description**

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

5. Set the IP address to an unused IP address belonging to the same network segment as that of the upstream AP. For example, if the IP address of the upstream AP 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 Rep	peater		
Set the IP address to an unused IP	address belonging to th	e network segment of upstream	AP.
<b>★</b> IP Address	192.168.2.10		
Subnet Mask	255.255.255.0		
			Previous Next

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

Quick Setup>>Universal Repeater	
The device is set to Universal Repeater, click "Save" to apply the settings.	
	Previous Save

### ----End

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

To access the internet with:

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

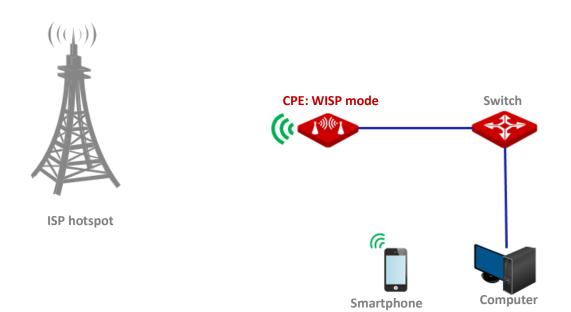
# 4.4 WISP mode

## 4.4.1 Overview

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

### **Application scenario**

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



# 4.4.2 Quick setup

- **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	g mode:
OAP In this m	ode, 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 Rep	peater In this mode, this device extends an existing wireless network for broader network coverage.
WISP In this wireless network	mode, this device connects to an access point provided by ISP in wireless manner, and provides the
Repeater In access point.	this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless
P2MP In this wireless access p	s mode, the device connects to multiple wired networks through wireless bridge, but does not provide oint.
Deutee	ect to modem in wired manner, and provide network access point

 Select the SSID of upstream AP, which is WiFi\_123456 in this example, and click Next at the bottom of the page.

Quick Setu	p>>WISP				
Click "Scan", a and click "Ne	and select the wireless	s network you war	nt to connect,		
	Scan	C Scan again	L		
	Upstream AP	WiFi_123456			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	WiFi_123456	165	D8:38:0D:5A:AA:34	WPA2-PSK,AES	.atl

# -Ğ Tip

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

If you cannot find the SSID of the upstream AP from the list:

- Ensure that the WiFi network of the upstream AP is enabled. Only the WiFi networks at the same band as that of the CPE will be displayed in the list.
- Adjust the direction of the CPE, and move it closer to the upstream AP.
- 4. Enter the WiFi password of the upstream AP in the Key text box, and click Next.

Quick Setup>>WISP	2
	ame channel, encryption, and encryption algorithm as those of upstream AP.
Upstream AP	WiFi_123456
Upstream AP MAC Address	D8:38:0D:5A:AA:34
Channel	165(5825MHz) •
Security Mode	WPA2-PSK T
Encryption Algorithm	● AES   ◎ TKIP   ◎ TKIP&AES
<b>*</b> Key	
	Previous Next

### Parameters description

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

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 connecti and click "Next".	on type, and enter the int	ernet parameters provid	ded by your ISP	2.	
Internet Connection Type	OHCP (Dynamic IP)	Static IP Address	PPPoE		
PPPoE User Name					
PPPoE Password					
			P	Previous	Next

### **Parameters description**

Name	Description
	<ul> <li>DHCP (Dynamic IP): The device obtains an IP address and other parameters form the DHCP server of upstream device for internet access.</li> </ul>
Internet Connection Type	<ul> <li>Static IP Address: The device access the internet by setting the IP address, subnet mask, default gateway and DNS server IP addresses manually.</li> </ul>
	<ul> <li>PPPoE: The device access the internet using the PPPoE user name and password provided by the ISP.</li> </ul>

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

			?
You can set up your wireless netwo	ork name and wireless	password here.	
Note down your wireless password			
<b>∗</b> SSID(WiFi Name)	Tom's WiFi		
Channel	165(5825MHz)	T	
Security Mode	WPA2-PSK	Ŧ	
Encryption Algorithm	AES OTKIP	○ TKIP&AES	
* Key	•••••		

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

Quick Setup>>WISP		
Specify the device with an IP addre or upstream AP.	ss whose network segment	is different from that of IP address of ISP access point
* IP Address	192.168.8.1	
Subnet Mask	255.255.255.0	
		Previous

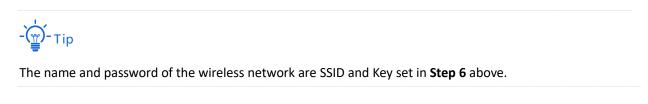
8. Click **Save**, and wait until the CPE reboots to activate the settings.

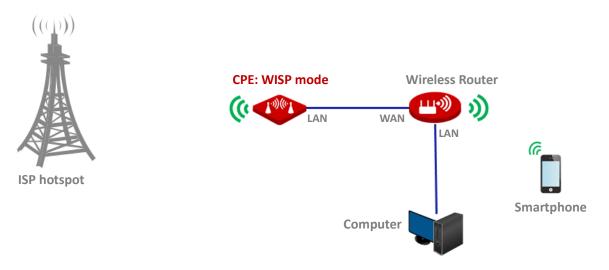
Quick Setup>>WISP	
The device is set to WISP, click "Save" to apply the settings.	?
	Previous

#### ----End

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

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





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



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

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

----End

To access the internet with:

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

# 4.4.3 Example of WISP mode

### **Network requirement**

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

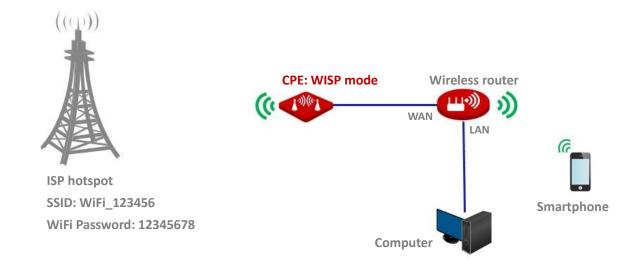
### Solution

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

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

- SSID: WiFi\_123456
- WiFi Password: 12345678
- Internet Connection Type: PPPoE
- User name: admin
- Password: admin

### **Network topology**



## **Configuration procedures**

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

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

(3) Select the SSID of your ISP hotspot, which is **WiFi\_123456** in this example, and click **Next** at the bottom of the page.

Quick Setu	ip>>WISP					?
Click "Scan", and click "Ne	and select the wireles	s network you wan	t to connect,			
	Scan	Scan again				
	Upstream AP	WiFi_123456				
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
۲	WiFi_123456	165	D8:38:0D:5A:AA:34	WPA2-PSK,AES		

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

Quick Setup>>WISP	
	ame channel, encryption, and encryption algorithm as those of upstream AP.
Upstream AP	WiFi_123456
Upstream AP MAC Address	D8:38:0D:5A:AA:34
Channel	165(5825MHz) •
Security Mode	WPA2-PSK •
Encryption Algorithm	● AES   ◎ TKIP   ◎ TKIP&AES
<b>*</b> Key	
	Previous

### (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 and click "Next".	on type, and enter the int	ernet parameters provid	ded by your ISP.	
Internet Connection Type	OHCP (Dynamic IP)	Static IP Address	PPPoE	
PPPoE User Name				
PPPoE Password				
			· ·	
			Previous	Next

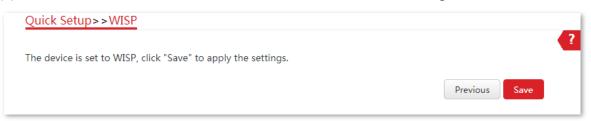
(6) Customize the SSID and key, and click **Next**.

Quick Setup>>WISP		
You can set up your wireless netwo	ork name and wireless password here.	?
Note down your wireless password	l.	
* SSID(WiFi Name)	Tom's WiFi	
Channel	165(5825MHz) <b>v</b>	
Security Mode	WPA2-PSK V	
Encryption Algorithm	● AES   ◎ TKIP   ◎ TKIP&AES	
<b>*</b> Key		
		Previous

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

Quick Setup>>WISP		
Specify the device with an IP addre or upstream AP.	ss whose network segment	is different from that of IP address of ISP access point
<b>∗</b> IP Address	192.168.8.1	
Subnet Mask	255.255.255.0	
		Previous Next

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



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

- 2. Set the wireless router.
  - (1) Log in to the Wed UI of the router.
  - (2) Select Dynamic IP as the Internet Connection Type, and save the settings.

----End

### Verification

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

# 4.5 Repeater mode

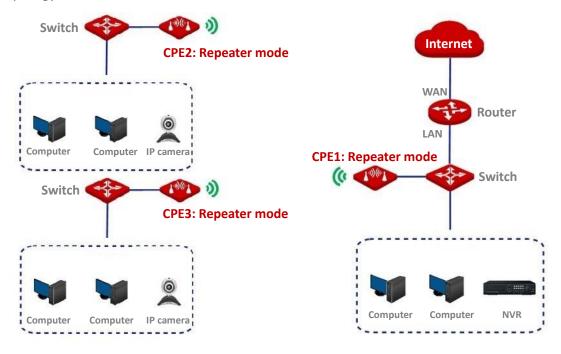
## 4.5.1 Overview

In Repeater mode, the CPE connects 2 or more (this CPE 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.

The CPE in Repeater mode can works with the CPE in Repeater or P2MP mode. Repeater mode is usually used to achieve communication between multiple offices of an enterprise in a city.

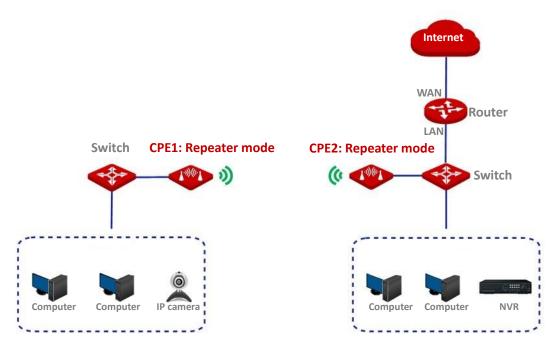
### **Application scenario**

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



## 4.5.2 Quick setup

### Peer to peer bridging



Assume that the related parameters are as follows:

#### CPE1

- **SSID**: IP-COM\_123456
- Channel: 165
- Security mode: WEP
- Authentication type: Shared
- Key1 to key4: 12345

#### CPE2

- **SSID**: IP-COM\_1
- WLAN MAC Address: D8:38:0D:5A:AA:34

Tip

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

- 1. Set the CPE2 to the **Repeater** mode.
  - Log in to the web UI of CPE2, and choose Wireless > Basic to enter the configuration page.

(2) Modify the **Channel** (165 in this example) and **Channel Bandwidth** (20MHz in this example), and click **Save**.

Enable Wireless			
Country/Region	China	•	
SSID	IP-COM_1		
Broadcast SSID	◉ Enable 🛛 🔘	Disable	
Network Mode	<b>1</b> 1a/n	•	
* Channel	165(5825MHz	) •	
Channel Shift	🔍 Enable 🛛 🖲	Disable	
Transmit Power	1dBm	10dBm	
* Channel Bandwidth	20MHz	•	
Transmit Rate	Auto	•	
Security Mode	WEP	•	
Authentication Type	Shared	•	
Default Key	Key 1	•	
Key 1	12345		ASCII •
Key 2	12345		ASCII •
Key 3	12345		ASCII 🔻
Key 4	12345		ASCII •

(3) Choose Quick Setup to enter the configuration page. Select Repeater mode, and click Next.

Select a workir	ng mode:
○ AP In this n	node, the device creates a wireless network based on the current wired network.
Client In th	is mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
🔘 Universal Re	peater In this mode, this device extends an existing wireless network for broader network coverage.
• WISP In this wireless network	s mode, this device connects to an access point provided by ISP in wireless manner, and provides the k.
Repeater Ir access point.	n this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless
P2MP In th wireless access p	is mode, the device connects to multiple wired networks through wireless bridge, but does not provide point.
Router con	nect to modem in wired manner, and provide network access point

(4) Select the SSID of CPE1 from the list, which is **IP-COM\_123456** in this example, and click **Next** at the bottom of the page.

d click "N	ext".				
	Scan	C Scan again	2		
	Peer AP1	D8:38:0D:5A:AA	D8:38:0D:5A:AA:34		
	Peer AP2	Select an SSID or enter a MAC			
	Peer AP3	Select an SSID or enter a MAC			
	Peer AP4	Select an SSID of	or enter a MAC		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
1	IP-COM_123456	165	D8:38:0D:5A:AA:34	WEP	lin.



Only the WiFi networks whose Security Modes are None or WEP can be displayed on the list.

(5) Set the Authentication Type and Default Key to the same as those of CPE1, which are Shared and Key 1 in this example, enter the Key 1, Key 2, Key 3 and Key 4, 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 clic	Enter the key of peer AP1, and click "Next".					
Peer AP1	IP-COM_123456					
MAC Address of Peer AP1	D8:38:0D:5A:AA:34					
Channel	165(5825MHz) •					
Security Mode	WEP •					
* Authentication Type	Shared •					
\star Default Key	Key 1					
* Key 1		ASCII V				
<b>★</b> Key 2	•••••	ASCII V				
* Key 3	•••••	ASCII •				
* Key 4	•••••	ASCII V				
		Previous				

### **Parameters description**

Name	Description
Peer AP1	It specifies the wireless network name (SSID) of the peer AP1.
MAC Address of Peer AP1	It specifies the MAC address of the wireless network to be bridged.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	- Tip

The Repeater mode only supports WEP and None security modes.

(6) Set the IP address to an unused IP address belonging to the same network segment as that of CPE1. Then set the Subnet Mask to the same one of the CPE1 and click **Next**.

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).

Quick Setup>>Repeater				2
Set the IP address to an unused IP	address belonging to the	network segment of peer AP.		
<b>★</b> IP Address	192.168.2.10			
Subnet Mask	255.255.255.0			
				_
			Previous	Next

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

Quick Setup>>Repeater			
			?
The device is set to Repeater, click "Save" to apply the settings.			
	Previous	Save	

- Perform the procedure in <u>Step 1</u> above to set the CPE1 to **Repeater** mode. The differences are listed below:
  - Select the SSID of CPE2, which is IP-COM\_1 in this example.
  - Do not need to change the IP address of CPE1.



If there are multiple wireless networks with the same SSID, select the one with the WLAN MAC address of the CPE2, which is **D8:38:0D:5A:AA:34** in this example.

