Wireless Bridge Operation Manual

V 7 . 8

HG-CPE5.8G-1

Table of contents

1. About the Manual

1.1.Purpose

This document provides information and procedures for the installation, setup, configuration, and management of CPE units.

1.2.Definitions, Acronyms and Abbreviations

The following typographical conventions and symbols are used in this document:

Additional information that may be helpful but is not required.

This is important information that we should observe.

Bold Menu commands, buttons, input fields, links, and configuration keys appear in bold.

Italic References to sections in the document are shown in italics.

Code File names, directory names, form names, system-generated output, and user-entered entries are displayed as constant-width types.

1.3.List of abbreviations

Abbreviations	describe
ACL	Access Control List
ACK	confirm
AES	Advanced Encryption Standard
AMSDU	Aggregate Mac Service Data Unit
AP	Access Point
ATPC	Automatic transmit power control
CCQ	Client connection quality
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
GHz	megahertz
GMT	Greenwich Mean Time
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
ISP	Internet Service Providers
IP	Network Protocol
LAN	local area network

led	Light Emitting Diode

Abbreviations	describe
MAC	Media Access Control
Mbps	Megabits per second
MCS	Modulation and coding scheme
MHz	megahertz
MIMO	Multiple Inputs, Multiple Outputs
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol
NAS	Network Access Server
NAT	Network Address Translation
NTP	Network Time Protocol
PC	PC
PDA	Personal Digital Assistant
PTP	peer to peer
PTMP	Point-to-multipoint
PSK	Pre-shared key
QoS	Quality of Service
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Authentication Dial-In User Service
RSSI	Received Signal Strength Indicator - Received signal strength in mV, measured at the BNC outdoor unit connector
RX	take over
SISO	Simple input, simple output
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TTLS	EAP-TTLS
TX	transmission
UDP	User Datagram Protocol
UAM	Common access methods
VLAN	Virtual Local Area Network
VoIP	voip voice over internet protocol
WACL	Wireless Access Control List
WDS	Wireless distribution system
WEP	Wired Equivalent Privacy (WEP) protocol
WISPr	Wireless Internet Service Roaming Providers
WLAN	Wireless LAN
WPA	Wireless Protected Access
WPA2	Wireless Protected Access Version 2

2. Quick Access

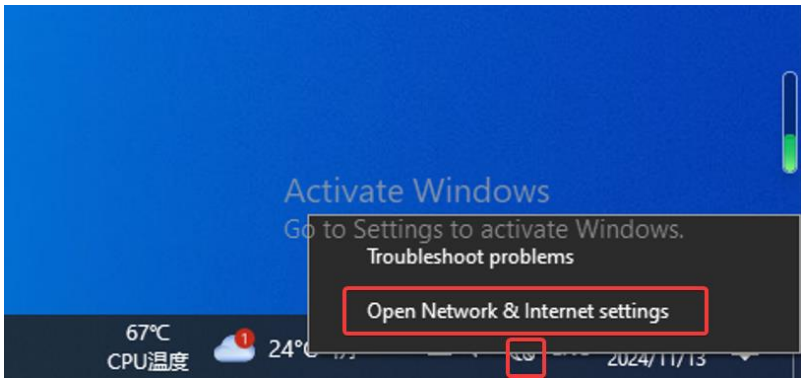
3. Browser access device

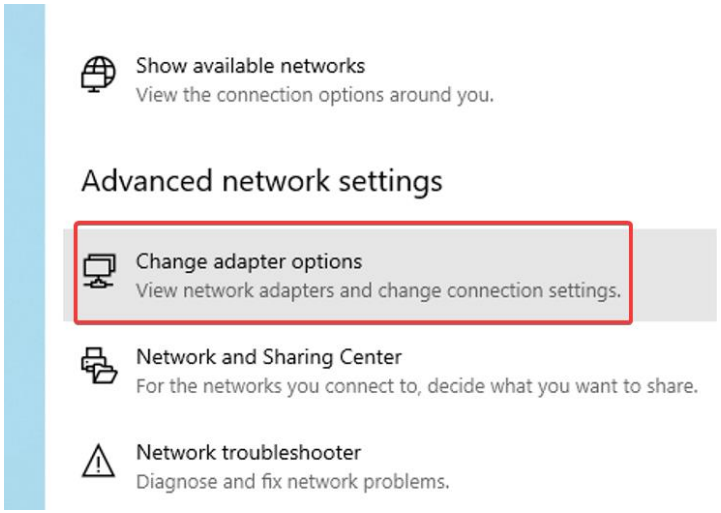
3.1.First time connecting via Ethernet

By default, the default static IP address of the CPE is based on the body sticker (for example, IP: 192.168.188.253).

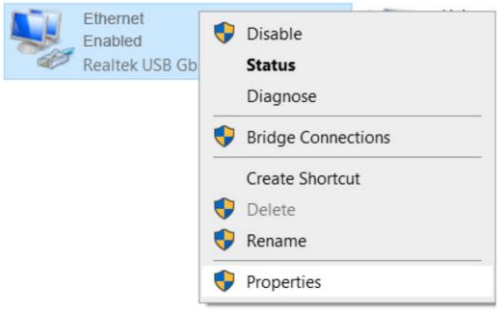
3.2. Configuring a static IP address for Windows system

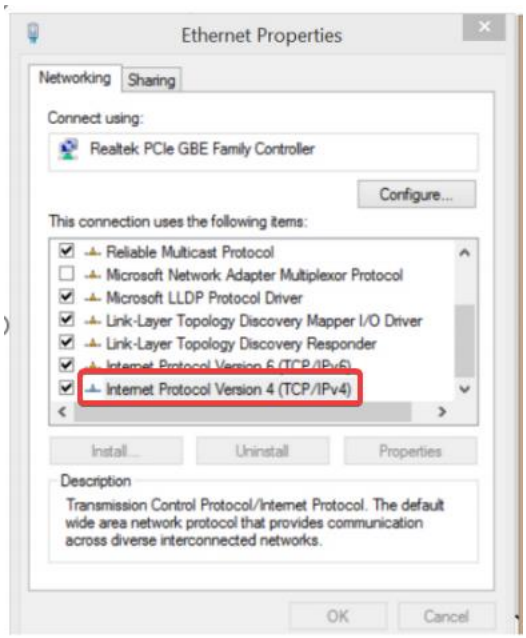
first step: Connect the computer to the LAN port of the CPE , right-click the network icon to open the network settings .



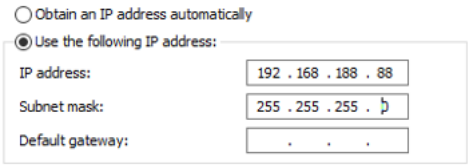


Step 2: Right-click Properties and double-click IPV4 :





Step 3: Change the IP address to the 188 network segment , press OK twice, and save. After debugging, change it back to automatically obtain the IP address.



3.3.Accessing the web management interface for the first time

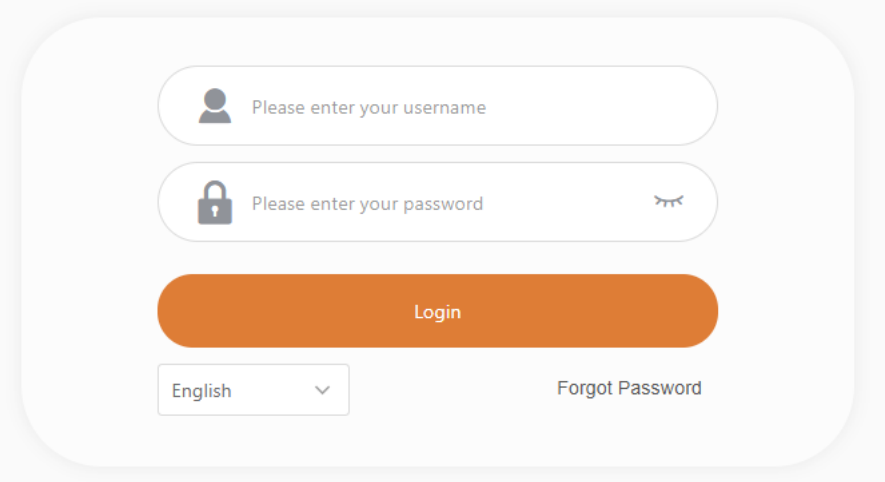
The steps to connect to the CPE device web management interface for the first time are as follows :

Step 1. Open your browser .

Step 2. Enter the device's IP address in the web browser address bar .

Step 3: Default administrator login username: **admin** , password: **admin**

The initial login interface is as follows :



Step 4 : After the administrator successfully logs in, he will see the main interface of the device web management interface. Now you can configure the device.

4. CPE Configuration

This document contains configuration descriptions for the product's powerful web management interface, ranging from very simple to very complex setups .

4.1. Apply and save configuration changes

In the upper right corner of the web interface there is a general button containing 4 actions that allow managing device configuration:

Save changes – If pressed new configuration settings are applied immediately and written to permanent device memory.

Testing Changes – Once pressed, the device will start operating with the newly set configuration for 3 minutes. During this test period, the administrator is able to evaluate whether the device is working properly and then save the changes. If the wrong setting is selected (even after the administrator loses connection with the device), the device automatically reverts to the old configuration.

Undo changes – If you press Parameter changes will be discarded. It should be noted that if you press Save changes, it is not possible to discard changes.

quit – If pressed, will log in again.

save changes in every web interface tab . The device remembers all changes and after each tab and action button all changes will be applied.

4.2. state

After logging in, the Web management interface displays the status information interface. The secondary menus under it mainly include: Information, Statistics, and Network .

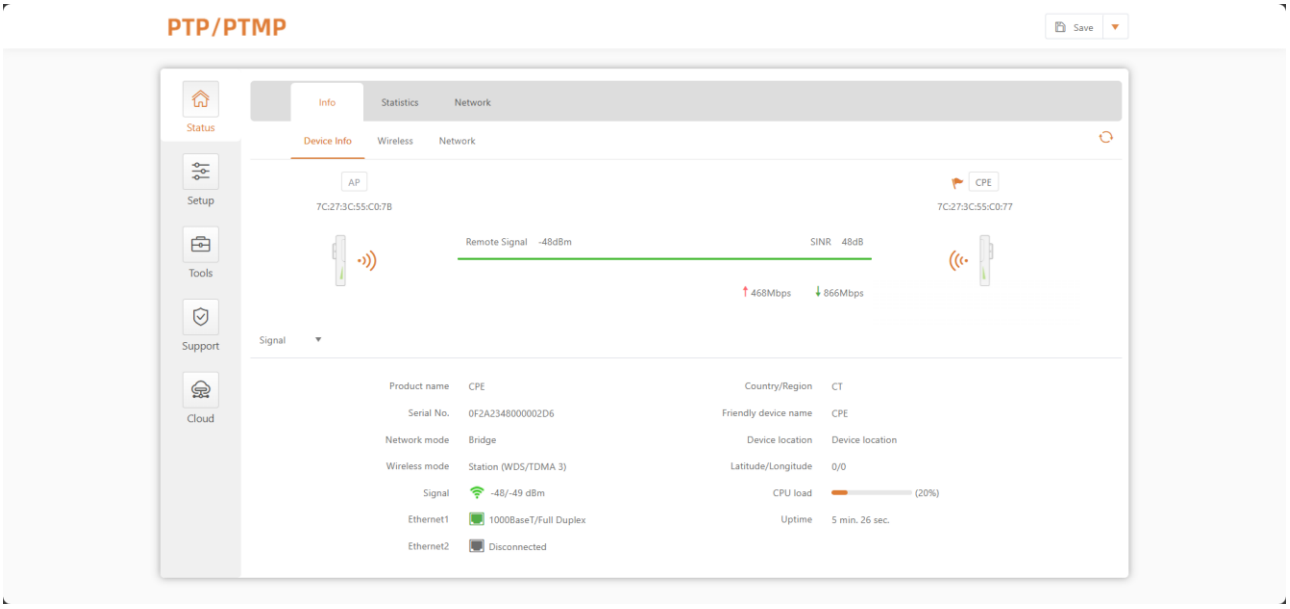


Figure 1 - Web management page

4.3.1. information

The Information page displays a summary of device status information. It shows important information about device information , wireless, and network settings.

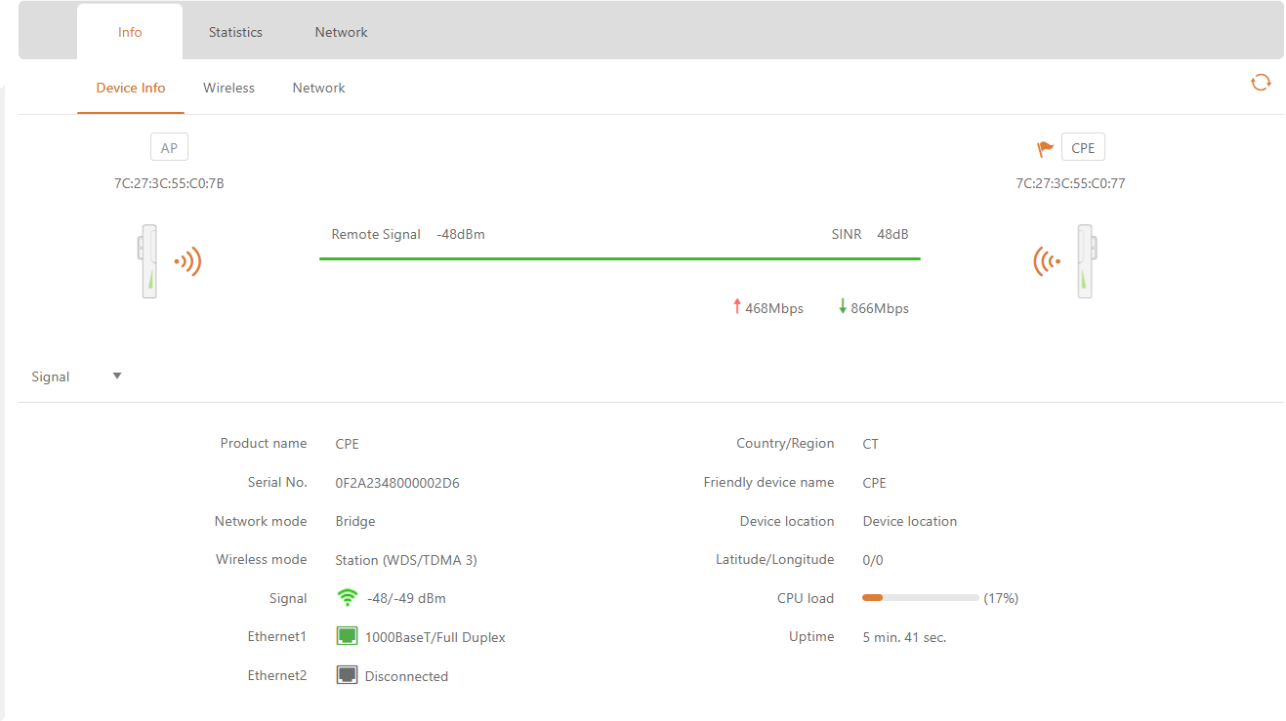


Figure 2 – Device Information Page

the Radio section on the information page will be divided into two tabs (2.4GHz and 5GHz Radio), each containing the corresponding information.

- **Device Information** – Display the equipment operation status and related information .
- **wireless** – Displays summary information about the radio interface configuration.
- **network** – Displays a brief summary about the current network configuration (bridge or router).

Click the refresh icon , in the upper right corner, to update information.

