

User Guide

Outdoor CPE

Applicable to single and kit product



www.tendacn.com

differ with product models. The actual product prevails.

Document Version: V2.1

Copyright Statement

© 2021-2023 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

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

Disclaimer

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

Document Version: V2.1

Preface

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

Conventions

This user guide applies to the Tenda CPEs (single and kit products). O4 is used for illustrations here unless otherwise specified.

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 contained images and web UI screenshots are subject to the actual products.

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

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

For more documents

If you want to get more documents about the device, visit <u>www.tendacn.com</u> and search for the corresponding product model.

Document Version: V2.1

Technical support

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

Email address: support@tenda.cn

Website: www.tendacn.com

Revision history

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since this guide was first published.

Version	Date	Description
		 Added the description of the <u>Packet filter</u> and <u>Management</u> <u>RF</u> function.
V2.1	2023-11-30	 Optimized the description of the <u>CCTV surveillance</u>, <u>Login</u>, <u>Wireless status</u> and <u>Spectrum analysis</u> function. Optimized sentence expression.
V2.0	2021-11-25	 Added the description of <u>Transparent WDS</u> function. Fixed some known issues.
V1.0	2020-07-04	Original publication.

Document Version: V2.1

Contents

1	Typical application scenario	1
	1.1 CCTV surveillance	1
	1.2 ISP hotspot connection-WISP mode	12
2	Login and logout	16
	2.1 Login	16
	2.2 Logout	21
3	Web UI	22
	3.1 Web UI layout	22
	3.2 Common buttons	23
4	Quick setup	24
	4.1 AP mode	25
	4.2 Client mode	28
	4.3 Universal repeater mode	31
	4.4 WISP mode	34
	4.5 Repeater mode	40
	4.6 P2MP mode	52
	4.7 Router mode	59
		64
5	Status	64
	5.1 System status	64
	5.2 Wireless status	67
	5.3 Statistics	70
6	Network	76
	6.1 LAN setup	76
	6.2 Packet filter	82

Document Version: V2.1

	6.3 MAC clone	
	6.4 DHCP server	86
	6.5 DHCP client	
	6.6 VLAN settings	
7	Wireless settings	
	7.1 Basic configuration	
	7.2 Advanced settings	
	7.3 Access control	
	7.4 Management RF	
8	Advanced	
	8.1 LAN rate	
	8.2 Diagnose	
	8.3 Bandwidth control	142
	8.4 Port forwarding	145
	8.5 MAC filter	
	8.6 Network service	
9	Tools	
	9.1 Date & time	
	9.2 Maintenance	
	9.3 Account	
	9.4 System log	
Ар	pendix	
	A.1 Default parameters	
	A.2 Acronyms and Abbreviations	
	A.3 How to assign a fixed IP address to your computer	
	A.4 How to check the gateway IP address of a computer	

Document Version: V2.1

1 Typical application scenario

₽TIP

- At least two CPEs are required for bridging. Different application scenarios require different CPE models. For more information, visit <u>www.tendacn.com</u>.
- A CPE can use 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 O1-5G.
 You only need to <u>install the CPEs</u> to easily manage the CCTV surveillance for the community.
- Method 2: Use two CPEs to set up a monitoring network, such as the CPE O4. You only
 need to <u>Set up the CPEs</u> > <u>Install the CPEs</u> to easily manage the CCTV surveillance for
 the community.

₽TIP

To facilitate you to quickly set up a monitoring network, it is recommended to set up the CPEs first and then install the CPEs.

Document Version: V2.1

1.1.2 Set up the CPEs (Example: O4)

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

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

Step 1 Place the two CPEs next to each other.



- **Step 2** Power on the CPEs (powered by PoE in this example).
 - 1. Uncover the housing of the CPE.
 - 2. Use an Ethernet cable (CAT5e or above is recommended) to connect the PoE/LAN port of the device 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.

Document Version: V2.1

¥TIP

- If the CPE supports DC power supply, you can use the correct power adapter to power on the CPE. The power parameters can be checked on the label of the CPE. If the power adapter is not included in the product package, you can purchase it by yourself (interface specification: 5.5*2.1 mm).
- Some CPEs can use PoE power supply device with IEEE 802.3af standard. For details, visit <u>www.tendacn.com</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.tendacn.com</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 will bridge to each other automatically, and the LED1, LED2 and LED3 indicators of the two CPEs blink fast. When the LED1, LED2 and LED3 indicators of a CPE light solid on while the LED1, LED2 and LED3 indicators of the other CPE blink slowly, the peer-to-peer bridging succeeds.

₽_{TIP}

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

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



₽_{TIP}

If the peer-to-peer automatic bridging fails, reset the two CPEs to factory settings, and try again. Reset method: After CPE completes startup, hold down the reset button (such as RST, RESET or Reset) for about 8 seconds, and then release it when all indicators light up.

Option 2: Manual bridging



Step 1 Place the two CPEs next to each other.

1. Power on the CPE1 (powered by PoE in this example).

Uncover the housing of the CPE. Use an Ethernet cable (CAT5e or above is recommended) to connect the PoE/LAN port of the device to the PoE port of the PoE injector. Use the

Document Version: V2.1

included power cord to connect the PoE injector to a power socket. The PoE/LAN LED indicator of the CPE lights up.

₽TIP

- If the CPE supports DC power supply, you can use the correct power adapter to power on the CPE.
 The power parameters can be checked on the label of the CPE. If the power adapter is not included in the product package, you can purchase it by yourself (interface specification: 5.5*2.1 mm).
- Some CPEs can use PoE power supply device with IEEE 802.3af standard. For details, visit <u>www.tendacn.com</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.tendacn.com</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 (**192.168.2.1** by default) in the address bar, and press the **Enter** (or **Return**) key on your keyboard.



Document Version: V2.1

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

O4V1.0			
Default user name: admin Default password: admin			
Login			
Forget password?			

₽TIP

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

- Ensure that the CPE is powered on properly.
- Ensure that the computer is connected to the LAN port of the CPE properly.
- Ensure that the IP address of the computer is on the same network segment as that of the CPE's IP address. For example, if the IP address of the CPE is 192.168.2.1, you can set the IP address of the computer to 192.168.2.X (X ranges from 2 to 254 and is not occupied).
- If more than one CPE is connected, modify the IP address of each one to avoid the login failure due to IP address conflict.
- Reset the CPE to factory settings. Reset method: After CPE completes startup, hold down the reset button (such as RST, RESET or Reset) for about 8 seconds, and then release it when all indicators light up.

Step 3 Set CPE1 to AP Mode.

1. Navigate to Quick Setup. Select AP mode, and click Next.

Document Version: V2.1

Select a v	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.
Univer	rsal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
WISP wireless n	In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the letwork.
Repea wireless a	ter In this mode, the device connects to multiple wired networks through wireless bridge, and provides ccess point.
P2MP wireless a	In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide ccess point.
Route	r connect to modem in wired manner, and provide network access point

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

Quick Setup>>AP	
	2
You can set up your wireless netwo	ork name and wireless password here.
Note down your wireless password	
SSID	Tenda_123456
Channel	·
Security Mode	WPA2-PSK
Encryption Algorithm	● AES ◎ TKIP ◎ TKIP&AES
Кеу	
	Previous

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

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

- **Step 4** Log in to the web UI of CPE2 and set to the 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.

Document Version: V2.1

Select a w	rorking mode:
OAP 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.
University	sal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
○ WISP wireless net	In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the etwork.
Repeat wireless ac	er In this mode, the device connects to multiple wired networks through wireless bridge, and provides ccess point.
P2MP wireless ac	In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide ccess point.
Router	connect to modem in wired manner, and provide network access point

3. Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next**.



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

Quick Setu	ıp>>Client				. 2
Click "Scan", and click "Ne	and select the wireles ext".	s network you wa	int to connect,		2
	Scan	Scan agai	<u>n</u>		
	Upstream AP	Tenda_123456			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	Tenda_123456			WPA2-PSK,AES	.atl

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

Quick Setup>>Client	6 7
Ensure that the device uses the sa Then enter the remote AP's WiFi p	me channel, encryption, and encryption algorithm as those of upstream AP. password, and click "Next" to continue.
Upstream AP	Tenda_123456
Upstream AP MAC Address	
Channel	T
Security Mode	WPA2-PSK
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Key	
	Previous

Document Version: V2.1

 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 of the first CPE, and click Next.

For example, if the IP address of CPE1 is 192.168.2.1, you can set this CPE's IP address to 192.168.2.*X* (*X* ranges from 2 to 254 and is not occupied). Then click **Next**.

Quick Setup>>Client					2
Set the IP address to an unused IP	address belonging to the n	etwork segment of upstream AP.			-
IP Address	192.168.2.100				
Subnet Mask	255.255.255.0				
			Previous	Next	

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

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

----End

When the two CPEs are bridging to each other, all the LED1, LED2 and LED3 indicators blink fast. When the LED1, LED2 and LED3 indicators of a CPE light solid on while the LED1, LED2 and LED3 indicators of the other CPE blink slowly, the bridging succeeds. 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 O2 and O3, the bridging procedure is as follows:

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

Document Version: V2.1

1.1.3 Install the CPEs (Example: O4)

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 2

Document Version: V2.1

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

LED Indicator	Status	Description
LED1, LED2, LED3 (Received signal strength LED indicators)	Solid on/Blinking	 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. ✓ You can change them 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).

Document Version: V2.1

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

O4 is used as an example to illustrate the installation procedures. Procedures for other CPEs are similar.

₽TIP

To facilitate you to quickly set up a monitoring network, it is recommended to set up the CPEs first and then install the CPEs.

1.2.2 Set up the CPE

Step 1 Power on the CPE (powered by PoE in this example).

- 1. Uncover the housing of the CPE.
- 2. Use an Ethernet cable (CAT5e or above is recommended) to connect the PoE/LAN port of the device 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.



VTIP

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

Step 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: V2.1



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

Quick Set	<u>up</u>
Select a wo	rking mode:
● AP In th	is mode, the device creates a wireless network based on the current wired network.
Client Ir	n this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
Universal	Repeater In this mode, this device extends an existing wireless network for broader network coverage.
WISP In wireless netv	this mode, this device connects to an access point provided by ISP in wireless manner, and provides the work.
Repeater wireless acce	\cdot In this mode, the device connects to multiple wired networks through wireless bridge, and provides ess point.
P2MP Ir wireless acce	n this mode, the device connects to multiple wired networks through wireless bridge, but does not provide ess point.
O Router	connect to modem in wired manner, and provide network access point
	Next

4. Select the wireless network of your ISP hotspot, which is **Tenda_123456** in this example, and click **Next**.

Document Version: V2.1

Quick Setu	ip>>WISP				
Click "Scan", and click "Ne	and select the wireless ext".	network you war	nt to connect,		
	Scan	Scan again	I		
	Upstream AP	Tenda_123456			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	Tenda_123456			WPA2-PSK,AES	.atl

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

Quick Setup>>WISP	
Ensure that the device uses the sa	ame channel, encryption, and encryption algorithm as those of upstream AP.
Then enter the remote AP's WiFi	password, and click "Next" to continue.
Upstream AP	Tenda_123456
Upstream AP MAC Address	
Channel	T
Security Mode	WPA2-PSK T
Encryption Algorithm	● AES
Key	
	Previous

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

Quick Setup>>WISP			
Please select an internet connect and click "Next".	on type, and enter the in	ternet parameters provi	ded by your ISP.
Internet Connection Type	DHCP (Dynamic IP)	Static IP Address	PPPoE
PPPoE User Name			
PPPoE Password			
			Previous Next

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

Document Version: V2.1

rou can set up your wireless netw	fork name and wireless password here.
Note down your wireless passwor	d.
SSID(Wireless Network	Tenda
Name)	
Channel	T
Security Mode	WPA2-PSK T
Encryption Algorithm	● AES
Кеу	

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

Quick Setup>>WISP			
Specify the device with an IP addre or upstream AP.	ess whose network segmen	t is different from that of IP address of ISP ac	cess point
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: V2.1

2 Login and logout

2.1 Login

2.1.1 Login with computer

- **Step 1** Connect the computer to the CPE or the switch connected to the CPE.
- **Step 2** Set the IP address of the computer to an unused one belonging to the same network segment of the IP address of the CPE. (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 subnet mask to 255.255.255.0.

