tp-link

PHAROS

For TP-Link Pharos Series Products

User Guide

1910012245 REV3.0.0

August 2017

CONTENTS

About This Guide **1**

Chapter 1 Overview **2**

Introduction 2

System Requirements 2

Getting Started 2

Navigation 4

Chapter 2 Operation Modes **6**

Access Point 6

Client 7

Repeater (Range Extender) 8

Bridge 8

AP Router 9

AP Client Router (WISP Client) 9

Chapter 3 Quick Setup Guide **11**

Access Point 11

Client 13

Repeater (Range Extender) 16

Bridge 19

AP Router 23

AP Client Router (WISP Client) 27

Chapter 4 Status Tab **33**

Status Information 34

Monitor 38

Chapter 5 Network Tab **43**

WAN 44

LAN 50

Management VLAN 54

Forwarding 54

Security 59

Access Control 62
Static Routing 63
Bandwidth Control 64
IP&MAC Binding 65
Chapter 6 Wireless Tab 67
Wireless Basic Settings 68
Wireless Client Settings 70
Wireless AP Settings 71
Multi-SSID 77
Wireless MAC Filtering 78
Wireless Advanced Settings 79
Chapter 7 Management Tab 82
System Log 83
Miscellaneous 84
Ping Watch Dog 85
Dynamic DNS 86
Web Server 87
SNMP Agent 88
SSH Server 90
RSSI LED Thresholds 90
Chapter 8 System Tab 92
Device 93
Location 93
User Account 93
Time Setting 94
Firmware Update 96
Configuration 97
Chapter 9 Tools List 99
Ping 99
Traceroute 100
Speed Test 100

Survey 102
Spectrum Analysis 103
Appendix A: Pharos MAXtream TDMA 104
Appendix B: Glossary 105

About This Guide

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

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

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

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

More Info

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

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

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

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

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

Chapter 1 Overview

Introduction

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

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

New features of Pharos series products are listed as follows:

- Provides User-friendly UI design.
- TP-Link Pharos MAXtream (Time-Division-Multiple-Access) technology improves product performance in throughput, capacity and latency, which are ideal for Point-to-multipoint applications.
- Supports multiple operation modes: Access Point, Client, Repeater (Range Extender), Bridge, AP Router and AP Client Router (WISP Client).
- Provides system-level optimization for long-distance wireless transmission.
- Supports selectable bandwidth of 5/10/20/40MHz.
- Supports easy antenna alignment with Wireless Signal Indicators on Web interface.
- Provides Throughput Monitor, Spectrum Analyzer, Speed Test and Ping tools.
- Supports discovery and management via Pharos Control application.

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.

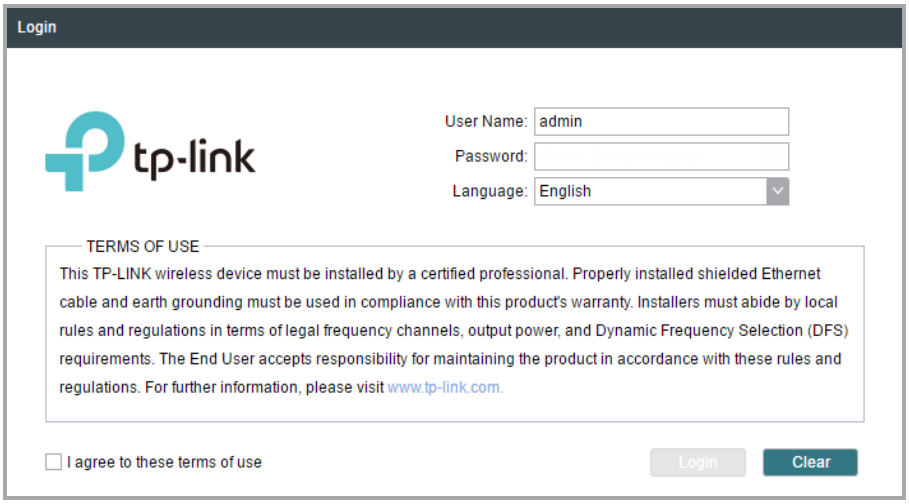
Getting Started

To access the PharOS Configuration Interface, perform the following steps:

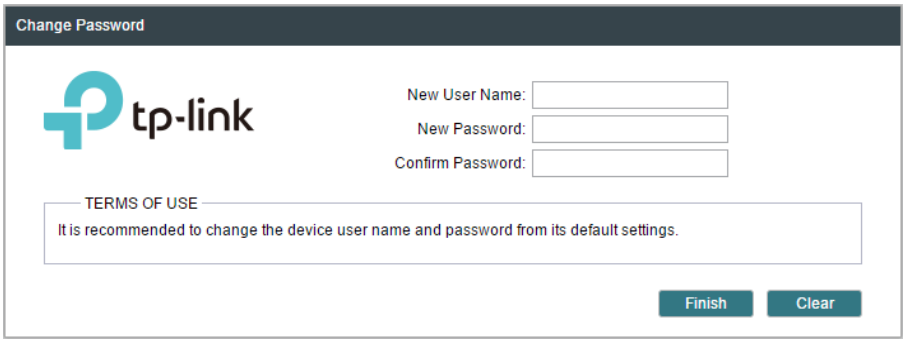
1. Configure the Ethernet adapter on your computer with a static IP address on the 192.168.0.x subnet (for example, IP address: 192.168.0.100 and subnet mask: 255.255.255.0).
2. Launch your Web browser. Enter the default IP address of your device in the address field. Press **Enter** (PC) or **Return** (Mac).

For Example, enter 192.168.0.254 to access the PharOS.

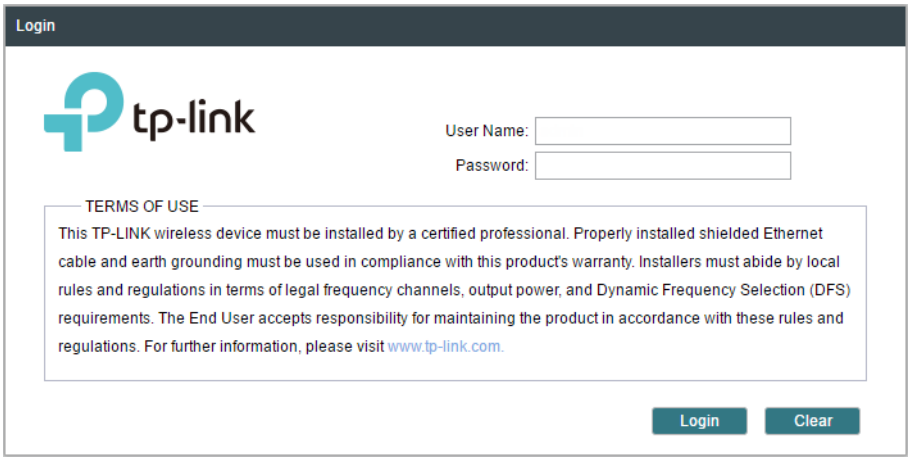
3. Upon initial login, enter **admin** in the ***Username*** and ***Password*** fields, and select the appropriate language from the ***Language*** drop-down lists. Check the box next to ***I agree to these terms of use***, and click **Login**.



4. We recommend you change the device's user name and password from its default settings for network security. Enter and confirm new user name and password, then click **Finish**.

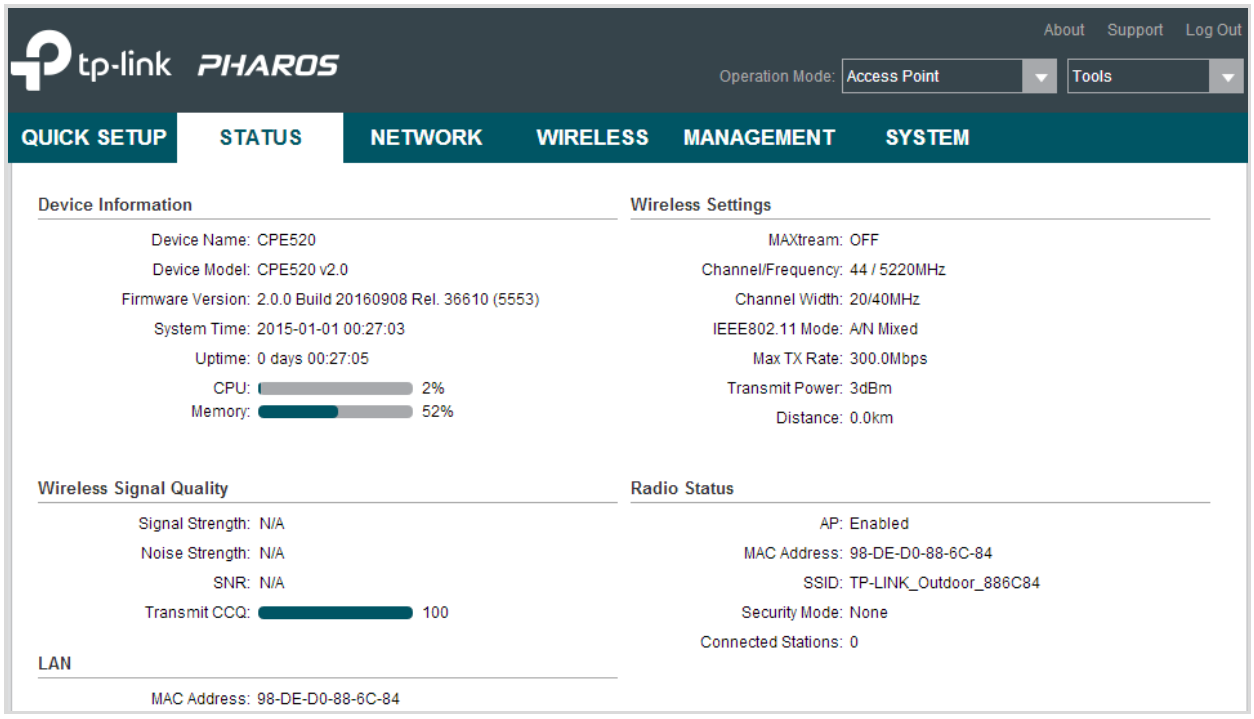


5. For subsequent logins, you only need to enter the user name and password that you have set to log in.



Navigation

The PharOS Web Interface contains six main tabs, each of which provides a Web-based management page to configure the specific parameters of the Pharos series products.



- **Quick Setup**

On **Quick Setup Guide**, you can quickly configure your device through the step-by-step Quick Setup Wizard.

- **Status**

The **Status Tab** displays a summary of the link status information, current values of the basic configuration settings (depending on the operating mode), network settings and information, and traffic statistics.

- **Network**

The **Network Tab** configures the function of WAN, LAN, Management VLAN, forwarding, security, access control, static routing, bandwidth control and IP&MAC binding.

- **Wireless**

On The **Wireless Tab**, you can configure the related wireless parameters in different modes.

- **Management**

The **Management Tab** configures system management services: System Log, Miscellaneous, Ping Watch Dog, and Dynamic Domain Name System (DDNS). Web server, Simple Network Management Protocol (SNMP), SSH server, RSSI LED Thresholds are also available.

- **System**

The **System Tab** controls system maintenance routines, device customization, location management, user account management, firmware update, Time setting and configuration backup.

- **Tools**

The **Tools list** provides some useful tools including Ping, Traceroute, Speed Test, Survey and Spectrum Analysis.

Chapter 2 Operation Modes

The Pharos series products support six modes to satisfy user's diversified network requirements including Access Point mode, Client mode, Repeater (Range Extender) mode, Bridge mode, AP Router mode and AP Client Router (WISP Client) mode. This chapter introduces typical usage scenarios of each mode. You can choose the desired scenario according to your needs, and refer to the Installation Guide for hardware connection instruction and **Chapter 3 Quick Setup Guide** for software configuration.

Access Point

In AP mode, the device acts as a central hub and provides wireless access point for wireless clients, thus the AP mode is very 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.

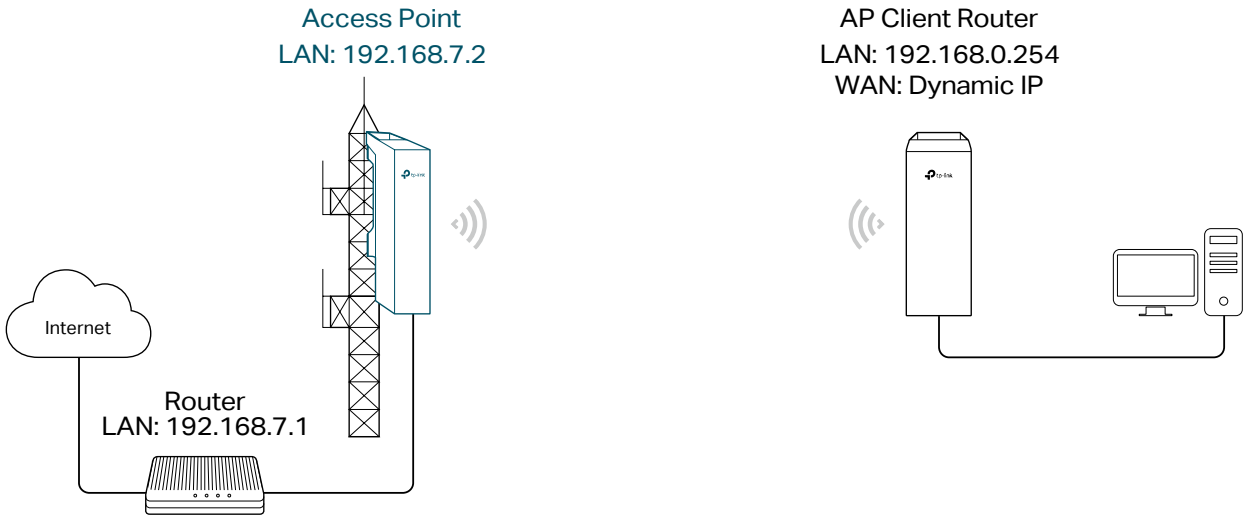
- **Scenario 1**

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 with the access to ISP network by connecting to ISP's router to transform wired signal into wireless one. The remote users can put up a device in AP Client Router mode to access the Internet the AP device provides wirelessly.

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

Network diagram:



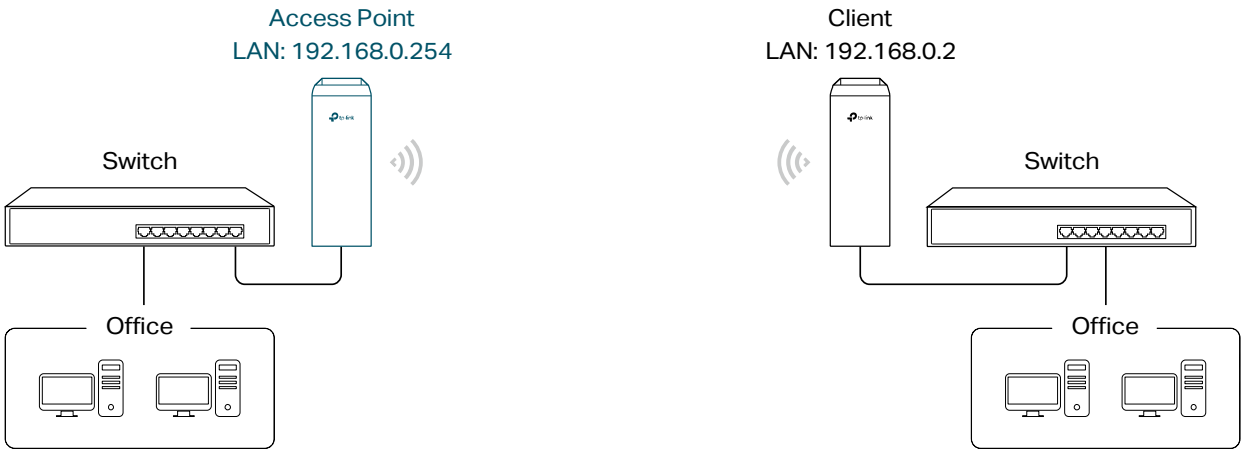
- **Scenario 2**

Network requirements: Combine two separate office networks as one.

The device in the network: Two devices in AP and Client mode respectively connect to the switches in two office networks so as to connect two office networks.

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

Network diagram:



- **Scenario 3**

Network requirements: Establish wireless network coverage in the campus, community, industrial park or public places to provide wireless access points for wireless 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 point based on the existing wired network for wireless clients, such as smart phones, laptops and tablets.

Advantages: Increase wireless access points and enrich the access ways of local area network.

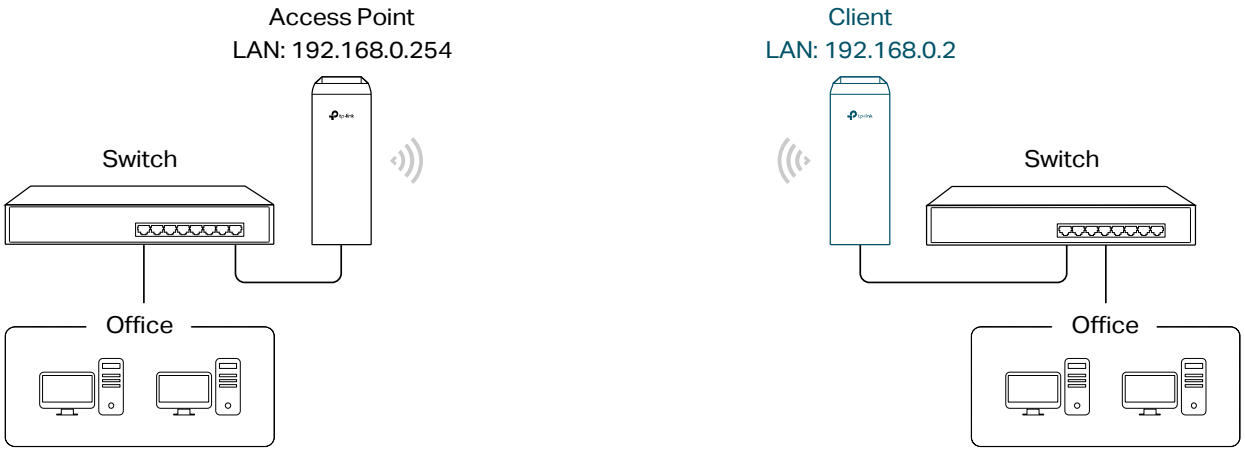
Network diagram:

Client

Network requirements: The most common usage scenario of Client is point-to-point networking with AP for combining two separate office networks. Please refer to **Scenario 2 of Access Point** for detailed information.

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

Network diagram:



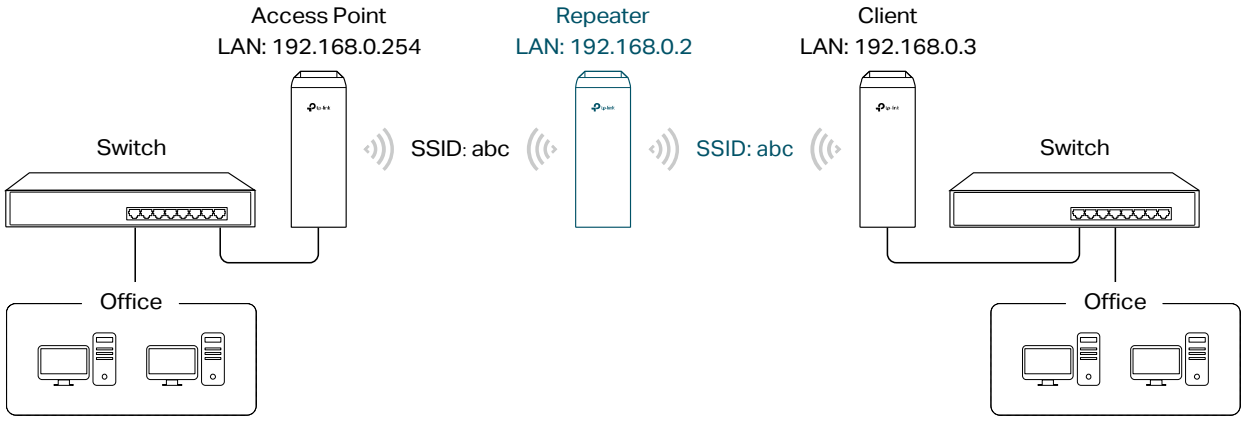
Repeater (Range Extender)

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

Network requirements: Repeat wireless signal.

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

Network diagram:

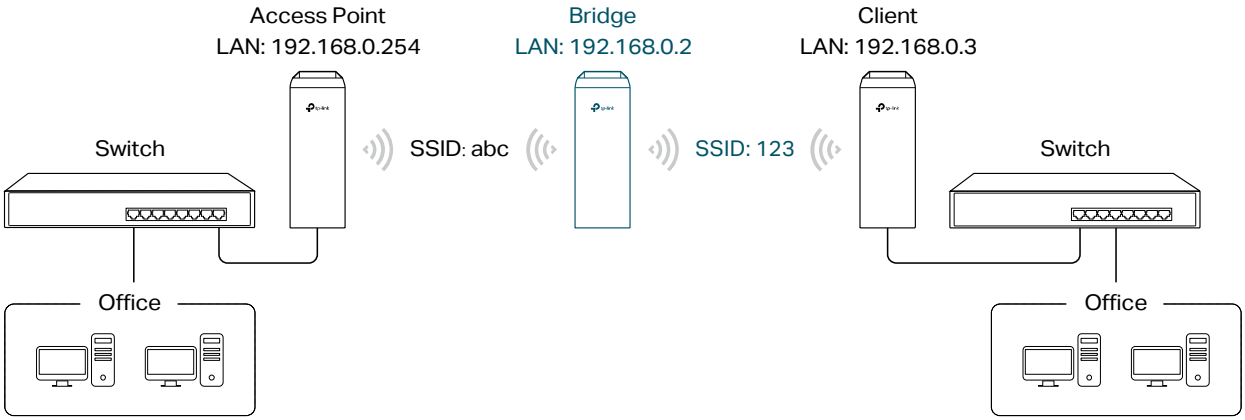


Bridge

Network requirements: Reinforce the wireless signal strength of the root AP device to eliminate the wireless signal-blind areas. Meanwhile, the wireless users can use the SSID and encryption type different from those of the root AP device to access the network.

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

Network diagram:



AP Router

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: Similar to the home wireless router, the device in AP Router mode connects to root ADSL/Cable Modem. The difference lies in that the coverage area of this device is wider. Smart phones, laptops, and other wireless clients can share wide area network via the access to wireless network this device provides.

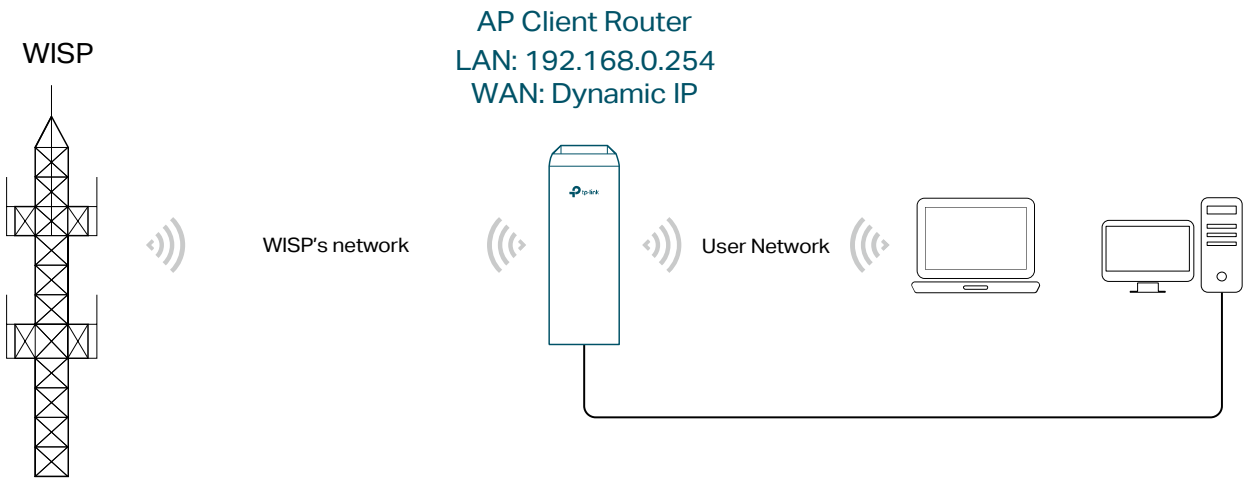
Network diagram:

NOTE:

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

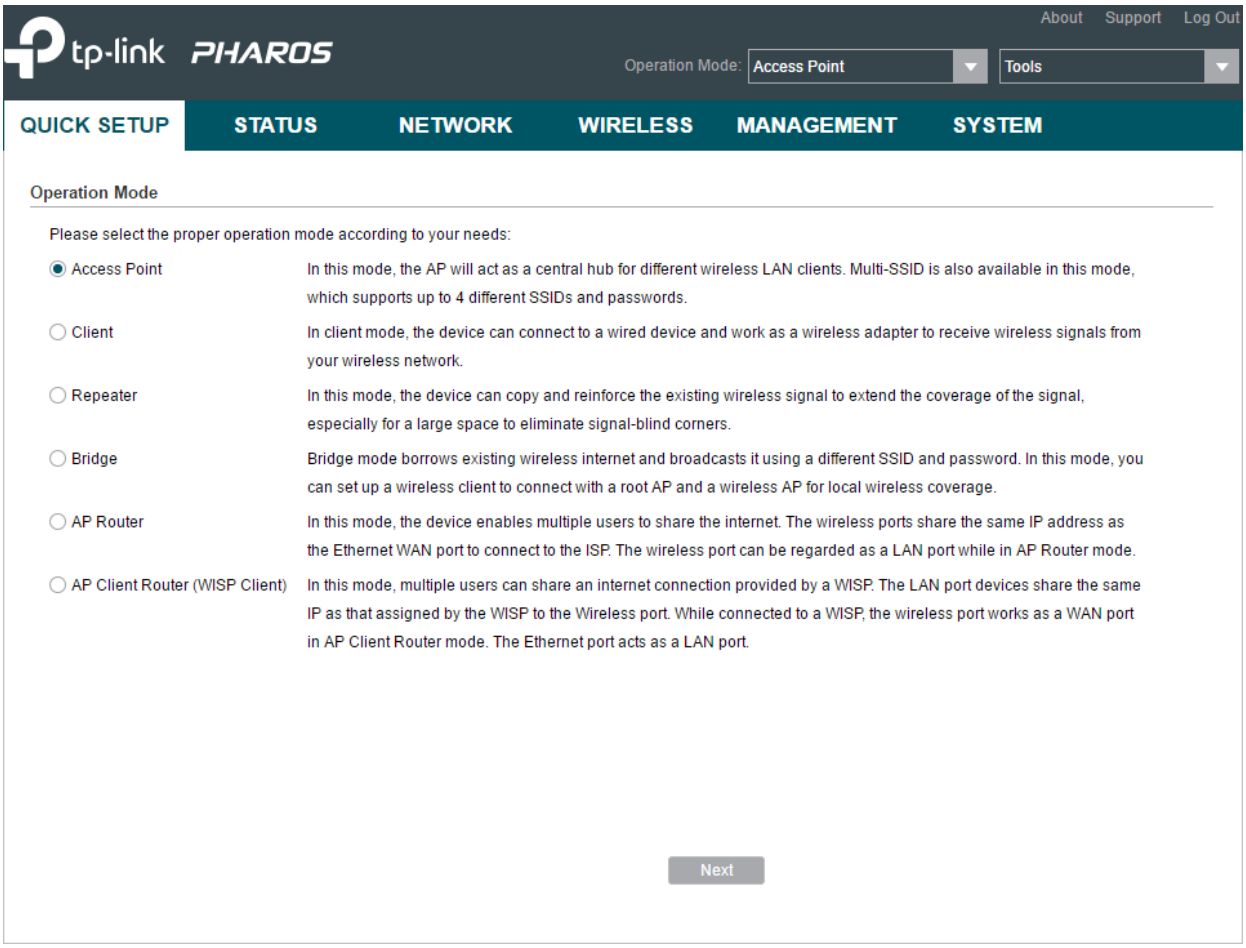
AP Client Router (WISP Client)

In AP Client Router mode, after accessing the wireless network provided by WISP, the device provides wireless network service for downstream wireless clients. Meanwhile, the device allows wired devices, such as desktop computer, to access it via LAN1 port or PoE adapter's LAN port. In this way, all members of a home user can share the Internet using one account applied from WISP.


AP Client Router
LAN: 192.168.0.254
WAN: Dynamic IP
WISP
WISP's network
User Network

Chapter 3 Quick Setup Guide

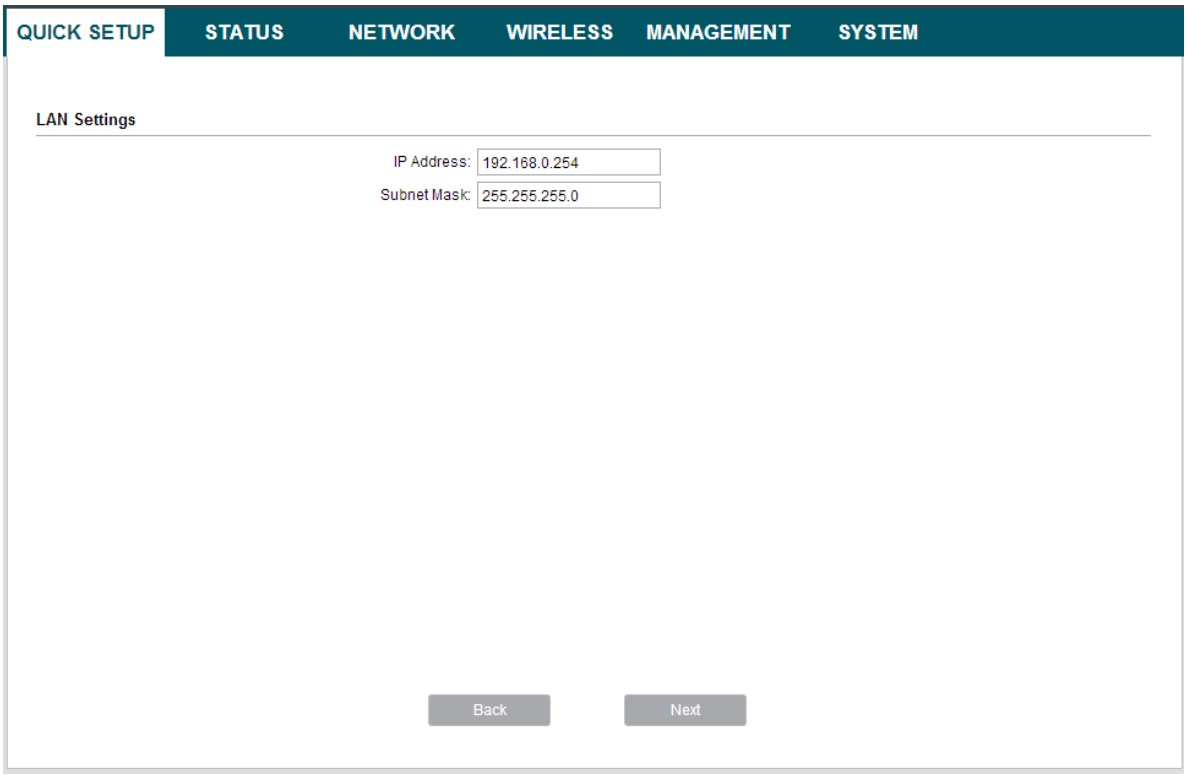
Quick Setup wizard allows you to quickly configure your device step by step. Choose the suitable operation mode according to your network environment and follow the step-by-step instructions.



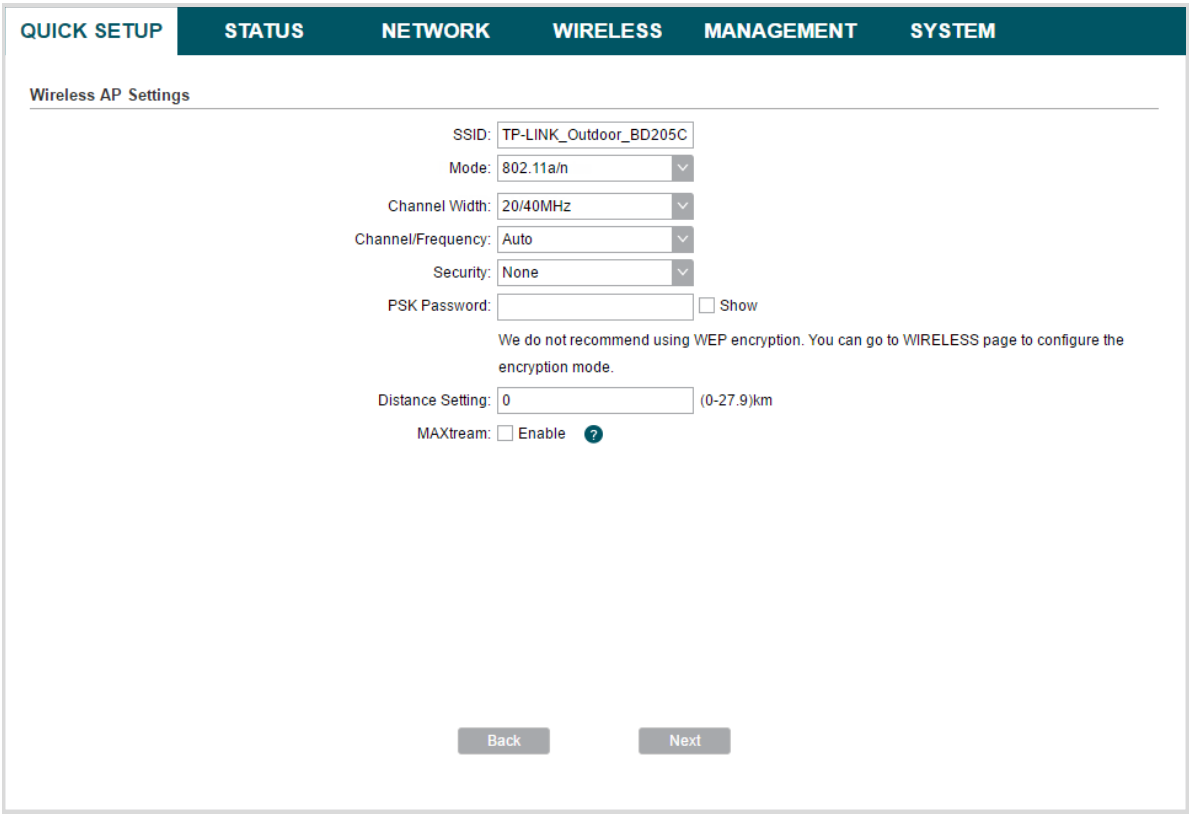
Access Point

If **Access Point** is selected, click **Next** and take the following steps:

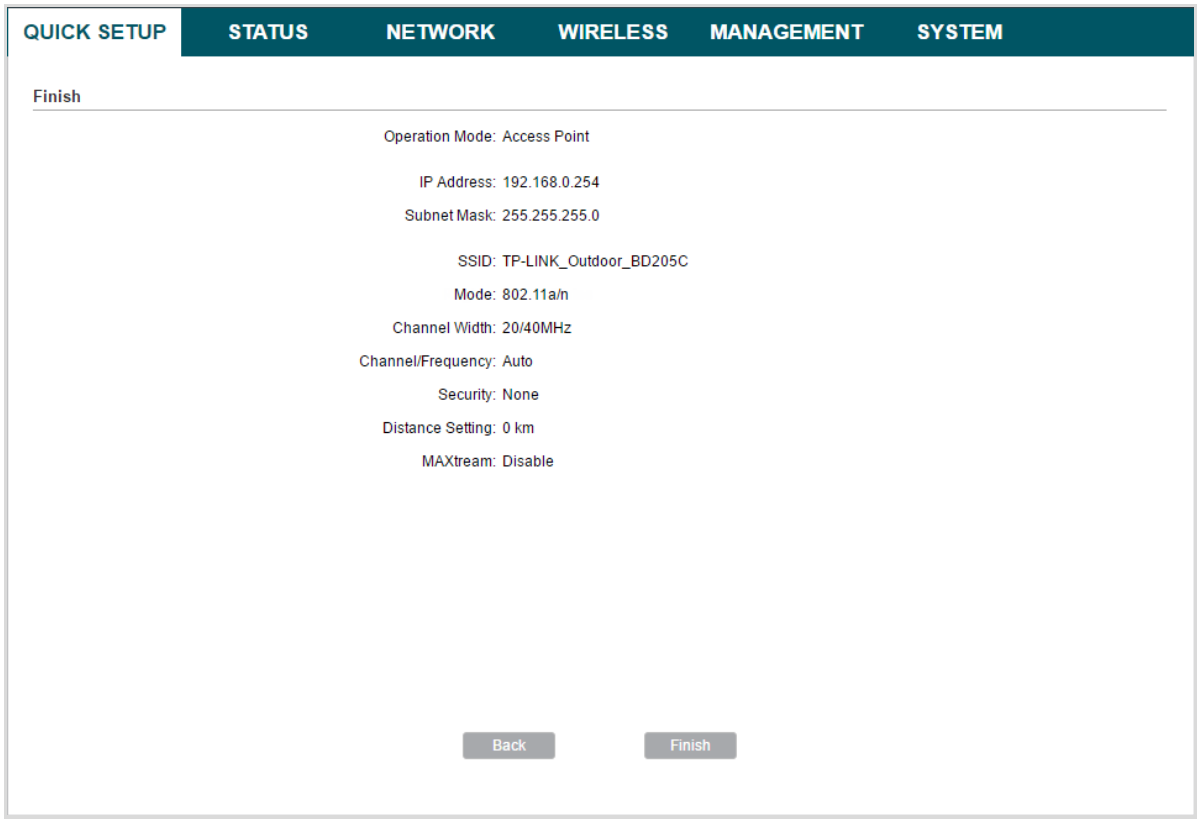
1. The **LAN Settings** page will appear as shown below. The default ***IP Address*** is 192.168.0.254 and the default ***Subnet Mask*** is 255.255.255.0. You can change the IP Address and Subnet Mask on this page when there is an IP conflict with other devices. Click **Next**.



