User Manual

VT-LTE500

Industrial router

Contents

Disclaimer

- The Company shall not be liable for any losses or damages caused by the voluntary disclosure of information by users or teams, or resulting from cyberattacks, fraud, or other malicious activities conducted by third parties. Users shall seek legal remedies from the responsible parties through applicable legal or administrative channels.
- The SDLAN function of this device shall not be used for the following purposes:
    1) Design, construction, operation, or maintenance of nuclear facilities;
    2) Aircraft navigation or aviation operation systems;
    3) Medical equipment used for life support or emergency medical treatment;
    4) Continuous long-term or high-volume data transmission.
- This device shall not be used for any illegal activities, including but not limited to unauthorized access to computer systems, interference with network services, cyberattacks, or any activities prohibited by applicable laws and regulations or harmful to public interests.
- Due to the nature of computers, wireless communication, and Internet networks, Shanghai Valtoris Electronic Technology Co., Ltd. shall not be held responsible for communication interruptions, system failures, or service instability caused by cyber incidents, telecommunications adjustments, government regulations, or force majeure events.
- During the use of the device, users shall not utilize the SDLAN function for abnormal continuous high-traffic data transmission. If such activities are identified, the Company reserves the right to suspend the related remote tunnel services.
- In the event of any dispute arising from the use of the device or related services, both parties shall first attempt to resolve the matter through friendly negotiation. If no agreement can be reached, either party may submit the dispute to a court with competent jurisdiction in Shanghai, China. Shanghai Valtoris Electronic Technology Co., Ltd. reserves the right to final interpretation of this document.

1. Overview

1.1 Product features

- **Easy Remote Networking:** No public IP address or complex configuration required. Easily establish remote networking and device access.
- **Flexible Port Forwarding:** Supports custom port forwarding without port restrictions.
- **Static Routing:** Supports static routing and inter-subnet communication.
- **Secure & Controllable:** Tunnel server IP address and encryption keys can be modified at any time. Multi-level key authentication ensures secure communication.
- **Privacy Protection:** Encrypted P2P tunnel communication enables direct device-to-device connectivity. In most scenarios, no server relay is required.
- **No Hidden Fees:** Only device purchase costs apply, with no additional hidden service charges.
- **Multi-Function Support:** Supports cellular-to-Ethernet network access and automatic multi-link failover.
- **Customized Deployment:** Supports device-account binding for simplified deployment without complicated configuration.
- **Convenient Maintenance:** Supports remote device management through a web-based cloud platform and PC management software.
- **1 RS485 + 1 RS232 Ports:** Equipped with 2 serial ports for industrial communication applications.

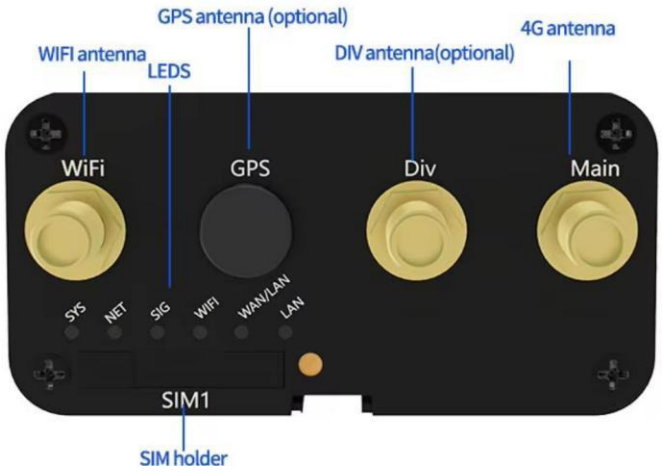
1.2 Product Optional

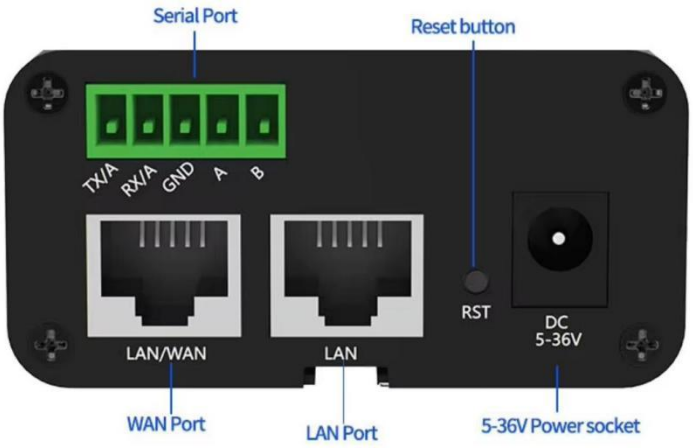
Model	Parameter	Suport Areas
VT-LTE500-AF (Cat 4)	LTE-FDD: B2/B4/B5/B12/B13/B14/B66/B71 WCDMA:B2/B4/B5	US
VT-LTE500-EU (Cat 4)	4G (LTE-FDD): B1, B3, B5, B7, B8, B20, B28 4G (LTE-TDD): B38, B40, B41 WCDMA:B1, B5, B8 GSM: B3, B8	Europe
VT-LTE500-CN (Cat 4)	4G (LTE-FDD): B1, B3, B5, B8 4G (LTE-TDD): B34, B38, B39, B40, B41 WCDMA:B1, B5, B8 GSM: B3, B8	China & India
VT-LTE500-AU (Cat 4)	4G (LTE-FDD): B1, B2, B3, B4, B5, B7, B8, B28, B66 4G (LTE-TDD): B40 WCDMA: B1, B2, B4, B5, B8 GSM/ EDGE: B2, B3, B5, B8	Latin America, Australia, New Zealand

Model	Parameter	Suport Areas
VT-LTE500-5G (RedCap)	5G SA：n1, n3, n5, n8, n28, n41, n78, n79 4G (LTE-FDD): B1, B3, B5, B8 4G (LTE-TDD): B34, B38, B39, B40, B41 LTE 1.8G: B59, B62 WCDMA: B1, B5, B8	China & India

2. Hardware Description

2.1 Product appearance





2.2 LED indicators

This product provides eight LED indicators. The status of each indicator is shown in Table 2-1.

Table 2-1 LED Indicator Status

LED Name	Indicator	Status
Power LED	SYS	Power normal:ON Power abnormal:OFF
Module LED	NET	Module dailing:ON Module idle:OFF
Signal LED	SIG	Internet connected via SIM: Blinking/SteadyON
Wi-Fi LED	Wi-Fi	Wi-Fi connected:Blinking
WAN/LAN LED	WAN/LAN	WAN/LAN connected:ON WAN/LAN disconnected:OFF
LAN LED	LAN	LAN connected:ON LAN disconnected:OFF

2.3 Ethernet Ports

This product features two standard RJ45 Ethernet ports, including one LAN ports and one WAN/LAN port. The WAN/LAN port operates in two modes, with WAN mode being the default setting. Users can switch between these modes through the web interface, as illustrated in Figure 2-1.

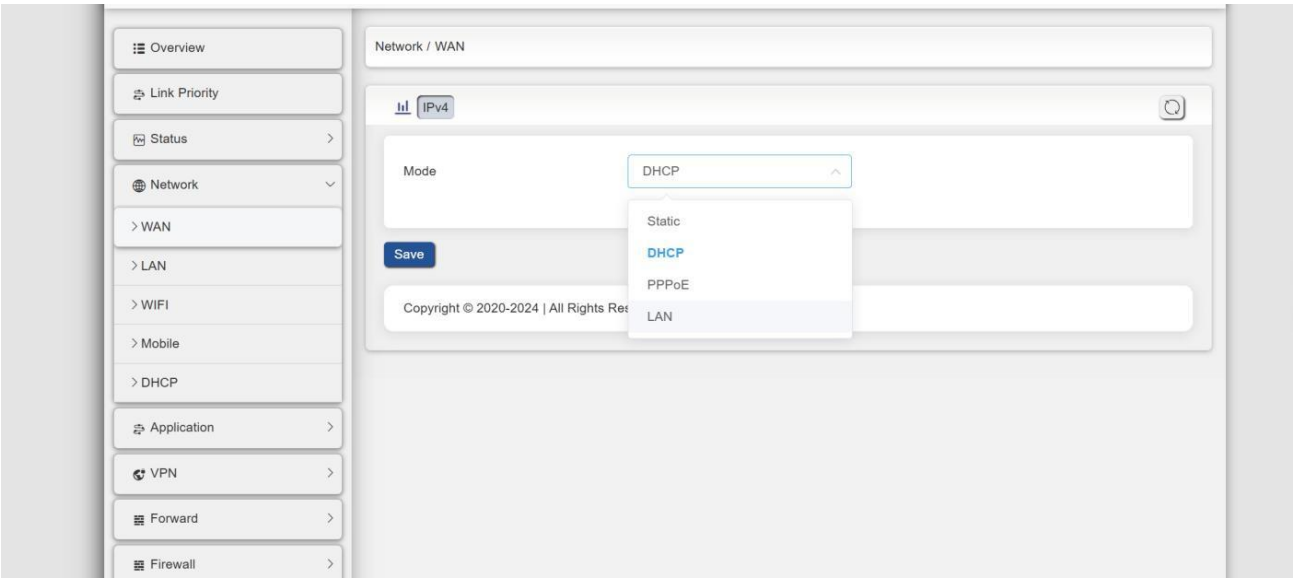


Figure 2-1

The Ethernet port mode is described in Table 2-2.

Table 2-2 Ethernet Port Mode Description

Ethernet	Mode	Default	DHCP Service
WAN/LAN	WAN/LAN switchable Default:WAN	DHCP dynamically obtains IP	/
LAN	LAN	Default address: 192.168.8.1	Automatic / Static IP Assignment

2.4 Product parameters

Other detailed parameters are shown in Table 2-3.

Table 2-3 MT280-4G router parameters

Parameters		Description
Cellular Network	4G	APN, user name, password and authentication type
Ethernet Port	Interface Standard	RJ45, with Data and Network LED indicators, 10/100/1000Mbps
	Number	WAN/LAN*1 + LAN*1
WAN	IP	Default: DHCP (dynamic acquisition)
LAN	IP	Default: 192.168.8.1
	Subnet Mask	Default: 255.255.255.0

	DHCP	Support
Hardware Interface	Power	12V DC, with over-voltage and reverse-polarity protection
	Antenna Interfaces	2 × Magnetic antennas, Wi-Fi antanna, SMA female, 50 Ω impedance
	SIM	2 × Drawer-type SIM card slots (1.8V / 3.3V)
	Reset Button	Reboot device or restore factory settings
	LED Indicators	SYS,NET,SIG,Wi-Fi, WAN/LAN, LAN
Hardware Parameters	CPU	MT7621AT
	FLASH	16MB
	DDR3	512MB
Dimension	Size (mm)	84.81 mm*65.09 mm*32.70 mm
Weight	Unit ： g	130g
Mounting	/	DIN mounting
Temperature Range	Working Temperature	-30%~+75℃
	Storage Temperature	-40%~+85℃
Humidity Range	Humidity	<95% (no frost)
Hardware Interface	Power Supply	5–36 VDC, with over-voltage and reverse-polarity protection
Software Function	Configuration	Built-in Web
	Networking Protocol	HTTP、MQTT
	SSL Rncryption	Supports transparent encrypted transmission for MQTT protocol
	Routing	Static routing supported
	Port Forwarding	Supports DNAT, SNAT, DMZ, MASQ
	VPN	Supports OPENVPN, SDLAN, L2TP_CLIENT/L2TP_SERVER, GRE, VXLAN, IPSEC
Standby Specifications	Standby Power Consumption	1.8W~2.6W
	Standby Current	12VDC/144mA~254mA

Physical Characteristics	Housing Material	Sheet Metal
	Ingress Protection	IP30
	Cooling Method	Fanless cooling

3. Router Configuration

The device supports configuration through the web management interface.

Before configuration, connect the router to the PC using an Ethernet cable. Connect one end of the cable to the router's LAN port and the other end to the PC's Ethernet port.

3.1 Log in to the WEB configuration Interface

1. Set IP address for PC (two methods)

Method 1: The PC selects the automatic acquisition of IP address, as shown in Figure 3-1

Figure 3-1 PC automatically obtains IP

Method 2: Specify an IP address, as shown in Figure 3-2.

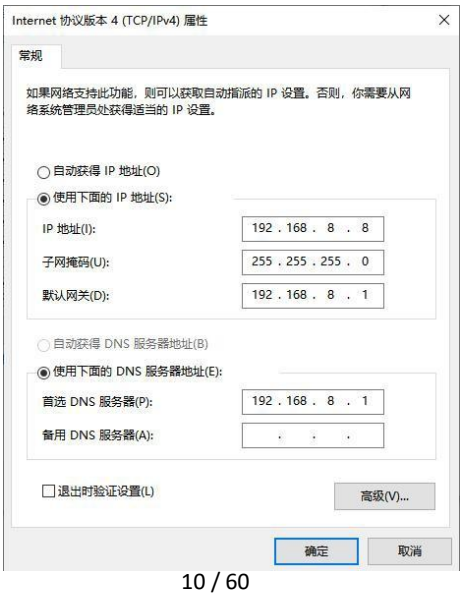


Figure 3-2 PC designated IP address

IP address: 192.168.8.x (cannot be set to 192.168.8.1)

- Subnet mask: 255.255.255.0
- Default gateway: 192.168.8.1
- DNS: Gateway address or locally available DNS server

2. Open the browser and enter the LAN port initial address "192.168.8.1" in the address bar. Press the Enter key to enter the login interface, as shown in Figure 3-3. The initial user name is admin and the initial password is admin. After entering the correct account and password, click login to enter the configuration page.

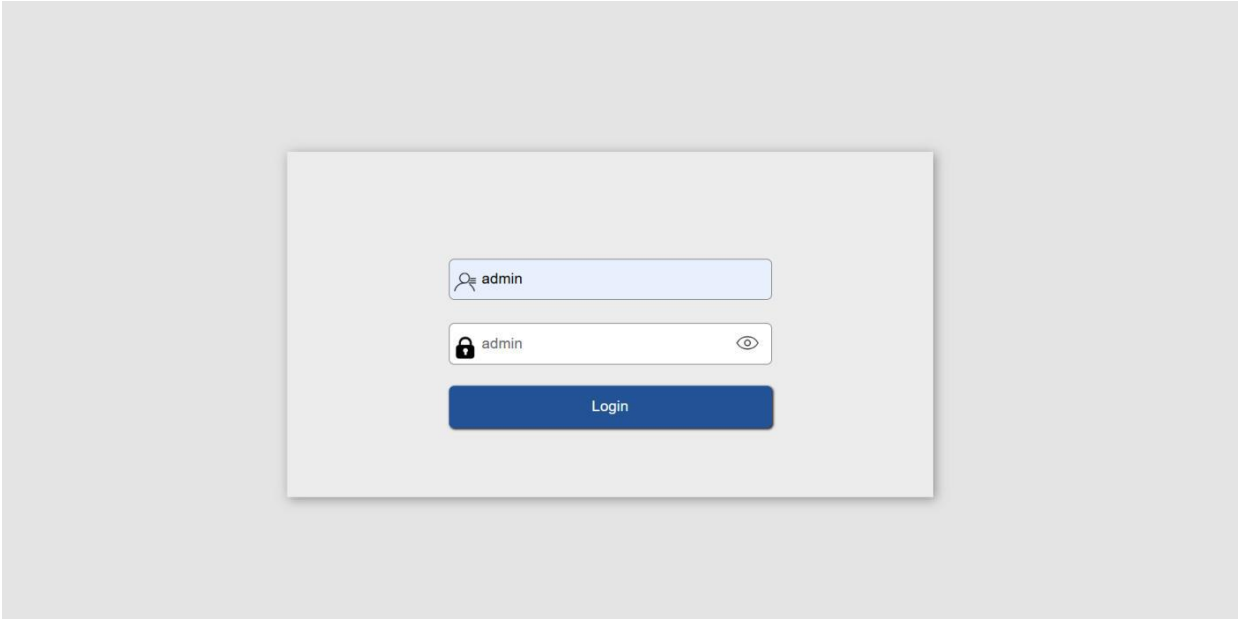


Figure 3-3 Login interface

3.2 Home Page

The home page provides a brief overview of the device information, so that you can quickly understand the basic situation of the device. Detailed device information can be viewed on the system status page. The home page is shown in Figure 3-4.

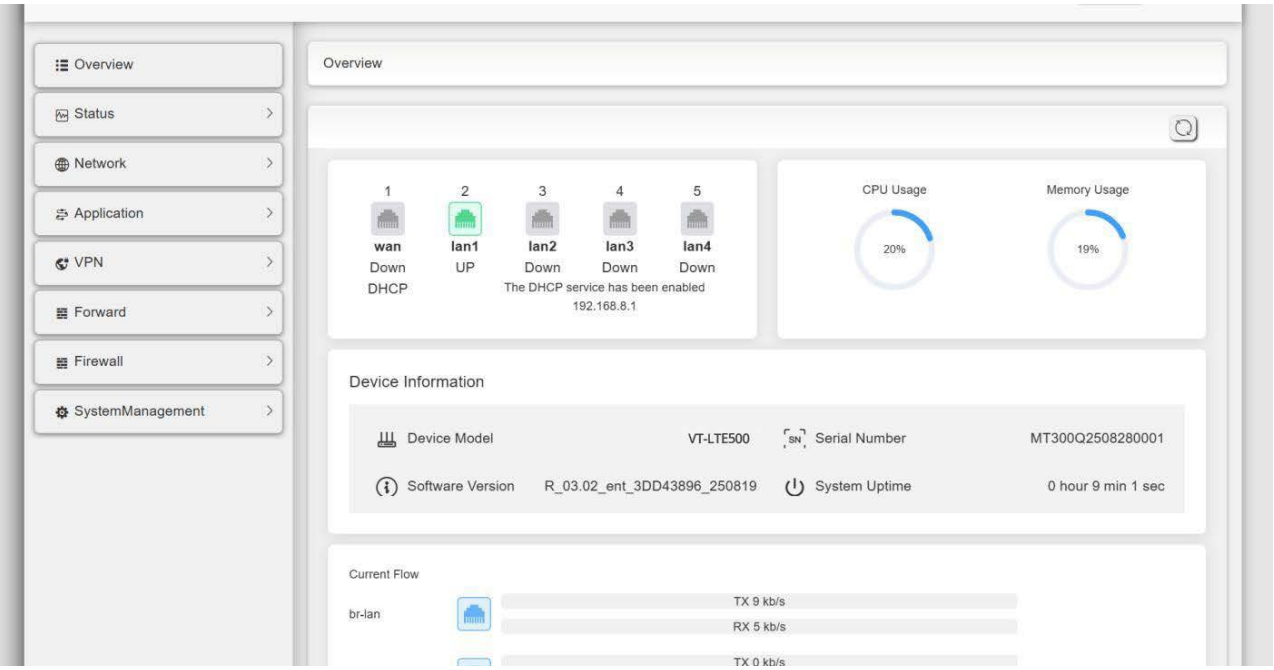


Figure 3-4 Homepage

3.3 Internet Priority

This product supports both Ethernet and cellular networks (4G) for simultaneous operation. The multi-network connectivity feature provides users with enhanced flexibility and reliability, enabling efficient and stable network connections across various environments to meet diverse application requirements.

Furthermore, this product features a link detection function that allows users to customize detection addresses for rapid network connectivity checks. When detecting network anomalies, it automatically switches between different networks to ensure uninterrupted communication and stable data flow. The priority web page configuration is illustrated in Figure 3-5.

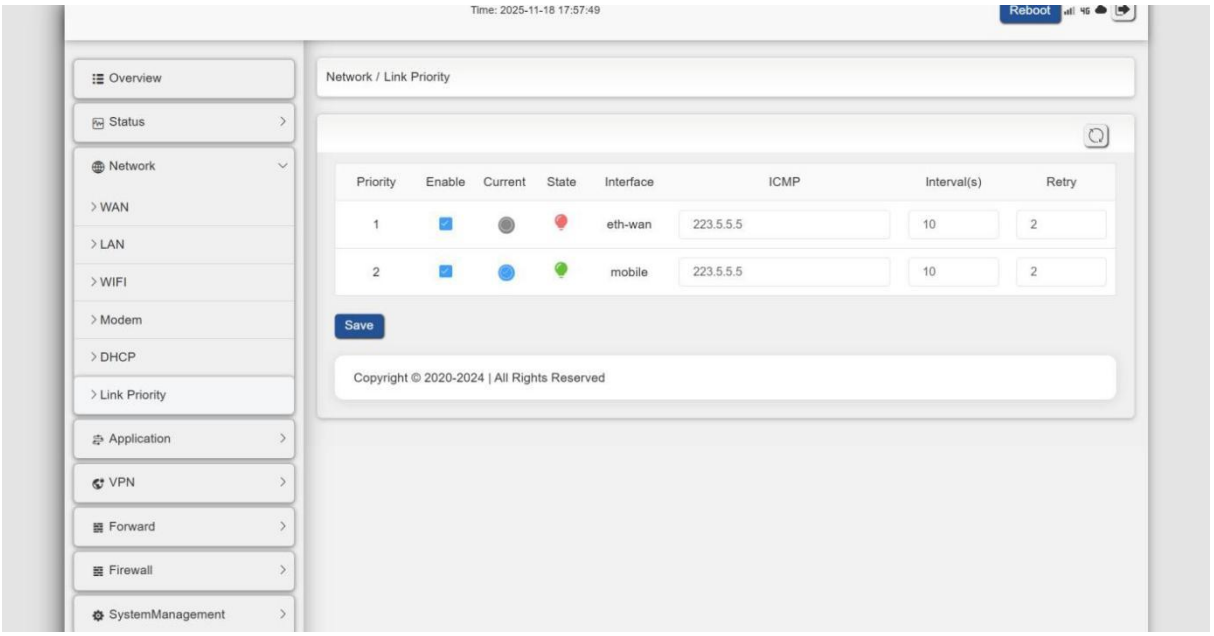


Figure 3-5 Internet Priority Configuration

The main parameters of the Internet priority are shown in Table 3-1.

