



5G Industrial Router FNR500

User Manual

V1.0.1

*This manual applies to the following product model: FNR500.

Xiamen Four-Faith Communication Technology Co., Ltd.
www.four-faith.com

Document Revision History

Date	Version	Remark	Author
2024-11-21	V1.0.0	English Version	YYL
2025-04-30	V1.0.1	New WEB Version	Jonas



Note: There may be differences in accessories and interfaces for different models. Please refer to the actual product for details.

Copyright Declaration

All materials or contents contained in this document are protected by copyright law. All Copyrights are owned by Xiamen Four-Faith communication technology co., LTD. Four-Faith without company's written permission, any person may not be any content in any way on this document copying, distribution, reproduction, connection, transmission, such as the use of any commercial purposes, but for non-commercial purposes, personal use, download or print (on the condition that may not be modified, and shall retain the copyright in the material or other ownership).

Trademark Statement

Four-faith is registered trademarks of Xiamen Four-Faith communication technology co., LTD. Without prior written permission, no one shall use the name of Xiamen Four-Faith and the trademarks and

marks of Four-Faith in any way.     

Contact Us

Address:

11th Floor, Building A06, No. 370 Chengyi Avenue, Software Park Phase III, Jimei District, Xiamen, Fujian Province, China

Website:

www.four-faith.com

Hotline:

400-8838-199

Phone:

+86-592-6300320 / 6300321

Postal Code:

361021

Email:

info@four-faith.com

Contents

Chapter 1 Product Introduction	1
1.1 Product Overview.....	1
1.2 Block Diagram of Working Principle & Key Feature	2
Chapter 2 Installation	3
2.1 Overview	3
2.2 Packing List.....	3
2.3 Installation and Cable Connection	4
2.4 Power Supply	7
2.5 Indicator Lights	7
2.6 Reset Button.....	8
Chapter 3 Parameter Configuration	9
3.1 Configuration Connection	9
3.2 Access to the Configuration Page.....	9
3.2.1 PC IP Address Setting(two methods)	9
3.2.2 Access to Configuration Web Page.....	10
3.3 Startup Guide.....	11
3.4 Navigation Bar.....	13
3.5 Operating Status	13
3.6 Network Setting	13
3.6.1 WAN	18
3.6.1.1 WAN.....	18
3.6.1.2 Global Setting.....	22
3.6.2 LAN	22
3.6.3 WIFI.....	22
3.6.3.1 WIFI	24
3.6.3.2 Virtual Interface	25
3.6.4 VPN.....	25
3.6.4.1 PPTP.....	25
3.6.4.2 L2TP.....	26

3.6.4.3	OPENVPN.....	28
3.6.4.4	IPSEC.....	31
3.6.4.5	GRE.....	35
3.6.4.6	GRETAP.....	36
3.6.4.7	VXLAN.....	37
3.6.4.8	EOIP.....	37
3.6.4.9	FRP.....	38
3.6.5	NAT.....	39
3.6.5.1	Port Forwarding.....	39
3.6.5.2	DMZ.....	41
3.6.5.3	Virtual IP Setting.....	41
3.6.6	VLAN.....	42
3.6.7	Bridge.....	42
3.6.8	Routing.....	44
3.6.9	LAN Settings.....	46
3.6.10	MAC Clone.....	46
3.7	Application Setting.....	46
3.7.1	Active Policy.....	46
3.7.2	Security Policy.....	46
3.7.2.1	IP Restriction.....	47
3.7.2.2	URL Restriction.....	47
3.7.2.3	MAC Restriction.....	47
3.7.2.4	Firewall.....	47
3.7.2.5	WEB Access.....	49
3.7.3	QOS.....	49
3.8	Maintenance.....	46
3.8.1	Diagnostics.....	50
3.8.2	Network Tools.....	50
3.8.3	Command Debugging.....	51
3.8.4	Log Management.....	52
3.8.5	Traffic Statistics.....	53
3.8.6	Storage Settings.....	54
3.8.7	Remote Management.....	55

3.8.7.1	SSH.....	55
3.8.7.2	Telnet.....	55
3.8.7.3	SNMP	55
3.9	Cloud Platform Management	56
3.10	System Management.....	56
3.10.1	System Settings.....	56
3.10.2	Login Management	56
3.10.3	Restore to Factory Defaults	56
3.10.4	Configuration Backup	58
3.10.5	Firmware Upgrade.....	58
Appendix.....	错误!未定义书签。	

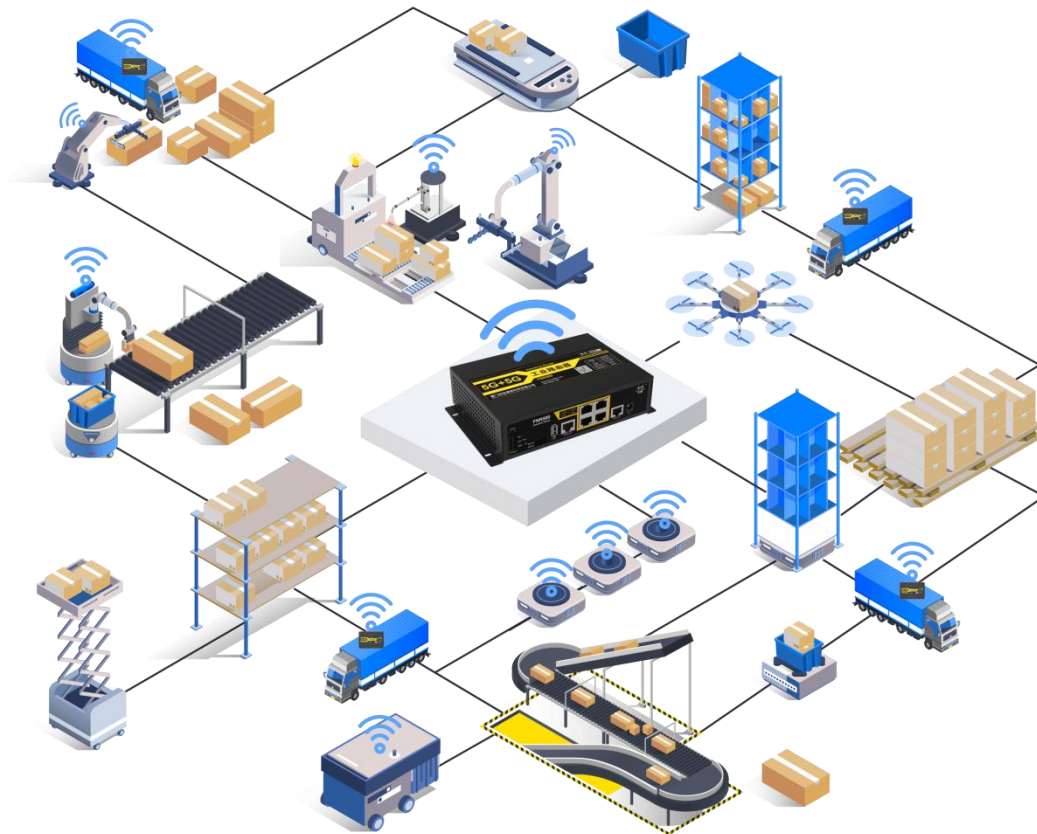
Chapter 1 Product Introduction

1.1 Product Overview

The FNR500 is a dual-SIM dual-module 5G IoT wireless communication router that leverages public 3G/4G/5G networks to provide users with wireless, long-distance, large data transmission capabilities.

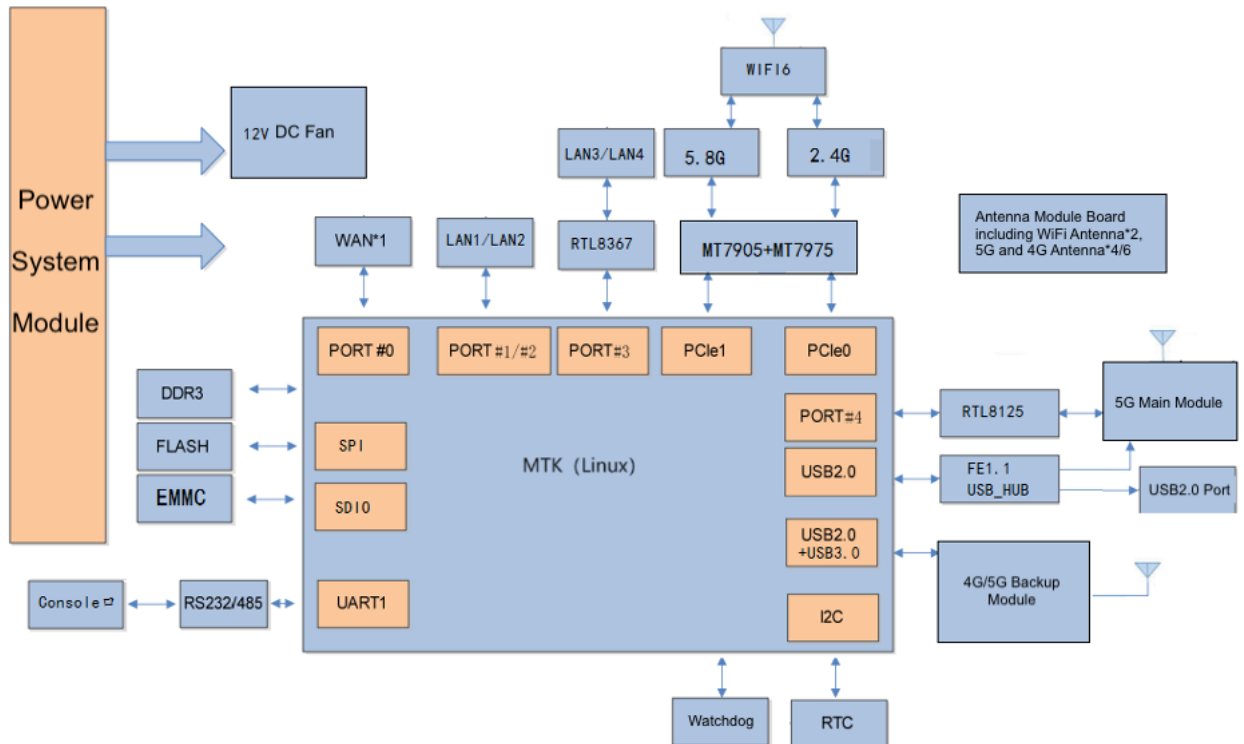
This product features a high-performance industrial-grade 32-bit communication processor and an industrial-grade wireless module. It uses an embedded real-time operating system as the software support platform, providing 1 Gigabit Ethernet WAN/LAN port, 4 Gigabit Ethernet LAN ports, 1 USB interface, and 1 RS232 (or RS485) port. It supports simultaneous connections to serial devices, Ethernet devices, and WiFi devices, enabling transparent data transmission, WiFi 6, VxLAN, and intelligent dual-link switching between primary and backup SIMs, along with routing functionality.

The product has been widely applied in the IoT industry chain across M2M sectors such as smart grids, intelligent transportation, smart homes, finance, mobile POS terminals, supply chain automation, industrial automation, smart buildings, fire protection, public safety, environmental protection, meteorology, digital healthcare, remote sensing exploration, military, space exploration, agriculture, forestry, water resources, coal mining, petrochemical industries, and more.



1.2 Block Diagram of Working Principle & Key Feature

5G Router Working Principle:



Key Features of the Product:

- Supports 5G LAN functionality
- Enables dual 5G intelligent switching
- Provides intelligent load balancing for data stream distribution
- Supports dual-link intelligent failover and backup for 3G/4G/5G and wired WAN
- Compatible with VPN protocols including PPTP, L2TP, GRE, IPSEC, and OPENVPN
- Supports remote management via SYSLOG, SNMP, TELNET, SSHD, and HTTPS
- Includes SPI firewall, VPN passthrough, access control, and URL filtering
- WiFi supports multiple encryption methods such as WEP, WPA, WPA2, and MAC address filtering
- Supports lock screen, cell lock, EOIP, bridge mode, VxLAN, virtual IP, and GRE-TAP functionality
- Supports multiple DHCP servers, DHCP-MAC address binding, DDNS, firewall, NAT, DMZ host, QoS, traffic statistics, VLAN management, and segmentation
- Supports various WAN connection methods including Static IP, DHCP, PPPoE, 3G/UMTS/4G/LTE, and DHCP-4G/5G
- Facilitates local and remote online upgrades and configuration file import/export
- Supports NTP and built-in RTC
- Compatible with a wide range of domestic and international DDNS providers
- Includes VLAN, MAC address cloning, and PPPoE server support
- WiFi supports 802.11b/g/n/ac/ax and multiple operating modes including WiFi AP, AP Client, repeater, and relay bridge (optional)
- Offers multiple online/offline triggers such as SMS, phone ring, serial data, and network data
- Supports APN/VPDN
- Features multiple DHCP servers and clients, DHCP-MAC address binding, DDNS, firewall, NAT, DMZ host, QoS, traffic statistics, and real-time data transfer rate display
- Compatible with network protocols including TCP/IP, UDP, FTP (optional), and HTTP

Chapter 2 Installation

2.1 Overview

5G routers must be installed correctly to achieve the designed functions. Usually the installation of the equipment must be carried out under the guidance of qualified engineers approved by the company.

Caution: Do not install the 5G router while it is powered on.

