



# ***PHAROS***

---

## **User Guide**

For TP-Link Pharos Series Products

CPE210 / CPE220 / CPE510 / CPE520 / CPE610  
WBS210 / WBS510

1910012335 REV 3.0.1

March 2018

# CONTENTS

About this User Guide.....	1
Overview .....	2
<b>1 Operation Modes.....</b>	<b>3</b>
1.1 Access Point.....	4
1.2 Client.....	5
1.3 Repeater (Range Extender) .....	6
1.4 Bridge .....	7
1.5 AP Router .....	7
1.6 AP Client Router (WISP Client) .....	8
<b>2 Quick Start.....</b>	<b>9</b>
2.1 Check the System Requirements .....	10
2.2 Log In to the Device .....	10
2.3 Set Up the Wireless Network.....	11
Access Point.....	12
Client .....	15
Repeater (Range Extender) .....	18
Bridge .....	22
AP Router .....	26
AP Client Router (WISP Client) .....	31
<b>3 Monitor the Network .....</b>	<b>37</b>
3.1 View the Device Information.....	38
3.2 View the Wireless Settings.....	38
3.3 View Wireless Signal Quality.....	39
3.4 View Radio Status .....	40
3.5 View the LAN Settings.....	42
3.6 View the WAN Settings .....	42

3.7	Monitor Throughput.....	43
3.8	Monitor Stations.....	43
3.9	Monitor Interfaces .....	44
3.10	Monitor ARP Table .....	45
3.11	Monitor Routes .....	45
3.12	Monitor DHCP Clients.....	46
3.13	Monitor Dynamic WAN.....	46
<b>4</b>	<b>Configure the Network.....</b>	<b>48</b>
4.1	Configure WAN Parameters.....	49
4.2	Configure LAN Parameters .....	56
	Access Point/Client/Repeater/Bridge Mode .....	56
	AP Router/AP Client Router Mode.....	59
4.3	Configure Management VLAN .....	60
4.4	Configure the Forwarding Feature .....	61
4.5	Configure the Security Feature .....	65
4.6	Configure Access Control .....	68
4.7	Configure Static Routing.....	69
4.8	Configure Bandwidth Control.....	70
4.9	Configure IP & MAC Binding.....	72
<b>5</b>	<b>Configure the Wireless Parameters.....</b>	<b>74</b>
5.1	Configure Basic Wireless Parameters .....	75
5.2	Configure Wireless Client Parameters .....	77
5.3	Configure Wireless AP Parameters.....	81
5.4	Configure Multi-SSID.....	87
5.5	Configure Wireless MAC Filtering .....	89
5.6	Configure Advanced Wireless Parameters.....	90
<b>6</b>	<b>Manage the Device .....</b>	<b>93</b>
6.1	Manage System Logs .....	94

6.2	Specify the Miscellaneous Parameters .....	95
6.3	Configure Ping Watch Dog .....	96
6.4	Configure Dynamic DNS .....	97
6.5	Configure Web Server .....	98
6.6	Configure SNMP Agent .....	99
6.7	Configure SSH Server .....	101
6.8	Configure RSSI LED Thresholds .....	101
<b>7</b>	<b>Configure the System .....</b>	<b>103</b>
7.1	Configure Device Information .....	104
7.2	Configure Location Information .....	104
7.3	Configure User Account .....	104
7.4	Configure Time Settings .....	105
7.5	Update Firmware .....	107
7.6	Configure Other Settings .....	108
<b>8</b>	<b>Use the System Tools .....</b>	<b>109</b>
8.1	Configure Ping .....	110
8.2	Configure Traceroute .....	110
8.3	Test Speed .....	111
8.4	Survey .....	112
8.5	Analyze Spectrum .....	114

# About this User Guide

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

When using this guide, please notice that features of the product may vary slightly depending on the model and software version you have, and on your location, language, and internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

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

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

Specifications can be found on the product page at <http://www.tp-link.com>.

A Technical Support Forum is provided for you to discuss our products at <http://forum.tp-link.com>.

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

# 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 are ideal for point-to-multipoint applications.
- Supports multiple operation modes: Access Point, Client, Repeater (Range Extender), Bridge, AP Router and AP Client Router (WISP Client).
- Provides system-level optimization for long-distance wireless transmission.
- Supports selectable bandwidth of 5/10/20/40MHz.
- 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.

# 1 **Operation Modes**

The Pharos series products support six operation modes to satisfy user's diversified network requirements. This chapter introduces typical usage scenarios of different modes, including:

1.1 *Access Point*

1.2 *Client*

1.3 *Repeater (Range Extender)*

1.4 *Bridge*

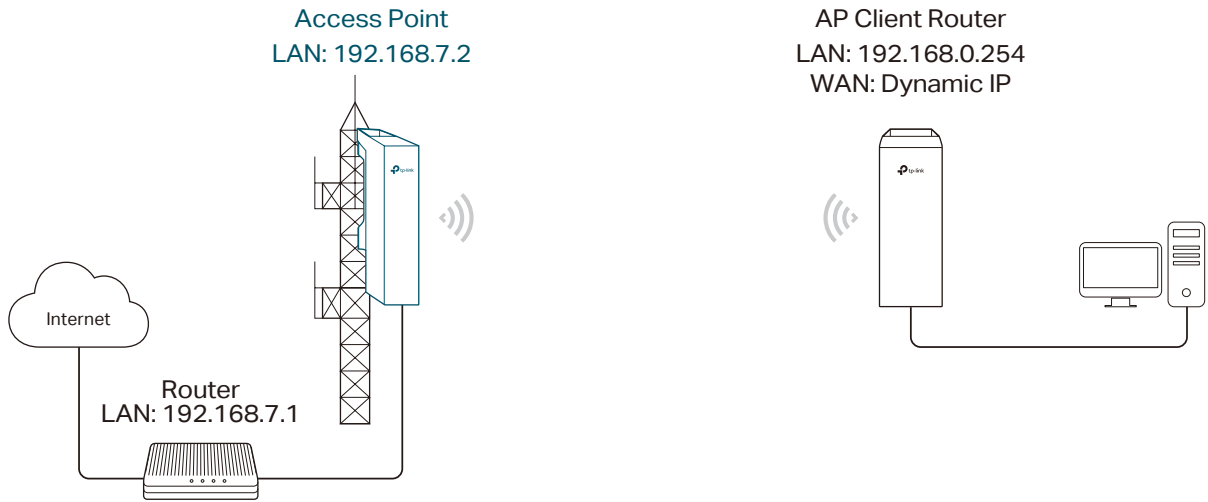
1.5 *AP Router*

1.6 *AP Client Router (WISP Client)*

# 1.1 Access Point

In 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

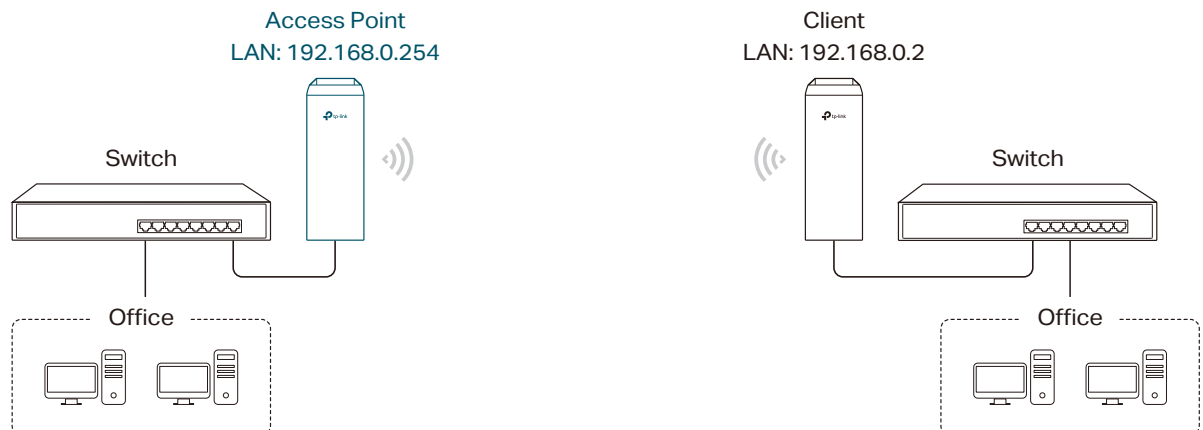


**Network requirements:** Establish the network coverage in the remote areas without long-distance cabling.

**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



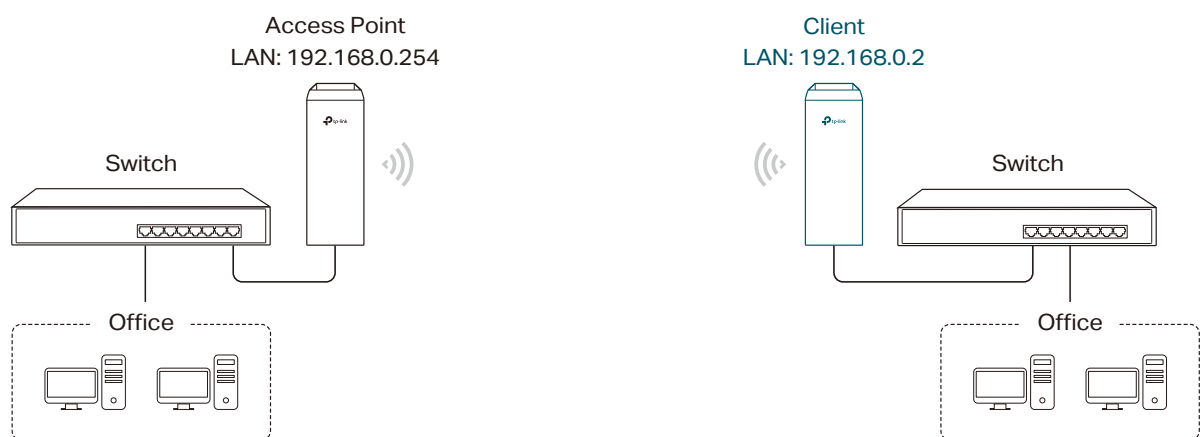
**Network requirements:** Establish wireless network coverage in the campus, community, industrial park or public place to provide wireless access for users.

**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.

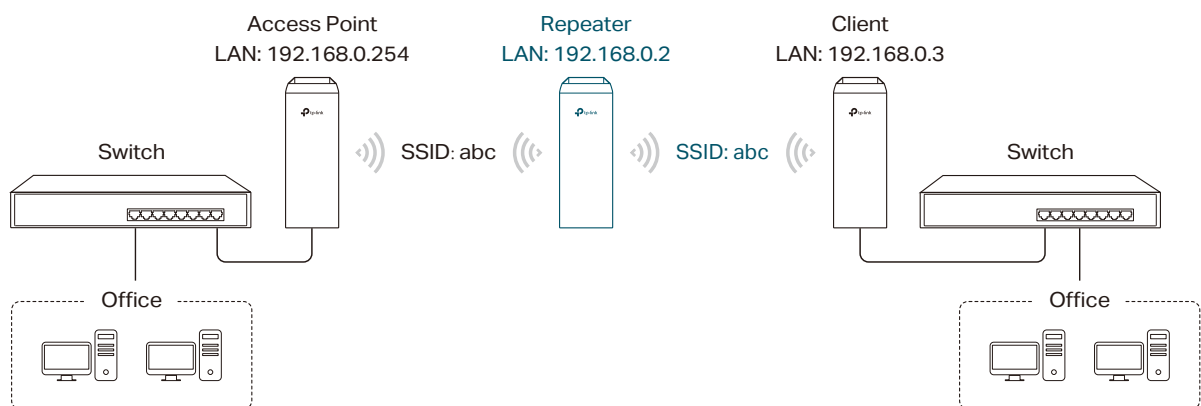


**Network requirements:** Help the wired devices to connect to the wireless network.

**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 Repeater (Range Extender)

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.

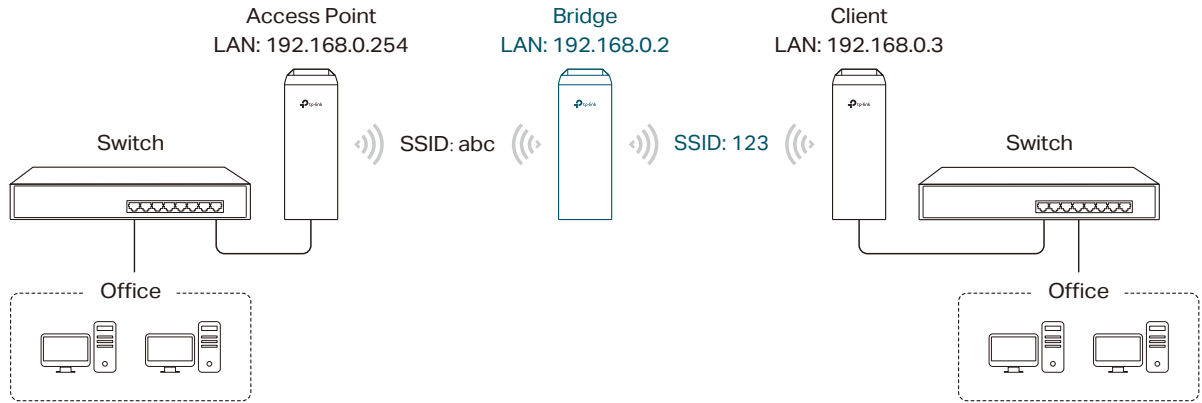


**Network requirements:** Repeat wireless signal and extend the wireless network coverage.

**The device in the network:** If you want to combine two networks via wireless connection but the distance is beyond the networks' wireless coverage range, you can put one or more devices in Repeater mode along the path to repeat the wireless signal and extend the wireless transmission range.

## 1.4 Bridge

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 root AP.



**Network requirements:** Extend the wireless network to eliminate the wireless signal-blind areas. Users can use different SSID and encryption type from those of the root AP device to access the network.

**The device in the network:** Similar to the Repeater mode, the Bridge mode is used to enhance the exiting wireless signal. However, the difference is that the extended wireless network has its own SSID and encryption type different from those of root AP.

## 1.5 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

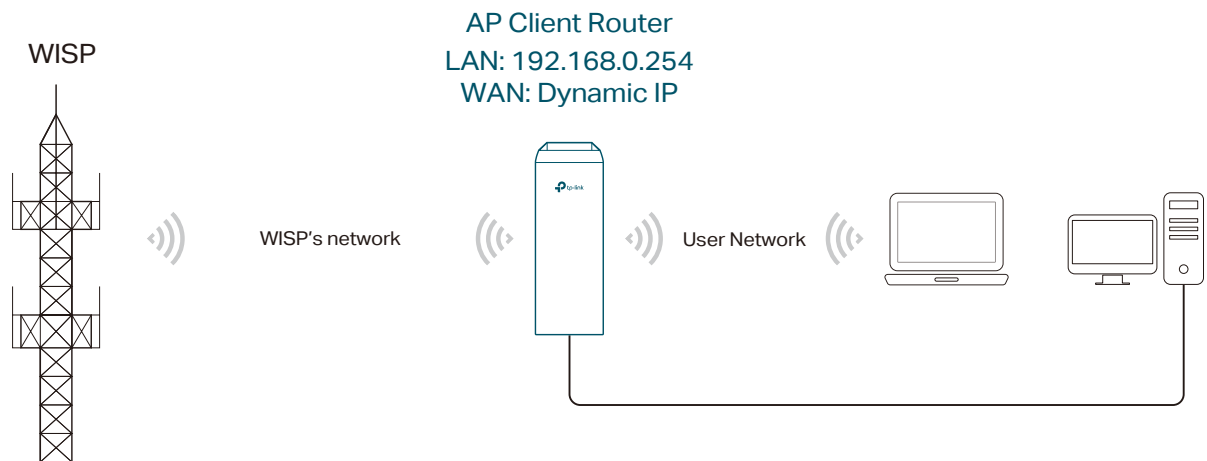
Modem for internet access. Meanwhile, it creates a wireless network for the wireless clients to connect to the internet.

