IP-COM

User Guide

Outdoor CPE

Applicable to single and kit product

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails

www.ip-com.com.cn

Document Version: V1.0

Copyright statement

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

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

Disclaimer

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

Document Version: V1.0



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

This user guide applies to the IP-COM CPEs (single and kit products). CPE12V1.0 is used for illustrations here unless otherwise specified.

This user guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The contained images and web UI screenshots are subject to the actual products.

Conventions

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

ltem	Presentation	Example
Cascading menus	>	Choose System > Live Users .
Parameter and value	Bold	Set User Name to Tom .
Variable	Italic	Format: XX:XX:XX:XX:XX:XX
UI control	Bold	On the Policy page, click the OK button.
Message	<i>u n</i>	The "Success" message appears.

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

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

For more documents

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

Document Version: V1.0

Technical support

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

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

Website: www.ip-com.com.cn

Revision history

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

Version	Description	Date
V1.0	Original publication.	2024-3-29

Document Version: V1.0

Contents

1 Typical application scenario1
1.1 CCTV surveillance1
1.1.1 Solution1
1.1.2 Configure the CPEs (Example: MS- Loco5ACV1.0)2
1.1.3 Install the CPEs (Example: MS- Loco5ACV1.0)11
1.2 ISP hotspot connection-WISP mode 13
1.2.1 Solution13
1.2.2 Configure the CPE13
2 Login and logout17
2.1 Login 17
2.1.1 Login with computer17
2.1.2 Login with smartphone or tablet 19
2.2 Logout22
3 Web UI 23
3.1 Web UI layout 23
3.2 Common buttons24
4 Quick setup 25
4.1 AP mode26
4.1.1 Overview26
4.1.2 Set AP mode27

	4.2	Client mode	29
		4.2.1 Overview	29
		4.2.2 Set Client mode	29
	4.3	Universal Repeater mode	33
		4.3.1 Overview	33
		4.3.2 Set Universal Repeater mode	33
	4.4	WISP mode	37
		4.4.1 Overview	37
		4.4.2 Set WISP mode	37
	4.5	Repeater mode	13
		4.5.1 Overview	13
		4.5.2 Set repeater mode	13
	4.6	P2MP mode	56
		4.6.1 Overview	56
		4.6.2 Set P2MP mode	56
	4.7	Router mode	54
		4.7.1 Overview	54
		4.7.2 Set router mode	54
5	Stat	tus6	59
	5.1	System status	59
	5.2	Wireless status	72
		5.2.1 View operating RF status	72

Document Version: V1.0

5.2.2 View management RF status 74
5.3 Statistics75
5.3.1 Throughput75
5.3.2 Wireless client76
5.3.3 Upstream AP77
5.3.4 Interface78
5.3.5 ARP table79
5.3.6 Routing table80
6 Network 81
6.1 LAN setup81
6.1.1 Overview81
6.1.2 Modify LAN IP address83
6.2 Packet filter86
6.3 MAC clone88
6.3.1 Overview88
6.3.2 Clone a MAC address88
6.4 DHCP server90
6.4.1 Overview90
6.4.2 Configure the DHCP server90
6.5 DHCP client92
6.6 VLAN settings93
6.6.1 Overview93
6.6.2 Configure VLAN (Example: CPE6SV2.0)93
6.6.3 Example of configuring VLAN on MS-Loco5ACV1.094
7 Wireless settings 98
7.1 Basic configuration98
7.1.1 Overview

	7.1.2 Basic wireless settings10	0
	7.1.3 Set up a non-encrypted wireless network10	8
	7.1.4 Set up a wireless network encrypte using WPA2-PSK11	
	7.1.5 Set up a wireless network encrypte using WPA or WPA211	
7.2	Advanced settings12	9
7.3	Access control13	3
	7.3.1 Overview13	3
	7.3.2 Example of configuring access control	4
7.4	Management RF13	
	7.4.1 Overview	
	7.4.2 Delay duration of management RF's wireless network13	
8 Adv	vanced13	9
	vanced13 LAN rate13	
8.1		9
8.1	LAN rate13	9 1
8.1	LAN rate13 Diagnose14	9 1
8.1	LAN rate13 Diagnose14 8.2.1 Site survey14	9 1 1
8.1	LAN rate	9 1 1 2 3
8.1	LAN rate	9 1 2 3
8.1 8.2	LAN rate	9 1 2 3 4 7
8.1 8.2	LAN rate	9 1 1 2 3 4 7 50
8.1 8.2	LAN rate	9 1 2 3 4 7 50
8.1 8.2 8.3	LAN rate	9 1 2 3 4 7 50 50
8.1 8.2 8.3	LAN rate	9 1 1 2 3 4 7 50 50 51 53

Document Version: V1.0

	8.4.2 Example of configuring port	
	forwarding	154
8.5	MAC filter	158
	8.5.1 Overview	158
	8.5.2 Example of configuring MAC fi	lter
		159
8.6	Network service	161
	8.6.1 DDNS	161
	8.6.2 Remote web management	165
	8.6.3 Reboot schedule	167
	8.6.4 Login timeout interval	167
	8.6.5 SNMP agent	168
	8.6.6 Ping watch dog	172
	8.6.7 DMZ host	173
	8.6.8 Telnet service	176
	8.6.9 UPnP	176
	8.6.10 Hardware watch dog	176

8.6.11 STP1	77
9 Tools1	78
9.1 Date & time1	78
9.1.1 Synchronized with the internet1	78
9.1.2 Manual1	79
9.2 Maintenance1	81
9.2.1 Reboot device1	81
9.2.2 Restore to factory settings1	82
9.2.3 Upgrade firmware1	.83
9.2.4 Backup/restore1	.84
9.3 Account1	.87
9.3.1 Administrator1	.87
9.3.2 Guest1	88
9.4 System log1	.89
Appendix1	90

Document Version: V1.0

1 Typical application scenario



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

1.1 CCTV surveillance

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

1.1.1 Solution

- Method 1: Use the CPE kit to set up a monitoring network, such as the CPE kit CPE5.
 You only need to install the CPEs to easily manage the CCTV surveillance for the community.
- Method 2: Use two CPEs to set up a monitoring network, such as the MS-Loco5AC.
 You only need to <u>Configure the CPEs</u> > <u>Install the CPEs</u> to easily manage the CCTV surveillance for the community.



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

Document Version: V1.0

1.1.2 Configure the CPEs (Example: MS-Loco5ACV1.0)

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

- Note

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



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



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



----End

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

- С Тір

For CPE6 and CPE9, the peer-to-peer bridging procedure is as follows:

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



- <u></u>- Tip

Option 2: Manual bridging

1. Place the two CPEs next to each other.



- 2. Log in to the web UI of CPE1.
 - 1) Power on the CPE1 (powered by PoE in this example).
 - Remove the cover of the CPE.

If the peer-to-peer automatic bridging fails, reset the two CPEs to factory settings, and try again.

Document Version: V1.0

- Use an Ethernet cable (CAT5e or above is recommended) to connect the PoE/LAN port of the CPE to the PoE port of the PoE injector.
- Use the included power cord to connect the PoE injector to a power socket. The PoE/LAN LED indicator of the CPE lights up.



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



2) Connect the computer to the LAN port of the PoE power supply using an Ethernet cable.



3) Start a web browser on your computer, visit the IP address of the CPE (default: **192.168.2.1**) in the address bar, and press **Enter** (or **Return**) on your keyboard.

Document Version: V1.0



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



- - Tip

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

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE properly.
- Ensure that the IP address of the computer is on the same network segment as the CPE' s IP address.
 For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied).
- If more than one CPE is connected, modify the IP address of each one to avoid login failure due to IP address conflict.
- <u>Reset the CPE to factory settings</u>.
- 3. Set **CPE1** to AP mode.
 - 1) Navigate to **Quick Setup**. Select **AP** mode, and click **Next**.

Document Version: V1.0

Select a workin AP In this r	-
AP In this r	and the definition of the sector of the sector of the sector build a the second sector of
	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 R	epeater In this mode, this device extends an existing wireless network for broader network coverage.
⊖WISP In th netw	is mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless ork.
	n this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
	is mode, the device connects to multiple wired networks through wireless bridge, but does not provide less access point.
Cor	nect to modem in wired manner, and provide network access point

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

/ou can set up your wireless netwo	ork name and wireless password here.	
Note down your wireless password	d.	
SSID	IP-COM_1	
Channel	Auto 🗸	
Security Mode	WPA2-PSK	
Encryption Algorithm		
Кеу		

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



Document Version: V1.0

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

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

Quick Setup
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 coverage.
○ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
O Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
O 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 wireless network to bridge from the list, which is **IP-COM_1** in this example, and click **Next**.

Tip

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

Quick Set	tup >> Client				Current Mode:
	and select the wirel	ess network you	want to connect,		
and click "Ne					
	Scan	C Scan aga	in		
	Upstream AP	IP-COM_1			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	IP-COM_1			WPA2-PSK,AES	.atl

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

Document Version: V1.0

Quick Setup >> Client	Current Mode: AP
	same channel, encryption, and encryption algorithm as those of upstream AP.
Upstream AP	
Upstream AP MAC Address	
Channel	~
Security Mode	WPA2-PSK V
Encryption Algorithm	
Кеу	
	Previous Next

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

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

Quick Setup >> Client			Current Mode: AP
Set the IP address to an unused	IP address belonging to t	he network segment of upstream AP.	?
IP Address	192.168.2.100		
Subnet Mask	255.255.255.0		
		Previou	s Next

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

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

----End

Document Version: V1.0

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



For CPE6 and CPE9, the bridging procedure is as follows:

When the two CPEs start bridging each other, their LED1, LED2 and LED3 indicators blink. When the LED1, LED2 and LED3 indicators of one CPE are lit solid and the same indicators of the other CPE keep blinking, the bridging succeeds.

Document Version: V1.0

1.1.3 Install the CPEs (Example: MS-Loco5ACV1.0)

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

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



Scenario 1





Document Version: V1.0

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

LED Indicator	Status	Description
LED1, LED2, LED3 (Received signal streng LED indicators)	Solid on/Blinking th	 The CPE is connected to the device. Solid on: The CPE may work in AP, Repeater, P2MP or Router mode. Blinking: The CPE may work in Client, Universal Repeater or WISP mode. Each LED indicator is set with a received signal strength value, which is the threshold for the corresponding LED indicator to light up. You can judge the connection quality through the status of these indicators. ✓ Tip You can make changes on the Wireless > Advanced page of the web UI of the CPE. Different models of CPEs have different LED indicators and working modes. The actual product prevails.
	Off	No device is connected to the CPE, or the received signal strength is less than the RSSI threshold (default: -90 dBm).

The LED indicator descriptions of the CPEs below are for reference.

Document Version: V1.0

1.2 ISP hotspot connection-WISP mode

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

1.2.1 Solution

MS-Loco5ACV1.0 is used as an example to illustrate the installation procedures. Procedures for other CPEs are similar.

. Тір

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

1.2.2 Configure the CPE

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



- 2. Set the CPE to WISP mode.
 - 1) Use an Ethernet cable to connect your computer to the LAN port of the PoE injector.

Document Version: V1.0



- 2) Log in to the web UI of CPE, and navigate to **Quick Setup**.
- 3) Select **WISP** mode, and click **Next**.

Quick Se	etup
Select a wo	orking mode:
OAP In t	his 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.
⊖ Universa	al Repeater In this mode, this device extends an existing wireless network for broader network coverage.
_	n this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
⊖ Repeate	In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
	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 wireless network of your ISP hotspot, which is **IP-COM_ERIC** in this example, and click **Next**.

Document Version: V1.0

Quick Setu	p>>WISP				
Click "Scan", a	and select the wireles xt".	s network you wan	t to connect,		
	Scan	Scan again	l		
	Upstream AP	IP-COM_ERIC]	
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	IP-COM_ERIC			WPA-PSK,AES	llee.

5) Enter the WiFi password of your ISP hotspot in the **Key** field, and click **Next**.

Quick Setup>>WISP	2
Then enter the remote AP's WiFi p	me channel, encryption, and encryption algorithm as those of upstream AP. assword, and click "Next" to continue.
Upstream AP	IP-COM_ERIC
Channel Security Mode	WPA-PSK V
Encryption Algorithm Key	AES O TKIP O TKIP&AES
	Previous Next

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					
Please select an internet connection and click "Next".	on type, and enter the int	ernet parameters provid	ded by your ISP	:	
Internet Connection Type	O DHCP (Dynamic IP)	○ Static IP Address	PPPoE		
PPPoE User Name					
PPPoE Password					
			F	Previous	Next

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

Document Version: V1.0

Quick Setup>>WISP	4 2
You can set up your wireless netwo	rk name and wireless password here.
Note down your wireless password	
SSID(WiFi Name)	IP-COM_ERIC
Channel	~
Security Mode	WPA-PSK V
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Кеу	••••••
	Previous Next

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

Quick Setup>>WISP			?
Specify the device with an IP addre upstream AP.	ss whose network segment is	is different from that of IP address of ISP access point or	
IP Address	192.168.3.1		
Subnet Mask	255.255.255.0		
		Previous Next	

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



----End

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

Document Version: V1.0

2 Login and logout



CPE6SV1.0 is used for illustration below.

2.1 Login

2.1.1 Login with computer

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

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

Internet Protocol Version 4 (TCP/IPv4)	Properties ? X
General	
You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings.	
Obtain an IP address automatical	ly 🔤
• Use the following IP address:	
IP address:	192.168.2.10
Subnet mask:	255.255.255.0
Default gateway:	· · ·
Obtain DNS server address auton	natically
• Use the following DNS server add	resses:
Preferred DNS server:	
<u>A</u> lternate DNS server:	· · ·
Validate settings upon exit	Ad <u>v</u> anced
	OK Cancel

Document Version: V1.0

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



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

CPE6S	V1.0	
2	Default user name: admin	
8	Default password: admin	
Q	English 🗸	
	Login	
	Forget password?	

