tp-link

PHAROS

User Guide

For TP-Link Pharos Series Products

1910012759 REV 3.3.0

April 2020

CONTENTS

About this User Guide 1

Overview 2

1 Operation Modes 3

1.1 Access Point 4

1.2 Client 5

1.3 AP Client Router (WISP Client) 6

1.4 AP Router 6

1.5 Repeater 7

1.6 Bridge 7

2 Quick Start 8

2.1 Check the System Requirements 9

2.2 Log In to the Device 9

2.3 Set Up the Wireless Network 10

Access Point 11

Client 15

Repeater 20

Bridge 25

AP Router 30

AP Client Router (WISP Client) 36

3 Monitor the Network 43

3.1 View the Device Information 44

3.2 View the Wireless Settings 44

3.3 View Wireless Signal Quality 45

3.4 View Radio Status 46

3.5 View the LAN Settings 48

3.6 View the WAN Settings 49

3.7 Monitor Throughput 50
3.8 Monitor Stations 50
3.9 Monitor Interfaces 53
3.10 Monitor ARP Table 53
3.11 Monitor Routes 54
3.12 Monitor DHCP Clients 55
3.13 Monitor Dynamic WAN 55

4 Configure the Network 58
4.1 Configure WAN Parameters 59
4.2 Configure LAN Parameters 69
Access Point/Client/Repeater/Bridge Mode 69
AP Router/AP Client Router Mode 74
4.3 Configure Management VLAN 76
4.4 Configure the Forwarding Feature 77
4.5 Configure the Security Feature 81
4.6 Configure Access Control 84
4.7 Configure Static Routing 85
4.8 Configure Bandwidth Control 86
4.9 Configure IP & MAC Binding 88

5 Configure the Wireless Parameters 90
5.1 Configure Basic Wireless Parameters 91
5.2 Configure Wireless Client Parameters 94
5.3 Configure Wireless AP Parameters 98
5.4 Configure Multi-SSID 104
5.5 Configure Wireless MAC Filtering 106
5.6 Configure Advanced Wireless Parameters 107

6 Manage the Device 110
6.1 Manage System Logs 111

6.2 Specify the Miscellaneous Parameters 112
6.3 Configure Ping Watch Dog 113
6.4 Configure Dynamic DNS 114
6.5 Configure Web Server 115
6.6 Configure SNMP Agent 116
6.7 Configure SSH Server 118
6.8 Configure RSSI LED Thresholds 119

7 Configure the System 120
7.1 Configure Device Information 121
7.2 Configure Location Information 121
7.3 Configure User Account 121
7.4 Configure Time Settings 122
7.5 Update Firmware 124
7.6 Configure Other Settings 125

8 Use the System Tools 126
8.1 Configure Ping 127
8.2 Configure Traceroute 127
8.3 Test Speed 128
8.4 Survey 129
8.5 Analyze Spectrum 131
8.6 Antenna Alignment 132

About this User Guide

This User Guide contains information for setup and management of TP-Link Pharos series products. Read this guide carefully before operation.

When using this guide, notice that features available in Pharos series products may vary by model and software version. Availability of Pharos series products may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit *https://www.tp-link.com*.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure the accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

Convention

Unless otherwise noted, the introduction in this guide takes CPE510 as an example.

More Info

The latest software, management app and utility can be found at Download Center at *https://www.tp-link.com/support*.

The Quick Installation Guide can be found where you find this guide or inside the package of the product.

The authentication information can be found where you find this guide.

Specifications can be found on the product page at *https://www.tp-link.com*.

Our Technical Support contact information can be found at the Contact Technical Support page at *https://www.tp-link.com/support*.

To ask questions, find answers, and communicate with TP-Link users or engineers, please visit *https://community.tp-link.com* to join TP-Link Community.

Overview

PHAROS is TP-Link's next generation outdoor product series dedicated to long-distance outdoor wireless networking solutions.

PHAROS is a powerful Web-based operating system, which is integrated into all Pharos series products.

New features of Pharos series products are listed as follows:

- Provides User-friendly UI design.
- TP-Link Pharos MAXtream (Time-Division-Multiple-Access) technology improves product performance in throughput, capacity and latency, which is ideal for point-to-multipoint applications.
- Supports multiple operation modes: Access Point, Client, Repeater, Bridge, AP Router and AP Client Router (WISP Client).
- Provides system-level optimization for long-distance wireless transmission.
- Supports selectable bandwidth options.
- Supports easy antenna alignment with Wireless Signal Indicators on Web interface.
- Provides Throughput Monitor, Spectrum Analyzer, Speed Test and Ping tools.
- Supports discovery and management via Pharos Control application.

Note:

- MAXtream is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.
- Repeater mode or Bridge mode is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

1 Operation Modes

The Pharos series products support multiple operation modes to satisfy user's diverse network requirements. This chapter introduces typical usage scenarios of different modes. For more information, refer to Common Applications for Pharos Products.

1.1 Access Point

1.2 Client

1.3 AP Client Router (WISP Client)

1.4 AP Router

1.5 Repeater

1.6 Bridge

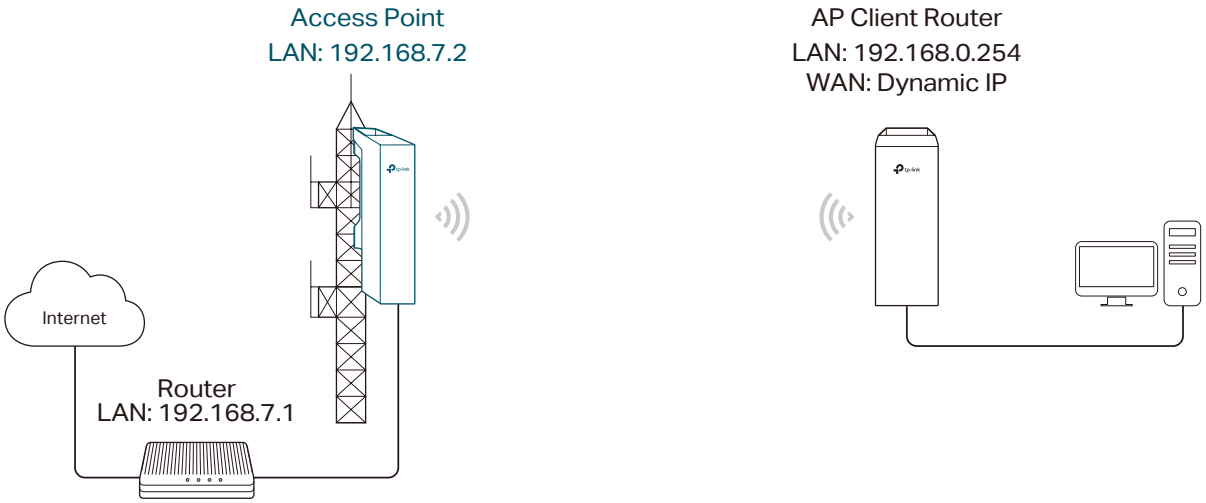
Note:

Repeater mode or Bridge mode is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

1.1 Access Point

In Access Point (AP) Mode, the device acts as a central hub and provides wireless access point for wireless clients, thus the AP Mode is applicable to the following three scenarios. Meanwhile, Multi-SSID function can be enabled in this mode, providing up to four wireless networks with different SSIDs and passwords.

■ **Scenario 1**

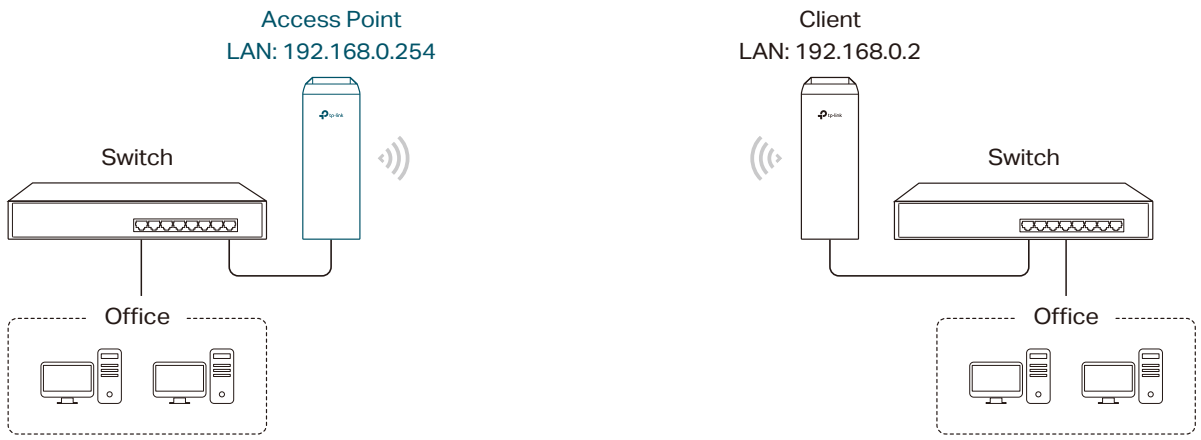


Network requirements: Establish the network coverage in the remote areas without long-distance cabling.

The device in the network: In the adjacent town covered by wired network, ISP (Internet Service Provider) can put up a device in AP Mode to access the internet and transform wired signal into wireless one. In the remote area, users can put up a device in AP Client Router Mode to access the wireless network.

Advantages: Transmit data wirelessly across a long distance and reduce the cabling cost.

■ **Scenario 2**



Network requirements: Combine two separate office networks into one.

The device in the network: The device in AP Mode connects to one office network and creates a wireless network. The device in Client Mode connects to the other office network and the wireless network.

Advantages: Establish a point-to-point WLAN across a long distance to achieve the connectivity between two networks and avoid the cabling trouble.

■ **Scenario 3**



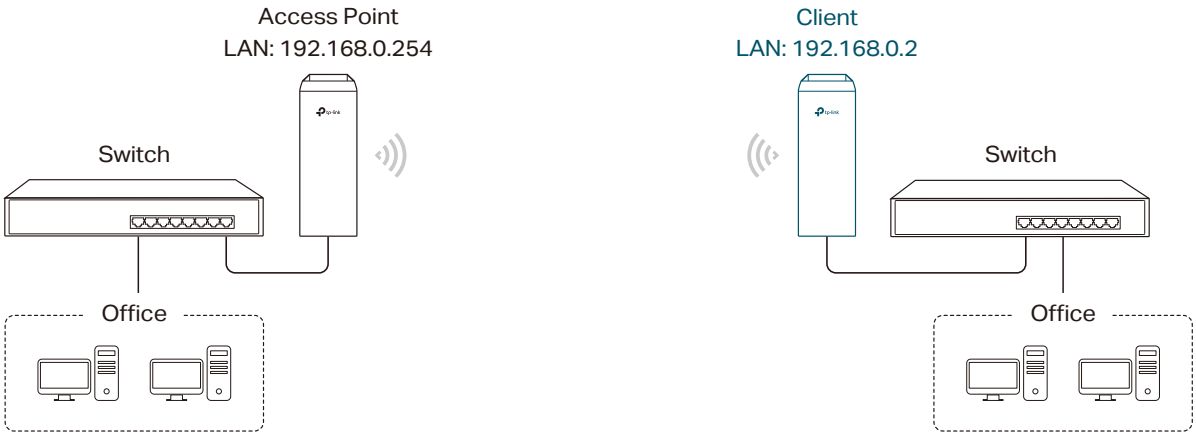
Network requirements: Establish wireless network coverage in the campus, community, industrial park or public place to provide wireless access for users.

The device in the network: With the access to campus wired network or other wired local area networks, the device in AP Mode provides the wireless access for wireless clients, such as smart phones, laptops and tablets to connect to the network.

Advantages: Enrich the access ways of local area network and extend the network coverage.

1.2 Client

For the device in Client Mode, the most common usage scenario is point-to-point networking. The device is used to transform wireless signal into wired one.

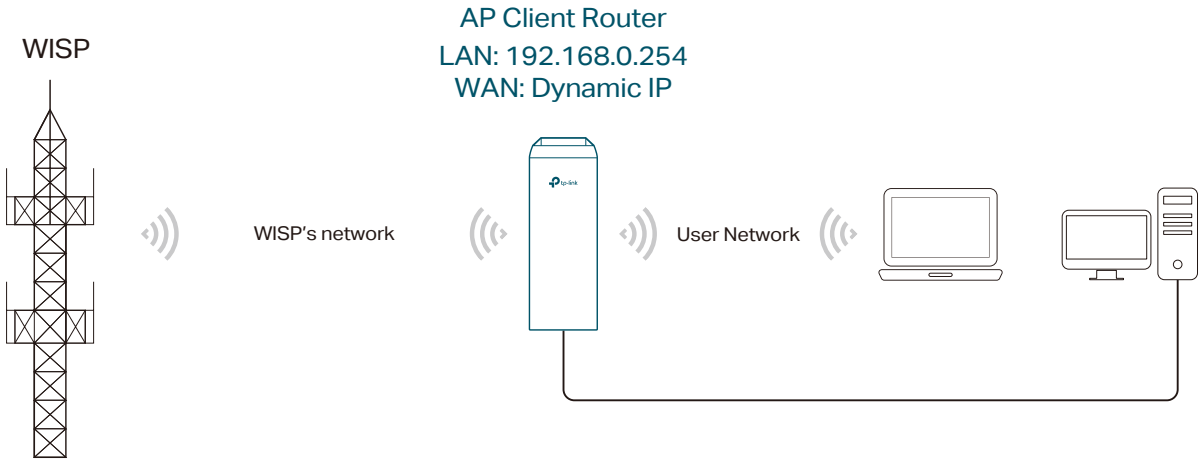


Network requirements: Help the wired devices to connect to the wireless network.

The device in the network: In Client Mode, the device actually serves as a wireless adapter to receive the wireless signal from root AP or Station. In this case, wired devices can access the wireless network by connecting to the device in Client Mode.

1.3 AP Client Router (WISP Client)

In AP Client Router Mode, the device access the internet provided by WISP (Wireless Internet Service Provider) through wireless connection. For the downstream clients, the device serves as a normal home wireless router. It can provide wired connection and wireless connection simultaneously.



Network requirements: Get internet service from WISP.

The device in the network: The device in Client Router Mode connects to WISP wirelessly for internet service. It provides both wired access and wireless access for the clients.

1.4 AP Router

The device in AP Router Mode serves as a normal home wireless router but provides a wider wireless network range.



Network requirements: Establish the wireless network coverage in the campus, community, industrial park or other public places and so on.

The device in the network: The device in AP Router Mode connects to root ADSL/Cable Modem for internet access. Meanwhile, it creates a wireless network for the wireless clients to connect to the internet.

Note:

In this mode, the device cannot be managed directly through the port connected to ADSL/Cable Modem. To manage the device, connect the management host to the device wirelessly or via the other LAN port.

1.5 Repeater

Note:

Repeater mode is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

The device in Repeater Mode can extend wireless coverage of an existing wireless network. The SSID and encryption type of the device should be the same as those of the root AP.

1.6 Bridge

Note:

Bridge mode is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

The device in Bridge Mode can extend wireless coverage of an existing wireless network. The SSID and encryption type of the device can be different from those of the root AP.

2 Quick Start

This chapter introduces how to quickly build a wireless network in different operation modes. Follow the steps below:

2.1 Check the System Requirements

2.2 Log In to the Device

2.3 Set Up the Wireless Network

2.1 Check the System Requirements

- **Operating System:**

  Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux, or Mac OS X.

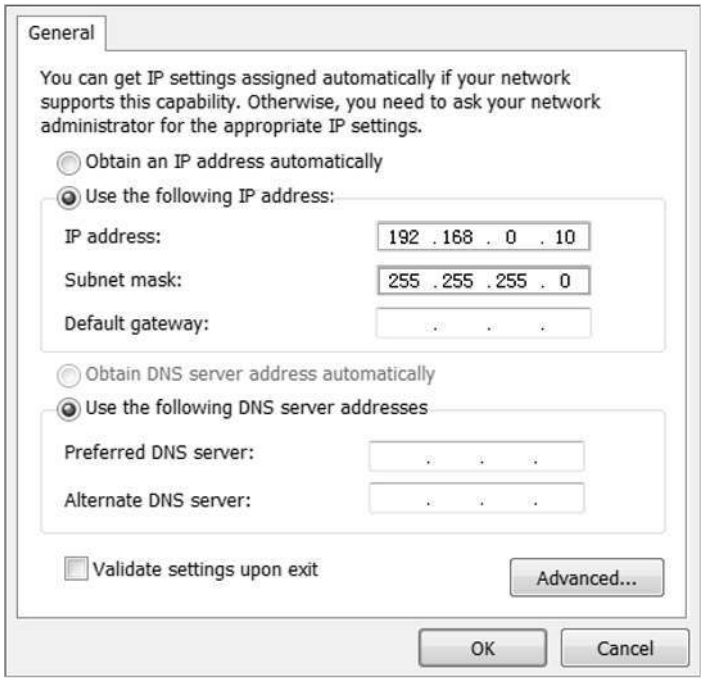
- **Web Browser**

  Google Chrome, Safari, Firefox, and Apple Safari. IE browsers are not recommended.

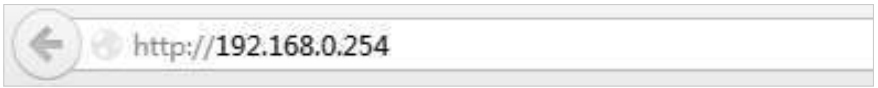
2.2 Log In to the Device

Before configuring the device, you need to access the PharOS configuration interface. Follow the steps below:

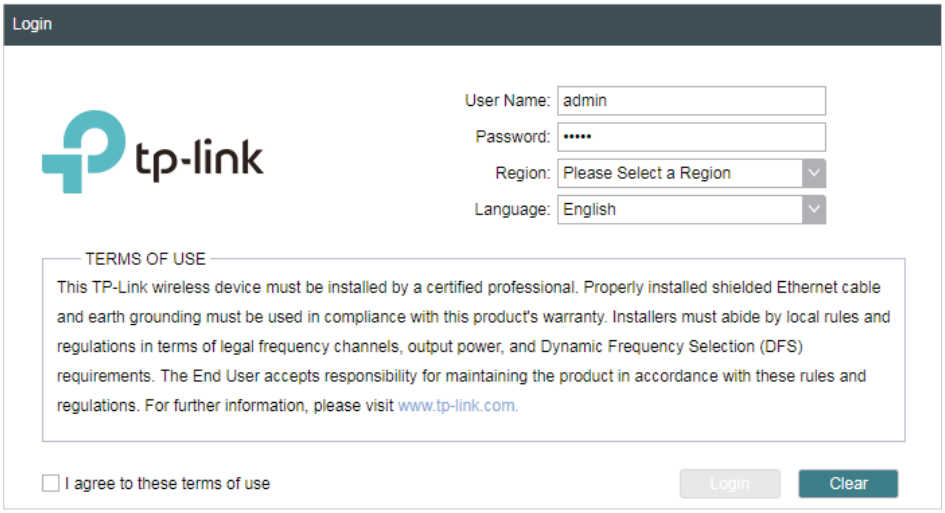
1. Connect your PC to the device.
2. Set the IP address of your PC as static IP address on 192.168.0.X subnet (X ranges from 2 to 253, e.g.192.168.0.10).



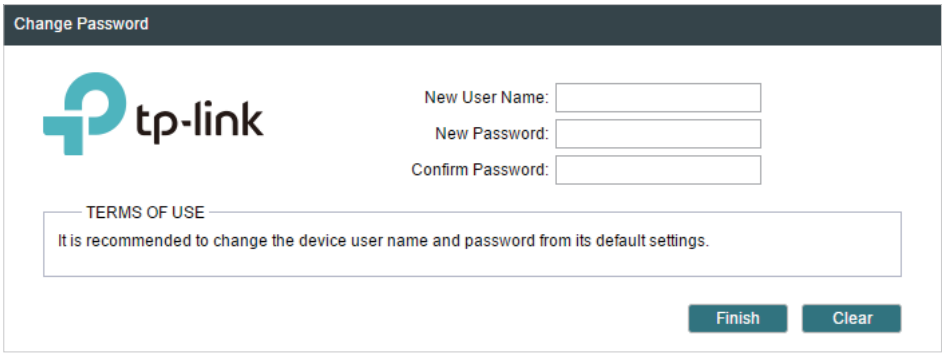
3. Launch a web browser on and enter **the management IP address of the device (192.168.0.254 by default)** in the address bar to load the login page of the PharOS configuration interface.



4. Use **admin** for both of *User Name* and *Password*. Specify the region where you use the device. Available channels and maximum Transmit Power will be determined by the selected region according to the local laws and regulations. Select the appropriate language from the Language drop-down list. Read and agree the terms of use, then click *Login*.



5. Create a new username and password for network security. Click *Finish* to log in to the PharOS.



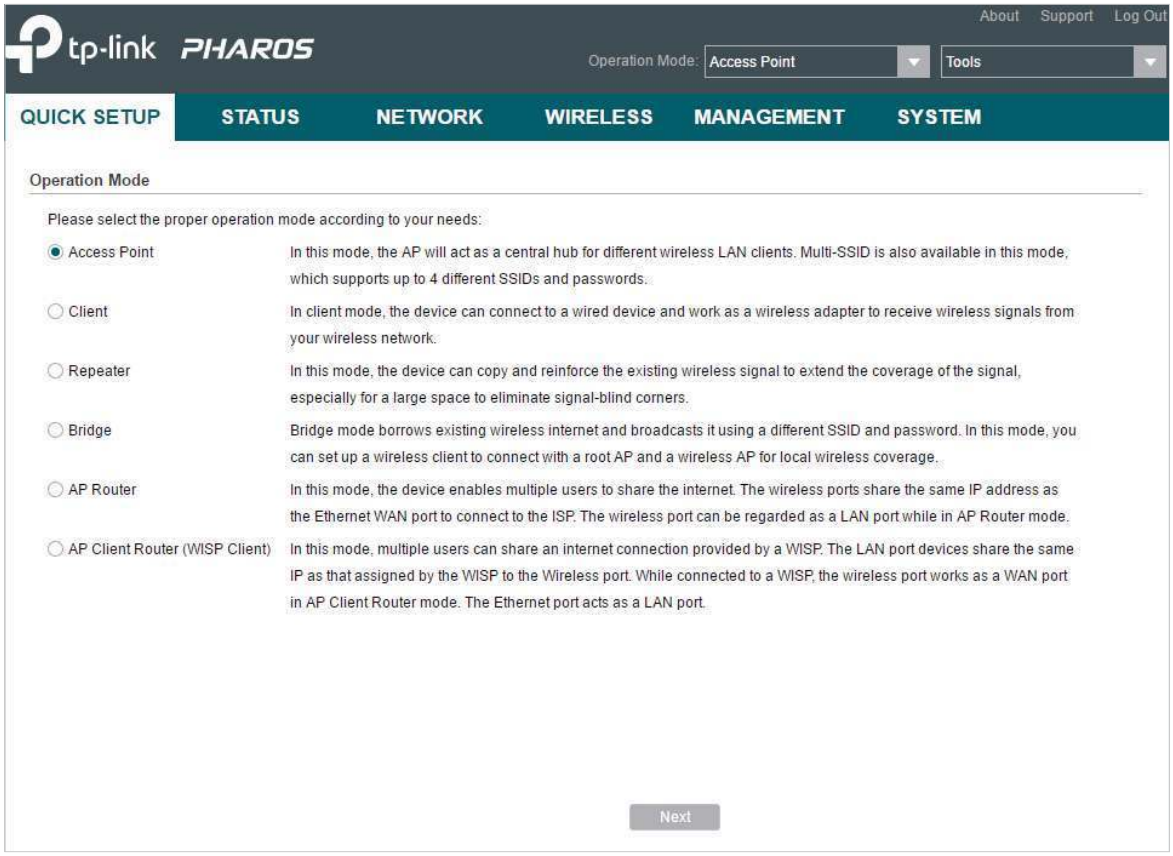
2.3 Set Up the Wireless Network

Use the Quick Setup wizard to quickly configure your device step by step. Choose the suitable operation mode according to your network environment and follow the step-by-step instructions.

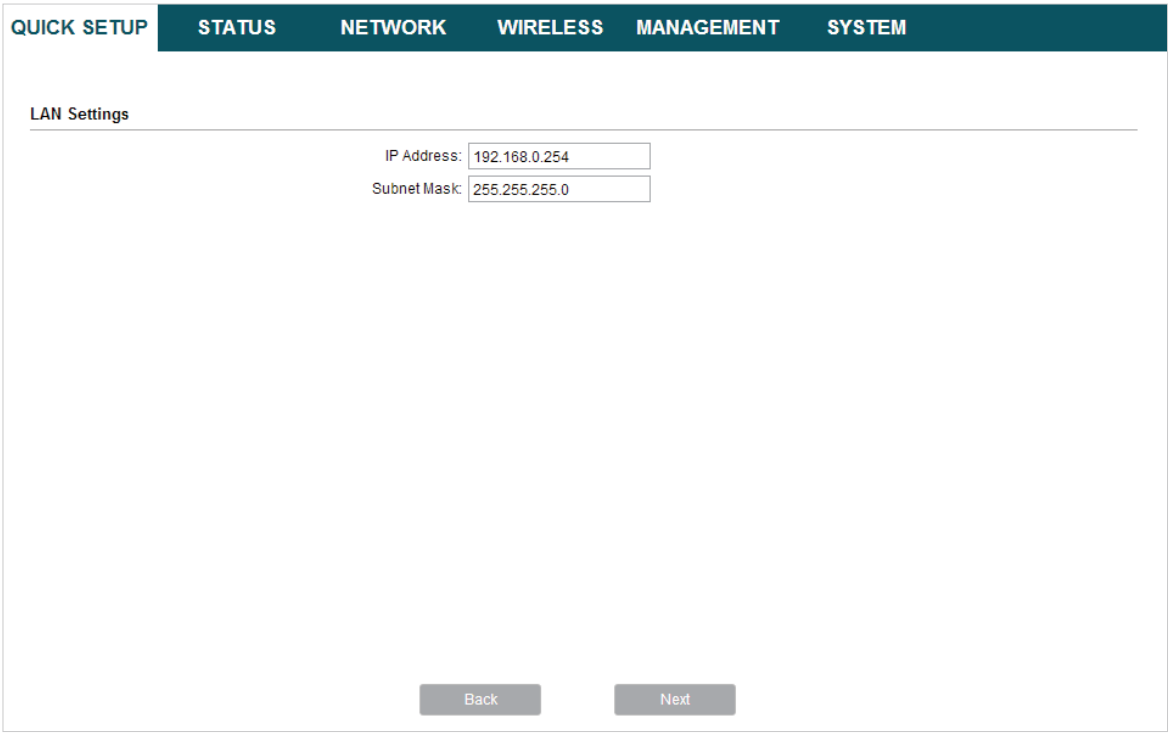
Access Point

Follow the steps below to configure the device as Access Point Mode:

1. Go to the **QUICK SETUP** page, select *Access Point* and click *Next*.



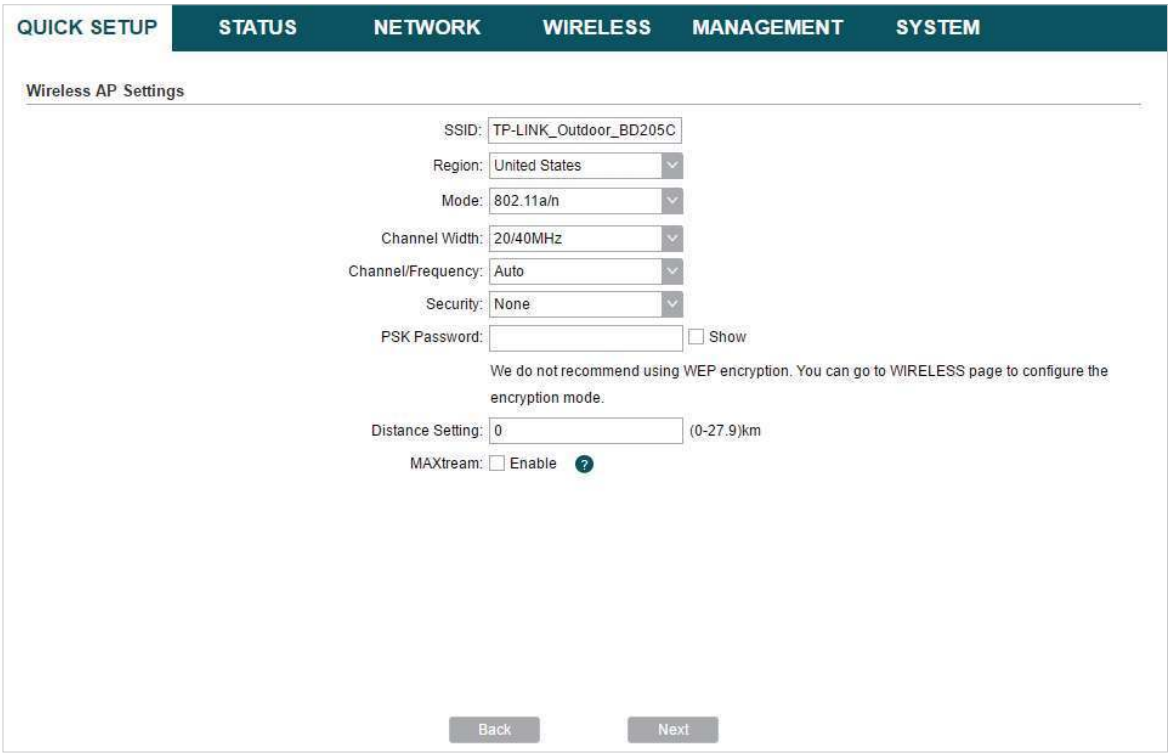
2. In the **LAN Settings** section, specify the LAN IP address and the Subnet Mask for the device. Then, click *Next*.



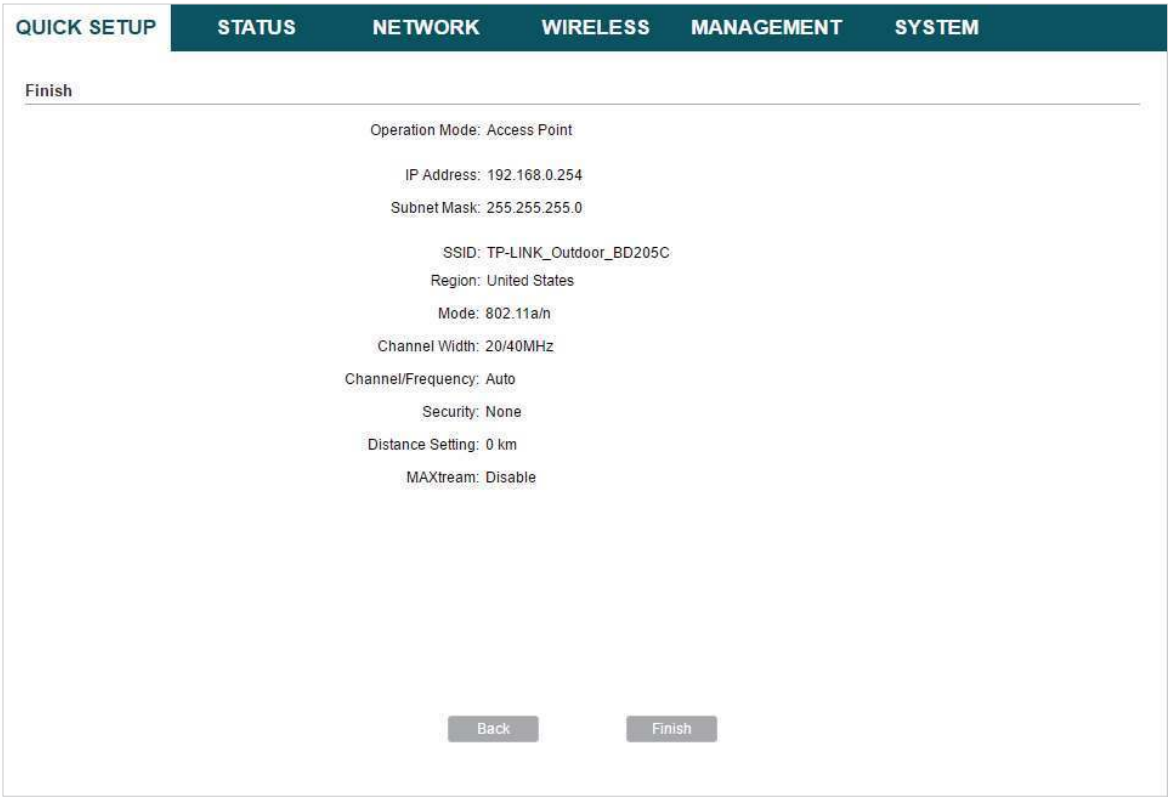
3. In the **Wireless AP Settings** section, specify the basic wireless parameters to create a wireless network. Click *Next*.

Note:

- It is recommended to specify *Security* as **WPA-PSK/WPA2-PSK** for the network security.
- You can keep the default settings or specify the parameters according to your need. For details, refer to *5. Configure the Wireless Parameters*.



4. In the **Finish** section, review the configurations and click *Finish* to complete the quick setup.

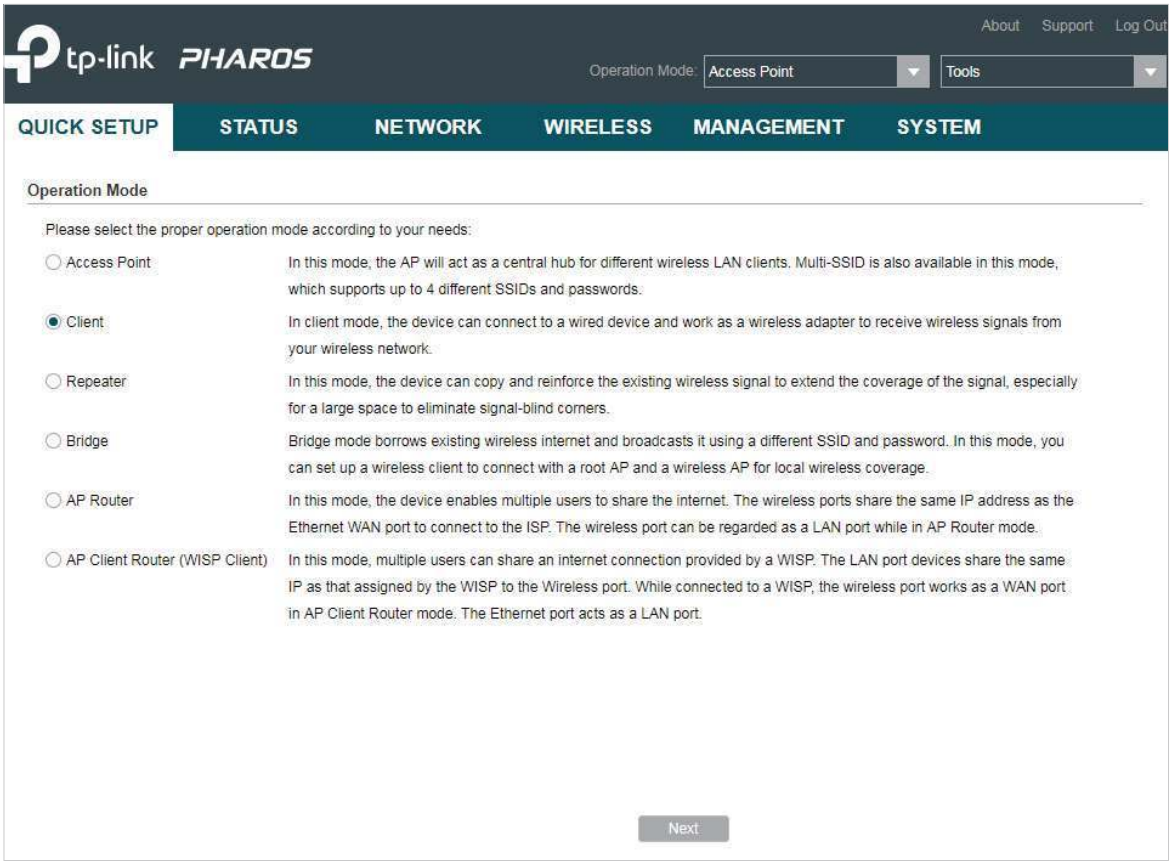


5. Connect the device according to your network topology and use it normally.

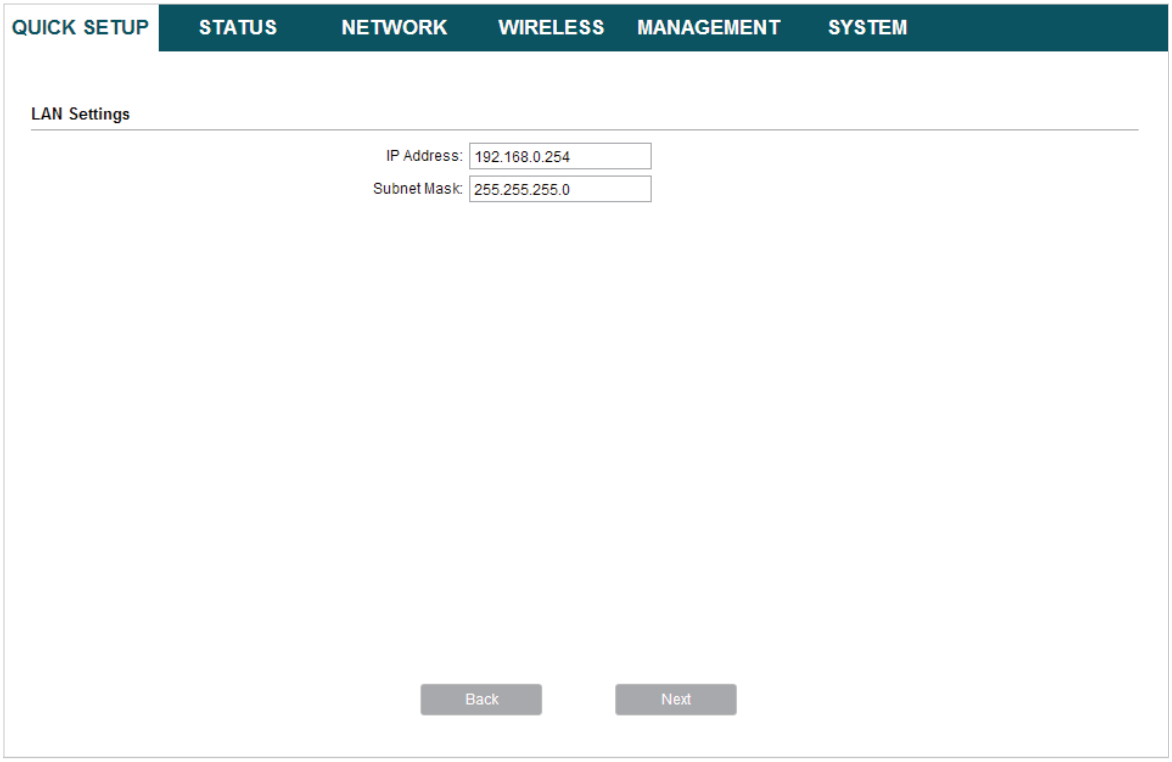
Client

Follow the steps below to configure the device as Client Mode:

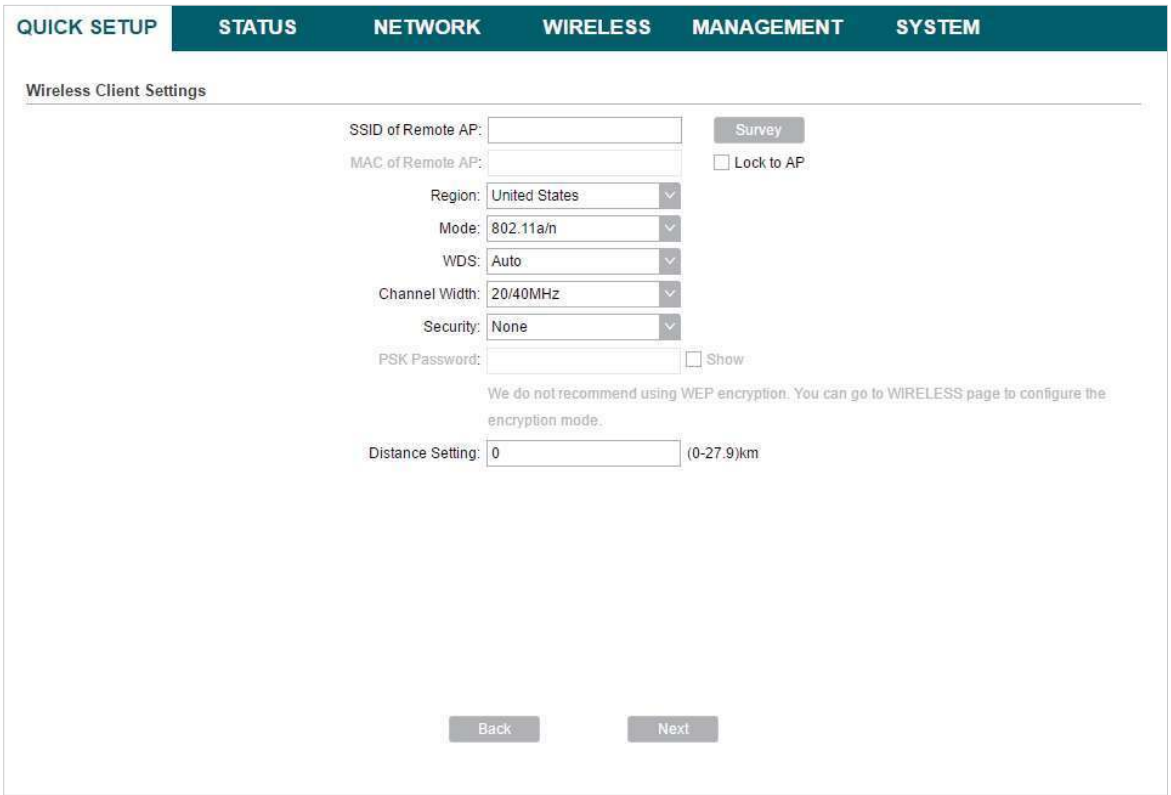
1. Go to the **QUICK SETUP** page, select *Client* and click *Next*.



