300Mbps Wireless N Access Point

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

This user guide applies to the following access points: AP4 and AP5. AP4 is used for illustrations here unless otherwise specified. The contained images and UI screenshots are subject to the actual products.

Product model	Description
AP4	300Mbps Wireless N Access Point
AP5	300Mbps Wireless N Access Point

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	“ ”	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
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
AES	Advanced Encryption Standard
CCQ	Client Connection Quality
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DDNS	Dynamic Domain Name Server
DTIM	Delivery Traffic Indication Message
GMT	Greenwich Mean Time
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
OS	Operating System
PoE	Power Over Ethernet
PVID	Port-based VLAN ID
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RSSI	Received Signal Strength Indicator
RX	Receive
SSID	Service Set Identifier
TCP	Transmission Control Protocol

Acronym or Abbreviation	Full Spelling
TKIP	Temporal Key Integrity Protocol
TX	Transmit
UDP	User Datagram Protocol
UI	User Interface
VID	Virtual Local Area Network Identification
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Networks
WMM	Wi-Fi multi-media
WPA-PSK	WPA-Preshared Key
WPA	Wi-Fi Protected Access

Getting more documents

If you want to get more documents of the device, visit www.tendacn.com and search for the corresponding product model. The related documents are listed as below:

Document	Description
Quick Installation Guide	It introduces how to set up the device quickly for internet access, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on.
User Guide	It introduces how to set up more functions of the device for more requirements, including all functions on the web UI of the device.
Data Sheet	It introduces the basic information of the device, including product overview, selling points, and specifications.

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.

Hotline

Global: (86) 755-27657180

Toll Free: Mon - Fri 9 am - 6 pm (China Time Zone)

United States: 1-800-570-5892

Toll Free: Daily-9am to 6pm PST

Canada: 1-888-998-8966

Toll Free: Mon - Fri 9 am - 6 pm PST

Hong Kong: 00852-81931998

Toll Free: Mon - Fri 9 am - 6 pm (China Time Zone)

Email

support@tenda.com.cn

Contents

1 Login 1

1.1 Login 1

1.2 Logout 3

2 Web UI 4

2.1 Web UI layout 4

2.2 Common buttons 5

3 Status 6

3.1 System status 6

3.2 Wireless status 9

3.3 Statistics 11

4 Quick setup 16

4.1 AP mode 16

4.2 Client mode 22

4.3 Universal repeater mode 29

4.4 WISP mode 38

4.5 Client + AP mode 46

4.6 Router mode 53

5 Network 59

5.1 LAN setup 59

5.2 MAC clone 66

5.3 DHCP server 68

5.4 DHCP client 70

5.5 VLAN settings 71

6 Wireless 76

6.1 Basic 76

6.2 Advanced 88

6.3 Access control 91

7 Advanced 94

7.1 LAN rate 94

7.2 Diagnose 95

7.3 Bandwidth control 99

7.4 Port forwarding 103

7.5 MAC filter 108

7.6 Network service 112

8 Tools 124

8.1 Date & time 124

8.2 Maintenance 126

8.3 Account 131

8.4 System log 132

Appendix 133

Default parameters 133

1 Login

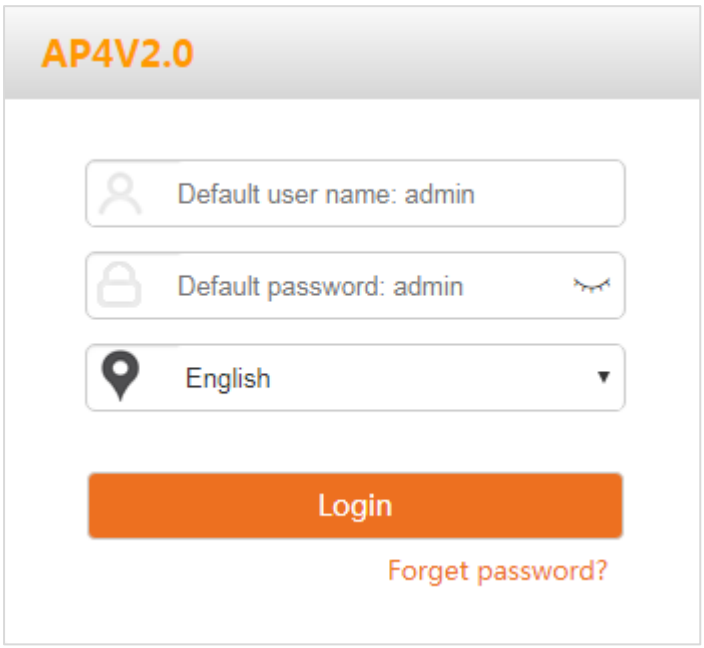
1.1 Login

The login methods for the AP in different modes are different. Select one of the following situations to perform.

- **When you log in to the web UI at the first time or after the AP is reset to factory settings, follow the steps below:**

Step 1 Connect a computer to the LAN1 port of the AP using an Ethernet cable, and power it on using the included power adapter.

Step 2 Start a web browser on the computer, and visit **192.168.0.254**. Enter your user name and password (both are **admin** by default), and click **Login**.

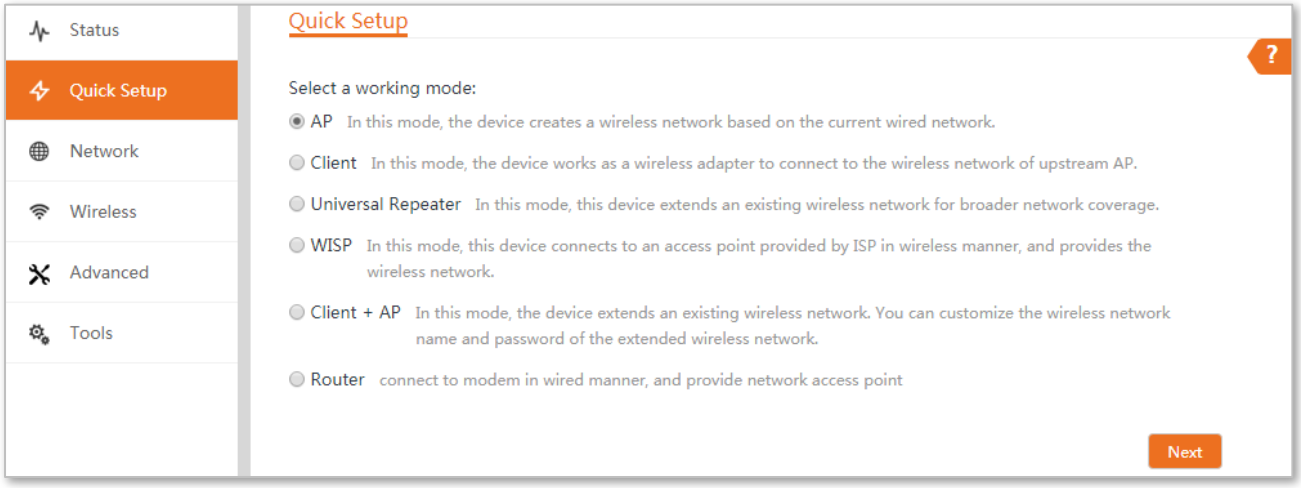


----End

TIP

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

The following page appears.



- **If you want to log in to the AP in AP mode, perform the following procedure.**

Step 1 Connect a computer to the LAN1 port of the AP using an Ethernet cable.

Step 2 Set the IP address of the computer to **192.168.0.*X*** (*X* ranges from 1 to 253), and subnet mask to **255.255.255.0**.

Step 3 Start a web browser on the computer, and visit **192.168.0.254**. Enter your user name and password you set, and click **Login**.

----End

- **If you want to log in to the AP in Client mode, Universal Repeater mode, or Client + AP mode, perform the following procedure.**

Step 1 Connect a computer to the LAN1 port of the AP using an Ethernet cable.

Step 2 Start a web browser on the computer, and visit the IP address of the AP you set before. Enter your user name and password you set, and click **Login**.

TIP

If you forget the IP address you set for the AP, you can log in to the web UI of the upstream AP and check its DHCP client list.

----End

- **If you want to log in to the AP in Router mode or WISP mode, perform the following procedure.**

Step 1 Connect a computer to the LAN1 port of the AP using an Ethernet cable.

Step 2 Start a web browser on the computer, and visit the IP address of the AP you set before. Enter your user name and password you set, and click **Login**.

TIP

If you forget the IP address you set for the AP, you check the gateway IP address of the computer, and use this IP address for login.

----End

1.2 Logout

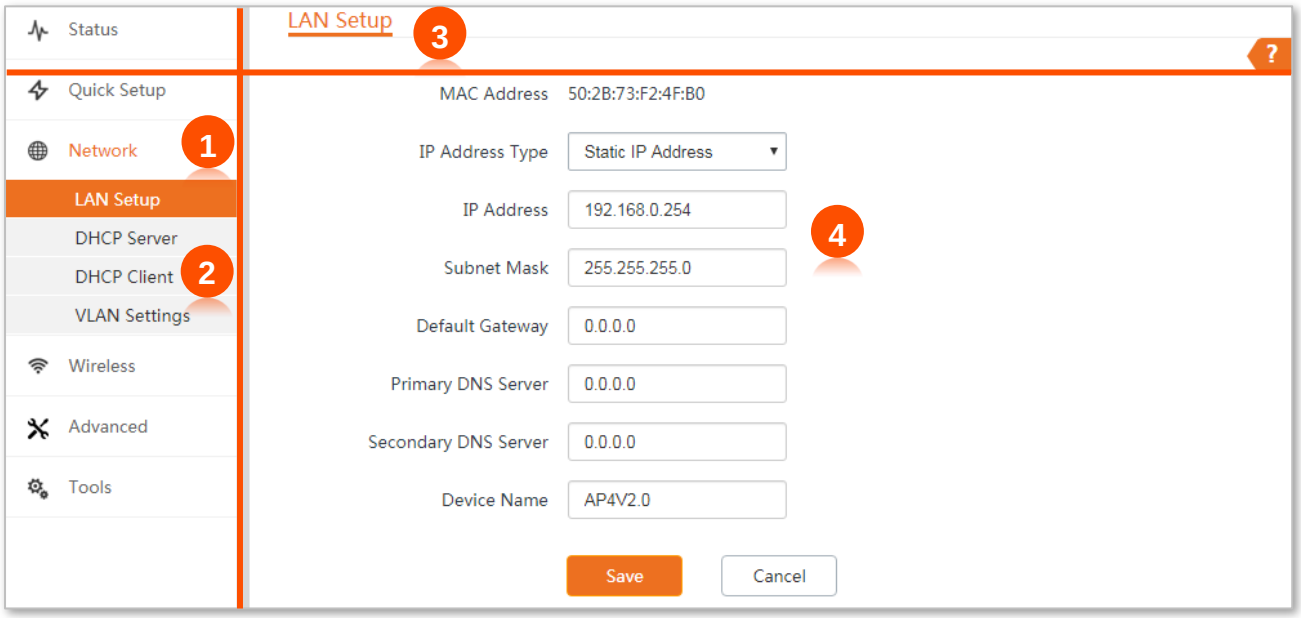
The AP logs you out when you:

- Click the **Logout** button on the upper-right corner of the web UI.
- Close the web browser.
- Perform no operation within the login timeout interval (default: 5 minutes). You can change the login timeout interval on the **Advanced** > **Network Service** page.

2 Web UI

2.1 Web UI layout

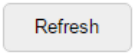
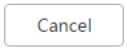
The web UI of the device is composed of 4 parts, including the level-1 navigation tree, level-2 navigation tree, tab page area, and configuration area. See the following figure.



No.	Name	Description
1	Level-1 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.
2	Level-2 navigation tree	
3	Tab page area	
4	Configuration area	It enables you to view and modify configuration.

2.2 Common buttons

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

Common Buttons	Description
	It is used to update the content of the current page.
	It is used to save the configuration on the current page and enable the configuration to take effect.
	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.

3 Status

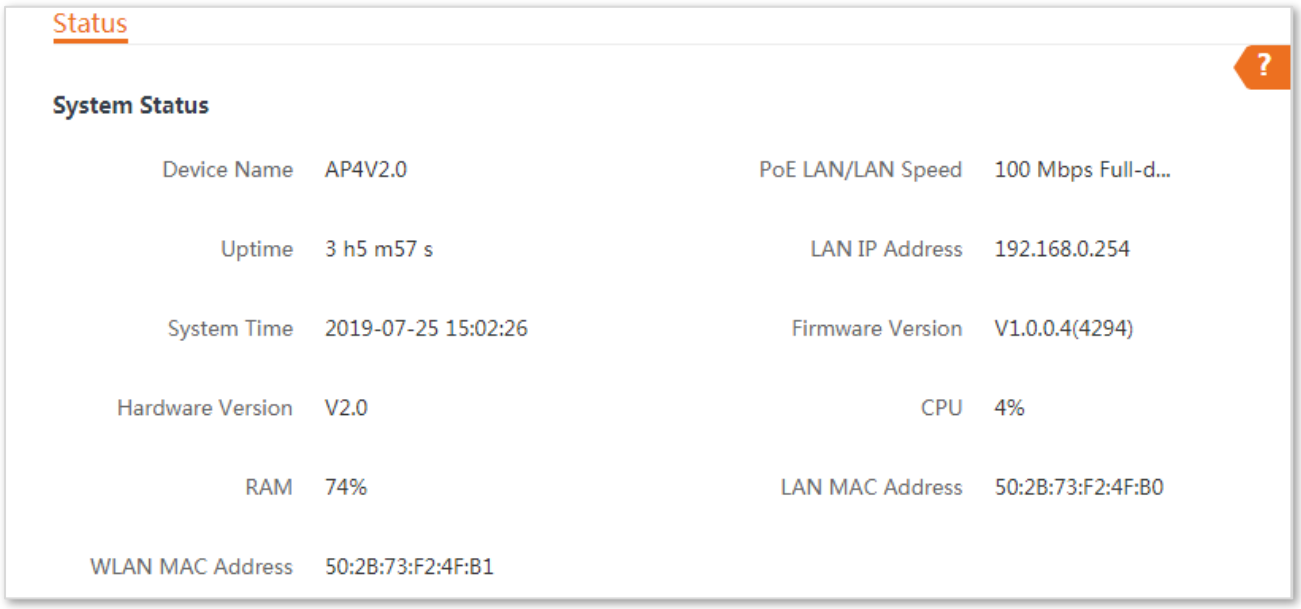
This module includes three parts: system status, wireless status, and statistics.

3.1 System status

On the **System Status** page, you can view the system status here.

To access the page, log in to the web UI of the device, and choose **Status**.

In **AP** mode, **Client** mode, **Universal Repeater** mode, or **Client + AP** mode, the system status is shown as follows:

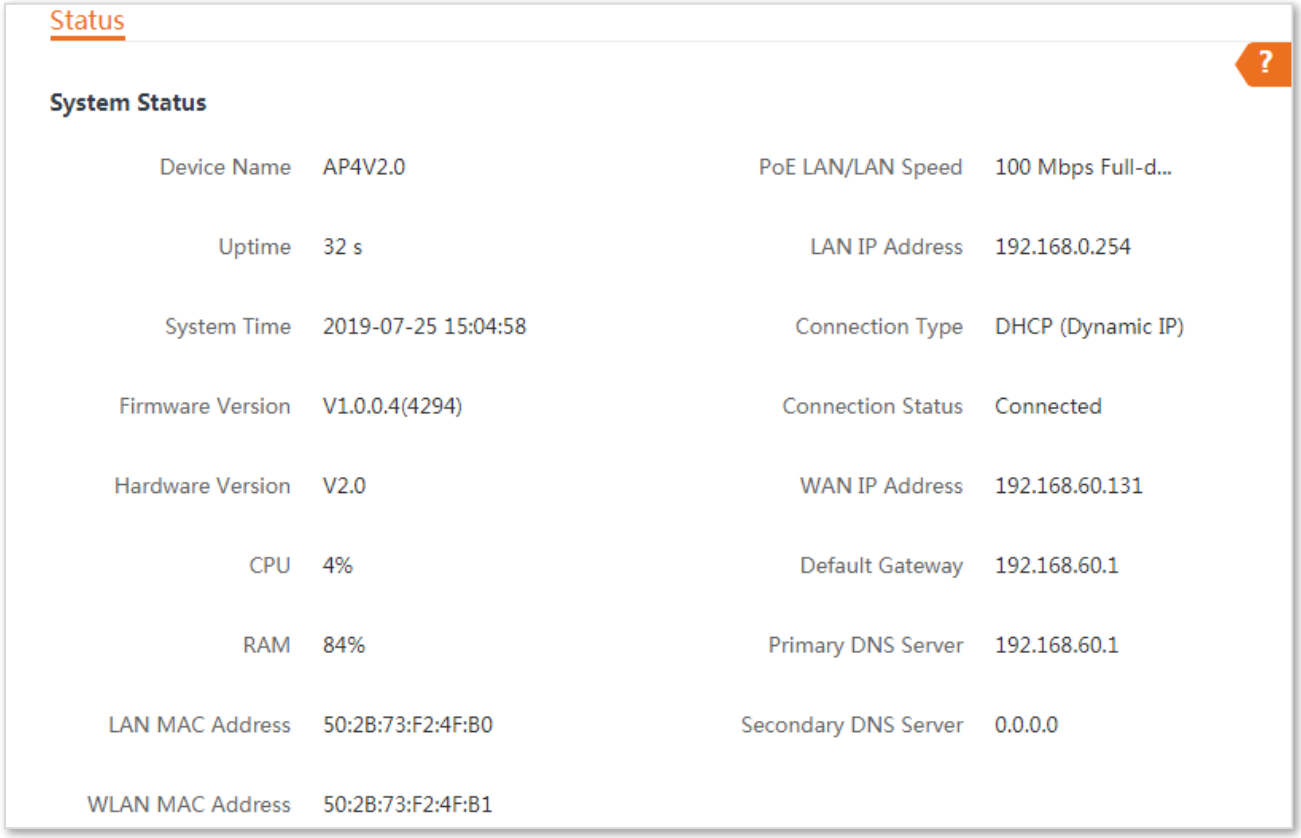


Parameters description

Name	Description
Device Name	It specifies the name of this device. A unique device name helps you manage multiple devices that are of the same model on LAN easily. To modify the device name, go to **Network** > **LAN Setup** page. You are allowed to modify only when the device works in **AP**, **Client**, **Universal Repeater**, or **Client + AP** mode.
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 number of this device.

Name	Description
RAM	Random Access Memory. It specifies the memory usage of this device.
WLAN MAC Address	It specifies the MAC address of the WiFi network of this device.
PoE LAN/LAN Speed	It specifies connection status of LAN port. It includes connection rate and duplex mode.
LAN IP Address	It specifies the IP address (also called login or management IP address) of this device. By default, it is **192.168.0.254**.
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 ports of this device.

In **WISP** or **Router** mode, the system status is shown as follows:



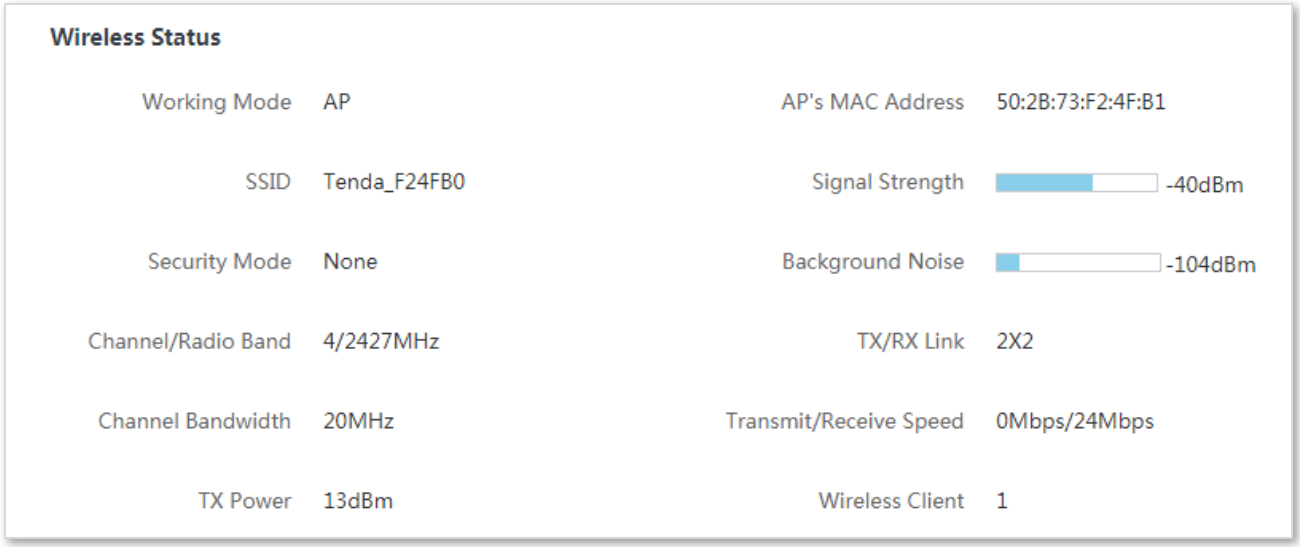
Parameters description

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

3.2 Wireless status

On the **Wireless Status** page, you can view wireless status here, including working mode, SSID, security mode, and so on.

To access the page, log in to the web UI of the device, and choose **Status**.



Parameters description

Name	Description
Working Mode	It specifies the working mode the device operates.
SSID	It specifies the WiFi name of this device. In Client mode, it displays N/A.
Security Mode	It specifies the security mode of the WiFi network of this device.
Channel/Radio Band	It specifies the channel and frequency band the device operates.
Channel Bandwidth	It specifies the channel bandwidth of this device.
TX Power	It specifies the transmit power of this device.
AP's MAC Address	In **Client**, **Universal Repeater**, **WISP** or **Client + AP** modes, it displays the MAC address of peer AP to which this device bridged. In **AP** or **Router** mode, it displays **No Peer AP** if the device works.
Signal Strength	In **AP** or **Router** mode, it displays the signal strength of the first device connected to the WiFi network of the device. In **Client**, **Universal Repeater**, **WISP** or **Client + AP** mode, it displays the received signal strength from peer AP.
Background Noise	It specifies the strength of ambient radio interference. Larger absolute value indicates less interference. For example, -95 dBm indicates less interference than that of -75 dBm.

Name	Description
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 client connected to the WiFi network of this device. • In **Client**, **Universal Repeater**, **WISP** or **Client + AP** mode: it displays transmitting/receiving rate of this device.
Wireless Client	It specifies the number of wireless clients connected to this device. In **Client** mode, it displays **N/A**.

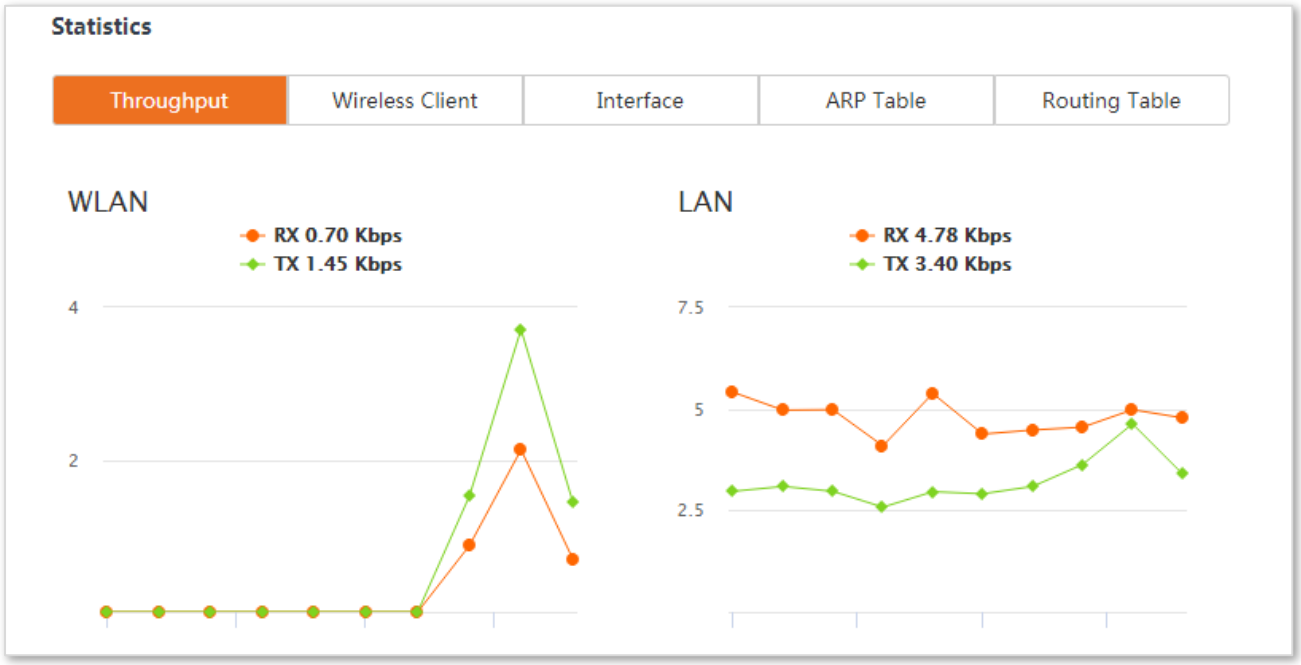
3.3 Statistics

On the **Statistics** page, you can view statistics information here, including throughput, wireless client, interface, ARP table and routing table.

To access the page, log in to the web UI of the device, and choose **Status**.

3.3.1 Throughput

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

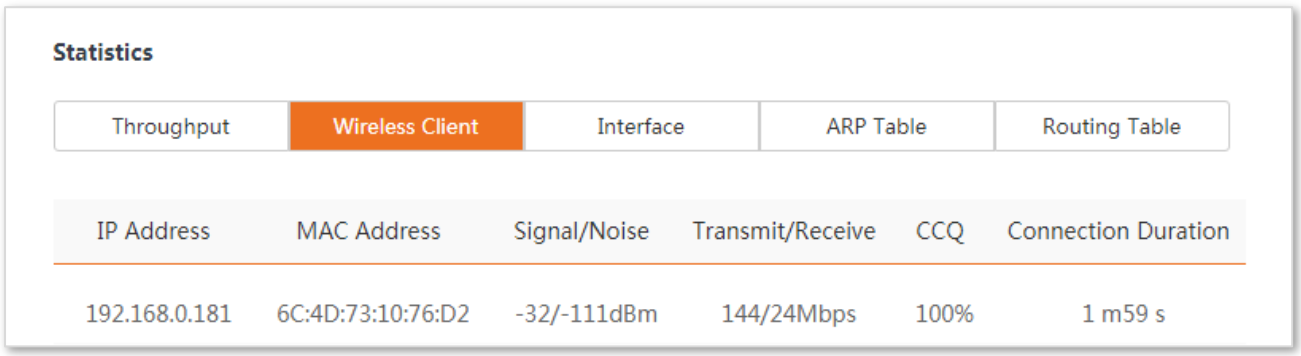


3.3.2 Wireless client/Upstream AP

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

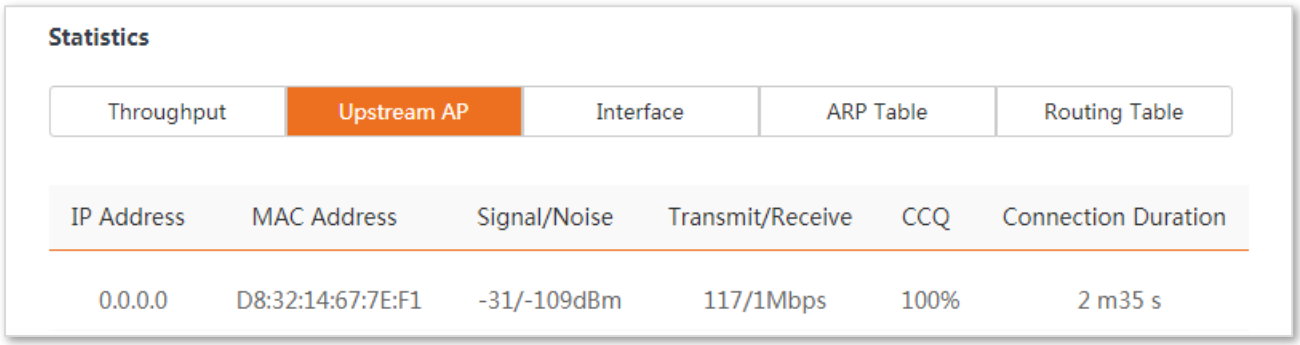
-In **AP** or **Router** mode, it displays information of connected wireless clients.

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



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	• **Signal**: It specifies the WiFi signal strength of the corresponding wireless client. • **Noise**: It specifies the ambitus interference signal and electromagnetic interference strength.
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 WiFi network of the device last time.

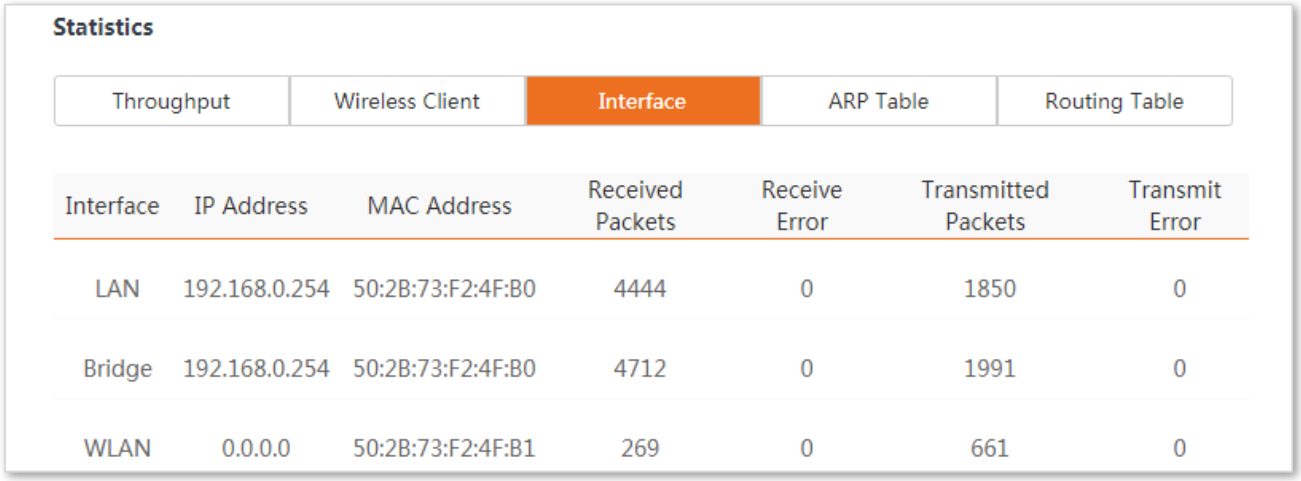


Parameters description

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	• **Signal**: It specifies the WiFi signal strength of the corresponding wireless client. • **Noise**: It specifies the ambitus interference signal and electromagnetic interference strength.
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 is connected to the upstream AP last time.

3.3.3 Interface

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

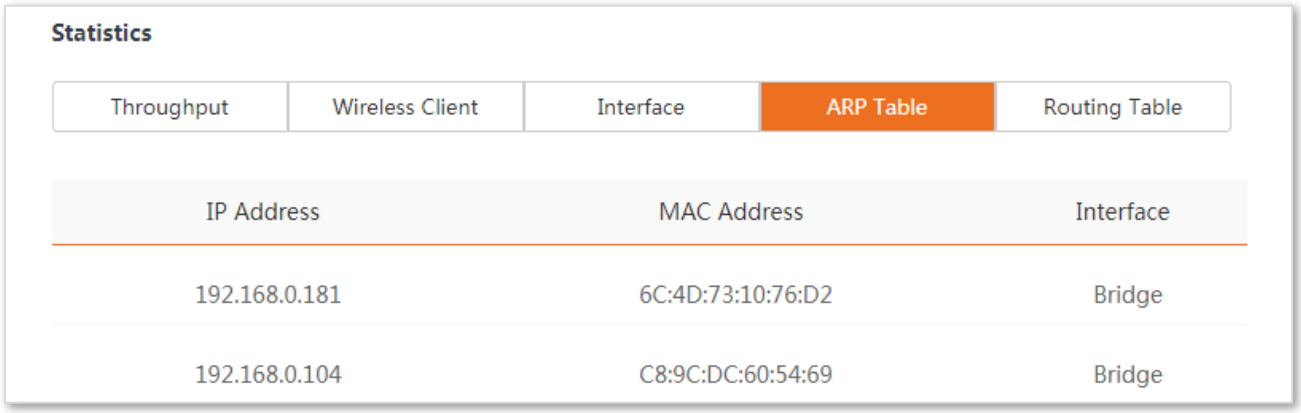


Parameters description

Name	Description
Interface	It specifies the interface type that packets passes through, including LAN, Bridge, and WLAN interfaces.
IP Address	It displays the IP addresses of wired interface, bridge interface, and WLAN interface.
MAC Address	It displays the MAC addresses of an interface.
Received Packets	It displays the received and transmitted packets of the interface.
Transmitted Packets	
Receive Error	It displays the number of error packets received/transmitted by the interface.
Transmit Error	

3.3.4 ARP table

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



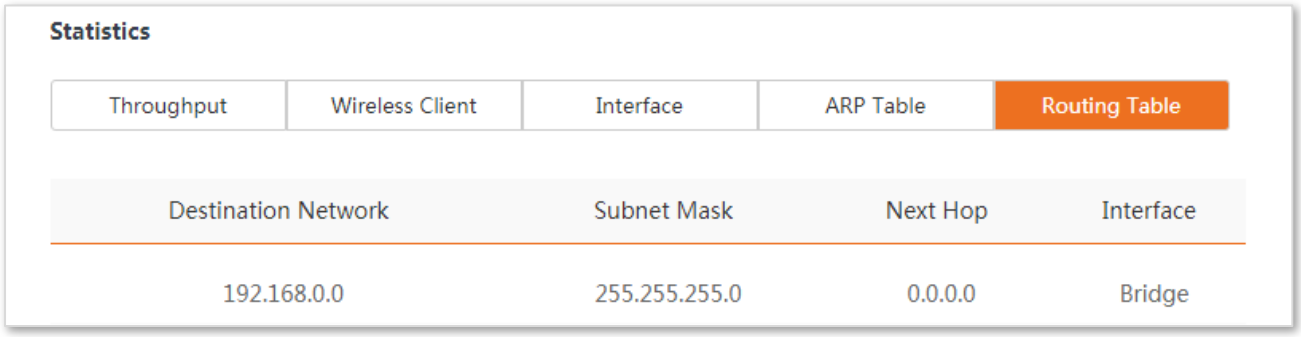
Parameters description

Name	Description
IP Address	It specifies the IP address of the host in the APR table.
MAC Address	It specifies the MAC address corresponding to the IP address.
Interface	It specifies the interface used to communicate with the host, including LAN, WLAN and bridge interfaces.

3.3.5 Routing table

It specifies the destination networks that the device can access.

To access the page, log in to the web UI of the device, and choose **Status**, then **Routing Table** in **Statistics** part.



Parameters description

Name	Description
Destination Network	It specifies the IP address of the destination network.
Subnet Mask	It specifies the subnet mask of the destination network.
Next Hop	It specifies the IP address of entrance of the next hop route when the packets egress from the interface of the device. 0.0.0.0 indicates that the destination network is the network which is directly connected to the interface.
Interface	It specifies the interface that the packets egress.

4 Quick setup

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

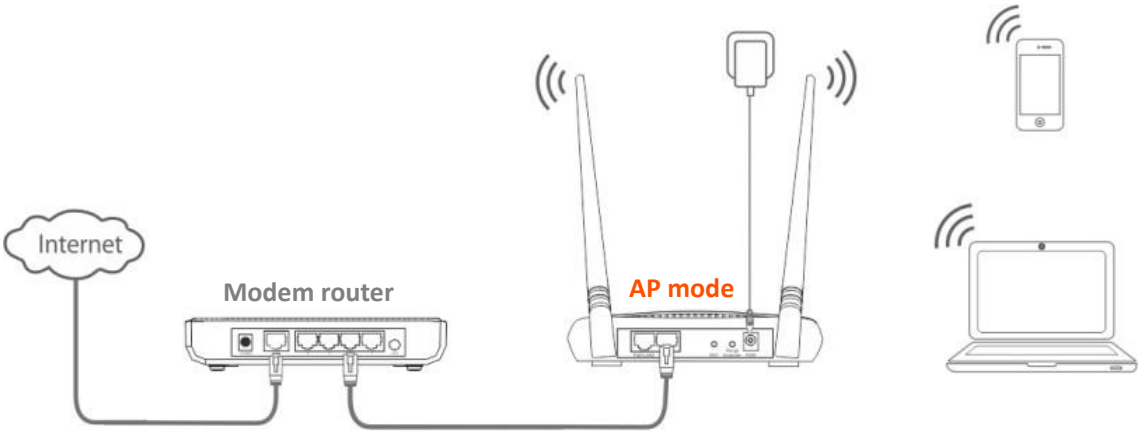
This AP supports AP, Client, Universal Repeater, WISP, Client + AP, and Router modes.

4.1 AP mode

4.1.1 Overview

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

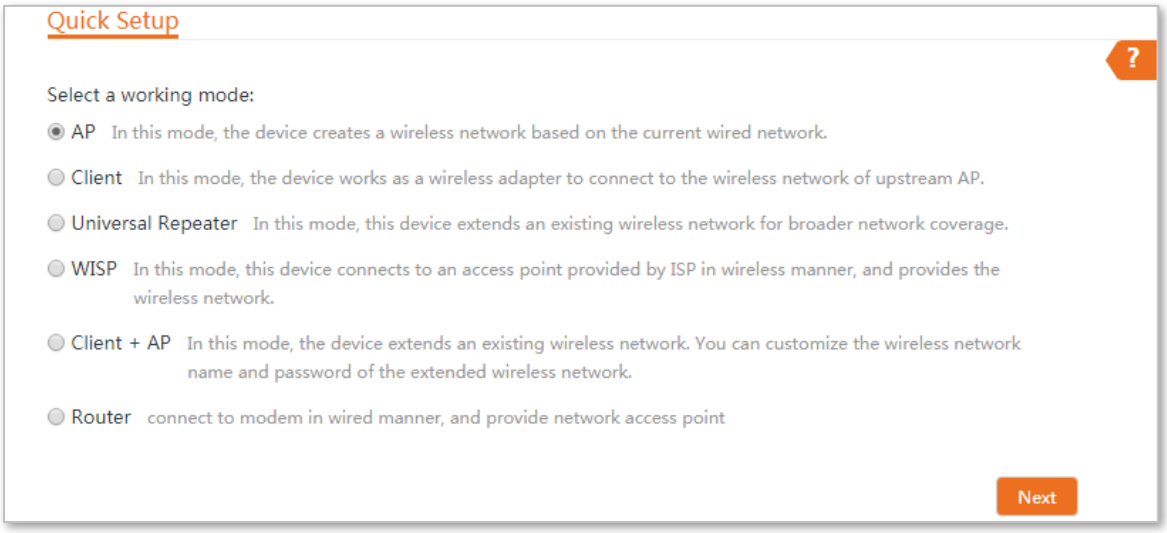
Network requirement: You want to transform your wired network to a wireless one for your wireless devices to access the internet.



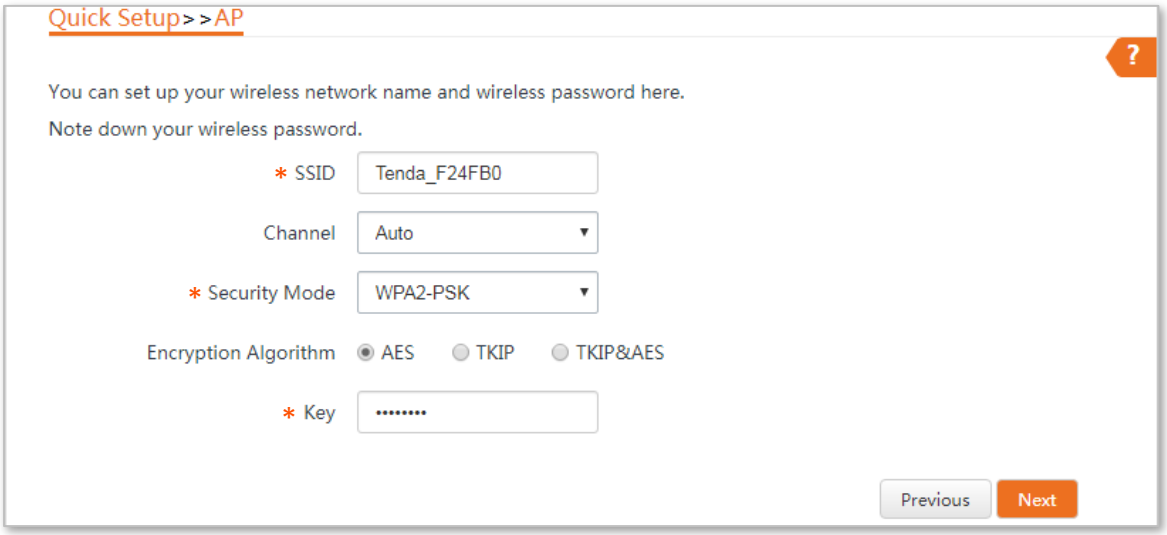
Configuration procedure of setting AP mode

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

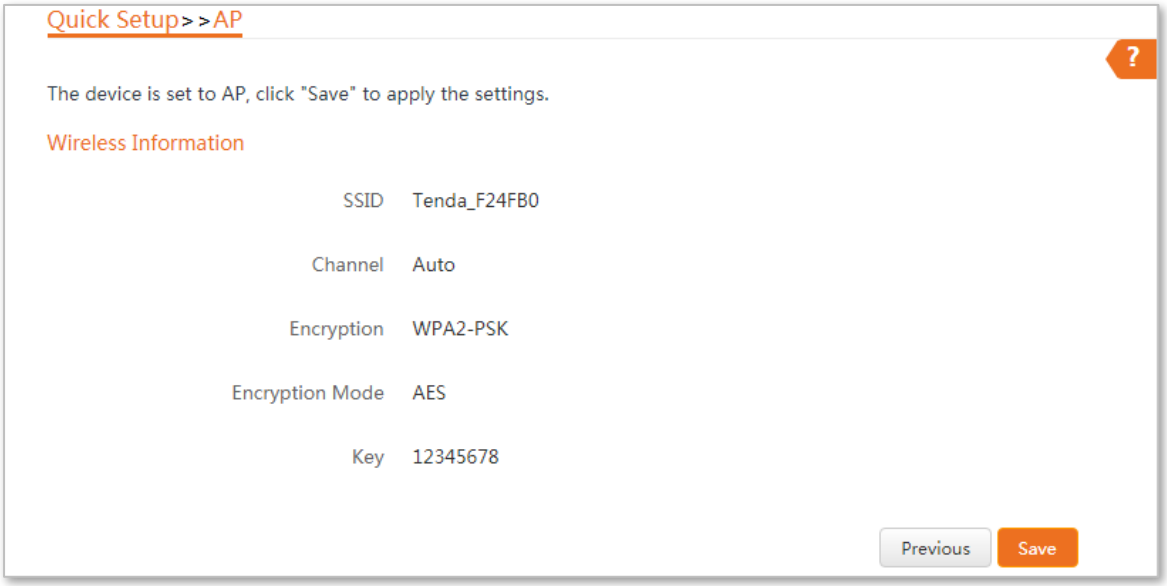
Step 2 Select **AP** mode and click **Next**.



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



Step 4 Note down the **SSID** and **Key** and keep them well. Then click **Save**.



----End

Wait until the device completes rebooting to apply your settings.

Then connect your WiFi-enabled devices using the **SSID** (WiFi network name) and **Key** (WiFi password) you set and enjoy the internet access.

TIP

You can navigate to **Wireless** > **Basic** to view and modify the wireless information later.

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **AP** mode: In this mode, the device creates a WiFi network based on the current wired network.
SSID	It specifies the WiFi name of this device.
Channel	It specifies the operating channel of this device. **Auto** (Default): It indicates that the device automatically adjusts its operating channel according to the ambient environment.
Security Mode Encryption	It specifies the security mode of the WiFi network, including: None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.
Encryption Algorithm Encryption Mode	It specifies the encryption method of the WiFi network. • **AES**: It indicates the Advanced Encryption Standard. • **TKIP**: It indicates the Temporal Key Integrity Protocol. If **TKIP** is used, the maximum wireless throughput of the 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 WiFi network corresponding to the selected SSID using **TKIP** or **AES**.
Key	It specifies the WiFi password of the WiFi network.

