

maiwe

4G Router

User Manual

➤ **MIR652R-W**

Version: V1.0

Please read this user manual carefully before using this product

Copyright Statement

Copyright © Wuhan Maiwe Communications Co., LTD.

MAIWE[®] It is the special brand trademark of Wuhan Maiwe Communications Co., LTD.

Microsoft and Windows are registered trademarks of Microsoft Corp.

All relevant trademarks mentioned in this operating manual are separately owned by the relevant manufacturer.

Explain

This user operator manual is applicable to the MIR652R-W 4G router.

Before using this manual, please read the following disclaimer statement carefully. Only if agreeing to using the disclaimer below can use the products described in this manual.

Disclaimer

Any information provided in this manual by our company does not represent the corresponding authorization for this information.

The company strives to ensure that the information provided in this manual is accurate and relevant. However, our company does not assume any responsibility or any consequential liability for the use of this information. There may be technical or printing errors in the product and the user manual.

The company reserves the right to change all or part of the content of this user manual without prior notice.

Version	Date	Reasons
V1.0	2023.08	Create document

Safety Instructions:

This product has reliable performance within its designed scope of use. However, it is essential to avoid any human-caused damage or destruction to the device.

- Read the manual carefully and keep it for future reference.
- Do not place the device near water sources or in humid areas.
- Do not place anything on the power cord; keep it out of reach.
- To prevent fire hazards, do not tie or wrap the cables.
- The power plug and other device connectors should be firmly connected; please check regularly.
- Ensure the device is clean; wipe with a soft cotton cloth if necessary.
- Do not attempt to repair the device yourself unless explicitly instructed in the manual.

In the following situations, please disconnect the power immediately and contact our company:

- If the device gets wet.
- If the device is damaged due to a fall.
- If the device malfunctions or shows completely altered performance.
- If the device emits an odor, smoke, or noise.



Note: Essential explanatory information during the use of this device.



Caution: Matters that require special attention during the use of this device.

Contents

1	Product Introduction	1
1.1	Product Introduction	1
1.2	Product Features	1
1.3	Product Display	3
1.4	Specifications	3
1.5	Interfaces and Indicator Lights	6
1.5.1	Power input interface and RS232/485 interface	7
1.5.2	Restart / restore the factory setting button	7
1.5.3	WAN Interface	7
1.5.4	LAN Interface	8
1.5.5	Status Indicator	8
1.5.6	Antenna	9
1.5.7	SIM card slot and its button	9
1.6	Installation Size	9
2	Quick Internet Connection	10
2.1	Environmental preparation	10
2.2	Network Connection	10
2.3	Router indicator	11
2.4	WEB login and networking test	12
3	WEB Basic Function Configuration	13
3.1	Log in to WEB	13
3.2	Introduction to the New User Guide Page	15
3.2.1	WAN Settings	15
3.2.2	4G Settings	17
3.2.3	Wireless Settings	18
3.3	Main Page Introduction	19
3.3.1	Function Menu	19
3.4	Status	21
3.4.1	Running state	21
3.4.2	network status	22
3.4.3	local address	22
3.4.4	Traffic Statistics	23
3.5	Network	24
3.5.1	Interface	24
3.5.2	WAN port settings	25
3.5.3	LAN port settings	27
3.5.4	4G Settings	28
3.5.5	Wireless settings	30
3.5.6	Access Device	32

3.5.7	Static routing	33
3.5.8	Link check	36
3.5.9	Network Diagnosis	37
3.6	Firewall	38
3.6.1	Basic Settings	38
3.6.2	Port forwarding	39
3.6.3	Access control	40
3.6.4	Custom rules	43
3.6.5	DMZ	43
3.6.6	UPnP	44
3.6.7	Network speed control	45
3.6.8	QoS	46
3.7	System	47
3.7.1	System Property	47
3.7.2	Administration Authority	48
3.7.3	Reboot	48
3.7.4	Backup and upgrade	49
3.7.5	Scheduled task	51
3.7.6	System log	51
4	WEB Advanced Function Configuration	54
4.1	Serial port to network	54
4.1.1	Network	54
4.1.2	Serial port	57
4.1.3	Heartbeat packet	59
4.1.4	Registration package	60
4.1.5	Timeout restart	61
4.1.6	Modbus function	61
4.1.6.1	ModbusMaster	61
4.1.6.2	Slave mode (Modbus Slave)	65
4.1.6.3	Slave Address Mapping	69
4.1.6.4	Modbus Slave Read Ahead	70
4.1.6.5	Modbus Feature Function	71
4.1.7	RealCOM function	73
4.1.8	Httpd Client function	75
4.1.9	WebSocket Client function	77
4.1.10	MQTT function	79
4.1.11	JSON function	82
4.2	Intranet Through Of Peanut Shell	88
4.3	Dynamic DNS	93
4.4	VPN	94
4.4.1	VPN	94
4.4.2	VPN client	95
4.4.2.1	PPTP client	95
4.4.2.2	L2TP client	97

4.4.2.3	GRE Client	99
4.4.2.4	OPENVPN client	101
4.4.3	VPN server	104
4.4.3.1	PPTP server	104
4.4.3.2	L2TP server	105
4.4.3.3	IPSec server	106
4.5	SNMP settings	109
4.6	LLDP settings	111
4.7	Cloud Service	112
5	Maintenance and Service	114
5.1	Internet Service	114
5.2	Technical Support Phone Service	114
5.3	Product Repair or Replacement	114
5.4	Contact Information	114

1 Product Introduction

1.1 Product Introduction

MIR652R-W is a 2-port 100M card-rail 4G wireless industrial router specially designed and developed for industrial communication network applications. It supports multi-network online such as LAN, WAN, WLAN, 4G LTE, etc., intelligent Switch multi-network backup, which can realize serial port, wireless, and wired terminal equipment networking. This product provides 1 100M WAN port, 1 100M LAN port, 1 RS232/485 serial port, 1 4G antenna interface and 2 2.4G antenna interfaces, etc., and supports 1 DC 9~36V power input, using standard DIN rail installation, to meet the needs of various network sites.

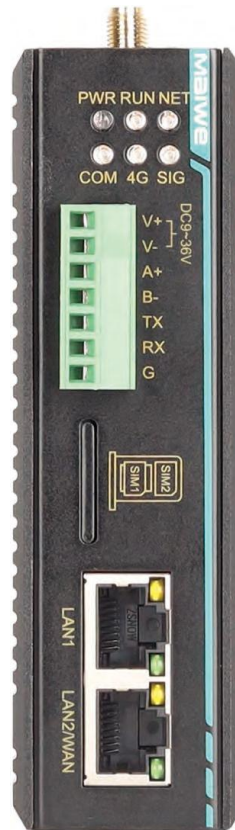
The product supports WEB configuration of various network management functions, such as PPPoE dial-up, DHCP server, 4G network, wireless settings, IP/MAC binding, static routing, firewall, VPN, serial port to network, network diagnosis, SNMP, LLDP, cloud services, etc.; the system provides user management with different permissions, supports local/remote log management, supports scheduled restart, configuration backup and recovery, firmware upgrade, and restore factory settings. Support one-key restart or restore factory settings. The hardware adopts high-standard industrial protection design, selected industrial-grade components, and uses high-strength aluminum alloy shell, which is durable; low power consumption, wide temperature design, fanless shell heat dissipation, and supports -40°C ~+75°C working temperature, passed strict safety regulations and EMC tests, to meet the harsh industrial environment application requirements. The products can be widely used in industrial automation, comprehensive energy, smart cities, smart transportation, smart mines, smart factories and other fields.

1.2 Product Features

- Support 4G cellular wireless network, Wi-Fi wireless network and WAN port wired network, support multi-network backup
- The WAN port supports DHCP protocol, static address, PPPoE dial-up, etc. to connect to the external network, or as a LAN port to connect to the intranet
- The LAN port supports a DHCP server, which centrally manages and configures user IP addresses dynamically
- Support 4G cellular network, compatible with 2G/3G, support three networks, dual card single standby, APN
- Support link check, periodically check 4G network link status, and perform link recovery
- Wi-Fi supports AP, Client or AP+Client and other modes, which can realize wireless terminal access, wireless network access or bridging

- Support IPv4/IPv6 Ping, IPv4/IPv6 Traceroute, Nslookup, and packet capture for network diagnosis or fault analysis
- The firewall supports SYN-flood defense, port mapping, IP/MAC/DNS address filtering, iptables command custom rules, DMZ isolated area, UPnP, IP/MAC speed limit, QoS limit upload/download Speed and other functions
- Support NTP client and server functions, which can perform clock synchronization or provide clock source
- Support ordinary users and administrator users, user rights hierarchical management
- Support online system management such as scheduled restart, restore factory settings, configuration file backup and batch restore, firmware upgrade, etc.
- Log information records multiple levels of kernel, application, and network information, and supports local download, scheduled storage, and remote monitoring.
- Serial ports support UDP, TCP Client/Server, UDP Multicast, Modbus RTU Master/Slave, Modbus ASCII Master/Slave, Realcom MCP/CCP/MW, Pair Connection Master/Slave 、 Httpd Client, WebSocket Client, MQTT and other serial port conversion modes, realize serial port to Ethernet or Modbus RTU/ASCII protocol
- Support intranet penetration of peanut shells, and use peanut shell dynamic domain name to remotely log in and manage devices
- Support VPN client and server to build a private network, the client supports PPTP, L2TP, IPSec, OPENVPN, GRE and other tunneling protocols, and the server supports PPTP, L2TP and IPSec and other protocols
- Support SNMPv1/v2c, information query, information modification and troubleshooting can be performed through MIB, and centralized management can be realized
- Support LLDP, obtain LLDP neighbor device information, monitor link status, facilitate topology management and fault location
- Support Maiwei cloud platform management to realize remote management of equipment and monitoring of on-site network status

1.3 Product Display



1.4 Specifications

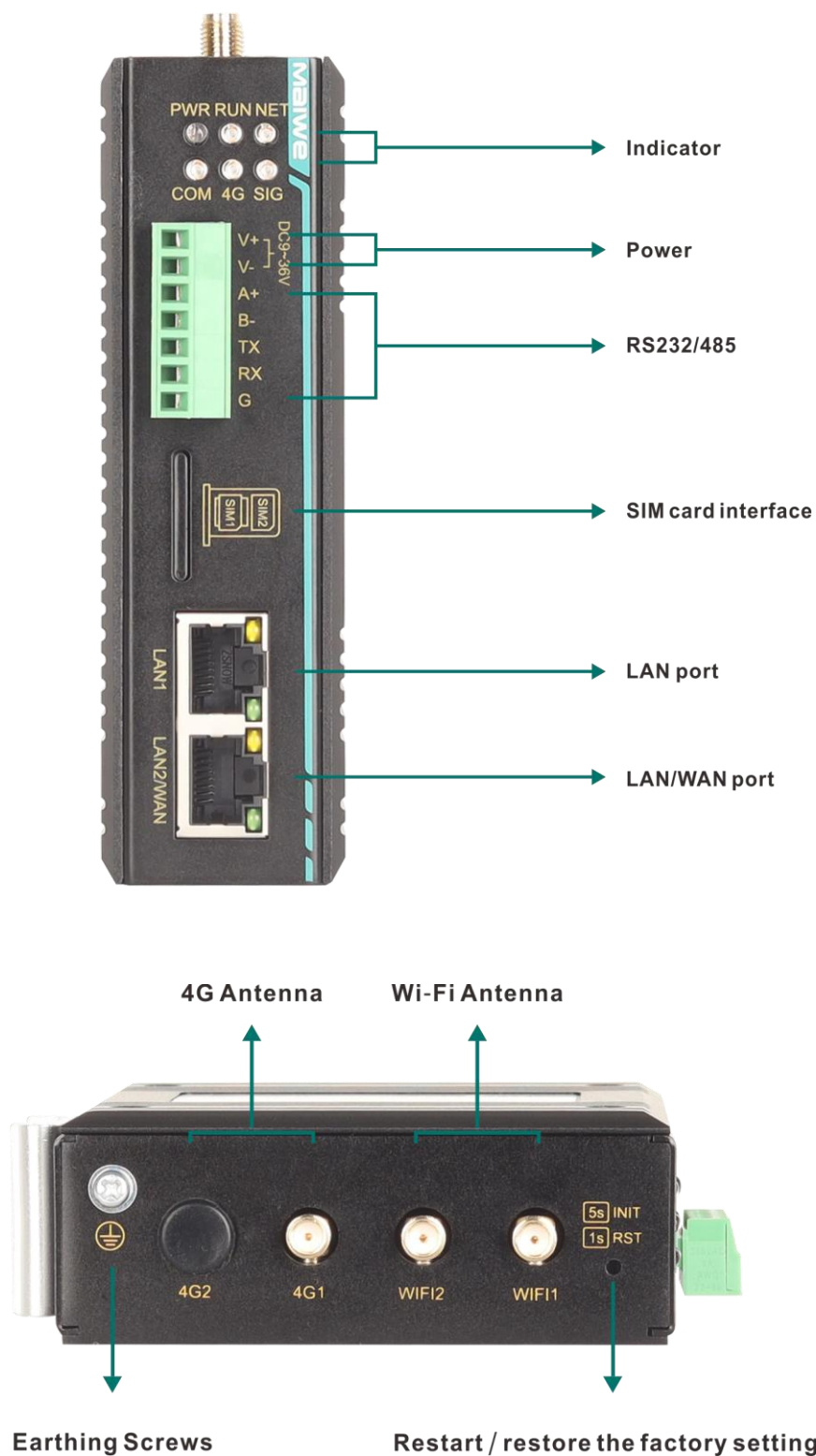
Table 1-1 MIR652R-W Performance Specification Table

Software function	
Network management function	• Support traffic statistics, running status, network status, local machine address and other status information • Support static address, DHCP, PPPoE external network connection, support WAN/LAN mode • Support DHCP server, IP/MAC binding • Support 4G network, dual card management, APN, link check • Support wireless AP mode, Client mode, AP+Client mode • Support static routing • Support serial port to network, peanut shell intranet penetration, dynamic DNS, SNMP, LLDP, cloud service • Support PPTP/L2TP/GRE/TUN/TAP protocol VPN client • Support PPTP/L2TP/IPsec protocol VPN server
firewall	• Support SYN-flood defense, IP dynamic masquerading, MSS clamping, inbound/outbound data control • Support WAN/LAN port TCP/UDP port mapping

	Support IP/MAC/domain name filtering, iptables, DMZ, UPnP, IP/MAC/QoS speed limit
system management	- Support IPv4/IPv6 Ping, IPv4/IPv6 Traceroute, Nslookup, capture network packets - Support time zone, NTP client/server, management port, Crontab, remote/local log - Support user rights management - Support online restart, scheduled restart, configuration backup/restore, flash firmware, restore factory settings
4G cellular network	LTE-FDD, LTE-TDD, WCDMA, GSM/EDGE
Network format	LTE-FDD: B1/B3/B5/B8 LTE-TDD: B34/B38/B39/B40/B41 WCDMA: B1/B5/B8 GSM/EDGE: B3/B8
Working frequency band	LTE-FDD: DL150Mbps/UL50Mbps LTE-TDD: DL130Mbps/UL30Mbps HSPA+: DL21Mbps/UL5.76Mbps WCDMA: DL384kbps/UL384kbps EDGE: DL236.8kbps/UL236.8kbps GRPS: DL85.6kbps/UL85.6kbps
Maximum transfer rate (theoretical value)	LTE-FDD: DL150Mbps/UL50Mbps LTE-TDD: DL130Mbps/UL30Mbps HSPA+: DL21Mbps/UL5.76Mbps WCDMA: DL384kbps/UL384kbps EDGE: DL236.8kbps/UL236.8kbps GRPS: DL85.6kbps/UL85.6kbps
Wi-Fi RF parameters	
Working frequency band	2.4GHz (2.412GHz~2.484GHz)
Maximum transfer rate (theoretical value)	300Mbps
Maximum transmit power	802.11b: 17dBm~19dBm@11Mbps 802.11g: 15dBm~18dBm@54Mbps 802.11n: 15dBm~18dBm@MCS7HT20/40
Receiving sensitivity	802.11b: -91.5dBm~-87.5dBm@11Mbps (PER<8%) 802.11g: -78dBm~-74dBm@54Mbps (PER<10%)
Interface specifications	
100M WAN	1-way 10/100Base-T(X) adaptive 100M RJ45 WAN port (supports LAN mode), supports full/half duplex, MDI/MDI-X adaptive
100M LAN	1 10/100Base-T(X) adaptive 100M RJ45 LAN port, supporting full/half duplex, MDI/MDI-X adaptive
serial port	- Serial port type: 1 way RS232/485 - Connection method: 3.81mm pitch 7PIN terminals, serial port occupies 5 positions

	• Baud rate: 300bps-230400bps • Data bits: 5bit, 6bit, 7bit, 8bit • Stop bit: 1bit, 2bit • Check digit: None, Odd, Even
Antenna interface	3-way SMA-K (external threaded inner hole) antenna interface, one of which is used to connect to a 4G cellular antenna, and the other two are used to connect to a 2.4G Wi-Fi antenna
SIM card interface	1-way dual Nano SIM card slot, dual card single standby, support China Mobile/Unicom/Telecom 4G, China Unicom 3G, China Mobile/China Unicom 2G
indicator	Power indicator light, running indicator light, network indicator light, serial port indicator light, 4G indicator light, signal strength indicator light, electrical port speed and connection/activity indicator light
Power parameters	
power input	DC9~36V
full load power consumption	<3.5W@DC24V
connection method	3.81mm pitch 7PIN terminals, power supply occupies 2 positions
power protection	Anti-reverse connection
Mechanical parameters	
Size	118×35×88(mm) (excluding ding rail)
installation method	35mm standard DIN rail installation
Case protection	IP40
weight	About 0.37kg (without antenna)
Working environment	
working temperature	-40°C~+75°C
Storage temperature	-40°C~+85°C
Relative humidity	5%~95%(No condensation)
Industry standard	
EMC	• IEC 61000-4-2 (ESD): Level 4 (contact discharge ±8kV, air discharge ±15kV) • IEC 61000-4-5 (Surge): Level 4 (Power supply: common mode ±4kV, differential mode ±2kV; Network port: common mode ±6kV, differential mode ±2kV; Serial port: common mode ±4kV) • IEC 61000-4-4 (EFT): Level 4 (power supply: ±4kV; network port, serial port: ±2kV)

1.5 Interfaces and Indicator Lights

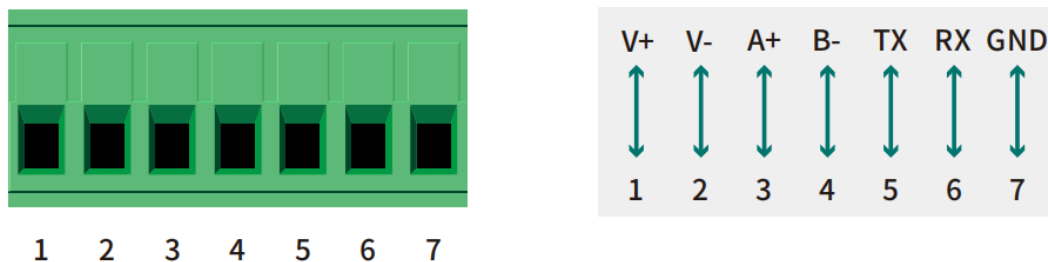


Note:

MIR652R-W is equipped with a 4G antenna.

1.5.1 Power input interface and RS232/485 interface

It adopts 7-position 3.81mm spacing terminals, 1 and 2 are power input interfaces, and the voltage input range is: DC 9~36V; 3, 4, 7 are RS485 interfaces, 5, 6, 7 are RS232 interfaces mouth, defined as shown in the figure.

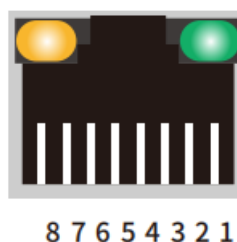


1.5.2 Restart / restore the factory setting button

Press and release the button within 1 second, the system will reset, the 'Run' light will turn off, and the system will return to normal after startup; if you press for more than 5 seconds, the 'Run' light will flash frequently (flashing once every 0.2 seconds). At this point, release the button, the parameters will be reset to factory settings, and the system will reset.

1.5.3 WAN Interface

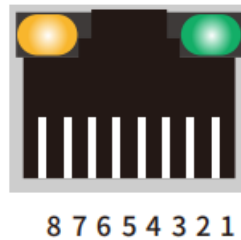
WAN port, mainly used for wired connection between the router and the wide area network (external network). It supports static IP, dynamic IP, and PPPoE dial-up networking modes.



Pin No.	Signal Name
1	Transmit Data+ (TD+)
2	Transmit Data- (TD-)
3	Receive Data+ (RD+)
6	Receive Data- (RD-)
4, 5, 7, 8	Unused

1.5.4 LAN Interface

Local Area Network (LAN) interface, mainly used for wired communication between the router and devices within the local network.



Pin No.	Signal Name
1	Transmit Data+ (TD+)
2	Transmit Data- (TD-)
3	Receive Data+ (RD+)
6	Receive Data- (RD-)
4, 5, 7, 8	Unused

1.5.5 Status Indicator

The panel indicator light shows the current working status of the device, as detailed in Table 1-2.

Table 1-2 System Status Indicator Explanation

Indicator	Status	Definition
PWR	On	Power supply is normal
	Off	No power supply or abnormal power supply
RUN	flashing	The equipment is in normal operation
	On,off	The equipment is running abnormally
NET	On	Connect to the router in Client mode or connect to other devices in AP mode, or connect to other devices through a network cable;
	Off	no device connected
COM	flashing	The RS485 interface is sending and receiving data
	Off	No data
4G	On	The 4G network is already connected
	Off	The 4G network is not connected or the dial-up fails
SIG	On	Strong signal
	Fast flashing (0.5s flashing once)	Medium signal
	Slow flashing (1s flashes once)	weak signal
	off	no signal

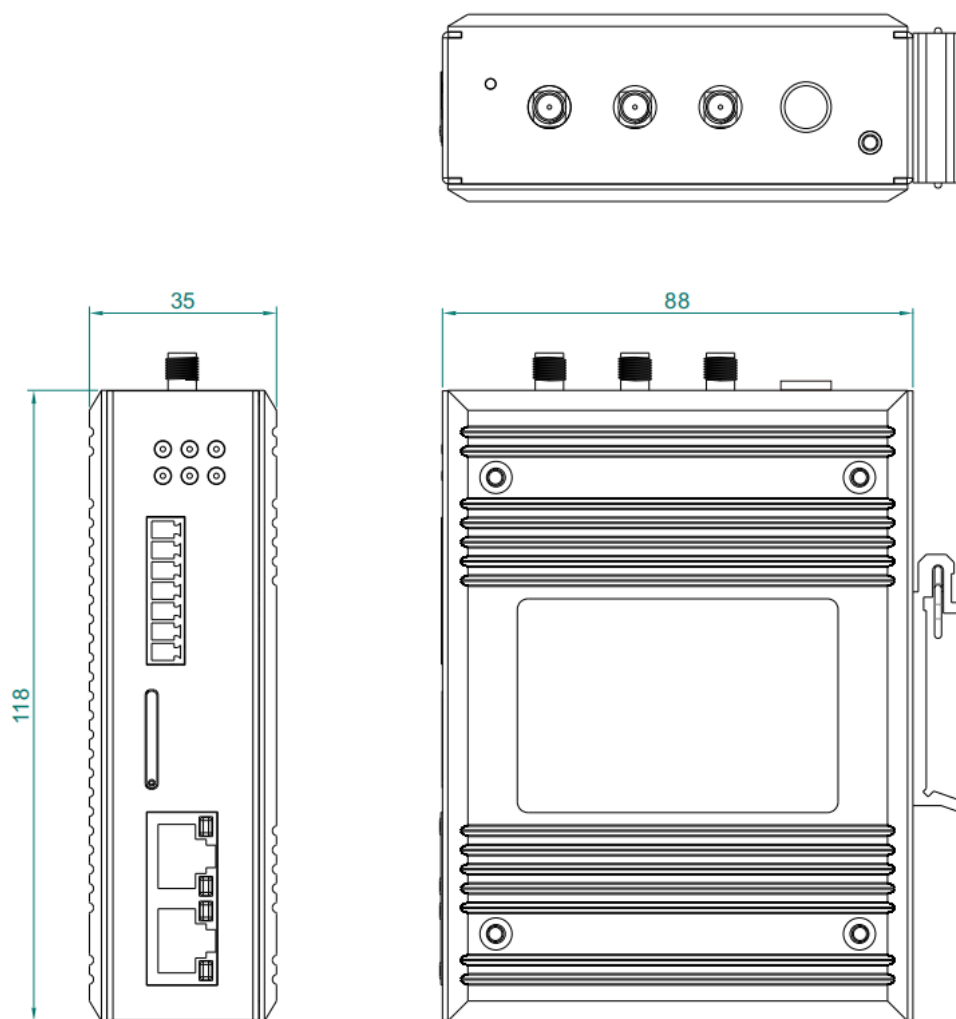
1.5.6 Antenna

1* 4G antenna and 2*Wi-Fi antennas.

1.5.7 SIM card slot and its button

By default, it supports dual Nano SIM card slots, dual SIM and single standby.

1.6 Installation Size



MIR652R-W Size (in mm)

2 Quick Internet Connection

2.1 Environmental preparation

For a quick internet connection with the 4G router, you need to prepare a PC, One router, One ethernet cable, One DC12V/1A power supply, One 4G SIM card, The hardware connection is shown in Figure 2-1.

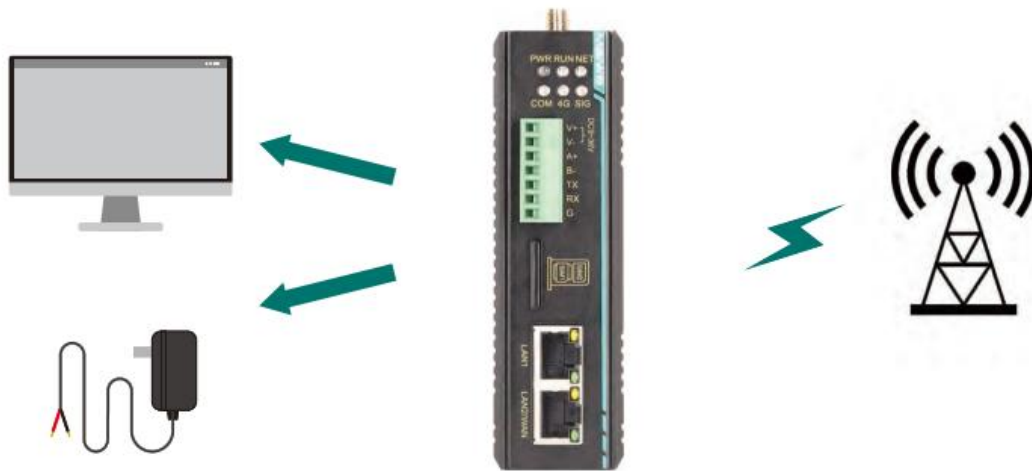


Figure 2-1, the hardware connection

2.2 Network Connection

- Insert the SIM card into the SIM1 slot (the factory default setting recognizes the SIM1 slot), with the chip side of the SIM card facing down.
- Connect the Wi-Fi antennas (2 pieces) and the 4G antennas (1 piece) in sequence to the corresponding antenna ports of the router.
- Connect the PC's ethernet port to the router's LAN port using an ethernet cable.
- Configure the PC's network card to automatically obtain an IP address, as shown in Figure 2-2.

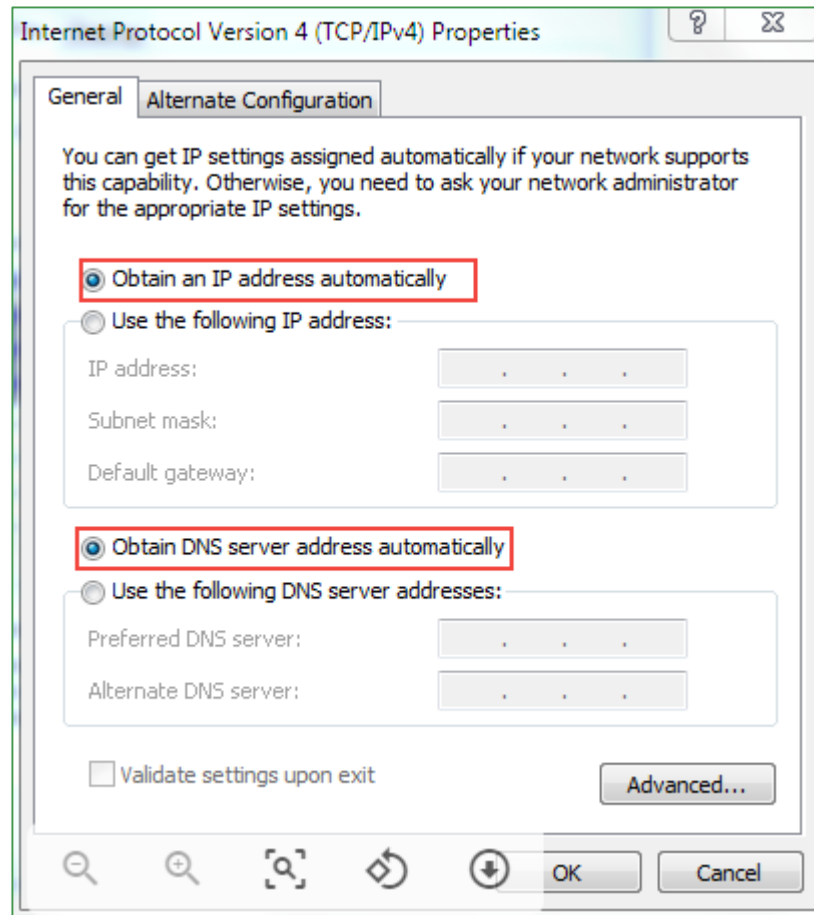


Figure 2-2 network connection

- Use the standard DC12V power supply to power on the router.
- After powering on, wait for about 2 minutes. When the 4G network connection status light and the signal strength light are on, it indicates that the 4G router is successfully connected to the network and can access the internet normally.

2.3 Router indicator

The router's front panel indicator lights are defined according to the status indicator light table.

Explanation:

- After the router is powered on, the power light (PWR) will always be on. Only when the operation light (RUN) is flashing can the router work properly.
- After the module connects to the network via 4G dial-up, the 4G network status light will light up.
- The operation of the WAN and LAN ports is indicated by the built-in indicator lights of the ports. Only when the cable is plugged in and the network device at the other end is also working properly (not just when the cable is plugged in, the port light will flash), will the corresponding WAN/LAN indicator light flash.