2. In the **LAN Settings** section, specify the LAN IP Address and the Subnet Mask for the device. Then, click *Next*.



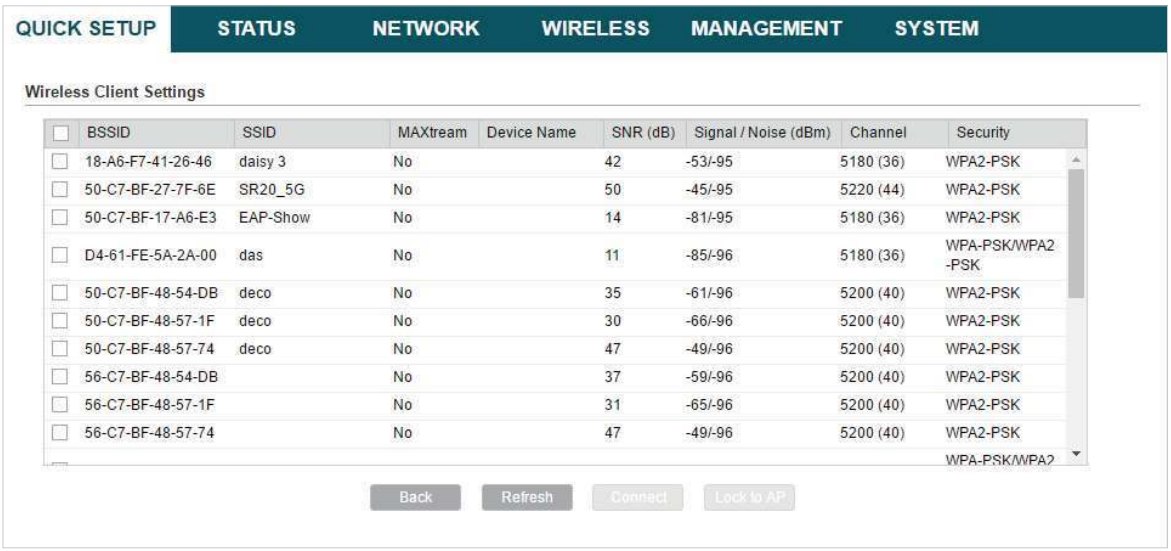
3. In the **Wireless Client Settings** section, click *Survey* to search for the upstream wireless network.



4. Select the desired wireless network and click *Connect*.

Note:

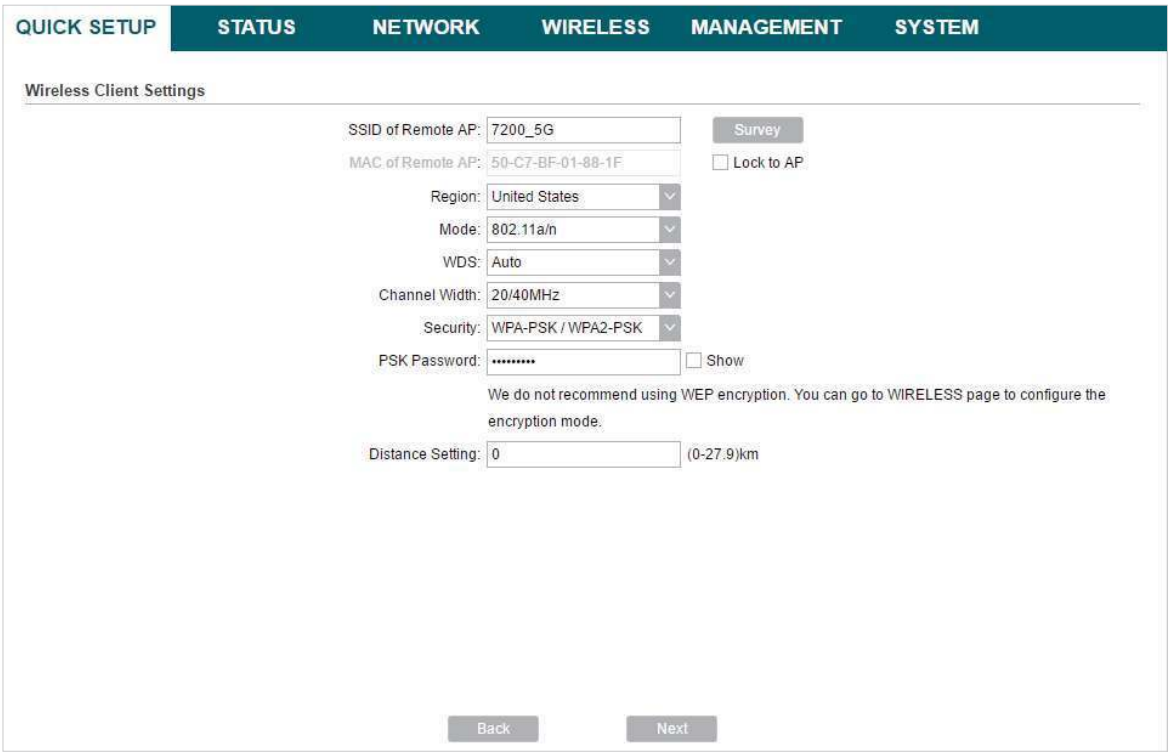
There may be two or more networks with the same SSID in the AP list. Click *Lock to AP* to select the SSID and AP simultaneously, which can make the device connect to the specific AP next time.



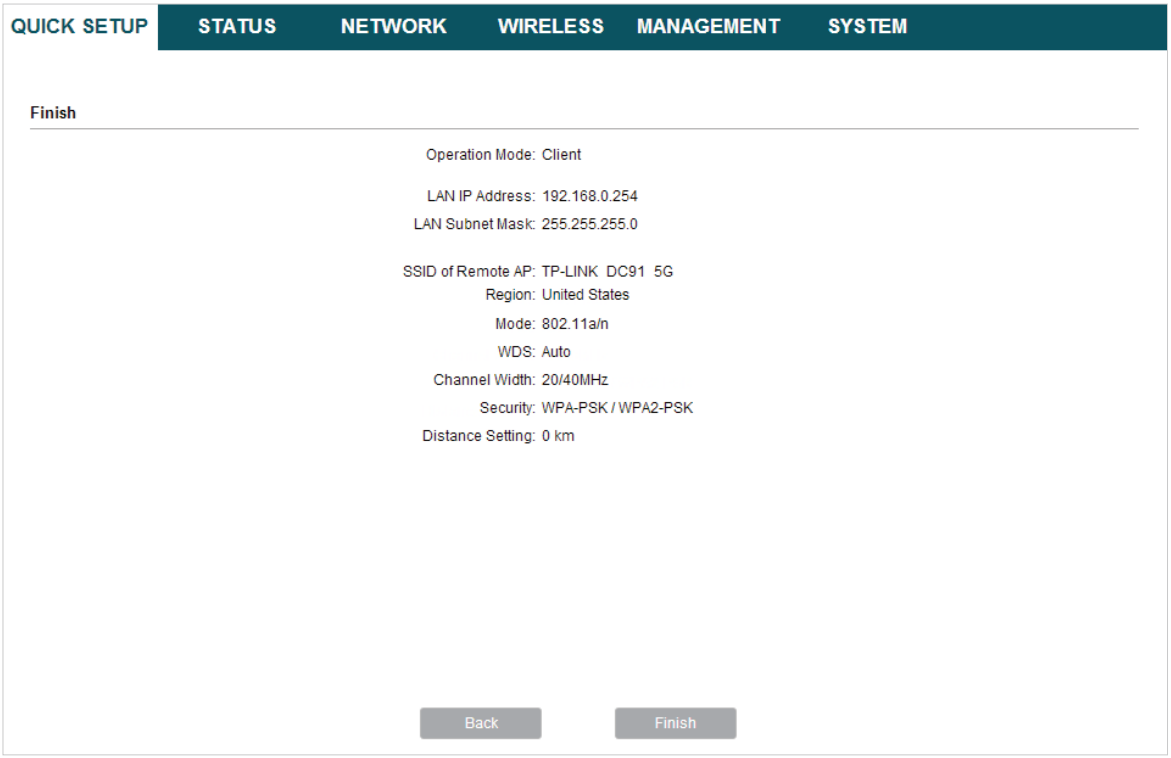
5. In the **Wireless Client Settings** section, specify the wireless parameters to connect to the specified wireless network. Click *Next*.

Note:

Make sure that *Security* and *PSK Password* are the same as the upstream wireless network's. Other parameters set in this page and those of the upstream wireless network should be compatible with each other. For details, refer to *5. Configure the Wireless Parameters*



6. In the **Finish** section, review the configurations and click *Finish* to complete the quick setup.



7. Connect the device according to your network topology and use it normally.

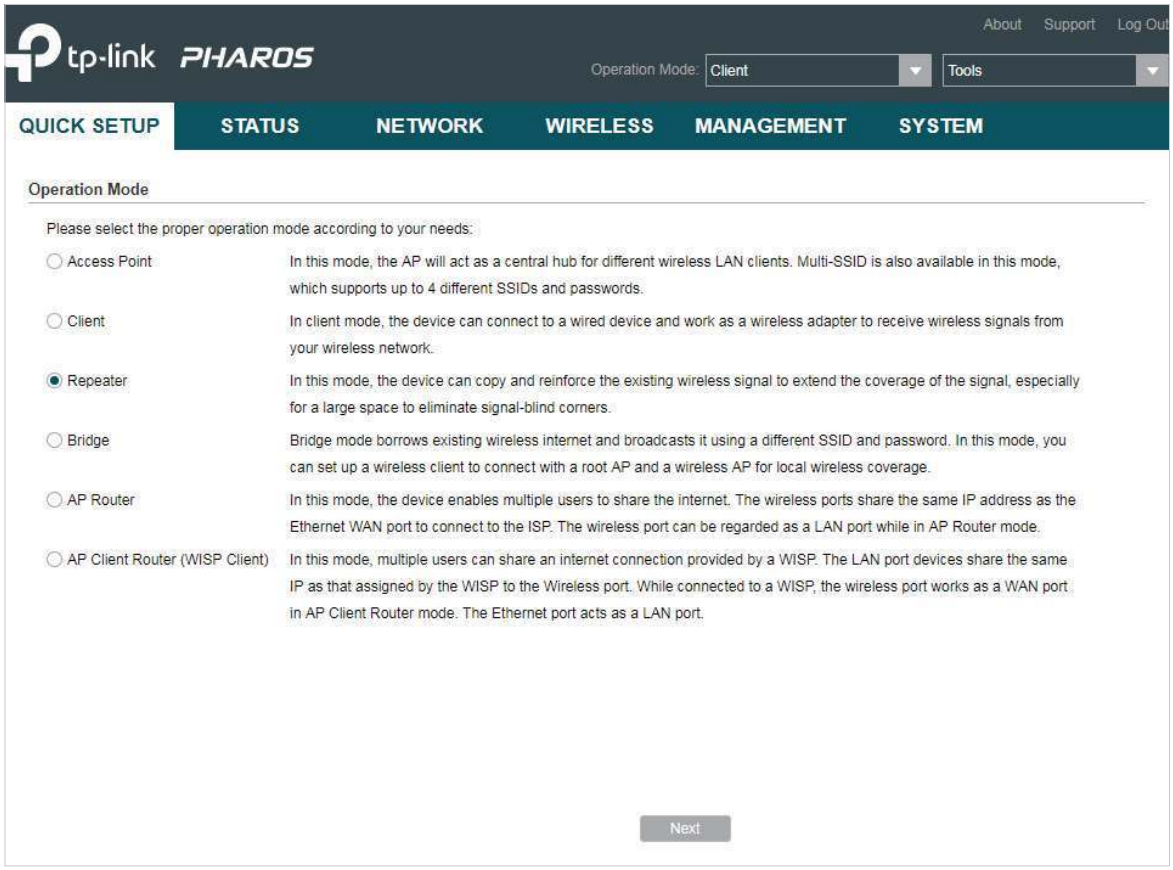
Repeater

Note:

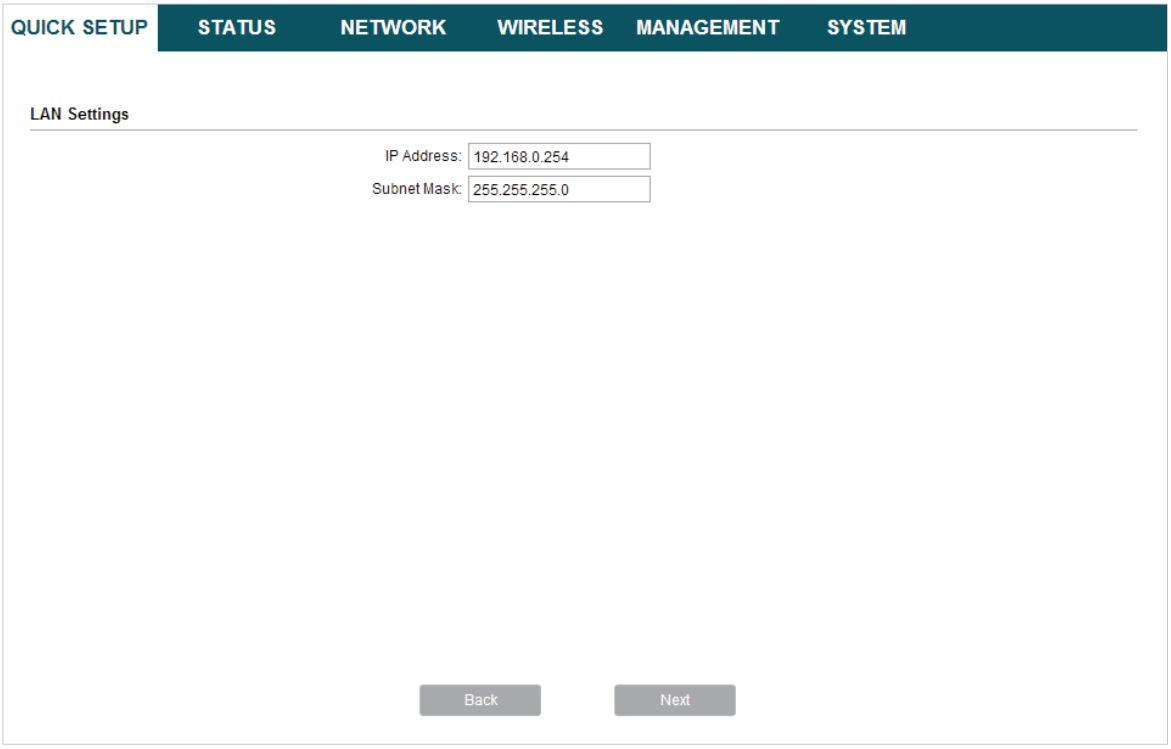
Repeater mode is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

Follow the steps below to configure the device as Repeater Mode:

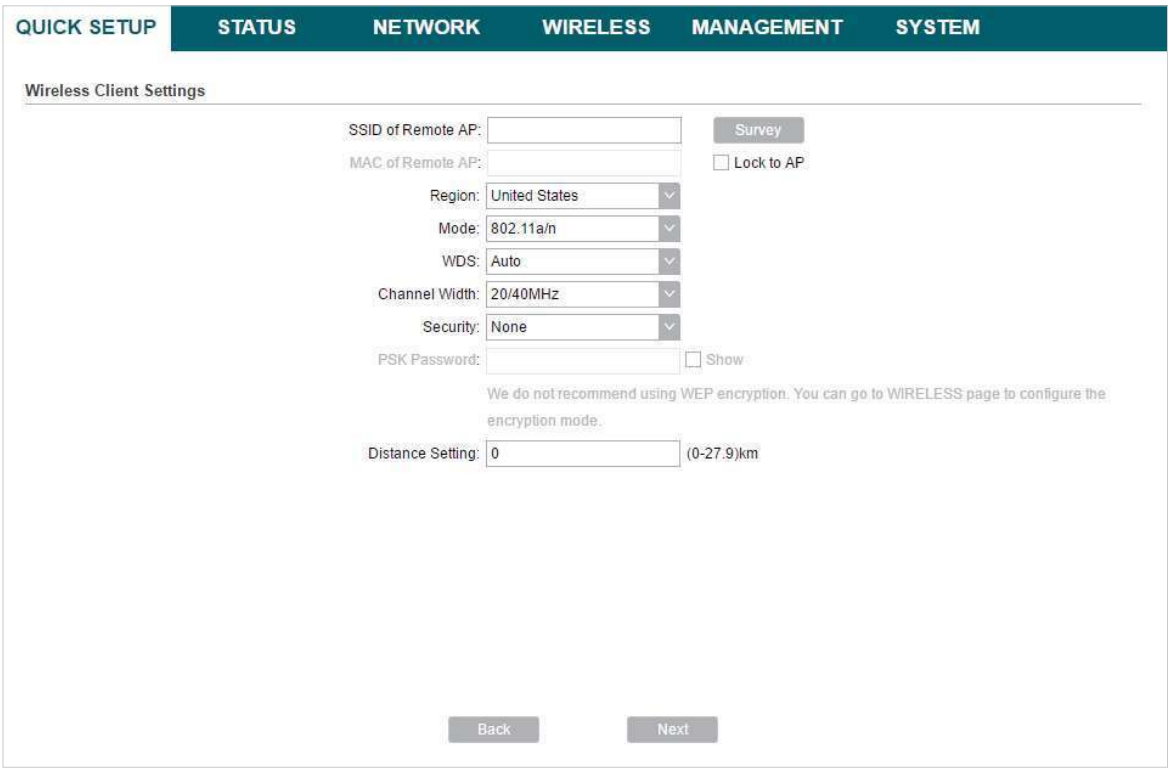
1. Go to the **QUICK SETUP** page, select *Repeater* and click *Next*.



2. In the **LAN Settings** section, specify the LAN IP address and the Subnet Mask for the device. Then, click *Next*.



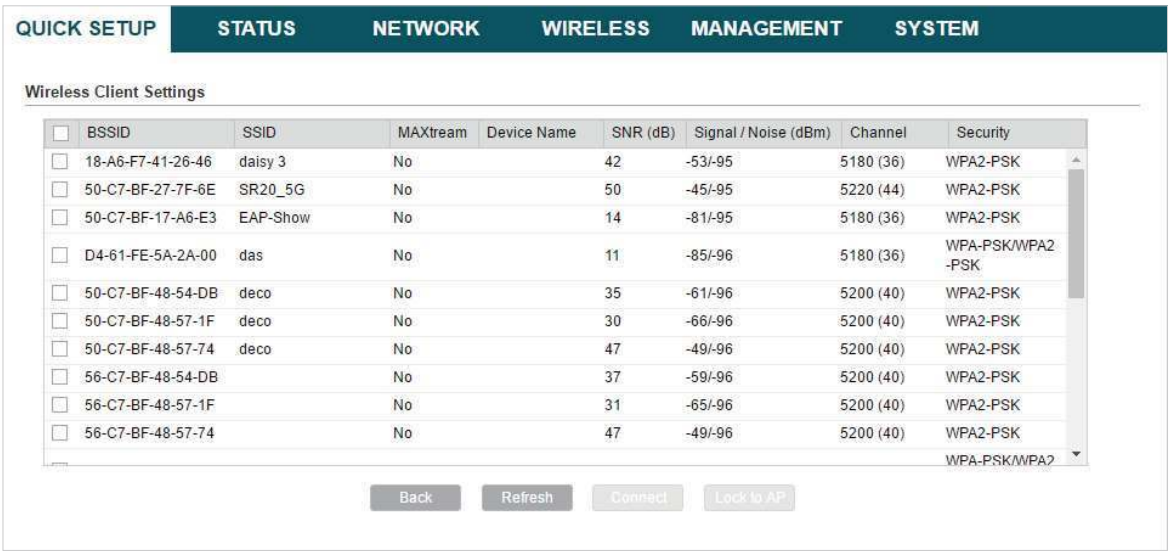
3. In the **Wireless Client Settings** section, click *Survey* to search for the upstream wireless network.



4. Select the desired wireless network and click *Connect*.

Note:

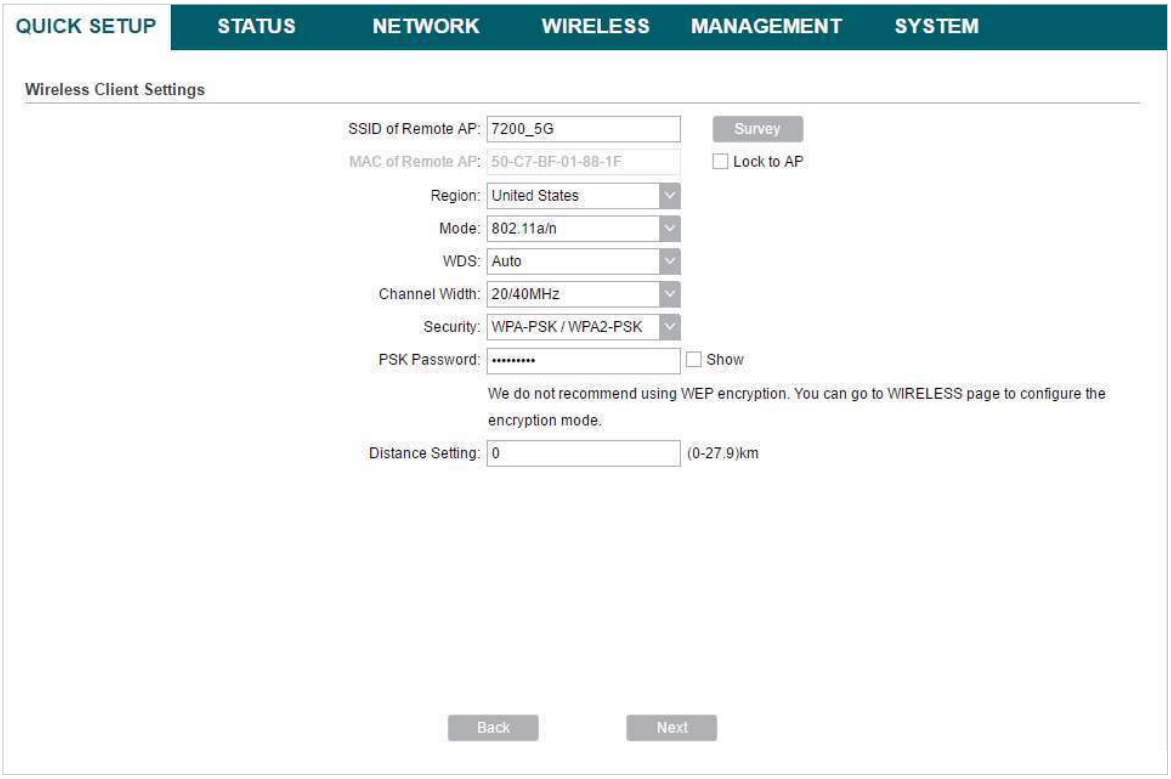
There may be two or more networks with the same SSID in the AP list. Click *Lock to AP* to select the SSID and AP simultaneously, which can make the device connect to the specific AP next time.



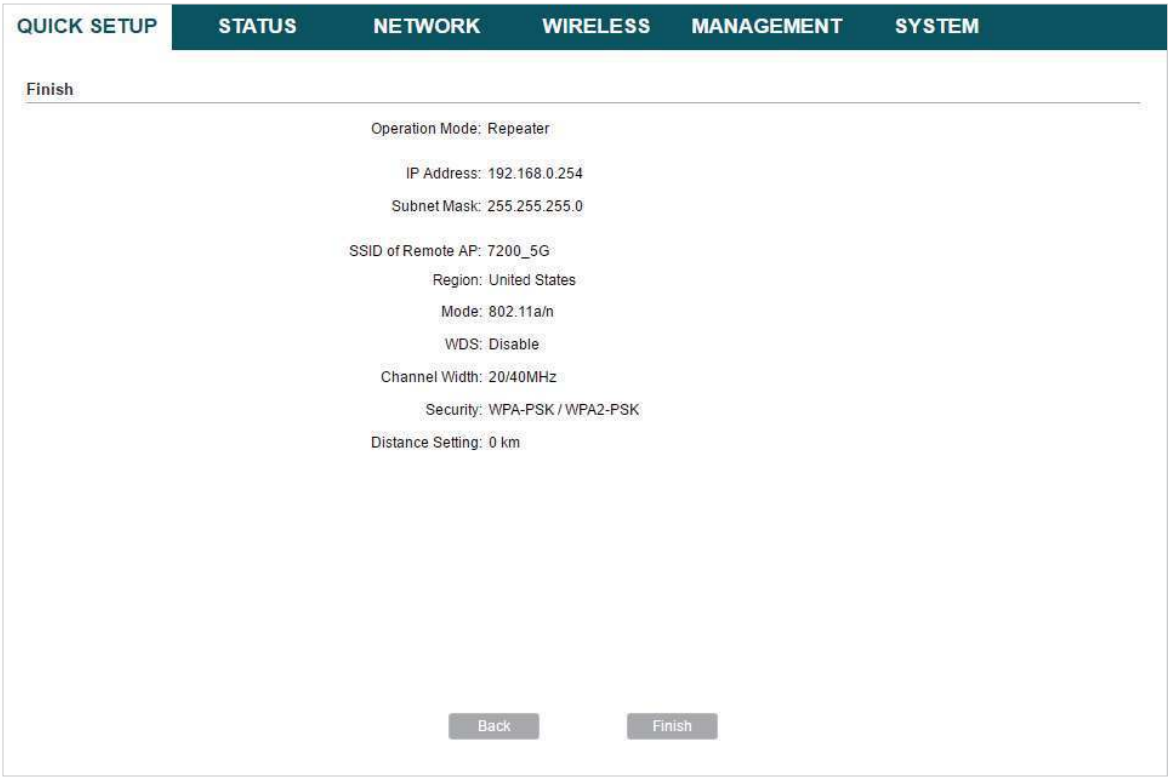
5. In the **Wireless Client Settings** section, specify the wireless parameters to connect to the specified wireless network. Click *Next*.

Note:

Make sure that *Security* and *PSK Password* are the same as the upstream wireless network's. Other parameters set in this page and those of the upstream wireless network should be compatible with each other. For details, refer to *5. Configure the Wireless Parameters*.



6. In the **Finish** section, review the configurations and click *Finish* to complete the quick setup.



7. Connect the device according to your network topology and use it normally.

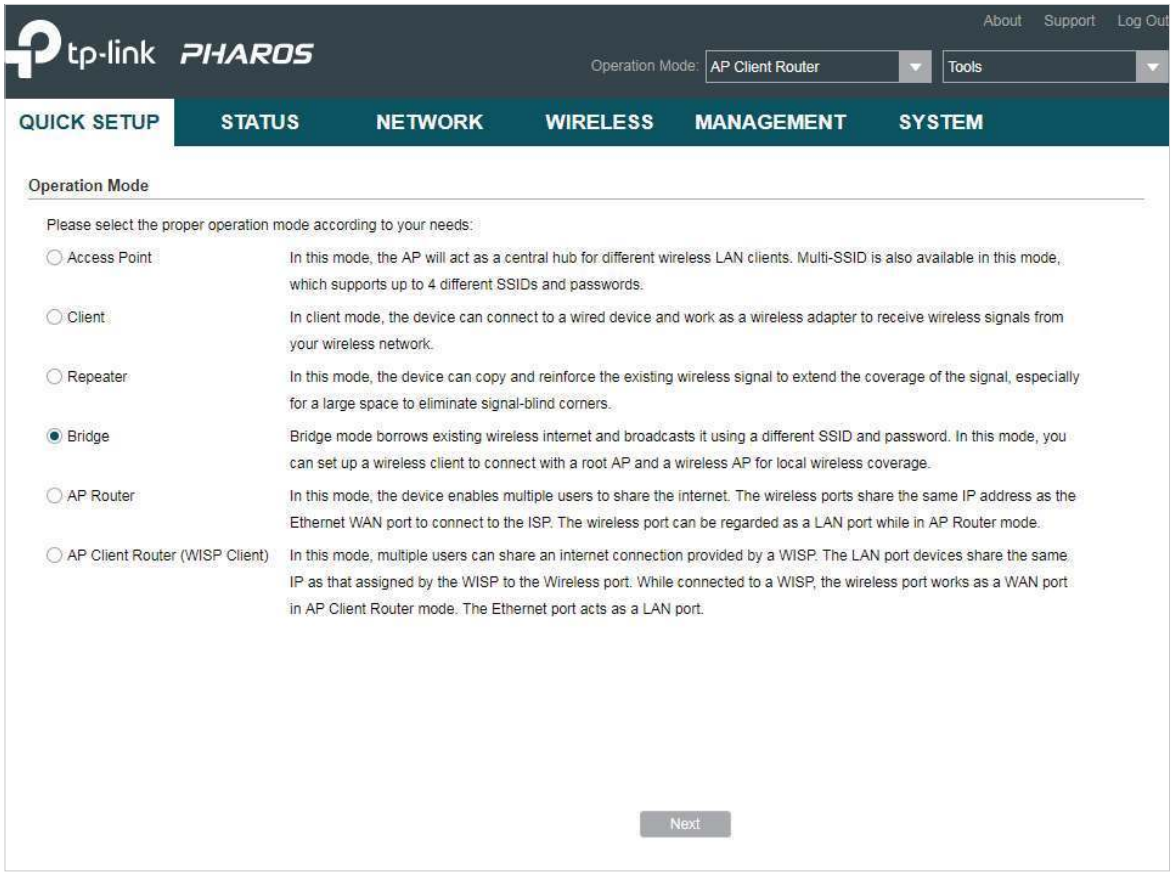
Bridge

Note:

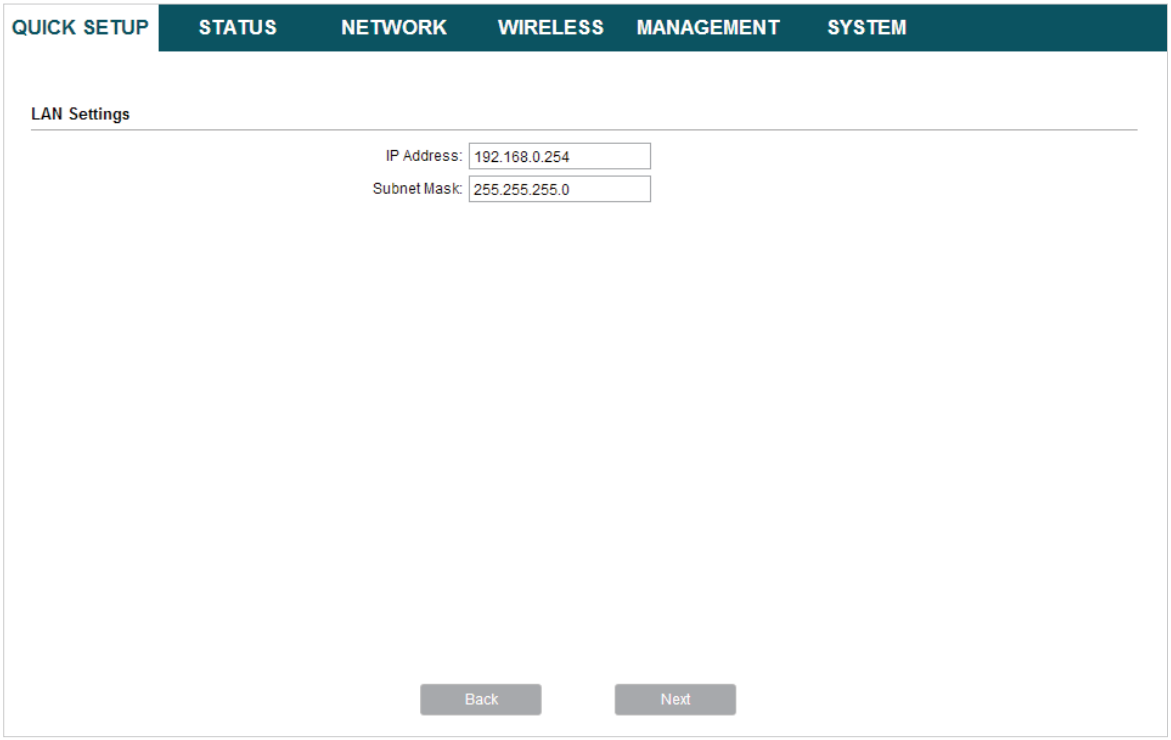
Bridge mode is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

Follow the steps below to configure the device as Bridge Mode:

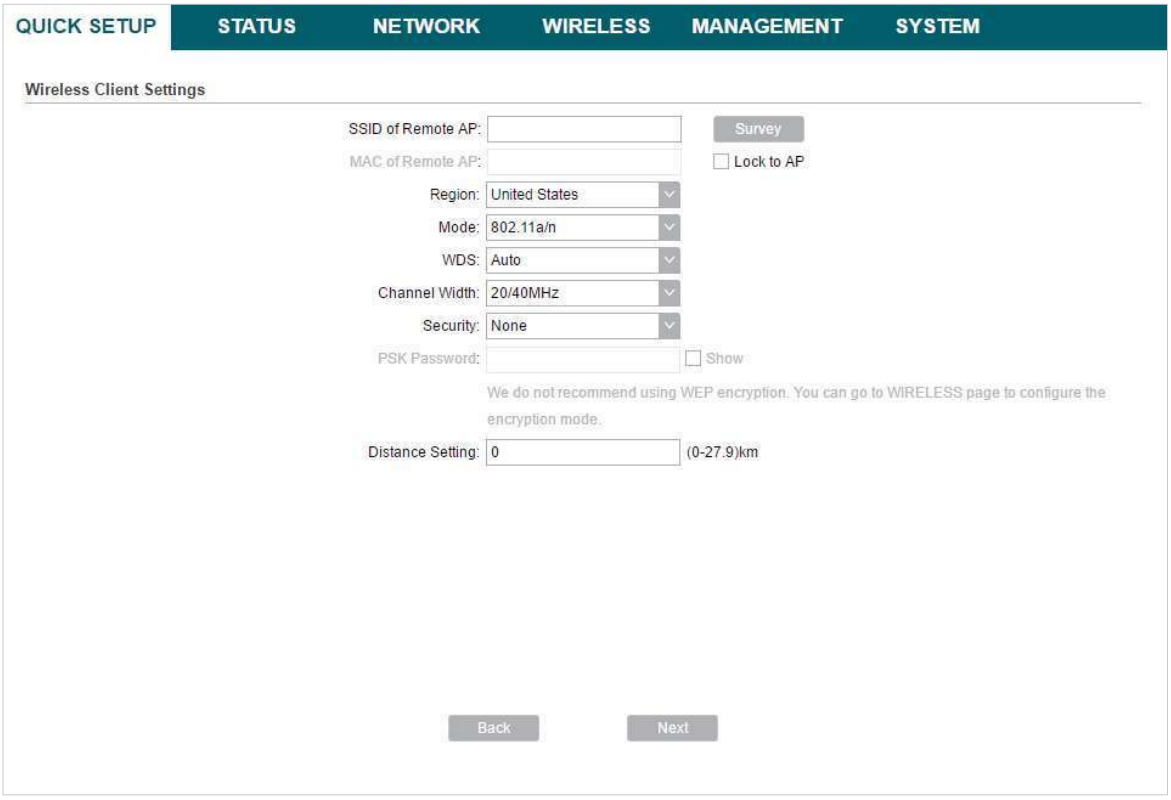
1. Go to the **QUICK SETUP** page, select *Bridge* and click *Next*.



2. In the **LAN Settings** section, specify the LAN IP address and the Subnet Mask for the device. Then, click *Next*.



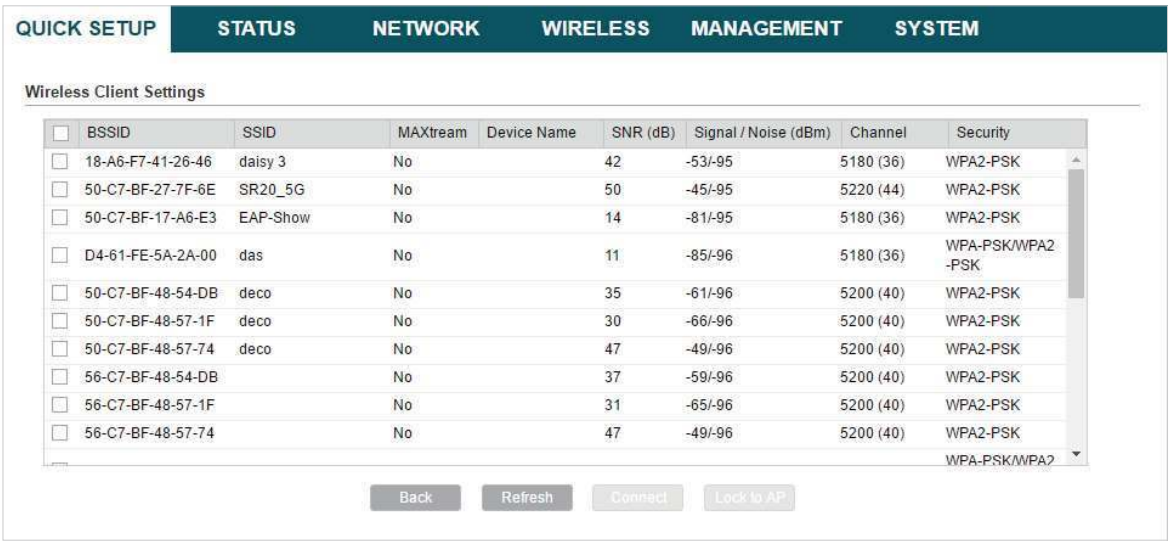
3. In the **Wireless Client Settings** section, click *Survey* to search for the upstream wireless network.