Internet Protocol Version	4 (TCP/IPv4) Properties		
General			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.			
Obtain an IP addre	ss automatically		
─◎ Use the following If	P address:		
IP address:	192.168.2.10		
Subnet mask:	255.255.255.0		
Default gateway:			
 Obtain DNS server address automatically 			
• Use the following D	NS server addresses:		
Preferred DNS server	:		
Alternate DNS server	:		
🔲 Vaļidate settings u	pon exit Ad <u>v</u> anced		
	OK Cancel		

Step 3 Start a web browser on your computer, visit the IP address of the CPE (By default, AP mode: 192.168.2.1. Client mode: 192.168.2.2), and press the Enter (or Return) key on your keyboard.

 $\leftarrow \rightarrow$ C (3) 192.168.2.1 (1) (2) (3) (3)

Document Version: V2.1

Step 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 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.
- Reset the CPE to factory settings. Reset method: After CPE completes startup, hold down the reset button (such as RST, RESET or Reset) for about 8 seconds, and then release it when all indicators light up.
- The default login user name and password of the CPE are **admin**. For the network security, refer to the <u>Account</u> to change the login user name and password.

----End

Document Version: V2.1

After the successful login, the following page appears.

🕨 Status	Quick Setup
Quick Setup	Select a working mode:
Network	 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.
Wireless	O Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
🕻 Advanced	WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
% Tools	Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
	P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
	Router connect to modem in wired manner, and provide network access point
	Next

2.1.2 Login with smartphone or tablet

Take iPhone as an example. Other mobile clients are similar.

Step 1 Connect the smartphone to the wireless network of the CPE, which is **Tenda_123456** in this example.

Settings	WLAN
WLAN	
NETWORKS	
Tenda_123456	₽ ? (1)
	■ ? (1)
	∎ ? (i)
	🔒 🗢 📋
	a 🗢 (i)
	? (j)
	a 🗢 (i)

Document Version: V2.1

Step 2 Set the IP address of the smartphone to an unused one belonging to the same network segment of the IP address of 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 subnet mask to 255.255.255.0.

〈 WLAN Tenda_123	456	K Back	Configure IPv4	Save
Join This Network		Automotio		
		Automatic		
Private Address		Manual		
WLAN Address	10000	BootP		
Using a private address helps reduc across different WLAN networks.	e tracking of your iPhone	•		
IPV4 ADDRESS		MANUAL IP		
Configure IP	Automatic >	IP Address	192	2.168.2.10
DNS		Subnet Mask	255.2	255.255.0
Configure DNS	Automatic >	Router	19	92.168.2.1
HTTP PROXY		<u>.</u>		
Configure Proxy	Off >			

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

Settings WLAN	
WLAN	
✓ Tenda_123456	₽ ? (i)
NETWORKS	
	🔒 🗟 i
	a 🗢 (i)
	a 🗟 i
	🔒 🗟 i
	🔒 🗢 i
	🔒 🗟 i
	a 🗟 🕯

Step 4 Start a browser on your smartphone, 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.

Document Version: V2.1



Step 5 Enter your user name and password, and click **Login**.

The following figure is for reference only.

AA	19	2.168.2.1		Ċ
Ten da				
	Q6¥3.0			
	A. Deta	ult upper names, polimies		
	A 0-6	at passard active 🛛 😽		
	Q inc	i.a 💌		
		Forget password?		
,		•	~	
<	>		Ш	Ū

----End

After the successful login, the following page appears.



20

Document Version: V2.1

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: V2.1

3 Web UI

3.1 Web UI layout

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

	Ctatus	LAN Setup	Current Mode: AP
.14	Status		4
\$	Quick Setup	MAC Address	C8:3A:35:15:87:50
	Network	IP Address Type	Static IP Address
	LAN Setup	IP Address	192.168.2.1
	DHCP Server	Subnet Mask	255 255 255 0
	DHCP Client	Sublict Mask	233.233.233.0
	VLAN Settings	Default Gateway	0.0.0.0
((r	Wireless	Primary DNS Server	0.0.0.0
*	Advanced	Secondary DNS Server	0.0.0.0
۵,	Tools	Device Name	O4V1.0
			Save

₽TIP

Functions or parameters in grey fields indicate that are not available for the CPE or they cannot be modified under the current configurations.

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

Document Version: V2.1

3.2 Common buttons

Common Buttons	Description
Refresh	Used to update the contents on the current page.
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.
?	Used to view help information corresponding to the settings on the current page.

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

Document Version: V2.1

4 Quick setup

₽_{TIP}

If it is the CPE kit, the two CPEs are already bridged at the factory and can be installed directly.

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

Refer to the following instructions to select the appropriate working mode:

- <u>AP</u>: In this mode, the CPE creates a wireless network based on the current wired network.
- <u>Client</u>: In this mode, the CPE works as a wireless adapter to connect to the wireless network of upstream AP. Working in Client mode, the CPE does not provide wireless access service, and a client needs to be connected to the CPE with an Ethernet cable.
- <u>Universal Repeater</u>: In this mode, the CPE extends an existing wireless network for broader network coverage. The new wireless network has the same SSID, password, and related wireless information as the upstream wireless network.
- <u>WISP</u>: In this mode, the CPE connects to a hotspot provided by ISP in a wireless manner, and provides the wireless network. The CPE can also be connected to the 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: V2.1

4.1 AP mode

4.1.1 Overview

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

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



Document Version: V2.1

4.1.2 Set AP mode

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

Step 2 Select AP mode and click Next.

Quick Setup
Colorte condec
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.
Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
Router connect to modem in wired manner, and provide network access point
Next

- **Step 3** Set **SSID**, which is **Tenda_123456** in this example.
- **Step 4** Set **Security Mode**, which is **WPA2-PSK** in this example.
- **Step 5** Set **Encryption Algorithm**, which is **AES** in this example.
- **Step 6** Set **Key**, which is **UmXmL9UK** in this example. And click **Next**.

You can set up your wireless network name and wireless password here.	Setup>>AP																Cu	rrent	Mo	de:	AP
You can set up your wireless network name and wireless password here.																					?
	i set up your wireless network name and	eless passv	assw	sw	SW	w	/0	ore	rar	ner	re.										
Note down your wireless password.	own your wireless password.																				
* SSID Tenda_123456	* SSID Tenda_123																				
				5	-																
Channel Auto 🔻	Channel Auto	•	٠	•	'																
* Security Mode WPA2-PSK V	* Security Mode WPA2-PSK	•	•	•	,	1															
* Encryption Algorithm 💿 AES 💿 TKIP 💿 TKIP&AES	* Encryption Algorithm AES 	IP O TK) TK	ΓKI	KI	KIF	[P	P8	βłΑ	ES											
* Kay	* Key		_		٦	١															
i key	. Key																				
																	_		_		
Previous Next															Previ	ious		Nex	t		

Step 7 Click Save, and wait until the device reboots automatically to make the settings take effect.

Document Version: V2.1

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

----End

Parameters description

Name	Description
SSID	specifies the WiFi name of CPE.
Channel	Specifies the operating channel of this device. Select a less used channel in the ambient environment to reduce interference. Auto indicates that the device automatically adjusts its operating channel according to the ambient environment.
Security Mode	Specifies the security mode of the wireless network, including: <u>None</u> , <u>WPA-PSK</u> , <u>WPA2-PSK</u> , and <u>Mixed WPA/WPA2-PSK</u> .
Encryption Algorithm	 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.

Document Version: V2.1

4.2 Client mode

4.2.1 Overview

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

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



4.2.2 Set client mode

- **Step 1** Log in to the web UI of the CPE, and navigate to **Quick Setup**.
- **Step 2** 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.
Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
■ WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the wireless network.
Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
Router connect to modem in wired manner, and provide network access point
Next

Document Version: V2.1

Step 3 Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next** at the bottom of the page.



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

Quick Setu	up>>Client			Cı	urrent Mode: Repeater
Click "Scan", and click "Ne	and select the wireles ext".	s network you wa	nt to connect,		•
	Scan	Scan agai	<u>n</u>		
	Upstream AP	Tenda_123456			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	Tenda_123456			WPA2-PSK,AES	1000

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

Quick Setup>>Client	21			
Ensure that the device uses the same channel, encryption, and encryption algorithm as those of upstream AP. Then enter the remote AP's WiFi password, and click "Next" to continue.				
Upstream AP	Tenda_123456			
Upstream AP MAC Address				
Channel	T			
Security Mode	WPA2-PSK T			
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES			
* Key				
	Previous			

Parameters description

Name	Description
Upstream AP	Specifies the WiFi name (SSID) of the upstream AP.
Upstream AP MAC Address	Specifies the MAC address of the upstream AP.

Document Version: V2.1

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 has a WiFi password, you need to enter the password manually.		
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.		

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

For example, if the IP address of the upstream AP is 192.168.2.1, you can set the IP address of this device to 192.168.2.X (X ranges from 2 to 254 and is not occupied).

Quick Setup>>Client					
Set the IP address to an unused IP	address belonging to the n	etwork segment of upstream A	۱P.		٦
IP Address	192.168.2.100				
Subnet Mask	255.255.255.0				
			Destaura		
			Previous	Next	

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

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

----End

After the CPE is rebooted, <u>log in to the web UI</u> of the CPE and navigate to **Status**. On the **Wireless Status** module, when the **Working Mode** is the Client mode and the **AP's MAC Address** is the WLAN MAC address of the peer device, the configuration is successful.
Document Version: V2.1

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 those of 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

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

Quick Se	tup
Select a wo	orking mode:
● AP In th	his mode, the device creates a wireless network based on the current wired network.
Client I	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.
• WISP In wireless net	n this mode, this device connects to an access point provided by ISP in wireless manner, and provides the work.
Repeate access point	r In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless t.
P2MP 1 wireless acc	In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide sess point.
Router	connect to modem in wired manner, and provide network access point
	Next

Step 3 Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next** at the bottom of the page.

Document Version: V2.1

Quick Setu	ıp>>Universal Rej	peater			
Click "Scan", and click "Ne	and select the wireles ext".	s network you w	ant to connect,		
	Scan	C Scan aga	in		
	Upstream AP	Tenda_123456	5		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	Tenda_123456			WPA2-PSK,AES	.atl

₽TIP

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

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

Quick Setup>>Universal Re	peater
	2
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those of upstream AP.
Then enter the remote AP's WiFi g	password, and click "Next" to continue.
Upstream AP	Tenda_123456
Upstream AP MAC Address	
Channel	T
Security Mode	WPA2-PSK •
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
* Key	
	Previous

Parameters description

Name	Description
Upstream AP	Specifies the WiFi name (SSID) of the upstream AP.
Upstream AP MAC Address	Specifies the MAC address of the upstream AP.
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.

Document Version: V2.1

Previous

Name		Description					
		Specifies the e	ncryption method	of the wireless network.			
		- AES:	It indicates the Ad	vanced Encryption Standard.			
Encryption Algorithm		- TKIP : maxi	 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 availa the s	&AES : It indicates table. Wireless clier elected SSID using	that both TKIP and AES encryption algorithms are its can connect to the wireless network corresponding to TKIP or AES.			
Кеу		Specifies the W	/iFi password of th	e wireless network.			
tep 5	Set the IP a of the route For exampl	ddress to an u er. e. if the IP add	nused IP address	s belonging to the same network segment as that er is 192.168.2.1. you can set this device's IP			
	address to	192.168.2.X (X	ranges from 2 to	5 254 and is not occupied). Then click Next .			
	Quick Setu	o>>Universal Re	peater	· · ·			
	Set the IP add	ress to an unused IP	address belonging to 1	? the network segment of upstream AP.			
		IP Address	192.168.2.100				
		Subnet Mask	255,255,255.0				

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



----End

After the CPE is rebooted, <u>log in to the web UI</u> of the CPE and navigate to **Status**. On the **Wireless Status** module, with the **Working Mode** is the Universal Repeater mode, if the SSID of the CPE is the same as the peer CPE and the **AP's MAC Address** is the WLAN MAC address of the peer device, the configuration is successful.

₽TIP

After the bridging is successful, the SSID and key of the CPE will become the same as those of the peer CPE.