2.2 Packing List

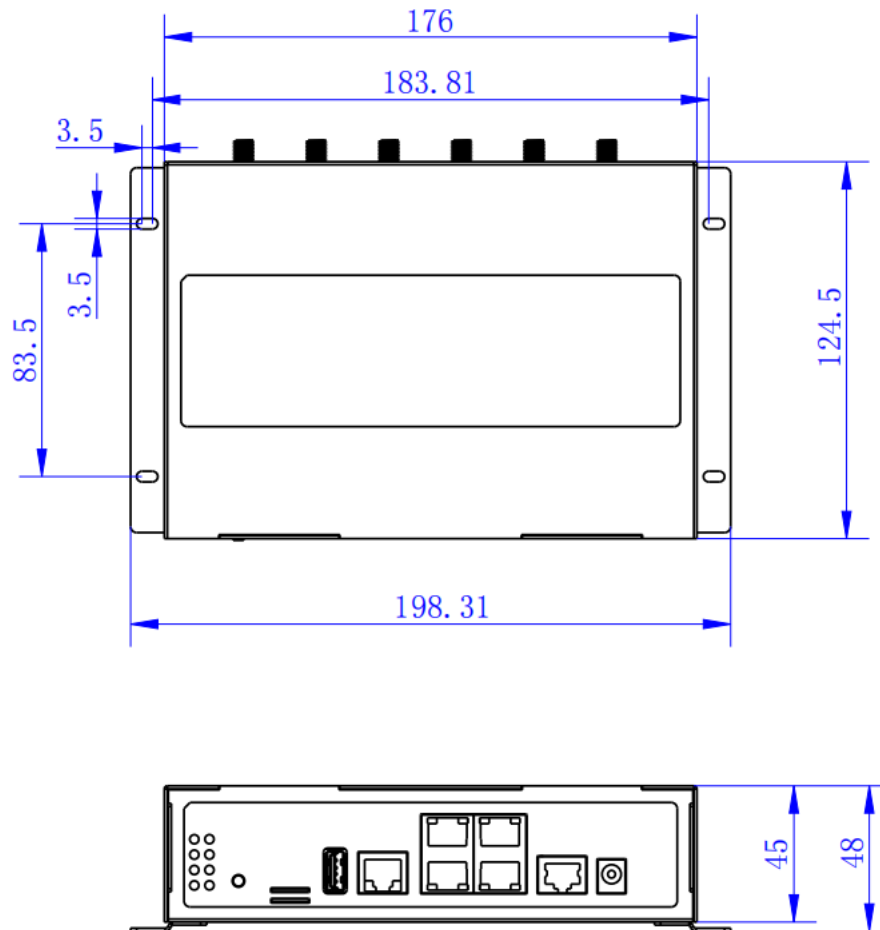
When you open the box, please keep the packing materials, so that you can use it when you need to transfer in the future.

The list is as follows:

- 1 x 5G router host
- 8 x 5G wireless cellular antennas (SMA male)
- x WIFI antenna (SMA female)
- 1 x Matching power supply
- 1 x Ethernet direct connection
- 1 x Warranty card

2.3 Installation and Cable Connection

Size(mm):



5G Router Dimension

Antenna Installation:

The 5G antenna interface is an SMA female socket(4 “5G-1”, 4 “5G-2”). Screw the SMA male of the matching wireless cellular antenna to the antenna interface and make sure to tighten it. To increase the isolation of the 5G antenna, try to keep the antenna at an angle of 30 degrees to enhance signal quality. Figure as follow.



The WIFI antenna interface is an SMA male socket("WiFi1", "WiFi2"). Screw the SMA female of the matching WIFI antenna to the antenna interface and make sure to tighten it. In addition, to increase the isolation of the Wi-Fi antenna, it is recommended that the two Wi-Fi are placed at a 90-degree angle.



SIM/UIM Card Installation:



Not Installed



Installed

SIM-1 and SIM-2 chip orientation: SIM-1 chip faces downward, SIM-2 chip faces upward

- Installing SIM/USIM Card: When inserting a Micro SIM card, orient the SIM-1 chip facing downward and the SIM-2 chip facing upward. Use a pointed object to push the SIM card inward until it is securely fixed.
- Removing SIM/USIM Card: Use a pointed object to press the SIM card. Once the card pops out, remove it.

Connecting Network Cable:

Insert one end of the network straight-through cable into any of the LAN1~LAN4 ports on the 5G router, and the other end into the Ethernet interface of the user device. The signal connections for the network straight-through cable are as follows:

RJ45-1	RJ45-2	Wire Color
1	1	White/Orange
2	2	Orange
3	3	White/Green
4	4	Blue
5	5	White/Blue
6	6	Green
7	7	White/Brown
8	8	Brown



Connect Console Cable:

Plug the RJ45 end of the Console line into the Console interface (RS232) of the Router and plug the DB9 end into the RS232 serial interface of the user device. The signal connections of the Console are as follows:

Console Wire Signal Definition(RS232)				
RJ45	Wire Color	Signal Definition	DB9F	Signal Description
1	White/Orange	A	8	RS485-A (Optional)
2	Orange	B	6	RS485-B (Optional)
3	White/Green	RXD	2	RS232 Receive Data
4	Blue	--	1	--
5	White/Blue	GND	5	Power Light
6	Green	TXD	3	RS232 Send Data
7	White/Brown	--	4	--
8	Brown	--	7	--



2.4 Power Supply

5G routers are usually used in complex external environments. To adapt to the complex application environment and improve the stability of the system, the router adopts advanced power supply technology. Users can use the standard 12VDC/1.5A power adapter to power the 5G router, or directly use the DC 9~36V power supply to power the router. When the user uses an external power supply to power the router, the stability of the power supply must be ensured (the ripple is less than 300mV, and the instantaneous voltage does not exceed 36V), and the power supply must be greater than 8W.

It is recommended to use the standard 12VDC/1.5A power supply.

2.5 Indicator Lights



5G Router provide indicators as below: “Power”, “System”, “WIFI”, “Online1”, “Online2”, “Signal”:

Indicator	Status	Content
Power	On	Device powered on
	Off	Device not powered on
System	Flashing	System running normally
	Off	System running abnormally
Online1	On	SIM 1 is online
	Off	SIM 1 is not online
Online2	On	SIM 2 is online
	Off	SIM 2 is not online

WIFI	On	2.4G or 5.8G is on, or are both on
	Off	2.4G and 5.8G are both off
WAN	Off	WAN port not connected
	On/Flashing	WAN port connected/communicating
LAN1~LAN4	Off	LAN port not connected
	On/blank	LAN port connected/communicating
Signal Strength	One light on	Weak(<-90dBm)
	Two lights on	Medium(-70dBm~-90dBm)
	Three lights on	Good(>-70dBm)

Note: The indicator lights for the WAN and LAN ports only show green; the yellow light is not active.

2.6 Reset Button

The 5G router has a reset button, marked as "RST"

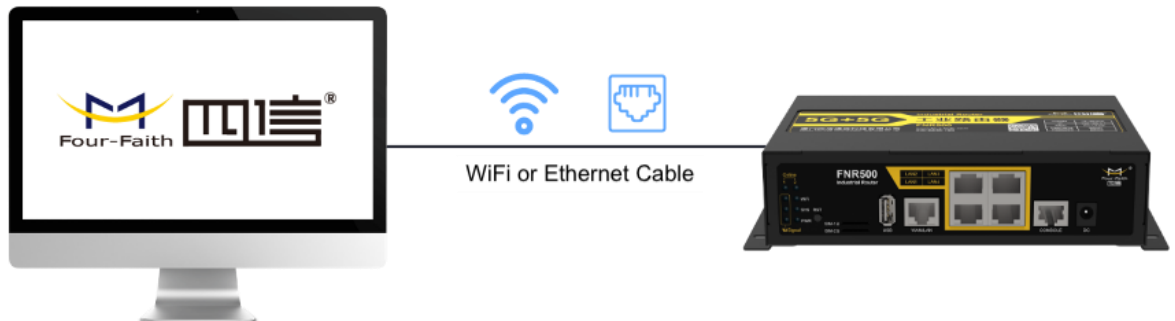
The function of this button is to restore the parameter configuration of the 5G router to factory values

Methods as below: Power on device, let it running for 30 seconds, use a pen keep pressing the reset button for about 15 seconds, until all led turn off, the device will restart and reset to factory.

Chapter 3 Parameter Configuration

3.1 Configuration Connection

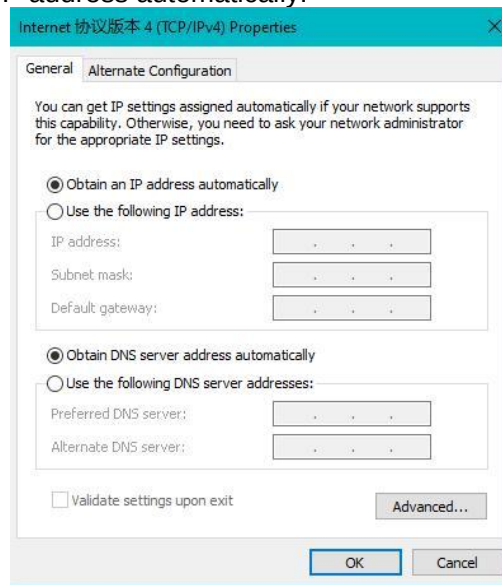
Before configuration, you should connect the Router and your configuration PC with the supplied network cable. Plug the cable's one end into the Local Network port (LAN Port) of the Router, and another end into your configure PC's Ethernet port. When connecting via WiFi, the factory default SSID for the 5G router is "FOUR-FAITH", and no password is required. The connection diagram is as following:



3.2 Access to the Configuration Page

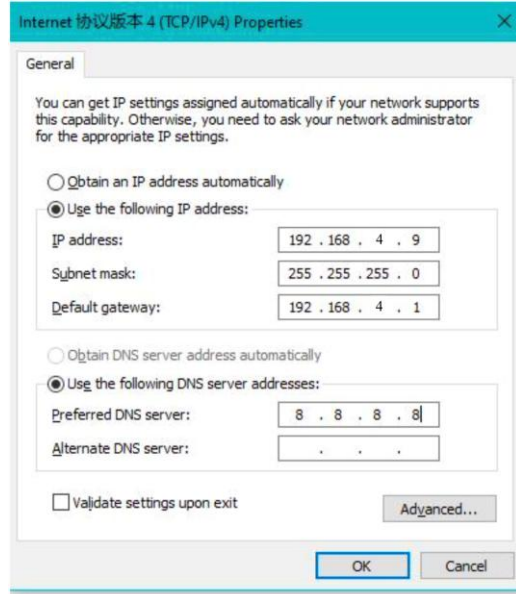
3.2.1 PC IP Address Setting (Two methods)

The first method: Obtain an IP address automatically:



The second way: specify the IP address

Set the PC's IP address to 192.168.4.9 (or any other IP address within the 192.168.4 subnet), subnet mask to 255.255.255.0, and default gateway to 192.168.4.1. Set the DNS to the gateway address or a locally available DNS server.



3.2.2 Access to Configuration Web Page

This chapter describes the main functions of each page. The web-based tool can be accessed through a computer connected to the 5G gateway using a web browser. There are a total of seven main pages: Operation Status, Data Acquisition Application, Network Settings, Application Settings, Operation & Maintenance Settings, Cloud Platform Management, and System Management. Clicking on any of these main pages will display additional subpages.

To access the web-based management tool of the 5G gateway, launch Internet Explorer or another browser, enter the default IP address of the 5G gateway (192.168.4.1) in the address bar, and press Enter. If this is the first time logging into the web interface, a page will appear prompting the user to change the default username and password of the 5G gateway. To set a custom username and password, click the "Change Password" button to apply the changes.



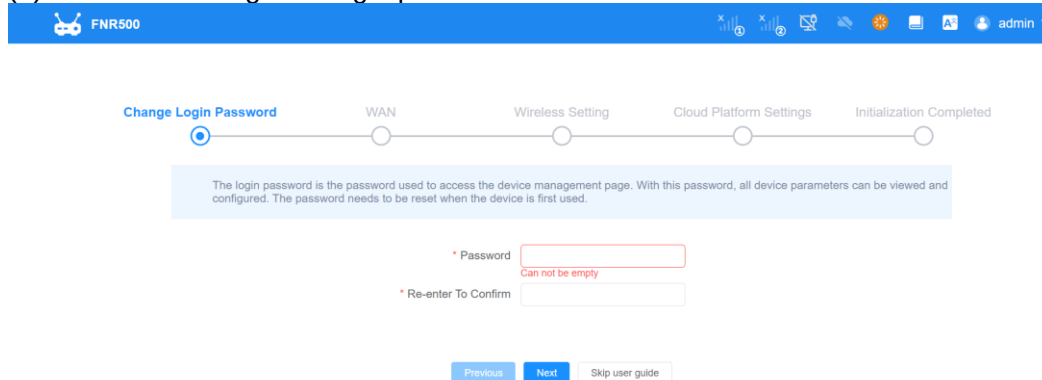
After access to the information main page.

3.3 Startup Guide

(1) The default IP address of the gateway is 192.168.4.1. Before accessing it, please set your computer to the same subnet or configure it to obtain an IP address automatically. As shown in the figure, this is the startup guide page for the initial gateway configuration. The default username and password for the first login are both admin.



(2) Users can change the login password as needed.



(3) Perform the initial configuration based on the network environment. If the gateway connects to the internet via a SIM card, select Cellular Network. If it uses a wired connection, select Ethernet. When choosing Ethernet, ensure that the corresponding IP fields are configured correctly in order to access the internet.

Change Login Password

WAN

Wireless Setting

Cloud Platform Settings

Initialization Completed

Please choose to use cellular or Ethernet networks based on the current device network environment, and set the correct network parameters to ensure that the device can access the internet normally.

* Internet Access

Cellular Network

Cellular Network

Ethernet

Previous

Next

Setup user guide

(4) Users can choose whether to enable the Wi-Fi hotspot and set a password as needed.

Change Login Password

WAN

Wireless Setting

Cloud Platform Settings

Initialization Completed

Configure wireless settings.

2.4G

Enable

* SSID

Four-Faith

* Security Mode

Open

5G

Enable

* SSID

Four-Faith_5G

* Security Mode

Open

Previous

Next

Skip user guide

(5) After configuring the cloud platform, it enables convenient remote operations, NAT traversal, and other functions through the cloud platform.

Change Login Password

WAN

Wireless Setting

Cloud Platform Settings

Initialization Completed

The Device Cloud Platform supports remote operation and maintenance device parameter configuration, upgrading device firmware, intranet penetration of operation and maintenance sub device firmware, data reports, etc. Configuring devices to the Device cloud platform can facilitate subsequent remote operation of devices. To use the Device Cloud Platform, you need to register a Device Cloud account in advance. Click to go to Device Cloud to register and log in for use. device.fourfaith-cloud.com

Cloud Platform Connection

* Platform

Four-Faith Cloud

Private Cloud

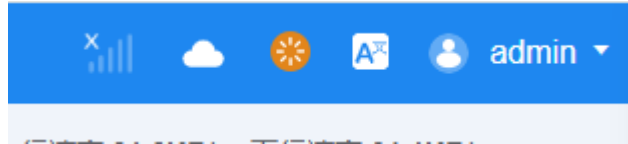
Previous

Next

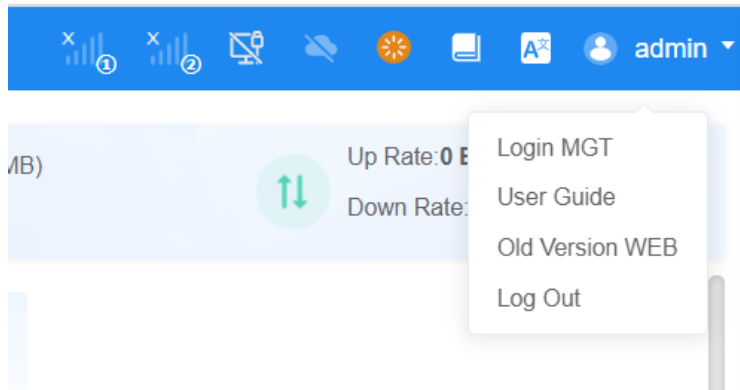
Skip user guide

(6) Initialization is complete, and the device now has basic internet access. For more advanced configurations, parameters need to be set in the corresponding sections.

