

maiwe


Industrial Router

Quick User Manual


- MIR675-W
- MIR675-WB
- MIR685-W


Chapter 1 Quick Start


MIR675/MIR685 series of industrial routers provide a wireless long-distance fast networking solution for user equipment. The parameters can be set through the built-in web page to meet the scene application. This chapter is an introduction to the quick start of MIR675/685 series industrial router products. It is recommended that users read this chapter and follow the instructions to have a basic understanding of the product. For specific function details and descriptions, please refer to the subsequent chapters. For product related information, you can go to the official website link to download the corresponding product manual: <http://www.maiwe.com>



<















>

MIR675-WB

- 1 WAN Port + 4 LAN Port 100M Dual SIM 4G LTE Router

Features and Benefits

- ⌚ Support 4 wired LAN ports, 1 wired WAN port, and 1 WLAN wireless local area network
- ⌚ Support APN automatic network detection, 2/3/4G automatic switching, SIM card information display, and APN dedicated network card
- ⌚ Ethernet interface up to 6KV lightning protection, RS-232/RS-485/RS-422 interface up to 4KV surge protection

Online consultation →

Figure 1 Product page on the official website

1.1 Environment Preparation

MIR series routers are quickly connected to the Internet. You need to prepare a PC, a MIR series router, a network cable, a DC12V/1A power supply, and a SIM card. The hardware connection is shown in Figure 2.



Figure 2 Hardware connection

1.2 Network connection

- Put the SIM card into the card tray and insert it into the card slot of the router with the SIM card chip facing up.
- Connect the WiFi antenna (2) and the 4G/5G antenna to the corresponding antenna port of the router in turn.
- Connect the network port of the PC to any LAN port of the router with a network cable.
- Configure the PC network card to automatically obtain an IP address mode, as shown in Figure 3.

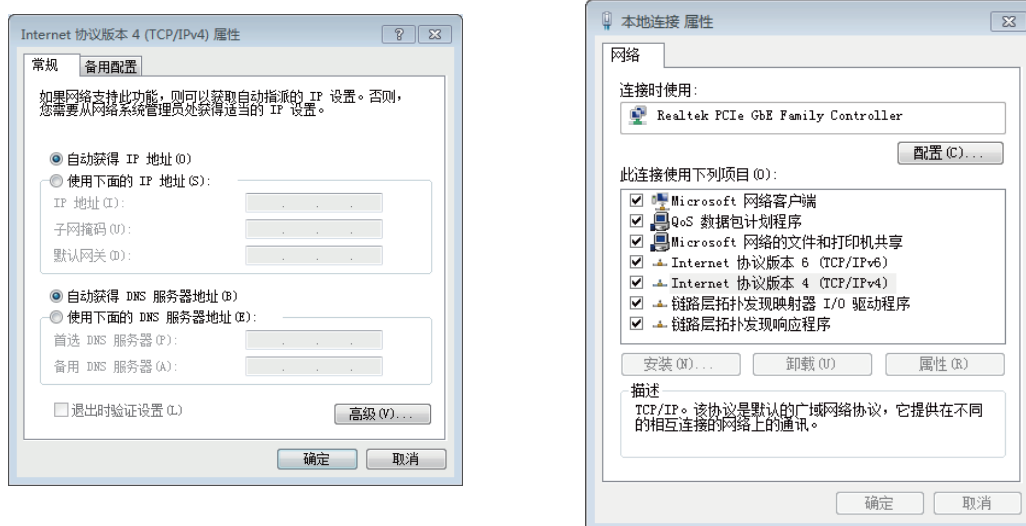


Figure 3 Network connection

- Use the standard DC12V power supply to power on the router.
- Power on and wait for about 2 minutes, the 4G/5G network connection status light and signal strength light are on, indicating that the router is successfully connected to the Internet and can access the Internet normally.

1.3 WEB login and networking test

Table 1 lists the initial account parameters for Web login of MIR series routers.

Parameter	Initial value
LAN port IP address	192.168.16.253
User name	admin
Password	admin

Table 1 Web initial account table

Enter: 192.168.16.253 in the PC browser (recommended to use Chrome browser or Firefox browser) (you can also use the management domain name <http://we.linocn> to log in), fill in admin for both the username and password, and then press the Enter key, The login interface of the router is shown in Figure 4.



Figure 4 Login page

If the PC can access the Web interface normally, it can normally connect to the external network through the router, and can browse the web normally.

Chapter 2 WEB Basic Function Configuration

When using the MIR series router to configure the WEB interface, you can connect the LAN port of the router through a PC network cable, or connect to the WLAN wireless network of the router through a wireless network, and then log in to the WEB management interface to configure.

By default, the default SSID name of the wireless AP of MIR675 is MIR675-W-XXXX (XXXX is the last 4 digits of the MAC address of the router's LAN port, and the MAC addresses of different routers are different), and the default SSID name of the wireless AP of MIR685 is MIR685-W-XXXX. The initial value configuration parameter table of IP address, username and password is shown in Table 2.

Parameter	Initial value
SSID	MIR675-W-XXXX(MIR675) MIR685-W-XXXX(MIR685)
wireless password	www.maiwe.com
LAN port IP address	192.168.16.253
User name	admin
Password	admin

Table 2 Initial value configuration parameter table

You can use the wireless network card of PC or mobile phone, join the wireless network with SSID of MIR675-W-XXXX or MIR685-W-XXXX, wait for the wireless connection to succeed, open the browser, and enter the router's LAN port IP (192.168.16.253 or <http://welinos.cn>), enter the user name and password after pressing Enter and click the login button to log in to the router WEB management interface.

2.1 Login to WEB

Open the browser, enter the default IP address of the router in the address bar, press the Enter key, and the window shown in Figure 5 will pop up, prompting the user to enter the user name and password.



Figure 5 Enter the user name and password interface

There is only one default login user of this router, the role is super administrator, the user name is "admin", and the password is "admin", which can configure all functions of the router. If you need to create other users, please refer to chapter 2.7.2 Administration Rights .

After entering the user name and password, click "Login", and the router web server performs authentication to determine whether the user is logging in to the router web interface for the first time. If yes, enter the novice guide page (if the user does not want to configure parameters in the novice guide interface, you can directly click the "€" button in the upper right corner of the interface to exit the novice guide interface), as shown in Figure 6.



Figure 6 Newbie guide page

If it is not the first time to log in, go directly to the main web management page, as shown in Figure 7.



Figure 7 Web main page

2.2 Introduction to the novice guide page

When the user logs in to the web server for the first time, the system will enter the novice guide page, as shown in Figure 4-2 above. The novice guide is divided into three parts, external network settings, 4G/5G settings and wireless settings. The first step is to enter the external network settings by default, the second step is 4G/5G settings, and the last is wireless settings. After all settings are completed, you will enter the main page.

2.2.1 External network settings

When the user enters the Web server for the first time, he will enter the page as shown in Figure 4-2, click the icon, and enter the external network setting page to set the external network information. It mainly includes two parameters, WAN/LAN mode selection and WAN port protocol. As shown in Figure 8.

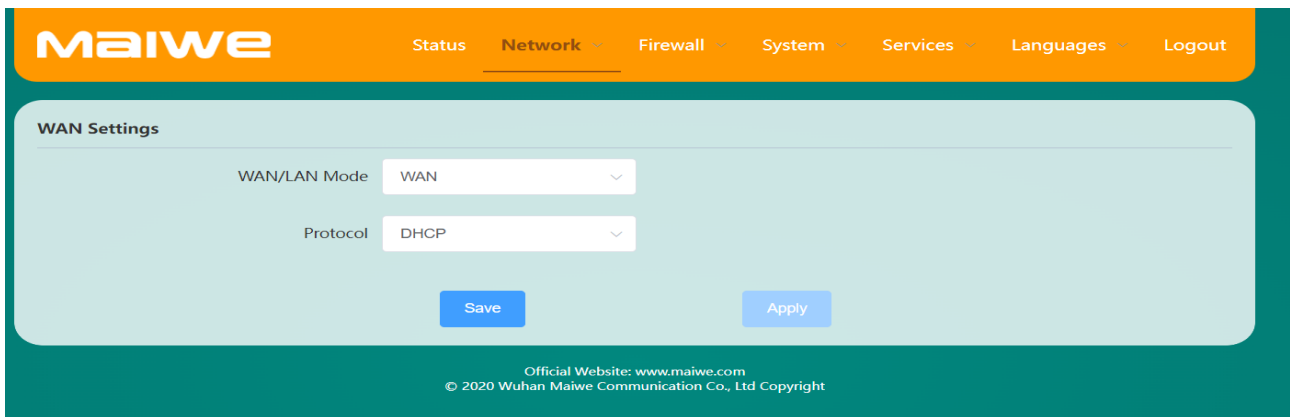


Figure 8 External network information interface

- **WAN/LAN mode:** When connecting to the external network through the WAN port, it must be set to WAN mode (the default is WAN mode)
- **Protocol:** WAN port protocol includes static address, DHCP and PPPoE, the default is DHCP mode
- **Static address:** Networking by manually specifying the IP address, subnet mask and gateway, as shown in Figure 9

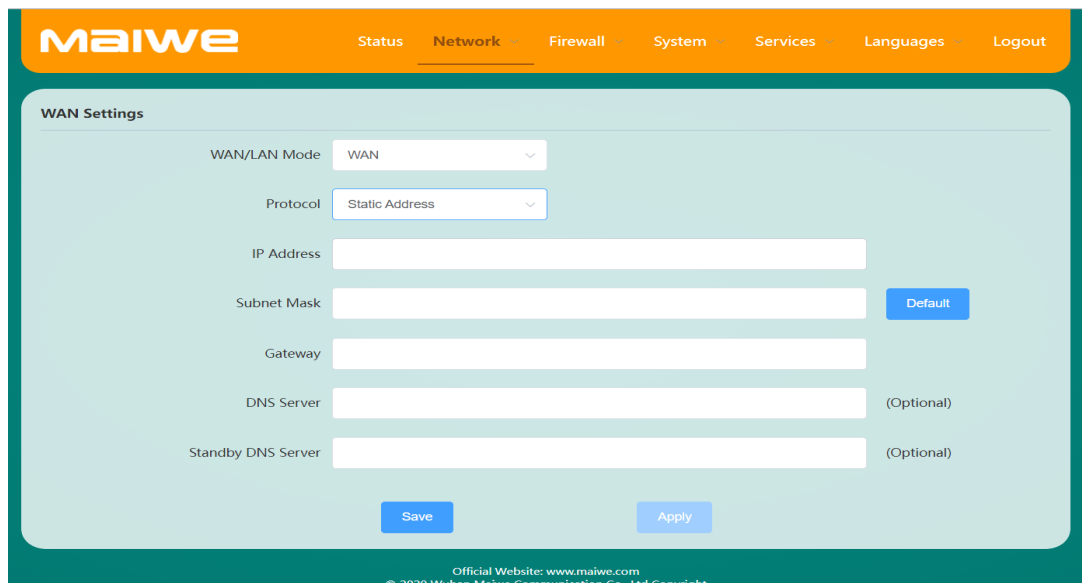


Figure 9 Static IP page

- **DHCP:** Automatically obtain the IP address, gateway and DNS assigned by the server by requesting the DHCP server
- **PPPoE:** Dial-up connection by setting the account name and password (obtained from the broadband operator), as shown in Figure 10

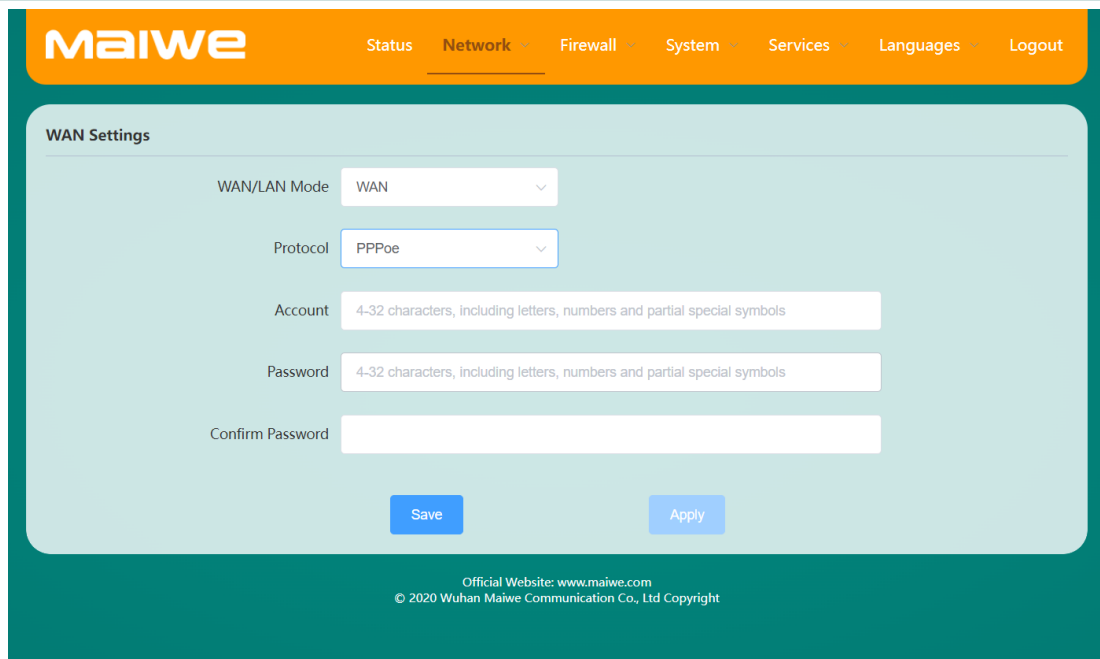


Figure 10 PPPoE interface

2.2.2 4G/5G settings

The 4G/5G setting parameters mainly include protocol settings, and the protocol currently supports the DHCP client protocol. If you use an ordinary mobile phone SIM card or an IoT SIM card, you can use the default parameters for 4G/5G setting parameters (APN, username and password do not need to be set); if you use an APN dedicated network card to connect to the Internet, you also need to set the APN name, username and password (usually null). The DNS server and the alternate DNS server can be set as public DNS, or not set (if not set, the DNS assigned by the operator will be used), as shown in Figure 11.

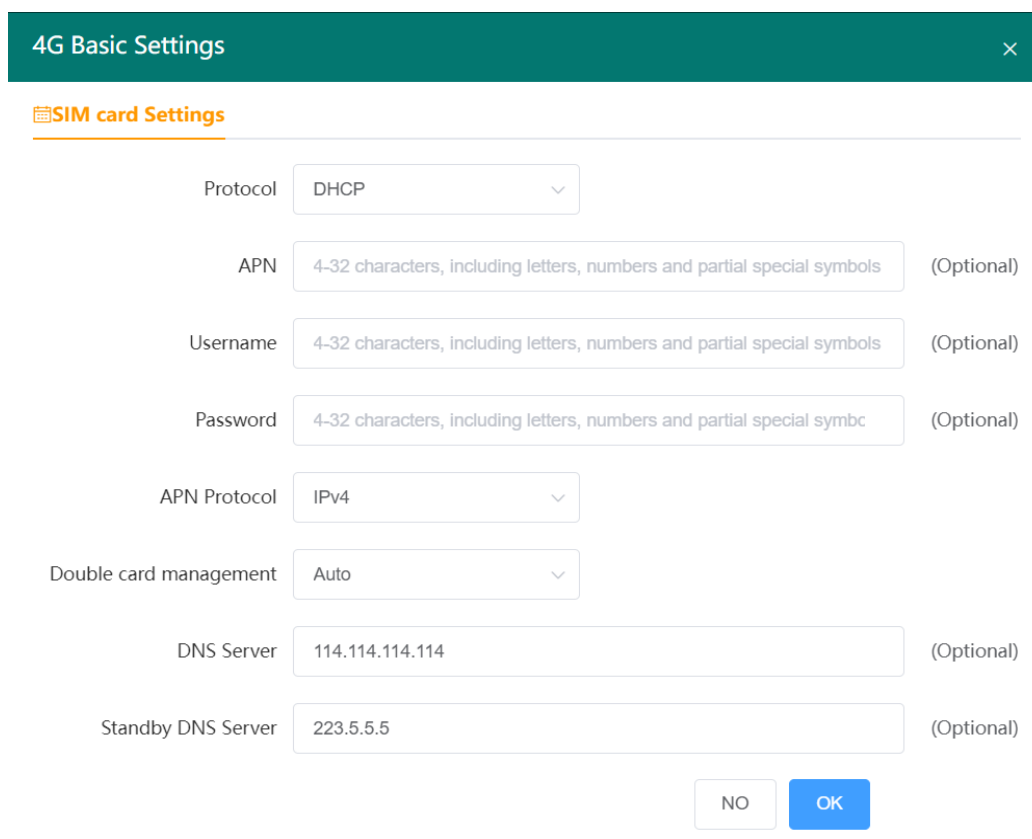


Figure 11 4G/5G setting interface

2.2.3 Wireless Settings

Wireless settings mainly include AP mode and Client mode. When the working mode is set to AP mode, as shown in Figure 3-8, when the working mode is set to Client mode, as shown in Figure 12.

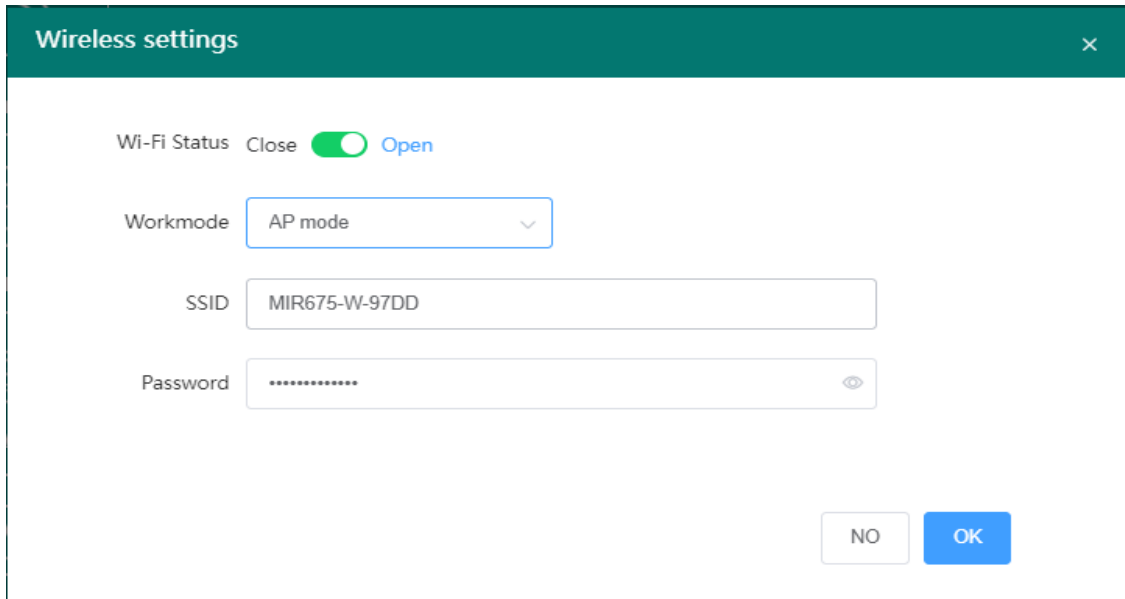


Figure 12 AP mode interface

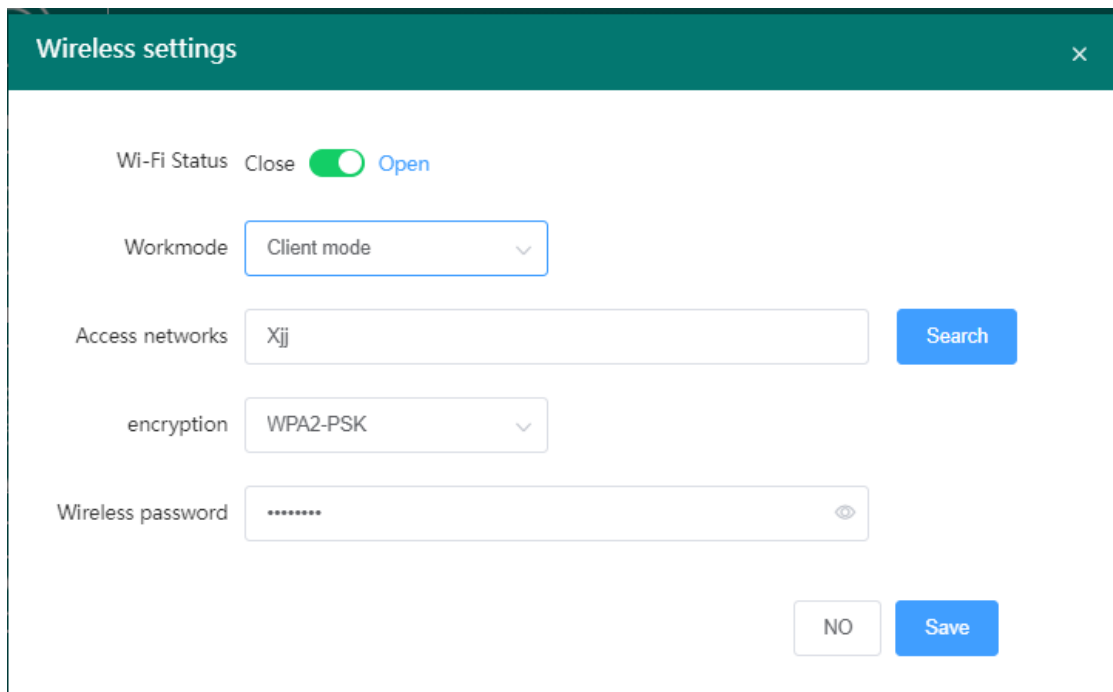


Figure 13 Client mode interface

2.3 Introduction to the main page

After the user logs in to the web interface for the first time and completes the novice guide operation, he can enter the main interface of the web, as shown in Figure 7 above. It is mainly composed of upper and lower areas. The left side of the upper part is the Logo area, and the right side is the function menu area. The lower part is the function display and setting area, which is used to set the functions of the router, as shown in Figure 14, the main web management interface.