4. Select the desired wireless network and click *Connect*.

Note:

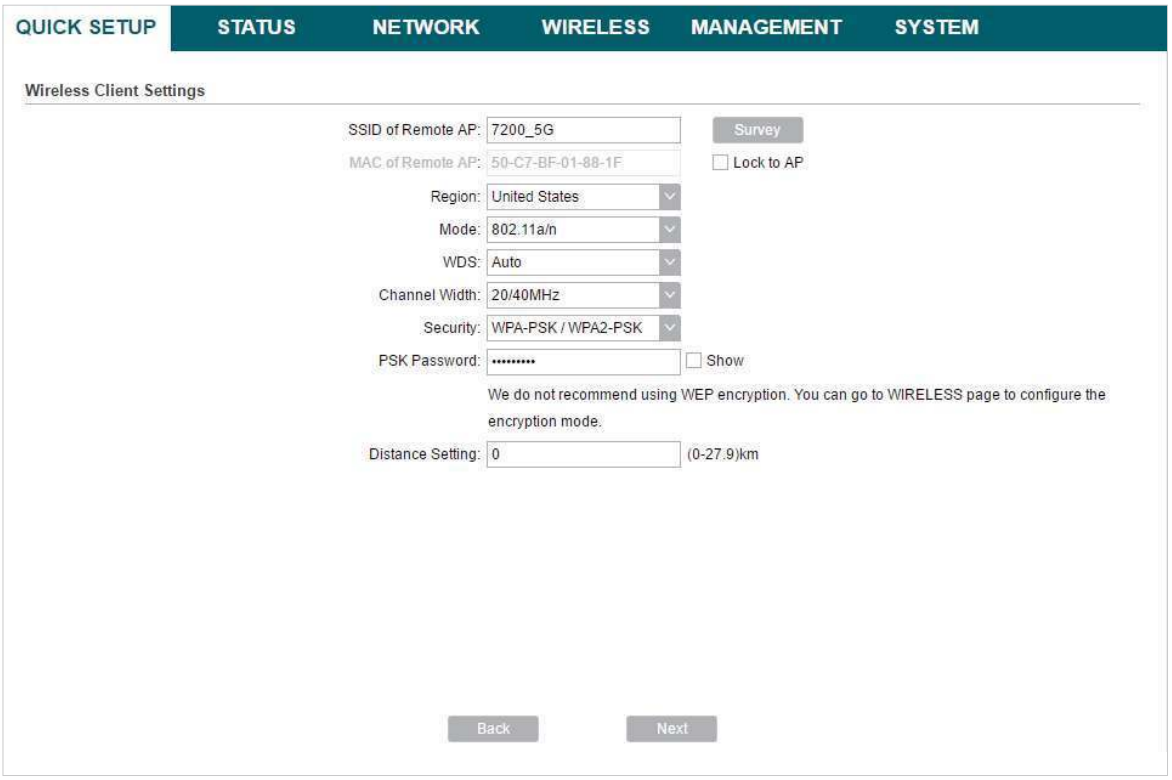
There may be two or more networks with the same SSID in the AP list. Click *Lock to AP* to select the SSID and AP simultaneously, which can make the device connect to the specific AP next time.



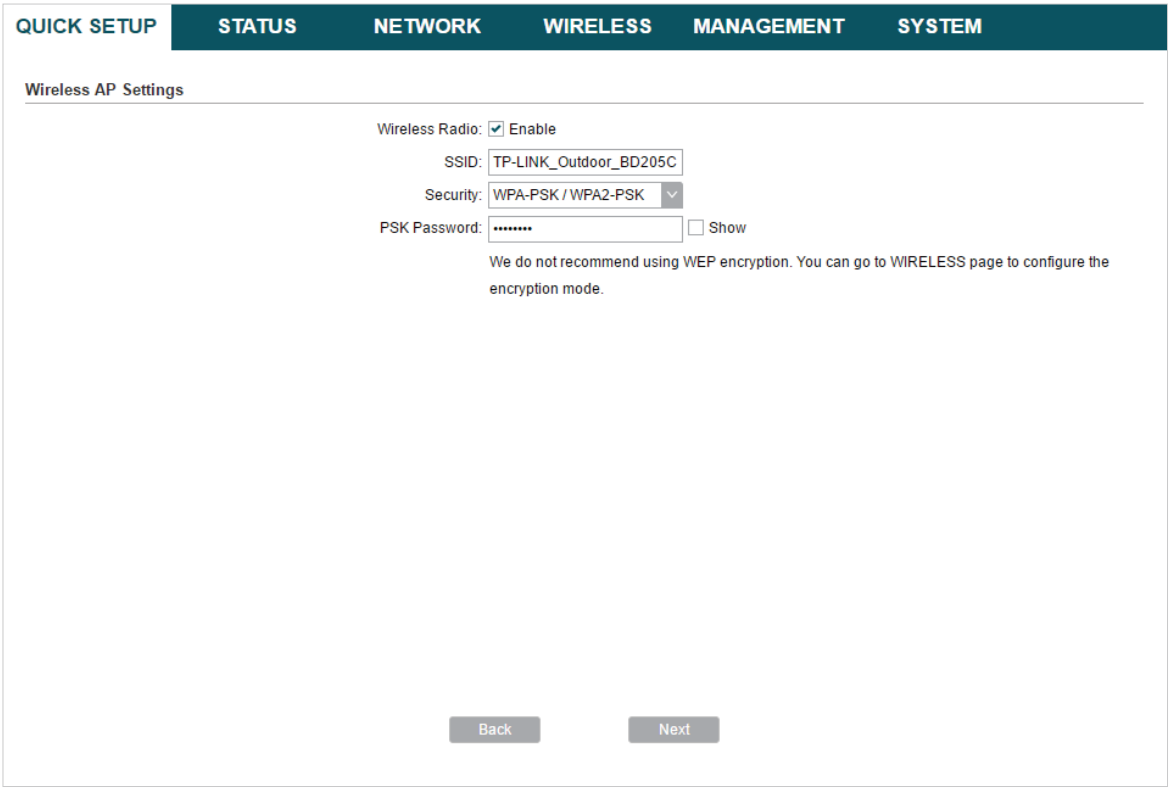
5. In the **Wireless Client Settings** section, specify the wireless parameters to connect to the specified wireless network. Click *Next*.

Note:

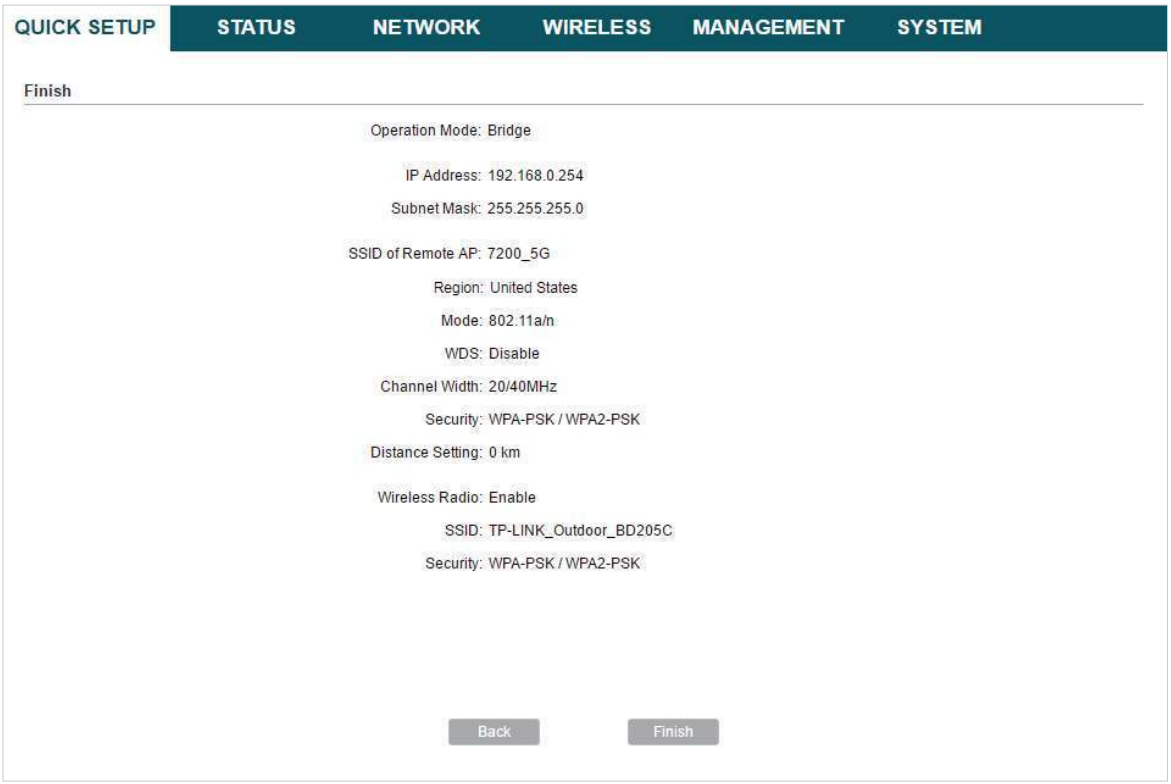
Make sure that the *Security* and *PSK Password* are the same as the upstream wireless network's. Other parameters set in this page and those of the upstream wireless network should be compatible with each other. For details, refer to *5. Configure the Wireless Parameters*.



6. In the **Wireless AP Settings** section, specify the parameters to create a new wireless network for the downstream clients. Click *Next*.



7. In the **Finish** section, review the configurations and click *Finish* to complete the quick setup.

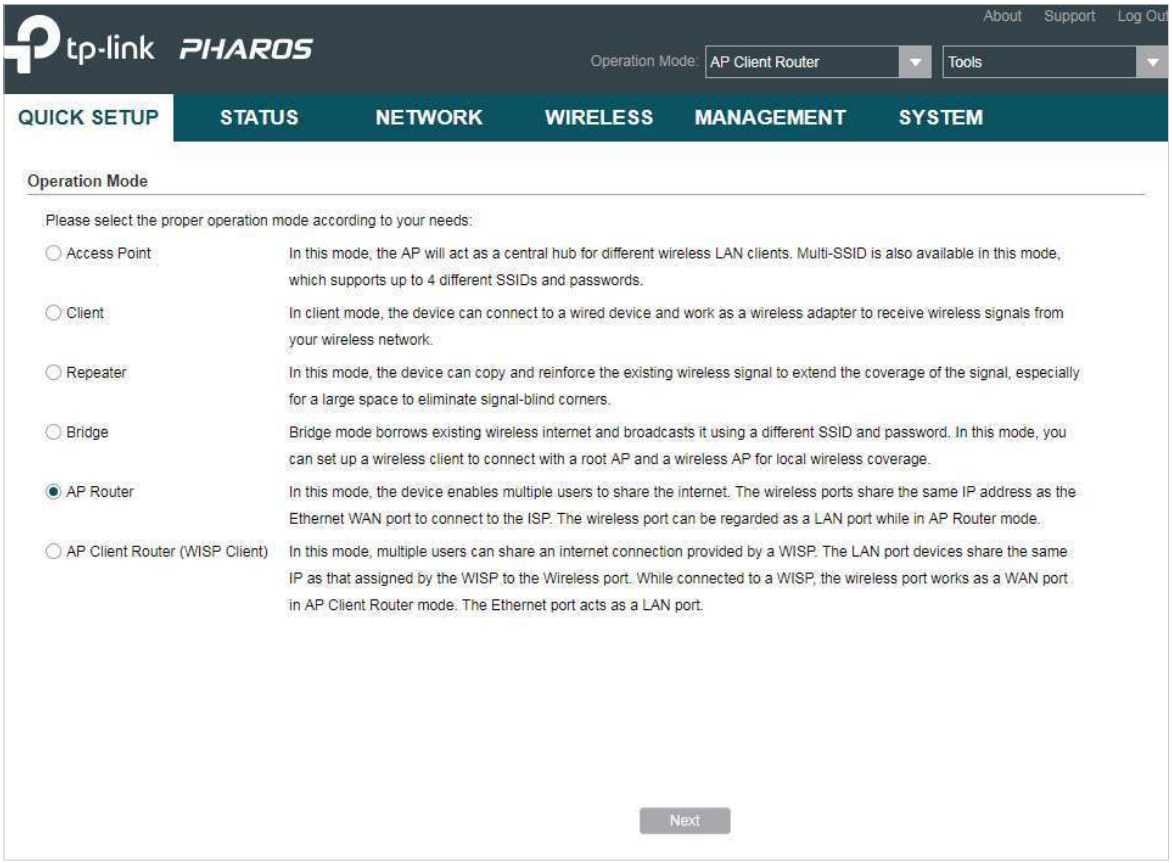


8. Connect the device according to your network topology and use it normally.

AP Router

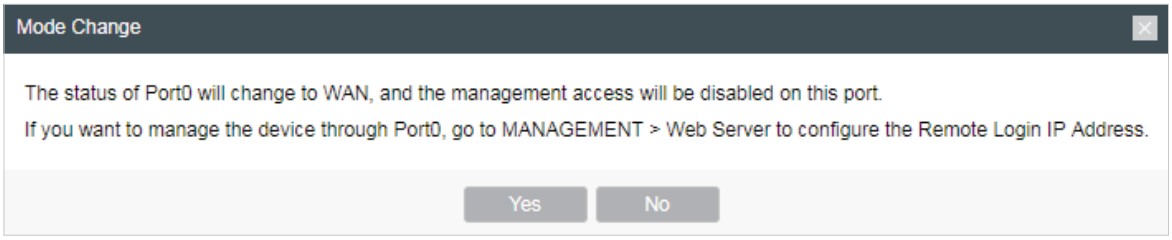
Follow the steps below to configure the device as AP Router Mode:

1. Go to the **QUICK SETUP** page, select *AP Router* and click *Next*.



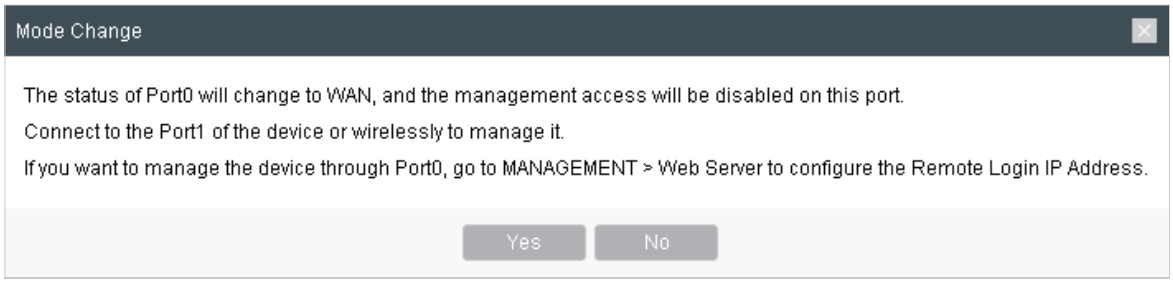
The following window will pop up. Click Yes.

- For devices with one Ethernet port.



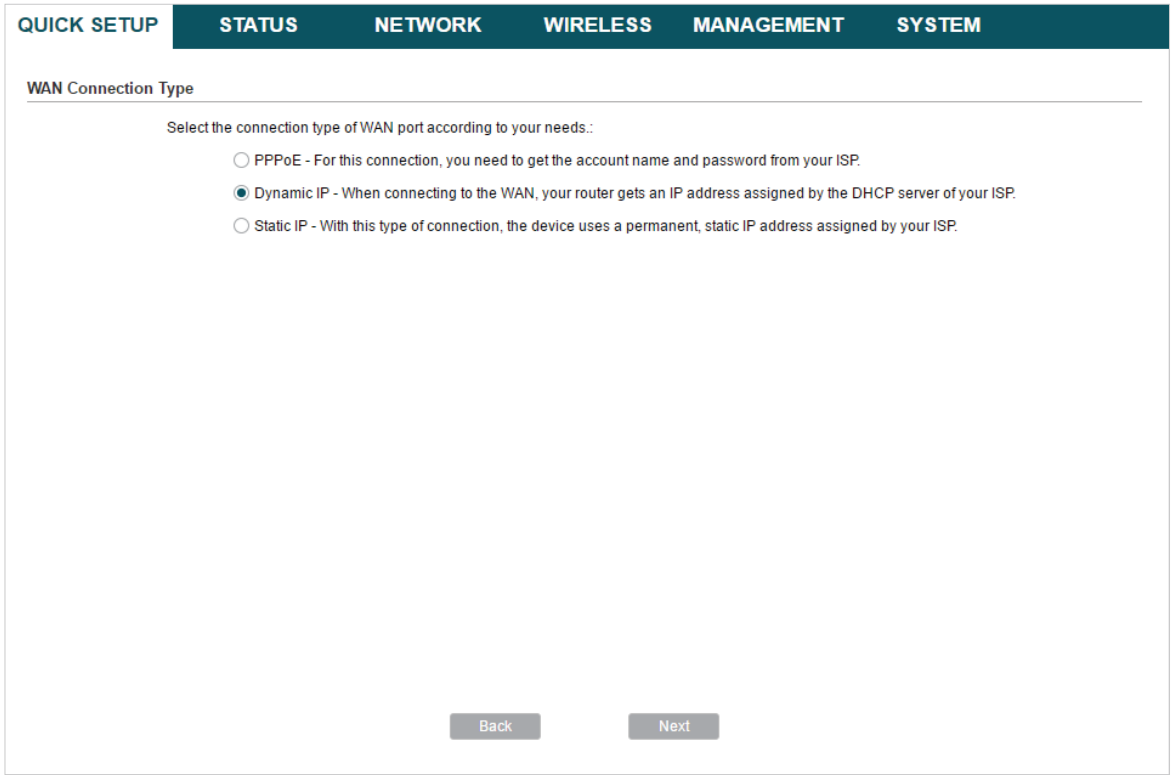
Note that if you select AP Router as the operation mode, the status of Port0 will change to WAN, and the management access will be disabled on this port after the process of quick setup. If you want to manage the device through Port0, configure the Remote Login IP Address. For details, refer to *6.5. Configure Web Server*.

- For devices with two Ethernet ports.



Note that if you select AP Router as the operation mode, the status of Port0 will change to WAN, and the management access will be disabled on this port after the process of quick setup. You can connect to the Port1 of the device or wirelessly to manage it. If your want to manage the device through Port0, configure the Remote Login IP Address. For details, refer to *6.5. Configure Web Server*.

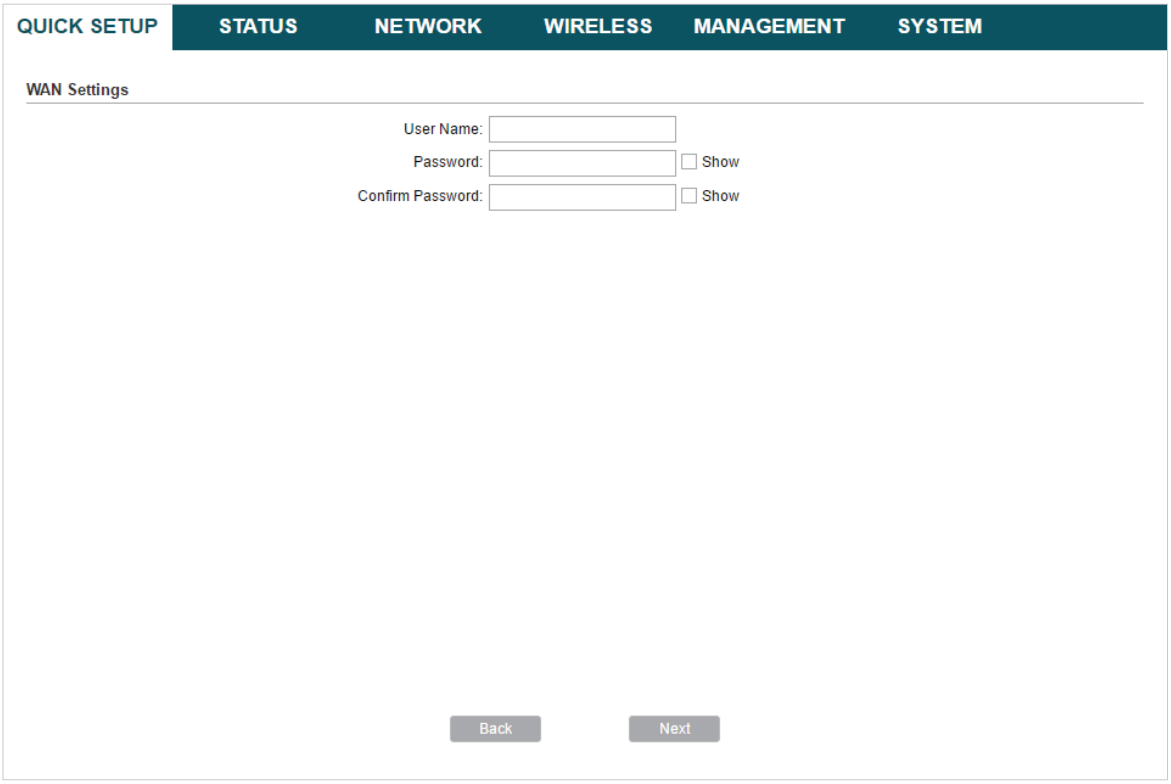
2. In the **WAN Connection Type** section, specify the connection type according to your need and click *Next*.



The device supports three types of the WAN connection, including *PPPoE*, *Dynamic IP* and *Static IP*. Contact your ISP to confirm your WAN connection type.

■ PPPoE

Select *PPPoE* and click *Next*, then the following page will appear. In the **WAN Settings** section, specify the parameters that are provided by your ISP and click *Next*.

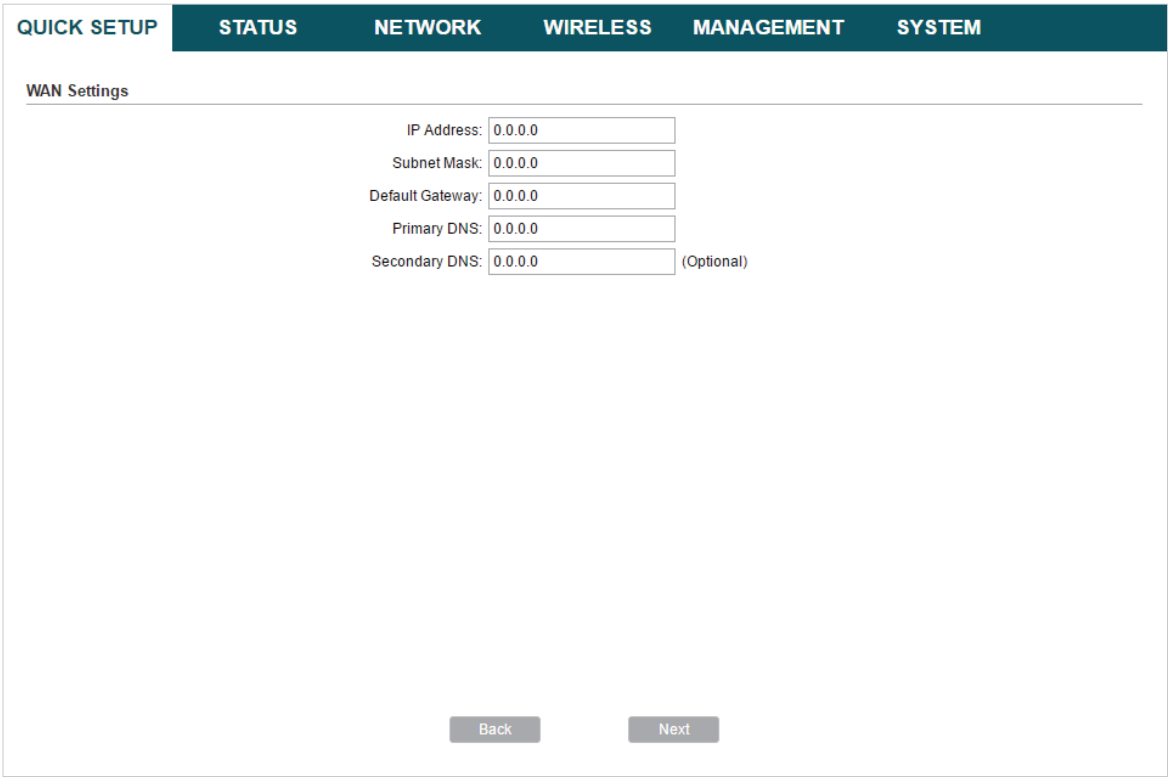


■ Dynamic IP

Select *Dynamic IP* and click *Next*. In this type, the device will obtain a WAN connection automatically without any WAN configurations.

■ Static IP

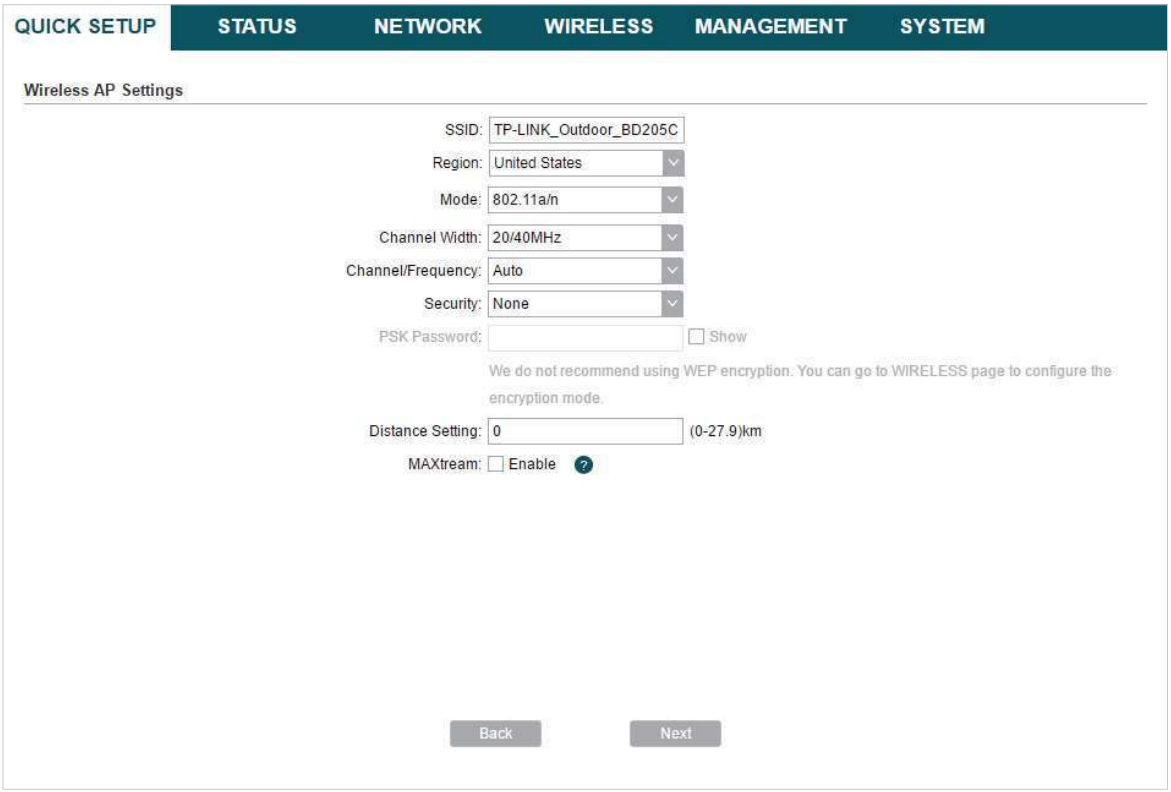
Select *Static IP* and click *Next*, then the following page will appear. In the **WAN Settings** section, specify the parameters that are provided by your ISP and click *Next*.



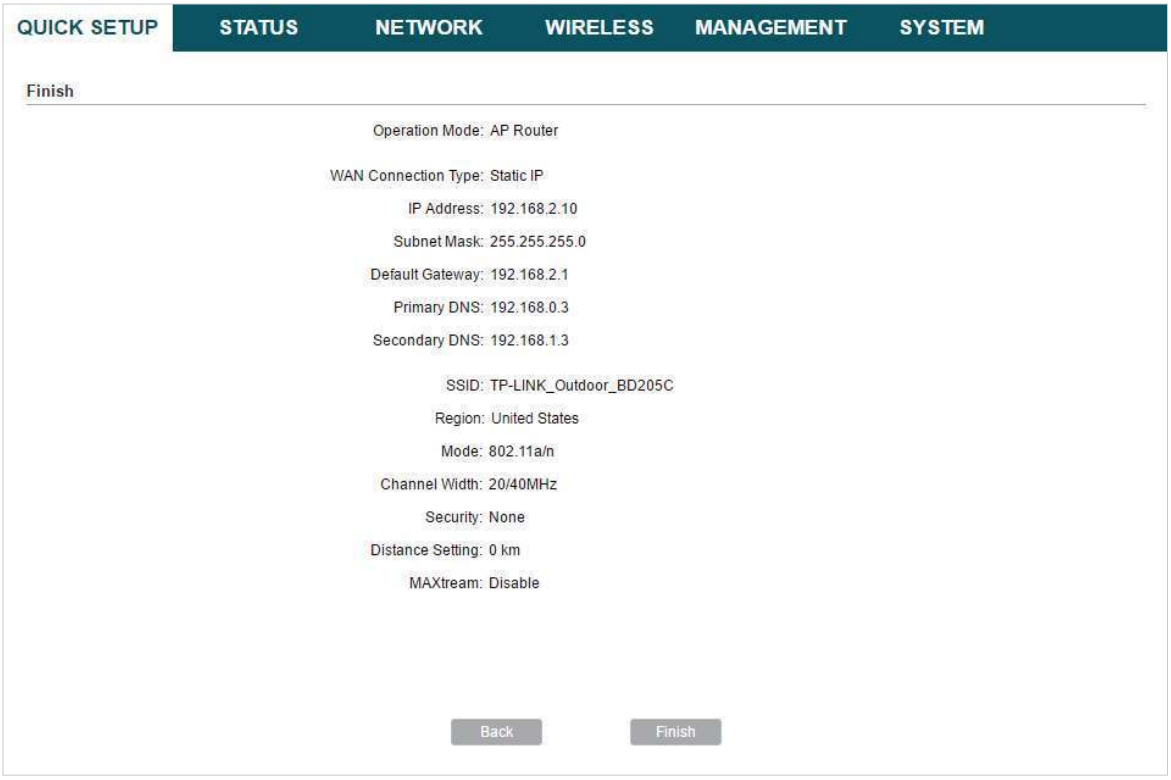
3. In the **Wireless AP Settings** section, specify the basic wireless parameters to create a wireless network. Click *Next*.

Note:

- It is recommended to specify *Security* as **WPA-PSK/WPA2-PSK** for the network security.
- You can keep the default settings or specify the parameters according to your need. For details, refer to *5. Configure the Wireless Parameters*.



4. In the **Finish** section, review the configurations and click *Finish* to complete the quick setup.

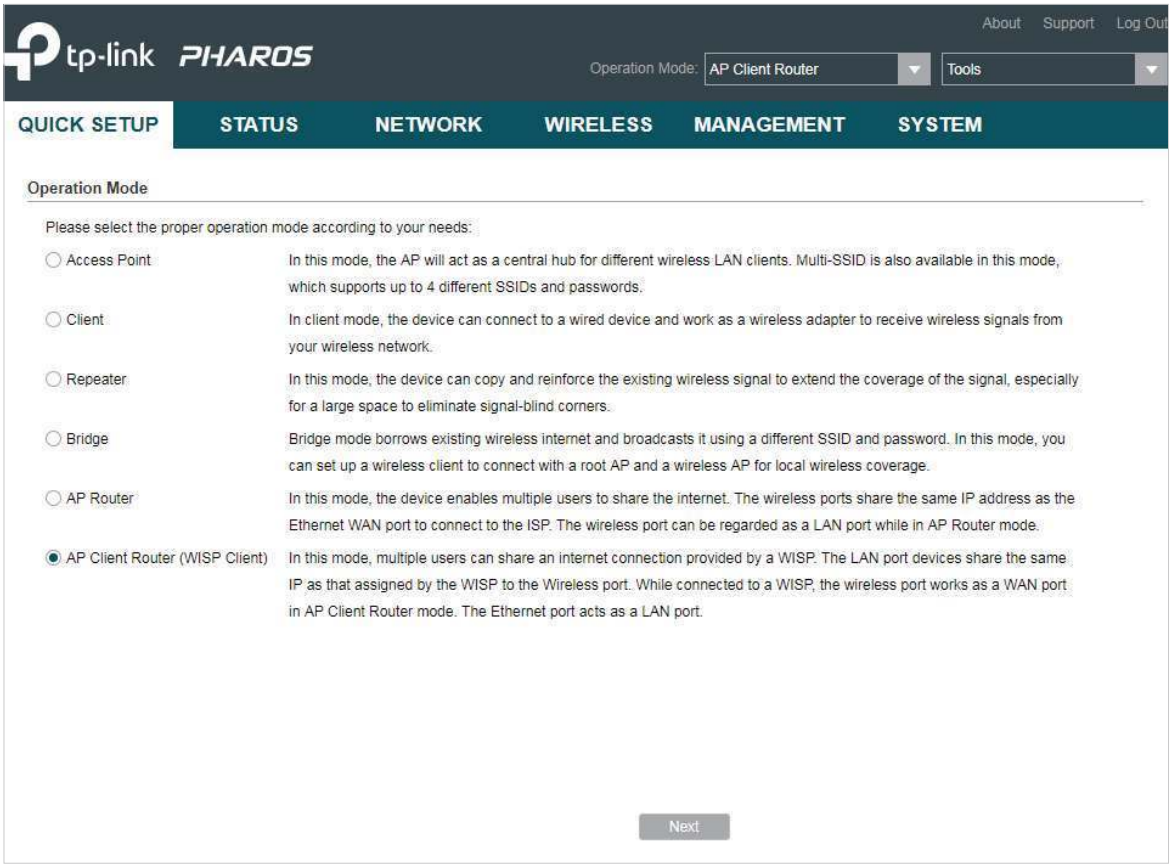


5. Connect the device according to your network topology and use it normally.

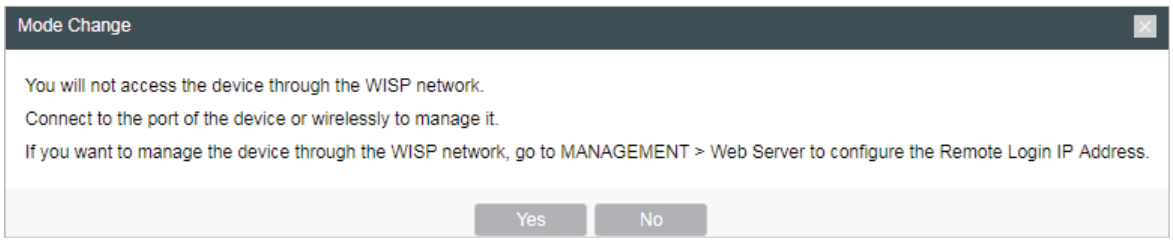
AP Client Router (WISP Client)

Follow the steps below to configure the device as AP Client Router (WISP Client) Mode:

1. Go to the **QUICK SETUP** page, select *AP Client Router (WISP Client)* and click *Next*.

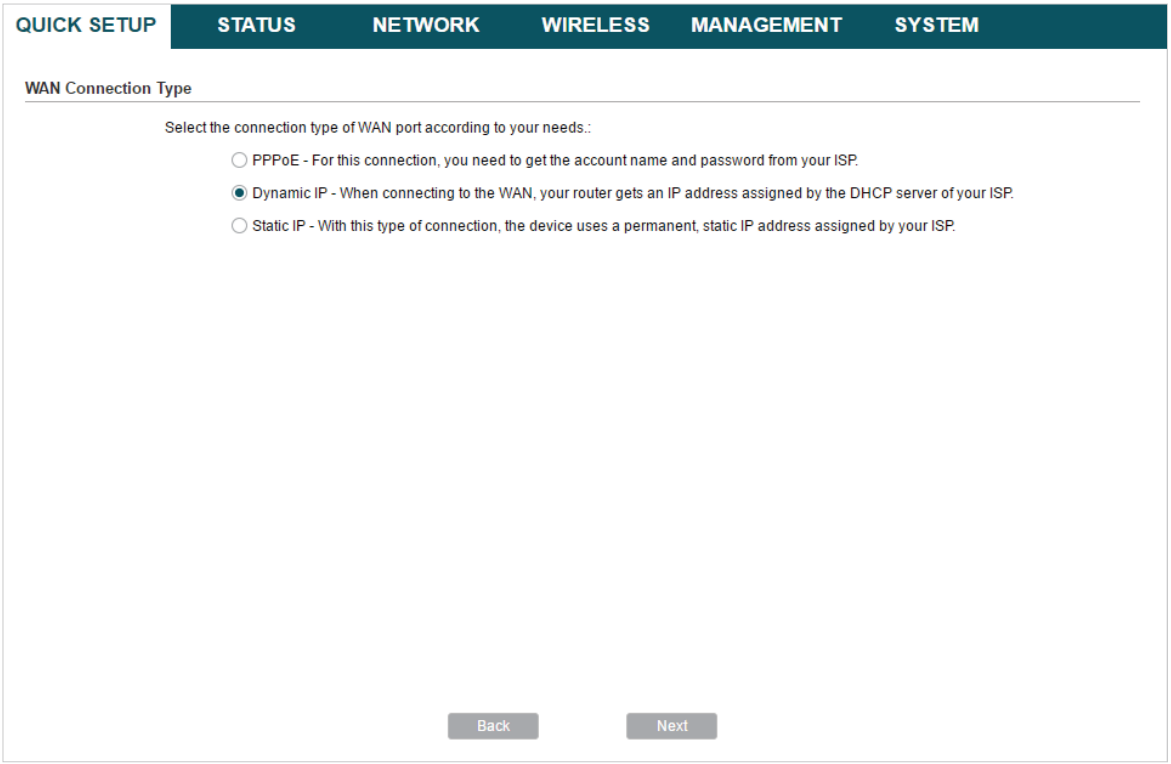


The following window will pop up. Click *Yes*.



Note that if you select AP Client Router (WISP Client) as the operation mode, you will not access the device through the WISP network after the process of quick setup. You can connect to the port of the device or wirelessly to manage it. If you want to manage the device through the WISP network, configure the Remote Login IP Address. For details, refer to *6.5. Configure Web Server*.

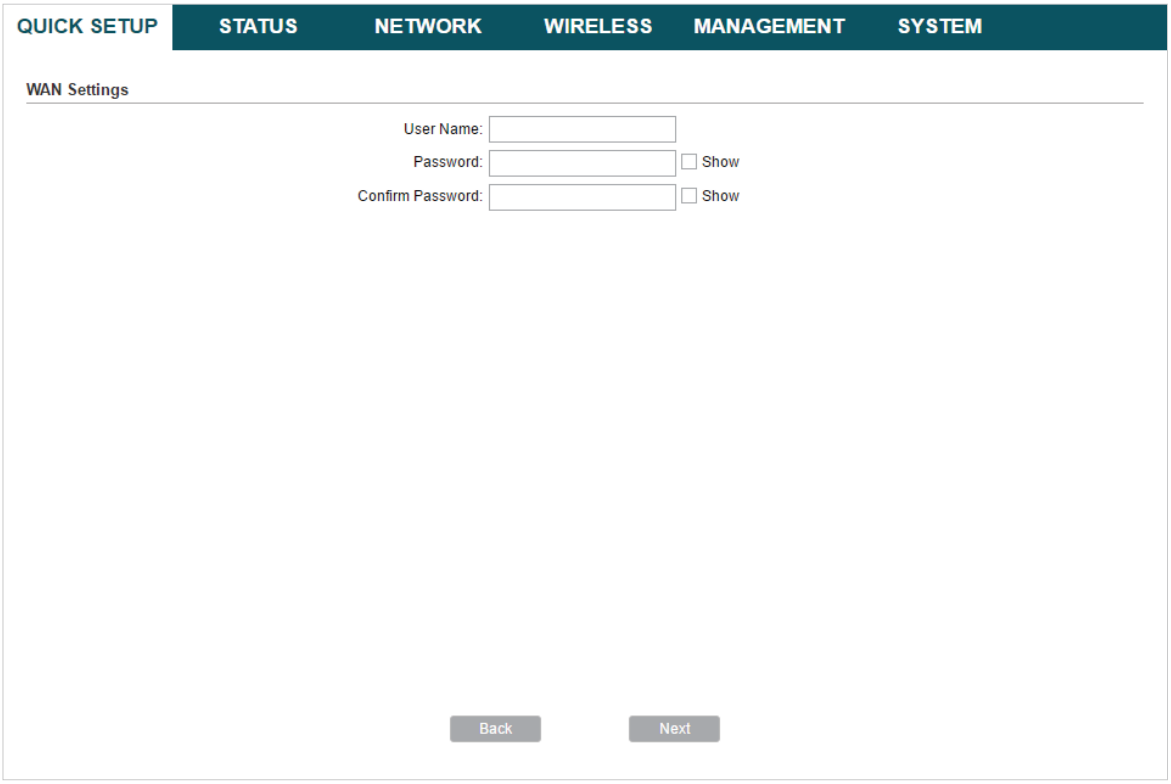
2. In the **WAN Connection Type** section, choose the connection type according to your need and click *Next*.



