



PHAROS

User Guide

For TP-Link Pharos Series Products

CPE210 / CPE220 / CPE510 / CPE610 / CPE710
WBS210 / WBS510

1910012759 REV 3.3.0

February 2020

CONTENTS

About this User Guide.....	1
Overview	2
1 Operation Modes.....	3
1.1 Access Point.....	4
1.2 Client.....	5
1.3 AP Client Router (WISP Client)	6
1.4 AP Router	6
1.5 Repeater	7
1.6 Bridge	7
2 Quick Start.....	8
2.1 Check the System Requirements	9
2.2 Log In to the Device	9
2.3 Set Up the Wireless Network.....	10
Access Point.....	11
Client	15
Repeater	19
Bridge	23
AP Router	27
AP Client Router (WISP Client)	33
3 Monitor the Network	39
3.1 View the Device Information.....	40
3.2 View the Wireless Settings.....	40
3.3 View Wireless Signal Quality.....	41
3.4 View Radio Status	42
3.5 View the LAN Settings.....	44
3.6 View the WAN Settings	45

3.7	Monitor Throughput.....	46
3.8	Monitor Stations.....	46
3.9	Monitor Interfaces	49
3.10	Monitor ARP Table	49
3.11	Monitor Routes	50
3.12	Monitor DHCP Clients.....	51
3.13	Monitor Dynamic WAN.....	51
4	Configure the Network.....	54
4.1	Configure WAN Parameters.....	55
4.2	Configure LAN Parameters	65
	Access Point/Client/Repeater/Bridge Mode	65
	AP Router/AP Client Router Mode.....	70
4.3	Configure Management VLAN	72
4.4	Configure the Forwarding Feature	73
4.5	Configure the Security Feature	77
4.6	Configure Access Control	80
4.7	Configure Static Routing.....	81
4.8	Configure Bandwidth Control.....	82
4.9	Configure IP & MAC Binding.....	84
5	Configure the Wireless Parameters.....	86
5.1	Configure Basic Wireless Parameters	87
5.2	Configure Wireless Client Parameters	90
5.3	Configure Wireless AP Parameters.....	94
5.4	Configure Multi-SSID.....	99
5.5	Configure Wireless MAC Filtering	101
5.6	Configure Advanced Wireless Parameters.....	102
6	Manage the Device	106
6.1	Manage System Logs	107

6.2	Specify the Miscellaneous Parameters	108
6.3	Configure Ping Watch Dog	109
6.4	Configure Dynamic DNS	110
6.5	Configure Web Server	111
6.6	Configure SNMP Agent	112
6.7	Configure SSH Server	114
6.8	Configure RSSI LED Thresholds	114
7	Configure the System	116
7.1	Configure Device Information	117
7.2	Configure Location Information	117
7.3	Configure User Account	117
7.4	Configure Time Settings	118
7.5	Update Firmware	120
7.6	Configure Other Settings	121
8	Use the System Tools	122
8.1	Configure Ping	123
8.2	Configure Traceroute	123
8.3	Test Speed	124
8.4	Survey	125
8.5	Analyze Spectrum	127
8.6	Antenna Alignment	128

About this User Guide

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

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

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

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

Convention

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

More Info

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

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

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

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

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

Overview

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

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

New features of Pharos series products are listed as follows:

- Provides User-friendly UI design.
- TP-Link Pharos MAXtream (Time-Division-Multiple-Access) technology improves product performance in throughput, capacity and latency, which is ideal for point-to-multipoint applications.
- Supports multiple operation modes: Access Point, Client, Repeater, Bridge, AP Router and AP Client Router (WISP Client).
- Provides system-level optimization for long-distance wireless transmission.
- Supports selectable bandwidth of 5/10/20/40 MHz.
- 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. For more information, refer to [Common Applications for Pharos Products](#).

1.1 Access Point

1.2 Client

1.3 AP Client Router (WISP Client)

1.4 AP Router

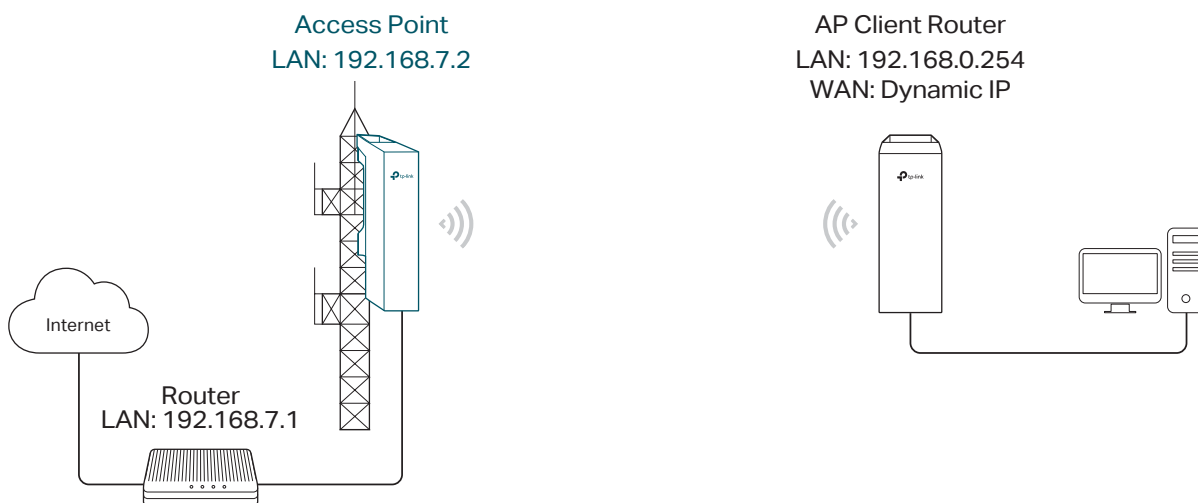
1.5 Repeater

1.6 Bridge

1.1 Access Point

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

■ Scenario 1

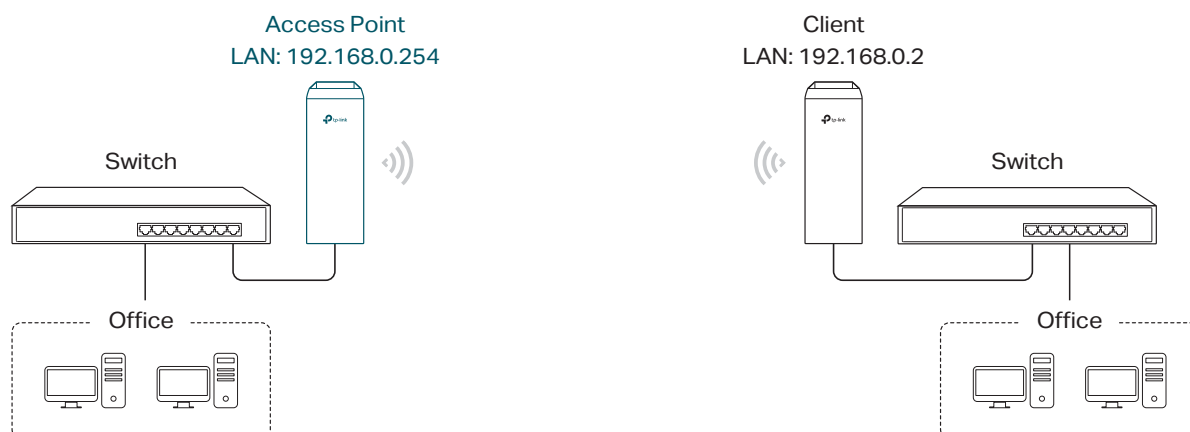


Network requirements: Establish the network coverage in the remote areas without long-distance cabling.

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

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

■ Scenario 2



Network requirements: Combine two separate office networks into one.

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

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

■ Scenario 3



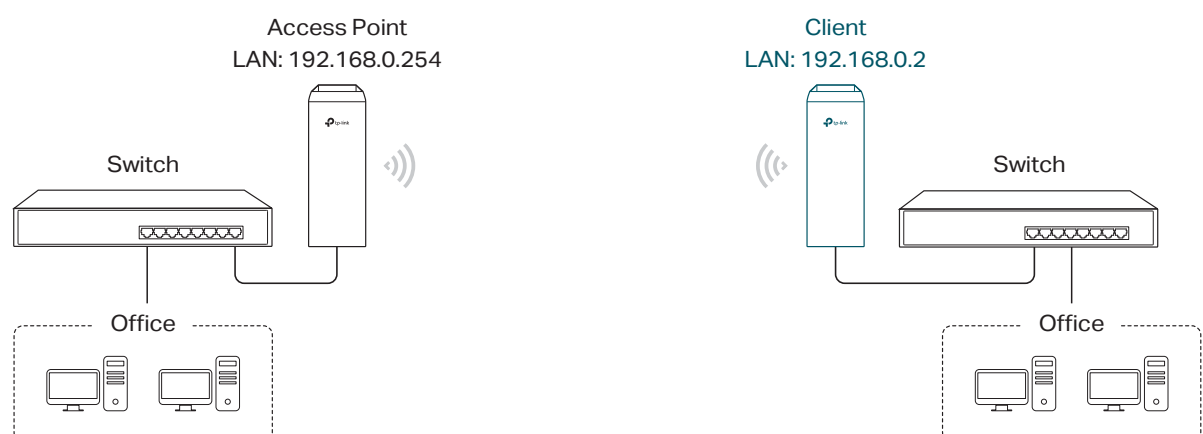
Network requirements: Establish wireless network coverage in the campus, community, industrial park or public place to provide wireless access for users.

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

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

1.2 Client

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

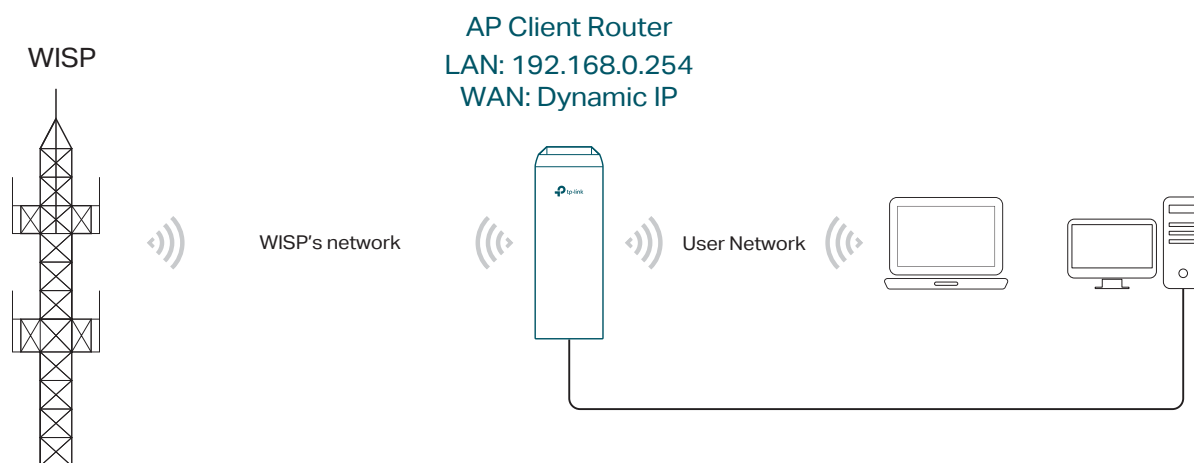


Network requirements: Help the wired devices to connect to the wireless network.

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

1.3 AP Client Router (WISP Client)

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



Network requirements: Get internet service from WISP.

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

1.4 AP Router

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



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

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

Note:

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

1.5 Repeater

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

1.6 Bridge

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

2 Quick Start

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

2.1 Check the System Requirements

2.2 Log In to the Device

2.3 Set Up the Wireless Network

2.1 Check the System Requirements

■ Operating System:

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

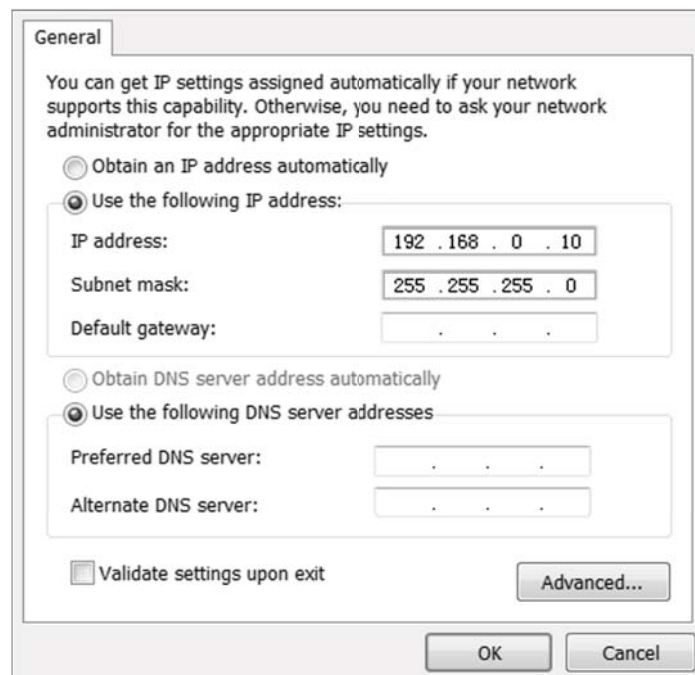
■ Web Browser

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

2.2 Log In to the Device

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

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



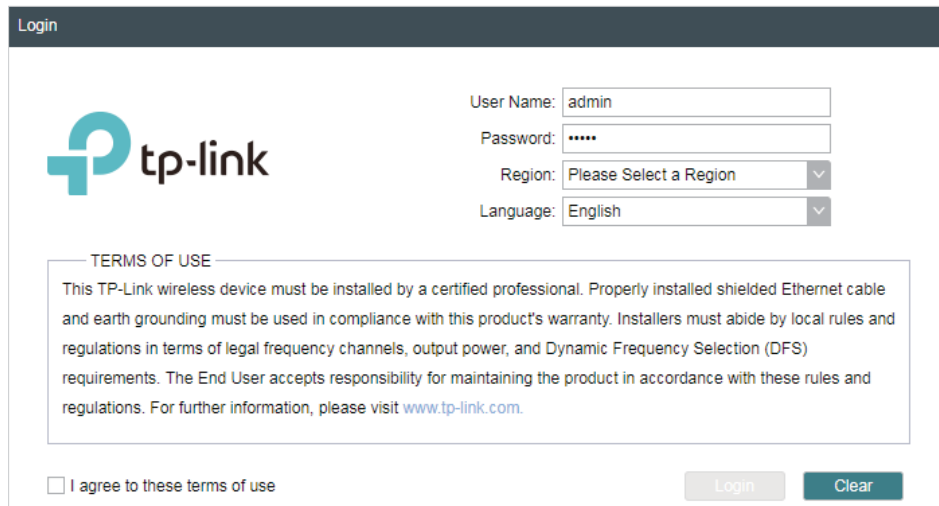
The screenshot shows a 'General' network configuration window. It contains a text box explaining that IP settings can be assigned automatically or manually. There are two radio buttons: 'Obtain an IP address automatically' (unselected) and 'Use the following IP address:' (selected). Below the selected option are three input fields: 'IP address:' with the value '192 . 168 . 0 . 10', 'Subnet mask:' with the value '255 . 255 . 255 . 0', and 'Default gateway:' with three empty fields. There are also two radio buttons for DNS: 'Obtain DNS server address automatically' (unselected) and 'Use the following DNS server addresses' (selected). Below the selected option are two input fields: 'Preferred DNS server:' and 'Alternate DNS server:', both with three empty fields. At the bottom left is a checkbox labeled 'Validate settings upon exit' which is unchecked. At the bottom right is an 'Advanced...' button. At the very bottom are 'OK' and 'Cancel' buttons.

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.



The screenshot shows a web browser address bar. It contains a back arrow icon, a globe icon, and the text 'http://192.168.0.254'.

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



The image shows the TP-Link login interface. At the top left is the TP-Link logo. To the right are four input fields: 'User Name' with 'admin' entered, 'Password' with masked characters, 'Region' with a dropdown menu showing 'Please Select a Region', and 'Language' with a dropdown menu showing 'English'. Below these fields is a 'TERMS OF USE' section with a text box containing a disclaimer. At the bottom left is a checkbox labeled 'I agree to these terms of use'. At the bottom right are two buttons: 'Login' and 'Clear'.

tp-link

User Name: admin

Password:

Region: Please Select a Region

Language: English

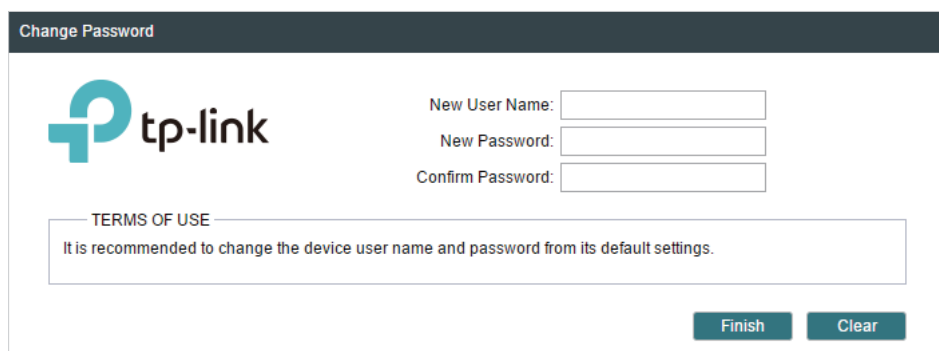
TERMS OF USE

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.

