F-NR200 5G Industrial CPE User Manual

This user manual suits modem as follows:

Model	Description
F-NR200	5G Industrial CPE

Four-Faith

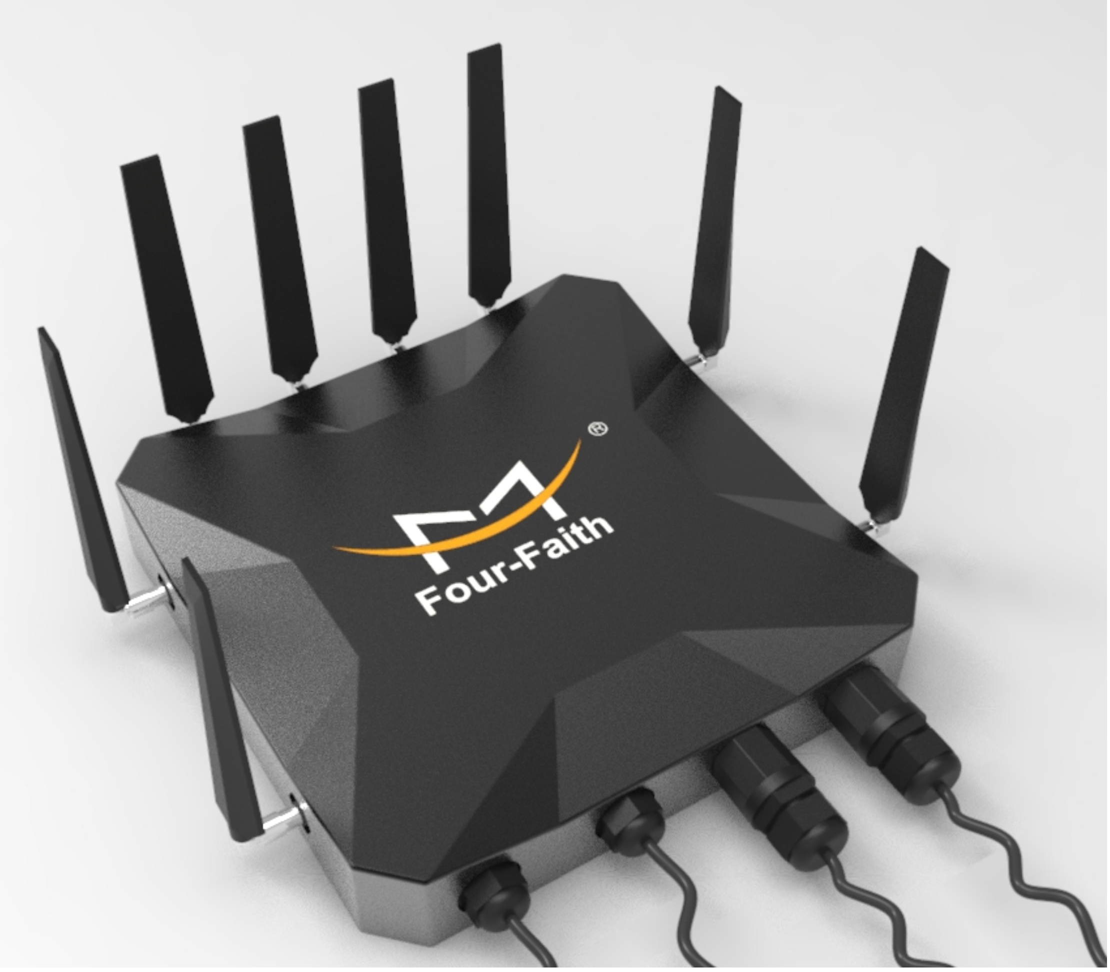
四信

Files Revised Record

Date	Version	Description	Author
2020-12-16	V1.0.0	**Initial version**	XRC

Copyright Notice

Trademark Notice



Note: There may be different components and interfaces in different model,please in kind prevail.

Content

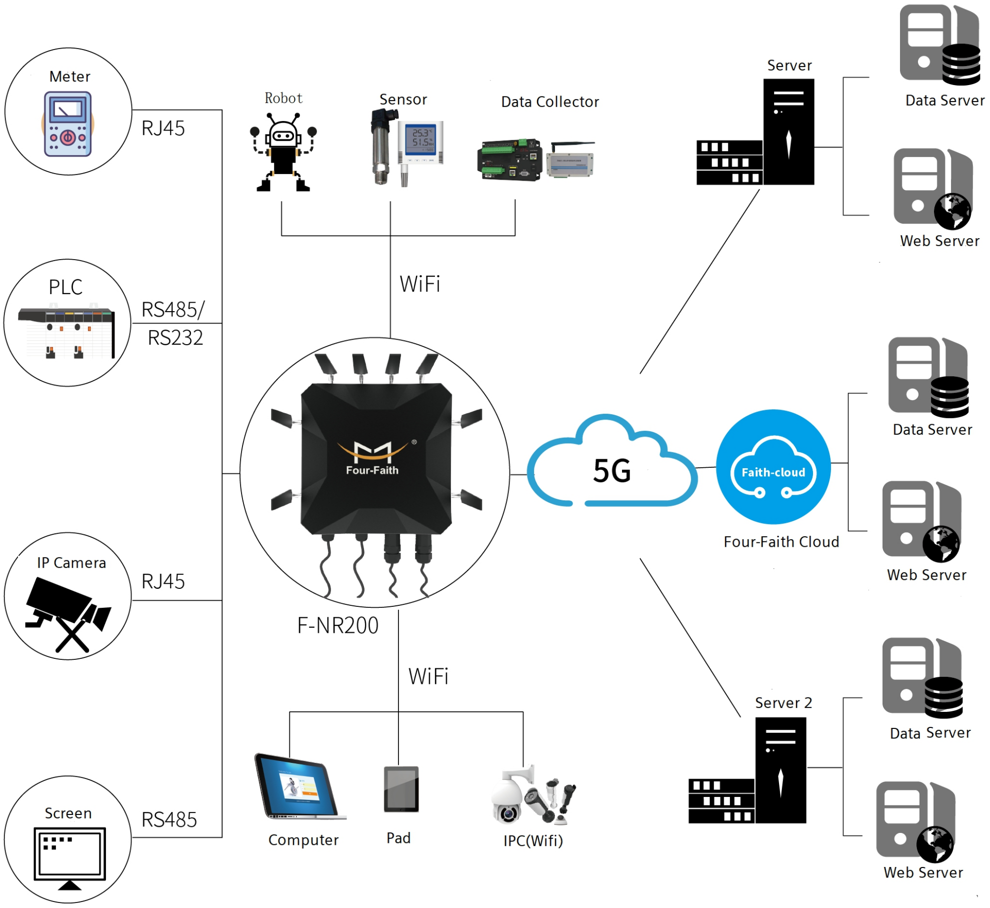
Chapter 1 Product Introduction

1.1 Product description

F-NR200 is a 5G industrial CPE that uses public 3G/4G/5G networks to provide users with wireless long-distance big data transmission functions.

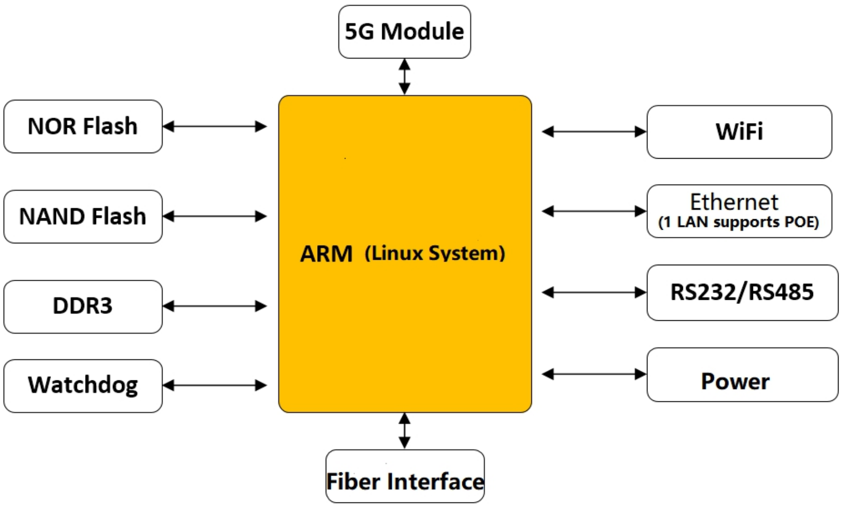
F-NR200 adopts high-performance industrial-grade 32-bit communication processors and industrial-grade wireless modules, with embedded real-time operating system as the software support platform. It provides 1 RS232 (or RS485), 1 Ethernet LAN, and 1 Ethernet WAN, 1 optical fiber interface and support WIFI function, can connect serial device, Ethernet device and WIFI device at the same time, realize data transparent transmission and routing function.

F-NR200 has been widely used in the M2M industry in the IoT industry chain, such as smart grid, smart transportation, smart home, finance, mobile POS terminals, supply chain automation, industrial automation, smart buildings, fire protection, public safety, environmental protection, meteorology , Digital medical treatment, remote sensing survey, military, space exploration, agriculture, forestry, water affairs, coal mine, petrochemical and other fields.



1.2 Working Principle Diagram

5G Industrial CPE working principle diagram is as follows



Chapter 2 Installation

2.1 Overview

The 5G industrial CPE must be installed correctly to achieve the designed function. Usually, the installation of the equipment must be carried out under the guidance of qualified engineers approved by the company.

➢ *Notices:*
Please do no install it with power on.

2.2 Package List

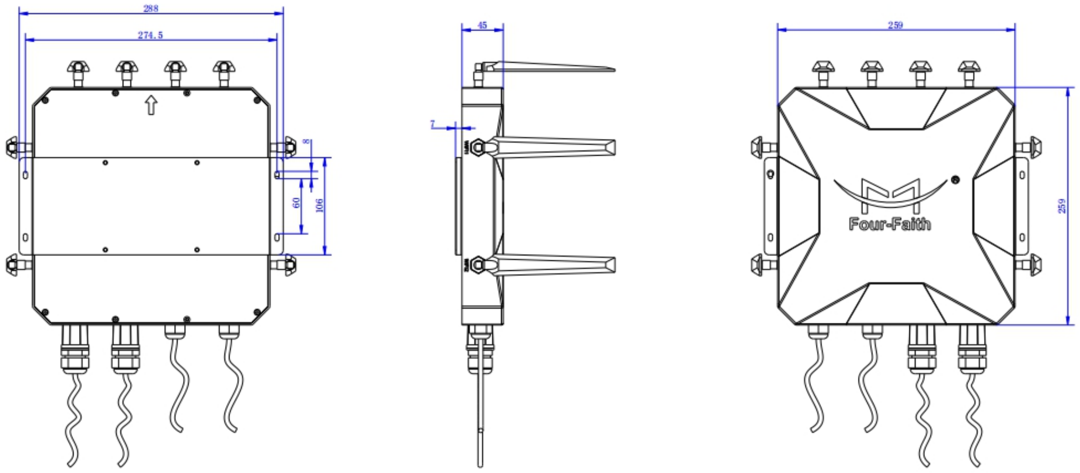
Please keep the packing materials when you unpack the box, so that you can use it when you need to transfer it in the future. The list is as follows:

- ✧ 5G industrial CPE 1unit
- ✧ 5G cellular antenna(SMA male) 4 pieces
- ✧ WIFI antenna(SMA female) 4 pieces
- ✧ Power adapter 1 piece
- ✧ Ethernet cable 1 piece
- ✧ Serial port cable 1 piece
- ✧ Wall mounting plate 1 piece
- ✧ Warranty Card

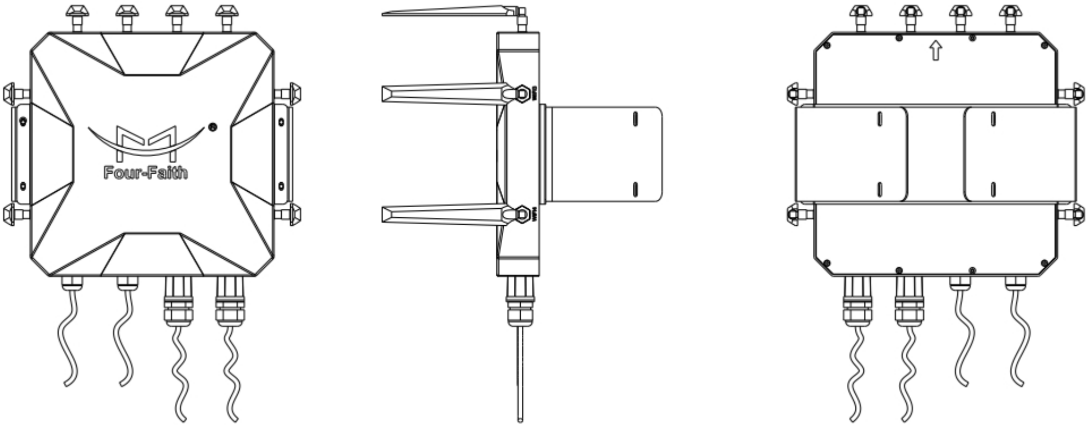
2.3 Installation and Connection

Size and installation:

The dimensions are as shown in the figure below. (Unit: mm)



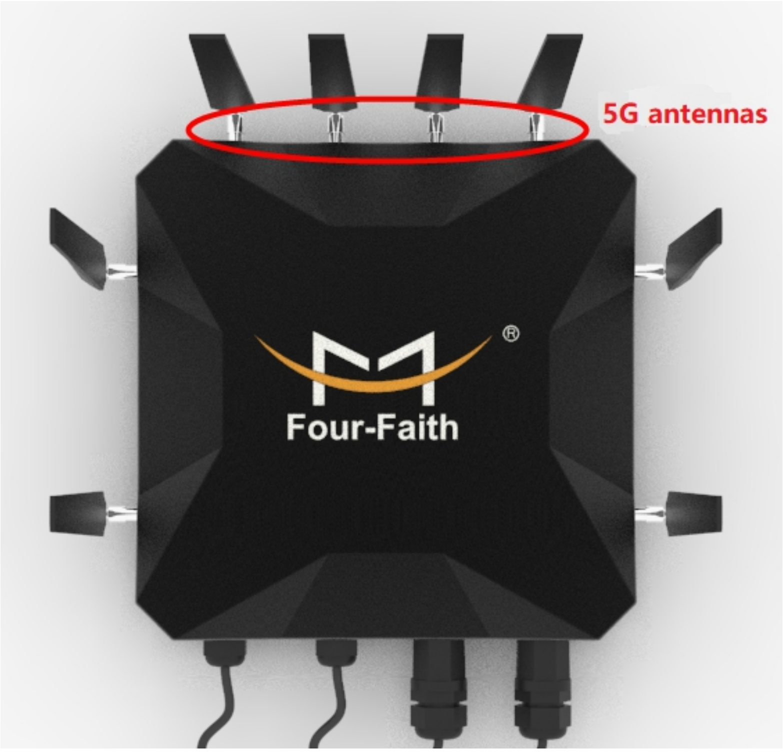
Wall mounting(by default)



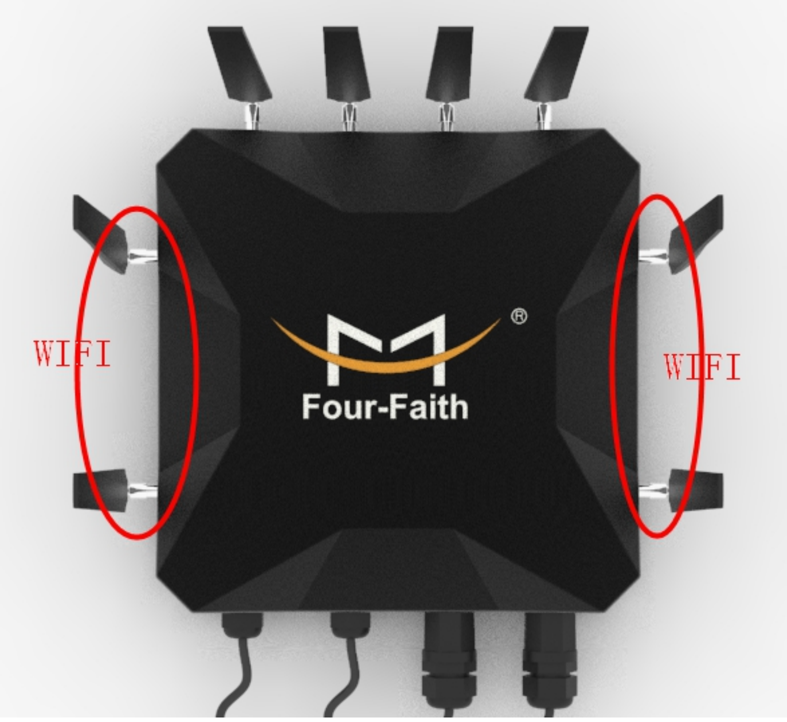
Pole installation(optional)

Antenna installation:

The 5G antenna interface is an SMA female socket. Screw the SMA male of the matching wireless cellular antenna to the antenna interface and make sure to tighten it. In order to increase the 5G antenna isolation, try to keep the antenna at an angle of 30 degrees to enhance Signal quality. As shown below:

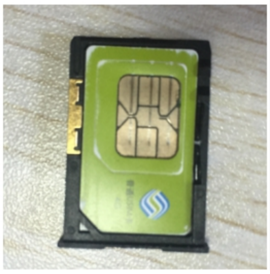


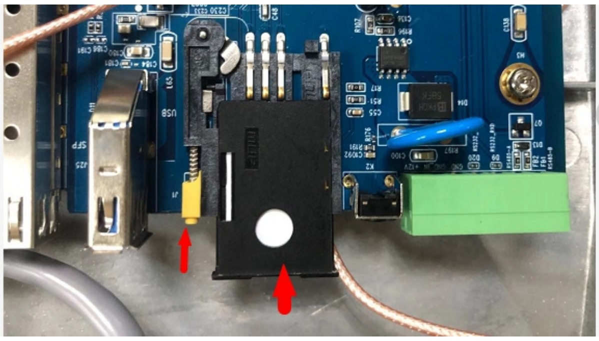
The WIFI antenna interface is an SMA male socket. Screw the SMA female of the WIFI antenna to the antenna interface and make sure to tighten it.



SIM/UIM card installation:

You must open the top cover when installing or removing the SIM/UIM card. First gently hold the eject button (the small round dot on the left side of the SIM/UIM) with a pointed object, and the SIM/UIM card sleeve will pop out. Put the SIM/UIM card into the card holder first, and make sure that the metal contact surface of the SIM/UIM card is facing outward, then insert the SIM/UIM card holder into the drawer and make sure it is inserted in place.

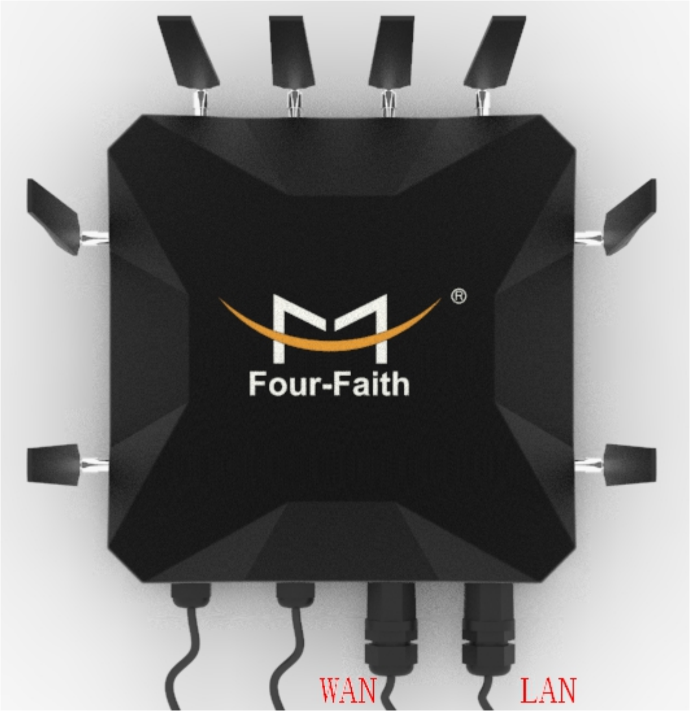




Ethernet cable connection:

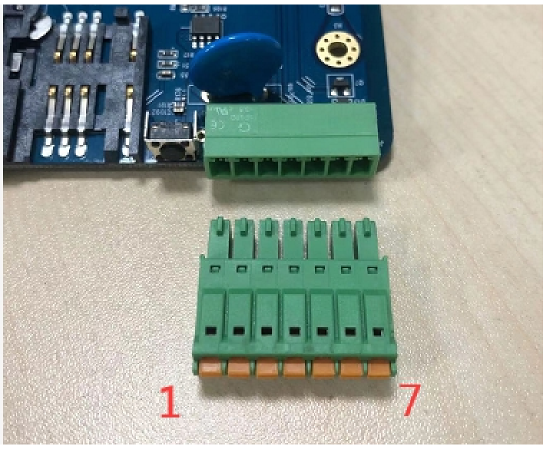
Plug one end of the direct network cable into the LAN port or WAN port of the 5G industrial CPE, and plug the other end into the Ethernet port of the user equipment. The direct network signal connection is as follows:

RJ45-1	RJ45-2	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



Power and serial port connection:

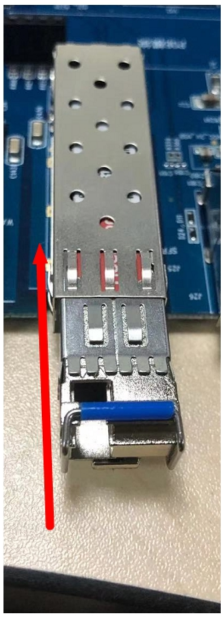
Open the shell and use the 7Pin terminal to connect the external wiring. The terminal signal connection is as follows:

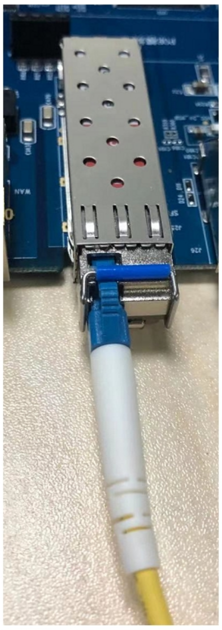


7PinTerminal Definition						
1	2	3	4	5	6	7
Power+	Power-	GND	232-RX	232-TX	485-A	485-B
Power positive	Power negative	GND	Receive end, connect to user end TX	Sending end, connect to user end RX	485 A	485 B

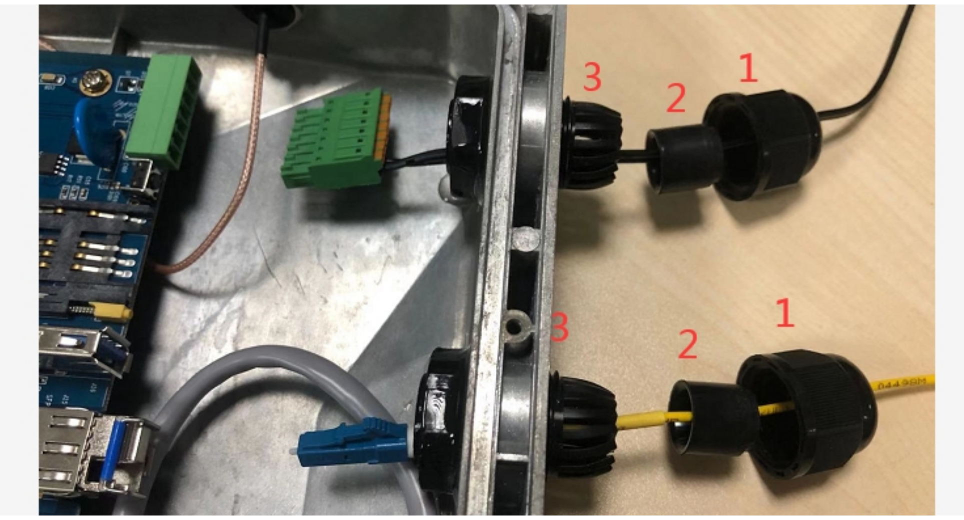
SPF Connection:

Open the shell, insert the SFP port into the optical module, and then insert the optical fiber:





Note: The waterproof connector should be installed as follows when installing the power supply and optical fiber, and the wires should be connected to the shell in order (1 interface cover-2 rubber ring-3 shell hole)

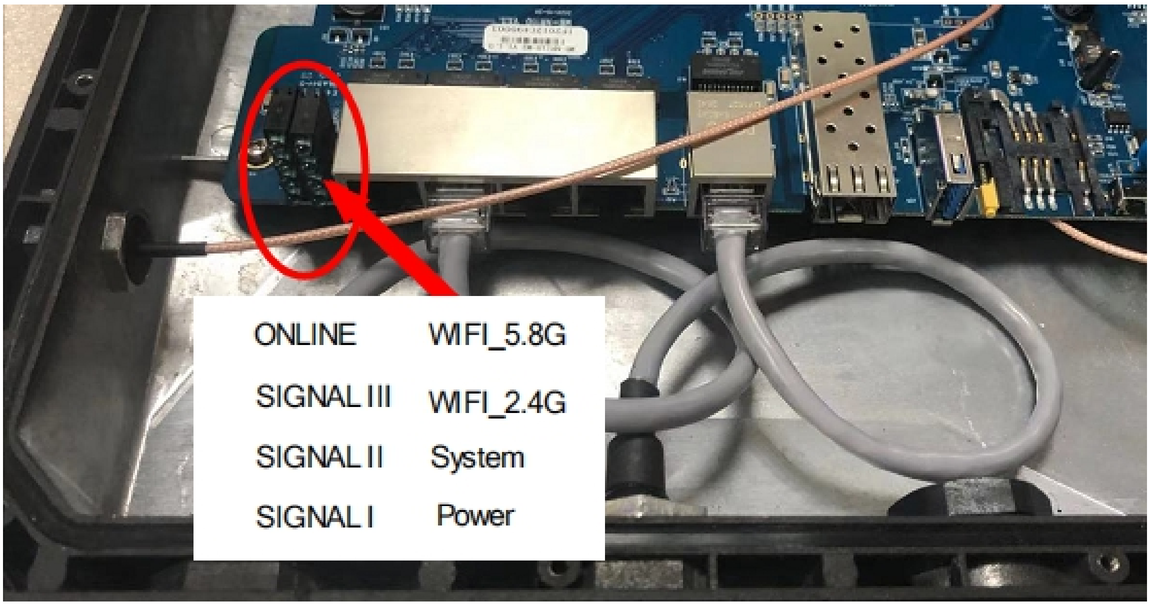


2.4 Power Description

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

12VDC/1.5A power supply is recommended.