2. The **Wireless AP Settings** page will appear as shown below. Create an easy-to-remember name for your wireless network. We recommend to select **WPA-PSK/WPA2-PSK** in the ***Security*** box and enter the PSK Password below to prevent unauthorized access to your AP. Enter the distance between this device and the furthest client in ***Distance Setting***. Then click **Next**.



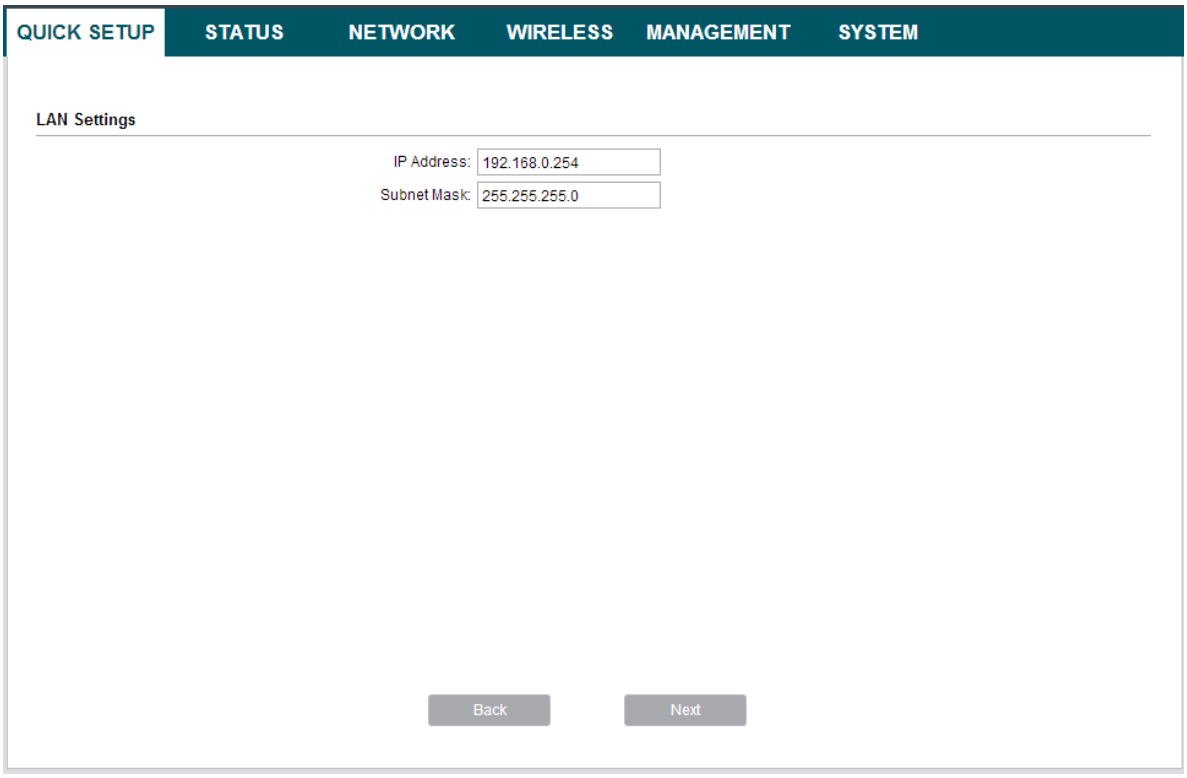
3. The **Finish** page will appear and display what you've configured previously. If you want to modify any parameter, click **Back** to reconfigure it. If all are confirmed, click **Finish** to complete the configuration.



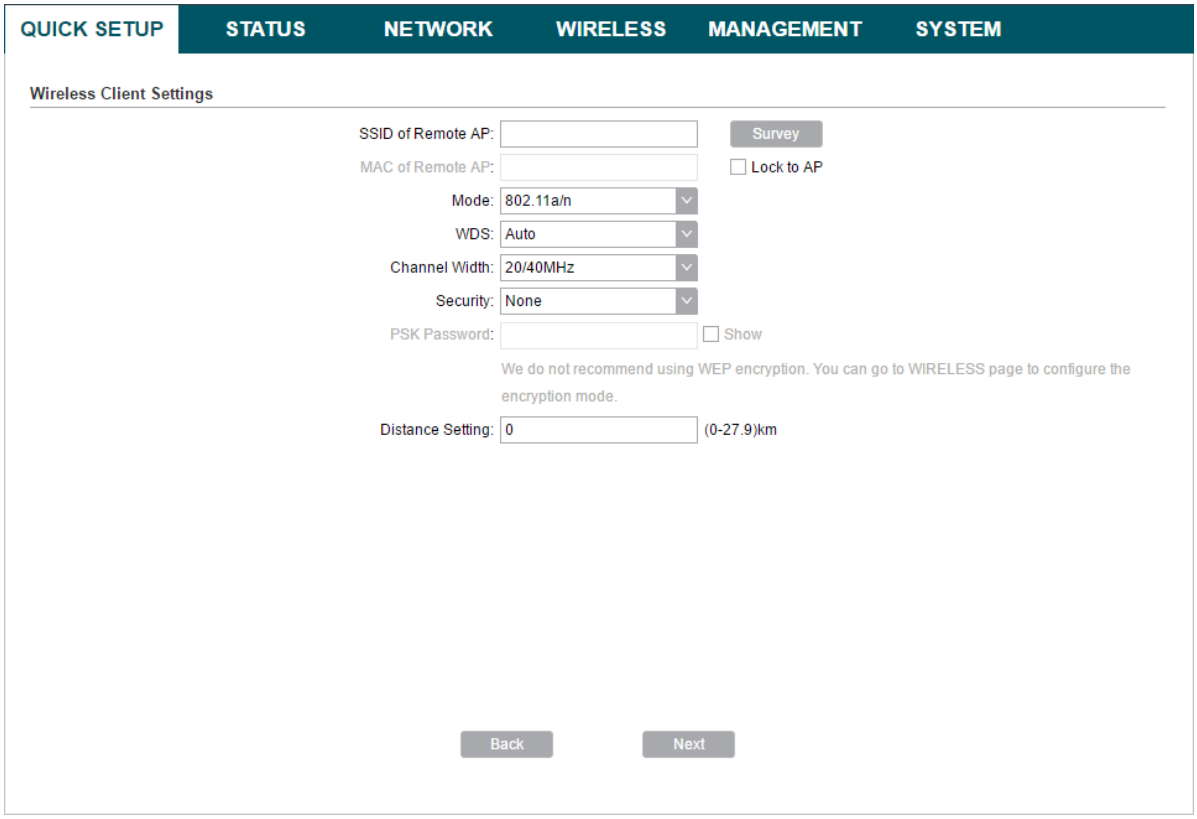
Client

If **Client** is selected, click **Next** and take the following steps:

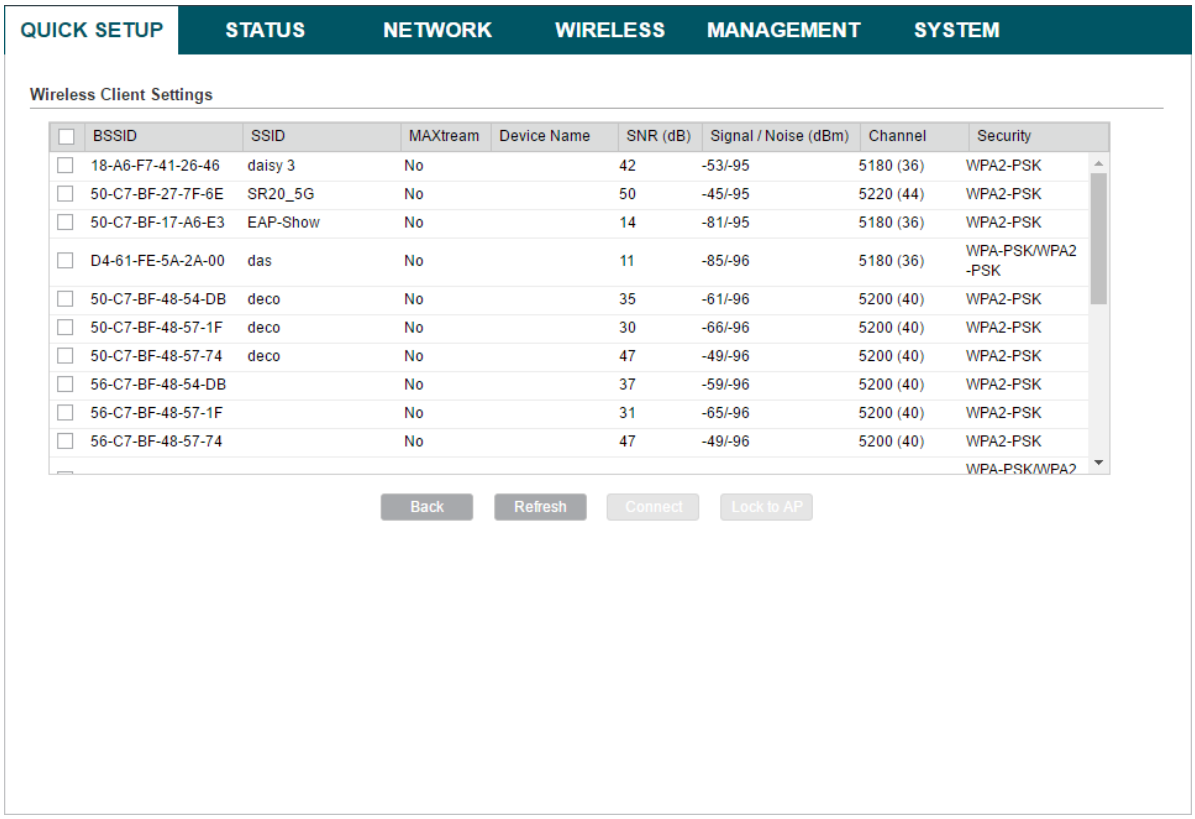
1. The **LAN Settings** page will appear as shown below. The default *IP Address* is 192.168.0.254 and the default *Subnet Mask* is 255.255.255.0. You can change the IP Address and Subnet Mask on this page when there is an IP conflict with other devices. We recommend you keep it by default. Click **Next**.



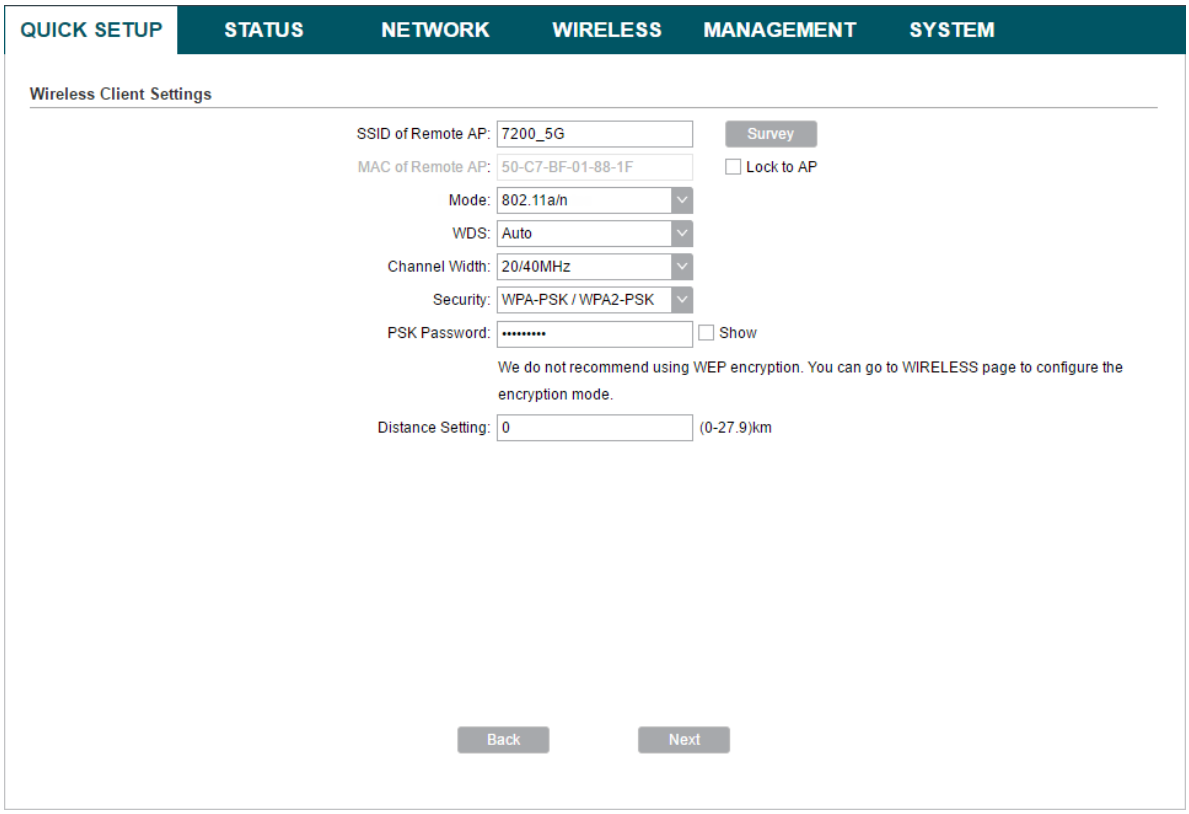
2. The **Wireless Client Settings** page will appear as shown below. Click **Survey** to search for wireless networks.



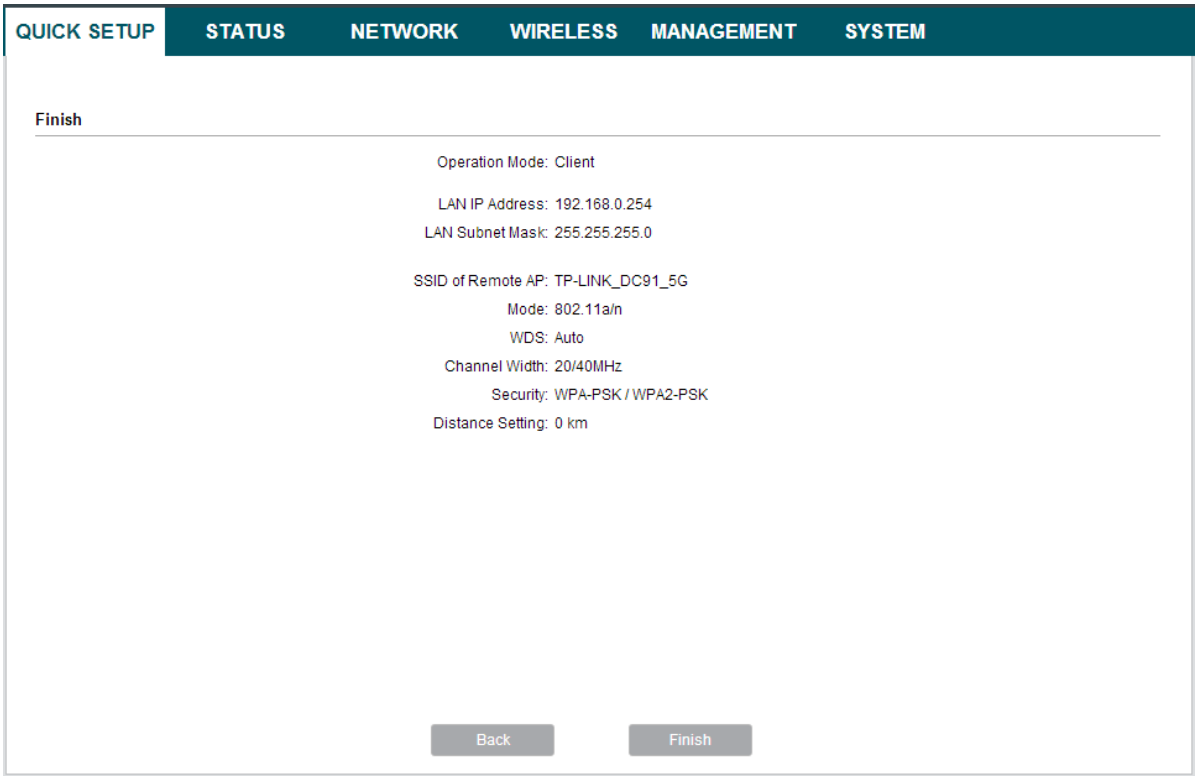
3. The AP list will appear as shown below. Select the desired wireless network and click **Connect**. It's possible that two or more networks use the same SSID in the AP list. **Lock to AP** can make the device connect to the specified AP you had connected before the next time.



4. If the root AP needs password to be connected, you should select the same **Mode**, **Channel Width** and **Security** type and enter the same ***PSK Password*** as entered on the root AP/router. Enter the distance between this device and the root AP in ***Distance*** setting. Then click **Next**.



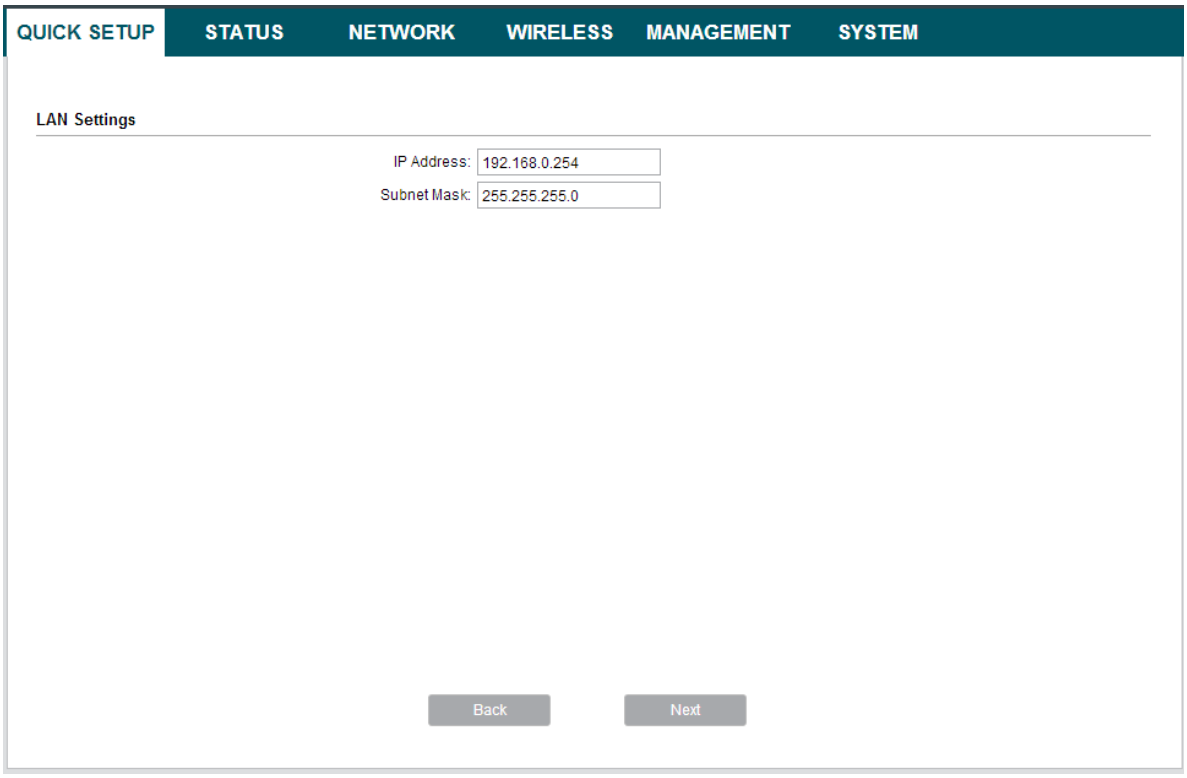
5. The **Finish** page will appear and display what you've configured previously. If you want to modify any parameter, click **Back** to reconfigure it. If all are confirmed, click **Finish** to complete the configuration.



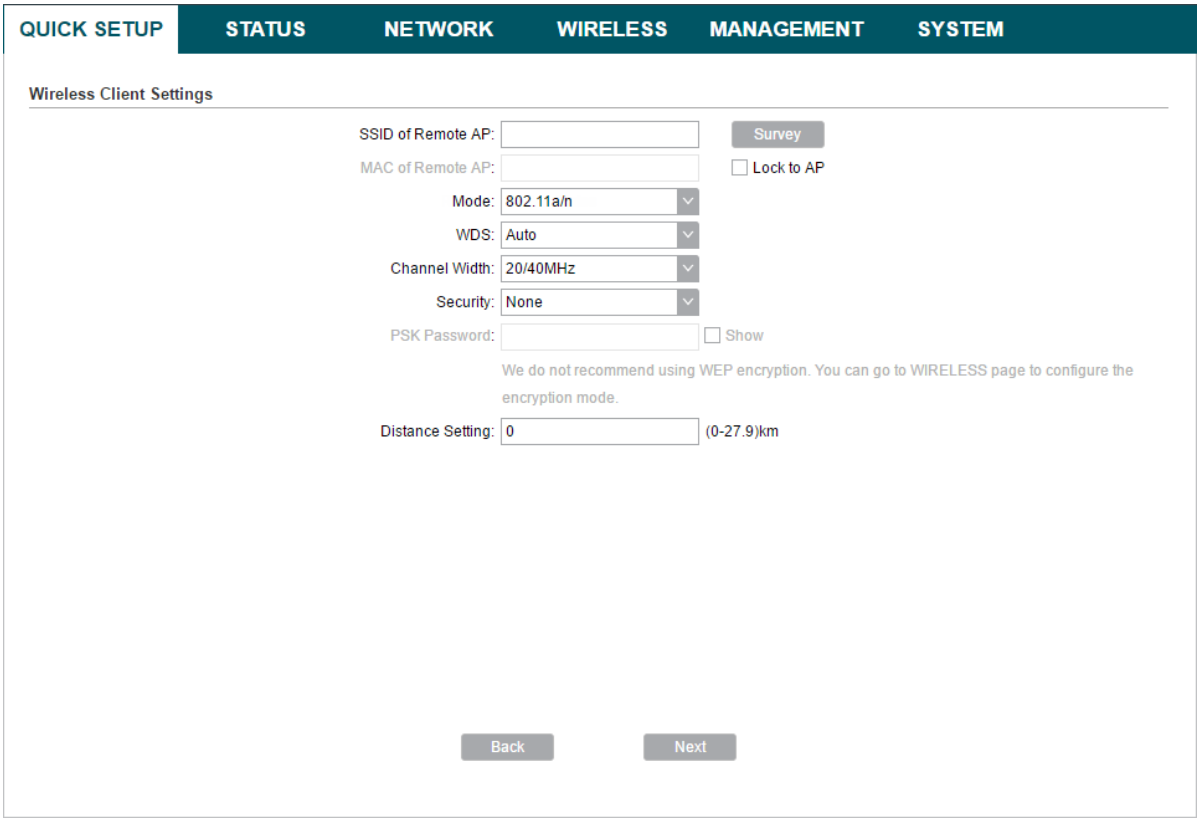
Repeater (Range Extender)

If **Repeater (Range Extender)** is selected, click **Next** and take the following steps:

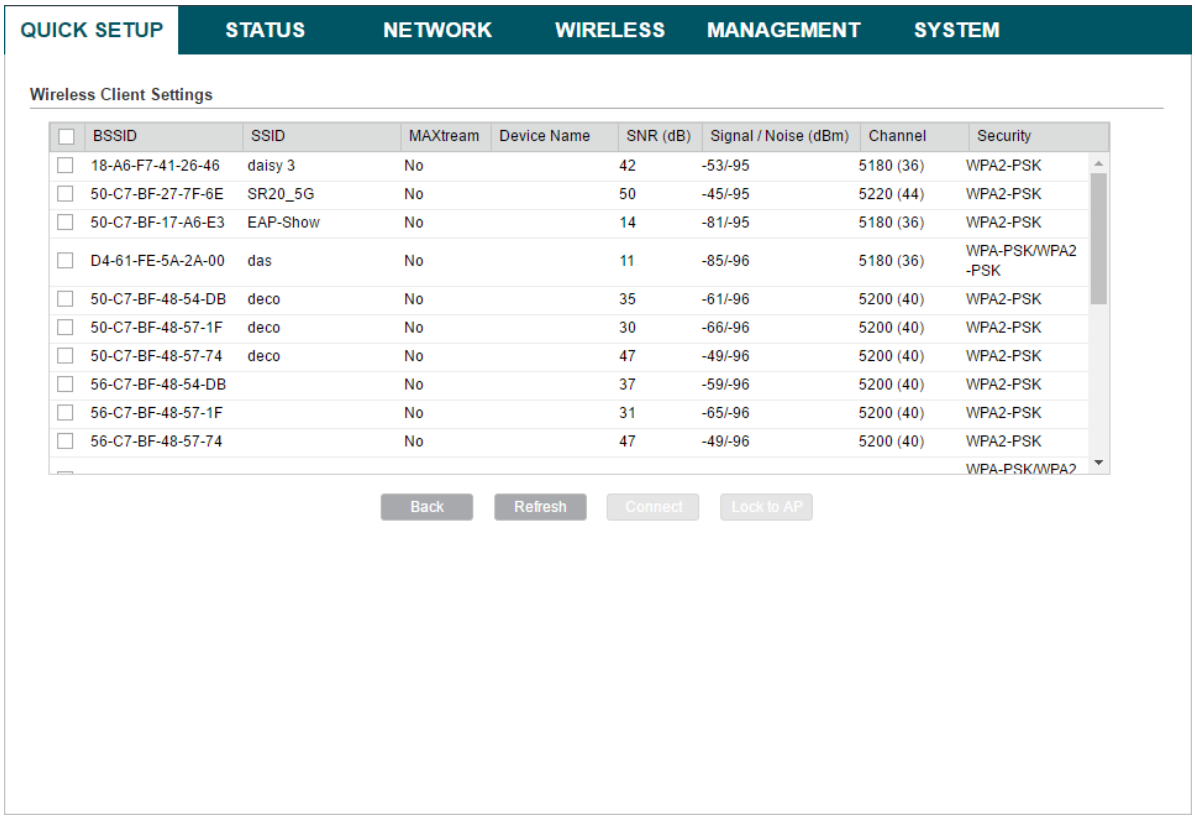
1. The **LAN Settings** page will appear as shown below. The default *IP Address* is 192.168.0.254 and the default *Subnet Mask* is 255.255.255.0. You can change the IP Address and Subnet Mask on this page when there is an IP conflict with other devices. We recommend you keep it by default. Click **Next**.



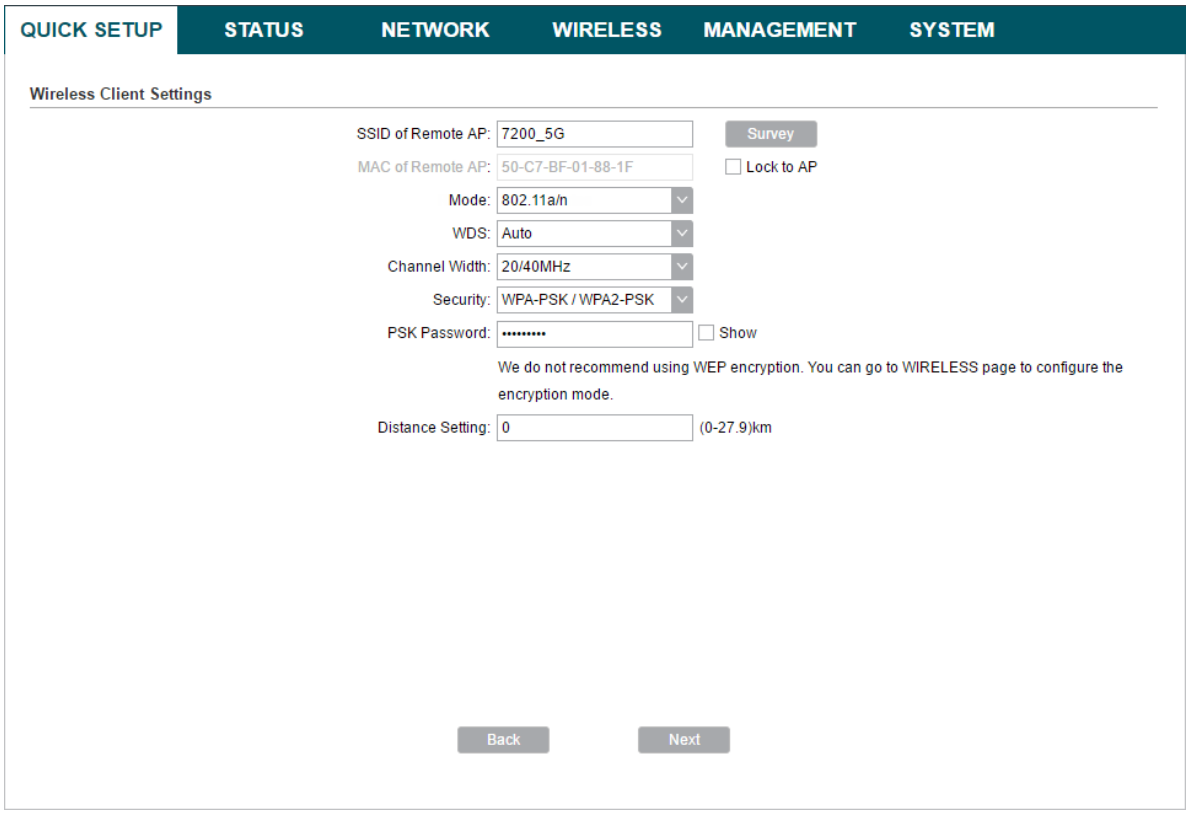
2. The **Wireless Client Settings** page will appear as shown below. Click **Survey** to search for wireless networks.



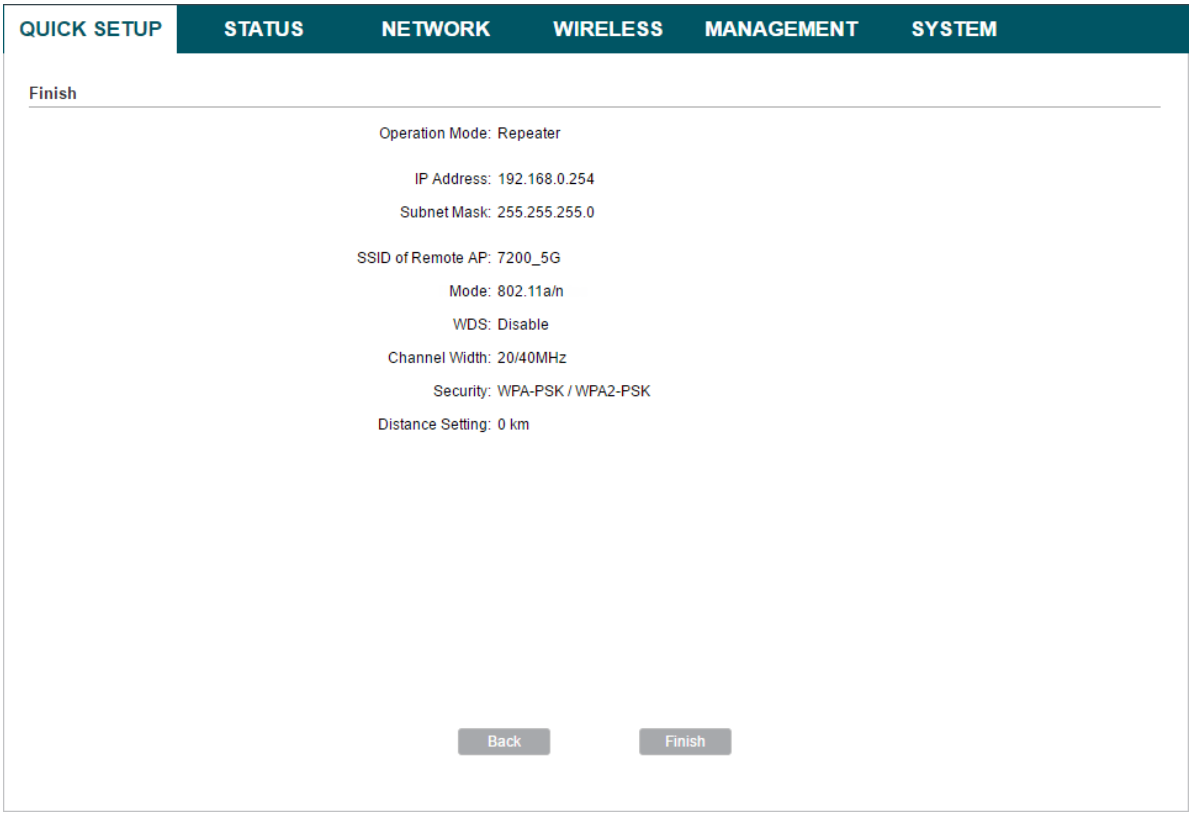
3. The AP list will appear as shown below. Select the desired wireless network and click **Connect**. It's possible that two or more networks use the same SSID in the AP list. **Lock to AP** can make the device connect to the specified AP you had connected before the next time.



4. If the root AP needs password to be connected, you should select the same ***Mode***, ***Channel Width*** and ***Security*** type and enter the same ***PSK Password*** as entered on the root AP/router. Enter the distance between this device and the root AP/router in ***Distance setting***. Then click **Next**.



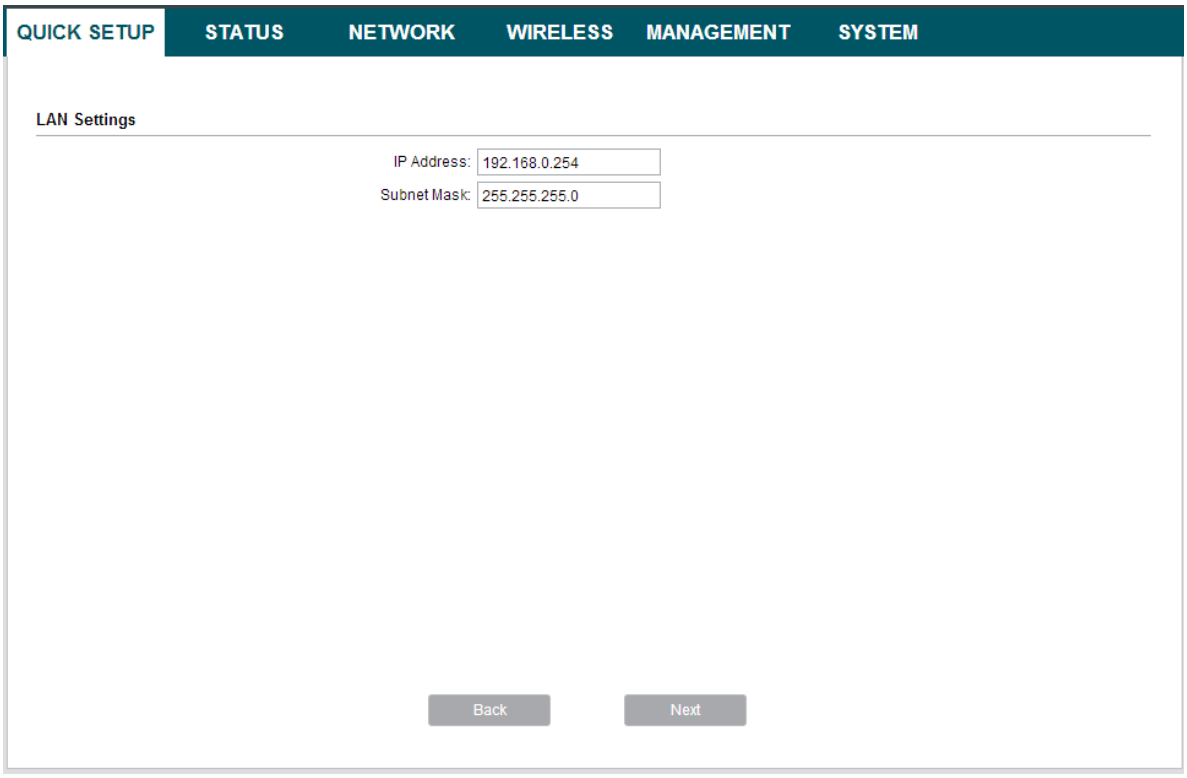
5. The **Finish** page will appear and display what you've configured previously. If you want to modify any parameter, click **Back** to reconfigure it. If all are confirmed, click **Finish** to complete the configuration.