The device supports *PPPoE*, *Dynamic IP* and *Static IP* for the WAN connection. Contact your ISP to confirm your WAN connection type.

■ PPPoE

Select *PPPoE* and click *Next*, then the following page will appear. In the **WAN Settings** section, specify the parameters that are provided by your ISP and click *Next*.

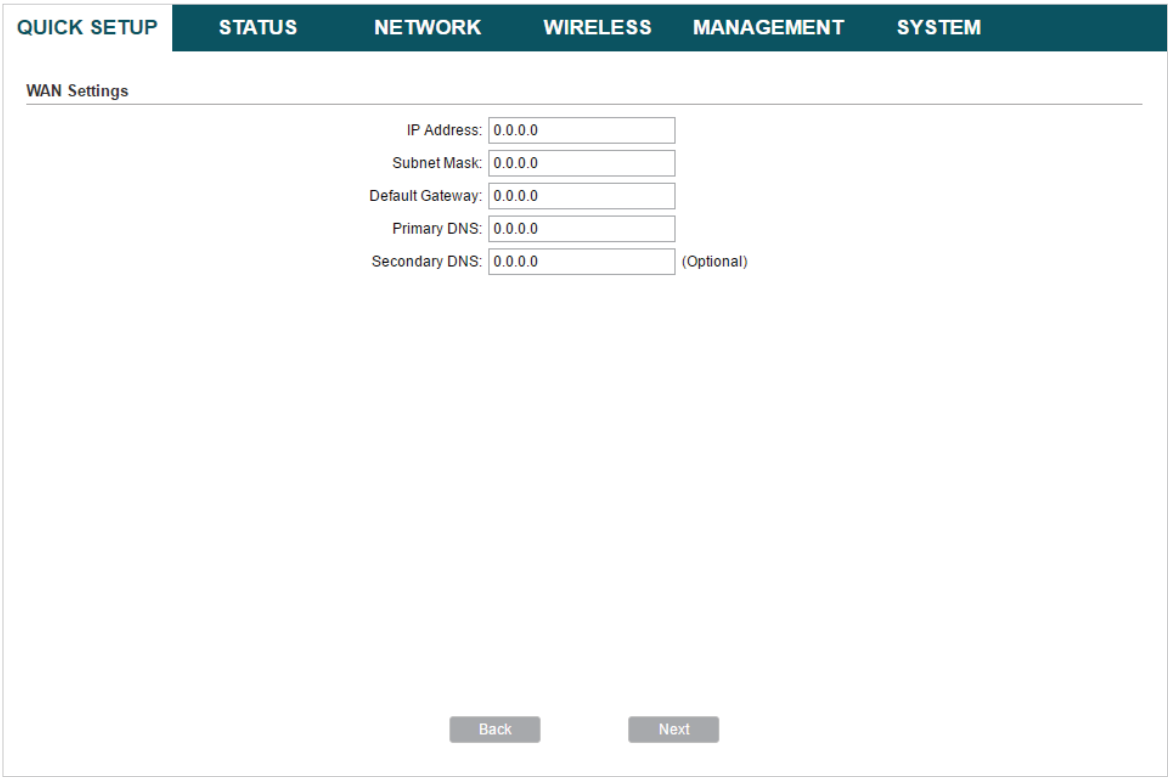


■ Dynamic IP

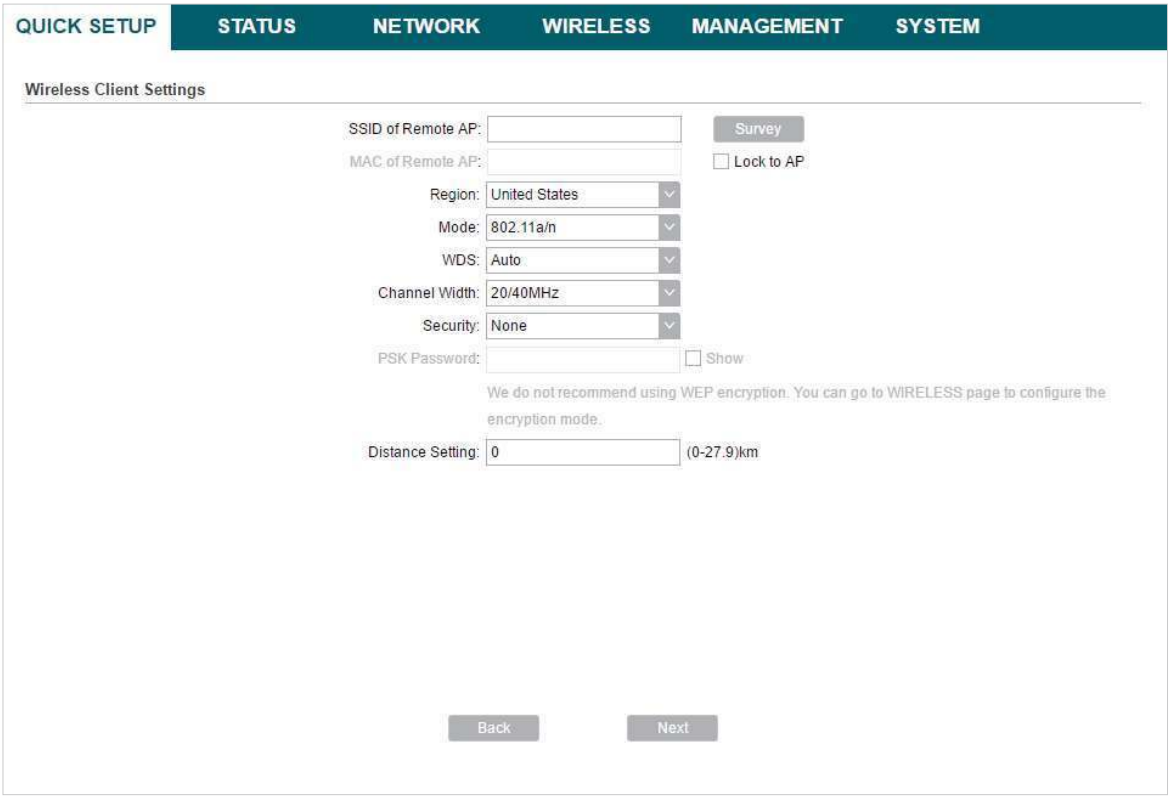
Select *Dynamic IP* and click *Next*. In this type, the device will obtain a WAN connection automatically without any WAN configurations.

■ Static IP

Select *Static IP* and click *Next*, then the following page will appear. In the **WAN Settings** section, specify the parameters that are provided by your ISP and click *Next*.



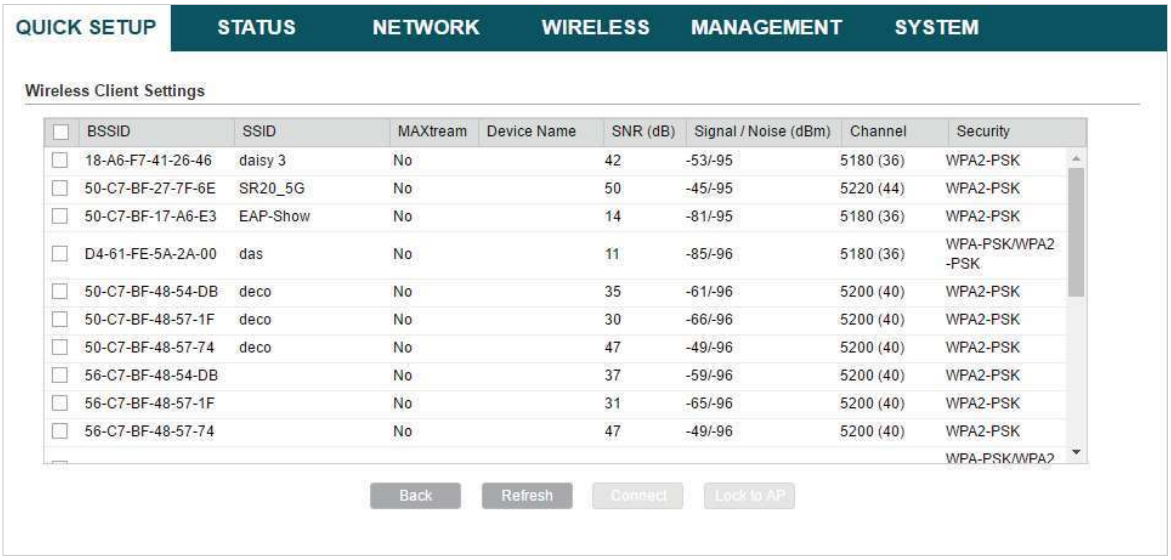
3. In the **Wireless Client Settings** section, click *Survey* to search for the upstream wireless network.



4. Select the desired wireless network and click *Connect*.

Note:

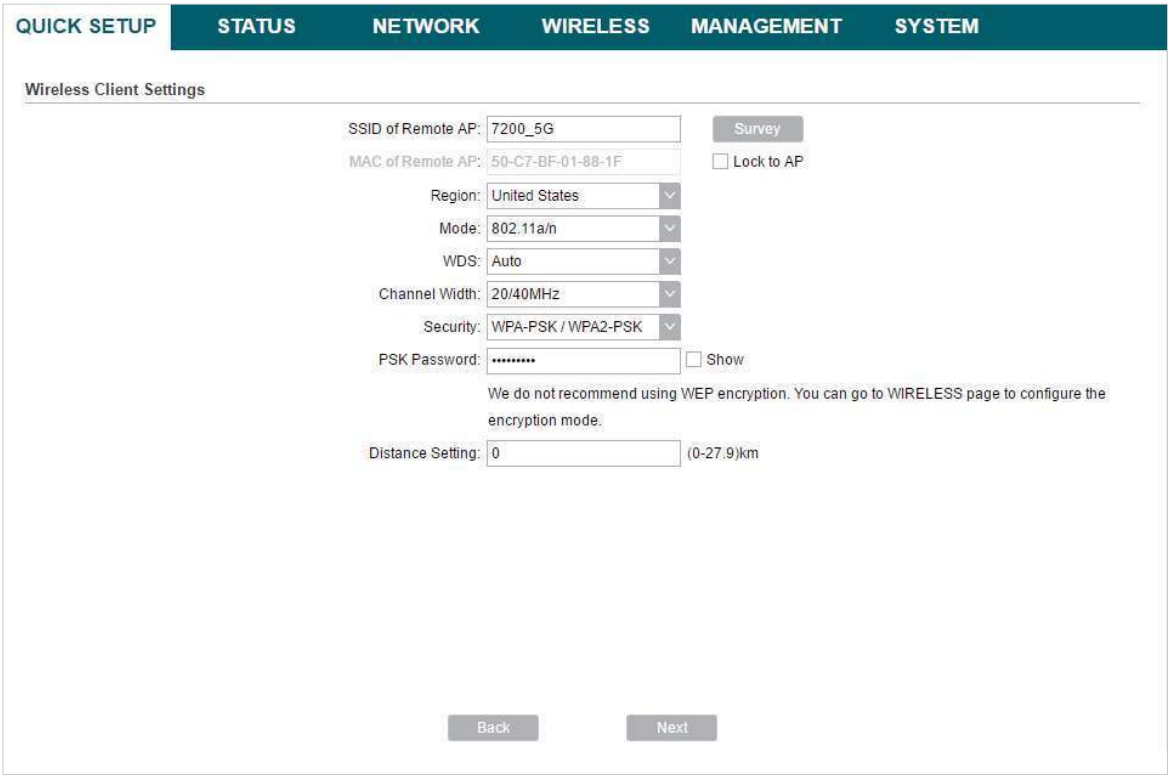
There may be two or more networks with the same SSID in the AP list. Click *Lock to AP* to select the SSID and AP simultaneously, which can make the device connect to the specific AP next time.



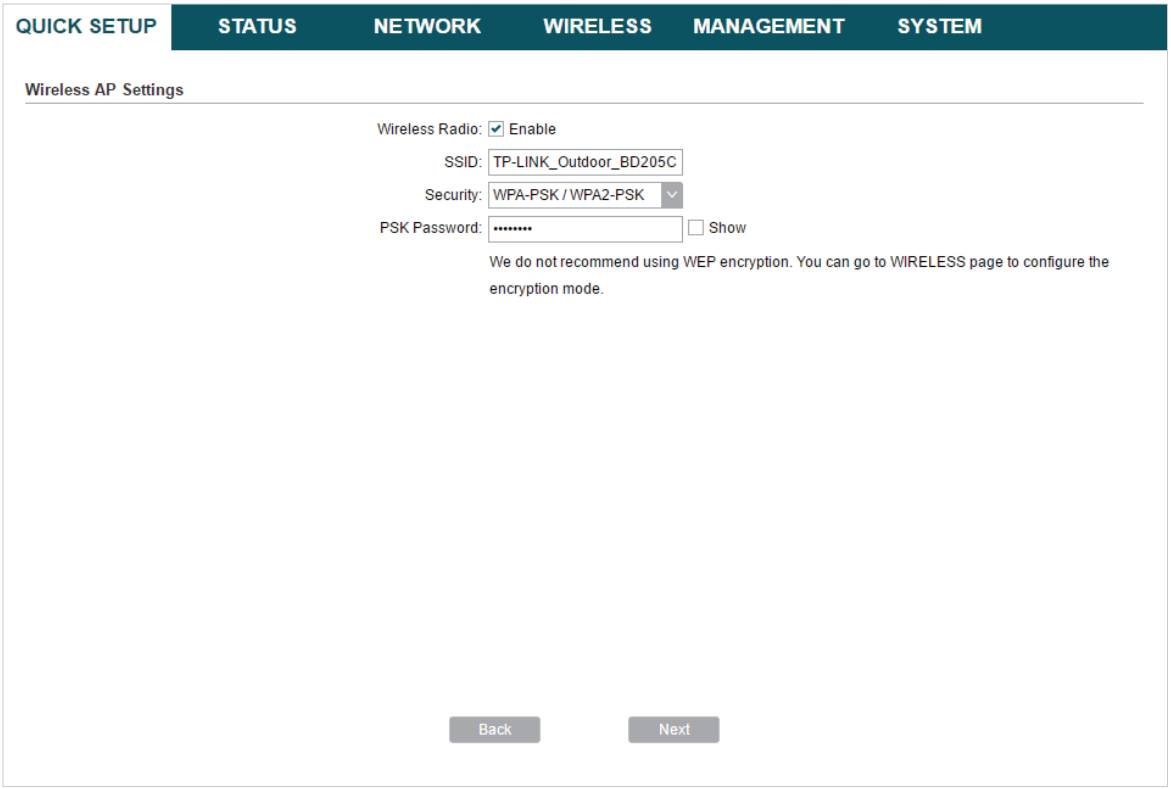
5. In the **Wireless Client Settings** section, specify the wireless parameters to connect to the specified wireless network. Click *Next*.

Note:

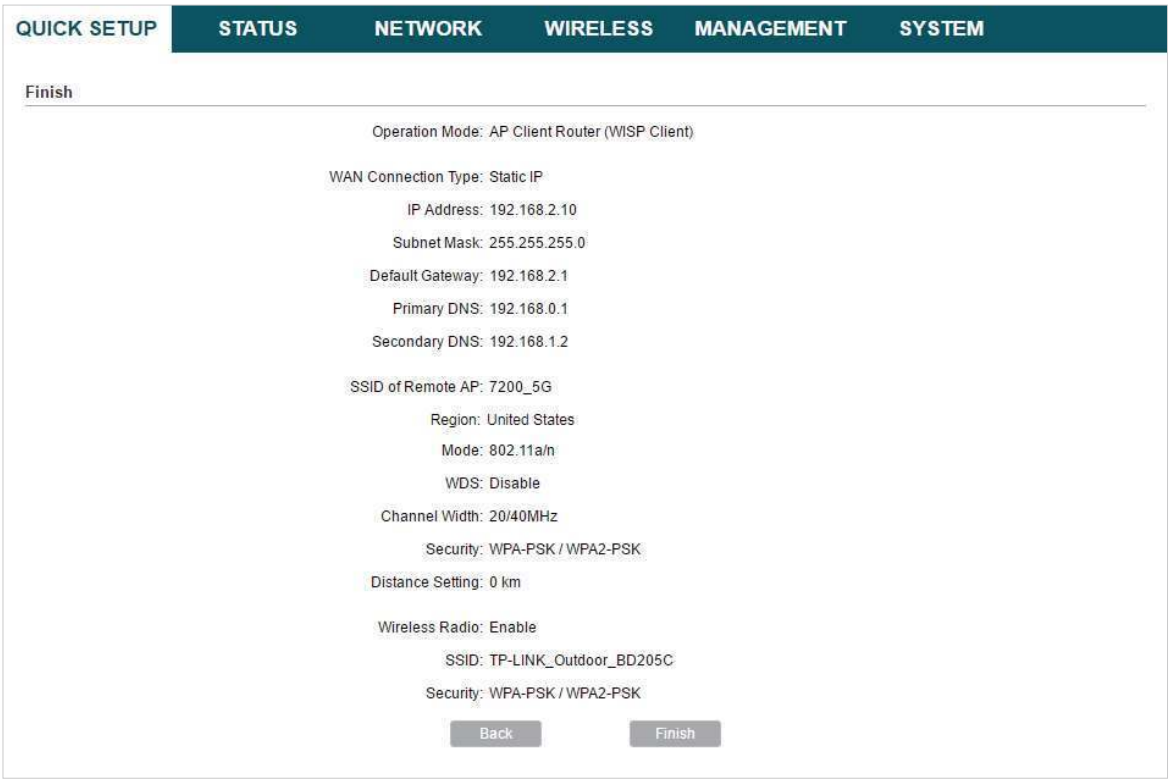
Make sure that *Security* and *PSK Password* are the same as the upstream wireless network's. Other parameters set in this page and those of the upstream wireless network should be compatible with each other. For details, refer to *5. Configure the Wireless Parameters*.



6. In the **Wireless AP Settings** section, specify the parameters to create a new wireless network for the downstream clients. Click *Next*.



7. In the **Finish** section, review the configurations and click *Finish* to complete the quick setup.



8. Connect the device according to your network topology and use it normally.

3 Monitor the Network

This chapter introduces how to monitor the running status and statistics of the wireless network, including:

3.1 View the Device Information

3.2 View the Wireless Settings

3.3 View Wireless Signal Quality

3.4 View Radio Status

3.5 View the LAN Settings

3.6 View the WAN Settings

3.7 Monitor Throughput

3.8 Monitor Stations

3.9 Monitor Interfaces

3.10 Monitor ARP Table

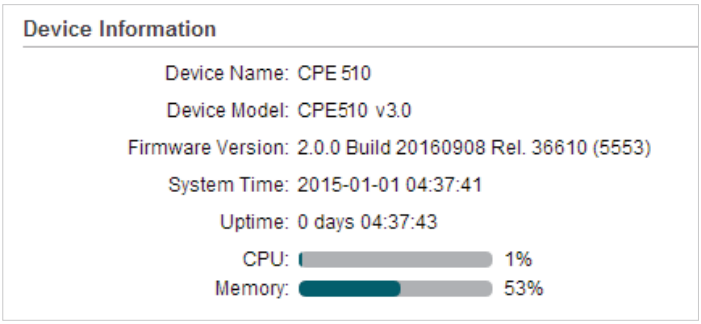
3.11 Monitor Routes

3.12 Monitor DHCP Clients

3.13 Monitor Dynamic WAN

3.1 View the Device Information

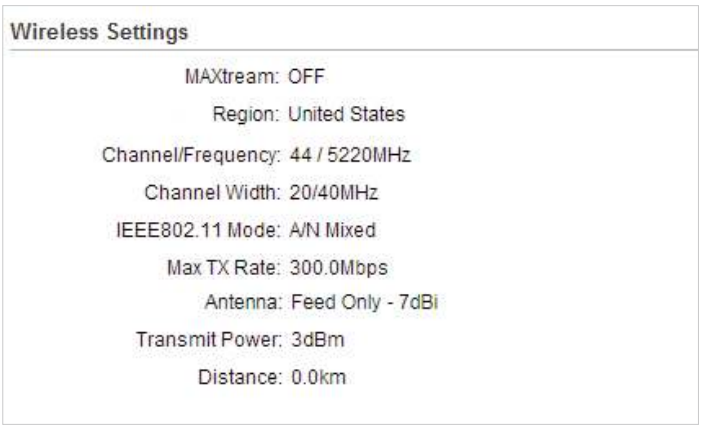
Go to the **STATUS** page. In the **Device Information** section, view the basic information of the device. To configure the device information, refer to *7. Configure the System*.



Device Name	Displays the name of the device. By default, it is the product model.
Device Model	Displays the product model and the hardware version of the device.
Firmware Version	Displays the current firmware version of the device.
System Time	Displays the current system time.
Uptime	Displays the running time of the device.
CPU	Displays the CPU occupancy.
Memory	Displays the memory occupancy.

3.2 View the Wireless Settings

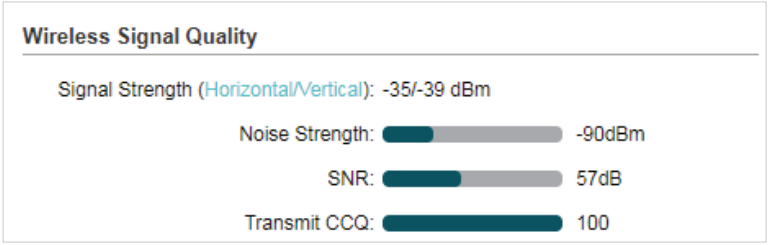
Go to the **STATUS** page. In the **Wireless Settings** section, view the parameters of the wireless network created by the device. To configure the parameters, refer to *5. Configure the Wireless Parameters*.



MAXtream	**Note:** • MAXtream is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. • MAXtream Technology is only compatible with Pharos series products. Working with products from other manufacturer will cause network fault. Displays the status of the MAXtream function. This function is only available in Access Point Mode and AP Router Mode. MAXtream is a TP-Link proprietary technology. It is based on TDMA (Time Division Multiple Access) so that data streams are transmitted in their own time slots. MAXtream aims to maximize throughput and minimize latency. "Hidden nodes" problem can also be eliminated with MAXtream enabled.
Region	Displays the region where you use the device. Available channels and maximum Transmit Power will be determined by the selected region according to the local laws and regulations.
Channel/ Frequency	Displays the channel and frequency which are currently used by the device.
Channel Width	Displays the channel width which is currently used by the device.
IEEE802.11 Mode	Displays the IEEE802.11 protocol currently used by the device.
Max TX Rate	Displays the maximum data rate of the device during the sending of the wireless packets.
Antenna	Displays the antenna that you use.
Transmit Power	Displays the transmit power which is currently used by the device.
Distance	Displays the wireless coverage distance. In the coverage of the device, the clients can be placed to get good wireless performance.

3.3 View Wireless Signal Quality

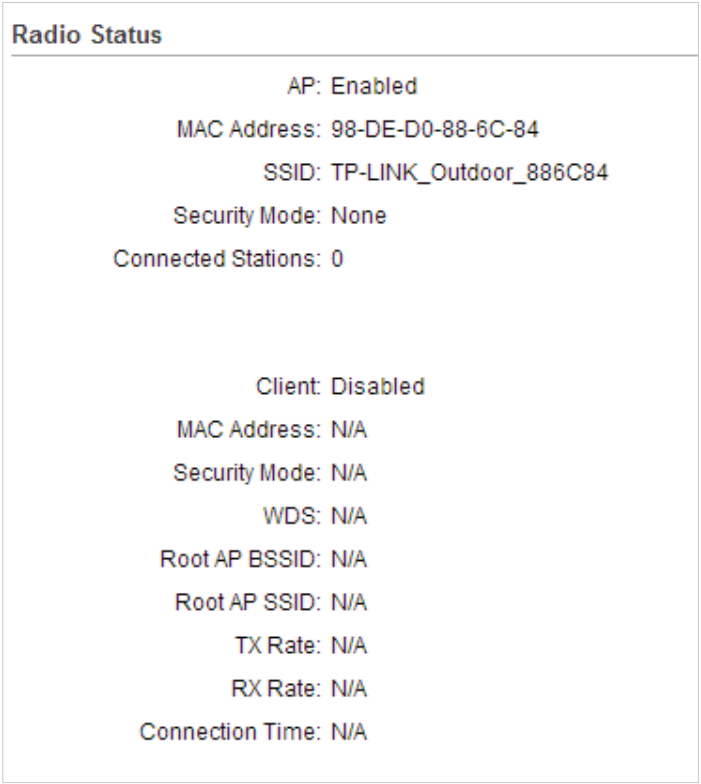
Go to the **STATUS** page. In the **Wireless Signal Quality** section, view the current signal quality of the upstream wireless network. It is only applicable for the Client, Repeater, Bridge and AP Client Router (WISP Client) Modes.



Signal Strength	Displays the received wireless signal strength of the root AP. There are two display modes. Values of the two chains are displyed separately in Horizontal/Vertical Mode, and together in Combined Mode. You can switch between display modes by clicking on it.
Noise Strength	Displays the received environmental noise from wireless interference on the operating frequency.
SNR	Displays the Signal to Noise Ratio (SNR) of the device. SNR refers to the power ratio between the received wireless signal strength and the environmental noise strength. The larger SNR value is, the better network performance the device can provide.
Transmit CCQ	Displays the wireless Client Connection Quality (CCQ). CCQ refers to the ratio of effective transmission bandwidth and the actual total bandwidth. It reflects the quality of the actual link. A larger value means a better utilization of the bandwidth.

3.4 View Radio Status

Go to the **STATUS** page. In the **Radio Status** section, view the radio status of the device.



- AP Status.

AP	Displays the status of the wireless AP function. With this enabled, the device can provide a wireless network for the clients. By default, it is enabled in Access Point, Repeater, Bridge, AP Router and AP Client Router Modes and disabled in Client Mode.
MAC Address	Displays the MAC address of the wireless interface connected to the clients.
SSID	Displays the wireless network name (SSID) created by the device.
Security Mode	**Note:** WEP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Displays the security mode you've selected for your wireless network. There are three security modes: WPA-PSK, WPA and WEP. None means that no security mode is selected and all the hosts are allowed to access the wireless network directly. The security mode which is set on the clients should be the same as that on this device.
Connected Stations	Displays the number of the connected stations.

- Client Status.

Client	Displays the status of the wireless client function. With this function enabled, the device can connect to the root AP through wireless connection. By default, it is enabled in Client, Repeater, Bridge and AP Client Router Modes and disabled in Access Point and AP Router Modes.
MAC Address	Displays the MAC address of the wireless interface connected to the root AP.
Security Mode	**Note:** WEP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Displays the security mode you've selected for your wireless network. There are three security modes: WPA-PSK, WPA and WEP. None means that no security mode is selected and all the hosts are allowed to access the wireless network directly. The security mode which is set on the device should be the same as that on the root AP.

WDS	Displays the status of the WDS (Wireless Distribution System) function. WDS is a communication system among multiple wireless networks . It is established between APs through wireless connection. WDS is used during the connection process between the device and the root AP. **Enable:** Forward data frames using four address fields. **Disable:** Forward data frames using three address fields. **Auto:** The device automatically negotiates the wireless data frame structure (three or four address fields) with the root AP. The selection of Auto is recommended.
Root AP BSSID	Displays the BSSID (Basic Service Set ID) of the root AP. BSSID is used to identify a BSS. Each BSS has its own BSSID. The BSSID is decided by the manufacturers, and it is usually related to the device's MAC address.
Root AP SSID	Displays the wireless network name of the root AP.
TX Rate	Displays the data rate of the device during the sending of the wireless packets.
RX Rate	Displays the data rate of the device during the receiving of the wireless packets.
Connection Time	Displays the amount of time the device has been connected to the root AP.

3.5 View the LAN Settings

Go to the **STATUS** page. In the **LAN** section, view the LAN information of the device. To configure the LAN settings, refer to *4. Configure the Network*.

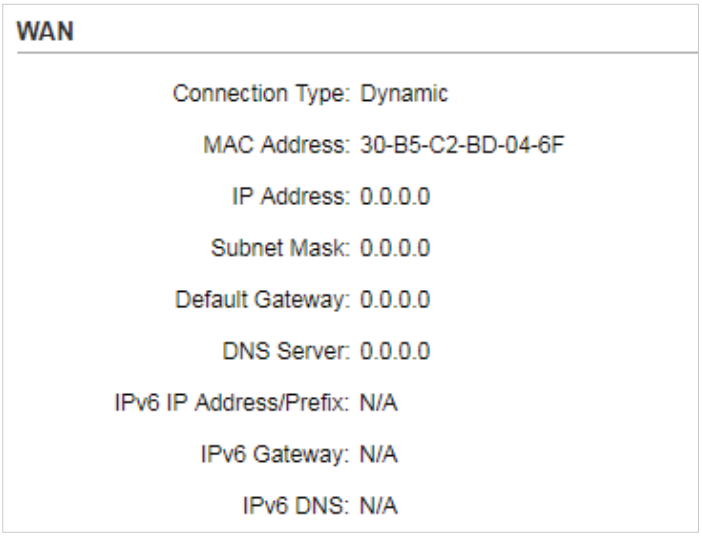


MAC Address	Displays the LAN port MAC address of the device.
IP Address	Displays the LAN port IP address of the device.
Subnet Mask	Displays the subnet mask of the LAN.

Port	Displays the current status of the LAN Ethernet port connections and the Maximum transmission rate of the plugged port.
IPv6 IP Address/Prefix	Displays the LAN port IPv6 address and prefix of the device.

3.6 View the WAN Settings

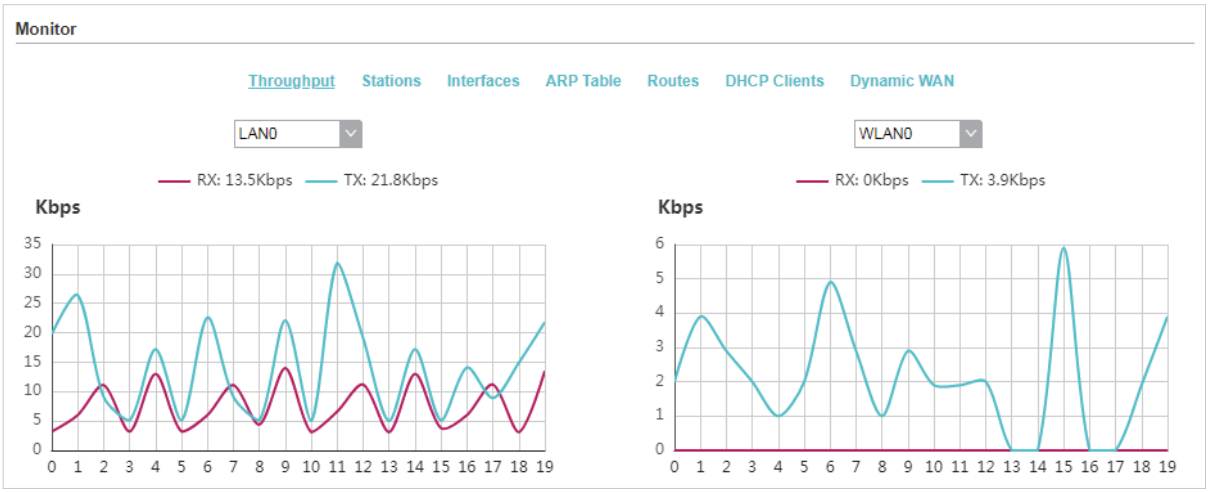
Go to the **STATUS** page. In the **WAN** section, view the WAN information of the device. To configure the WAN settings, refer to *4. Configure the Network*.



Connection Type	Displays the connection type of the device.
MAC Address	Displays the MAC address of the wireless interface connected to the root AP.
IP Address	Displays the IP address of the wireless interface connected to the root AP.
Subnet Mask	Displays the subnet mask of the wireless interface connected to the root AP.
Default Gateway	Displays the default gateway.
DNS Server	Displays the DNS server.
IPv6 IP Address/Prefix	Displays the WAN port IPv6 address and prefix of the device.
IPv6 Gateway	Displays the default IPv6 gateway.
IPv6 DNS	Displays the IPv6 DNS server.

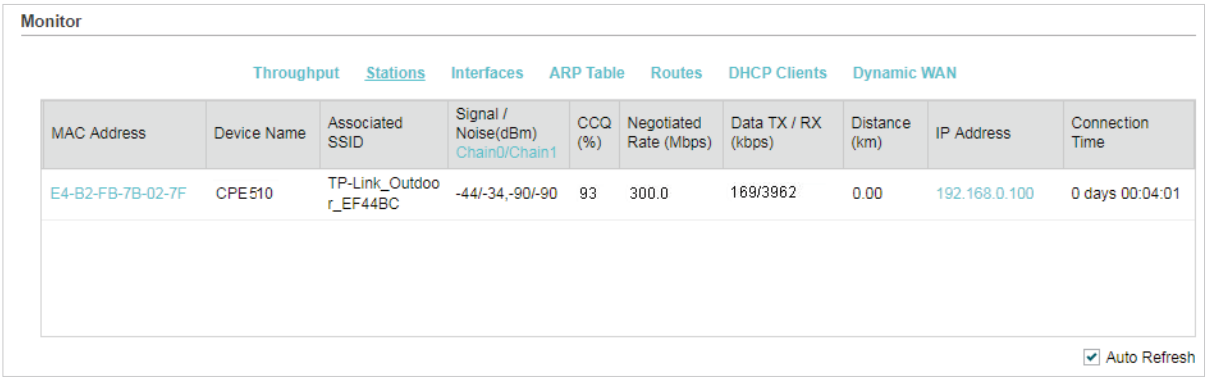
3.7 Monitor Throughput

Go to the **STATUS** page. In the **Monitor** section, select *Throughput* and monitor the current data traffic of specified interfaces including LAN, WAN, WLAN, WWAN and BRIDGE. Note that the interfaces which you can monitor are different among different operation modes.



3.8 Monitor Stations

Go to the **STATUS** page. In the **Monitor** section, select *Stations* and monitor the information of all the stations that are connected to the device.



MAC Address	Displays the MAC address of the station.
Device Name	Displays the device name of the station.
Associated SSID	Displays the SSID that the station is connected to.
Signal/Noise (dBm)	Displays the signal strength and the noise strength of the wireless network. There are two display modes. Values of the two chains are displayed separately in Chain0/Chain1 Mode, and together in Combined Mode. You can switch between display modes by clicking on it.

CCQ (%)	Displays the wireless Client Connection Quality (CCQ). CCQ refers to the ratio of effective transmission bandwidth and the actual total bandwidth. It reflects the quality of the actual link. A larger value means a better utilization of the bandwidth.
Negotiated Rate (Mbps)	Displays the negotiated rates of the packets which the device transmits to the station.
Data TX/RX (kbps)	Displays the data rates of the last transmitted and received packets. TX means that the device transmits data to the station, while RX means that the device receives data from the station.
Distance (km)	Displays the distance between the device and the station.
IP Address	Displays the IP address of the station.
Connection Time	Displays the connection duration.
Auto Refresh	Enable or disable Auto Refresh. With this feature enabled, the table will refresh automatically.

Click the MAC Address of a station to view the detailed information.



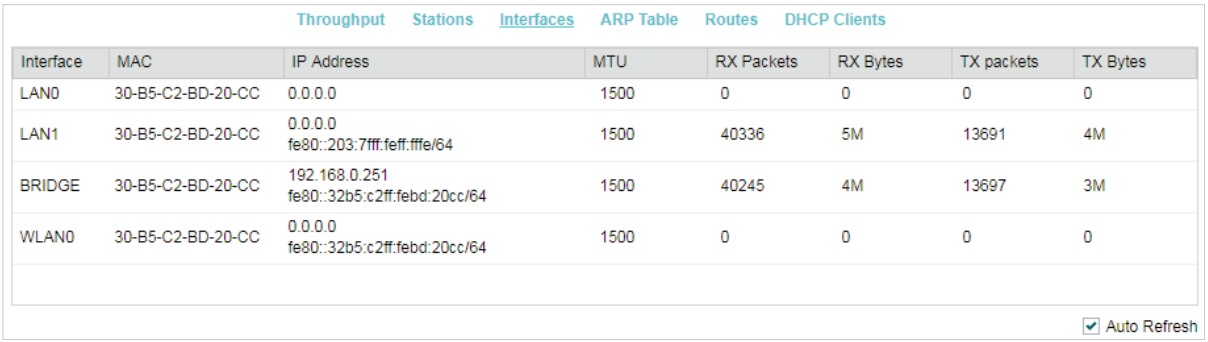
Device Name	Displays the device name of the station.
Product	Displays the product name of the station.
Firmware	Displays the firmware version of the station.
Connection Time	Displays the connection duration.

RX Signal	Displays the signal strength of the wireless network.
Noise Floor	Displays the noise strength of the wireless network.
CCQ	Displays the wireless Client Connection Quality (CCQ). CCQ refers to the ratio of effective transmission bandwidth and the actual total bandwidth. It reflects the quality of the actual link. A larger value means a better utilization of the bandwidth.
Last IP	Displays the IP address of the station.
TX/RX Rate	Displays the negotiated rates of the transmitted and received packets. TX means that the device transmits data to the station, while RX means that the device receives data from the station.
TX/RX Bit Rate	Displays the data rates of the last transmitted and received packets. TX means that the device transmits data to the station, while RX means that the device receives data from the station.
TX/RX Packets	Displays the total number of the transmitted and received packets. TX means that the device transmits data to the station, while RX means that the device receives data from the station.
TX/RX Packets Rate, pps	Displays the packet rates of the transmitted and received packets. TX means that the device transmits data to the station, while RX means that the device receives data from the station.
Bytes Transmitted	Displays the total amount of data which the device transmits to the station.
Bytes Received	Displays the total amount of data which the device receives from the station.
Negotiated Rate	Displays the possible negotiated rates of the packets which the device receives from the station.
Last Signal, dBm	Displays the signal strength of the last packet which the device receives from the station at the corresponding negotiated rate.

Click the IP Address of a station to access the web management page of the station.

3.9 Monitor Interfaces

Go to the **STATUS** page. In the **Monitor** section, select *Interfaces* and monitor the relevant information of the interfaces.