**Note:**

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

## 1.6 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.

# 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

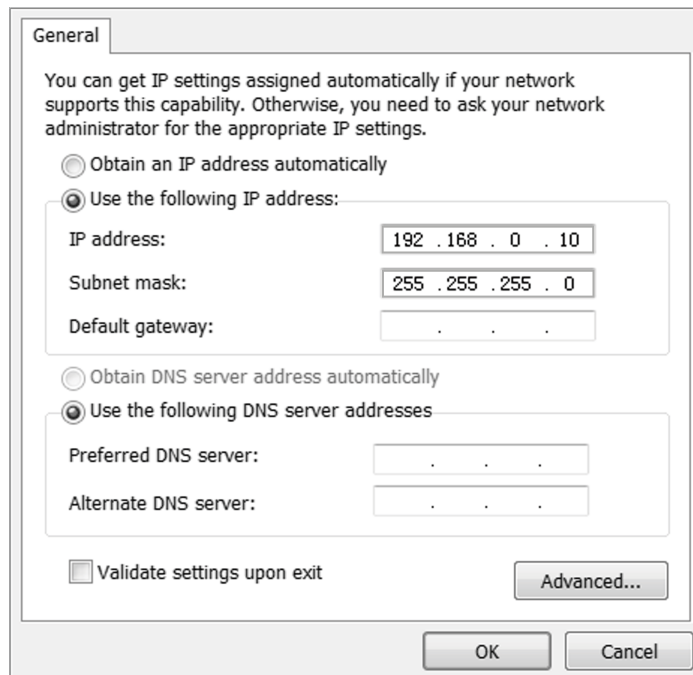
- **Web Browser**

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*. Select the appropriate language from the Language drop-down list. Read and agree the terms of use, then click *Login*.

Login


 User Name:   
Password:   
Language:

**TERMS OF USE**  
This TP-LINK wireless device must be installed by a certified professional. Properly installed shielded Ethernet cable and earth grounding must be used in compliance with this product's warranty. Installers must abide by local rules and regulations in terms of legal frequency channels, output power, and Dynamic Frequency Selection (DFS) requirements. The End User accepts responsibility for maintaining the product in accordance with these rules and regulations. For further information, please visit [www.tp-link.com](http://www.tp-link.com).

I agree to these terms of use

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

Change Password

 New User Name:   
New Password:   
Confirm Password:

**TERMS OF USE**  
It is recommended to change the device user name and password from its default settings.

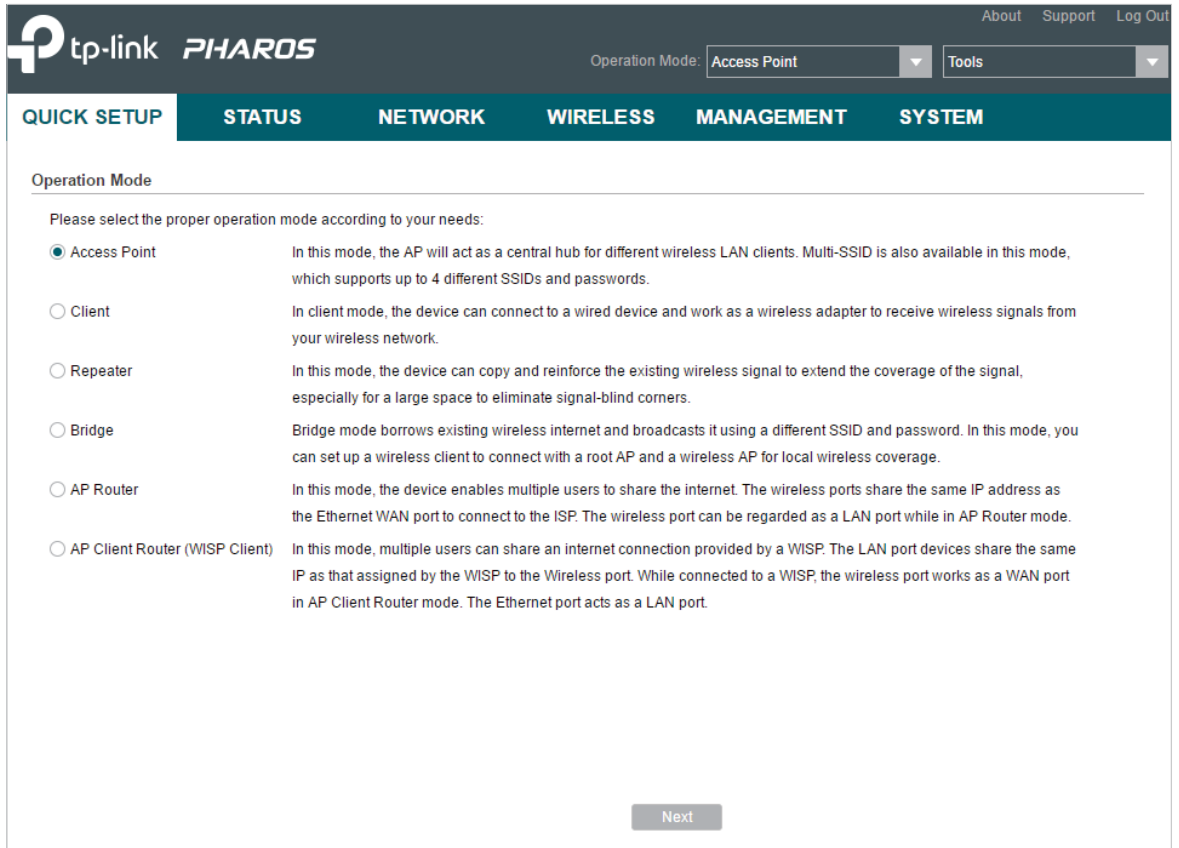
## 2.3 Set Up the Wireless Network

You can 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*.



The screenshot shows the TP-Link PHAROS web interface. At the top, there is a navigation bar with the TP-Link logo and 'PHAROS' text. On the right, there are links for 'About', 'Support', and 'Log Out'. Below the navigation bar, there is a header with 'Operation Mode: Access Point' and a 'Tools' dropdown menu. The main content area has a dark teal navigation bar with tabs for 'QUICK SETUP', 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is active. Below the navigation bar, the 'Operation Mode' section is displayed. It contains the instruction 'Please select the proper operation mode according to your needs:' followed by a list of six modes, each with a radio button and a description:

- Access Point** In this mode, the AP will act as a central hub for different wireless LAN clients. Multi-SSID is also available in this mode, which supports up to 4 different SSIDs and passwords.
- Client** In client mode, the device can connect to a wired device and work as a wireless adapter to receive wireless signals from your wireless network.
- Repeater** In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners.
- Bridge** Bridge mode borrows existing wireless internet and broadcasts it using a different SSID and password. In this mode, you can set up a wireless client to connect with a root AP and a wireless AP for local wireless coverage.
- AP Router** In this mode, the device enables multiple users to share the internet. The wireless ports share the same IP address as the Ethernet WAN port to connect to the ISP. The wireless port can be regarded as a LAN port while in AP Router mode.
- AP Client Router (WISP Client)** In this mode, multiple users can share an internet connection provided by a WISP. The LAN port devices share the same IP as that assigned by the WISP to the Wireless port. While connected to a WISP, the wireless port works as a WAN port in AP Client Router mode. The Ethernet port acts as a LAN port.

At the bottom right of the form, there is a 'Next' button.



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

The screenshot shows a web interface for configuring a network device. At the top, there is a dark teal navigation bar with the following tabs: **QUICK SETUP**, **STATUS**, **NETWORK**, **WIRELESS**, **MANAGEMENT**, and **SYSTEM**. Below the navigation bar, the **LAN Settings** section is visible. It contains two input fields: "IP Address" with the value "192.168.0.254" and "Subnet Mask" with the value "255.255.255.0". At the bottom of the page, there are two buttons: "Back" and "Next".

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

**Tips:**

- 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*.

QUICK SETUP STATUS NETWORK WIRELESS MANAGEMENT SYSTEM

Wireless AP Settings

SSID: TP-LINK\_Outdoor\_BD205C

Mode: 802.11a/n

Channel Width: 20/40MHz

Channel/Frequency: Auto

Security: None

PSK Password:   Show

We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.

Distance Setting: 0 (0-27.9)km

MAXstream:  Enable ?

Back Next

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

QUICK SETUP STATUS NETWORK WIRELESS MANAGEMENT SYSTEM

Finish

Operation Mode: Access Point

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

SSID: TP-LINK\_Outdoor\_BD205C

Mode: 802.11a/n

Channel Width: 20/40MHz

Channel/Frequency: Auto

Security: None

Distance Setting: 0 km

MAXstream: Disable

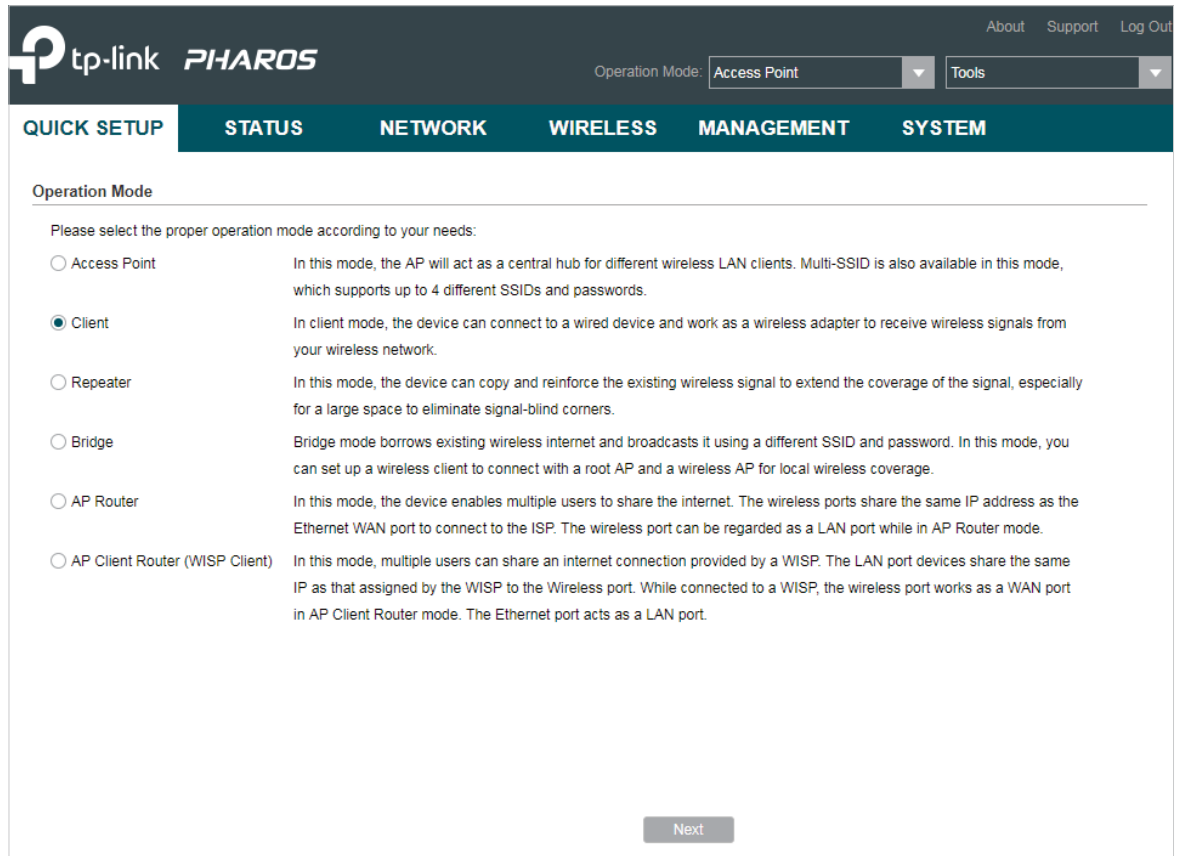
Back Finish

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*.



The screenshot shows the TP-Link PHAROS web interface. At the top, there is a navigation bar with the TP-Link logo, the product name "PHAROS", and links for "About", "Support", and "Log Out". Below the navigation bar, there is a header with tabs for "QUICK SETUP", "STATUS", "NETWORK", "WIRELESS", "MANAGEMENT", and "SYSTEM". The "QUICK SETUP" tab is active. Underneath, the "Operation Mode" section is displayed. It contains a heading "Operation Mode" and a sub-heading "Please select the proper operation mode according to your needs:". There are six radio button options, each with a description:

- Access Point: In this mode, the AP will act as a central hub for different wireless LAN clients. Multi-SSID is also available in this mode, which supports up to 4 different SSIDs and passwords.
- Client: In client mode, the device can connect to a wired device and work as a wireless adapter to receive wireless signals from your wireless network.
- Repeater: In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners.
- Bridge: Bridge mode borrows existing wireless internet and broadcasts it using a different SSID and password. In this mode, you can set up a wireless client to connect with a root AP and a wireless AP for local wireless coverage.
- AP Router: In this mode, the device enables multiple users to share the internet. The wireless ports share the same IP address as the Ethernet WAN port to connect to the ISP. The wireless port can be regarded as a LAN port while in AP Router mode.
- AP Client Router (WISP Client): In this mode, multiple users can share an internet connection provided by a WISP. The LAN port devices share the same IP as that assigned by the WISP to the Wireless port. While connected to a WISP, the wireless port works as a WAN port in AP Client Router mode. The Ethernet port acts as a LAN port.

At the bottom right of the form, there is a "Next" button.

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

The screenshot shows the 'LAN Settings' configuration page. At the top, there is a navigation bar with tabs: 'QUICK SETUP', 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is selected. Below the navigation bar, the page title is 'LAN Settings'. There are two input fields: 'IP Address' with the value '192.168.0.254' and 'Subnet Mask' with the value '255.255.255.0'. At the bottom of the page, there are two buttons: 'Back' and 'Next'.

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

The screenshot shows the 'Wireless Client Settings' configuration page. At the top, there is a navigation bar with tabs: 'QUICK SETUP', 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'WIRELESS' tab is selected. Below the navigation bar, the page title is 'Wireless Client Settings'. There are several input fields and a button: 'SSID of Remote AP' (empty), 'MAC of Remote AP' (empty), 'Mode' (802.11a/n), 'WDS' (Auto), 'Channel Width' (20/40MHz), 'Security' (None), and 'PSK Password' (empty). There is a 'Survey' button next to the SSID field and a 'Lock to AP' checkbox. Below the input fields, there is a note: 'We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.' At the bottom, there is a 'Distance Setting' field with the value '0' and a range '(0-27.9)km'. At the bottom of the page, there are two buttons: 'Back' and 'Next'.

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

### Tips:

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.

The screenshot shows the 'Wireless Client Settings' page with a table of detected wireless networks. The table has columns for BSSID, SSID, MAXtream, Device Name, SNR (dB), Signal / Noise (dBm), Channel, and Security. Below the table are buttons for Back, Refresh, Connect, and Lock to AP.

<input type="checkbox"/>	BSSID	SSID	MAXtream	Device Name	SNR (dB)	Signal / Noise (dBm)	Channel	Security
<input type="checkbox"/>	18-A6-F7-41-26-46	daisy 3	No		42	-53/-95	5180 (36)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-27-7F-6E	SR20_5G	No		50	-45/-95	5220 (44)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-17-A6-E3	EAP-Show	No		14	-81/-95	5180 (36)	WPA2-PSK
<input type="checkbox"/>	D4-61-FE-5A-2A-00	das	No		11	-85/-96	5180 (36)	WPA-PSK/WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-54-DB	deco	No		35	-61/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-57-1F	deco	No		30	-66/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-57-74	deco	No		47	-49/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-54-DB		No		37	-59/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-57-1F		No		31	-65/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-57-74		No		47	-49/-96	5200 (40)	WPA2-PSK

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](#).

The screenshot shows the 'Wireless Client Settings' page with configuration options for a selected network. The SSID of Remote AP is '7200\_5G' and the MAC of Remote AP is '50-C7-BF-01-88-1F'. The Mode is '802.11a/n', WDS is 'Auto', Channel Width is '20/40MHz', and Security is 'WPA-PSK / WPA2-PSK'. The PSK Password is masked with dots. There is a 'Survey' button and a 'Lock to AP' checkbox. A note states: 'We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.' The Distance Setting is '0' (0-27.9)km. Buttons for Back and Next are at the bottom.

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

The screenshot displays the 'Finish' configuration page. At the top, there is a navigation bar with tabs: QUICK SETUP (selected), STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. Below the navigation bar, the word 'Finish' is displayed. The main content area shows the following configuration details:

- Operation Mode: Client
- LAN IP Address: 192.168.0.254
- LAN Subnet Mask: 255.255.255.0
- SSID of Remote AP: TP-LINK\_DC91\_5G
- Mode: 802.11a/n
- WDS: Auto
- Channel Width: 20/40MHz
- Security: WPA-PSK / WPA2-PSK
- Distance Setting: 0 km

At the bottom of the page, there are two buttons: 'Back' and 'Finish'.