Table 3-1 Connection Priority Settings

Item	Description	Default
Priority	Switches to a backup network when the primary network fails; restores to primary when it recovers	Wired Ethernet Priority
Enabled	Only enabled rules will be monitored and switched	Enabled
ICMP	IP address for connectivity check; successful response indicates the network is reachable	223.5.5.5
Interval	Sets the check period in seconds	10
Retry	Number of retry attempts for connectivity check	2

Note: The network priority being switched is not always higher or lower than the current network.

3.4 System Status

In the system status page, users can view more detailed device information, including WAN, LAN, cellular network (4G), GPS and routing table. Through this information, users can fully understand the operation and performance of the device.

3.4.1 WAN

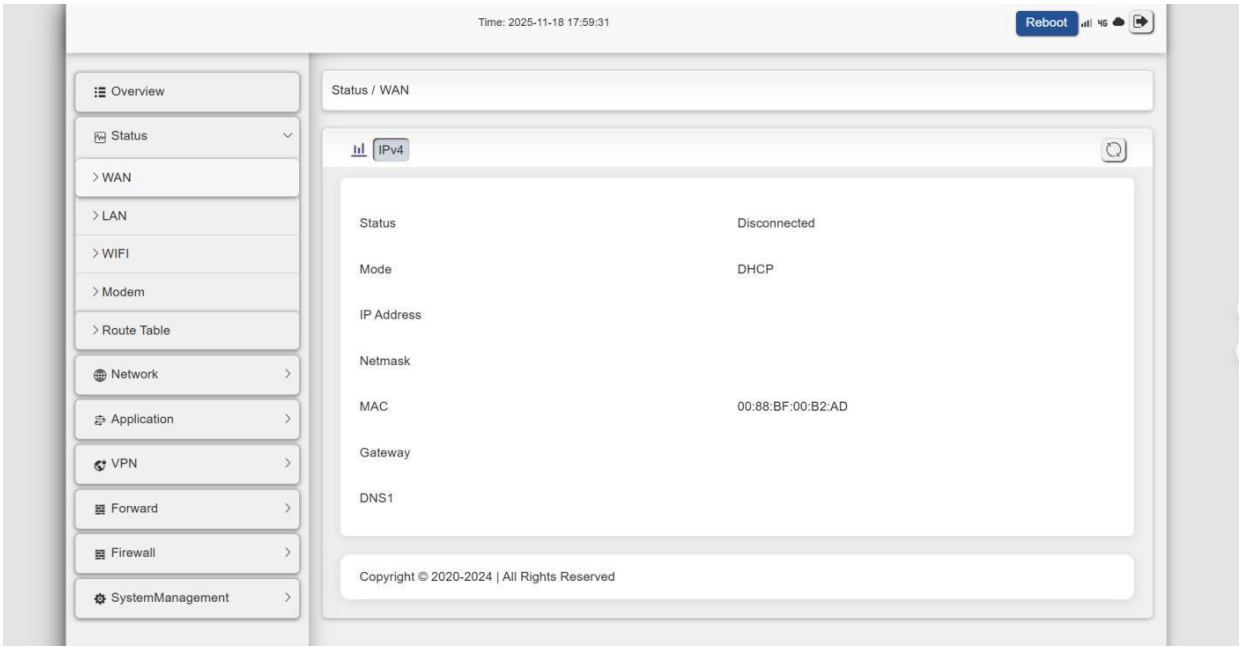


Figure 3-6 WAN Status

3.4.2 LAN

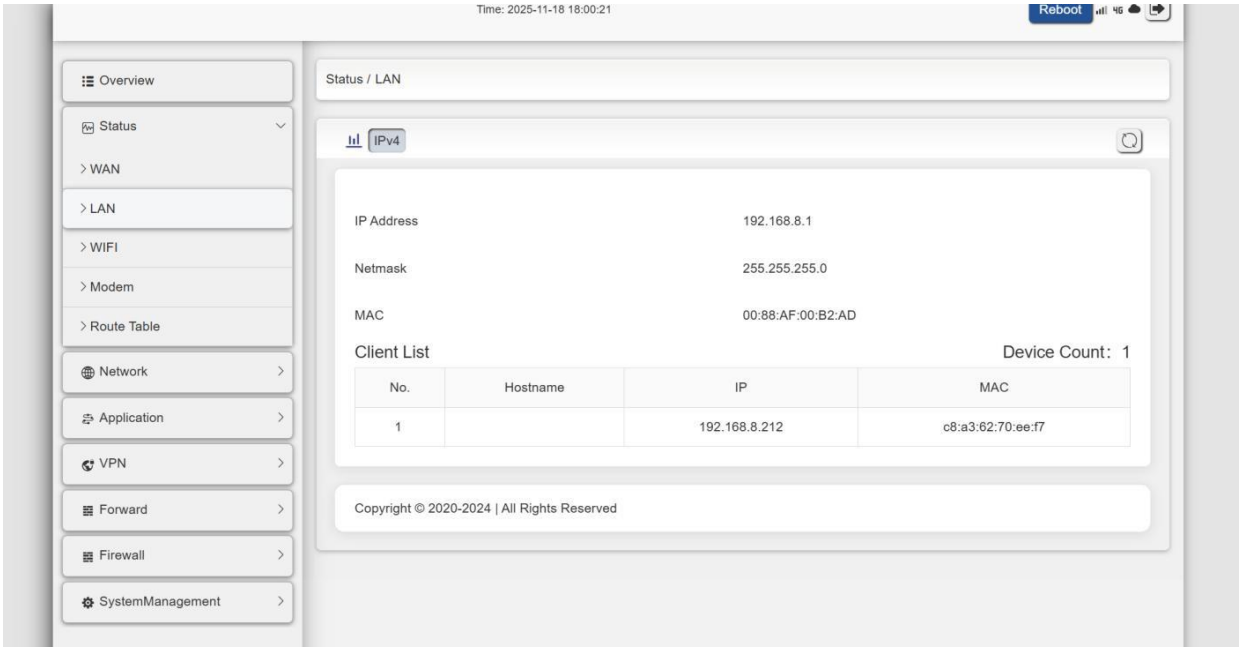


Figure 3-7 LAN Status

3.4.3 WIFI

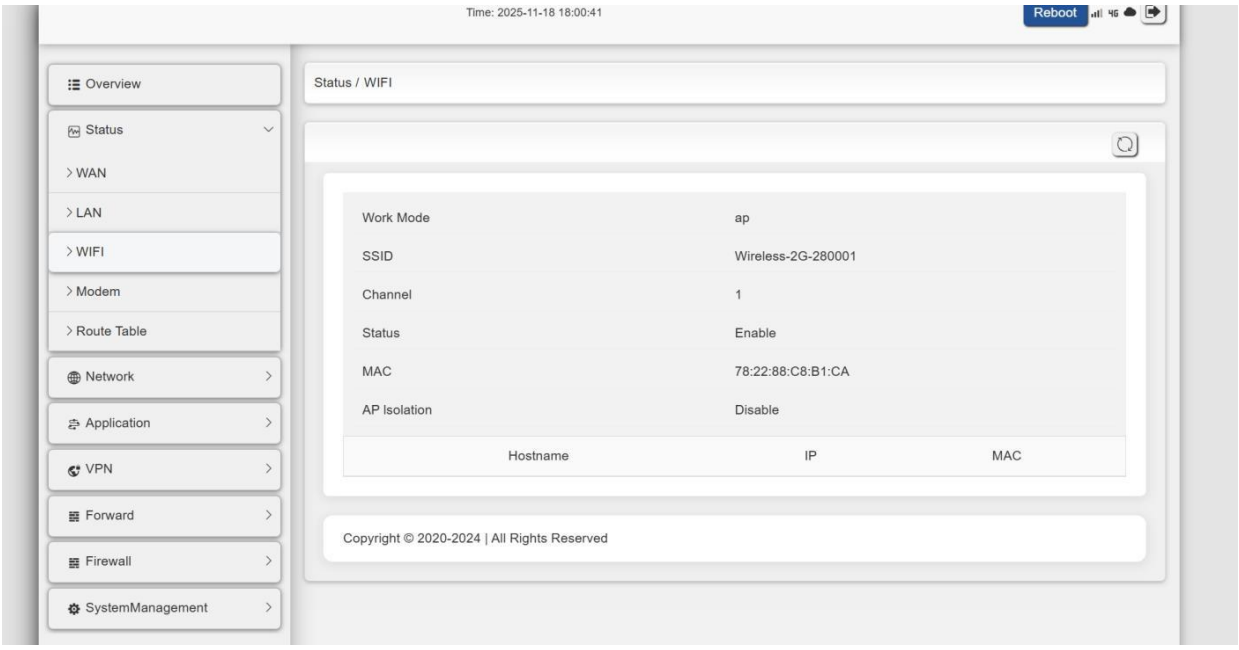


Figure 3-8 WIFI Status

3.4.4 Cellular Network (Mobile)

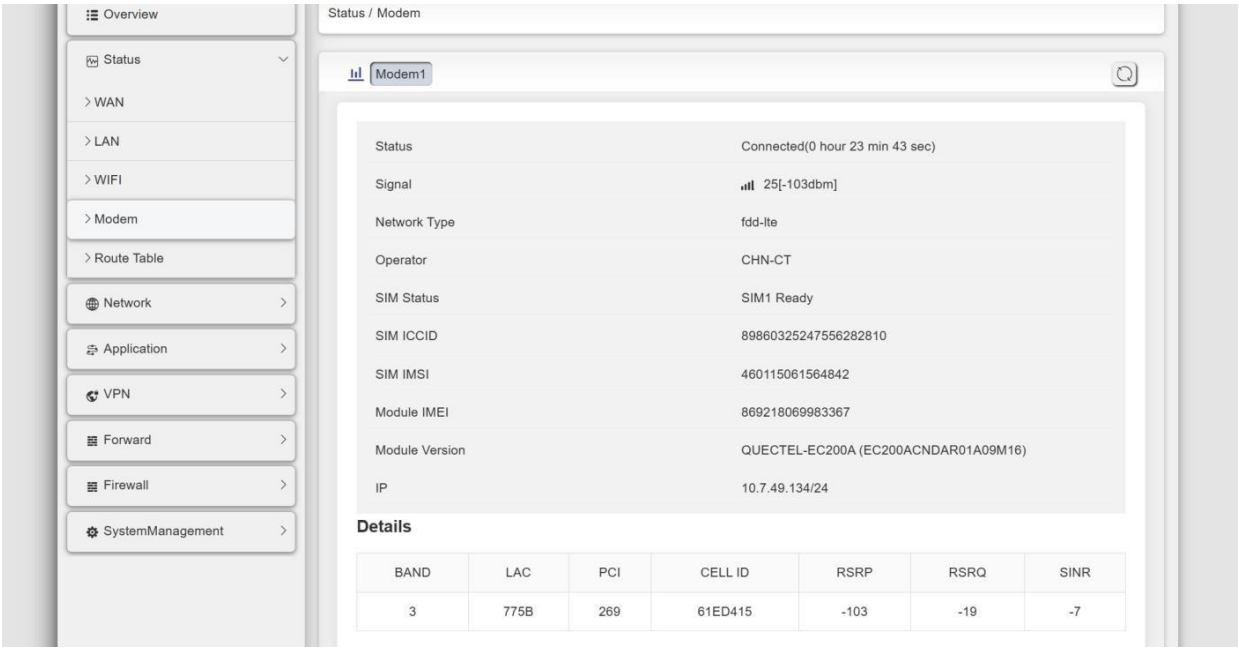


Figure 3-9 Mobile Status

3.4.5 GPS (optional)

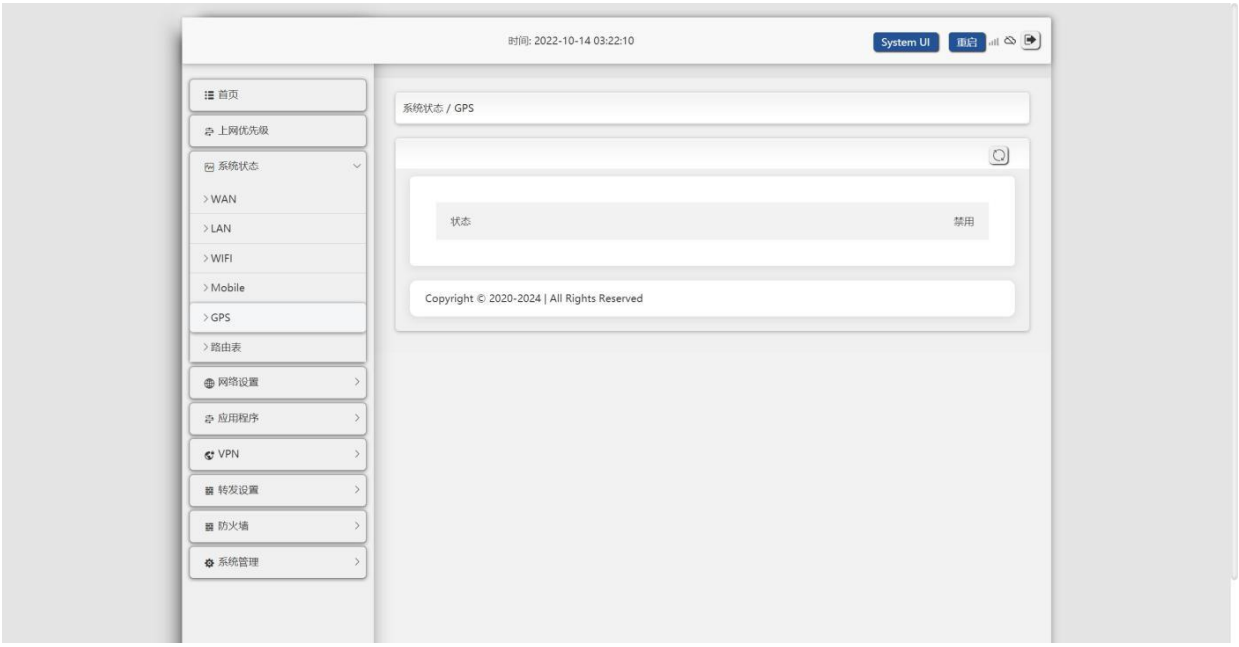


Figure3-10 GPSstatus

3.4.6 Routing Tables

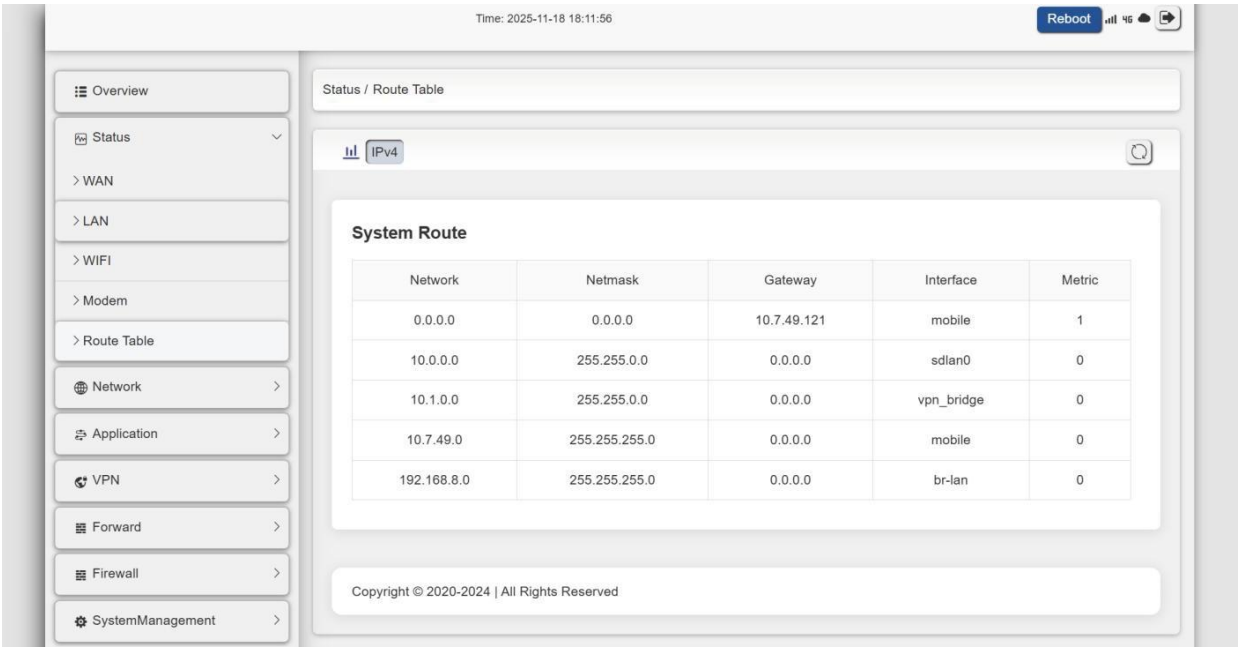


Figure 3-11 routing table

3.5 Network Settings

3.5.1 WAN

This product is designed with five Ethernet ports at the hardware level, with the WAN/LAN port operating in WAN mode by default. The WAN port supports three connection modes: Static IP, Dynamic IP (DHCP), and PPPoE. When the WAN/LAN port is switched to LAN mode, it shares the same LAN configuration as all other LAN ports. The WAN configuration interface is shown in Figure 3-11.

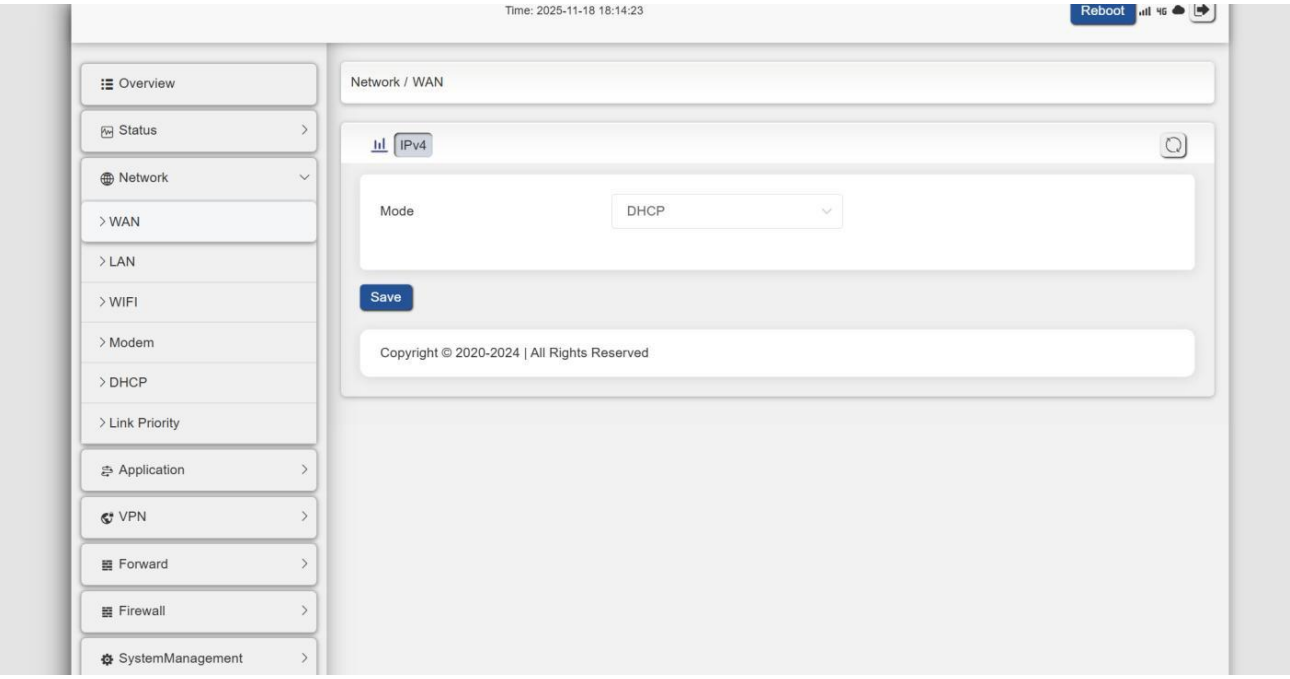


Figure 3-11 WAN Configuration Interface

The main parameters of WAN Settings are shown in Table 3-2.

Table 3-2 Main Parameters of WAN Settings

Item	Description	Default
Connection Mode	Static IP: Manually configure the IP address, subnet mask, and related parameters for the Ethernet interface. PPPoE: Connect to the Internet using the broadband account provided by the ISP. Dynamic IP (DHCP): Obtains IP address and subnet mask automatically from an upstream DHCP server. LAN: Converts the WAN port into a LAN port.	Dynamic IP (DHCP)
IP Address	IP address configured under Static IP mode	192.168.9.1
Subnet Mask	Subnet mask configured under Static IP mode	255.255.255.0
Gateway	Gateway address configured under Static IP mode	192.168.9.2
DNS	DNS server address configured under Static IP mode	192.168.9.2
Username	Username provided by the ISP for PPPoE authentication	Blank
Password	Password provided by the ISP for PPPoE authentication	Blank

3.5.2 LAN

This product is equipped with two dedicated LAN ports, and the WAN/LAN port can be switched to operate in LAN mode. LAN ports are primarily used for local network applications, including LAN networking and IP address allocation for downstream devices. Therefore, the LAN interface provides a built-in DHCP service. Information about connected client devices can be viewed under the LAN section on the System Status page.The LAN configuration interface is shown in Figure 3-12.