4.1.2 Example of AP mode

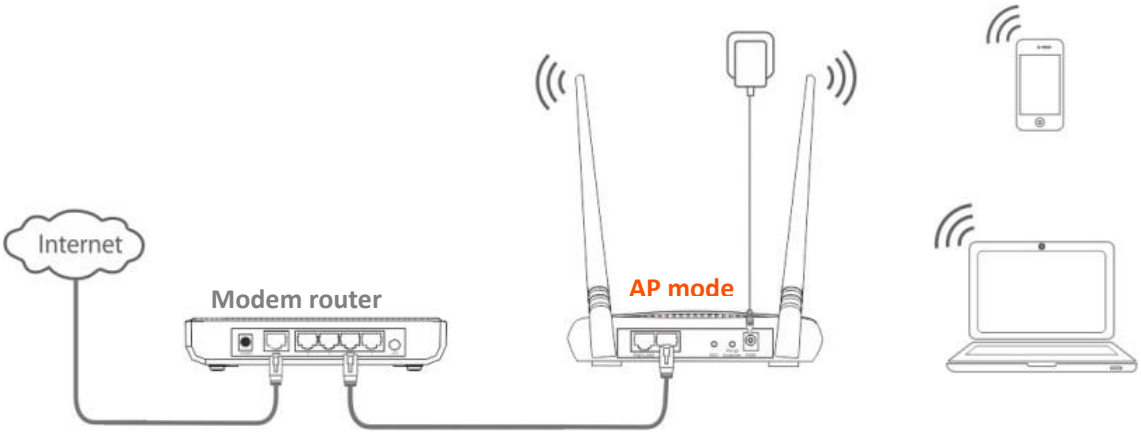
Network requirement

You have several WiFi-enabled devices at your home, such as smart phones, tablets, smart speakers etc. But the modem router at your home can only provide internet access to wired devices. Now you want to establish a WiFi network for these wireless devices.

Solution

To meet the requirement, you can set the device to **AP** mode to establish a WiFi network.

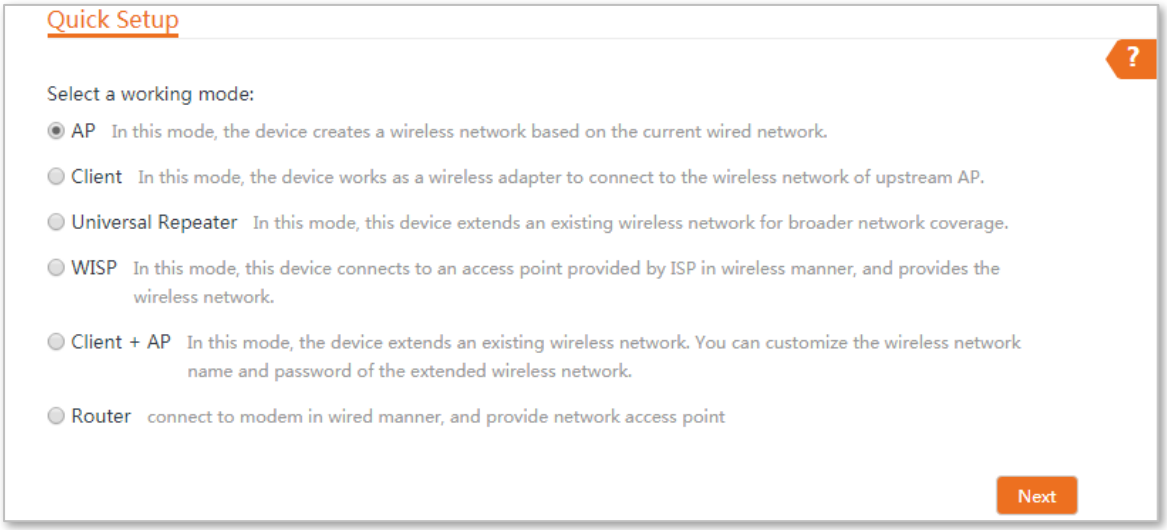
Network topology



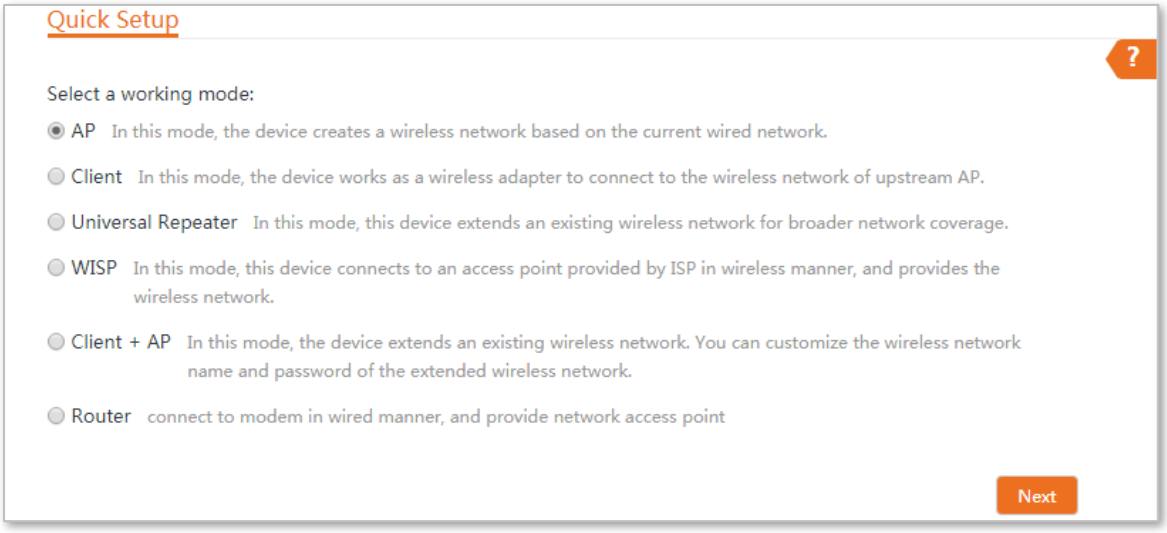
Configuration procedure

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

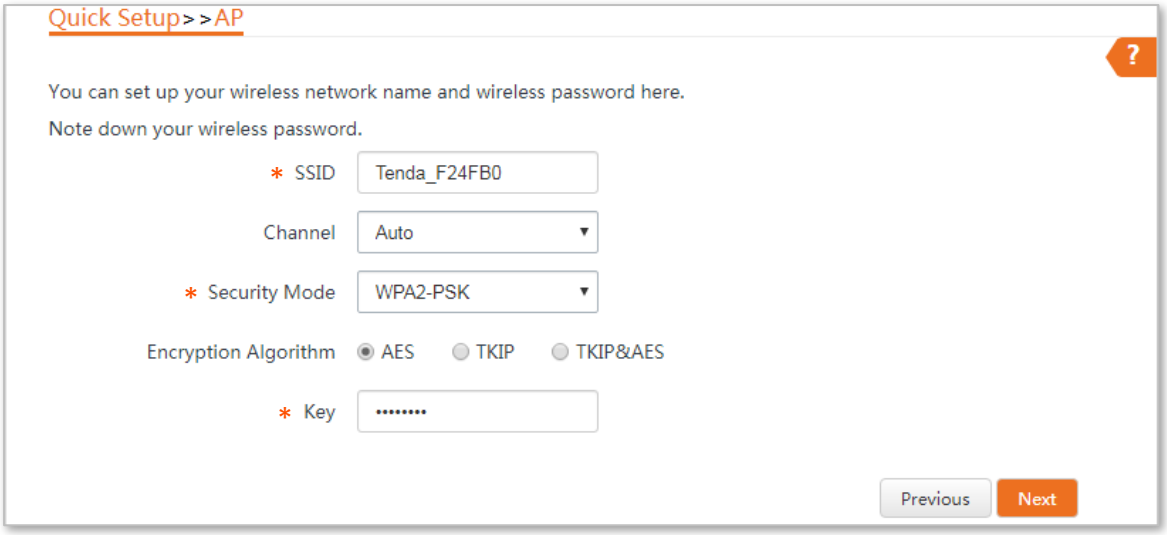
Step 2 Select **AP**, and click **Next**.



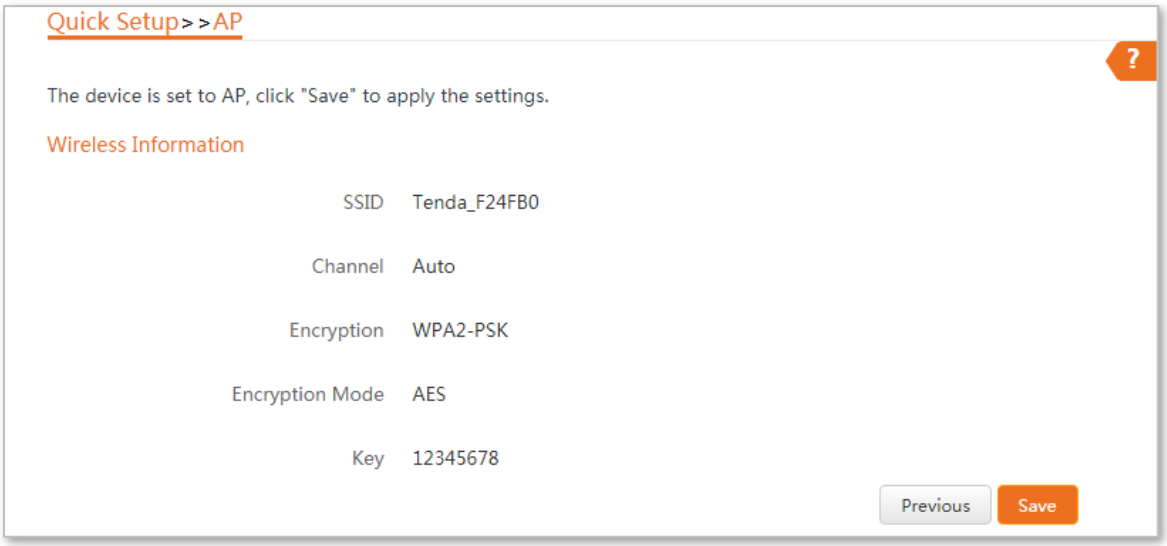
Step 3 Select **AP** mode and click **Next**.



Step 4 Set an SSID, which is **Tenda_F24FB0** in this example, **Security Mode** (WPA2-PSK is recommended) and **Key**, and click **Next**.



Step 5 Note down the **SSID** and **Key** and keep them well. Then click **Save**.



----End

Verification

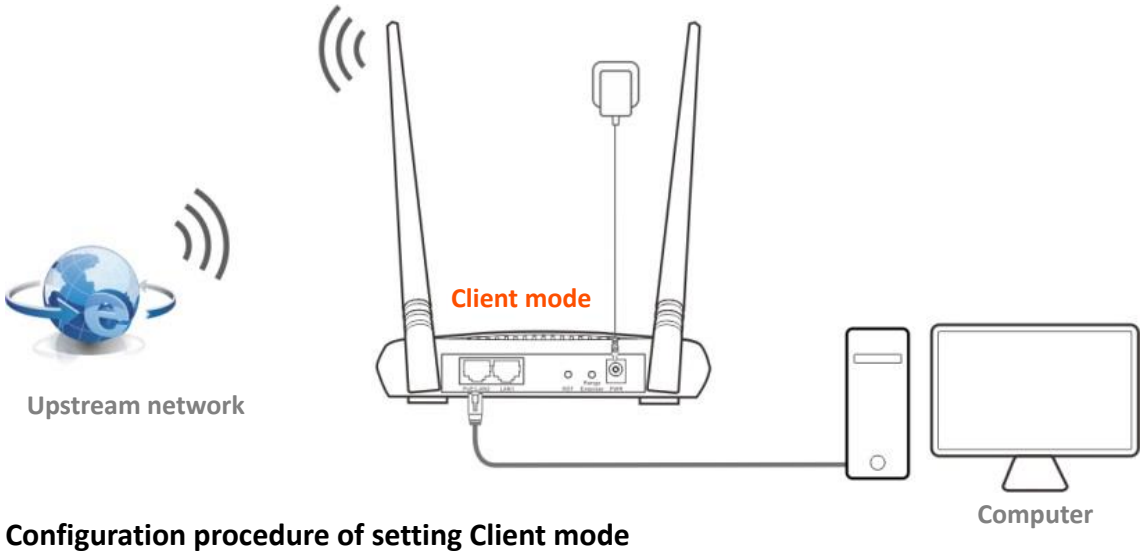
Connect your WiFi-enabled clients to the wireless network of the device using the SSID (WiFi network name) and Key (WiFi password) you set. You can enjoy wireless network now.

4.2 Client mode

4.2.1 Overview

In **Client** mode, this device serves as a wireless adapter, and connects wired devices to an upstream network.

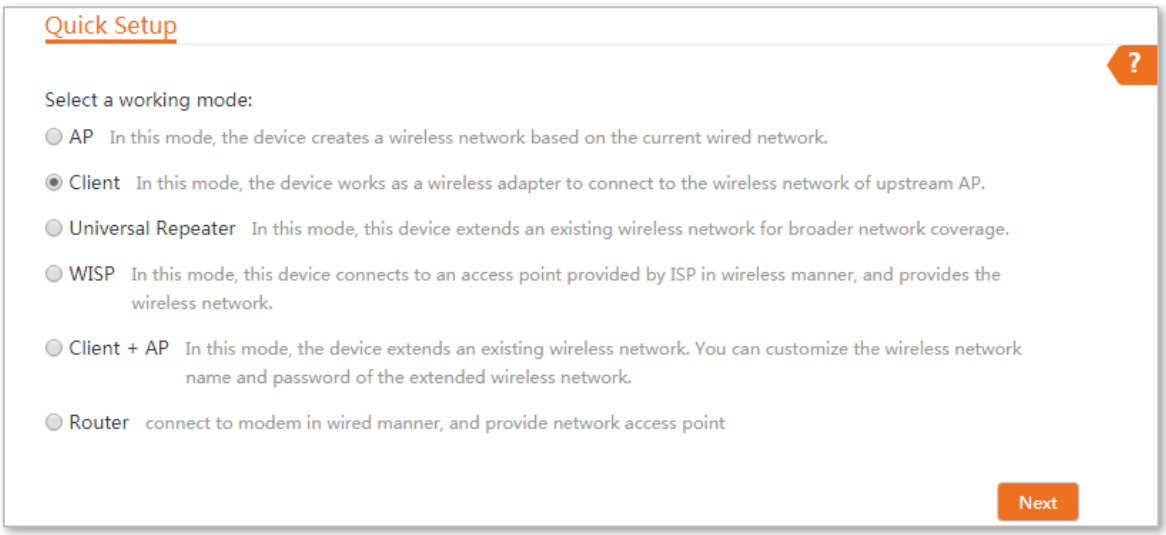
Network requirement: You want to connect your wired devices to a WiFi network.



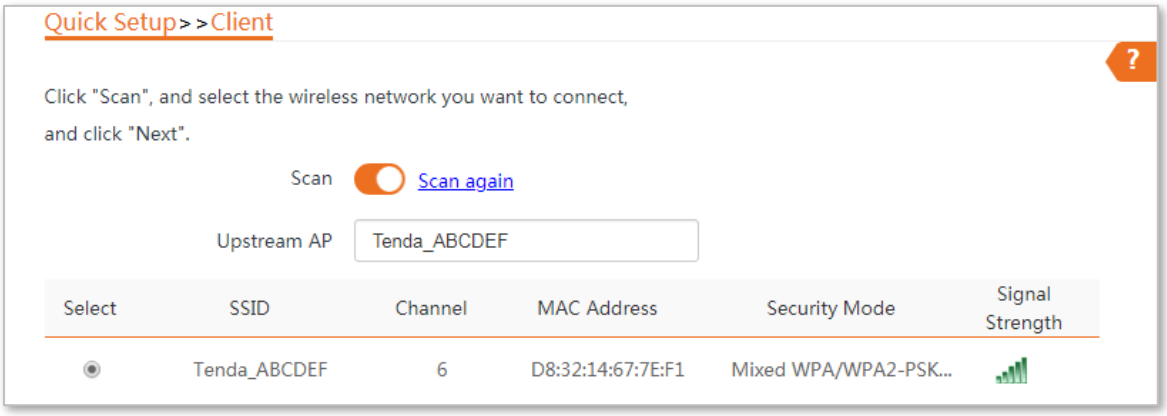
Configuration procedure of setting Client mode

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

Step 2 Select **Client**, and click **Next**.



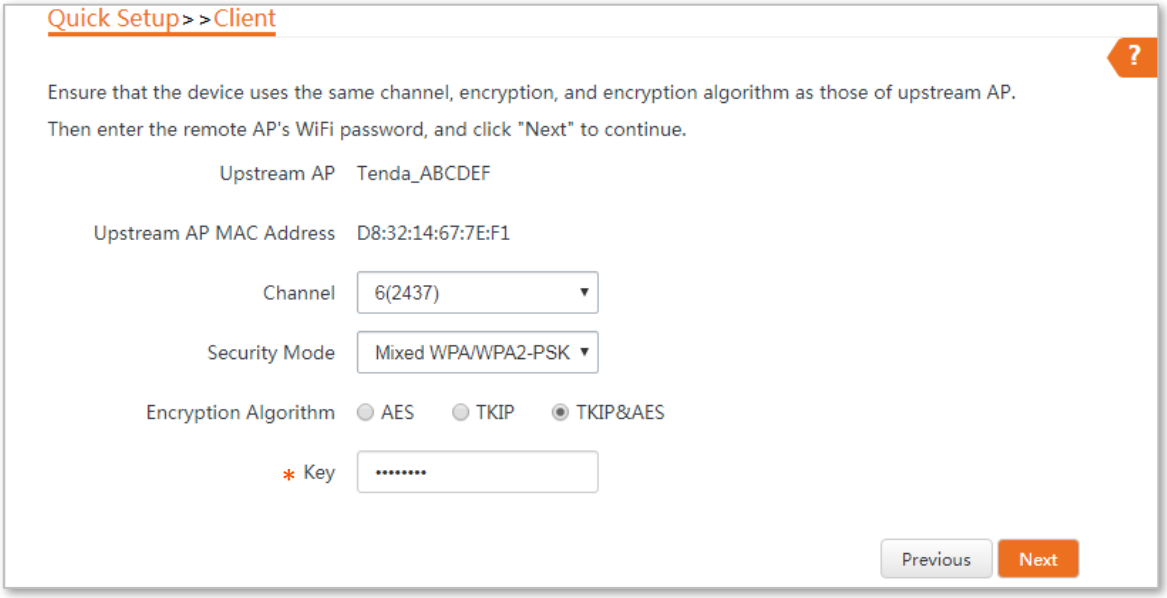
Step 3 Select the SSID of the upstream AP and click **Next** at the bottom of the page.



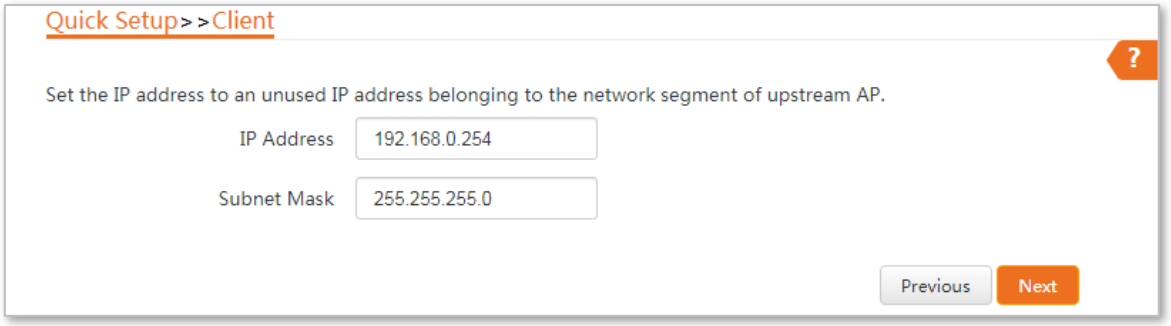
TIP

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

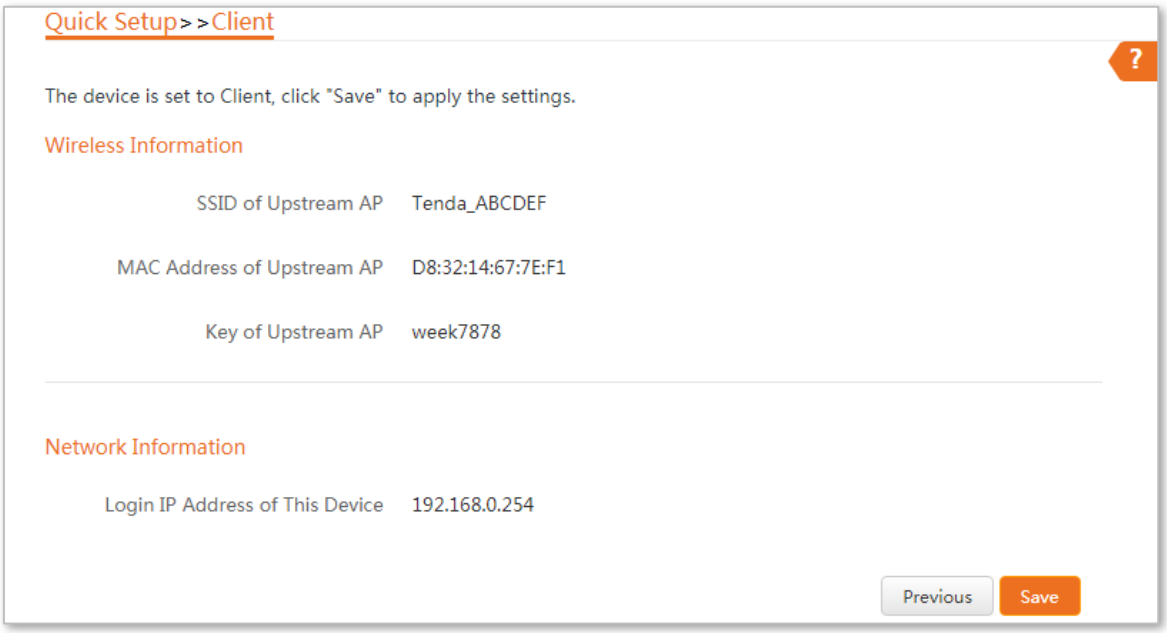
Step 4 Enter the WiFi password of your upstream network in the **Key** text box, and click **Next**.



Step 5 Set the IP address to an unused IP address belonging to the same network segment as that of the upstream AP. For example, if the IP address of the upstream AP is 192.168.0.1, you can set the IP address of this device to 192.168.0.*X* (*X* ranges from 2 to 254). Then click **Next**.



Step 6 Check whether the SSID you selected and WiFi password you entered are correct. Then click **Save**.



----End

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **Client** mode: In this mode, the device works as a wireless adapter to connect to the WiFi network of upstream AP, and does not provide WiFi network.
Upstream AP	It specifies the SSID (WiFi name) of the upstream AP.
Channel	It specifies the operating channel of the device, which is the same as the upstream AP to be bridged.
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 key, you need to enter the password manually.
Key	It specifies the WiFi key of the upstream AP.

4.2.2 Example of client mode

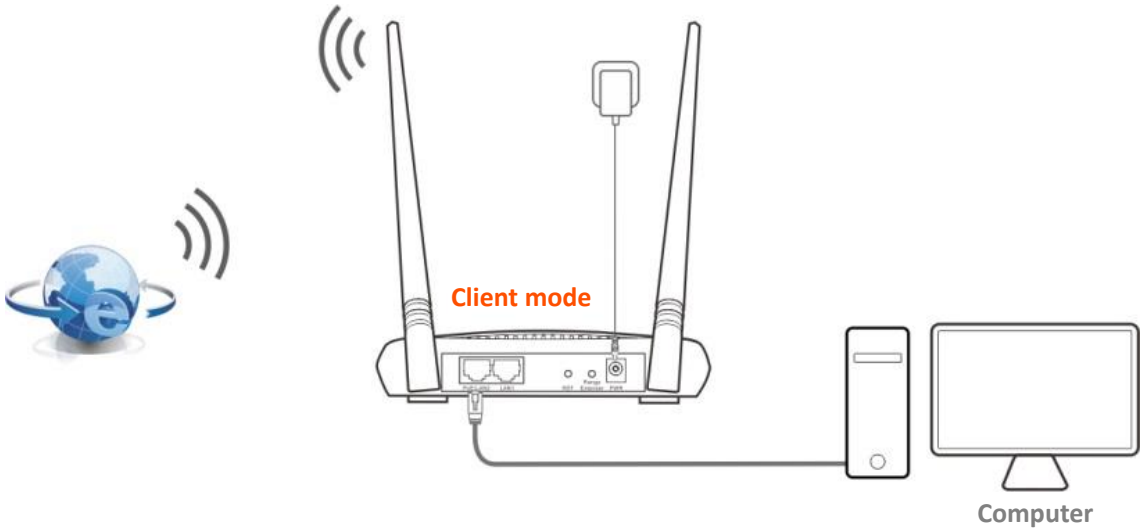
Network requirement

You already have a wireless router for internet access. However, your desktop computer without a wireless adapter in your study room is far away from your WiFi router. Thus, connecting your computer to your WiFi router with a long Ethernet cable costs and makes your home clutter. Now you want to connect the computer to your wireless router in wireless manner.

Solution

To meet the requirement, you can set the device to **Client** mode, and connect your computer to a LAN port of the AP for internet access.

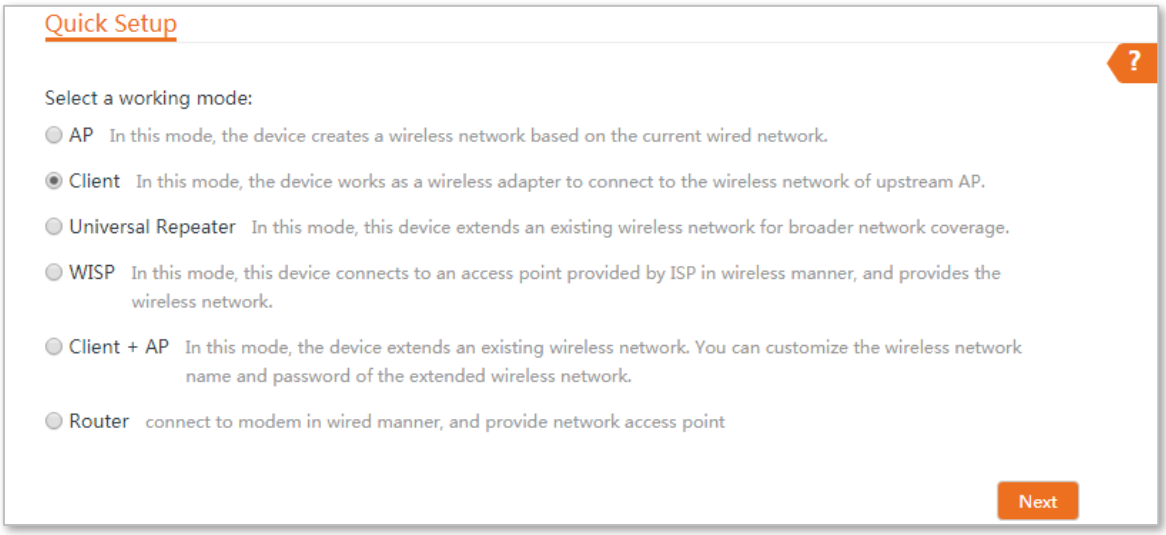
Network topology



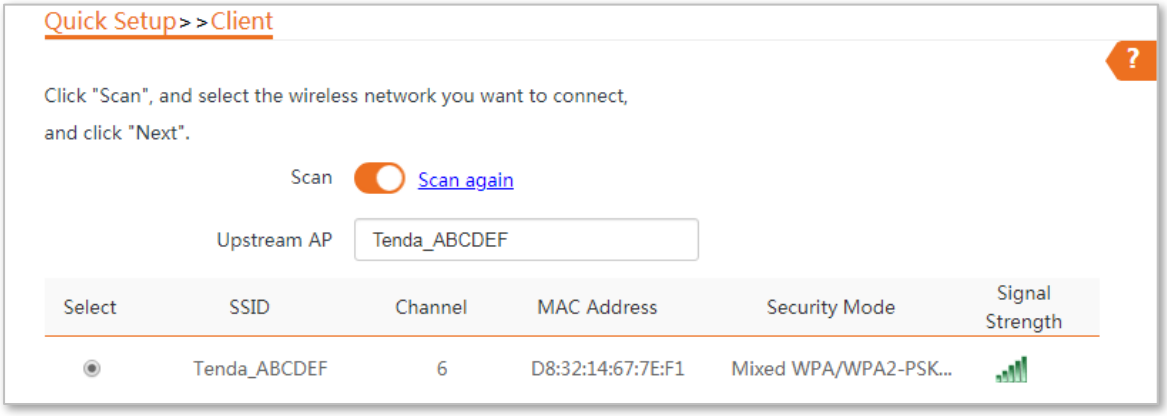
Configuration procedure

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

Step 2 Select **Client**, and click **Next**.



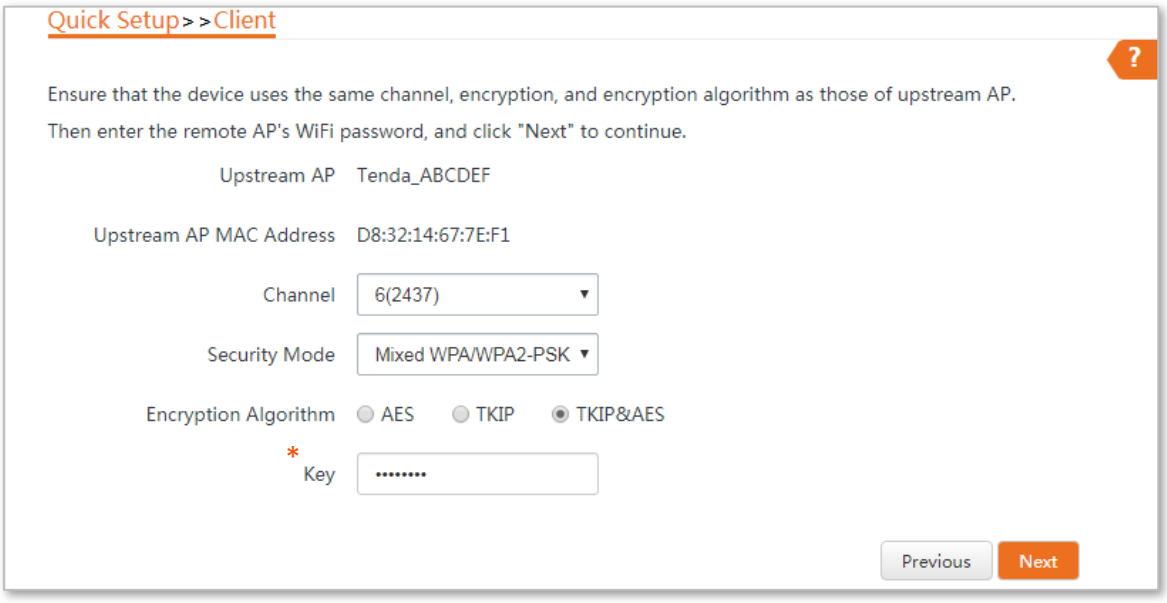
Step 3 Select the SSID of your wireless router and click **Next** at the bottom of the page.



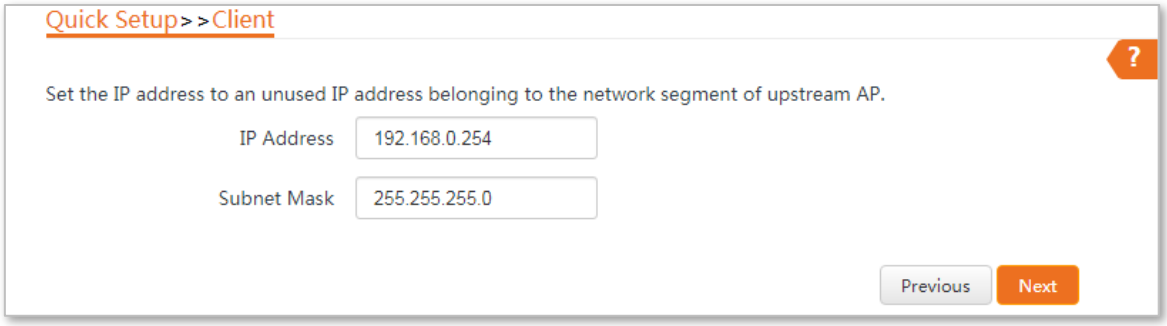
TIP

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

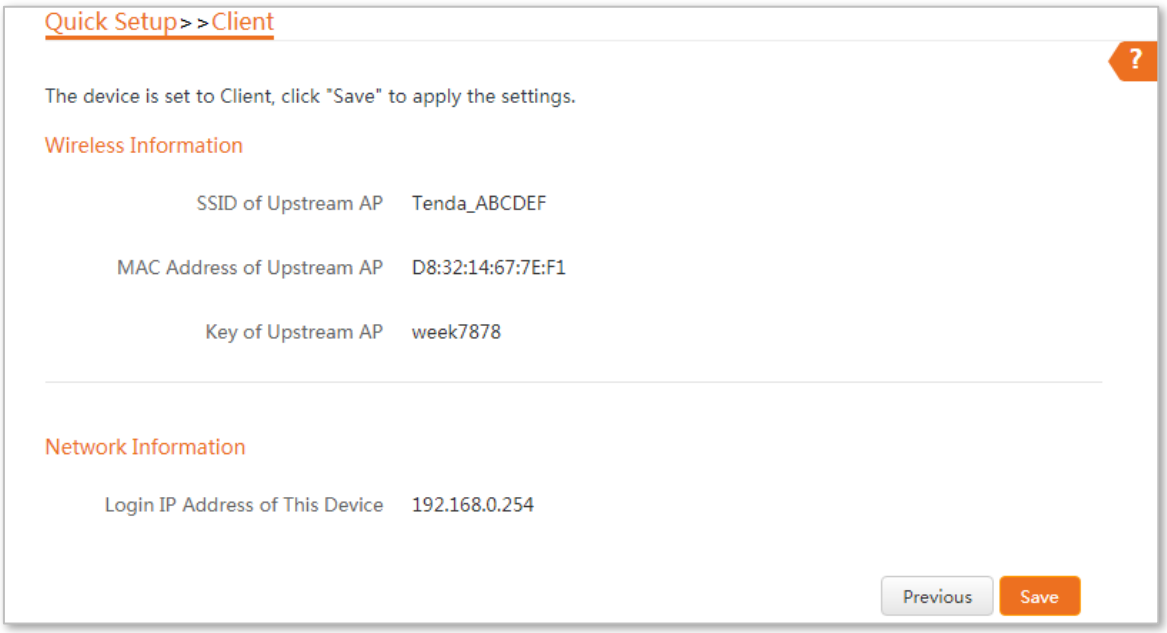
Step 4 Enter the WiFi key of your WiFi network in the **Key** text box, and click **Next**.



Step 5 Set the IP address to an unused IP address belonging to the same network segment as that of your wireless router. For example, if the IP address of your wireless router is 192.168.0.1, you can set the IP address of this device to 192.168.0.*X* (*X* ranges from 2 to 254). Then click **Next**.



Step 6 Check whether the SSID you select and WiFi password you enter are correct. Then click **Save**.



----End

Verification

The computer connected to the LAN port of the AP can access the internet now.

TIP

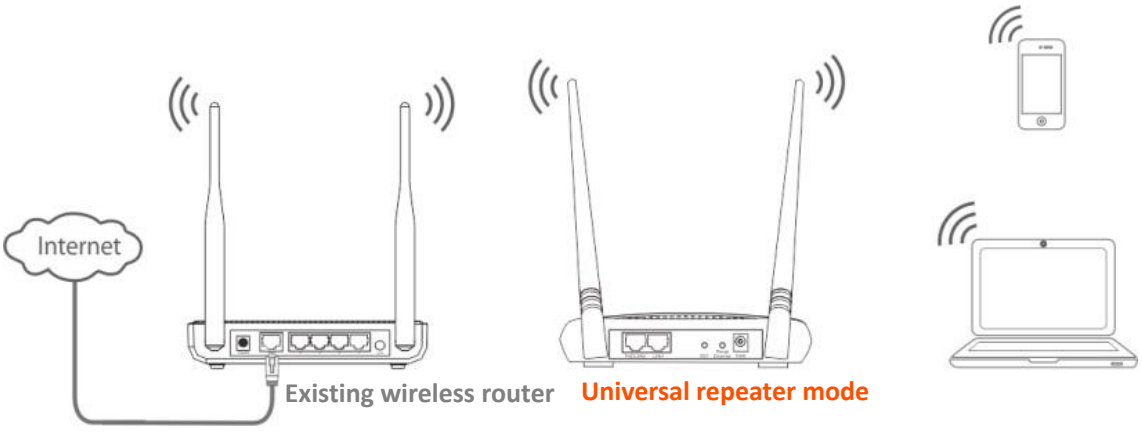
In client mode, the two Ethernet ports are both LAN ports.

4.3 Universal repeater mode

4.3.1 Overview

In **Universal Repeater** mode, this device expands your existing WiFi network for broader network coverage. After bridging, the WiFi name and password of this device are the same as those of your existing WiFi network.

Network requirement: You want to use the AP to extend your existing WiFi network. And after bridging, the WiFi name and key need to be the same as those of your existing WiFi network.



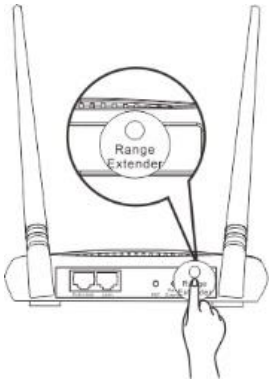
Option 1: Using the Range Extender button

To use this option, your existing wireless router must have a WPS button.

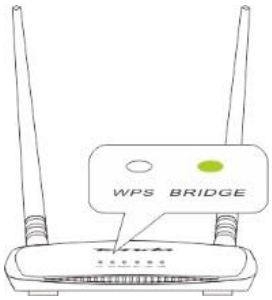
Step 1 Place the AP near your existing wireless router, power it on and wait until its SYS LED indicator blinks.

Step 2 Press the WPS button on your existing router.

Step 3 Within 2 minutes, press the **Range Extender** button on the AP for about 3 seconds, and then release it when its WPS LED indicator blinks.



Step 4 Wait until the **BRIDGE** LED indicator of the AP turns to solid on, which indicates that the AP bridges to your existing WiFi router successfully.



Step 5 Relocate the AP. Place it:

- In a high and open area.
- Within the WiFi coverage range of your existing WiFi router.
- In the middle place between your existing WiFi router and the WiFi dead zone.

----End

The AP's WiFi network name: Same as that of your existing WiFi router.

The AP's WiFi password: Same as that of your existing WiFi router.

Now you can connect your WiFi-enabled clients to the AP's WiFi network and enjoy internet access.

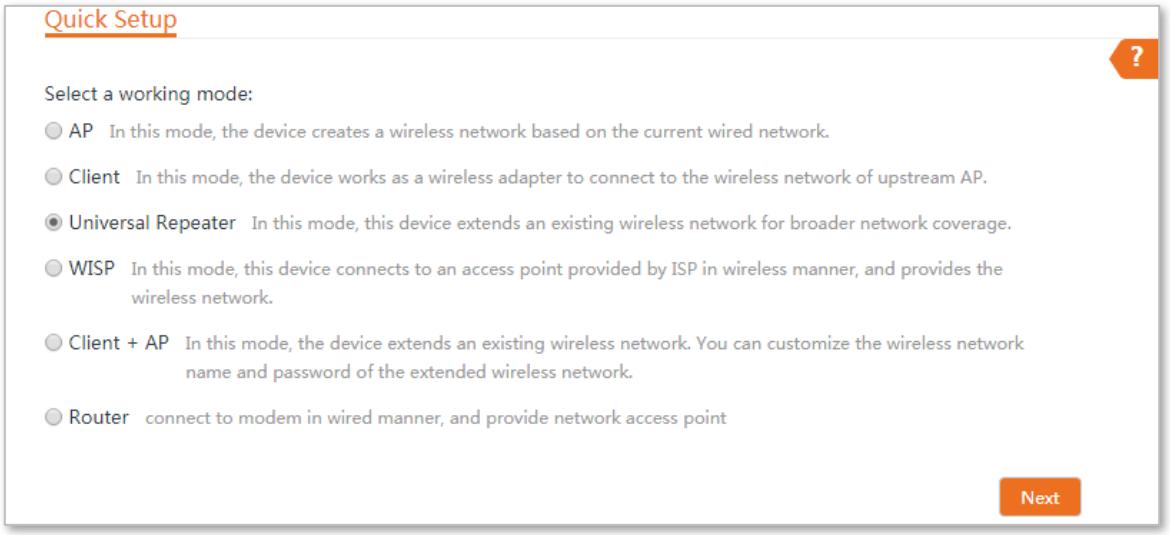
Option 2: Using the web UI

Configuration procedure of setting Universal Repeater mode

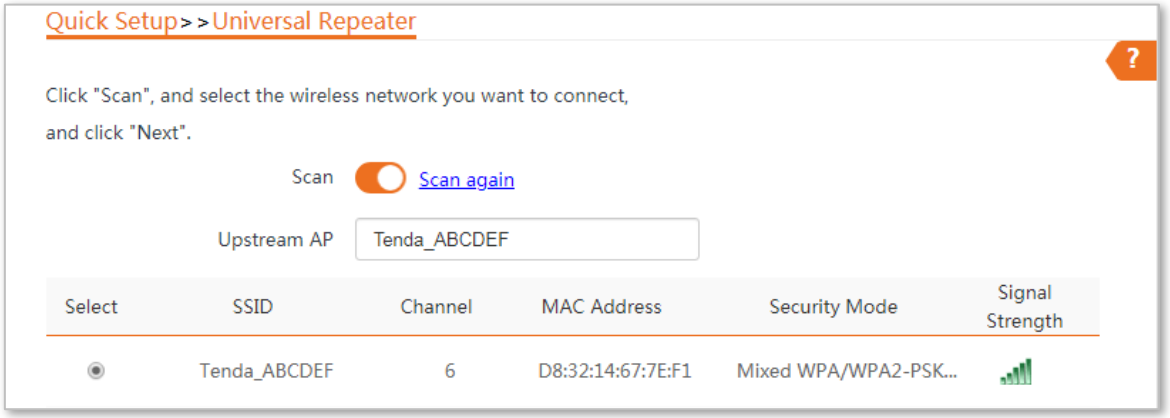
Step 1 Place the AP near your existing WiFi router, and power it on.

Step 2 Log in to the web UI of the AP and choose **Quick Setup** to enter the configuration page.

Step 3 Select **Universal Repeater**, and click **Next**.



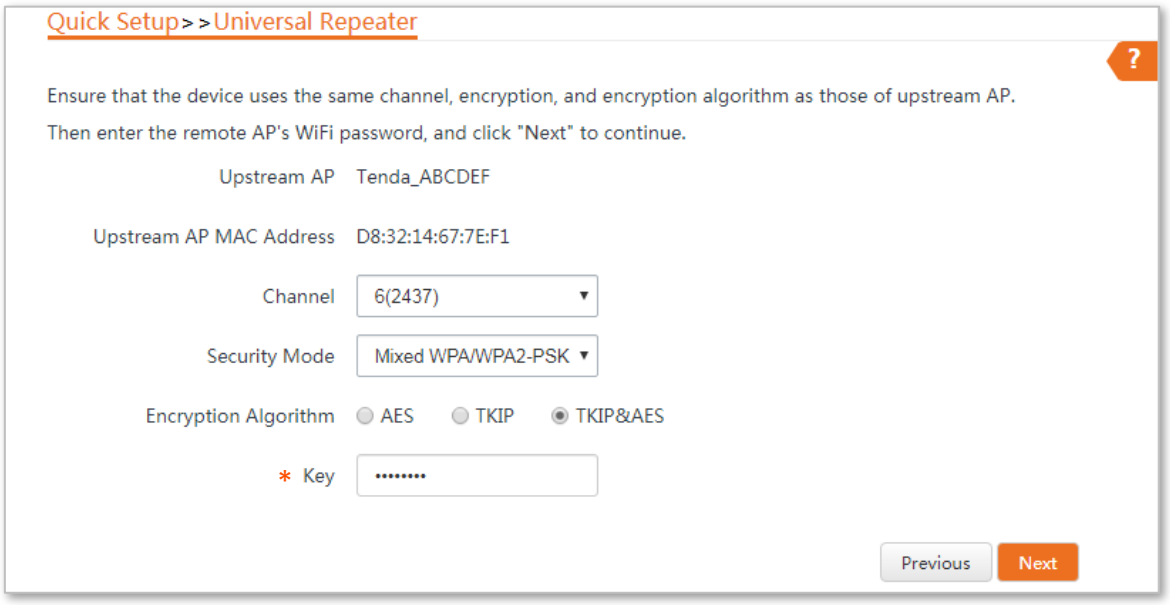
Step 4 Select the SSID of your existing WiFi router and click **Next** at the bottom of the page.