☐ I agree to these terms of use

Login Clear

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



The image shows the TP-Link 'Change Password' interface. At the top left is the TP-Link logo. To the right are three input fields: 'New User Name', 'New Password', and 'Confirm Password'. Below these fields is a 'TERMS OF USE' section with a text box containing a recommendation. At the bottom right are two buttons: 'Finish' and 'Clear'.

tp-link

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.

Finish Clear

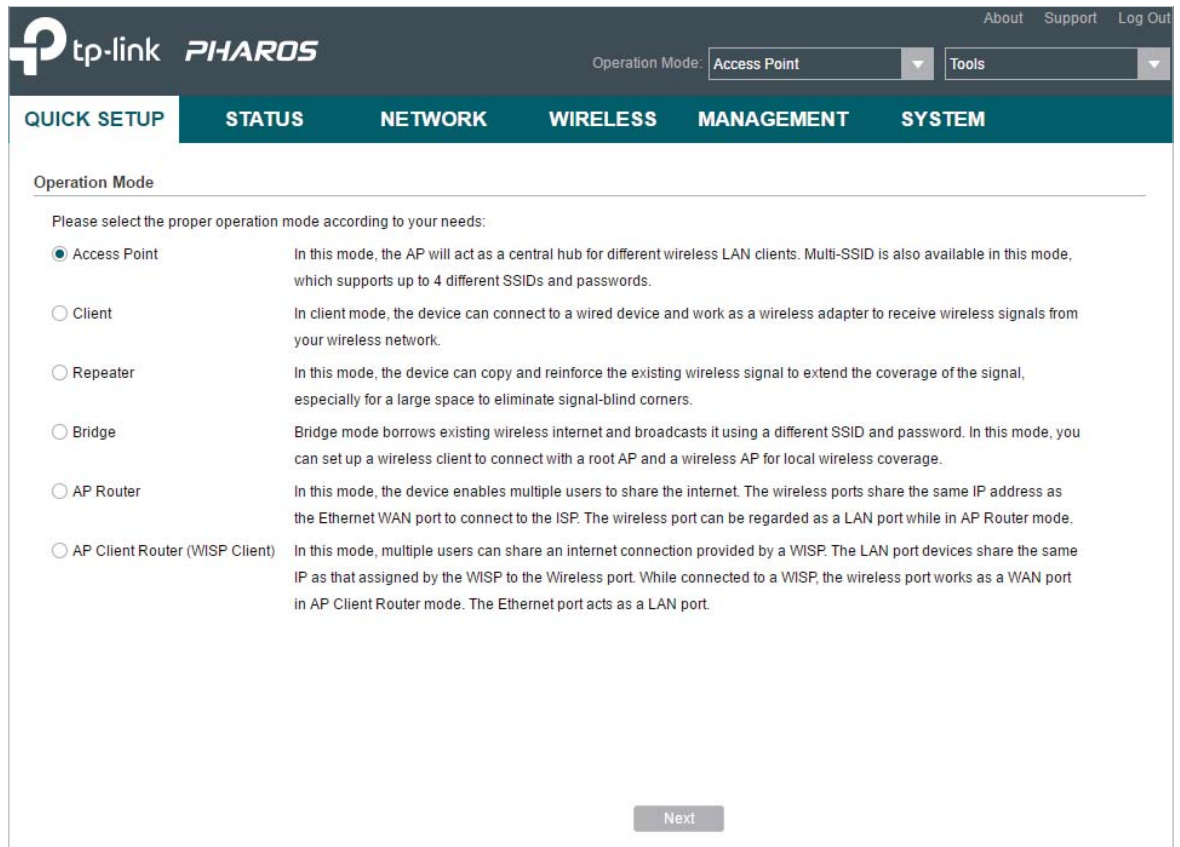
2.3 Set Up the Wireless Network

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

Access Point

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

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



The screenshot shows the TP-Link PHAROS web interface. At the top, there's a header with the TP-Link logo, the model name 'PHAROS', and links for 'About', 'Support', and 'Log Out'. Below the header is a navigation bar with tabs: 'QUICK SETUP' (active), 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is selected, and the 'Operation Mode' section is visible. It prompts the user to 'Please select the proper operation mode according to your needs:'. There are six radio button options, each with a description: 'Access Point' (selected), 'Client', 'Repeater', 'Bridge', 'AP Router', and 'AP Client Router (WISP Client)'. A 'Next' button is located at the bottom right of the selection area.

tp-link PHAROS

Operation Mode: Access Point 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 **LAN Settings** section, specify the LAN IP address and the Subnet Mask for the device. Then, click Next.

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

LAN Settings

IP Address:

192.168.0.254

Subnet Mask:

255.255.255.0

Back

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					
Region: United States					
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					
MAXtream: ☐ Enable 					
BackNext					

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

Region: United States

Mode: 802.11a/n

Channel Width: 20/40MHz

Channel/Frequency: Auto

Security: None

Distance Setting: 0 km

MAXtream: Disable

Back

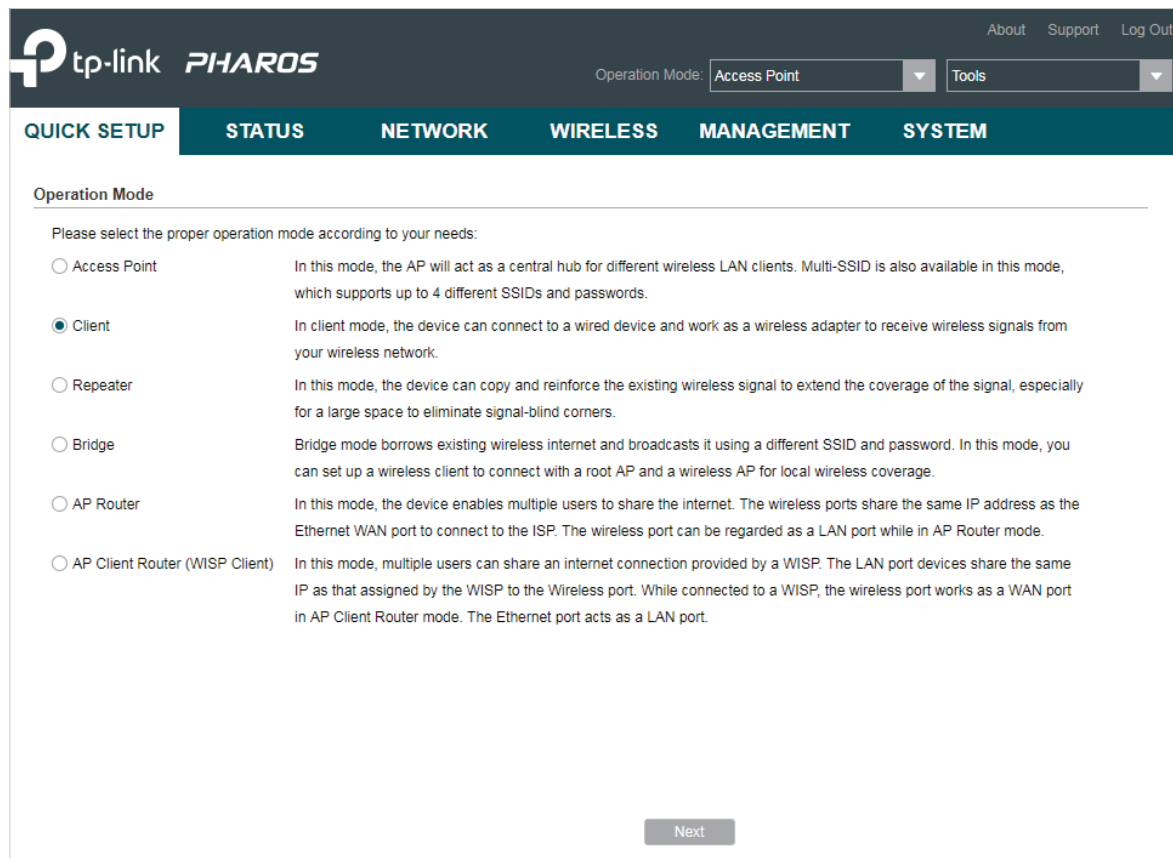
Finish

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 header with the TP-Link logo, the model name 'PHAROS', and links for 'About', 'Support', and 'Log Out'. Below the header is a navigation bar with tabs: 'QUICK SETUP' (active), 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is selected, and the 'Operation Mode' section is displayed. The 'Operation Mode' section has a title 'Operation Mode' and a subtitle '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 'Operation Mode' section, 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' page within a configuration 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 'LAN Settings' section is titled. 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 Client Settings** section, click *Survey* to search for the upstream wireless network.

The screenshot shows the 'Wireless Client Settings' page within the same configuration interface. The navigation bar at the top is identical, with 'QUICK SETUP' selected. The 'Wireless Client Settings' section is titled. It contains several input fields and a 'Survey' button. The fields are: 'SSID of Remote AP' (empty), 'MAC of Remote AP' (empty), 'Region' (set to 'United States'), 'Mode' (set to '802.11a/n'), 'WDS' (set to 'Auto'), 'Channel Width' (set to '20/40MHz'), 'Security' (set to 'None'), and 'PSK Password' (empty). There is a 'Show' checkbox next to the 'PSK Password' field. A 'Survey' button is located to the right of the 'SSID of Remote AP' field. Below the 'PSK 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, 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.

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

Wireless Client Settings

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

Back Refresh Connect Lock to AP

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](#).

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

Wireless Client Settings

SSID of Remote AP: 7200_5G

MAC of Remote AP: 50-C7-BF-01-88-1F

Region: United States

Mode: 802.11a/n

WDS: Auto

Channel Width: 20/40MHz

Security: WPA-PSK / WPA2-PSK

PSK Password: *****

Distance Setting: 0 (0-27.9)km

Survey

☐ Lock to AP

☐ Show

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

Back Next

6. 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: Client

LAN IP Address: 192.168.0.254

LAN Subnet Mask: 255.255.255.0

SSID of Remote AP: TP-LINK DC91 5G

Region: United States

Mode: 802.11a/n

WDS: Auto

Channel Width: 20/40MHz

Security: WPA-PSK / WPA2-PSK

Distance Setting: 0 km

Back

Finish

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

Repeater

Follow the steps below to configure the device as Repeater 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 header with the TP-Link logo, the model name 'PHAROS', and links for 'About', 'Support', and 'Log Out'. Below the header is a navigation bar with tabs: 'QUICK SETUP', 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is active. In the top right corner of the main content area, there is a dropdown menu for 'Operation Mode' currently set to 'Client', and a 'Tools' button. The main content area is titled 'Operation Mode' and contains a section with the text 'Please select the proper operation mode according to your needs:'. Below this text are six 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.

tp-link PHAROS

Operation Mode: Client 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 **LAN Settings** section, specify the LAN IP address and the Subnet Mask for the device. Then, click Next.

The screenshot shows the 'LAN Settings' page within a web interface. 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 'LAN Settings' is displayed. 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 the 'Wireless Client Settings' page within a web interface. 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 'Wireless Client Settings' is displayed. The main content area contains several input fields and a 'Survey' button. The fields are: 'SSID of Remote AP:', 'MAC of Remote AP:', 'Region:' (set to 'United States'), 'Mode:' (set to '802.11a/n'), 'WDS:' (set to 'Auto'), 'Channel Width:' (set to '20/40MHz'), 'Security:' (set to 'None'), and 'PSK Password:'. There is a 'Show' checkbox next to the 'PSK Password' field. A 'Survey' button is located to the right of the 'SSID of Remote AP' field. Below the 'PSK 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'.

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.

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

Wireless Client Settings

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

Back Refresh Connect Lock to AP

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](#).

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

Wireless Client Settings

SSID of Remote AP: 7200_5G

MAC of Remote AP: 50-C7-BF-01-88-1F

Region: United States

Mode: 802.11a/n

WDS: Auto

Channel Width: 20/40MHz

Security: WPA-PSK / WPA2-PSK

PSK Password: *****

Distance Setting: 0 (0-27.9)km

Survey

☐ Lock to AP

Show

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

Back Next

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

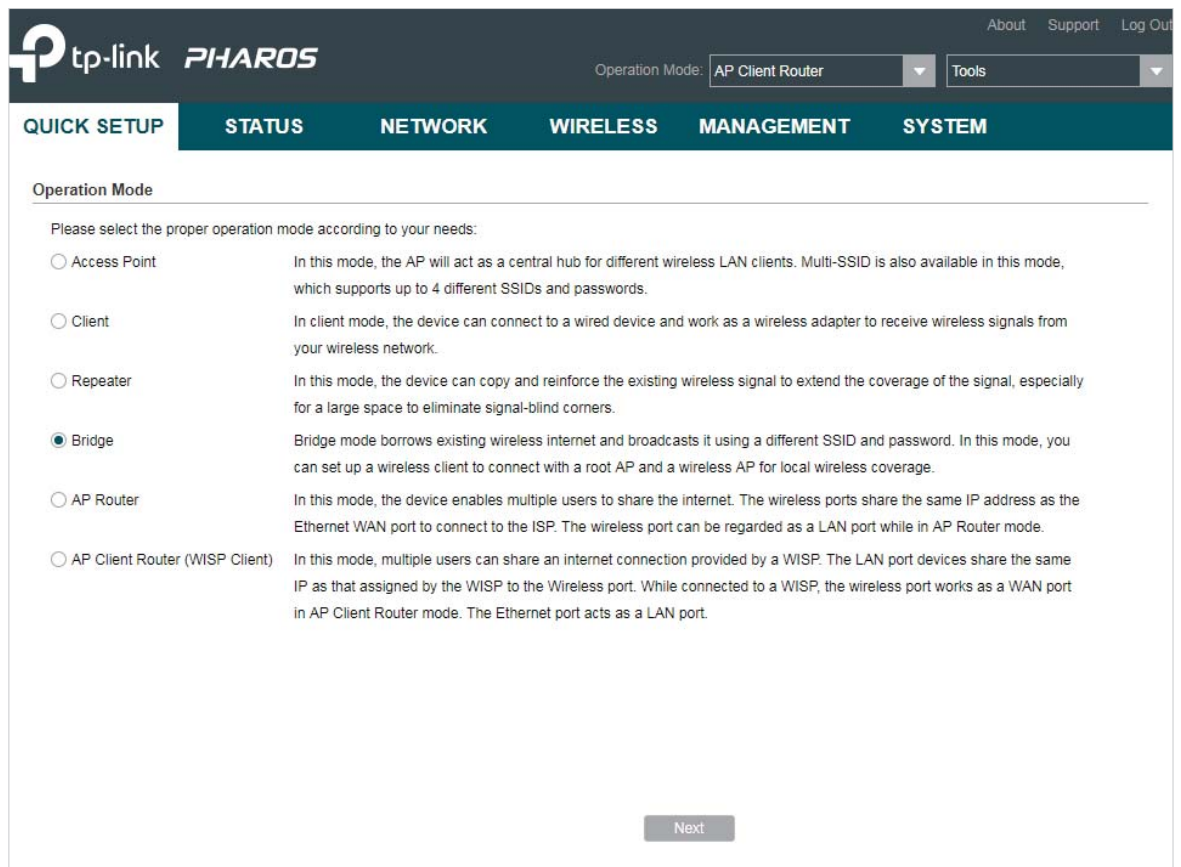
QUICK SETUP	STATUS	NETWORK	WIRELESS	MANAGEMENT	SYSTEM
Finish					
Operation Mode: Repeater					
IP Address: 192.168.0.254					
Subnet Mask: 255.255.255.0					
SSID of Remote AP: 7200_5G					
Region: United States					
Mode: 802.11a/n					
WDS: Disable					
Channel Width: 20/40MHz					
Security: WPA-PSK / WPA2-PSK					
Distance Setting: 0 km					
BackFinish					

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's a header with the TP-Link logo, the model name 'PHAROS', and links for 'About', 'Support', and 'Log Out'. Below the header is a navigation bar with tabs: 'QUICK SETUP' (active), 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' page displays the 'Operation Mode' section. It asks the user to select the proper operation mode. The 'Bridge' mode is selected with a radio button. Below the 'Bridge' mode, there is a description: '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.' At the bottom right of the 'Operation Mode' section, there is a 'Next' button.

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

The screenshot shows the 'LAN Settings' page within a web interface. 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 'LAN Settings' is displayed. 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 the 'Wireless Client Settings' page within a web interface. 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 'Wireless Client Settings' is displayed. The main content area contains several input fields and a 'Survey' button. The fields are: 'SSID of Remote AP:', 'MAC of Remote AP:', 'Region:' (set to 'United States'), 'Mode:' (set to '802.11a/n'), 'WDS:' (set to 'Auto'), 'Channel Width:' (set to '20/40MHz'), 'Security:' (set to 'None'), and 'PSK Password:'. There is a 'Survey' button next to the 'SSID of Remote AP' field. A checkbox labeled 'Lock to AP' is also present. A note states: '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.

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

Wireless Client Settings

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

Back Refresh Connect Lock to AP

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](#).