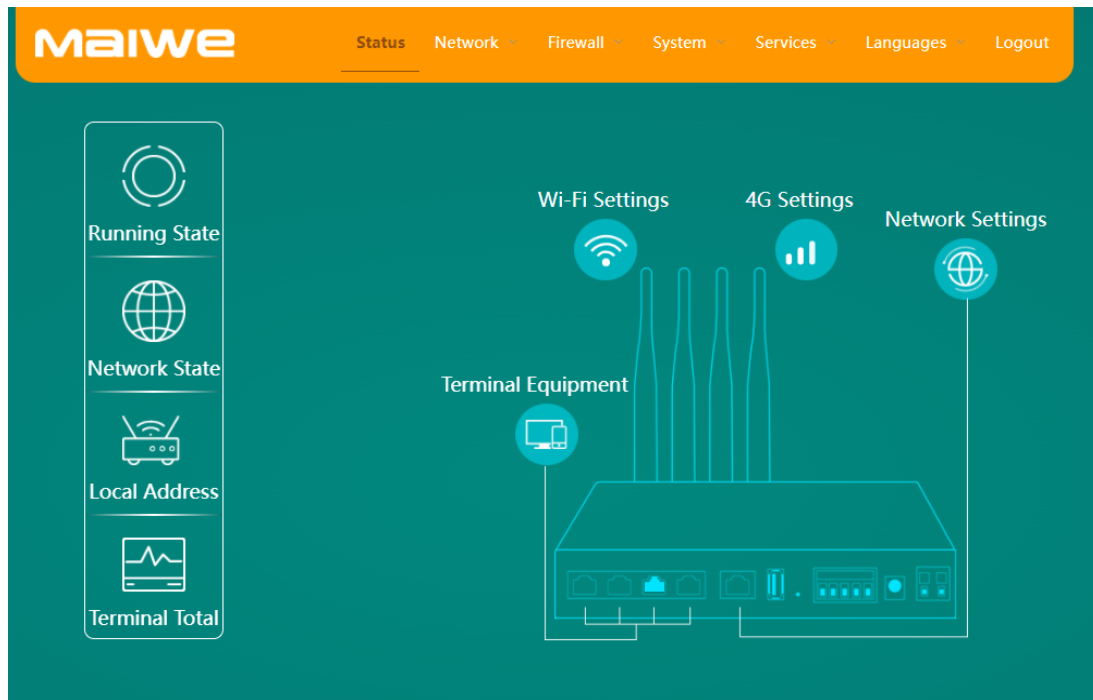


Figure 14 Main interface

2.3.1 Function menu

The upper right part of the web page is the function menu, which displays all the configurable software functions of this router. Among them, the function menu is status, network, firewall, system, language selection, and exit. Each menu includes several sub-functions. The status, system and network functions are shown in Table 3.

Menu	Tab Page	Function
Status	Operating status	Display device information and running time, such as: platform number, device model, device code, hardware version, firmware version, running time
	Network status	Display the external network connection type and the corresponding IP address and real-time traffic
	Local address	Display router LAN port MAC and IP, CPU and memory load
	Terminal statistics	Display the number of all connected terminals in the LAN where the router is located
Network	Interface	Display the MAC, IP address of WAN, LAN, WAN_4G/5G, and the basic information of some interfaces of the newly added VPN Client.
	WAN port settings	Configure the external network connection parameters of the WAN port
	LAN port settings	Configure the network parameters of the LAN port and DHCP service parameters
	4G settings	Display the signal strength of the SIM card and configure the network parameters of WAN 4G/5G
	Wireless setting	Set the basic parameters of wireless and basic parameters of wireless security
	Access device	Displays the end devices connected to the router
	Static routing	Configure static routing table
	Ping watchdog	Configure Ping watchdog parameters to monitor router network connectivity
	Network diagnostics	Diagnose the connection status of the router's current network

Firewall	Basic settings	Set the basic inbound, outbound and port forwarding rules of the router, and set the routing rules for the corresponding ports
	Port forwarding	Set up router port forwarding rules
	Restriction of visit	Set IP, MAC and domain name filtering parameters
	Custom rules	Provides custom firewall rule setting function
	DMZ	Set the DMZ host function in the LAN
	UPnP	Turn on and off the UPnP function, check the connection information of the UPnP device
	Internet speed control	Network speed control configuration based on IP or MAC
	QoS service	Enable and disable QoS traffic bandwidth display function
System	System properties	Display and set system time, host name and time zone
	Management rights	Modify administrator password and manage common user information
	Reboot	Configure the immediate restart and scheduled restart functions of the device
	Backup/Upgrade	Backup or import configuration files, upgrade system firmware
	Scheduled Tasks	Manually add device scheduled task function
	System log	Configure remote and local log information, and view and download system logs
Service	Serial to network	Set network, serial port, heartbeat packet, registration packet parameters
	Peanut shell inner mesh penetration	Remote login and management of equipment can be realized
	Dynamic DNS	Set the basic information of dynamic domain name
	VPN server	Set the basic information of servers such as PPTP, L2TP, and IPSec
	SNMP settings	Configure settings, groups, traps and other parameters
	LLDP settings	Set basic LLDP information
Language	Chinese	Switch the web interface language to Chinese
	English	Switch the web interface language to English
Exit		Log out the currently logged in user

Table 3 Menu function description table

2.4 Status

The status module includes: device information, network connection information.

2.4.1 Device Information

The function of the device information is to display some specific information of the current device, including the platform number, device model, device code, hardware version, firmware version, current CPU load, MAC address, etc. of the device, as shown in Figure 15.

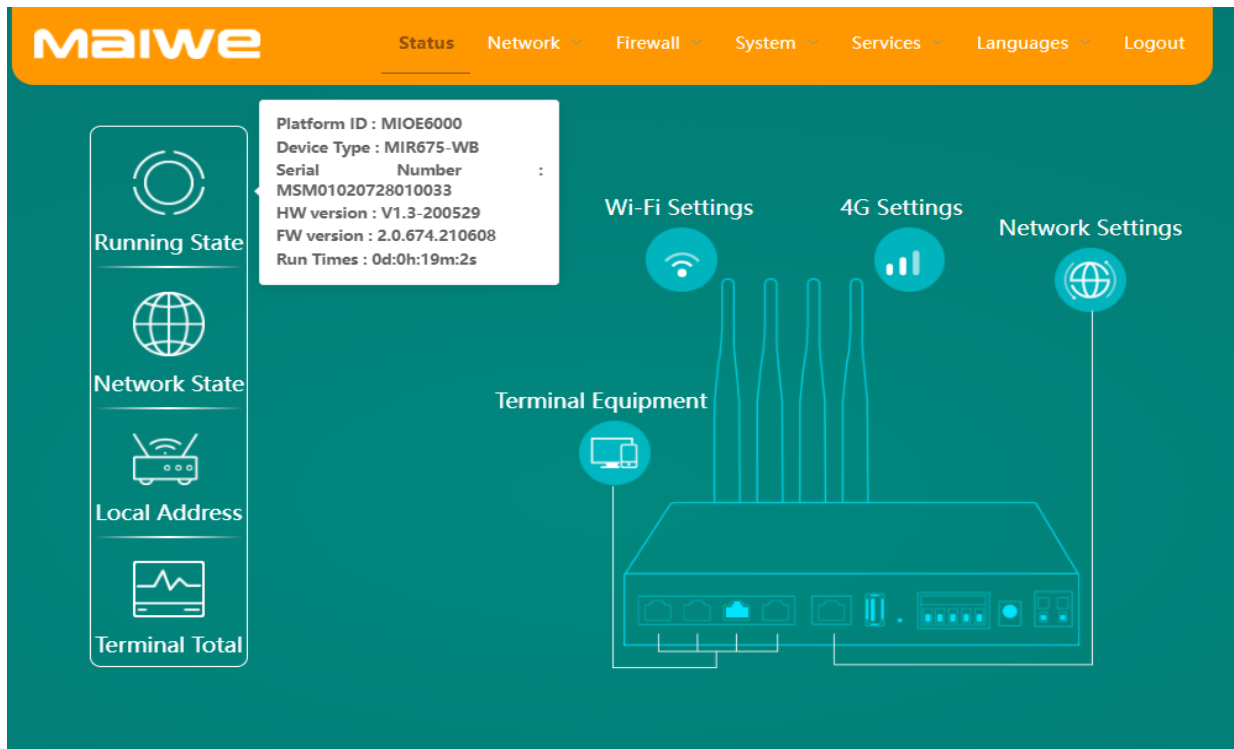


Figure 15 Device Information

- **Platform ID:** the platform ID of the router
- **Device model:** the device model of the router
- **Device Code:** the device number of the router when it leaves the factory
- **Hardware Version:** router hardware version number
- **Firmware Version:** the firmware version number of the router
- **Running time:** the current continuous running time of the router
- **MAC address:** the MAC address of the router's LAN port, an address with a length of 48 bits, usually expressed as 12 hexadecimal numbers, separated by colons between each 2 hexadecimal numbers.
- **IP address:** the IP address of the router's LAN port, a 32-bit address assigned to devices connected to the Internet. An IP address consists of two fields: a network number field (net-id) and a host number field (host-id). IP addresses are assigned by the Defense Data Network's Network Information Center (NIC). In order to facilitate the management of IP addresses, IP addresses are divided into five categories: A, B, and C addresses are unicast addresses; class D addresses are multicast addresses; and class E addresses are reserved addresses for future use. Special Purpose. Currently, the IP addresses in use in large numbers belong to three types of addresses: A, B, and C.
- **Subnet mask:** the mask is a 32-bit number corresponding to an IP address, some of which are 1 and some are 0. The mask divides the IP address into two parts: the subnet address and the host address. The part of the IP address corresponding to the bit 1 in the mask is the subnet address, and the other bits are the host address. The mask corresponding to class A address is 255.0.0.0; the mask of class B address is 255.255.0.0; the mask of class C address is 255.255.255.0.
- **CPU Load:** the current CPU usage.
- **Memory usage:** memory usage (such as 45.87M / 129.36M, a total of 129.36M memory, currently using 45.87M).

The connection status of the five network ports of the router is identified by whether the corresponding five network ports in the router block diagram on the status page are highlighted. From left to right are the LAN1~LAN4 and WAN ports; the corresponding network port is highlighted to indicate that the network cable of the network port is inserted and connected to the device.

2.4.2 Network connection information

- **External network connection type:** WAN port connection type, wired network, 4G/5G network or 4G2 network (dual 4G module router)
- **MAC address:** the MAC address of the router connected to the external network card
- **IP address:** the IP address of the router connecting to the external network card
- **Implement downlink traffic:** the current real-time downlink traffic of the router
- **Implement upstream traffic:** the current real-time upstream traffic of the router
- **Cumulative Terminals:** the total number of terminals connected to the router
- **Total downloads:** the total data traffic currently downloaded by the router
- **Total Upload:** the total data traffic currently uploaded by the router

2.5 Network

The network module includes interface, WAN settings, LAN settings, WAN 4G/5G settings, wireless settings, access devices, static routes and network diagnostics.

2.5.1 Interface

The interface is divided into two parts: interface and new interface. The interface information page displays the basic information of the interface, including the MAC address of the WAN port (wired WAN), the MAC address of the LAN port, the IP address and the default gateway, as well as the IP, DNS and other information of the WAN 4G/5G, as shown in Figure 16 .

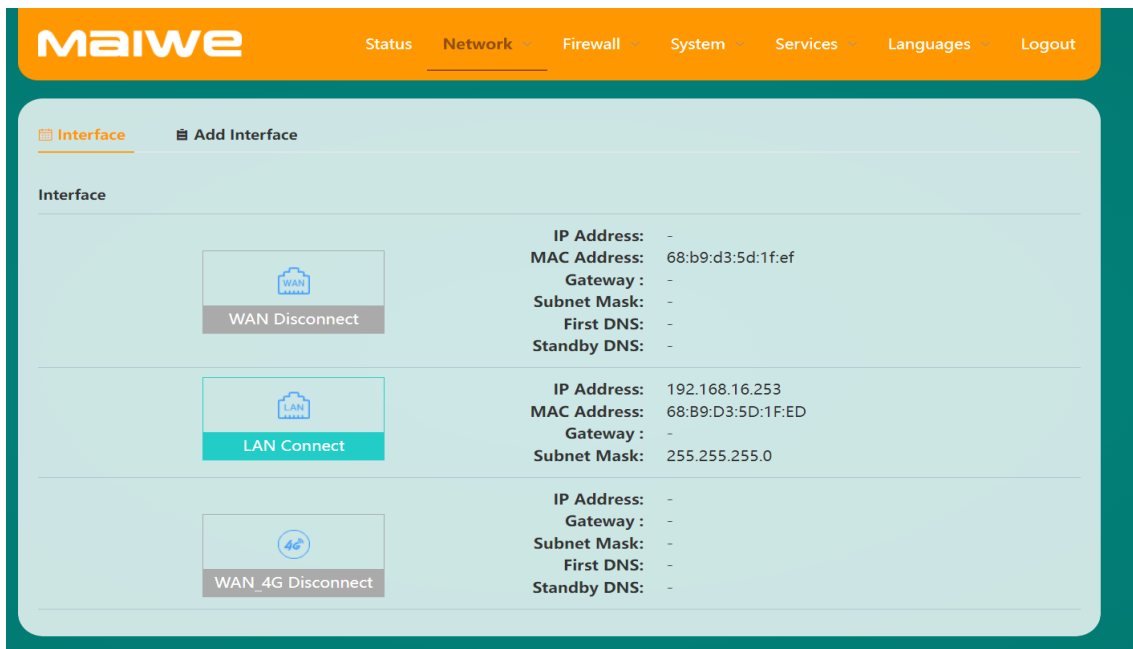
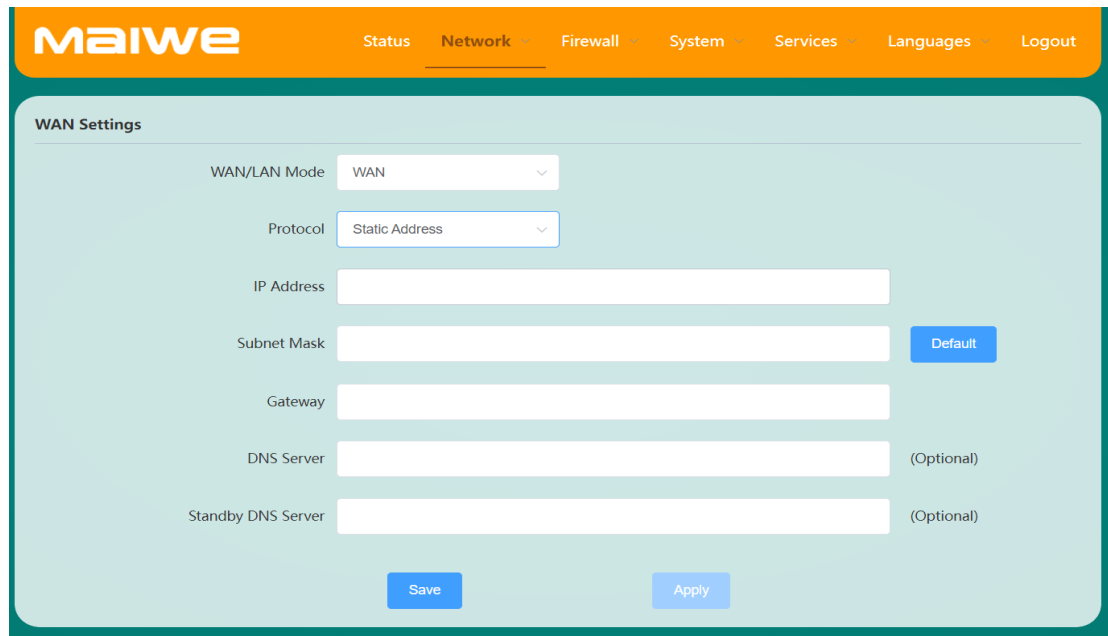


Figure 16 Basic interface information

The newly added interface is mainly to add a VPN client network interface. The protocols of the new interface include PPTP, L2TP, GRE, OPENVPN (TUN/TAP), and SSTP. For VPN client network interface creation, refer to the chapter "VPN Client".

2.5.2 WAN port settings

Used to configure the working mode and protocol parameters of the WAN port. WAN/LAN mode is configured as WAN mode by default, which is used to connect to the external network. If it is configured as LAN mode, the WAN port can be used as a common LAN port (in this mode, all 5 network ports of the router are LAN ports). The WAN port protocol has three parts, static address, DHCP and PPPoE. The static address protocol is shown in Figure 17 below, and the PPPoE protocol is shown in Figure 18 below.



The screenshot shows the MAIWE WAN Settings interface. At the top, there is a navigation bar with the MAIWE logo and menu items: Status, Network (selected), Firewall, System, Services, Languages, and Logout. Below the navigation bar, the page title is "WAN Settings". The main content area contains several configuration fields:

- WAN/LAN Mode:** A dropdown menu set to "WAN".
- Protocol:** A dropdown menu set to "Static Address".
- IP Address:** A text input field.
- Subnet Mask:** A text input field with a "Default" button to its right.
- Gateway:** A text input field.
- DNS Server:** A text input field with "(Optional)" to its right.
- Standby DNS Server:** A text input field with "(Optional)" to its right.

At the bottom of the form, there are two buttons: "Save" and "Apply".

Figure 17 Static address interface

- **WAN/LAN mode:** configure the working mode of the WAN port, the default is WAN mode (used to connect to the external network).
- **Protocol:** the currently selected WAN port networking protocol (static address, DHCP and PPPoE).
- **IP address:** IP is a 32-bit address assigned to devices connected to the Internet. An IP address consists of two fields: a network number field (net-id) and a host number field (host-id). IP addresses are assigned by the Defense Data Network's Network Information Center (NIC). In order to facilitate the management of IP addresses, IP addresses are divided into five categories: A, B, and C addresses are unicast addresses; class D addresses are multicast addresses; and class E addresses are reserved addresses for future use special purpose. Currently, the IP addresses in use in large numbers belong to three types of addresses: A, B, and C.
- **Subnet mask:** the 32-bit number corresponding to the mask IP address, some of these numbers are 1 and some are 0. The mask divides the IP address into two parts: the subnet address and the host address. The part of the IP address corresponding to the bit 1 in the mask is the subnet address, and the other bits are the host address. The mask corresponding to class A address is 255.0.0.0; the mask of class B address is 255.255.0.0; the mask of class C address is 255.255.255.0.
- **IP gateway:** a device that connects data using different transmission protocols in two network segments.
- **DNS server:** used to resolve domain names.
- **Alternate DNS server:** used to resolve domain names.

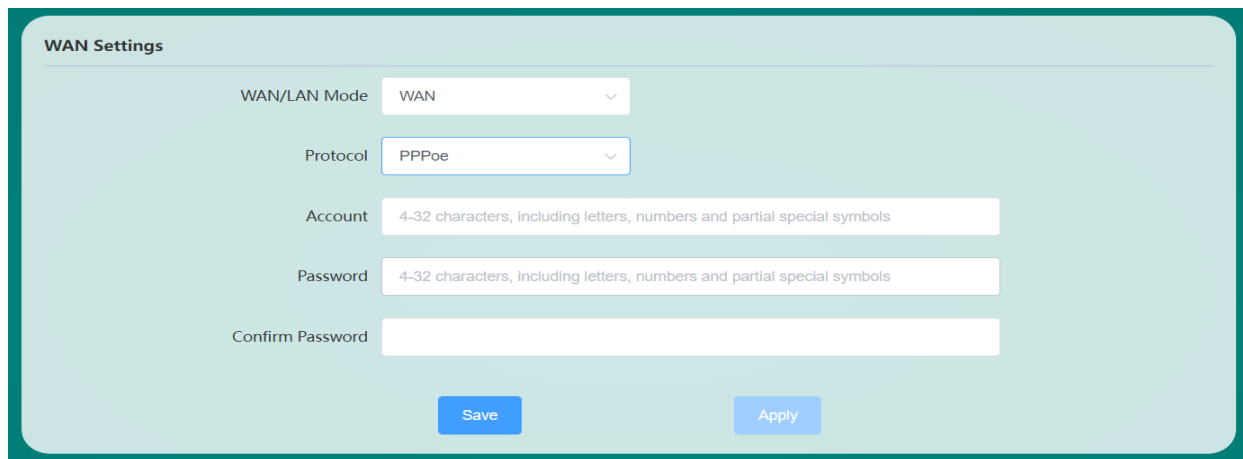


Figure 18 PPPoE protocol interface

- Internet account: Enter the Internet account, the length is 4-32 digits, and it can only include numbers and letters.
- Internet password: The password is 4-32 digits long and can only include numbers, letters and some special symbols (~!@#\$\$%^&*()_+-.).
- Confirm Internet Password: Confirm the Internet password to prevent wrong password.

2.5.3 LAN port settings

Basic information for configuring the LAN port, as shown in Figure 19 below.

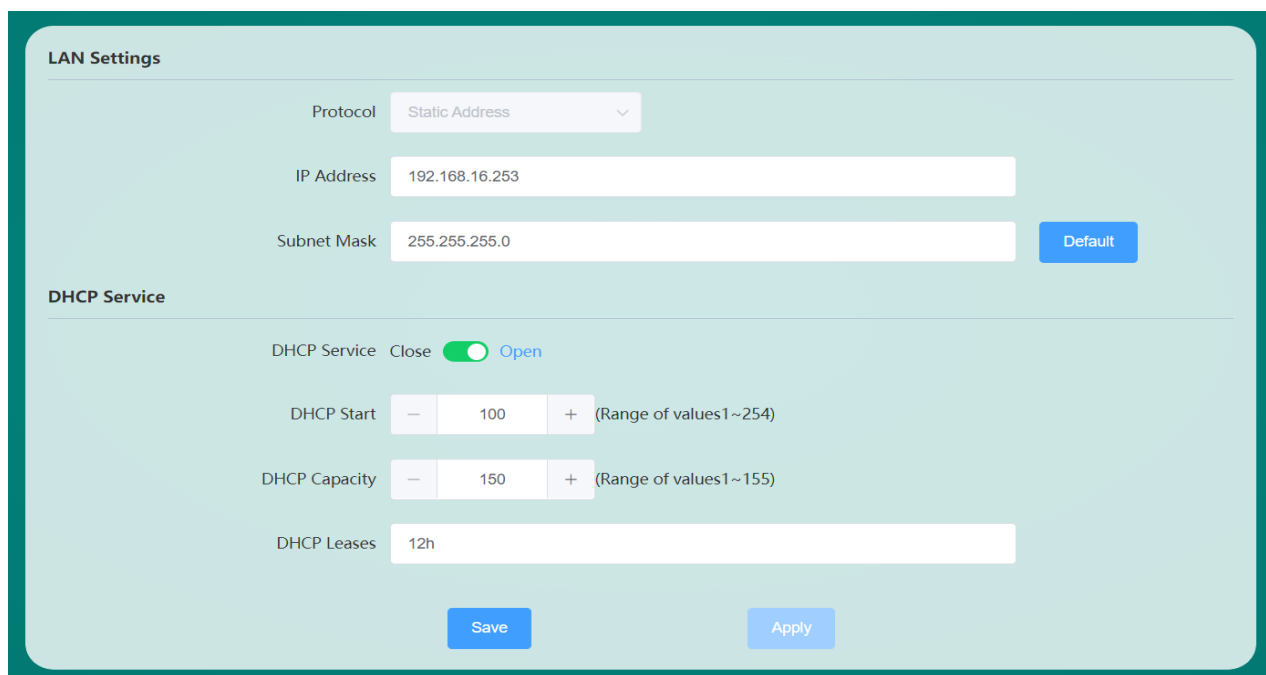



Figure 19 LAN port configuration interface

The configuration parameters of this interface are detailed in Table 4.