- 🍟 - Тір

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

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE properly.
- Ensure that the IP address of the computer is on the same subnet as that of the CPE's IP address. For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied).
- If more than one CPE is connected, modify the IP address of each one to avoid the login failure due to IP address conflict.
- <u>Reset the CPE to factory settings.</u>
- The default login user name and password of the CPE are **admin**. For network security, refer to the
 <u>Account</u> and change the login user name and password.

----End

Document Version: V1.0

After the successful login, the following page appears.

小 Status	Quick Setup
ϟ Quick Setup	 Select a working mode: AP In this mode, the device creates a wireless network based on the current wired network.
Metwork	O Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
🛜 Wireless	O Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
X Advanced	O WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
🖏 Tools	O 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

2.1.2 Login with smartphone or tablet

Take iPhone as an example.

1. Connect the smartphone to the wireless network of the CPE, which is **IP-COM_ERIC** in this example.

Settings	WLAN	Edit
WLAN		
NETWORKS		,
IP-COM_E	ERIC	🔒 🗢 🛈
# (186.)		₹ (j)
# 1286.7		∻ (j)
# - 1284.J		? (j)
# 1286.7	10000.00	? (j)
10,07		ê 🤶 🚺
	and the	🔒 🗢 🚺
		🔒 🗢 🚺

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

Document Version: V1.0

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

VILAN IP-COM_ERIC	K Back Configure IPv4 Save
Join This Network	Automatic
	Manual 🗸 🗸
Private WLAN Address	BootP
WLAN Address	
Using a private address helps reduce tracking of your iPhone across different WLAN networks.	MANUAL IP IP Address 192.168.2.20
IPV4 ADDRESS	Subnet Mask 255.255.255.0
Configure IP Automatic >	Router 192.168.2.1
DNS	
Configure DNS Automatic >	
HTTP PROXY	
Configure Proxy Off >	

3. Connect to the CPE's wireless network successfully.

Settings	WLAN	Edit
WLAN		
V IP-COM_E	RIC	ê 🗢 i
NETWORKS		
		ê 🗢 🚺
		🔒 🗢 🚺
		🔒 🗢 🚺
		🕯 🗢 i
		∻ (i)
		🕯 🗢 i
		🕯 🗢 i
		🔒 🗢 i

Document Version: V1.0

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

192.168.2.1	Ŷ	0

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

CPE6SV1.0
R. Default user name: admin
🕒 Detault passwort: admin 🔛
P English 0
Login
Forget pasaword?

----End

Document Version: V1.0

2.2 Logout

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

Document Version: V1.0



3.1 Web UI layout

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

Here takes CPE6SV1.0 as an example. See the following figure.

	Status	LAN Setup 3	Current Mode: AP
4	Quick Setup	MAC Address	? B8:3A:08:AC:8C:08
	Network	IP Address Type	Static IP Address
	LAN Setup DHCP Server	IP Address	192.168.2.1
	DHCP Client 2	Subnet Mask	255.255.255.0
	VLAN Settings	Default Gateway	0.0.0.0
(i:-	Wireless	Primary DNS Server	0.0.0.0
*	Advanced	Secondary DNS Server	0.0.0.0
Φ,	Tools	Device Name	CPE6SV1.0
			Save

- 🍟 - Tip

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

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

Document Version: V1.0

3.2 Common buttons

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

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

Document Version: V1.0

4 Quick setup

- Тір

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

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

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

- <u>AP</u>: In this mode, the CPE converts a wired network into a wireless one.
- <u>Client</u>: In this mode, the CPE works as a wireless adapter that can connect to other wireless networks. The CPE does not provide wireless connection, so client devices need to be connected with an Ethernet cable.
- <u>Universal Repeater</u>: In this mode, the CPE extends an existing wireless network for broader network coverage. The wireless information (such as SSID and password) of the new network is the same as the upstream wireless network.
- <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 LAN port of an 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 bridging, and provides wireless access point.
- <u>P2MP</u>: In this mode, the CPE connects multiple wired networks through wireless bridging, but does not provide wireless access point.
- <u>Router</u>: In this mode, the CPE connects to a modem in wired manner to obtain the IP address by DHCP (Dynamic IP), static IP address or PPPoE for internet access.

Document Version: V1.0

4.1 AP mode

4.1.1 Overview

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

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



Document Version: V1.0

4.1.2 Set AP mode

1. Log in to the web UI of the CPE, and navigate to Quick Setup.

2. Select AP mode and click Next.



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

ote down your wireless passwor	d.			
*SSID	IP-COM_1			
Channel	Auto	~		
*Security Mode	WPA2-PSK	~		
*Encryption Algorithm	● AES ○ TK	(IP O TKIP&A	ES	
*Key	•••••			

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

Document Version: V1.0

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

----End

Parameters description

Name	Description
SSID	Specifies the WiFi name of the CPE.
Channel	Specifies the operating channel of the CPE. To reduce interference, it is recommended to use the least used channel in the current area. Auto indicates that the CPE automatically adjusts its operating channel according to the ambient environment.
Security Mode	Specifies the security mode of the wireless network, including <u>None</u> , <u>WEP</u> , <u>WPA-PSK</u> , <u>WPA2-PSK</u> , and <u>Mixed WPA/WPA2-PSK</u> .
Encryption Algorithm	 Specifies the encryption method of the wireless network. AES: Indicates the Advanced Encryption Standard. TKIP: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. TKIP&AES: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Кеу	Specifies the WiFi password of the wireless network.

Document Version: V1.0

4.2 Client mode

4.2.1 Overview

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

The CPE in Client mode usually works with the CPE in <u>AP mode</u> to establish a video surveillance network. The network topology is shown as below.



4.2.2 Set Client mode

- 1. Log in to the web UI of the CPE, and navigate to Quick Setup.
- 2. Select Client mode, 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.	
O 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.	
O Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.	
O 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	
Document Version: V1.0

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

- Č Tip

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

Quick Set	tup >> Client				Current Mode: AP		
? Click "Scan", and select the wireless network you want to connect, and click "Next".							
	Scan	C Scan again	l				
	Upstream AP	IP-COM_1					
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength		
۲	IP-COM_1			WPA-PSK,AES	.atl		

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

Quick Setup >> Client				Current Mode: AP
Ensure that the device uses the Then enter the remote AP's Wif				orithm as those of upstream AP.
Upstream AP	IP-COM_1			
Upstream AP MAC Address				
Channel		~		
Security Mode	WPA-PSK	~		
Encryption Algorithm		IP 🔿 TKIP&	AES	
Key				
				Previous Next

Document Version: V1.0

Parameters description

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

5. Specify IP address parameters and click Next.

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

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

Quick Setup >> Client			Current Mode: AP
Set the IP address to an unused	IP address belonging to t	ne network segment of upstream	? AP.
IP Address	192.168.2.10		
Subnet Mask	255.255.255.0		
		P	Previous Next

Document Version: V1.0

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



----End

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

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

Document Version: V1.0

4.3 Universal Repeater mode

4.3.1 Overview

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

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



4.3.2 Set Universal Repeater mode

- 1. Log in to the web UI of the CPE, and navigate to Quick Setup.
- 2. Select Universal Repeater mode, 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.
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.
O WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
O Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
O 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

Document Version: V1.0

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

Quick Se	tup >> Universal	Repeater		Cu	rrent Mode: Stat
Click "Scan",	and select the wirel	ess network you	want to connect,		
	Scan	C Scan agai	in .		
	Upstream AP	IP-COM_1			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	IP-COM_1			WPA-PSK,AES	liter

- Ф-тір

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

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

Quick Setup >> Universal Re	peater		Current Mode: Station
Then enter the remote AP's Wife	i password, and clic		? prithm as those of upstream AP.
Upstream AP	IP-COM_1		
Upstream AP MAC Address			
Channel		•	
Security Mode	WPA-PSK	~	
Encryption Algorithm	● AES ○ TKIP	⊖ TKIP&AES	
* Key	••••••		
			Previous Next

Document Version: V1.0

Parameters description

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

- 5. Specify IP address parameters and click Next.
 - For IP address, enter an unused IP address that belongs to the same subnet as the peer CPE.
 - For **Subnet Mask**, enter the subnet mask of the peer CPE.

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

Quick Setup>>Universal Rep	eater		2
Set the IP address to an unused IP	address belonging to th	e network segment of u	
IP Address	192.168.2.10		
Subnet Mask	255.255.255.0		
			Previous Next

Document Version: V1.0

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

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

----End

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

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



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

Document Version: V1.0

4.4 WISP mode

4.4.1 Overview

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

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



4.4.2 Set WISP mode

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



Document Version: V1.0

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

Quick Set	tup >> WISP		Current Mode:	Universal Repeat		
Click "Scan", and click "Ne	and select the wire ext".	ess network you	want to connect,			?
	Scan	C Scan agai	in			
	Upstream AP	IP-COM_1				
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
۲	IP-COM_1			WPA2-PSK,AES	.ail	



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

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

Quick Setup >> WISP			Current Mode: Universal Repeater
Ensure that the device uses the Then enter the remote AP's Wil			algorithm as those of upstream AP.
Upstream AP	IP-COM_1		
Upstream AP MAC Address			
Channel		~	
Security Mode	WPA2-PSK	~	
Encryption Algorithm	● AES ○ TKIP	⊖ TKIP&AES	
Кеу	•••••		
			Previous Next

Parameters description

Name	Description
Upstream AP	Specifies the WiFi name (SSID) of the wireless network to be bridged.
Upstream AP MAC Address	Specifies the MAC address of the wireless network to be bridged.

Document Version: V1.0

Name	Description		
Channel	Specifies the operating channel of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge.		
Security Mode	Specifies the security mode of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge. If the wireless network to be bridged is encrypted, you need to enter the password manually.		
Encryption Algorithm	 Specifies the encryption method of the wireless network. AES: Indicates the Advanced Encryption Standard. TKIP: Indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. TKIP&AES: Indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. 		
Кеу	Specifies the WiFi password of the wireless network.		

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

Quick Setup >> WISP			Current Mode: Universal Repeater
Please select an internet conne and click "Next".	ction type, and enter the	internet parameters pro	? pvided by your ISP.
Internet Connection Type	○ DHCP (Dynamic IP)	⊖ Static IP Address	PPPoE
PPPoE User Name			
PPPoE Password			
			Previous Next

Document Version: V1.0

Parameter description

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

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

Quick Setup >> WISP			Current Mode: Universal Repeater
You can set up your wireless net Note down your wireless passwo		eless password here.	?
SSID(WiFi Name)	IP-COM_1		
Channel		~	
Security Mode	WPA2-PSK	~	
Encryption Algorithm	● AES ○ TKIP	⊖ TKIP&AES	
Кеу	••••••		
			Previous Next

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

Document Version: V1.0

Quick Setup >> WISP		Current Mode: Universal Repeater
Specify the device with an IP add point or upstream AP.	dress whose network seg	? nent is different from that of IP address of ISP access
IP Address	192.168.2.1	
Subnet Mask	255.255.255.0	
		Previous
		Previous

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

Quick Setup >> WISP	Current Mode: Universal Repeater
The device is set to WISP, click "Save" to apply the settings.	?
	Previous Save

----End

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

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

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



WiFi name and WiFi password are SSID and Key set in step 6 above.

Document Version: V1.0



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

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

----End

To access the internet with:

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



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

Document Version: V1.0

4.5 Repeater mode

4.5.1 Overview

In Repeater mode, the CPE connects two or more (four at most) wired networks with a wireless link, and can be connected with both wired and wireless clients.

Repeater mode can be used to achieve communication between multiple office sites of an enterprise in a city.

The CPE in Repeater mode can work with the CPE in Repeater or <u>P2MP mode</u>.

4.5.2 Set repeater mode

-`@ - Tip

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

Peer to peer bridging

Assume that two CPEs are set to Repeater mode. The network topology is shown as below.



Document Version: V1.0

Configuration procedure



To check the SSID and key of the CPE, you can <u>log in to the web UI of the CPE</u> and navigate to **Wireless** > **Basic**.

- **1.** Set the CPE1 to Repeater mode.
 - 1) Log in to the web UI of CPE1, and navigate to Wireless > Basic.
 - 2) Modify the **Channel** and **Channel Bandwidth** as required, and click **Save**.

asic			
Enable Wireless			
Country/Region	China 🗸		
SSID	IP-COM_SQW9		
Broadcast SSID	Enable Oisable		
Network Mode	11ac 🗸		
Channel			
Channel Shift	○ Enable		
Transmit Power	1dBm 20dBm		
Channel Bandwidth	40MHz 🗸		
Transmit Rate	Auto 🗸		
Security Mode	None 🗸		
Isolate Client	○ Enable		
Max. Number of Clients	48 (Ran	ge: 1 to 128)	
	Save]	

3) Navigate to Quick Setup. Select Repeater and then click Next.

Document Version: V1.0

Select a w	vorking 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 Univers	sal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
-	In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
Repeat	ter 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 wireless network to bridge from the list, which is **IP-COM_1** in this example, and click **Next**.

Quick Setup	>> > Repeater				,	2
Click "Scan", a	nd select the wireles t".	s network you wa	nt to connect,		,	?
	Scan	Scan agai	n			
	Peer AP1	D8:32:14:90:8E:	39			
	Peer AP2	Select an SSID	or enter a MAC			
	Peer AP3	Select an SSID	or enter a MAC			
	Peer AP4	Select an SSID	or enter a MAC			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
	IP-COM_1		D8:32:14:90:8E:39	None	.atl	

- Ť

- If wireless networks cannot be scanned, navigate to Wireless > Basic and enable the wireless function.
 Then try again.
- Only the wireless networks whose security modes are set to **None** or **WEP** can be displayed on the list.
- 5) Set Authentication Type and Default Key, enter Key 1, and click Next.