----End

To check whether the bridging is successful:

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

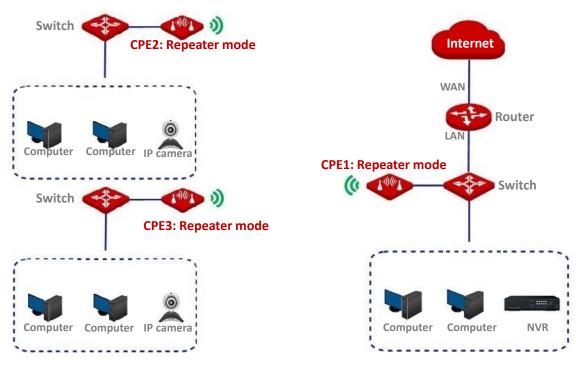
Method 2:

- **1.** Log in to the web UI of CPE1.
- Choose Advanced > Diagnose, select Ping from the Diagnose drop-down list menu, enter the IP address of CPE2 and click Start.

Diagnose		
* Diagnose	Ping ~	
* IP Address	Manual ~	
* IP Address/Domain Name		
Ping Packet	4	(Range: 1 to 10000)
Packet Size	32	Byte (Range: 1 to 60000)
l	Start	

The bridging is successful when the ping succeeds.

## Peer to multiple peers bridging



Assume that the related parameters are shown as follows:

### CPE1:

- IP Address: 192.168.2.1
- SSID: IP-COM\_1

- Channel: 165
- Channel bandwidth: 20MHz
- Security mode: None

CPE2:

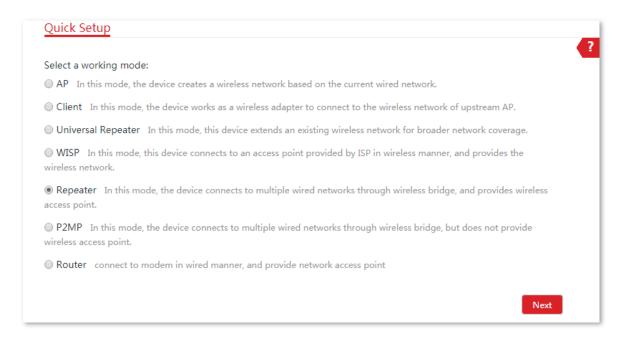
- SSID: IP-COM\_2
- WLAN MAC Address: D8:3A:0D:15:88:09

CPE3:

- SSID: IP-COM\_3
- WLAN MAC Address: D8:3A:0D:15:88:16
- **1.** Set the CPE2 to the **Repeater** mode.
  - Log in to the web UI of CPE2, and choose Wireless > Basic to enter the configuration page.
  - (2) Modify the **Channel** (165 in this example) and **Channel Bandwidth** (20MHz in this example), and click **Save**.

Enable Wireless	
Country/Region	China •
SSID	IP-COM_2
Broadcast SSID	Enable     Disable
Network Mode	11a/n 🔻
<b>∗</b> Channel	165(5825MHz) •
Channel Shift	Enable
Transmit Power	1dBm 10dBm
* Channel Bandwidth	20MHz •
Transmit Rate	Auto 🔻
Security Mode	None •
Isolate Client	Enable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

(3) Choose **Quick Setup**, and select **Repeater** and then **Next**.



- (4) Select the SSID of CPE1 from the list, which is **IP-COM\_1** in this example, and click **Next**.
- 🍎 Tip
- If you cannot scan the SSID of CPE1 from the list, choose Wireless > Basic and enable the wireless function. Then try again.
- Only the WiFi networks whose security modes are set to none or WEP can be displayed on the list.

Quick Setu	p>>Repeater				
Click "Scan", a	and select the wireles	s network you wa	ant to connect,		
and click "Ne	xt".				
	Scan	C Scan agai	'n		
	Peer AP1	D8:38:0D:15:88	:11		
Peer AP2 Select an SSID or enter a MAC			or enter a MAC		
	Peer AP3	Select an SSID	or enter a MAC		
Peer AP4 Select an SSID or enter a MAC		or enter a MAC			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
s.	IP-COM_1	165	D8:38:0D:15:88:11	None	.atl

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

Quick Setup>>Repeater		
		?
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those of peer AP.	
Enter the key of peer AP1, and clic	k "Next".	
Peer AP1	IP-COM_1	
MAC Address of Peer AP1	D8:38:0D:15:88:11	
Channel	165(5825MHz) ▼	
Security Mode	None •	
	Previous	

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

Quick Setup>>Repeater				
Set the IP address to an unused IP	address belonging to the	network segment of peer AP.		
IP Address	192.168.2.100			
Subnet Mask	255.255.255.0			
			Previous	Next

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

Quick Setup>>Repeater	
The device is set to Repeater, click "Save" to apply the settings.	•
	Previous Save

- 2. Perform <u>Step 1</u> to set CPE3 to **Repeater** mode, and bridge to CPE1.
- 3. Set CPE1 to **Repeater** mode and bridge to CPE2 and CPE3.
  - (1) Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
  - (2) Select **Repeater** mode, and click **Next**.
  - (3) Select SSIDs of CPE2 and CPE3, and click Next.



If there are multiple wireless networks with the same SSID, select the ones with the WLAN MAC addresses of the CPE2 and CPE3, which are D8:3A:0D:15:88:09 and D8:3A:0D:15:88:16 in this example.

Quick Setu	o>>Repeater				
Click "Scan", a and click "Nex	nd select the wireles	s network you wa	ant to connect,		
	Scan	C Scan agai	<u>n</u>		
	Peer AP1	D8:3A:0D:15:88	:09		
Peer AP2 D8:3A:0D:15:			:16		
	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_2	165	D8:3A:0D:15:88:09	None	lin.
	IP-COM_3	165	D8:3A:0D:15:88:16	None	-10

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

Quick Setup>>Repeater	
	?
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those of peer AP.
Enter the key of peer AP1, and clic	:k "Next".
Peer AP1	IP-COM_2
MAC Address of Peer AP1	D8:3A:0D:15:88:09
Channel	165(5825MHz) ▼
Security Mode	None •
	Previous

(5) Click Next.

Quick Setup>>Repeater				2
Set the IP address to an unused IP	address belonging to the n	etwork segment of peer AP.		
IP Address	192.168.2.1			
Subnet Mask	255.255.255.0			
			Previous Ne	xt

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

Quick Setup>>Repeater			
			?
The device is set to Repeater, click "Save" to apply the settings.			
	Previous	Save	

#### ----End

To check whether the bridging is successful:

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

### Method 2:

- **1.** Log in to the web UI of CPE1.
- Choose Advanced > Diagnose, select Ping from the Diagnose drop-down list menu, enter the IP address of CPE2 and CPE3 respectively, and click Start.

The bridging is successful when the ping succeeds.

Diagnose		
* Diagnose	Ping ~	
* IP Address	Manual ~	
* IP Address/Domain Name		
Ping Packet	4	(Range: 1 to 10000)
Packet Size	32	Byte (Range: 1 to 60000)
	Start	

# 4.6 P2MP mode

## 4.6.1 Overview

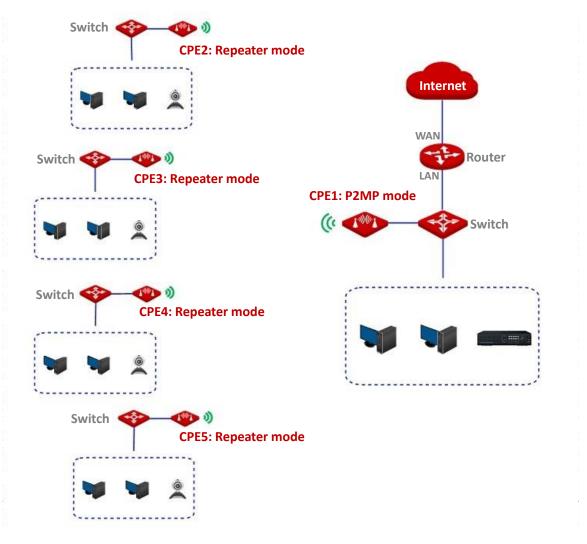
In P2MP mode, the CPE connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot provide wireless access service.

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

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

### **Application scenario**

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



# 4.6.2 Quick setup

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

- IP Address: 192.168.2.1
- **SSID**: IP-COM\_1
- Channel: 165
- Security Mode: None

#### CPE2 to CPE5:

СРЕ	SSID	WLAN MAC address
CPE2	IP-COM_2	D8:3A:0D:15:88:09
CPE3	IP-COM_3	D8:3A:0D:15:88:16
CPE4	IP-COM_4	D8:3A:0D:15:88:13
CPE5	IP-COM_5	D8:3A:0D:15:88:05

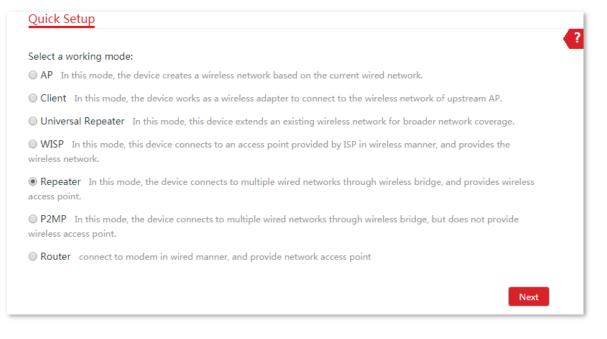
### **Configuration procedures:**

# - 🏹 - Tip

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

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

(1) Log in to the web UI of CPE2, choose Quick Setup, select Repeater mode, and click Next.



#### (2) Select the SSID of CPE1, which is **IP-COM\_1** in this example, and click **Next**.

Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
	Peer AP4	Select an SSID or enter a MAC			
	Peer AP3	Select an SSID	or enter a MAC		
	Peer AP2	Select an SSID or enter a MAC			
	Peer AP1	D8:3A:0D:15:88:02			
	Scan	C Scan again			
nd click "Next"					
ick "Scan", and	d select the wireles	s network you wa	ant to connect,		



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

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

me channel, encryptic	on, and encrypt	ion algorithm a	s those of peer AP.	
		, , , , , , , , , , , , , , , , , , ,		
IP-COM_1				
D8:3A:0D:15:88:02				
165(5825MHz)	•			
None	•			
	ck "Next". IP-COM_1 D8:3A:0D:15:88:02 165(5825MHz)	ck "Next". IP-COM_1 D8:3A:0D:15:88:02 165(5825MHz)	<pre>ck "Next". IP-COM_1 D8:3A:0D:15:88:02 165(5825MHz) </pre>	IP-COM_1 D8:3A:0D:15:88:02 165(5825MHz)

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

Quick Setup>>Repeater					2
Set the IP address to an unused IP	address belonging to ti	ne network segment of peer AP.			1
IP Address	192.168.2.100				
Subnet Mask	255.255.255.0				
			Previous	Next	

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

uick Setup>>Repeater		6
The device is set to P2MP, click "Save" to apply the settings.		
	Previous Save	

- 2. Perform <u>Step 1</u> to set the CPE3, CPE4 and CPE5 to Repeater mode, and bridge to the CPE1.
- 3. Set CPE1 to **P2MP** mode and bridge to CPE2, CPE3, CPE4 and CPE5.
  - (1) Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
  - (2) Select **P2MP** mode, and click **Next**.
  - (3) Select the SSID of CPE2, CPE3, CPE4 and CPE5, which are **IP-COM\_2**, **IP-COM\_3**, **IP-COM\_4** and **IP-COM\_5** in this example, and click **Next**.

ick "Scan", a id click "Nei	and select the wireles	s network you wa	ant to connect,		
id click Tie.	Scan	C Scan aga	in		
	Peer AP1	D8:38:0D:15:88	09		
	Peer AP2	D8:38:0D:15:88	:16		
	Peer AP3	D8:38:0D:15:88	.13		
	Peer AP4	D8:38:0D:15:88	:05		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
•	IP-COM_2	165	D8:38:0D:15:88:09	None	lin.
	IP-COM_3	165	D8:38:0D:15:88:16	None	lite.
	IP-COM_4	165	D8:38:0D:15:88:13	None	liter.
	IP-COM_5	165	D8:38:0D:15:88:05	None	1000

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

Quick Setup>>P2MP	2
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those of peer AP.
Enter the key of peer AP1, and clie	:k "Next".
Peer AP1	IP-COM_2
MAC Address of Peer AP1	D8:38:0D:15:88:09
Channel	165(5825MHz) ▼
Security Mode	None •
	Previous Next

### **Parameters description**

Name	Description	
Peer AP1	It specifies the wireless network name (SSID) of the first peer AP.	
MAC Address of Peer AP1	It specifies the MAC address of the first wireless network to be bridged.	
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.	
	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.	
Security Mode	- Ţ	
	The P2MP mode only supports WEP and None security modes.	
(5) Click Next on	the following page.	
Quick Setup>>P2	<u>2MP</u>	
Set the IP address to	an unused IP address belonging to the network segment of peer AP.	
	IP Address 192.168.2.1	
S	ubnet Mask 255.255.255.0	
	Previous	

(6) 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.	
	Previous Save

#### ----End

To check whether the bridging is successful:

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

Method 2:

- **1.** Log in to the web UI of CPE1.
- 2. Choose Advanced > Diagnose, select Ping from the Diagnose drop-down list menu, enter the IP address of each peer CPE and click Start.

Diagnose		
* Diagnose	Ping ~	
* IP Address	Manual	
* IP Address/Domain Name		
Ping Packet	4	(Range: 1 to 10000)
Packet Size	32	Byte (Range: 1 to 60000)
	Start	
	-	

The bridging is successful when the ping succeeds.

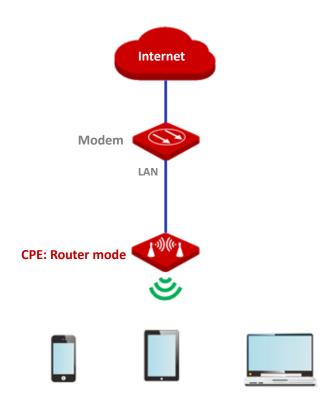
## 4.7 Router mode

## 4.7.1 Overview

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

#### **Application scenario**

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



## 4.7.2 Quick setup

- 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.

Select a	working mode:
● AP Ir	n 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.
O Unive	rsal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
• WISP wireless r	In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the network.
Repeating access point	ater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless int.
	In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide access point.
Route	r connect to modem in wired manner, and provide network access point

**3.** Select your internet connection type, and set the related parameters. Take **DHCP** as an example here. Select **DHCP (Dynamic IP)** and click **Next**.