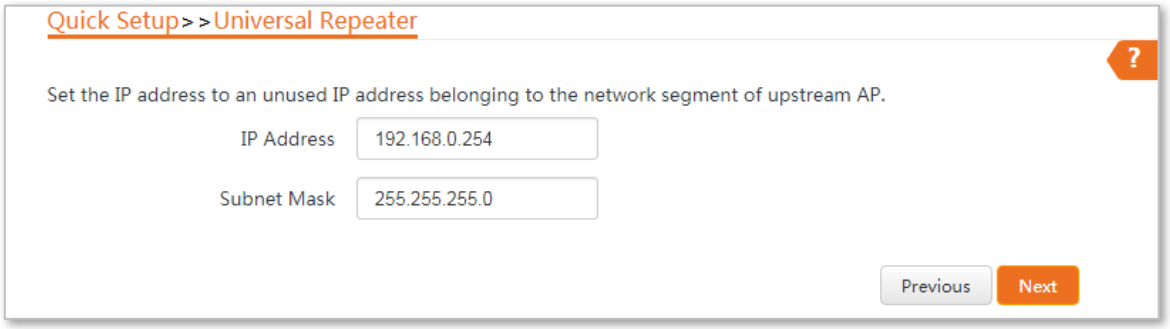
TIP

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

Step 5 Enter the WiFi password of your existing WiFi router in the **Key** text box, and click **Next**.



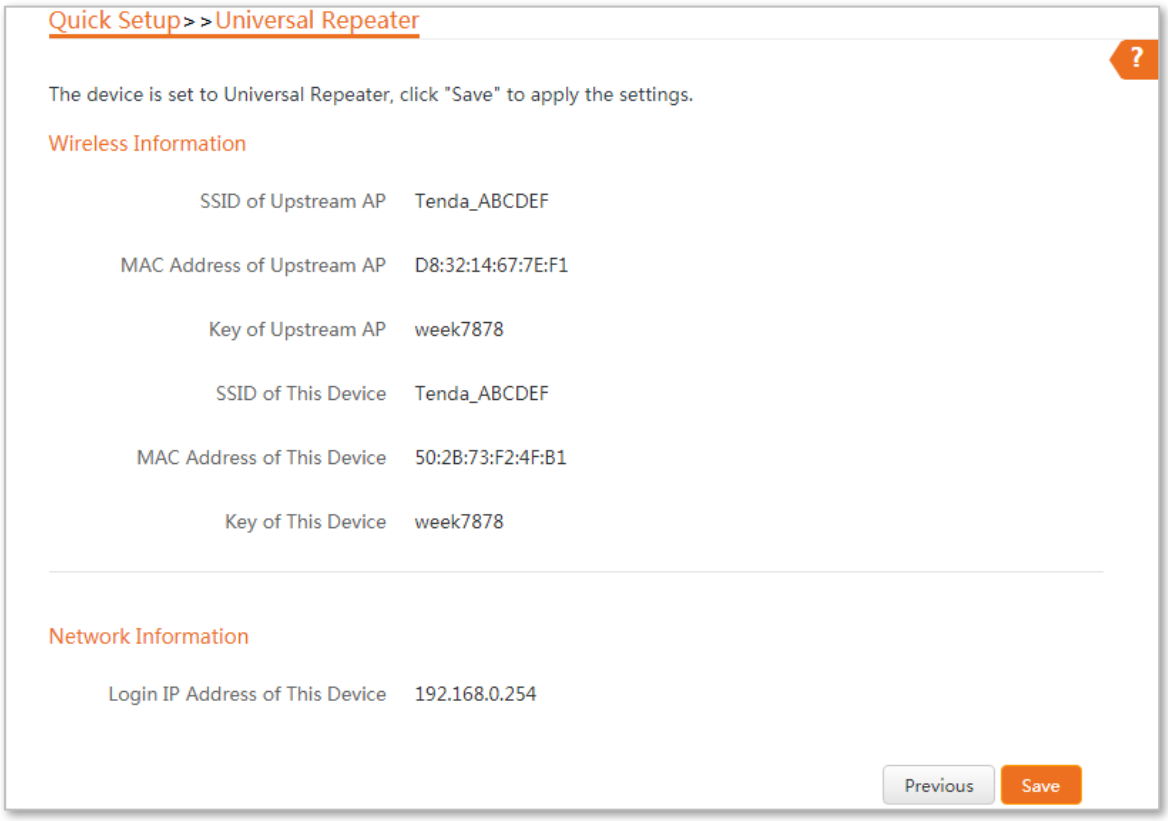
Step 6 Set the IP address to an unused IP address belonging to the same network segment as that of the router. For example, if the IP address of the router is 192.168.0.1, you can set this device's IP address to 192.168.0.*X* (*X* ranges from 2 to 254). Then click **Next**.



Step 7 Note down the **SSID** and **Key** and keep them well. Then click **Save**.

TIP

You can check the SSID and key on the **Wireless** > **Basic** page, but cannot change them.



Step 8 After the device completes reboot, relocate it:

- In a high and open area.
- Within the WiFi coverage range of your existing WiFi router.
- In the middle place between your existing WiFi router and the WiFi dead zone.

----End

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **Universal Repeater** mode: In this mode, the device expands your WiFi network for broader network coverage. After bridging, the WiFi name and key are changed to the same as those of the upstream AP.
Upstream AP	It specifies the WiFi 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.

Parameter	Description
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 key, you need to enter the password manually.

4.3.2 Example of universal repeater mode

Network requirement

You already have a wireless router and place it in the dining room for internet access, but in some places at home, such as bedrooms, balconies, and washing rooms, the WiFi signal is weak. Now you want to have a larger WiFi network coverage through your home.

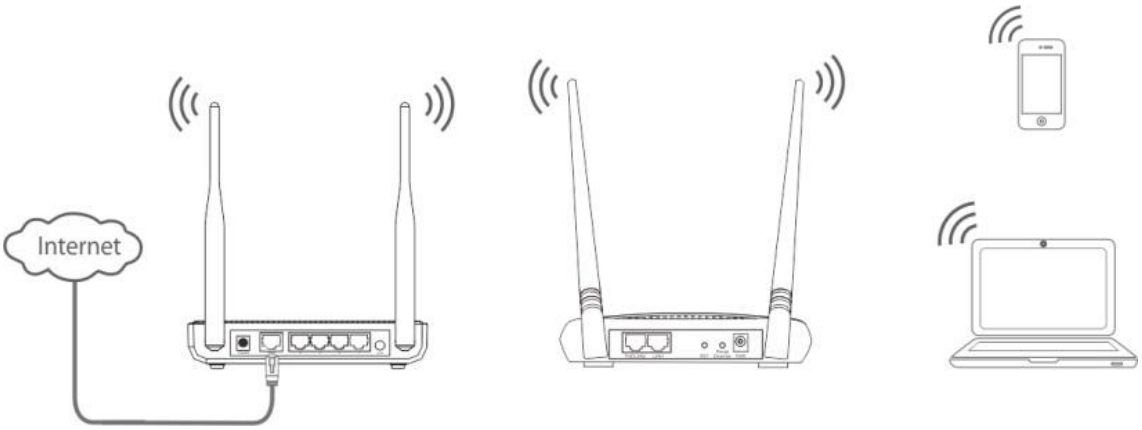
Solution

To meet the requirement, you can set the AP to **Universal Repeater** mode to extend the WiFi network of your existing WiFi router.

Assume that the SSID and password of your existing router are shown as follows:

- **SSID**: Tenda_ABCDEF
- **Password**: week7878

Network topology

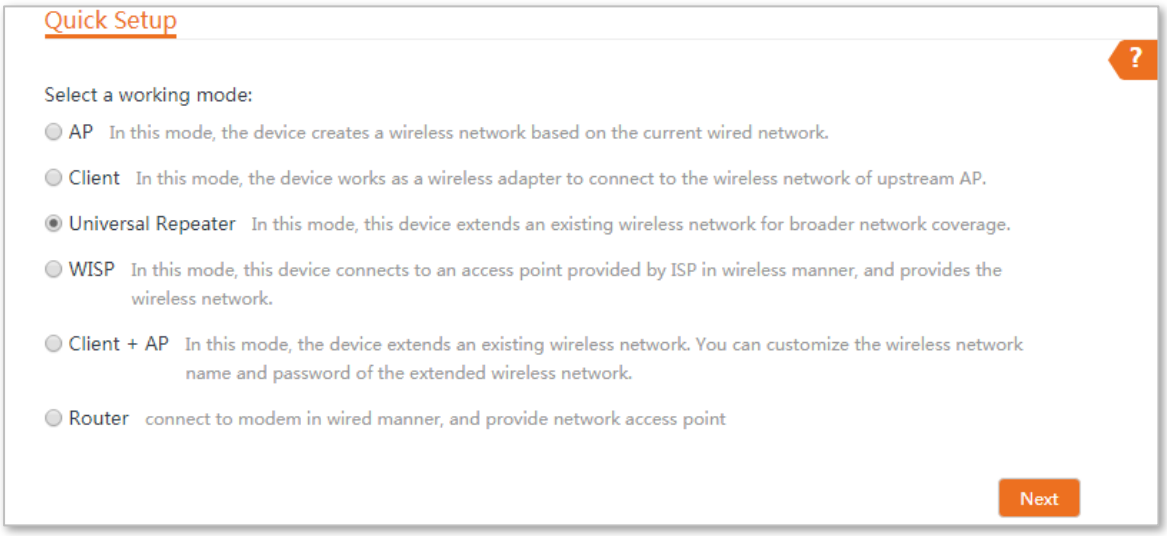


Configuration procedure

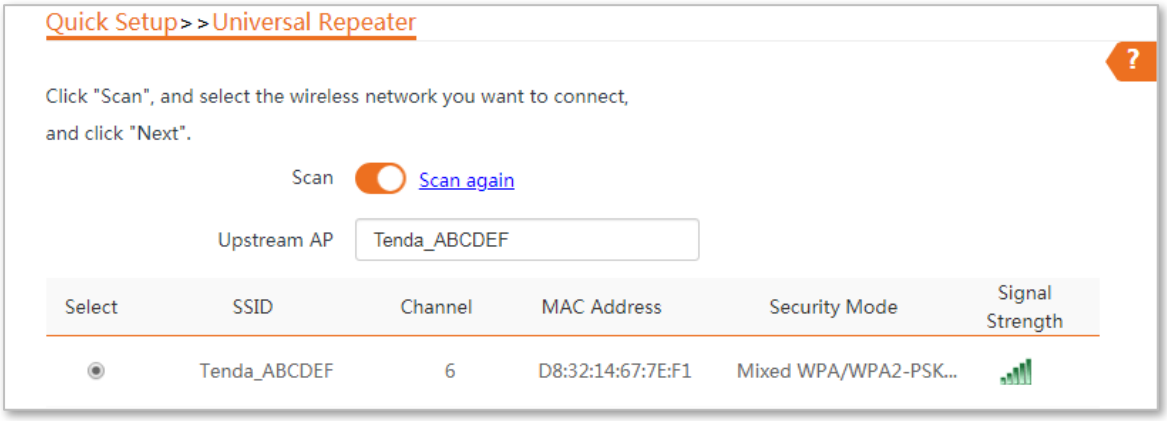
Step 1 Place the AP near your existing WiFi router, and power it on.

Step 2 Log in to the web UI of the AP and choose **Quick Setup** to enter the configuration page.

Step 3 Select **Universal Repeater**, and click **Next**.



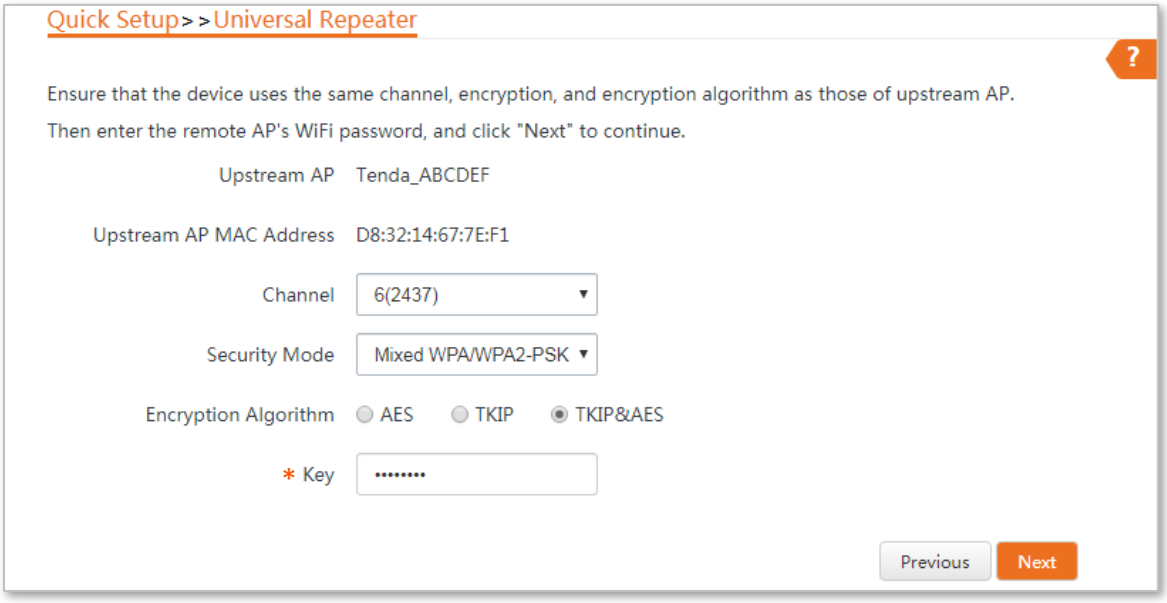
Step 4 Select the SSID of the router, which is **Tenda_ABCDEF** in this example, and click **Next**.



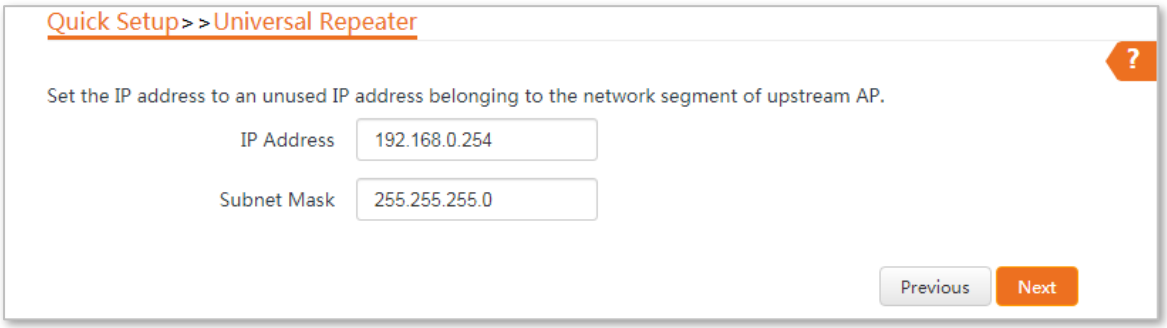
TIP

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

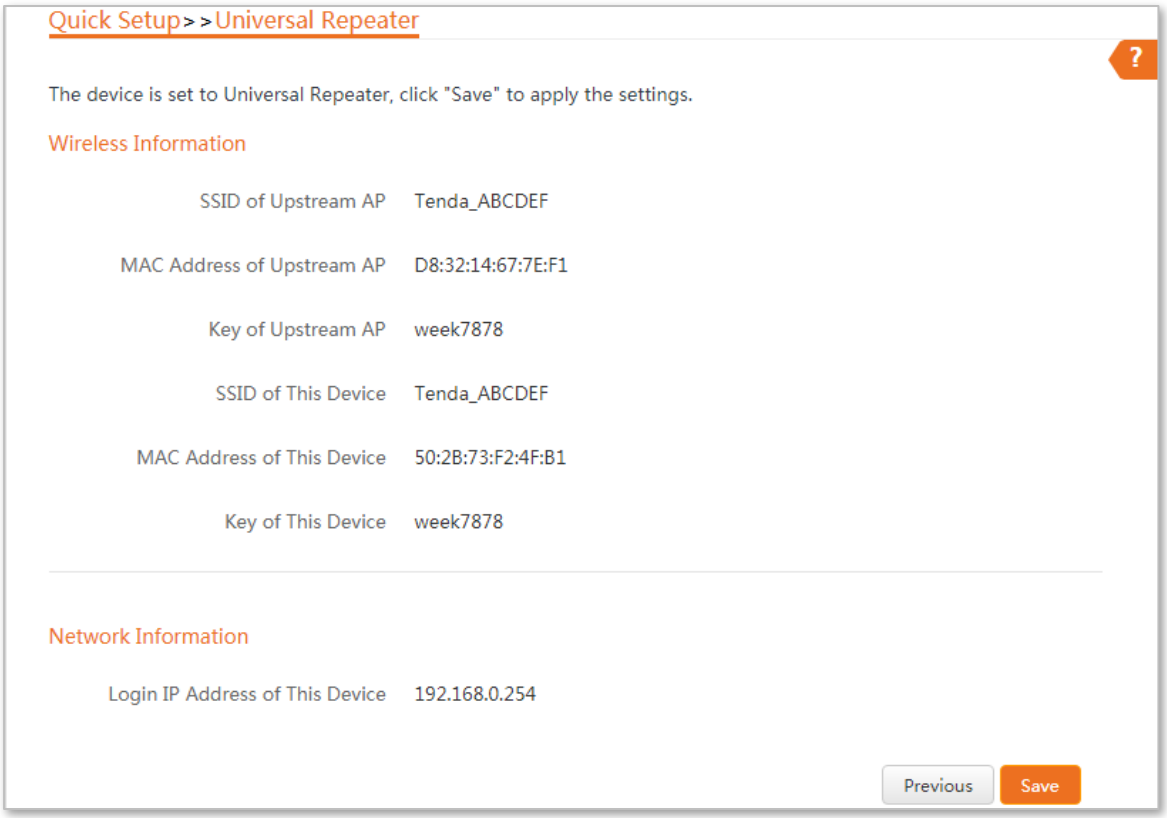
Step 5 Enter the WiFi password of the router in the **Key** text box, and click **Next**.



Step 6 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 192.168.0.1, you can set this device's IP address to 192.168.0.*X* (*X* ranges from 2 to 254). Then click **Next**.



Step 7 Check whether the SSID you select and WiFi password you enter are correct. Then click **Save**.



Step 8 After the device completes reboot, relocate it:

- In a high and open area.
- Within the WiFi coverage range of your existing WiFi router.
- In the middle place between your existing WiFi router and the WiFi dead zone.

----End

Verification

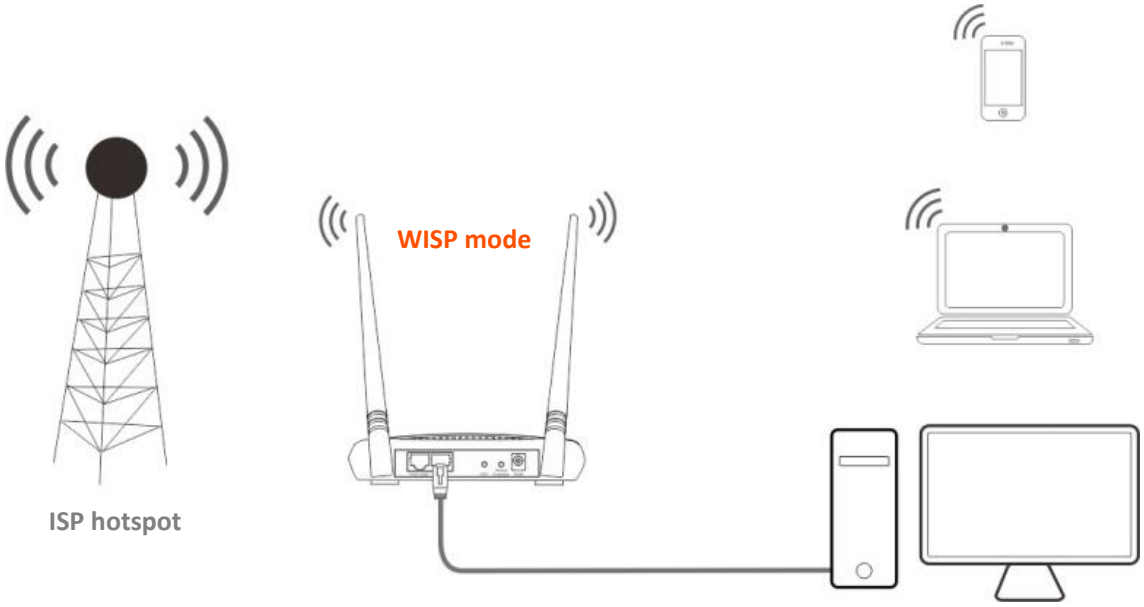
The WiFi signal is strong in bedrooms, balconies, and washing rooms. Connect wireless devices to the WiFi network of the AP using the WiFi name and password of your existing router. You can enjoy videos smoothly.

4.4 WISP mode

4.4.1 Overview

In **WISP** mode, the device connects to the hotspot provided by the internet service provider (ISP), and offers a separate WiFi network.

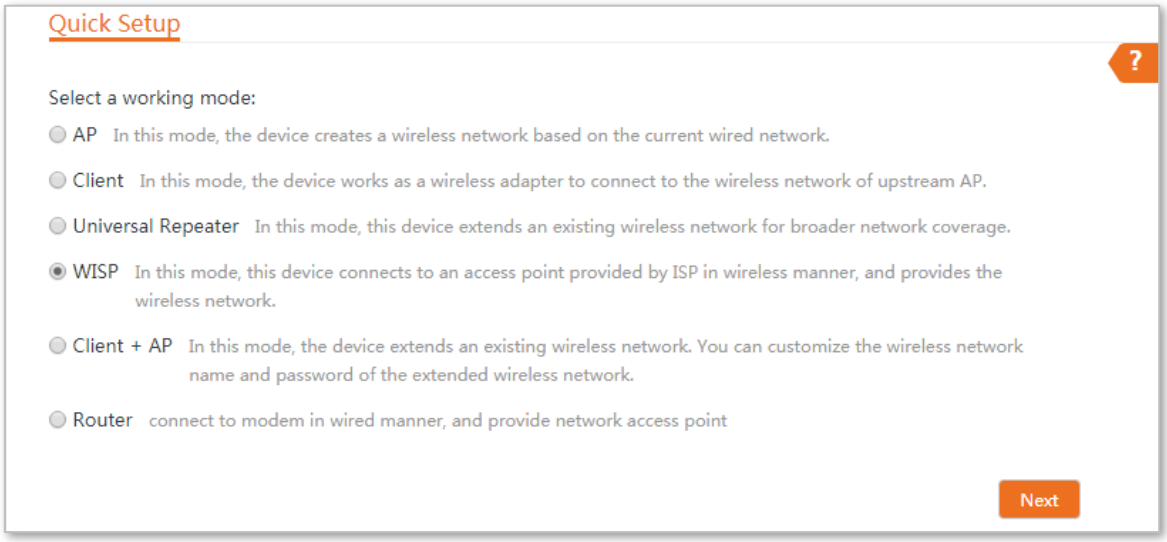
Network requirement: You want to use the AP to extend the ISP hotspot to your home, and establish a separate WiFi network for wireless clients.



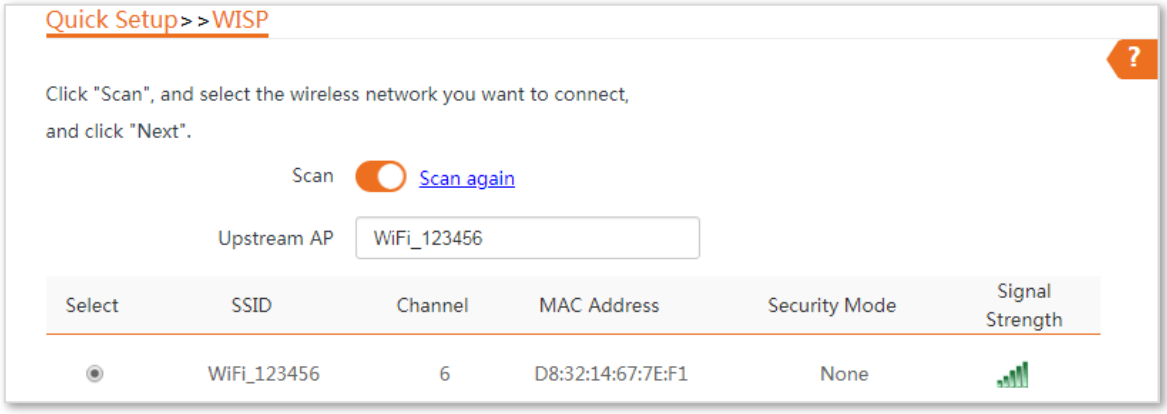
Configuration procedure of setting WISP mode

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

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



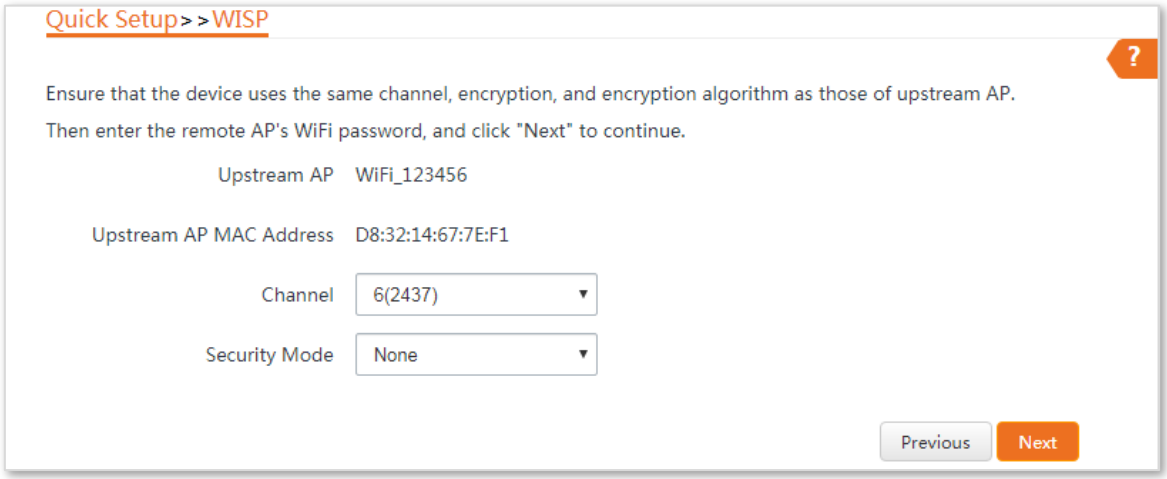
Step 3 Select the SSID of your ISP (Internet Service Provider) hotspot and click **Next** at the bottom of the page.



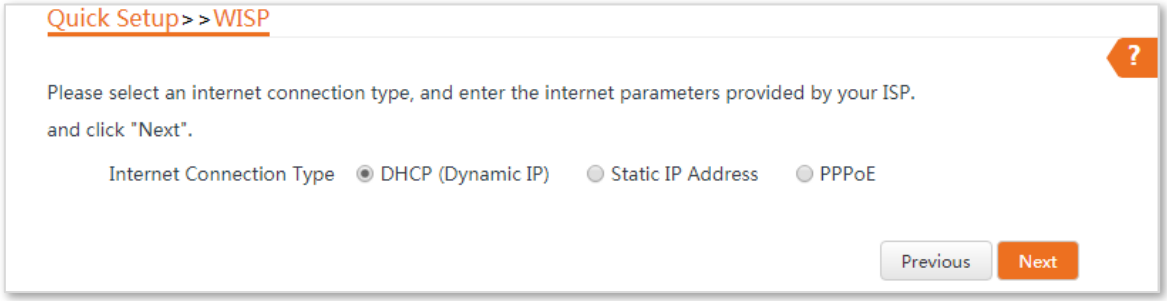
TIP

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

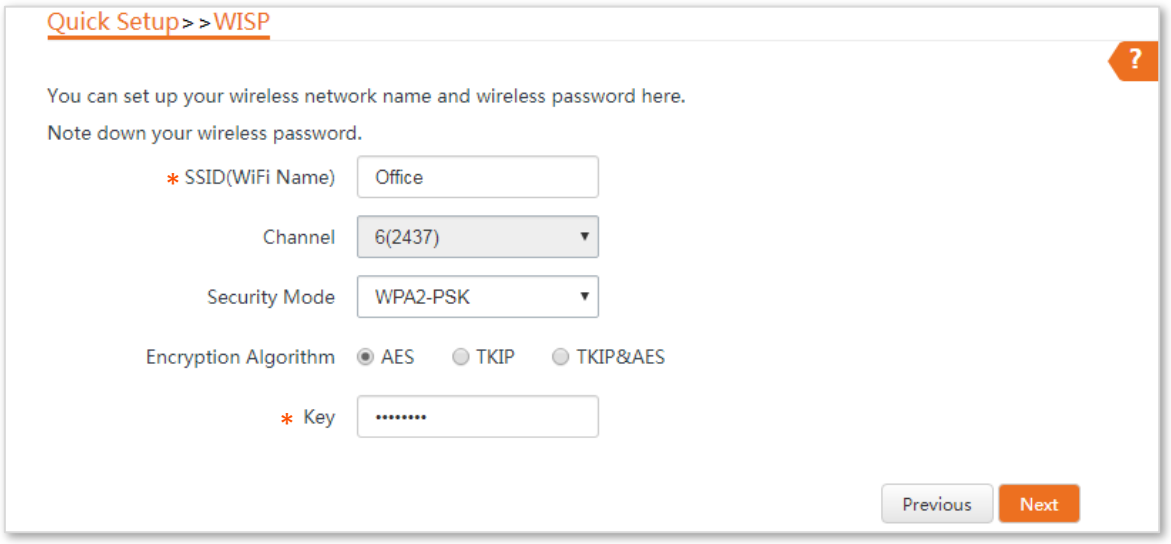
Step 4 Click **Next**.



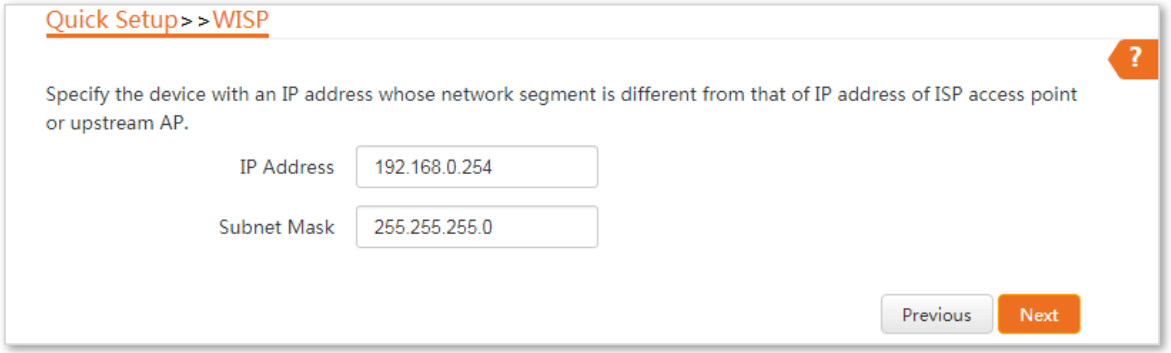
Step 5 Select the **Internet Connection Type** of your ISP hotspot, enter the internet parameters provided by your ISP (if any), and click **Next**.



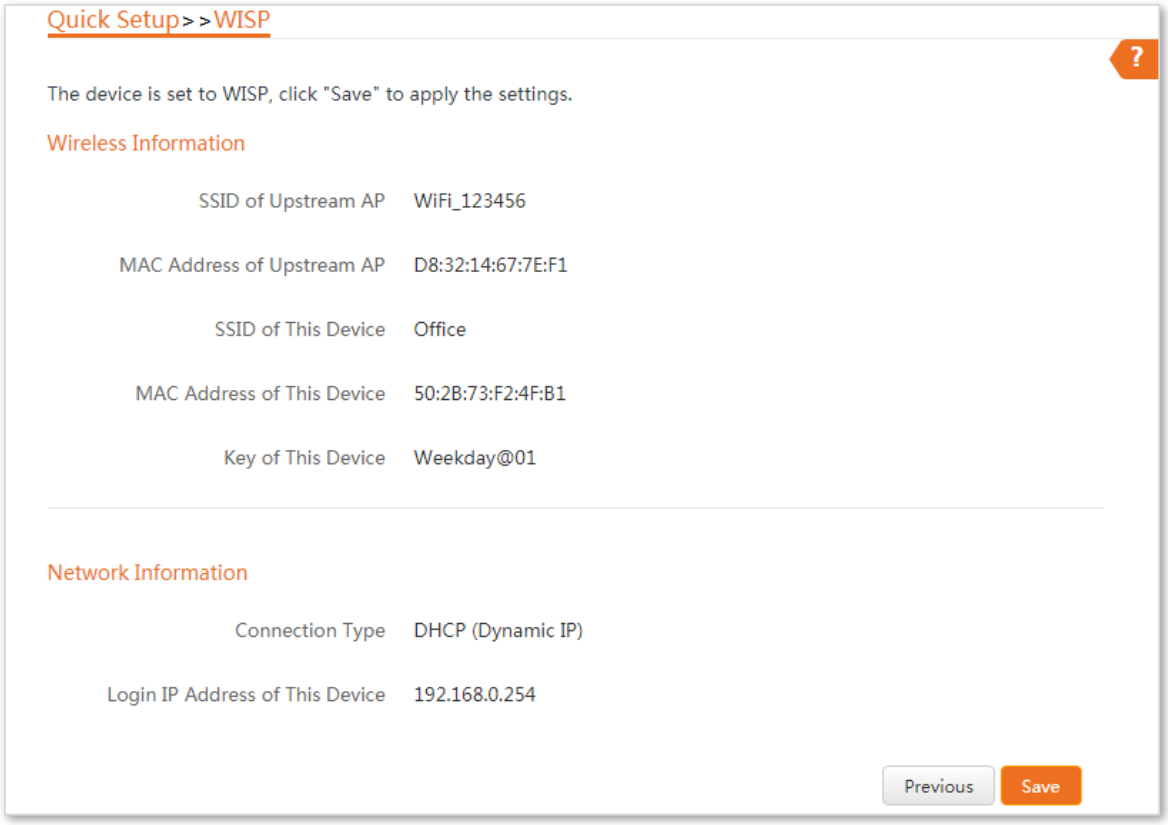
Step 6 Customize an SSID and key, and click **Next**.



Step 7 Set an IP address belonging to different network segment of your ISP hotspot. For example, if the IP address of your ISP hotspot is 192.168.5.1, you can set this device's IP address to 192.168.*X*.254 (*X* ranges from 0 to 254 excluding 5) which is also the login IP address of the AP. Then click **Next**.



Step 8 Note down the **SSID** and **Key** of this device and keep them well. Then click **Save**.



----End

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **WISP** mode: In this mode, the device connects to the hotspot provided by the wireless internet service provider (WISP), and offers a separate WiFi network.
Upstream AP	It specifies the WiFi 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, including: None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.
Internet Connection Type/Connection Type	• **DHCP (Dynamic IP)**: The device obtains IP address and other parameters from the DHCP server of upstream device for internet access. • **Static IP Address**: The device accesses the internet by setting the IP address, subnet mask, default gateway and DNS server IP addresses manually. • **PPPoE**: The device accesses the internet using the PPPoE user name and password provided by the ISP.

4.4.2 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

You can set the AP to WISP mode, and bridge to the ISP hotspot.

Assume that:

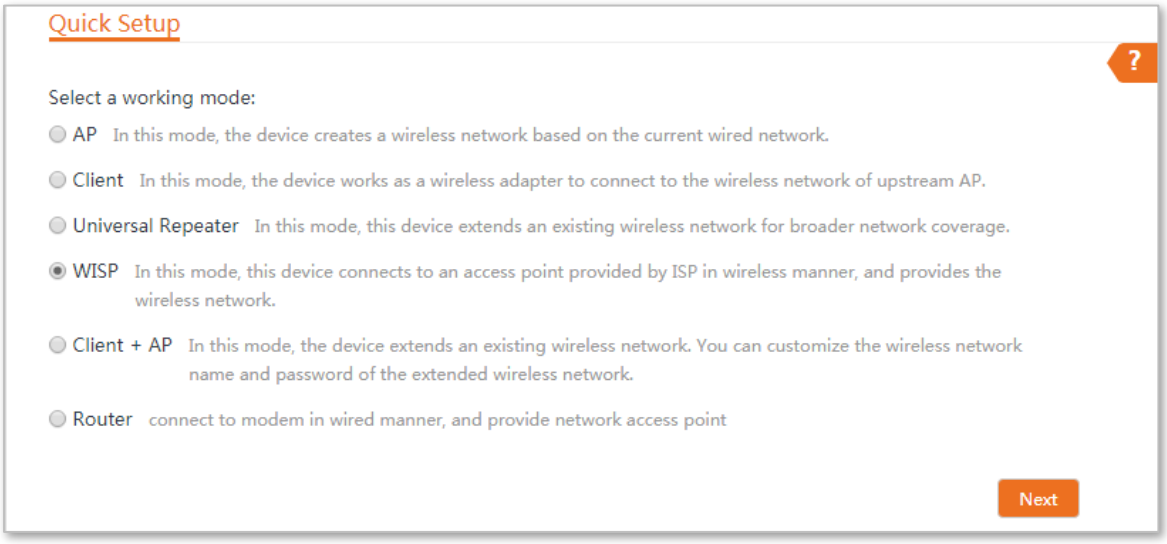
- SSID the ISP hotspot is **WiFi_123456**
- No WiFi password
- Internet connection type is PPPoE, and PPPoE user name and password are both **admin**

Network topology

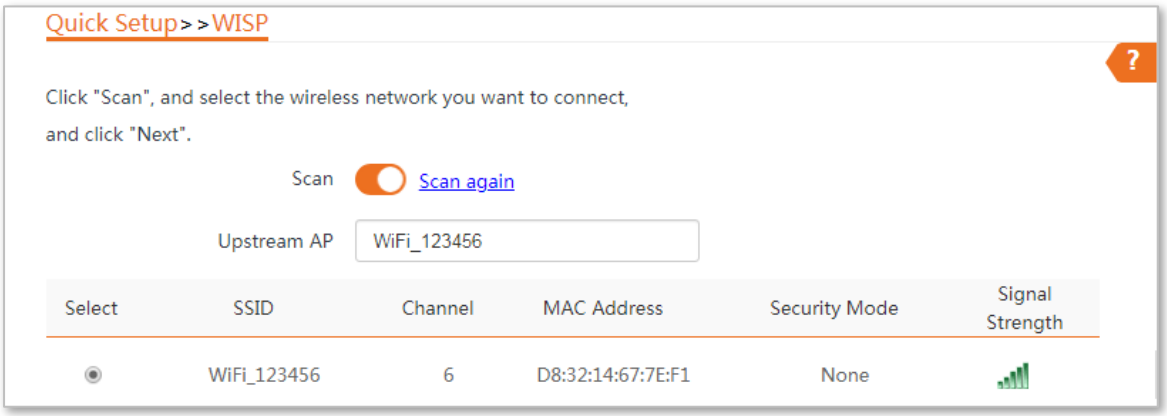
Configuration procedure

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

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



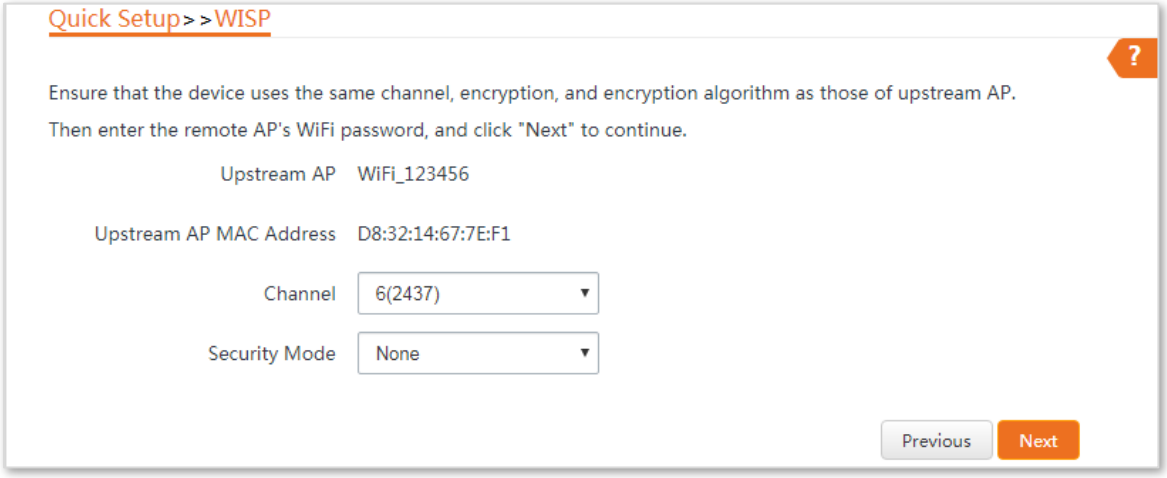
Step 3 Select the SSID of your ISP (Internet Service Provider) hotspot, which is **WiFi_123456** in this example, and click **Next**.



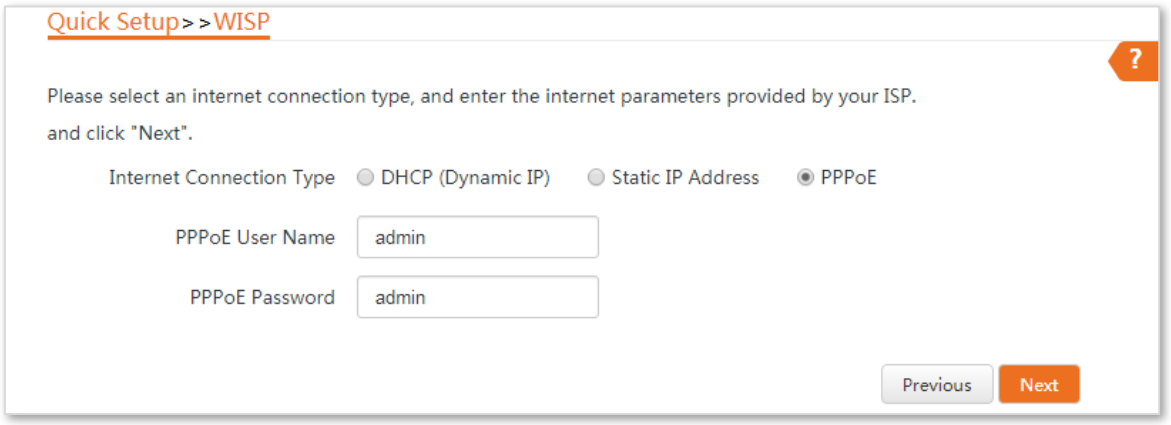
TIP

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

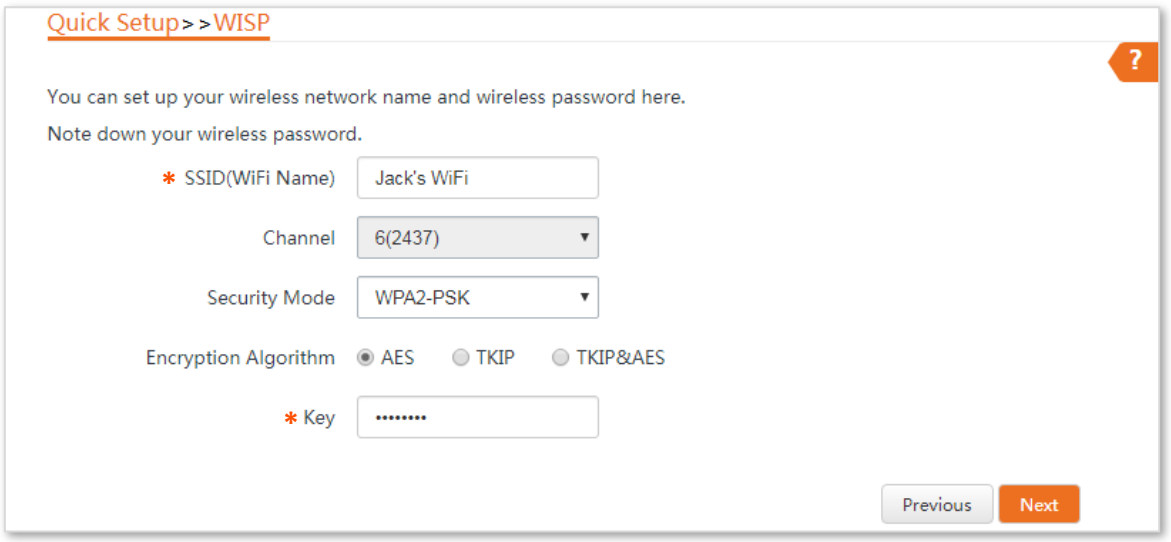
Step 4 Click **Next**.