4.3.2. statistics

The statistics section id divided into two parts, showing the network interface counters and the traffic graphs for the wired and wireless interfaces respectively:

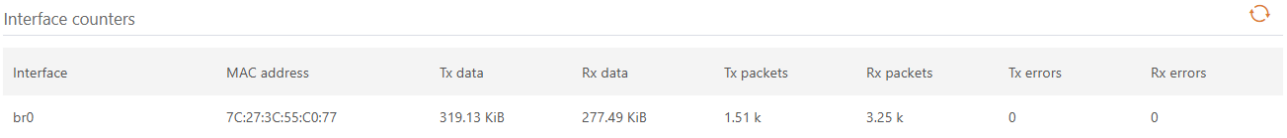


Figure 3 – Network Statistics : Interface Statistics

Network interface statistics – Displays the interface statistics table. The SSID name is displayed in brackets near the wireless interface (and VAPs).

MAC Address – Displays the MAC address of the specified interface

Tx Send Data – Displays the data sent .

Rx Receive Data – Displays the received data.

Tx Packets – Displays the number of packets sent.

Rx Packets – Displays the number of packets received .

Tx Errors – Displays the number of transmit errors.

Rx Errors – Displays the number of receive errors .

Graphical display of real-time data traffic for wired and wireless interfaces.

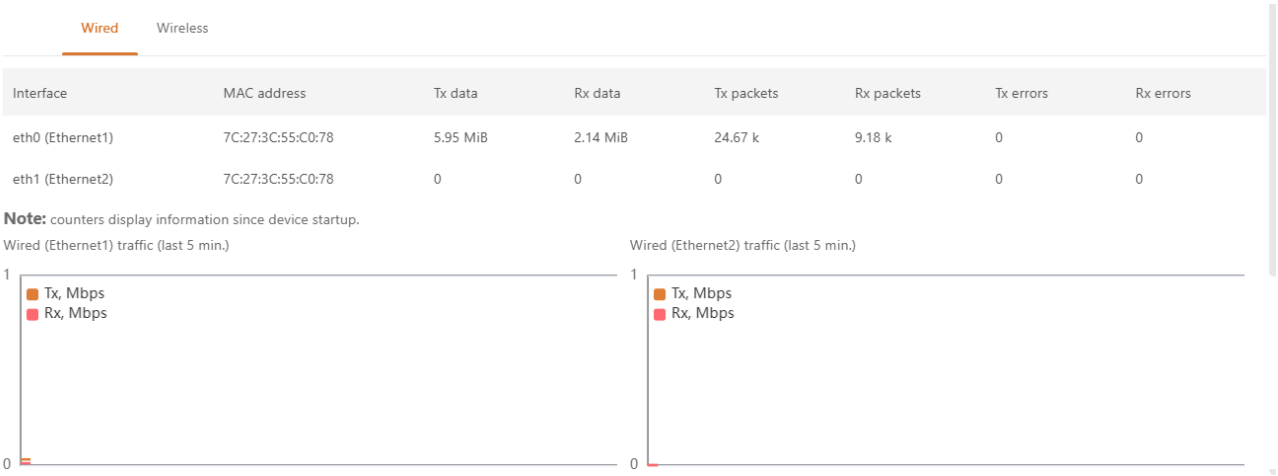


Figure 4 – Network Statistics: Graph

If the unit is operating in station mode , additional graphics of signal and noise levels will be displayed.

4.3.3. network

In the " **Network** " interface, you can view the networking information : routing table , ARP table and bridge MAC address table :

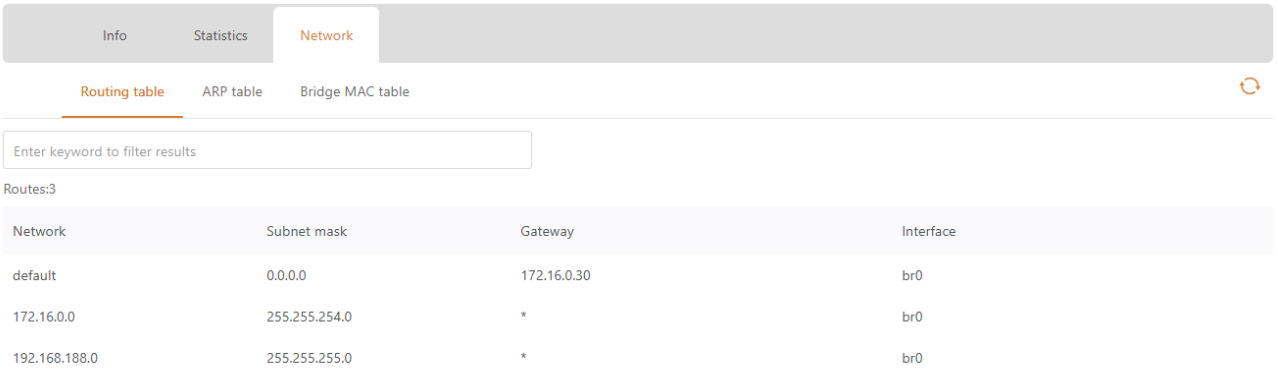
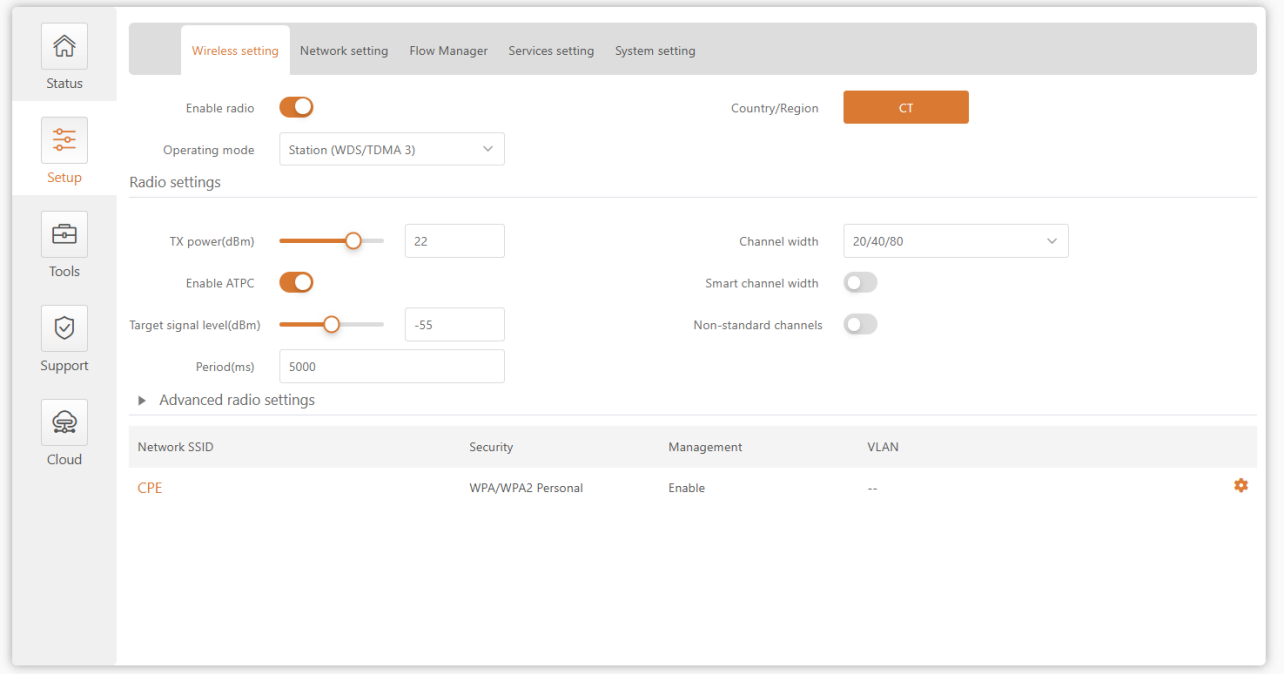


Figure 6 – Web form

4.4. set up



4.4.1. Network Configuration

Using the features of the Settings | Network Configuration interface, you can control the network configuration of the device.

4.4.1.1. Ethernet Settings

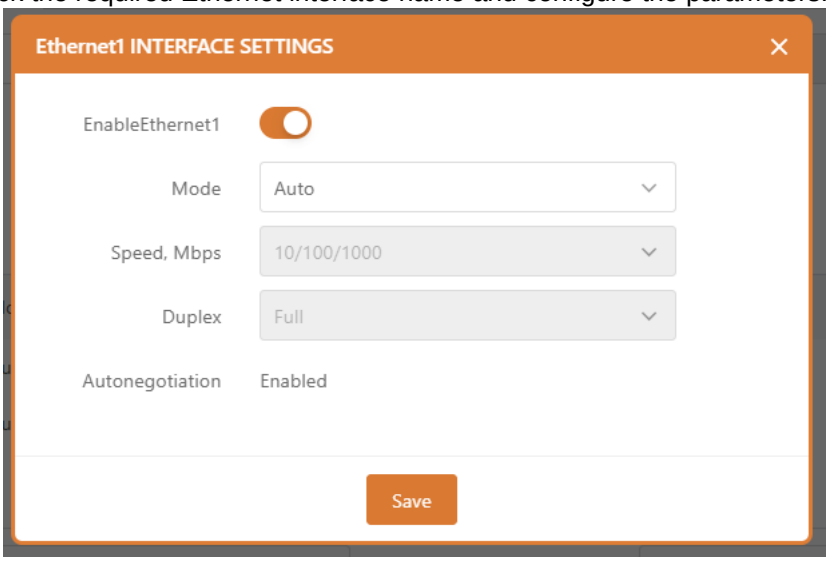
Ethernet interface can be configured through the Ethernet configuration table .

Ethernet settings

Interface	Mode	Speed, Mbps	Duplex	Autonegotiation
Ethernet1	Auto	10/100/1000	Full	Enabled
Ethernet2	Auto	10/100/1000	Full	Enabled

picture 7 – Ethernet Table

Click the required Ethernet interface name and configure the parameters:



picture 8 – Ethernet Configuration

model – Select the configuration mode for the Ethernet port:

- automatic
- Fixed
- advanced

Speed , Mbps – Select the Ethernet link speed for the specific Ethernet port.

Duplex – Select the duplex mode for the specific Ethernet port .

Auto Negotiation – Select Auto Negotiation to announce and negotiate the Ethernet link duplex configuration (half/full) for the highest possible data rate.

4.4.1.2. Bridge

When configuring the device in bridge mode, you only need to configure the device's LAN settings in the " **Network Configuration** " page:

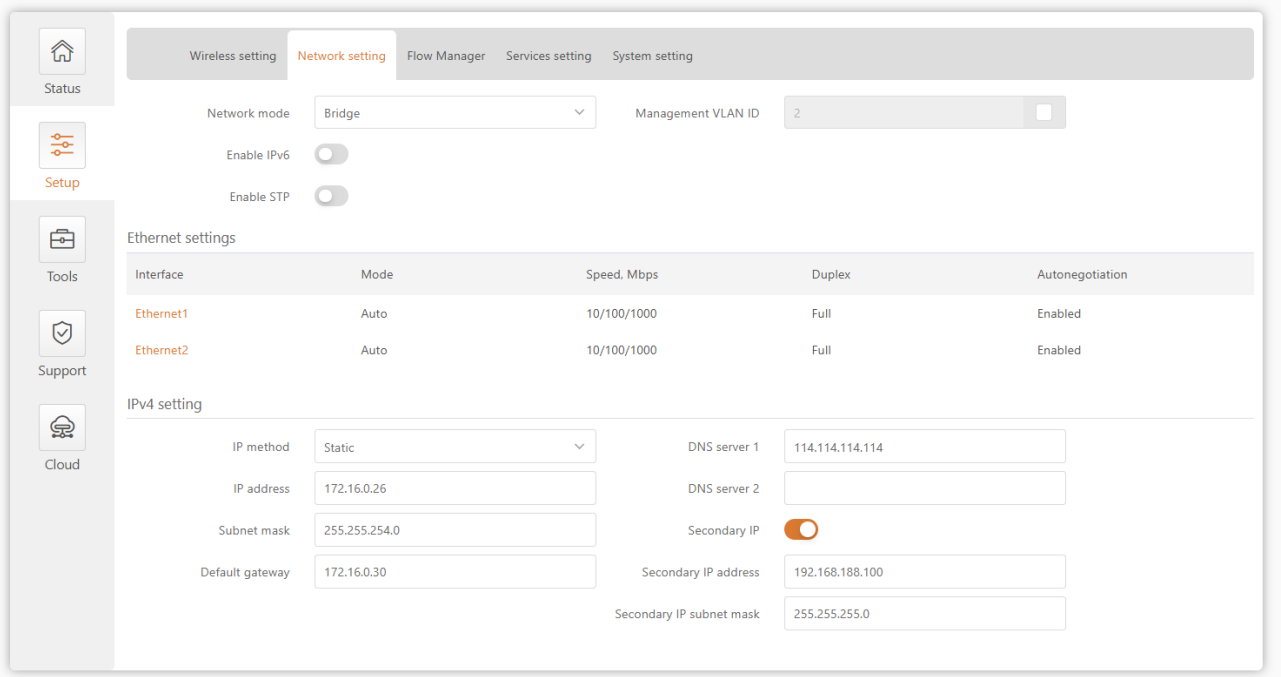


Figure 9 – Bridge Mode Settings

Enable Management VLAN – Enable VLAN tagging for management traffic. Using VLAN tagging, you can further restrict management access to the AP. By defining a management VLAN, the device will only accept management frames with the corresponding management VLAN ID. All other frames using any management protocol will be rejected.

Management VLAN ID – Please specify a VLAN ID [2-4095]. When a specific VLAN ID is configured on a device interface, only management frames matching the configured VLAN ID will be received by the device.

When you specify a new management VLAN, your HTTP connection to the device will be lost. Therefore, you should establish a connection between your management station and a port in the new management VLAN, or connect to the new management VLAN through a multi-VLAN router.

1.1.1.1.1.IPv4 Configuration

When assigning an IP address, make sure the IP address selected is unused and belongs to the same IP subnet as the wired LAN, otherwise you will lose connection to the device from your current PC. When the DHCP client is enabled, the browser will lose connection after saving it because the IP address assigned by the DHCP server is unpredictable.

IP Type – Specifies the IP receiving method: The IP address can be obtained from a DHCP server

or configured manually :

- **Static** – The IP address must be configured manually.
- **dynamic** – The IP address for this device will be assigned from a DHCP server. If a DHCP server is not available, the device will attempt to obtain an IP address. If that is unsuccessful, it will use the preconfigured fallback IP address. The fallback IP setting can be changed to a custom value.

IP Address – The IP address of the device

Subnet Mask –Specify the subnet mask of the device.

Default Gateway –Specify the gateway IP address of the device.

DNS Servers – Specify domain name servers.

Secondary IP – Specifies the secondary IP address and subnet mask for CPE management .