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

## Repeater (Range Extender)

Follow the steps below to configure the device as Repeater (Range Extender) mode:

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

The screenshot shows the TP-Link PHAROS web interface. At the top, there is a navigation bar with the TP-Link logo and 'PHAROS' text. To the right, there are links for 'About', 'Support', and 'Log Out'. Below the navigation bar, there is a header with tabs: 'QUICK SETUP', 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is active. The main content area is titled 'Operation Mode' and contains the following text: 'Please select the proper operation mode according to your needs:'. Below this text, there are seven radio button options, each with a description: 'Access Point', 'Client', 'Repeater' (which is selected), 'Bridge', 'AP Router', and 'AP Client Router (WISP Client)'. At the bottom right of the main content area, there is a 'Next' button.

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

The screenshot shows the TP-Link PHAROS web interface, specifically the 'LAN Settings' section. The navigation bar at the top is the same as in the previous screenshot. The 'QUICK SETUP' tab is active. The main content area is titled 'LAN Settings' and contains two input fields: 'IP Address:' with the value '192.168.0.254' and 'Subnet Mask:' with the value '255.255.255.0'. At the bottom of the main content area, there are two buttons: 'Back' and 'Next'.

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

**Wireless Client Settings**

SSID of Remote AP:

MAC of Remote AP:   Lock to AP

Mode: 802.11a/n

WDS: Auto

Channel Width: 20/40MHz

Security: None

PSK Password:   Show

We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.

Distance Setting: 0 (0-27.9)km

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

**Tips:**

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.

**Wireless Client Settings**

<input type="checkbox"/>	BSSID	SSID	MAXtream	Device Name	SNR (dB)	Signal / Noise (dBm)	Channel	Security
<input type="checkbox"/>	18-A6-F7-41-26-46	daisy 3	No		42	-53/-95	5180 (36)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-27-7F-6E	SR20_5G	No		50	-45/-95	5220 (44)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-17-A6-E3	EAP-Show	No		14	-81/-95	5180 (36)	WPA2-PSK
<input type="checkbox"/>	D4-61-FE-5A-2A-00	das	No		11	-85/-96	5180 (36)	WPA-PSK/WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-54-DB	deco	No		35	-61/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-57-1F	deco	No		30	-66/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-57-74	deco	No		47	-49/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-54-DB		No		37	-59/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-57-1F		No		31	-65/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-57-74		No		47	-49/-96	5200 (40)	WPA2-PSK

- 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](#).

QUICK SETUP	STATUS	NETWORK	WIRELESS	MANAGEMENT	SYSTEM
<b>Wireless Client Settings</b>					
SSID of Remote AP:		<input type="text" value="7200_5G"/>	<input type="button" value="Survey"/>		
MAC of Remote AP:		<input type="text" value="50-C7-BF-01-88-1F"/>	<input type="checkbox"/> Lock to AP		
Mode:		<input type="text" value="802.11a/n"/>			
WDS:		<input type="text" value="Auto"/>			
Channel Width:		<input type="text" value="20/40MHz"/>			
Security:		<input type="text" value="WPA-PSK / WPA2-PSK"/>			
PSK Password:		<input type="password" value="*****"/>	<input type="checkbox"/> Show		
We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.					
Distance Setting:		<input type="text" value="0"/>	<input type="text" value="(0-27.9)km"/>		
<input type="button" value="Back"/>			<input type="button" value="Next"/>		

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

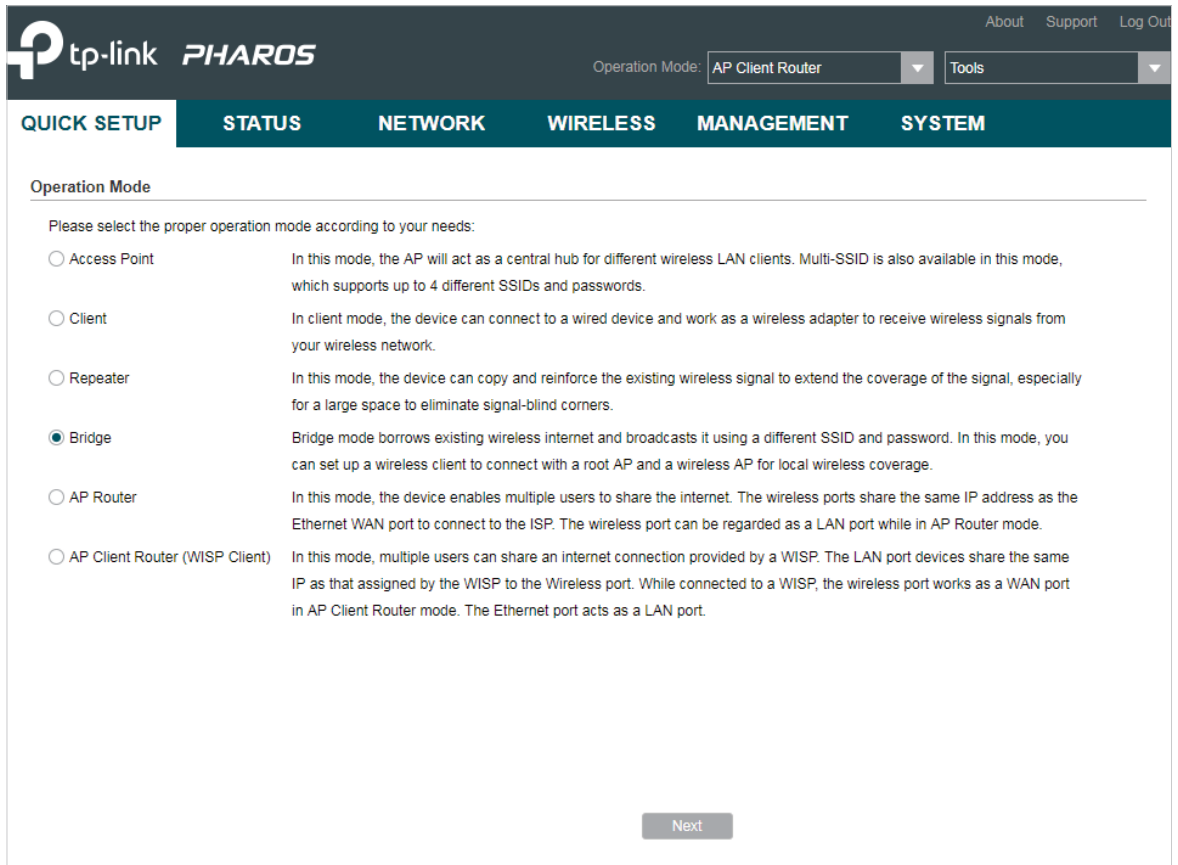
QUICK SETUP	STATUS	NETWORK	WIRELESS	MANAGEMENT	SYSTEM
<b>Finish</b>					
Operation Mode: Repeater					
IP Address: 192.168.0.254					
Subnet Mask: 255.255.255.0					
SSID of Remote AP: 7200_5G					
Mode: 802.11a/n					
WDS: Disable					
Channel Width: 20/40MHz					
Security: WPA-PSK / WPA2-PSK					
Distance Setting: 0 km					
<input type="button" value="Back"/>			<input type="button" value="Finish"/>		

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

## Bridge

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

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



The screenshot shows the TP-Link PHAROS web interface. At the top, there is a navigation bar with the TP-Link logo and 'PHAROS' text. On the right, there are links for 'About', 'Support', and 'Log Out'. Below the navigation bar, there is a header with 'Operation Mode: AP Client Router' and a 'Tools' dropdown menu. The main content area has a dark teal navigation bar with tabs for 'QUICK SETUP', 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is active. Below the navigation bar, there is a section titled 'Operation Mode' with a sub-header 'Please select the proper operation mode according to your needs:'. There are six radio button options, each with a description:

- Access Point: In this mode, the AP will act as a central hub for different wireless LAN clients. Multi-SSID is also available in this mode, which supports up to 4 different SSIDs and passwords.
- Client: In client mode, the device can connect to a wired device and work as a wireless adapter to receive wireless signals from your wireless network.
- Repeater: In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners.
- Bridge: Bridge mode borrows existing wireless internet and broadcasts it using a different SSID and password. In this mode, you can set up a wireless client to connect with a root AP and a wireless AP for local wireless coverage.
- AP Router: In this mode, the device enables multiple users to share the internet. The wireless ports share the same IP address as the Ethernet WAN port to connect to the ISP. The wireless port can be regarded as a LAN port while in AP Router mode.
- AP Client Router (WISP Client): In this mode, multiple users can share an internet connection provided by a WISP. The LAN port devices share the same IP as that assigned by the WISP to the Wireless port. While connected to a WISP, the wireless port works as a WAN port in AP Client Router mode. The Ethernet port acts as a LAN port.

At the bottom of the form, there is a 'Next' button.

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

The screenshot shows a web interface with a dark teal navigation bar at the top containing the following tabs: QUICK SETUP, STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. The 'QUICK SETUP' tab is active. Below the navigation bar, the page title is 'LAN Settings'. The main content area contains two input fields: 'IP Address' with the value '192.168.0.254' and 'Subnet Mask' with the value '255.255.255.0'. At the bottom of the page, there are two buttons: 'Back' and 'Next'.

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

The screenshot shows a web interface with a dark teal navigation bar at the top containing the following tabs: QUICK SETUP, STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. The 'WIRELESS' tab is active. Below the navigation bar, the page title is 'Wireless Client Settings'. The main content area contains several configuration options: 'SSID of Remote AP:' with an empty input field and a 'Survey' button; 'MAC of Remote AP:' with an empty input field and a 'Lock to AP' checkbox; 'Mode:' with a dropdown menu set to '802.11a/n'; 'WDS:' with a dropdown menu set to 'Auto'; 'Channel Width:' with a dropdown menu set to '20/40MHz'; 'Security:' with a dropdown menu set to 'None'; 'PSK Password:' with an empty input field and a 'Show' checkbox; a note: 'We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.'; and 'Distance Setting:' with an input field set to '0' and a range '(0-27.9)km'. At the bottom of the page, there are two buttons: 'Back' and 'Next'.

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

## Tips:

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.

The screenshot shows the 'Wireless Client Settings' page with a table of detected wireless networks. The table has columns for BSSID, SSID, MAXtream, Device Name, SNR (dB), Signal / Noise (dBm), Channel, and Security. Below the table are buttons for 'Back', 'Refresh', 'Connect', and 'Lock to AP'.

<input type="checkbox"/>	BSSID	SSID	MAXtream	Device Name	SNR (dB)	Signal / Noise (dBm)	Channel	Security
<input type="checkbox"/>	18-A6-F7-41-26-46	daisy 3	No		42	-53/-95	5180 (36)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-27-7F-6E	SR20_5G	No		50	-45/-95	5220 (44)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-17-A6-E3	EAP-Show	No		14	-81/-95	5180 (36)	WPA2-PSK
<input type="checkbox"/>	D4-61-FE-5A-2A-00	das	No		11	-85/-96	5180 (36)	WPA-PSK/WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-54-DB	deco	No		35	-61/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-57-1F	deco	No		30	-66/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-57-74	deco	No		47	-49/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-54-DB		No		37	-59/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-57-1F		No		31	-65/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-57-74		No		47	-49/-96	5200 (40)	WPA2-PSK

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](#).

The screenshot shows the 'Wireless Client Settings' page with configuration options for a selected wireless network. The options include SSID of Remote AP, MAC of Remote AP, Mode, WDS, Channel Width, Security, PSK Password, and Distance Setting. There are also buttons for 'Survey', 'Lock to AP', and 'Show'.

SSID of Remote AP:

MAC of Remote AP:   Lock to AP

Mode:

WDS:

Channel Width:

Security:

PSK Password:   Show

We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.

Distance Setting:  (0-27.9)km

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

The screenshot shows the 'Wireless AP Settings' page. At the top, there is a navigation bar with tabs: QUICK SETUP (selected), STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. Below the navigation bar, the page title is 'Wireless AP Settings'. The configuration options are as follows:

- Wireless Radio:  Enable
- SSID:
- Security:
- PSK Password:   Show

Below the password field, there is a note: "We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode."

At the bottom of the page, there are two buttons: "Back" and "Next".

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

The screenshot shows the 'Finish' page. At the top, there is a navigation bar with tabs: QUICK SETUP (selected), STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. Below the navigation bar, the page title is 'Finish'. The configuration summary is as follows:

- Operation Mode: Bridge
- IP Address: 192.168.0.254
- Subnet Mask: 255.255.255.0
- SSID of Remote AP: 7200\_5G
- Mode: 802.11a/n
- WDS: Disable
- Channel Width: 20/40MHz
- Security: WPA-PSK / WPA2-PSK
- Distance Setting: 0 km
- Wireless Radio: Enable
- SSID: TP-LINK\_Outdoor\_BD205C
- Security: WPA-PSK / WPA2-PSK

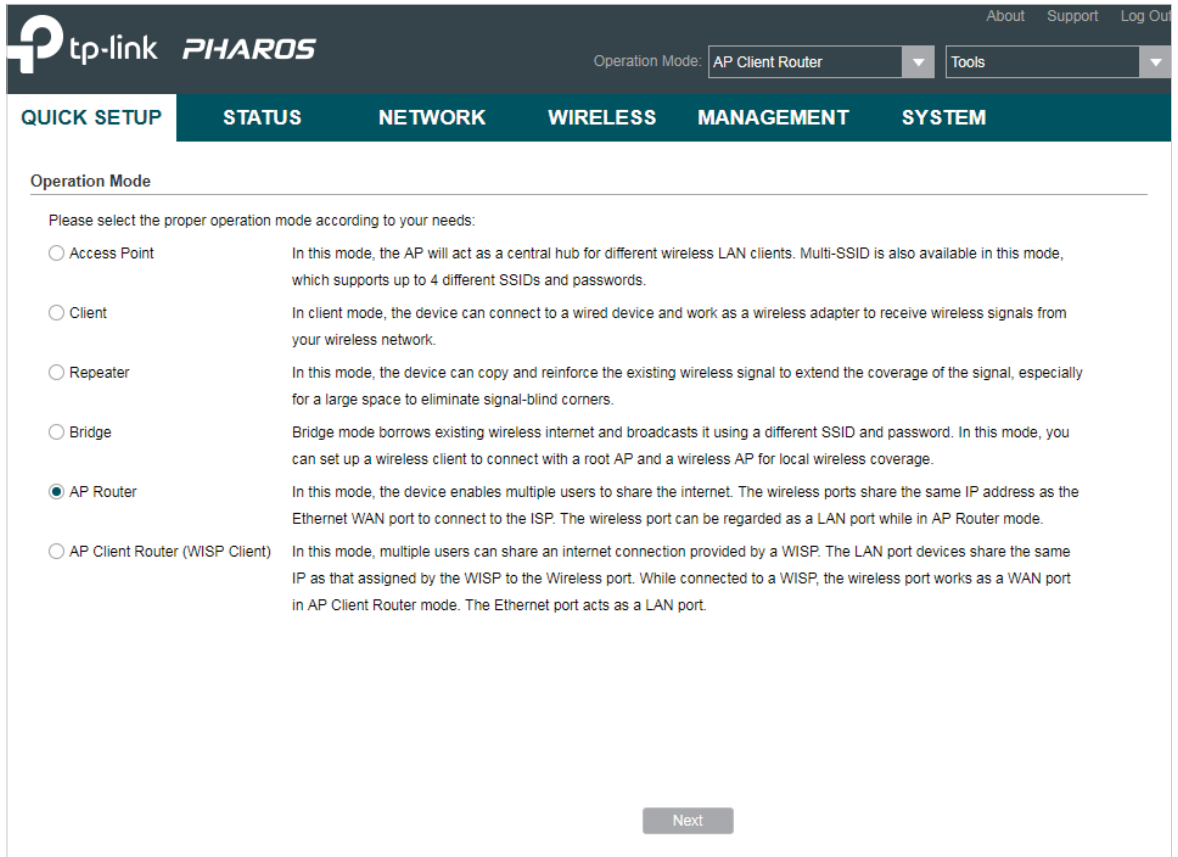
At the bottom of the page, there are two buttons: "Back" and "Finish".