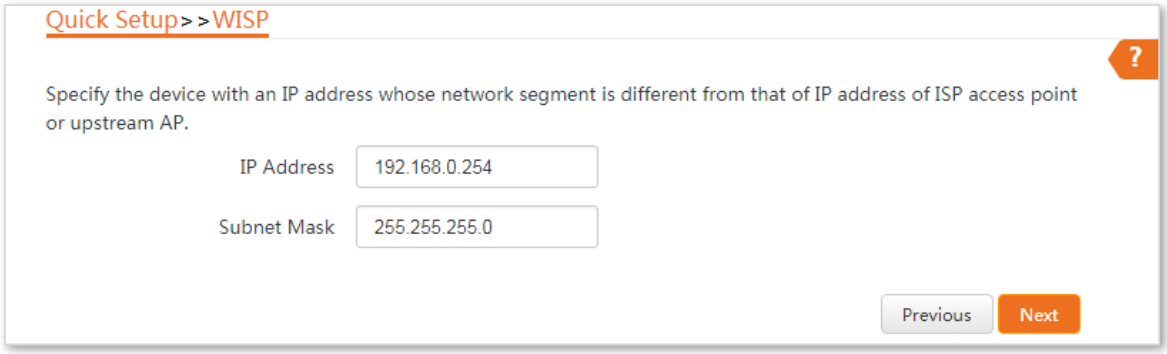
Step 5 Select the **Internet Connection Type** of your ISP hotspot, which is **PPPoE** in this example. Enter the PPPoE user name and password provided by your ISP, and click Next.



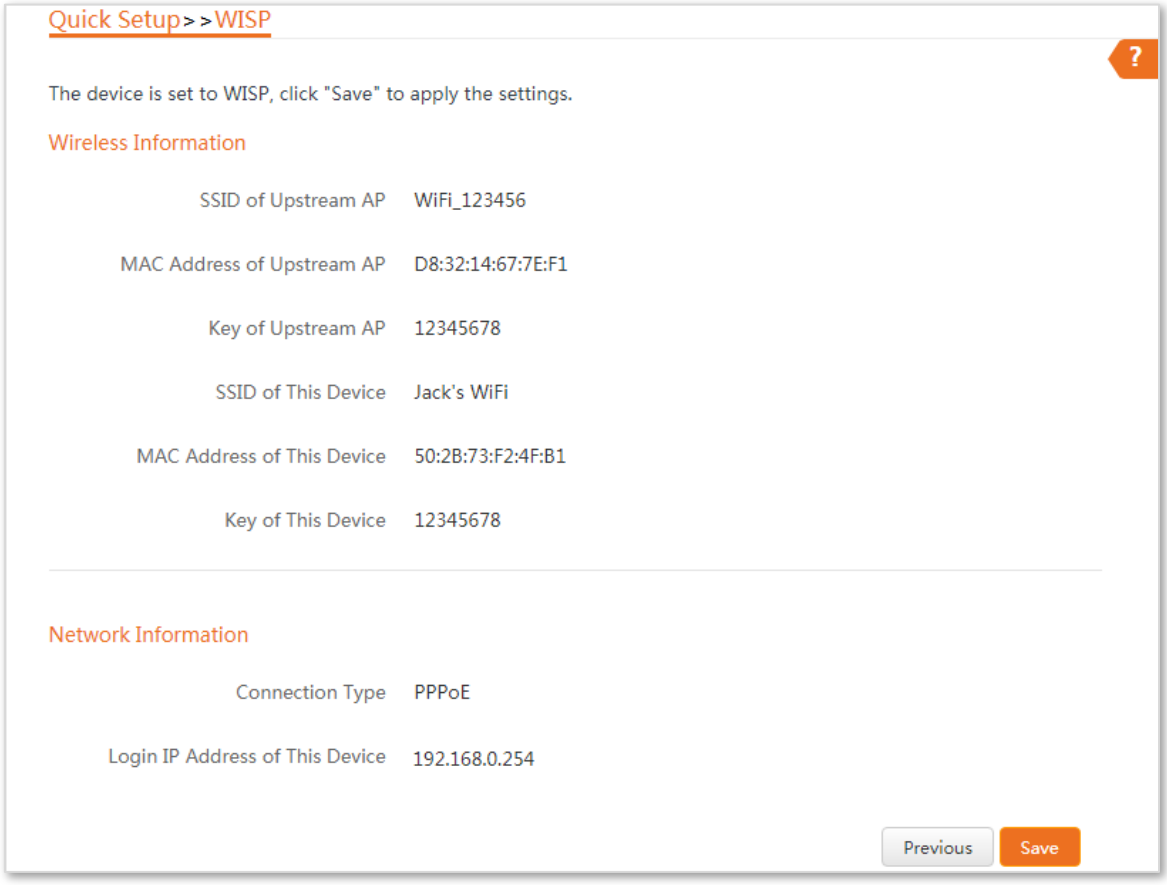
Step 6 Customize an **SSID** and **Key**, and click **Next**.



Step 7 Set an IP address belonging to different network segment of your ISP hotspot. For example, if the IP address of your ISP hotspot is 192.168.1.1, you can set this device's IP address to 192.168.*X*.254 (*X* ranges from 0 to 254 excluding 1) which is also the login IP address of the AP. Then click **Next**.



Step 8 Note down the **SSID** and **Key** of this device and keep them well. Then click **Save**.



----End

Verification

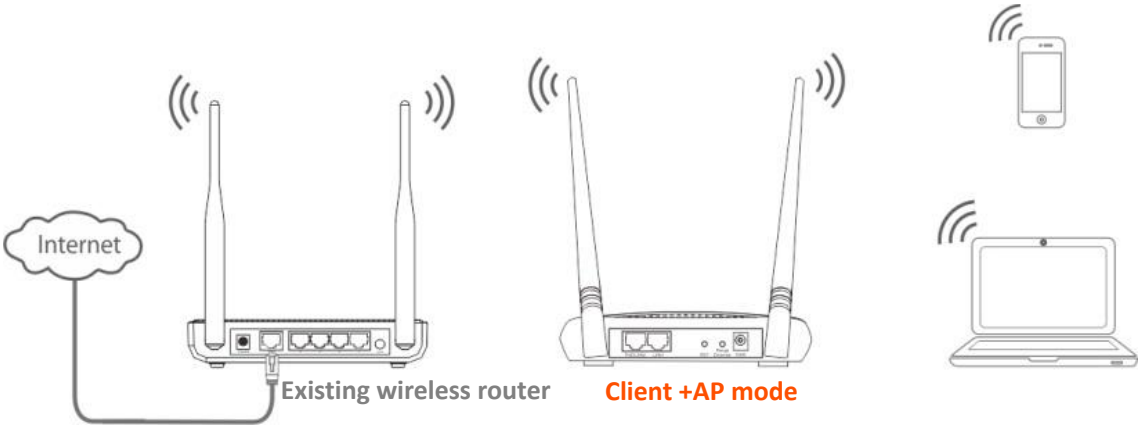
Connect wired devices to the LAN ports of the device, and wireless devices to the WiFi network using the **SSID** and **Key** you set. Both wired and wireless devices can access the internet through the device now.

4.5 Client + AP mode

4.5.1 Overview

In **Client + AP** mode, this device expands your existing WiFi network for broader network coverage, and allows you to create a separate WiFi network.

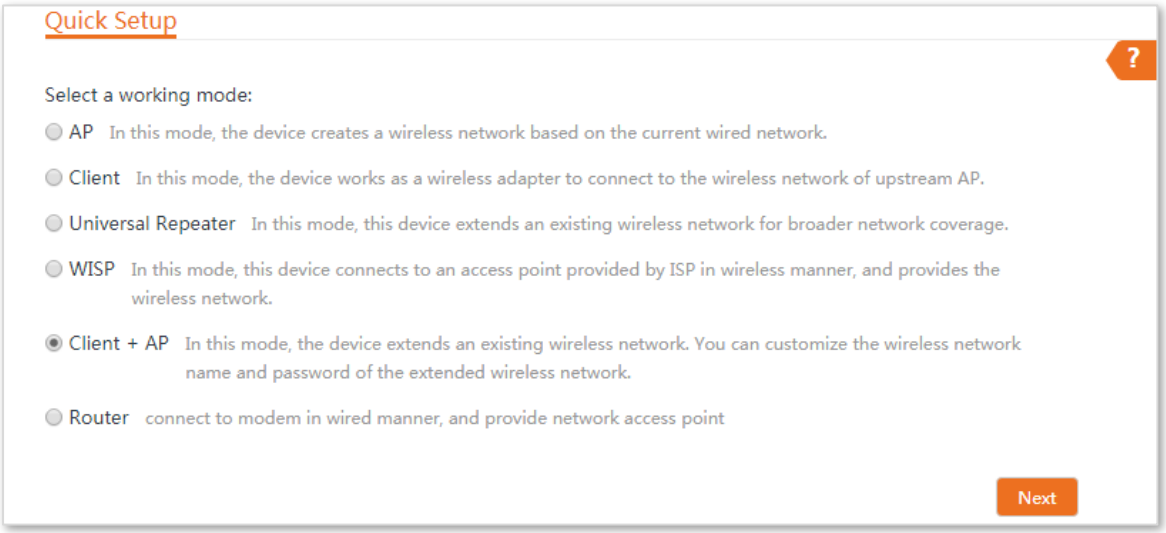
Network requirement: You want to use the AP to extend your existing WiFi network, and customize a new WiFi name and password for the WiFi network of the AP.



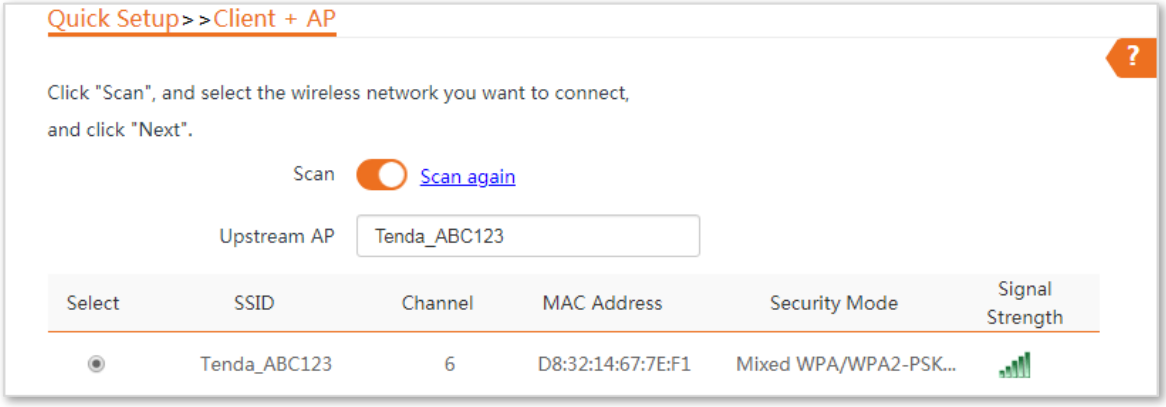
Configuration procedure of setting Client + AP mode

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

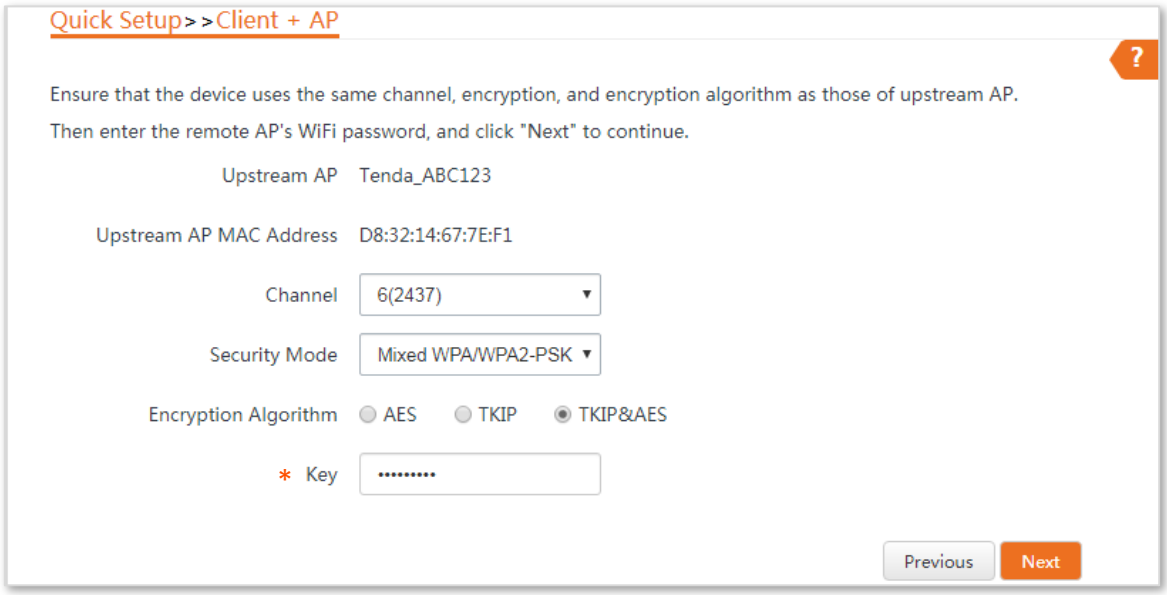
Step 2 Select **Client + AP**, and click **Next**.



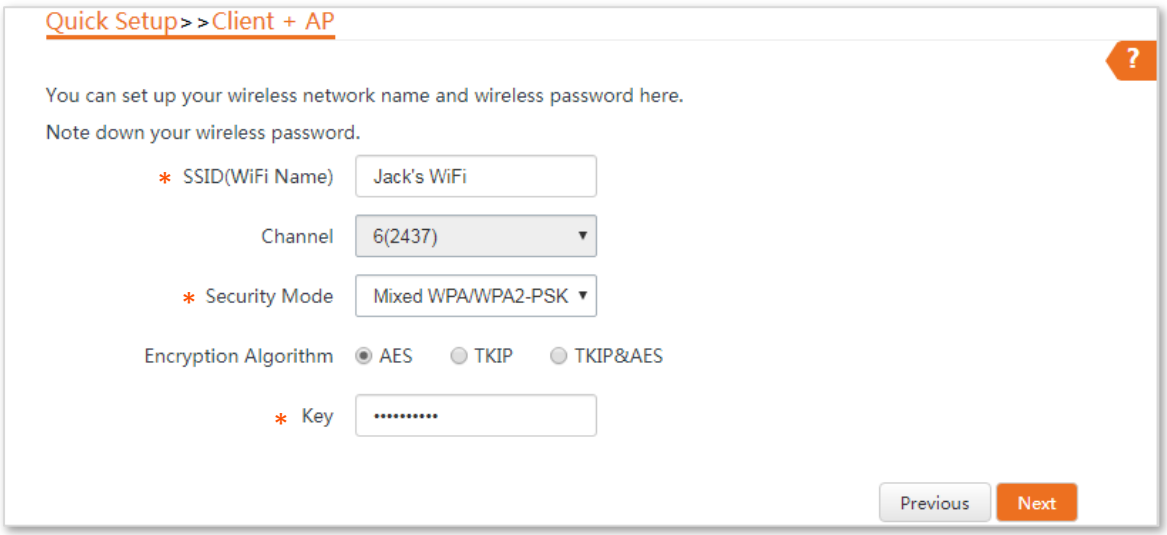
Step 3 Select the SSID of your existing wireless router and click **Next**.



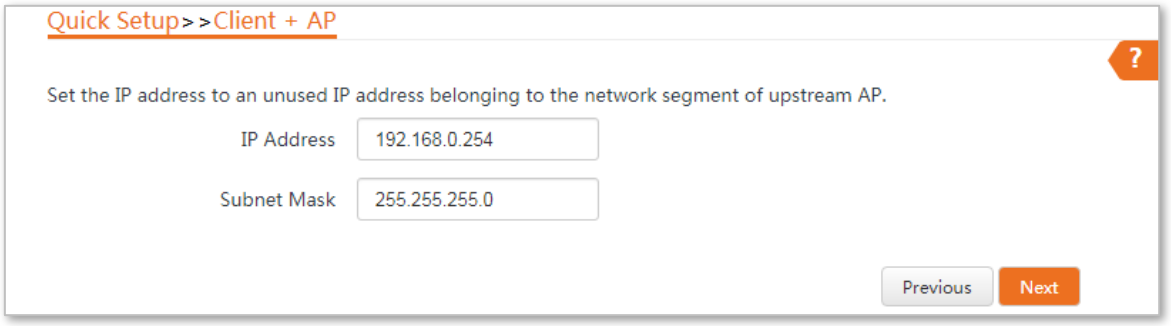
Step 4 Enter the WiFi key of the router in the **Key** text box, and click **Next**.



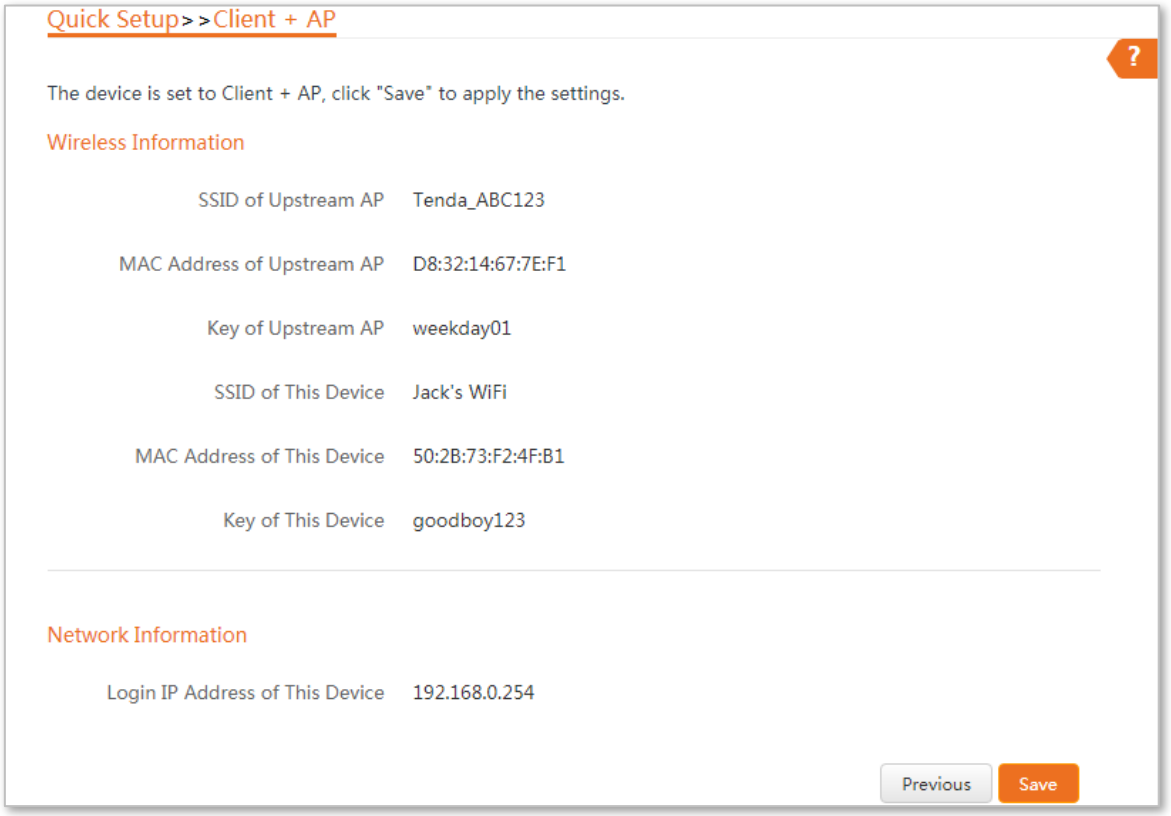
Step 5 Customize an **SSID** and **Key** for the AP, and click **Next**.



Step 6 Set the IP address to an unused IP address belonging to the same network segment of your existing wireless router. For example, if the IP address of the router is 192.168.0.1, you can set this device's IP address to 192.168.0.*X* (*X* ranges from 2 to 254). Then click **Next**.



Step 7 Note down the **SSID** and **Key** of this device and keep them well. Then click **Save**.



----End

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **Client + AP** mode: In this mode, this device expands your existing WiFi network for broader network coverage, and allows you to create a separate WiFi network.
Upstream AP	It specifies the SSID (WiFi name) of the upstream AP.

Parameter	Description
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, including: None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

4.5.2 Example of Client + AP mode

Network requirement

You already have a wireless router and place it in the dining room for internet access, but in some places at home, such as bedrooms, balconies, and washing rooms, the WiFi signal is weak. Now you want to have a larger WiFi network coverage through his home, and customize a new SSID and key for the new WiFi network.

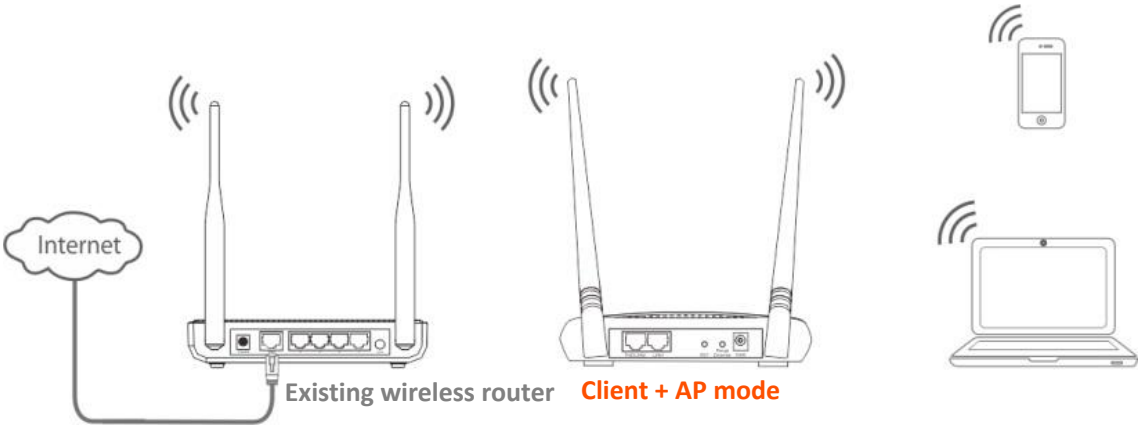
Solution

To meet the requirement, you can set the AP to **Client + AP** mode to extend the WiFi network of your existing router.

Assume that the SSID and key of your existing router are shown as follows:

- **SSID**: Tenda_ABC123
- **Password**: goodboy123

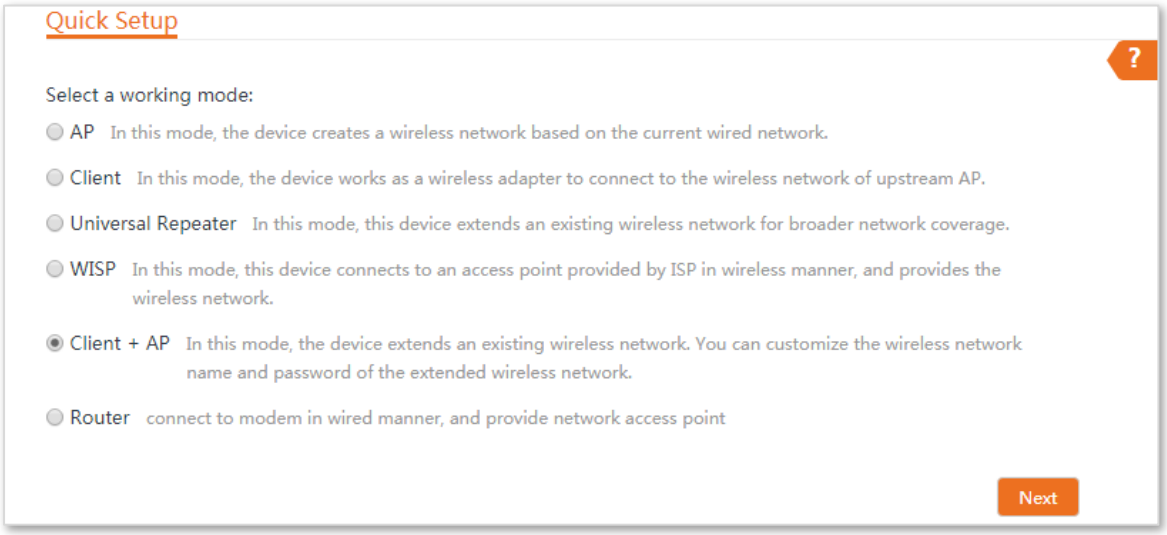
Network topology



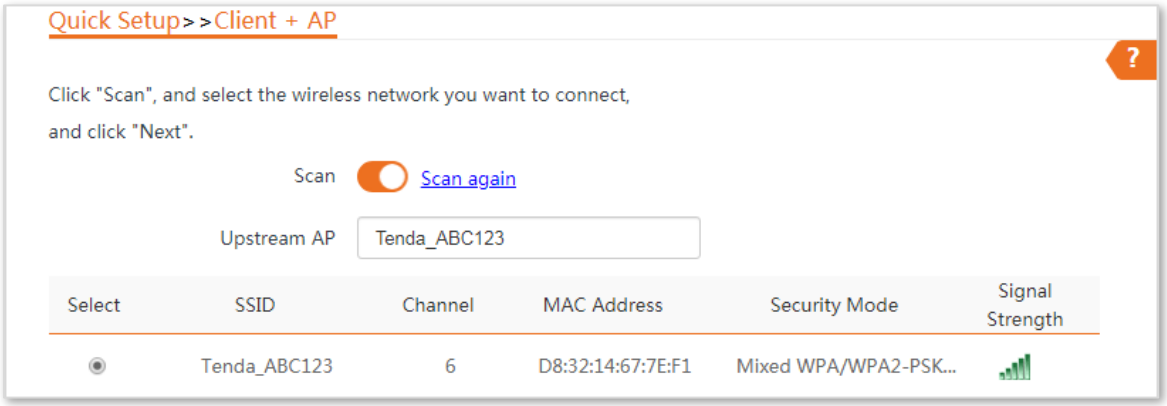
Configuration procedure

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

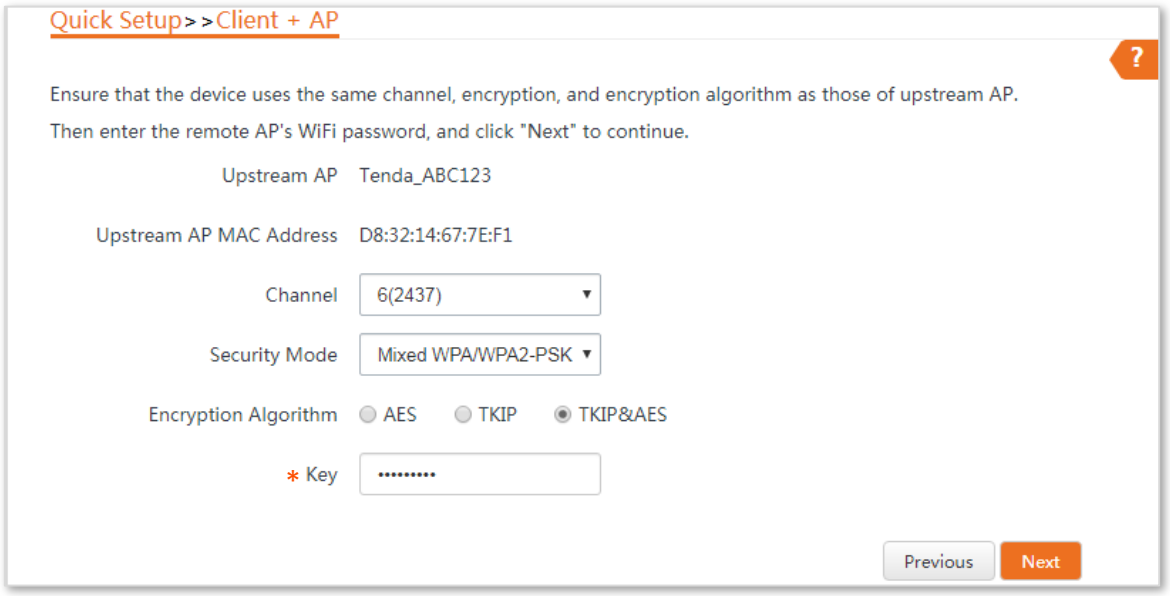
Step 2 Select **Client + AP**, and click **Next**.



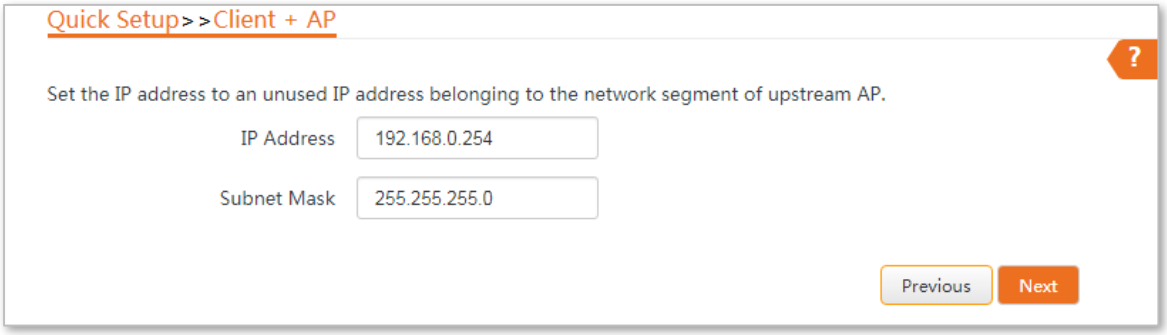
Step 3 Select the SSID of your existing wireless router, which is **Tenda_ABC123** in this example, and click **Next**.



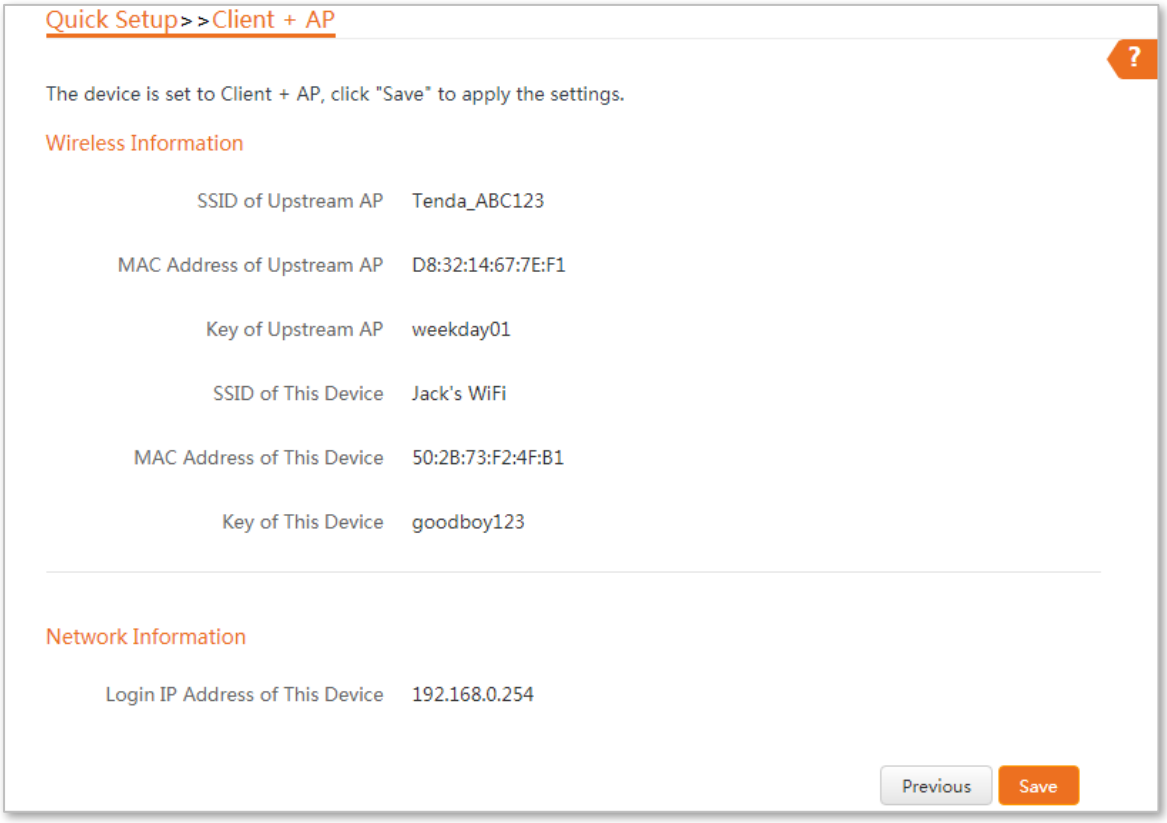
Step 4 Enter the WiFi key of the router in the **Key** text box, and click **Next**.



Step 5 Set the IP address to an unused IP address belonging to the same network segment of the router. For example, if the IP address of the router is 192.168.0.1, you can set this device's IP address to 192.168.0.*X* (*X* ranges from 2 to 254). Then click **Next**.



Step 6 Note down the **SSID** and **Key** of this device and keep them well. Then click **Save**.



----End

Verification

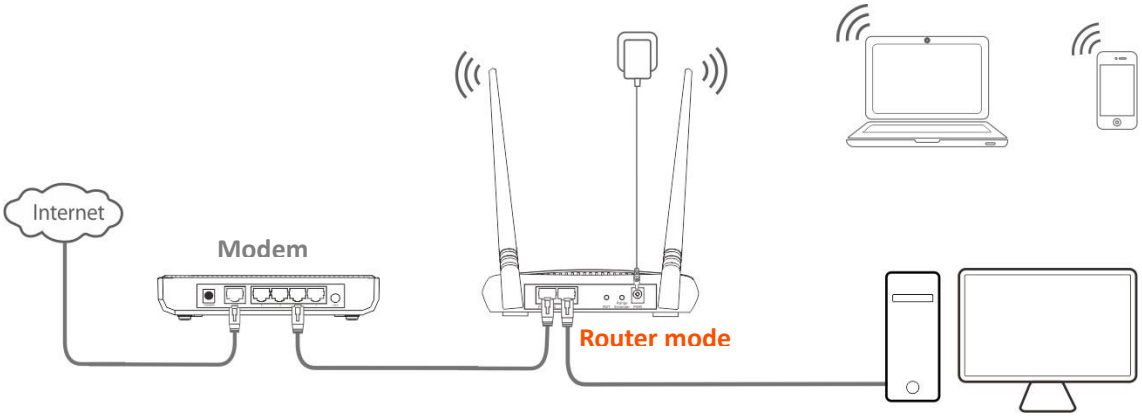
The WiFi signal is strong in bedrooms, balconies, and washing rooms. Connect wireless devices to the WiFi network of the AP using the WiFi name and password you customize. You can enjoy videos smoothly.

4.6 Router mode

4.6.1 Overview

In Router mode, this device serves as a router to provide internet access for wired and wireless clients. The PoE/WAN/LAN2 port functions as a WAN port used to connect to the internet.

Network requirement: You want to use the AP to provide a WiFi network to provide internet access for wired and wireless clients.

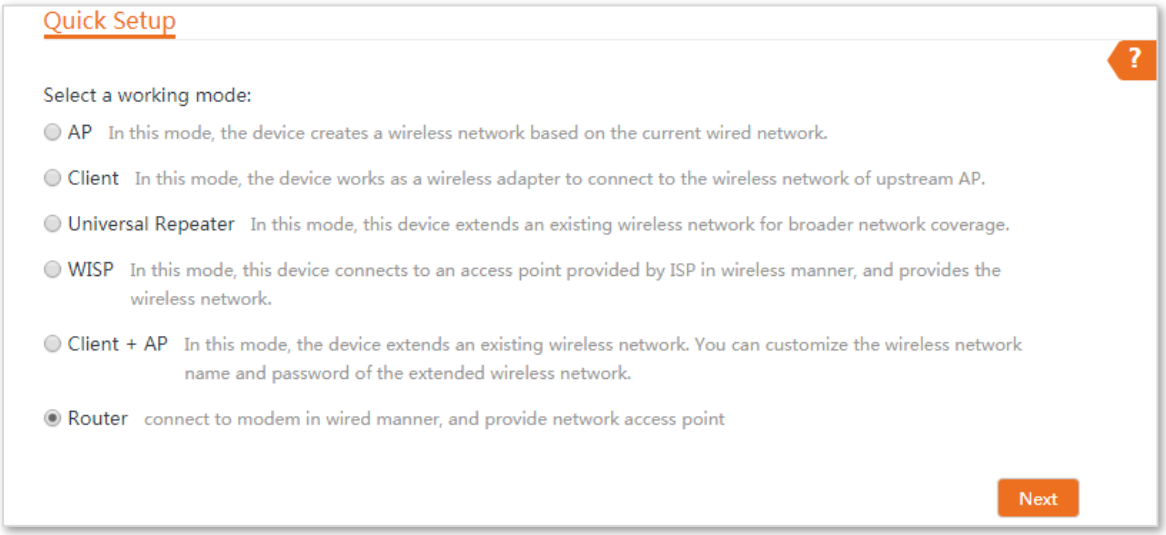


Configuration procedure of setting Router mode

Step 1 Connect a computer to the LAN1 port of the AP.

Step 2 Log in to the web UI of the AP, and choose **Quick Setup** to enter the configuration page.

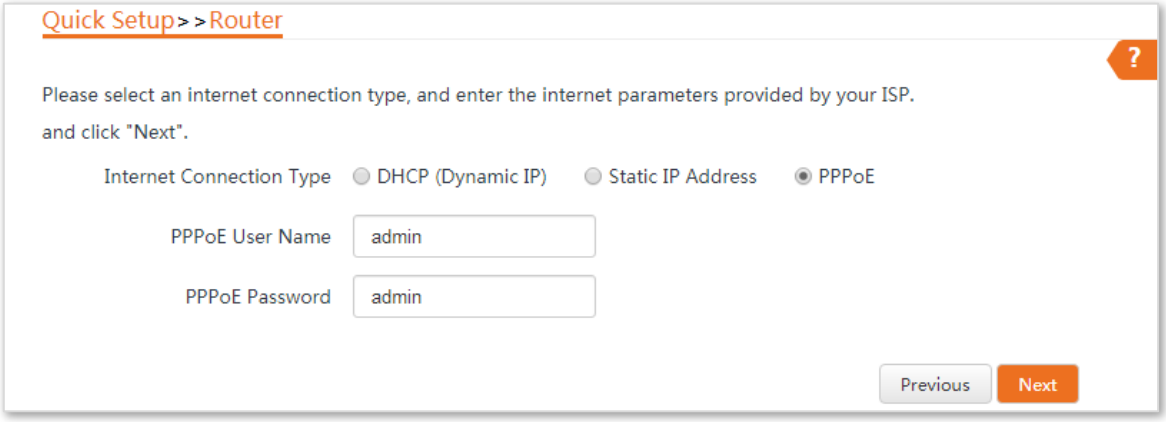
Step 3 Select **Router** mode, and click **Next**.



Step 4 Select your internet connection type, and set the related parameters. Take **PPPoE** as an example here.

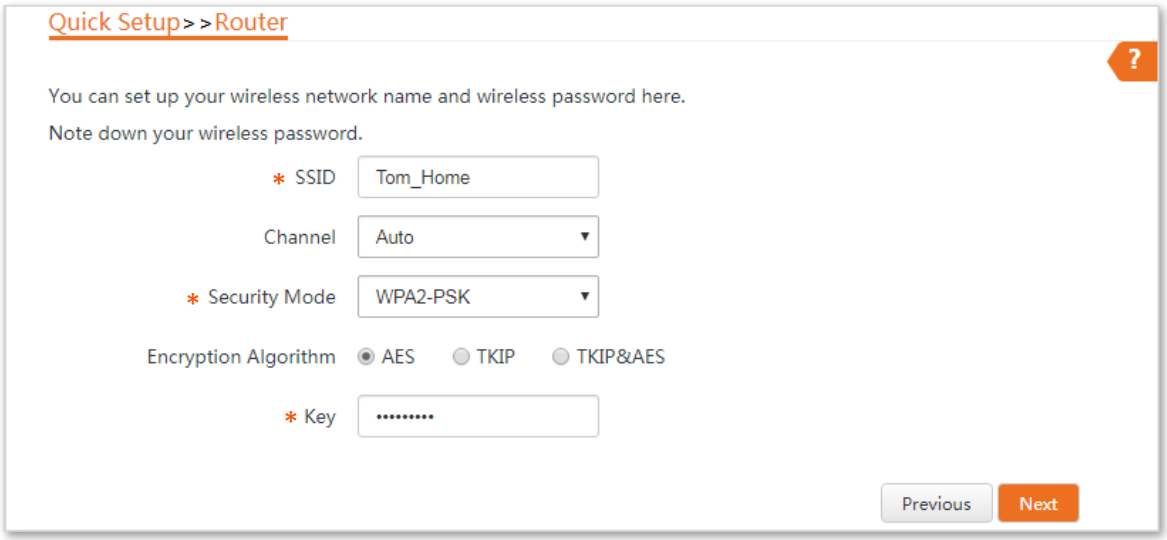
1. Select **PPPoE**.
2. Enter the PPPoE user name and password provided by your ISP, which are both **admin** in this example.

3. Click **Next**.

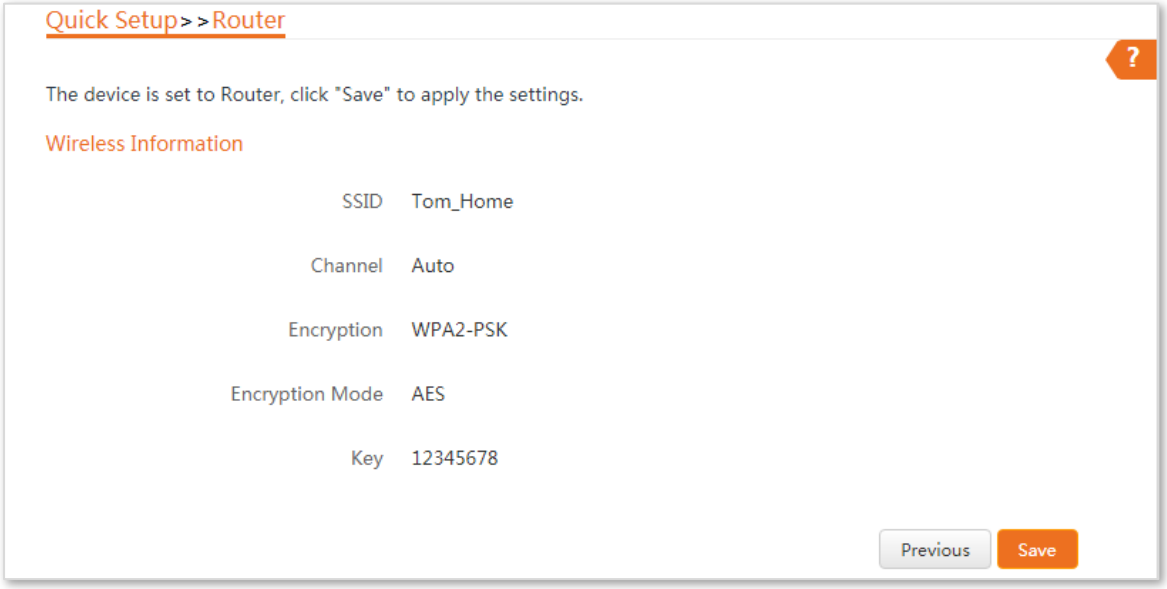


Step 5 Set wireless parameters of the AP.

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



Step 6 Note down the **SSID** and **Key** of this device and keep them well. Then click **Save**.



----End

Parameters description

Parameter	Description
Working modes	It specifies the working mode of this device. **Router** mode: In this mode, this device serves as a router to provide internet access for wired and wireless clients. The PoE/WAN/LAN2 port functions as a WAN port used to connect to the internet.
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 WiFi name of the device.
Channel	It specifies the operating channel of this device. **Auto** (Default): It indicates that the device automatically adjusts its operating channel according to the ambient environment.
Security Mode	It specifies the security mode of the WiFi network of the device. It includes None, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

4.6.2 Example of router mode

Network requirement

You only have a modem at home for internet access, and only one client can access the internet through the modem at one time. Now you want to use the device to serve as a wireless router to share the internet service with multiple clients.

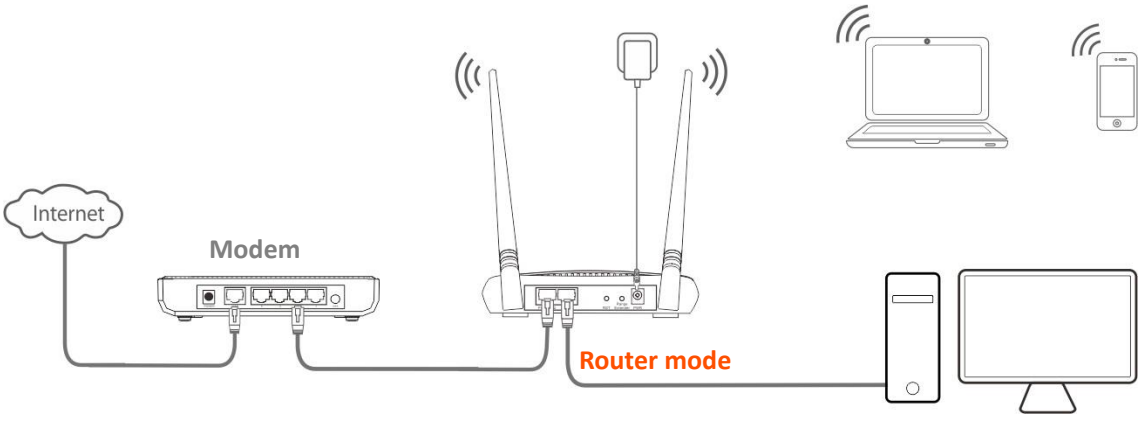
Solution

Set the AP to Router mode.