Document Version: V1.0

Quick Setup>>Repeater		2
Ensure that the device uses the sa	ame channel, encryption, ar	d encryption algorithm as those of peer AP.
Enter the key of peer AP1, and cli	ck "Next".	
Peer AP1	IP-COM_1	
MAC Address of Peer AP1		
Channel		•
Security Mode	WEP	·
Authentication Type	Shared	•
Default Key	Key 1	·
Key 1	•••••	ASCII 🗸
Key 2	•••••	ASCII 🗸
Key 3	•••••	ASCII 🗸
Key 4	•••••	ASCII 🗸
		Previous Next

Parameters description

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

Document Version: V1.0

Name	Description	
	Specifies the authentication type for the WEP security mode. The options include Open and Shared . The options share the same encryption process.	
Authentication Type	 Open: Specifies that authentication is not required and data exchange is encrypted using WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. 	
	 Shared: 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. 	
	Specifies the WEP key for the Open or Shared encryption type.	
Default Key	For example, if Default Key is set to Key 1 , a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Key 1 .	
Key 1/2/3/4	Used to enter the WEP key. You can enter four keys, but only the key specified in the Default Key takes effect.	

6) Set the IP address to an unused IP address belonging to the same network segment as that of the peer CPE, which is **192.168.2.100** in this example. Then set **Subnet Mask** to the same one used by the peer CPE, and click **Next**.

Quick Setup>>Repeater				2
Set the IP address to an unused IP	address belonging to the r	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 make the settings take effect.



2. Refer to step <u>1</u> to set the CPE2 to Repeater mode.

----End

Document Version: V1.0

To check whether the bridging is successful:

- **1.** Log in to the web UI of CPE2.
- 2. Navigate to Advanced > Diagnose.
- 3. Select **Ping** from the **Diagnose** drop-down list.
- 4. Select Manual from the IP Address drop-down list.
- 5. Enter the IP address of CPE1, which is **192.168.2.100** in this example. And click **Start**.

Diagnose		
Diagnose	Ping 🗸	
IP Address	Manual 🗸	
IP Address/Domain Name	192.168.2.100	
Ping Packet	4	(Range: 1 to 10000)
Packet Size	32	Byte (Range: 1 to 60000)
	Start	

----End

The bridging is successful when the ping succeeds.

Peer to four peers bridging

Assuming that all CPEs uses the Repeater mode. The network topology is shown as below.

Document Version: V1.0



Assume that the parameters of the primary CPE are shown as follows:

- IP Address: 192.168.2.1
- Subnet Mask: 255.255.255.0
- SSID: IP-COM_1
- Channel: 157
- Channel Bandwidth: 40 MHz
- Security Mode: None

Assume that the SSIDs and MAC addresses of CPE1, CPE2, CPE3, and CPE4 are as follows:

СРЕ	SSID	MAC Address
CPE1	IP-COM_2	D8:32:14:90:8E:39
CPE2	IP-COM_3	D8:38:0D:CB:3D:77
CPE3	IP-COM_4	D8:38:0D:CB:3D:78
CPE4	IP-COM_5	C8:3A:35:96:AB:31

Document Version: V1.0

Configuration procedure

- **1.** Set the CPE1 to Repeater mode.
 - 1) Log in to the web UI of CPE1, and navigate to Wireless > Basic.
 - 2) Modify the **Channel** and **Channel Bandwidth** as required, and click **Save**.

sic	
Enable Wireless	
Country/Region	China 🗸
SSID	IP-COM_2
Broadcast SSID	Enable O Disable
Network Mode	11ac 🗸
Channel	✓
Channel Shift	○ Enable
DFS function	○ Enable
Transmit Power	1dBm 20dBm
Channel Bandwidth	40MHz ~
Transmit Rate	Auto 🗸
Security Mode	None 🗸
Isolate Client	○ Enable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

3) Navigate to Quick Setup. Select Repeater and then click Next.

Document Version: V1.0

elect a w	vorking 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.
) Univers	sal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
	In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
🖲 Repeat	er 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 wireless network to bridge from the list, which is **IP-COM_1** in this example, and click **Next**.

- 🍟 - Тір

- If wireless networks cannot be scanned, navigate to Wireless > Basic and enable the wireless function.
 Then try again.
- Only the wireless networks whose security modes are set to **None** or **WEP** can be displayed on the list.

Quick Setup	>>Repeater				
Click "Scan", a	nd select the wireles	s network you wa	nt to connect,		
and click "Nex	t".				
	Scan	C Scan agai	<u>n</u>		
	Peer AP1	D8:32:14:90:8E	-39		
	TeerArt	D0.32.14.30.0L			
	Peer AP2		or enter a MAC		
	Peer AP3		or enter a MAC		
	Peer AP4	Select an SSID	or enter a MAC		
Select	SSID	Channel	MAC Address	Security Mode	Signal
Sciect	3512	charmer	mile nauless	Security Mode	Strength
	IP-COM_1		D8:32:14:90:8E:39	None	.18

5) Click **Next**.

Document Version: V1.0

nsure that the device uses the sa	me channel, encr	yption, and encryptio	n algorithm as tho	se of peer AP.	
nter the key of peer AP1, and cli	ck "Next".				
Peer AP1	IP-COM_1				
MAC Address of Peer AP1					
Channel		~			
Security Mode	None	~			

6) Set the IP address to an unused IP address belonging to the same network segment as that of the peer CPE, which is **192.168.2.100** in this example. Then set **Subnet Mask** to the same one used by the peer CPE, 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 make the settings take effect.

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

- 2. Refer to step <u>1</u> to set CPE2, CPE3 and CPE4 to Repeater mode, and bridge the primary CPE.
- 3. Set the primary CPE to Repeater mode and bridge CPE1, CPE2, CPE3 and CPE4.
 - 1) Log in to the web UI of the primary CPE, and navigate to **Quick Setup**.
 - 2) Select **Repeater** mode, and click **Next**.
 - 3) Select SSIDs of CPE1, CPE2, CPE3 and CPE4, and click Next.

-) - Tip

- If wireless networks cannot be scanned, navigate to Wireless > Basic and enable the wireless function.
 Then try again.
- Only the wireless networks whose security modes are set to **None** or **WEP** can be displayed on the list.

Quick Setup>>Repeater					
Click "Scan", a	nd select the wireles	s network you wa	int to connect,		
and click "Nex	κt".				
	Scan	Scan agai	n		
	Peer AP1	D8:32:14:90:8E	:39		
	Peer AP2	D8:38:0D:CB:31	D8:38:0D:CB:3D:77		
	Peer AP3	D8:38:0D:CB:30	D8:38:0D:CB:3D:78		
	Peer AP4	C8:3A:35:96:A8	C8:3A:35:96:A8:31		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
~	IP-COM_1	36	D8:32:14:90:8E:39	None	line,
	IP-COM_2	153	D8:38:0D:CB:3D:77	None	
1	IP-COM_3	153	D8:38:0D:CB:3D:78	None	
v	IP-COM_4	149	C8:3A:35:96:A8:31	None	lle.

4) Click Next.

Quick Setup>>Repeater	·
Ensure that the device uses the sa Enter the key of peer AP1, and cliv	me channel, encryption, and encryption algorithm as those of peer AP.
Peer AP1	IP-COM_2
MAC Address of Peer AP1	D8:38:0D:CB:3D:77
Channel	~
Security Mode	None 🗸
	Previous Next

5) Click Next.

Document Version: V1.0

Set the IP addres	s to an unused IP	address belonging to	the network segment of	f peer AP.	
	IP Address	192.168.2.1			
	Subnet Mask	255.255.255.0			

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

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:

You can ping the IP addresses of CPE 1 to CPE 4 on the primary CPE to check the connectivity in sequence (CPE1 used as example).

- **1.** Log in to the web UI of the primary CPE.
- 2. Navigate to Advanced > Diagnose.
- 3. Select **Ping** from the **Diagnose** drop-down list.
- 4. Select Manual from the IP Address drop-down list.
- 5. Enter the IP address of CPE1, which is 192.168.2.10 in this example. And click Start.

Diagnose		
Diagnose	Ping	~
IP Address	Manual	~
IP Address/Domain Name	192.168.2.10	
Ping Packet	4	(Range: 1 to 10000)
Packet Size	32	Byte (Range: 1 to 60000)
l	Start	

----End

Document Version: V1.0

The bridging is successful when the ping succeeds.



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

Document Version: V1.0

4.6 P2MP mode

4.6.1 Overview

In P2MP mode, the CPE connects up to four wired networks through bridging, and it does not provide wireless access. Using P2MP mode, you can enable communication between offices in different parts of a city.

The CPE in P2MP mode can work with the CPE in <u>Repeater mode</u>.

4.6.2 Set P2MP mode

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

The network topology is shown as below.



Document Version: V1.0

- Tip

When configuring the P2MP mode, ensure that the **Channel** and **Channel Bandwidth** of all CPEs are the same.

Assume that the related parameters of the primary CPE are shown as follows:

- **IP Address**: 192.168.2.1
- Subnet Mask: 255.255.255.0
- SSID: IP-COM_1
- **Channel:** 157
- Channel Bandwidth: 40 MHz
- Security Mode: None

Assume that the SSIDs and MAC addresses of CPE1, CPE2, CPE3, and CPE4 are as follows:

СРЕ	SSID	MAC Address
CPE1	IP-COM_2	D8:32:14:90:8E:39
CPE2	IP-COM _3	08:40:F3:CB:D9:CA
CPE3	IP-COM_4	08:40:F3:CB:D9:C9
CPE4	IP-COM_5	08:40:F3:CB:D9:CC

Configuration procedure



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

- 1. Set CPE1 to Repeater mode and bridge the primary CPE.
 - 1) Log in to the web UI of CPE1, and navigate to Wireless > Basic.
 - 2) Modify the **Channel** and **Channel Bandwidth** as required, and click **Save**.

Document Version: V1.0

Basic	
Enable Wireless	
Country/Region	China 🗸
SSID	IP-COM_2
Broadcast SSID	Enable O Disable
Network Mode	11ac 🗸
Channel	
Channel Shift	🔿 Enable 💿 Disable
DFS function	○ Enable
Transmit Power	1dBm 20dBm
Channel Bandwidth	40MHz •
Transmit Rate	Auto 🗸
Security Mode	None ~
Isolate Client	○ Enable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

3) Navigate to **Quick Setup**. Select **Repeater** mode, and click **Next**.

Quick Setu	<u>up</u>
Select a worl	king mode:
○ AP In this	s 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.
-	this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless twork.
Repeater	In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
	this mode, the device connects to multiple wired networks through wireless bridge, but does not provide reless access point.
O Router co	onnect to modem in wired manner, and provide network access point
	Next

Document Version: V1.0

4) Select the wireless network to bridge from the list, which is **IP-COM_1** in this example, and click **Next** at the bottom of the page.

Quick Setup	Quick Setup>>Repeater ?					
Click "Scan", ar and click "Next	nd select the wireles	s network you wa	nt to connect,			
	Scan	C Scan agai	<u>n</u>			
	Peer AP1	D8:32:14:90:8E	D8:32:14:90:8E:39			
	Peer AP2	Select an SSID	or enter a MAC			
	Peer AP3	Select an SSID	or enter a MAC			
	Peer AP4	Select an SSID	or enter a MAC			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
	IP-COM_1		D8:32:14:90:8E:39	None	.atl	

- 🍎 - Tip

- If wireless networks cannot be scanned, navigate to Wireless > Basic and enable the wireless function.
 Then try again.
- Only the wireless networks whose security modes are set to **None** or **WEP** can be displayed on the list.

5) Click Next.

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	D8:32:14:90:8E:39
Channel	↓
Security Mode	None 🗸
	Previous

Document Version: V1.0

6) Set the IP address to an unused IP address belonging to the same network segment as that of the peer CPE, which is **192.168.2.100** in this example. Then set the **Subnet Mask** to the same one used by the peer CPE, and click **Next**.

Quick Setup>>Repeater				2
Set the IP address to an unused IP	address belonging to the r	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 make the settings take effect.

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

- 2. Refer to step <u>1</u> to set the CPE2, CPE3 and CPE4 to Repeater mode, and bridge the primary CPE.
- 3. Set the primary CPE to **P2MP** mode and bridge CPE1, CPE2, CPE3 and CPE4.
 - 1) Log in to the web UI of the primary CPE, and navigate to **Quick Setup**.
 - 2) Select **P2MP** mode, and click **Next**.
 - 3) Select the SSIDs of CPE1, CPE2, CPE3 and CPE4, which are IP-COM_2, IP-COM_3, IP-COM_4 and IP-COM_5 in this example, and click Next.

Document Version: V1.0

Quick Setup>>P2MP					
	and select the wireles	s network you wa	ant to connect,		
and click "Ne	ext".				
	Scan	C Scan agai	in		
	Peer AP1	D8:32:14:90:8E	:39		
	Peer AP2	08:40:F3:CB:D9	9:CA		
	Peer AP3	08:40:F3:CB:D9	08:40:F3:CB:D9:C9		
	Peer AP4	08:40:F3:CB:D9	9:CC		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
v	IP-COM_2		D8:32:14:90:8E:39	None	-11
\checkmark	IP-COM_3		08:40:F3:CB:D9:CA	None	lite.
\checkmark	IP-COM_4		08:40:F3:CB:D9:C9	None	-11
v	IP-COM_5		08:40:F3:CB:D9:CC	None	

4) Click Next.

Quick Setup>>P2MP	· · · · · · · · · · · · · · · · · · ·
	?
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	D8:32:14:90:8E:39
Channel	✓
Security Mode	None 🗸
	Previous Next

Parameters description

Name	Description
Peer AP1	Specifies the WiFi name (SSID) of the peer AP.
MAC Address of Peer AP1	Specifies the MAC address of the wireless network to be bridged.

Document Version: V1.0

Name	Description
Channel	Specifies the operating channel of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	Specifies the security mode of the wireless network to be bridged. It will be automatically populated when you select an SSID to bridge.
	- Tip The P2MP mode only supports WEP and None security modes.

5) Click Next.

Quick Setup>>P2MP				
Set the IP address to an unused IP	address belonging to the I	network segment of peer AP.		
IP Address	192.168.2.1]		
Subnet Mask	255.255.255.0			
			Previous	Next

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

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

----End

To check whether the bridging is successful:

You can ping the IP addresses of CPE 1 to CPE 4 on the primary CPE to check the connectivity in sequence. Below takes CPE1 for illustration.

