



User Guide

For

WI-FW5625, WI-FW5620-H,
WI-FW5619, WI-FW5618-H,
WI-FW5600

Release version: V1.0.0

March 2026

Table of Contents

| | | |
|-----------|-------------------------------------|----|
| Chapter 1 | Device Login | 1 |
| Chapter 2 | Quick Connection Setup | 3 |
| 2.1 | Steps for AP - Client Pairing | 3 |
| 2.2 | AP Mode Configuration | 4 |
| 2.3 | Client Mode Configuration | 7 |
| Chapter 3 | Status | 10 |
| 3.1 | Overview | 10 |
| 3.1.1 | Controller | 10 |
| 3.1.2 | Access Point | 11 |
| 3.1.3 | Clients | 14 |
| 3.1.4 | Wireless connection status | 15 |
| 3.2 | Routing | 15 |
| Chapter 4 | Network | 16 |
| 4.1 | Network | 16 |
| 4.1.1 | Bridge | 16 |
| 4.1.2 | Router | 20 |
| 4.2 | DHCP | 27 |
| 4.2.1 | DHCP Server | 27 |
| 4.2.2 | Static Lease | 28 |
| 4.2.3 | DHCP Leases | 29 |
| 4.3 | QOS | 29 |
| 4.4 | TR069 | 30 |
| 4.5 | SNMP | 31 |
| Chapter 5 | Wireless | 32 |
| 5.1 | Wireless Configuration | 32 |
| 5.1.1 | Access Point | 32 |
| 5.1.2 | Client | 34 |
| 5.3 | MAC Acl | 37 |
| Chapter 6 | Firewall | 40 |
| 6.1 | Port Forwards | 40 |
| 6.2 | Traffic Rules | 41 |
| Chapter 7 | System | 43 |
| 7.1 | System | 43 |
| 7.1.1 | System Properties | 43 |
| 7.1.2 | Language | 43 |
| 7.1.3 | Web server | 44 |
| 7.1.4 | Time Synchronization | 44 |
| 7.1.5 | Logging | 45 |
| 7.2 | Administration | 45 |
| 7.3 | Backup / Upgrade | 45 |

| | |
|--------------------------------------|----|
| 7.3.1 Backup / Restore | 45 |
| 7.3.2 Restore | 47 |
| 7.3.3 Flash new firmware image | 47 |
| 7.4 Reboot | 49 |
| 7.4.1 Reboot | 49 |
| 7.4.2 Schedule Reboot | 49 |
| 7.5 System Log | 50 |
| Chapter 8 Tools | 52 |
| 8.1 Network Utilities | 52 |
| 8.2 Ping WatchDog | 54 |
| 8.3 Discovery | 55 |
| 8.4 Antenna Alignment Tool | 56 |
| 8.5 Spectrum Analysis | 56 |
| 8.6 Wireless Link Test | 58 |
| Appendix | 60 |
| 9.1 Computer IP settings | 60 |

Chapter 1 Device Login

Login to the Management System

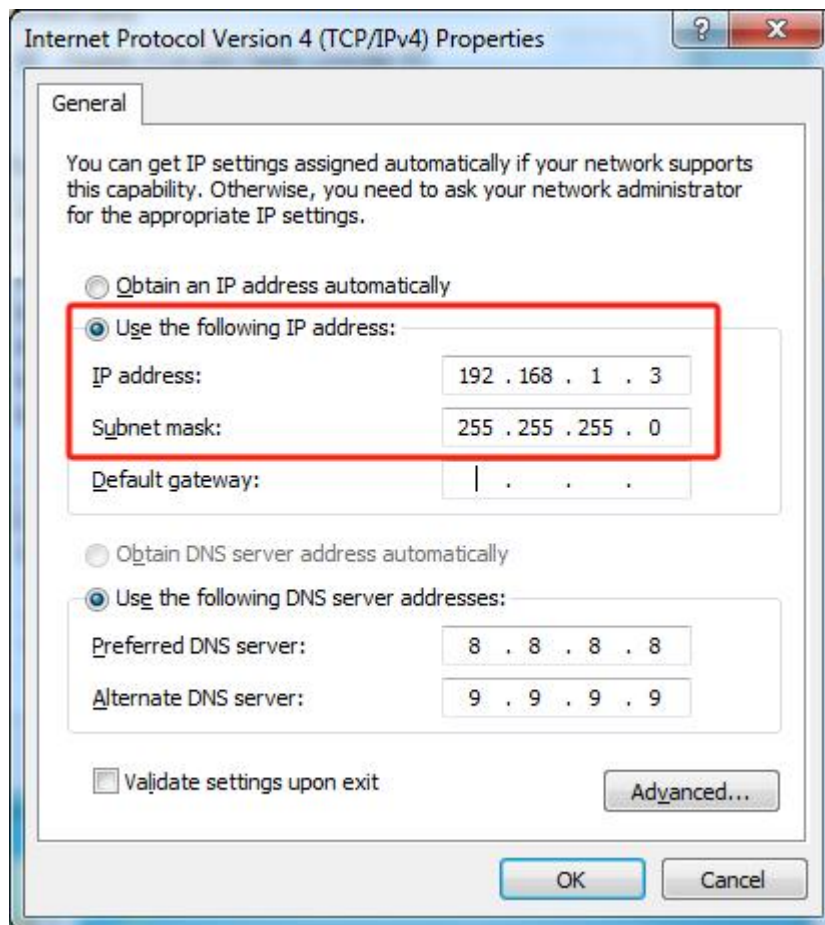
When the device is powered on and the system is running normally, access the management interface via a web browser. The default login information for the device is as follows:

Login Information & Default Configuration:

| Parameter | Default Configuration |
|------------|-----------------------|
| IP address | 192.168.1.2 |
| Password | admin |


Bridge Login Setup Steps:

1. Ensure the bridge is connected to the management computer;
2. Manually set "Use the following IP address" with an IP address of "192.168.1.XXX" (X=3~254) and a subnet mask of "255.255.255.0" (If connected to a switch or router on the same subnet, avoid conflicts with the IP address of the switch/router/bridge);



3. Open a browser on the computer (Google, Chrome or Firefox recommended). Enter the bridge's IP address in the address bar (192.168.1.2 for initial use or after reset; use the new IP address if modified previously) and press the "Enter" key;

⚠ 不安全 | https://192.168.1.2

4. Enter the bridge login interface, input the password "admin", and select language "English";
5. Click  to enter the system.



Wi-Tek
Communication Solution

Password

Language



6. After entering the system, you can configure bridge information using the "Setup Wizard".
7. Device login is complete. Proceed to the target configuration.

Setup Wizard



Lan

IP

Netmask

Gateway

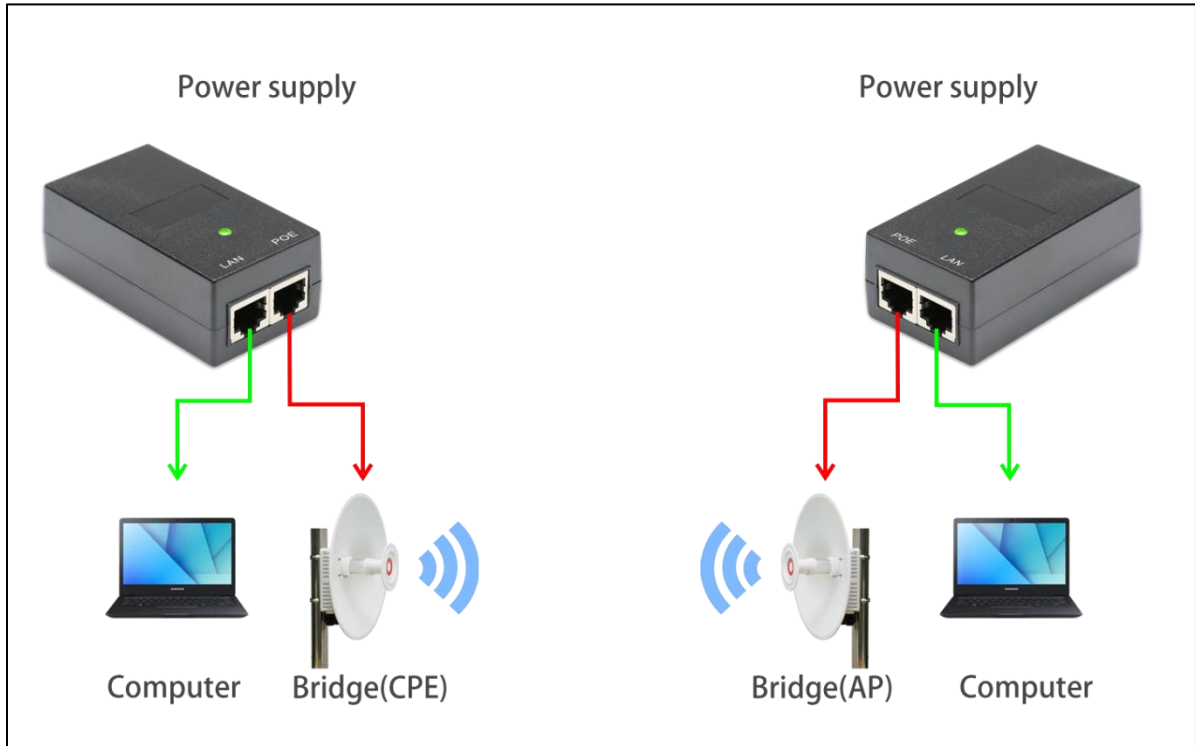
DNS

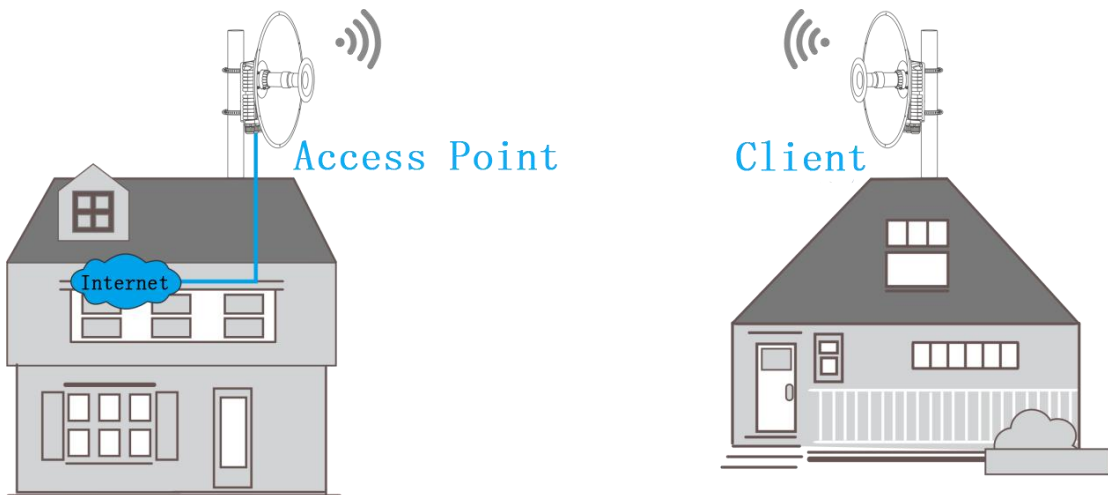
Chapter 2 Quick Connection Setup

2.1 Steps for AP - Client Pairing

AP-client Mode Connection Diagram



AP-Client Mode Connection Effect, as shown:



2.2 AP Mode Configuration

1. Enter the device wizard.

2. Set the bridge IP address information. After configuration, click

Next

Partial Parameter Description:

| Parameter | Description |
|-----------|--|
| IP | The IP address of device. |
| Netmask | A 32-bit binary number, typically expressed as a dotted decimal (e.g., 255.255.255.0), that is used to identify the boundary between the network and host parts of an IP address, in order to divide a large IP network into logical subnets. |
| Gateway | A system that connects different networks, serving as a hub for transmitting, forwarding, and transforming data between them to enable communication across dissimilar networks. (The gateway address is typically the LAN port address of the upstream router.) |
| DNS | DNS server, translates domain names into corresponding IP addresses, enabling users to access websites or network services via domain names (Common DNS servers: 8.8.8.8, 9.9.9.9, 114.114.114.114). |
| Home Page | Directly enter the management interface instead of modifying the configuration through the setup wizard. |
| Next | Proceed to the "Next" configuration step (Wireless page). |

Setup Wizard

Lan

IP

Netmask

Gateway

DNS

3. Set WiFi information.



Note: AP configuration "SSID, Encryption Mode, Password" must match the Client configuration for the Client device to connect correctly.

Partial Parameter Description:

| Parameter | Description |
|-----------|---|
| Mode | Select "Access Point mode" (Wireless Transmitting End). |

| | |
|--------------|---|
| SSID | The name of the WiFi network, uniquely identifying a wireless LAN (e.g., WIFI7-bridge). |
| Encrypt Mode | Wireless encryption method. Supported options: WPA3-SAE, WPA2-PSK/WPA3-SAE, WPA2-PSK, WPA2 with Radius. |
| Key | WiFi password (e.g., 12345678). |
| Channel | The channel for signal transmission, referring to the medium or path for communication. Select the wireless working channel from the dropdown list. |
| Power | Transmission power used by the wireless device when sending signals (Supported input: 1-26dBm, unit: dBm). |
| HT mode | The bandwidth occupied by the WiFi wireless signal on the spectrum (Supports 20MHz, 40MHz,80MHz, 160MHz). |
| Password | Administrator password for system management login. |

Setup Wizard

WIFI

5G Radio Settings

| | | |
|--------------|----------------|---|
| Mode | Access Point | ▼ |
| SSID | WIFI7-bridge | |
| Encrypt Mode | WPA3-SAE | ▼ |
| Key | 12345678 | 👁 |
| Channel | 120 (5600 Mhz) | ▼ |
| Power | 26 dBm | ▼ |
| HT mode | 160MHz | ▼ |
| Country Code | No Country | ▼ |

System

| | | |
|----------|-------|---|
| Password | admin | 👁 |
|----------|-------|---|

Use Wi-Fi password as router management password

Please note that this equipment may be subjecto local legislative rastrictions, It is the end users responsibly to ensure thathe instalaton complies wth any such restrictionthat areinfore

Please tick the box to acknowledge that you understand this device must be set to the correct country of operation.

Back
Next

Note: The device must be configured with the correct country code and "Country Code Configuration Prompt" must be checked to proceed.

- After completion, click

Next

Setup Confirmation

Network

| | |
|---------|---------------|
| IP | 192.168.1.2 |
| Netmask | 255.255.255.0 |
| Gateway | 192.168.1.1 |
| DNS | 8.8.8.8 |

WIFI

5G Radio Settings

| | |
|--------------|--------------|
| Mode | Access Point |
| SSID | WIFI7-bridge |
| Encrypt Mode | WPA3-SAE |
| Key | 12345678 |
| Channel | 120 |
| Power | 26 dBm |
| HT mode | 160MHz |
| Country Code | No Country |

System

| | |
|--|--|
| | |
|--|--|

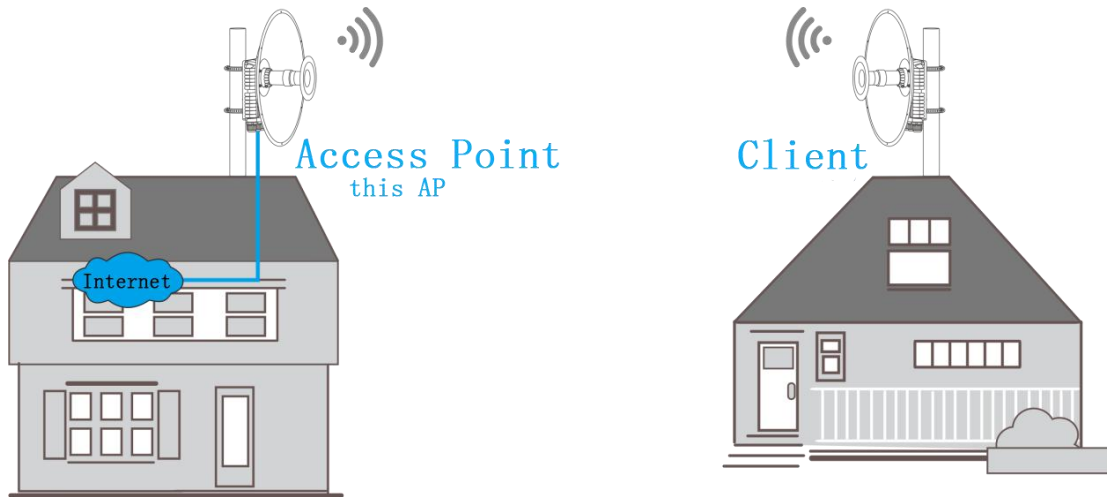
System

| | |
|----------|-------|
| Password | admin |
|----------|-------|

Back Finish

4. Confirm network information and wireless configuration are correct, then click
5. AP device configuration is complete.
6. Implementation effect, as shown:

Finish



2.3 Client Mode Configuration

1. Enter the Setup Wizard.
2. Set the bridge address information.

Setup Wizard

Lan

IP

Netmask

Gateway

DNS

Partial Parameter Description:

| Parameter | Description |
|-----------|--|
| IP | The IP address of device. |
| Netmask | A 32-bit binary number, typically expressed as a dotted decimal (e.g., 255.255.255.0), that is used to identify the boundary between the network and host parts of an IP address, in order to divide a large IP network into logical subnets. |
| Gateway | A system that connects different networks, serving as a hub for transmitting, forwarding, and transforming data between them to enable communication across dissimilar networks. (The gateway address is typically the LAN port address of the upstream router.) |
| DNS | DNS server, translates domain names into corresponding IP addresses, |

| | |
|-----------|---|
| | enabling users to access websites or network services via domain names (Common DNS servers: 8.8.8.8, 9.9.9.9, 114.114.114.114). |
| Home page | Directly enter the management interface instead of modifying the configuration through the setup wizard. |
| Next | Proceed to the " Next " configuration step (Wireless page). |

After completing the configuration, click



3. Set WiFi information.



Note: Client configuration "SSID, Encryption Mode, Password" must match the AP configuration to connect correctly to the AP.

