



2Km Outdoor Point to Point CPE

User Guide

Copyright Statement

© 2019 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.

Preface

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

Conventions

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

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

Acronyms and Abbreviations

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

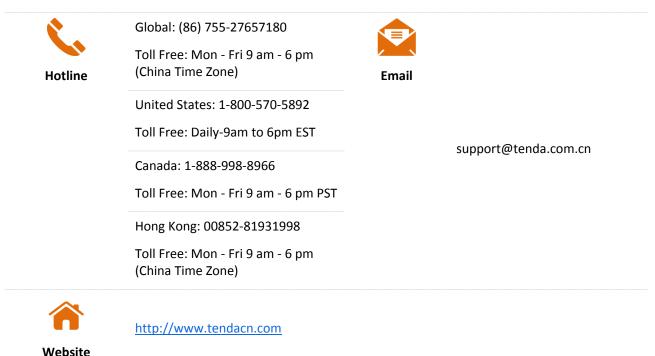
Acronym or Abbreviation	Full Spelling	
GMT	Greenwich Mean Time	
IP	Internet Protocol	
ICMP	Internet Control Message Protocol	
LAN	Local Area Network	
MAC	Media Access Control	
PoE	Power Over Ethernet	
P2MP	Point-to-MultiPoint	
PVID	Port-based VLAN ID	
RADIUS	Remote Authentication Dial In User Service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

Additional Information

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

Technical Support

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



Contents

1	Introduction
	1.1 Overview
	1.2 Getting to know your device
2	Quick setup
	2.1 AP mode
	2.2 Client mode
	2.3 Example of AP mode and client mode10
	2.4 Universal repeater mode
	2.5 WISP mode
	2.6 Repeater mode
	2.7 P2MP mode42
	2.8 Example of repeater mode and P2MP mode45
	2.9 Router mode
3	Web UI
	3.1 Login
	3.2 Logout
	3.3 Web UI layout
	3.4 Common buttons
4	Status
	4.1 System status60
	4.2 Wireless status
	4.3 Statistics
5	Network70
	5.1 LAN setup
	5.2 MAC clone

	5.4 DHCP client	81
	5.5 VLAN settings	82
6	Wireless	86
	6.1 Basic	86
	6.2 Advanced	114
	6.3 Access control	118
7	Advanced	121
	7.1 LAN rate	121
	7.2 Diagnose	123
	7.3 Bandwidth control	130
	7.4 Port forwarding	133
	7.5 MAC filter	137
	7.6 Network service	141
8	Tools	159
	8.1 Date & time	159
	8.2 Maintenance	161
	8.3 Account	166
	8.4 System log	169
Арр	pendix	170
	A.1 FAQ	170
	A.2 Default parameters	173

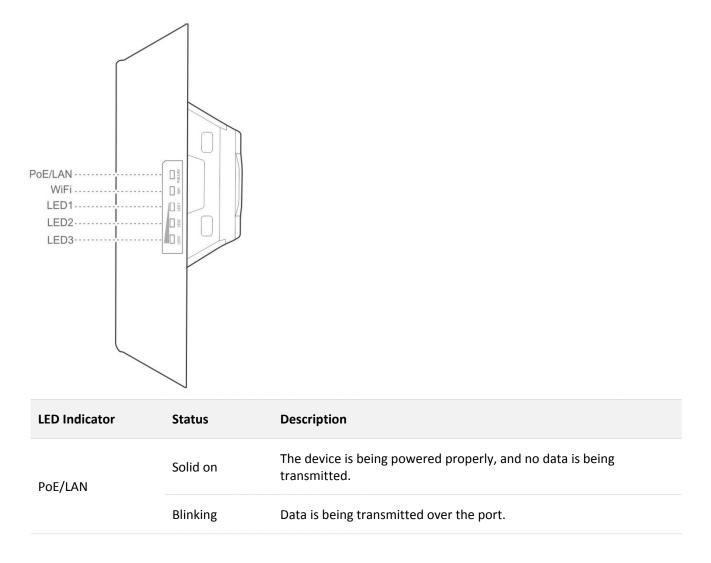


1.1 Overview

The Tenda outdoor point to point CPE is dedicated for ISP and CCTV surveillance. Featured 12 dBi directional antennas, it offers strong and stable WiFi signals and a wireless connection up to 2 kilometers. The industry grade waterproof and dustproof housing allows it to work properly even in harsh environments. With auto-bridging technology, two CPEs can connect to each other automatically to make setup a breeze.

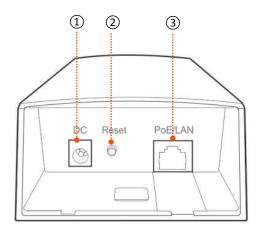
1.2 Getting to know your device

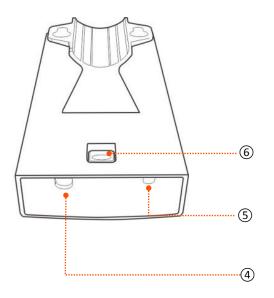
LED indicators



LED Indicator	Status	Description		
	Off	The device is not powered on.		
	Solid on	The wireless function is enabled, but no data is being transmitted.		
WiFi	Blinking	Data is being transmitted in a wireless manner.		
	Off	The wireless function is disabled.		
LED1, LED2, LED3 (Signal strength LED)	Solid on/Blinking	 Signal strength LED indicators. Solid on indicates the device works in AP, P2MP, Repeater or Router mode, while blinking indicates the device works in Client, Universal Repeater or WISP mode. The corresponding LED indicator lights up when the received signal strength reaches the threshold of the corresponding LED indicator which is set on the Wireless > Advanced page. The default threshold for LED1, LED2, and LED3 are -90 dBm, -80 dBm, and -70 dBm respectively. LED1, LED2 and LED3 are solid on/blinking: Good signal LED1 and LED2 are sold on/blinking, and LED3 is off: Fair signal LED1 is solid on/blinking, and LED2 and LED3 are off: Weak signal. Please adjust the direction or location of your devices. 		
	Off	The received signal does not reach the minimum threshold of the signal strength LED indicator.		

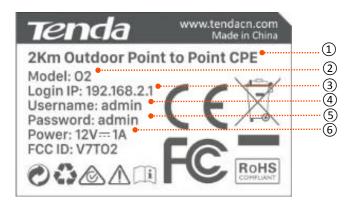
Button and ports





ID	Port/Button	Description
1	DC	Power jack. Use the included power adapter to connect this jack to a power source for power supply.
2	Reset	Reset Button. After the device is powered on for 1 minute, hold down this button for about 8 seconds. When all the LED indicators on the device light up, the device is restored factory settings.
3	PoE/LAN	 This port is used to supply power or transmit data. To power on the device using PoE, connect this port to the PoE port of the included PoE injector. If the device is powered on using a DC power adapter, this port functions as a LAN port, and can be connected to a switch.
4	/	Ethernet cable inlet.
5	/	Power cord inlet.
6	/	Press this button to uncover the device.

Product label



- $(1) \rightarrow$ Product name of the device
- (2)→Product model of the device
- (3)→Default login IP address of the device
- ④→Default login user name of the device
- (5)→Default login password of the device
- $(6) \rightarrow$ Power input standard of the device

2 Quick setup

This module enables you to quickly configure the device or change the working mode of the device

to deploy your wireless network.

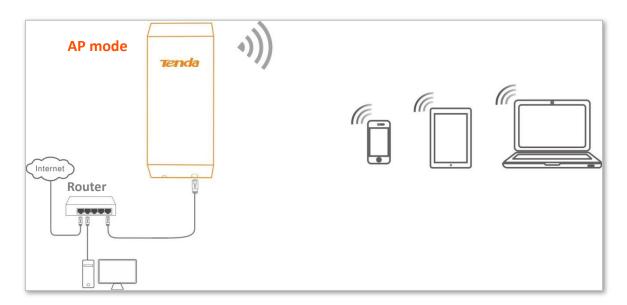
O2 supports AP, Client, Universal Repeater, WISP, Repeater, P2MP, and Router modes.

2.1 AP mode

In AP mode, this device connects to a wired network, and provides a wireless network for wireless clients.

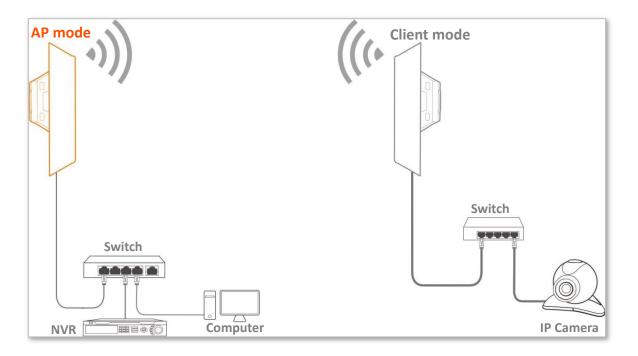
Application scenario 1

Network requirement: You want to transform your wired network to a wireless one for your wireless devices to access the internet.



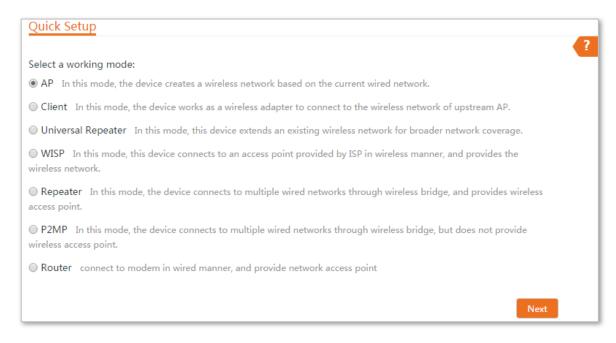
Application scenario 2

Network requirement: You want to establish a CCTV surveillance network, and use the CPE to connect to the NVR.



Configuration procedure of setting AP mode

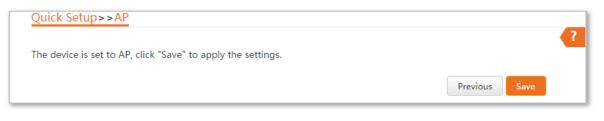
- **Step 1** Log in to the web UI of the CPE and choose **Quick Setup** to enter the configuration page.
- Step 2 Select AP mode and click Next.



Step 3 Set an SSID, **Security Mode** (WPA2-PSK is recommended) and **Key**, and click **Next**.

Quick Setup>>AP	Current Mode: A
You can set up your wireless netwo	ork name and wireless password here.
Note down your wireless password	ł.
SSID	Tenda_123456
Channel	Auto
Security Mode	WPA2-PSK V
Encryption Algorithm	● AES
Key	
	Previous

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



----End

Parameters description

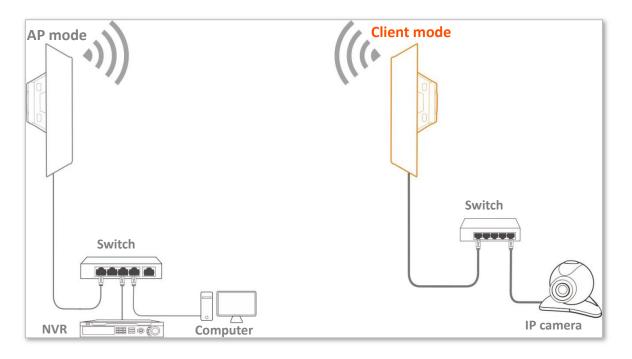
Name	Description
	It specifies the working mode of this device.
Working modes	AP mode: in this mode, the device creates a wireless network based on the current wired network.
SSID	It specifies the wireless network name of this device.
	It specifies the operating channel of this device.
Channel	Auto : It indicates that the device automatically adjusts its operating channel according to the ambient environment.
Security Mode	It specifies the security mode of the wireless network, including: <u>None</u> , <u>WPA-PSK</u> , <u>WPA2-PSK</u> , and <u>Mixed WPA/WPA2-PSK</u> .
Security Mode	Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.
Encryption Algorithm	It specifies the encryption method of the wireless network.
Кеу	It specifies the WiFi password of the wireless network.

2.2 Client mode

In Client mode, this device servers as a wireless adapter, and connects to a wireless network of upstream AP.

Application scenario

Network requirement: you want to establish a CCTV surveillance network, and use the CPE to connect to IP cameras.



Configuration procedure of setting Client mode

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

Quick Setup	
Select a working mod	e:
AP In this mode, th	e 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, wireless network.	this device connects to an access point provided by ISP in wireless manner, and provides the
Repeater In this movine less access point.	ode, the device connects to multiple wired networks through wireless bridge, and provides
P2MP In this mode wireless access point.	e, the device connects to multiple wired networks through wireless bridge, but does not provide
Deuter	modem in wired manner, and provide network access point

Step 3 Select the SSID of the peer device and click **Next**.

	Quick Setup>>Client							
	Click "Scan", and select the wireless network you want to connect,							
	and click "Next".							
		Scan	Scan again	1				
		Upstream AP	Tenda_123456					
	Select	SSID	Channel	MAC Address	Security Mode	Signal Strength		
_	۲	Tenda_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	-11		

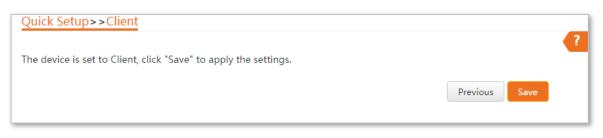
- If you cannot find any SSID from the list, choose **Wireless** > **Basic** and enable the wireless function. Then try again.
- If you cannot find the SSID of CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1.
- **Step 4** Enter the WiFi password you set on the peer device in the **Key** text box, and click **Next**.

Quick Setup>>Client	
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those of upstream AP.
Then enter the remote AP's WiFi	password, and click "Next" to continue.
Upstream AP	Tenda_123456
Upstream AP MAC Address	C8:3A:35:15:86:A1
Channel	165(5825MHz) v
Security Mode	WPA2-PSK
Encryption Algorithm	● AES
Кеу	
	Previous

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

Quick Setup>>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	

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



----End

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



- If you cannot find any SSID from the list, choose Wireless > Basic and enable the wireless function.
 Then try again.
- If you cannot find the SSID of CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1

Parameters description

Name	Description
	It specifies the working mode of this device.
Working modes	Client mode : in this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP, and does not provide wireless access point.
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

2.3 Example of AP mode and client mode

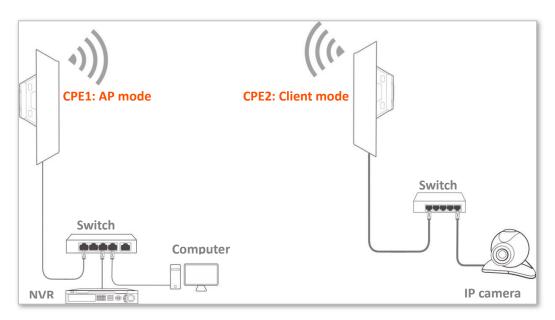
Network requirement

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

Solution

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

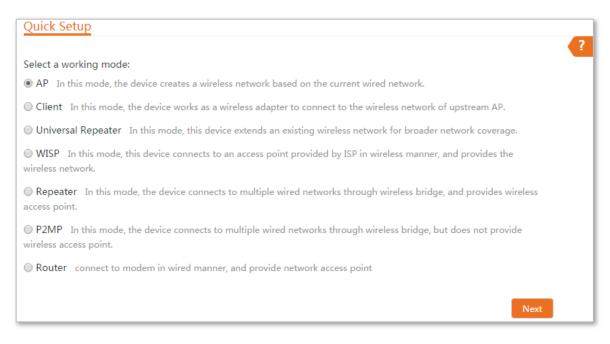
Network topology



Configuration procedure

Step 1 Set up CPE1.

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



 Set an SSID, which is Tenda_123456 in this example, Security Mode (WPA2-PSK is recommended) and Key, and click Next.

Quick Setup>>AP		Current Mode: AF
	ork name and wireless password here.	2
Note down your wireless password	L	
SSID	Tenda_123456	
Channel	Auto	
Security Mode	WPA2-PSK V	
Encryption Algorithm	● AES ◎ TKIP ◎ TKIP&AES	
Key		
	Prev	vious

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

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

Step 2 Set up CPE2.