- 1. Log in to the web UI of the primary CPE.
- 2. Navigate to Advanced > Diagnose.
- 3. Select **Ping** from the **Diagnose** drop-down list.
- 4. Select Manual from the IP Address drop-down list.
- 5. Enter the IP address of CPE1, which is **192.168.2.10** in this example. And click **Start**.

Document Version: V1.0

Diagnose		
Diagnose	Ping 🗸]
IP Address	Manual 🗸]
IP Address/Domain Name	192.168.2.10	
Ping Packet	4	(Range: 1 to 10000)
Packet Size	32	Byte (Range: 1 to 60000)
	Start	

----End

The bridging is successful when the ping succeeds.

Document Version: V1.0

4.7 Router mode

4.7.1 Overview

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

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



4.7.2 Set router mode

-) - Tip

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

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

Document Version: V1.0

Quick Se	etup 7
Select a w	vorking mode:
⊖ AP In f	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.
⊖ Univers	sal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
	In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
⊖ Repeate	er In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
_	In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
Router	connect to modem in wired manner, and provide network access point

- **3.** Select your internet connection type of your ISP hotspot, and set parameters. Take **PPPoE** as an example here.
 - 1) Select **PPPoE**.
 - 2) Enter the **PPPoE User Name** and **PPPoE Password** provided by your ISP.
 - 3) Click Next.

Quick Setup >> Router			Cu	urrent Mode: AP
Please select an internet connect and click "Next".	ction type, and enter the	internet parameters pro	ovided by your ISP.	?
Internet Connection Type	○ DHCP (Dynamic IP)	⊖ Static IP Address	PPPoE	
PPPoE User Name				
PPPoE Password				
			Previous	Next
Document Version: V1.0

Parameters description

Name	Description		
Internet Connection Type	 Refer to the following instructions to select the appropriate internet connection types: DHCP (Dynamic IP): The device obtains the IP address and other parameters from the DHCP server of upstream device for internet access. Static IP Address: The device accesses the internet using the IP address, subnet mask, default gateway and DNS server IP addresses provided by your ISP. PPPOE: The device accesses the internet using the PPPOE user name and password provided by the ISP. 		

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

Quick Setup >> Router				Current Mode: AP
You can set up your wireless ne	twork name and wir	eless p	assword here.	?
Note down your wireless passw	ord.			
SSID	IP-COM_AS1DF3			
Channel	Auto	~		
Security Mode	WPA2-PSK	~		
Encryption Algorithm	● AES ○ TKIP	OT	KIP&AES	
Кеу	•••••			
				Previous Next

Name	Description
SSID	Specifies the WiFi name of the CPE.

Document Version: V1.0

Name	Description		
Channel	Specifies the channel that the wireless network operates. Auto indicates that the device automatically adjusts its operating channel according to the ambient environment.		
Security Mode	Specifies the security mode of the wireless network of the device. It includes <u>None</u> , <u>WEP</u> , <u>WPA-PSK</u> , <u>WPA2-PSK</u> , and <u>Mixed WPA/WPA2-PSK</u> .		
Encryption Algorithm	 Specifies the encryption method of the wireless network. AES: It indicates the Advanced Encryption Standard. TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the device is limited to 54 Mbps. TKIP&AES: It indicates that both TKIP and AES encryption algorithms are available. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. 		
Кеу	Specifies the WiFi password of the wireless network.		

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

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

----End

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

- <u>Log in to the web UI</u> of the CPE and navigate to **Status**.
- Ensure that the WAN IP address, default gateway and DNS server information obtained by the WAN port are displayed on the System Status module.

After the 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 WiFi-enabled devices to the wireless
 network of the CPE to access the internet.
- The name and password of the wireless network are SSID and Key set in step 4.

Document Version: V1.0





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

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

----End

To access the internet with:

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



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

Document Version: V1.0



This module allows you to view the information of system and wireless network, including system status, wireless status, and statistics.

5.1 System status

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

You can view the system status here. CPE6SV1.0 is used for illustration.

If the CPE is set to AP mode, Client mode, Universal Repeater mode, Repeater mode or P2MP mode, the system status is shown as follows. If the CPE has multiple Ethernet ports, this page displays the current connection rate of each LAN port.

System Status			?
Device Name	CPE6SV1.0	PoE/LAN1 Speed	100 Mbps Full-d
Uptime	6 d23 h57 m25 s	LAN2 Speed	Disconnected
System Time	2024-03-07 14:29:46	LAN3 Speed	Disconnected
Firmware Version	V1.0.0.2(5410)	LAN4 Speed	Disconnected
Hardware Version	V1.0	CPU	85%
RAM	51%	LAN MAC Address	
WLAN MAC Address		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 serves as a WAN port.

Document Version: V1.0

System Status			?
Device Name	CPE6SV1.0	PoE/LAN1 Speed	Disconnected
Uptime	43 s	LAN2 Speed	100 Mbps Full-d
System Time	2024-03-07 14:55:45	LAN3 Speed	Disconnected
Firmware Version	V1.0.0.2(5410)	LAN4 Speed	Disconnected
Hardware Version	V1.0	Connection Type	DHCP (Dynamic IP)
CPU	6%	Connection Status	Disconnected
RAM	52%	WAN IP Address	
LAN MAC Address		Default Gateway	
WLAN MAC Address		Primary DNS Server	
LAN IP Address	192.168.2.1	Secondary DNS Server	

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

Document Version: V1.0

Name	Description	
WLAN MAC Address	Specifies the MAC address of the wireless interface of this device.	
Transparent Bridge	Specifies the status of transparent bridge.	
LAN Speed	Specifies the PoE/LAN or LAN port speed and duplex mode of this device.	
LAN IP Address	Specifies the IP address of this device, which is also the management IP address of this device. A LAN user can access the web UI of this device using this IP address. You can	
	modify this IP address on the <u>LAN Setup</u> page.	
Connection Type	 Specifies the internet connection type of this device in WISP or Router mode. DHCP (Dynamic IP): The CPE obtains IP address from the upstream DHCP server for internet access. Static IP Address: The CPE uses a fixed IP address, subnet mask, default gateway, and DNS server info for internet access. PPPOE: The CPE uses a user name and password for internet access. 	
Connection Status	Specifies the connection status of WAN port of this device in WISP or Router mode.	
WAN IP Address	Specifies the IP address of WAN port of this device in WISP or Router mode.	
Default Gateway	Specifies the default gateway address of this device in WISP or Router mode.	
Primary DNS Server	Specifies the IP address of primary DNS server of this device in WISP or Router mode.	
Secondary DNS Server	Specifies the IP address of secondary DNS server of this device in WISP or Router mode.	

Document Version: V1.0

5.2 Wireless status

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

You can view wireless status here, including working mode, SSID, security mode and so on. O6V3.0 is used for illustration here.

5.2.1 View operating RF status

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

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

Wireless Status			
Operating RF Status	5		
Working Mode	Client	AP's MAC Address	
SSID	N/A	Signal Strength	-10dBm
Security Mode	N/A	Background Noise	-79dBm
Channel/Radio Band		TX/RX Link	2X2
Channel Bandwidth	80MHz	Transmit/Receive Speed	866Mbps/6Mbps
TX Power	27dBm	ipMAX	Disabled
Wireless Client	N/A	Distance	N/Akm

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

Document Version: V1.0

Name	Description
Wireless Client	Specifies the number of wireless clients connected to the wireless network of the CPE's operating RF.
AP's MAC Address	 Specifies the MAC address of the upstream device. In AP, Router, Repeater, or P2MP mode, it displays the WLAN MAC address of this CPE. In Client, Universal Repeater or WISP mode, when the bridging succeeds, it displays the WLAN MAC address of the upstream AP. When the bridging fails, it displays N/A.
Signal Strength	 Specifies the wireless signal strength of the peer device. In AP or Router mode, it displays the signal strength of the first device connected to the wireless network of this device. In Client, Universal Repeater, WISP, Repeater or P2MP mode, it displays the received signal strength of the peer AP.
Background Noise	Specifies the strength of radio interference signals in the ambient environment that interferes with the wireless signal of this device in the same channel. Larger absolute value indicates less interference. For example, -95 dBm indicates less interference than that of -75 dBm.
TX/RX Link	Specifies the number of spatial streams of wireless data the device is transmitting or receiving. The more links indicates the more traffic.
Transmit/Receive Speed	 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.
ipMAX	Specifies the status of the ipMAX function. For details, refer to <u>ipMAX</u> .
Distance	Specifies the distance between the two CPEs after the bridging succeeds. If there are more than two CPEs, it specifies the bridging distance between this CPE and the farthest CPE.

Document Version: V1.0

5.2.2 View management RF status

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

On the **Management RF Status** module, you can view the wireless status information of the CPE's management RF, including working status, SSID, status of management RF enabled upon power on, and so on. Relevant configurations can be set on the <u>Management RF</u> page.

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

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

Document Version: V1.0

5.3 Statistics

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

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

Statistics				
Throughput	Wireless Client	Interface	ARP Table	Routing Table
	X 0.00 Kbps X 0.00 Kbps	LAN	-● RX 43.86 Kbps -◆ TX 1017.13 Kb	
1.5		1500		
1		1000		Ţ
0.5		500		
• • • •	• • • •	-• •	• • • • •	

5.3.1 Throughput

On the **Statistics** module, click **Throughput** to access the page. The line charts visually show the real-time transmitting and receiving traffic of WLAN and LAN port of the CPE.

Throughput	Wireless Client	Interface	ARP Table	Routing Table
	X 0.00 Kbps X 0.00 Kbps	LAN	 ● RX 43.86 Kbp ◆ TX 1017.13 I 	
1.5		1500		
1		1000		Ţ
0.5		500		

Document Version: V1.0

5.3.2 Wireless client

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

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.

Throughput	Wireless Client	Interfac	e	ARP	able	Routing Table
IP Address	MAC Address	Signal/Noise	Transmit	Receive	CCQ	Connection Duration
		-21/-75dBm		0Mbps	94%	20 m14 s

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

Document Version: V1.0

5.3.3 Upstream AP

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

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

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

tatistics						
Throughput	Upstream AF	Inter	face	ARP	Table	Routing Table
IP Address	MAC Address	Signal/Noise	Transmi	t/Receive	CCQ	Connection Duration
0.0.0.0		-43/-113dBm	300/2	70Mbps	100%	33 m33 s

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

Document Version: V1.0

5.3.4 Interface

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

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

atistics						
Throu	ghput	Wireless Client	Interface	ARP	Table	Routing Table
Interface	IP Address	MAC Address	Received Packets	Receive Error	Transmitted Packets	l Transmit Error
LAN	0.0.0.0		2187	0	3511	0
Bridge	192.168.2.10)	2274	0	1468	0
WLAN	0.0.0.0		110	0	4819	0

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

Document Version: V1.0

5.3.5 ARP table

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

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

istics				
Throughput	Wireless Client	Interface	ARP Table	Routing Table
IP Addr	ess	MAC Addr	ess	Interface
192.168.	2.100			Bridge

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

Document Version: V1.0

5.3.6 Routing table

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

It specifies the destination networks that the CPE can access.

tistics				
Throughput	Wireless Client	Interface	ARP Table	Routing Table
Destination	Network	Subnet Mask	Next Hop	Interface
192.16	58.2.0	255.255.255.0	0.0.0.0	Bridge
239.255.	255.250	255.255.255.255	0.0.0.0	Bridge

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

Document Version: V1.0



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. CPE6SV1.0 is used for illustration.

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

LAN Setup		
MAC Address		
MAC Address		
IP Address Type	Static IP Address	~
IP Address	192.168.2.2	
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	CPE6SV1.0	
	Save	Cancel

Document Version: V1.0

Name	Description		
	Specifies the MAC address of LAN port.		
MAC Address	By default, the SSID of the CPE is IP-COM_XXXXXX , and XXXXXX is the last six characters of the MAC address.		
	Specifies the type of obtaining an IP address. The default is Static IP Address.		
	 Static IP Address: Specify the IP address, subnet mask, default gateway, and DNS server IP addresses manually. 		
IP Address Type	 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. 		
	- Ţ		
	If the IP Address Type is set to DHCP (Dynamic IP Address) , you need to check the device's IP address on the clients list of the DHCP server in the network, and use this IP address to log in to the web UI of the device.		
IP Address	Specifies the IP address of the device. A LAN user can use this IP address to log in to the web UI of the device.		
	To access the internet, change this IP address to the same network segment of the LAN IP address of the egress router.		
Subnet Mask	Specifies the subnet mask of the device. The default is 255.255.255.0 .		
	Specifies the default gateway of the device.		
Default Gateway	You can set it to the LAN IP address of the egress router to enable the device to access the internet.		
	Specifies the primary DNS server IP address of the device.		
Primary DNS Server	If the egress router has the DNS proxy function, it can be set to the LAN IP address of the egress router. Otherwise, specify a DNS server IP address manually.		
	If there is only one DNS server IP address, enter it in this box.		
Secondary DNS Server	Specifies the secondary DNS server IP address of the device. If there are two DNS server IP addresses, enter one in this box.		
	Specifies the name of the device. The default name is the product model 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.		

Document Version: V1.0

6.1.2 Modify LAN IP address

Set the LAN IP address manually

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

Configuration procedure

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

LAN Setup	
MAC Address	
* IP Address Type	Static IP Address
* IP Address	192.168.2.30
* Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Device Name	CPE6SV1.0
	Save

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

Document Version: V1.0

Please click OK to confirm to change IP address. After IP address changed, please login with new IP address 192.168.2.3	Note	×
	Ū	address 192 168 2 3(
	Anter in address changed, piedse login with new in a)

----End

After changing the LAN IP address of the CPE:

- If the new and original IP addresses belong to the same subnet, you will be directed to the web UI of the device.
- If the new and original IP address belong to different subnets, assign your computer an IP address that falls in the same subnet as the new IP address before login with the new IP address. Refer to <u>How to assign a fixed IP address to your computer</u> in **Appendix** for details.