Item	Statement
Basic settings	
Protocol	Default is static address
IP address	The default IP address is 192.168.16.253, which can be modified

Subnet mask	The default subnet mask is 255.255.255.0, which can be modified
DHCPservice	
DHCP service	Select DHCP service, enable or disable it
DHCP start	Set the starting value of DHCP, the value range is between 1-254
DHCP capacity	Set the capacity of DHCP, the value range is between 1-254
DHCP lease	Set the DHCP lease period, such as 2m (two minutes), 8h (eight hours) or 5d (five days), etc.

Table 4 Description of LAN port configuration parameters

 When the router's LAN port provides DHCP service to the outside world, it is not allowed to connect the LAN port to the network of other routers that also have DHCP service enabled.

2.5.4 WAN 4G/5G Settings

It is mainly used to display and set the basic information of the SIM card, as shown in Figure 20.

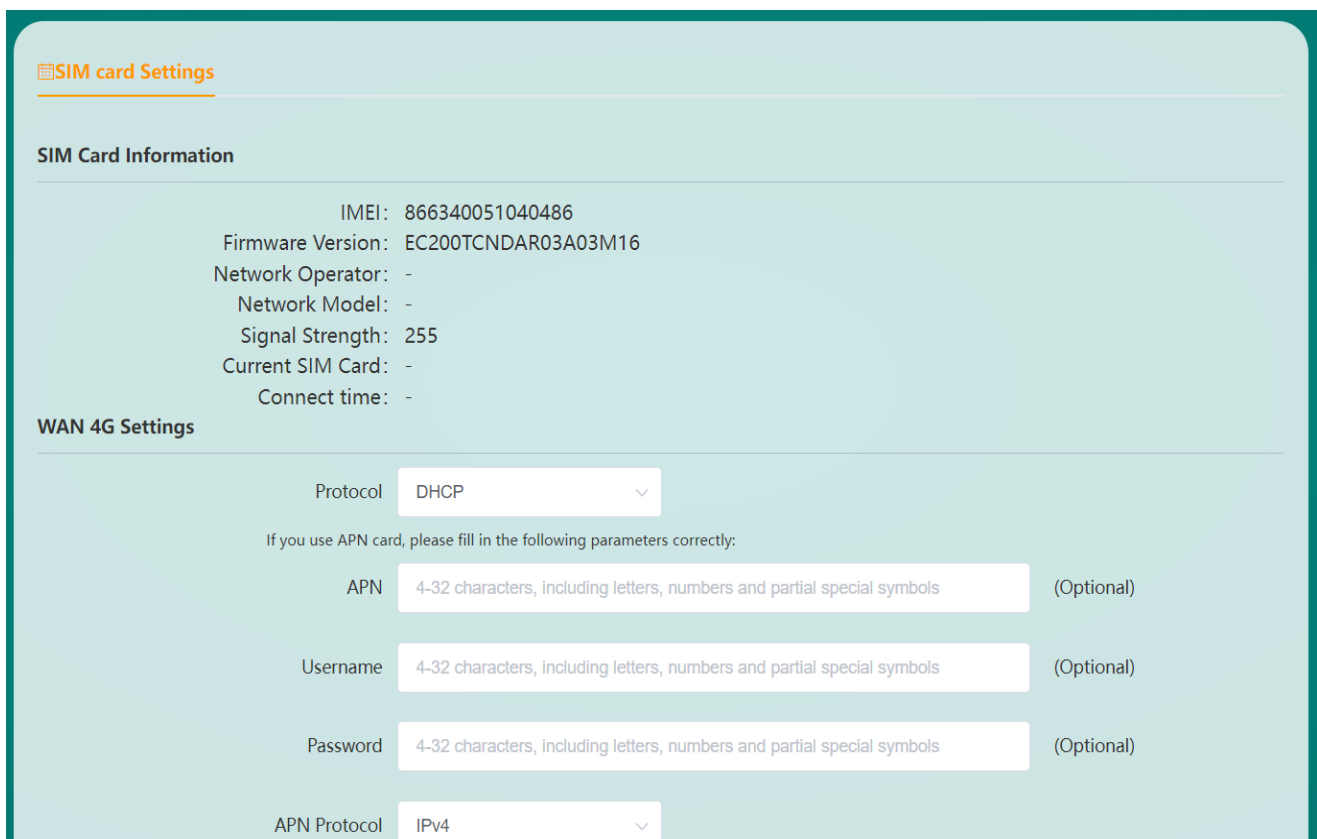


Figure 20 SIM card configuration interface

- **IMEI number:** 4G/5G module serial number.
- **Firmware version:** 4G/5G module firmware version number.
- **Network Operator:** The current network operator.

- **Network Mode:** The current router's network mode is 5G/4G/3G/2G.
- **Signal Strength:** The signal strength of the current router (the larger the value of -113--51, the stronger the signal, 255 means no signal).
- **Connection Time:** The duration of the router's mobile network connection.
- **Protocol:** The currently selected protocol.
- **APN name:** the name of the access point (the APN name needs to be set when using the APN dedicated network card).
- **Username:** Enter the username (usually empty).
- **Password:** Enter the password, you can choose to display the password (usually empty).
- **DNS server:** network domain name resolution server address.
- **Alternate DNS Server:** Alternate network domain name resolution server address.

The configuration of the dual 4G module router SIM card 2 is shown in Figure 21.

The screenshot displays the configuration interface for SIM card 2, divided into two main sections: SIM Card Information and WAN 4G Settings.

SIM Card Information:

- IMEI: 864650052377667
- Firmware Version: EC20CEHCLGR06A05M1G
- Network Operator: -
- Network Model: -
- Signal Strength: 255
- Connect time: -

WAN 4G Settings:

- Protocol: DHCP Client (dropdown menu)
- Note: If you use APN card, please fill in the following parameters correctly:
- APN: 4-32 characters, including letters, numbers and partial special symbols (Optional)
- Username: 4-32 characters, including letters, numbers and partial special symbols (Optional)
- Password: 4-32 characters, including letters, numbers and partial special symbols (Optional)
- APN Protocol: IPv4 (dropdown menu)
- DNS Server: 114.114.114.114 (Optional)
- Standby DNS Server: 223.5.5.5 (Optional)

At the bottom of the settings area, there are two buttons: "Save" and "Apply".

Figure 21 SIM card 2 configuration interface

2.5.5 Wireless Settings

Select the working mode, the working mode can be divided into AP mode and Client mode, when the working mode is selected as the AP mode, as shown in Figure 22.

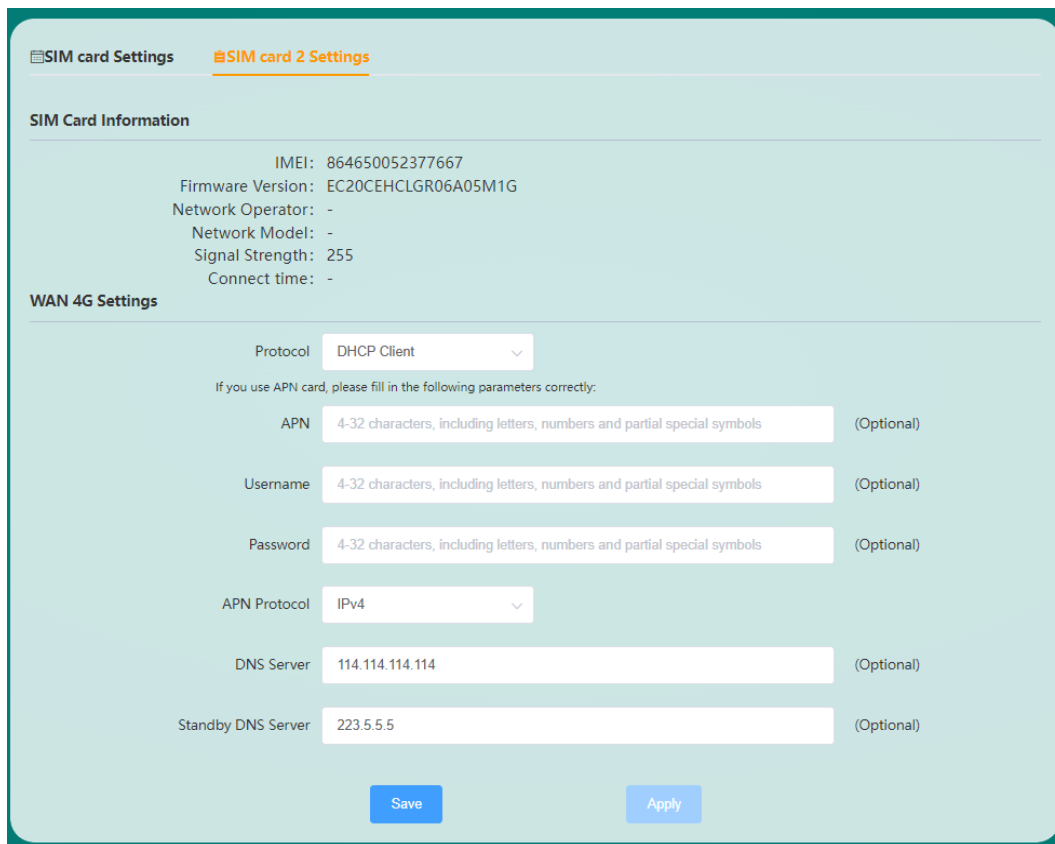


Figure 22 AP mode interface

This interface can switch the wireless network, set wireless parameters such as SSID, and modify the Wi-Fi encryption method and password. The legal value length of the wireless password is 8-32 bytes, which can only include numbers, letters and some special symbols (~!@#%&*()_+-.).

When the working mode is Client mode, as shown in Figure 23.

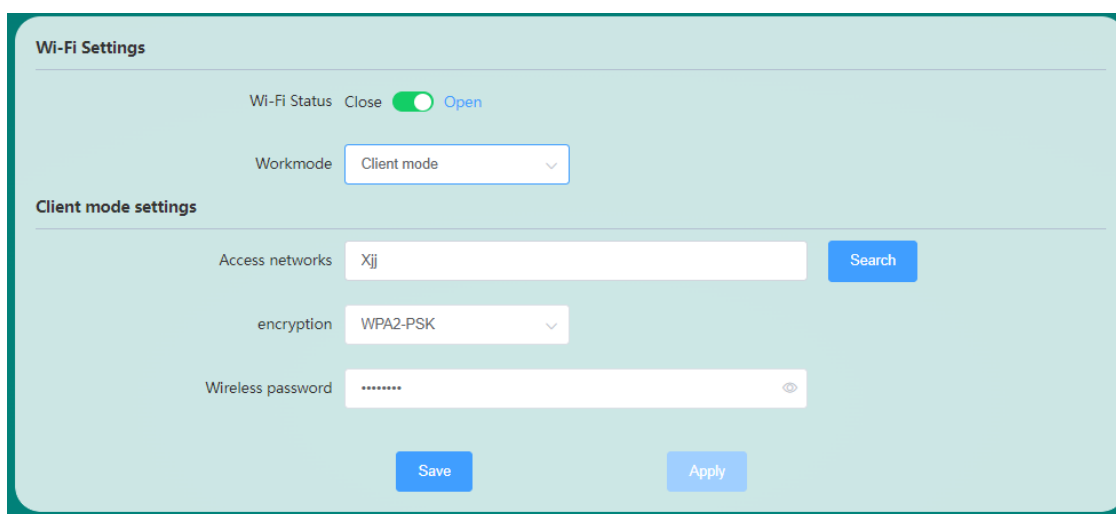


Figure 23 Client mode interface

The legal value length of the wireless password is 8-32 bytes, which can only include numbers, letters and some special symbols (~!@#%&*()_+-.).

Click Search to search for wireless hotspots in the area where the router is located, as shown in Figure 24, select the name of the wireless network to be accessed, and click Connect to jump to the interface for entering the wireless password, as shown in Figure 25.

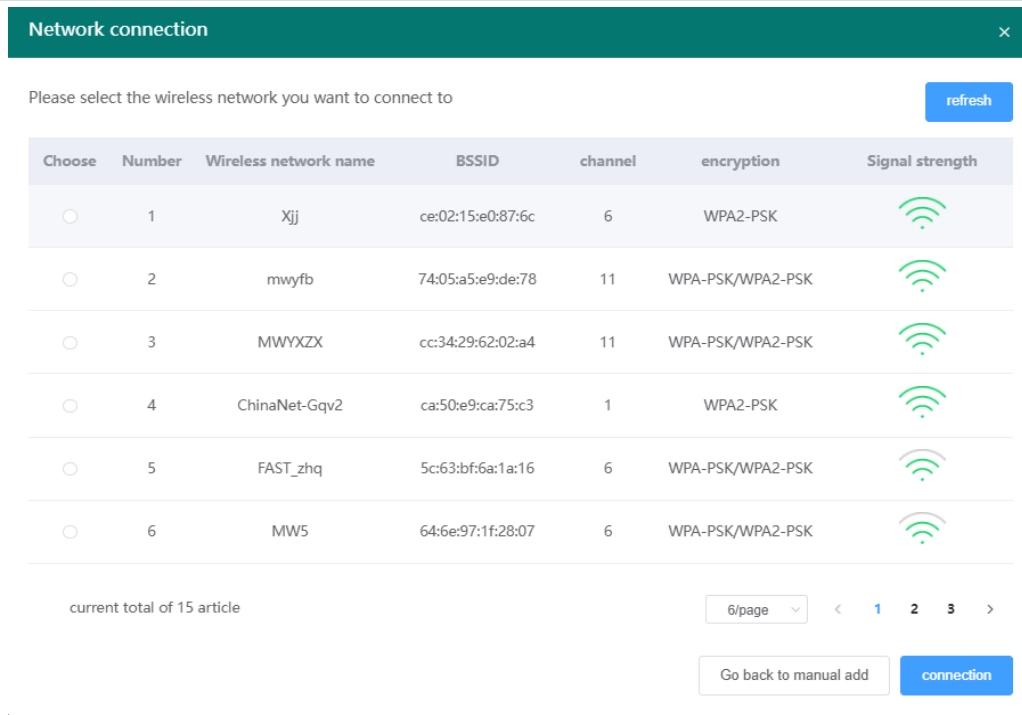


Figure 24 Search interface

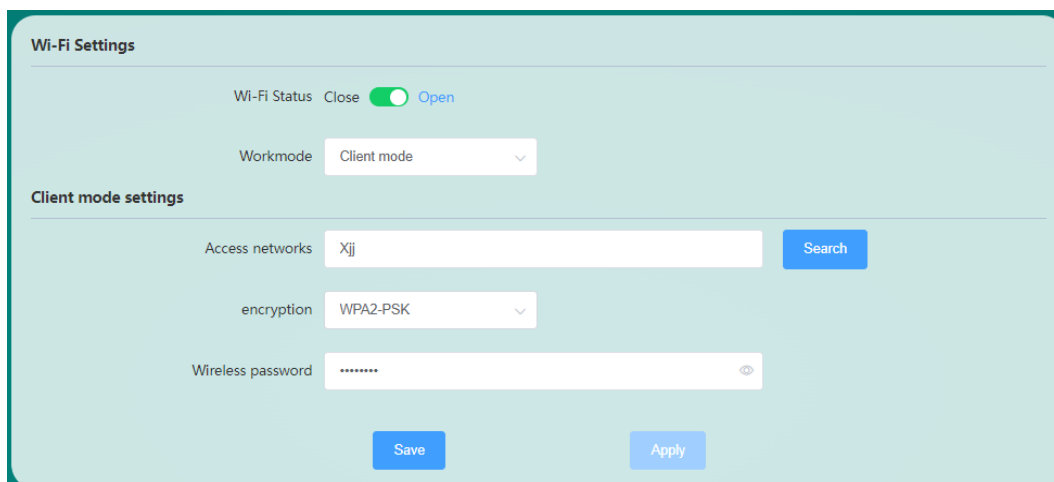


Figure 25 The interface after clicking connect

Enter the correct wireless password, and after saving the application, the router will actively connect to the selected wireless hotspot. After the connection is successful, the connection information of the WWAN wireless network card will be displayed on the network interface interface.

2.5.6 Access device

Displays a list of terminal devices currently connected to the router. As shown in Figure 26.

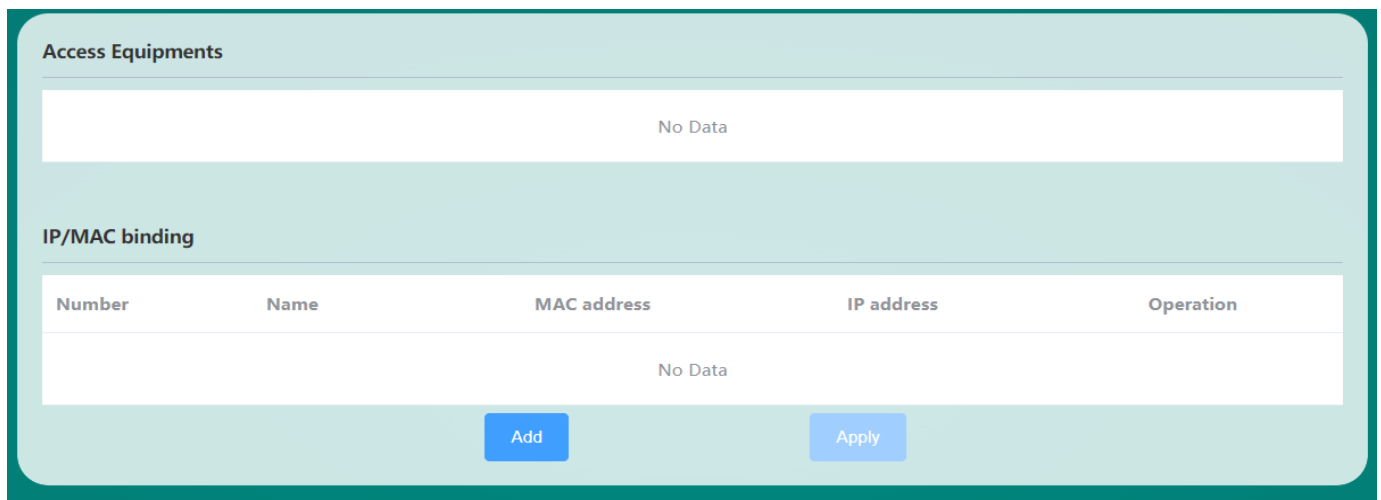


Figure 26 Access device interface

The access device in this chapter is the terminal device whose IP is assigned by the router's DHCP Server. If it is a static IP device, it can be viewed from the "Terminal Device" list on the status page.

IP/MAC binding is mainly used to bind the IP address of the LAN terminal to prevent the terminal from modifying the IP arbitrarily, resulting in IP address conflict in the network, thus causing the network to fail. IP/MAC binding requires the router LAN port to enable the DHCP Server function.

2.5.7 Static Routing

Static routing is a routing method that describes the routing rules on the Ethernet. Static routing items are manually added and configured instead of dynamically determined. Unlike dynamic routing, static routing is fixed and does not change even if network conditions have changed or been reconfigured. The parameters for adding static routes are shown in Table 5.

Name	Meaning	Remarks
Interface	The port on which the static routing rule is executed	The WAN port is selected by default
Destination network	The destination network address or address range to be accessed	such as 192.168.30.0
Subnet mask	Subnet mask of the destination network to access	255.255.255.0
Gateway	Gateway address to forward to	such as 192.168.1.102
Hop count	The number of packet jumps	Fill in 0 by default

Table 5 Static routing parameter table

The router does not add any static routing rules by default. The addition of static routes needs to be configured according to the actual network deployment environment. An example of the use of static routes is as follows: Figure 27 shows the network deployment of two routers A and B and connected devices T1 to T4.

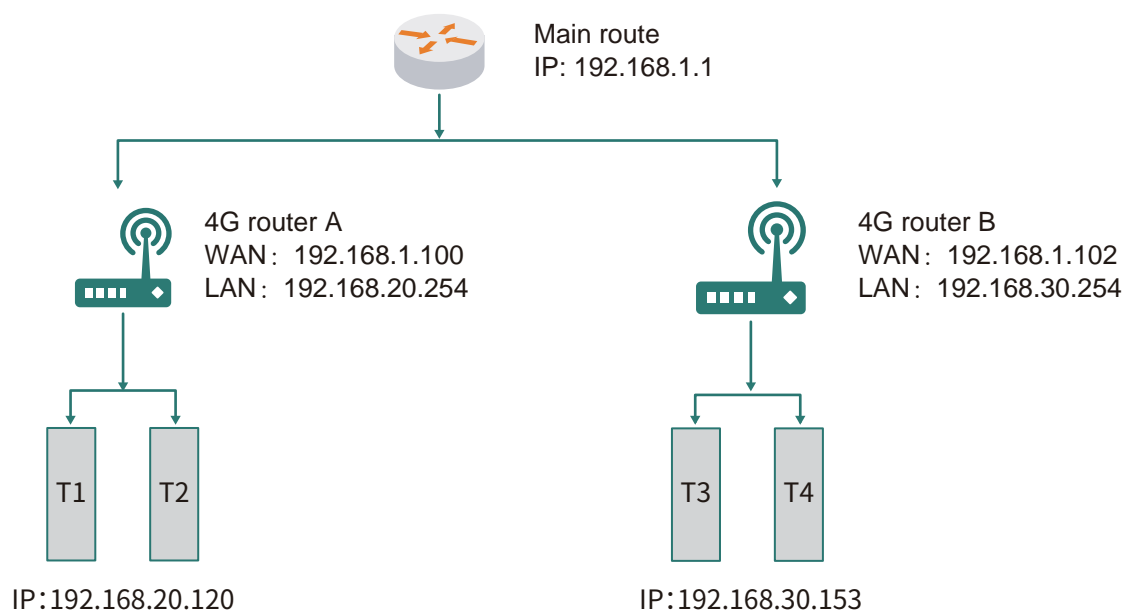


Figure 27 Network connection diagram

The WAN ports of routers A and B are both connected to the network of the main route 192.168.1.0, the LAN port of router A is the 192.168.20.0 subnet (the static IP of the LAN port of router A needs to be modified first to 192.168.20.254), the router B's LAN port is on the 192.168.20.0 subnet The LAN is the 192.168.30.0 subnet (you need to modify the static IP of the LAN port of router B to 192.168.30.254 first).

Now, if we want to make a route on router A, when router A accesses the 192.168.30.x address, it will be automatically forwarded to router B. Set up a static route on router A first, as shown in Figure 28.