2.4 WEB login and networking test

The initial account parameters for logging into the MIR652R-W series 4G router WEB are shown in Table 2-1.

Table 2-1 WEB Initial Account Table

Parameter	Initial value
LAN port IP address	192.168.16.253
User name	admin
Password	Admin-985#

In the PC browser (it is recommended to use Chrome or Firefox), enter: 192.168.16.253 (you can also use the management domain <http://welinos.cn> to log in). Enter the correct username and password, then press the Enter key. The router's login interface is shown as in Figure 2-3.

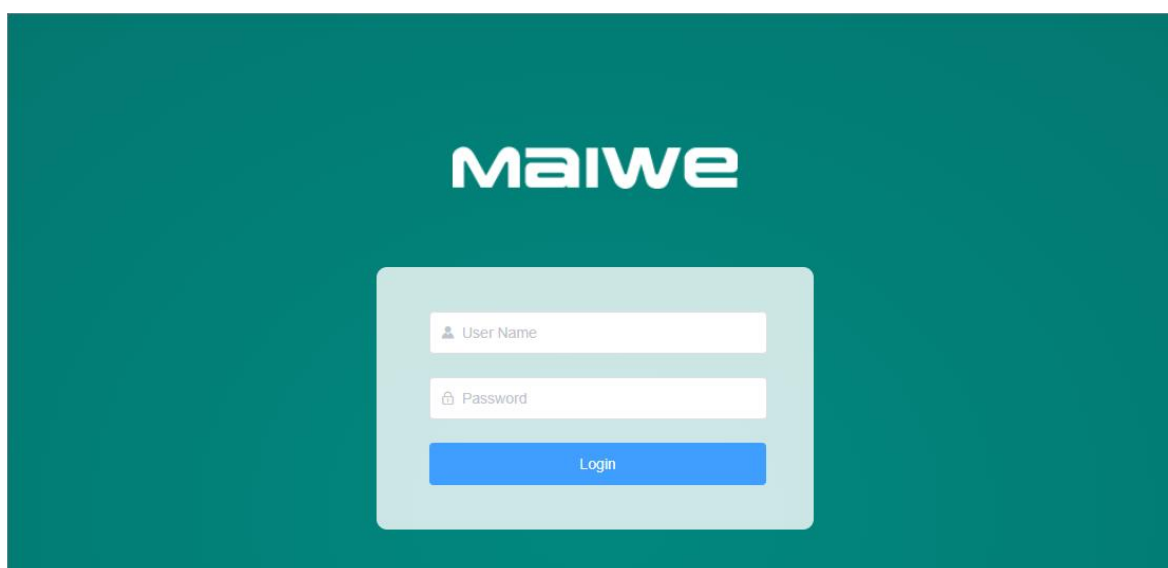


Figure 2-3 Login page

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.

3 WEB Basic Function Configuration

When using the MIR652R-W series 4G router for WEB interface configuration, you can connect via a PC using an Ethernet cable to the LAN port of the MIR652R-W series 4G router, or connect wirelessly to the router's WLAN. After connecting, you can log in to the WEB management interface for configuration.

By default, the MIR652R-W series 4G router's default SSID name is "Device Model-XXXX", such as MIR652R-W-XXXX (different device models have different default SSIDs, where XXXX represents the last 4 digits of the router's LAN port MAC address, and each router's MAC address is unique). The initial configuration values for the IP address, username, and password are shown in Table 3-1.

Table 3-1 Table of initial value configuration parameters

Parameter	Initial value
SSID	MIR652R-W-XXXX
Wireless password	Admin-985#
LAN port IP address	192.168.16.253
User name	admin
Password	Admin-985#

You can use a PC or mobile's wireless card to join the wireless network with SSID MIR652R-W-XXXX. After successfully connecting wirelessly, open your browser and enter the router's LAN port IP in the address bar (192.168.16.253 or <http://welinos.cn>). Press enter, then input the username and password and click the login button to access the router's WEB management interface (the default page language is in Chinese).

3.1 Log in to WEB

Open your browser and enter the router's default IP address in the address bar. After pressing the enter key, a window as shown in Figure 3-1 will pop up, prompting the user to enter their username and password.



Figure 3-1: User name and password input interface

The default login user for this router is only one, with the role of a super administrator. The username is "admin", and it can configure all the functionalities of the router. If you need to create other users, please refer to section 3.7.2.

After entering the username and password, click "Login". The router's WEB server will authenticate and determine if the user is logging into the router WEB interface for the first time. If so, it will lead to the newbie guidance page. (If users do not wish to configure parameters in the newbie guidance interface, they can directly click on the "X" button in the top right corner to exit the newbie guidance page), as shown in Figure 3-2.

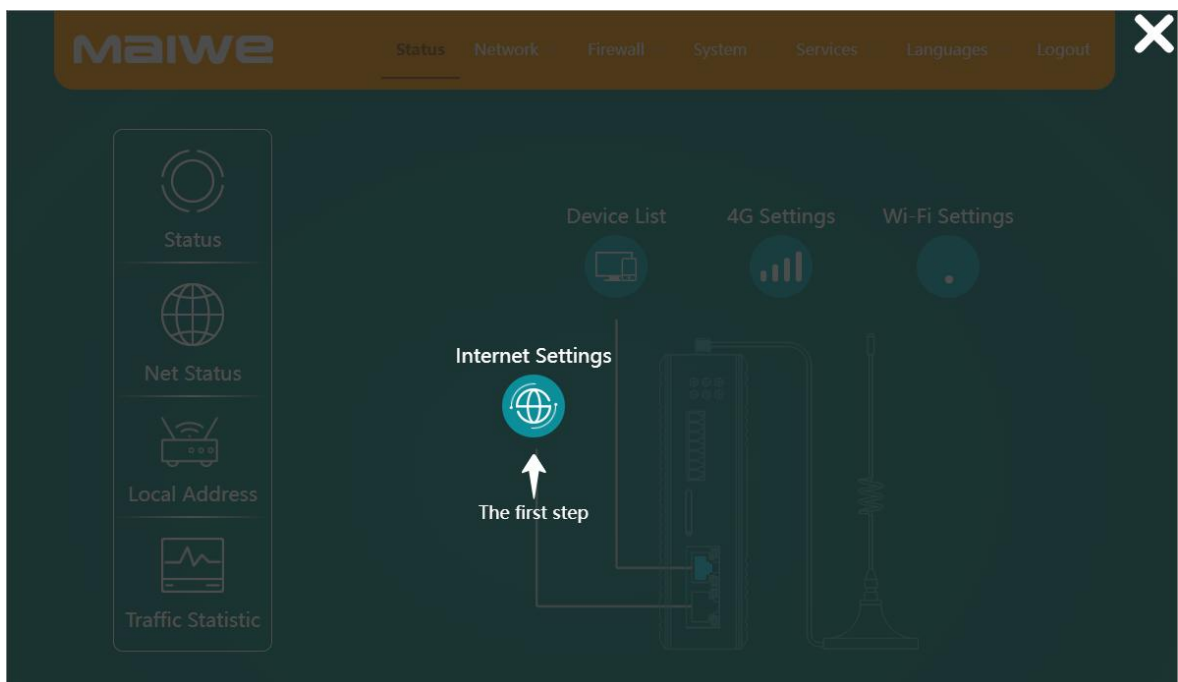


Figure 3-2: Newbie Guidance Page.

If it's not the first time logging in, you will be directed straight to the WEB management main page, as shown in Figure 3-3.

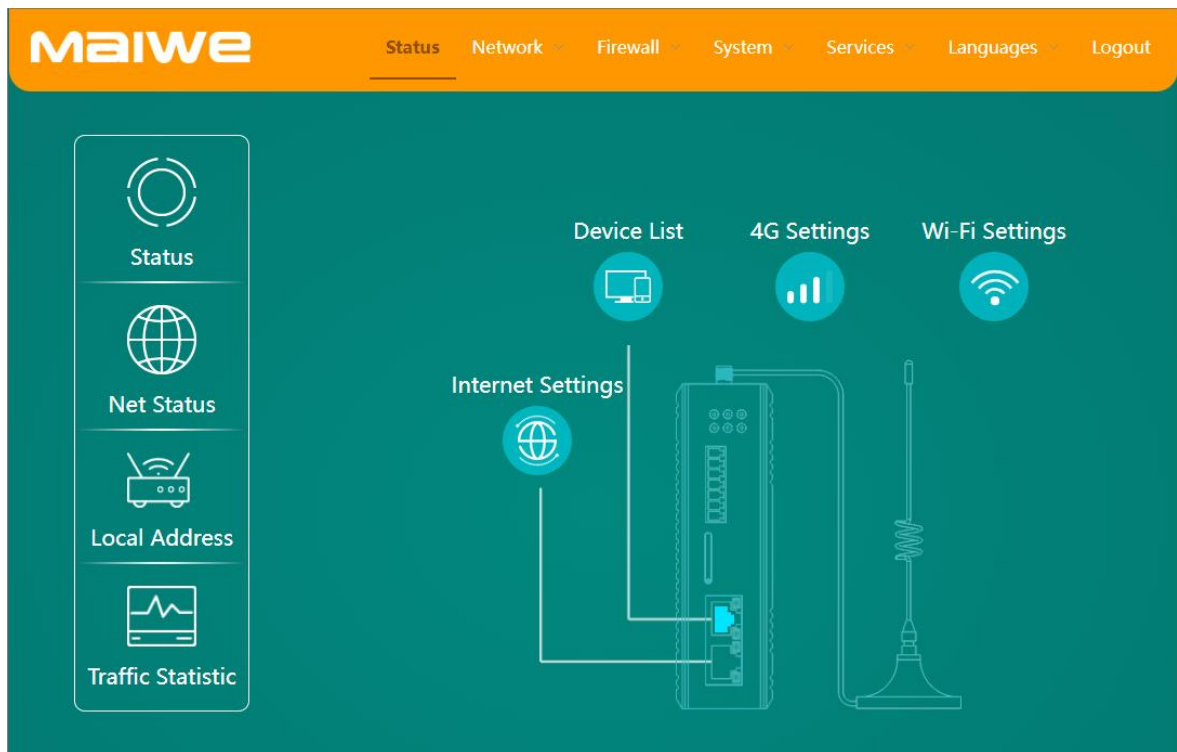


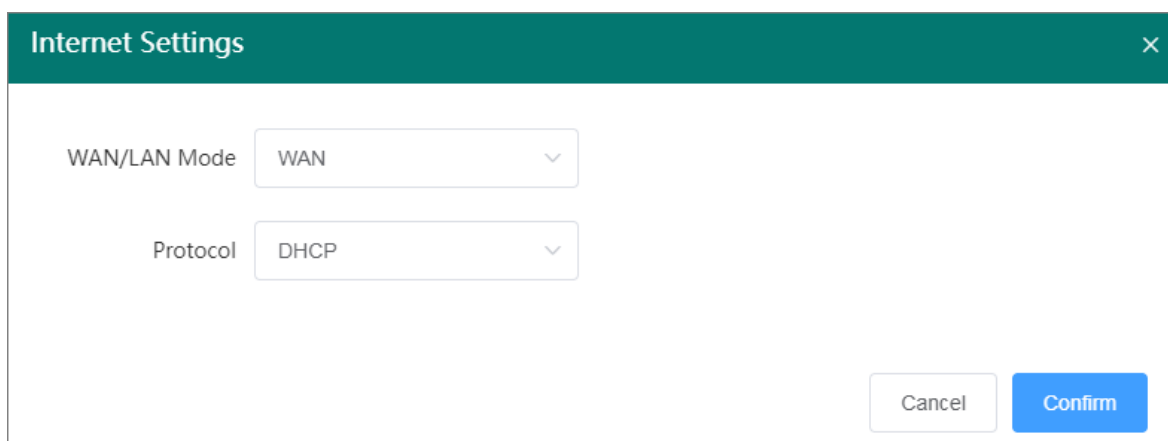
Figure 3-3 WEB main page

3.2 Introduction to the New User Guide Page

When users log in to the WEB server for the first time, the system will enter the new user guide page, as shown in the above Figure 3-2. The new user guide is divided into three parts: WAN (Wide Area Network) settings, 4G settings, and wireless settings. Initially, it will default to WAN settings, followed by 4G settings, and finally wireless settings. Only after all the settings are completed will it enter the main page.

3.2.1 WAN Settings

When users access the WEB server for the first time, they will be taken to the page as shown in Figure 3-2. By clicking on the icon, they will be directed to the WAN settings page to set up WAN information. This primarily includes two parameters: the WAN/LAN mode selection and the WAN port protocol, as depicted in Figure 3-4.



Internet Settings

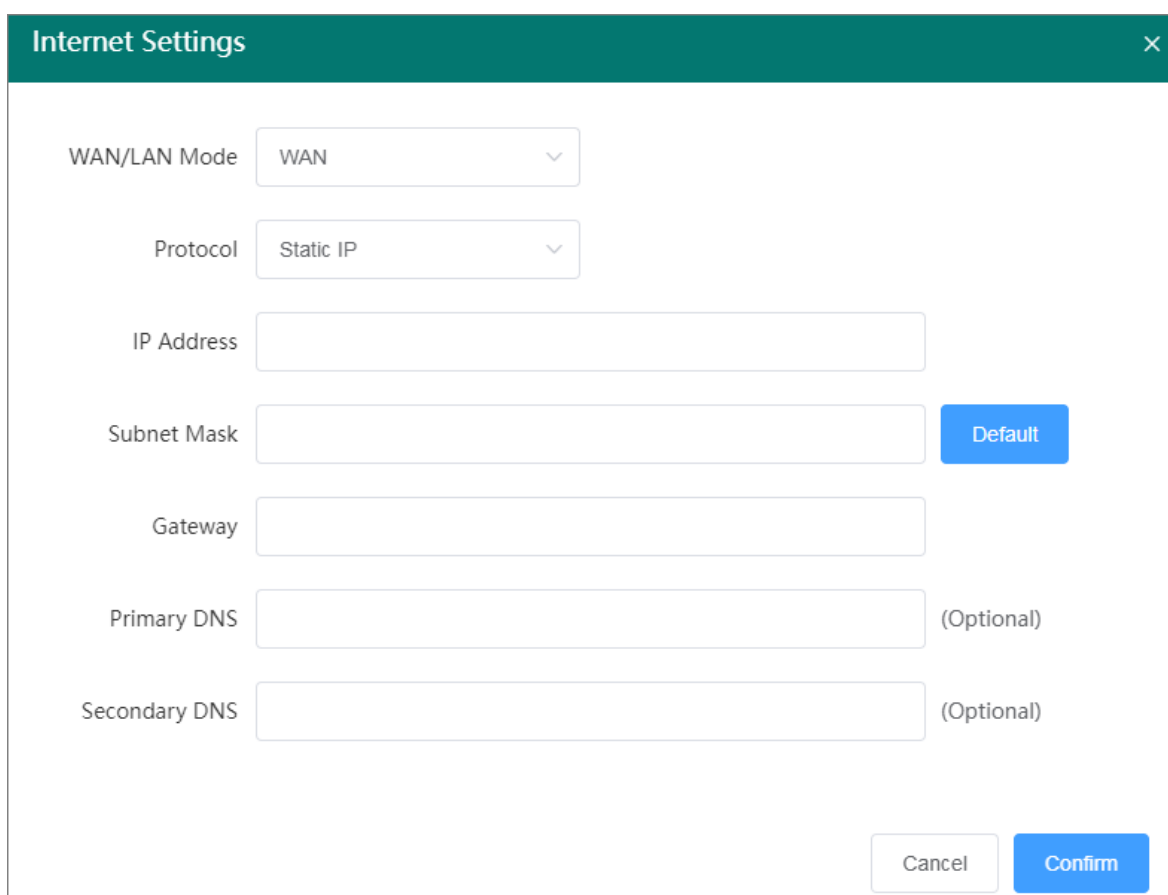
WAN/LAN Mode: WAN

Protocol: DHCP

Cancel Confirm

Figure 3-4: WAN Information Interface

- WAN/LAN Mode: When connecting to the external network via the WAN port, it must be set to WAN mode (default is WAN mode).
- Protocol: WAN port protocols include static address, DHCP, and PPPoE. The default is DHCP mode.
- Static Address: Connect to the network by manually specifying the IP address, subnet mask, and gateway, as shown in Figure 3-5.



Internet Settings

WAN/LAN Mode: WAN

Protocol: Static IP

IP Address

Subnet Mask: Default

Gateway

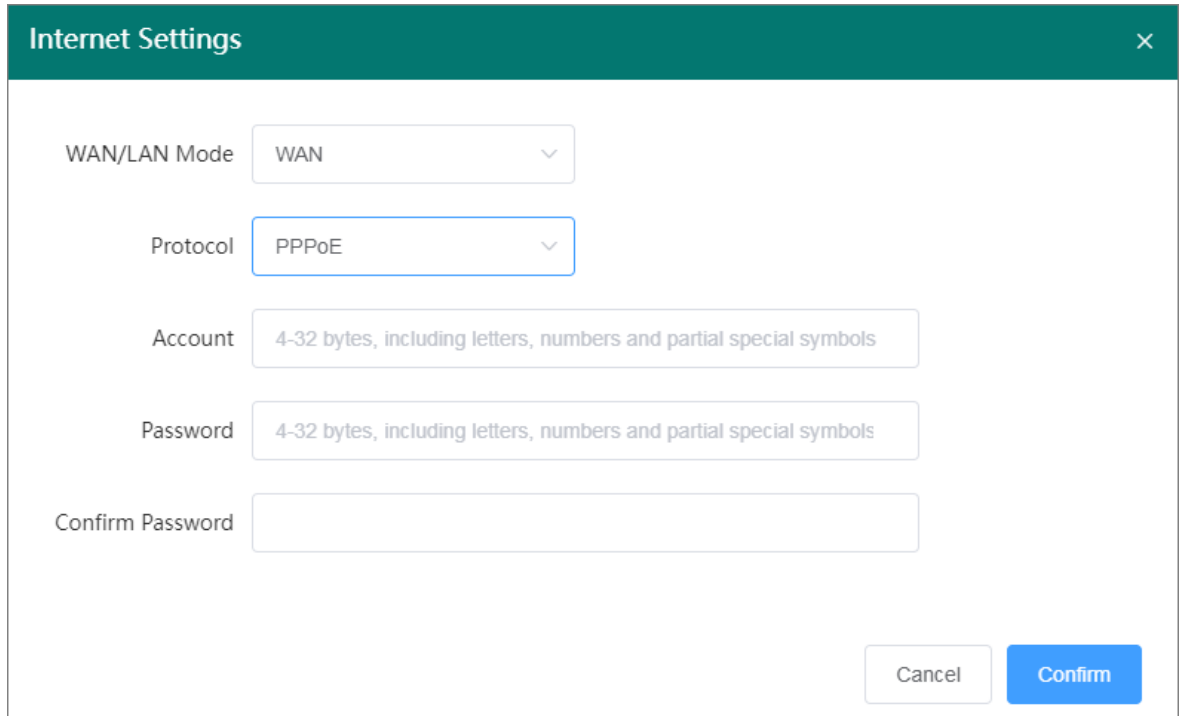
Primary DNS (Optional)

Secondary DNS (Optional)

Cancel Confirm

Figure 3-5 Static IP page

- DHCP: By making a request to the DHCP server, it automatically obtains the IP address, gateway, and DNS assigned by the server.
- PPPoE: Connect by setting up a username and password (obtained from the broadband service provider), as shown in Figure 3-6.



The screenshot shows a window titled "Internet Settings" with a close button (X) in the top right corner. Inside the window, there are five input fields and two buttons at the bottom right. The first field is "WAN/LAN Mode" with a dropdown menu showing "WAN". The second field is "Protocol" with a dropdown menu showing "PPPoE". The third field is "Account" with a placeholder text "4-32 bytes, including letters, numbers and partial special symbols". The fourth field is "Password" with the same placeholder text. The fifth field is "Confirm Password" which is currently empty. At the bottom right, there are two buttons: "Cancel" and "Confirm".

Figure 3-6 The PPPoE interface

3.2.2 4G Settings

4G configuration parameters mainly include protocol settings, APN protocol settings, and dual card management settings. If using a regular mobile SIM card or IoT SIM card, the 4G settings can be left at default parameters (there's no need to set the APN, username, or password). However, if you're connecting with a specialized APN card, you'll also need to set up the APN name, username, and password (which can be obtained from the service provider). The DNS server and alternative DNS server can be set to public DNS, or they can be left unset (if not set, the carrier-assigned DNS will be used), as shown in Figure 3-7.

4G Parameter Settings

SIM Settings

Setting the APN dedicated network card

APN
1-100 bytes, including letters, numbers and partial special symbols
(Optional)

Username
1-127 bytes, including letters, numbers and partial special symbols
(Optional)

Password
1-127 bytes, including letters, numbers and partial special symbols
(Optional)

Authentication Type
NONE

Primary DNS
114.114.114.114
(Optional)

Secondary DNS
223.5.5.5
(Optional)

Cancel
Confirm

Figure 3-7 4G setting interface

3.2.3 Wireless Settings

You can configure the Wi-Fi status, SSID name, and password, as shown in Figure 3-8.

Wi-Fi Settings

Wi-Fi Status
Disable
Enable

Work Mode
AP Mode

SSID
MIR652R-W-6D1D

Password

Cancel
Save

Figure 3-8 The Wi-Fi setting interface

3.3 Main Page Introduction

After the user logs into the WEB interface for the first time and completes the novice guide operation, they can enter the WEB main interface, as shown in the aforementioned Figure 3-3. It mainly consists of two areas: top and bottom. The upper part has a Logo area on the left and a function menu area on the right. The lower part is the function display and setting area, where the router's features are set, as illustrated in Figure 3-9 WEB management main interface.

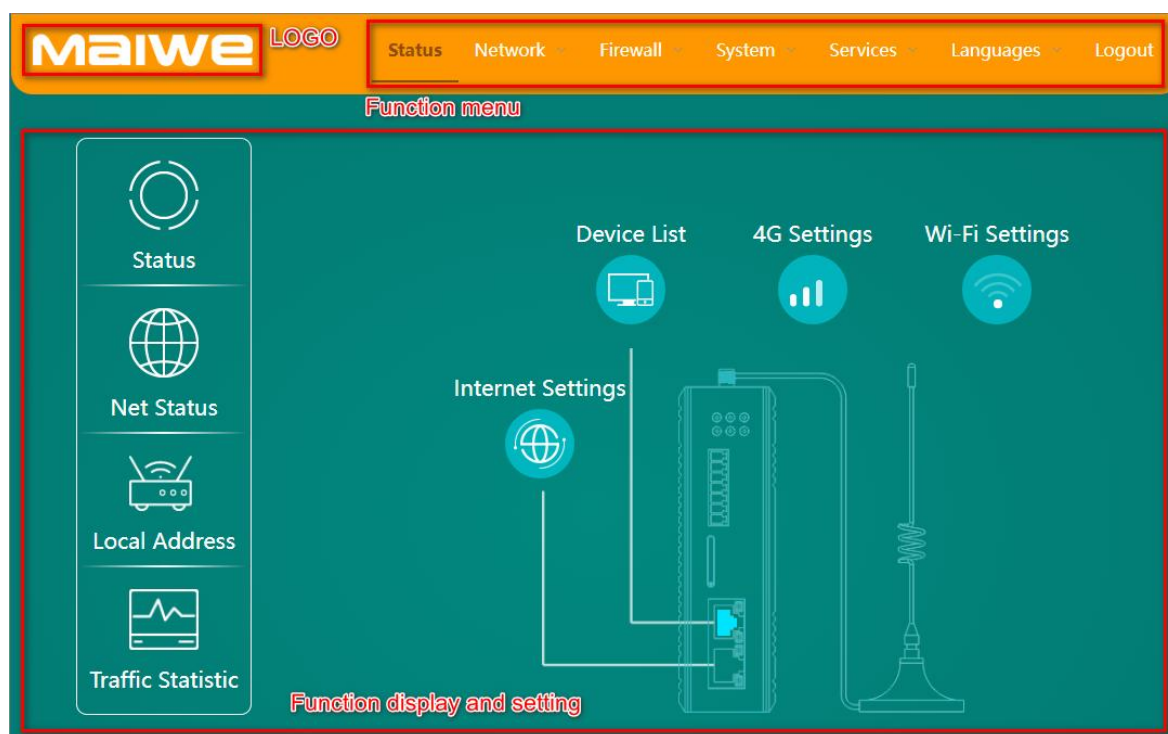


Figure 3-9. Main page

3.3.1 Function Menu

The top right part of the page is the function menu, which displays all the configurable software features of this router. The function menu includes Status, Network, Firewall, System, Services, Language, and Logout. Each menu contains several sub-functions, with the Status, System, and Network functions shown in Table 3-2.

Table 3-2: Menu Function Description Table

Menu	Pages	Functions
Status	Status	Display the device information such as:platform ID,device model,device SN,hardware version,firmware version,uptime
	Net status	Display the connection type , IP address and real-time flow
	Local address	Display router LAN port MAC and IP, CPU and memory load
	Traffic statistics	Display the current total data traffic downloaded and uploaded

Network	Interface	Display the MAC and IP addresses of WAN, LAN, and WAN_4G and add basic information of some VPN Client interfaces.
	WAN setting	Configure connection parameters for WAN
	LAN setting	Configure network parameters for LAN and DHCP
	4G Settings	Display the signal strength of the SIM card and configure the network parameters of 4G
	Wireless settings	Set the basic parameters of wireless and wireless security
	access device	Displays the terminal device connected by the router
	Static routing	Configure the static routing table
	link check	Perform ping detection on the specified target IP, once the maximum number of failures is reached, the Perform appropriate recovery operations
	network diagnosis	Diagnose the current network connection status of the router
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	Sets the router port forwarding rule
	Access control	Set the IP, MAC, and domain name filtering parameters
	Custom rules	Provides custom firewall rule settings
	DMZ	Set up the DMZ host function in the LAN
	UPnP	Open and close the UPnP function, and view the UPnP device connection information
	Network speed control	Speed control configuration according to IP or MAC
	QoS serve	Open and close the QoS traffic bandwidth limit function
System	System Properties	Displays and sets the system time, the host name, and the time zone
	administration authority	Modify administrator password and manage common user information
	restart	Configure the immediate restart and scheduled restart functions of the device
	Backup / upgrade	Backup or import the configuration files, and upgrade the system firmware
	Scheduled task	Manually add device timing schedule task function
	log	Configure remote and local log information, and view and download system logs
Services	Serial to network	Set the network, serial port, heartbeat package, registration package, timeout restart parameters
	Peanut Shell Intranet Penetration	Remote login and management of equipment can be realized

	Dynamic DNS	Set the basic information of the dynamic domain name
	VPN server	Set the basic information of servers such as PPTP, L2TP, and IPSec
	SNMP settings	Configure parameters such as setting information, community, trap, etc.
	LLDP settings	Set LLDP protocol connection parameters
	Cloud service	Set the cloud platform connection parameters
language	Chinese	Switch the WEB interface language to Chinese
	English	Switch the WEB interface language to English
Exit		Log out of the currently logged in user

3.4 Status

The status module includes: running status, network status, local address and traffic statistics.

3.4.1 Running state

The function of running status is to display some specific information of the current device, including the platform number, device model, device code, hardware version, firmware version, running time, etc., as shown in Figure 3-10.

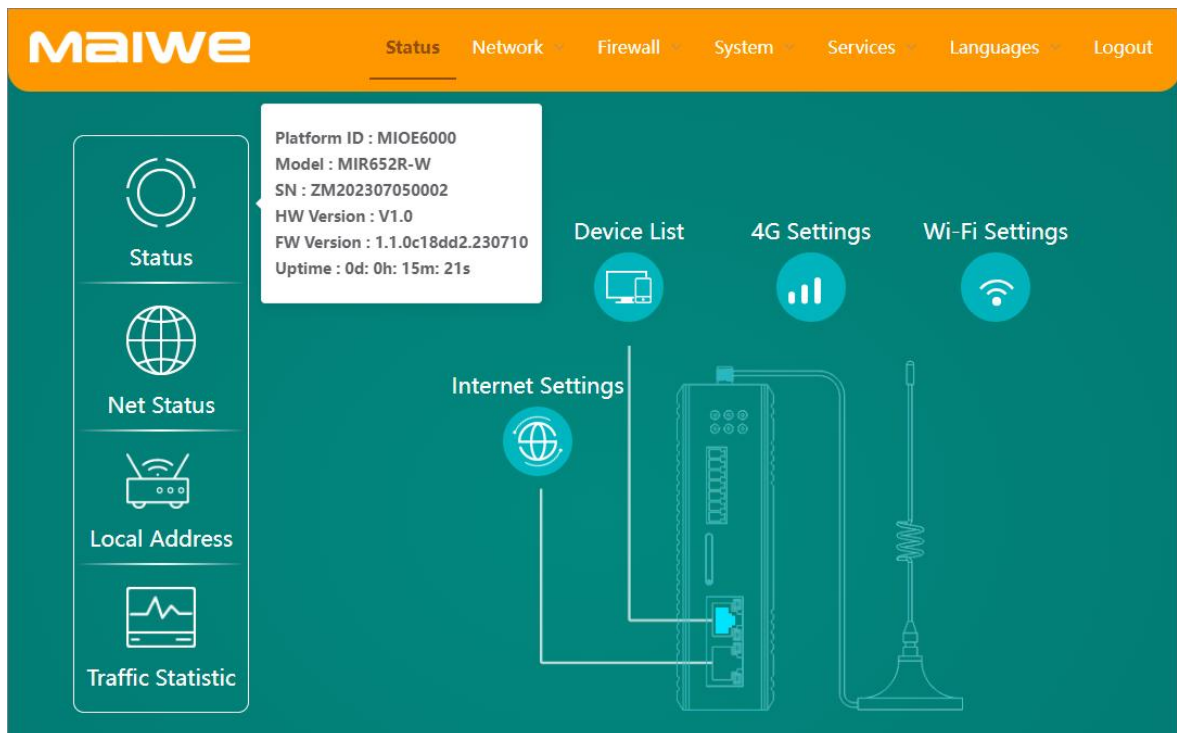


Figure 3-10 Equipment information

- Platform ID: The platform ID of the router
- Device Model: The device model of the router
- Device code: the device code of the router when it leaves the factory
- Hardware Version: Router hardware version number
- Firmware Version: The firmware version number of the router
- Uptime: The current continuous running time of the router

3.4.2 network status

The function of the network status is to display the specific information of the network connection of the current device, including the external network connection type, IP address, real-time downlink traffic, real-time uplink traffic, etc., as shown in Figure 3-11.