Setup Wizard

WIFI

5G Radio Settings

| | | |
|--------------|----------------|---|
| Mode | Client | ▼ |
| Scan | | |
| SSID | WIFI7-bridge | |
| Encrypt Mode | WPA3-SAE | ▼ |
| Key | 12345678 | |
| Channel | 120 (5600 Mhz) | ▼ |
| Power | 26 dBm | ▼ |
| HT mode | 160MHz | ▼ |
| Country Code | No Country | ▼ |

System

Password

Use Wi-Fi password as router management password

Please note that this equipment may be subjecto local legislative rastrictions. It is the end users responsibly to ensure thathe instalaton compls with any such restrictionthat areinfore

Please tick the box to acknowledge that you understand this device must be set to the correct country of operation.

Back
Next

Partial Parameter Description:

| Parameter | Description |
|--------------|--|
| Mode | Select " Client " (Wireless Signal Receiving End) here to pair with an AP. |
| SSID | Set the bridge's wireless signal name (e.g., WIFI7-bridge). |
| Encrypt Mode | WiFi encryption method (Supports WPA3-SAE, WPA2-PSK/WPA3-SAE, WPA2-PSK, WPA2 with Radius). |
| Key | WiFi password (e.g., 12345678). |
| Channel | Select the wireless working channel from the dropdown list. |
| Power | Wireless signal transmission power. |
| HT mode | Wireless signal working bandwidth (Supports 20MHz, 40MHz, 80MHz, 160MHz). |
| Password | Administrator password for system management login. |

Finish

4. Confirm the information is correct and click .

Setup Confirmation

网络

| | |
|------|---------------|
| IP | 192.168.1.3 |
| 网络掩码 | 255.255.255.0 |
| 网关 | 192.168.1.1 |
| DNS | 8.8.8.8 |

WIFI

5G Radio Settings

| | |
|---------|-----------------|
| 模式 | Client |
| 无线网络名称 | wireless-bridge |
| 加密模式 | WPA3-SAE |
| 密钥 | 12345678 |
| 信道 | 120 |
| Power | 26 dBm |
| HT mode | 160MHz |
| 国家代码 | No Country |

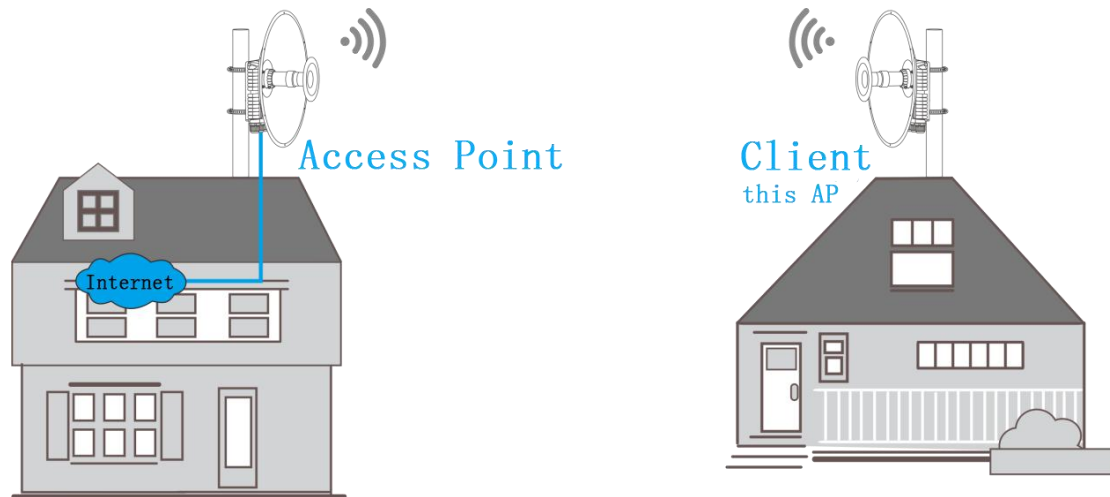
系统

| | |
|----|-------|
| 密码 | admin |
|----|-------|

返回 完成

5. Client device configuration is complete.

The connection is successful, as shown in the following figure:

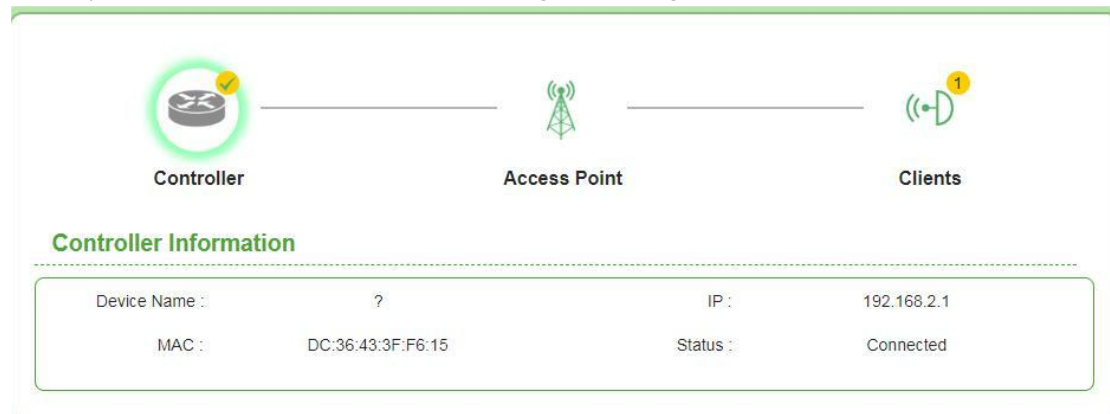


Chapter 3 Status

3.1 Overview

3.1.1 Controller

View upstream device information for the bridge, including device name, MAC, IP, and status.



Parameter Description:

| Parameter | Description |
|-------------|--------------------------------------|
| Device Name | Name of the main device. |
| MAC | Physical address of the main device. |

| | |
|--------|--|
| IP | IP address of the main device. |
| Status | Connection status between the wireless bridge and the main device. |

3.1.2 Access Point

In the "Access Point AP" interface, view basic information about this bridge, wireless configuration and Ethernet ports.

3.1.2.1 System

View basic bridge information, including uptime, average load, SN and key.

The screenshot shows a 'System' configuration page with the following details:

- Product Model: E5
- Mac: b0:96:6c:b5:c3:02
- Local Time: 2025-05-27 11:07:27
- Uptime: 0h 11m 35s
- SN: W0B26250400078
- BindCode: ayrmr5MwkvVkt23QmlR49mDYL1zcFXs
- Firmware Version: 2.2.0.release
- Load Average: 0.70, 0.51, 0.29
- CPU Usage: 6%
- Memory Usage: 198.40 MiB / 412.63 MiB (48%)

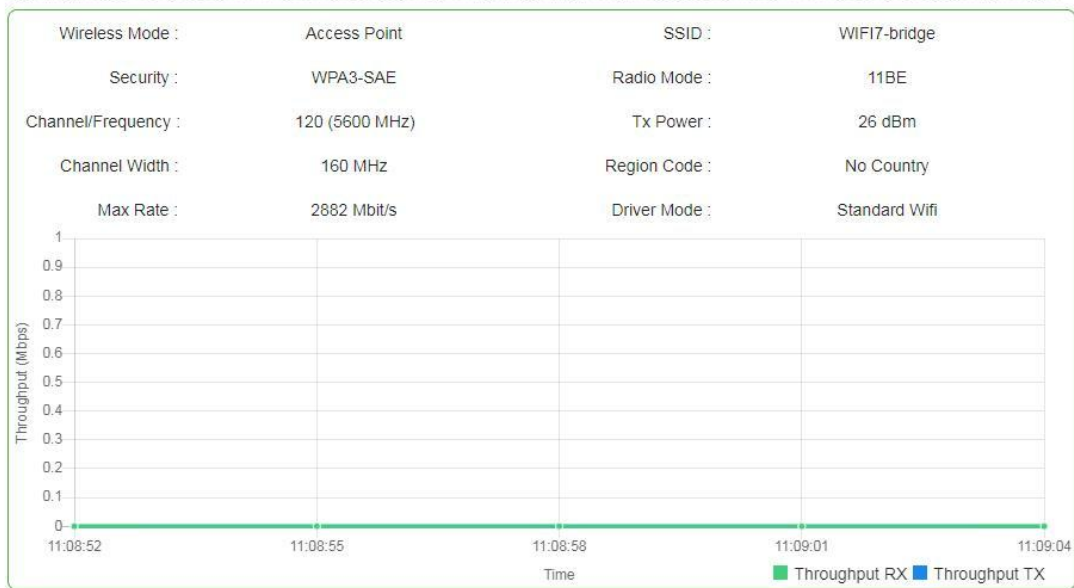
Parameter Description:

| Parameter | Description |
|------------------|---|
| Product Model | Product model number used to identify the product. |
| Firmware Version | Indicates firmware update and iteration status. |
| MAC | Physical address (MAC address) used to identify the network device. |
| Load Average | Measures overall system load, reflecting resource contention (especially CPU, memory, I/O) over a period. |
| Local Time | Device local time (Default: UTC). Can be modified in "System" > "System Properties". |
| CPU Usage | An indicator measuring the busyness of the computer's central processor over a period. |
| Uptime | The continuous normal operating time of the device since startup, measuring system stability, reliability, or task duration. |
| Memory Usage | Amount of memory resources occupied by the system during operation. |
| SN | Serial Number: Unique identifier for each product, used for tracking production batch, date, warranty status (Acts as identifier for cloud management). |
| BindCode | The binding code for cloud management. |

3.1.2.2 Wireless

View detailed wireless configuration information, such as wireless mode, wireless name, wireless encryption, channel, bandwidth, transmission, power, country code, etc.

Wireless



Parameter Description:

| Parameter | Description |
|-------------------|--|
| Wireless Mode | Supported options: Access Point AP, Client. |
| SSID | Name of the WiFi network, uniquely identifying a wireless LAN. |
| Security | Wireless encryption method. Supported options: WPA3-SAE, WPA2-PSK/WPA3-SAE, WPA2-PSK, WPA2 with Radius. |
| Radio Mode | Radio mode under which the wireless device operates according to IEEE 802.11 standards. |
| Channel/Frequency | Channel: The medium/path for signal transmission in communication. Frequency: Number of vibrations/changes per unit time for a periodic signal (Unit: Hz). |
| Tx Power | Power used by the wireless device when transmitting signals (Unit: dBm). |
| Chanel Width | Bandwidth occupied by the WiFi wireless signal on the spectrum. Currently supported: 20MHz, 40MHz, 80MHz, 160MHz, 320MHz. |
| Region Code | Region code. Select the code compliant with local laws/regulations as different countries/regions may have different open frequency bands, power limits (Tx Power), channel/tech restrictions. |
| Max Rate | Theoretical maximum data transfer rate of the device under specific conditions (Unit: Mbps). |
| Driver Mode | WiFi mode, supports "Standard WiFi" or "Wis TDMA" (selectable in "Wireless Interface"). |
| Wireless traffic | Displays real-time download and upload traffic for the wireless interface. |

3.1.2.3 Network

View the status of the bridge's RJ45 and SFP+ network interfaces, such as assigned interface number, MAC address, IP address protocol, IP address, gateway address, DNS server, actual interface LINK rate, max Ethernet port link rate, QOS status, STP status, and interface connection status.



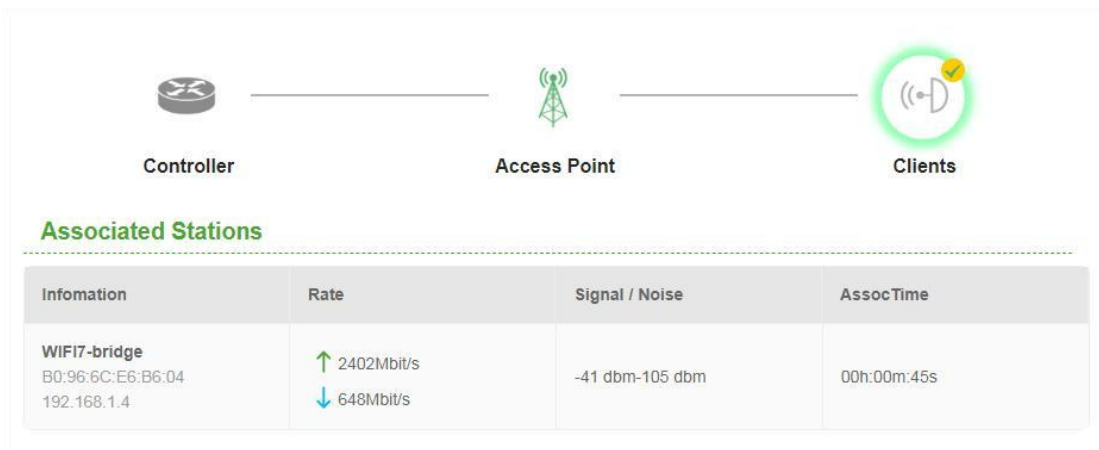
Parameter Description:

| Parameter | Description |
|------------|---|
| Name | Device physical interface: Connects to LAN devices. Usually the internal network port, separate from the WAN (external) port. |
| Port Name | Physical interface assigned by the device |
| MAC | Physical layer address (MAC address) used to identify the network device. |
| Protocol | Ethernet interface protocol. Supports Static address, DHCP client, DHCPv6 client. |
| IP Address | Digital label of a device connected to a computer network, used to uniquely identify the device and enable data communication. IP address 192.168.1.2/24 is a common private LAN IPv4 address (32-bit binary, dotted decimal). Subnet Mask (/24): Indicates the first 24 bits are the network part, last 8 bits are the host part (Decimal subnet mask: 255.255.255.0). |
| Gateway | A system that connects different networks, serving as a hub for transmitting, forwarding, and transforming data between them to enable communication across dissimilar networks. |
| DNS | DNS server: Converts domain names into corresponding IP addresses, enabling users to access websites or network services via domain names |

| | |
|------------------|--|
| | (e.g., resolving www.baidu.com to Baidu server IP). |
| Link Rate | Actual data transfer rate of the Ethernet port connected to the network (Unit: Mbps). |
| Max Rate | Theoretical maximum data transfer rate of the device under specific conditions (Unit: Mbps). |
| QOS | Status of the QOS function (On/Off). |
| Bridge STP | Status of the Spanning Tree function (On/Off). Spanning Tree resolves loop issues when bridges interconnect by blocking redundant links, building a loop-free tree topology while retaining backup paths for quick failover. |
| Status | Connection status of the ETH1 physical interface. |
| Ethernet Traffic | Displays real-time download and upload traffic for the ETH1 physical interface. |

3.1.3 Clients

The client connection list records information about clients currently connected to the "Access Point".



Parameter Description:

| Parameter | Description |
|--------------|---|
| Information | Information about the wireless access point (AP), such as SSID, physical MAC address, IP address. |
| Rate | Theoretical data transfer rate per second during wireless communication. |
| Signal/Noise | Core factors affecting network quality; their relative relationship determines signal reliability and transmission efficiency. Larger signal value indicates better signal. |
| Assoc Time | Duration connected to the wireless access point (AP). |
| Distance | Distance difference between the client and the wireless access point (AP). |

3.1.4 Wireless connection status

The diagram illustrates the wireless connection status. It shows a Controller connected to an Access Point, which is then connected to Clients. Below this, there is a section titled "Associated Stations" with a table showing details for a specific station.

| Information | Rate | Signal / Noise | AssocTime |
|---|-----------------------------|-----------------|-------------|
| WiFi7-bridge B0:96:6C:E6:B6:04 192.168.1.4 | ↑ 2402Mbit/s ↓ 648Mbit/s | -41 dbm-105 dbm | 00h:00m:45s |

If login to the AP page, click “**client**” icon to view the client's signal and other connection information.

If login to the client page, click the “**Access Point**” icon to view the remote AP's signal and other connection information.

3.2 Routing

View the IP addresses, MAC addresses of devices connected within the LAN, and the IPv4 routing forwarding path.

ARP (Address Resolution Protocol): Protocol used in IPv4 networks to map IP addresses to physical MAC addresses.