1.1.1.1.2.IPv6 Configuration

Click the **IPv6** tab to enable IPv6 configuration. The IPv6 settings will appear in the IPv6 Configuration section:

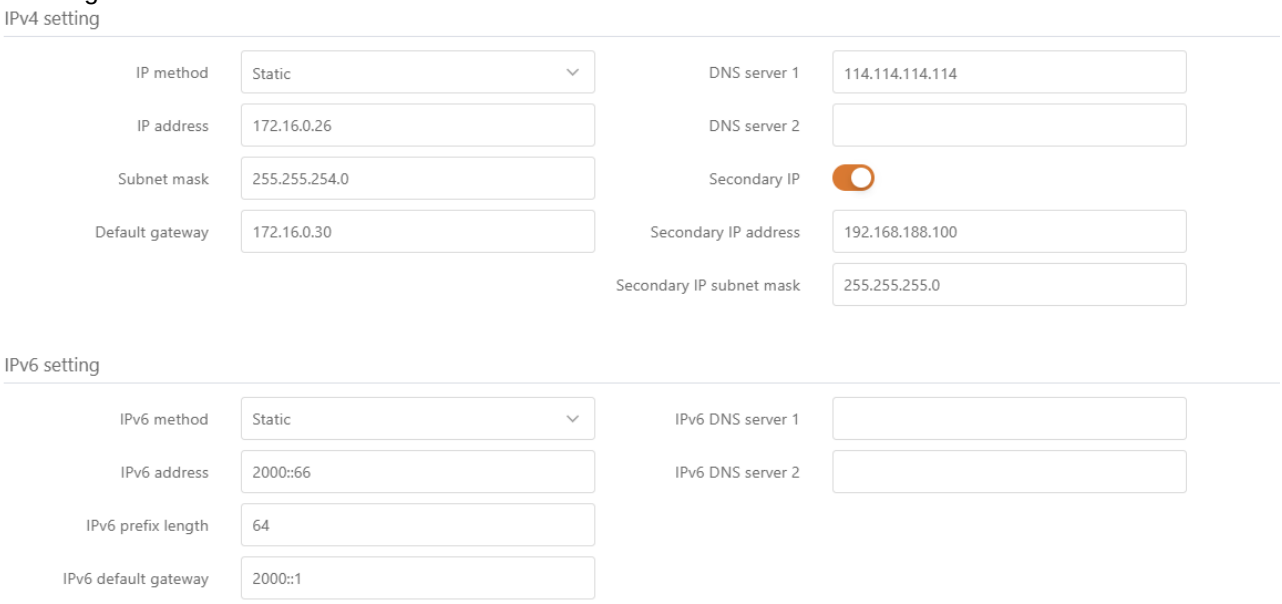


Figure 1.0 – Bridge IPV6 Setup

IPv6 Type – Specifies the IPv6 receiving method : The IPv6 address can be obtained from a DHCPv6 server or can be configured manually:

- **Static** – D HCPv6 client only obtains network parameters other than IPv6 address
- **dynamic** – The DHCPv6 client requires an IPv6 address and other network parameters (such as DNS server, domain name, etc.).
- **Static** – IPv6 addresses must be configured manually
  - **IPv6 Address** – Configure the **IPv6** address of the interface .
  - **IPv6 Prefix Length** – Enter **the prefix length for the address** .
  - **IPv6 Default Gateway** –Please specify the IPv6 address of the default gateway.
  - **IPv6 DNS Servers** – Specify the IPv6 addresses of the domain name servers.

4.4.2. Wireless Configuration

Before changing the radio settings, manually verify that your settings comply with local government regulations. At all times, it is the end user's responsibility to ensure that the installation complies with local radio regulations.

CPE devices have two wireless modes : access point (TDMA3) and station (WDS/TDMA3). TDMA3

wireless mode is a private protocol designed for point-to-multipoint wireless solutions. It uses a polling mode to effectively combat interference and improve wireless transmission performance.

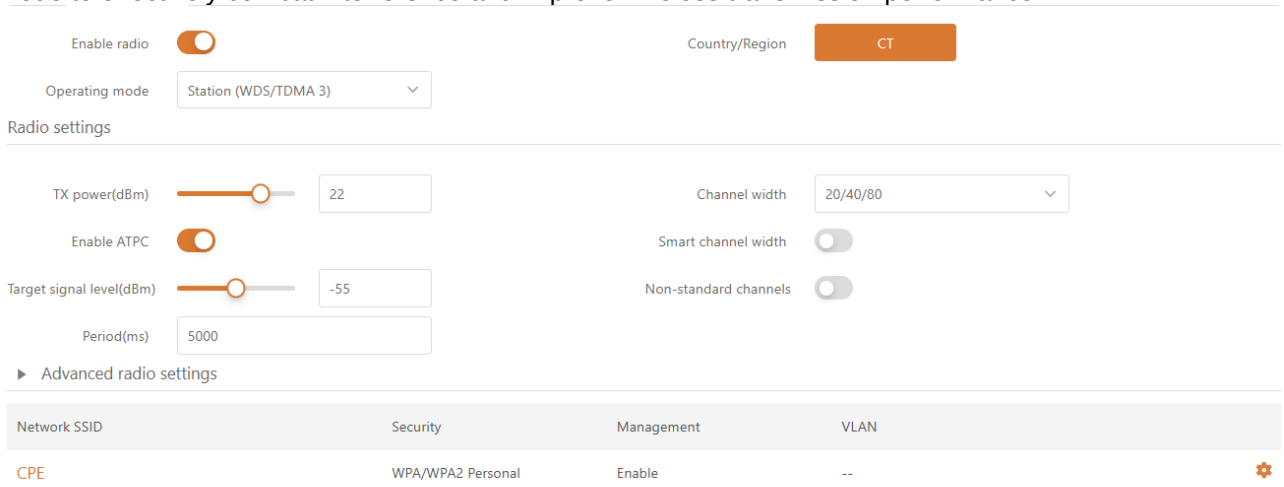


Figure 11 – Device wireless operation mode

If the CPE device is dual-band, the wireless configuration page will be divided into two tabs (for the 2.4GHz and 5GHz radios), each containing the corresponding wireless settings.

Depending on the wireless operating mode selected, some of the displayed configuration parameters may differ (such as security or advanced wireless settings).

Working Mode – Select wireless working mode:

- **Access Point (TDMA3)** – Enables the CPE to act as an access point (master bridge) to connect multiple wireless clients. Auto WDS mode allows wireless clients to connect with and without WDS (Layer 2 forwarding) enabled.
- **Wireless Client (WDS/TDMA3)** – In this wireless mode, the CPE is configured to act as a client (slave bridge) and connect to other wireless devices acting as access points.

4.4.2.1. Wireless Mode: Access Point

Access points and wireless clients must operate on the same frequency channel, using the same wireless bandwidth and the same security settings.

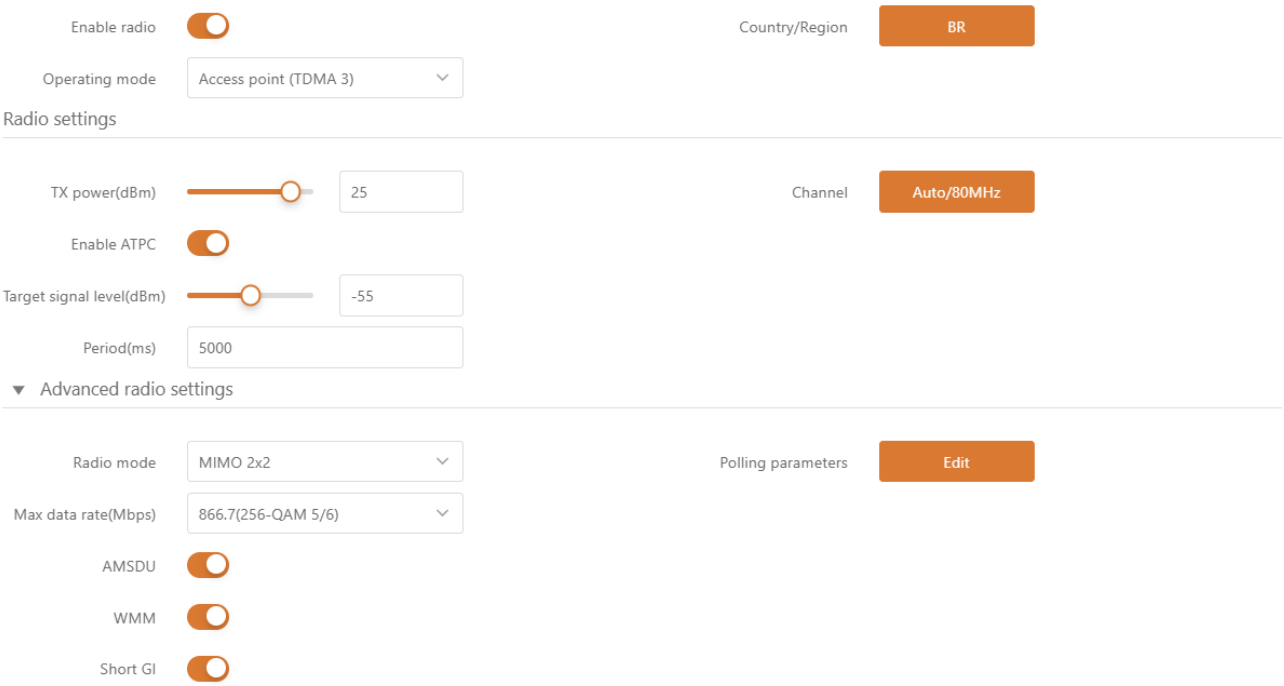


Figure 12 – Wireless Access Point Settings

Enable Radio – Enable or disable the CPE wireless switch .

nation – Displays the country in which the CPE Bridge is operating . The country selection determines the available channels, frequencies, and transmit power levels based on the regulatory restrictions of the country of operation. The country is selected during the first step of the CPE device installation, but can be updated if necessary.

IEEE Mode – Configure the wireless network mode [802.11a, 802.11n, 802.11a/n].

Transmit Power (dBm) – Sets the transmit power of the device when transmitting data. The greater the distance, the more transmit power is required. To set the transmit power level, use the slider or enter a value manually. When manually entering a transmit power value, the slider position changes based on the value entered. The maximum transmit power level is limited to the value permitted by the regulatory authority in the country where the device is operating.

ATPC – Select to enable Automatic Transmit Power Control (ATPC). If enabled, the CPE radio will continuously communicate with the remote device's radio to automatically adjust the optimal transmit power.

Channel – Displays the channel the AP is operating on , or click to use the automatic channel feature. Clicking the button will display the channel selection window:

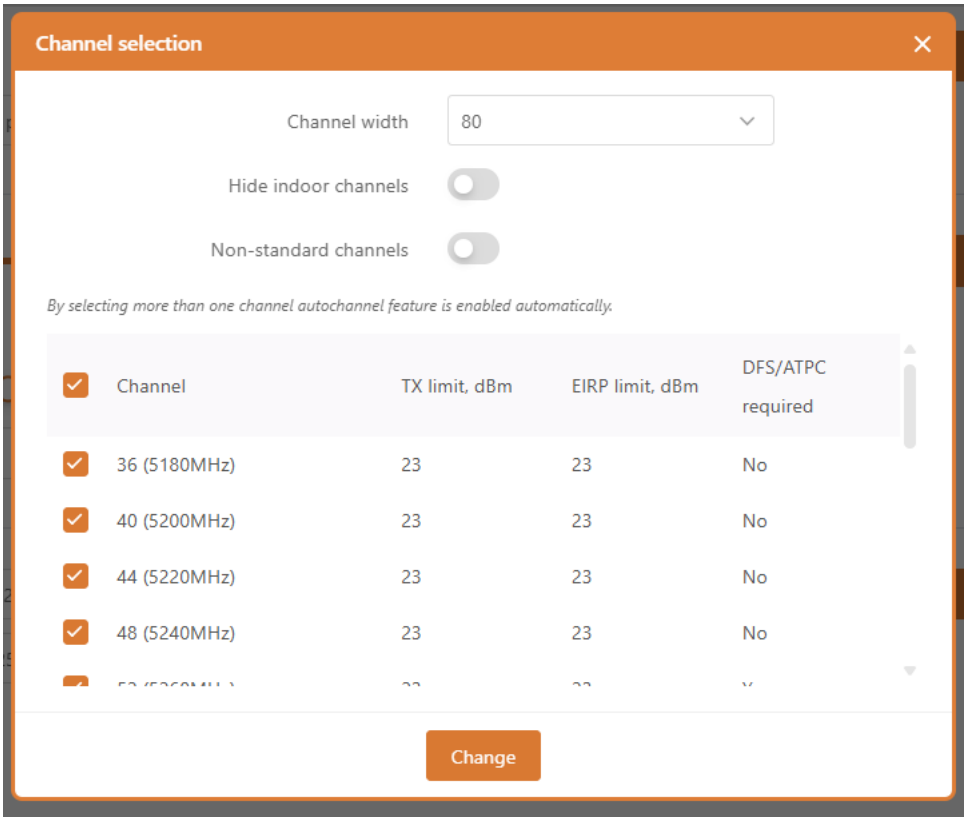


Figure 13 – Channel List

Channel Width – Select the width of the operating radio channel. The CPE supports 20, 40 and 80MHz channel widths.

Hidden indoor channel – Use the toggle to show outdoor channels only.

Non-standard channels – Select this option to enable non-standard channels . Non-standard channels have a 5MHz channel step size, so some center frequencies are invalid in the 802.11 specification. This feature may interfere with other networks and may not be supported by all A/N standard clients or access points.

The access point and station must have the same configured non-standard channel option ; otherwise, the channel connections will not match well due to interference .

Channel Table – Select the channel on which the access point will operate. If multiple channels are selected, the Auto Channel feature will be enabled. Auto Channel Selection allows the AP to select a channel that is not in use by any other wireless device, or if no free channels are available - select the least occupied channel. The table displays detailed information about each channel: TX Limit, EIRP Limit, and DFS or ATPC.

1.1.1.1.3. Radio Advanced Settings

Advanced parameters allow configuring the device to get the best performance/capacity for the link.

Max 802.11n MCS index – Select the maximum rate to specify the modulation and coding scheme (MCS) rate at which data can be transmitted between the access point and the client. If interference is encountered, the CPE will drop to the highest rate allowed for data transmission. Applicable only in 802.11n or 802.11a/n IEEE mode.

Max data rate, Mbps: – Select the maximum data rate (in Mbps) at which the AP should transmit packets. The AP will attempt to transmit at the highest data rate set. If interference is encountered, the CPE will drop to the highest rate allowed for data transmission. Applies only to 802.11a or 802.11a/n IEEE modes.

AMSDU – Enables AMSDU packet aggregation. If enabled, the maximum size of 802.11 MAC frames will be increased. Applicable only in 802.11n or 802.11a/n IEEE mode.

Short GI— Enables short interval packet transmission, which can significantly improve network speed when data interference is small.