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

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

3. Select the SSID of the CPE1, which is **Tenda_123456** in this example, and click **Next**.

Quick Set	up>>Client					?
Click "Scan" and click "N	, and select the wireless lext".	s network you wa	nt to connect,			
	Scan	C Scan again	<u>n</u>			
	Upstream AP	Tenda_123456				
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
۲	Tenda_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	lite.	

₽_{TIP}

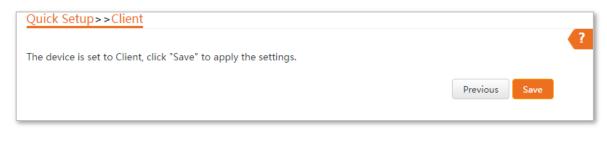
- If you cannot find any SSID from the list, choose Wireless > Basic and enable the wireless function.
 Then try again.
- If you cannot find the SSID of CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1.
- 4. Enter the WiFi password you set on CPE1 in the Key text box, and click Next.

Quick Setup>>Client	?
	ame channel, encryption, and encryption algorithm as those of upstream AP. password, and click "Next" to continue.
Upstream AP	Tenda_123456
Upstream AP MAC Address	C8:3A:35:15:86:A1
Channel	165(5825MHz) •
Security Mode	WPA2-PSK •
Encryption Algorithm	● AES
Key	•••••
	Previous

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

Quick Setup>>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 device reboots to activate the settings.



----End

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

₽

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

Verification

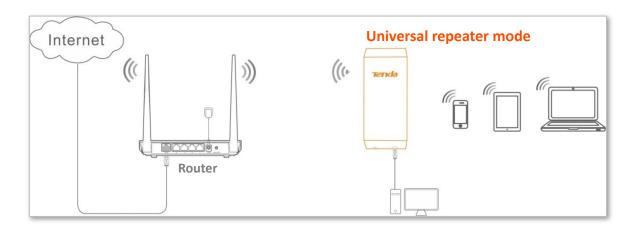
Surveillance videos can be seen on the computer in the side of CPE1.

2.4 Universal repeater mode

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

Application scenario

Network requirement: You want to use the CPE to extend your existing wireless network. And your existing router does not support WDS mode.



Configuration procedure of setting Universal Repeater mode

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

Quick Setup
Select a working mode:
◎ AP In this mode, the device creates a wireless network based on the current wired network.
Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
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 Select the SSID of the router and click **Next**.

uick Setu	p>>Universal Re	peater			
lick "Scan", a nd click "Nex	and select the wireles	s network you w	ant to connect,		
	Scan	Scan aga	in		
	Upstream AP	WiFi_123456			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	WiFi_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	

₽

If you cannot find the SSID of the router from the list, ensure that the 5 GHz WiFi network of the router is enabled. Only the WiFi networks at 5 GHz band will be displayed in the list.

Step 4 Enter the WiFi password of the router in the **Key** text box, 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	password, and click "Next" to continue.
Upstream AP	WiFi_123456
Upstream AP MAC Address	C8:3A:35:15:86:A1
Channel	165(5825MHz) •
Security Mode	WPA2-PSK •
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Key	
	Previous Next

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

Quick Setup>>Universal Rep	peater		
Set the IP address to an unused IP	address belonging to the n	etwork segment of unstream AP.	2
IP Address	192.168.2.100		
Subnet Mask	255.255.255.0		
		Previous	Next

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

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

₽

- If you cannot find any SSID from the list, choose Wireless > Basic and enable the wireless function.
 Then try again.
- If you cannot find the SSID of CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1

Parameters description

Name	Description
	It specifies the working mode of this device.
Working modes	Universal Repeater mode : in this mode, the device expands your WiFi network for broader network coverage.
	Advantage of Universal Repeater compared with Repeater mode: This mode does not require that the upstream AP supports WDS function.
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.

Example of universal repeater mode

Network requirement

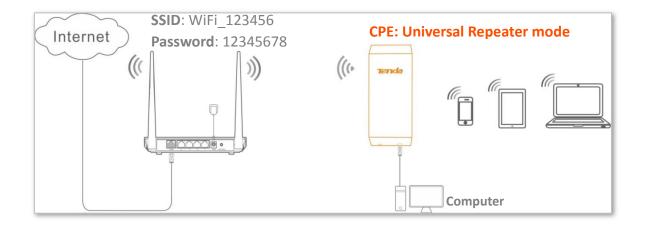
You are in a WiFi dead zone or a place with weak wireless signal, and have a wireless router that does not support WDS function. Now you want to have a larger WiFi network coverage through your home or office.

Solution

Set the CPE to **Universal Repeater** mode, and extend the WiFi network of the router. Assume that the SSID and password of the router are shown as follows:

- **SSID**: WiFi 123456
- Password: 12345678

Network topology



Configuration procedure

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

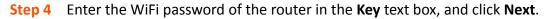
Quick Setup
?
Select a working mode:
○ AP In this mode, the device creates a wireless network based on the current wired network.
Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
O Universal Repeater In this mode, this device extends an existing 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 Select the SSID of the router, which is **WiFi_123456** in this example, and click **Next**.

Quick Setur	o>>Universal Re	peater				?
Click "Scan", a and click "Nex	nd select the wireles	s network you w	ant to connect,			
	Scan	Scan aga	in			
	Upstream AP	WiFi_123456				
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
۲	WiFi_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	lle.	

₽

If you cannot find the SSID of the router from the list, ensure that the 5 GHz WiFi network of the router is enabled. Only the WiFi networks at 5 GHz band will be displayed in the list.

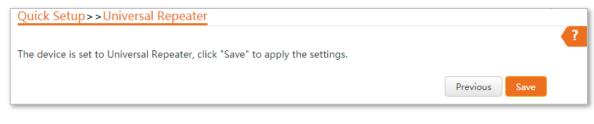


Quick Setup>>Universal Repeater		
	me channel, encryption, and encryption algorithm as those of upstream AP.	
Upstream AP		
Upstream AP MAC Address	C8:3A:35:15:86:A1	
Channel	165(5825MHz) •	
Security Mode	WPA2-PSK V	
Encryption Algorithm	● AES ○ TKIP ◎ TKIP&AES	
Key		
	Previous Next	

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

Quick Setup>>Universal Re	peater	?
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

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



----End

₽_{TIP}

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

Verification

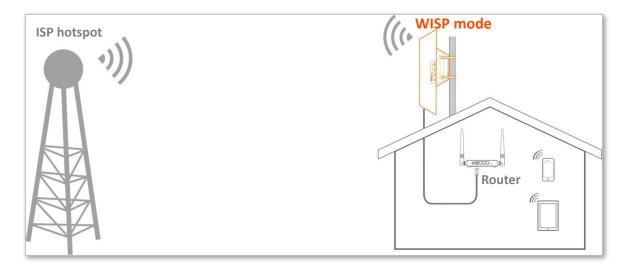
Your wireless devices can search the SSID of the CPE, and connect to its wireless network for internet access.

2.5 WISP mode

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

Application scenario

Network requirement: You want to use the CPE to extend the ISP hotspot to your home.



Configuration procedure of setting WISP mode

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

 Quick Setup
2
Select a working mode:
◎ AP In this mode, the device creates a wireless network based on the current wired network.
O Client In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
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 Select the SSID of your ISP (Internet Service Provider) hotspot and click **Next**.

Quick Setu	p>>WISP				
Click "Scan", and click "Ne	and select the wireles xt".	s network you wa	ant to connect,		
	Scan	Scan aga	in		
	Upstream AP	WiFi_123456			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength
۲	WiFi_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	lie.

If you cannot find the ISP hotspot from the list, ensure that the hotspot is at 5 GHz. Only the WiFi networks at 5 GHz band will be displayed in the list.

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

Quick Setup>>WISP	?
	ame channel, encryption, and encryption algorithm as those of upstream AP.
Upstream AP	WiFi_123456
Upstream AP MAC Address	C8:3A:35:15:86:A1
Channel	165(5825MHz) •
Security Mode	WPA2-PSK •
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Key	
	Previous

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

Quick Setup>>WISP				?
Please select an internet connection and click "Next".	on type, and enter the inte	rnet parameters provic	led by your ISP.	
Internet Connection Type	DHCP (Dynamic IP)	Static IP Address	PPPoE	
PPPoE User Name				
PPPoE Password				
			Previous	Next

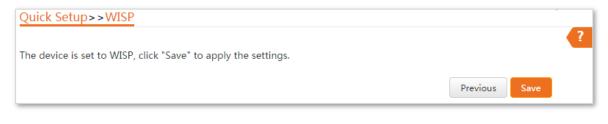
Step 6 Customize the SSID and key, and click **Next**.

Quick Setup>>WISP	?
You can set up your wireless netwo	
Note down your wireless password.	
SSID(WiFi Name)	Marry's WiFi
Channel	165(5825MHz) •
Security Mode	WPA2-PSK V
Encryption Algorithm	AES O TKIP O TKIP&AES
Кеу	••••••
	Previous

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

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

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



----End

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

₽_{TIP}

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

Parameters description

Name	Description
	It specifies the working mode of this device.
Working modes	WISP mode : in this mode, the device connects to an access point provided by ISP in wireless manner.
Upstream AP	It specifies the wireless network name (SSID) of the upstream AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge. If the WiFi network to be bridged has a WiFi password, you need to enter the password manually.
	DHCP (Dynamic IP) : The device obtains IP address and other parameters form the DHCP server of upstream device for internet access.
Internet Connection Type	Static IP Address : The device access the internet by setting the IP address, subnet mask, default gateway and DNS server IP addresses manually.
	PPPoE : The device access the internet using the PPPoE user name and password provided by the ISP.

Example of WISP mode

Network requirement

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

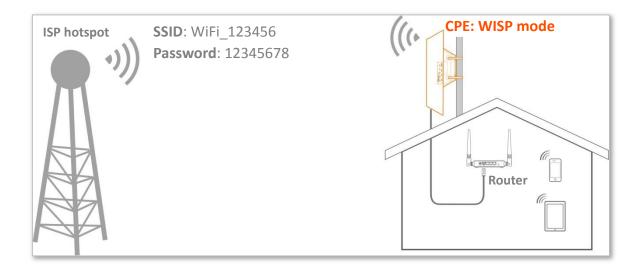
Solution

Set the CPE to WISP mode, and bridge to the ISP hotspot.

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

- SSID: WiFi_123456
- Password: 12345678

Network topology



Configuration procedure

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

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

Step 3 Select the SSID of your ISP (Internet Service Provider) hotspot, which is WiFi_123456 in this example, and click Next.

Quick Setu	p>>WISP					
Click "Scan", a and click "Nex	and select the wireles	s network you wa	ant to connect,			
	Scan	Scan aga	in			
	Upstream AP	WiFi_123456				
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
۲	WiFi_123456	165	C8:3A:35:15:86:A1	WPA2-PSK,AES	110.	

₽

If you cannot find the ISP hotspot from the list, ensure that the hotspot is at 5 GHz. Only the WiFi networks at 5 GHz band will be displayed in the list.

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

Quick Setup>>WISP	2
	me channel, encryption, and encryption algorithm as those of upstream AP.
Upstream AP	
Upstream AP MAC Address	C8:3A:35:15:86:A1
Channel	165(5825MHz)
Security Mode	WPA2-PSK
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Кеу	
	Previous

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

Quick Setup>>WISP			· · · · ·	2
Please select an internet connection and click "Next".	on type, and enter the int	ernet parameters provid	led by your ISP.	
Internet Connection Type	OHCP (Dynamic IP)	Static IP Address	PPPoE	
PPPoE User Name				
PPPoE Password				
			Previous Next	

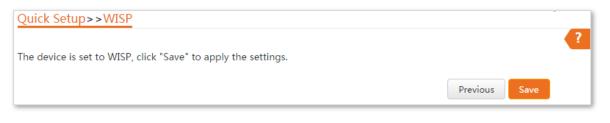
Step 6 Customize the SSID and key, and click **Next**.

Quick Setup>>WISP	2
You can set up your wireless netwo	ork name and wireless password here.
Note down your wireless password	
SSID(WiFi Name)	Marry's WiFi
Channel	165(5825MHz) v
Security Mode	WPA2-PSK V
Encryption Algorithm	● AES
Key	
	Previous

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

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



----End

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

₽

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

Verification

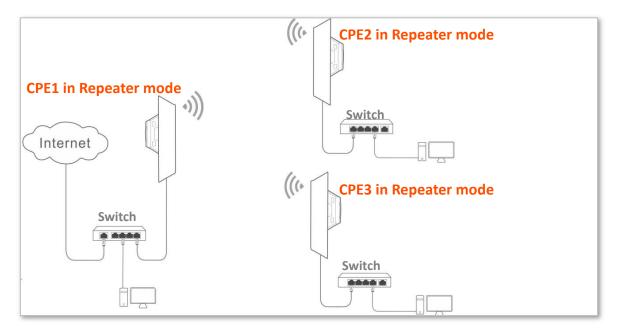
Your wired and wireless devices can connect your router which is connected to the CPE for internet access.

2.6 Repeater mode

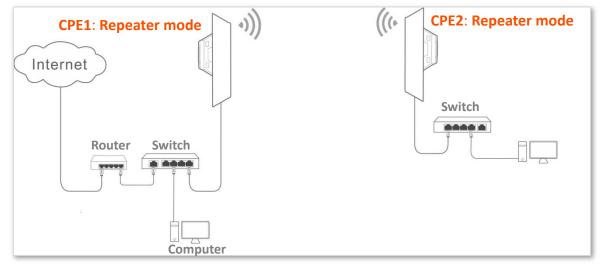
In Repeater mode, this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use this function, the peer AP is required to support WDS function.

Application scenario

Network requirement: You want to combine multiple wired networks into one in wireless manner.



Configuration procedure of one to one bridging



Assume that the wireless parameters of CPE1 are as follows:

- **SSID**: Tenda_123456
- Channel: 165
- Security mode: WEP
- Authentication type: Shared
- Key1 to key4: 12345

- **Step 1** Configure the wireless settings of CPE2.
 - Log in to the web UI of CPE2, and choose Wireless > Basic to enter the configuration page.
 - 2. Change the SSID, which is **Tenda_123** in this example.
 - 3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
 - 4. Set the **Security Mode** to the same as that of CPE1, which is **WEP** in this example.
 - 5. Click Save to apply the settings.

Basic		
Enable Wireless		
Country/Region	China •]
SSID	Tenda_123]
Broadcast SSID	🖲 Enable 🛛 🔘 Disable	
Network Mode	11a/n •]
Channel	165 🔹]
Channel Shift	Enable Isable	
Transmit Power	1dBm 23dBm	D
Channel Bandwidth	20MHz 🔻]
Transmit Rate	Auto]
Security Mode	WEP]

Step 2 Set **CPE2** to the **Repeater** mode.

- **1.** Log in to the web UI of CPE2 and choose **Quick Setup** to enter the configuration page.
- 2. Select the SSID of CPE1, which is **Tenda_123456** in this example, and click **Next**.

Quick S	etup
Select a v	vorking mode:
● AP In	this mode, the device creates a wireless network based on the current wired network.
Client	In this mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
Univer	sal 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 etwork.
Repeat access poi	ter In this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless int.
	In this mode, the device connects to multiple wired networks through wireless bridge, but does not provide ccess point.
Router	connect to modem in wired manner, and provide network access point

3. Select the SSID of CPE1 from the list and click **Next**.

Quick Setu	ip>>Repeater					
Click "Scan".	and select the wireless	s network vou wa	nt to connect.			?
and click "Ne		,	,			
	Scan	C Scan again	n			
Peer AP1 C8:3A:35:15:86:A1						
	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			or enter a MAC			
Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
	Tenda_123456	165	C8:3A:35:15:86:A1	WEP	lite.	

₽

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

4. Set the Authentication Type and Default Key to the same as those of CPE1, enter the key 1, key2, key 3 and key4, and click Next.