2.5 Indicator Description (Inside)



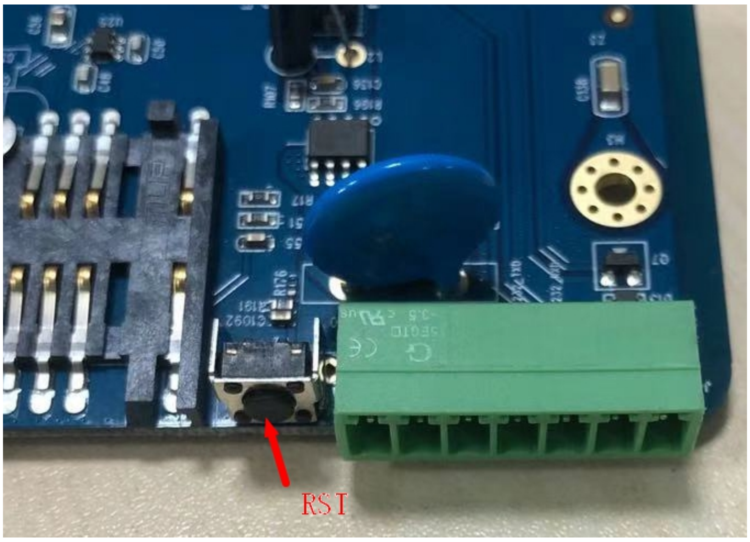
5G industrial CPE indicators are inside the shell, “Power”, “System”, “2.4G”, “5.8G”, “ONLINE”, “Signal”.The description of the status of each indicator is as follows.

Indicator	Status	Description
Power	On	Device power runs well
	Off	Device is not powered on
System	Flashing	System runs well
	Off	System runs abnormally
Online	On	Device is registered to network
	Off	Device is not registered to network
2.4G	On	2.4G WIFI is enable
	Off	2.4G WIFI is disable
5.8G	On	5.8G WIFI is enable
	Off	5.8G WIFI is disable
WAN	Off	WAN is not connected
	On/Flashing	WAN is connected/ is transferring data
LAN1~LAN4	Off	LAN is not connected
	On/Flashing	LAN is connected/is transferring data
Signal	One led light is on	Weak signal(<-90dbm)
	Two led lights are on	Medium signal strength(-70dbm~-90dbm)
	Three led lights are on	Good signal(>-70dbm)

Note: The indicator lights of the WAN port and the LAN port are only green, and the yellow light has no indication.

2.6 Reset Button Description(Inside)

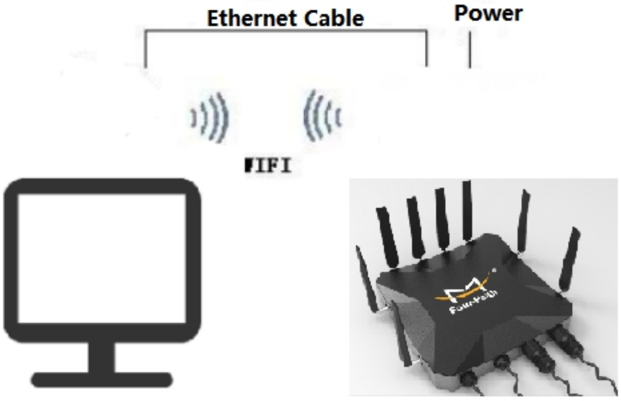
The 5G industrial CPE has a reset button. The function of this button is to restore the 5G industrial CPE to the factory default. Press and hold the reset button for about 15 seconds and release it, the 5G industrial CPE will automatically restore the parameter configuration to the factory default value, and after about 10 seconds, the 5G industrial CPE will automatically restart itself(the automatic restart phenomenon is as follows: "System" indicator light goes out for about 10 seconds, and then it works normally).



Chapter 3 Configuration

3.1 Connection

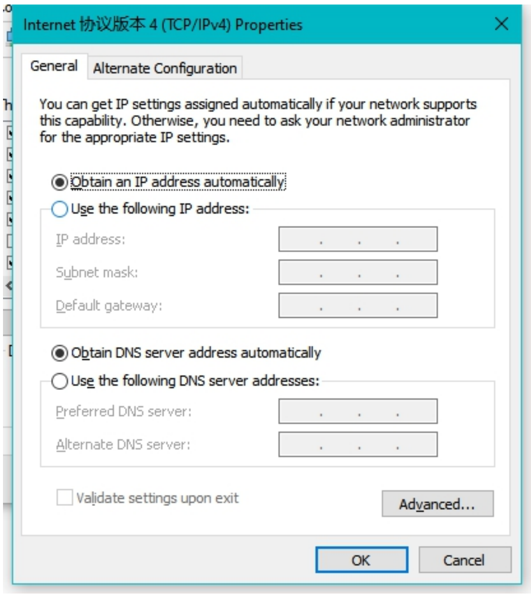
Before configuring the 5G industrial CPE, you need to connect the 5G industrial CPE and the PC used for configuration through the Ethernet cable or WIFI. When connecting with a Ethernet cable, one end of the network cable is connected to any Ethernet port of the 5G industrial CPE "Local Network" (hereinafter referred to as the LAN port), and the other end is connected to the Ethernet port of the PC. When connecting with WIFI, the factory default SSID of 5G industrial CPE is "FOUR-FAITH", no password verification is required.



3.2 Login

3.2.1 PC IP Address Setup (Two ways）

One way: Obtain an IP address automatically



Internet 协议版本 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

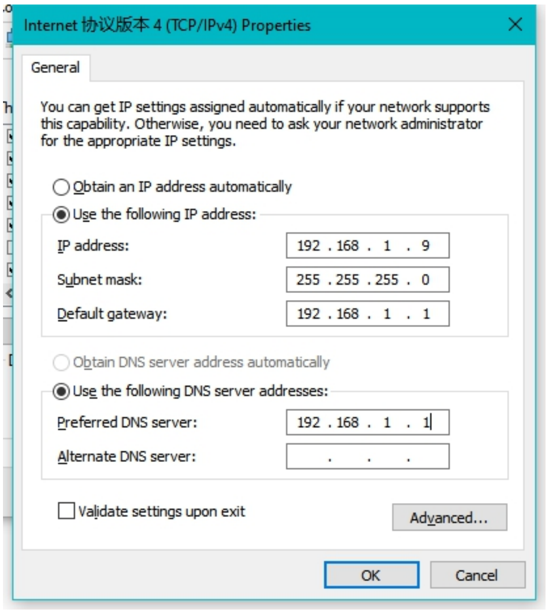
● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

Another way：Fixed IP address

Set the PC IP address to 192.168.1.9 (or other IP addresses in the 192.168.1 network segment), the subnet mask is set to: 255.255.255.0, and the default gateway is set to: 192.168.1.1. DNS is set to gateway address or local available DNS server.



Internet 协议版本 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 9
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

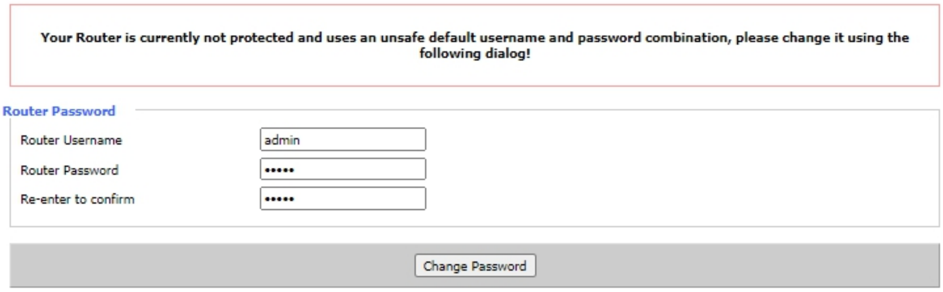
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

3.2.2Login

This chapter describes the main functions of each page. You can use a computer connected to the 5G industrial CPE to access web configure page through a web browser. There have eleven main pages, namely: settings, wireless, services, VPN, security, access restrictions, NAT, QoS settings, applications, management, and status. Click on one of the master pages, and more slave pages will appear.

In order to access the 5G industrial CPE web configure page, start IE or other browsers and enter the default IP address 192.168.1.1 of the 5G industrial CPE in the "Address" field. Press the Enter key. You will see the page as shown blown if you are the first time to log in to the Web page, prompting the user whether to modify the default user name and password of the 5G industrial CPE. Click the “Changing Password” button to continue or to make it effective if you need to enter the user-defined user name and password.

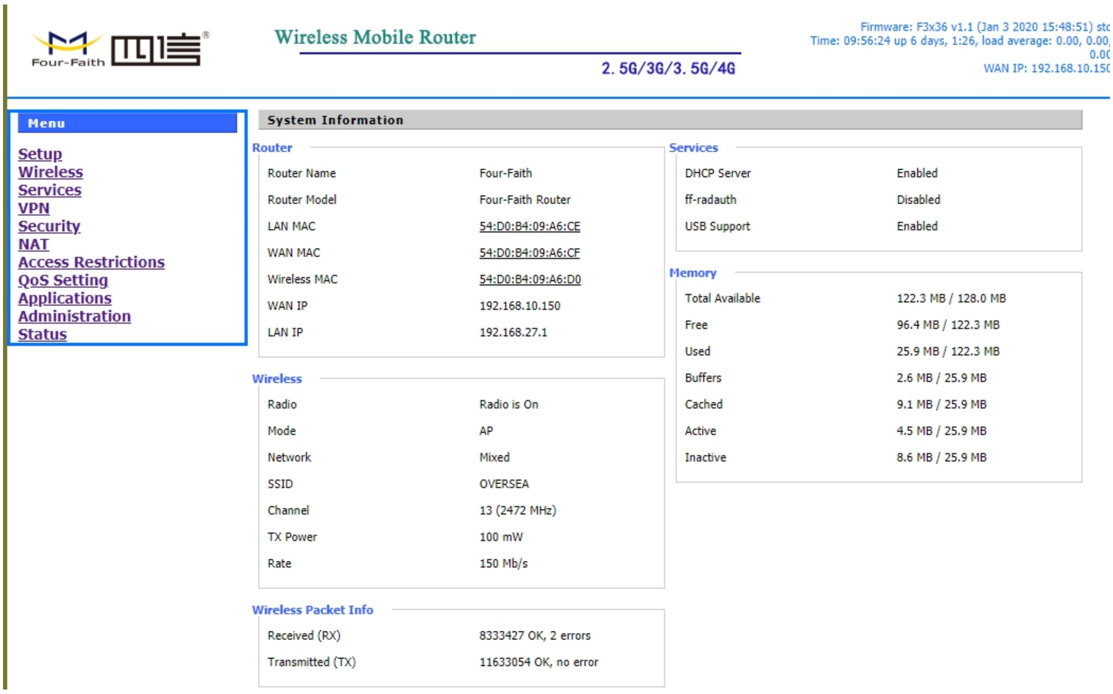


Your Router is currently not protected and uses an unsafe default username and password combination, please change it using the following dialog!

Router Password

Router Username	admin
Router Password	•••••
Re-enter to confirm	•••••

Then you will enter the main page.



Wireless Mobile Router
2. 5G/3G/3. 5G/4G

Firmware: F3x36 v1.1 (Jan 3 2020 15:48:51) std
Time: 09:56:24 up 6 days, 1:26, load average: 0.00, 0.00, 0.00
WAN IP: 192.168.10.150

System Information

Router

Router Name	Four-Faith
Router Model	Four-Faith Router
LAN MAC	54:D0:B4:09:A6:CE
WAN MAC	54:D0:B4:09:A6:CF
Wireless MAC	54:D0:B4:09:A6:D0
WAN IP	192.168.10.150
LAN IP	192.168.27.1

Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Enabled

Memory

Total Available	122.3 MB / 128.0 MB
Free	96.4 MB / 122.3 MB
Used	25.9 MB / 122.3 MB
Buffers	2.6 MB / 25.9 MB
Cached	9.1 MB / 25.9 MB
Active	4.5 MB / 25.9 MB
Inactive	8.6 MB / 25.9 MB

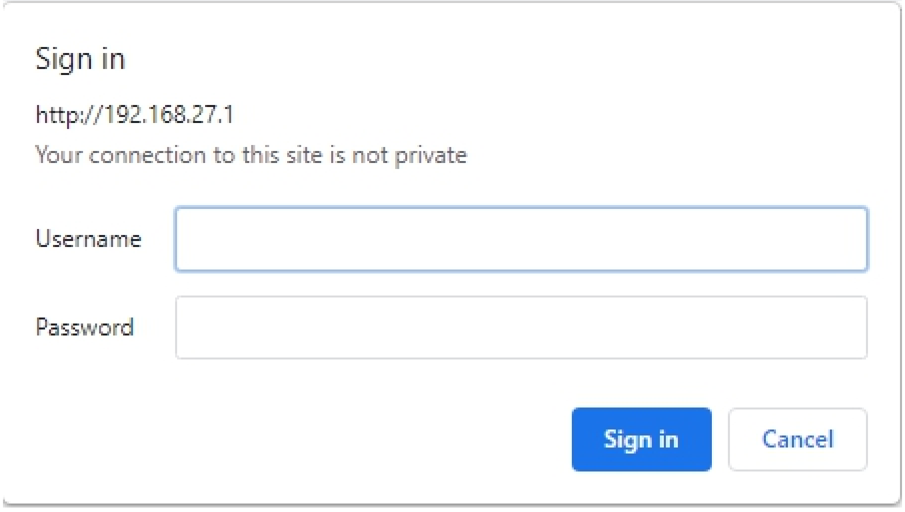
Wireless

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	OVERSEA
Channel	13 (2472 MHz)
TX Power	100 mW
Rate	150 Mb/s

Wireless Packet Info

Received (RX)	8333427 OK, 2 errors
Transmitted (TX)	11633054 OK, no error

You need you need to enter the corresponding user name and password if you click the main menu for the first time.



Sign in

http://192.168.27.1

Your connection to this site is not private

Username

Password

3.3 Management and configuration

3.3.1 Set up

Click "Settings" to open the first page is the basic settings. Through this page, you can follow the prompts to make changes to the basic settings, click the "Save Settings" button to make changes but do not take effect, click the "Apply" button to make the changes take effect, or click the "Cancel Changes" button to cancel change.

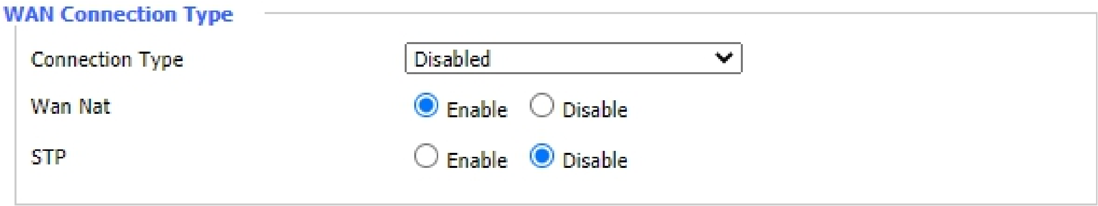
3.3.1.1 Basic setup

The "WAN connection type" setting section describes how to configure the 5G industrial CPE to connect to the Internet. You can get detailed information about this from your ISP.

WAN Connection Type

Select the Internet connection type provided by your ISP from the drop-down menu. The WAN connection type includes 6 methods: disabled, static IP, automatic DHCP, PPPOE, 3G/UMTS/4G/LTE, DHCP-4G/5G.

1.: disable



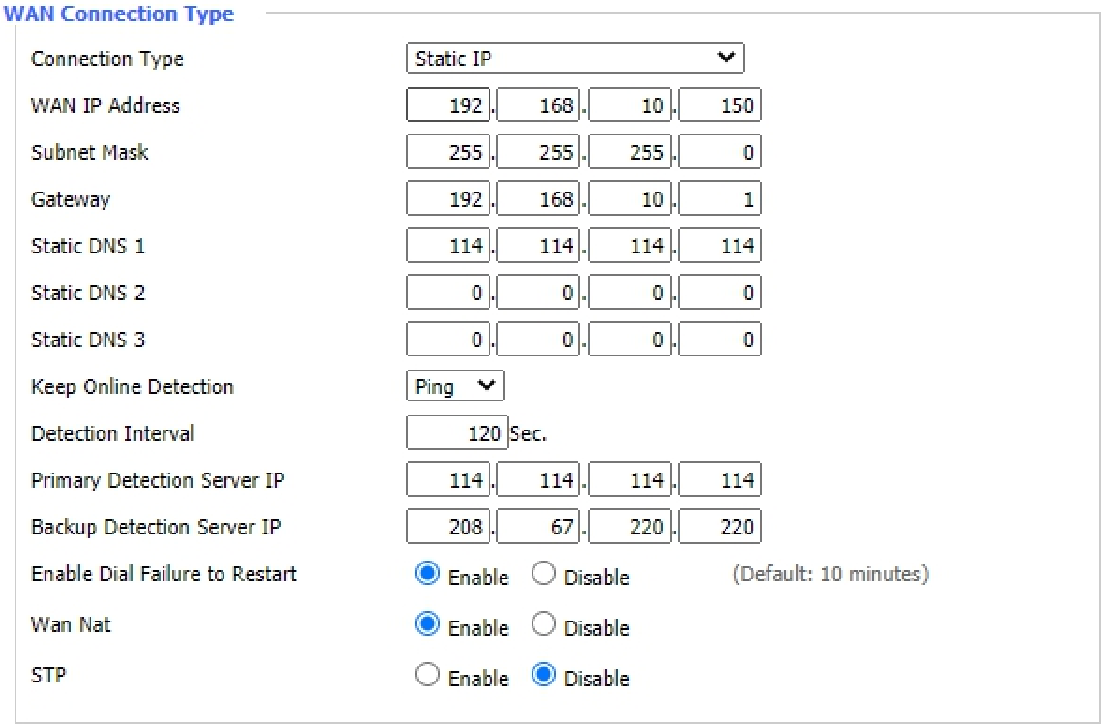
WAN Connection Type

Connection Type	Disabled
Wan Nat	● Enable ○ Disable
STP	○ Enable ● Disable

Prohibit the connection type setting of the WAN port

2.: Static IP

This type of connection is usually used for dedicated line access such as commercial optical fiber. The broadband service provider will provide you with detailed parameters such as IP address, subnet mask, gateway, and DNS. You need to set these parameters on the 5G industrial CPE.

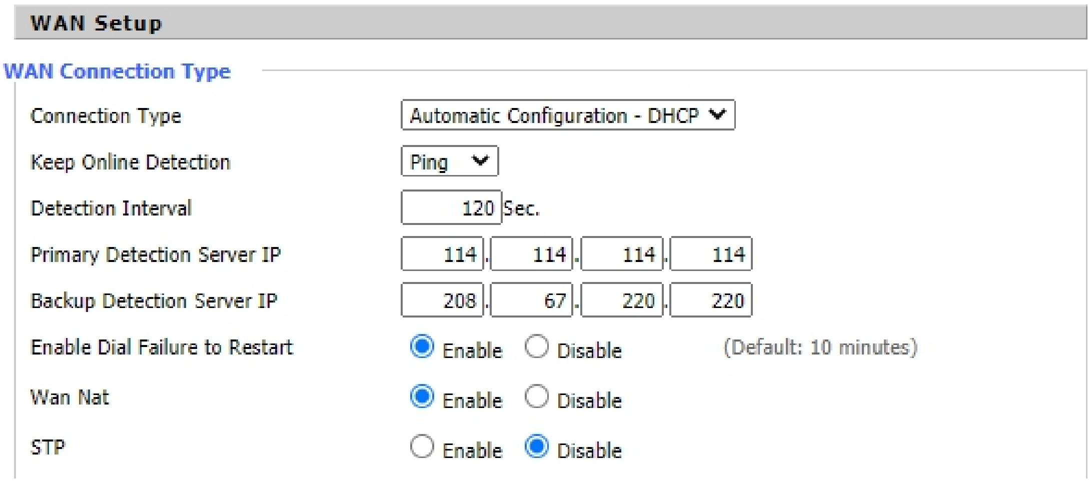


WAN Connection Type

Connection Type	Static IP
WAN IP Address	192 . 168 . 10 . 150
Subnet Mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 10 . 1
Static DNS 1	114 . 114 . 114 . 114
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
Keep Online Detection	Ping
Detection Interval	120 Sec.
Primary Detection Server IP	114 . 114 . 114 . 114
Backup Detection Server IP	208 . 67 . 220 . 220
Enable Dial Failure to Restart	● Enable ○ Disable (Default: 10 minutes)
Wan Nat	● Enable ○ Disable
STP	○ Enable ● Disable

WAN IP address: The IP address set by the user according to his or ISP allocation
Sub net mask: The sub net mask set by the user according to his or ISP allocation
Gateway: The gateway set by the user according to his or ISP allocation
Static DNS (1-3): The static DNS set by users according to their own or ISP allocation

3: Automatic configuration -DHCP



WAN Setup

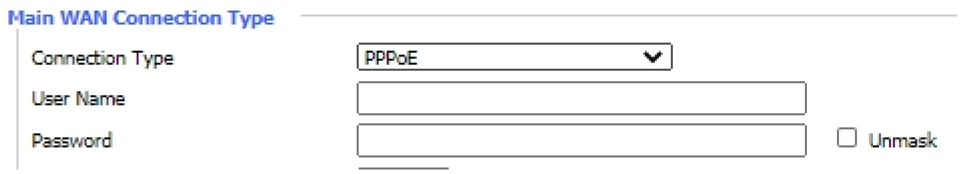
WAN Connection Type

Connection Type	Automatic Configuration - DHCP
Keep Online Detection	Ping
Detection Interval	120 Sec.
Primary Detection Server IP	114 . 114 . 114 . 114
Backup Detection Server IP	208 . 67 . 220 . 220
Enable Dial Failure to Restart	● Enable ○ Disable (Default: 10 minutes)
Wan Nat	● Enable ○ Disable
STP	○ Enable ● Disable

The IP address of the WAN port is obtained by DHCP

4.: PPPOE

China Telecom and China Netcom ADSL broadband services usually use this connection type, and some other broadband service providers also use this method. The PPPoE connection type requires the ISP to provide you with a user name, password, and service name, and this information needs to be set on the 5G industrial CPE.



Main WAN Connection Type

Connection Type: PPPoE

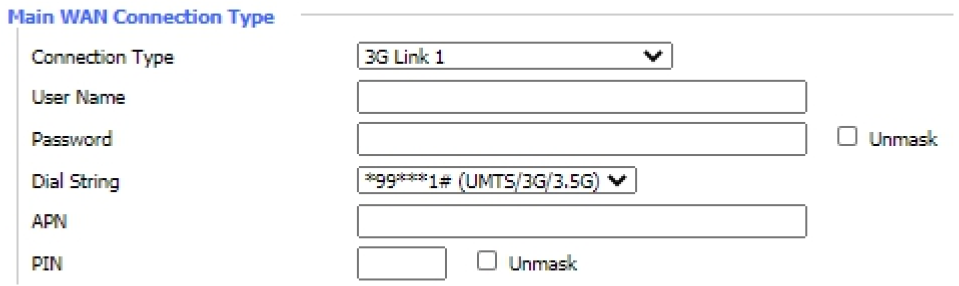
User Name:

Password: □ Unmask

Username: username to login internet

Password: password to login internet

5.: 3G/UMTS/4G/LTE or 3G Link1



Main WAN Connection Type

Connection Type: 3G Link 1

User Name:

Password: □ Unmask

Dial String: *99***1# (UMTS/3G/3.5G)

APN:

PIN: □ Unmask

Username: username to login internet

Password: password to login internet

Dial String: dial number of users' ISP

APN : access point name of users' ISP

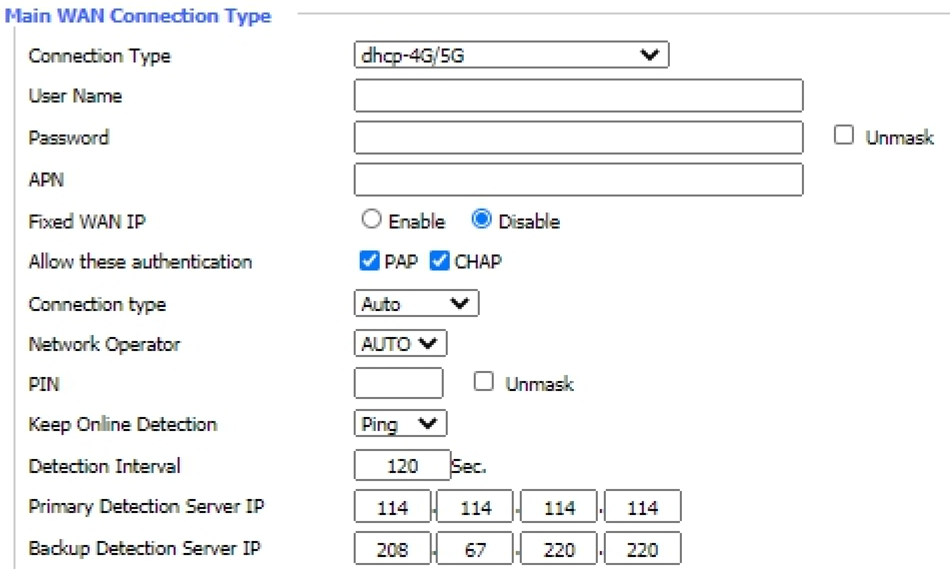
PIN: PIN code of users' SIM card

Network type

Connection type: Auto

Connection type: Auto, Force 3G, Force 2G, Prefer 3G, Prefer 2G options. If using 4G module,there has 4G network option. Users select different mode depending on their need

Type Six: DHCP-4G/5G



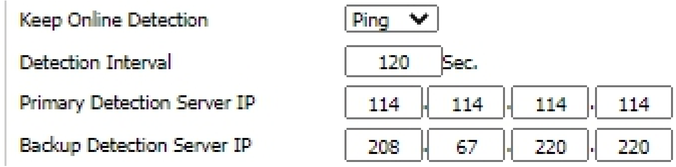
Main WAN Connection Type

Connection Type	dhcp-4G/5G	
User Name		
Password		□ Unmask
APN		
Fixed WAN IP	○ Enable ● Disable	
Allow these authentication	☑ PAP ☑ CHAP	
Connection type	Auto	
Network Operator	AUTO	
PIN		□ Unmask
Keep Online Detection	Ping	
Detection Interval	120 Sec.	
Primary Detection Server IP	114.114.114.114	
Backup Detection Server IP	208.67.220.220	

IP address of WAN port gets automatic via DHCP-4G/5G

Select the default setting “Auto” for the network type, which means that both NSA and SA are supported. This option is best set to a separate SA or a separate NSA according to the actual network environment.