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 screenshot shows the TP-Link PHAROS web interface. At the top, there is a navigation bar with the TP-Link logo, the word 'PHAROS', and links for 'About', 'Support', and 'Log Out'. Below the navigation bar, there is a header with 'Operation Mode: AP Client Router' and a 'Tools' dropdown menu. The main content area is titled 'QUICK SETUP' and has a dark teal navigation bar with tabs for 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is active. Below the navigation bar, there is a section titled 'Operation Mode' with the instruction 'Please select the proper operation mode according to your needs:'. There are six radio button options, each with a description: 'Access Point', 'Client', 'Repeater', 'Bridge', 'AP Router' (which is selected), and 'AP Client Router (WISP Client)'. A 'Next' button is located at the bottom right of the form.

tp-link PHAROS

Operation Mode: AP Client Router Tools

QUICK SETUP STATUS NETWORK WIRELESS MANAGEMENT SYSTEM

Operation Mode

Please select the proper operation mode according to your needs:

- Access Point In this mode, the AP will act as a central hub for different wireless LAN clients. Multi-SSID is also available in this mode, which supports up to 4 different SSIDs and passwords.
- Client In client mode, the device can connect to a wired device and work as a wireless adapter to receive wireless signals from your wireless network.
- Repeater In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners.
- Bridge Bridge mode borrows existing wireless internet and broadcasts it using a different SSID and password. In this mode, you can set up a wireless client to connect with a root AP and a wireless AP for local wireless coverage.
- AP Router In this mode, the device enables multiple users to share the internet. The wireless ports share the same IP address as the Ethernet WAN port to connect to the ISP. The wireless port can be regarded as a LAN port while in AP Router mode.
- AP Client Router (WISP Client) In this mode, multiple users can share an internet connection provided by a WISP. The LAN port devices share the same IP as that assigned by the WISP to the Wireless port. While connected to a WISP, the wireless port works as a WAN port in AP Client Router mode. The Ethernet port acts as a LAN port.

Next

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

The screenshot shows a web interface for configuring a WAN connection. At the top, there is a navigation bar with tabs: **QUICK SETUP**, **STATUS**, **NETWORK**, **WIRELESS**, **MANAGEMENT**, and **SYSTEM**. Below the navigation bar, the page title is **WAN Connection Type**. The main content area contains the following text and options:

Select the connection type of WAN port according to your needs.:

- PPPoE - For this connection, you need to get the account name and password from your ISP.
- Dynamic IP - When connecting to the WAN, your router gets an IP address assigned by the DHCP server of your ISP.
- Static IP - With this type of connection, the device uses a permanent, static IP address assigned by your ISP.

At the bottom of the page, there are two buttons: **Back** and **Next**.

The device supports three types of the WAN connection, including *PPPoE*, *Dynamic IP* and *Static IP*. You can contact with 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*.

The screenshot shows a web interface with a dark teal navigation bar at the top containing the following tabs: QUICK SETUP, STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. The 'QUICK SETUP' tab is currently selected. Below the navigation bar, the page title is 'WAN Settings'. The main content area contains three input fields: 'User Name:' followed by a text box, 'Password:' followed by a text box and a 'Show' checkbox, and 'Confirm Password:' followed by a text box and a 'Show' checkbox. At the bottom of the page, there are two buttons: 'Back' and '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*.

The screenshot shows a web-based configuration interface for a network device. At the top, there is a navigation bar with six tabs: **QUICK SETUP**, **STATUS**, **NETWORK**, **WIRELESS**, **MANAGEMENT**, and **SYSTEM**. The **QUICK SETUP** tab is currently selected. Below the navigation bar, the page title is **WAN Settings**. The main content area contains five input fields, each with a label and a text box containing the value **0.0.0.0**:

- IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Default Gateway: 0.0.0.0
- Primary DNS: 0.0.0.0
- Secondary DNS: 0.0.0.0 (Optional)

At the bottom of the form, there are two buttons: **Back** and **Next**.

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

### Tips:

- 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*.

The screenshot shows the 'Wireless AP Settings' page. At the top, there is a navigation bar with tabs: QUICK SETUP (selected), STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. Below the navigation bar, the page title is 'Wireless AP Settings'. The configuration fields are as follows:

- SSID: TP-LINK\_Outdoor\_BD205C
- Mode: 802.11a/n
- Channel Width: 20/40MHz
- Channel/Frequency: Auto
- Security: None
- PSK Password: (empty field) with a 'Show' checkbox.
- A note: 'We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.'
- Distance Setting: 0 (0-27.9)km
- MAXstream:  Enable ?

At the bottom of the page, there are two buttons: 'Back' and 'Next'.

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

The screenshot shows the 'Finish' page. At the top, there is a navigation bar with tabs: QUICK SETUP (selected), STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. Below the navigation bar, the page title is 'Finish'. The configuration summary is as follows:

- Operation Mode: AP Router
- WAN Connection Type: Static IP
  - IP Address: 192.168.2.10
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.2.1
  - Primary DNS: 192.168.0.3
  - Secondary DNS: 192.168.1.3
- SSID: TP-LINK\_Outdoor\_BD205C
- Mode: 802.11a/n
- Channel Width: 20/40MHz
- Security: None
- Distance Setting: 0 km
- MAXstream: Disable

At the bottom of the page, there are two buttons: 'Back' and 'Finish'.

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 screenshot shows the TP-Link PHAROS web interface. At the top, there is a navigation bar with the TP-Link logo, the product name 'PHAROS', and links for 'About', 'Support', and 'Log Out'. Below the navigation bar, there is a header with 'Operation Mode: AP Client Router' and a 'Tools' dropdown menu. The main content area is titled 'QUICK SETUP' and has a dark teal navigation bar with tabs for 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is active. Below the navigation bar, there is a section titled 'Operation Mode' with the instruction 'Please select the proper operation mode according to your needs:'. There are six radio button options, each with a description: 'Access Point', 'Client', 'Repeater', 'Bridge', 'AP Router', and 'AP Client Router (WISP Client)'. The 'AP Client Router (WISP Client)' option is selected. At the bottom right of the form, there is a 'Next' button.

Operation Mode	Description
<input type="radio"/> Access Point	In this mode, the AP will act as a central hub for different wireless LAN clients. Multi-SSID is also available in this mode, which supports up to 4 different SSIDs and passwords.
<input type="radio"/> Client	In client mode, the device can connect to a wired device and work as a wireless adapter to receive wireless signals from your wireless network.
<input type="radio"/> Repeater	In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners.
<input type="radio"/> Bridge	Bridge mode borrows existing wireless internet and broadcasts it using a different SSID and password. In this mode, you can set up a wireless client to connect with a root AP and a wireless AP for local wireless coverage.
<input type="radio"/> AP Router	In this mode, the device enables multiple users to share the internet. The wireless ports share the same IP address as the Ethernet WAN port to connect to the ISP. The wireless port can be regarded as a LAN port while in AP Router mode.
<input checked="" type="radio"/> AP Client Router (WISP Client)	In this mode, multiple users can share an internet connection provided by a WISP. The LAN port devices share the same IP as that assigned by the WISP to the Wireless port. While connected to a WISP, the wireless port works as a WAN port in AP Client Router mode. The Ethernet port acts as a LAN port.

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

The screenshot shows a web interface for configuring a WAN connection. At the top, there is a navigation bar with tabs: **QUICK SETUP**, **STATUS**, **NETWORK**, **WIRELESS**, **MANAGEMENT**, and **SYSTEM**. Below the navigation bar, the page title is **WAN Connection Type**. The main content area contains the following text and options:

Select the connection type of WAN port according to your needs.:

- PPPoE - For this connection, you need to get the account name and password from your ISP.
- Dynamic IP - When connecting to the WAN, your router gets an IP address assigned by the DHCP server of your ISP.
- Static IP - With this type of connection, the device uses a permanent, static IP address assigned by your ISP.

At the bottom of the page, there are two buttons: **Back** and **Next**.

The device supports types, *PPPoE*, *Dynamic IP* and *Static IP* for the WAN connection. You can contact with 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*.

The screenshot shows a web interface with a dark teal navigation bar at the top containing the following tabs: QUICK SETUP, STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. The 'QUICK SETUP' tab is currently selected. Below the navigation bar, the page title is 'WAN Settings'. The main content area contains three input fields: 'User Name:' followed by a text box, 'Password:' followed by a text box and a 'Show' checkbox, and 'Confirm Password:' followed by a text box and a 'Show' checkbox. At the bottom of the page, there are two buttons: 'Back' and '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*.

QUICK SETUP STATUS NETWORK WIRELESS MANAGEMENT SYSTEM

WAN Settings

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0 (Optional)

Back Next

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

QUICK SETUP STATUS NETWORK WIRELESS MANAGEMENT SYSTEM

Wireless Client Settings

SSID of Remote AP: [input] Survey

MAC of Remote AP: [input] Lock to AP

Mode: 802.11a/n

WDS: Auto

Channel Width: 20/40MHz

Security: None

PSK Password: [input] Show

We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.

Distance Setting: 0 (0-27.9)km

Back Next

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

**Tips:**

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.

<input type="checkbox"/>	BSSID	SSID	MAXstream	Device Name	SNR (dB)	Signal / Noise (dBm)	Channel	Security
<input type="checkbox"/>	18-A6-F7-41-26-46	daisy 3	No		42	-53/-95	5180 (36)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-27-7F-6E	SR20_5G	No		50	-45/-95	5220 (44)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-17-A6-E3	EAP-Show	No		14	-81/-95	5180 (36)	WPA2-PSK
<input type="checkbox"/>	D4-61-FE-5A-2A-00	das	No		11	-85/-96	5180 (36)	WPA-PSK/WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-54-DB	deco	No		35	-61/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-57-1F	deco	No		30	-66/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	50-C7-BF-48-57-74	deco	No		47	-49/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-54-DB		No		37	-59/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-57-1F		No		31	-65/-96	5200 (40)	WPA2-PSK
<input type="checkbox"/>	56-C7-BF-48-57-74		No		47	-49/-96	5200 (40)	WPA2-PSK

- 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](#).

SSID of Remote AP:    
 MAC of Remote AP:   Lock to AP  
 Mode:   
 WDS:   
 Channel Width:   
 Security:   
 PSK Password:   Show  
 We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.  
 Distance Setting:  (0-27.9)km

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

The screenshot shows the 'Wireless AP Settings' page in a web interface. At the top, there is a navigation bar with tabs: QUICK SETUP (selected), STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. Below the navigation bar, the page title is 'Wireless AP Settings'. The main content area contains the following configuration options:

- Wireless Radio:  Enable
- SSID: TP-LINK\_Outdoor\_BD205C
- Security: WPA-PSK / WPA2-PSK (dropdown menu)
- PSK Password: [masked with dots]  Show

Below these fields, there is a note: "We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode." At the bottom of the page, there are two buttons: 'Back' and 'Next'.

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

The screenshot shows the 'Finish' page in the web interface. At the top, there is a navigation bar with tabs: QUICK SETUP (selected), STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. Below the navigation bar, the page title is 'Finish'. The main content area displays the following configuration summary:

- Operation Mode: AP Client Router (WISP Client)
- WAN Connection Type: Static IP
  - IP Address: 192.168.2.10
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.2.1
  - Primary DNS: 192.168.0.1
  - Secondary DNS: 192.168.1.2
- SSID of Remote AP: 7200\_5G
  - Mode: 802.11a/n
  - WDS: Disable
  - Channel Width: 20/40MHz
  - Security: WPA-PSK / WPA2-PSK
- Distance Setting: 0 km
- Wireless Radio: Enable
  - SSID: TP-LINK\_Outdoor\_BD205C
  - Security: WPA-PSK / WPA2-PSK

At the bottom of the page, there are two buttons: 'Back' and 'Finish'.

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*

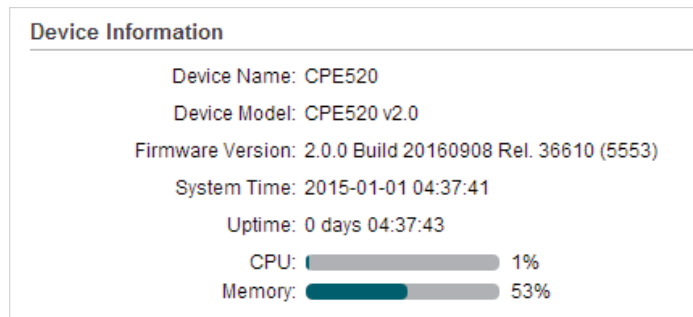
*3.11 Monitor Routes*

*3.12 Monitor DHCP Clients*

*3.13 Monitor Dynamic WAN*

## 3.1 View the Device Information

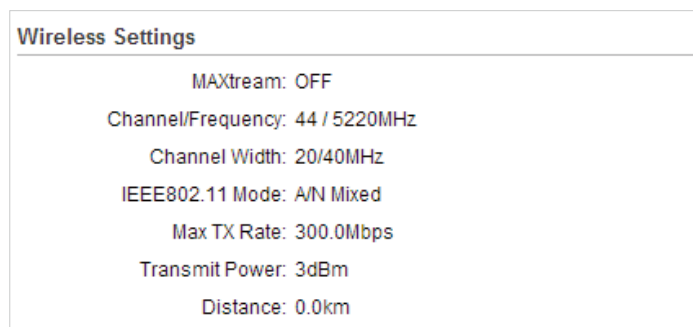
Go to the **STATUS** page. In the **Device Information** section, you can view the basic information of the device. To configure the device information, refer to [7. Configure the System](#).



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

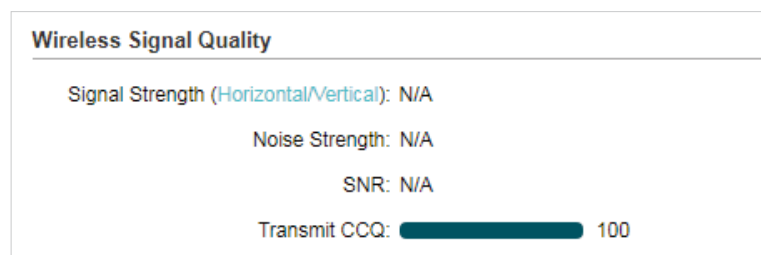
Go to the **STATUS** page. In the **Wireless Settings** section, you can view the parameters of the wireless network created by the device. To configure the parameters, refer to [5. Configure the Wireless Parameters](#).



<b>MAXtream</b>	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.  <b>Note:</b> MAXtream Technology is only compatible with Pharos series products. Working with products from other manufacturer will cause network fault.
<b>Channel/ Frequency</b>	Displays the channel and frequency which are currently used by the device.
<b>Channel Width</b>	Displays the channel width which is currently used by the device.
<b>IEEE802.11 Mode</b>	Displays the IEEE802.11 protocol currently used by the device.
<b>Max TX Rate</b>	Displays the maximum data rate of the device during the sending of the wireless packets.
<b>Transmit Power</b>	Displays the transmit power which is currently used by the device.
<b>Distance</b>	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, you can view the current signal quality of the upstream wireless network. It is only applicable for the Client, Repeater (Range Extender), Bridge and AP Client Router (WISP Client) modes.

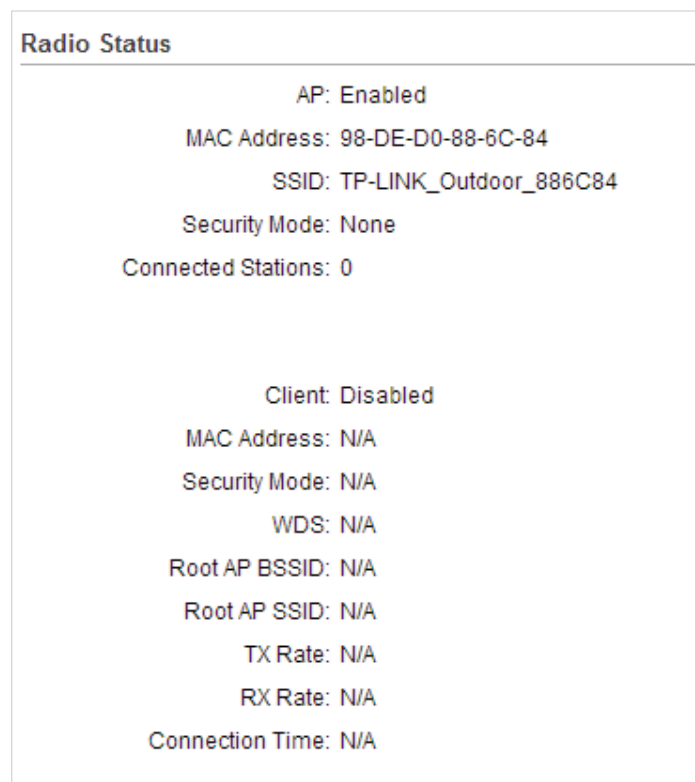


<b>Signal Strength (Horizontal/ Vertical)</b>	Displays the received wireless signal strength of the root AP.
<b>Noise Strength</b>	Displays the received environmental noise from wireless interference on the operating frequency.