Ensure that the device uses the sa	me channel encryption	and	encryption algorith	m as those of	neer AP	
Enter the key of peer AP1, and clic		i, and	eneryption algorith	in us those of	peerval	
	Tenda_123456					
reel Ari	Tenua_125450					
MAC Address of Peer AP1	C8:3A:35:15:86:A1					
Channel	165(5825MHz)	•				
Security Mode	WEP	•				
Authentication Type	Shared	•				
Default Key	Key 1	•				
Delaut Key	Ney I	•				
Key 1	•••••		ASCII •			
Key 2	•••••		ASCII V			
		_				
Key 3	•••••		ASCII V			
Key 4	•••••		ASCII 🔻			

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

Quick Setup>>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	

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

Quick S	etup>>Repeater			
				?
The devi	e is set to Repeater, click "Save" to apply the settings.			
		Previous	Save	
		Frevious	Save	

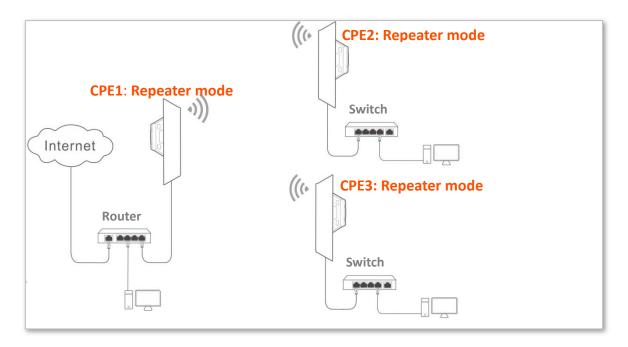
Step 3 Perform the procedure in <u>Step 2</u> above to set **CPE1** to the **Repeater** mode.

----End

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

Name	Description
	It specifies the working mode of this device.
Working modes	Repeater mode: in this mode, the device can connect 2 or more (this device supports 4 at most) wired networks with a wireless link, and can be connected with both wired and wireless clients. To use the Repeater function of this device, the peer AP is required to support WDS function, and use the same radio band as that of this device.
Peer AP	It specifies the wireless network name (SSID) of the peer AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	₽ _{TIP}
	The Repeater mode only supports WEP and None security modes.

Configuration procedure of one to multiple briding



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

- IP Address: 192.168.2.1
- **SSID**: Tenda_123456
- Channel: 165
- Security mode: None
- **Step 1** Configure the wireless settings of CPE2.
 - Log in to the web UI of CPE2, and choose Wireless > Basic to enter the configuration page.
 - 2. Change the SSID, which is **Tenda_1** in this example.
 - 3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
 - 4. Set the **Security Mode** to the same as that of CPE1, which is **None** in this example.
 - 5. Click Save to apply the settings.

Basic			
Enable	Wireless 🚺		
Country	y/Region China	٣	
	SSID Tenda_	1	
Broade	cast SSID 💿 Enabl	e 🔘 Disable	•••
Netwo	ork Mode 11a/n	•	
	Channel 165	•	
Char	nnel Shift 🔘 Enable	e 💿 Disable	
Transm	nit Power	23dBm]
Channel Ba	andwidth 20MHz	•	
Trans	smit Rate Auto	٣	
Secur	ity Mode None	T	

Step 2 Set CPE2 to the **Repeater** mode.

1. Choose Quick Setup, and select Repeater.

Quick Setup
Select a working mode:
◎ AP In this mode, the device creates a wireless network based on the current wired network.
Olient 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

 Select the SSID of CPE1 from the list, which is Tenda_123456 in this example, and click Next.

₽_{TIP}

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

Qu	iick Set	up>>Repeater				-	?
	k "Scan' d click "N	', and select the wireles lext".	s network you wa	ant to connect,			
		Scan	Scan aga	in			
		Peer AP1	C8:3A:35:15:86	:A1			
	Peer AP2 Select an SSID or enter a MAC			or enter a MAC			
		Peer AP3	Select an SSID	or enter a MAC			
		Peer AP4	Select an SSID	or enter a MAC			
s	elect	SSID	Channel	MAC Address	Security Mode	Signal Strength	
		Tenda_123456	165	C8:3A:35:15:86:A1	None	.atl	

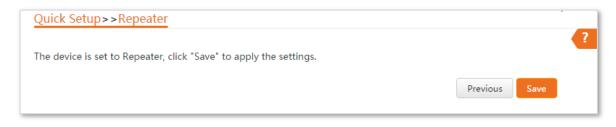
3. Click **Next** directly on the following page.

Quick Setup>>Repeater	
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those of peer AP.
Enter the key of peer AP1, and clic	k "Next".
Peer AP1	Tenda_123456
MAC Address of Peer AP1	C8:3A:35:15:86:A1
Channel	165(5825MHz) •
Security Mode	None •
	Previous

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

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	

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



- Step 3 Perform <u>Step 1</u> and <u>Step 2</u> above to change the wireless settings of CPE3, whose SSID is Tenda_2 in this example, set it to Repeater mode, and bridge to CPE1.
- **Step 4** Set CPE1 to **Repeater** mode and bridge to CPE2 and CPE3.
 - **1.** Log in to the web UI of CPE1, and choose Quick Setup to enter the configuration page.
 - 2. Select Repeater mode, and click Next.
 - 3. Select SSIDs of CPE2 and CPE3, and click Next.
 - 4. Click **Next** at the bottom of the following page.

Qu	uick Se	tup>>Repeater					?
	ck "Scan d click "l	ı", and select the wireles Next".	s network you wa	ant to connect,			
		Scan	Scan aga	in			
Peer AP1			C8:3A:35:15:86	:A1			
		Peer AP2	C8:3A:35:01:80	2:C9			
	Peer AP3		Select an SSID	or enter a MAC			
		Peer AP4	Select an SSID	or enter a MAC			
9	Select	SSID	Channel	MAC Address	Security Mode	Signal Strength	
	✓ Tenda_1		165	C8:3A:35:15:86:A1	None	lin.	
		Tenda_2	165	C8:3A:35:01:8C:C9	None	line.	

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

Quick Setup>>Repeater	
Ensure that the device uses the sa	me channel, encryption, and encryption algorithm as those of peer AP.
Enter the key of peer AP1, and clic	k "Next".
Peer AP1	Tenda_1
MAC Address of Peer AP1	C8:3A:35:15:86:A1
Channel	165(5825MHz) •
Security Mode	None 🔻
	Previous

6. Click Next.

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

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

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

----End

2.7 P2MP mode

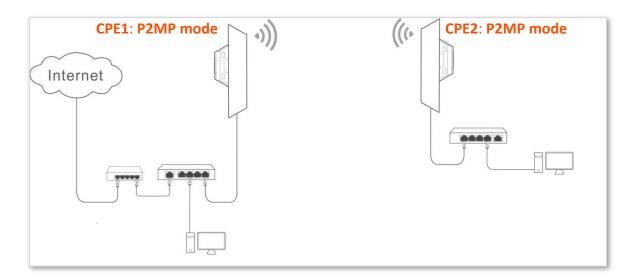
In P2MP mode, this device connects 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients.

₽_{TIP}

The device in P2MP mode can work with the device in Repeater or P2MP mode.

Application scenario

Network requirement: You want to combine two local networks into one in wireless manner.



Configuration procedure

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

- IP Address: 192.168.2.1
- SSID: Tenda_1
- Channel: 165
- Security Mode: None
- **Step 1** Change the wireless settings of CPE2.
 - Log in to the web UI of CPE2, and choose Wireless > Basic to enter the configuration page.
 - 2. Change the SSID, which is Tenda_2 in this example.
 - 3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
 - 4. Set the Security mode to the same as that of CPE1, which is None in this example.
 - 5. Click Save to apply the settings.

isic	
Enable Wireless	
Country/Region	China •
SSID	Tenda_2
Broadcast SSID	Enable
Network Mode	11a/n •
Channel	165(5825MHz)
Channel Shift	Enable Isable
Transmit Power	1dBm 23dBm
Channel Bandwidth	20MHz •
Transmit Rate	Auto •
Security Mode	None 🔻

Step 2 Set CPE2 to **P2MP** mode and bridge to CPE1.

- 1. Choose Quick Setup, select P2MPmode, and click Next.
- 2. Select the SSID of CPE1, which is **Tenda_1** in this example, and click **Next**.

Quick Setup>>	P2MP					?	
Click "Scan", and select the wireless network you want to connect, and click "Next".							
	Scan	C Scan aga	in				
	Peer AP1	C8:3A:35:15:86	5:A1				
	Peer AP2	Select an SSID	or enter a MAC				
	Peer AP3	Select an SSID) or enter a MAC				
Peer AP4		Select an SSIE) or enter a MAC				
Select SSID		Channel	MAC Address	Security Mode	Signal Strength		
₹ T	enda_1	165	C8:3A:35:15:86:A1	None	lin.		

₽_{TIP}

- If you cannot find any SSID from the list, choose Wireless > Basic and enable the wireless function.
 Then try again.
- If you cannot find the SSID of CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1.
- 3. Click **Next** on the following page.

Quick Setup>>P2MP		?
Ensure that the device uses the sa	ne channel, encryption, and encryption algorithm as those of peer AP.	
Enter the key of peer AP1, and clie	k "Next".	
Peer AP1	Tenda_1	
MAC Address of Peer AP1	C8:3A:35:15:86:A1	
Channel	165(5825MHz)	
Security Mode	None •	
	Previous	

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

Quick Setup>>P2MP					
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	

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

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

- **Step 3** Set CPE1 to **P2MP** mode and bridge to CPE2.
 - **1.** Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
 - 2. Select the SSID of CPE2, which is **Tenda_2** in this example, and click **Next**.

Quick Set	up>>P2MP					?
Click "Scan", and click "N	, and select the wireles ext".	s network you w	ant to connect,			
Scan 🥢 <u>Scan again</u>						
	Peer AP1	C8:3A:35:01:80	0:09			
	Peer AP2	Select an SSID) or enter a MAC			
	Peer AP3	Select an SSID or enter a MAC				
	Peer AP4	Select an SSIE) or enter a MAC			
Select SSID		Channel	MAC Address	Security Mode	Signal Strength	
	Tenda_2	165	C8:3A:35:01:8C:C9	None	lite.	

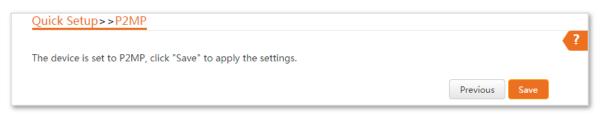
3. Click **Next** on the following page.

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 cli	ck "Next".
Peer AP1	Tenda_2
MAC Address of Peer AP1	C8:3A:35:01:8C:C9
Channel	165(5825MHz)
Security Mode	None •
	Previous

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

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

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



----End

Parameters description

Name	Description
	It specifies the working mode of this device.
Working modes	P2MP mode: in this mode, the device can connect 2 or more (this device supports 4 at most) wired networks with a wireless link, but cannot be connected with wireless clients. P2MP mode is used to achieve communication between multiple offices of an enterprise in a city.
Peer AP	It specifies the wireless network name (SSID) of the peer AP.
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
	It specifies the security mode of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.
Security Mode	⊘ _{TIP}
	The P2MP mode only supports WEP and None security modes.

2.8 Example of repeater mode and P2MP mode

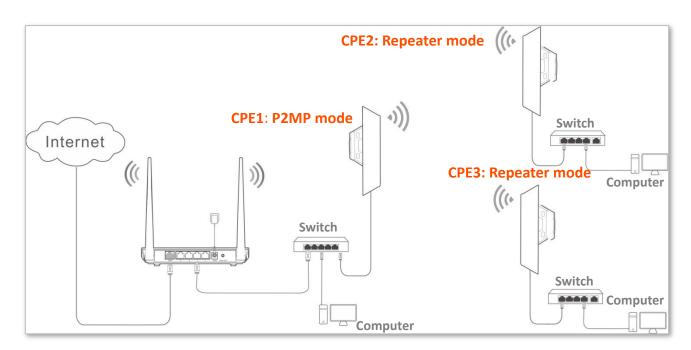
Network requirement

You have three offices which are not far away from each other, and only one office has internet service. Now you want to combine the networks in three offices into one, and provide wireless networks to wireless devices in the offices without internet service.

Solution

Set CPE1 to P2MP mode, and set CPE2 and CPE3 to Repeater mode.

Network typology



Configuration procedure

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

- IP Address: 192.168.2.1
- **SSID**: Tenda_123456
- Channel: 165
- Security mode: None
- **Step 1** Configure the wireless settings of CPE2.
 - Log in to the web UI of CPE2, and choose Wireless > Basic to enter the configuration page.
 - 2. Change the SSID, which is **Tenda_1** in this example.
 - 3. Set the **Channel** to the same as that of CPE1, which is **165** in this example.
 - 4. Set the **Security Mode** to the same as that of CPE1, which is **None** in this example.
 - 5. Click Save to apply the settings.

Basic							
	Enable Wireless						
	Country/Region	China	۲]			
	SSID	Tenda_1]			
	Broadcast SSID	Enable	Disable				
	Network Mode	11a/n	۲]			
	Channel	Auto	۲]			
	Channel Shift	🔘 Enable	Disable				
	Transmit Power	 1dBm	23dBm	n			
Ch	annel Bandwidth	20MHz	۲]			
	Transmit Rate	Auto	۲]			
	Security Mode	None	۲]			

Step 2 Set CPE2 to the **Repeater** mode.

1. Choose **Quick Setup**, and select **Repeater**.

Quick Setup	
Select a workin	g mode:
○ AP In this m	ode, the device creates a wireless network based on the current wired network.
Client In thi	s mode, the device works as a wireless adapter to connect to the wireless network of upstream AP.
Universal Re	peater In this mode, this device extends an existing wireless network for broader network coverage.
• WISP In this wireless network	s mode, this device connects to an access point provided by ISP in wireless manner, and provides the c.
Repeater In access point.	this mode, the device connects to multiple wired networks through wireless bridge, and provides wireless
P2MP In thi wireless access p	s mode, the device connects to multiple wired networks through wireless bridge, but does not provide point.
ORouter conr	nect to modem in wired manner, and provide network access point
	Next

 Select the SSID of CPE1 from the list, which is Tenda_123456 in this example, and click Next.

₽

- If you cannot find any SSID from the list, choose Wireless > Basic and enable the wireless function.
 Then try again.
- If you cannot find the SSID of CPE1 from the list, adjust the direction of CPE2, and move it close to the CPE1.

Quick Setu	Quick Setup>>Repeater ?								
Click "Scan", and select the wireless network you want to connect, and click "Next".									
Scan <u>Scan again</u>									
	Peer AP1	C8:3A:35:15:86	::A1						
	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				
۷	Tenda_123456	165	C8:3A:35:15:86:A1	None	.atl				

3. Click **Next** directly on the following page.

Quick Setup>>Repeater	?
Ensure that the device uses the sa	ne channel, encryption, and encryption algorithm as those of peer AP.
Enter the key of peer AP1, and clic	: "Next".
Peer AP1	Tenda_123456
MAC Address of Peer AP1	C8:3A:35:15:86:A1
Channel	165(5825MHz) •
Security Mode	None •
	Previous

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

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	

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

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

- Step 3 Perform <u>Step 1</u> and <u>Step 2</u> above to change the wireless settings of CPE3, whose SSID is Tenda_2 in this example, set it to Repeater mode, and bridge to CPE1.
- **Step 4** Set CPE1 to **Repeater** mode and bridge to CPE2 and CPE3.
 - **1.** Log in to the web UI of CPE1, and choose **Quick Setup** to enter the configuration page.
 - 2. Select Repeater mode, and click Next.
 - 3. Select SSIDs of CPE2 and CPE3, and click Next.
 - 4. Click **Next** at the bottom of the following page.

Quick Setup>>Repeater							
Click "Scan' and click "N	', and select the wireles lext".	s network you wa	ant to connect,			?	
	Scan	C Scan agai	in				
	Peer AP1	C8:3A:35:15:86	:A1				
	Peer AP2	C8:3A:35:01:8C:C9					
	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	165	C8:3A:35:15:86:A1	None	all.		
	Tenda_2	165	C8:3A:35:01:8C:C9	None	line.		