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

Wireless Client Settings

SSID of Remote AP: 7200_5G

MAC of Remote AP: 50-C7-BF-01-88-1F

Region: United States

Mode: 802.11a/n

WDS: Auto

Channel Width: 20/40MHz

Security: WPA-PSK / WPA2-PSK

PSK Password: *****

Distance Setting: 0 (0-27.9)km

Survey

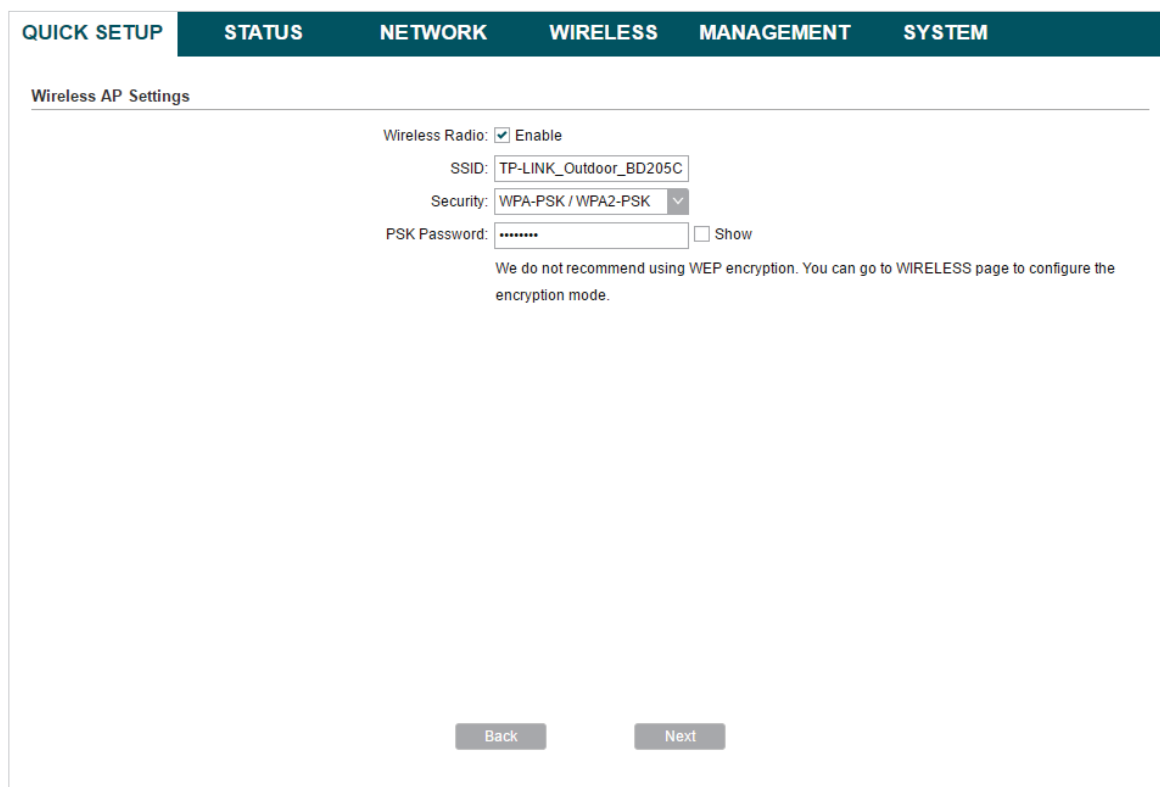
☐ Lock to AP

☐ Show

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

Back Next

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

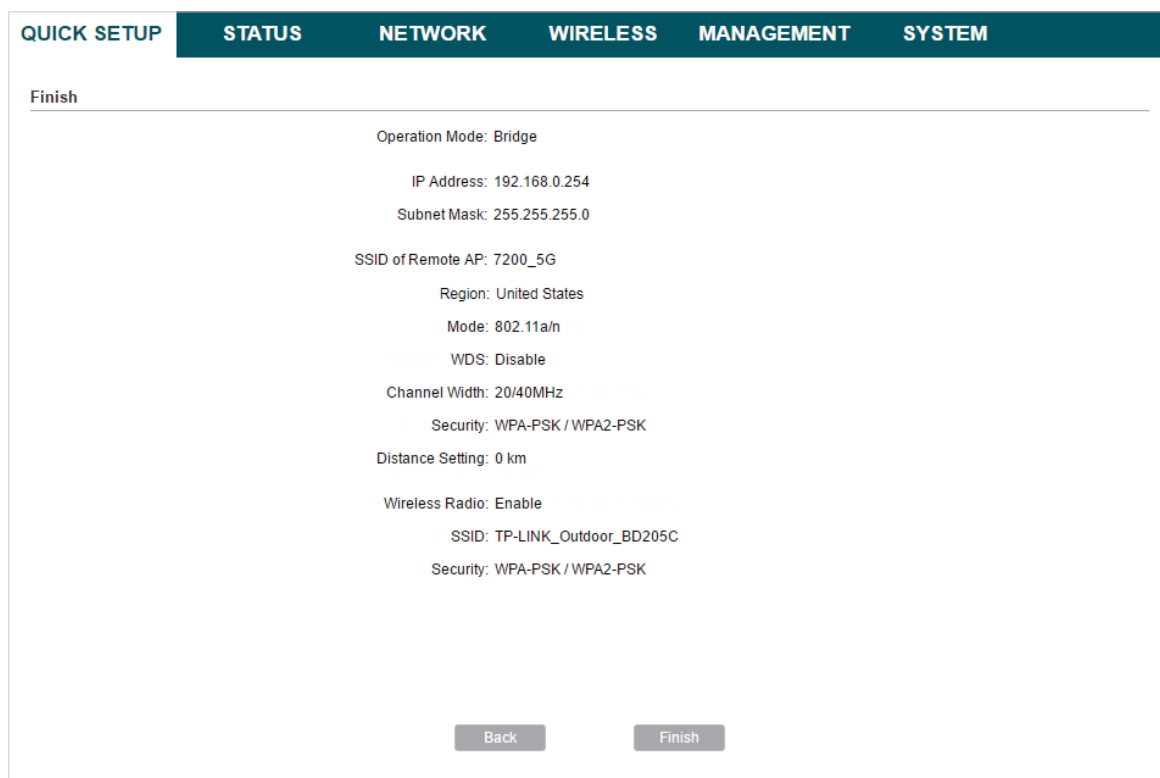


The screenshot shows the 'Wireless AP Settings' page in a web interface. At the top, there is a navigation bar with tabs: QUICK SETUP, STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. The 'QUICK SETUP' tab is active. Below the navigation bar, the page title is 'Wireless AP Settings'. The main content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

- Wireless Radio: ☒ Enable
- SSID: TP-LINK_Outdoor_BD205C
- Security: WPA-PSK / WPA2-PSK (dropdown menu)
- PSK Password: [masked with dots] ☐ Show

Below the settings, 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 same web interface. The navigation bar is identical, with 'QUICK SETUP' selected. The page title is 'Finish'. The main content area displays a summary of the configured settings:

- Operation Mode: Bridge
- IP Address: 192.168.0.254
- Subnet Mask: 255.255.255.0
- SSID of Remote AP: 7200_5G
- Region: United States
- 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

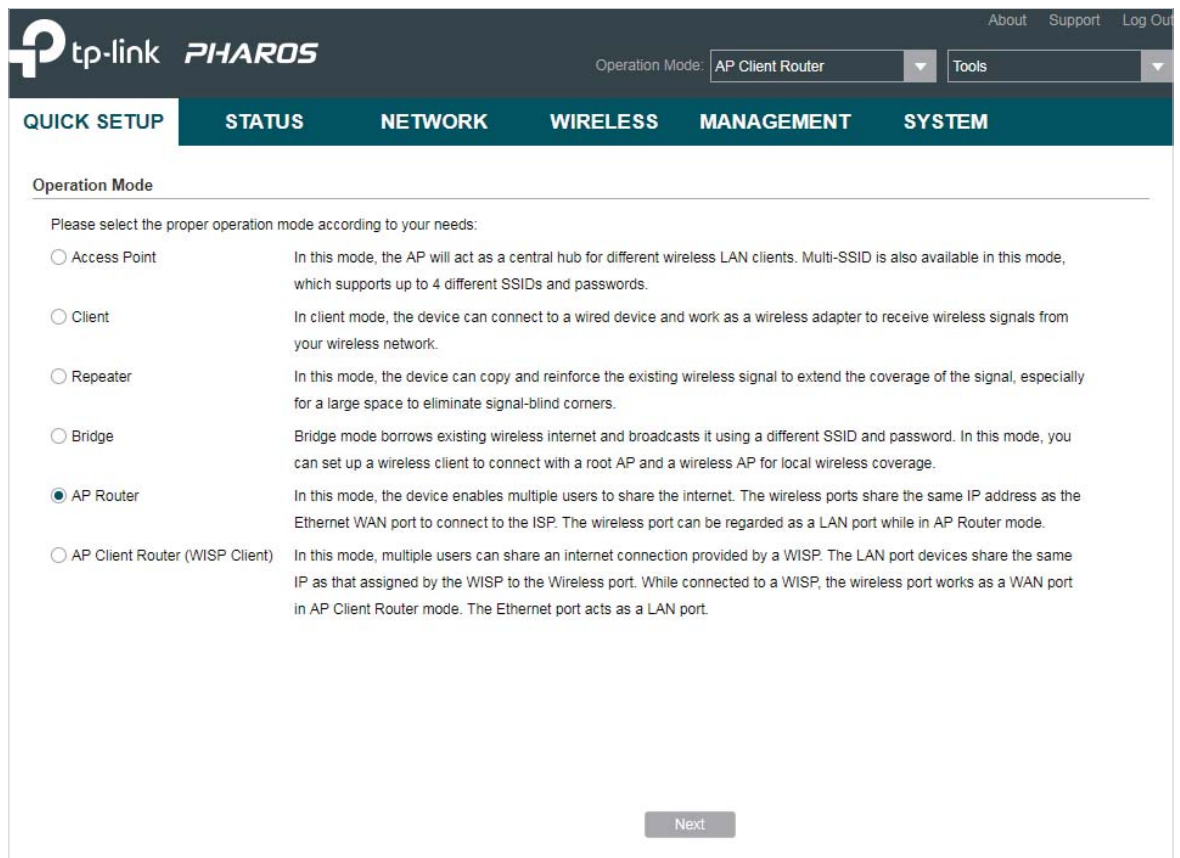
At the bottom of the page, there are two buttons: 'Back' and 'Finish'.

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**.



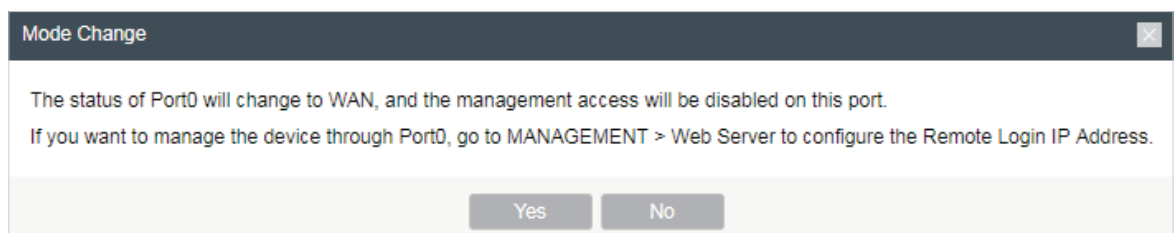
The screenshot shows the TP-Link PHAROS web interface. At the top, there's a header with the TP-Link logo, the model name 'PHAROS', and links for 'About', 'Support', and 'Log Out'. Below the header is a navigation bar with tabs: 'QUICK SETUP' (active), 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' page displays the 'Operation Mode' section. It asks the user to select the proper operation mode. There are six radio button options: 'Access Point', 'Client', 'Repeater', 'Bridge', 'AP Router' (selected), and 'AP Client Router (WISP Client)'. Each option has a brief description of its function. A 'Next' button is located at the bottom right of the selection area.

Operation Mode	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.

Note:

The following window will pop up. Click Yes.

- For CPE210/CPE510/CPE610



The screenshot shows a 'Mode Change' dialog box. The text inside reads: 'The status of Port0 will change to WAN, and the management access will be disabled on this port. If you want to manage the device through Port0, go to MANAGEMENT > Web Server to configure the Remote Login IP Address.' At the bottom, there are two buttons: 'Yes' and 'No'.

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

- For CPE220/WBS210/WBS510

Mode Change

The status of Port0 will change to WAN, and the management access will be disabled on this port.

Connect to the Port1 of the device or wirelessly to manage it.

If you want to manage the device through Port0, go to MANAGEMENT > Web Server to configure the Remote Login IP Address.

Yes

No

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

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

QUICK SETUP

STATUS

NETWORK

WIRELESS

MANAGEMENT

SYSTEM

WAN Connection Type

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.

Back

Next

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

■ PPPoE

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

The screenshot shows a web-based configuration interface for a router. At the top, there is a dark teal 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 three input fields for PPPoE configuration: **User Name:** with a text input box, **Password:** with a text input box and a ☐ **Show** toggle, and **Confirm Password:** with a text input box and a ☐ **Show** toggle. 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 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					
Region: United States					
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					
MAXtream: ☐ Enable ?					
BackNext					

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

The screenshot shows the 'Finish' section of the 'QUICK SETUP' menu. The menu has tabs for QUICK SETUP, STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. The 'Finish' section displays the following configuration details:

- 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
- Region: United States
- Mode: 802.11a/n
- Channel Width: 20/40MHz
- Security: None
- Distance Setting: 0 km
- MAXtream: Disable

At the bottom of the section 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's a header with the TP-Link logo, the model name 'PHAROS', and links for 'About', 'Support', and 'Log Out'. Below the header is a navigation bar with tabs: 'QUICK SETUP' (active), 'STATUS', 'NETWORK', 'WIRELESS', 'MANAGEMENT', and 'SYSTEM'. The 'QUICK SETUP' tab is selected, and the 'Operation Mode' section is displayed. It asks the user to select the proper operation mode. There are six radio button options: 'Access Point', 'Client', 'Repeater', 'Bridge', 'AP Router', and 'AP Client Router (WISP Client)'. The 'AP Client Router (WISP Client)' option is selected. Each option has a brief description of its function. At the bottom right of the selection area is a 'Next' button.

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

Note:

The following window will pop up. Click Yes.

The screenshot shows a 'Mode Change' dialog box. It contains the following text: 'You will not access the device through the WISP network. Connect to the port of the device or wirelessly to manage it. If you want to manage the device through the WISP network, go to MANAGEMENT > Web Server to configure the Remote Login IP Address.' At the bottom of the dialog box are two buttons: 'Yes' and 'No'.

Mode Change

You will not access the device through the WISP network.
Connect to the port of the device or wirelessly to manage it.
If you want to manage the device through the WISP network, go to MANAGEMENT > Web Server to configure the Remote Login IP Address.

Yes No

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

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

The screenshot shows a web interface for configuring a router. At the top, there is a navigation bar with tabs: **QUICK SETUP**, **STATUS**, **NETWORK**, **WIRELESS**, **MANAGEMENT**, and **SYSTEM**. The **QUICK SETUP** tab is active. Below the navigation bar, the section is titled **WAN Connection Type**. Under this title, there is a text prompt: "Select the connection type of WAN port according to your needs.:". Below the prompt, there are three radio button options:
1. ☐ PPPoE - For this connection, you need to get the account name and password from your ISP.
2. ☒ Dynamic IP - When connecting to the WAN, your router gets an IP address assigned by the DHCP server of your ISP.
3. ☐ Static IP - With this type of connection, the device uses a permanent, static IP address assigned by your ISP.
At the bottom of the form, there are two buttons: **Back** and **Next**.

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

■ PPPoE

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

The screenshot shows a web-based configuration interface for a router. At the top, there is a dark teal navigation bar with the following tabs: **QUICK SETUP**, **STATUS**, **NETWORK**, **WIRELESS**, **MANAGEMENT**, and **SYSTEM**. The **QUICK SETUP** tab is currently selected. Below the navigation bar, the page is titled **WAN Settings**. The main content area contains three input fields for PPPoE configuration: **User Name:** with a text input box, **Password:** with a text input box and a ☐ **Show** toggle, and **Confirm Password:** with a text input box and a ☐ **Show** toggle. 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)

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:		Survey
MAC of Remote AP:		☐ Lock to AP
Region:	United States	▼
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

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.

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

Wireless Client Settings

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

Back Refresh Connect Lock to AP

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](#).