<b>SNR</b>	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.
<b>Transmit CCQ</b>	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, you can view the radio status of the device.



<b>AP</b>	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.
<b>MAC Address</b>	Displays the MAC address of the wireless interface connected to the clients.
<b>SSID</b>	Displays the wireless network name (SSID) created by the device.

Security Mode	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.
Connected Stations	Displays the number of the connected stations.
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	Displays the security mode you've selected for your wireless network. There are three security modes: WPA-PSK, WPA and WEP. The security mode which is set on the device should be the same as that on the root AP.
WDS	<p>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.</p> <p><b>Enable:</b> Forward data frames using four address fields.</p> <p><b>Disable:</b> Forward data frames using three address fields.</p> <p><b>Auto:</b> The device automatically negotiates the wireless data frame structure (three or four address fields) with the root AP. The selection of Auto is recommended.</p>
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, you can view the LAN information of the device. To configure the LAN settings, refer to [4. Configure the Network](#).

LAN
MAC Address: 30-B5-C2-BD-04-6E
IP Address: 192.168.0.210
Subnet Mask: 255.255.255.0
Port0: Unplugged
Port1: 100Mbps - FD

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.

## 3.6 View the WAN Settings

Go to the **STATUS** page. In the **WAN** section, you can view the WAN information of the device. To configure the LAN settings, refer to [4. Configure the Network](#).

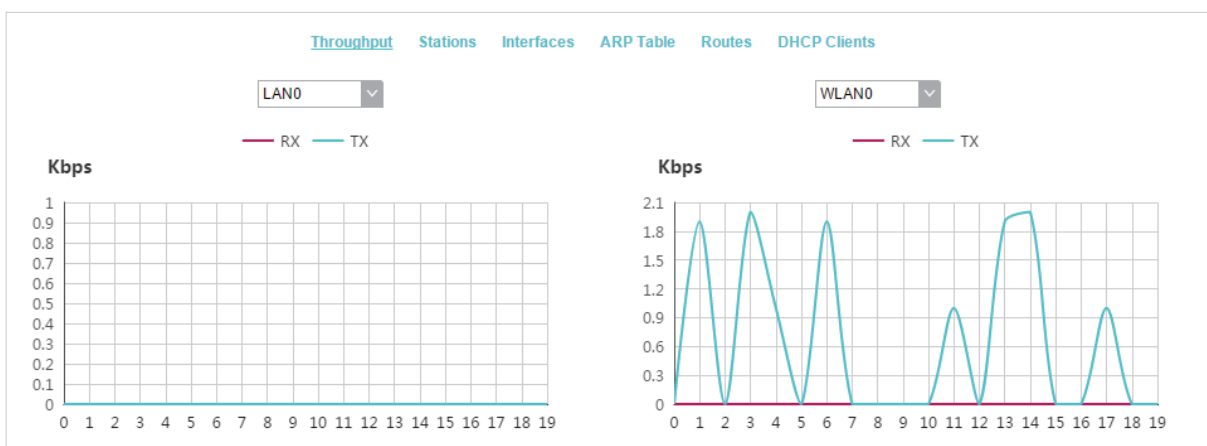
WAN
Connection Type: Dynamic
MAC Address: 30-B5-C2-BD-04-6F
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
DNS Server: 0.0.0.0

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.

### 3.7 Monitor Throughput

Go to the **STATUS** page. In the **Monitor** section, select *Throughput* and you can monitor the current data traffic of specified interfaces including LAN, WAN and BRIDGE.



### 3.8 Monitor Stations

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

MAC Address	Device Name	Associated SSID	Signal / Noise(dBm)	CCQ (%)	Negotiated Rate(Mbps)	Data TX / RX (kbps)	Distance (km)	IP Address	Connection Time
00-0A-EB-21-01-10	Jim	TP-LINK_Out...	-50/-105	93	300.0	169/3962	0.00	192.168.0.102	0 days 00:04:30

Auto Refresh

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. The values of Chain0 and Chain1 can be displayed separately and can be displayed unitedly.

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.
Negotiate Rate (Mbps)	Displays the station's data rates of the last transmitted packets.
Data TX/RX (kbps)	Displays the station's average data rates of the transmitted and received packets over the connection time.
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.

### 3.9 Monitor Interfaces

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

Monitor							
Throughput Stations Interfaces ARP Table Routes DHCP Clients							
Interface	MAC	IP Address	MTU	RX packets	RX Bytes	TX packets	TX Bytes
LAN0	98-DE-D0-88-6C-84	0.0.0.0	1500	0	0	0	0
LAN1	98-DE-D0-88-6C-84	0.0.0.0	1500	20945	1M	21169	20M
BRIDGE	98-DE-D0-88-6C-84	192.168.0.254	1500	11819	1M	21170	20M
WLAN0	98-DE-D0-88-6C-84	0.0.0.0	1500	0	0	5321	1M

Auto Refresh

Interface	Displays the interface of the device.
MAC	Displays the MAC address of the interface.
IP Address	Displays the IP 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.



<b>TX packets</b>	Displays the total amount of packets sent by the interface after the device is powered on.
<b>TX Bytes</b>	Displays the total amount of data (in bytes) sent by the interface after the device is powered on.
<b>Auto Refresh</b>	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 you can 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.

Monitor		
<a href="#">Throughput</a> <a href="#">Stations</a> <a href="#">Interfaces</a> <a href="#">ARP Table</a> <a href="#">Routes</a> <a href="#">DHCP Clients</a>		
IP Address	MAC	Interface
192.168.0.200	00-19-66-35-E1-B0	BRIDGE
192.168.0.16	00-0A-EB-13-23-7B	BRIDGE
192.168.0.61	F4-F2-6D-C3-28-62	BRIDGE
169.254.60.119	DC-9B-9C-D3-17-61	BRIDGE

Auto Refresh

<b>IP Address</b>	Displays the IP address of the corresponding ARP entry.
<b>MAC</b>	Displays the MAC address of the corresponding ARP entry.
<b>Interface</b>	Displays the interface connected to the device.
<b>Auto Refresh</b>	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 you can monitor the routing entries recorded by the device.

Routing table is used for the device to decide the interface to forward the packets.

Monitor			
<a href="#">Throughput</a> <a href="#">Stations</a> <a href="#">Interfaces</a> <a href="#">ARP Table</a> <a href="#">Routes</a> <a href="#">DHCP Clients</a>			
Destination	Gateway	SubnetMask	Interface
192.168.0.0	0.0.0.0	255.255.255.0	BRIDGE

Auto Refresh

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.
Auto Refresh	Enable or disable Auto Refresh. With this feature enabled, the table will refresh automatically.

## 3.12 Monitor DHCP Clients

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

<a href="#">Throughput</a> <a href="#">Stations</a> <a href="#">Interfaces</a> <a href="#">ARP Table</a> <a href="#">Routes</a> <a href="#">DHCP Clients</a> <a href="#">Dynamic WAN</a>			
Client Name	MAC Address	Assigned IP	Lease Time
Jim	00-0A-EB-21-01-10	192.168.0.102	0 days 01:57:57

Auto Refresh

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 you can monitor the WAN connection status of the device.

**Monitor**

[Throughput](#)   [Stations](#)   [Interfaces](#)   [ARP Table](#)   [Routes](#)   [DHCP Clients](#)   [Dynamic WAN](#)

**DHCP Status**

<p>Status: <b>Disconnected</b></p> <p>IP Address: 0.0.0.0</p> <p>Subnet Mask: 0.0.0.0</p> <p>Gateway IP: 0.0.0.0</p>	<p>Primary DNS: 0.0.0.0</p> <p>Secondary DNS: 0.0.0.0</p> <p>Connection Uptime: 0 days 00:00:00</p>
	<p><a href="#">Obtain</a>   <a href="#">Release</a></p>

Auto Refresh

<b>Status</b>	Displays the status of the WAN connection.
<b>IP Address</b>	Displays the IP address of the WAN.
<b>Subnet Mask</b>	Displays the subnet mask of the WAN.
<b>Gateway IP</b>	Displays the gateway address of the device.
<b>Primary DNS</b>	Displays the primary DNS of the device.
<b>Secondary DNS</b>	Displays the secondary DNS of the device.
<b>Connection Uptime</b>	Displays the time that the latest WAN connection lasts.
<b>Obtain</b>	Click <i>Obtain</i> to obtain the WAN IP address from the upstream device.
<b>Release</b>	Click <i>Release</i> to release the WAN IP address.
<b>Auto Refresh</b>	Enable or disable Auto Refresh. With this feature enabled, the table will refresh automatically.

# 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.

The screenshot shows the WAN configuration interface. At the top, the 'Connection Type' is set to 'Dynamic'. Below this, there is an 'Advanced Settings' section with the following fields: 'MTU Size' (1500), 'Use These DNS Servers' (checked 'Enable'), 'Primary DNS' (0.0.0.0), 'Secondary DNS' (0.0.0.0), 'WAN MAC Address' (30-B5-C2-BD-02-2F) with a 'Restore to Factory MAC' button, and 'Your PC's MAC Address' (00-19-66-35-E1-B0) with a 'Clone PC's MAC' button. An 'Apply' button is located at the bottom right.

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.

### ■ 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.

The screenshot shows the WAN configuration interface with 'Connection Type' set to 'Static'. The main configuration fields are: 'IP Address' (0.0.0.0), 'Netmask' (0.0.0.0), 'Gateway IP' (0.0.0.0), 'Primary DNS' (0.0.0.0), and 'Secondary DNS' (0.0.0.0). The 'Advanced Settings' section is expanded, showing 'MTU Size' (1500), 'WAN MAC Address' (30-B5-C2-BD-02-2F) with a 'Restore to Factory MAC' button, and 'Your PC's MAC Address' (00-19-66-35-E1-B0) with a 'Clone PC's MAC' button. An 'Apply' button is at the bottom right.

---

#### IP address

Enter the IP address provided by your ISP.

---

<b>Netmask</b>	Enter the netmask provided by your ISP. Normally use 255.255.255.0.
<b>Gateway IP</b>	Enter the gateway IP address provided by your ISP.
<b>Primary DNS</b>	Enter the DNS IP address provided by your ISP.
<b>Secondary DNS</b>	Enter alternative DNS IP address if your ISP provides it.
<b>MTU Size</b>	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.
<b>WAN MAC Address</b>	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 <i>Restore Factory MAC</i> to restore the MAC address of WAN port to the factory default value.
<b>Your PC's MAC Address</b>	Displays the MAC address of the PC that is managing the router. Some ISPs require that you should register the MAC address of your PC. If the MAC address is required, you can click <i>Clone PC's MAC</i> 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.

The screenshot shows the WAN configuration page. At the top, the title is "WAN". Below it, the "Connection Type" is set to "Dynamic". An "Advanced Settings" section is expanded, showing the following fields and buttons:

- MTU Size: 1500
- Use These DNS Servers:  Enable
- Primary DNS: 0.0.0.0
- Secondary DNS: 0.0.0.0
- WAN MAC Address: 30-B5-C2-BD-02-2F (with a "Restore to Factory MAC" button)
- Your PC's MAC Address: 00-19-66-35-E1-B0 (with a "Clone PC's MAC" button)

An "Apply" button is located at the bottom right of the configuration area.

## 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.

<b>Use These DNS Servers</b>	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.
<b>Primary DNS</b>	Enter the DNS IP address provided by your ISP.
<b>Secondary DNS</b>	Enter another DNS IP address provided by your ISP.
<b>WAN MAC Address</b>	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 <i>Restore Factory MAC</i> to restore the MAC address of WAN port to the factory default value.
<b>Your PC's MAC Address</b>	Displays the MAC address of the PC that is managing the router. Some ISPs require that you should register the MAC address of your PC. If the MAC address is required, you can click <i>Clone PC's MAC</i> 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.

The screenshot shows the WAN configuration interface. At the top, the title is "WAN". Below it, there are several configuration fields:

- Connection Type:** A dropdown menu set to "PPPoE". To its right are "Connect" and "Disconnect" buttons.
- User Name:** An empty text input field.
- Password:** An empty text input field with a "Show" checkbox to its right.
- Connection Mode:** A dropdown menu set to "Automatic".
- Second Connection:** A dropdown menu set to "disabled".

Below these fields is an "Advanced Settings" section, which is expanded. It contains the following fields and options:

- MTU Size:** A text input field containing "1480".
- Service Name:** An empty text input field.
- AC Name:** An empty text input field.
- Detect Interval:** A text input field containing "0" followed by "seconds".
- Use ISP-Specified IP:** A checkbox that is checked, with the label "Enable".
- ISP-Specified IP:** A text input field containing "0.0.0.0".
- Use These DNS Servers:** A checkbox that is checked, with the label "Enable".
- Primary DNS:** A text input field containing "0.0.0.0".
- Secondary DNS:** A text input field containing "0.0.0.0".
- WAN MAC Address:** A text input field containing "30-B5-C2-BD-02-2F". To its right is a "Restore to Factory MAC" button.
- Your PC's MAC Address:** A text input field containing "00-19-66-35-E1-B0". To its right is a "Clone PC's MAC" button.

At the bottom right of the form is an "Apply" button.

<b>User Name</b>	Enter the User Name that is provided by your ISP.
------------------	---

Password	Enter the Password that is provided by your ISP.																					
<b>Connection Mode</b>	<p>Select the Connection Mode.</p> <ul style="list-style-type: none"> <li> <b>On Demand</b> <p>You can 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. Users those pay by time for their internet access can choose this mode to save their internet-access fee.</p> <div data-bbox="742 734 1284 828" data-label="Form"> <table border="1"> <tr> <td>Connection Mode:</td> <td>On Demand</td> <td>▼</td> </tr> <tr> <td>Idle Time:</td> <td>15</td> <td>minutes</td> </tr> </table> </div> </li> <li> <b>Automatic</b> <p>Connect automatically after the device is disconnected. Users those are charged a flat monthly fee can choose this mode.</p> </li> <li> <b>Time-based</b> <p>You can 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. Users those need to control the time period of internet access can choose this mode.</p> <div data-bbox="778 1209 1248 1348" data-label="Form"> <table border="1"> <tr> <td>Connection Mode:</td> <td>Time-based</td> <td>▼</td> </tr> <tr> <td>From(HH:MM):</td> <td>00:00</td> <td></td> </tr> <tr> <td>To(HH:MM):</td> <td>23:59</td> <td></td> </tr> </table> </div> </li> <li> <b>Manual</b> <p>You can 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 <i>Connect</i> 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. Users charged by time for their internet access can choose this mode to save their internet-access fee.</p> <div data-bbox="737 1738 1289 1832" data-label="Form"> <table border="1"> <tr> <td>Connection Mode:</td> <td>Manual</td> <td>▼</td> </tr> <tr> <td>Idle Time:</td> <td>15</td> <td>minutes</td> </tr> </table> </div> </li> </ul>	Connection Mode:	On Demand	▼	Idle Time:	15	minutes	Connection Mode:	Time-based	▼	From(HH:MM):	00:00		To(HH:MM):	23:59		Connection Mode:	Manual	▼	Idle Time:	15	minutes
Connection Mode:	On Demand	▼																				
Idle Time:	15	minutes																				
Connection Mode:	Time-based	▼																				
From(HH:MM):	00:00																					
To(HH:MM):	23:59																					
Connection Mode:	Manual	▼																				
Idle Time:	15	minutes																				



Second Connection	<p>If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, you can activate this secondary connection.</p> <p><b>Disable:</b> The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.</p> <p><b>Dynamic IP:</b> Use dynamic IP address to connect to the local area network provided by ISP.</p> <p><b>Static IP:</b> Use static IP address to connect to the local area network provided by ISP.</p>
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.
Service Name	Specify the Service Name provided by your ISP. Please keep it empty if your ISP doesn't provide the name.
AC Name	Specify the AC Name provided by your ISP. Please keep it empty if your ISP doesn't provide the name.
Detect Internal	Specify the Detect Interval. The default value is 0. You can 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 <i>Restore Factory MAC</i> 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 router. You can click <i>Clone PC's MAC</i> 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

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.