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

Quick Setup>>Repeater	
Ensure that the device uses the sa	ne channel, encryption, and encryption algorithm as those of peer AP.
Enter the key of peer AP1, and clie	k "Next".
Peer AP1	Tenda_1
MAC Address of Peer AP1	C8:3A:35:15:86:A1
Channel	165(5825MHz) •
Security Mode	None •
	Previous Next

6. Click Next.

Quick Setup>>Repeater				2
Set the IP address to an unused IP	address belonging to the r	network segment of peer AP.		
IP Address	192.168.2.1]		
Subnet Mask	255.255.255.0]		
			Previous	Next

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

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

----End

Verification

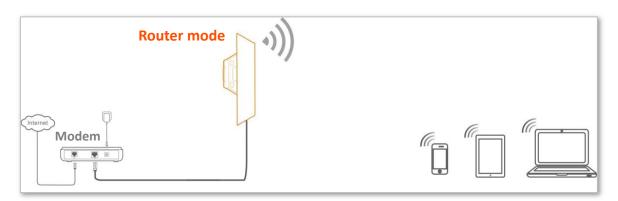
Wired or wireless devices connected to CPE2 and CPE3 can access the internet.

2.9 Router mode

In Router mode, this device serves as a router to provide a wireless network.

Application scenario

Network requirement: You want to use the CPE to provide a wireless network and assign IP addresses to your wireless devices.



Configuration procedure of setting Router mode

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

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

- **Step 4** Set wireless parameters of the CPE.
 - 1. Customize a SSID, which is **Tenda_123456** in this example.
 - 2. Select a security mode, which is **WPA2-PSK** in this example.

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

Quick Setup>>Router		
		?
You can set up your wireless netwo	rk name and wireless password here.	
Note down your wireless password		
SSID	Tenda_123456	
Channel	161(5805MHz)	
Security Mode	WPA2-PSK •	
Encryption Algorithm	● AES ◎ TKIP ◎ TKIP&AES	
Key	•••••	
		Previous Next

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

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

----End

Name	Description	
Working modes	It specifies the working mode of this device. Router mode : in this mode, the PoE/LAN port works as the WAN port and is used to connect to a modem for internet access.	
Internet Connection Type	 The device in Router mode supports three internet connection types: DHCP (Dynamic IP): The device obtains the IP address and other parameters from the DHCP server of upstream device for internet access. Static IP Address: The device accesses the internet using the IP address, subnet mask, default gateway and DNS server IP addresses you manually entered. PPPOE: The device accesses the internet using the PPPoE user name and password provided by the ISP. 	
SSID It specifies the wireless network name of the device.		
Channel	It specifies the operating channel of the WiFi network to be bridged. It will be automatically populated when you select an SSID to bridge.	

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

2.9.2 Example of router mode

Network requirement

You want to use the CPE to server as a wireless router.

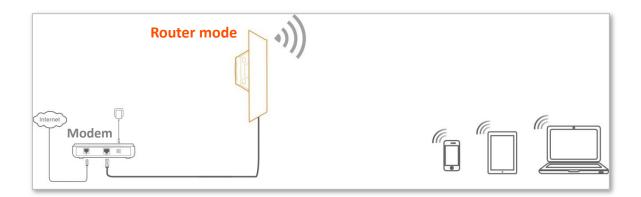
Solution

Set the CPE to Router mode.

Assume that:

- Your internet connection type: **PPPoE**
- User name: admin
- Password: admin

Network typology



Configuration procedure

- **Step 1** Log in to the web UI of the CPE, and choose **Quick Setup** to enter the configuration page.
- **Step 2** Select **Router** mode, and click **Next**.
- **Step 3** Select **PPPoE**, enter **admin** in both **PPPoE User Name** and **PPPoE Password** boxes, and click **Next**.

Quick Setup>>Router	2
Please select an internet connection type, and enter the internet parame and click "Next".	eters provided by your ISP.
Internet Connection Type 💿 DHCP (Dynamic IP) 💿 Static IP	Address
PPPoE User Name admin	
PPPoE Password admin	
	Previous

Step 4 Set wireless parameters of the CPE.

- **1.** Customize a SSID, which is **Tenda_123456** in this example.
- 2. Select a security mode, which is **WPA2-PSK** in this example.
- 3. Set a Key for the wireless network, and click Next.

Quick Setup>>Router	2
You can set up your wireless netwo	ork name and wireless password here.
Note down your wireless password	
SSID	Tenda_123456
Channel	161(5805MHz)
Security Mode	WPA2-PSK T
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
Кеу	••••••
	Previous Next

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

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

----End

Verification

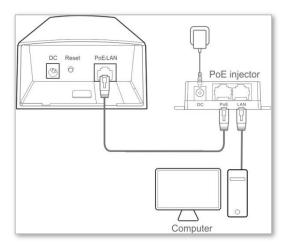
Wireless devices connected to the wireless network of the CPE can access the internet.



3.1 Login

When you log in to the web UI at the first time, follow the steps below:

- **Step 1** Connect the computer to the device.
 - **1.** Uncover the housing of the device.
 - 2. Use an Ethernet cable to connect the **PoE/LAN** port of the device to the **PoE** port of the included PoE injector.
 - **3.** Use the included power adapter to connect the PoE injector to a power source. The **LAN/WAN** LED indicator of the device lights up.
 - 4. Use an Ethernet cable to connect your computer to the LAN port of the PoE injector.



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

8	Default user name: admin
8	Default password: admin
9	English
	Login
	Forget password?

\frown	· ·		
())	_	
¥	TI	P	

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

Then the following page appears.

小 Status	Quick Setup
✤ Quick Setup	Select a working mode:
Metwork	 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.
奈 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	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

When you log in to the web UI after the device is configured, select one of the following situations to perform.

- If you want to log in to the CPE in Client mode (LED1, LED2, and LED3 are blinking) after one-to-one auto-bridge, perform the following procedure.
- **Step 1** Connect the computer to the **PoE/LAN** port of one of the CPEs, or connect to the wireless network using the SSID and password set on the CPE in AP mode.
- **Step 2** Start a web browser on your computer, and visit **192.168.2.2**. Enter your user name and password you set (default: **admin**), and click **Login**.

₽_{TIP}

If you want to log in to the CPEs in client mode (LED1, LED2, and LED3 are blinking) after one-to-multiple bridge, connect the computer to the **PoE/LAN** port of the corresponding CPE you want to log in one by one using an Ethernet cable, and visit **192.168.2.2**.

----End

- If you want to log in to the CPE in Router mode, perform the following procedure.
- **Step 1** Connect the computer to the wireless network using the SSID and password set on the CPE.
- **Step 2** Visit the LAN IP address you set for the CPE.

----End

3.2 Logout

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

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

3.3 Web UI layout

The web UI of the device 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.

*	Status	LAN Setup	Current Mode: AP
4	Quick Setup	MAC Address	C8:3A:35:15:86:A0
	Network	IP Address Type	Static IP Address v
	LAN Setup DHCP Server	IP Address	192.168.2.1
2	DHCP Client	Subnet Mask	255.255.255.0
	VLAN Settings	Default Gateway	0.0.0.0
(iç	Wireless	Primary DNS Server	0.0.0.0
*	Advanced	Secondary DNS Server	0.0.0.0
۵,	Tools	Device Name	O2V1.0
			Save

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

3.4 Common buttons

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

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

4 Status

This module includes three parts: system status, wireless status, and statistics.

4.1 System status

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

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

Status			?
System Status			
Device Name	O2V1.0	LAN Speed	100 Mbps Full-d
Uptime	54 s	LAN IP Address	192.168.2.1
System Time	2019-01-14 11:25:01	Transparent Bridge	Enabled
Firmware Version	V1.0.0.6(3749)	Hardware Version	V1.0
CPU	4%	RAM	79%
LAN MAC Address	50:2B:73:F1:10:A0	WLAN MAC Address	50:2B:73:F1:10:A1

Name	Description
Device Name	It specifies the name of this device. Different device names help you manage multiple devices on LAN easily. You can change the name of this device on the Network > LAN Setup 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	It specifies the time that has elapsed since the device was started last time.
System Time	It specifies the current system time of this device.
Hardware Version	It specifies the hardware version of this device.
RAM	Random Access Memory. It specifies the memory usage of this device.

Name	Description
WLAN MAC Address	It specifies the MAC address of the wireless network of this device.
LAN Speed	It specifies the PoE/LAN port speed and duplex mode of this device.
LAN IP Address	It specifies the IP address (also named management IP address) of this device. By default, it is 192.168.2.1. You can access the web UI of this device using this IP address.
Firmware Version	It specifies the system software version number of this device.
CPU	Central Processing Unit. It specifies the CPU usage of this device.
LAN MAC Address	It specifies the MAC address of LAN port of this device. When connecting to another device using an Ethernet cable, the device uses this MAC address to communicate with the device.

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

Status			?
System Status			-
Device Name	O2V1.0	LAN Speed	100 Mbps Full-d
Uptime	2 h12 m22 s	LAN IP Address	192.168.2.1
System Time	2019-01-14 13:55:59	Connection Type	PPPoE
Firmware Version	V1.0.0.6(3749)	Connection Status	Connected
Hardware Version	V1.0	WAN IP Address	172.20.20.2
CPU	7%	Default Gateway	172.20.20.1
RAM	91%	Primary DNS Server	192.168.60.1
LAN MAC Address	50:2B:73:F1:10:A0	Secondary DNS Server	8.8.8.8
WLAN MAC Address	50:2B:73:F1:10:A1		

Name	Description
Connection Type	It specifies the internet connection type of this device in WISP or Router mode.
Connection Status	It specifies the connection status of WAN port of this device in WISP or Router

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

4.2 Wireless status

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

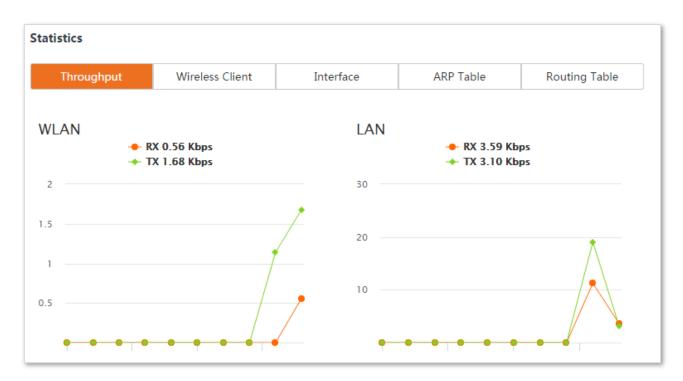
Wireless Status			
Working Mode	AP	AP's MAC Address	50:2B:73:F1:10:A1
SSID	Tenda_F110A0	Signal Strength	N/A
Security Mode	None	Background Noise	-95dBm
Channel/Radio Band	165/5825MHz	TX/RX Link	2X2
Channel Bandwidth	20MHz	Transmit/Receive Speed	N/A
TX Power	23dBm	TD-MAX	Disabled
Wireless Client	0		

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

Name	Description
	interference. For example, -95 dBm indicates less interference than -75 dBm.
TX/RX Link	It specifies the number of spatial streams the device is transmitting or receiving.
Transmit/Receive Speed	It specifies the wireless transmitting/receiving rate.
	In AP or Router mode: it displays the transmitting/receiving rate of the first device connected to the wireless network of this device.
	In Client, Universal Repeater, WISP, Repeater, or P2MP mode: it displays transmitting/receiving rate of this device.
TD-MAX	It specifies the status of the TD-MAX function.

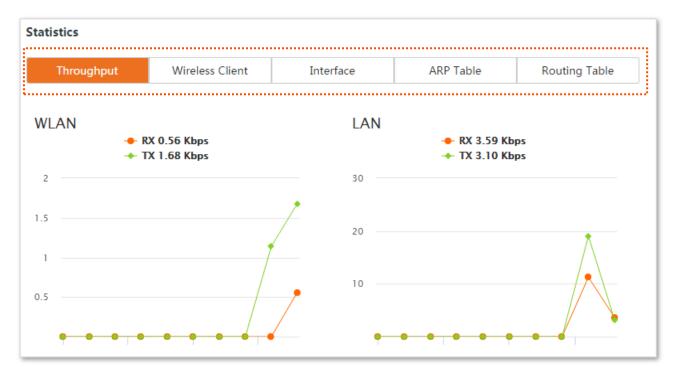
4.3 Statistics

Log in to the web UI of the device, and choose **Status**. You can view statistics information here, including throughput, wireless client, interface, ARP table and routing table.



4.3.1 Throughput

It displays the throughput of WLAN and LAN ports here.



4.3.2 Wireless client

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

atistics						
Throughput	Wireless Client	Interfac	e	ARP Ta	ble	Routing Table
IP Address	MAC Address	Signal/Noise	Transn	nit/Receive	CCQ	Connection Duration
192.168.2.133	1C:5C:F2:B4:40:08	-30/-112dBm	144/	130Mbps	100%	4 s

Parameters description

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

4.3.3 Upstream AP

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

Throughput	Upstream AP	Interface	9	ARP Ta	ble	Routing Table
IP Address	MAC Address	Signal/Noise	Transn	nit/Receive	CCQ	Connection Duration

Parameters description

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

4.3.4 Interface

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

Throu	ghput	Upstream AP	Interface	ARP 1	Table	Routing Table
Interface	IP Address	MAC Address	Received Packets	Receive Error	Transmit Packet	
LAN	192.168.2.1	50:2B:73:F1:10:A0	1046	0	280	0
Bridge	192.168.2.1	50:2B:73:F1:10:A0	1041	0	275	0
WLAN	192.168.11.21	50:2B:73:F1:10:A1	418	0	32	0

Name	Description
Interface	It displays the wired interface, bridge interface, and WLAN interface of the device.
IP Address	It displays the IP addresses of wired interface, bridge interface, and WLAN interface.
MAC Address	It displays the MAC addresses of wired interface, bridge interface, and WLAN interface.
Received Packets	It displays the received and transmitted packets of the interface.

Transmitted Packets

Receive Error

It displays the received and transmitted error packets of the interface.

Transmit Error

4.3.5 ARP table

It specifies the current ARP table of the device.

istics				
Throughput	Upstream AP	Interface	ARP Table	Routing Table
IP Address		MAC Addre	Interface	
192.168.11.1		D8:32:14:4C:CB:70		WLAN
192.168.2.11		C8:9C:DC:60:	54:69	Bridge

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

4.3.6 Routing table

It specifies the destination networks that the device can access.

istics				
Throughput	Upstream AP	Interface	ARP Table	Routing Table
Destination I	Network	Subnet Mask	Next Hop	Interface
0.0.0.0		0.0.0.0	192.168.11.1	WLAN
192.168.2.0		255.255.255.0	0.0.0.0	Bridge
192.168.11.0		255.255.255.0	0.0.0.0	WLAN
239.255.255.250		255.255.255.255	0.0.0.0	Bridge

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



5.1 LAN setup

5.1.1 Overview

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

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

When the CPE is in **AP**, **Client**, **Universal Repeater**, **Repeater**, and **P2MP** modes, the page displays:

LAN Setup	
MAC Addre	ess 50:2B:73:F1:10:A0
IP Address Ty	pe Static IP Address
IP Addre	955 192.168.2.1
Subnet Ma	sk 255.255.255.0
Default Gatew	ay 0.0.0.0
Primary DNS Serv	ver 0.0.0.0
Secondary DNS Serv	0.0.0.0
Device Nan	ne 02V1.0
	Save

Name	Description
MAC Address	It specifies the MAC address of LAN port.
	It specifies the type of obtaining an IP address. The default is Static IP Address.
IP Address Type	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

Name	Description
	gateway and DNS server IP address from the 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 in the network, and use this IP address to log in.
IP Address	It specifies the LAN IP address of the device.
Subnet Mask	It specifies the subnet mask corresponding to the LAN IP address of the device. The default is 255.255.255.0 .
	It specifies the default gateway of the device.
Default Gateway	You can set it to the IP address of the egress router to enable the device to access the internet.
	It specifies the primary DNS server IP address of the device.
Primary DNS Server	If the egress router has the DNS agency function, it can be set to the LAN IP address the egress router. Otherwise, specify a DNS server IP address manually.
Secondary DNS Server	It specifies the secondary DNS server IP address of the device.
Secondary Divis Server	If there are two DNS server IP addresses, enter one in this box.
	It specifies the name of the device. The default name indicates the product 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.