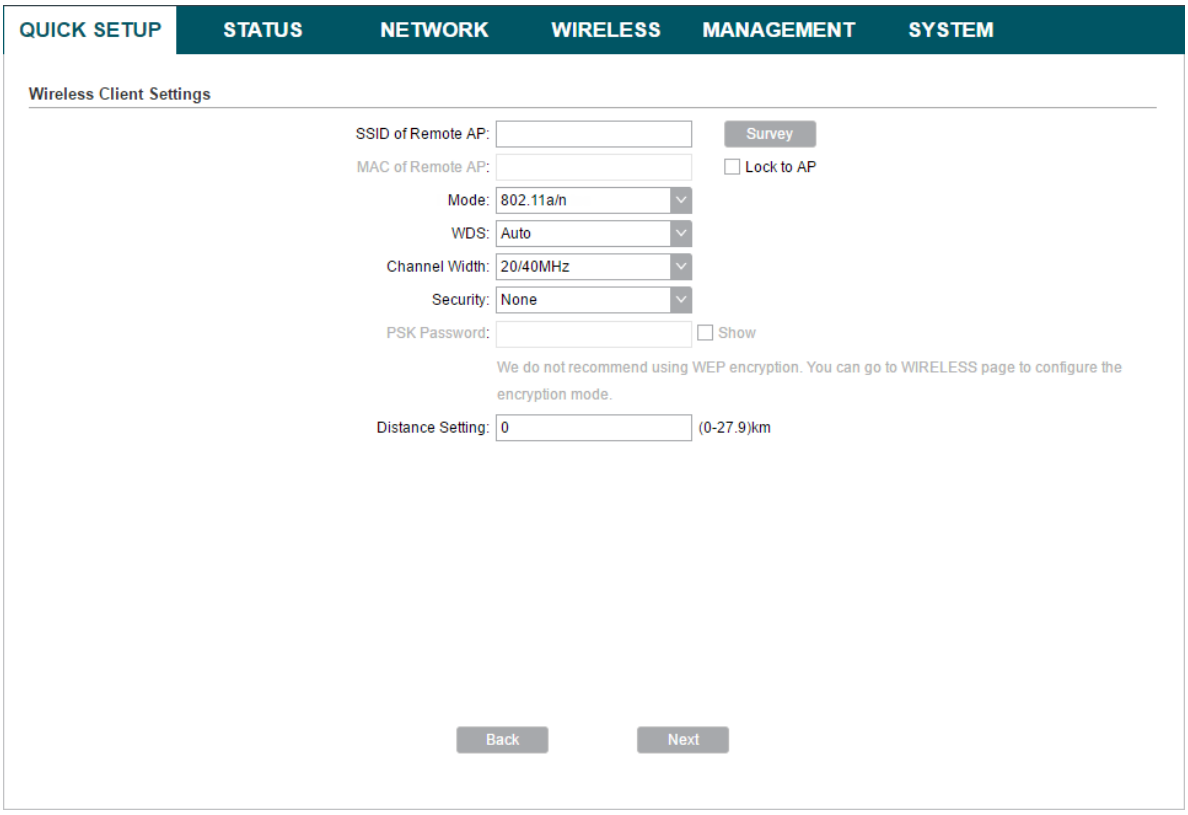
Bridge

If **Bridge** is selected, click **Next** and take the following steps:

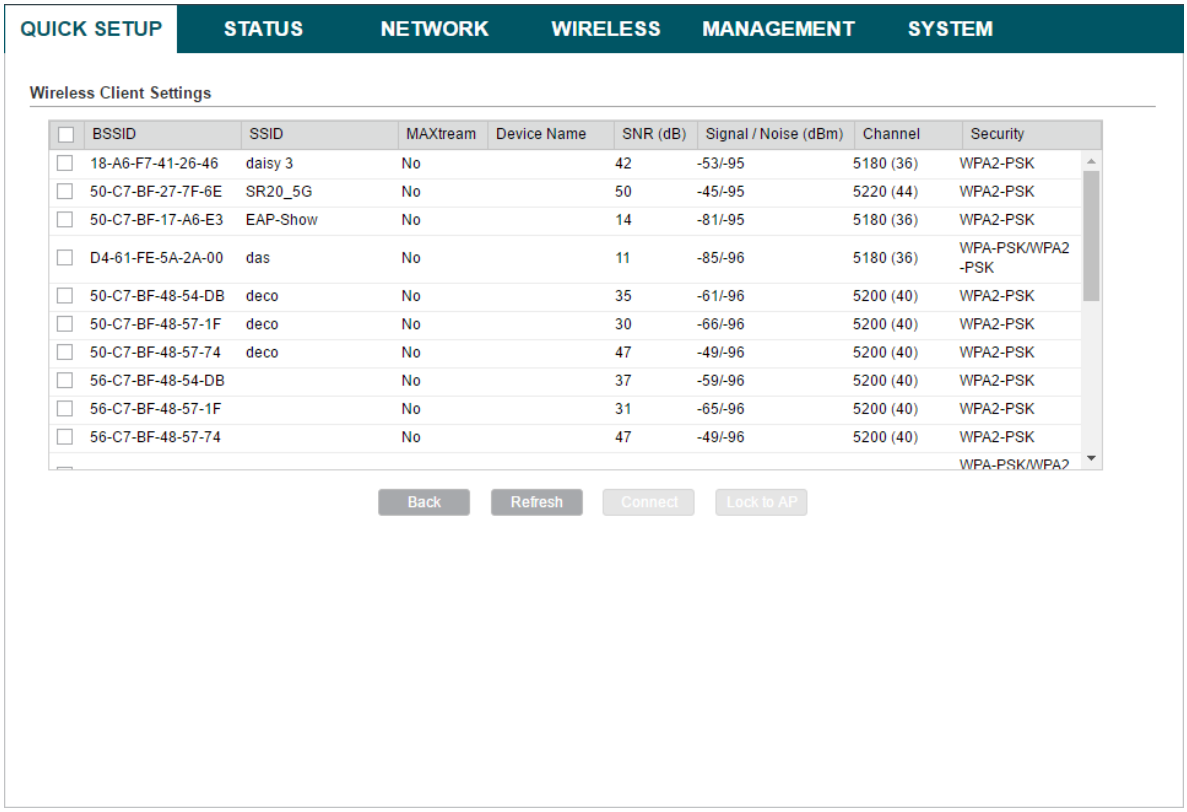
1. The **LAN Settings** page will appear as shown below. The default *IP Address* is 192.168.0.254 and the default *Subnet Mask* is 255.255.255.0. You can change the IP Address and Subnet Mask on this page when there is an IP conflict with other devices. We recommend you keep it by default. Click **Next**.



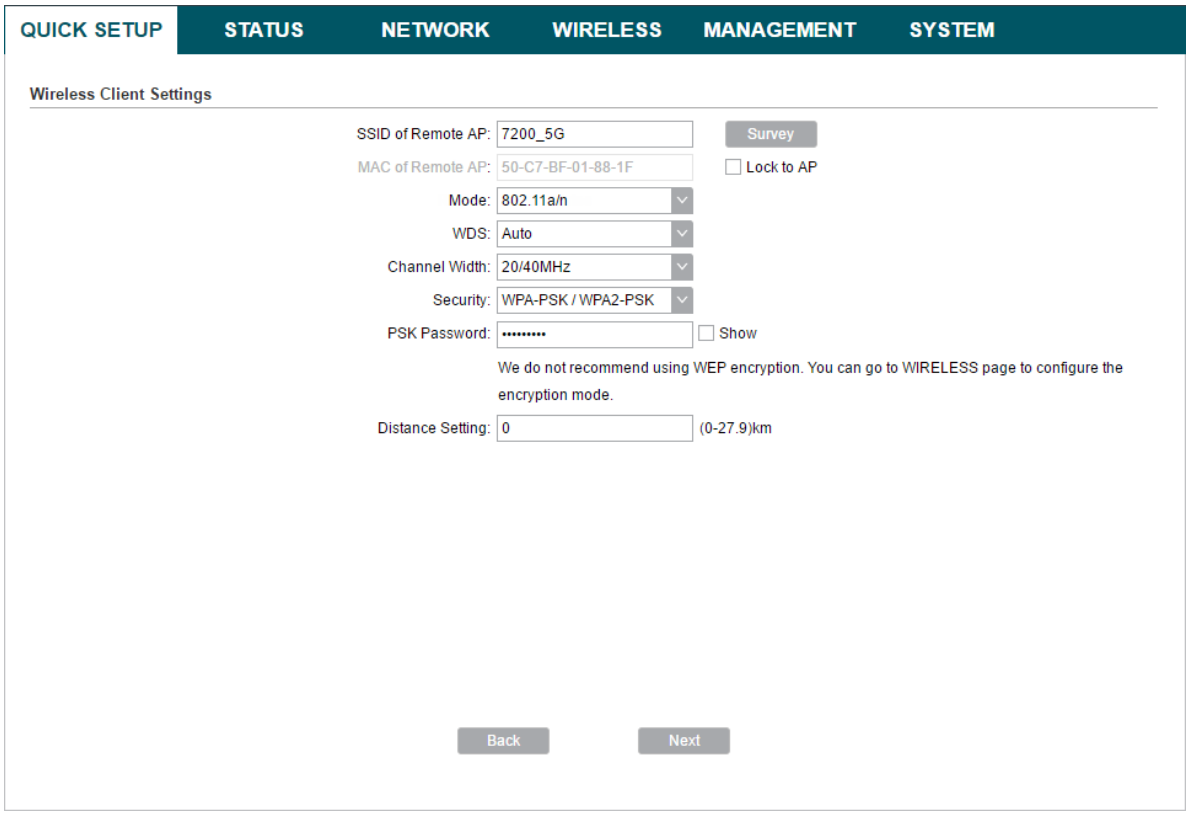
2. The **Wireless Client Settings** page will appear as shown below. Click **Survey** to search for wireless networks.



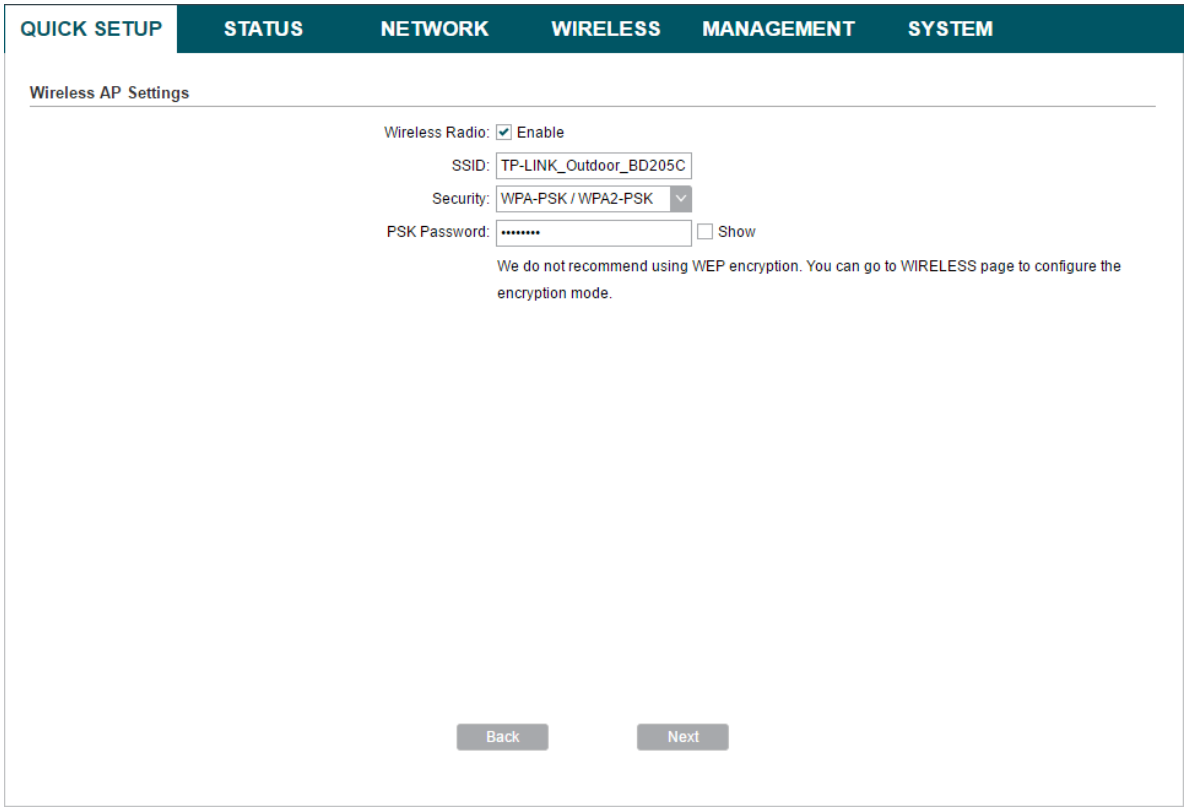
3. The AP list will appear as shown below. Select the desired wireless network and click **Connect**. It's possible that two or more networks use the same SSID in the AP list. **Lock to AP** can make the device connect to the specified AP you had connected before the next time.



4. If the root AP needs password to be connected, you should select the same **Mode**, **Channel Width** and **Security** type and enter the same ***PSK Password*** as entered on the root AP. Enter the distance between this device and the root AP/router in ***Distance setting***. Then click **Next**.



5. Create a new *SSID* and *PSK password* for the local wireless network. The wireless AP settings for the local network will be set the same as your root AP by default. Click **Next**.

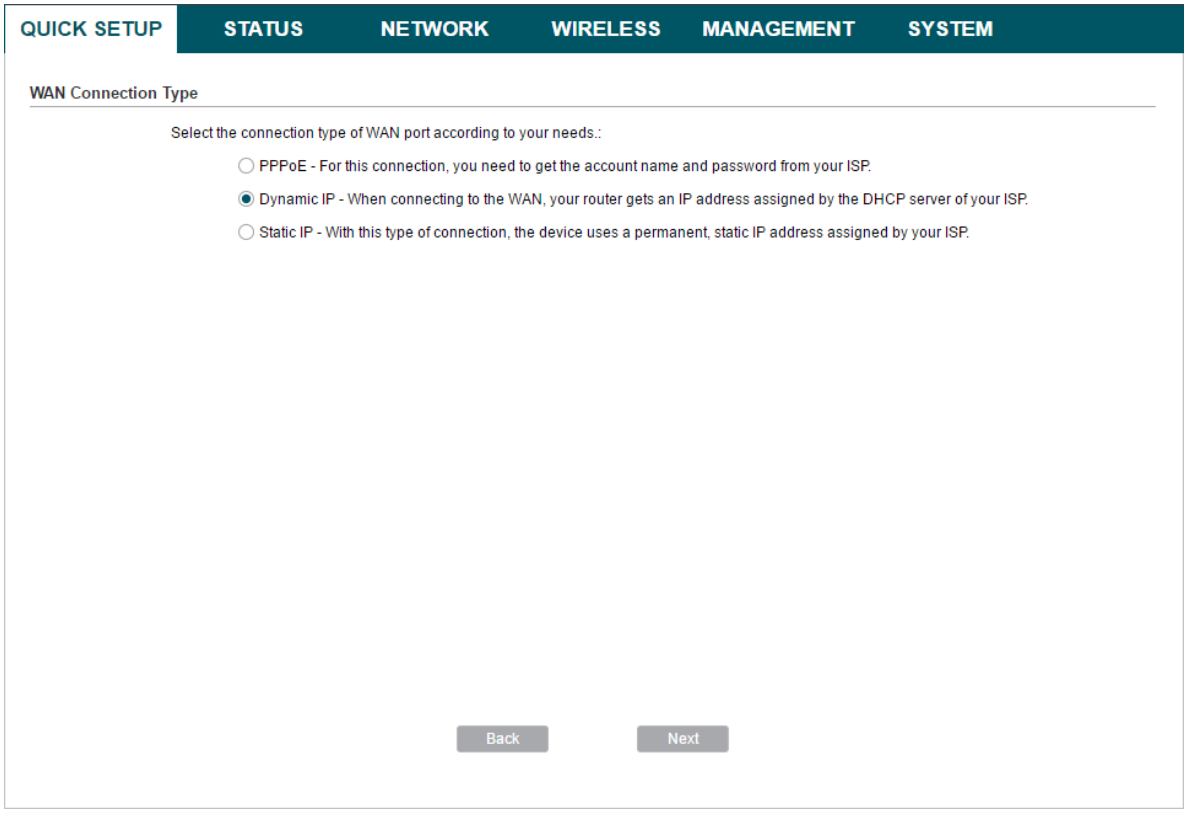


6. The **Finish** page will appear and display what you've configured previously. If you want to modify any parameter, click **Back** to reconfigure it. If all are confirmed, click **Finish** to complete the configuration.

AP Router

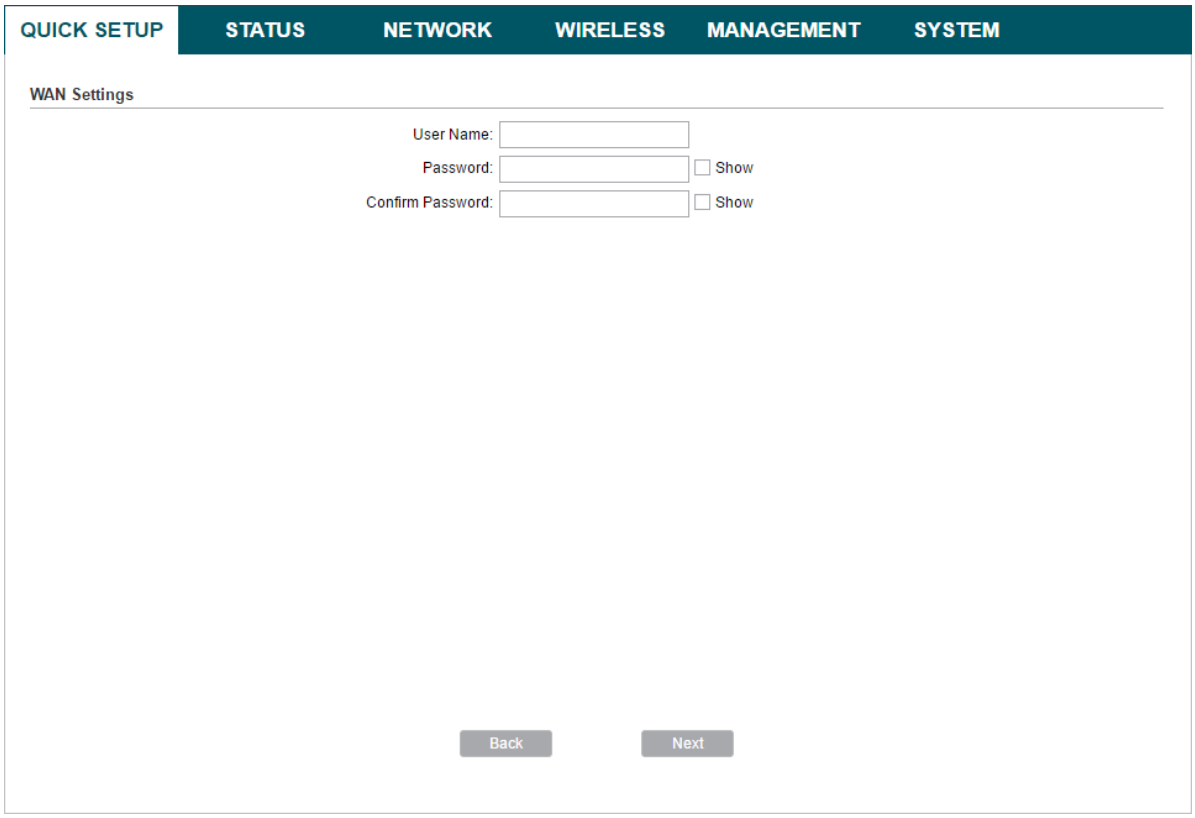
If **AP Router** is selected, click **Next** and take the following steps:

1. The **WAN Connection Type** page will appear as shown below. Choose the suitable WAN connection type, and then click **Next**.



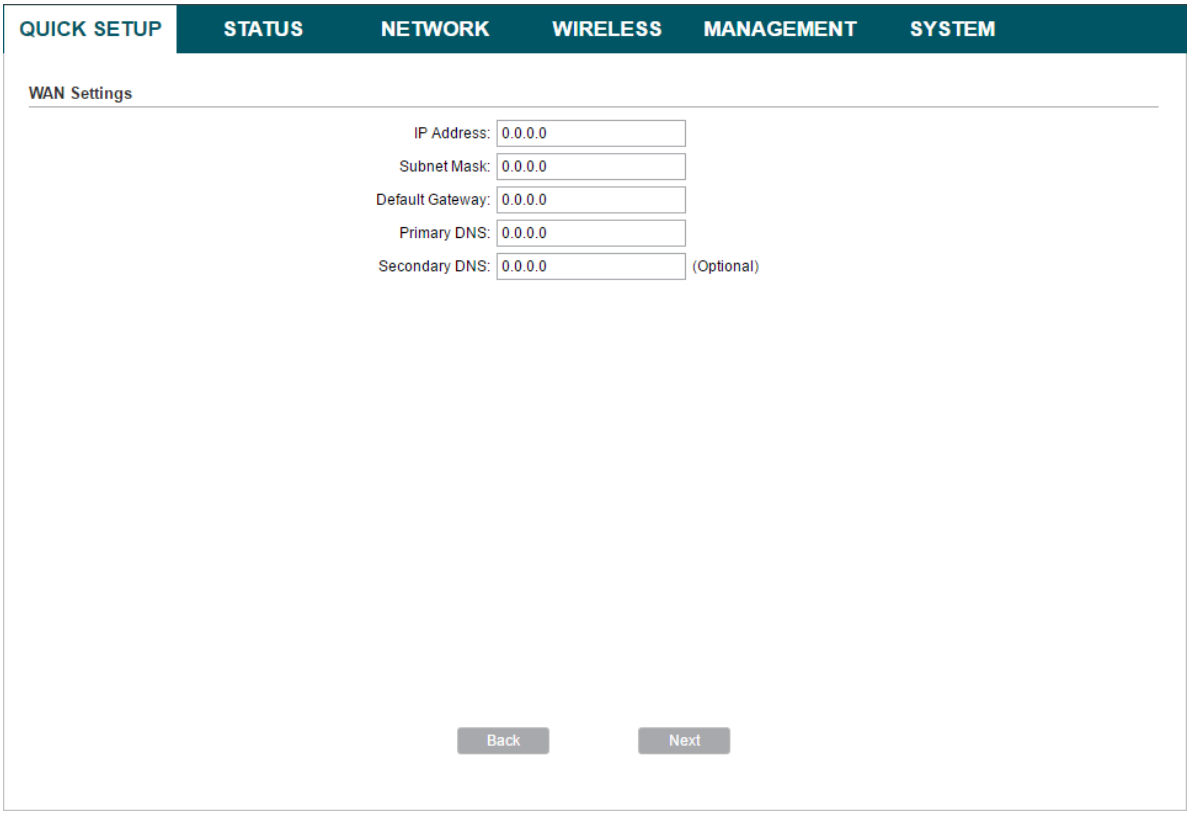
2. The device supports three popular ways PPPoE, Dynamic IP and Static IP to connect to the Internet. If you are not sure of the connection type, please consult your ISP.

- **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, and then click **Next** to proceed. Please note that these fields are case-sensitive.

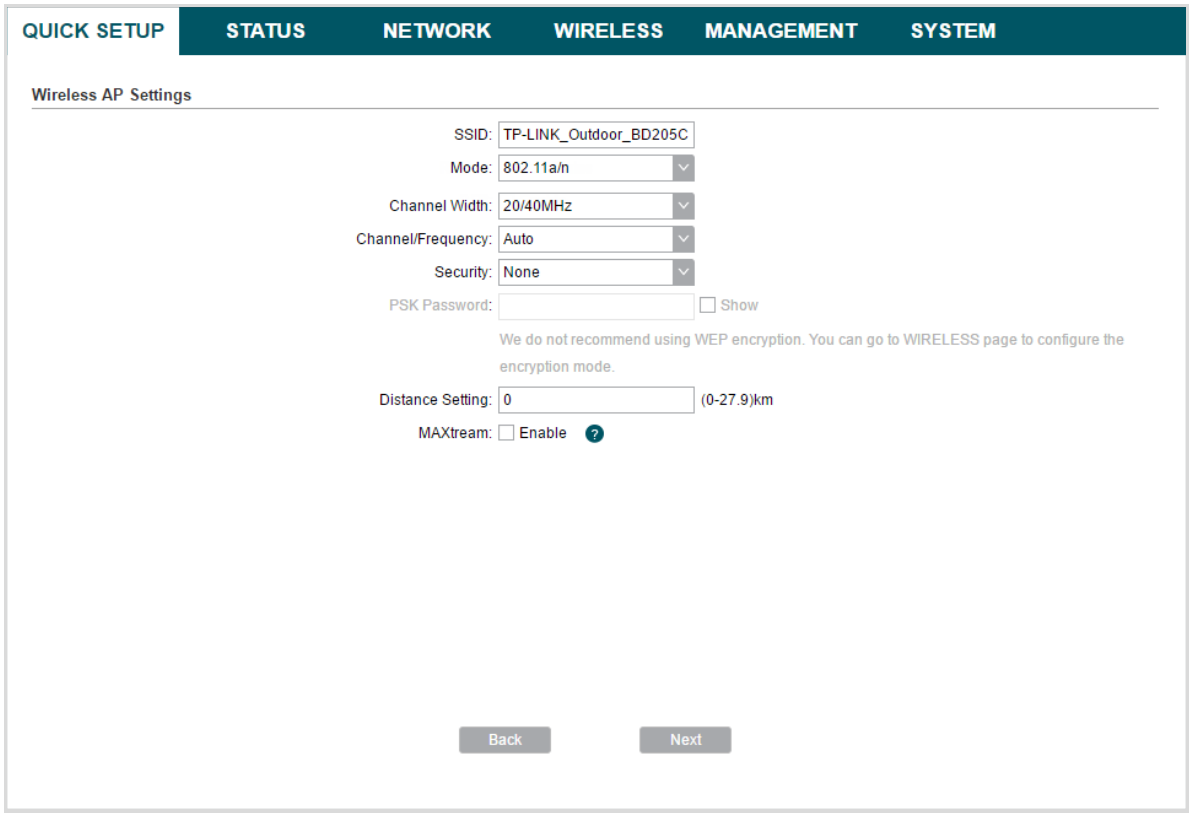


- **Dynamic IP** - For this connection, Your ISP uses a DHCP server to assign your router an IP address for connecting to the Internet. You don't need to configure any parameters, Click **Next** to proceed.

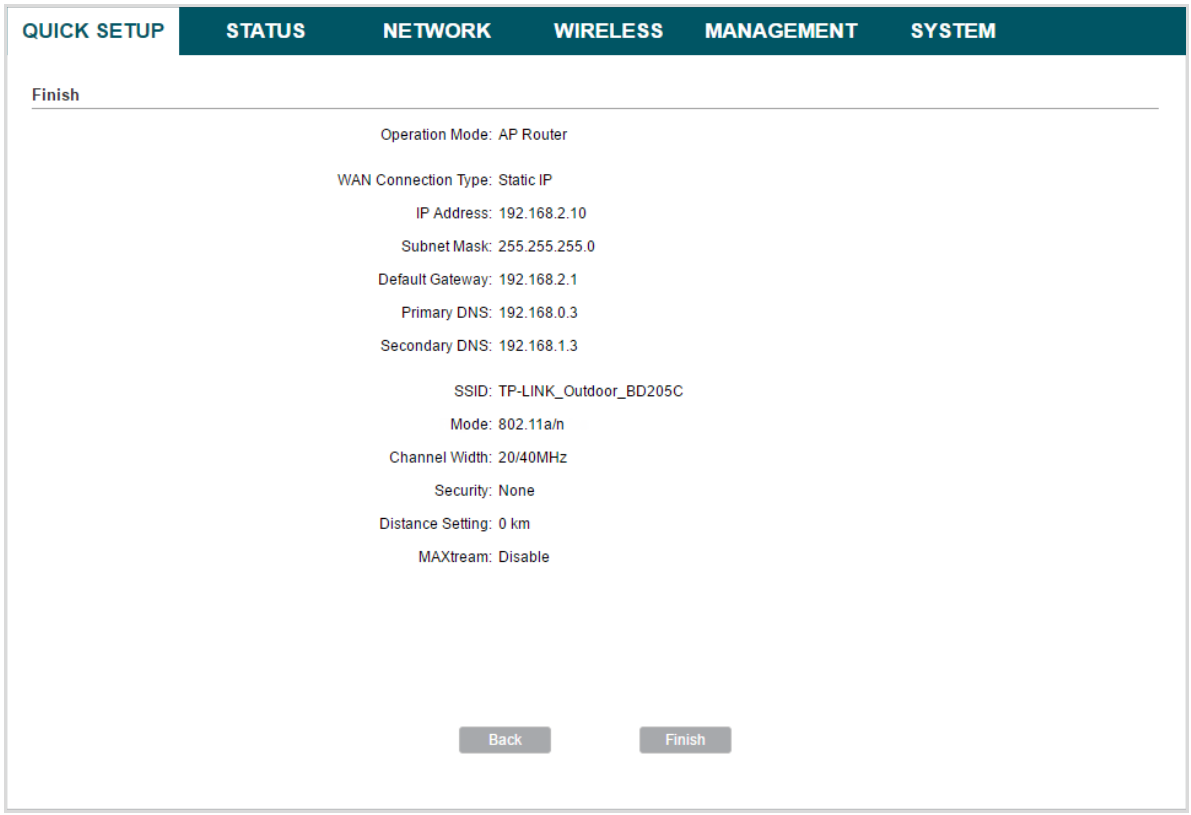
- **Static IP** - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned. In this type, you should fill in the IP address, Subnet Mask, Default Gateway, and DNS IP address manually, which are specified by your ISP. Then click **Next** to proceed.



3. After configuring WAN connection type, the **Wireless AP Settings** page will appear as shown below. Create an easy-to-remember name for your wireless network. We recommend to select **WPA-PSK/WPA2-PSK** in the ***Security*** box and enter the ***PSK Password*** below to prevent unauthorized access to your AP. Enter the distance between this device and the furthest client in ***Distance Setting***. Then click **Next**.



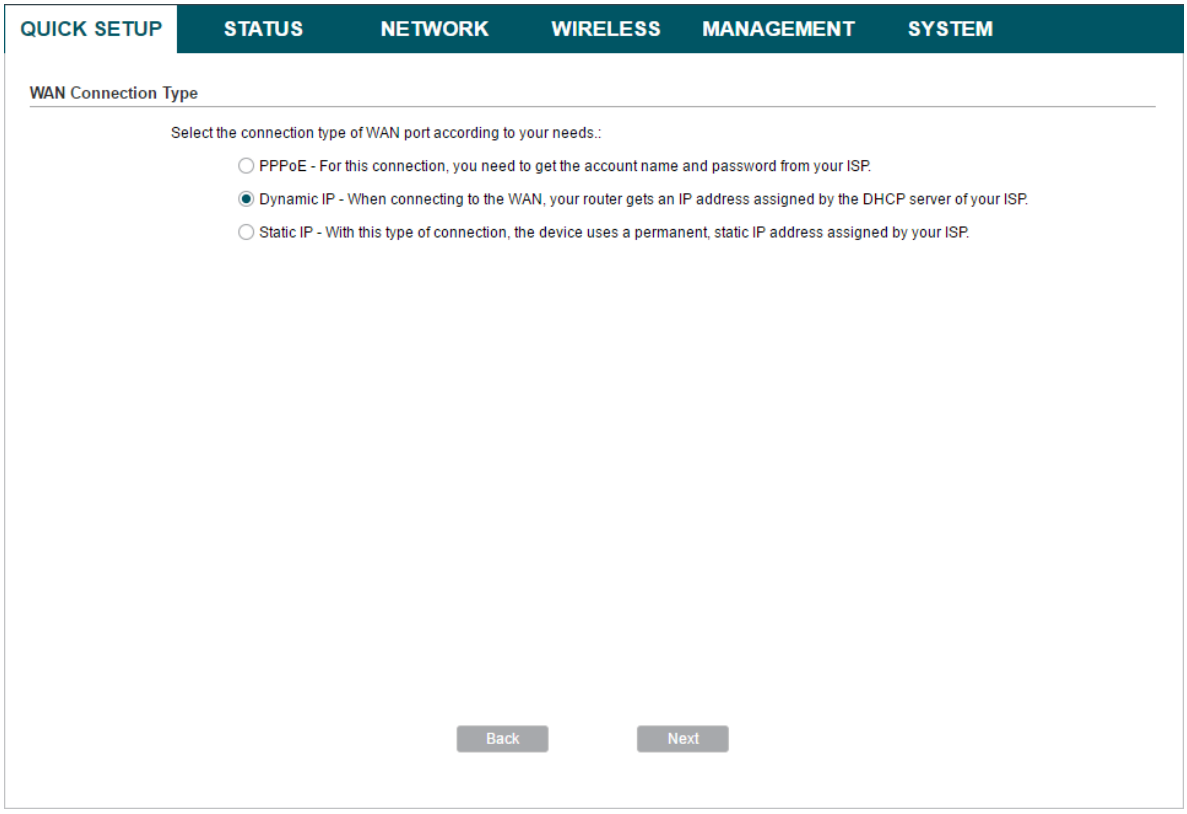
4. The **Finish** page will appear and display what you've configured previously. If you want to modify any parameter, click **Back** to reconfigure it. If all are confirmed, click **Finish** to complete the configuration.