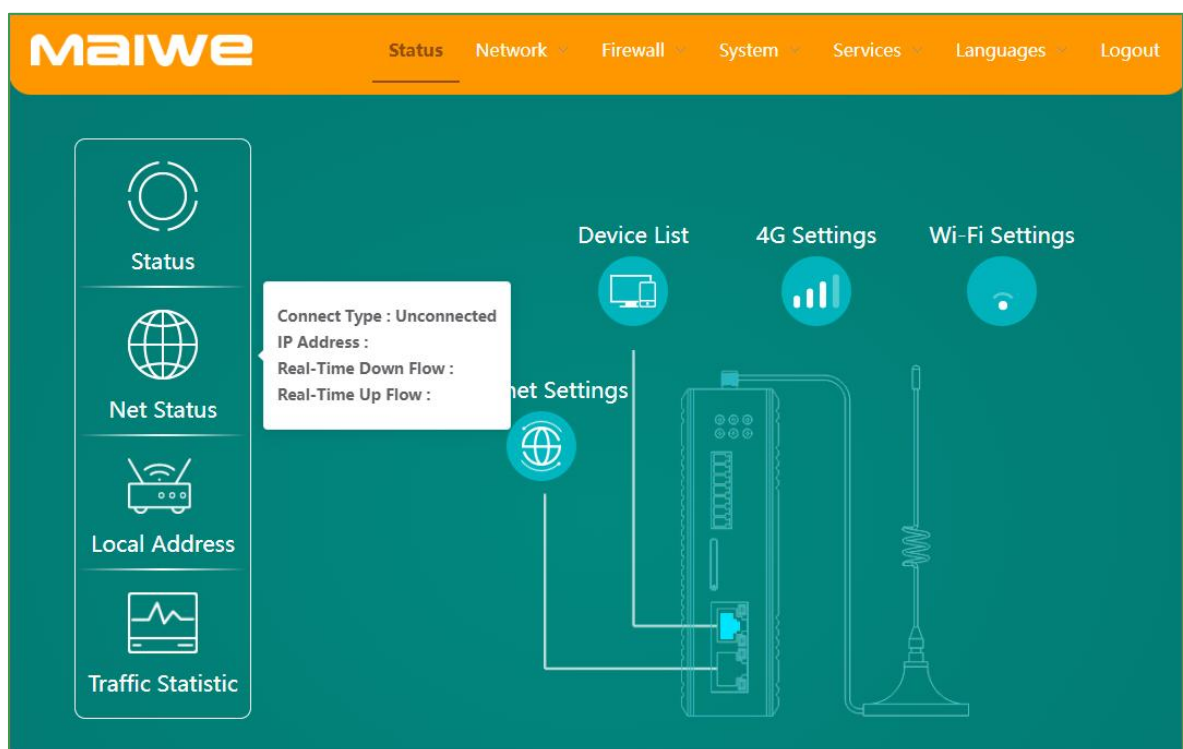


Figure 3-11 Network status information

- External network connection type: the type of router connected to external network (wired network or 4G network)
- IP address: The IP address of the router connected 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

3.4.3 local address

The local machine address mainly displays information such as MAC address, IP address, subnet mask, CPU load, and memory load, as shown in Figure 3-12.

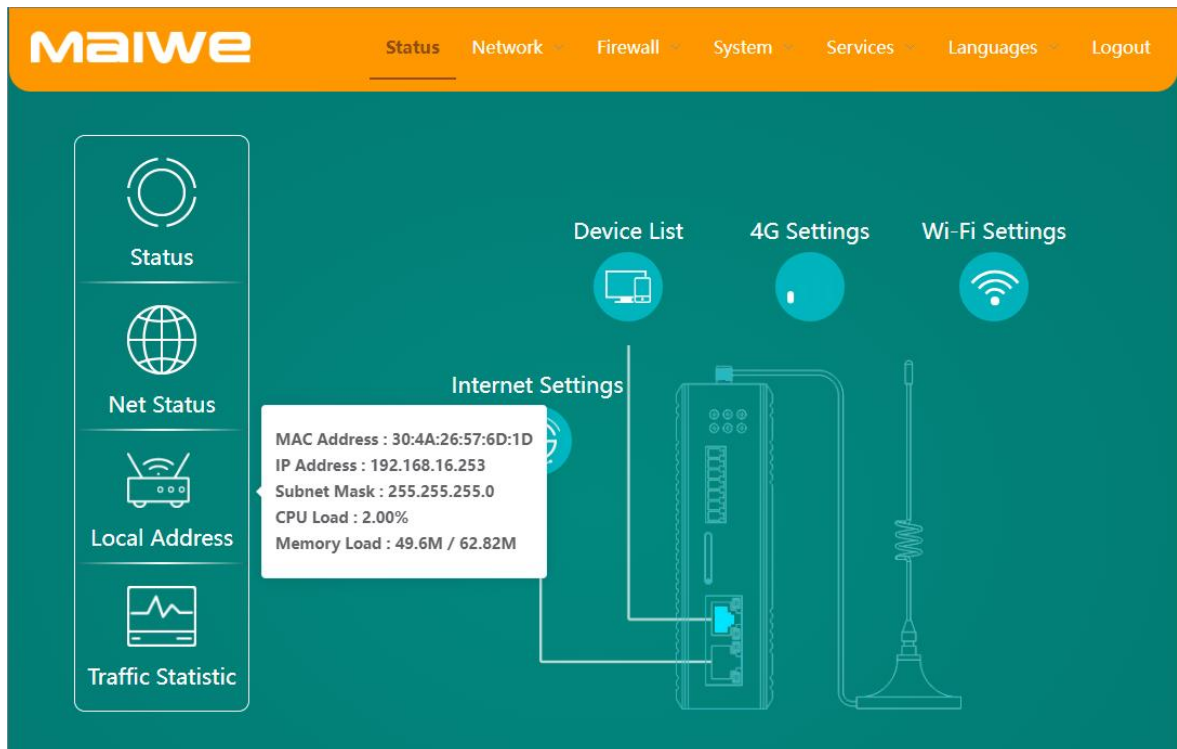


Figure 3-12 Local machine address information

- MAC address: router LAN port MAC address
- IP Address: The IP address of the LAN port of the router
- Subnet mask: It is used to indicate which bits of an IP address are the subnet where the host is located, and which bits are the bit mask of the host. The subnet mask divides the IP address into network address and The host address has two parts.
- CPU load: current CPU usage
- Memory usage: current memory usage (as shown in the figure, a total of 62.82M memory, 49.6M memory used)

3.4.4 Traffic Statistics

The traffic statistics display the current total download and upload data traffic of the router, as shown in Figure 3-13.

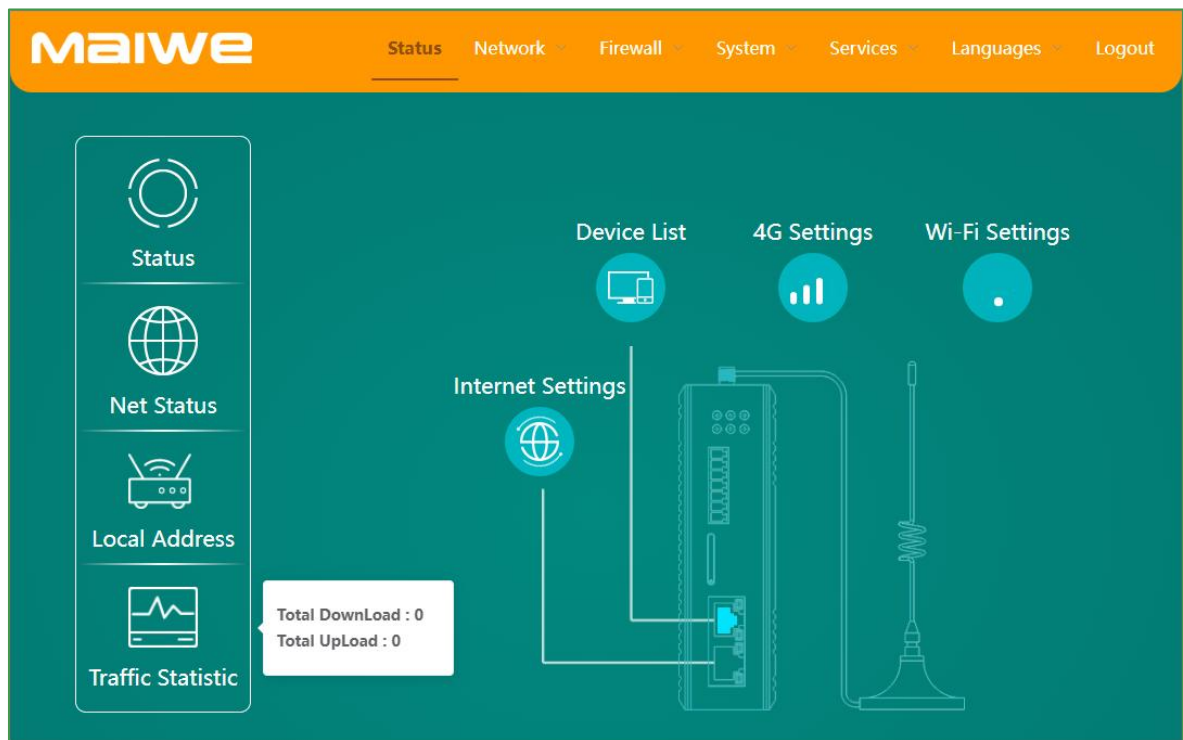


Figure 3-13 Flow statistics

- Total download volume: the current total download data flow of the router
- Total upload volume: The current total upload data flow of the router

3.5 Network

The network module includes interface, WAN setting, LAN setting, 4G setting, wireless setting, access device, static route, link check and network diagnosis.

3.5.1 Interface

The interface is divided into two parts: interface and new interface. The interface information page displays the basic information of the interface, mainly including the MAC address of the WAN port (wired WAN), the MAC address, IP address and default gateway of the LAN port, and the MAC, IP, DNS and other information of 4G, such as As shown in Figure 3-14.

Interface

New Interface

WAN WAN Disconnect	IP Address: - MAC Address: 30:4A:26:57:6D:1F Gateway : - Subnet Mask: - Primary DNS: - Secondary DNS: -
LAN LAN Connect	IP Address: 192.168.16.253 MAC Address: 30:4A:26:57:6D:1D Gateway : - Subnet Mask: 255.255.255.0
4G WAN_4G Disconnect	IP Address: - Gateway : - Subnet Mask: - Primary DNS: - Secondary DNS: -

Figure 3-14 Basic information of the interface

The new interface is mainly to add the VPN client network interface, and the protocols of the new interface include PPTP, L2TP, GRE, OPENVPN (TUN/TAP). For creating a VPN client network interface, please refer to the "4.4.2 VPN Client" section.

3.5.2 WAN port settings

It is used to configure the working mode and protocol parameters of the WAN port. The 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 normal LAN port (in this mode, all router 2 network ports are LAN ports). The WAN port protocol has three parts, static address, DHCP, and PPPoE. The static address protocol is shown in Figure 3-15, and the PPPoE protocol is shown in Figure 3-16.

The screenshot shows the 'WAN Settings' interface. At the top, 'WAN/LAN Mode' is set to 'WAN' and 'Protocol' is set to 'Static IP'. Below these are input fields for 'IP Address', 'Subnet Mask' (with a 'Default' button), 'Gateway', 'Primary DNS' (marked as optional), and 'Secondary DNS' (marked as optional). At the bottom are 'Save' and 'Apply' buttons.

Figure 3-15 Static address page

- WAN/LAN mode: Configure the working mode of the WAN port. The default is WAN mode (used to connect to the external network). If it is configured as LAN mode, the network port is equivalent to a LAN port, and its usage is the same as other LAN ports
- Protocol: The currently selected WAN port networking protocol (static address, DHCP and PPPoE)
- IP Address: The network address assigned to the WAN port of the router
- Subnet mask: It is used to indicate which bits of an IP address are the subnet where the host is located, and which bits are the bit mask of the host. The subnet mask divides the IP address into network address and The host address has two parts.
- Gateway: A device that connects data in two network segments using different transmission protocols
- DNS server: used to resolve domain names
- Alternate DNS server: used to resolve domain names

The screenshot shows the 'WAN Settings' interface with 'Protocol' set to 'PPPoE'. It includes input fields for 'Account' and 'Password', both with a hint '4-32 bytes, including letters, numbers and partial special symbols', and a 'Confirm Password' field. 'Save' and 'Apply' buttons are at the bottom.

Figure 3-16 The PPPoE protocol page

- Internet account: Enter the Internet account, the length is 4-32 characters, only numbers and letters can be included
- Internet password: The password length is 4-32 digits and can only include numbers, letters and some special symbols (~!@#\$\$%^&*()_+-.)
- Confirm Internet access password: Confirm the Internet access password in case of wrong password

3.5.3 LAN port settings

It is used to configure the basic information of the LAN port, as shown in Figure 3-17 below.

LAN

Protocol: Static IP

IP: 192.168.16.253

Subnet Mask: 255.255.255.0 Default

Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

DHCP Server

DHCP Server: Disable ☒ Enable

DHCP Start: — 100 + (Range of values 1-254)

DHCP Capacity: — 150 + (Range of values 1-155)

Lease Time: 720 (minutes)

Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Save

Figure 3-17 The LAN port configuration page

The configuration parameters of this interface are detailed in Table 3-3.

Table 3-3 Description of LAN port configuration parameters

Item	description
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
gateway	IP address of the device for the end user interface for other networks (optional)
DNS server	Used to resolve domain names (optional)
Backup DNS server	Used to resolve domain names (optional)
DHCP server	
DHCP service	Select DHCP service, enable or disable it
DHCP start	Set the initial 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 lease period of DHCP, the unit is minute. The default is 720 minutes (12 hours)
gateway	Set the gateway address of the LAN, which can be the IP address of the LAN (optional)
DNS server	Use this DNS first for domain name resolution
Backup DNS server	When the domain name that cannot be resolved by the preferred DNS can be resolved through this DNS



Notice :

- When the LAN port of the 4G router provides DHCP service to the outside world, it is not allowed to connect the LAN port to the network of other routers that also enable the DHCP service, otherwise it may cause the LAN port device connected to the 4G router to fail to obtain IP networking normally.
- When the device uses wired WAN and 4G WAN to connect to the external network at the same time, the DNS server and backup DNS server of the DHCP service need to be configured as available DNS addresses. To ensure that when the device switches between wired WAN and 4G WAN network, the connected terminal device can normally use the domain name to access the external network.

3.5.4 4G Settings

It is mainly used to display and set the basic information of the SIM card, as shown in Figure 3-18.

SIM Settings

SIM Information

IMEI: 868703058574658

FW Version: EC200ACNDAR01A05M16

ICCID: -

ISP Internet Service Provider: -

Network Mode: -

Signal Level: 255

Current SIM: SIM1

Connection Time: -

4G Interface Settings

APN

1-100 bytes, including letters, numbers and partial special symbols

(Optional)

Username

1-127 bytes, including letters, numbers and partial special symbols

(Optional)

Password

1-127 bytes, including letters, numbers and partial special symbols

(Optional)

Authentication Type

NONE

Double Card Management

SIM1

Primary DNS

114.114.114.114

(Optional)

Secondary DNS

223.5.5.5

(Optional)

Save

Apply

Figure 3-18 The SIM card configuration page

- IMEI number: 4G module serial number
- Firmware version: 4G module firmware version number
- ICCID: SIM card number
- Network Operator: current network operator
- Network Mode: The network mode of the current router
- Signal strength: The signal strength of the current router (the larger the value of -113~-51, the stronger the signal, and 255 means no signal)
- Current SIM card: SIM card slot currently used for dialing
- Connection time: The duration of the router's mobile network connection
- APN Name: the name of the access point
- Username: Enter the username
- Password : Enter the password, you can choose to display the password
- Authentication method: the currently selected authentication method
- Dual card management: current dual card selection mode (automatic, SIM1, SIM2)
- DNS server: network domain name resolution server address
- Alternate DNS server: the address of the alternate network domain name resolution server

3.5.5 Wireless settings

It is mainly used to display and set the basic information of wireless.

Wireless AP settings, as shown in Figure 3-19:

The image shows a web-based configuration interface for wireless settings. At the top, under 'Wi-Fi Settings', there is a 'Wi-Fi Status' toggle switch currently set to 'Enable'. Below this is a 'Work Mode' dropdown menu set to 'AP Mode'. The main section is titled 'AP Mode Settings' and contains several configuration options: 'SSID' is a text field with the value 'MIR652R-W-6D1D'; 'Network Mode' is a dropdown set to '802.11b/g/n'; 'Channel' is a dropdown set to 'auto'; 'Channel Width' is a dropdown set to '40MHz'; 'Hide SSID' is a toggle switch set to 'Disable'; 'Security' is a dropdown set to 'WPA2-PSK'; 'Algorithm' is a dropdown set to 'Enforce CCMP(AES) Secur'; and 'Password' is a text field with masked characters. At the bottom right of the settings area are two buttons: 'Save' and 'Apply'.

Figure 3-19 Wireless configuration page

In this interface, you can switch the wireless network on and off, set wireless parameters such as SSID, and modify the Wi-Fi encryption method and password.

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

Wireless Client settings are shown in Figure 3-20:

Wi-Fi Settings

Wi-Fi Status

Disable

☒

Enable

Work Mode

Client Mode

▼

Client Mode Settings

Access Networks

1-32 bytes, including numbers, letters, Chinese and some special sy

Search

Channel

2412MHz(Channel 1)

▼

Security

WPA2-PSK

▼

Wireless Password

1-63 bytes, including numbers, letters and connector

Protocol

DHCP

▼

Save

Apply

Figure 3-20 Wireless Client configuration page

Click "Search" on the interface to search the list of wireless hotspots around you. Users can select the wireless hotspot they need to connect to, enter the hotspot password, and connect to the hotspot after application.

Wireless AP+Client settings are shown in Figure 3-21:

The screenshot displays the 'Wi-Fi Settings' interface. At the top, 'Wi-Fi Status' is set to 'Enable' with a green toggle. Below it, 'Work Mode' is set to 'AP + Client Mode'. The 'AP + Client Mode Settings' section is divided into two parts: 'AP Settings' and 'Client Settings'. Under 'AP Settings', the 'SSID' is 'MIR652R-W-6D1D', 'Security' is 'WPA/WPA2-PSK', and 'Wireless Password' is masked with dots. Under 'Client Settings', there is a 'Search' button next to a text input for 'Access Networks' (with a hint: '1-32 bytes, including numbers, letters, Chinese and some special symbols'). Below this, 'Channel' is '2412MHz(Channel 1)', 'Security' is 'WPA2-PSK', 'Wireless Password' has a hint '1-63 bytes, including numbers, letters and connector', and 'Protocol' is 'DHCP'. At the bottom are 'Save' and 'Apply' buttons.

Figure 3-21 The wireless AP + Client configuration page

AP parameter setting can set wireless parameters such as SSID, and can also modify the encryption method and password. The legal length of the wireless password is 8-32 bytes, which can only include numbers, letters, and some special symbols (~!@#\$%^&*()_+-.). Client parameter settings Click "Search" to search the list of wireless hotspots around you. Users can select the wireless hotspot they need to connect to, enter the hotspot password, and connect to the hotspot after application.

3.5.6 Access Device

Displays a list of terminal devices currently connected to the router. As shown in Figure 3-22.

Device List

No.	Name	MAC Address	IP Address	Status
No Data				

IP & MAC Binding

No.	Name	MAC Address	IP Address	Action
No Data				

Add
Apply

Figure 3-22 Access device page

The access device in this chapter is the terminal device assigned IP by the router DHCP Server. If it is a static IP device, you can view it 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 casually, causing IP address conflicts in the network, and causing network interruption. IP/MAC binding requires the router LAN port to enable the DHCP Server function.

3.5.7 Static routing

Static routing is a routing method that describes the routing rules on the Ethernet. Static routing items are manually added configurations, rather than dynamically determined. with dynamic way. By contrast, static routes are fixed and will not change even if network conditions change or are reconfigured. Table 3-4 shows the static route adding parameters.

Table 3-4 Static routing parameters table

Name	Define	Notice
Interface	The port use for the Static routing rule	Default WAN
Destination network	The destination network address or address range to be accessed	For example 192.168.30.0
Subnet mask	The subnet mask of the network to access	255.255.255.0
Gateway	Gateway address to forward to	For example 192.168.1.102
metric	Number of packet jumps	Default 0

The router does not add any static routing rules by default, and the addition of static routing needs to be configured according to the actual network deployment environment. Examples of using static routes. Refer to the following: The network deployment of two 4G routers A, B and connected devices T1~T4 is shown in Figure 3-23.

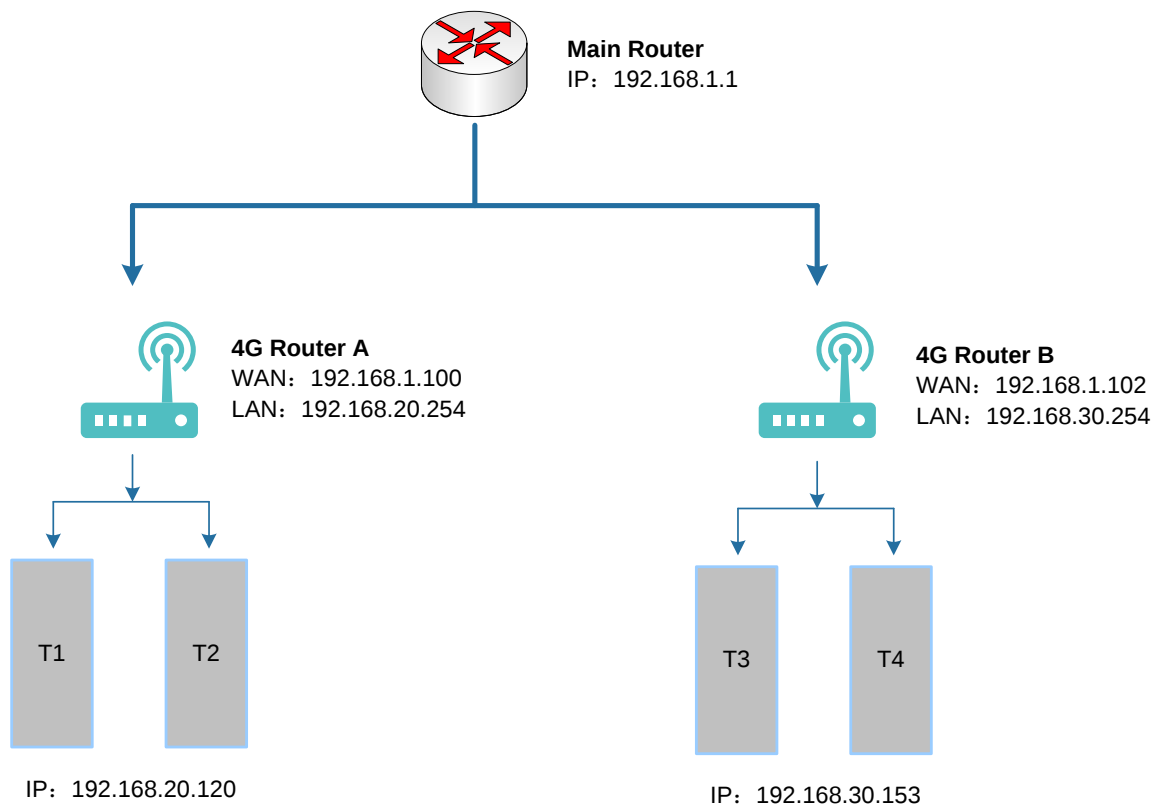


Figure 3-23 Network connection diagram

The WAN ports of 4G routers A and B are both connected to the network of the main router 192.168.1.0, and the LAN port of router A is 192.168.20.0 subnet (you need to modify the static IP of the LAN port of router A to 192.168.20.254 first), the LAN of router B 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 visits the 192.168.30.x address, it will automatically forward to router B. First, configure static routing on Router A, as shown in Figure 3-24.

Static Route					
Interface	Destination Network	Subnet Mask	Gateway	Metric	Action
wan	192.168.30.0	255.255.255.0	192.168.1.102	0	Edit Delete

[New Interface](#)
[Apply](#)

Figure 3-24 Static routing page

On T1 (use a PC as T1), use the ping command to access 192.168.30.254 (that is, the IP of the LAN port of 4G router B), as shown in Figure 3-25.

```

PING 192.168.30.254 (192.168.30.254): 56 data bytes
64 bytes from 192.168.30.254: seq=0 ttl=64 time=0.384 ms
64 bytes from 192.168.30.254: seq=1 ttl=64 time=0.327 ms
64 bytes from 192.168.30.254: seq=2 ttl=64 time=0.302 ms
    
```

```
64 bytes from 192.168.30.254: seq=3 ttl=64 time=0.302 ms
64 bytes from 192.168.30.254: seq=4 ttl=64 time=0.288 ms

--- 192.168.16.253 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.288/0.320/0.384 ms
```

Figure 3-25 ping page

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 still 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 MIR65R router has enabled the WAN port to LAN port forwarding function by default (no need Then set it), as shown in Figure 3-26.

Figure 3-26 Basic settings page

When the firewall rules of router B are set, you can access T3. As shown in Figure 3-27, T3 (192.168.30.153) under Router B can be accessed.

```
PING 192.168.30.153 (192.168.30.153): 56 data bytes
64 bytes from 192.168.30.153: seq=0 ttl=128 time=0.561 ms
64 bytes from 192.168.30.153: seq=1 ttl=128 time=0.479 ms
64 bytes from 192.168.30.153: seq=2 ttl=128 time=0.467 ms
64 bytes from 192.168.30.153: seq=3 ttl=128 time=0.508 ms
64 bytes from 192.168.30.153: seq=4 ttl=128 time=0.537 ms

--- 192.168.16.250 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.467/0.510/0.561 ms
```

Figure 3-27 Ping page data



Note:

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

3.5.8 Link check

The link check can perform ping detection on the specified target IP, and once the maximum number of failures is reached, the corresponding recovery operation can be performed. The link check configuration interface is shown in Figure 3-28:

Figure 3-28 Link check configuration page

- Enable: link check switch. After it is turned on, the network connection status can be detected in real time.
- Preferred Destination IP: Preferred IP for Ping detection. If you use a common SIM card, you can set it to a public DNS server address that can be pinged (such as 223.6.6.6 or 8.8.8.8); if you use an APN private network card, it is recommended to set it to the private network gateway address or the same private network The server address below.
- Alternate target IP: Alternate Ping detection IP. First, after the target IP detection fails, try to detect alternative target IPs. Can be set to empty.
- Check period (s): Ping check interval, unit second, range 5~600.
- Number of retries: the maximum number of failed Ping detections, ranging from 3 to 65535.
- Recovery operation: The recovery operation can choose module restart or device restart, and the default module restart.

**Notice:**

Enabling it will improve the stability of the network. It is strongly recommended to configure a suitable target IP and enable this function.

3.5.9 Network Diagnosis

This interface provides simple gateway network testing functions, including Ping diagnosis, TraceRoute, Nslookup query, etc. Figure 3-29 shows the diagnostic result of Ping through the gateway:

Network Diagnosis

IP Version	IP Version	IP Version
IPv4	IPv4	IPv4
URL or IP Address	URL or IP Address	URL or IP Address
Diagnosis Mode Ping	Diagnosis Mode Traceroute	Diagnosis Mode Nslookup

Clear

Grab Network Package

Interface	Package Numbers
any	100 (100-1000)

Generate Network Package

Figure 3-29 Network diagnosis page

This interface also provides the network packet capture function, select the interface to capture the packet (the network data packets of all network card interfaces are captured by default) and the number of network packets, and click "Generate Network Packet" to download the captured network packet data.

3.6 Firewall

3.6.1 Basic Settings

The default configuration in the basic firewall settings is shown in Figure 3-30.

Basics					
SYN-flood Defense Disable ☒ Enable					
Discard Invalid Packets Disable ☐ Enable					
Inbound Data		Accept ▼			
Outbound Data		Accept ▼			
Forwarding		Accept ▼			
Port Forwarding					
Area	Input Data	Output Data	Forwarding	Masquerading	MSS Clamping
LAN	Accept ▼	Accept ▼	Accept ▼	Disable ☐ Enable	Disable ☐ Enable
WAN	Accept ▼	Accept ▼	Accept ▼	Disable ☒ Enable	Disable ☒ Enable
Save Apply					

Figure 3-30 Basic settings page

- Inbound: data packets accessing the router IP
- Outbound: the data packet to be sent out by the router IP
- Forwarding : data forwarding between WAN port and LAN port, without going through the router itself
- IP dynamic masquerading: IP address masquerading when accessing the external network, only meaningful for WAN ports
- MSS clamping: limit the size of message MSS

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, then this rule allows the data packet to be forwarded from the LAN port to the WAN port, which belongs to "forwarding";
under the LAN port, open the router's web page, which belongs to "Inbound"; the router itself accesses other devices in the LAN through the LAN port, such as synchronizing time, which belongs to "outbound".
- **Rule 2:** Rule 2: WAN port (wired WAN port and 4G WAN port), accept "inbound", accept "outbound", accept "forwarding".

If there is an "inbound" packet, such as someone intending to log in to the router's webpage from the WAN port, it will be allowed.

If there is an "outbound" data packet, such as a router accessing the external network through a WAN port or a 4G port, this action is allowed. If you want to access the device under the LAN port of the router from the external network, this is "forwarding".

3.6.2 Port forwarding

Port forwarding is to map a specified port of the WAN address to a host in the intranet. If we want to access a device in the LAN from the external network (the router must be accessible by 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 port to 1000. The network IP is 192.168.30.129, and 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 rules are shown in Figure 3-31.

New Port Forwarding

NameForward

ProtocolTCP+UDP

Source Areawan

Source Port1000

Destination Arealan

Destination IP Address192.168.30.129

Destination Port8848

Status

Disable

Enable

Cancel

Confirm

Figure 3-31 New port forwarding page

- Name: The name of the port forwarding rule note, the legal value length is 1-32 bytes, and can only include numbers, letters and some special symbols (~!@#\$%^&*()_+-.)
- Protocol: The default is TCP+UDP, the network protocol corresponding to the current forwarding rule
- Source area: the default is wan port, the default value is fine
- Source port: external network port number, support input port number (1-65535) or port range (8848-8948) configuration format
- Destination area: the default is lan port, the default value is fine
- Destination IP address: the IP address of the internal host to be mapped and forwarded
- Destination port: The port number of the internal host to be mapped and forwarded. It supports the input port number (1-65535) or port range (8848-8948) configuration format. When entering the port range, the external port The port range and internal port range must be consistent
- Status: Whether the newly added port forwarding rule is enabled and effective, and the default is enabled and effective

3.6.3 Access control

Access control implements permission management for devices in the LAN to access the external network, including IP address filtering, MAC address filtering, and domain name filtering, as shown in Figure 3-32.

