F-G300 5G Smart Light Pole Gateway User Manual	Product Version	Secret Level
	V1.0.1	
	Product Name：F-G300	Total 87 pages

F-G300 5G Smart Light Pole Gateway User Manual

This manual applies to the following models:

Models	Product Categories
F-G300-MP	5G Smart Light Pole Gateway
F-G300-M2	5G Smart Light Pole Gateway
F-G300-4G	4G Smart Light Pole Gateway
F-G300-N	Smart Light Pole Gateway

Xiamen Four-Faith Communication Technology Co., Ltd.

Add: No. 370, Chengyi Street, Phase III, Software Park, Jimei District, Xiamen
11th Floor, Building A06
Customer Hotline: 400-8838-199
Tel: +86-592-6300320
Fax: +86-592-591273
Website: www.four-faith.com

Document Revision History

Date	Version	Remarks	Writer
2020-11-10	V1.0.0	Initial version	XRC/YWC
2021-09-27	V1.0.1	Coprocessor page acquisition part modification	YWC

Copyright Notice

Trademark Notice


F-G300
Intelligent Gateway

Content

1.F-G300 Introduction

1.1 Overview

F-G300 is an IoT wireless smart light pole gateway, which utilizes public 4G/5G network to provide users with wireless long-distance big data transmission function.

This product adopts high-performance industrial-grade 32-bit communication processor and industrial-grade wireless module, and uses an embedded real-time operating system as a software support platform. It also provides 1 AC input, 3 AC outputs, 2 DC outputs, and 3 SFPs. , 7 Gigabit Ethernet LANs (4 of which support POE+), 1 Gigabit Ethernet WAN, 4 RS485 and 1 RS232, 2 ADC acquisitions, 4 DI, 4 DO and WIFI interfaces, which can be connected at the same time Connect multiple serial devices, multiple Ethernet devices and WIFI devices.

5G smart light pole gateway F-G300 is a smart gateway specially developed for 5G smart light poles, ubiquitous power Internet of Things and other scenarios. It has powerful device access capabilities, communication protocol conversion, and computing processing capabilities. The gateway can be connected to devices with functions such as intelligent lighting, video surveillance, traffic indication, traffic monitoring, environment, weather monitoring, information release, public broadcasting, public WLAN, emergency assistance, information interaction, charging services, etc., through wired, optical fiber, 4G, 5G communication.

The product has been widely used in various types of light poles in smart cities, municipalities, highways, characteristic towns, scenic spots, parks and other occasions.

1.2 Product Features

Industrial-grade Design

- Adopt high-performance industrial grade wireless module
- High-performance industrial-grade 32-bit communication processor
- The metal shell is adopted, and the protection level is IP30. Metal housing and system safety isolation, especially suitable for harsh environments

Stability & Reliability

- WDT watchdog design to ensure system stability
- Adopt a complete anti-drop mechanism to ensure that the data terminal is always online
- Ethernet interface built-in 1.5KV electromagnetic isolation protection
- RS232/RS485 interface power and data isolation, in line with CSA, UL and IEC standards
- SIM/UIM card interface built-in 15KV ESD protection
- Power interface built-in reverse phase protection and overvoltage protection

- Lightning protection of antenna interface (optional)

Standard & Convenience

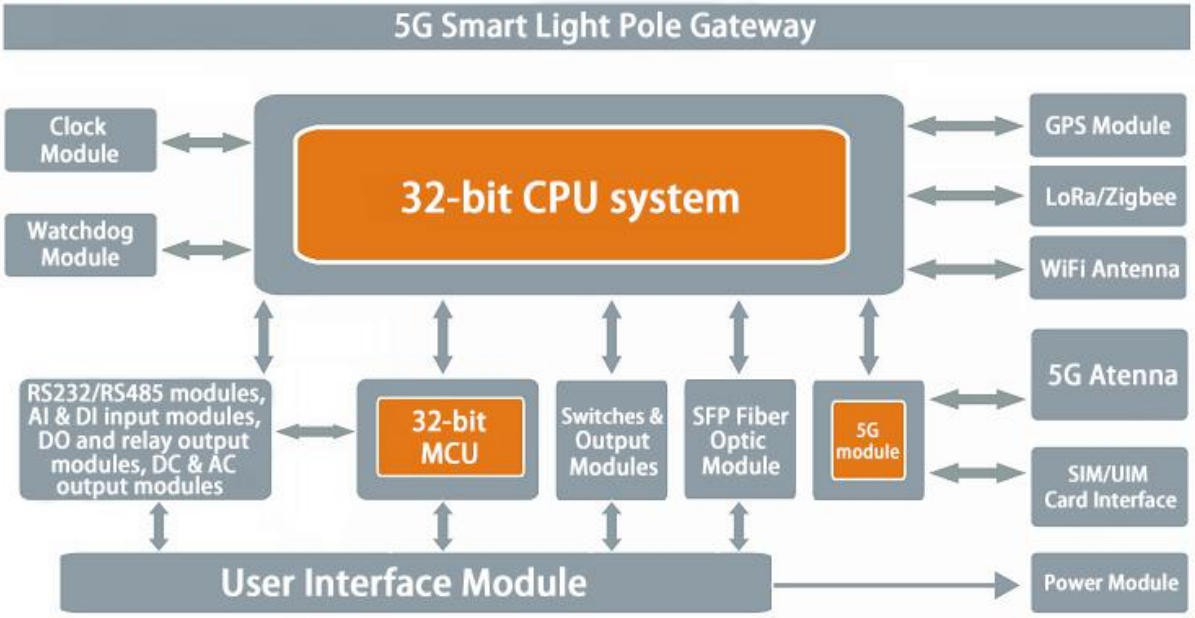
- Provide standard RS232, RS485, Ethernet and WIFI interfaces, which can directly connect serial devices, Ethernet devices and WIFI devices
- Provides standard wired WAN port (supports standard PPPOE protocol), which can be directly connected to ADSL equipment
- Intelligent data terminal, it can enter the data transmission state after power-on
- Convenient system configuration and maintenance interface (including local and remote WEB mode or CLI mode)
- Supports rail or wall mounting

High Performance

- Support multiple WAN connection methods, including static IP, DHCP, PPPOE, 3G/UMTS/4G/LTE, dhcp-4G, 5G-NR
- Support 4G/5G and wired WAN dual-link intelligent switching backup function (optional)
- Support VPN client (PPTP, L2TP, IPSEC) (Note: Only VPN version supports)
- Support VPN sever (PPTP, L2TP, IPSEC) (Note: Only VPN version supports)
- Support remote management, SYSLOG, SNMP, TELNET, SSHD, HTTPS
- Support local and remote online upgrade, import and export configuration files
- Support NTP, built-in RTC
- Support a variety of DDNS at home and abroad
- Support VLAN, MAC address cloning, PPPoE server
- WIFI supports 802.11b/g/n/ac, supports WIFI AP, AP Client, repeater, repeater bridge and other working modes (optional)
- WIFI supports WEP, WPA, WPA2 and other encryption methods, MAC address filtering
- Support a variety of online and offline trigger modes, including SMS, phone ringing, serial port data, network data trigger online and offline modes
- Support APN/VPDN
- Support multi-channel DHCP server and DHCP client, DHCP binding MAC address, DDNS, firewall, NAT, DMZ host, QoS, traffic statistics, real-time display of data transmission rate
- Support TCP/IP, UDP, FTP (optional), HTTP and other network protocols
- Support SPI firewall, VPN traversal, access control, URL filtering

1.3 Working Principle Block Diagram

The block diagram of the 5G smart light pole gateway is as follows:



1.4 Product Specifications

Wireless Specification

Items	Contents
Module	Industrial-grade wireless module
Standard	5G NR: n1/n2/n3/n5/n7/n8/n20/n28/n41/n66/n71/n77/n78/n79 LTE: B1/B2/B3/B4(66)/B5(18/19/26)/B7/B8/B12(17)/B13/B14/B20/B25/B26/B28/B29/B30/B38/B39 /B40/B41/B42/B43/B46/B48/B71 P.S.:Choose different modules according to user needs, can support different network standards
Theoretical Bandwidth	5G NR: Downlink rate 3.4Gbps, uplink rate 350Mbps LTE Cat20: Downlink rate 2.0Gbps, uplink rate 150Mbps HSPA+: Downlink rate 42Mpbs, uplink rate 5.76 Mbps
TX	<23dBm
RX	<-107dBm

WIFI Specification

Items	Contents
Standard	Support IEEE802.11b/g/n, 2.4G, 2*2 MIMO, support AP mode, Station mode (optional) Support IEEE802.11ac, 5.8G, 2*2 MIMO, support AP mode, Station mode

	(optional)
Bandwidth	IEEE802.11b/g: The highest rate is 108Mbps IEEE802.11n: The highest speed is up to 300Mbps IEEE802.11ac: Maximum speed up to 780Mbps
Encryption	Support WEP, WPA, WPA2 and other encryption methods, optional WPS function
Power	26dBm（11b），21.5dBm（11g），20dBm（11n），16dBm（11ac）
Sensitivity	<-72dBm@54Mpbs

Hardware System

Items	Contents
CPU	Industrial-grade 32-bit communications processor
FLASH	32MB
DDR3	512MB
TF	8GB/32GB, optional

Interfaces

Items	Contents
AC Input	1 channel 85~264V/35A
AC Output	3 channels of 85~264V/10A, providing 220V output power supply to the corresponding equipment; remote control switch, voltage and current detection, single channel allows the maximum current to pass 10A, default closed
DC Output	1 channel 12V/2A, can realize remote switch and current detection, default on
	1 channel 24V/2A, can realize remote switch and current detection, default on
SFP Optical Port	3-way SFP optical interface, 10/100/1000M SFP slot, support single-mode, multi-mode fiber, support ring network management, ring, chain and other network topologies
WAN Interfaces	1 10/100/1000M Ethernet port (RJ45 socket), adaptive MDI/MDIX, built-in 1.5KV electromagnetic isolation protection, WAN/LAN reusable
LAN Interfaces	7 10/100/1000M Ethernet ports (RJ45 socket), adaptive MDI/MDIX, built-in 1.5KV electromagnetic isolation protection, Among them, 4 channels of POE, support POE+ single channel power up to 30W
Serial Port	4 RS485 serial ports, built-in 15KV ESD protection, serial port parameters are as follows: Data bits: 5, 6, 7, 8 bits Stop bits: 1, 1.5 (optional), 2 bits Check: no check, even check, odd check, SPACE (optional) and MARK check (optional) Serial port rate: 2400~115200bits/s

Indicator Light	With "Power", "System", "Online", "Signal" and other indicators
DI	4 DIs Input high level: 5 to 30 VDC Input Low: 0 to 3 VDC
DO	2 switch output D0, load current: < 50mA @ 30VDC
Relay	2 passive relay control outputs, relay load: 5A 250VAC/30VDC
AI	2 ADC interfaces of 4~20mA
GPS	1 GPS/Beidou (optional)
Antenna Interface	Cellular: 4 standard SMA female antenna ports, characteristic impedance 50 ohms WIFI: 2 standard SMA male antenna ports, characteristic impedance 50 ohms GPS: 1 standard SMA female antenna interface, characteristic impedance 50 ohms (optional) LoRa/ZigBee: 1 standard SMA female antenna interface, characteristic impedance 50 ohms (optional)
SIM/UIM Card Interface	2 standard drawer user card interfaces, support 1.8V/3V SIM/UIM card, built-in 15KV ESD protection P.S.: Compatible with eSIM
TF Card Interface	1 standard pop-up TF card interface, support various TF cards
Reset Reset Button	Through this button, the parameter configuration can be restored to the factory value

Power Supply

Items	Contents
AC Power Supply	AC 85~264/35A(max)
Working Current	0.15~0.25A (all output ports are unloaded)
Stand-by Current	0.1A (all output ports are unloaded)

Physical Properties

Items	Contents
Shell	Metal shell, protection class IP30
Size	215*134.7*70.2mm (excluding antenna and mounting parts)
Weight	1.8kg(excluding antenna and mounting parts)

Others

Items	Contents

Operating Temperature	-35~+75ºC(-31~+167℉)
Storage Temperature	-40~+85ºC(-40~+185℉)
Relative Humidity	95%(No condensation)

2.Installation

2.1 Overview

The 5G smart light pole gateway 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.

➢ Note:
Please do not install the equipment with electricity.

2.2 Packing List

Please keep the packing material when you unpack it in case you need to transfer it in the future. The list is as follows:

✧ 5G smart light pole gateway host 1 set
✧ 4 5G wireless cellular antennas (SMA male)
✧ WIFI antenna (SMA female) 2
✧ Matching AC power input cable 1
✧ Matching AC power output cable 3
✧ 1 Ethernet direct connection
✧ 4 7P terminals
✧ 4 2P terminals
✧ Warranty card

2.3 Installation and Cable Connection

Size：

The size is as shown below. (unit: mm)

5G Smart Light Pole Gateway Appearance

Antenna installation:

The 5G cellular antenna interface is an SMA female socket (identified as "ANT-1", "ANT-2", "ANT-3", "ANT-4"), and screw the supporting 5G cellular antenna to the antenna interface, And make sure to tighten it so as not to affect the signal quality.

The WiFi antenna interface is an SMA male socket (identified as "WIFI1", "WIFI2"), screw the supporting WiFi antenna to the antenna interface, and make sure to screw it tightly so as not to affect the signal quality.

SIM card installation:

When installing or taking out the SIM card, gently press the eject button (yellow dot) with a pointed object, and the SIM card sleeve can be ejected. Put the SIM card into the card sleeve first, and make sure that the metal contact surface of the SIM card is facing outward, then insert the SIM card sleeve into the drawer, and make sure that it is inserted in place. Note that the SIM1 card is facing up and the SIM2 card is facing down.

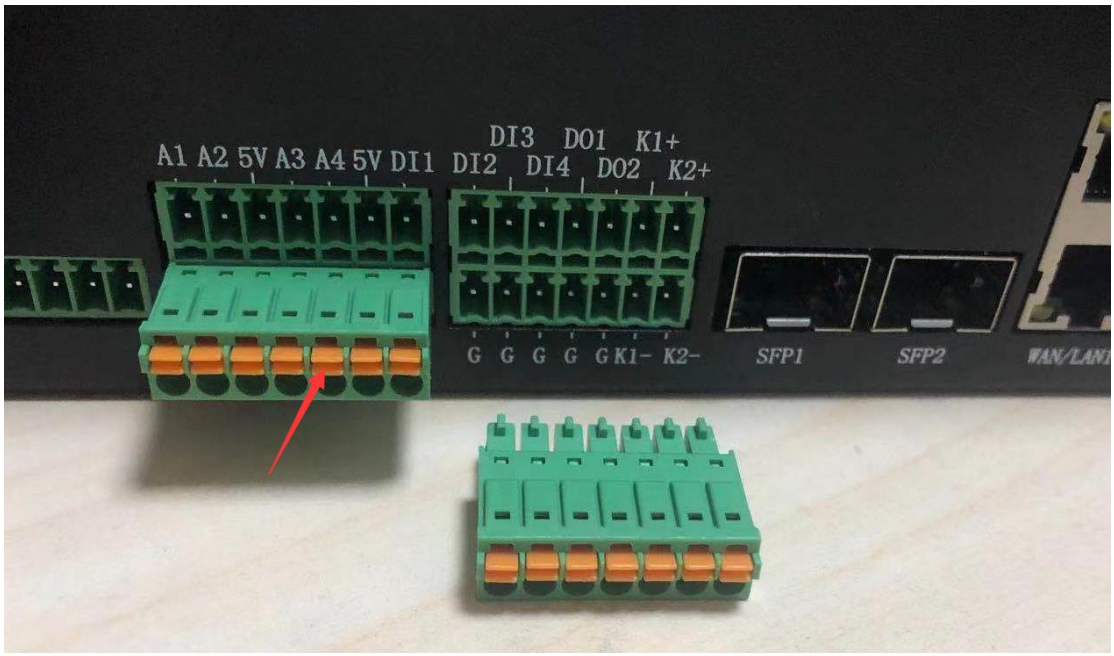
Connect the network cable:

Plug one end of the direct network cable into any port of the Local Network of the device, and the other end into the Ethernet port of the user equipment. The network direct connection signal connection is as follows:

RJ45-1	RJ45-2	Line 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

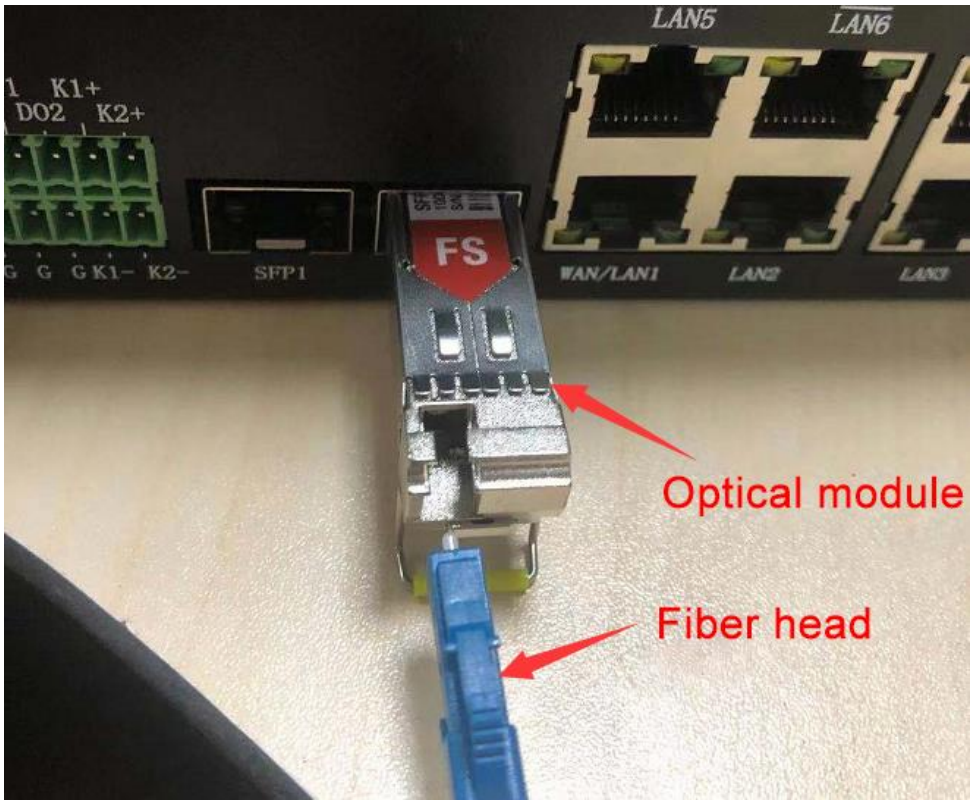
Connection terminal: (7Pin terminal is required)

Insert the 7Pin terminal into the corresponding interface, press the yellow switch firmly to insert the bare wire into the terminal, and connect the required signal. As shown below:



Connecting the optical fiber interface: (requires an optical module)

Insert the optical module and the optical fiber head into the SFP optical fiber interface respectively. As shown below:



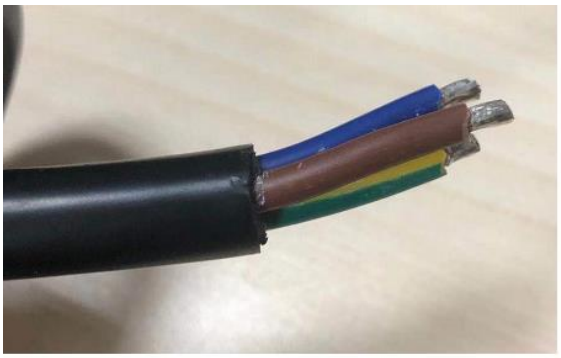
To connect the AC input cable and the AC output cable:

To connect the matching AC input cable and AC output cable to the corresponding port, you need to open the protective cover first, align the cable end with the port on the panel (the ports have a foolproof design), and then screw it tightly. As shown below:

Note:

The core of the input line (thick) is defined as: blue-brown L-N, yellow-green PE.

The core of the output line (thin) is defined as: red-black L-N, yellow PE



2.4 Power Supply

5G smart light pole gateways are usually used in complex external environments. In order to adapt to the complex application environment and improve the working stability of the system, the equipment adopts advanced power technology. Users can use the standard 220V power supply to power the device.

2.5 Indicator Light

The device provides the following indicators: "Power", "System", "Online", "Signal". The status of each indicator light is described in the following table:

Indicator Light	State	Remarks
Power	On	The device power is OK
	Off	The device is not powered on/is in the shutdown period of the timer switch function
System	Blinking	The system is running normally
	Off	The system is abnormal
Online	On	The device is logged into the network
	Off	The device is not logged into the network
Signal	Not on	No signal coverage
	Blinking slowly	Weak signal strength (less than -90dbm)
	Blinking fast	Moderate signal strength (-70dbm~-90dbm)
	Always on	Excellent signal strength (greater than -70dbm)

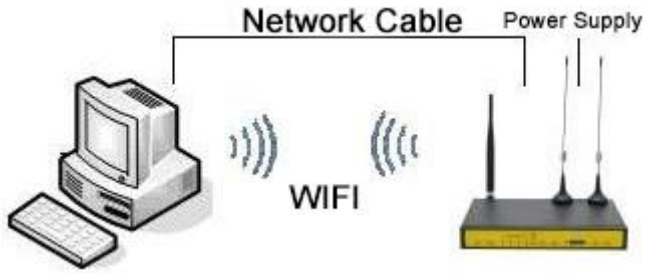
2.6 Reset Button

The device has a reset button, identified as "Reset". The function of this button is to restore the parameter configuration of the device to the factory value. The method is as follows: insert a pointed object into the "Reset" hole, and gently press and hold the reset button for about 15 seconds, then release, at this time, the device will automatically restore the parameter configuration to the factory value, and after about 10 seconds , the device restarts automatically (the phenomenon of automatic restart is as follows: the "System" indicator goes off for about 10 seconds, and then works normally again).

3.Parameter Configuration

3.1 Configuration Connection Diagram

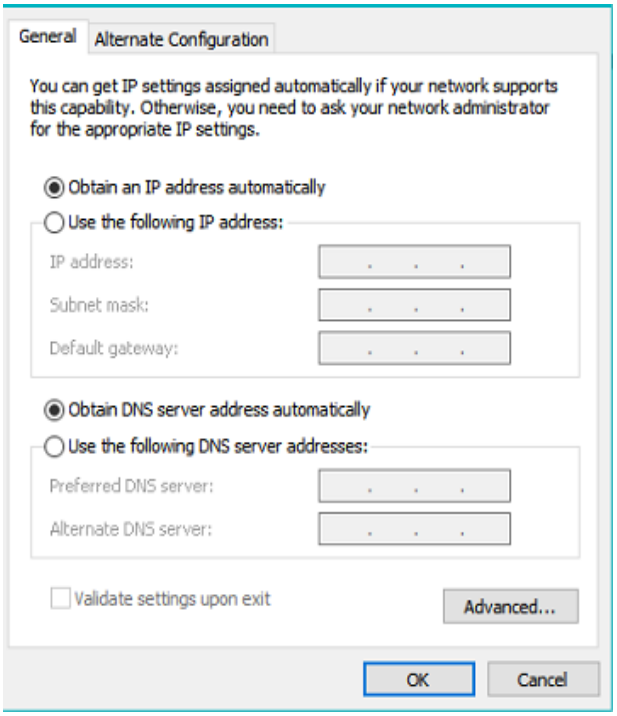
Before configuring the router, you need to connect the router and the PC used for configuration through the factory-configured network cable or WIFI. When connecting with a network cable, one end of the network cable is connected to any Ethernet port of the router's "Local Network" (hereinafter referred to as the LAN port), and the other end is connected to the Ethernet port of the PC. When connected by WIFI, the default SSID of the router is "FOUR-FAITH", and no password verification is required.



3.2 Login to the Configuration Page

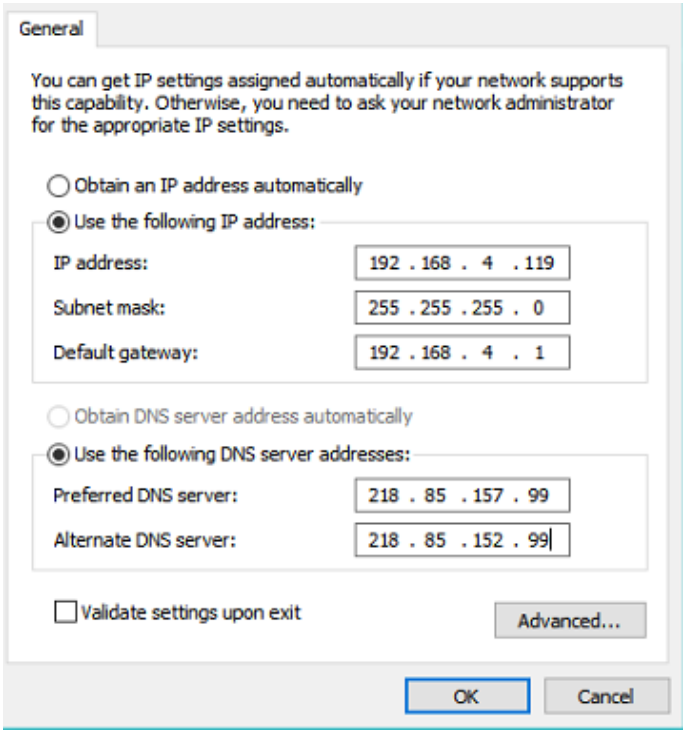
3.2.1 PC IP Address Setting (two ways)

The first way: get an IP address automatically



The second way: specify the IP address

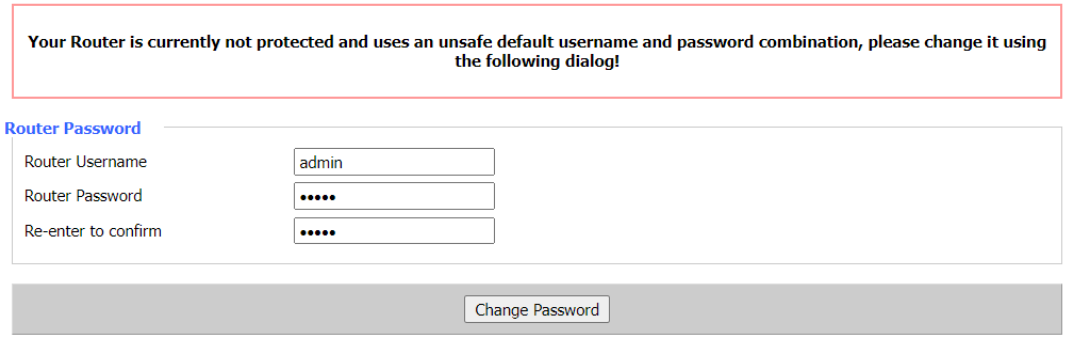
Set the IP address of the PC to 192.168.4.9 (or another IP address of the 192.168.4 network segment), the subnet mask to 255.255.255.0, and the default gateway to 192.168.4.1. DNS is set to a locally available DNS server.