3.4 Navigation Bar

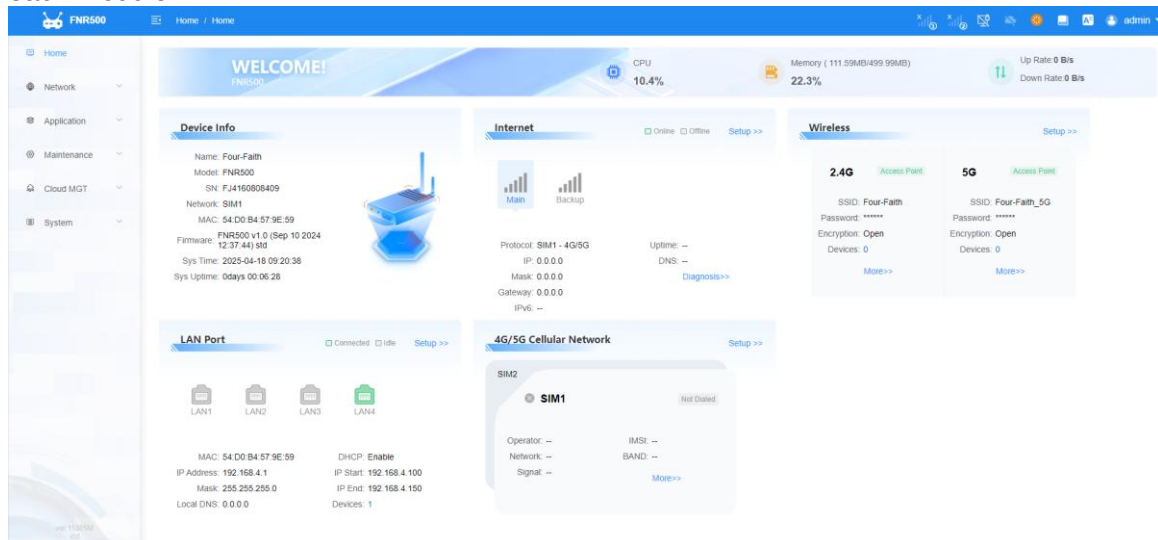


From left to right: cellular signal, cloud platform connection indicator, reboot button, language options, and a button to switch back to the legacy router page.



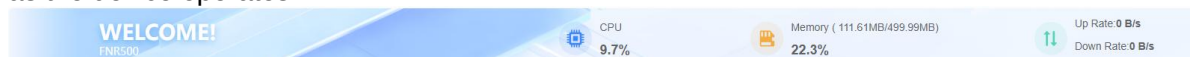
3.5 Operating Status

The homepage displays the operating status of the router. On this page, you can view the status parameters of all modules in a centralized manner. The following sections introduce each module.



Real-time Operating Parameters:

In the top bar, you can see the CPU usage, memory consumption, and the real-time upload and download speeds of the internet connection. These data dynamically update in real-time as the device operates.



Device Information:

- **Product Name:** The name of the device, which can be changed in the System Management - System Settings.
- **Product Model:** Displays the specific model of the device.
- **Device SN:** The serial number (SN) of the gateway, which uniquely identifies the device.
- **Current Network:** The current internet connection. If connected via a wired network, it will display "Ethernet."
- **MAC:** The MAC address of the device.
- **Firmware Information:** The current firmware version.
- **System Time:** The current system time.

Device Info

Name: Four-Faith

Model: FNR500

SN: FJ4160808409

Network: SIM1

MAC: 54:D0:B4:57:9E:59

Firmware: FNR500 v1.0 (Sep 10 2024 12:37:44) std

Sys Time: 2025-04-18 09:21:35

Sys Uptime: 0days 00:07:25



Internet Connection:

This module displays the WAN port connection information.

- **Main Link:** Green indicates normal connection, while gray means not yet connected.
- **Protocol:** The type of device connected to the WAN port.
- **IP:** The WAN IP address.
- **Subnet Mask:** The subnet mask for the device's internet connection.
- **Gateway:** The configured gateway IP address.
- **DNS:** The configured DNS address.
- **Uptime:** The duration since the WAN successfully dialed for internet connection.

Internet

☒ Online ☐ Offline [Setup >>](#)



Main



Backup

Protocol: SIM1 - 4G/5G

IP: 0.0.0.0

Mask: 0.0.0.0

Gateway: 0.0.0.0

IPv6: --

Uptime: --

DNS: --

[Diagnosis>>](#)

Clicking on "Setup" allows you to configure the internet connection link, as shown in the image.

WAN Global Settings

Dual Link Option

Enable WAN Failover ☐

Main

* Connection Type Username

Password APN

* Connection type PIN Code

* Keep Online Detection

* Detection Interval * Main Detection IP

* Backup Detection IP

[> Advance](#)

Clicking on "Diagnosis" allows for detailed network analysis, as shown in the image.

Diagnosis

* Diagnostic Content

Diagnostic Results

DNS resolution failed, please check if the correct DNS address is set. If it is a dedicated network card, please ignore it

Main Link

Network Config SIM1 - 4G/5G Normal

WIFI STA Status: Not Connected Error

Channel: Channel 48

Signal: --%

RSSI: -- dBm

Please check if the SSID or password is correct

Bkup Link

Network Config SIM2 - 4G/5G Normal

Module Status Diagnosing

Wireless

Displays information related to the dual-band WiFi. By clicking on "Settings," you can access more detailed wireless (WiFi) settings. WiFi supports AP and client bridge modes, and you can also view information about devices connected to the WiFi.

Wireless

Setup >>

2.4G

Access Point

SSID: Four-Faith

Password: *****

Encryption: Open

Devices: 0

More>>

5G

Access Point

SSID: Four-Faith_5G

Password: *****

Encryption: Open

Devices: 0

More>>

WIFI

Virtual Interface

2.4G

Enable ☒

* Wireless Mode

Access Point

Access Point Only

* SSID

Four-Faith

* Signal

Through Walls

* Security Mode

Open

Hide SSID ☐

> Advance

5G

Enable ☒

* Wireless Mode

Access Point

Access Point Only

* SSID

Four-Faith_5G

* Signal

Through Walls

* Security Mode

Open

Hide SSID ☐

> Advance

LAN Port

- If the port is displayed in green, it indicates that a device is connected; if it is displayed in gray, it means no device is connected.
 - MAC Address:** The MAC address of the LAN port.
 - IP Address:** The gateway's IP address in the local area network (LAN).
 - Subnet Mask:** The gateway's subnet mask.
 - Client:** Click to view information about the connected device.
 - Setup:** Click to access detailed LAN port parameter settings.

LAN Port

☒ Connected
 ☐ Idle

Setup >>

LAN1

LAN2

LAN3

LAN4

MAC: 54:D0:B4:57:9E:59

DHCP: Enable

IP Address: 192.168.4.1

IP Start: 192.168.4.100

Mask: 255.255.255.0

IP End: 192.168.4.150

Local DNS: 0.0.0.0

Devices: 1

Click "Setup" to view configuration:

Router IP

* LAN IP

192.168.4.1

* Mask

255.255.255.0

* Gateway

0.0.0.0

* Local DNS

0.0.0.0

DHCP

* DHCP Type

DHCP Server

DHCP Server

☒

* IP Start

192.168.4

100

* Maximum DHCP Users

50

[Advance](#)

Multiple LAN IP

☒

Select All

☐

Add

☐

Delete

No.	IP Address	Mask	Operation
No Data			

Total 0

10/page

< 1 >

Go to 1

Save

Apply

Cellular:

When the main link is set to cellular, if the dial-up is successful, the related cellular information will be displayed. Clicking "More" will show detailed cellular information. If the main link is set to wired mode, no dial-up will occur, and no cellular information will be displayed.

4G/5G Cellular Network

Setup >>

SIM2

☒

SIM1

Not Dialed

Operator: --

IMSI: --

Network: --

BAND: --

Signal: --

More>>

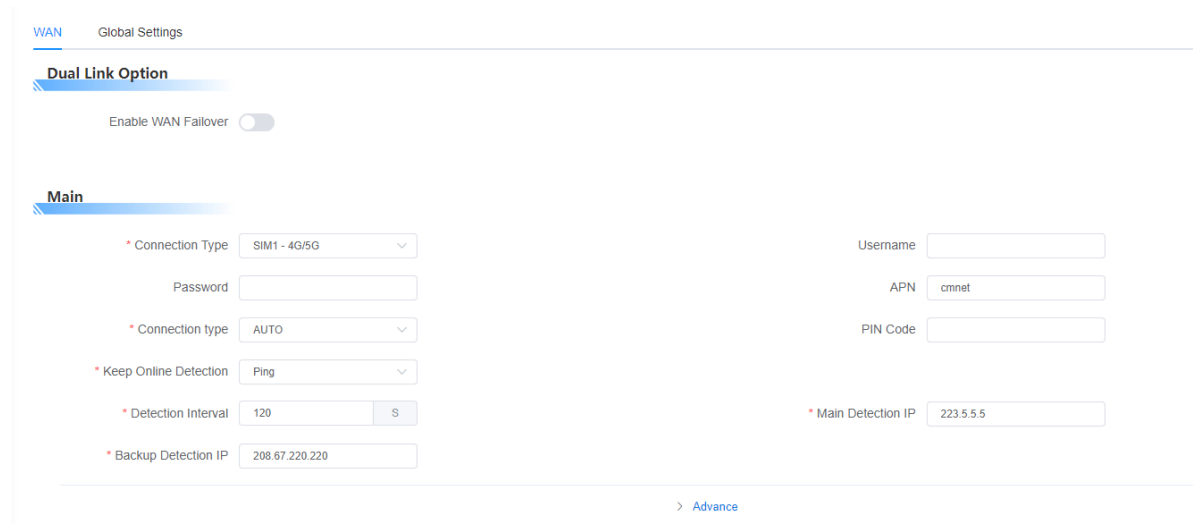
Serial Port:

When a device is connected to the serial port and a subdevice has been successfully added, the serial port will be green; otherwise, it will be gray. Below, the parameters of each serial port and the number of connected devices are displayed. Click to view details.

3.6 Network Setting

3.6.1 WAN

3.6.1.1 WAN



The screenshot shows the WAN configuration page. At the top, there's a 'WAN' tab and 'Global Settings'. Below this is the 'Dual Link Option' section with a toggle for 'Enable WAN Failover'. The 'Main' section contains several fields: 'Connection Type' (SIM1 - 4G/5G), 'Password', 'Connection type' (AUTO), 'Keep Online Detection' (Ping), 'Detection Interval' (120 S), 'Backup Detection IP' (208.67.220.220), 'Username', 'APN' (cmnet), 'PIN Code', and 'Main Detection IP' (223.5.5.5). An 'Advance' button is at the bottom right.

Dual Link Configuration Options

Dual Link Option

Enable WAN Failover ☐

This option allows you to enable or disable dual-link functionality, meaning whether two links are active. Disabling this option means only the main link is active, and the backup link will not work. When enabled, you will see configuration options for dual links being online simultaneously, which works as follows:

- **Enabled:** When the main link is online, all default data is sent through the main link to the Internet. If the main link goes offline and the backup link is online, the system will switch to the backup link, sending the default data through the backup link to the Internet. Meanwhile, the main link will continuously try to reconnect. Once the main link reconnects, the system will switch back to the main link. In summary, the main link is prioritized, and the backup link serves as a backup.

Note: When both SIM cards are online, enabling load balancing and traffic distribution, the detailed data flow will be explained in the load balancing menu.

Attention: When the dual-link backup function is enabled, if the "Main Link Connection Type" or "Backup Link Connection Type" is set to "Static IP" or "DHCP," the corresponding online persistence function must be configured. For detailed configuration, refer to the online persistence description. The "Main Link Connection Type" and "Backup Link Connection Type" cannot be the same, and they cannot share the same physical WAN port.

Main Link/Backup Link

Select the Internet connection type from the dropdown menu. There are 8 WAN connection types available:

1. Disabled

Main

* Connection Type

Disables the WAN port connection type.

2. Static IP

Main

* Connection Type

* WAN IP Address

* Mask

* Gateway

* Static DNS

* Keep Online Detection

* Detection Interval

* Main Detection IP

* Backup Detection IP

This connection type is commonly used for business fiber optic or leased line access. The broadband service provider will provide details such as the IP address, subnet mask, gateway, and DNS, which need to be configured on the 5G gateway.

- **WAN IP Address:** The IP address set by the user or provided by the ISP.
- **Subnet Mask:** The subnet mask set by the user or provided by the ISP.
- **Gateway:** The gateway set by the user or provided by the ISP.
- **Static DNS:** The static DNS set by the user or provided by the ISP.

3. Automatic Configuration – DHCP

Main

* Connection Type

* Keep Online Detection

* Detection Interval

* Main Detection IP

* Backup Detection IP

This connection type is commonly used for cable TV (Cable) or some residential broadband services, such as Shenzhen Tianwei Video and Shanghai Cable Communication. The WAN port's IP address is obtained via DHCP.

4. PPPOE

Main

* Connection Type

Username

Password

* Keep Online Detection

* Detection Interval

* Main Detection IP

* Backup Detection IP

This connection type is typically used for ADSL broadband services from China Telecom and China Netcom, as well as other broadband providers. The PPPOE connection type requires the ISP to provide a username and password, which need to be configured on the 5G gateway.

- **Username:** The username used to log in to the Internet.
- **Password:** The password used to log in to the Internet.

5. 4G/5G

Main

* Connection Type	SIM1 - 4G/5G	Username	
Password		APN	cmnet
* Connection type	AUTO	PIN Code	
* Keep Online Detection	Ping		
* Detection Interval	120 S	* Main Detection IP	223.5.5.5
* Backup Detection IP	208.67.220.220		

- **Username:** The username used to log in to the Internet.
- **Password:** The password used to log in to the Internet.
- **APN:** The Access Point Name.
- **PIN:** The PIN code provided by the SIM card.