QUICK SETUP **STATUS** **NETWORK** **WIRELESS** **MANAGEMENT** **SYSTEM**

Wireless Client Settings

SSID of Remote AP: 7200_5G

MAC of Remote AP: 50-C7-BF-01-88-1F

Region: United States

Mode: 802.11a/n

WDS: Auto

Channel Width: 20/40MHz

Security: WPA-PSK / WPA2-PSK

PSK Password: *****

Distance Setting: 0 (0-27.9)km

Survey

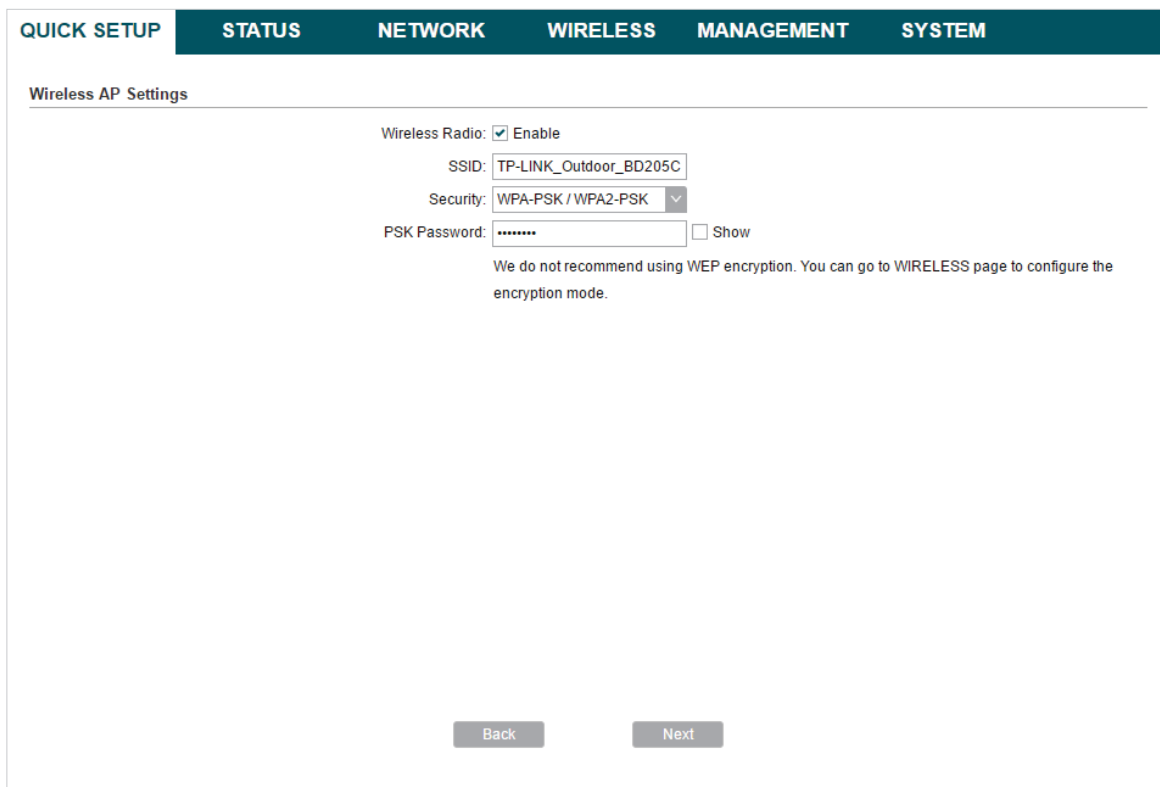
☐ Lock to AP

Show

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

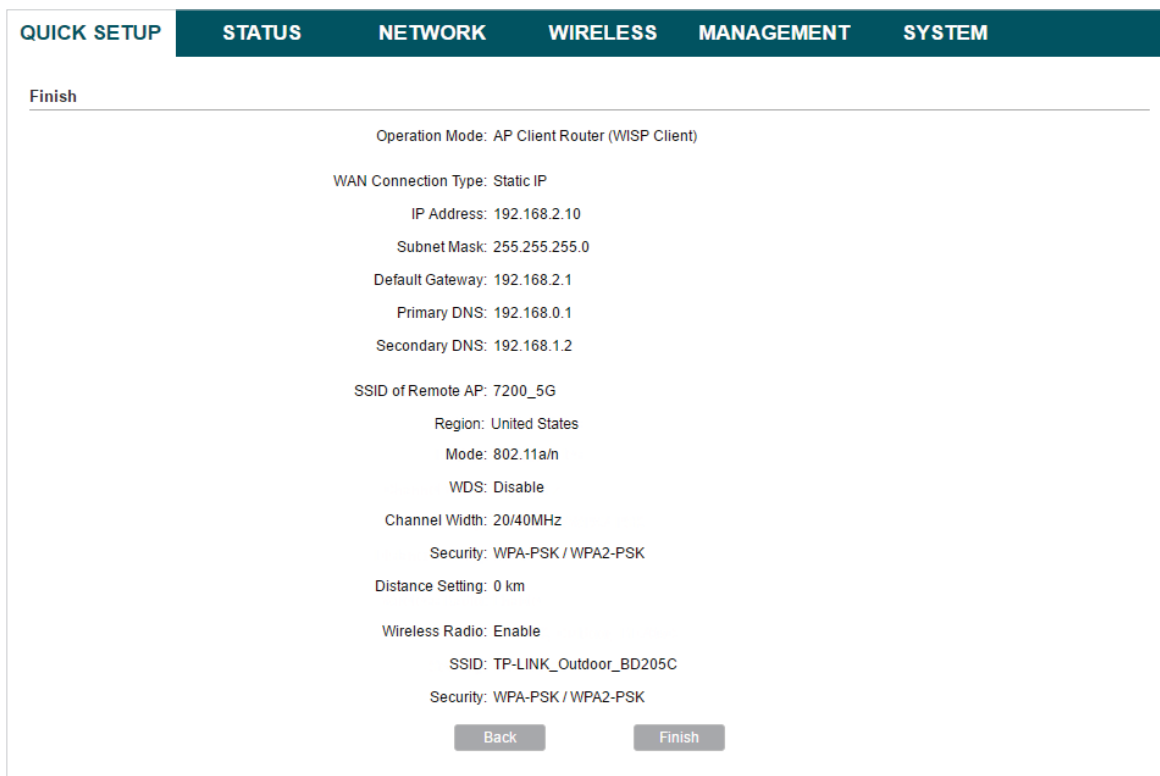
Back Next

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, STATUS, NETWORK, WIRELESS, MANAGEMENT, and SYSTEM. The 'WIRELESS' tab is selected. Below the navigation bar, the page title is 'Wireless AP Settings'. The configuration area includes: 'Wireless Radio' with a checked 'Enable' checkbox; 'SSID' with a text field containing 'TP-LINK_Outdoor_BD205C'; 'Security' with a dropdown menu showing 'WPA-PSK / WPA2-PSK'; and 'PSK Password' with a text field containing eight asterisks and a 'Show' checkbox. A note states: 'We do not recommend using WEP encryption. You can go to WIRELESS page to configure the encryption mode.' At the bottom, there are 'Back' and 'Next' buttons.

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



The screenshot shows the 'Finish' page in the same web interface. The navigation bar is identical, with 'WIRELESS' selected. The page title is 'Finish'. The configuration summary includes: 'Operation Mode: AP Client Router (WISP Client)'; 'WAN Connection Type: Static IP' with details: IP Address: 192.168.2.10, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.2.1, Primary DNS: 192.168.0.1, and Secondary DNS: 192.168.1.2; 'SSID of Remote AP: 7200_5G' with details: Region: United States, Mode: 802.11a/n, WDS: Disable, Channel Width: 20/40MHz, Security: WPA-PSK / WPA2-PSK, and Distance Setting: 0 km; and 'Wireless Radio: Enable' with details: SSID: TP-LINK_Outdoor_BD205C and Security: WPA-PSK / WPA2-PSK. At the bottom, there are 'Back' and 'Finish' buttons.

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

3

Monitor the Network

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

3.1 View the Device Information

3.2 View the Wireless Settings

3.3 View Wireless Signal Quality

3.4 View Radio Status

3.5 View the LAN Settings

3.6 View the WAN Settings

3.7 Monitor Throughput

3.8 Monitor Stations

3.9 Monitor Interfaces

3.10 Monitor ARP Table

3.11 Monitor Routes

3.12 Monitor DHCP Clients

3.13 Monitor Dynamic WAN

3.1 View the Device Information

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

Device Information	
Device Name:	CPE 510
Device Model:	CPE510 v3.0
Firmware Version:	2.0.0 Build 20160908 Rel. 36610 (5553)
System Time:	2015-01-01 04:37:41
Uptime:	0 days 04:37:43
CPU:	1%
Memory:	53%

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

3.2 View the Wireless Settings

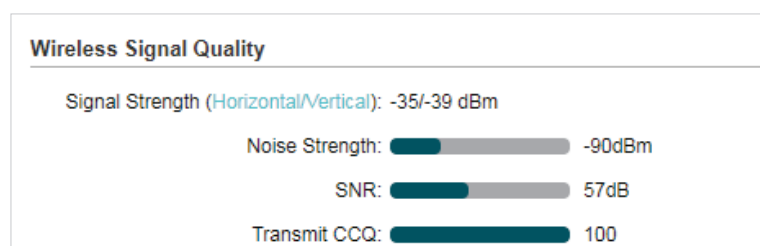
Go to the **STATUS** page. In the **Wireless Settings** section, view the parameters of the wireless network created by the device. To configure the parameters, refer to [5. Configure the Wireless Parameters](#).

Wireless Settings	
MAXtream:	OFF
Region:	United States
Channel/Frequency:	44 / 5220MHz
Channel Width:	20/40MHz
IEEE802.11 Mode:	A/N Mixed
Max TX Rate:	300.0Mbps
Antenna:	Feed Only - 7dBi
Transmit Power:	3dBm
Distance:	0.0km

MAXtream	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. Note: MAXtream Technology is only compatible with Pharos series products. Working with products from other manufacturer will cause network fault.
Region	Displays the region where you use the device. Available channels and maximum Transmit Power will be determined by the selected region according to the local laws and regulations.
Channel/ Frequency	Displays the channel and frequency which are currently used by the device.
Channel Width	Displays the channel width which is currently used by the device.
IEEE802.11 Mode	Displays the IEEE802.11 protocol currently used by the device.
Max TX Rate	Displays the maximum data rate of the device during the sending of the wireless packets.
Antenna	Displays the antenna that you use.
Transmit Power	Displays the transmit power which is currently used by the device.
Distance	Displays the wireless coverage distance. In the coverage of the device, the clients can be placed to get good wireless performance.

3.3 View Wireless Signal Quality

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



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

3.4 View Radio Status

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

Radio Status

AP: Enabled

MAC Address: 98-DE-D0-88-6C-84

SSID: TP-LINK_Outdoor_886C84

Security Mode: None

Connected Stations: 0

Client: Disabled

MAC Address: N/A

Security Mode: N/A

WDS: N/A

Root AP BSSID: N/A

Root AP SSID: N/A

TX Rate: N/A

RX Rate: N/A

Connection Time: N/A

AP	Displays the status of the wireless AP function. With this enabled, the device can provide a wireless network for the clients. By default, it is enabled in Access Point, Repeater, Bridge, AP Router and AP Client Router Modes and disabled in Client Mode.
----	---

MAC Address	Displays the MAC address of the wireless interface connected to the clients.
SSID	Displays the wireless network name (SSID) created by the device.
Security Mode	Displays the security mode you've selected for your wireless network. There are three security modes: WPA-PSK, WPA and WEP. None means that no security mode is selected and all the hosts are allowed to access the wireless network directly. The security mode which is set on the clients should be the same as that on this device.
Connected Stations	Displays the number of the connected stations.
Client	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. None means that no security mode is selected and all the hosts are allowed to access the wireless network directly. The security mode which is set on the device should be the same as that on the root AP.
WDS	Displays the status of the WDS (Wireless Distribution System) function. WDS is a communication system among multiple wireless networks . It is established between APs through wireless connection. WDS is used during the connection process between the device and the root AP. Enable: Forward data frames using four address fields. Disable: Forward data frames using three address fields. Auto: The device automatically negotiates the wireless data frame structure (three or four address fields) with the root AP. The selection of Auto is recommended.
Root AP BSSID	Displays the BSSID (Basic Service Set ID) of the root AP. BSSID is used to identify a BSS. Each BSS has its own BSSID. The BSSID is decided by the manufacturers, and it is usually related to the device's MAC address.
Root AP SSID	Displays the wireless network name of the root AP.
TX Rate	Displays the data rate of the device during the sending of the wireless packets.

RX Rate	Displays the data rate of the device during the receiving of the wireless packets.
Connection Time	Displays the amount of time the device has been connected to the root AP.

3.5 View the LAN Settings

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

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 IPv6 IP Address/Prefix: N/A

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

3.6 View the WAN Settings

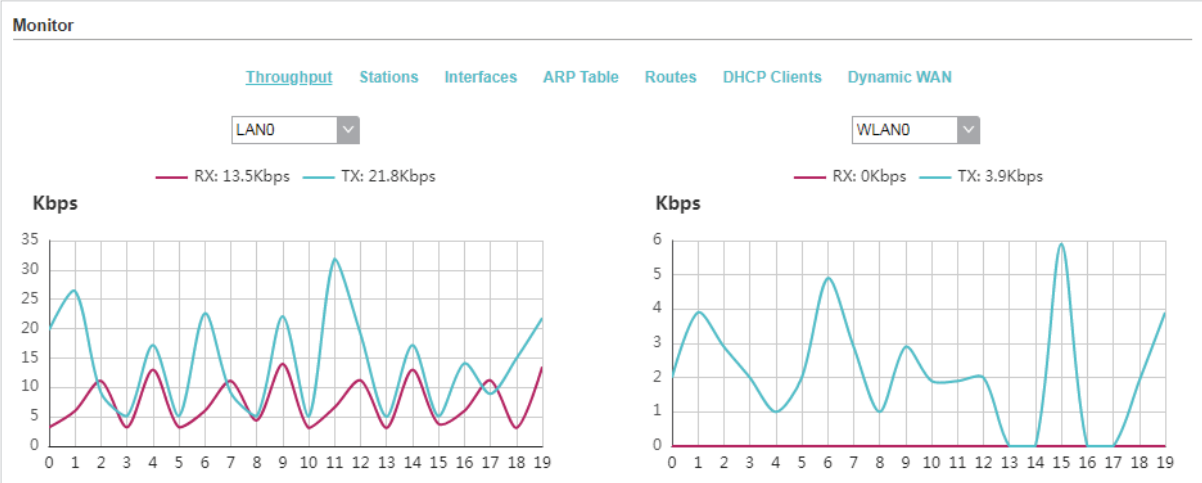
Go to the **STATUS** page. In the **WAN** section, view the WAN information of the device. To configure the WAN settings, refer to [4. Configure the Network](#).

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
IPv6 IP Address/Prefix: N/A
IPv6 Gateway: N/A
IPv6 DNS: N/A

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

3.7 Monitor Throughput

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



3.8 Monitor Stations

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

Monitor

Throughput Stations Interfaces ARP Table Routes DHCP Clients Dynamic WAN

MAC Address	Device Name	Associated SSID	Signal / Noise(dBm) Chain0/Chain1	CCQ (%)	Negotiated Rate (Mbps)	Data TX / RX (kbps)	Distance (km)	IP Address	Connection Time
E4-B2-FB-7B-02-7F	CPE510	TP-Link_Outdoor_EF44BC	-44/-34,-90/-90	93	300.0	169/3962	0.00	192.168.0.100	0 days 00:04:01

☒ 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. There are two display modes. Values of the two chains are displayed separately in Chain0/Chain1 Mode, and together in Combined Mode. You can switch between display modes by clicking on it.

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

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

Station:E4-B2-FB-7B-02-7F

Device Name:	Negotiated Rate	Last Signal, dBm
Product:	6.0Mbps	N/A
Firmware:	9.0Mbps	N/A
Connection Time: 00:10:30	12.0Mbps	N/A
RX Signal: -33 dBm	18.0Mbps	N/A
Noise Floor: -90 dBm	24.0Mbps	-33
CCQ: 100%	36.0Mbps	N/A
Last IP: 192.168.0.101	48.0Mbps	N/A
	54.0Mbps	N/A

TX/RX Rate: 300.0Mbps / 24.0Mbps
TX/RX Bit Rate: 0.00kbps / 0.00kbps
TX/RX Packets: 553 / 2241
TX/RX Packets Rate,pps: 0 / 0
Bytes Transmitted: 87653 (85.60kBytes)
Bytes Received: 169733 (165.75kBytes)

Refresh

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

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

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

3.9 Monitor Interfaces

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

		Throughput	Stations	Interfaces	ARP Table	Routes	DHCP Clients
Interface	MAC	IP Address	MTU	RX Packets	RX Bytes	TX packets	TX Bytes
LAN0	30-B5-C2-BD-20-CC	0.0.0.0	1500	0	0	0	0
LAN1	30-B5-C2-BD-20-CC	0.0.0.0 fe80::203:7fff:feff:ffe/64	1500	40336	5M	13691	4M
BRIDGE	30-B5-C2-BD-20-CC	192.168.0.251 fe80::32b5:c2ff:febd:20cc/64	1500	40245	4M	13697	3M
WLAN0	30-B5-C2-BD-20-CC	0.0.0.0 fe80::32b5:c2ff:febd:20cc/64	1500	0	0	0	0

☒ Auto Refresh

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

3.10 Monitor ARP Table

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

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

Monitor		
Throughput Stations Interfaces ARP Table Routes DHCP Clients		
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

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

3.11 Monitor Routes

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

Monitor			
Throughput Stations Interfaces ARP Table Routes DHCP Clients			
IPv4 Routes			
Destination	Gateway	SubnetMask	Interface
192.168.0.0	0.0.0.0	255.255.255.0	BRIDGE
IPv6 Routes			
Destination	Gateway	Interface	
fe80::	::	LAN0	

☒ Auto Refresh

- IPv4 Routes

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

Interface	Displays the interface that the destination device is on.
-----------	---

- IPv6 Routes

Destination	Displays the IPv6 address of the destination device or destination network.
-------------	---

Gateway	Displays the IPv6 address of the appropriate gateway.
---------	---

Interface	Displays the interface that the destination device is on.
-----------	---

3.12 Monitor DHCP Clients

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

Throughput	Stations	Interfaces	ARP Table	Routes	DHCP Clients	Dynamic WAN
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 monitor the WAN connection status of the device. You can enable or disable Auto Refresh. With this feature enabled, the table will refresh automatically.