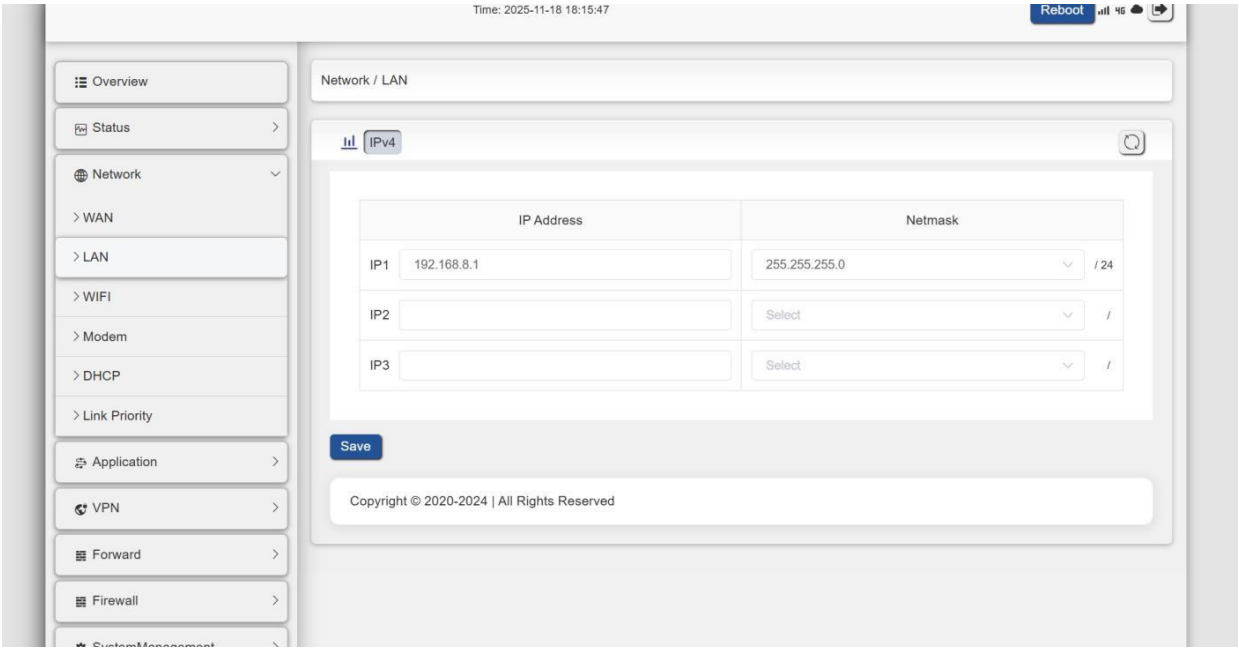


Figure 3-12 LAN Configuration Interface

3.5.3 WIFI

This product supports two Wi-Fi modes: Access Point (AP) and Client (Station). In AP mode, the router functions as a wireless access point, allowing other devices to connect and access the network, with selectable transmission frequencies of 2.4 GHz and 5.8 GHz. In Station mode, the router scans for nearby wireless access points and attempts to connect to them. Before use, ensure that the antennas are properly installed to allow the AP to be detected or to enable the device to scan and connect to other access points successfully. Proper antenna installation ensures stable and reliable wireless connections. The WIFI configuration interface is shown in Figure 3-14.

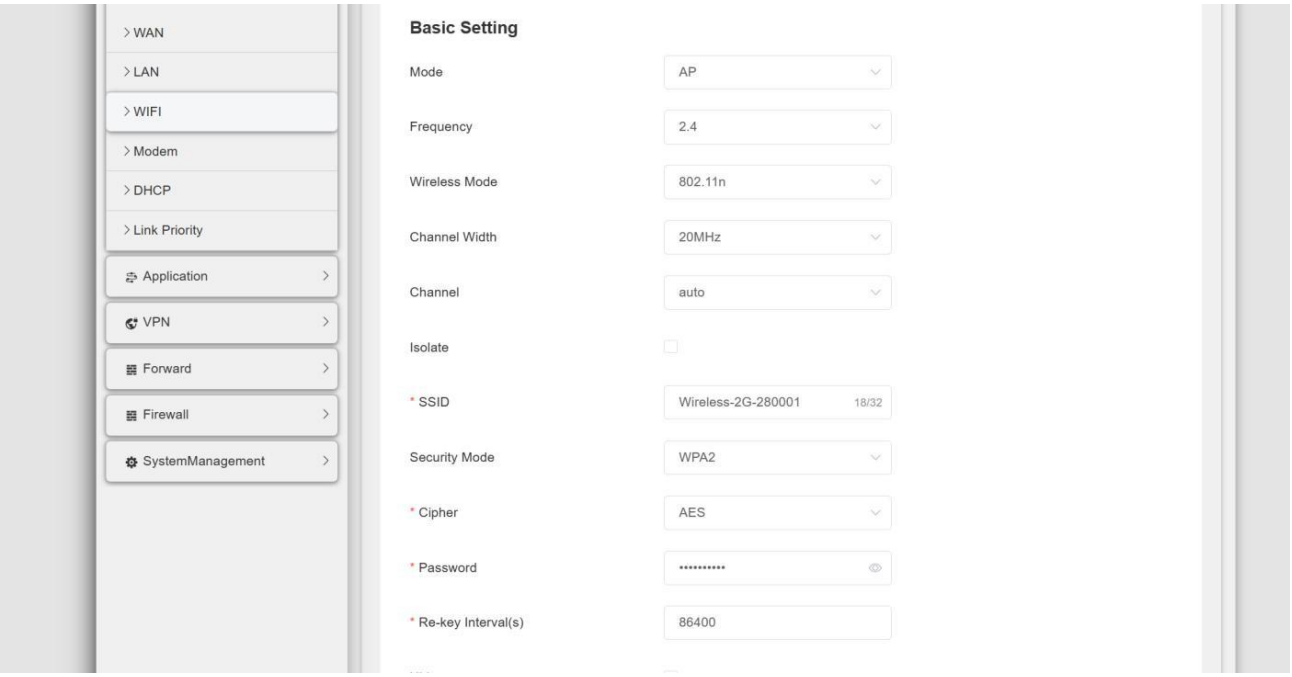


Figure 3-14 WIFI Configuration Interface

The main parameters of the AP mode are shown in Table 3-3.

Table 3-3 Main parameters of WIFI AP mode

Item	Description	Default
Frequency	Specifies the transmission frequency, supports 2.4G,	2.4G
Wireless Mode	Support 802.11b,802.11g,802.11n,802.11bg,802.11gn,802.11bgn	802.11n
Channel	The transmission path of the wireless signal within a specific frequency range, supporting 1-13 and auto	auto
SSID	The name used to identify and distinguish different wireless networks in a WIFI network	Wireless-4G-xx
Security Mode	Support no (no password), wpa, wpa2	none
WPA Password	The password required to connect to the wireless access point	none
Reauthentication Interval	The time interval between which the client device and the wireless access point reauthenticate	86400

The main parameters of the Station mode are shown in Table 3-4.

Table 3-4 Main Parameters of WIFI Station Mode

Name	Description	Default
SSID	The name of the wireless access point to be connected can be filled by scanning	not have
BSSID	The MAC address used to uniquely identify each Wi-Fi access point; can be filled in via scanning.	not have
Channel	Support 1 to 13, can be scanned and filled	not have
Security Mode	Supports none, WPA, and WPA2 through scanning and filling	wpa2
WPA Password	The password required to connect the client device to the wireless access point	not have

3.5.4 Mobile

This product utilizes an LTE Cat1/Cat4 (4G) cellular network. The design employs a dual-SIM single-standby configuration with both SIM1 and SIM2 being external cards housed in a push-in SIM card slot. The cellular network configuration interface is illustrated in Figure 3-15.

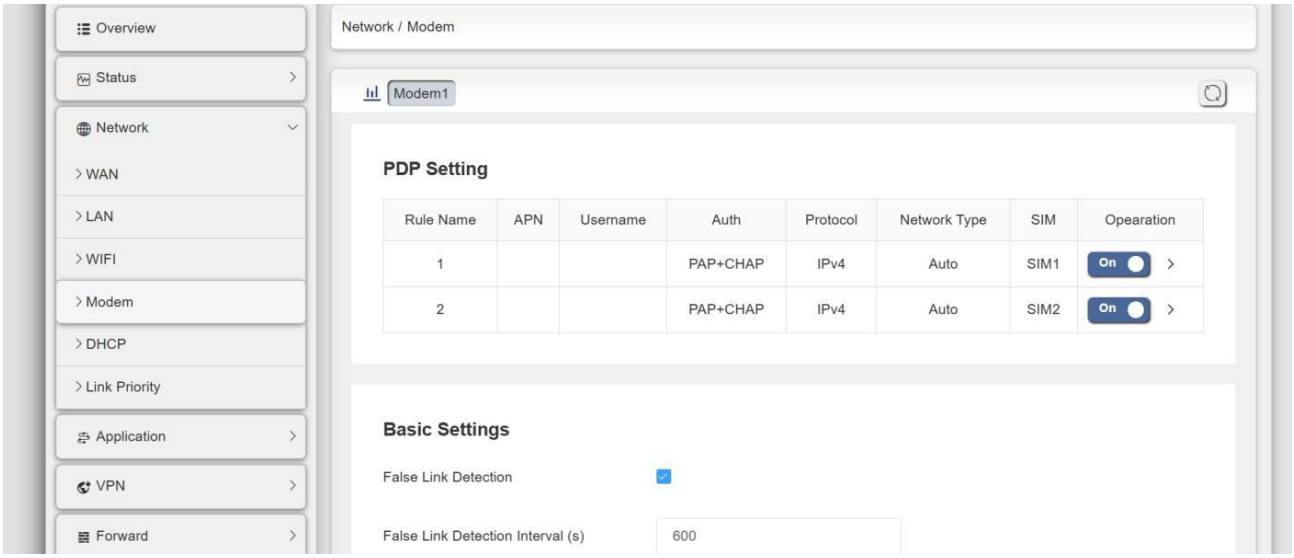


Figure 3-15 Mobile Configuration Interface

The main parameters of the mobile are shown in Table 3-5.

Table 3-5 Mobile Main Parameter Description

Name	Description	Default
APN	Used to identify the service type of WCDMA/LTE network	None
Username	Specifies the user name for a user connected to an external PDN network	None
Password	Specifies the password for users connected to external PDN networks	None
PIN	PIN code is the personal identification password of the SIM card. The correct PIN code must be enabled to dial properly	None
Authentication Type	Supports PAP, CHAP, and PAP+CHAP	PAP+CHAP
Link-Drop Detection	Monitor whether the SIM is disconnected	Enabled

3.5.5 DHCP

This product supports DHCP function. After enabling it, the lower computer can dynamically obtain IP address through automatic acquisition without manual configuration, which simplifies the workload of network management and maintenance. The DHCP configuration interface is shown in Figure 3-16.

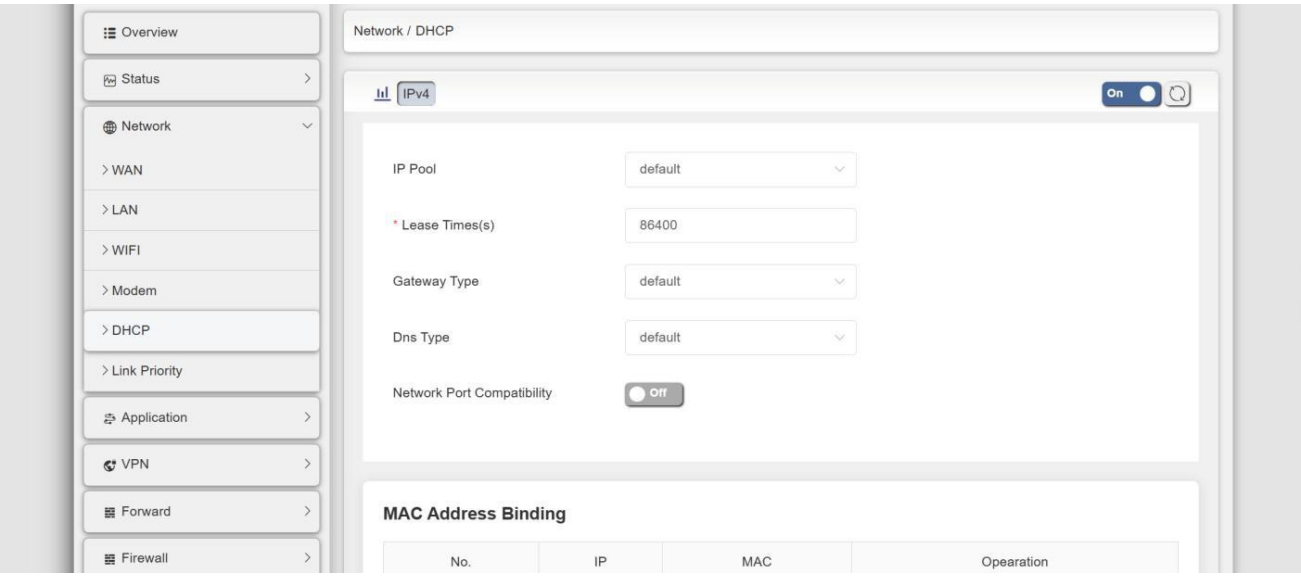


Figure 3-16 DHCP Configuration Interface

The main parameters of DHCP are shown in Table 3-6.

Table 3-6 DHCP main parameters description

Name	Description	Default
IP pool	Supports default or custom, indicating default/custom DHCP address allocation.	default
Start IP	The minimum address assigned to the subordinate machine	192.168.8.2
End IP	The maximum address assigned to the subordinate machine	192.168.8.254
Lease Time	Set the validity period of the assigned IP address. After expiration, the DHCP server will reclaim the IP address assigned to the client and reassign the IP address. Unit: seconds	86400
Gateway Type	Support default, custom, respectively represent the default/Custom DHCP gateway	default
Gateway	The gateway address served by the DHCP server is the default LAN IP address	192.168.8.1
DNS Type	Support default, custom, respectively represent the default/Custom DHCP DNS server	default
DNS	The LAN port client domain name resolution server address is changed to the gateway address and the WAN port proxy DNS is used by default	192.168.8.1

3.6 Applications

3.6.1 ICMP

This product supports ICMP link monitoring functionality. Routers can detect communication link status, and when abnormal links are detected, the ICMP feature will execute corresponding actions based on user configurations to quickly restore normal operation of both links and the system. The product supports up to 10 ICMP monitoring rules to provide more comprehensive and reliable link status monitoring and maintenance capabilities. The ICMP configuration interface is shown in Figure 3-17.

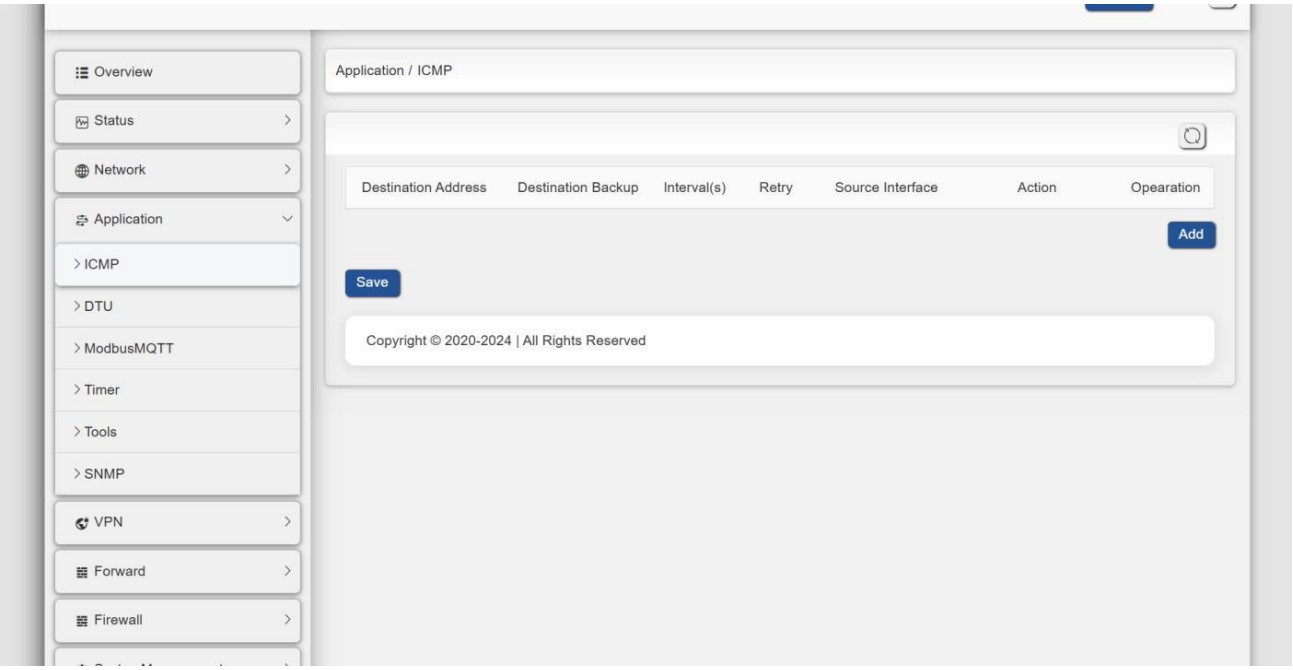


Figure 3-17 ICMP configuration interface

The main parameters of ICMP are shown in Table 3-7.

Table 3-7 Description of main ICMP parameters

name	parametric description	Default parameters
destination address	The test address is detected and the test is passed, indicating that the network is smooth	223.5.5.5
Backup address	The detection address used when the target address network is not working properly	not have
margin	Set the detection cycle, unit s	5
retry	Set the number of tests	3
Source interface	The data outlet of the network can be set as br-lan, eth-wan, mobile, etc.	mobile
movement	The action to be performed after detecting a network disconnection can be set to reboot (reboot) or mobile-reset (4G Mobile restart)	reboot

3.6.2 GPS (Optional)

The GPS feature of this product enables a wider range of IoT application scenarios and enhanced functionality. By integrating a GPS module, the device can obtain real-time location information. The GPS configuration interface is shown in Figure 3-18.

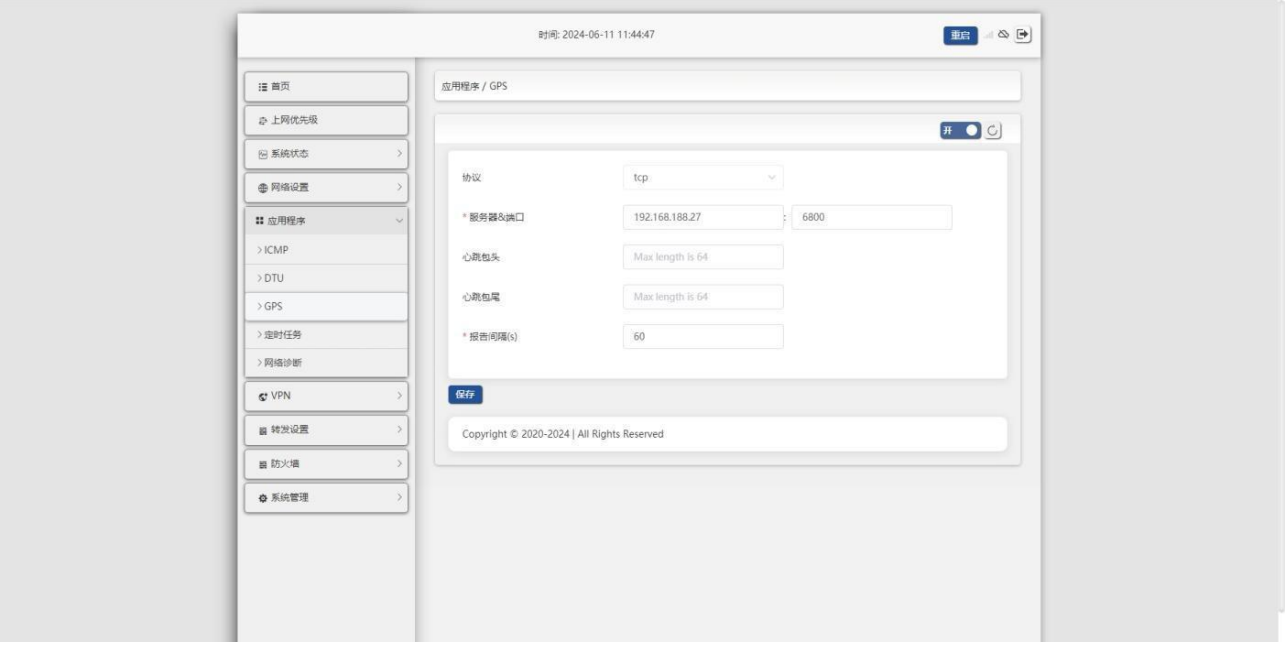


Figure 3-18 GPS configuration interface

The main parameters of GPS are shown in Table 3-8.

Table 3-8 Description of main GPS parameters

name	parametric description	Default parameters
protocol	Support TCP, UDP	tcp
Server & Port	The server address and port to which the GPS information is sent	not have
Heart beats at the head and tail	The GPS information is stitched between the head and tail of the heartbeat packet	not have
Report intervals	GPS information report server interval	60

3.6.3 Scheduled tasks

The router scheduled task is an automatically executed task preset on the router, which can perform network management and maintenance operations such as restarting the router at a specific time to improve network stability and management efficiency. The scheduled task configuration interface is shown in Figure 3-19.

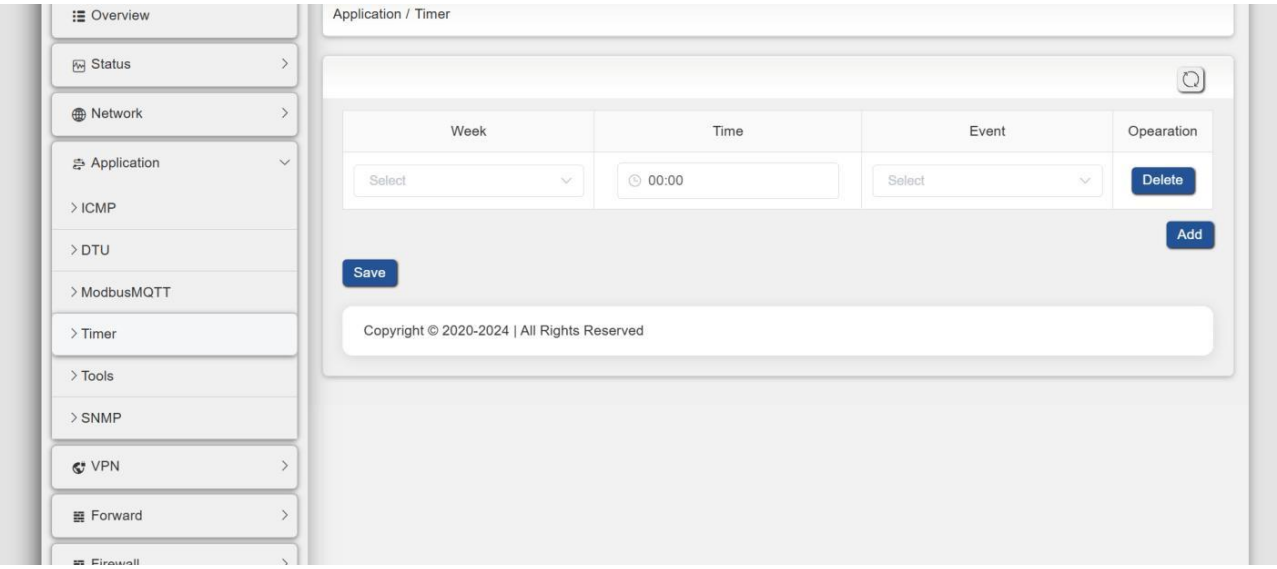


Figure 3-19 Timer task configuration interface

The main parameters of the scheduled task are shown in Table 3-9.