Assume that:

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

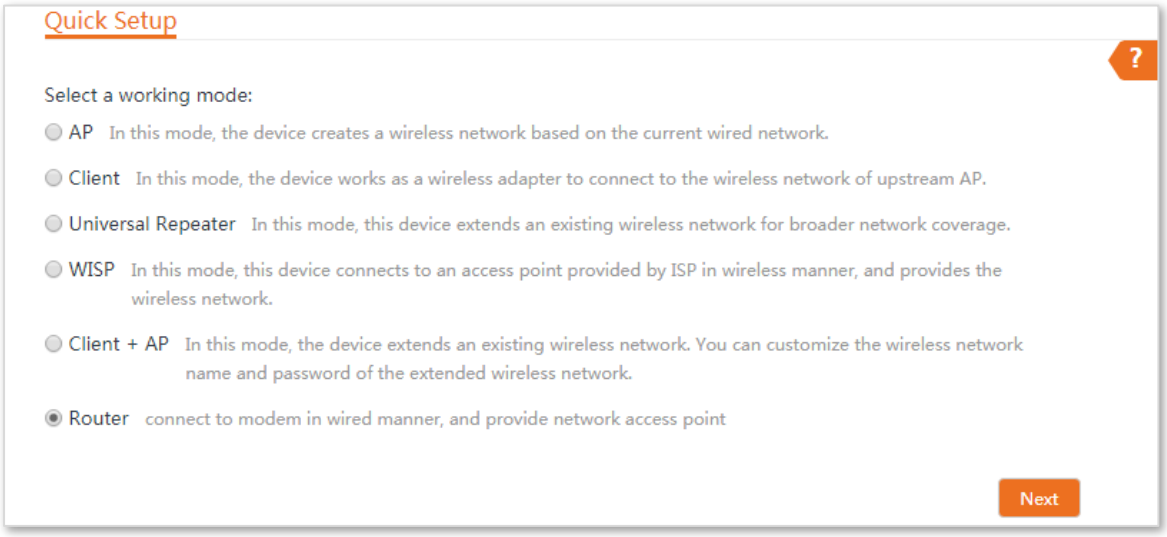
Network topology



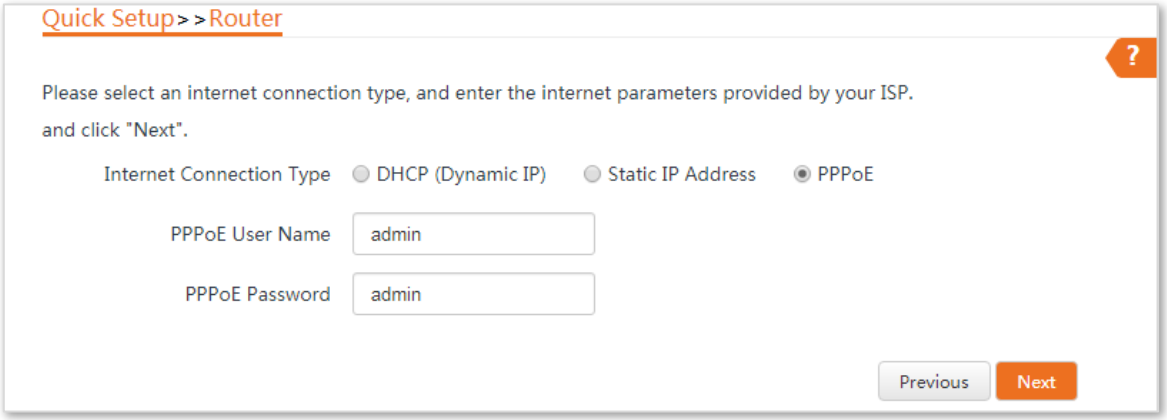
Configuration procedure

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

Step 2 Select **Router** mode, and click **Next**.

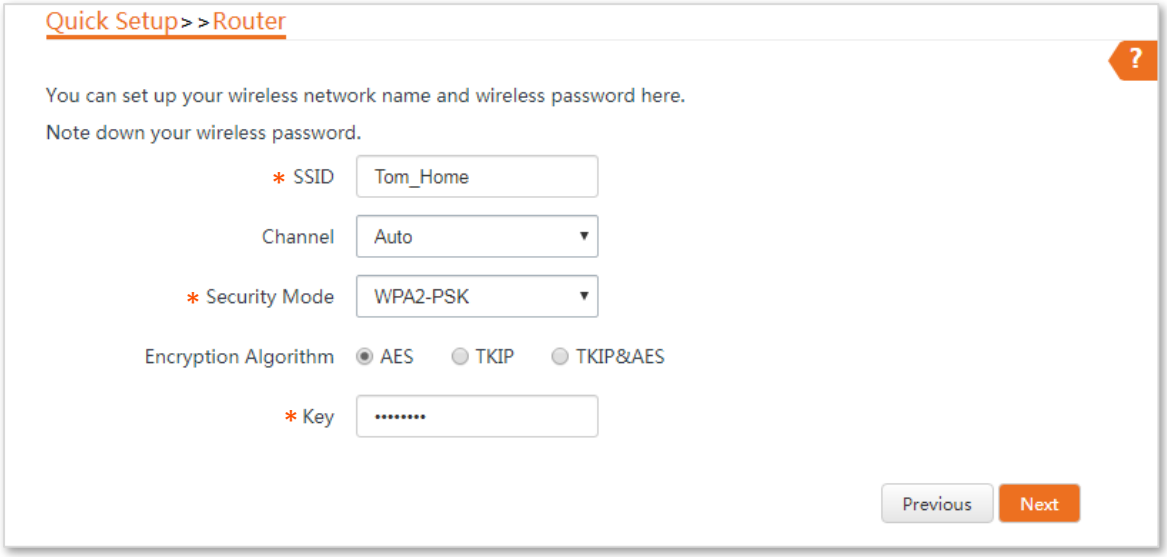


Step 3 Select **PPPoE**, enter **admin** in both **PPPoE User Name** and **PPPoE Password** input boxes, and click **Next**.

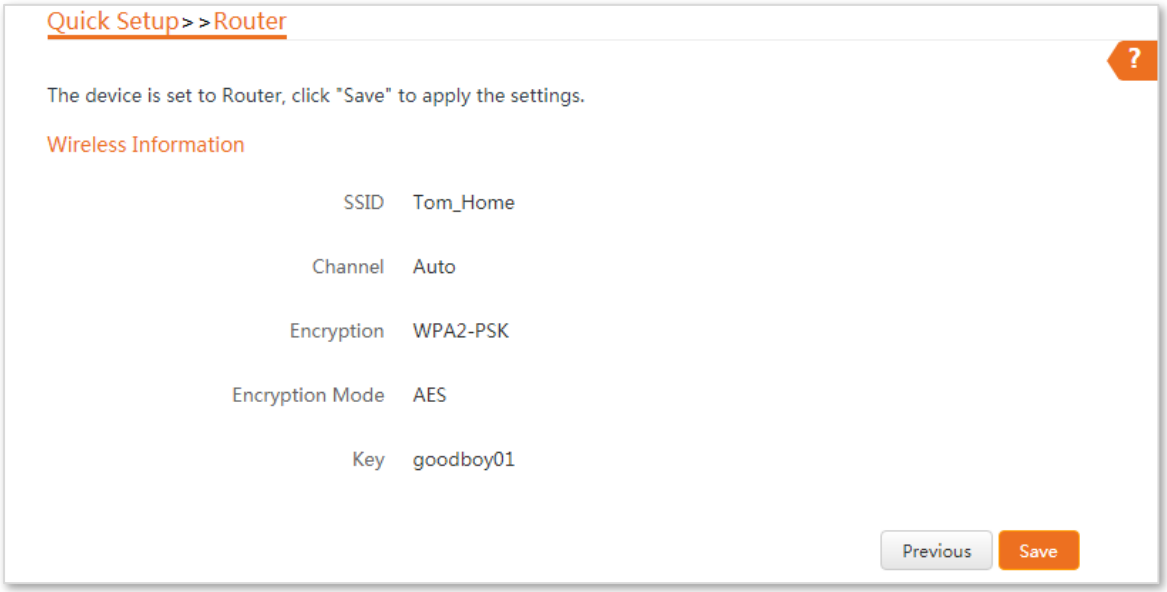


Step 4 Set wireless parameters of the device.

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



Step 5 Note down the **SSID** and **Key** of this device and keep them well. Then click **Save**.



----End

Verification

Wireless devices connected to the WiFi network (**Tom_Home**) of the device can access the internet.

The Wired device connected to the LAN1 port can access the internet.

5 Network

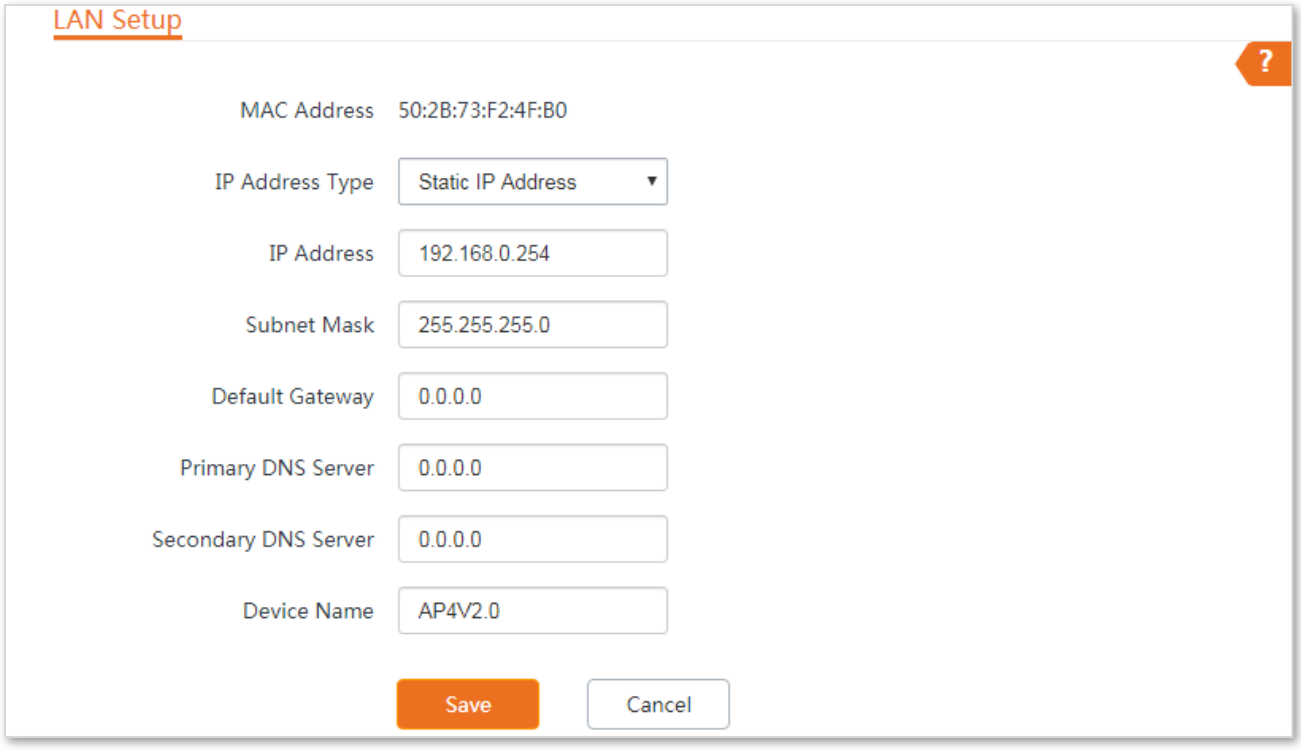
5.1 LAN setup

5.1.1 Overview

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

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

In **AP**, **Client**, **Universal Repeater** and **Client + AP** modes, the page displays:

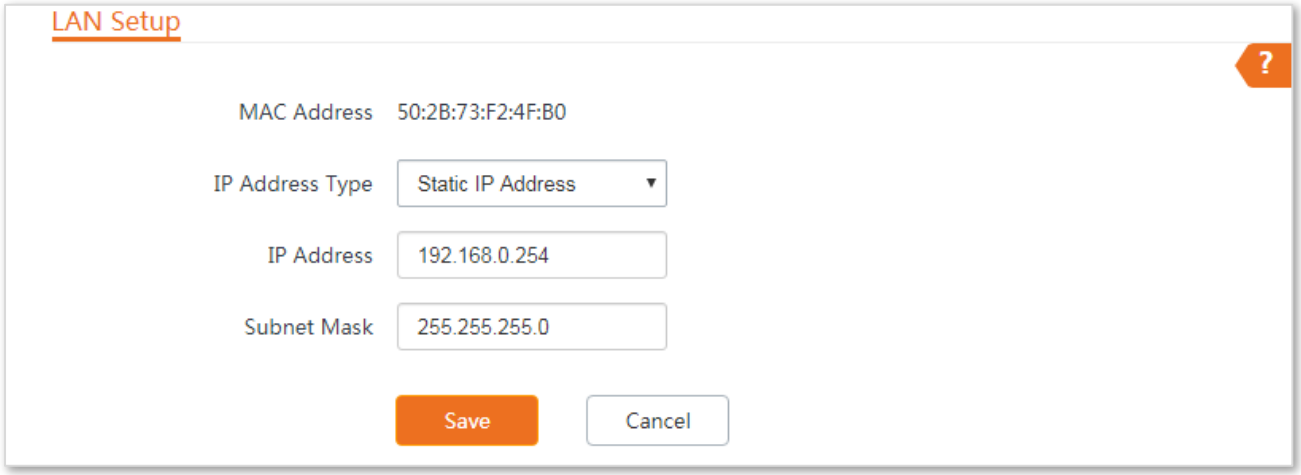


Parameters description

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**. • **Static IP Address**: Specify the IP address, subnet mask, default gateway, and DNS server IP addresses manually. • **DHCP (Dynamic IP Address)**: The device obtains an IP address, subnet mask, default gateway and DNS server IP address from the DHCP server to which it

Name	Description
	connects. 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 to which it connects, and use this IP address to log in.
IP Address	It specifies the LAN IP address of the device. The default is **192.168.0.254**.
Subnet Mask	It specifies the subnet mask of the device. The default is **255.255.255.0**.
Default Gateway	It specifies the default gateway of the device. You can set it to the IP address of the egress router to enable the device to access the internet.
Primary DNS Server	It specifies the primary DNS server IP address of the device. If the egress router has the DNS agent function, you can manually set this parameter to the LAN IP address of the egress router.
Secondary DNS Server	Optional. It specifies the secondary DNS server IP address of the device.
Device Name	It specifies the name of the device. The default name indicates the product model and version. A unique device name helps you manage multiple devices that are of the same model on LAN easily. You are allowed to modify only when the device works in **AP**, **Client**, **Universal Repeater**, or **Client + AP** mode.

In **WISP** and **Router** modes, the page displays:



Parameters description

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**. • **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. The default is **192.168.0.254**.
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 Setting an LAN IP address manually

This method applies to a small LAN network with a few APs. With this method, you need 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:

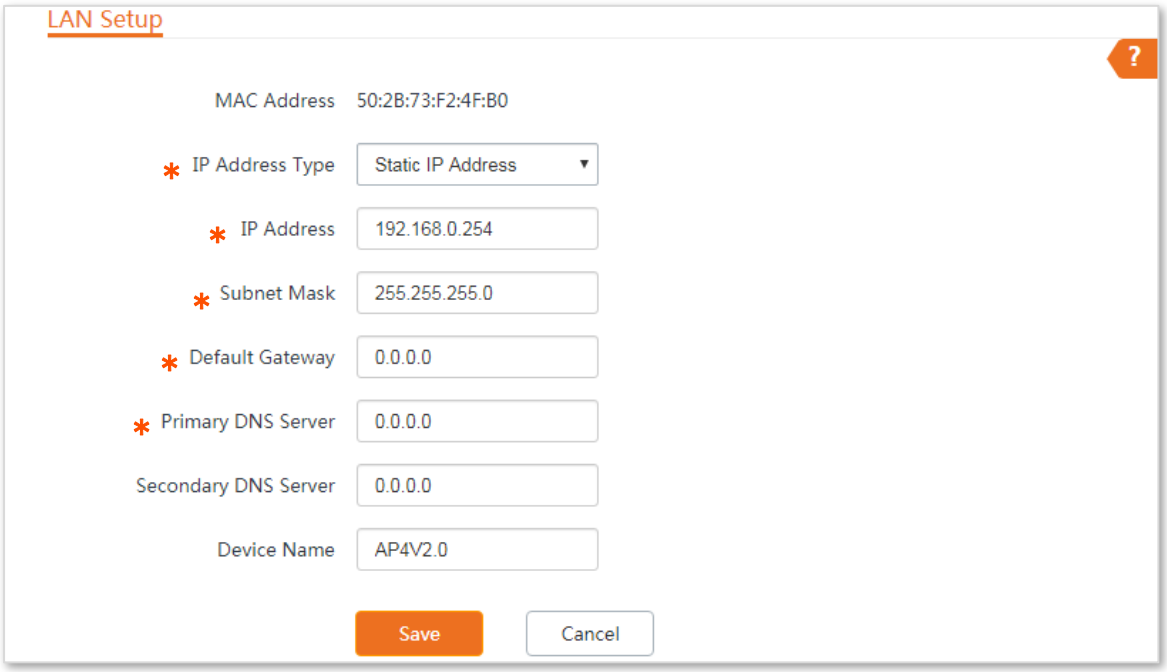
Step 1 Choose **Network** > **LAN Setup** to enter the configuration page.

Step 2 Select **Static IP Address** from the **IP Address Type** drop-down list.

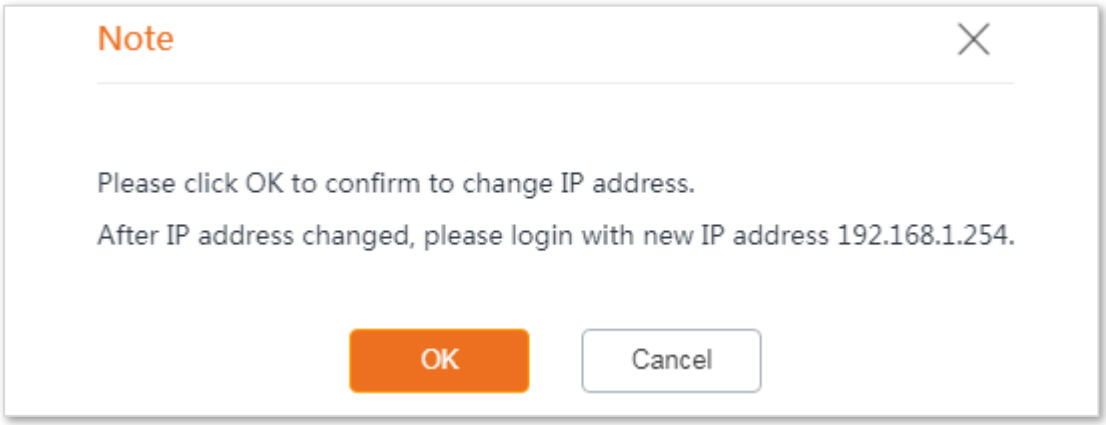
Step 3 Set **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**.

Step 4 Customize a device name as required.

Step 5 Click **Save**.



Step 6 Click **OK** on the pop-up window.



----End

5.1.3 Logging in to the web UI after changing the LAN IP address

After changing the LAN IP address, 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.

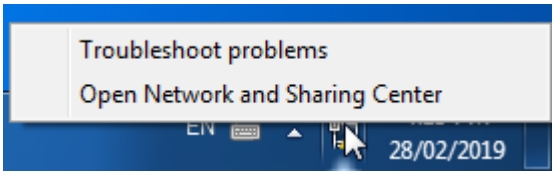
Otherwise, assign your computer an IP address that belongs to the same network segment as the new IP address of the device before login with the new IP address.

Assume that: The new IP address of the device is **192.168.1.254**, and subnet mask is **255.255.255.0**, then assign an unused IP address belonging to the same segment.

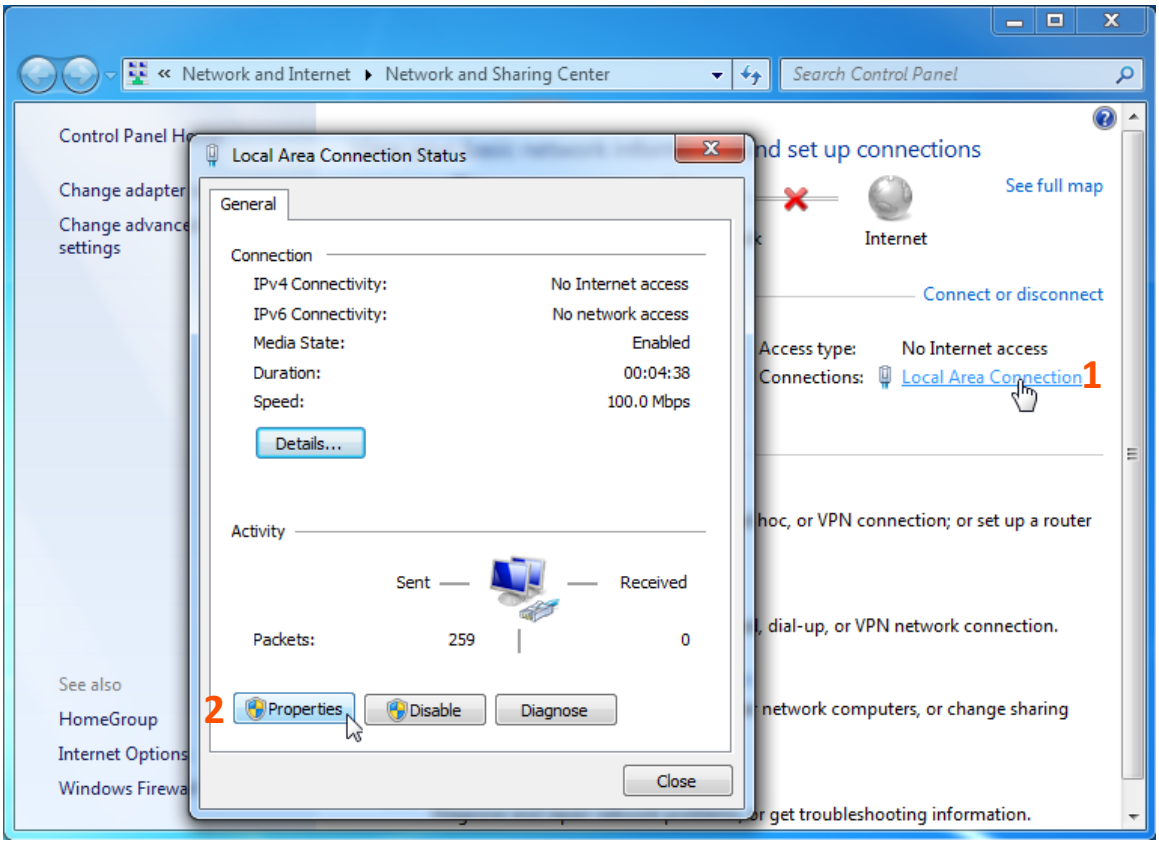
Configuration procedure (OS example: Windows 7)**:**

Step 1 Right-click the network icon on the bottom-right corner of the desktop.

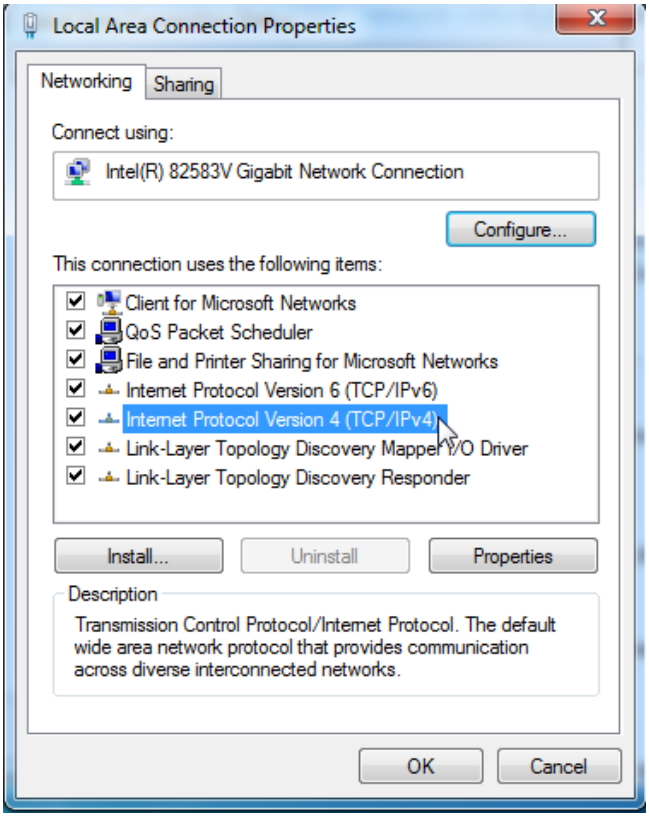
Step 2 Click **Open Network and Sharing Center**.



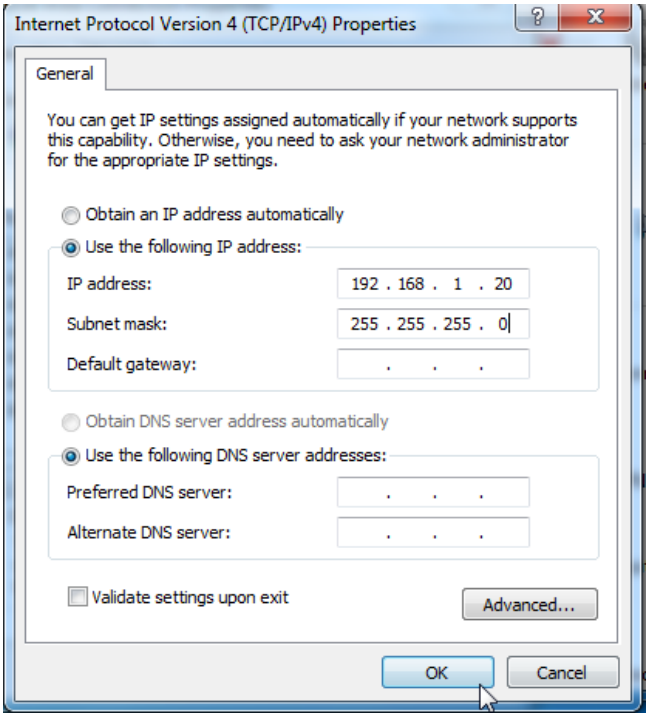
Step 3 Click **Local Area Connection**, then click **Properties**.



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



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**.



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

----End

5.1.4 Setting the device to obtaining an LAN IP address automatically

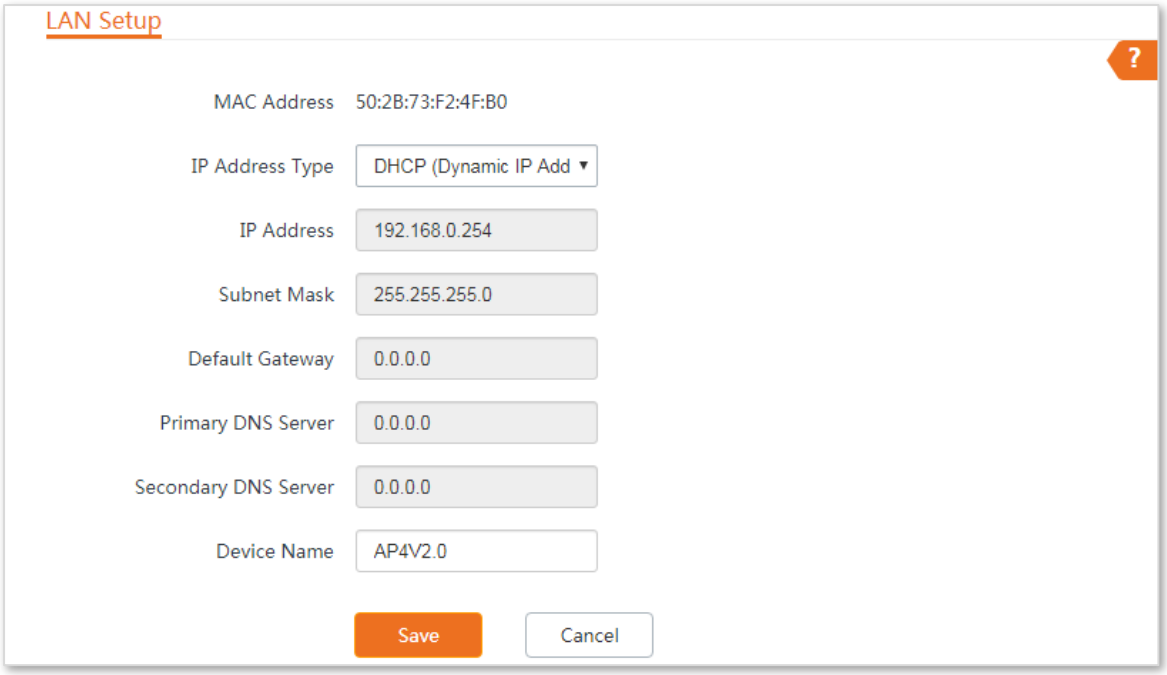
This method applies to a large LAN network with a large number of APs. With this method, the device automatically obtains an IP address, a subnet mask, a gateway IP address, DNS server IP addresses assigned by the DHCP server of the upstream device.

Configuration procedure:

Step 1 Choose **Network** > **LAN Setup** to enter the configuration page.

Step 2 Select **DHCP (Dynamic IP Address)** from the **IP Address Type** drop-down list.

Step 3 Click **Save**.



----End

After changing 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 Logging in to the web UI after changing the LAN IP address 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.

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

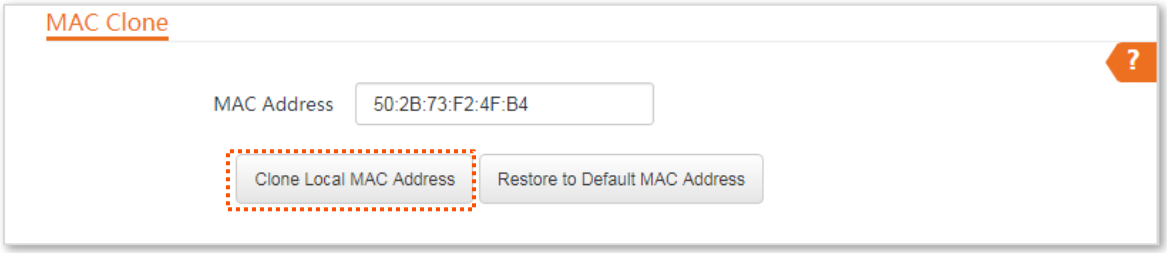
If you use the computer with the MAC address bound to your internet service to set up the function, perform the following steps:

Step 1 Connect the computer to the device.

Step 2 Log in to the web UI, and choose **Network** > **MAC Clone** to enter the configuration page.

Step 3 Click **Clone Local MAC Address**.

Step 4 Click **Save**.



----End

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

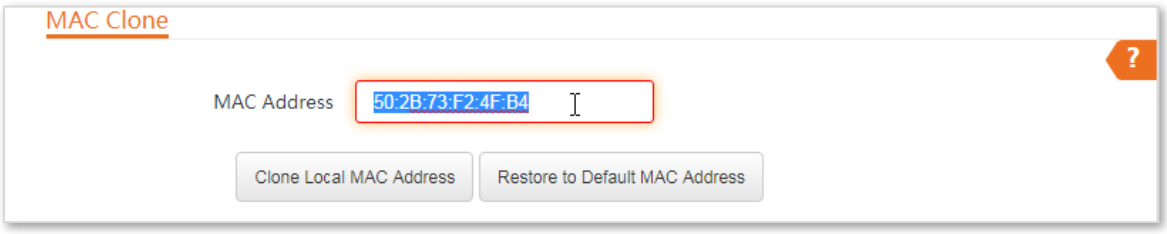
If you use a device whose MAC address is not bound to your internet service to set up the function, perform the following steps:

Step 1 Connect the device (such as a smart phone or tablet) to the device.

Step 2 Log in to the web UI, and choose **Network** > **MAC Clone** to enter the configuration page.

Step 3 Enter the MAC address of the computer that can access the internet in the **MAC Address** input box.

Step 4 Click **Save**.



----End

TIP

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

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.

TIP

If the network segment of the device's LAN port changes, the network segment of the device's DHCP server pool changes accordingly.

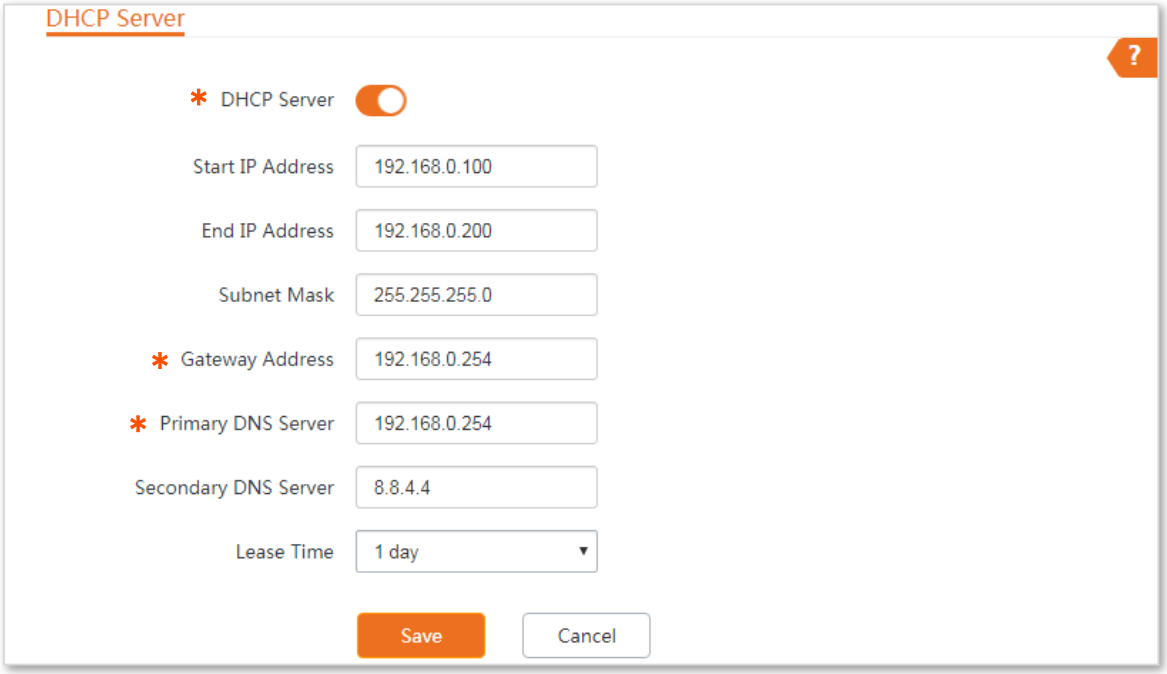
5.3.2 Configuring the DHCP server

Step 1 Choose **Network** > **DHCP Server** to enter the configuration page.

Step 2 Enable the **DHCP server**.

Step 3 Set the parameters. Generally, you only need to set **Gateway Address** and **Primary DNS Server**.

Step 4 Click **Save**.



----End

TIP

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.

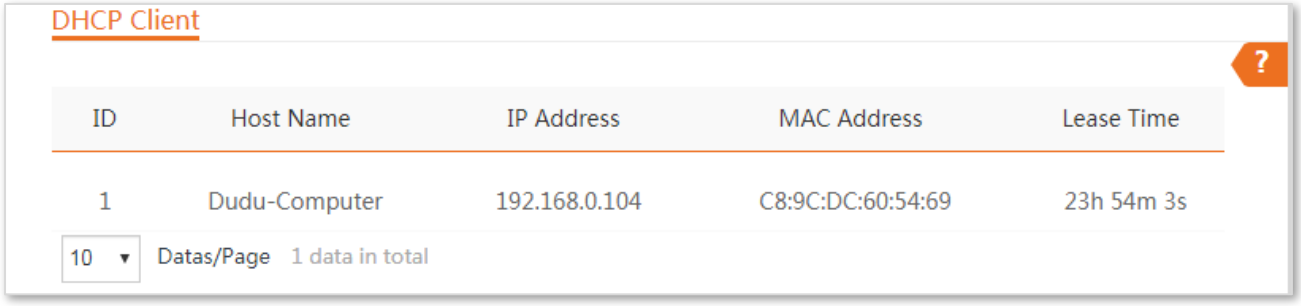
Parameters description

Name	Description
DHCP Server	It specifies whether to enable the DHCP server function of the device. By default, it is disabled.
Start IP Address	It specifies the start IP address of the IP address pool of the DHCP server. The default value is **192.168.0.100**.
End IP Address	It specifies the end IP address of the IP address pool of the DHCP server. The default value is **192.168.0.200**. The start and end IP addresses must belong to the same network segment as the IP address of the LAN port of the device.
Subnet Mask	It specifies the subnet mask assigned by the DHCP server. The default value is **255.255.255.0**.
Gateway Address	It specifies the default gateway IP address assigned by the DHCP server. Generally, it is the IP address of the LAN port of the egress router. The default value is **192.168.0.254**. A client can access a server or host not in the local network segment only through a gateway.
Primary DNS Server	It specifies the primary DNS server IP address assigned by the DHCP server. The default value is **8.8.8.8**. To enable clients to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server	It specifies the secondary DNS server IP address assigned by the DHCP server. This parameter is optional. The default value is **8.8.4.4**.
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client. When half of the lease time has elapsed, the client sends a DHCP request to the DHCP server to renew the lease time. If the request succeeds, the lease time is extended according to the request. Otherwise, the client sends the request again when 7/8 of the lease time has elapsed. If the request succeeds, the lease time is extended according to the request. Otherwise, the client must request an IP address from the DHCP server after the lease time expires. It is recommended that you retain the default value **1 day**.

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.

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



Parameters description

Name	Description
ID	It specifies the serial number.
Host Name	It specifies the name of the host whose IP address is assigned by the DHCP server of the device.
IP Address	It specifies the IP address that the DHCP server assigns to the host.
MAC Address	It specifies the MAC address of the host.
Lease Time	It specifies the validity period of the IP address assigned by the DHCP server to the host.

5.5 VLAN settings

This function can be configured only when the device works in **AP** mode.

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.

After the VLAN settings take effect, packets with tags are forwarded to the ports of the corresponding VLAN according to the VID of the packet, and packets without tag are forwarded to the ports of the corresponding VLAN according to the PVID of the port.

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

<table>
<tr><th rowspan="2">Link Type of the Port</th><th colspan="2">Type of Received Packets</th><th rowspan="2">Transmitted Packets</th></tr>
<tr><th>Packet with Tag</th><th>Packet without Tag</th></tr>
<tr><td>Access</td><td rowspan="2">Forward the data to the ports of the corresponding VLAN based on the VID in the tag.</td><td rowspan="2">Forward the data to the ports of the corresponding VLAN based on the PVID of ports</td><td>Strip the tag in the packet and then forward it</td></tr>
<tr><td>Trunk</td><td>VID ＝ PVID of the port, strip the tag in the packet and then forward it
VID ≠ PVID of the port, retain the tag in the packet and then forward it</td></tr>
</table>

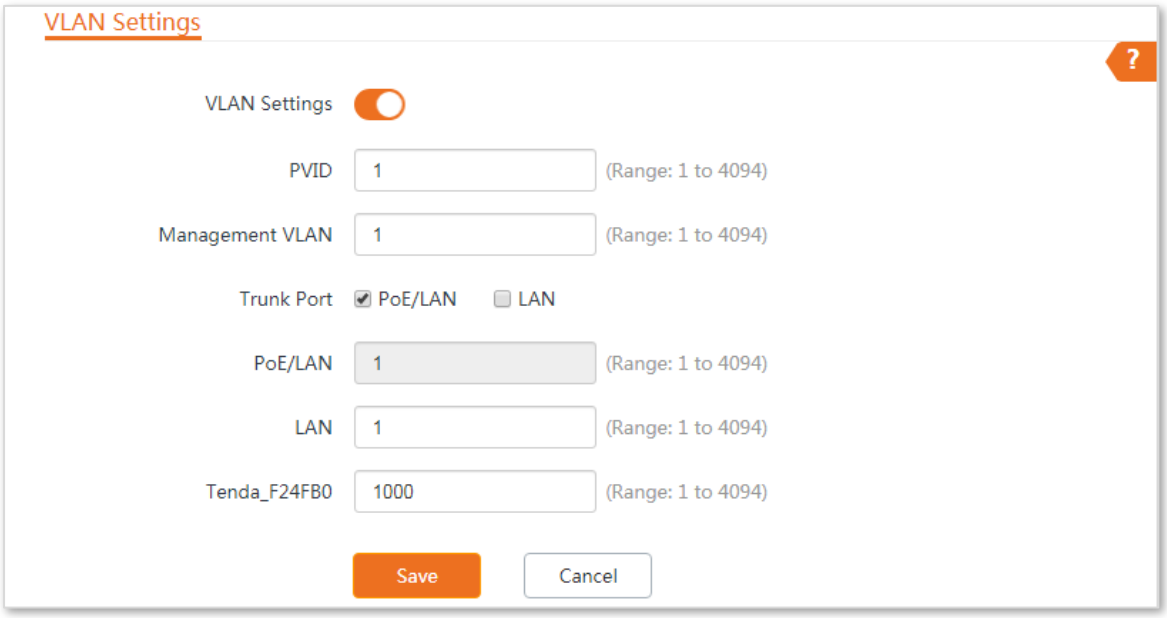
5.5.2 Setting up VLAN

Step 1 Choose **Network** > **VLAN Settings** to enter the configuration page.

Step 2 Enable the **VLAN Settings** function.

Step 3 Set the parameters as needed.

Step 4 Click **Save**.



----End

Parameters description

Name	Description
VLAN Settings	It specifies whether to enable the VLAN function of this device. By default, it is disabled.
PVID	It specifies the default native VLAN ID of the trunk port. The default ID is **1**.
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.
Trunk Port	It allows you to specify a port as a trunk port. At least one port should be selected. When a port is specified as a trunk port, its VLAN ID cannot be edited. • **PoE/LAN**: It specifies the VLAN ID of the PoE/LAN2 port. • **LAN**: It specifies the VLAN ID of the LAN1 port.
Tenda_F24FB0	"Tenda_F24FB0" specifies the current SSID of the WiFi network of this device, and is changed when the SSID changes. This parameter is used to set the VLAN ID for the WiFi network of this device. The default is **1000**. After the VLAN function is enabled, the WLAN interface functions as an access port, whose PVID is the same as its VLAN ID.

5.5.3 Example of configuring VLAN settings

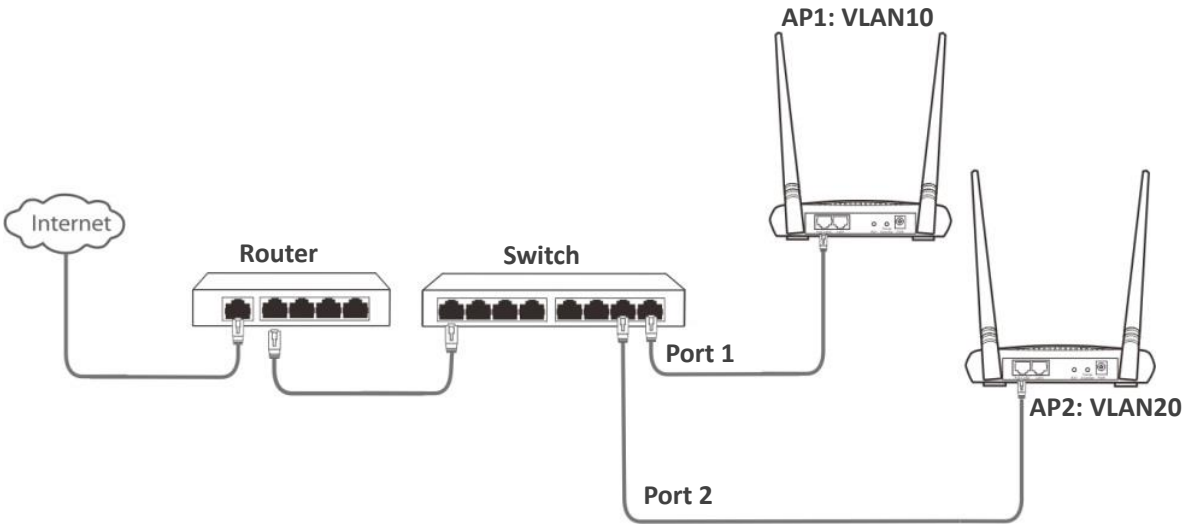
Networking requirement

You use the APs to deploy wireless networks in your company. Now you want to make APs used by different departments cannot communicate with each other to secure data transmission of some special departments, such as the finance department.