6. 3G/UMTS/4G/LTE

Main

* Connection Type	SIM1 - 3G/UMTS/4G/LTE	Username	
Password		APN	cmnet
* Dial String	*98*1# (TD-SCDMA)	* Connection type	AUTO
PIN Code			
* Keep Online Detection	Ping		
* Detection Interval	120 S	* Main Detection IP	223.5.5.5
* Backup Detection IP	208.67.220.220		

- **Username:** The username used to log in to the Internet.
- **Password:** The password used to log in to the Internet.
- **Call Center Number:** The call number to contact the operator.
- **APN:** The Access Point Name.
- **PIN:** The PIN code provided by the SIM card.

Network Type

* Connection type	AUTO
-------------------	-----------------------------------

Network Selection: Includes various options such as Automatic, Force to 3G, Force to 2G, 3G Preferred, 2G Preferred, etc. If a 5G module is used, the 5G network option will be added accordingly. Choose based on user needs and the type of module.

Online Persistence

* Keep Online Detection	Ping		
* Detection Interval	120 S	* Main Detection IP	223.5.5.5
* Backup Detection IP	208.67.220.220		

The online persistence function is used to detect whether the Internet link is valid. If enabled, the 5G gateway will automatically detect the Internet link. Once a disconnection or invalid link is detected, the system will automatically reconnect and establish a valid link. If the network environment is poor or in a private network, it is recommended to use 5G routing mode.

Online Persistence Methods:

- **None:** No online persistence function used.
- **Ping:** Sends ping packets to check the link. If this method is selected, the "Online Persistence Detection Interval," "Primary Server IP for Online Persistence Detection," and "Secondary Server IP for Online Persistence Detection" must be configured properly.

- **Route:** Uses the route method to check the link. If this method is selected, the "Online Persistence Detection Interval," "Primary Server IP for Online Persistence Detection," and "Secondary Server IP for Online Persistence Detection" must be configured properly.
- **TCP:** Uses the TCP method to check the link. If this method is selected, the "Online Persistence Detection Interval," "Primary Server IP for Online Persistence Detection," and "Secondary Server IP for Online Persistence Detection," and the "Check Times" configuration must be properly configured.

Online Persistence Detection Interval:

The time interval between two online persistence checks, in seconds.

Link Detection Interval:

When dual links are enabled, the time interval between two ping detection checks after obtaining the IP address, in seconds.

Primary Server IP for Online Persistence Detection:

The IP address of the primary server that responds to the 5G gateway's online detection packets. This configuration is only effective when the "Online Persistence Method" is set to "Ping" or "Route."

Secondary Server IP for Online Persistence Detection:

The IP address of the secondary server that responds to the 5G gateway's online detection packets. This configuration is only effective when the "Online Persistence Method" is set to "Ping" or "Route."

Advanced

[Advance](#)

Fixed WAN IP ☐

Fixed WAN GW Address ☐

* Allow these authentication ☒ PAP ☒ CHAP
☒ MS-CHAP ☒ MS-CHAPv2

Force reconnect ☐

STP ☐

Dial Failure to Restart ☒

Ppp Asyncmap ☒

Wan Nat ☒

* Band AUTO

Dial-up Failure Restart Mechanism:

This setting determines whether the device should restart if the dial-up fails for 10 minutes. If enabled, the device will restart; if disabled, it will attempt to redial.

Manual WAN IP/Gateway Setting:

If enabled, users can manually set the WAN port's IP address and gateway.

STP (Spanning Tree Protocol):

STP is a protocol used in loop networks to implement path redundancy through a specific algorithm, transforming a loop network into a loop-free tree network. This prevents packet duplication and infinite loops in the network.

3.6.1.2 Global Settings

WAN [Global Settings](#)

Global Settings

* Force Net Card Mode When setting to 100M or above, select automatic

* MTU

Assign WAN Port to Switch ☒

Force NIC Mode:

Default is set to automatic, but can be adjusted to 10M or 100M.

Assign WAN Port as Switch Port:

This configuration allows the device's WAN port to be set as a LAN port.

3.6.2 LAN

Router IP

* LAN IP

* Mask

* Gateway

* Local DNS

Gateway IP

● LAN IP:

This is the IP address of the 5G gateway as seen by your local area network (LAN).

● Subnet Mask:

The subnet mask corresponding to the 5G gateway's LAN IP.

● Gateway:

This sets the internal gateway of the 5G gateway. If left as default, the internal gateway is the IP address of the 5G gateway itself.

● Local DNS:

The DNS server is automatically assigned by the carrier's access server. However, if you have your own DNS server or prefer to use a more stable and reliable one, you may configure it here. Otherwise, the default settings will be used.

DHCP

These settings are used to configure the Dynamic Host Configuration Protocol (DHCP) server functionality of the 5G gateway. The gateway can act as a DHCP server in the network, automatically assigning IP addresses to each device. If you enable this feature, make sure that no other DHCP servers exist in the network, and all LAN devices should be set to automatically obtain IP and DNS.

DHCP

* DHCP Type

DHCP Server ☒

* IP Start

* Maximum DHCP Users

▼ Advance

* Client Lease Time

* WINS

Use DNSMasq for DHCP ☒

Use DNSMasq for DNS ☒

DHCP-Authoritative ☒

● DHCP Type:

Options include DHCP Server and DHCP Relay. If you select DHCP Relay, you must enter the IP address of the external DHCP server.

● DHCP Server:

DHCP is enabled by default. If another DHCP server is already in use in your network, or if you prefer not to use this feature, disable it. If you choose **DHCP Relay**, input the appropriate server IP.

● Start IP Address:

Enter a number from 1 to 254 for the starting address used by the DHCP server. Since the gateway's default IP is 192.168.4.1, the starting address must be 192.168.4.2 or higher, and no greater than 192.168.4.254. Default is 192.168.4.100.

● Maximum DHCP Users:

Set the maximum number of devices that the DHCP server can assign IPs to. Cannot exceed 253, and the total of start IP + user count must not exceed 255. Default is 50.

● Client Lease Time:

This defines how long a dynamic IP is leased to a client, in minutes. When the lease expires, the IP will be reassigned. Default is 1440 minutes (1 day). Range: 0–99999.

● WINS:

Windows Internet Name Service (WINS) manages computer names in networks. If using a WINS server, enter its IP here; otherwise, leave it blank.

● DNSMasq:

Allows your domain name to join the local search domain and enables extended host options. With DNSMasq, IP and DNS can be assigned to subnet devices. If not selected, the system defaults to using dhcpd to assign IP and DNS.

Multi-Subnet on LAN Port

Multiple LAN IP

				✓ Select All	+ Add	⊗ Delete
☐	No.	IP Address	Mask	Operation		
No Data						
Total 0		10/page	< 1 >	Go to	1	

You can define multiple LAN subnets by clicking the Add button and entering the corresponding IP address and subnet mask. You can also delete existing configurations as needed.

Static IP Assignment

Static Allocation

					Select All	Add	Delete
☐	No.	MAC	Name	IP Address	Client Lease Time	Operation	
No Data							
Total 0				10/page	< 1 >	Go to	1

You can add devices by selecting their MAC address, setting a device name and IPv4 address. This binds the selected device to a fixed IP address and lease time. Upon lease expiration, the lease is automatically renewed by default.

Add

×

* MAC

Please enter MAC

▼

* Name

* IPv4

* Client Lease Time

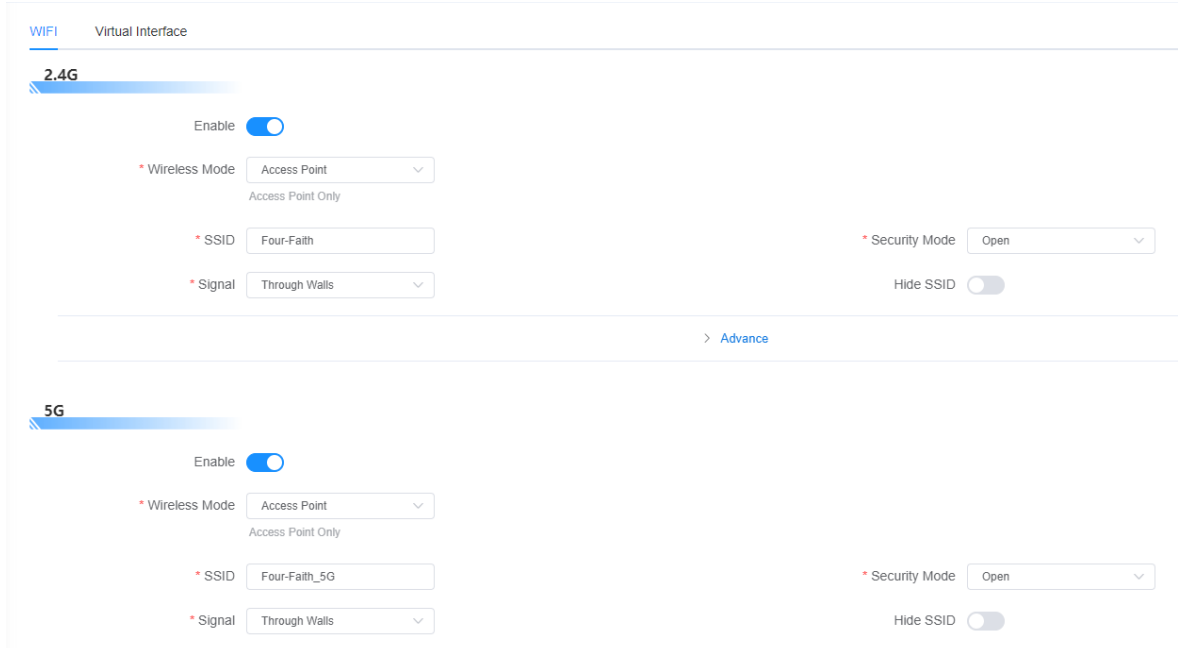
minutes

Cancel

OK

3.6.3 WiFi

3.6.3.1 WiFi



The screenshot shows the WiFi configuration interface for the FNR500. It is divided into two sections: 2.4G and 5G. Each section has an 'Enable' toggle switch, a 'Wireless Mode' dropdown menu, an 'SSID' text input, a 'Signal' dropdown menu, a 'Security Mode' dropdown menu, and a 'Hide SSID' toggle switch. The 2.4G section is currently selected, and the 5G section is also visible below it.

2.4G

Enable ☒

* Wireless Mode: Access Point (dropdown)
Access Point Only

* SSID: Four-Faith

* Signal: Through Walls (dropdown)

* Security Mode: Open (dropdown)

Hide SSID: ☐

> Advance

5G

Enable ☒

* Wireless Mode: Access Point (dropdown)
Access Point Only

* SSID: Four-Faith_5G

* Signal: Through Walls (dropdown)

* Security Mode: Open (dropdown)

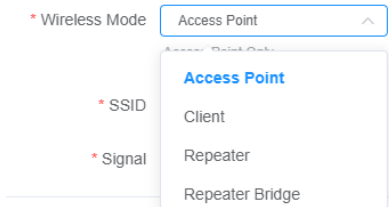
Hide SSID: ☐

Enable: Turns WiFi on.

Disable: Turns WiFi off.

Wireless Mode:

Four selectable modes: Access Point, Client, Repeater, Repeater Bridge.



The screenshot shows the 'Wireless Mode' dropdown menu. The 'Access Point' option is selected and highlighted in blue. The other options are 'Client', 'Repeater', and 'Repeater Bridge'.

* Wireless Mode: Access Point (dropdown)
Access Point Only

* SSID: Four-Faith

* Signal: Through Walls (dropdown)

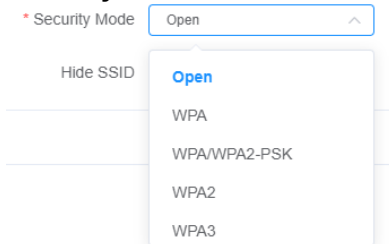
* Security Mode: Open (dropdown)

Hide SSID: ☐

SSID:

You can set the name of the wireless AP (access point). All devices in the wireless network must share the same SSID. SSIDs are case-sensitive, must consist of letters and/or numbers, and cannot exceed 32 characters.

Security Mode:



The screenshot shows the 'Security Mode' dropdown menu. The 'Open' option is selected and highlighted in blue. The other options are 'WPA', 'WPA/WPA2-PSK', 'WPA2', and 'WPA3'.

* Security Mode: Open (dropdown)

Hide SSID: ☐

Options include Open, WPA, WPA/WPA2-PSK, WPA2, and WPA3.

Signal Strength:

* Signal Through Walls

Through Walls

Standard

Energy Saving

Selectable modes include Through Walls, Standard, and Energy Saving.

3.6.3.2 Virtual Interface

Click Add to create a virtual interface. After successful creation, click Remove to delete the virtual interface.

WiFi Virtual Interface

2.4G

Select All Add Delete

No.	SSID	Security Mode	Hide SSID	Operation
No Data				

Total 0 10/page < 1 > Go to 1

3.6.4 VPN

3.6.4.1 PPTP

PPTP L2TP OPENVPN IPSEC GRE GRE-TAP VXLAN EOIP FRP

PPTP Server

PPTP Server ☒

Broadcast Support ☐

DNS1

WINS1

Server IP

Force MPPE Encryption ☐

DNS2

WINS2

Client IP(s)

Users Connection Status

PPTP Client

PPTP Client Options ☒

Server IP or DNS Name

Remote Subnet Mask

* MTU

NAT ☒

Username

ping Detection ☐

* Remote Subnet

MPPE Encryption

* MRU

Fixed IP ☐

Password

Connection Status

Broadcast Support:

Enable or disable broadcast support for the PPTP server.

Force MPPE Encryption:

Specify whether to force MPPE encryption for PPTP data.

DNS1, DNS2, WINS1, WINS2:

Set the primary and secondary DNS and WINS server addresses.

Server IP:

Enter the IP address of the 5G gateway to be used as the PPTP server. This must be different from the LAN address.

Client IP:

Specify the IP address range for clients in the format xxx.xxx.xxx.xxx-xxx.

Note: The client IP range must not overlap with the DHCP IP pool of the 5G gateway. Any range outside of the DHCP pool is acceptable.

Server IP or DNS Name:

The IP address or DNS name of the remote PPTP server.

Remote Subnet:

The internal network of the remote PPTP server.

Remote Subnet Mask:

The subnet mask of the remote PPTP server's internal network.

MPPE Encryption:

Specify whether MPPE encryption is supported.

MTU (Maximum Transmission Unit):

Set value between 0 and 1500.

MRU (Maximum Receive Unit):

Set value between 0 and 1500.

NAT:

Enable or disable NAT traversal.