Keep Online



Keep Online Detection	Ping
Detection Interval	120 Sec.
Primary Detection Server IP	114.114.114.114
Backup Detection Server IP	208.67.220.220

This function is used to detect whether the Internet connection is active, if users set it and when the 5G CPE detect the connection is inactive, it will redial to users' ISP immediately to make the connection active. If the network is busy or the user is in private network , we recommend that Router mode will be better

Detection Method:

None: do not set this function

Ping: Send ping packet to detect the connection, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

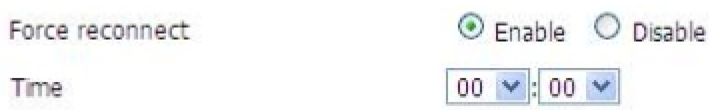
Route: Detect connection with route method, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

PPP: Detect connection with PPP method, when choose this method, users should also configure "Detection Interval" item.

Detection Interval: time interval between two detections, unit is second

Primary Detection Server IP: the server used to response the 5G CPE’ s detection packet. This item is only valid for method "Ping" and "Route".

Backup Detection Server IP: the server used to response the 5G CPE’ s detection packet. This item is valid for method "Ping" and "Route".



Force reconnect	● Enable ○ Disable
Time	00 : 00

Force reconnect: this option schedules the pppoe or 3G reconnection by killing the pppd daemon and restart it.

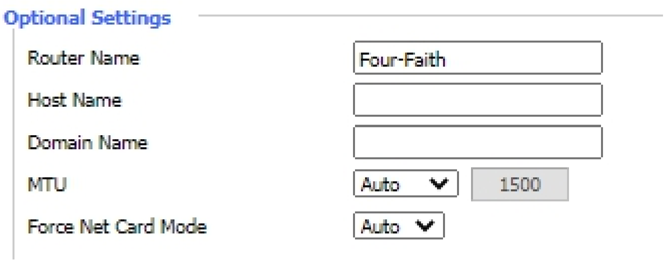
Time: needed time to reconnect

STP

STP	○ Enable ● Disable

STP (Spaning Tree Protocol) can be applied to loop network. Through certain algorithm achieves path redundancy, and loop network cuts to tree-based network without loop in the meantime, thus to avoid the hyperplasia and infinite circulation of a message in the loop network

Optional Configuration



Optional Settings

Router Name	Four-Faith
Host Name	
Domain Name	
MTU	Auto 1500
Force Net Card Mode	Auto

In this field, you can enter up to 39 characters of name that represents a 5G industrial CPE.

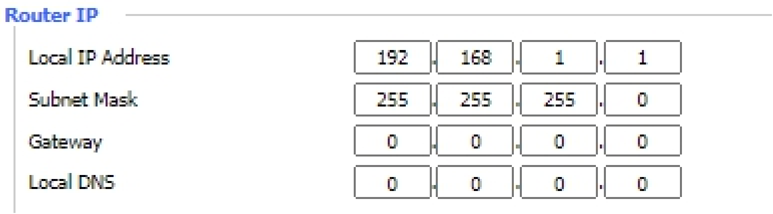
Host Name: ISP provides

Domain Name: ISP provides

MTU： MTU refers to the maximum transmission unit. The maximum transmission unit setting specifies the maximum packet value allowed in Internet transmission. The default state is "Auto", you can manually enter the maximum packet value that will be transmitted. The recommended range for this value is 1200 to 1500. For most DSL users, 1492 is recommended. You should keep this value in the range of 1200 to 1500. If you want the 5G industrial CPE to be able to select the best MTU for your Internet, select the "Auto" option.

Network Settings

The network settings part can modify the network settings connected to the 5G industrial CPE Ethernet port.



Router IP

Local IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
Gateway	0 . 0 . 0 . 0
Local DNS	0 . 0 . 0 . 0

Local IPAddress: IP address of the 5G CPE

Subnet Mask: the subnet mask of the 5G CPE

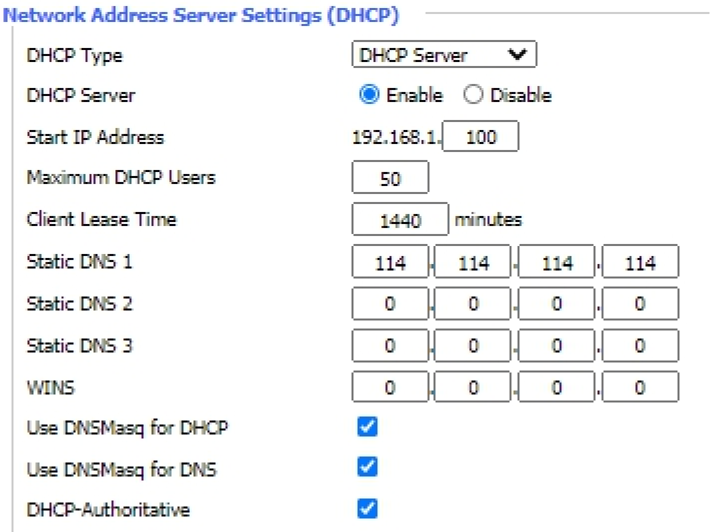
Gateway: set internal gateway of the 5G CPE. If default, internal gateway is the address of the

5G CPE

Local DNS: DNS server is auto assigned by network operator server. Users enable to use their own DNS server or other stable DNS servers, if not, keep it default

NetworkAddress Server Settings (DHCP)

These settings for the 5G CPE'Dynamic Host Configuration Protocol (DHCP) server functionality configuration. The 5G CPE can serve as a network DHCP server. DHCP server automatically assigns an IP address for each computer in the network. If they choose to enable the 5G CPE' DHCP server option, users can set all the computers on the LAN to automatically obtain an IP address and DNS, and make sure no other DHCP server in the network

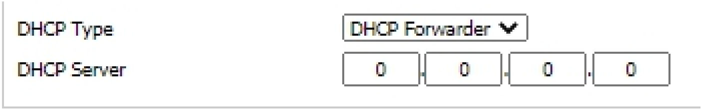


Network Address Server Settings (DHCP)

DHCP Type	DHCP Server
DHCP Server	● Enable ○ Disable
Start IP Address	192.168.1. 100
Maximum DHCP Users	50
Client Lease Time	1440 minutes
Static DNS 1	114 . 114 . 114 . 114
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
WINS	0 . 0 . 0 . 0
Use DNSMasq for DHCP	☑
Use DNSMasq for DNS	☑
DHCP-Authoritative	☑

DHCPType: DHCP Server and DHCP Forwarder

Enter DHCP Server if set DHCP Type to DHCP Forwarder as blow:



DHCP Type	DHCP Forwarder
DHCP Server	0 . 0 . 0 . 0

DHCP Server: keep the default Enable to enable the 5G CPE's DHCP server option. If users have already have a DHCP server on their network or users do not want a DHCP server, then select Disable

Start IP Address: enter a numerical value for the DHCP server to start with when issuing IP addresses. Do not start with 192.168.1.1 (the 5G CPE's own IP address).

Maximum DHCP Users: enter the maximum number of PCs that users want the DHCP server to assign IP addresses to. The absolute maximum is 253 if 192.168.1.2 is users' starting IP address.

Client Lease Time: the Client Lease Time is the amount of time a network user will be allowed connection to the 5G CPE with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.

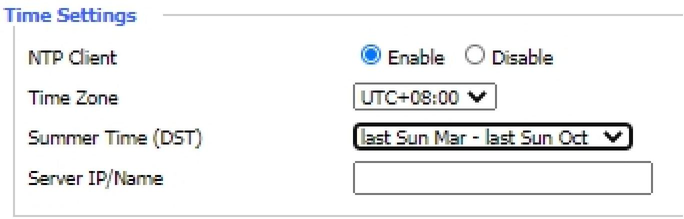
Static DNS (1-3): the Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Users' ISP will provide them with at least one DNS Server IP address. If users wish to utilize another, enter that IP address in one of these fields. Users can enter up to three DNS Server IP addresses here. The 5G CPE will utilize them for quicker

access to functioning DNS servers.

WINS: the Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If users use a WINS server, enter that server's IP address here. Otherwise, leave it blank.

DNSMasq: users' domain name in the field of local search, increase the expansion of the host option, to adopt DNSMasq can assign IP addresses and DNS for the subnet, if select DNSMasq, dhcpd service is used for the subnet IP address and DNS.

Time Settings



Time Settings

NTP Client ● Enable ○ Disable

Time Zone UTC+08:00

Summer Time (DST) last Sun Mar - last Sun Oct

Server IP/Name

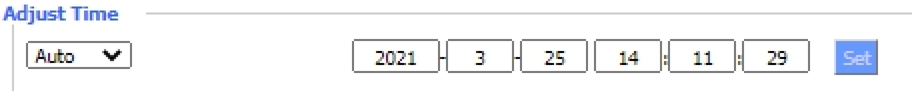
NTP Client: Get the system time from NTP server

Time Zone: Time zone options

Summer Time (DST): set it depends on users' location

Server IP/Name: IP address of NTP server, up to 32 characters. If blank, the system will find a server by default

Adjust Time



Adjust Time

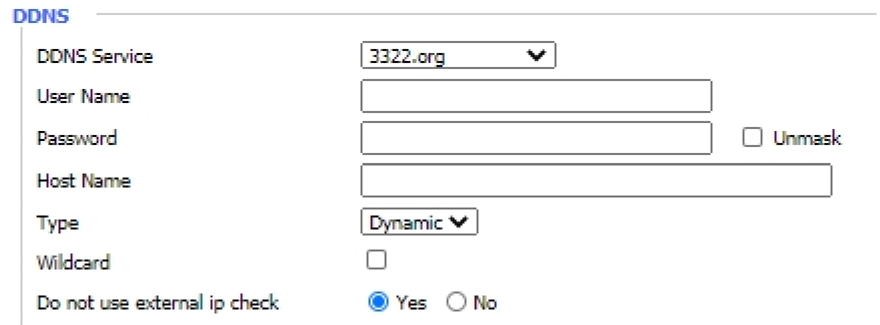
Auto 2021-3-25 14:11:29

To adjust time by the system and refresh to get the time of the web, user can set to modify the time of the system. They can change to adjust time by manual to achieve adjust time by the system if the system fails to get NTP server

3.3.1.2 Dynamic DNS(DDNS)

If the IP address obtained by the 5G industrial CPE Internet access is dynamically allocated by the operator, the IP address obtained by the 5G industrial CPE may be different each time. In this case, a dynamic domain name service can be used. The domain name provider allows you to register a domain name, which always corresponds to the current dynamic IP address of the 5G industrial CPE. In this way, you can access the latest Internet IP address of the 5G industrial CPE by accessing the domain name

DDNS Service: Router currently support DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP and Custom based on the user.



DDNS

DDNS Service	3322.org
User Name	
Password	□ Unmask
Host Name	
Type	Dynamic
Wildcard	□
Do not use external ip check	● Yes ○ No

User Name: users register in DDNS server, up to 64 characteristic

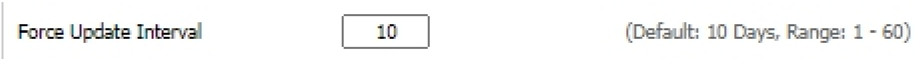
Password: password for the user name that users register in DDNS server, up to 32 characteristic

Host Name: users register in DDNS server, no limited for input characteristic for now

Type: depends on the server

Wildcard: support wildcard or not, the default is OFF. ON means *.host.3322.org is equal to host.3322.org

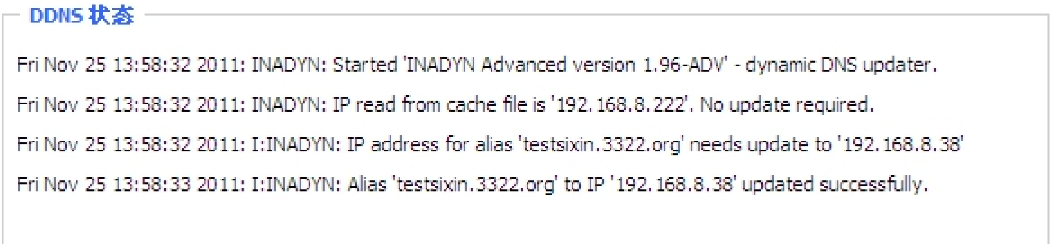
Do not use external ip check: enable or disable the function of 'do not use external ip check'



Force Update Interval 10 (Default: 10 Days, Range: 1 - 60)

Force Update Interval: unit is day, try forcing the update dynamic DNS to the server by setted days

Status



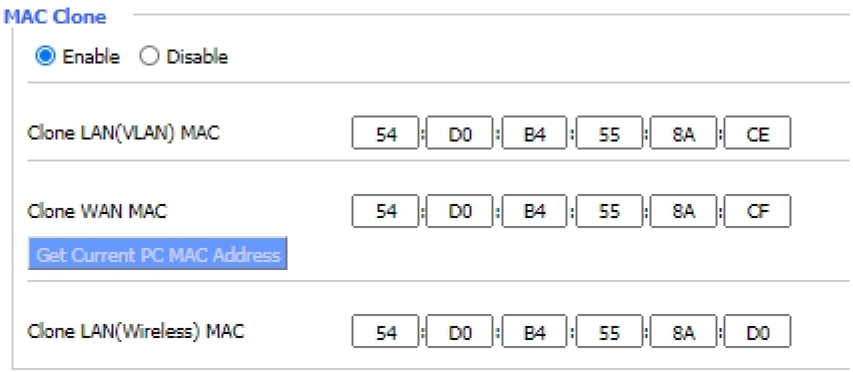
DDNS 状态

```
Fri Nov 25 13:58:32 2011: INADYN: Started 'INADYN Advanced version 1.96-ADV' - dynamic DNS updater.
Fri Nov 25 13:58:32 2011: INADYN: IP read from cache file is '192.168.8.222'. No update required.
Fri Nov 25 13:58:32 2011: I:INADYN: IP address for alias 'testsixin.3322.org' needs update to '192.168.8.38'
Fri Nov 25 13:58:33 2011: I:INADYN: Alias 'testsixin.3322.org' to IP '192.168.8.38' updated successfully.
```

DDNS Status shows connection log information

3.3.1.3 Clone MAC Address

Some ISP need the users to register their MAC address. The users can clone the 5G CPEMAC address to their MAC address registered in ISP if they do not want to re-register their MAC Address



MAC Clone

● Enable ○ Disable

Clone LAN(VLAN) MAC	54 : D0 : B4 : 55 : 8A : CE
Clone WAN MAC	54 : D0 : B4 : 55 : 8A : CF
Clone LAN(Wireless) MAC	54 : D0 : B4 : 55 : 8A : D0

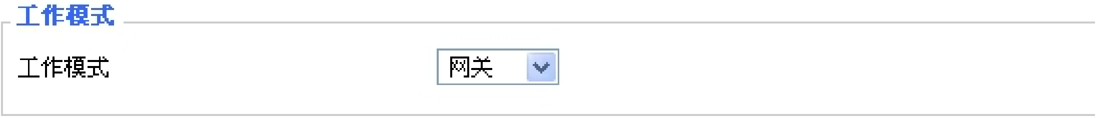
Clone MAC address can clone three parts: Clone LAN MAC, Clone WAN MAC, Clone Wireless

MAC.

Noted that one MAC address is 48 characteristic, can not be set to the multicast address, the first byte must be even. And MAC address value of network bridge br0 is determined by the smaller value of wireless MAC address and LAN port MAC address

3.3.1.4 Advance Router

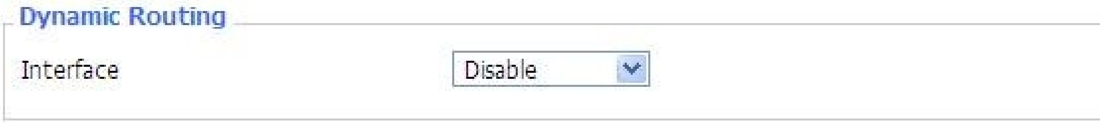
Operating Mode: Gateway and Router, for most users, suggest to use gateway mode



工作模式 网关

If the Router is hosting users' Internet connection, select Gateway mode. If another Router exists on their network, select Router mode.

Dynamic Routing



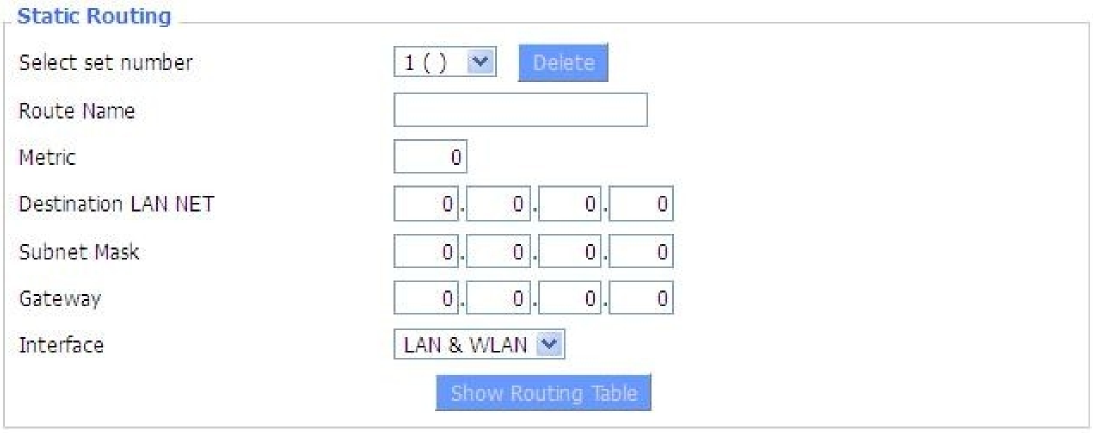
Interface Disable

Dynamic Routing enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with other Routers. The Router determines the network packets’ route based on the fewest number of hops between the source and destination. To enable the Dynamic Routing feature for the WAN side, select WAN. To enable this feature for the LAN and wireless side, select LAN&WLAN. To enable the feature for both the WAN and LAN, select Both. To disable the Dynamic Routing feature for all data transmissions, keep the default setting, Disable.

Note：Dynamic Routing is not available in Gateway mode

Static Routing

To set a static route between the 5G industrial CPE and another network, please select a number from the static route drop-down list to set it. (Static routing is a predetermined path that network information must be transmitted to a specific host or network.)



Select set number	1 ( )
Route Name	
Metric	0
Destination LAN NET	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0
Gateway	0 . 0 . 0 . 0
Interface	LAN & WLAN

Select set number:
1-50

Route Name: defined routing name by users, up to 25 characters

Metric:
0-9999

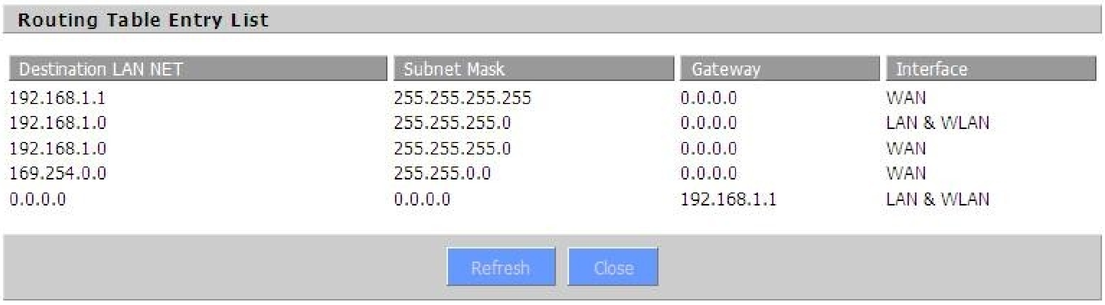
Destination LAN NET: the Destination IP Address is the address of the network or host to which users want to assign a static route

Subnet Mask: the Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion

Gateway: IP address of the gateway device that allows for contact between the 5G CPE and the network or host.

Interface: indicate users whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), the WAN (Internet), or Loopback (a dummy network in which one PC acts like a network, necessary for certain software programs)

To delete the configured static route , select the corresponding route table number and click the "Delete" button. To view the detailed routing information of the 5G industrial CPE, click the "Show routing table" button.

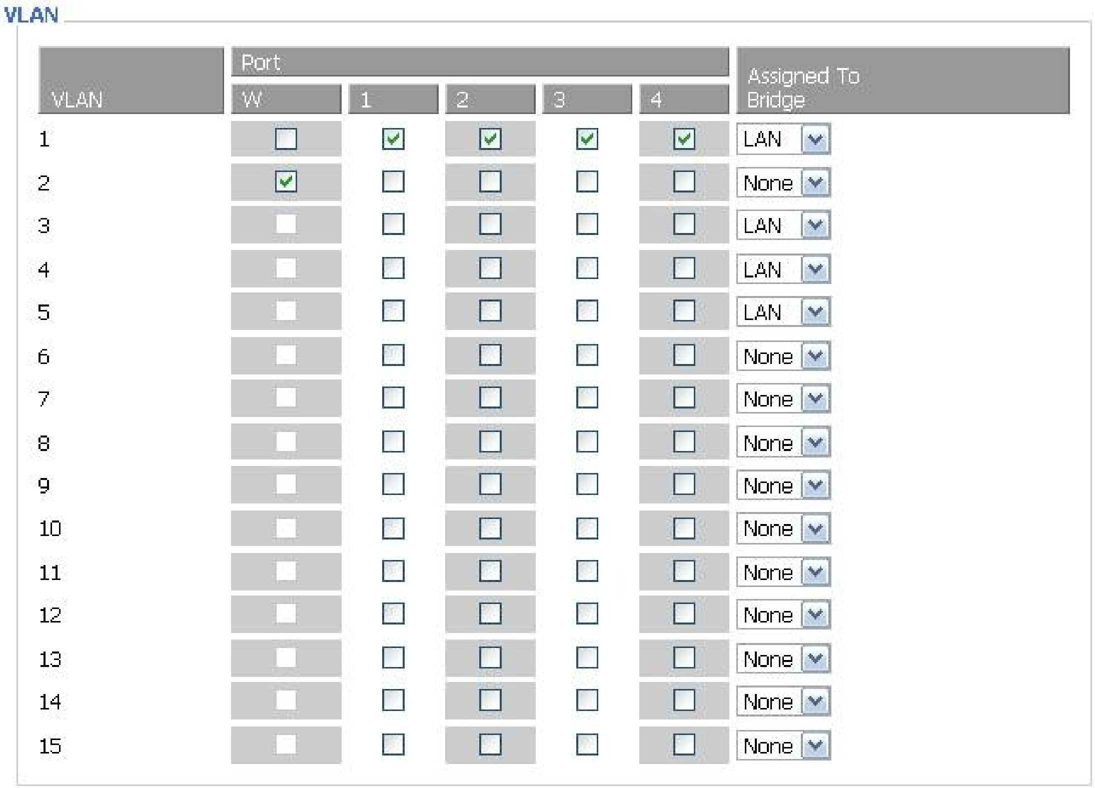


Routing Table Entry List

Destination LAN NET	Subnet Mask	Gateway	Interface
192.168.1.1	255.255.255.255	0.0.0.0	WAN
192.168.1.0	255.255.255.0	0.0.0.0	LAN & WLAN
192.168.1.0	255.255.255.0	0.0.0.0	WAN
169.254.0.0	255.255.0.0	0.0.0.0	WAN
0.0.0.0	0.0.0.0	192.168.1.1	LAN & WLAN

After completing the modification, click the "Save Settings" button to make the changes but do not take effect, click the "Apply" button to make the changes take effect, or click the "Cancel Changes" button to cancel the changes. The help information is on the right side of the screen.

3.3.1.5 VLAN

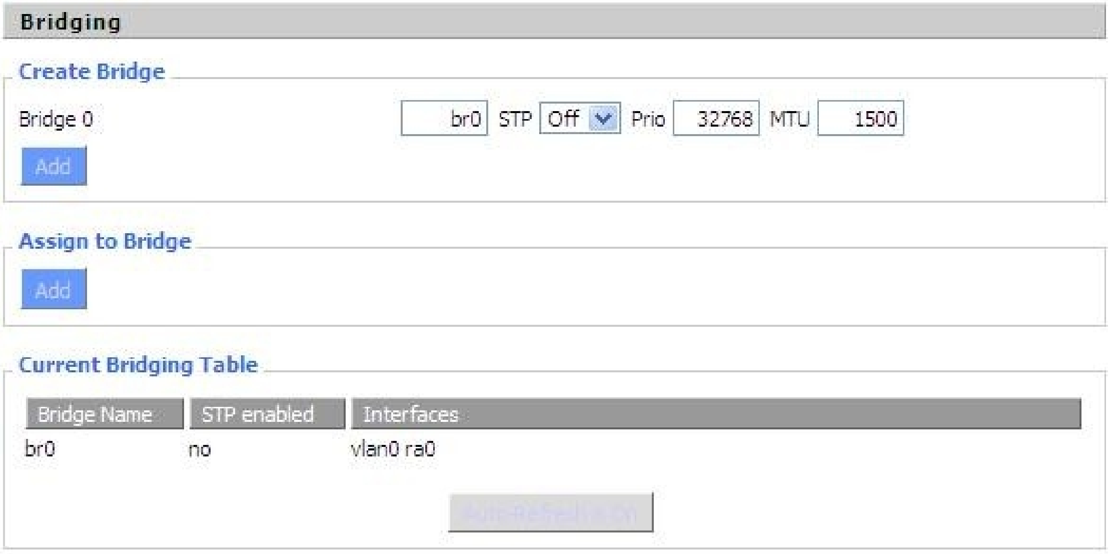


VLAN

VLAN	Port					Assigned To Bridge
	W	1	2	3	4	
1	□	☑	☑	☑	☑	LAN
2	☑	□	□	□	□	None
3	□	□	□	□	□	LAN
4	□	□	□	□	□	LAN
5	□	□	□	□	□	LAN
6	□	□	□	□	□	None
7	□	□	□	□	□	None
8	□	□	□	□	□	None
9	□	□	□	□	□	None
10	□	□	□	□	□	None
11	□	□	□	□	□	None
12	□	□	□	□	□	None
13	□	□	□	□	□	None
14	□	□	□	□	□	None
15	□	□	□	□	□	None

VLANs function is to divide different VLAN ports by users' will. The system supports 15 VLAN port from VLAN1-VLAN15. However there is only 5 time ports (1 WAN port and 4 LAN port) divided by users themselves,and LAN port and WAN port disable to divide into one VLAN port meanwhile.