AP Client Router (WISP Client)

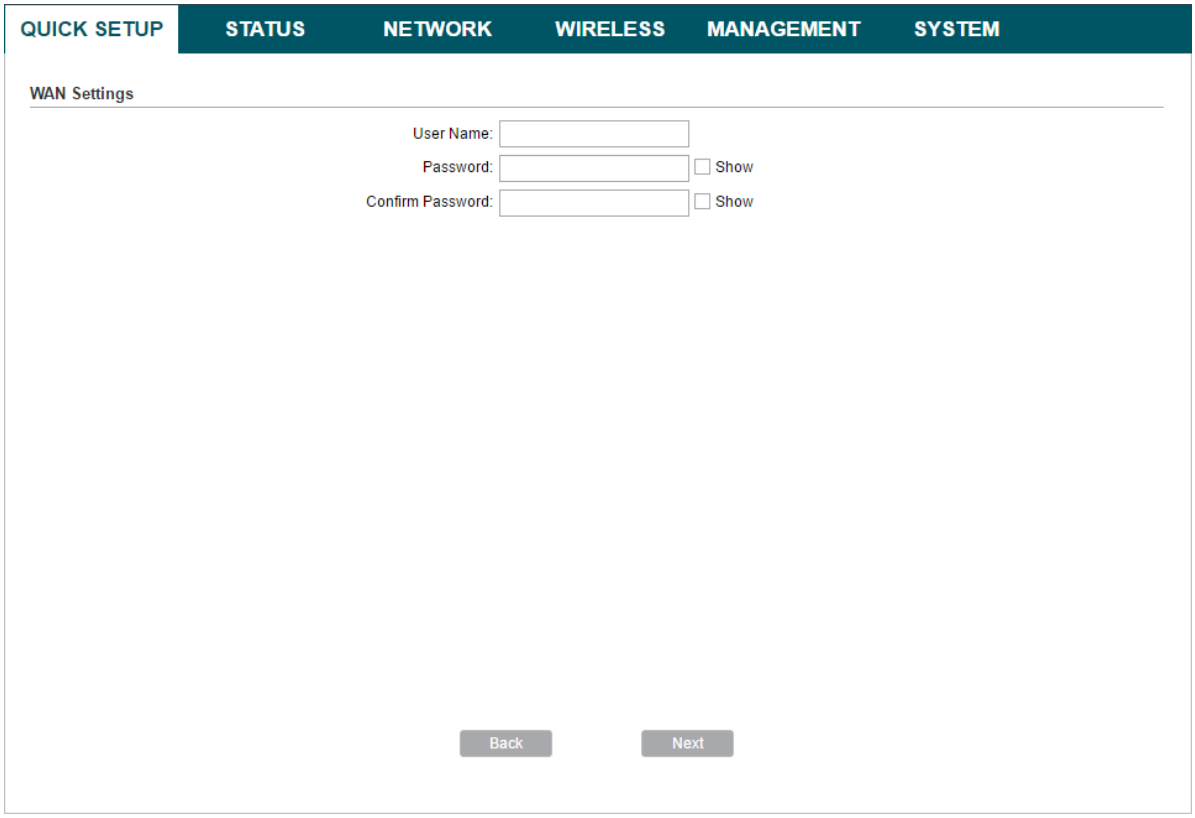
If **AP Client Router (WISP Client)** is selected, click **Next** and take the following steps:

1. The **WAN Connection Type** page will appear as shown below. Choose the suitable WAN connection type, and then click **Next**.

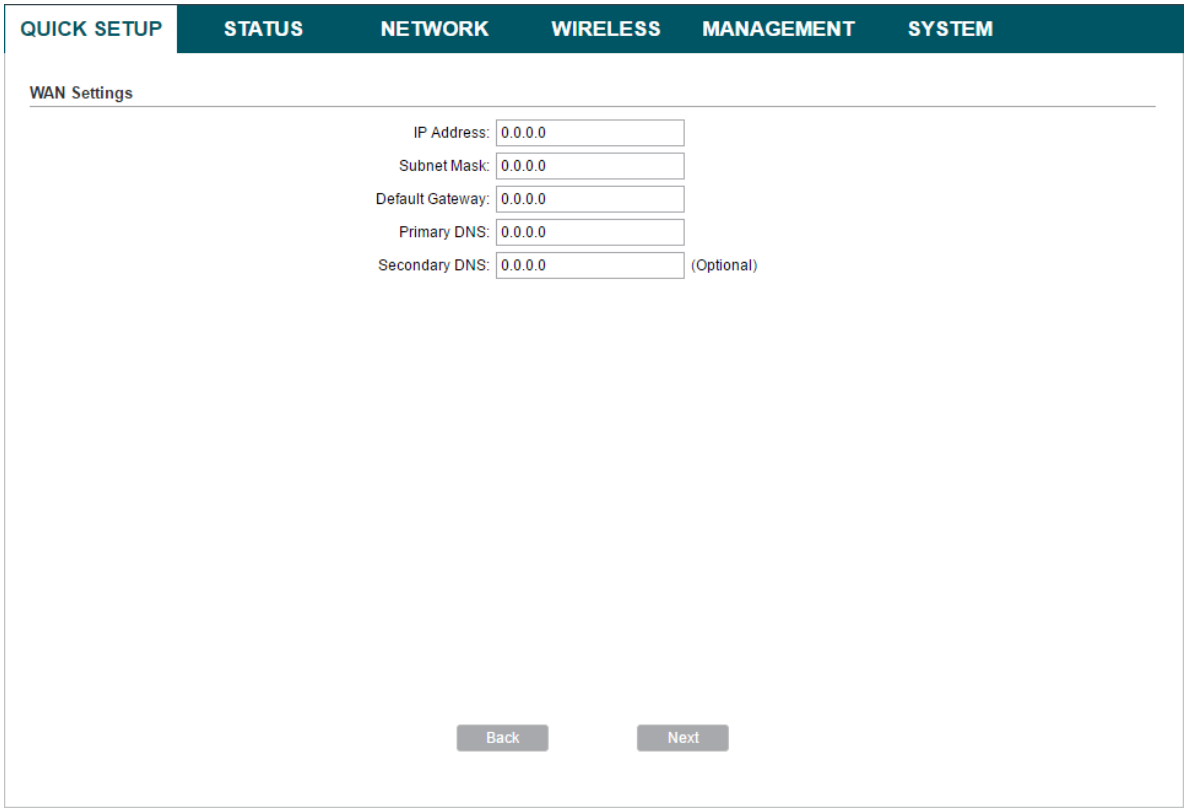


2. The device supports three popular ways **PPPoE**, **Dynamic IP** and **Static IP** to connect to the Internet. To make sure the connection type your ISP provides, please refer to your ISP.

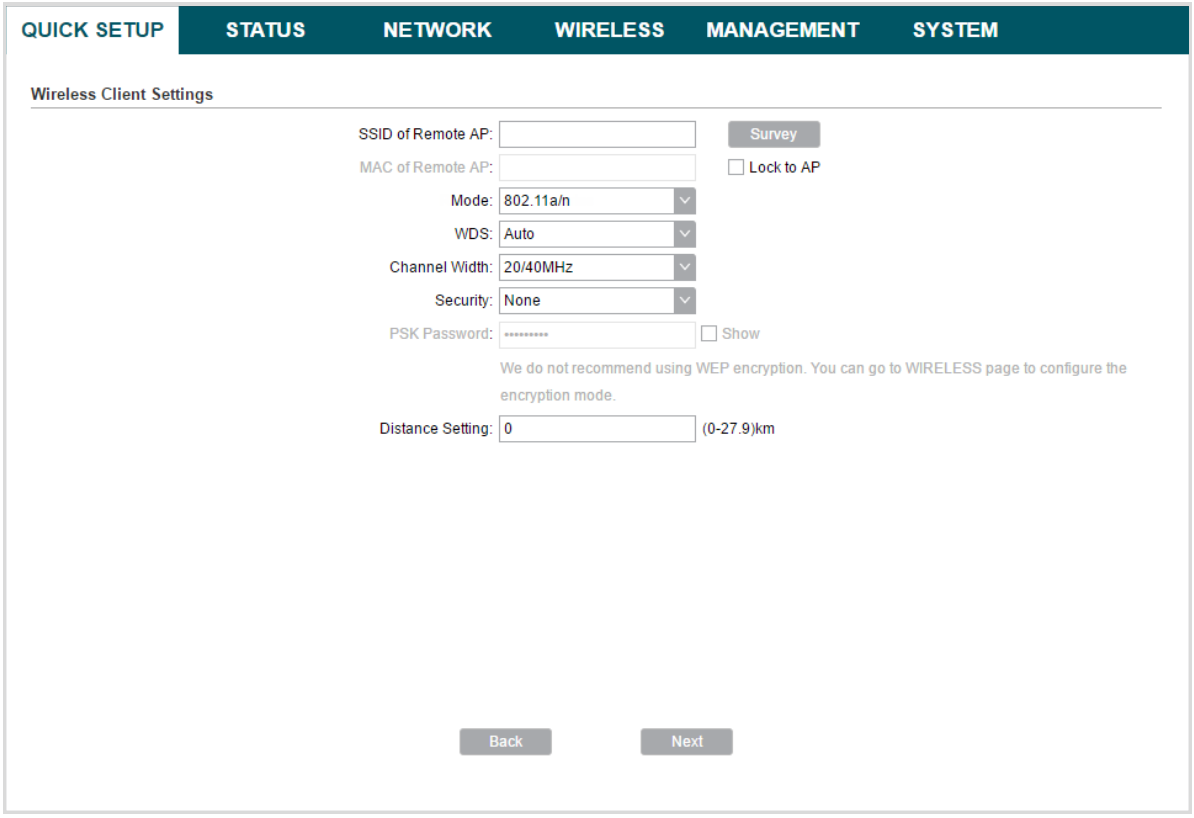
- **PPPoE** - If your ISP delivers Internet through phone line and provides you with username and password, you should choose this type. Under this condition, you should fill in both ***User Name*** and ***Password*** that the ISP supplied, and then click **Next** to proceed. Please note that these fields are case-sensitive.



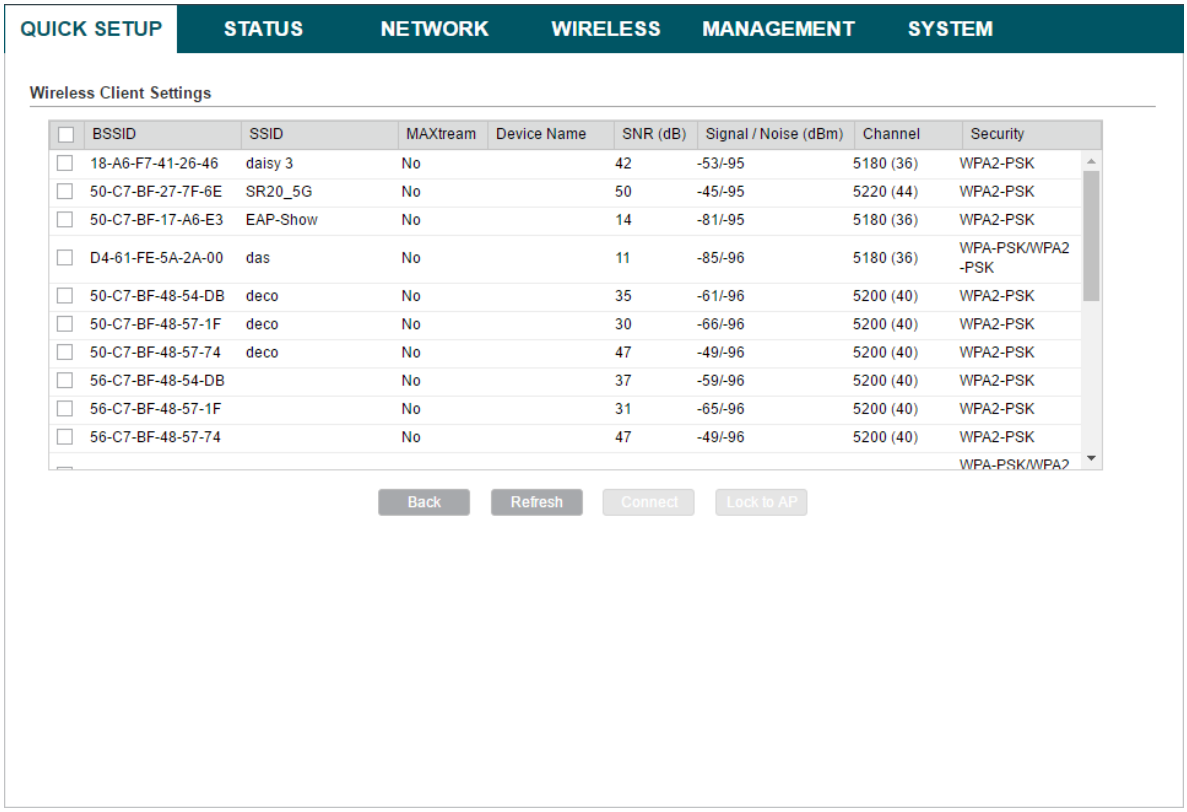
- **Dynamic IP** - For this connection, Your ISP uses a DHCP server to assign your router an IP address for connecting to the Internet. You don't need to configure any parameters, Click **Next** to proceed.
- **Static IP** - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned. In this type, you should fill in the IP address, Subnet Mask, Default Gateway, and DNS IP address manually, which are specified by your ISP. Then click **Next** to proceed.



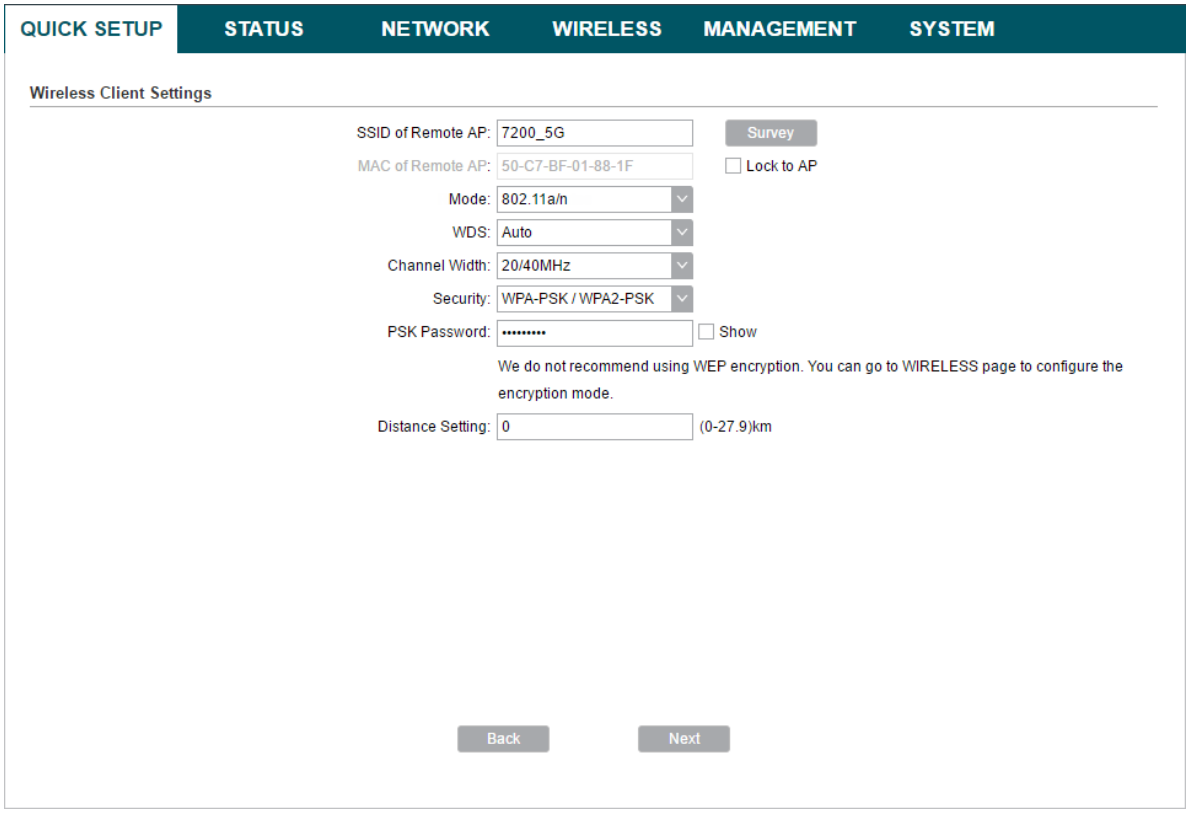
3. After configuring WAN connection type, The **Wireless Client Settings** page will appear as shown below. Click **Survey** to search for wireless networks.



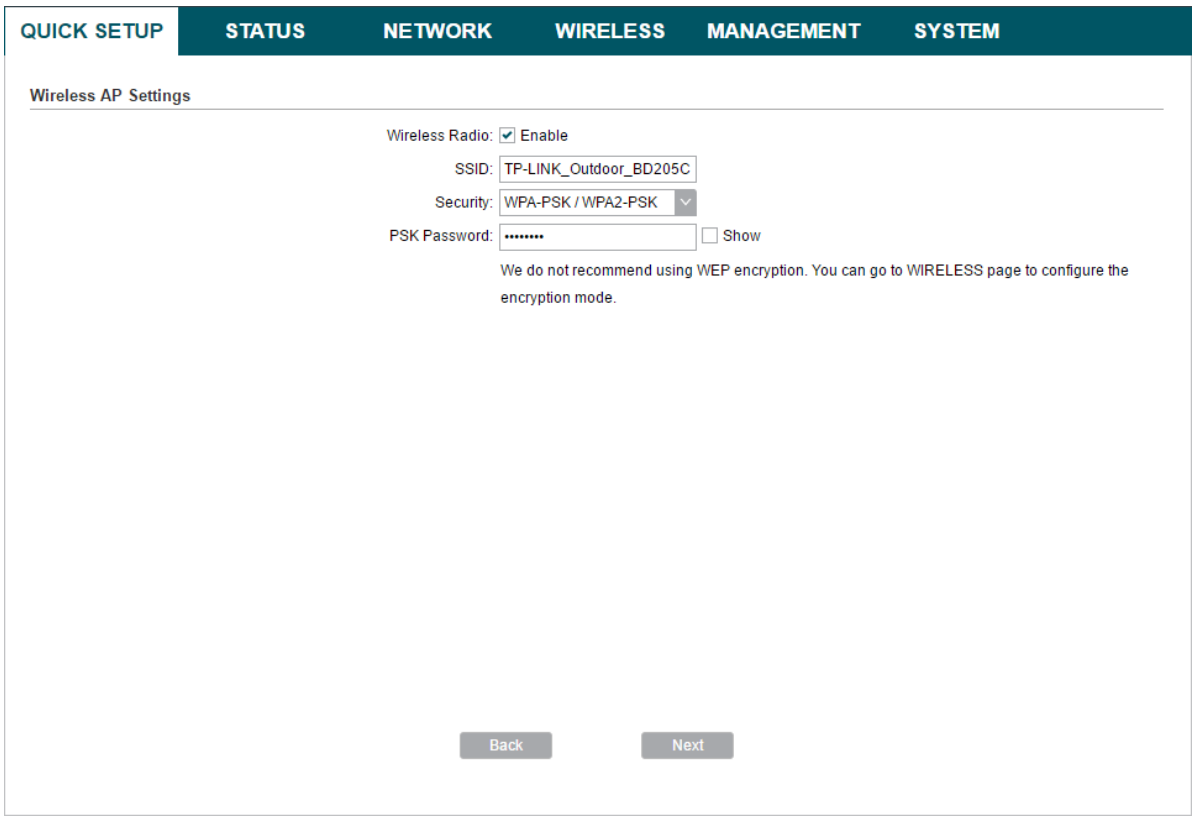
4. The AP list will appear as shown below. Select the desired wireless network and click **Connect**. It's possible that two or more networks use the same SSID in the AP list. **Lock to AP** can make the device connect to the specified AP you had connected before the next time.



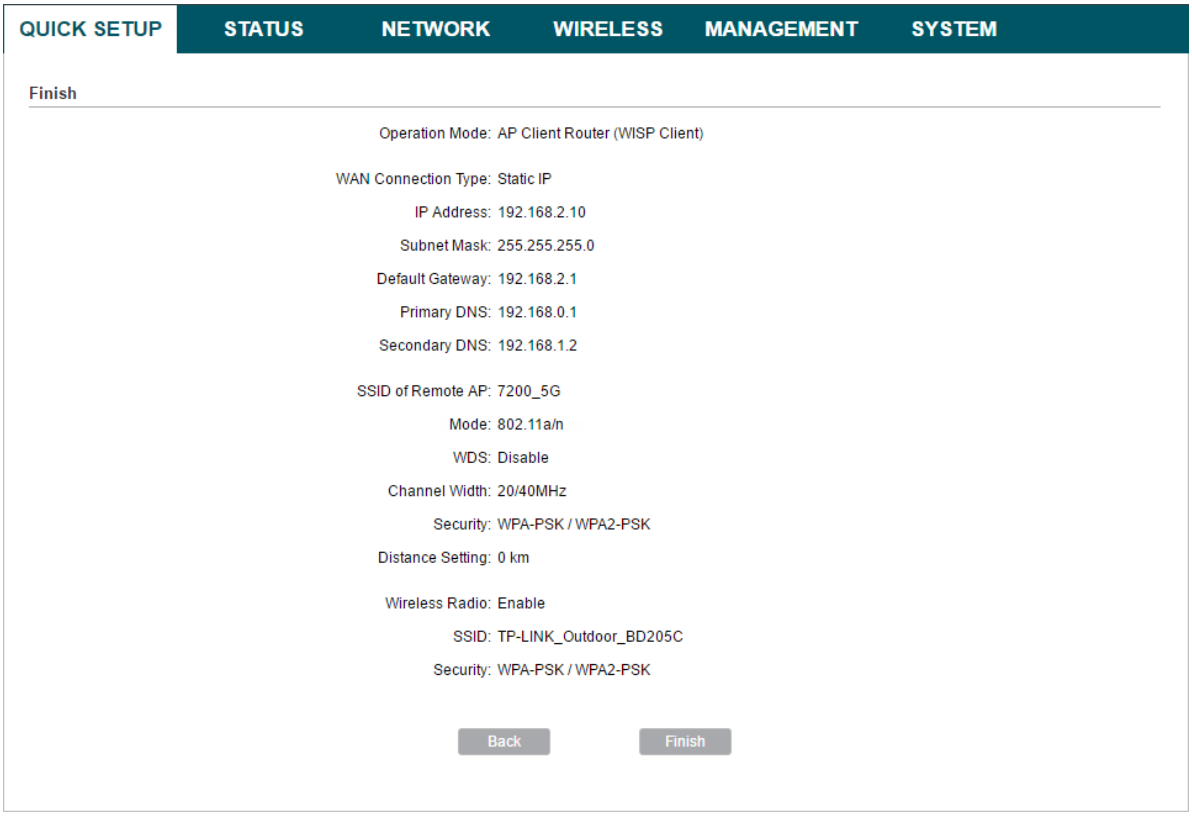
5. If the root AP needs password to be connected, you should select the same **Mode**, **Channel Width** and **Security** type and enter the same ***PSK Password*** as entered on the root AP/router. Enter the distance between this device and the root AP/router in ***Distance setting***. Then click **Next**.



6. Create a new ***SSID*** and ***PSK Password*** for the local wireless network. The wireless AP settings for the local network will be set the same as your root AP by default. Click **Next**.

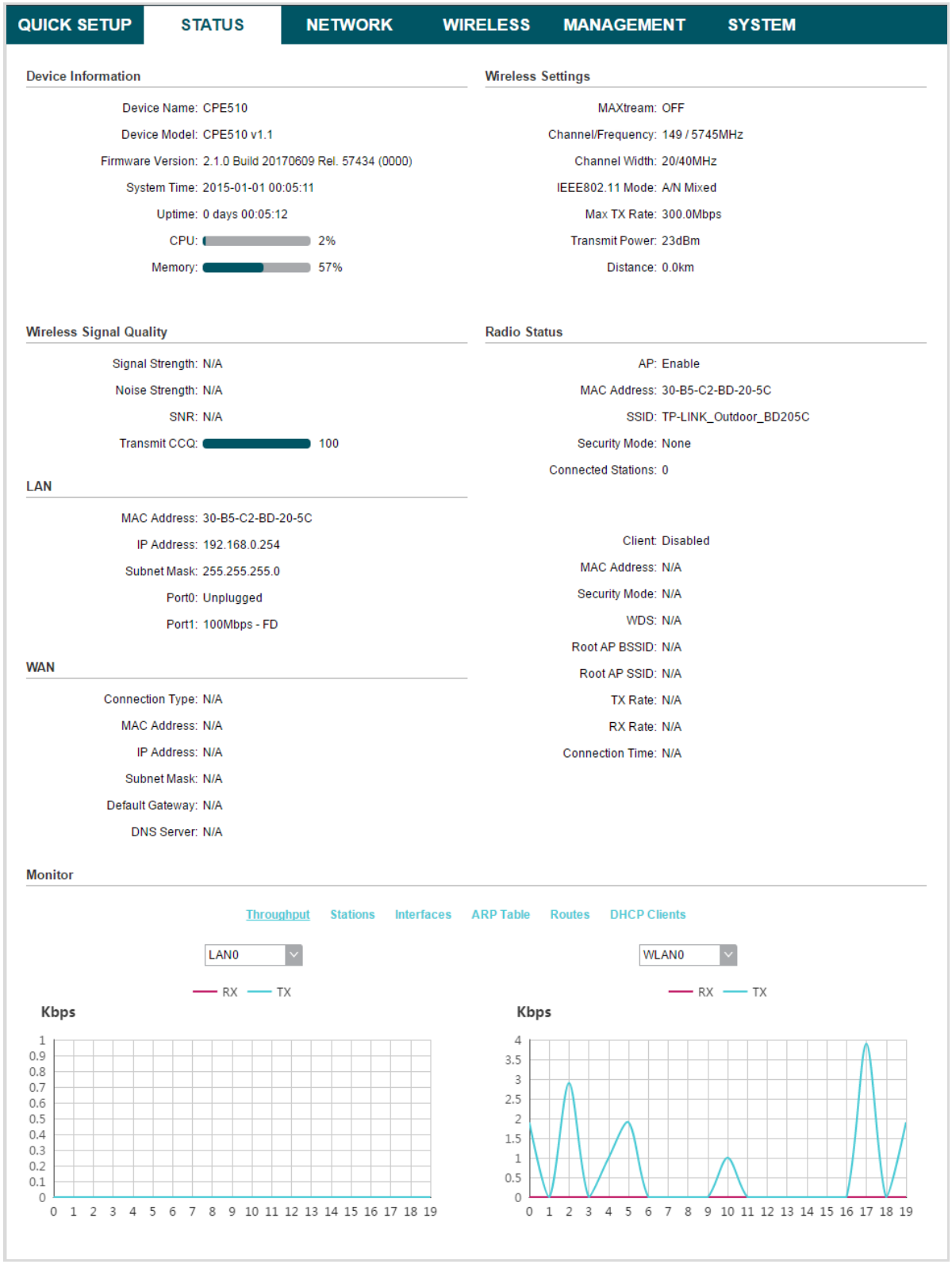


7. The **Finish** page will appear and display what you've configured previously. If you want to modify any parameter, click **Back** to reconfigure it. If all are confirmed, click **Finish** to complete the configuration.



Chapter 4 Status Tab

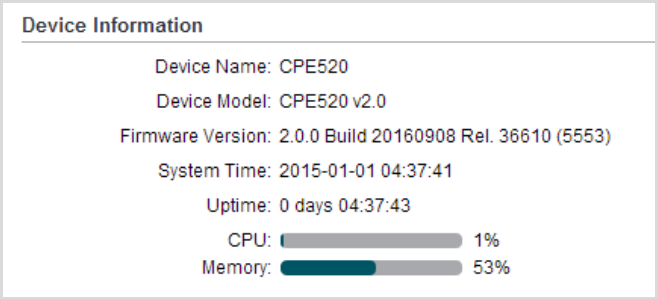
The **Status** tab displays a summary of the link status information, current values of the basic configuration settings (depending on the operating mode), network settings and information, and traffic statistics.



Status Information

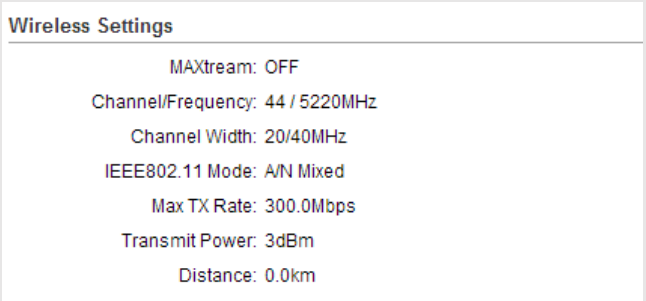
- **Device Information**

Device information displays the customizable name, model, firmware version, system time, uptime, CPU and memory of the device.



- **Wireless Settings**

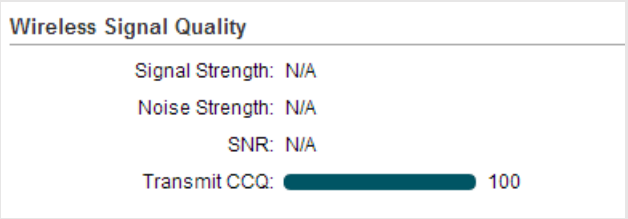
Wireless settings display the relative wireless parameters of the current device. You can change the parameters in **Wireless tab**.



MAXtream	Displays whether the MAXtream function is ON.
Channel/Frequency	Displays the channel number and corresponding operating frequency. The device uses the channel and radio frequency specified to transmit and receive data. Valid channel and frequency ranges will vary depending on local regulations.
Channel Width	Displays the spectral width of the radio channel used by the device.
IEEE802.11 Mode	Displays the radio standard used for operation of your device.
Max TX Rate	Displays the data rate at which the device should transmit wireless packets.
Transmit Power	Displays the current transmit power of the device.
Distance	Displays the wireless coverage distance where the client devices can be placed from the AP to get good wireless performance. You can change the value in **Wireless Advanced Settings**.

- **Wireless Signal Quality**

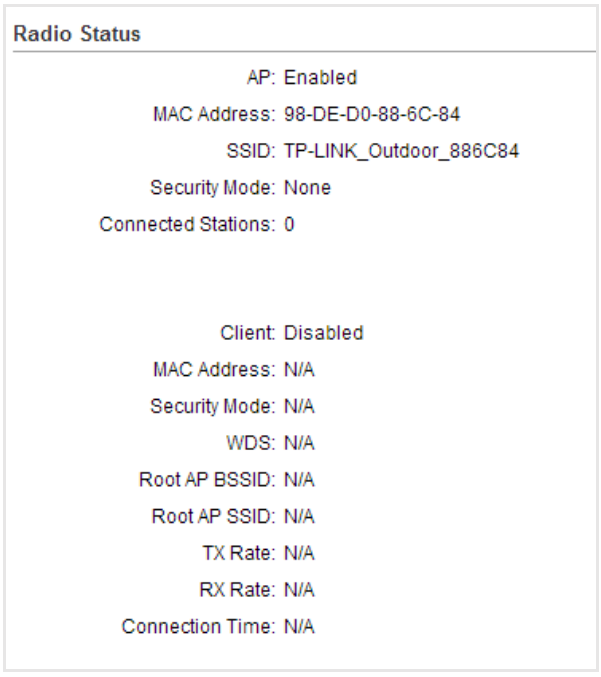
Status of wireless signal quality displays the parameters of the received wireless signal in the modes of Client, Repeater (Range Extender), Bridge and AP Client Router. The parameters here is not applicable for other two modes.



Signal Strength	Displays the received wireless signal strength of the root AP.
Noise Strength	Displays the received environmental noise from wireless interference on the operating frequency.
SNR	Signal to Noise Ratio, the power ratio between the received wireless signal strength and the environmental noise strength. Generally, in order to achieve the best performance, users need to adjust the antenna to get the best SNR.
Transmit CCQ	Displays the wireless Client Connection Quality (CCQ). CCQ refers to the ratio of current effective transmission bandwidth and the theoretically maximum available bandwidth. CCQ reflects the actual link condition.

- **Radio Status**

Radio status shows the MAC address, SSID, security mode and connected station number of the enabled AP. If the Client mode is enabled, the information of MAC address, security mode, WDS, root AP BSSID, root AP SSID, TX rate, RX rate and connection time of the client will also be displayed.

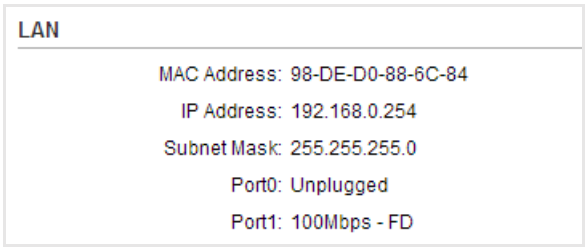


AP	Displays whether the AP function is Enabled or Disabled. It is enabled in Access Point, Repeater, Bridge, AP Router and AP Client Router modes and disabled in Client mode by default.
MAC Address	Displays the MAC address of AP interface or client interface.
SSID	Displays the wireless network name (SSID).
Security Mode	Displays the security mode you've chosen 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.
Connected Station	Displays the number of the connected stations.
Client	Displays whether the Client function is Enabled or Disabled. It is enabled in Client, Repeater, Bridge and AP Client Router modes and disabled in Access Point and AP Router modes by default.
WDS	Displays whether the Wireless Distribution System (WDS) is enabled or not.
Root AP BSSID	Displays the basic service set identification (MAC address) of root AP.
Root AP SSID	Displays the wireless network name of root AP.
TX Rate	Displays the data rate at which the device transmits wireless packets.
RX Rate	Displays the data rate at which the device receives wireless packets.

Connection Time	Displays the amount of time the device has been connected to the root AP.

- **LAN**

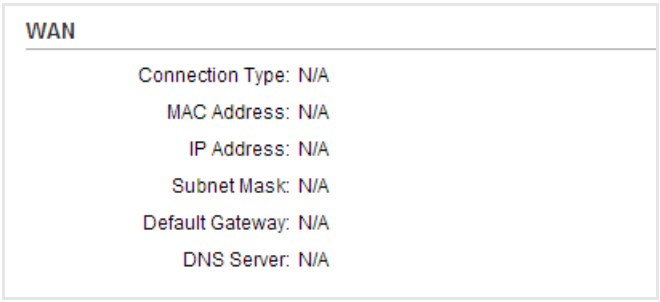
It displays the relative LAN parameters of the current device. You can change the parameters in **Network Tab**.



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

- **WAN**

It displays the relative WAN parameters of the current device. You can change the parameters in **Network Tab**.



Connection Type	Displays the WAN connection type of the device.
MAC Address	Displays the MAC address of the device's WAN port.
IP Address	Displays the IP address of the device's WAN port.
Subnet Mask	Displays the Subnet Mask of the WAN.
Default Gateway	Displays the default gateway.

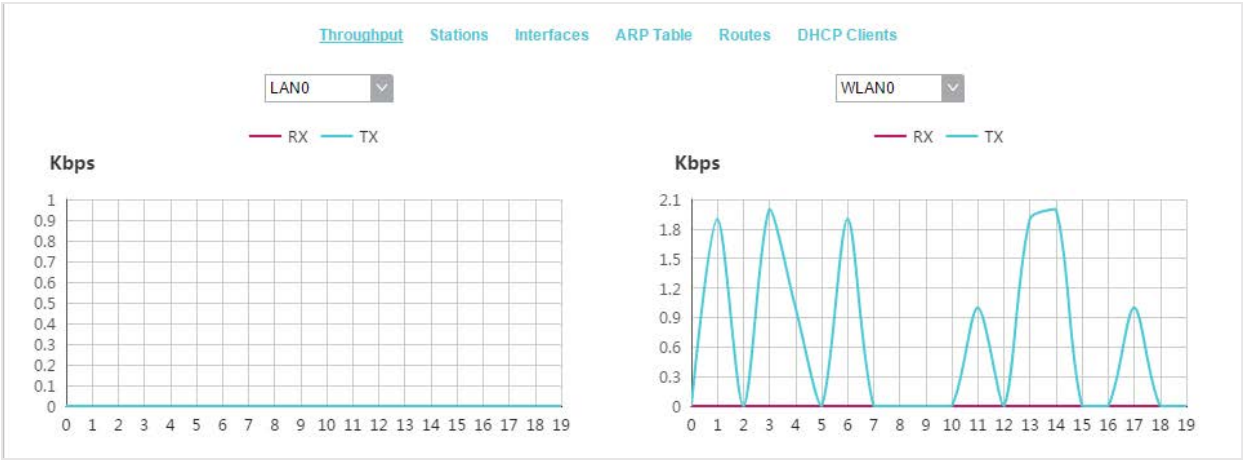
DNS Server	Displays the current DNS IP address.

Monitor

The monitor displays the data changes of throughput, Stations, Interfaces, ARP table, Routes, DHCP Clients and Dynamic WAN of the device.

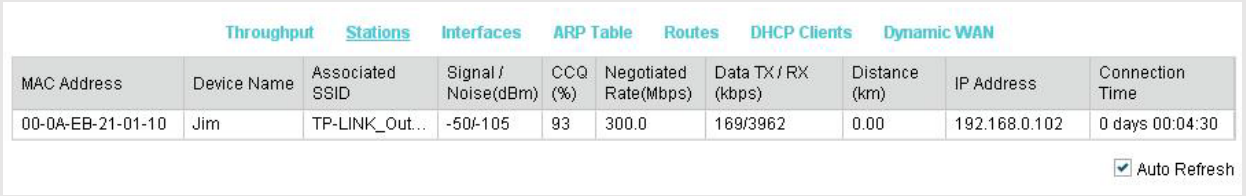
- **Throughput**

Throughput displays the current data traffic on the interfaces of LAN, WLAN and BRIDGE in both graphical and numerical form. You can choose the specific interface to monitor from the drop-down list above the chart.