Active IPv4 Routes: **Routing** refers to the process of forwarding IP packets from a source host to a target host across networks. **Active Routes** are the currently effective routing entries used to guide packet forwarding. These entries are stored in the device's routing table (i.e., the current page) and maintained by network devices (e.g., routers, bridges).

Routing

Active IPv4 ARP

| IP address | MAC address | Interface |
|---------------|-------------------|-----------|
| 192.168.1.4 | B0:96:6C:E6:B6:01 | lan |
| 192.168.1.1 | DC:36:43:3F:F6:15 | lan |
| 192.168.1.157 | 00:13:3B:13:14:BE | lan |

Active IPv4 Routes

| Network | Target | Gateway | Metric | Table | Protocol |
|---------|----------------|-------------|--------|-------|----------|
| lan | 0.0.0.0/0 | 192.168.1.1 | 0 | main | static |
| lan | 192.168.1.0/24 | - | 0 | main | kernel |

Chapter 4 Network

4.1 Network

4.1.1 Bridge

Network Mode: Bridge



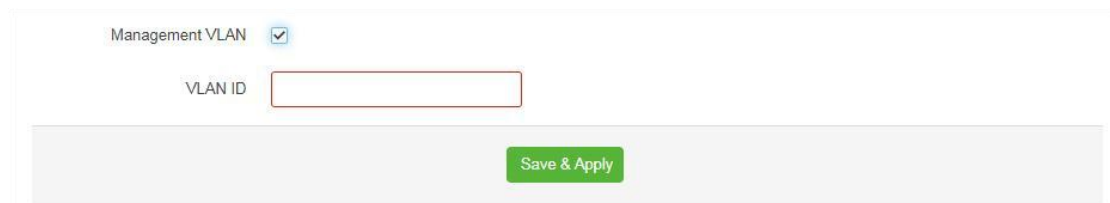
The screenshot shows a configuration panel titled "Network". It features a "Network Mode" dropdown menu set to "Bridge". Below it, the "Spanning Tree" section has two radio buttons: "None" (unselected) and "STP" (selected).

- **Spanning Tree (STP)**

Spanning Tree is disabled by default. Check "**STP**" to enable the Spanning Tree function. STP solves loop problems when bridges interconnect by blocking redundant links, building a loop-free tree topology while retaining backup paths for quick failover.

- **Management VLAN**

VLAN is a technology that divides a physical LAN into multiple logical subnets via software, used to isolate broadcast domains, enhance network security, and improve management efficiency. The **Management VLAN** is a dedicated logical subnet for managing network devices. By segregating management traffic into an independent VLAN, remote configuration, monitoring, and maintenance of devices are achieved.



The screenshot shows a configuration panel for "Management VLAN". It includes a checked checkbox for "Management VLAN" and an empty text input field for "VLAN ID". A green "Save & Apply" button is located at the bottom right of the panel.

- **LAN**

LAN (Local Area Network) refers to a computer network connecting multiple devices (computers, printers, servers, etc.) within a limited geographical area (e.g., office, home, campus, factory) via communication lines or wireless signals to achieve data transmission and resource sharing.

View the IP acquisition method and related IP information of the bridge.

The current bridge supports three IP acquisition methods: "**Static IP**", "**DHCP Client**", "**DHCPv6 Client**".

LAN

Protocol: Static address ▼

IPv4 address: Static address
DHCP client
DHCPv6 client

 **Protocol Description & Notes:**

| Protocol | Description |
|----------------|--|
| Static address | Fixed IP address manually assigned to a network device; does not update automatically with network connection changes. Note: If the network device's IP address is modified, the new IP address must be used for the next login (computer address must be on the same subnet as the bridge's IP). |
| DHCP Client | Device that requests and accepts network parameters (IP address, subnet mask, gateway, DNS server, etc.) assigned by a DHCP server. Automatically obtains network configuration via DHCP protocol, no manual IP setup required. Note: When the bridge uses "DHCP Client", check the IP address assigned to the bridge in the upstream device's DHCP server first, then use that IP address to access the management interface. |
| DHCPv6 Client | Device that requests and accepts network parameters (IP address, subnet mask, gateway, DNS server, etc.) assigned by a DHCPv6 server. Automatically obtains network configuration via DHCPv6 protocol, no manual IP setup required. Note: When the bridge uses "DHCPv6 Client", check the IP address assigned to the bridge in the upstream device's DHCP server first, then use that IP address to access the management interface. |

➤ **Protocol---Static address**

LAN

Protocol: Static address ▼



IPv4 address:

IPv4 netmask: 255.255.255.0 ▼

IPv4 gateway:

IPv6 address:

IPv6 gateway:

DNS: 
 

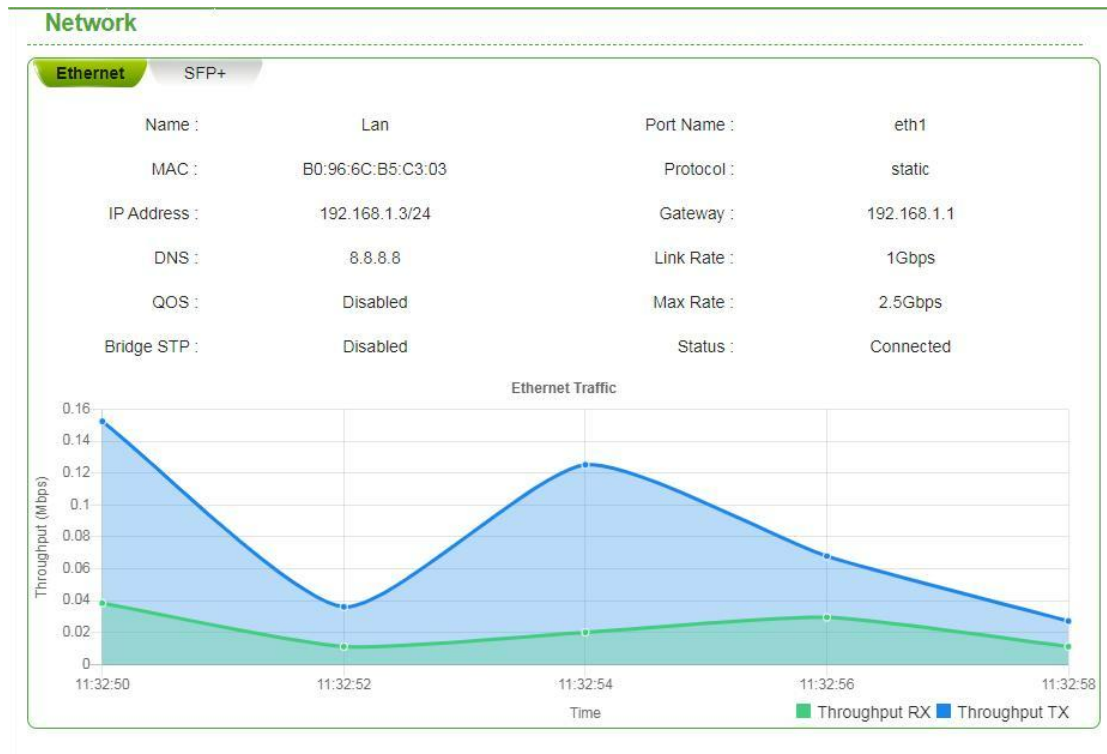
Management VLAN:

Save & Apply

Manually assign a fixed IP address to the network device; does not update automatically.

Static IP Setup Steps:

1. Protocol: Select "**Static address**" from the dropdown menu.
2. IPv4 address: Set the bridge IP address (e.g., 192.168.1.2).
3. IPv4 netmask: Set the subnet mask for the IP address (e.g., "**255.255.255.0**").
4. IPv4 gateway: Set the gateway address (i.e., the LAN port address of the upstream router, e.g., 192.168.1.1).
5. DNS: Set the DNS server address. If there are multiple DNS servers, enter them all.
6. Set and apply. View the configuration under "**Status**" → "Overview" → "Network".



Partial Parameter Description:

| Parameter | Description |
|------------|--|
| Protocol | Static Address: Fixed IP address manually assigned to the network device; does not update automatically. Note: If modified, use the new IP for next login (computer must be on same subnet). |
| MAC | Physical address of the current bridge LAN interface. |
| IP Address | Digital label for a device on the network, used for unique identification and data communication. Set the bridge's static IP based on network status (e.g., 192.168.1.3). |
| Gateway | Manually specify the gateway address for the bridge's LAN port. |
| DNS | Manually specify the DNS server for the bridge's LAN port. |

➤ **Protocol ---DHCP client**

Network

Network Mode:

Spanning Tree: None STP

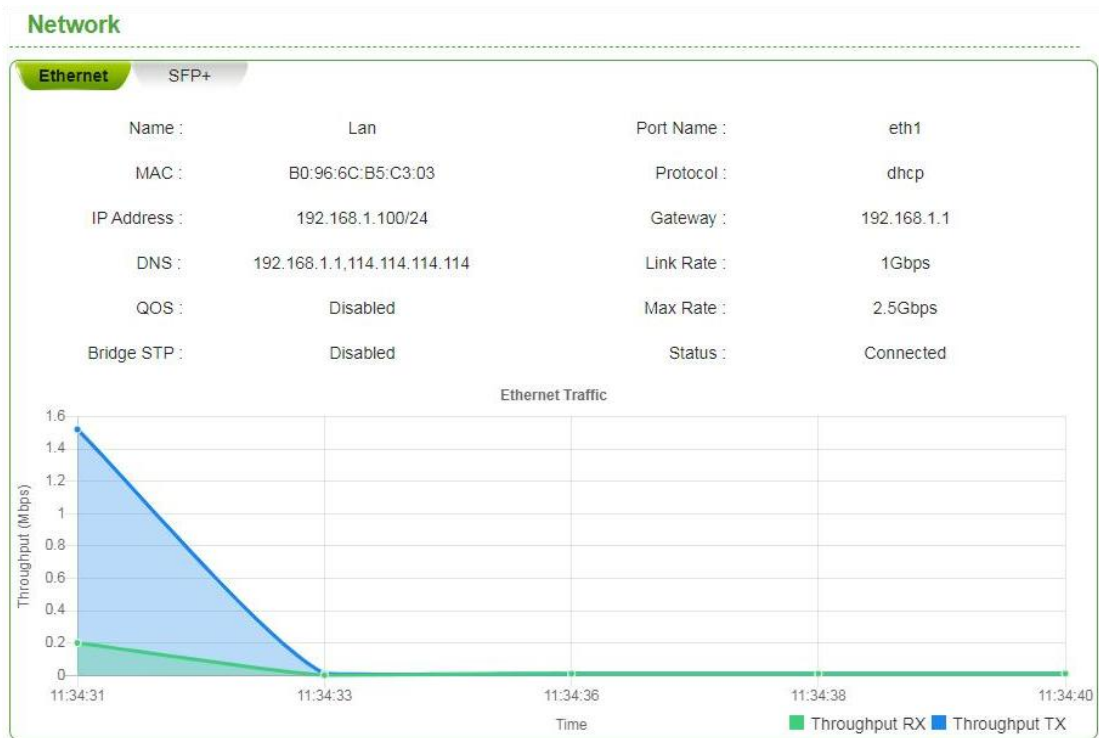
LAN

Protocol:

Management VLAN:

The bridge automatically obtains IP address, subnet mask, default gateway, and DNS server from a DHCP server. This method avoids IP conflicts and reduces management workload.

View the configuration obtained from the DHCP server under **【 Status 】** → **【 Overview 】** → **【 Network 】** .



➤ **Protocol--DHCPv6 Client**

Network

Network Mode:

Spanning Tree: None STP

LAN

Protocol:

Management VLAN:

The bridge automatically obtains configuration from a DHCPv6 server. Prerequisite: The upstream device supports IPv6 addresses and has the DHCPv6 server enabled.

View the IPv6 address assigned to the bridge on the upstream DHCPv6 server. Use "[IPv6 Address]" to access the management interface (e.g., [2409:8754:4c30:70:b288:7cff:fe56:4321]).

View the configuration obtained from the DHCP server under **【 Status 】** → **【 Overview 】** → "Network".

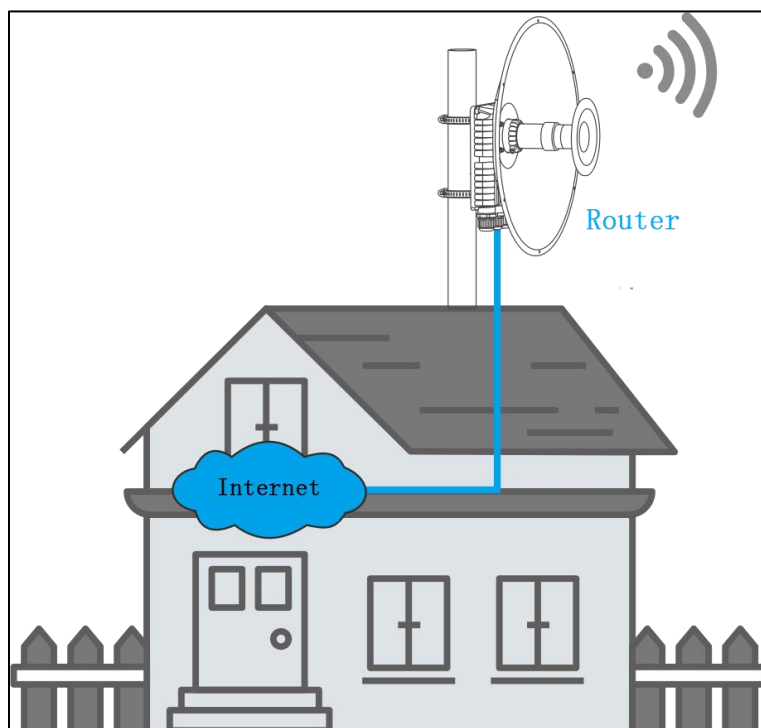
LAN IPv6 Parameter Description:

| Parameter | Description |
|------------|--|
| Protocol | "DHCPv6 Client": Automatically obtains IP address, subnet mask, gateway, DNS server information from a DHCPv6 server. |
| MAC | Physical address of the LAN port. |
| IP Address | Address assigned to the bridge by the DHCPv6 server; also the management address. When using, remove the trailing mask bits (e.g., [2409:8754:4c30:70:b288:7cff:fe56:4321]). |
| Gateway | Gateway address assigned by DHCPv6. ":::" here is similar to 0.0.0.0 in IPv4. |
| DNS | DNS server information assigned by DHCPv6. |

4.1.2 Router

The working method or strategy adopted by the router when forwarding data between different networks.

Application as shown:



Network Mode: Router

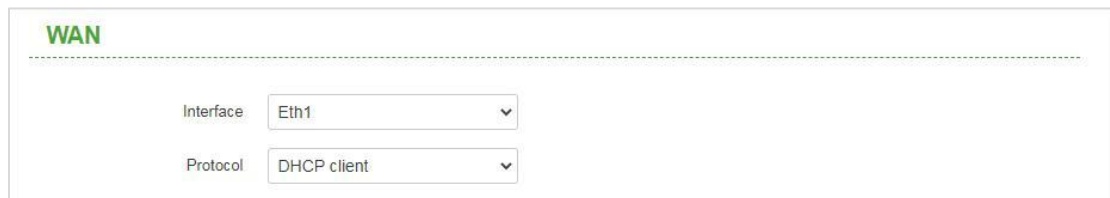


The screenshot shows a configuration window titled "Network". Below the title, there is a label "Network Mode" followed by a dropdown menu. The dropdown menu is open, and "Router" is selected.

● WAN

WAN (Wide Area Network) is a computer network covering a wide geographical area, used to connect LANs or other network devices in different regions, cities, or even countries, enabling long-distance data communication.

View the WAN interface type and WAN port address protocol type. The default protocol is "DHCP client".

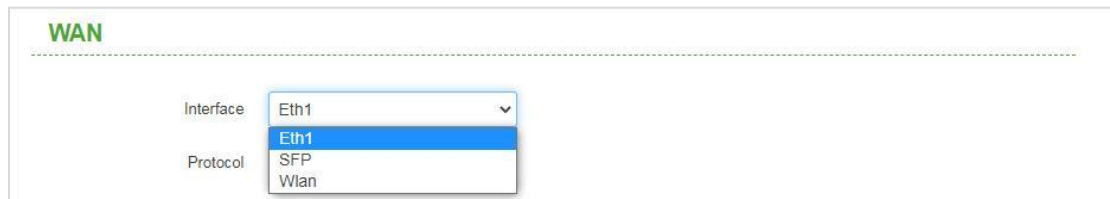


The screenshot shows a configuration window titled "WAN". Below the title, there are two labels: "Interface" and "Protocol". The "Interface" dropdown menu is open, and "Eth1" is selected. The "Protocol" dropdown menu is also open, and "DHCP client" is selected.

Interface Description:

1. ETH1: Designate the **ETH1** port as the WAN access port.
2. SFP: Designate the **SFP** port as the WAN access port.
3. Wlan: Designate the wireless interface as the **WAN** access port.