3.3.1.6 Network



Bridging

Create Bridge

Bridge 0 br0 STP Off Prio 32768 MTU 1500

Assign to Bridge

Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0 ra0

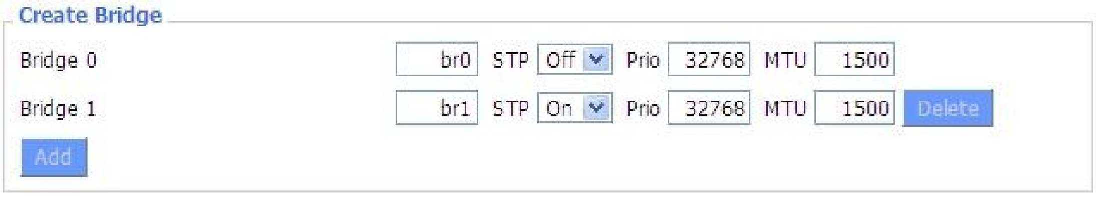
Bridging-Create Bridge: creates a new empty network bridge for later use. STP means Spanning Tree Protocol and with PRIO users are able to set the bridge priority order. The lowest number has the highest priority.

Bridging - Assign to Bridge: allows users to assign any valid interface to a network bridge. Consider setting the Wireless Interface options to Bridged if they want to assign any Wireless Interface here. Any system specific bridge setting can be overridden here in this field

Current Bridging Table: shows current bridging table

Create steps as below:

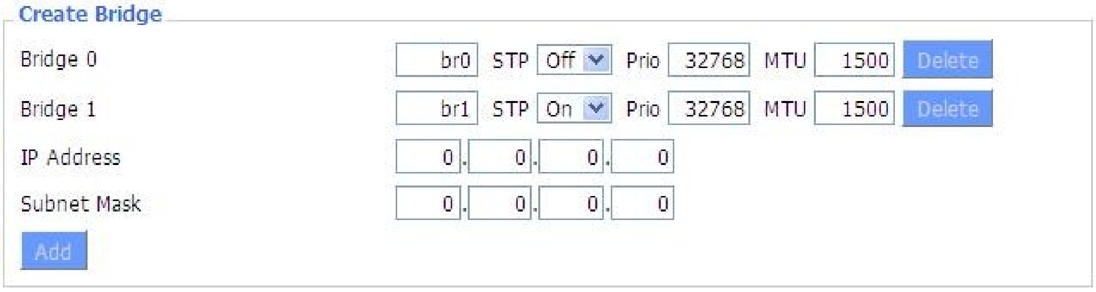
Click 'Add' to create a new bridge, configuration is as below:



Create Bridge

Bridge 0	br0	STP	Off	Prio	32768	MTU	1500	
Bridge 1	br1	STP	On	Prio	32768	MTU	1500	Delete

Create bridge option: the first br0 means bridge name. STP means to on/off spanning tree protocol. Prio means priority level of STP, the smaller the number, the higher the level. MTU means maximum transfer unit, default is 1500, delete if it is not need. And then click 'Save' or 'Add'. Bride properties is as below:

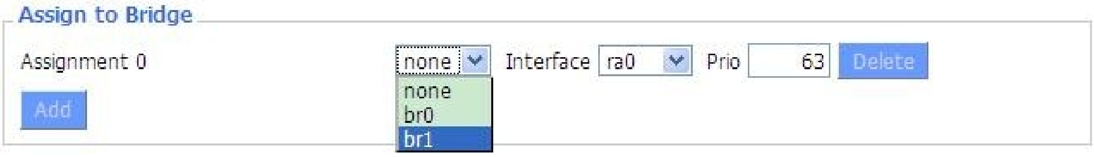


Create Bridge

Bridge 0	br0	STP	Off	Prio	32768	MTU	1500	Delete
Bridge 1	br1	STP	On	Prio	32768	MTU	1500	Delete
IP Address	0. 0. 0. 0							
Subnet Mask	0. 0. 0. 0							

Enter relewant bridge IP address and subnet mask, click 'Add' to create a bridge.

Note: Only create a bride can apply it.



Assign to Bridge

Assignment 0	none	Interface	ra0	Prio	63	Delete

Assign to Bridge option:

to assign different ports to created bridge. For example: assign port (wireless port) is ra0 in br1 bridge as below:

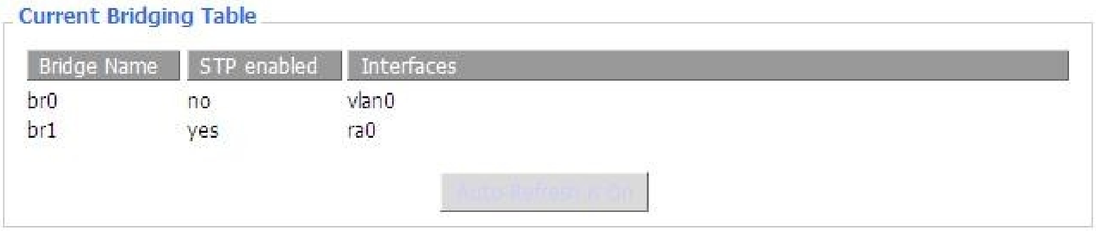
Prio means priority level:

work if multiple ports are within the same bridge. The smaller the number, the higher the level. Click 'Add' to take it effect.

Note:

corresponding interface of WAN ports interface should not be binding, this bridge function is basically used for LAN port, and should not be binding with WAN port

If bind success, bridge binding list in the list of current bridging table is as below:

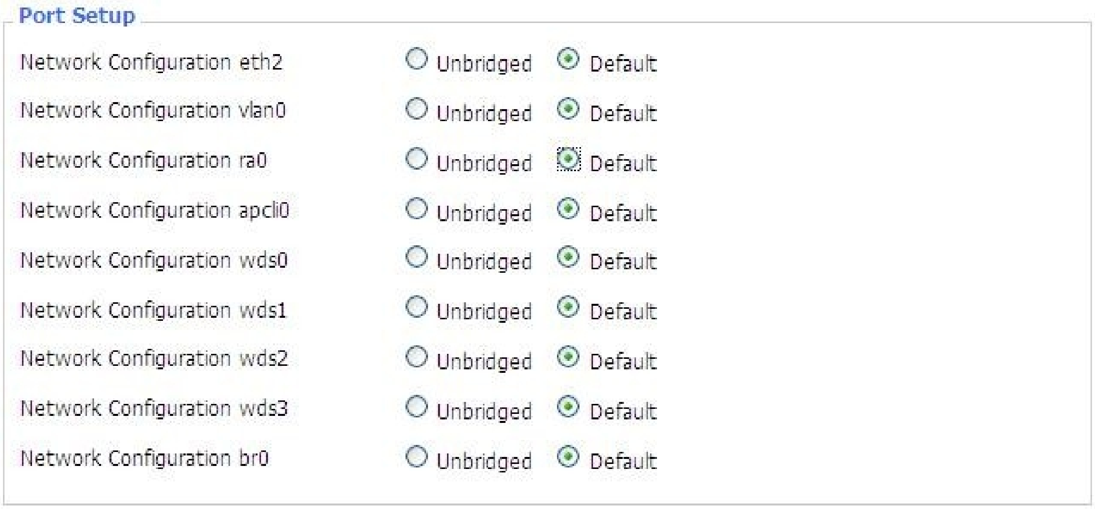


Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0
br1	yes	ra0

Auto-Refresh is On

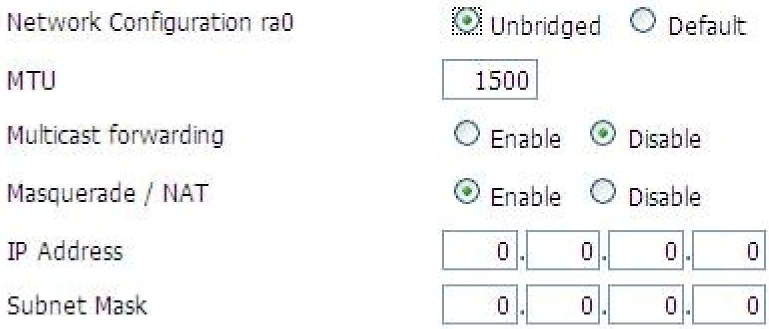
To make br1 bridge has the same function with DHCP assigned address, users need to set multiple DHCP function, see the introduction of multi-channel DHCPD:



Port Setup

Network Configuration eth2	○ Unbridged	● Default
Network Configuration vlan0	○ Unbridged	● Default
Network Configuration ra0	○ Unbridged	● Default
Network Configuration apcli0	○ Unbridged	● Default
Network Configuration wds0	○ Unbridged	● Default
Network Configuration wds1	○ Unbridged	● Default
Network Configuration wds2	○ Unbridged	● Default
Network Configuration wds3	○ Unbridged	● Default
Network Configuration br0	○ Unbridged	● Default

Port Setup: Set the port property, the default is not set



Network Configuration ra0	● Unbridged ○ Default
MTU	1500
Multicast forwarding	○ Enable ● Disable
Masquerade / NAT	● Enable ○ Disable
IP Address	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0

Choose not bridge to set the port's own properties, detailed properties are as below:

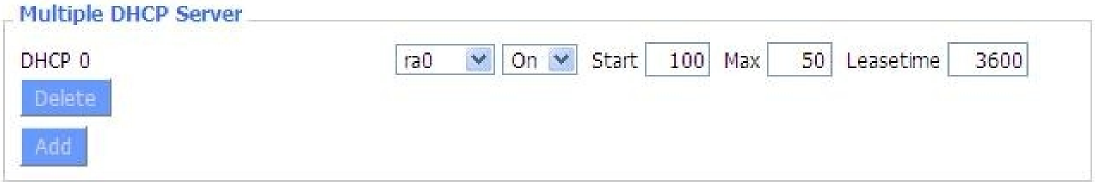
MTU: maximum transfer unit

Multicast forwarding: enable or disable multicast forwarding

Masquerade/NAT: enable or disable Masquerade/NAT

IP Address: set ra0's IP address, and do not conflict with other ports or bridge

Subnet Mask: set the port's subnet mask



Multiple DHCP Server

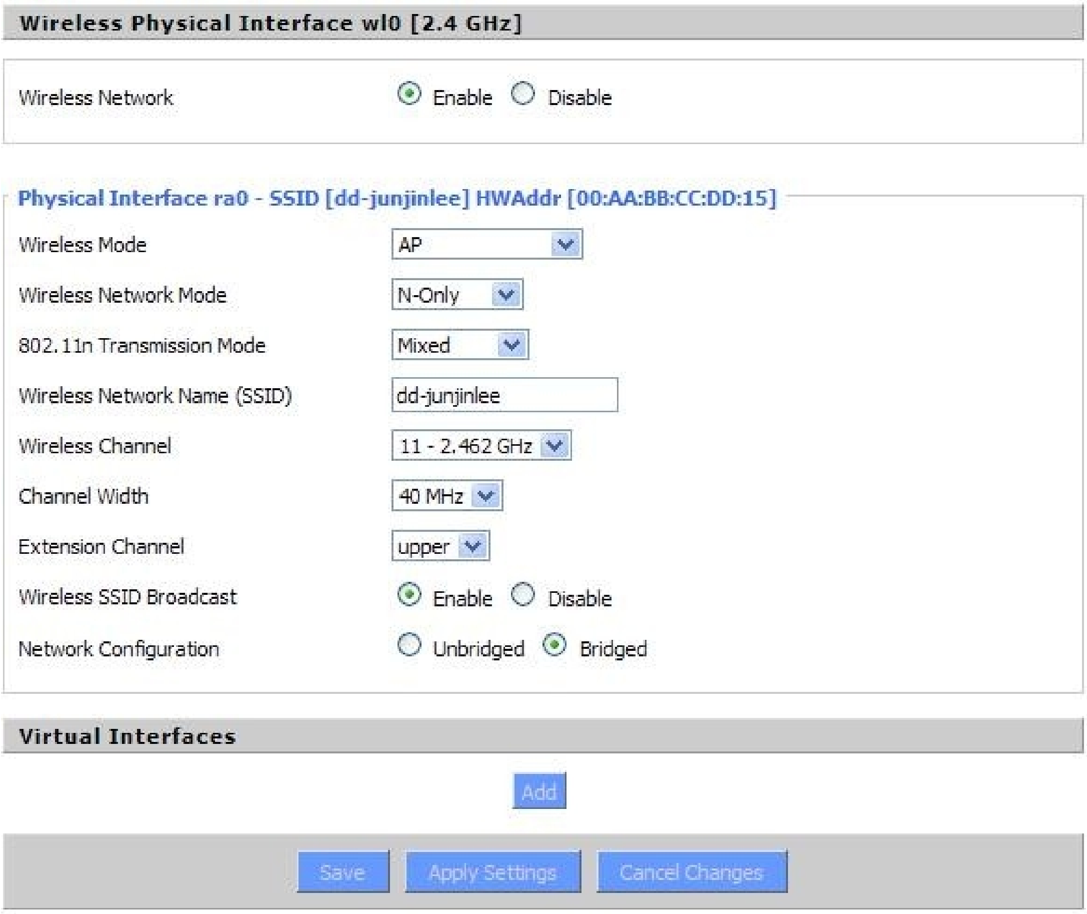
DHCP 0 | ra0 | On | Start 100 | Max 50 | Leasetime 3600

Multiple DHCPD: using multiple DHCP service. Click 'Add' in multiple DHCP server to appear relevant configuration. The first means the name of port or bridge (do not be configured as eth0), the second means whether to on DHCP. Start means start address, Max means maximum assigned DHCP clients, Leasetime means the client lease time, the unit is second, click 'Save' or 'Apply' to put it into effect after setting.

Note: Only configure and click 'Save' can configure the next, can not configure multiple DHCP at the same time.

3.3.2 Wireless

3.3.2.1 Basic Settings



Wireless Physical Interface wl0 [2.4 GHz]

Wireless Network: ● Enable ○ Disable

Physical Interface ra0 - SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Wireless Mode	AP
Wireless Network Mode	N-Only
802.11n Transmission Mode	Mixed
Wireless Network Name (SSID)	dd-junjinlee
Wireless Channel	11 - 2.462 GHz
Channel Width	40 MHz
Extension Channel	upper
Wireless SSID Broadcast	● Enable ○ Disable
Network Configuration	○ Unbridged ● Bridged

Virtual Interfaces

Wireless Network： “Eanble”, radio on. “Disable”, radio off.

Wireless Mode： AP, Client, Adhoc, Repeater, Repeater Bridge four options。

Wireless Network Mode：

Mixed： Support 802.11b, 802.11g, 802.11n wireless devices.

BG-Mixed： Support 802.11b, 802.11g wireless devices.

B-only： Only supports the 802.11b standard wireless devices.

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

NG-Mixed： Support 802.11g, 802.11n wireless devices.

N-only： Only supports the 802.11g standard wireless devices.

5.8G: support ac / na mode

8021.11n Transmission Mode ： In the wireless network mode to "N-only" choose to transfer its transmission mode.

Greenfield: When you determine the surrounding environment, there is no other 802.11a/b/g devices use the same channel, use this mode to increase throughput. Other 802.11a/b/g devices use the same channel in the environment, the information you send may generate an error, re-issued.

Mixed： This mode is contrary to the green mode, but will reduce the throughput.

Wireless Network Name(SSID): The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all devices in your wireless network.。

Wireless Channel： A total of 1-13 channels to choose more than one wireless device environment, please try to avoid using the same channel with other devices.。

5.8G has 149 153 157 161 165 MhzChannels

Channel Width： 20MHZ and 40MHZ ,5.8G wifi can support 80MHZ。

Wireless SSID Broadcast：

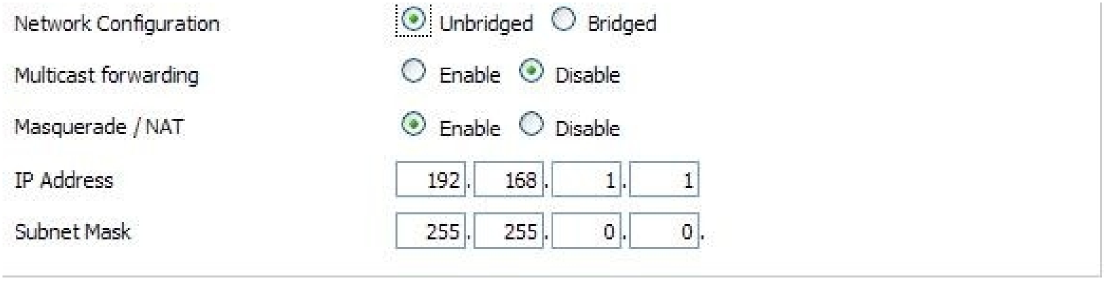
Enable：SSID broadcasting.

Disable：Hidden SSID.

Network Configuration：

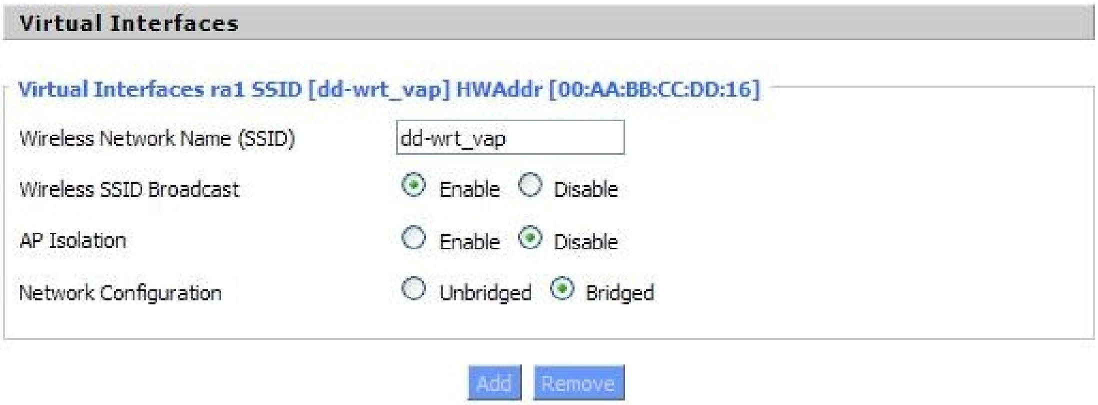
Bridged： Bridge to the Router, under normal circumstances, please select the bridge.

Unbridged： There is no bridge to the 5G CPE, IP addresses need to manually configure.



Network Configuration	● Unbridged ○ Bridged
Multicast forwarding	○ Enable ● Disable
Masquerade / NAT	● Enable ○ Disable
IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 0 . 0

Virtual Interfaces： Click Add to add a virtual interface. Add successfully, click on the remove, you can remove the virtual interface。



Virtual Interfaces

Virtual Interfaces ra1 SSID [dd-wrt_vap] HWAddr [00:AA:BB:CC:DD:16]

Wireless Network Name (SSID) dd-wrt_vap

Wireless SSID Broadcast ● Enable ○ Disable

AP Isolation ○ Enable ● Disable

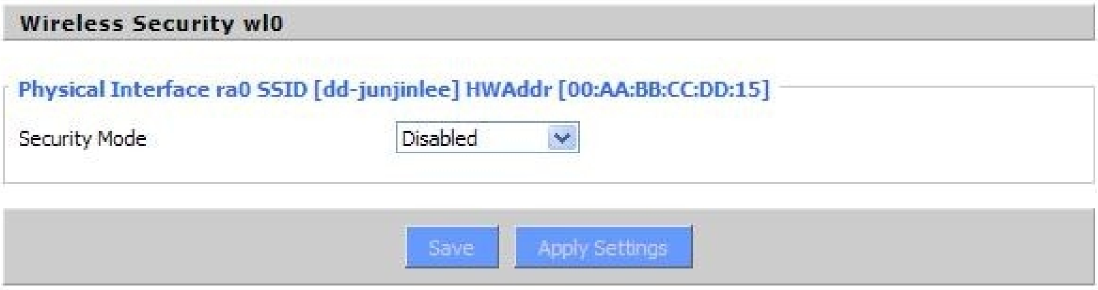
Network Configuration ○ Unbridged ● Bridged

AP Isolation： This setting isolates wireless clients so access to and from other wireless clients are stopped.

Note ： Save your changes, after changing the "Wireless Mode", "Wireless Network Mode", "wireless width", "broadband" option, please click on this button, and then configure the other options.

3.3.2.2 Wireless Security

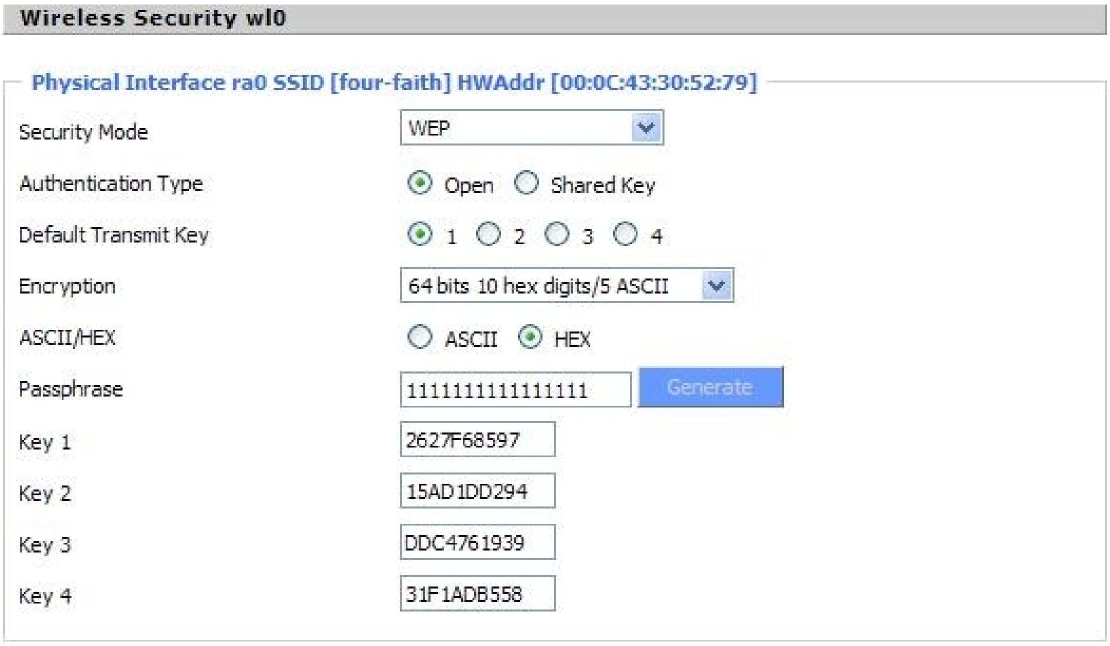
Wireless security options used to configure the security of your wireless network. This route is a total of seven kinds of wireless security mode. Disabled by default, not safe mode is enabled. Such as changes in Safe Mode, click Apply to take effect immediately.



Wireless Security wl0

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode Disabled



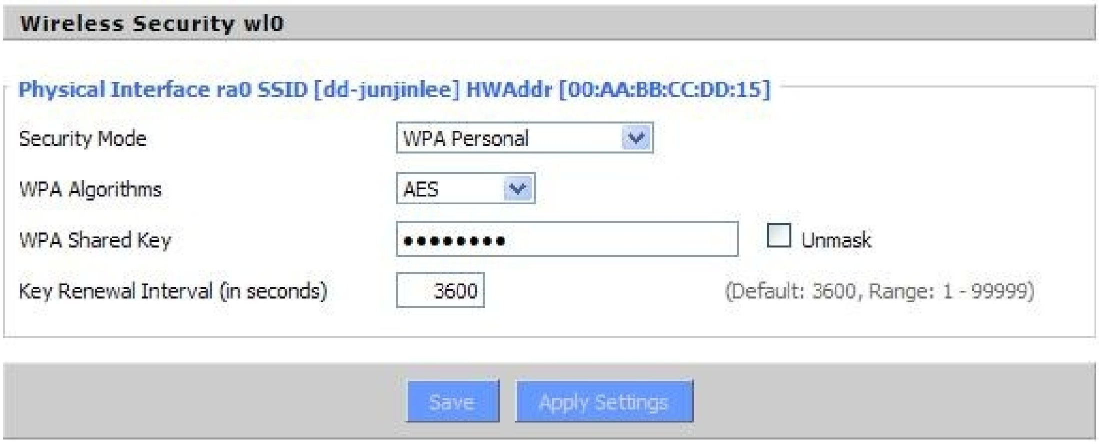
Wireless Security wl0

Physical Interface ra0 SSID [four-faith] HWAddr [00:0C:43:30:52:79]

Security Mode	WEP
Authentication Type	● Open ○ Shared Key
Default Transmit Key	● 1 ○ 2 ○ 3 ○ 4
Encryption	64 bits 10 hex digits/5 ASCII
ASCII/HEX	○ ASCII ● HEX
Passphrase	1111111111111111 Generate
Key 1	2627F68597
Key 2	15AD1DD294
Key 3	DDC4761939
Key 4	31F1ADB558

WEP：Is a basic encryption algorithm is less secure than WPA.Use of WEP is discouraged due to security weaknesses, and one of the WPA modes should be used whenever possible. Only use WEP if you have clients that can only support WEP (usually older, 802.11b-only clients).
Authentication Type：Open or shared key。
Default Transmit Key：Select the key form Key 1 - Key 4 key.
Encryption：There are two levels of WEP encryption, 64-bit (40-bit) and 128-bit. To utilize WEP, select the desired encryption bit, and enter a passphrase or up to four WEP key in hexadecimal format. If you are using 64-bit (40-bit), then each key must consist of exactly 10 hexadecimal characters or 5 ASCII charceters. For 128-bit, each key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0"-"9" and "A"-"F".

ASCII/HEX: ASCII, the keys is 5 bit ASCII characters/13bit ASCII characters.
HEX, the keys is 10bit/26 bit hex digits.
Passphrase：The letters and numbers used to generate a key.
Key1-Key4：Manually fill out or generated according to input the pass phrase.