Table 3-9 Main parameters of scheduled tasks

name	parametric description	Default parameters
week	Support settings are set to Monday through Sunday and daily, Monday-Sunday, Everyday	not have
time	24-hour system	00：00
event	Support reboot (restart), mobile-reset (4G Mobile restart)	not have

3.6.4 Network Diagnostics

This product supports two network diagnostic tools: Ping and Tracert, designed to detect network connections and troubleshoot connectivity issues. Ping is used to test host connectivity and latency by sending Ping packets and waiting for responses to determine if the target host is reachable. Tracert tracks network paths by sending specialized data packets and recording the routers and nodes they pass through, thereby mapping the route to the target host and helping identify bottlenecks or failures in network connections. The network diagnostic interface is shown in Figure 3-20.

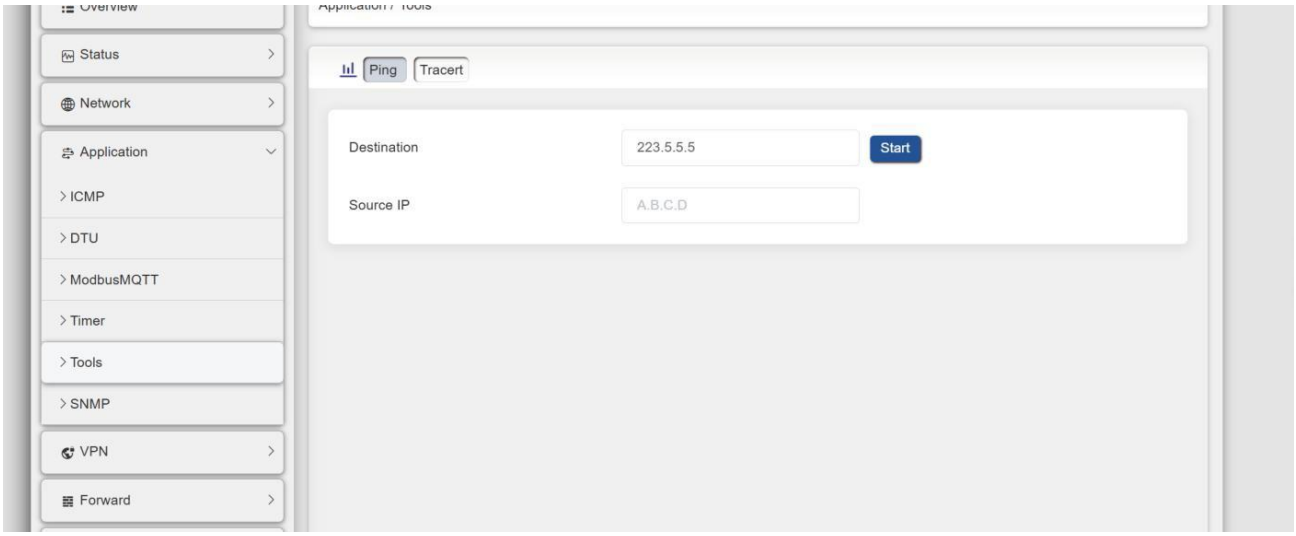


Figure 3-20 Network diagnostic interface

The main parameters of network diagnosis are shown in Table 3-10.

Table 3-10 Description of main parameters of network diagnosis

Name	Description	Default
destination address	Used to detect the address of a network connection	223.5.5.5
source address	Specifies the source address of the data packet to be sent	not have

3.7 VPN

3.7.1 L2TP

L2TP, the Layer 2 Tunneling Protocol (LTP), is used to support Virtual Private Networks (VPNs). By encapsulating data within IP packets at the network layer, L2TP enables users to establish virtual tunnels between two private networks over public networks like the Internet. The configuration interface for L2TP is illustrated in Figure 3-21.

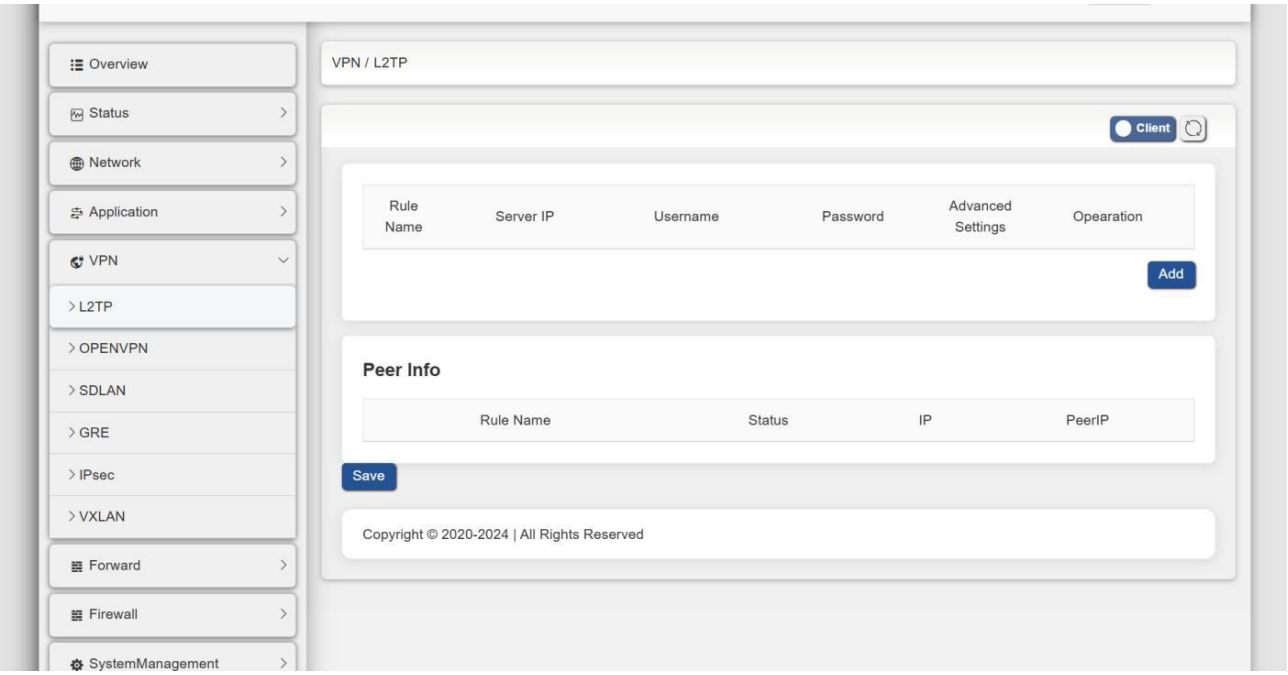


Figure 3-21 L2TP configuration interface

The main parameters of L2TP Client are shown in Table 3-11.

Table 3-11 L2TP Client main parameters description

Name	Description	Default
Rule name	A unique identifier that distinguishes multiple L2TP connections	not have
server IP	L2TP server address	not have
user name	The unique identifier assigned to a client user by the LTP server	not have
password	The L2TP password is the confidential information paired with the account name. The L2TP client needs to provide this password when connecting to the L2TP server to complete authentication	not have
advanced setup	Includes Settings for L2TP connection authentication, data compression, LCP interval (s), LCP retry, MTU, and MRU	/
Peer information		
Rule name	The rule name for an L2TP connection, which is used to distinguish between multiple different L2TP connections	/
state	Disconnect indicates not connected, Connected indicates	/

	connected	
IP	The server is assigned a virtual IP for the L2TP connection	/
end on IP	Virtual IP for LTP server	/

The main parameters of L2TP Server are shown in Table 3-12.

Table 3-12 L2TP Server main parameters table

name	parametric description	Default parameters
Local address	The service IP of the LTP server	empty
IP pool	Assign a virtual IP to the L2TP connection, such as 172.16.10.1-172.16.10.253	empty
user name	The unique identifier assigned to a client user by the LTP server	empty
password	The L2TP password is the confidential information paired with the account name. The user needs to provide this password when connecting to the L2TP server to complete the authentication	empty
attestation	Supports simultaneous verification of CHAP, PAP, MS-CHAP, MS2-CHAP, and EAP with zero or more	Full validation
compress	Supports compression of L2TP data	empty
LCP interval (s)	In the LCP phase, the time interval (s) between control packets sent periodically during the L2TP tunnel establishment	30
LCP retry	In the LCP phase, if the previous LCP request is not responded to, the number of retries for sending the LCP request again	5
MTU	The maximum packet size (in bytes) that can be transmitted in an LTP connection	1400
MRU	The maximum packet size (in bytes) that an LTP connection can receive	1400

3.7.2 OPENVPN

OPENVPN is an open-source virtual private network (VPN) solution that enables secure remote access and communication through encryption and tunneling technologies. To utilize OPENVPN, users need to configure an OPENVPN server on the public network and perform corresponding

settings on their routers, including server address, port number, certificates, and keys. After successful connection, the router can securely transmit data via the OPENVPN tunnel, enabling remote access and communication while ensuring data security and privacy. This allows the product to provide users with a reliable remote access solution, facilitating cross-regional network connectivity. The OPENVPN configuration interface is shown in Figure 3-22.

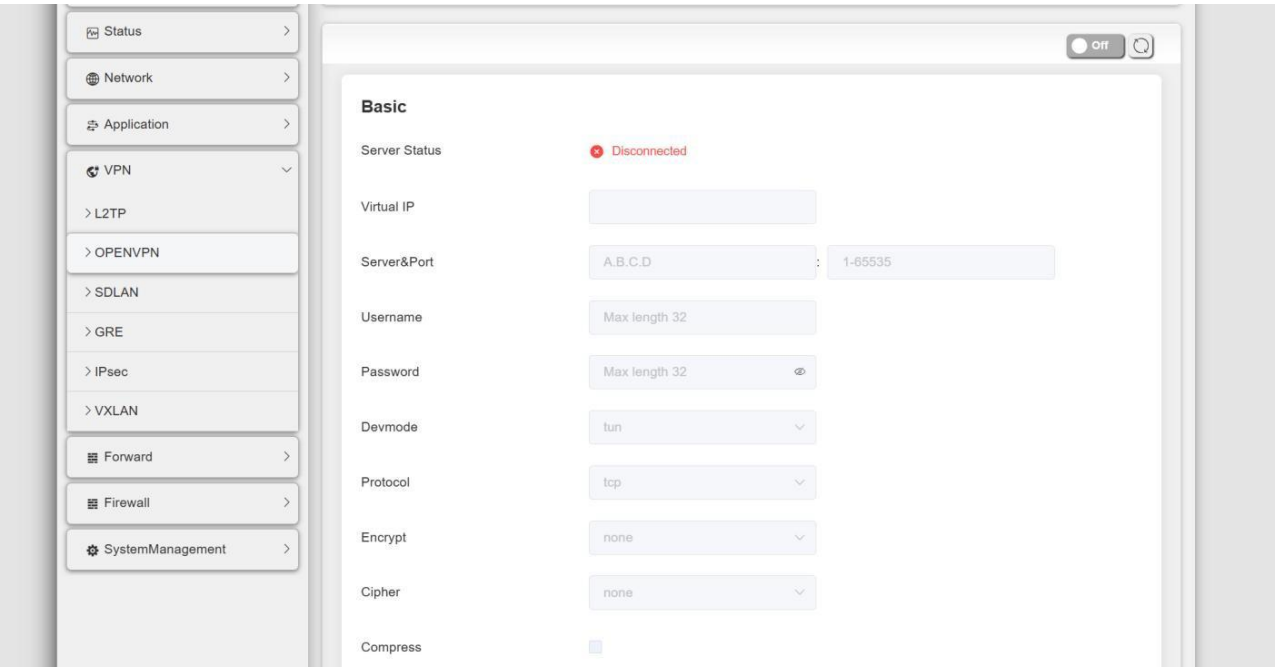


Figure 3-22 OPENVPN configuration interface

The main parameters of OPENVPN are shown in Table 3-13.

Table 3-13 OPENVPN main parameter description

name	parametric description	Default parameters
invented IP	The virtual IP assigned by the OPENVPN server is read only	not have
Server & Port	OPENVPN server address and port	not have
user name	The user name used to log into the OPENVPN server	not have
password	The password used to open the OPENVPN server	not have
Dev pattern	Support tun, tap	tun
protocol	Support TCP, UDP	tcp

encryption	The OPENVPN authentication and signature algorithms are used for digital signatures during the authentication and key negotiation processes.	not have
Cipher	OPENVPN is a password suite for encrypted data transmission, which is mainly used to protect the confidentiality of data.	not have
CA	CA is a trusted entity responsible for issuing digital certificates to verify the identity of an entity and the authenticity of a digital signature. It needs to be imported	not have
cipher code	A key is an algorithmic parameter used to encrypt and decrypt data. It can be a symmetric key or an asymmetric key. It needs to be imported	not have
certificate	A certificate is a digital file issued by the CA that contains public key, identity information of the holder, and digital signature. It is used to verify the identity of the entity and the authenticity of the digital signature. It needs to be imported	not have

3.7.2.1 OPENVPN connection instance

The address and port of the OPENVPN server is 43.139.192.212:20002. The required files are ca.crt, clientX.key, clientX.crt. The steps to connect to the OPENVPN server are as follows:

Step 1: Import the ca.crt, clientX.key, clientX.crt file. The import process is shown in Figure 3-23.

Figure 3-23 OPENVPN file import process diagram

Step 2: Open the OPENVPN service and fill in the server IP and port, and then fill in or select the corresponding configuration according to the server configured parameters. The configuration process is shown in Figure 3-24.

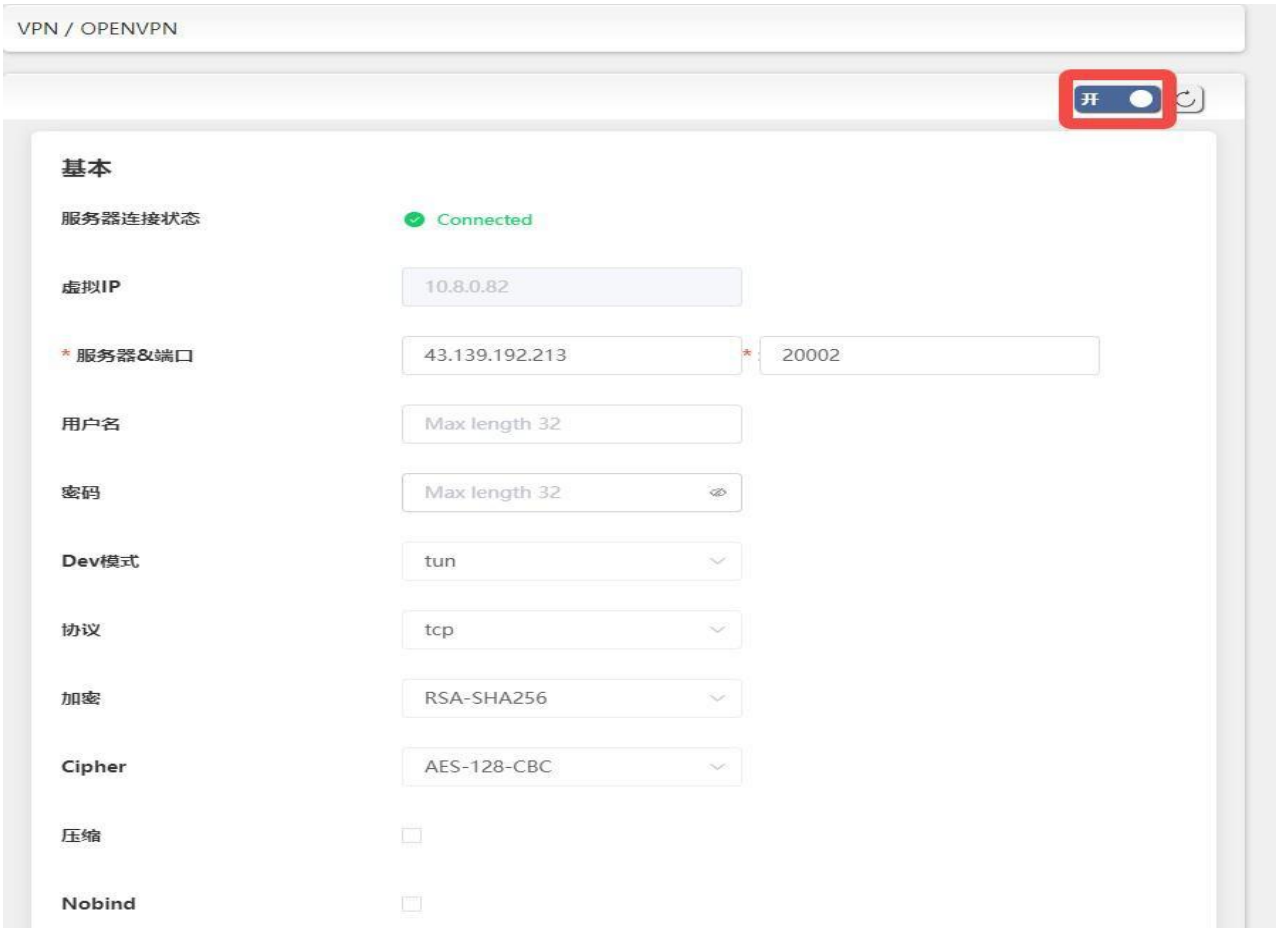


Figure 3-24 OPENVPN parameter configuration process diagram

Step 3: Configure the certificate and save it. The configuration entries are shown in Figure 3-25.

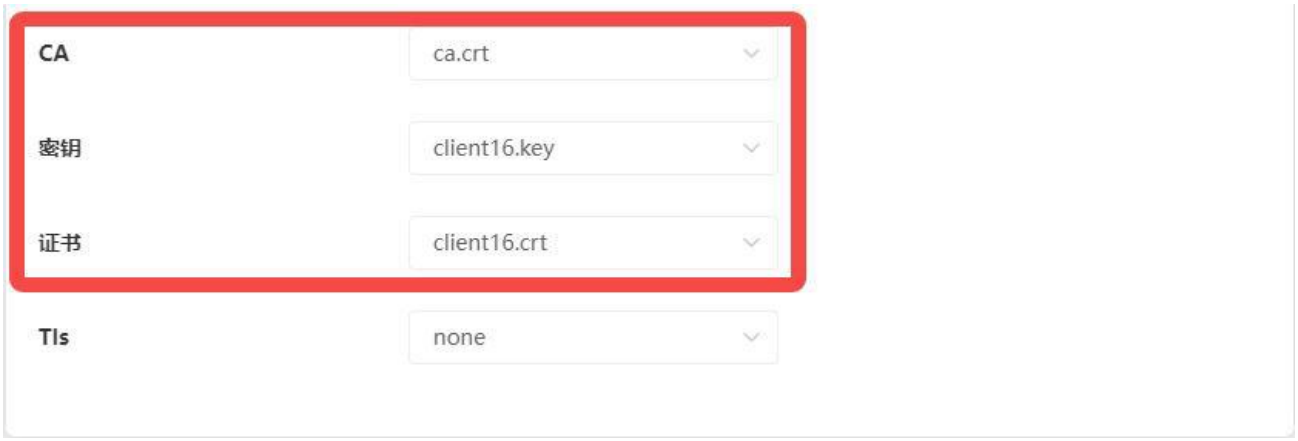


Figure 3-25 OPENVPN certificate configuration diagram

Step 4: Refresh the page and wait for the connection to succeed.

3.7.3 SDLAN

This product has a built-in SDLAN client to connect to the SDLAN server for point-to-point communication. The configured peer information can penetrate the virtual address to connect to the peer subnet, enabling direct communication between the device and the peer subnet. The SDLAN configuration interface is shown in Figure 3-26.

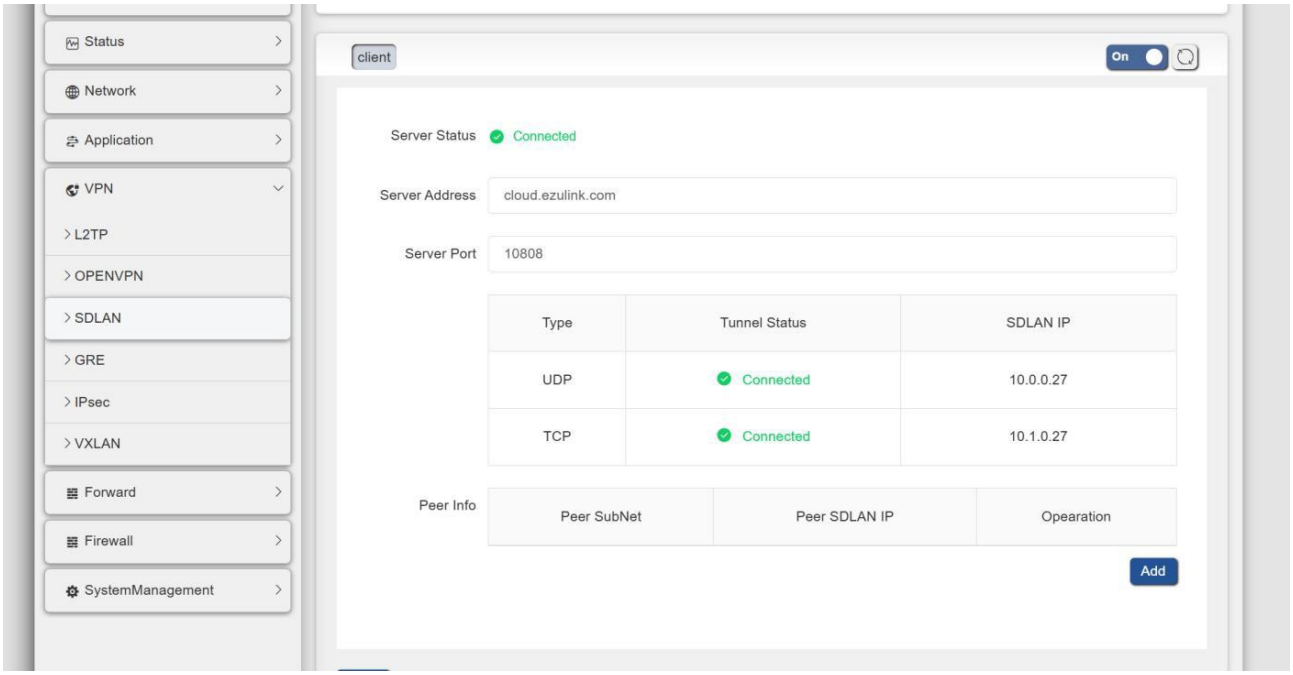


Figure 3-26 SDLAN configuration interface

The main parameters of SDLAN are shown in Table 3-14.