Assume that:

Assign AP1 to VLAN10, and AP2 to VLAN20.

Network Topology



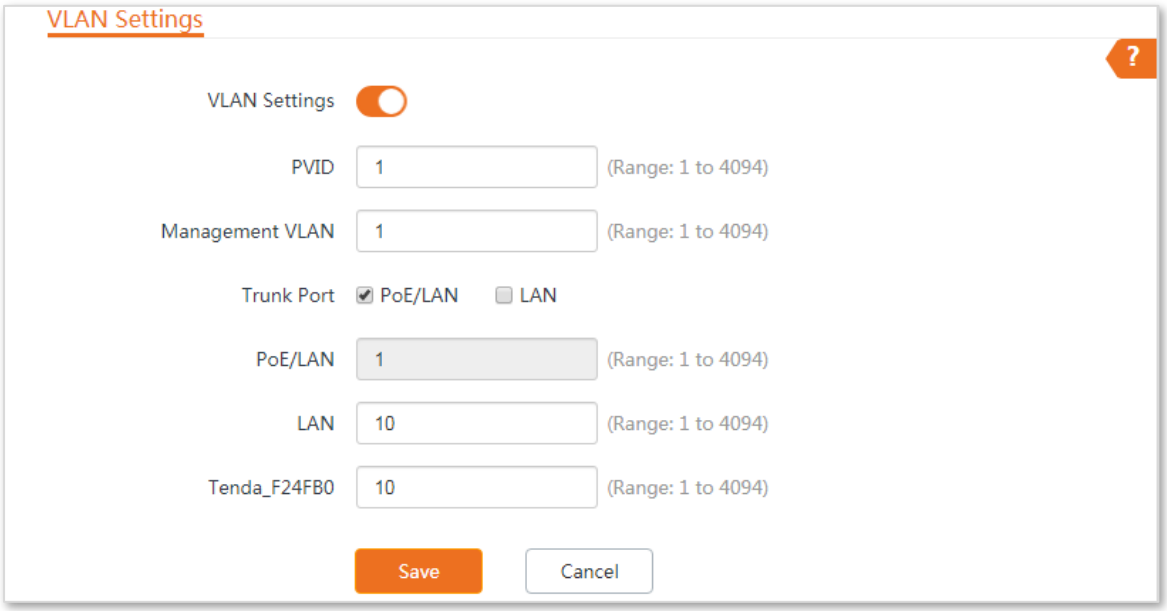
Hardware connection:

- The router is connected to the uplink port.
- The PoE/WAN/LAN2 port of AP1 is connected to port 1.
- The PoE/WAN/LAN2 port of AP2 is connected to port 2.

Configuration procedure

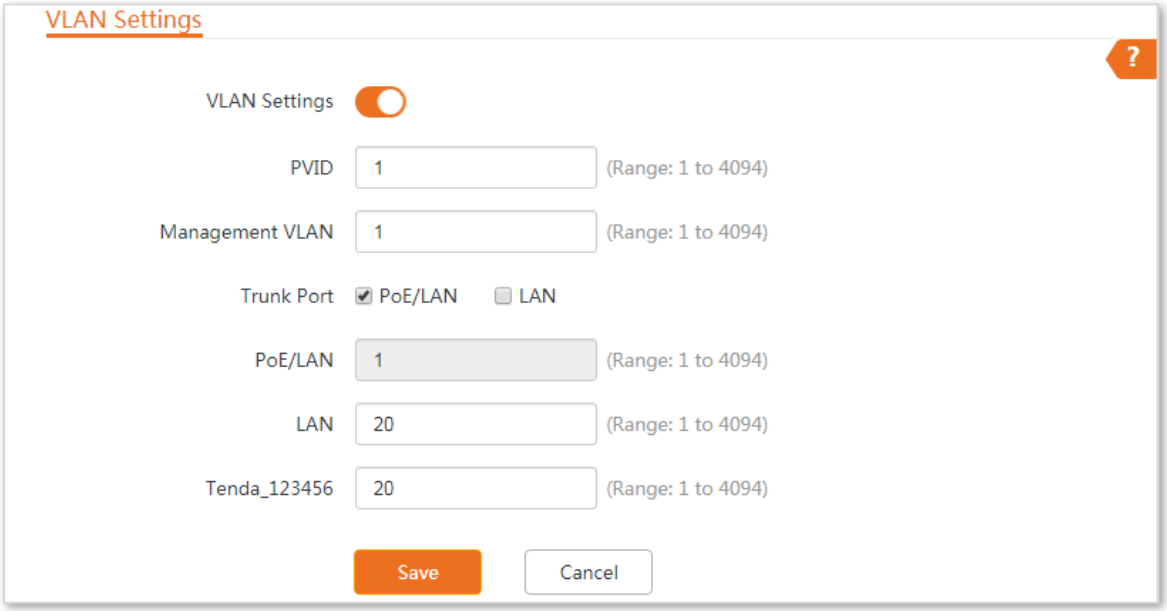
Step 1 Set up AP1.

1. Log in to the web UI of AP1, and choose **Network** > **VLAN Settings**.
2. Enable the **VLAN Settings** function.
3. Set **PVID** and **Management VLAN** to **1**.
4. Set **Trunk Port** to **PoE/LAN**.
5. Set **LAN** and **Tenda_F24FB0** to **10**.
6. Click **Save**.



7. Click **OK** on the pop-up window, and wait until the AP1 completes reboot.

Step 2 Set up AP2 by referring to **Step 1**.



Step 3 Set up the switch.

Configure the VLAN settings on the switch as shown in the table below:

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 AP1)	1,10	Trunk	1
Port 2 (Connected to AP2)	1,20	Trunk	1

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

Step 4 Set up the router.

Configure the VLAN settings on the router as shown in the table below:

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 AP1 obtains an IP address and related parameters from the DHCP server belonging to VLAN10, and the second client connected to AP2 obtains these parameters from the DHCP sever belonging to VLAN20.

6 Wireless

6.1 Basic

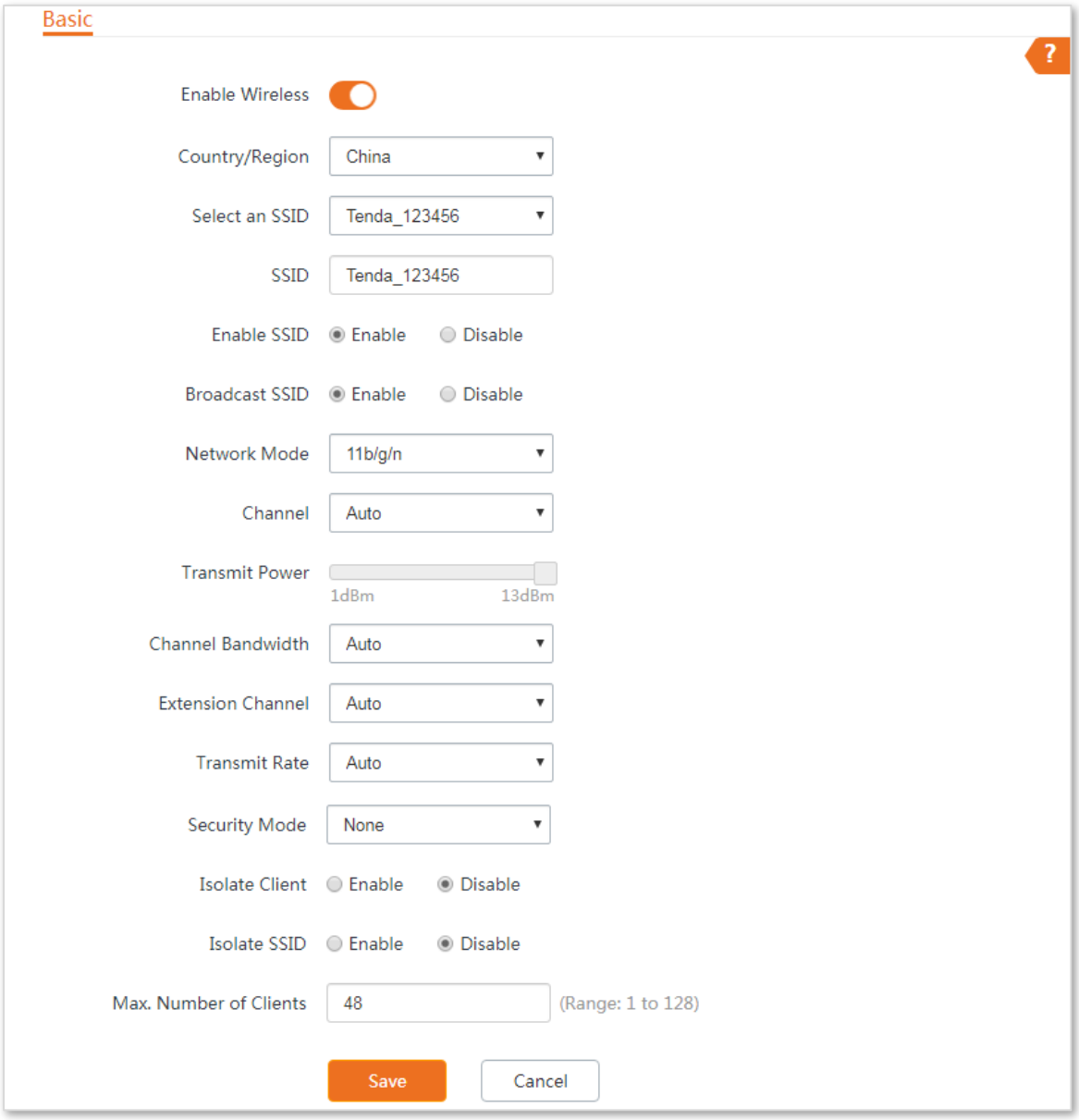
This module enables you to set basic wireless settings of the device, including SSID-related parameters, network mode, channel, transmit power and so on. This module is not available when the device works in **Client** or **Universal Repeater** mode.

6.1.1 Changing the basic settings

Step 1 Choose **Wireless** > **Basic**.

Step 2 Change the parameters as required.

Step 3 Click **Save**.



----End

Parameters description

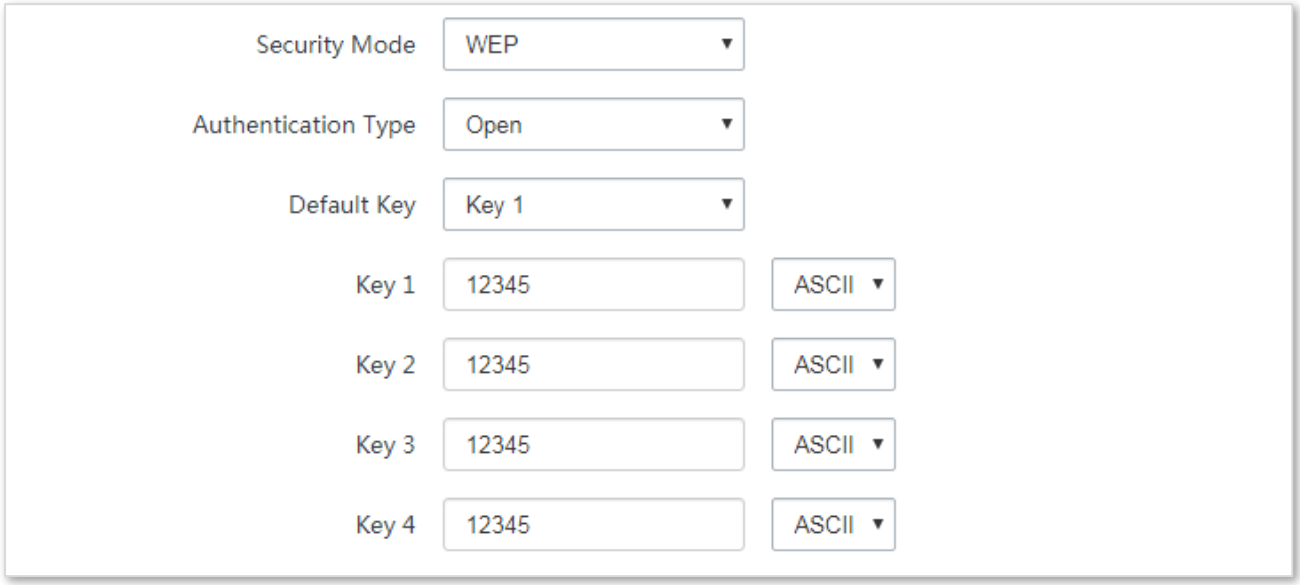
Name	Description
Enable Wireless	It specifies whether to enable the wireless function. By default, it is enabled.
Country/Region	It specifies country or region where this device is located. You can select the country or region to ensure that this device complies with the channel regulations of the country or region.
Select an SSID	The device supports two WiFi networks at most, and only one is enabled by default. It allows you to select one WiFi network from the drop-down list to configure.
SSID	It specifies the WiFi name of the selected WiFi network.

Name	Description
Enable SSID	It specifies whether to enable the selected WiFi network.
Broadcast SSID	It specifies whether to broadcast the 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 SSID manually on your wireless client if you want to connect to the WiFi network corresponding to the SSID. This to some extent enhances the security of the WiFi network. It is worth noting that after **Broadcast SSID** is set to **Disable**, a hacker can still connect to the corresponding WiFi network if he/she manages to obtain the SSID by other means.
Network Mode	It specifies the WiFi network mode of this device. The available options include **11a**, **11n**, and **11 a/n**. • **11b**: It indicates that clients compliant with the IEEE 802.11b protocol can connect to the WiFi networks of the device. • **11g**: It indicates that clients compliant with IEEE 802.11g can connect to the WiFi networks of the device. • **11 b/g**: It indicates that all clients compliant with the IEEE 802.11b or IEEE 802.11g protocol can connect to the WiFi networks of the device. • **11b/g/n**: It indicates that all clients working at 2.4 GHz band and compliant with the IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n protocols can connect to the WiFi networks of 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.
Transmit Power	It specifies the transmit power of this device. Higher number indicates wider WiFi coverage. Setting a proper transmit power helps improve the performance and security of the WiFi network.
Channel Bandwidth	It specifies the bandwidth of the operating channel of a WiFi network. Change the default setting only when necessary. • **20MHz**: It indicates that the channel bandwidth of the device is 20 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 between 20 MHz and 40 MHz based on the ambient environment.
Extension Channel	Available only when the Channel Bandwidth is set to **Auto** or **40MHz**. It specifies an additional channel used to increase the channel bandwidth.
Transmit Rate	It specifies wireless transmit rate of the device.

Name	Description
	• When the channel bandwidth is set to **20MHz**, the rate automatically reduces, and the maximum rate is 144.4 Mbps. • When the channel bandwidth is set to **40MHz**, the maximum rate is 300 Mbps. • When the channel bandwidth is set to **Auto**, the maximum rate is 300 Mbps.
Security Mode	A WiFi network uses radio, which is open to the public, as its data transmission medium. If the WiFi 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 WiFi 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 WiFi 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 WiFi 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. 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 WiFi 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 WiFi 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

Name	Description
	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 WiFi network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key (WiFi password). 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. **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 WiFi 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.
Isolate SSID	It specifies whether to isolate the wireless clients connected to the AP with different SSIDs. • **Enable**: It indicates that the wireless clients connected to the AP with different SSID cannot communicate with each other. This improves wireless network security. • **Disable**: It indicates that the wireless clients connected to the AP with different SSIDs can communicate with each other.
Max. Number of Clients	This parameter specifies the maximum number of clients that can connect to the WiFi network corresponding to an SSID. If the number is reached, the WiFi network rejects new connection requests from clients. This limit helps balance load among devices.

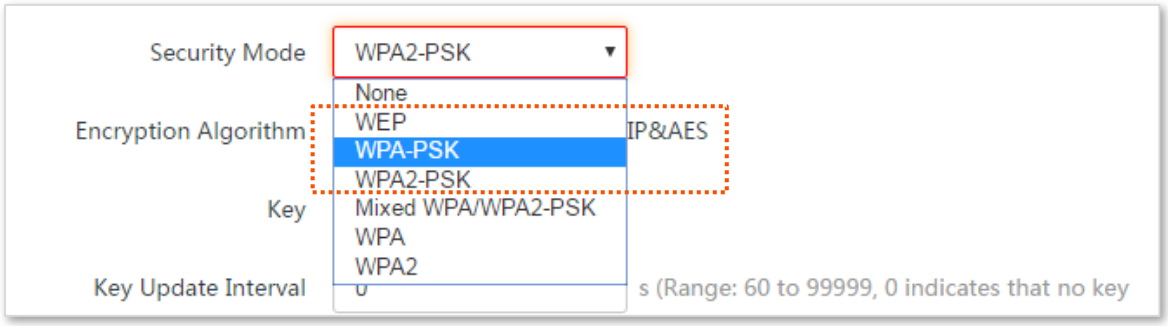
WEP



Parameters description

Name	Description
Authentication Type	It specifies the authentication type for the WEP security mode. The options include **Open** and **Shared**. The options share the same encryption process. • **Open**: It specifies that authentication is not required and data exchanged is encrypted using WEP. In this case, a wireless client can connect to the WiFi 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 WiFi network corresponding to the selected SSID. The wireless client can be connected to the WiFi network only if they use the same WEP key.
Default Key	It specifies the WEP key for the **Open** or **Shared** encryption type. For example, if Default Key is set to Security Key 2, a wireless client can connect to the WiFi 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.

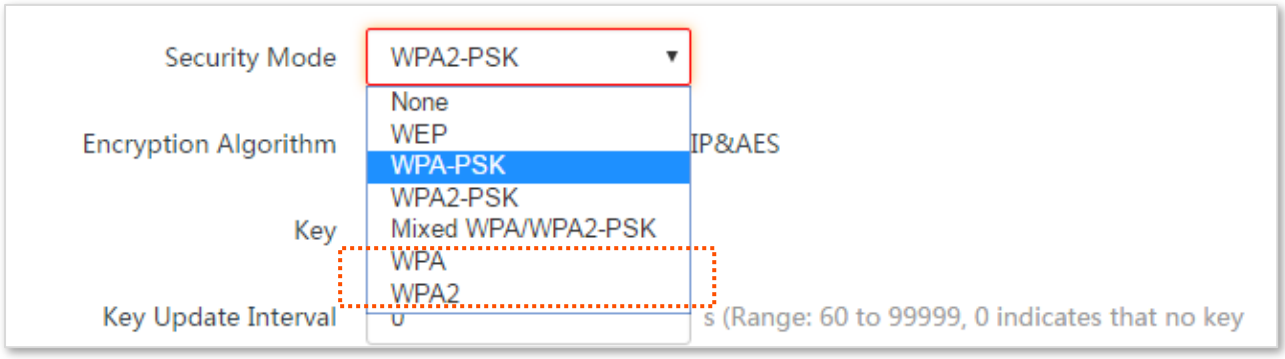
WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK

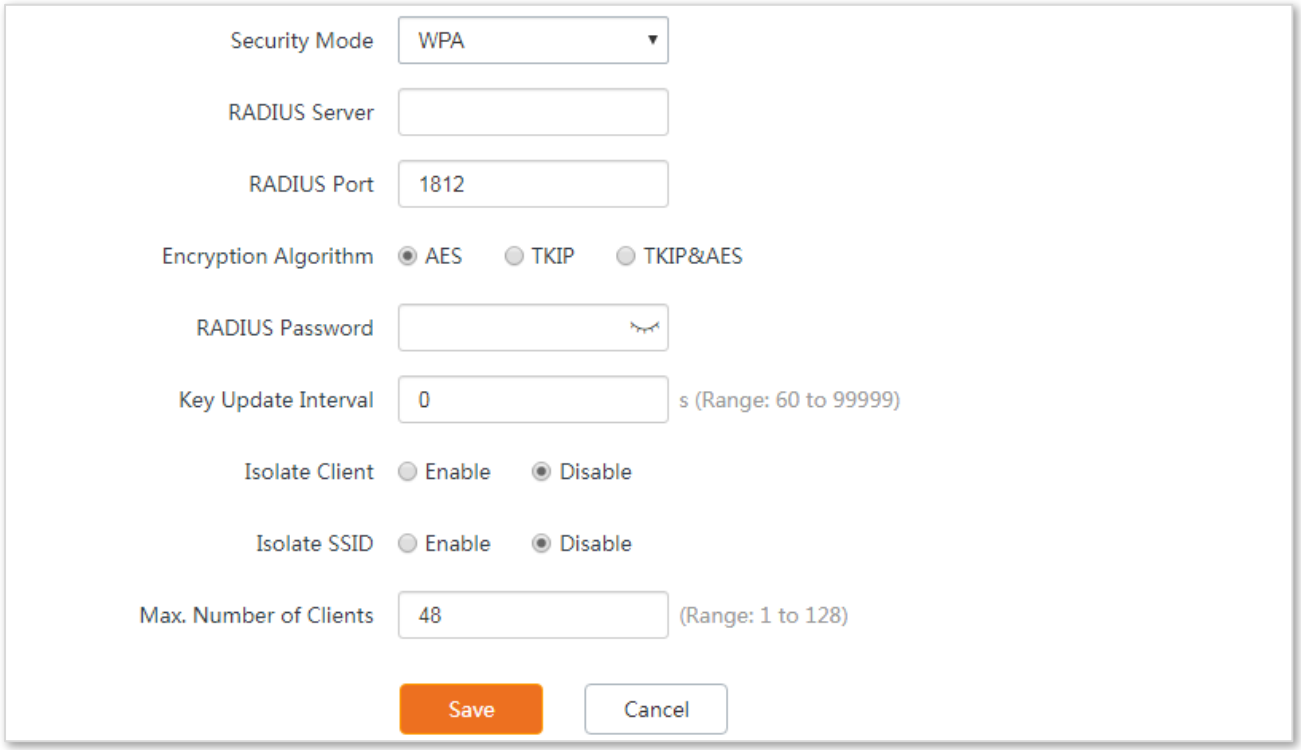


Parameters description

Name	Description
Security Mode	It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. • **WPA-PSK**: It indicates that the WiFi network corresponding to the selected SSID is encrypted using WPA-PSK. • **WPA2-PSK**: It indicates that the WiFi network corresponding to the selected SSID is encrypted using WPA2-PSK. • **Mixed WPA/WPA2-PSK**: It indicates that wireless clients can connect to the WiFi 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 WiFi network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. 0 indicates that a WAP key is not updated.

WPA and WPA2





Parameters description

Name	Description
Security Mode	The **WPA** and **WPA2** options are available for network protection with a RADIUS server. • **WPA**: It indicates that the WiFi network corresponding to the selected SSID is encrypted using WPA. • **WPA2**: It indicates that the WiFi network corresponding to the selected SSID is encrypted using WPA2.
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.

Name	Description
RADIUS Password	It specifies the shared password of the RADIUS server.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. The available options include **AES**, **TKIP**, and **TKIP&AES**. • **AES**: It indicates the Advanced Encryption Standard. • **TKIP**: It indicates the Temporal Key Integrity Protocol. • **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the WiFi 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. 0 indicates that a WAP key is not updated.

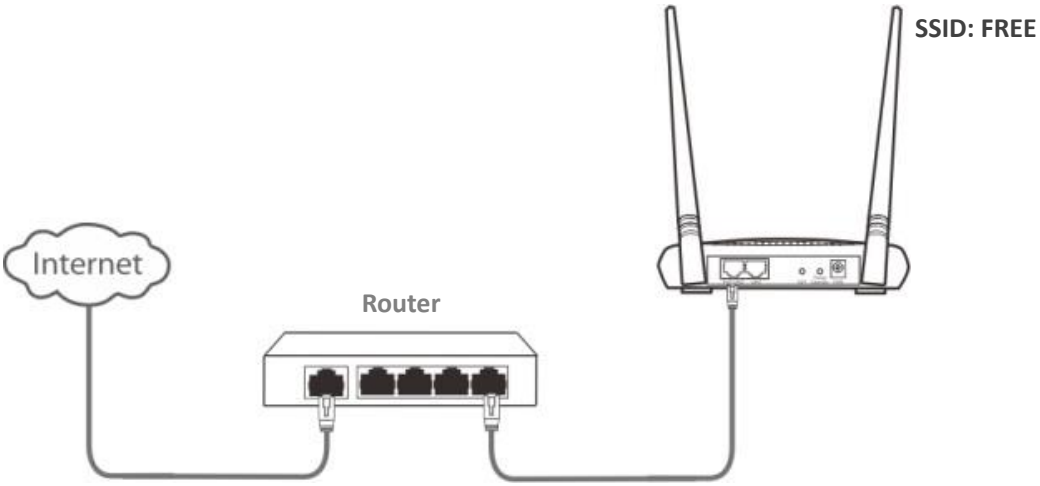
6.1.2 Example of configuring basic settings

Setting up a non-encrypted WiFi network

Networking requirement

An office uses the device to deploy its network. It requires that the SSID is FREE and there is no WiFi key.

Network topology



Configuration procedure

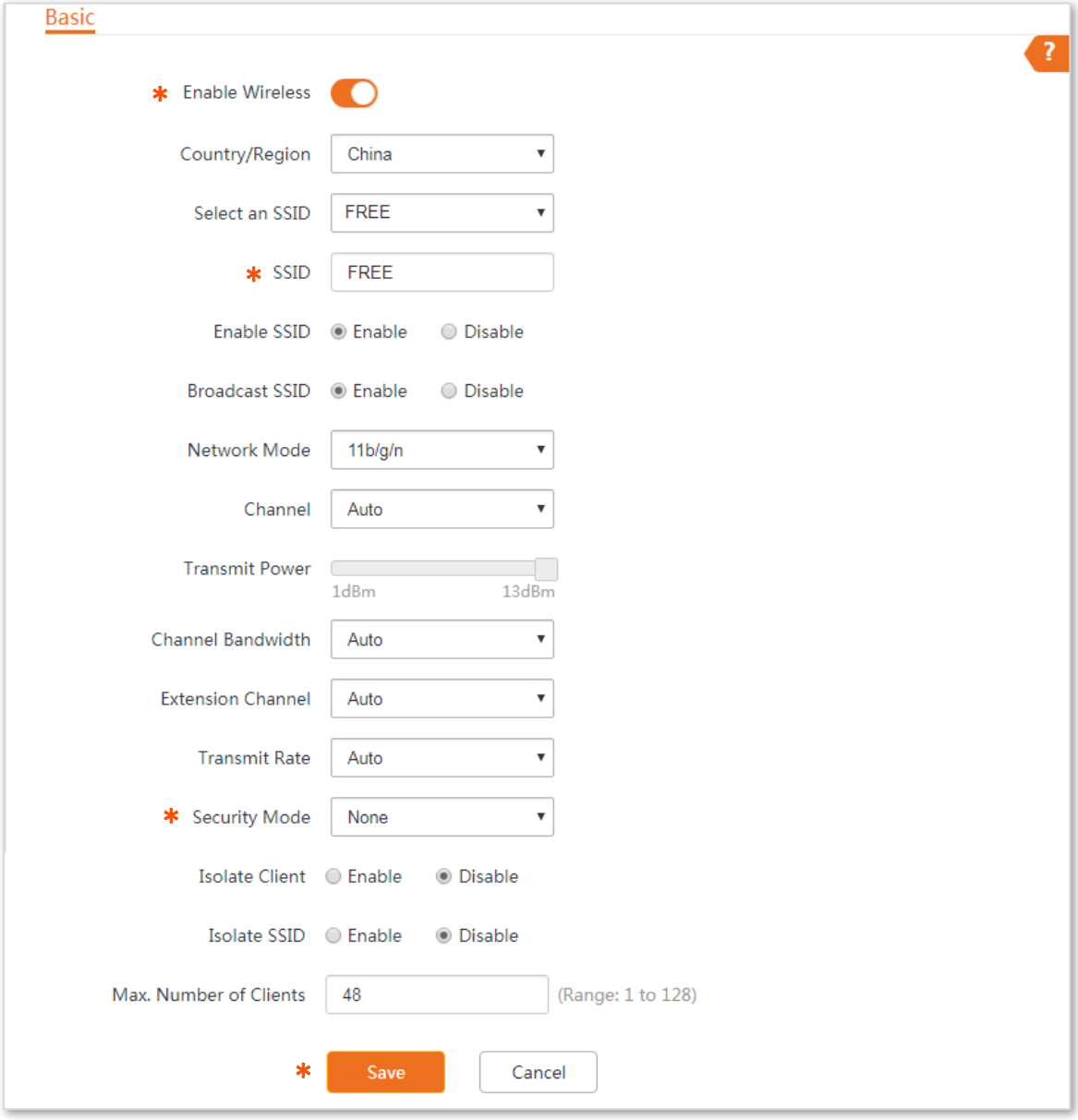
Step 1 Choose **Wireless** > **Basic**.

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**.



----End

Verification

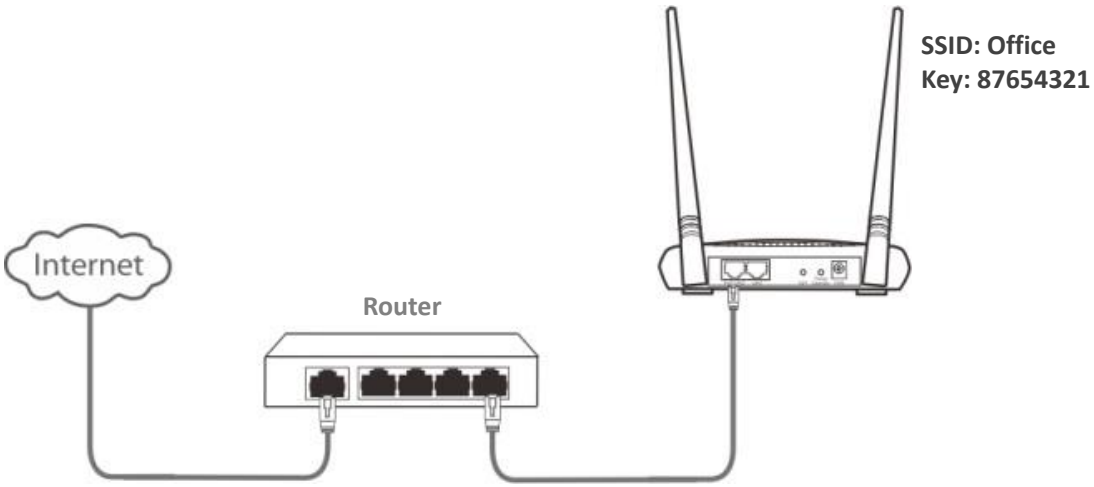
Wireless devices can connect to the WiFi network named **FREE** without a password.

Setting up a WiFi network encrypted using WPA2-PSK

Networking requirement

An office's WiFi 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.

Network topology



Configuration procedure

Step 1 Log in to the web UI of the device, and choose **Wireless** > **Basic**.

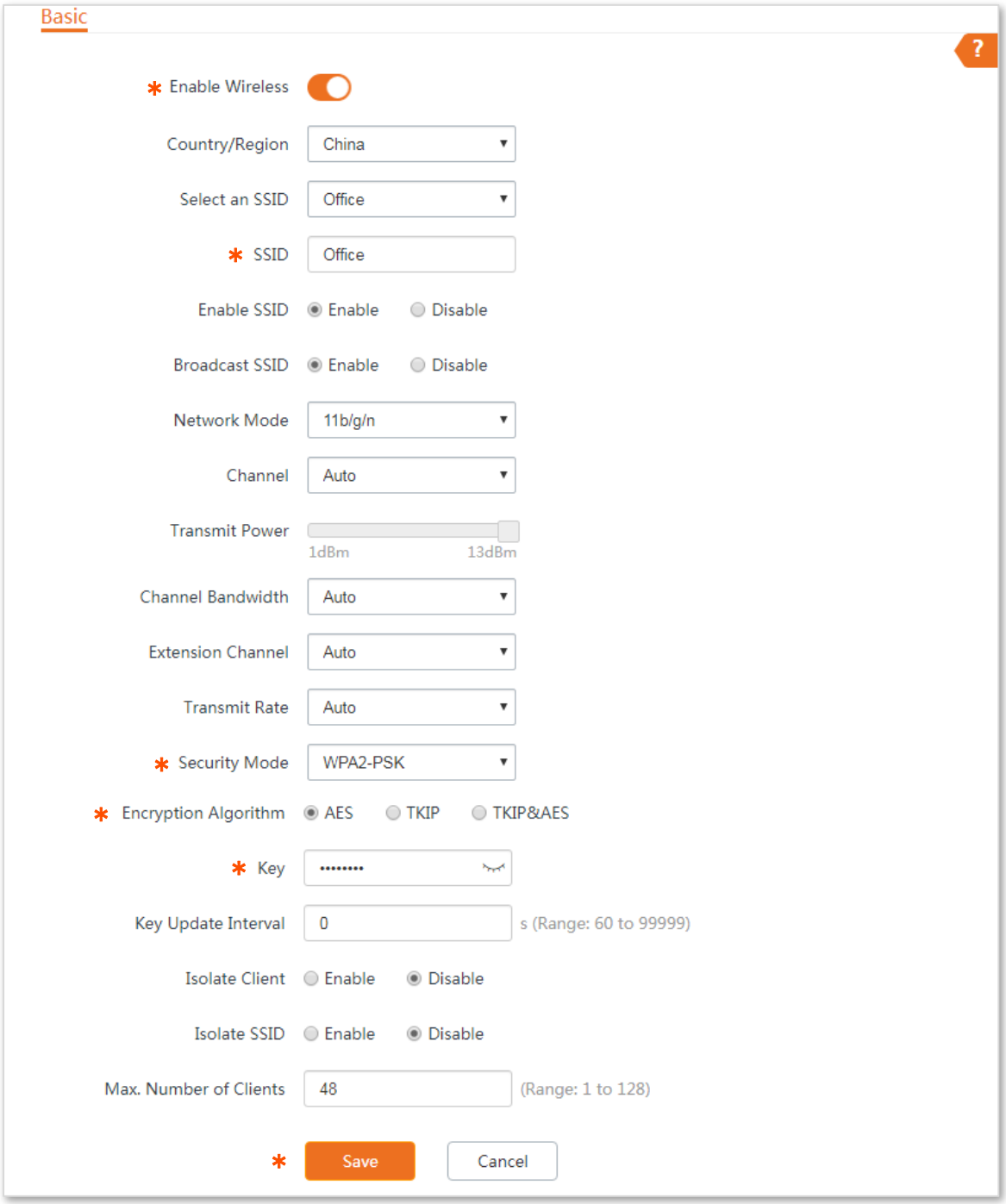
Step 2 Set the Enable wireless function.

Step 3 Change the value of the SSID text box to **Office**.

Step 4 Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.

Step 5 Set **Key** to **87654321**.

Step 6 Click **Save**.



----End

Verification

Wireless devices can connect to the WiFi network named **Office** with the password **87654321**.

6.2 Advanced

6.2.1 Overview

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

6.2.2 Changing advanced settings

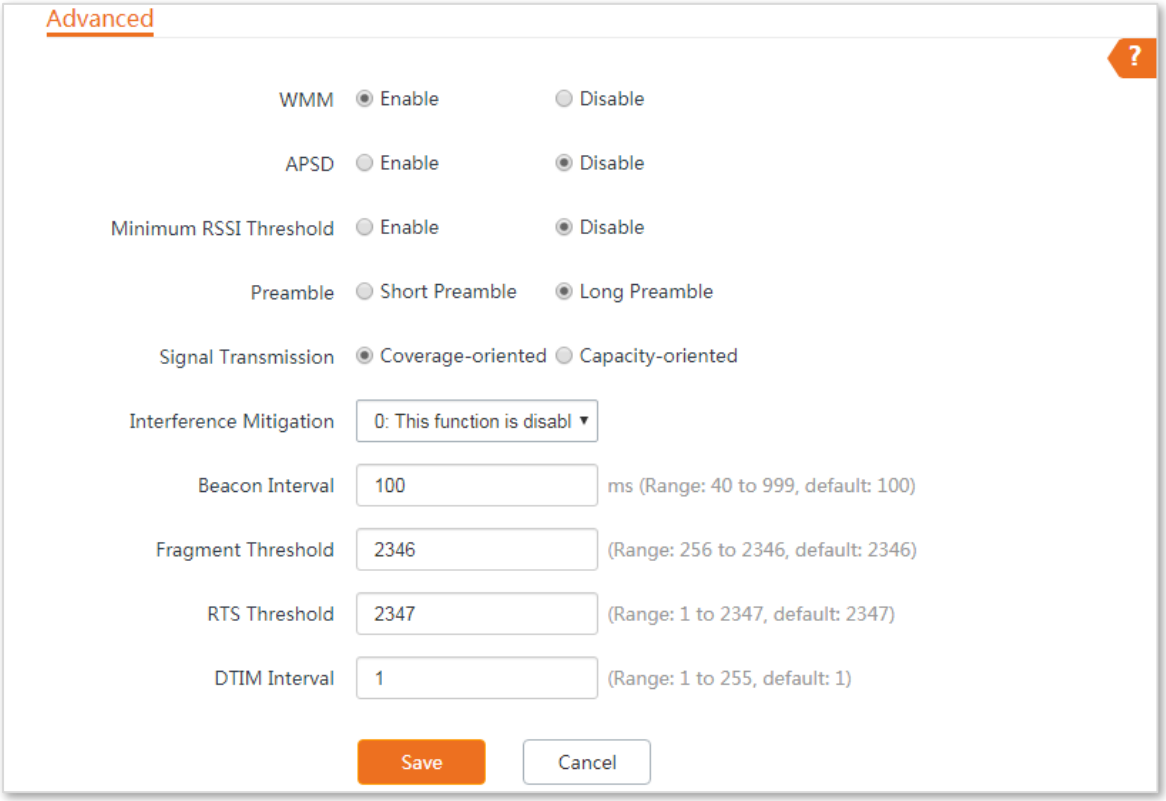
TIP

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 Log in to the web UI of the device, and choose **Wireless** > **Advanced**.

Step 2 Change parameters as required.

Step 3 Click **Save**.



----End

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 WiFi networks.

Name	Description
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 WiFi network with better WiFi signal.
Preamble	It specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. • **Long Preamble (default)**: Select this option for compatibility with old network adapters installed on wireless clients. • **Short Preamble**: Select this option to achieve better synchronization performance of networks.
Signal Transmission	It specifies the wall penetrating capability of the device. • **Coverage-oriented**: Applies to a large area with less interference nearby. • **Capacity-oriented**: Applies to an area with strong interference nearby. This mode improves the device's anti-interference capability.
Interference Mitigation	It specifies the device's capacity to mitigate interference in different environments. Select a proper option from the drop-down list menu according to your actual situation. The default is 0.
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 WiFi network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the WiFi network to transmit data quicker.
Fragment Threshold	It specifies the threshold of a fragment. The unit is byte. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold to enable this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput. Frame length threshold for triggering the RTS/CTS mechanism. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a WiFi network to recover from conflicts quicker. For a WiFi 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.

Name	Description
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 WiFi network to recover from conflicts quicker. For a WiFi 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.

6.3 Access control

6.3.1 Overview

The device allows you to set whitelist (allow to access the internet) or blacklist (disallow to access the internet) based on wireless clients' MAC addresses.

6.3.2 Configuring access control

Step 1 Log into the web UI of the device, and choose **Wireless** > **Access Control**.

Step 2 Select a SSID to which the rule applies.

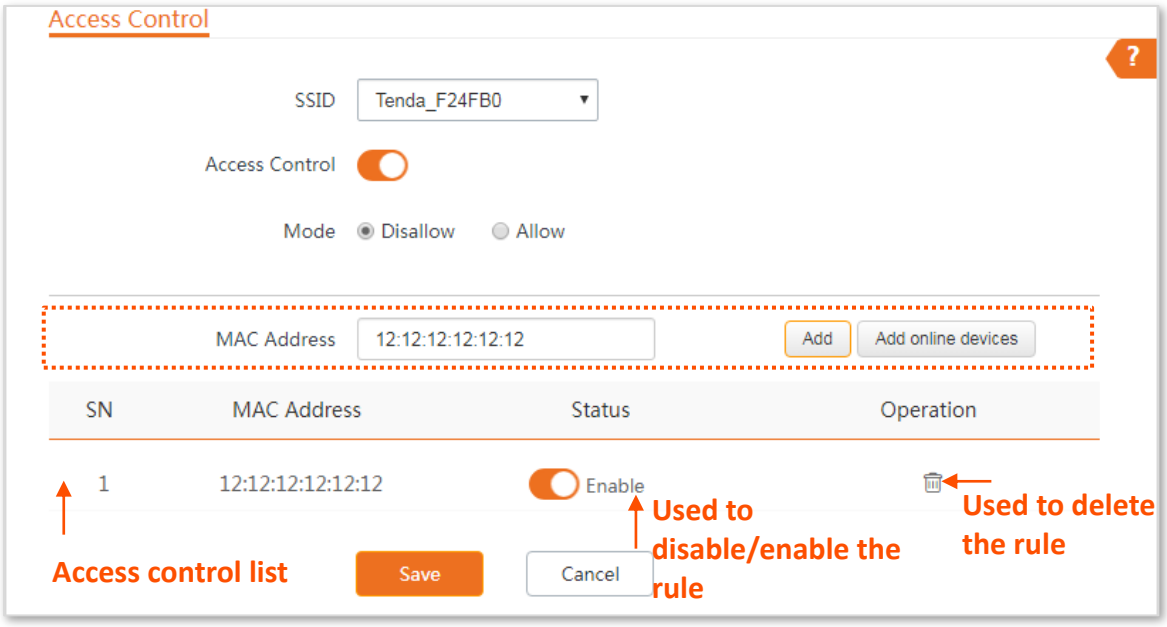
Step 3 Enable the **Access Control** function.

Step 4 Select a MAC address filter mode, **Disallow** or **Allow**.

Step 5 Add the client to be controlled.

- Manual enter: Enter the MAC address of the client in the **MAC Address** input box, and click **Add**.
- Quick add: Click **Add online devices** to add all connected clients to the access control list quickly.

Step 6 Click **Save**.



----End

Parameters description

Name	Description
SSID	It specifies the WiFi networks supported by the device.
Access Control	It specifies whether to enable the function.
Mode	It specifies the mode for filtering MAC addresses. • **Allow**: It indicates that only the wireless clients on the access control list can connect to the selected WiFi network of the device. • **Disallow**: It indicates that only the wireless clients on the access control list cannot connect to the selected WiFi network of the device.

6.3.3 Example of configuring access control

Networking requirement

A WiFi network named **Connect Me** has been set up in a residential community. Only the community members are allowed to connect to the WiFi network.

Solution

The **Access Control** function is recommended. Assume that the community members' 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 Log into the web UI of the device, and choose **Wireless** > **Access Control**.

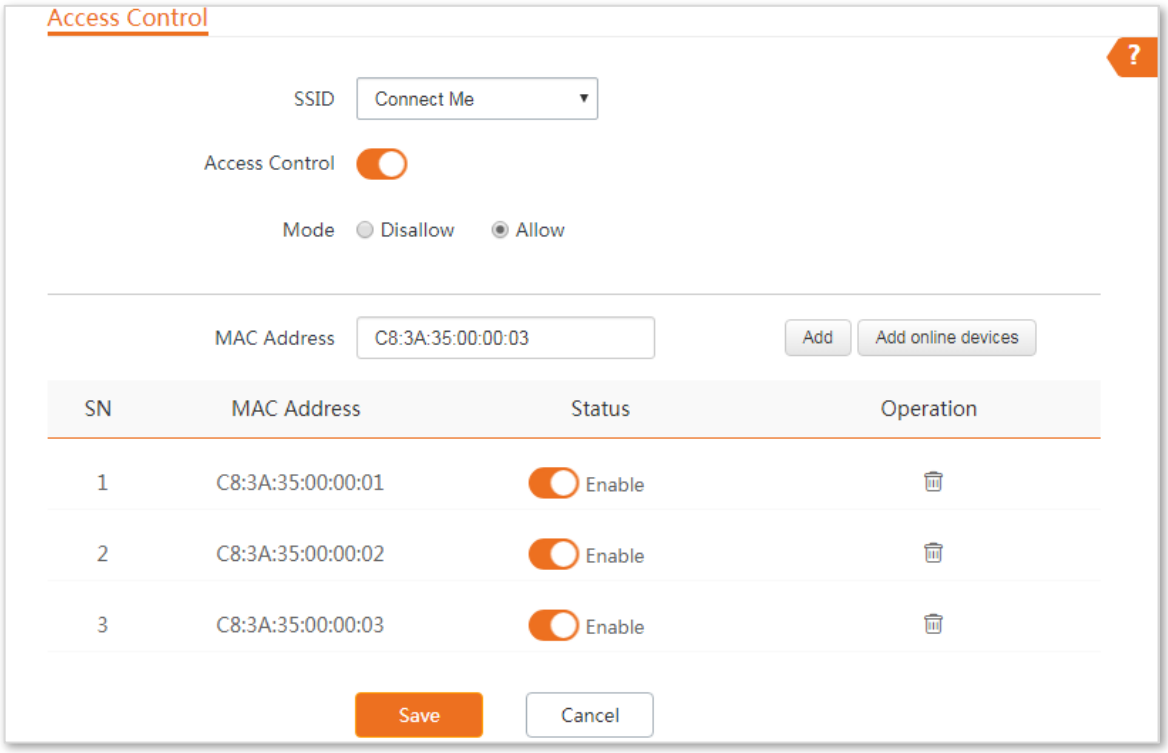
Step 2 Select **Connect Me** from the SSID drop-down list.