Wireless Security wl0

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

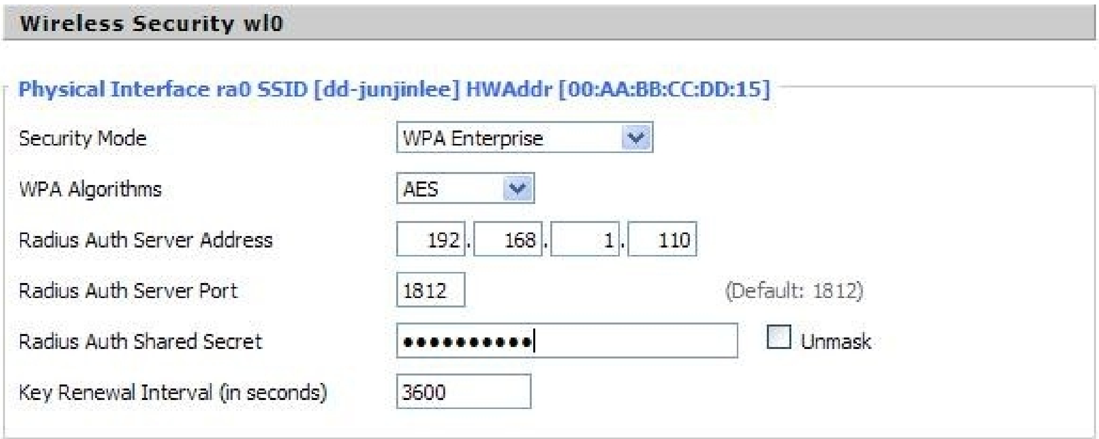
Security Mode	WPA Personal	
WPA Algorithms	AES	
WPA Shared Key	••••••••	□ Unmask
Key Renewal Interval (in seconds)	3600	(Default: 3600, Range: 1 - 99999)

WPA Personal/WPA2 Personal/WPA2 Person Mixed: Provides three WPA algorithms, TKIP and AES, TKIP+AES, using dynamic encryption keys. TKIP+AES, self-applicable TKIP or AES.

WPA Person Mixed, allows WPA Personal and WPA2 Personal clients to be mixed.

WPA Shared Key：Between 8 and 63 ASCII character or hexadecimal digits.。

Key Renewal Interval（in seconds）1-99999。



Wireless Security wl0

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode	WPA Enterprise	
WPA Algorithms	AES	
Radius Auth Server Address	192 . 168 . 1 . 110	
Radius Auth Server Port	1812	(Default: 1812)
Radius Auth Shared Secret	••••••••••	□ Unmask
Key Renewal Interval (in seconds)	3600	

WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed: WPA Enterprise uses an external

RADIUS server to perform user authentication.

WPA Algorithms: AES/TKIP/TPIP+AES.

Radius Auth Sever Address：The IP address of the RADIUS server.

Radius Auth Server Port：The RADIUS Port (default is 1812)。

Radius Auth Shared Secret：The shared secret from the RADIUS server。

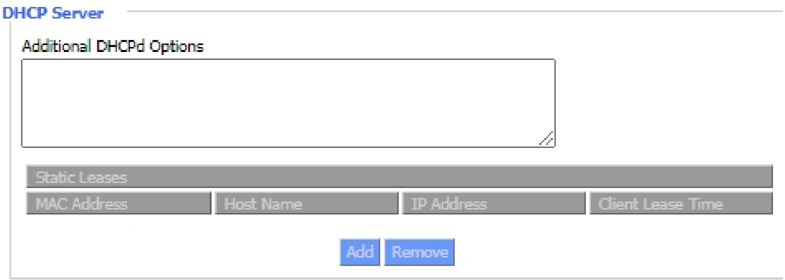
Key Renewal Interva(in seconds): 1-99999。

3.3.3 Service

3.3.3.1 Service

DHCP Server

DHCP assigns IP addresses to users local devices. While the main configuration is on the setup page users can program some nifty special functions here.



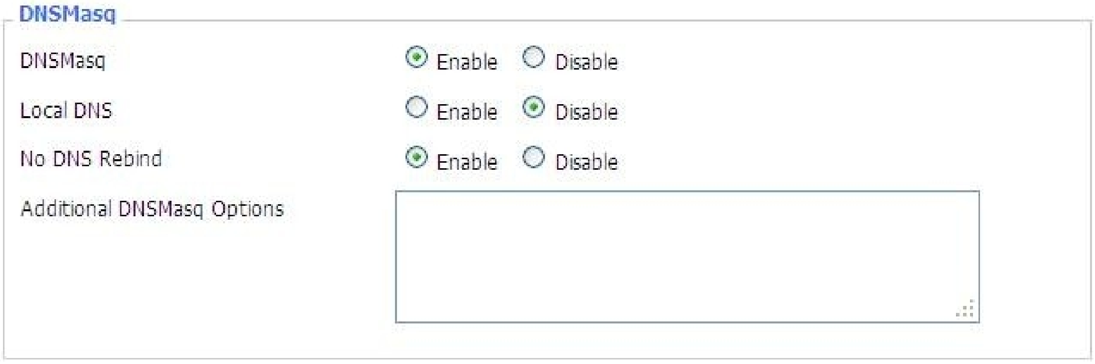
DHCP Server

Additional DHCPd Options

Static Leases			
MAC Address	Host Name	IP Address	Client Lease Time

DNSMasq

DNSmasq is a local DNS server. It will resolve all host names known to the Router from dhcp (dynamic and static) as well as forwarding and caching DNS entries from remote DNS servers. Local DNS enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.



DNSMasq

DNSMasq	● Enable ○ Disable
Local DNS	○ Enable ● Disable
No DNS Rebind	● Enable ○ Disable
Additional DNSMasq Options	

Local DNS: enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames

No DNS Rebind: when enabled, it can prevent an external attacker to access the Router's internal

Web interface. It is a security measure

Additional DNSMasq Options: some extra options users can set by entering them in Additional

DNS Options.

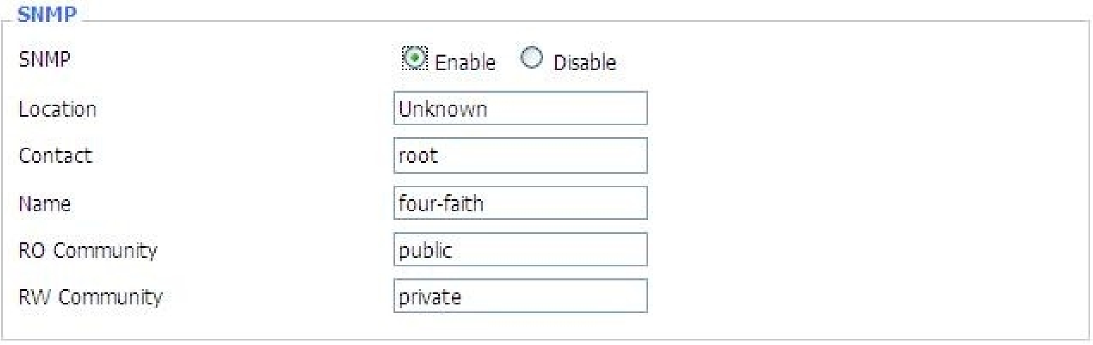
For example:

static allocation: dhcp-host=AB:CD:EF:11:22:33,192.168.0.10,myhost,myhost.domain,12h

max lease number: dhcp-lease-max=2

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

SNMP (Simple Network Management Protocol). This is a widely used network management protocol. The data is passed through the SNMP agent. SNMP agent refers to the hardware and/or software process, which reports the activities of each network device (such as hub, 5G industrial CPE, bridge, etc.) to the workstation, so as to achieve the purpose of monitoring the network. The agent will return the information contained in the MIB (Management Information Base). MIB is a data structure used to define options that can be obtained from the device and that can be controlled (such as on or off).



SNMP

SNMP	● Enable ○ Disable
Location	Unknown
Contact	root
Name	four-faith
RO Community	public
RW Community	private

Location: equipment location

Contact: contact this equipment management

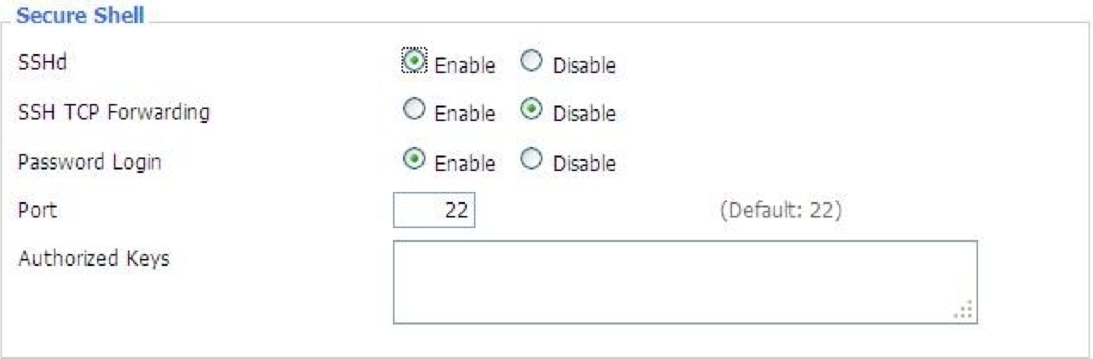
Name: device name

RO Community: SNMP RO community name, the default is public, Only to read.

RW Community: SNMP RW community name, the default is private, Read-write permissions

SSHD

Enabling SSHd allows users to access the Linux OS of their 5G CPE with an SSH client


Secure Shell

SSHd ● Enable ○ Disable

SSH TCP Forwarding ○ Enable ● Disable

Password Login ● Enable ○ Disable

Port 22 (Default: 22)

Authorized Keys

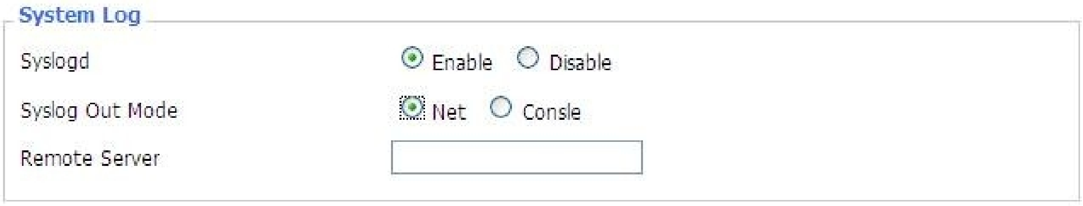
SSH TCP Forwarding: enable or disable to support the TCP forwarding

Password Login: allows login with the Router password (username is

admin) **Port:** port number for SSHd (default is 22)

Authorized Keys: here users paste their public keys to enable key-based login (more secure than a simple password)

System log


System Log

Syslogd ● Enable ○ Disable

Syslog Out Mode ● Net ○ Consle

Remote Server

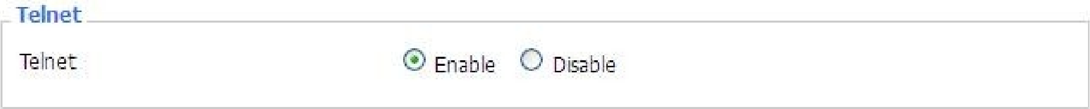
Syslog Out Mode: two log mode

Net: the log information output to a syslog server

Console: the log information output to console port

Remote Server: if choose net mode, users should input a syslog server's IP Address and run a syslog server program on it.

Telnet

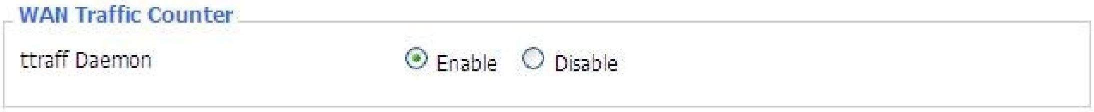

Telnet

Telnet ● Enable ○ Disable

Telnet: enable a telnet server to connect to the Router with telnet. The username is admin and the password is the Router's password.

Note: If users use the Router in an untrusted environment (for example as a public hotspot), it is strongly recommended to use SSHd and deactivate telnet.

WAN Traffic Counter



WAN Traffic Counter

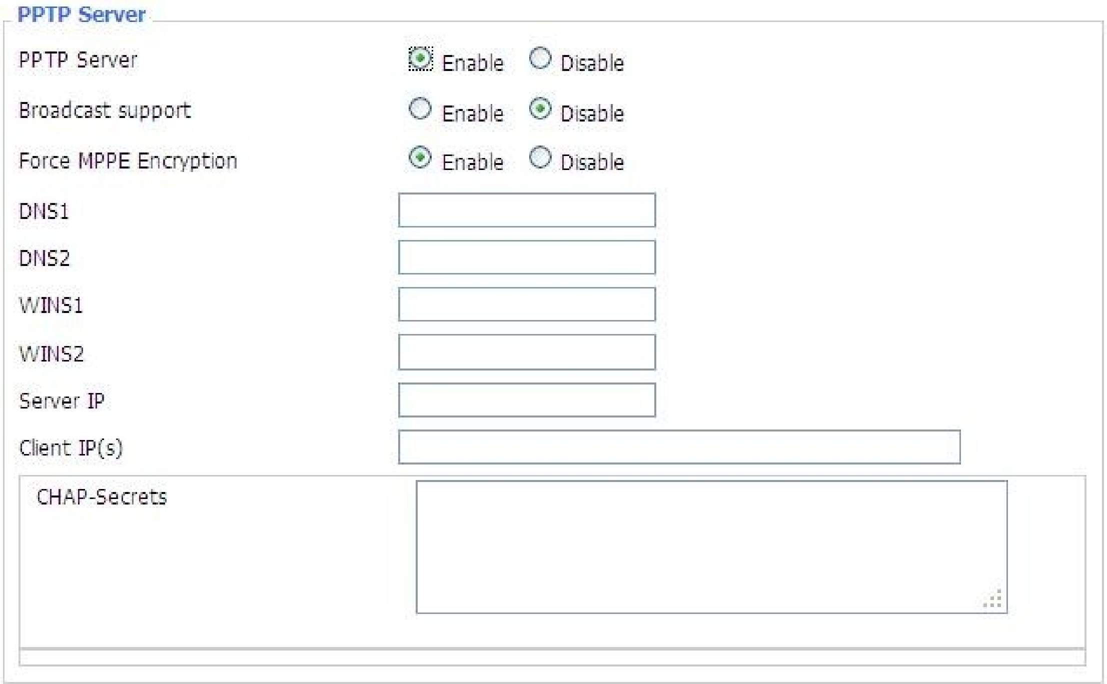
ttraff Daemon ● Enable ○ Disable

Ttraff Daemon: enable or disable wan traffic counter function

3.3.4 VPN

3.3.4.1 PPTP

PPTP Server



PPTP Server

PPTP Server	● Enable ○ Disable
Broadcast support	○ Enable ● Disable
Force MPPE Encryption	● Enable ○ Disable
DNS1	
DNS2	
WINS1	
WINS2	
Server IP	
Client IP(s)	
CHAP-Secrets	

Broadcast support: enable or disable broadcast support of PPTP server

Force MPPE Encryption: enable of disable force MPPE encryption of PPTP data

DNS1/DNS2/WINS1/WINS2: set DNS1/DNS2/WINS1/WINS2

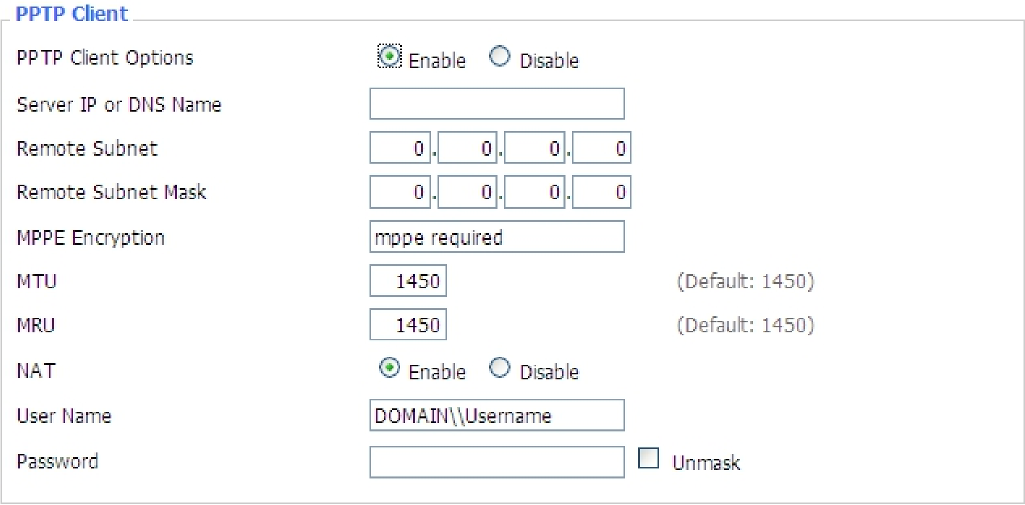
Server IP: input IP address of the Router as PPTP server, differ from LAN address

Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx CHAP Secrets: user name and password of the client using PPTP service

Note: client IP must be different with IP assigned by Router DHCP.

The format of CHAP Secrets is user * password *.

PPTP Client



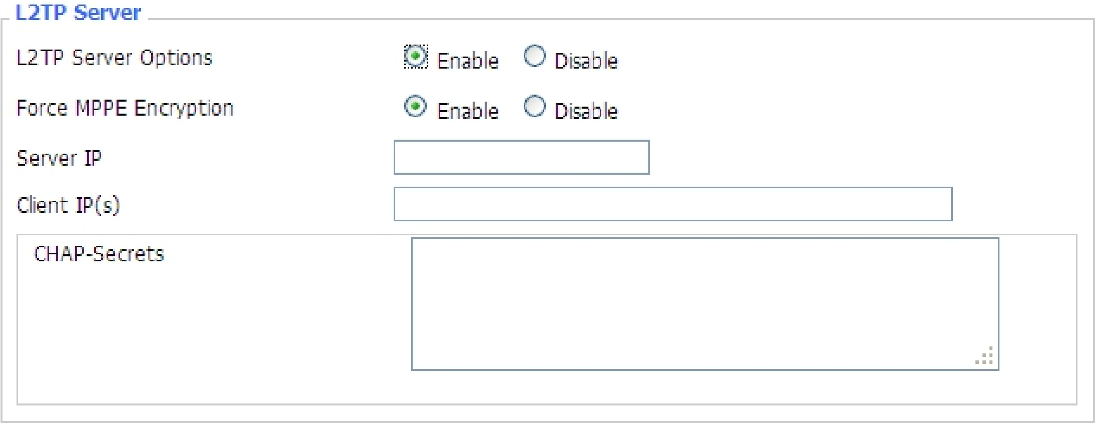
PPTP Client

PPTP Client Options	● Enable ○ Disable
Server IP or DNS Name	
Remote Subnet	0. 0. 0. 0
Remote Subnet Mask	0. 0. 0. 0
MPPE Encryption	mppe required
MTU	1450 (Default: 1450)
MRU	1450 (Default: 1450)
NAT	● Enable ○ Disable
User Name	DOMAIN\\Username
Password	□ Unmask

Server IP or DNS Name: PPTP server's IP Address or DNS Name
Remote Subnet: the network of the remote PPTP server
Remote Subnet Mask: subnet mask of remote PPTP server
MPPE Encryption: enable or disable Microsoft Point-to-Point Encryption。
MTU: maximum Transmission Unit
MRU: maximum Receive Unit
NAT: network Address Translation
User Name: user name to login PPTP Server.
Password: password to log into PPTP Server.

3.3.4.2 L2TP

L2TP Server



L2TP Server

L2TP Server Options	● Enable ○ Disable
Force MPPE Encryption	● Enable ○ Disable
Server IP	
Client IP(s)	
CHAP-Secrets	

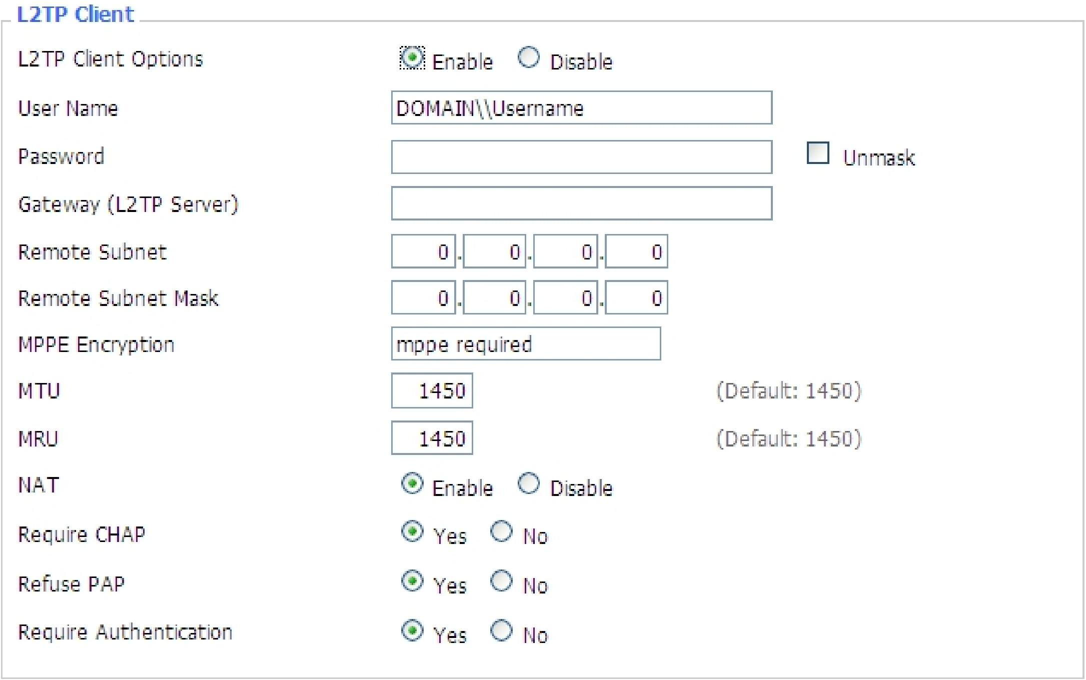
Force MPPE Encryption: enable or disable force MPPE encryption of L2TP data
Server IP: input IP address of the 5G CPE as PPTP server, differ from LAN address
Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx

CHAP Secrets: user name and password of the client using L2TP service

Note: client IP must be different with IP assigned by DHCP.

The format of CHAP Secrets is user * password *.

L2TP Client



L2TP Client

L2TP Client Options	● Enable ○ Disable	
User Name	DOMAIN\\Username	
Password		□ Unmask
Gateway (L2TP Server)		
Remote Subnet	0. 0. 0. 0	
Remote Subnet Mask	0. 0. 0. 0	
MPPE Encryption	mppe required	
MTU	1450	(Default: 1450)
MRU	1450	(Default: 1450)
NAT	● Enable ○ Disable	
Require CHAP	● Yes ○ No	
Refuse PAP	● Yes ○ No	
Require Authentication	● Yes ○ No	

Gateway(L2TP Server): L2TP server’s IP Address or DNS Name

Remote Subnet: the network of remote PPTP server

Remote Subnet Mask: subnet mask of remote PPTP server

MPPE Encryption: enable or disable Microsoft Point-to-Point Encryption

MTU: maximum transmission unit

MRU: maximum receive unit

NAT: network address translation

User Name: user name to login L2TP Server

Password: password to login L2TP Server

Require CHAP: enable or disable support chap authentication protocol

Refuse PAP: enable or disable refuse to support the pap authentication

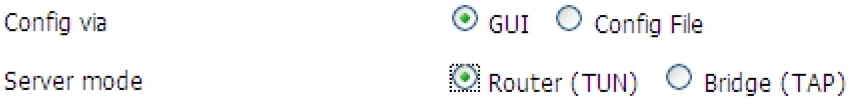
Require Authentication: enable or disable support authentication protocol

3.3.4.3 OPENVPN

OPENVPN Server

Start Type ○ WAN Up ● System

Start Type: WAN UP----start after on-line, System----start when boot up



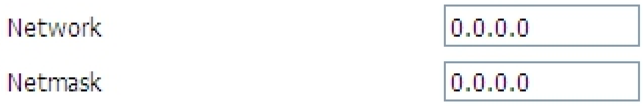
Config via ● GUI ○ Config File

Server mode ● Router (TUN) ○ Bridge (TAP)

Config via: GUI----Page configuration, Config File----config File configuration

Server mode: Router (TUN)-route mode, Bridge (TAP)----bridge mode

Router (TUN):



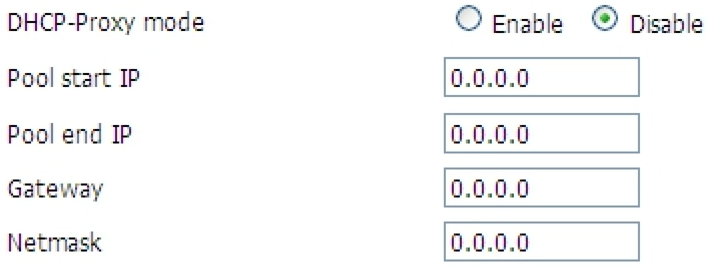
Network 0.0.0.0

Netmask 0.0.0.0

Network: network address allowed by OPENVPN server

Netmask: netmask allowed by OPENVPN server

Bridge (TAP):



DHCP-Proxy mode ○ Enable ● Disable

Pool start IP 0.0.0.0

Pool end IP 0.0.0.0

Gateway 0.0.0.0

Netmask 0.0.0.0

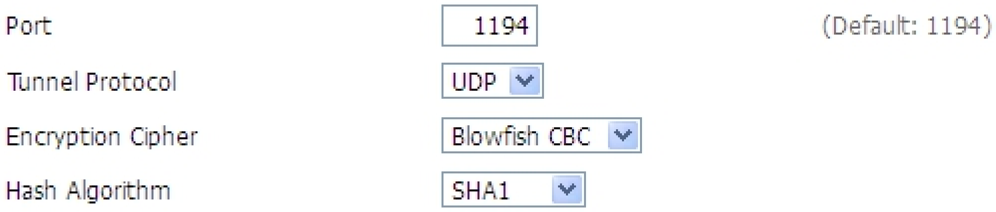
DHCP-Proxy mode: enable or disable DHCP-Proxy mode

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

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

Gateway: the gateway of the client allowed by OPENVPN server

Netmask: netmask of the client allowed by OPENVPN server



Port 1194 (Default: 1194)