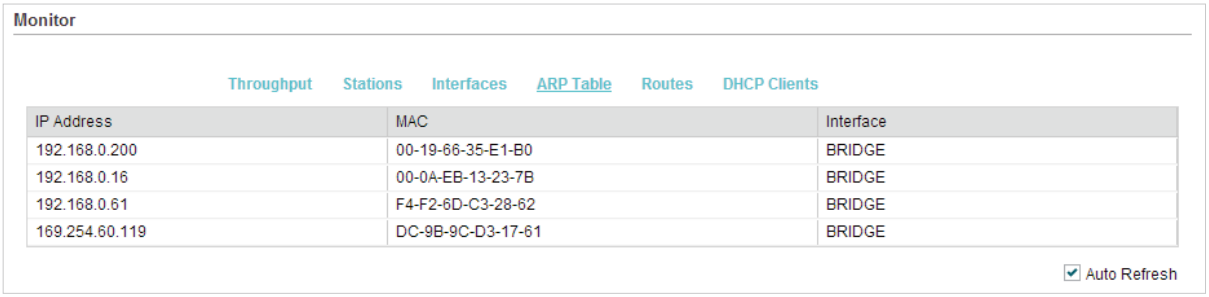


Interface	Displays the interface of the device.
MAC	Displays the MAC address of the interface.
IP Address	Displays the IP address and IPv6 address of the interface.
MTU	Displays the Maximum Transmission Unit (MTU) of the interface. It is the maximum packet size (in bytes) that the interface can transmit.
RX packets	Displays the total amount of packets received by the interface after the device is powered on.
RX Bytes	Displays the total amount of data (in bytes) received by the interface after the device is powered on.
TX packets	Displays the total amount of packets sent by the interface after the device is powered on.
TX Bytes	Displays the total amount of data (in bytes) sent by the interface after the device is powered on.
Auto Refresh	Enable or disable Auto Refresh. With this feature enabled, the table will refresh automatically.

3.10 Monitor ARP Table

Go to the **STATUS** page. In the **Monitor** section, select *ARP Table* and monitor the ARP (Address Resolution Protocol) information recorded by the device.

ARP is used to associate each IP address to the unique hardware MAC address of each device on the network.



IP Address	Displays the IP address of the corresponding ARP entry.
MAC	Displays the MAC address of the corresponding ARP entry.
Interface	Displays the interface connected to the device.
Auto Refresh	Enable or disable Auto Refresh. With this feature enabled, the table will refresh automatically.

3.11 Monitor Routes

Go to the **STATUS** page. In the **Monitor** section, select *Routes* and monitor the routing entries recorded by the device in the Routing table. Routing table is used for the device to decide the interface to forward the packets. You can enable or disable *Auto Refresh*. With this feature enabled, the table will refresh automatically.



- IPv4 Routes

Destination	Displays the IP address of the destination device or destination network.
Gateway	Displays the IP address of the appropriate gateway.
SubnetMask	Displays the Subnet Mask of the destination network.

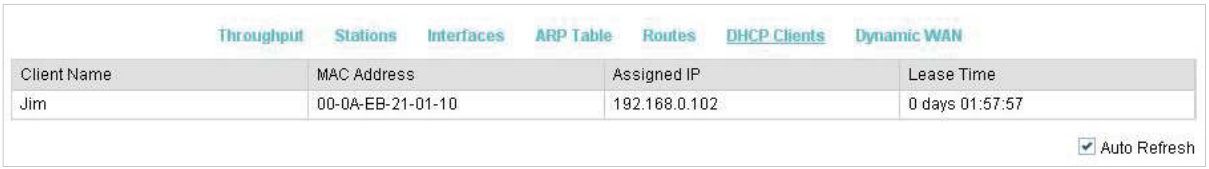
Interface	Displays the interface that the destination device is on.

- IPv6 Routes

Destination	Displays the IPv6 address of the destination device or destination network.
Gateway	Displays the IPv6 address of the appropriate gateway.
Interface	Displays the interface that the destination device is on.

3.12 Monitor DHCP Clients

Go to the **STATUS** page. In the **Monitor** section, select *DHCP Clients* and monitor the information of all the DHCP clients.



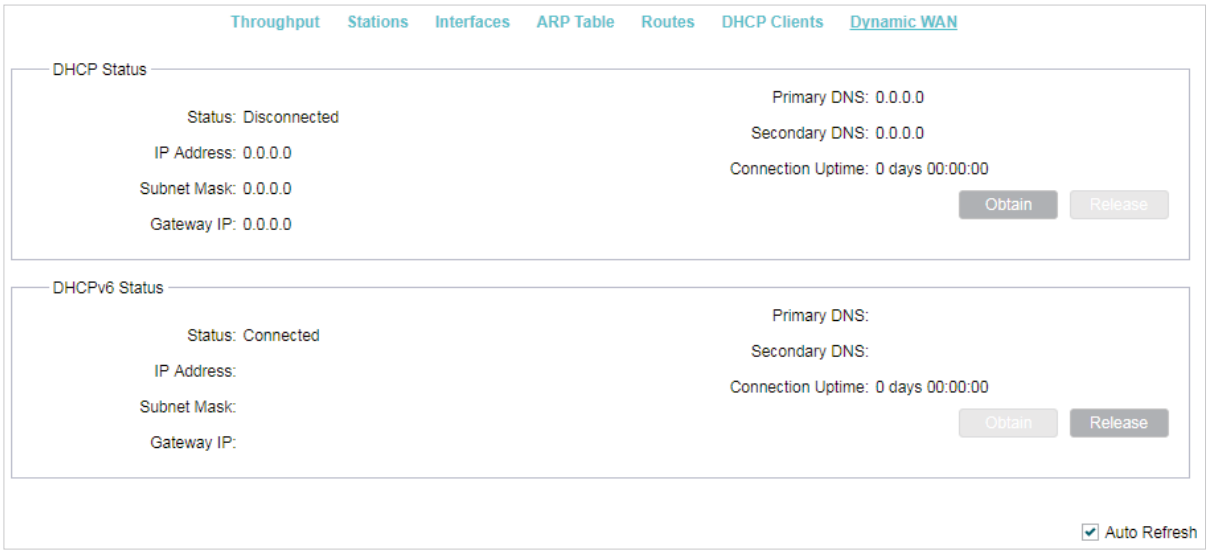
Client Name	Displays the device name of the client.
MAC Address	Displays the MAC address of the client.
Assigned IP	Displays the IP address that the device assigned to the client.
Lease Time	Displays the time that the client leased. When the time expires, the clients will request to renew the lease automatically.
Auto Refresh	Enable or disable Auto Refresh. With this feature enabled, the table will refresh automatically.

3.13 Monitor Dynamic WAN

Note:

Dynamic WAN submenu is only available in AP Router Mode and AP Client Router (WISP Client) Mode when the WAN connection type is PPPoE, PPTP, L2TP or Dynamic.

Go to the **STATUS** page. In the **Monitor** section, select *Dynamic WAN* and monitor the WAN connection status of the device. You can enable or disable Auto Refresh. With this feature enabled, the table will refresh automatically.



- DHCP Status

Status	Displays the status of the WAN connection.
IP Address	Displays the IP address of the WAN.
Subnet Mask	Displays the subnet mask of the WAN.
Gateway IP	Displays the gateway address of the device.
Primary DNS	Displays the primary DNS of the device.
Secondary DNS	Displays the secondary DNS of the device.
Connection Uptime	Displays the time that the latest WAN connection lasts.
Obtain	Click *Obtain* to obtain the WAN IP address from the upstream device.
Release	Click *Release* to release the WAN IP address.

- DHCPv6 Status

Status	Displays the status of the WAN connection.
IP Address	Displays the IPv6 address of the WAN.
Subnet Mask	Displays the subnet mask of the WAN.
Gateway IP	Displays the gateway address of the device.

Primary DNS	Displays the primary DNS of the device.
Secondary DNS	Displays the secondary DNS of the device.
Connection Uptime	Displays the time that the latest WAN connection lasts.
Obtain	Click *Obtain* to obtain the WAN IPv6 address from the upstream device.
Release	Click *Release* to release the WAN IPv6 address.

4 Configure the Network

This chapter introduces how to configure the network parameters and the advanced features, including:

4.1 Configure WAN Parameters

4.2 Configure LAN Parameters

4.3 Configure Management VLAN

4.4 Configure the Forwarding Feature

4.5 Configure the Security Feature

4.6 Configure Access Control

4.7 Configure Static Routing

4.8 Configure Bandwidth Control

4.9 Configure IP & MAC Binding

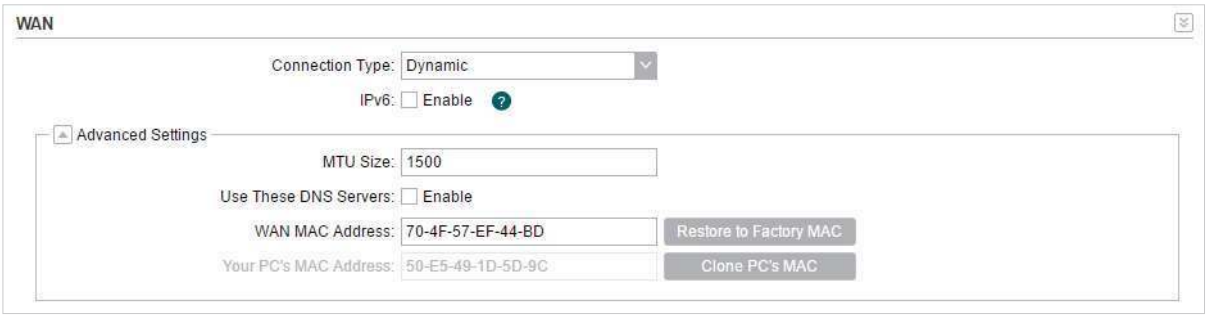
4.1 Configure WAN Parameters

Note:

WAN submenu is only available in AP Router Mode and AP Client Router (WISP Client) Mode.

WAN submenu is used to create the WAN connection and configure the related advanced parameters.

Go to the **Network** page. In the **WAN** section, configure the WAN parameters of the device.



Follow the steps below to configure the WAN parameters:

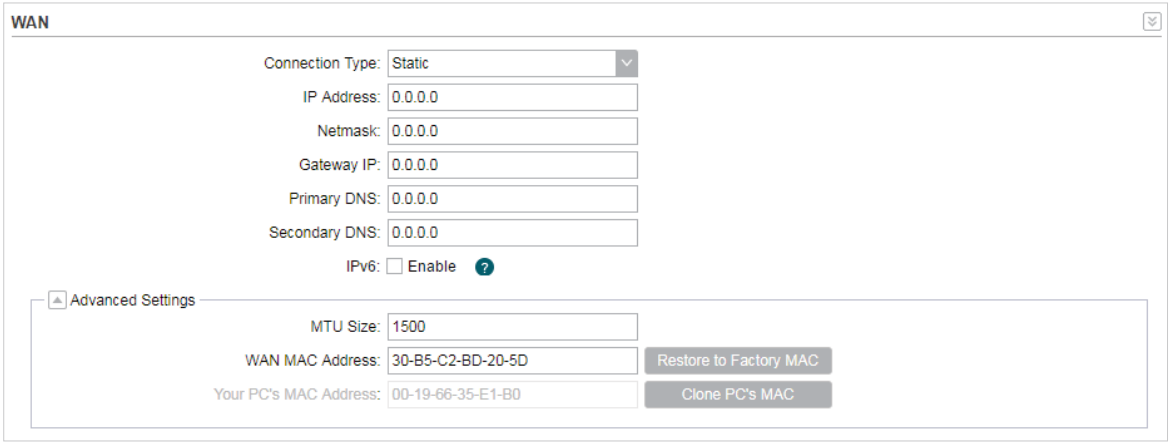
1. Select the connection type according to your need. The device supports five types: Static, Dynamic, PPPoE, L2TP, and PPTP.

Note:

L2TP or PPTP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

■ **Static**

This connection type uses a permanent, fixed (static) IP address that is assigned by your ISP. In this type, you should fill in the IP address, Netmask, Gateway IP, and DNS IP address manually, which are assigned by your ISP.

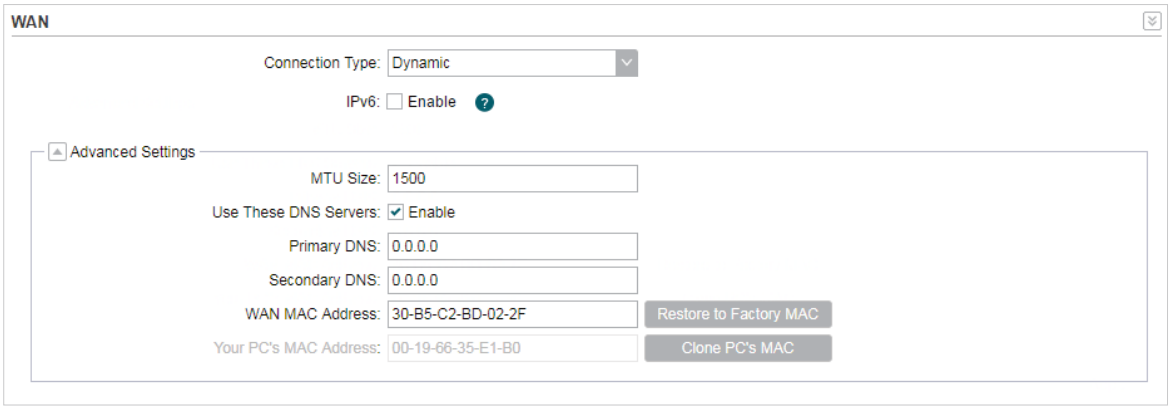


IP address	Enter the IP address provided by your ISP.
Netmask	Enter the netmask provided by your ISP. Normally use 255.255.255.0.
Gateway IP	Enter the gateway IP address provided by your ISP.
Primary DNS	Enter the DNS IP address provided by your ISP.
Secondary DNS	Enter alternative DNS IP address if your ISP provides it.
IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a WAN IPv6 address. Select a method for the device to obtain the WAN IPv6 address according to the information provided by your ISP. • **Static** Select static and enter the WAN IPv6 address, IPv6 netmask, IPv6 gateway, primary DNS and secondary DNS provided by your ISP.  • **SLAAC** Select SLAAC and the device will obtain the WAN IPv6 address automatically.  • **DHCPv6** Select DHCPv6 and the device will obtain the WAN IPv6 address automatically. 
MTU Size	The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. This number should be an integer between 576 and 2026.

WAN MAC Address	Specify the MAC address of WAN interface. This field displays the current MAC address of the WAN port. If your ISP requires that you register the MAC address, enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Click *Restore Factory MAC* to restore the MAC address of WAN port to the factory default value.
Your PC's MAC Address	Displays the MAC address of the PC that is managing the device. Some ISPs require that you should register the MAC address of your PC. If the MAC address is required, click *Clone PC's MAC* to set the WAN MAC address the same as your management PC's MAC address.

■ Dynamic

For this connection, your ISP uses a DHCP server to assign your router an IP address for connecting to the internet. You don't need to configure any parameters.

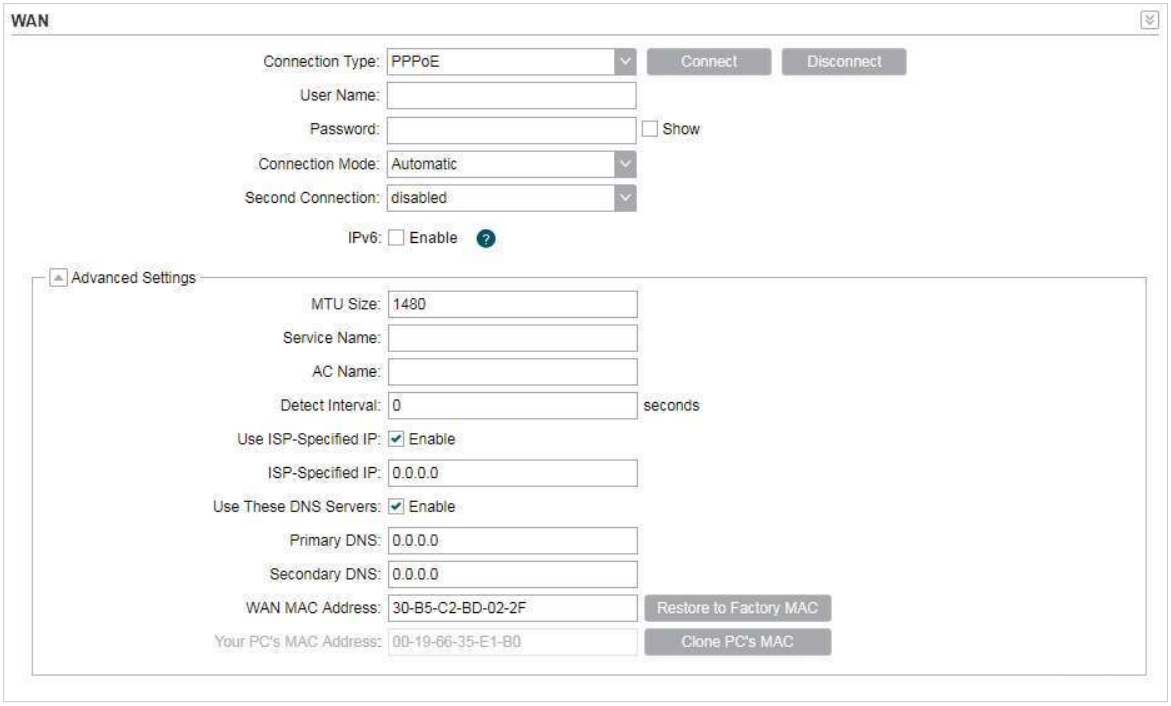


IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a WAN IPv6 address. Select a method for the device to obtain the WAN IPv6 address according to the information provided by your ISP. • **Static** Select static and enter the WAN IPv6 address, IPv6 netmask, IPv6 gateway, primary DNS and secondary DNS provided by your ISP.  • **SLAAC** Select SLAAC and the device will obtain the WAN IPv6 address automatically.  • **DHCPv6** Select DHCPv6 and the device will obtain the WAN IPv6 address automatically. 
MTU Size	Specify the MTU size. The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. This number should be an integer between 576 and 2026.
Use These DNS Servers	If your ISP gives you one or two DNS IP addresses, select Use These DNS Servers and enter the Primary DNS and Secondary DNS into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.
Primary DNS	Enter the DNS IP address provided by your ISP.
Secondary DNS	Enter another DNS IP address provided by your ISP.

WAN MAC Address	Specify the WAN MAC address. This field displays the current MAC address of the WAN port. If your ISP binds the MAC address of your previous computer/router, enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Click *Restore Factory MAC* to restore the MAC address of WAN port to the factory default value.
Your PC's MAC Address	Displays the MAC address of the PC that is managing the device. Some ISPs require that you should register the MAC address of your PC. If the MAC address is required, click *Clone PC's MAC* to set the WAN MAC address the same as your management PC's MAC address.

■ PPPoE

If your ISP delivers internet through phone line and provides you with username and password, you should choose this type. Under this condition, you should fill in both User Name and Password that the ISP supplied. Note that these fields are case-sensitive.



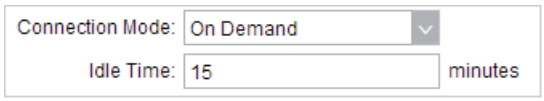
Specify the parameters below and click *Connect*:

User Name	Enter the User Name that is provided by your ISP.
Password	Enter the Password that is provided by your ISP.

Connection Mode	Select the Connection Mode.

- **On Demand**

  Configure the device to disconnect your internet connection after a specified period of inactivity (Idle Time). If your internet connection has been terminated due to inactivity, Connection on Demand enables the device to automatically re-establish your connection when you attempt to access the internet again. The default Idle Time is 15 minutes. If your internet connection is expected to remain active all the time, enter 0 in the Idle Time field. If you pay by time for your internet access, choose this mode to save your internet-access fee.

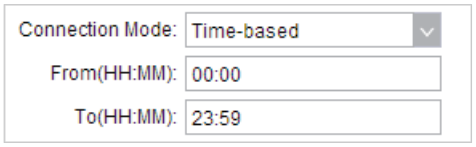


- **Automatic**

  Connect automatically after the device is disconnected. If you are charged a flat monthly fee, choose this mode.

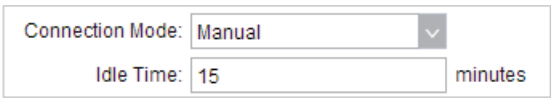
- **Time-based**

  Configure the device to make it connect or disconnect based on time. Enter the start time in From (HH:MM) for connecting and end time in To (HH:MM) for disconnecting. If you need to control the time period of internet access, choose this mode.



- **Manual**

  Configure the device to make it connect or disconnect manually. After a specified period of inactivity (Idle Time), the device will disconnect your internet connection, and you must click *Connect* manually to access the internet again. If your internet connection is expected to remain active all the times, enter 0 in the Idle Time field. Otherwise, enter the desired Idle Time in minutes you wish to use. If you pay by time for your internet access, choose this mode to save your internet-access fee.



Second Connection	**Note:** Second Connection is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, activate this secondary connection. **Disable:** The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended. **Dynamic IP:** Use dynamic IP address to connect to the local area network provided by ISP. **Static IP:** Use static IP address to connect to the local area network provided by ISP.
IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a WAN IPv6 address. Select a method for the device to obtain the WAN IPv6 address according to the information provided by your ISP. • **SLAAC** Select SLAAC and the device will obtain the WAN IPv6 address automatically.  • **DHCPv6** Select DHCPv6 and the device will obtain the WAN IPv6 address automatically. 
MTU Size	Specify the MTU size. The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually appropriate. For some ISPs, you need modify the MTU. This should not be done unless your ISP told you to. This number should be an integer between 576 and 2026.
Service Name	Specify the Service Name provided by your ISP. Keep it empty if your ISP doesn't provide the name.
AC Name	Specify the AC Name provided by your ISP. Keep it empty if your ISP doesn't provide the name.
Detect Internal	Specify the Detect Interval. The default value is 0. Input the value between 0 and 120. The device will detect Access Concentrator online every interval seconds. If the value is 0, it means not detecting.

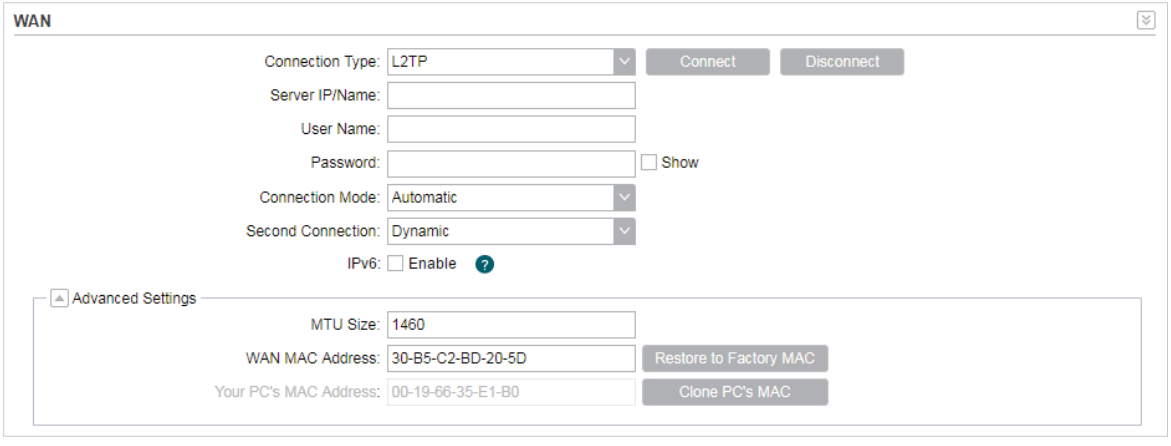
Use ISP-specified IP	If your service provider provides you with an IP address along with the user name and password, Enable "Use ISP-specified IP" and enter the IP address.
Use These DNS Servers	If the ISP provides a DNS server IP address for you, Enable Use These DNS Server, and fill the Primary DNS and Secondary DNS fields below. Otherwise, the DNS servers will obtain automatically from ISP.
WAN MAC Address	Specify the WAN MAC address. This field displays the current MAC address of the WAN port. If your ISP binds the MAC address of your previous computer/router, enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Click *Restore Factory MAC* to restore the MAC address of WAN port to the factory default value.
Your PC's MAC Address	Displays the MAC address of the PC that is managing the device. Click *Clone PC's MAC* to set the WAN MAC address the same as your management PC's MAC address.
Restore to Factory MAC	Click this button to restore the WAN MAC address as factory MAC address.
Clone PC's MAC	Click this button to set the WAN MAC address as PC's MAC address.

■ L2TP/PPTP

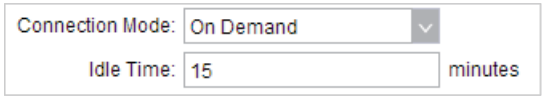
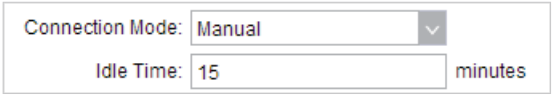
Note:

L2TP or PPTP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

If your ISP supplies internet access through L2TP or PPTP, it will provide the following parameters. The configurations of L2TP and PPTP are the same, and the following introduction takes L2TP as an example.



Specify the parameters below and click *Connect*:

Server IP/Name	Enter the server IP address or the domain name provided by your ISP.
User Name	Enter the User Name provided by your ISP. This field is case-sensitive.
Password	Enter the Password provided by your ISP. This field is case-sensitive.
Connection Mode	Select the Connection Mode. • **On Demand** Configure the device to disconnect your internet connection after a specified period of inactivity (Idle Time). If your internet connection has been terminated due to inactivity, Connection on Demand enables the device to automatically re-establish your connection when you attempt to access the internet again. The default Idle Time is 15 minutes. If your internet connection is expected to remain active all the time, enter 0 in the Idle Time field. If you pay by time for your internet access, choose this mode to save your internet-access fee.  • **Automatic** Connect automatically after the device is disconnected. If you are charged a flat monthly fee, choose this mode. • **Manual** Configure the device to make it connect or disconnect manually. After a specified period of inactivity (Idle Time), the device will disconnect your internet connection, and you must click *Connect* manually to access the internet again. If your internet connection is expected to remain active all the times, enter 0 in the Idle Time field. Otherwise, enter the desired Idle Time in minutes you wish to use. If you pay by time for your internet access, choose this mode to save your internet-access fee. 
Second Connection	If your ISP provides a Connection type such as Dynamic/Static IP to connect to a local area network, activate this secondary connection. **Dynamic IP:** Use dynamic IP address to connect to the local area network provided by ISP. **Static IP:** Use static IP address to connect to the local area network provided by ISP.

IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a WAN IPv6 address. Select a method for the device to obtain the WAN IPv6 address according to the information provided by your ISP. • **Static** Select static and enter the WAN IPv6 address, IPv6 netmask, IPv6 gateway, primary DNS and secondary DNS provided by your ISP.  • **SLAAC** Select SLAAC and the device will obtain the WAN IPv6 address automatically.  • **DHCPv6** Select DHCPv6 and the device will obtain the WAN IPv6 address automatically. 
MTU Size	Specify the MTU size. The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. This number should be an integer between 576 and 2026.
WAN MAC Address	Specify the WAN MAC address. This field displays the current MAC address of the WAN port. If your ISP requires that you register the MAC address, enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Click *Restore Factory MAC* to restore the MAC address of WAN port to the factory default value.
Your PC's MAC Address	Displays the MAC address of the PC that is managing the device. Some ISPs require that you should register the MAC address of your PC. If the MAC address is required, click *Clone PC's MAC* to set the WAN MAC address the same as your management PC's MAC.

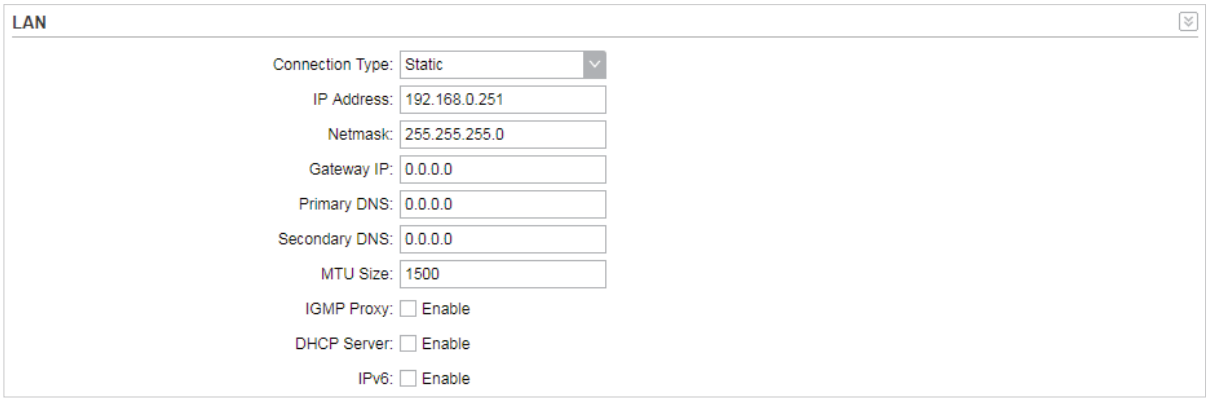
3. Click *Apply*, then click *Save*.

4.2 Configure LAN Parameters

LAN submenu is used to configure the LAN parameters for the device and the clients.

Access Point/Client/Repeater/Bridge Mode

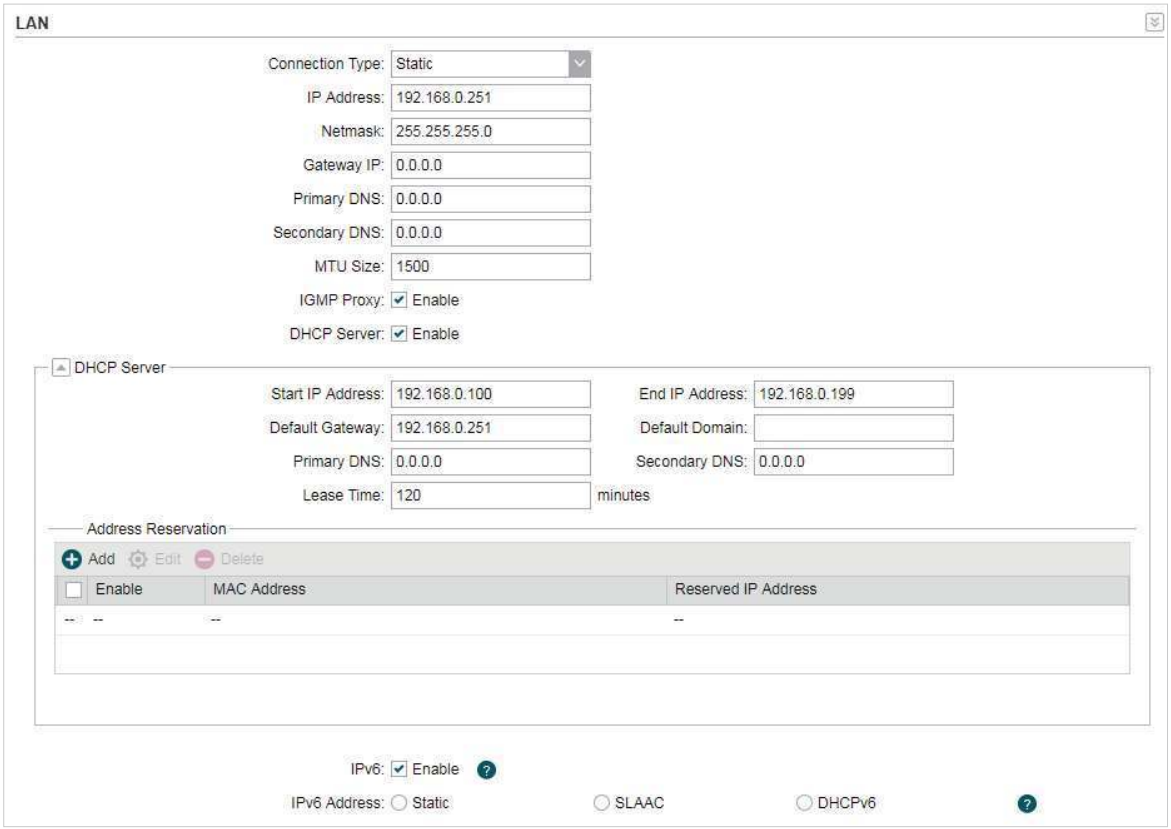
Go to the **Network** page. In the **LAN** section, configure the following parameters.



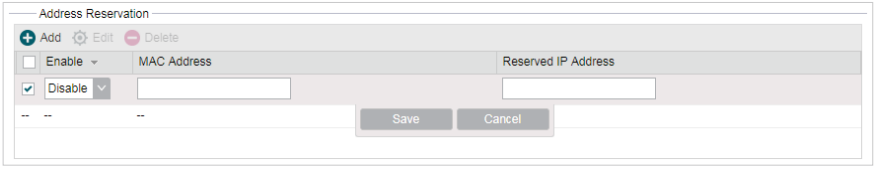
Follow the steps below to configure the LAN parameters:

1. Select the connection type according to your need. The device supports two types: Static and Dynamic.

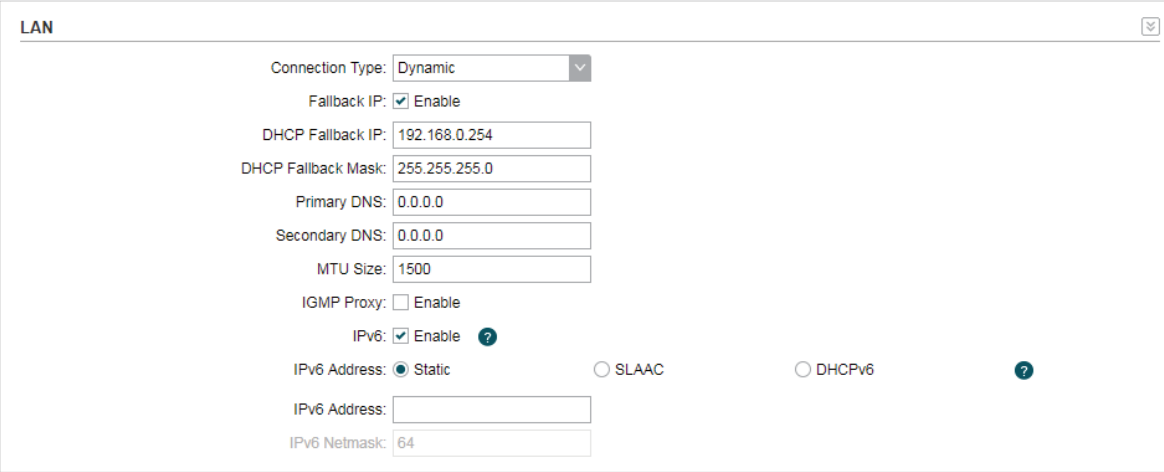
   ■ **Static**



IP address	Enter the LAN IP address of your device. By default, it is 192.168.0.254. **Note:** When you change the LAN IP address in the **Network** tab, you should log in with the new IP address and save the settings for the configuration change to take effect. Otherwise the configuration will be lost after the reboot.
Netmask	Enter the Netmask provided by your ISP. Normally use 255.255.255.0.
Gateway IP	Enter the gateway IP address for your device.
Primary DNS	Enter the primary DNS IP address provided by your ISP. Consult your ISP if you don't know the DNS value. The factory default setting is 0.0.0.0, which means no primary DNS is assigned.
Secondary DNS	Enter the secondary DNS IP address of alternative DNS server if your ISP has two DNS servers. The factory default setting is 0.0.0.0, which means no secondary DNS is assigned.
MTU Size	Specify the MTU size. The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. This number should be an integer between 576 and 2026.
IGMP Proxy	Enable or disable IGMP (Internet Group Management Protocol) Proxy. IGMP proxy is used to process the multicast stream in the netwok. It normally works for IPTV service.
DHCP Server	Enable or disable the DHCP server function. With this function enabled, the build-in DHCP server will assign IP address to the clients connected to the device.
Start IP Address	Specify the first IP address of the IP address pool. By default, it is 192.168.0.100.
End IP Address	Specify the last IP address of the IP address pool. By default, it is 192.168.0.199.
Default Gateway	Specify the gateway IP address for the LAN network. By default, it is 192.168.0.254.
Default Domain	(Optional) Specify the domain name for the DHCP server.
Primary DNS	Enter the DNS IP address for the LAN. By default, it is 0.0.0.0, which means no primary DNS is assigned.

Secondary DNS	Enter the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0, which means no secondary DNS is assigned.
Lease Time	Enter the amount time of the leased IP address assigned by the DHCP server. When the time expires, the clients will request to renew the lease automatically.
Address Reservation	Enable Address Reservation and specify a reserved IP address for a PC on the local area network, so the PC will always obtain the same IP address each time when it starts up. Reserved IP addresses could be assigned to servers that require permanent IP settings.  To configure Address Reservation: Click *Add*, specify the MAC address and the IP address. Enable this entry, then click *Save*.
IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a LAN IPv6 address. Select a method for the device to obtain the LAN IPv6 address according to the information provided by your ISP. • **Static** Select static and enter the LAN IPv6 address and IPv6 netmask.  • **SLAAC** Select SLAAC and the device will obtain the LAN IPv6 address automatically.  • **DHCPv6** Select DHCPv6 and the device will obtain the LAN IPv6 address automatically. 

Dynamic



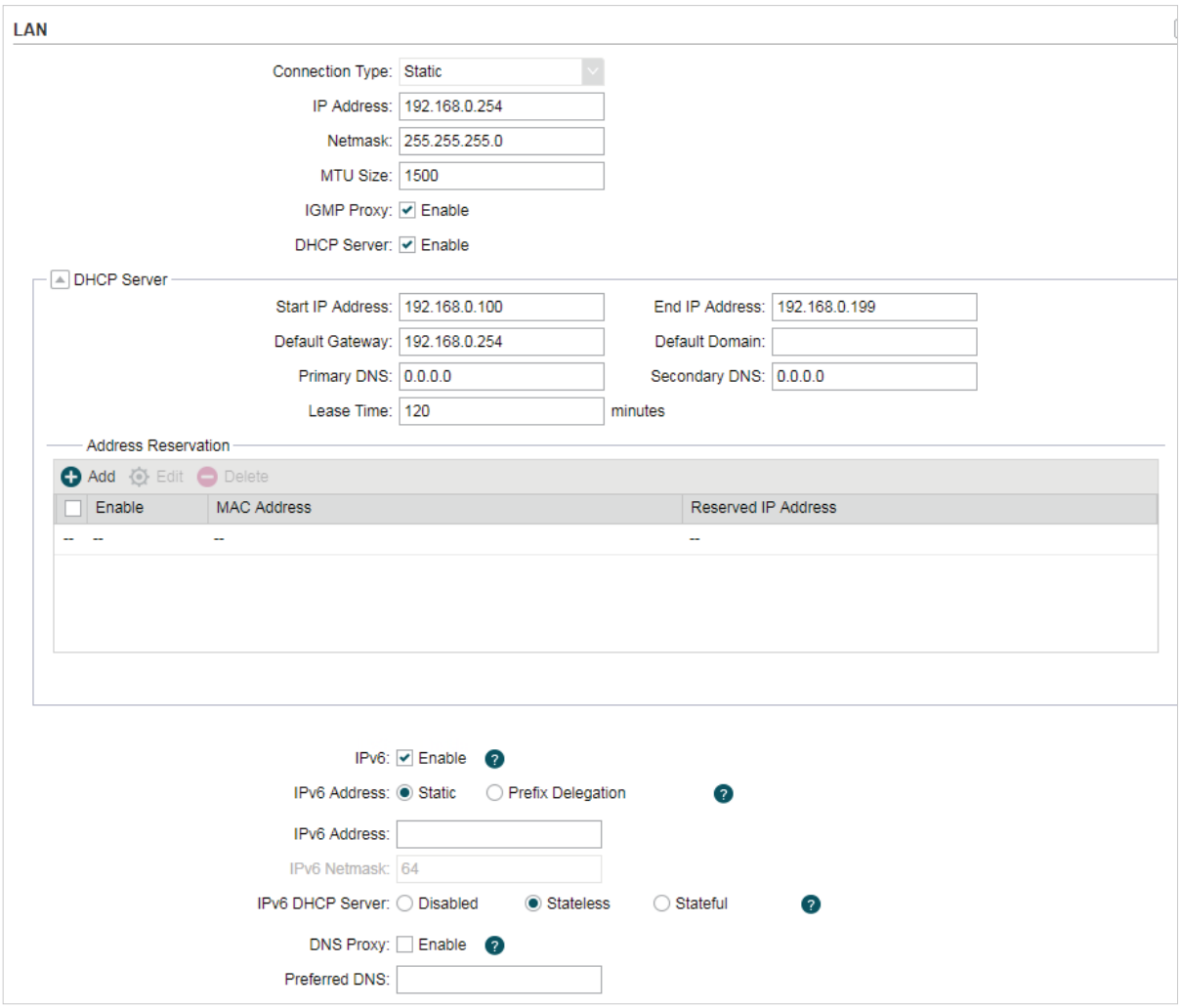
Fallback IP	Enable or disable the Fallback IP. When the device fails to find the DHCP server, it will use the fallback IP as the LAN IP address.
DHCP Fallback IP	Specify the fallback IP for the device. By default, it is 192.168.0.254.
DHCP Fallback Mask	Specify the fallback netmask for the device.
Primary DNS	Enter the DNS IP address for the LAN. By default, it is 0.0.0.0, which means no primary DNS is assigned.
Secondary DNS	Enter the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0, which means no secondary DNS is assigned.
MTU Size	Specify the MTU size. The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. This number should be an integer between 576 and 2026.
IGMP Proxy	Enable or disable IGMP (Internet Group Management Protocol) Proxy. IGMP proxy is used to process the multicast stream in the network. It normally works for IPTV service.

IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a LAN IPv6 address. Select a method for the device to obtain the LAN IPv6 address according to the information provided by your ISP. • **Static** Select static and enter the LAN IPv6 address and IPv6 netmask.  • **SLAAC** Select SLAAC and the device will obtain the LAN IPv6 address automatically.  • **DHCPv6** Select DHCPv6 and the device will obtain the LAN IPv6 address automatically. 

2. Click *Apply*, then click *Save*.

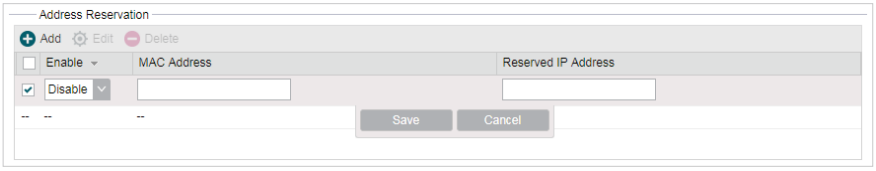
AP Router/AP Client Router Mode

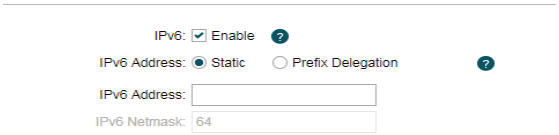
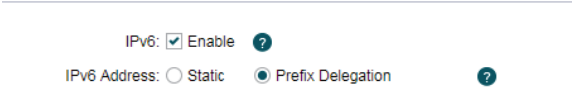
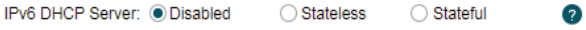
Go to the **Network** page. In the **LAN** section, configure the following parameters.



1. For LAN connection type, the device only supports Static.

IP address	Enter the LAN IP address of your device. By default, it is 192.168.0.254. **Note:** When you change the LAN IP address in the **Network** tab, you should log in with the new IP address and save the settings for the configuration change to take effect. Otherwise the configuration will be lost after the reboot.
Netmask	Enter the Netmask provided by your ISP. Normally use 255.255.255.0.
MTU Size	Specify the MTU size. The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. This number should be an integer between 576 and 2026.

IGMP Proxy	Enable or disable IGMP (Internet Group Management Protocol) Proxy. IGMP proxy is used to process the multicast stream in the netwok. It normally works for IPTV service.
DHCP Server	Enable or disable the DHCP server function. With this function enabled, the build-in DHCP server will assign IP address to the clients connected to the device.
Start IP Address	Specify the first IP address of the IP address pool. By default, it is 192.168.0.100.
End IP Address	Specify the last IP address of the IP address pool. By default, it is 192.168.0.199.
Default Gateway	Specify the gateway IP address for the LAN network. By default, it is 192.168.0.254.
Default Domain	(Optional) Specify the domain name for the DHCP server.
Primary DNS	Enter the DNS IP address for the LAN. By default, it is 0.0.0.0, which means no primary DNS is assigned.
Secondary DNS	Enter the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0, which means no secondary DNS is assigned.
Lease Time	Enter the amount time of the leased IP address assigned by the DHCP server. When the time expires, the clients will request to renew the lease automatically.
Address Reservation	Enable Address Reservation and specify a reserved IP address for a PC on the local area network, so the PC will always obtain the same IP address each time when it starts up. Reserved IP addresses could be assigned to servers that require permanent IP settings.  To configure Address Reservation: Click *Add*, specify the MAC address and the IP address. Enable this entry, then click *Save*.

IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a LAN IPv6 address. Select a method for the device to obtain the LAN IPv6 address according to the information provided by your ISP. • **Static** Select static and enter the LAN IPv6 address and IPv6 netmask.  • **Prefix Delegation** Select Prefix Delegation and the device will obtain the LAN IPv6 address automatically. 
IPv6 DHCP Server	Enable or disable the IPv6 DHCP server function. With IPv6 DHCP server enabled, the clients will obtain the IPv6 address from the DHCP server. • **Disabled** Select Disabled to disable the IPv6 DHCP server function  • **Stateless/Stateful** Select Stateless or Stateful, and the clients will obtain the IPv6 address from the IPv6 DHCP server automatically. Enable or disable the DNS proxy. With this feature enabled, the device will obtain the DNS server automatically. With this feature disabled, you should specify the DNS address manually. 

2. Click *Apply*, then click *Save*.

4.3 Configure Management VLAN

Management VLAN provides a safer way for you to manage the device. With Management VLAN enabled, only the hosts in the management VLAN can manage the device. Since most hosts cannot process VLAN tags, connect the management host to the network via a switch, and set up correct VLAN settings to ensure the communication between the host and the device in the management VLAN.

Go to the **Network** page. In the **Management VLAN Interfaces** section, enable the Management VLAN function, specify *VLAN ID* and click *Apply*. Then click *Save*.



Management VLAN	Enable or disable the Management VLAN function. By default, it is disabled.
VLAN ID	Specify the Management VLAN ID. The valid values are from 2 to 4094.

4.4 Configure the Forwarding Feature

Note:

Forwarding submenu is only available in AP Router Mode and AP Client Router (WISP Client) Mode.

The IP address used on the internet is public IP address, while IP address used on local area network is private IP address. The hosts using private IP addresses cannot access the internet directly and vice versa.

The hosts using private IP addresses visit internet through NAT (Network Address Translation) technology. NAT can transfer private IP addresses into public IP addresses to realize the communication from internal hosts to external hosts.

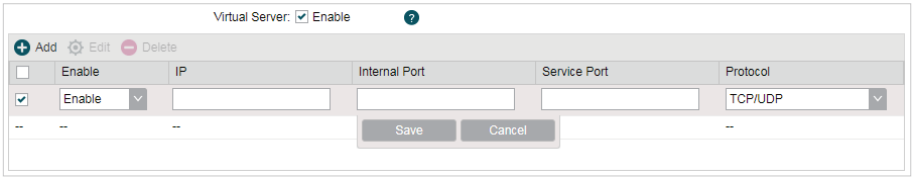
If the hosts on the internet want to visit the hosts on local area network, the forwarding function should be used, including DMZ, Virtual server, Port triggering and UPnP.

Go to the **Network** page. In the **Forwarding** section, configure the following parameters and click *Apply*. Then click *Save*.



DMZ	Enable or disable the DMZ function. DMZ (Demilitarized Zone) specifically allows one computer/device behind NAT to become “demilitarized”, so all packets from the external network are forwarded to this computer/device. The demilitarized host is exposed to the wide area network, which can realize the unlimited bidirectional communication between internal hosts and external hosts.
DMZ IP	Specify the IP address of the local host network device. The DMZ host device will be completely exposed to the external network. Any PC that was used for a DMZ must have a static or reserved IP Address because its IP Address may change when using the DHCP function.
ALG	Select the type of ALG to enable the corresponding feature. Common NAT only translates the address of packets at network layer and the port number at transport layer but cannot deal with the packets with embedded source/destination information in the application layer. Application layer gateway (ALG) can deal with protocols with embedded source/destination information in the application payload. Some protocols such as FTP, TFTP, H323 and RTSP require ALG (Application Layer Gateway) support to pass through NAT. **FTP ALG:** Allows FTP clients and servers to transfer data across NAT. **TFTP ALG:** Allows TFTP clients and servers to transfer data across NAT. **H323 ALG:** Allows Microsoft NetMeeting clients to communicate across NAT. **RTSP ALG:** Allows some media player clients to communicate with some streaming media servers across NAT.

Virtual Server	Enable or disable Virtual Server. Virtual servers can be used for setting up public services on your local area network, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the internet to this service port will be redirected to the LAN server. Virtual Server function not only makes the users from internet visit the local area network, but also keeps network security within the intranet as other services are still invisible from internet. The LAN server must have a static or reserved IP Address because its IP Address may change when using the DHCP function.



To configure Virtual Server:

Click *Add*, specify the following parameters and *Enable* the entry. Click *Save*.

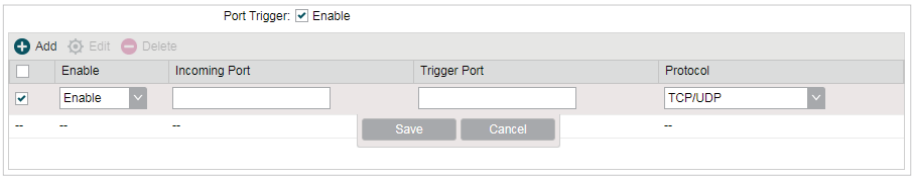
IP: Enter the IP Address of the PC providing the service application.

Internal Port: Enter the Internal Port number of the PC running the service application. You can leave it blank if the Internal Port is the same as the Service Port, or enter a specific port number.

Service Port: Enter the numbers of external Service Port. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is the start port, YYY is the end port). Internet users send request to the port for services.

Protocol: Choose the one of the protocols used for this application: TCP, UDP, or TCP/UDP.

Port Trigger	Enable or disable port trigger. Due to the existence of the firewall, some applications such as online games, video conferences, VoIPs and P2P downloads need the device to configure the forwarding to work properly, and these applications require multiple ports connection, for single-port virtual server cannot meet the demand. Port trigger function comes at this time. When an application initiates a connection to the trigger port, all the incoming ports will open for subsequent connections.



To configure port trigger:

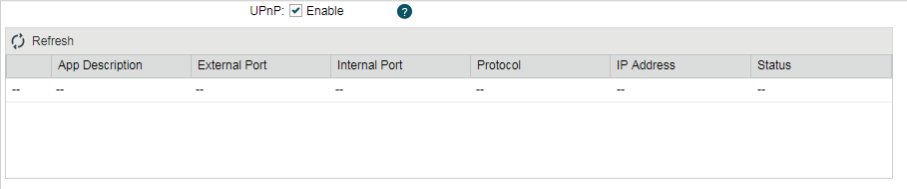
Click *Add*, specify the following parameters and *Enable* the entry. Click *Save*.

Incoming Port: Enter the incoming port for incoming traffic. The port or port range is used by the remote system when it responds to the outgoing request. A response to one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.

Trigger Port: Enter the trigger port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.

Protocol: Choose the one of the protocols used for this application: TCP, UDP, or TCP/UDP.

UPnP	Enable or disable UPnP. If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance (a feature in Windows XP), you should enable the UPnP function. The Universal Plug and Play (UPnP) function allows the devices, such as internet computers, to access the local host resources or devices as needed. Host in the local area network can automatically open the corresponding ports on a router, and make the application of external host access the resources of the internal host through the opened ports. Therefore, the functions limited to the NAT can work properly. Compared to virtual server and port triggering, the application of UPnP doesn't need manual settings. It is more convenient for some applications required unfixed ports.



App Description: Displays the description provided by the application in the UPnP request.

External Port: Displays the external port number that the router opened for the service application.

Internal Port: Displays the internal service port number of the local host running the service application.

Protocol: Displays which type of protocol is opened.

IP Address: Displays the IP address of the local host which initiates the UPnP request.

Status: Enabled means that port is still active. Otherwise, the port is inactive.

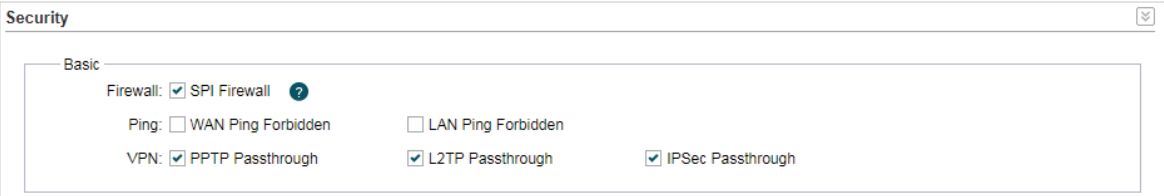
4.5 Configure the Security Feature

Note:

Security submenu is only available in AP Router Mode and AP Client Router (WISP Client) Mode.

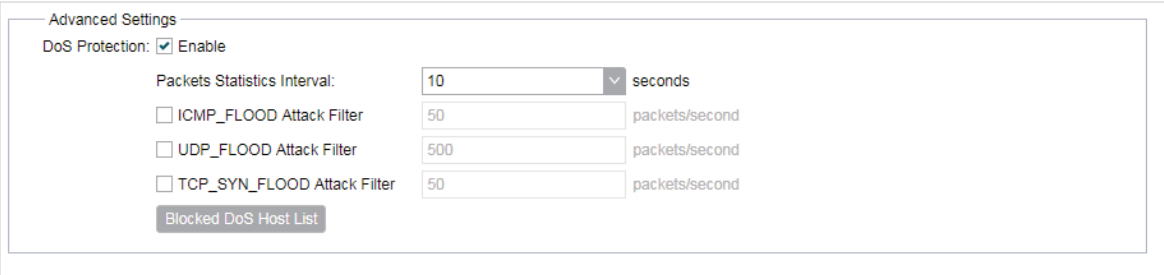
Stateful Packet Inspection (SPI) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed to pass through by the firewall and others will be rejected. SPI Firewall is enabled by factory default.

1. Go to the **Network** page. In the **Security > Basic** section, configure the following parameters and click *Apply*.



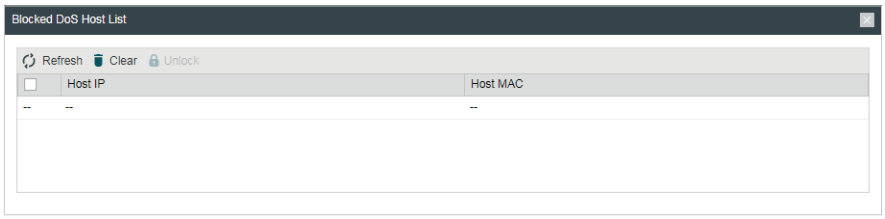
SPI Firewall	Check the Enable box to use the SPI Firewall function. If forwarding rules are enabled at the same time, the device will give priority to meet forwarding rules.
Ping	Select and enable the ping forbidden function. **WAN Ping Forbidden:** Enable or disable this function. With this option enabled, the device will not reply the ping request originates from internet. By default, it is disabled. **LAN Ping Forbidden:** Enable or disable this function. With this option enabled, the device will not reply the ping request originates from local network.
VPN	Select and enable the VPN function. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions. Through VPN you can access your private network over internet. A virtual private network connection across the internet is similar to a wide area network (WAN) link between sites. From a user perspective, the extended network resources are accessed in the same way as resources available within the private network. When hosts in the local area network want to visit the remote virtual private network using virtual tunneling protocols, the corresponding VPN protocol should be enabled. **PPTP Passthrough:** PPTP (Point-to-Point Tunneling Protocol) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP (Internet Protocol) network. Check the box to allow PPTP tunnels to pass through the Device. **L2TP Passthrough:** L2TP (Layer Two Tunneling Protocol) is the method used to enable Point-to-Point connections via the internet on the Layer Two level. Check the box to allow L2TP tunnels to pass through the Device. **IPSec Passthrough:** IPSec (Internet Protocol Security) is a suite of protocols for ensuring private, secure communications over IP (Internet Protocol) networks, through the use of cryptographic security services. Check the box to allow IPSec tunnels to pass through the Device.

2. In the **Security > Advanced Settings** section, configure the following parameters and click *Apply*.



DoS Protection	Enable the DoS Protection and specify the parameters. DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host, which incurs an abnormal service or even breakdown of the network. With DoS Protection function enabled, the device can analyze the specific fields of the IP packets and distinguish the malicious DoS attack packets. Upon detecting the packets, the device will discard the illegal packets directly and limit the transmission rate of the legal packets if the over legal packets may incur a breakdown of the network. The hosts sending these packets will be added into the *Blocked DoS Host* List. The device can defend a few types of DoS attack such as ICMP_FLOOD, UDP_FLOOD and TCP_SYN_FLOOD. **Packets Statistics Interval:** Select a value between 5 and 60 seconds from the drop-down list. The default value is 10. The value indicates the time interval of the packets statistics. The result of the statistic is used for analysis by ICMP-Flood, UDP Flood and TCP-SYN Flood. **ICMP_FLOOD Attack Filter:** Enter a value between 5 and 3600. The default value is 50. When the current ICMP-FLOOD Packets number is beyond the set value, the device will start up the blocking function immediately. **UDP_FLOOD Attack Filter:** Enter a value between 5 and 3600. The default value is 500. When the current UPD-FLOOD Packets number is beyond the set value, the device will start up the blocking function immediately. **TCP_SYN_FLOOD Attack Filter:** Enter a value between 5 and 3600. The default value is 50. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Device will start up the blocking function immediately.

Blocked DoS Host List	Click *Blocked DoS Host List* to display the blocked DoS host table including host IP and host MAC. Click *Refresh* to renewal the table list. Click *Clear* to release all the blocked hosts. If you want to release one or some of the blocked hosts, select them and Click *Unlock*.



3. Click *Save*.

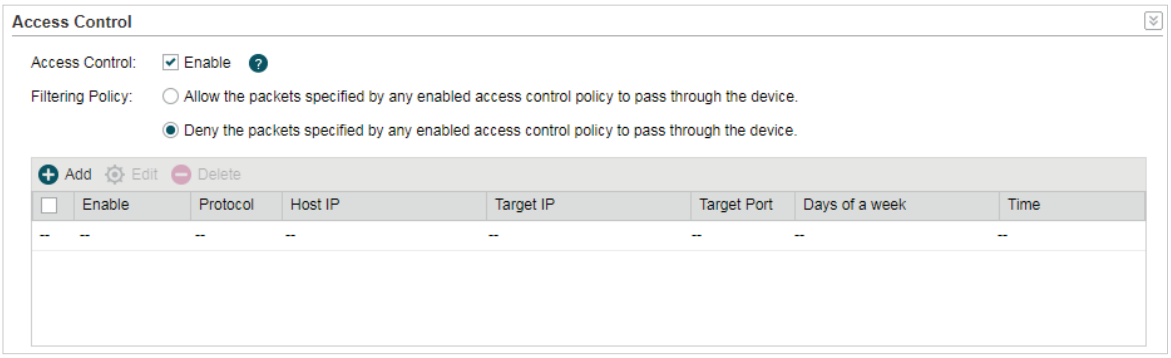
4.6 Configure Access Control

Note:

Access Control submenu is only available in AP Router Mode and AP Client Router (WISP Client) Mode.

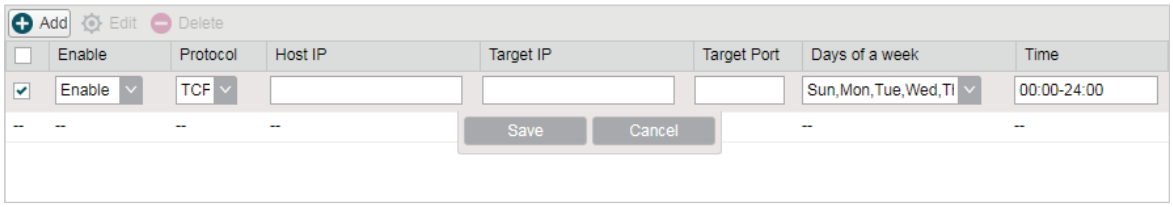
The function can be used to control the internet activities of hosts in the local area network. For example, the online time limit and the specified web stations to visit can be controlled by the filtering policy.

1. Go to the **Network** page. In the **Access Control** section, enable Access Control and select the Filtering Policy.



Access Control	Enable or disable Access Control.
Filtering Policy	Select the filtering policy according to your need. **Allow the packets specified by any enabled access control policy to pass through the Device:** The hosts listed below are allowed to access the internet under the rules. While others are forbidden to access. **Deny the packets specified by any enabled access control policy to pass through the Device:** The hosts listed below are forbidden to access the internet under the rules. While others are allowed to access.

2. Click *Add* and create the filtering entries.



Enable	Enable or disable the desired entry.
Protocol	Choose one of the protocols from the drop-down list used for the target, any of IP, TCP, UDP, or ICMP.
Host IP	Enter the IP address or address range of the hosts that you need to control, for example 192.168.0.12-192.168.0.25.
Target IP	Enter the IP address or address range of the targets that you need to control, for example 192.168.3.12-192.168.3.25.
Target Port	Specify the port or port range for the target when protocol is TCP or UDP.
Days of a week	Specify the days in which the rules take effect.
Time	Enter the time rule in HH:MM-HH:MM format, the default value is 00:00-24:00.

3. Click *Save* and click *Apply*, then click *Save*.

4.7 Configure Static Routing

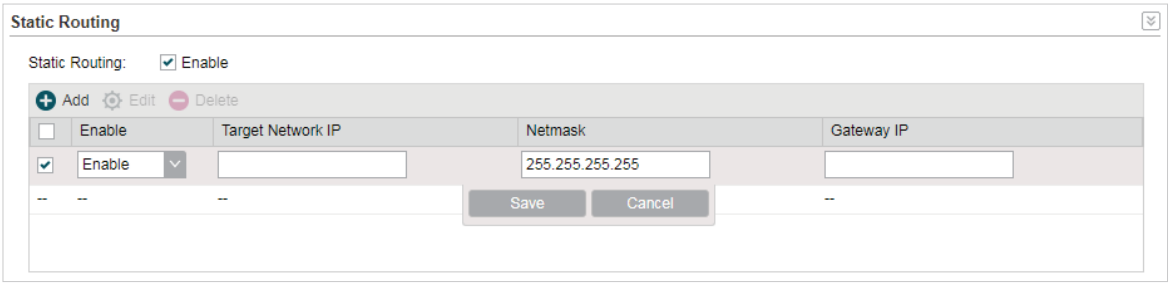
Note:

Static Routing submenu is only available in AP Router Mode and AP Client Router (WISP Client) Mode.

A static route is a pre-determined path that network information must travel to reach a specific host or network. If static route is used properly in the network, it can decrease the network overhead and improve the speed of forwarding packets.

Static routing is generally suitable for simple network environment, in which users clearly understand the topology of the network so as to set the routing information correctly. When the network topology is complicated and users are not so familiar with the topology structure, this function should be used with caution or under the guidance of the experienced administrator.

1. Go to the **Network** page. In the **Static Routing** section, click *Add* and specify the following parameters.



Enable	Enable or disable the desired entry.
Target Network IP	Enter the Target Network IP, the address of the network or host to be visited. The IP address cannot be on the same network segment with the device's WAN or LAN port.
Netmask	Specify the netmask for the desired entry.
Gateway IP	Enter the Gateway IP, the address of the gateway that allows for contact between the Device and the network or host

2. Click *Save* and click *Apply*, then click *Save*.

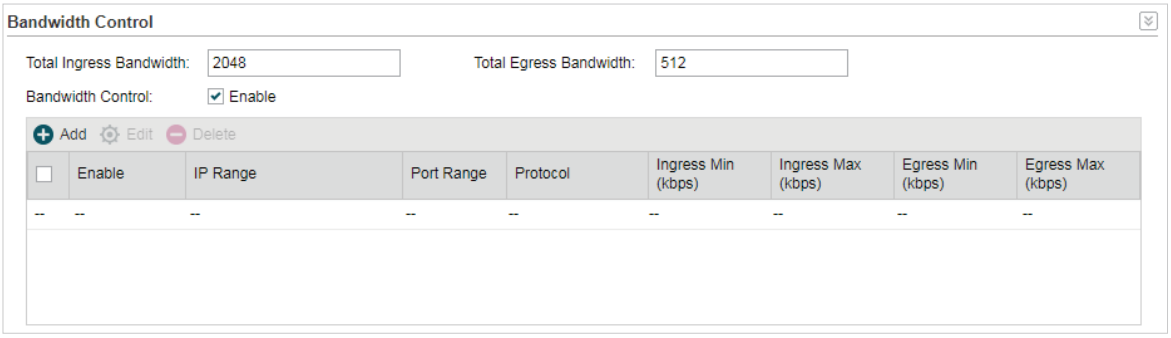
4.8 Configure Bandwidth Control

Note:

Bandwidth Control submenu is only available in AP Router Mode and AP Client Router (WISP Client) Mode.

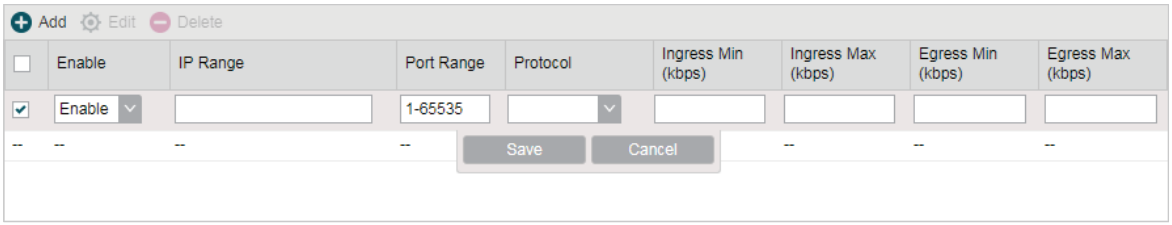
Bandwidth control function is used to control the internet bandwidth in the local area network. In the case of insufficient bandwidth resources, enable the function to make the device allocate reasonable bandwidth to the clients and achieve the purpose of efficient use of the existing bandwidth. Via IP bandwidth control function, set the upper and lower limit in the bandwidth of the computer network and guarantee a smooth sharing network.

1. Go to the **Network** page. In the **Bandwidth Control** section, enable the Bandwidth Control function.



Total Ingress Bandwidth	Specify the upper bandwidth for receiving packets from the WAN port. The maximum value is 100,000kbps.
Total Egress Bandwidth	Specify the upper bandwidth for sending packets from the WAN port. The maximum value is 100,000kbps.

2. Click *Add* and specify the following parameters.



Enable	Enable or disable the desired entry.
IP Range	Enter the IP Range of the target hosts which need to be controlled of bandwidth, for example 192.168.0.12-192.168.0.25.
Port Range	Enter the Port Range through which the target hosts visit external server, for example 1-63258.
Protocol	Choose one of the protocols used for this application: TCP, UDP, or TCP/UDP.
Ingress Min (kbps)	Specify the minimum ingress bandwidth for the desired entry.
Ingress Max (kbps)	Specify the maximum ingress bandwidth for the desired entry.
Egress Min (kbps)	Specify the minimum egress bandwidth for the desired entry.

Egress Max (kbps)	Specify the maximum egress bandwidth for the desired entry.

3. Click *Save* and click *Apply*, then click *Save*.

4.9 Configure IP & MAC Binding

We can effectively prevent ARP attack and IP embezzlement by enabling the IP&MAC binding. Within the local network, the device transmits IP packets to the certain target identified by the MAC address. Therefore, the IP and MAC address should be one-to-one correspondence and their corresponding relations are maintained by the ARP table. ARP attack can use forged information to renewal the ARP table, and destroy the corresponding relations between IP and MAC addresses, which would prevent the communication between the device and the corresponding host. When the IP&MAC Binding function is enabled, the IP and MAC relations in the ARP table won't be expired and renewed automatically, which effectively prevents the ARP attack.

Some functions such as access control and bandwidth control, are based on the IP addresses to identify the access clients. The network administrator can allocate every client a static IP, according to which he makes the access and bandwidth rules to control the clients' online behavior and the bandwidth they've used. Some illegal users may change the IP address in order to get higher internet access. Enabling IP & MAC binding function can effectively prevent the IP embezzlement.

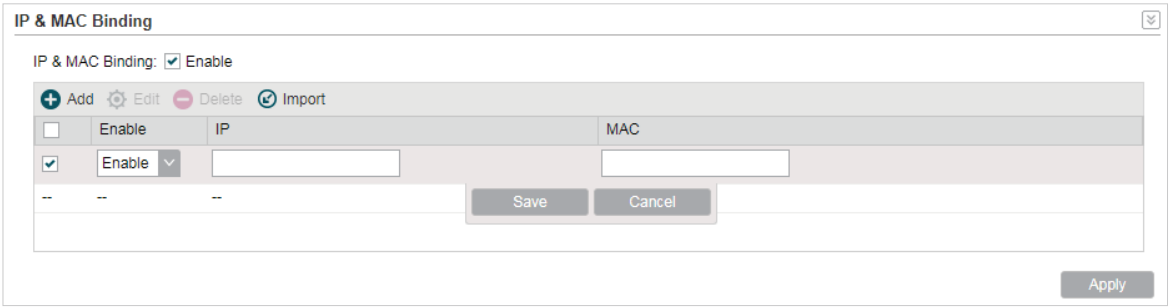
Note:

After IP & MAC binding function is enabled, the IP bound to the MAC cannot be used by other MACs. However this MAC can use other IPs within the same segment, which are not bounded by other MACs, to access the network.

1. Go to the **Network** page. In the **IP & MAC Binding** section, click *Add* and specify the IP address and MAC address.

Note:

Click *Import* to quick import the entries in ARP table to IP & MAC Binding table. The imported entries are disabled by default. Select the desired entries and click *Edit* to enable it.



IP	Enter the IP address that you want to bind with the MAC address.
MAC	Enter the MAC address that you want to bind with the IP address.

2. Enable the desired entry and click *Save*. Click *Apply*, then click *Save*.

5 Configure the Wireless Parameters

This chapter introduces how to configure the parameters of the wireless network, including:

5.1 Configure Basic Wireless Parameters

5.2 Configure Wireless Client Parameters

5.3 Configure Wireless AP Parameters

5.4 Configure Multi-SSID

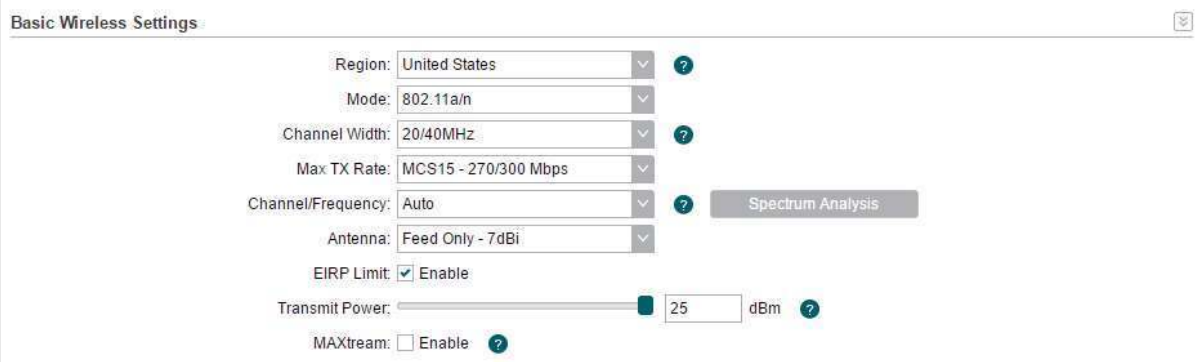
5.5 Configure Wireless MAC Filtering

5.6 Configure Advanced Wireless Parameters

5.1 Configure Basic Wireless Parameters

This section allows you to configure wireless basic parameters, such as 802.11 mode, Transmit Power, and data rates.

Go to the **Wireless** Page. In the **Basic Wireless Settings** section, configure the basic wireless settings and click *Apply*. Then click *Save*.



Region	Specify the region where you use the device. Available channels and maximum Transmit Power will be determined by the selected region according to the local laws and regulations.
Mode	Select the protocol standard used in the wireless network. To check what protocol standards your device supports, refer to the actual web interface. Certain devices have a frequency band of 2.4GHz, supporting 802.11b, 802.11g, 802.11n, 802.11b/g, and 802.11b/g/n modes. We recommend that you set the mode as 802.11b/g/n, allowing all 802.11b, 802.11g and 802.11n wireless stations to access the device. Certain devices have a frequency band of 5GHz, supporting 802.11a, 802.11n, and 802.11a/n modes. We recommend that you set the mode as 802.11a/n, allowing both 802.11a and 802.11n wireless stations to access the device. Certain devices have a frequency band of 5GHz, supporting 802.11ac, 802.11n/ac, and 802.11a/n/ac modes. We recommend that you set the mode as 802.11a/n/ac, allowing all 802.11a, 802.11n, and 802.11ac wireless stations to access the device.

Channel Width	Select the channel width of this device. To check what channel width your device supports, refer to the actual web interface. For certain devices, options include 5 MHz, 10 MHz, 20 MHz, 40 MHz and 20/40 MHz (the device automatically selects 40 MHz, and 20 MHz will be used if 40 MHz is not available). For certain devices, options include 20 MHz, 40 MHz, 80 MHz and 20/40/80 MHz (the device automatically selects 80 MHz, and 40 MHz will be used if 80 MHz is not available, and so on). According to IEEE 802.11n standard, using a wider channel can increase wireless throughput. However, you may need to choose lower bandwidth due to the following reasons: • To increase the available number of channels within the limited total bandwidth. • To avoid interference from overlapping channels occupied by other devices in the environment. • Lower bandwidth can concentrate higher transmit power, increasing stability of wireless links over long distances. • In Client / AP Client Router / Repeater / Bridge Mode, the device should have the same channel width as the root AP. • In Access Point / AP Router / Repeater / Bridge Mode, select the channel width which your clients support.
Max TX Rate	Set the maximum transmit data rate.
Channel/ Frequency	Select appropriate channel used by this device to improve wireless performance. 1/2412 MHz refers to Channel 1 and the frequency is 2412 MHz. This setting is only available in Access Point Mode and AP Router Mode. We highly recommend that you use the *Spectrum Analysis* tool to select a proper channel.
Antenna	Select your antenna from the list.
Antenna Gain	Antenna Gain is only available in WBS products. Enter the antenna gain value according to the antennas and the value ranges from 0 to 30dBi. It can work together with the transmit power to improve the transmit signal quality. 
EIRP Limit	This option should remain enabled. With EIRP Limit enabled, the transmit power is restricted so that the EIRP (Effecitive Isotropic Radiated Power) of the device is kept below the amount which is allowed in the selected region.

Channel Shifting	**Note:** Channel Shifting is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Enable or disable the Channel Shifting function. This function is only available when MAXtream is enabled in Access Point Mode and AP Router Mode. Channel Shifting is a TP-Link proprietary technology. With Channel Shifting enabled, the AP will use non-standard channels by adding a frequency offset to the standard 802.11 b/g/n channels. Your network can then only be detected by the wireless devices with Channel Shifting enabled and so is less likely to be detected by other wireless networks, which benefits network security.
Transmit Power	**Note:** In most scenarios, it is unnecessary to select the maximum transmit power. Selecting larger transmit power than your need may cause interference to neighborhood. Also it consumes more power and will reduce longevity of the device. Select appropriate transmit power to achieve the best performance. Use the *Speed Test* tool to find the best performance. Specify the transmit power of the device. Use the slider or manually enter the transmit power value. For Outdoor Wireless Base Stations, the maximum transmit power varies according to the antenna gain value.
MAXtream	**Note:** • MAXtream is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. • MAXtream Technology is only compatible with Pharos series products. Working with products from other manufacturer will cause network fault. Enable or disable the MAXtream function. This function is only available in Access Point Mode and AP Router Mode. MAXtream is a TP-Link proprietary technology. It is based on TDMA (Time Division Multiple Access) so that data streams are transmitted in their own time slots. MAXtream aims to maximize throughput and minimize latency. “Hidden nodes” problem can also be eliminated with MAXtream enabled.

MAXtream Station Mode	**Note:** MAXtream is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. MAXtream Station Mode is available in Client Mode, Bridge Mode and AP Client Router Mode with the wireless AP settings disabled. **Auto Adjust:** The device will choose the MAXtream Station Mode automatically. **Latency First:** Set the MAXtream Station Mode as Latency First and the time sensitive stream such as VoIP will take precedence in MAXtream system. **Throughput First:** Set the MAXtream Station Mode as Throughput First and the stream that needs high throughput such as online games will take precedence in MAXtream system.

5.2 Configure Wireless Client Parameters

Note:

Wireless Client Settings submenu is only available in Client, Repeater, Bridge and AP Client Router (WISP Client) Mode.

In this section, configure wireless client parameters used for the connection with the root AP.



1. Go to the **Wireless** Page. In the **Wireless Client Settings** section, configure the following parameters.

SSID of AP	Specify the SSID of the root AP. You can enter the SSID of the specific AP manually, or directly survey all the APs around by clicking *Survey* and select one.
MAC of AP	Displays the MAC address of the root AP. It's possible that two or more networks use the same SSID in the AP list. Enable **Lock to AP** to select SSID and AP simultaneously, which can make the device connect to the specific AP you had connected before the next time.

WDS	Displays the status of the WDS (Wireless distribution System) function. WDS is a communication system among multiple wireless networks . It is established between APs through wireless connection. WDS is used to during the connection between the device and the root AP. **Enable:** Forward data frames to use four address fields. **Disable:** Forward data frames to use three address fields. **Auto:** The device automatically negotiates the wireless data frame structure (three or four address fields) with the root AP. The selection of Auto is recommended.

2. Specify the security mode. Make sure the security mode and the related parameters are the same as the upstream wireless network's.

■ None

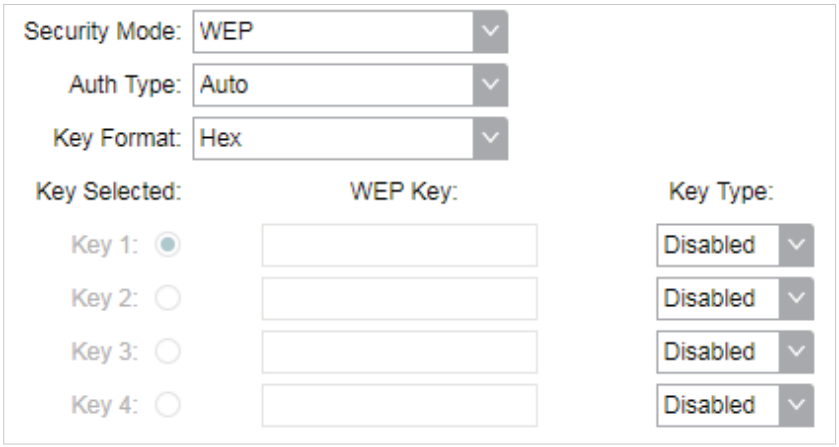
Select this option if the root AP has no encryption. When connecting to the root AP, it's no need to enter a password to access the wireless network.

■ WEP

Note:

- WEP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.
- WEP is not supported in 802.11n mode or 802.11ac mode. If WEP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network. If WEP is applied in 802.11b/g/n mode (2.4GHz) or 802.11a/n (5GHz), the device may work at a low transmission rate.