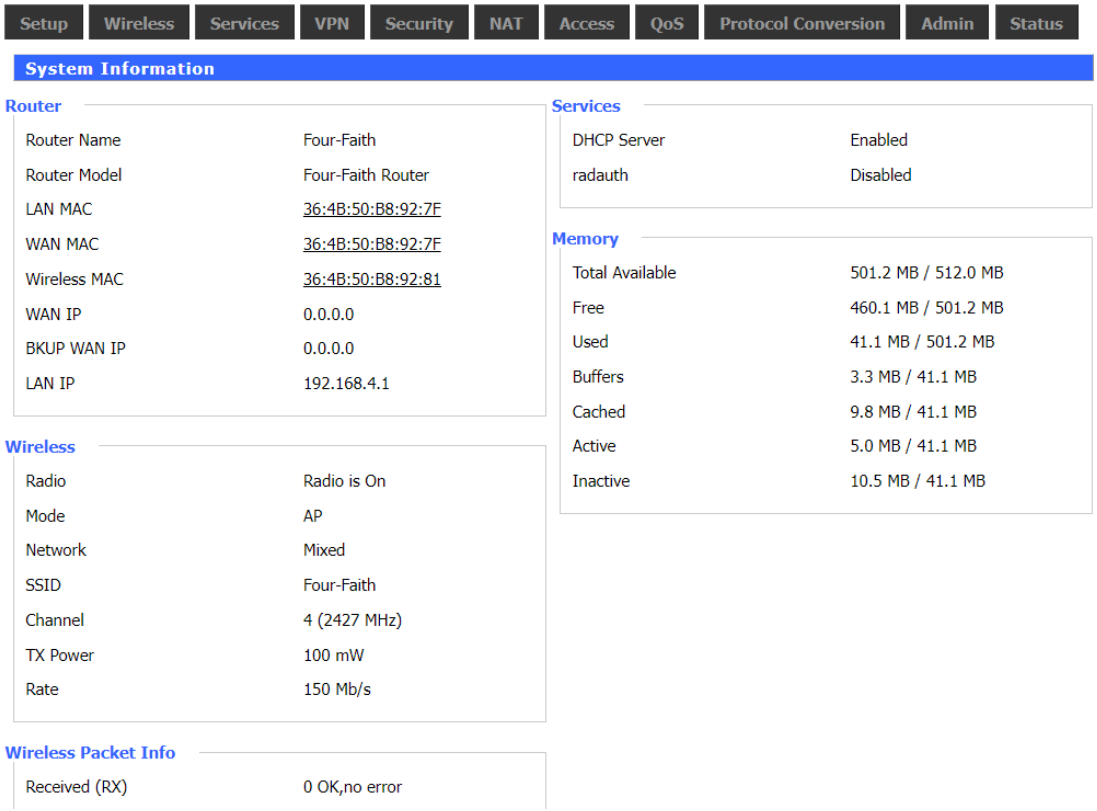
3.2.2 Login

This chapter describes the main functions of each page. The web tools can be accessed through a web browser using a computer connected to the router. There are eleven main pages, namely: Settings, Wireless, Services, VPN, Security, Access Restrictions, NAT, QoS Settings, Applications, Administration, and Status. Click on one of the master pages and more slave pages will appear.

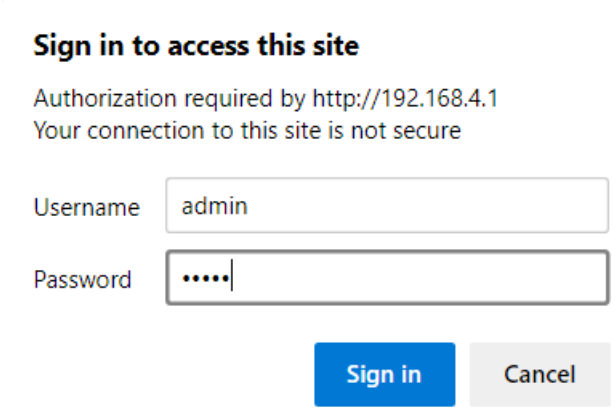
To access the router's web-based web management tool, launch IE or other browser and enter the router's default IP address of 192.168.4.1 in the "Address" field. Press Enter. If you log in to the web page for the first time, you can see the page shown below, prompting the user whether to modify the default user name and password of the router. If you need to enter the user-defined user name and password, click the "Change Password" button to take effect.



Then you can go to the main information page:



If you click the main menu for the first time, you need to enter the corresponding user name and password:



Enter the correct user and password to access the corresponding menu page. The default user name is admin, and the default password is admin. (Username and password can be changed on the admin page). Then click "OK".

3.3 Management and Configuration

3.3.1 Setup

The first page opened by clicking "Settings" is the basic settings. From this page, you can follow the prompts to make changes to the basic settings, click the "Apply Settings" button to make changes but not take effect, click the "Apply" button to make the changes effective, or click the "Cancel Changes" button to cancel Change.

3.3.1.1 Basic Settings

The WAN Connection Type settings section describes how to configure the router to connect to the Internet. Details on this can be obtained from your ISP.

WAN Connection Type

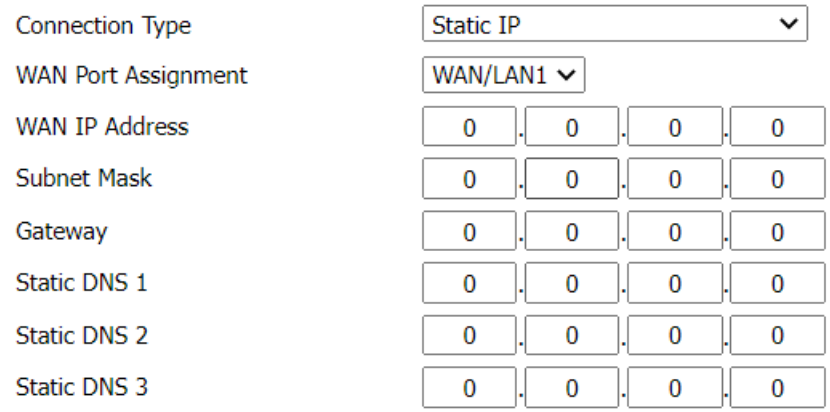
Select the type of Internet connection your ISP provides you from the drop-down menu, WAN connection type includes 7 ways: Disabled, Static IP, Automatic Configuration - DHCP, PPPOE, 3G Link, DHCP-4G/5G.

Method 1: Disabled

Disable the connection type setting of the WAN port

Method 2: Static IP

Dedicated line access, such as business fiber, typically uses this connection type. The broadband service provider will provide you with detailed parameters such as IP address, subnet mask, gateway and DNS, which you need to set on the router.



WAN IP address: The IP address set by users according to their own or ISP allocation.

Subnet Mask: The subnet mask set by users according to their own or ISP distribution.

Gateway: The gateway set by users according to their own or ISP distribution.

Static DNS (1-3): Static DNS set by users according to their own or ISP distribution.

Method 3: Automatic Configuration - DHCP

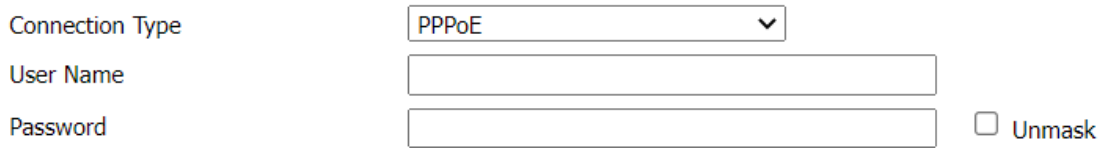
The router's default WAN connection type. Cable TV and some residential broadband use

this connection method. Such as Shenzhen Tianwei Video, Shanghai Cable Communication and so on.

The IP address of the WAN port is obtained by DHCP.

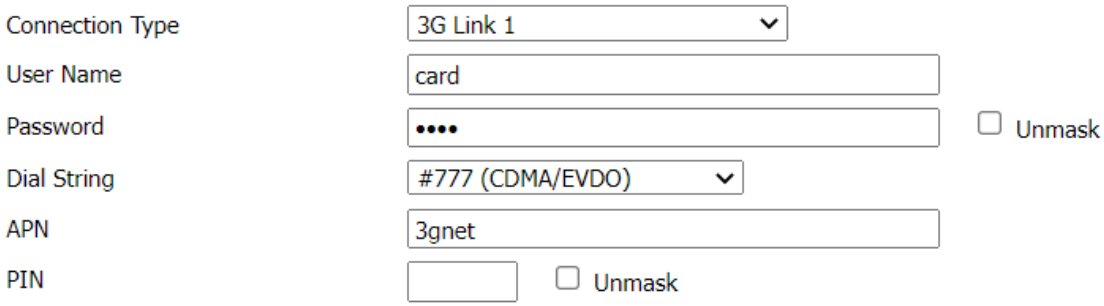
Method 4: PPPOE

This connection type is commonly used by China Telecom and China Netcom ADSL broadband services, but also by some other broadband service providers. The PPPoE connection type requires the ISP to provide you with a username, password and service name, which need to be set up on the router.



User name: Username for logging on to the Internet.
Password: The password used to log in to the Internet.

Method 5:3G Link



User name: Username for logging on to the Internet.
Password: The password used to log in to the Internet.
Dial String: The calling number to call to the operator.
APN: Access point name.
PIN: The PIN code provided by the SIM card.

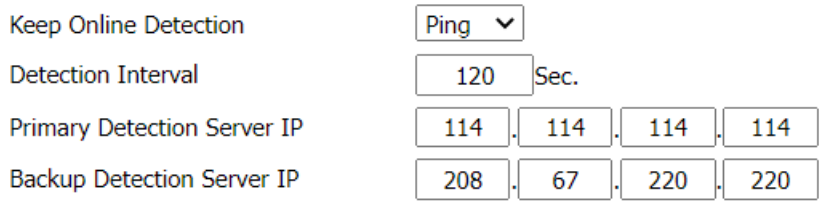
Network Type

Connection type: Including automatic mode, forced to 3G, forced to 2G, 3G first, 2G first, etc. If 4G module is used, 4G network options will be added accordingly, according to user needs and different module types to choose.

Method 6:DHCP-4G/5G

The IP address of the WAN port is obtained by DHCP-4G/5G

Keep Online



The keep-alive function is used to detect whether the Internet link is in a valid state. If this item is set, the router will automatically detect the Internet link. Once it detects that the link is disconnected or invalid, the system will automatically reconnect and re-establish a valid link. If the network environment is relatively poor, or in the case of a private network, it is recommended to use the Router mode.

Keep Online Detection:

None: Do not use the online hold function.

Ping: Send ping packets to check the link. If it is set to this mode, the configuration items of "Online Keeping Detection Time Interval", "Online Keeping Checking Primary Server IP" and "Online Keeping Checking Secondary Server IP" must also be configured correctly.

Route: Use the route method to detect the link. If this method is set, you must also correctly configure the "Online maintenance detection interval", "Online maintenance detection main server IP" and "Online maintenance detection secondary server IP" configuration items.

TCP: Use TCP mode to detect the link. If this mode is set, the configuration item "Online Keeping Detection Time Interval" must also be correctly configured.

Detection Interval:

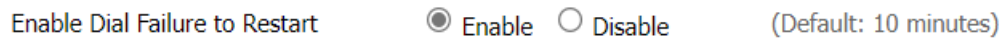
The time interval between two online hold detections, in seconds.

Primary Detection Server IP:

The IP address of the primary server that responds to router online detection packets. This configuration item is valid only when "Preservation Mode" is set to "Ping" or "Route".

Backup Detection Server IP:

The IP address of the secondary server that responds to router online detection packets. This configuration item is valid only when "Preservation Mode" is set to "Ping" or "Route".

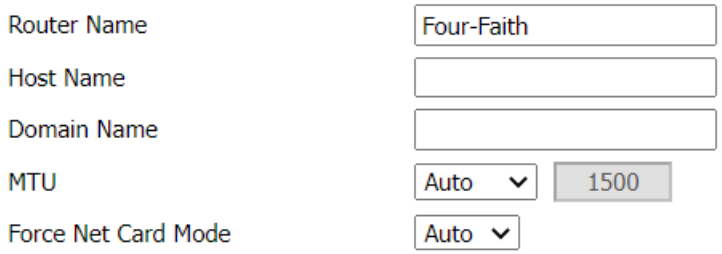


Enable Dial Failure to Restart: This function can reconnect to the Internet when the router fails to dial. (Default: 10 minutes)

STP

STP stands for spanning Tree Protocol. The protocol can be applied to the loop network to realize path redundancy through certain algorithms, and at the same time, the loop network is pruned into a loop-free tree network, so as to avoid packet proliferation and infinite loop in the loop network.

Optional Settings



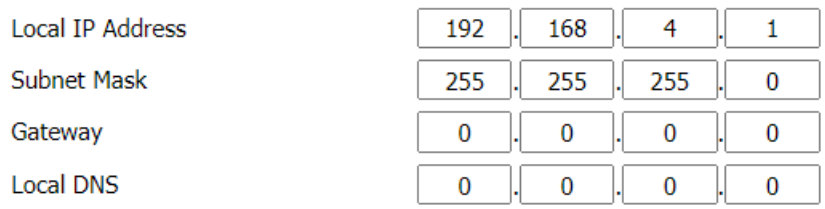
Router Name: In this field, you can enter a name of up to 39 characters that represents the router.

Hostname and Domain Name: These options can be used to provide a hostname and domain name. Some ISPs (usually fixed network ISPs) require these names for identification. You'll want to check with your ISP to see if your broadband internet service has a hostname and domain name configured. In most cases, leaving this information blank is fine.

MTU: MTU refers to the maximum transmission unit. The MTU setting specifies the maximum packet size allowed in Internet transmission. The default state is "Auto", and the maximum packet value that will be transmitted can be manually entered. The recommended range for this value is 1200 to 1500. For most DSL users, 1492 is recommended. You should make this number in the range of 1200 to 1500. Select the Automatic option if you want the router to be able to choose the best MTU for your internet.

Network Setup

The Network Settings section allows you to modify the network settings connected to the router's Ethernet port.



Local IP Address: Indicates the router IP address that can be seen by your local area

network.

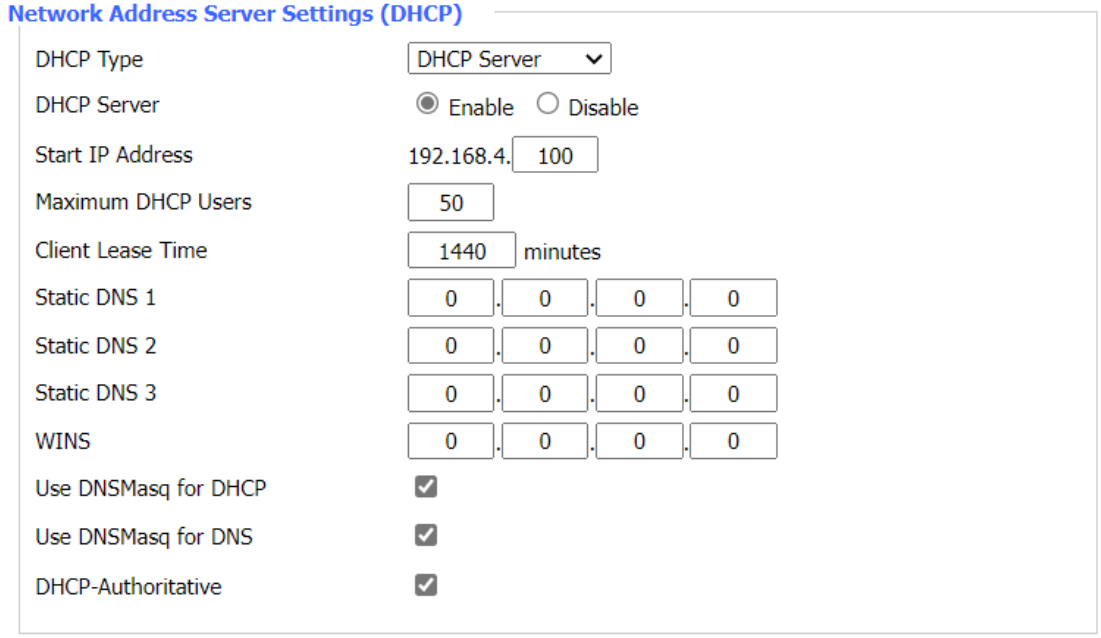
Subnet Mask: Indicates the router IP address subnet mask as seen by your LAN.

Gateway: Set the internal gateway of the router. If it is set by default, the internal gateway is the address of the router itself.

Local DNS: The DNS server is automatically assigned by the operator access server. If you have your own DNS server or other stable and reliable DNS servers, you can choose to use these reliable DNS servers. Otherwise, the default setting

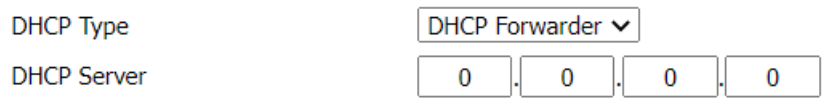
Network Address Server Settings (DHCP)

These settings are used to configure the router's Dynamic Host Configuration Protocol (DHCP) server function. The router can act as a DHCP server for the network. A DHCP server automatically assigns an IP address to every computer on the network. If you choose to enable the router's DHCP server option, you can set all computers on the LAN to automatically obtain IP addresses and DNS, and ensure that there are no other DHCP servers on the network.



DHCP Type: Including DHCP server and DHCP forwarder

If set to DHCP forwarder, enter the DHCP server address, as follows



DHCP Server: DHCP is enabled by default at the factory. Click Disable if there is already a DHCP server on the network, or if you do not wish to have a DHCP server. If you choose DHCP forwarder, fill in the corresponding DHCP server IP.

Start IP Address: Enter a value in the range 1-254 to use as the starting value when the DHCP server assigns an IP address. Since the default IP address of this router is 192.168.4.1, the starting IP address must be 192.168.4.2 or greater but less than

192.168.4.254. The default starting IP address is 192.168.4.100.

Maximum DHCP Users: Enter the maximum number of computers you want the DHCP server to assign IP addresses to. This number cannot exceed 253, and the starting IP address plus the number of users cannot exceed 255. The default value is 50.

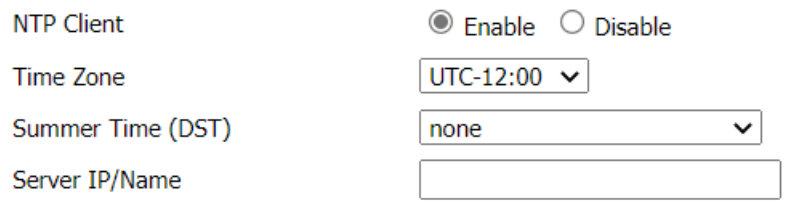
Client Lease Time: refers to the lease period of the IP address occupied by the network user of the dynamic IP address. Enter the time in minutes that this user "leases" this dynamic IP address. After the dynamic IP address expires, a new dynamic IP address is automatically assigned to the user. The default setting is 1440 minutes, which represents 1 day. The setting range is 0-99999.

Static DNS (1-3): The Domain Name System (DNS) is used by the Internet to translate domain names or web page names into Internet addresses or URLs (Universal Resource Locators). Your ISP will give you the IP address of at least one DNS server. You can enter up to three DNS server IP addresses. By using these addresses, quick access to a working DNS server can be achieved.

WINS: The Windows Internet Naming Service (WINS) manages every computer that interacts with the Internet. If using a WINS server, enter the server's IP address here. Otherwise, do not fill in any address.

DNSMasq: Add your domain name to the local search field, add extended host options, use DNSMasq to assign IP addresses and DNS to the subnet, if you do not select DNSMasq, use the dhcpd service to provide IP addresses and DNS for the subnet.

Time Settings



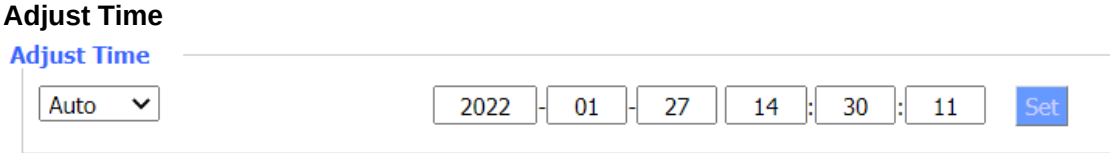
NTP Client: Enable and disable to provide a time synchronization function for the system, that is, to set the system time.

Time Zone: West 12th to East 12th, set by your own location.

Summer Time(DST): Set according to your location.

Server IP/Name: IP address of your NTP server, up to 32 characters, if not, the system will find the server by default.

Adjust Time



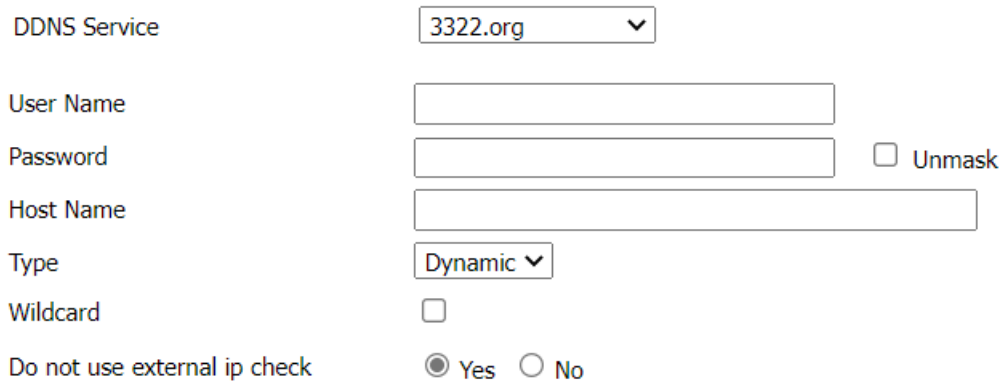
Adjust the time for the system, refresh to get the current time of the web page, and set it to modify the system time. The function of system time calibration, especially when the NTP service cannot be obtained, you can manually adjust the system time.

After making changes, click the **"Save"** button to make the changes but not take effect, click the **"Apply Settings"** button to make the changes effective, or click the **"Cancel Changes"** button to cancel the changes. Help information is located on the right side of the screen.

3.3.1.2 DDNS

If the IP address obtained by the router's Internet access is dynamically assigned by the operator, the IP address obtained by the router may be different each time. In this case, dynamic domain name service can be used. The domain name provider allows you to register a domain name that always corresponds to the current dynamic IP address of the router. In this way, you can access the latest Internet IP address of the router by accessing the domain name.

DDNS Service: This router supports a variety of DDNS servers, such as: DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP. You can also define your own.



User Name: Username registered on the DDNS server, with a maximum length of 64 characters.

Password: The password entered by the user when registering the user name on the DDNS server, the maximum length is 32 characters.

Host Name: The hostname applied by the user on the DDNS server, the current input length is not limited.

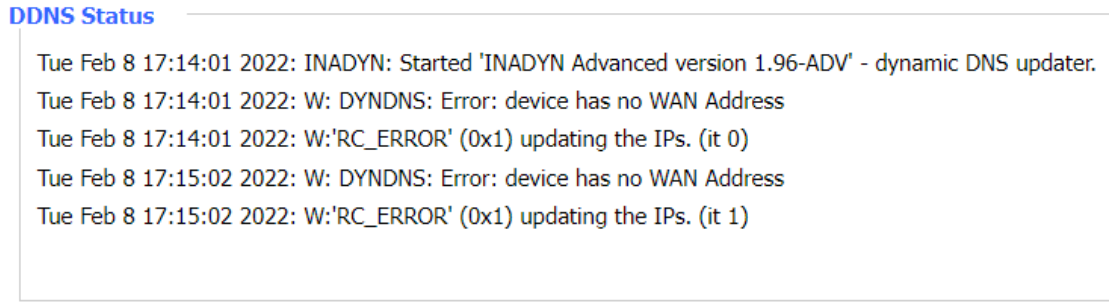
Type: different servers are different.

Wildcard: Whether to support wildcard, the default is OFF. ON means *.host.3322.org is equivalent to host.3322.org.

Do not use external ip check: Enable or disable Do not use external IP detection.

Force Update Interval: unit day, in the set number of days, it is forced to update the dynamic DNS to the server

Status



The status shows the status of the current connection, the information that is already in the process of connecting.

After making changes, click the **"Save"** button to make the changes but not take effect, click the **"Apply Settings"** button to make the changes effective, or click the **"Cancel Changes"** button to cancel the changes. Help information is located on the right side of the screen.

3.3.1.3 MAC Address Cloning

Some ISPs may require you to register your MAC address. If you don't want to re-register your MAC address, you can clone the router's MAC address to the one you registered with your ISP.

Mac address clone can clone 3 parts, one is the clone of the LAN port, the other is the clone of the WAN port, and the other is the clone of the wireless MAC address. There are two points to note. First, the MAC address is 48 bits and cannot be set to The address of the multicast, i.e. the first byte should be an even number. Second, since the wireless and LAN ports are connected by a bridge br0, the MAC address of the bridge br0 is determined by the smaller value of the LAN MAC address and the wireless MAC address.

3.3.1.4 Advanced Routing

On the Advanced Routing page, run mode and static routing can be set. Gateway mode is recommended for most users.

Main Mode: Select the correct running mode. If the router shares an Internet broadband connection, keep the default gateway setting (gateway mode is recommended for most users). Select Router if you want to use only the router's routing functions on the network.

Dynamic Routing

This feature is not available in gateway mode. The dynamic routing feature enables routers to automatically adjust to physical changes in the network layout and to exchange routing tables with other routers. Routers determine the route of network packets based on the minimum number of hops between source and destination.

To enable dynamic routing on the WAN side, select WAN. To enable this feature on the LAN and wireless side, select LAN&WLAN. To enable this feature for both WAN and LAN, select Both. To disable dynamic routing for all data transfers, keep the default setting Disabled.

Static Routing

To set up a static route between the router and another network, select a number from the Static Route drop-down list to set it up. (A static route is a predetermined path through which network information must travel to a specific host or network).

Select Set Number: 1-50 static routes.

Route Name: User-defined routing name, up to 25 characters can be entered.

Metric: The unit of measure for the route between the source address and the destination address. Range 0-9999

Destination LAN NET: The destination IP address is the address of the destination

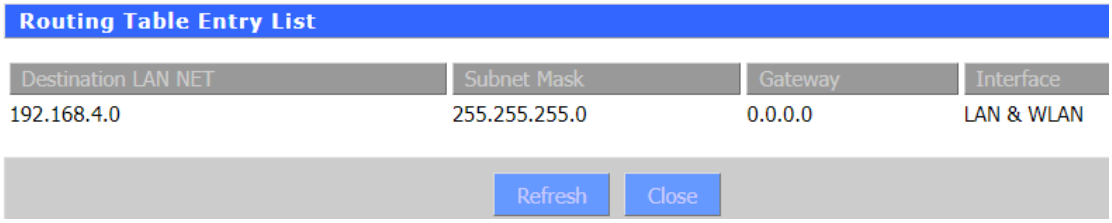
network or host for the static route.

Subnet Mask: The subnet mask determines which part of the destination IP address is the network part and which part is the host part.

Gateway: This is the IP address of the gateway device that allows communication between the router and the destination network or host.