Table 3-14 Main parameters of SDLAN

name	parametric description	Default parameters
Server address	SDLAN server address, supports domain name and IP	cloud.ezulink.com
Server port	SDLAN server port	10808
SDLAN IP	The identifier IP connected to the SDLAN server is used to distinguish different devices and network, read only	not have
On the end subnet	Address of the subnet of the peer device to be connected	not have
The peer-side SDLAN IP	The SDLAN IP of the peer device that needs to be connected	not have

Let's learn how to use SDLAN through a simple example. The specific scenario is: several

routers in different geographical locations can communicate with each other without configuration and power on in a networked environment. The network topology diagram is shown in Figure 3-27.

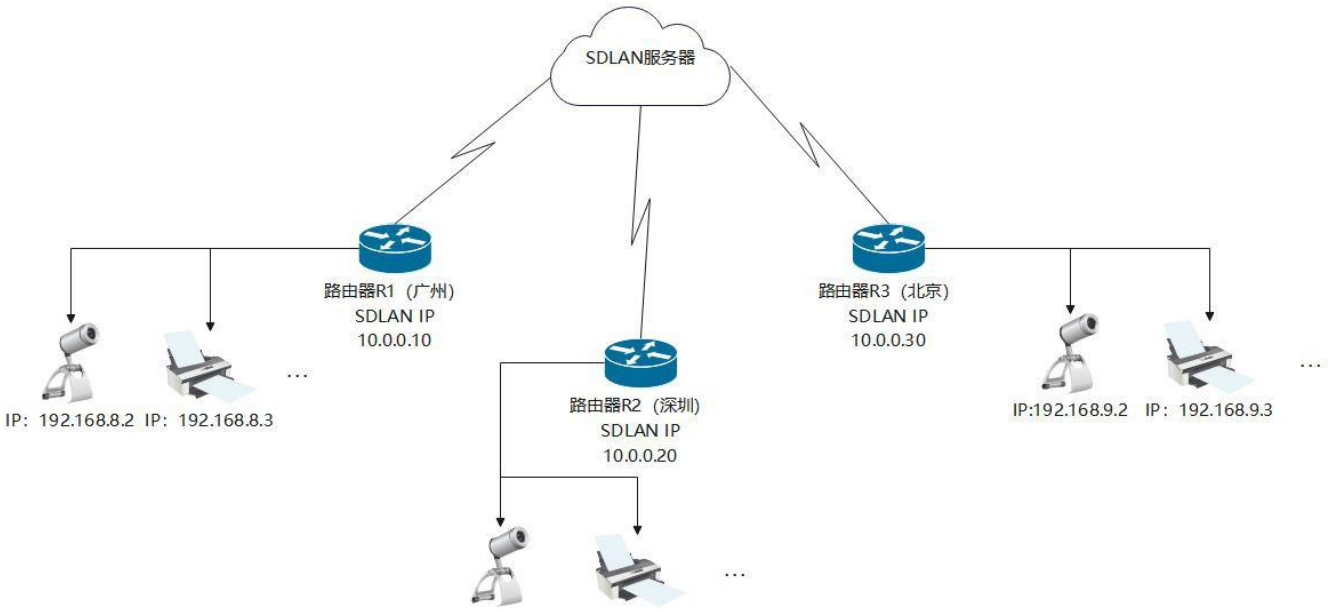


Figure 3-27 Example network topology of SDLAN

Before equipment leaves the factory, we pre-allocate SDLAN IP addresses and other essential information for devices requiring network configuration. Users simply need to power on the router and connect to the internet, completing setup without any configuration. Once the server is activated, encrypted data communicates through tunnel-based peer-to-peer communication without server mediation. To access devices within the router's subnet, simply specify the peer subnet and SDLAN IP address. For example, to access a camera in Beijing from Guangzhou, configure the peer subnet on router R1 as 192.168.9.0/24 and the peer SDLAN IP as 10.0.0.30. Detailed configuration is shown in Figure 3-28.

Note: Router subnet segments cannot be the same.

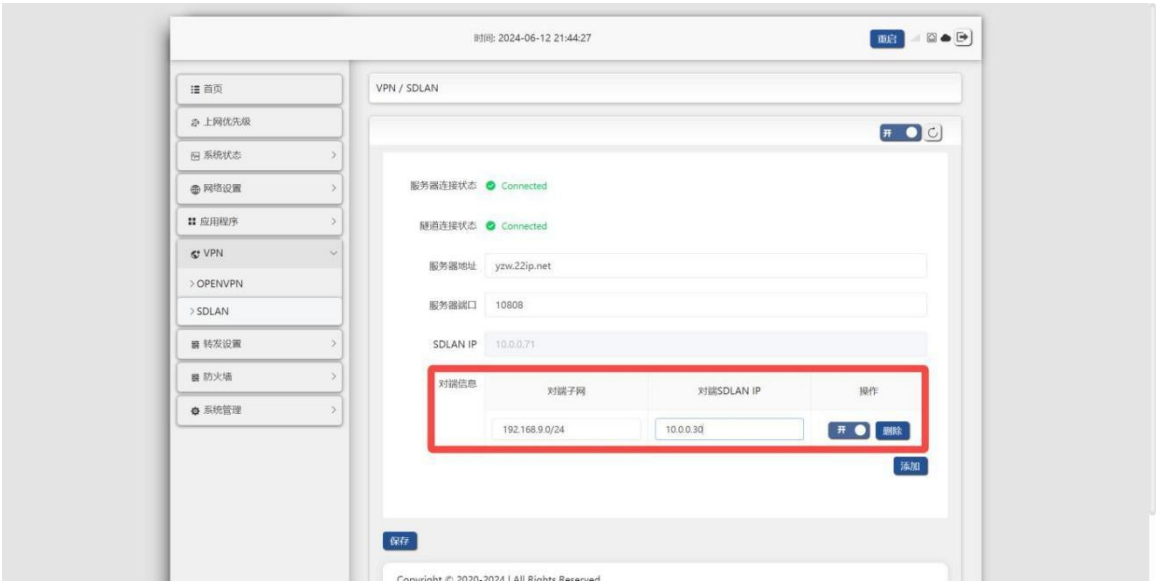


Figure 3-28 SDLAN configuration

3.7.4 GRE

GRE (Generic Routing Encapsulation), a Layer 2 tunneling technology, enables the encapsulation of data packets from various network layer protocols and facilitates their transmission across different physical networks through dedicated tunnels. The latest version of this product supports GRE functionality to achieve packet encapsulation and transmission of diverse network layer protocols. Figure 3-29 illustrates the GRE configuration interface.

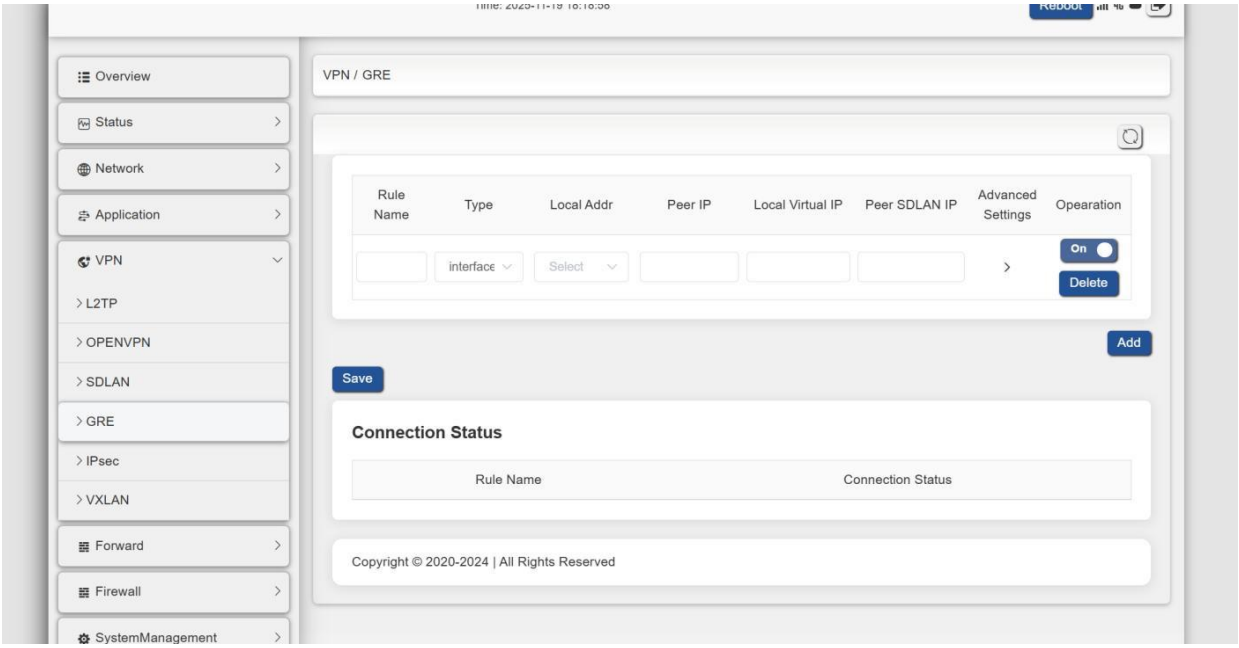


Figure 3-29 GRE configuration interface

The main parameters of GRE are shown in Table 3-15.

Table 3-15 Main parameters of GRE

Name	Description	Default
Specifications name	GRE rule name, the difference between rules identification	not have
this locality IP	The interface IP of the encapsulated network protocol	not have
end on IP	The interface IP of the peer-end network protocol	not have
Local virtual IP	The virtual address used after the connection is successful	not have
Peer-end virtual IP	The virtual address used by the peer after a successful connection	not have
Tunnel keys	The matching key must be the same for both sides of the GRE connection	not have
Maintain activity intervals (s)	GRE connection and detection interval (seconds)	30
Keep activities retrying	GRE connections and retry times	5

Note: Two identical GRE rules must be guaranteed to have different names and tunnel keys at the same time.

3.7.5 IPSEC

IPsec (Internet Protocol Security) is a protocol suite designed to protect IP network communications. It ensures data security during transmission through encryption and authentication mechanisms. Primarily used to establish secure virtual private networks (VPNs) over insecure networks like the Internet, IPsec safeguards data confidentiality, integrity, and identity verification. The latest version of this product supports IPsec functionality to achieve data encryption and transmission protection. The IPsec configuration interface is illustrated in Figure 3-30.

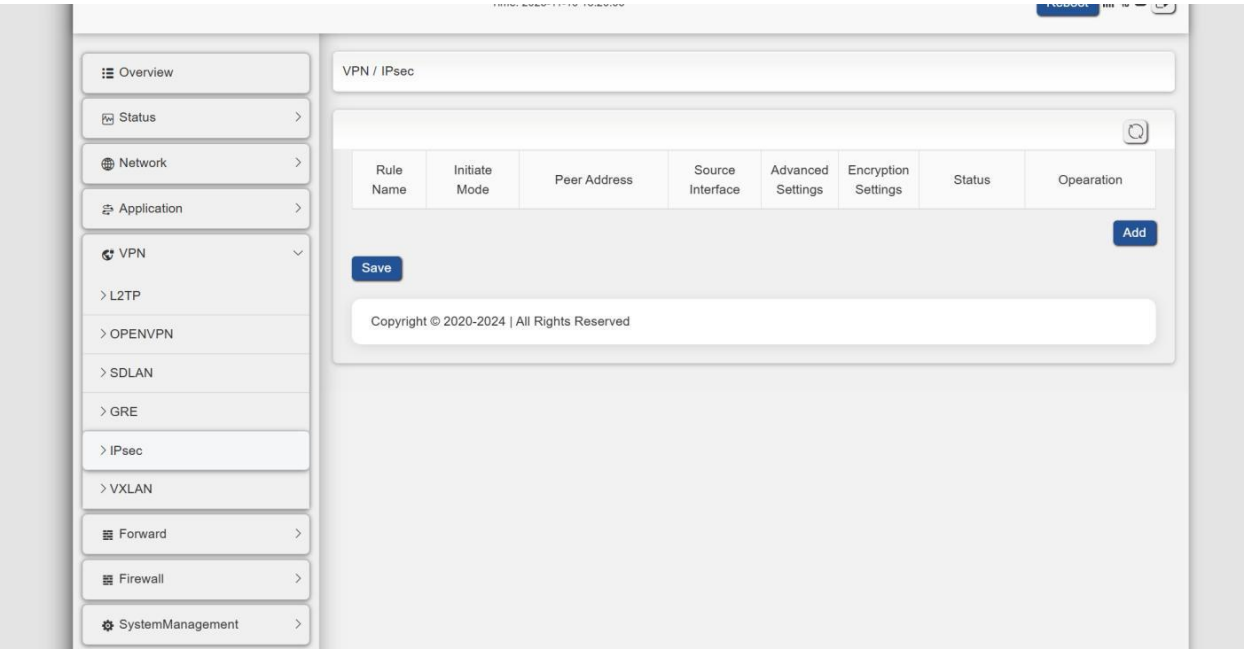


Figure 3-30 IPsec configuration interface diagram

The main parameters of IPSec are shown in Table 3-16.

Table 3-16 IPsec main parameters table

name	parametric description	Default parameters
Specifications name	IPSec rule name, the difference between rules identification	not have
Launch mode	Support main/aggr mode switch	main
Target address	Encrypt the interface IP of the peer	not have
Source interface	IPSec data encryption interface	br-lan
advanced setup	Supports the selection of policy patterns	transport
Encryption Settings	Includes the parameter configuration for ike and ipsec	/

3.7.6 VXLAN

VXLAN (Virtual Extensible LAN) is a network virtualization technology designed to address scalability and flexibility challenges in traditional VLAN (Virtual Local Area Network) deployments within large-scale data center networks. By encapsulating Ethernet frames into UDP packets, VXLAN enables Layer 2 network expansion across multiple physical networks. This allows virtual machines (VMs)and containers to communicate across different physical locations, providing enhanced network isolation and flexible

network topology. The latest version of this product supports VXLAN virtual LAN technology to provide network scalability and flexibility. The VXLAN configuration interface is shown in Figure 3-31.

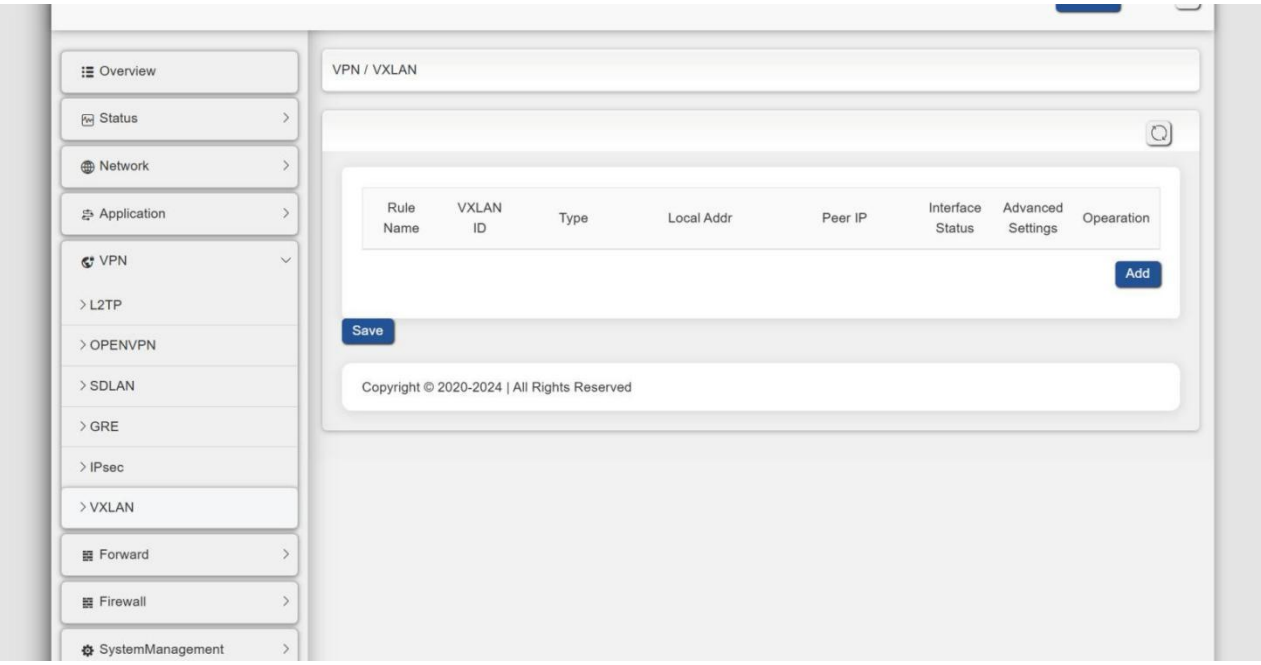


Figure 3-31 VXLAN configuration interface diagram

The main parameters of VXLAN are shown in Table 3-17.

Table 3-17 Main parameters of VXLAN

name	parametric description	Defaultparameters
Specifications name	VXLAN rule name, the difference between rules identification	not have
VXLAN ID	The VXLAN ID of the two parties connected must be equal to the unique identifier of the VXLAN in the network. Scope: 1-16777215	not have
this locality IP	Java native interface Java IP	not have
end on IP	Outbound interface IP	not have
interface message	VXLAN interface status: DOWN/UP	/
End-to-end ports	VXLAN peer enabled on the peer	4789
Local virtual IP	The virtual IP of VXLAN interface is not mandatory	not have

3.8 Forwarding Settings

3.8.1 NAT

This product supports NAT functionality, which converts IP addresses based on user-defined rules. The system features three core functionalities: Destination Network Address Translation (DNAT), Source Network Address Translation (SNAT), and Demilitarized Zone (DMZ). The NAT configuration interface is illustrated in Figure 3-32.

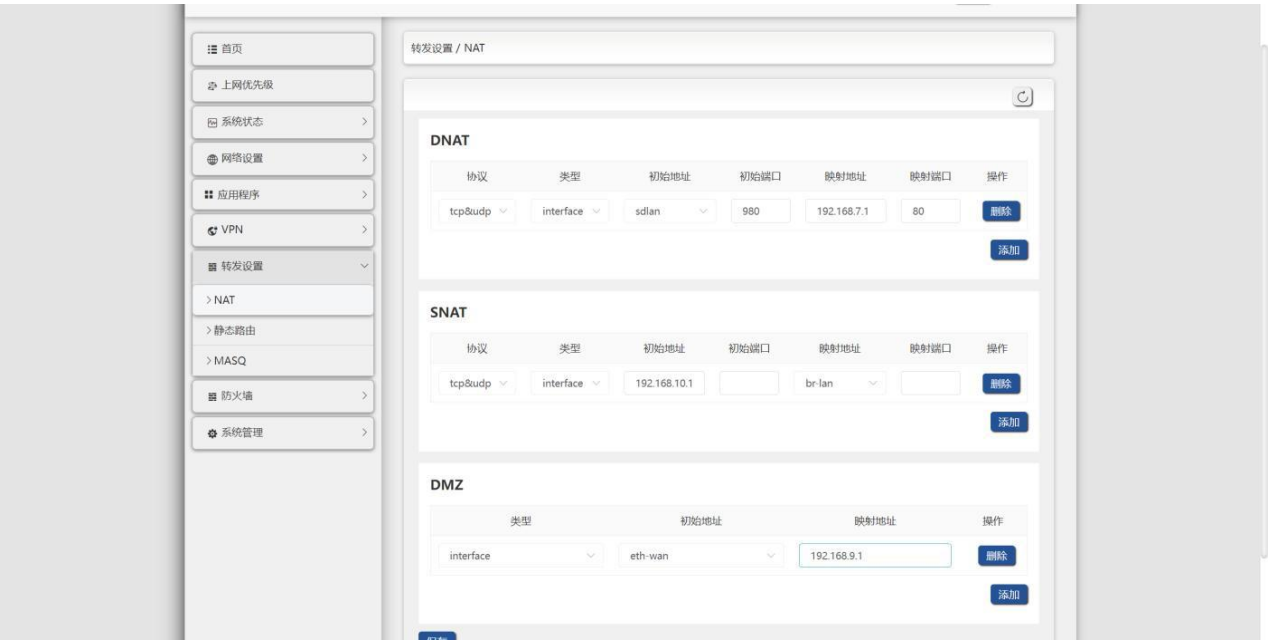


Figure 3-32 NAT configuration interface

The main parameters of NAT are shown in Table 3-18.

Table 3-18 NAT main parameters description

name	parametric description	Default parameters
DNAT (Target Network Address Translation)		
protocol	Support TCP, UDP, TCP&UDP, ICMP	tcp&udp
type	Support interface,ip	interface
Initial address	Client addresses in external networks, support interfaces and IP	not have
Initial port	The port used by the external client is not filled in. The default option is all ports	not have
Mapping address	Server address in the internal network	not have
Mapping port	The server port provided by the internal server. Do not fill in the default selection of all ports	not have

SNAT (Source Network Address Translation)		
name	parametric description	Default parameters
Protocol	Support TCP, UDP, TCP&UDP, ICMP	tcp&udp
type	Support interface,ip	interface
Initial address	Client address in the internal network	not have
Initial port	The port used by the internal client is not filled in. The default is all ports	not have
Mapping address	External network addresses, support interfaces and IP	not have
Mapping port	The server port provided by the external network is not filled in. The default selection is all interfaces	not have
DMZ		
type	Support interface,ip	interface
Initial address	Client addresses in external networks, support interfaces and IP	not have
Mapping address	Server address on the internal network	not have

Let's learn the use of NAT through a simple example. The specific scenario is: access the device with IP address 192.168.7.2 in the subnet of router R1 in the same network segment without adding static routes, and the network topology diagram is shown in Figure 3-33.