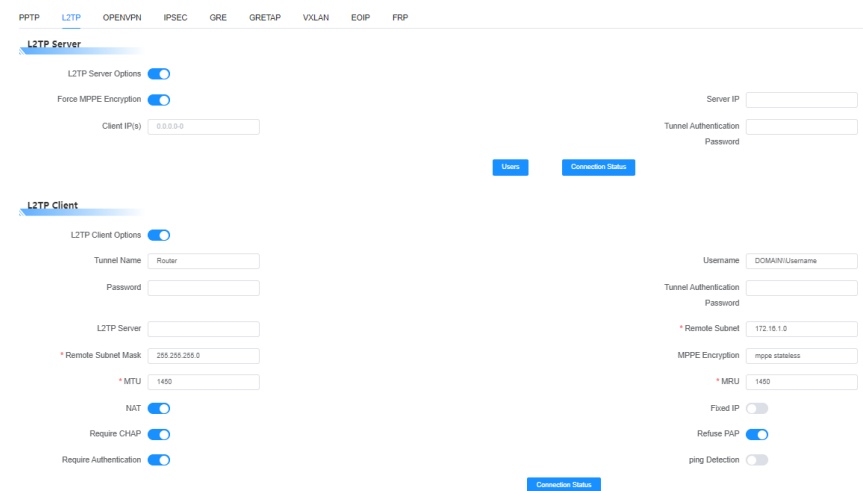
Username:

Username authorized by the PPTP server.

Password:

Password associated with the username.

3.6.4.2 L2TP



The screenshot displays the L2TP configuration page, which is divided into two main sections: L2TP Server and L2TP Client. The L2TP Server section includes options for L2TP Server Options (checked), Force MPPE Encryption (checked), Client IP(s) (0.0.0.0), Server IP, Tunnel Authentication, and Password. The L2TP Client section includes options for L2TP Client Options (checked), Tunnel Name (Router), Password, L2TP Server, Remote Subnet Mask (255.255.255.0), MTU (1450), NAT (checked), Require CHAP (checked), Require Authentication (checked), Username (COMAN/Username), Tunnel Authentication, Password, Remote Subnet (172.16.1.0), MPPE Encryption (mppe statistics), MRU (1450), Fixed IP, Refuse PAP (checked), and ping Detection.

Force MPPE Encryption:

Specify whether to force MPPE encryption for L2TP data.

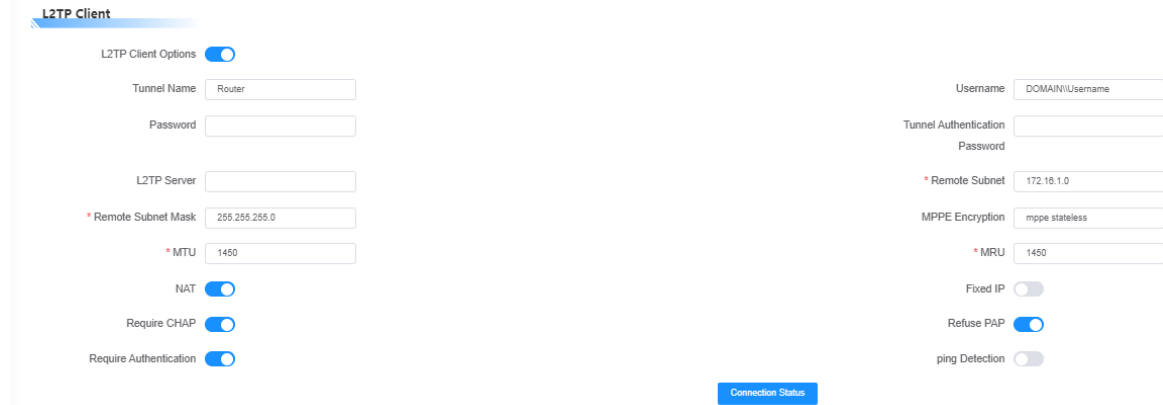
Server IP:

Enter the IP address of the 5G gateway to be used as the L2TP server. This must differ from the LAN address.

Client IP:

Specify the IP address range for clients in the format xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx.

Note: The client IP range must not overlap with the DHCP IP pool of the 5G gateway.



L2TP Server:

IP address or DNS name of the L2TP server.

Remote Subnet:

The internal network of the remote L2TP server.

Remote Subnet Mask:

Subnet mask of the remote L2TP server's network.

MPPE Encryption:

Specify whether MPPE encryption is supported.

MTU:

Maximum transmission unit, range 0–1500.

MRU:

Maximum receive unit, range 0–1500.

NAT:

Enable or disable NAT traversal.

Username:

Username authorized by the L2TP server.

Password:

Password associated with the username.

Allow CHAP Authentication Protocol:

Specify whether to allow CHAP authentication.

Reject PAP Authentication Protocol:

Specify whether to reject PAP authentication.

Allow Authentication Protocols:
Specify whether to allow authentication protocols.

3.6.4.3 OPENVPN

OpenVPN Server

Enable ☒

Connection Status [Show](#)

* Start Type ☒ System ☐ WAN Up

* Config Via ☒ Daemon ☐ Server

CA Cert [+ Select Upload File](#)

Public Server Cert [+ Select Upload File](#)

Private Server Key [+ Select Upload File](#)

DH PEM [+ Select Upload File](#)

Additional Config

Public CA Certificate:
The shared CA certificate for both the server and clients.

Public Server Certificate:
The server's certificate.

Server Private Key:
The private key configured on the server side.

DH PEM [+ Select Upload File](#)

Additional Config

TLS Auth Key [+ Select Upload File](#)

Certificate Revoke List

DH PEM Certificate:

The server's PEM certificate.

Additional Configuration:

Other optional server configuration settings.

TLS Authentication Key:

The authentication key used for TLS (Transport Layer Security).

Certificate Revocation List:

A list of revoked certificates.

OpenVPN Client

Enable ☒

Connection Status [Show](#)

* Server IP/Name

* Tunnel Device

* Encryption Cipher

User Pass Authentication ☐

ping Detection ☐

CA Cert [+ Select Upload File](#)

Public Client Cert [+ Select Upload File](#)

Private Client Key [+ Select Upload File](#)

* Port

* Tunnel Protocol

* Hash Algorithm

Server IP/Hostname:

The IP address or domain name of the OpenVPN server.

Port:

The port on which the OpenVPN client listens.

Tunnel Device:

- **TUN** – Routing mode
- **TAP** – Bridged mode

Tunnel Protocol:

Supports UDP and TCP protocols.

Encryption Standard:

Supported encryption standards for the tunnel include: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC

Hash Algorithm:

Provides fast data access, with options including: SHA1, SHA256, SHA512, MD5

Public CA Certificate:

The shared CA certificate for both the server and clients.

Public Client Certificate:

The certificate used by the client.

Client Private Key:

The private key used by the client.

[高级配置](#)

* TLS加密标准 None NAT TAP绑定到br0网桥上 IP地址 * TUN MTU设置 1500 TCP MSS TLS认证密钥 额外配置 基于路由策略 PKCS12 Key 	* 使用LZO压缩 Adaptive 子网掩码 UDP隧道片段 Disable ns证书类型(nsCertType)
---	---

Enable LZO Compression:

Enable or disable the use of LZO compression for data transmission.

NAT:

Enable or disable NAT traversal.

Bind TAP to br0 Bridge:

Enable or disable binding of the TAP interface to the br0 bridge.

Local IP Address:

Set the local IP address of the OpenVPN client.

TUN MTU Setting:

Configure the MTU value for the tunnel.

TCP MSS:

Set the maximum segment size for TCP data.

TLS Encryption Standard:

Supported TLS encryption standards include **AES-128 SHA** and **AES-256 SHA**.

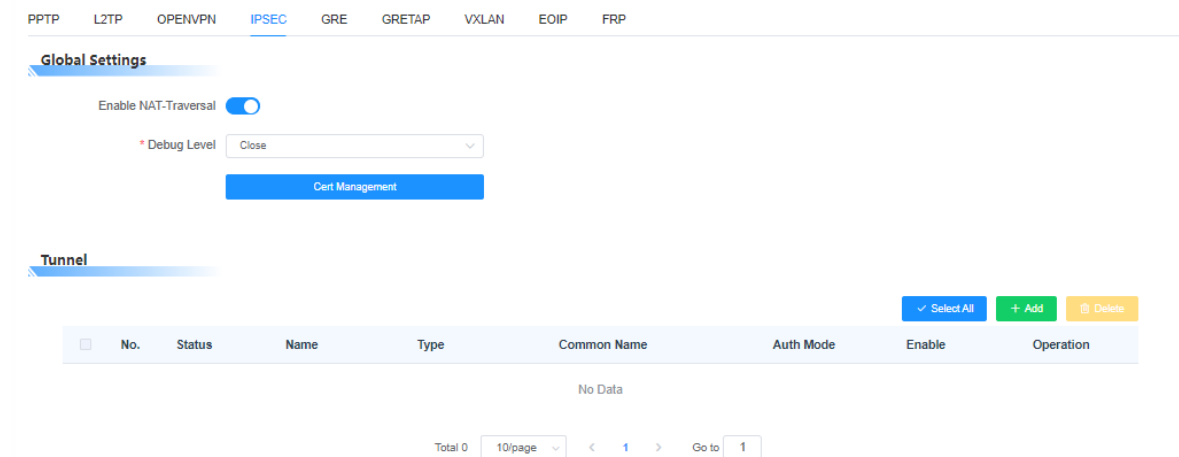
TLS Authentication Key:

Authentication key used for TLS.

Additional Configuration (Routing Policy Based):

Enter custom routing policies as part of additional server configuration.

3.6.4.4 IPSEC



The IPSEC page displays all current IPSEC connections and their statuses.

Status:

Indicates the current connection status, with three possible states:

- **Disconnected:** No connection request has been initiated to the remote end.
- **Negotiating:** A connection request has been sent and is in the negotiation process, but the connection is not yet established.
- **Established:** The connection is successfully established and can be used.

Operations:

Available operations for each connection include:

- **Delete:** Removes the connection. If the IPSEC tunnel is established, it will be torn down.
- **Edit:** Modify the connection settings. After editing, you must reload the connection to apply changes.
- **Reconnect:** Tears down the current tunnel and re-initiates the connection.
- **Enable:** When enabled, the connection will attempt to establish automatically upon system reboot or manual reconnection. If disabled, it will not.

Add New:

Used to create a new IPSEC connection.

Delete:

Used to remove an existing IPSEC connection.

Name:

The name of the IPSEC connection.

Detection:

This section contains the configuration information for connection detection (DPD).

Detection

Enable DPD Detection ☒

* Time Interval * Timeout

* Operation

ping Detection ☐

* Detection Interval S * IP Address

* Restart times

Enable DPD (Dead Peer Detection):

Enable or disable DPD.

Time Interval:

DPD detection interval time.

Timeout:

Timeout period for DPD.

Action:

Action to be taken upon DPD timeout.

Detection

Enable DPD Detection ☒

* Time Interval * Timeout

Sign:

Choose between pre-shared key or certificate authentication. Currently, only pre-shared key is supported.

Sign

* Auth Mode * Secret Key

Advanced Configuration:

This section contains configuration settings related to IKE, ESP, and negotiation modes.

Phase 1

* IKE Encryption

AES (256 bit)

* IKE Integrity

MD5

* IKE Groupype

Group2(1024)

* IKE Lifetime

24

Phase 2

* ESP Encryption

AES (256 bit)

* ESP Integrity

SHA2 (512)

* ESP Groupype

NULL

* ESP Lifetime

24

IKEv2

Use IKEv2

☐

Aggressive Mode

☐

Perfect Forward Secrecy

☒

Enable Advanced Configuration:

Enable this to manually set Phase 1 and 2 parameters; otherwise, the system will auto-negotiate.

IKE Encryption:

Encryption method for the IKE phase.

IKE Integrity:

Integrity algorithm for the IKE phase.

IKE DH Group:

Diffie-Hellman group.

IKE Lifetime:

IKE lifetime (in hours), default is 0.

ESP Encryption:

Encryption method for ESP.

ESP Integrity:

Integrity algorithm for ESP.

ESP Lifetime:

ESP lifetime (in hours), default is 0.

Aggressive Mode:

Enable to use aggressive mode, otherwise main mode is used.

Perfect Forward Secrecy (PFS):

Enable to use session key forward encryption.

3.6.4.5 GRE

GRE Tunnel

GRE Tunnel ☒

Tunnel	Name	Through	Peer Wan IP Addr	Peer subnet	Peer Tunnel IP	Local Tunnel IP	Enable	Operation
No Data								

Total 0 10page < 1 > Go to 1

GRE (Generic Routing Encapsulation) is a tunneling protocol that encapsulates certain network layer protocols (e.g., IP, IPX) to transmit them over another network layer protocol (e.g., IP). GRE uses tunnel technology and is a Layer 3 VPN protocol.

Add

Name

* Through

* Peer Wan IP Addr

* Peer subnet

* Peer Tunnel IP

* Local Tunnel IP

* Local Netmask

NAT ☐

* MTU

Keepalive ☐

ping Detection ☐

Cancel OK

GRE Tunnel:

Enable or disable GRE functionality.

Tunnel Count:

Up to 12 GRE tunnels can be configured.

Status:

Indicates whether the current GRE tunnel is enabled.

Name:

Tunnel name, up to 30 characters.

Interface:

GRE send/receive interface (LAN or PPP dial-up).

Peer WAN IP Addr:

WAN IP of the peer GRE.

Peer Subnet:

Subnet of the peer GRE (e.g., 192.168.4.0/24).

Peer Tunnel IP:

Tunnel IP of the remote GRE peer.

Local Tunnel IP:

Tunnel IP address of the local GRE.

Local Subnet Mask:

Subnet mask for the local GRE tunnel.

Keepalive:

Enable or disable GRE keepalive.

Retry Count:

Max retry count for failed keepalive.