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

DHCP Status

Status: Disconnected

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway IP: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Connection Uptime: 0 days 00:00:00

Obtain

Release

DHCPv6 Status

Status: Connected

IP Address:

Subnet Mask:

Gateway IP:

Primary DNS:

Secondary DNS:

Connection Uptime: 0 days 00:00:00

Obtain

Release

☒ Auto Refresh

- DHCP Status

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

- DHCPv6 Status

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

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

4 **Configure the Network**

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

4.1 Configure WAN Parameters

4.2 Configure LAN Parameters

4.3 Configure Management VLAN

4.4 Configure the Forwarding Feature

4.5 Configure the Security Feature

4.6 Configure Access Control

4.7 Configure Static Routing

4.8 Configure Bandwidth Control

4.9 Configure IP & MAC Binding

4.1 Configure WAN Parameters

Note:

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

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

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

WAN

Connection Type: Dynamic

IPv6: ☐ Enable

Advanced Settings

MTU Size: 1500

Use These DNS Servers: ☐ Enable

WAN MAC Address: 70-4F-57-EF-44-BD

Restore to Factory MAC

Your PC's MAC Address: 50-E5-49-1D-5D-9C

Clone PC's MAC

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.

WAN

Connection Type: Static

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Gateway IP: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

IPv6: ☐ Enable

Advanced Settings

MTU Size: 1500

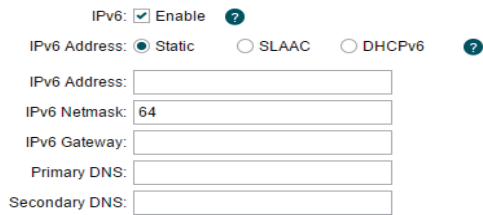
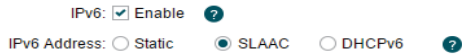
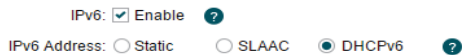
WAN MAC Address: 30-B5-C2-BD-20-5D

Restore to Factory MAC

Your PC's MAC Address: 00-19-66-35-E1-B0

Clone PC's MAC

IP address	Enter the IP address provided by your ISP.
Netmask	Enter the netmask provided by your ISP. Normally use 255.255.255.0.
Gateway IP	Enter the gateway IP address provided by your ISP.

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

■ Dynamic

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

WAN

Connection Type: Dynamic

IPv6: ☐ Enable ?

Advanced Settings

MTU Size: 1500

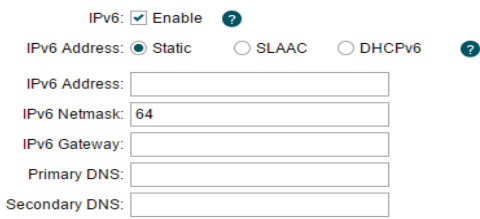
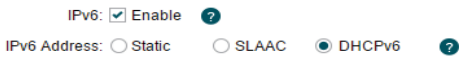
Use These DNS Servers: ☒ Enable

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

WAN MAC Address: 30-B5-C2-BD-02-2F Restore to Factory MAC

Your PC's MAC Address: 00-19-66-35-E1-B0 Clone PC's MAC

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

WAN MAC Address

Specify the WAN MAC address. This field displays the current MAC address of the WAN port. If your ISP binds the MAC address of your previous computer/router, enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Click *Restore Factory MAC* to restore the MAC address of WAN port to the factory default value.

Your PC's MAC Address

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

■ PPPoE

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

The screenshot shows the WAN configuration interface. At the top, the 'WAN' tab is selected. The 'Connection Type' is set to 'PPPoE'. Below this, there are fields for 'User Name' and 'Password', with a 'Show' checkbox next to the password field. The 'Connection Mode' is set to 'Automatic' and the 'Second Connection' is set to 'disabled'. There is an 'IPv6' section with an 'Enable' checkbox and a help icon. Below this is an 'Advanced Settings' section. Inside, there are fields for 'MTU Size' (1480), 'Service Name', 'AC Name', and 'Detect Interval' (0 seconds). There are checkboxes for 'Use ISP-Specified IP' (checked) and 'Use These DNS Servers' (checked). Below these are fields for 'ISP-Specified IP' (0.0.0.0), 'Primary DNS' (0.0.0.0), and 'Secondary DNS' (0.0.0.0). At the bottom, there are fields for 'WAN MAC Address' (30-B5-C2-BD-02-2F) and 'Your PC's MAC Address' (00-19-66-35-E1-B0), each with a button to 'Restore to Factory MAC' or 'Clone PC's MAC' respectively.

Specify the parameters below and click *Connect*:

User Name

Enter the User Name that is provided by your ISP.

Password

Enter the Password that is provided by your ISP.

Connection Mode

Select the Connection Mode.

- **On Demand**

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

Connection Mode:	On Demand	▼
Idle Time:	15	minutes

- **Automatic**

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

- **Time-based**

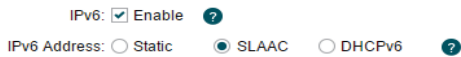
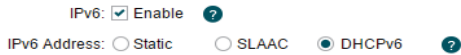
Configure the device to make it connect or disconnect based on time. Enter the start time in From (HH:MM) for connecting and end time in To (HH:MM) for disconnecting. If you need to control the time period of internet access, choose this mode.

Connection Mode:	Time-based	▼
From(HH:MM):	00:00	
To(HH:MM):	23:59	

- **Manual**

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

Connection Mode:	Manual	▼
Idle Time:	15	minutes

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

Use These DNS Servers	If the ISP provides a DNS server IP address for you, Enable Use These DNS Server, and fill the Primary DNS and Secondary DNS fields below. Otherwise, the DNS servers will obtain automatically from ISP.
WAN MAC Address	Specify the WAN MAC address. This field displays the current MAC address of the WAN port. If your ISP binds the MAC address of your previous computer/router, enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Click <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 device. 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.

The screenshot shows the WAN configuration window. At the top, the title is 'WAN'. Below it, there are several fields and buttons:

- Connection Type:** A dropdown menu set to 'L2TP'. To its right are 'Connect' and 'Disconnect' buttons.
- Server IP/Name:** An empty text input field.
- 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 'Dynamic'.
- IPv6:** A checkbox labeled 'Enable' with a question mark icon next to it.
- Advanced Settings:** A section with a collapse/expand icon and the text 'Advanced Settings'. Inside this section:
 - MTU Size:** A text input field containing '1460'.
 - WAN MAC Address:** A text input field containing '30-B5-C2-BD-20-5D'. 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.

Specify the parameters below and click *Connect*:

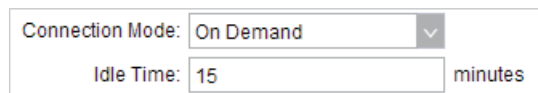
Server IP/Name	Enter the server IP address or the domain name provided by your ISP.
User Name	Enter the User Name provided by your ISP. This field is case-sensitive.
Password	Enter the Password provided by your ISP. This field is case-sensitive.

Connection Mode

Select the Connection Mode.

- **On Demand**

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



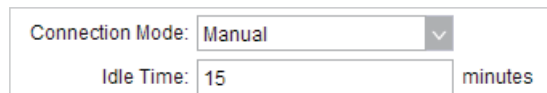
The screenshot shows a configuration box for the 'On Demand' connection mode. It contains two fields: 'Connection Mode:' with a dropdown menu set to 'On Demand', and 'Idle Time:' with a text input field containing '15' and a 'minutes' label to its right.

- **Automatic**

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

- **Manual**

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



The screenshot shows a configuration box for the 'Manual' connection mode. It contains two fields: 'Connection Mode:' with a dropdown menu set to 'Manual', and 'Idle Time:' with a text input field containing '15' and a 'minutes' label to its right.

Second Connection

If your ISP provides a Connection type such as Dynamic/Static IP to connect to a local area network, activate this secondary connection.

Dynamic IP: Use dynamic IP address to connect to the local area network provided by ISP.

Static IP: Use static IP address to connect to the local area network provided by ISP.

IPv6

Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a WAN IPv6 address. Select a method for the device to obtain the WAN IPv6 address according to the information provided by your ISP.

- **Static**

Select static and enter the WAN IPv6 address, IPv6 netmask, IPv6 gateway, primary DNS and secondary DNS provided by your ISP.

The screenshot shows the IPv6 configuration interface. At the top, 'IPv6' is checked and 'Enable' is selected with a help icon. Below, 'IPv6 Address' is set to 'Static' with a help icon. The 'IPv6 Address' field is empty, 'IPv6 Netmask' is set to '64', 'IPv6 Gateway' is empty, 'Primary DNS' is empty, and 'Secondary DNS' is empty.

- **SLAAC**

Select SLAAC and the device will obtain the WAN IPv6 address automatically.

The screenshot shows the IPv6 configuration interface. 'IPv6' is checked and 'Enable' is selected with a help icon. 'IPv6 Address' is set to 'SLAAC' with a help icon. 'Static' and 'DHCPv6' are unselected.

- **DHCPv6**

Select DHCPv6 and the device will obtain the WAN IPv6 address automatically.

The screenshot shows the IPv6 configuration interface. 'IPv6' is checked and 'Enable' is selected with a help icon. 'IPv6 Address' is set to 'DHCPv6' with a help icon. 'Static' and 'SLAAC' are unselected.

MTU Size

Specify the MTU size. The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. This number should be an integer between 576 and 2026.

WAN MAC Address

Specify the WAN MAC address. This field displays the current MAC address of the WAN port. If your ISP requires that you register the MAC address, enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Click *Restore Factory MAC* to restore the MAC address of WAN port to the factory default value.

Your PC's MAC Address

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

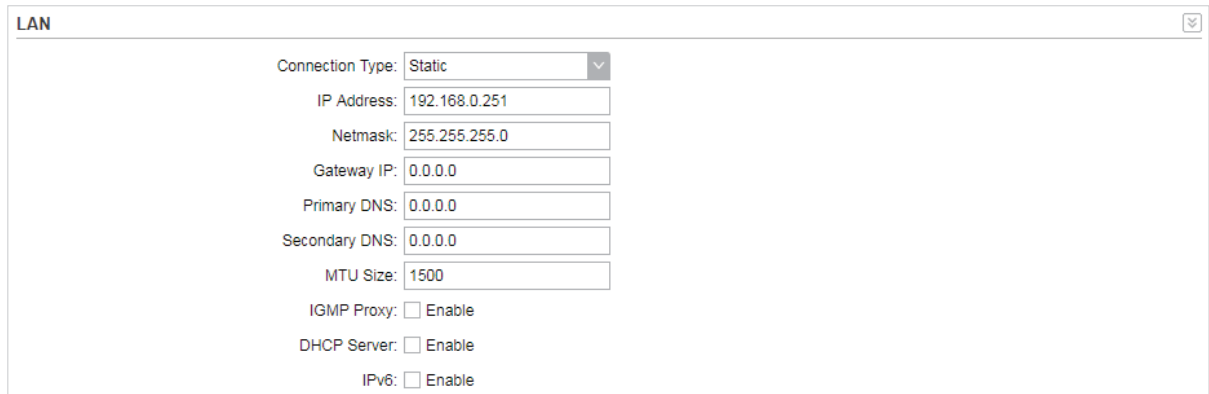
2. Click *Apply*, then click *Save*.

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.

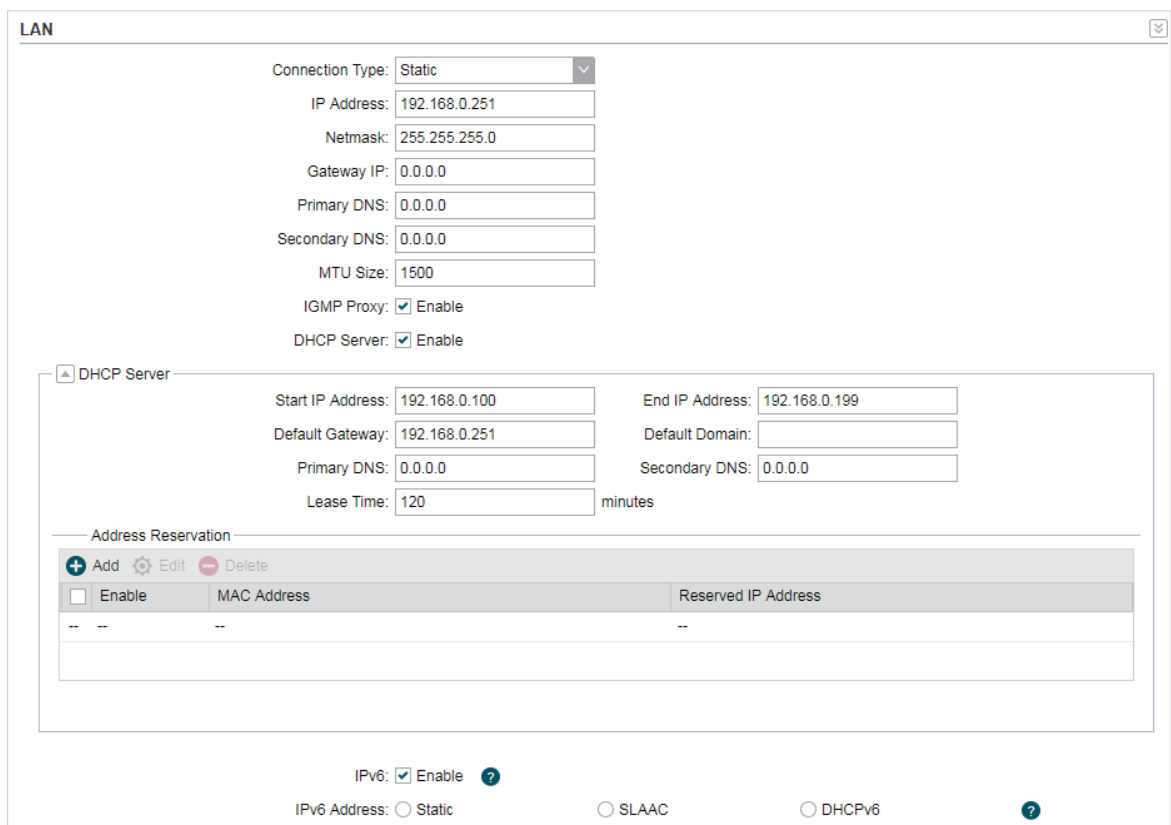


The screenshot shows the 'LAN' configuration window. The 'Connection Type' is set to 'Static'. The IP Address is 192.168.0.251, Netmask is 255.255.255.0, Gateway IP is 0.0.0.0, Primary DNS is 0.0.0.0, Secondary DNS is 0.0.0.0, and MTU Size is 1500. The checkboxes for IGMP Proxy, DHCP Server, and IPv6 are all disabled.

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



The screenshot shows the 'LAN' configuration window with the 'Static' connection type. The IP Address is 192.168.0.251, Netmask is 255.255.255.0, Gateway IP is 0.0.0.0, Primary DNS is 0.0.0.0, Secondary DNS is 0.0.0.0, and MTU Size is 1500. The checkboxes for IGMP Proxy and DHCP Server are enabled. The DHCP Server section is expanded, showing Start IP Address (192.168.0.100), End IP Address (192.168.0.199), Default Gateway (192.168.0.251), Default Domain, Primary DNS (0.0.0.0), Secondary DNS (0.0.0.0), and Lease Time (120 minutes). The Address Reservation section is also expanded, showing a table with columns for Enable, MAC Address, and Reserved IP Address. The IPv6 section is expanded, showing IPv6 enabled, with options for Static, SLAAC, and DHCPv6.

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

Secondary DNS	Enter the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0, which means no secondary DNS is assigned.
Lease Time	Enter the amount time of the leased IP address assigned by the DHCP server. When the time expires, the clients will request to renew the lease automatically.
Address Reservation	Enable Address Reservation and specify a reserved IP address for a PC on the local area network, so the PC will always obtain the same IP address each time when it starts up. Reserved IP addresses could be assigned to servers that require permanent IP settings.

To configure Address Reservation:

Click *Add*, specify the MAC address and the IP address. Enable this entry, then click *Save*.

IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a LAN IPv6 address. Select a method for the device to obtain the LAN IPv6 address according to the information provided by your ISP.
------	---

- **Static**

Select static and enter the LAN IPv6 address and IPv6 netmask.

- **SLAAC**

Select SLAAC and the device will obtain the LAN IPv6 address automatically.

- **DHCPv6**

Select DHCPv6 and the device will obtain the LAN IPv6 address automatically.

■ Dynamic

LAN

Connection Type:
Dynamic

Fallback IP:
☒ Enable

DHCP Fallback IP:

DHCP Fallback Mask:

Primary DNS:

Secondary DNS:

MTU Size:

IGMP Proxy:
☐ Enable

IPv6:
☒ Enable

IPv6 Address:
☒ Static
☐ SLAAC
☐ DHCPv6

IPv6 Address:

IPv6 Netmask:

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

IPv6

Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a LAN IPv6 address. Select a method for the device to obtain the LAN IPv6 address according to the information provided by your ISP.

- **Static**

Select static and enter the LAN IPv6 address and IPv6 netmask.

IPv6: ☒ Enable ?

IPv6 Address: ☒ Static ☐ SLAAC ☐ DHCPv6 ?

IPv6 Address:

IPv6 Netmask:

- **SLAAC**

Select SLAAC and the device will obtain the LAN IPv6 address automatically.

IPv6: ☒ Enable ?

IPv6 Address: ☐ Static ☒ SLAAC ☐ DHCPv6 ?

- **DHCPv6**

Select DHCPv6 and the device will obtain the LAN IPv6 address automatically.

IPv6: ☒ Enable ?

IPv6 Address: ☐ Static ☐ SLAAC ☒ DHCPv6 ?

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: Static

IP Address: 192.168.0.254

Netmask: 255.255.255.0

MTU Size: 1500

IGMP Proxy: ☒ Enable

DHCP Server: ☒ Enable

⌵ DHCP Server

Start IP Address: 192.168.0.100

End IP Address: 192.168.0.199

Default Gateway: 192.168.0.254

Default Domain:

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Lease Time: 120 minutes

Address Reservation

+ Add ⚙ Edit - Delete

☐ Enable	MAC Address	Reserved IP Address
--	--	--

IPv6: ☒ Enable ?