Tunnel Protocol UDP

Encryption Cipher Blowfish CBC

Hash Algorithm SHA1

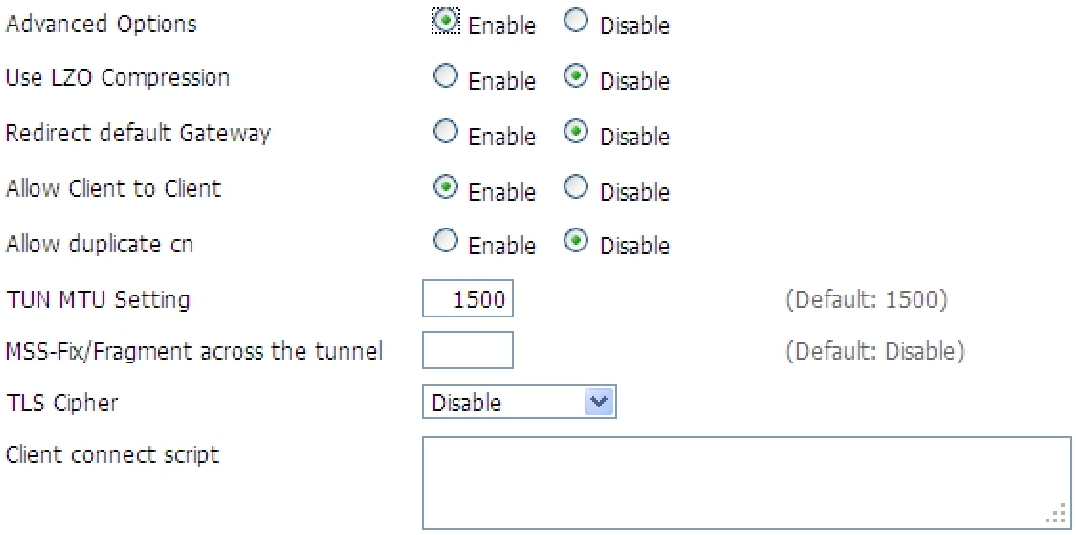
Port: listen port of OPENVPN server

Tunnel Protocol: UCP or TCP of OPENVPN tunnel protocol

Encryption Cipher: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC

Hash Algorithm: Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, MD5

Advanced Options



Advanced Options	● Enable ○ Disable	
Use LZO Compression	○ Enable ● Disable	
Redirect default Gateway	○ Enable ● Disable	
Allow Client to Client	● Enable ○ Disable	
Allow duplicate cn	○ Enable ● Disable	
TUN MTU Setting	1500	(Default: 1500)
MSS-Fix/Fragment across the tunnel		(Default: Disable)
TLS Cipher	Disable	
Client connect script		

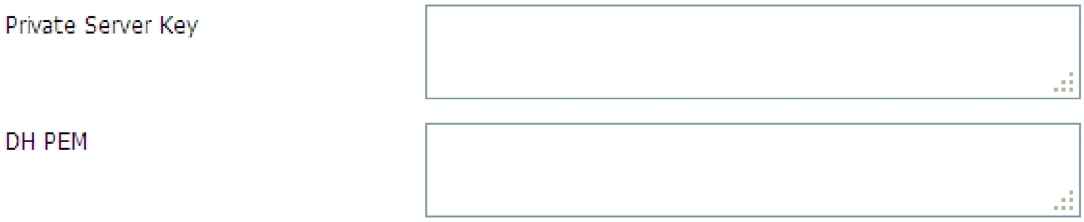
Use LZO Compression: enable or disable use LZO compression for data transfer
Redirect default Gateway: enable or disable redirect default gateway
Allow Client to Client: enable or disable allow client to client
Allow duplicate cn: enable or disable allow duplicate cn
TUN MTU Setting: set the value of TUN MTU
TCP MSS: MSS of TCP data
TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA
Client connect script: define some client script by user self

CA Cert

CA Cert: CA certificate

Public Server Cert

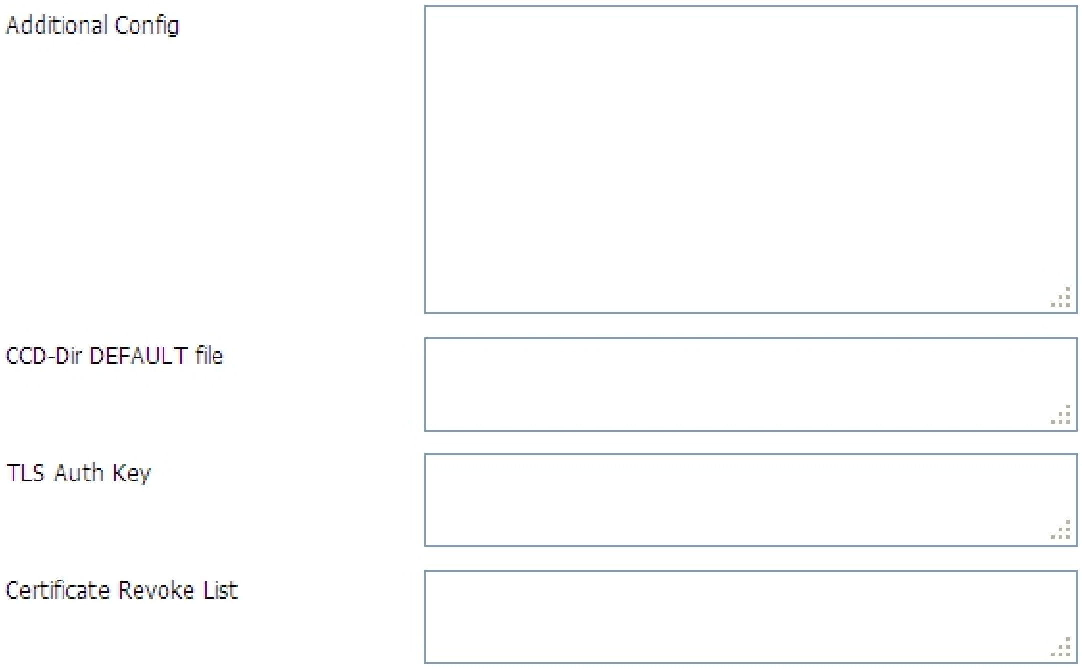
Public Server Cert: server certificate



Private Server Key

DH PEM

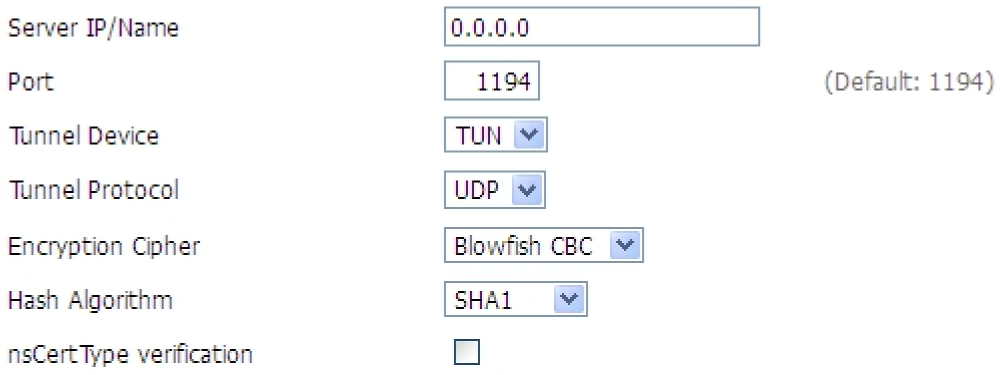
Private Server Key: the key seted by the server
DH PEM: PEM of the server



Additional Config	
CCD-Dir DEFAULT file	
TLS Auth Key	
Certificate Revoke List	

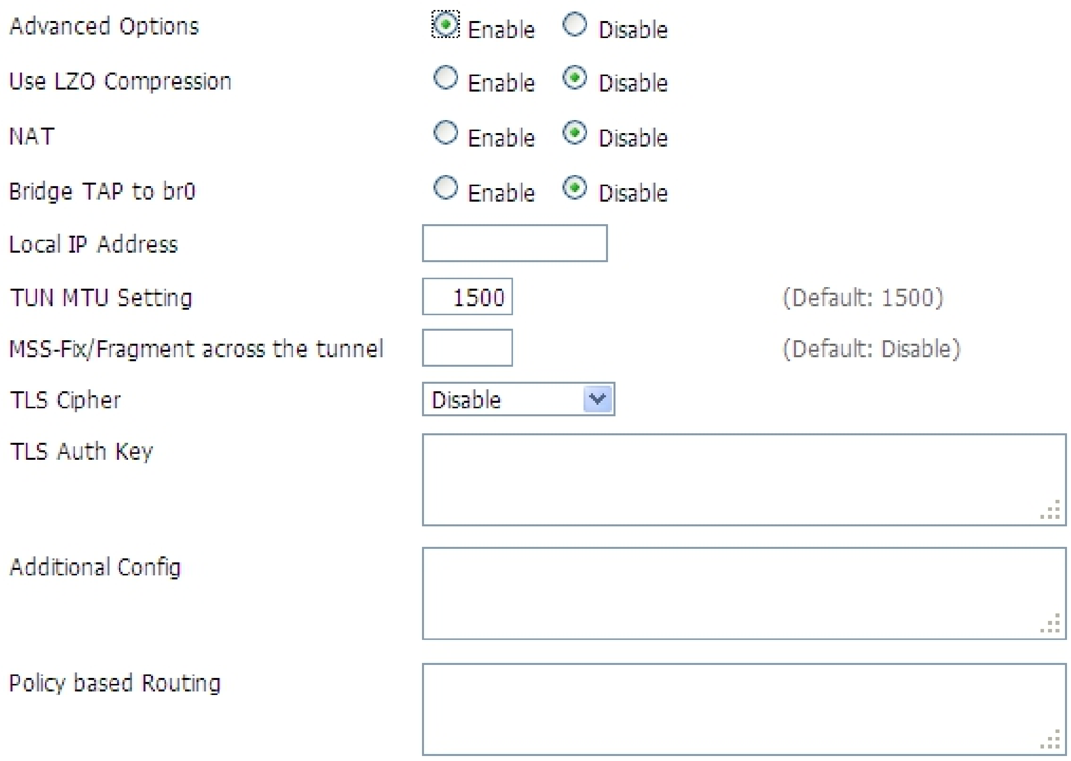
Additional Config: additional configurations of the server
CCD-Dir DEFAULT file: other file approaches
TLS Auth Key: authority key of Transport Layer Security
Certificate Revoke List: configure some revoke certificates

OPENVPN Client



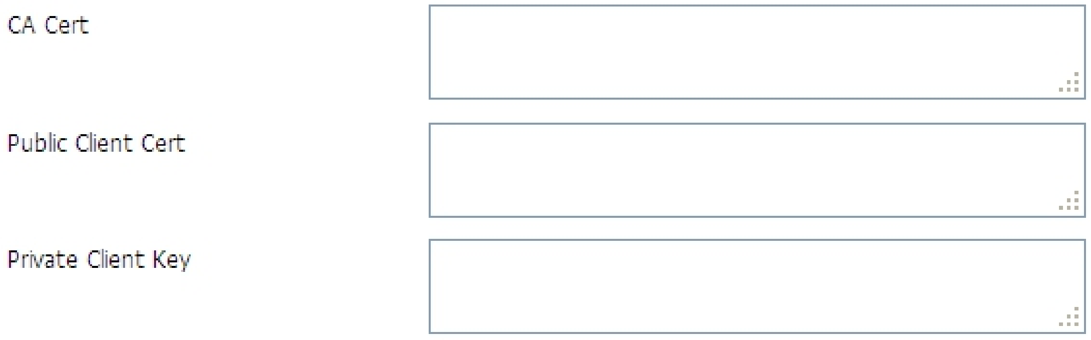
Server IP/Name	0.0.0.0	
Port	1194	(Default: 1194)
Tunnel Device	TUN	
Tunnel Protocol	UDP	
Encryption Cipher	Blowfish CBC	
Hash Algorithm	SHA1	
nsCertType verification	□	

Server IP/Name: IP address or domain name of OPENVPN server
Port: listen port of OPENVPN client
Tunnel Device: TUN----Router mode, TAP----Bridge mode
Tunnel Protocol: UDP and TCP protocol
Encryption Cipher: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC
Hash Algorithm: Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, MD5
nsCertType verification: support ns certificate type



Advanced Options	● Enable ○ Disable	
Use LZO Compression	○ Enable ● Disable	
NAT	○ Enable ● Disable	
Bridge TAP to br0	○ Enable ● Disable	
Local IP Address		
TUN MTU Setting	1500	(Default: 1500)
MSS-Fix/Fragment across the tunnel		(Default: Disable)
TLS Cipher	Disable	
TLS Auth Key		
Additional Config		
Policy based Routing		

Use LZO Compression: enable or disable use LZO compression for data transfer
NAT: enable or disable NAT through function
Bridge TAP to br0: enable or disable bridge TAP to br0
Local IP Address: set IP address of local OPENVPN client
TUN MTU Setting: set MTU value of the tunnel
TCP MSS: mss of TCP data
TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA
TLS Auth Key: authority key of Transport Layer Security
Additional Config: additional configurations of OPENVPN server
Policy based Routing: input some defined routing policy



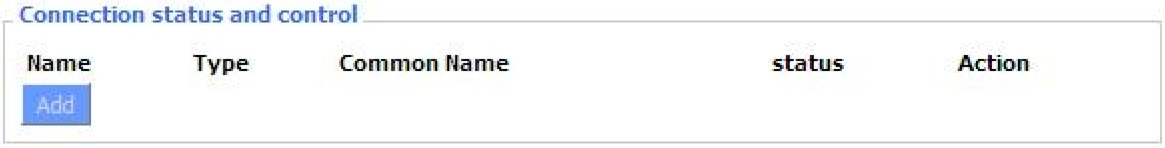
CA Cert	
Public Client Cert	
Private Client Key	

CA Cert: CA certificate
Public Client Cert: client certificate
Private Client Key: client key

3.3.4.4 IPSEC

Connect Status and Control

Show IPSEC connection and status of current 5G CPE on IPSEC page.



Connection status and control

Name	Type	Common Name	status	Action
Add				

Name: the name of IPSEC connection

Type: The type and function of current IPSEC connection

Common name: local subnet, local address, opposite end address and opposite end subnet of current connection

Status: connection status: closed, negotiating, establish

Closed: this connection does not launch a connection request to opposite end

Negotiating: this connection launch a request to opposite end, is under negotiating, the connection has not been established yet

Establish: the connection has been established, enabled to use this tunnel

Action: the action of this connection, current is to delete, edit, reconnect and enable

Delete: to delete the connection, also will delete IPSEC if IPSEC has set up

Edit: to edit the configure information of this connection, reload this connection to make the configuration effect after edit

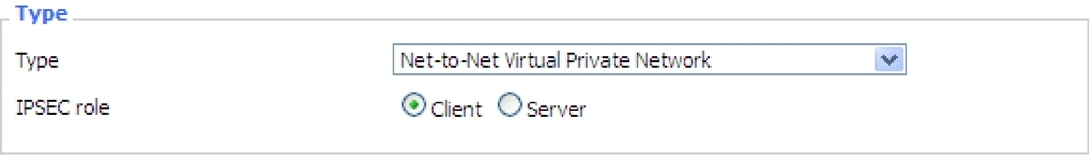
Reconnect: this action will remove current tunnel, and re-launch tunnel establish request

Enable: when the connection is enable, it will launch tunnel establish request when the system reboot or reconnect, otherwise the connection will not do it

Add: to add a new IPSEC connection

Add IPSEC connection or edit IPSEC connection

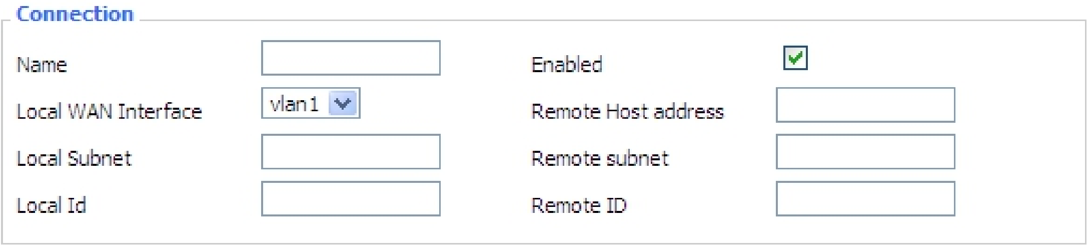
Type: to choose IPSEC mode and relevant functions in this part, supports tunnel mode client, tunnel mode server and transfer mode currently



Type

Type	Net-to-Net Virtual Private Network
IPSEC role	● Client ○ Server

Connection: this part contains basic address information of the tunnel



Connection

Name		Enabled	☑
Local WAN Interface	vlan1	Remote Host address	
Local Subnet		Remote subnet	
Local Id		Remote ID	

Name: to indicate this connection name, must be unique

Enabled: If enable, the connection will send tunnel connection request when it is reboot or re-connection, otherwise it is no need if disable

Local WAN Interface: local addresss of the tunnel

Remote Host Address: IP/domain name of end opposite; this option can not fill in if using tunnel mode server

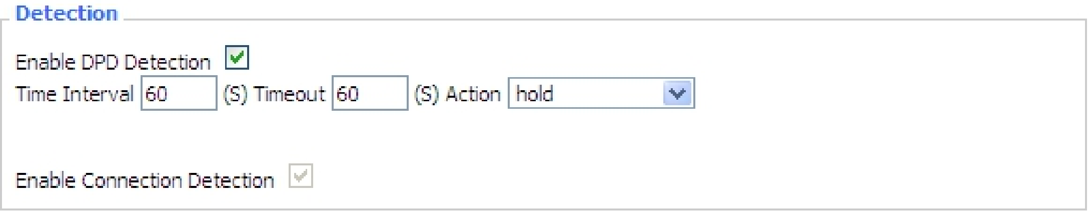
Local Subnet: IPSec local protects subnet and subnet mask, i.e. 192.168.1.0/24; this option can not fill in if using transfer mode

Remote Subnet: IPSec opposite end protects subnet and subnet mask, i.e.192.168.7.0/24; this option can not fill in if using transfer mode

Local ID: tunnel local end identification, IP and domain name are available

Remote ID: tunnel opposite end identification, IP and domain name are available

Detection: this part contains configure information of connection detection



Detection

Enable DPD Detection ☑

Time Interval 60 (S) Timeout 60 (S) Action hold

Enable Connection Detection ☑

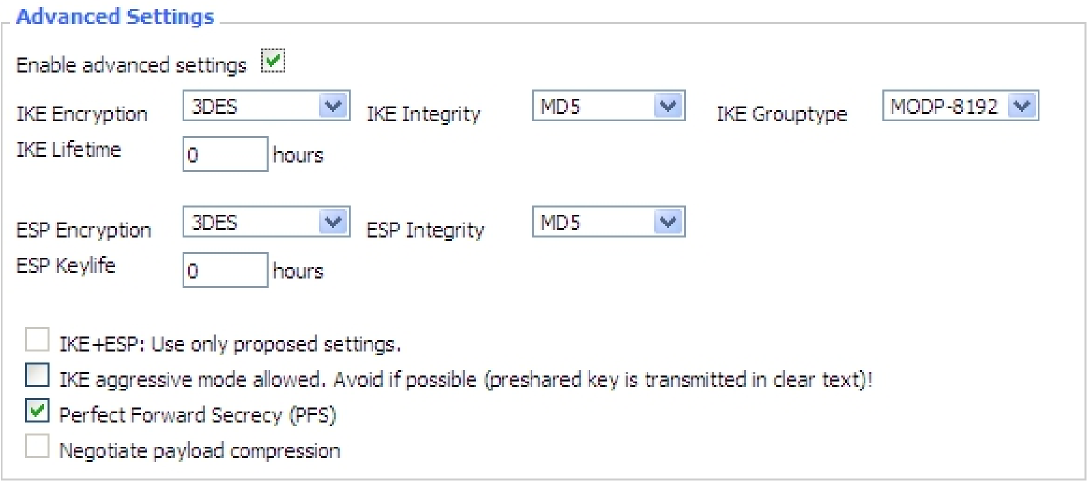
Enable DPD Detection: enable or disable this function, tick means enable

Time Interval: set time interval of connect detection (DPD)

Timeout: set the timeout of connect detection

Action: set the action of connect detection

Advanced Settings: this part contains relevant setting of IKE, ESP, negotiation mode, etc.



Advanced Settings

Enable advanced settings ☑

IKE Encryption 3DES IKE Integrity MD5 IKE Grouptype MODP-8192

IKE Lifetime 0 hours

ESP Encryption 3DES ESP Integrity MD5

ESP Keylife 0 hours

□ IKE+ESP: Use only proposed settings.

□ IKE aggressive mode allowed. Avoid if possible (preshared key is transmitted in clear text)!

☑ Perfect Forward Secrecy (PFS)

□ Negotiate payload compression

Enable Advanced Settings: enable to configure 1st and 2nd phase information, otherwise it

will automic negotiation according to opposite end

IKE Encryption: IKE phased encryption mode

IKE Integrity: IKE phased integrity solution

IKE Grouptype: DH exchange algorithm

IKE Lifetime: set IKE lifetime, current unit is hour, the default is 0

ESP Encryption: ESP encryption type

ESP Integrity: ESP integrity solution

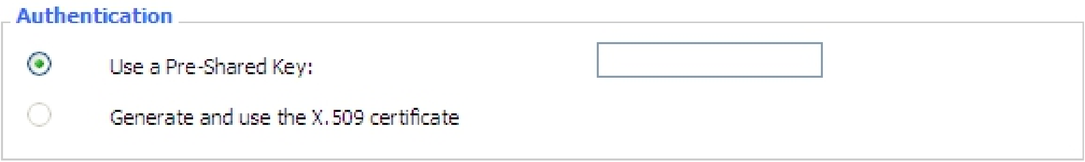
ESP Keylife: set ESP keylife, current unit is hour, the default is 0

IKE aggressive mode allowed: negotiation mode adopt aggressive mode if tick; it is main

mode if non-tick

Negotiate payload compression: Tick to enable PFS, non-tick to diable PFS

Authentication: choose use share encryption option or certificate authentication option. Current is only to choose use share encryption option.



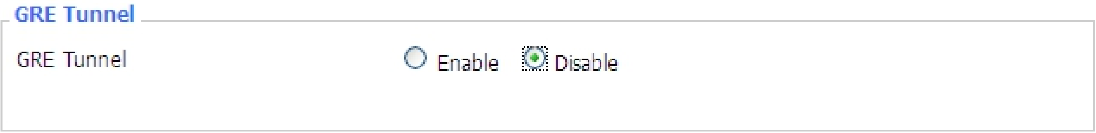
Authentication

● Use a Pre-Shared Key:

○ Generate and use the X.509 certificate

3.3.4.5 GRE

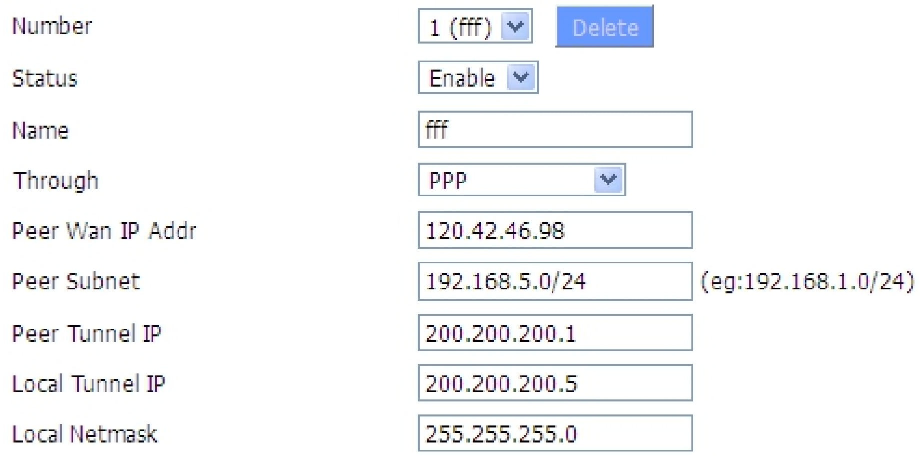
GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) protocol is a network layer protocol (such as IP and IPX) data packets are encapsulated, so these encapsulated data packets to another network layer protocol (IP)transmission. GRE Tunnel (tunnel) technology, Layer Two Tunneling Protocol VPN (Virtual Private Network).



GRE Tunnel

GRE Tunnel	○ Enable ● Disable

GRE Tunnel: enable or disable GRE function



Number	1 (fff) Delete
Status	Enable
Name	fff
Through	PPP
Peer Wan IP Addr	120.42.46.98
Peer Subnet	192.168.5.0/24 (eg:192.168.1.0/24)
Peer Tunnel IP	200.200.200.1
Local Tunnel IP	200.200.200.5
Local Netmask	255.255.255.0

Number：Switch on/off GRE tunnel app

Status：Switch on/off someone GRE tunnel app

Name：GRE tunnel name

Through：The GRE packet transmit interface

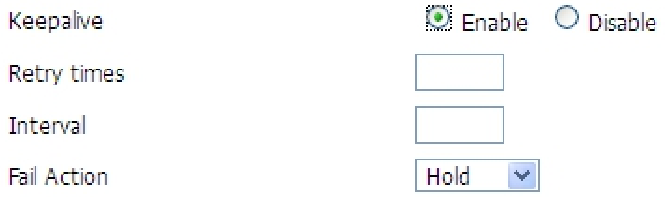
Peer Wan IP Addr：The remote WAN address

Peer Subnet：The remote gateway local subnet, eg: 192.168.1.0/24

Peer Tunnel IP：The remote tunnel ip address

Local Tunnel IP：The local tunnel ip address

Local Netmask：Netmask of local network



Keepalive	● Enable ○ Disable
Retry times	
Interval	
Fail Action	Hold

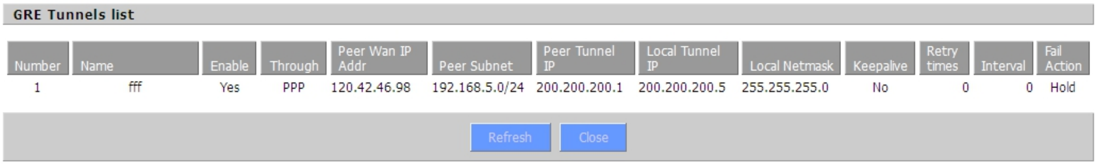
Keepalive：Enable or disable GRE Keepalive function

Retry times：GRE keepalive detect fail retries

Interval：The time interval of GRE keepalive packet sent

Fail Action：The action would be exec after keeping alive failed

Click on "**View GRE tunnels**" keys can view the information of GRE



GRE Tunnels list

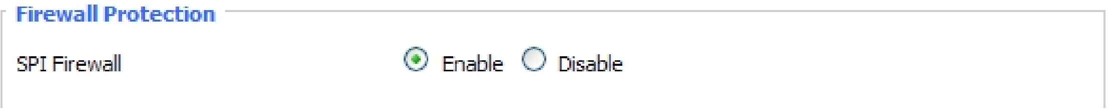
Number	Name	Enable	Through	Peer Wan IP Addr	Peer Subnet	Peer Tunnel IP	Local Tunnel IP	Local Netmask	Keepalive	Retry times	Interval	Fail Action
1	fff	Yes	PPP	120.42.46.98	192.168.5.0/24	200.200.200.1	200.200.200.5	255.255.255.0	No	0	0	Hold

3.3.5 SECURITY

3.3.5.1 Firewall

You can enable or disable the firewall, filter specific Internet data types,and prevent anonymous Internet requests,ultimately enhance network security.