Quick Setup>>Router			2
Please select an internet connection and click "Next".	n type, and enter the inte	ernet parameters provid	ed by your ISP.
Internet Connection Type	• DHCP (Dynamic IP)	Static IP Address	O PPPoE
			Previous Next

Name	Description
Internet Connection Type	<ul> <li>The device in Router mode supports three internet connection types:</li> <li>DHCP (Dynamic IP): The device obtains the IP address and other parameters from the DHCP server of upstream device for internet access.</li> <li>Static IP Address: The device accesses the internet using the IP address, subnet mask, default gateway and DNS server IP addresses provided by your ISP.</li> </ul>
	<ul> <li>PPPoE: The device accesses the internet using the PPPoE user name and password provided by the ISP.</li> </ul>

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

Quick Setup>>Router		?
You can set up your wireless netwo	ork name and wireless password here.	
Note down your wireless password		
* SSID	IP-COM_123456	
Channel	165(5825MHz)	
<b>☆</b> Security Mode	WPA2-PSK •	
Encryption Algorithm	● AES   ◎ TKIP   ◎ TKIP&AES	
* Key		
		Previous Next

#### **Parameters description**

Name	Description
SSID	It specifies the wireless network name of the device.
Channel	It specifies the channel that the WiFi network operates.
Security Mode	It specifies the security mode of the WiFi network of the device. It includes <u>None</u> , <u>WPA-PSK</u> , <u>WPA2-PSK</u> , and <u>Mixed WPA/WPA2-PSK</u> .
	Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

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

Quick Setup>>Router			
			?
The device is set to Router, click "Save" to apply the settings.			
	Previous	Save	

#### ----End

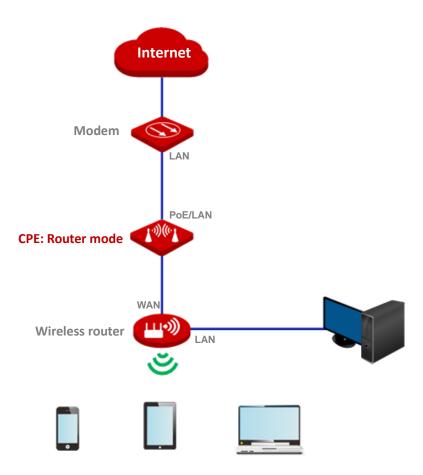
After the CPE reboots, log in to the Wed UI of the CPE again and choose **Status** to enter the page. If the WAN IP address, default gateway and DNS server information obtained by the WAN port are displayed on the System Status section, the configuration succeeds.

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



- If there is only 1 LAN port on the CPE, you can connect your wireless devices to the wireless network of the CPE to access the internet.
- The name and password of the wireless network are **SSID** and **Key** set in <u>Step 4</u> above.

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



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



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

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

----End

To access the internet with:

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

# **5** Status

This module allows you to view the information of system and wireless network, includes three parts: <u>system status</u>, <u>wireless status</u>, and <u>statistics</u>.

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

## 5.1 System status

You can view the system status here. CPE6S is used for illustration 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. If the CPE has multiple Ethernet ports, this page displays the current connection rate of each LAN port.

Status			(7)
System Status			
Device Name	CPE6SV1.0	PoE/LAN1 Speed	Disconnected
Uptime	1 h47 m2 s	LAN2 Speed	Disconnected
System Time	2020-03-23 13:41:15	LAN3 Speed	100 Mbps Full-d
Firmware Version	V1.0.0.1(5410)	LAN4 Speed	Disconnected
Hardware Version	V1.0	CPU	5%
RAM	48%	LAN MAC Address	D8:38:0D:14:88:00
WLAN MAC Address	D8:38:0D:14:88:01	LAN IP Address	192.168.2.1
Transparent Bridge	Enabled		

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



When the CPE works in Router mode, the PoE port is changed from LAN port to WAN port.

Status			
System Status			
Device Name	CPE6SV1.0	PoE/LAN1 Speed	Disconnected
Uptime	2 m42 s	LAN2 Speed	Disconnected
System Time	2020-03-23 13:52:01	LAN3 Speed	100 Mbps Full-d
Firmware Version	V1.0.0.1(5410)	LAN4 Speed	Disconnected
Hardware Version	V1.0	Connection Type	DHCP (Dynamic IP)
CPU	4%	Connection Status	Disconnected
RAM	50%	WAN IP Address	0.0.0.0
LAN MAC Address	D8:38:0D:14:88:00	Default Gateway	0.0.0.0
WLAN MAC Address	D8:38:0D:14:88:01	Primary DNS Server	0.0.0.0
LAN IP Address	192.168.2.1	Secondary DNS Server	0.0.0.0

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

Name	Description
WLAN MAC Address	It specifies the MAC address of the wireless network of this device.
LAN Speed	It specifies the PoE/LAN port speed and duplex mode of this device.
LAN IP Address	It specifies the IP address (also named management IP address) of this device. By default, it is 192.168.2.1. You can access the web UI of this device using this IP address.
Transparent Bridge	It displays the status of the Transparent Bridge.
Connection Type	It specifies the internet connection type of this device in <b>WISP</b> or <b>Router</b> mode.
	<ul> <li>DHCP (Dynamic IP): The CPE obtains IP address from the upstream DHCP server for internet access.</li> </ul>
	<ul> <li>Static IP Address: The CPE uses a fixed IP address, subnet mask, default gateway, and DNS server info for internet access.</li> </ul>
	<ul> <li>PPPoE: The CPE uses a user name and password for internet access.</li> </ul>
Connection Status	It specifies the connection status of WAN port of this device in <b>WISP</b> or <b>Router</b> mode.
WAN IP Address	It specifies the IP address of WAN port of this device in <b>WISP</b> or <b>Router</b> mode.
Default Gateway	It specifies the default gateway address of this device in <b>WISP</b> or <b>Router</b> mode.
Primary DNS Server	It specifies the IP address of primary DNS server of this device in <b>WISP</b> or <b>Router</b> mode.
Secondary DNS Server	It specifies the IP address of secondary DNS server of this device in <b>WISP</b> or <b>Router</b> mode.

## 5.2 Wireless status

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

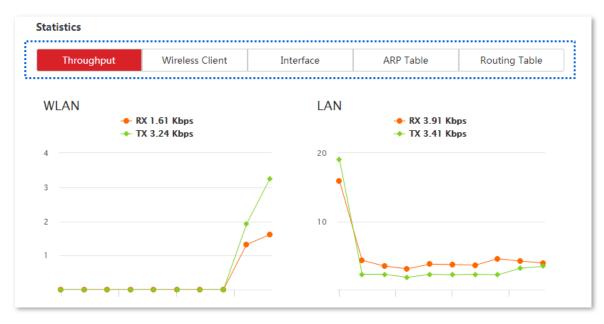
Wireless Status			
Working Mode	AP	AP's MAC Address	00:B0:C6:15:87:71
SSID	IP-COM_158770	Signal Strength	N/A
Security Mode	None	Background Noise	-95dBm
Channel/Radio Band	165/5825MHz	TX/RX Link	2X2
Channel Bandwidth	20MHz	Transmit/Receive Speed	N/A
TX Power	23dBm	IMAX	Disabled
Wireless Client	0		

Name	Description
Working Mode	It specifies the current working mode in which the device operates.
SSID	It specifies the wireless network name of this device.
Security Mode	It specifies the security mode of the wireless network of this device.
Channel/Radio Band	It specifies the channel and radio band used by this device to transmit radio signals.
Channel Bandwidth	It specifies the channel bandwidth of this device.
TX Power	It specifies the transmitted power of this device.
Wireless Client	It specifies the number of wireless clients connected to this device.
AP's MAC Address	<ul> <li>It displays the MAC address of the upstream device.</li> <li>In AP, Router, Repeater, or P2MP mode, it displays the WLAN MAC address of the CPE.</li> <li>In Client, Universal Repeater or WISP mode, or when the bridging succeeds, it displays the WLAN MAC address of the upstream AP. When the bridging fails, it displays N/A.</li> </ul>
Signal Strength	<ul> <li>It displays the wireless signal strength of peer device.</li> <li>In AP or Router mode, it displays the signal strength of the first device connected to the wireless network of the device.</li> <li>In Client, Universal Repeater, WISP, Repeater or P2MP mode, it displays the received signal strength from peer AP.</li> </ul>

Name	Description
Background Noise	It specifies the strength of radio interference signals in the ambient environment that interfere with the wireless signal of this device in the same channel. Larger absolute value indicates less interference. For example, -95 dBm indicates less interference than that of -75 dBm.
TX/RX Link	It specifies the number of spatial streams of wireless data the device is transmitting or receiving. The more links indicates the more traffic.
Transmit/Receive Speed	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.
IMAX	It specifies the status of the <u>IMAX</u> function.

## **5.3** Statistics

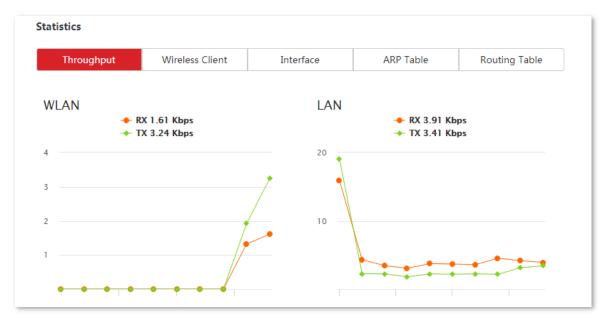
You can view statistics information here, including <u>throughput</u>, <u>wireless client</u>, <u>interface</u>, <u>ARP</u> <u>table</u> and <u>routing table</u>.



## 5.3.1 Throughput

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

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



## 5.3.2 Wireless client/Upstream AP

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

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

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

Statistics						
Throughput	Wireless Client	Interface	e	ARP Ta	ble	Routing Table
IP Address	MAC Address	Signal/Noise	Transr	nit/Receive	CCQ	Connection Duration
192.168.2.181	6C:4D:73:10:76:D2	-17/-112dBm	144/	72Mbps	100%	6 s

#### **Parameters description**

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

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

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

hroughput	Opstrea	m AP	Interface		ARP Tal	ble	Routing Table
ddress	MAC Address	Signal	/Noise Tra	nsmit/Re	ceive	CCQ	Connection Duratio
ddress	MAC Address	Signal	/Noise Tra	nsmit/Re	ceive	CCQ	Connection D

#### **Parameters description**

Name	Description
IP Address	It specifies the IP address of the upstream device.
MAC Address	It specifies the MAC address of the upstream device.
Signal/Noise	<ul> <li>Signal: It specifies the WiFi signal strength of the corresponding upstream AP.</li> <li>Noise: It specifies the ambient interference signal and electromagnetic interference strength.</li> </ul>
Transmit/Receive	It specifies the transmitting and receiving rate of the upstream device.
CCQ	It specifies the connection quality of the upstream device. A higher percentage indicates a better connection quality.
Connection Duration	It specifies the time that has elapsed since this device bridges to the upstream device.

## **5.3.3** Interface

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

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

Throu	ighput	Wireless Client	Interface	ARP	Table Ro	uting Table
Interface	IP Address	MAC Address	Received Packets	Receive Error	Transmitted Packets	Transmit Error
LAN	192.168.2.1	D8:38:0D:15:88:10	2479	0	977	0
Bridge	192.168.2.1	D8:38:0D:15:88:10	2603	0	851	0
WLAN	0.0.0.0	D8:38:0D:15:88:11	127	0	383	0

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

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

## 5.3.4 ARP table

ARP (Address Resolution Protocol) is a network layer protocol used to convert an IP address into a physical address. The ARP table displays the IP address and its corresponding MAC address the CPE visits, and the interface the packets pass through.

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

tatistics					
Throughput	Wireless Client	Interface	ARP Table	Routing Table	
IP Address		MAC Address		Interface	
192.168.2.181		6C:4D:73:10	:76:D2	Bridge	
192.168.2.104		C8:9C:DC:60	:54:69	Bridge	

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

## 5.3.5 Routing table

It specifies the destination networks that the CPE can access.

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

tatistics					
Throughput	Wireless Client	Interface	ARP Table	Routing Table	
Destination	Destination Network		Next Hop	Interface	
192.16	192.168.2.0		0.0.0.0	Bridge	
239.255.255.250		255.255.255.255	0.0.0.0	Bridge	

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

# 6 Network

## 6.1 LAN setup

### 6.1.1 Overview

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

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

When the CPE is in **AP**, **Client**, **Universal Repeater**, **Repeater**, or **P2MP** mode, the page shows as below.

LAN Setup	
MAC Address	D8:38:0D:21:81:50
IP Address Type	Static IP Address
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Device Name	iLBE-5ACV1.0
	Save

Name	Description	
MAC Address	It specifies the MAC address of LAN port.	
	<ul> <li>It specifies the type of obtaining an IP address. The default is Static IP Address.</li> <li>Static IP Address: Specify the IP address, subnet mask, default gateway, and DNS server IP addresses manually.</li> </ul>	
IP Address Type	<ul> <li>DHCP (Dynamic IP Address): The device obtains an IP address, subnet mask, default gateway and DNS server IP address from the DHCP server in the network.</li> </ul>	
	- Tip	
	If the <b>IP Address Type</b> is set to <b>DHCP (Dynamic IP Address)</b> , you need to check the device's IP address on the clients list of the DHCP server in the network, and use this IP address to log in to the web UI of the device.	
	It specifies the IP address of the device. A LAN user can visit this address to enter the web UI of the device. The default is <b>192.168.2.1</b> .	
IP Address	To access the internet, change this IP address to the same network segment of the LAN IP address of the egress router.	
Subnet Mask	It specifies the subnet mask of the device. The default is <b>255.255.255.0</b> .	
	It specifies the default gateway of the device.	
Default Gateway	You can set it to the IP address of the egress router to enable the device to acces the internet.	
	It specifies the primary DNS server IP address of the device.	
Primary DNS Server	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. If there is only one DNS server IP address, enter it in this box.	
Secondary DNS Server	It specifies the secondary DNS server IP address of the device. r If there are two DNS server IP addresses, enter one in this box.	
	It specifies the name of the device. The default name indicates the product mode and version.	
Device Name	You are recommended to change the name to indicate the location of the device so that you can easily identify the device when there are multiple devices in the network.	

LAN Setup		?
MAC Address	D8:38:0D:15:87:70	
IP Address Type	Static IP Address 🔹	
IP Address	192.168.2.1	
Subnet Mask	255.255.255.0	
	Save	
	Carcer	

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

#### **Parameters description**

Name	Description
MAC Address	It specifies the MAC address of LAN port.
IP Address Type	<ul> <li>It specifies the type of obtaining an IP address. The default is Static IP Address.</li> <li>Static IP Address: Specify the IP address and subnet mask manually.</li> <li>DHCP (Dynamic IP Address): The device obtains an IP address and subnet mask from the upstream DHCP server in the network.</li> </ul>
	If the IP Address Type is set to DHCP (Dynamic IP Address), you need to check the device's IP address on the clients list of the DHCP server of the upstream device, and use this IP address to log in to the web UI of the device.
IP Address	It specifies the IP address of the device. A LAN user can visit this address to enter the web UI of the device. The default is <b>192.168.2.1</b> .
Subnet Mask	It specifies the subnet mask corresponding to the LAN IP address of the device. The default is <b>255.255.255.0</b> .