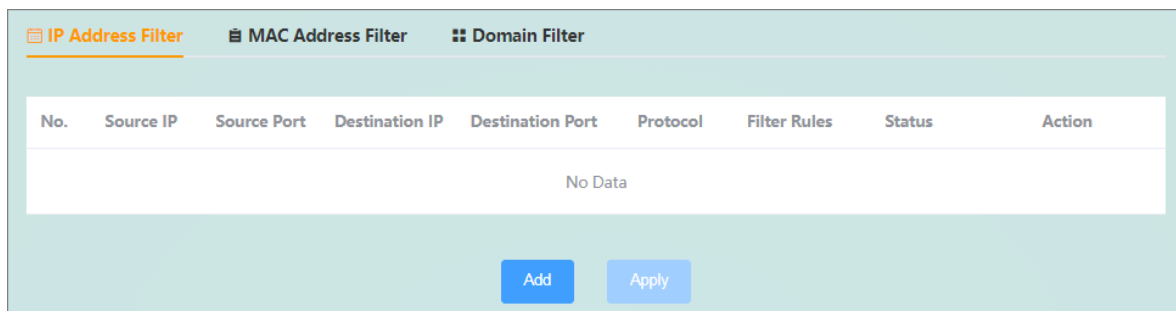


Figure 3-32 The IP address filtering page

IP address filtering: To filter hosts with IP address 192.168.30.246 from accessing the external network, as shown in Figure 3-33.

Add IP
×

Source IP192.168.30.246

Source Port1-65535, or empty

Destination IP

Destination Port1-65535, or empty

ProtocolTCP+UDP

Filter RulesReject

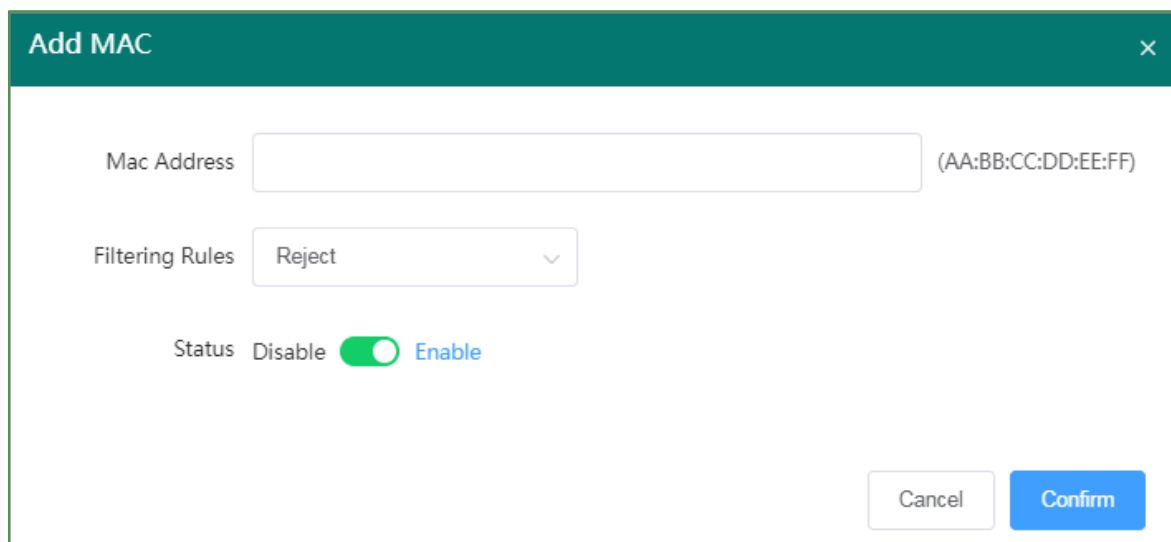
Status
Disable
☒
Enable

Cancel
Confirm

Figure 3-33 Add to the IP page

- Source IP address: the IP address of the host to be filtered
- Source port: Generally, this parameter does not need to be set, and the default is to filter all ports of the IP host
- Destination IP: Generally, this parameter does not need to be set, and the default is to restrict IP hosts from accessing all external networks
- Destination port: Generally, this parameter does not need to be set, and the default is to filter all ports that IP hosts access to all external networks
- Protocol: The protocol defaults to TCP+UDP, and restricts the access of IP hosts in tcp and udp protocols
- Filtering rules: Deny by default, restricting IP hosts from accessing the external network
- Status: Whether the newly added IP filtering rule is enabled and effective, and it is enabled by default

MAC address filtering, as shown in Figure 3-34.

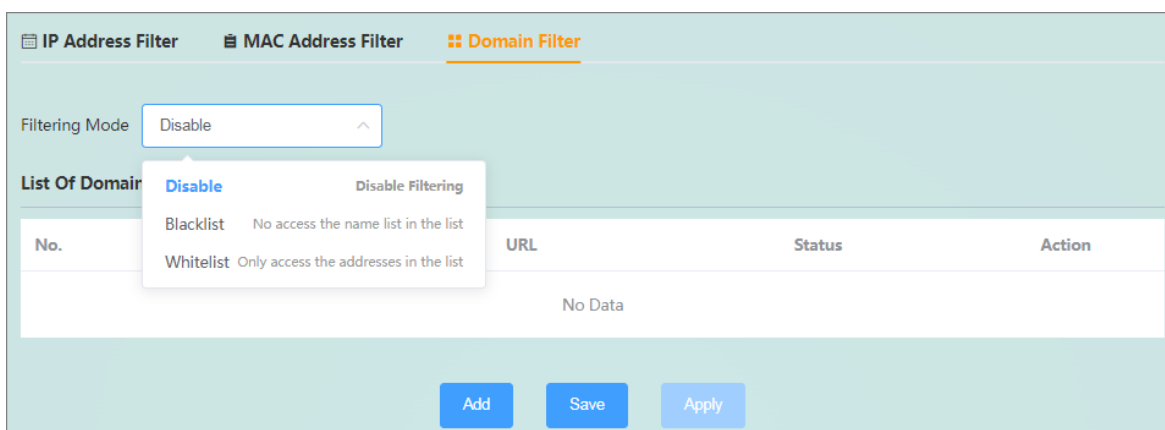


The 'Add MAC' window features a teal header with a close button. It contains three main sections: a 'Mac Address' input field with a placeholder '(AA:BB:CC:DD:EE:FF)', a 'Filtering Rules' dropdown menu currently set to 'Reject', and a 'Status' section with 'Disable' and 'Enable' radio buttons, where 'Enable' is selected. At the bottom right are 'Cancel' and 'Confirm' buttons.

Figure 3-34 Add MAC page

- MAC address: the MAC address of the host to be filtered.
- Filter rules: The filter rules default to deny, that is, to restrict hosts with MAC addresses from accessing the external network through routers.
- Status : Whether the newly added MAC address filtering rule is enabled or not, and it is enabled by default.

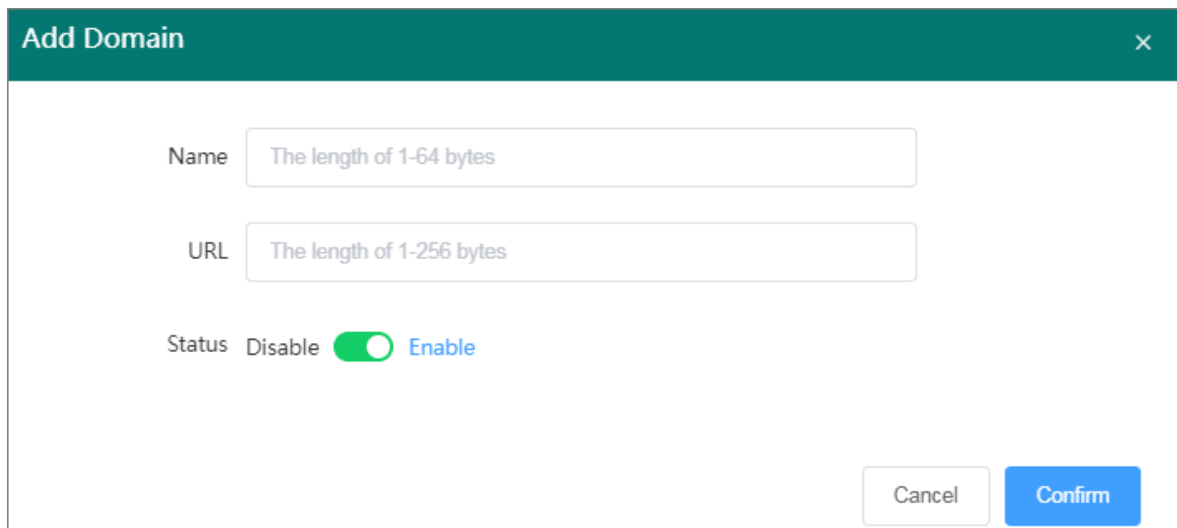
Domain name filtering: restrict access to specified domain names, and support blacklist and whitelist settings for domain name addresses, as shown in Figure 3-35.



The 'Domain Filter' page has a teal header with tabs for 'IP Address Filter', 'MAC Address Filter', and 'Domain Filter'. Below the header, the 'Filtering Mode' is set to 'Disable'. A dropdown menu is open, showing 'Disable' (selected), 'Blacklist' (with description 'No access the name list in the list'), and 'Whitelist' (with description 'Only access the addresses in the list'). Below this is a table with columns 'No.', 'URL', 'Status', and 'Action'. The table is currently empty, showing 'No Data'. At the bottom are 'Add', 'Save', and 'Apply' buttons.

Figure 3-35 Domain name filtering page

Domain name filtering is disabled by default. When the black list is selected, the devices connected to the router cannot access the domain names in the black list, and other domain names can be accessed normally; Normal access, blacklist and whitelist can set up to 8 domain name filtering rules. Add domain name setting interface as shown in Figure 3-36.



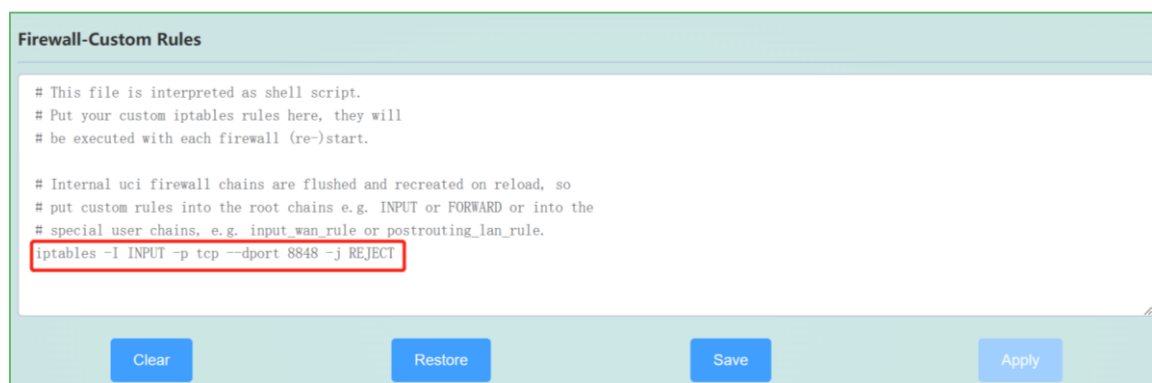
The image shows a dialog box titled "Add Domain" with a close button (X) in the top right corner. It contains three input fields: "Name" with a placeholder "The length of 1-64 bytes", "URL" with a placeholder "The length of 1-256 bytes", and a "Status" section with a "Disable" label and a toggle switch currently set to "Enable". At the bottom right, there are two buttons: "Cancel" and "Confirm".

Figure 3-36 Add domain name page

- Name : the comment name of the domain filter to be added
- URL: domain name URL or domain name URL keyword to add domain filtering
- Status: Whether the currently added domain name filter rule is enabled and effective, and it is enabled by default

3.6.4 Custom rules

The router firewall supports custom configuration rules to expand more complex firewall configuration functions. The iptables command is currently supported, and you need to refer to the Linux iptables related command description to write the command and run it. If access to port 8848 of the router is denied, the reference command is shown in Figure 3-37.



The image shows a page titled "Firewall-Custom Rules". It contains a text area with the following content:

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
iptables -I INPUT -p tcp --dport 8848 -j REJECT
```

At the bottom of the page, there are four buttons: "Clear", "Restore", "Save", and "Apply". The command line in the text area is highlighted with a red box.

Figure 3-37 Custom rules page

3.6.5 DMZ

DMZ is the abbreviation of "Demilitarized zone" in English, which is called "isolation zone", also known as "demilitarized zone". It is to solve the problem that the external network cannot access

the internal network server after installing a firewall, and set up a buffer between the non-secure system and the secure system. This buffer is located between the internal network and the external network of the enterprise. In the small network area between networks, some server facilities that must be disclosed can be placed in this small network area, such as enterprise WEB servers, FTP servers, 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 3-38.

Figure 3-38 Firewall-DMZ page

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



Notice:

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

3.6.6 UPnP

Universal Plug and Play (English: Universal Plug and Play, UPnP for short) is an application promoted by the "Universal Plug and Play Forum" (UPnP™ Forum) set of network protocols. 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 achieves this goal by defining and publishing UPnP device control protocols based on open, Internet communication network protocol standards. The UPnP function is disabled by default, and the interface configuration is shown in Figure 3-39.

UPnP Settings

Status Disable ☐ Enable

UPnP Client List

No.	Service Description	External Port	Internal Port	IP Address	Status
No Data					

Save Apply

Figure 3-39 UPnP settings

3.6.7 Network speed control

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

IP segment address rate limit: You need to fill in the start IP address, end IP address, downlink rate, and uplink rate. As shown in Figure 3-40, the maximum uplink and downlink speeds of the network segment 192.168.30.10-192.168.30.100 are limited to 100KB/s.

Add IP Network Control

Start IP

End IP

Download Bandwidth(KB/s) (10-125000)

Upload Bandwidth(KB/s) (10-125000)

Cancel Confirm

Figure 3-40 Add IP network speed control page

MAC address rate limit: You need to fill in the MAC address, fill in the uplink rate and downlink rate, and the rule settings will take effect immediately after clicking OK and Apply. As shown in Figure 3-41, 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 QoS Priority Rule by MAC

MAC Address

30:4A:26:56:1A:05

Download Bandwidth(KB/s)

–

200

+

(10-125000)

Upload Bandwidth(KB/s)

–

200

+

(10-125000)

Cancel

Confirm

Figure 3-41 Add MAC network speed control page

3.6.8 QoS

The full name of QoS is Quality of Service, which means service quality. It is specially used to solve the problem that the signal quality on the congested network is not treated equally. The QoS service is disabled by default, and the configuration interface is shown in Figure 3-42.

QoS

QoS

Disable

Enable

Download Bandwidth(Kbps)

–

4096

+

(0-1024000)

Upload Bandwidth(Kbps)

–

512

+

(0-1024000)

Save

Apply

Figure 3-42 QoS

- QoS service: close or open the QoS service function, QoS service is closed by default
- Download speed: set it 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 it 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

3.7 System

3.7.1 System Property

The purpose of this function is to display the current system time, as well as the host name and time zone of the 4G router, which can be set, as shown in Figure 3-43.

The screenshot shows the 'System Property' configuration page. It has two main sections: 'Basics' and 'Time Sync'.
In the 'Basics' section:
- 'System Time' is displayed as 2023-09-04 20:05:27 with a clock icon for editing.
- 'Hostname' is set to MIR652R-W.
- 'Time Zone' is set to Asia/Shanghai.
- 'Management Port' is set to 80.
In the 'Time Sync' section:
- 'NTP Client' is enabled (toggle switch is green).
- 'Primary NTP Server' is disabled (toggle switch is grey).
- There are three 'Secondary NTP Server' input fields containing: ntp1.aliyun.com, time1.cloud.tencent.com, and time.ustc.edu.cn.
A 'Save' button is located at the bottom right of the 'Time Sync' section.

Figure 3-43 System properties

- System time: Get the current system time, you can click the clock icon to modify it, or you can synchronize the browser time to the router time
- hostname: the name of the current host
- Time zone: the time zone used by the current router
- Management port: the port number for accessing the WEB page, the range is 80,443,1024~65534, the default is 80
- The router also provides NTP network time automatic synchronization function, the corresponding parameters are as follows:
 - NTP client: enable the router to synchronize the time of the NTP server
 - Primary NTP server: enable the router to function as an NTP server, providing external NTP time synchronization services
 - Alternative NTP server 1~3: The router is configured with a default NTP server address, and users can also add candidate NTP server addresses by themselves. A total of three candidate NTP server addresses can be added.

3.7.2 Administration Authority

You can modify the administrator password on the management rights page, and you can also add new ordinary users (up to 5 ordinary users can be added, ordinary users cannot operate the network, firewall, service configuration interface, and can open SSH switch and set the SSH port number), as shown in Figure 3-44.

The screenshot displays the 'Administration Authority' interface with the following sections:

- Change Administrator Password:** Contains two input fields for 'New Password' and 'Confirm Password', both with a placeholder text '4-32 bytes, including letters, numbers and partial special symbols'. Below these fields is a blue 'Save' button.
- General User Management:** Features a table with columns 'ID', 'Username', and 'Action'. The table is currently empty, displaying 'No Data'.
- Add New User:** Includes a notice bar stating 'Notice: The maximum number of ordinary users is 5!'. Below this are three input fields for 'New Username', 'Password', and 'Confirm Password', all with a placeholder text '4-32 bytes, including letters, numbers and special symbols- _ @'. A blue 'Save' button is positioned below the fields.
- SSH Access:** Contains a toggle switch for 'SSH' (currently set to 'Disable') and a text input field for 'SSH Port' with the value '22'. A blue 'Save' button is located at the bottom of this section.

Figure 3-44 Administration Authority interface

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

3.7.3 Reboot

On the restart page, the user can restart the router immediately or set the function of restarting the router at a fixed time, as shown in Figure 3-45.

Reboot

Reboot [Reboot Now](#)

Scheduled Reboot Parameter Setting

Reboot Schedule ☐ Disable ☒ Enable

Repeat [Mon](#) [Tue](#) [Wed](#) [Thu](#) [Fri](#) [Sat](#) [Sun](#)

Reboot Time 3 : 58

[Save](#)

Figure 3-45 System restart page

The scheduled restart function is enabled by default (the default scheduled restart time is set to 3:58 on Monday morning, and the scheduled restart function can be turned off), the scheduled restart is triggered cyclically on a weekly basis, and the router can be restarted at any time on any day of the week.

3.7.4 Backup and upgrade

On this page, you can back up and restore configuration files, restore factory settings, and flash and upgrade new firmware for the router, as shown in Figure 3-46.

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

Backup Configuration Settings [Backup](#)

Factory Default Restore [Restore](#)

Restore Configuration Settings

Restore Mode Batch Config Sync(Skip IP)

[Browse](#) [Upload backup](#)

Only upload *.tar.gz file

Local Upgrade

Keep Settings ☒ Yes ☐ NO

Check Firmware ☒ Yes ☐ NO

Firmware File

[Browse](#) [Upgrade...](#)

Only upload *.bin file

Figure 3-46 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-MIR652R-20230427172519.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 dialing up the router RESET button for more than 7 seconds and then dialing it down.
- **Configuration recovery mode:** The configuration recovery mode supports batch synchronization and local/replacement recovery. Batch synchronization does not modify the LAN IP of the device, and local/replacement recovery will modify the LAN IP of the device as the parameter of the backup file.
- **Upload backup:** Select the backup parameter configuration file, such as backup-MIR652R-20230427172519.tar.gz, and then click the "Upload Backup" button, the router will save the uploaded parameters and upload them after restarting parameters to take effect.
- **Keep settings:** When flashing new firmware, you can choose whether to keep the current parameter settings of the router, and the default settings are kept (when the version to be upgraded has a large span or the version is upgraded forward, it is recommended to choose not to keep the settings for upgrade).
- **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 MIR652R-1.1.08543d5.230523REC.bin, and then click the "Flash Firmware" button, the router will first check the integrity of the firmware, and then burn the firmware to the system and restart automatically. The flashing firmware process takes about five minutes.

Notice

- Restoring the factory settings will cause all the parameters of the device to be at the factory settings, and the IP address of the LAN port will be restored to "192.168.16.253". Users need to use this IP address to access the WEB management interface;
- In the operation of uploading the backup configuration file, do not select the configuration file of a non-4G router. Uploading an incorrect file may cause damage to the router;
- Do not cut off the power during the operation of uploading the backup configuration file, otherwise the 4G router may be damaged;
- When flashing the firmware, please pay attention to the matching of the device model and version. Using an upgrade program that does not match may cause permanent damage to the 4G router;
- The entire firmware upgrade process is not allowed to cut off the power, which may cause permanent damage to the 4G router. If there is an accidental power failure during the upgrade process, please mail the product to our company immediately for possible solutions;
- If the settings are disordered, consider restoring the 4G router to the factory settings and then reset reasonable parameters;

3.7.5 Scheduled task

You can set custom plans on this page, as shown in Figure 3-47.

Scheduled Tasks

Customize the scheduled tasks in the system Crontab