4.4 WISP mode

4.4.1 Overview

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

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



4.4.2 Set WISP mode

Computer

- **Step 1** Log in to the web UI of the CPE, and navigate to **Quick Setup**.
- Step 2 Select WISP 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.
Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless access point.
P2MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide wireless access point.
Router connect to modem in wired manner, and provide network access point
Next

Document Version: V2.1

Step 3 Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next** at the bottom of the page.

9	<u>uick Set</u>	up>>WISP					?
C a	lick "Scan", nd click "N	, and select the wireless ext".	s network you wa	int to connect,			
		Scan	C Scan agai	<u>n</u>			
		Upstream AP	Tenda_123456				
	Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
_	۲	Tenda_123456			WPA2-PSK,AES	lle.	

₽_{TIP}

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

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

Quick Setup>>WISP	2
Ensure that the device uses the sam Then enter the remote AP's WiFi pas	e channel, encryption, and encryption algorithm as those of upstream AP. ssword, and click "Next" to continue.
Upstream AP	Tenda_123456
Upstream AP MAC Address	
Channel	▼
Security Mode	WPA2-PSK •
Encryption Algorithm	● AES ◎ TKIP ◎ TKIP&AES
··· Key	
	Previous

Parameters description

Name	Description
Upstream AP	Specifies the WiFi name (SSID) of the upstream AP.
Upstream AP MAC Address	Specifies the MAC address of the upstream AP.

Document Version: V2.1

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 has a WiFi password, you need to enter the password manually.
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: 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.

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

Quick Setup>>WISP				
				?
Please select an internet connection	type, and enter the int	ernet parameters provid	ded by your ISP.	
and click "Next".				
Internet Connection Type	DHCP (Dynamic IP)	Static IP Address	PPPoE	
PPPoF User Name				
PPPoE Password				
			Previous Next	

Document Version: V2.1

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.		

Step 6 Customize the **SSID**, set **Security Mode**, **Encryption Algorithm** and **Key**, and click **Next**.

Quick Setup>>WISP	
You can set up your wireless netwo	rk name and wireless password here.
Note down your wireless password	
SSID(WiFi Name)	Tenda_F11020
Channel	T
Security Mode	WPA2-PSK T
Encryption Algorithm	● AES
Key	
	Previous Next

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

Quick Setup>>WISP			
Specify the device with an IP addre or upstream AP.	ess whose network segment	is different from that of IP address of ISP access point	?
IP Address	192.168.5.1		
Subnet Mask	255.255.255.0		
		Previous	

Document Version: V2.1

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

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

----End

After the CPE is rebooted, 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, with the Working Mode is the WISP mode, if the SSID is the WiFi name you set in <u>Step 7</u> and the AP's MAC Address is the WLAN MAC address of the peer device, the configuration is successful.

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.



Document Version: V2.1

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

₽TIP

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

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

----End

To access the internet with:

- 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.

Document Version: V2.1

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



Configuration procedure

₽TIP

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**.

- **Step 1** Set the CPE1 to the **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.

Document Vers	ion: V	2.1
----------------------	--------	-----

Basic	
Enable Wireless	
Country/Region	China 🔻
SSID	Tenda_654321
Broadcast SSID	Enable Disable
Network Mode	11a/n 🔻
≭ Channel	×
Channel Shift	Enable
Transmit Power	1dBm 26dBm
* Channel Bandwidth	20MHz v
Transmit Rate	Auto 🔻
Security Mode	None •
Isolate Client	Enable Isable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

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

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

Document Version: V2.1

4. Select the wireless network to bridge from the list, which is **Tenda_123456** in this example, and click **Next** at the bottom of the page.

Quick Setu	p>>Repeater				
Click "Scan", a and click "Ne:	and select the wireles	s network you war	nt to connect,		
	Scan	C Scan agair	1		
	Peer AP1				
	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
	Tenda_123456			WEP	.ul

₽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. Set Authentication Type and Default Key, enter the Key 1, and click Next.

Quick Setup>>Repeater				
<u>2</u>				
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	ck "Next".			
Peer AP1	Tenda_123456			
MAC Address of Peer AP1				
Channel	•			
Security Mode	WEP •			
Authentication Type	Shared •			
Default Key	Key 1 🔻			
Key 1	•••••	ASCII V		
Key 2	•••••	ASCII V		
Key 3	•••••	ASCII V		
Key 4	•••••	ASCII •		
		Previous		

Document Version: V2.1

Parameters description

Name	Description	
Peer AP1	Specifies the WiFi name (SSID) of the peer AP1.	
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.	
Authentication Type	 Specifies the authentication type for the WEP security mode. The options include Open and Shared. The options share the same encryption process. Open: It specifies that authentication is not required and data exchange is encrypted using WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. Shared: It specifies that a shared key is used for authentication and data exchanged is encrypted using WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key. 	
Default Key	Specifies the WEP key for the Open or Shared encryption type. 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 the **Subnet Mask** to the same one of the peer CPE, and click **Next**.

Document Version: V2.1

Quick Setup>>Repeater					?
Set the IP address to an unused IP	address belonging to the n	etwork 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

Step 2 Refer to **Step 1** to set the CPE2 to **Repeater** mode.

----End

To check whether the bridging is successful:

- Step 1 Log in to the web UI of CPE2.
- **Step 2** Navigate to **Advanced > Diagnose**.
- **Step 3** Select **Ping** from the **Diagnose** drop-down list.
- **Step 4** Select **Manual** from the **IP Address** drop-down list.
- Step 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)
	Start	

----End

The bridging is successful when the ping succeeds.

Document Version: V2.1

Peer to four peers bridging

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



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: Tenda_1
- Channel Bandwidth: 20 MHz
- Security Mode: None

Document Version: V2.1

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

СРЕ	SSID	MAC Address
CPE1	Tenda_2	C8:3A:35:FE:F6:69
CPE2	Tenda_3	C8:3A:35:35:BA:01
CPE3	Tenda_4	C8:3A:35:FD:8D:A1
CPE4	Tenda_5	C8:3A:35:09:93:51

Configuration procedure

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

- 1. <u>Log in to the web UI</u> of CPE1, and navigate to **Wireless** > **Basic**.
- 2. Modify the **Channel** and **Channel Bandwidth** as required, and click **Save**.

C
hina 🔻
enda_2
nable 🔘 Disable
a/n 🔻
T
nable 💿 Disable
m 26dBm
MHz 🔻
uto 🔻
one 🔻
nable 💿 Disable
(Range: 1 to 128)
Save

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

Document Version: V2.1

Sele	ect a working mode:
•	AP In this mode, the device creates a wireless network based on the current wired network.
0	Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
0 (Jniversal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
ا () wire	WISP In this mode, this device connects to an access point provided by ISP in wireless manner, and provides the eless network.
• F acce	Repeater In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless ess point.
● F wire	22MP In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide eless access point.
⊖ F	Router connect to modem in wired manner, and provide network access point

4. Select the wireless network to bridge from the list, which is **Tenda_1** in this example, and click **Next** at the bottom of the page.



- 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 Setu	p>>Repeater				
Click "Scan", a	and select the wireles xt".	s network you wa	ant to connect,		
	Scan	Scan agai	n		
	Peer AP1				
	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
	Tenda_1			None	line.

5. Click Next.

		Document Version: V2.
Quick Setup>>Repeater		
		2
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those	e of peer AP.
Enter the key of peer AP1, and cli	k "Next".	
Peer AP1	Tenda_1	
MAC Address of Peer AP1		
Channel	T	
Security Mode	Nono	
Security Mode	None .	
		Previous Next

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 of the peer CPE, and click **Next**.

Quick Setup>>Repeater			~
Set the IP address to an unused IP	ddress belonging to the network segm	ent 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	

- Step 2 Refer to <u>Step 1</u> to set CPE2, CPE3 and CPE4 to **Repeater** mode, and bridge to the primary CPE.
- **Step 3** Set the primary CPE to **Repeater** mode and bridge to 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** at the bottom of the page.

Document Version: V2.1

₽

- 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 Setu	ıp>>Repeater				
Click "Scan",	and select the wireles	s network you wa	ant to connect,		
and click "Ne	ext".				
	Scan	Scan agai	in		
	Peer AP1	C8:3A:35:FE:F6	:69		
	Peer AP2	C8:3A:35:35:BA	:01		
	Peer AP3	C8:3A:35:FD:8D):A1		
	Peer AP4	C8:3A:35:09:93:	51		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
	Tenda_2	165	C8:3A:35:FE:F6:69	None	.atl
	Tenda_3	165	C8:3A:35:35:BA:01	None	lin.
	Tenda_4	165	C8:3A:35:FD:8D:A1	None	.atl
	Tenda_5	165	C8:3A:35:09:93:51	None	line.

4. Click Next.

Quick Setup>>Repeater	2
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those of peer AP.
Enter the key of peer AP1, and clic	k "Next".
Peer AP1	Tenda_2
MAC Address of Peer AP1	C8:3A:35:FE:F6:69
Channel	
Security Mode	None •
	Previous

5. Click Next.

Document Version: V2.1

Set the IP addres	s to an unused IP	address belonging to	the network segment of	of 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).

- **Step 1** Log in to the web UI of the primary CPE.
- **Step 2** Navigate to **Advanced** > **Diagnose.**
- **Step 3** Select **Ping** from the **Diagnose** drop-down list.
- **Step 4** Select **Manual** from the **IP Address** drop-down list.
- Step 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)
	Start	

----End

The bridging is successful when the ping succeeds.

Document Version: V2.1

₽TIP

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: V2.1

4.6 P2MP mode

4.6.1 Overview

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

The CPE in P2MP mode can work with the CPE in <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 to four CPEs work in Repeater mode.

The network topology is shown as below.



Document Version: V2.1

₽_{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: Tenda_1
- Channel Bandwidth: 20 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	Tenda_2	C8:3A:35:FE:F6:69
CPE2	Tenda_3	C8:3A:35:35:BA:01
CPE3	Tenda_4	C8:3A:35:FD:8D:A1
CPE4	Tenda_5	C8:3A:35:09:93:51

Configuration procedure

₽TIP

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

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

Document Version: V2.1

Basic		
Enable Wireless		
Country/Region	China •	
SSID	Tenda_2	
Broadcast SSID	enable	
Network Mode	11a/n 🔻	
* Channel	T	
Channel Shift	Enable	
Transmit Power	1dBm 23dBm	
* Channel Bandwidth	20MHz V	
Transmit Rate	Auto 🔻	
Security Mode	None •	

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

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

Document Version: V2.1

 Select the wireless network to bridge from the list, which is Tenda_1 in this example, and click Next at the bottom of the page.

Quick Setup>>Repeater				2
Click "Scan", and select the wireles and click "Next".	s network you wa	int to connect,		
Scan	C Scan agai	n		
Peer AP1				
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
✓ Tenda_1			None	.all

₽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	Tenda_1
MAC Address of Poor AP1	
MAC Address of Feel AFT	
Channel	T
Security Mode	None
Security Mode	
	Previous

Document Version: V2.1

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 of the peer CPE, and click **Next**.

Quick Setup>>Repeater			
Set the IP address to an unused IP	address belonging to the ne	etwork 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 P2MP, click "Save" to apply the settings.			
	Previous	Save	
		_	

- Step 2 Refer to <u>Step 1</u> to set the CPE2, CPE3 and CPE4 to Repeater mode, and bridge to the primary CPE.
- Step 3 Set the primary CPE to **P2MP** mode and bridge to 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**.
 - Select the SSIDs of CPE1, CPE2, CPE3 and CPE4, which are Tenda_2, Tenda_3, Tenda_4 and Tenda_5 in this example, and click Next.

Quick Set	up>>P2MP				
Click "Scan"	, and select the wirele	s network you w	ant to connect,		1
and click "N	lext".				
	Scan	Scan aga	in		
	Peer AP1	C8:3A:35:FE:F6	:69		
	Peer AP2	C8:3A:35:35:BA	:01		
	Peer AP3	C8:3A:35:FD:8D	:A1		
	Peer AP4	C8:3A:35:09:93:	51		
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
	Tenda_2		C8:3A:35:FE:F6:69	None	lite.
	Tenda_3		C8:3A:35:35:BA:01	None	
	Tenda_4		C8:3A:35:FD:8D:A1	None	llee.
st.	Tenda_5		C8:3A:35:09:93:51	None	lin.