Polling - Support setting TDMA intelligent polling parameters

1.1.1.1.4. AP Wireless Settings

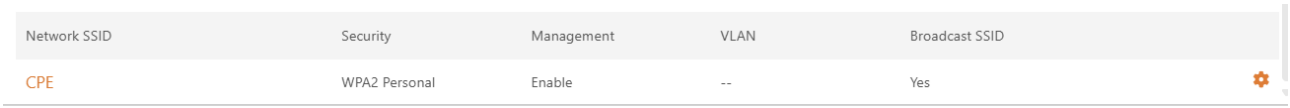


Figure 14 - Wireless Settings

Click the icon  You can edit the AP wireless settings:

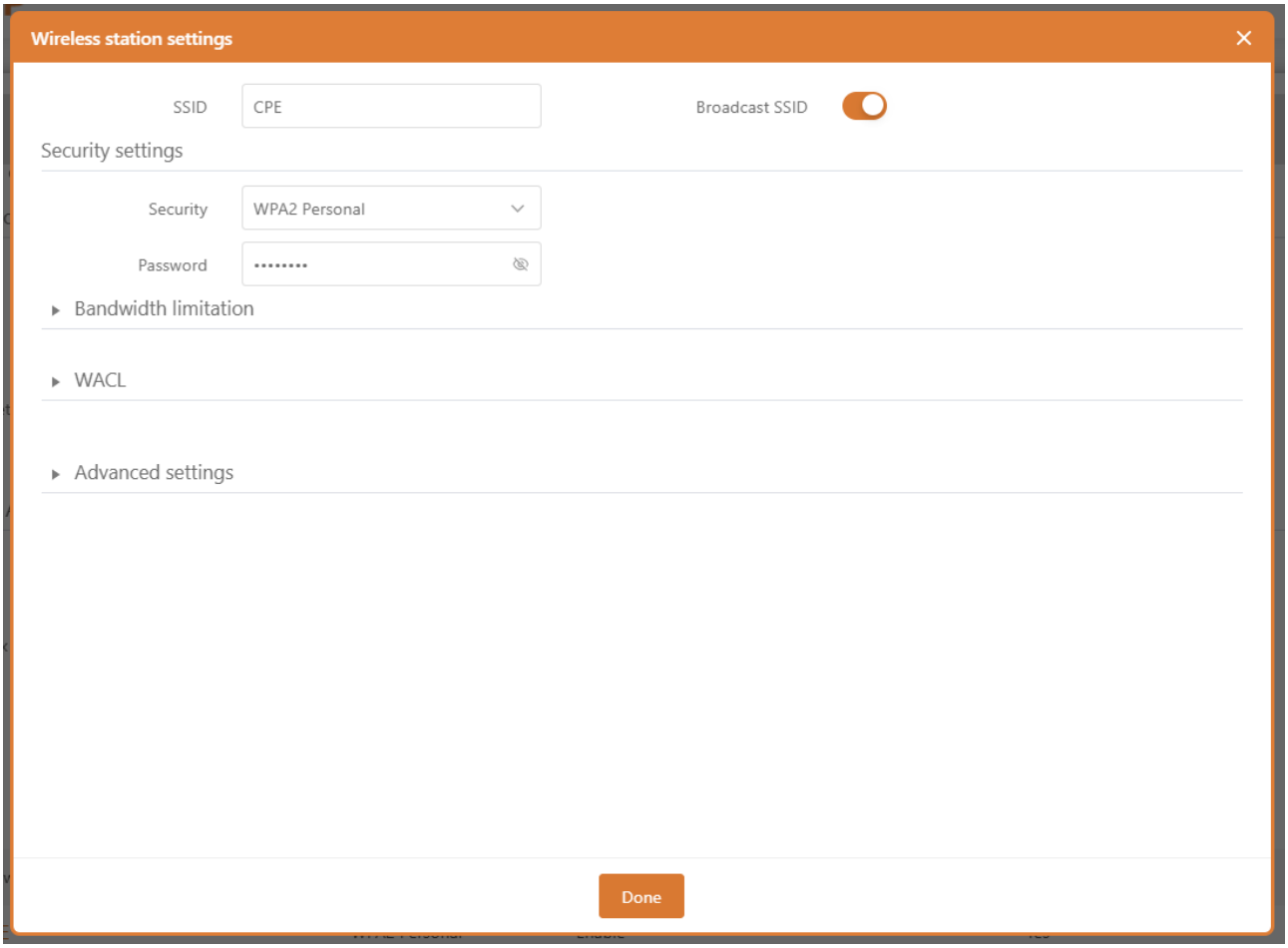


Figure 15 – Wireless Settings

SSID – Specifies a unique name for a wireless network device. The device will broadcast messages to all stations within range, advertising this SSID.

Broadcast SSID – If this option is disabled, the CPE device will not broadcast its SSID to station devices.

For more information on **bandwidth limiting** and **WACLs** , refer to the appropriate Wireless Security and Wireless ACLs sections.

1.1.1.1.4.1. Advanced settings:

User Isolation – Select to enable Layer 2 isolation that prevents clients from communicating with each other.

Business VLAN ID – Specifies the VLAN ID for traffic tagging on a specific VAP interface. Devices associated using a specific SSID will be grouped into this VLAN. Mapping to Data VLAN ID is not available if the device is operating in Router Network Mode.

Maximum Client Connections - Specifies the maximum number of associated wireless clients on the AP radio.

Minimum client signal, dBm - If enabled, the AP will disconnect clients that fall below the configured threshold.

Manage Over the Air – Controls wireless management access. For security reasons, it is recommended to disable wireless access and require a physical network connection using an Ethernet cable for management access to the CPE. Wireless management is not possible if the device is operating in router network mode.

Multicast Enhancement – If clients do not send IGMP (Internet Group Management Protocol) messages, they do not register as receivers of multicast traffic. Using IGMP snooping, the Multicast Enhancement option isolates multicast traffic from unregistered clients and allows the device to use a higher data rate to send multicast traffic to registered clients. This reduces the risk of traffic overload on the PtMP link and improves the reliability of multicast traffic because packets are transmitted again if the first transmission fails. If clients do not send IGMP messages but should receive multicast traffic, you may want to disable the Multicast Enhancement option. This option is enabled by default.

4.4.2.2. Wireless Mode: Site (WDS/ TDMA 3)

In this wireless mode, the CPE will operate as a wireless station.

Wireless Configuration sets up the wireless interface of the device .

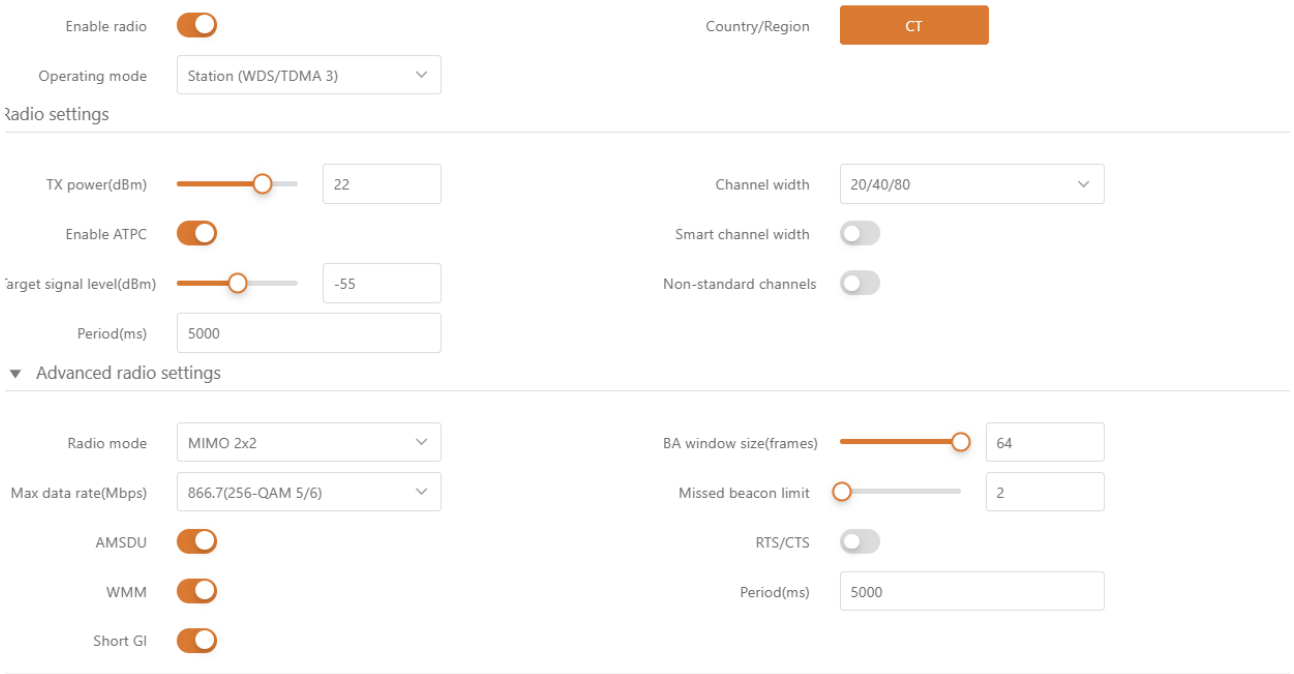


Figure 16 – Site Wireless Settings

Enable Radio – Use the switch to enable or disable the CPE radio.

nation - Displays the country in which the CPE Bridge is operating . The country selection

determines the available channels, frequencies, and transmit power levels based on the regulatory restrictions of the country of operation. The country is selected during the first step of the CPE device installation, but can be updated if necessary.

Transmit Power (dBm) – Sets the transmit power of the device when transmitting data. The greater the distance, the more transmit power is required. To set the transmit power level, use the slider or enter a value manually. When manually entering a transmit power value, the slider position changes based on the value entered. The maximum transmit power level is limited to the value permitted by the regulatory authority in the country where the device is operating.

ATPC – Select to enable Automatic Transmit Power Control (ATPC). If enabled, the CPE radio will continuously communicate with the remote unit's radio to automatically adjust the optimal transmit power.

Channel Width -Select the width of the operating radio channel. The CPE supports 20 and 20/40/80MHz channel widths.

Intelligent channel bandwidth – Select Enable Smart Channel Width on the site . Enabling this option allows the CPE station to automatically change the channel width whenever a connection to the AP is established if the connection to the AP is unsuccessful.

1.1.1.1.5. Radio Advanced Settings

Advanced parameters allow configuring the device to get the best performance/capacity for the link.

Max 802.11n MCS index – Select the maximum rate to specify the modulation and coding scheme (MCS) rate at which data can be transmitted between the access point and the client. If interference is encountered, the CPE will drop to the highest rate allowed for data transmission. Applicable only in 802.11n or 802.11a/n IEEE mode.

Max data rate, Mbps: – Select the maximum data rate (in Mbps) at which the AP should transmit packets. The AP will attempt to transmit at the highest data rate set. If interference is encountered, the CPE will drop to the highest rate allowed for data transmission. Applies only to 802.11a or 802.11a/n IEEE modes.

AMSDU – Enables AMSDU packet aggregation. If enabled, the maximum size of 802.11 MAC frames will be increased. Applicable only in 802.11n or 802.11a/n IEEE modes.

Short GI— Enables short interval packet transmission, which can significantly improve network speed when data interference is small.

Lost Beacon Limit - This parameter is used to set the maximum number or time range of lost beacons allowed. When a wireless device (such as a Wi-Fi client) receives beacons, if a certain number of beacons are lost within the specified limit, some actions may be triggered, such as attempting to reconnect, adjusting the reception sensitivity, or warning the user.

RTS/CTS —When the function is turned on, before sending data, the sender will first send an RTS frame to request to send data. If the receiver can receive data, it will reply with a CTS frame to indicate that it is allowed to send. The exchange of these two frames can let other devices around (including hidden nodes) know that the channel is about to be occupied, thereby avoiding conflicts.

1.1.1.1.6. Basic Wireless Site Setup

The Wireless table allows configuration of key parameters such as SSID, security and advanced settings of the AP unit.

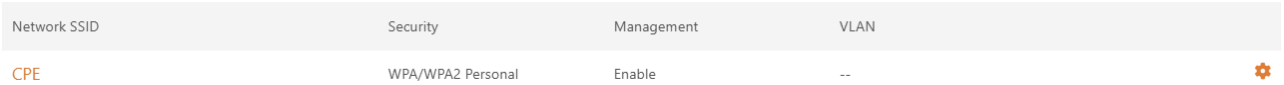


Figure 17 - Wireless Settings

Click the Edit icon The Wireless Settings window will be displayed:

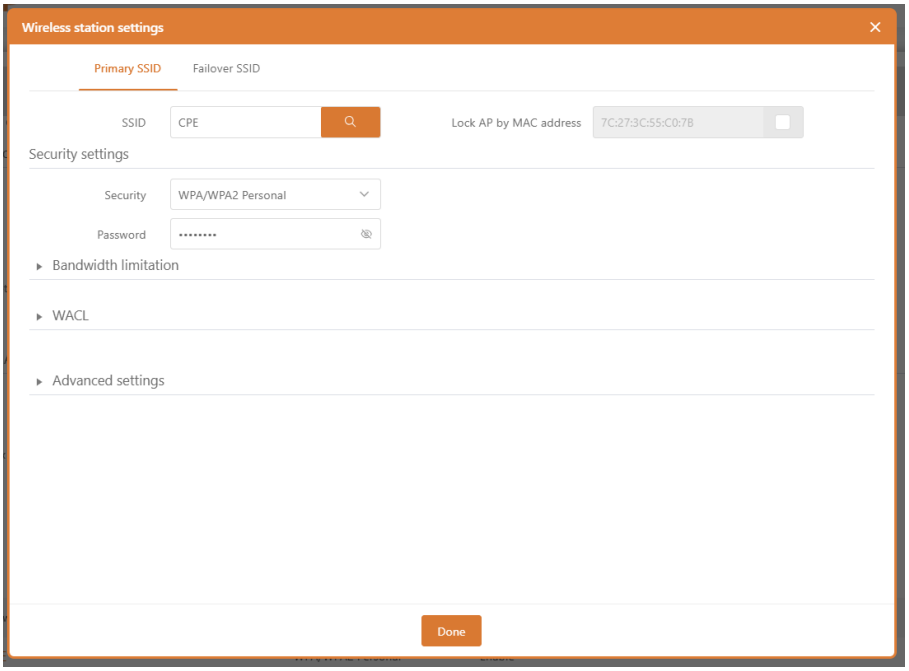
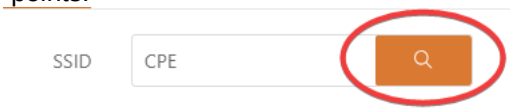
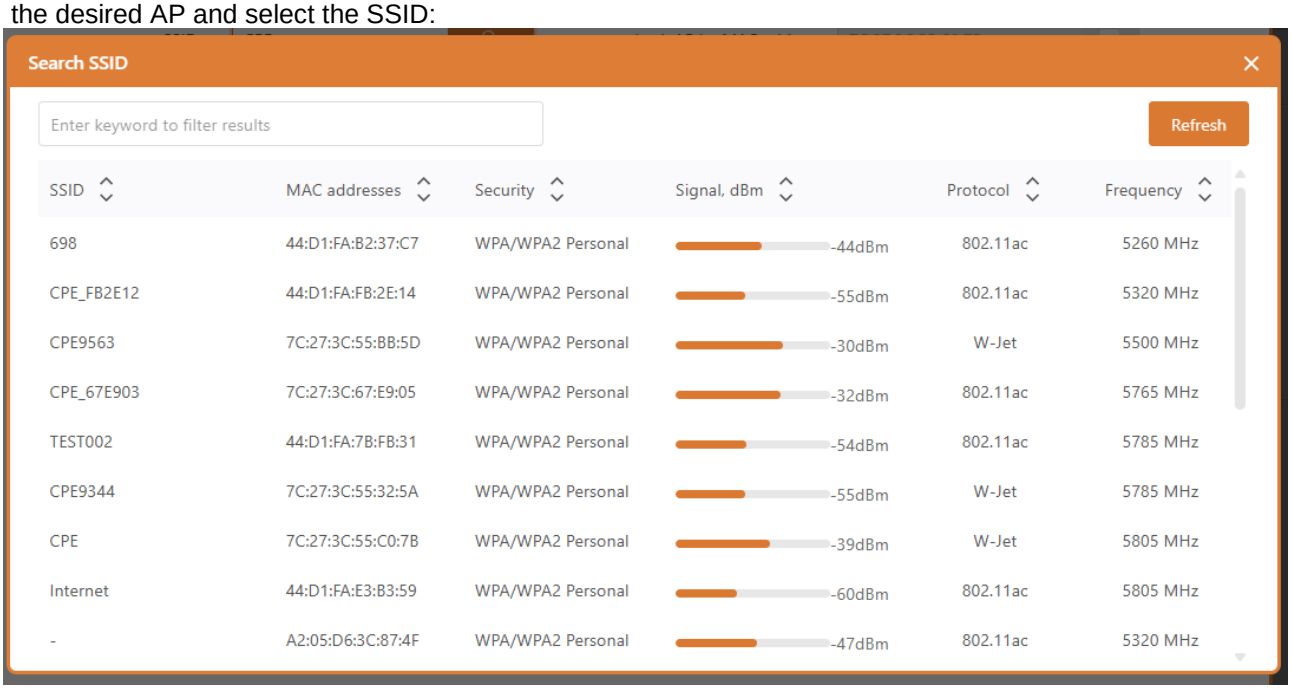


Figure 18 – Wireless AP Setting

SSID – Manually specify the SSID of your wireless network device, or automatically scan for access points:



If you used automatic SSID scanning, the results will appear in the Search SSID table, so just click on the desired AP and select the SSID:



Lock AP by MAC address – Select the check box and specify the MAC address of the desired access point to prevent roaming between access points with the same SSID.

For more information on **security settings** , see the appropriate wireless security section.