When the CPE is in **WISP** and **Router** modes, the page displays:

50:2B:73:F1:11:00
Static IP Address v
192.168.3.10
255.255.255.0
Save

Name	Description
MAC Address	It specifies the MAC address of LAN port.
IP Address Type	It specifies the type of obtaining an IP address. The default is Static IP Address.

Name	Description
	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.
	₽ _{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 of the upstream device, and use this IP address to log in.
IP Address	It specifies the LAN IP address of the device.
Subnet Mask	It specifies the subnet mask corresponding to the LAN IP address of the device. The default is 255.255.255.0 .

5.1.2 Changing the LAN IP address

Manually setting the IP address

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

Configuration procedure:

- **Step 1** Choose **Network** > **LAN Setup** to enter the configuration page.
- **Step 2** Set **IP Address Type** to **Static IP Address**.
- **Step 3** Set **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**. If another DNS server is available, set **Secondary DNS Server** to the IP address of the additional DNS server.
- **Step 4** Click **Save**.

LAN Setup	
MAC Address	50:2B:73:F1:10:A0
IP Address Type	Static IP Address
IP Address	192.168.2.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.2.4
Device Name	O2V1.0
	Save

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

Note		×
	o confirm to change IP addres changed, please login with ne	
	OK	icel

----End

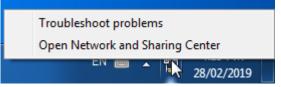
After the configuration, if the new and original IP addresses belong to the same network segment, you can log in to the web UI of the device by accessing the new IP address.

Otherwise, assign your computer an IP address that belongs to the same network segment as the new IP address of the device before login with the new IP address.

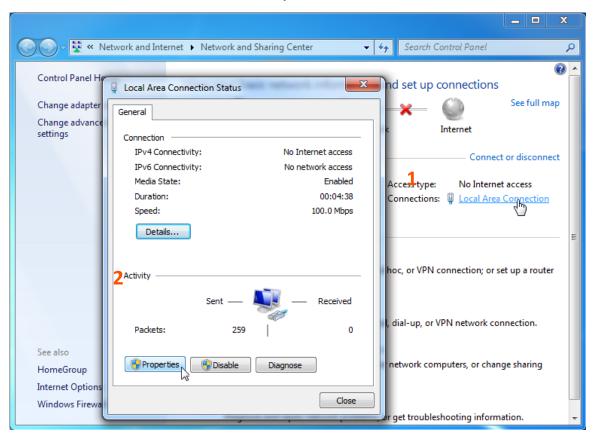
Assume that: the new IP address of the device is **192.168.1.1**, and subnet mask is **255.255.255.0**, then assign an IP address belonging to the same segment.

Configuration procedure (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**.



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



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

Networking Sharing
Connect using:
Intel(R) 82583V Gigabit Network Connection
Configure This connection uses the following items:
 Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 9 (TCP/IPv4)
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 **192.168.1.***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 auton this capability. Otherwise, you need to for the appropriate IP settings.	
Obtain an IP address automatical	y
O Use the following IP address:	
IP address:	192.168.1.20
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	· · ·
Obtain DNS server address autom	natically
Use the following DNS server add	resses:
Preferred DNS server:	
Alternate DNS server:	· · ·
Validate settings upon exit	Advanced
	OK Cancel

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

----End

Automatically obtaining an IP address

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

LAN Setup		
MAC Address	50:2B:73:F1:10:A0	
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	O2V1.0	
	Save	el

----End

After the configuration, if you want to re-log in to the web UI of the device, 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 device belong to the same network segment, and access the IP address of the device. Refer to <u>steps</u> in the **Manually setting the IP address** part to assign an IP address to the computer manually.

5.2 MAC clone

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

5.2.1 Overview

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

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

5.2.2 Cloning a MAC address

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

Method 1

If you can find the computer that can access the internet after it connects to the modem directly, perform the following steps:

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

MAC Clone			?
	MAC Address	50:2B:73:F1:10:A1	_
		IAC Address Restore to Default MAC Address	



Method 2

If you cannot find the computer that can access the internet after it connects to the modem directly, but you know the MAC address of this computer, perform the following steps:

- **Step 1** Connect another device (such as a smart phone or tablet) to the device.
- **Step 2** Log in to the web UI.

- **Step 3** Choose **Network > MAC Clone**.
- **Step 4** Enter the MAC address of the computer that can access the internet in the **MAC Address** box.
- **Step 5** Click **Save**.

MAC Address	50:2B:73:F1	:10:A1		
Clone Local I	MAC Address	Restore to De	efault MAC Address	



₽_{TIP}

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

5.3 DHCP server

5.3.1 Overview

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

₽

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

5.3.2 Configuring the DHCP server

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

DHCP Server		
* DHCP Server		
Start IP Address	192.168.2.100	
End IP Address	192.168.2.200	
Subnet Mask	255.255.255.0	
≭ Gateway Address	192.168.2.1	
* Primary DNS Server	192.168.2.1	
Secondary DNS Server	8.8.4.4	
Lease Time	1 day 🔻	
	Save	əl

----End

₽

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

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

5.4 DHCP client

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

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

DHCP C	lient			
ID	Host Name	IP Address	MAC Address	Lease Time
1	iPhone	192.168.2.133	1C:5C:F2:B4:40:08	23h 59m 44s
10 🔻	Datas/Page 1 data i	n total		

5.5 VLAN settings

5.5.1 Overview

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

5.5.2 Setting up VLAN

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

Step 4 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)
	Save	icel

----End

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

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

The fellowing forms shows the details showt how a	different link type ports address received packets:
The following form shows the defails about how (Different link type ports address received backets:
The following form shows the details about now e	

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

5.5.3 Example of configuring VLAN settings

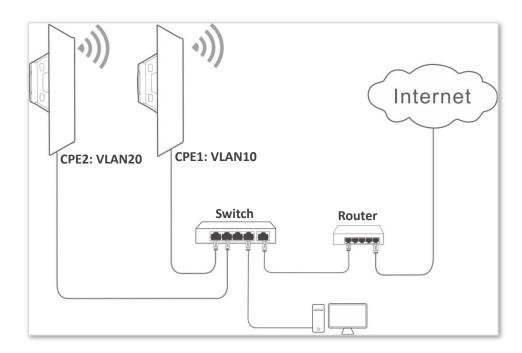
Networking requirement

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

Assumption:

CPE1 belongs to VLAN10, and CPE2 belongs to VLAN20.

Network Topology



The connections of the switch:

The router is connected to the uplink port.

- CPE1 is connected to port 1
- CPE2 is connected to port 2

Configuration procedure

Step 1 Set up CPE1.

- 1. Log in to the web UI of CPE1, and choose Network > VLAN Settings.
- 2. Enable the function.
- 3. Set Management VLAN to 1.
- 4. Set WLAN VLAN ID to 10.
- 5. 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

- 6. Click OK on the pop-up window, and wait until the CPE1 completes reboot.
- **Step 2** Set up CPE2 according to the steps in <u>step 1</u>.
- **Step 3** Set up the switch.

The following table shows the configuration on the switch:

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

Port 2 (Connected to	1,20	Trunk	1
CPE2)			

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

The following form shows the configuration on the router:

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

Refer to the user guide of the router for details.

----End

Verification

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



6.1 Basic

6.1.1 Overview

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

6.1.2 Changing the basic settings

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

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

Basic	
Enable Wireless	?
Country/Region	China •
* SSID	Connect me
Broadcast SSID	Inable Obisable
Network Mode	11a/n •
* Channel	36(5180MHz)
Channel Shift	Enable
Transmit Power	1dBm 23dBm
Channel Bandwidth	20MHz v
Transmit Rate	Auto •
≭ Security Mode	WPA2-PSK
Encryption Algorithm	● AES
Key	······
Key Update Interval	0 s (Range: 60 to 99999, 0 indicates that no key
Isolate Client	update is performed.) © Enable © Disable
Max. Number of Clients	48 (Range: 1 to 128)
	Save

----End

Name	Description
Enable Wireless	It specifies whether to enable the wireless function. By default, it is enabled.
Country/Region	It specifies country or region where this device is located. You can select the country or region to ensure that this device complies with the channel regulations of the country or region.
SSID	It specifies the wireless network name.
	It specifies whether to broadcast the SSID.
Broadcast SSID	When the device broadcasts an SSID, nearby wireless clients can detect the SSID. When this parameter is set to Disable , the device does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the

Name	Description
	SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This to some extent enhances the security of the wireless network.
	It is worth noting that after Broadcast SSID is set to Disable, a hacker can still connect to the corresponding wireless network if he/she manages to obtain the SSID by other means.
	It specifies the wireless network mode of this device. The available options include 11a, 11n, and 11 a/n.
Noture via N de de	11a : It indicates that clients compliant with the 802.11a protocol can connect to the device.
Network Mode	11n : It indicates that clients working at 5 GHz and compliant with 802.11n can connect to the device.
	11 a/n : It indicates that all clients working at 5 GHz and compliant with the 802.11a or 802.11n protocol can connect to the device.
Channel	It specifies channel in which this device operates. Auto indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.
Channel Shift	It specifies the shift of the channel center frequency. With this function enabled, the channel center frequency shifts 5 MHz based on the frequency defined by the IEEE 802.11 standard, so that the device can exchange data on less interference channels.
	It specifies the transmit power of this device.
Transmit Power	Higher number indicates wider WiFi coverage. Setting a proper transmit power helps improve the performance and security of the wireless network.
	It specifies the bandwidth of the operating channel of a wireless network. Change the default setting only when necessary.
	10MHz : It indicates that the channel bandwidth of the device is 10 MHz.
Channel Bandwidth	20MHz : It indicates that the channel bandwidth of the device is 20 MHz.
	30MHz : It indicates that the channel bandwidth of the device is 30 MHz.
	40MHz : It indicates that the channel bandwidth of the device is 40 MHz.
	Auto : It specifies that the device can switch its channel bandwidth among 10MHz, 20 MHz, 30MHz and 40 MHz based on the ambient environment.
	It specifies wireless transmission rate of the device.
Transmit Rate	When the channel bandwidth is set to 10 MHz, the rate automatically reduces, and the maximum rate is 72.2 Mbps.
	When the channel bandwidth is set to 20 MHz, the rate automatically reduces, and the maximum rate is 144.4 Mbps.
	When the channel bandwidth is set to 30 MHz, the rate automatically reduces, and the maximum rate is 216.6 Mbps.

Name	Description	
	When the channel bandwidth is set to 40 MHz, the maximum rate is 300 Mbps.	
	When the channel bandwidth is set to Auto, the maximum rate is 300 Mbps.	
	A wireless network uses radio, which is open to the public, as its data transmission medium. If the wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network. To ensure communication security, transmission links of wireless networks must be encrypted for protection.	
	The device supports various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2.	
	None : It indicates that any wireless client can connect to the wireless network. This option is not recommended because it affects network security.	
	WEP : It uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. Data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum wireless network throughput of only 54 Mbps. Therefore, this security mode is not recommended.	
	WPA-PSK/WPA2-PSK/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.	
Security Mode	WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK adopt a pre-shared key for authentication, while the AP generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.	
	To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate clients and generate data encryption—oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.	
	WPA/WPA2 : WPA and WPA2 uses 802.1x to authenticate clients and the login information of a client is managed by the client. This effectively reduces the probability of information leakage. In addition, each time a client connects to an AP that adopts the WPA or WPA2 security mode, the RADIUS server generates a data encryption key and assigns it to the client. This makes it difficult for attackers to obtain the key. These features of WPA and WPA2 help significantly increase network security, making WPA and WPA2 the preferred security modes of wireless networks that require high security.	
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK, this parameter has the AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter has the AES, TKIP, and TKIP&AES values.	
	AES: It indicates the Advanced Encryption Standard.	
	TKIP : It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum	

Name	Description	
	wireless throughput of the AP is limited to 54 Mbps.	
	TKIP&AES : It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.	
Кеу	It specifies a pre-shared WPA key. It consists of 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.	
Key Update Interval	It specifies interval at which a WPA key is updated. A shorter interval leads to higher security. The value 0 indicates that no key update is performed.	
Isolate Client	This parameter implements a function similar to the VLAN function for wired networks. It isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can access only the wired network connected to the device. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.	
Max. Number of Clients	This parameter specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID. If the number is reached, the wireless network rejects new connection requests from clients. This limit helps balance load among devices.	

None

It indicates that any wireless client can connect to the wireless network. Choose this option only when necessary.

WEP

Authentication Type	Open •	
Default Key	Key 1	
Key 1	12345	ASCII •
Key 2	12345	ASCII V
Key 3	12345	ASCII 🔻
Key 4	12345	ASCII •

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

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

Security Mode	WPA2-PSK •	
Encryption Algorithm	None WEP WPA-PSK WPA2-PSK	IP&AES
Key	Mixed WPA/WPA2-PSK WPA	
Key Update Interval	WPA2	s (Range: 60 to 99999, 0 indicates that no key

Parameters description

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

WPA and WPA2

Security Mode	WPA2-PSK •	
Encryption Algorithm	None WEP WPA-PSK	IP&AES
Key	WPA2-PSK Mixed WPA/WPA2-PSK	
Key Update Interval	WPA WPA2	s (Range: 60 to 99999, 0 indicates that no key

Security Mode	WPA •	
RADIUS Server		
RADIUS Port	1812	
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES	
RADIUS Password	hand.	
Key Update Interval	0 s (Range: 60 to 99999, 0 indicates that no	key
Isolate Client	update is performed.) © Enable © Disable	
Max. Number of Clients	48 (Range: 1 to 128)	

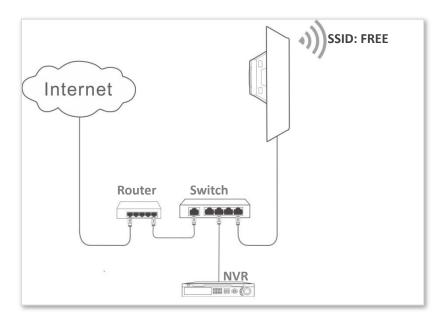
Name	Description
Security Mode	The WPA and WPA2 options are available for network protection with a RADIUS server.
	WPA: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA.
	WPA : It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA.
RADIUS Server	It specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	It specifies the port number of the RADIUS server for client authentication.
RADIUS Password	It specifies the shared password of the RADIUS server.
	It specifies the encryption algorithm corresponding to the selected security mode. The available options include AES , TKIP , and TKIP&AES .
	AES: It indicates the Advanced Encryption Standard.
Encryption Algorithm	TKIP : It indicates the Temporal Key Integrity Protocol.
	TKIP&AES : It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.
	The value 0 indicates that a WAP key is not updated.