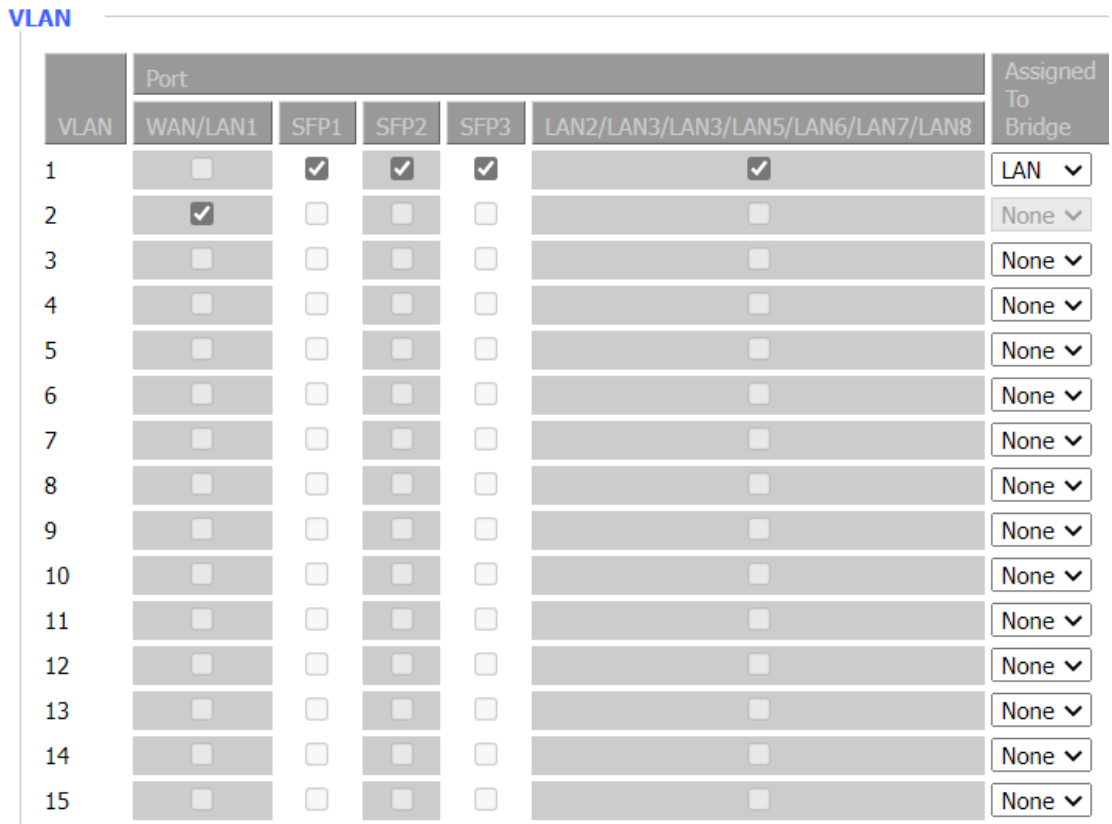
Interface: According to the location of the target IP address, several ports such as LAN and wireless or WAN (Internet) can be selected.

To delete the static route that has been set, please select the corresponding routing table number and click the **"Delete"** button. To view the detailed routing information of the current router, click the **"Show Routing Table"** button.



After making changes, click the **"Save"** button to make the changes but not take effect, click the **"Apply Settings"** button to make the changes effective, or click the **"Cancel Changes"** button to cancel the changes. Help information is located on the right side of the screen.

3.3.1.5 VLANs



The VLANs function can be divided into different VLAN ports according to the user's own wishes. The system supports 15 VLAN ports of VLAN1-VLAN15, but only 5 ports are used at the same time, including one WAN port and 4 LAN ports. The ports are divided according to your own needs, and the LAN port and the WAN port cannot be divided into the same VLAN port.

3.3.1.6 Networking

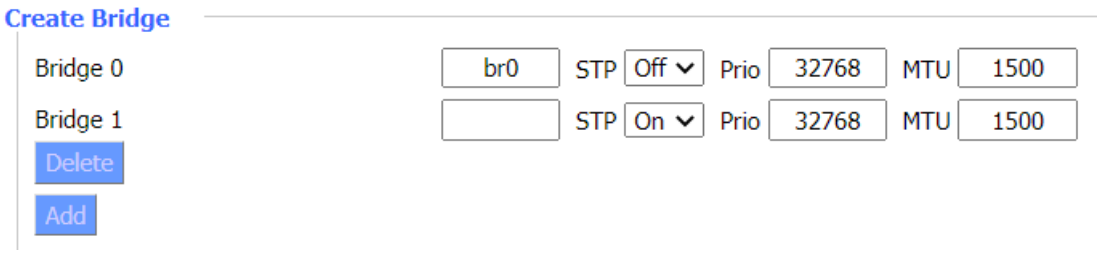
Create Bridge: Create a new bridge for use. STP stands for Spanning Tree Protocol, and you can set bridge priorities. The lowest number has the highest priority.

Assign to Bridge: Allows you to assign any valid interface to an already established bridge.

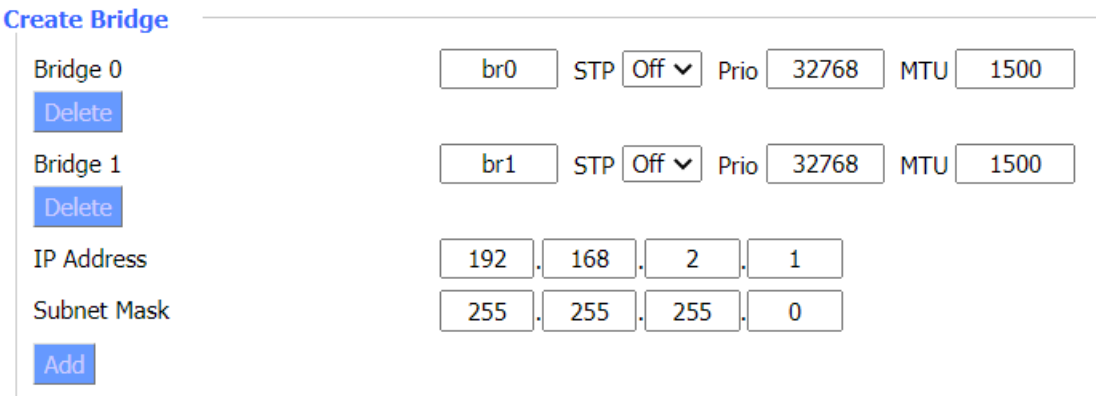
Current Bridging Table: Displays the current bridge list.

The steps to create are as follows:

In creating a bridge, click the **"Add"** button first, and then the following configuration appears:

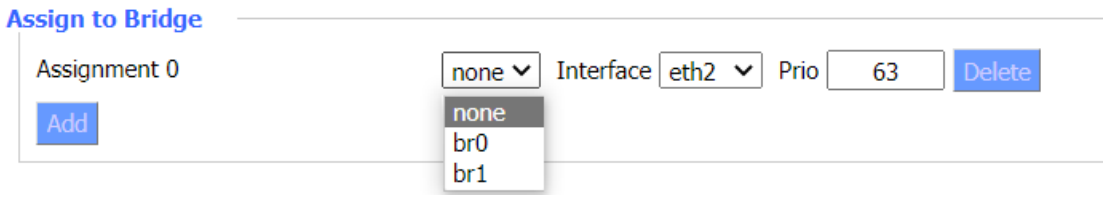


This item is an option for creating a bridge. The first br0 represents the name of the bridge, STP represents whether the spanning tree protocol is enabled, Prio represents the priority level of the spanning tree protocol, the smaller the number, the higher the level, and the MTU represents the maximum transmission unit. The default is 1500. If you don't need it, delete it, and then click **"Save"** or **"Apply settings"**, and the bridge property configuration as shown below will appear:



After entering the IP address and subnet mask of the corresponding bridge, click the Apply button to generate the bridge.

Note: Bridges can only be applied after they have been generated

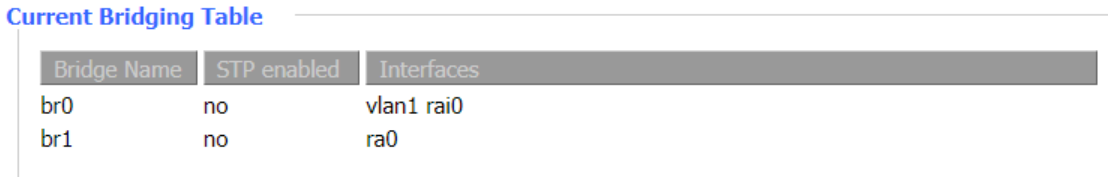


This item is assigned to the bridge, you can assign different interfaces to the already created bridge, for example, in the bridge of br1, assign the interface of ra0 (that is, the wireless interface), as shown below

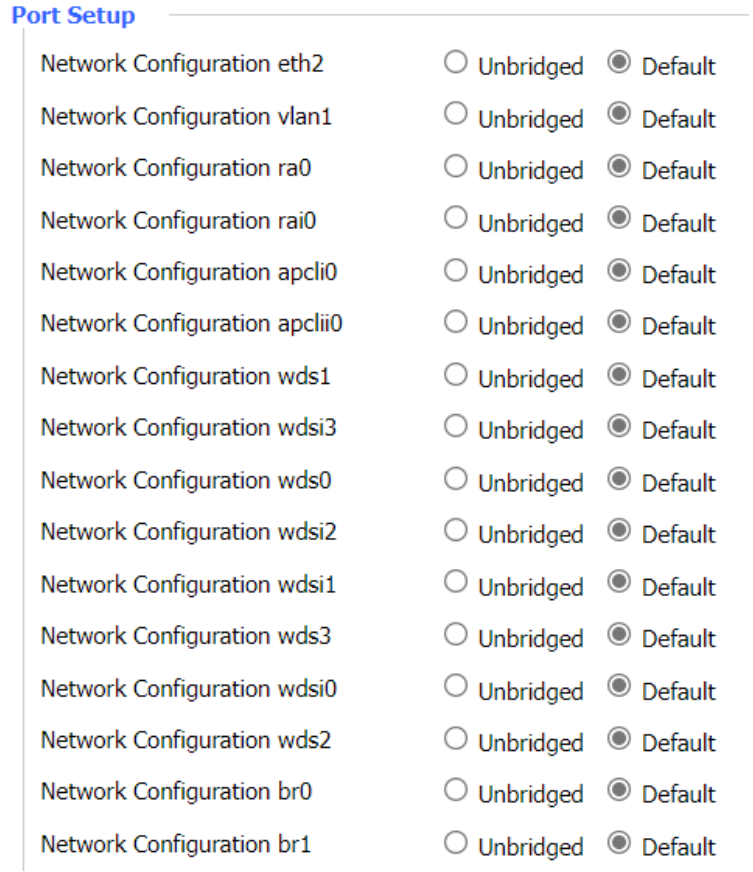
Prio represents the priority level, which is useful if multiple interfaces are bound to the same bridge. The smaller the value, the higher the level. Click **"Apply settings"** for it to take effect.

Note: The interfaces of some WAN ports that appear in the corresponding interface should not be bound. This bridge function is basically used on the LAN port side and should not be bound with the WAN port.

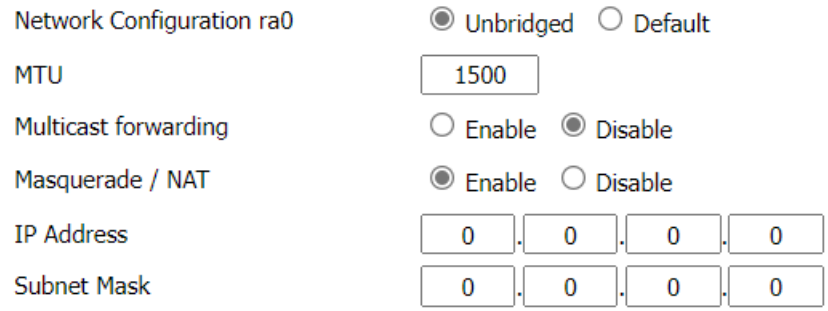
If the binding is successful, the binding list of the bridge will appear in the Current Bridge Table, as follows:



If the bridge of br1 also has the function of DHCP address allocation, it is necessary to set the multi-channel DHCP function. For details, see the introduction of multi-channel DHCPD.



Network Configuration: configure the properties of each port, the following is an ra0 port as an illustration:



If you choose not bridged, you can set the properties of the port itself. The detailed properties are as follows:

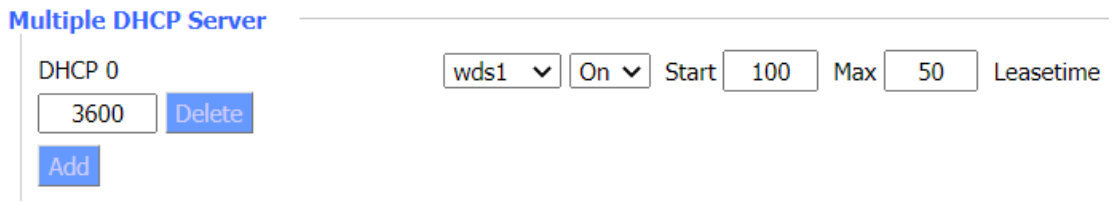
MTU: Maximum Transmission Unit

Multicast forwarding: whether to enable the multicast forwarding function

Masquerade/NAT: Whether to enable Masquerade/NAT

IP Address: Set the IP address of ra0, do not conflict with other ports or bridges

Subnet Mask: Configure the subnet mask of the port

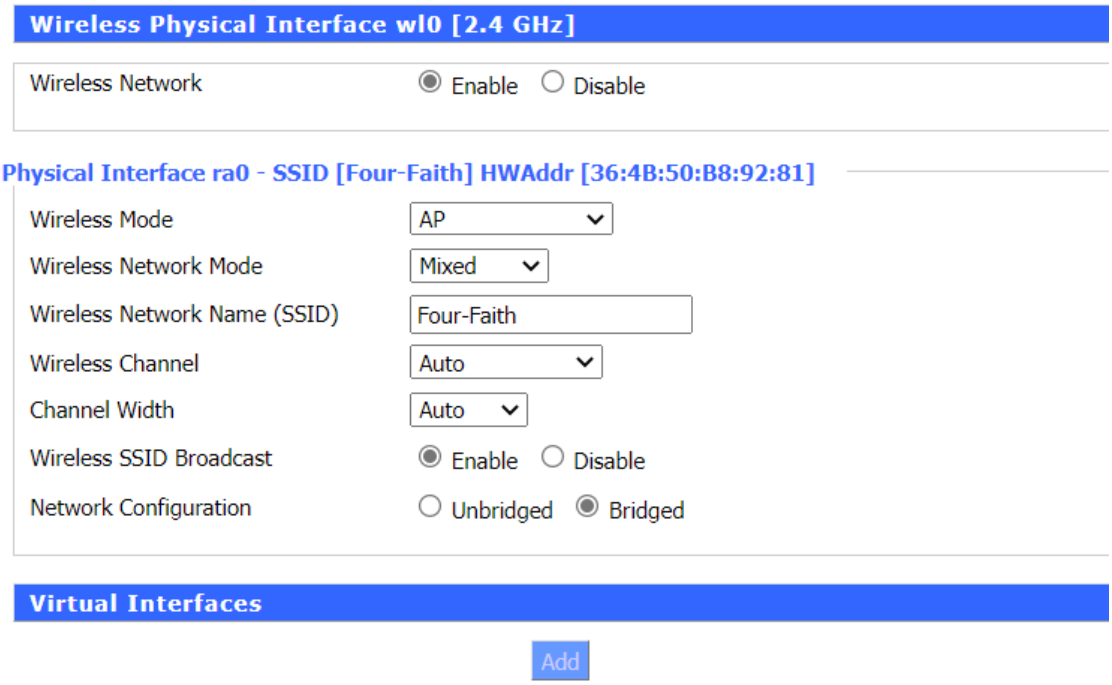


Multiple DHCP Server: Use multiple DHCP services. Click Add in the multi-channel DHCP server, and the corresponding configuration will appear. The first one represents the name of the interface or bridge (do not configure it as eth0), the second represents whether the DHCP function is enabled, and **"Start"** represents the starting address is How many, **"Max"** represents the maximum number of DHCP clients allocated, **"Leasetime"** represents the client lease time, the unit is minutes, after setting, click **"Save"** or **"Apply Settings"** to make it take effect.

Note: You can only configure the next one by clicking Save after one configuration is complete, instead of setting multiple DHCP at the same time at one time.

3.3.2 Wireless

3.3.2.1 Basic Configuration



Enable: Turn on WIFI.

Disable: Turn off WIFI.

Wireless Mode: AP, client, Ad-hoc, relay, relay bridge four modes are optional.

Wireless Network Mode:

Mixed: Wireless devices that simultaneously support 802.11b, 802.11g, and 802.11n standards.

BG-Mixed: Wireless devices that support both 802.11b and 802.11g standards.

B-only: Wireless devices that only support the 802.11b standard.

G-only: Only wireless devices that support the 802.11g standard.

NG-Mixed: Wireless devices that support both 802.11g and 802.11n standards.

N-Only: Wireless devices that only support the 802.11n standard.

Wireless Network Name (SSID): The network name shared by all devices in the wireless network, and the SSID of all devices is the same. The SSID consists of numbers and letters, is case-sensitive, and cannot exceed 32 characters.

Wireless Channel: There are 1-13 channels to choose from. In the environment of multiple wireless devices, please try to avoid using the same channel with other devices.

Channel Width: 20MHZ and 40MHZ are available.

Wireless SSID Broadcast:

Enable: Broadcast SSID.

Disable: Hide the SSID.

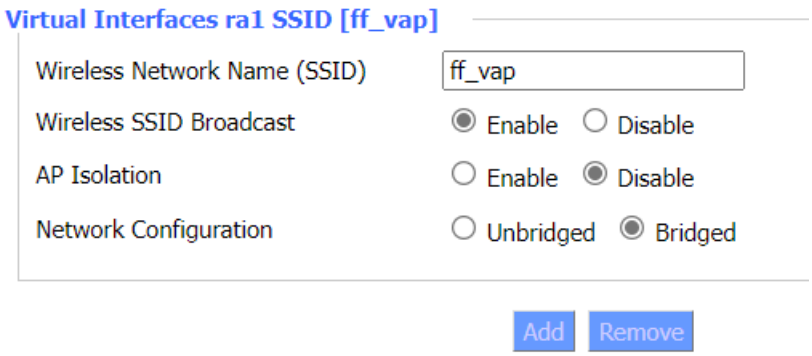
Network Configuration:

Bridged: Bridged to the router, under normal circumstances, please select Bridged.

Unbridged: not bridged to the router, the IP address needs to be configured

manually.

Virtual Interface: Click Add to add a virtual interface. After the addition is successful, click Remove to remove the virtual interface.

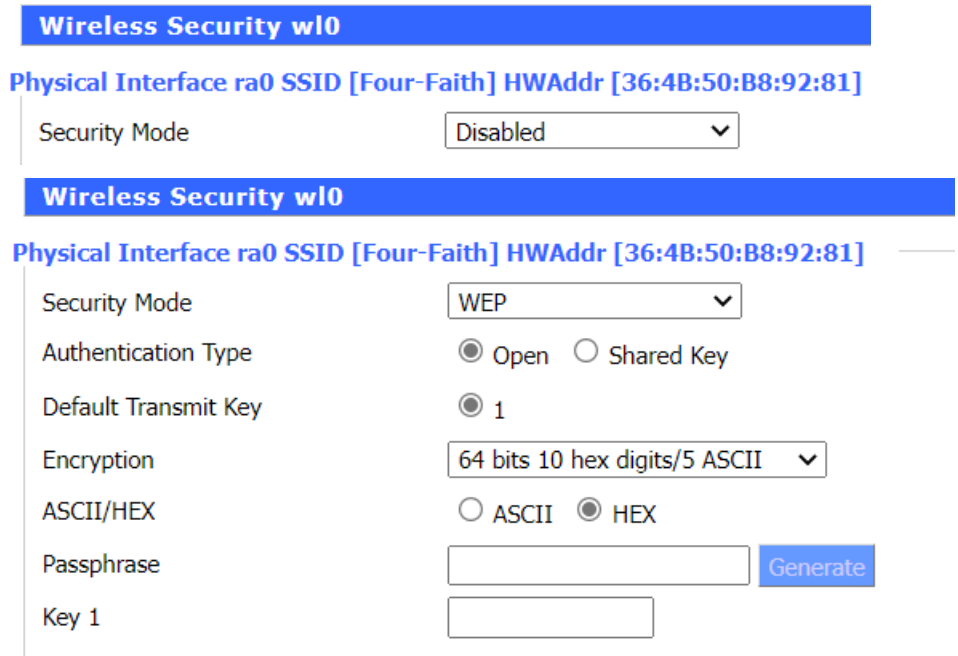


AP Isolation: Completely isolate all wireless client devices so that they can only access the fixed network connected to the AP.

Note: Apply Settings: Save the changes, after changing the "Wireless Mode", "Wireless Network Mode", "Wireless Width", "Broadband" options, please click this button first, and then configure other options.

3.3.2.2 Wireless Security

Wireless security options are used to configure the security of your wireless network. There are 7 wireless security modes in this router.The default mode is disabled and safe mode is not enabled. To change the safety mode, click Apply to take effect immediately.



WEP: is a basic encryption algorithm, not as secure as WPA.

Authentication Type: Open or Shared Key can be selected.

Default Transmit Key: Choose to use one of Key 1-Key 4 to use for transport encryption.
Encryption: There are "64 bit 10 hex digits/5 ASCII", "128 bit 26 hex digits/13 ASCII". Can be generated using a passphrase or entered manually.

64 bit 10 hex digits/5 ASCII: Each key is 10 hexadecimal characters or 5 ASCII characters.

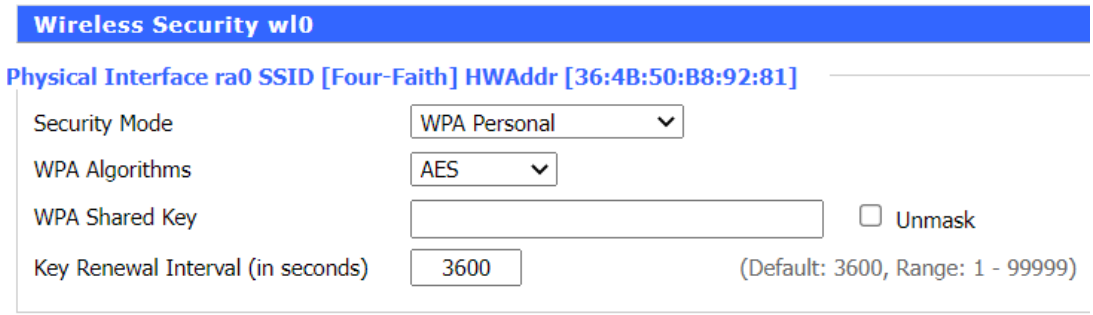
128 bit 26 hex digits/13 ASCII: Each key is 26 decimal characters or 13 ASCII characters.

ASCII/HEX: ASCII, select the key as ASCII code.

HEX, the selection key is a hexadecimal number.

Passphrase: A combination of letters and numbers used to generate a key.

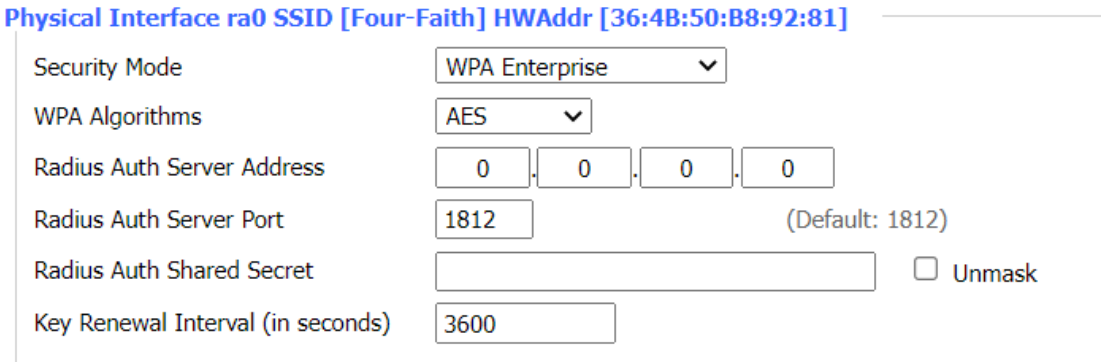
Key 1: It can be filled in manually or generated by the router based on the input passphrase.



WPA Personal/WPA2 Personal/WPA2 Person Mixed: Provides three WPA algorithms, TKIP and AES, TKIP+AES, using dynamic encryption keys. TKIP+AES, self-applied TKIP or AES. WPA Person Mixed, allows WPA Personal and WPA2 Personal clients to be mixed.

WPA Shared Key: 8-63 characters, consisting of letters and numbers.

Key Renewal Interval (in seconds): 1-99999.



WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed: Enterprise WPA/WPA2 encryption, the router needs to connect to the Radius authentication server.

WPA Algorithm: AES/TKIP/TPIP+AES.

Radius Auth Server Address: The IP of the Radius server connected to the router.

Radius Auth Server Port: the port used by the radius service on the Radius server.

Radius Auth Shared Secret: The shared key between the Radius server and the router.

Key Renewal Interval (in seconds): 1-99999.

3.3.3 Service

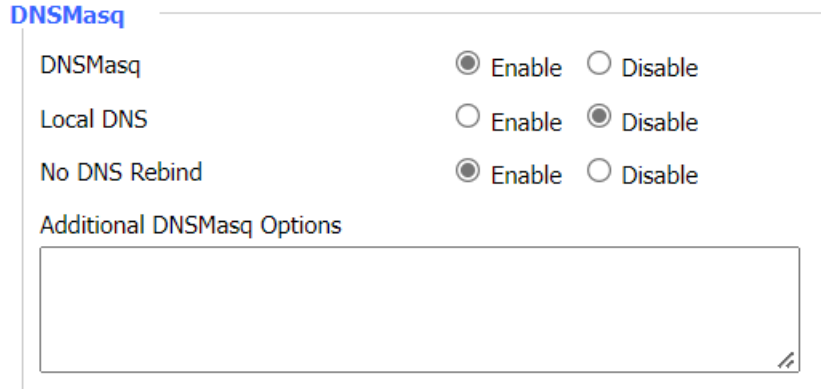
3.3.3.1 Service

DHCP Server

The DHCP service assigns an IP address to your local device. You can enter the main menu, and then go to the setting page to configure the special functions of DHCP that you need.

DNSMasq

DNSMasq is a local DNS server. This will resolve all known host names from DHCP (dynamic and static) routers as well as forwarding and cached DNS entries from remote DNS servers. Local DNS enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.



Local DNS: Use the local DNS, you can set the DNS server in the setting page

No DNS Rebind: When enabled it prevents external attackers from accessing the router's internal web interface and is a security measure

Additional DNSMasq Options: There are some additional options that can be set, enter your own corresponding configuration.

For example:

Statically assigned address:dhcp-host=AB:CD:EF:11:22:33,192.168.0.10,myhost,myhost.