IPv6 Address: ☐ Static ☐ Prefix Delegation ?

IPv6 Address:

IPv6 Netmask: 64

IPv6 DHCP Server: ☐ Disabled ☒ Stateless ☐ Stateful ?

DNS Proxy: ☐ Enable ?

Preferred DNS:

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

IP address

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

Note:

When you change the LAN IP address in the **Network** tab, you should log in with the new IP address and save the settings for the configuration change to take effect. Otherwise the configuration will be lost after the reboot.

Netmask

Enter the Netmask provided by your ISP. Normally use 255.255.255.0.

MTU Size

Specify the MTU size. The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. This number should be an integer between 576 and 2026.

IGMP Proxy	Enable or disable IGMP (Internet Group Management Protocol) Proxy. IGMP proxy is used to process the multicast stream in the 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, which means no primary DNS is assigned.
Secondary DNS	Enter the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0, which means no secondary DNS is assigned.
Lease Time	Enter the amount time of the leased IP address assigned by the DHCP server. When the time expires, the clients will request to renew the lease automatically.
Address Reservation	Enable Address Reservation and specify a reserved IP address for a PC on the local area network, so the PC will always obtain the same IP address each time when it starts up. Reserved IP addresses could be assigned to servers that require permanent IP settings.

To configure Address Reservation:

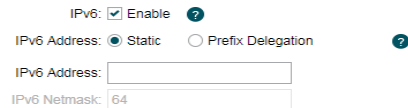
Click *Add*, specify the MAC address and the IP address. Enable this entry, then click *Save*.

IPv6

Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a LAN IPv6 address. Select a method for the device to obtain the LAN IPv6 address according to the information provided by your ISP.

- **Static**

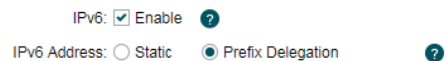
Select static and enter the LAN IPv6 address and IPv6 netmask.



IPv6: ☒ Enable ?
IPv6 Address: ☒ Static ☐ Prefix Delegation ?
IPv6 Address:
IPv6 Netmask: 64

- **Prefix Delegation**

Select Prefix Delegation and the device will obtain the LAN IPv6 address automatically.



IPv6: ☒ Enable ?
IPv6 Address: ☐ Static ☒ Prefix Delegation ?

IPv6 DHCP Server

Enable or disable the IPv6 DHCP server function. With IPv6 DHCP server enabled, the clients will obtain the IPv6 address from the DHCP server.

- **Disabled**

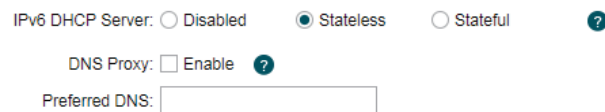
Select Disabled to disable the IPv6 DHCP server function



IPv6 DHCP Server: ☒ Disabled ☐ Stateless ☐ Stateful ?

- **Stateless/Stateful**

Select Stateless or Stateful, and the clients will obtain the IPv6 address from the IPv6 DHCP server automatically. Enable or disable the DNS proxy. With this feature enabled, the device will obtain the DNS server automatically. With this feature disabled, you should specify the DNS address manually.



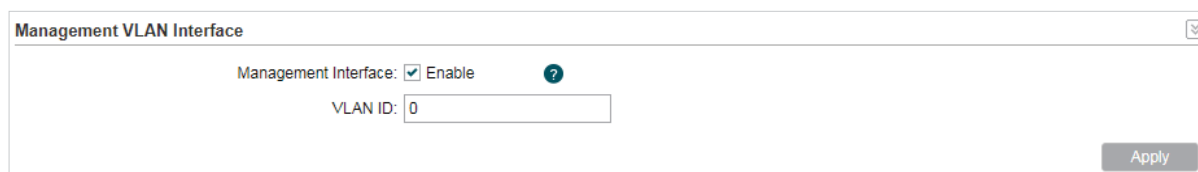
IPv6 DHCP Server: ☐ Disabled ☒ Stateless ☐ Stateful ?
DNS Proxy: ☐ Enable ?
Preferred DNS:

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

4.3 Configure Management VLAN

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

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



Management VLAN	Enable or disable the Management VLAN function. By default, it is disabled.
-----------------	---

VLAN ID	Specify the Management VLAN ID. The valid values are from 2 to 4094.
---------	--

4.4 Configure the Forwarding Feature

Note:

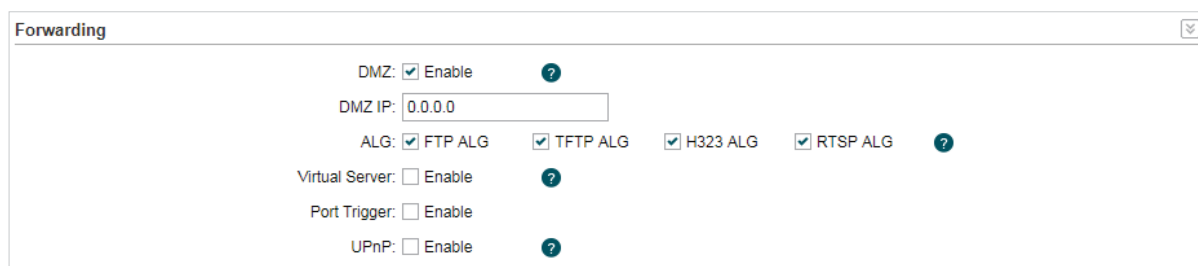
Forwarding submenu is only available in AP Router Mode and AP Client Router (WISP Client) Mode.

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

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

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

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



DMZ	Enable or disable the DMZ function. DMZ (Demilitarized Zone) specifically allows one computer/device behind NAT to become "demilitarized", so all packets from the external network are forwarded to this computer/device. The demilitarized host is exposed to the wide area network, which can realize the unlimited bidirectional communication between internal hosts and external hosts.
-----	---

DMZ IP	Specify the IP address of the local host network device. The DMZ host device will be completely exposed to the external network. Any PC that was used for a DMZ must have a static or reserved IP Address because its IP Address may change when using the DHCP function.
ALG	Select the type of ALG to enable the corresponding feature. Common NAT only translates the address of packets at network layer and the port number at transport layer but cannot deal with the packets with embedded source/destination information in the application layer. Application layer gateway (ALG) can deal with protocols with embedded source/destination information in the application payload. Some protocols such as FTP, TFTP, H323 and RTSP require ALG (Application Layer Gateway) support to pass through NAT. FTP ALG: Allows FTP clients and servers to transfer data across NAT. TFTP ALG: Allows TFTP clients and servers to transfer data across NAT. H323 ALG: Allows Microsoft NetMeeting clients to communicate across NAT. RTSP ALG: Allows some media player clients to communicate with some streaming media servers across NAT.

Virtual Server

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

Enable	IP	Internal Port	Service Port	Protocol
☒				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
☒			TCP/UDP

To configure port trigger:

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

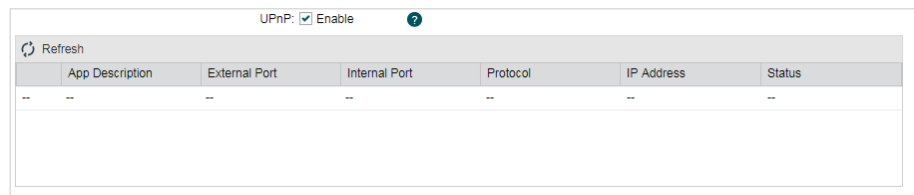
Incoming Port: Enter the incoming port for incoming traffic. The port or port range is used by the remote system when it responds to the outgoing request. A response to one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). 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: ☒ 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.

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

Protocol: Displays which type of protocol is opened.

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

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

4.5 Configure the Security Feature

Note:

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

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

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

Security

Basic

Firewall: ☒ SPI Firewall ?

Ping: ☐ WAN Ping Forbidden ☐ LAN Ping Forbidden

VPN: ☒ PPTP Passthrough ☒ L2TP Passthrough ☒ 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.

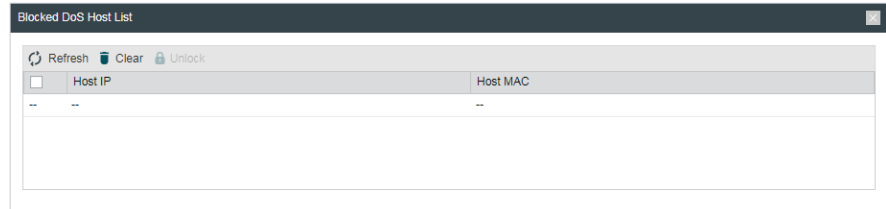
ICMP_FLOOD Attack Filter: Enter a value between 5 and 3600. The default value is 50. When the current ICMP-FLOOD Packets number is beyond the set value, the device will start up the blocking function immediately.

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.

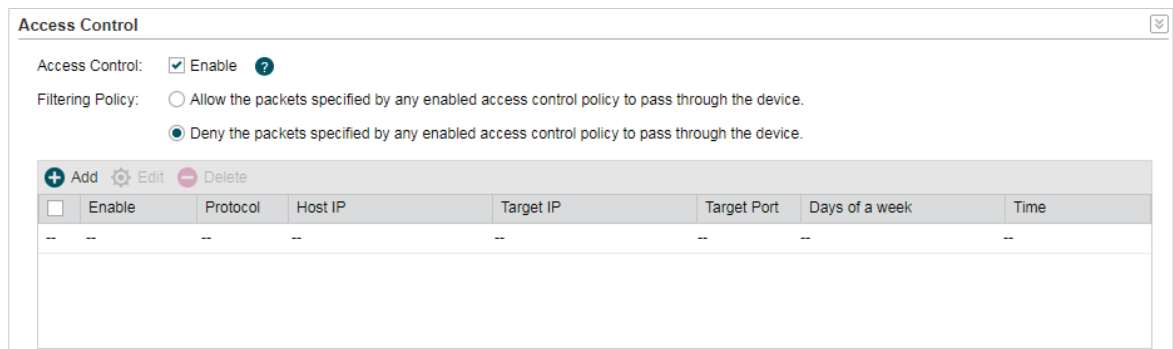
4.6 Configure Access Control

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
☒	TCF				Sun, Mon, Tue, Wed, Th	00:00-24:00
Save Cancel						

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

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

4.7 Configure Static Routing

Note:

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

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

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

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

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

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

4.8 Configure Bandwidth Control

Note:

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

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

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

Bandwidth Control

Total Ingress Bandwidth: Total Egress Bandwidth:

Bandwidth Control: ☒ Enable

☐	Enable	IP Range	Port Range	Protocol	Ingress Min (kbps)	Ingress Max (kbps)	Egress Min (kbps)	Egress Max (kbps)
--	--	--	--	--	--	--	--	--

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	IP Range	Port Range	Protocol	Ingress Min (kbps)	Ingress Max (kbps)	Egress Min (kbps)	Egress Max (kbps)
☒	Enable		1-65535	TCP				

-- -- -- -- -- Save Cancel -- -- --

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. Select the desired entries and click *Edit* to enable it.

The screenshot shows the 'IP & MAC Binding' configuration window. At the top, there's a title bar with a close button. Below it, the 'IP & MAC Binding' section has a checkbox labeled 'Enable' which is checked. Underneath, there are four buttons: 'Add' (with a plus icon), 'Edit' (with a gear icon), 'Delete' (with a minus icon), and 'Import' (with a circular arrow icon). Below these buttons is a table with two columns: 'Enable' and 'IP'. The 'Enable' column has a checkbox that is checked, and the 'IP' column has a text input field. To the right of the 'IP' column is a 'MAC' column with a text input field. At the bottom of the table, there are 'Save' and 'Cancel' buttons. In the bottom right corner of the window, there 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**.

Basic Wireless Settings

Region: United States

Mode: 802.11a/n

Channel Width: 20/40MHz

Max TX Rate: MCS15 - 270/300 Mbps

Channel/Frequency: Auto

Antenna: Feed Only - 7dBi

EIRP Limit: ☒ Enable

Transmit Power: 25 dBm

MAXstream: ☐ Enable

?

?

?

?

?

Spectrum Analysis

?

?

Region	Specify the region where you use the device. Available channels and maximum Transmit Power will be determined by the selected region according to the local laws and regulations.
Mode	Select the protocol standard used in the wireless network. 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. CPE510/CPE610/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 5 MHz, 10 MHz, 20 MHz, 40 MHz and 20/40 MHz (the device automatically selects 40 MHz, and 20 MHz will be used if 40 MHz is not available). According to IEEE 802.11n standard, using a channel width of 40 MHz can increase wireless throughput. However, you may need choose lower bandwidth due to the following reasons: • To increase the available number of channels within the limited total bandwidth. • To avoid interference from overlapping channels occupied by other devices in the environment. • Lower bandwidth can concentrate higher transmit power, increasing stability of wireless links over long distances. • In Client / AP Client Router / Repeater / Bridge Mode, the device should have the same channel width as the root AP. • In Access Point / AP Router / Repeater / Bridge Mode, select the channel width which your clients support.
Max TX Rate	Set the maximum transmit data rate.
Channel/ Frequency	Select appropriate channel used by this device to improve wireless performance. 1/2412 MHz refers to Channel 1 and the frequency is 2412 MHz. This setting is only available in Access Point Mode and AP Router Mode. CPE210/CPE220/WBS210 is a device with a frequency of 2.4GHz and CPE510/CPE610/WBS510 has a frequency of 5GHz. We highly recommend that you use the <i>Spectrum Analysis</i> tool to select a proper channel.
Antenna	Select your antenna from the list.
Antenna Gain	Antenna Gain is only available in WBS products. Enter the antenna gain value according to the antennas and the value ranges from 0 to 30dBi. It can work together with the transmit power to improve the transmit signal quality. Channel/Frequency: Auto ? Spectrum Analysis Antenna Gain: 0 (0-30)dBi
EIRP Limit	This option should remain enabled. With EIRP Limit enabled, the transmit power is restricted so that the EIRP (Effective Isotropic Radiated Power) of the device is kept below the amount which is allowed in the selected region.

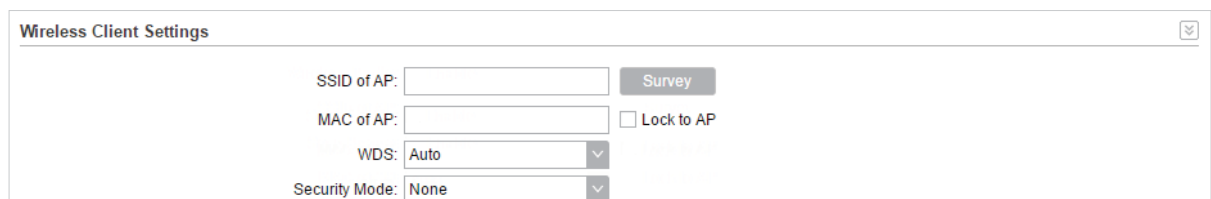
Channel Shifting	Note: Only CPE210(US) 2.0, CPE210(UN/EU/ES) 3.0, CPE220(UN) 3.0 and WBS210(UN) 2.0 support this function. Enable or disable the Channel Shifting function. This function is only available when MAXtream is enabled in Access Point Mode and AP Router Mode. Channel Shifting is a TP-Link proprietary technology. With Channel Shifting enabled, the AP will use non-standard channels by adding a frequency offset to the standard 802.11 b/g/n channels. Your network can then only be detected by the wireless devices with Channel Shifting enabled and so is less likely to be detected by other wireless networks, which benefits network security.
Transmit Power	Specify the transmit power of the device. 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. Note: In most scenarios, it is unnecessary to select the maximum transmit power. Selecting larger transmit power than your need may cause interference to neighborhood. Also it consumes more power and will reduce longevity of the device. Select appropriate transmit power to achieve the best performance. Use the <i>Speed Test</i> tool to find the best performance.
MAXtream	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. Note: MAXtream Technology is only compatible with Pharos series products. Working with products from other manufacturer will cause network fault.
MAXtream Station Mode	MAXtream Station Mode is available in Client Mode, Bridge Mode and AP Client Router Mode with the wireless AP settings disabled. Auto Adjust: The device will choose the MAXtream Station Mode automatically. Latency First: Set the MAXtream Station Mode as Latency First and the time sensitive stream such as VoIP will take precedence in MAXtream system. Throughput First: Set the MAXtream Station Mode as Throughput First and the stream that needs high throughput such as online games will take precedence in MAXtream system.

5.2 Configure Wireless Client Parameters

Note:

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

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

A screenshot of the 'Wireless Client Settings' configuration window. It contains several input fields: 'SSID of AP' with a 'Survey' button next to it, 'MAC of AP' with a 'Lock to AP' checkbox, 'WDS' set to 'Auto', and 'Security Mode' set to 'None'. Each field has a dropdown arrow on its right side.

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

SSID of AP	Specify the SSID of the root AP. You can enter the SSID of the specific AP manually, or directly survey all the APs around by clicking Survey and select one.
MAC of AP	Displays the MAC address of the root AP. It's possible that two or more networks use the same SSID in the AP list. Enable Lock to AP to select SSID and AP simultaneously, which can make the device connect to the specific AP you had connected before the next time.
WDS	Displays the status of the WDS (Wireless distribution System) function. WDS is a communication system among multiple wireless networks . It is established between APs through wireless connection. WDS is used to during the connection between the device and the root AP. Enable: Forward data frames to use four address fields. Disable: Forward data frames to use three address fields. Auto: The device automatically negotiates the wireless data frame structure (three or four address fields) with the root AP. The selection of Auto is recommended.