6.1.3 Example of configuring basic settings

Setting up a non-encrypted wireless network

Networking requirement

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



Configuration procedure

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

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

* Enable Wireless	
Country/Region	China •
* SSID	FREE
Broadcast SSID	Inable Obsable
Network Mode	11a/n ▼
Channel	36(5180MHz)
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

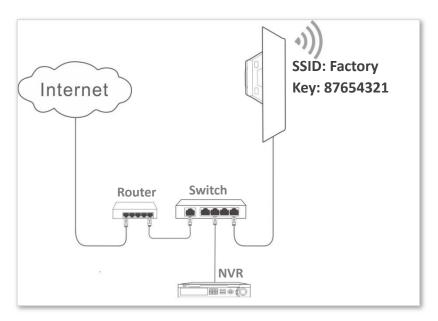
Verification

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

Setting up a wireless network encrypted using WPA2-PSK

Networking requirement

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



Configuration procedure

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

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

Basic	
* Enable Wireless	?
Country/Region	China
* SSID	Factory
Broadcast SSID	Inable Inable
Network Mode	11a/n 🔻
Channel	36(5180MHz) •
Channel Shift	○ Enable ● Disable
Transmit Power	1dBm 23dBm
Channel Bandwidth	20MHz 🔻
Transmit Rate	Auto •
★ Security Mode	WPA2-PSK T
* Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES
* Key	^b ert
Key Update Interval	0 s (Range: 60 to 99999, 0 indicates that no key update is performed.)
Isolate Client Max. Number of Clients	 Enable Disable (Range: 1 to 128)
*	Save

----End

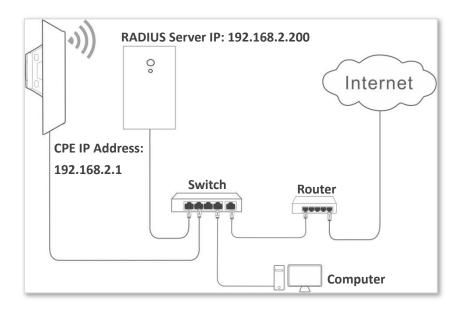
Verification

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

Setting up a wireless network encrypted using WPA or WPA2

Networking requirement

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



Configuration procedure

Configure the device

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

Assume that the second SSID of the AP is used.

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

Basic					
* Enable Wireless		?			
Country/Region	China 🔻				
* SSID	hotspot				
Broadcast SSID	Enable				
Network Mode	11a/n •				
Channel	36(5180MHz) •				
Channel Shift	Enable				
Transmit Power	1dBm 23dBm				
Channel Bandwidth	20MHz 🔻				
Transmit Rate	Auto 🔻				
☆ Security Mode	WPA2 •				
★ RADIUS Server	192.168.0.200				
* RADIUS Port	1812				
* RADIUS Password	12345678 ©				
🜟 Key Update Interval	0	s (Range: 60 to 99999, 0 indicates that no key			
Isolate Client	Enable	update is performed.)			
Max. Number of Clients	48	(Range: 1 to 128)			
* Save Cancel					

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

🐤 Internet Authentie	cation Service			
<u>F</u> ile <u>A</u> ction <u>V</u> iew	<u>H</u> elp			
Internet Authenticati		Frier	ndly Name	Address
RADIUS Clients	New RADIUS <u>C</u> li	ent	There are no iter	ns to show in this view.
Remote Access	Now	•		
🦉 Connection	<u></u>	•		
	Re <u>f</u> resh			
	Export <u>L</u> ist			
	<u>H</u> elp			
		•		Þ
New Client				

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

RADIUS Client			
Name and Address			
Type a friendly name and	either an IP Address or DI	NS name for the	e client.
Eriendly name:	root		
Client address (IP or DNS)			
192.168.2.1			⊻erify
IP address of the C	PE		
	< <u>F</u>	ack <u>N</u>	ext > Cancel

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

Nev	v RADIUS Client	×					
_	Additional Information						
	If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.						
	Client-Vendor:						
	RADIUS Standard						
	Shared secret						
	Confirm shared secret:						
	Equest must contain the Message Authenticator attribute						
	Password same as that specified						
	by RADIUS Password on the CPE.						
	< <u>B</u> ack Finish Cancel						

Step 2 Configure a remote access policy.

Right-click Remote Access Policies and choose New Remote Access Policy.

Internet Authentication S	ervice		_ 0	×
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp				
⇐ ⇒ 🗈 🖬 🔮 🕞	3			
 Internet Authentication Service (Local) ADIUS Clients Remote Access Logging 		Name Connections to Microsoft Routing and Remote A Connections to other access servers	Order 1 2	
Remote Access Policies 	New Remote Access Pol	icy		
	New	•		
	⊻iew			
	Refresh Export <u>L</u> ist			
	<u>H</u> elp			- 1
New Remote Access Policy				

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

Internet Authentication Service File Action New Remote Access Policy V	√izard	
Internet Ar RADIL Remo Remo Conne	Welcome to the New Remote Access Policy Wizard This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server. To continue, click Next.	
🏂 Start 🛛 🚱 🥌 🔹 🗫 Internet Auth	henticati 2, dnsmgmt · [DNS\WIN200	🍇 📵 2:36 PM

5. Enter a policy name and click Next.

New Remote Access	Policy Wizard X			
Policy Configurat The wizard can	ion Method create a typical policy, or you can create a custom policy.			
How do you wan	it to set up this policy?			
Use the w	izard to set up a typical policy for a common scenario			
◯ <u>S</u> et up a c	© Set up a custom policy			
Type a name that	describes this policy.			
Policy name:	root			
E	xample: Authenticate all VPN connections.			
	< <u>B</u> ack <u>N</u> ext > Cancel			

6. Select Ethernet and click Next.

Access Method Policy conditions are based on the metho	d used to gain access to the network.	
Select the method of access for which you	want to create a policy.	
Use for all VPN connections. To crea previous page, and select Set up a c	ate a policy for a specific VPN type, go back to t sustom policy.	he
Dial-up Use for dial-up connections that use Digital Network (ISDN) line.	a traditional phone line or an Integrated Services	s
C Wireless Use for wireless LAN connections on	ıly.	
 Ethernet Use for Ethernet connections, such a 	as connections that use a switch.	
		1

7. Select Group and click Add.

New Remote Access Policy Wizard		×
User or Group Access You can grant access to individual u groups.	users, or you can grant access to selected	ŷ
Grant access based on the following:		
C User User access permissions are specil	fied in the user account.	
Group Individual user permissions override Group name:		įd
		nove
	< <u>B</u> ack <u>N</u> ext> (Cancel

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

elect Groups	?
Select this object type:	
Groups	Object Types
From this location:	
comba.com	Locations
Enter the object names to select (<u>examp</u>	les):
Enter the object names to select (<u>examp</u>	les):

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

		20.
Authentication Methods EAP uses different types of security devic	es to authenticate users.	ſ
Select the EAP type for this policy.		
<u>I</u> ype:		
Protected EAP (PEAP)	•	Configure

10. Click **Finish**. The remote access policy is created.

New Remote Access Policy Wizard		
6	Completing the New Remote Access Policy Wizard	
	You have successfully completed the New Remote Access Policy Wizard. You created the following policy:	
	root	
	Conditions: NAS-Port-Type matches ''Ethernet'' AND VVindows-Groups matches "COMBA\802.1x"	
	Authentication: EAP(Protected EAP (PEAP))	
	Encryption: Basic, Strong, Strongest, No encryption	
	To close this wizard, click Finish.	
	< Back Finish Cancel	

11. 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 <u>conditions</u> : NAS-Port-Type matches "Ethernet" AND Windows-Groups matches "COMBA\802.1x"
A <u>d</u> d <u>E</u> dit <u>R</u> emove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection. Edit <u>P</u> rofile
Unless individual access permissions are specified in the user profile, this policy controls access to the network.
If a connection request matches the specified conditions: Deny remote access permission
Grant remote access permission
OK Cancel Apply

12. Select **Wireless – Other**, click **Add**, and click **OK**.

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

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

it Dial-in Profile		?
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Select the authentication i	methods you want to allow	o for this connection.
	Authentication version <u>2</u> nge password after it has	
	Authentication (MS-CHA) nge password after it has ation (CHAP)	
Unauthenticated acces	ntication (PAP, SPAP)	¹ /
Allow clients to conr method.	nect without negotiating a	n authentication
		- 1
	OK C	ancel <u>Apply</u>

- **14.** When a message appears, click **No**.
- **Step 3** Configure user information. Create a user and add the user to group **802.1x**.

----End

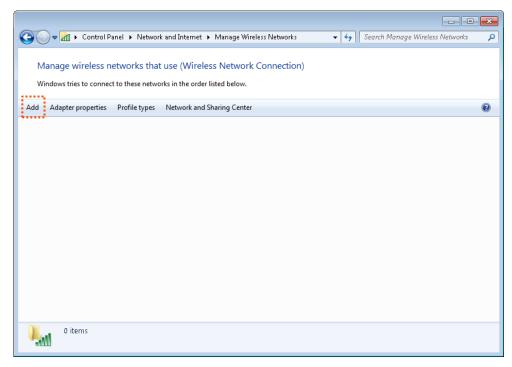
₽

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

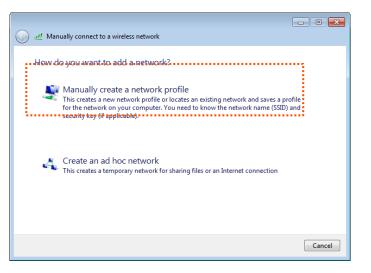
Step 1 Choose **Start > Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.

🚱 🔍 👻 🕨 Control Panel 🕨	Network and Internet 🔸 Network and Sharing Cent	nter 👻 🍫 Search Control Panel 🔎
Control Panel Home Manage wireless networks	View your basic network information	n and set up connections
Change adapter settings Change advanced sharing	ADMIN-PC Netw (This computer)	work 4 Internet
settings	View your active networks	Connect or disconnect
	Network 4 Work network	Access type: No Internet access Connections: U Local Area Connection 5
	Change your networking settings	
	Set up a new connection or network Set up a wireless, broadband, dial-up, a	, ad hoc, or VPN connection; or set up a router or access point.
	Connect to a network Connect or reconnect to a wireless, wir	vired, dial-up, or VPN network connection.
	Choose homegroup and sharing optio Access files and printers located on oth	ions ther network computers, or change sharing settings.
See also	Troubleshoot problems	
HomeGroup	Diagnose and repair network problems	ns, or get troubleshooting information.
Internet Options		
Windows Firewall		

Step 2 Click Add.



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



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

🚱 📶 Manua	lly connect to a v	vireless network	
Enter inf	ormation for	the wireless network you w	vant to add
Network na	ime:	hot_spot	Same as the <u>security mode</u>
Security typ	be:	WPA2-Enterprise 🔹	of the SSID of the AP
Encryption	type:	AES 🔹	
Security Ke	y:		Hide characters
📝 Stari	t this connection	automatically	
		network is not broadcasting t this option, your computer's priva	cy might be at risk.
	5 ,		, ,
			Next Cancel

Step 5 Click **Change connection settings**.

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

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

hot_spot Wireless Netwo	ork Properties 🛛 🗾 🖻	٢.
Connection Security		
Security type:	WPA2-Enterprise	
Encryption type:	AES 🔹	
Choose a network aut Microsoft: Protected Remember my creatime I'm logged on Advanced settings		
	OK Cancel	

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

Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
GlobalSign Root CA
Microsoft Root Authority
Microsoft Root Certificate Authority
Microsoft Root Certificate Authority 2011
Thawte Timestamping CA
۲
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
✓ Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
OK Cancel

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



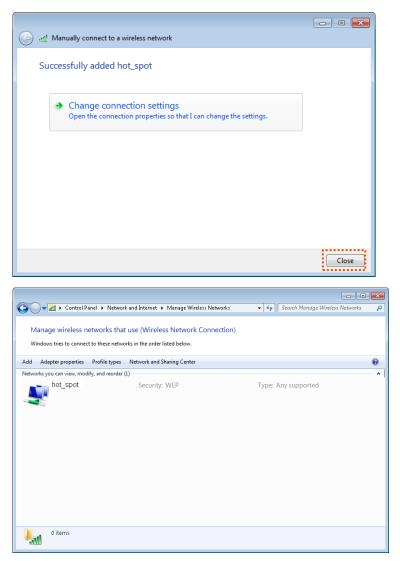
Step 9 Click **Advanced settings**.

hot_spot Wireless Network Properties		
Connection Security		
Security type:	WPA2-Enterprise	
Encryption type:	AES 🗸	
Ch <u>o</u> ose a network aut	······	
Microsoft: Protected	EAP (PEAP)	
Remember my creat time I'm logged on	dentials for this connection each	
Advanced settings		
	OK Car	icel

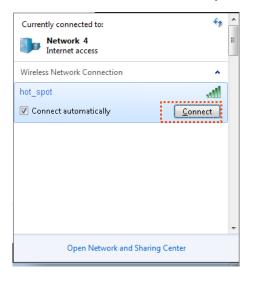
Step 10 Select User or computer authentication and click OK.

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

Step 11 Click Close.



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



Step 13 In the Windows Security dialog box that appears, enter the user name and password set

on the RADIUS server and click **OK**.

Windows Security	×
Network Authentication Please enter user credentials	
	OK Cancel

----End

Verification

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

6.2 Advanced

6.2.1 Overview

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

6.2.2 Changing advanced settings

₽_{TIP}

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

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

Advanced			
WMM	Enable	Disable	
APSD	Enable	Oisable	
Minimum RSSI Threshold	Enable	Oisable	
Preamble	Short Preamble	Iong Preamble	
TD-MAX	Enable	• Disable	
Signal Transmission	Coverage-orientee	d 🔘 Capacity-oriented	
TPC	Enable	Disable	
Signal Reception Level	Auto	Y	
Transmission Distance	3	Auto km (Range: 0.1 to 20, default: 3)	
Beacon Interval	100	ms (Range: 40 to 999, default: 100)	
Fragment Threshold	2346	(Range: 256 to 2346, default: 2346)	
RTS Threshold	2347	(Range: 1 to 2347, default: 2347)	
DTIM Interval	1	(Range: 1 to 255, default: 1)	
Signal LED1 Threshold	-90	dBm (Range: -99 to 0, default: -90)	
Signal LED2 Threshold	-80	dBm (Range: -99 to 0, default: -80)	
Signal LED3 Threshold	-70	dBm (Range: -99 to 0, default: -70)	
	Save	Cancel	

Parameters description

Name	Description
WMM	WMM (Wi-Fi Multi-media) is a wireless QoS protocol making packets with higher priorities are transmitted earlier. This ensures better QoS of voice and video applications over wireless networks. You are recommended to configure the advanced setting instructed by professional.
APSD	It specifies whether to enable the Automatic Power Save Delivery (APSD) mode. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
Minimum RSSI Threshold	It specifies the minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device. If there are multiple devices in a network, setting a proper value helps wireless devices connect to WiF

Name	Description		
	network with better WiFi signal.		
Preamble	It specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the Short Preamble option.		
	TD-MAX is Tenda's proprietary Time Division Multiple Access (TDMA) polling technology. It assigns time slots for each device communication to avoid the "hidden node" problem, which occurs when a node is visible from a wireless AP, but not from other nodes communicating with the originating AP. TD-MAX improves overall performance in Point-to-MultiPoint (PtMP) installations		
TD-MAX	and noisy environments, because it reduces latency, and offers better tolerance against interference. Because of its advantages, TD-MAX also increases the maximum possible number of users that can associate with an AP that uses TD-MAX.		
	EXAMPLE 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 Wi-Fi devices, such as laptops, tablets, or smart phones, to the CPE.		
	It specifies the wall penetrating capability of the device.		
Signal Transmission	Coverage-oriented : With less interference nearby, this mode enables the device to cover wider area.		
	Capacity-oriented : With strong interference nearby, this mode improves the device's anti-interference capability.		
	The Transmit Power Control (TPC) function decreases the TX power of this device automatically to improve the negotiation rate when the two devices are too close		
ТРС	By default, when the received signal strength is greater than -25 dBm, the device decreases its TX power. The received signal strength can be checked on the Status > Wireless Status page.		
Signal Reception Level	It is used to adjust the signal reception level. A higher level leads to better signal reception capability, but lower throughput. Adjust the level based on your actual situation.		
Transmission Distance	It specifies the wireless transmission distance of this device. You can set it based on the actual installation distance.		
Beacon Interval	It specifies the interval at which this device sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.		
Fragment Threshold	It specifies the threshold of a fragment. The unit is byte. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold to enable this		

Name	Description
	device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput. Frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
RTS Threshold	It specifies the frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	It specifies the countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval. For example, if DTIM Interval is set to 1, this device transmits all cached frames at one Beacon interval.
Signal LED1/2/3 Threshold	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.

6.3 Access control

6.3.1 Overview

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

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

6.3.2 Configuring access control

Configuration procedure

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

₽TIP

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

Step 5 Click Save.