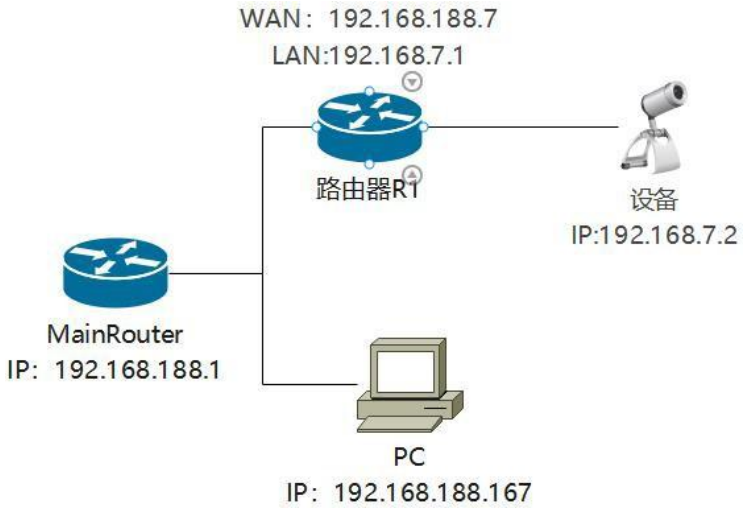


Figure 3-33 NAT example network topology

Method 1: Configure DNAT (recommended)

To map Router R1's port 980 to the device's port 80 (HTTP port), enter 192.168.188.7:980 in your browser to access the device page. Note that leaving ports unconfigured (default settings apply) creates a DMZ. The configuration is illustrated in Figure 3-34.

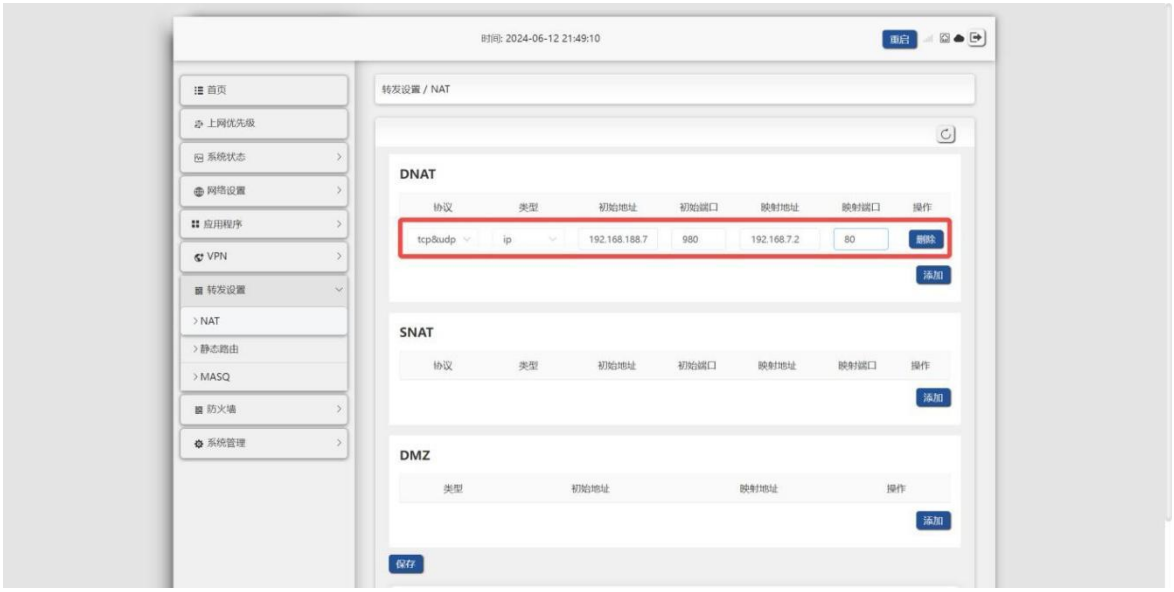


Figure 3-34 DNAT configuration

Method 2: Configure DMZ (not recommended)

Map all ports of router R1 to the corresponding device ports. Use a browser and enter 192.168.188.7 to access the device page. (The interface of router R1 cannot be accessed because all ports of router R1 are mapped to the device). The specific configuration is shown in Figure 3-35.

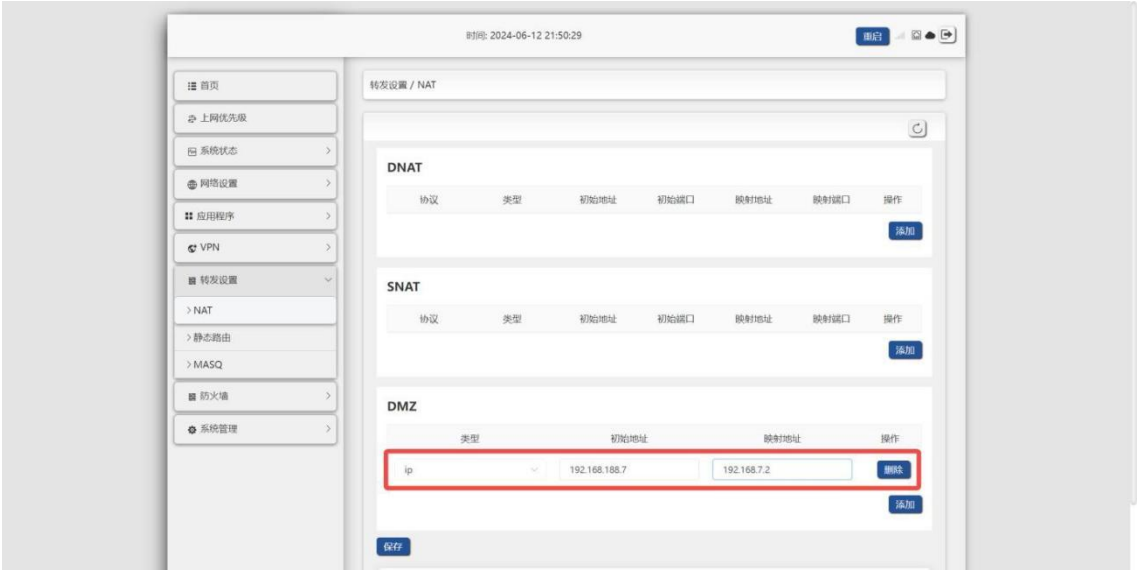


Figure 3-35 DMZ configuration

Note: If you accidentally configure the full DNAT port or DMZ and cannot access the R1 router webpage, you can set a static route on the PC to enter the page from the LAN port (192.168.7.1) of R1 router to delete or modify the configuration. The static route configuration on the PC (invalid after shutdown)

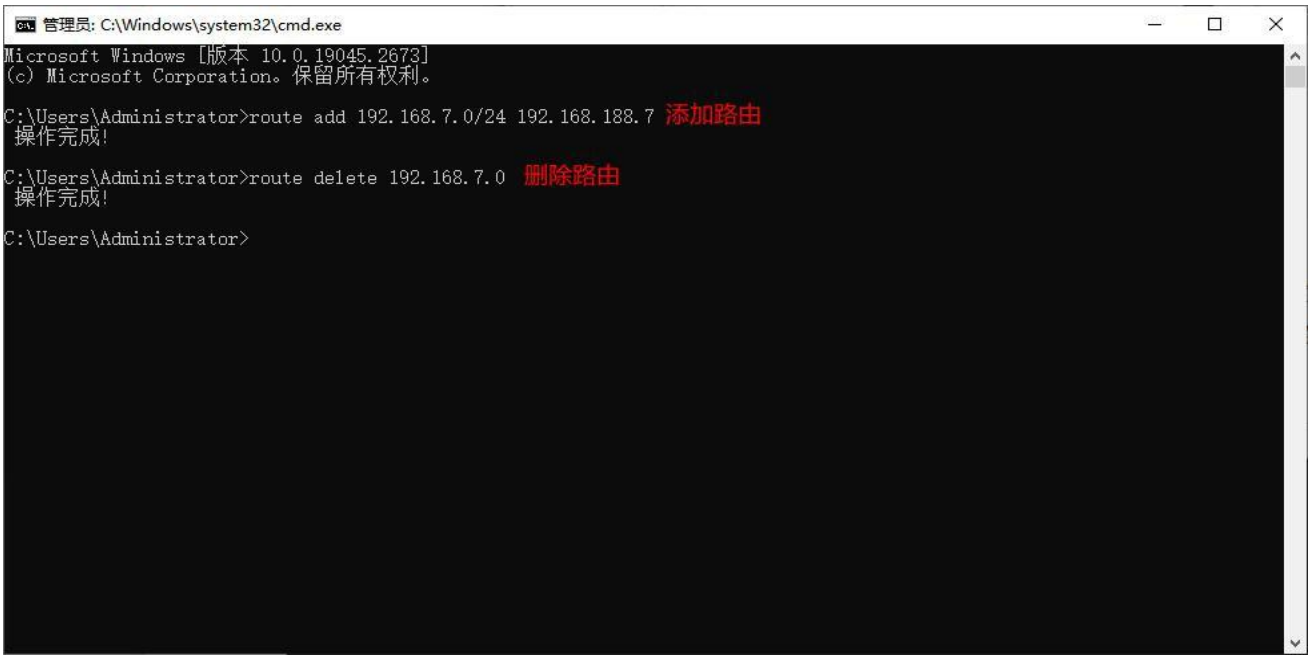


Figure 3-36 Adding and removing static routes on a PC

3.8.2 Static routing

This product supports static routing Settings, allowing users to manually configure routes to specify the transmission path of packets and provide fine network traffic control. The static routing configuration interface is shown in Figure 3-37.

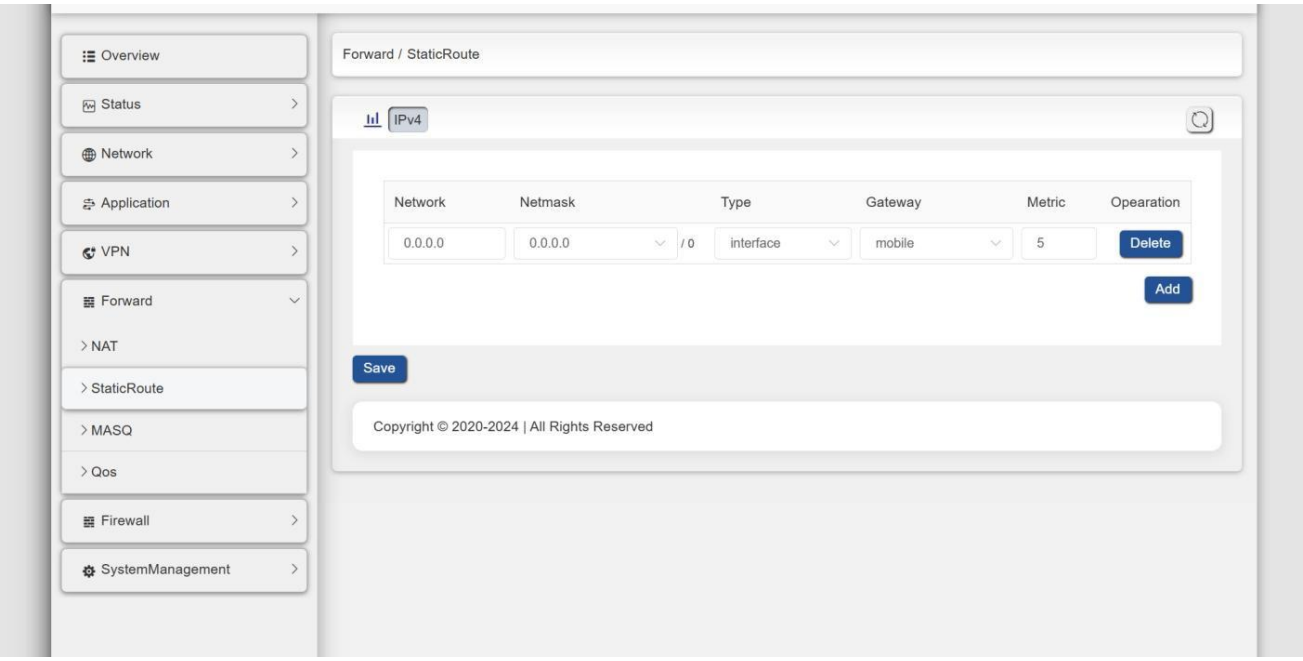


Figure 3-37 Static routing configuration interface

The main parameters of static routing are shown in Table 3-19.

Table 3-19 Description of main parameters of static routing

Name	Description	Default
network	destination address	not have
subnet mask	Subnet mask of the destination address	empty
type	Support interface,ip	interface
gateway	The next router IP address, supporting interface and IP that the data needs to pass through before reaching the destination address	Superior gateway address
priority	Rule priority, the lower the number, the higher the priority	5

Static routing describes the routing rules for data packets on an Ethernet network. The following example shows how static routing works in a simple scenario: A device on the 192.168.2.0 network accesses a device on the 192.168.1.0 network by configuring static routing. The network topology is shown in Figure 3-38.

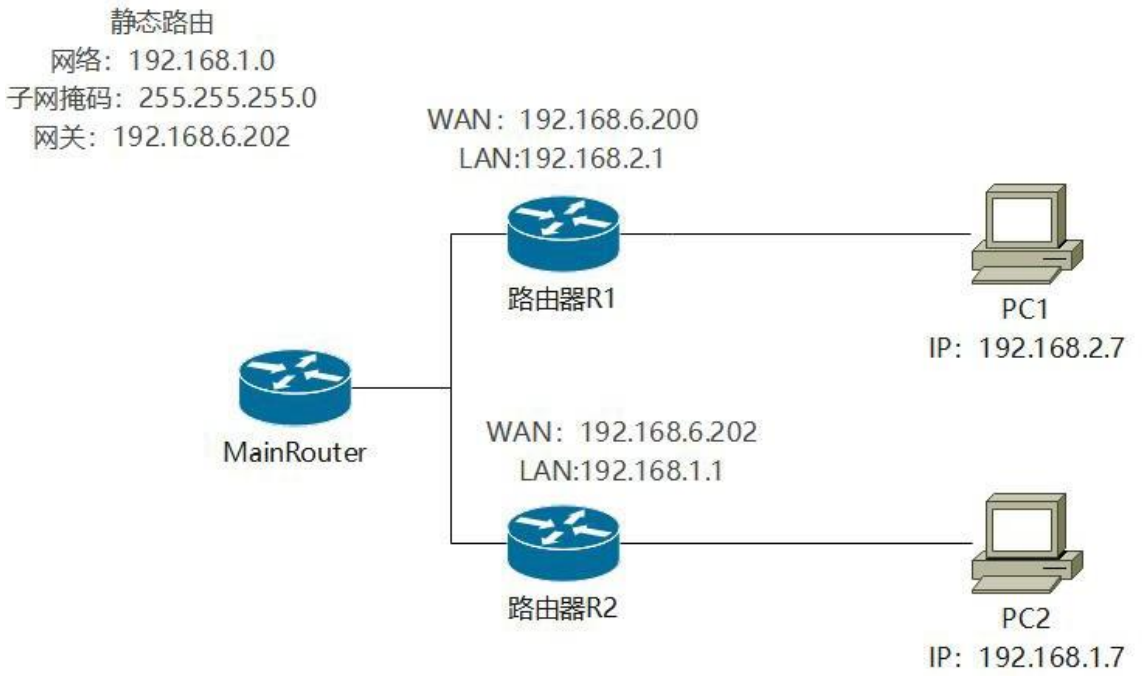


Figure 3-38 Static routing example network topology

All WAN ports of the routers are connected to the 192.168.6.0 network. Router R1's LAN port belongs to the 192.168.2.0 subnet, while Router R2's LAN is in the 192.168.1.0 subnet. We need to configure a route on Router R1 to automatically forward 192.168.1.x addresses to Router R2. Since this route needs to forward to all 192.168.1.x network segments, the subnet mask is set to 255.255.255.0 during configuration. The detailed setup is shown in Figure 3-39.

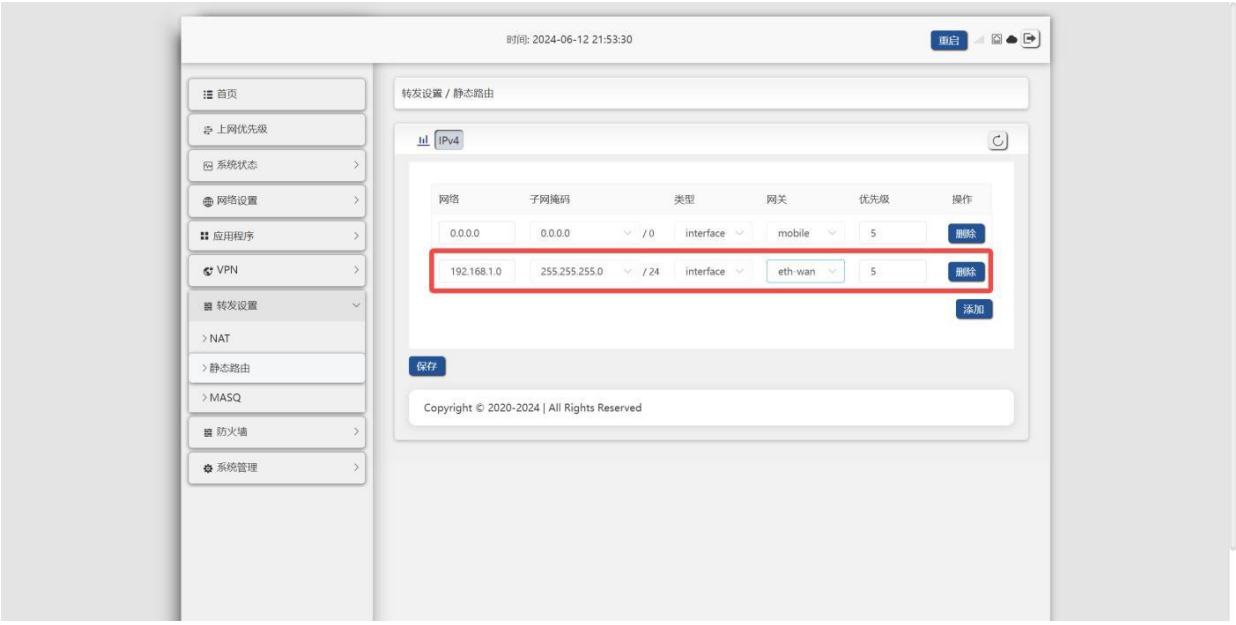


Figure 3-39 Static routing configuration

3.8.3 MASQ

This product supports MASQ functionality, which converts internal IP addresses within a local area network into public IP addresses for routers to enable internet communication. Additionally, MASQ effectively hides internal network IP addresses. The MASQ configuration interface is shown in Figure 3-40.

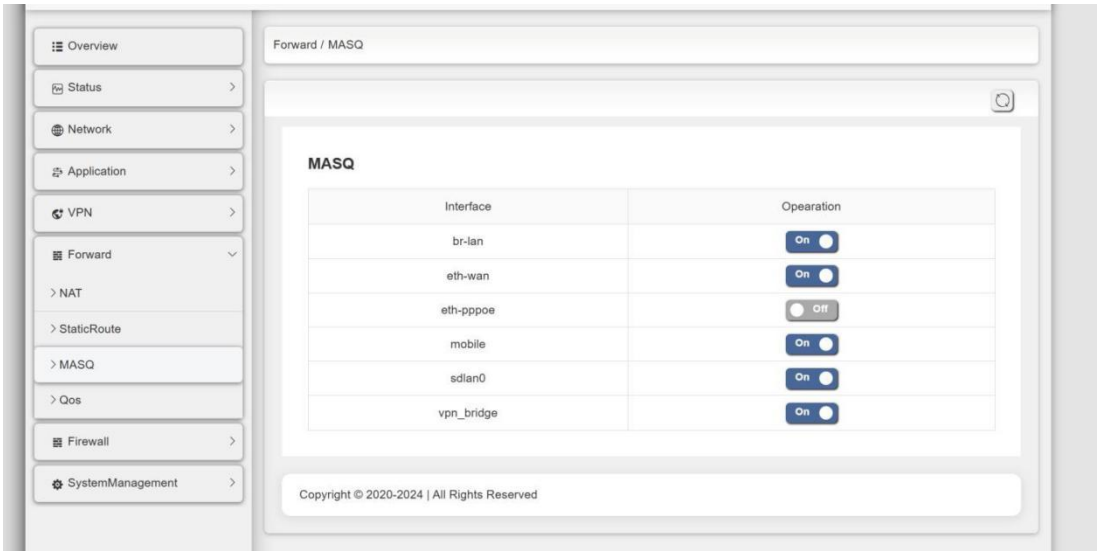


Figure 3-40 MASQ configuration interface

3.8.4 QoS

This product supports QoS function, which can manage the uplink/downlink rate of connected clients in the LAN to ensure that the data transmitted over the network meets certain performance requirements. The QoS configuration interface is shown in Figure 3-41.