## 6.1.2 Set the LAN IP address manually

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

AN Setup	
MAC Address	D8:38:0D:21:81:50
* IP Address Type	Static IP Address
*IP Address	192.168.2.1
* Subnet Mask	255.255.255.0
* Default Gateway	0.0.0.0
* Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Device Name	iLBE-5ACV1.0
	Save Cancel

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

Note			×
	to confirm to chan s changed, please l	nge IP address. ogin with new IP addres	ss 192.168.2.1.
	ОК	Cancel	

----End

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

After changing the LAN IP address of the CPE, if the new and original IP addresses belong to the same network segment, you can log in to the web UI of the 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 with the new IP address. Automatically obtain an IP address. Refer to <u>Assign a fixed IP address to your computer</u> in Appendix for details.

## 6.1.4 Set the CPE to obtaining a LAN IP address automatically

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

Configuration procedure:

- 1. 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	D8:38:0D:21:81:50
* IP Address Type	DHCP (Dynamic IP Add ~
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Device Name	iLBE-5ACV1.0
	Save

#### ----End

After completing configuration, if you want to re-log in to the web UI of the CPE, check the new IP address on the web UI of the upstream device which assigns the IP address to this 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.

Refer to steps in the <u>Assign a fixed IP address to your computer</u> part to assign an IP address to the computer manually.

## 6.2 MAC clone

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

## 6.2.1 Overview

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

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

## 6.2.2 Clone a MAC address

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

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

- **1.** Connect the computer to the CPE.
- Log in to the web UI of the CPE, and choose Network > MAC Clone to enter the configuration page.
- 3. Click Clone Local MAC Address.
- 4. Click Save.

MAC Clone			
			?
	MAC Address	00:B0:C6:15:87:71	
	Clone Local I	/IAC Address Restore to Default MAC Add	Jress

----End

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

If you do **NOT** use the computer that can access the internet after it connects to the modem directly to configure the CPE, but you know the MAC address (which is C8:9C:DC:60:54:69 in this example) of this computer, perform the following steps:

- 1. Log in to the web UI of the CPE, and choose **Network** > **MAC Clone** to enter the page.
- 2. Enter the MAC address of the computer that can access the internet in the MAC Address box.
- 3. Click Save.

MAC Clone			
			?
	MAC Address	C8:9C:DC:60:54:69	
	Clone Local N	AC Address Restore to Default MAC Address	

----End



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

## 6.3 DHCP server

## 6.3.1 Overview

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

## - Tip

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

## 6.3.2 Configure the DHCP server

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

ICP Server	
* DHCP Server	
Start IP Address	192.168.2.100
End IP Address	192.168.2.200
Subnet Mask	255.255.255.0
\star Gateway Address	192.168.2.254
* Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Lease Time	1 day 🔹
Secondary DNS Server	8.8.4.4

#### ----End



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

DHCP ServerIt specifies whether to enable the DHCP server function of default, it is enabled.Start IP AddressIt specifies the start IP address of the IP address pool of th default value is 192.168.2.100.It specifies the end IP address of the IP address pool of the default value is 192.168.2.200.End IP Address	ne DHCP server. The
Start IP Address       default value is 192.168.2.100.         It specifies the end IP address of the IP address pool of the default value is 192.168.2.200.         End IP Address	
End IP Address       -         The start and end IP addresses must belong to the same n	e DHCP server. The
The start and end IP addresses must belong to the same n	
the IP address of the LAN port of the device.	etwork segment as
Subnet Mask It specifies the subnet mask assigned by the DHCP server t value is <b>255.255.255.0</b> .	o clients. The default
It specifies the default IP address gateway assigned by the clients. Generally, it is the IP address of the LAN port of a r The default value is <b>192.168.2.254</b> .	
Gateway Address	
A client can access a server or host not in the local networ through a gateway.	k segment only
It specifies the primary DNS server IP address assigned by clients. The default value is <b>8.8.8.8</b> .	the DHCP server to
Primary DNS Server	
To enable clients to access the internet, set this parameter server IP address or DNS proxy IP address.	r to a correct DNS
Secondary DNS Server It specifies the secondary DNS server IP address assigned to clients. This parameter is optional.	by the DHCP server to
It specifies the validity period of an IP address assigned by client.	the DHCP server to a
Lease Time When half of the lease time has elapsed, the client sends a DHCP server to renew the lease time. If the request succes extended according to the request. Otherwise, the client s again when 7/8 of the lease time has elapsed. If the reque	eds, the lease time is sends the request

Name	Description
	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.

## 6.4 DHCP client

With the DHCP server enabled, you can view details about the clients that obtain IP addresses from the DHCP server, including host names, IP addresses, MAC addresses, and lease time.

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

DHCP Cli	ent			
ID	Host Name	IP Address	MAC Address	Lease Time
1	Dudu-Computer	192.168.2.104	C8:9C:DC:60:54:69	23h 52m 14s
10 <b>v</b> I	Datas/Page 1 data in total			

## 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.

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

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			$VID = PVID of the port, strip the tag in the packet and then forward it$ $VID \neq PVID of the port, retain the tag in the packet and then forward it$

To access the page, choose Network > VLAN Settings.

VLAN Settings		2
VLAN Settings		
PVID	1	(Range: 1 to 4094)
Management VLAN	1	(Range: 1 to 4094)
WLAN VLAN ID	1000	(Range: 1 to 4094)
	Save	ncel

Name	Description
VLAN Settings	It is used to enable or disable the VLAN function of this device. By default, it is disabled. After the VLAN function is enabled, the PoE/LAN port is used as a trunk port.
PVID	It specifies the ID of the default native VLAN ID of the trunk port. The default ID is

Name	Description
	<b>1</b> . After the VLAN function is enabled, the PoE/LAN port is used as a trunk port.
Management VLAN	It specifies the ID of the management VLAN of this device. The default ID is <b>1</b> . 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 <b>1000</b> .
	After the VLAN function is enabled, the WLAN interface functions as an access port, whose PVID is the same as VLAN ID.

## 6.5.2 Example of configuring VLAN

### **Network requirement**

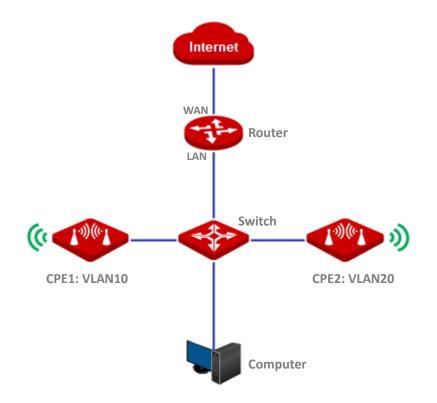
You use CPEs to set up CCTV surveillance networks. CPE1 and CPE2 are used to connect to IP cameras in different places and cannot communicate with each other.

You can assign CPE1 and CPE2 to different VLANs.

#### Assume that:

- CPE1 is assigned to VLAN10, and CPE2 is assigned to VLAN20.
- The router in the network supports IEEE 802.1q VLAN and enables two DHCP servers which belong to VLAN10 and VLAN 20 respectively.

### **Network topology**



The connections of the switch:

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

### **Configuration 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 WLAN VLAN ID to 10.
  - (4) Click Save.

VLAN Settings		?
* VLAN Settings		
PVID	1	(Range: 1 to 4094)
Management VLAN	1	(Range: 1 to 4094)
* WLAN VLAN ID	10	(Range: 1 to 4094)
	Save Car	ncel

- (5) Click **OK** on the pop-up window, and wait until the CPE1 completes reboot.
- 2. Set the WLAN VLAN ID of CPE2 to 20 according to the steps in <u>Step 1</u>.
- 3. Set up the switch as shown in the following table.

The following table shows the configuration on the switch.

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

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

The following form shows the configuration on the router:

Enables two DHCP servers on the router, and assign them to VLAN10 and VLAN20 respectively.

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 IP camera connected to the CPE1 obtains an IP address and related parameters from the DHCP server belonging to VLAN10, and the IP camera connected to CPE2 obtains these parameters from the DHCP sever belonging to VLAN20.

# **7** Wireless

## 7.1 Basic

## 7.1.1 Overview

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

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

Basic		
Enable Wireless		
Country/Region	China	~
SSID	IP-COM_218150	)
Broadcast SSID	● Enable 🛛 [	Disable
Network Mode	11ac	~
Channel	Auto	~
Channel Shift	🔿 Enable 🛛 🖲 [	Disable
DFS function	🔾 Enable 🛛 🖲 [	Disable
Transmit Power	1dBm	26dBm
Channel Bandwidth	80MHz	~
Transmit Rate	Auto	~
Security Mode	None	~
Isolate Client	🔿 Enable 🛛 🔘 [	Disable
Max. Number of Clients	48	(Range: 1 to 128)
	Save	Cancel

Country/RegionIt 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.SSIDIt specifies the wireless network name.Broadcast SSIDIt specifies whether to broadcast the SSID. When the device broadcasts an SSID, nearby wireless clients can detect the SSID. When the device broadcasts and teatry wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is case, you need to enter the SSID manually on your wireless client is some extent enhances the security of the wireless network.Network ModeIt specifies the wireless network mode of this device. Only wireless clients supporting the listed network mode can connect to the CPE.ChannelIt specifies the wireless network mode of this device, only wireless clients supporting the listed network mode can connect to the CPE.Channel ShiftIt specifies the shift of the channel center frequency shifts 5 MHz based on the frequency defined by th	Name	Description
Country/Region         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.           It specifies whether to broadcast the SSID.         When the device broadcasts an SSID, nearby wireless clients can detect the SSID.           Broadcast SSID         When this parameter is set to <b>Disable</b> , the device does not broadcast the SSID and nearby wireless clients cannot detect the SSID. This to see, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This to some extent enhances the security of the wireless network.           Network Mode         It specifies the wireless network mode of this device. Only wireless clients supporting the listed network mode can connect to the CPE.           Channel         It specifies channel in which this device automatically changes to a channel rarely used in the ambient environment to prevent interference.           Channel Shift         It specifies the shift of the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the device can exchange data on less interference channels.           DFS Function         With this function enabled, the CPE will automatically detect the frequency with the CPE itself, the CPE will automatically switch to another frequency to avoid interference with the radar system.           Transmit Power         It specifies the transmit power of this device.           Higher number indicates wider WiFi coverage. Setting a proper transmit power helps improve	Enable Wireless	It specifies whether to enable the wireless function. By default, it is enabled.
It specifies whether to broadcast the SSID.Broadcast SSIDWhen the device broadcasts an SSID, nearby wireless clients can detect 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 mode of this device. Only wireless clients supporting the listed network mode can connect to the CPE.ChannelIt specifies the wireless network mode can connect to the CPE.ChannelAuto indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.Channel ShiftIt specifies the shift of the channel center frequency.With this function enabled, the CABN 1 standard, so that the device can exchange data on less interference channels.Dynamic Frequency Selection.With this function enabled, the CPE will automatically detect the frequency of the radar system. When the CPE detects radar signals in the same frequency with the CPE itself, the CPE will automatically switch to another frequency to avoid interference with the radar system.Transmit PowerIt specifies the transmit power of this device.Transmit PowerIt specifies the abdividth of the operating channel of a wireless network. The channel bandwidth varies with different network modes. Please select it based on your actual operating environment.Auto indicates that this dive can switch its channel bandwidth based on the ambient environment.It specifies the transmitision rate of the device. Auto is recommended. The maximum negotiation rate varies with different channel bandwidth based on th	Country/Region	You can select the country or region to ensure that this device complies with the
When the device broadcasts an SSID, nearby wireless clients can detect the SSID.Broadcast SSIDWhen this parameter is set to Disable, the device does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to 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. 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. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the security of the wireless network mode of this device. Only wireless clients supporting the listed network mode can connect to the CPE.Network ModeIt specifies the wireless network mode can connect to the CPE.ChannelIt specifies channel in which this device operates.Channel ShiftIt specifies the shift of the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the device can exchange data on less interference channels.DFS FunctionWith this function enabled, the CPE will automatically detect the frequency of the radar system. When the CPE detects radar signals in the same frequency with the CPE itself, the CPE will automatically switch to another frequency to avoid interference with the radar system.Transmit PowerIt specifies the bandwidth of the operating channel of a wireless network. The channel BandwidthChannel BandwidthIt specifies that this device can switch its channel bandwidth based on the ambient environment.	SSID	It specifies the wireless network name.
Network Modesupporting the listed network mode can connect to the CPE.ChannelIt specifies channel in which this device operates.Auto indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.Channel ShiftIt specifies the shift of the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the device can exchange data on less interference channels.DFS FunctionWith this function enabled, the CPE will automatically detect the frequency of the radar system. When the CPE detects radar signals in the same frequency with the CPE itself, the CPE will automatically switch to another frequency to avoid interference with the radar system.Transmit PowerIt specifies the bandwidth of the operating channel of a wireless network. The channel bandwidth varies with different network modes. Please select it based on your actual operating environment.Channel BandwidthIt specifies wireless transmission rate of the device. Auto is recommended. The maximum negotiation rate varies with different channel bandwidths and network modes. Refer to the web UI of the device for details.	Broadcast SSID	When the device broadcasts an SSID, nearby wireless clients can detect the SSID. When this parameter is set to <b>Disable</b> , the device does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This to some extent enhances the
ChannelAuto indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.Channel ShiftIt specifies the shift of the channel center frequency. With this function enabled, the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the device can exchange data on less interference channels.DFS FunctionDynamic Frequency Selection. With this function enabled, the CPE will automatically detect the frequency of the radar system. When the CPE detects radar signals in the same frequency to avoid interference with the radar system.Transmit PowerIt 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. The channel bandwidth of the operating channel of a wireless network. The channel bandwidth varies with different network modes. Please select it based on your actual operating environment.Transmit RateIt specifies wireless transmission rate of the device. Auto is recommended. 	Network Mode	
Channel ShiftWith this function enabled, the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the device can exchange data on less interference channels.DFS FunctionDynamic Frequency Selection. With this function enabled, the CPE will automatically detect the frequency of the radar system. When the CPE detects radar signals in the same frequency to avoid interference with the radar system.Transmit PowerIt 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. The channel bandwidth varies with different network modes. Please select it based on your actual operating environment.Channel RateIt specifies transmission rate of the device. Auto is recommended. The maximum negotiation rate varies with different channel bandwidths and network modes. Refer to the web UI of the device for details.	Channel	Auto indicates that this device automatically changes to a channel rarely used in
DFS FunctionWith this function enabled, the CPE will automatically detect the frequency of the radar system. When the CPE detects radar signals in the same frequency with the CPE itself, the CPE will automatically switch to another frequency to avoid interference with the radar system.Transmit PowerIt 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 BandwidthIt specifies the bandwidth of the operating channel of a wireless network. The channel bandwidth varies with different network modes. Please select it based on your actual operating environment.Transmit RateIt specifies wireless transmission rate of the device. Auto is recommended. The maximum negotiation rate varies with different channel bandwidths and network modes. Refer to the web UI of the device for details.	Channel Shift	With this function enabled, the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the device can
Transmit PowerHigher number indicates wider WiFi coverage. Setting a proper transmit power helps improve the performance and security of the wireless network.Channel BandwidthIt specifies the bandwidth of the operating channel of a wireless network. The channel bandwidth varies with different network modes. Please select it based on your actual operating environment.Auto indicates that this device can switch its channel bandwidth based on the ambient environment.Transmit RateIt specifies wireless transmission rate of the device. Auto is recommended. The maximum negotiation rate varies with different channel bandwidths and network modes. Refer to the web UI of the device for details.	DFS Function	With this function enabled, the CPE will automatically detect the frequency of the radar system. When the CPE detects radar signals in the same frequency with the CPE itself, the CPE will automatically switch to another frequency to
Channel Bandwidthchannel bandwidth varies with different network modes. Please select it based on your actual operating environment.Autoindicates that this device can switch its channel bandwidth based on the ambient environment.Transmit RateIt specifies wireless transmission rate of the device. Auto is recommended. The maximum negotiation rate varies with different channel bandwidths and network modes. Refer to the web UI of the device for details.	Transmit Power	Higher number indicates wider WiFi coverage. Setting a proper transmit power
Transmit Rate The maximum negotiation rate varies with different channel bandwidths and network modes. Refer to the web UI of the device for details.	Channel Bandwidth	channel bandwidth varies with different network modes. Please select it based on your actual operating environment. Auto indicates that this device can switch its channel bandwidth based on the
Security Mode The device supports various security modes for network encryption, including	Transmit Rate	The maximum negotiation rate varies with different channel bandwidths and
	Security Mode	The device supports various security modes for network encryption, including