WAN

Connection Type: L2TP

Server IP/Name:

User Name:

Password:   Show

Connection Mode: Automatic

Second Connection: Dynamic

IPv6:  Enable

Advanced Settings

MTU Size:

WAN MAC Address:

Your PC's MAC Address:

Specify the parameters below and click *Connect*:

<b>Server IP/Name</b>	Enter the server IP address or the domain name provided by your ISP.
<b>User Name</b>	Enter the User Name provided by your ISP. This field is case-sensitive.
<b>Password</b>	Enter the Password provided by your ISP. This field is case-sensitive.

---

## Connection Mode

Select the Connection Mode.

- **On Demand**

You can 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. Users those pay by time for their internet access can choose this mode to save their internet-access fee.



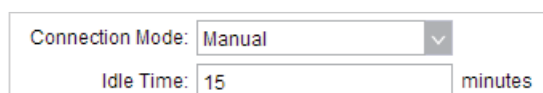
Connection Mode: On Demand    
Idle Time: 15  minutes

- **Automatic**

Connect automatically after the device is disconnected. Users those are charged a flat monthly fee can choose this mode.

- **Manual**

You can 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. Users charged by time for their internet access can choose this mode to save their internet-access fee.



Connection Mode: Manual    
Idle Time: 15  minutes

---

## Second Connection

If your ISP provides a Connection type such as Dynamic/Static IP to connect to a local area network, you can 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.

---

## 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.

---

**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 router. Some ISPs require that you should register the MAC address of your PC. If the MAC address is required, you can click *Clone PC's MAC* to set the WAN MAC address the same as your management PC's MAC.

2. 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.

The screenshot shows the LAN configuration interface. It includes the following fields and options:

- Connection Type: Static (dropdown menu)
- IP Address: 192.168.0.210
- Netmask: 255.255.255.0
- Gateway IP: 0.0.0.0
- Primary DNS: 0.0.0.0
- Secondary DNS: 0.0.0.0
- IGMP Proxy:  Enable
- DHCP Server:  Enable

An **Apply** button is located at the bottom right of the configuration area.

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

**LAN** ⌵

Connection Type: Static ▼

IP Address:

Netmask:

Gateway IP:

Primary DNS:

Secondary DNS:

MTU Size:

IGMP Proxy:  Enable

DHCP Server:  Enable

**DHCP Server**

Start IP Address:  End IP Address:

Default Gateway:  Default Domain:

Primary DNS:  Secondary DNS:

Lease Time:  minutes

**Address Reservation**

+ Add ⚙ Edit − Delete

	Enable	MAC Address	Reserved IP Address
	<input type="checkbox"/>	--	--

IPv6:  Enable

**IP address** Enter the LAN IP address of your device. By default, it is 192.168.0.254.

**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. Please consult your ISP if you don't know the DNS value. The factory default setting is 0.0.0.0.

**Secondary DNS** Enter the secondary DNS IP address of alternative DNS server if your ISP two DNS servers. The factory default setting is 0.0.0.0.

**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.

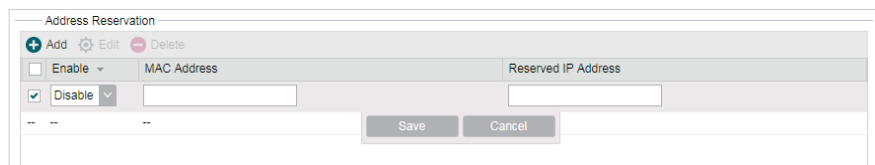
**IGMP Proxy** Enable or disable IGMP (Internet Group Management Protocol) Proxy. IGMP proxy is used to process the multicast stream in the network. It normally works for IPTV service.

**DHCP Server** Enable or disable the DHCP server function. With this function enabled, the built-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.
Secondary DNS	Enter the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0.
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 you can 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

### Dynamic

**LAN** ⌵

Connection Type: Dynamic

Fallback IP:  Enable

DHCP Fallback IP:

DHCP Fallback Mask:

Primary DNS:

Secondary DNS:

IGMP Proxy:  Enable

Apply

<b>Fallback IP</b>	Enable or disable the Fallback IP. When the device doesn't find DHCP server, it will use the fallback IP as the LAN IP address.
<b>DHCP Fallback IP</b>	Specify the fallback IP for the device. By default, it is 192.168.0.254.
<b>DHCP Fallback Mask</b>	Specify the fallback netmask for the device.
<b>Primary DNS</b>	Enter the DNS IP address for the LAN. By default, it is 0.0.0.0.
<b>Secondary DNS</b>	Enter the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0.
<b>IGMP Proxy</b>	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.

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.

**LAN** ⌵

Connection Type:  ⌵

IP Address:

Netmask:

IGMP Proxy:  Enable

DHCP Server:  Enable

**DHCP Server**

Start IP Address:       End IP Address:

Default Gateway:       Default Domain:

Primary DNS:       Secondary DNS:

Lease Time:  minutes

**Address Reservation**

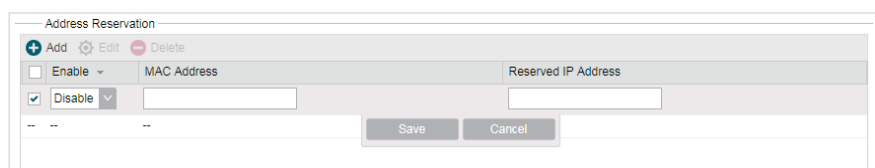
+ Add   ⚙ Edit   - Delete

	Enable	MAC Address	Reserved IP Address
	<input type="checkbox"/>	--	--

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

<b>IP address</b>	Enter the LAN IP address of your device. By default, it is 192.168.0.254.
<b>Netmask</b>	Enter the Netmask provided by your ISP. Normally use 255.255.255.0.

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.
DHCP Server	Enable or disable the DHCP server function. With this function enabled, the built-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.
Secondary DNS	Enter the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0.
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 you can 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*.

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

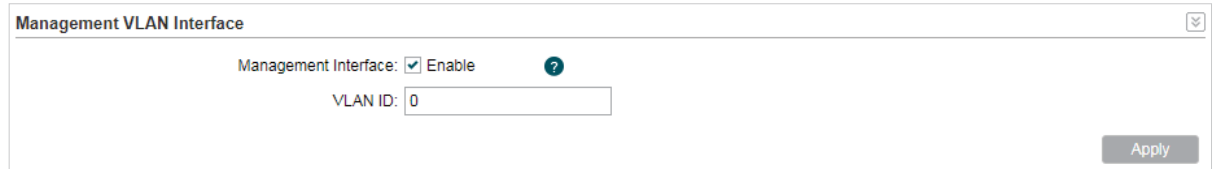
## 4.3 Configure Management VLAN

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 Interface

Management Interface:  Enable

VLAN ID:

Apply

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:

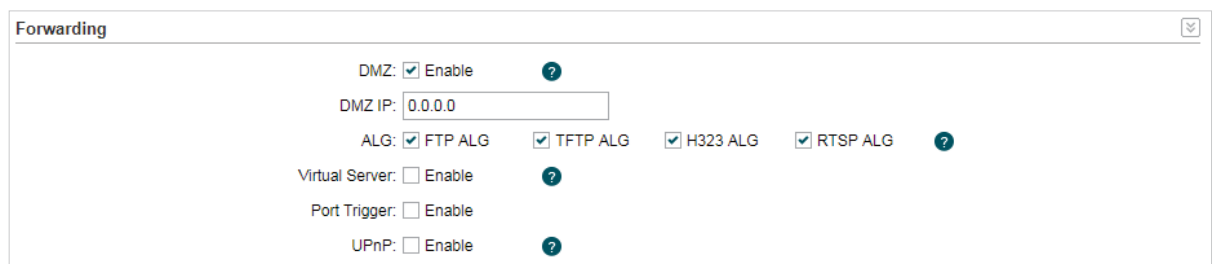
Forwarding submenu is only available in AP Router mode and AP client Router (WISP client) mode.

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*.



Forwarding

DMZ:  Enable

DMZ IP:

ALG:  FTP ALG  TFTP ALG  H323 ALG  RTSP ALG

Virtual Server:  Enable

Port Trigger:  Enable

UPnP:  Enable

---

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	<p>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.</p> <p><b>FTP ALG:</b> Allows FTP clients and servers to transfer data across NAT.</p> <p><b>TFTP ALG:</b> Allows TFTP clients and servers to transfer data across NAT.</p> <p><b>H323 ALG:</b> Allows Microsoft NetMeeting clients to communicate across NAT.</p> <p><b>RTSP ALG:</b> Allows some media player clients to communicate with some streaming media servers across NAT.</p>

---

---

## 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.

Enable	IP	Internal Port	Service Port	Protocol
<input checked="" type="checkbox"/>				TCP/UDP
--	--	--	--	--

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.

Enable	Incoming Port	Trigger Port	Protocol
<input checked="" type="checkbox"/>			TCP/UDP
--	--	--	--

Save Cancel

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.

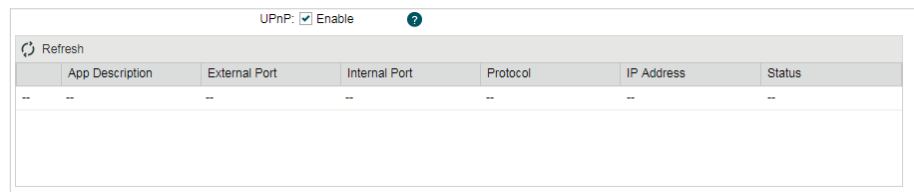
**Trigger Port:** Enter the trigger port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.

**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.



UPnP: <input checked="" type="checkbox"/> Enable					
Refresh					
App Description	External Port	Internal Port	Protocol	IP Address	Status
--	--	--	--	--	--

**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.

**Protocol:** Displays which type of protocol is opened.

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

**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*.

The screenshot shows a web interface for configuring security settings. The main heading is "Security" with a dropdown arrow. Below it is a sub-section titled "Basic". Inside this section, there are several configuration options:

- Firewall:  SPI Firewall (with a help icon)
- Ping:  WAN Ping Forbidden and  LAN Ping Forbidden
- VPN:  PPTP Passthrough,  L2TP Passthrough, and  IPSec Passthrough

---

### 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**.

Advanced Settings

DoS Protection:  Enable

Packets Statistics Interval: 10 seconds

ICMP\_FLOOD Attack Filter 50 packets/second

UDP\_FLOOD Attack Filter 500 packets/second

TCP\_SYN\_FLOOD Attack Filter 50 packets/second

Blocked DoS Host List

**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.

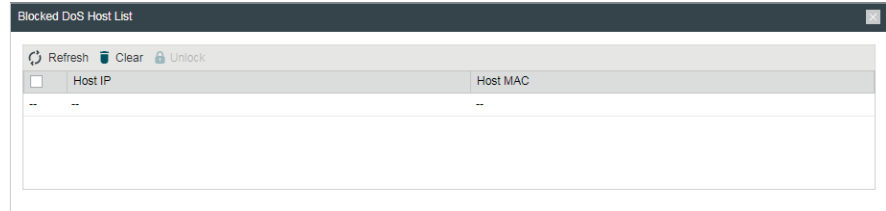
**ICMP\_FLOOD Attack Filter:** Enter a value between 5 and 3600. The default value is 50. When the current ICMP-FLOOD Packets number is beyond the set value, the device will start up the blocking function immediately.

**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.

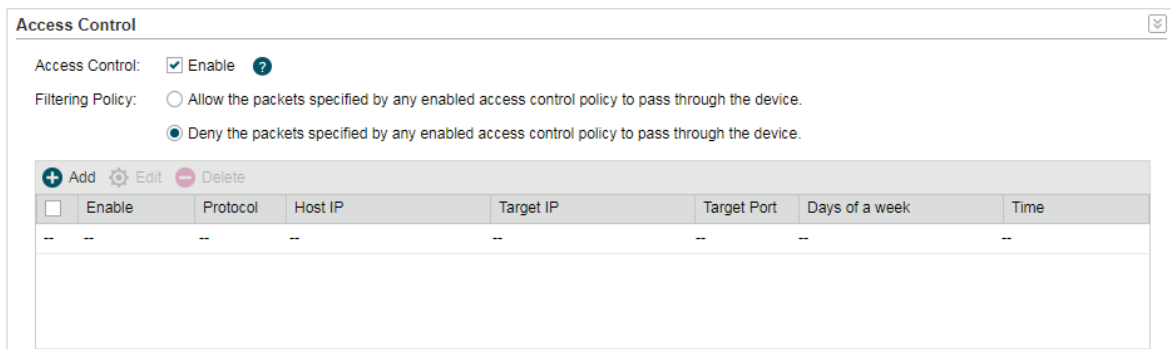
## 4.6 Configure Access Control

### 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	Protocol	Host IP	Target IP	Target Port	Days of a week	Time
<input checked="" type="checkbox"/>	TCF				Sun, Mon, Tue, Wed, Th	00:00-24:00

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.

<b>Enable</b>	Enable or disable the desired entry.
<b>Target Network IP</b>	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.
<b>Netmask</b>	Specify the netmask for the desired entry.
<b>Gateway IP</b>	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, you can 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 renew 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.

### Tips:

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

The screenshot shows the 'IP & MAC Binding' configuration window. At the top, there is a title bar with a close button. Below the title bar, the text 'IP & MAC Binding:  Enable' is displayed. A toolbar contains four icons: a plus sign for 'Add', a gear for 'Edit', a minus sign for 'Delete', and a circular arrow for 'Import'. Below the toolbar is a table with columns for 'Enable', 'IP', and 'MAC'. The first row has a checked checkbox, an 'Enable' dropdown menu, and empty input fields for IP and MAC. Below the table are 'Save' and 'Cancel' buttons. At the bottom right of the window is an 'Apply' button.

---

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**.

The screenshot shows the 'Basic Wireless Settings' configuration window. It contains several dropdown menus and input fields. The 'Mode' is set to '802.11a/n'. 'Channel Width' is '20/40MHz'. 'Max TX Rate' is 'MCS15 - 270/300 Mbps'. 'Channel/Frequency' is 'Auto'. 'Antenna Gain' is '0' with a range of '(0-30) dBi'. 'Transmit Power' is '23' dBm. 'MAXtream' has an 'Enable' checkbox checked. 'MAXtream Station Mode' is 'Auto Adjust'. There is a 'Spectrum Analysis' button and an 'Apply' button at the bottom right.

### Mode

Select the protocol standard used in the wireless network. With a frequency band of 2.4GHz, CPE210/CPE220/WBS210 supports five wireless modes: 802.11b, 802.11g, 802.11n, 802.11b/g and 802.11b/g/n. We recommend you to set the mode as 11b/g/n mixed, and all of 802.11b, 802.11g and 802.11n wireless stations can connect to the device. CPE610/CPE510/CPE520/WBS510 has a frequency band of 5GHz, supporting 802.11a, 802.11n and 802.11a/n modes. We recommend you to set the mode as 11a/n, allowing both 802.11a and 802.11n wireless stations to access the device.

### Channel Width

Select the channel width of this device. Options include 5MHz, 8MHz, 10MHz, 20MHz, 30MHz, 40MHz and 20/40MHz (the device automatically selects 20MHz/40MHz, and 20MHz will be used if 40MHz is not available). You can select corresponding channel width according to whether their devices support it. According to IEEE 802.11n standard, using a channel width of 40MHz can increase wireless throughput. However, you may need choose lower bandwidth due to the following reasons:

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.

Subject to the channel width of root AP in Client/ Bridge/ Repeater/ Client Router operation modes.

### Max TX Rate

Set the maximum transmit data rate.