Set the device to obtain a LAN IP address automatically

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

Configuration procedure

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

Document Version: V1.0

LAN Setup	
MAC Address	
IP Address Type	DHCP (Dynamic IP Ad 🗸
IP Address	192.168.2.15
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	CPE6SV1.0
	Save

----End

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

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

Document Version: V1.0

6.2 Packet filter

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

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

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

/ired port ne	etwork packet filtering	🗌 Enable				
	Indicates the iltering mode	Enable	⊖ Disable			
Adding a	filtering policy					
ID	Filter rule	9	Rule details	Regular switch state	Filter mode	Operation
1	UDP proto	col	Destination IP 255.255.255.255:5050	Enable	Prohibit	Delete Edit
2	UDP proto	col	Destination IP 239.255.255.251:37810	Enable	Prohibit	Delete Edit
3	ARP&MAC ad	dress	ARP packet Destination MAC FF:FF:FF:FF:FF:FF	Enable	Prohibit	Delete Edit

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

Name	Description
	Specifies the filter rule of packets that need to be filtered.
	 MAC address: Used to configure the packets corresponding to the MAC address to be filtered.
	 IP: Packets whose protocol type is IP protocol will be filtered.
Filter rule	 VLAN: Packets whose protocol type is IEEE 802.1q protocol will be filtered.
	 ARP: Packets whose protocol type is ARP protocol will be filtered.
	 Port No.: Used to configure the packets corresponding to the port number to be filtered.
	 Custom: Customize the protocol type field of the packets to be filtered.
Rule details	Specifies the parameter settings required for filtering rules to filter the packets.
Regular switch state	Specifies the status of the filter rule. Values: Enable and Disable.
Filter mode	Specifies whether to filter the packets. Values: Permit and Prohibit.
	Used to edit or delete the packet filter policy.
Operation	 Edit: Used to edit the packet filter policy.
	 Delete: Used to delete the packet filter policy.
Source MAC	Specifies the data frames originating from this MAC address will be filtered.
Destination MAC	Specifies the data frames going to this MAC address will be filtered.
Source IP	Specifies the packets originating from this IP address will be filtered.
Destination IP	Specifies the packets going to this IP address will be filtered.
IP protocol type	Specifies the type of transport layer protocol used by the data segments that need to be filtered. All means filtering both TCP and UDP protocols.
VLAN ID	Specifies the VLAN ID of the packets to be filtered.
Source port	Specifies the packets corresponding to the source port number will be filtered.
Destination port	Specifies the packets corresponding to the destination port number will be filtered.
Custom	Used to customize the protocol type field of the packets that need to be filtered (2 bytes, hexadecimal, such as 0x8010).

Document Version: V1.0

6.3 MAC clone

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

6.3.1 Overview

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

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

Note

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

6.3.2 Clone a MAC address

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

Method 1

- 1. Connect the computer to the CPE.
- 2. <u>Log in to the web UI</u> of the CPE, and navigate to **Network** > **MAC Clone**.
- 3. Click Clone Local MAC Address.
- 4. Click Save.

MAC Clone	
	MAC Address
	Clone Local MAC Address Restore to Default MAC Address

----End

Document Version: V1.0

Method 2

- 1. Log in to the web UI of the router, and record the MAC address.
- 2. <u>Log in to the web UI</u> of the CPE, and navigate to **Network > MAC Clone**.
- 3. Enter the MAC address of the router in the MAC Address field.
- 4. Click Save.

Clone Local MAC Address Restore to Default MAC Address	MAC Clone	_			
Clone Local MAC Address Restore to Default MAC Address		MAC Address			
		Clone Local MAC	Address Restore	e to Default MAC Addres	5

----End



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

Document Version: V1.0

6.4 DHCP server

6.4.1 Overview

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

- Tip

If you <u>change the LAN IP address of the CPE</u> and the new and original IP addresses belong to different subnet, the system automatically changes the IP address pool of the DHCP server to be in the same subnet as the new IP address of the LAN port.

6.4.2 Configure the DHCP server

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

DHCP Server		Current Mode: AP
* DHCP Server		?
Start IP Address	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 🗸	
	Save	

----End



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

Name	Description
DHCP Server	Specifies whether to enable the DHCP server function of the CPE.
Start IP Address	Specifies the start IP address of the IP address pool of the DHCP server. The default value is 192.168.2.100 .
	Specifies the end IP address of the IP address pool of the DHCP server. The default value is 192.168.2.200 .
End IP Address	- ġ- Tip
	The start and end IP addresses must belong to the same subnet as the LAN port of the CPE.
Subnet Mask	Specifies the subnet mask assigned by the DHCP server to clients. The default value is 255.255.255.0 .
	Specifies the IP address of default gateway assigned by the DHCP server to clients. Generally, it is the IP address of the LAN port of the router on the LAN. The default value is 192.168.2.254 .
Gateway Address	- Ţ
	A client can access servers or hosts outside the local network only through a gateway.
	Specifies the primary DNS server IP address assigned by the DHCP server to clients. The default value is 8.8.8.8 .
Primary DNS Server	- ф-тір
	To enable clients to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server	(Optional) Specifies the secondary DNS server IP address assigned by the DHCP server to clients.
Lease Time	Specifies the validity period that a client holds an IP address assigned by the DHCP server.
	When the IP address expires:
	 If the client is still connected to the CPE, the client will automatically renew and continue to occupy the IP address.
	 If the client is not connected to the CPE (due to shutdown or wireless disconnection), the CPE will release the IP address. If other clients send a request for an IP address, the CPE can assign this IP address to other clients.
	You are recommended to keep the default value.

6.5 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 configuration page, <u>log in to the web UI</u> of the CPE and navigate to **Network** > **DHCP Client**.

НСР С	Client			
ID	Host Name	IP Address	MAC Address	Lease Time
1	DESKTOP-2PAVGKC	192.168.2.147		23h 58m 33s
2	DESKTOP-0RMLE69	192.168.2.198		23h 24m 5s
3	DESKTOP-OE85T2C	192.168.2.100		22h 7m 48s
4	linux-c83a359c6c40	192.168.2.114		2h 6m 53s
5		192.168.2.173		1h 33m 50s
~ I	Datas/Page 5 data in total			

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

Document Version: V1.0

6.6 VLAN settings

6.6.1 Overview

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

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

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

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

6.6.2 Configure VLAN (Example: CPE6SV2.0)

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

VLAN Settings		
PVID	1	(Range: 1 to 4094)
Management VLAN	1	(Range: 1 to 4094)
WLAN VLAN ID	1000	(Range: 1 to 4094)
LAN2	1	(Range: 1 to 4094)
LAN3	1	(Range: 1 to 4094)
LAN4	1	(Range: 1 to 4094)

Document Version: V1.0

Parameters description

Name	Description
VLAN Settings	Specifies whether to enable the 802.1Q VLAN function of this CPE. By default, it is disabled. After the VLAN function is enabled, the PoE/LAN port is used as a trunk port.
PVID	Specifies the default native VLAN ID of the trunk port. The default is 1. After the VLAN function is enabled, the PoE/LAN port is used as a trunk port.
Management VLAN	Specifies the ID of the management VLAN of this CPE. The default ID is 1. After changing the management VLAN, you can manage this CPE only after connecting your computer to the new management VLAN.
WLAN VLAN ID	Used to set a VLAN ID for the wireless network of the CPE. By default, it is set to 1000. After the VLAN function is enabled, the WLAN interface functions is equivalent to an access port, whose PVID is the same as VLAN ID.
LAN2	Used to set a VLAN ID of the Ethernet port of the CPE. By default, it is set to 1.
LAN3	After the VLAN function is enabled, the Ethernet port is equivalent to an access
LAN4	port, whose PVID is the same as VLAN ID.

6.6.3 Example of configuring VLAN on MS-Loco5ACV1.0

Networking requirements

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

Solution

You can perform as follows:

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

Document Version: V1.0

Network topology



Configuration procedure

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

Document Version: V1.0

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	ncel

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

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

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

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

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

For details, see the user guide for the router.

----End

Document Version: V1.0

Verification

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

Document Version: V1.0

7 Wireless settings

7.1 Basic configuration

7.1.1 Overview

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

Broadcast SSID

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

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

Isolate client

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

Max. number of clients

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

Security mode

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

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

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

None

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

WEP

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

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

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

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

WPA and WPA2

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

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

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

These features of WPA and WPA2 help significantly increase network security, making WPA and WPA2 the preferred security modes of wireless networks that require high security.

Document Version: V1.0

7.1.2 Basic wireless settings

To access the configuration page, <u>log in to the web UI</u> of the CPE and navigate to **Wireless** > **Basic**.

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

CPE13V2.0 is used as an example for illustration here. When the CPE works in AP, WISP, Universal Repeater, or Router mode, the basic wireless settings page is displayed as below.

Basic	
Enable Wireless	
Country/Region	China 🗸
* SSID	IP-COM_ERIC
Transparent WDS	○ Enable
Broadcast SSID	Enable O Disable
Network Mode	11ac 🗸
Channel Bandwidth	Auto 🗸
* Channel	Auto 🗸
Channel Shift	⊖ Enable
DFS Function	⊖ Enable
Transmit Power	1dBm 7dBm
* Transmit Rate	Auto 🗸
Security Mode	None 🗸
Isolate Client	○ Enable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

Document Version: V1.0

Name	Description
Enable Wireless	Specifies whether to enable the wireless function.
Country/Region	Specifies the country or region where this CPE is located. You can select the country or region to ensure that this CPE complies with the channel regulations of the country or region. By default, it is set to China .
SSID	Specifies the name of the wireless network (SSID). By default, it is set to IP-COM_XXXXXX (XXXXXX indicates the last six digits of the <u>LAN MAC address</u>). You can modify it as required.
Transparent WDS	It is available when the CPE works in AP mode or Client mode. With this function enabled, the CPE can bridge to CPEs from other manufacturers. Devices connected to the CPE working in Client mode will be displayed on the ARP table of the CPE working in AP mode. $-\overleftarrow{g}^{-} Tip$ Transparent WDS and <u>Transparent Bridge</u> cannot be enabled at the same time.
Broadcast SSID	 Specifies whether to broadcast the SSID. Enable: When an SSID is broadcast, wireless clients can detect the SSID. Disable: When an SSID is not broadcast, you need to manually enter the SSID to connect to the wireless network.
Network Mode	Specifies the wireless network mode of the CPE. Only wireless clients supporting the listed network mode can connect to the CPE.
Channel Bandwidth	Specifies the bandwidth of the operating channel of a wireless network. The channel bandwidth varies with different network modes. Select it based on your actual operating environment. Auto indicates that the CPE can switch its channel bandwidth based on the ambient environment.
Channel	Specifies the channel in which the CPE operates. Auto indicates that the CPE automatically changes to a channel rarely used in the ambient environment to prevent interference.
Document Version: V1.0

Name	Description
Channel Shift	Specifies the shift of the channel center frequency. With this function enabled, the channel center frequency will shift based on the frequency defined by the IEEE 802.11 standard, so that the CPE can exchange data on less interference channels. Image: Note When the Channel Shift function is enabled, other CPEs that bridge with it should also enable this function, and the offset value must be consistent. Otherwise the bridge will fail.
Offset Value	Specifies the offset value of the channel center frequency. The parameter is available only when the Channel Shift function is enabled.
DFS Function	Specifies the Dynamic Frequency Selection (DFS). With this function enabled, the CPE automatically detects the frequency of the radar system. When the CPE detects radar signals in the same frequency with the CPE itself, the CPE will automatically switch to another frequency to avoid interference with the radar system.
Transmit Power	Specifies the transmit power of the CPE. Higher number indicates wider WiFi coverage. Setting a proper transmit power helps improve the performance and security of the wireless network.
Transmit Rate	Specifies wireless transmission rate of the CPE. Auto is recommended. The maximum negotiation rate varies with different channel bandwidths and network modes. Refer to the web UI of the CPE for details. When Auto is selected, the CPE will be adjusted to the maximum transmit rate under the corresponding network mode.
Security Mode	There are various security modes for network encryption, including <u>None</u> , <u>WEP</u> , <u>WPA-PSK</u> , <u>WPA2-PSK</u> , and <u>Mixed-WPA/WPA2-PSK</u> .
Isolate Client	 Enable: Clients connected to this wireless network cannot communicate with each other, which improves the wireless network security. Disable: Clients connected to this wireless network can communicate with each other. It is set to Disable by default.
Max. Number of Clients	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.

Document Version: V1.0

None

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

WEP

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

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

Document Version: V1.0

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



Name	Description				
	Specifies the security mechanism that protects the wireless network. Values:				
	 WPA-PSK: The wireless network of the selected SSID is encrypted using WPA-PSK. 				
Security Mode	 WPA2-PSK: The wireless network of the selected SSID is encrypted using WPA2-PSK. 				
	 Mixed WPA/WPA2-PSK: Wireless clients can connect to the wireless network of the selected SSID using either WPA-PSK or WPA2-PSK. 				
	Specifies the encryption algorithm corresponding to the selected security mode. Values:				
	 AES: Advanced Encryption Standard. 				
	 TKIP: Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. 				
Encryption Algorithm	 TKIP&AES: Both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network of the selected SSID using TKIP or AES. 				
	-ݖij́́́́́́́т-тір				
	If Security Mode is set to WPA-PSK, this parameter can be set to AES or TKIP. If it is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter can be set to AES, TKIP, or TKIP&AES.				
Кеу	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	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, WPA2

Document Version: V1.0

Security Mode	WPA 🗸
RADIUS Server	None WEP WPA-PSK
RADIUS Port	WPA2-PSK Mixed WPA/WPA2-PSK
Encryption Algorithm	WPA WPA2 KIP&AES
RADIUS Password	كميرة
Key Update Interval	0 s (Range: 60 to 99999)

Name	Description
	The WPA and WPA2 options are available for network protection with a RADIUS server.
Security Mode	 WPA: The wireless network of the selected SSID is encrypted using WPA.
	 WPA2: The wireless network of the selected SSID is encrypted using WPA2.
RADIUS Server	Specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	Specifies the port number of the RADIUS server for client authentication.
RADIUS Password	Specifies the shared key of the RADIUS server for client authentication.
	Specifies the encryption algorithm corresponding to the selected security mode. Values:
	 AES: Advanced Encryption Standard.
Encryption Algorithm	 TKIP: Temporal Key Integrity Protocol.
	 TKIP&AES: Both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network of the selected SSID using TKIP or AES.
Key Update Interval	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.