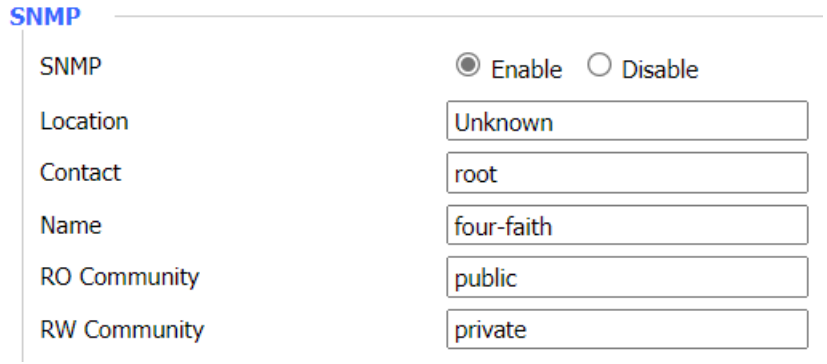
domain,12th

Maximum number of leases: dhcp-lease-max=2

IP range of DHCP server: dhcp-range=192.168.0.110,192.168.0.111,12h

SNMP

SNMP (Simple Network Management Protocol). This is a widely used network management protocol. Data is passed through an SNMP agent. SNMP agents refer to hardware and/or software processes that report the activities of each network device (such as hubs, routers, and bridges) to workstations for network monitoring purposes. The agent returns the information contained in the MIB (Management Information Base). A MIB is a data structure that defines options that can be obtained from a device and that can be controlled (such as turned on or off).



Location: The location identifier of the device, which is defined by the customer

Contact: User defined, should be consistent with the client

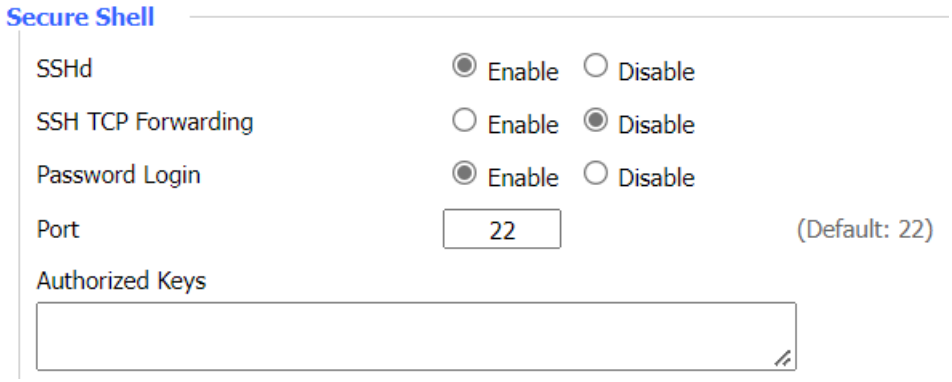
Name: User defined, should be consistent with the client

RO Community: user-defined, should be consistent with the client, only read permission

RW Community: user-defined, should be consistent with the client, with read and write permissions

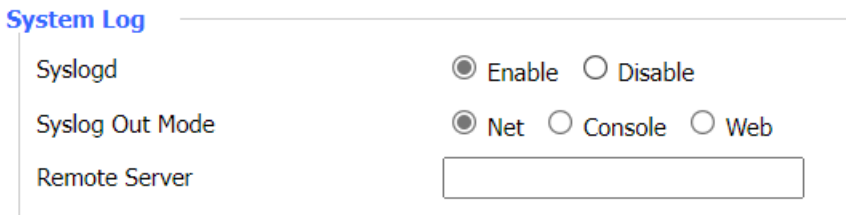
SSHD

Enable the SSHD service to allow remote access to your router's operating system via an SSH client.



SSH TCP Forwarding: Whether to support the TCP forwarding function
Password Login: whether password login is required
Port: Set the port of SSHD, the default system is set to port 22
Authorization Keys: set as needed, the system login password and user name are used by default

System Log



Syslog Out Mode: network and serial port, the remote server IP address needs to be set in the network mode
Remote Server: The IP address of the remote server that accepts syslogs

Telnet

This is a terminal emulation protocol commonly used on the Internet and in TCP/IP-based networks. It allows end users or computers to log on to remote devices and run programs.

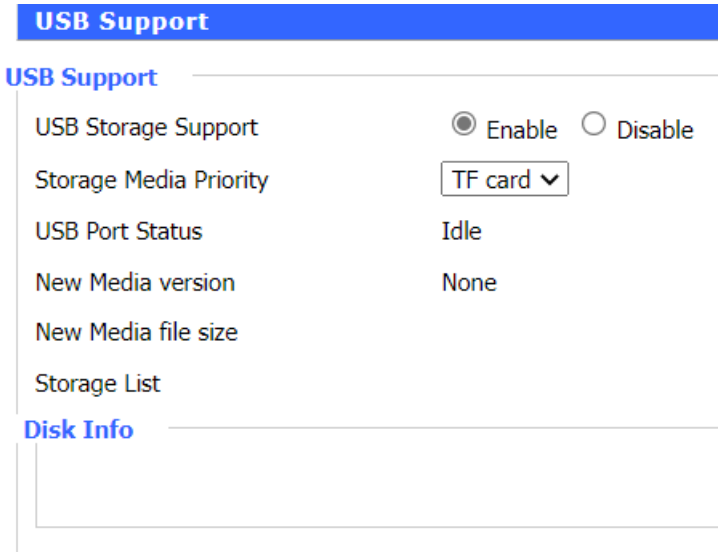
Telnet: Enable or disable the Telnet function

WAN traffic counter

Ttraff Daemon: enable or disable the traffic statistics function

3.3.3.2 USB

Enable this service to identify the U disk, TF card or SD memory card connected to the router, and use these types of storage media. The specific setting instructions are as follows:

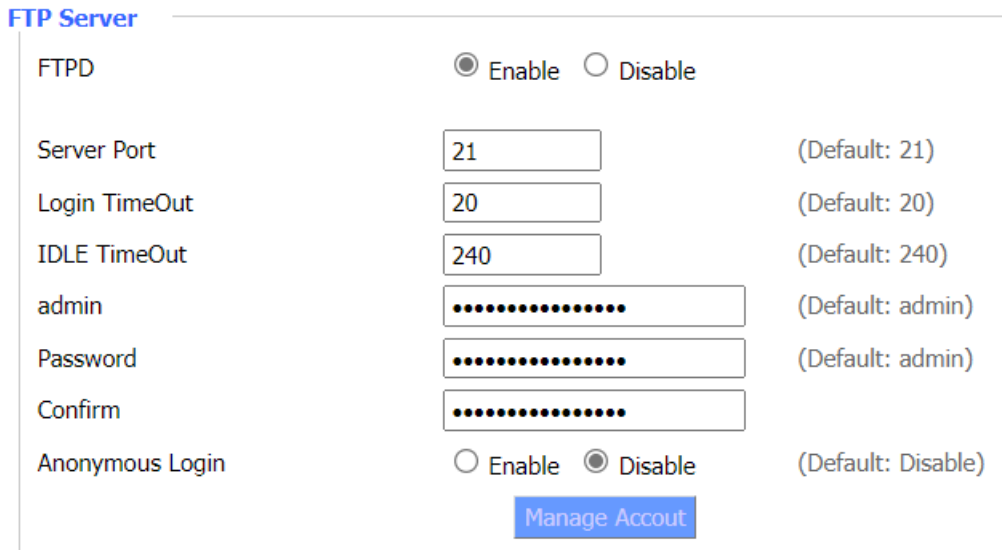


Storage Media Priority: TF card or SSD can be set as the priority storage medium in the router

Storage List: The storage medium currently recognized in the router, marked with TF and SSD.

3.3.3.3 FTP Service

When this service is enabled, the router is used as a simple FTP application server, and users can upload or download files to the router's external U disk, TF card or SD memory card as an FTP client.



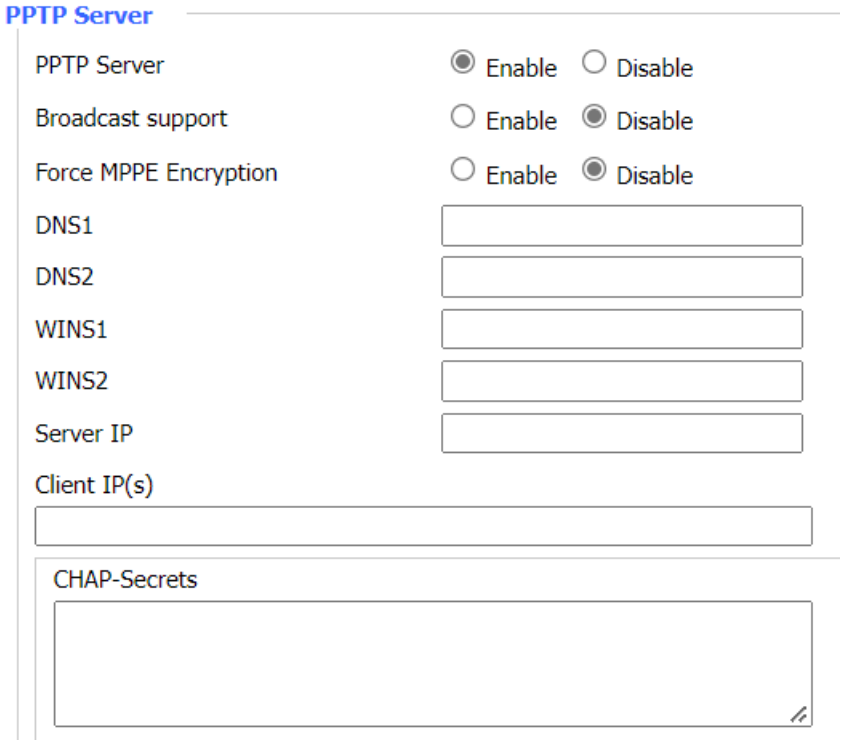
Server Port: The router acts as the local listening port of the FTP server, the default is 21.

Admin: The administrator account for logging in to the router's FTP server, the default is the user name "admin" for the router's WEB configuration management.
Password: the administrator password for logging in to the router's FTP server, the default is the password "admin" for the router's WEB configuration management.

3.3.4 VPN

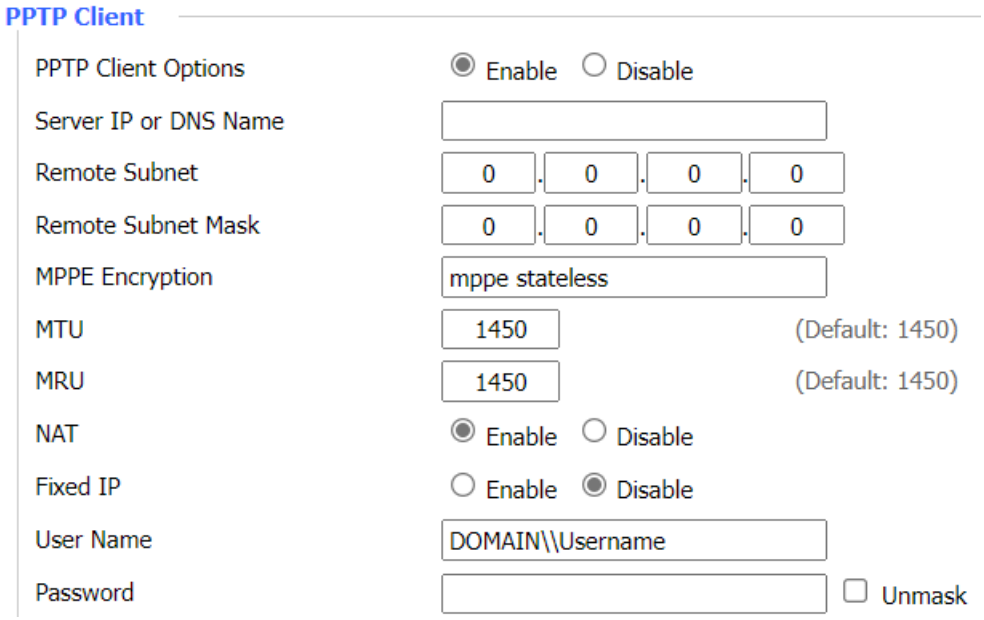
3.3.4.1 PPTP

PPTP Server



Broadcast support: enable or disable the PPTP server to support the broadcast function
Force MPPE Encryption: Whether to force PPTP data MPPE encryption
DNS1, DNS2, WINS1, WINS2: Set your 1st DNS, 2nd DNS, 1st WINS, 2nd WINS
Server IP: Enter the IP address of the router as the PPTP server, which should be different from the LAN address.
Client IP: The IP address assigned to the client, in the format xxx.xxx.xxx.xxx-xxx
CHAP-Secrets: Username and password when the client uses the PPTP service
Note: The client IP cannot be the same as the IP assigned by the router's DHCP, as long as it is outside this range.CHAP Secrets format is user space * space password space *

PPTP client



Server IP or DNS name: The IP address of the PPTP server or the corresponding DNS name

Remote Subnet: Intranet of the remote PPTP server

Remote Subnet Mask: The subnet mask of the remote PPTP server

MPPE Encryption: Whether to support MPPE encryption.

MTU: Maximum Transmission Unit 0-1500

MRU: Maximum receiving unit 0-1500

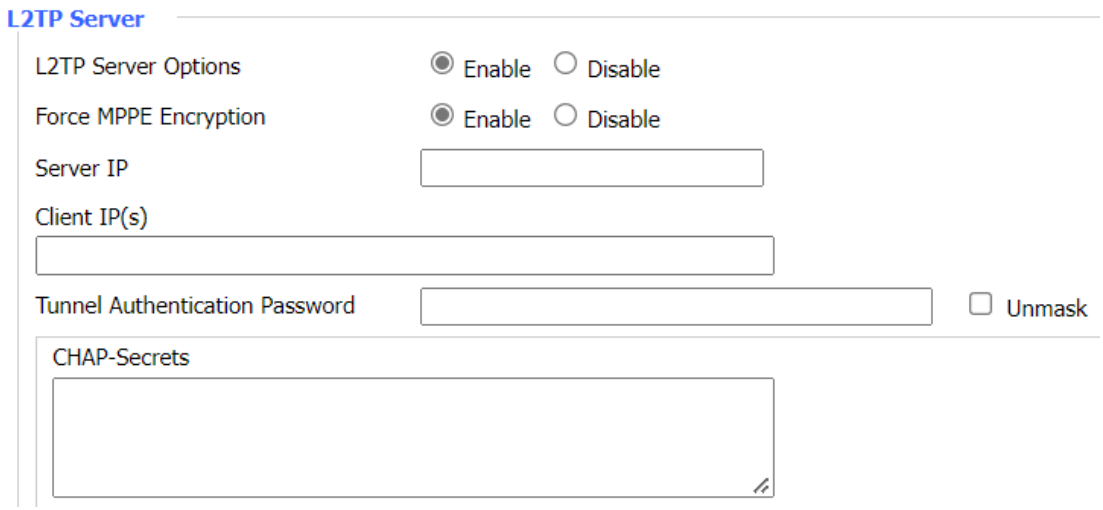
NAT: Enable or disable NAT traversal

User Name: Username allowed by the PPTP server

Password: The password corresponding to the username allowed by the PPTP server

3.3.4.2 L2TP

L2TP server



Force MPPE Encryption: Whether to force L2TP data MPPE encryption

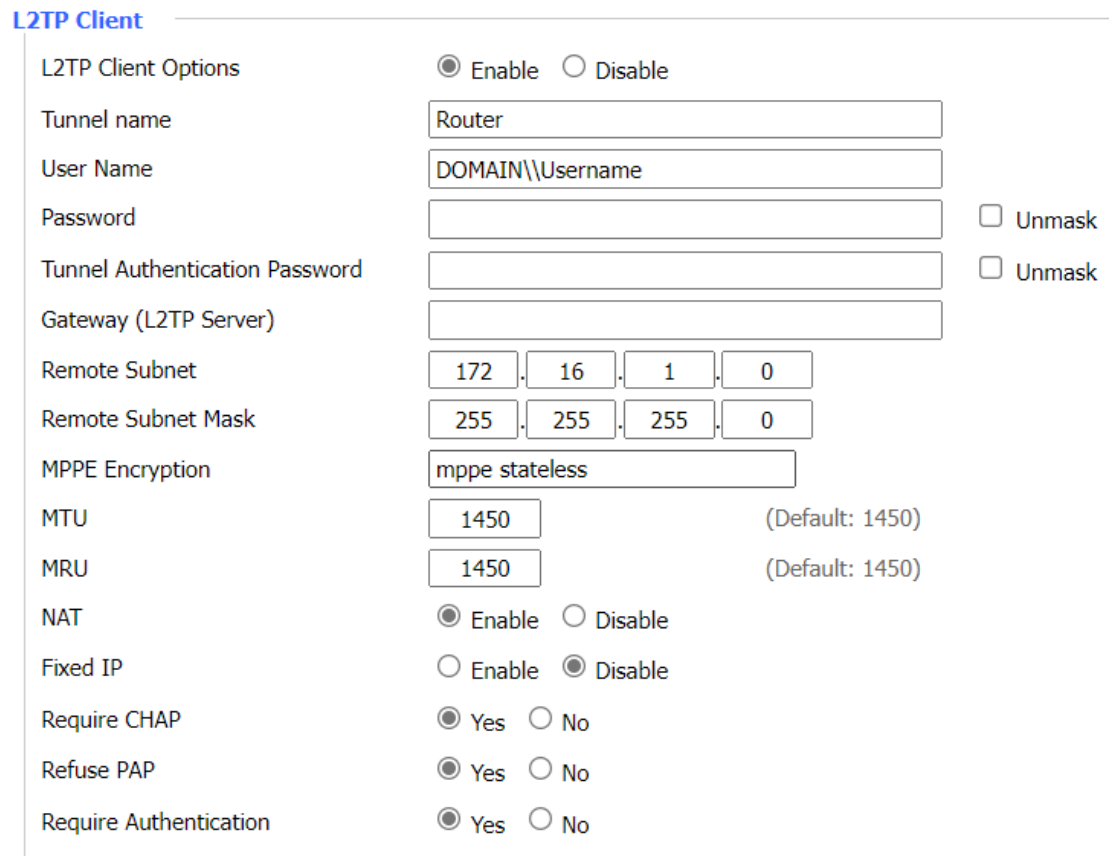
Server IP: Enter the IP address of the router as the L2TP server, which should be different from the LAN address.

Client IP: The IP address assigned to the client, the format is xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx

CHAP-Secrets: Username and password when the client uses the L2TP service

Note: The client IP cannot be the same as the IP assigned by the router's DHCP, as long as it is outside this range.CHAP Secrets format is user space * space password space *

L2TP client



Gateway(L2TP Server): IP address or corresponding DNS name of the L2TP server

Remote Subnet: The network to which the L2TP server intranet belongs

Remote Subnet Mask: The network mask to which the L2TP server's intranet belongs

MPPE Encryption: Whether to support MPPE encryption.

MTU: Maximum Transmission Unit 0-1500

MRU: Maximum receiving unit 0-1500

NAT: Enable or disable NAT traversal

User Name: Username allowed by the L2TP server

Password: The password corresponding to the username allowed by the L2TP server

Require CHAP: whether to support chap authentication

Refuse PAP: whether to refuse to support pap authentication

Require Authentication: Whether to support authentication protocol

3.3.4.3 OPENVPN

OPENVPN server

Start Type: WAN Up---Enable after going online, System---Enable at startup

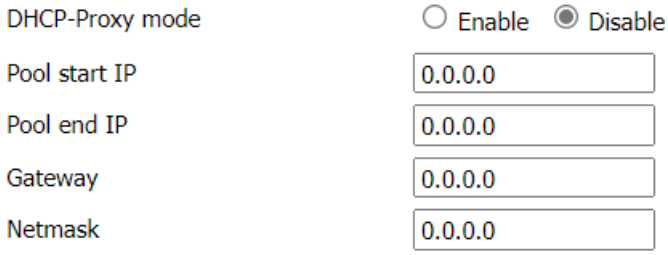
Server mode: Router---routing mode, Bridge---bridge mode

Route method:

Network: The network address allowed by the OPENVPN server

Netmask: The subnet mask allowed by the OPENVPN server

Bridge Mode:



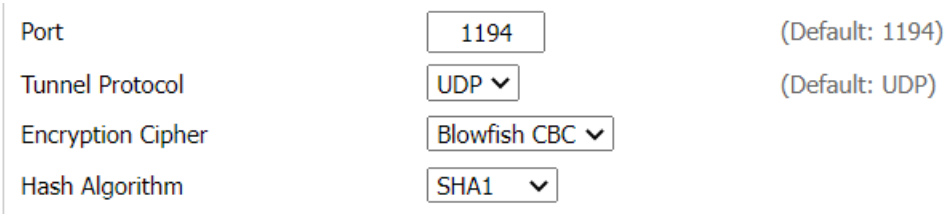
DHCP-Proxy mode: Enable or disable DHCP proxy mode

Pool start IP: the start address of the client allowed by the OPENVPN server

Pool end IP: the end address of the client allowed by the OPENVPN server

Gateway: OPENVPN server allows the client's gateway

Netmask: Allowed client subnet mask of OPENVPN server



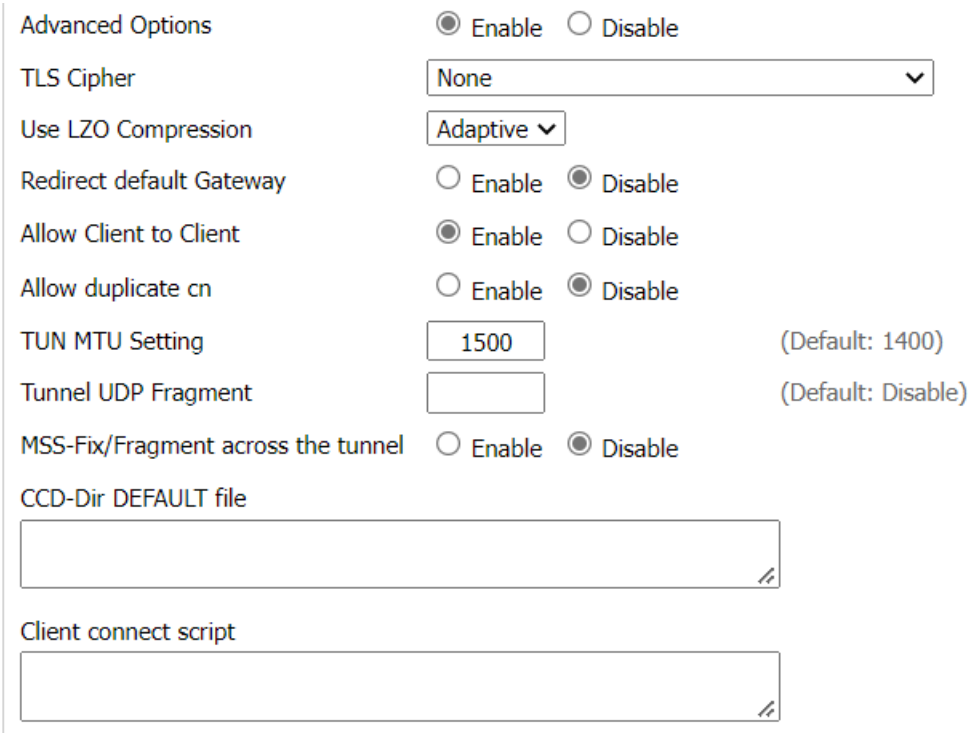
Port: The listening port of the OPENVPN server

Tunnel Protocol: OPENVPN's tunnel protocol UDP or TCP

Encryption Cipher: The encryption standard of the channel includes: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC five kinds of encryption

Hash Algorithm: Hash algorithm provides a fast way to access data, including SHA1, SHA256, SHA512, MD5 four algorithms

Advanced Options



Use LZO Compression: Enable or disable the use of LZO compression for transmitted data

Redirect Default Gateway: Enable or disable the relocation gateway

Allow Client to Client: Enable or disable allow client-to-client

Allow duplicate cn: Enable or disable Allow duplicate CN

TUN MTU setting: set the MTU value of the channel

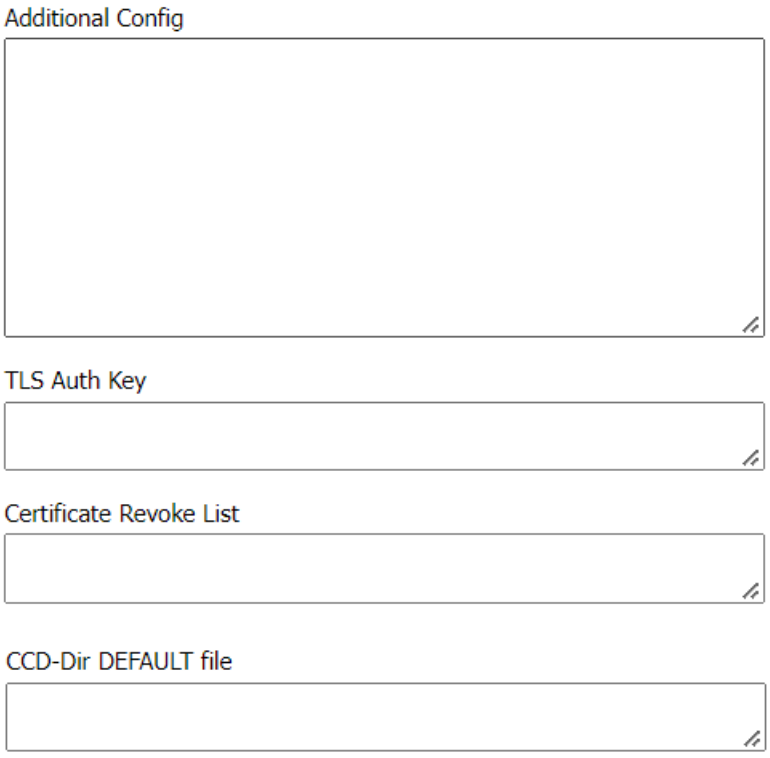
Client connection script: some self-defined client scripts

CA Cert: the server and client public CA certificate

Public Server Cert: server-side certificate

Private Server Key: the key set on the server-side

DH PEM: PEM certificate of the server



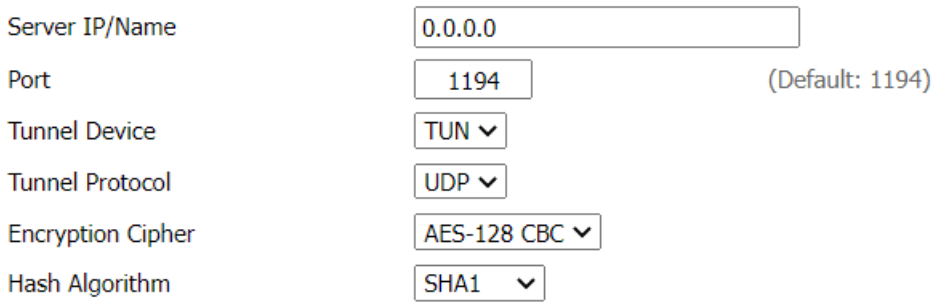
Additional Config: other additional configuration of the server