Name	Description
	None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2.
Isolate Client	<ul> <li>Enable: Clients connected to this wireless network cannot communicate with each other, which improves the wireless network security.</li> </ul>
	<ul> <li>Disable: Clients connected to this wireless network can communicate with each other. The default is Disable.</li> </ul>
Max. Number of Clients	This parameter specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID.
	If the number is reached, the wireless network rejects new connection requests from clients. This limit helps balance load among devices.

#### 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

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

#### WEP

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

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

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

#### Parameters description

Name	Description	
Authentication Type	It specifies the authentication type for the WEP security mode. The options include <b>Open</b> and <b>Shared</b> . The options share the same encryption process.	
	<ul> <li>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.</li> </ul>	
	<ul> <li>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.</li> </ul>	
	It specifies the WEP key for the <b>Open</b> or <b>Shared</b> encryption type.	
Default Key	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 <b>Open</b> or <b>Shared</b> 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

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

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK adopt a pre-shared key for authentication, while the CPE generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks.

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

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

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

Security Mode	WPA2-PSK ~	
Encryption Algorithm	None WEP	P&AES
	WPA-PSK	
-	WPA2-PSK Mixed WPA/WPA2-PSK	
Key Update Interval	WPA	s (Range: 60 to 99999)
Isolate Client	WPA2	
Max. Number of Clients	48	(Range: 1 to 128)
Save		

#### **Parameters description**

Name	Description
	It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK.
	<ul> <li>WPA-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA-PSK.</li> </ul>
Security Mode	<ul> <li>WPA2-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2-PSK.</li> </ul>
	<ul> <li>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.</li> </ul>

Name	Description
	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.
En annuations Alexanithus	<ul> <li>AES: It indicates the Advanced Encryption Standard.</li> </ul>
Encryption Algorithm	<ul> <li>TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the CPE is limited to 54 Mbps.</li> </ul>
	<ul> <li>TKIP&amp;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.</li> </ul>
Кеу	It specifies a pre-shared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.
	The value 0 indicates that a WAP key is not updated.

#### WPA and WPA2

WPA and WPA2 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.

Security Mode	WPA	~	
RADIUS Server	None WEP WPA-PSK WPA2-PSK		
RADIUS Port	Mixed WPA/WF	PA2-PSK	
Encryption Algorithm	WPA2 WPA2	IP UIKIP&	AES
RADIUS Password		~~~	
Key Update Interval	0	s (	Range: 60 to 99999)

#### **Parameters description**

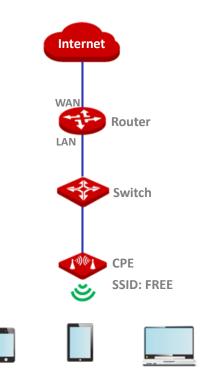
Name	Description
Security Mode	The <b>WPA</b> and <b>WPA2</b> options are available for network protection with a RADIUS server.
	<ul> <li>WPA: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA.</li> </ul>
	<ul> <li>WPA2: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2.</li> </ul>
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.
	It specifies the encryption algorithm corresponding to the selected security mode. The available options include <b>AES</b> , <b>TKIP</b> , and <b>TKIP&amp;AES</b> .
	<ul> <li>AES: It indicates the Advanced Encryption Standard.</li> </ul>
Encryption Algorithm	<ul> <li>TKIP: It indicates the Temporal Key Integrity Protocol.</li> </ul>
	<ul> <li>TKIP&amp;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.</li> </ul>
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.
, p	The value 0 indicates that a WAP key is not updated.

# 7.1.2 Set up a non-encrypted wireless network

#### **Network requirement**

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

#### **Network topology**



#### **Configuration procedure**

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

Enable Wireless	
Country/Region	China 🔻
* SSID	FREE
Broadcast SSID	Enable      Disable     Disable
Network Mode	11a/n •
Channel	40(5200MHz)
Channel Shift	Enable     Isable
Transmit Power	1dBm 10dBm
Channel Bandwidth	20MHz T
Transmit Rate	Auto 🔻
* Security Mode	None •
Isolate Client	Enable
Max. Number of Clients	48 (Range: 1 to 128)
	Save Cancel

----End

### Verification

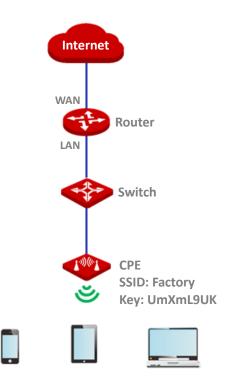
Wireless devices can connect to the wireless network whose SSID is **FREE** without a password.

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

#### **Network requirement**

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

#### **Network topology**



#### **Configuration procedure**

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

Basic	
Enable Wireless	?
Country/Region	China •
* SSID	Factory
Broadcast SSID	Enable      Disable     Disable
Network Mode	11a/n •
Channel	40(5200MHz) •
Channel Shift	○ Enable
Transmit Power	1dBm 10dBm
Channel Bandwidth	20MHz •
Transmit Rate	Auto •
* Security Mode	WPA2-PSK •
* Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
<b>*</b> Key	> <sub>&gt;per</sub> et
Key Update Interval	0 s (Range: 60 to 99999, 0 indicates that no key
Isolate Client	Update is performed.)
Max. Number of Clients	48 (Range: 1 to 128)
	Save

#### ----End

## Verification

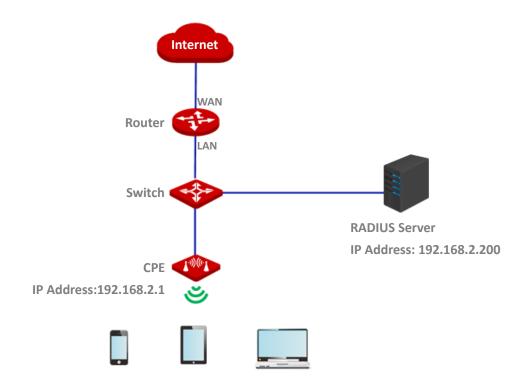
Wireless devices can connect to the wireless network named **Factory** with the password **UmXmL9UK**.

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

#### **Network requirement**

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

#### **Network topology**



#### **Configuration procedure**

I. 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**.
- The SSID of the CPE is hot\_spot, security mode is WPA2, and the encryption algorithm is AES.
- **1.** Log in to the web UI of CPE, choose **Wireless** > **Basic** to enter the configuration page.
- 2. Change the value of the SSID text box to **hot\_spot**.

- 3. Set Security Mode to WPA2.
- 4. Set RADIUS Server, RADIUS Port, and RADIUS Password to 192.168.0.200, 1812, and 12345678 respectively.
- 5. Set Encryption Algorithm to AES.
- 6. Click Save.

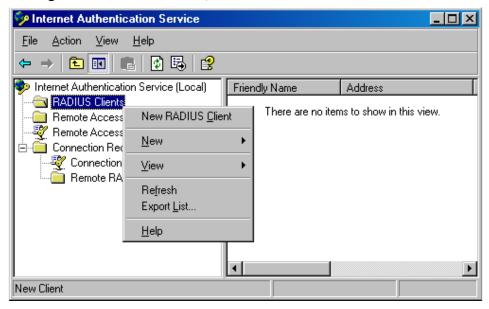
Basic	2
Enable Wireless	
Country/Region	China •
* SSID	hot_spot
Broadcast SSID	Enable      Disable
Network Mode	11a/n •
Channel	Auto 🔻
Channel Shift	Enable     Isable
Transmit Power	1dBm 10dBm
Channel Bandwidth	20MHz •
Transmit Rate	Auto 🔻
* Security Mode	WPA2 •
* RADIUS Server	192.168.0.200
* RADIUS Port	1812
* Encryption Algorithm	● AES ○ TKIP ◎ TKIP&AES
* RADIUS Password	
Key Update Interval	0 s (Range: 60 to 99999, 0 indicates that no key
Isolate Client	<ul> <li>Update is performed.)</li> <li>Enable</li> <li>Disable</li> </ul>
Max. Number of Clients	48 (Range: 1 to 128)
	Save

#### II. Configure the RADIUS server



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 CPE) and the IP address of the CPE, and click **Next**.

I ype a friendly name and	either an IP Address or DNS nam	ne for the client.
Friendly name:	root	2
Client address (IP or DNS)	):	
192.168.2.1		⊻erify
IP add	lress of the CPE	

(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 p vendor of the RADIUS client.	olicies based on the client vendor attribute, specify the
<u>Client-Vendor:</u>	
RADIUS Standard	-
<u>S</u> hared secret:	NAXXXXXXXX
Confirm shared secret:	XXXXXXXX
<u>R</u> equest must contain the l	Message Authenticator attribute
	Password same as that specified by
	RADIUS Password on the CPE.
	< <u>B</u> ack Finish Cancel

- 2. Configure a remote access policy.
  - (1) Right-click Remote Access Policies and choose New Remote Access Policy.

Internet Authentication S	ervice		_ 🗆 🗵
<u>File Action View H</u> elp			
⇔ → 🗈 🖬 🔮 🔩	12		
Internet Authentication Servic	e (Local)	Name	Order
- ADIUS Clients		S Connections to Microsoft Routing and Remote A	1
		S Connections to other access servers	2
🖅 🍈 Connection Request Pr	New Remote Access Po	licy	
1 - 1 - 1 - 1	New	•	
1	⊻iew		
	Refresh		
	Export List		
	<u>H</u> elp		
New Remote Access Policy			

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

Internet Authentication Service		, <u>– – ×</u>
Ele Action New Remote Access Policy	Wizard	×
<ul> <li>Internet Au Bemo Pierce</li> <li>Conne</li> </ul>	Welcome to the New Remote Access Policy Wizard	ler
	Cance	
灯 Start 🛛 🕑 进 👘 Internet Aut	henticati 🚊 dnsmgmt - [DNS\WIN200	🌯 📵 2:36 PM

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

New Remote Acces	ss Policy Wizard	×
<b>Policy Configur</b> The wizard c	ration Method an create a typical policy, or you can create a custom policy.	
	vant to set up this policy?	
<ul> <li>Use the wizard to set up a typical policy for a common scenario</li> <li>Set up a custom policy</li> </ul>		
	hat describes this policy.	
<u>P</u> olicy name:	root Example: Authenticate all VPN connections.	
	Example. Addrendeate all VEN connections.	
	< <u>B</u> ack <u>N</u> ext> Cancel	

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

Remote Access Policy Wizard		
Access Method Policy conditions are based on the meth	od used to gain access to the network.	ŷ
Select the method of access for which you	u want to create a policy.	
C <u>v</u> pn		
Use for all VPN connections. To cre previous page, and select Set up a	eate a policy for a specific VPN type, go bac custom policy.	ck to the
○ <u>D</u> ial-up		
Use for dial-up connections that use Digital Network (ISDN) line.	e a traditional phone line or an Integrated Se	ervices
○ Wireless		
Use for wireless LAN connections o	only.	
€ Ethernet		
Use for Ethernet connections, such	as connections that use a switch	

(5) Select Group and click Add.

ew Remote Access Policy Wizard	
User or Group Access You can grant access to individual groups.	l users, or you can grant access to selected
Grant access based on the following:	
C User	
User access permissions are spec	cified in the user account.
Group name:	Add
	<u>H</u> emove
	<u>≺B</u> ack <u>N</u> ext> Cancel

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

elect Groups	?
Select this object type:	
Groups	<u>O</u> bject Types
From this location:	
comba.com	Locations
Enter the object names to select (e	axamples):
802.1x	
	•
Advanced	OK Cancel

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

w Remote Access Policy Wizard	
Authentication Methods EAP uses different types of security	v devices to authenticate users.
Select the EAP type for this policy.	
<u>I</u> ype:	
Protected EAP (PEAP)	Configure
	< <u>B</u> ack <u>N</u> ext> Cancel

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

New Remote Access Policy Wizard		
6	Completing the New Remote Access Policy Wizard	
U	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.	
	< <u>B</u> ack Finish Cance	

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

root Properties ?X		
Settings		
Specify the conditions that connection requests must match.		
Policy conditions: NAS-Port-Type matches "Ethernet" AND Windows-Groups matches "COMBA/802:1X"		
A <u>d</u> d <u>E</u> dit <u>R</u> emove		
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.		
Edit <u>P</u> rofile		
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		
OK Cancel Apply		

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

NAS-Port-Type		? ×
Available types:		Selected types:
PIAFS SDSL - Symmetric DSL Sync (T1 Line) Token Ring Virtual (VPN) Wireless - IEEE 802.11 Wireless - Other X.25 X.75 xDSL - Digital Subscrib ▼	Add >> << Remove	Ethernet Wireless - IEEE 802.11
		OK Cancel

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

Dial-in Profile		
Dial-in Constraints Authentication	IP Encryption	Multilink   Advanced
Select the authentication n	nethods you want to all	ow for this connection.
Microsoft Encrypted	Authentication version nge password after it ha	
	Authentication (MS-CH	
Encrypted authentica	ation (CHAP)	
Unencrypted authen	tication (PAP, SPAP)	
Unauthenticated access		
Allow clients to conn method.	ect without negotiating	an authentication
1		
	ОК	Cancel Apply

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

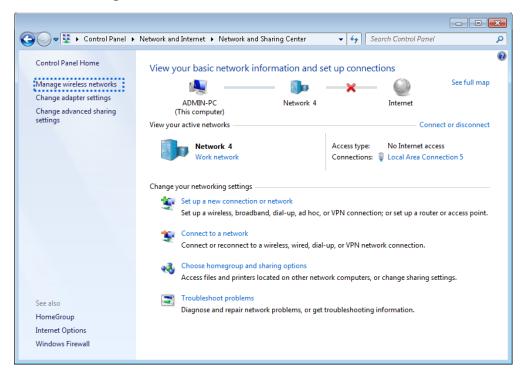
3. Configure user information. Create a user and add the user to group **802.1x**.