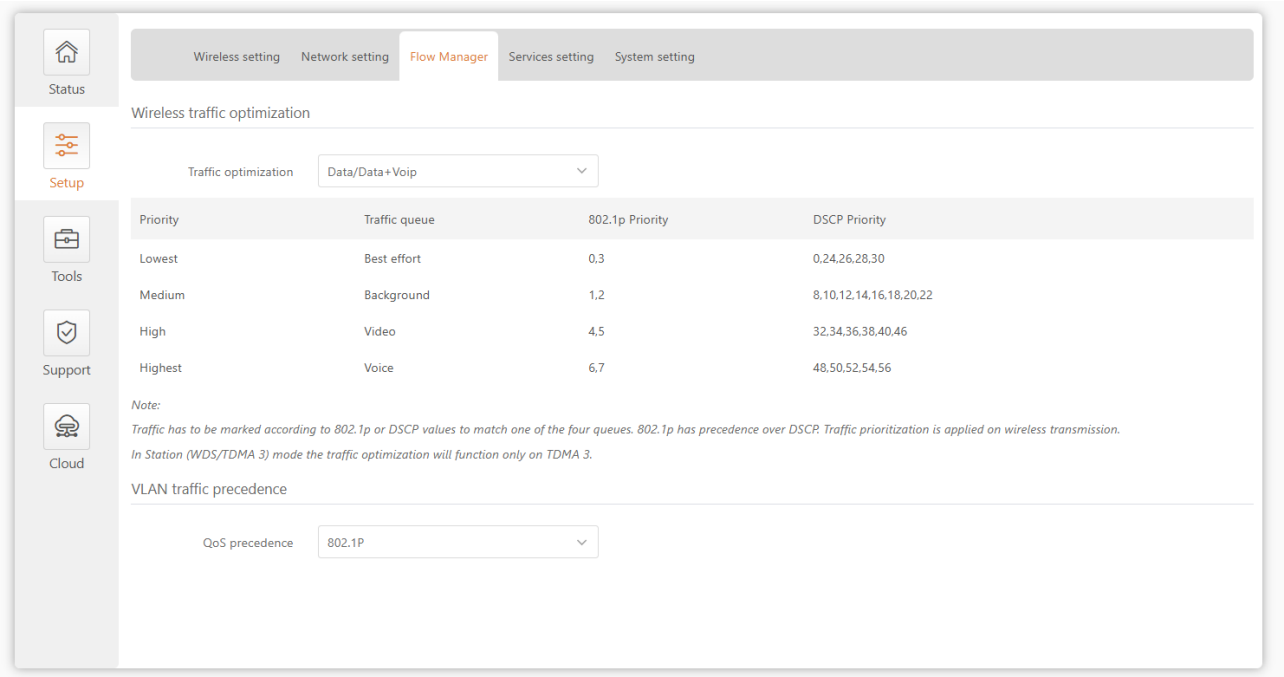
1.1.1.1.7. Advanced AP Settings

Service VLAN ID – Specifies the VLAN ID for traffic tagging on a specific radio interface. Station devices associated with a specific SSID will be grouped into this VLAN.

Wireless management – Control wireless management access. For security reasons, it is recommended to disable wireless access and require a physical network connection using an Ethernet cable for management access to the CPE.

4.4.3. Traffic Management

View and select traffic optimization solutions



4.4.4. Service Configuration

The Services menu is further divided into nine sections:

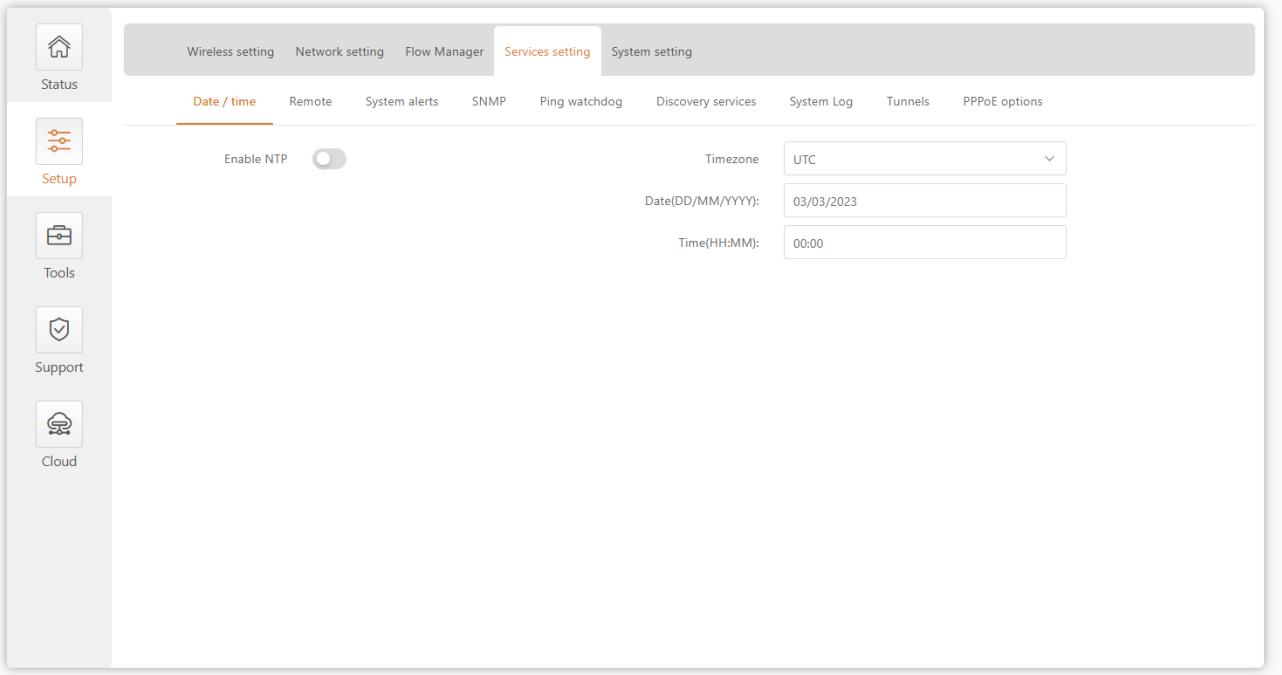


Figure 19 - Service Configuration Menu

- Date and time

Use this section to automatically manage the system time and date on the device using the Network Time Protocol (NTP), or to manually manage the system time and date by setting the time and date on the device.

The NTP (Network Time Protocol) client synchronizes the device's clock with a defined time server. Select NTP from the Configuration menu, select your time zone and enter the NTP server to use the NTP service.

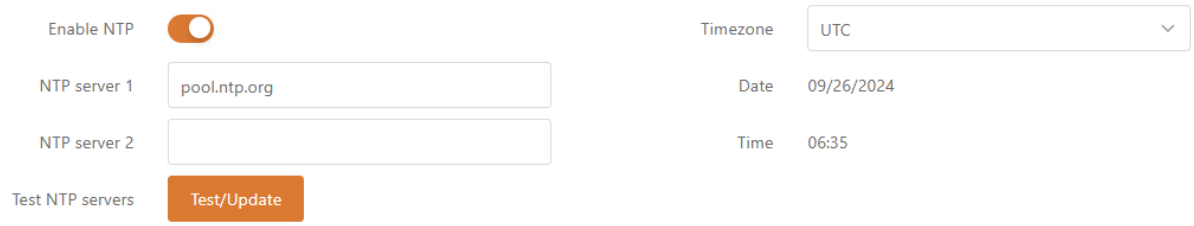


Figure 20 – Date and Time: NTP Configuration

Enable NTP – Select this option to enable configuring NTP.

Time Zone– Select a time zone. The time zone should be specified as the difference between local time and GMT time.

NTP Server – Specify the IP or hostname of a trusted NTP server for time synchronization.

Test NTP Server - Click this button to check if the specified server responds successfully.

To adjust the clock settings manually, disable the NTP option and specify the following settings:

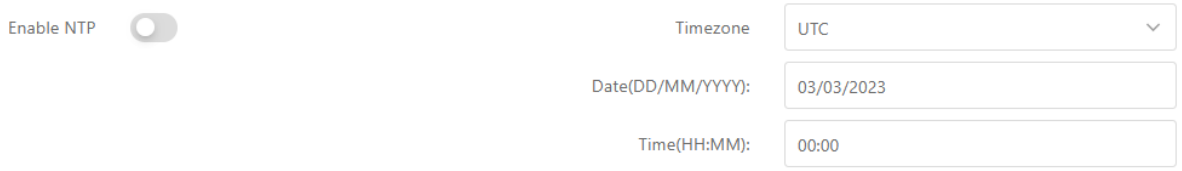


Figure 21 – Date and time: Manual Configuration

- ## Remote Management

Use this menu to manage access to the CPE via SSH, Telnet, and HTTP:

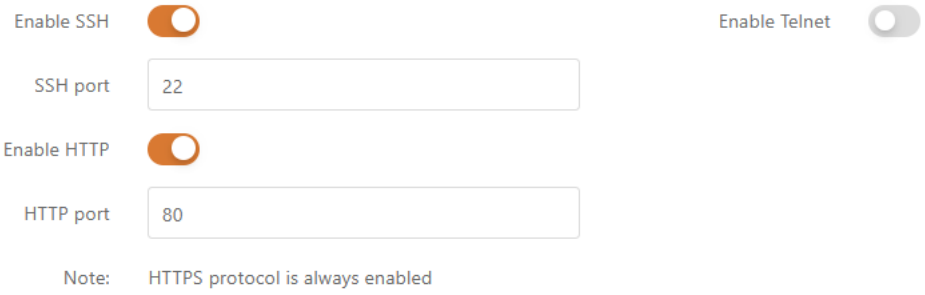


Figure 22 – Remote Management Configuration

Enable SSH – Enables or disables SSH access to the device.

SSH Port – Specify the SSH service port. The default SSH port is 22.

Enable telnet – Enable or disable telnet access to the device (factory default is off) .

Telnet Port – Specify the Telnet port. The default SSH port is 23.

Enable HTTP – Select the switch to enable or disable HTTP access to device management.

HTTP Port – Specify the HTTP port. The standard HTTP port is 80.

HTTPS connections are always enabled over the standard port 8080.

- ## SNMP

SNMP is a standard protocol widely used for remote network management over the Internet. When

SNMP is enabled, the CPE device acts as an SNMP agent. The SNMP agent uses the Simple Network Management Protocol to provide a device monitoring interface, allowing network administrators to monitor network performance and discover and resolve network problems.

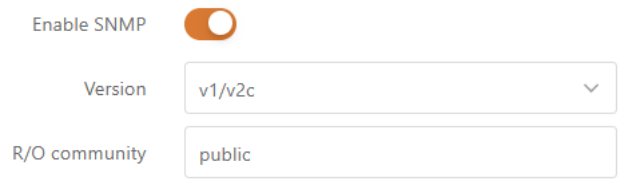


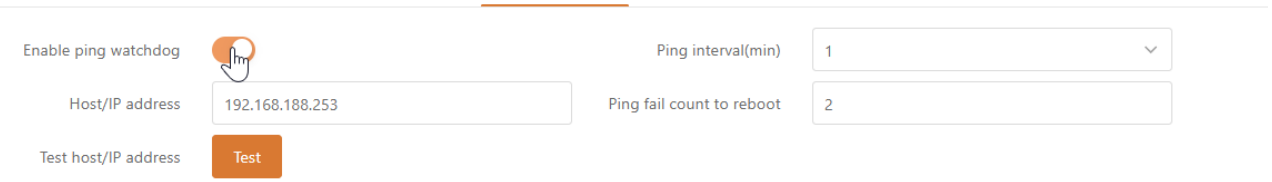
Figure 23 – SNMP Server Settings

Enable SNMP – Specifies the SNMP service status.

R/O Community – Specifies the read-only community name for SNMP Version 1 and Version 2c . The read-only community allows the CPE unit administrator to read the value but denies any attempt to change the value.

Ping Watchdog

Enable Ping Watchdog to continuously monitor the network connection between the CPE unit and the specified trusted host. If enabled, the CPE unit will periodically send Ping requests to the host, and if there is no response within the specified time period, Ping Watchdog will restart the CPE unit .



` *Figure 24 – Ping Watchdog*

Enable Ping Watchdog – Click to enable the Ping Watchdog feature.

Host /IP Address – Specifies the host to which the Ping request will be sent.

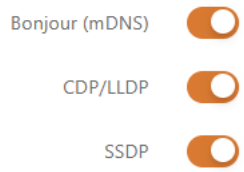
Test Host /IP Address - Click this button to check if the specified host responds successfully.

Ping Interval - Specify the time interval between ping requests in minutes.

Ping packet failure times -Specify the count of failed ping replies. After the specified number of ping failures, the CPE unit will automatically reboot.

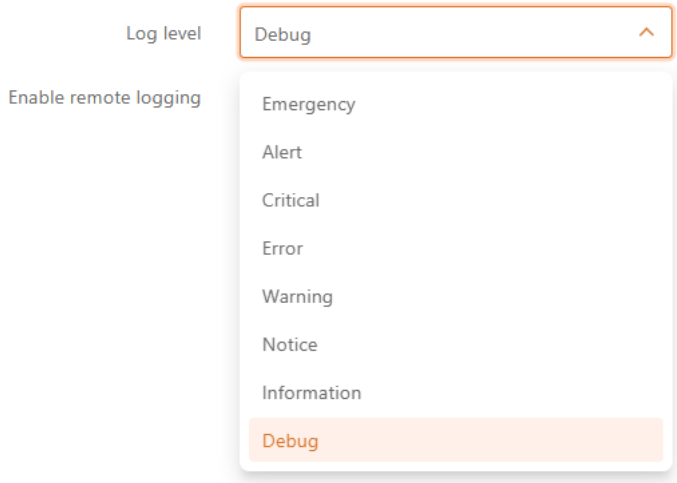
Discovery Services

The corresponding automatic discovery service is enabled by default.

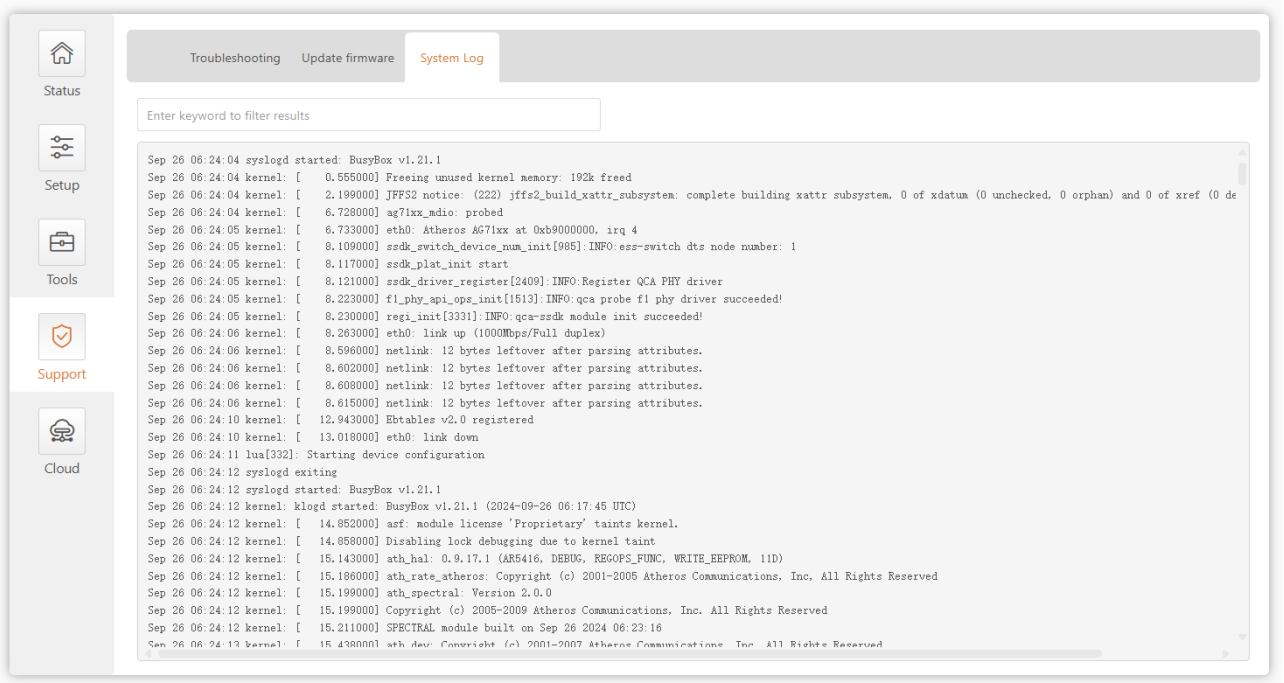


System log

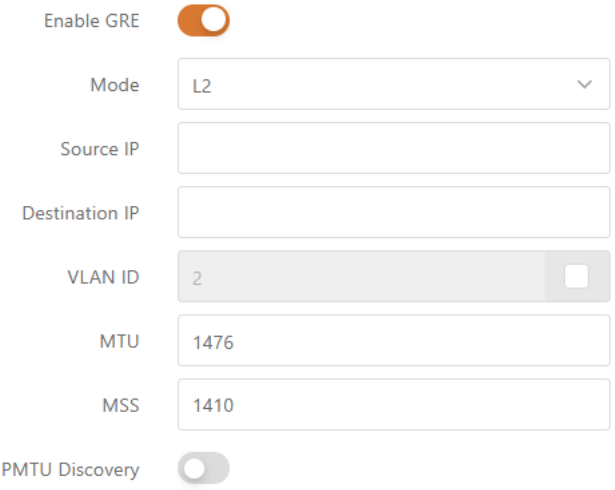
The corresponding log is selected by default and displayed in Support--System Log, where debug is the most detailed log level.