Channel/ Frequency	<p>Select appropriate channel used by this device to improve wireless performance. 1/2412MHz refers to Channel 1 and the frequency is 2412MHz. This setting is only available in Access Point mode and AP Router mode.</p> <p>CPE210/CPE220/WBS210 is a device with a frequency of 2.4GHz and CPE610/CPE510/CPE520/WBS510 has a frequency of 5GHz. We highly recommend that you use the <i>Spectrum Analysis</i> tool to select a proper channel.</p>
Antenna Gain	<p>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.</p> <div data-bbox="555 723 1393 815" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Channel/Frequency: <input type="text" value="Auto"/> <span style="float: right; border: 1px solid #ccc; padding: 2px 5px; background-color: #f0f0f0;">Spectrum Analysis</span></p> <p>Antenna Gain: <input type="text" value="0"/> (0-30)dBi</p> </div>
Transmit Power	<p>Specify the transmit power of the device. You can use the slider or manually enter the transmit power value. For WBS210 and WBS510, the maximum transmit power varies according to the antenna gain value.</p> <p><b>Note:</b></p> <p>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. You can use the <i>Speed Test</i> tool to find the best performance</p>
MAXtream	<p>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.</p> <p><b>Note:</b></p> <p>MAXtream Technology is only compatible with Pharos series products. Working with products from other manufacturer will cause network fault.</p>
MAXtream Station Mode	<p>MAXtream Station Mode is available in Client mode, Bridge mode and AP Client Router mode with the wireless AP settings disabled.</p> <p><b>Auto Adjust:</b> The device will choose the MAXtream station mode automatically.</p> <p><b>Latency First:</b> Set the MAXtream station mode as Latency First and the time sensitive stream such as VoIP will take precedence in MAXtream system.</p> <p><b>Throughput First:</b> 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.</p>

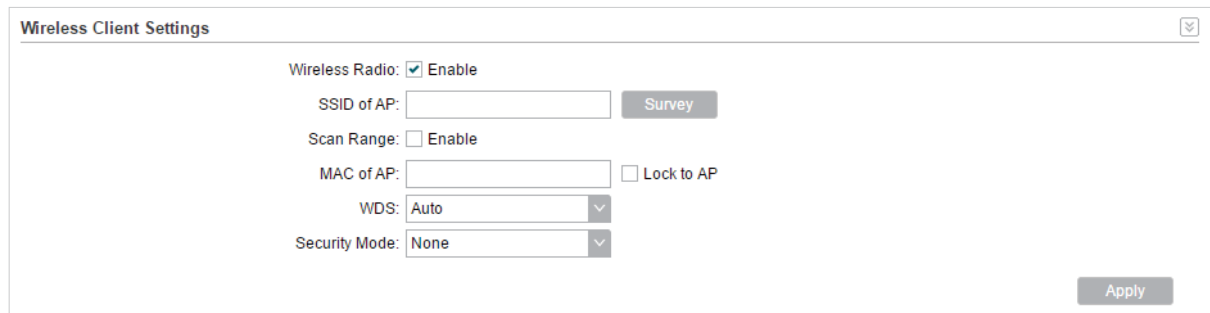


## 5.2 Configure Wireless Client Parameters

### Note:

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

In this section, you can 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.

<b>SSID of AP</b>	Specify the SSID of the root AP. You can enter the SSID of the specific AP manually, or you can directly survey all the APs around by clicking <b>Survey</b> and select one.
<b>Scan Range</b>	Enable or disable the Scan Range. With the Scan Range enabled, you need to specify the frequency range and the device will survey SSIDs in the coeersponding range.
<b>MAC of AP</b>	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 <b>Lock to AP</b> to select SSID and AP simultaneously, which can make the device connect to the specific AP you had connected before the next time.
<b>WDS</b>	<p>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.</p> <p><b>Enable:</b> Forward data frames to use four address fields.</p> <p><b>Disable:</b> Forward data frames to use three address fields.</p> <p><b>Auto:</b> The device automatically negotiates the wireless data frame structure (three or four address fields) with the root AP. The selection of Auto is recommended.</p>

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

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.

**Note:**

WEP is not supported in 802.11n mode or 802.11ac mode. If WEP is applied in 802.11n, 802.11ac 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.

Security Mode:	WEP	▼
Auth Type:	Auto	▼
Key Format:	Hex	▼
Key Selected:	WEP Key:	Key Type:
Key 1: <input checked="" type="radio"/>	<input type="text"/>	Disabled ▼
Key 2: <input type="radio"/>	<input type="text"/>	Disabled ▼
Key 3: <input type="radio"/>	<input type="text"/>	Disabled ▼
Key 4: <input type="radio"/>	<input type="text"/>	Disabled ▼

**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. <b>64Bit:</b> Enter 10 hexadecimal digits or 5 ASCII characters. <b>128Bit:</b> Enter 26 hexadecimal digits or 13 ASCII characters. <b>152Bit:</b> 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.

The image shows a configuration window for WPA. It contains several dropdown menus and text input fields. The dropdown menus are: Security Mode (set to WPA), Version (set to Auto), Encryption (set to Auto), Authentication (set to EAP-TTLS), and Phase 2 Auth (set to MSCHAPV2). Below these are two text input fields: WPA User Name and WPA User Password. To the right of the WPA User Password field is a checkbox labeled 'Show'.

Version	Select the version of WPA.  <b>Auto:</b> The device will automatically choose the version used by the root AP.  <b>WPA/WPA2:</b> 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	Select the Encryption type.  <b>Auto:</b> The default setting is Auto and the device will select TKIP or AES automatically according to the wireless network of root AP.  <b>TKIP:</b> 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.  <b>AES:</b> 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.

The screenshot shows a configuration window for WPA-PSK. It contains four rows of settings:

- Security Mode:** A dropdown menu with 'WPA-PSK' selected.
- Version:** A dropdown menu with 'Auto' selected.
- Encryption:** A dropdown menu with 'Auto' selected.
- PSK Password:** A text input field followed by a 'Show' checkbox.

Version	<p>Select the version of WPA-PSK.</p> <p><b>WPA-PSK/WPA2-PSK:</b> 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.</p> <p><b>Auto:</b> The device will automatically choose the version used by the root AP.</p> <p><b>WPA/WPA2:</b> 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.</p>
Encryption	<p>Select the Encryption type.</p> <p><b>Auto:</b> The default setting is Auto and the device will select TKIP or AES automatically according to the wireless network of root AP.</p> <p><b>TKIP:</b> 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.</p> <p><b>AES:</b> Advanced Encryption Standard. It is securer than TKIP.</p>

---

**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 Client Settings submenu is only available in Access Point, Bridge, AP Router and AP client Router (WISP client) mode.

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

Wireless AP Settings

Wireless Radio:  Enable

SSID:   Enable SSID Broadcast

Security Mode:

RADIUS MAC Authentication:  Enable ?

Authentication Server IP:

Authentication Server Port:

Authentication Server Key:   Show

Accounting Server:  Enable ?

Apply

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

---

<b>Enable SSID Broadcast</b>	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.

The screenshot shows a configuration window with two main sections. The first section is for RADIUS MAC Authentication, which is currently set to 'Enable'. It includes input fields for 'Authentication Server IP' (0.0.0.0), 'Authentication Server Port' (1812), and 'Authentication Server Key' (empty), with a 'Show' checkbox next to the key field. The second section is for the Accounting Server, also set to 'Enable'. It includes input fields for 'Accounting Server IP' (0.0.0.0), 'Accounting Server Port' (1813), and 'Accounting Server Key' (empty), with a 'Show' checkbox next to the key field.

<b>RADIUS MAC Authentication</b>	<p>Enable or disable the Radius MAC authentication. With this feature enabled, you can authenticate clients using their MAC addresses on your RADIUS authentication server.</p> <p>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).</p>
<b>Authentication Server IP</b>	Enter the IP address of the RADIUS authentication server.
<b>Authentication Server Port</b>	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.
<b>Authentication Server Key</b>	<p>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.</p> <p>Check the <b>Show</b> box to view the shared key characters.</p>
<b>Accounting Server</b>	Enable or disable Accounting Server. With this feature enabled, you can keep accounts on users using a RADIUS accounting server.
<b>Accounting Server IP</b>	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 <b>Show</b> box to view the shared key characters.

## ■ WEP

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.

The screenshot shows a configuration interface for WEP. It includes three dropdown menus: 'Security Mode' set to 'WEP', 'Auth Type' set to 'Auto', and 'Key Format' set to 'Hex'. Below these are four rows for WEP keys. Each row has a radio button for 'Key Selected', a text input field for the 'WEP Key', and a dropdown menu for 'Key Type' set to 'Disabled'.

### Note:

WEP is not supported in 802.11n mode or 802.11ac mode. If WEP is applied in 802.11n, 802.11ac 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.

Auth Type	Select the authentication type for WEP.  <b>Auto:</b> The device can select Open System or Shared Key automatically based on the wireless capability and request of the clients.  <b>Open System:</b> Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission.  <b>Shared Key:</b> Clients have to input the correct password to pass the authentication, otherwise the clients cannot associate with the wireless network or transmit data.
-----------	---

<b>Key Format</b>	Select ASCII or Hex as the WEP key format.  <b>ASCII:</b> With this format selected, the WEP key can be any combination of keyboard characters of the specified length.  <b>Hex:</b> With this format selected, the WEP key can be any combination of hexadecimal digits (0-9, a-f, A-F) with the specified length.
<b>Key Selected</b>	Select one key to specify. You can configure four keys at most.
<b>WEP Key</b>	Enter the WEP keys. The length and valid characters are determined by the key format and key type.
<b>Key Type</b>	Select the WEP key length for encryption.  <b>64Bit:</b> Enter 10 hexadecimal digits or 5 ASCII characters.  <b>128Bit:</b> Enter 26 hexadecimal digits or 13 ASCII characters.  <b>152Bit:</b> 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.

Security Mode:	WPA	▼
Version:	Auto	▼
Encryption:	Auto	▼
Authentication Server IP:	0.0.0.0	
Authentication Server Port:	1812	
Authentication Server Key:		<input type="checkbox"/> Show
Group Key Update Period:	0	seconds. (0 means no update.)
Accounting Server:	<input checked="" type="checkbox"/> Enable	?
Accounting Server IP:	0.0.0.0	
Accounting Server Port:	1813	
Accounting Server Key:		<input type="checkbox"/> Show



Version	<p>Select the version of WPA.</p> <p><b>Auto:</b> The device will automatically choose the version used by each client device.</p> <p><b>WPA/WPA2:</b> 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.</p>
Encryption	<p>Select the Encryption type.</p> <p><b>Auto:</b> The default setting is Auto and the device will select TKIP or AES automatically based on the client device's request.</p> <p><b>TKIP:</b> 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.</p> <p><b>AES:</b> Advanced Encryption Standard. It is securer than TKIP.</p>
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	<p>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.</p> <p>Check the <b>Show</b> box to view the shared key characters.</p>
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.

The image shows a configuration interface for WPA-PSK. It includes the following fields and options:

- Security Mode:** A dropdown menu set to "WPA-PSK".
- Version:** A dropdown menu set to "Auto".
- Encryption:** A dropdown menu set to "Auto".
- PSK Password:** A text input field with a "Show" checkbox to its right.
- Group Key Update Period:** A text input field set to "0", followed by the text "seconds. (0 means no update.)"

---

Version

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

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.

Enable	SSID	VLAN	SSID Broadcast	AP Isolation
<input type="checkbox"/>	TP-Link_Outdoor_BD046E	1	Enable	Disable

Security Settings

SSID:

Security Mode:

**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.

Security Settings

SSID:

Security Mode:

Version:

Encryption:

PSK Password:   Show

Group Key Update Period:  seconds. (0 means no update.)

<b>SSID</b>	Select the desired SSID to specify the security settings.
<b>Security</b>	Specify the security settings for the desired SSID. The device only supports WPA-PSK.
<b>Version</b>	<p>Select the version of WPA-PSK.</p> <p><b>WPA-PSK/WPA2-PSK:</b> 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.</p> <p><b>Auto:</b> The device will automatically choose the version used by the root AP.</p> <p><b>WPA/WPA2:</b> 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.</p>
<b>Encryption</b>	<p>Select the Encryption type.</p> <p><b>Auto:</b> The default setting is Auto and the device will select TKIP or AES automatically according to the wireless network of root AP.</p> <p><b>TKIP:</b> 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.</p> <p><b>AES:</b> Advanced Encryption Standard. It is securer than TKIP.</p>
<b>PSK Password</b>	Specify the PSK password used in the connection with the clients.
<b>Group Key Update Period</b>	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**

Wireless MAC Filtering:  Enable

Filtering Rules:

Deny the stations specified by any enabled entries in the list to access the network.

Allow the stations specified by any enabled entries in the list to access the network.

+ Add Edit Delete

<input type="checkbox"/>	Enable	SSID	MAC	Comment
--	--	--	--	--

### 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.

+ Add Edit Delete

<input type="checkbox"/>	Enable	SSID	MAC	Comment
<input checked="" type="checkbox"/>	Enable			

Save Cancel

### Enable

Enable or disable the desired entry.

### SSID

Select the 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 DIM Interval.

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

Advanced Wireless Settings

Distance Setting:  (0-200) km  Auto (Only works within 0-27.9km) ?

Long Range PTP:  ?

Beacon Interval:  (40-1000)

RTS Threshold:  (1-2346)

Fragmentation Threshold:  (256-2346)

DTIM Interval:  (1-255)

AP Isolation:  Enable

Short GI:  Enable

Wi-Fi MultiMedia (WMM):  Enable

QoS:  Enable

Apply

### 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.

### 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. You can specify a value from 40 to 1,000. The default value is 100.

RTS Threshold	<p>Specify the RTS threshold for the device.</p> <p>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.</p> <p>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.</p> <p>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. The recommended and default value is 2346 bytes.</p>
Fragmentation Threshold	<p>Specify the fragmentation threshold for packets.</p> <p>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.</p> <p>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.</p>
DTM Interval	<p>Specify the DTM (Delivery Traffic Indication Message) Interval for the device.</p> <p>The DTIM is contained in some Beacon frames. It indicates whether the device has buffered data for client devices. The <b>DTIM Period</b> indicates how often the clients served by this device should check for buffered data still on the device awaiting pickup.</p> <p>You can 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.</p>
AP Isolation	<p>Enable or disable AP Isolation. With this feature enabled, the clients can not communicate with each other directly.</p> <p><b>Note:</b></p> <p>AP Isolation is not available in Client mode.</p>

Short GI	<p>Enable or disable Short GI.</p> <p>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.</p> <p>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.</p>
Wi-Fi Multimedia (WMM)	<p>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.</p> <p>We recommend you enable this function when you are running the video or audio application.</p>
QoS	<p>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.</p>



# 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*

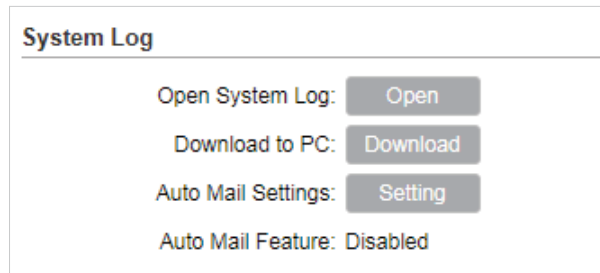
*6.7 Configure SSH Server*

*6.8 Configure RSSI LED Thresholds*

## 6.1 Manage System Logs

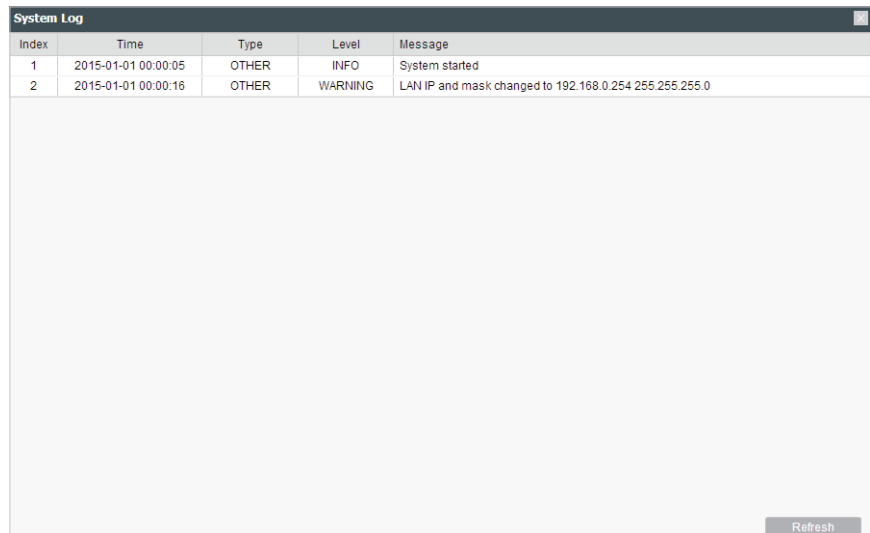
System logs record the events and activities while the device is running. If a failure happens on the router, System logs can help to diagnose the issue.

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



### Open System Log

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



The screenshot shows the 'System Log' view interface. It features a table with the following data:

Index	Time	Type	Level	Message
1	2015-01-01 00:00:05	OTHER	INFO	System started
2	2015-01-01 00:00:16	OTHER	WARNING	LAN IP and mask changed to 192.168.0.254 255.255.255.0

Below the table is a large empty area for displaying more logs, and a 'Refresh' button is located in the bottom right corner.