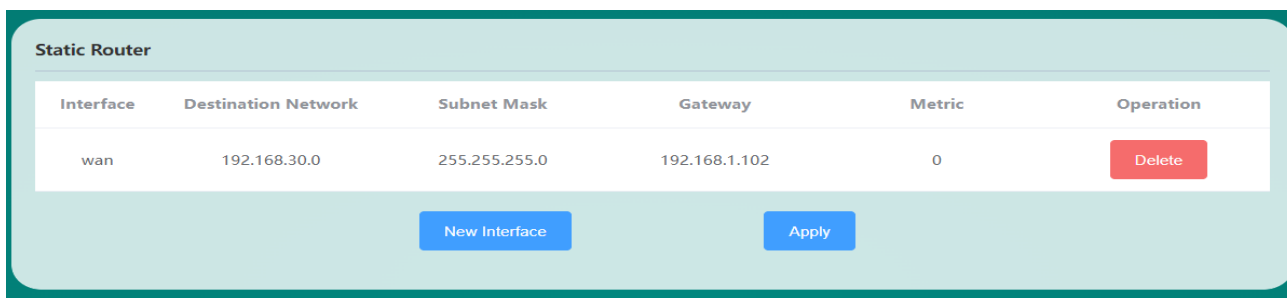


Figure 28 Static routing interface

On T1 (use a PC as T1), use the ping command to access 192.168.30.254 (that is, the LAN port IP of router B), as shown in Figure 29.

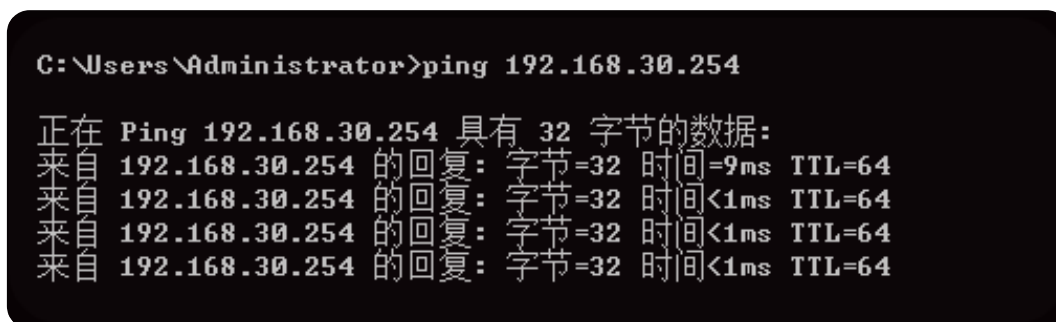


Figure 29 ping interface

It can be seen that the static route has taken effect, otherwise the LAN port of router B cannot be accessed from T1. If we also want to access the devices under router B, such as T3, we also need to enable the WAN port to LAN forwarding function in the basic firewall settings of router B. The MIR675 router enables the forwarding function from the WAN port to the LAN port by default (no further settings are required), as shown in Figure 30.

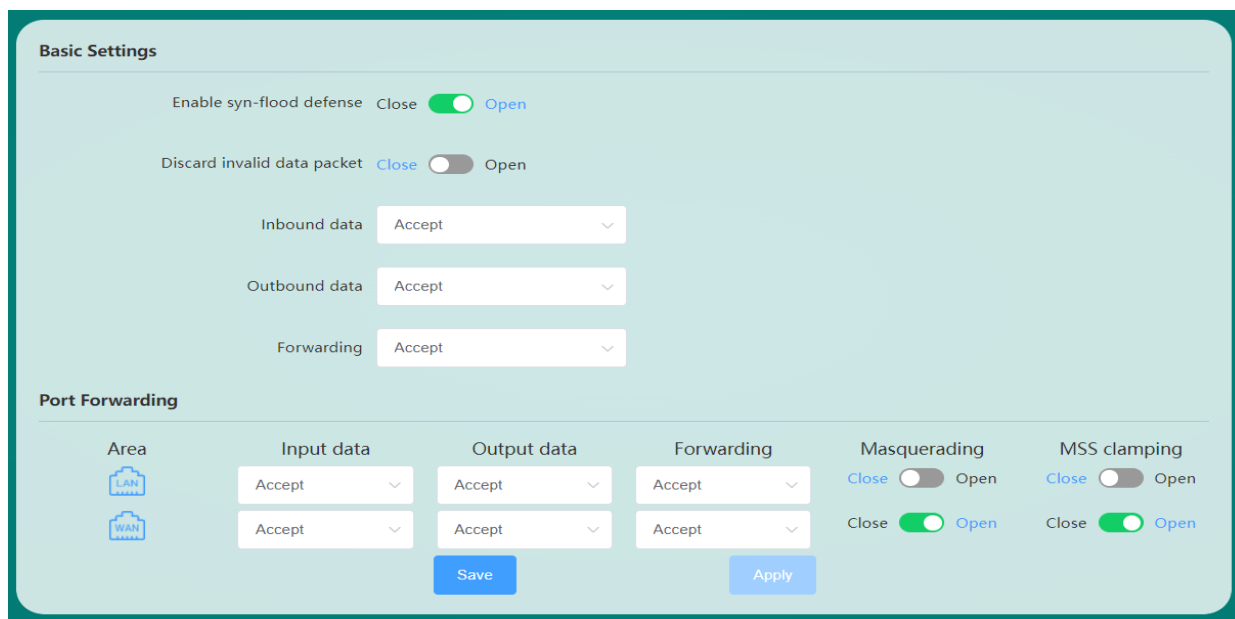


Figure 30 Basic settings page

When the firewall rules of router B are set, T3 can be accessed. Figure 31 shows that T3 (192.168.30.153) under router B can be accessed.

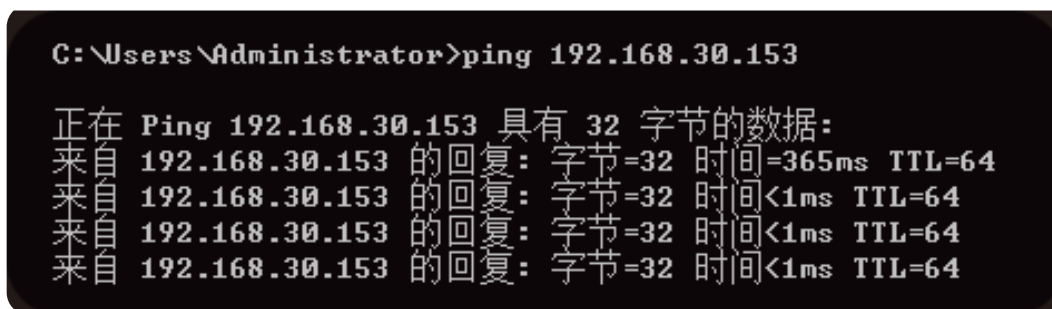


Figure 31 ping page data

The above static routing example shows the routing configuration for device T1 under router A to access device T3 under router B. If you want device T3 under router B to access device T1 under router A, you need to set the same on router B. A static route, and then enable the forwarding function from the WAN port of router A to the LAN port.

2.5.8 Ping Watchdog

The Ping watchdog function is a function of the router to detect the network connectivity. It periodically sends ping packets to a specific IP. If a reply is received normally, the network is smooth. If there is no response within the maximum time limit, the 4G module or 4G router will automatically restart, and continue to detect after restarting until the network returns to normal. The Ping watchdog setting parameters are shown in Figure 32.

Figure 32 ping the watchdog

- **Enable Ping Watchdog:** Enable or disable the Ping watchdog detection function, which is enabled by default. 4G router network disconnection automatic detection, multi-network online automatic backup switching function needs to open the Ping watchdog detection function.
- **Preferred destination IP:** Generally, to detect the connectivity between the router and the external network, the destination IP address is recommended to be set to the public IP address of the cloud server (the factory default setting is the IP address of the public DNS server); if the router uses an APN dedicated network card to connect to the operator's dedicated network, the destination IP address is recommended to be set to the APN private network gateway or the server IP address under the same APN private network.
- **Alternate target IP:** After the connection detection of the preferred target IP fails, try to detect the alternate target IP. Can be set to empty.
- **Packet sending cycle:** The sending cycle of ping detection packets (unit is second, the default value is 30 seconds), which can be set as required. If there are many routers, it is recommended that the sending cycle should not be too small, so as not to cause a large network burden.
- **Maximum number of failures:** After the number of consecutive ping packet failures reaches the set maximum value, the 4G router will restart the module or restart the system to restore the network connection.
- **Recovery operation:** After the number of consecutive ping packet failures reaches the set maximum value, the router will perform a recovery operation to try to recover the network. The recovery operation can choose to restart the module (factory default is to restart the module) or restart the system.

➤ Example of restart time calculation method:

The ping watchdog function will restart the module or system when the number of consecutive detection failures reaches the maximum number of failures when the ping of the preferred target IP and the backup target IP fails. Therefore, to calculate how long it takes to restart, as long as the multiplication of the packet sending period and the maximum number of lost packets is equal to the time value. For example, we want the router to restart the module every 30 minutes when the network is always disconnected, then $30 \text{ minutes} = 30 * 60 = 1800 \text{ seconds}$, the packet sending period is 30 seconds, and the maximum packet loss is 60.

2.5.9 Network Diagnosis

This interface provides a simple router network test function, such as the diagnostic result of pinging the router, as shown in Figure 33.

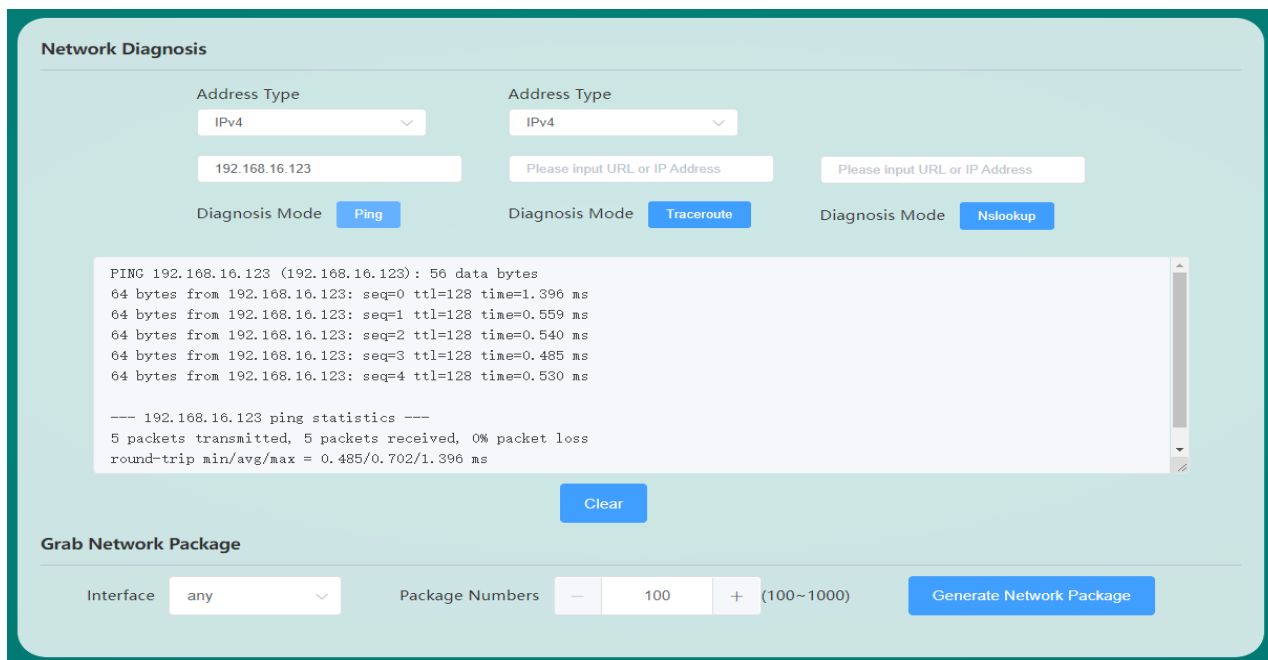


Figure 33 Network Diagnostics Page

The interface also provides network packet capture function, select the interface to be captured (default capture network data packets of all network card interfaces) and the number of network packets, click "Generate Network Download Package" to download the captured network packet data.

2.6 Firewall

2.6.1 Basic settings

The default configuration in the firewall basic settings, as shown in Figure 34.

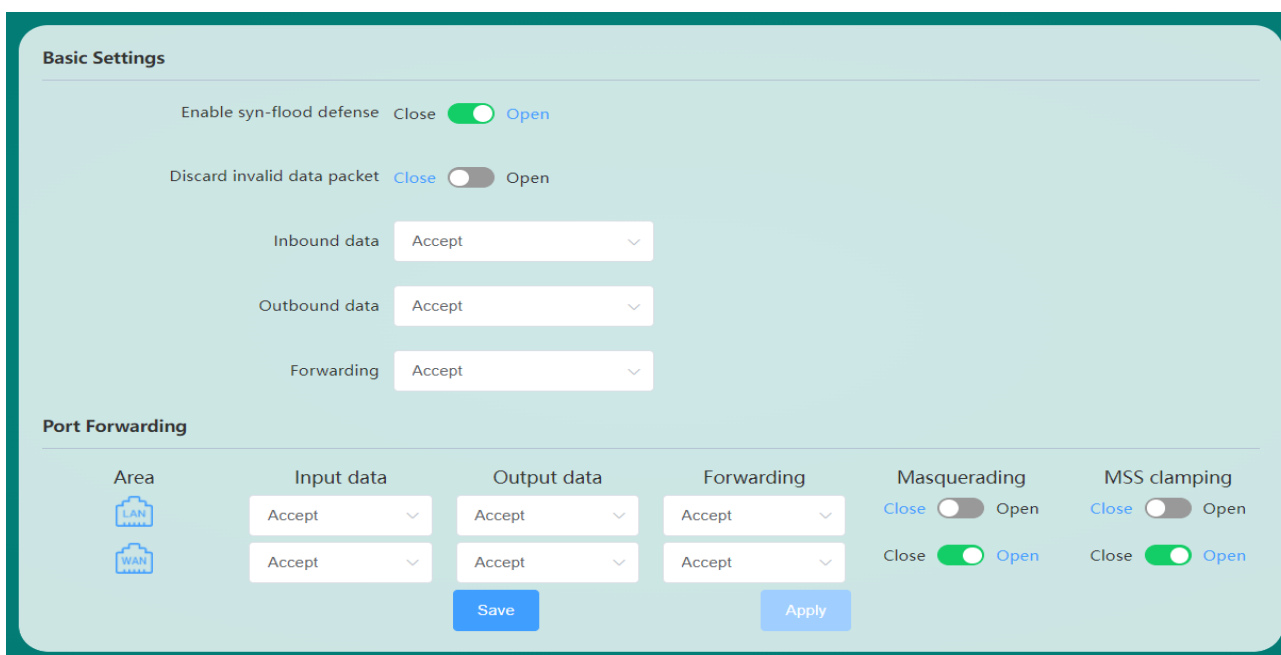


Figure 34 Basic settings page

- **Inbound:** Packets that access the router's IP.
- **Outbound:** The data packets to be sent out by the router IP.
- **Forwarding:** Data forwarding between the WAN port and the LAN port does not pass through the router itself.
- **IP dynamic masquerading:** IP address masquerading when accessing the external network is only meaningful for the WAN port.
- **MSS clamp:** limit the size of the MSS of the message. .

➤ As shown above, there are two firewall rules by default:

Rule 1: Inbound and forwarding from the LAN port to the wired WAN port are accepted.

If a data packet comes from the LAN port and wants to access the WAN port, this rule allows the data packet to be forwarded from the LAN port to the WAN port, which is "forwarding"; under the LAN port, open the router's web page, which is "inbound" "; the router itself accesses other devices in the LAN through the LAN port, such as synchronizing the time, which belongs to "outbound".

Rule 2: WAN port (wired WAN port and 4G/5G WAN port), accept "inbound", accept "outbound", and reject "forwarding".

If there are "inbound" packets, such as someone intending to log into the router's web page from the WAN port, it will be allowed.

This action is allowed if there are "outbound" packets, such as the router accessing the external network through the WAN port or 4G/5G port. If you want to access the device under the router's LAN port from the external network, this is "forwarding", and "forwarding" is rejected by default. If you need to configure static routes and other requirements, you need to configure "forwarding" as an acceptance rule.

2.6.2 Port Forwarding

Port mapping forwarding is to map a specified port of the WAN port address to a host on the intranet. If we want to access a device in the LAN from the external network (the router must be accessible from the external network), then we need to set the mapping from the external network to the internal network, such as setting the external network port to 1000 and the internal network IP to 192.168.30.129, the intranet port is 8848. When we access port 1000 from the WAN port, the access request will be transferred to 192.168.30.129:8848, and the corresponding port forwarding rule is shown in Figure 35.

The screenshot shows a 'New Port Forwarding' dialog box with the following configuration:

- Name: Foward
- Protocol: TCP+UDP
- Source area: wan
- Source port: 1000
- Destination area: lan
- Destination IP address: 192.168.30.129
- Destination port: 8848
- Status: Open (toggle switch)

Figure 35 New port forwarding page

- **Name:** The name of the port forwarding rule remark. The legal value is 1-32 bytes in length. It can only include numbers, letters and some special symbols (-!@#\$\$%^&*()_+-.).
- **Protocol:** The default is tcpudp, the network protocol corresponding to the current forwarding rule.
- **External area:** The default is wan port, the default value is fine.
- **External Port:** External port number, supports input port number (1-65535) or port range (8848-8948) configuration format.
- **Internal area:** The default is the lan port, the default value is fine.
- **Internal IP Address:** The IP address of the internal host to which to map forwarding.
- **Internal port:** The port number of the internal host to be mapped and forwarded, supports the input port number (1-65535) or the port range (8848-8948) configuration format. When entering the port range, the external port range and the internal port range must be consistent.
- **Status:** Whether the new port forwarding rule is enabled or not, the default is the enabled state.

2.6.3 Access restrictions

Access restriction implements permission management for devices in the local area network to access the external network, including IP address filtering, MAC address filtering, and domain name filtering, as shown in Figure 36.

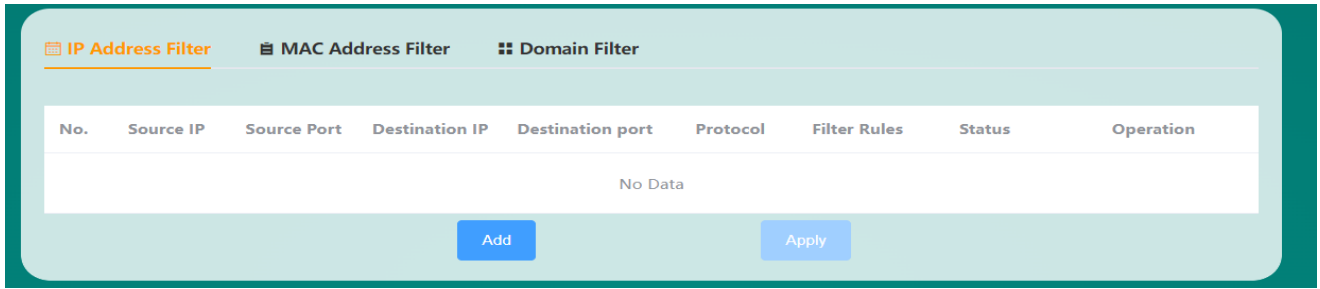


Figure 36 IP address filtering page

➤ IP address filtering

To filter hosts whose IP address is 192.168.30.246 to access the external network, as shown in Figure 37.

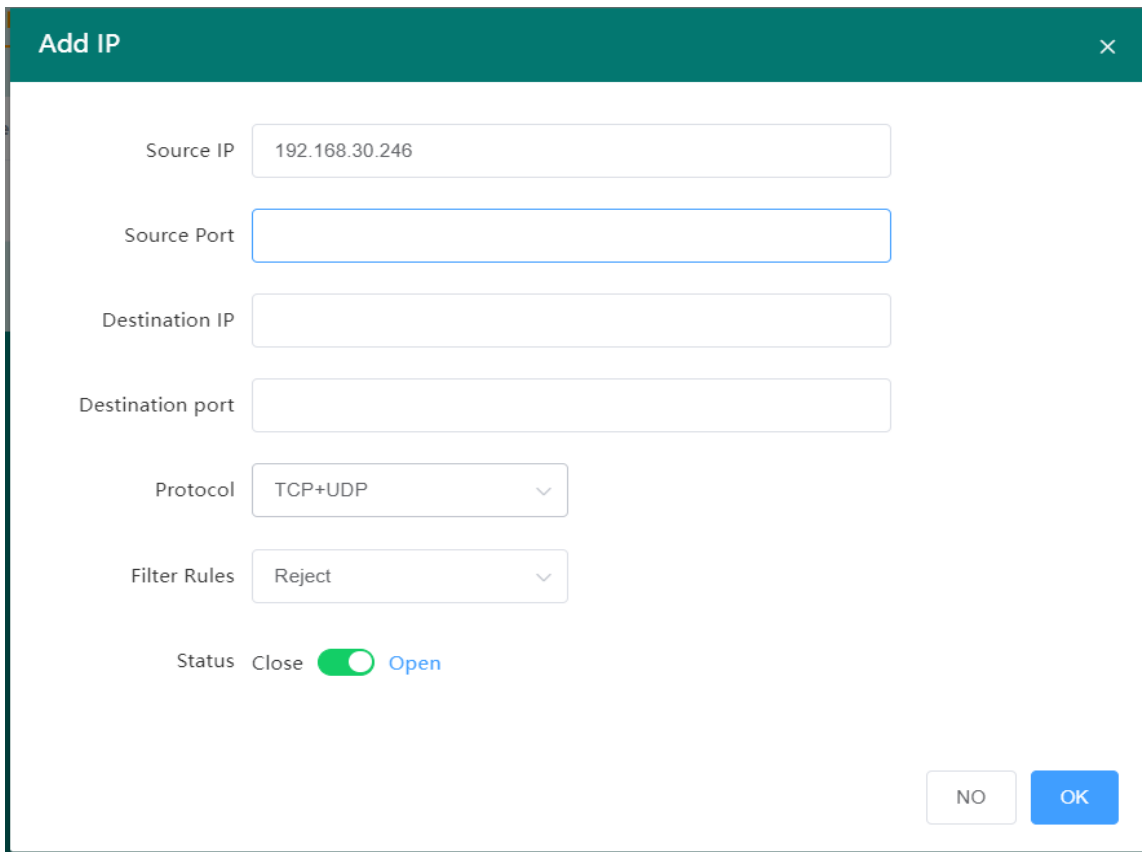


Figure 37 Add IP page

- **Source IP Address:** The IP address of the host to be filtered.
- **Source port:** Generally do not need to set this parameter, the default is to filter all ports of IP hosts.
- **Destination IP:** Generally, this parameter does not need to be set. The default is to restrict IP hosts from accessing all external networks.
- **Destination port:** Generally, this parameter does not need to be set. The default is to filter all ports of IP hosts accessing all external networks.
- **Protocol:** The default protocol is tcpudp, which restricts the access of IP hosts by tcp and udp protocols.
- **Filtering rules:** The default is Deny, which restricts IP hosts from accessing the external network.
- **Status:** Whether the newly added IP filtering rule is enabled or not, it is enabled by default.