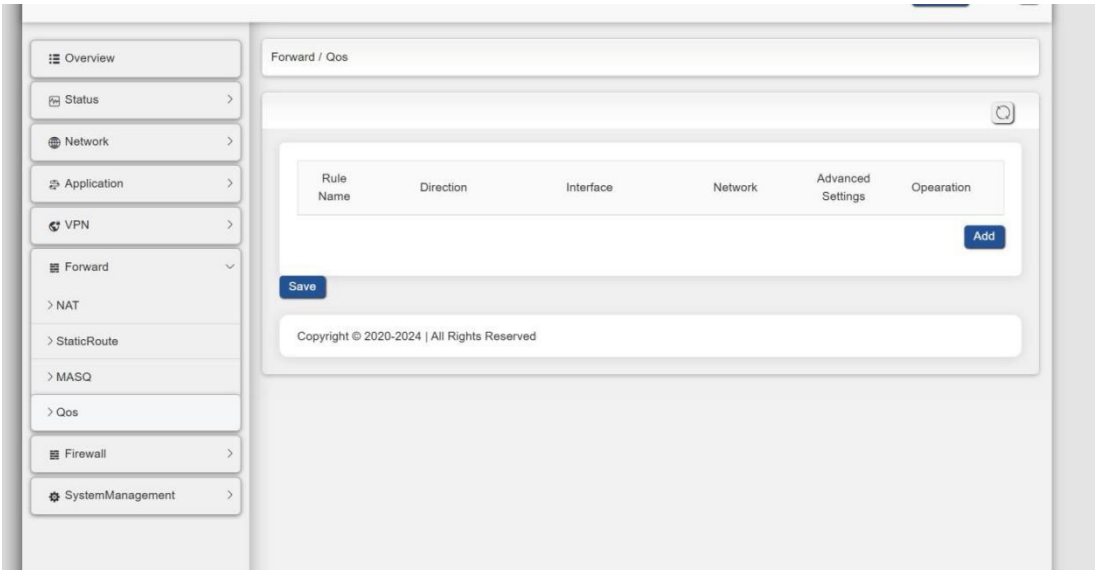


Figure 3-41 Qos configuration interface

The main parameters of QOS are shown in Table 3-20.

Table 3-20 QoS main parameters table

name	parametric description	Default parameters
Rule name	QoS rule name, used to uniquely identify a QoS rule	not have
direction	upload means that the uplink interface is selected and download means that the downlink interface is selected	upload
joggle	Data connectivity interface, optional eth-wan/eth-pppoe/mobile	eth-wan
network	The network target can be 192.168.8.0/24 by default	not have
advanced setup	Ports (empty for all ports), rates, maximum rates, and priorities can be configured	not have

3.9 Firewalls

3.9.1 Port Settings

In the port configuration interface, users can modify the HTTP port and CLI mode. By default, the HTTP port is set to 80. If the HTTP port is modified, users must specify the new port when accessing the device's web interface. For example, if the HTTP port is changed to 980, users need to enter 192.168.8.1:980 to access the device's management page. The port configuration interface is illustrated in Figure 3-42.

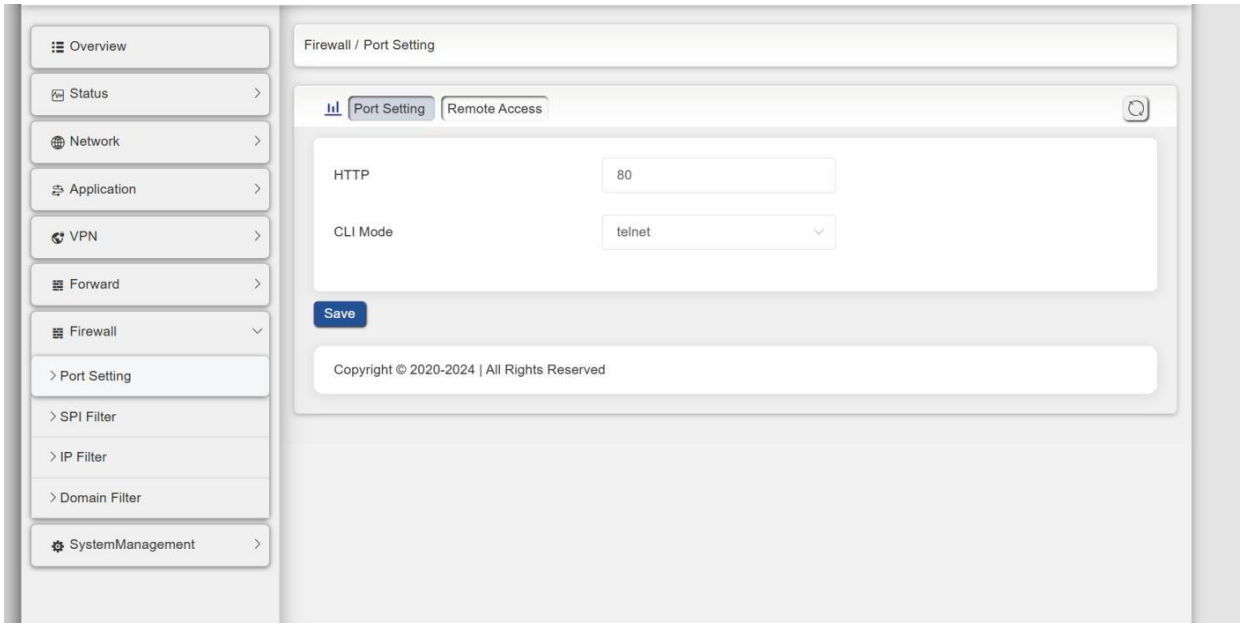


Figure 3-42 Port configuration interface

In the remote access interface, data access restrictions can be imposed on LAN, WAN and VPN (OpenVPN) interfaces by specifying the allowed protocol types, thereby improving network security and management flexibility. The remote management configuration interface is shown in Figure 3-43.

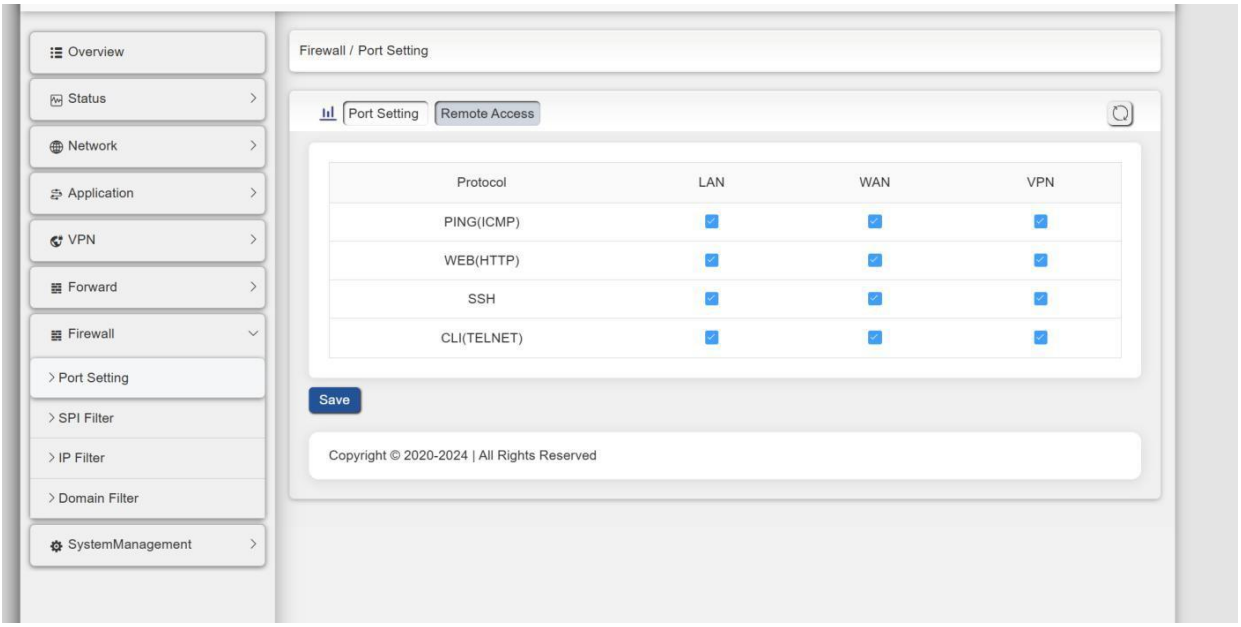


Figure 3-43 Remote access configuration interface

3.9.2 SPI filtering

This product supports SPI (state packet detection) filtering function, which improves network security and prevents illegal access and attacks by detecting and filtering data packets entering and leaving the network. SPI filtering configuration interface is shown in Figure 3-44.

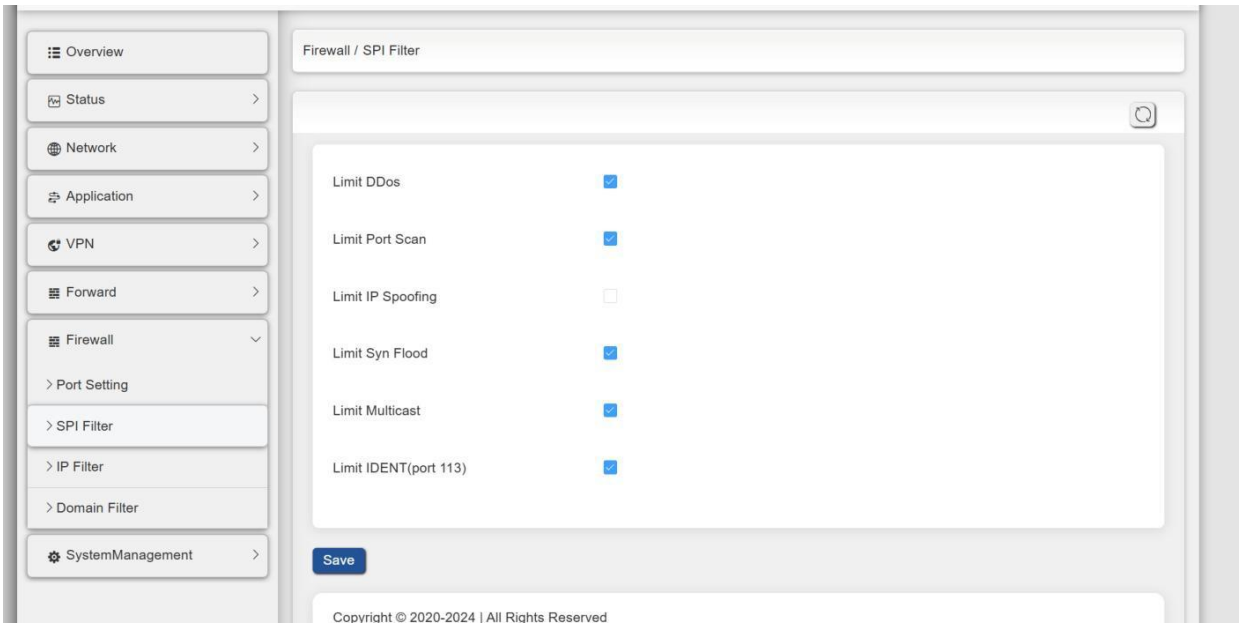


Figure 3-44 SPI filter configuration interface

The main parameters of SPI filtering are shown in Table 3-21.

Table 3-21 SPI filter main parameters description

name	parametric description	Default parameters
Limit DDoS attacks	Prevent service outages caused by large-scale network attacks.	open
Limit port scanning	Prevent potential attackers from finding vulnerabilities and breaking into the network.	open
Limit IP spoofing	Identify and block traffic using forged IP addresses	open
Limiting Syn Floods	Prevents attacks that consume server resources by sending large SYN packets.	close
Restrict multicast	Control and filter multicast traffic that is unnecessary or potentially malicious.	open
Restriction ID (port 113)	Prevent leakage of service information, improve network privacy and security.	open

3.9.3 IP filtering

The IP filtering feature in this product enables users to control and manage network traffic based on IP addresses, including allowing or denying access from specific IP addresses, blocking attacks from malicious IP addresses, protecting network resources from unauthorized access, and filtering outbound traffic. This functionality enhances network security and management efficiency. The IP filtering configuration interface is shown in Figure 3-45.

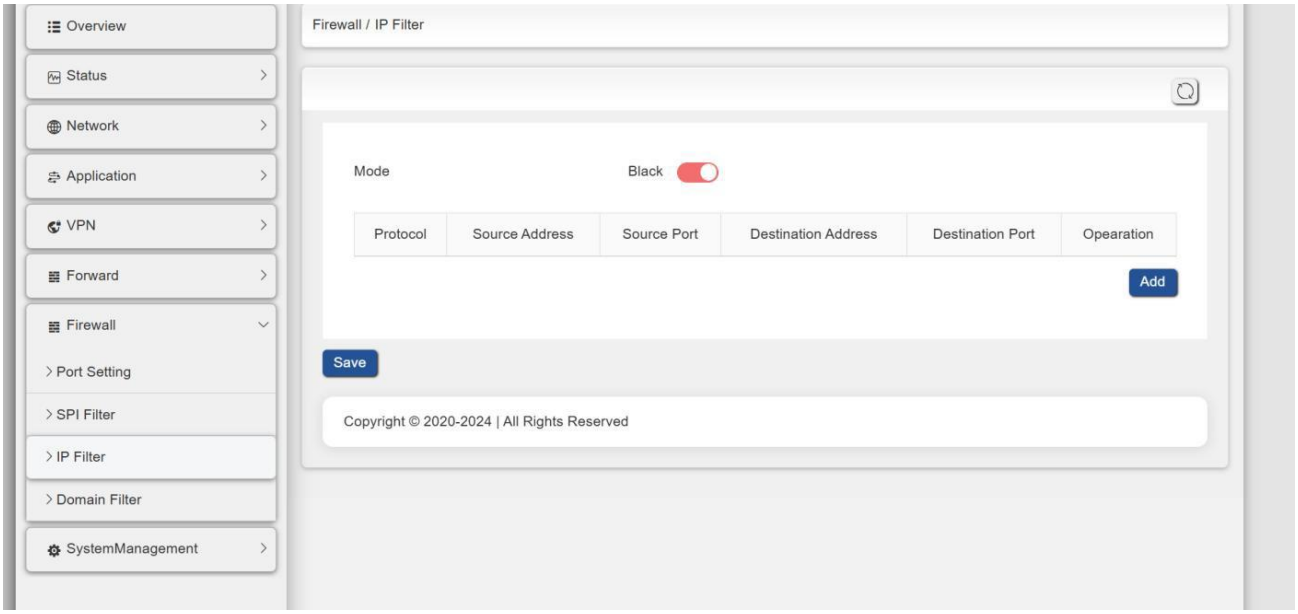


Figure 3-45 IP filtering configuration interface

The main parameters of IP filter are shown in Table 3-22.

Table 3-22 IP filtering main parameters description

name	parametric description	Default parameters
State	Support black (blacklist) and white (whitelist)	black
Protocol	The network protocol used by the IP to be filtered supports tcp,udp,tcp&udp, icmp	not have
Source address	Address of the source of traffic to be filtered	not have
Source port	The port of the traffic source to be filtered is not filled in by default	not have
Destination address	The target address of the traffic to be filtered	not have
Target port	The target port of the traffic to be filtered. If not specified, all ports are assumed	not have

Let's learn how to use IP filtering with a simple example. Let's say you want to limit Ping requests from PC (192.168.8.8) to address 223.5.5.5. The configuration is shown in Figure 3-46.

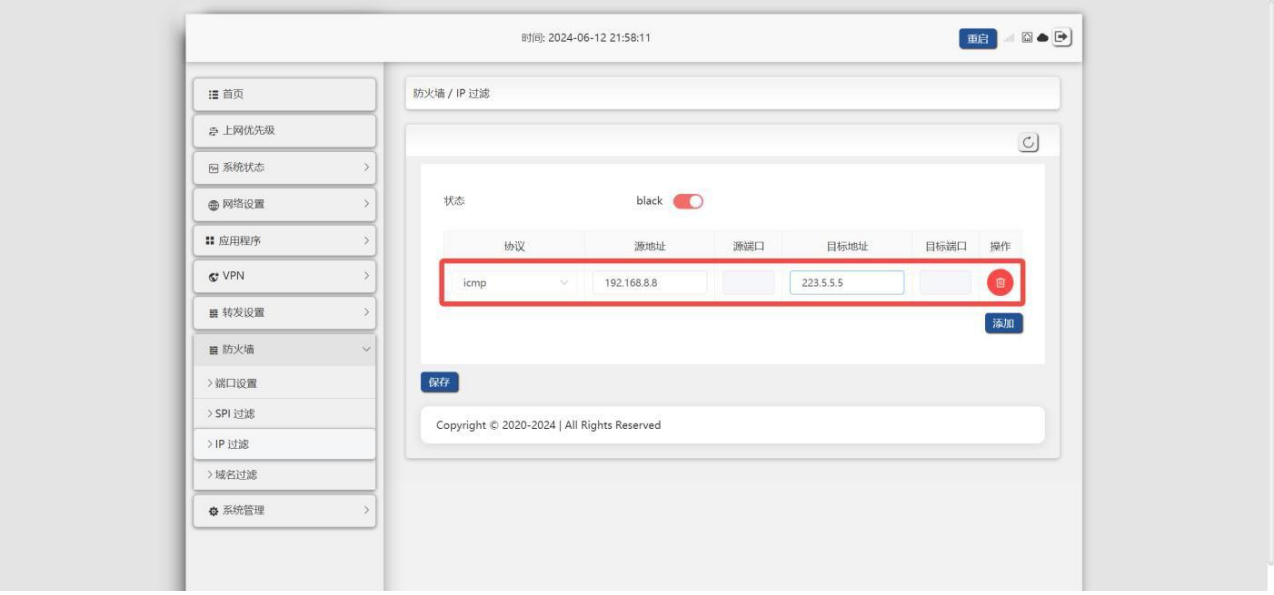


Figure 3-46 IP filtering configuration

3.9.4 Domain name filtering

The domain name filtering feature of this product allows users to control network traffic based on domain names, allowing or denying access to specific domains. This feature enhances network security and management efficiency. The domain name filtering configuration interface is shown in Figure 3-47.

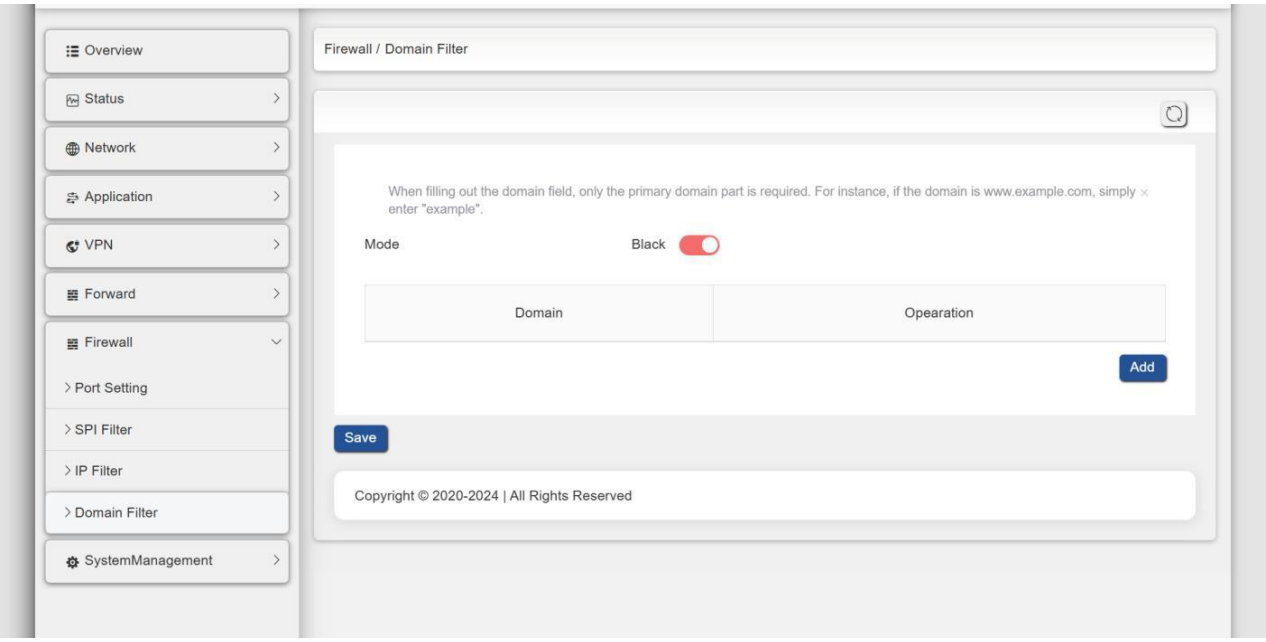


Figure 3-47 Domain name filtering configuration interface

The main parameters of domain name filtering are shown in Table 3-23.

Table 3-23 Domain name filtering main parameters description

name	parametric description	Default parameters
state	Support black (blacklist), white (whitelist)	black
realm name	To fill in the domain name, you only need to fill in the main domain part, such as www.example.com, then fill in example	not have

Let's learn how to use domain filtering with a simple example. Assume that users need to restrict access to all websites containing the "baidu" string, and that all devices connected to the router cannot access these domains. The configuration is shown in Figure 3-48.

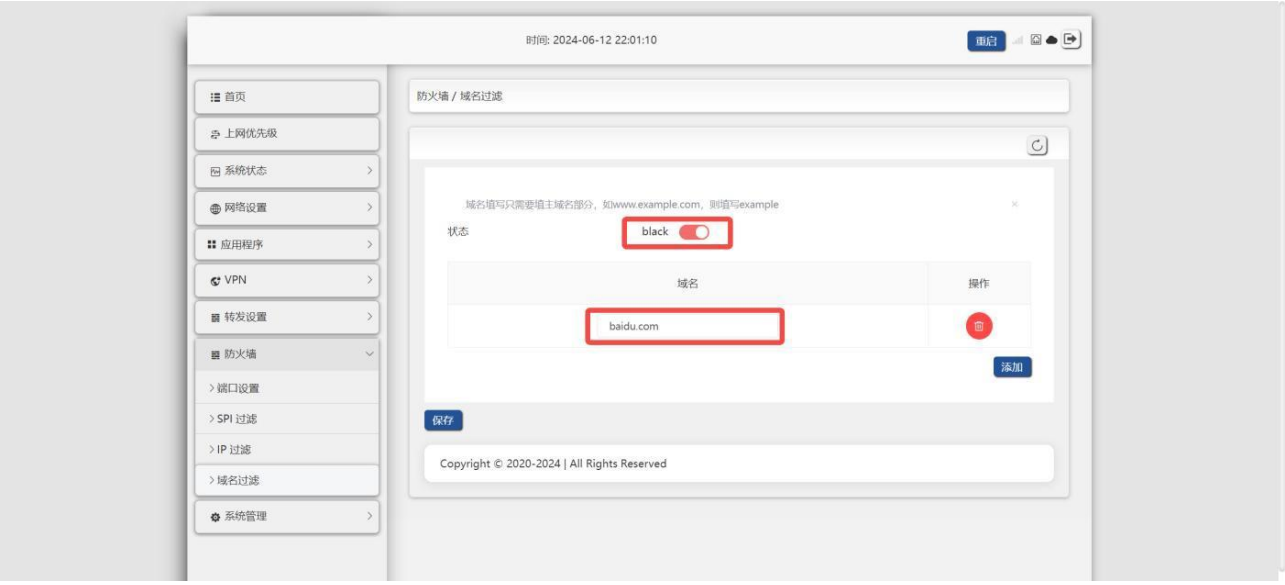


Figure 3-48 Domain name filtering configuration

3.10 System management

3.10.1 Local logs

The local log feature of this product allows users to export and view the device log. The local log interface is shown in Figure 3-49.