Firewall Protection

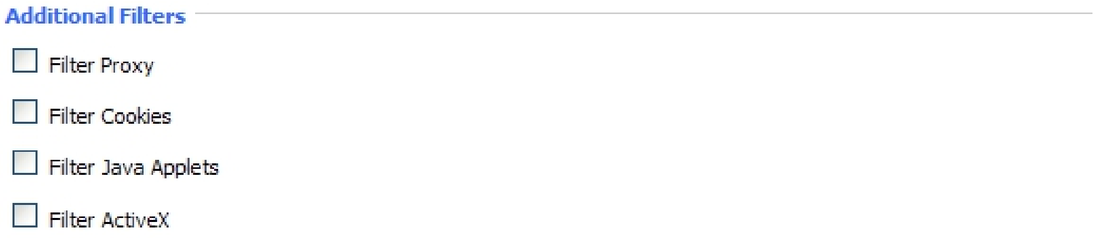


Firewall Protection

SPI Firewall ● Enable ○ Disable

Firewall enhance network security and use SPI to check the packets into the network.To use firewall protection, choose to enable otherwise disabled. Only enable the SPI firewall, you can use other firewall functions: filtering proxy, block WAN requests, etc.

Additional Filters



Additional Filters

□ Filter Proxy
□ Filter Cookies
□ Filter Java Applets
□ Filter ActiveX

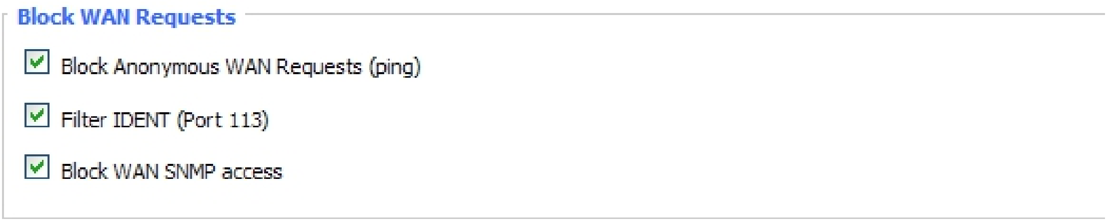
Filter Proxy: Wan proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

Filter Cookies: Cookies are the website of data the data stored on your computer.When you interact with the site ,the cookies will be used. Click the check box to enable the function otherwise disabled.

Filter Java Applets: If refuse to Java, you may not be able to open web pages using the Java programming.. Click the check box to enable the function otherwise disabled.

Filter ActiveX: If refuse to ActiveX, you may not be able to open web pages using the ActiveX programming. Click the check box to enable the function otherwise disabled.

Prevent WAN Request



Block WAN Requests

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

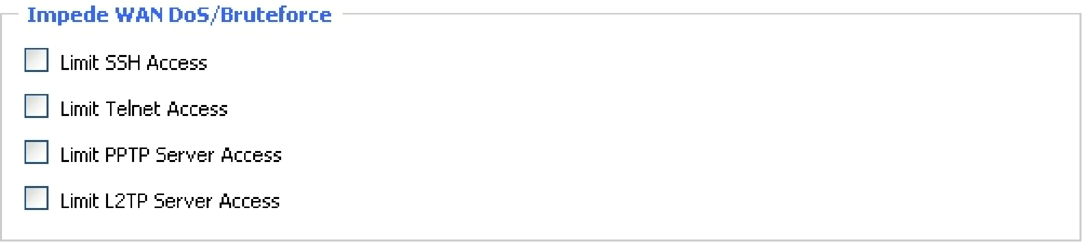
Block Anonymous WAN Requests (ping): By selecting "Block Anonymous WAN Requests (ping)" box to enable this feature, you can prevent your network from the Ping or detection of other Internet users. so that make More difficult to break into your network. The default state of this feature is enabled ,choose to disable allow anonymous Internet requests.

Filter IDENT (Port 113): Enable this feature can prevent port 113 from being scaned from outside. Click the check box to enable the function otherwise disabled.

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

After Complete the changes, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

Impede WAN DoS/Bruteforce



Impede WAN DoS/Bruteforce

□ Limit SSH Access

□ Limit Telnet Access

□ Limit PPTP Server Access

□ Limit L2TP Server Access

Limit ssh Access: This feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

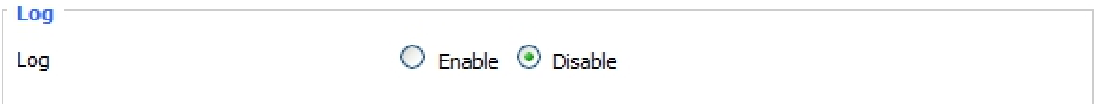
Limit Telnet Access: This feature limits the access request from the WAN by Telnet, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit PPTP Server Access: When build a PPTP Server in the 5G CPE,this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP . Any new access request will be automatically dropped.

Limit L2TP Server Access: When build a L2TP Server in the 5G CPE, this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Log Management

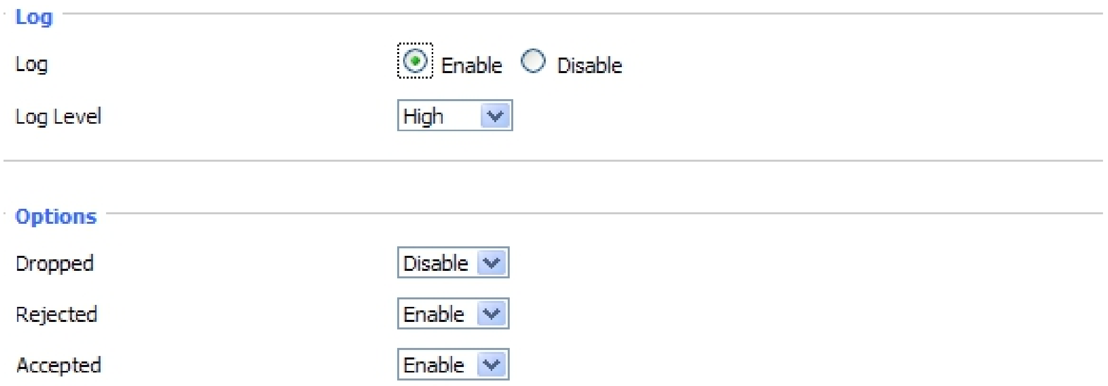
5G CPE can keep logs of all incoming or outgoing traffic for your Internet connection.



Log

Log ○ Enable ● Disable

Log: To keep activity logs, select Enable. To stop logging, select Disable. When select enable, the following page will appear.



Log

Log	● Enable ○ Disable
Log Level	High

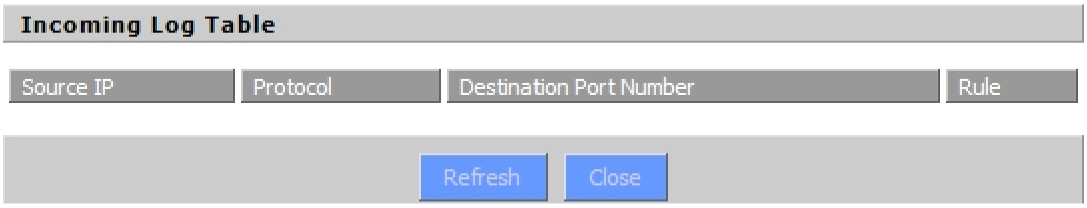
Options

Dropped	Disable
Rejected	Enable
Accepted	Enable

Log Level: Set this to the required log level. Set Log Level higher to log more actions.

Options: When select Enable, the corresponding connection will be recorded in the journal, the disabled are not recorded.

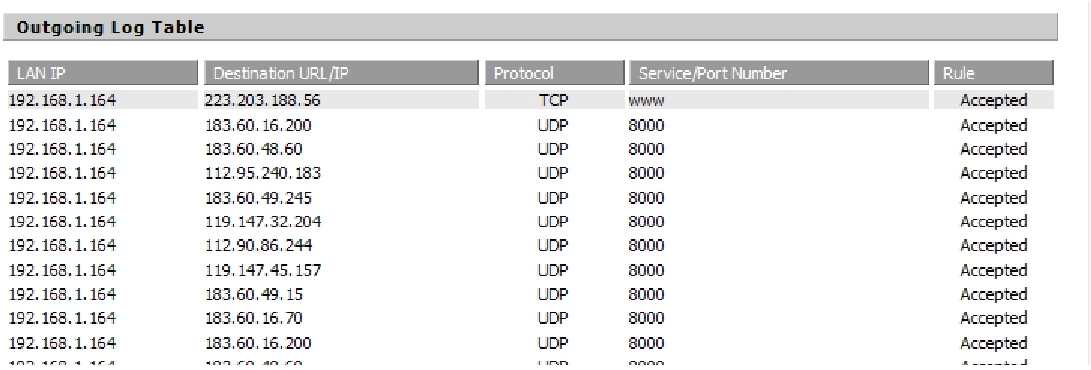
Incoming Log: To see a temporary log of the 5G CPE's most recent incoming traffic, click the Incoming Log button.



Incoming Log Table

Source IP	Protocol	Destination Port Number	Rule

Outgoing Log: To see a temporary log of the 5G CPE's most recent outgoing traffic, click the Outgoing Log button.



Outgoing Log Table

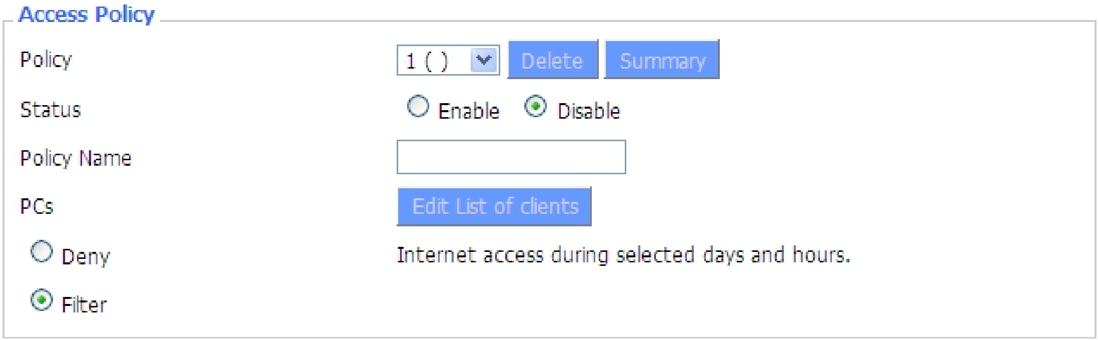
LAN IP	Destination URL/IP	Protocol	Service/Port Number	Rule
192.168.1.164	223.203.188.56	TCP	www	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted
192.168.1.164	112.95.240.183	UDP	8000	Accepted
192.168.1.164	183.60.49.245	UDP	8000	Accepted
192.168.1.164	119.147.32.204	UDP	8000	Accepted
192.168.1.164	112.90.86.244	UDP	8000	Accepted
192.168.1.164	119.147.45.157	UDP	8000	Accepted
192.168.1.164	183.60.49.15	UDP	8000	Accepted
192.168.1.164	183.60.16.70	UDP	8000	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted

Click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

3.3.6 Access Restrictions

3.3.6.1 WAN Access

Use access restrictions, you can block or allow specific types of Internet applications. You can set specific PC-based Internet access policies. This feature allows you to customize up to ten different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses.


Access Policy

Policy: 1 ( ) [Delete] [Summary]

Status: ○ Enable ● Disable

Policy Name:

PCs: [Edit List of clients]

○ Deny
● Filter

Internet access during selected days and hours.

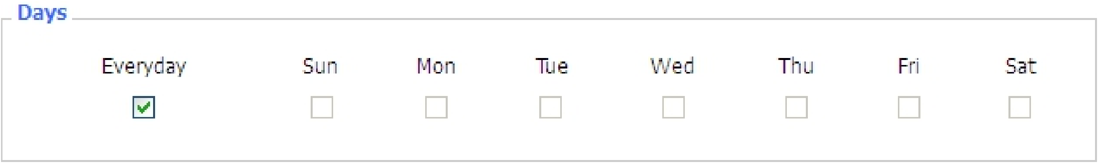
Two options in the default policy rules: "Filter" and "reject". If select "Deny”, you will deny specific computers to access any Internet service at a particular time period. If you choose to "filter"，It will block specific computers to access the specific sites at a specific time period. You can set up 10 Internet access policies filtering specific PCs access Internet services at a particular time period.

Access Policy: You may define up to 10 access policies. Click Delete to delete a policy or Summary to see a summary of the policy.

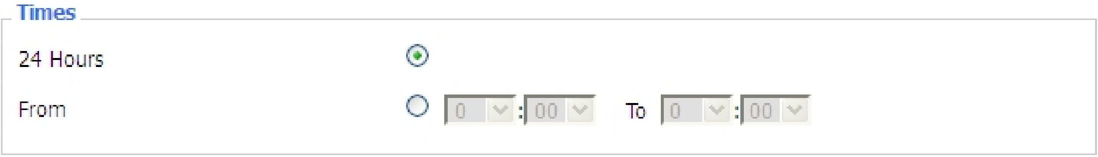
Status: Enable or disable a policy.

Policy Name: You may assign a name to your policy.

PCs: The part is used to edit client list, the strategy is only effective for the PC in the list.


Days

Everyday	Sun	Mon	Tue	Wed	Thu	Fri	Sat
☑	□	□	□	□	□	□	□

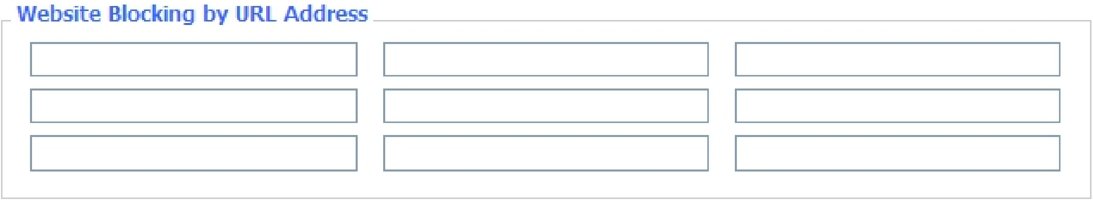

Times

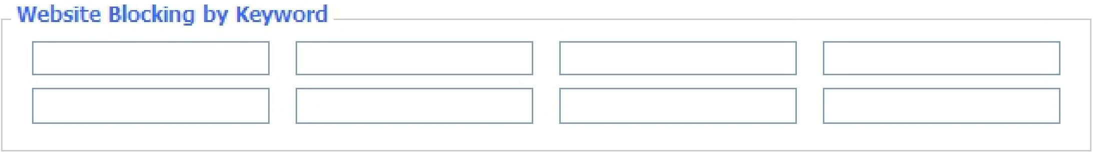
24 Hours: ●

From: ○ 0 : 00 To 0 : 00

Days: Choose the day of the week you would like your policy to be applied.

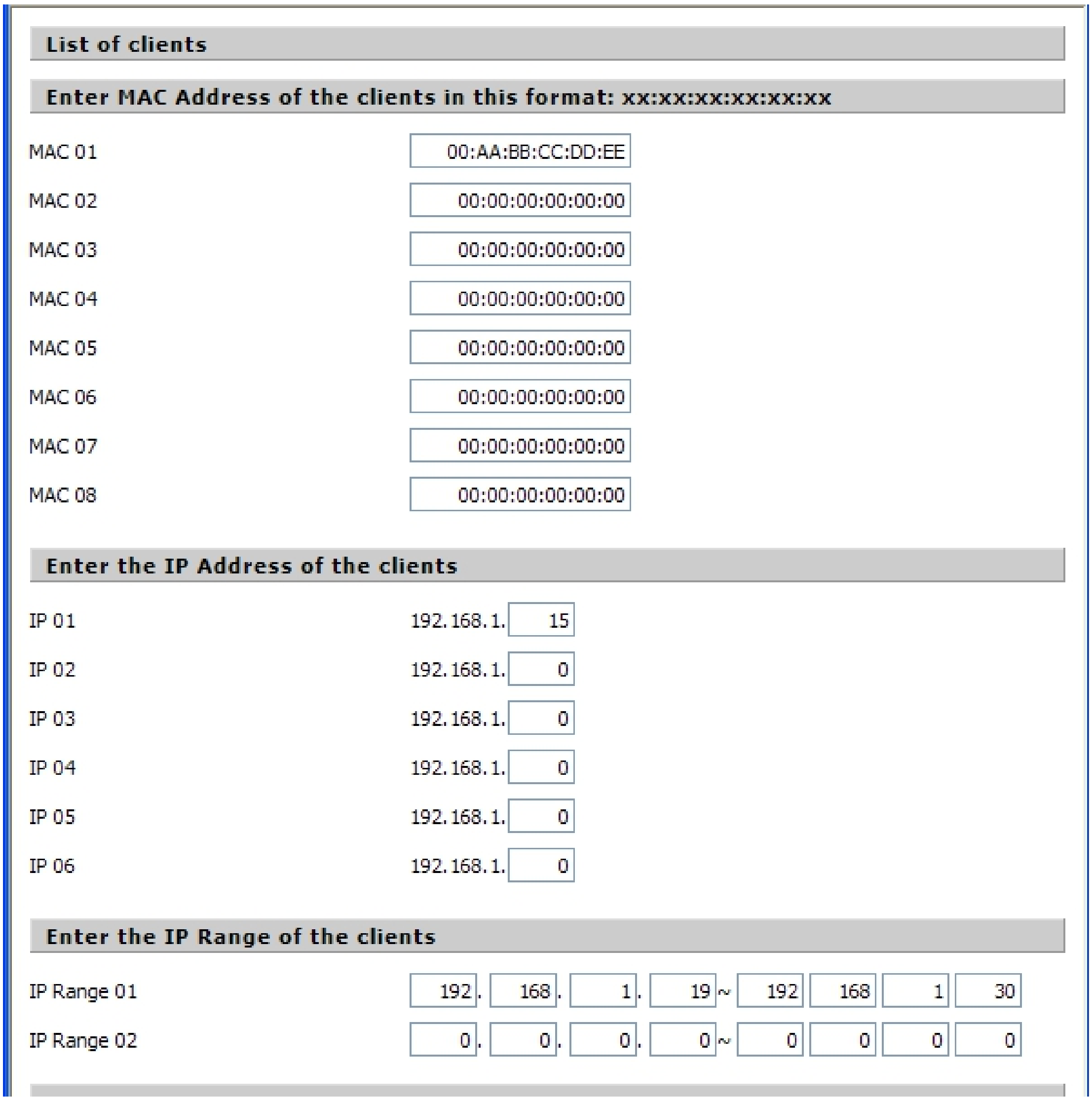
Times: Enter the time of the day you would like your policy to be applied.


Website Blocking by URL Address


Website Blocking by Keyword

Website Blocking by URL Address: You can block access to certain websites by entering their URL.

Website Blocking by Keyword: You can block access to certain website by the keywords contained in their webpage



List of clients

Enter MAC Address of the clients in this format: xx:xx:xx:xx:xx:xx

MAC 01	00:AA:BB:CC:DD:EE
MAC 02	00:00:00:00:00:00
MAC 03	00:00:00:00:00:00
MAC 04	00:00:00:00:00:00
MAC 05	00:00:00:00:00:00
MAC 06	00:00:00:00:00:00
MAC 07	00:00:00:00:00:00
MAC 08	00:00:00:00:00:00

Enter the IP Address of the clients

IP 01	192.168.1. 15
IP 02	192.168.1. 0
IP 03	192.168.1. 0
IP 04	192.168.1. 0
IP 05	192.168.1. 0
IP 06	192.168.1. 0

Enter the IP Range of the clients

IP Range 01	192 . 168 . 1 . 19 ~ 192 168 1 30
IP Range 02	0 . 0 . 0 . 0 ~ 0 0 0 0

set up Internet access policy

1、Select the policy number (1-10) in the drop-down menu.

For this policy is enabled, click the radio button next to "Enable"

2、Enter a name in the Policy Name field.

3、Click the Edit List of PCs button.

4、 On the List of PCs screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the IP fields. If you have a range of IP addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC addresses into the MAC fields.

5、Click the Apply button to save your changes. Click the Cancel button to cancel your unsaved changes. Click the Close button to return to the Filters screen.

If you want to block the listed PCs from Internet access during the designated days and time, then keep the default setting, Deny. If you want the listed PCs to have Internet filtered during the designated days and time, then click the radio button next to Filter.

6、Set the days when access will be filtered. Select Everyday or the appropriate days of the week.

7、Set the time when access will be filtered. Select 24 Hours, or check the box next to From and use the drop-down boxes to designate a specific time period. Click the Add to Policy button to save your changes and active it.

8、To create or edit additional policies, repeat steps 1-9.

9、To delete an Internet Access Policy, select the policy number, and click the Delete button.

Note:

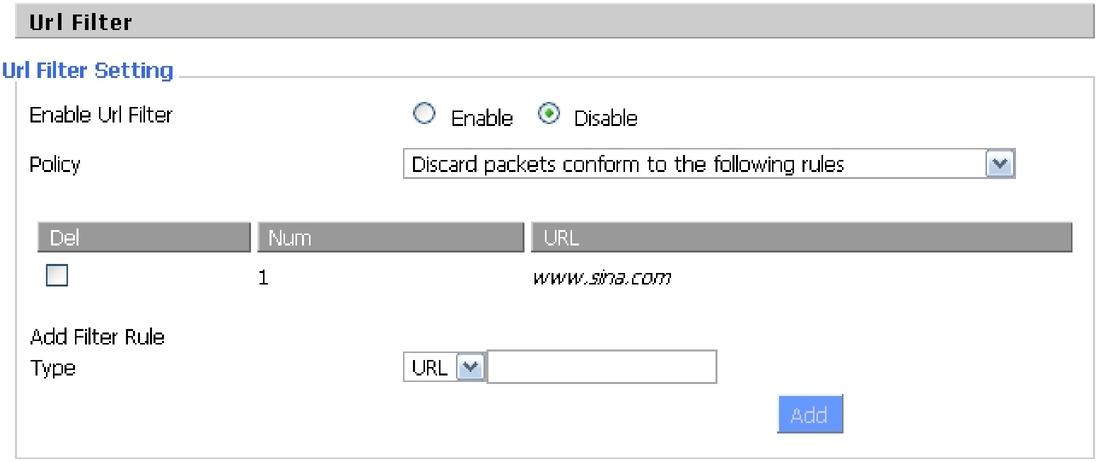
1、The default factory value of policy rules is "filtered". If the user chooses the default policy rules for "refuse", and editing strategies to save or directly to save the settings. If the strategy edited is the first, it will be automatically saved into the second, if not the first, keep the original number.

2、Turn off the power of the 5G CPE or reboot can cause a temporary failure。After that if can not automatically synchronized NTP time server, you need to recalibrate to ensure the correct implementation of the relevant period control function.

3.3.6.2 URL Filter

If you want to prevent certain client access to specific network domain name, such as www.sina.com. We can achieved it through the function of URL filter.

URL filtering function



Url Filter

Url Filter Setting

Enable Url Filter ○ Enable ● Disable

Policy: Discard packets conform to the following rules

Del	Num	URL
□	1	www.sina.com

Add Filter Rule

Type: URL

Discard packets conform to the following rules: only discard the matching URL address in the list .

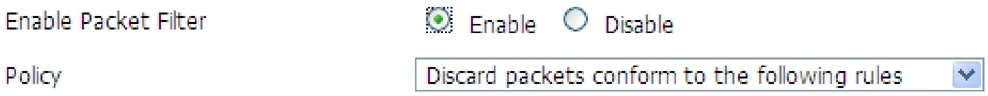
Accept only the data packets conform to the following rules: receive only with custom rules of network address, discarded all other URL address.

3.3.6.3 Packet Filter

To block some packets getting Internet access or block some Internet packets getting local network access, you can configure filter items to block these packets.

Packet Filter

Packet filter function is realized based on IP address or port of packets.



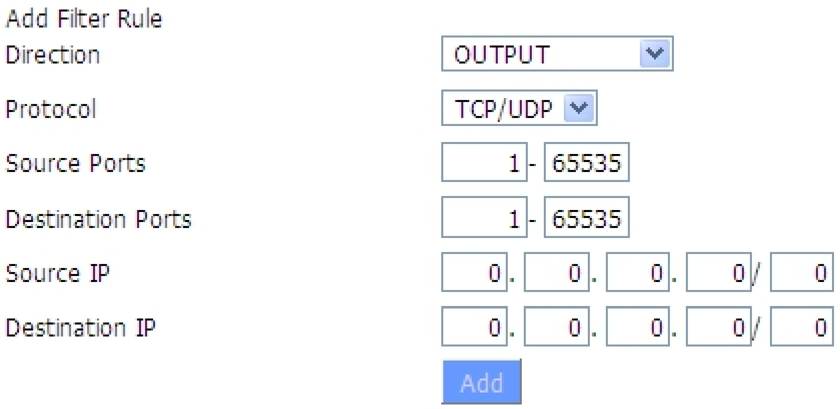
Enable Packet Filter	● Enable ○ Disable
Policy	Discard packets conform to the following rules

Enable Packet Filter: Enable or disable "packet filter" function

Policy: The filter rule's policy, you can choose the following options

Discard The Following--Discard packets conform to the following rules, Accept all other packets

Only Accept The Following-- Accept only the data packets conform to the following rules, Discard all other packets



Add Filter Rule

Direction	OUTPUT
Protocol	TCP/UDP
Source Ports	1 - 65535
Destination Ports	1 - 65535
Source IP	0 . 0 . 0 . 0 / 0
Destination IP	0 . 0 . 0 . 0 / 0

Direction

input: packet from WAN to LAN

output: packet from LAN to WAN

Protocol: packet protocol type

Source Ports: packet's source port

Destination Ports: packet's destination port

Source IP: packet's source IP address

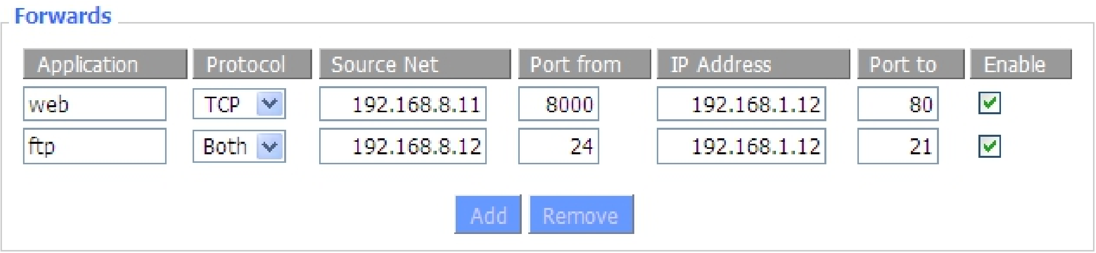
Destination IP: packet's destination IP address

Note: "Source Port" ,"Destination Port" ,"Source IP" ,"Destination IP" could not be all empty ,you have to input at least one of these four parameters.