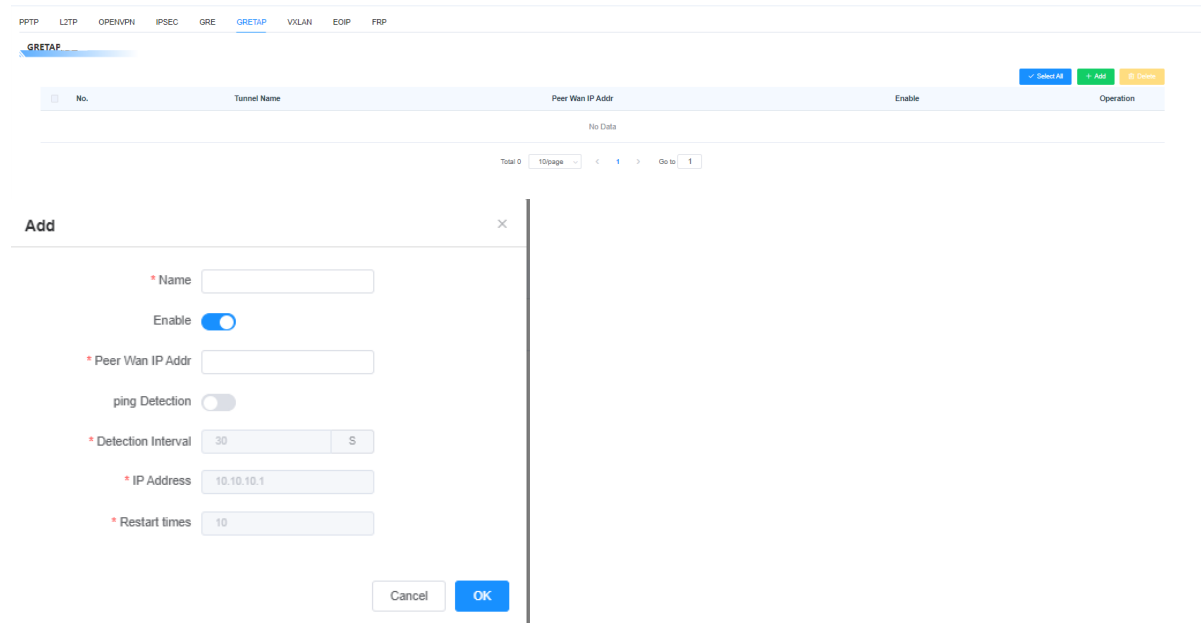
Retry Interval:

Interval between keepalive packets.

Failure Policy:

Policy on keepalive failure.

3.6.4.6 GRE TAP



The screenshot displays the GRE TAP configuration page. At the top, there are navigation tabs: PPTP, L2TP, OPENVPN, IPSEC, GRE, GRE TAP (selected), VXLAN, EOIP, and FRP. Below the tabs is a table with the following columns: No., Tunnel Name, Peer Wan IP Addr, Enable, and Operation. The table is currently empty, showing 'No Data'. Below the table, there is a form to add a new GRE TAP tunnel. The form includes the following fields and controls:

- Name:** A text input field.
- Enable:** A toggle switch, currently turned on.
- Peer Wan IP Addr:** A text input field.
- ping Detection:** A toggle switch, currently turned off.
- Detection Interval:** A text input field with '30' and a unit dropdown set to 'S'.
- IP Address:** A text input field with '10.10.10.1'.
- Restart times:** A text input field with '10'.

At the bottom of the form, there are 'Cancel' and 'OK' buttons.

Name:

Interface name of GRE TAP, max 32 characters.

Enable:

Enable or disable this GRE TAP tunnel.

Peer WAN IP Addr:

WAN IP address of the remote GRE TAP.

Ping Detection:

Enable link detection for GRE TAP.

Detection Interval:

Time interval for link detection.

IP Address:

Target IP address for GRETAP detection.

Restart Times:

Number of failed checks before reinitiating GRETAP.

3.6.4.7 VXLAN



The VXLAN configuration interface shows a toggle for 'Enable' which is turned on. Below it are four input fields: 'VXLAN Tunnel Name' (containing 'vxlan1'), 'VXLAN Network Identifier' (empty), 'VXLAN MTU' (containing '1450'), 'VXLAN remote ip addr' (empty), and 'VXLAN destination port' (containing '8472').

Enable:

Enable or disable VXLAN.

VXLAN Tunnel Name:

Name of the VXLAN network interface.

VXLAN Remote IP Addr:

WAN IP of the remote VXLAN peer.

VXLAN Network Identifier:

VXLAN network identifier (must match on both ends).

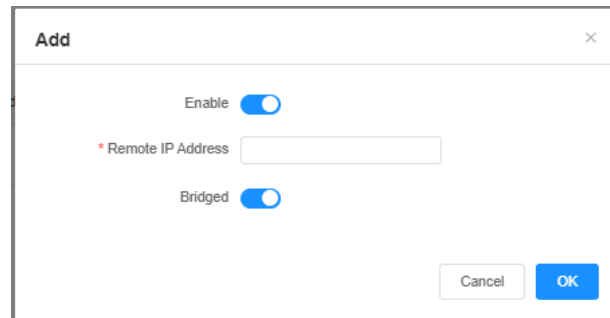
VXLAN Destination Port:

Default is 8472.

VXLAN MTU:

MTU size for VXLAN transmission (default 1450).

3.6.4.8 EOIP



The EOIP configuration dialog, titled 'Add', contains three settings: 'Enable' (toggle on), 'Remote IP Address' (empty input field), and 'Bridged' (toggle on). At the bottom are 'Cancel' and 'OK' buttons.

Enable:

Enable or disable EOIP.

Remote IP Address:

WAN IP of the peer EOIP.

Bridge:

Whether to enable bridging. If disabled, EOIP subnets differ; if enabled, subnets must match.

EOIPTunnel

☐ Tunnel
 Remote IP Address
 Bridged
 IP Address
 Mask
 Enable
 Operation

No Data

Total 0 10/page < 1 > Go to 1

IP Address:

Tunnel IP for EOIP.

Mask:

Subnet mask for EOIP tunnel.

3.6.4.9 FRP

FRP

Enable ☒

* FRP FRP Server Addr

* FRP FRP Remote Token

* FRP FRP Server Port

☐ No.
 Name
 Local IP
 Local Port
 Remote Port
 Operation

No Data

Total 0 10/page < 1 > Go to 1

Enable:

Enable or disable FRP.

FRP Server Address:

Public IP address of the FRP server.

FRP Server Port:

Port of the public FRP server.

FRP Remote Token:

Authentication key of the public FRP server.

Local IP:

Target IP to be accessed via FRP mapping.

Local Port:

Target port to be accessed.

Remote Port:

Port used by external users to access the device through the public FRP server.

3.6.5 NAT

3.6.5.1 Port Forwarding

Port forwarding allows you to set up public services (e.g., web server, FTP server, or other internet applications) on the network.

Port Forward
DMZ
Virtual IP Setting

Port Forward

No.	Name	Protocol	Action	Enable	Operation
No Data					

Total 0
10page
1
Go to 1

Port Range Forward

No.	Name	Protocol	Action	Enable	Operation
No Data					

Total 0
10page
1
Go to 1

Add

Name

Enable

* Protocol
Select

Source Net
0.0.0.0/24

* Port From

* IP Address

* Port To

Cancel
OK

Name:

Enter the name of the application.

Protocol:

Select UDP or TCP; both can be selected.

Allowed Source IP Range:

Enter the IP addresses of Internet users.

Source Port:

Enter the external port number used by the service.

IP Address:

Enter the internal IP address of the server to be accessed.

Destination Port:

Enter the internal port number used by the service.

Enable:

Check to enable the defined port forwarding rule. Default is disabled.

After modifying the page, click "Save Settings" to apply changes or "Cancel" to discard.

Port Range Forwarding

Port Range Forward

						✓ Select All	+ Add	⊞ Delete
☐	No.	Name	Protocol	Action		Ena ble	Operation	
No Data								
Total: 0 10/page < 1 > Go to: 1								

Some applications require a specific port range to operate correctly. The 5G gateway will forward these requests to the designated device.

Add

Name

Enable

* Protocol

Select

* Start Port

* End Port

* IP Address

Cancel

OK

Name:

Name of the application.

Enable:

Check to enable this port range forwarding rule. Default is disabled.

Protocol:

Select UDP or TCP; both can be selected.

Start Port:

Start port number of the range.

End Port:

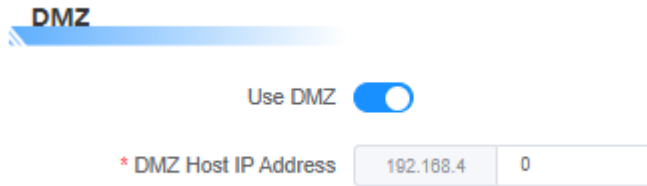
End port number of the range.

Destination IP:

Internal IP address of the server to be accessed.

Click "Save Settings" to save changes or "Apply" to make the settings effective.

3.6.5.2 DMZ



DMZ

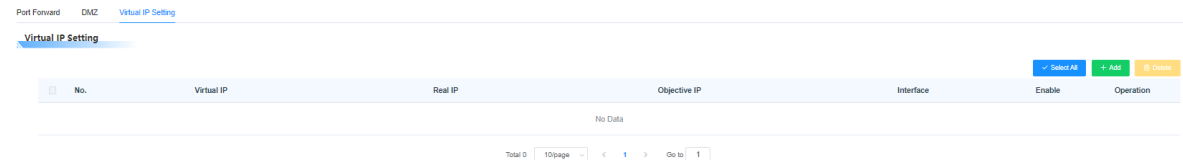
Use DMZ ☒

* DMZ Host IP Address

The DMZ function allows a network user to be exposed to the Internet in order to use specific services. The DMZ host forwards all ports to a specific computer. Since only desired ports are opened in port forwarding, it is more secure. However, the DMZ host opens all ports, exposing the computer to the Internet.

To enable the DMZ function, select "Enable," then enter the IP address of the computer in the "DMZ Host IP Address" field.

3.6.5.3 Virtual IP Setting



Port Forward DMZ Virtual IP Setting

Virtual IP Setting

No.	Virtual IP	Real IP	Objective IP	Interface	Enable	Operation
No Data						

Total 0 10page < 1 > Go to 1

Virtual IP:

The virtual IP address.

Real IP:

The actual IP address to be accessed, such as an IP under the router (e.g., 192.168.4.100).

Destination IP:

The subnet address and gateway of the peer; default is empty (0.0.0.0/0).

Interface:

The interface through which the virtual IP is forwarded.

3.6.6 VLAN

Virtual Local Area Network (VLAN)						
VLAN	W	1	2	3	4	Assigned To Default Bridge
1	☐	☒	☒	☒	☒	Yes
2	☒	☐	☐	☐	☐	No
3	☐	☐	☐	☐	☐	No
4	☐	☐	☐	☐	☐	No
5	☐	☐	☐	☐	☐	No
6	☐	☐	☐	☐	☐	No
7	☐	☐	☐	☐	☐	No
8	☐	☐	☐	☐	☐	No
9	☐	☐	☐	☐	☐	No
10	☐	☐	☐	☐	☐	No
11	☐	☐	☐	☐	☐	No
12	☐	☐	☐	☐	☐	No
13	☐	☐	☐	☐	☐	No
14	☐	☐	☐	☐	☐	No
15	☐	☐	☐	☐	☐	No

The VLAN feature allows users to flexibly divide VLAN ports as needed. The system supports VLAN1 to VLAN15, a total of 15 VLANs. However, the device only has 5 physical ports—1 WAN and 4 LAN ports. Ports can be grouped based on specific needs, but LAN and WAN ports cannot be assigned to the same VLAN.

3.6.7 Bridge

Bridge					
No.	Bridge Name	Priority	MTU	Assign To Interface	Operation
LAN	br0	32768	1500	—	Edit

Create Bridge:

Create a new bridge for use. STP stands for Spanning Tree Protocol, and you can set the priority for the bridge. A lower number indicates a higher priority.

Assign to Bridge:

This allows you to assign any valid interface to an already created bridge.

Current Bridge List:

Displays the list of currently active bridges.

Bridge Parameters

* Bridge Name

STP ☐

* Priority

* MTU

IP Address

Mask

Steps to create a bridge:

Click the “Add” button in the Create Bridge section to access the configuration page.

- **Bridge Name** is the name of the bridge.
- **STP** indicates whether to enable the Spanning Tree Protocol.
- **Priority** indicates priority for STP (lower value = higher priority).
- **MTU** is the Maximum Transmission Unit (default is 1500).

If unnecessary, you can delete it. Click “Save” or “Apply” to proceed to the next step:

After entering the bridge’s IP address and subnet mask, click “Confirm” to generate the bridge.

Note: The bridge must be created before it can be applied.

To assign interfaces to a bridge (e.g., assigning ra0—the wireless interface—to bridge br1):

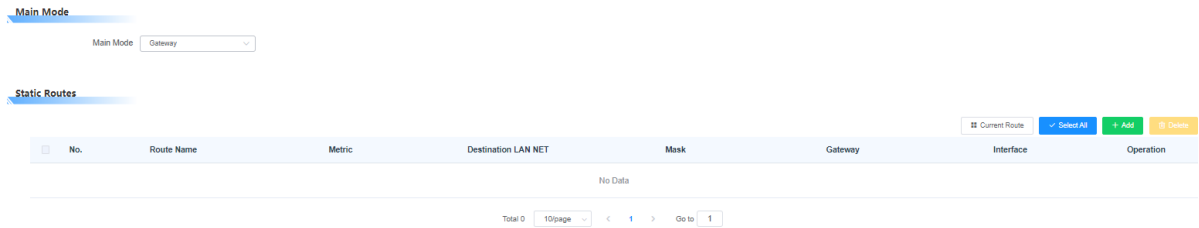
Assign To Interface

			✓ Select All	+ Add	🗑 Delete
☐	Interface	Priority	Operation		
No Data					

- **Prio** indicates interface priority. If multiple interfaces are bound to the same bridge, this becomes relevant (lower value = higher priority). Click “Apply” to activate.

Note: Some WAN interfaces listed should not be bound. This bridge function is primarily used for the LAN side and should not be bound to the WAN port.

3.6.8 Routing



On the Routing page, you can set the operation mode and configure static routing. For most users, Gateway mode is recommended.

Main Mode

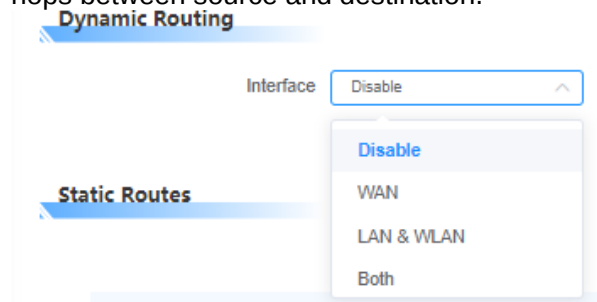
Main Mode Gateway

Main Mode:

Select the appropriate operation mode. If the 5G gateway shares an Internet connection, keep the default setting as Gateway mode (recommended for most users). To use only the routing function of the 5G gateway on the network, select “5G Gateway.”

Dynamic Routing:

This feature is not available in Gateway mode. Dynamic routing allows the 5G gateway to automatically adjust to physical changes in the network layout and exchange routing tables with other 5G gateways. It determines the packet route based on the minimum number of hops between source and destination.