- **Stations**

In the modes with the AP function enabled, you can monitor the information of all the stations that are connected to the device.

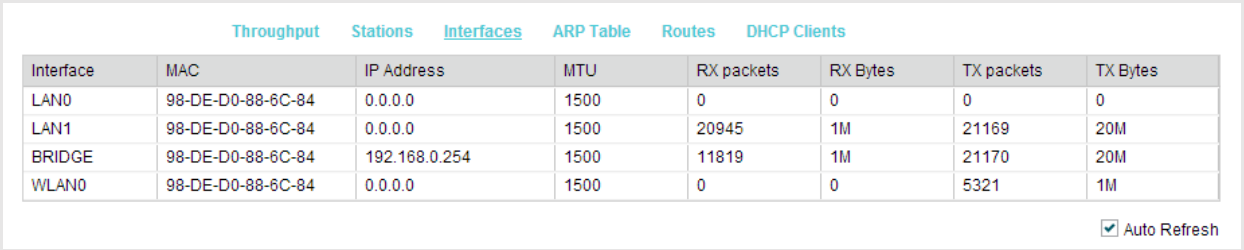


MAC Address	Displays the MAC address of the station.
Device Name	Displays the station's host name.
Associated SSID	The SSID that the station connected to.
Signal/Noise (dBm)	Signal to Noise Ratio, the power ratio between the received wireless signal strength and the environmental noise strength. Generally, in order to achieve the best performance, users need to adjust the antenna to get the best SNR.

CCQ (%)	Displays the wireless Client Connection Quality (CCQ) of the station.
Negotiate Rate (Mbps)	Displays the station's data rates of the last transmitted packets.
Data TX/RX (kbps)	Displays the station's average data rates of the transmitted and received packet over the connection time.
Distance (km)	Displays the distance between the station and the device.
IP Address	Displays the IP address of the station.
Connection Time	Displays the connection duration.
Auto Refresh	If **Auto Refresh** is checked, parameters in the table will refresh automatically.

- **Interfaces**

The table displays the relevant information of each interface including MAC, IP address, etc.



MAC	Displays the MAC address of the interface.
IP Address	Displays the IP address of the interface.
MTU	Displays the Maximum Transmission Unit (MTU), which is the maximum packet size (in bytes) that a network 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 transmitted by the interface after the device is powered on.
TX Byte	Displays the total amount of data (in bytes) transmitted by the interface after the device is powered on.

Auto Refresh	If **Auto Refresh** is checked, parameters in the table will refresh automatically.

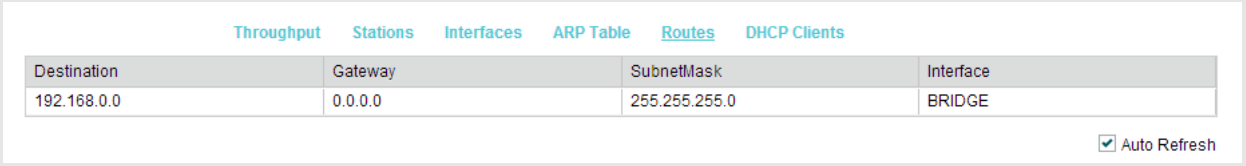
- **ARP table**

Lists all the entries of the Address Resolution Protocol (ARP) table currently recorded on the device. ARP is used to associate each IP address to the unique hardware MAC address of each device on the network.

IP Address	Displays the IP address assigned to a network device.
MAC	Displays the MAC address of the device.
Interface	Displays the interface that connects to the device.
Auto Refresh	If **Auto Refresh** is checked, parameters in the table will refresh automatically.

- **Routes**

List all the entries in the system routing table. PharOS examines the destination IP address of each data packet traveling through the system and chooses the appropriate interface to forward the packet to. Routing depends on static routing rules, which are registered in the system routing table. Static routes to specific hosts, networks, or the default gateway are set up automatically according to the IP configuration of all the Interfaces.

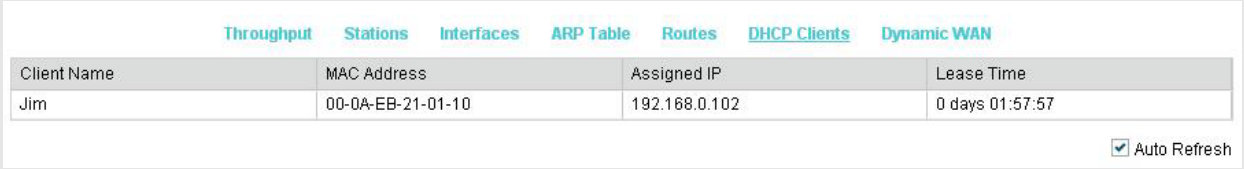


Destination	Displays the IP address of the destination device or destination network.
Gateway	Displays the IP address of the appropriate gateway.
Subnet Mask	Displays the Subnet Mask of the destination device.
Interface	Displays the interface that the destination device is on.

Auto Refresh	If **Auto Refresh** is checked, parameters in the table will refresh automatically.

- **DHCP Clients**

DHCP Clients display the current information of the clients including client names, MAC addresses, IP addresses assigned by the device's DHCP server and their lease time.



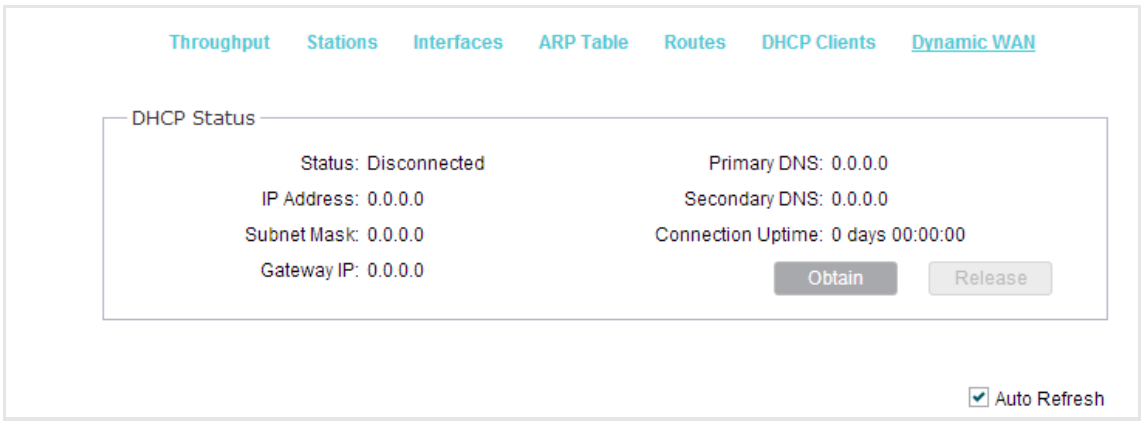
• **Client Name**	Displays the device name of the client.
• **MAC Address**	Displays the client's MAC Address.
• **IP Address**	Displays the IP address assigned to the client.
• **Lease Time**	Displays the time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.
• **Auto Refresh**	If **Auto Refresh** is checked, parameters in the table will refresh automatically.

- **Dynamic WAN**

NOTE:

This 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.

Dynamic WAN displays the WAN connection status of your device.



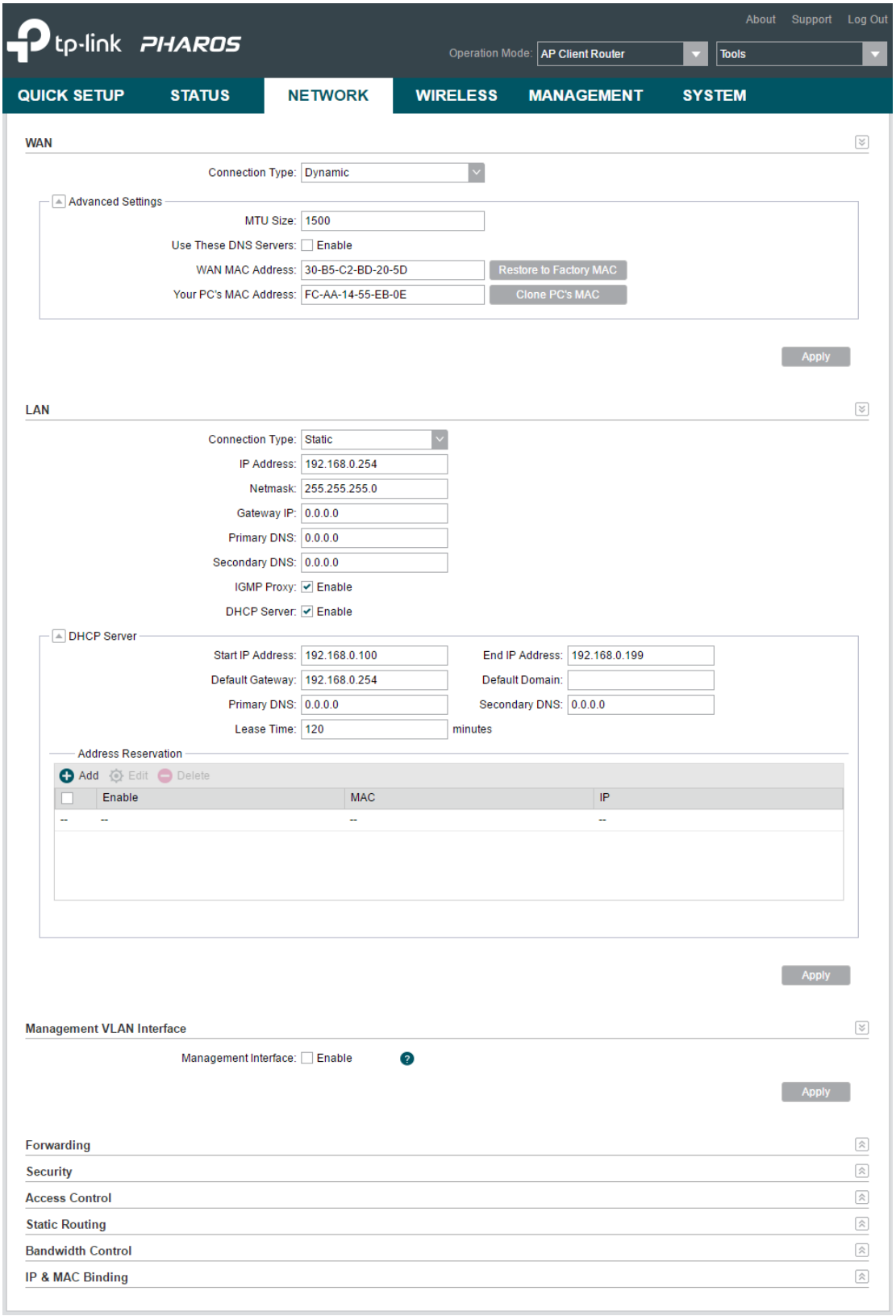
Status	Displays the WAN status is disconnected or connected.

IP Address	Displays the IP address of the WAN.
Subnet Mask	Displays the Subnet Mask of the WAN.
Gateway IP	Displays the address of the gateway.
Primary DNS/Secondary DNS	Displays the DNS IP address provided by your ISP.
Connection Uptime	Displays the time that the latest WAN connection lasts.
Auto Refresh	If **Auto Refresh** is checked, parameters in the table will refresh automatically.

Click **Obtain** to gain the WAN IP address from DHCP server, and click **Release** to release the WAN IP address.

Chapter 5 Network Tab

On **Network** Tab, you can configure the parameters of WAN, LAN, Management VLAN, Forwarding, Security, Access Control, Static Routing, Bandwidth control and IP&MAC Binding.

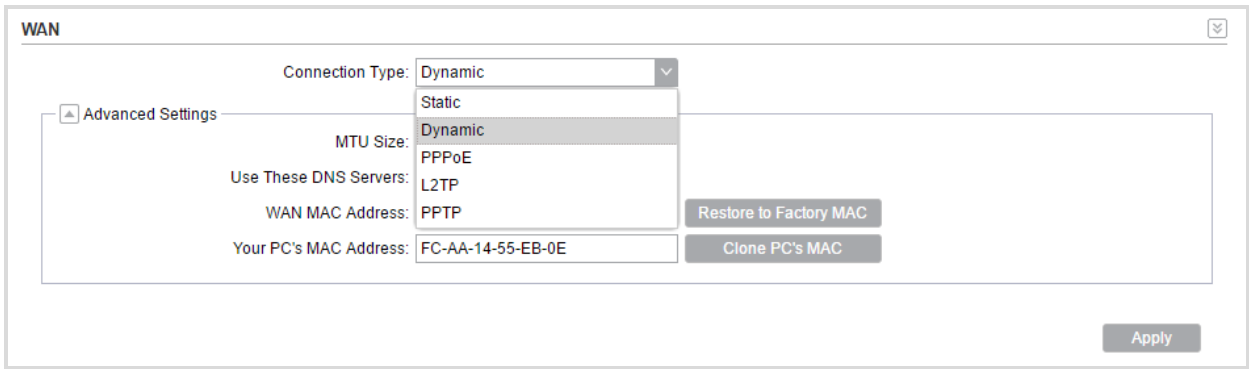


If you've made any change of the parameters, click **Apply** to make the configuration take effect. There will be a blue bar at the top of the page to remind you to save the configuration. Click **Save Changes** when you finish all settings, otherwise all the settings will be recovered to last saved settings at reboot or power off.

WAN

NOTE:

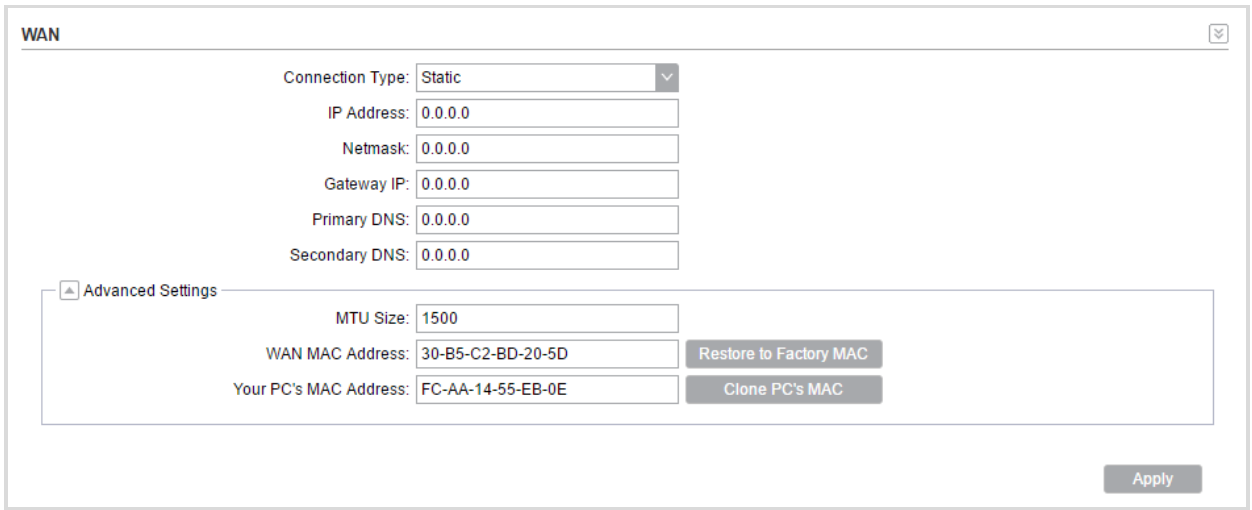
WAN submenu is only available on **AP router** mode and **AP client router (WISP Client)** mode.



There are five WAN connection types: Static, Dynamic, PPPoE, L2TP, and PPTP. Select the suitable one to configure the IP parameters of the WAN on the screen below. If you are not sure of the connection type, please consult your ISP.

- **Static**

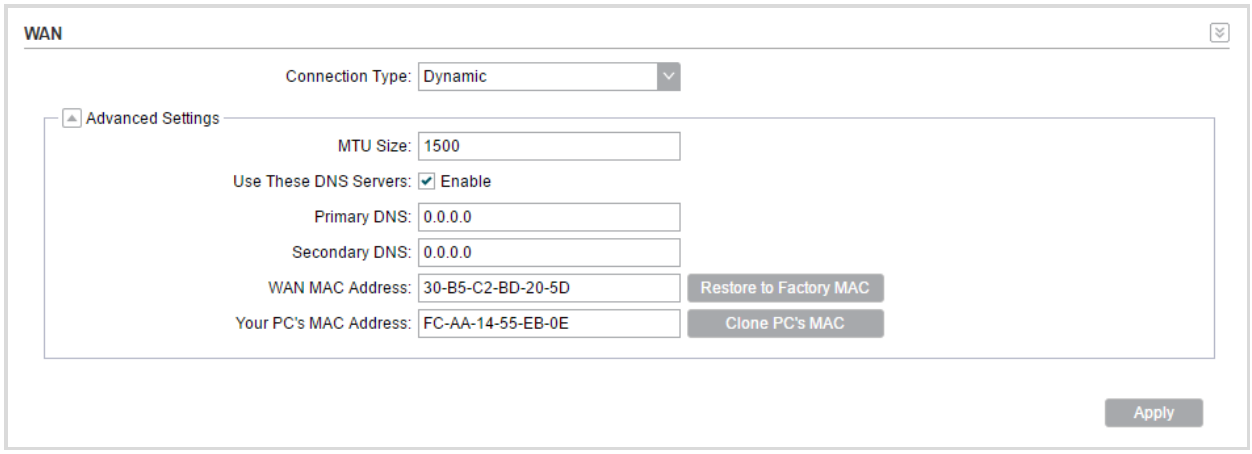
This connection type uses a permanent, fixed (static) IP address that your ISP assigned. In this type, you should fill in the IP address, Netmask, Gateway IP, and DNS IP address manually, which are specified by your ISP.



IP Address	Enter the IP address provided by your ISP.
Netmask	Enter the Netmask provided by your ISP. Normally use 255.255.255.0.
Gateway IP	Enter the gateway IP address provided by your ISP.
Primary DNS	Enter the DNS IP address provided by your ISP.
Secondary DNS	Enter alternative DNS IP address if your ISP provides.
MTU Size	The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
WAN MAC Address	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	This field displays the MAC address of the PC that is managing the router. Some ISPs require that you should register the MAC address of your PC. If the MAC address is required, you can click **Clone PC's MAC** to set the WAN MAC address the same as your management PC's MAC.

- **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.

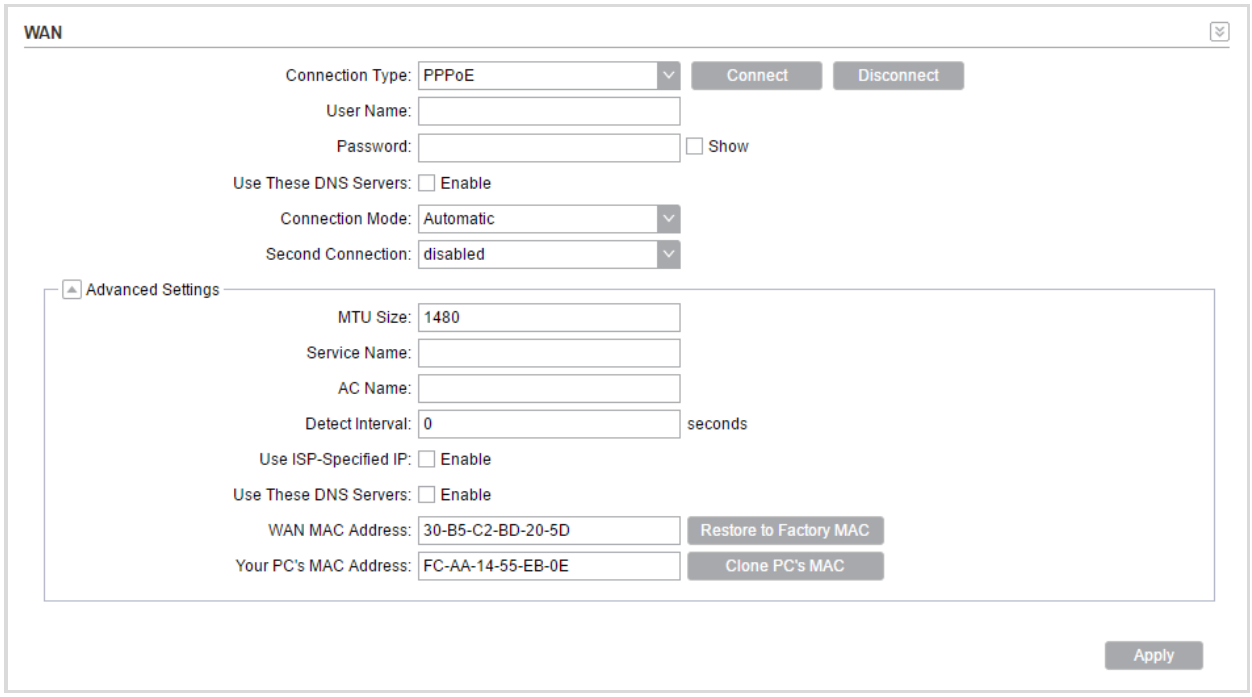


MTU Size	The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is

	necessary for your ISP connection.
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	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	This field displays the MAC address of the PC that is managing the router. Some ISPs require that you should register the MAC address of your PC. If the MAC address is required, you can click **Clone PC's MAC** to set the WAN MAC address the same as your management PC's MAC.

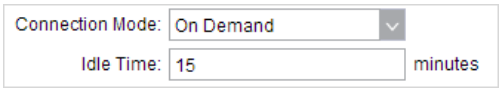
- **PPPoE**

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.



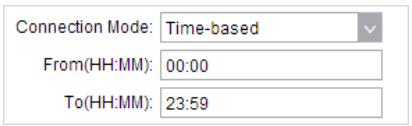
User Name/Password	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
User These DNS Servers	
Connection Mode	Please choose the Connection mode.

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

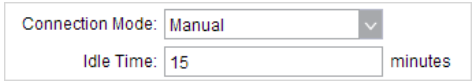


NOTE: Sometimes the connection cannot be disconnected although you specify a time to **Idle Time** (0~99 minutes) because some applications visit the Internet continually in the background.

- **Automatic -** Connect automatically after the device is disconnected. Users those are charged a flat monthly fee can choose this mode.
- **Time-based -** You can configure the device to make it connect or disconnect based on time. Enter the start time in ***From (HH:MM)*** for connecting and end time in ***To (HH:MM)*** for disconnecting. Users those need to control the time period of Internet access can choose this mode.



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

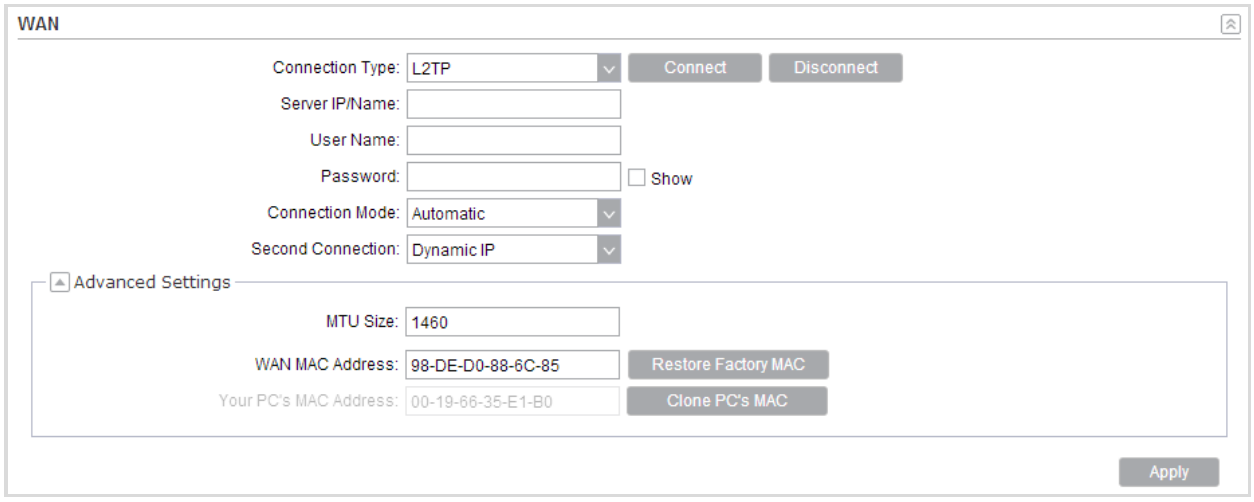


Secondary Connection	If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, you can activate this secondary connection. • **Disable -** The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended. • **Dynamic 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.
MTU Size	The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually appropriate. For some ISPs, you need modify the MTU. This should not be done unless your ISP told you to.
Service Name/AC Name	Do not change it unless your ISP told you to.
Detect Interval	The default value is 0. You can input the value between 0 and 120. The device will detect Access Concentrator online every interval seconds. If the value is 0, it means not detecting.
Use ISP-Specified IP	If your service provider give you an IP address along with the user name and password, **Enable** "Use ISP-specified IP" and enter the IP address, which is provided by your ISP.
Use These DNS Servers	If the ISP specifies 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	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	This field displays the MAC address of the PC that is managing the router. You can click **Clone PC's MAC** to set the WAN MAC address the same as your management PC's MAC.

Click **Connect** to connect immediately. Click **Disconnect** to disconnect immediately. You can check and control the status of WAN connection on **Monitor > Dynamic WAN** page**.**

- **L2TP/PPTP**

The configuration steps of these two WAN connections are the same. Take L2TP as an example to introduce.



Server IP/Name — Enter the server IP address or the domain name given by your ISP.

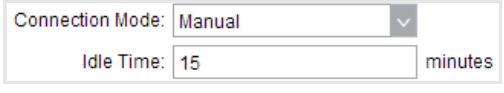
User Name/Password — Enter the *User Name* and *Password* provided by your ISP. These fields are case-sensitive.

Connection Mode

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

NOTE: Sometimes the connection cannot be disconnected although you specify a time to **Idle Time** (0~99 minutes) because some applications visit the Internet continually in the background.

- **Automatic -** Connect automatically after the device is disconnected. Users those are charged a flat monthly fee can choose this mode.
- **Manual -** You can configure the device to make it connect or disconnect manually. After a specified period of inactivity (**Idle Time**), the device will disconnect your Internet connection, and you must click **Connect** manually to access the Internet again. If you want your Internet connection to remain active all the times, enter **0** in the *Idle Time* field. Otherwise, enter the desired Idle Time in minutes you wish to use. Users those pay by time for their Internet access can choose this mode to save their Internet-access fee.

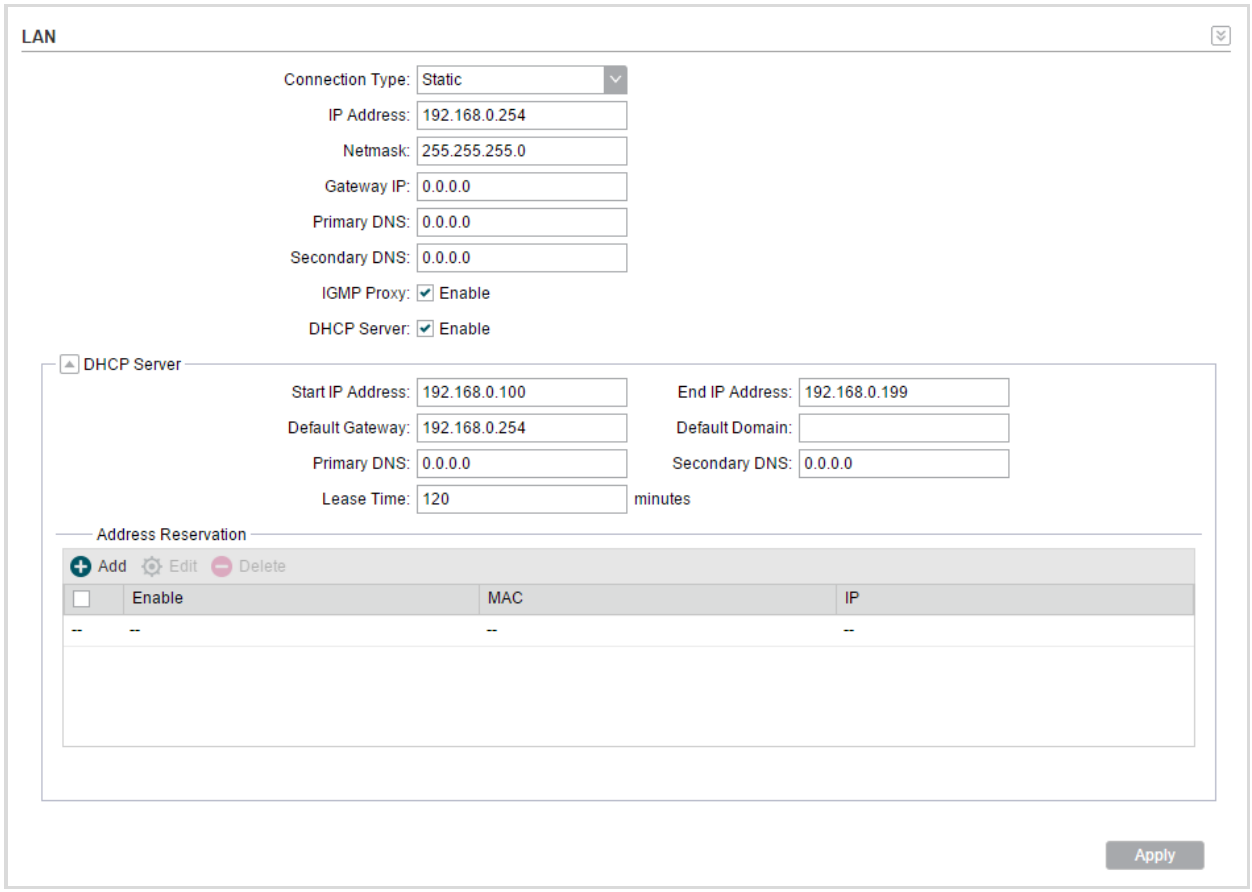


Secondary Connection	If your ISP provides a Connection type such as Dynamic/Static IP to connect to a local area network, you can activate this secondary connection. • **Dynamic -** Use dynamic IP address to connect to the local area network provided by ISP. • **Static -** Use static IP address to connect to the local area network provided by ISP.
MTU Size	The default MTU (Maximum Transmission Unit) size is 1460 bytes in L2TP and 1420 bytes in PPTP, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
WAN MAC Address	This field displays the current MAC address of the WAN port, which is used for 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	This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click **Clone PC's MAC** to set the WAN MAC address the same as your management PC's MAC.

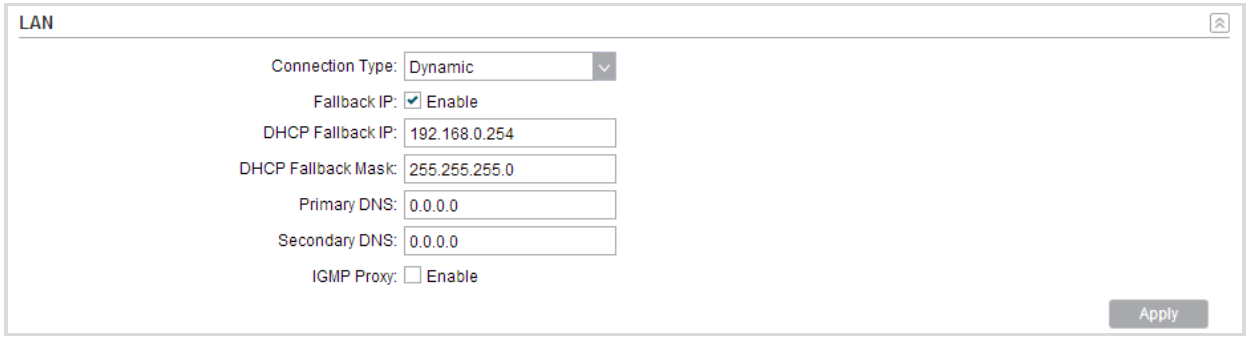
Click **Connect** to connect immediately. Click **Disconnect** to disconnect immediately. You can check and control the status of WAN connection on **Monitor > Dynamic WAN** page**.**

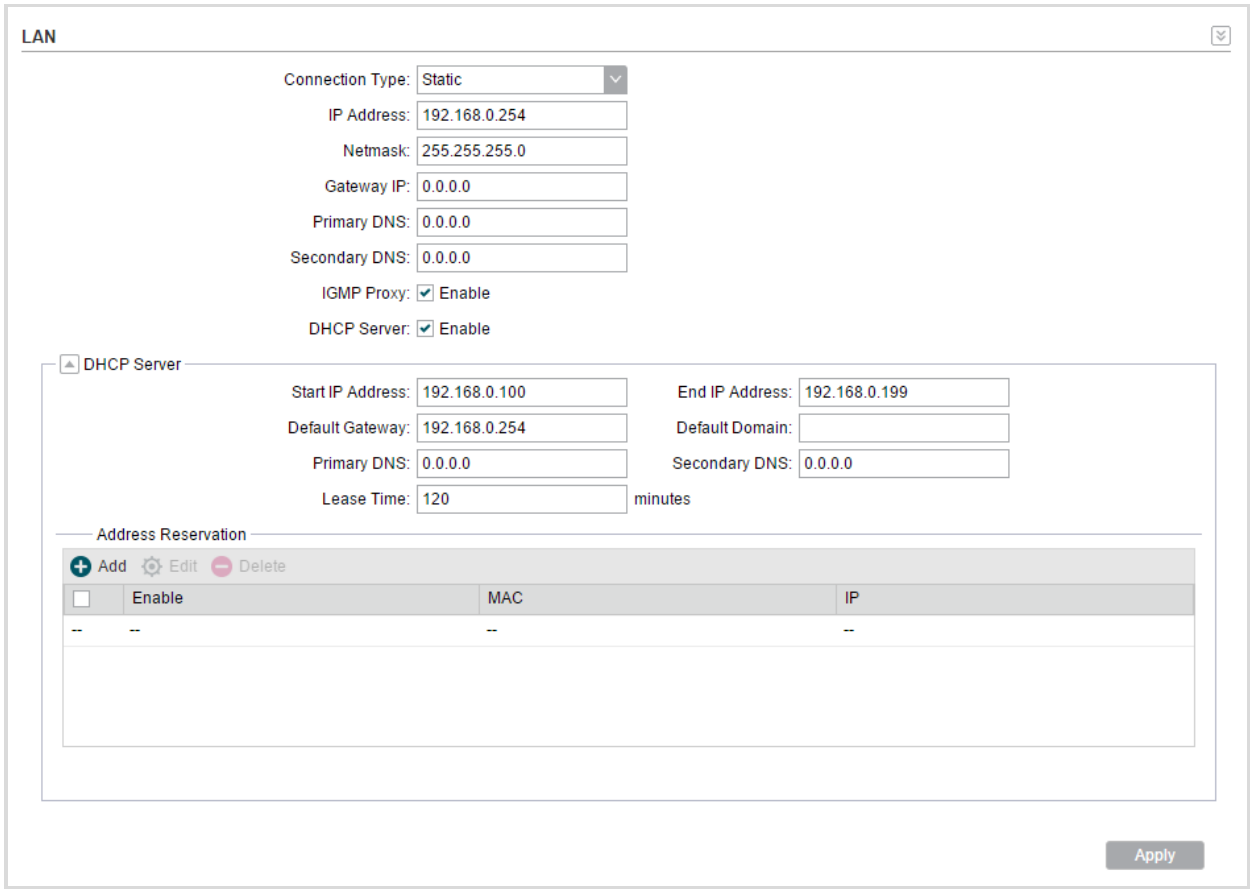
LAN

The display of this submenu is different in modes. The page of **AP router** mode and **AP client router (WISP Client)** mode is shown as below. In these two modes, static is the only one connection type.



While the page of **Access Point** mode, **Client** mode, **Repeater (Range extender)** mode and **Bridge** mode is shown as below. There are two connection types including dynamic and static.