```
# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan, feb, mar, apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun, mon, tue, wed, thu, fri, sat
# | | | | |
# * * * * * user-name command to be executed
```

Save

Figure 3-47 Scheduled task page

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

3.7.6 System log

The router provides system log management functions, mainly including remote logs, local log recording and saving, and viewing and downloading, as shown in Figure 3-48, 3-49, and 3-50.

Remote Log Local Log View & Download

Remote Log **Disable** Enable

Remote Address

Remote Port 1-65535

Save Apply

Figure 3-48 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

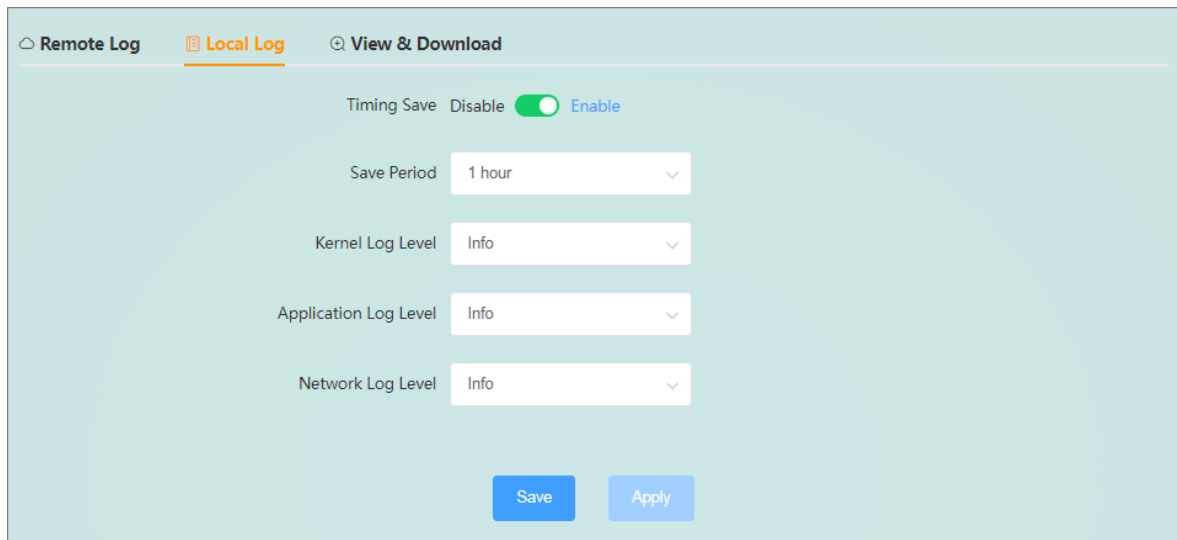


Figure 3-49 Local log interface

- Timed save: local log timed save switch, enabled by default
- Storage cycle: The cycle setting for saving local logs at regular intervals. By default, the logs are saved and backed up once every hour. It supports the functions of saving logs after power failure and saving logs immediately after system restart
- Kernel/application/network log levels: System logs are divided into kernel, application and network logs, and log levels can be set. The log level is defined as 8 levels, which are debug, information, attention, warning, error, critical, warning, and emergency in order. Debug is the lowest and emergency is the highest in order; the default log level is information level.

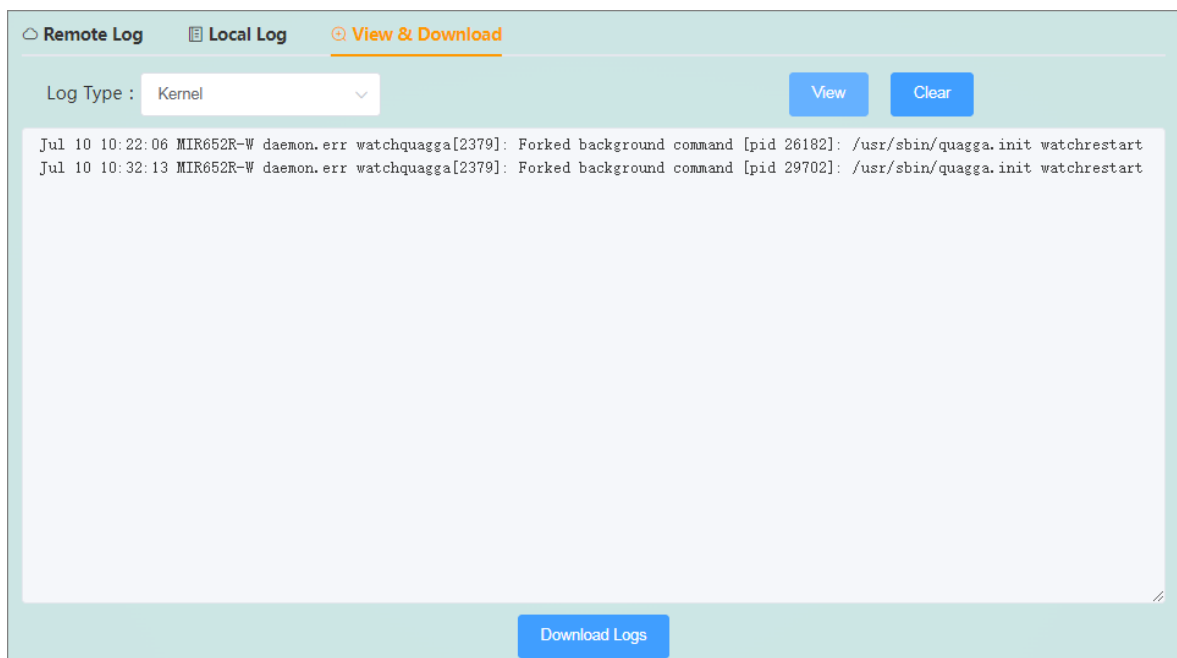


Figure 3-50 View and download page

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

4 WEB Advanced Function Configuration

The advanced functions of the router are mainly located in the service module. Service modules include serial port to network, peanut shell intranet penetration, dynamic DNS, VPN (client and service device), SNMP settings, LLDP settings.

4.1 Serial port to network

4.1.1 Network

This device supports 1 RS232/485 serial port, which can convert serial port data into TCP/IP network data, realize two-way transparent transmission of serial port and TCP/IP network interface data, and facilitate serial device networking. The serial port to network interface includes six parts: network, serial port, heartbeat package, registration package, timeout restart, and data encryption. The network parameter configuration page is shown in Figure 4-1.

Serial To Network

Serial Port No.

COM1

Serial Port Status

Disable

☒

Enable

Network

Serial Port

Heartbeat Packets

Register Packets

Timeout Restart Interval

Data Security

Network Mode

UDP

Local Port

51001

Number Of Network Connections

No.	Status	Destination Address	Destination Port
1	☒	192.168.30.140	51501
2	☐	192.168.30.140	51502
3	☐	192.168.30.140	51503
4	☐	192.168.30.140	51504
5	☐	192.168.30.140	51505
6	☐	192.168.30.140	51506
7	☐	192.168.30.140	51507

Figure 4-1 Network parameter configuration interface

The detailed configuration parameters of this interface are shown in Table 4-1.

Table 4-1 Network configuration parameter list

Network parameters	
working mode	This device supports the following working modes: Modbus RTU Master, Modbus RTU Slave, Modbus ASCII Master, Modbus ASCII Slave, UDP, UDP Multicast, TCP Client, TCP Server, RealCOM_MCP, RealCOM_CCP, RealCOM_MW, Pair Connection Master, Pair Connection Slave, Httpd Client, WebSocket Client, MQTT, etc. 16 types Communication methods are available. The factory default setting is UDP mode.
Modbus RTU Master	When the working mode of this device is Modbus RTU Master, if the Modbus Over TCP function is not enabled, the remote device must work in Modbus TCP Slave mode; otherwise, enable the Modbus Over TCP function, The remote device must work in Modbus RTU Slave mode, which supports up to 16 connections.
Modbus RTU Slave	When the working mode of this device is Modbus RTU Slave, if the Modbus Over TCP function is not enabled, the remote device must work in the Modbus TCP Master mode; otherwise, enable the Modbus Over TCP function, The remote device must work in Modbus RTU Master mode, which supports up to 32 connections.
Modbus ASCII Master	When the working mode of this device is Modbus ASCII Master, if the Modbus Over TCP function is not enabled, the remote device must work in the Modbus TCP Slave mode; otherwise, enable the Modbus Over TCP function, The remote device must work in Modbus ASCII Slave mode, which supports up to 16 connections.
Modbus ASCII Slave	When the working mode of this device is Modbus ASCII Slave, if the Modbus Over TCP function is not enabled, the remote device must work in the Modbus TCP Master mode; otherwise, enable the Modbus Over TCP function, The remote device must work in Modbus ASCII Master mode, which supports up to 32 connections.
UDP/UDP Multicast	When the working mode of this device is UDP, the remote device must also work in UDP mode. This device can establish a UDP connection with up to 16 remote devices, and the IP address and port number of the remote device can be configured on the page. When the working mode of this device is UDP Multicast, it is required that the remote device must work in UDP Multicast mode. This device can join up to 16 UDP multicast groups, and the multicast IP address and port number can be configured on the page.
TCP Client/ TCP Server	When the working mode of this device is TCP Client, it is required that the remote device must work in TCP Server mode, and its IP address and port number must be configured, which can be configured in the options corresponding to the network connection . When the working mode of this device is TCP Server, it is required that the remote device must work in TCP Client mode. In this mode, up to 32 remote TCP Client connections are accepted.
RealCOM_MCP/ RealCOM_CCP/ RealCOM_MW	When the working mode of this device is RealCOM_MCP, RealCOM_CCP or RealCOM_MW, the corresponding virtual serial port software needs to be installed on the PC for use. The virtual serial port software maps the serial port of the remote

	device to the local serial port, so as to realize the transparent communication between the original serial port software and the serial port of the device. One serial port of this device supports up to 32 virtual serial port accesses.
Pair Connection Master/Pair Connection Slave	When the working mode of this device is Pair Connection Master mode, it is required that the remote device must work in Pair Connection Slave mode, and its IP address and port number must be configured. Configure in the options. When the working mode of this device is Pair Connection Slave, it is required that the remote device must work in Pair Connection Master mode. In this mode, up to 32 remote Pair Connection Master connections are accepted.
Httpd Client	When the working mode of this device is Httpd Client, the user needs to specify the address, port, method and other parameters of the remote httpd server. The device will submit the data received by the serial port to the httpd server in the form of GET or POST. At the same time, the data sent by the httpd server can also be transparently transmitted to the serial port.
WebSocket Client	When the working mode of the device is WebSocket Client, the user needs to specify the main parameters such as the address, port, and method of the WebSocket server, and can also set the Ping interval to maintain the connection between the device and the server. The device will upload the data received by the serial port to the WebSocket server in hexadecimal format, and can also transparently transmit the data sent by the server to the serial port
MQTT	When the working mode of this device is MQTT, the user needs to select the server platform type, and the optional platforms include Alibaba Cloud, OneNet, Huawei Cloud, Maiwe Cloud, Tencent Cloud, and other clouds. Then configure the MQTT address, port number, subscription topic, device key, etc. The device will send the data received by the serial port to the cloud platform. The data sent by the cloud platform can also be transparently transmitted to the serial port.
local port	Local port on the network connection side.
SSL encryption	The encryption method and authentication method of the network connection. One-way authentication means that the device only verifies the encryption authentication certificate of the remote server; two-way authentication means that both the device and the remote server need to verify the certificates of both parties.
Certificate Scheme	Select a certificate scheme for encryption. The user selects a certificate scheme for the network connection of this serial port.
certificate type	Select the type of encryption certificate. Allow expired certificates means that the device accepts expired authentication certificates, and reject expired certificates means that if the certificate uploaded by the user has expired, the connection will not succeed. Accepting self-signed certificates means that the device allows users to self-sign certificates, and accepting commercial certificates means that the device accepts certificates issued by commercial organizations.
heartbeat interval	When the network working mode is in TCP mode, a TCP heartbeat detection packet is sent at the specified interval to test whether the connection exists, and if it does not exist, the connection will be automatically disconnected, ranging from 1 to 6000 seconds.

overtime time	When the network working mode is in TCP mode, it detects the idle time of the current connection and the corresponding serial port, and disconnects the TCP connection when it exceeds the set value.
encryption method	Crypto_DES_ECB/Crypto_DES_CBC/Crypto_DES_NCBC/Crypto_DES_PCBC/ Crypto_DES_CFB/Crypto_DES_CFB64/Crypto_DES_OFB/Crypto_DES_OFB64/ Crypto_3DES_ECB/Crypto_3DES_CBC/Crypto_3DES_CFB/Crypto_3DES_CFB64/ Crypto_3DES_OFB64/Crypto_AES_ECB/Crypto_AES_CBC/Crypto_AES_CFB1/ Crypto_AES_CFB8/Crypto_AES_CFB128/Crypto_AES_OFB128/Crypto_RC2_ECB/ Crypto_RC2_CBC/Crypto_RC2_OFB64/Crypto_RC4/Crypto_BlowFish_ECB/ Crypto_BlowFish_CBC/Crypto_BlowFish_CFB64/Crypto_BlowFish_OFB64/ Cryptonone
Filling method	PCKS5 padding, PCKS7 padding, Zero padding, ANSI X9.23 padding, ISO10126 padding, no padding
Number of network connections	
destination address	The IP address of the network connection peer
purpose terminal	The port number of the peer end of the network connection
Number of network connections in Modbus_RTU/ASCII_Master mode	
destination address	The IP address of the network connection peer
purpose terminal	The port number of the peer end of the network connection
Modbus ID range	The data whose Modbus slave ID is within this range will be forwarded to the corresponding destination network address

4.1.2 Serial port

The serial port page displays RFC2217, baud rate, data bits, stop bits, parity bits, packing time, packing length, frame header and frame tail mode, start byte, end byte, total number of received and total number of sent , as shown in Figure 4-2:

Network

Serial Port

Heartbeat Packets

Register Packets

Timeout Restart Interval

Data Security

RFC2217

Disable

Enable

(Only TCP Client and TCP Server mode are valid)

	The Actual Value	Configuration Value
BaudRate	9600	115200
DataBits	8	8
StopBit	1	1
ParityBit	None	None
Packing Interval(ms)	50	(0-255)
PackingLength(Byte)	1000	(0-1460)

Frame Head Frame Tail Mode

Disable

Enable

Start Byte

0x00

(HEX:0x00-0xff)

End Byte

0xff

(HEX:0x00-0xff)

Receive Bytes

0

Bytes

Send Bytes

0

Bytes

Save

Figure 4-2 Serial port parameter configuration interface

- RFC2217: RFC2217 enable control.
- Baud rate: the baud rate of serial communication, the unit is bps.
- Data bits: Set the valid data bits for serial communication.
- Stop bit: Set the stop bit length for serial communication.
- Parity: There are three types of parity, including no parity, odd parity and even parity.
- Packing time: When the time interval between receiving adjacent data by the serial port of the device is greater than the set value, a frame is considered to be over, and the data of this frame is packed and sent to the network end. The unit is milliseconds.
- Packing length: within the packing time, when the data length 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.
- Frame header and frame tail mode: After enabling this mode, the serial port will divide packets according to the start byte and end byte of the frame, and the data packets that do not start with the start byte and end with the end byte will be discarded.
- Start Byte: Set the start byte of the serial port to the range of hexadecimal numbers 0x00~0xff.
- End Byte: Set the end byte range of the serial port to be between 0x00~0xff in hexadecimal.

- Receive Bytes: The number of bytes received by the serial port.
- Sent Bytes: The number of bytes sent by the serial port.

4.1.3 Heartbeat packet

A heartbeat packet refers to a custom command word that regularly notifies the other party of its status between the client and the server, and is sent at a certain time interval, as shown in Figure 4-3:

Figure 4-3 Heartbeat packet configuration interface

- Heartbeat packet function: the sending method of heartbeat packets. Disable: disable this function; send heartbeat to the serial port terminal: send the heartbeat packet to the serial port direction; send heartbeat to the server: send the heartbeat packet to the network port direction. This function is only allowed when the network working mode is UDP, TCP Server and TCP Client.
- Heartbeat packet cycle: the time interval for the module to send heartbeat packet data to the serial port terminal or server.
- Heartbeat packet content: the content of the data sent by the module to the serial port terminal or server (currently supports hexadecimal format), taking the module working in TCP Client mode as an example, the remote address is set to the IP of the PC, the port The

slogan is 20225. Then enable the heartbeat packet function 1, 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 build a TCP Server on the PC to view the data received by the server, as shown in Figure 4-4:

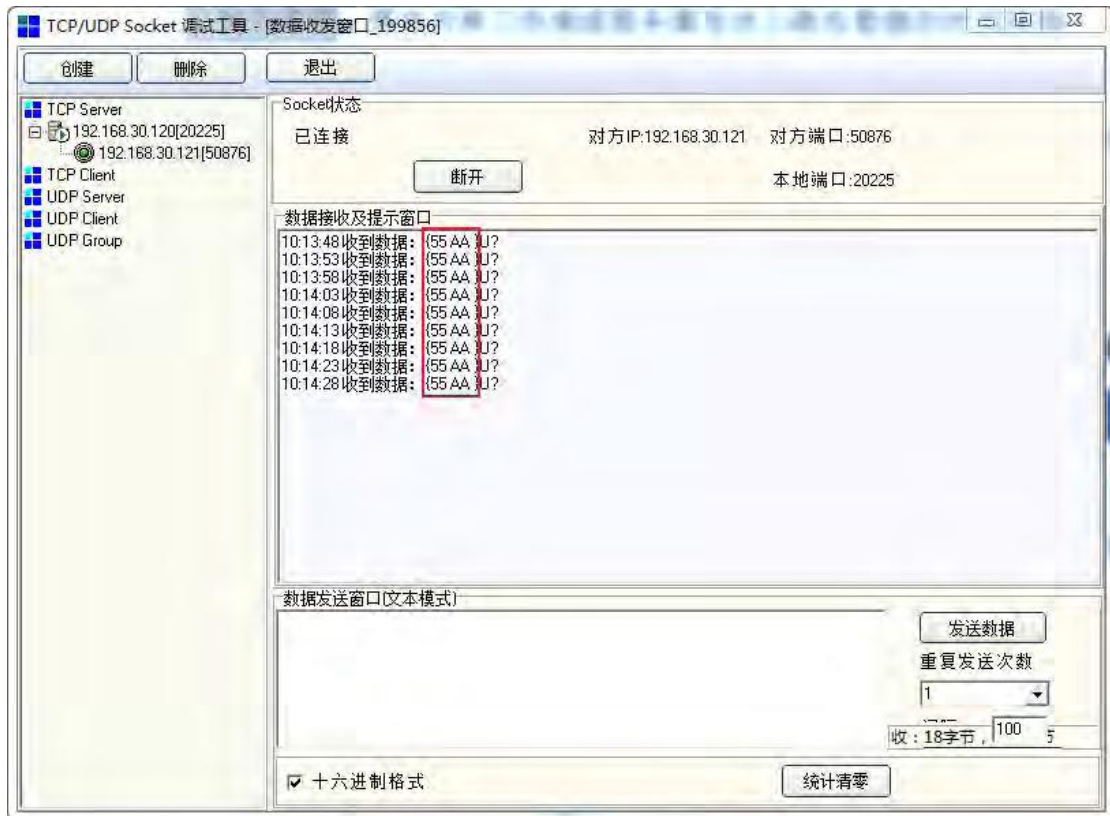


Figure 4-4 TCP Server receives heartbeat data

4.1.4 Registration package

The registration package is to enable the server to identify the data source device, as shown in Figure 4-5:

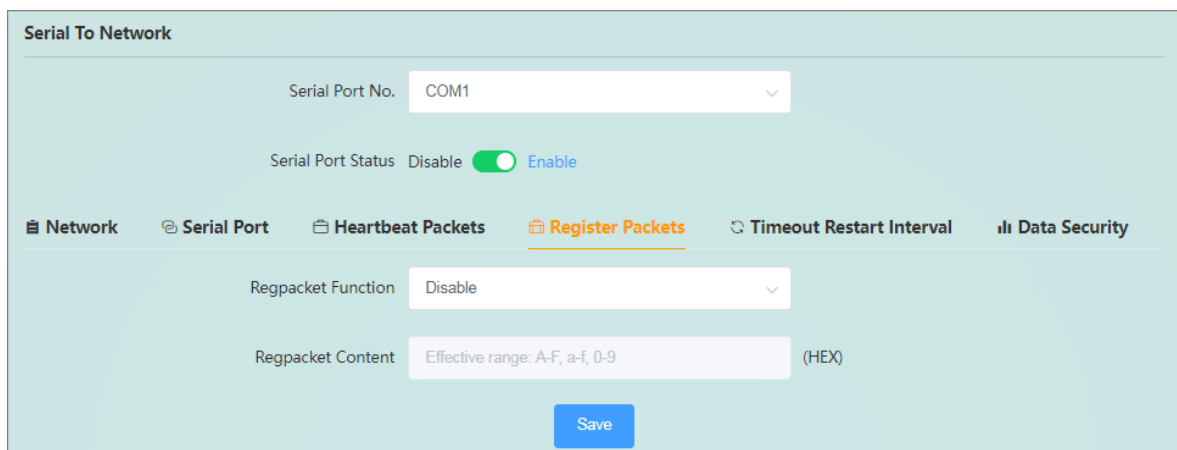


Figure 4-5 Registration package configuration interface

- Registration package function: the sending method of the registration package. Disable: Disable this function; Send once when establishing a connection with the server: The registration packet is only sent once when the network connection is established; Add a registration packet before each frame of data: The registration packet is sent to the network every time When sending data over the network, it is filled in front of the serial port data. This function is only allowed when the network working mode is UDP and TCP Client.
- Registration package content: You can input the content of the data to be sent (currently supports hexadecimal data format, the maximum supported is 64 bytes).

4.1.5 Timeout restart

Timeout restart means that when there is no data in either direction of the network or serial port within a certain period of time, the serial port to network process will restart, as shown in Figure 4-6:

Figure 4-6 Timeout restart configuration interface

- Network no data timeout restart time: The restart time of the network data timeout, setting 0 means turning off this function, setting between 60-65535 means turning on this function, the unit is second.
- Serial port no data timeout restart time: The serial port data timeout restart process time, setting 0 means turning off this function, setting between 60-65535 means turning on this function, the unit is second.

4.1.6 Modbus function

When the serial port works in Modbus mode, the device is equivalent to a Modbus gateway, and the Modbus gateway in this section refers to this device. Next, the Modbus Poll software is used to simulate the master, and the Modbus Slave software is used to simulate the slave.

4.1.6.1 ModbusMaster

Take Modbus RTU Master as an example (the same applies to Modbus ASCII Master):

In RTU Master mode, the RTU master device accesses the TCP slave device through the gateway.

- 1. The RTU master device sends a request to the gateway;
- 2. The gateway forwards the request to the TCP slave device;
- 3. The TCP slave device returns a response;
- 4. The gateway sends back a response.

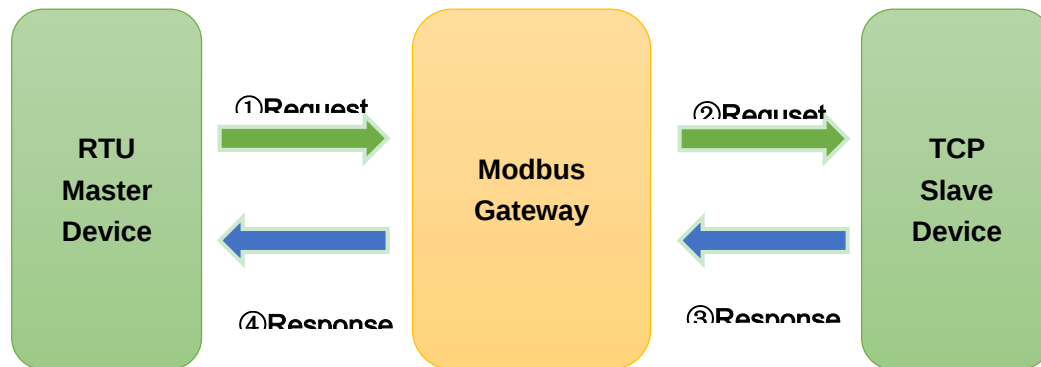


Figure 4-7 Modbus Master mode

Configure the "serial port parameter" of the Modbus gateway to 9600-8-N-1, the working mode in the "network parameter" is Modbus RTU Master, and the network address in the "number of network connections" is configured as a slave IP and port. The physical connection is described as follows:

- Serial port: connect to the host
- Network port: connect to the slave

The configuration parameters of the RTU master station are as follows	Modbus gateway parameter configuration
Serial port number: COM1 Baud rate: 9600 Data bits: 8 Stop bits: 1 Parity bit: None	Destination address 1: 192.168.30.100 Destination: 31501 port: 31501 Modbus ID range: 1-1

Serial To Network

Serial Port No.

COM1

Serial Port Status

Disable

Enable

Network

Serial Port

Timeout Restart Interval

Network Mode

Modbus RTU Master

Modbus Over TCP

Modbus Response Timeout

350

(100-9999)ms

Modbus Initial Time Delay

0

(0-30000)ms

Modbus Character Interval Delay

0

(0,10-500)ms

Modbus From Machine Address Mapping

Virtual Address

1

-

1

(1-247)

Offset Quantity

0

(-246-246)

Real Address

1

-

1

(1-247)

Number Of Network Connections

No.	Status	Destination Address	Destination Port	Modbus ID(1-247)
1	☒	192.168.30.140	51501	1 - 1
2	☐	192.168.30.140	51502	2 - 2

Figure 4-8 Modbus WEB parameter configuration

Modbus Poll software configuration:

- Open the Modbus Poll software, go to "Connect" -> "Connect", the connection parameter configuration and read parameter configuration are as follows:

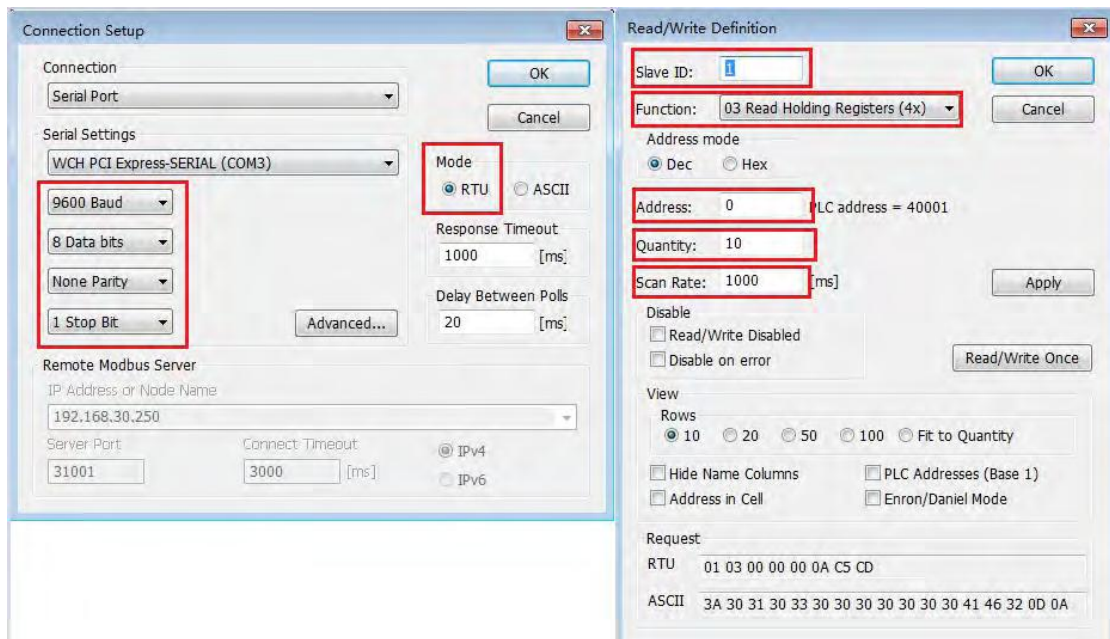


Figure 4-9 Modbus host serial port parameter configuration and read parameter configuration

- Read parameter configuration: the slave ID is 1, the function code is 03, the starting address of the register to be read is 0, the number of registers to be read is 10, and the cycle is read, the interval is 1000ms.
- Open the Modbus Slave software: Go to "Connect"->"Connect", and configure the connection parameters and slave device properties as follows:

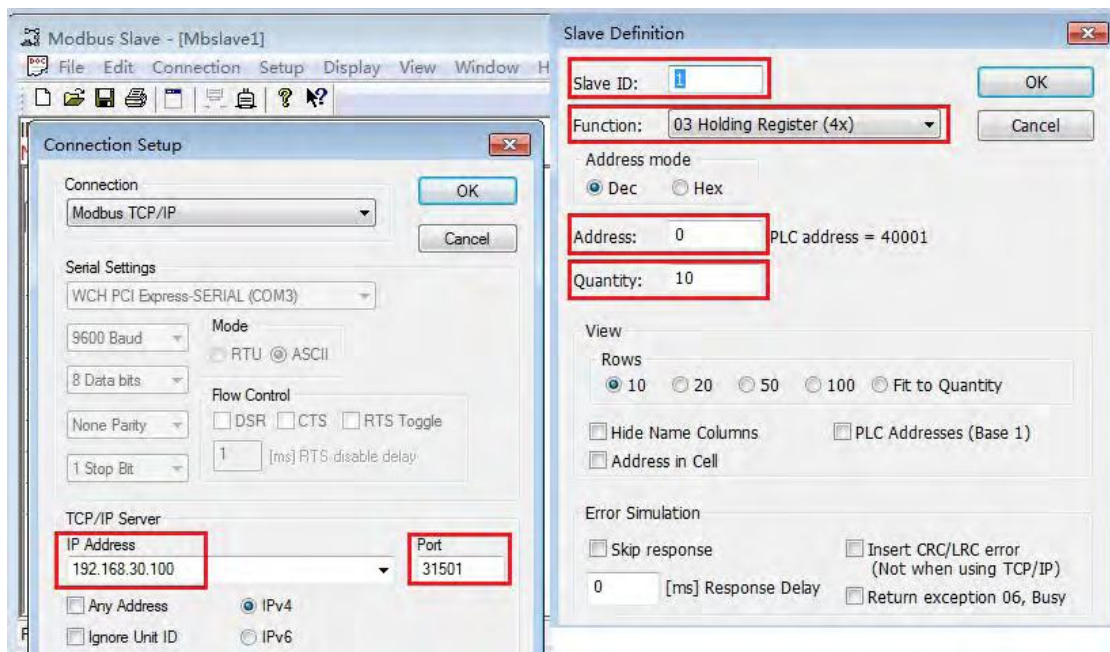


Figure 4-10 Modbus slave connection parameter configuration and slave device property configuration

Slave device definition configuration: the slave ID is 1, the function code is 03, the register start address is 0, and the total number of registers is 10.

View test results:

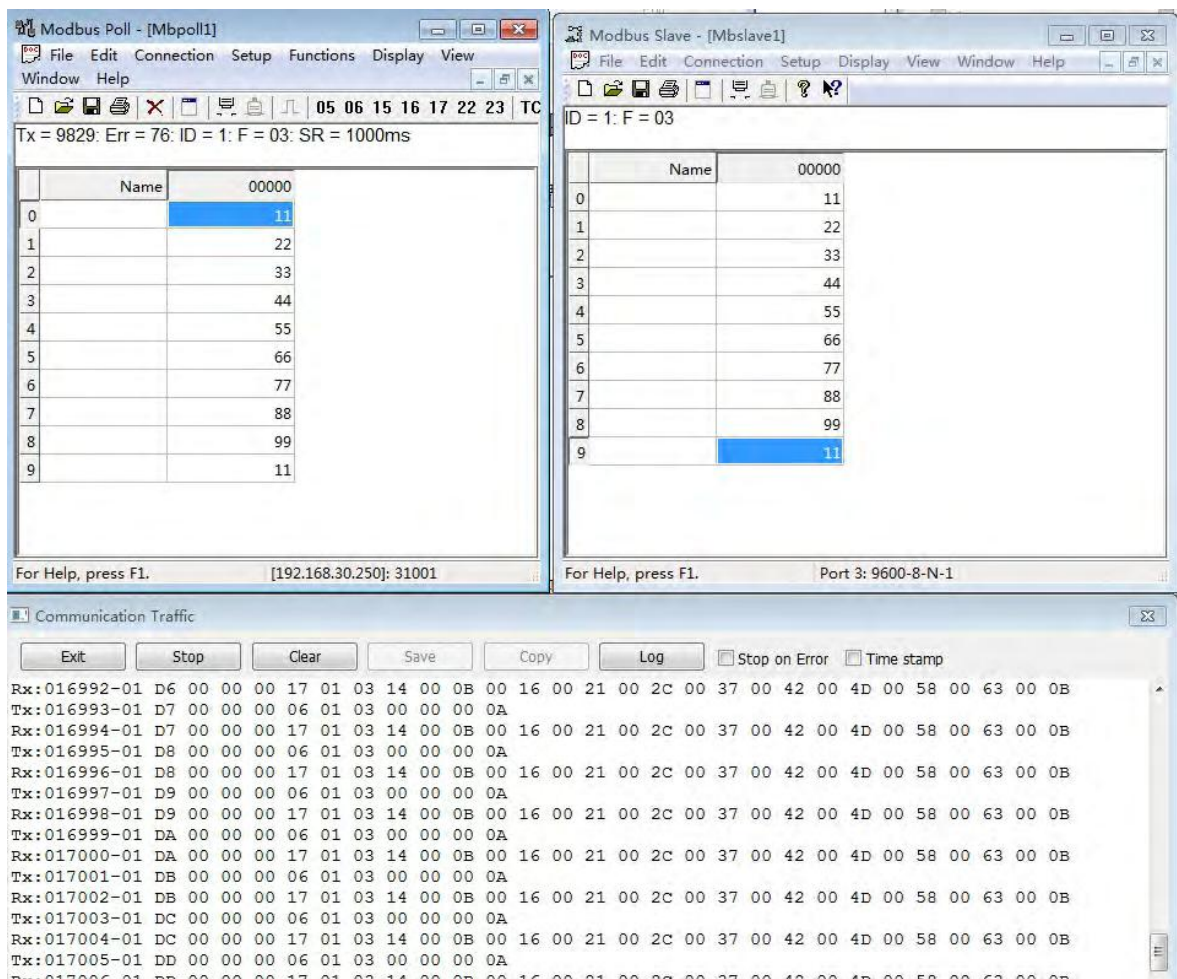


Figure 4-11 The normal response of Modbus slave register value to the host

The communication is normal, and the master can read the register data of the slave through the Modbus gateway device.

4.1.6.2 Slave mode (Modbus Slave)

Take Modbus_RTU_Slave as an example (Modbus ASCII Slave is the same): In Modbus RTU Slave mode, the TCP master device accesses the RTU slave device through the gateway.

1. The TCP master device sends a request to the gateway;
2. The gateway forwards the request to the RTU slave device;
3. The RTU slave device returns a response;
4. The gateway sends back a response.

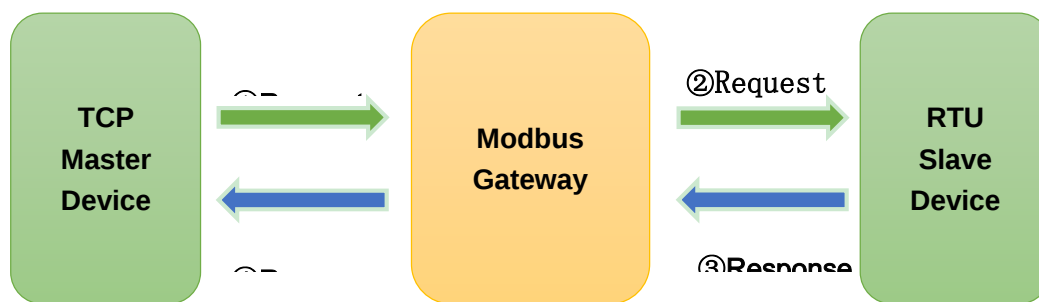


Figure 4-12 Modbus Slave mode

Configure the "serial port parameters" of the Modbus gateway as 9600-8-N-1, the working mode in the "network parameters" as Modbus RTU Slave, and the local port as 31001.

The configuration parameters of the RTU master station are as follows	Modbus gateway parameter configuration
Serial port number: COM1	IP: 192.168.30.250
Baud rate: 9600	Port number: 31001
Data bits: 8	
Stop bits: 1	
Check digit: none	

The physical connection is described as follows:

- Network port: connect to the host
- Serial port: connect to the slave

Serial To Network

Serial Port No.
COM1

Serial Port Status
Disable
Enable

Network
Serial Port
Timeout Restart Interval

Network Mode
Modbus RTU Slave

Local Port
51001

Modbus Over TCP
☐

Modbus TCP Exception
☐

Modbus Response Timeout
350
(100-9999)ms

Modbus Initial Time Delay
0
(0-30000)ms

Modbus Character Interval Delay
0
(0,10-500)ms

Modbus Frame Interval Delay
0
(0,10-500)ms

Modbus ID Filing
☐
1
-
247
(1-247)

Modbus From Machine Address Mapping
☐

Virtual Address
1
-
1
(1-247)

Offset Quantity
0
(-246-246)

Real Address
1
-
1
(1-247)

Modbus Read-ached From Machine
☐

Modbus Polling Time From The Machine
200
(0-65535)ms

Modbus Aging Time Of The Machine Address
60
(10-65535)s

Save

Figure 4-13 Modbus WEB parameter configuration

Open the Modbus Poll software: Go to "Connect" -> "Connect", and configure the connection parameters as follows:

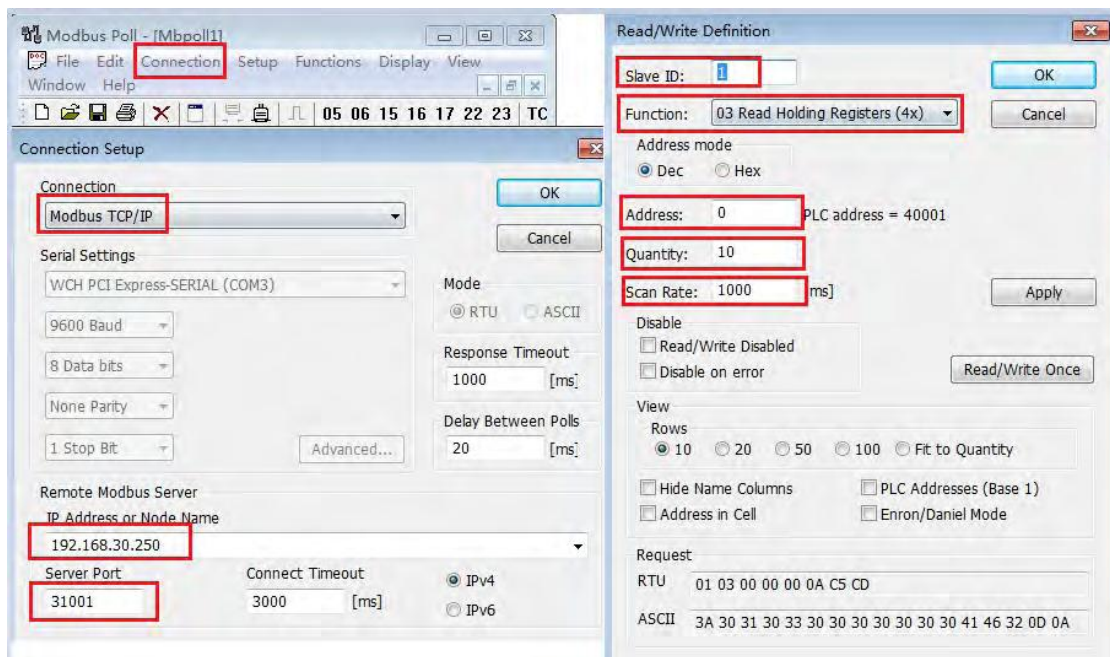


Figure 4-14 Modbus host network connection parameter configuration and device attribute definition

Reading parameter configuration: the slave ID is 1, the function code is 03, the starting address of the register to be read is 0, the number of registers to be read is 10, and the cycle reading interval is 1000ms.

Open the Modbus Slave software: Go to "Connect" -> "Connect", and configure the connection parameters as follows:

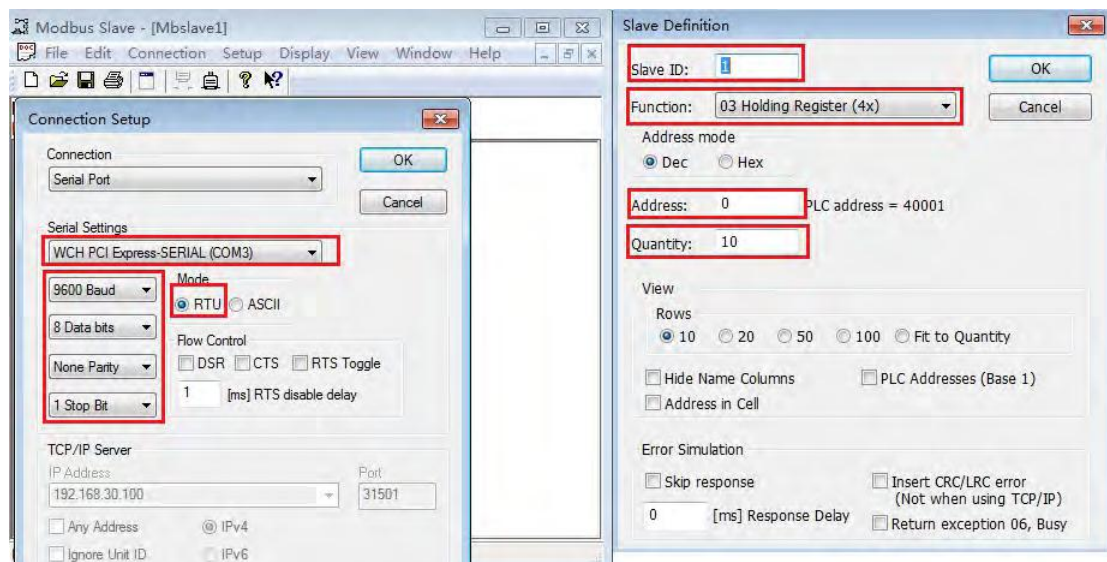


Figure 4-15 Modbus slave serial port parameter configuration and slave property definition

Slave device definition configuration: the slave ID is 1, the function code is 03, the register start address is 0, and the total number of registers is 10.

Test Results:

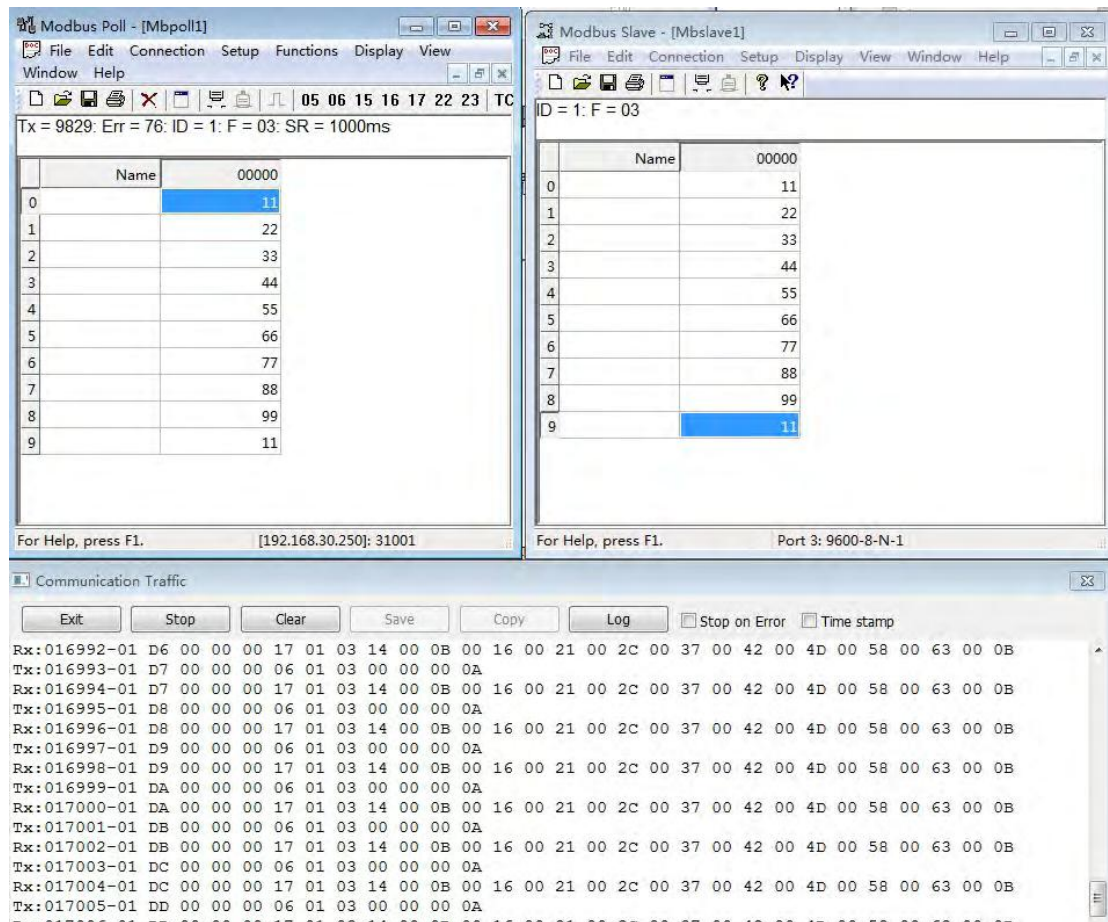


Figure 4-16 The normal response of Modbus slave register value to the host

4.1.6.3 Slave Address Mapping

The Modbus protocol stipulates that all slave devices must have a unique ID number (1~247). This ID number is used to identify the slave address in response to the request from the master device. The Modbus device ID number is set by the manufacturer.

Slave ID mapping: each slave device has 2 ID addresses, namely virtual ID address and real ID address. The real ID exists in the slave device, and other devices directly access the slave device through the real ID. The virtual ID exists in the gateway and is the only access address of the slave device on the gateway. Other devices use the virtual ID to indirectly access the slave device through the gateway.