Access Cor	ntrol				?
	SSID	Connect me			1
	Access Control				
	Mode	Disallow	Allow		
	MAC Address	12:12:12:12:	12:12	Add Add online devices	
SN	MAC Addre	SS	Status	Operation	
1	12:12:12:12:1	2:12	Enable	Î	
T Access C	Control List	Save	Cancel		

Parameters description

Name	Description		
SSID	It specifies the SSID of this device. With the rule enabled, clients connected to the network with this SSID will be controlled by the rule.		
Access Control	It specifies whether to enable the Access Control function.		
	It 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 WiFi network of the device.		
	Disallow : It indicates that only the wireless clients on the access control list cannot connect to the WiFi network of the device.		

6.3.3 Example of configuring access control

Networking requirement

A wireless network whose SSID is **Connect me** has been set up in a residential community. Only the community members are allowed to connect to the wireless network.

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

Configuration procedure

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

Access Co	Access Control				
	SSID	Connect me			
	Access Control				
	Mode	O Disallow	Allow		
	MAC Address	C8:3A:35:0	0:00:03	Add Add online devices	
SN	MAC Addres	SS	Status	Operation	
1	C8:3A:35:00:0	0:01	Enable	Ē	
2	C8:3A:35:00:0	0:02	Enable	Ē	
3	C8:3A:35:00:0	0:03	Enable	Ē	
		Save	Cancel		

Verification

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



7.1 LAN rate

7.1.1 Overview

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

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

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

LAN Rate	
	?
LAN Speed	Auto Negotiation 🔻
	Save

7.1.2 Changing the LAN speed and duplex mode

Configuration procedure

- **Step 1** Choose **Advanced** > **LAN Rate**.
- **Step 2** Select a LAN speed and duplex mode for each LAN port.

Step 3 Click Save.

LAN Speed Auto Negotiation Auto Negotiation 100Mbps Full-Duplex 100Mbps Half-Duplex 10Mbps Full-Duplex	LAN Rate		
100Mbps Full-Duplex 100Mbps Half-Duplex	LAN Speed		·
		100Mbps Full-Duplex	
			el

----End

Verification

Choose Status and check the changes in System Status part.

			•
System Status			
Device Name	O2V1.0	LAN Speed	100 Mbps Full-d
Uptime	2 h5 m23 s	LAN IP Address	192.168.2.1
System Time	2019-01-15 17:38:53	Connection Type	DHCP (Dynamic IP)
Firmware Version	V1.0.0.6(3749)	Connection Status	Connected
Hardware Version	V1.0	WAN IP Address	192.168.11.21
CPU	9%	Default Gateway	192.168.11.1
RAM	81%	Primary DNS Server	192.168.11.1
LAN MAC Address	50:2B:73:F1:10:A0	Secondary DNS Server	
WLAN MAC Address	50:2B:73:F1:10:A1		

7.2 Diagnose

7.2.1 Overview

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

If the network connection fails, you can use the diagnosis tools for troubleshooting. The device supports the following four tools:

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

7.2.2 Site Survey

Site survey gives you an insight into the information of nearby wireless signals.

Configuration pocedure

- **Step 1** Choose **Advanced** > **Diagnose**.
- **Step 2** Select **Site Survey** in the **Diagnose** drop-down list menu.

----End

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

iagnos	e				
	Diagnose	Site Survey	v		
ID	SSID	MAC Address	Channel	Security	Signal Strength
1	zhangsan	00:B0:C6:60:E0:29	48	WPA2-PSK,AES	.atl
2	psst-ceshi-ew9	50:2B:73:F0:39:D4	40	WPA2-PSK,AES	lin.
3	psst-ceshi-w15e	C8:3A:35:84:2D:C9	48	Mixed WPA/WPA2-PSK	.atl

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

7.2.3 Ping

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

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

Configuration procedure

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

Diagnose		?
Diagnose	Ping •	
IP Address	Manual •	
IP Address/Domain Name	cn.bing.com	
Ping Packet	4	(Range: 1 to 10000)
Packet Size	32	Byte (Range: 1 to 60000)
	Start	

----End

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

IP Address		Time	TTL
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

7.2.4 Traceroute

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

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

Configuration procedure

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

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

----End

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

following figure:

Diagnose		?
	Diagnose Traceroute	
IP Addre	ss/Domain Name cn.bing.co	m
	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	192.168.21.254	1.885 ms 4.249 ms 2.758 ms
5	100.64.0.1	50.352 ms 3.056 ms 3.428 ms
6	202.105.159.149	4.340 ms 8.592 ms 7.126 ms

7.2.5 Speed test

It is used to test the throughput between two Tenda CPEs in the same network. The test requires one of the two devices to be set as a server and the other as a client. The client launches the test request to the server and the server responds to it.

- **Step 1** Choose **Advanced** > **Diagnose** to enter the page.
- **Step 2** Set **Diagnose** to **Speed Test**.
- **Step 3** Set **IP Address of Peer AP** to **Manual**, and enter an IP address in the **IP Address** box. Or select an IP address from the drop-down list. All IP addresses of the devices connected to the CPE are displayed in the list.
- **Step 4** Specify a HTTP port.
- **Step 5** Enter a user name and password of peer CPE.
- **Step 6** Specify the test group.
- **Step 7** Select the test speed direction.
- **Step 8** Specify the time of speed test.

----End

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

Parameters description

Name	Description
IP Address of Peer AP	It specifies the LAN IP address of peer CPE. You can enter it manually or select an IP address from the drop-down list if there are devices 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	It specifies the port number of HTTP service. Default: 80 . You are recommended to keep the default value.
User Name	It specifies the login user name of peer CPE.
Password	It specifies the login password of peer CPE.
Test Group	It specifies the number of test connection launched by the client.
Direction	It specifies the test speed direction. RX (Receive): only test the speed that the peer device transmits data to this device.

Name	Description
	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	It specifies the period of speed test.

Example of configuring the speed test

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

Configuration procedure

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

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

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

Diagno	ose		
	Diagnose	Speed Test	¥
	🕇 AVG RX	👃 AVG TX	🕼 AVG Total
	103.28 Mbps	105.17 Mbps	208.45 Mbps

7.3 Bandwidth control

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

7.3.1 Overview

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

Choose Advanced >	Bandwidth	Control to	o enter the pa	age.
-------------------	-----------	------------	----------------	------

andwidth Control					
Rer	mark				
IP Address Ra	ange 192.168.3.	~ 192.168.3.			
Max. Upload	Rate	Mbps	; •		
Max. Download	Rate	Mbps	; T		
	Add				
		•			
ID Remark IP A	ddress Range	Max. Upload Rate	Max. Download Rate	Status	Action

Configuring bandwidth control

- **Step 1** Choose **Advanced** >**Bandwidth Control**.
- **Step 2** Set related parameters.
- Step 3 Click Add.

Bandwidth Control			?
Remark	Tom's computer		
IP Address Range	192.168.3. 100 ~ 192.168.3	. 100	
Max. Upload Rate	2	Mbps •	
Max. Download Rate	2	Mbps •	
	Add		

Parameters description

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

7.3.2 Example of configuring bandwidth control

Networking requirement

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

Assumption: The maximum upload rate of each device connected to the WiFi network of the device is **5 Mbps**, and download rate is **10 Mbps**. And the IP address range of the devices connected to the WiFi network is **192.168.3.100** to **192.168.3.200**.

Configuration procedure

- **Step 1** Choose **Advanced** > **Bandwidth Control**.
- **Step 2** Enter a remark, such as **Devices of Office1**.
- **Step 3** Specify an IP address range, which are **100** and **200** in this example.
- **Step 4** Specify the maximum upload rate and download rate respectively, which are **5** and **10** in this example.
- Step 5 Click Add.

Bandwidth Control		?
Remark	Devices of Office1	
IP Address Range	192.168.3. 100 ~ 192.168.3	. 200
Max. Upload Rate	5	Mbps •
Max. Download Rate	10	Mbps •
	Add	

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

ID	Remark	IP Address Range	Max. Upload Rate	Max. Download Rate	Status	Action
1	Devices of	192.168.3.100~192.168.3.200	5Mbps	10Mbps	☑ Enable	
10 🔹	Datas/Page	1 data in total				
10 •	Datas/Page	1 data in total				

Verification

For a device whose IP address is within the range of 192.168.3.100 to 192.168.3.200, its maximum upload rate is 5 Mbps and its maximum download rate is 10 Mbps.

7.4 Port forwarding

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

7.4.1 Overview

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

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

Internal IP Address						
Internal IP Address						
Internal Port	23					
External Port	23					
Protocol	TCP&UDP	•				
Application	Telnet	T				
	Add					
Internal IP Address		External Port	Protocol	Application	Status	

7.4.2 Configuring port forwarding

Configuration procedure

- **Step 1** Choose **Advanced** > **Port Forwarding**.
- **Step 2** Enter an IP address in LAN.
- **Step 3** Select an **Application**, and the internal and external ports will be automatically populated.
- **Step 4** Select a protocol.
- Step 5 Click Add.

Port Forwarding						
Internal IP Address	192.168.3.100					
Internal Port	23					
External Port	23					
Protocol	TCP&UDP	T				
Application	Telnet	T				
	Add					
ID Internal IP Address	Internal Port	External Port	Protocol	Application	Status	Action

Parameters description

Name	Description
Internal IP Address	It specifies the IP address of the host that establishes a server in LAN.
Internal Port	It specifies the service port of the server in LAN. A single port is supported.
External Port	It specifies the ports enabled for WAN users by this device.
Protocol	It specifies the protocol type of the selected applications. Select TCP&UDP when you are not sure.
Application	It specifies the application services established in LAN. The device provides some common services. After you select an application, the internal and external ports will be populated.
Action	Click 🔟 to delete the rule.

7.4.3 Example of configuring port forwarding

Networking requirement

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode.

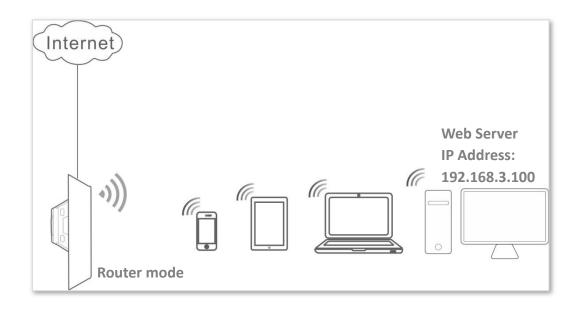
Requirement: Families who are not at home can visit the resources on the web server in LAN over the internet.

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

Assumption:

- IP Address of the web server: 192.168.3.100
- Service port (internal port) of the web server in LAN: 80
- External port that this device enables for internet devices: 80
- WAN IP Address of the device: 202.105.11.22

Network topology



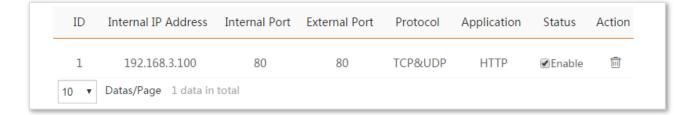
Configuration procedure

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

- **Step 1** Log in to the web UI of the device which works in **Router** mode.
- **Step 2** Choose **Advanced** > **Port Forwarding**.
- **Step 3** Enter the IP address of the web server in the **Internal IP Address** box, which is **192.168.3.100** in this example.
- **Step 4** Select **HTTP** from the drop-down list of **Application**, and the **Internal Port** and **External Port** boxes will be automatically populated.
- **Step 5** Select **TCP&UDP** from the drop-down list of **Protocol**.
- Step 6 Click Add.

Port Forwarding	
Internal IP Address	192.168.3.100
Internal Port	80
External Port	80
Protocol	TCP&UDP •
Application	HTTP •
	Add

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



Verification

Enter **Protocol name**://**WAN port IP address:External port** in the address bar of a web browser on a computer over the internet to access the resources on the web server. In this example, enter **http://202.105.11.22:80**.



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

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

7.5 MAC filter

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

7.5.1 Overview

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

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

The function is disabled by default.

MAC Filter					
	Mode	Disable	•		
		Save			
		Save			

7.5.2 Configuring MAC filter

Configuration procedure

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

MAC Filt	ter					
	Mode	Allow	•			
	Remark					
	MAC Address					
	Time	00 • : 00 • ~ 00	• : 00 •			
	Date			Thur. ry Day		
		Add				
ID	Remark	MAC Address	Time	Mode	Status	Action

Parameters description

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

7.5.3 Example of configuring MAC filter

Network topology

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode.

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

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

Assumption:

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

Configuration procedure

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

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

----End

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

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

Verification

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

7.6 Network service

7.6.1 DDNS

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

Overview

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

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

Choose Advanced > Network Service to enter the page.

Network Service	
DDNS	\bigcirc
Service Provider	3322.org
User Name	
Password	
Domain Name	

Configuring DDNS

Configuration procedure

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

Network Service		
DDNS		
Service Provider	Dyndns •	Register
User Name	admin	
Password	•••••	
Domain Name	tenda.dyndns.com	

Parameters description

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

Example of configuring DDNS

Networking requirement

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode. The WAN IP address of the device is dynamic.

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

Assumption:

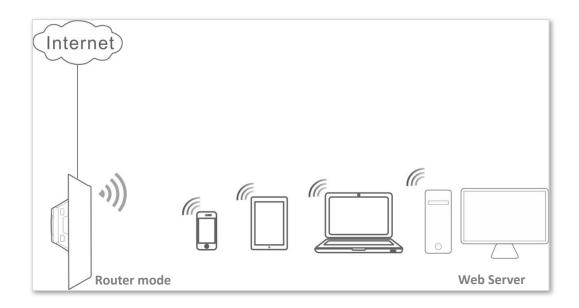
The information of the web server in LAN is shown as follows:

- **IP Address**: 192.168.3.100
- Service Port of the Web Server: 80

The registered domain name information is shown as follows:

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

Network topology



Configuration procedure

Step 1 Set up the DDNS function.

- **1.** Log in to the web UI of the device which works in Router mode.
- 2. Choose Advanced > Network Service.
- 3. Enable the **DDNS** function.
- 4. Select a service provider, which is **Dyndns** in this example.
- 5. Enter the user name and password you registered with DDNS service provider, which are **tenda** and **tenda** in this example.
- 6. Enter the domain name you registered, which is **tenda.dyndns.com**.
- 7. Click **Save** on the bottom of this page.

DDNS		
Service Provider	Dyndns •	<u>Register</u>
User Name	tenda	
Password	•••••	
Domain Name	tenda.dyndns.com	

Step 2 Set up the port forwarding function.

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

- **1.** Choose **Advanced** > **Port Forwarding**.
- 2. Enter the IP address of the web server, which is **192.168.3.100** in this example.
- **3.** Select an application, which is **HTTP** in this example, and the Internal Port and External Port will be populated automatically.
- **4.** Select the protocol of the service. **TCP&UDP** is recommended if you are not sure.
- 5. Click Add.

Port Forwarding		
Internal IP Address	192.168.3.100	
Internal Port	80	
External Port	80	
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	192.168.3.100	80	80	TCP&UDP	HTTP	✓Enable	
[10 🔻	Datas/Page 1 data in	total					

Verification

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

₽_{TIP}

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

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

7.6.2 Remote web management

Overview

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

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

Configuring remote web management

Configuration procedure

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

Remote Web Management		
IP Address	All]
Port	8080]

----End

Parameters description

Name	Description
Remote Web Management	It specifies whether to enable the remote web management function.
	It specifies the IP address of a device which is allowed to access the web UI of the device.
IP Address	All : It indicates that any computer in WAN can manage this device remotely. Select this option only when necessary.
	Manual : It indicates that only the device with specified IP address can manage this device remotely. If this device belongs to a LAN, the gateway address (a public IP address) of the device should be entered.
Port	It specifies the port number used for remote management of device. Default: 8080 . You can change it if necessary.

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

Example of configuring remote web management

Networking requirement

The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode.