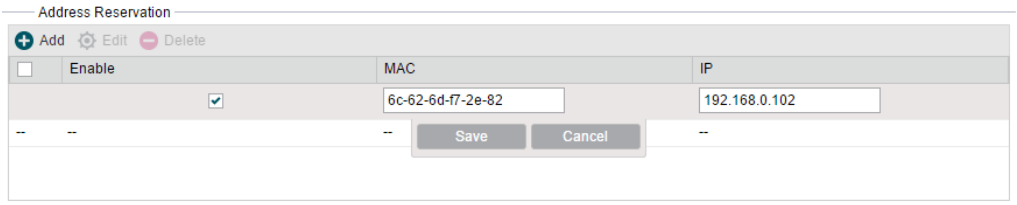


Connection type	There is only one LAN Connection type **Static** in AP Router mode and AP Client Router (WISP Client) mode. While there are **Static** and **Dynamic** of Connection types in Access Point mode, Client mode, Repeater (Range Extender) mode and Bridge mode.
IP Address	Enter the IP address of your AP/router (factory default: 192.168.0.254).
Netmask	Enter the Netmask provided by your ISP. Normally use 255.255.255.0 as the netmask.
Gateway IP	Enter the IP address of the gateway for your device.
Primary DNS	Enter the primary DNS IP address provided by your ISP. Please consult your ISP if you don't know the DNS value. The factory default setting is 0.0.0.0.
Secondary DNS	Enter the secondary DNS IP address of alternative DNS server if your ISP two DNS servers. The factory default setting is 0.0.0.0.
IGMP Proxy	IGMP (Internet Group Management Protocol) works for IPTV multicast stream. If you want to watch IPTV, **Enable** it.
DHCP Server	If the built-in DHCP server is expected to assign IP addresses to clients connected to the wireless interface and LAN interface, **Enable** it.

Fallback IP	When Dynamic IP is selected as the connection type, you can enable this function. The fallback IP will be used as the LAN IP when a DHCP server is not found.
DHCP Fallback IP	Specify the IP address for the device to use if a DHCP server is not found.
DHCP Fallback Mask	Specify the mask for the device to use if a DHCP server is not found.
Start IP Address	This field specifies the first address in the IP Address pool. 192.168.0.100 is the default start IP address.
End IP Address	This field specifies the last address in the IP Address pool. 192.168.0.199 is the default end IP address.
Default Gateway	Enter the IP address of the gateway for your LAN. The factory default setting is 192.168.0.254.
Default Domain	Enter the domain name of your DHCP server. You can leave the field blank.
Primary DNS	Enter the DNS IP address for the LAN. The factory default setting is 0.0.0.0.
Secondary DNS	Enter the IP address of alternative DNS server if there are two DNS servers. The factory default setting is 0.0.0.0.
Lease Time	Enter the amount time of the leased IP address assigned by the DHCP server. Before the time is up, DHCP client will request to renew the lease automatically and DHCP server would not assign this IP address to other clients.

Address Reservation

Address Reservation will enable you to 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 Reserve IP addresses:

Click **Add** in the table of Address Reservation.

Enter the ***MAC address*** in the format of XX-XX-XX-XX-XX-XX and the ***IP address*** in dotted-decimal notation of the station you want to add.

Click **Save** after finishing the configuration.

Select the added entries, you can edit or delete them.

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 for the switches on the network to ensure the communication between the host and the device in the management VLAN.

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

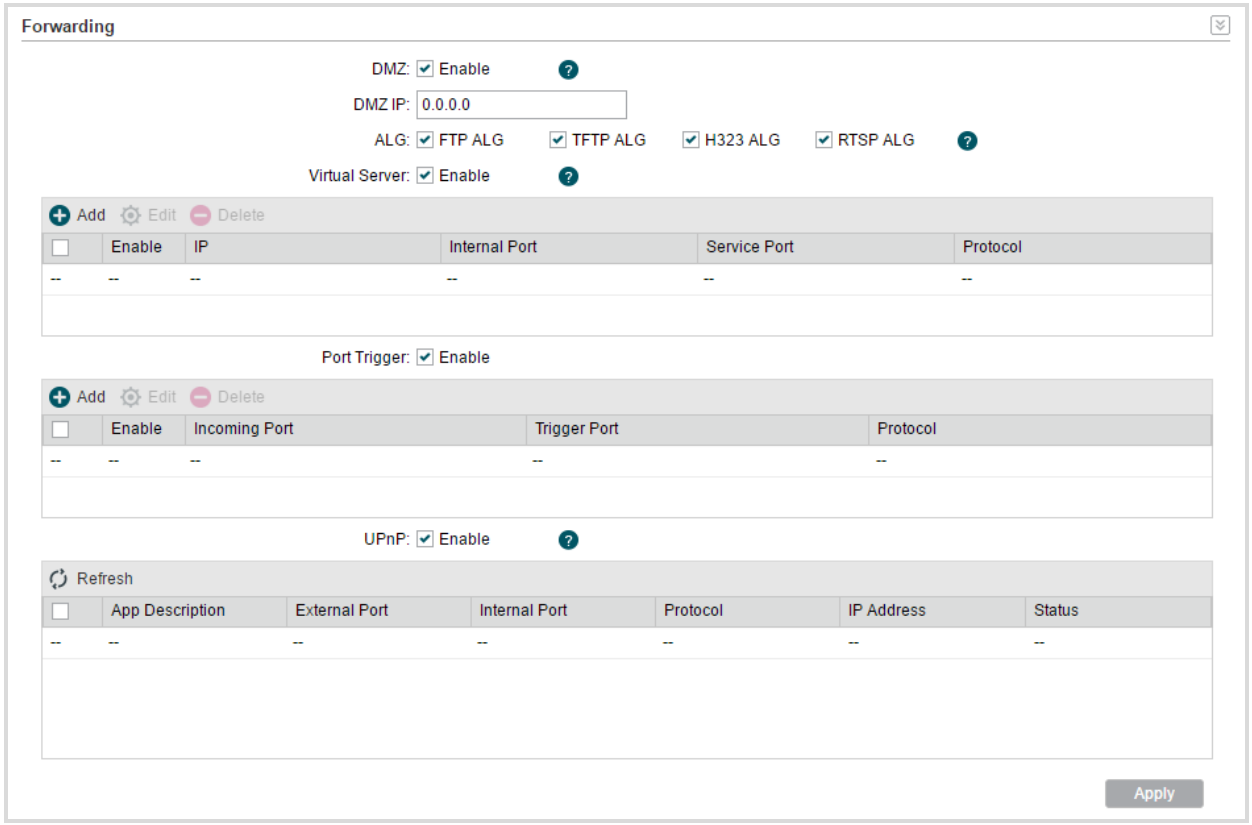
Forwarding

The Forwarding feature is available only 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.



DMZ	Check the **Enable** box to use 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

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

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

To use the virtual server:

Click **Add** in the table of Virtual Server.

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

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.

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.

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

Click **Save** after finishing the configuration.

Select the added entries, you can edit or delete them.

Port Trigger

Check the **Enable** box to use the port trigger function. 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.

Once configured, operation is as follows:

A local host makes an outgoing connection to an external host using a destination port number defined in the ***Trigger Port*** field.

The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.

When necessary the external host will be able to connect to the local host using one of the ports defined in the ***Incoming Port*** field.

To use the port trigger:

Click **Add** in the table of Port Trigger.

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.

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

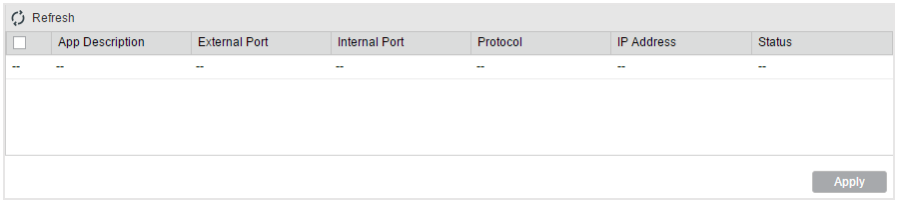
Choose the one of the protocols used for this application: TCP, UDP, or TCP/UDP.

Click **Save** after finishing the configuration.

Select the added entries, you can edit or delete them.

UPnP

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

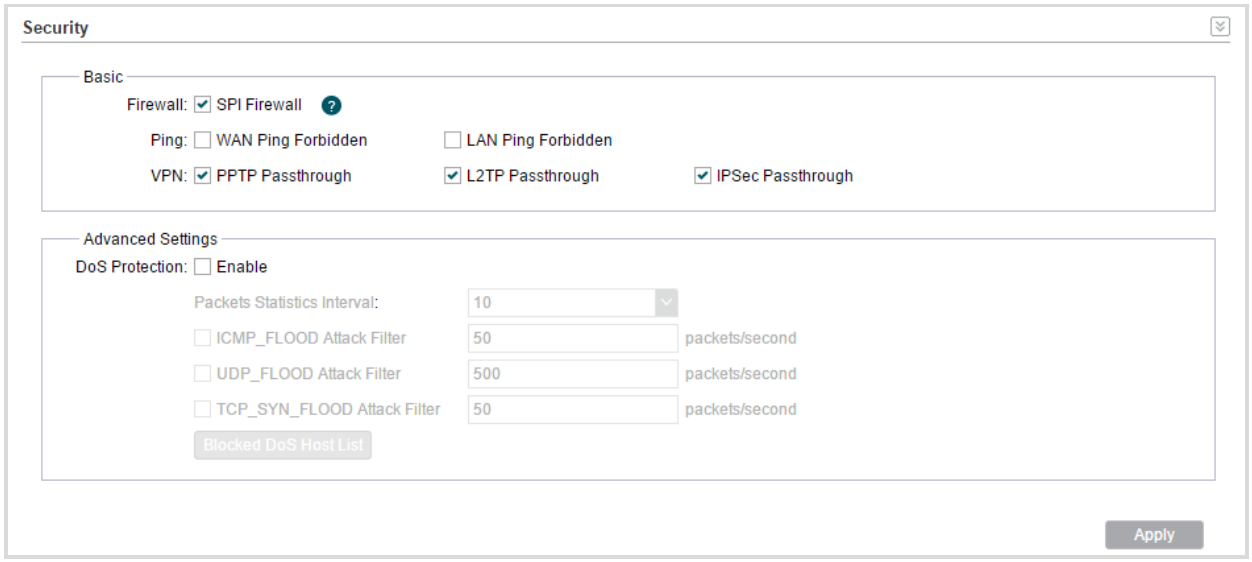


- **App Description** – Displays the description provided by the application in the UPnP request.
- **External Port** – Displays the external port number that the router opened for the service application.
- **Protocol** - Displays which type of protocol is opened.
- **Internal Port** – Displays the internal service port number of the local host running the service application.
- **IP Address** - Displays the IP address of the local host which initiates the UPnP request.
- **Status** - **Enabled** means that port is still active. Otherwise, the port is inactive.

Security

The **Security** function is available only 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.



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	• **WAN Ping Forbidden**: The default setting is disabled. If enabled, the device will not reply the ping request originates from Internet. • **LAN Ping Forbidden**: The default setting is disabled. If enabled, the device will not reply the ping request originates from local network.

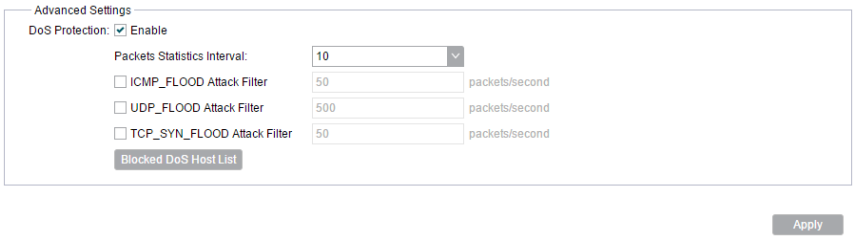
VPN

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.

DoS Protection

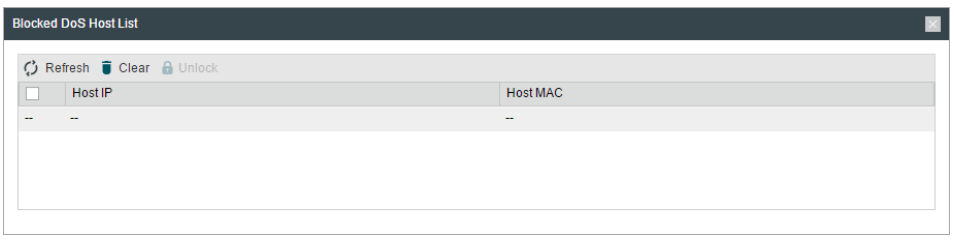
DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host, which incurs an abnormal service or even breakdown of the network. With DoS Protection function enabled, the device can analyze the 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**.



Access Control

The function of **Access Control** is available only 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.

Access Control	Check the **Enable** box to use the access control function.

Filtering Policy

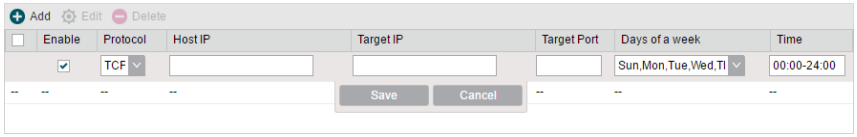
There are two filtering policies to control the Internet activities:

- 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.



To use the access control:

Click **Add** in the table to create control rules.

Choose one of the protocols from the drop-down list used for the target, any of IP, TCP, UDP, or ICMP.

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.

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.

Specify the port or port range for the target when protocol is TCP or UDP.

Select the certain day (days) for the rule.

Enter the time rule in HH:MM-HH:MM format, the default value is 00:00-24:00.

Click **Save** after finishing the configuration.

Select the added entries, you can edit or delete them.

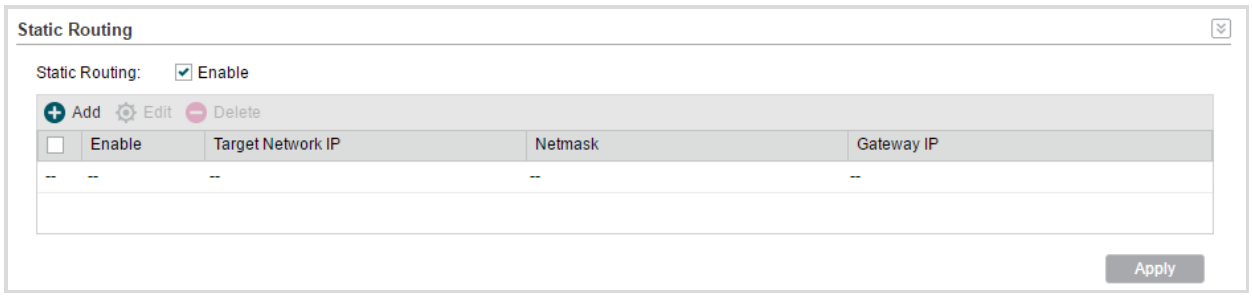
Static Routing

The function of **Static Routing** is available only 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.

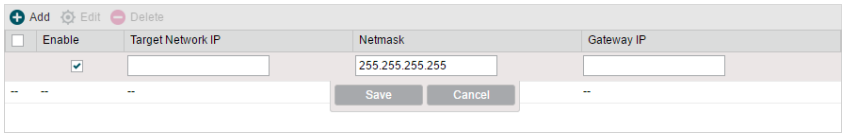
Static routing is generally suitable for simple network environment, in which users clearly understand the topology of the network so as to set the routing information correctly. When the

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.



Static Routing

Check the **Enable** box to use the static routing function.



To use the static routing:

Click **Add** to create a new static routing.

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.

Enter the ***Netmask***.

Enter the ***Gateway IP***, the address of the gateway that allows for contact between the Device and the network or host.

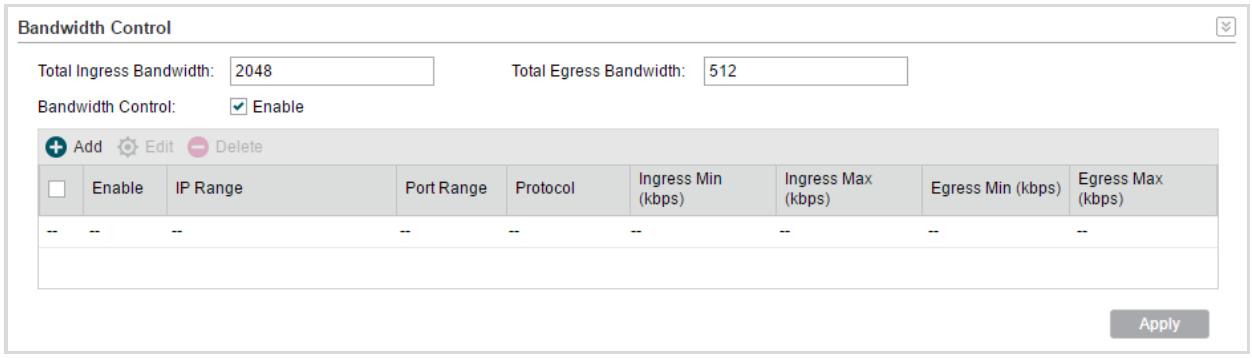
Click **Save** after finishing the configuration.

Select the added entries, you can edit or delete them.

Bandwidth Control

The function of **Bandwidth Control** is available only in **AP router** mode and **AP client router (WISP Client)** mode.

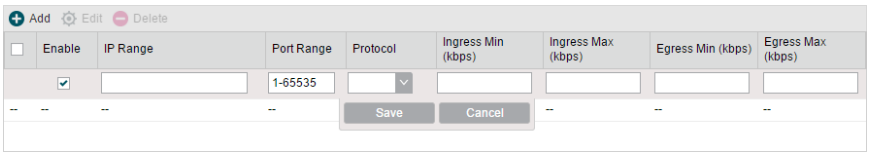
Bandwidth control function is used to control the Internet bandwidth in the local area network. In the case of insufficient bandwidth resources, enable the function to make the device allocate reasonable bandwidth to the clients and achieve the purpose of efficient use of the existing bandwidth. Via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



Total Ingress Bandwidth — The total download speed limited through the WAN port. The maximum value is 100,000kbps.

Total Egress Bandwidth — The total upload speed limited through the WAN port. The maximum value is 100,000kbps.

Bandwidth Control — Check the **Enable** box to use the bandwidth control function.



To use the bandwidth control:

Click **Add** in the table of bandwidth control.

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.

Enter the ***Port Range*** through which the target hosts visit external server, for example 1-63258.

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

Enter the minimum ingress, maximum ingress, minimum egress and maximum egress of these IP addresses.

Click **Save** after finishing the configuration.

Select the added entries, you can edit or delete them.

IP&MAC Binding

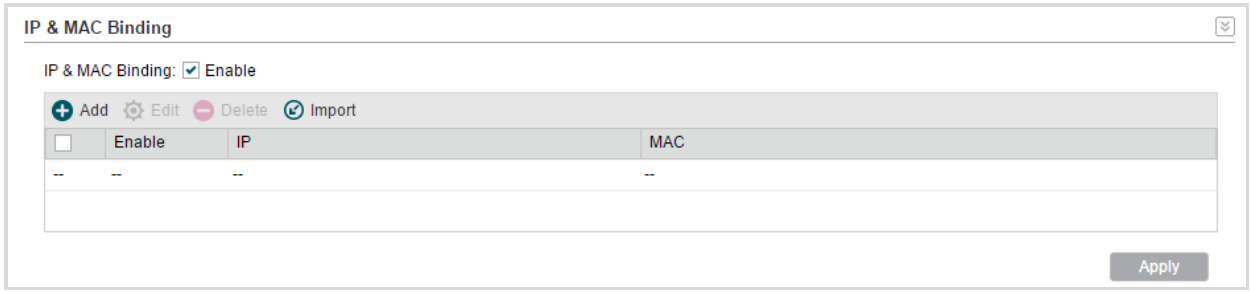
We can effectively prevent ARP attack and IP embezzlement by enabling the IP&MAC binding. Within the local network, the device transmits IP packets to the certain target identified by the MAC address. Therefore, the IP and MAC address should be one-to-one correspondence and their corresponding relations are maintained by the ARP table. ARP attack can use forged information to renewal the ARP table, and destroy the corresponding relations between IP and MAC addresses, which would prevent the communication between the device and the

corresponding host. When the IP&MAC Binding function is enabled, the IP and MAC relations in the ARP table won't be expired and renewed automatically, which effectively prevents the ARP attack.

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

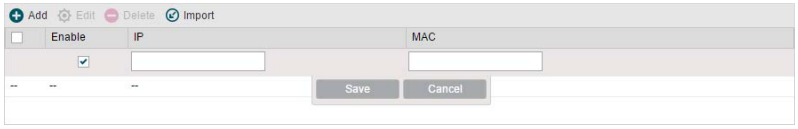
NOTE:

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



IP&MAC Binding

Check the **Enable** box to use the IP&MAC binding function.



To use the IP&MAC Binding:

Click **Add** in the table of IP&MAC binding.

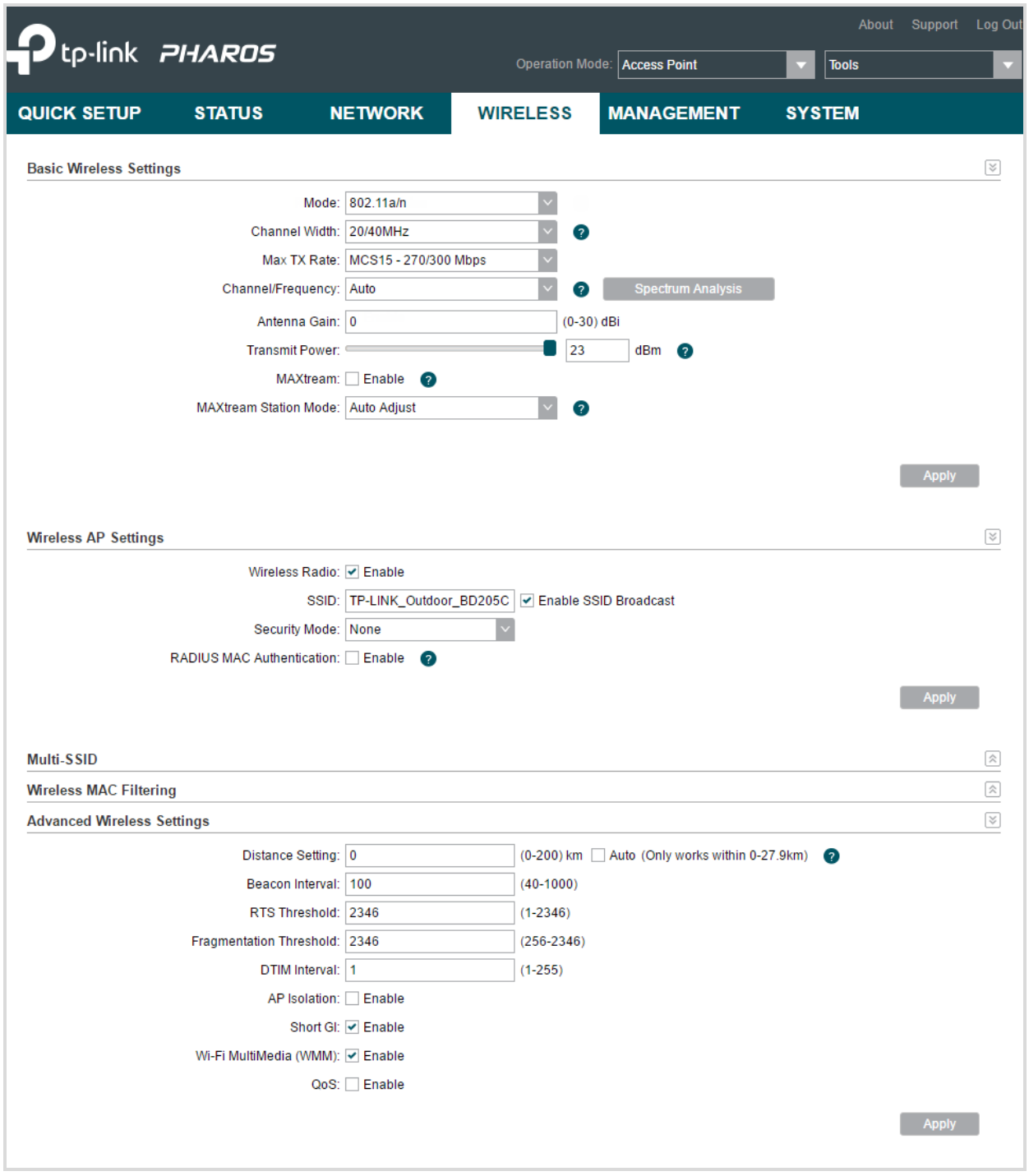
Enter the ***IP*** address and ***MAC*** address that you want to bind, for example 192.168.0.12, 00-23-5A-15-99-42. The new added entry is enabled by default.

Click **Save** after finishing the configuration.

Select the added entries, you can edit or delete them. Click **Import** to import all the entries in **Monitor > ARP Table.** The imported entries are disabled by default. You can select the certain entry and click **Edit** to enable it.

Chapter 6 Wireless Tab

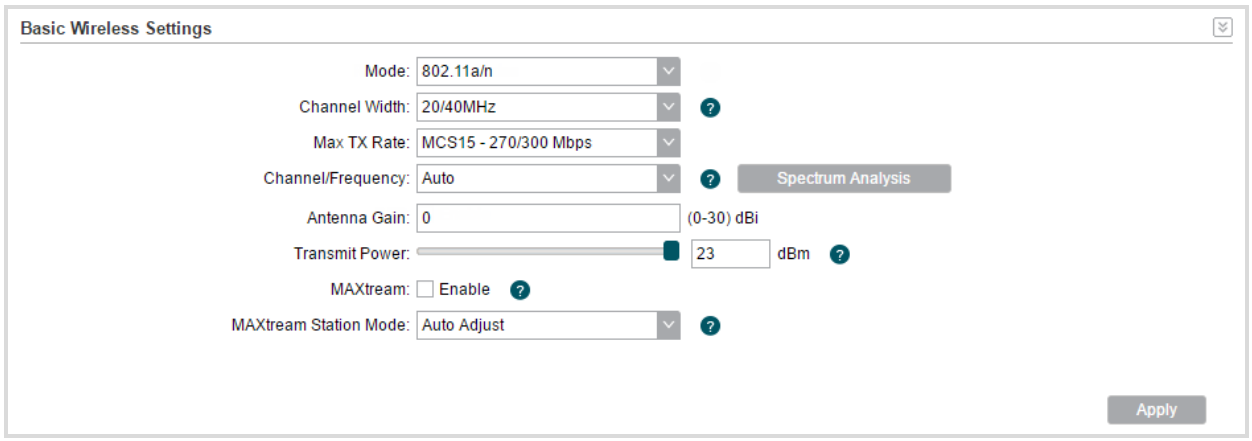
On **Wireless** Tab, you can configure the related wireless parameters in different modes. Please selectively read the details according to the working mode of your device.



If you have made any change of the parameters, click **Apply** to make the configuration take effect. There will be a blue bar at the top of the page to remind you to save the configuration. Click **Save Changes** when you finish all settings, otherwise all the settings will be recovered to last saved settings at reboot or power off.

Wireless Basic Settings

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



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. You are recommended to set the 11b/g/n mixed mode, and all of 802.11b, 802.11g and 802.11n wireless stations can connect to the device. CPE610/CPE510/CPE520/WBS510 has a frequency band of 5GHz, supporting 802.11a, 802.11n and 802.11a/n modes. We suggest to set in 11a/n mode, allowing both 802.11a and 802.11n wireless stations to access the device.

Channel Width	Select the channel width of this device. Options include 5MHz, 10MHz, 20MHz and 20/40MHz (this device automatically selects 20MHz or 40MHz, and 20MHz will be used if 40MHz is not available). Users select corresponding channel width according to whether their devices support it. According to IEEE 802.11n standard, using a channel width of 40MHz can increase wireless throughput. However, users may choose lower bandwidth due to the following reasons: Increase the available number of channels within the limited total bandwidth. To avoid interference from overlapping channels occupied by other devices in the environment. Lower bandwidth can concentrate higher transmit power, increasing stability of wireless links over long distances. Subject to the channel width of root AP in Client/ Bridge/ Repeater/ Client Router operation modes.
Max TX Rate	Set the maximum transmit data rate.
Channel/Frequency	Select the channel used by this device to improve wireless performance. 1/2412MHz refers to Channel 1 and the frequency is 2412MHz. This setting is only available in the modes of Access Point and AP Router. CPE210/CPE220/WBS210 is a device with a frequency of 2.4GHz and CPE610/CPE510/CPE520/WBS510 has a frequency of 5GHz. We highly recommend you use the **Spectrum Analysis** tool to select a proper channel.
Antenna Gain	Antenna Gain is only available in the page of WBS products. Enter the antenna gain value according to the antennas and the value ranges from 0 to 30dBi.
Transmit Power	You can use the slider or manually enter the transmit power value. For WBS210 and WBS510, the maximum transmit power varies according to the antenna gain value. ***NOTE***: In most cases, it is unnecessary to select maximum transmit power. Selecting larger transmit power than needed may cause interference to neighborhood. Also it consumes more power and will reduce longevity of the device. Select a certain transmit power is enough to achieve the best performance. You can use the **Speed Test** tool to find the best performance.

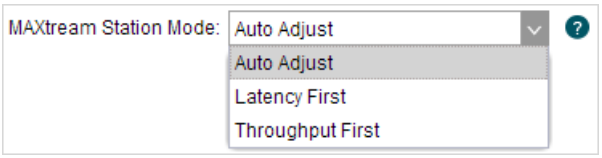
MAXtream

This setting is only available in the modes of Access Point and AP Router. MAXtream is a proprietary technology of TP-Link for Wi-Fi system. It is based on TDMA (Time Division Multiple Access) so that data streams are transmitted in strict order. **MAXtream** aims to maximize throughput and minimize latency especially in a multi-STAs circumstance. "Hidden nodes" problem can also be eliminated with MAXtream enabled. We highly recommend you turn on MAXtream in a large scale wireless deployment to achieve better performance.

NOTE: MAXtream Technology is only compatible with Pharos series products. You cannot connect other Wi-Fi devices to an AP with MAXtream enabled.

MAXtream Station Mode

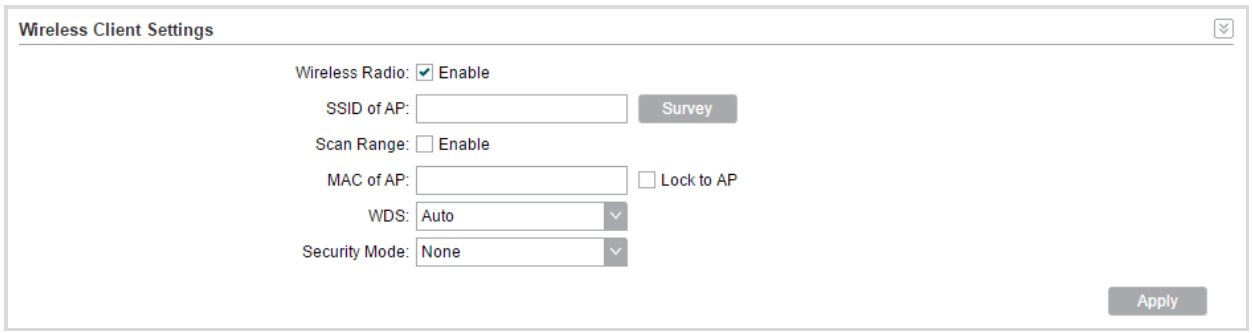
This setting is available in Client and Bridge mode and in the AP Client Router mode when the wireless AP settings is disabled.



For client devices connected to a root AP with MAXtream enabled, you can choose "Latency First" or "Throughput First" mode to better fit your application. For example, VoIP has a high demand for low latency. If you need a good experience for VoIP, you can select **Latency First**. Games and downloads ask for high throughput. You should select **Throughput First** to guarantee the high throughput for the games and downloads. Please choose **Auto Adjust** if you are not sure or you have no special requirements.

Wireless Client Settings

When this device is configured in the modes of Client, Repeater, Bridge and AP Client Router, the function of wireless client settings is available.



SSID of AP

You can enter the SSID of the specific AP manually to connect to it or directly survey all the APs around by clicking **Survey**.

Scan Range	Check the **Scan Range** box and enter the scan range to make the device survey in the specified frequency range.
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. **Lock to AP** can make the device connect to the specified AP you had connected before the next time.
WDS	WDS (Wireless Distribution System) is a communication system among multiple wireless local area networks established between APs through wireless connection. In this system, only data frames with four address fields can be transparently forwarded at the link layer. In a WDS network, it is necessary that the root AP supports forwarding of data frames four address fields. If not, only data frames with the ARP/IP/PPPOE protocol can be forwarded among APs. • **Enable** – Forward data frames to use four address fields. • **Disable** – Forward data frames to use three address fields. • **Auto** – The system automatically detects whether root device supports data frames with the format of three/four address fields, giving priority to the format of four address fields. The selection of Auto is recommended.
Security Mode	Select the security mode of this device. To access the wireless network of root AP, the security mode should be set the same as that of root AP. • **None** - Select this option if the root AP has no encryption. At the moment, it's no need to enter a password to access the wireless network of root AP. • **WPA-PSK** - Select this option if the security mode of the root AP is WPA-PSK. Enter the parameters including the version and encryption of WPA and PSK key, which must coincide with those of the root AP. • **WPA** – Select this option if the security mode of the root AP is WPA. Enter the parameters including the version, encryption, authentication, Phase 2 authentication, WPA user name and WPA user password, which must coincide with those of the root AP. • **WEP** - Select this option if the security mode of the root AP is WEP. Enter the parameters including authentication type, key format and WEP key, which must coincide with those of the root AP.

Wireless AP Settings

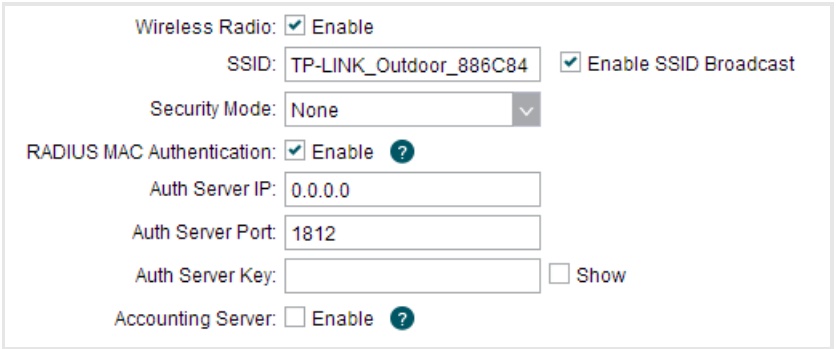
Wireless AP settings are only available in the modes of Access Point, Bridge, AP Router, and AP Client Router.

Wireless Radio	Check the **Wireless Radio** box to enable this device to send and receive the wireless signal.
SSID	Enter a character string no more than 32 characters to name your wireless network. The default SSID is TP-Link_Outdoor_xxxxxx (xxxxxx is the last six characters of the MAC address of this device). We suggest you to set an easy-to-remember SSID to conveniently identify your wireless network.
Enable SSID Broadcast	With this option checked, AP will broadcast its SSID to hosts in the surrounding environment, as thus hosts can find the wireless network identified by this SSID. If SSID Broadcast is not enabled, hosts must enter the AP's SSID manually to connect to this AP.
Security Mode	Select the security mode of wireless network. This device provides four security modes: None, WPA (Wi-Fi Protected Access), WPA-PSK (WPA Pre-Shared Key) and WEP (Wired Equivalent Privacy). WPA-PSK is recommended. Settings vary in different security modes as the details in the following introduction.