➤ **MAC address filtering**

As shown in Figure 38.

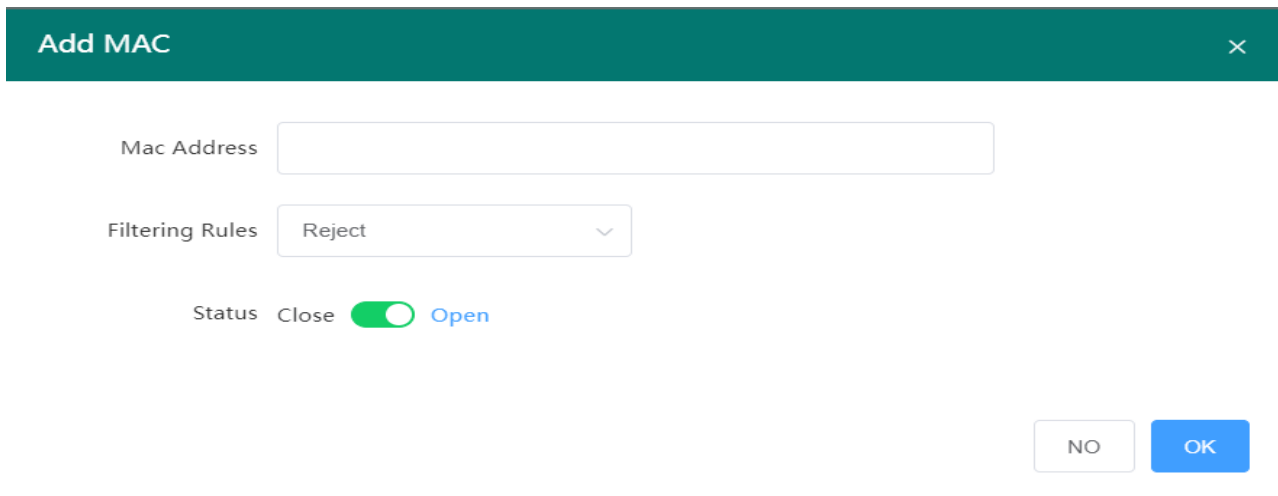


Figure 38 Add MAC page

- **MAC Address:** The MAC address of the host to be filtered.
- **Filtering rule:** The default filtering rule is deny, that is, the host with the MAC address is restricted from accessing the external network through the router.
- **Status:** Whether the newly added MAC address filtering rule is enabled to take effect. It is enabled by default to take effect.

➤ **Domain name filtering**

The access restriction to the specified domain name supports the blacklist and whitelist settings of domain name addresses, as shown in Figure 39.

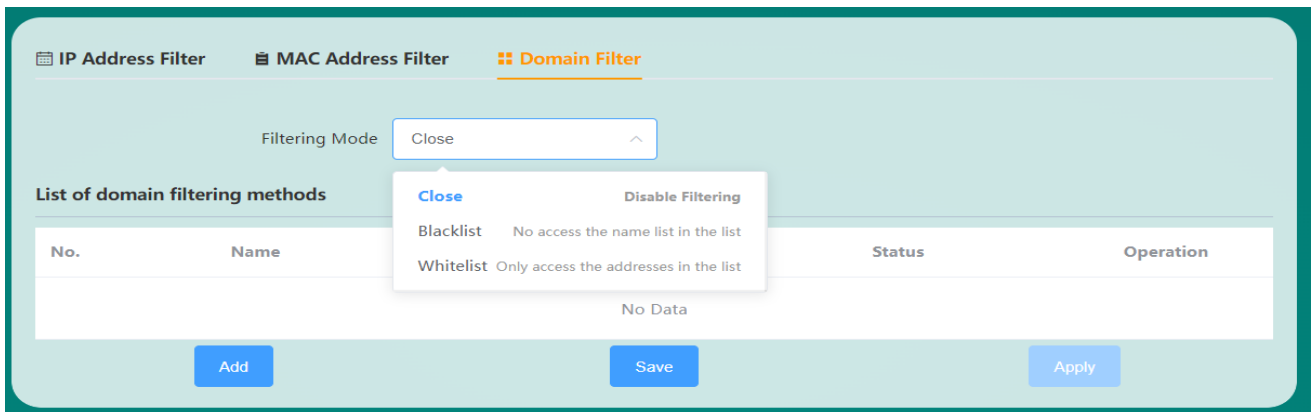


Figure 39 Domain name filtering page

Domain filtering is disabled by default. When the blacklist is selected, the devices connected to the router cannot access the blacklisted domain names, and other domain names can be accessed normally; when the whitelist is selected, the devices connected to the router can access the domain names set in the whitelist, but other domain names cannot be accessed normally. Access, blacklist and whitelist can set up to 8 domain name filtering rules. The add domain name setting interface is shown in Figure 40.

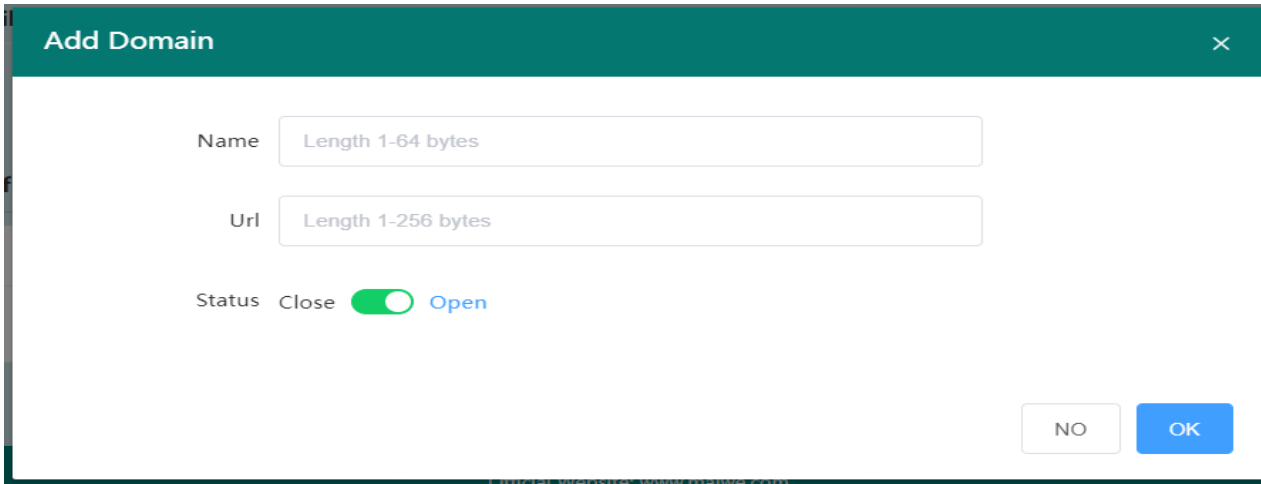


Figure 40 Add domain name page

- **Name:** The name of the annotation for the domain filter to add.
- **URL:** The domain URL or domain URL keyword to be added for domain filtering.
- **Status:** Whether the currently added domain name filtering rule is enabled or not, it is enabled by default.

2.6.4 Custom Rules

The router firewall supports custom configuration rules to extend more complex firewall configuration functions. Currently supports iptables instructions, you need to refer to the Linux iptables related instructions to write instructions to run. If access to router port 8848 is denied, refer to the instruction shown in Figure 41.

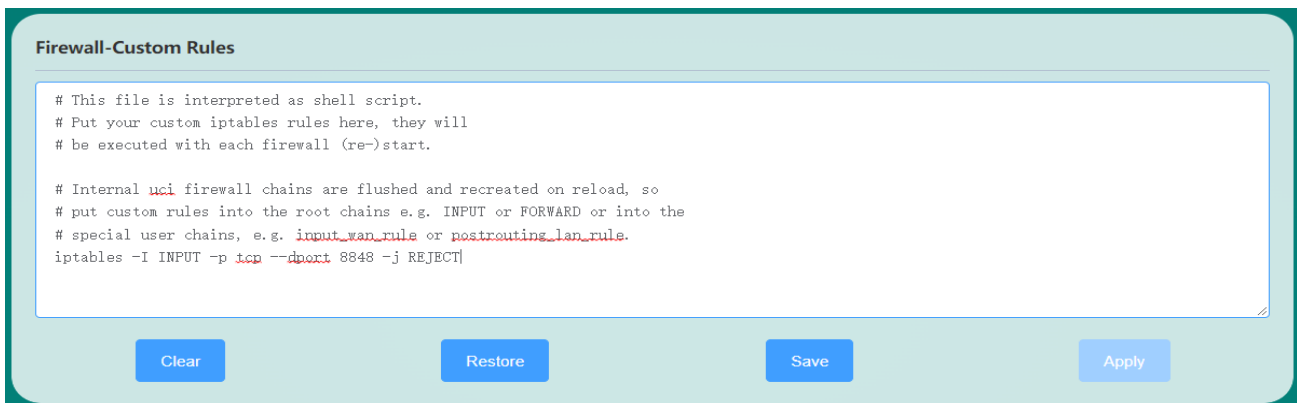


Figure 41 Custom Rules page

2.6.5 DMZ

DMZ is the abbreviation of "demilitarized zone" in English, and the Chinese name is "demilitarized zone", also known as "demilitarized zone". It is to solve the problem that the external network cannot access the internal network server after the firewall is installed, and a buffer zone between the non-security system and the security system is established. This buffer zone is located in the small network area between the internal network of the enterprise and the external network. , some server facilities that must be exposed can be placed in this small network area,

Such as enterprise Web server, FTP server, etc. Through such a DMZ area, the internal network is more effectively protected. The DMZ host function is disabled by default, and it needs to be enabled in the manual configuration interface. The DMZ setting interface is shown in Figure 42.

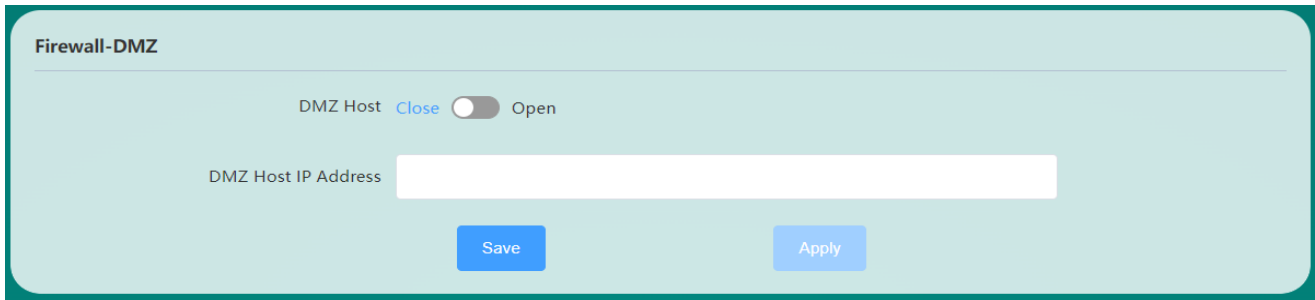


Figure 42 Firewall-DMZ page

- **DMZ host IP address:** the IP address of the DMZ host in the LAN.

The DMZ function is to expose the DMZ host in the gateway and map all ports of the DMZ host, so port forwarding and DMZ function cannot be used at the same time.

2.6.6 UPnP

Universal Plug and Play (UPnP) is a set of network protocols promoted by the "Universal Plug and Play Forum" (UPnP™ Forum). The goal of this protocol is to enable various devices in home networks (data sharing, communication and entertainment) and corporate networks to seamlessly connect to each other and to simplify the implementation of related networks. UPnP accomplishes this by defining and publishing a UPnP device control protocol based on open, Internet Protocol standards. The UPnP function is disabled by default, and the interface configuration is shown in Figure 43.

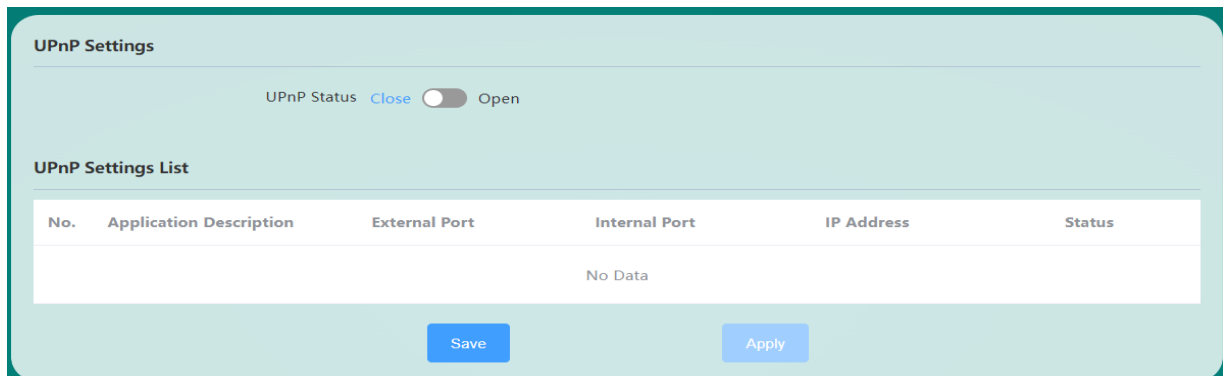


Figure 43 UPnP settings

2.6.7 Internet Speed Control

Network speed control can limit the uplink and downlink rates of devices connected to the router accessing the network. It supports IP segment address speed limit and MAC address speed limit, and multiple rules can be added at the same time.

IP segment address speed limit: You need to fill in the starting IP address, ending IP address, downlink rate, and uplink rate. As shown in Figure 44, the maximum uplink and downlink rates of the network segment 192.168.30.10-192.168.30.100 are limited to 100KB/S.



Add IP Network Control ×

Starting IP

Ending IP

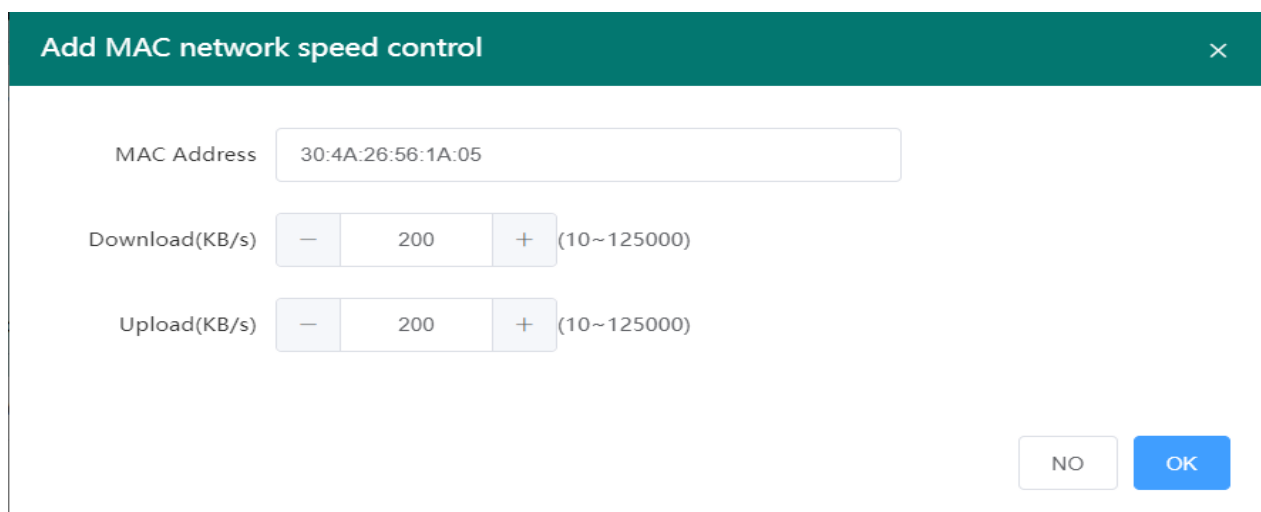
Download(KB/s) (10~125000)

Upload(KB/s) (10~125000)

Figure 44 Add IP speed control page

➤ MAC address speed limit

You need to fill in the MAC address, and fill in the uplink rate and downlink rate. The rule setting will take effect immediately after clicking OK and applying. As shown in Figure 45, the device corresponding to the MAC address 30:4A:26:56:1A:05 restricts access to the network with a maximum uplink and downlink rate of 200KB/S.



Add MAC network speed control ×

MAC Address

Download(KB/s) (10~125000)

Upload(KB/s) (10~125000)

Figure 45 Add MAC speed control page

2.6.8 QoS Services

The full name of QoS is Quality of Service, which means quality of service. It is specially designed to solve the problem of non-discriminatory signal quality on congested networks. The QoS service is disabled by default, and the configuration interface is shown in Figure 46.



Figure 46 QoS service

- **QoS service:** Disable or enable QoS service function, QoS service is disabled by default.
- **Download speed:** Set to the current downlink bandwidth value, generally bandwidth*90%, for example, the measured bandwidth is 10Mbps, and the download speed value is set to $10 \times 1000 \times 0.9 = 9000$ kbps.
- **Upload speed:** Set to the current upload bandwidth value, generally bandwidth*90%, for example, the measured bandwidth is 10Mbps, and the download speed value is set to $10 \times 1000 \times 0.9 = 9000$ kbps.

2.7 System

System modules include system properties, administrative rights, restart, backup/upgrade, scheduled tasks, and system logs.

2.7.1 System Properties

The function of this function is to display the current system time, as well as the host name and time zone of the router, which can be set, as shown in Figure 47.

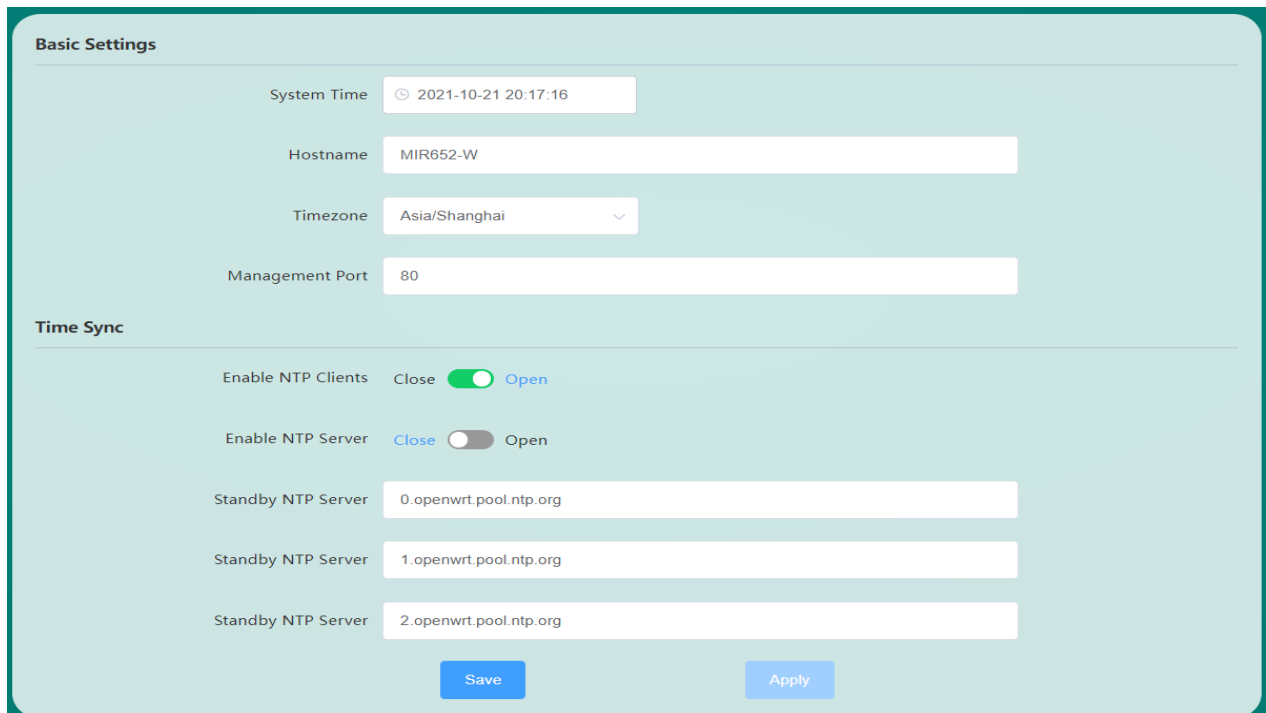


Figure 47 System Properties

- **System Time:** Get the current system time, which can be modified by clicking the clock icon, or synchronizing the browser's time with the router's time.
- **Host Name:** The name of the current host.
- **Time Zone:** The time zone used by the current router.

➤ The router also provides the NTP network time automatic synchronization function. The corresponding parameters are as follows:

- **Enable NTP Client:** Enable the router to synchronize the time of the NTP server.
- **Enable NTP server:** Enable the router to function as an NTP server to provide NTP time synchronization services to the outside world.
- **Candidate NTP servers 1~3:** The router is configured with three NTP server addresses by default, and the user can specify and modify the candidate NTP server addresses.

2.7.2 Management rights

You can modify the administrator password on the management rights page, or add new common users (up to 5 common users can be added, and common users cannot operate the firewall configuration interface), as shown in Figure 48.

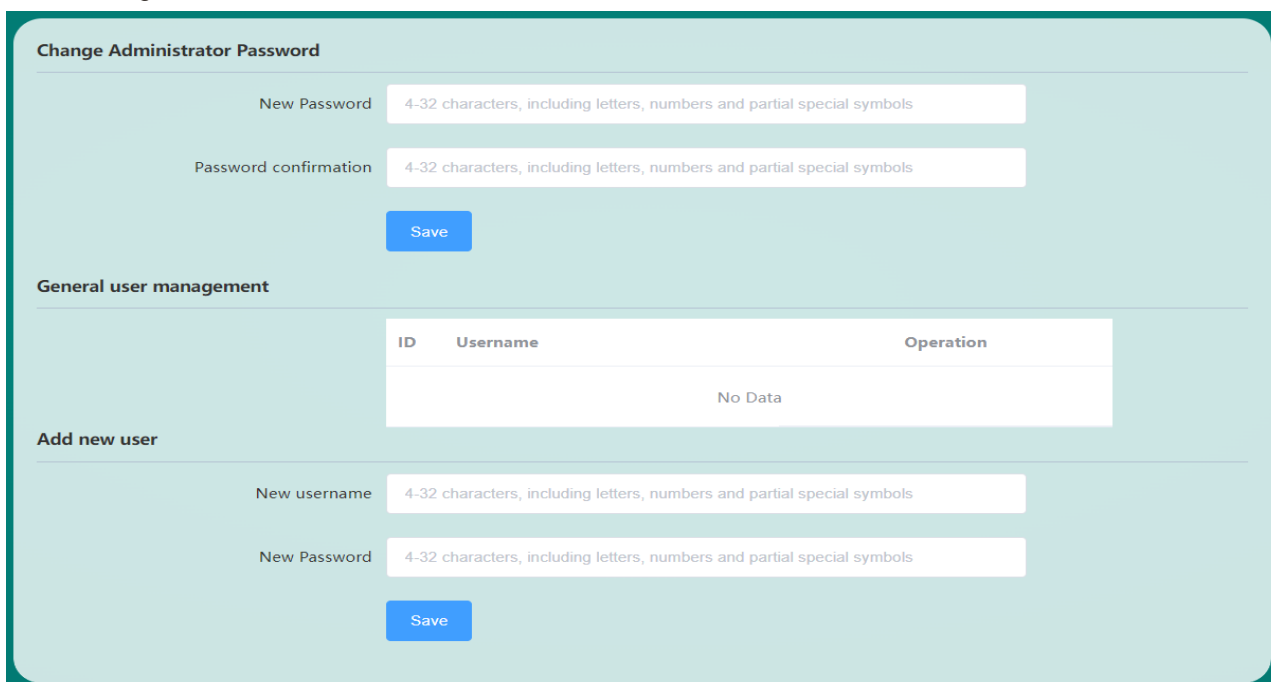


Figure 48 Management rights interface

The legal value length of the administrator password and new user password is 4-32 bytes, and can only include numbers, letters and some special symbols (~!@#%&^&*(*)_+-.).