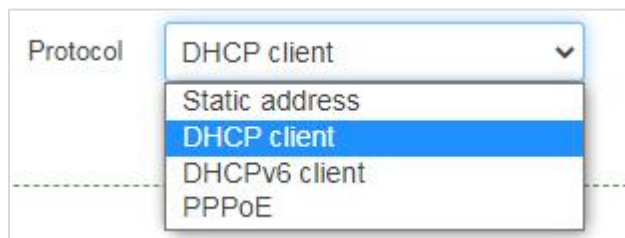
Common network types: Wired Router AP + Wireless Bridge CPE.



The screenshot shows a configuration window titled "WAN". Below the title, there are two labels: "Interface" and "Protocol". The "Interface" dropdown menu is open, and "Eth1" is selected. The "Protocol" dropdown menu is also open, and "SFP" is selected.

Set the bridge's IP address protocol and modify the address in router mode.

The current bridge WAN port supports four IP acquisition methods: "Static IP", "DHCP Client", "DHCPv6 Client", "PPPoE".



The screenshot shows a configuration window titled "WAN". Below the title, there is a label "Protocol" followed by a dropdown menu. The dropdown menu is open, and "DHCP client" is selected.

| Protocol Type | Description |
|----------------|---|
| Static address | Fixed IP address, subnet mask, gateway, DNS server, etc., manually assigned to a network device; does not update automatically. |
| DHCP client | Device that requests and accepts network parameters (IP address, subnet mask, gateway, DNS server, etc.) assigned by a DHCP server. Automatically obtains network configuration via DHCP protocol, no manual IP setup required. |
| DHCPv6 client | Device that requests and accepts network parameters (IP address, subnet mask, gateway, DNS server, etc.) assigned by a DHCPv6 server. Automatically obtains network configuration via DHCPv6 protocol, no manual IP setup required. |
| PPPOE | A network protocol for transmitting PPP (Point-to-Point Protocol) over Ethernet, mainly used for broadband dial-up internet access. Requires broadband username and password authentication for network communication. |

➤ **Protocol—Static address**

Manually specify the IP address, subnet mask, gateway, and DNS server for the WAN port.


Note: Fill in IP information on the same subnet as the upstream router to access the internet correctly.


The screenshot shows a configuration window titled "WAN". It contains the following fields and values:

- Interface: SFP
- Protocol: Static address
- IPv4 address: 192.168.22.199
- IPv4 netmask: 255.255.255.0
- IPv4 gateway: 192.168.22.1
- IPv6 Mode: Native
- IPv6 address: (empty)
- IPv6 gateway: (empty)
- DNS: 8.8.8.8 (with a red 'X' icon) and 9.9.9.9 (with a green '+' icon)

Setup Steps:

1. Interface: Designate the **WAN** interface.
2. Protocol: Select "**Static address**" from the dropdown menu.
3. IPv4 Address: Set an IP address on the same subnet as the upstream router (e.g., 192.168.22.199).
4. IPv4 Subnet Mask: Set the subnet mask (e.g., 255.255.255.0).
5. IPv4 Gateway: Set the gateway address (i.e., the LAN port IP of the upstream router, e.g., 192.168.22.1).

6. DNS: Set the DNS server. Add multiple using  .

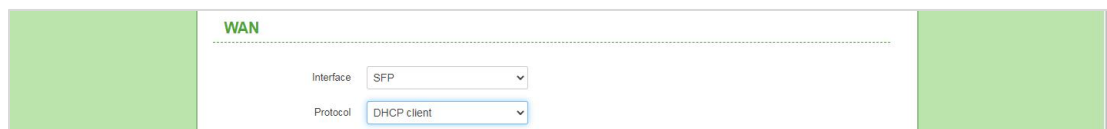
7. Click  to save the configuration.

View WAN port configuration under **【Status】** → **【 Overview】** → **【Network】** → **【SFP+】** .



➤ Protocol—DHCP Client


The bridge automatically obtains IP address, subnet mask, default gateway, and DNS server from a DHCP server on the network. This method avoids IP conflicts and reduces management workload.



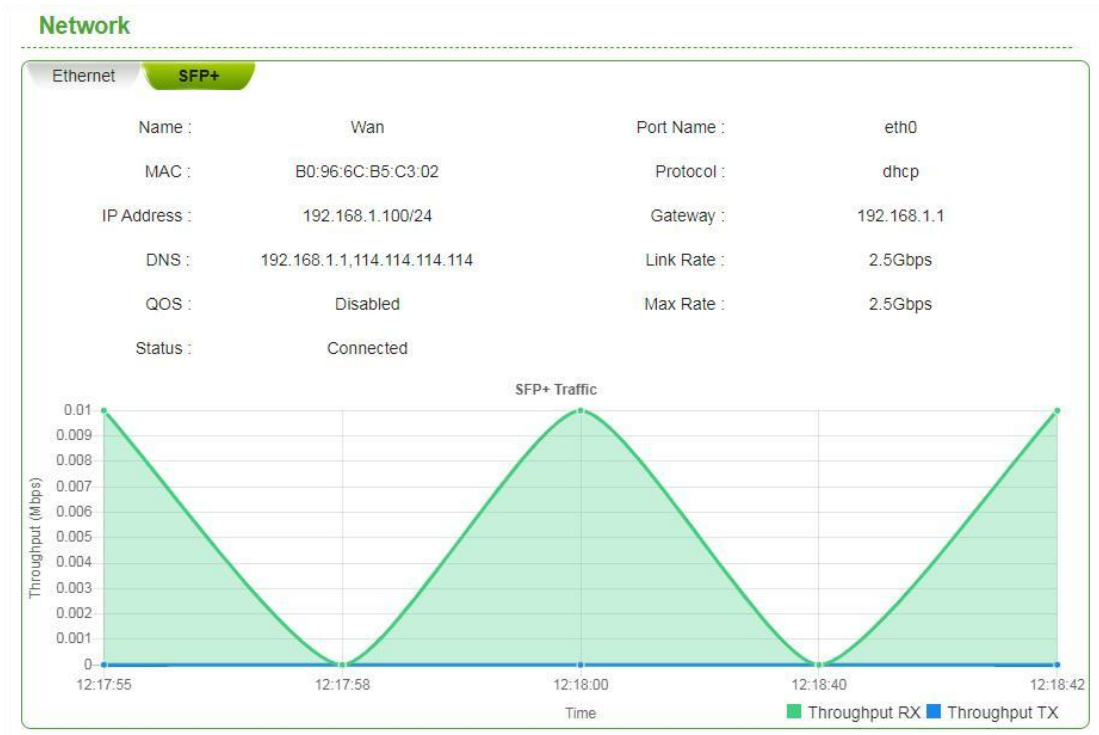
The figure shows the WAN configuration page. The "Interface" dropdown menu is set to "SFP" and the "Protocol" dropdown menu is set to "DHCP client".

Setup Steps:

1. Protocol Type: Select "DHCP client" from the dropdown menu (default is "DHCP client").

2. Click  to save the configuration.

View DHCP client configuration under **【Status】** → **【 Overview】** → **【Network】** → **【SFP+】** .



Partial Parameter Description:


| Parameter | Description |
|--------------|---|
| Name | Interface name. |
| Port Name | Name of the hardware interface designated as WAN. |
| MAC | Physical address of the WAN port. |
| Protocol | DHCP client, automatically obtains IP address information from the upstream router's DHCP server. |
| IP Address | IP address assigned by the DHCP server. |
| Gateway | Gateway address assigned by the DHCP server, usually the LAN port address of the upstream router. |
| DNS | DNS address assigned by the DHCP server. Supports multiple DNS server input. |
| Link Rate | Actual data transfer rate of the SFP+ hardware interface connected to the network. |
| Max Rate | Theoretical maximum data transfer rate of the SFP+ hardware interface. |
| QOS | Status of the QOS function (On/Off). |
| Status | Connection status of the SFP+ interface. |
| SFP+ Traffic | Displays real-time download and upload traffic for the ETH1 physical interface. |

➤ **Protocol—DHCPv6 Client**

The bridge automatically obtains IP address, subnet mask, default gateway and DNS server from a DHCPv6 server on the network. This method avoids IP conflicts and reduces management workload.

The screenshot shows the WAN configuration interface. It features three dropdown menus: '接口' (Interface) set to 'SFP', '协议' (Protocol) set to 'DHCPv6 client', and 'IPv6 Mode' set to 'Native'.

Setup Steps:


1. Select "DHCPv6 client" from the dropdown menu.
2. Click  at the bottom of the page to complete the configuration.

View DHCPv6 client configuration under **【Status】** → **【Overview】** → **【Network】** → **【SFP+】** .

➤ **Protocol—PPPOE**

A network protocol for transmitting PPP (Point-to-Point Protocol) over Ethernet, mainly used for broadband dial-up internet access. Requires broadband username and password authentication for network communication.

Setup Steps:

1. Interface: Designate the WAN port.
2. Protocol: Select "PPPOE" from the dropdown list.
3. Username: Enter the username provided by the ISP/server (e.g., 11).
4. Password: Enter the password provided by the ISP/server (e.g., 11).
5. Access Concentrator: Enter as provided by ISP/server; default "Auto".
6. Service Name: Enter as provided by ISP/server; default "Auto".
7. Click  to complete the configuration.

The screenshot shows the WAN configuration interface for PPPOE. It includes the following fields: 'Interface' (SFP), 'Protocol' (PPPoE), 'Username' (11), 'Password' (masked with dots), 'Access Concentrator' (auto), and 'Service Name' (auto).

Partial Parameter Description

| Parameter | Description |
|---------------------|--|
| Interface | Designate the WAN port. |
| Protocol | PPPOE, communication via point-to-point protocol. |
| Username | PPPOE username, provided by ISP/server. |
| Password | PPPOE password, provided by ISP/server. |
| Access Concentrator | Default "Auto". |
| Service Name | PPPOE server name, provided by ISP/server; default "Auto". |

View PPPOE configuration under **【Status】** → **【Overview】** → **【Network】** → **【SFP+】** .



Partial Parameter Description:

| Parameter | Description |
|------------|---|
| Protocol | Dial-up Internet (PPPOE). |
| IP Address | IP address assigned by the PPPOE server (e.g., 10.1.1.2 is the IP address, 32 is the subnet mask length). |
| DNS | DNS server issued by the PPPOE server. |
| Gateway | LAN address of the upstream server. |

● **LAN**

LAN (Local Area Network) refers to a computer network connecting multiple devices (computers, printers, servers, etc.) within a limited geographical area (e.g., office, home, campus, factory) via communication lines or wireless signals to achieve data transmission and resource sharing.

Set the bridge's LAN interface IP address information in router mode on this page.



Note: If the device's IP address is modified, the new IP address must be used for the next login (computer must be on the same subnet) to enter the management interface.

LAN

IPv4 地址

IPv4 子网掩码

DNS ✕

+

保存并应用

4.2 DHCP

4.2.1 DHCP Server

Go to **【Network】** → **【Network】** → "Network" → "Network Mode: Router" → " Save & Apply ", to enable router mode.

The DHCP server can automatically assign IP addresses, network parameters (subnet mask, default gateway, DNS server address), and address leases (assignment, renewal, release) to clients, avoiding manual configuration hassles and errors. If "Network Mode: Bridge", the DHCP server is disabled and hidden by default.

Go to **【Network】** → **【DHCP】** to enter the settings page.

DHCP Server » Lan

Enable

Start IP address

End IP address

Lease time (e.g. 2m, 12h, 7d)

DHCP Server Setup Steps (Default: Enabled):

1. Enable: Click "**Enable**" to start the DHCP server.
2. Start IP address: Set the starting IP address of the IP pool.
3. End Address: Set the ending IP address of the IP pool.
4. Lease Time: Duration the IP is available to the client.
5. Click Save & Apply to complete the configuration.



Note: If other DHCP servers exist in this network, ensure the IP addresses set for the bridge's DHCP server do not conflict with those of other DHCP servers.

Parameter Description:

| Parameter | Description |
|------------------|---|
| Enable | Enable/Disable the DHCP server. Default: Enabled. |
| Start IP address | Starting IP address of the DHCP server's IP pool. |
| End IP address | Ending IP address of the DHCP server's IP pool. |
| Lease time | Duration the IP address assigned by the DHCP server is available to the client. |

4.2.2 Static Lease

Convert dynamically assigned DHCP IP addresses into static addresses. To avoid conflicts, ensure the static IP address is not in use by any client before setting.

Static Lease

| Hostname | MAC-Address | IPv4-Address | Lease time |
|--|-------------|--------------|------------|
| <i>This section contains no values yet</i> | | | |

Add Static Lease Steps:

1. Click .
2. Hostname: Custom hostname for identification.
3. MAC-Address: Select MAC address from the dropdown list. If the target MAC is not listed, add it manually. If unsure, check the "**Assigned DHCP Leases**" list.
4. IPv4-Address: Assign a specific IP address to this user. Ensure the IP is unused to avoid conflicts.
5. Lease time: Specify the available lease duration for the IP. Default: 12h. Other units: m (minutes), h (hours), d (days).
6. Click to save the configuration.
7. Click to complete the configuration.

Static Lease - Add Entry

Hostname

MAC-Address

IPv4-Address

Lease time (e.g. 2m, 12h, 7d)

The static lease list shows created static lease rules.

Static Lease

| Hostname | MAC-Address | IPv4-Address | Lease time | |
|----------|-------------------|--------------|------------|---|
| PC-01 | 00:13:3B:13:14:BE | 192.168.1.88 | 12h | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| PC-02 | B0:55:21:AB:CC:22 | 192.168.1.99 | 2d | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

4.2.3 DHCP Leases

Display IP address information obtained by clients from the DHCP server.

Go to **【Network】** → **【DHCP】** → "Assigned DHCP Leases" to view client information.

Active DHCP Leases

| Hostname | IPv4 address | MAC address | Lease time remaining |
|-------------------|---------------|-------------------|----------------------|
| - | 192.168.1.185 | 00:50:BA:50:73:2E | 11h 59m 46s |
| - | 192.168.1.184 | 00:50:BA:50:73:2D | 11h 59m 46s |
| - | 192.168.1.183 | 00:50:BA:50:73:2C | 11h 59m 46s |
| - | 192.168.1.182 | 00:50:BA:50:73:2B | 11h 59m 46s |
| - | 192.168.1.181 | 00:50:BA:50:73:2A | 11h 59m 46s |
| - | 192.168.1.180 | 00:50:BA:50:73:29 | 11h 59m 46s |
| - | 192.168.1.178 | 00:50:BA:50:73:27 | 11h 59m 46s |
| - | 192.168.1.179 | 00:50:BA:50:73:28 | 11h 59m 46s |
| - | 192.168.1.176 | 00:50:BA:50:73:25 | 11h 59m 46s |
| rbwww (rbwww.lan) | 192.168.1.177 | 00:50:BA:50:73:26 | 11h 59m 46s |

Active DHCPv6 Leases

| Host | IPv6 address | DUID | Lease time remaining |
|------|--------------------------|---|----------------------|
| qwe1 | fd4d:eae0:f5db::5bc3/128 | 00:01:00:01:29:b0:6f:37:30:5a:3a:54:f5:28 | 11h 35m 35s |

Parameter Description:

| Parameter | Description |
|----------------------|--|
| Hostname | Client host name. |
| IPv4 address | IP address assigned to the client by the DHCP server. |
| MAC address | Physical address of the client. |
| Lease time remaining | Remaining available time for the IP address assigned to the client by the DHCP server. |

4.3 QOS

QOS(Quality of Service)is used to solve network latency, bandwidth contention, data packet loss

and other issues, ensuring priority transmission of critical business data (e.g., video conferencing, online gaming, realtime communication) to enhance user experience.

Maximum Rate:

QOS is disabled by default. Click " **Enabled** " to enable QOS service.

Maximum Rate

Maximum Rate Disabled Enabled

Download (kbps)

Upload (kbps)

Parameter Description:

| Parameter | Description |
|----------------|--|
| Maximum Rate | QOS function switch button. Default: Off. |
| Download(kbps) | Enable QOS function, specify download data transfer rate for the device. |
| Upload(kbps) | Enable QOS function, specify upload data transfer rate for the device. |

4.4 TR069

CPE WAN Management Protocol: The network management protocol is used to enable service providers (SPs) to remotely manage and configure user-side equipment (CPE, such as routers, optical modems, set-top boxes, etc.). It is widely used in broadband, Internet of Things and other scenarios.

TR069 Configuration

Enable

ACS URL

ACS Username

ACS Password

Periodic Enable

Periodic Interval

Connect Request

Username

Password

[Save & Apply](#)

4.5 SNMP

SNMP (Simple Network Management Protocol) is a standard protocol for managing devices in IP networks (such as routers, switches, servers, printers, etc.) and is an application layer protocol. It monitors and manages network devices through the network management system (NMS) to implement functions such as device status query, configuration management, performance statistics, and fault alarms.