III. Configure your wireless device

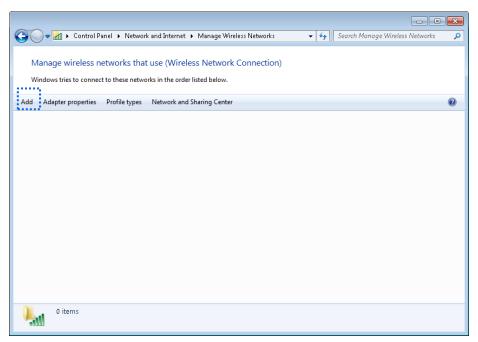


Windows 7 is taken as an example to describe the procedure.

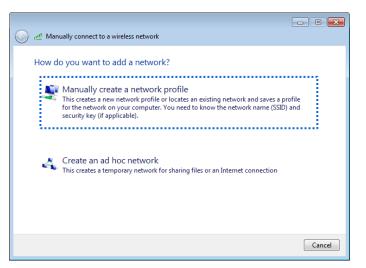
1. Choose Start > Control Panel, click Network and Internet, click Network and Sharing Center, and click Manage wireless networks.



2. Click Add.



3. Click Manually create a network profile.



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

	for the wireless network yo	ou want to add
Network name: Security type:	hot_spot WPA2-Enterprise	Same as the security mode of the SSID of th
Encryption type:	AES	✓ CPE
Security Key:		Hide characters
	tion automatically the network is not broadcasting select this option, your computer's	privacy might be at risk.

5. Click Change connection settings.

	- • •
🕞 🔐 Manually connect to a wireless network	
Successfully added hot_spot	
<ul> <li>Change connection settings</li> <li>Open the connection properties so that I can change the settings.</li> </ul>	
open die connection properties so daar ean enange die settings.	
· · · · · · · · · · · · · · · · · · ·	
	Close

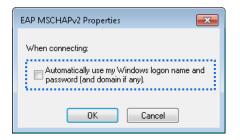
6. Click the Security tab, select Microsoft: Protected EAP (PEAP), and click Settings.

hot_spot Wireless Netw	ork Properties	×
Connection Security		
÷	) 	
Security type:	WPA2-Enterprise	
Encryption type:	AES 🔹	
Choose a network au		
Microsoft: Protected	EAP (PEAP)	
time I'm logged on		
Advanced settings		
	OK Can	icel

7. Deselect Validate server certificate and click Configure.

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted <u>R</u> oot 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 East Reconnect     Enforce Network Access Protection     Disconnect if server does not present cryptobinding TLV     Enable Identity Privacy
OK Cancel

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



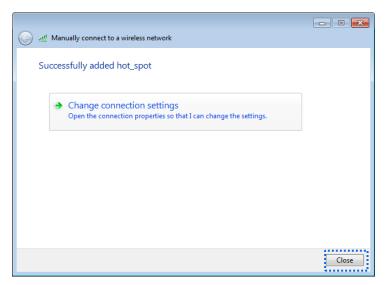
#### 9. Click Advanced settings.

hot_spot Wireless Netw	ork Properties	×
Connection Security		
S <u>e</u> curity type:	WPA2-Enterprise	<b>•</b>
Encryption type:	AES	<b>—</b>
Choose a network aut	hentication method:	
Microsoft: Protected		ettings
Remember my creative I'm logged on	dentials for this connection ea	ch
Advanced settings		
	ОК	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):
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.



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

Currently connected to: Network 4 Internet access	<b>*</b> 3 <b>=</b>
Wireless Network Connection	^
hot_spot	lle.
Connect automatically	<u>C</u> onnect
	-
Open Network and Sharing	Center

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

Windows Security
Network Authentication Please enter user credentials
OK Cancel

----End

## Verification

Wireless devices can connect to the wireless network **hot\_spot**.

# 7.2 Advanced

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

Advanced		
WMM	Enable	O Disable
APSD	⊖ Enable	O Disable
Minimum RSSI Threshold	⊖ Enable	O Disable
Preamble	○ Short Preamble	● Long Preamble
Transparent Bridge	Enable	○ Disable
iMAX	⊖ Enable	O Disable
Signal Transmission	Overage-oriented	○ Capacity-oriented
TPC	Enable	○ Disable
Signal Reception Level	Auto	~
Transmission Distance	15	Auto km (Range: 0.1 to 20, default: 15)
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)
	Save	Cancel

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

#### **Parameters description**

Name	Description
WMM	WMM (Wi-Fi Multi-media) is a wireless QoS (Quality of Service) protocol making packets with higher priorities to be transmitted earlier. This ensures better QoS of voice and video applications over wireless networks.
APSD	APSD (Automatic Power Save Delivery) is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
Minimum RSSI Threshold	It specifies the minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device. If there are multiple CPEs in a network, setting a proper value helps wireless
	devices connect to WiFi network with better WiFi signal. It specifies a group of bits located at the beginning of a packet to enable a
Preamble	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.
Transparent Bridge	With this function enabled, the CPE can achieve bidirectional transparent transmission, solving the problem that the NVR cannot detect IP cameras.
	Only available in AP, Client, and Universal Repeater modes.
IMAX	<ul> <li>IMAX is IP-COM's proprietary Time Division Multiple Access (IMAX) polling technology. It assigns time slots for each device communication to avoid the "hidden node" problem, which occurs when a node is visible from a wireless AP, but not from other nodes communicating with the originating AP.</li> <li>IMAX improves overall performance in Point-to-MultiPoint (PtMP) installations and noisy environments, because it reduces latency, and offers better tolerance against interference. Because of its advantages, IMAX also increases the maximum possible number of users that can associate with an AP that uses IMAX.</li> <li>IMAX is enabled, the device operates in IMAX mode and only accepts connections from IMAX devices. And you cannot connect standard Wi-Fi devices a use a batter tolerance to the CPE.</li> </ul>
	devices, such as laptops, tablets, or smart phones, to the CPE.
Signal Transmission	It specifies the wall penetrating capability of the CPE.

Name	Description
	<ul> <li>Coverage-oriented: With less interference nearby, this mode enables the device to cover wider area.</li> </ul>
	<ul> <li>Capacity-oriented: With strong interference nearby, this mode improves the device's anti-interference capability.</li> </ul>
ТРС	The Transmit Power Control (TPC) function decreases the TX power of this device automatically to improve the negotiation rate when the two devices are too close.
	By default, when the received signal strength is greater than -25 dBm, the CPE decreases its TX power. The received signal strength can be checked on the <b>Status</b> > <b>Wireless Status</b> page.
Signal Reception Level	It is used to adjust the signal reception level. A higher level leads to better signal reception capability and more wireless networks can be searched, but lower throughput. Adjust the level based on your actual situation.
Transmission Distance	It specifies the wireless transmission distance of this device. You can set it based on the actual installation distance.
	It specifies the interval at which this device sends Beacon frames.
Beacon Interval	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.
	It specifies the threshold of a fragment. The unit is byte.
Fragment Threshold	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. If the transmission fails, this device resends 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 fragments, so as to increase the frame throughput.
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

Name	Description
	at one Beacon interval.
Signal LED1/2/3 Threshold	The device uses three signal LED indicators to indicate the received signal strength in an intuitive way, and allows you to customize the threshold for triggering each signal LED indicator to light up.
mesnoù	The default threshold for LED1, LED2, and LED3 are - <b>90, -80</b> , and - <b>70</b> respectively.

# 7.3 Access control

# 7.3.1 Overview

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

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

To access the page, choose Wireless > Access Control.

Access Cor	ntrol			
	SSID	IP-COM_158810		?
	Access Control			
	Mode	Disallow     O     Allow		
	MAC Address	12:12:12:12:12:12	Add Add online devic	es
SN	MAC Addres	ss Status	Operation	
1	12:12:12:12:1	2:12 Enable	e 🔟	
Ac	cess Control List	Save Cancel		

#### **Parameters description**

Name	Description
SSID	It specifies the SSID of this device. With the rule enabled, clients connected to the network with this SSID will be controlled by the rule.
Access Control	It specifies whether to enable the Access Control function.
Mode	<ul> <li>It specifies the mode for filtering MAC addresses.</li> <li>Allow: It indicates that only the wireless clients on the access control list can connect to the WiFi network of the CPE.</li> </ul>
	<ul> <li>Disallow: It indicates that only the wireless clients on the access control list cannot connect to the WiFi network of the CPE.</li> </ul>

# 7.3.2 Example of configuring access control

#### **Network requirement**

A wireless network whose SSID is **IP-COM\_158810** has been set up in an estate. Only specific members in this estate are allowed to connect to the wireless network.

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

#### **Configuration procedure**

- 1. Choose Wireless > Access Control to enter the configuration page.
- 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**.



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

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

Access Co	ontrol				?
	SSID II	P-COM_15881	0		
	Access Control				
	Mode 🤇	Disallow	Allow		
	MAC Address	C8:3A:35:00:0	)0:03	Add Add online devices	
SN	MAC Address		Status	Operation	
1	C8:3A:35:00:00:0	01	Enable		
2	C8:3A:35:00:00:0	02	Enable	Î	
3	C8:3A:35:00:00:0	03	Enable	Ē	
		Save	Cancel		

----End

## Verification

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

# 8 Advanced

# 8.1 LAN rate

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

When you change the settings, ensure that the LAN speed and duplex mode of the port of the CPE is the same as that of peer device. By default, the LAN speed settings of the LAN port is **Auto Negotiation**. CPE6S is used for illustration here.

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

AN Rate	
PoE/LAN Speed	Auto Negotiation
LAN2 Speed	Auto Negotiation
LAN3 Speed	Auto Negotiation
LAN4 Speed	Auto Negotiation
	Save

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

Name	Description
	same time.

- Č \_\_\_\_\_\_ Tip

The low speed mode can improve the transmission distance of the port. If you want to extend the PoE power supply distance, you can change the speed mode to a low speed mode, such as 10 Mbps full duplex. And ensure that the speed mode for peer port is also 10 Mbps full duplex or auto negotiation.

# 8.2 Diagnose

You can use the diagnosis tools for troubleshooting. The CPE supports the following tools:

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

# 8.2.1 Site Survey

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

Configuration procedure:

- 1. Choose Advanced > Diagnose to enter the configuration page.
- 2. Select **Site Survey** in the **Diagnose** drop-down list menu.

#### ----End

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

Diagnose					
	Diagnose	Site Survey	•		
ID	SSID	MAC Address	Channel	Security	Signal Strength
1	IP-COM_2	D8:38:0D:15:88:09	165	None	lin.
2	IP-COM_F03A60	D8:38:0D:F0:3A:65	40	None	lite.
3	0124_7C98	D8:32:14:79:0A:B4	40	Mixed WPA/WPA2- PSK	lin.

## 8.2.2 Ping

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

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

Configuration procedure:

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

nose		
Diagnose	Ping •	]
IP Address	Manual 🔻	]
IP Address/Domain Name	cn.bing.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.

IP Address		Time	TTL
202.89.233.101		41.513ms	116
202.89.233.100		42.262ms	116
202.89.233.100		45.226ms	116
202.89.233.101		40.738ms	116
10 • Datas/Page 4 data in total			
		4 of 4 packets rece	ived, 0.00% loss0.00%
Min. 40.738 ms	Average 42.43 ms	Max	. 45.226 ms

# 8.2.3 Traceroute

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

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

Configuration procedure:

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

#### 4. Click Start.

agnose				
Diagnose	Traceroute	•		
IP Address/Domain Name	cn.bing.com			
	Start			

#### ----End

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

SN	IP Address	Time
1	192.168.5.1	3.099 ms 6.053 ms 3.305 ms
2	172.16.200.1	8.645 ms 3.270 ms 9.431 ms
3	192.168.20.1	4.845 ms 5.009 ms 4.968 ms
4	192.168.21.254	5.200 ms 4.471 ms 3.033 ms
5	100.64.0.1	20.525 ms 15.491 ms 9.747 ms
6	59.38.106.221	18.160 ms 9.391 ms 6.092 ms
7	183.56.65.46	12.042 ms
8	202.97.65.97	44.627 ms
9	36.110.244.18	42.582 ms
10	220.181.17.86	40.299 ms 43.297 ms 39.520 ms
10 <b>v</b> Da	tas/Page 10 data in total	

# 8.2.4 Speed test

You can use the **Speed Test** to test the throughput between two CPEs in the same network. The test requires that both sides support the **Speed Test** function.

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

Diagno	se		
	Diagnose	Speed Test	•
	↑ AVG RX	👃 AVG TX	🕼 AVG Total
	0 Mbps	0 Mbps	0 Mbps
		Client     Server	
	IP Address of Peer AP	Manual	Ŧ
	IP Address		
	HTTP Port	80	
	User Name		
	Password		
	Test Group	10	(Range: 1 to 20)
	Direction	Bidirectional	T
	Time	30	s (Range: 1 to 60)
		Start	

### **Parameters description**

Name	Description
IP Address of Peer AP	It specifies the LAN IP address of peer CPE. You can enter it manually or select an IP address of the peer AP from the drop-down list if there are peer CPEs connected to the CPE.
IP Address	If the <b>IP Address of Peer AP</b> is set to <b>Manual</b> , you need to enter the LAN IP address of peer CPE in the box manually.
HTTP Port	It specifies the HTTP service port number of peer device, which is used to establish speed test connection based on TCP/IP. Default: 80. You are recommended to keep the default value.
User Name	It specifies the login user name and password of poor device
Password	It specifies the login user name and password of peer device.