2.7.3 Reboot

On the restart page, users can restart the router immediately or set the router to restart regularly, as shown in Figure 49.

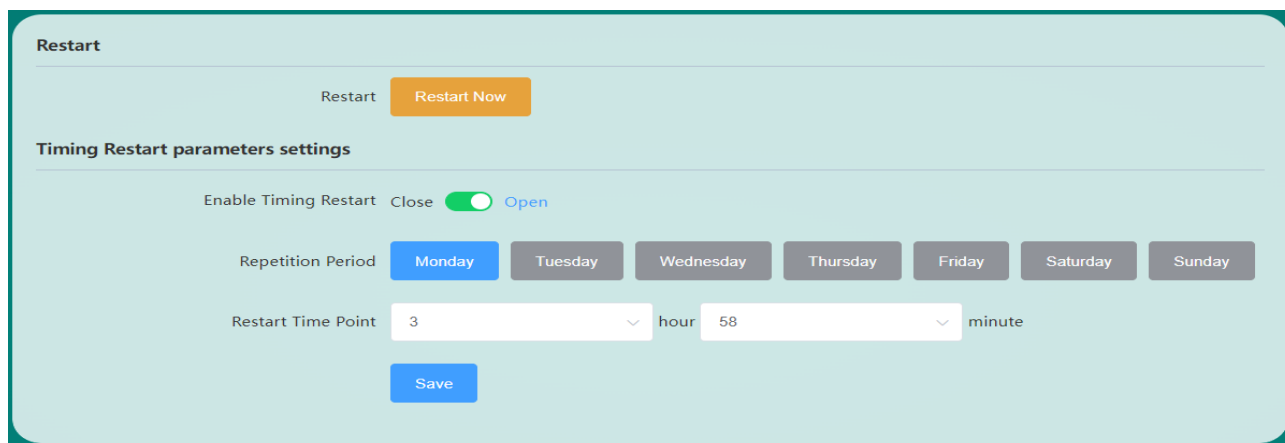


Figure 49 System restart page

The scheduled restart function is enabled by default (the default scheduled restart time is set to 3:58 a.m. every Monday, and the scheduled restart function can be turned off).

2.7.4 Backup and Restore

On this page, you can perform configuration file backup and restore operations, restore factory settings, and flash and upgrade new firmware for the router, as shown in Figure 50.

Backup and Restore Notice: the backup router configuration can be used for recovery after reswiping the router or resetting the router

Generate Download Backup

Restore Factory Settings

Upload backup archive to restore the settings

Only upload *.tar.gz file

Refresh new firmware

Keep settings OK NO

Firmware upgrade check OK NO

Firmware file

Only upload *.bin file

Figure 50 Backup and restore

- **Backup:** After clicking the "Backup" button, the router will back up the currently used parameters into a compressed package file, such as backup-MIR675-W-20200606172519.tar.gz, and then download and save it locally.
- **Restore:** After clicking the "Restore" button, the router will restore the factory parameter settings and restart automatically. In addition, you can restore the factory settings by pressing and holding the router INIT button for more than 5 seconds.
- **Upload backup:** Select the backup parameter configuration file, such as backup-MIR675-W-20200606172519.tar.gz, and then click the "Upload Backup" button, the router will save and use the uploaded parameters, and the uploaded parameters will take effect after restarting.
- **Retain settings:** When flashing new firmware, you can choose whether to retain the current parameter settings of the router, and retain the settings by default (it is recommended to choose not to retain the settings to upgrade when the version to be upgraded has a large span or upgrades forward).
- **Firmware upgrade check:** Whether to enable the check function when flashing new firmware, the check function is enabled by default.
- **Flash firmware:** Select a normal firmware file, such as MIR675-1.0.238.200522.bin, and then click the "Flash firmware" button, the router will first check the integrity of the firmware, then flash the firmware to the system and restart automatically. The process of flashing the firmware takes about two minutes.



1. Restoring the factory settings will cause all the parameters of the device to be in the factory settings, and the IP address of the LAN port will be restored to "192.168.16.253". Users need this IP address to access the web management interface.
2. During the operation of uploading backup configuration files, be sure not to select non-router configuration files. Uploading incorrect files may cause damage to the router.
3. Do not power off during uploading the backup configuration file, otherwise the router may be damaged.
4. When flashing the firmware, please pay attention to the matching of the device model and version. Using an unmatched upgrade program may cause permanent damage to the router.
5. Power failure is not allowed during the entire firmware flashing and upgrading process. Power failure may cause permanent damage to the router. If there is an unexpected power failure during the upgrade process, please mail the product to our company immediately for possible solutions.
6. If the settings are disordered, consider restoring the router to factory settings and then reset the reasonable parameters.

2.7.5 Scheduled tasks

This page can set custom schedule, as shown in Figure 51.

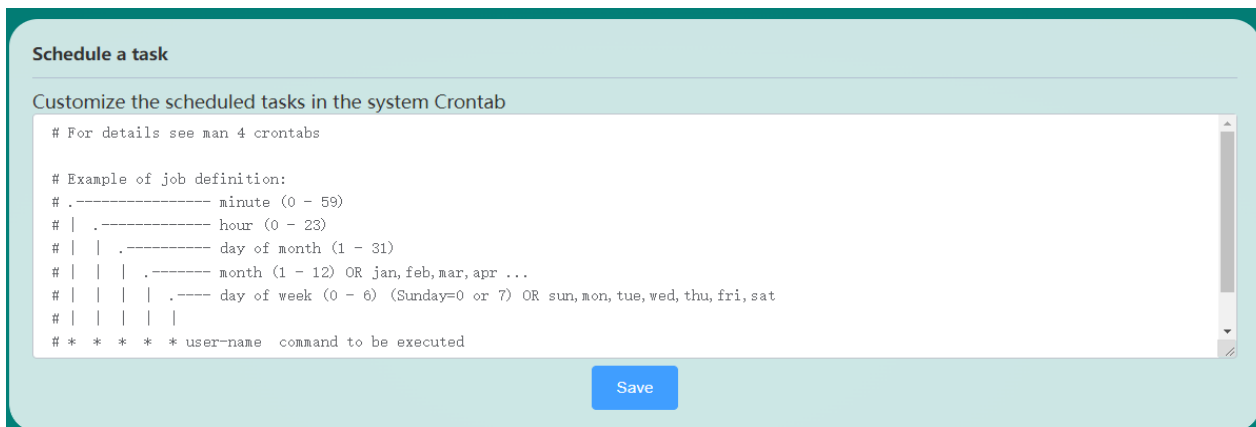


Figure 51 Scheduled tasks page

Writing a scheduled task requires the user to first understand the setting format of the scheduled task (refer to the notes). After the scheduled task is saved, the corresponding commands can be executed automatically without human intervention.

2.7.6 System log

The router provides system log management functions, mainly including three parts: remote log, local log recording and saving, and viewing and downloading, as shown in Figure 52, 53, and 54.

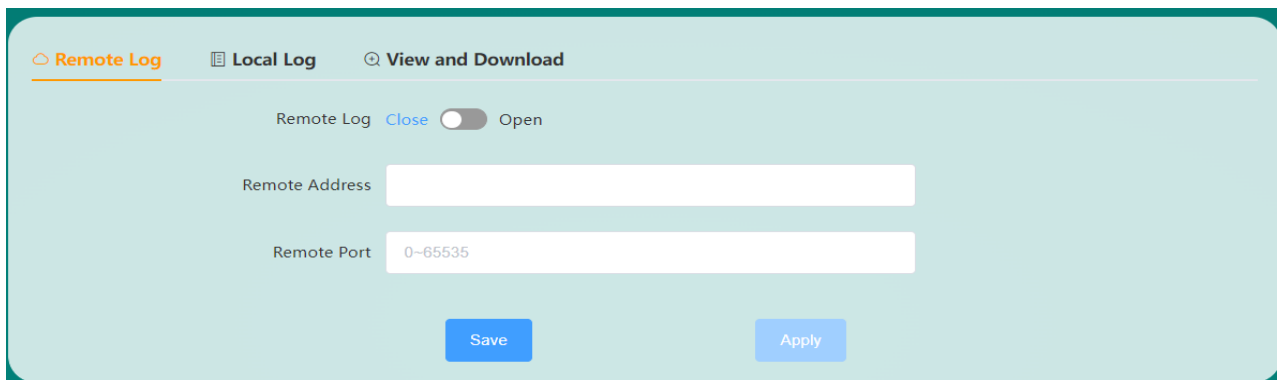


Figure 52 Remote log page

- **Remote log:** switch the remote log function, which is disabled by default. To enable it, you need to set the remote address and port at the same time and enable the syslog service function on the server side.
- **Remote address:** the IP address or domain name of the remote Log server.
- **Remote Port:** the port number of the remote Log server.

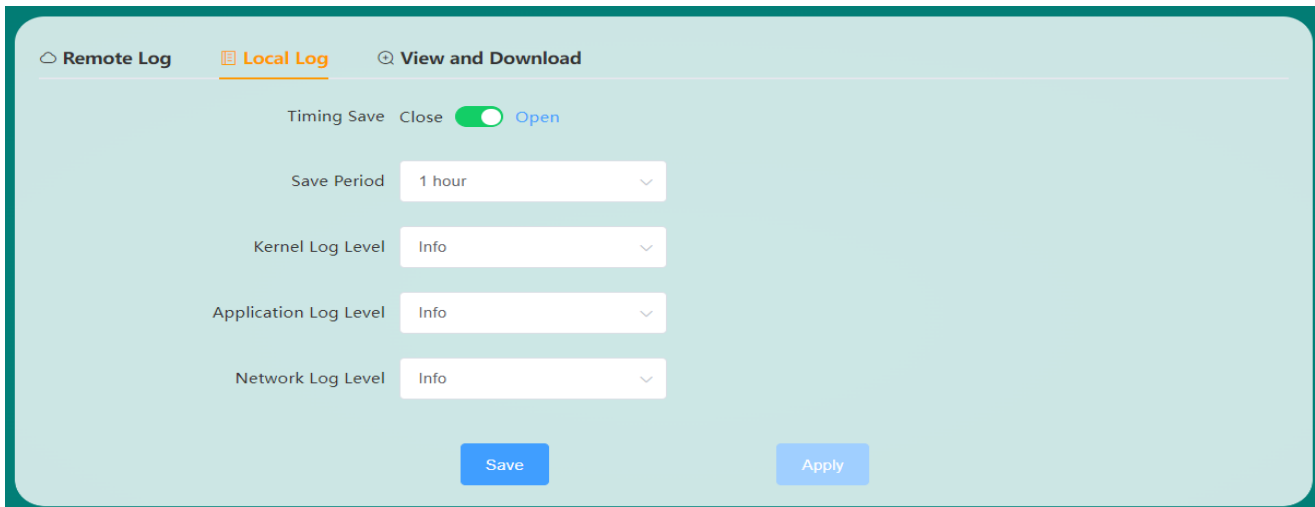


Figure 53 Local log interface

- **Timing save:** local log timing save switch, enabled by default.
- **Save Period:** the periodic setting for the local log to be saved regularly. The default is to save and backup the log once every hour. It supports the function of saving the log after power failure and saving the log immediately after the system restarts.
- **Kernel/application/network log level:** The system log is divided into kernel, application and network log, which supports setting the log level. The log level is defined as 8 levels, which are debugging, information, attention, warning, error, critical, alarm, and emergency.

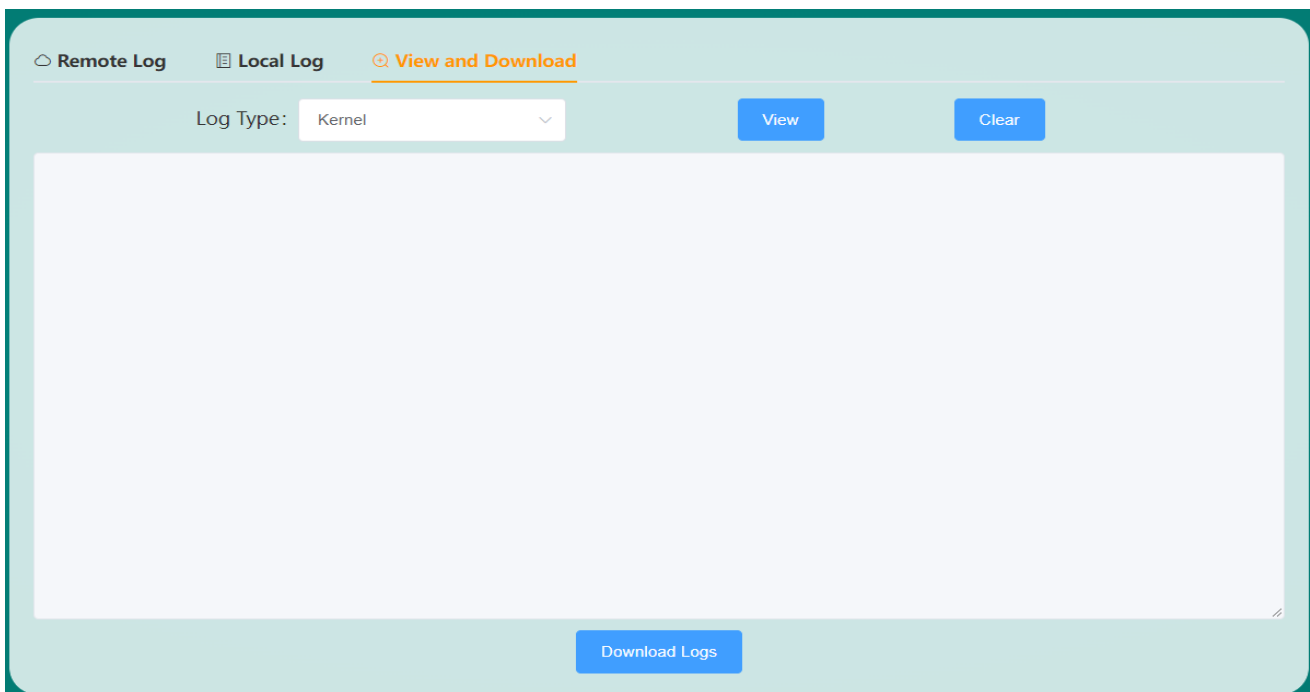


Figure 54 View and download page

- **View:** Logs can be viewed by type. After selecting the log type to be viewed, click View to view the latest log content.
- **Download log:** If you want to view all saved history logs, click Download log to save all saved history logs and the latest log download to the local for viewing.

Chapter 3 WEB Advanced Function Configuration

The advanced functions of the router are mainly located in the service module. The service module includes serial to network, peanut shell intranet penetration, dynamic DNS, VPN (client and server) and SNMP settings.

3.1 Serial to network

Serial port to network function, MIR675 can convert RS-232/485 serial port data into TCP/IP network data, realize bidirectional transparent data transmission between serial port and TCP/IP network interface, and facilitate the networking of serial port devices. The serial port to network interface includes four parts: network, serial port, heartbeat packet, and registration packet. The network parameter configuration page is shown in Figure 55.

The screenshot shows the 'Serial to network' configuration interface. At the top, there is a 'Serial number' dropdown menu currently set to 'COM1'. Below it is a 'Serial port state' toggle switch, currently in the 'Open' position. A horizontal menu below the toggle includes 'Network' (highlighted), 'Serial', 'Heartbeat packets', 'Register packets', and 'Timeout to restart'. Under the 'Network' tab, there is a 'Network mode' dropdown menu set to 'UDP' and a 'Local port' input field containing '51001'. A section titled 'Number of network connections' contains four rows, each with a checkbox, a 'Destination address' input field, and a 'Destination port' input field. The destination ports are pre-filled with 51501, 51502, 51503, and 51504, with a range '(1-65535)' shown to the right of each. At the bottom of the page are two buttons: 'Save' and 'Apply'.

Figure 55 Network parameter configuration page

- **Transmission mode:** The way to transmit data, currently supports serial data transparent transmission mode.
- **Network mode:** The module has 4 transparent transmission network working modes, namely TCP Client, TCP Server, UDP Client, and UDP Server.
- **Remote address:** When the module works in Client mode, the remote address is the IP address or domain name of the Server.
- **Remote port:** When the module works in Client mode, the remote port is the port number of the Server.
- **Local Port:** The local port number when the module is working.
- **Disconnection and reconnection time:** When the device receives the Socket disconnection request sent by the server, it will try to connect again after waiting for the set time. The unit is seconds.
- **No data timeout time:** When set to 0, the reconnection function of no data timeout is disabled; when set to 60~3600, the device will actively disconnect from the server after the time that the device cannot receive data from the network reaches the set time. connect and re-initiate the connection. This function can prevent the device from being in a false connection state for a long time due to the abnormal disconnection of the socket. The unit is seconds.

The serial port page displays the baud rate, data bits, stop bits, parity bits, packing time and packing length, as shown in Figure 56.

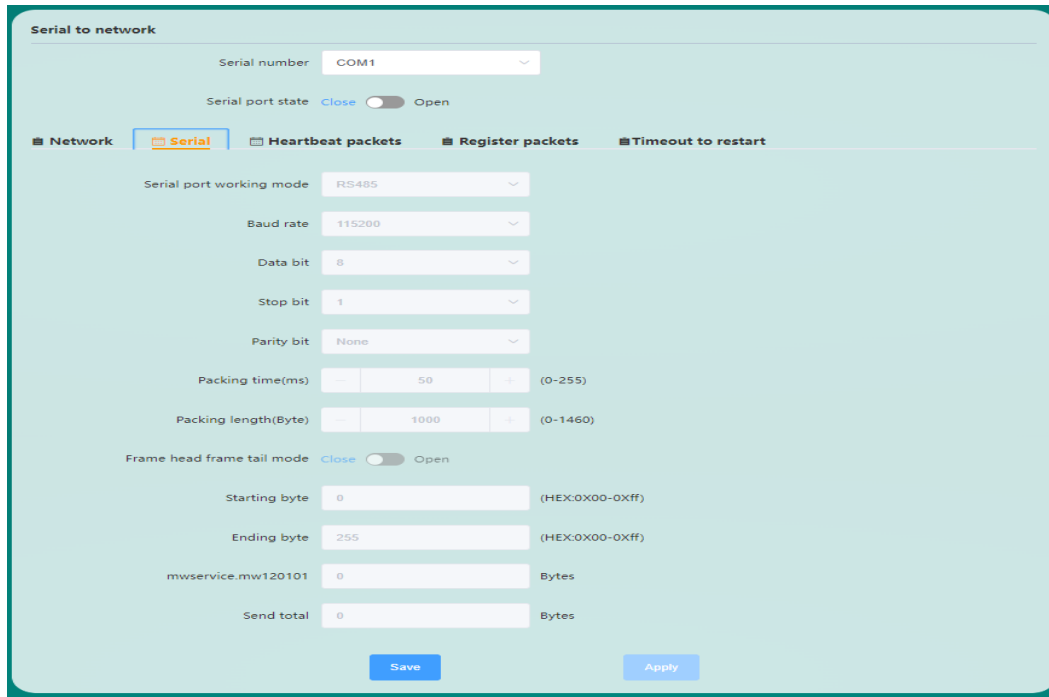


Figure 56 Serial port parameter configuration page

- **Baud rate:** The baud rate of serial communication, the unit is bps.
- **Data Bits:** Set the valid data bits in serial communication.
- **Stop bit:** Set the stop bit length during serial communication.
- **Check digit:** There are three check modes to choose from, including no check, odd check and even check.
- **Packing time:** When the time interval between the serial port of the device receiving adjacent data is greater than the set value, it is considered that one frame is over, and the data of this frame is packaged and sent to the network. The unit is ms.
- **Packing length:** During the packing time, when the length of the data received by the serial port of the device is greater than the set packing length, the received data will be packed and sent to the network immediately. The unit is bytes.

The heartbeat packet refers to a custom command word that periodically informs the other party of their own status between the client and the server, and is sent at a certain time interval, as shown in Figure 57.

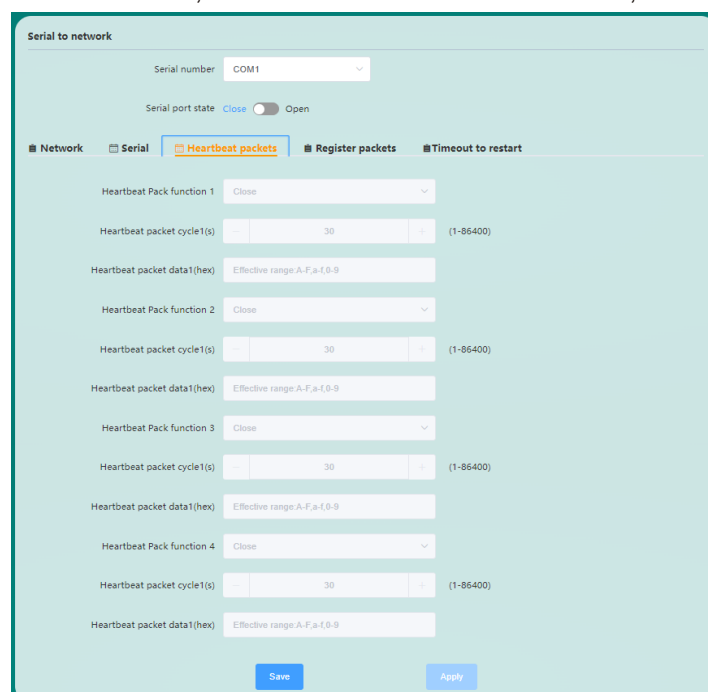


Figure 57 Heartbeat packet configuration page

- **On:** Status of heartbeat packets.
- **Sending method:** Including sending heartbeat to serial terminal and sending heartbeat to server.
- **Heartbeat packet cycle:** The time interval that the module sends heartbeat packet data to the serial terminal or server.
- **Heartbeat packet data:** The content of the data sent by the module to the serial terminal or server (currently supports hexadecimal format). Take the module working in TCP Client mode as an example, the remote address is set to the IP of the PC, and the port number is 20225 by default. Then open the heartbeat packet, select the sending method as "Send heartbeat to the server", set the heartbeat packet period to 5 seconds, and set the heartbeat packet data to hexadecimal 55aa. Then set up a TCP Server on the PC to view the data received by the server, as shown in Figure 58.