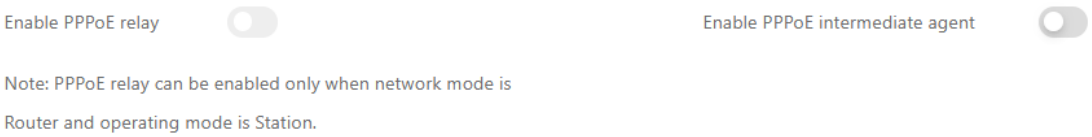
Log results:



- tunnel



- PPOE



4.4.5. System Configuration

The System menu allows you to manage main CPE settings and perform main system operations (reboot, restore configuration, etc.). This section is further divided into four parts:

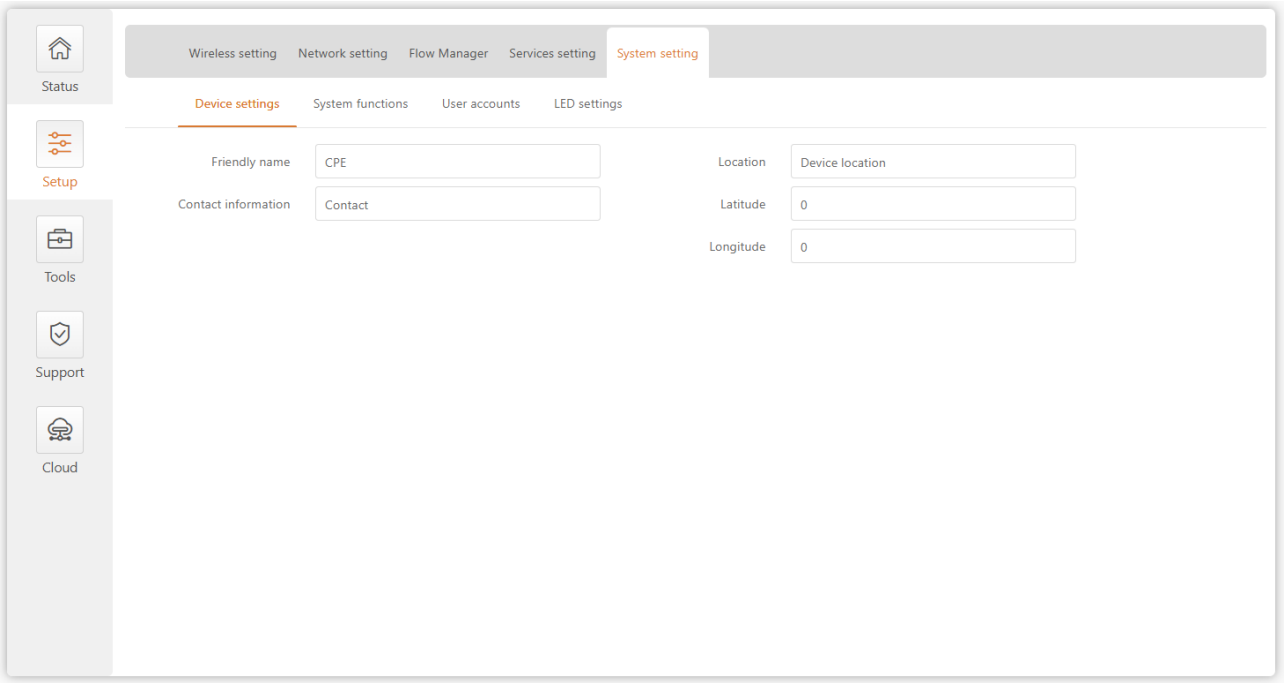


Figure 25 - System Configuration Menu

- Device Information Settings

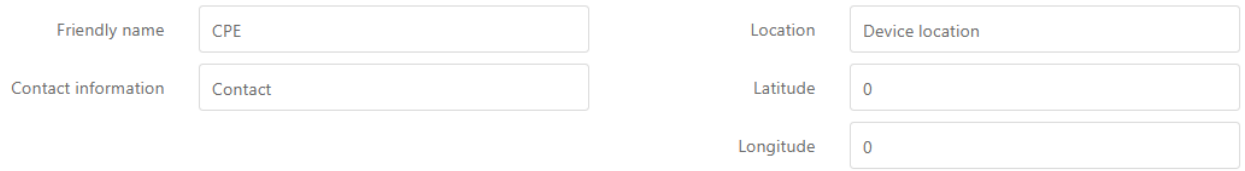


Figure 26 - Device Information Settings

Device Name –Specify the name of the CPE that will be used to identify the device .

contact information – Specify the contact name for the CPE, such as a network administrator.

Location – describes the physical location of the device.

longitude – Specifies the longitude coordinate of the device [in a specific decimal format, such as 114.03].

latitude –Specifies the latitude coordinate of the device in a specific decimal format, such as 22.32 . Both coordinates help indicate the exact location of the device.

- Equipment system function

Figure 27 - Device system functions

Backup Configuration – Click to save the current configuration file. The saved configuration file can be used to recover the configuration in case of a device configuration error or to upload a standard configuration to multiple devices without manually configuring each device through the web interface.

Restore Configuration – Click to upload an existing configuration file to the device. After the configuration file is uploaded, the new configuration will take effect after clicking the Save Changes button.

Restart your device – Restart the device using the last saved configuration .

Restore default configuration – Click to restore the device to factory configuration.

Resetting the device is an irreversible process. The current configuration and administrator password will be restored to the factory default settings.

- ## User Account Management

For security reasons, it is recommended to change the default administrator username and password as soon as possible.

Use this section to modify CPE device user access credentials to prevent unauthorized device configuration.

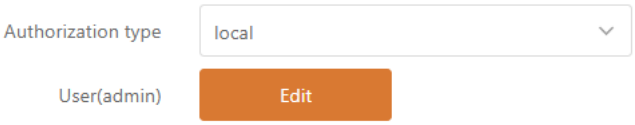


Figure 28 – User Account Management

The default administrator login settings are:
username: **admin**
password: **admin**

Click **Edit** to enter the editing window:

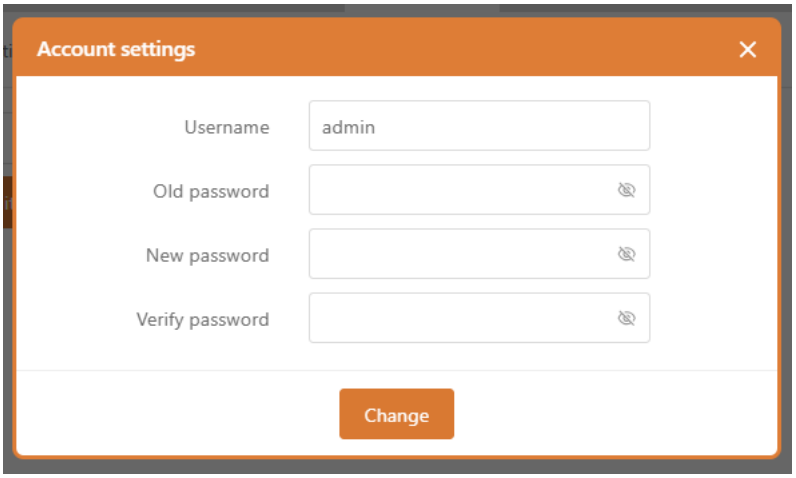


Figure 29 – User Account Settings

Username – Change the administrator's username.

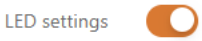
Old Password –Enter the current administrator password.

New Password –Enter a new administrator password for the user account.

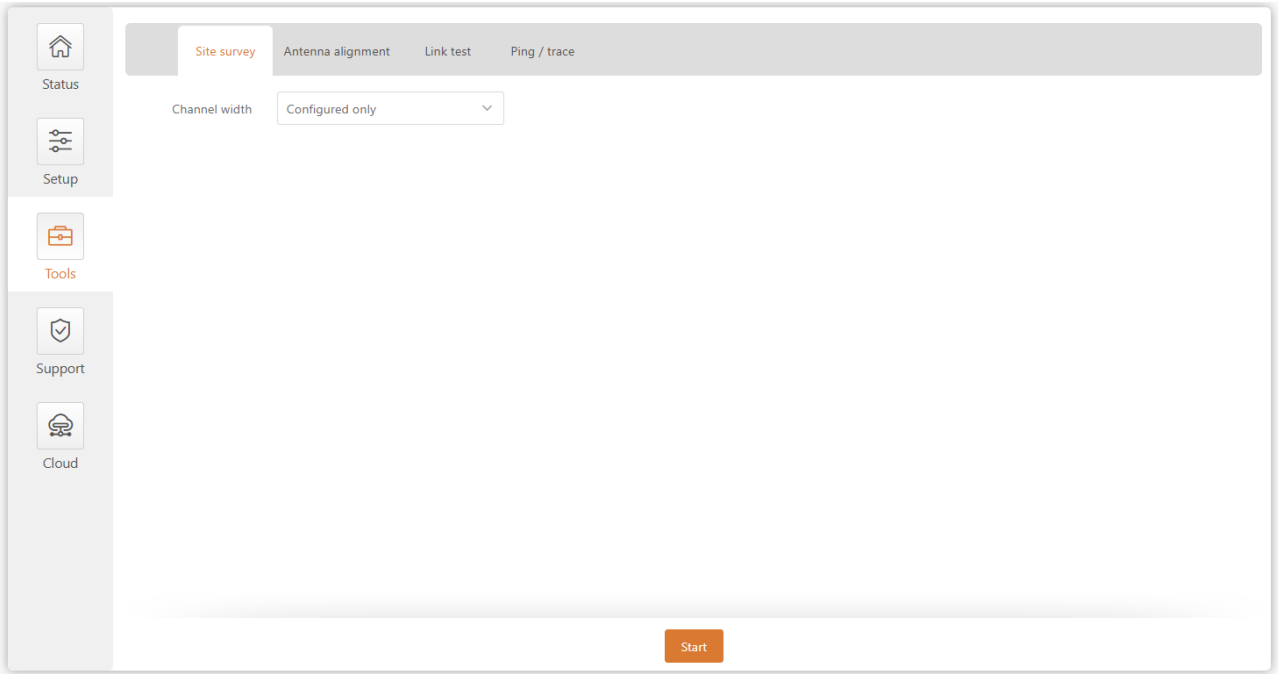
Confirm Password – Re-enter your new password to verify its accuracy.

If you forget the administrator password, the only way to access Web Management is to reset the device to factory defaults.

- LED Settings



4.5. tool



4.6.1. Wireless environment survey

The Site Survey Tool displays an overview of wireless networks in the local geographic area. Using this test, administrators can scan for active wireless devices, check their operating channels, encryption, and view signal/noise levels.

To perform a site survey test now, click **Start Scan** :

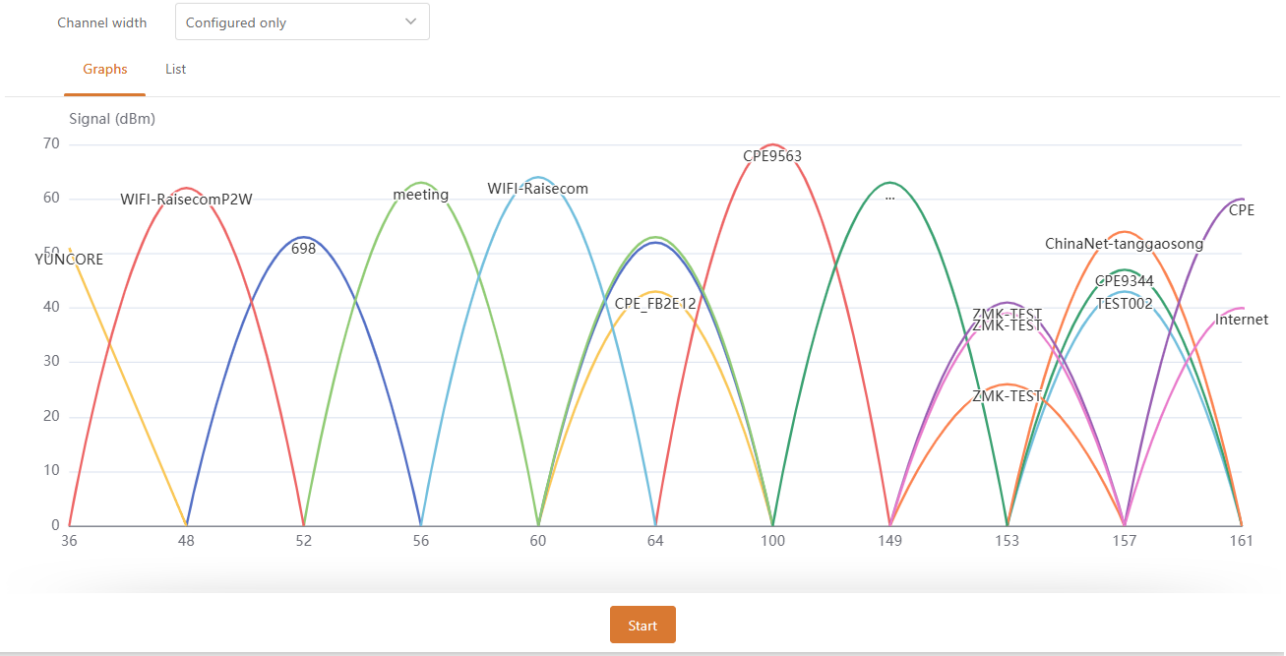


Figure 33 – Site survey results

bandwidth – Select the channel width over which the scan will be performed:

- **Configuration only** – With this option, the scan will be performed on the configured channel width (see the Status | Information page indicating the operating channel width)
- **All possibilities** – With this option, the scan will be performed on all available channel widths [5/10/20/40 /80]

Start Scan – Click to start scanning.

4.6.2. Antenna calibration

The Antenna Alignment Tool measures the signal quality between the base station and the AP. For best results during the antenna alignment test, turn off all wireless networking equipment within range of the device, except for the device you are trying to align the antenna with. As you adjust the antenna, pay attention to the constantly updating display.