TLS Auth Key: The authentication key of the secure transport layer

Certificate Revoke List: configure some revoked certificate lists

CCD-Dir DEFAULT file: other file paths

OPENVPN client



Server IP/Name: IP address or domain name of OPENVPN server

Port: The listening port of the OPENVPN client

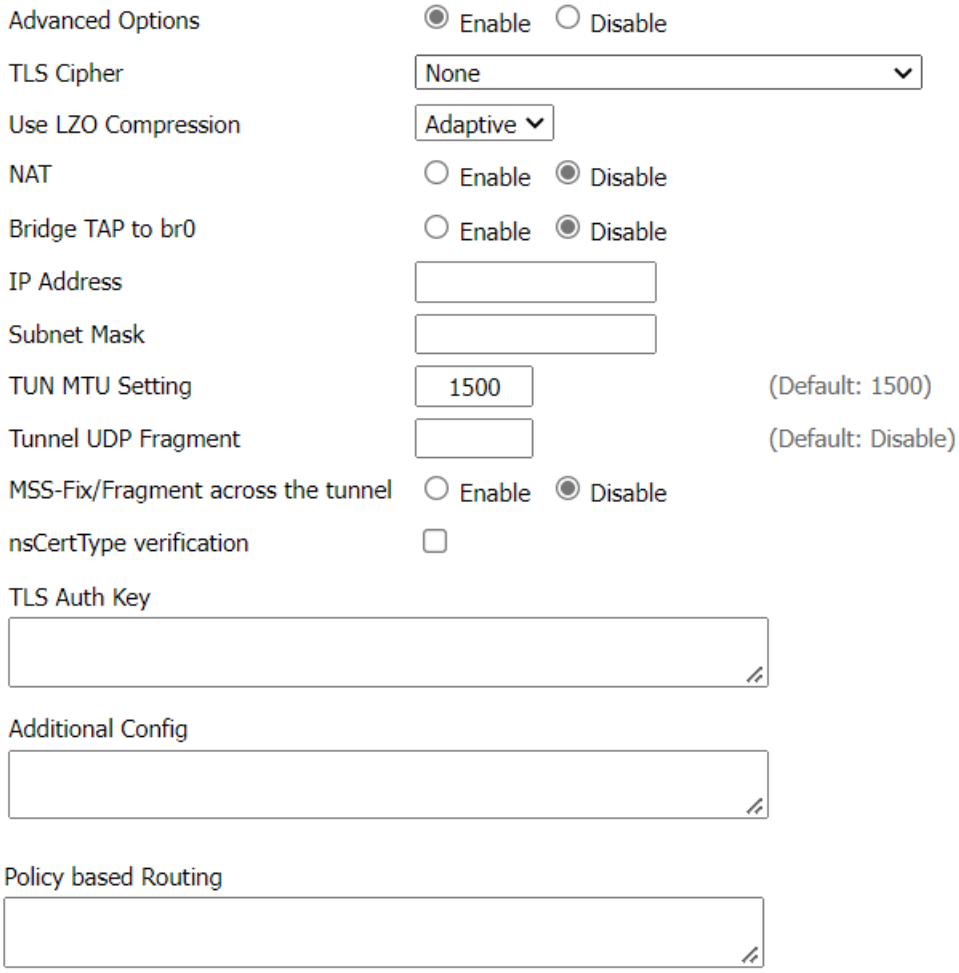
Tunnel Device: TUN---routing mode, mode TAP---bridge mode

Tunnel Protocol: UDP and TCP protocols

Encryption Cipher: The encryption standard of the channel includes: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC five kinds of encryption

Hash Algorithm: Hash algorithm provides a fast way to access data, including SHA1,

SHA256, SHA512, MD5 four algorithms



Use LZO Compression: Enable or disable the use of LZO compression for transmitted data

NAT: Enable or disable NAT traversal function

Bridge TAP to br0 : Enable or disable TAP binding to br0 bridge

IP Address: Set the IP address of the local OPENVN client

TUN MTU Setting: set the MTU value of the channel

TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA

TLS Auth Key: The authentication key of the secure transport layer

Additional Config: OPENVPN server other additional configuration

Policy based Routing: enter some custom routing policies

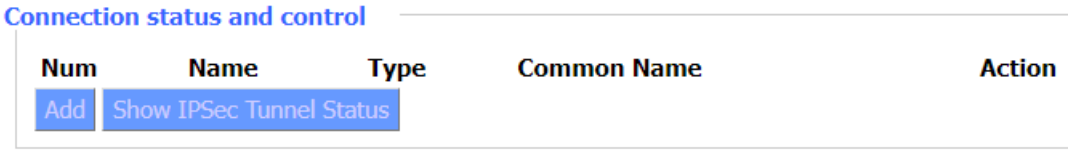
nsCertType verification: whether to support the ns certificate type

CA Cert: the server and client public CA certificate
Public Client Cert: client certificate
Private Client Key: the client's secret key

3.3.4.4 IPSEC

Connection Status and Operation

On the IPSEC page, the IPSEC connection and status of the current device will be displayed.



Name: the name of the IPSEC connection;
Type: the type and function of the current IPSEC connection;
Common name: the currently connected local network, local address, peer address and peer network;
Action: There are four types of operations that can be performed on the connection, namely delete, edit, reconnect and enable.

Delete: This operation will delete the connection, and if the IPSEC channel has been established, it will also be torn down;

Edit: Modify the configuration information of the connection. After the modification, if you want the configuration to take effect, you need to reload the connection;

Reconnect: This operation will remove the current channel and re-initiate the channel establishment request;

Enable: When the connection is enabled, the connection will initiate a channel establishment when the system restarts or performs a reconnection operation.

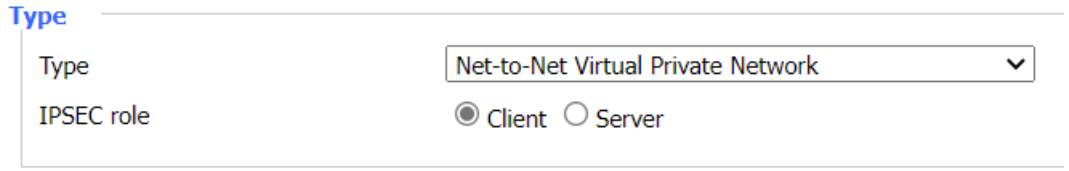
request; conversely, no request will be made.

Add: This function is used to add a new IPSEC connection.

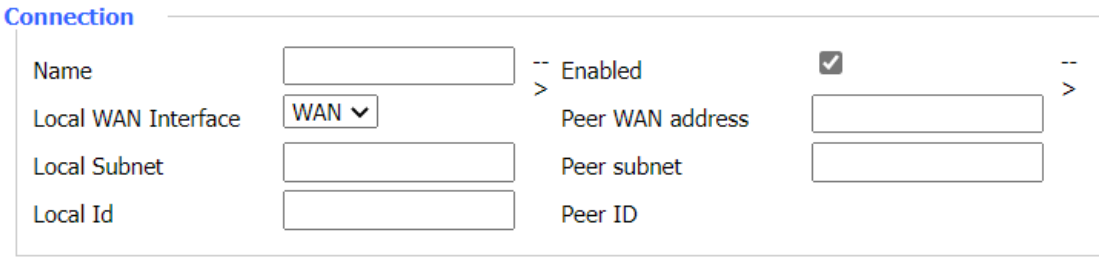
Add IPSEC connection or edit IPSEC connection

Type: Select the IPSEC mode and the corresponding function in this column. Currently,

the client function of the tunnel mode, the server function of the tunnel mode and the transmission mode are supported.

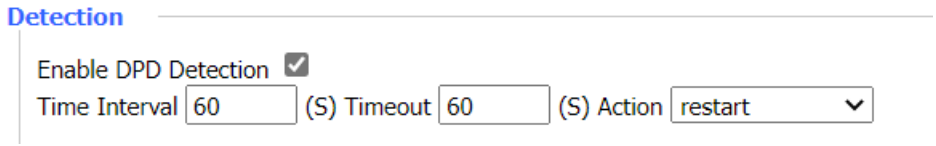


Connection: This column contains the basic address information of the channel.



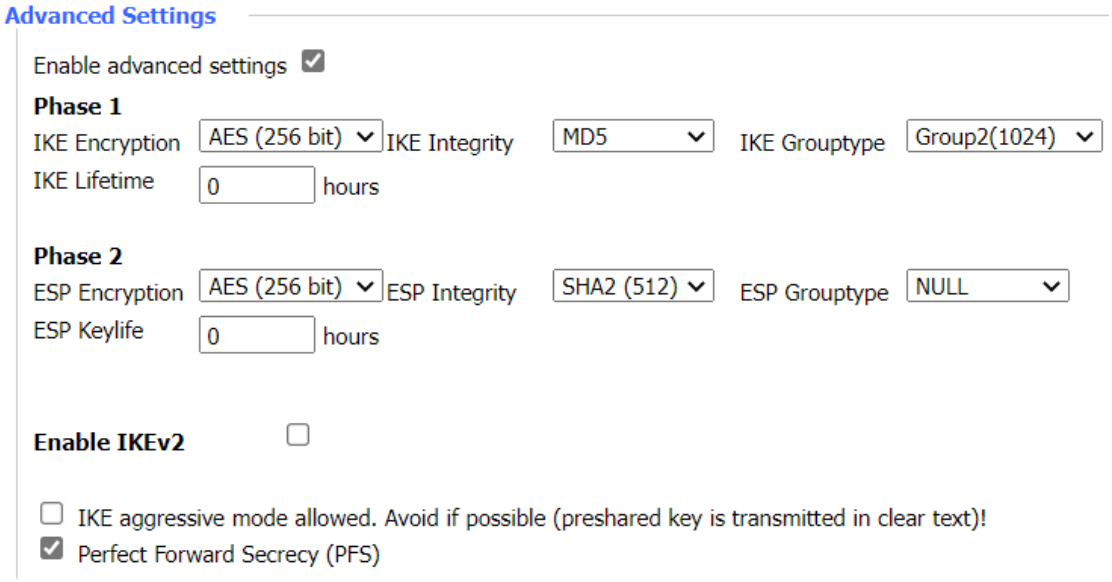
Name: The name used to identify the connection, which must be unique;
Enabled: Select Enable, then the connection will initiate a channel connection request when the system starts or reconnects; otherwise, it will not;
Local WAN Interface: the local address of the channel;
Peer WAN address: the IP/domain name of the peer. If the server function in tunnel mode is used, this option cannot be filled;
Local Subnet: IPSec local protection subnet and subnet mask, for example: 192.168.1.0/24; if the transmission mode is used, this option cannot be filled;
Peer Subnet: IPSec peer protection subnet and subnet mask, for example: 192.168.7.0/24; if the transmission mode is used, this option cannot be filled;
Local Id: the local identifier of the channel, which can be IP and domain name;
Peer Id: channel peer identifier, which can be IP and domain name.

Detection: This column contains configuration information for connection detection (DPD).



Enable DPD Detection: whether to enable this function, check it to enable it;
Time Interval: Set the time interval for connection detection (DPD);
Timeout: Set the connection detection (DPD) timeout;
Action: Set the action for connection detection.

Advanced configuration: This column contains related configurations such as IKE, ESP and negotiation mode.



Enable advanced settings: Enable, you can configure the information of the first stage and the second stage, otherwise, it will be automatically negotiated according to the peer end;

IKE Encryption: the encryption method in the IKE phase;

IKE Integrity: the integrity scheme of the IKE phase;

IKE Grouptype: DH exchange algorithm;

IKE Lifetime: set the life cycle of IKE, currently in hours, the default is 0;

ESP Encryption: the encryption method of ESP;

ESP Integrity: ESP integrity scheme;

ESP Keylife: Set the life cycle of ESP, currently in hours, the default is 0;

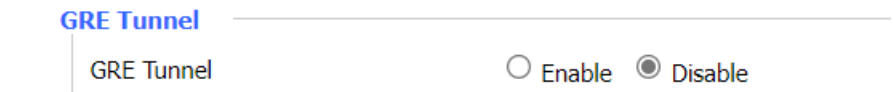
IKE aggressive mode: if checked, the negotiation mode will adopt the aggressive mode, otherwise the main mode;

Perfect Forward Secrecy: if checked, PFS is enabled, otherwise it is not enabled;

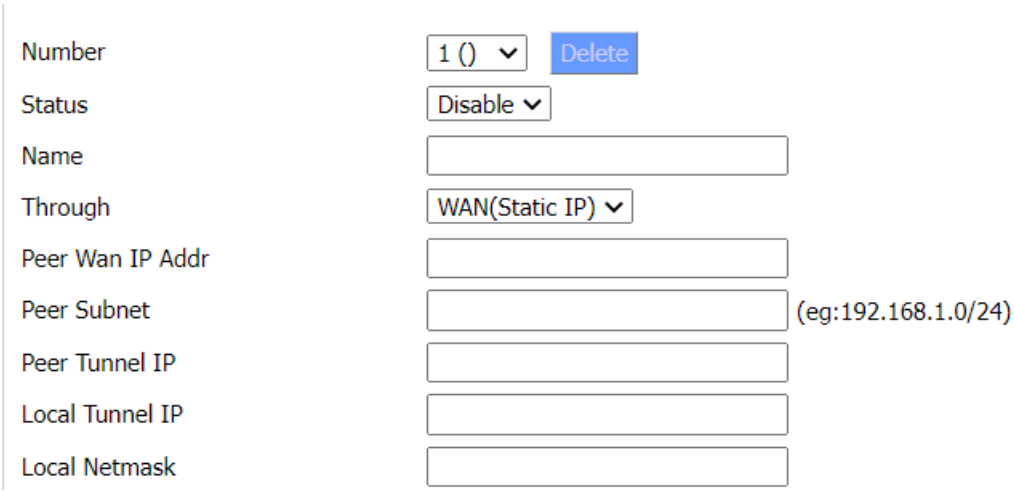
Authentication: You can choose shared key or certificate authentication according to your needs. Currently, only the shared key method can be selected.

3.3.4.5 GRE

GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) protocol encapsulates the data packets of some network layer protocols (such as IP and IPX), so that these encapsulated data packets can be used in another network layer protocol (such as IP) in transmission. GRE adopts Tunnel technology, which is the third layer tunneling protocol of VPN (Virtual Private Network).



GRE Tunnel: Enable or disable GRE function



Number: A channel that can be set, currently up to 12 GRE tunnels can be set

Status: Enable means enable the currently configured GRE tunnel, otherwise means close the current GRE tunnel

Name: The name of the tunnel can be up to 30 characters long

Through: GRE transceiver interface, currently there are LAN port, and PPP dial-up port

Peer WAN IP Addr: Enter the WAN port IP address of the peer GRE

Peer Subnet: Subnet IP of the GRE peer, for example: 192.168.1.0/24

Peer Tunnel IP: peer GRE tunnel IP

Local Tunnel IP: local GRE tunnel IP address

Local Netmask: Local Subnet Mask

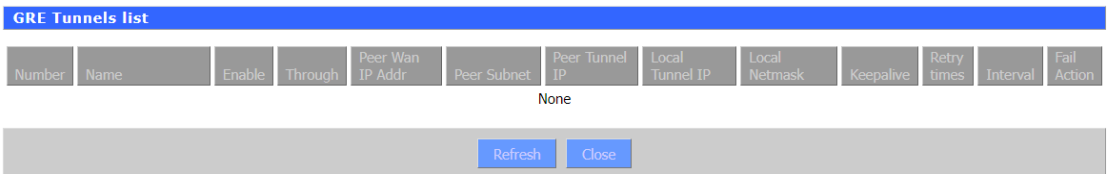
Keepalive: Enable/disable GRE keepalive

Retry times: the maximum number of GRE keepalive failures

Interval: GRE keep-alive packet sending interval

Fail Action: Keepalive Failure Policy

Click the "View GRE Tunnels" button to view GRE information



3.3.5 Security

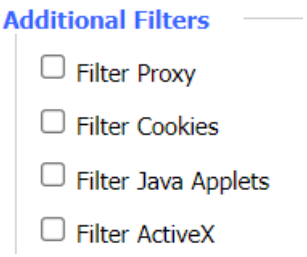
3.3.5.1 Firewall

You can enhance the security of your network by enabling or disabling the firewall, choosing to filter specific types of Internet data, and blocking anonymous Internet requests.

Firewall Protection

Firewall enhances network security and uses Stateful Inspection (SPI) to inspect packets entering the network. To use firewall protection, select Enable, otherwise disable. Other firewall functions: filtering proxies, blocking WAN requests, etc., are only available if the SPI firewall is enabled.

Additional Filters



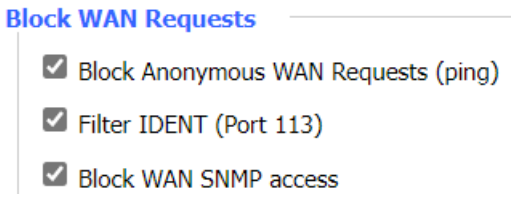
Filter Proxy: Using a wan proxy server may reduce the security of the gateway. Filter Proxy will deny any access to any wan proxy server. Click the checkbox to enable proxy filtering or deselect it to disable this function.

Filter Cookies: Cookies are data that web sites store on your computer and are used when you interact with Internet sites. Click the checkbox to enable cookie filtering or uncheck it to disable the feature.

Filter Java Applets: If Java is denied, web pages programmed with Java tools may not open, click the checkbox to enable Java applet filtering or uncheck to disable the feature.

Filter ActiveX: If ActiveX is denied, web pages programmed with ActiveX tools may not be opened, click the checkbox to enable ActiveX filtering or deselect it to disable the feature.

Block WAN Requests



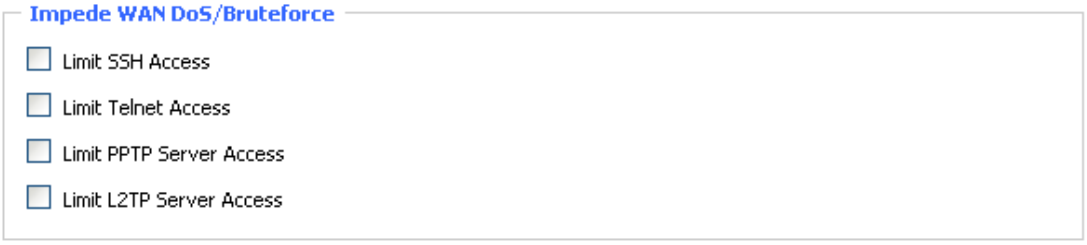
Block Anonymous WAN Requests(ping): Enable this feature by checking the box next to "Block anonymous Internet requests", thereby preventing your network from being pinged or probed by other Internet users, making it more difficult for external users to break into your network. Network, this feature is enabled by default, select Disable to allow anonymous Internet requests.

Filter IDENT (Port 113): This feature prevents port 113 from being scanned by devices outside your local network. Select Enable to filter port 113, or deselect to disable this feature.

Block WAN SNMP access: This feature blocks SNMP connection requests from the WAN.

After making changes, click **"Apply Settings"** to save the changes, or **"Cancel Changes"** to cancel the changes.

Impede WAN DoS/Bruteforce



Limit SSH Access: This function limits SSH access requests from the WAN, and accepts a maximum of 2 SSH connection requests per minute for the same IP.

Limit Telnet Access: This function limits Telnet access requests from the WAN. For the same IP, a maximum of 2 Telnet connection requests are accepted per minute.

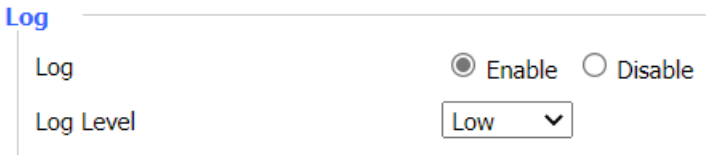
Limit PPTP Server Access: When the device establishes a PPTP server, this function limits the PPTP access requests from the WAN. For the same IP, a maximum of 2 PPTP connection requests are accepted per minute.

Limit L2TP Server Access: When the device establishes an L2TP server, this function limits the L2TP access requests from the WAN. For the same IP, a maximum of 2 L2TP connection requests are accepted per minute.

Log Management

The router can keep a log of all your Internet connections, both incoming and outgoing.

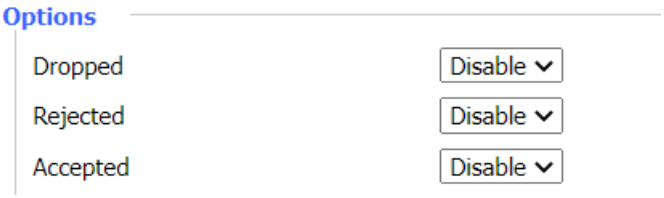
Log



To keep the log active, select "Enable", to stop logging, select "Disable". When enabled, the following selection page will appear.

Log Level: Set the "Log Level", a higher level will record more logs.

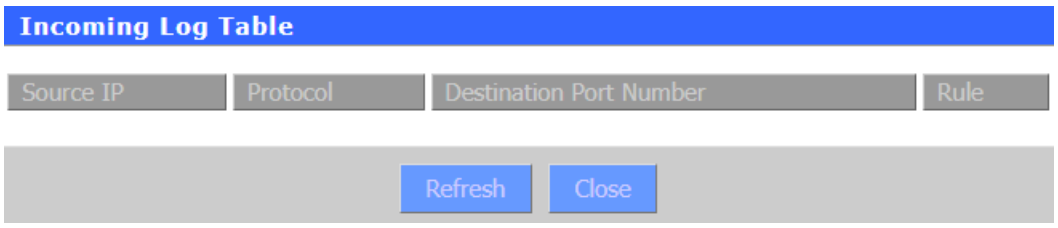
Options



When each of the above three options is enabled, the corresponding connection will be recorded in the log, and if disabled, it will not be recorded.

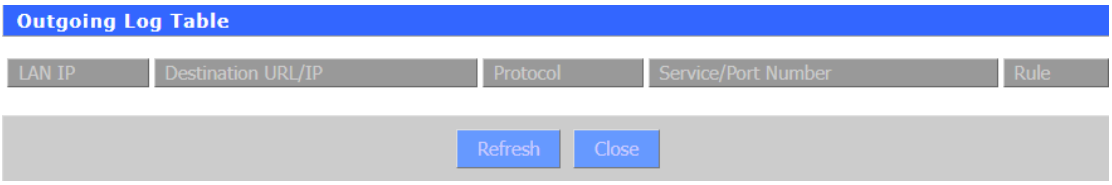
Incoming Log Table

To see the router's most recent incoming temporary log, click the "Connect Log" button.



Outgoing Log Table

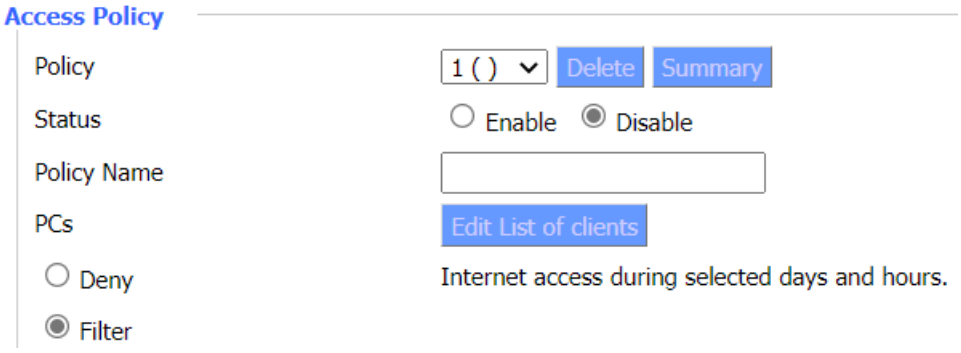
To see the router's most recent incoming temporary log, click the "Connect Out Log" button.



3.3.6 Access

3.3.6.1 WAN Access

Use the Internet Access page to block or allow specific types of Internet applications, and you can set Internet access policies for specific PCs.



There are two options of "Filter" and "Deny" in the default policy rule. If you select "Deny",

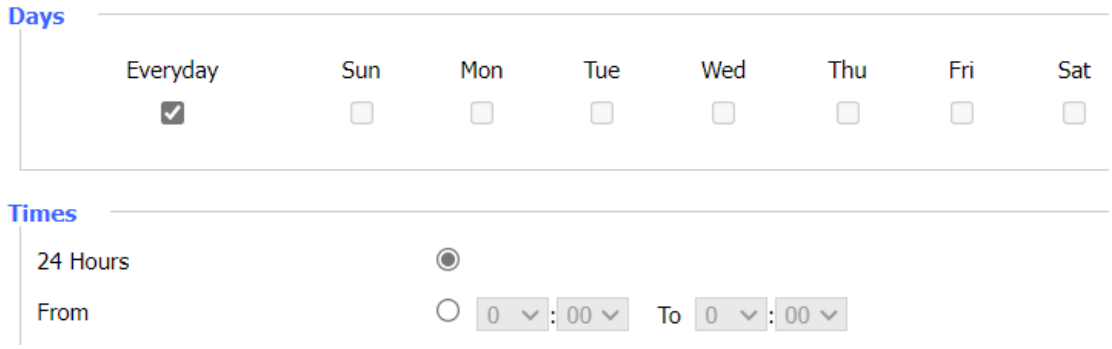
it will deny a specific computer to access any Internet service during a specific period of time; if you select "Filter", it will prevent a specific computer from accessing any Internet service within a specific period of time. Access to a specific website; you can set 10 Internet access policies to filter the Internet services accessed by a specific PC in a specific time period.

Policy: You can define up to 10 access policies. Click the Delete button to delete a strategy, or click the Summary button to view a strategy overview.

Status: Enable or disable a policy.

Policy Name: You should give your policy a name.

PCs: This column is used to edit the client list. The policy is only valid for PCs in this list.

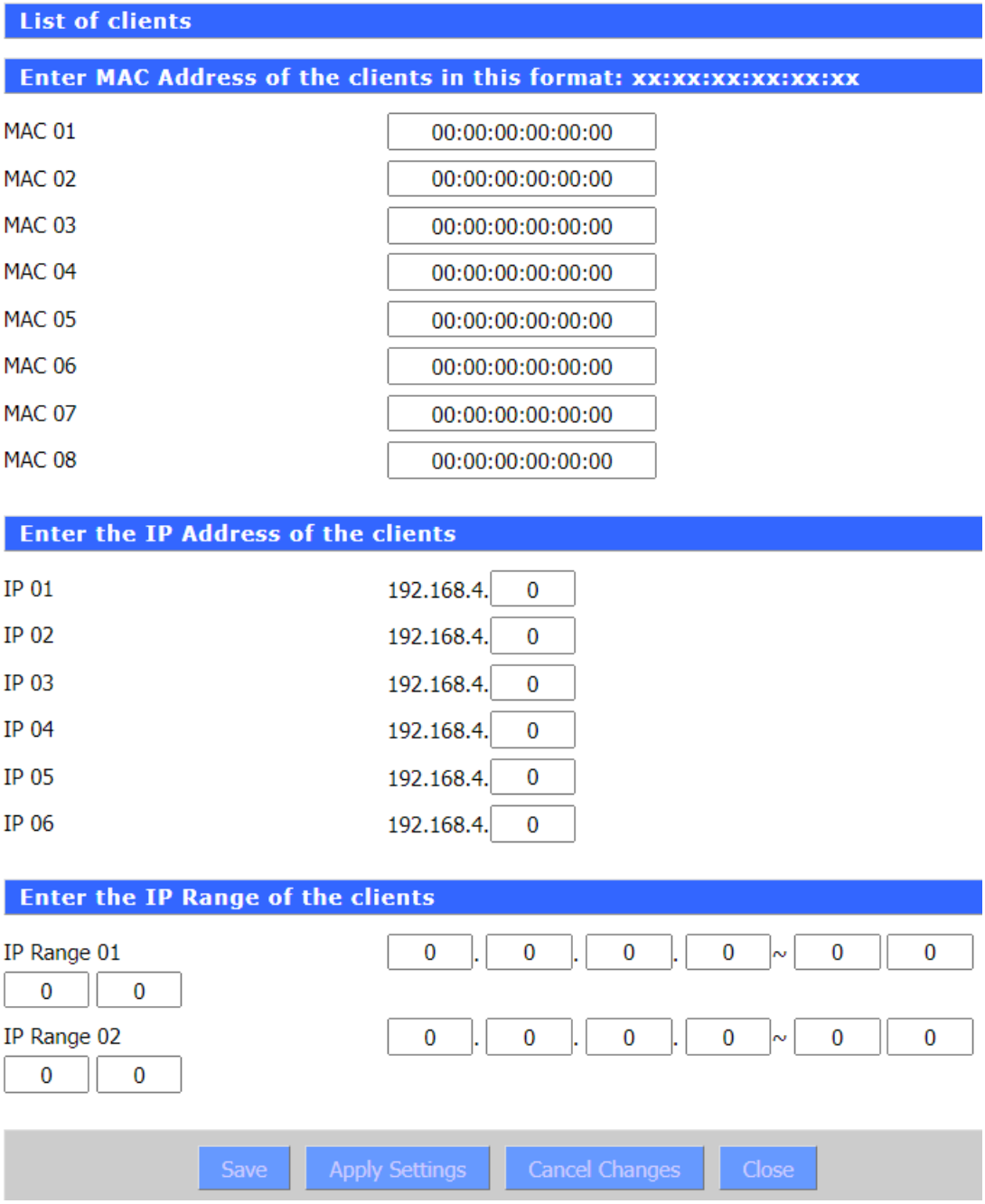


Days: Please select the day you want your policy to be applied.