Security Mode

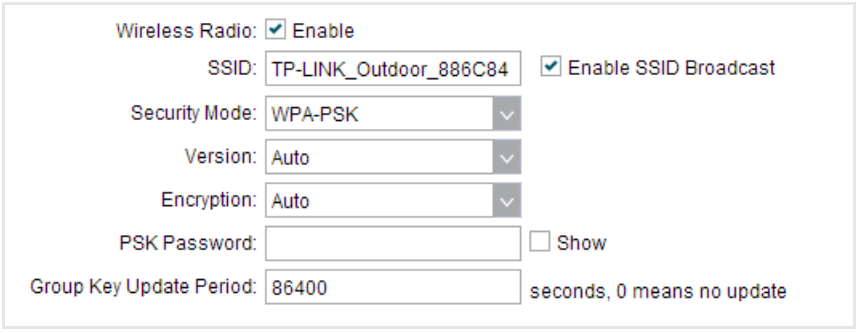
You can select one of the following security modes:

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



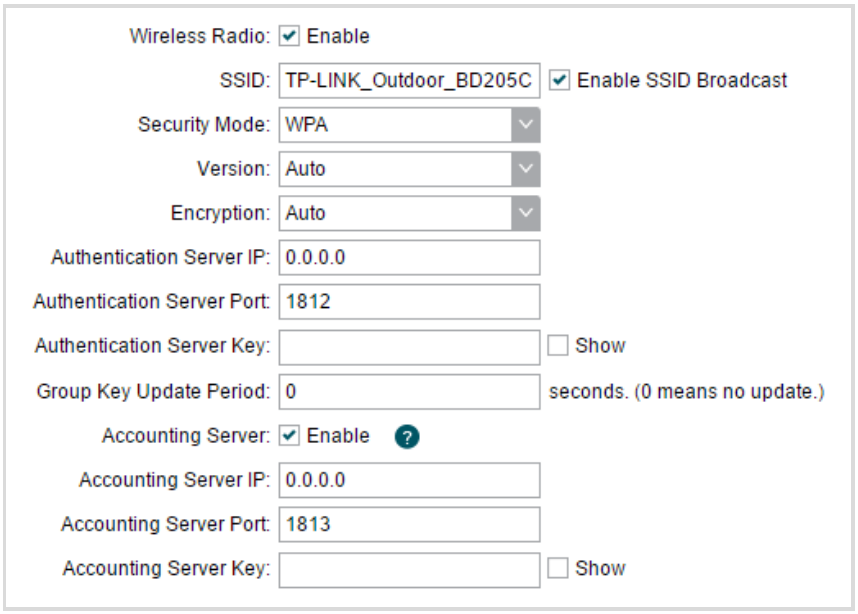
RADIUS MAC Authentication	With this option checked, you can authenticate clients using their MAC addresses on your RADIUS authentication server. Remember to log into your RADIUS authentication server and create authentication entries whose username and password are both the access-enabled clients' MAC 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. The shared key characters will be shown if you check the box of **show**.
Accounting Server	With this option checked, 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 the default, 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. The shared key characters will be shown if you check the box of **show**.

2. **WPA-PSK**: Based on pre-shared key. It is characterized by higher safety and simple settings, which suits for common households and small business. **WPA-PSK** has two versions: WPA-PSK and WPA2-PSK.



Version	Select one of the following versions: • **Auto** –Select WPA or WPA2 automatically based on the wireless station's capability and request. • **WPA** –Pre-shared key of WPA. • **WPA2** –Pre-shared key of WPA2.
Encryption	Select the Encryption type, including Auto, TKIP and AES. The default setting is Auto, which can select TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) automatically based on the wireless station's capability and request. AES is more secure than TKIP and **TKIP** is not supported in 802.11n mode. We recommend you select AES as the encryption type.
PSK Password	Configure the WPA-PSK/WPA2-PSK password with ASCII or Hexadecimal characters. For ASCII, the length should be between 8 and 63 characters with combination of numbers, letters (case-sensitive) and common punctuations; for Hexadecimal, the length should be 64 characters (case-insensitive, 0-9, a-f, A-F).
Group Key Update Period	Specify the group key update period in seconds. The value can be either 0 or at least 30, 0 means no update.

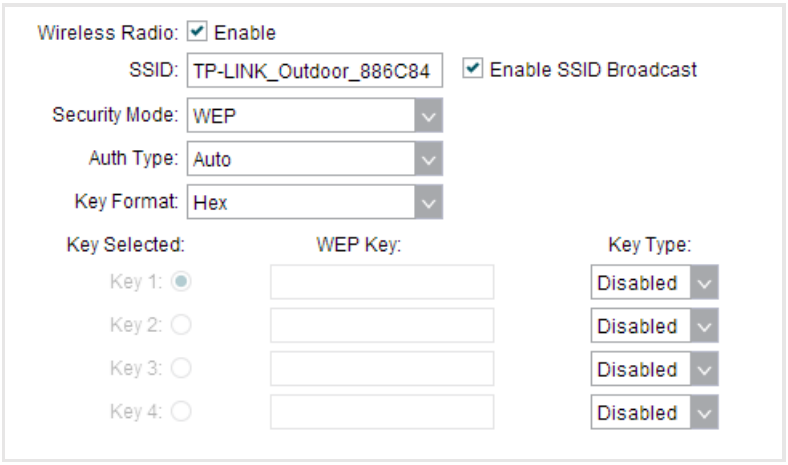
3. **WPA**: Based on RADIUS Server, WPA can assign different password for different users and it is much safer than WPA-PSK. However, its maintenance costs much which is only suitable for enterprise users. At present, WPA has two versions: WPA and WPA2.



Version	Select one of the following versions: • **Auto** –Select WPA or WPA2 automatically based on the wireless station's capability and request. • **WPA** –Pre-shared key of WPA. • **WPA2** –Pre-shred key of WPA2.
Encryption	Select the Encryption type, including Auto, TKIP, and AES. The default setting is Auto, which can select TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) automatically based on the wireless station's capability and request. AES is more secure than TKIP and TKIP is not supported in 802.11n mode. We recommend you select AES as the encryption type.
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 RADIUS authentication server. The shared key is a case-sensitive text string used to validate communication between this device and the RADIUS authentication server. The shared key characters will be shown if you check the box of **show**.
Group Key Update Period	Specify the group key update period in seconds. The value can be either 0 or at least 30, 0 means no update.

Accounting Server	With this option checked, 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 the default, 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. The shared key characters will be shown if you check the box of **show**.

4. **WEP**: Based on the IEEE 802.11 standard, this encryption is less safe than the above two modes. The **WEP** are not supported in 802.11n mode.



Auth Type	Select the Auth type of the WEP security on the drop-down list. The default setting is Auto, which can select Open System or Shared Key authentication type automatically based on the wireless station's capability and request.
Key Format	Select **Hex** or **ASCII**. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
Key Selected	You can configure four keys in advance and select the present valid key.
WEP Key	Enter the WEP keys. The length and valid characters of the key are affected by key type.

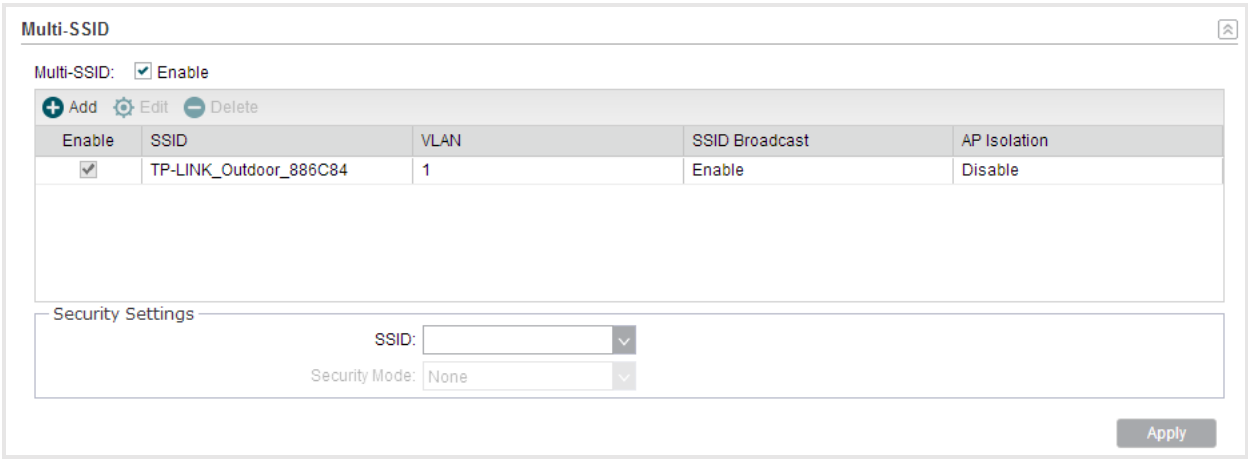
Key Type	Select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. **Disabled** means this WEP key is not used. • **64bit** -You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. • **128bit** -You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. • **152bit** -You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

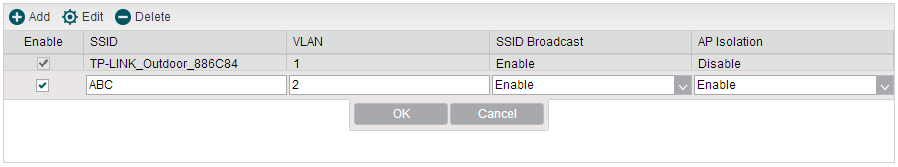
Multi-SSID

Multi-SSID is only available in Access Point mode.

This device can build up to four virtual wireless networks for users to access. When the Multi-SSID function of the device is enabled, its 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 with different VLAN ID cannot directly communicate with each other.

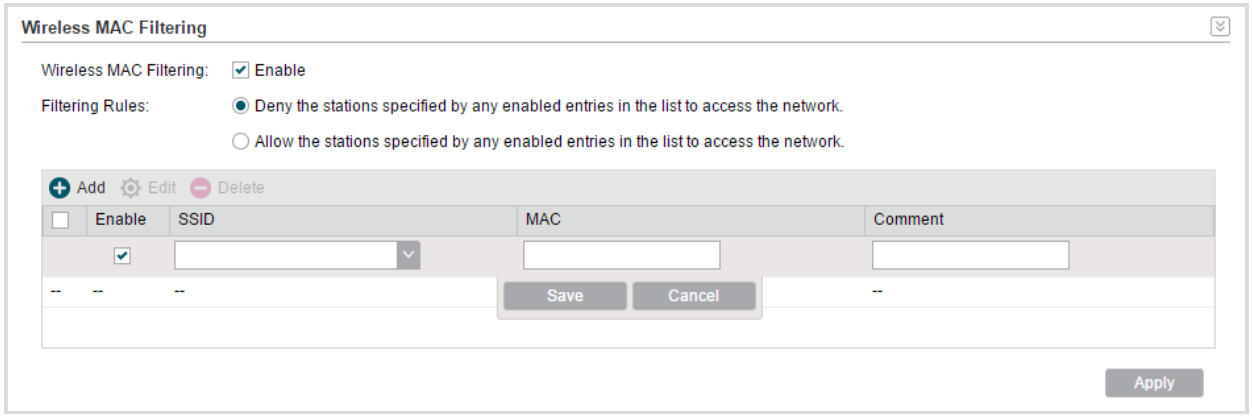
Clients connected to the device via cable don't belong to any VLAN. Thus wired client can communicate with all the wireless clients despite the VLAN settings.



Multi-SSID	Check the **Enable** box to use the Multi-SSID function.  Click **Add** in the table of Multi-SSID. Create a wireless network name (***SSID***), a string from 1 to 32 characters. Set the ***VLAN*** ID of wireless network identified by this SSID, and the value ranges from 1 to 4094. Select whether to broadcast this SSID or not. Enable ***AP Isolation***, the device would isolate the hosts within the same wireless network. All the hosts cannot communicate with each other. The default setting is **Disable**.
SSID	Select the added SSID to configure its security mode.
Security Mode	If all the hosts are allowed to access the wireless network, select **None**. For the safety of wireless network, you are suggested to encrypt your wireless network. This device provides three security modes: WPA-PSK (Pre-Shared Key), WPA (Wi-Fi Protected Access) and WEP (Wired Equivalent Privacy). WPA-PSK is recommended. Please refer to **Security Mode** in the Wireless AP Settings section for further information.

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.



Wireless MAC Filtering

Check the **Enable** box to use wireless MAC filtering function.

Click **Add** in the table of wireless MAC filtering.

Select the wireless network (***SSID***) that you need to filter. In AP mode, if Multi-SSID is enabled, you should set different filtering rules for each SSID.

Enter the ***MAC*** address of the wireless host that you need to filter.

Enter the description information of this filtering rule in the **Comment** filed.

Filtering Rules

There are two filtering policies to control the MAC filtering:

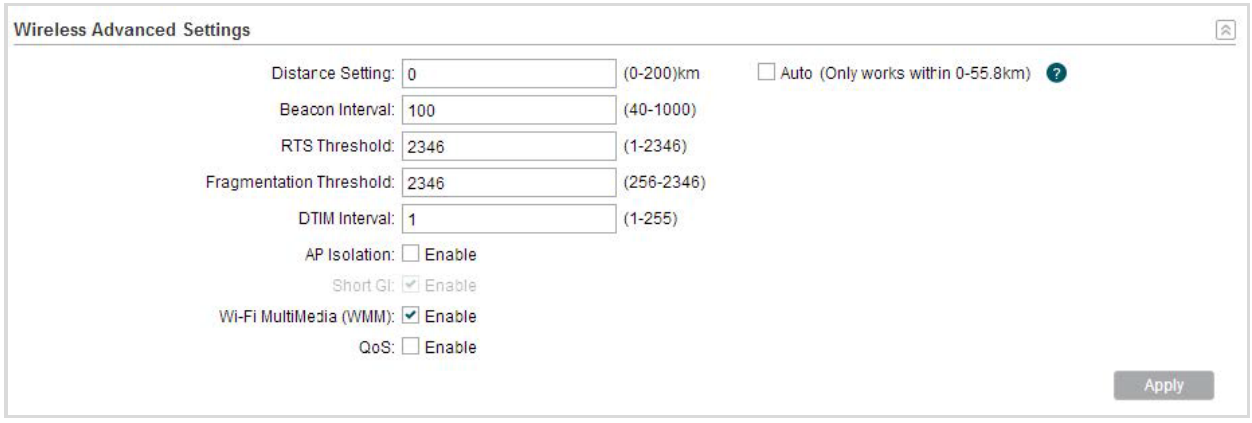
- Allow the stations specified by any enabled entries in the list to access.

The stations listed below 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 stations listed below are forbidden to access the wireless network under the rules. While others are allowed to access.

Wireless Advanced Settings

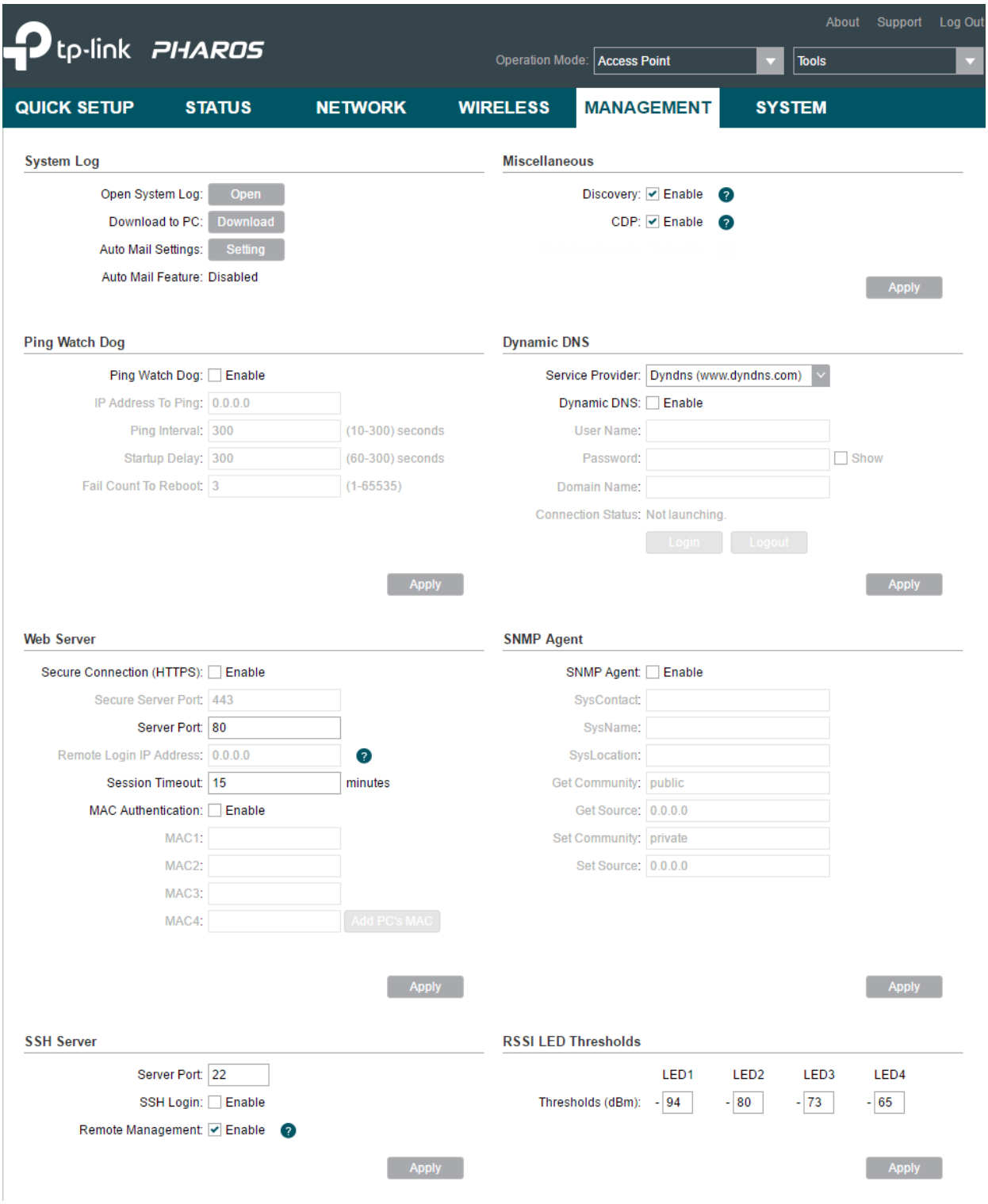


Distance Setting	Specify the distance between AP and Station. If this device serves as a client, the value is the distance between this device and the root AP. If this device serves as an AP, the value is the distance between the farthest client and this AP. You can manually enter the value or enable 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. Suppose device A is sending data frames to device B. Every time device A sends a data frame, it waits for the ACK frame from device B. If the ACK frame arrives within the ACK timeout, device A will send the next data frame. Otherwise, device A will re-send the data frame. The throughput performance drops either if too many data frames are re-sent (the ACK timeout is too short) or if device A waits too long to send the next data frame (the ACK timeout is too long). Therefore, a proper distance value determines an appropriate timeout value, which would greatly improve the throughput performance.
Beacon Interval	Beacons are transmitted periodically by the device to announce the presence of a Wireless network for the clients. Beacon Interval value determines the time interval of the beacons sent by the device. You can specify a value from 40 to 1,000. The default value is 100.
RTS Threshold	When the RTS threshold is activated, all the stations and APs follow the Request to Send (RTS) protocol. When the station is to send packets, it will send a RTS to AP to inform the AP that it will send data. After receiving the RTS, the AP notice other stations in the same wireless network to delay their transmitting of data. At the same time, the AP inform the requesting station to send data. The value range is from 0 to 2346 bytes. The default value is 2346, which means that RTS is disabled.
Fragmentation Threshold	Specify the fragmentation threshold for packets. If the size of the packet is larger than the fragmentation threshold, the packet will be fragmented into several packets. Too low fragmentation threshold may result in poor wireless performance caused by the excessive packets. The recommended and default value is 2346 bytes.

DTIM Interval	This value indicates the number of beacon intervals between successive Delivery Traffic Indication Messages (DTIMs) and this number is included in each Beacon frame. A DTIM is contained in Beacon frames to indicate whether the access point has buffered broadcast and/or multicast data for the client devices. Following a Beacon frame containing a DTIM, the access point will release the buffered broadcast and/or multicast data, if any exists. You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating the DTIM Interval is the same as Beacon Interval. An excessive DTIM interval may reduce the performance of multicast applications. We recommend you keep it by default.
AP Isolation	With this option enabled, AP Isolation to isolate all wireless stations connected to this device so that they cannot communicate with each other. This function will be disabled if WDS/Bridge is enabled.
Short GI	Short GI is used to increase the throughput by reducing the guard interval time. We recommend you enable this function.
Wi-Fi MultiMedia (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	The QoS function improves the transmission performance of video or audio traffic by optimizing the scheduling policy between the AP and the clients.

Chapter 7 Management Tab

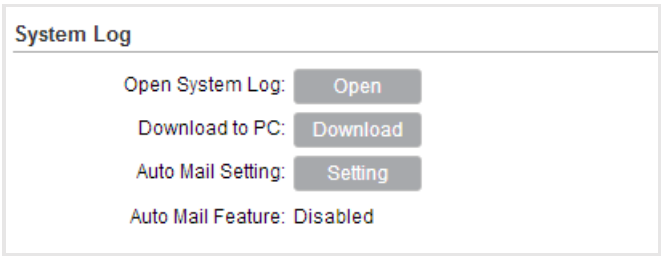
On **Management** Tab, you can configure system management services: System Log, Miscellaneous, Ping Watch Dog, and Dynamic Domain Name System (DDNS). Web server, Simple Network Management Protocol (SNMP), SSH server, RSSI LED Thresholds are also available.



If you have made any change of the parameters, click **Apply** to make the configuration take effect. There will be a blue bar at the top of the page to remind you to save the configuration. Click **Save Changes** when you finish all settings, otherwise all the settings will be recovered to last saved settings at reboot or power off.

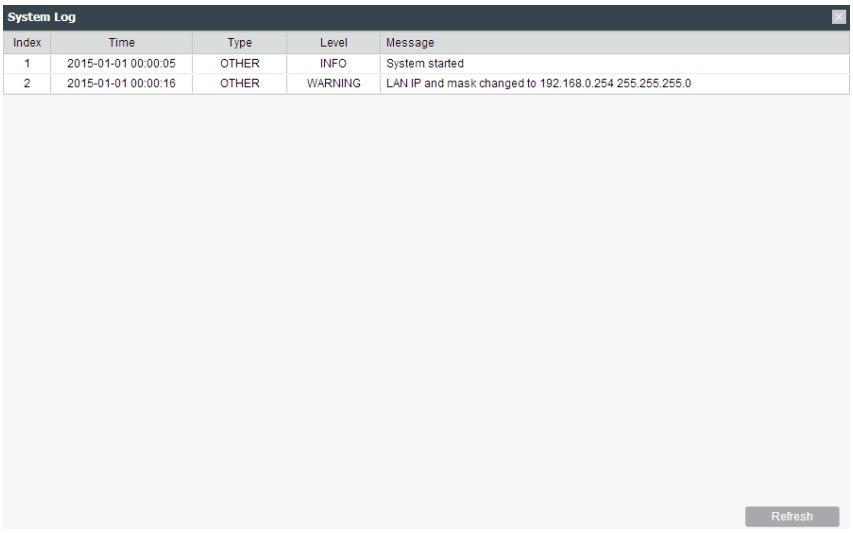
System Log

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



Open System Log

Check system log by clicking **Open** and then appears the following popup page.



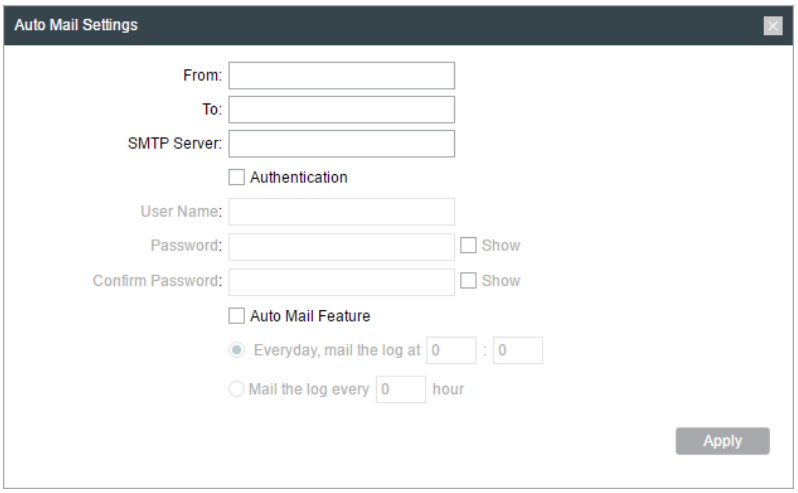
This page displays detailed system logs that can be sorted on columns by ascending or descending order. Columns can be chosen from Time, Type, Level, and Message.

Download to PC

Enables users to download system logs to PC.

Auto Mail Setting

Enables users to mail system logs automatically. Click **Setting** and the following page appears.



Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.

- **From** – Enter sender's mail box address.
- **To** – Enter the recipient's address.
- **SMTP Server** – Enter sender's SMTP server.
- **Authentication** - Most SMTP Server requires Authentication.
- **User Name** – Sender's mail account name.
- **Password** – Sender's mail account password.
- **Confirm Password** –Re-enter your mail account password.

Check **Auto Mail Feature** box, you can set the device how and when to send the log to the specified mailbox.

Miscellaneous

Discovery

Enable the function to let TP-Link Pharos Control software discover the device. With its main function to centralize monitoring and managing network devices in the network platform, Pharos Control is network management software developed independently by TP-Link and it currently supports Pharos series products.

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).

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.

Ping Watch Dog	Check the **Enable** box to use the function of Ping Watch Dog.
IP Address To Ping	Specify the IP address of the target host to which the Ping Watch Dog Utility will send ping packets.
Ping Interval	Enter the time interval (in seconds) between two successive ping packets. The default value is 300 seconds.
Startup Delay	Enter the initial time delay (in seconds) 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 as the device's initialization takes a considerable amount of time.
Failure 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.

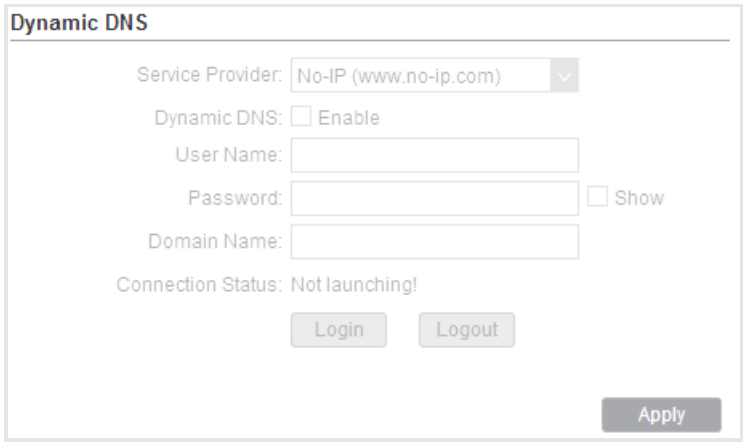
Dynamic DNS

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. Dynamic DNS function allows users to access servers using a fixed domain name.

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

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

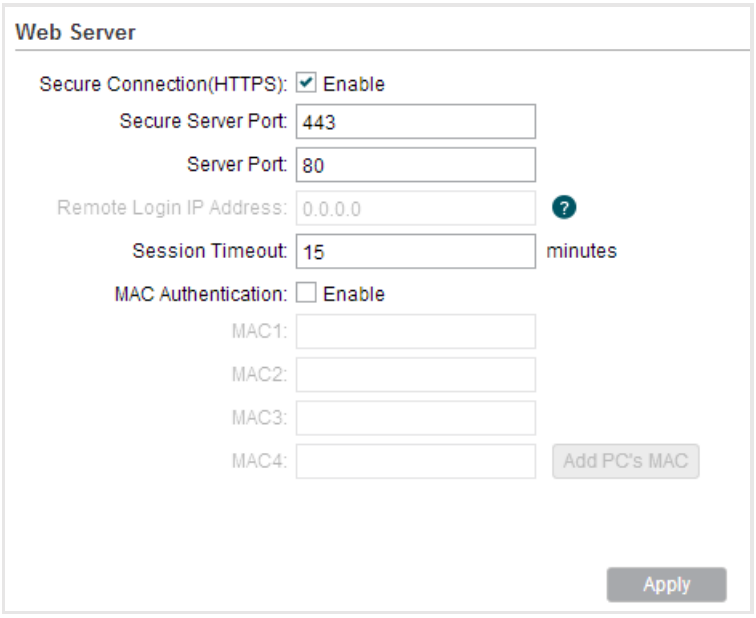


Service Provider	Select your DDNS service provider from the available DDNS service providers including NO-IP (www.no-ip.com), Dyndns (www.dyndns.com) and Comexe (www.comexe.net).

Dynamic DNS	Check the **Enable** box to use the function. • **User Name -** Enter the user name of the DDNS account. • **Password -** Enter the password of the DDNS account. • **Show -** Check the box to display the password characters. • **Domain Name** -Enter a customized domain name. Even if your IP is dynamic, other users on the Internet can still access your server via this fixed domain name after enabling the DDNS function. • **Connection Status** -Displays the connection status between this device and the DDNS server.

Web Server

The Web Server function enables users to log in to the web management page to manage this device remotely over the Internet.



Secure Connection (HTTPS)	The Secure Connection (HTTPS) mode is enabled by default.
Secure Server Port	Specify the server port that the Web server uses in the Secure Connection (HTTPS) mode, and the default is 443.
Server Port	Specify the server port that the Web server uses in the HTTP mode, and the default is 80.
Remote Login IP Address	Configure the IP address that can remotely visit the web management page of this device. Enter 0.0.0.0 to forbid any remote IP's login. Enter 255.255.255.255 to allow all the remote IP to visit.

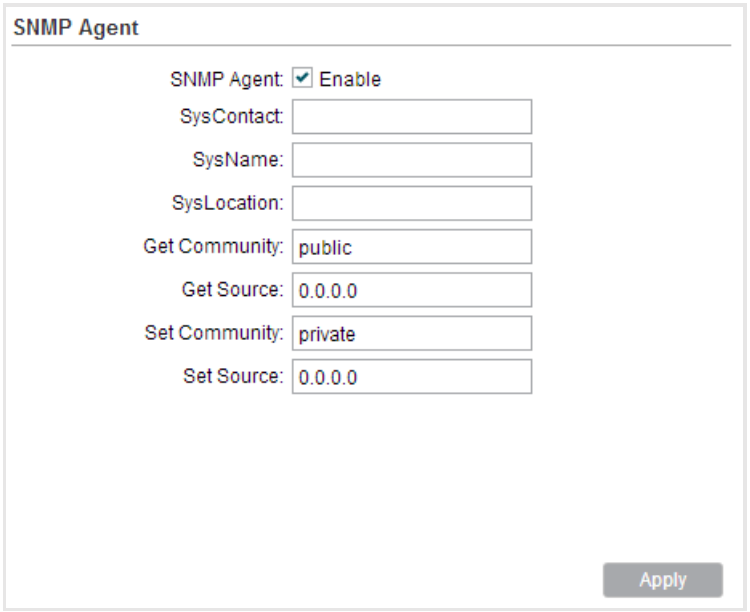
Session Timeout	Enter the maximum timeout before the session expires. Once a session expires, you must log in again using the username and password.
MAC Authentication	Enable this function to allow PCs with specific MAC addresses to access the web management page. And then enter each MAC address in the MAC field. The format for the MAC addresses is XX-XX-XX-XX-XX-XX. Only the PCs with the MAC addresses listed can use the password to access the device's web management page and the others will be blocked. By default, the function is not enabled. All the PCs in the local area network are allowed to access the device's web management page. Click **Add PC's MAC**, your PC's MAC address will be added in the list above. Click **Apply** to save your settings.

SNMP Agent

You can get the traffic information and transmit condition by using the SNMP Agent function.

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. Main functions of SNMP include monitoring network performance, detecting and analyzing network error, configuring network devices, and so on. Under the circumstance of network working normally, SNMP can play a part in statistics, configuration and testing. When networks have troubles, SNMP can detect and restore these troubles.

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



SNMP Agent	**Enable** the SNMP Agent function and the SNMP Agent will gather the information of this device and respond to information requests from one or more management systems.
SysContact	Enter the information of the contact person for this managed node.
SysName	Enter an administratively-assigned name for this managed node.
SysLocation	Enter the physical location of this managed node.
Get Community	Community refers to a host group aiming at network management. Get Community only has the read-only right of the device's SNMP information. The get community name can be considered as a password used to restrict the access right of SMNP managers. The default name is public.
Get Source	Defines the IP address (for example, 10.10.10.1) or subnet (for example, 10.10.10.0/24) for management systems that can serve as Get Community to read the SNMP information of this device. The default is 0.0.0.0, which means all hosts can read the SNMP information of this device.
Set Community	Set Community has the read and write right of the device's SNMP information. Enter the community name that allows read/write access to the device's SNMP information. The community name can be considered as a password to restrict the access right of SNMP managers. The default name is private.
Set Source	Defines the IP address (for example, 10.10.10.1) or subnet (for example, 10.10.10.0/24) for management systems that can serve as Set Community to read and write the SNMP information of this device. The default is 0.0.0.0, which means all hosts can read and write the SNMP information of this device.

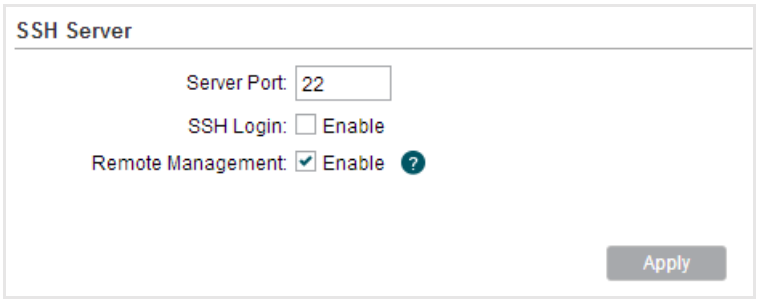
NOTE:

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.

SSH Server

The SSH Server function allows 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.



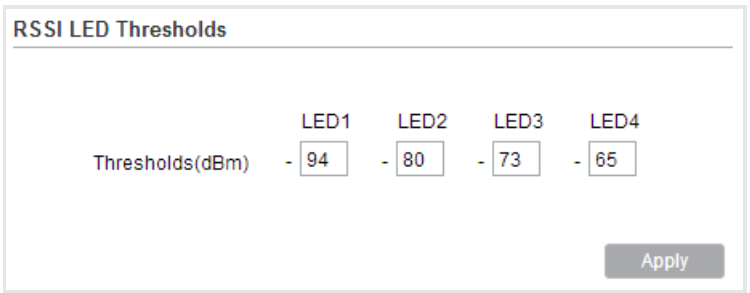
Server Port	Enter the TCP/IP port of the SSH Server. The default port is 22.
SSH Login	Enable the SSH Server function.
Remote Management	Enable the function to let TP-Link Pharos Control software manage the device remotely.

RSSI LED Thresholds

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

NOTE:

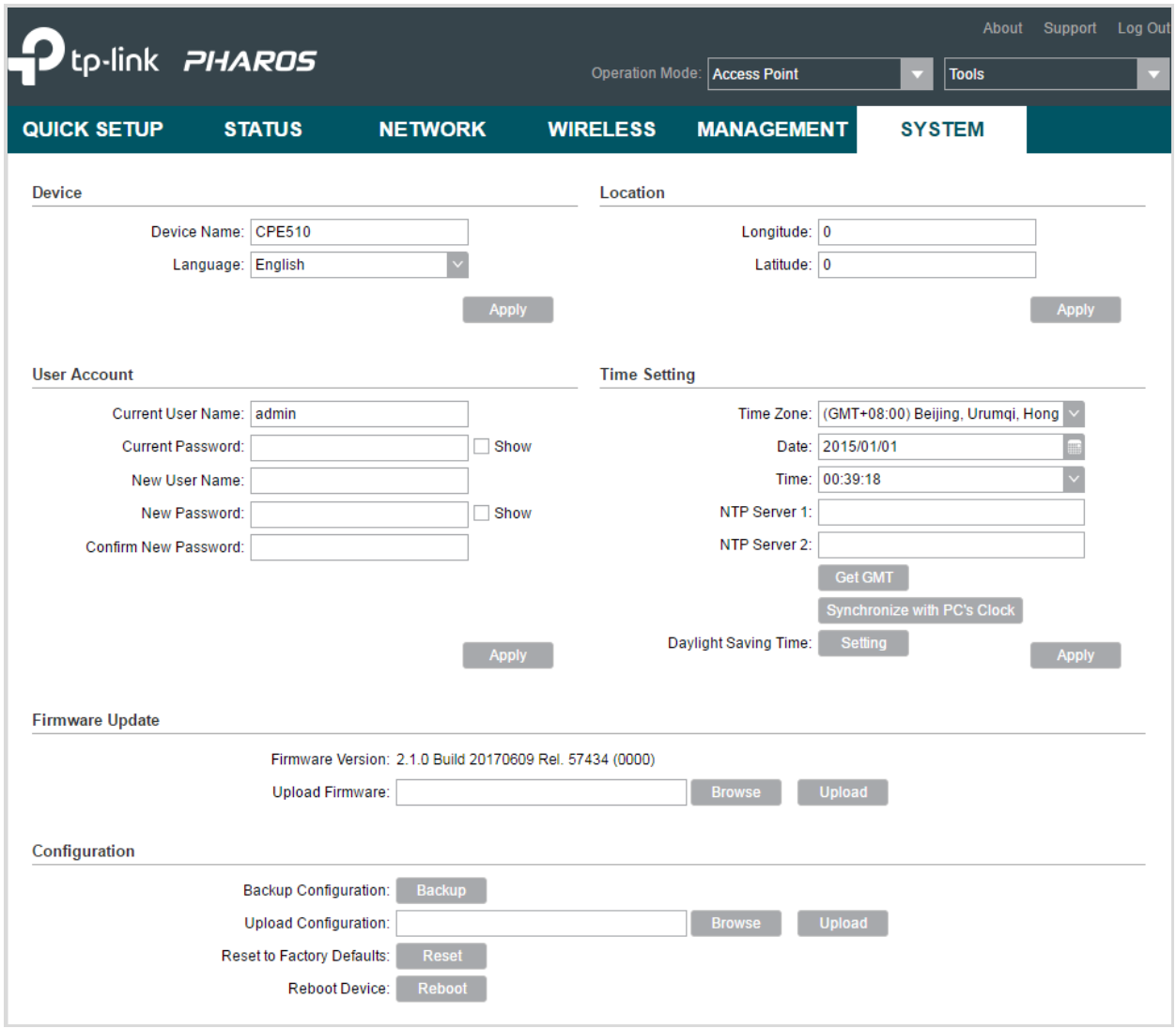
CPE610 does not support this feature.