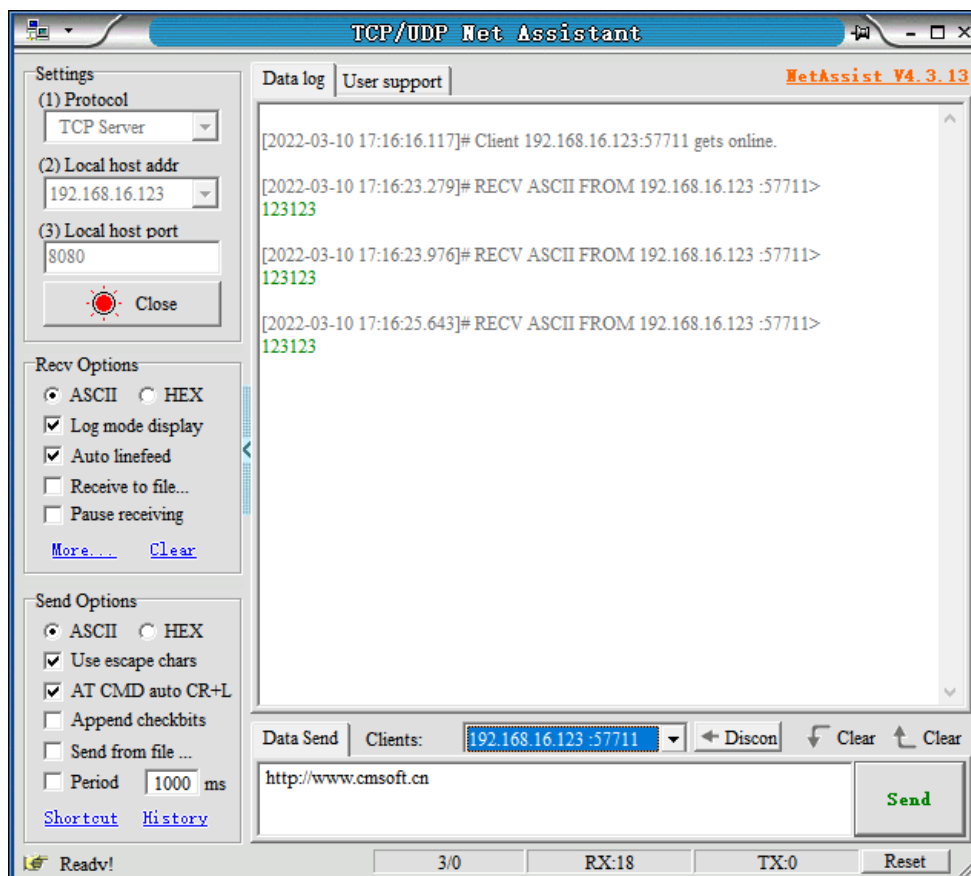


Figure 58 TCP Server receives heartbeat data

The registration package is used to allow the server to identify the data source device, or as a password to obtain server function authorization, as shown in Figure 59.

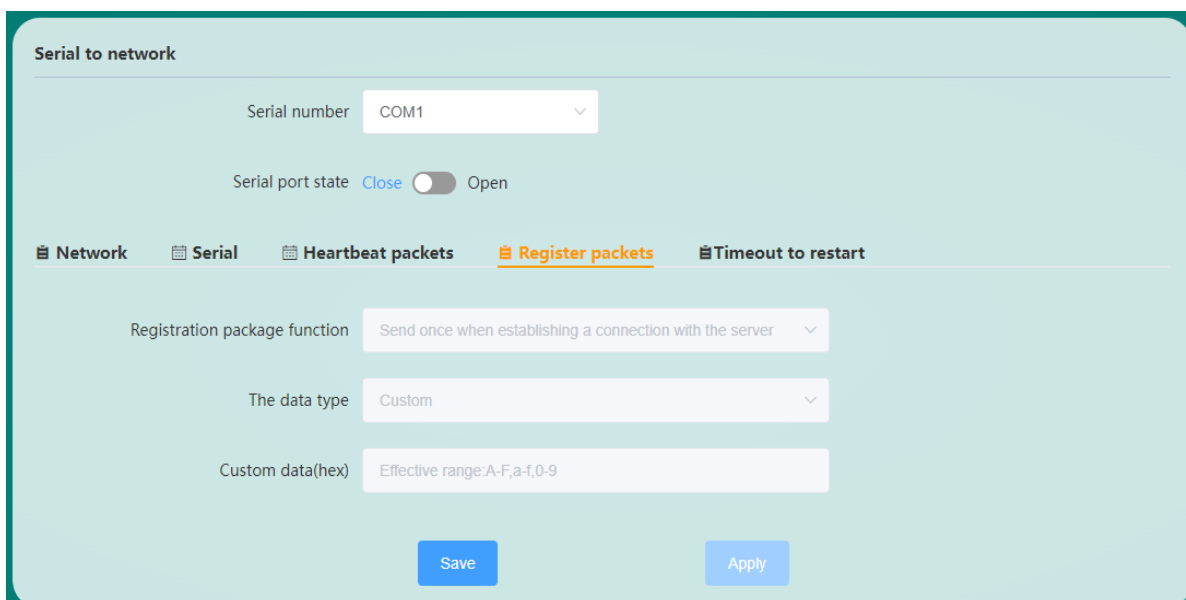


Figure 59 Registration package configuration page

- **On:** The status of the registration package.
- **Sending method:** There are two ways to send data in the registration package: send it once when establishing a connection with the server, and add a registration package before each frame of data.
- **Data type:** There are three types of data types: IMEI, ICCID and custom.
- **IMEI:** The unique identification code of the Internet access router in the router device. It is suitable for applications based on device identification and has nothing to do with the SIM card installed in it.
- **ICCID:** The unique identification code of the SIM card, which is suitable for applications based on SIM card identification.
- **Custom:** You can enter the data content to be sent (currently supports hexadecimal data format), as shown in Figure 60.

The screenshot displays a configuration window titled "Serial to network". At the top, there is a "Serial number" dropdown menu set to "COM1" and a "Serial port state" toggle switch currently in the "Close" position. Below this is a horizontal menu with five items: "Network", "Serial", "Heartbeat packets", "Register packets", and "Timeout to restart", with the last item highlighted in orange. Under the "Timeout to restart" section, there are two input fields: "Network restarted without data timeout" and "Serial port reboot without data timeout", both containing the value "3600". To the right of each input field is a range "(0,60-65535)". At the bottom of the window are two buttons: "Save" and "Apply".

Figure 60 Registration package custom data

3.2 Dynamic DNS

Dynamic DNS configuration parameters are shown in Figure 61.

Figure 61 Dynamic DNS settings

- **Enable:** Enable or disable DDNS function, DDNS is disabled by default.
- **Effective interface:** Select the corresponding WAN port as needed, such as wan (wired network port), g4wan (4G/5G WAN port).
- **Service Provider:** DDNS server address, the above picture takes peanut shell as an example, fill in oray.com. You can also fill in the customized service provider, select the last item of customization, fill in the customized DDNS and fill in the updated URL address.
- **Updated URL:** When the service provider selects custom, fill in the custom DDNS URL address here.
- **Host Name:** Fill in the applied domain name.
- **Username:** The account name of the registered DDNS service provider.
- **Password:** The password of the registered DDNS service provider.
- **IP address source:** The source of the IP address to be mapped, including interface, script, network, URL, and the default selection is network.
- **Network:** When the IP address source selects the network, here select the network interface name corresponding to the IP address, such as wan.
- **Time unit:** The time unit for detecting IP changes, including hours, minutes, and seconds.
- **Interval for checking IP changes:** The IP pointed to by the domain name may change frequently, and the smaller the value, the more frequent the detection.
- **Force update time unit:** Including minutes, hours and days.
- **Force Update Interval:** Force update time interval.

The dynamic DNS function needs the support of the public network IP. If the network where the router is located is not assigned an independent public network IP, the dynamic DNS function cannot be used.

3.3 VPN

3.3.1 VPN Overview

VPN (Virtual Private Network, virtual private network) is a private network established on a public network, and the private network has no actual physical lines, so it becomes a virtual private network. VPN is divided into client (Client) and server (Server) two ways. In terms of protocols, it is divided into PPTP, L2TP, IPSec, OPENVPN, GRE, SSTP, etc. The principles of creating VPNs for these protocols are described as follows:

PPTP: It is a point-to-point tunneling protocol. It uses a TCP (port 1723) connection to maintain the tunnel, and uses the general routing encapsulation (GRE) technology to encapsulate the data into PPP data frames for transmission through the tunnel. Payload data is encrypted or compressed.

L2TP: L2TP (Layer 2 Tunneling Protocol, Layer 2 Tunneling Protocol) is a Layer 2 VPN tunneling protocol that uses PPP (Point to Point Protocol, Point to Point Protocol) for data encapsulation, similar to PPTP, and adds extra headers to the data .

IPSEC: IPsec (IP Security, IP Security) is a collection of services and protocols that protect the security of end-to-end communications and prevent network attacks in IP networks. It provides a complete set of architecture for network data security on the application and IP layer, including network authentication protocols AH, ESP, IKE and some algorithms for network authentication and encryption. The AH protocol and the ESP protocol are used to provide security services, and the IKE protocol is used for key exchange.

OPENVPN: is an application layer VPN implementation based on the Openssl library. It supports certificatebased two-way authentication, that is, the client needs to authenticate the server, and the server also needs to authenticate the client.

GRE: GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) protocol is to encapsulate the datagrams of some network layer protocols (such as IP and IPX), so that these encapsulated datagrams can be used in another network layer protocol (such as IP) in transmission. GRE adopts the technology of Tunnel, which is the third layer tunneling protocol of VPN.

SSTP: Also known as Secure Socket Tunneling Protocol, is a protocol applied to the Internet that creates a VPN tunnel over HTTPS. SSTP is only for remote access and cannot support site-to-site VPN tunnels.

3.3.2 VPN Client

➤ PPTP client

A point-to-point tunneling protocol, which uses a TCP port connection to maintain the tunnel, and uses the general routing subassembly technology to encapsulate the data into PPP data frames for transmission through the tunnel, and encrypt or compress the payload data. Create a new interface for the PPTP client as shown in Figure 62.

Figure 62 Create PPTP client page

- **The name of the new interface:** 1-63 characters in length, can be numbers, letters or _.
- **Protocol of the new interface:** Create a PPTP client. The PPTP protocol must be selected here.
- **VPN Server:** Set the IP address or domain name of the PPTP server.
- **PAP/CHAP username:** Set the username for PPTP server login authentication.
- **PAP/CHAP password:** Set the password for PPTP server login authentication.

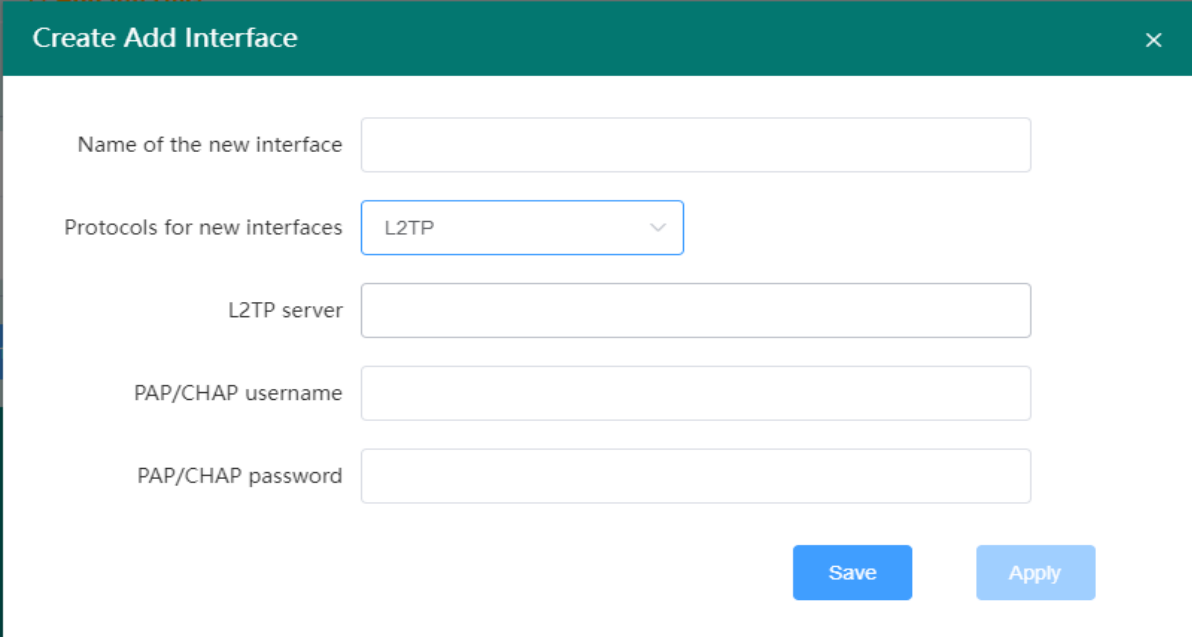
The PPTP advanced setting parameters are shown in Figure 63.

Figure 63 PPTP advanced settings page

- **Set MTU:** Set the MTU of the PPTP channel, the default is 1500.
- **Set Default Route:** Whether to set the system default route on the PPTP client network interface, it is not set by default.
- **Use DNS negotiated by server:** Whether to use the DNS server advertised by the PPTP server, which is used by default. If unchecked, DNS server and alternate DNS server can be set manually.
- **DNS server:** If the DNS negotiated by the server is not used, the DNS server address can be set here.
- **Alternate DNS server:** If the DNS negotiated by the server is not used, the alternate DNS server address can be set here.

➤ L2TP client

The L2TP protocol is a Layer 2 tunneling protocol, similar to the PPTP protocol. Create an L2TP client as shown in Figure 64.



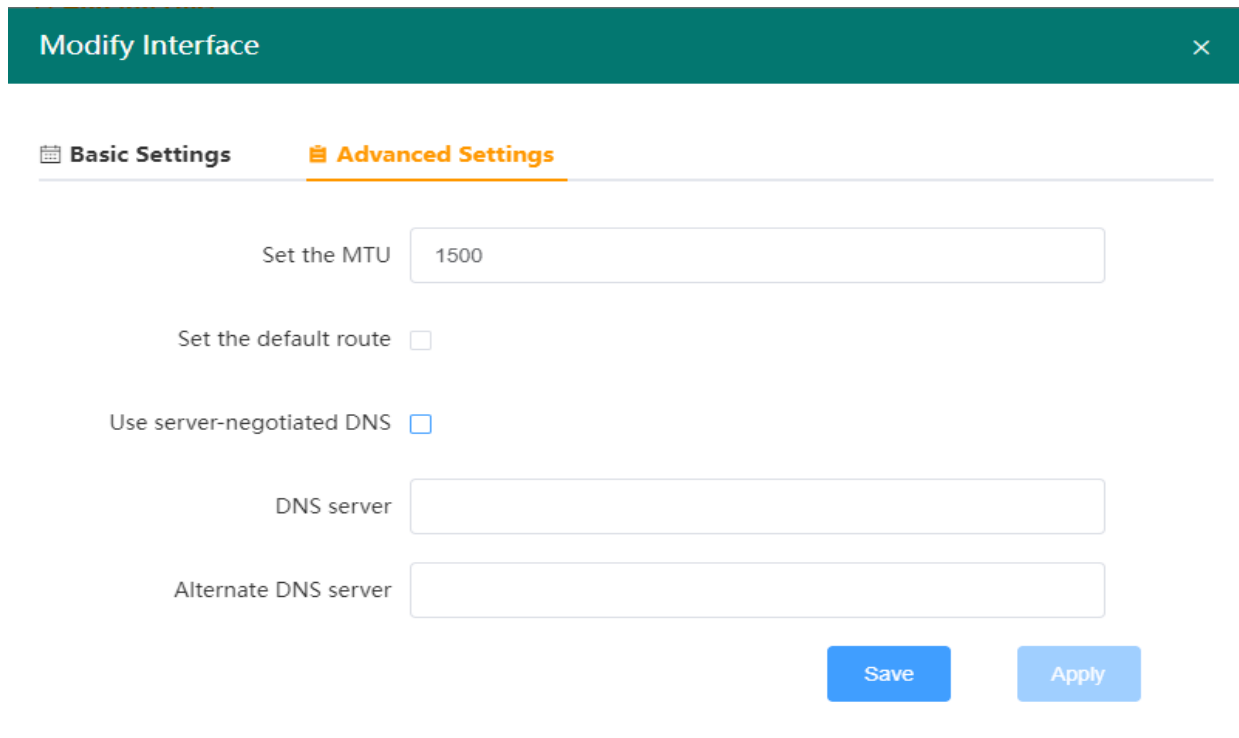
The screenshot shows a dialog box titled "Create Add Interface" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name of the new interface:** A text input field.
- Protocols for new interfaces:** A dropdown menu with "L2TP" selected.
- L2TP server:** A text input field.
- PAP/CHAP username:** A text input field.
- PAP/CHAP password:** A text input field.
- Buttons:** "Save" and "Apply" buttons at the bottom right.

Figure 64 Add L2TP client interface page

- **The name of the new interface:** 1-63 characters in length, can be numbers, letters or _.
- **Protocol for the new interface:** Create an L2TP client. The L2TP protocol must be selected here.
- **L2TP server:** Set the IP address or domain name of the L2TP server.
- **PAP/CHAP username:** Set the username for L2TP server login authentication.
- **PAP/CHAP password:** Set the password for L2TP server login authentication.

The L2TP advanced setting parameters are shown in Figure 65.



The screenshot shows a web interface titled "Modify Interface" with a close button (X) in the top right corner. Below the title bar, there are two tabs: "Basic Settings" and "Advanced Settings". The "Advanced Settings" tab is selected and highlighted in orange. The settings are as follows:

- "Set the MTU" is a text input field containing the value "1500".
- "Set the default route" is a checkbox that is unchecked.
- "Use server-negotiated DNS" is a checkbox that is unchecked.
- "DNS server" is a text input field.
- "Alternate DNS server" is a text input field.

At the bottom right of the form, there are two buttons: "Save" and "Apply".

Figure 65 L2TP advanced settings page

- **Set MTU:** Set the MTU of the L2TP channel, the default is 1500.
- **Set Default Route:** Whether to set the system default route on the network interface of L2TP client, it is not set by default.
- **Use DNS negotiated by server:** Whether to use the DNS server advertised by the L2TP server, which is used by default. If unchecked, DNS server and alternate DNS server can be set manually.
- **DNS server:** If the DNS negotiated by the server is not used, the DNS server address can be set here.
- **Alternate DNS server:** If the DNS negotiated by the server is not used, the alternate DNS server address can be set here.

➤ GRE client

The GRE protocol encapsulates some network layer protocols, so that these encapsulated datagrams can be transmitted in another network protocol. It is the third layer tunneling protocol in VPN. Create a GRE client interface as shown in Figure 66.

The screenshot shows a dialog box titled "Create Add Interface" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name of the new interface:** A text input field.
- Protocols for new interfaces:** A dropdown menu currently showing "GRE".
- Remote address:** A text input field.
- Local address:** A text input field.
- Distal tunnel address:** A text input field.
- Local tunnel address:** A text input field.
- Buttons:** "Save" and "Apply" buttons at the bottom right.

Figure 66 GRE protocol

- **The name of the new interface:** 1-63 characters in length, can be numbers, letters or _.
- **Protocol for the new interface:** Create a GRE client The GRE protocol must be selected here.
- **Remote address:** IP address of the WAN port of the peer GRE.
- **Local address:** The address of the local wan port (wired wan port) and g4wan port (4G/5G wan port).
- **Remote Tunnel Address:** The IP address of the peer GRE tunnel.
- **Local Tunnel Address:** The local GRE tunnel IP address.

The GRE advanced setting parameters are shown in Figure 67.

The screenshot shows a dialog box titled "Modify Interface" with a close button (X) in the top right corner. It features two tabs: "Basic Settings" and "Advanced Settings", with "Advanced Settings" currently selected. The advanced settings section includes:

- TTL Settings:** A text input field containing the value "255".
- Set the MTU:** A text input field containing the value "1500".
- Buttons:** "Save" and "Apply" buttons at the bottom right.

Figure 67 GRE Advanced Settings Page

- **TTL setting:** Set the TTL of the GRE channel, the default is 255.
- **Set MTU:** Set the MTU of the GRE channel, the default is 1500.

➤ **OPENVPN client**

OPENVPN is a two-way authentication that supports certificates. The client needs to authenticate the server, and the server also needs to authenticate the client. OPENVPN includes two protocols, TUN and TAP. TUN is in routing mode, as shown in Figure 68, and TAP is in bridge mode, as shown in Figure 69.

Figure 68 TUN protocol

Figure 69 TAP protocol

- The name of the new interface: 1-63 characters in length, can be numbers, letters or _.
- Protocol for new interface: Create OPENVPN client can choose TUN (router mode) or TAP (bridge mode).

- **TCP/UDP communication:** The protocol used by the channel, you can choose UDP or TCP, which must be consistent with the server channel protocol.
- **Remote Address:** IP/domain name of the GRE server.
- **Remote Port:** The listening port of the GRE server.

The OPENVPN advanced setting parameters are shown in Figure 70.