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

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

Assumption:

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

Configuration procedure

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

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

----End

Verification

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

7.6.3 Reboot schedule

Overview

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

Configuration procedure

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

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



7.6.4 Login timeout interval

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

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

Login Timeout Interval	5	min Range: 1-60 minutes

7.6.5 SNMP agent

Overview

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

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

SNMP Management Framework

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

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

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

Basic SNMP Operations

The device allows the following basic SNMP operations:

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

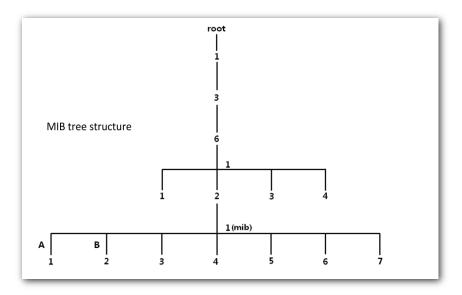
SNMP Protocol Version

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

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

MIB Introduction

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



Configuring the SNMP agent function

Configuration procedure

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

SNMP Agent	
Device Name	O2V1.0
Read Community	public
Read/Write Community	private
Location	ShenZhen

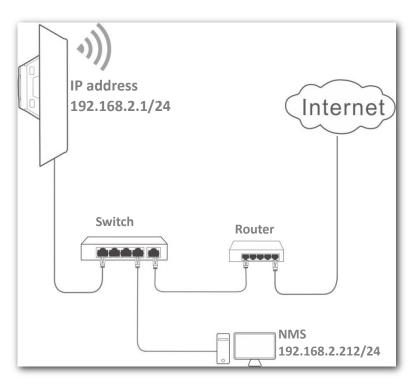
Parameters description

Name	Description
	It specifies whether to enable the SNMP agent function of the AP. 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 device supports SNMP V1 and SNMP V2C.
	It specifies the device name of the device. The default device name is the model and version number of the device. For example, the default name of this device is O2V1.0
Device Name	₽ _{TIP}
	It is recommended that you change the device name so that you can easily identify the device when managing it using SNMP.
Deed Community	It 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 password to read variables in the MIB of the device.
Read/Write Community	It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is private.
Ready write Community	The SNMP agent function of the device allows an SNMP manager to use the password to read/write variables in the MIB of the device.
Location	It specifies the location where the device is used. You can change the location as required.

Example of configuring the SNMP function

Networking requirement

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



Configuration procedure

Step 1 Set up the device.

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

- 1. Choose Advanced > Network Service.
- 2. Enable the SNMP Agent function.
- 3. Set the **Read Community**, which is **Jack** in this example.
- 4. Set **Read/Write Community**, which is **Jack123** in this example.
- 5. Click **Save** on the bottom of this page.

SNMP Agent		
Device Name	O2V1.0	
Read Community	Jack	
Read/Write Community	Jack123	
Location	ShenZhen	

Step 2 Set up the NMS.

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

----End

Verification

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

7.6.6 Ping watch dog

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

Configuring ping watch dog

Configuration procedure

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

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

Parameters description

Name	Description
Ping Watch Dog	It specifies whether to enable the Ping Watch Dog function.
IP Address	It specifies the target IP address that the device pings.
Ping Interval	It specifies the interval at which the device transmits packets to ping the target IP address.
Ping Startup Delay	It specifies the delay time for the device to enable the Ping Watch Dog function after the device completes startup.
Threshold of Lost Packets	It specifies the threshold of lost packet that triggers reboot. Range: 1 to 65535, default: 3.
	For example, if 5 is set, the device will reboot automatically when it sends 5 Ping packets to target IP address/domain name, and does not receive response.

7.6.7 DMZ host

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

Overview

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

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

Configuring DMZ host

Configuration procedure

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

DMZ Host	
DMZ Host IP Address	

----End

Example of configuring DMZ host

Networking requirement

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

Requirement: The administrator on business can visit the resources on web server in LAN. You can use DMZ Host function to solve the problem.

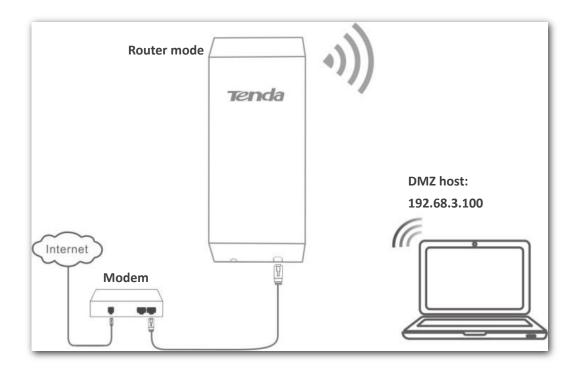
Assumption:

The WAN IP address of the device is **202.105.106.55**. The information of the internal web server is shown as follows:

IP Address: 192.168.3.100

Service Port of the Web Server: 80

Network topology



Configuration procedure

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

- **Step 1** Choose **Advanced** > **Network Service**.
- **Step 2** Enable the **DMZ Host** function.
- **Step 3** Enter the IP address of the computer to be set to DMZ host, which is **192.168.3.100** in this example.
- **Step 4** Click **Save** on the bottom of this page.

DMZ Host	
DMZ Host IP Address	192.168.3.100

----End

Verification

Enter **Protocol name**://**WAN port IP address**:**port number** in the address bar of a web browser on a computer over the internet to access the resources on the web server. In this example, enter **http://202.105.106.55:80**.

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

₽

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

- Ensure that the WAN IP address of the device is a public IP address.
- Security software, antivirus software, and the built-in OS firewall of the computer may cause the function failures. Disable them and try again.

7.6.8 Telnet service

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

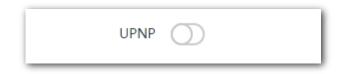
Choose **Advanced** > **Network Service** to enter the page. By default, the function is enabled.



7.6.9 UPnP

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

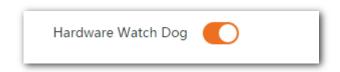
Choose **Advanced** > **Network Service** to enter this page. By default, the function is disabled.



7.6.10 Hardware watch dog

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

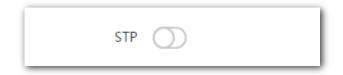
Choose **Advanced** > **Network Service** to enter the page. By default, the function is enabled.



7.6.11 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 inability of processing packets caused by receiving duplicate packets.

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





8.1 Date & time

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

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

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

Date & Time	2
Time Settings	Synchronized with the Internet Manual
Time Interval	30 minutes v
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei 🔹
	Save

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

Synchronized with the Internet

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

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

Configuration procedure

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

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

----End

Manual

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

Configuration procedure

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

Date & Time		2
	Time Settings	Synchronized with the Internet Nanual
	Date & Time	2019 Y 01 M 16 D 14 h 51 m 26 s
		Synchronize with PC Time
		Save Cancel

8.2 Maintenance

8.2.1 Reboot device

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

₽

When the device reboots, the current connections will be disconnected. Perform this operation when the device does not work busy.

Configuration procedure

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

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

Note		\times
Do you want to reb	oot it?	
ОК	Cancel]

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

8.2.2 Reset to factory settings

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

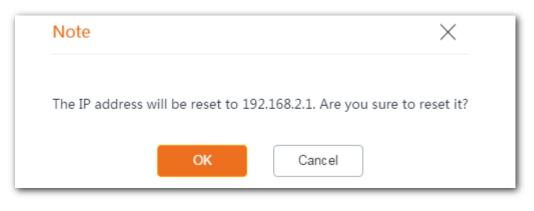
- When the factory settings are restored, the configuration of the device is lost. Therefore, you need to reconfigure the device to connect to the internet. Restore the factory settings of the device only when necessary.
- To prevent device damages, ensure that the power supply of the device is normal when the device is reset.
- When the factory settings are restored, the login IP address is 192.168.2.1, and both login user name and password are **admin**.

Configuration procedure

- **Step 1** Choose **Tools > Maintenance**.
- Step 2 Click Reset.

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

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



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

8.2.3 Upgrade firmware

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

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

Configuration procedure

- **Step 1** Download the package of a later firmware version for the device from <u>http://www.tendacn.com</u> to your local computer, and decompress the package.
- **Step 2** Log in to the web UI of the device and choose **Tools** > **Maintenance**.
- Step 3 Click Upgrade.



Step 4 Select the file from your local computer for upgrading the firmware.

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

----End

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

8.2.4 Backup/restore

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

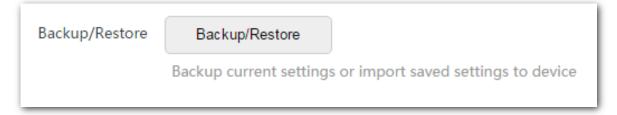
If the device enters the optimal condition after you greatly change the configuration of the device, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the device.

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

Configuration Proceudre

- **Step 1** Choose **Tools > Maintenance**.
- Step 2 Click Backup/Restore.



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

Backup/Restore		×
Backup configurations	Backup	
Import configurations	Restore	

----End

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

Restore

Configuration procedure

- **Step 1** Choose **Tools > Maintenance**.
- **Step 2** Click **Backup/Restore**.

Step 3 Click Restore on the pop-up window.

	X
Backup	
Restore	

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

----End

The file is being uploaded.

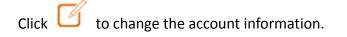
Backup/Restore		×
Backup configurations	Backup	
Import configurations	Uploading	

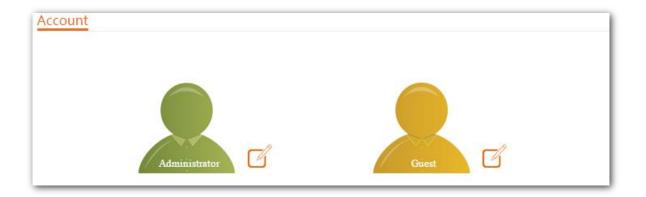
A progress bar is displayed on the page. Wait for it to elapse. Then the device is restored the settings successfully.

8.3 Account

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

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





8.3.1 Administrator

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

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

8.3.2 Guest

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

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

Parameters description

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

8.4 System log

To access the page, choose **Tools** > **System Log**. The maximum of 300 items can be saved. After the total log items exceed the maximum number, the previous logs will be cleared.

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

System Lo	<u>g</u>		
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 device. You can correct the system time of the device by choosing **Tools** > **Date & Time**.

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

- 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.

Appendix

A.1 FAQ

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

Try the following methods:

- Ensure that the device has been connected to the power supply and the computer properly.
- Ensure that the IP address of the login computer is 192.168.2.X (X ranges from 2 to 254).
- If the CPE has performed one-to-one bridge, its IP address is changed to 192.168.2.2. Visit the new IP address for login.
- If the CPE is set to Router mode, the PoE/LAN port is changed to a WAN port. You need to connect to the wireless network of the CPE, and visit its LAN IP address for login.
- Restore the device to factory settings.

Q2: How to reset the device to factory settings?

Note: Resetting the device clears all settings, and you need to configure it again.

- Method One: 1 minute after the device is powered on, remove the cover of the device, and hold down the Reset button for about 8 seconds. When all LED indicators light up once, the device is restored to factory settings.
- Method Two: Log in to the web UI of the device, choose Tools > Maintenance, and click the Reset button.

Q3: How to determine whether the signal strength LED indicators are optimal when the devices are used for CCTV surveillance?

- **Option One**: Observe the LED indicators of the devices. The bridging signal is optimum when all of the LED1, LED2 and LED3 indicators are solid on or blinking.
- Option Two: Log in to the web UI of one device, choose Status, and check the Wireless Status on the following page:

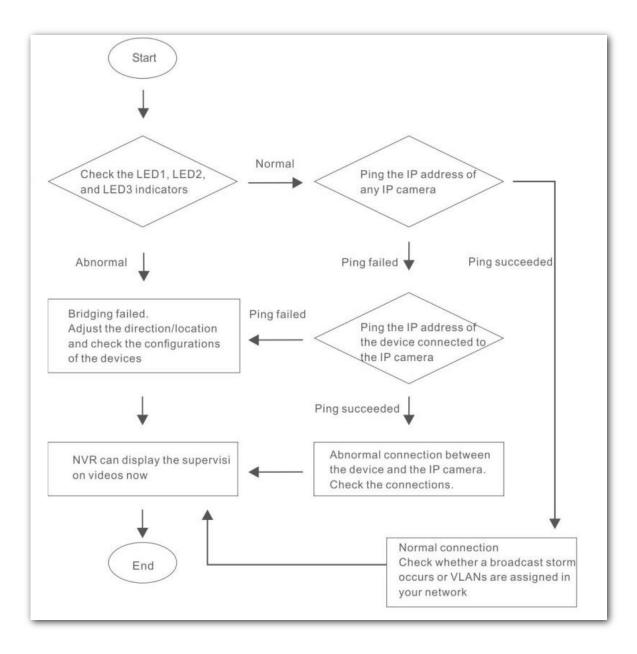
Wireless Status			
Working Mode	Client	AP's MAC Address	00:90:4C:88:88:91
SSID	N/A	Signal Strength	-65dBm
Security Mode	N/A	Background Noise	-116dBm
Channel/Radio Band	157/5785MHz	TX/RX Link	3X3
Channel Bandwidth	40MHz	Transmit/Receive Speed	216Mbps/216Mbp
TX Power	23dBm	TD-MAX	Disabled
Wireless Client	N/A		

Stronger signal strength (-60 is better than -70) and less background noise (-100 is better than -90) lead to better bridging signal.

Q4: After the installation succeeds, the IP cameras connected to the NVR cannot display the surveillance videos. What should I do?

Try the following solutions:

- Ensure that all devices are working normally, and connected properly.
- Refer to the following figure to find the problem. Ensure that the IP addresses of computer, NVR, and IP cameras are in the same network segment.



A.2 Default parameters

By default, the parameters are shown in the following table:

Parameters			02
	Login IP Address		192.168.2.1
Login	Account	Administrator	admin/admin
		Guest	Disabled
Quick Setup	Working Mode		AP mode
	IP Address Type		Static IP address
	IP Address		192.168.2.1
	Subnet Mask		255.255.255.0
LAN Setup	Default Gateway		0.0.0.0
	Primary DNS Server		0.0.0.0
	Secondary DNS Server		0.0.0.0
	Device Name		O2V1.0
	DHCP Server		Enable
	Start IP Address		192.168.2.100
	End IP Address		192.168.2.200
DHCP Server	Subnet Mask		255.255.255.0
Difer Server	Gateway Address		192.168.2.254
	Primary DNS Server		8.8.8.8
	Secondary DNS Server		8.8.4.4
	Lease Time		1 day
	VLAN Settings		Disable
VLAN Settings	PVID		1
	Management VLAN		1
	WLAN		1000
Wireless-Basic	c Wireless Network		Enable

Parameters		02	
	Country/Region	China	
	SSID	Tenda_XXXXXX, and XXXXXX is the last LAN MAC address of the device	t six characters of the
	Broadcast SSID	Enable	
	Network Mode	11a/n	
	Channel	Auto	
	Channel Shift	Disable	
	Transmit Power	23 dBm	
	Channel Bandwidth	20 MHz	
	Transmit Rate	Auto	
	Security Mode	None	
	Isolate Client	Disable	
	Max. Number of Clients	48	
	WMM	Enable	
	APSD	Disable	
	Minimum RSSI Threshold	Disable	
	Preamble	Long Preamble	
	Transparent Bridge	Enable	
	TD-MAX	Disable	
Wireless-Advanced	Signal Transmission	Coverage-oriented	
	ТРС	Enable	
	Signal Reception Level	Auto	
	Transmission Distance	3 km	
	Beacon Interval	100ms	
	Fragment Threshold	2346	
	RTS Threshold	2347	
	DTIM Interval	1 1	

Parameters		02	
	Signal LED1 Threshold	-90 dBm	
	Signal LED2 Threshold	-80 dBm	
	Signal LED3 Threshold	-70 dBm	
Wireless –Access C	ontrol	Disable	
LAN Rate		Auto Negotiation	
Diagnose		Disable	
	Reboot Schedule	Disable	
	Login Timeout Interval	5 min	
	SNMP Agent	Disable	
Network Service	Ping Watch Dog	Disable	
Network Service	Telnet Service	Enable	
	UPnP	Disable	
	Hardware Watch Dog	Enable	
	STP	Disable	
Tools	Date & Time	Synchronized with the Internet (GTM+8:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei Time Interval: 30 minutes	