Step 3 Enable the **Access Control** function.

Step 4 Set the **Mode** to **Allow**.

Step 5 Enter the MAC addresses one by one and click **Add**.

Step 6 Click **Save**.



----End

Verification

Only wireless devices with the MAC addresses included in the rules can connect to the WiFi network named **Connect Me**.

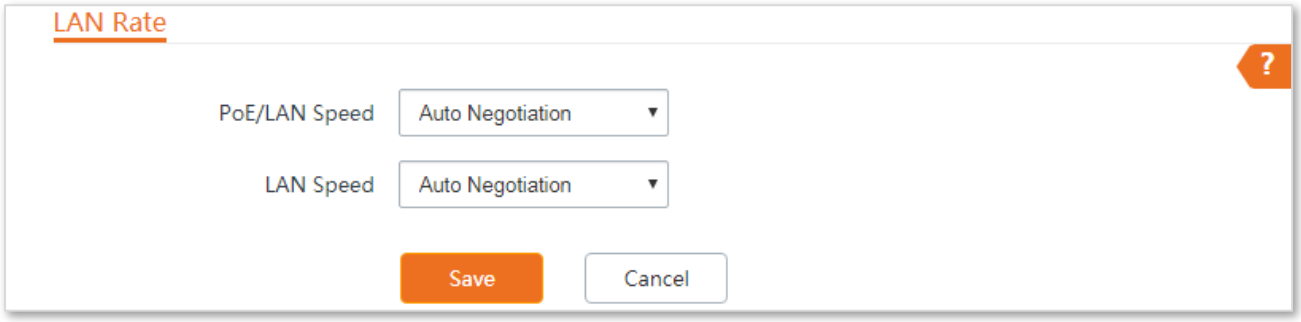
7 Advanced

7.1 LAN rate

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

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

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



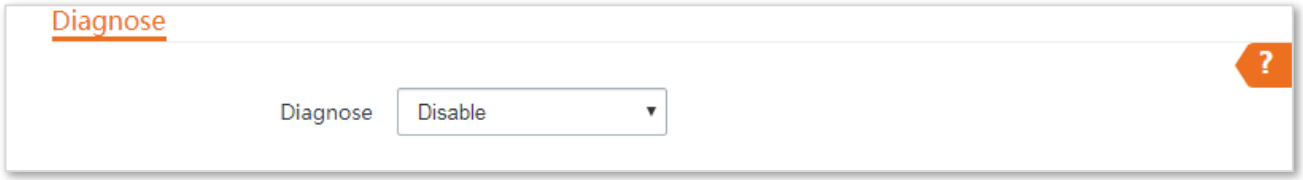
7.2 Diagnose

7.2.1 Overview

You can use the diagnosis tools for troubleshooting. The device supports the following 3 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

To access the page, choose **Advanced** > **Diagnose**.



7.2.2 Site Survey

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

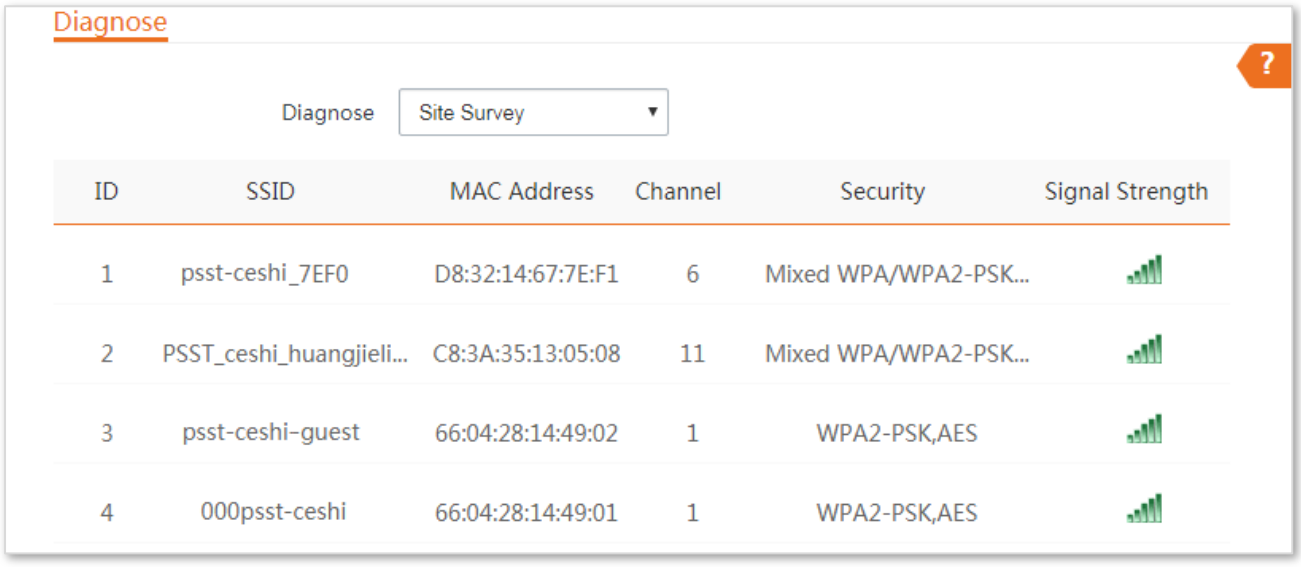
Configuration procedure

Step 1 Log in to the web UI of the device, and choose **Advanced** > **Diagnose**.

Step 2 Select **Site Survey** from the **Diagnose** drop-down list menu.

----End

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



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 Log in to the web UI of the device, and choose **Advanced** > **Diagnose**.

Step 2 Select **Ping** from the **Diagnose** drop-down list menu.

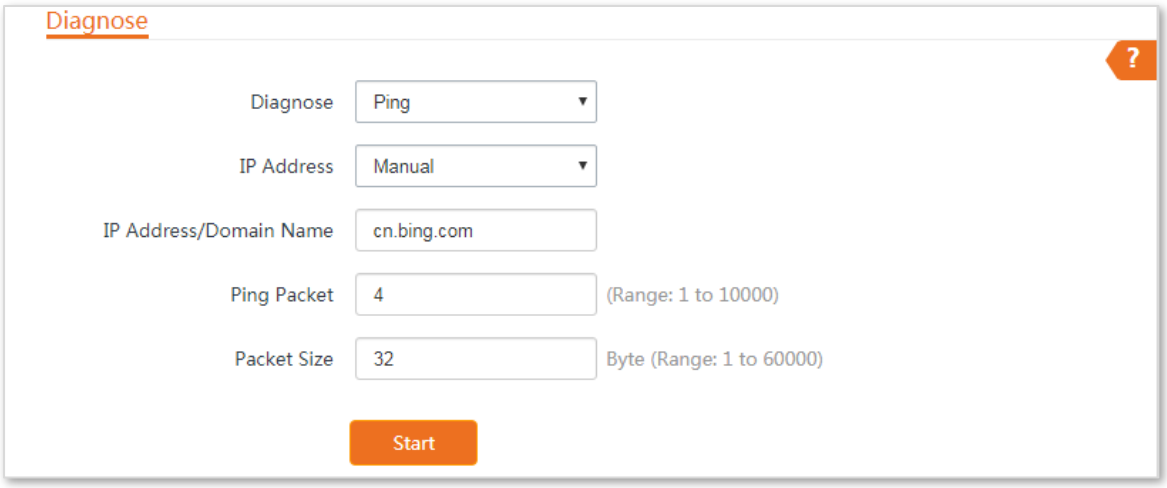
Step 3 Set **IP Address** to **Manual**.

Step 4 Enter an IP address or a domain name, which is **cn.bing.com** in this example.

Step 5 Enter the number of packets.

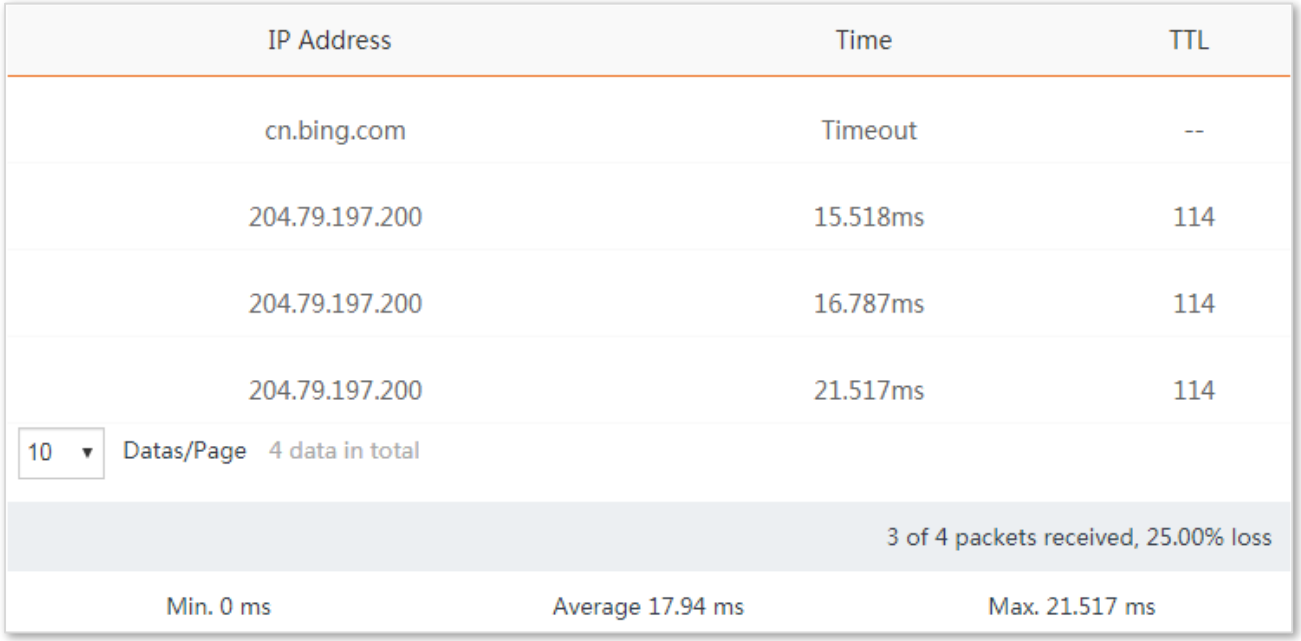
Step 6 Enter the size of packet.

Step 7 Click **Start**.



----End

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



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**.

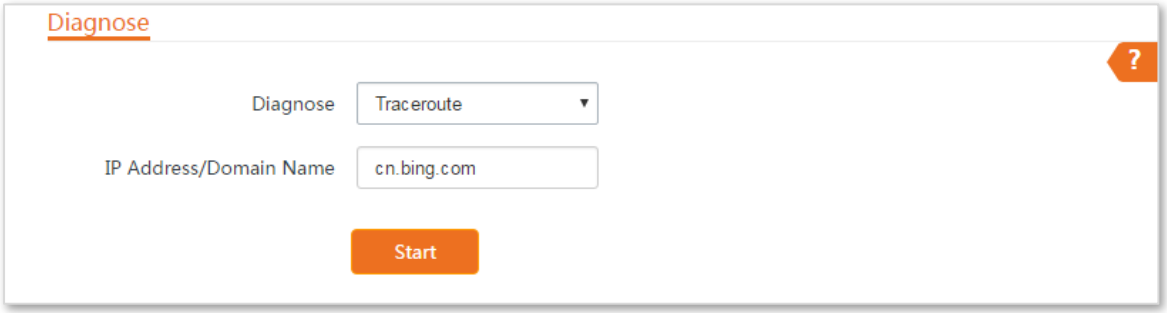
Configuration procedure

Step 1 Log in to the web UI of the device, and choose **Advanced** > **Diagnose**.

Step 2 Select **Traceroute** from the **Diagnose** drop-down list menu.

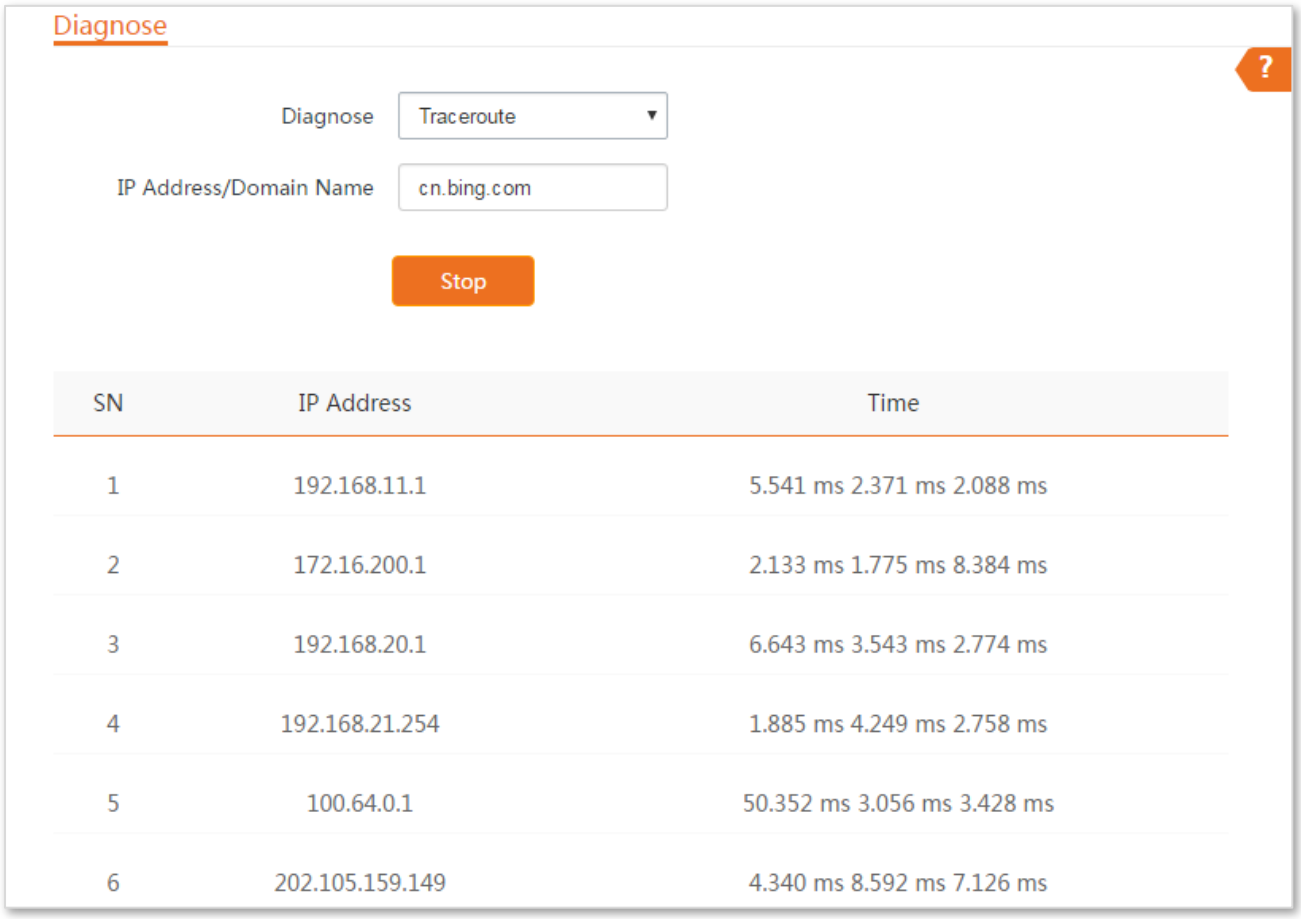
Step 3 Enter an IP address or a domain name, which is **cn.bing.com** in this example.

Step 4 Click **Start**.



----End

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


Diagnose
Diagnose
Traceroute
IP Address/Domain Name
cn.bing.com
Stop
SN
IP Address
Time
1
192.168.11.1
5.541 ms 2.371 ms 2.088 ms
2
172.16.200.1
2.133 ms 1.775 ms 8.384 ms
3
192.168.20.1
6.643 ms 3.543 ms 2.774 ms
4
192.168.21.254
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

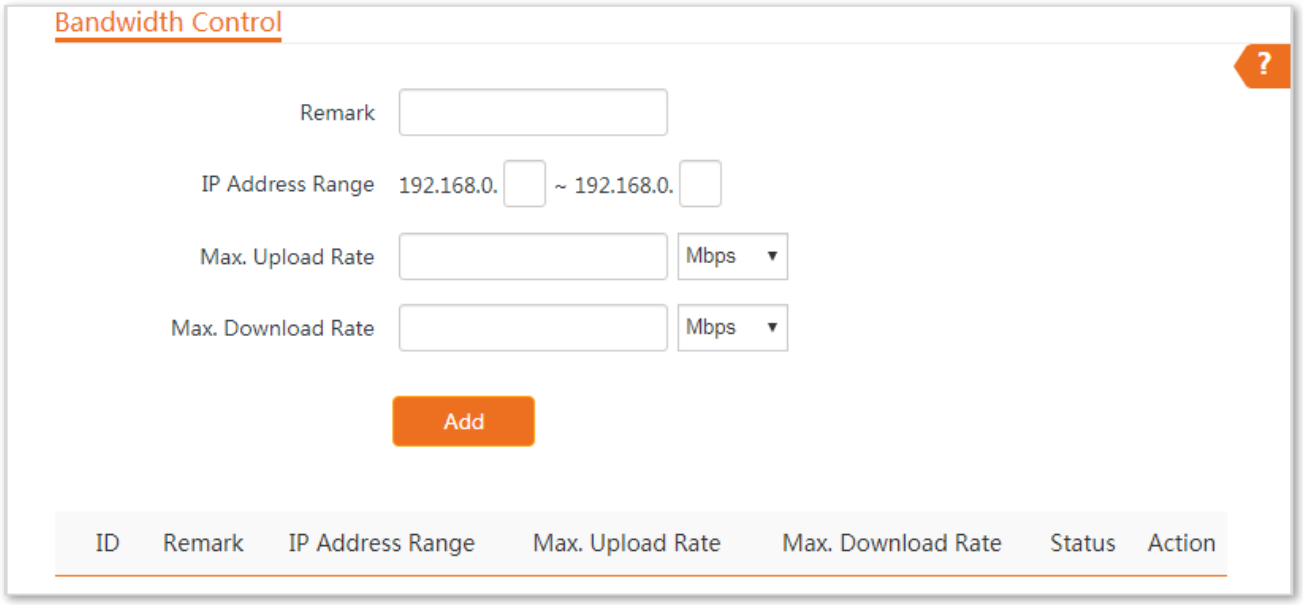
7.3 Bandwidth control

7.3.1 Overview

Only available in **WISP** or **Router** mode.

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.

To access the page, choose **Advanced** > **Bandwidth Control**.

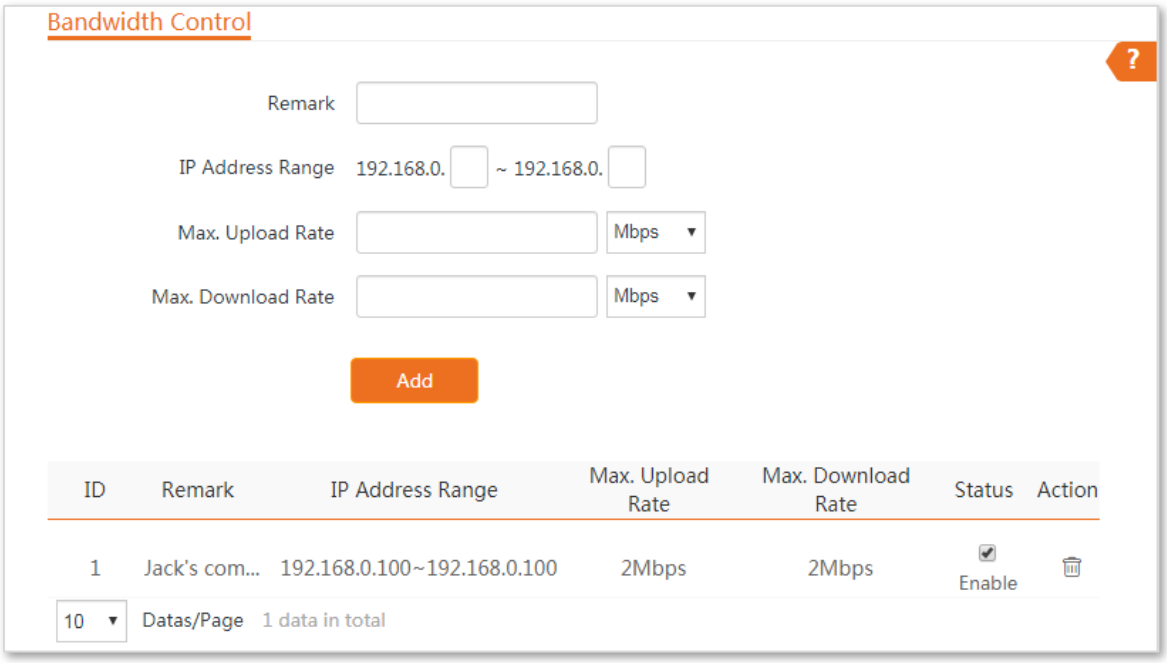


7.3.2 Configuring bandwidth control

Step 1 Log into the web UI of the device, and choose **Advanced** >**Bandwidth Control**.

Step 2 Set related parameters.

Step 3 Click **Add**.



----End

Parameters description

Name	Description
Remark	Mandatory. It specifies the additional information of the bandwidth control rule. For convenient management, you'd better specify different remarks for different rules.
IP Address Range	It specifies the IP address or IP address range of devices that this rule applies to. • **To control a single device**: Enter the same IP address in the two input boxes. • **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 clients controlled by the rule.
Max. Download Rate	
Status	It specifies the current status of the rule. You can enable or disable it as required.
Action	Click to delete the rule.

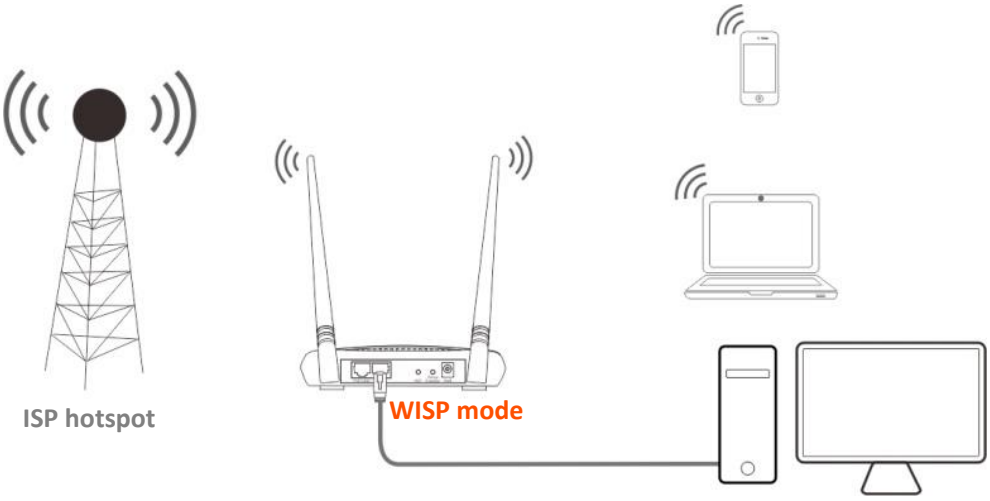
7.3.3 Example of configuring bandwidth control

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.

Assume that: 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 **192.168.0.100** to **192.168.0.200**.

Network topology



Configuration procedure

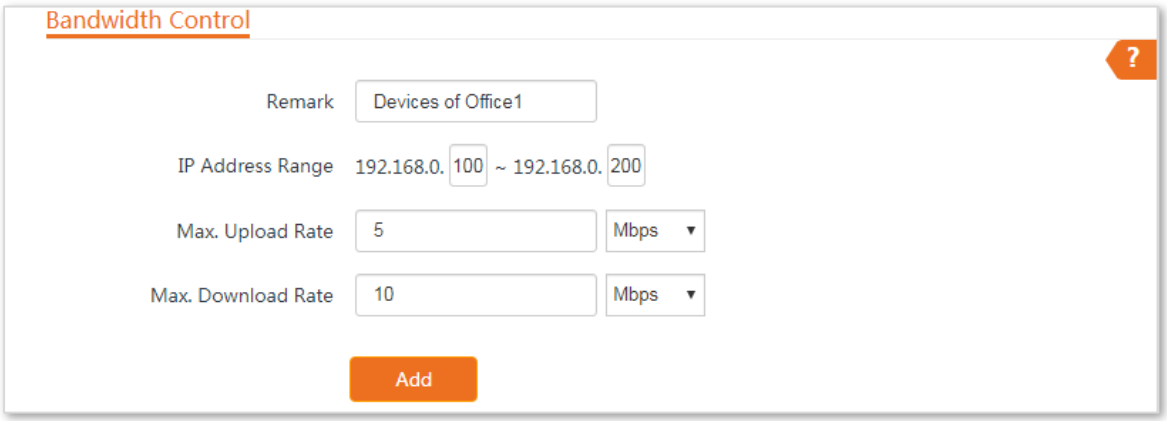
Step 1 Log into the web UI of the device, and choose **Advanced** > **Bandwidth Control**.

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.

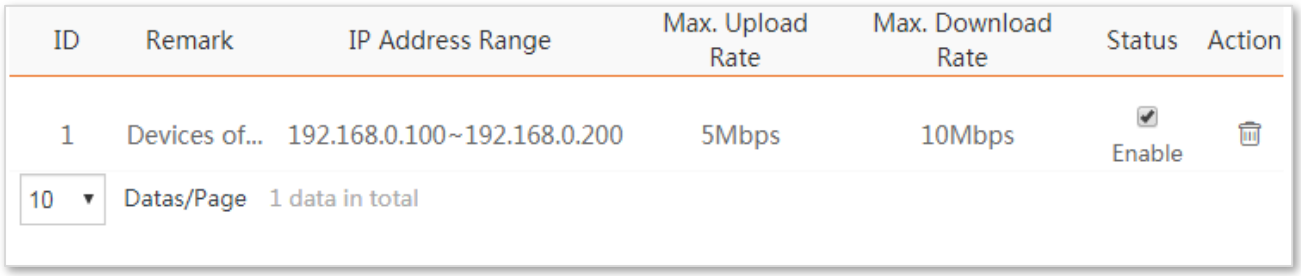
Step 4 Specify the maximum upload rate and download rate respectively, which are **5** and **10** in this example.

Step 5 Click **Add**.



----End

Added successfully. See the following figure:



Verification

For clients with IP addresses falling into the range through 192.168.0.100 to 192.168.0.200 , their upload and download rates will not exceed the maximum and minimum limits you set.

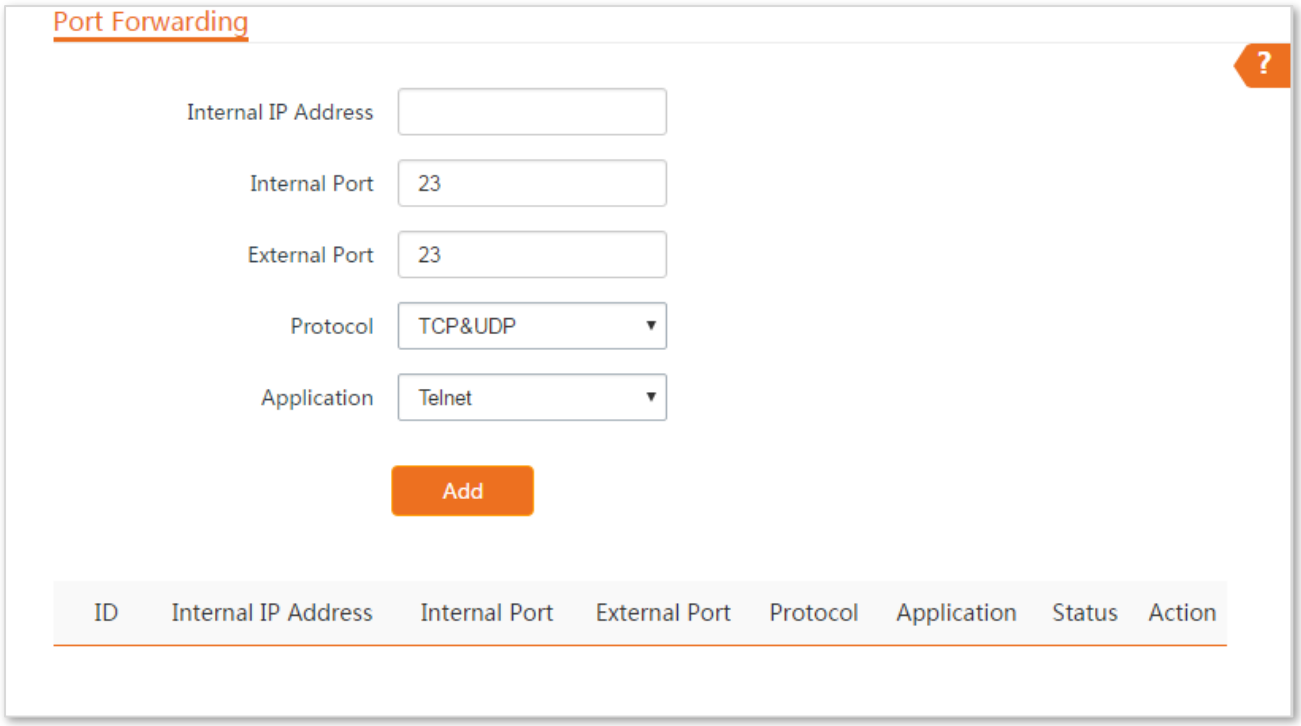
7.4 Port forwarding

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.

To access the page, choose **Advanced** > **Port Forwarding**.



7.4.2 Configuring port forwarding

Step 1 Log into the web UI of the device, and choose **Advanced** > **Port Forwarding**.

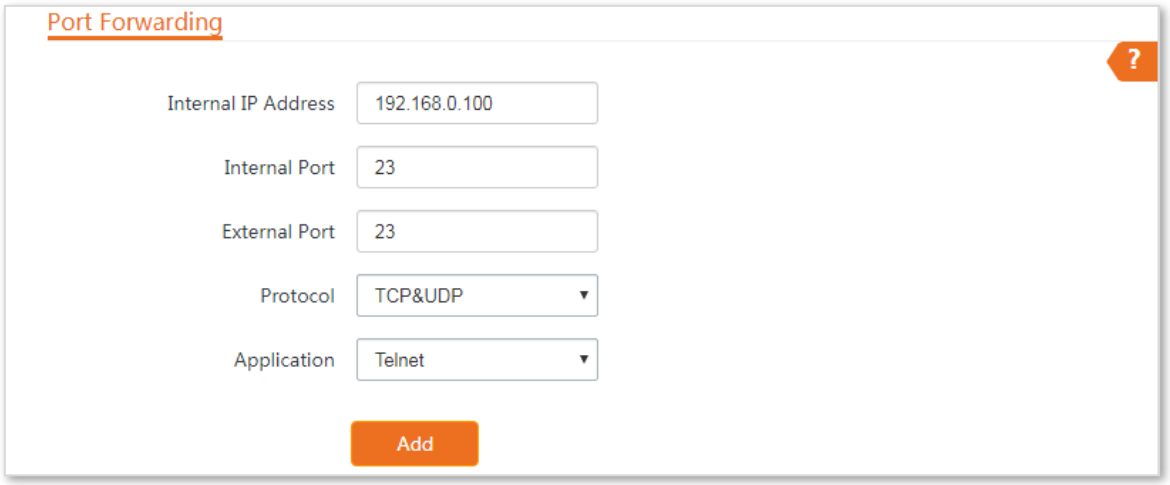
Step 2 Enter the IP address of a server established in LAN.

Step 3 Enter the internal and external ports you enable for the service.
If you are uncertain about them, select an **Application** and the internal and external ports will be populated automatically.

Step 4 Select the protocol.

If you are uncertain about it, select **TCP&UDP**.

Step 5 Click **Add**.



----End

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.
External Port	It specifies the ports enabled for WAN users.
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. If you are uncertain about the internal and external port number, you can select an application, the internal and external port number will be auto 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.

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

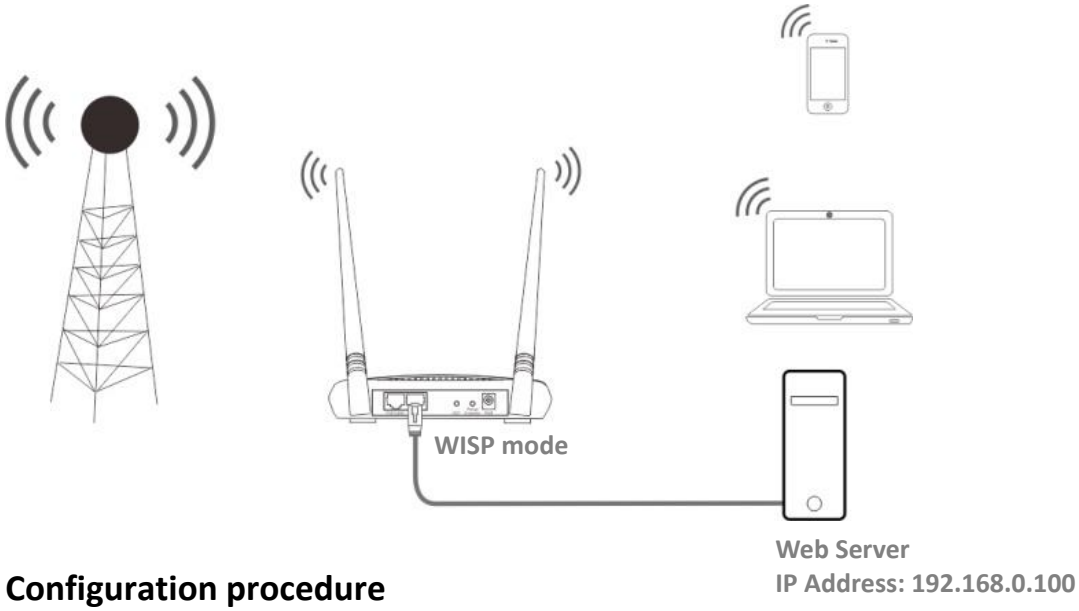
You are recommended to use port forwarding function to meet the requirement.

Assume that:

- IP Address of the web server: 192.168.0.100

- 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

TIP

A dynamic IP address of the web server may invalidate the port forwarding function. Therefore, set the web server to use a static IP address.

Step 1 Log in to the web UI of the device, and choose **Advanced** > **Port Forwarding**.

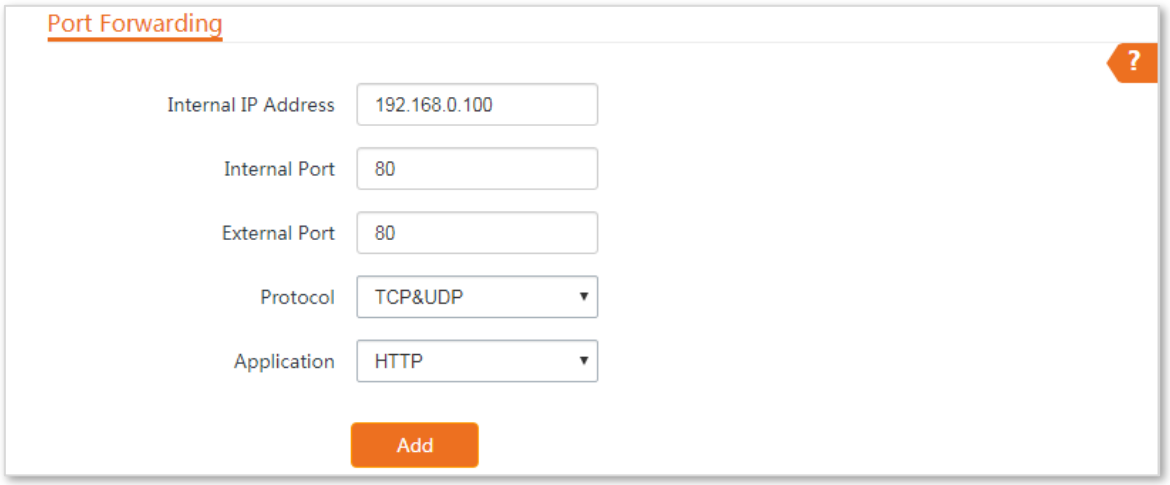
Step 2 Enter the IP address of the web server in the **Internal IP Address** box, which is **192.168.0.100** in this example.

Step 3 Enter the internal and external ports you enable for the service.

If you are uncertain about them, select an **Application** and the internal and external ports will be populated automatically.

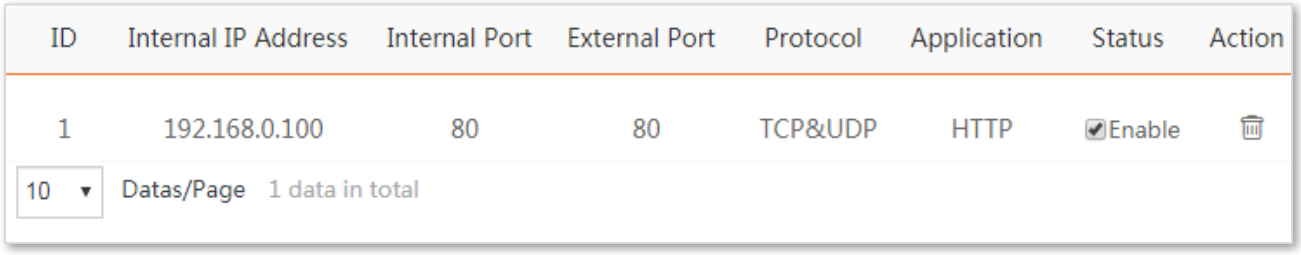
Step 4 Select **TCP&UDP** from the drop-down list of **Protocol**.

Step 5 Click **Add**.



----End

Added successfully. 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**.

NOTE

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

- Ensure that the WAN IP address is a public IP address. A private WAN IP address may invalidate the port forwarding function. Common IPv4 IP addresses include A, B, and C types: A type ranges from 10.0.0.0 to 10.255.255.255; B type ranges from 172.16.0.0 to 172.31.255.255; C type ranges from 192.168.0.0 to 192.168.255.255.
- Ensure that the internal and external port you entered are 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.
- Assign a static IP address to the web server in case of service disconnection caused by the dynamic IP address.

7.5 MAC filter

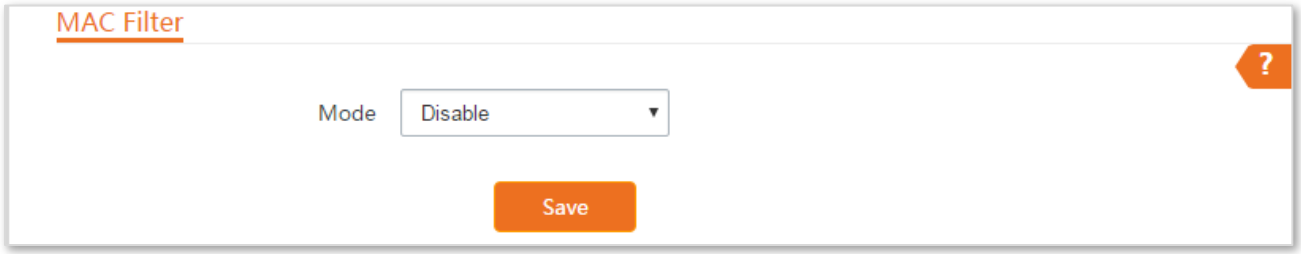
This function is available only when the device works in **WISP** or **Router** mode.

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 at what time and on what days based on their MAC addresses.

To access the page, choose **Advanced** > **MAC Filter**.

The function is disabled by default.



7.5.2 Configuring MAC filter

Step 1 Log into the web UI of the device, and choose **Advanced** > **MAC Filter**.

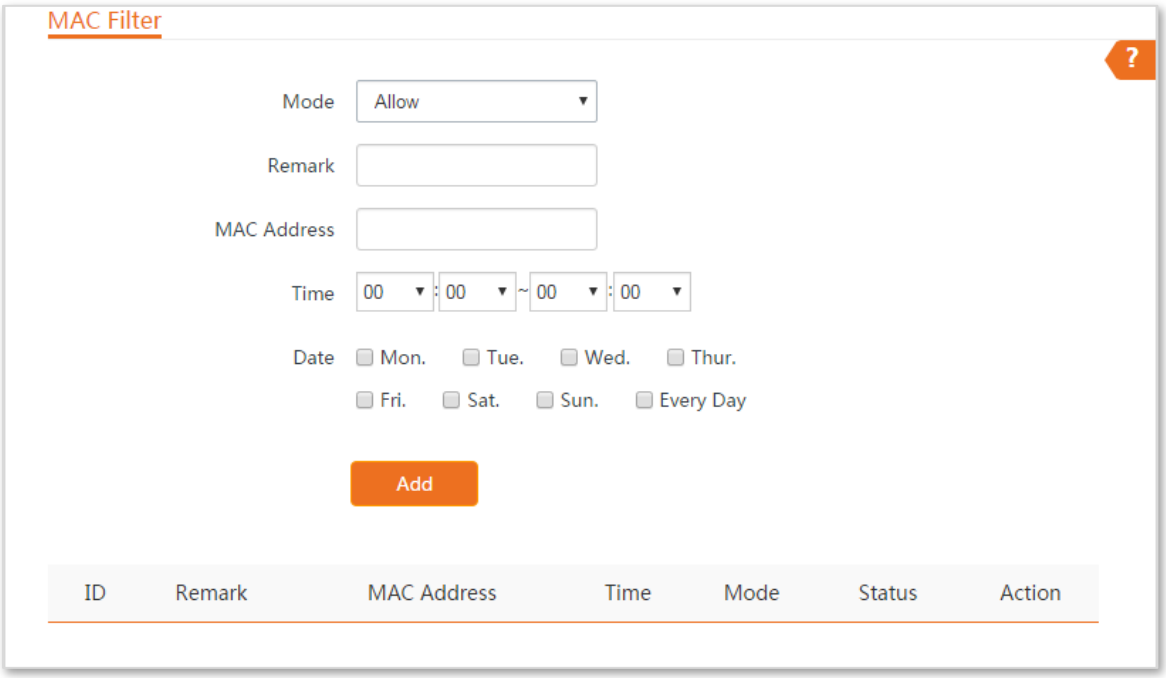
Step 2 Select a MAC filter mode, **Disallow** or **Allow**.

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**.



----End

Parameters description

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

7.5.3 Example of configuring MAC filter

Network requirement

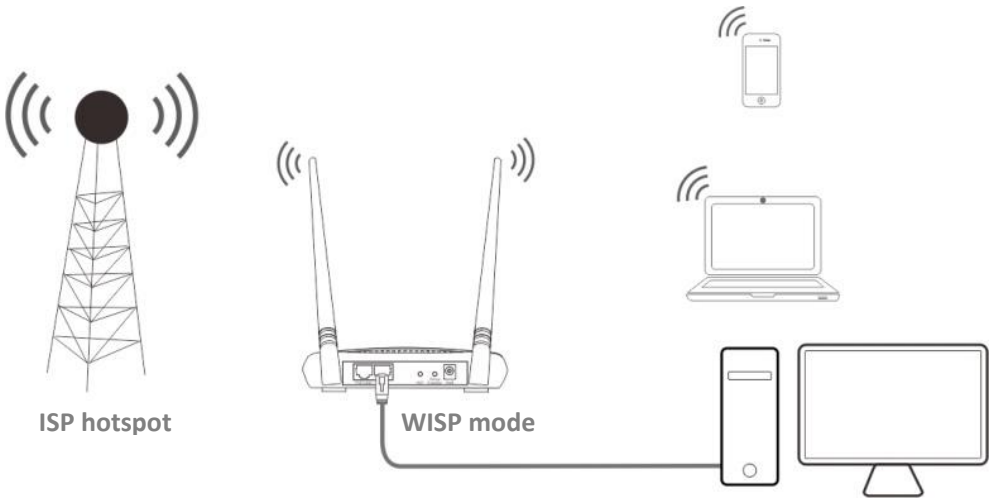
The device is used to bridge to the ISP hotspot for internet access in a house in the countryside, and the device is set to WISP mode.