Snmp Setting

Server Enabled

Protocol Version

Server Port

Get Community

Set Community

Location

Contact

Name

[Save & Apply](#)

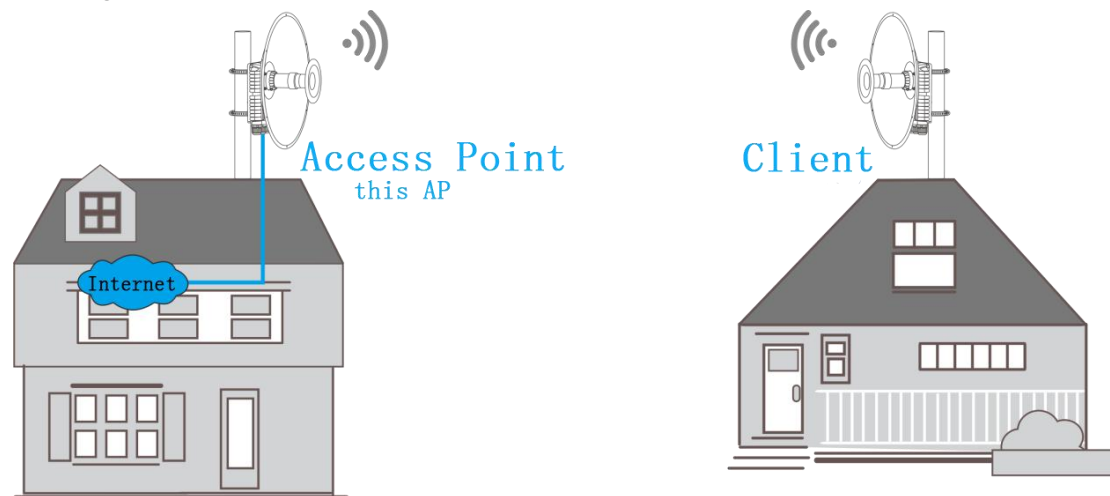
Chapter 5 Wireless

5.1 Wireless Configuration

5.1.1 Access Point

AP is mainly used to connect wired network and wireless devices (such as mobile phones, laptops, etc.) to enable wireless terminals to access wired network.

The usage scenarios are as follows:



Setting up the wireless configuration of the bridge.

Click the first-level directory [**Wireless**] to enter the configuration page.

Wireless Configuration

Driver Mode Standard Wifi Wis TDMA

Mode **Access Point** Client

SSID: WIF17-bridge

Encryption: WPA3-SAE

Key: 12345678

Hide SSID

Isolate Clients

Output Power (EIRP) 26 dBm

Operating frequency Mode: BE Channel: 120 (5600 Mhz) Width: 160 MHz

Max Rate: AUTO

Country Code: No Country

Antenna Gain

Antenna Gain: 8 dBi

Save & Apply

Setup Steps:

1. Mode: Select the bridge working mode, the default is "Access Point AP". Select "Access Point AP" for AP mode.
2. SSID: Modify the wireless signal name of the bridge, eg. Wireless-WIF17.
3. Encryption: Select the encryption method. Recommend to select "WPA3-SAE".
4. Key: Wireless WIFI password, the default is: "12345678".
5. Channel: Pull down menu and select wireless working channel.
6. Click **Save & Apply**, Complete the configuration.

Parameter Description:

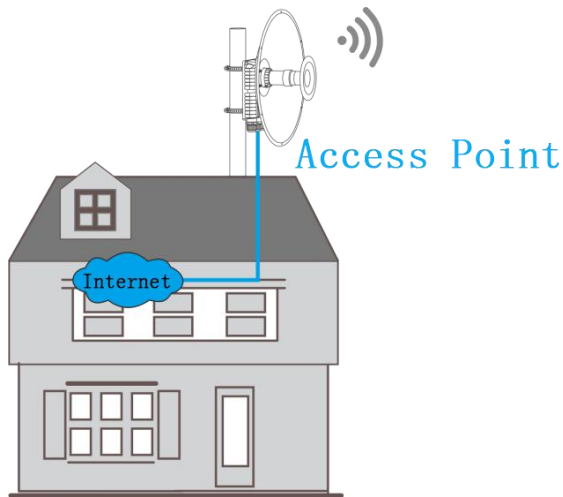
| Parameter | Description |
|-------------|--|
| Driver Mode | Radio operating mode, support standard WIFI, Wis TDMA. |
| SSID | Service Set Identifier, it is the name used in wireless local area networks (WLANs) to identify a specific wireless network. When a device (such as a mobile phone or computer) searches for WIFI, the displayed network name is called SSID. Users can connect to the corresponding wireless network by selecting the correct SSID and entering the password (if encryption is enabled). |
| Encryption | Wireless encryption method. Support "WPA3-SAE, WPA3-SAE/WPA2-PSK, |

| | |
|----------------|--|
| | WPA2-PSK". |
| Key | Wireless WIFI password. Default is 12345678. |
| Hide ESSID | Tick the button to hide the wireless signal name. The default setting is: Untick. |
| Isolate Client | Wireless clients connected to the same AP cannot discover or communicate with each other; they can only communicate with the wired network of the access point. |
| Output Power | The power value used by wireless communication devices when transmitting signals directly affects the coverage range, penetration power and possible interference level of the wireless signal. The range of values: 1 - 26 dBm |
| Mode | Select the 802.11 working mode. By default, the bridge is set to the BE mode. It supports modes such as 11N, 11AC, 11AX, and 11BE. |
| Channel | In wireless communication, the "virtual channels" for signal transmission are similar to lanes on a highway. Different frequency channels are independent of each other, and devices avoid interference by using specific channels. |
| Channel Width | Also named channel bandwidth. Refers to the frequency range occupied by the signal in wireless communication (unit: MHz). It directly affects the transmission rate, anti-interference capability and spectrum utilization rate of the network. The default frequency is 160 MHz. It supports 20 MHz, 40 MHz, 80 MHz and 160 MHz. |
| Max Rate | MCS is the core mechanism for achieving a balance between "reliability" and "efficiency" in wireless communication. By dynamically adjusting modulation and coding methods, it enables the network to efficiently transmit data under different channel conditions. The default setting is: auto. It supports the selection of: auto, MCS0 to MCS13. |
| Country Code | Select the current country to adapt to the local wireless communication standards and laws / regulations. |
| Antenna Gain | Antenna gain is an important indicator for measuring the ability of an antenna to concentrate the input power and radiate it in a specific direction. It directly affects the coverage range, transmission distance and anti-interference capability of the wireless signal. By measuring the actual gain of the antenna when it is externally connected to the equipment, it helps to improve the performance of the equipment. |

5.1.2 Client

Switch the wireless network mode to "Client". Generally used in conjunction with the "Access Point" mode.

Click **【Wireless】** , enter this page, Change "Mode" to "Client". The usage scenario is as follows:



Client side setup steps:

1. Mode: Choose "Client";
2. SSID: Specify the name of the wireless signal, eg. Wireless-WIFI7;
3. Encryption: Choose the encryption method. It is recommended to select "WPA3-SAE";
4. Key: Wireless WIFI password, eg. 12345678;
5. Width: Select wireless bandwidth, the default frequency is 160 MHz. It supports 20 MHz, 40 MHz, 80 MHz, 160 MHz, and 320 MHz;
6. Click Save & Apply, Complete configuration.

⚠️ Note: The above configurations in the client mode must be consistent with those of the upper-level AP in order to successfully connect to the AP.

Wireless Configuration

Driver Mode Standard Wifi Wis TDMA

Mode Access Point Client

Scan ▶

SSID

Encryption

Key 👁

Output Power (EIRP) 26 dBm ⬇

Operating frequency Mode Channel 120 (5600 Mhz) Width

Max Rate

Country Code



Antenna Gain

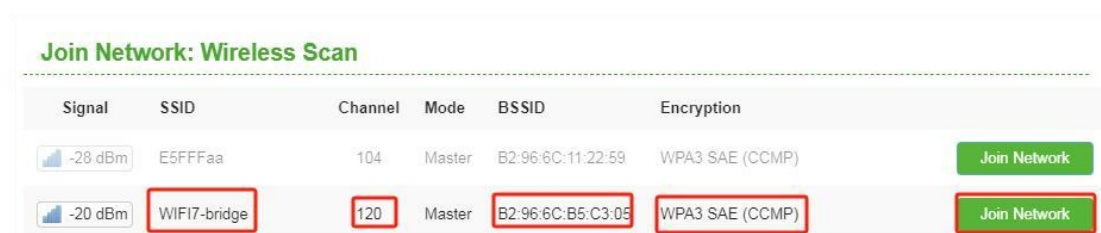
Antenna Gain dBi

SCAN Usage steps:

Using the "SCAN" function, add the target AP.


execution step:

1. Click .
2. Select the target AP through "SSID" and "BSSID".
3. Confirm the target AP. Click .



Part of Parameter Description:

| Parameter | Description |
|------------|--|
| Signal | The client detects the wireless signal strength of the AP by scanning. |
| SSID | The wireless signal name of the AP in the wireless network. |
| Channel | Wireless channel used by the superior AP. |
| Mode | The wireless mode of the superior AP. |
| BSSID | The wireless physical address of the superior AP. |
| Encryption | The wireless encryption method of the superior AP. |

4. After the page is redirected, enter the WIFI password.
5. Enter the AP password.
6. Click . Complete configuration.
7. Wait for a few seconds, and the client device will automatically connect to the superior AP.

Wireless Configuration

Driver Mode Standard Wifi Wis TDMA

Mode

Scan

SSID

Encryption

Key

Output Power (EIRP) 26 dBm

Operating frequency

| Mode | Channel | Width |
|---------------------------------|---|--------------------------------------|
| <input type="text" value="BE"/> | <input type="text" value="120 (5600 Mhz)"/> | <input type="text" value="160 MHz"/> |

Max Rate

Country Code

Antenna Gain

5.3 MAC Acl

MAC Acl is a type of cybersecurity measure that enhances network access control by restricting the MAC addresses of devices that are allowed to connect to the network. The use of smart phones, laptops, computers and tablets is increasing gradually. Each device has its own corresponding MAC address. The access to the Internet of local network clients can be controlled through the MAC address filtering function. MAC address filtering has two access control modes: "Deny" and "Allow".

MAC rules

Select the MAC address filtering rule. It supports allowing MAC addresses to pass through or denying access to MAC addresses. The settings can be specified through the drop-down menu.

Mac Acl

Rules:

Deny Lists

| Hostname | MAC-Address |
|-------------------------------------|-------------|
| This section contains no values yet | |

Allow Lists

| Hostname | MAC-Address |
|-------------------------------------|-------------|
| This section contains no values yet | |

Deny Lists:

Add the client's MAC address to the list and prohibit the user from accessing the Internet.

Click , Create MAC address filtering rules.

Mac List - Add Entry

Hostname:

MAC-Address:

Create MAC address filtering rules:

1. Rule: Specify filtering rules. Default: Deny.
2. Click . The system pops up the creation interface.
3. Host name: Customized restriction on the host name of users based on MAC address, for easy distinction, such as PC01.
4. MAC address: Click on the drop-down menu and select the MAC address that needs to be restricted. You can also customize the MAC address, eg, B0:96:6C:E6:B6:04.
5. Click , Save configuration.
6. Click , complete configuration.

Added successfully. As shown in the following picture.

Mac Acl

Rules

Deny Lists

| Hostname | MAC-Address | |
|----------|-------------------|---|
| PC01 | B0:96:6C:E6:B6:04 | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

Allow Lists:

The MAC Acl is set to "Allow", which means that only the MACs listed in the "Allow Internet Access" table are permitted to access the internet.

Mac Acl

Rules

Allow Lists

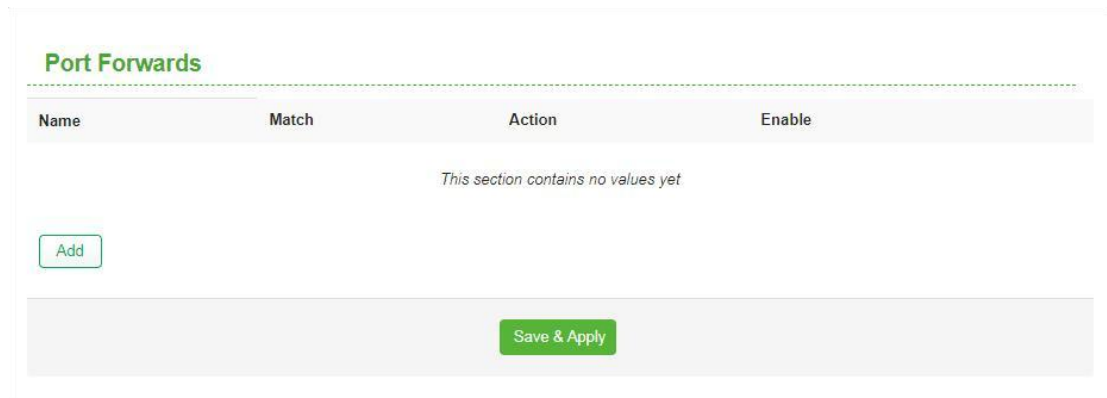
| Hostname | MAC-Address | |
|----------|-------------------|---|
| PC02 | 00:50:BA:50:73:2B | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| PC03 | 00:50:BA:50:73:29 | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

Chapter 6 Firewall

6.1 Port Forwards

Generally speaking, hosts in the WAN cannot actively access hosts in the LAN. Port forwarding enables WAN users to access the LAN host while protecting the internal LAN from intrusion. Port forwarding defines a service port and specifies its corresponding LAN server via IP address. The device directs service requests from the WAN for this port to that server.

Click **【Firewall】** → **【Port Forwards】** to enter this page.



Parameter Description:

| Parameter | Description |
|-----------|---|
| Name | The name of this port rule. |
| Match | Forward the matching rules from the WAN. If the service protocol type is uncertain, it is recommended to use TCP/UDP. |
| Action | Forward the messages of the WAN to the designated address within the LAN. |
| Enable | Enable/Disable this port forwarding rule. |

Port Forwarding Rule Example: Establish the network structure with the bridge and set the working mode to routing mode. The WAN port IP address of the device is: 192.168.2.100. When the network administrator is on a business trip and needs to access the device page to modify the configuration, this can be achieved through port forwarding rules. First, create the rule on the port forwarding page.

Note:

- Ensure the bridge WAN port has obtained a public IP address.
- If the bridge WAN port IP is dynamic, be prepared in advance.
- System firewalls, some antivirus software, and security guards may prevent other computers from accessing the server. It is recommended to temporarily disable them before using this function.

Step 1. Create port forwarding and add it successfully as follows:

Port Forwards

| Name | Match | Action | Enable | |
|-------|--|-------------------------|-------------------------------------|--|
| HTTPS | Incoming IPv4 From wan To this device, port 8888 | Forward to lan port 443 | <input checked="" type="checkbox"/> | <input type="button" value="⋮"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

Step 2. Internet users access the bridge management interface.

When Internet users access the intranet management interface, they only need to visit: <https://192.168.2.100:8888> on a computer that has obtained a public IP address.

System

| | | | |
|---------------|---------------------------------|-------------------------------------|---|
| Product Model | E5 | Firmware Version | 2.2.0.release |
| Mac | b0:96:6c:b5:c3:02 | Load Average | 0.39, 0.39, 0.20 |
| Local Time | 2025-05-28 01:59:40 | CPU Usage | <div style="width: 10%; background-color: green;">10%</div> |
| Uptime | 0h 5m 38s | Memory Usage | <div style="width: 47%; background-color: green;">197.74 MiB / 412.63 MiB (47%)</div> |
| SN | W0B26250400078 | <input type="button" value="Copy"/> | |
| BindCode | nCrVHqRTKQekp94GleJYUmS7H0jJpLC | <input type="button" value="Copy"/> | |

⚠️ Note:

- The "external interface" of the port forwarding rule cannot be the same as the "port number" of the remote WEB access, which will cause a conflict and lead to port forwarding failure.
- After setting the rule, Internet users can access it in the form of "protocol name://bridge wan port IP address: external interface".

6.2 Traffic Rules

Communication rules define the packet transmission strategy between different areas, for example: denying communication between some hosts and opening ports on the router WAN.

Traffic Rules

| Name | Match | Action | Enable | |
|--------------------|--|------------------------------|-------------------------------------|---|
| Allow-DHCP-Renew | Incoming <i>IPv4</i> , protocol <i>UDP</i> From wan To this device, port 68 | Accept input | <input checked="" type="checkbox"/> | <div style="display: flex; gap: 10px;"> ☰ Edit Delete </div> |
| Allow-Ping | Incoming <i>IPv4</i> , protocol <i>ICMP</i> From wan To this device | Accept input | <input checked="" type="checkbox"/> | <div style="display: flex; gap: 10px;"> ☰ Edit Delete </div> |
| Allow-IGMP | Incoming <i>IPv4</i> , protocol <i>IGMP</i> From wan To this device | Accept input | <input checked="" type="checkbox"/> | <div style="display: flex; gap: 10px;"> ☰ Edit Delete </div> |
| Allow-DHCPv6 | Incoming <i>IPv6</i> , protocol <i>UDP</i> From wan To this device, port 546 | Accept input | <input checked="" type="checkbox"/> | <div style="display: flex; gap: 10px;"> ☰ Edit Delete </div> |
| Allow-MLD | Incoming <i>IPv6</i> , protocol <i>ICMP</i> From wan, IP fe80::/10 To this device | Accept input | <input checked="" type="checkbox"/> | <div style="display: flex; gap: 10px;"> ☰ Edit Delete </div> |
| Allow-ICMPv6-Input | Incoming <i>IPv6</i> , protocol <i>ICMP</i> From wan To this device Limit matching to 1000 packets per second | Accept input | <input checked="" type="checkbox"/> | <div style="display: flex; gap: 10px;"> ☰ Edit Delete </div> |

Chapter 7 System

7.1 System

7.1.1 System Properties

Identify the device through system properties, view the device's Local Time and Timezone, and customize the "Hostname".