Document Version: V2.1

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	ck "Next".		
Peer AP1	Tenda_2		
MAC Address of Peer AP1	C8:3A:35:FE:F6:69		
Channel	T		
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.
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.

5. Click Next.

Quick Setup>>P2MP					2
Set the IP address to an unused IP	address belonging to the n	etwork segment of peer AP.			
IP Address	192.168.2.1				
Subnet Mask	255.255.255.0				
			Previous	Next	

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

Document Version: V2.1

The device is set to P2	MP, click "Save	' to apply the sett	ings.		
	,				
				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).

- **Step 4** Log in to the web UI of the primary CPE.
- **Step 5** Navigate to **Advanced > Diagnose.**
- **Step 6** Select **Ping** from the **Diagnose** drop-down list.
- **Step 7** Select **Manual** from the **IP Address** drop-down list.
- Step 8 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)
	Start	

E 10	
 ЕП	
	_

The bridging is successful when the ping succeeds.

Document Version: V2.1

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.

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

Quick Setup	
Select a working r	node:
○ AP In this mod	e, the device creates a wireless network based on the current wired network.
Client In this n	node, the device works as a wireless adapter to connect to the wireless network of upstream AP.
🔵 Universal Repe	ater In this mode, this device extends an existing wireless network for broader network coverage.
• WISP In this m wireless network.	ode, this device connects to an access point provided by ISP in wireless manner, and provides the
Repeater In th access point.	is mode, the device connects to multiple wired networks through wireless bridge, and provides wireless
• P2MP In this n wireless access poir	rode, the device connects to multiple wired networks through wireless bridge, but does not provide nt.
Doutor composition	t to modem in wired manner, and provide network access point

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

Document Version: V2.1

1. Select **PPPoE**.

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

Quick Setup>>Router				?
Please select an internet connecti and click "Next".	on type, and enter the int	ternet parameters provid	ded by your ISP.	
Internet Connection Type	OHCP (Dynamic IP)	Static IP Address	PPPoE	
PPPoE User Name				
PPPoE Password				
			Previous	s Next

Parameters description

Refer to the followi - DHCP (Dy from the followi Internet Connection Type - Static IP A subnet ma ISP. - PPPoE: The password	ng instructions to select the appropriate internet connection types: namic IP) : The device obtains the IP address and other parameters DHCP server of upstream device for internet access. Address : The device accesses the internet using the IP address, ask, default gateway and DNS server IP addresses provided by your he device accesses the internet using the PPPoE user name and provided by the ISP.

- **Step 4** Set wireless parameters of the CPE, and click **Next**.
 - 1. Customize an SSID, which is **Tenda_123456** in this example.
 - 2. 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.

Document Version: V2.1

Quick Setup>>Router	
You can set up your wireless netwo	ork name and wireless password here.
Note down your wireless password	
SSID	Tenda_123456
Channel	T
Security Mode	WPA2-PSK T
Encryption Algorithm	● AES
Key	
	Previous

Parameters description

Name	Description
SSID	Specifies the WiFi name of the CPE.
Channel	Specifies the channel that the wireless network operates. Auto indicates that the device automatically adjusts its operating channel according to the ambient environment.
Security Mode	Specifies the security mode of the wireless network of the device. It includes <u>None</u> , <u>WPA-PSK</u> , <u>WPA2-PSK</u> , and <u>Mixed WPA/WPA2-PSK</u> .
Encryption Algorithn	 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.
Step 5 Click Save,	and wait until the device reboots to make the settings take effect.
Quick Setup	>>Router

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

----End

Document Version: V2.1

After the CPE is rebooted, <u>log in to the web UI</u> of the CPE and navigate to **Status**. If the WAN IP address, default gateway and DNS server information obtained by the WAN port are displayed on the **System Status** module, the configuration is successful.

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 <u>Step 4</u>.

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



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

₽_{TIP}

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

- **Step 1** Log in to the web UI of the router.
- **Step 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.

Document Version: V2.1

 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.

Document Version: V2.1



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

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. O8V1.0 is used for illustration.

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

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

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

₽TIP

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

Document Version: V2.1

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

Parameters description

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: V2.:	n: V2.1
------------------------	---------

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: V2.1

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.

Operating RF Status	5		
Working Mode	AP	AP's MAC Address	
SSID	Tenda_123456	Signal Strength	-57dBm
Security Mode	None	Background Noise	-95dBm
Channel/Radio Band		TX/RX Link	2X2
Channel Bandwidth	40MHz	Transmit/Receive Speed	72Mbps/292Mbps
TX Power	27dBm	TD-MAX	Disabled
Wireless Client	0	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.
Wireless Client	Specifies the number of wireless clients connected to the wireless network of the CPE's operating RF.

Document Version: V2.1

Name	Description
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.
AT 5 WINC Address	 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.
	Specifies the wireless signal strength of the peer device.
Signal Strength	 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.
	Specifies the wireless transmitting/receiving rate.
Transmit/Receive Speed	 In AP or Router mode, it displays the transmitting/receiving rate of the first device connected to the wireless network of this device.
	 In Client, Universal Repeater, WISP, Repeater, or P2MP mode, it displays transmitting/receiving rate of this device.
TD-MAX	Specifies the status of the TD-MAX function. For details, refer to <u>TD-MAX</u> .
Distance	Specifies the distance between the two CPEs after the bridging succeeds.
Distance	If there are more than two CPEs, it specifies the bridging distance between this CPE and the farthest CPE.

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	Enable	Enabled upon Power on	Enable
SSID	Tenda_03CB80_MG	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 duration</u> of management RF's wireless network, the management RF will be automatically disabled after the auto-start duration is exceeded.

Document Version: V2.1

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.



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.



Document Version: V2.1

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.

tatistics						
Throughput	Wireless Client	Interface		ARP Ta	ble	Routing Table
IP Address	MAC Address	Signal/Noise	Transm	it/Receive	CCQ	Connection Duration
192.168.1.15		-37/-104dBm	120/	351Mbps	100%	7 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: V2.1

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.

Throughput	Upstream AP	Interfa	ce	ARP Ta	ble	Routing Table
IP Address	MAC Address	Signal/Noise	Transm	it/Receive	CCQ	Connection Duration
N/A		-56/-103dBm	292/3	25Mbps	97%	19 m13 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: V2.1

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.

Statistics						
Throu	ighput	Wireless Client	Interface	ARI	P Table	Routing Table
Interface	IP Address	MAC Address	Received Packets	Receive Error	Transmitted Pa	ckets Transmit Error
LAN	0.0.0.0		22776	0	7750	0
Bridge	192.168.2.1		22678	0	5134	0
WLAN	0.0.0.0		175	0	60341	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	Creative the number of reastived (transmitted nearly to 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: V2.1

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.

Statistics							
Throughput Wireless Client		Interface	ARP Table	Routing Table			
IP Address		MAC Add	ress	Interface			
192.168.2.170				Bridge			
192.168.	2.130			Bridge			
192.168.	2.125			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: V2.1

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	Upstream AP	Interface	ARP Table	Routing Table
Destination Network		Subnet Mask	Next Hop	Interface
0.0.0.0		0.0.0.0	192.168.0.1	WLAN
192.168.0.0		255.255.255.0	0.0.0.0	WLAN
192.168	.2.0	255.255.255.0	0.0.0.0	Bridge
239.255.255.250		255.255.255.255	0.0.0.0	Bridge

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: V2.1



6.1 LAN setup

6.1.1 Overview

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

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

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

N Setup	
MAC Address	
IP Address Type	Static IP Address
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Device Name	O4V1.0
	Save Cancel

Name	Description
MAC Address	Specifies the MAC address of LAN port. By default, the SSID of the CPE is Tenda_ <i>XXXXXX</i> , and <i>XXXXXX</i> is the last six characters of the MAC address.

Document Version: V2.1

Name	Description
IP Address Type	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.
	 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.
	¥ TIP
	If the IP Address Type is set to DHCP (Dynamic IP Address) , you need to check the device's IP address on the clients list of the DHCP server in the network, and use this IP address to log in to the web UI of the device.
ID Addross	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.
IP Address	To access the internet, change this IP address to the same network segment of the LAN IP address of the egress router.
Subnet Mask	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 agency function, it can be set to the LAN IP address of the egress router. Otherwise, specify a DNS server IP address manually.
	If there is only one DNS server IP address, enter it in this box.
Secondary DNC Server	Specifies the secondary DNS server IP address of the device.
Secondary DNS Server	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: V2.1

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

LAN Setup	
MAC Address	
mile riddress	
IP Address Type	Static IP Address
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
	Save Cancel

Name	Description
MAC Address	Specifies the MAC address of LAN port. By default, the SSID of the CPE is Tenda_ <i>XXXXXX</i> , and <i>XXXXXX</i> is the last six characters of the MAC address.
IP Address Type	 Specifies the type of obtaining an IP address. The default is Static IP Address. Static IP Address: Specify the IP address and subnet mask manually. DHCP (Dynamic IP Address): The device obtains an IP address and subnet mask from the upstream DHCP server in the network. If the IP Address Type is set to DHCP (Dynamic IP Address), you need to check the device's IP address on the clients list of the DHCP server of the upstream device, and use this IP address to log in to the web UI of the device.
IP Address	Specifies the LAN IP address of the device. A LAN user can visit this address to log in to the web UI of the device.
Subnet Mask	Specifies the subnet mask corresponding to the LAN IP address of the device. The default is 255.255.255.0 .

Document Version: V2.1

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

- **Step 1** Log in to the web UI of the CPE.
- **Step 2** Navigate to **Network > LAN Setup**.
- **Step 3** Set **IP Address Type** to **Static IP Address**.
- **Step 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**.
- Step 5 Click Save.

Static IP Address
192.168.2.100
255.255.255.0
0.0.0.0
0.0.0.0
0.0.0.0
O4V1.0
Save Cancel

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

Note		×
Please click Of After IP addre	K to confirm to change IP address. ss changed, please login with new II	P address 192.168.2.100

----End

Document Version: V2.1

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

Otherwise, assign your computer an IP address that belongs to the same network segment as the new IP address of the CPE before login with the new IP address. Refer to <u>How to assign a fixed IP</u> <u>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

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

LAN Setup	
MAC Address	
¥ IP Address Type	DHCP (Dynamic IP Add V
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Device Name	O4V1.0
	Save

----End

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

Document Version: V2.1

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

6.2 Packet filter

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

To access the 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 parameters related to the packet filtering function of the wired Ethernet port. The CPE kit O1 is taken as an example.

Packet Filte	r						
Wired port net	work packet filtering	🖌 Enable					
Filter Rule I packet fil	ndicates the tering mode	○ Enable	Disable				
Adding a filte	ering policy						
ID	Filter ru	le	Rule details	Regular switch state	Filter mode	Operation	
1	VLAN&A	ARP	VLAN ID 555 ARP packet	Enable	Prohibit	Delete Edit	
			Save	el			

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.

Document Version: V2.1

Name	Description
Filter rule	 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. 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 including Enable and Disable .
Filter mode	Specifies whether to filter the packets including Permit and Prohibit .
Operation	 Used to edit or delete the packet filter policy. Edit: Used to edit the packet filter policy. Delete: Used to delete the packet filter policy.
Source MAC	Specifies the data frames from this MAC address will be filtered.
Destination MAC	Specifies the data frames with this MAC address as the destination address will be filtered.
Source IP	Specifies the packets from this IP address will be filtered.
Destination IP	Specifies the packets with this IP address as the destination 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: V2.1

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 configuring the internet settings, your ISP may have bound your internet service account with the MAC address of your computer that was used to verify the internet connectivity after you subscribed to the internet service.

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

6.3.2 Clone a MAC address

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

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

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

MAC Clone		
	MAC Address	
	Clone Local MAC Address Restore to Default MAC Address	
	1	_

----End

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

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

- **Step 1** Log in to the web UI of the CPE, and navigate to **Network > MAC Clone.**
- Step 2 Enter the MAC address of the computer in the MAC Address.
- Step 3 Click Save.

Document Version: V2.1

MAC Clone				(?
	MAC Address			_
	Clone Local MAC	Address	Restore to Default MAC Address	

----End



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

Document Version: V2.1

6.4 DHCP server

6.4.1 Overview

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

₽_{TIP}

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

6.4.2 Configure the DHCP server

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

Step 5 Click Save.