The screenshot shows the 'Network' configuration tab in the Maiwe software. The 'Modbus From Machine Address Mapping' section is highlighted with a red border. The settings are as follows:

Setting	Value	Range
Network Mode	Modbus RTU Slave	
Local Port	51001	
Modbus Over TCP	☐	
Modbus TCP Exception	☐	
Modbus Response Timeout	350	(100-9999)ms
Modbus Initial Time Delay	0	(0-30000)ms
Modbus Character Interval Delay	0	(0,10-500)ms
Modbus Frame Interval Delay	0	(0,10-500)ms
Modbus ID Filtering	☐ 1 - 247	(1-247)
Modbus From Machine Address Mapping	☒	
Virtual Address	1 - 5	(1-247)
Offset Quantity	2	(-246-246)
Real Address	3 - 7	(1-247)

Figure 4-17 Slave station address mapping function setting

4.1.6.4 Modbus Slave Read Ahead

After the slave pre-reading function is enabled, the Modbus gateway will automatically record up to 256 RTU or 128 ASCII commands, and then automatically execute these commands, and save the results in the Modbus gateway. When the Modbus master sends a command, it can get a quick response.

The screenshot shows the 'Modbus Read-ached From Machine' section in the Maiwe software. The settings are as follows:

Setting	Value	Range
Modbus Read-ached From Machine	☒	
Modbus Polling Time From The Machine	200	(0-65535)ms
Modbus Aging Time Of The Machine Address	60	(10-65535)s

Figure 4-18 Slave pre-read function setting

- **Modbus slave machine polling time:** If the user enables the slave machine pre-reading function, setting this polling time can control the time interval for the Modbus gateway to poll the slave machine.

- Modbus slave address aging time: If the user enables the slave pre-reading function, and a recorded Modbus command exceeds the set time and does not continue to read the command from the slave, the command will be deleted from the Modbus gateway .

4.1.6.5 Modbus Feature Function

The Modbus function of this device also has the following features:

Modbus Over TCP	Modbus (RTU/ASCII) protocol transparent transmission enable
Modbus ID filtering	Filtering of Modbus slave ID ranges
Modbus response timeout	Modbus serial port receiving timeout time, after the gateway forwards the request to the slave device, if it does not receive a response within this parameter time, it will be considered a timeout response.
Modbus initial delay	After the device is powered on, the Modbus message communication starts after a delay.
Modbus TCP exception	When the RTU slave station responds abnormally, the Modbus gateway sends an abnormal message to the TCP master station.
Modbus character interval delay	RTU message sending interval (both master and slave modes are supported).
Modbus frame interval delay	The time interval between the current RTU response and the next RTU request (only supported in slave mode).
Modbus ID mapping (virtual ID, offset, real ID)	When this command is enabled, the Modbus gateway will establish a mapping relationship between the virtual address and the real address according to the offset, and the Modbus gateway will convert the received slave address within the virtual address range into a real slave address, and Request data from the slave, and then convert the real slave address into a virtual address and return it to the Modbus master.
Modbus Slave Read Ahead	After the slave pre-reading function is enabled, the Modbus gateway will automatically record up to 256 RTU or 128 ASCII commands, and then automatically execute these commands and save the results in the Modbus gateway. When the Modbus master sends commands , can get a quick response.
Modbus slave polling time	Interval for polling slaves

The configuration in slave mode is as follows:

Network

Serial Port

Timeout Restart Interval

Network Mode

Modbus RTU Slave

Local Port

51001

Modbus Over TCP

☐

Modbus TCP Exception

☐

Modbus Response Timeout

350

(100-9999)ms

Modbus Initial Time Delay

0

(0-30000)ms

Modbus Character Interval Delay

0

(0,10-500)ms

Modbus Frame Interval Delay

0

(0,10-500)ms

Modbus ID Filtering

☐

1

-

247

(1-247)

Modbus From Machine Address Mapping

☐

Virtual Address

1

-

1

(1-247)

Offset Quantity

0

(-246-246)

Real Address

1

-

1

(1-247)

Modbus Read-ached From Machine

☒

Modbus Polling Time From The Machine

200

(0-65535)ms

Modbus Aging Time Of The Machine Address

60

(10-65535)s

Save

Figure 4-19 Modbus feature function in slave mode

The configuration in master mode is as follows:

Network

Serial Port

Timeout Restart Interval

Network Mode

Modbus RTU Master

Modbus Over TCP

Modbus Response Timeout

350

(100-9999)ms

Modbus Initial Time Delay

0

(0-30000)ms

Modbus Character Interval Delay

0

(0,10-500)ms

Modbus From Machine Address Mapping

Virtual Address

1

-

1

(1-247)

Offset Quantity

0

(-246-246)

Real Address

1

-

1

(1-247)

Number Of Network Connections

No.	Status	Destination Address	Destination Port	Modbus ID(1-247)
1	☒	192.168.30.140	51501	1 - 1
2	☐	192.168.30.140	51502	2 - 2
3	☐	192.168.30.140	51503	3 - 3

Figure 4-20 Modbus feature function in master mode

4.1.7 RealCOM function

In RealCOM mode, the device works with the operating system with RealCOM driver software installed. The RealCOM driver software maps the serial port of the device to the local COM interface of the host, so that the original serial device software or communication module on the host can be used directly without modification.

The RealCOM driver software transparently transmits the data received by the virtual COM interface on the host to the serial port of the device in the form of TCP/IP. The device transparently transmits the data received by the serial port to the virtual COM port of the host in the form of TCP/IP.

This device supports three RealCOM protocols: RealCOM_MCP mode is compatible with Moxa's virtual serial port tool; RealCOM_CCP mode is compatible with Kanghai's virtual serial port tool; RealCOM_MW mode supports Maiwe's virtual serial port tool software.

Serial To Network

Serial Port No. COM1

Serial Port Status Disable ☒ Enable

Network
Serial Port
Timeout Restart Interval
Data Security

Network Mode Realcom MW

Heartbeat Interval 10 (1-6000)s

Timeout 30 (1-65535)s

Save

Figure 4-21 RealCOM function configuration

How to use Maiwe RealCOM:

1. The WEB of this device is configured as RealCOM_MW mode;
2. Install and open Maiwe virtual serial port management software;
3. Click [Add Device], and the add serial port mapping interface will pop up;
4. Click [Scan], the software will scan the devices in the LAN;
5. Select the corresponding device according to the MAC address and IP address;
6. Click [Serial Port Mapping] and wait for the local virtual serial port to be created;

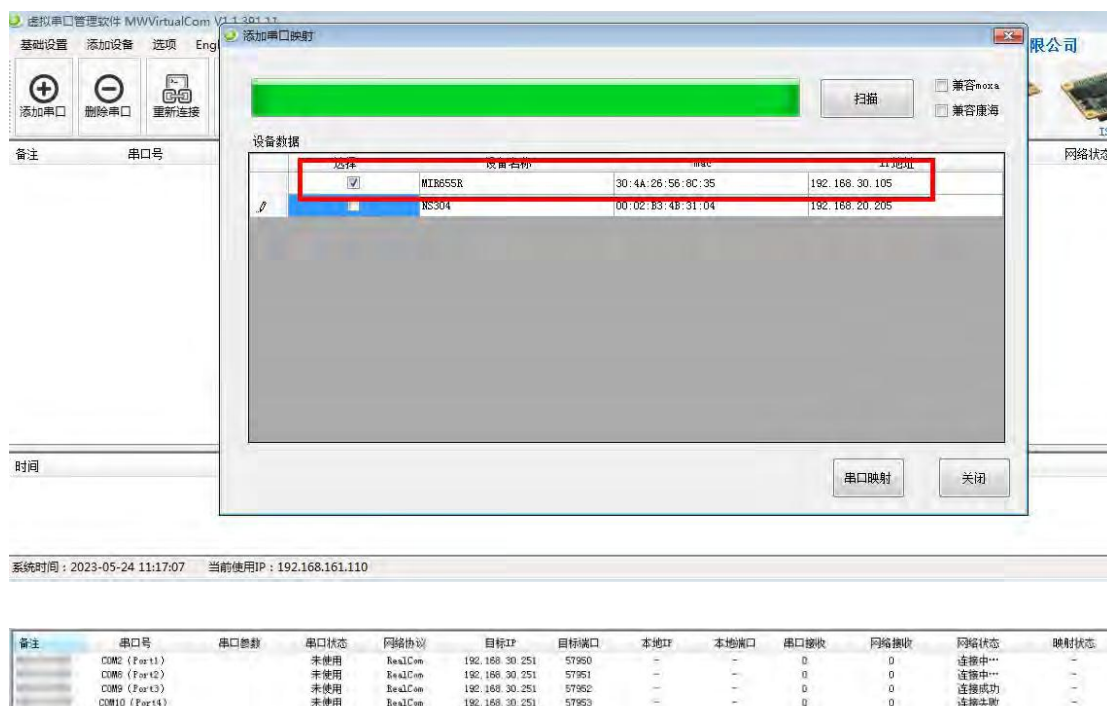


Figure 4-22 Virtual serial port management software creates a virtual serial port

Connect the serial port of this device with the real serial port on the host, and use the serial port debugging tool to open the serial port created by the virtual serial port management software and the host respectively. The real serial port on the computer, and the two send data to each other for testing.



Figure 4-23 Virtual serial port communication test

4.1.8 Httpd Client function

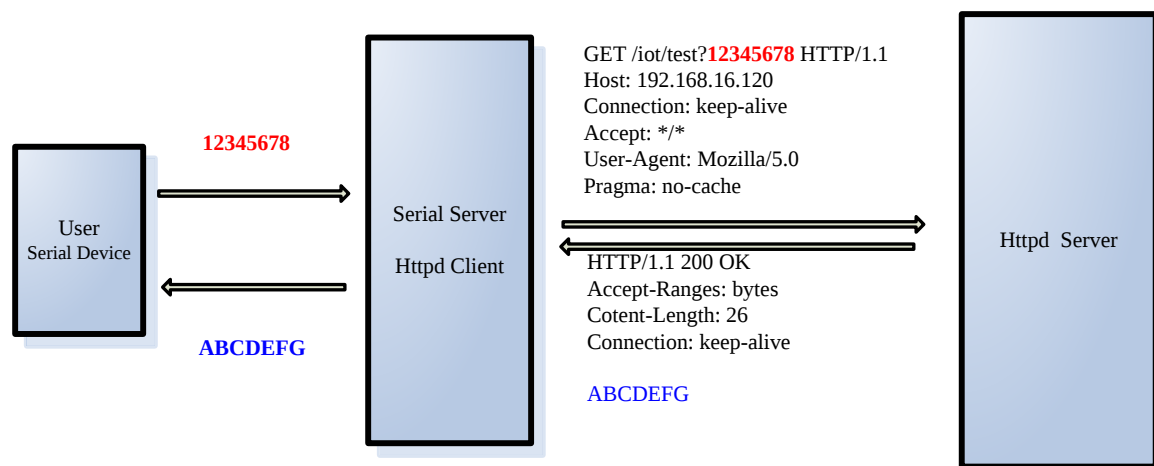


Figure 4-24 Httpd Client mode introduction

This function is that the device submits the data received by the serial port to the HTTP server in the form of HTTP. If the HTTP server has data to be delivered, the device transparently transmits the HTTP body data to the serial port.

Specific usage method:

1. Select "Httpd Client" as the working mode;
2. Fill in the HTTPD address, that is, the HTTP server address, which can be an IP address or a domain name (the ability to connect to the external network is required);
3. Fill in the HTTPD port number;
4. The HTTPD method needs to fill in the correct URL path, and select the GET or POST method as required;
5. The user fills in the HTTPD request header as required;
6. Finally click the Configure button to save the parameters.

Serial To Network

Serial Port No.

COM1

Serial Port Status

Disable

Enable

Network

Serial Port

Timeout Restart Interval

Data Security

Certificate Status

Network Mode

Httpd Client

SSL Security

Disable

HTTPD Address

192.168.30.180

HTTPD Port

8080

(1-65535)

HTTPD Method

/iot/test

GET

HTTPD Request Header

Connection: keep-alive\r\nAccept: */*\r\nUser-Agent: Mozilla/5.0\r\nPragma: no-cache

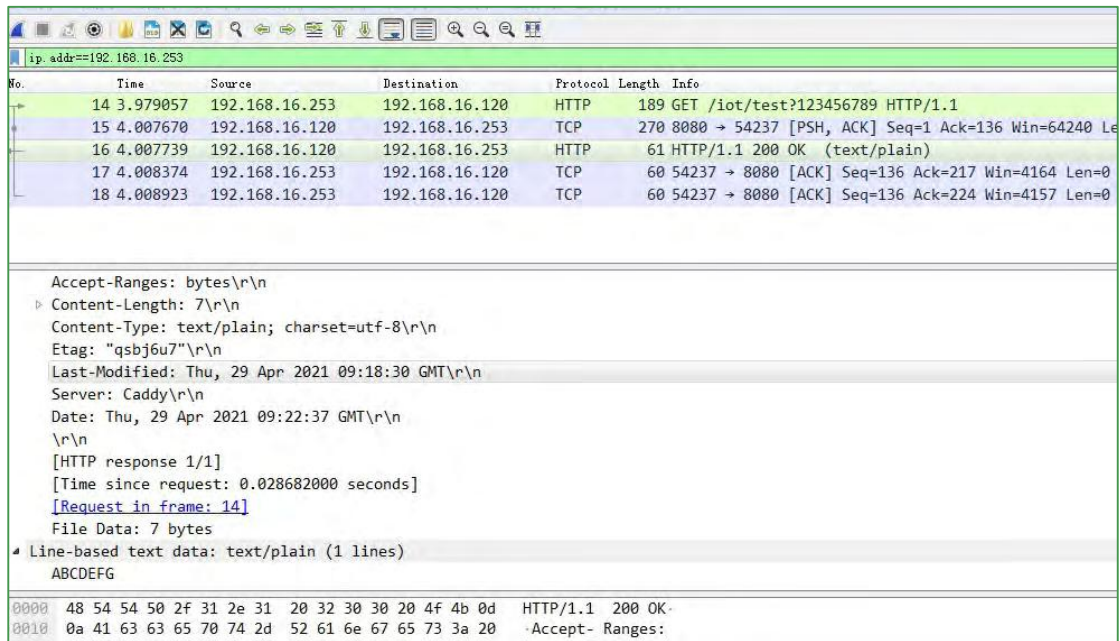
Data Transmission

Transmission Mode

Pass Through

Save

Figure 4-25 Httpd Client configuration introduction



No.	Time	Source	Destination	Protocol	Length	Info
14	3.979057	192.168.16.253	192.168.16.120	HTTP	189	GET /iot/test?123456789 HTTP/1.1
15	4.007670	192.168.16.120	192.168.16.253	TCP	270	8080 → 54237 [PSH, ACK] Seq=1 Ack=136 Win=64240 Len=0
16	4.007739	192.168.16.120	192.168.16.253	HTTP	61	HTTP/1.1 200 OK (text/plain)
17	4.008374	192.168.16.253	192.168.16.120	TCP	60	54237 → 8080 [ACK] Seq=136 Ack=217 Win=4164 Len=0
18	4.008923	192.168.16.253	192.168.16.120	TCP	60	54237 → 8080 [ACK] Seq=136 Ack=224 Win=4157 Len=0

Accept-Ranges: bytes\r\n
Content-Length: 7\r\n
Content-Type: text/plain; charset=utf-8\r\n
Etag: "qsbj6u7"\r\n
Last-Modified: Thu, 29 Apr 2021 09:18:30 GMT\r\n
Server: Caddy\r\n
Date: Thu, 29 Apr 2021 09:22:37 GMT\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.028682000 seconds]
[Request in frame: 14]
File Data: 7 bytes
Line-based text data: text/plain (1 lines)
ABCEFG

0000	48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d	HTTP/1.1 200 OK
0010	0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20	Accept- Ranges:

Figure 4-26 Httpd Client communication Wireshark packet capture example

4.1.9 WebSocket Client function

This function is that the device acts as a WebSocket Client, transparently transmits the data received by the serial port to the WebSocket server in hexadecimal format, and the WebSocket server can also send data to the serial port device at any time.

The screenshot displays the 'Serial To Network' configuration page. At the top, the 'Serial Port No.' is set to 'COM1'. Below it, the 'Serial Port Status' is 'Disable' with a toggle switch set to 'Enable'. A horizontal menu bar contains five items: 'Network' (selected), 'Serial Port', 'Timeout Restart Interval', 'Data Security', and 'Certificate Status'. Under the 'Network' tab, the following settings are visible: 'Network Mode' is 'WebSocket Client'; 'SSL Security' is 'Disable'; 'WebSocket Address' is '192.168.30.180'; 'WebSocket Port' is '8443' with a range '(1-65535)'; 'WebSocket Method' is '/v1'; and 'WebSocket Ping' is '120' with a range '(0-255)s'. Below these is a 'Data Transmission' section with 'Transmission Mode' set to 'Pass Through'. A blue 'Save' button is located at the bottom right of the configuration area.

Figure 4-27 WebSocket Client configuration introduction

Specific usage method:

- Select "WebSocket Client" as the working mode;
- Fill in the address of the WebSocket server, which can be an IP address or a domain name (the ability to connect to the external network is required);
- Fill in the WebSocket server port number;
- The WebSocket method needs to fill in the correct URL path;
- Users can choose the WebSocket Ping time interval according to their needs, filling in 0 means not using the Ping function; 6Finally, click the Configure button to save the parameters.

No.	Time	Source	Destination	Protocol	Length	Info
2655	34.583069	192.168.16.253	192.168.16.120	TCP	60	54241 → 8443 [SYN] Seq=0 Win=4380 Len=0 MSS=1460
2656	34.583138	192.168.16.120	192.168.16.253	TCP	58	8443 → 54241 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M
2658	34.584744	192.168.16.253	192.168.16.120	TCP	60	54241 → 8443 [ACK] Seq=1 Ack=1 Win=4380 Len=0
2670	34.685202	192.168.16.253	192.168.16.120	HTTP	349	GET /v1/websocketTest HTTP/1.1
2671	34.688711	192.168.16.120	192.168.16.253	HTTP	411	HTTP/1.1 101 Switching Protocols
2672	34.689425	192.168.16.253	192.168.16.120	TCP	60	54241 → 8443 [ACK] Seq=296 Ack=358 Win=4023 Len=0
3360	42.334997	192.168.16.253	192.168.16.120	WebSocket	74	WebSocket Binary [FIN] [MASKED]
3363	42.534316	192.168.16.120	192.168.16.253	TCP	54	8443 → 54241 [ACK] Seq=358 Ack=316 Win=64220 Len=0
4094	52.200039	192.168.16.120	192.168.16.253	WebSocket	86	WebSocket Text [FIN]
4095	52.200800	192.168.16.253	192.168.16.120	TCP	60	54241 → 8443 [ACK] Seq=316 Ack=390 Win=3991 Len=0

Frame 3360: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Watanabe_3b:32:08 (00:02:b7:3b:32:08), Dst: AsustekC_41:e3:9a (4c:ed:fb:41:e3:9a)
Internet Protocol Version 4, Src: 192.168.16.253, Dst: 192.168.16.120
Transmission Control Protocol, Src Port: 54241, Dst Port: 8443, Seq: 296, Ack: 358, Len: 20
WebSocket
Data (14 bytes)
Data: 776562736f636b65742054657374
[Length: 14]

0000	4c ed fb 41 e3 9a 00 02 b7 3b 32 08 08 00 45 00	L..A....;2...E.
0010	00 3c 00 1c 00 00 ff 06 18 da c0 a8 10 fd c0 a8	.<.....
0020	10 78 d3 e1 20 fb 00 00 1b e0 51 76 2e 73 50 18	.x.....Qv.sP.
0030	0f b7 64 17 00 00 82 8e 12 34 56 78 65 51 34 0b	.d.....4VxeQ4.
0040	7d 57 3d 1d 66 14 02 1d 61 40	}W=.f...a@

Figure 4-28 Example of Wireshark packet capture for WebSocket Client communication

4.1.10 MQTT function

This function is that the device acts as an MQTT client to communicate with the cloud platform server. The data received by the serial port is sent to the MQTT server, and then the MQTT server can also send messages to the serial port transparently. (The premise is that the device is in a state that can connect to the external network)

Let's take Maiwe Cloud as the MQTT server as an example:

- Platform selection: Maiwe Cloud
- MQTT address: 113.57.111.67
- MQTT port: 1883

For other specific settings, see the figure below:

Network

Serial Port

Timeout Restart Interval

Data Security

Certificate Status

Network Mode

MQTT

SSL Security

Disable

Platform

Ali Cloud

OneNet(Multiprotocol)

OneNet(IoT suite)

Tencent Cloud

Huawei Cloud

Maiwe Cloud

Other Cloud

MQTT Address

113.57.111.67

MQTT Port

1883

(1-65535)

MQTT Ping

60

(10-255)s

MQTT CLIENT ID

Client_ID

MQTT Username

UserName

MQTT Password

Subscription Topic1

/sub1

☒

Publish Topic1

/pub1

☒

Subscription Topic2

/sub2

☐

Publish Topic2

/pub2

☐

Figure 4-29 MQTT configuration introduction

 Notice:

Each server has different MQTT Ping interval requirements, which are:

- Alibaba Cloud: 60-300s, the actual measurement set the ping interval to 30s and it will keep disconnecting and reconnecting;
- onenet:10-1800s;
- Huawei Cloud: 30-120s;
- Tencent Cloud: 0s and above, the actual measurement setting 1s ping interval will always disconnect and reconnect, and the 2s ping interval can be successfully connected;

It is recommended that this value should not be too large or too small, and the typical value is 60s or 120s.

Then log in to Maiwe Cloud:

Find our product device in device management, click to connect.

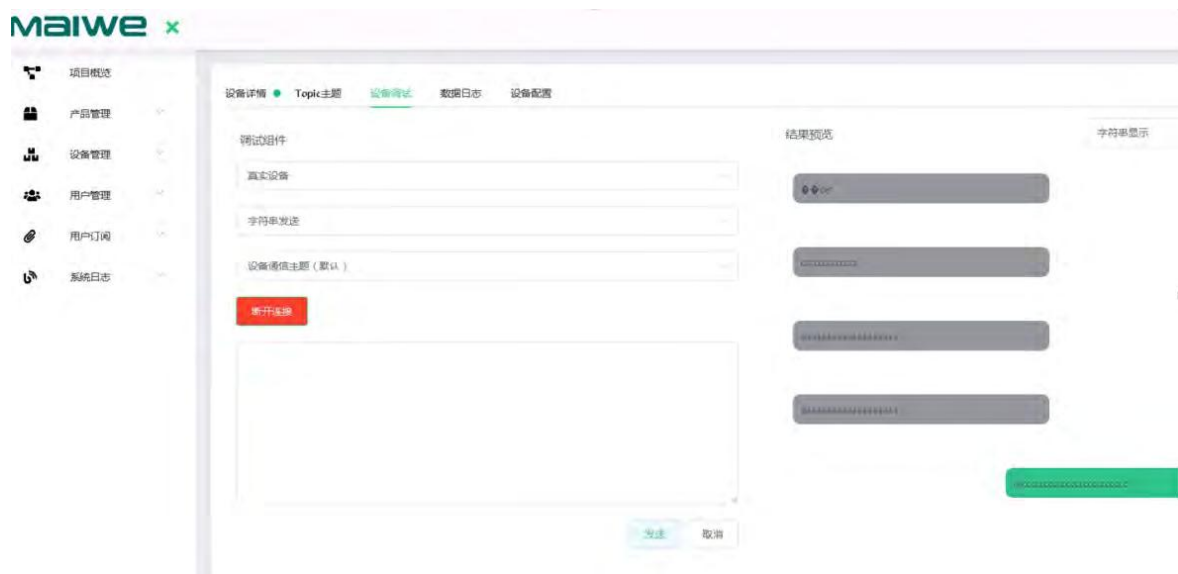


Figure 4-30 MQTT Maiwe cloud platform sending and receiving information example

After connecting, use the serial port tool to open the corresponding serial port, and then send the string, the data can be sent and received normally on the Maiwe cloud server and the serial port, and the MQTT function verification is normal.

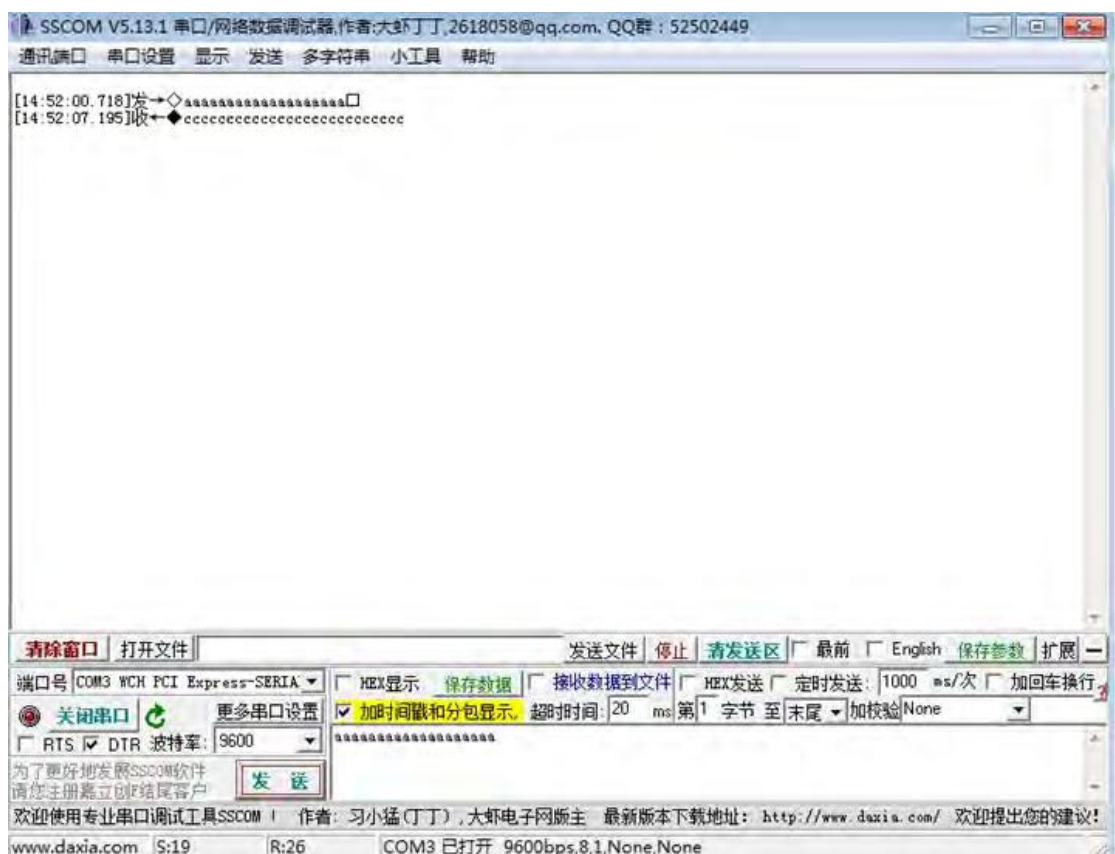


Figure 4-31 Example of sending messages between MQTT serial port and Maiwe Cloud

4.1.11 JSON function

The JSON function is only available in the three working modes of WebSocket Client, Httpd Client and MQTT.

The JSON function is a data reporting function. The serial port is connected to the Modbus Slave device. This product acts as a Modbus Master to collect the data information of the slave device, and then compose JSON format data and send it to the server.

Detailed JSON configuration parameters are shown in Table 4-2.

Table 4-2 JSON configuration parameter table

JSON configuration	
Encoding format	Support GB2312 and UTF-8 two encoding formats. If you need to switch the encoding format, you need to clear the previous format first. Clearing the format will also clear the previous JSON configuration. Determine the encoding format before configuring JSON.
JSON method	JSON data upload or download mode selection
JSON polling interval	The interval time between sending JSON commands to the slave station
JSON timeout	After the gateway forwards the request to the slave device, if it does not receive a response within the parameter time, it is considered a timeout response
Timeout processing	When the timeout expires, fill in the corresponding value to form JSON format data. Clear 00 at timeout/clear FF at timeout/no change at timeout
time prefix	Add time and date information at the front end of the reported JSON data
JSON upload command parameters	
device address	The address of the slave device that needs to be read
function code	JSON upload currently only supports function codes 01, 02, 03, and 04
register address	The corresponding register address of the slave station to be read
number of registers	Number of registers to read
type of data	Supports unsigned integer, signed integer, floating point, Boolean. Send JSON data according to settings
JSON name	The name of the corresponding data when uploading in JSON format
unit	Read the unit corresponding to the value of the corresponding register, which can be set to empty, that is, without a unit.
zoom	The read value is multiplied by the scaling value for data scaling. Example: If the value is magnified by 100 times, fill in 100 for the zoom value. If the value is reduced by 100 times, fill in 0.01 for the zoom value

offset	Offsets the read value. (offset calculation is after scaling)
key value	For the data part, it can be configured as unquoted or with quotes, which can be configured according to the actual situation
JSON delivery command parameters	
keywords	The keyword matched by the issued command
device address	The address of the device to be operated
function code	The function codes that need to be delivered currently only support 05 and 06. If you need to write multiple registers or coil values, you need to configure multiple delivery instructions
register address	The address of the register to be operated

Use of JSON function:

Take the WebSocket Client mode as an example:

First configure the parameters of the serial port WebSocket Client

- WebSocket address: 192.168.30.100 (that is, the PC address of the WebSocket server)
- WebSocket port number: 8443
- WebSocket method: /v1

The screenshot shows a configuration window with a tabbed interface. The 'Network' tab is selected. The settings are as follows:

Parameter	Value	Range/Unit
Network Mode	WebSocket Client	
SSL Security	Disable	
WebSocket Address	192.168.30.180	
WebSocket Port	8443	(1-65535)
WebSocket Method	/v1	
WebSocket Ping	120	(0-255)s

Figure 4-32 WebSocket parameter configuration example

Select JSON as the transmission mode, and then configure a JSON sending command.

- JSON method: JSON upload
- JSON polling interval: 1000ms (the polling interval of JSON commands)
- JSON timeout: 350ms
- Timeout processing: no change in timeout

The screenshot shows the 'JSON Config' window. It includes the following settings:

- JSON Way:** JSON Up Send
- JSON Poll Time:** 1000 (0-65535)ms
- JSON Timeout:** 350 (100-9999)ms
- Time Out Dispose:** Time Out No Change
- Time Prefix:** ☐

Below the settings is an 'Add' button and a table with the following data:

DeviceAddr	FuncCode	RegisterAddr	RegisterNum	Data Type	JSON Name	Unit	Action
1	3	0	1	Unsigned Int	Json_name	unit	Edit Delete

Figure 4-33 Example of JSON upload mode parameter configuration

Open the Modbus Slave software to simulate the slave device, and confirm that the serial port parameter configuration is consistent.

The screenshot shows the 'Modbus Slave - Mbslave1' window. The 'Serial Port' tab is selected. The 'Connection Setup' dialog is open, showing the following settings:

- Connection:** Serial Port
- Serial Settings:** WCH PCI Express-SERIAL (COM3)
- Mode:** RTU
- BaudRate:** 9600
- Data Bits:** 8
- Parity:** None
- Stop Bit:** 1
- Flow Control:** DSR, CTS, RTS Toggle
- TCP/IP Server:** IP Address: 192.168.16.100, Port: 51502

Figure 4-34 Example of serial port parameter configuration and Modbus Slave software configuration

Open a WebSocket server, here we use WebSocketMan.exe software. Configure server parameters, mainly the listening IP address, which is set to the IP address of the device. Click to start monitoring, and the connection from the device side will be received at this time, and the communication will start.



Figure 4-35 Websocket server configuration example

Since the JSON command we configured is to query the slave station whose device ID is 1, check the value of Modbus Slave software register address 1 is 11.

Modbus Slave - [Mbslave1]

File Edit Connection Setup Display View Window Help

D = 1: F = 03

	Name	00000	Name	00010
0		0		0
1		11		0
2		22		0
3		0		0
4		0		0
5		0		0
6		0		0
7		0		0
8		0		0
9		0		0

Figure 4-36 Example of Modbus Slave address value

Then open the Wireshark software to capture packets, and check that the data sent to the WebSocket server on the device is: {Dec202022-11:39:56,"json_name":11unit}, and the value on the corresponding address of the slave device is completed. Convert it to JSON format and send it to the server.

The screenshot displays the Wireshark network protocol analyzer interface. The top bar shows the active filter: `ip.addr==192.168.30.100 and websocket`. The packet list pane shows a series of WebSocket frames between 192.168.30.102 and 192.168.30.100. The selected packet is a WebSocket frame (114 bytes) with the following details:

- Internet Protocol Version 4, Src: 192.168.30.102, Dst: 192.168.30.100
- Transmission Control Protocol, Src Port: 33945, Dst Port: 8443, Seq: 1050, Ack: 358, Len: 48
- WebSocket
 - 1... = Fin: True
 - .000 = Reserved: 0x0
 - 0010 = Opcode: Binary (2)
 - 1... = Mask: True
 - .010 1010 = Payload length: 42
 - Masking-Key: 12345678
 - Masked payload
 - Payload
- Data (42 bytes)
 - Data: 7b44656320323020323032322d31313a333393a35362c226a_
 - [Length: 42]

The packet bytes pane shows the raw data of the frame, with a red box highlighting the timestamp and the 'son name' field:

```

0000 7b 44 65 63 20 32 30 20 32 30 32 32 2d 31 31 3a  (Dec 28 2022:11:
0010 33 39 3a 35 36 2c 22 6a 73 6f 6e 5f 6e 61 6d 65  39:56,"j son name
0020 22 3a 31 31 75 6e 69 74 2c 7d                  ":11unit ,)

```

Figure 4-37 Wireshark packet capture example

JSON delivery function:

JSON method selection: JSON delivery.

Then configure a delivery command:

The device address is 1, the function code is 6, and the register address is 5.



Figure 4-38 Configuration example of sending JSON parameters

Then, the corresponding register value of the slave device is modified on the WebSocket server side by issuing keyword adding values.

The issue format is keyword + colon + value + semicolon, as follows:

keyword: Value;

For example, change the value of the register address 5 of the slave device with device address 1 to 1123, input the instruction keyword: 1123 on the WebSocket server;

Watching the Modbus Slave software revealed that the values were indeed changed to 1123.

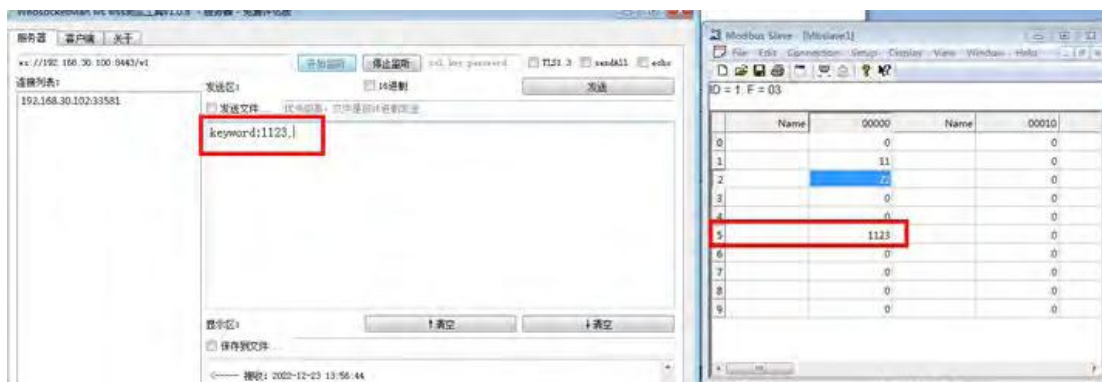


Figure 4-39 Example of implementing the function of sending parameters in JSON

**Notice:**

- Port numbers 80, 443, 4500, 4800, 57050, 57051, 57850, 57851 have been used by the system, please do not reuse them when configuring port numbers.
- The device and the remote device must have the same baud rate, parity bit, data bit and stop bit;
- If the working mode of this device is UDP multicast mode, the same multicast address can only be used once, and a multicast address is not allowed to be used in different serial port configurations.
- When you need to use long-frame data frequently or have high requirements for data transmission, please adjust the baud rate and send interval appropriately to prevent garbled characters or packet loss caused by slow serial port speed.
- When configuring the device, the user should ensure that the external serial device stops sending data to the device to avoid garbled characters.
- Affected by the serial port rate, when the Modbus data times out, the WEB should pay attention to configure the appropriate Modbus receiving timeout time, and at the same time, the read timeout time of the host computer should also be appropriately extended according to the baud rate.
- In the JSON sending function, when the sending function code is 6, the value range entered by the user is -32768~65535, and the value outside the range will be regarded as invalid data. When the issued function code is 5, it is the state of writing the coil, and the issued value is 0 or 1, and other non-zero values will be treated as 1.

4.2 Intranet Through Of Peanut Shell

The peanut shell intranet penetration module supports the use of the peanut shell dynamic domain name for intranet penetration. The bottom layer uses the latest PHTunnel technology of the peanut shell to easily realize remote login and Management, the setting steps are as follows:

1. Peanut shell intranet penetration function is disabled by default, and the preset APP ID and APP Key are used by default (APP ID and APP Key can be changed, and you need to log in to <https://open.oray.com> to register and apply) for login authentication. Select Enable, click Save and Apply, the page will display the SN code and service device status, as shown in Figure 4-40.

Intranet Through Of Peanut Shell

Enable
Disable
☐
Enable

APP ID
11675

APP Key
6bbf268aac69b571

Save
Apply

Figure 4-40 Get the front page of the QR code

When the status is ONLINE, the first login will display the QR code page that needs to be scanned and bound, as shown in Figure 4-41.

Intranet Through Of Peanut Shell

Enable
Disable
☒
Enable

APP ID
11675

APP Key
6bbf268aac69b571

SN Code
OFFLINE

Status
OFFLINE

Save
Apply

花生壳内网穿透

开启
关闭
☒
开启

APP ID
11675

APP Key
6bbf268aac69b571

SN码
phdd2ca08f8f1f47

状态
ONLINE



请使用手机花生壳管理APP扫码

保存
应用

Figure 4-41 Get the QR code page

- After obtaining the QR code, you need to use the "Peanut Shell Management" APP on your mobile phone to scan the code and bind it
- You need to bind an account for the first login. After binding the account, the bound account will be displayed on the page, as shown in Figure 4-42.

Figure 4-42 The page after scanning the QR code and binding it

- Click "Login Management" to automatically jump to the peanut shell management website, (if you can't automatically jump, please check whether the browser allows pop-up windows), and automatically log in to the bound account after the jump , as shown in Figure 4-43. If you want to unbind the currently bound account and re-scan to bind a new account, you can click the "Unbind" button.

Figure 4-43 Peanut shell management page

- Click intranet penetration on the left, and click Add Mapping, as shown in Figure 4-44

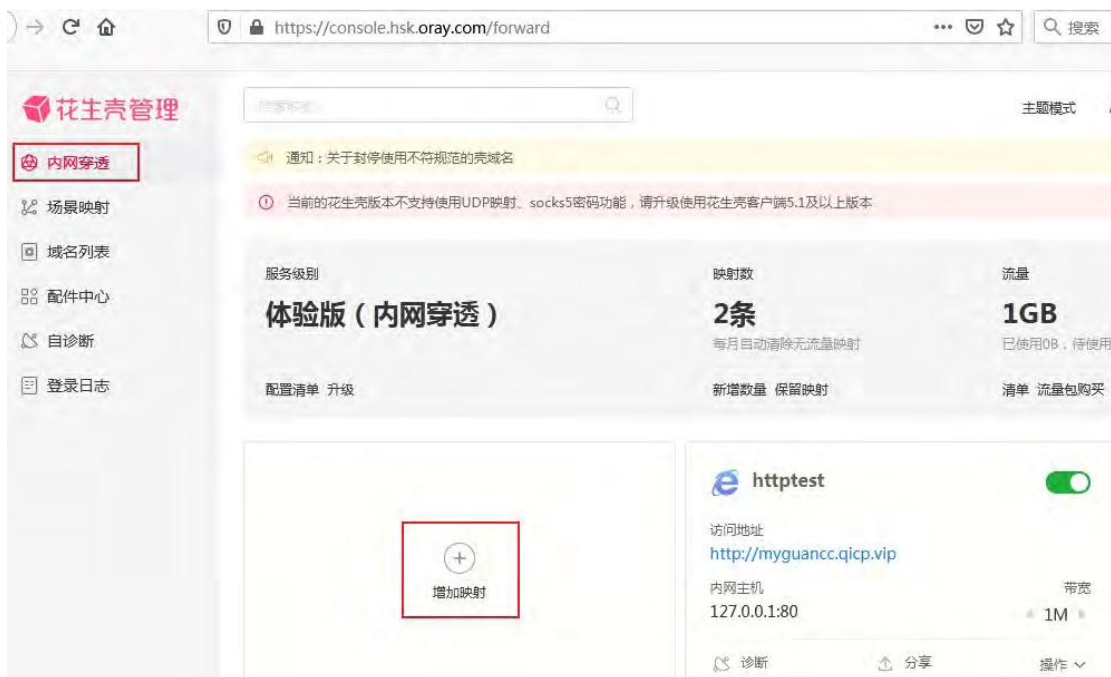


Figure 4-44 Add mapping page

6. Set mapping, add mapping interface as shown in Figure 4-45



Figure 4-45 Add mapping page

- Application name: Set the name of the currently added mapping (arbitrary setting)
- Mapping type: choose any mapping protocol such as TCP/UDP/HTTP/HTTPS

- Extranet domain name: Select the domain name to be mapped in the options (apply for a free domain name or purchase a paid domain name)
- Internet port: You can choose dynamic port (free) or fixed port (need to purchase)
- Intranet host: fill in the IP address of the LAN device that needs to be mapped, if you want to map the router, fill in 127.0.0.1
- Intranet port: fill in the network port number of the LAN device, fill in 80 for the router itself

After setting the mapping parameters, click the OK button to complete adding the mapping.

7. Test domain name login device

For any device that can connect to the Internet, use the domain name set for intranet mapping (you need to add a port number, such as: <http://29955e985h1.qicp.vip:34054>) Remotely log in to the router WEB management interface, as shown in Figure 4-46

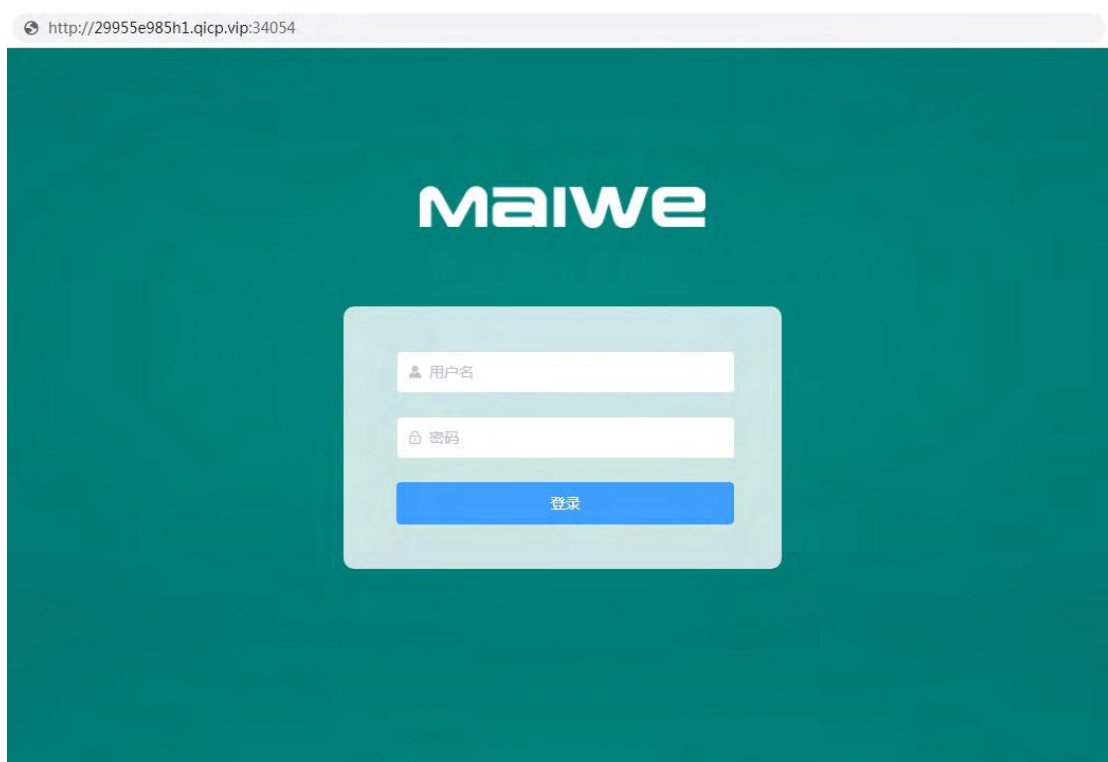


Figure 4-46 Domain name login page

If the mapped domain name does not take effect automatically, you need to manually click the switch button corresponding to the mapping on the intranet penetration page in the peanut shell management interface (turn it off first and then turn it on), as shown in Figure 4-47



Figure 4-47 Switch mapping page

4.3 Dynamic DNS

Dynamic DNS configuration parameters are shown in Figure 4-48

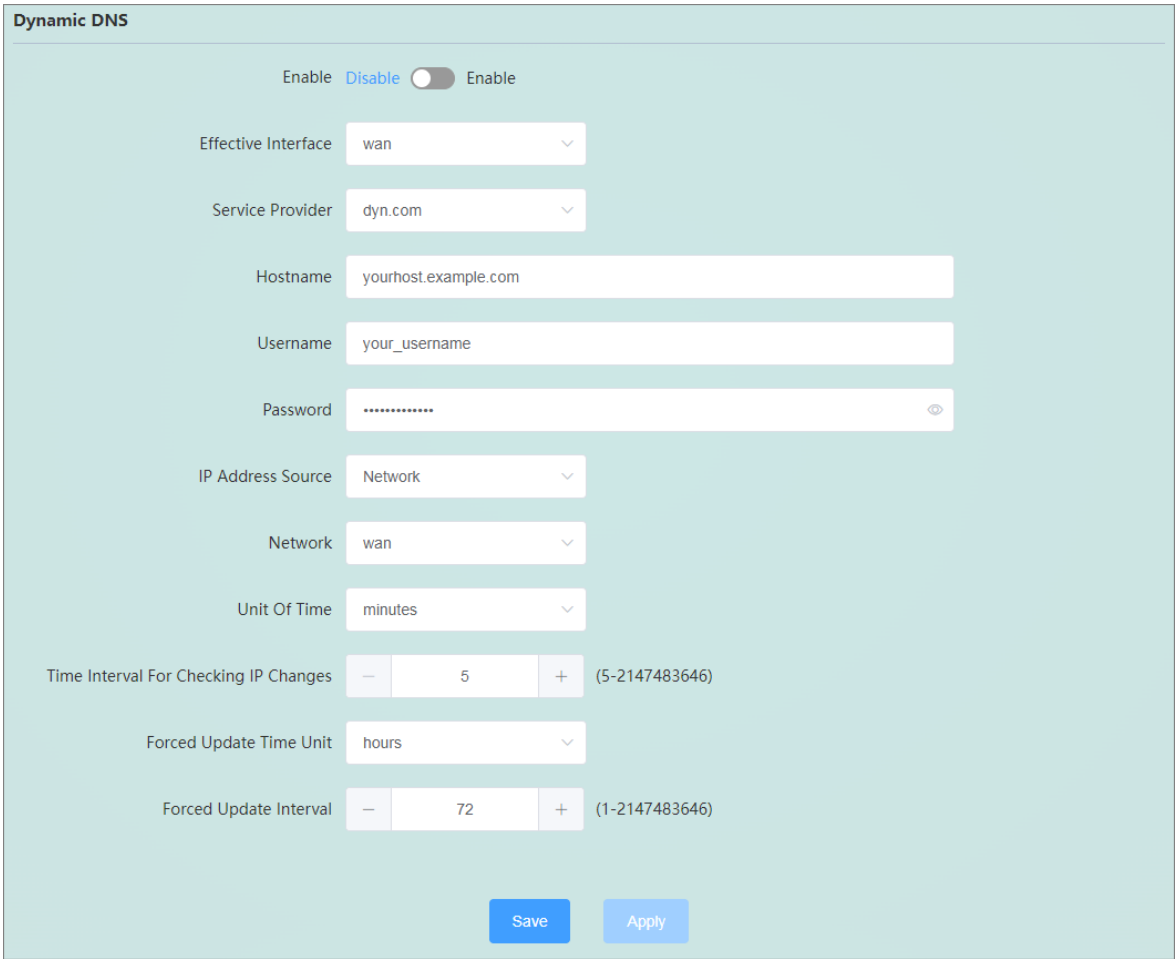


Figure 4-48 Dynamic DNS settings

- **Enable:** Enable or disable DDNS function, DDNS is disabled by default
- **Effective interface:** Select the corresponding WAN port according to the needs, such as wan (wired WAN port), g4wan (4G WAN port)
- **Service provider:** DDNS server address, the above picture uses peanut shells as an example, fill in oray.com. You can also fill in a custom service provider, select the last custom item, fill in the custom DDNS and fill in the updated URL address
- **Update URL:** When the service provider chooses to customize, fill in the custom DDNS URL address here
- **Host name:** fill in the applied domain name
- **Username:** account name of the registered DDNS service provider
- **Password:** Register the password of the DDNS service provider
- **IP address source:** The source of the IP address to be mapped, including interface, script, network, and URL. The network is selected by default.
- **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 three time units: hour, minute, and second
- **Time interval for checking IP changes:** the IP pointed to by the domain name may change frequently, the smaller the value, the more frequent the detection
- **Mandatory update time unit:** including minutes, hours and days
- **Mandatory Update Interval:** Mandatory update time interval

The dynamic DNS function requires 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.

4.4 VPN

4.4.1 VPN

VPN (Virtual Private Network, virtual private network) is a private network built on a public network. 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 further divided into PPTP, L2TP, IPSec, OPENVPN, GRE, etc. The principle of creating VPN for these protocols is introduced as follows.

- **PPTP:** It is a point-to-point tunneling protocol. It uses a TCP (port 1723) connection to maintain the tunnel, and uses general routing encapsulation (GRE) technology to encapsulate data into PPP data frames and transmit them through the tunnel. Encrypt or compress the payload data in the encapsulated PPP frame.

- **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 Both add extra headers to the data.
- **IPSEC:** IPSEC (IP Security, IP Security) is a collection of a series of services and protocols that protect the security of end-to-end communications and prevent network attacks in an IP network. 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 network authentication and
- Some encryption algorithms, etc. The AH protocol and ESP protocol are used to provide security services, and the IKE protocol is used for key exchange.
- **OPENVPN:** It is an application-layer VPN implementation based on the Openssl library. It supports certificate-based two-way authentication, that is to say, the client needs to authenticate the server, and the server also needs to authenticate the client.
- **GRE:** GRE (Generic Routing Encapsulation, general routing encapsulation) protocol is to encapsulate datagrams of certain network layer protocols (such as IP and IPX), so that these encapsulated datagrams can It is transmitted in a network layer protocol (such as IP). GRE adopts Tunnel (tunnel) technology, which is the third layer tunneling protocol of VPN.

4.4.2 VPN client

4.4.2.1 PPTP client

A point-to-point tunneling protocol that uses a TCP port connection to maintain the tunnel, uses general routing packaging technology to encapsulate data into PPP data frames and transmits them through the tunnel, and encrypts or compresses the payload data. Create a new interface for the PPTP client, as shown in Figure 4-49.

Create New Interface

×

Interface Name

1-6 bytes, including numbers, letters and special symbols_

Interface Protocol

PPTP

▼

VPN Server

PAP/CHAP Username

PAP/CHAP Password

Save

Apply

Figure 4-49 Create PPTP client page

- The name of the new interface: 1-6 characters in length, can be numbers, letters or _
- New interface protocol: PPTP protocol must be selected here to create a PPTP client
- 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

PPTP advanced setting parameters are shown in Figure 4-50.

The screenshot shows a 'Modify Interface' window with a dark green header and a close button. Below the header are two tabs: 'Basics' and 'Advanced Settings', with the latter being selected and highlighted in orange. The 'Advanced Settings' section contains three input fields: 'MPPE' with a dropdown menu showing 'Security', 'MTU' with a text box containing '1482', and 'MRU' with a text box containing '1482'. Below these are two checkboxes: 'Set the default route' which is unchecked, and 'Use server-negotiated DNS' which is checked. At the bottom right of the dialog are two blue buttons labeled 'Save' and 'Apply'.

Figure 4-50 PPTP advanced settings page

- MPPE: Set whether to enable MPPE encryption for the PPTP channel, which is enabled by default
- MTU: set the MTU of PPTP channel, the default is 1482
- MRU: set the MRU of PPTP channel, the default is 1482
- Set the default route: Whether to set the system default route for the network interface of the PPTP client, it is not set by default
- Use server-negotiated DNS: Whether to use the DNS server notified by the PPTP server, it is used by default. If the selection is canceled, you can move the DNS server and the DNS server
- DNS server: If you do not use the DNS negotiated by the server, you can set the DNS server address here
- Alternate DNS server: If you do not use the DNS negotiated by the server, you can set the address of the alternate DNS server here

4.4.2.2 L2TP client

The L2TP protocol is a Layer 2 tunneling protocol, similar to the PPTP protocol. Create an L2TP client as shown in Figure 4-51.

Create New Interface

×

Interface Name

1-6 bytes, including numbers, letters and special symbols_

Interface Protocol

L2TP

▼

L2TP server

PAP/CHAP Username

PAP/CHAP Password

L2TP Over IPSEC

Pre-shared Key

Max Length is 255 including digits ~!@#\$\$%^&*()_+

IKE Version

ikev1

▼

Local Identifier

Max Length is 100 including digits ~!@#\$\$%^&*()_+

Peer Identifier

Max Length is 100 including digits ~!@#\$\$%^&*()_+

Save

Apply

Figure 4-51 Add L2TP client interface page

- The name of the new interface: 1-6 characters in length, can be numbers, letters or _
- Protocol of the new interface: L2TP protocol must be selected here when creating an L2TP client
- 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
- Pre-shared key: set the pre-shared key for IPSec encryption
- IKE version: IKE version used for IPSec encryption
- Local identifier: The local identifier of the channel, which can be the local IP or the local domain name. Note that you need to add @ when setting the domain name. When setting, you need to pay attention to the same as the peer identifier of the peer gateway. Sincerely.
- Peer identifier: The peer identifier of the channel, which can be the peer IP or the peer domain name. Note that you need to add @ when setting the domain name. When setting, you need to pay attention to the same as the local identifier of the peer gateway To.

The L2TP advanced setting parameters are shown in Figure 4-52.

Modify Interface [X]

Basics **Advanced Settings**

MTU

MRU

Set the default route ☐

Use server-negotiated DNS ☐

Primary DNS

Secondary DNS

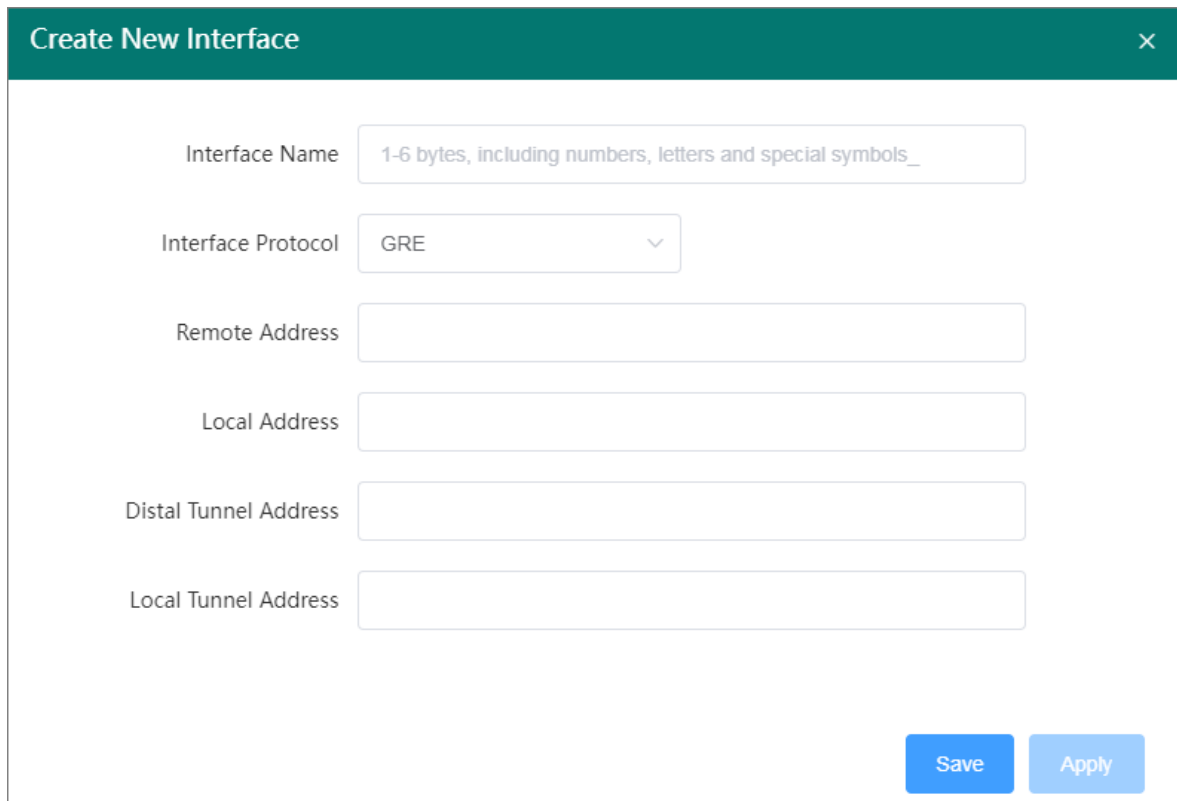
Save **Apply**

Figure 4-52 L2TP advanced settings page

- MTU: Set the MTU of the L2TP channel, the default is 1500
- MRU: Set the MRU of the L2TP channel, the default is 1500
- Set the default route: Whether to set the system default route for the network interface of the L2TP client, it is not set by default
- Use server-negotiated DNS: Whether to use the DNS server notified by the L2TP server, it is used by default. If unchecked, you can manually set the DNS server and alternate DNS server
- DNS server: If you do not use the DNS negotiated by the server, you can set the DNS server address here
- Alternative DNS server: If you do not use the DNS negotiated by the server, you can set an alternate DNS server address here.

4.4.2.3 GRE Client

The GRE protocol encapsulates certain network layer protocols so that these encapsulated datagrams can be transmitted in another network protocol. As shown in Figure 4-53.

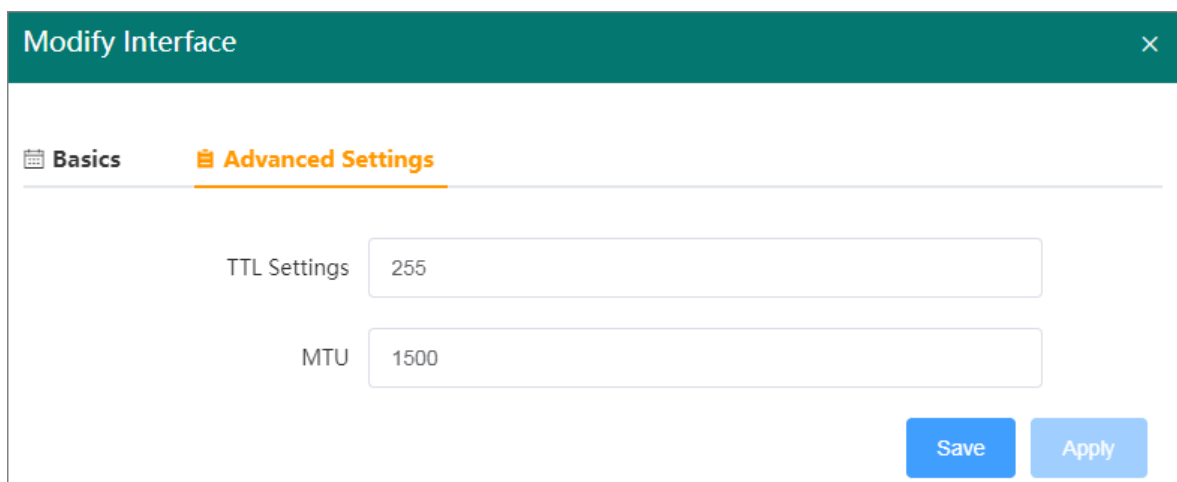


The 'Create New Interface' dialog box features a dark teal header with the title and a close button. The main area is white and contains six input fields: 'Interface Name' with a placeholder '1-6 bytes, including numbers, letters and special symbols_', 'Interface Protocol' with a dropdown menu set to 'GRE', 'Remote Address', 'Local Address', 'Distal Tunnel Address', and 'Local Tunnel Address'. At the bottom right, there are two blue buttons labeled 'Save' and 'Apply'.

Figure 4-53 GRE protocol

- The name of the new interface: 1-6 characters in length, can be numbers, letters or _
- Protocol of the new interface: to create a GRE client, the GRE protocol must be selected here
- Remote address: WAN port IP address of peer GRE
- Local address: address of local WAN port (wired WAN port), g4wan port (4G WAN port)
- Remote tunnel address: peer GRE tunnel IP address
- Local Tunnel Address: local GRE tunnel IP address

GRE advanced setting parameters are shown in Figure 4-54.



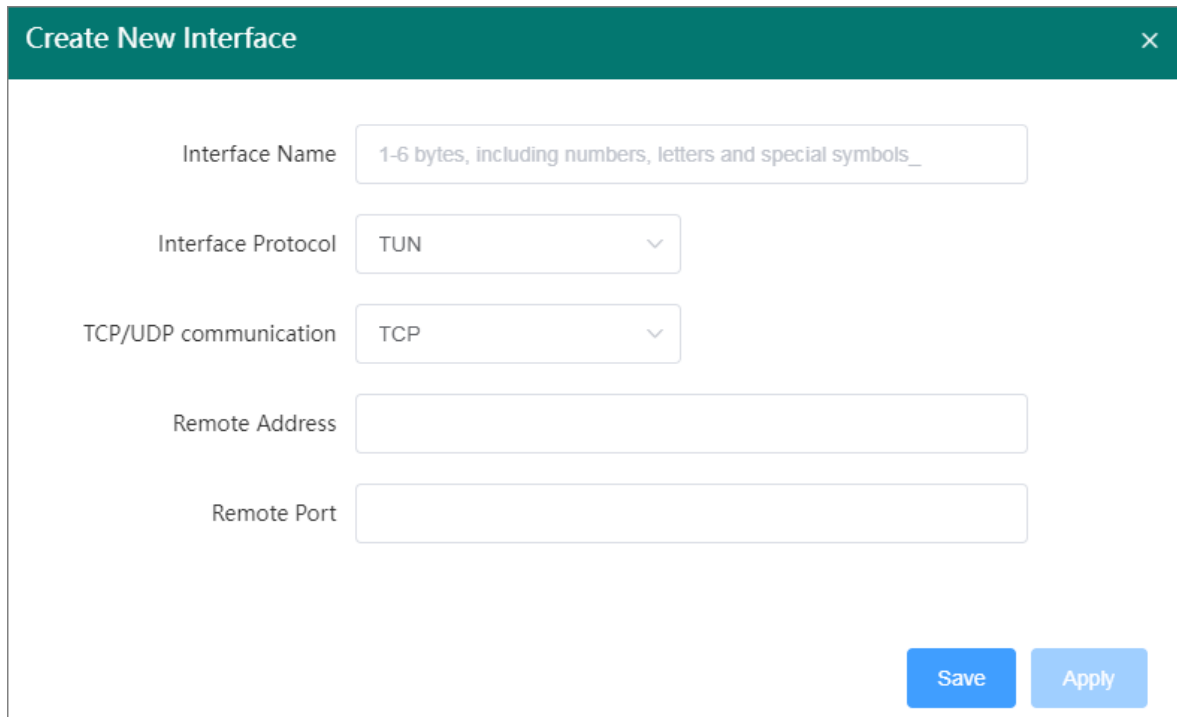
The 'Modify Interface' dialog box has a dark teal header. Below the header, there are two tabs: 'Basics' and 'Advanced Settings', with the latter being selected and highlighted in orange. The 'Advanced Settings' section contains two input fields: 'TTL Settings' with the value '255' and 'MTU' with the value '1500'. At the bottom right, there are two blue buttons labeled 'Save' and 'Apply'.

Figure 4-54 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

4.4.2.4 OPENVPN client