Document Version: V1.0

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

Basic	
Dasic	
Enable Wireless	
Country/Region	China 🗸
Broadcast SSID	Enable Disable
Network Mode	11ac 🗸 🗸
Channel Bandwidth	Auto 🗸
Channel	~
Channel Shift	○ Enable
DFS Function	Enable O Disable
Transmit Power	1dBm 7dBm
Transmit Rate	Auto 🗸
Primary Upstream SSID	IP-COM_ERIC Site Survey
Primary AP BSSID	B8:3A:08:AC:8C:09
Transparent WDS	⊖ Enable
Security Mode	WPA-PSK
Encryption Algorithm	
Key	hyper d
Key Update Interval	0 s (Range: 60 to 99999)
Secondary Upstream SSID	○ Enable
Secondary Upstream SSID	IP-COM Site Survey
Secondary Upstream BSSID	B8:3A:08:AC:8C:09
Transparent WDS	O Enable 💿 Disable
Security Mode	None 🗸
Reconnect Primary	O Enable
Upstream SSID	00 /0
Reconnection Interval	90 (Range: 1~720minutes)
Isolate Client	
Max. Number of Clients	48 (Range: 1 to 128)
	Save Cancel

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

The following only describes main parameters for Client mode. For other parameters, refer to_<u>Parameter description</u> for AP mode.

Document Version: V1.0

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

Document Version: V1.0

7.1.3 Set up a non-encrypted wireless network

Networking requirements

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

Network topology



Configuration procedure

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

Document Version: V1.0

Basic			
Enable Wireless			
Country/Region		~	
*SSID	FREE		
Transparent WDS	⊖ Enable	Disable	
Broadcast SSID	Enable	⊖ Disable	
Network Mode	11ac	~	
Channel Bandwidth	Auto	~	
Channel	Auto	~	
Channel Shift	⊖ Enable	Disable	
DFS Function	Enable	⊖ Disable	
Transmit Power	 1dBm	27dBm	
Transmit Rate	Auto	~	
*Security Mode	None	~	
Isolate Client	⊖ Enable	Disable	
Max. Number of Clients	48	(Range: 1 to 128)	
	Save	Cancel	

----End

Verification

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

Document Version: V1.0

7.1.4 Set up a wireless network encrypted using WPA2-PSK

Networking requirements

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

Network topology



Configuration procedure

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

Document Version: V1.0

Basic	
Enable Wireless	
Country/Region	~
SSID	Factory
Transparent WDS	⊖ Enable
Broadcast SSID	Enable O Disable
Network Mode	11ac 🗸
Channel Bandwidth	Auto 🗸
Channel	~
Channel Shift	○ Enable
DFS Function	Enable O Disable
Transmit Power	1dBm 27dBm
Transmit Rate	Auto 🗸
Security Mode	WPA2-PSK V
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Кеу	••••••••••••••••••••••••••••••••••••••
Key Update Interval	0 s (Range: 60 to 99999)
Isolate Client	⊖ Enable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

----End

Verification

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

Document Version: V1.0

7.1.5 Set up a wireless network encrypted using WPA or WPA2

Networking requirements

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

Network topology



Configuration procedure

I. Configure the CPE

Assume that:

- IP address of the RADIUS server: 192.168.2.200
- RADIUS password: UmXmL9UK
- Authentication port: 1812
- SSID of the CPE: hot_spot
- Security mode: WPA2
- Encryption algorithm: **AES**
- 1. <u>Log in to the web UI</u> of the CPE, and navigate to **Wireless** > **Basic**.

Document Version: V1.0

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

Basic		Current Mode: AP
Enable Wireless		2
Country/Region	~	
SSID	hot_spot	
Transparent WDS	⊖ Enable	
Broadcast SSID	Enable O Disable	
Network Mode	11a/n 🗸	
Channel Bandwidth	20MHz 🗸	
Channel	~	
Channel Shift	⊖ Enable	
DFS Function	Enable O Disable	
Transmit Power	1dBm 27dBm	
Transmit Rate	Auto 🗸	
Security Mode	WPA2 🗸	
RADIUS Server	192.168.2.200	
RADIUS Port	1812	
Encryption Algorithm	® AES ○ TKIP ○ TKIP&AES	
RADIUS Password	**************************************	
Key Update Interval	0 s (Range: 60 to 99999)	
Isolate Client	⊖ Enable	
Max. Number of Clients	48 (Range: 1 to 128)	
	Save	

----End

Document Version: V1.0

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**.

🤣 Internet Authentication Service					
<u>File Action View H</u> elp					
← → 1 1	R 🗗 🗟 😫				
Internet Authenticat		Frien	dly Name	Address	
1	New RADIUS <u>C</u> li	ent	There are no iten	ns to show in this view.	
Remote Access	Now	•			
Connection		•			
	Re <u>f</u> resh				
	Export <u>L</u> ist				
	<u>H</u> elp				
New 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**.

Type a friendly name and	either an IP Address	or DNS name for the	client.
Eriendly name:	root		9
Client address (IP or DNS):		
192.168.2.1			⊻erify
P address of the CI	ΡE		

Document Version: V1.0

3) Enter UmXmL9UK in the Shared secret and Confirm shared secret field, and click Finish.

RADIUS Client	
Additional Information	
vendor of the RADIUS client.	based on the client vendor attribute, specify the
<u>Client-Vendor</u>	
RADIUS Standard	•
Shared secret	жжжжжж
Confirm shared secret:	жжения
Eequest must contain the Messa	age Authenticator attribute
	Must be the same as RADIUS
	Password specified on the CPE
	< Back Finish Cancel
	< <u>B</u> ack Finish Cancel

- 2. Configure a remote access policy.
 - Right-click Remote Access Policies and choose New Remote Access Policy.
 In the New Remote Access Policy Wizard dialog box that appears, click Next.

Internet Authentication	Service		
<u>File Action ⊻iew H</u> elp			
⊨ → 🗈 🖪 🛃	12		
Internet Authentication Server RADIUS Clients Remote Access Logging Connection Request Pr Connection Request Pr	ice (Local)	Name Connections to Microsoft Routing and Remote A Connections to other access servers	Order 1 2

Document Version: V1.0

Internet Authentication Service File Actor New Remote Access Policy	Vizard
Conne	Welcome to the New Remote Image: Comparison of the New Remote Access Policy Wizard Image: Comparison of the New Remote This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server. Image: Comparison of the New Remote To continue, click Next. Image: Comparison of the Next of the Ne
By Start Image: Start	K Next > Cancel Cancel Image: Sector of the sec

2) Enter a policy name and click **Next**.

New Remote Access Policy Wizard
Policy Configuration Method The wizard can create a typical policy, or you can create a custom policy.
How do you want to set up this policy?
© Set up a custom policy
Type a name that describes this policy.
Policy name: root
Example: Authenticate all VPN connections.
< <u>B</u> ack <u>Next</u> > Cancel

Document Version: V1.0

3) Select Ethernet and click Next.

New Remote Access Policy Wizard	×
Access Method Policy conditions are based on the method used to gain access to the network.	
Select the method of access for which you want to create a policy.	
© ⊻PN	
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.	9
O <u>D</u> ial-up	
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.	
O <u>W</u> ireless	
Use for wireless LAN connections only.	
👁 Ethernet	
Use for Ethernet connections, such as connections that use a switch.	
< <u>₿</u> ack <u>N</u> ext> Cancel	

4) Select **Group** and click **Add**.

w Remote Access Policy Wizard	2
User or Group Access You can grant access to individu groups.	al users, or you can grant access to selected
Grant access based on the following	g:
C <u>U</u> ser	
User access permissions are sp	ecified in the user account.
Group Individual user permissions over Group name:	ride group permissions.

Document Version: V1.0

5) Enter **802.1x** in the **Enter the object names to select** field, click **Check Names**, and click **OK**.



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

In the New Remote Access Policy Wizard dialog box that appears, click Finish.

The remote access policy is created.

w Remote Access Policy Wizard		
Authentication Methods EAP uses different types of secu	urity devices to authenticate users.	Î
Select the EAP type for this policy	ı.	
<u>I</u> ype:		
Protected EAP (PEAP)	Conf	gure
	< <u>B</u> ack <u>N</u> ext >	Cancel
	;	
	47F	

Document Version: V1.0



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

Settings Specify the conditions that connection requests must match. Policy conditions: NAS-Port-Type matches "Ethernet" AND Windows-Groups matches "COMBA\802.1x"
Policy conditions: NAS-Port-Type matches "Ethernet" AND
Policy conditions: NAS-Port-Type matches "Ethernet" AND
NAS-Port-Type matches "Ethernet" AND
Add Edit Remove
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

Document Version: V1.0

8) 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	Ethernet Wireless - IEEE 802.11
	OK Cancel

9) Click **Edit Profile**, click the **Authentication** tab, configure settings as shown in the following figure, and click **OK**. When a message appears, click **No**.

Constraints tication	IP Encryption ethods you want to allov	Multilink Advanced v for this connection.
uthentication m		1
	ethods you want to allov	v for this connection.
1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 -	Authentication version <u>2</u>	
pted authentica	tion (CHAP)	
crypted authenti	ication (PAP, SPAP)	
nticated access		
	ect without negotiating a	n authentication
	isoft Encrypted A User can chan ipted authentica icrypted authent nticated access	upted authentication (CHAP) crypted authentication (PAP, SPAP) nticated access clients to connect without negotiating a

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

----End

Document Version: V1.0

Configure your wireless device



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

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



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

Document Version: V1.0

	×
🚱 🔍 🖬 🕨 Control Panel 🔸 Network and Internet 🔸 Manage Wireless Networks 💿 🗸 🍕 Search Manage Wireless Networks	م
Manage wireless networks that use (Wireless Network Connection)	
Windows tries to connect to these networks in the order listed below.	
Add Adapter properties Profile types Network and Sharing Center	
	/
0 items	
	_
Manually connect to a wireless network	
How do you want to add a network?	
Manually create a network profile This creates a new network profile or locates an existing network and saves a profile	
for the network on your computer. You need to know the network name (SSID) and	
security key (if applicable).	
security key (if applicable).	
security key (if applicable).	
security key (if applicable).]

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

	Document Version: V1.0
Manually connect to a wireless network Enter information for the wireless network you want to add Network name: hot_spot Security type: WPA2-Enterprise Encryption type: AES Security Key: Hide characters Image: Start this connection automatically Image: Start this connection automatically Image: Connect even if the network is not broadcasting Warning: If you select this option, your computer's privacy might be at risk.	Document Version: V1.0 Must be the same as the security mode for the SSID specified on the CPE
Next Caricel	

Document Version: V1.0

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

ر بينا Manually connect to a wireless network	
Successfully added hot_spot	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

Ŷ

hot_spot Wireless Netw	ork Properties	×
Connection Security)	
Security type:	WPA2-Enterprise	
Encryption type:	AES 💌	
Choose a network aut	hentication method:	
Microsoft: Protected	EAP (PEAP) 🔻 Settings	
Remember my creative I'm logged on	dentials for this connection each	
Advanced settings		
	OK Car	ncel

Document Version: V1.0

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

Protected EAP Properties
When connecting:
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:
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK Cancel

$\overline{\mathbf{V}}$
EAP MSCHAPv2 Properties
When connecting: Automatically use my Windows logon name and password (and domain if any).
OK Cancel

Document Version: V1.0

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

rk Properties 🛛 🛁
WPA2-Enterprise
AES 🔻
entication method:
AP (PEAP)
entials for this connection each
25
OK Cancel
<u>Ф</u>
↓
↓ settings
settings
settings stion mode:
settings ation mode: r authentication Save credentials
settings stion mode:
settings ation mode: r authentication Save credentials tials for all users
settings ation mode: r authentication Save credentials tials for all users on for this network
settings ation mode: r authentication Save credentials cials for all users on for this network diately before user logon
settings stion mode: r authentication Save credentials tials for all users on for this network diately before user logon diately after user logon
settings ation mode: r authentication Save credentials itials for all users on for this network diately before user logon
settings ation mode: r authentication Save credentials tials for all users on for this network diately before user logon diately after user logon diately after user logon econds): 10
settings ation mode: r authentication r authentication stials for all users on for this network diately before user logon diately after user logon econds): 10
settings ation mode: r authentication Save credentials tials for all users on for this network diately before user logon diately after user logon econds): 10 al dialogs to be displayed during single uses separate virtual LANs for machine
settings ation mode: r authentication Save credentials tials for all users on for this network diately before user logon diately after user logon diately after user logon econds): 10 10 ses separate virtual LANs for machine
settings ation mode: r authentication Save credentials tials for all users on for this network diately before user logon diately after user logon econds): 10 al dialogs to be displayed during single uses separate virtual LANs for machine

ОК

Cancel

Document Version: V1.0

7. Click Close.

الله Manually connect to a wi	reless network		
Successfully added ho	t_spot		
Change connect Open the connection	tion settings n properties so that I can change the settings		
		Close	
	<u>\$</u>		
🕒 🗢 📶 🕨 Control Panel 🕨 Net	work and Internet 🕨 Manage Wireless Networks	✓ 4y Search Manage Wireless Network	onks 🔎
			•
-	hat use (Wireless Network Connection)		
Windows tries to connect to these ne	tworks in the order listed below.		
Add Adapter properties Profile typ			0
Networks you can view, modify, and reord	ler (1) Security: WEP	Type: Any supported	^
0 items			

Document Version: V1.0

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

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

9. 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

----End

Verification

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

Document Version: V1.0

7.2 Advanced settings

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

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

Advanced		
WMM	Enable	⊖ Disable
APSD	⊖ Enable	Disable
Minimum RSSI Threshold	○ Enable	Disable
Preamble	○ Short Preamble	Long Preamble
ipMAX	○ Enable	Disable
Signal Transmission	Coverage-oriented	d ○ Capacity-oriented
TPC	Enable	⊖ Disable
Signal Reception Level	Auto	~
Transmission Distance	5	□ Auto km (Range: 0.1 to 30, default: 5)
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

Document Version: V1.0

Name	Description
WMM	WiFi Multi-media (WMM) is a wireless Quality of Service (QoS) protocol making packets with higher priorities to be transmitted earlier. This ensures better QoS of voice and video applications over wireless networks.
APSD	Automatic Power Save Delivery (APSD) is a WMM power saving protocol created by WiFi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
Minimum RSSI Threshold	Specifies the minimum strength of received signals acceptable to this 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 WiFi-enabled devices connect to wireless network with better wireless signal.
Preamble	Specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. 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	 The Transparent Bridge function enables the WLAN interface of this device to forward all packets. It is used to solve the problem that some NVRs cannot detect IP cameras, or cannot change the IP addresses of cameras in different networks. - Tip This function is only applicable when the CPE works in AP, Client or Universal Repeater mode. Transparent WDS and Transparent Bridge cannot be enabled at the same time.