DHCP Server	2
* DHCP Server	
Start IP Address	192.168.2.100
End IP Address	192.168.2.200
Subnet Mask	255.255.255.0
\star Gateway Address	192.168.2.254
* Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4
Lease Time	1 day 🔹
	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.

Document Version: V2.1

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	₽ _{TIP}
	The start and end IP addresses must belong to the same network segment as the IP address of the LAN port of the CPE.
Subnet Mask	Specifies the subnet mask assigned by the DHCP server to clients. The default value is 255.255.25.0 .
Gateway Address	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 .
	Q _{TIP}
	A client can access a server or host not in the local network segment 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	Q _{TIP}
	To enable clients to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server	Specifies the secondary DNS server IP address assigned by the DHCP server to clients. This parameter is optional.
	Specifies the validity period of an IP address assigned by the DHCP server to a client.
	When the IP address expires:
Lease Time	 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 (power off, wireless network disconnected, and so on) to the CPE, the CPE will release the IP address. If other clients request IP address information in the future, 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**.

ID	Host Name	IP Address	MAC Address	Lease Time
1	iPhone	192.168.2.133		23h 59m 44s

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 of an IP address assigned by the DHCP server to a client.

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, packet with tag will be forwarded to the ports of the corresponding VLAN according to the VID of the packet, and packet without tag will be forwarded to the ports of the corresponding VLAN according to the PVID of the port.

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

Type of the Port	Type of Rece	Transmitted Deducts	
	Packet with Tag	Packet without Tag	
Access	For word the data to the		Strip the tag in the packet and then forward it
Forward the da ports of the cor VLAN based on Truck the tag.	Porward the data to the ports of the corresponding VLAN based on the VID in the tag.	ports of the corresponding VLAN based on the PVID of ports	VID = Port PVID, strip the tag in the packet and then forward it
			VID ≠ port PVID, retain the tag in the packet and then forward it

6.6.2 Configure VLAN (Example: OS3)

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		2
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)
	Save	cel

Document Version: V2.1

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.	
	Specifies the ID of the management VLAN of this CPE. The default ID is 1.	
Management VLAN	After changing the management VLAN, you can manage this CPE only after connecting your computer to the new management VLAN.	
	Used to set a VLAN ID for the wireless network of the CPE. By default, it is set to 1000 .	
WLAN VLAN ID	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 VII AN ID of the Ethernat part of the CDE. By default, it is set to 1	
LAN3	After the VLAN function is enabled, the Ethernet port is equivalent to an access port.	
I AN4	whose PVID is the same as VLAN ID.	

6.6.3 Example of configuring VLAN (Example: O4)

Networking requirements

Two communities deploy the network with the CPE and connect to the internet through the same router. Now, the internet access of the two communities is required to not interfere with each other.

Solution

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

Document Version: V2.1

Network topology



The connections of the switch:

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

Configuration procedure

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

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

Document Version: V2.1

5. Confirm the prompt information, click **OK**, and wait until the CPE1 completes reboot.

Step 2 Set the **WLAN VLAN ID** of CPE2 to **20** according to the steps in <u>Step 1</u>.

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

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

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

Step 4 Set up the router.

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

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

Refer to the user guide of the router for details.

----End

Verification

If the router enables two DHCP servers for VLAN10 and VLAN20 respectively, the 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 these parameters from the DHCP sever belonging to VLAN20.

Document Version: V2.1

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-related parameters, network mode, channel, transmitted power and so on.

Broadcast SSID

After the broadcast SSID function is enabled, the nearby wireless clients can detect the SSID. After the SSID broadcast 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 corresponding to the SSID. This to some extent enhances the security of the wireless network.

After the SSID broadcast function is disabled, if hackers use other means to obtain the SSID, the target network still can be accessed.

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 connected by the CPE can be accessed. It is suitable for the establishment of public hotspots such as hotels and airports, so that the wireless clients connected 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 corresponding to 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.

Document Version: V2.1

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

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

None

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

WEP

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

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

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

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

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

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

WPA and WPA2

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

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

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

Document Version: V2.1

In AP, WISP, Repeater, P2MP and Router modes

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

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

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

Basic	Curren	t Mode: AP
Enable Wireless		?
Country/Region	China 🗸	
SSID	Tenda_F8CD00	
Transparent WDS	⊖ Enable ● Disable	
Broadcast SSID	● Enable ○ Disable	
Network Mode	11ac 🗸	
Channel Bandwidth	Auto 🗸	
Channel	161(5805MHz) ~	
Channel Shift	⊖ Enable	
DFS Function	⊖ Enable	
Transmit Power	1dBm 25dBm	
Transmit Rate	Auto 🗸	
Security Mode	None 🗸	
Isolate Client	⊖ Enable	
Max. Number of Clients	48 (Range: 1 to 128)	
	Save Cancel	

Document Version: V2.1

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 China .
SSID	Specifies the name of the wireless network (SSID). 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. \bigcirc_{TIP} Transparent WDS and <u>Transparent Bridge</u> cannot be enabled at the same time.
Broadcast SSID	 Specifies whether to broadcast the SSID. Enable: The device can broadcast an SSID, and wireless clients can detect the SSID. Disable: The device does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This to some extent enhances the security of the wireless network.
Network Mode	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: V2.1

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: Comparison of 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, WPA2-PSK, Mixed WPA/WPA2-PSK</u> , <u>WPA, and WPA2</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 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: V2.1

In Client and Universal Repeater modes

Basic		Current Mode: Station
Enable Wireless		2
Country/Region	China 🗸	
Broadcast SSID	Enable Disable	
Network Mode	11ac 🗸	
Channel Bandwidth	Auto	
Channel	161(5805MHz) V	
Channel Shift	○ Enable	
DFS Function	○ Enable	
Transmit Power		
	1dBm 25dBm	
Transmit Rate	Auto	
Primary Upstream SSID	NOVA_9JK3_AAAAA Site Survey	
Primary AP BSSID	50:2B:73:F8:F9:8A	
Transparent WDS	⊖ Enable ● Disable	
Security Mode	WPA2-PSK V	
Encryption Algorithm	● AES O TKIP O TKIP&AES	
Key		
Key Update Interval	0 s (Range: 60 to 99999)	
Secondary Upstream SSID	○ Enable ● Disable	
Secondary Upstream SSID	Tenda Site Survey	
Secondary Upstream BSSID	00:90:4C:88:88:88	
Transparent WDS	🔿 Enable 💿 Disable	
Security Mode	None 🗸	
Reconnect Primary Upstream	○ Enable	
SSID		
Reconnection Interval	90 (Range: 1~720minutes)	
Isolate Client	⊖ Enable	
Max. Number of Clients	48 (Range: 1 to 128)	
	Save	

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

Document Version: V2.1

Parameters on the **Basic** page vary with different modes. Refer to the actual web UI. Followings are descriptions of some main parameters. For other parameters, refer to <u>Parameter description</u> of AP mode.

Name	Description
Primary Upstream SSID	Specifies the SSID of the primary upstream wireless network that the CPE connects to. After bridging succeeds, the SSID of the primary upstream wireless network will automatically populate.
Primary AP BSSID	Specifies the MAC address of the primary upstream wireless network. After bridging succeeds, the MAC address of the primary upstream wireless network will automatically populate.
Lock	Used to lock the upstream wireless network. With this function enabled, the CPE can only connect to the wireless network with the current MAC address, and cannot connect to other upstream APs with the same WiFi name.
Secondary Upstream SSID	Specifies the SSID of the secondary upstream wireless network that the CPE connects to. With this function enabled, if the CPE fails to connect to the primary upstream SSID, it will automatically connect to the secondary upstream SSID.
Secondary Upstream BSSID	Specifies the wireless MAC address of the secondary upstream wireless network.
Reconnect Primary Upstream SSID	Used to reconnect to the primary upstream wireless network. With this function enabled, after connecting the secondary upstream SSID, the CPE tries to reconnect to the primary upstream SSID at intervals of the reconnection interval that you configure.
Reconnection Interval	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: V2.1

7.1.2 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

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

Document Version: V2.1

Basic	
Enable Wireless	
Country/Region	China •
*SSID	FREE
Broadcast SSID	Enable Disable
Network Mode	11a/n 🔻
Channel	T
Channel Shift	Enable Isable
Transmit Power	1dBm 23dBm
Channel Bandwidth	20MHz 🔻
Transmit Rate	Auto •
★ Security Mode	None •
Isolate Client	Enable Isable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

----End

Verification

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

Document Version: V2.1

7.1.3 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

- **Step 1** Log in to the web UI of the CPE.
- **Step 2** Navigate to **Wireless** > **Basic**.
- **Step 3** Set **SSID** to **Factory**.
- **Step 4** Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.
- Step 5 Set Key to UmXmL9UK.
- Step 6 Click Save.
| Document | Versie | $n \cdot \sqrt{21}$ |
|----------|--------|---------------------|
| Document | VEISIU | II. VZ.I |

Basic	2
Enable Wireless	
Country/Region	China •
* SSID	Factory
Broadcast SSID	Enable Obisable
Network Mode	11a/n •
Channel	T
Channel Shift	 Enable Disable
Transmit Power	1dBm 23dBm
Channel Bandwidth	20MHz •
Transmit Rate	Auto •
* Security Mode	WPA2-PSK
* Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
\star Key	
Key Update Interval	0 s (Range: 60 to 99999)
Isolate Client	Enable Isable
Max. Number of Clients	48 (Range: 1 to 128)
	Save



Verification

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

Document Version: V2.1

7.1.4 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
- **Step 1** Log in to the web UI of the CPE, and navigate to **Wireless** > **Basic**.
- **Step 2** Set **SSID** to **hot_spot**.
- **Step 3** Set **Security Mode** to **WPA2**.
- Step 4 Set RADIUS Server, RADIUS Port, and RADIUS Password to 192.168.0.200, 1812, and UmXmL9UK respectively.

Document Version: V2.1

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

Step 6 Click Save.

Basic	
Enable Wireless	?
Country/Region	China 🔹
* SSID	hot_spot
Broadcast SSID	Enable Disable
Network Mode	11a/n •
Channel	Auto •
Channel Shift	Enable Isable
Transmit Power	1dBm 26dBm
Channel Bandwidth	20MHz •
Transmit Rate	Auto •
* Security Mode	WPA2 •
* RADIUS Server	192.168.2.200
* RADIUS Port	1812
* Encryption Algorithm	● AES
* RADIUS Password	>
Key Update Interval	0 s (Range: 60 to 99999)
Isolate Client	Enable Isable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

----End

Configure the RADIUS server

₽TIP

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

Step 1 Configure a RADIUS client.

Document Version: V2.1

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

💖 Internet Authenti	cation Service			
<u>F</u> ile <u>A</u> ction <u>V</u> iew	<u>H</u> elp			
← → 主 🖬 1	🔋 🕼 🗟 😫			
🐤 Internet Authenticati	ion Service (Local)	Frien	dly Name	Address
RADIUS Clients Remote Access Remote Access Connection Rec Connection Rec Remote RA	New RADIUS <u>C</u> i <u>N</u> ew <u>V</u> iew Refresh Export List	ent	There are no iten	ns to show in this view.
	<u>H</u> elp			
				F
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 nar	me for the client.
Eriendly name:	root	
Client address (IP or DNS)):	
192.168.2.1		⊻erify
 IP address of the C	PE	

Document Version: V2.1

3. Enter UmXmL9UK in the Shared secret and Confirm shared secret text boxes, and click Finish.

	RADIUS Client
	Additional Information
e client vendor attribute, specify the	f you are using remote access polic vendor of the RADIUS client.
	<u>Client-Vendor</u>
•	RADIUS Standard
	Shared secret:
	Confirm shared secret:
sator attribute	<u>R</u> equest must contain the Me
assword same as that specified	
y RADIUS Password on the CPE.	
< Back Finish Cancel	
y RADIUS Password on the CPE.	