Test Group	It specifies the number of test connection launched by the client.
	It specifies the test speed direction.
Direction	<ul> <li>RX (Receive): only test the speed that the peer device transmits data to this device.</li> </ul>
	<ul> <li>TX (Transmit): only test the speed that this device transmits data to peer device.</li> </ul>
	<ul> <li>Bidirectional: test both transmit and receive speed between the two CPEs</li> </ul>
Time	It specifies the period of speed test.
AVG RX	It displays the average received rate.
AVG TX	It displays the average transmitted rate.
AVG Total	It displays the average total rate.

# Example of configuring the speed test

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

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

Assume that:

The IP address of CPE1 is **192.168.2.1**, and both the login user name and password are **admin**.

Configuration procedure:

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

Diagno	ose		
	Diagnose	Speed Test	v
	个 AVG RX	👃 AVG TX	👫 AVG Total
	0 Mbps	0 Mbps	0 Mbps
		● Client   ○ Server	
	IP Address of Peer AP	Manual	v
	IP Address	192.168.2.1	
	HTTP Port	80	
	User Name	admin	
	Password	admin	
	Test Group	10	(Range: 1 to 20)
	Direction	Bidirectional	•
	Time	30	s (Range: 1 to 60)
		Start	

### ----End

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

Diagn	ose		
	Diagnose	Speed Test	¥
	1 AVG RX	👃 AVG TX	🕼 AVG Total
	103.28 Mbps	105.17 Mbps	208.45 Mbps

# 8.2.5 Spectrum Analysis

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

Configuration procedure:

- 1. Choose Advanced > Diagnose to enter the page.
- 2. Select Spectrum Analysis from the Diagnose drop-down list menu.
- 3. Select the Frequency Band range you want to test from the drop-down list.
- 4. Click Start.

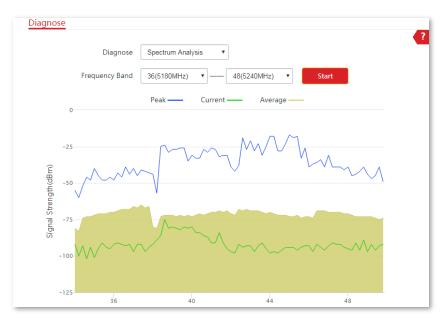
Diagnose	
	?
Diagnose	Spectrum Analysis 🔹
Frequency Band	36(5180MHz) ▼ 48(5240MHz) ▼ Start

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

All wireless connections will be terminat	ated when the spectr	rum analysis is launc	hing on the device!	Please click OK to Start.
	ок	Cancel		

#### ----End

The diagnosis result is displayed as follows.



# 8.3 Bandwidth control

# 8.3.1 Overview

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

The bandwidth control function allows you to assign proper bandwidth to connected clients, ensuring that the limited bandwidth is used to effectively access resources over the internet.

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

Remark Address Range						
Address Range						
	192.168.2.	~ 192.168.2				
ax. Upload Rate			Mbps	T		
Download Rate			Mbps	T		
	Add					
		•				
rk IP Addres	ss Range	Max. Upload	Rate	Max. Download Rate	e Status	Action
	ax. Upload Rate Download Rate rk IP Addres	Download Rate	Download Rate	Download Rate Mbps	Download Rate	Download Rate

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

# 8.3.2 Example of configuring bandwidth control

### **Network requirement**

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

Assume that: The maximum upload rate of each device connected to the WiFi network of the CPE is **5 Mbps**, and download rate is **10 Mbps**. And the IP address range of the devices connected to the WiFi network is **192.168.2.100** to **192.168.2.150**.

### **Configuration procedure**

- 1. Choose Advanced > Bandwidth Control to enter the configuration page.
- 2. Enter a remark (optional), such as Office1.
- 3. Specify an IP address range, which are **100** and **150** in this example.
- 4. Specify the maximum upload rate and download rate respectively, which are **5** and **10** in this example.

Bandwidth Control					
Remark	Office 1				
IP Address Range	192.168.2. 100 ~ 192.168.2	. 150			
Max. Upload Rate	5	Mbps •			
Max. Download Rate	10	Mbps •			
	Add				
ID Remark IP Addres	s Range Max. Upload	Rate N	lax. Download Rate	Status	Action

#### 5. Click Add.

#### ----End

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

ID	Remark	IP Address Range	Max. Upload Rate	Max. Download Rate	Status	Action
1	Office 1	192.168.2.100~192.168.2.150	5Mbps	10Mbps	€Enable	
10 🔻	Datas/Pag	ge 1 data in total				

# Verification

For a device whose IP address is within the range of 192.168.2.100 to 192.168.2.150, its maximum upload rate is 5 Mbps and its maximum download rate is 10 Mbps.

# 8.4 Port forwarding

# 8.4.1 Overview

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

If computers are connected to the CPE to form a LAN and access the internet through the CPE, internet users cannot access the hosts on the LAN. Therefore, the servers, such as web servers, email servers, and FTP servers, on the LAN are inaccessible to internet users.

To enable internet users to access a LAN server, enable the port forwarding function of the CPE, and map one service port to the IP address of the LAN server. This enables the CPE to forward the requests arriving at the port from the internet to the LAN server, and avoid the attacks from the WAN.

ort Foi	rwarding						
	Internal IP Address						
	Internal Port	23					
	External Port	23					
	Protocol	TCP&UDP	•				
	Application	Telnet	Ŧ				
	l	Add					
ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action

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

#### **Parameters description**

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

Name	Description
	After you select an <b>Application</b> , this option will be auto populated. You can also customize it.
Protocol	It specifies the protocol type of the selected applications. Select <b>TCP&amp;UDP</b> when you are not sure.
Application	It specifies the application services established in LAN. The device provides some common services. After you select an application, the internal and external ports will be populated.
Action	Click 🗐 to delete the rule.

# **8.4.2** Example of configuring port forwarding

### **Network requirement**

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

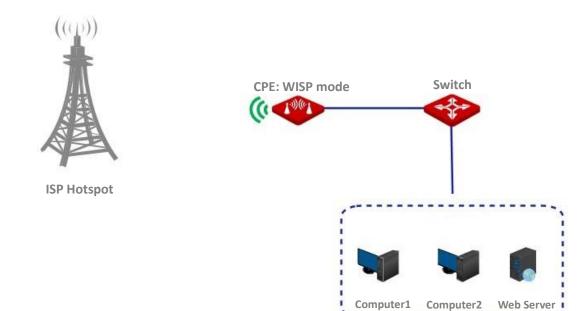
**Requirement**: Family members who are not at home can visit the resources on the web server in LAN over the internet.

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

Assume that:

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

# **Network topology**



# **Configuration procedure**

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

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

Internal IP Address	192.168.2.100	
Internal Ir Address	102.100.2.100	
Internal Port	80	
External Port	80	
Protocol	TCP&UDP •	
Application	HTTP •	
	(AAMO)A	
	Add Ju	

#### ----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	Î
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://202.105.11.22:80**.



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

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

# 8.5 MAC filter

# 8.5.1 Overview

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

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

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

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

Mode	Allow	•		
Remark				
MAC Address				
Time	00 • 00 • 00	) ▼:00 ▼		
Date	Mon. Tue.	Wed.	Thur.	
	Fri. Sat.	Sun. 🗌 Eve	ry Day	
	Add			

#### **Parameters description**

Name	Description
	It specifies the mode of MAC filter rule. <ul> <li>Disable: Disable the MAC Filter function.</li> </ul>
Mode	<ul> <li>Allow: Allow the devices with the MAC addresses in the list to access the internet via the CPE, and disallow the other devices to access the internet via the CPE.</li> </ul>
	<ul> <li>Disallow: Disallow the devices with the MAC addresses in the list to access the internet via the CPE, and allow the other devices to access the internet via the CPE.</li> </ul>
Remark	It specifies the additional information of the rule.

Name	Description
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 $\widehat{\blacksquare}$ to delete the rule.

# 8.5.2 Example of configuring MAC filter

### **Network requirement**

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

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

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

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

### **Configuration procedure**

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

MAC Filter	2
Mode	Allow
Remark	Dad's smartphone
MAC Address	CC:3A:61:71:1B:6E
Time	09 ▼:00 ▼~17 ▼:00 ▼
Date	🖉 Mon. 🖉 Tue. 🖉 Wed. 🕑 Thur.
	🖉 Fri. 🗌 Sat. 📄 Sun. 📄 Every Day
	Add 🛺

#### ----End

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

ID	Remark	MAC Address	Time	Mode	Status	Action
1	Dad's smar	CC:3A:61:71:1B:6E	Mon. 、Tue. 、Wed. 、Thur. 、Fri. 09:00- 17:00	Allow	<b>∢</b> Enable	Ī
2	Mum's lapt	CC:3A:61:75:1F:3E	Mon. 、Tue. 、Wed. 、Thur. 、Fri. 09:00- 17:00	Allow	✓ Enable	Ē
10 🔻	Datas/Page	2 data in total				

# Verification

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

# 8.6 Network service

# 8.6.1 DDNS

### **Overview**

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

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

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.

Network Service		2
DDNS	$\bigcirc$	
Service Provider	3322.org • <u>Re</u>	<u>egister</u>
User Name		
Password		
Domain Name		

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

#### **Parameters description**

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

# **Example of configuring DDNS**

### Network requirement

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

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

Assume that:

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

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

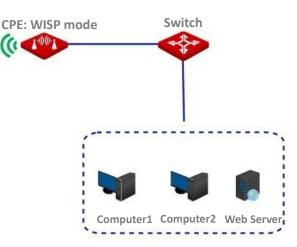
The registered domain name information is shown as follows:

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

### Network topology



**ISP Hotspot** 



### Configuration procedure

- I. Set up the DDNS function
- 1. Choose Advanced > Network Service to enter the configuration page.
- 2. Enable the **DDNS** function.

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

Network Service		?
DDNS		
Service Provider	Dyndns •	Register
User Name	ipcom	
Password	••••	
Domain Name	ipcom.dyndns.com	

II. Set up the port forwarding function

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

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

Internal IP Address	192.168.2.100	
Internal Port	80	
External Port	80	
Protocol	TCP&UDP •	
Application	HTTP <b>v</b>	

----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	Ē
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://ipcom.dyndns.com:80.



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

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

# 8.6.2 Remote web management

### **Overview**

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

Generally, only the devices connected to the LAN port or the wireless network of the CPE can access the web UI of the CPE.

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

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

Remote Web Management	
IP Address	All
Port	8080

#### **Parameters description**

Name	Description	
Remote Web Management	It specifies whether to enable the remote web management function.	
	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 the CPE remotely.	
IP Address	<ul> <li>For security, this option is not recommended.</li> <li>Manual: It indicates that only the device with specified IP address can manage the CPE remotely. If the CPE belongs to a LAN, the gateway address (a public IP address) of the CPE should be entered.</li> </ul>	
	It specifies the port number used for remote management of device. Default: <b>8080</b> . You can change it if necessary.	
Port	Ports 1 to 1024 have been used by well-known services. To avoid port conflicts, you can set the port number to one between 1025 and 65535. Then you can access the device from WAN by visiting an address in the form of http://WAN IP address:port number. If the DDNS function is enabled on the CPE, you can access the device by visiting an address in the form of http://Domain name of WAN port:port number.	

### Example of configuring remote web management

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

#### Network requirement

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

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

Assume that:

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

#### Configuration procedure

- 1. Choose Advanced > Network Service to enter the configuration page .
- 2. Enable the **Remote Web Management** function.
- 3. Set IP Address to Manual.
- 4. Enter the IP address of the computer which is allowed to access the device on WAN, which is **202.105.88.77** in this example.
- 5. Enter the port number, which is **8080** in this example.
- 6. Click **Save** in the bottom of this page.

Remote Web Management	
IP Address	Manual 🔻
Enter an IP address	202.105.88.77
Port	8080

#### ----End

#### Verification

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

# 8.6.3 Reboot schedule

### **Overview**

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

### **Configuration procedure**

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

Reboot Schedule	
Time	03:00
Date	🖉 Mon. 🖉 Tue. 🖉 Wed. 🖉 Thur.
	🗹 Fri. 🕑 Sat. 🕑 Sun. 🕑 Every Day

#### ----End

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

# 8.6.4 Login timeout interval

If you log in to the web UI of the CPE and perform no operation within the login timeout interval, the CPE logs 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 receiving network event alarms.

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

### **SNMP Management Framework**

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

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

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

### **Basic SNMP Operations**

The device allows the following basic SNMP operations:

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

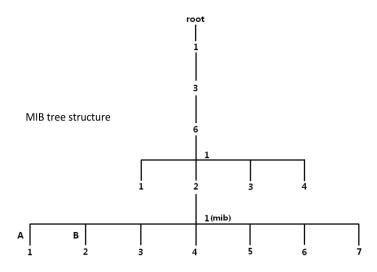
### **SNMP** Protocol Version

The 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.



### **Parameters description**

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

SNMP Agent	
Device Name	iLBE-5ACV1.0
Read Community	public
Read/Write Community	private
Location	ShenZhen

Name	Description
SNMP Agent	It specifies whether to enable the SNMP agent function of the CPE. 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 theCPE. $-\overleftarrow{g}^{-}-Tip$ It is recommended that you change the device name so that you can easily identify the CPE when managing it using SNMP.
Read Community	It specifies the read password shared between SNMP managers and this SNMP agent. The default password is <b>public</b> . The SNMP agent function of the device allows an SNMP manager to use the password to read variables in the MIB of the device.
Read/Write Community	It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is <b>private</b> . The SNMP agent function of the device allows an SNMP manager to use the password to read/write variables in the MIB of the device.
Location	It specifies the location where the CPE is used. You can change the location as required.

# Example of configuring the SNMP function

### Network requirement

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



### Configuration procedure

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

SNMP Agent	
Device Name	iLBE-5ACV1.0
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 CPE periodically pings target IP address to check the network connectivity and identify whether the device malfunctions. If it malfunctions, the CPE will reboot automatically to ensure the network performance.