Name	Description
	ipMAX is IP-COM's proprietary Time Division Multiple Access (TDMA) polling technology. It allows multiple clients to share the same channel for accessing to a network. With the ipMAX enabled, the CPE assigns time slots to each client, and transmits data according to the assigned time slots, achieving Point-to-MultiPoint (P2MP) connections.
	After the ipMAX is enabled, the CPE:
	 Avoids the "hidden node" problem, which occurs when a node is visible from a wireless AP, but not from other nodes communicating with the originating AP.
ipMAX	 Reduces latency.
	 Improves throughput and anti-interference performance.
	 Improves overall performance in Point-to-MultiPoint (PtMP) installations, and increases the maximum possible number of users that can associate with an AP that uses ipMAX.
	- тір
	If ipMAX is enabled, the device operates in ipMAX mode and only accepts connections from ipMAX devices. And you cannot connect standard WiFi devices, such as laptops, tablets, or smartphones, to the CPE.
	Specifies the CPE's signal travel through wall capability.
Signal Transmission	 Coverage-oriented: With less interference nearby, this mode enables the device to cover wider area.
	 Capacity-oriented: With strong interference nearby, this mode improves the device's anti-interference capability.
	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.
ТРС	By default, when the received signal strength is greater than -25 dBm, the CPE decreases its TX power.
Signal Reception Level	Used to adjust the signal reception level. 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.
	Specifies the wireless transmission distance of this device. You can set it based on the actual installation distance.
Transmission Distance	- Yip Modifying this distance will affect wireless transmission performance, and it is recommended to keep the default setting. If you want to set it manually, you should enter a value that is greater than the actual distance between the two CPEs.

Document Version: V1.0

Name	Description
	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.
	Specifies the threshold of a fragment. The unit is byte.
	Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented.
Fragment Threshold	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.
	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.
RTS Threshold	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	Specifies the countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval.
	For example, if Delivery Traffic Indication Map (DTIM) Interval is set to 1, this device transmits all cached frames 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.
	The default threshold for LED1, LED2, and LED3 are -90, -80, and -70 respectively.

Document Version: V1.0

7.3 Access control

7.3.1 Overview

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

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

Acc	cess Control		Current Mode: Router
	SSID	IP-COM_FAG37i	?
	Access Control		
	Mode	Disallow OAllow	
	MAC Address	12:12:12:12:12	Add Add online devices
SI	N MAC Addres	ss Status	Operation
	1 12:12:12:12:12	2:12 Enable	Ē
A	ccess Control List	Save	

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

Document Version: V1.0

7.3.2 Example of configuring access control

Networking requirements

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

Solution

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

Configuration procedure

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



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

- 6. Refer to step <u>5</u> to add the other two MAC addresses.
- 7. Click Save.

Document Version: V1.0

Access C	Control		Current Mode: Router
	SSID IP-COM_FA	G37i	•
	Access Control		
	Mode O Disallow	Allow	
	MAC Address C8:3A:35:	00:00:03	Add Add online devices
SN	MAC Address	Status	Operation
1	C8:3A:35:00:00:01	Enable	Ē
2	C8:3A:35:00:00:02	Enable	Ē
3	C8:3A:35:00:00:03	Enable	Ē
	Save	Cancel	

----End

Verification

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

Document Version: V1.0

7.4 Management RF

7.4.1 Overview

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

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

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

Management RF		Current Mode: AP
Management RF		2
Enabled upon Power on		
Duration	15 mins	
SSID	IP-COM_03CB00_MG	
Network Mode	11b/g/n 🗸	
Channel	Auto 🗸	
Encryption	None 🗸	
	Save	

Name	Description
Management RF	Specifies whether to enable the Management RF function of the CPE.
Enabled upon Power on	Specifies whether to enable the Enabled upon Power on function of the management RF.
	With this function enabled, the CPE's management RF will be automatically enabled when the CPE is powered off and on again.

Document Version: V1.0

Name	Description
	Specifies the duration of the management RF enabled.
Duration	With the management RF enabled, if the Duration is exceeded and the available time of the management RF is not delayed, the management RF will be automatically disabled.
	- ф-тір
	You can use a wireless client to connect the wireless network of the management RF. Log in to the web UI of the CPE, you can <u>delay the available time for the wireless</u> <u>network of the management RF</u> as required.
SSID	Specifies the WiFi name of the CPE management RF, which can be customized as required.
Network Mode	Specifies the wireless network mode of the CPE. Only wireless clients supporting the listed network mode can connect to the CPE.
Channel	Specifies the operating channel of the CPE management RF. When Auto is selected, the CPE will automatically adjust its operating channel according to the surrounding environment.
Encryption	Specifies the security mode of the wireless network of the CPE management RF. Refer to the <u>Security Mode</u> for details.

7.4.2 Delay duration of management RF's wireless network

With the management RF enabled, if the Duration is exceeded and the available time of the management RF is not delayed, the management RF will be automatically disabled. You can use a wireless client to connect the wireless network of the management RF. Log in to the web <u>UI of the CPE</u>, you can delay the available time for the wireless network of the management RF as required.

Configuration procedure

- 1. Connect the wireless client to the wireless network of management RF.
- 2. Start a browser on your wireless client, visit the CPE's management address (By default, AP mode: 192.168.2.1. Client mode: 192.168.2.2), and log in to the web UI of the CPE.
- 3. Click **Delay** in the upper right corner of the page. The following figure is for reference only.
Document Version: V1.0

P	COM			Left until the page close	d:4m 41s Delay Logou
≁	Status	Status			Current Mode: Station
4	Quick Setup	System Status			?
	Network	Device Name	CPE13V2.0	LAN Speed	1000 Mbps Full
((ı:-	Wireless	Uptime	10 m17 s	LAN IP Address	192.168.2.1
*	Advanced	System Time	2024-03-22 14:44:07	Transparent Bridge	Enabled
	-	Firmware Version	V1.0.0.2(2130)	Hardware Version	V2.0
ø,	Tools	CPU	16%	RAM	78%
		LAN MAC Address		WLAN MAC Address	

----End



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

Document Version: V1.0

8 Advanced

8.1 LAN rate

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

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

When you change the settings, ensure that the LAN speed and duplex mode of the port of the CPE is the same as that of peer device. By default, the LAN speed settings of the LAN port is **Auto Negotiation**. CPE6SV2.0 is used for illustration.

LAN Rate	4
PoE/LAN Speed	Auto Negotiation 🗸
LAN2 Speed	Auto Negotiation
LAN3 Speed	Auto Negotiation
LAN4 Speed	Auto Negotiation
	Save Cancel

After the LAN speed and duplex mode settings are changed, you can check on the <u>System</u> <u>status</u> page.

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

Document Version: V1.0

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



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

Document Version: V1.0

8.2 Diagnose

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

You can use the diagnosis tools for troubleshooting.

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

8.2.1 Site survey

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

Configuration procedure

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

----End

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

agnose					
	Diagnose	Site Survey	~		
ID	SSID	MAC Address	Channel	Security	Signal Strength
1	IP-COM_03CB48		149	None	.all
2	EW15D_E_T		153	None	lin.
3	IP-COM_0BC970		153	None	ite.

Document Version: V1.0

8.2.2 Ping

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

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

Configuration procedure

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

Diagnose		_
		?
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)
l	Start	

----End

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

IP Address		Time	TTL
204.79.197.200		14.761ms	112
204.79.197.200		14.627ms	112
cn.bing.com		Timeout	
204.79.197.200		14.523ms	112
10 • Datas/Page 4 data in total			
		3 of 4 packets received	, 25.00% loss25.00%
Min. 14.523 ms	Average 14.64 ms	Max. 1	4.761 ms

Document Version: V1.0

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

5. Click Start.

Diagnose		
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. See the following figure.

SN	IP Address	Time
1	192.168.11.1	5.541 ms 2.371 ms 2.088 ms
2	172.16.200.1	2.133 ms 1.775 ms 8.384 ms
3	192.168.20.1	6.643 ms 3.543 ms 2.774 ms
4	192.168.21.254	1.885 ms 4.249 ms 2.758 ms

Document Version: V1.0

8.2.4 Speed test

Overview

You can use the **Speed Test** to test the connection speed between two bridging CPEs, which helps estimate the throughput between the two CPEs. The test requires that both sides can use the **Speed Test** function.

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

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

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

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

Example of configuring the speed test

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

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

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

Configuration procedure

- **1.** <u>Log in to the web UI</u> of the CPE2.
- 2. Navigate to Advanced > Diagnose.

Document Version: V1.0

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

Diag	nose		
	Diagnose	Speed Test	~
	1 AVG RX	👃 AVG TX	🕼 AVG Total
	0 Mbps	0 Mbps	0 Mbps
		● Client ○ Serv	er
	IP Address of Peer AP	Manual	~
	IP Address	192.168.2.1	
	HTTP Port	80	
	User Name	admin	
	Password	admin	
	Test Group	10	(Range: 1 to 20)
	Direction	Bidirectional	~
	Time	30	s (Range: 1 to 60)
		Start	

----End

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

gnose		
Diagnose	Speed Test	*
1 AVG RX	👃 AVG TX	👫 AVG Total
8.83 Mbps	0 Mbps	4.86 Mbps

Document Version: V1.0

8.2.5 Spectrum analysis

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

- 🍎 - Tip

- Bridging CPEs must operate in the same channel.
- Only some CPE models support checking noise intensity. The actual product shall prevail.

Channel utilization (Example: CPE13V2.0)

Configuration procedure

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

Diagnose		
Diagnose	Spectrum Analysis	
	Channel Utilization	○ Noise Intensity
Frequency Band	36(5180MHz) 🗸 —	48(5240MHz) V
	Start	

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

Note	\times
All wireless connections will be terminated when the spectrum analysis is launching on the device! Please click OK	to Start.
OK Cancel	

----End

Document Version: V1.0

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



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

Noise intensity (Example: CPE13V2.0)

Configuration procedure

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

Document Version: V1.0

Diagnose		Current Mode: Station
Diagnose	Spectrum Analysis 🗸 🗸	?
	O Channel Utilization	Average Value 🗸
Frequency Band	36(5180MHz) ♥ ── 48(5240MHz) ♥	
	Start	

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

	~
ated when the spectrum analysis is launching on the	device! Please click OK to Start.
OK Cancel	
	nated when the spectrum analysis is launching on the OK Cancel

----End

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

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



Document Version: V1.0

8.3 Bandwidth control

8.3.1 Overview

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

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

To access the configuration page, <u>log in to the web UI</u> of the CPE and navigate to **Advanced** > **Bandwidth Control**.

Bandwidth Control	I			Current N	Node: Router
F	Remark				?
IP Address	Range 192.168.2.	~ 192.168.2.			
Max. Uploa	ad Rate	Mbps	~		
Max. Downloa	ad Rate	Mbps	~		
	Add				
ID Remark II	P Address Range	Max. Upload Rate	Max. Download Rate	Status	Action

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

Document Version: V1.0

8.3.2 Example of configuring bandwidth control

Networking requirements

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

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

Configuration procedure

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

andwidth Control				Current Mode:
Remark	Office_1			
IP Address Range	192.168.2. 100 ~ 192.16	58.2. 200		
Max. Upload Rate	5	Mbps	~	
Max. Download Rate	10	Mbps	~	

----End

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

ID	Remark	IP Address Range	Max. Upload Rate	Max. Download Rate	Status	Action
1	Offic_1	192.168.2.100~192.168.2.200	5Mbps	10Mbps	Enable	Ū
10 💉	 Datas/Pa 	age 1 data in total				

Document Version: V1.0

Verification

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

Document Version: V1.0

8.4 Port forwarding

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

8.4.1 Overview

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

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

To access the configuration page, <u>log in to the web UI</u> of the CPE and navigate to **Advanced** > **Port Forwarding**.

Port Forwarding			Current Mode: Rout	er
Internal IP Address			•	?
Internal Port	23			
External Port	23			
Protocol	TCP&UDP	~		
Application	Telnet	~		
	Add			

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

Document Version: V1.0

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

8.4.2 Example of configuring port forwarding

Networking requirements

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

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

Solution

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

Assume that:

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

Document Version: V1.0

- 🏹 - Tip

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



Configuration procedure

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

Document Version: V1.0

Forwarding			Current	Mod
Internal IP Address	192.168.2.100			
Internal Port	9999			
External Port	9999			
Protocol	TCP&UDP	~		
Application	HTTP	~		
	Add			

----End

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

ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	9999	9999	TCP&UDP	HTTP	Enable	Ī
1 10 🗸	192.168.2.100 Datas/Page 1 data in		9999	TCP&UDP	HTTP	Enable	

Verification

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

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

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

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



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

- Ensure that the WAN IP address of the CPE is a public IP address, and the internal port you entered is correct.
- Security software, antivirus software, and the built-in OS firewall of the server may cause port forwarding function failures. Disable them and try again.