- **Step 2** Configure a remote access policy.
 - 1. 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 S	ervice		_ 🗆 ×
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp			
⇔ → 🗈 💽 🕃 🕞	ß		
Internet Authentication Servic	e (Local)	Name	Order
- ADIUS Clients		S Connections to Microsoft Routing and Remote A	1
Remote Access Logging		Connections to other access servers	2
Connection Request P	New Remote Access Po	licy	
	New	•	
	⊻iew	•	
	Refresh Export <u>L</u> ist		
	<u>H</u> elp		
New Remote Access Policy		, 	

Û

Document Version: V2.1

Internet Authentication Service File Action New Remote Access Policy V	Vizard X
Conne	Welcome to the New Remote Access Policy Wizard
Stat	Cancel

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?
Use the wizard to set up a typical policy for a common scenario
○ <u>S</u> et 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: V2.1

3. Select Ethernet and click Next.

	Netheral O
Pol	icy conditions are based on the method used to gain access to the network.
Selec	t the method of access for which you want to create a policy.
C	<u>V</u> 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.
С	Dial-up
	Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
C	<u>W</u> ireless
	Use for wireless LAN connections only.
Ģ	Ethernet
	Use for Ethernet connections, such as connections that use a switch.
- 1	
	< <u>B</u> ack <u>N</u> ext> Cancel

4. Select Group and click Add.

New Remote Access Policy Wizard
User or Group Access You can grant access to individual users, or you can grant access to selected groups.
Grant access based on the following: User User access permissions are specified in the user account. Group Individual user permissions override group permissions. Group name: Add <u>Remove</u>
< <u>B</u> ack <u>N</u> ext > Cancel

Document Version: V2.1

5. Enter 802.1x in the Enter the object names to select text box, 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.

authenticate users.	Ċ
	Configure
< <u>Back</u> <u>N</u> ext	> Cancel
	< <u>■</u> × × ×

Document Version: V2.1



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

root Properties
Settings
Specify the conditions that connection requests must match. Policy conditions: INAS-Port-Type matches "Ethernet" AND Windows-Groups matches "COMBA\802.1x"
Add <u>E</u> dit <u>R</u> emove If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection. Edit <u>P</u> rofile
Unless individual access permissions are specified in the user profile, this policy controls access to the network.
If a connection request matches the specified conditions: © De <u>n</u> y remote access permission
Grant remote access permission
OK Cancel Apply

Document Version: V2.1

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.

Dial-in Profile		?
Dial-in Constraints	IP	Multilink
Authentication	Encryption	Advanced
Select the authentication m	ethods you want to allow	for this connection.
Microsoft Encrypted A	Authentication version <u>2</u> (ge password after it has i	MS-CHAP v2) expired
Microsoft Encrypted A	Authentication (MS-CHAF	?)
🔲 U <u>s</u> er can chan	ge password after it has i	expired
Encrypted authentica	ition (CHAP)	
☑ Unencrypted authent	ication (PAP, SPAP)	
Unauthenticated access		
Allow clients to conne method.	ect without negotiating ar	n authentication
	OK Ca	ancel <u>Apply</u>

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

----End

Configure your wireless device

₽_{TIP}

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

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

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



Document Version: V2.1

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

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

6	الله Manually connect to a v	vireless network	
	Enter information for	the wireless network you w	ant to add
	Network name:	hot_spot	
	Security type:	WPA2-Enterprise 👻	Same as the security
	Encryption type:	AES 🔹	mode of the SSID of the
	Security Key:		UPE Hide characters
	✓ Start this connection ✓ Connect even if the r Warning: If you select	automatically ietwork is not broadcasting t this option, your computer's privac	y might be at risk.
			Next Cancel

Document Version: V2.1

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

 \square

💮 💷 Ma	nually connect to a wi	reless network			
Succe	ssfully added hot	t_spot			
	Change connection Open the connection	tion settings n properties so that I i	can change the settings.		
					Close
hot_spot	Wireless Netwo	ork Properties			
Secur	ity type:	WPA2-Enterpris	ie	•	
Choo: Micro Re tir	se a network aut psoft: Protected f emember my crea ne I'm logged on	hentication meth EAP (PEAP) lentials for this c	od: Settings onnection each	;	
			ок	Cancel	

Document Version: V2.1

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

Protected EAP Properties
When connecting: Validate server certificate Connect to these servers:
Trusted Root Certification Authorities:
 Baltimore CyberTrust Root Class 3 Public Primary Certification Authority GlobalSign Root CA Microsoft Root Authority Microsoft Root Certificate Authority 2011 Thawte Timestamping CA Image: Compt user to authorize new servers or trusted certification authorities.
Select Authentication Method: Secured password (EAP-MSCHAP v2) Configure Finable East Reconnect Disconnect if server does not present cryptobinding TLV Enable Identity Privacy OK Cancel

仑

EAP MSCHAPv2 Properties	
When connecting	
when connecting.	
Automatically use my Windows logon name and password (and domain if any).	
OK Cancel	

Document Version: V2.1

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

hot spot Wireless Network Properties	ĸ
Connection Security	
	٦
Security type: WPA2-Enterprise	
Encryption type:	
Choose a network authentication method:	
Microsoft: Protected EAP (PEAP)	
Remember my credentials for this connection each time I'm logged on	
Advanced settings	
OK Cancel	
↓	
(
Advanced settings	3
802.1X settings 802.11 settings	_
Specify authentication mode:	
User or computer authentication 🔻 Save credentials	
Delete credentials for all users	
Enable single sign on for this network	
Perform immediately before user logon Perform immediately after user logon	
Maximum delay (seconds):	

802.1X settings 802.11 settings
Specify authentication mode:
User or computer authentication
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds): 10
✓ Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK Cancel

Document Version: V2.1

Step 7 Click Close.

0 items

-111

(Manually connect to a	wireless network		
Successfully added h	iot_spot		
Change connect Open the connect	ection settings tion properties so that I can change the setti	ings.	
		Close	
	Ŷ		
	CC	- fa Search Manage Wirelest Network	
😋 🔍 🛛 🕨 Control Panel 🕨 N	Ietwork and Internet Manage Wireless Networks	▼ 49 Search Manage Wireless Network	in (
	Ietwork and Internet Manage Wireless Networks that use (Wireless Network Connection networks in the order listed below.	Search Manage Wireless Network n)	e (
← ← Manage wireless networks Windows tries to connect to these Add Adapter properties Profile to	Ietwork and Internet Manage Wireless Networks that use (Wireless Network Connection networks in the order listed below. Hypes Network and Sharing Center		is (
♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥	Ietwork and Internet Manage Wireless Networks that use (Wireless Network Connection networks in the order listed below. ypes Network and Sharing Center order (1)	v ↔ Search Manage Wireless Network	n (
▼ Image wireless networks Manage wireless networks Windows tries to connect to these Add Adapter properties Profile ty Networks you can view, modify, and ree Image wireless hot_spot	Letwork and Internet Manage Wireless Networks that use (Wireless Network Connection networks in the order listed below. ypes Network and Sharing Center order (1) Security: WEP	n) Type: Any supported	• •
♥ Image wireless networks Windows tries to connect to these Add Adapter properties Profile ty Networks you can view, modify, and rest hot_spot	Letwork and Internet Manage Wireless Networks that use (Wireless Network Connection networks in the order listed below. ypes Network and Sharing Center order (1) Security: WEP	n) Type: Any supported	e (
▼ Iff ► Control Panel ► N Manage wireless networks Windows tries to connect to these Add Adapter properties Profile ty Networks you can view, modify, and rest hot_spot	Letwork and Internet Manage Wireless Networks that use (Wireless Network Connection networks in the order listed below. ypes Network and Sharing Center order (1) Security: WEP	n) Type: Any supported	25
▼ all ► Control Panel ► N Manage wireless networks Windows tries to connect to these Add Adapter properties Profile to Networks you can view, modify, and real hot_spot	Letwork and Internet Manage Wireless Networks that use (Wireless Network Connection networks in the order listed below. ypes Network and Sharing Center order (1) Security: WEP	n) Type: Any supported	ta la
Image wireless networks Windows tries to connect to these Add Adapter properties Profile ty Networks you can view, modify, and rest Image wireless Not_spot	Letwork and Internet Manage Wireless Networks that use (Wireless Network Connection networks in the order listed below. ypes Network and Sharing Center order (1) Security: WEP	n) Type: Any supported	n (

Document Version: V2.1

Step 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	* III
Wireless Network Connection	^	
hot_spot	الد	
Connect automatically	<u>C</u> onnect	
		•
Open Network and Sharing Cer	nter	_

Step 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 Cancel

----End

Verification

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

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	Oisable
Preamble	⊖ Short Preamble	Long Preamble
Transparent Bridge	Enable	○ Disable
TD-MAX	⊖ Enable	Disable
Signal Transmission	 Coverage-oriented 	○ Capacity-oriented
TPC	Enable	○ Disable
Signal Reception Level	Auto	
Transmission Distance	5	Auto km (Range: 0.1 to 20, 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

Parameters description

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

Name	Description		
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.		
	Specifies the minimum strength of received signals acceptable to this device.		
Minimum RSSI Threshold	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.		
	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.		
Preamble	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.		
	The Transparent Bridge function enables the WIAN 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.		
Transparent Bridge	Q _{TIP}		
	 This function is only applicable when the CPE works in AP, Client or Universal Repeater mode. 		
	- <u>Transparent WDS</u> and Transparent Bridge cannot be enabled at the same time.		

Name	Description		
	TD-MAX is Tenda's proprietary Time Division Multiple Access (TDMA) polling technology. It allows multiple clients to share the same channel for accessing to a network. With the TD-MAX enabled, the CPE assigns time slots to each client, and transmits data according to the assigned time slots, achieving Point-to-MultiPoint (P2MP) connections.		
	After the TD-MAX 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. 		
TD-MAX	- 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 TD-MAX. 		
	If TD-MAX is enabled, the device operates in TD-MAX mode and only accepts connections from TD-MAX devices. And you cannot connect standard 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. 		
TRO	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.		
IPC	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	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: V2.1

Name	Description
Beacon Interval	Specifies the interval at which this device sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.
Fragment Threshold	 Specifies the threshold of a fragment. The unit is byte. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold. If the transmission fails, this device resends only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of fragments, so as to increase the frame throughput.
RTS Threshold	Specifies the frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	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: V2.1

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.

Access C	Control			
	SSID	Tenda_123456		?
	Access Control			
	Mode	● Disallow ○ Allow		
	MAC Address	12:12:12:12:12:12	Add Add online devices	
SN	MAC Addres	ss Status	Operation	
1	12:12:12:12:12	2:12 Enable	ī	
Acc	ess Control List	Save		

Parameters description

Name	Description
SSID	Specifies the SSID of this device. With the rule enabled, clients connected to the network with this SSID will be controlled by the rule.
Access Control	Specifies whether to enable the Access Control function.
	Specifies the mode for filtering MAC addresses.
Mode	 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: V2.1

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 WiFienabled 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

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

₽_{TIP}

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

- Step 6 Refer to Step 5 to add the other two MAC addresses.
- Step 7 Click Save.

Document Version: V2.1

Access (Control		
	SSID Ten	da_123456	
	\star Access Control	C	
	★ Mode 🔾 🛛	Disallow 💿 Allow	
	*MAC Address	8:3A:35:00:00:03	Add Add online devices
SN	MAC Address	Status	Operation
1	C8:3A:35:00:00:01	Enable	Ŵ
2	C8:3A:35:00:00:02	Enable	Ŵ
3	C8:3A:35:00:00:03	Enable	ŵ
		Save	

----End

Verification

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

Document Version: V2.1

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		
Management RF		?
Enabled upon Power on		
Duration	10	mins
SSID	Tenda_123456_MG	
Network Mode	11b/g/n 🗸	
Channel	Auto 🗸	
Encryption	None 🗸	
	Save	cel

Parameters description

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.
Duration	Specifies the duration of the management RF enabled.

Name	Description
	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.
	ਊ ⊤IP
	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 UI of the CPE, you can delay the available time for the wireless network of the management RF as required.

Configuration procedure

- Step 1 Connect the wireless client to the wireless network of management RF.
- Step 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.
- **Step 3** Click **Delay** in the upper right corner of the page. The following figure is for reference only.