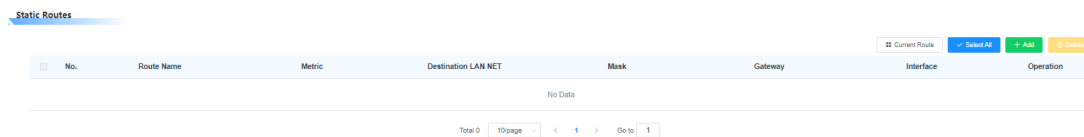
To enable dynamic routing for the WAN side, select WAN.

To enable it for the LAN and WLAN, select LAN & WLAN.

To enable it for both WAN and LAN, select Both.

To disable dynamic routing for all traffic, keep the default setting (Disabled).

Static Routes:



To set up a static route between the 5G gateway and another network, select a route ID from the static route dropdown list. (Static routing refers to predetermined paths for data to reach specific hosts or networks.)

Add
×

Route Name
* Metric
* Destination LAN NET
* Mask
* Gateway
* Interface

Cancel
OK

Route Name:

User-defined name, up to 25 characters.

Metric:

Metric for the route from source to destination. Range: 0–9999.

Destination LAN NET:

Target IP address for the route.

Mask:

Determines which part of the destination IP is the network and which part is the host.

Gateway:

IP address of the gateway device used to reach the destination network or host.

Interface:

Choose an interface such as LAN, WLAN, or WAN based on the destination location.

To delete a configured static route, select the corresponding route ID and click the "Delete" button.

To view the current routing table of the 5G gateway, click the "Current Route" button.

Current Route
×

Destination LAN N ET	Gateway	Subnet Mask	Metric	Interface
127.0.0.0	0.0.0.0	255.0.0.0	0	lo
192.168.4.0	0.0.0.0	255.255.255.0	0	br0

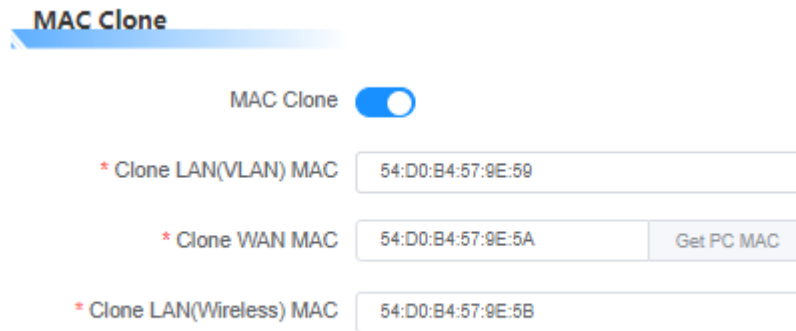
Click "Save Settings" to save changes without applying them. Click "Apply" to make changes effective immediately.

3.6.9 5G LAN Settings

The 5G LAN feature is related to the 5G module. Only specific 5G modules support this feature.

3.6.10 MAC Clone

Some ISPs require MAC address registration. If you want to avoid re-registering your MAC address, you can clone the registered MAC address to the 5G gateway.



MAC Clone

MAC Clone ☒

* Clone LAN(VLAN) MAC

* Clone WAN MAC

* Clone LAN(Wireless) MAC

MAC Address Cloning includes three parts: LAN port cloning, WAN port cloning, and Wireless MAC address cloning.

Two important notes:

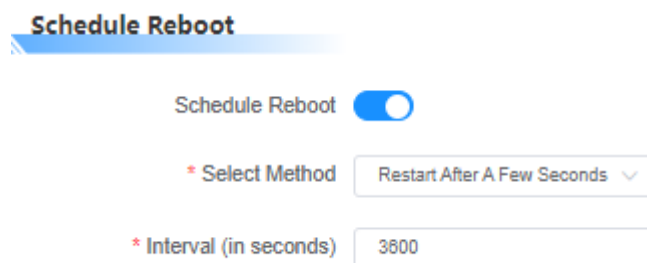
1. MAC addresses are 48-bit and must not be multicast addresses. This means the first byte should be an even number.
2. Because the wireless and LAN ports are connected through the br0 bridge, the MAC address of bridge br0 is determined by the lower value between the LAN and Wireless MAC addresses.

3.7 Application Settings

3.7.1 Active Policy

The Active Policy page allows you to configure scheduled reboots and scheduled tasks.

Scheduled Reboot:



Schedule Reboot

Schedule Reboot ☒

* Select Method

* Interval (in seconds)

You can set the router to reboot:

- After a specified number of seconds (e.g., reboot after xxx seconds).
- At a specific date/time, on specific days of the week, or daily.

Timed Tasks:

Timed Tasks

Enable ☒

☐ Cycle

☐ Every minute

☐ Every minutes(s) starting at minute

☐ Specific minute (choose one or many)

☐ Every minute between minute and minute

Task

3.7.2 Security Policy

3.7.2.1 IP Restriction

You can configure a blacklist or whitelist to restrict the source or destination IP addresses for incoming and outgoing traffic, including the communication protocols.

IP Restrictions

Enable ☒

* Strategy

Discard compliant data

No.	Direction	Protocol	Source Address	Target Address	Operation
No Data					

Total 0

3.7.2.2 URL Restriction

You can configure a blacklist or whitelist of URL addresses. Only traffic that matches the defined rules will be accepted; all others will be discarded.

URL Restrictions

Enable ☒

* Strategy

Discard compliant data

No.	URL	Operation
No Data		

Total 0

3.7.2.3 MAC Restriction

You can configure a blacklist or whitelist of MAC addresses. Only traffic that matches the defined rules will be accepted; all others will be discarded.

MAC Restrictions

Enable ☒

* Strategy

Discard compliant data

No.	MAC	Operation
No Data		

Total 0

3.7.2.4 Firewall

You can enable or disable the firewall, select to filter specific types of Internet data, and block anonymous Internet requests to enhance network security.

Firewall Protection

Firewall Protection

SPI Firewall ☒

The firewall enhances network security and uses Stateful Packet Inspection (SPI) to check incoming packets. To enable firewall protection, select "Enable." SPI must be enabled to use

other firewall features like proxy filtering and WAN request blocking.

Additional Filters

Additional Filters

- ☐ Filter Proxy
 ☐ Filter Cookies
☐ Filter Java Applets
 ☐ Filter ActiveX

- **Filter Proxy:**
Proxy servers over WAN can reduce gateway security. This option blocks access to any WAN proxy server. Check the box to enable Proxy filtering, or uncheck to disable.
- **Filter Cookies:**
Cookies are data stored by websites on your computer. Enable this option to filter cookies.
- **Filter Java Applets:**
Blocking Java may prevent certain Java-based web pages from loading. Enable this option to filter Java applets.
- **Filter ActiveX:**
Blocking ActiveX may prevent certain ActiveX-based web pages from loading. Enable this option to filter ActiveX controls.

Block WAN Requests

Block WAN Requests

- ☒ Block Anonymous WAN Requests (ping)
 ☒ Filter IDENT (Port 113)
☒ Block WAN SNMP access

- **Block Anonymous WAN Requests (Ping):**
Check this option to block anonymous Internet requests, preventing external users from pinging or probing your network. This feature is enabled by default. Disable to allow anonymous requests.
- **Filter IDENT (Port 113):**
This prevents external devices from scanning port 113. Enable or disable this filter as needed.
- **Block WAN SNMP Access:**
Blocks SNMP connection requests from the WAN.

Impede WAN DoS/Brute Force

Impede WAN DoS/Bruteforce

- ☐ Limit SSH Access
 ☐ Limit Telnet Access
☐ Limit PPTP Server Access
 ☐ Limit L2TP Server Access

- **Limit SSH Access:**
Limits SSH requests from the WAN. Only 2 SSH connections per minute are allowed from the same IP.
- **Limit Telnet Access:**
Limits Telnet requests from the WAN. Only 2 Telnet connections per minute are allowed from the same IP.
- **Limit PPTP Server Access:**
When a PPTP server is enabled, this option limits WAN-side PPTP requests to 2

- connections per minute per IP.
- **Limit L2TP Server Access:**
When an L2TP server is enabled, this option limits WAN-side L2TP requests to 2 connections per minute per IP.

3.7.2.5 WEB Access

You can configure the local web access protocol, port, and user logout time, as well as enable remote web access management.

WEB

Web GUI Management ☒

Protocol ☒ HTTP ☐ HTTPS

* HTTP Port

* User Automatic Logout Time S

Automatically log out after closing the page for a few seconds, if 0, do not automatically log out

Remote WEB

Remote HTTP Management ☒

Support accessing management pages through HTTP from WAN port/VPN

Remote HTTPS Management ☐

Support accessing management pages through HTTPS from WAN port/VPN

3.7.3 QoS

The QoS (Quality of Service) function allows you to limit upload and download traffic, and separately configure the maximum upload and download speeds for the main and backup links.

Main

Enable ☒

* Uplink (kbps)

* Downlink (kbps)

Backup

Enable ☒

* Uplink (kbps)

* Downlink (kbps)

- **Uplink (kbps):**
Enter the allocated upload bandwidth. Typically set to 80–90% of your actual available bandwidth.
- **Downlink (kbps):**
Enter the allocated download bandwidth. Typically set to 80–90% of your actual available bandwidth.

3.8 Maintenance

3.8.1 Diagnostics

Click “Start Diagnosis” to let the device run diagnostics on the primary and backup links. Any detected anomalies will be prompted. You can also export the diagnostic report.

Diagnosis

* Diagnostic Content

Network

⚙️ Diagnosing

Diagnostic Results

Global Network

Current Link
Main Link
Normal

DNS Resolution
Test Address: www.baidu.com
Abnormal

IPv4 Resolution: --

IPv6 Resolution: --

DNS resolution failed, please check if the correct DNS address is set. If it is a dedicated network card, please ignore it

Main Link

Network Config
SIM1 - 4G/5G
Normal

WIFI STA
Status: Not Connected
Error

Channel: Channel 36

Signal: --%

RSSI: -- dBm

3.8.2 Network Tools

There are three modes in the network tools section: ping, traceroute, and nslookup, which can be used for device analysis.

Network Tools

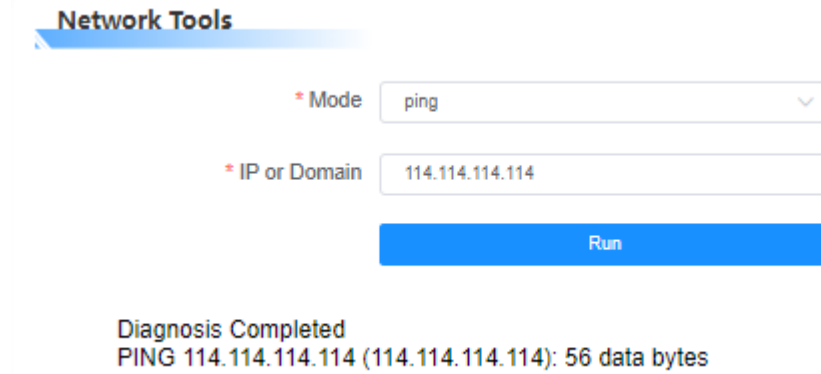
* Mode

ping

* IP or Domain

Run

Reference as follows:



Network Tools

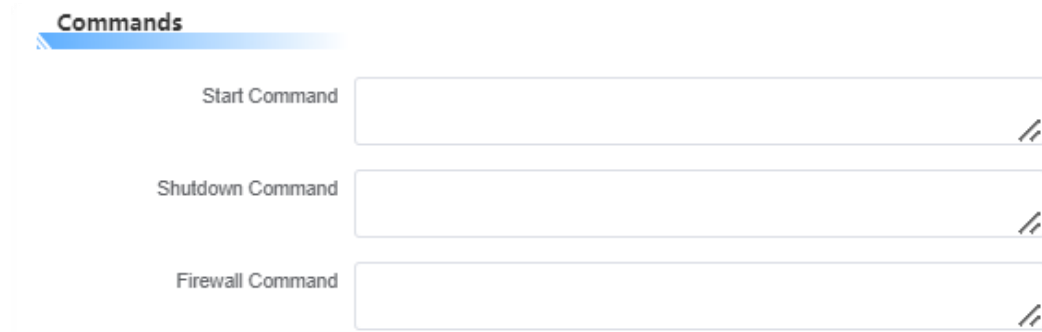
* Mode: ping

* IP or Domain: 114.114.114.114

Run

Diagnosis Completed
PING 114.114.114.114 (114.114.114.114): 56 data bytes

3.8.3 Command Debugging



Commands

Start Command:

Shutdown Command:

Firewall Command:

You can execute commands via the command window.

- **Startup Command:**
Command executed automatically when the 5G gateway boots.
- **Shutdown Command:**
Command executed automatically when the 5G gateway shuts down.
- **Firewall Command:**
Custom iptables commands executed each time the firewall is started.

Terminal

```
Four-Faith v2.0 std (c) 2012
Release: Sep 10 2024 12:37:17 (SVN revision: std)

Four-Faith login:
Four-Faith v2.0 std (c) 2012
Release: Sep 10 2024 12:37:17 (SVN revision: std)

Four-Faith login: | |
```

This terminal window allows you to log into the device using its username and password, enabling you to run commands or queries.

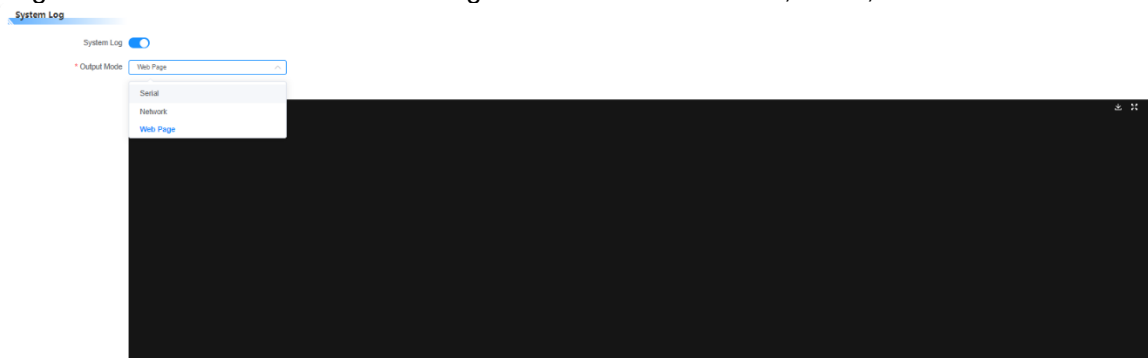
3.8.4 Log Management

[Realtime Log](#) [History Log](#)

You can choose to view real-time logs or configure historical logs.