Document Version: V1.0

 Manually set an IP address and related parameters for the server to avoid the service disconnection caused by the dynamic IP address.

Document Version: V1.0

8.5 MAC filter

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

8.5.1 Overview

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

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

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

MAC Filter	
Mode	Allow 🗸
Remark	
MAC Address	
Time	00 •: 00 • ~ 00 •: 00 •
Date	☐ Mon. ☐ Tue. ☐ Wed. ☐ Thur.
	□ Fri. □ Sat. □ Sun. □ Every Day
	Add

Name	Description
	Specifies the mode of MAC filter rule.
	 Disable: Disable the MAC Filter function.
Mode	 Allow: Only allow devices with the MAC addresses in the list to access the internet with the CPE.
	 Disallow: Only disallow devices with the MAC addresses in the list to access the internet with the CPE.
Remark	Specifies the additional information of the rule.
MAC Address	Specifies the MAC address of the device to which the rule applies.

Document Version: V1.0

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

8.5.2 Example of configuring MAC filter

Networking requirements

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

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

Solution

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

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

Configuration procedure

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

Document Version: V1.0

Mode	Allow 🗸	
Remark	Purchasing	
MAC Address	CC:3A:61:71:1B:6E	
Time	08 •:00 • ~ 18 •:00	~
Date	☑ Mon. ☑ Tue. ☑ Wed.	Thur.
	🗹 Fri. 🗌 Sat. 🗌 Sun.	🗌 Every Day

----End

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

ID	Remark	MAC Address	Time	Mode	Status	Action
1	Purchasing	CC:3A:61:71:1B:6E	Mon. 、Tue. 、Wed. 、Thur. 、Fri. 00:00-00:00	Allow	✓ Enable	
10 🗸	Datas/Page	1 data in total				

Verification

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

Document Version: V1.0

8.6 Network service

8.6.1 DDNS

Overview

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

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

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

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

Network Service		Current Mode: Router
DDNS	\bigcirc	?
Service Provider	3322.org 🗸	Register
User Name		
Password		
Domain Name		

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

Document Version: V1.0

Example of configuring DDNS

Networking requirements

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

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

Solution

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

Assume that:

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

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

The registered domain name information is shown as below:

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



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

Document Version: V1.0



Configuration procedure

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

DDNS		
Service Provider	Dyndns 🗸	<u>Reg</u>
User Name	JohnDoe	
Password	•••••	
Domain Name	JohnDoe.dyndns.com]

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

Document Version: V1.0

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

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

6) Click Add.

Port Forwarding			Current Mode: Rou
Internal IP Address	192.168.2.100		
Internal Port	9999		
External Port	9999		
Protocol	TCP&UDP	~	
Application	HTTP	~	
	Add		

----End

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

ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	9999	9999	TCP&UDP	HTTP	✓Enable	
10 V Datas/Page 1 data in total							

Verification

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

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



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

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

Document Version: V1.0

8.6.2 Remote web management

Overview

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

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

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

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

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

Remote Web Management		
IP Address	All	~
Port	8080	

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

Document Version: V1.0

Example of configuring remote web management

Networking requirements

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

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

Solution

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

Assume that:

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

Configuration procedure

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

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

----End

Verification

The host can log in to the web UI of the CPE by visiting <u>http://202.105.106.55:8080</u> on the computer (the IP address of the computer is 202.105.88.77). If the <u>DDNS</u> function is enabled

Document Version: V1.0

on the CPE, you can access the CPE by visiting an address in the form of http://WAN port's domain name:8080.

8.6.3 Reboot schedule

Overview

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

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

Configuration procedure

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

Reboot Schedule	
Time	01:00
Date	🗹 Mon. 🗹 Tue. 🗹 Wed. 🗹 Thur.
	🗹 Fri. 🗹 Sat. 🗹 Sun. 🗹 Every Day

----End

After successfully configured, the CPE will automatically reboot at 1 a.m. every day.

8.6.4 Login timeout interval

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

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

Document Version: V1.0

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.

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.

Document Version: V1.0

SNMP protocol version

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

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

MIB introduction

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



SNMP agent basic configuration

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

Document Version: V1.0

SNMP Agent	
Device Name	CPE6SV2.0
Read Community	public
Read/Write Community	private
Location	

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

Document Version: V1.0

Example of configuring the SNMP function

Networking requirements

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



Configuration procedure

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

SNMP Agent	
Device Name	CPE6SV2.0
Read Community	FLASH
Read/Write Community	FLASH-11
Location	

2. Set up the NMS.

Document Version: V1.0

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

----End

Verification

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

8.6.6 Ping watch dog

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

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

Configuration procedure

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

Ping Watch Dog		
IP Address	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

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

Document Version: V1.0

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

8.6.7 DMZ host

Overview

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

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



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

To access the configuration page, <u>log in to the web UI</u> of the CPE and navigate to **Advanced** > **Network Service**.
Document Version: V1.0

DMZ Host	
DMZ Host IP Address	

Parameters description

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

Example of configuring DMZ host

Networking requirements

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

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

Solution

You can use DMZ Host function to solve the problem.

Assume that:

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



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

Document Version: V1.0



Configuration procedure

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

----End

Verification

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

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

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

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

Document Version: V1.0

- 🍎 - Tip

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

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

8.6.8 Telnet service

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

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



8.6.9 UPnP

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

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

By default, the function is disabled. You can enable it as required.



8.6.10 Hardware watch dog

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

Document Version: V1.0

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

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.

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

By default, the function is disabled.



Document Version: V1.0

9 Tools

9.1 Date & time

To access the configuration page, <u>log in to the web UI</u> of the CPE and navigate to **Tools** > **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.

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

- Тір

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 on the internet. This enables the CPE to automatically correct its system time after being connected to the internet.

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

Configuration Procedure

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

Document Version: V1.0

Date & Time	?
Time Settings	Synchronized with the Internet O Manual
Time Interval	30 minutes V
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei 🖌
	Save

----End

After the configuration is completed, you can navigate to <u>Status</u> page to check whether the system time of the CPE is correct.

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

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

Document Version: V1.0

Date & Time		2
	Time Settings	○ Synchronized with the Internet
	Date & Time	2024 Y 03 M 14 D 08 h 44 m 18 s
		Synchronize with PC Time
		Save

----End

After the configuration is completed, you can navigate to <u>Status</u> page to check whether the system time of the CPE is correct.

Parameters description

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

Document Version: V1.0

9.2 Maintenance

9.2.1 Reboot device

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

- - Tip

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

Configuration procedure

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

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(5410) ; Release Date: 2021-07-14 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. Confirm the prompt information, and click **OK**.

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

----End

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

Document Version: V1.0

9.2.2 Restore 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.

Wote

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

Option 1: Reset the CPE through the web UI

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

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(5410) ; Release Date: 2021-07-14 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. Confirm the prompt information, and click **OK**.

The IP addre	ess will be reset to 19	2.168.2.1. Are you su	e to reset it?
The fir double		ErroolErrivito you ou	0 10 10001 111

----End

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

Document Version: V1.0

Option 2: Reset the CPE through the Reset button

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

9.2.3 Upgrade firmware

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

Note

To prevent damaging the device, ensure that:

- The new firmware version is applicable to the device before upgrading the firmware. Generally, the suffix of the upgrade file is .bin.
- Keep the power supply of the CPE connected during an upgrade.

Configuration procedure

- 1. Download the firmware upgrade package for the CPE from <u>www.ip-com.com.cn</u> to your local computer, and decompress the package.
- 2. Log in to the web UI of CPE, and navigate to Tools > Maintenance.
- 3. Click Upgrade.

Maintenance	
Reboot Device	Reboot
Reset to Factory Settings	All connections will disconnect during reboot.
Upgrade Firmware	All configurations will restore to default factory setting after reset.
	Current Software Version: V1.0.0.2(5410) ; Release Date: 2021-07-14 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 (extension: bin) from your local computer and the system will upgrade automatically.

----End

Document Version: V1.0

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

- Тір

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

9.2.4 Backup/restore

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

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

Tip

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

Backup

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

Maintenance	
	?
Reboot Device	Reboot
	All connections will disconnect during reboot.
December Fristerie Cattlene	
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(5410) ; Release Date: 2021-07-14
	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
	banap canon county of importance settings to donto

Document Version: V1.0

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

ckup/Restore		~
Backup configurations	Backup	
Import configurations	Restore	

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

 ΕI	n	d
_		-

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

Restore

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

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(5410) ; Release Date: 2021-07-14 Note: Do not disconnect the power supply of the device during upgrade
Backup/Restore	Backup/Restore Backup current settings or import saved settings to device

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

Backup/Restore		×
Backup configurations	Backup	
Import configurations	Restore	

Document Version: V1.0

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

----End

After the file is uploaded, the CPE reboots automatically.

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

9.3 Account

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

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



Click 🥑 to change the account information.

9.3.1 Administrator

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

- ф-тір

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

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

Document Version: V1.0

Parameters description

Name	Description
Old User Name	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
	Guest user name/password: user
New User Name	Specifies a new login user name.
New Password	Specifies a new login password.
Confirm Password	Enter the new login password again.

9.3.2 Guest

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

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

9.4 System log

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

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

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

System Log			
Refresh	Clear		Log Type All 🗸
ID	Time	Туре	Log
1	2024-03-14 10:35:40	System	web 192.168.2.20 login
2	2024-03-14 10:35:31	System	web login time expired
3	2024-03-14 10:10:53	System	web 192.168.2.20 login
4	2024-03-14 10:10:46	System	web login time expired

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

- Note

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

Document Version: V1.0

Appendix

A.1 Default parameters

The main default parameters are shown in the following table.

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

Document Version: V1.0

		Document version. V1.0
Parameters		Default settings
	Gateway Address	192.168.2.254
	Primary DNS Server	8.8.8.8
	Lease Time	1 day
	VLAN Settings	Disable
	PVID	1
VLAN Settings	Management VLAN	1
	WLAN	1000
	Wireless Network	Enable
		Operating RF: IP-COM_XXXXXX, and XXXXXX is the last six characters of the LAN MAC address of the device.
	SSID	Management RF: IP-COM_XXXXXX_MG, and XXXXXX is the last six characters of the LAN MAC address of the device.
Wireless		⁻с҉ш҉҈Ѓ-тір
		The management RF is not available for some CPEs.
	Security Mode	None
	Transparent Bridge	Enable
	TD-MAX	Disable
	ТРС	Enable
	Login Timeout Interval	5 min
	Ping Watch Dog	Disable
Network Service	Telnet Service	Enable
NELWOIK SERVICE	UPnP	Disable
	Hardware Watch Dog	Enable
	STP	Disable

Document Version: V1.0

Parameters		Default settings	
Tools	Date & Time	Synchronized with the internet	

A.2 Acronyms and Abbreviations

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

Document Version: V1.0

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

Document Version: V1.0

Acronym or Abbreviation	Full Spelling	
STP	Spanning Tree Protocol	
SNMP	Simple Network Management Protocol	
ТСР	Transmission Control Protocol	
TDMA	Time Division Multiple Access	
ТРС	Transmit Power Control	
ТКІР	Temporal Key Integrity Protocol	
тх	Transmit	
UDP	User Datagram Protocol	
UI	User Interface	
UPnP	Universal Plug and Play	
VID	VLAN Identifier	
VLAN	Virtual Local Area Network	
WAN	Wide Area Network	
WDS	Wireless Distribution System	
WEP	Wired Equivalent Privacy	
WISP	Wireless Internet Service Provider	
WLAN	Wireless Local Area Networks	
WMM	WiFi Multi-Media	
WPA	WiFi Protected Access	
WPA-PSK	WPA-Preshared Key	

Document Version: V1.0

A.3 How to 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.

	Local Area Connection Status	X	
🕞 💬 🐺 « Network a	" 		th Control Panel 🔎
	General		0 ^
Control Panel Home	Connection		up connections
Change adapter settings	IPv4 Connectivity:	Internet	See full map
	IPv6 Connectivity:	No network access	1 👻 · ·
Change advanced sharing settings	Media State:	Enabled	Internet
	Duration:	00:03:46	
	Speed:	1.0 Gbps	Connect or disconnect
	Details		pe: Internet
			ons: U Local Area Connection
	Activity		
	Sent —	Received	Ξ
	Bytes: 302,00	2 4,743,842	PN connection; or set up a router
	Properties Disable	Diagnose	or VPN network connection.
See also		Close	
HomeGroup			computers, or change sharing
Internet Options	settings.		
Windows Firewall	Troubleshoot	problems	
Windows Filewan		repair network problems, or get tr	oubleshooting information.

Document Version: V1.0

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 Mapper 🖄 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**.

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 automatical	у		
O Use the following IP address:			
IP address:	192.168.2.20		
Subnet mask:	255.255.0		
Default gateway:	· · ·		
Obtain DNS server address automatically			
O Use the following DNS server add	resses:		
Preferred DNS server:			
Alternate DNS server:	· · ·		
Validate settings upon exit	Advanced		
	OK Cancel		

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

----End

Document Version: V1.0

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

OS example: Windows 7

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



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

				_ D X
💮 🖓 🖳 🖉 « Ne	etwork and Internet 🕨 Network a	nd Sharing Center	🗸 🍫 Search Control Panel	Q
Control Panel He Change adapter Change advance settings	Local Area Connection Status General Connection		nd set up connections	See full map
	IPv4 Connectivity: IPv6 Connectivity: Media State: Duration: Speed: Details	No Internet access No network access Enabled 00:04:38 100.0 Mbps	Access type: No Intern	et or disconnect et access a <u>Connection</u>
	Activity ————————————————————————————————————	- Received	hoc, or VPN connection; or : I, dial-up, or VPN network co	
See also HomeGroup Internet Options Windows Firewa	Properties Disable	Diagnose	network computers, or char	

----End

Document Version: V1.0

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

	s
Network Connection Details:	
Property	Value
Connection-specific DN	tendawifi.com
Description	Intel(R) 82583V Gigabit Network Connect
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
	Close
	Close