Document Version: V2.1

Tenda	Left until the page closed:6m 10s Delay Logout
♣ Status	Quick Setup Current Mode: AP
Quick Setup	Select a working mode:
Network	 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.
< Wireless	O Universal Repeater In this mode, this device extends an existing wireless network for broader network coverage.
X Advanced	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.
	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

----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: V2.1



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**. OS3 is used for illustration.

Auto Negotiation 🔻
Auto Negotiation 🔻
Auto Negotiation 🔻
Auto Negotiation 🔻
Save Cancel

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

Parameters description

Name	Description
Auto Negotiation	Specifies the speed and duplex mode of the port is determined by the negotiation between the port of the CPE and the port of the peer device.
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 at the same time.

Document Version: V2.1

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 at the same time.

₽TIP

- 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 10 Mbps full duplex or **Auto Negotiation**.

Document Version: V2.1

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 less interference channel (used by few devices) for the wireless network of the CPE to improve the transmission efficiency.

Configuration procedure

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

----End

agnos	e				
	Diagnose	Site Survey	•		
ID	SSID	MAC Address	Channel	Security	Signal Strength
1	Tenda_6A1672		48	WPA2-PSK,AES	line
2	Tenda_859D21		40	WPA2-PSK,AES	liter
3	Tenda_34E625		48	Mixed WPA/WPA2-PSK	liter.

Document Version: V2.1

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

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

Step 8 Click Start.

ignose		
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)
	Start	

----End

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 receive	ed, 25.00% loss25.00%
Min. 14.523 ms	Average 14.64 ms	Max	. 14.761 ms

Document Version: V2.1

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

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

Diagnose		
	[]	1
Diagnose	Traceroute •]
IP Address/Domain Name	cn.bing.com	
	Start	



Diagnose			
	Diagnose	Traceroute 🔹	
IP Addre	ss/Domain Name	cn.bing.com	
		Stop	
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	192.168.21.2	54	1.885 ms 4.249 ms 2.758 ms
5	100.64.0.1		50.352 ms 3.056 ms 3.428 ms
6	202.105.159.1	49	4.340 ms 8.592 ms 7.126 ms

Document Version: V2.1

8.2.4 Speed test

Overview

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

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

Diagnose		
Diagr	Speed Test	•
↑ AVG RX	👃 AVG TX	🕼 AVG Total
0 Mbps	0 Mbps	0 Mbps
	● Client ○ Serve	er
IP Address of Pee	r AP Manual	T
IP Add	Iress	
HTTP	Port 80	
User N	ame	
Passv	vord	
Test Gr	roup 10	(Range: 1 to 20)
Direc	tion Bidirectional	¥
1	Time 30	s (Range: 1 to 60)
	Start	

Parameters description

Name	Description
AVG RX	Specifies the average receive rate.
AVG TX	Specifies the average transmit rate.
AVG Total	Specifies the average total rate.

Document Version: V2.1

Name	Description	
Client	This version is not supported vet.	
Server		
IP Address of Peer AP	Specifies the LAN IP address of peer CPE. You can enter it manually or select the IP address of the peer AP from the drop-down list if there are peer CPEs connected to the CPE.	
IP Address	If the IP Address of Peer AP is set to Manual , you need to enter the LAN IP address of peer CPE in the box manually.	
HTTP Port	Specifies the HTTP service port number of peer device, 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 near device	
Password	specify the login user hame and password of the peer device.	
Test Group	Specifies the number of test connections launched.	
Direction	 Specifies the test direction. RX (Receive): Only test the speed that the peer device transmits data to this device. TX (Transmit): Only test the speed that this device transmits data to peer device. Bidirectional: Test both transmit and receive speed between the two CPEs. 	
Time	Specifies the duration of speed test, which is 30s by default.	

Example of configuring the speed test

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

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

Assume that:

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

Document Version: V2.1

Configuration procedure

- **Step 1** Log in to the web UI of the CPE2.
- **Step 2** Navigate to **Advanced** > **Diagnose**.
- **Step 3** Select **Speed Test** in the **Diagnose** drop-down list.
- **Step 4** Set **IP Address of Peer AP** to **Manual**.
- **Step 5** Enter the IP address of CPE1 to the **IP Address**, which is **192.168.2.100** in this example.
- Step 6 Enter the login user name and password of the web UI of the CPE1 in the User name and Password boxes, which are both admin in this example.
- **Step 7** Set **Direction** to **Bidirectional**.
- Step 8 Click Start.

Diagnose		
* Diagno	Speed Test	•
🕇 AVG RX	👃 AVG TX	🕼 AVG Total
0 Mbps	0 Mbps	0 Mbps
	● Client	er
¥ IP Address of Peer	AP Manual	v
* IP Addr	ess 192.168.2.100	
HTTP P	ort 80	
* User Na	me admin	
Passwo	admin	
Test Gro	up 10	(Range: 1 to 20)
* Directi	Bidirectional	¥
Ti	me 30	s (Range: 1 to 60)
	Start	

----End

Diagno	se		
	Diagnose	Speed Test	•
	↑ AVG RX	👃 AVG TX	🕼 AVG Total
	103.28 Mbps	105.17 Mbps	208.45 Mbps

8.2.5 Spectrum analysis

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

₽TIP

- The frequency bands of bridging CPEs must be consistent.
- Some CPE models only can check the wireless noise of each channel. And you can select a frequency band with less wireless noise for the CPE based on the diagnose result. Please refer to the product you purchased.

O4 as an example

Configuration procedure

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

Diagnose		
		?
Diagnose	Spectrum Analysis 🔹	
Fraguency Pand		
Frequency band	36(5180MHZ) • 48(5240MHZ) • Start	

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

Note		×
All wireless connections will	be terminated when the spectrum analysis is launching on the device! P	lease click OK to Start.
	OK Cancel	

----End
Document Version: V2.1

To select a frequency band with less signal strength for the CPE based on the diagnosis result, 48 can be selected as the frequency band of the CPE.



O6V3.0 as an example

Configuration procedure of checking channel utilization:

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

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

Document Version: V2.1

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



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

To select a frequency band with less channel utilization for the CPE based on the diagnosis result, 44 can be selected as the frequency band of the CPE.



Configuration procedure of checking noise intensity:

- Step 1 Log in to the web UI of the CPE.
- **Step 2** Navigate to **Advanced > Diagnose**.
- Step 3 Select Spectrum Analysis from the Diagnose drop-down list.
- Step 4 Select Noise Intensity.
- **Step 5** Select the value to be tested, which is **Average Value** in this example.

Document Version: V2.1

Step 6 Select the frequency band range you want to test, which is **36(5180 MHz)** to **48(5240MHz)** in this example.

Step 7 Click Start.

Diagnose	Spectrum Analysis 🗸		
	○ Channel Utilization	Noise Intensity	Average Value 🖌
Frequency Band	36(5180MHz) 🗸 —	48(5240MHz) ¥	

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

All wireless connections will	be terminated when the spectrum analysis	s launching on the device! Please	click OK to Start
		Ū	
	ОК Салса	اد	

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

To select a frequency band with less signal strength for the CPE based on the diagnosis result, 40 can be selected as the frequency band of the CPE.

Diagnos	e Spectrum Analysis 🗸		
	○ Channel Utilization	Noise Intensity	Average Value 🗸
Frequency Ban	d 36(5180MHz) 🗸	48(5240MHz) 🗸	
	Start		
0			
072			
-25			
-25			
-25 -50 -75			
-25 -50 -75 -100			
-25 -50 -75 -100 -125			

Document Version: V2.1

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				2
Remark				-
IP Address Range	192.168.2. ~ 192.168.2.			
Max. Upload Rate	Mbps	¥		
Max. Download Rate	Mbps	v		
	Add			
ID Remark IP Addres	s Range Max. Upload Rate	Max. Download Rate	Status	Action

Name	Description
Remark	Specifies the additional information of the bandwidth control rule. This field is optional. For convenient management, you'd better specify different remarks for different rules.
IP Address Range	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.

Parameters description

Document Version: V2.1

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

- **Step 1** Log in to the web UI of the CPE.
- **Step 2** Navigate to **Advanced** > **Bandwidth Control**.
- **Step 3** Enter a remark (optional), which is **Devices of Office1** on this example.
- **Step 4** Set **IP Address Range**, which is **192.168.2.100** ~ **192.168.2.200** in this example.
- **Step 5** Set the maximum upload rate and download rate respectively, which are **5** and **10** in this example.
- Step 6 Click Add.

Bandwidth Control			
Remark	Devices of Office1		?
IP Address Range	192.168.2. 100 ~ 192.168.2	200	
Max. Upload Rate	5	Mbps •	
Max. Download Rate	10	Mbps •	
	Add		

----End

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

Document Version: V2.1

ID	Remark	IP Address Range	Max. Upload Rate	Max. Download Rate	Status	Action
1	Devices of	192.168.2.100~192.168.2.200	5Mbps	10Mbps	⊘ Enable	Ī
10 🔻	Datas/Page	1 data in total				

Verification

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

Document Version: V2.1

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**.

ort Forwarding						
Internal IP Address						
Internal Port	23					
External Port	23					
Protocol	TCP&UDP	•				
Application	Telnet	•				
	Add					
ID Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action

Parameters description

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

Document Version: V2.1

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: V2.1

₽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

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

Document Version: V2.1

orwarding		
Internal IP Address	192.168.2.100	
Internal Port	9999	
External Port	9999	
Protocol	TCP&UDP 🗸	
Application	HTTP 🗸	

----End

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

ID	Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action
1	192.168.2.100	9999	9999	TCP&UDP	HTTP	✓Enable	
10 🗸	Datas/Page 1 data in	n 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 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 domain name:External port**.



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

8.5 MAC filter

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

8.5.1 Overview

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

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

MAC Filter	
Mode	Allow
Remark	
MAC Address	
Time	00 • : 00 • ~ 00 • : 00 •
Date	Mon. Tue. Wed. Thur.

Fri. Sat. Sun. Every Day

Time

Mode

Status

Action

MAC Address

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

Parameters description

Remark

ID

Name	Description
	Specifies the mode of MAC filter rule.
	- Disable : Disable the MAC Filter function.
Mode	 Allow: Allow the devices with the MAC addresses in the list to access the internet with the CPE, and disallow the other devices to access the internet with the CPE.
	 Disallow: Disallow the devices with the MAC addresses in the list to access the internet with the CPE, and allow the other devices 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: V2.1

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: Only allow the device of a purchasing staff to access the internet during 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 staff's computer is CC:3A:61:71:1B:6E.

Configuration procedure

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

Document Version: V2.1

Mode	Allow	~
Remark	Purchasing	
MAC Address	CC:3A:61:71:1B:6E	
Time	08 🗸:00 🗸 ~ 18	♥:00 ♥
Date	Mon. 🔽 Tue.	Ved. Ved.
	🖌 Fri. 🗌 Sat. 🗌	Sun. 🗌 Every Day



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

ID	Remark	MAC Address	Time	Mode	Status	Action
1	Purchasing	CC:3A:61:71:1B:6E	Mon. 、Tue. 、Wed. 、Thur. 、Fri. 08:00- 18:00	Allow	✓ Enable	
10 🗸	Datas/Page	1 data in total				

Verification

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

Document Version: V2.1

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		
DDNS	\bigcirc	
Service Provider	3322.org • R	<u>egister</u>
User Name		
Password		
Domain Name		

Parameters description

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

Example of configuring DDNS

Networking 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

₽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.

Document Version: V2.1



Configuration procedure

- **Step 1** Log in to the web UI of the CPE.
- Step 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 🗸	Register
User Name	JohnDoe	
Password		
Domain Name	JohnDoe.dyndns.com	

- **Step 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.

Document Version: V2.1

- 3. Set Internal Port and External Port, which are 9999 in this example.
- 4. Set Protocol, which is TCP&UDP in this example
- 5. Set **Application**, which is **HTTP** in this example.
- 6. Click Add.

ort Forwarding		
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 🗸	Datas/Page 1 data in	n 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 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.

Document Version: V2.1

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

8.6.2 Remote web management

Overview

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

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

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	

Parameters description

Name	Description
Remote Web Management	Specifies whether to enable the remote web management function.
IP Address	 Specifies the IP address of a CPE which is 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. Manual: It indicates that only the device with specified IP address can manage the CPE remotely. If the CPE belongs to a LAN, the gateway address (a public IP address) of the CPE should be entered.
Port	Specifies the port number used for remote management of CPE. Default: 8080 . You can change it as required.