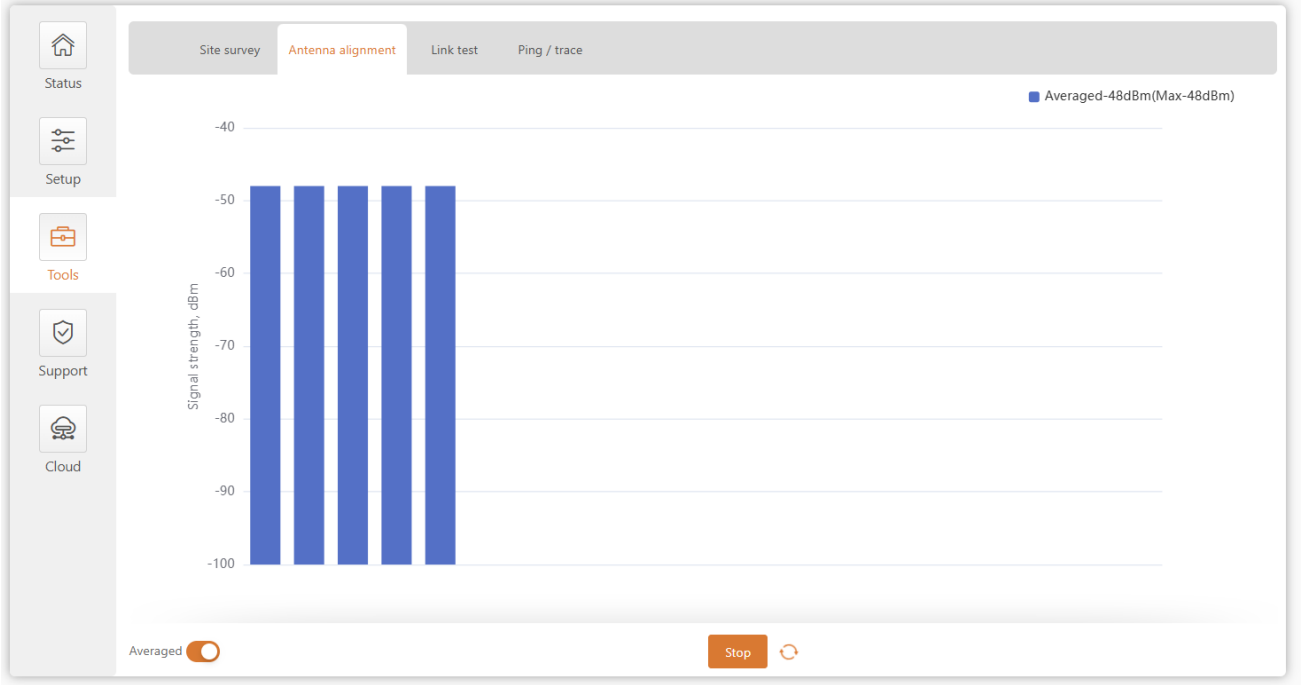


Figure 34 – Antenna calibration

Start – Press this button to start antenna calibration.

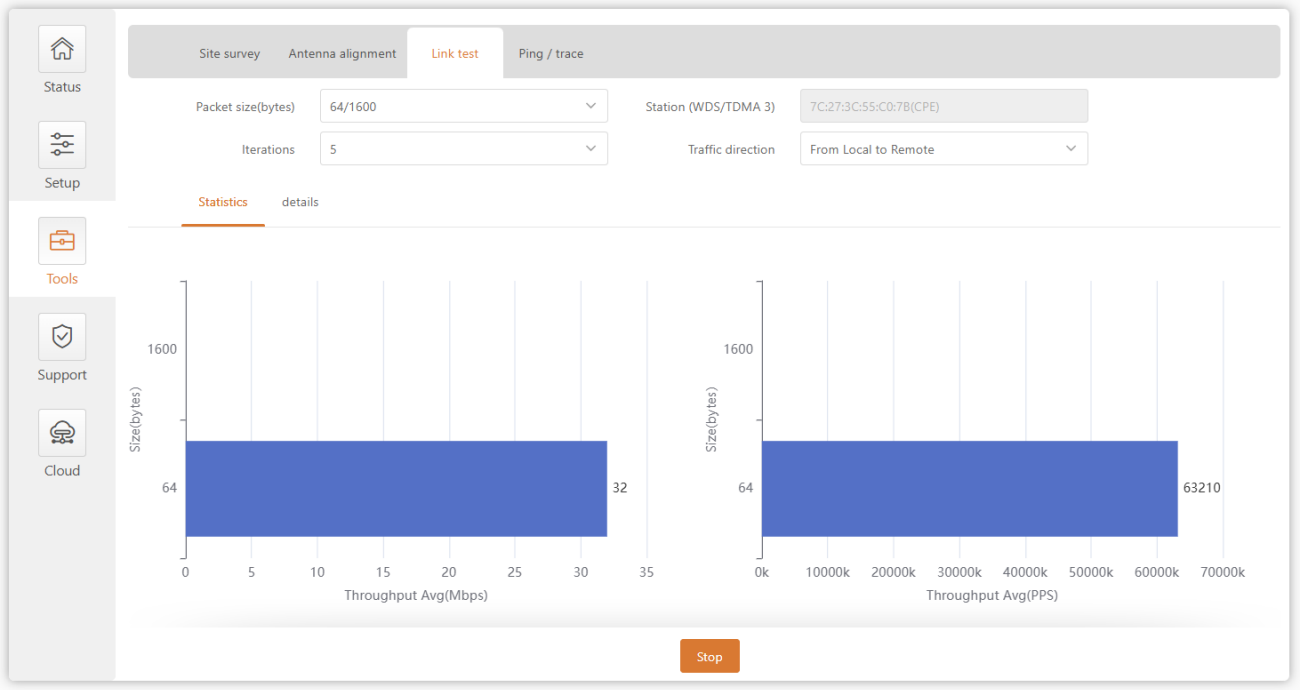
Stop – Press this button to stop antenna calibration .

Average – If this option is enabled, the graph will show the average signal strength of both antennas.

4.6.3. Link test

It is recommended to ensure there is no traffic on the link before running a link test as the results may not be completely accurate.

Use the Link Test Tool to check the quality of an established TDMA3 link. The tool tests throughput at a selected packet size and iterations.



Pkt. size(bytes)	Throughput(Mbps)	Throughput(PPS)	Packet loss(%)
64	31	61723	0
1600	321	25112	0

Figure 35 – Link test results

Packet size -Select the packet size (in bytes) for which the test will be performed.

Repeats - Select the number of test iterations.

TDMA 3 Site – Display access point information (if link test is performed from TMDA 3 station side) , select the station to perform link test by MAC address (if link test is performed from TDMA 3 access point side).

Traffic trends – Select the traffic direction in which to perform the test.

Start – Click to start the throughput test.

Stop – Click to stop the throughput test .

4.6.4. Shipping and tracking

Use the **PING** tool to discover how long it takes for packets to reach a specified trusted host. **PING** results are displayed in a table and graphically:

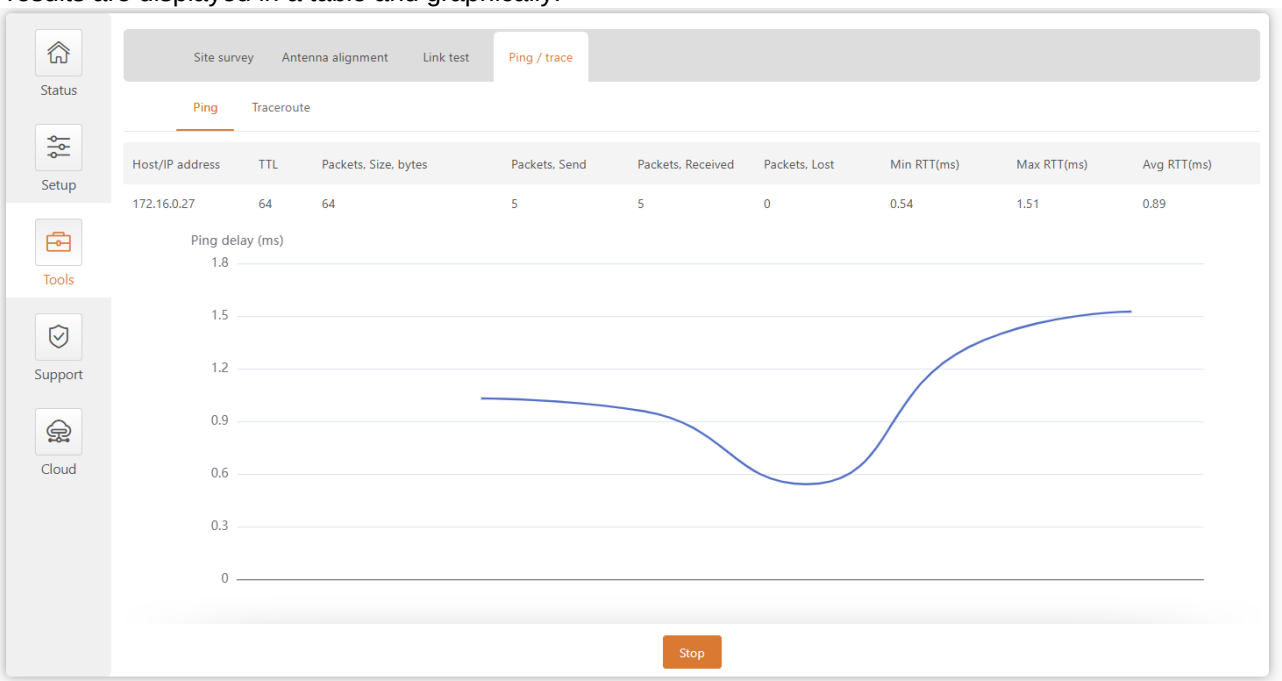


Figure 3 7 - Ping Tool

Host /IP Address – Specifies the host to which the Ping request will be sent.

Packet size (bytes) – Specifies the size of the packet in bytes.

Start/Stop – Click to start or stop the ping tool .

Use the **traceroute** tool to trace the route that a packet takes from the CPE unit to the destination host. This is useful when trying to figure out why a destination cannot be reached, as you will be able to see where the connection is failing.

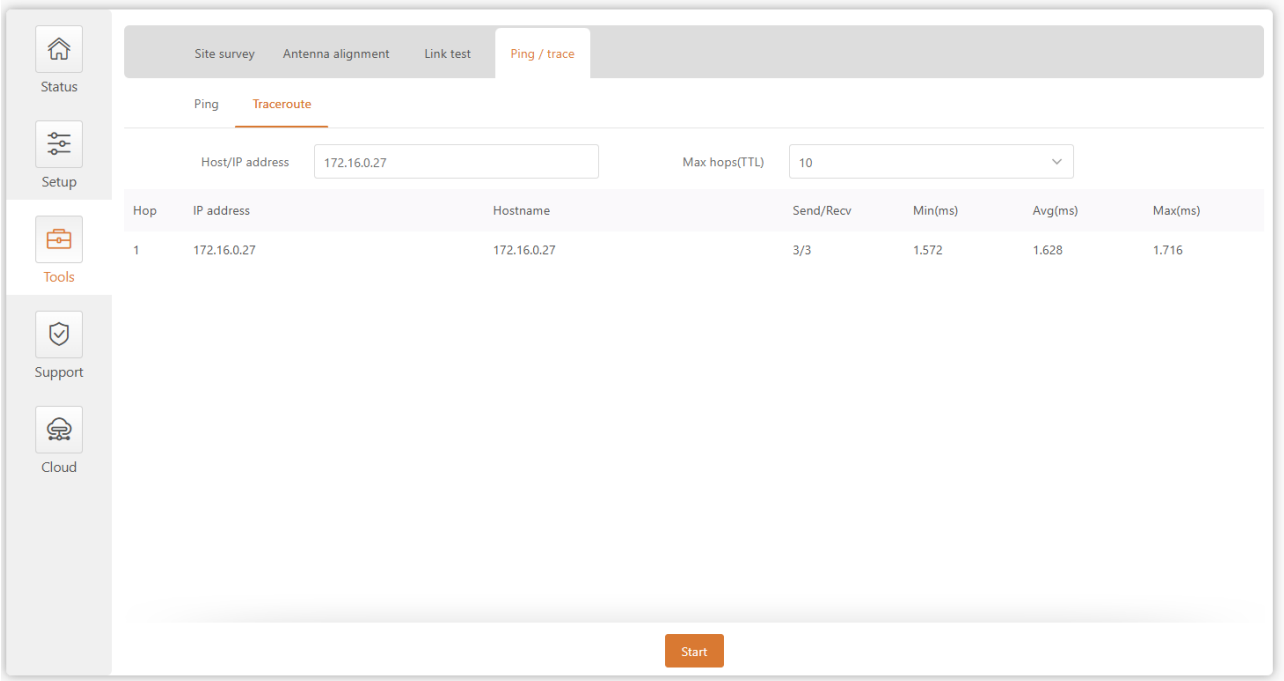


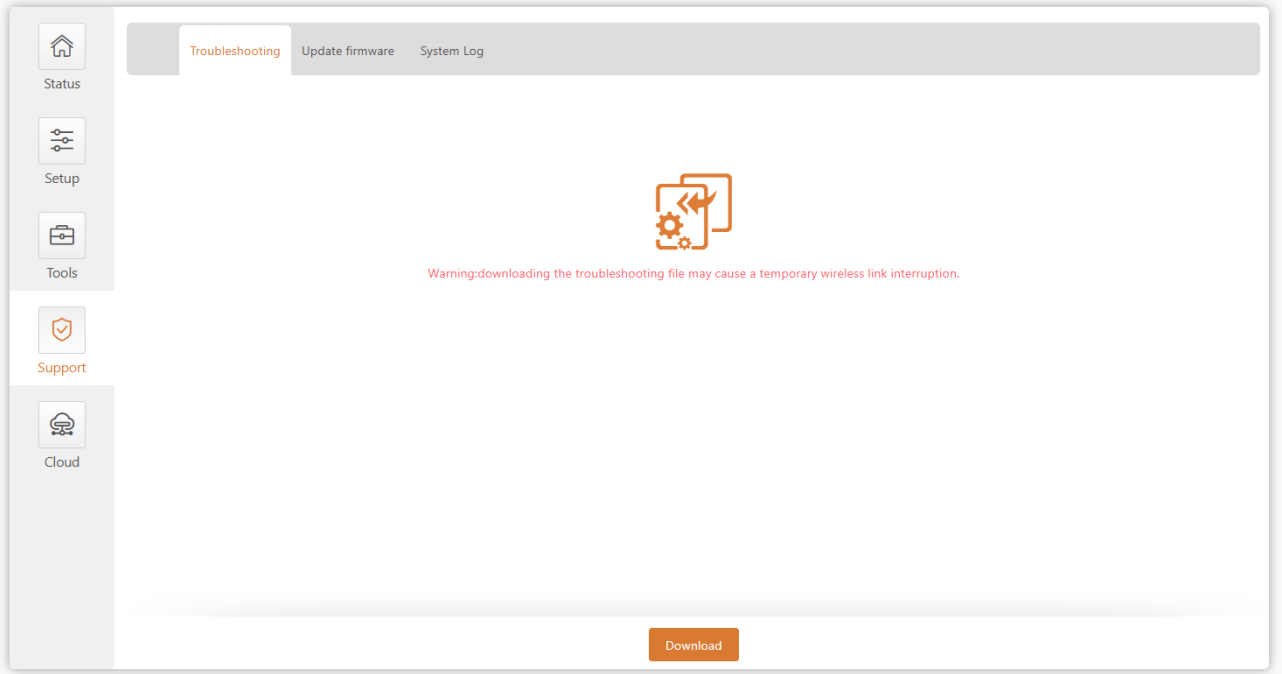
Figure 38 - Traceroute Tool

Host /IP Address – Specify the host name or IP address of the target host.

Maximum Hop Count (TTL) – Specifies the maximum number of hops to search for the target.

Start / Stop – Click to start or stop the tracking tool.