Properties

Local Time:

Hostname:

Timezone:

Parameter Description:

| Parameter | Description |
|------------|--|
| Local Time | Displays the device system time. After changing the time zone, you can correct it by clicking the time verification button (the default time zone is: UTC). |
| Hostname | Device identifier, used to uniquely identify and distinguish different devices in the network. |
| Timezone | A region divided by the coordinated global time, used to unify the standard time within a specific geographic area. Due to the rotation of the earth, there are differences in the alternation of day and night in areas of different longitudes. Time zones ensure that the time in the same area is consistent by dividing the earth into 24 areas with a theoretical width of 15 degrees of longitude (actually adjusted due to national boundaries, administrative regions, etc.). |

7.1.2 Language

Pull down the menu button and select "Language".

Language options: English, Spanish, Hebrew, Korean, Portuguese, Russian, Vietnamese, Chinese Simplified.

Language

Language:



7.1.3 Web server

A web server is a network-based (usually the Internet) software system that aims to enable data interaction and function sharing between different systems through standard communication protocols (such as HTTP/HTTPS).

Check Secure Connection (HTTPS) to enable HTTPS protocol access.

Web server

Secure Connection (HTTPS)

Secure server port

Server port

7.1.4 Time Synchronization

Time synchronization refers to the use of technical means to keep the clocks of different devices in the network (such as servers, computers, routers, etc.) consistent. Accurate time synchronization is crucial in scenarios such as distributed systems, financial transactions, log auditing, and scientific computing.

Time Synchronization

Enable NTP client

Provide NTP server

NTP server candidates

-
-
-
-
-

7.1.5 Logging

Log service related configuration.

Logging

System log buffer size:

External system log server:

External system log server port:

Log output level:

Cron Log Level:

7.2 Administration

Changing the administrator password for accessing the management interface.

Click **【System】** → **【Administration】** , enter this interface.

Password

Password:

Confirmation:

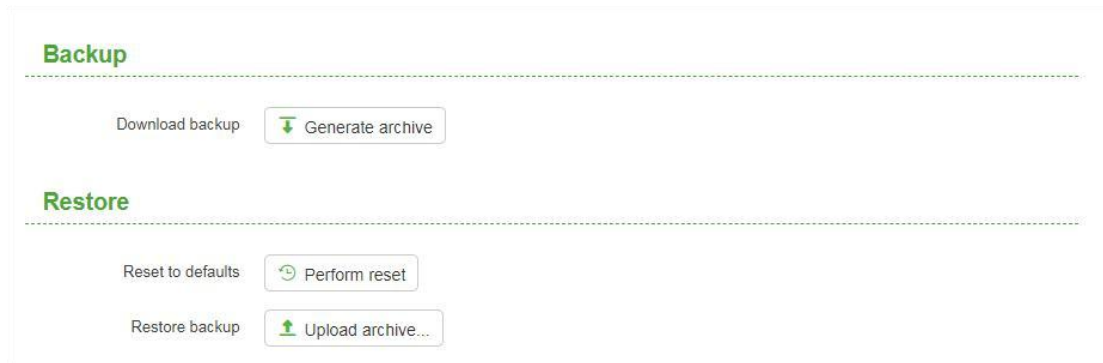
 **Note:**

Click to view the entered administrator password. The password here only applies to the administrator login password, not the WIFI password.

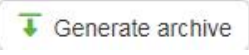
7.3 Backup / Upgrade

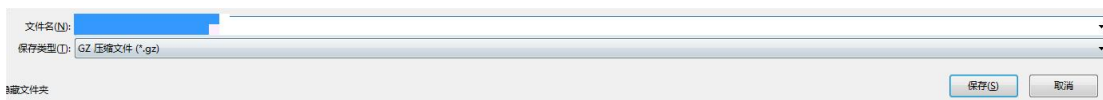
7.3.1 Backup / Restore

Back up the software configuration to facilitate import into other devices.





Backup steps:

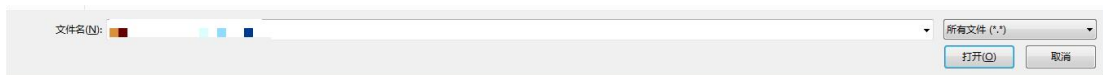
1. Click .
2. Specify the backup file path. It is recommended to modify the file name.




3. Select the backup file to upload.


Restore backup steps:

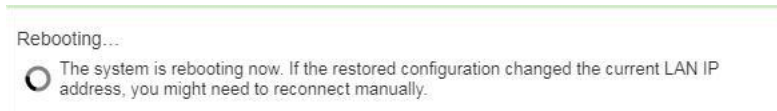
1. Click .
2. Click .
3. Select backup file to upload.



4. Confirm the uploaded file and click .



5. Find the button  and click.
6. Wait for the backup to be restored. After the system configuration is restored successfully, it will automatically jump to the login interface.



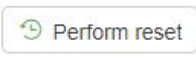
 **Note:** When restoring the system, please do not power off the device or unplug the network cable to avoid failure.

7.3.2 Restore

Through "Perform", the bridge configuration is restored to factory settings, and the configuration can also be restored to factory settings through the hardware (RST) key.



Steps:

1. Click .



2. System pop-up prompt "Do you really want to erase all settings?", then click "Yes".
3. Wait for firmware initialization.



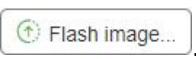

4. Device configuration reset complete.

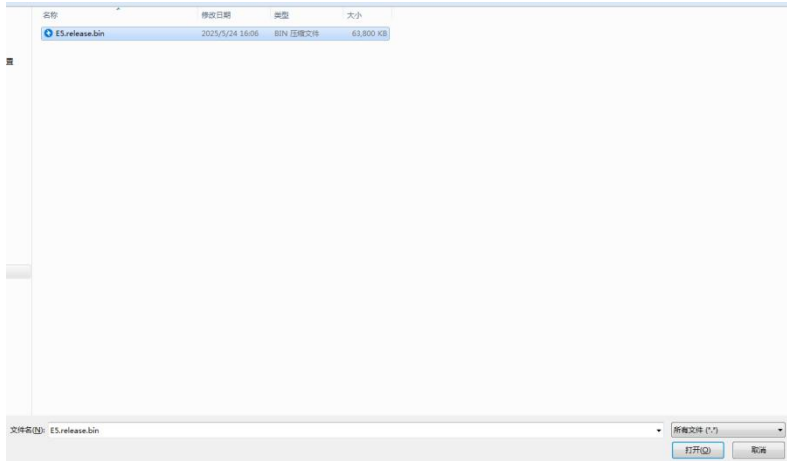
 **Note:** During the system reset process, please do not disconnect the power supply or unplug the network cable to avoid failure.

7.3.3 Flash new firmware image

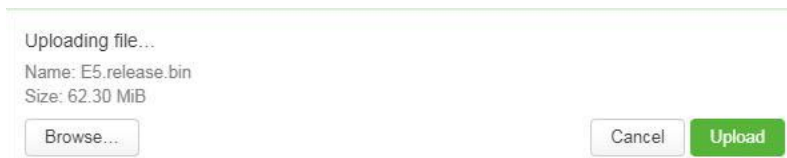
Upgrade the firmware version.

Steps:

1. Click .
2. Click , select the correct software version.



3. Confirm that the firmware has been uploaded correctly and click **Upload**.



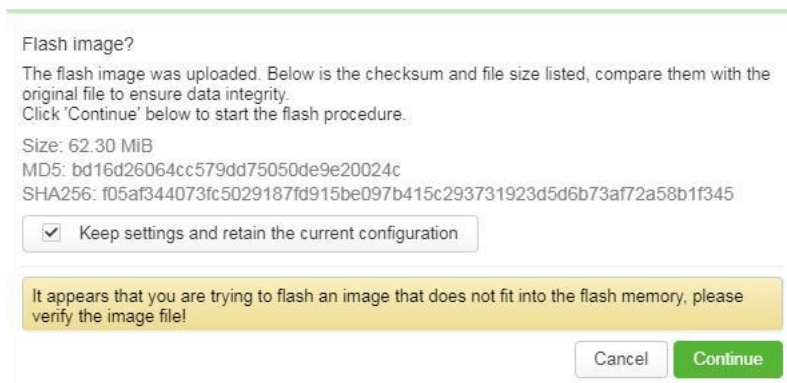
4. Waiting for firmware to upload.



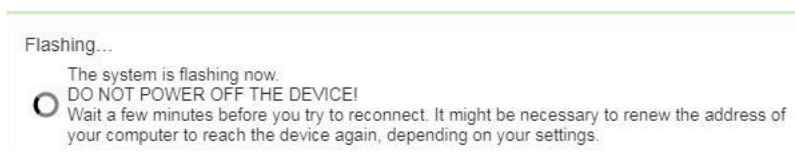
5. Click **Continue**, if you need to keep the original configuration after upgrading,

check **Keep settings and retain the current configuration**.


If you do not want to keep the configuration, do not check **Keep settings and retain the current configuration**.



6. Wait for the firmware to upgrade.



7. After the upgrade is completed, it will automatically jump to the login interface.

 **Note:** During the device upgrade process, please do not turn off the power or unplug the network cable to avoid upgrade failure, it will cause the system damage .

7.4 Reboot

7.4.1 Reboot

Restart the system immediately.



The screenshot shows a web interface titled "Reboot". Below the title, it says "Reboots the operating system of your device". There is a button with a power icon and the text "Perform reboot".

7.4.2 Schedule Reboot

Specify a device system to restart at a fixed time period. This function is often used in scenarios such as releasing resources, application updates, and fault self-healing.




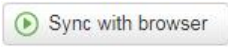
The screenshot shows a web interface titled "Schedule Reboot". It displays the "Current Time | 2025-05-23 11:40:42". There is a toggle switch for "Enable" which is currently turned off. Below that is a "Time" field with a "--:--" placeholder and a clock icon. Underneath is a "Week" section with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked. A green "Save & Apply" button is located at the bottom right.

Setup Steps:

1. Go to **【System】** → **【System】** → “System Properties”;
2. Change “Timezone” to the local time zone;

Timezone

3. Scroll to the bottom of the page, click  ;

4. After configuring the application, click  , the local time is converted to the local browser time;

5. Go to **【System】** → **【Reboot】** → “Schedule Reboot”, the current time has been converted to the local browser time;

6. Enable: Enable scheduled restart;
7. Time: You can select the corresponding time through the clock table, or enter the value by hour and minute (e.g., 9:00);
8. Week: Specify on which day(s) of the week when the device system reboots. You can select all or select one, such as Monday/Thursday;
9. Click Save & Apply, complete configuration.

Schedule Reboot

Current Time | 2025-05-23 11:45:32

Enable

Time

Week Sun Mon Tue Wed Thu Fri Sat

Save & Apply

7.5 System Log

System Logs is a collection of files or data that records the operating status, events, and error information of the operating system, applications, hardware devices, etc. It is like a "black box" of the system, used to monitor health status, troubleshoot, audit operations and optimize performance.

System Log

Log Type DEFAULT

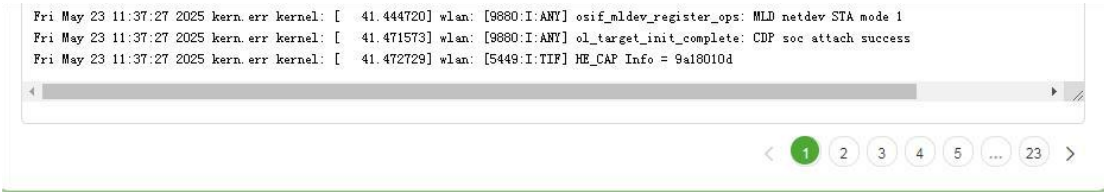
Current Time | 2025-05-23 11:46:22

Refresh
↓

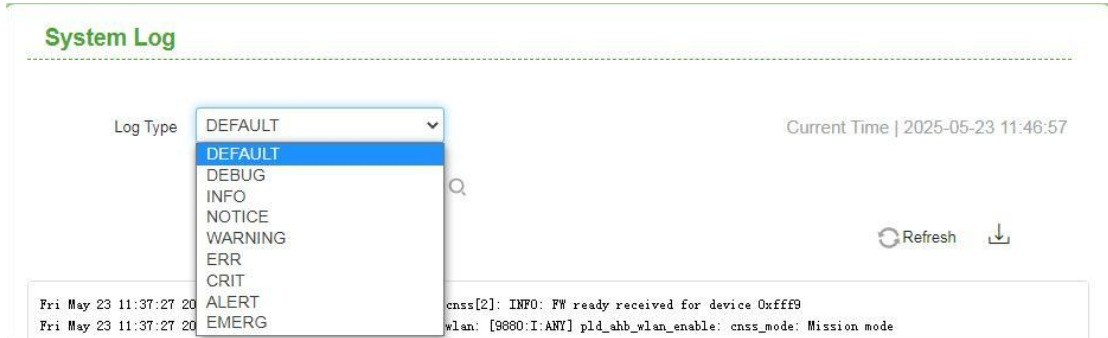
```


Fri May 23 11:37:27 2025 kern.err kernel: [ 41.209652] cnss[2]: INFO: FW ready received for device 0xffff9
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.209974] wlan: [9880:I:ANY] pld_ahb_wlan_enable: cnss_mode: Mission mode
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.218703] cnss[2]: INFO: Sending mode message, mode: MISSION(0), state: 0x7
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.277368] cnss[2]: INFO: Starting QDSS for QCA5332
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.277383] cnss[2]: INFO: Sending QDSS config download message, state: 0x7
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.281456] cnss[2]: INFO: No Custom QDSS config found, loading default file IPQ5332/qdss_trace_config
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.291244] wlan: [9880:D:dfs] WLAN_DEBUG_DFS1 : dfs_psoc_obj_create_notification: DFS obj attach to p
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.297846] cnss[2]: INFO: Sending QDSS Mode 1, option 0
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.297967] wlan: [9880:I:ANY] qdf_ini_parse: INI values read: 0
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.313955] wlan: [9880:I:ANY] qdf_ini_parse: INI file parse fail: invalid file format
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.319951] wlan: [9880:E:CONFIG] cfg_ini_parse_to_store: Failed to parse *.ini file @ QCA5332.ini; st
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.358996] wlan: [9880:E:CONFIG] cfg_uint_item_handler: num_vdevs=16 - Out of range [1, 9]; Using 9
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.359058] wlan: [9880:E:CONFIG] cfg_uint_item_handler: num_peers=512 - Out of range [1, 128]; Using
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.367237] wlan: [9880:E:CONFIG] cfg_uint_item_handler: num_monitor_vaps=1 - Out of range [0, 0]; Usin
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.379035] wlan: [9880:I:ANY] qdf_ini_parse: INI values read: 112
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.386204] wlan: [9880:I:ANY] qdf_ini_parse: INI file parse successful
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.395749] wlan: [9880:I:ANY] qdf_ini_section_parse: INI values parse successful read: 12 from section
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.400924] wlan: [9880:I:ANY] qdf_ini_section_parse: INI values parse successful read: 6 from section
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.410988] wlan: [9880:I:ANY] qdf_ini_section_parse: INI values parse successful read: 6 from section
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.420236] wlan: [9880:I:ANY] mlo_setup_update_num_links: Grp_id 0 Total MLD links = 1
Fri May 23 11:37:27 2025 kern.err kernel: [ 41.430287] wlan: [9880:I:ANY] ol_ath_soc_attach: WDS Extended is enabled

```





Through the "log type" drop-down list, select the system log type, the system supports log type filtering: DEFAULT, DEBUG, INFO, NOTICE, WARNING, ERROR, CRIT, ALERT, EMERG.



Through the "Search" filter box, filter the specified information, such as filtering: cfg. Input completed, then click .




Click  Refresh to refresh the system log.

Click the  on the right side of the page to save the filtered logs locally.

Download LOG steps:

1. Select "Log Type" or filter the specified LOG through "Search".


2. Click  . The system pops up a file box.
3. Select the local file save path (e.g., E:\benfeiwenjian).
4. Modify the file name as needed; default: Event_Logs_2025-05-27T02-28-20-414Z.txt.
5. Click “**Save**”. Confirm to save to local.
6. Wait for the file to download. Go to the E:\benfeiwenjian path and check the LOG.