Document Version: V2.1

Name

Description

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.

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 Tenda 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

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

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

----End

Document Version: V2.1

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 on the CPE, you can access the CPE by visiting an address in the form of **http://Domain name of WAN port: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

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

Reboot Schedule				
Time	3:00			
Date	Mon.	🖌 Tue.	🗹 Wed.	Thur.
	🗸 Fri.	Sat.	Sun.	Every Day

----End

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

8.6.4 Login timeout interval

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

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

Document Version: V2.1

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

Document Version: V2.1

8.6.5 SNMP agent

Overview

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

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

SNMP management framework

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

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

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

Basic SNMP operations

The device allows the following basic SNMP operations:

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

SNMP protocol version

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

Document Version: V2.1

SNMP manager. If the community name contained in an SNMP packet is rejected by a device, the packet is discarded. A community name functions as a password to control SNMP agent access attempts of SNMP managers.

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

MIB introduction

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



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**.

SNMP Agent		
Device Name	O4V1.0	
Read Community	public	
Read/Write Community	private	
Location		

Document Version: V2.1

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 the model and version number of the CPE.
Device Name	
	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: V2.1

Example of configuring the SNMP function

Networking requirements

- The CPE connects to an NMS over a LAN. This network address of the CPE is 192.168.2.1/24 and the network IP address of the NMS is 192.168.2.212/24.
- The NMS 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

- Step 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 **Jack** in this example.
 - 5. Set Read/Write Community, which is Jack123 in this example.
 - 6. Click **Save** on the bottom of this page.

* SNMP Agent	
Device Name	O4V1.0
\star Read Community	Jack
★ Read/Write Community	Jack123
Location	

Step 2 Set up the NMS.

Document Version: V2.1

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

----End

Verification

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

8.6.6 Ping watch dog

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

- **Step 1** Log in to the web UI of the CPE.
- **Step 2** Navigate to **Advanced > Network Service**.
- **Step 3** Enable the **Ping Watch Dog** function.
- **Step 4** Set the related parameters as required.
- Step 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

Parameters description

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

Document Version: V2.1

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 packet that triggers reboot. The value range is 1 to 65535. The default value is 3. For example, if 5 is set, the device will reboot automatically when it does not receive response after sending 5 Ping packets to target IP address/domain name.

8.6.7 DMZ host

Overview

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

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: V2.1

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 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 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

₽_{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.

Document Version: V2.1



- Step 1 Log in to the web UI of the CPE.
- **Step 2** Navigate to **Advanced > Network Service**.
- Step 3 Enable the DMZ Host function.
- Step 4 Set DMZ Host IP Address, which is 192.168.2.100 in this example.
- Step 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 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 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 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 domain name: Intranet service port**.

Document Version: V2.1

₽

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, it requires that the operating system support 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.

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

Document Version: V2.1

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: V2.1

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.

₽_{TIP}

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

9.1.1 Synchronized with the internet

The CPE automatically synchronizes its system time with a time server 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 the configuration procedure of corresponding mode in <u>Quick Setup</u>.

Configuration Procedure

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

Document Version: V2.1

Date & Time	
	2
Time Settings	Synchronized with the Internet Manual
Time Interval	30 minutes •
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, 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.

Parameters description

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

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

Document Version: V2.1

Date & Time	
Time Settings	○ Synchronized with the Internet
Date & Time	2023 Y 08 M 24 D 11 h 41 m 17 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: V2.1

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

- Step 1 Log in to the web UI of the CPE.
- **Step 2** Navigate to **Tools > Maintenance**.

Step 3 Click Reboot.

Maintenance	2
Reboot Device	Reboot
Reset to Factory Settings	Reset
Upgrade Firmware	All configurations will restore to default factory setting after reset. Upgrade
	Current Software Version: V1.0.0.15(4409) ; Release Date: 2019-05-28 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

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

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

----End

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

Document Version: V2.1

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.

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

Option 1: Reset the CPE through the web UI

Step 1 Log in to the web UI of the CPE.

Step 2 Navigate to **Tools > Maintenance**.

Step 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: V1.0.0.15(4409) ; Release Date: 2019-05-28 Note: Do not disconnect the power supply of the device during ungrade
Backup/Restore	process, or the device will be damaged. Backup/Restore Backup current settings or import saved settings to device

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

	es will be reset to 102.160	2.2.1. Ann
The IP addre	ess will be reset to 192.100	5.2.1. Are you sure to reset it?
The IP addre	55 WIII DE TESEL LO 192,100	s.2.1. Are you sure to reset it?

----End

A progress bar is displayed on the page. Wait for it to complete.
Document Version: V2.1

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.

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

- Step 1 Download the package of a later firmware version for the CPE from <u>www.tendacn.com</u> to your local computer, and decompress the package.
- **Step 2** Log in to the web UI of CPE, and navigate to **Tools** > **Maintenance**.

Step 3 Click Upgrade.

Maintenance	2
Reboot Device	Reboot
	All connections will disconnect during reboot.
Reset to Factory Settings	Reset
	All configurations will restore to default factory setting after reset.
Upgrade Firmware	Upgrade
	Current Software Version: V1.0.0.15(4409) ; Release Date: 2019-05-28 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

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

----End

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

Document Version: V2.1



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.

UNOTE

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

Backup

- Step 1 Log in to the web UI of CPE.
- **Step 2** Navigate to **Tools > Maintenance**.
- **Step 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: V1.0.0.15(4409) ; Release Date: 2019-05-28 Note: Do not disconnect the power supply of the device during upgrade
Backup/Restore	process, or the device will be damaged. Backup/Restore Backup current settings or import saved settings to device

Step 4 Click Backup on the pop-up window.

Document Version: V2.1

ckup/Restore			×
Backup configurations	Backup	J	

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

```
----End
```

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

Restore

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

Maintenance	
	?
Reboot Device	Reboot
	All connections will disconnect during reboot.
Reset to Factory Settings	Reset
	All configurations will restore to default factory setting after reset.
Upgrade Firmware	Upgrade
	Current Software Variant V1001E(4400) - Balance Date: 2010.0E-28
	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
Upgrade Firmware Backup/Restore	All configurations will restore to default factory setting after reset. Upgrade Current Software Version: V1.0.0.15(4409) ; Release Date: 2019-05-28 Note: Do not disconnect the power supply of the device during upgrade process, or the device will be damaged. Backup/Restore Backup current settings or import saved settings to device

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

Document Version: V2.1

Step 5 Select and upload the file you back up before (the suffix of the backup file: .cfg).
----End

After the file is uploaded, the CPE reboots automatically.

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

Document Version: V2.1

9.3 Account

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

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

Guest

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**.

₽TIP

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

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

Document Version: V2.1

Parameters description

Name	Description		
	Specifies the user name/password of the current login account.		
Old User Name/Old	By default, the CPE has one administrator account and one guest account.		
Password	Administrator user name/password: admin/admin (all lowercase)		
	Guest user name/password: user/user (all lowercase)		
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

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

Guest Account		×
Enable	\bigcirc	
Old User Name	user	
Old Password]
New User Name]
New Password]
Confirm Password]
	Save	1

9.4 System log

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

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

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

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

System Log	9		
Refresh	Clear		Log Type All 🔻
ID	Time	Туре	Log
1	2019-01-16 15:03:15	System	SNMP Stop
2	2019-01-16 15:03:04	System	web 192.168.2.11 login
3	2019-01-16 15:02:59	System	web login time expired

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

- 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: V2.1

Appendix

A.1 Default parameters

The main default parameters are shown in the following table.

Parameters			Default settings
	Login IP Address	Single	192.168.2.1
		Kit	AP mode: 192.168.2.1 Client mode: 192.168.2.2
Login		User name	admin
	Administrator	Password	admin
	Guest		Disable
Quick Setup		Single	AP mode
Quick Setup		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
	DHCP Server	Single	Enable
DHCP Server		Kit	Disable
	Start IP Address		192.168.2.100
	End IP Address		192.168.2.200
	Subnet Mask		255.255.255.0
	Gateway Address		192.168.2.254

Document Version: V2.1

Parameters		Default settings
	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: Tenda_XXXXXX, and XXXXXX is the last six characters of the LAN MAC address of the device.
	SSID	Management RF: Tenda_XXXXXX_MG, and XXXXXX is the last six characters of the LAN MAC address of the device.
Wireless		
wireless		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
Network Service	Ping Watch Dog	Disable
	Telnet Service	Enable
	UPnP	Disable
	Hardware Watch Dog	Enable
	STP	Disable
Tools	Date & Time	Synchronized with the internet

Document Version: V2.1

A.2 Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling	
AES	Advanced Encryption Standard	
AP	Access Point	
ARP	Address Resolution Protocol	
BSSID	Basic Service Set Identifier	
CAT5e	Category 5 Enhanced	
CCQ	Client Connection Quality	
CPE	Customer Premises Equipment	
CPU	Central Processing Unit	
DFS	Dynamic Frequency Selection	
DHCP	Dynamic Host Configuration Protocol	
DNS	Domain Name System	
DDNS	Dynamic Domain Name Server	
DTIM	Delivery Traffic Indication Map	
DMZ	Demilitarized Zone	
GMT	Greenwich Mean Time	
НТТР	Hypertext Transfer Protocol	
IP	Internet Protocol	
ISP	Internet Service Provider	
ICMP	Internet Control Message Protocol	
LAN	Local Area Network	
MAC	Media Access Control	
MIB	Management Information Base	

Document Version: V2.1

Acronym or Abbreviation	Full Spelling	
NMS	Network Management System	
NVR	Network Video Recorder	
OID	Object Identifier	
РоЕ	Power over Ethernet	
РРРоЕ	Point-to-Point Protocol over Ethernet	
Р2МР	Point-to-Multi-Point	
PVID	Port-based VLAN ID	
RADIUS	Remote Authentication Dial In User Service	
RAM	Random Access Memory	
RSSI	Received Signal Strength Indicator	
RTS	Request to Send	
RX	Receive	
SSID	Service Set Identifier	
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	

Document Version: V2.1

Acronym or Abbreviation	Full Spelling
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: V2.1

A.3 How to assign a fixed IP address to your computer

OS example: Windows 7

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

Troubleshoot problems
Open Network and Sharing Center
30/09/2019

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

	Local Area Connection Status	
Network a	General h Control Panel	Q
Control Panel Home Change adapter settings	Connection Ip connections IPv4 Connectivity: Internet IPv6 Connectivity: No network access	See full map
settings	Media State: Enabled Internet	
	Speed: 1.0 Gbps Connect or	disconnect
	Details pe: Internet Activity	unnection E
See also	Close computers of change	charing
HomeGroup	settings.	sharing
Internet Options		
Windows Firewall	Diagnose and repair network problems, or get troubleshooting information	on. 👻

Document Version: V2.1

Step 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 ✓ GoS 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 ✓ ➡ 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

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

Internet Protocol Version 4 (TCP/IPv4)	Properties ? X	
General		
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.		
Obtain an IP address automatically		
Ouse the following IP address:		
IP address:	192.168.2.20	
Subnet mask:	255.255.0	
Default gateway:		
 Obtain DNS server address automatically Use the following DNS server addresses: 		
Preferred DNS server:		
Alternate DNS server:	· · ·	
Validate settings upon exit	Advanced	
	OK Cancel	

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

----End

Document Version: V2.1

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

OS example: Windows 7

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

Troubleshoot problems		
	Open Network and Sharing	Center
		28/02/2019

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



----End

Document Version: V2.1

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

Network Connection Details		
Network Connection Details:		
Property	Value	
Connection-specific DN Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask Lease Obtained	tendawifi.com Intel(R) 82583V Gigabit Network Connect 44-8A-5B-F5-10-1F Yes 192.168.0.194 255.255.255.0 Monday, 30 September 2019 3:24:56 PM	
Lease Expires	Tuesday, 1 October 2019 3:24:56 PM	
IPv4 DHCP Server IPv4 DNS Server IPv4 WINS Server	192.168.0.1 192.168.0.1	
NetBIOS over Tcpip En Link-local IPv6 Address IPv6 Default Gateway IPv6 DNS Server	Yes fe80::e80ff267:320e:67c0%10	
•	۱۱۱	
	Close	