4.7. support



4.7.1. troubleshooting

Troubleshooting files contain valuable information such as device configuration, routes, log files, command output, etc. When you use troubleshooting files, the device can quickly and automatically collect troubleshooting information without requiring you to manually collect each piece of information. This helps when submitting issues to the support team .

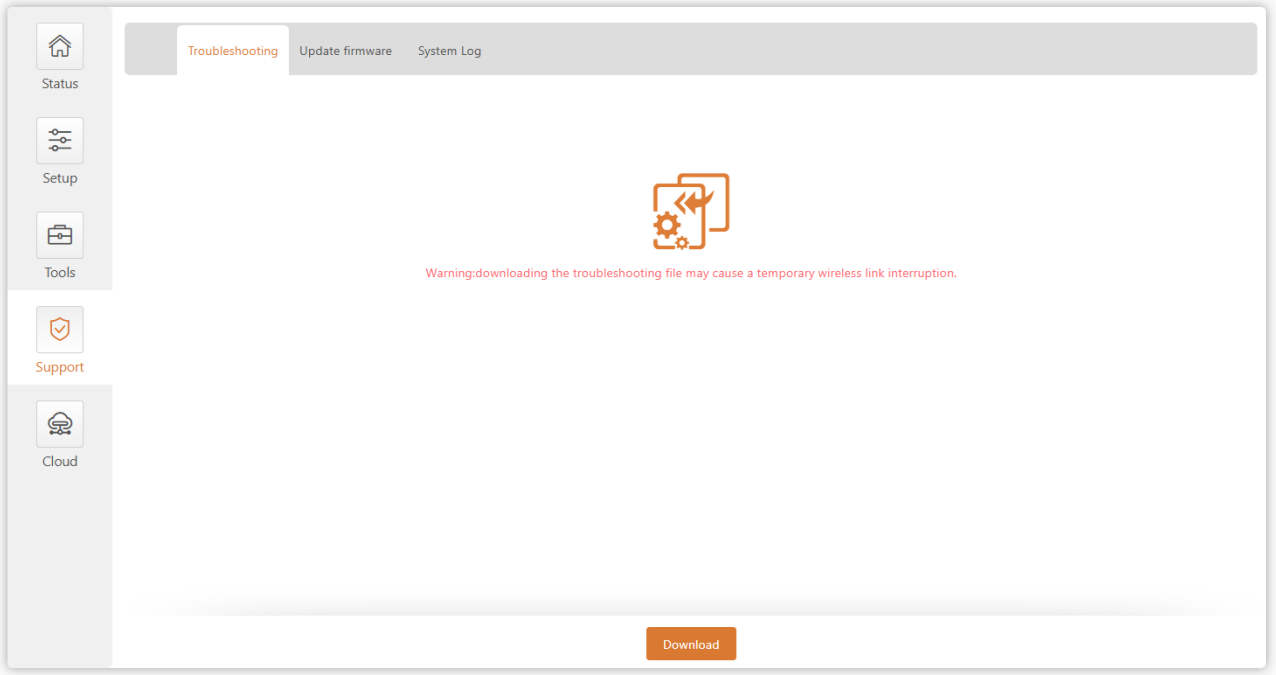


Figure 39 – File download troubleshooting

Download – Click to download the troubleshooting file. This may take several minutes to gather information and complete the download.

4.7.2. Firmware Upgrade

The current version of the device firmware is displayed on the first line of this menu .

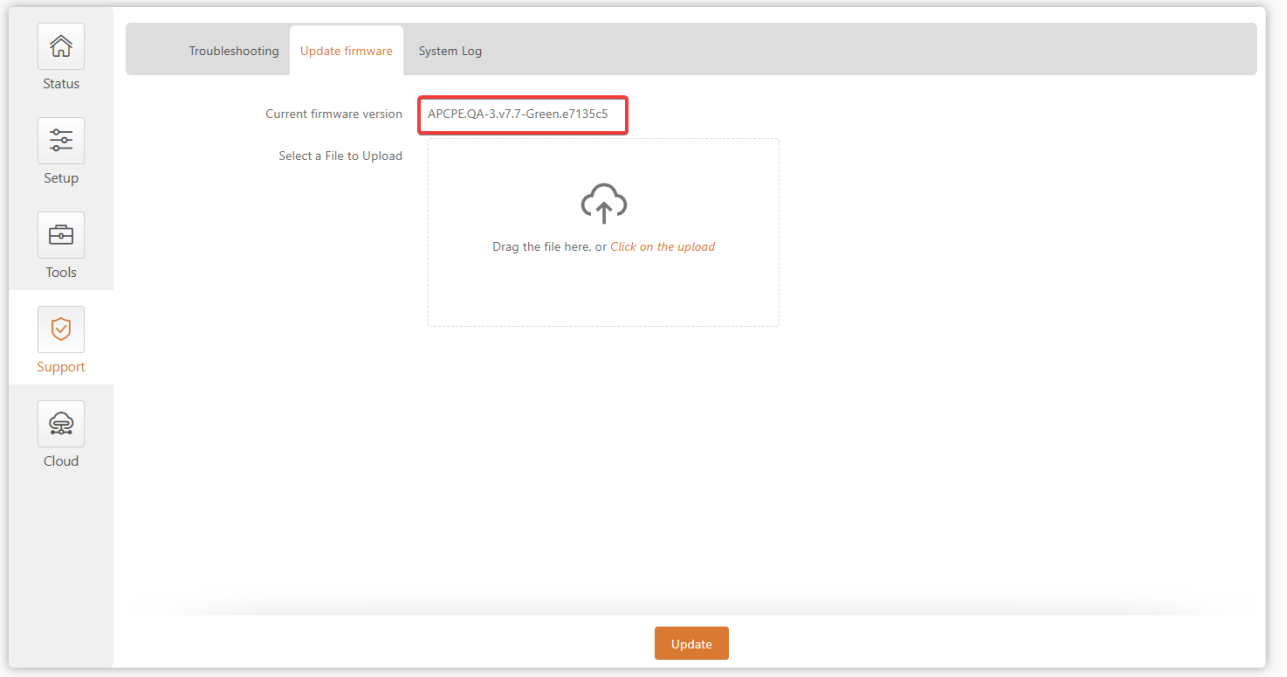


Figure 31 – Firmware Version

The device system firmware upgrade is compatible with all configuration settings. When the device is upgraded to a new version or built to the same version, all configurations of the upgraded system will be retained.

Figure 32 – Firmware Update

Drag the upgrade package to the upload box or select the upgrade package in the stand-alone upload box. The new firmware image is uploaded to the temporary storage of the controller. The next step is to save the firmware to the device's permanent storage. Click the Upgrade button:

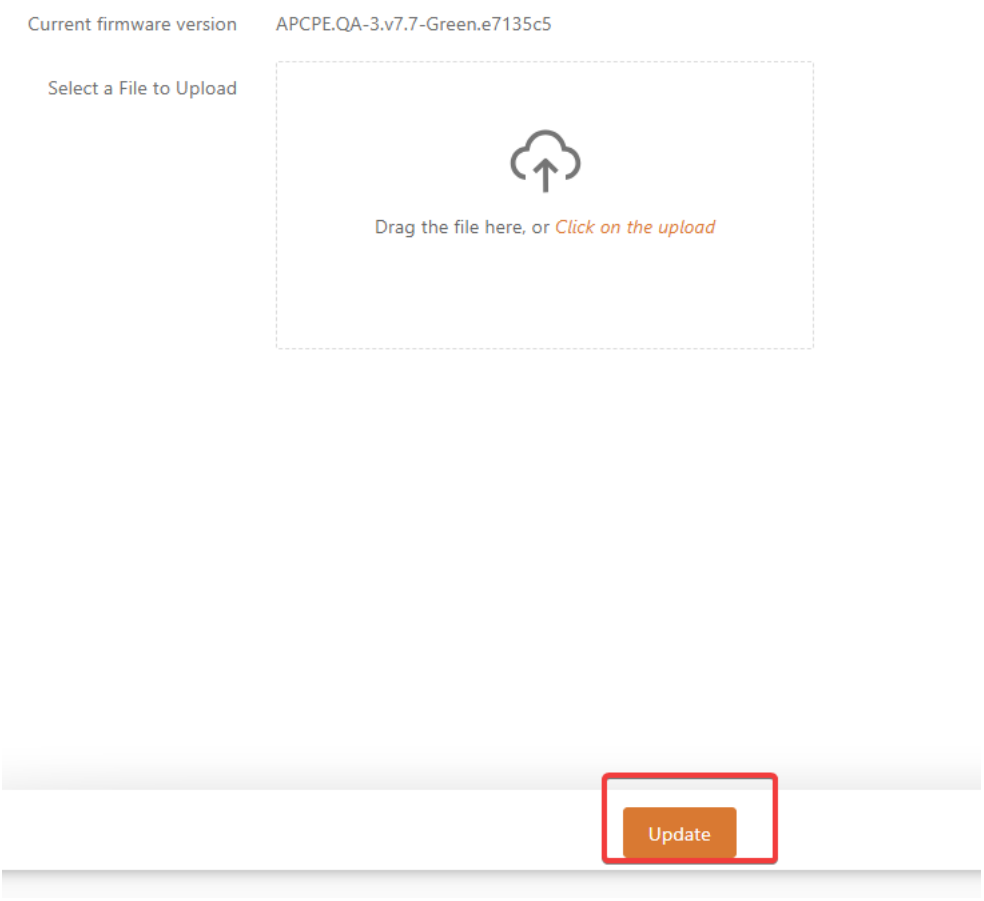


Figure 32 – Firmware Upgrade

Current version – Displays the current firmware version.

Uploaded version – Displays the version of the uploaded firmware.

upgrade – Upgrade the device using the uploaded image and reboot the system.

Do not turn off the device or disconnect the device from the power source during the firmware upgrade process; otherwise, the device may be damaged.

4.7.3. System log

The System Log Viewer utility provides debug information about system services and protocols. If a device fails, the logged messages can help operators locate misconfigurations and system errors.

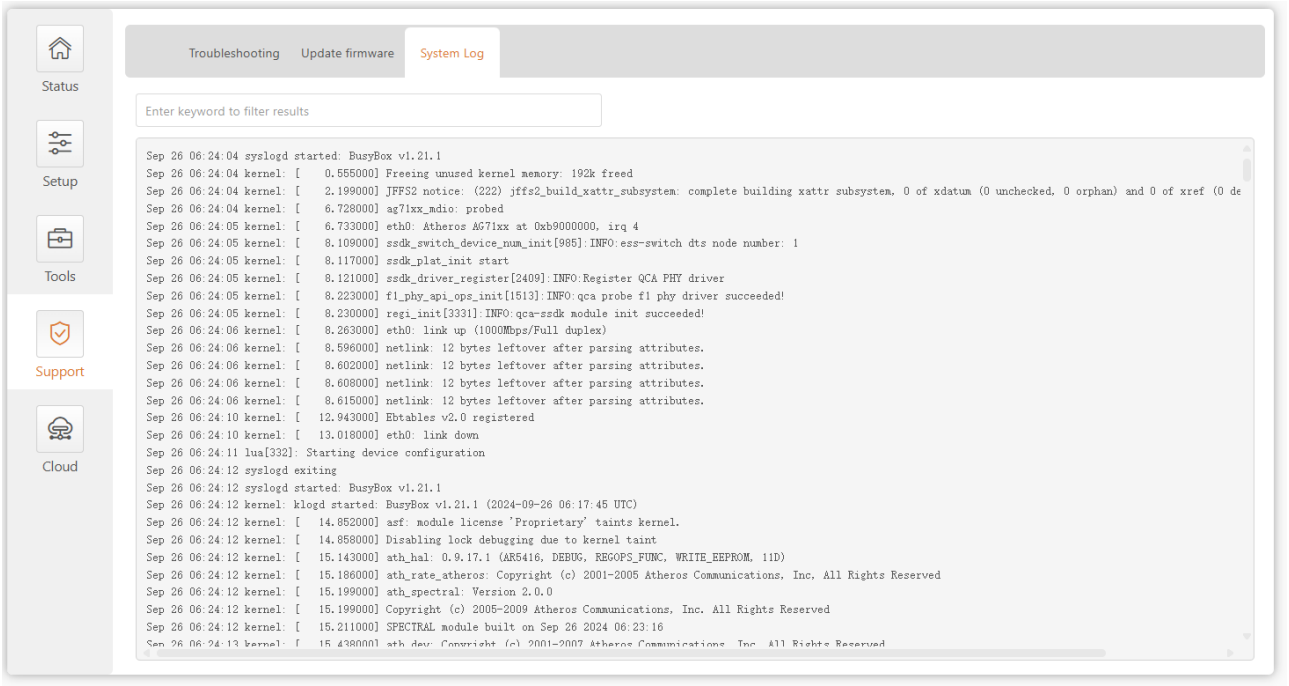
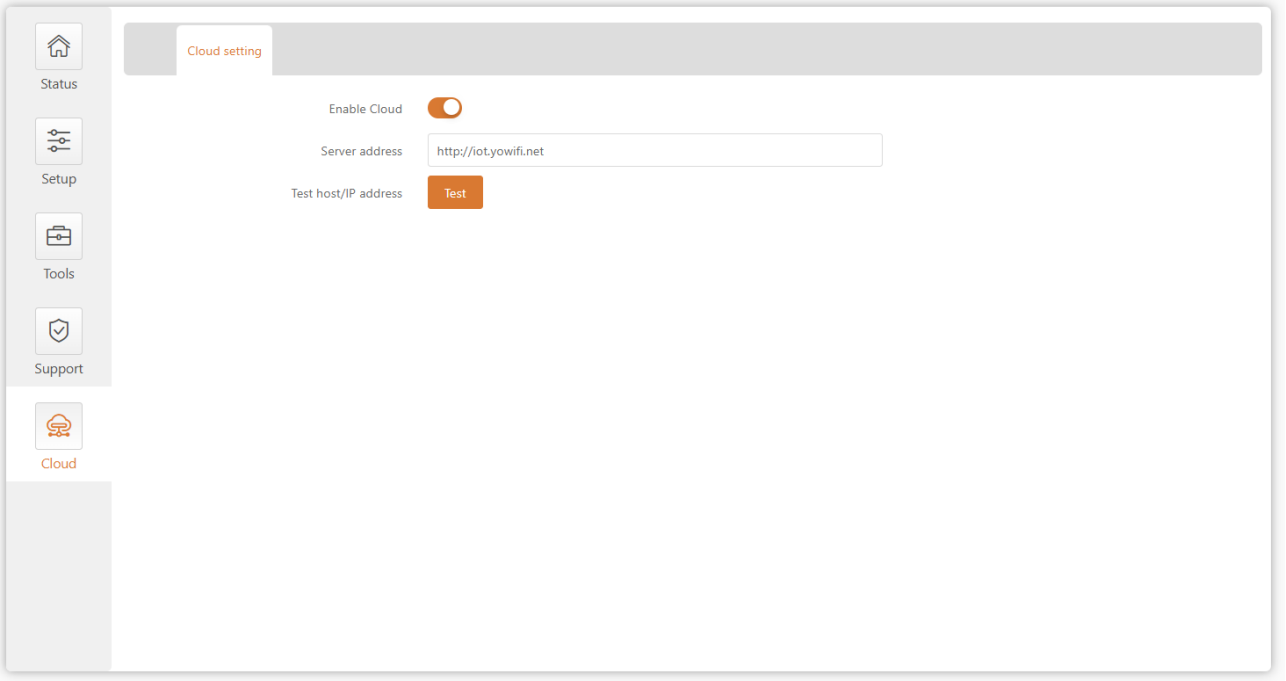


Figure 4 0 – Device system log

4.8. Could



After the device is connected, enable the cloud platform function, configure the cloud platform server address, and complete the corresponding configuration on the cloud platform to bind the device to the cloud platform.
Test host/IP address: After the device is connected to the external network, test whether it can connect to the cloud platform.