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

■ None

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

■ WEP

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.

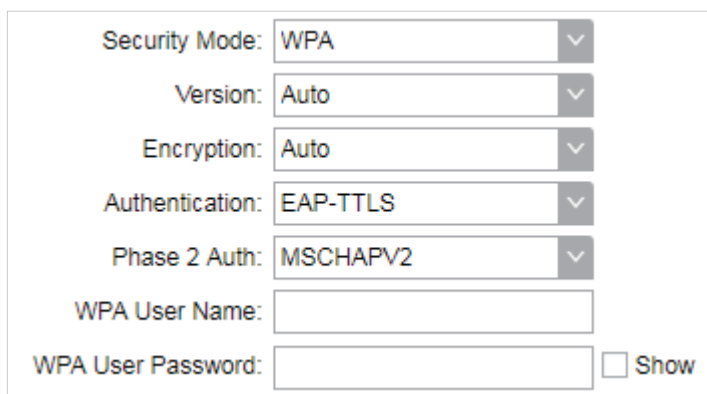
Security Mode:	WEP	▼
Auth Type:	Auto	▼
Key Format:	Hex	▼
Key Selected:	WEP Key:	Key Type:
Key 1: ☒		Disabled ▼
Key 2: ☐		Disabled ▼
Key 3: ☐		Disabled ▼
Key 4: ☐		Disabled ▼

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. 64Bit: Enter 10 hexadecimal digits or 5 ASCII characters. 128Bit: Enter 26 hexadecimal digits or 13 ASCII characters. 152Bit: Enter 32 hexadecimal digits or 16 ASCII characters.
----------	---

■ WPA

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



Security Mode: WPA

Version: Auto

Encryption: Auto

Authentication: EAP-TTLS

Phase 2 Auth: MSCHAPV2

WPA User Name:

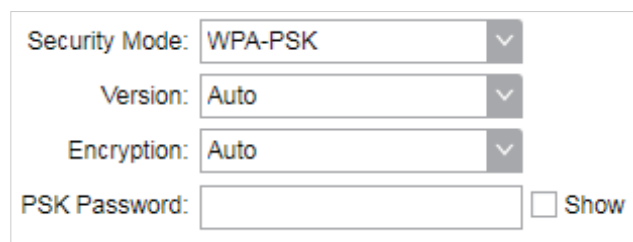
WPA User Password: ☐ Show

Version	Select the version of WPA. Auto: The device will automatically choose the version used by the root AP. WPA/WPA2: They're two versions of WPA security mode. WPA2 is an update of WPA. Compared with WPA, WPA2 introduces AES algorithm and CCMP encryption. Theoretically, WPA2 is securer than WPA.
Encryption	Select the Encryption type. Auto: The default setting is Auto and the device will select TKIP or AES automatically according to the wireless network of root AP. TKIP: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the device may not be able to access the root wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. AES: Advanced Encryption Standard. It is securer than TKIP.
Authentication	Select the type of the authentication.

Phase 2 Auth	Select the type of Phase 2 Auth. The device only supports MSCHAPV2 currently.
WPA User Name	Specify the WPA User Name used in the connection with the root AP.
WPA User Password	Specify the WPA User Password used in the connection with the root AP.

■ WPA-PSK

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



The screenshot shows a configuration window for WPA-PSK. It contains four fields: 'Security Mode' set to 'WPA-PSK', 'Version' set to 'Auto', 'Encryption' set to 'Auto', and 'PSK Password' which is an empty text box followed by a 'Show' checkbox.

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

Wireless AP Settings

Wireless Radio: ☒ Enable

SSID: ☒ Enable SSID Broadcast

Security Mode:

None

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.

Enable SSID Broadcast

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

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

■ **None**

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

RADIUS MAC Authentication: ☒ Enable ?

Authentication Server IP:

Authentication Server Port:

Authentication Server Key: ☐ Show

Accounting Server: ☒ Enable ?

Accounting Server IP:

Accounting Server Port:

Accounting Server Key: ☐ Show

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

■ WEP

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.

Security Mode:	WEP	
Auth Type:	Auto	
Key Format:	Hex	
Key Selected:	WEP Key:	Key Type:
Key 1: ☒		Disabled
Key 2: ☐		Disabled
Key 3: ☐		Disabled
Key 4: ☐		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. Auto: The device can select Open System or Shared Key automatically based on the wireless capability and request of the clients. Open System: Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission. Shared Key: Clients have to input the correct password to pass the authentication, otherwise the clients cannot associate with the wireless network or transmit data.
Key Format	Select ASCII or Hex as the WEP key format. ASCII: With this format selected, the WEP key can be any combination of keyboard characters of the specified length. Hex: With this format selected, the WEP key can be any combination of hexadecimal digits (0-9, a-f, A-F) with the specified length.
Key Selected	Select one key to specify. You can configure four keys at most.
WEP Key	Enter the WEP keys. The length and valid characters are determined by the key format and key type.
Key Type	Select the WEP key length for encryption. 64Bit: Enter 10 hexadecimal digits or 5 ASCII characters. 128Bit: Enter 26 hexadecimal digits or 13 ASCII characters. 152Bit: Enter 32 hexadecimal digits or 16 ASCII characters.

■ WPA

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

Security Mode:	WPA	▼
Version:	Auto	▼
Encryption:	Auto	▼
Authentication Server IP:	0.0.0.0	
Authentication Server Port:	1812	
Authentication Server Key:		☐ Show
Group Key Update Period:	0	seconds. (0 means no update.)
Accounting Server:	☒ Enable	?
Accounting Server IP:	0.0.0.0	
Accounting Server Port:	1813	
Accounting Server Key:		☐ Show

Version	Select the version of WPA. Auto: The device will automatically choose the version used by each client device. WPA/WPA2: They're two versions of WPA security mode. WPA2 is an update of WPA. Compared with WPA, WPA2 introduces AES algorithm and CCMP encryption. Theoretically, WPA2 is securer than WPA.
Encryption	Select the Encryption type. Auto: The default setting is Auto and the device will select TKIP or AES automatically based on the client device's request. TKIP: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the device may not be able to access the root wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. AES: Advanced Encryption Standard. It is securer than TKIP.
Authentication Server IP	Enter the IP address of the Radius Authentication Server.

Authentication Server Port	Enter the UDP port of the RADIUS authentication server. The most commonly used port is 1812, but this may vary depending on the RADIUS authentication server you are using.
Authentication Server Key	Enter the shared key used between this device and the authentication server. The shared key is a case-sensitive text string used to validate communication between this device and the RADIUS authentication server. Check the Show box to view the shared key characters.
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the device should change the encryption key. 0 means that the encryption key does not change at anytime.
Accounting Server	Enable or disable Accounting Server. With this feature enabled, you can keep accounts on users using a RADIUS accounting server.
Accounting Server IP	Enter the IP address of the RADIUS accounting server.
Accounting Server Port	Enter the UDP port of the RADIUS accounting server. The most commonly used port is 1813, but this may vary depending on the RADIUS accounting server you are using.
Accounting Server Key	Enter the password used between this device and the RADIUS accounting server. The shared key is a case-sensitive text string used to validate communication between this device and the RADIUS accounting server. Check the Show box to view the shared key characters.

■ WPA-PSK

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

Security Mode:	WPA-PSK	▼
Version:	Auto	▼
Encryption:	Auto	▼
PSK Password:		☐ Show
Group Key Update Period:	0	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.

Multi-SSID

Multi-SSID: ☒ Enable

+ Add Edit - Delete

☐ Enable	SSID	VLAN	SSID Broadcast	AP Isolation
☐ Enable	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.)

SSID Select the desired SSID to specify the security settings.

Security Mode Specify the security mode for the desired SSID. The device only supports WPA-PSK.

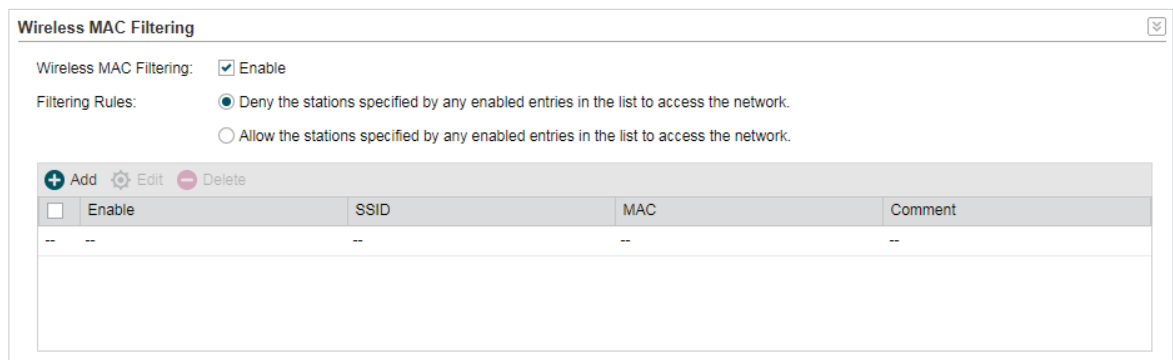
Version	Select the version of WPA-PSK. WPA-PSK/WPA2-PSK: They're two versions of WPA-PSK security mode. WPA2-PSK is an update of WPA-PSK. Compared with WPA, Theoretically, WPA2 is securer than WPA. Auto: The device will automatically choose the version used by the root AP. WPA/WPA2: They're two versions 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.

5.5 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.



The screenshot shows the 'Wireless MAC Filtering' configuration window. At the top, there's a title bar with a close button. Below it, the 'Wireless MAC Filtering' section has a checkbox labeled 'Enable' which is checked. Underneath, there are two radio buttons for 'Filtering Rules': 'Deny the stations specified by any enabled entries in the list to access the network.' (selected) and 'Allow the stations specified by any enabled entries in the list to access the network.' Below the radio buttons is a table with columns: 'Enable', 'SSID', 'MAC', and 'Comment'. The table has a header row and one data row with dashes. Above the table are buttons for '+ Add', 'Edit', and '- Delete'.

Wireless MAC Filtering

Enable or disable the Wireless MAC Filtering function.

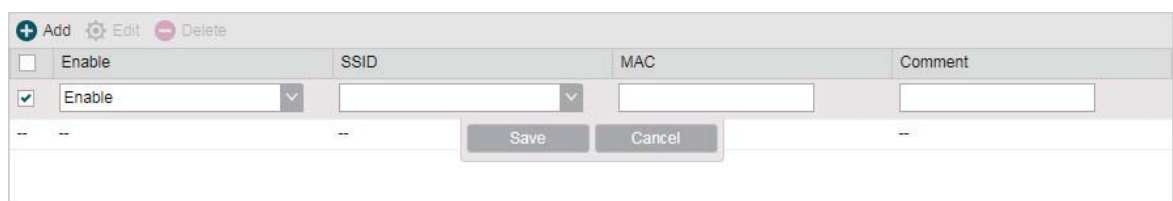
Filtering Rules

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.



The screenshot shows the 'Wireless MAC Filtering' configuration window with the 'Add' button clicked. The 'Enable' checkbox is checked. The 'SSID' dropdown menu is open, showing a list of SSIDs. The 'MAC' and 'Comment' fields are empty. The 'Save' and 'Cancel' buttons are visible at the bottom.

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 DTIM 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.

Long Range PtP

Note: Only WBS510, WBS210 and CPE610 support this feature.

Long Range PtP is only available when MAXstream function is enabled. With this function enabled, it is allowed to specify a larger distance which can be helpful in the following situations:

- The AP is connected to a single client or AP.
- The distance between the two devices exceeds the distance allowed by the AP's hardware specifications.

The distance is used to calculate the Acknowledge timeout (ACK timeout). Long Range PtP allows the AP to get a larger ACK timeout and reduce unnecessary retransmission in the situations above.

Beacon Interval	Specify the beacon interval for the device. Beacons are transmitted periodically by the device to announce the presence of a wireless network for the clients. Beacon Interval value determines the time interval of the beacons sent by the device. Specify a value from 40 to 1,000. The default value is 100.
RTS Threshold	Specify the RTS threshold for the device. RTS/CTS (Request to Send/Clear to Send) is used to improve the data transmission efficiency of the network with hidden nodes, especially when there are lots of large packets to be transmitted. When the size of a data packet is larger than the RTS Threshold, the RTS/CTS mechanism will be activated. With this mechanism activated, before sending a data packet, the client will send an RTS packet to the device to request data transmitting. And then the device will send CTS packet to inform other clients to delay their data transmitting. In this way, packet collisions can be avoided. For a busy network with hidden nodes, a low threshold value will help reduce interference and packet collisions. But for a not-so-busy network, a too low threshold value will cause bandwidth wasting and reduce the data throughput. The recommended and default value is 2346 bytes.
Fragmentation Threshold	Specify the fragmentation threshold for packets. The fragmentation function can limit the size of packets transmitted over the network. If the size of a packet exceeds the Fragmentation Threshold, the fragmentation function is activated and the packet will be fragmented into several packets. Fragmentation helps improve network performance if properly configured. However, a too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.
DTIM Interval	Specify the DTIM (Delivery Traffic Indication Message) Interval for the device. The DTIM is contained in some Beacon frames. It indicates whether the device has buffered data for client devices. The DTIM Period indicates how often the clients served by this device should check for buffered data still on the device awaiting pickup. Specify the value between 1-255 Beacon Intervals. The default value is 1, indicating that clients check for buffered data at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend you keep the default value.

AP Isolation	Enable or disable AP Isolation. With this feature enabled, the clients can not communicate with each other directly. Note: AP Isolation is not available in Client Mode.
Short GI	Enable or disable Short GI. Propagation delays often occurs in data transmission process and influence the capability of the wireless network. It can result from multiple factors, such as multipath effect. GI (Guard Interval) is intended to solve the problem based on delays, and Short GI is used to improve the throughput of the wireless network based on the GI in the environment with small delays. When the delays are small. When Short GI is enabled, the guard interval will be set as 400ns and this function will boost the performance about 11%. In the with serious multipath time delay. Short GI function will reduce the throughput instead of improving it.
Wi-Fi Multimedia (WMM)	Enable or disable WMM. With WMM enabled, the system will prioritize traffic according to the data type when forwarding data. Time-dependent traffic, such as video or audio packets, gets a higher priority than normal traffic. We recommend you enable this function when you are running the video or audio application.
QoS	Enable or disable QoS. The QoS function improves the transmission performance of video or audio traffic by optimizing the scheduling policy between the AP and the clients.

6

Manage the Device

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

6.1 Manage System Logs

6.2 Specify the Miscellaneous Parameters

6.3 Configure Ping Watch Dog

6.4 Configure Dynamic DNS

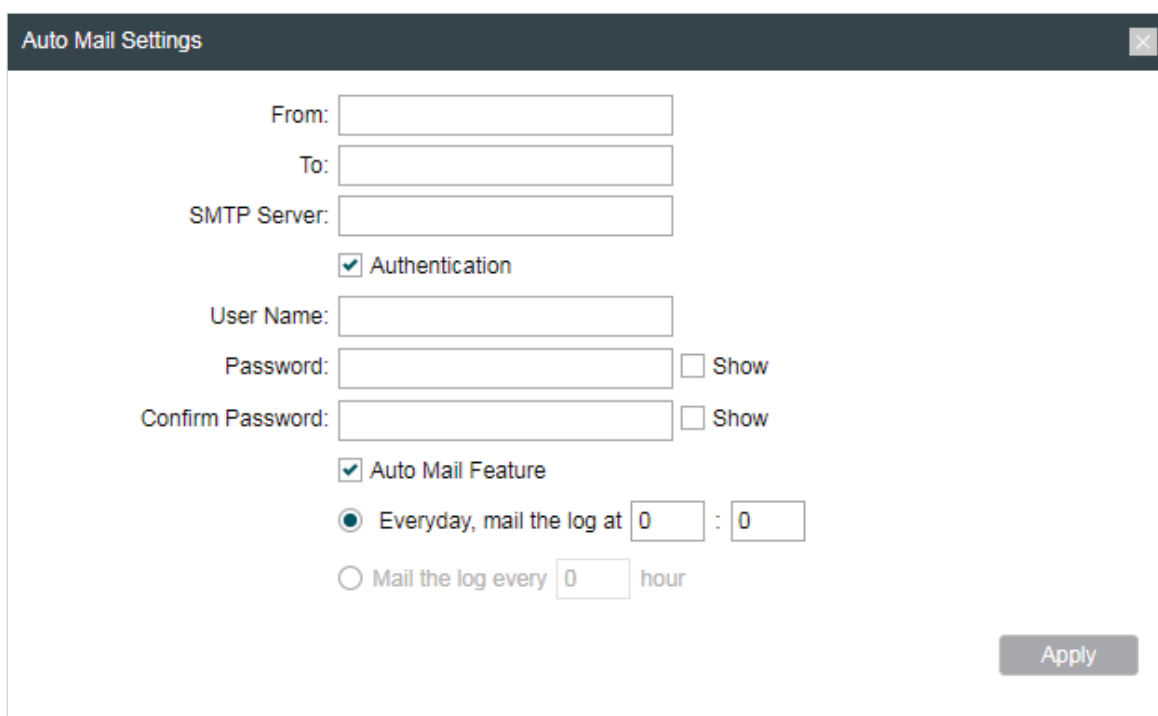
6.5 Configure Web Server

6.6 Configure SNMP Agent

6.7 Configure SSH Server

6.8 Configure RSSI LED Thresholds

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

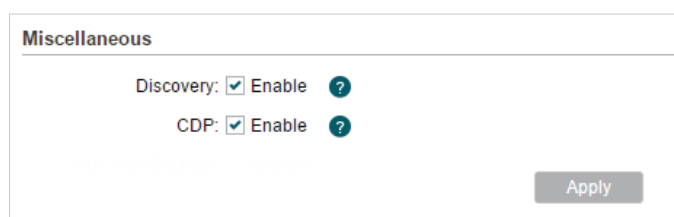


From	Enter the sender's E-mail address.
To	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address of the sender's SMTP server.
Authentication	Enable or disable the authentication function. If the sender's mailbox is configured, check the box to enable mail server authentication. Enter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

6.2 Specify the Miscellaneous Parameters

This section is used to specify miscellaneous parameters.