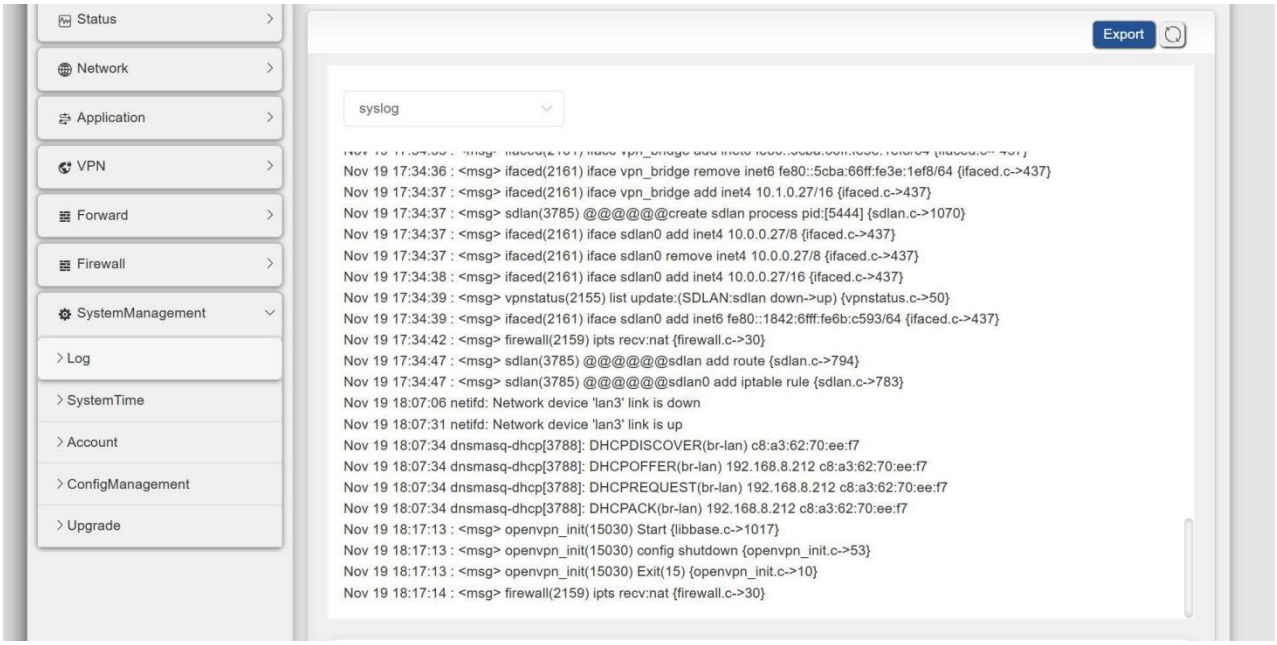


Figure 3-49 Local log interface

3.10.2 System time

In order to ensure the coordination with other devices and the accuracy of the timer, this product needs NTP to obtain the correct time. The system time configuration interface is shown in Figure 3-50.

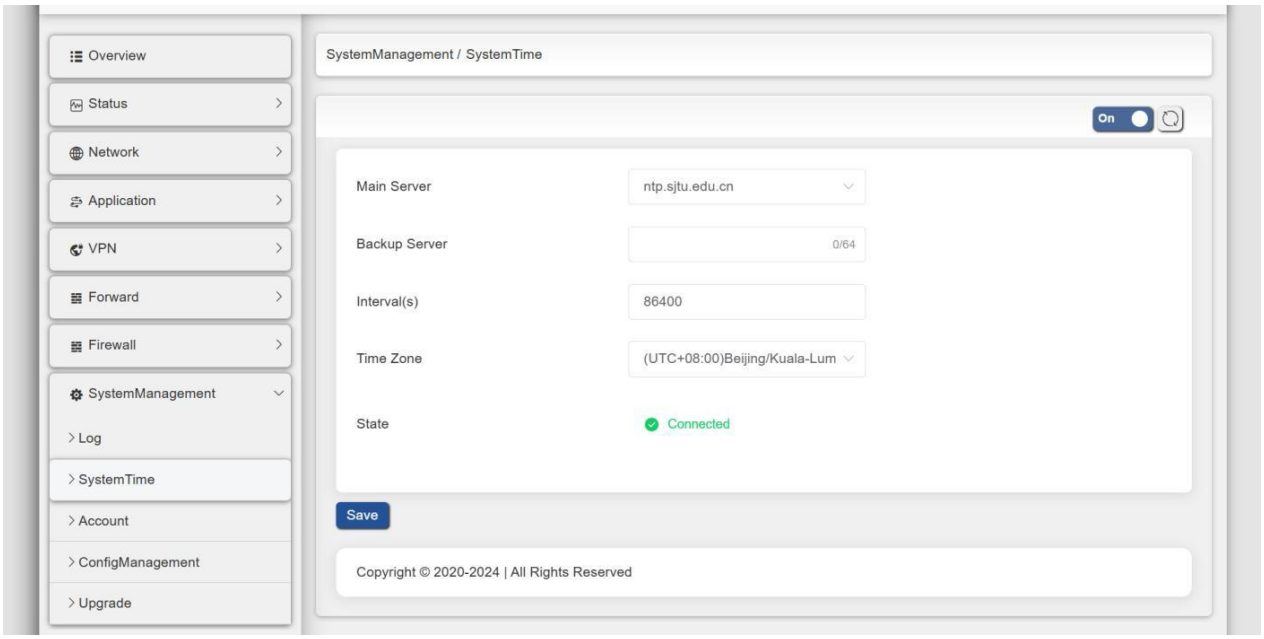


Figure 3-50 System time configuration interface

The main parameters of system time are shown in Table 3-24.

Table 3-24 Main system time parameter description

name	parametric description	Default parameters
Master server	navobs1.gatech.edu, ntp.sjtu.edu.cn, clock.fmt.he.net	ntp.sjtu.edu.cn
Backup server	Use when the master server connection fails	not have
margin	Interval to retime with the server	86400
time zone	Select according to the time zone where the device is located	(UTC+08:00)

3.10.3 User management

The core functionalities of this product's user management system include password modification and permission configuration. Access to the user management interface is restricted to the admin account. The device comes pre-configured with two default accounts: the guest account, which initially has no privileges and remains disabled, must be activated by the admin account to become operational. The user management interface is illustrated in Figure 3-51.

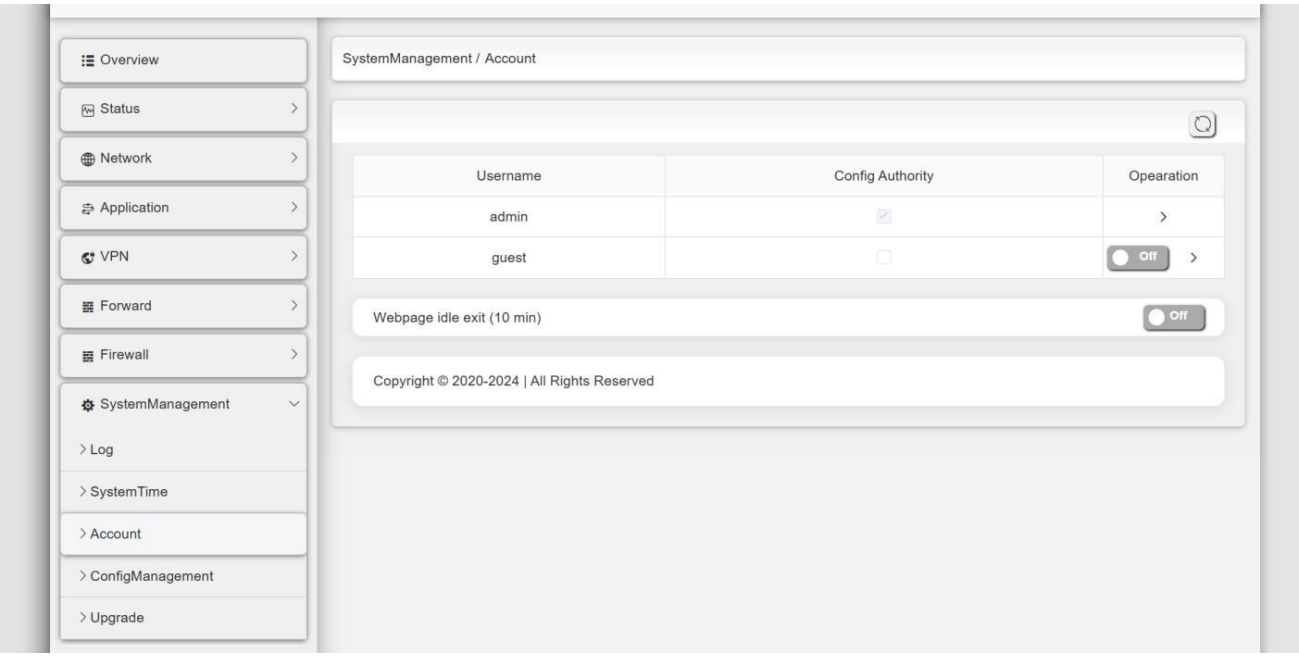


Figure 3-51 User management configuration interface

3.10.4 Configuration management

This product's configuration management system primarily features three core functions: Import/Export Configuration, Export Configuration (Backup), and Factory Reset. The Import/Export Configuration files enable quick replication of product settings, requiring users to verify file validity during these operations. The configuration management interface is illustrated in Figure 3-52.

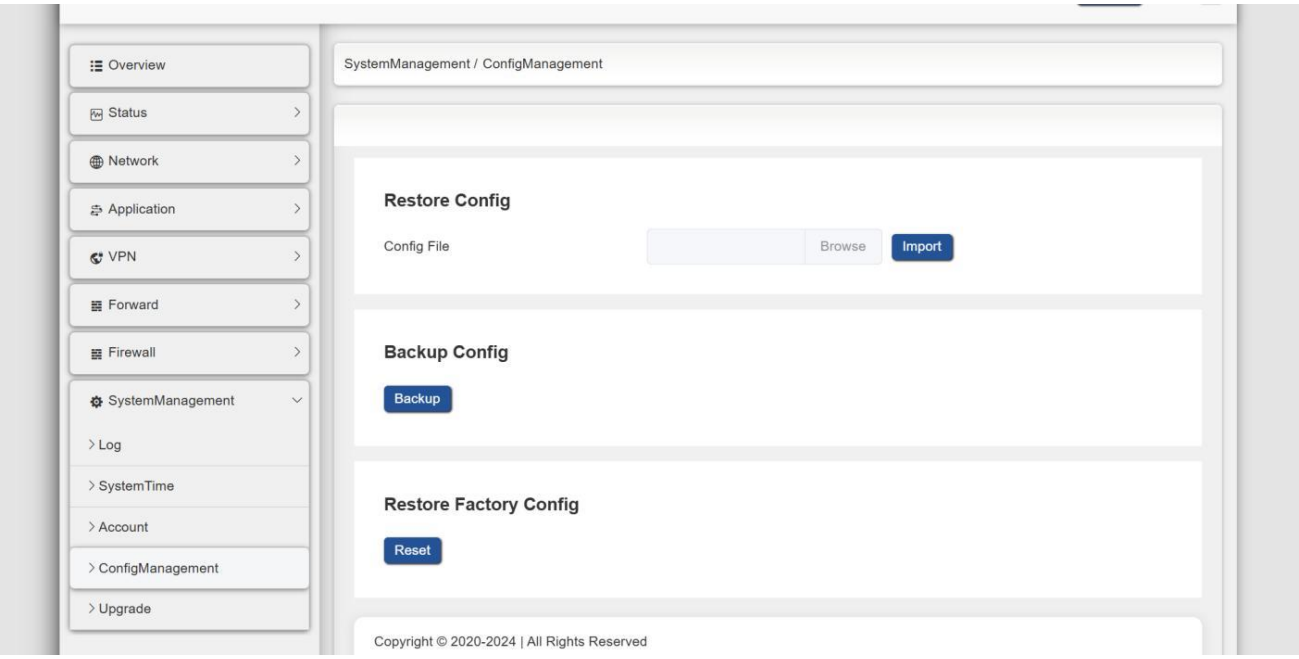


Figure 3-52 Configuration management interface

3.10.5 Software upgrades

The software upgrade interface of this product is used for firmware upgrade operation. After selecting the legal firmware, click "Upgrade" and wait for the product to complete the automatic upgrade. It should be noted that check the factory reset configuration after upgrading the device configuration will be cleared. The software upgrade interface is shown in Figure 3-53.

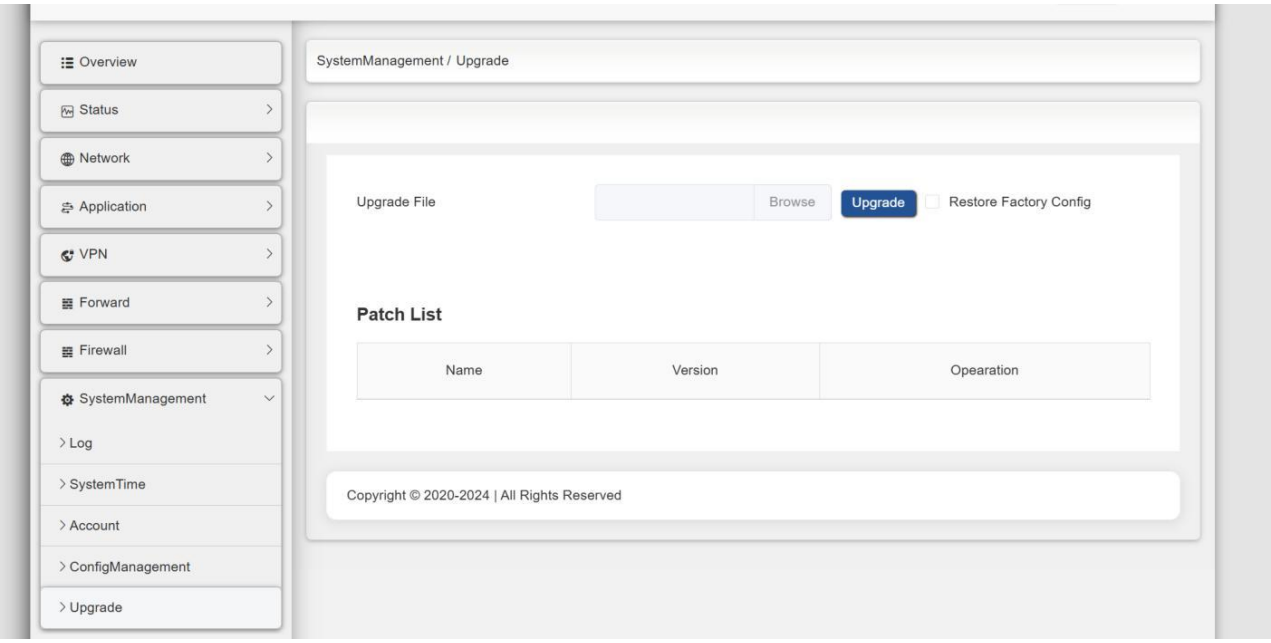


Figure 3-53 Software upgrade interface

Software upgrade process:

1. Click Browse and select the correct upgrade package.

2. Click Upgrade and wait for the upgrade to complete. If you check Restore factory configuration, the device configuration will be cleared after the upgrade.

3. Do not turn off the power during the upgrade.

4. FAQ

4.1 Hardware issues

4.1.1 Power indicator light is not on

Problem phenomenon

The power indicator light is not on.

Analysis of causes

- The power supply is not connected to the router's power port.
- The power supply does not meet the requirements.

Resolvent

- If the power supply is not connected to the router's power port, please plug the power cord into the power port.
- If the power supply is not up to standard, please replace it with a suitable power supply.

4.1.2 SIM card connector problem

Problem phenomenon

The SIM card cannot be inserted into the SIM card properly.

Analysis of causes

- The SIM card is inserted in the wrong direction.

Resolvent

- If the SIM card is inserted in the wrong direction, please insert it again in the correct way.

4.1.3 Network port connection problem

Problem phenomenon

The LAN port indicator is not lit and the router page cannot be accessed.

Analysis of causes

- There is a problem with the network cable connection.
- The network cable is broken.
- The PC terminal network card is working abnormally.

Resolvent

- If there is a problem with the network cable connection, please reconnect the network cable.
- If the network cable is damaged, please replace the network cable.
- If the PC network card is working abnormally, please replace the network card.

4.1.4 Antenna connection problem

Problem phenomenon

The antenna cannot be installed properly.

Analysis of causes

- The antenna does not meet the accessory requirements.
- The antenna is not connected correctly.

Resolvent

- If the antenna is not up to standard, replace it with a compliant antenna.
- If the antenna is not connected correctly, please reconnect the antenna.

4.2 Dial-up issues

4.2.1 Dial-up failure

Problem phenomenon

The mobile phone cannot dial up to the Internet.

Analysis of causes

- SIM card arrears.
- The SIM card is not inserted or not powered off before insertion.
- Mobile dialing is not configured correctly.
- The antenna is not properly connected or installed.

Resolvent

- If the SIM card is in arrears, please recharge the SIM card.
- If the SIM card is not inserted or there is no power failure before insertion, please insert the SIM card after power failure.
- If the Mobile dialing configuration is incorrect, re-dial using the correct configuration.
- If the antenna is not properly connected or installed, install the antenna correctly. See Section 4.1.4, Antenna Connection Problems for details.

4.2.2 Communication signal is weak

Problem phenomenon

The mobile status page shows no signal or poor signal.

Analysis of causes

- The antenna is not properly connected or installed.
- The network coverage and signal strength in the area where the device is located are weak.

Resolvent

- If the antenna is not properly connected or installed, install the antenna correctly. See 4.1.4 Antenna Connection Problems for details.
- If the network coverage and signal strength of the device area are weak, please contact the network operator for reasonable solutions.

4.3 VPN connection issues

4.3.1 SDLAN cannot be connected

Problem phenomenon

The SDLAN server connection status is disconnected.

Analysis of causes

- The device has no network.
- Device information was not imported to the server.
- The SDLAN configuration is incorrect.
- The server is not functioning properly.

Resolvent

- If the device is not connected to the network, reconnect it after restoring the network.
- If the device information is not imported to the server, please contact our relevant person in charge to import it.
- If the SDLAN is not configured correctly, reconnect it with the correct configuration.
- If the server is working abnormally, check the server configuration and working status.

4.3.2 SDLAN connection is normal and cannot communicate with the other subnet

Problem phenomenon

The device communicates normally with the other end, but cannot communicate with the subnet of the other end.

Analysis of causes

- No additional subnet routing is added or errors are added.
- Added a subnet routing but did not enable MASQ.
- The terminal subnet and local subnet have the same subnet.

Resolvent

- If you do not add a subnet route or add an incorrect one, add the correct route and try again.
- If you have added a terminal network but have not enabled MASQ, enable MASQ and retry.
- If the subnet and local subnet are the same, change the subnet and try again.

4.4 WEB class issues

4.4.1 Forget router login password

Problem phenomenon

Forgot the router login password.

Analysis of causes

- The user has changed the password in the user management interface.

Resolvent

- Long press RST (reset key) for more than 5 seconds and release to restore the factory configuration. Initial user name/password: admin/admin.

4.4.2 Unable to access built-in web pages

Problem phenomenon

Unable to access the built-in web page.

Analysis of causes

- The PC is not properly connected to the router.
- The guest account is logged in but not enabled.
- Remote access is not enabled.

Resolvent

- If the PC is not properly connected to the router, see 3.1 Login to the WEB Configuration interface.
- If you are logging in with a guest account but it is not enabled, enable it and log in again
- If remote access is not enabled, please enter through another network port. If all network ports are not enabled, you can hold down RST (reset button) for more than 5 seconds and then release to restore factory configuration.

4.4.3 Configuration changes do not take effect

Problem phenomenon

Changes to the configuration do not take effect.

Analysis of causes

- The changes made are unreasonable.
- Modification and verification do not act on the same device.
- Other configurations are abnormal.

Resolvent

- If the modification is not reasonable, please correct the modification.

- If the modification and verification do not apply to the same device, ensure that the modification and verification apply to the same device.
- If other configuration is abnormal, please contact our relevant person in charge to intervene.

4.4.4 Firmware upgrade failed

Problem phenomenon

The firmware upgrade was not successful.

Analysis of causes

- The firmware upgrade was incorrect.
- During the upgrade, the router restarts due to other functions (such as scheduled tasks).
- The router is powered off during the upgrade.

Resolvent

- If the firmware is not upgraded correctly, replace the correct firmware for the upgrade.
- If the router restarts during the upgrade due to other functions, please close other functions and then reupgrade.
- If the router is powered off during the upgrade, ensure that the power supply is normal during the upgrade.

4.5 DHCP class issues

4.5.1 PC can not access the address

Problem phenomenon

The PC can not obtain the router address by automatically acquiring IP.

Analysis of causes

- The DHCP function is not enabled.
- DHCP address pool configuration is abnormal.
- The WAN port is connected to the host computer in LAN mode.
- Other functions are abnormal.

Resolvent

- If the DHCP function is not enabled, go to the DHCP interface to enable the DHCP function.
- If the DHCP address pool is improperly configured, modify the DHCP address pool configuration.

- If the WAN port is connected to the host computer and the mode is LAN, change the WAN mode to DHCP.
- If other functions are abnormal, please contact our relevant person in charge to intervene.

5. After-sales service and Technical Support

Phone/WhatsApp: +86 18321985506

Web: www.valtoris.com

Email: support@valtoris.com