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. You can 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, you can 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**

Ping Watch Dog:  Enable

IP Address To Ping:

Ping Interval:  (10-300) seconds

Startup Delay:  (60-300) seconds

Fail Count To Reboot:  (1-65535)

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. Please register an account to DDNS service provider (NO-IP, DynDNS or Comex) first.

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

**Dynamic DNS**

Service Provider:  ▼

Dynamic DNS:  Enable

User Name:

Password:   Show

Domain Name:

Connection Status: Not launching.

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*.

**Web Server**

Secure Connection (HTTPS):  Enable

Secure Server Port:

Server Port:

Remote Login IP Address:  ?

Session Timeout:  minutes

MAC Authentication:  Enable

MAC1:

MAC2:

MAC3:

MAC4:  Add PC's MAC

<b>Secure Connection (HTTPS)</b>	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.
<b>Secure Server Port</b>	Specify the server port number used in HTTPS. The default value is 443.
<b>Server Port</b>	Specify the server port number used in HTTP. The default value is 80.
<b>Remote Login IP Address</b>	Specify the IP address of the remote host. With this configured, the remote device can access the management interface remotely.
<b>Session Timeout</b>	Specify the session timeout time. The system will automatically release the connection when the time is up.
<b>MAC Authentication</b>	<p>Enable or disable MAC Authentication. When it is enabled, you can specify up to four MAC address for authentication.</p> <p>With this function enabled, only the device whose MAC address is in the MAC list can access the management interface to configure the device.</p> <p>You can click <i>Add PC's MAC</i> to quickly add your PC's MAC address to the MAC list.</p>

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

## 6.6 Configure SNMP Agent

You can 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. When the network working normally, SNMP can monitor the statistics, configuration. When networks have troubles, SNMP can detect and restore these troubles.

Configure the device as SNMP Agent, and it can receive and process the management message from the network management system.

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

**SNMP Agent**

SNMP Agent:  Enable

SysContact:

SysName:

SysLocation:

Get Community:

Get Source:

Set Community:

Set Source:

<b>SNMP Agent</b>	Enable or disable the SNMP Agent function.
<b>SysContaact</b>	Enter the textual identification of the contact person for this the device, for example, contact or e-mail address.
<b>SysName</b>	Enter a name for the device.
<b>Syslocation</b>	Enter the location of the device. For example, the name can be composed of the building, floor number, and room location.
<b>Get Community</b>	Specify the community that has read-only access to the device's SNMP information.
<b>Get Source</b>	Enter the IP address that can serve as Get Community to read the SNMP information of this device.
<b>Set Community</b>	Specify the community who has the read and write right of the device's SNMP information.
<b>Set Source</b>	Enter the IP address that can serve as Set Community to read and write the SNMP information of this device.



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*.

**SSH Server**

---

Server Port:

SSH Login:  Enable

Remote Management:  Enable ?

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

You can 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).

**Note:**

CPE610 doesn't support this feature.

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

	LED1	LED2	LED3	LED4
Thresholds (dBm):	- 94	- 80	- 73	- 65

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*

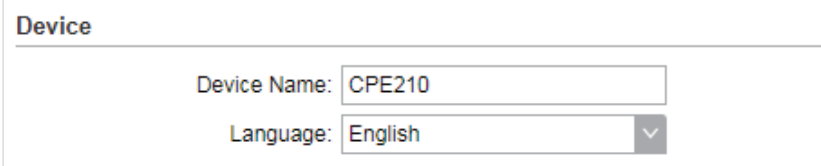
*7.5 Update Firmware*

*7.6 Configure Other Settings*

## 7.1 Configure Device Information

In this section, you can 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**.



The screenshot shows a configuration form titled "Device". It contains two fields: "Device Name" with the value "CPE210" and "Language" with a dropdown menu set to "English".

---

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

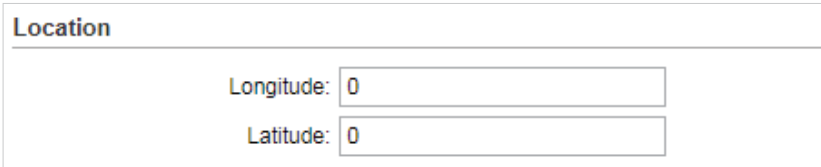
---

2. Click **Save**.

## 7.2 Configure Location Information

In this section, you can configure the location for the device.

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



The screenshot shows a configuration form titled "Location". It contains two fields: "Longitude" with the value "0" and "Latitude" with the value "0".

---

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*.

**User Account**

---

Current User Name:

Current Password:   Show

New User Name:

New Password:   Show

Confirm New Password:

Current User Name	Displays the current user name.
Current Password	Enter the current password for the user account. Check the <i>Show</i> 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 <i>Show</i> 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, you can configure the system time and the daylight saving time.

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

**Time Setting**

---

Time Zone:  ▼

Date:

Time:  ▼

NTP Server 1:

NTP Server 2:

Daylight Saving 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.

Daylight Saving Time

DST Status:  Enable

Predefined Mode

USA  European  Australia  New Zealand

Recurring Mode

Time Offset: 60 minutes

Start Time: Last in March at 01 : 00

End Time: Last in October at 01 : 00

Date Mode

Time Offset: 60 minutes

Start Time: 2000 - March - 1 at 01 : 00

End Time: 2000 - October - 1 at 01 : 00

Apply

## 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.

#### ■ Recurring mode

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*.

<b>Firmware Update</b>	
Firmware Version: 2.1.6 Build 20170908 Rel. 45233 (0000)	
Upload Firmware:	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="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.
- Please select the proper software version that matches your hardware to upgrade. You can visit TP-Link website to download the latest firmware.
- To avoid damage, please 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, you can perform the following operations.



Configuration

Backup Configuration:

Upload Configuration:

Reset to Factory Defaults:

Reboot Device:

<b>Backup Configuration</b>	Click <i>Backup</i> to back up the current configuration to your PC.
<b>Upload Configuration</b>	Click <i>Browser</i> to select the desired configuration file in your PC. Then click <i>Upload</i> to upload the configuration file to your device. We recommend that you back up your current system configuration before uploading the new configuration.
<b>Reset to Factory Defaults</b>	Click <i>Reset</i> 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.
<b>Reboot Device</b>	Click <i>Reboot</i> 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*

## 8.1 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.

The screenshot shows a 'Ping' configuration window. At the top, there's a title bar with the word 'Ping' and a close button. Below the title bar, there are four input fields: 'Destination IP/Domain' (empty), 'Packet Count' (4, with a range of 1-50), 'Ping Timeout' (800, with a range of 100-2000 milliseconds), and 'Packet Size' (64, with a range of 4-1472 bytes). Below these fields is a 'Ping Results' section. It has a sub-header 'Ping Results' and an 'Enable' checkbox. Below the checkbox is a large empty text area. At the bottom right of the window is a 'Start' button.

---

### 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 any 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.

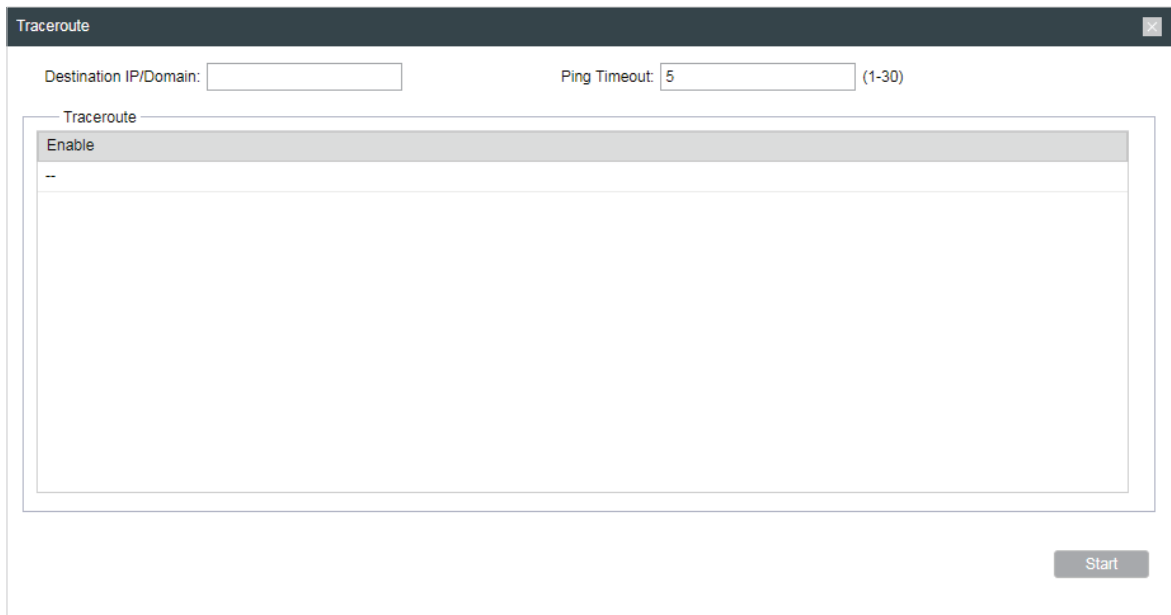
---

2. Click *Start*.

## 8.2 Configure Traceroute

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

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



The screenshot shows a 'Traceroute' configuration window. At the top, there are two input fields: 'Destination IP/Domain:' and 'Ping Timeout: 5 (1-30)'. Below these is a 'Traceroute' section with a dropdown menu set to 'Enable'. A 'Start' button is located at the bottom right of the window.

**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.

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

Survey									
Index	BSSID	SSID	MAXtream	Device Name	SNR(dB)	Signal / Noise(dBm)	Channel	Security	
1	50-C7-BF-04-BF-26	TP-LINK_BF28_5G	No		38	-63/-101	5805 (161)	WPA2-PSK	▲
2	60-E3-27-D0-E2-2A	jjj5	No		34	-61/-95	5220 (44)	WPA2-PSK	
3	50-C7-BF-08-5D-86	TP-LINK_Cui5	No		38	-57/-95	5220 (44)	WPA2-PSK	
4	18-A6-F7-F3-47-1A	TP-LINK_Cui5re	No		41	-54/-95	5220 (44)	WPA-PSK/WPA2-PSK	
5	18-A6-F7-20-02-E1	EAP225 5g	No		38	-61/-99	5765 (153)	WPA2-PSK	
6	18-A6-F7-F3-71-BA	hubiao2.5	No		33	-62/-95	5180 (36)	WPA-PSK/WPA2-PSK	
7	EC-08-6B-00-F4-3A	TP-LINK_F43A	No		20	-75/-95	5180 (36)	WPA-PSK/WPA2-PSK	
8	50-C7-BF-01-88-1F	7200_5G	No		45	-50/-95	5180 (36)	WPA-PSK/WPA2-PSK	
9	C4-E9-84-ED-08-C3	ap3200_5G_1	No		28	-67/-95	5180 (36)	WPA2-PSK	
10	18-A6-F7-2D-CA-77	EAP_TEST	No		35	-60/-95	5180 (36)	WPA2-PSK	
11	50-C7-BF-01-0B-FA	C9test-5	No		34	-61/-95	5180 (36)	WPA-PSK/WPA2-PSK	
12	50-C7-BF-06-A8-BD	TP-LINK_A8BE_5G	No		38	-57/-95	5200 (40)	WPA-PSK/WPA2-PSK	
13	18-A6-F7-F3-4D-42	jjj5re	No		36	-59/-95	5220 (44)	WPA-PSK/WPA2-PSK	
14	F4-F2-6D-EF-69-53	ARC2_5G	No		30	-65/-95	5220 (44)	WPA2-PSK	
15	50-C7-BF-0B-BE-01	eap_fuck000_5G	No		29	-66/-95	5240 (48)	WPA2-PSK	
16	F4-F2-6D-D2-8F-7D	TP-LINK_8F7C_5G	No		29	-66/-95	5240 (48)	WPA-PSK/WPA2-PSK	
17	F4-F2-6D-B6-AC-5D	TP-LINK_AC5E_5G	No		45	-53/-98	5745 (149)	WPA-PSK/WPA2-PSK	
18	D0-EE-07-1C-89-54	autoss	No		7	-91/-98	5745 (149)	WPA-PSK/WPA2-PSK	
19	00-0A-EB-13-7A-FE	TP-LINK_7AFE_5G	No		44	-42/-86	5765 (153)	WPA-PSK/WPA2-PSK	
20	90-F6-52-C3-B0-B8	TestingRoom	No		32	-67/-99	5765 (153)	WPA-PSK/WPA2-PSK	
21	EC-08-6B-9F-BD-2A	Smart Home5G	No		47	-52/-99	5765 (153)	WPA-PSK/WPA2-PSK	
22	F6-F2-6D-2F-A3-24	onhub	No		42	-57/-99	5765 (153)	WPA2-PSK	▼

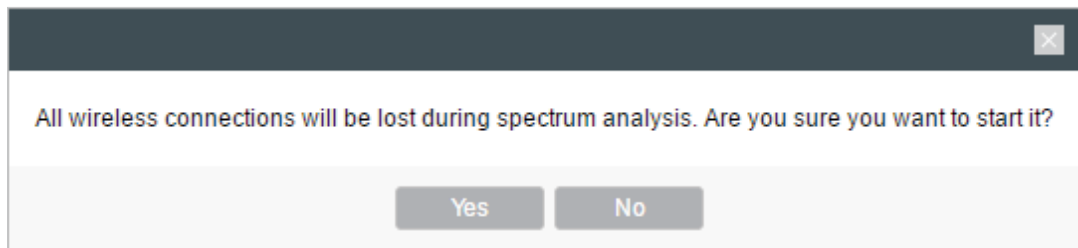
AP Count: 26 Refresh

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

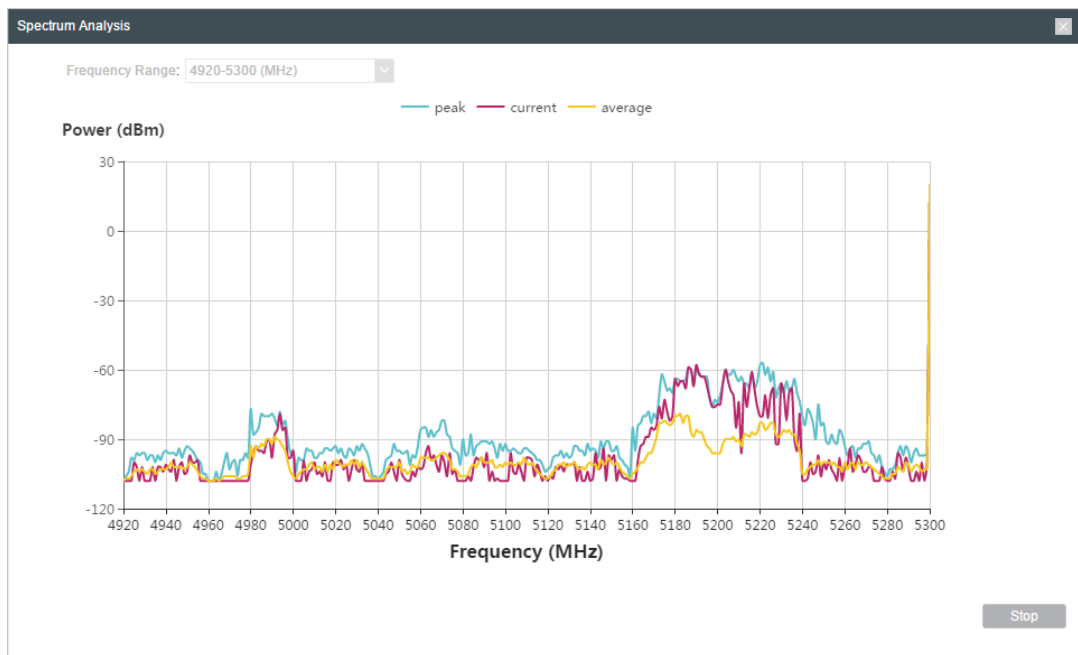
## 8.5 Analyze Spectrum

Spectrum Analysis can help you to choose the proper channel/frequency. Through the spectrum analysis you can 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:**

- Only CPE610/CPE510/CPE520/WBS510 has the select box of Frequency Range at the upper-left corner. Select the required range and then click *Start*.

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

## 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 © 2018 TP-Link Technologies Co., Ltd.. All rights reserved.