Times: Enter the time you want your policy to be applied.

Websites Blocking by URL Address: You can block access to some websites by entering the URL.

Websites Blocking by Keyword: You can block access to Web pages by keywords contained in them.



Create an Internet Access Policy

1. Select one from the Internet Access Policy drop-down menu.
2. To enable this policy, click the radio button next to Enable.
3. Enter a policy name in the field provided.
4. Click the "Edit PC List" button, and the "PC List" page appears. Enter the PC to which the policy is applied. You can use the MAC address or PC address to specify the PC. If you want this policy to be applied to a group of PCs, you can enter a group of IP address ranges, and after modifying the page, click "Apply Settings" to save the

changes, or click "Cancel Changes" to complete the changes then close this window.

5. Determine when this policy will take effect. Select a specific day for the policy to take effect or select "Daily" and then enter a specific time period for this policy to take effect, or select "24 hours".
6. To deny or only allow access to websites at specific URL addresses, enter each URL address in the separate field next to "Website URL Addresses".
7. If you want to deny or only allow access to websites with specific keywords, enter each keyword in a separate field in the "Site Keywords" narration.
8. Click the "Apply Settings" button to save the policy settings, if you want to cancel the policy settings, click the "Cancel Changes" button.

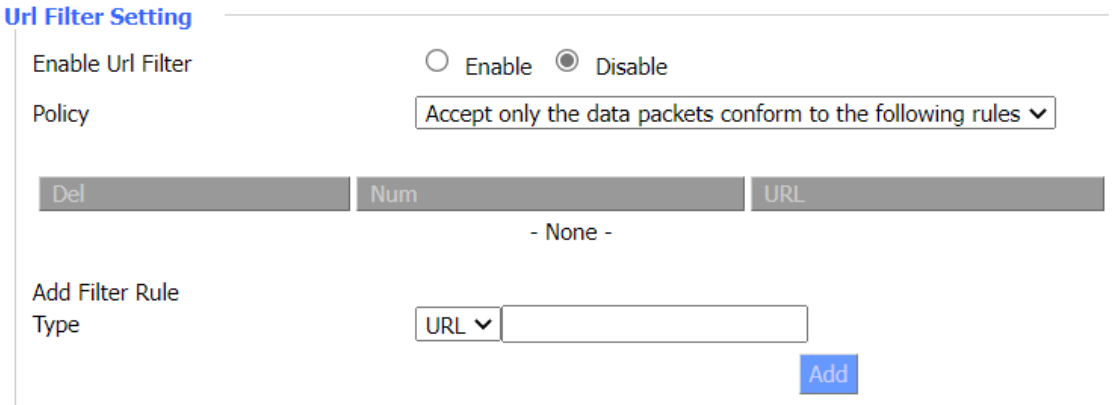
Note:

1. The factory default value of the policy rule is "Filter". If the user selects the default policy rule to be "Deny", edit the relevant policy to save or save the settings directly. If the strategy you edited is the first, it will automatically become the second after saving, and if it is not the first, it will be saved with the original number.
2. The router itself does not have a battery to keep the clock running. Powering off the router or restarting the router will temporarily invalidate the router clock. After the router fails, if the NTP time server cannot be automatically synchronized, the time needs to be recalibrated to ensure the correct execution of the relevant "control by time period" function.

3.3.6.2 URL Filter

If you want to prevent some clients from accessing specific external domain names, such as www.sina.com. This can be achieved through the URL filtering function.

URL Filter Setting



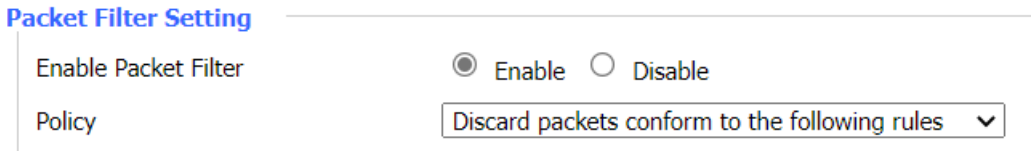
Accept only the data packets conform to the followin rules: Only allow access to matching URL addresses.

Discard packets conform to the following rules: Only accept network addresses that meet the custom rules, and discard all other URLs.

3.3.6.3 Packet Filter

If you want to block certain packets from entering the Internet through the router, or block certain packets from the Internet, you can do so through filters.

Packet Filter Setting

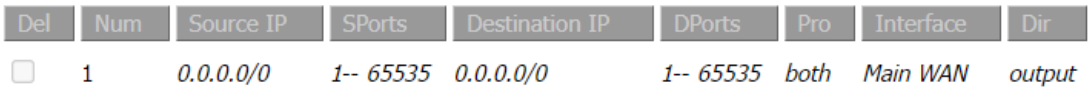


Enable Packet Filter: Whether to enable the packet filtering function.

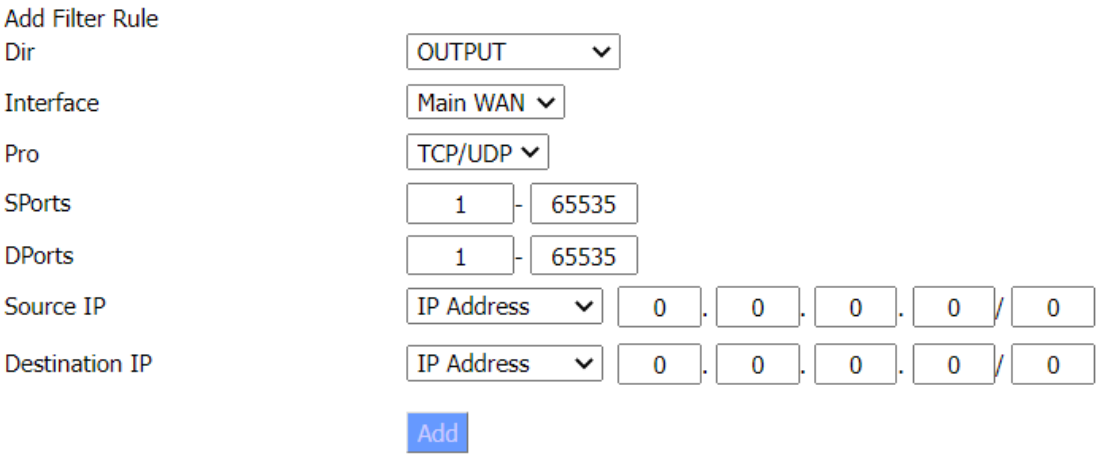
Policy

Discard packets conform to the following rules: drop packets matching custom rules, accept all other packets.

Accept only the data packets conform to the following rules: Receive only packets matching the custom rules, discard all other packets.



The custom packet filtering rules list will list the set packet filtering rules. If you want to delete one of the items, select the corresponding item, check the **"Delete"** button, and then click the **"Save"** button.



Add Filter Rule

Add custom packet filtering rules. "Source Port", "Destination Port", "Source Address", "Destination Address" must be filled in at least one item.

Dir

Input: The data packet goes from the WAN port to the LAN port.

Output: Data packets from the LAN port to the WAN port.

Pro: The protocol type of the packet.

SPorts: The source port of the packet.

DPorts: The destination port of the packet.

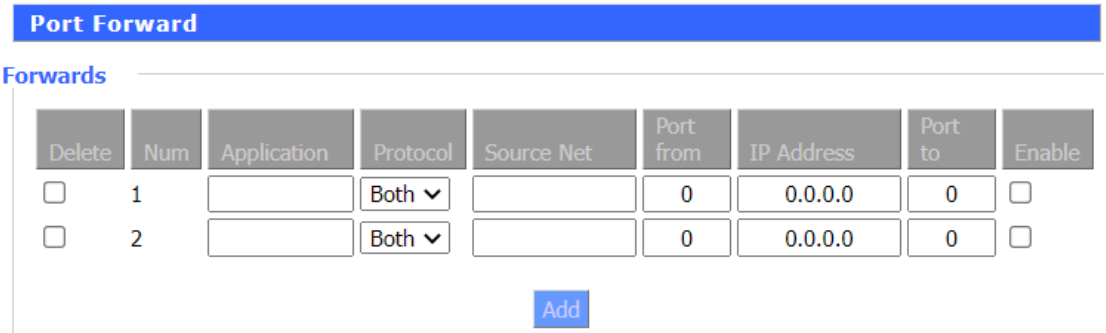
Source IP: The source IP address of the packet.

Destination IP: The destination IP address of the data packet.

3.3.7 NAT

3.3.7.1 Port Forwarding

Port forwarding is used to set up public services on the network, such as web servers, ftp servers, or other dedicated internet applications (a dedicated internet application is any application that uses internet access to use functionality).

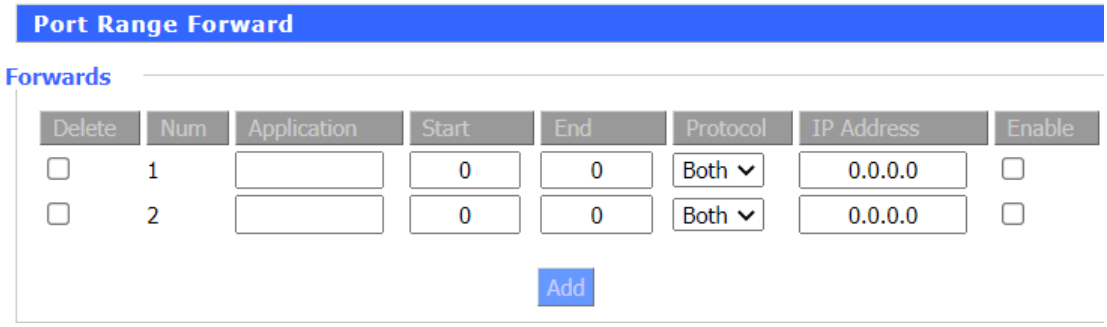


Application: Enter the name of the application in the field provided by the application.
Protocol: Choose UDP or TCP protocol for each application, choose two protocols when both are at the same time.
Source Net: Fill in the IP address of the Internet user in this field.
Port from: Enter the external port number used by the service in this field.
IP Address: Enter the intranet IP address of the server you want internet users to access.
Port to: Enter the internal port number used by the service in this field.
Enable: Check the Enable box to enable the multi-port forwarding service you have defined. The default configuration is disabled (not selected).

After completing the page modification, click the **"Apply Settings"** button to save the changes, or click the **"Cancel Changes"** button
to cancel the modification, the help information is on the right, for details, click **"More"**.

3.3.7.2 Port Range Forwarding

Some applications may require specific port ranges to be forwarded to function properly, and when a request for a port range is made from the Internet, the router sends this data to the designated computer. For security reasons, it may be desirable to limit port forwarding to only those ports that are in use, and if the port forwarding is no longer used, it is recommended to uncheck the "Enable" checkbox to temporarily disable the port forwarding.

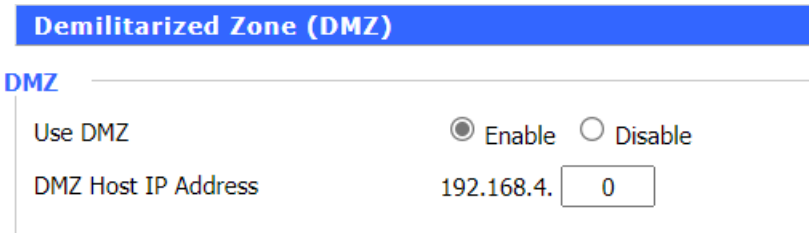


Application: Enter the name of the application in the field provided by the application;
Start: Enter the start port number of the port forwarding range;
End: Enter the end port number of the port forwarding range;
Protocol: Choose UDP or TCP protocol for each application, and choose two protocols when both are at the same time;
IP Address: Enter the intranet IP address of the server you want Internet users to access.
Enable: Check the Enable box to enable the multi-port forwarding service you have defined. The default configuration is disabled (not selected).

After completing the page modification, click the **"Save"** button to save the changes, or click the **"Cancel Changes"** button
to cancel the modification, the help information is on the right, for details, click **"More"**.

3.3.7.3 DMZ

The DMZ function allows a network user to be exposed to the Internet to use certain services. A DMZ host forwards all ports to one computer at the same time, port forwarding is more secure because only the ports you want are open, while a DMZ host opens all ports, exposing the computer to the Internet.



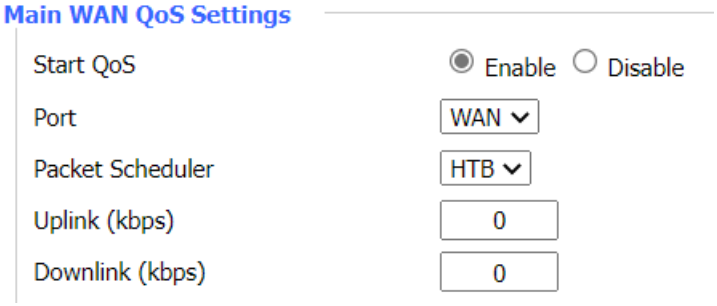
To enable the DMZ feature, select Enable, then enter the computer's IP address in the "DMZ Host IP Address" field.

After completing the page modification, click the **"Save"** button to save the changes, or click the **"Cancel Changes"** button
to cancel the modification, the help information is on the right, for details, click **"More"**.

3.3.8 QoS settings

3.3.8.1 Basic

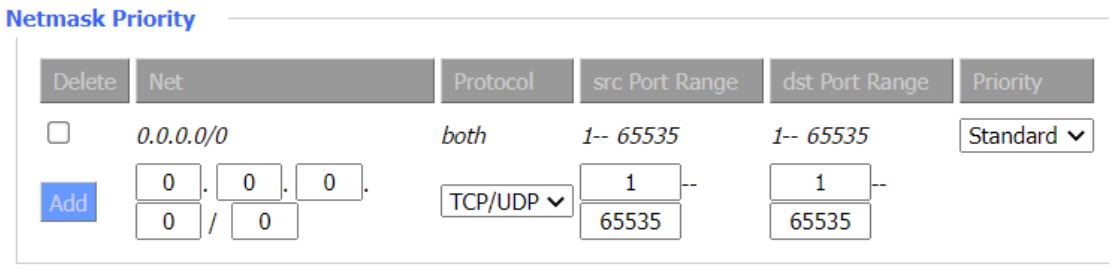
Using the QOS function can limit upload and download traffic separately, and can assign priority to specific IP or MAC.



Uplink (kbps): Fill in the bandwidth you allocate to upload in this column. In actual use, it is generally 80% to 90% of the maximum bandwidth you have.
Downlink (kbps): Fill in the bandwidth you allocate to download in this column. In actual use, it is generally 80% to 90% of the maximum bandwidth you have.

3.3.8.2 Classification

Netmask Priority



You can specify a priority order for all traffic to a given IP address or IP range.

Priority description: This system provides five priorities, of which the "unrestricted" priority is independent of the other four priorities, the other four priorities are: high priority (Premium), priority (Express) , Standard, and Bulk.
Unrestricted: A data stream at the Exempt level, its bandwidth is only limited by hardware, and the relationship between the unrestricted bandwidth and the other four priorities is as follows:

Let the total upload bandwidth be Max_Up, the total download bandwidth be Max_Down, the upload limit in "QOS Settings" is Uplink, the download limit is Downlink, and the traffic rates of unrestricted data streams are Exempt_Rate_Up and Exempt_Rate_Do.

Then the total upload bandwidth of other priorities is: mini(Max _Up –

Exempt_Rate_Up, Uplink);

The total download bandwidth for other priorities is: mini (Max _Downlink– Exempt_Rate_Do, Downlink).

The remaining four priorities

After the unrestricted data stream is sent, the remaining bandwidth of the system is allocated by the remaining four priority data streams according to a certain proportion. Assuming that the remaining upload bandwidth is 1000kbps and download is 1000kbps, there are four data streams at this time. The levels are high priority, priority, standard, and low, respectively, then the upload and download bandwidths of each data stream are as follows:

High priority: (75/100) * Uplink; (75/100) * Downlink

Priority: (15/100)*Uplink; (15/100)*Downlink

Standard: (10/100)*Uplink; (10/100)*Downlink

Low: 1000bit (almost 0); 1000bit (almost 0);

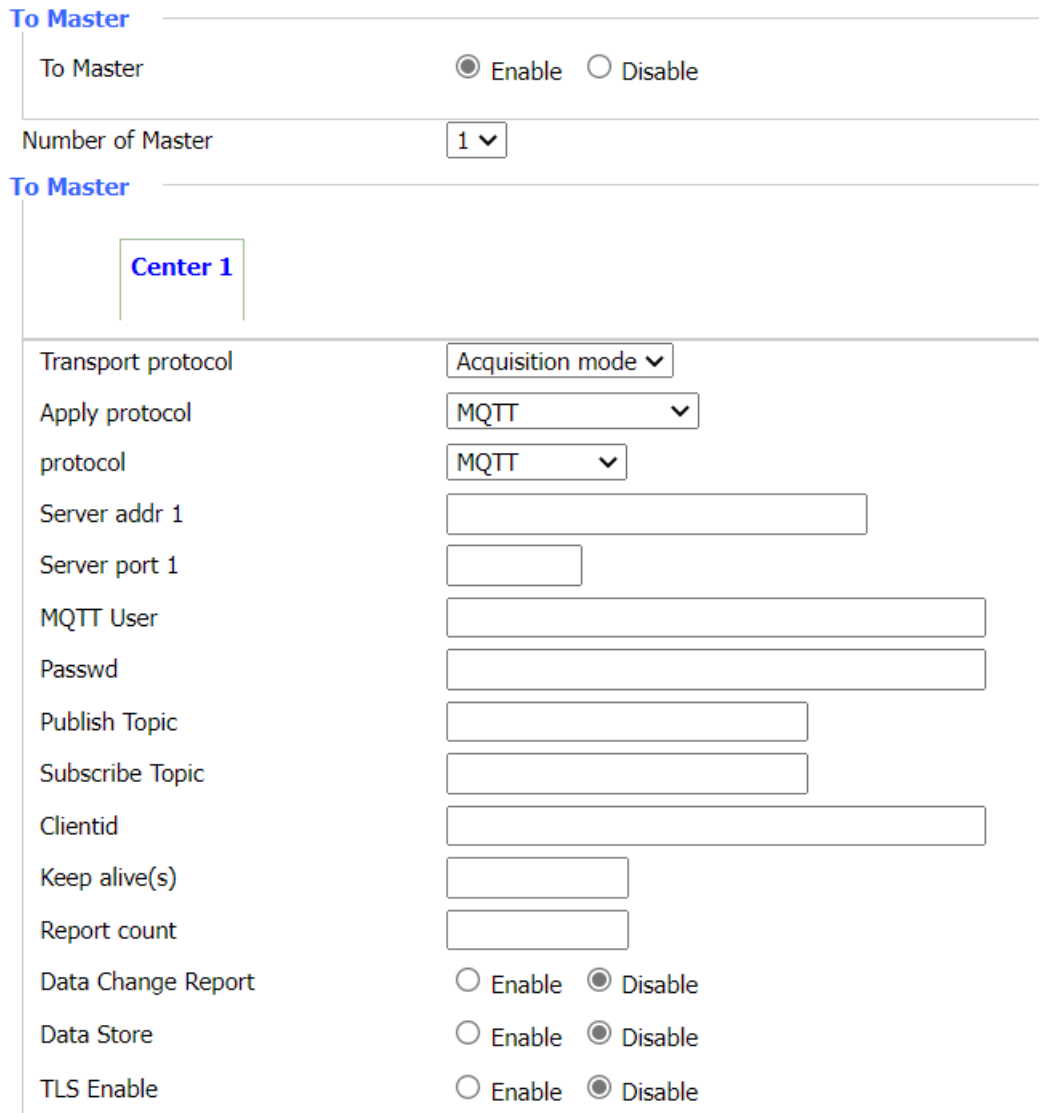
For low priority, the upload and download rates are both 1000bit, and it is its turn when the data streams of other priorities are sent;

When there is only one level of data flow, the bandwidth of the data flow is only limited by the upload and download limits in "QOS Settings";

Note: When a connection meets the control conditions in both MAC priority and netmask priority, the rule added first shall prevail.

3.3.9 Application

3.3.9.1 Protocol Conversation



To Master: Open or enable the current application of the entire smart function gateway.

Number of Master: Configure the number of servers.

Server addr 1: The main configuration is to fill in the ip address of the server. When multiple servers are selected, configure the corresponding ip address of each.

Port: Configure the port of the server. When multiple servers are selected, configure the corresponding port number of each server.

Protocol: It mainly configures some protocols related to communication with the server cente. The default MQTT protocol is used for this configuration.

MQTT User: The account used to provide user authentication.

Passwd: The password used to provide user authentication.

Publish Topic: Used to set the topic content to be published.

Subscribe Topic: Used to set the topic content that needs to be subscribed.

Clientid: Each MQTT connection requires a unique client ID, and the connection ID needs to be configured here.

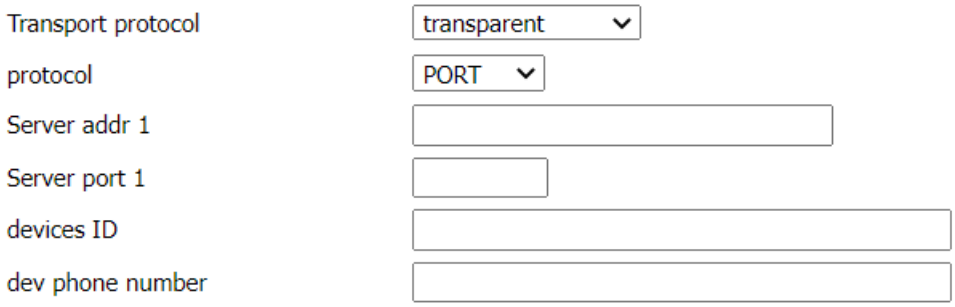
Keep alive(s): The time interval for data reporting.

Report count: the number of data reported each time.

Data Change Report: It is used to configure whether a data change is reported immediately, instead of waiting until the reporting period arrives, which is equivalent to reporting a piece of information immediately when the data changes.

Data Store: Whether the data needs to be cached to related storage devices such as TF card.

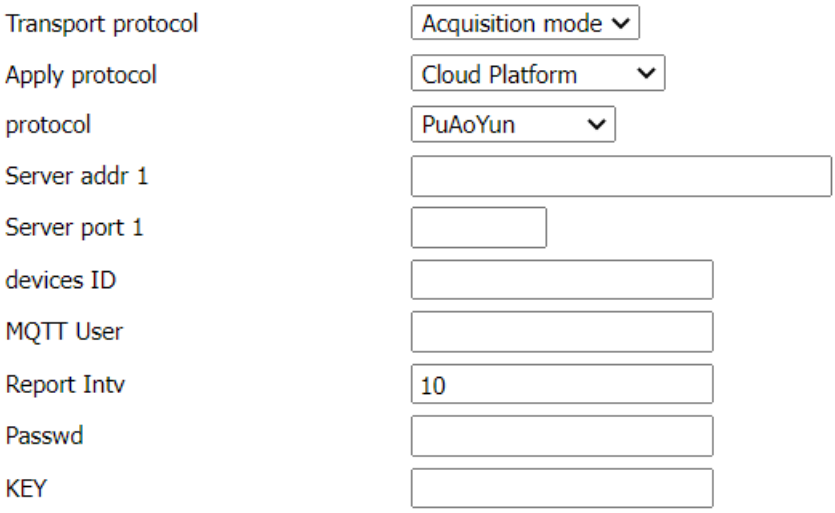
TLS Enable: Whether to encrypt the data, encrypt it according to the selected encryption method.



Transmission protocol: port mode.

Devices ID: The ID of the device that needs to communicate.

Dev phone number: The phone number of the sim card of the communication device.



Transmission protocol: PuAoYun.

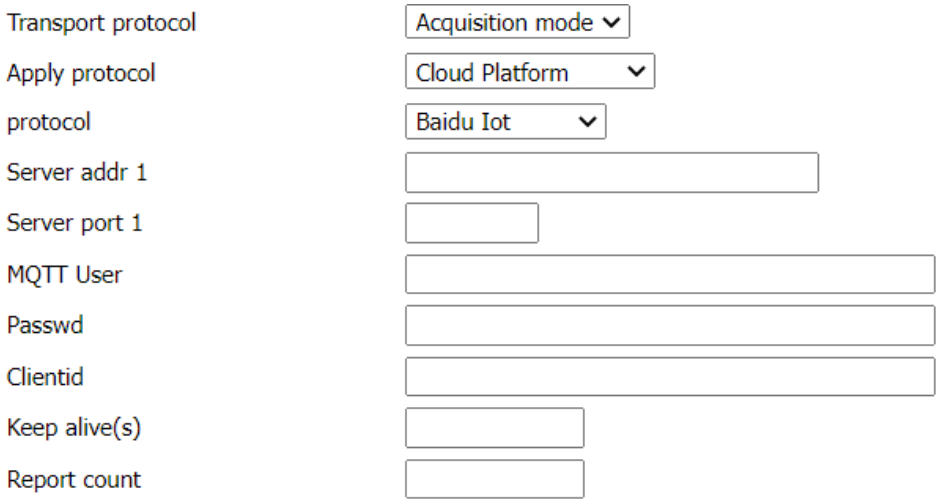
Devices ID: The ID number required by the device connected to the cloud.

MQTT User: the account required for mqtt connection.