Real-Time Logs

Logs can be viewed in real-time through the local web interface, serial, or network.



For the network mode, UDP is used by default. You need to configure the remote server's IP address and port to receive log messages. Please note that enabling this mode will consume device data, so use caution with limited data plans.

System Log

System Log

Output Mode

Network

Output logs to remote server port using UDP protocol

Remote Server

Port

514

Historical Logs

Log caching requires the device to support eMMC or large JFFS. If these features are unavailable, historical log caching is not supported.

Realtime Log

History Log

Log Cache

Enable

Attention: Before using this function, please ensure that eMMC is correctly mounted or JFFS function is enabled, and enable real-time logging function!

2025 April

Previous Month

Today

Next Month

Mon	Tue	Wed	Thu	Fri	Sat	Sun
31	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	01	02	03	04
05	06	07	08	09	10	11

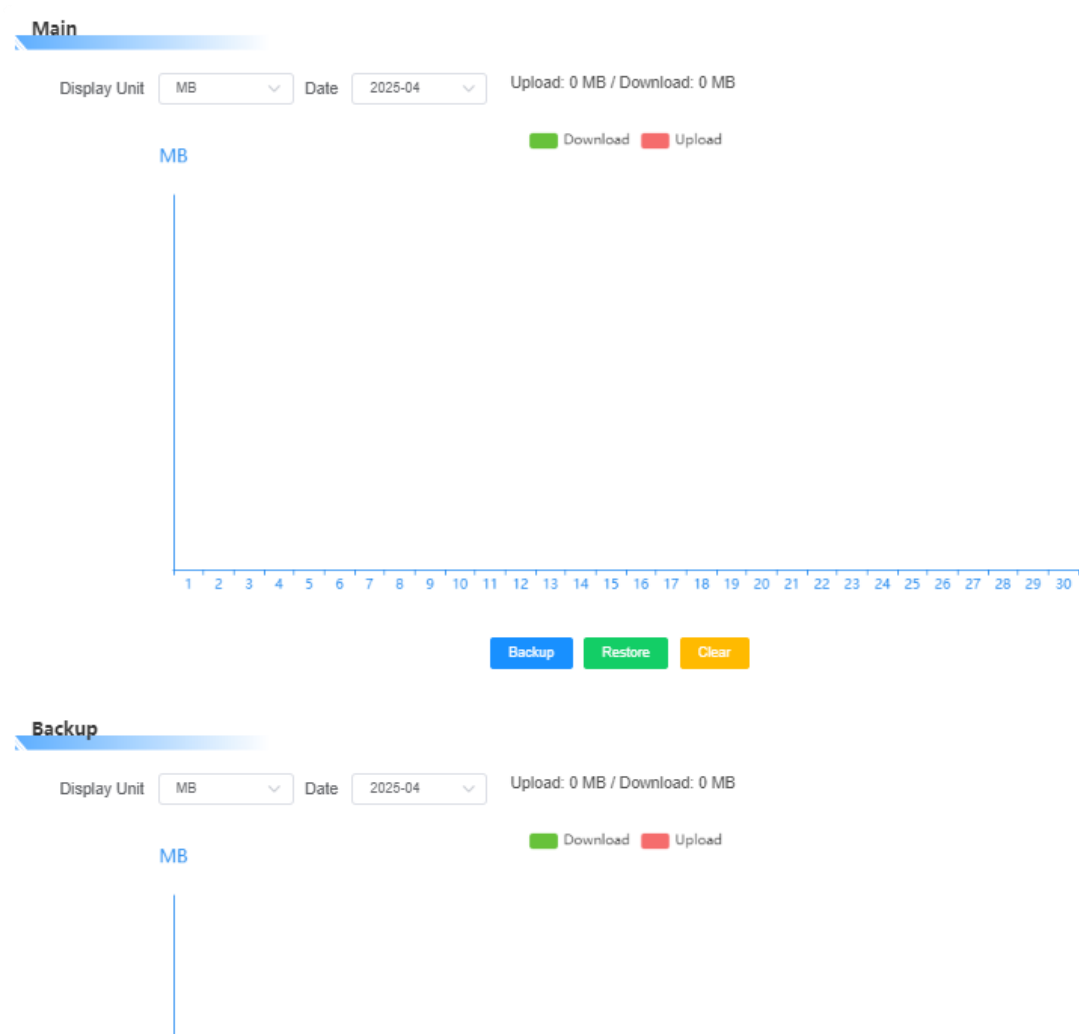
Save

Apply

3.8.5 Traffic Statistics

This page is used to display the traffic statistics for the device during the current month. It records and displays daily uplink and downlink total traffic for the WAN port throughout the current month.

53



3.8.6 Storage Settings

By default, this function is disabled. When enabling it for the first time, you may perform a formatting operation (this is not required for subsequent uses to avoid accidental deletion). Once enabled, the size of JFFS or eMMC storage can be viewed. If historical log caching or other storage-related features are needed, this function must be enabled first.

JFFS

Enable ☐

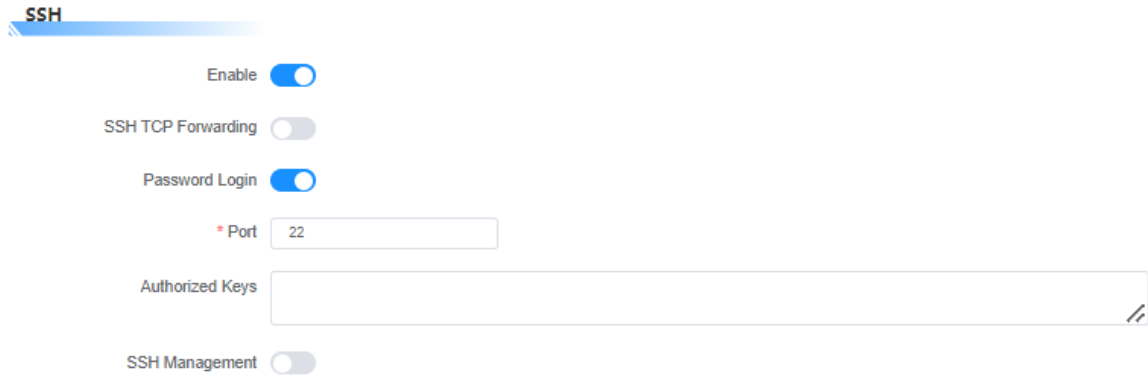
Status Disable

Format

3.8.7 Remote Management

3.8.7.1 SSH

After enabling the SSHD service, remote access to the 5G gateway's operating system via an SSH client is allowed.



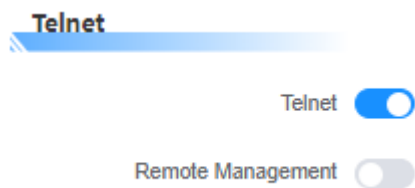
The SSH configuration interface shows the following settings:

- SSH** (Section Header)
- Enable**: ☒
- SSH TCP Forwarding**: ☐
- Password Login**: ☒
- * Port**:
- Authorized Keys**:
- SSH Management**: ☐

- **SSH TCP Forwarding**: Whether to support TCP forwarding.
- **Password Login**: Whether a password is required for login.
- **Port**: Set the SSHD port; the default is port 22.
- **Authorized Key**: Can be set as needed. By default, the system uses the login username and password.

3.8.7.2 Telnet

Enable or disable the Telnet function.



The Telnet configuration interface shows the following settings:

- Telnet** (Section Header)
- Telnet**: ☒
- Remote Management**: ☐

The local Telnet function is enabled by default, while remote Telnet management is disabled by default.

3.8.7.3 SNMP

You can set parameters such as location, contact, name, read-only community string, and read-write community string.

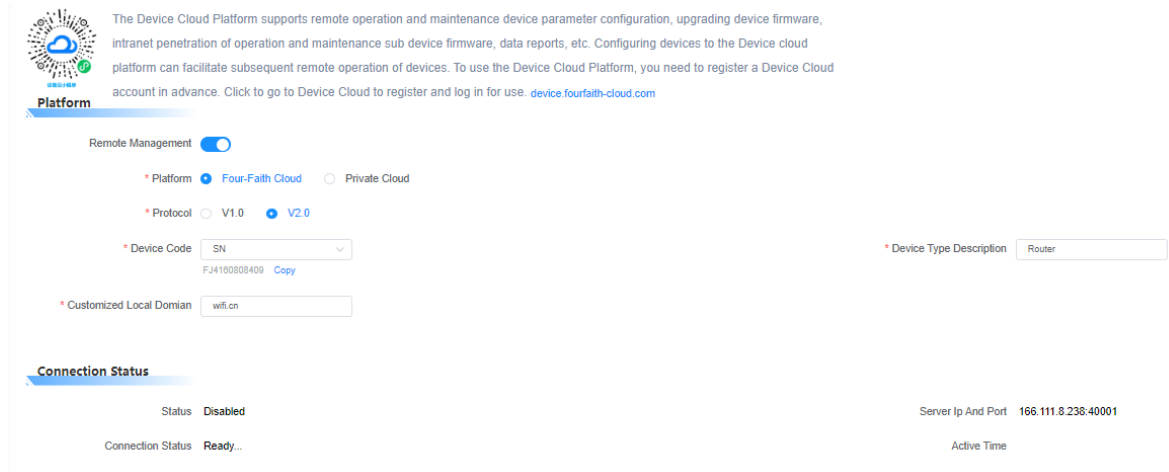


The SNMP configuration interface shows the following settings:

- SNMP** (Section Header)
- Enable**: ☒
- * Location**:
- * Name**:
- * RW Community**:
- * Contact**:
- * RO Community**:

- **Enable**: Turn SNMP function on or off.
- **Location**: Describes the physical location of the SNMP device.
- **Contact**: SNMP administrator's name.
- **Name**: The SNMP device name.
- **Read-Only Community**: A string that allows SNMP clients to read information from the device.
- **Read-Write Community**: A string that allows SNMP clients to read and modify the device's information.

3.9 Cloud Platform Management



The Device Cloud Platform supports remote operation and maintenance device parameter configuration, upgrading device firmware, intranet penetration of operation and maintenance sub device firmware, data reports, etc. Configuring devices to the Device cloud platform can facilitate subsequent remote operation of devices. To use the Device Cloud Platform, you need to register a Device Cloud account in advance. Click to go to Device Cloud to register and log in for use. device.fourfaith-cloud.com

Platform

Remote Management ☒

* Platform ☒ Four-Faith Cloud ☐ Private Cloud

* Protocol ☐ V1.0 ☒ V2.0

* Device Code
 FJ4100808409 [Copy](#)

* Device Type Description

* Customized Local Domain

Connection Status

Status ☐ Disabled ☒ Enabled

Connection Status

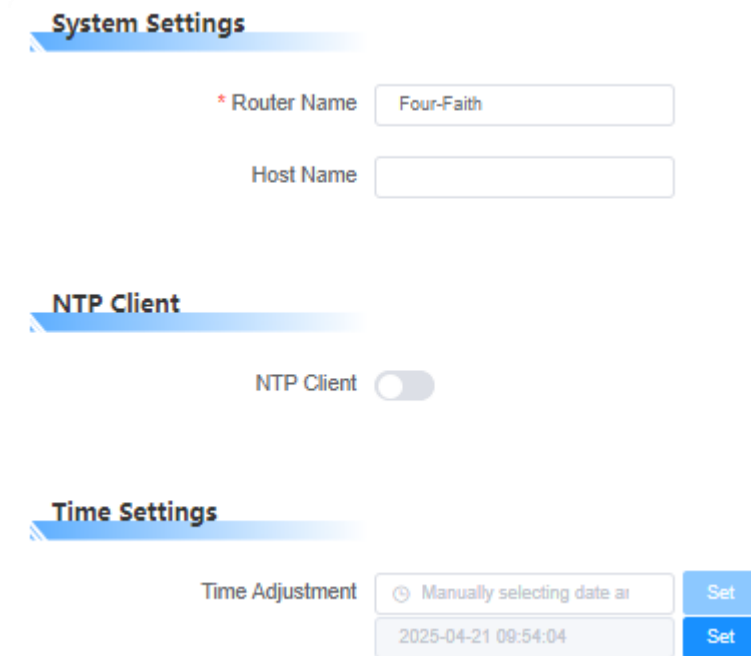
Server Ip And Port

Active Time

During the device initialization page, there will be a prompt for cloud management. If you have an account for the device management platform, you can set the cloud platform address provided by our company. If you have subscribed to a private cloud platform deployment, you can set the corresponding cloud address and port. The device code defaults to the device's SN and is unique.

3.10 System Management

3.10.1 System Settings



System Settings

* Router Name

Host Name

NTP Client

NTP Client ☐

Time Settings

Time Adjustment

- **System Settings:** You can set the gateway name and hostname. These settings have default values, but you can also customize them.
- **NTP Client:** The NTP client is disabled by default. Once enabled, you can set the server address, and the gateway will synchronize time with the NTP server.

NTP Client

NTP Client ☒

* Time Zone

* Summer Time (DST)

Server IP/Name

- **Time Settings:** You can manually adjust the current time of the device.

Time Settings

Time Adjustment

3.10.2 Login Management

This page allows you to change the device's login username and password.

Account Login

Password Setting

* Router Username

* Password

* Re-enter To Confirm

3.10.3 Restore to Factory Defaults

Clicking "Restore Factory Defaults" will reset the device to its factory settings. Please ensure you have saved any necessary parameters before proceeding, as all current configurations will be erased.

Restore Router Settings

This operation resets the settings back to the factory preset values. All your settings will be erased.

3.10.4 Configuration Backup

Backup Config

Backup Config

Back up your current configuration in case you need to reset the router to factory settings in the future.

Recovery Config

Recovery Config

Only backup files of the same model router that use this firmware can be uploaded. Please do not upload any files that were not created through this interface!

- **Backup Configuration:** Click the backup button to download the current device configuration for storage or for importing into another device.
- **Restore Configuration:** You can import a backup file from the same model gateway using the restore button. Note: Do not upload any file not created through this interface!

3.10.5 Firmware Upgrade

Upgrade

* Select upgrade file

Browse

Upgrade

You can upload new firmware to the 5G gateway. If the gateway is functioning properly, upgrading is not necessary unless the new version includes features you require. Click "Browse" to select the firmware file, then click "Upgrade" to begin. The upgrade process takes several minutes.

Note: Upgrading the 5G gateway firmware may reset configuration settings. Please ensure you have backed up your configuration before proceeding. And do not power off the device or press the reset button during this time.