OPENVPN supports two-way certificate authentication. The client needs to authenticate the server, and the server also needs to authenticate the client. OPENVPN includes TUN and TAP two protocols, TUN is the routing mode, as shown in Figure 4-55, and TAP is the bridge mode, as shown in Figure 4-56



The screenshot shows a 'Create New Interface' dialog box with a dark green header bar containing a close button (X). The dialog contains the following fields and controls:

- Interface Name:** A text input field with a placeholder hint: '1-6 bytes, including numbers, letters and special symbols_'. Below the field is a small 'v' icon.
- Interface Protocol:** A dropdown menu currently showing 'TUN'.
- TCP/UDP communication:** A dropdown menu currently showing 'TCP'.
- Remote Address:** An empty text input field.
- Remote Port:** An empty text input field.

At the bottom right of the dialog, there are two buttons: a blue 'Save' button and a light blue 'Apply' button.

Figure 4-55 TUN protocol

Create New Interface

×

Interface Name

1-6 bytes, including numbers, letters and special symbols_

Interface Protocol

TAP

▼

TCP/UDP communication

TCP

▼

Remote Address

Remote Port

Save

Apply

Figure 4-56 TAP protocol

- The name of the new interface: 1-6 characters in length, can be numbers, letters or _
- New interface protocol: create OPENVPN client can choose TUN (routing mode) or TAP (bridge mode)
- TCP/UDP communication: the protocol used by the channel, UDP or TCP can be selected, and must be consistent with the server channel protocol
- Remote address: IP/domain name of GRE server
- Remote port: the listening port of the GRE server

The advanced setting parameters of OPENVPN are shown in Figure 4-57.

Modify Interface

×

Basics

Advanced Settings

Use LZO compression

☒

The use of TLS

☒

TLS authenticates the secret key

Browse

Only *.key files can be uploaded

Common CA certificate

Browse

Only *.crt files can be uploaded

Client certificate

Browse

Only *.crt files can be uploaded

Client private key

Browse

Only *.key files can be uploaded

Save

Apply

Figure 4-57 Advanced settings page

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



Notice:

- 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 before normal connection
- 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.

4.4.3 VPN server

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

4.4.3.1 PPTP server

The PPTP server includes two parts: PPTP VPN server and user management, as shown in Figure 4-58.

PPTP VPN Server

PPTP VPN Disable ☐ Enable

MPPE Security

PPTP Server IP 192.168.0.1

Client IP Range 192.168.0.20 - 192.168.0.30

Primary DNS

Secondary DNS

MTU 1482

MRU 1482

User Management

No.	Enable	Username	Password	IP Address	Action
No Data					

Add

Save Apply

Figure 4-58 PPTP server

- PPTP VPN: Enable or disable PPTP VPN server, PPTP VPN server is disabled by default
- MPPE: Set whether to enable MPPE encryption for the PPTP channel, which is enabled by default
- PPTP server IP: The virtual IP address of the VPN server, which cannot be located on the same network segment as the LAN port IP
- Client IP address range: the IP address range assigned to the client, which must be in the same network segment as the server IP
- Primary DNS Server: Assigned to the client's preferred DNS server address, such as 8.8.8.8
- Alternative DNS server: Assign the address of the alternate DNS server to the client

- MTU: set the MTU of PPTP channel, the default is 1482
- MRU: set the MRU of PPTP channel, the default is 1482
- Enable: Set whether to enable the login authentication user name and password in the corresponding list
- 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 will use the IP address automatically assigned by the server. If you want to fix the VPN client IP, please set it to an IP within the client IP address range.

4.4.3.2 L2TP server

The L2TP server includes two parts: L2TP VPN server and user management, as shown in Figure 4-59.

L2TP VPN Server

L2TP VPN Disable Enable

L2TP Server IP

192.168.10.1

Client IP Range

192.168.10.20 - 192.168.10.30

Primary DNS

Secondary DNS

MTU

1500

MRU

1500

L2TP Over IPSEC

Pre-shared Key

Max Length is 255 including digits ~!@#\$\$%^&*()_+

IKE Version

ike

Local Identifier

Max Length is 100 including digits ~!@#\$\$%^&*()_+

Peer Identifier

Max Length is 100 including digits ~!@#\$\$%^&*()_+

Prohibit Unencrypted Links Disable Enable

User Management

No.	Enable	Username	Password	IP Address	Action
No Data					

Add

Save

Apply

Figure 4-59 L2TP server

- L2TP VPN: Enable or disable L2TP VPN server
- L2TP server IP: The virtual IP address of the VPN server, which cannot be located on the same network segment as the LAN port IP
- Client IP address range: The IP address range assigned to the client, which must be in the same network segment as the VPN server IP
- Primary DNS Server: Assigned to the client's preferred DNS server address, such as 8.8.8.8
- Alternative DNS server: Assign the address of the alternate DNS server to the client
- MTU: Set the MTU of the L2TP channel, the default is 1500
- MRU: Set the MRU of the L2TP channel, the default is 1500
- Pre-shared key: set the pre-shared key for IPSec encryption
- IKE version: IKE version used for IPSec encryption
- Local identifier: The local identifier of the channel, which can be the local IP or the local domain name. Note that you need to add @ when setting the domain name. When setting, you need to pay attention to the same as the peer identifier of the peer gateway.
- Peer identifier: The peer identifier of the channel, which can be the peer IP or the peer domain name. Note that you need to add @ when setting the domain name. When setting, you need to pay attention to the same as the local identifier of the peer gateway to.

4.4.3.3 IPSec server

The IPSec server consists of three parts: basic settings, advanced settings, and connection logs. The basic settings are shown in Figure 4-60.

The screenshot displays the 'IPSec VPN Server' configuration page. At the top, there are three tabs: 'Basics' (selected), 'Advanced Setting', and 'Connection Log'. Below the tabs, the 'IPSec VPN' status is shown as 'Disable' with a toggle switch to 'Enable'. The configuration fields include: 'Connection Name' (text input: 'nettonet'), 'Network Mode' (dropdown: 'Site To Site'), 'Work Mode' (dropdown: 'VPN Server'), 'Local Interface' (dropdown: 'lan'), 'Local Subnet' (text input: '10.10.10.0' and '24' with an example '(Example: 192.168.16.1/24)'), 'Peer Gateway' (text input: '192.168.0.2'), 'Peer Subnet' (text input: '20.20.20.0' and '24' with an example '(Example: 192.168.16.1/24)'), 'Authentication' (dropdown: 'Secret'), and 'Pre-shared Key' (password input field). At the bottom, there are 'Save' and 'Apply' buttons.

Figure 4-60 Basic settings

- IPsecVPN: Enable or disable IPsec VPN server, IPsec VPN server is disabled by default
- Connection name: Indicates the name of the connection, the length is 1~32 characters, and the value is a letter, a number or _
- Networking mode: divided into 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 WAN port)
- Local subnet: 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 subnet
- Peer gateway: IP or domain name of IPsec peer gateway
- Peer subnet: the subnet protected by the IPsec peer gateway and the subnet mask
- Authentication method: currently supports pre-shared key (Secret) authentication method
- Pre-shared key: set the pre-shared key for IPsec encryption

Figure 4-61 shows the advanced settings of IPsec VPN.

IPSec VPN Server

Basics

Advanced Setting

Connection Log

Stage 1 Setup

IKE Version

ike

Negotiation Mode

Main Mode

Local Identifier

@local

Peer Identifier

@remote

IKE Security

Security:

Auto

Verification:

Auto

Secret Key Group:

Auto

IKE Life Cycle(s)

28800

(1-86400)

Enable DPD Detection

Disable

☒

Enable

Stage 2 Setup

Encapsulation Mode

Tunnel Mode

ESP Security

Security:

Auto

Verification:

Auto

ESP Life Cycle(s)

3600

(1-86400)

Save

Apply

Figure 4-61 Advanced settings page

- Phase 1 settings 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 the main mode.
- Local identifier: the local identifier of the channel, which can be the local IP or the local domain name. Note that you need to add @ when setting the domain name. When setting, you need to 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 the peer domain name. Note that you need to add @ when setting the domain name. When setting, you need to be consistent with the local identifier of the peer gateway
- IKE encryption: the first phase includes three methods of encryption, authentication and key group in the IKE phase
- IKE life cycle: set the life time of the first phase IPSec session key in IKE negotiation mode, the unit is “s”.

- Enable DPD detection: whether to enable the DPD detection function, which will send DPD packets regularly to quickly find out whether the peer is online
- Phase 2 Settings Set the relevant parameters of the second phase of IKEv1
- Encapsulation mode: divided into tunnel mode and transmission mode, the default is tunnel mode, the encapsulation mode must be the same as the peer. The tunnel mode will add an extra IP header to the original IP packet, but the transport mode will not. In terms of security, the tunnel mode is better than the transmission mode, and is suitable for more general VPN applications.
- ESP encryption: 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 to check whether the IPsec server is successfully connected, as shown in Figure 4-62.

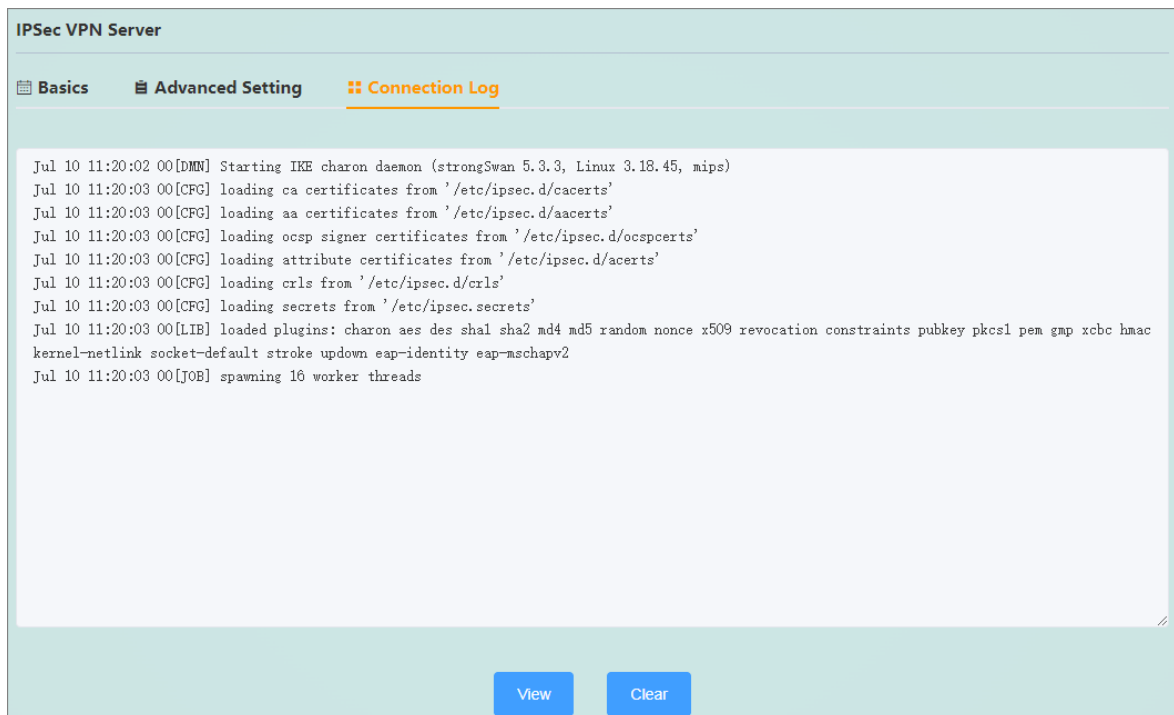


Figure 4-62 Connection log

4.5 SNMP settings

SNMP (Simple Network Management Protocol, Simple Network Management Protocol) is a communication rule between the management device and the managed device in the network, which is used to manage network nodes (servers, workstations, routers, etc.) , switches, and HUBS, etc.), it is an application layer protocol. SNMP settings support two versions of SNMP v1 and SNMP v2c, and consists of three parts: settings, groups, and traps.

The SNMP setting page is shown in Figure 4-63.

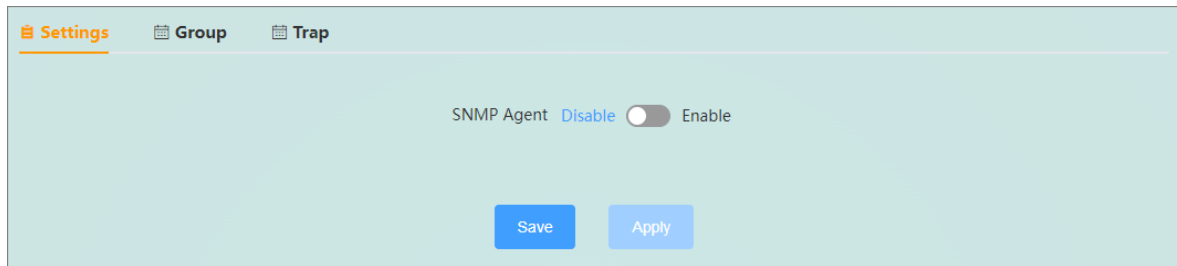


Figure 4-63 Setting page

- SNMP Agent: Turn on or off the SNMP Agent function, the default SNMP Agent function is off

The SNMP community setting page is shown in Figure 4-64.

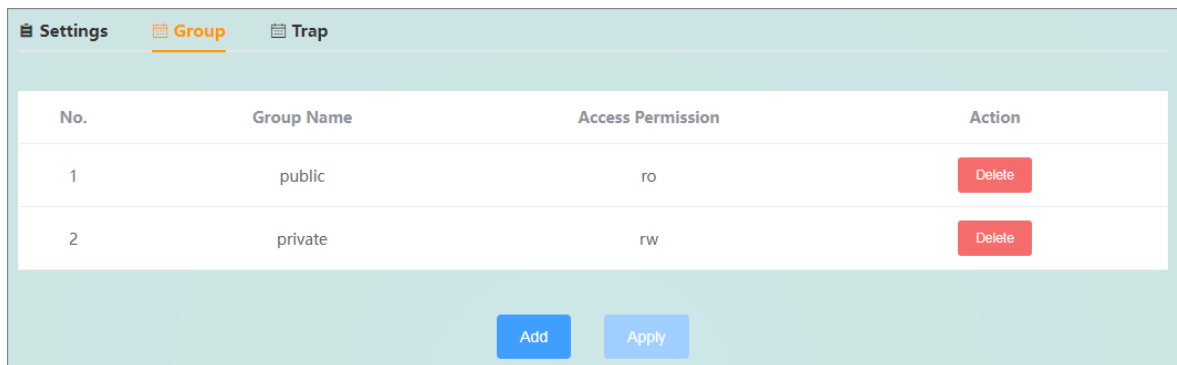


Figure 4-64 Community setting page

- Community name: set the name of the SNMP community, the length is 1-63 letters or numbers
- Access permission: set the permission for NMS to use this group to access the Agent, there are two types: read-only (ro) and read-write (rw)

The SNMP community setting page is shown in Figure 4-65.

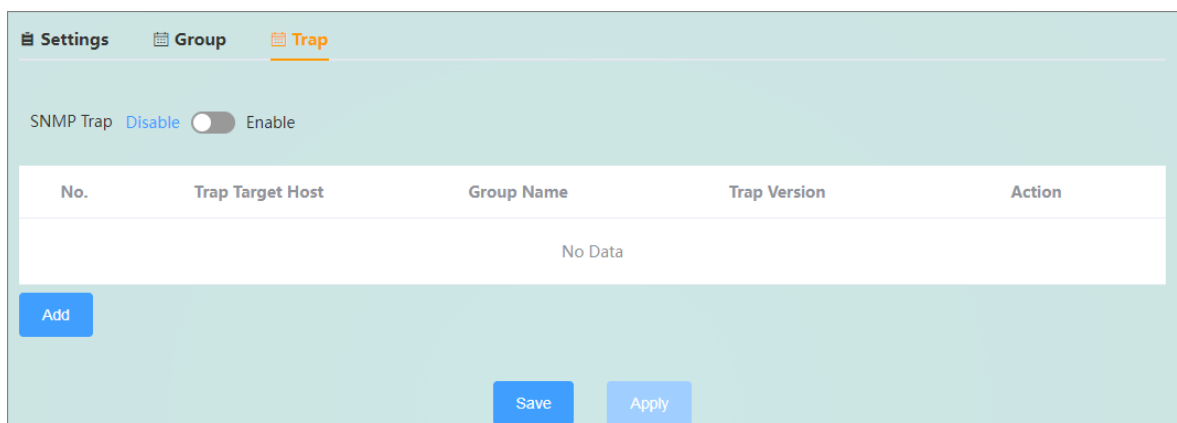


Figure 4-65 Trap setting page

- Enable SNMP Trap: Enable or disable the SNMP Trap function. The SNMP Trap function is disabled by default. Before enabling the SNMP Trap function, you must first enable the SNMP Agent.
- 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 complete, click Save to apply, and you can manage the router through NMS.

4.6 LLDP settings

LLDP (Link Layer Discovery Protocol, Link Layer Discovery Protocol), which provides a standard link layer discovery method, can use the main capabilities, management addresses, device identifiers, and interfaces of the local device Information such as identification is organized into different TLVs (Type/Length/Value, type/length/value), and encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit, Link Layer Discovery Protocol Data Unit) for publication Give the neighbor or network management system directly connected to itself, so that the network management system can query and judge the communication status of the link.

The LLDP setting page is shown in Figure 4-66.

Figure 4-66 LLDP setting page

- LLDP function: enable or disable LLDP function, LLDP function is disabled by default
- Sending cycle (s): LLDPDU data packet sending cycle, in seconds
- TTL multiplier: TTL is aging time. The LLDP receiver will set the aging time of the neighbor information on the local device according to the TTL value carried by the router LLDPDU. If the received TTL value is 0, the neighbor device information will be aged immediately. The product 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*30=120 seconds).

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

4.7 Cloud Service

The device supports a very simple cloud service access configuration process. Only simple configuration steps are required to quickly realize the communication function between devices and cloud servers in various regions. Realize remote maintenance and management of equipment and monitoring and management of on-site network status through cloud servers, such as viewing equipment online status, basic information, equipment parameters, network signal strength, interface and terminal equipment connection status, etc. The device cloud service setting interface is shown in Figure 4-67.

Figure 4-67 Device cloud service setting page

- Device cloud service: Enable or disable the device cloud service function, and the device cloud service function is disabled by default.
- Server address: device cloud server address, which can be IP address or domain name.
- Port number: The port number of the device cloud server device access, just match with the cloud server.
- Access verification code: If the cloud server enables the access "verification code" function, it is necessary to configure the correct access verification code (obtained from the cloud server user profile) to establish a connection normally; if the cloud server disables the "verification code" function, set to null. The legal value is 0~64 characters, which can be letters, numbers and special characters~!@#\$%^&*()_+`-={}[]|;<>?,./\
- Data port number: The data communication port number of the device cloud server, 1883 is used by default (generally no modification is required).
- Information reporting cycle: Device information is reported every 10 seconds by default, and the legal value is 5~65535, and the unit is second.

**Notice:**

If you need to modify the factory value of the configuration parameters of the device cloud service, please contact our technical staff.

5 Maintenance and Service

From the day of product shipment, Wuhan Maiwe Communication Co., Ltd. offers a five-year product warranty. According to the product specifications of Wuhan Maiwe Communication Co., Ltd., during the warranty period, if the product has any malfunction or operational failure, Wuhan Maiwe Communication Co., Ltd. will repair or replace the product for the user free of charge. However, the above commitment does not cover damages caused by improper use, accidents, natural disasters, incorrect operation, or incorrect installation. To ensure that consumers benefit from the range of products offered by Wuhan Maiwe Communication Co., Ltd., you can obtain assistance and problem resolution in the following ways:

- Internet Service
- Contact the Technical Support Office
- Product Repair or Replacement

5.1 Internet Service

Through the technical support section of Wuhan Maiwe Communication Co., Ltd.'s website, you can obtain more useful information and usage tips.

5.2 Technical Support Phone Service

Users of products from Wuhan Maiwe Communication Co., Ltd. can call the technical support office of Wuhan Maiwe Communication Co., Ltd. Professional engineers from Wuhan Maiwe Communication Co., Ltd. will communicate with you to assist in resolving any product usage issues you encounter as soon as possible.

5.3 Product Repair or Replacement

For product repairs, replacements, or returns, according to the handling procedures of Wuhan Maiwe Communication Co., Ltd., you should first confirm with the technical staff of Wuhan Maiwe Communication Co., Ltd. and then negotiate with the sales staff of Wuhan Maiwe Communication Co., Ltd. to complete the product repair, replacement, or return.

5.4 Contact Information

- Address: No.52, Liufang Road, East Lake Hi-tech Development Zone, Wuhan, China
- Postal Code:430205
- Phone: 027-87170215/16
- Fax:027-87170217
- Website:www.maiwe.com