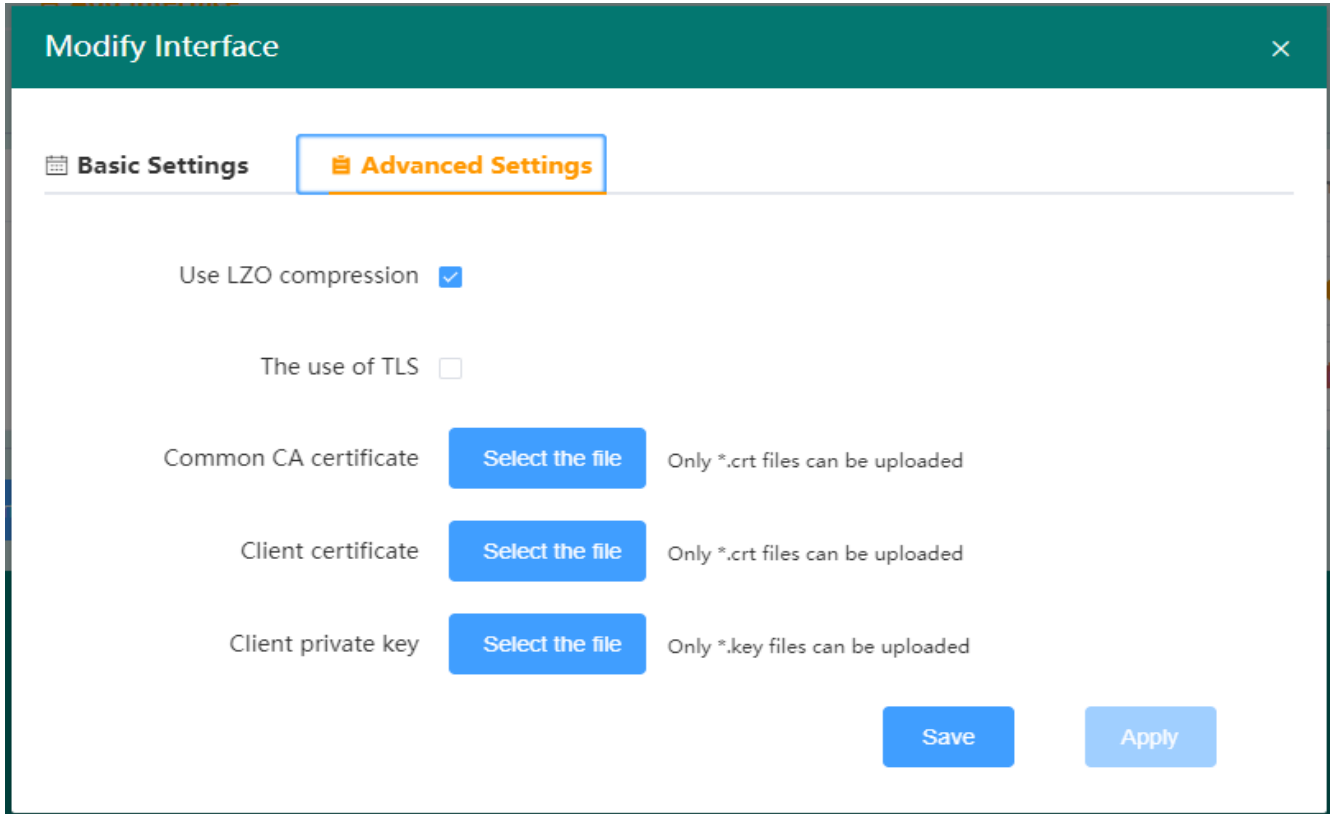


Figure 70 Advanced settings page

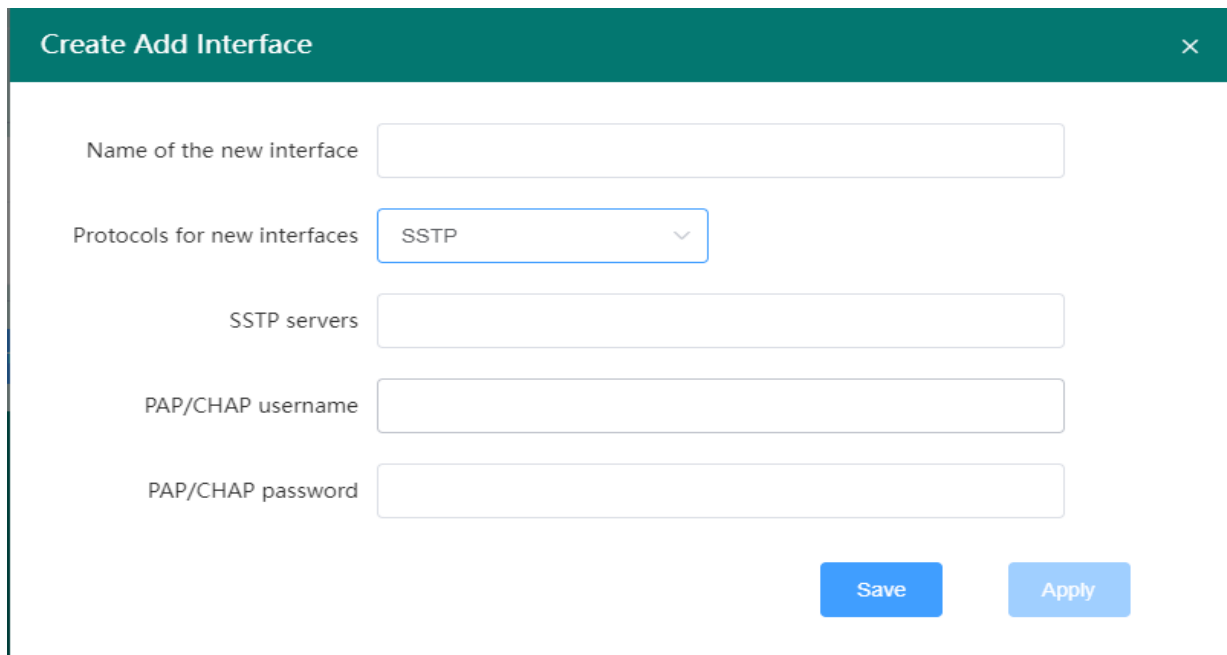
- **Use LZO compression:** Enable or disable the use of LZO compression for transmitted data.
- **Use TLS:** Whether to enable the method with TLS.
- **TLS authentication key:** The authentication key of the secure transport layer.
- **Public CA certificate:** The CA certificate common to the server and client.
- **Client Certificate:** Client certificate.
- **Client Private Key:** Client Secret.



1. After the OPENVPN client interface is created, it cannot connect to the server immediately. You need to click the Modify button in the corresponding network interface to enter the advanced setting interface to upload the relevant certificate and private key, save and apply it to connect normally.
2. Before the OPENVPN client connects to the server, the public CA certificate, client certificate, client private key, and TLS authentication key need to be provided by the OPENVPN server.

➤ SSTP client

The SSTP protocol is a protocol applied to the Internet. It can create a VPN tunnel transmitted over HTTPS. It is only suitable for remote access and cannot support VPN tunnels between sites, as shown in Figure 71.



The screenshot shows a configuration window titled "Create Add Interface" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Name of the new interface:** A text input field.
- Protocols for new interfaces:** A dropdown menu with "SSTP" selected.
- SSTP servers:** A text input field.
- PAP/CHAP username:** A text input field.
- PAP/CHAP password:** A text input field.
- Buttons:** "Save" and "Apply" buttons located at the bottom right.

Figure 71 SSTP protocol

- **The name of the new interface:** 1-63 characters in length, can be numbers, letters or _.
- **Protocol for the new interface:** Create an SSTP client The SSTP protocol must be selected here.
- **SSTP server:** Set the IP address or domain name of the SSTP server.
- **PAP/CHAP username:** Set the username for SSTP server login authentication.
- **PAP/CHAP password:** Set the password for SSTP server login authentication.

3.3.3 VPN server

The VPN server supports three protocols: PPTP server, L2TP server, and IPsec server. The configuration methods are as follows.

➤ PPTP server

The PPTP server includes two parts: PPTP VPN server and user management, as shown in Figure 72.

PPTP VPNserver

Enable VPN server Close Open

PPTP server IP

Client IP address range -

Client DNS server

Alternate DNS server

User management

Number	Enable	Username	Password	IP address	operation
1	<input checked="" type="checkbox"/>	admin	admin	192.168.0.24	Edit Delete

Add Save Apply

Figure 72 PPTP server

- **Enable VPN Server:** Enable or disable the PPTP VPN server, the PPTP VPN server is disabled by default.
- **PPTP server IP:** The virtual IP address of the VPN server, which cannot be located in the same network segment as the LAN port IP.
- **Client IP address range:** The IP address range assigned to the client must be in the same network segment as the server IP.
- **Client DNS Server:** Assign the preferred DNS server address to the client, such as 8.8.8.8.
- **Alternate DNS Server:** Assign an alternate DNS server address to the client.
- **Enable:** Set whether the login authentication user name and password in the corresponding list are enabled.
- **Username:** Set the username for PPTP client login authentication.
- **Password:** Set the password for PPTP client login authentication.
- **IP Address:** The IP address assigned by the client. If no IP address is set by default, the client uses the IP address automatically assigned by the server. If you want to fix the VPN client IP, set it to an IP within the client IP address range.

➤ L2TP server

The L2TP server includes two parts, the L2TP VPN server and the user management, as shown in Figure 73.

L2TP VPN Server

Enable VPN server Close Open

L2TP Server IP

Client IP address range -

Client DNS server

Alternate DNS server

User management

Number	Enable	Username	Password	IP address	operation
1	<input checked="" type="checkbox"/>	admin	admin	192.168.10.21	<input style="margin-right: 5px;" type="button" value="Edit"/> <input style="margin-right: 5px;" type="button" value="Delete"/>

Figure 73 L2TP server

- **Enable VPN Server:** Enable or disable the L2TP VPN server.
- **L2TP server IP:** VPN server virtual IP address, which cannot be located in the same network segment as the LAN port IP.
- **Client IP address range:** The IP address range assigned to the client must be in the same network segment as the VPN server IP.
- **Client DNS Server:** Assign the preferred DNS server address to the client, such as 8.8.8.8.
- **Alternate DNS Server:** Assign an alternate DNS server address to the client.
- **Enable:** Set whether the login authentication user name and password in the corresponding list are enabled.
- **Username:** Set the user name for L2TP client login authentication.
- **Password:** Set the password for L2TP client login authentication.
- **IP Address:** The IP address assigned by the client. If no IP address is set, the client uses the IP address automatically assigned by the server. If you want to fix the VPN client IP, set it to an IP within the client IP address range.

➤ IPsec server

The IPsec server consists of three parts: basic settings, advanced settings, and connection logs. The basic settings are shown in Figure 74.

IPSec VPN Server

Basic Settings | Advanced Setting | Connection Log

Start VPN server Close Open

Connection name

Networking mode

Work Model

Local interface

Local subnet / (Example: 192.168.16.1/24)

Peer gateway

Peer subnet / (Example: 192.168.16.1/24)

Authentication method

Pre shared secret key

Save Apply

Figure 74 Basic settings

- **Enable VPN Server:** Enable or disable IPsec VPN server, IPsec VPN server is disabled by default.
- **Connection Name:** Indicates the name of the connection, with a length of 1 to 32 characters, and can be letters, numbers or _.
- **Networking mode:** There are two modes: site-to-site and PC-to-site.
- **Working mode: divided into two types:** VPN client and VPN server.
- **Local interface:** Specify the network interface used locally, you can choose wan (wired WAN port), g4wan (4G/5G WAN port).
- **Local network:** IPsec local protection subnet and subnet mask, if the networking mode is PC-to-site and the working mode is VPN client, you do not need to fill in the local network.
- **Peer gateway:** IP or domain name of the IPsec peer gateway.
- **Peer network:** The subnet protected by the IPsec peer gateway and the subnet mask.
- **Authentication method:** The authentication method of pre-shared key (Secret) is currently supported.
- **Pre-shared key:** Set the pre-shared key for IPsec encryption.

IPSec VPN advanced settings are shown in Figure 75.

The screenshot shows the 'Advanced Setting' tab for IPSec VPN configuration. It is organized into two stages:

- Stage 1 setup:**
 - IKE Version:
 - Negotiation model:
 - Local identifier:
 - Peer identifier:
 - IKE encryption: Encryption: ; Verification: ; Secret key group:
 - IKE life cycle(s): (1~86400)
 - Enable DPD detection: Close Open
- Stage 2 setup:**
 - Encapsulation mode:
 - ESP encryption: Encryption: ; Verification:
 - ESP life cycle(s): (1~86400)

Buttons for 'Save' and 'Apply' are located at the bottom of the form.

Figure 75 Advanced settings page

Phase 1 Set the relevant parameters of the first phase of IKEv1

- **Negotiation mode:** IKEv1 version supports two modes: main mode and aggressive mode. The default is to select main mode.
- **Local identifier:** The local identifier of the channel, which can be the local IP or local domain name. Note that @ should be added when setting the domain name, and it should be consistent with the peer identifier of the peer gateway.
- **Peer identifier:** The peer identifier of the channel, which can be the peer IP or peer domain name. Note that @ should be added when setting the domain name, and it should be consistent with the local identifier of the peer gateway.
- **IKE encryption:** The first phase includes three methods of encryption, verification and key group in the IKE phase.
- **IKE lifetime:** Set the lifetime of the IPSec session key in the first phase in IKE negotiation mode, the unit is s.
- **Enable DPD detection:** Whether to enable the DPD detection function, enabling this function will send DPD data packets regularly to quickly find out whether the peer is online.

Phase 2 Set the relevant parameters of the second phase of IKEv1

- **Encapsulation mode:** It is divided into tunnel mode and transmission mode. The default is tunnel mode. The encapsulation mode must be the same as that of the peer. Tunnel mode will add an additional IP header to the original IP packet, while transport mode will not. In terms of security, tunnel mode is superior to transport mode and is suitable for more general VPN applications.
- **ESP encryption:** It consists of two parts: encryption and verification. Select the corresponding encryption method and integrity scheme.

- ESP life cycle: set the ESP life cycle, the unit is s, the default value is 3600 seconds.

The connection log is mainly used to check whether the IPsec server is successfully connected, as shown in Figure 76.

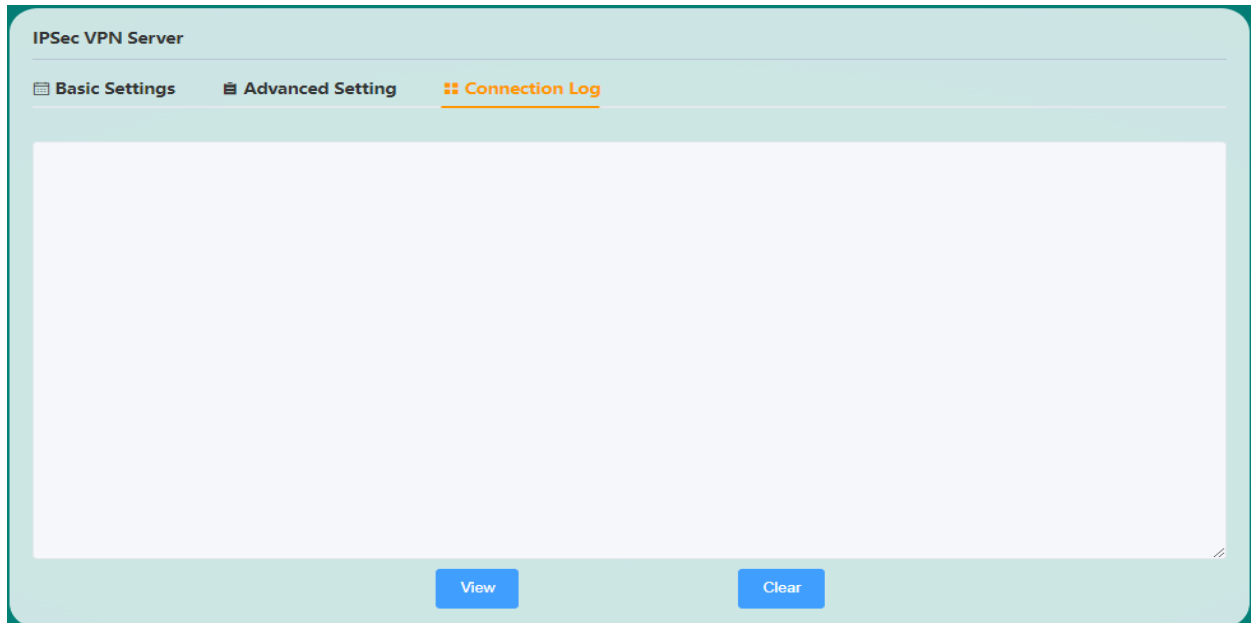


Figure 76 Connection log

3.4 SNMP Settings

SNMP (Simple Network Management Protocol, Simple Network Management Protocol) is a communication rule between management devices and managed devices in the network. It is used to manage network nodes (servers, workstations, routers, switches, and HUBS, etc.) in an IP network. Standard protocol, which is an application layer protocol. SNMP settings support two versions of SNMP v1 and SNMP v2c, and consist of three parts: Settings, Community, and Trap.

The SNMP settings page is shown in Figure 77.

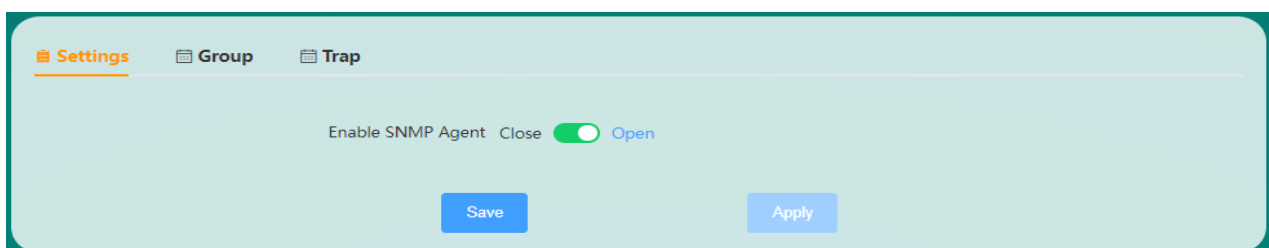


Figure 77 Settings page

- **Enable SNMP Agent:** Enable or disable the SNMP Agent function. By default, the SNMP Agent function is disabled.

The SNMP Community Settings page is shown in Figure 78.

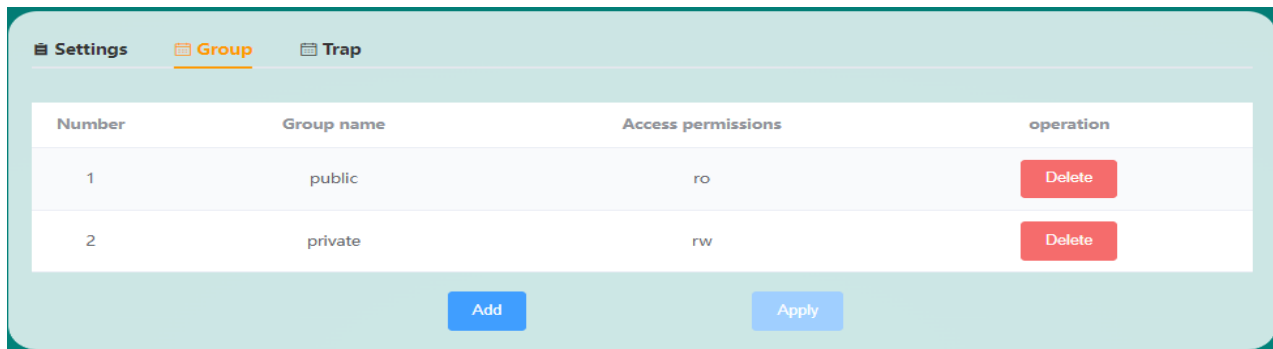


Figure 78 Group Settings Page

- **Community Name:** Set the name of the SNMP community, with a length of 1-63 letters or numbers.
- **Access permission:** Set the permission when NMS uses this group to access the Agent, there are two types: read-only (ro) and read-write (rw).

The SNMP Trap settings page is shown in Figure 79.

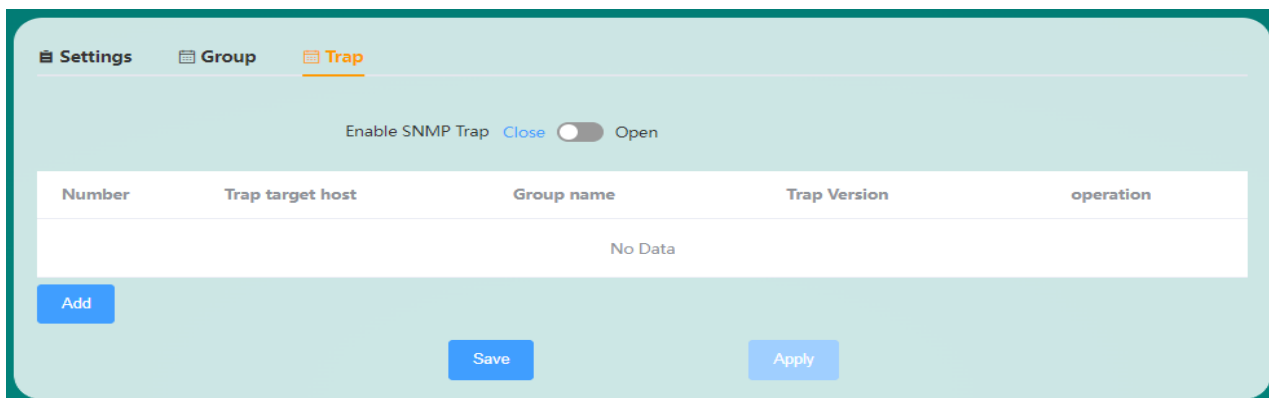


Figure 79 Trap setting page

- **Enable SNMP Trap:** Enable or disable the SNMP Trap function. The SNMP Trap function is disabled by default. Before enabling the SNMP Trap function, SNMPAgent must be enabled.
- **Trap target host:** Set the IP address of the Trap target host.
- **Community Name:** Set the community name.
- **Trap version:** Set the version sent by SNMP Trap, which can be SNMP v1(v1) or SNMP v2c(v2c).

After the SNMP settings are completed, click Save to apply, and then you can manage the router through NMS.

3.5 LLDP Settings

LLDP (Link Layer Discovery Protocol, Link Layer Discovery Protocol), it provides a standard link layer discovery method, which can organize the main capabilities, management addresses, device IDs, interface IDs and other information of the local device into different TLV (Type/Length/Value, type/length/value), and encapsulate it in LLDPDU (Link Layer Discovery Protocol Data Unit, Link Layer Discovery Protocol Data Unit) and publish it to its directly connected neighbors or network management system, convenient The network management system queries and judges the communication status of the link.

The LLDP settings page is shown in Figure 80.

LLDP Basic Settings

Enable LLDP [Close](#) Open

Sending interval(s) (1~3600)

TTL multiplier (1~100)

LLDP listens on the interface loopback lan wan wan6 g4wan g4wan1 wwan

LLDP neighbor information

No.	Local port	Neighborhood equipment identification	Neighbor port identification	Neighbor system name	LLDP manages addresses
No Data					

[Save](#) [Apply](#)

Figure 80 LLDP Settings Page

- **Enable LLDP:** Enable or disable the LLDP function. The LLDP function is disabled by default.
- **Sending cycle (s):** The sending cycle of LLDPDU data packets, in seconds.
- **TTL multiplier:** TTL is the aging expiration time. The LLDP receiver will set the aging time of neighbor information on the local device according to the TTL value carried in the router LLDPDU. If the received TTL value is 0, the neighbor device information will be immediately aged out. The product value of the TTL multiplier and the sending interval is the aging time of LLDP (the TTL multiplier is 4 and the sending interval is 30 seconds, so the TTL value is $4 \times 30 = 120$ seconds).
- **LLDP monitor interface:** Set the monitor network port for LLDPDU data packets, and monitor LLDP data packets on the LAN port by default.

The LLDP neighbor information list displays the LLDP neighbor device information discovered by the router in real time.