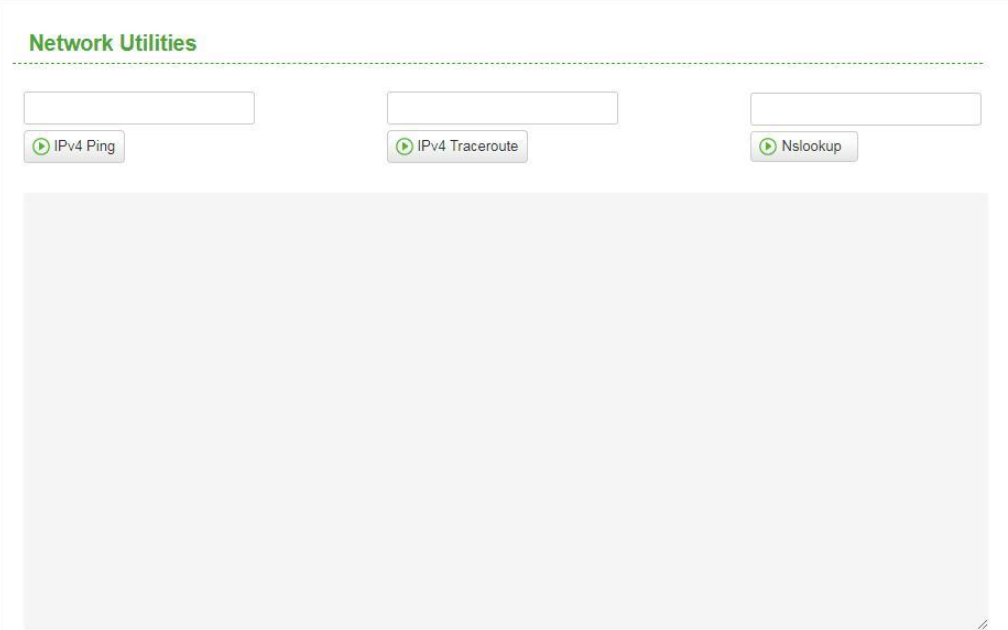
Chapter 8 Tools

8.1 Network Utilities

Network Utilities Tools, e.g., IPv4 Ping, IPv4 Traceroute, Nslookup.

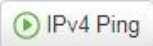
Click **【Tools】** → **【Network Utilities】** to enter this page.

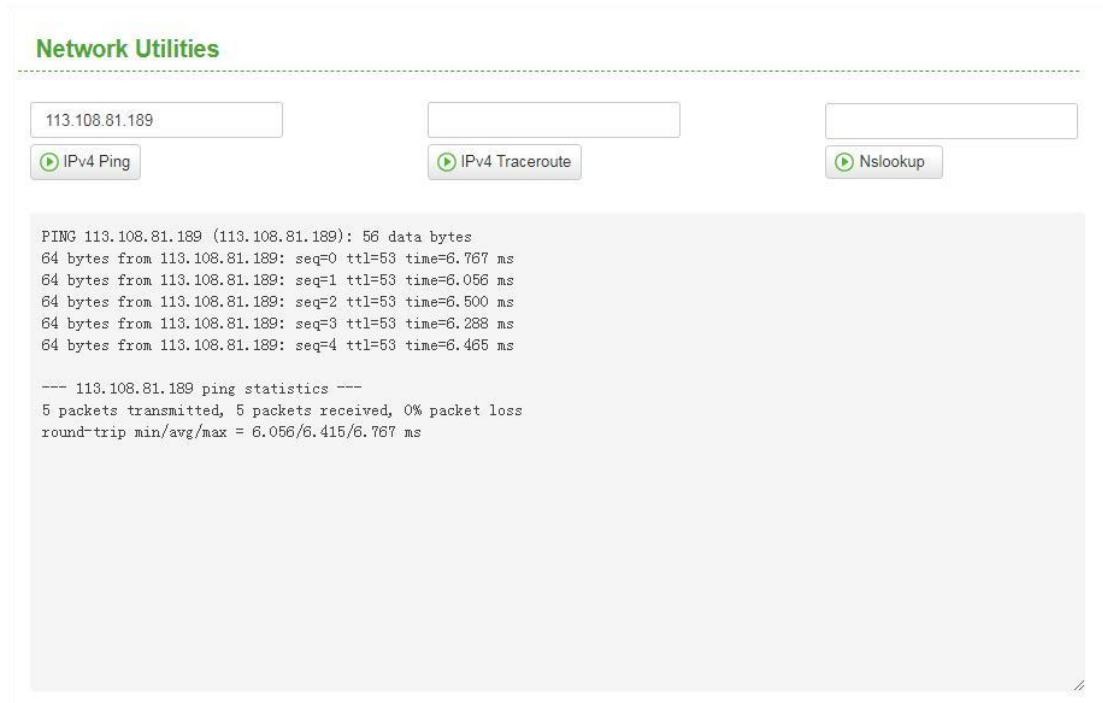
 **Note:** When using this tool, the wireless bridge is required to connect to the Internet, or only test addresses within the LAN.




Network Utilities

Ping Tool Usage Steps:

1. Specify the target IP address in the ping tool input box, eg. 113.108.81.189.
2. Click .
3. Wait a few seconds and the result will be displayed. The test is completed.




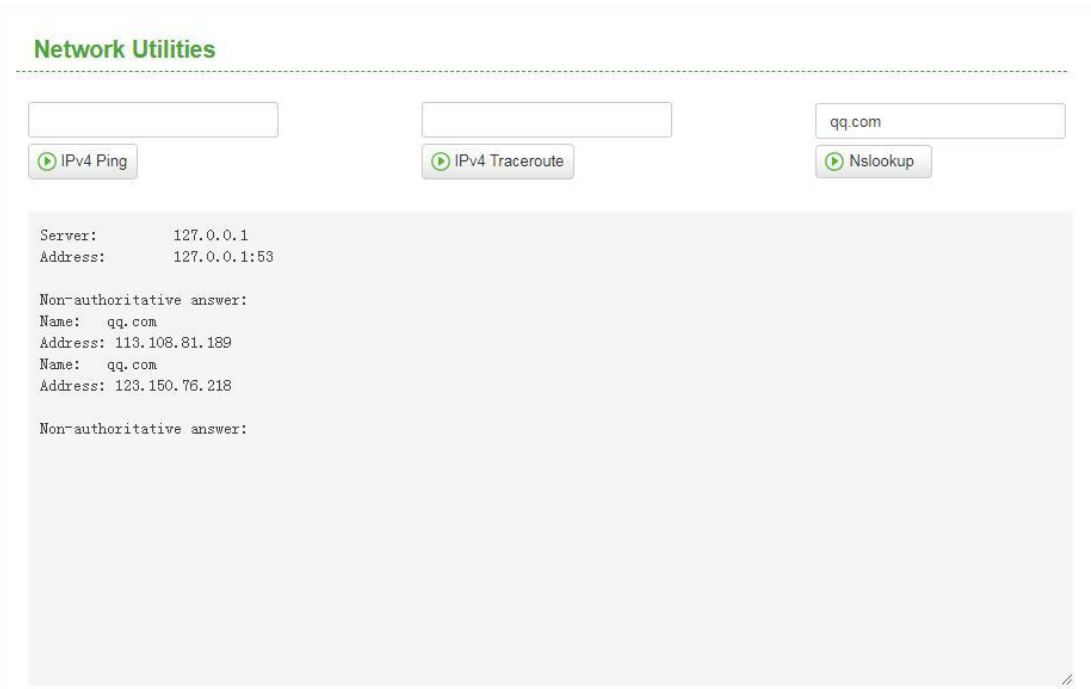
Traceroute Tool Usage Steps:

1. Specify the target IP address in the traceroute input box. e.g. 113.108.81.189.
2. Click .
3. Wait for a few seconds and the result will show that the route tracing is completed.



DNS Resolution Usage Steps:

1. Specify the target domain name in the domain name resolution input box, e.g., qq.com.
2. Click .
3. Wait a few seconds and the result will show that the domain name resolution is complete.



Network Utilities

IPv4 Ping IPv4 Traceroute qq.com Nslookup

```
Server:      127.0.0.1
Address:    127.0.0.1:53

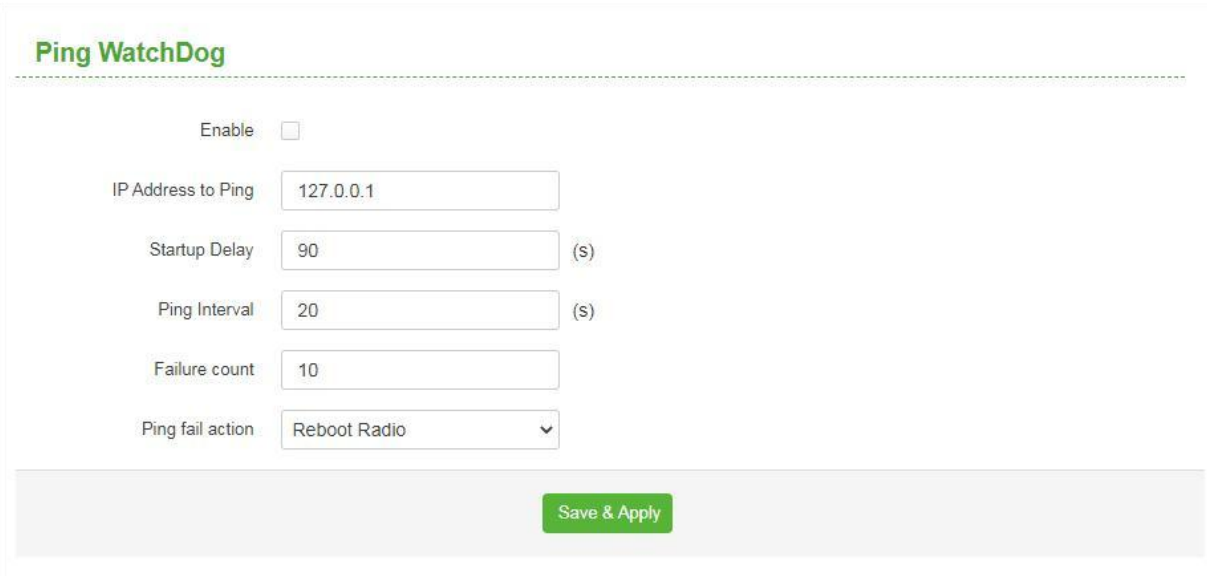
Non-authoritative answer:
Name:   qq.com
Address: 113.108.81.189
Name:   qq.com
Address: 123.150.76.218

Non-authoritative answer:
```

8.2 Ping WatchDog

Ping watchdog can be used to detect the network connectivity of the bridge in real time. However, if the network/destination address is not accessible, the bridge is specified to restart the system/network after the specified number of ping failures. By default, Ping watchdog is turned off.

Click **【Tools】** → **【Ping WatchDog】** , and enter this page.



Ping WatchDog

Enable

IP Address to Ping

Startup Delay (s)

Ping Interval (s)

Failure count


Ping fail action

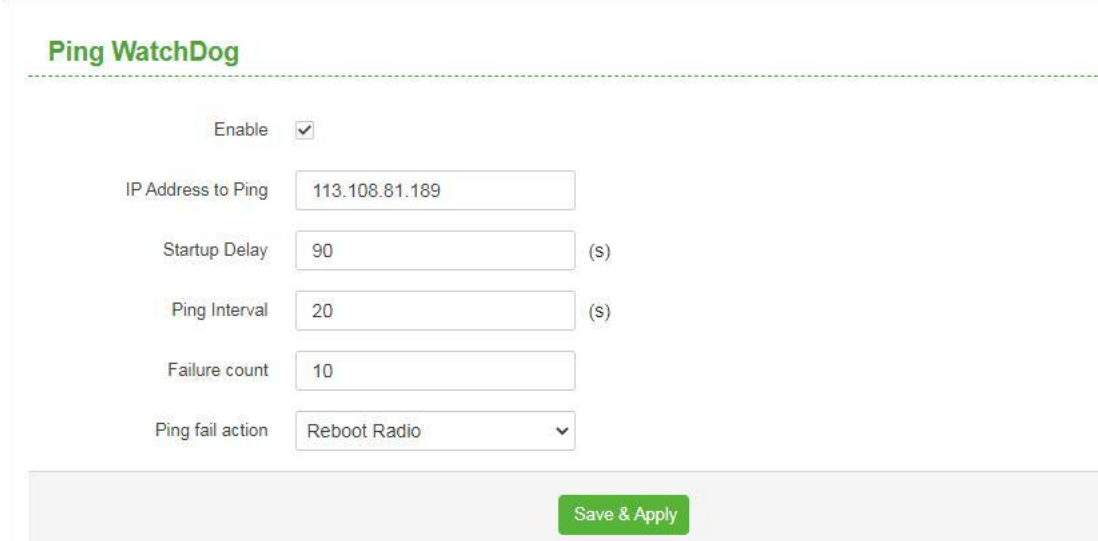
Save & Apply

Parameter Description:

| Parameter | Description |
|----------------------|---|
| Enable | Enable/Disable Ping Watchdog. |
| Ping Address to Ping | Specifies the target IP address to ping. |
| Startup Delay | How long to wait before detecting activation. |
| Ping Interval | Specify the time interval between pings. |
| Failure count | Ping failure count detected. |
| Ping fail action | When the Ping detection fails for a specified number of times, the program will perform the specified operation, e.g., Reboot Radio、Restart wireless. |

Ping Watchdog Steps:

1. Enable: Enable the Ping watchdog.
2. Ping Address to Ping: Specify the target IP address for Ping (e.g., 113.108.81.189).
3. Startup Delay: Specify the delay time before detecting the target IP(e.g., 90).
4. Ping Interval: Specify the Ping Interval (e.g., 20).
5. Failure count: Specify the number of ping failure (e.g., 10).
6. Ping fail action: When the ping detection fails for a specified number of times, the specified action is performed. In this example, the device is restarted.
7. Click  , and complete configuration.



Ping WatchDog

Enable


IP Address to Ping

Startup Delay (s)

Ping Interval (s)

Failure count

Ping fail action



8.3 Discovery

Scan the product models and related information in the wireless bridge LAN.
Click **【Tools】** → **【discovery】** and enter this page.

| DEVICE DISCOVERY | | | | | | | |
|-------------------|-----------|--------------|------|-----------|-------------|----------------|-------------|
| MAC ADDRESS | PRODUCT | IP ADDRESS | MODE | SSID | DEVICE NAME | FIRMWARE | DEVICE TYPE |
| dc:36:43:3f:f6:15 | WI-FW5625 | 192.168.22.1 | AP | WI-FW5625 | WI-FW5625 | 20240802010629 | ROUTER |

Parameter Description:

| Parameter | Description |
|-------------|--|
| MAC ADDRESS | The physical address of the device scanned in the LAN. |
| RPRODUCT | The identification number used on the product to distinguish it from others. |
| IP ADDRESS | The IP address of the device in the LAN can be either static or dynamic. |
| MODE | Wireless working mode of the device. Support: Access Point (AP), Client (STA) . It can be modified in 【Wireless】 → 【Wireless Configuration】 →“Mode”. |
| SSID | Wireless signal name, i.e., WIFI name. |
| DEVICE NAME | The host name of the device can be modified in 【System】 → 【System】 →“System Properties”→“Hostname”. |
| FIRMWARE | System firmware version number, each system update will be replaced with a new firmware version number. |
| DEVICE TYPE | The device's working type, such as bridge, router, AP. |

8.4 Antenna Alignment Tool

Wireless bridge antenna alignment is the core link to ensure the stability of long-distance wireless links, and its precision directly affects signal strength, transmission rate and anti-interference ability.

Use the antenna alignment tool to check the signal strength of the local and remote devices during long-distance interconnections. By adjusting the direction or elevation angle, you can achieve the ideal signal strength for the device connection.



8.5 Spectrum Analysis

Spectrum scanning is a core part of wireless communication system planning, deployment and maintenance. It provides data support for frequency planning, channel selection and network

optimization by analyzing signal distribution, strength and interference characteristics in the electromagnetic environment.

Spectrum Analysis

Note: Use this page to obtain under the current environment, when radio interference, wireless wifi function will not work!

Start Scan :

Stop Scan :

Show scan history :

Waterfall View

Waveform View

Waveform View

Perform the "Spectrum Scan" steps:

1. Click "".
2. Wait for the spectrum scan time to end.

Spectrum Analysis

Note: Use this page to obtain under the current environment, when radio interference, wireless wifi function will not work!

Start Scan : Scanning...,Waiting for waterfall and waveform charts to be displayed...119sec

3. During spectrum scanning, you can stop the spectrum scanning by clicking "".
4. When the countdown ends, observe the "Waterfall" and "Waveform View".