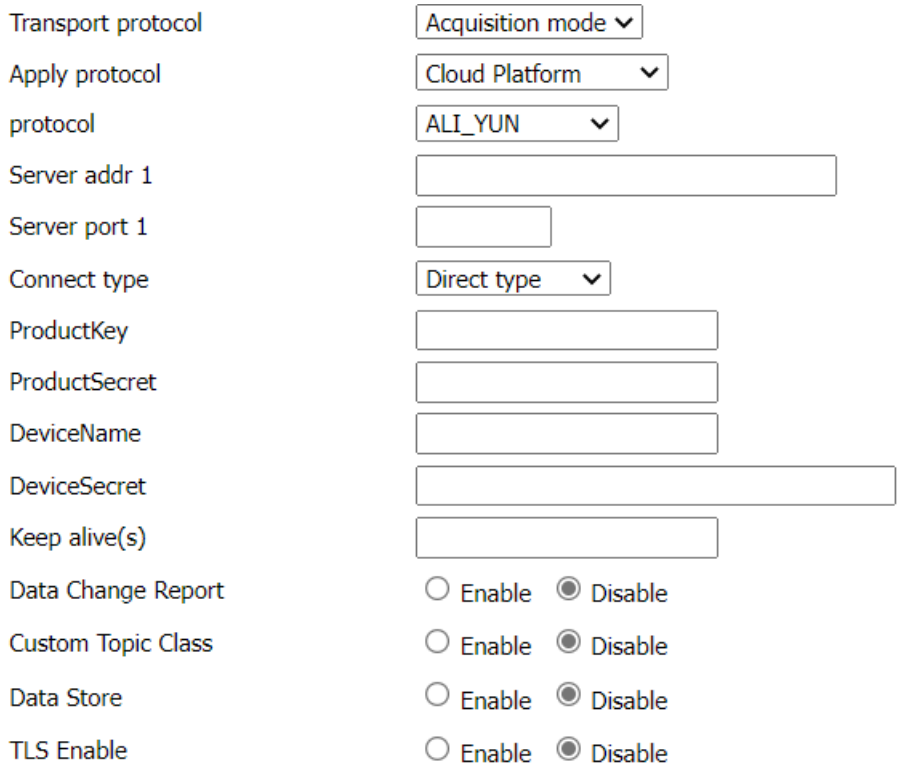
Report Intv: the periodic interval of data reporting.

Passwd: The password required for the mqtt connection.

Key: The secret key required to connect to the platform.



Protocol: Baidu Iot.
Server addr1: Baidu Cloud's server IP address.
MQTT User: The username required to connect to the platform.
Passwd: The password required to connect to the platform.
Clientid: The ID number required by the device connected to the cloud.
Keep alive(s): the interval time for data transmission.



Protocol: ALI_YUN.
Connection type: direct connection type or gateway type, used for direct data transmission or forwarding.
ProductKey: Product key.

ProductSecret: Product encryption.

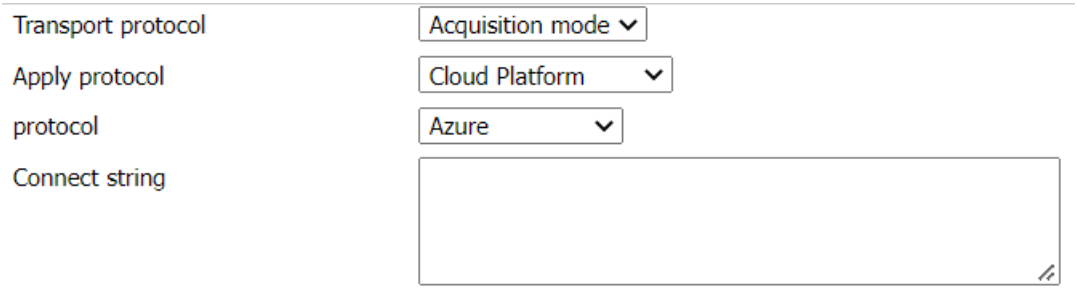
DeviceName: Device name.

DeviceName: Device encryption.

Keep alive(s): The time interval for data upload.

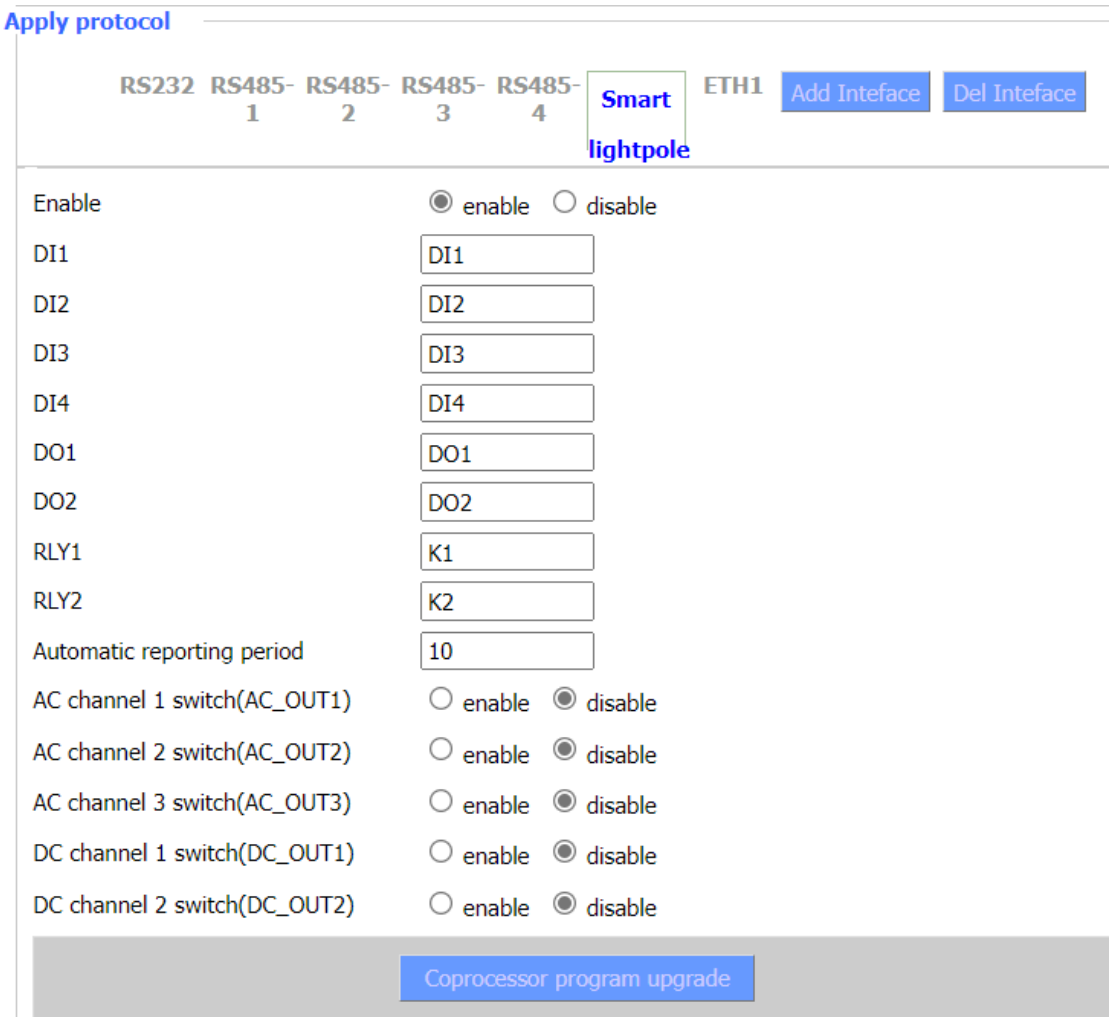
Data Change Report: Whether to report the data to the cloud immediately when the data changes.

Custom Topic Class: To fill in the topic for publishing and subscribing.



Transport Protocol: Azure (Microsoft Cloud).

Connect string: The string required to connect to Azure.



Interface selection and mode selection: used to select and configure the related COM port and LAN port, as well as some parameters set in the smart light pole to communicate with the coprocessor.

DI1: Input signal 1.

DO1: Output signal 1.

RLY1: Relay 1 output.

RLY2: Relay 2 output.

Automatic reporting period: The time interval at which the page collects data from the coprocessor. By default, it is not collected in real time. After it is turned on, the data is collected once every 10s by default. It can also be set as required.

AC channel 1 switch: used to control the closed state of a relay switch of the mcu AC channel, and the delivered field is AC_OUT1.

AC channel 2 switch: used to control the closed state of the MCU AC channel 2 relay switch, and the delivered field is AC_OUT2.

AC channel 3 switch: It is used to control the closed state of the MCU AC channel three relay switch, and the delivered field is AC_OUT3.

DC channel 1 switch: used to control the closed state of the MCU DC channel 1 relay switch, and the field to be sent is DC_OUT1.

DC channel 2 switch: used to control the closed state of the mcu DC channel 2 relay switch, and the delivered field is DC_OUT2.

Coprocessor program upgrade: upgrade the firmware of the mcu module. After the button is triggered, it will enter the upgrade process. After the upgrade is completed or canceled, click the continue button.

3.3.10 Management

3.3.10.1 Management

This page allows network administrators to manage specific router functions to ensure access and security.

The new password must be no longer than 32 characters and must not contain any spaces. The confirmation password should be the same as the new password you set, otherwise the setting will be unsuccessful.

Warn:

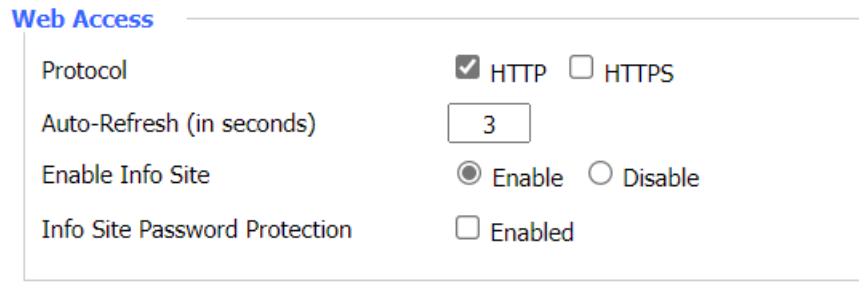
The default username is: admin.

We strongly recommend that you modify the factory default password admin, so that all users who try to access and modify the router should only be able to access and use the

router by entering the correct router password.

Web Access

This feature allows you to manage the router using HTTP protocol or HTTPS protocol. If you choose to disable this feature, a manual restart will be required. You can also activate or deactivate the router's information web pages. That way you can password protect this page (enter the correct username and password).

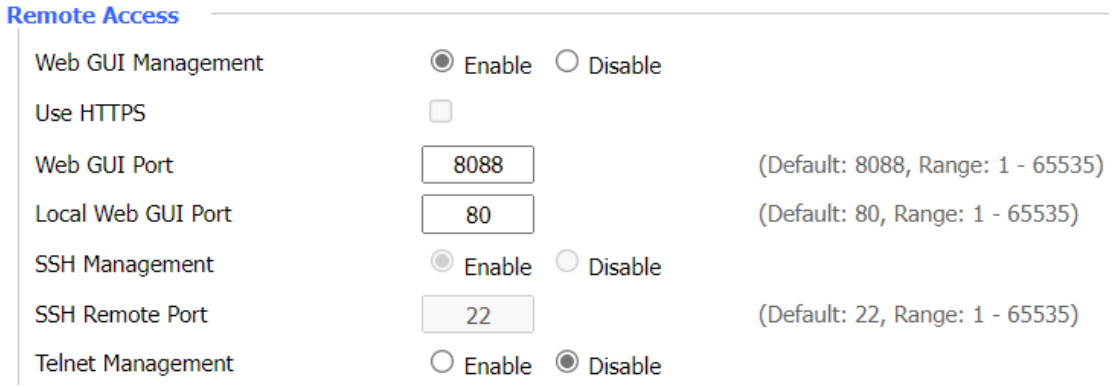


Protocol: The protocols supported by web pages include HTTP and HTTPS

Auto-Refresh (in seconds): Adjust the web interface auto refresh interval. 0 means disable this feature.

Enable Info Site: whether to enable display system information page before login

Info Site Password Protection: whether to enable the system information site password protection function



Web GUI Management: This feature allows you to manage the router from a remote location via the internet. To disable this feature, keep the default setting, which is disabled. To enable this feature, select Enable and use the designated port on your computer (8080 by default) to remotely manage the router. If you haven't set a password, you must also set the default password for your own router.

To remotely manage the router, enter http://xxx.xxx.xxx.xxx:8080 (x represents the router's Internet IP address, 8080 represents the designated port) in your web browser's address bar. You will be asked to enter your router's password.

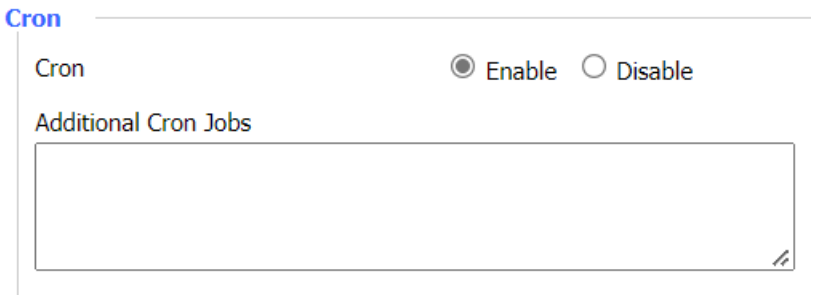
If you use HTTPS, you need to specify the URL as https://xxx.xxx.xxx.xxx:8080 (not all firmwares support SSL rebuild)

SSH Management: You can enable SSH to remotely and securely access the router. Note that more information on the settings of the SSH daemon can be found on the Services page.

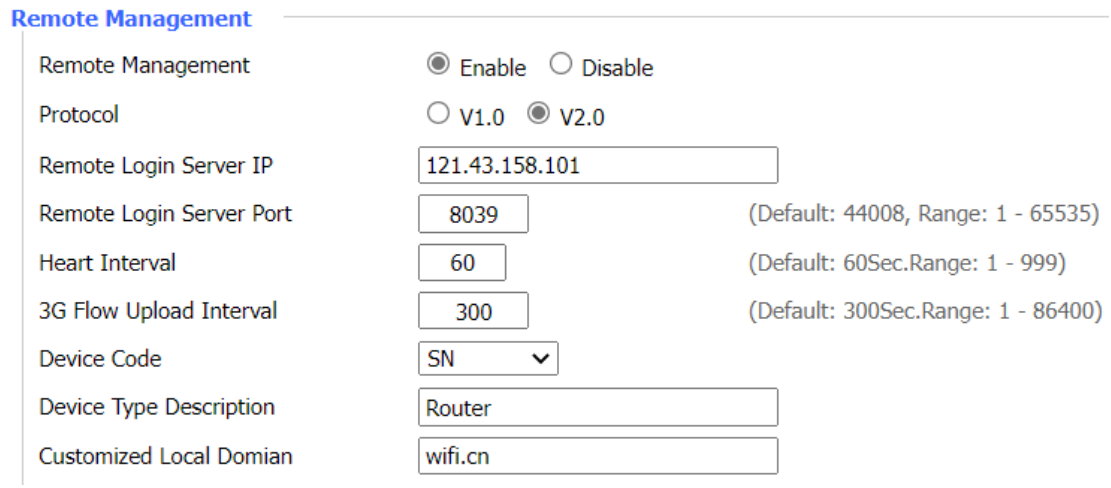
Warn:

If remote router access is enabled, anyone who knows the router's Internet IP address and password will be able to change the router's settings.

Telnet Management: Enable or disable the remote Telnet function.



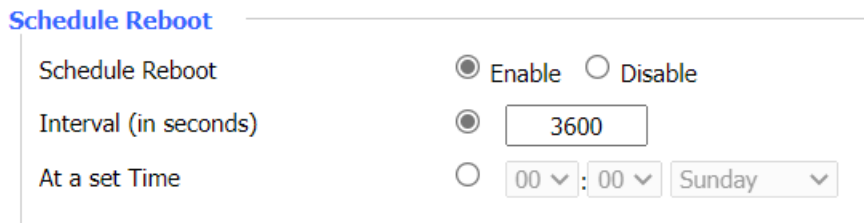
Cron: The subsystem of cron, which is the Linux command you plan to execute. You need to use the command line or startup script in actual use.



Remote management: Monitor and manage this router, configure parameters, and update WIFI advertisements through a custom-developed remote management server.

3.3.10.2 Keep Active

Schedule Reboot



You can set a schedule to restart the route:

Restart after timing xxx seconds

Reboot on a specific date time, week or day.

Warn:

Choose when to restart the router. In the Admin tab, the Cron option must be enabled.

3.3.10.3 Command

Instructions: You can run the command line through the web interface. Fill in the text area with your command and click the Run Command button to submit.

Run Command: You can run the command line through the web interface. Fill in the text area with your command and submit it by clicking the Run Command button.

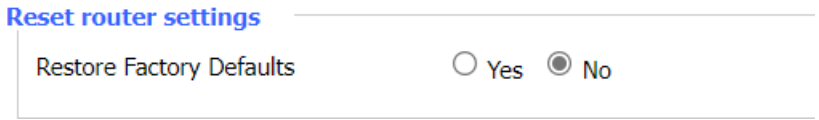
Save Startup: You can save certain command lines that are executed when the router is started. Enter the command (only one command line) into the text area and click Save as Startup Command.

Save Shutdown: You can save certain command lines that are executed when the router is shut down. Enter the command (only one command line) into the text area and click Save as Shutdown Command.

Save Firewall: Every time you start the firewall, it can run some custom iptables commands. Enter the firewall command (only one command line) into the text area and click Save as Firewall Command.

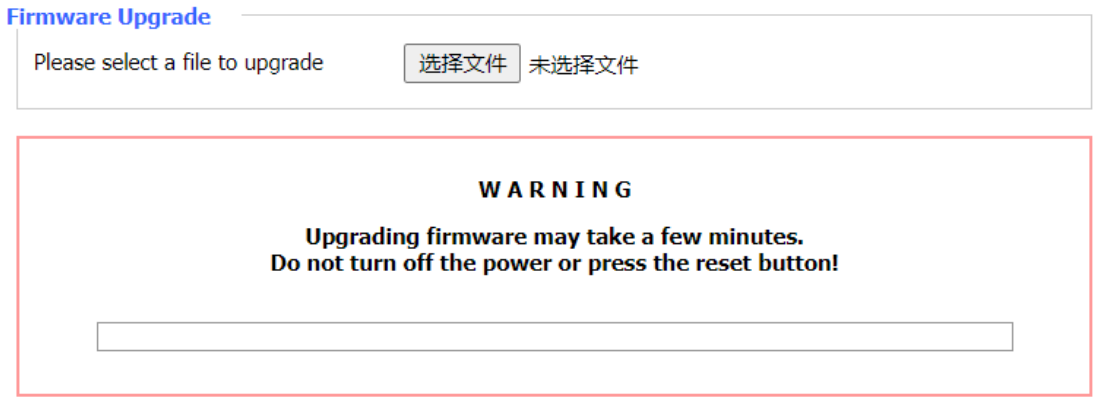
Save Custom Script: Custom directives are stored in the /tmp/custom.sh file. You can receive run or use cron to call it. Enter the script's command (only one command line) into the text area and click Save as Custom Command.

3.3.10.4 Factory default



Restore factory defaults: Click the **"Yes"** button and save the settings to restore all configurations to factory defaults. All settings you made will be lost when you revert to default settings. The default configuration for this feature is **"No"**. For more information, please click **"More"**.

3.3.10.5 Firmware Upgrade



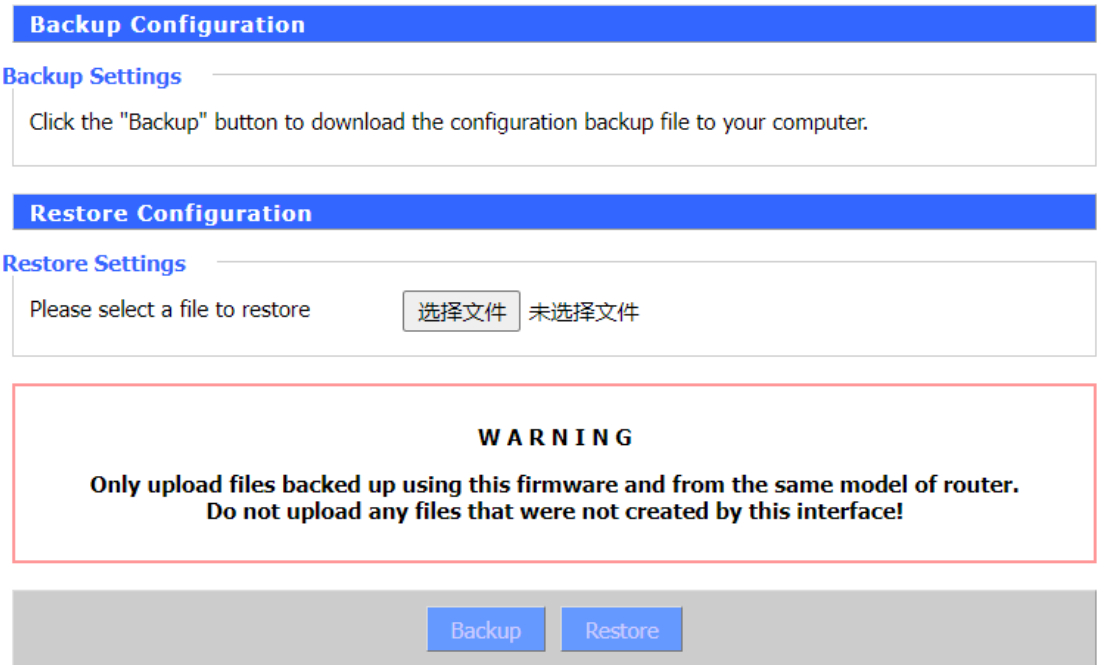
Firmware Upgrade: New firmware can be loaded onto the router. The new firmware version will be published on www.four-faith.com and can be downloaded free of charge. If there is no problem with the router, there is no need to download a newer firmware version unless the new version includes the new features you want to use.

Note: When upgrading the router's firmware, its configuration settings may be lost, so make sure to back up the router's settings before upgrading the firmware.

Click Browse, select the firmware file to be upgraded, and then click the Upgrade button to start the firmware upgrade. It will take a few minutes to upgrade the firmware, please do not power off or press the reset button.

3.3.10.6 Backup

This page is used to backup or restore the router's configuration files.



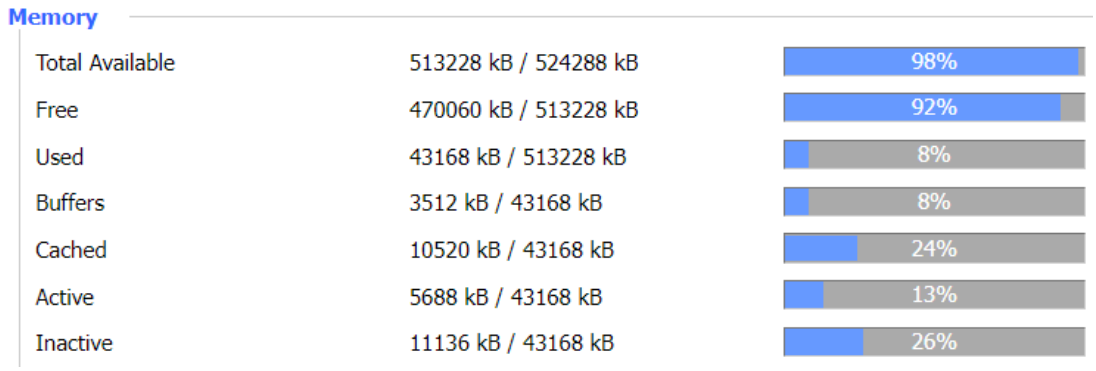
To back up the router's configuration files, click the **"Backup"** button. After that, follow the on-screen instructions.

To restore the router's configuration file, click the **"Browse"** button, and after locating the backup file, follow the on-screen instructions. Select the backup file and click the **"Restore"** button.

3.3.11 Status

3.3.11.1 Router

Router Name: the name of this router, which can be modified in the basic settings
Router Model: the model of the router, which is fixed by the system and cannot be modified
Firmware Version: The firmware version number of the software, which is fixed by the system and cannot be modified
MAC Address: It reflects the MAC address of the WAN, which can be modified in the setting of the MAC address clone
Host Name: The hostname of the router, which can be modified in the basic settings
WAN Domain Name: The domain name of the WAN port, which can be modified in the basic settings
LAN Domain Name: The domain name of the LAN port, which is fixed by the system and cannot be modified
Current Time: The system's local time
Uptime: The time the system is powered on



Total Available: All available RAM size (i.e. physical memory minus some reserved bits and the kernel's binary code size)

Free: Unused memory is reserved by the system. If the memory is less than 500kB, it will restart.

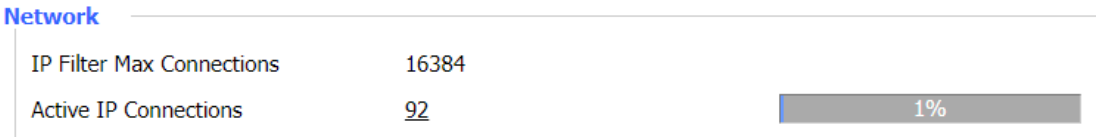
Used: used memory, all available memory minus free memory

Buffers: The memory used by the buffer, the total memory minus the allocated memory is the buffer memory.

Cached: The amount of memory used by the cache memory

Active: The size of the buffer or cache page file that is actively in use

Inactive: The size of the buffer or cache page file that is infrequently used



IP Filter Max Connections: default 4096, which can be managed in

Active IP Connections: real-time detection of the number of active IP connections in the system, if you click it, you can see the following

Active IP Connections 49

No.	Protocol	Timeout (s)	Source Address	Remote Address	Service Name	State
1	TCP	117	192.168.4.110	192.168.4.1	80	TIME_WAIT
2	TCP	117	192.168.4.110	192.168.4.1	80	TIME_WAIT
3	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
4	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
5	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
6	UDP	16	192.168.4.110	192.168.4.1	53	UNREPLIED
7	UDP	22	192.168.4.110	192.168.4.1	53	UNREPLIED
8	TCP	112	192.168.4.110	192.168.4.1	80	TIME_WAIT
9	UDP	16	192.168.4.110	192.168.4.1	53	UNREPLIED
10	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
11	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
12	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
13	TCP	112	192.168.4.110	192.168.4.1	80	TIME_WAIT
14	TCP	115	192.168.4.110	192.168.4.1	80	TIME_WAIT
15	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
16	TCP	115	192.168.4.110	192.168.4.1	80	TIME_WAIT
17	TCP	117	192.168.4.110	192.168.4.1	80	TIME_WAIT
18	UDP	18	192.168.4.110	192.168.4.255	138	UNREPLIED
19	TCP	3599	192.168.4.110	192.168.4.1	80	ESTABLISHED
20	TCP	115	192.168.4.110	192.168.4.1	80	TIME_WAIT
21	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
22	TCP	117	192.168.4.110	192.168.4.1	80	TIME_WAIT
23	TCP	115	192.168.4.110	192.168.4.1	80	TIME_WAIT
24	TCP	112	192.168.4.110	192.168.4.1	80	TIME_WAIT
25	TCP	112	192.168.4.110	192.168.4.1	80	TIME_WAIT
26	TCP	111	192.168.4.110	192.168.4.1	80	TIME_WAIT
27	TCP	112	192.168.4.110	192.168.4.1	80	TIME_WAIT
28	TCP	3599	192.168.4.110	192.168.4.1	80	ESTABLISHED

Active IP Connections: Total active IP connections
Protocol: the protocol of the connection
Timeout: the timeout in seconds for the connection
Source Address: The IP address of the source
Remote Address: The IP address of the remote
Service Name: The service port number to connect to
State: Displays detailed status of active IPs

3.3.11.2 **WAN**

Connection Type	Automatic Configuration - DHCP
Connection Uptime	Not available
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS 1	
DNS 2	
DNS 3	

Connection Type: Include 7 ways: Disable, Static IP, Auto-Config-DHCP, PPPOE, PPTP,

L2TP, 3G/UMTS.