Thresholds (dBm)	The specified LED will light up if the signal strength reaches the values in the field. For example, if the signal strength fluctuates around -63 dBm, then the LED threshold values can be set to the following: -70, -65, -62, and -60. 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. The figure above shows the default values of CPE210.

Chapter 8 System Tab

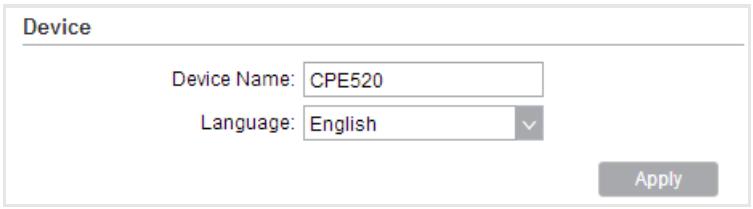
The **System** Tab controls system maintenance routines, device customization, location management, user account management, firmware update, time setting and configuration backup.



If you have made any change of the parameters, click **Apply** to make the configuration take effect. There will be a blue bar at the top of the page to remind you to save the configuration. Click **Save Changes** when you finish all settings, otherwise all the settings will be recovered to last saved settings at reboot or power off.

Device

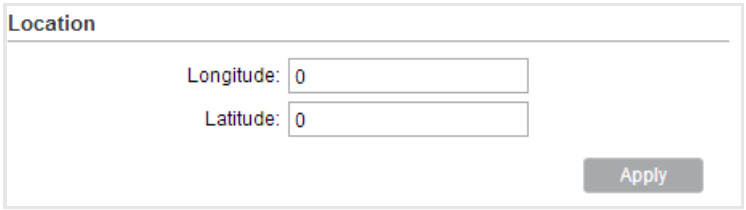
The Device Name is the model of device by default. You can customize a new personal and easy-to-remember name.



Device Name	Customize the name of the device.
Language	Displays the default language in the web management page is English.

Location

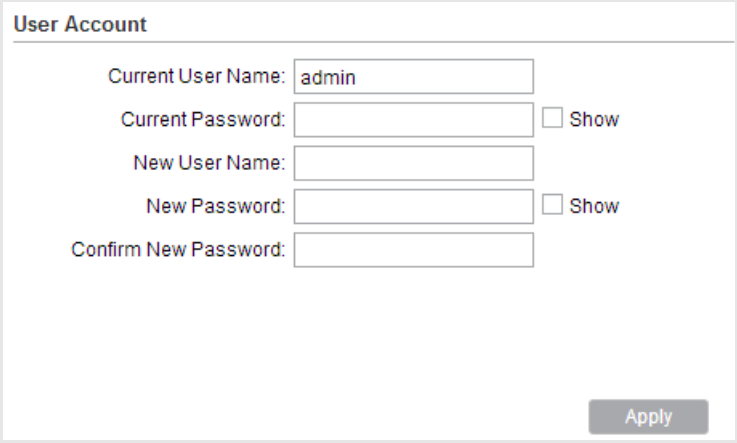
Longitude and latitude define the device's coordinates.



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.

User Account

You can change the user password to protect your device from unauthorized login. We recommend that you change the default user password on the very first system setup.

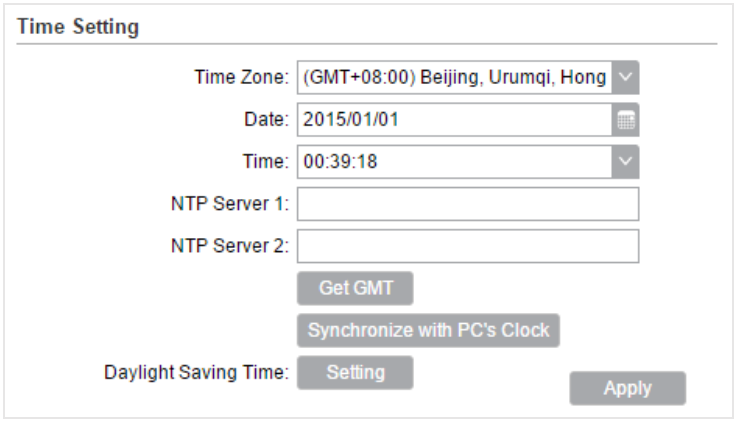


Current User Name	Displays the current user name.
Current Password	Enter the current password for the user account. Check the **Show** box to display what you've entered.
New User Name	Enter the new user name for the user account.
New Password	Enter the new password for the user account. Check the **Show**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

NOTE:

The password is a string from 1 to15 alphanumeric characters or symbols.

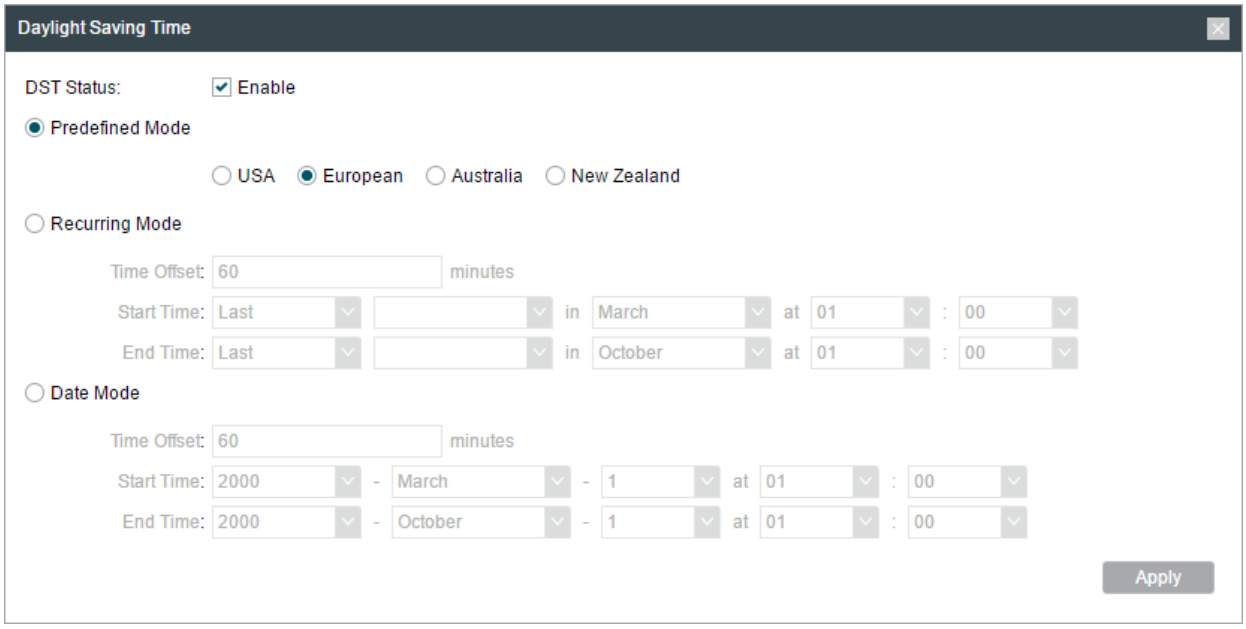
Time Setting



Time Zone	Select your local time zone from the drop-down list.

Date	Specify the device's date. Click the calendar icon or manually enter the date in the following format: YYYY/MM/DD. For example, for November 25, 2013, enter 2013/11/25 in the field.
Time	Specify the device's date. Select the time from the drop-down list or manually enter the date in HH:MM:SS format.
NTP Server 1	Enter the primary NTP Sever address.
NTP Server 2	Enter an alternative NTP Server address.
Get GMT	Click **Get GMT** to get GMT from the NTP server.
Synchronize with PC's Clock	Date and time of the device can be synced with your PC's system time.
Daylight Saving Time	Click **Setting** to set the daylight saving time on the following page.

Daylight Saving Time



DST Status	Check the **Enable** box to use the function.

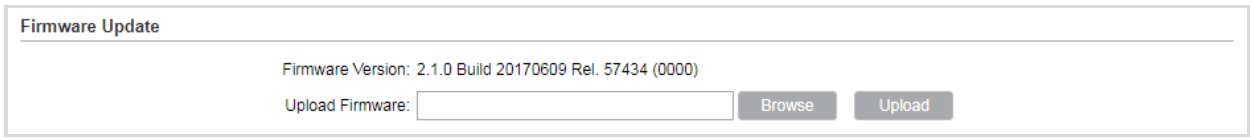
Predefined Mode	Select a predefined DST configuration. • **USA**: Second Sunday in March, 02:00 ~ First Sunday in November, 02:00. • **European**: Last Sunday in March, 01:00 ~ Last Sunday in October, 01:00. • **Australia**: First Sunday in October, 02:00 ~ First Sunday in April, 03:00. • **New Zealand**: Last Sunday in September, 02:00 ~ First Sunday in April, 03:00.
Recurring Mode	Specify the DST configuration in recurring mode. This configuration is recurring in use. • **Time Offset**: Specify the time offset in minutes when Daylight Saving Time comes. • **Start/End Time**: Select the start time and end time of Daylight Saving Time. The start time is the standard time, and the end time is the Daylight Saving Time.
Date Mode	Specify the DST configuration in Date mode. This configuration is one-off in use. • **Time Offset**: Specify the time adding in minutes when Daylight Saving Time comes. • **Start/End Time**: Select the start time and end time of Daylight Saving Time. The start time is the standard time, and the end time is the Daylight Saving Time.

NOTE:

When the DST is enabled, the default daylight saving time is European in predefined mode.

Firmware Update

Firmware update can improve the function of the device.



Firmware version	Displays the current firmware version.

Upload Firmware	Please visit TP-Link website **www.tp-link.com/en/support/download/** to download the latest firmware. The system configuration can be preserved while the device is updated with a new firmware version. However, we recommend that you back up current system configuration before updating the firmware. Firmware update takes three steps: Click **Browse** to locate the new firmware file. Select the file and click **Open**. The new firmware to be uploaded is displayed in the field. Click **Upload** and there will be a pop-up page which gives you three options of keeping your configurations or restoring to factory default after the upgrade or just cancel the upgrade.

NOTE:

Please select the proper software version that matches your hardware to upgrade.

To avoid damage, please do not power off the device while upgrading.

After upgrading, the device will reboot automatically.

Configuration

The controls in this section manage the device configuration routines and the option to reset the device to factory default settings.

The device configuration is stored in the plain text file. You can back up, restore, or update the system configuration file.

Backup Configuration	Click **Backup** to back up the current system configuration file.
Upload Configuration	Click **Browse** to locate the new configuration file. Select the file and click **Open**, then the new configuration to be uploaded is displayed in the field. Click **Upload** to upload the new configuration to the device. We recommend that you back up your current system configuration before uploading the new configuration.

Reset to Factory Defaults	Resets the device to the default settings. This option will reboot the device, and all factory default settings will be restored. It's recommended that you back up your current system configuration before resetting the device to its defaults.
Reboot Device	Initiates a full reboot cycle of the device. The system configuration stays the same after the reboot cycle completes. Any changes that have not been applied will be lost.

NOTE:

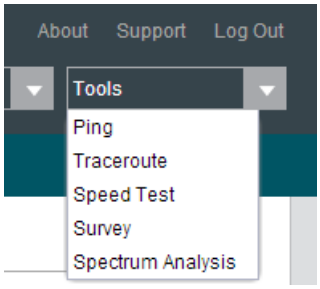
After backing up, the device will reboot automatically.

To avoid damage, please don't turn off the device while uploading.

You are suggested to back up the configuration before upgrading.

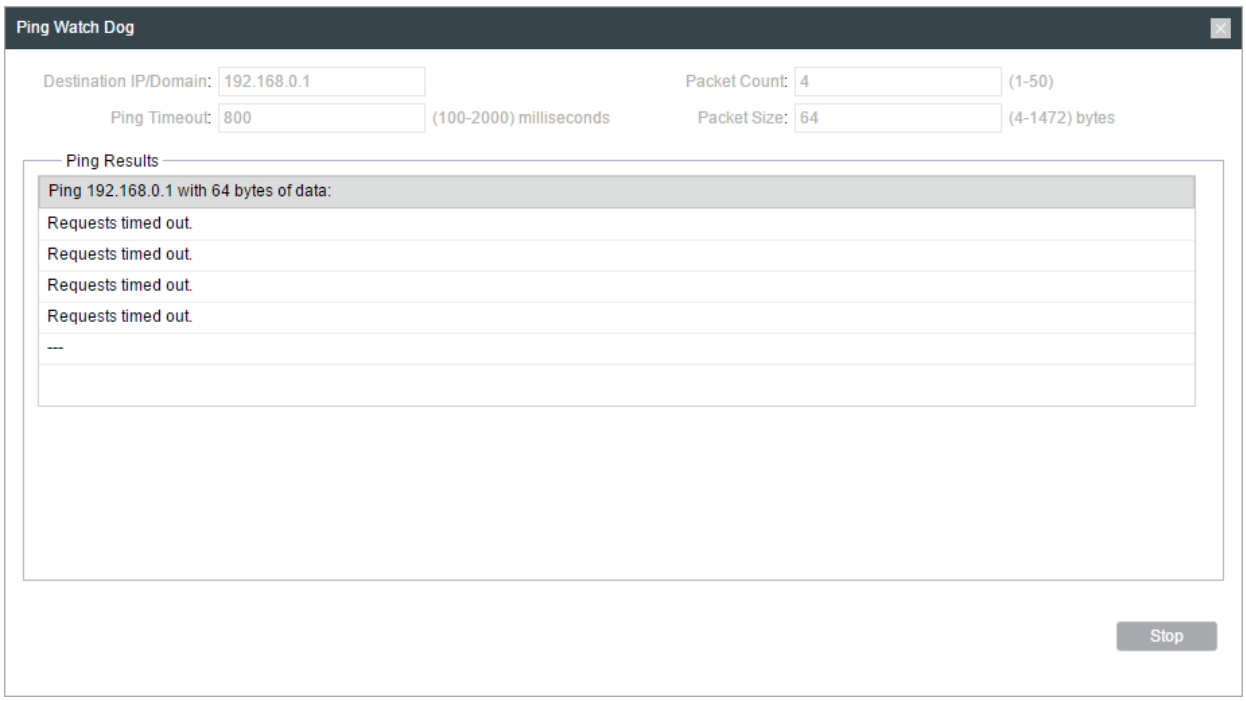
Chapter 9 Tools List

This device provides some useful tools including Ping, Traceroute, Speed Test, Survey and Spectrum Analysis.



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.

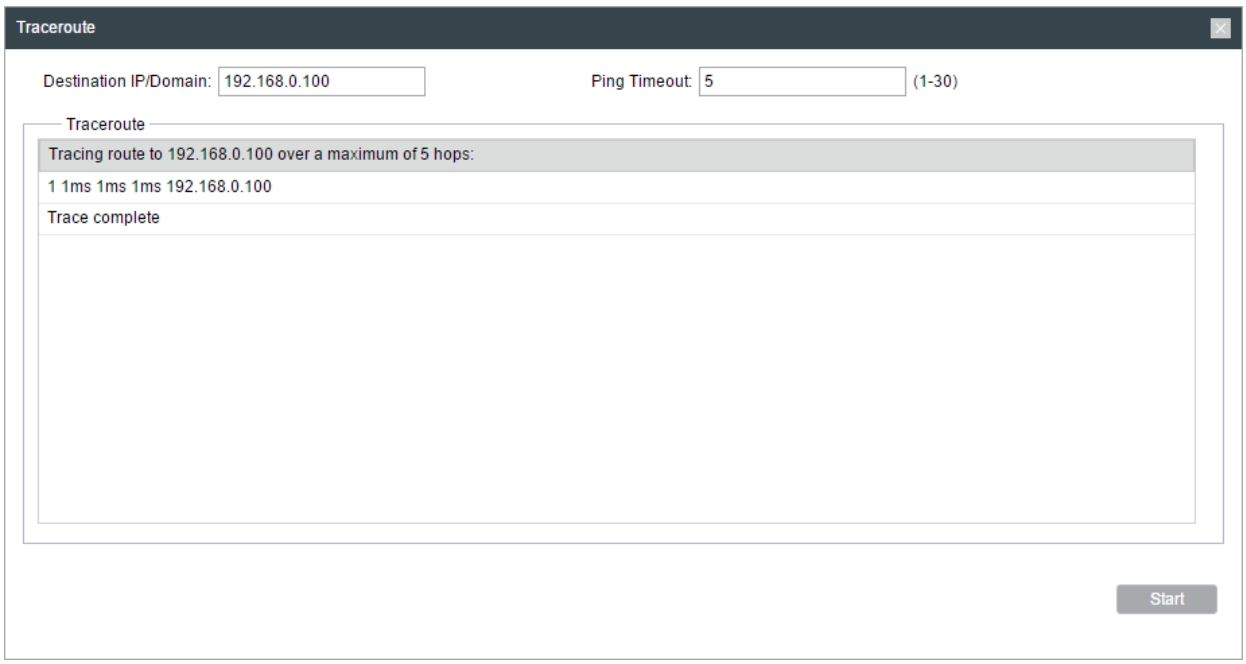


Destination IP/Domain	Enter the IP address of the destination node for Ping test. Click **Start**, the device will send Ping packets to test the network connectivity and reachability of the host and the results will be displayed in the list below.
Packet Count	Enter the number of packets to be sent during the testing. It can be 1 to 50 and the default is 4.

Ping Timeout	Enter a time value to wait for a response. 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.

Traceroute

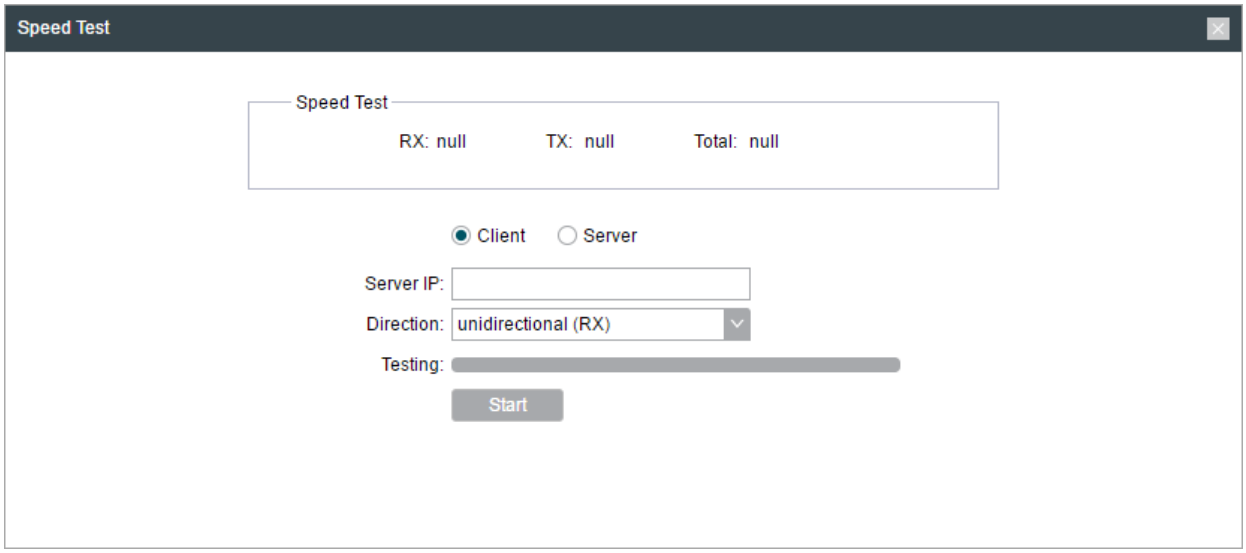
Tracertroute function is used to tracks the route packets taken from source on their way to a given target host. When malfunctions occur in the network, you can troubleshooting with traceroute utility.



Destination IP/Domain	Enter the destination IP address or the Domain name. Click **Start**, the device will send Tracert packets to the target host and the results will be displayed in the list below.
Traceroute Max TTL	Set the maximum number of hops (max TTL to be reached) in the path to reach the target (destination). The default is 5.

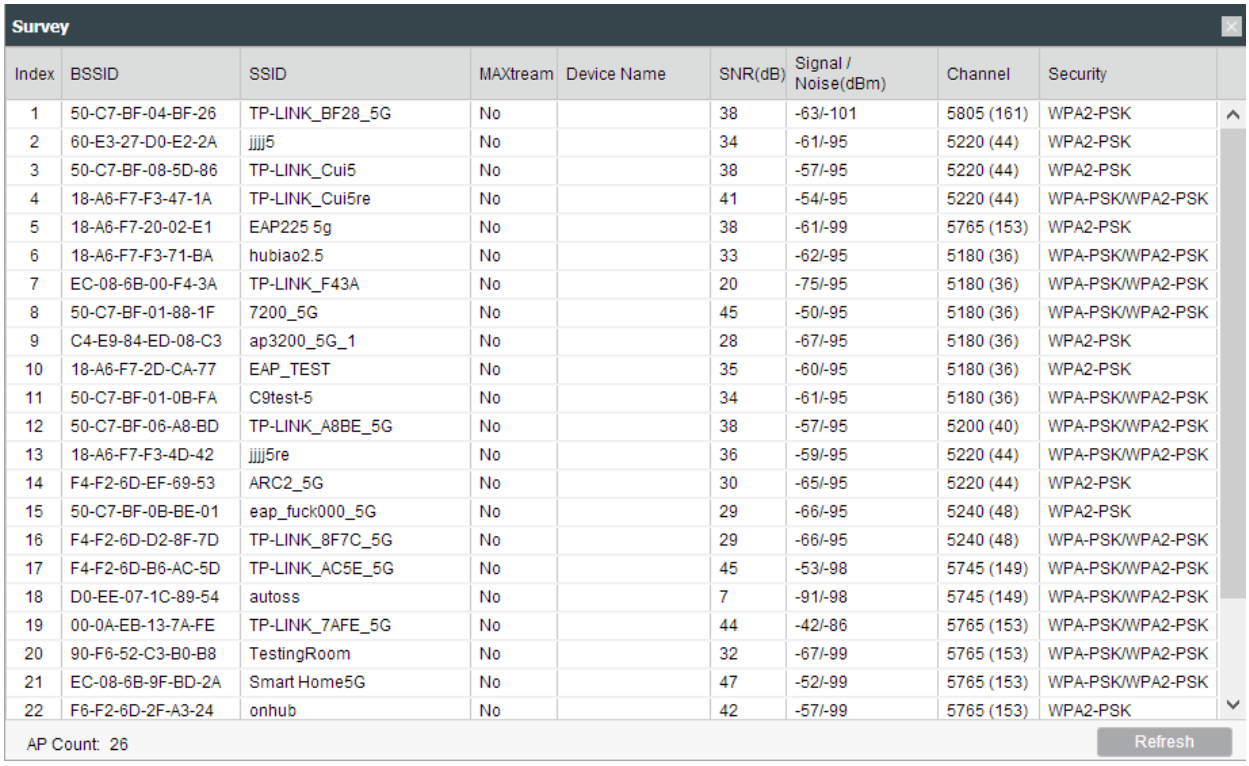
Speed Test

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.



Test Result	Displays the data streams that the device is transmitting (TX), receiving (RX) and both of them (Total).
Client	The side to initiatively launch the test request. The client side can configure parameters including server's IP and direction.
Server	The side to passively accept the test request.
Server IP	The IP address of the server.
Direction	Select the direction of the speed test including **unidirectional (RX)**, **unidirectional (TX)** and **bidirectional**.
Testing	Testing progress bar. Click **Start** to displays the testing progress.

Survey



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

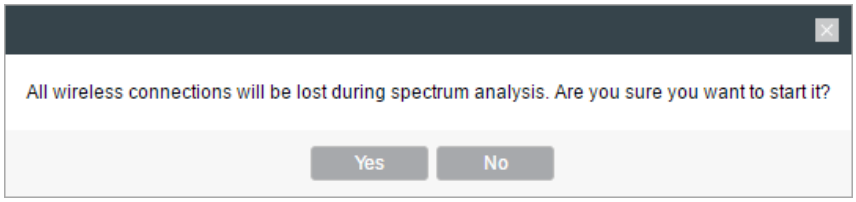
Refresh

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 other APs surveyed by this device.
AP Count	Displays the number of other APs surveyed by this device.
Refresh	Refresh this page by clicking **Refresh**.

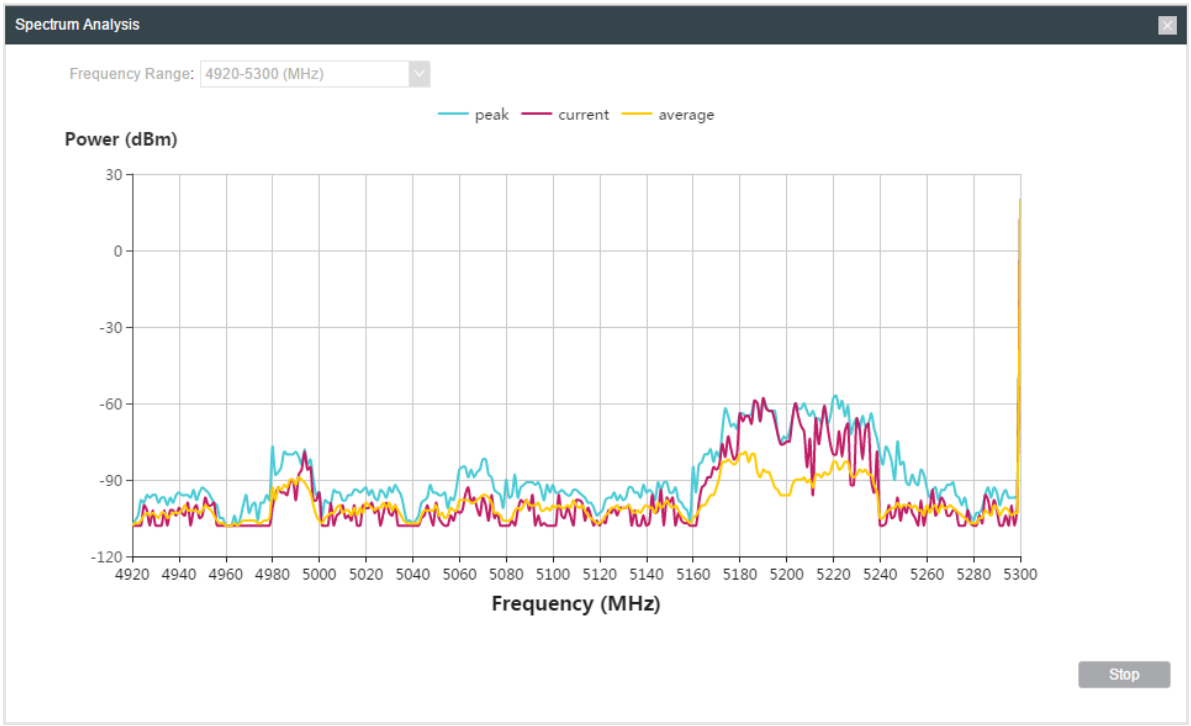
Spectrum Analysis

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

1. Click **Spectrum Analysis** in the tools' drop-down list, the following window will pop up to remind you that all wireless connections will be lost during spectrum analysis. Click **Yes** and you will then get into Spectrum Analysis page.



2. Click **Start**, the PharOS will begin to analyze the power of frequency. Observe the curves for a period of time, and then click **stop**. Note that the relatively low and continuous part of the average curve indicates less radio noise. Here we take the figure below as an example.



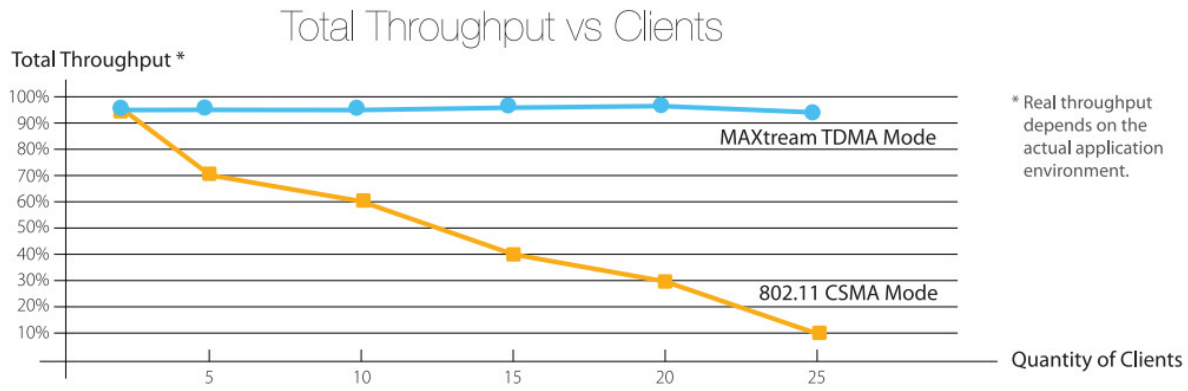
NOTE:

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

3. When choosing channel/frequency, we should try to avoid the spectrum with large radio noise. In this example, the recommended channel/frequency is 1/2412MHz.

Appendix A: Pharos MAXtream TDMA

With the fast expansion of network scale, wireless competition and collisions among CPEs and base stations will be so enormous that the real throughout of the network will drop, resulting in a serious impact on end-user experience. To mitigate these effects, TP-Link's Pharos series develops MAXtream TDMA Technology.

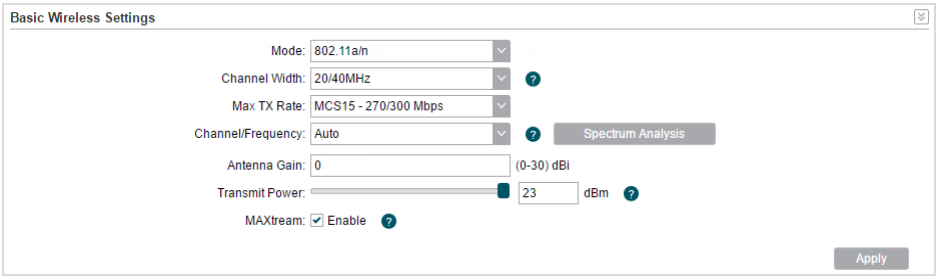


Pharos MAXtream is a proprietary protocol developed on the basis of TDMA (Time Division Multiple Access) by TP-Link. MAXtream cuts each wireless data frame transmission into certain number of time slots according to the client connections priority, greatly boosting efficiency of the wireless channel.

The MAXtream technology has the following advantages which make it ideal for point to multi-point links:

- Eliminates hidden node collisions and improves channel efficiency
- Lower latency, higher throughput, larger network capacity and more stability

To enable the MAXtream function among the AP and stations, you only need to select **MAXtream** option on the **Wireless** tab of the Pharos web management page of the AP, as shown in the following figure. Stations will automatically adjust their connections according to AP's MAXtream capability.



NOTE:

Pharos MAXtream is a non-standard Wi-Fi protocol that is only compatible with TP-Link's Pharos series products. Please notice that you will not be able to connect other Wi-Fi devices to an AP with MAXtream enabled.

Appendix B: Glossary

	Glossary	Description
A	ALG (Application Layer Gateway)	Application Level Gateway (ALG) is application specific translation agent that allows an application on a host in one address realm to connect to its counterpart running on a host in different realm transparently.
	ARP (Address Resolution Protocol)	Internet protocol used to map an IP address to a MAC address.
C	CPE (Customer Premise Equipment)	A terminal located at a subscriber's premises and connected with a carrier's telecommunication channel at the demarcation point. The point is established in a building or complex to separate customer equipment from the equipment located in either the distribution infrastructure or central office of the Communications Service Provider.
D	DDNS (Dynamic Domain Name Server)	The capability of assigning a fixed host and domain name to a dynamic Internet IP address.
	DFS (Dynamic Frequency Selection)	A method applied in wireless networks, which is used for radar avoidance and is supported by the novel IEEE 802.11h wireless local area network standard.
	DHCP (Dynamic Host Configuration Protocol)	A protocol that automatically configures the TCP/IP parameters for all the PCs that are connected to a DHCP server.
	DMZ (Demilitarized Zone)	A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
	DNS (Domain Name Server)	An Internet Server that translates the names of websites into IP addresses.
	DoS (Denial of Service)	A hacker attack designed to prevent your computer or network from operating or communicating.
F	FTP (File Transfer Protocol)	Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes.
H	HTTP (Hypertext Transfer Protocol)	The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

	Glossary	Description
I	ICMP (Internet Control Messages Protocol)	Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
	Internet	Largest global Internetwork, connecting tens of thousands of networks worldwide and having a "culture" that focuses on research and standardization based on real-life use.
	IP (Internet Protocol)	Network layer protocol in the TCP/IP stack offering a connectionless Internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.
	ISP (Internet Service Provider)	Company that provides Internet access to other companies and individuals.
	IPsec (IP Security)	A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers.
L	LAN (Local Area Network)	High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area.
M	MAC address (Media Access Control address)	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE.
	MTU (Maximum Transmission Unit)	The size in bytes of the largest packet that can be transmitted.
N	NAT (Network Address Translator)	Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.
	NTP Server	NTP Server is used for synchronizing the time across computer networks.
P	PPPoE (Point-to-Point Protocol over Ethernet)	PPPoE is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames.

	Glossary	Description
S	SMTP (Simple Mail Transfer Protocol)	SMTP is an Internet standard for electronic mail (e-mail) transmission
	SSH (Secure Shell Protocol)	SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
	SSID	A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
	SNMP (Simple Network Management Protocol)	SNMP provides a management frame to monitor and maintain the network devices. With SNMP function enabled, network administrators can easily monitor the network performance, detect the malfunctions and configure the network devices.
T	TCP (Transfer Control Protocol)	Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.
	TCP/IP (Transmission Control Protocol/ Internet Protocol)	Common name for the suite of protocols to support the construction of worldwide Internet works. TCP and IP are the two best-known protocols in the suite.
	TDMA (Time Division Multiple Access)	TDMA (Time Division Multiple Access) cuts each wireless data frame into certain number of time slots according to the client connections priority, greatly boosting efficiency of the wireless channel.
U	UDP (User Datagram Protocol)	UDP is a simple protocol that exchanges datagram without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.
	UPnP (Universal Plug and Play)	UPnP is a set of networking protocols for primarily residential networks without enterprise class devices that permits networked devices.
V	VLAN (Virtual Local Area Network)	Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
	VPN (Virtual Private Network)	Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another.

	Glossary	Description
W	WAN (Wide Area Network)	Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers.
	WEP (Wired Equivalent Privacy)	A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
	Wi-Fi	A trademark of the Wi-Fi Alliance, founded in 1999 as Wireless Internet Compatibility Alliance (WICA), comprising more than 300 companies, whose products are certified by the Wi-Fi Alliance, based on the IEEE 802.11 standards (also called Wireless LAN (WLAN) and Wi-Fi). This certification warrants interoperability between different wireless devices.
	WISP (Wireless Internet Service Provider)	WISPs are Internet service providers with networks built around wireless networking. The technology used ranges from commonplace Wi-Fi mesh networking or proprietary equipment designed to operate over open 900MHz, 2.4GHz, 4.9, 5.2, 5.4, and 5.8GHz bands or licensed frequencies in the UHF or MMDS bands.
	WLAN (Wireless Local Area Network)	A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.