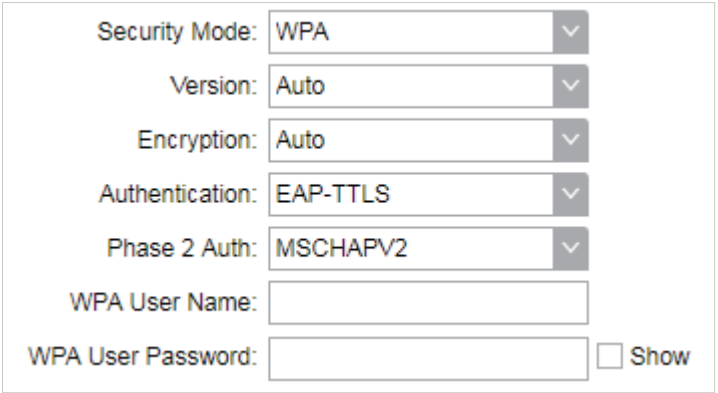
WEP (Wired Equivalent Privacy) is a traditional encryption method. It has been proved that WEP has security flaws and can easily be cracked, so WEP is rarely used in normal wireless network. Select this option if the security mode of the root AP is WEP.



Auth Type	Select the authentication type for WEP. **Auto:** The device can select Open System or Shared Key automatically according to the wireless network of the root AP. **Open System:** The device can pass the authentication and associate with the root wireless network without password. However, correct password is necessary for data transmission. **Shared Key:** The device needs the correct password to pass the authentication, otherwise the device cannot associate with the root wireless network or transmit data.
Key Format	Select ASCII or Hex as the WEP key format. **ASCII:** With this format selected, the WEP key can be any combination of keyboard characters of the specified length. **Hex:** With this format selected, the WEP key can be any combination of hexadecimal digits (0-9, a-f, A-F) with the specified length.
Key Selected	Select one key to specify. You can configure four keys at most.
WEP Key	Enter the WEP keys. The length and valid characters are determined by the key format and key type.
Key Type	Select the WEP key length for encryption. **64Bit:** Enter 10 hexadecimal digits or 5 ASCII characters. **128Bit:** Enter 26 hexadecimal digits or 13 ASCII characters. **152Bit:** Enter 32 hexadecimal digits or 16 ASCII characters.

■ WPA

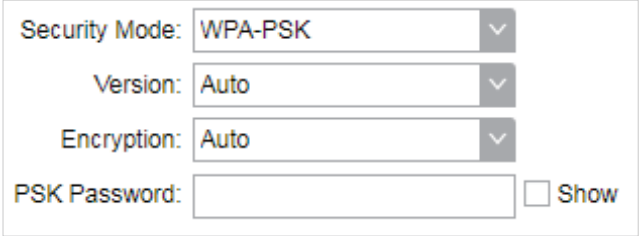
WPA (Wi-Fi Protected Access) is a safer encryption method compared with WEP and WAP-PSK. It requires a RADIUS server to authenticate the clients via 802.1X and EAP (Extensible Authentication Protocol). WPA can generate different passwords for different clients, which ensures higher network security. But it also costs more to maintain the network, so it is more suitable for business networks.



Version	Select the version of WPA. **Auto:** The device will automatically choose the version used by the root AP. **WPA/WPA2:** They're two versions of WPA security mode. WPA2 is an update of WPA. Compared with WPA, WPA2 introduces AES algorithm and CCMP encryption. Theoretically, WPA2 is securer than WPA.
Encryption	**Note:** TKIP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the Encryption type. **Auto:** The default setting is Auto and the device will select TKIP or AES automatically according to the wireless network of root AP. **TKIP:** Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the device may not be able to access the root wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES:** Advanced Encryption Standard. It is securer than TKIP.
Authentication	Select the type of the authentication.
Phase 2 Auth	Select the type of Phase 2 Auth. The device only supports MSCHAPV2 currently.
WPA User Name	Specify the WPA User Name used in the connection with the root AP.
WPA User Password	Specify the WPA User Password used in the connection with the root AP.

■ WPA-PSK

WPA-PSK (Wi-Fi Protected Access-PSK) is based on a pre-shared key. It is characterized by high safety and simple settings, so it is mostly used by common households and small businesses.



Version	**Note:** WPA-PSK/WPA2-PSK is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the version of WPA-PSK. WPA-PSK/WPA2-PSK: They're two versions of WPA-PSK security mode. WPA2-PSK is an update of WPA-PSK. Compared with WPA, Theoretically, WPA2 is securer than WPA. **Auto:** The device will automatically choose the version used by the root AP. **WPA/WPA2:** They're two versions of WPA-PSK security mode normally called WPA-PSK/WPA2-PSK. WPA2-PSK is an update of WPA-PSK. Compared with WPA-PSK, theoretically, WPA2-PSK is securer than WPA-PSK.
Encryption	**Note:** TKIP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the Encryption type. **Auto:** The default setting is Auto and the device will select TKIP or AES automatically according to the wireless network of root AP. **TKIP:** Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the device may not be able to access the root wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES:** Advanced Encryption Standard. It is securer than TKIP.
PSK Password	Specify the PSK password used in the connection with the root AP.

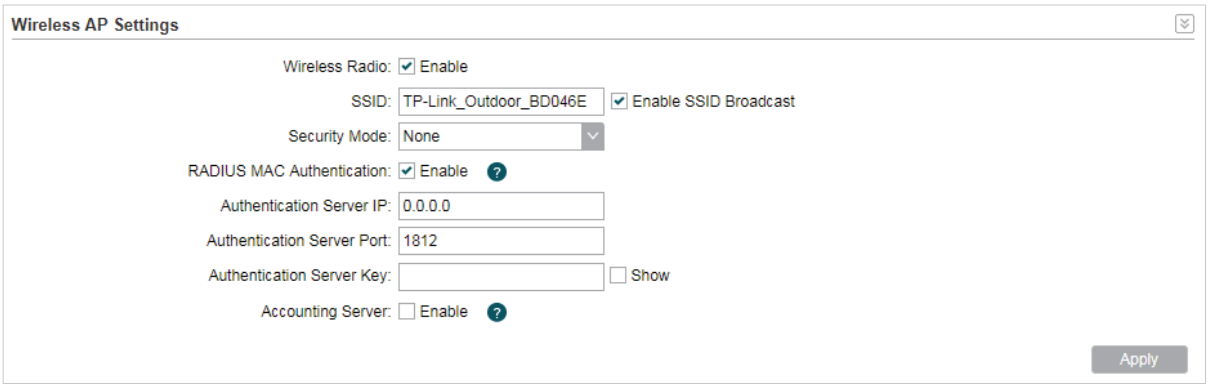
3. Click *Apply*, then click *Save*.

5.3 Configure Wireless AP Parameters

Note:

Wireless AP Settings submenu is only available in Access Point, Bridge, AP Router and AP Client Router (WISP Client) Mode.

In this section, configure wireless AP parameters used for the connection with the clients.



1. Go to the **Wireless** Page. In the **Wireless AP Settings** section, specify the SSID.

Enable SSID Broadcast	Enable or disable SSID broadcast. With this function enabled, the device will broadcast the SSID periodically.

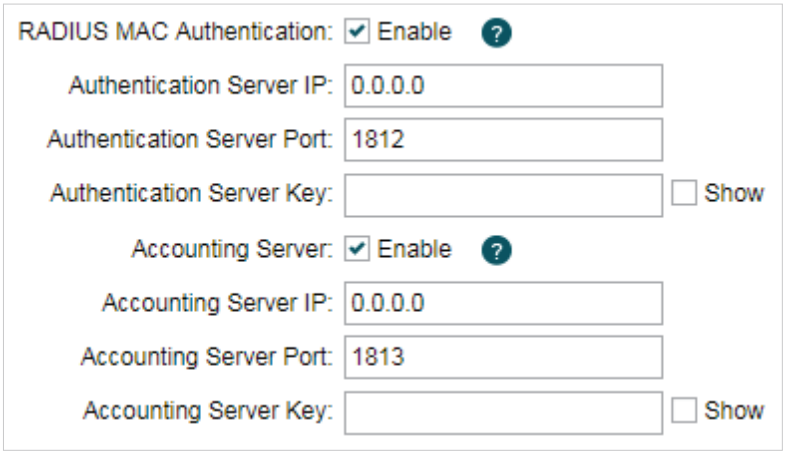
2. Specify the security mode used for the clients to access the wireless network.

■ None

Select **None** when you want an open network without wireless security. In this mode, network data is not encrypted, but you can still authenticate clients by enabling the RADIUS MAC Authentication function.

Note:

RADIUS MAC Authentication is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.



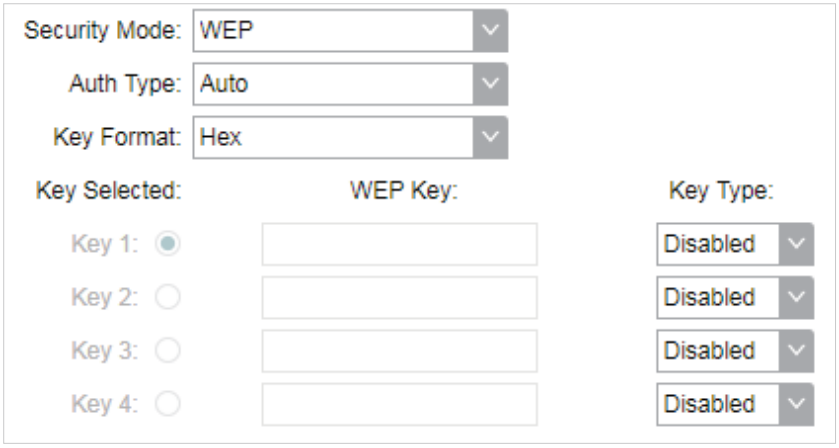
RADIUS MAC Authentication	Enable or disable the Radius MAC authentication. With this feature enabled, you can authenticate clients using their MAC addresses on your RADIUS authentication server. Remember to log into your RADIUS authentication server and create authentication entries whose username and password are both the access-enabled clients' MAC address (for MAC address 11-22-33-AA-BB-CC, create an authentication entry whose username and password are both 112233aabbcc on the RADIUS server).
Authentication Server IP	Enter the IP address of the RADIUS authentication server.
Authentication Server Port	Enter the UDP port of the RADIUS authentication server. The most commonly used port is the default, 1812, but this may vary depending on the RADIUS authentication server you are using.
Authentication Server Key	Enter the shared key used between this device and the authentication server. The shared key is a case-sensitive text string used to validate communication between this device and the RADIUS authentication server. Check the **Show** box to view the shared key characters.
Accounting Server	Enable or disable Accounting Server. With this feature enabled, you can keep accounts on users using a RADIUS accounting server.
Accounting Server IP	Enter the IP address of the RADIUS accounting server.
Accounting Server Port	Enter the UDP port of the RADIUS accounting server. The most commonly used port is 1813, but this may vary depending on the RADIUS accounting server you are using.
Accounting Server Key	Enter the password used between this device and the RADIUS accounting server. The shared key is a case-sensitive text string used to validate communication between this device and the RADIUS accounting server. Check the **Show** box to view the shared key characters.

■ WEP

Note:

- WEP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.
- WEP is not supported in 802.11n mode or 802.11ac mode. If WEP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network. If WEP is applied in 802.11b/g/n mode (2.4GHz) or 802.11a/n (5GHz), the device may work at a low transmission rate.

WEP (Wired Equivalent Privacy) is a traditional encryption method. It has been proved that WEP has security flaws and can easily be cracked, so WEP cannot provide effective protection for wireless networks. Since WPA-PSK and WPA-Enterprise are much safer than WEP, we recommend that you choose WPA-PSK or WPA-Enterprise if your clients also support them.



Auth Type	Select the authentication type for WEP. **Auto:** The device can select Open System or Shared Key automatically based on the wireless capability and request of the clients. **Open System:** Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission. **Shared Key:** Clients have to input the correct password to pass the authentication, otherwise the clients cannot associate with the wireless network or transmit data.
Key Format	Select ASCII or Hex as the WEP key format. **ASCII:** With this format selected, the WEP key can be any combination of keyboard characters of the specified length. **Hex:** With this format selected, the WEP key can be any combination of hexadecimal digits (0-9, a-f, A-F) with the specified length.
Key Selected	Select one key to specify. You can configure four keys at most.

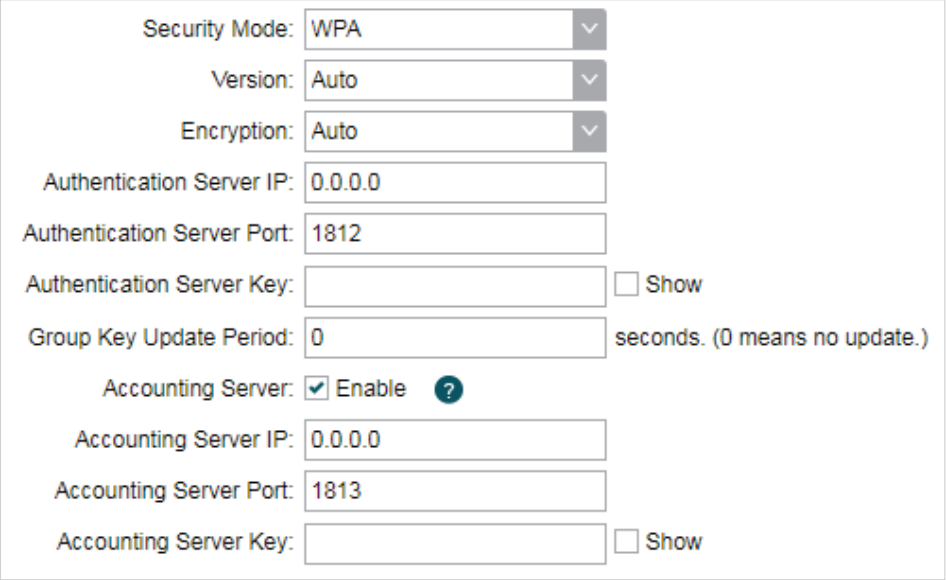
WEP Key	Enter the WEP keys. The length and valid characters are determined by the key format and key type.
Key Type	Select the WEP key length for encryption. **64Bit:** Enter 10 hexadecimal digits or 5 ASCII characters. **128Bit:** Enter 26 hexadecimal digits or 13 ASCII characters. **152Bit:** Enter 32 hexadecimal digits or 16 ASCII characters.

■ WPA

WPA (Wi-Fi Protected Access) is a safer encryption method compared with WEP and WAP-PSK. It requires a RADIUS server to authenticate the clients via 802.1X and EAP (Extensible Authentication Protocol). WPA can generate different passwords for different clients, which ensures higher network security. But it also costs more to maintain the network, so it is more suitable for business networks.

Note:

Accounting Server is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

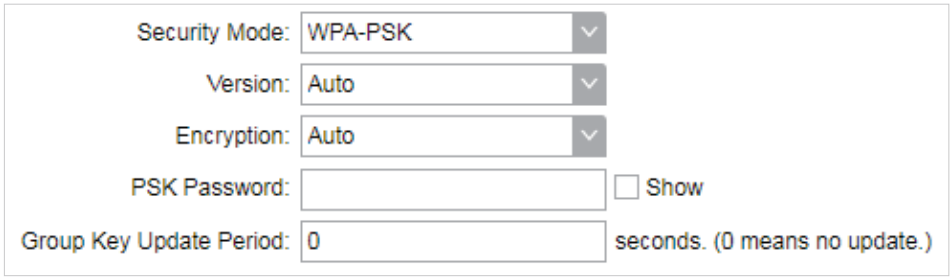


Version	Select the version of WPA. **Auto:** The device will automatically choose the version used by each client device. **WPA/WPA2:** They're two versions of WPA security mode. WPA2 is an update of WPA. Compared with WPA, WPA2 introduces AES algorithm and CCMP encryption. Theoretically, WPA2 is securer than WPA.

Encryption	**Note:** TKIP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the Encryption type. **Auto:** The default setting is Auto and the device will select TKIP or AES automatically based on the client device's request. **TKIP:** Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the device may not be able to access the root wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES:** Advanced Encryption Standard. It is securer than TKIP.
Authentication Server IP	Enter the IP address of the Radius Authentication Server.
Authentication Server Port	Enter the UDP port of the RADIUS authentication server. The most commonly used port is 1812, but this may vary depending on the RADIUS authentication server you are using.
Authentication Server Key	Enter the shared key used between this device and the authentication server. The shared key is a case-sensitive text string used to validate communication between this device and the RADIUS authentication server. Check the **Show** box to view the shared key characters.
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the device should change the encryption key. 0 means that the encryption key does not change at anytime.
Accounting Server	Enable or disable Accounting Server. With this feature enabled, you can keep accounts on users using a RADIUS accounting server.
Accounting Server IP	Enter the IP address of the RADIUS accounting server.
Accounting Server Port	Enter the UDP port of the RADIUS accounting server. The most commonly used port is 1813, but this may vary depending on the RADIUS accounting server you are using.
Accounting Server Key	Enter the password used between this device and the RADIUS accounting server. The shared key is a case-sensitive text string used to validate communication between this device and the RADIUS accounting server. Check the **Show** box to view the shared key characters.

■ WPA-PSK

WPA-PSK (Wi-Fi Protected Access-PSK) is based on a pre-shared key. It is characterized by high safety and simple settings, so it is mostly used by common households and small businesses.



Version	**Note:** WPA-PSK/WPA2-PSK is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the version of WPA-PSK. **WPA-PSK/WPA2-PSK**: They're two versions of WPA-PSK security mode. WPA2-PSK is an update of WPA-PSK. Compared with WPA, theoretically, WPA2 is securer than WPA. **Auto:** The device will automatically choose the version used by the root AP. **WPA/WPA2:** They're two versions of WPA-PSK security mode normally called WPA-PSK/WPA2-PSK. WPA2-PSK is an update of WPA-PSK. Compared with WPA-PSK, theoretically, WPA2-PSK is securer than WPA-PSK.
Encryption	**Note:** TKIP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the Encryption type. **Auto:** The default setting is Auto and the device will select TKIP or AES automatically according to the wireless network of root AP. **TKIP:** Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the device may not be able to access the root wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES:** Advanced Encryption Standard. It is securer than TKIP.
PSK Password	Specify the PSK password used in the connection with the clients.

Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the device should change the encryption key. 0 means that the encryption key does not change at anytime.

3. Click *Apply*, then click *Save*.

5.4 Configure Multi-SSID

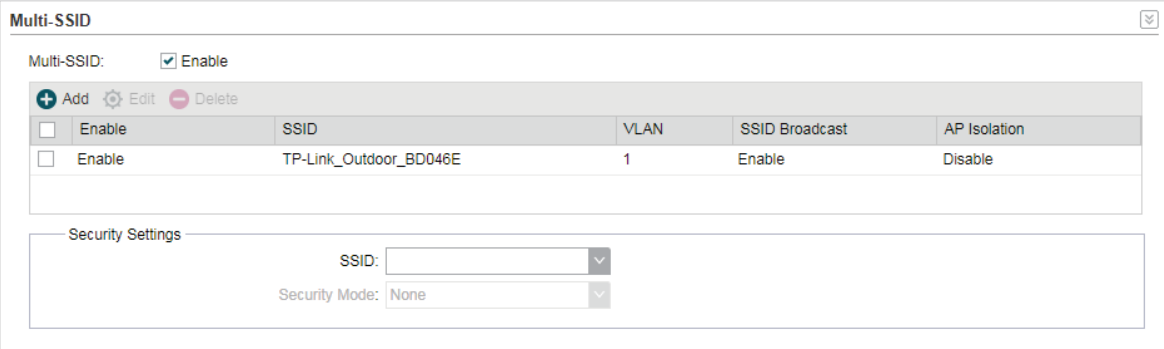
Note:

Multi-SSID submenu is only available in Access Point Mode.

The device can build up to four virtual wireless networks for users to access. When the Multi-SSID function is enabled, the VLAN function is enabled at the same time. It can work together with switches supporting 802.1 Q VLAN and supports maximum four VLANs. The device adds different VLAN tag to the clients which connect to the corresponding wireless network. The clients in different VLANs cannot directly communicate with each other.

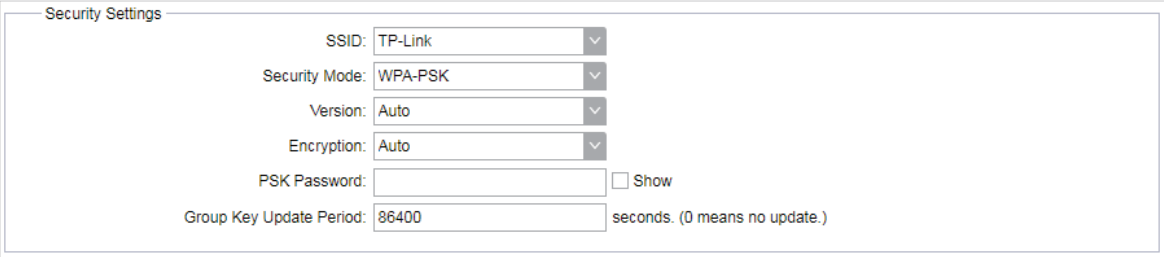
The wired client can communicate with all the wireless clients despite the VLAN settings.

1. Go to the **Wireless** page. In the **Multi-SSID** section, Enable Multi-SSID. Click *Add* and create a new wireless network.



SSID	Specify the SSID of the wireless network.
VLAN	Specify the VLAN to which the new wireless network belongs. The valid value ranges from 1 to 4094.
SSID Broadcast	Enable or disable SSID broadcast . With this feature enabled, the device will broadcast the SSID.
AP Isolation	Enable or disable AP Isolation. With this feature enabled, all the hosts cannot communicate with each other.

2. Select the desired SSID and specify the Security Mode.



SSID	Select the desired SSID to specify the security settings.
Security Mode	Specify the security mode for the desired SSID. The device only supports WPA-PSK.
Version	**Note:** WPA-PSK/WPA2-PSK is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the version of WPA-PSK. WPA-PSK/WPA2-PSK: They're two versions of WPA-PSK security mode. WPA2-PSK is an update of WPA-PSK. Compared with WPA, Theoretically, WPA2 is securer than WPA. **Auto:** The device will automatically choose the version used by the root AP. **WPA/WPA2:** They're two versions of WPA-PSK security mode normally called WPA-PSK/WPA2-PSK. WPA2-PSK is an update of WPA-PSK. Compared with WPA-PSK, theoretically, WPA2-PSK is securer than WPA-PSK.
Encryption	**Note:** TKIP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the Encryption type. **Auto:** The default setting is Auto and the device will select TKIP or AES automatically according to the wireless network of root AP. **TKIP:** Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the device may not be able to access the root wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES:** Advanced Encryption Standard. It is securer than TKIP.
PSK Password	Specify the PSK password used in the connection with the clients.

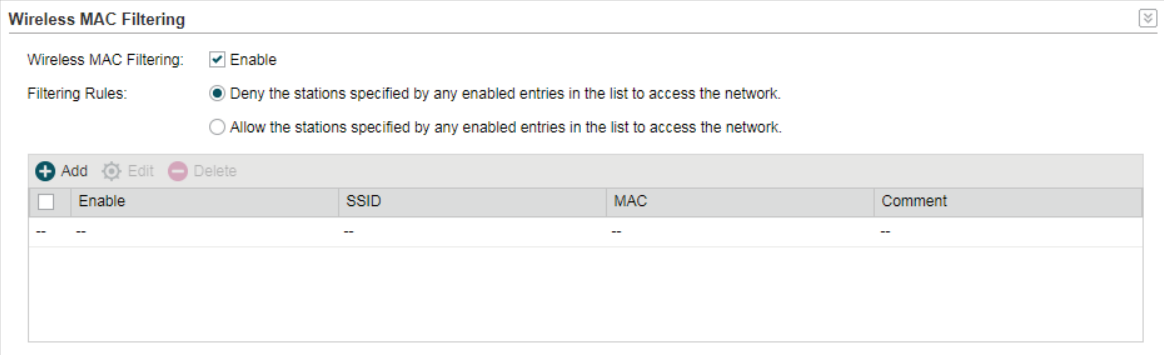
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the device should change the encryption key. 0 means that the encryption key does not change at anytime.

3. Click *Apply*, then click *Save*.

5.5 Configure Wireless MAC Filtering

Wireless MAC Filtering function uses MAC addresses to determine whether one host can access the wireless network or not. Thereby it can effectively control the user access in the wireless network. This function is available in all modes except the Client Mode.

1. Go to the **Wireless** page. In the **Wireless MAC Filtering** section, enable this feature and specify the filtering rule.



Wireless MAC Filtering	Enable or disable the Wireless MAC Filtering function.
Filtering Rules	Specify the filtering rules. **Allow the stations specified by any enabled entries in the list to access the network:** The stations listed in the table are allowed to access the wireless network under the rules. While others are forbidden to access. **Deny the stations specified by any enabled entries in the list to access the network:** The stations listed in the table are forbidden to access the wireless network under the rules. While others are allowed to access.

2. Click *Add* and specify the following parameters.



Enable	Enable or disable the desired entry.

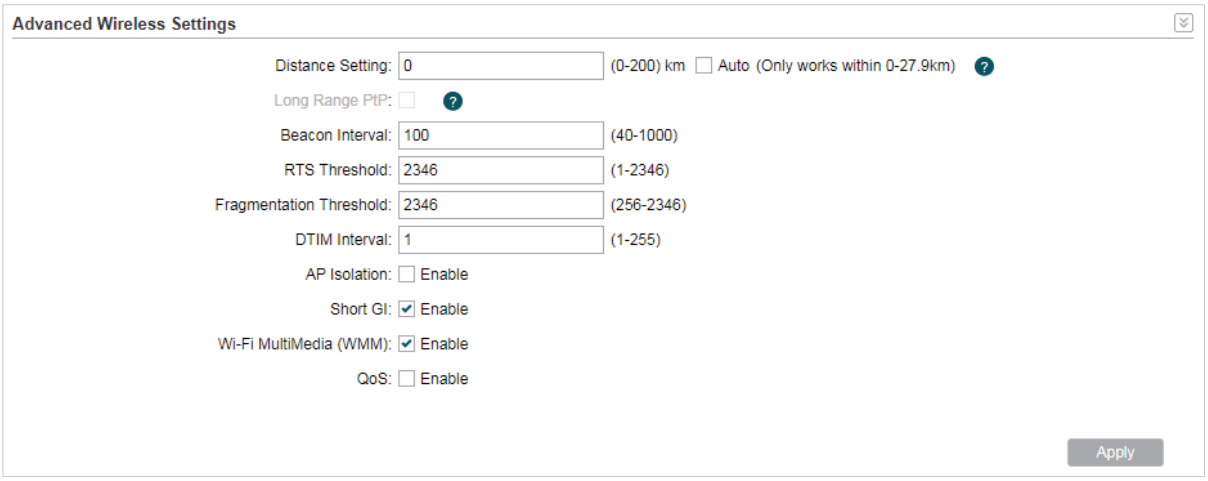
SSID	Select te SSID to which the filtering rules apply. In AP Mode, if Multi-SSID is enabled, you should set different filtering rules for each SSID.
MAC	Enter the MAC address of the wireless host that you need to filter.
Comment	Enter the description information for the filtering rule

3. Click *Save* and click *Apply*. Then click *Save*.

5.6 Configure Advanced Wireless Parameters

This section is used to specify the advanced wireless parameters, such as Beacon Interval, RTS threshold and DTIM Interval.

Go to the **Wireless** page. In the **Advanced Wireless Settings** section, specify the following parameters and click *Apply*. Then click *Save*.



Distance Setting	Specify the distance between AP and Station. If this device serves as a client, the value is the distance between this device and the root AP. If this device serves as an AP, the value is the distance between the farthest client and this AP. You can manually enter the value or enable the Auto option. **Manual:** Enter the distance manually in the input box. The value is limited to 0-200km, and we recommend you set the value to 110% of the real distance. **Auto (Only works within 0-xx km):** Check the Auto option, then the system will dynamically detect the distance. This function is available only when the distance is less than xx kilometers. The value xx varies according to the channel width you set. CPE210 does not support this option. The distance value will be converted to a corresponding ACK timeout value, and the ACK timeout value will influence the throughput performance to a large extent.

Long Range PtP	**Note:** Long Range PtP is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Long Rage PtP is only available when MAXtream function is enabled. With this function enabled, it is allowed to specify a larger distance which can be helpful in the following situations: • The AP is connected to a single client or AP. • The distance between the two devices exceeds the distance allowed by the AP's hardware specifications. The distance is used to calculate the Acknowledge timeout (ACK timeout). Long Range PtP allows the AP to get a larger ACK timeout and reduce unnecessary retransmission in the situations above.
Beacon Interval	Specify the beacon interval for the device. Beacons are transmitted periodically by the device to announce the presence of a wireless network for the clients. Beacon Interval value determines the time interval of the beacons sent by the device. Specify a value from 40 to 1,000. The default value is 100.
RTS Threshold	Specify the RTS threshold for the device. RTS/CTS (Request to Send/Clear to Send) is used to improve the data transmission efficiency of the network with hidden nodes, especially when there are lots of large packets to be transmitted. When the size of a data packet is larger than the RTS Threshold, the RTS/CTS mechanism will be activated. With this mechanism activated, before sending a data packet, the client will send an RTS packet to the device to request data transmitting. And then the device will send CTS packet to inform other clients to delay their data transmitting. In this way, packet collisions can be avoided. For a busy network with hidden nodes, a low threshold value will help reduce interference and packet collisions. But for a not-so-busy network, a too low threshold value will cause bandwidth wasting and reduce the data throughput.
Fragmentation Threshold	Specify the fragmentation threshold for packets. The fragmentation function can limit the size of packets transmitted over the network. If the size of a packet exceeds the Fragmentation Threshold, the fragmentation function is activated and the packet will be fragmented into several packets. Fragmentation helps improve network performance if properly configured. However, a too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.

DTIM Interval	Specify the DTIM (Delivery Traffic Indication Message) Interval for the device. The DTIM is contained in some Beacon frames. It indicates whether the device has buffered data for client devices. The **DTIM Period** indicates how often the clients served by this device should check for buffered data still on the device awaiting pickup. Specify the value between 1-255 Beacon Intervals. The default value is 1, indicating that clients check for buffered data at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend you keep the default value.
AP Isolation	Enable or disable AP Isolation. With this feature enabled, the clients can not communicate with each other directly. **Note:** AP Isolation is not available in Client Mode.
Short GI	Enable or disable Short GI. Propagation delays often occurs in data transmission process and influence the capability of the wireless network. It can result from multiple factors, such as multipath effect. GI (Guard Interval) is intended to solve the problem based on delays, and Short GI is used to improve the throughput of the wireless network based on the GI in the environment with small delays. When the delays are small. When Short GI is enabled, the guard interval will be set as 400ns and this function will boost the performance about 11%. In the with serious multipath time delay. Short GI function will reduce the throughput instead of improving it.
Wi-Fi Multimedia (WMM)	Enable or disable WMM. With WMM enabled, the system will prioritize traffic according to the data type when forwarding data. Time-dependent traffic, such as video or audio packets, gets a higher priority than normal traffic. We recommend you enable this function when you are running the video or audio application.
QoS	Enable or disable QoS. The QoS function improves the transmission performance of video or audio traffic by optimizing the scheduling policy between the AP and the clients.

6 Manage the Device

The device provides powerful functions of management and maintenance. This chapter introduces how to manage the device, including:

6.1 Manage System Logs

6.2 Specify the Miscellaneous Parameters

6.3 Configure Ping Watch Dog

6.4 Configure Dynamic DNS

6.5 Configure Web Server

6.6 Configure SNMP Agent

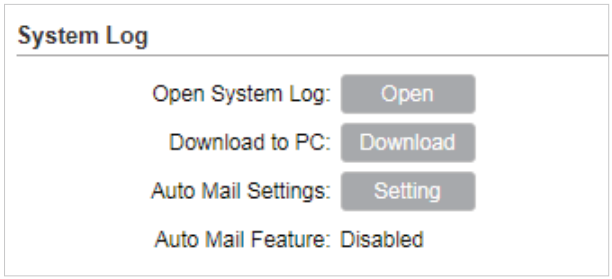
6.7 Configure SSH Server

6.8 Configure RSSI LED Thresholds

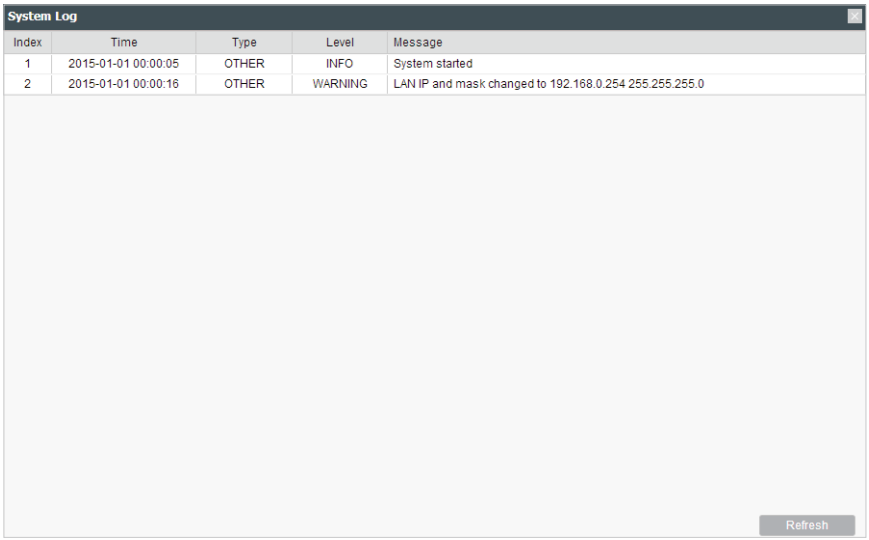
6.1 Manage System Logs

System logs record the events and activities while the device is running. If a failure happens on the device, System logs can help to diagnose the issue.

1. Go to the **Management** page. In the **System Log** section, perform the following operations.



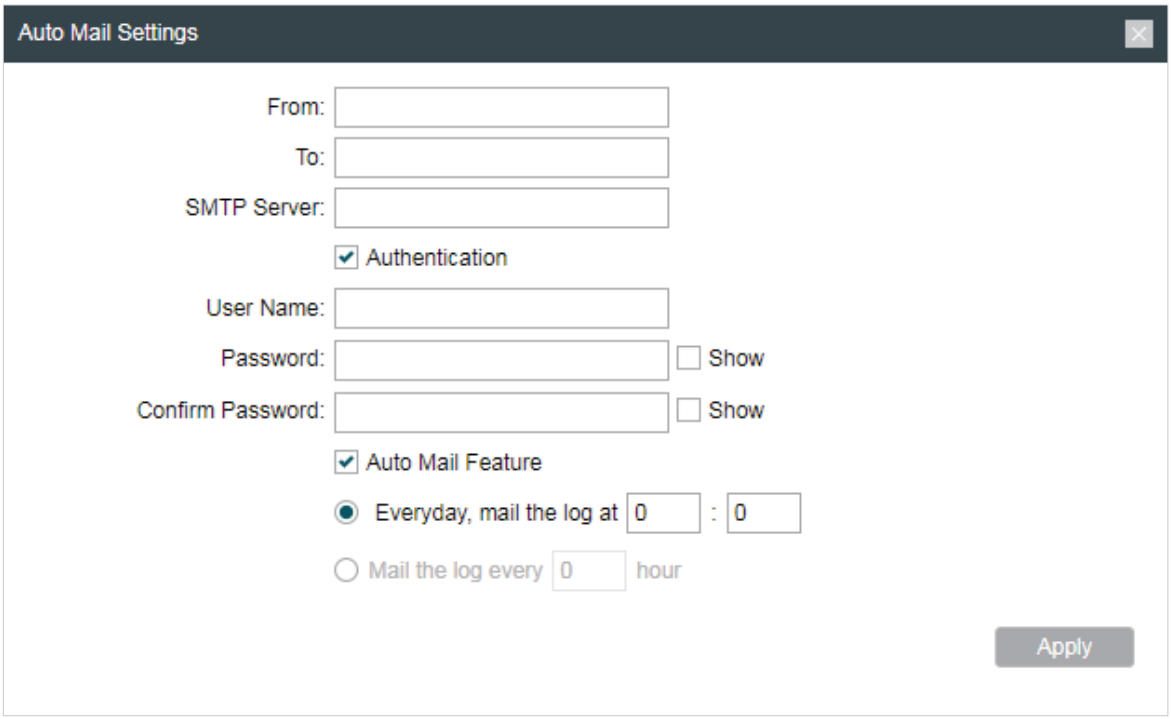
Open System Log	Click the *Open* button to view the system log.



This page displays detailed system logs that can be sorted on columns by ascending or descending order. Columns can be chosen from Time, Type, Level, and Message.

Download to PC	Click the *Download* button to download the system logs to your PC.

2. Click the *Setting* button to specify the Auto Mail Settings.



From	Enter the sender's E-mail address.
To	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address of the sender's SMTP server.
Authentication	Enable or disable the authentication function. If the sender's mailbox is configured, check the box to enable mail server authentication. Enter the sender's username and password.
Auto Mail Feature	Enable or disable Auto Mail Feature. With this feature enabled, specify the way for the device to send the system log.

6.2 Specify the Miscellaneous Parameters

This section is used to specify miscellaneous parameters.

1. Go to the **Management** Page. In the **Miscellaneous** section, configure the following features and click *Apply*.



Discovery	Enable or disable Discovery. With this feature enabled, TP-Link Pharos Control software can discover the device. Pharos Control is a network management software developed independently by TP-Link and it currently supports Pharos series products. It can centralize monitoring and managing network devices in the network platform
CDP	Enable or disable CDP. With this function enabled, this device can share its information with the neighboring devices that support CDP (Cisco Discovery Protocol, a device discovery protocol developed by Cisco).

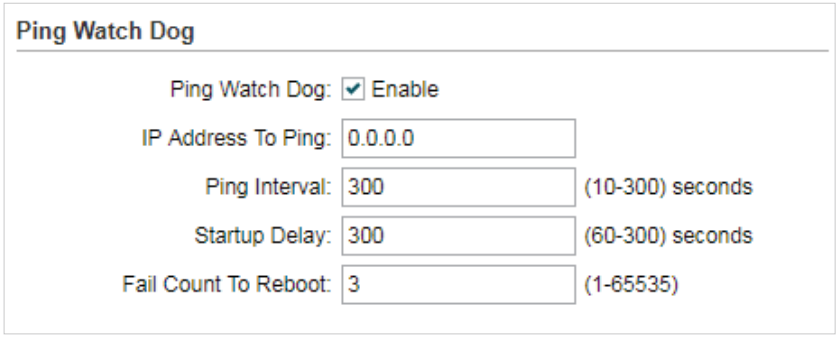
2. Click *Save*.

6.3 Configure Ping Watch Dog

Ping Watch Dog sets the device to continuously ping a user-defined IP address (it can be the internet gateway, for example) to check the network connectivity. If there is a connection failure then the device will automatically reboot.

Ping Watch Dog is dedicated to continuously monitoring the connectivity to a specific host using the Ping tool. The Ping tool sends ICMP echo request packets to the target host and listens for ICMP echo response. If the defined number of replies is not received, the tool reboots the device.

1. Go to the **Management** Page. In the **Ping Watch Dog** section, Enable this feature and configure the following features. Click *Apply*.



Ping Watch Dog	Enable or disable Ping Watch Dog.
IP Address To Ping	Specify the IP address of the target host to which the device will send ping packets.
Ping Interval	Enter the time interval between two ping packets. The default value is 300 seconds.

Startup Delay	Enter the initial time delay from device startup to the first ICMP echo requests sent by Ping Watch Dog. The default value is 300 seconds. The Startup Delay value should be at least 60 seconds taking the device's initialization time in account.
Fail Count To Reboot	Enter the fail count of ICMP echo request. If the device sends the specified count of ICMP echo requests to the host and none of the corresponding ICMP echo response packets is received, Ping Watch Dog will reboot the device. The default value is 3.

2. Click *Save*.

6.4 Configure Dynamic DNS

Note:

The Dynamic DNS function is only available in AP Router and AP Client Router (WISP Client) Mode.