Configuration procedure:

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

Ping Watch Dog		
IP Address	127.0.0.1	
Ping Interval	300	Range : 20-86400 s
Ping Startup Delay	300	Range : 180-86400 s
Threshold of Lost Packets	3	

#### ----End

#### **Parameters description**

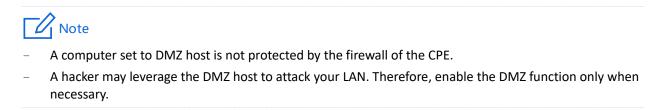
Name	Description
Ping Watch Dog	It specifies whether to enable the Ping Watch Dog function.
IP Address	It specifies the target IP address that the CPE pings.
Ping Interval	It specifies the interval at which the CPE transmits packets to ping the target IP address.
Ping Startup Delay	It specifies the delay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

# 8.6.7 DMZ host

### **Overview**

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

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.



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

DMZ Host	t 💽
DMZ Host IP Address	5

#### **Parameters description**

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

# **Example of configuring DMZ host**

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

#### Network requirement

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

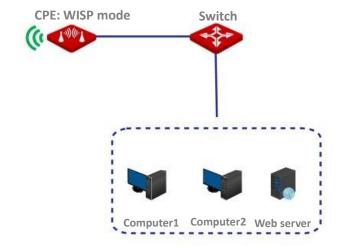
You can use DMZ Host function to solve the problem.

Assume that:

- The WAN IP address of the device is **202.105.106.55**.
- The IP address of the internal web server is 192.168.2.100

- The port number is: **9999**.
- Network topology





### Configuration procedure

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

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

#### ----End

### Verification

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

If the <u>DDNS</u> function is enabled, you can visit an address in the form of **Protocol** name://domain name:9999.



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

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

# 8.6.8 Telnet service

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

	DMZ Host	$\bigcirc$	
Tel	net Service		
	UPNP	$\bigcirc$	
Hardware	Watch Dog		
	STP	$\bigcirc$	
		Save	Cancel

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

# 8.6.9 UPnP

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

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

DMZ Host	$\bigcirc$
Telnet Service	
UPNP	$\bigcirc$
Hardware Watch Dog	
STP	$\bigcirc$
	Save

# 8.6.10 Hardware watch dog

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



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

# 8.6.11 STP

Spanning Tree Protocol (STP) is a network protocol standardized by IEEE 802.1d. It helps establish a loop-free logical topology for Ethernet network, and allows a network design to include backup links to provide fault tolerance if an active link fails. The STP-enabled device creates a spanning tree within a network of connected layer-2 bridges, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. So that it prevents packets from continued proliferation and endless loop in a loop network to avoid reducing the capability of processing packets caused by receiving duplicate packets.

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



# 9 Tools

# 9.1 Date & time

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

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

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

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

#### -) - Tip

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

# 9.1.1 Synchronized with the Internet

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

For details about how to connect the CPE to the internet, refer to the configuration procedure of corresponding mode in <u>Quick Setup</u>.

Configuration procedure:

- 1. Choose **Tools** > **Date & Time** to enter the configuration page.
- 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
Time Interval	30 minutes •
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei 🔹
	Save

----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** to enter the configuration page.
- 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		2
	Time Settings	<ul> <li>Synchronized with the Internet</li> <li>Manual</li> </ul>
	Date & Time	2019 Y 05 M 30 D 17 h 04 m 18 s
		Synchronize with PC Time
		Save

----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.

# - Тір

When the CPE reboots, the current connections will be disconnected. Perform this operation when the CPE is **NOT** busy.

Configuration procedure:

1. Choose **Tools** > **Maintenance** to enter the configuration page.

#### 2. Click Reboot.

Maintenance			
			<u> </u>
	Reboot Device	Reboot	
		All connections will disconnect during reboot.	
Reset to F	actory Settings	Reset	
		All configurations will restore to default factory setting after reset.	
Upg	grade Firmware	Upgrade	
		Current Software Version: V1.0.0.2(4045) ; Release Date: 2019-03-18 Note: Do not disconnect the power supply of the device during upgrade	
		process, or the device will be damaged.	
E	Backup/Restore	Backup/Restore	
		Backup current settings or import saved settings to device	

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

Note	×
Do you want to reb	oot it?
ОК	Cancel

#### ----End

A progress bar is displayed on the page. Wait until it elapses.

## 9.2.2 Reset to factory settings

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

# Note

- After you reset the CPE, the configurations of the CPE are restored to factory settings. Therefore, you
  need to reconfigure the CPE. Restore the factory settings of the CPE only when necessary.
- To prevent device damages, ensure that the power supply of the device is normal when the device is resetting.
- After you reset the CPE, the login IP address is 192.168.2.1, and both login user name and password are admin.

## **Option 1: Reset the CPE using the web UI**

- 1. Choose **Tools** > **Maintenance** to enter the configuration page.
- 2. Click Reset.

Mai	ntenance		
	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(4045) ; Release Date: 2019-03-18	
	Backup/Restore	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. Click **OK** on the pop-up window.

The IP address wi	II be reset to 19	)2.168.2.1. Are you su	ure to reset it?
ine ir dddress wi	1 60 10501 10 13	2.100.2.1.7.10 you se	ne to reser it.

#### ----End

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

## **Option 2: Reset the CPE using the RESET button**

When the CPE is operating, hold down the **RESET** button for about 8 seconds and release it when all LED indicators light up and then turn off. The CPE is restored to factory settings.

## 9.2.3 Upgrade firmware

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



To prevent damaging the CPE:

- Ensure that the new firmware version is applicable to the CPE before upgrading the firmware. Generally, the suffix of the upgrade file is **.bin**.
- keep the power supply of the CPE connected during an upgrade.

Configuration procedure:

- Download the package of a later firmware version for the CPE from <u>www.ip-com.com.cn</u> to your local computer, and decompress the package.
- Log in to the web UI of the CPE and choose Tools > Maintenance to enter the configuration page.
- 3. Click Upgrade.

Maintenance	2
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(4045) ; Release Date: 2019-03-18 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

4. Select the correct upgrade file from your local computer and the system will upgrade automatically.

#### ----End

Wait for the progress bar to complete. Then log in to the web UI of the CPE. On the Status page, check if the current Firmware Version is consistent with the firmware version you selected for upgrade.



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

## 9.2.4 Backup/Restore

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

If the CPE enters the optimal 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.



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

### Backup

- 1. Choose **Tools** > **Maintenance** to enter the configuration page.
- 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(4045) ; Release Date: 2019-03-18
	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. Then click **Backup** on the pop-up window.

Backup/Restore		~
Backup configurations	Backup	
Import configurations	Restore	

#### ----End

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

## Restore

- 1. Choose **Tools** > **Maintenance** to enter the configuration page.
- 2. Click Backup/Restore.

Maintenance	?
Reboot Devi	ice Reboot All connections will disconnect during reboot.
Reset to Factory Settin	All configurations will restore to default factory setting after reset.
Upgrade Firmwa	Current Software Version: V1.0.0.2(4045) ; Release Date: 2019-03-18 Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged.
Backup/Resto	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	

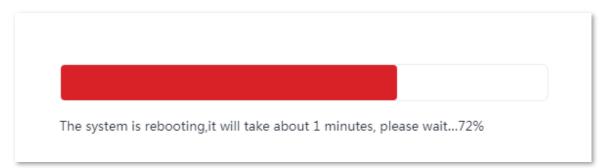
4. Select and upload the file you back up before (the suffix of the backup file: .cfg).

#### ----End

The file is being uploaded.

Backup configurations	Backup
Import configurations	Uploading

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

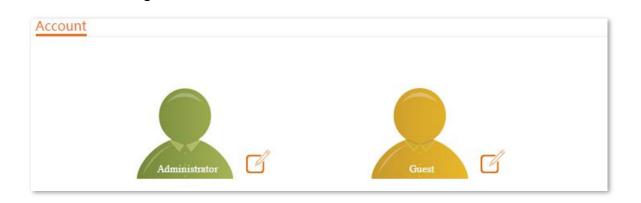


# 9.3 Account

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

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

Click  $\square$  to change the account information.



## 9.3.1 Administrator

You can modify and view the settings with the administrator account. Both the default user name and password of the administrator account are **admin**.



For network security, it is recommended to modify your login password regularly. A password of high security is preferred, such as a combination of lower-case letters, capital letters and numbers.

Administrator Account		×
Old User Name	admin	
Old Password		
New User Name		
New Password		
Confirm Password		
_		
	Save Cancel	

#### **Parameters description**

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

## **9.3.2** Guest

This account only allows you to view the settings. By default, this account is disabled. Both the default user name and password are **user**.

Guest Account		×
Enable	$\bigcirc$	
Old User Name	user	
Old Password		
New User Name		
New Password		
Confirm Password		
_		
	Save Cancel	

# 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. A maximum of 300 items can be saved. After the total log items exceed the maximum number, the previous logs will be cleared.

ystem Log			
Refresh	Clear		Log Type All 🔻
ID	Time	Туре	Log
1	2019-05-30 17:21:31	WAN	Broadcasting DHCP_DISCOVER
2	2019-05-30 17:21:30	System	Sync time failed!
3	2019-05-30 17:20:35	System	Sync time failed!
4	2019-05-30 17:20:35	WAN	Broadcasting DHCP_DISCOVER
5	2019-05-30 17:19:49	WAN	Broadcasting DHCP_DISCOVER
6	2019-05-30 17:19:40	System	Sync time failed!
7	2011-05-01 00:01:00	System	web 192.168.60.104 login

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

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

To clear the existing logs, click **Clear**.



- When the CPE reboots, the previous logs are lost.
- The CPE reboots when one of the following situations occurs: the CPE is powered on after a power failure, the VLAN function is configured, the firmware is upgraded, the configuration of the CPE is backed up or restored or the factory settings are restored.

# Appendix

# A.1 Default parameters

By default, the parameters are shown in the following table. (iLBE-5AC is used as an example here).

Parameters			Default settings		
Login IP Addres		55	192.168.2.1		
Login Administrator	A due in internation	User name	admin		
	Password	admin			
Quick Setup	Working Mode		AP mode		
	IP Address Type		Static IP address		
LAN Setup	IP Address		192.168.2.1		
	Subnet Mask		255.255.255.0		
S DHCP Server C F S	DHCP Server		Enable		
	Start IP Address		192.168.2.100		
	End IP Address		192.168.2.200		
	Subnet Mask		255.255.255.0		
	Gateway Address		192.168.2.254		
	Primary DNS Server		8.8.8.8		
	Secondary DNS Server		8.8.4.4		
	Lease Time		1 day		
VLAN Settings	VLAN Settings		Disable		
	PVID		1		
	Management VLAN		1		
	WLAN		1000		
	Wireless Network		Enable		
Wireless	SSID		IP-COM_XXXXXX, and XXXXXX is the last six characters of the LAN MAC address of the device		
	Security Mode		None		

Parameters		Default settings
	Transparent Bridge	Enable
	ΙΜΑΧ	Disable
	ТРС	Enable
	Signal LED1 Threshold	-90 dBm
	Signal LED2 Threshold	-80 dBm
	Signal LED3 Threshold	-70 dBm
Network Service	Login Timeout Interval	5 min
	Ping Watch Dog	Disable
	Telnet Service	Enable
	UPnP	Disable
	Hardware Watch Dog	Enable
	STP	Disable
Tools	Date & Time	Synchronized with the Internet

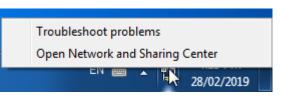
# A.2 Acronyms and Abbreviations

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

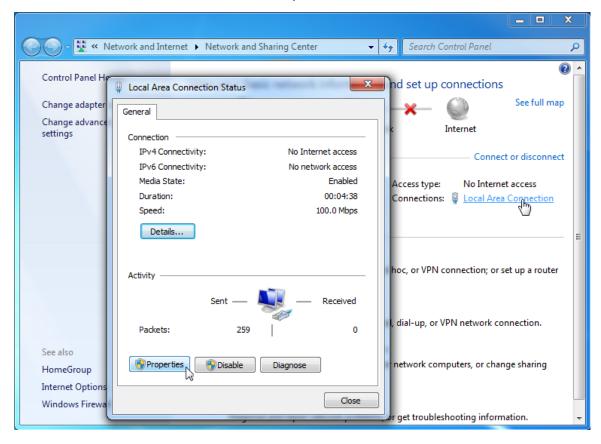
# A.3 Assign a fixed IP address to your computer

OS example: Windows 7

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



3. Click Local Area Connection, then click Properties.



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

Local Area Connection Properties
Networking Sharing
Connect using:
Intel(R) 82583V Gigabit Network Connection
Configure
This connection uses the following items:
Client for Microsoft Networks
🗹 🚚 QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mappel <sup>A</sup> /O Driver     Link-Layer Topology Discovery Responder
Install Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication
across diverse interconnected networks.
OK Cancel

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

General			
You can get IP settings assigne this capability. Otherwise, you for the appropriate IP settings.	need to ask your networ		
🔘 Obtain an IP address auto	matically		
Ouse the following IP address	ss:		
IP address: Subnet mask: Default gateway:	192.168.2.20		
	255 . 255 . 255 . 0		
Obtain DNS server addres	s automatically		
Ose the following DNS served			
Preferred DNS server:		8	
Alternate DNS server:			
Validate settings upon ex	it	Advance	d

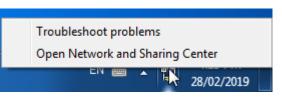
6. Click **OK** on the Local Area Connection Properties window, and close the other windows.

----End

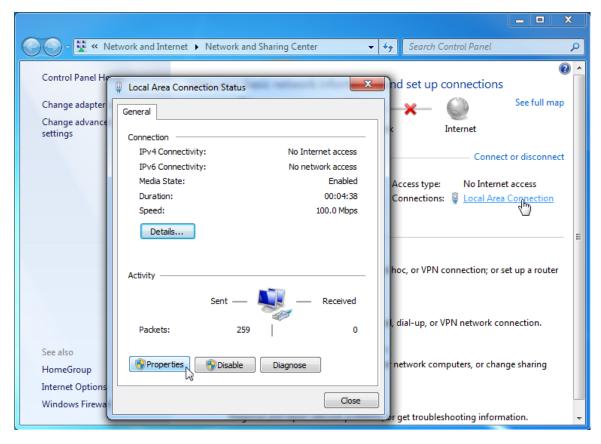
# A.4 Check the gateway IP address of a computer

OS example: Windows 7

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



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



----End

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

Property	Value
Connection-specific DN	tendawifi.com
Description	Intel(R) 82583V Gigabit Network Connec
Physical Address	44-8A-5B-F5-10-1F
DHCP Enabled	Yes
IPv4 Address	192.168.0.194
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Monday, 30 September 2019 3:24:56 PM
Lease Expires	Tuesday, 1 October 2019 3:24:56 PM
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En	Yes
Link-local IPv6 Address	fe80::e80f.f267:320e:67c0%10
IPv6 Default Gateway	
IPv6 DNS Server	
•	4 111