Connection Uptime: the time when connected, if not connected, it will ask "unavailable"

IP Address: the IP address obtained by the WAN port of the router

Subnet Mask: The subnet mask obtained by the WAN port of the router

Gateway: The gateway obtained by the WAN port of the router

DNS1, DNS2, DNS3: The first DNS, the second DNS, and the third DNS obtained by the WAN port of the router

Remaining Lease Time	0 days 00:00:00

Remaining Lease Time: the remaining time for obtaining an IP address in DHCP mode

Signal Status	-113 dBm
Network	NONE

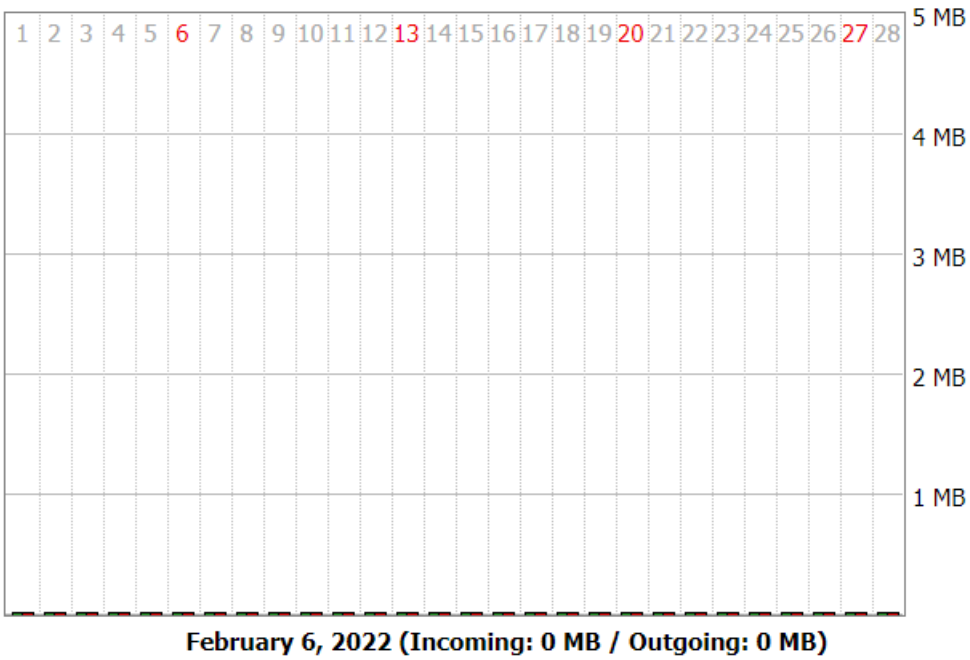
Signal Status: module module signal strength in 3G/UMTS mode

Network: The network type of the module in 3G/UMTS mode

Total Traffic

Incoming (MBytes)	0
Outgoing (MBytes)	0

Traffic by Month



February 6, 2022 (Incoming: 0 MB / Outgoing: 0 MB)

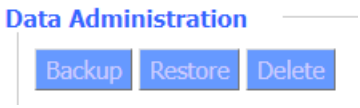
Previous Month Next Month

Total Traffic: Statistics on the traffic used since the last power outage are divided into two directions: download and upload

Traffic by Month: MB of traffic units counted in one month

Previous Month: View the traffic of the previous month

Next Month: View traffic for the next month

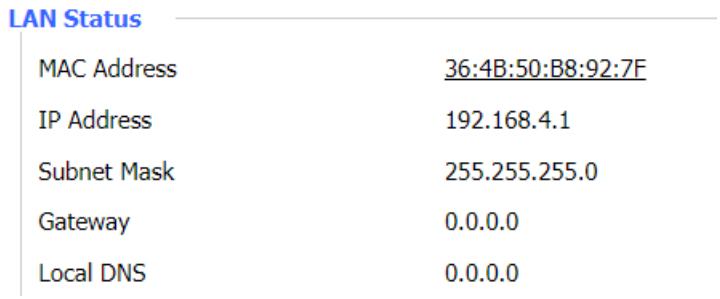


Backup: Backup data traffic statistics

Restore: Restore data traffic statistics

Delete: Delete data traffic statistics

3.3.11.3 LAN



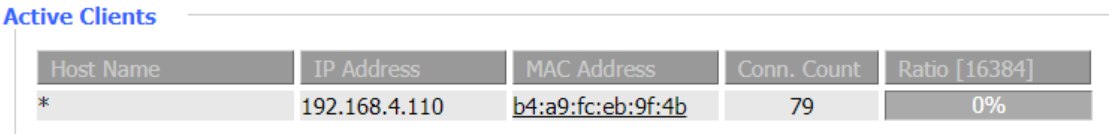
MAC Address: MAC address of the LAN port

IP Address: IP address of the LAN port

Subnet Mask: The subnet mask of the LAN port

Gateway: The gateway of the LAN port

Local DNS: DNS of LAN port



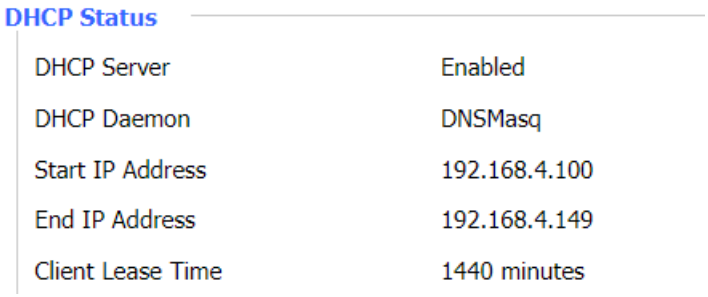
Host Name: The hostname of the LAN port client

IP Address: The IP address of the client

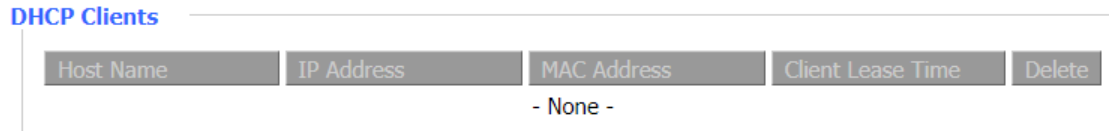
MAC Address: The MAC address of the client

Conn.Count: The number of connections made by the client

Ratio: % of 4096 connections



DHCP Server: whether to enable DHCP server
DHCP Daemon: The protocol distribution used by DHCP mainly includes DNSMasq and DHCPd
Start IP Address: The starting IP address of the DHCP client
End IP Address: The end IP address of the DHCP client
Client Lease Time: The lease time of the DHCP client



Host Name: The hostname of the LAN port client
IP Address: The IP address of the client
MAC Address: The MAC address of the client
Client Lease Time: The time the client leases this IP address
Delete: Click to delete the DHCP client

3.3.11.4 Wireless

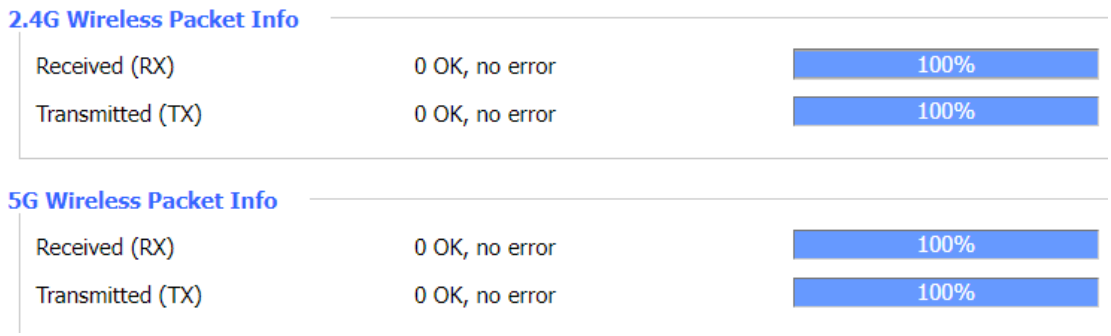
2.4G Wireless Status

MAC Address	36:4B:50:B8:92:81
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	Four-Faith
Channel	1 (2412 MHz)
TX Power	100 mW
Rate	150 Mb/s
Encryption - Interface wl0	Disabled

5G Wireless Status

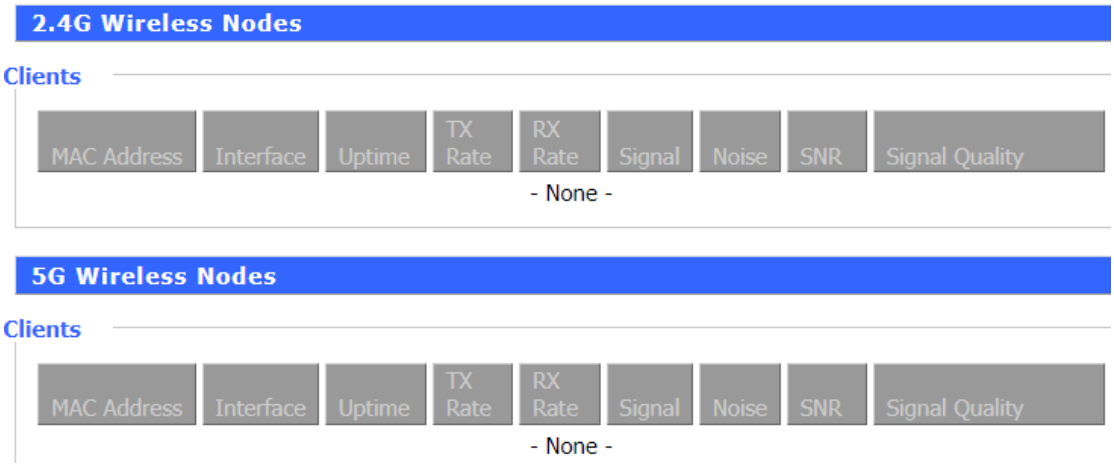
MAC Address	36:4B:50:B8:92:82
WiFi	Radio is On
Mode	AP
Network	Mixed
SSID	Four-Faith_5G
Channel	165 (5512 MHz)
TX Power	100 mW
Rate	Auto
Encryption - Interface wl0_5G	Disabled

MAC Address: The wireless MAC address
WiFi: Displays whether Wi-Fi is enabled
Mode: wireless mode
Network: The mode of the wireless network
SSID: The name of the wireless network
Channel: The channel of the wireless network
TX Power: The reflected power of the wireless network
Rate: The reflection rate of the wireless network
Encryption-interface wl0: whether to encrypt the wl0 interface



Received (RX): Packets that have been received

Transmitted (TX): Packets that have been sent



MAC Address: The MAC address of the wireless client

Interface: The interface of the wireless client

Uptime: Access time for wireless clients

TX Rate: The transfer rate of the wireless client

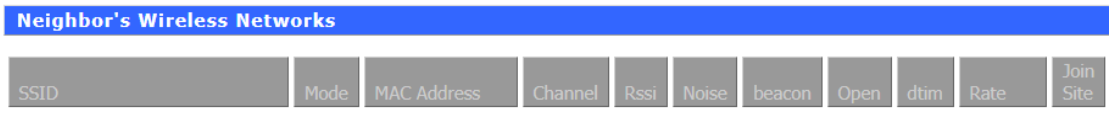
RX Rate: The receive rate of the wireless client

Signal: The signal of the wireless client

Noise: Noise from wireless clients

SNR: Signal-to-Noise Ratio of Wireless Clients

Signal Quality: The signal quality of the wireless client



Neighbor's Wireless Networks: Show other nearby networks

Mode: Proximity wireless working mode

MAC Address: The MAC address of the neighboring wireless

Channel: Nearby wireless channel

Rssi: nearby wireless signal strength

Noise: Nearby wireless noise

Beacon: Proximity wireless signal markers

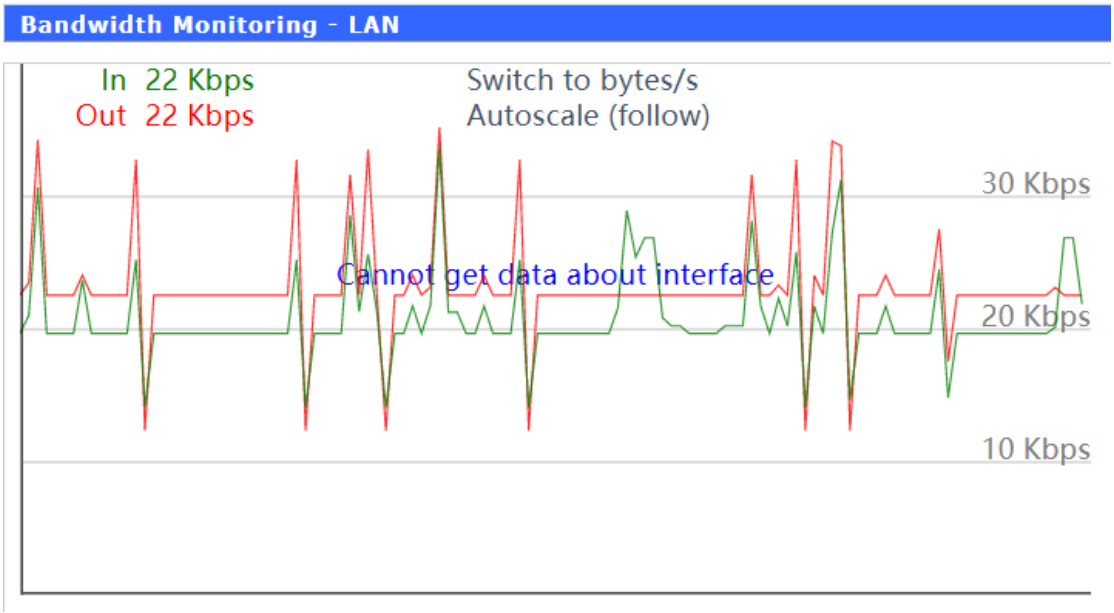
Open: Whether the proximity wireless is on

Dtim: Delivery and transmission indication information of the adjacent wireless

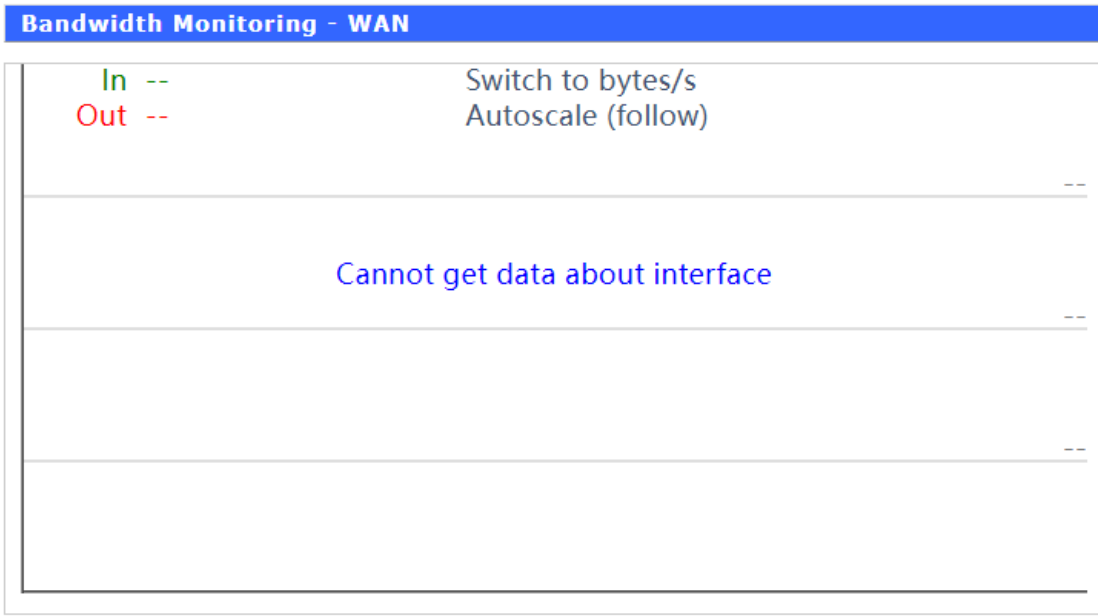
Rate: The speed of the adjacent wireless

Join Site: Click to join a nearby wireless network

3.3.11.5 Bandwidth

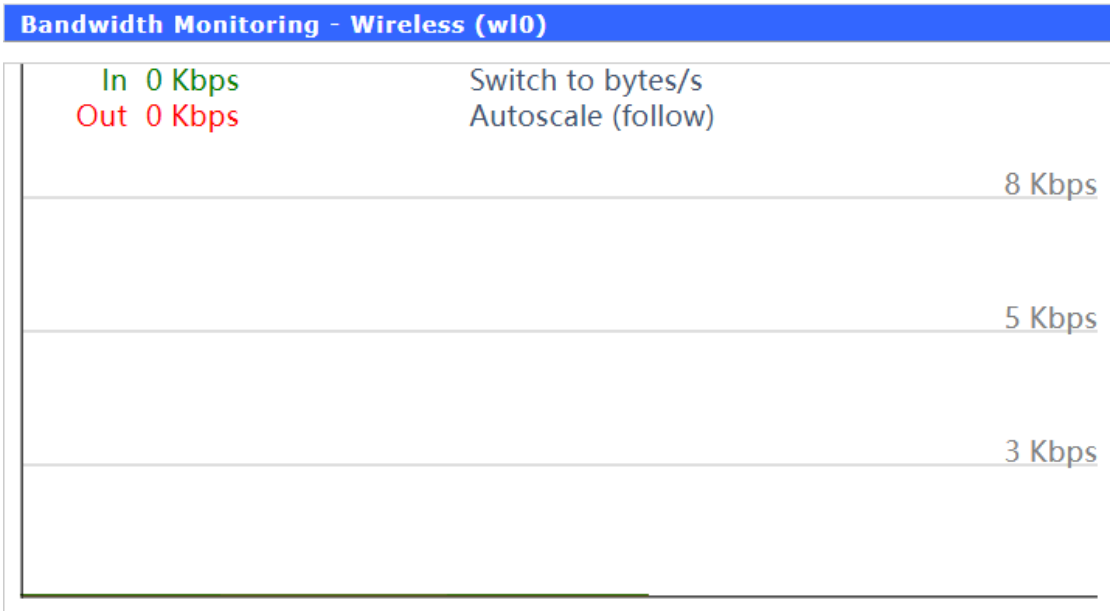


The abscissa of the LAN port's constant detection state diagram represents the code rate of the time ordinate.



The abscissa of the WAN port's time-to-time detection state diagram represents the code

rate of the time ordinate.

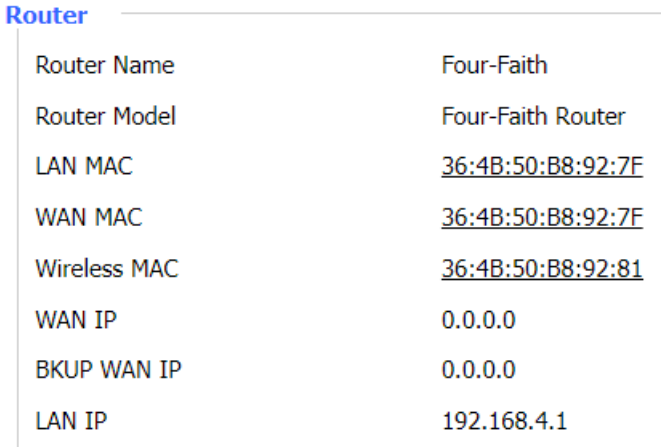


The time-to-time detection state diagram of the wireless network The abscissa represents the code rate of the time ordinate.

Switch to: Click on the label to select the unit (bytes/second or bits/second).

Autoscale: Click the tab to select the type of graph autoscale.

3.3.11.6 System Information



Router Name: The name of the local router

Router Model: the model of the local router

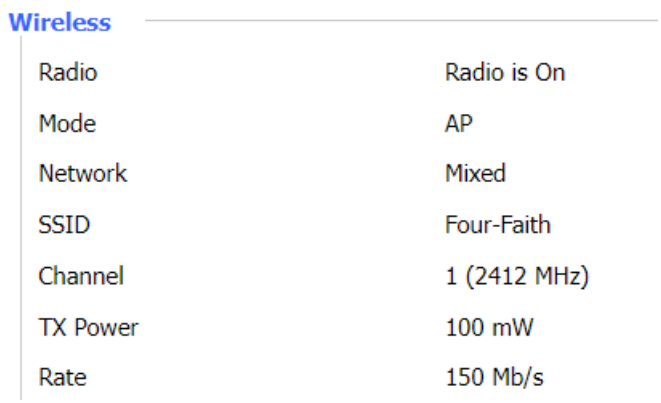
LAN MAC: MAC address of the LAN port

WAN MAC: The MAC address of the WAN port

Wireless MAC: Wireless MAC address

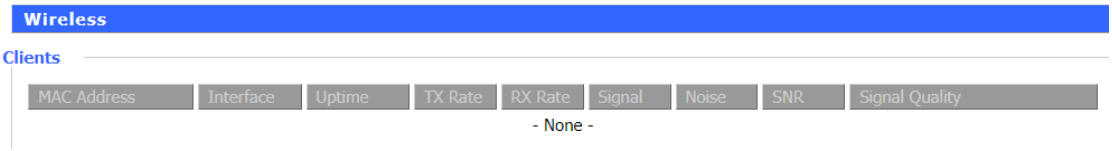
WAN IP: IP address of the WAN port

LAN IP: IP address of the LAN port

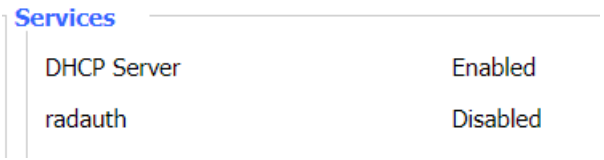


Radio: Displays whether radio is on
Mode: Wireless mode
Network: The mode of the wireless network
SSID: The name of the wireless network
Channel: The channel of the wireless network
TX power: the reflected power of the wireless network
Rate: The reflection rate of the wireless network

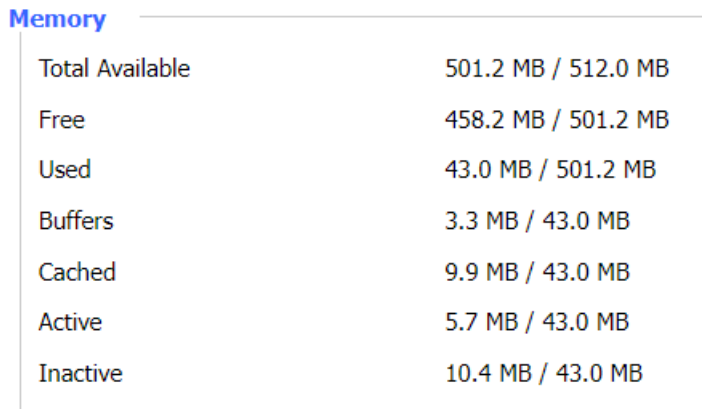
Received (RX): Packets that have been received
Transmitted (TX): Packets that have been sent



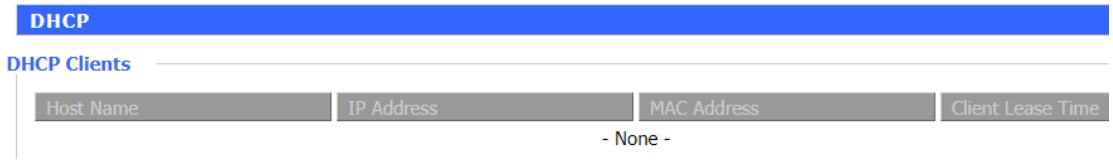
MAC Address: The MAC address of the wireless client
Interface: The interface of the wireless client
Uptime: Access time for wireless clients
TX Rate: The transfer rate of the wireless client
RX Rate: The receive rate of the wireless client
Signal: The signal of the wireless client
Noise: Noise from wireless clients
SNR: Signal-to-Noise Ratio of Wireless Clients
Signal Quality: The signal quality of the wireless client



DHCP server: whether to enable DHCP server
radauth: whether to enable radauth service

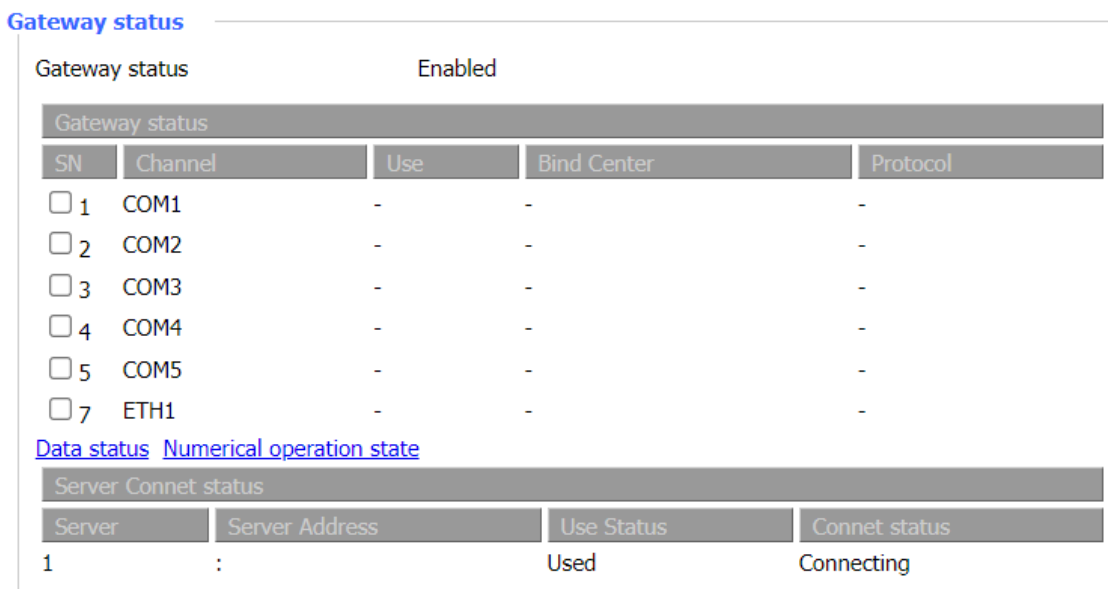


Total Available: All available RAM size (i.e. physical memory minus some reserved bits and the kernel's binary code size)
Free: Unused memory is reserved by the system. If the memory is less than 500kB, it will restart.
Used: used memory, all available memory minus free memory
Buffers: The memory used by the buffer, the total memory minus the allocated memory is the buffer memory.
Cached: The amount of memory used by the cache memory
Active: The size of the buffer or cache page file that is actively in use
Inactive: The size of the buffer or cache page file that is infrequently used



Host Name: The hostname of the LAN port client
IP Address: The IP address of the client
MAC Address: The MAC address of the client
Client Lease Time: The time the client leases this IP address

3.3.11.7 Smart Gataway Status



Gateway status: The current page is displayed when the smart gateway is turned on.

Data status: Enable configuration and data display corresponding to the relevant functions of the smart gateway application in the application.