Only allow the kids' devices to access the internet during 17:00 to 21:00, Monday to Friday).

You are recommended to use the MAC Filter function to meet the requirement.

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

Network topology



Configuration procedure

Step 1 Log in to the web UI of the device, and choose **Advanced** > **MAC Filter**.

Step 2 Select a mode, which is **Allow** in this example.

Step 3 Enter a brief description in the **Remark** input box, which is **Tom's smartphone** in this example.

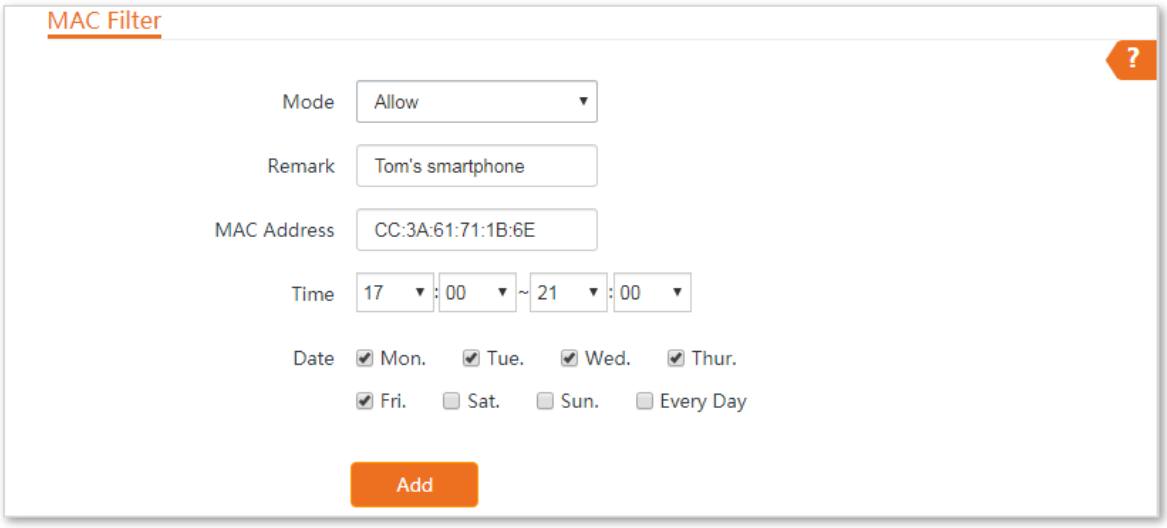
Step 4 Enter the MAC address of the device, which is **CC:3A:61:71:1B:6E** in this example.

Step 5 Specify a period, which is **17:00** to **21:00** 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.



----End

Added successfully. See the following figure:

ID	Remark	MAC Address	Time	Mode	Status	Action
1	Tom's smar...	CC:3A:61:71:1B:6E	Mon.、Tue.、Wed.、Thur.、Fri. 17:00-21:00	Allow	Enable	
2	Marry's la...	CC:3A:61:75:1F:3E	Mon.、Tue.、Wed.、Thur.、Fri. 17:00-21:00	Allow	Enable	

10 Datas/Page 2 data in total

Verification

The devices with the MAC addresses of CC:3A:61:71:1B:6E and CC:3A:61:75:1F:3E can only access the internet at 17:00 to 21:00 from Monday to Friday.

7.6 Network service

7.6.1 DDNS

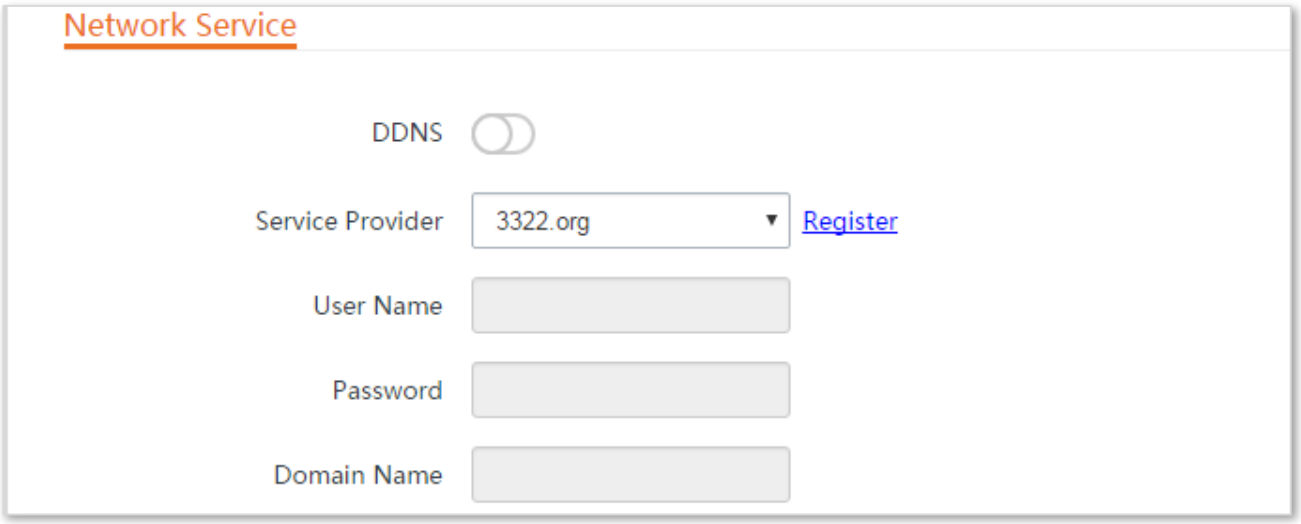
This function is available only when the device works in **WISP** or **Router** mode.

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

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.

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

Configuring DDNS



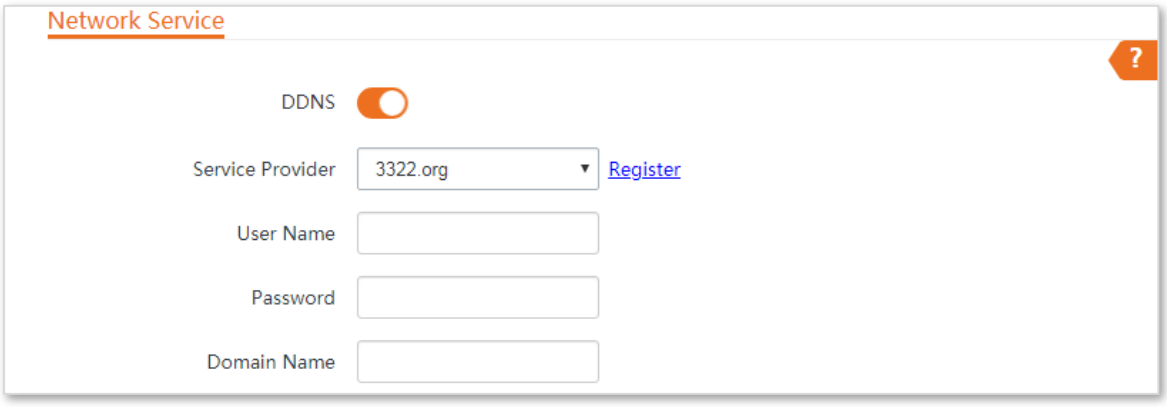
Step 1 Log in to the web UI, and choose **Advanced** > **Network Service**.

Step 2 Enable the **DDNS** function.

Step 3 Select a DDNS provider from the drop-down list.

Step 4 Enter the user name and password used to log in to a DDNS provider, and domain name you registered with DDNS service provider.

Step 5 Click **Save** on the bottom of this page.



----End

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 username and password used to log in to a DDNS service provider.
Password	
Domain Name	It specifies the domain name information obtained from the dynamic DNS server.

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.

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 meet the requirement.

Assume that:

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

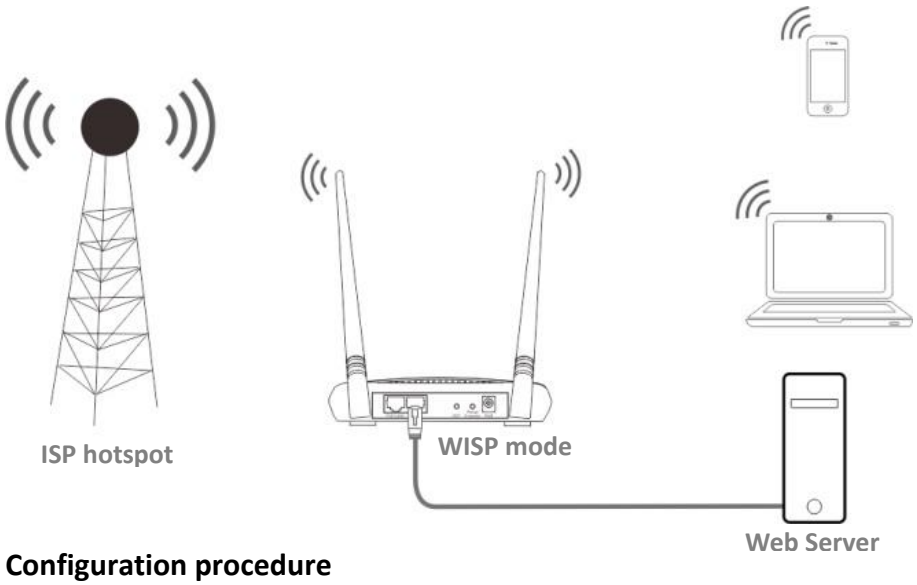
- **Static IP Address**: 192.168.0.100
- **Service Port of the Web Server**: 80

The registered domain name information is shown as follows:

- **Service Provider**: Dyndns
- **User Name**: tenda

- **Password**: tenda
- **Domain Name**: tenda.dyndns.com

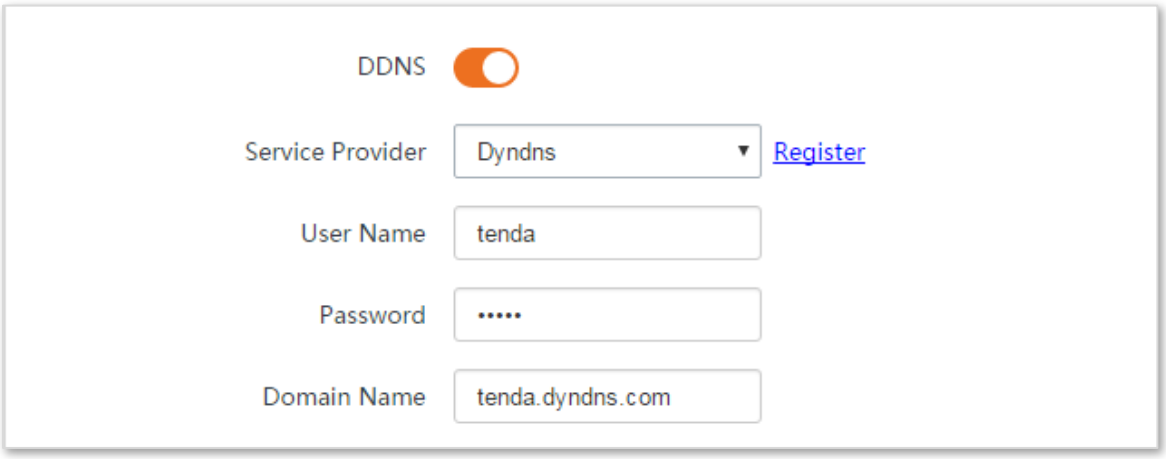
Network topology



Configuration procedure

Step 1 Set up the DDNS function.

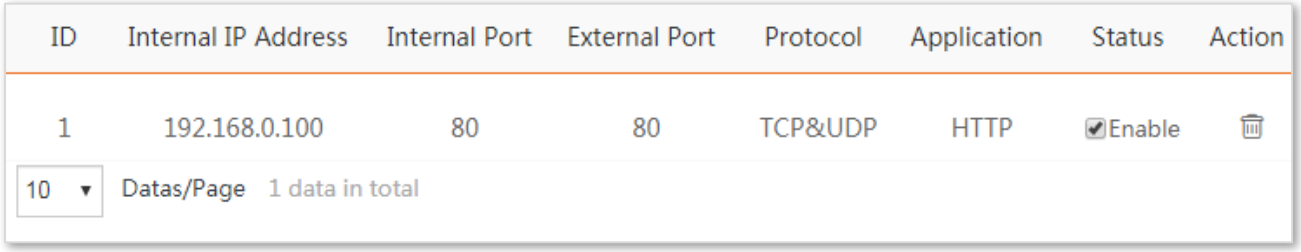
1. Log in to the web UI of the device, and choose **Advanced** > **Network Service**.
2. Enable the **DDNS** function.
3. Select a service provider, which is **Dyndns** in this example.
4. Enter the user name and password you registered with DDNS service provider, which are **tenda** and **tenda** in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



Step 2 Set up the port forwarding function by referring to Port forwarding.

----End

Added successfully. See the following figure:



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**.

7.6.2 Remote web management

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.

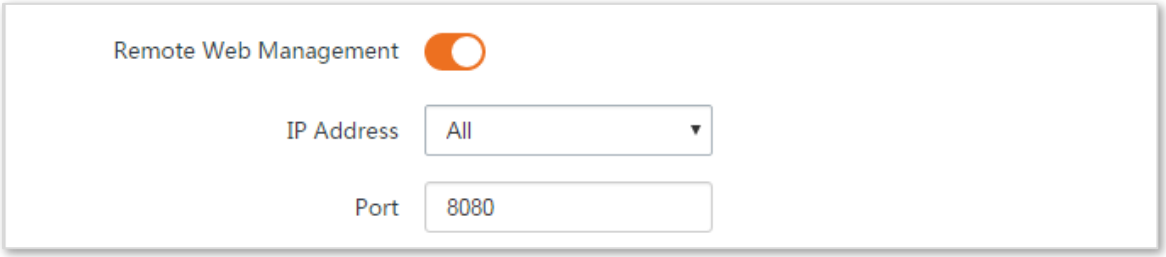
Configuring remote web management

Step 1 Log in to the web UI of the device, and choose **Advanced** > **Network Service**.

Step 2 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 3 Enter a port number.

Step 4 Click **Save** on the bottom of this page.



----End

Parameters description

Name	Description
Remote Web Management	It specifies whether to enable the remote web management function.
IP Address	It specifies the IP address of a device which is allowed to access the web UI of the

Name	Description
	device. • **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. 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

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.

Networking requirement

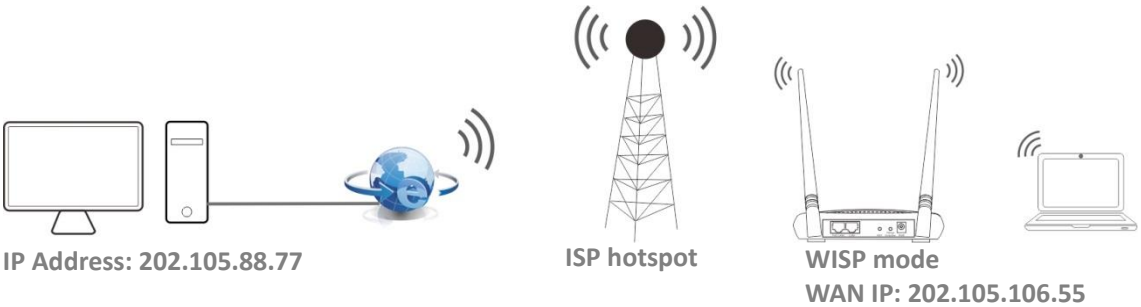
The host needs to troubleshoot the network when he is on business. So he needs to access the device's web UI on WAN.

You are recommended to use the remote web management function to meet the requirement.

Assume that:

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

Network topology



Configuration procedure

Step 1 Log in to the web UI of the device, and choose **Advanced** > **Network Service**.

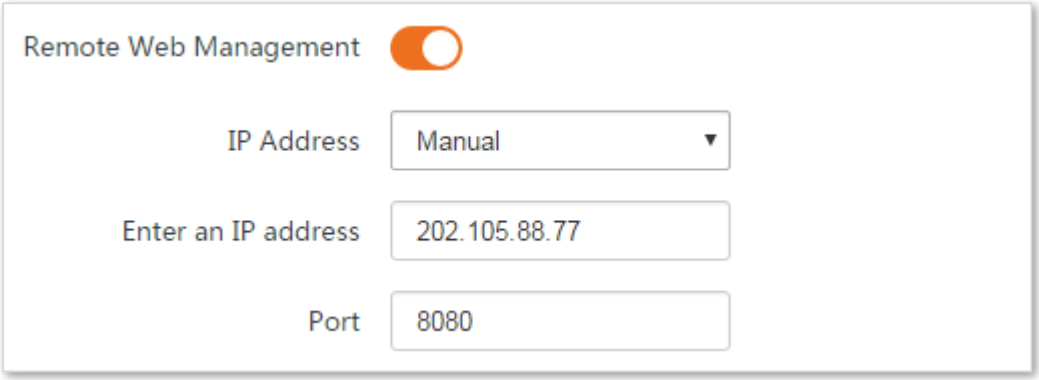
Step 2 Enable the **Remote Web Management** function.

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.



----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.

Configuring reboot schedule

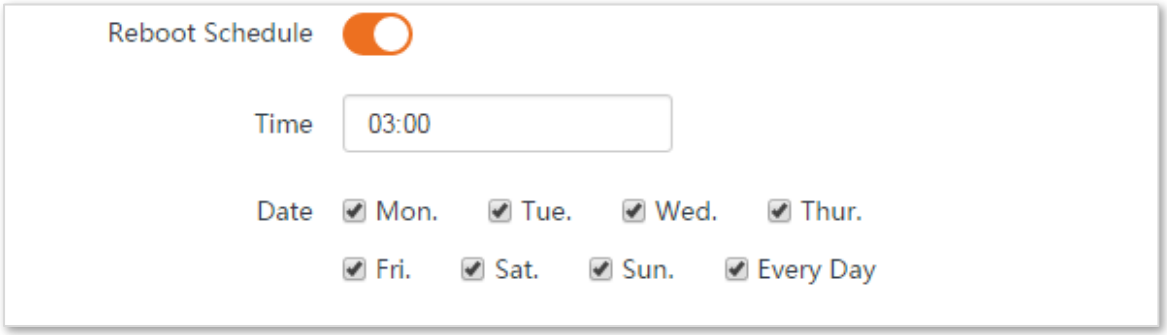
Step 1 Log in to the web UI of the device, and choose **Advanced** > **Network Service**.

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.



----End

The device reboots every day at 3:00.

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.

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

You can change the login timeout interval as required.

7.6.5 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.

Configuration procedure

Step 1 Log in to the web UI of the device, and 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.

----End

Parameters description

Name	Description
Ping Watch Dog	It specifies whether to enable the **Ping Watch Dog** function.
IP Address	It specifies the target IP address that the device pings.

Name	Description
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, but does not receive response.

7.6.6 DMZ host

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

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

NOTE

- 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

Step 1 Log into the web UI of the device, and 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.

----End

Example of configuring DMZ host

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

Networking requirement

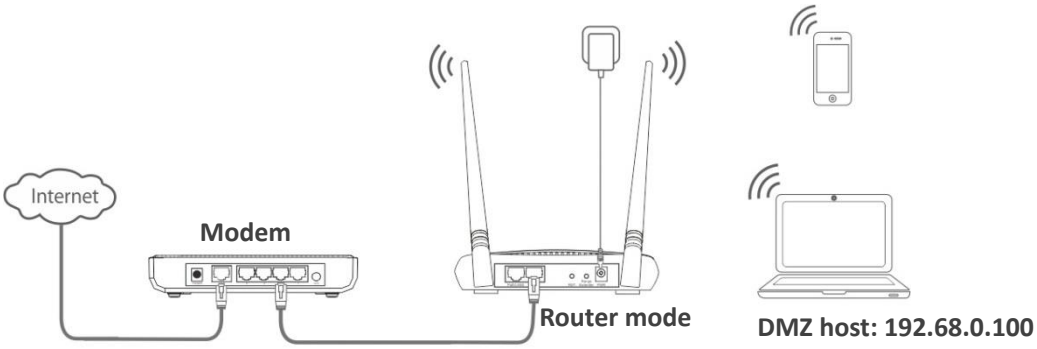
The administrator on business can visit the resources on web server in LAN.

You can use DMZ Host function to meet the requirement.

Assume that:

- 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

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 into the web UI of the device, and 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 **192.168.0.100** in this example.

Step 4 Click **Save** on the bottom of this page.

----End

Verification

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

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

NOTE

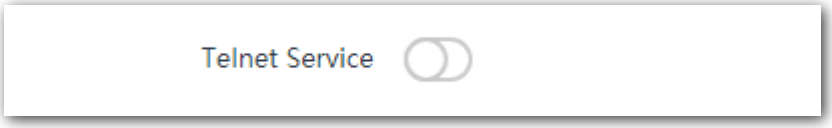
If the administrator still cannot visit the web server in LAN after the configuration, try the following solutions:

- Ensure that the WAN IP address is a public IP address. A private WAN IP address may invalidate the port forwarding function. Common IPv4 IP addresses include A, B, and C types: A type ranges from 10.0.0.0 to 10.255.255.255; B type ranges from 172.16.0.0 to 172.31.255.255; C type ranges from 192.168.0.0 to 192.168.255.255.
- Try accessing **Protocol name**://**domain name:port number**
- Security software, antivirus software, and the built-in OS firewall of the computer may cause port forwarding function failures. Disable them and try again.
- Assign a static IP address to the DMZ host in case of service interrupt caused by the dynamic IP address.

7.6.7 Telnet service

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

To access the page, choose **Advanced** > **Network Service**. By default, the function is disabled.



7.6.8 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.

To access the page, choose **Advanced** > **Network Service**. By default, the function is disabled. You can enable it as required.

7.6.9 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.

To access the page, choose **Advanced** > **Network Service**. By default, the function is enabled.

8 Tools

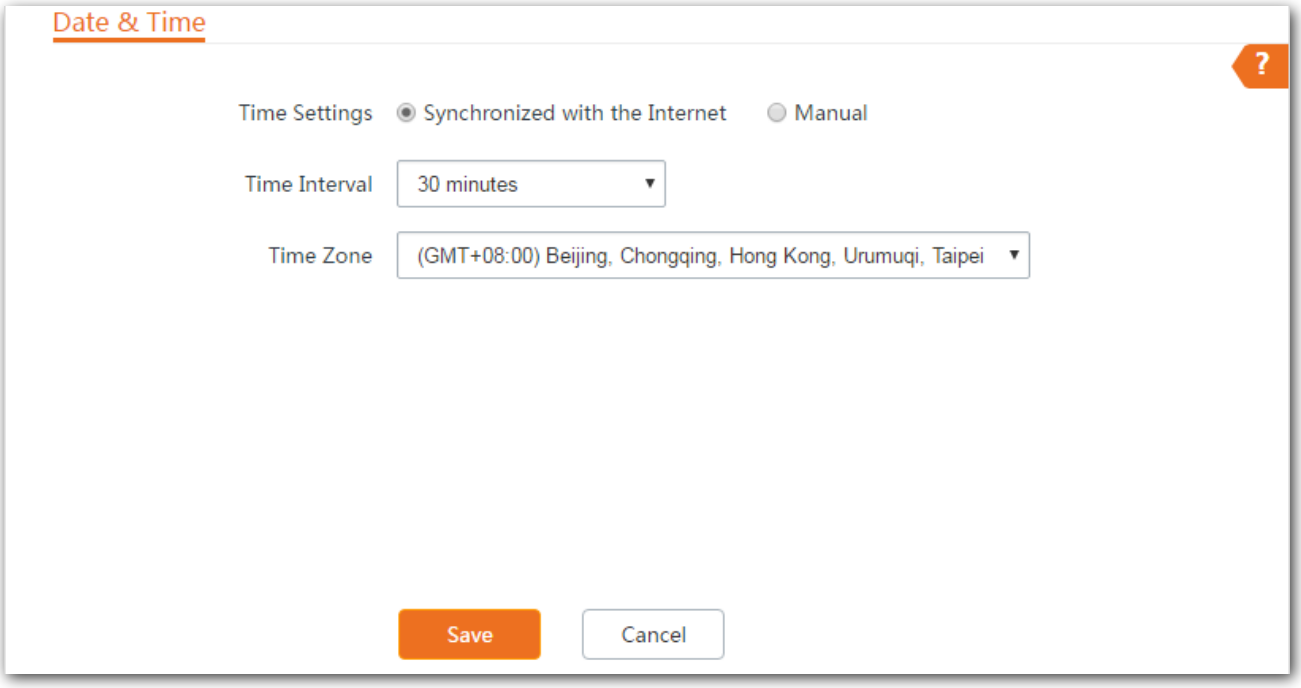
8.1 Date & time

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

Ensure that the system time of the device is correct, so that time-based functions can be executed correctly.

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.

To access the page, choose **Tools** > **Date & Time**.



8.1.1 Synchronized with the Internet

The device automatically synchronizes its system time with a time server of the internet.

TIP

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

Configuration procedure

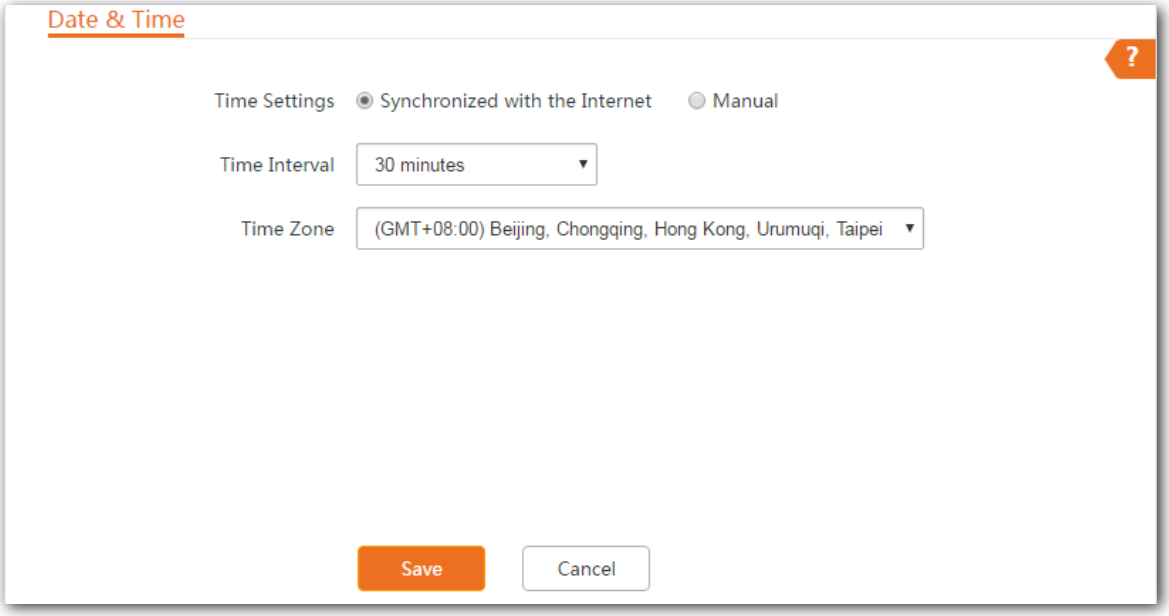
Step 1 Log in to the web UI of the device, and choose **Tools** > **Date & Time**.

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**.



----End

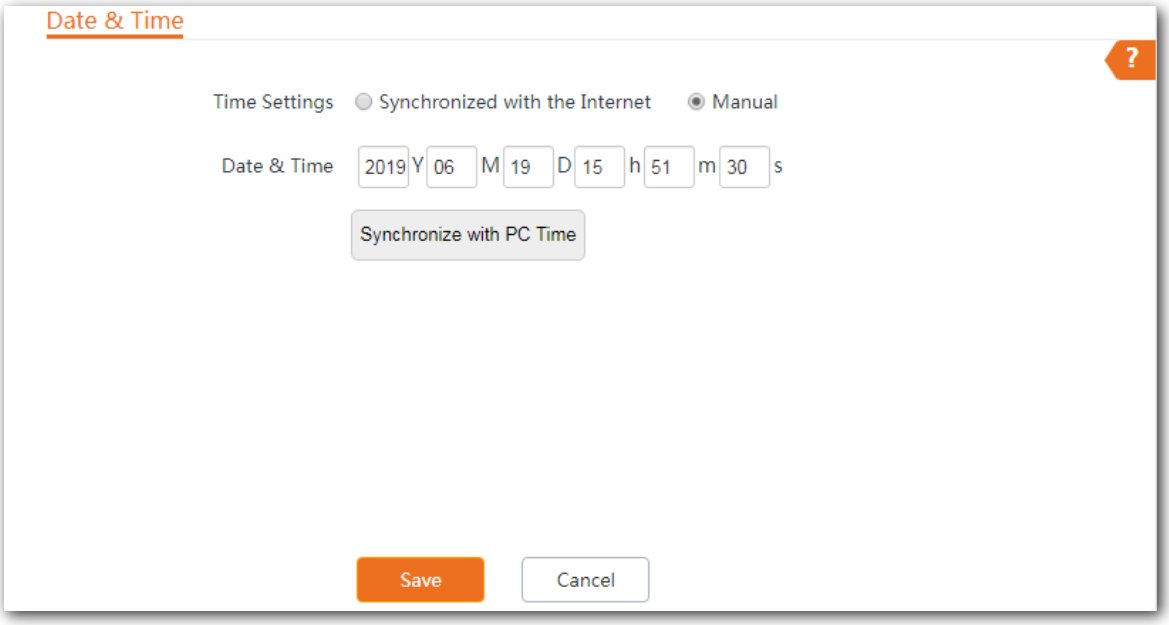
8.1.2 Specifing the date and time manually

Step 1 Log in to the web UI of the device, and 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 of the management computer.

Step 4 Click **Save**.



----End

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.

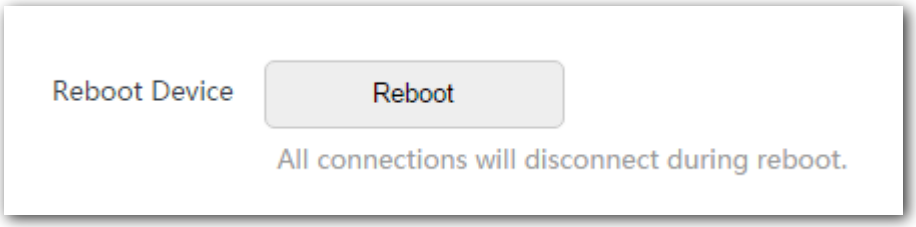
TIP

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

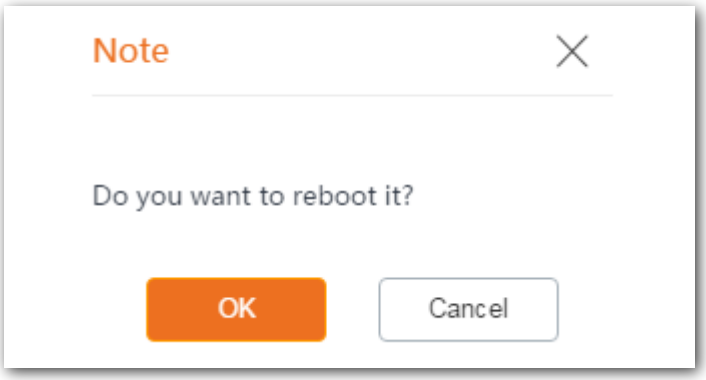
Configuration procedure

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

Step 2 Click **Reboot**.



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



----End

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.

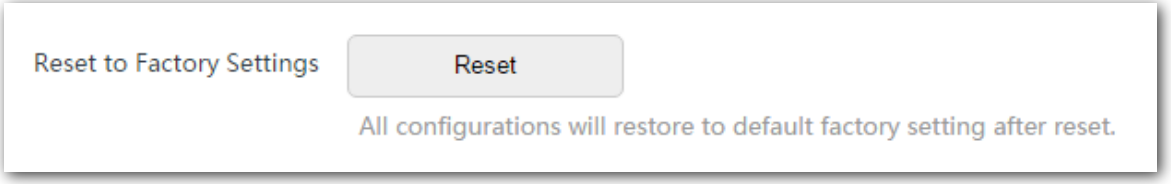
NOTE

- When the factory settings are restored, the configuration of the device is cleared.
- To prevent device damages, do not power off the device during resetting.
- When the factory settings are restored, the login IP address is **192.168.0.254**, and both login user name and password are **admin**.

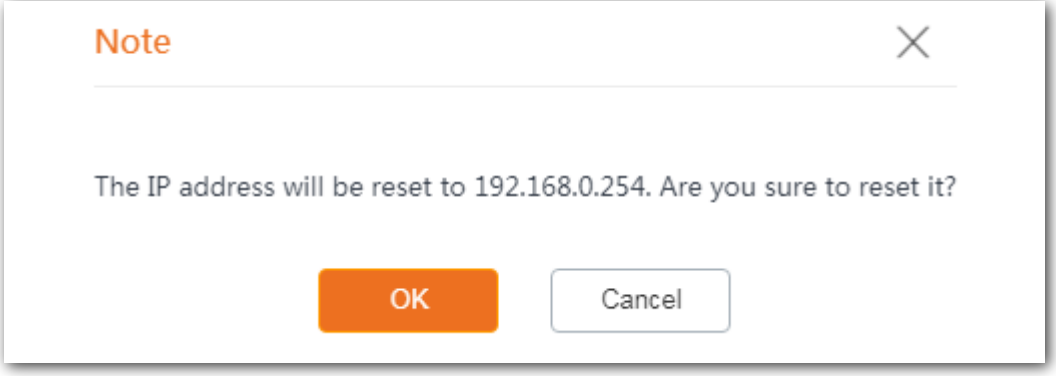
Configuration procedure

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

Step 2 Click **Reset**.



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



----End

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.

NOTE

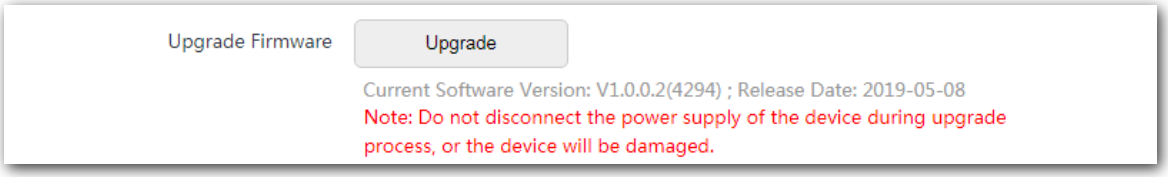
To prevent damaging the device, verify that the new firmware version is applicable to the device before upgrading the firmware and keep the power supply of the device connected during an upgrade.

Configuration procedure

Step 1 Download the file of the latest firmware version for the device from www.tendacn.com to your local computer, and unzip it.

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. Ensure that the suffix of the upgrade file is **.bin**.

----End

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

TIP

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

8.2.4 Backup/restore

The backup function enables you to export the configuration of the device to a local computer, and import the configuration file you export before.

You are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the device.

NOTE

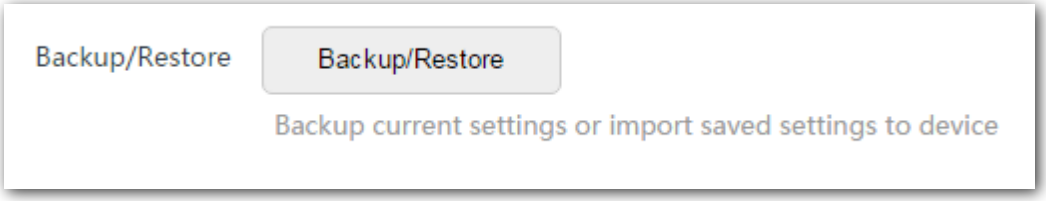
If you need to apply same or similar configurations to many devices, you can configure one of the devices, back up the configuration of the device, and use the backup to restore the configuration on the other devices. This improves configuration efficiency.

Backup

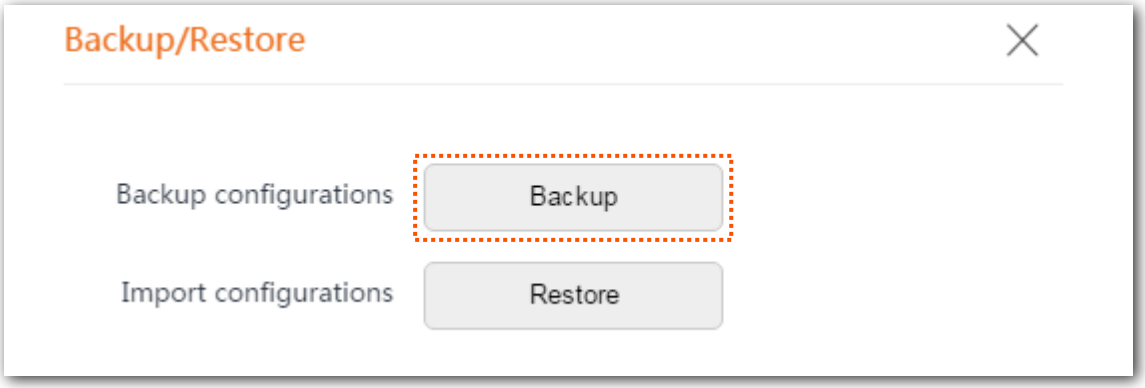
Configuration procedure

Step 1 Log in to the web UI of the device, and choose **Tools** > **Maintenance**.

Step 2 Click **Backup/Restore**.



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



----End

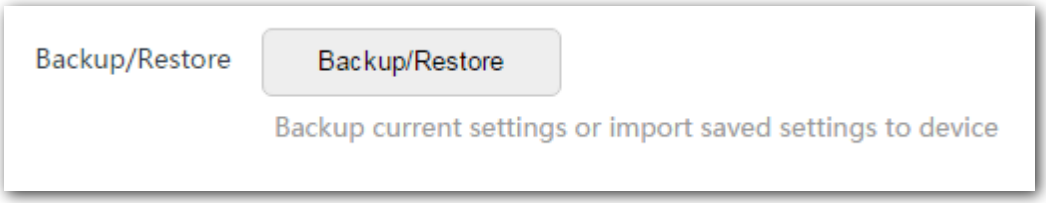
A file named **APCfm.cfg** is downloaded to your local computer.

Restore

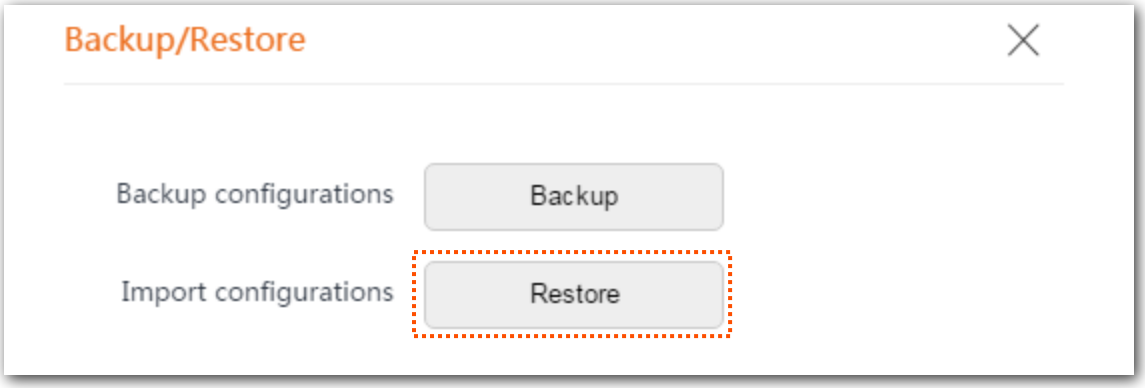
Configuration procedure

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

Step 2 Click **Backup/Restore**.



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



Step 4 Select and upload the file you export before.

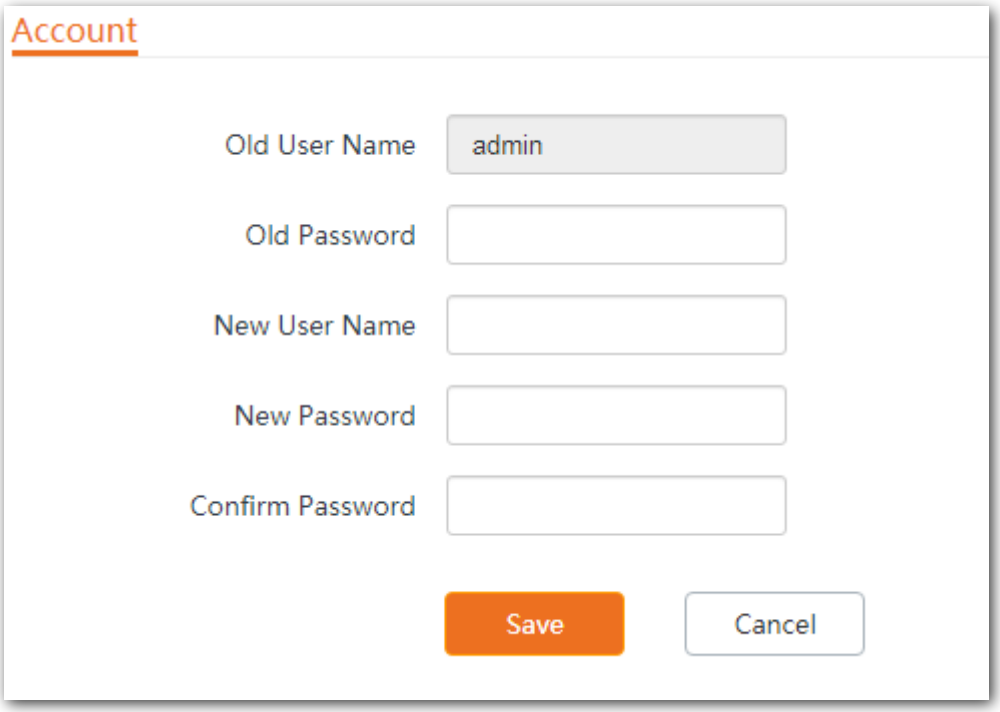
----End

Wait for the progress bar completes. 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. Both the default user name and password are **admin**.



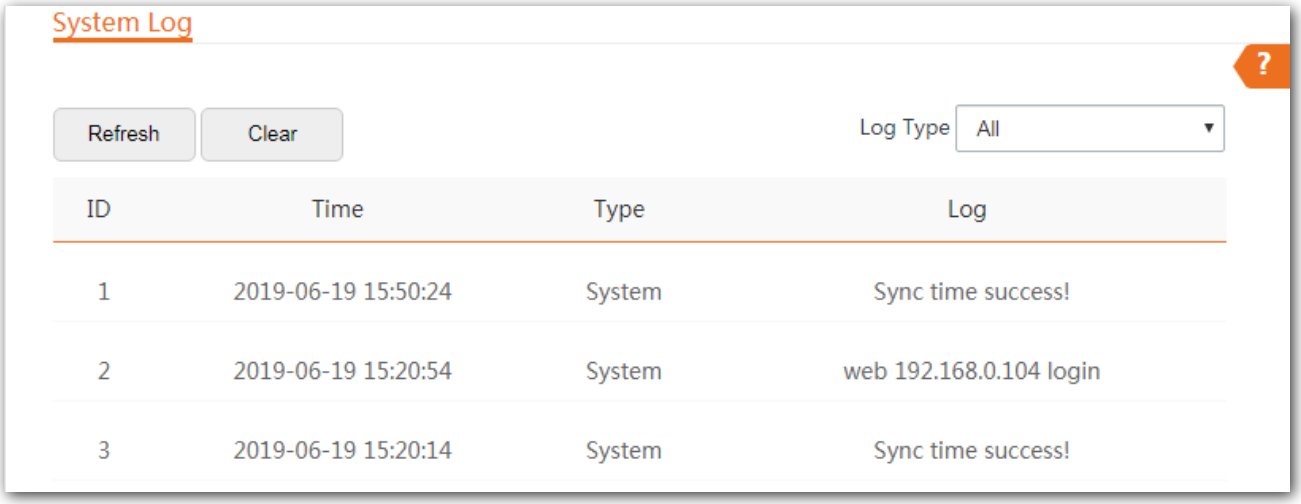
Parameters description

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

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.



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**.

NOTE

- When the device reboots, the previous logs are cleared.
- 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

Default parameters

The default parameters are shown in the following table:

Parameters		AP4/AP5
Login	Login IP Address	192.168.0.254
	Account	admin/admin
Quick Setup	Working Mode	AP mode
LAN Setup	IP Address Type	Static IP address
	IP Address	192.168.0.254
	Subnet Mask	255.255.255.0
DHCP Server		Enable
VLAN Settings	VLAN Settings	Disable
SSID		Support 2 WiFi networks at most. The default SSID is Tenda_*XXXXXX*. *XXXXXX* is the last six characters of the LAN MAC address with a range of XXXXXX to XXXXXX + 1. The first SSID is enabled and the other one is disabled.
Wireless > Basic	WiFi network	Enabled
	Network mode	11b/g/n
LAN Rate	PoE/LAN Speed	Auto Negotiation
	LAN Speed	