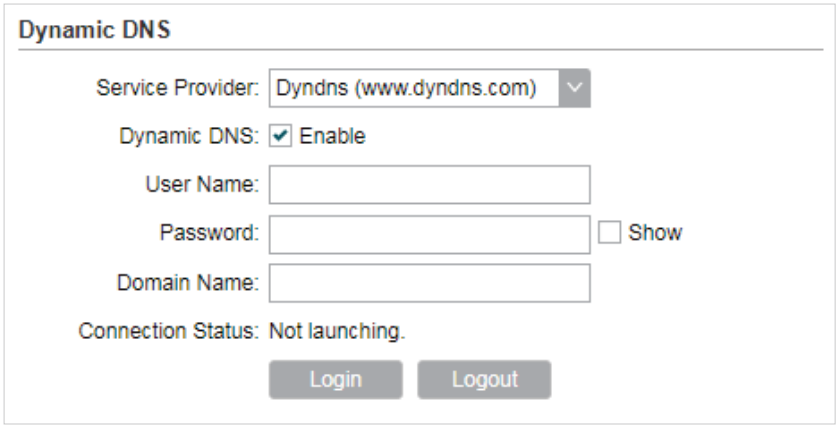
The main function of Dynamic DNS (DDNS) is mapping the fixed domain name to dynamic IP address.

When a device connects to the internet through PPPoE or Dynamic IP, the WAN IP address it gets is not fixed, which is inconvenient for the internet users to access the servers in the local area network through IP address. With Dynamic DNS function enabled, users can access servers using a fixed domain name.

The DDNS server will establish a mapping table about the dynamic IP address and the fixed domain name. When the WAN IP address of the device changes, it will make an update request to the specified DDNS server, and then the DDNS server will update the mapping relation between the IP address and the domain name. Therefore, whenever the WAN IP address changes, users on the internet can still access the servers in the local area network using a fixed, easy-to-remember domain name.

The DDNS function that serves as the client of DDNS service must work with DDNS server. Register an account to DDNS service provider (NO-IP, Dyndns or Comexe) first.

1. Go to the **Management** page. In the **Dynamic DNS** section, configure the following parameters and click *Login*.



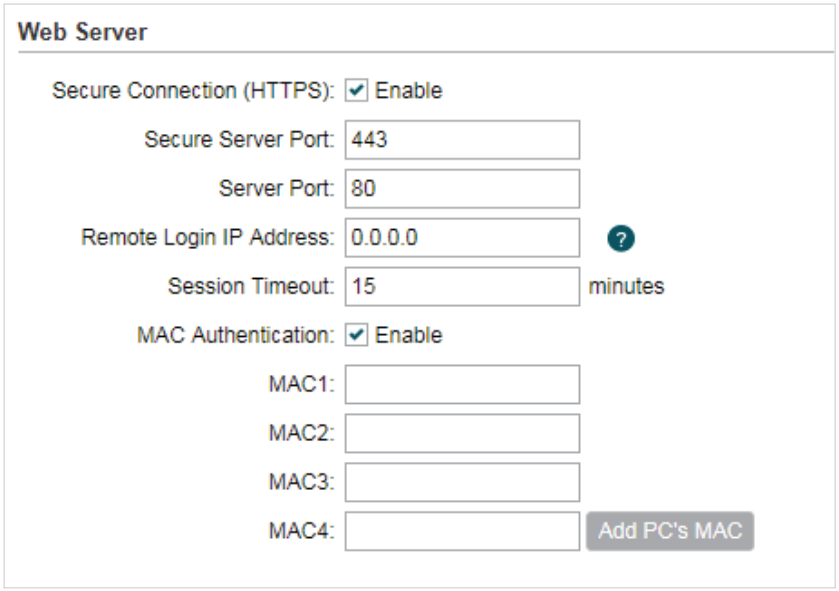
Service Provider	Select the service provider.
Dynamic DNS	Enable or disable the Dynamic DNS feature.
User Name	Enter the user name of your DDNS account.
Password	Enter the password of your DDNS account.
Domain Name	Specify the domain name that you registered with your DDNS service provider.
Connection Status	Displays the connection status of the DDNS service.

2. Click *Apply*, then click *Save*.

6.5 Configure Web Server

This function is used to configure the related parameters of Web server. Users can log in to the web management page to manage this device remotely over the internet through Web Server.

1. Go to the **Management** page. In the **Web Server** section, configure the following parameters and click *Apply*.



Secure Connection (HTTPS)	Enable or disable the HTTPS feature. HTTPS function is based on the SSL or TLS protocol working in transport layer. It supports a security access via a web browser.
Secure Server Port	Specify the server port number used in HTTPS. The default value is 443.
Server Port	Specify the server port number used in HTTP. The default value is 80.
Remote Login IP Address	Specify the IP address of the remote host. With this configured, the remote host can access the management interface remotely using the WAN IP of this device.
Session Timeout	Specify the session timeout time. The system will automatically release the connection when the time is up.
MAC Authentication	Enable or disable MAC Authentication. When it is enabled, you can specify up to four MAC address for authentication. With this function enabled, only the device whose MAC address is in the MAC list can access the management interface to configure the device. Click *Add PC's MAC* to quickly add your PC's MAC address to the MAC list.

2. Click *Apply*, then click *Save*.

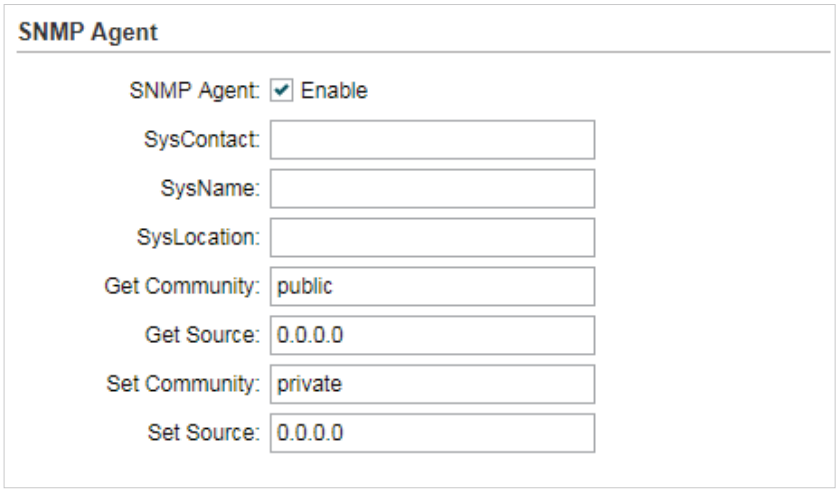
6.6 Configure SNMP Agent

Get the traffic information and transmit condition by using the SNMP Agent function.

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. Main functions of SNMP include monitoring network performance, detecting and analyzing network error, configuring network devices, and so on.

Configure the device as SNMP Agent, and it can receive and process the management message from the NMS (Network Management System).

1. Go to the **Management** page. In the **SNMP Agent** section, configure the following parameters and click *Apply*.



SNMP Agent	Enable or disable the SNMP Agent function.
SysContact	Enter the textual identification of the contact person for this device, for example, contact number or e-mail address.
SysName	Enter a name for the device.
Syslocation	Enter the location of the device. For example, the name can be composed of the building, floor number, and room location.
Get Community	Specify the community that has read-only access to the device's SNMP information.
Get Source	Enter the IP address of the NMS that can serve as Get Community to read the SNMP information of this device. By default, it is 0.0.0.0, which means an NMS of any IP address is available.
Set Community	Specify the community who has the read-and-write right of the device's SNMP information.
Set Source	Enter the IP address of the NMS that can serve as Set Community to read and write the SNMP information of this device. By default, it is 0.0.0.0, which means an NMS of any IP address is available.

2. Click *Apply*, then click *Save*.

Note:

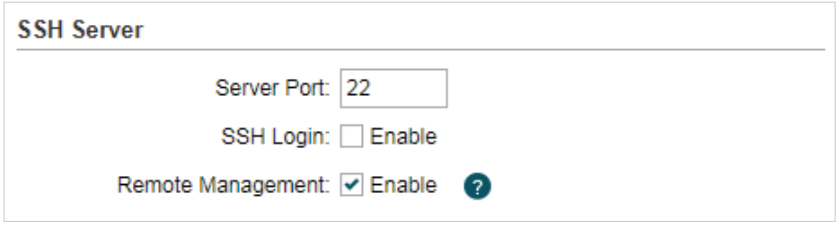
Defining community can allow management systems in the same community to communicate with the SNMP Agent. The community name can be seen as the shared password of the network hosts group. Thus, for the safety, we suggest modifying the default community name before enabling the SNMP Agent service. If the field of community is blank, the SNMP Agent will not respond to any community name.

6.7 Configure SSH Server

The SSH Server function is used for the users to log in and manage the device through SSH connection on the SSH client software.

SSH (Secure Shell) is a security protocol established on application and transport layers. SSH-encrypted-connection is similar to a telnet connection, but essentially the old telnet remote management method is not safe, because the password and data transmitted with plain-text can be easily intercepted. SSH can provide information security and powerful authentication when you log in this device remotely through an insecure network environment. It can encrypt all the transmission data and prevent the information in remote management from being leaked.

1. Go to the **Management** page. In the **SSH Server** section, configure the following parameters and click *Apply*.



Server Port	Enter the TCP/IP port of the SSH Server. The default port is 22.
SSH Login	Enable or disable SSH function.
Remote Management	Enable or disable Remote Management. With this function enabled, TP-Link Pharos Control software can manage the device remotely.

2. Click *Save*.

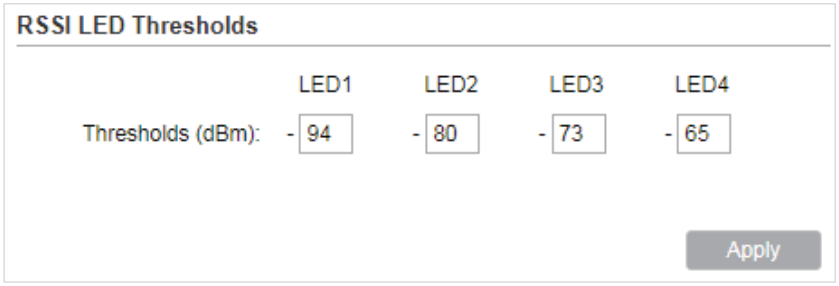
6.8 Configure RSSI LED Thresholds

Note:

RSSI LED Thresholds is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

Configure the LEDs on the device to light up when received signal levels reach the values defined in the following fields. This function can help a technician to easily deploy a Pharos series product without logging into the device (for example, for antenna alignment operation).

1. Go to the **Management** page. In the **RSSI LED Thresholds** section, configure the following parameters and click *Apply*.



LED1/LED2/ LED3/LED4	Displays the LED number.
Thresholds	Specify the threshold for the desired LED. The specified LED will light up if the signal strength reaches the values in the field. The default values are set according to the verified optimum values. We recommend you keep it by default. The default LED threshold values may vary among different product models in terms of radio features.

2. Click *Apply*, then click *Save*.

7 Configure the System

This chapter introduces how to configure the system of the device, including:

7.1 Configure Device Information

7.2 Configure Location Information

7.3 Configure User Account

7.4 Configure Time Settings

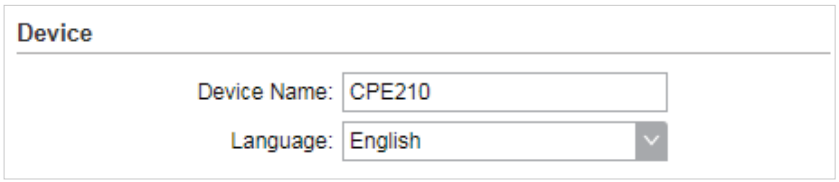
7.5 Update Firmware

7.6 Configure Other Settings

7.1 Configure Device Information

In this section, configure the device name and the system language.

1. Go to the **System** page. In the **Device** section, configure the following parameters and click *Apply*.



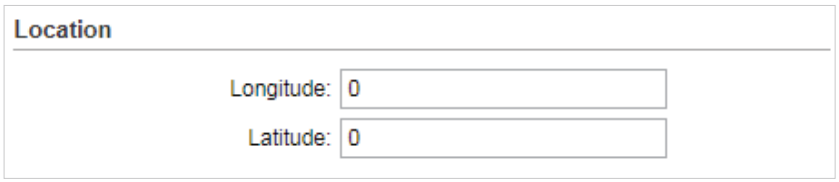
Device Name	Specify the device name.
Language	Specify the system language used in the management interface.

2. Click *Save*.

7.2 Configure Location Information

In this section, configure the location for the device.

1. Go to the **System** page. In the **Location** section, configure the following parameters and click *Apply*.



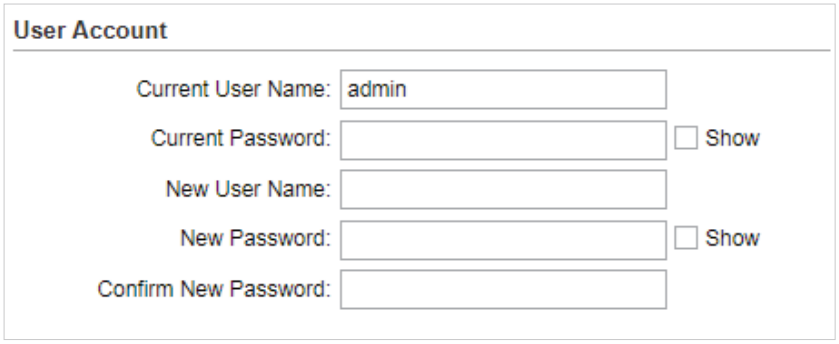
Longitude	Enter the longitude of the device's location in decimal degree. The positive number indicates the east longitude while the negative number indicates the west longitude.
Latitude	Enter the latitude of the device's location in decimal degree. The positive number indicates the north latitude while the negative number indicates the south latitude.

2. Click *Save*.

7.3 Configure User Account

This section is used to configure user account.

1. Go to the **System** page. In the **User Account** section, configure the following parameters and click *Apply*.



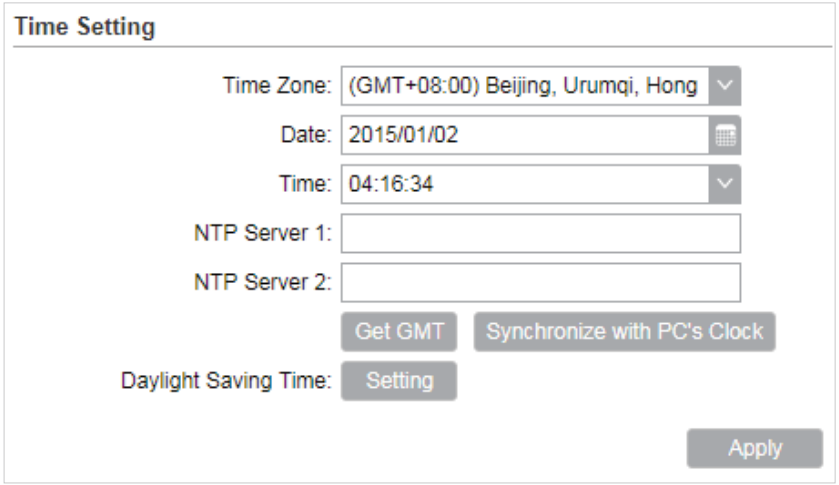
Current User Name	Displays the current user name.
Current Password	Enter the current password for the user account. Check the *Show* box to display what you've entered.
New User Name	Enter a new user name for the user account.
New Password	Enter a new password for the user account. Check the *Show* box to display what you've entered.
Confirm New Password	Confirm the new password.

2. Click *Save*.

7.4 Configure Time Settings

In this section, configure the system time and the daylight saving time.

1. Go to the **System** page. In the **Time Settings** section, configure the system time.



■ Manually

Configure the System time manually.

Time Zone	Select your local time zone.
Date	Click the calendar button to choose the date or enter the date in the format: YYYY/MM/DD.
Time	Select the time from the drop-down list or enter the time in the format HH:MM:SS.

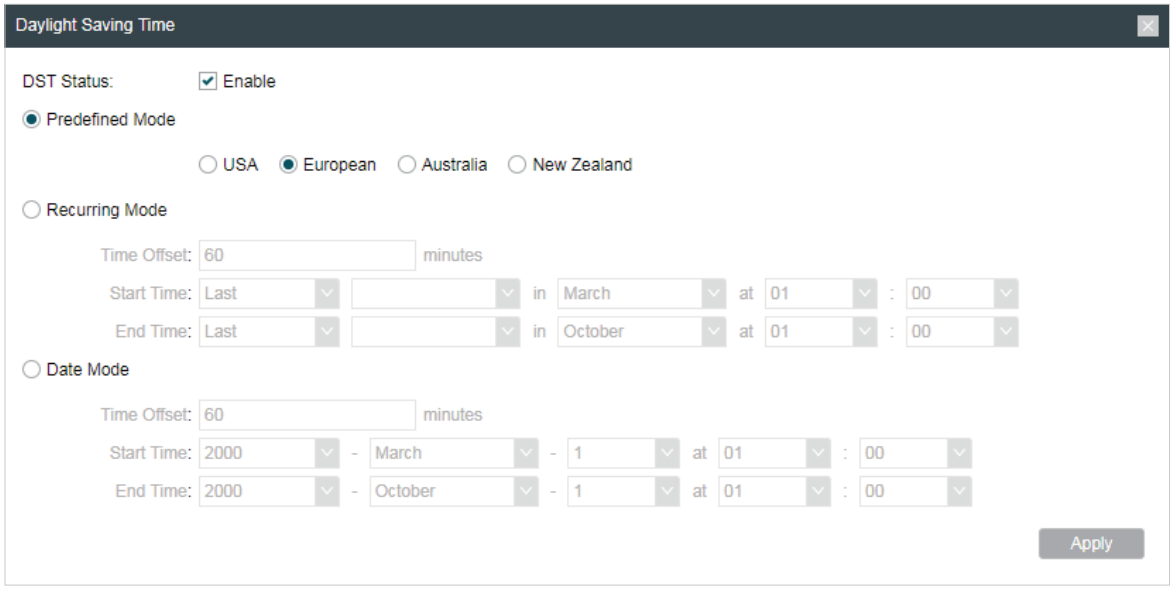
■ Automatically

- Specify the NTP Server, then click the *Get GMT* button to get the system time from the NTP server

NTP Server 1	Specify the primary NTP server used to get time automatically.
NTP Server 2	Specify the alternate NTP server used to get time automatically.

- Click *Synchronize with PC's Clock* to synchronize the system time with the PC's time.

2. Click the *Setting* button to specify the daylight saving time.



■ Predefined Mode

Select Predefined Mode and select the predefined daylight saving time schedule for the device.

USA	The daylight saving time of USA is from Second Sunday in March, 02:00 to First Sunday in November, 02:00.
European	The daylight saving time of European is from Last Sunday in March, 01:00 to Last Sunday in October, 01:00.

Australia	The daylight saving time of Australia is from First Sunday in October, 02:00 to First Sunday in April, 03:00.
New Zealand	The daylight saving time of New Zealand is from Last Sunday in September, 02:00 to First Sunday in April, 03:00.

■ **Recurring Mode**

Select Recurring Mode and configure the related parameters for the device. This configuration will be used every year.

Offset	Specify the time to set the clock forward by.
Start Time	Specify the start time of Daylight Saving Time.
End Time	Specify the end time of Daylight Saving Time.

■ **Date Mode**

Note:

Date Mode is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

Select Date Mode and configure the related parameters for the device. This configuration will be used only one time.

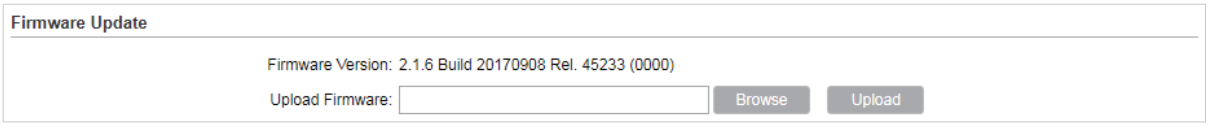
Offset	Specify the time to set the clock forward by.
Start Time	Specify the start time of Daylight Saving Time.
End Time	Specify the end time of Daylight Saving Time.

3. Click *Apply*, then click *Save*.

7.5 Update Firmware

This section is used to view the current firmware and update the firmware of the device.

Go to the **System** page. In the **Firmware Update** section, click *Browser* to select a firmware file then click *Upload*.



Firmware Version	Displays the current firmware version of the device.

Note:

- We recommend that you back up current system configuration before updating the firmware.
- Select the proper software version that matches your hardware to upgrade. Visit TP-Link website to download the latest firmware.
- To avoid damage, do not power off the device while upgrading.
- After upgrading, the device will reboot automatically.

7.6 Configure Other Settings

This section is used to back up or upload the configuration file, reset the device and reboot the device.

Go to the System Page. In the Configuration section, perform the following operations.



Backup Configuration	Click *Backup* to back up the current configuration to your PC.
Upload Configuration	Click *Browser* to select the desired configuration file in your PC. Then click *Upload* to upload the configuration file to your device. We recommend that you back up your current system configuration before uploading the new configuration.
Reset to Factory Defaults	Click *Reset* to restore the device to its factory defaults. It's recommended to back up your current system configuration before restoring the device to its defaults.
Reboot Device	Click *Reboot* to reboot the device. Note that any changes that have not been saved will be lost.

Note:

- After backup, the device will reboot automatically.
- To avoid damage, DO NOT turn off the device while uploading.

8 Use the System Tools

This chapter introduces how to configure the system tools:

8.1 Configure Ping

8.2 Configure Traceroute

8.3 Test Speed

8.4 Survey

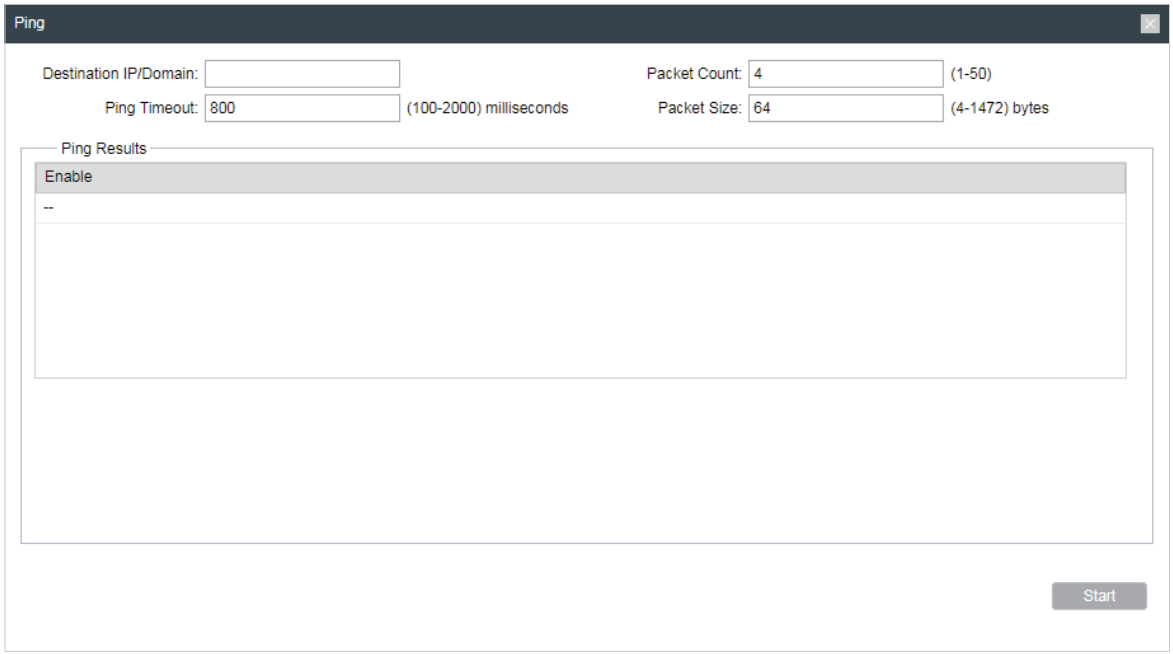
8.5 Analyze Spectrum

8.6 Antenna Alignment

8.1 Configure Ping

Ping test function is used to test the connectivity and reachability between the device and the target host so as to locate the network malfunctions.

1. Click *Ping* from the drop-down list on the upper-right corner and specify the following parameters.



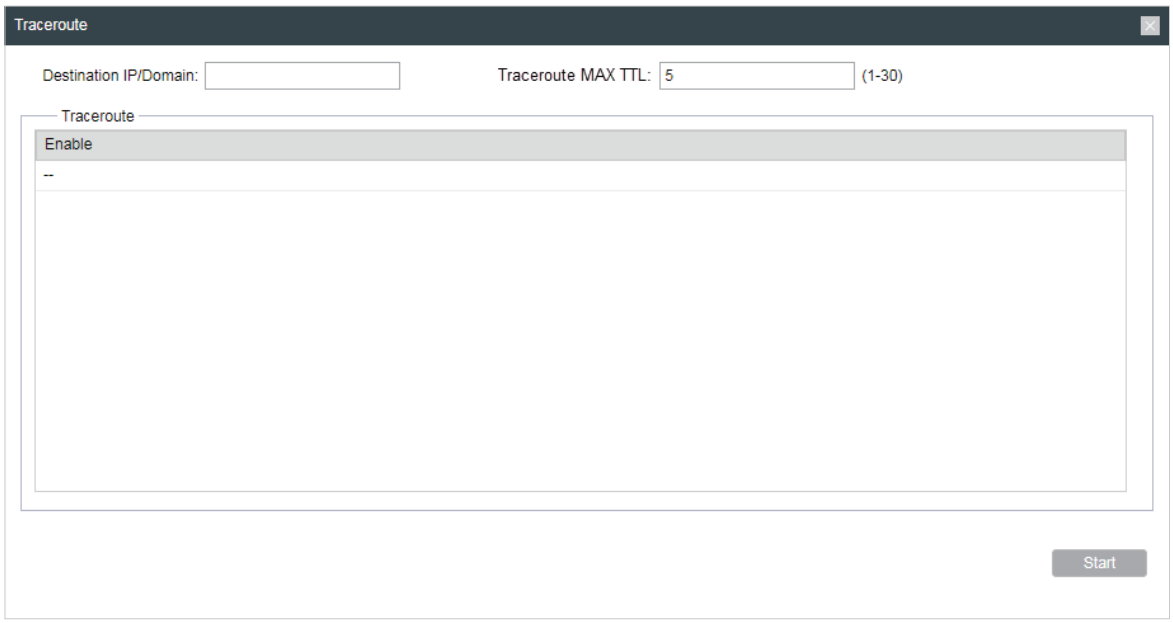
Destination IP/ Domain	Enter the IP address of the destination node for Ping test. The device will send Ping packets to test the network connectivity and reachability of the host and the results will be displayed in the Ping Result.
Packet Count	Enter the number of packets to be sent during the testing. It can be 1 to 50 and the default is 4.
Ping Timeout	Enter a time value to wait for a response. If the device doesn't receive ant response during the timeout time, the connection will be considered to be failed. It can be 100-2000 milliseconds. The default value is 800 milliseconds.
Packet Size	Enter the number of data bytes to be sent. It can be 4-1472 bytes and the default is 64.

2. Click *Start*.

8.2 Configure Traceroute

Tracertroute function is used to tracks the route packets taken from source on their way to a given target host. When malfunctions occur in the network, troubleshoot with traceroute utility.

1. Click *Traceroute* from the drop-down list on the upper-right corner and specify the following parameters.



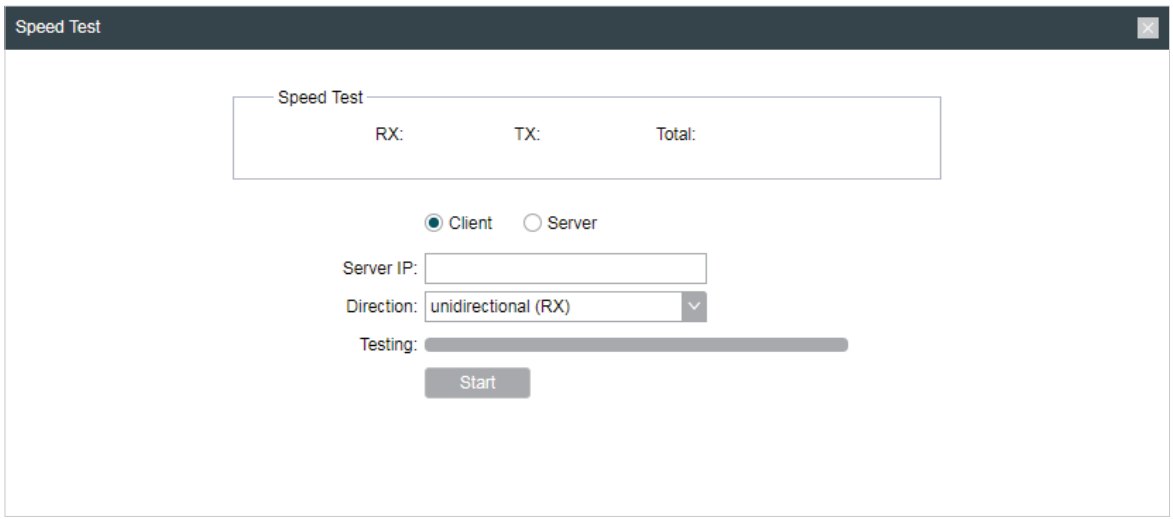
Destination IP/ Domain	Enter the IP address of the destination node for Traceroute test. The device will send Traceroute packets to test the network connectivity and reachability of the host and the results will be displayed in the Traceroute.
Traceroute Max TTL	Specify the traceroute max TTL (Time To Live) during the traceroute process. It is the maximum number of the route hops the test packets can pass through.

2. Click *Start*.

8.3 Test Speed

Speed Test tool is used for testing the throughput between two Pharos products in the same network. The test requires one of the two devices to be set as a server and the other as a client. The client launches the test request to the server and the server respond to it. The test result will display on the page of the client.

1. Click *Speed Test* from the drop-down list on the upper-right corner and specify the following parameters.



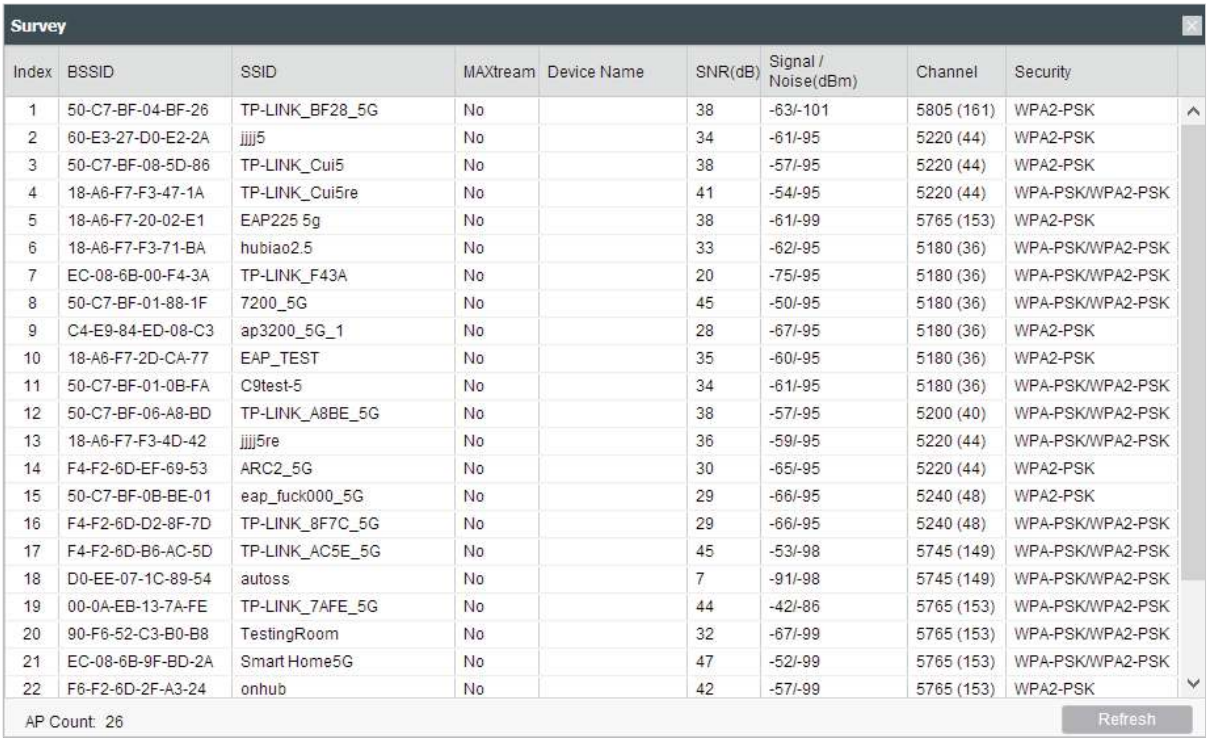
Speed Test	Displays the data streams that the device is transmitting (TX), receiving (RX) and both of them (Total).
Server	Select Server and the device will passively accept the test request from the clients in the speed test process.
Client	Select Client and the device will launch the test request to the server in speed test process.
Server IP	Specify the server IP for speed test.
Direction	Select the direction of the speed test including unidirectional (RX), unidirectional (TX) and bidirectional.
Testing	Displays the process of the test.

2. Click *Start*.

8.4 Survey

The survey tool is used to survey the wireless network around the device.

Click *Survey* from the drop-down list on the upper-right corner and the following page will appear.

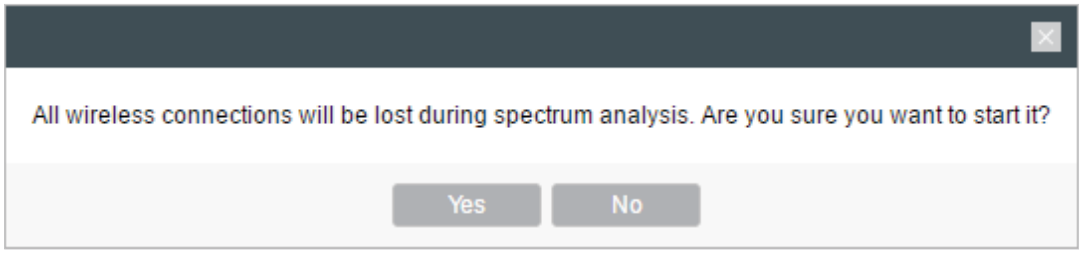


BSSID	Displays the BSSID of other APs surveyed by this device.
SSID	Displays the SSID of other APs surveyed by this device.
MAXtream	Displays the MAXtream capability of other APs surveyed by this device.
Device Name	Displays the names of other APs surveyed by this device.
SNR(dB)	Displays the Signal Noise Ratio (Unit: dB) of other APs surveyed by this device.
Signal/Noise (dBm)	Displays the signal and noise value (Unit: dBm) of other APs surveyed by this device.
Channel	Displays the channels of other APs surveyed by this device.
Security	Displays the security mode of APs surveyed by this device.
AP Count	Displays the number of other APs surveyed by this device.
Refresh	Click *Refresh* to refresh this page.

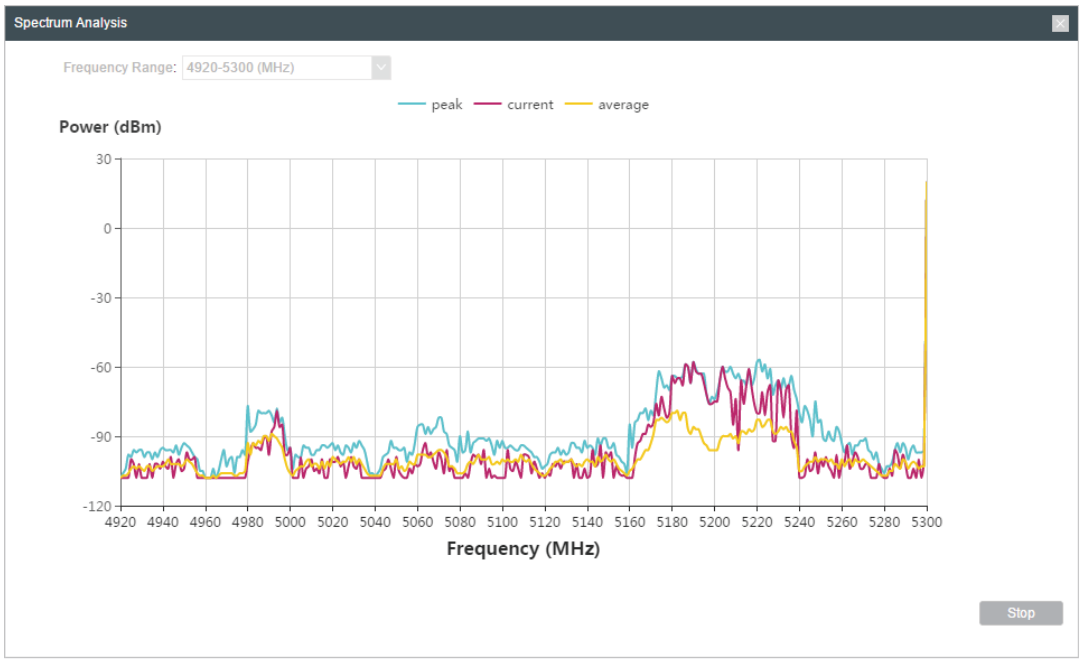
8.5 Analyze Spectrum

Spectrum Analysis can help you choose the proper channel/frequency. Through the spectrum analysis, learn the distribution of the radio noise and intelligently select the channel/frequency in low noise.

1. Click *Spectrum Analysis* from the drop-down list on the upper-right corner and click *Yes* on the pop-up window.



2. Click *Start*. Observe the curves for a period of time, and then click *Stop*. The relatively low and continuous part of the average curve indicates less radio noise. Here we take the figure below as an example.



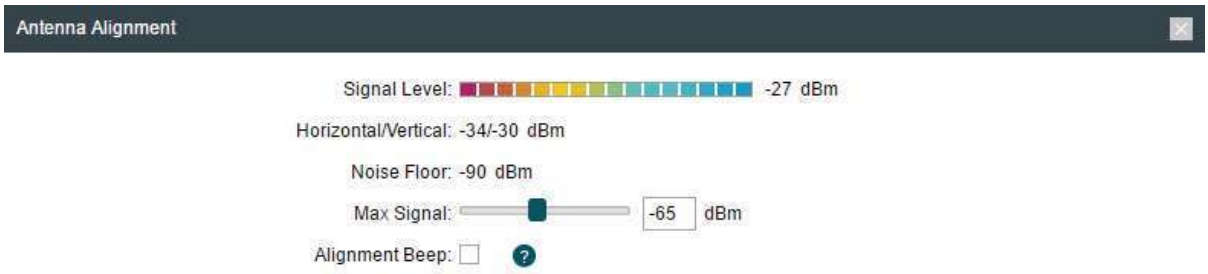
Note:

The select box of Frequency Range is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. Select the required range and then click *Start*.

3. When choosing Channel/Frequency, try to avoid the spectrum with large radio noise.

8.6 Antenna Alignment

Antenna alignment can help you to optimize the antenna. Click *Antenna Alignment* from the drop-down list on the upper-right corner. Adjust your antenna according to the following parameters. Point the antenna in the direction of maximum signal and minimum noise.



Signal Level	Displays the signal strength of the last received packet. The signal strength is the combined value of the two chains.
Horizontal/Vertical	Displays the signal strength of the last received packet. The signal strength of the two chains is displayed separately.
Noise Floor	Displays the noise strength of the wireless network.
Max Signal	Specify the maximum value of the Signal Level indicator. Adjust the sensitivity of the Signal Level indicator by changing this value.
Alignment Beep	Enable the beep sound during the device antenna alignment. This function can help users to align the antenna easily without looking at the management interface. When received signal levels reach the defined levels, the different beep sound will be played. The lower the sound frequency, the stronger the signal strength.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2020 TP-Link Technologies Co., Ltd.. All rights reserved.