5. Click " " to view the spectrum scan records again.

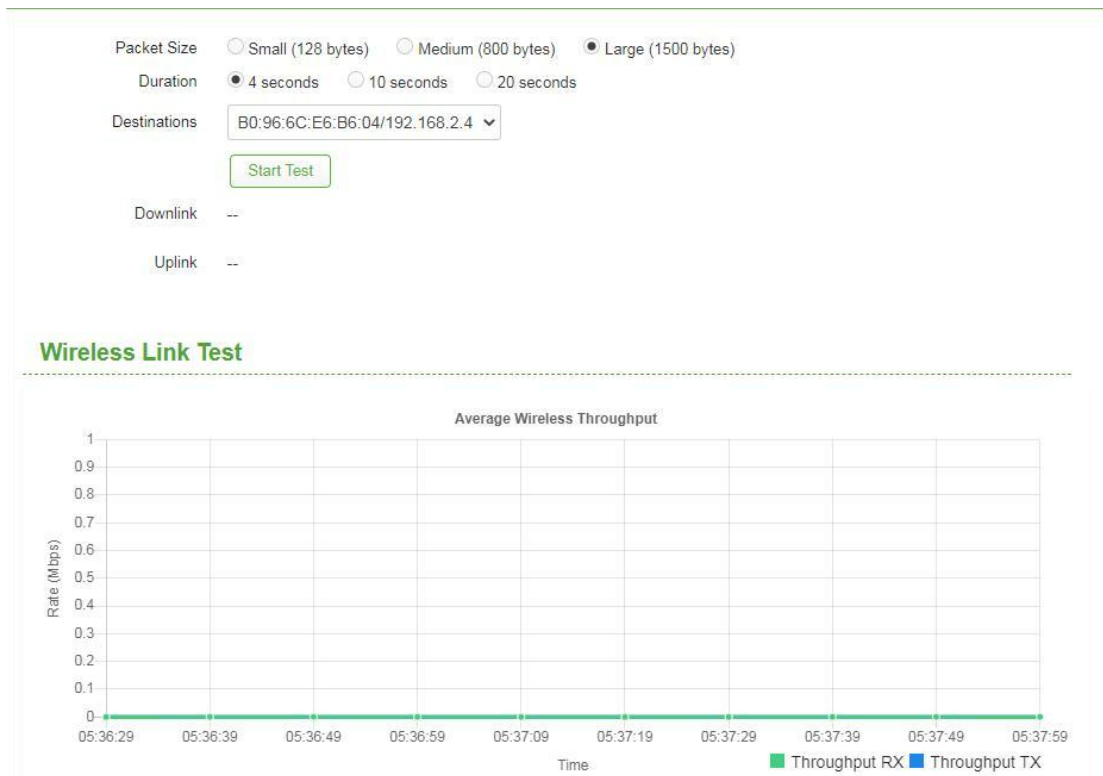
Notes:

1. When using the device to perform "Spectrum Analysis", the WiFi function will not work.
2. Devices in Client (STA) working mode do not support "Spectrum Analysis" now.

8.6 Wireless Link Test

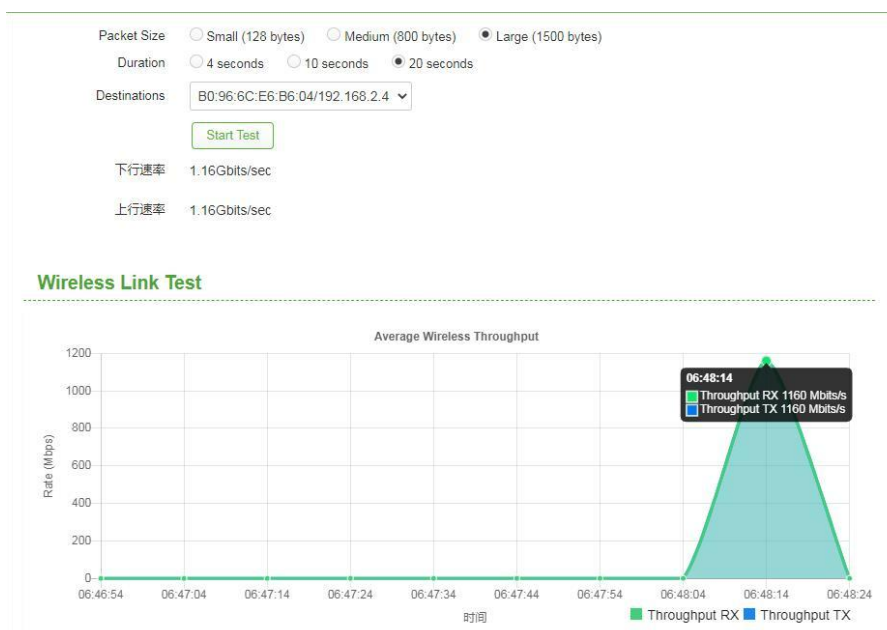
Wireless Link Test is an important means to evaluate wireless connection performance. It is mainly used to test the transmission rate, stability and bandwidth utilization between wireless devices.

Test the actual bandwidth of the point-to-point (PTMP) link to ensure smooth operation of services such as video surveillance and data backhaul.



“Test Setup” Execution Steps:

1. At least one client device is successfully connected.
2. Select "Packet Size"; "Large (1500 bytes)" is recommended.
3. Select "Duration"; "20 seconds" is recommended.
4. Select the terminal "Destinations". If there are multiple terminals, select the specified destination address by dropping down.
5. Click to start speed test. Select "Packet Size", it is recommended to use "Large (1500bytes)".
6. After the speed test is completed, check the "Downlink", "Uplink" and speed test traffic graph.



Appendix

9.1 Computer IP settings

Refer to the corresponding system version based on the computer OS to modify IP address settings: currently supports Window 7, Window 10, Window 11.

Window 7

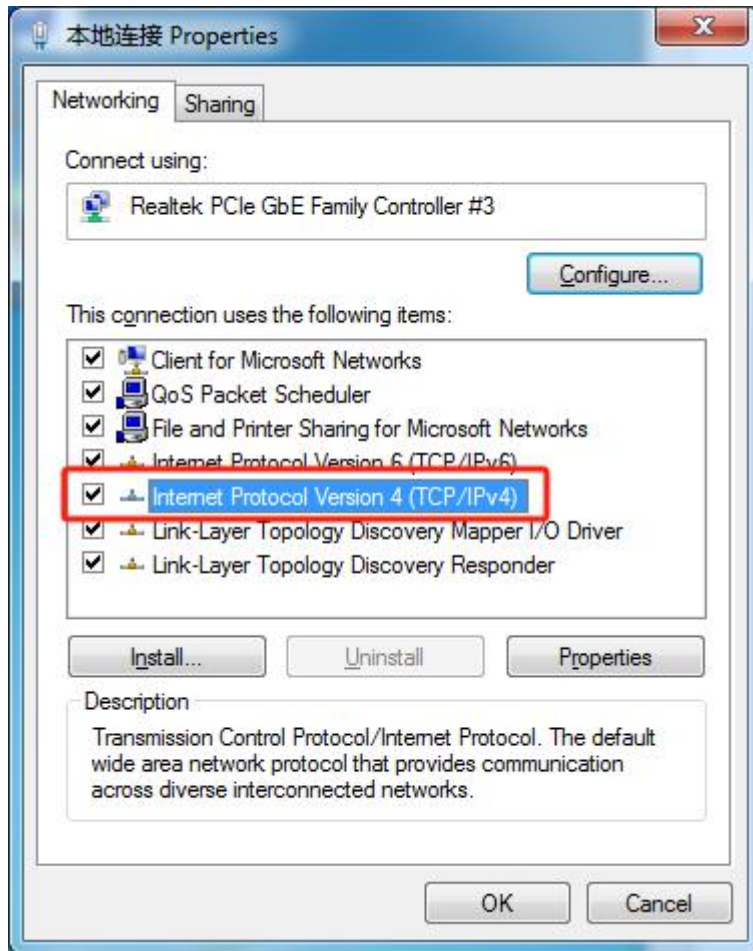
1. Right-click "Network" on the desktop and select "Properties";



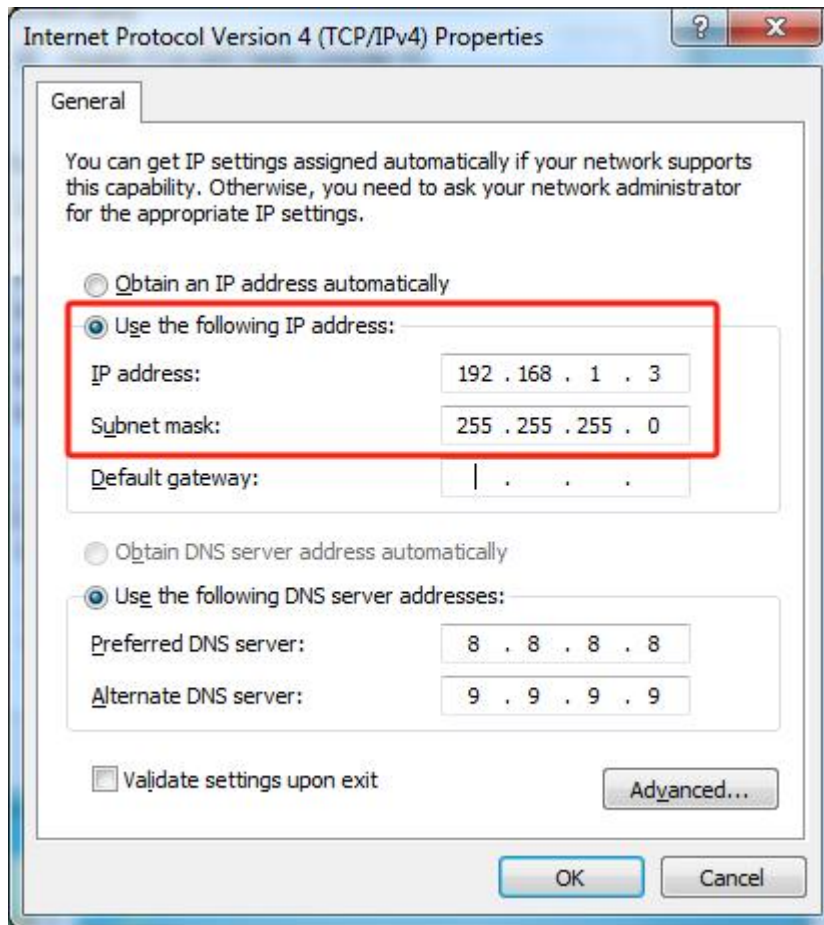
2. Click "Change adapter settings" and select the network interface directly connected to the wireless bridge;



3. Right-click the network interface, click "Properties", find and double-click "Internet Protocol Version 4 (TCP/IPv4)";

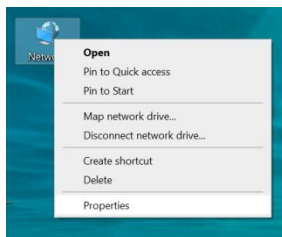


4. Manually set the IP address to "192.168.1.X (X: 3~254)" and the subnet mask to "255.255.255.0";
5. Click "OK", return to "Local Area Connection Properties", and click "OK" again";

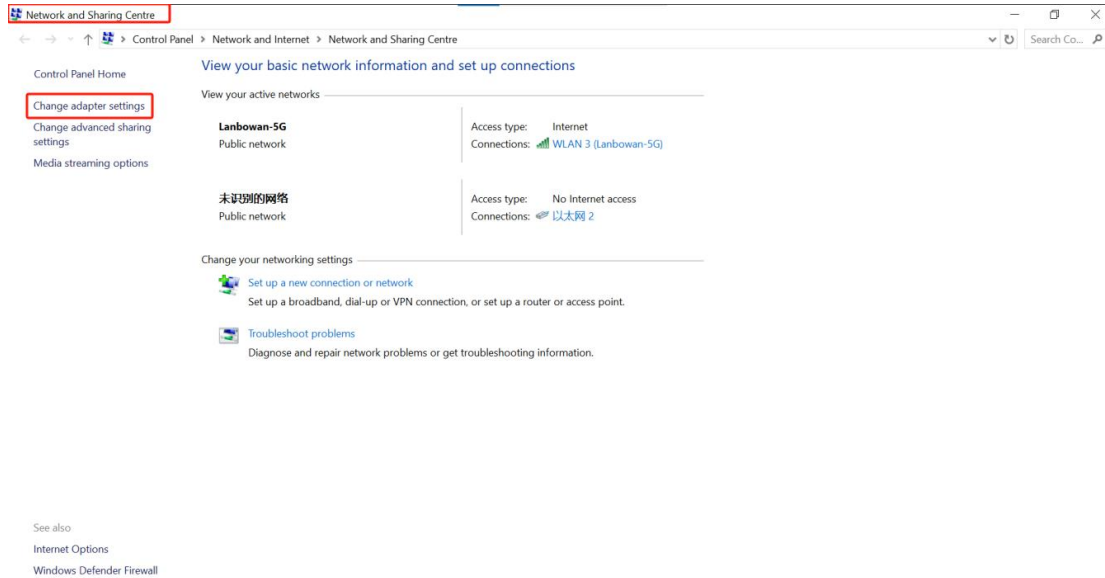


Window 10

1. Right-click the "Network" icon on the desktop and select "Properties";



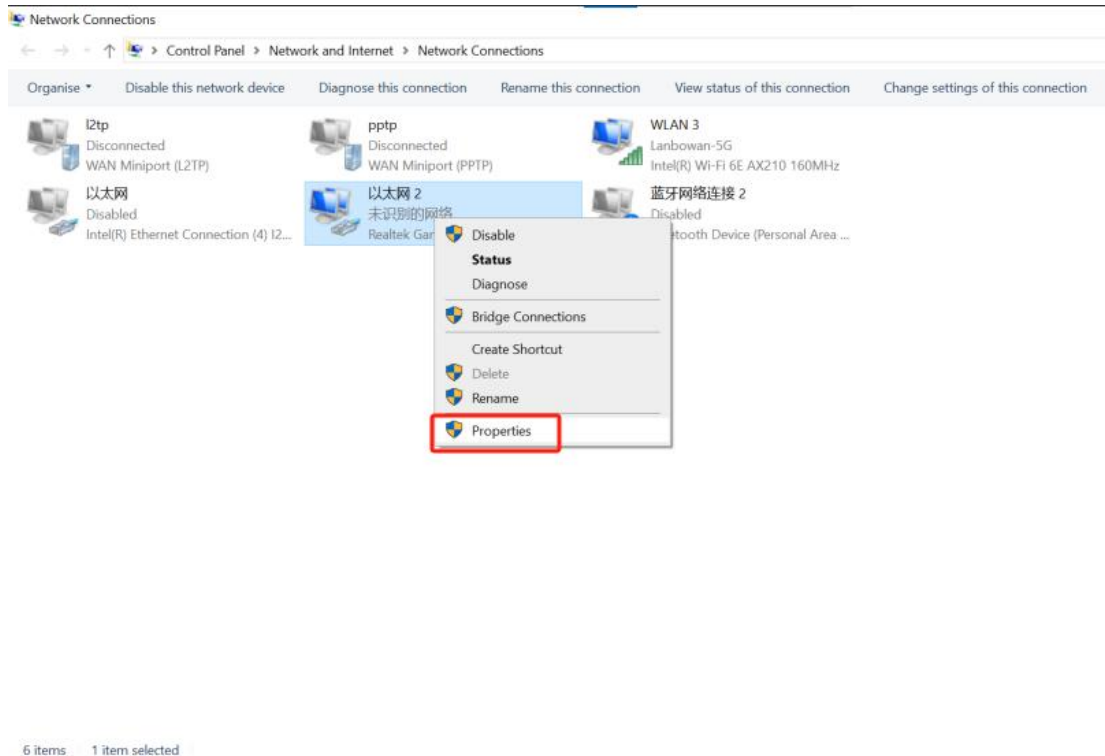
2. In the "Network and Sharing Centre", click "Change adapter settings";



3. Select the computer Ethernet port connected to the LAN port of "bridge";

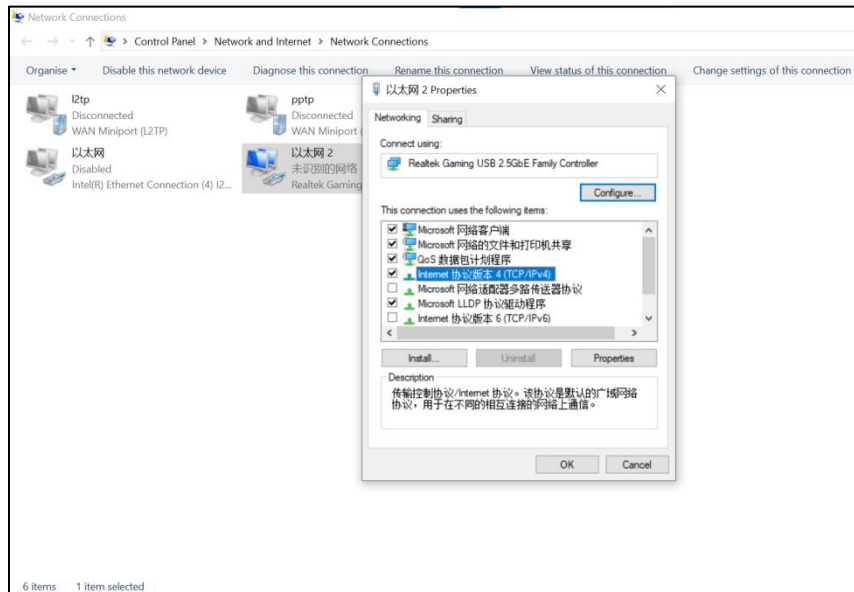


4. Right-click the Ethernet port to which the "Wireless Network Bridge" is connected and select "Properties";



5. In "This connection uses the following items", double-click "Internet Protocol Version 4

(TCP/IPv4)";



6. "Obtain an IP address automatically", select "Use the following IP address" to manually set the IP address "192.168.1.X (X: 3~254)", Subnet mask "255.255.255.0"; After the settings are completed, click "OK" below to apply the configuration.