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



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

2. Click Save.

6.3 Configure Ping Watch Dog

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

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

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

Ping Watch Dog

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. Register an account to DDNS service provider (NO-IP, Dyndns or Comexe) first.

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

Dynamic DNS

Service Provider: Dyn dns (www.dyndns.com) ▼

Dynamic DNS: ☒ Enable

User Name:

Password: ☐ Show

Domain Name:

Connection Status: Not launching.

Login

Logout

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:

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

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

6.6 Configure SNMP Agent

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

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

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

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

SNMP Agent

SNMP Agent: ☒ Enable

SysContact:

SysName:

SysLocation:

Get Community:

Get Source:

Set Community:

Set Source:

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

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

Note:

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

6.7 Configure SSH Server

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

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

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

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

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, configure the device name and the system language.

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

Device

Device Name:

CPE210

Language:

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, configure the location for the device.

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

Location

Longitude:

0

Latitude:

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, 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:

Get GMT

Synchronize with PC's Clock

Daylight Saving Time:

Setting

Apply

■ 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: minutes

Start Time: Last in March at 01 : 00

End Time: Last in October at 01 : 00

☐ Date Mode

Time Offset: 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.

■ Date 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*.

Firmware Update	
Firmware Version: 2.1.6 Build 20170908 Rel. 45233 (0000)	
Upload Firmware:	Browse Upload

Firmware Version	Displays the current firmware version of the device.
------------------	--

Note:

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

7.6 Configure Other Settings

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

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

Configuration

Backup Configuration:

Backup

Upload Configuration:

Browse

Upload

Reset to Factory Defaults:

Reset

Reboot Device:

Reboot

Backup Configuration	Click <i>Backup</i> to back up the current configuration to your PC.
Upload Configuration	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.
Reset to Factory Defaults	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.
Reboot Device	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

8.6 Antenna Alignment

8.1 Configure Ping

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

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

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 arranged in two rows. The first row has 'Destination IP/Domain:' followed by an empty text box, and 'Packet Count:' followed by a text box containing '4' and a range '(1-50)' to its right. The second row has 'Ping Timeout:' followed by a text box containing '800' and a range '(100-2000) milliseconds' to its right, and 'Packet Size:' followed by a text box containing '64' and a range '(4-1472) bytes' to its right. Below these fields is a section titled 'Ping Results'. Inside this section, there's a checkbox labeled 'Enable' which is currently checked. Below the checkbox is a large, empty rectangular area for displaying results. At the bottom right of the window, there is a 'Start' button.

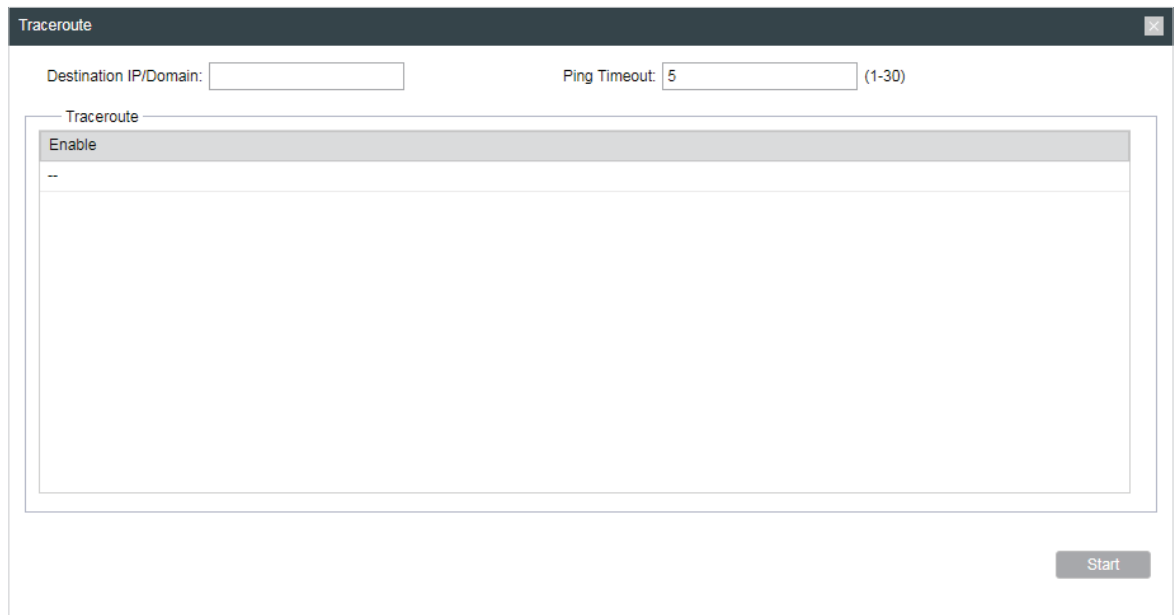
Destination IP/ Domain	Enter the IP address of the destination node for Ping test. The device will send Ping packets to test the network connectivity and reachability of the host and the results will be displayed in the Ping Result.
Packet Count	Enter the number of packets to be sent during the testing. 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, troubleshoot with traceroute utility.

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



Traceroute

Destination IP/Domain: Ping Timeout: (1-30)

Traceroute

Enable

--

Start

**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**

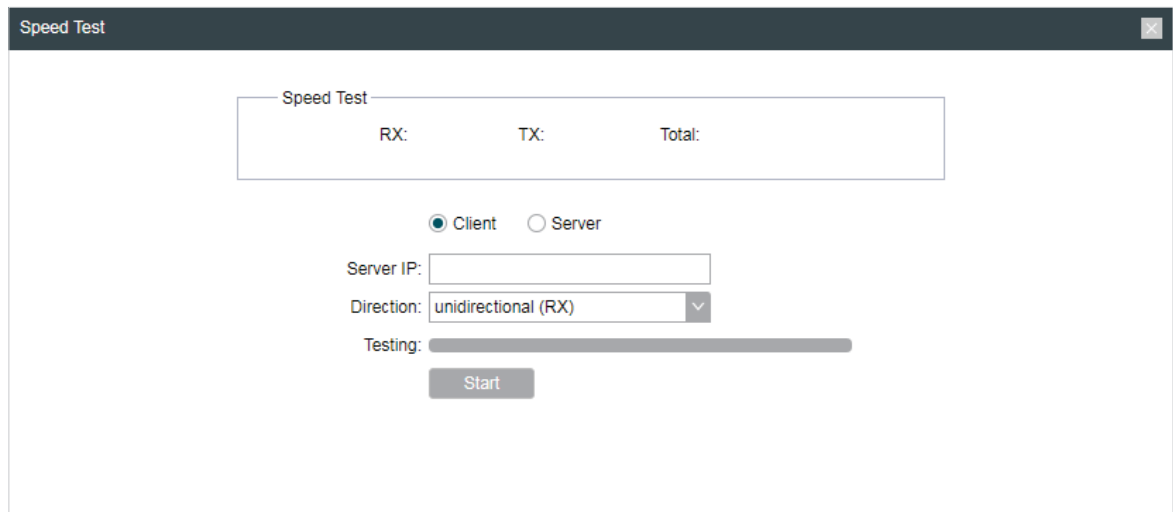
Specify the traceroute max TTL (Time To Live) during the traceroute process. It is the maximum number of the route hops the test packets can pass through.

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.



The screenshot shows a window titled "Speed Test" with a close button in the top right corner. Inside the window, there is a section titled "Speed Test" containing three labels: "RX:", "TX:", and "Total:". Below this, there are two radio buttons: "Client" (which is selected) and "Server". Under the radio buttons, there is a text input field for "Server IP:". Below that is a dropdown menu for "Direction:" currently showing "unidirectional (RX)". At the bottom, there is a progress bar labeled "Testing:" and a "Start" button.

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

2. Click *Start*.

8.4 Survey

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

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

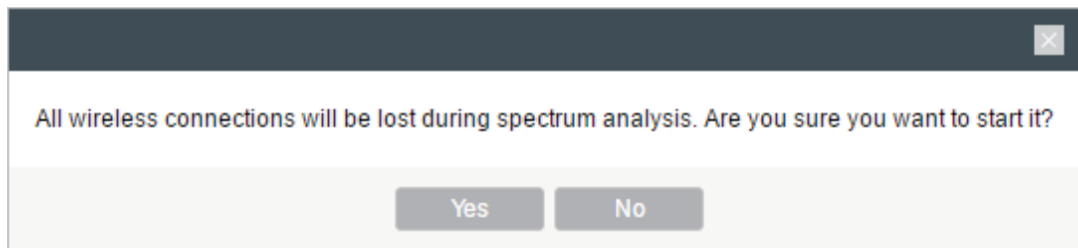
Survey									
Index	BSSID	SSID	MAXtream	Device Name	SNR(dB)	Signal / Noise(dBm)	Channel	Security	
1	50-C7-BF-04-BF-26	TP-LINK_BF28_5G	No		38	-63/-101	5805 (161)	WPA2-PSK	▲
2	60-E3-27-D0-E2-2A	jjjj5	No		34	-61/-95	5220 (44)	WPA2-PSK	
3	50-C7-BF-08-5D-86	TP-LINK_Cui5	No		38	-57/-95	5220 (44)	WPA2-PSK	
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	jjjj5re	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

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

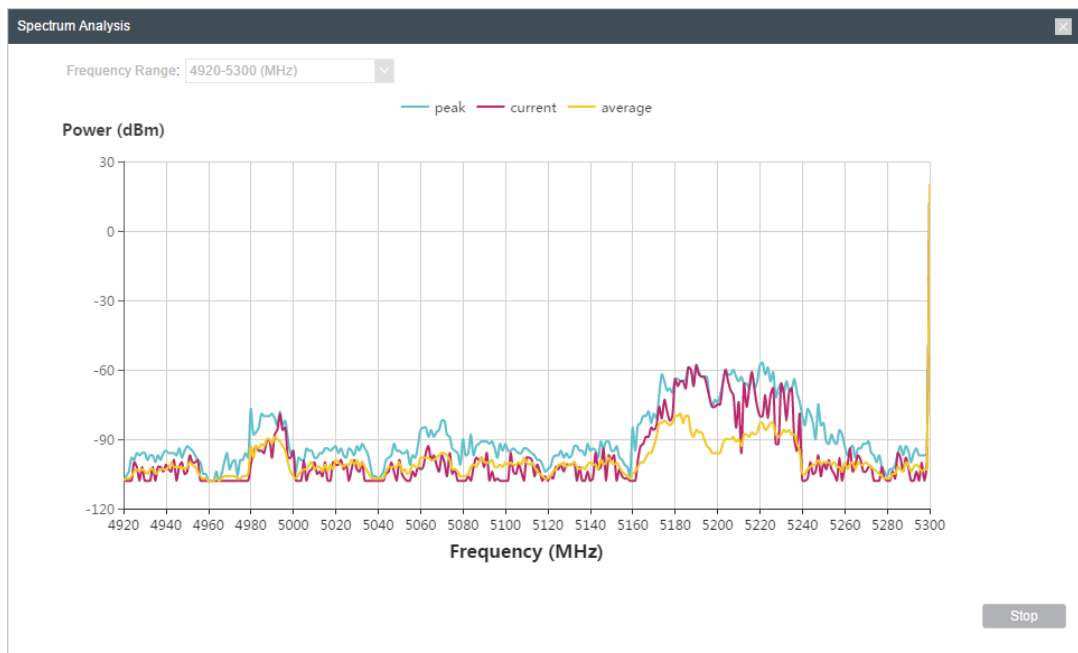
8.5 Analyze Spectrum

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

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



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



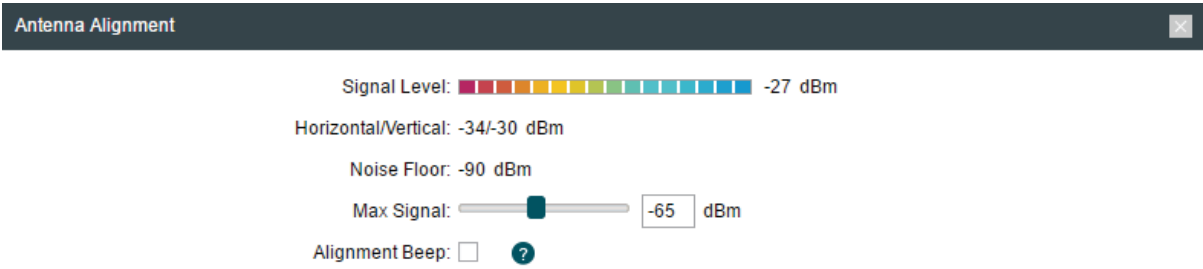
Note:

- Only CPE510/CPE610/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.

8.6 Antenna Alignment

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



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

FCC compliance information statement

Product Name: Outdoor CPE

Model Number: CPE210/CPE220/CPE510/CPE610/CPE710

Component Name	Model
PoE Adapter	TL-POE2412G (For CPE210, CPE220, CPE510, CPE610) T240050-2-POE (For CPE710)

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: <https://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

For CPE220/CPE510/CPE610/CPE710:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For CPE210:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

Product Name: Outdoor Wireless Base Station

Model Number: WBS210/WBS510

Component Name	Model
PoE Adapter	T240100-2-PoE

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: <https://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

Product Name: PoE Adapter

Model Number: TL-POE2412G/T240050-2-POE/T240100-2-PoE

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: <https://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1) This device may not cause harmful interference.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

We, TP-Link USA Corporation, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2020/02/17

CE Mark Warning



For CPE220/CPE510/CPE610/CPE710/WBS210/WBS510:

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

For CPE210:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

operation temperature: -40°C ~ 70°C

OPERATING FREQUENCY (the maximum transmitted power)

For CPE210/CPE220/WBS210:

2412 MHz—2472 MHz (20 dBm)

For CPE510/CPE610/CPE710/WBS510:

5500 MHz—5700 MHz (30 dBm)

EU declaration of conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/53/EU, 2009/125/EC, 2011/65/EU and (EU)2015/863.

The original EU declaration of conformity may be found at <https://www.tp-link.com/en/ce>

RF Exposure Information

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm from your body.

Canadian Compliance Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

- 1) This device may not cause interference.
- 2) This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- 1) L'appareil ne doit pas produire de brouillage;

- 2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

For WBS210/WBS510:

This radio transmitter (IC: 8853A-WBS210/ Model: WBS210)/(IC: 8853A-WBS510/ Model: WBS510) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list below, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (IC: 8853A-WBS210/ Model: WBS210)/(IC: 8853A-WBS510/ Model: WBS510) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste ci-dessous et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Model	WBS210 (8853A-WBS210)	WBS510 (8853A-WBS510)
Antenna	2 dBi omni (50 ohm) 15 dBi sector (50 ohm)	3 dBi omni (50 ohm) 19 dBi sector (50 ohm)

Caution:

For CPE510/CPE610/CPE710:

- 1) The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

For WBS510:

- 1) The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- 2) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;
- 3) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and

DFS (Dynamic Frequency Selection) products that operate in the bands 5250- 5350 MHz, 5470-5600 MHz, and 5650-5725 MHz.

Avertissement:

For CPE510/CPE610/CPE710:

- 1) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

For WBS510:

- 1) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- 2) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant les bandes 5250-5350 MHz et 5470-5725 MHz doit se conformer à la limitation P.I.R.E.;
- 3) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

Les produits utilisant la technique d'atténuation DFS (sélection dynamique des fréquences) sur les bandes 5250- 5350 MHz, 5470-5600 MHz et 5650-5725 MHz.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

For CPE220/CPE510/CPE610/CPE710/WBS210/WBS510:

CAN ICES-3 (A)/NMB-3(A)

For CPE210:

CAN ICES-3 (B)/NMB-3(B)



Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.



Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

NCC Notice & BSMI Notice

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

For CPE510/CPE610/CPE710/WBS510:

4.7.9.1應避免影響附近雷達系統之操作。

4.7.9.2高增益指向性天線只得應用於固定式點對點系統。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

For CPE220/CPE510/CPE610/CPE710/WBS210/WBS510

此為甲類資訊技術設備，于居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

限用物質含有情況標示聲明書

產品元件名稱	限用物質及其化學符號					
	鉛 Pb	鎘 Cd	汞 Hg	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	—	○	○	○	○	○
備考1. "超出0.1 wt %" 及 "超出0.01 wt %" 系指限用物質之百分比含量超出百分比含量基準值。 備考2. "○"系指該項限用物質之百分比含量未超出百分比含量基準值。 備考3. "—" 系指該項限用物質為排除項目。						



Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

For CPE220/CPE510/CPE610/CPE710/WBS210/WBS510:

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Explanation of the symbols on the product label

Symbol	Explanation
	DC voltage
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.

COPYRIGHT & TRADEMARKS

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

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