3.3.7 NAT

3.3.7.1 Port Forwarding

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, 5G CPE will forward those requests to the appropriate PC. If you want to forward a whole range of ports, see Port Range Forwarding.



Forwards

Application	Protocol	Source Net	Port from	IP Address	Port to	Enable
web	TCP	192.168.8.11	8000	192.168.1.12	80	☑
ftp	Both	192.168.8.12	24	192.168.1.12	21	☑

Application: Enter the name of the application in the field provided.

Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.

Source Net: Forward only if sender matches this ip/net (example 192.168.1.0/24).

Port from: Enter the number of the external port (the port number seen by users on the Internet).

IP Address: Enter the IP Address of the PC running the application.

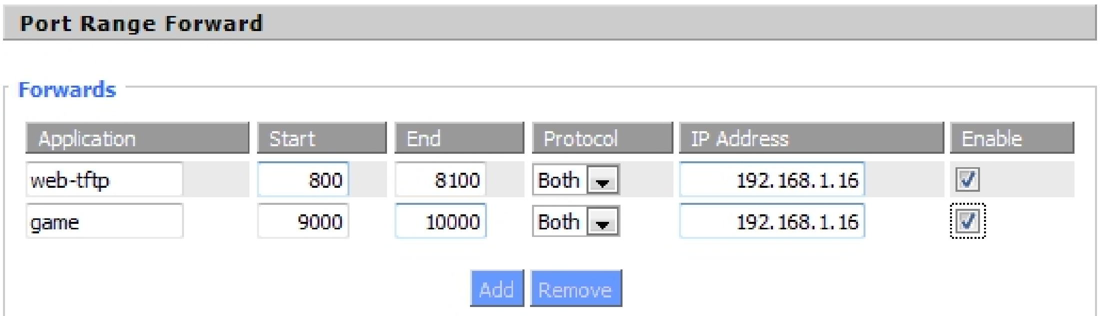
Port to: Enter the number of the internal port (the port number used by the application).

Enable: Click the Enable checkbox to enable port forwarding for the application.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.7.1 Port Range Forwarding

Port Range Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, 5G CPE will forward those requests to the appropriate PC. If you only want to forward a single port, see Port Forwarding.



Port Range Forward

Forwards

Application	Start	End	Protocol	IP Address	Enable
web-tftp	800	8100	Both	192.168.1.16	☑
game	9000	10000	Both	192.168.1.16	☑

Application: Enter the name of the application in the field provided.

Start: Enter the number of the first port of the range you want to seen by users on the Internet and forwarded to your PC.

End: Enter the number of the last port of the range you want to seen by users on the Internet and forwarded to your PC.

Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.

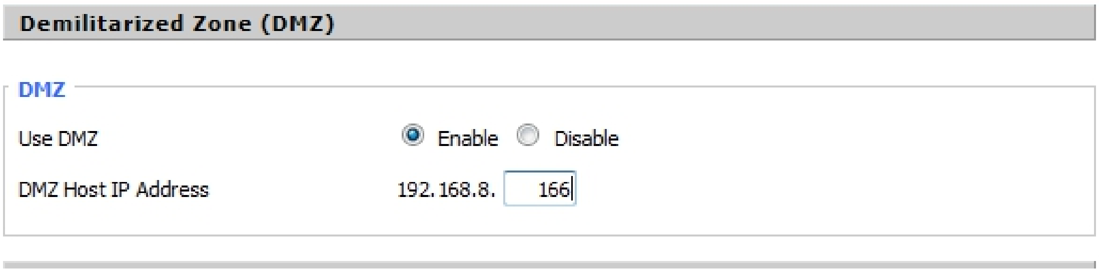
IP Address: Enter the IP Address of the PC running the application.

Enable: Click the Enable checkbox to enable port forwarding for the application.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.7.2 DMZ

The DMZ (DeMilitarized Zone) hosting feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.



Demilitarized Zone (DMZ)

DMZ

Use DMZ ● Enable ○ Disable

DMZ Host IP Address 192.168.8. 166

Any PC whose port is being forwarded must should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ Host IP Address: To expose one PC to the Internet, select Enable and enter the computer's IP address in the DMZ Host IP Address field. To disable the DMZ, keep the default setting：Disable

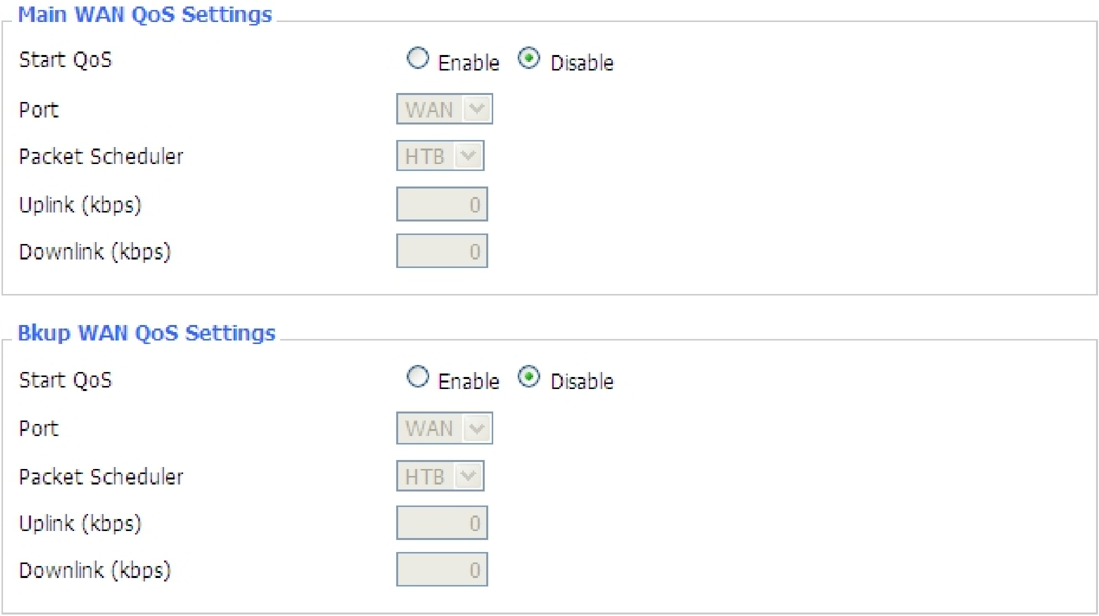
Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.8 QoS

3.3.8.1 Basic

Bandwidth management prioritizes the traffic on your 5G CPE. Interactive traffic (telephony, browsing, telnet, etc.) gets priority and bulk traffic (file transfer, P2P) gets low priority. The main goal is to allow both types to live side-by side without unimportant traffic disturbing more critical things. All of this is more or less automatic.

QoS allows control of the bandwidth allocation to different services, netmasks, MAC addresses and the four LAN ports.



Main WAN QoS Settings

Start QoS	○ Enable ● Disable
Port	WAN
Packet Scheduler	HTB
Uplink (kbps)	0
Downlink (kbps)	0

Bkup WAN QoS Settings

Start QoS	○ Enable ● Disable
Port	WAN
Packet Scheduler	HTB
Uplink (kbps)	0
Downlink (kbps)	0

Uplink (kbps)：In order to use bandwidth management (QoS) you must enter bandwidth values for your uplink. These are generally 80% to 90% of your maximum bandwidth.

Downlink (kbps)：In order to use bandwidth management (QoS) you must enter bandwidth values for your downlink. These are generally 80% to 90% of your maximum bandwidth.

3.3.8.2 Classify

Net mask Priority

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

Priority description: The system provides five priority levels, among which the "Exempt" priority level is independent of the other four priority levels

The other four priorities are：Premium、Express、Standard、Bulk

Exempt: For data streams at the Exempt level, the bandwidth is only limited by the hardware

The relationship between Exempt bandwidth and the other four priorities is as follows:

Suppose the total upload bandwidth is Max_Up, the total download bandwidth is Max_Down, the upload limit in "QOS Settings" is Uplink, the download limit is Downlink, and the flow 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 priority levels 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 the download is 1000kbps,At this time, there are four data streams, and their priorities are Premium, Express, standard, and Bulk. Then the upload and download bandwidths of each data stream are as follows：

Premium:（75/100） * Uplink ； （75/100） * Downlink

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

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

Bulk:1000bit；1000bit；

For Bulk, the upload and download rates are both 1000bit, and it’s its turn when other priority data streams are sent.；

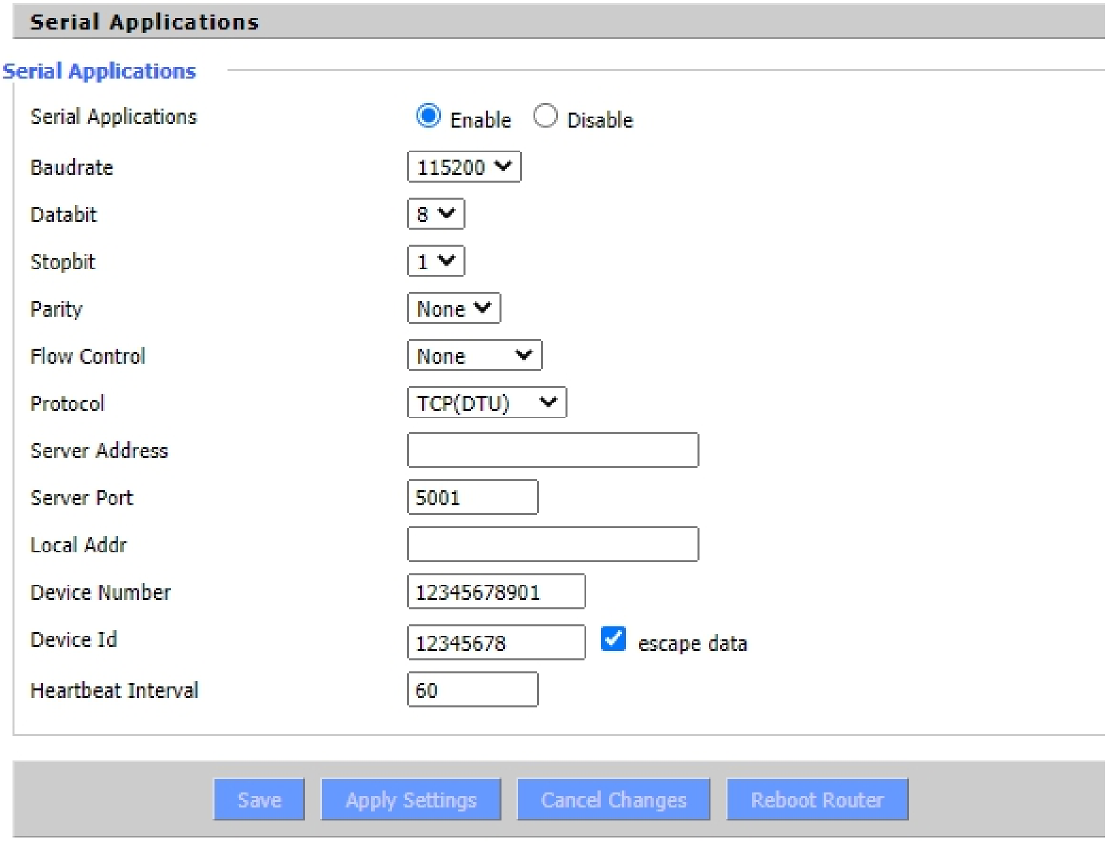
Note: When a connection meets the control conditions in MAC priority and net mask priority at the same time, the rule added first shall prevail.

3.3.9 Application

3.3.9.1 Serial Application

Under normal circumstances, the Console port of the 5G industrial CPE is used as a console. The Console port can also be configured as a common serial port. The 5G industrial CPE has a built-in serial port to TCP/IP program.

Through configuration, the Console port of the 5G industrial CPE is used as a serial port protocol conversion device, or it is completely equivalent to a Four-Faith DTU device.



Serial Applications

Serial Applications

Serial Applications	● Enable ○ Disable
Baudrate	115200
Databit	8
Stopbit	1
Parity	None
Flow Control	None
Protocol	TCP(DTU)
Server Address	
Server Port	5001
Local Addr	
Device Number	12345678901
Device Id	12345678 ☑ escape data
Heartbeat Interval	60

Baud rate: Indicates the number of bytes transmitted by the device per second. Commonly used baud rates are 115200, 57600, 38400, 19200, etc.

Data Bit: The number of data bits can be 4, 5, 6, 7, 8, etc. to form a character.

ASCII code is usually used. The transmission starts from the lowest bit and is positioned by the clock.

Stop bit: It is the end sign of a character data.Can be 1-bit, 1.5-bit, 2-bit high level

Parity: Indicates the data error checking method adopted by a group of data, and there are two ways of parity checking.

Flow Control: Including the hardware part and the software part in two ways.

Protocol Type

UDP(DTU) : Serial port to UDP connection, including custom application layer protocol, completely equivalent to the function of a four-faith IP MODEM.

PURE UDP: Standard serial port to UDP connection.

TCP(DTU) : Serial port to TCP connection, including custom application layer protocol, completely equivalent to the function of a Four-Faith IP MODEM.

PURE TCP : Standard serial port to TCP connection.

TCP SERVER: Standard TCP server connection

TCST: Custom TCP connection

Server address: The IP address or domain name of the data service center that communicates with the 5G industrial CPE serial port to TCP program.

Server Port: The port that the data service center program listens to.

Device Number: The ID number of the device, an 11-byte data string. This configuration item is valid only when the protocol type is set to "UDP(DTU)" or "TCP(DTU)".

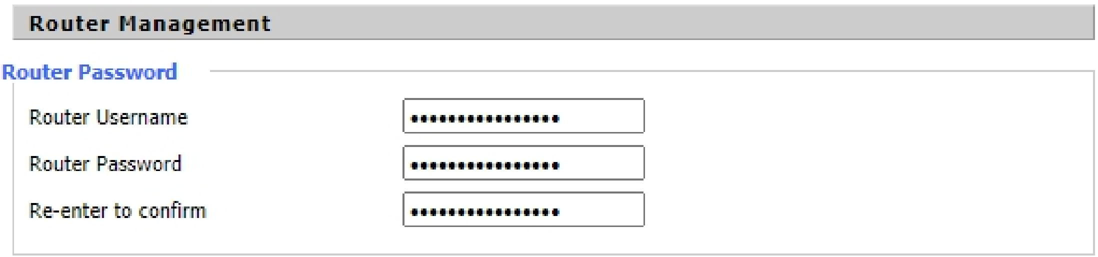
设备 ID： 8-byte data string, this configuration item is valid only when the protocol type is set to "UDP(DTU)" or "TCP(DTU)".

Heartbeat Interval：The time interval of the heartbeat packet, this configuration item is valid only when the protocol type is set to "UDP(DTU)" or "TCP(DTU)".

3.3.10 Administration

3.3.10.1 Administration

This page can allow network administrators to manage specific 5G industrial CPE functions to ensure access and security.



Router Management

Router Password

Router Username	••••••••••••••••
Router Password	••••••••••••••••
Re-enter to confirm	••••••••••••••••

The new password must not exceed 32 characters in length 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.

warning：

The default user name is: admin.

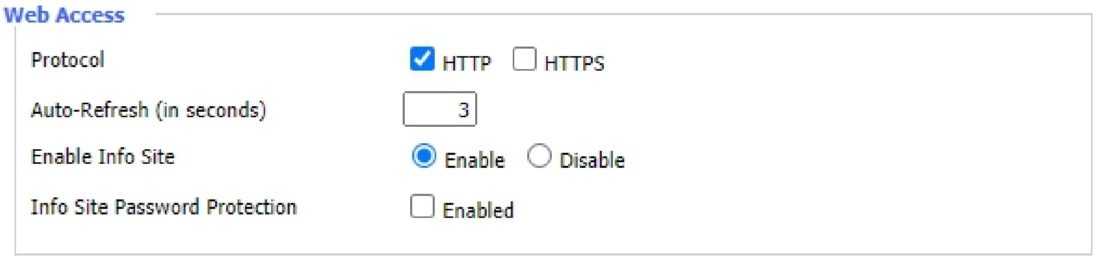
We strongly recommend that you modify the factory default password admin, so that all users trying to access and modify the 5G industrial CPE should be based on entering the correct 5G industrial CPE password before they can access and use it.

Web access

This feature allows you to use HTTP protocol or HTTPS protocol to manage 5G industrial CPE.

If you choose to disable this feature, you will need to restart it manually.

You can also activate or deactivate the 5G industrial CPE information web page, so that you can password protect this page (enter the correct user name and password).



Web Access

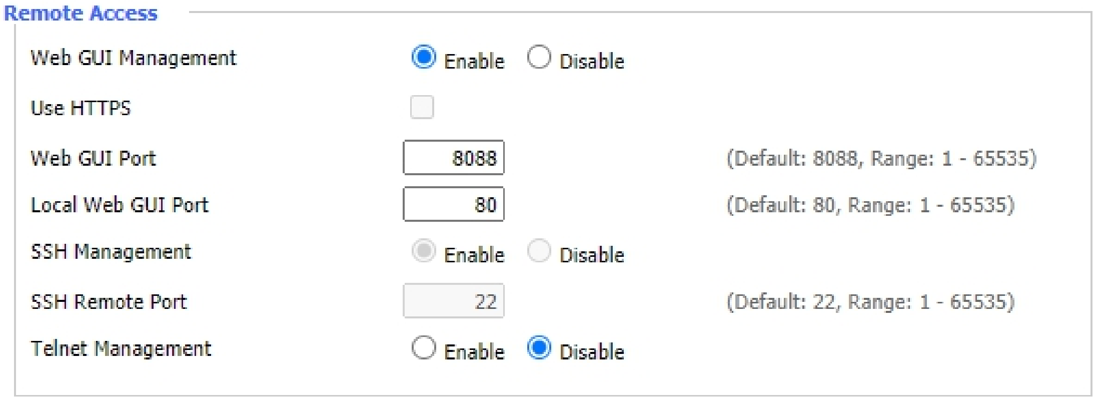
Protocol	☑ HTTP ☐ HTTPS
Auto-Refresh (in seconds)	3
Enable Info Site	● Enable ○ Disable
Info Site Password Protection	☐ Enabled

Protocol： Protocols supported by web pages include HTTP and HTTPS

Auto Refresh(in seconds)： Adjust the automatic refresh interval of the Web interface.0 means turn off this feature.

Enable Info Site： Whether to enable the display of system information page before login

Info site password protection： Enable password protection for system information web pages



Remote Access

Web GUI Management ● Enable ○ Disable

Use HTTPS □

Web GUI Port 8088 (Default: 8088, Range: 1 - 65535)

Local Web GUI Port 80 (Default: 80, Range: 1 - 65535)

SSH Management ● Enable ○ Disable

SSH Remote Port 22 (Default: 22, Range: 1 - 65535)

Telnet Management ○ Enable ● Disable

Web GUI Management： This feature allows you to manage 5G industrial CPE from a remote location via the Internet. To disable this feature, keep the default setting, which is disabled. To enable this function, please select Enable and use the designated port on the computer (8080 by default) to remotely manage 5G industrial CPE. If you have not set a password, you must also set the default password for your own 5G industrial CPE

To remotely manage 5G industrial CPE, enter http://xxx.xxx.xxx.xxx:8080 (x represents the Internet IP address of the 5G industrial CPE, 8080 represents the designated port), in the address bar of your web browser. You will be asked to enter the 5G industrial CPE password.

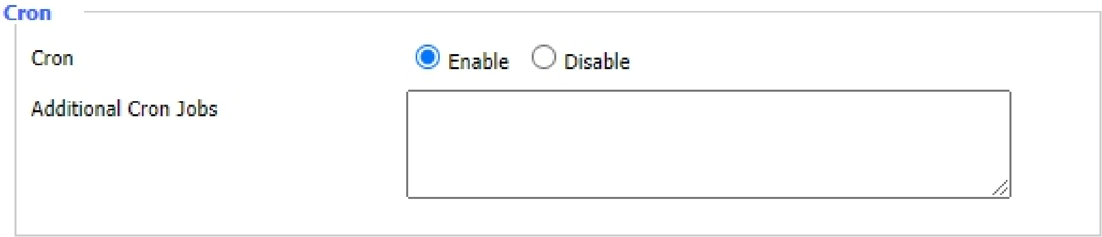
If you use HTTPS, you need to specify the URL as https://xxx.xxx.xxx.xxx:8080 (not all firmware supports SSL reconstruction)

SSH Management： You can enable SSH to remotely and securely access 5G industrial CPE. Please note that if you want to know the settings of the SSH daemon, you can visit more on the service page.

Warning:

If the access function of the remote 5G industrial CPE is enabled, anyone who knows the Internet IP address and password of the 5G industrial CPE can change the settings of the 5G industrial CPE.

Telnet Management： Enable or disable remote Telnet function

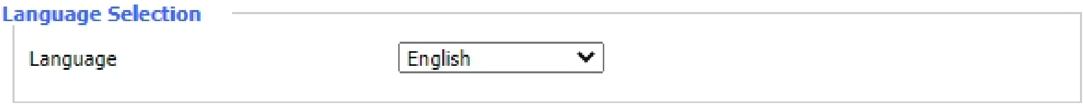


Cron

Cron ● Enable ○ Disable

Additional Cron Jobs

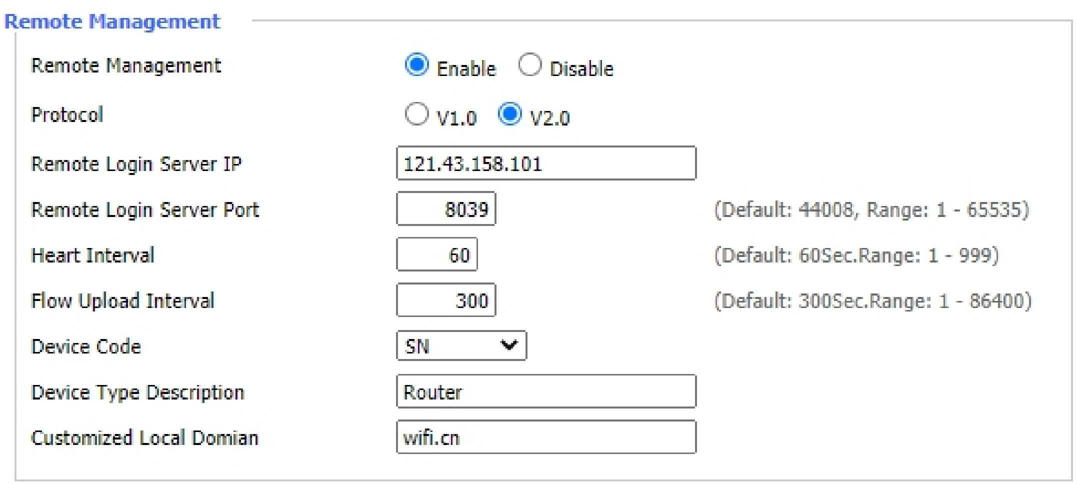
Cron： The subsystem of cron is the Linux command you plan to execute. You need to use the command line or startup script in actual use.



Language Selection

Language English

Language： Set the language type displayed on the 5G industrial CPE page, including simplified Chinese and English.



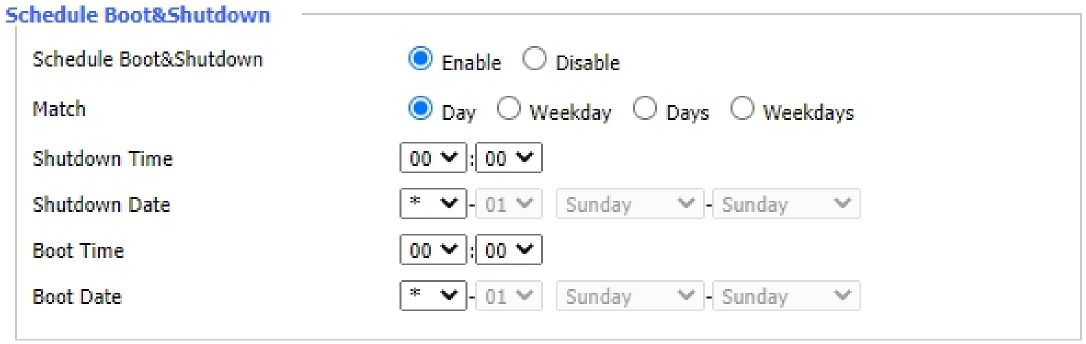
Remote Management

Remote Management	● Enable ○ Disable	
Protocol	○ V1.0 ● V2.0	
Remote Login Server IP	121.43.158.101	
Remote Login Server Port	8039	(Default: 44008, Range: 1 - 65535)
Heart Interval	60	(Default: 60Sec.Range: 1 - 999)
Flow Upload Interval	300	(Default: 300Sec.Range: 1 - 86400)
Device Code	SN	
Device Type Description	Router	
Customized Local Domian	wifi.cn	

Remote management: Monitor and manage the 5G industrial CPE, configure parameters, and update firmware through a custom-developed remote management server.

3.3.10.2 Keep alive

Schedule Boot&Shutdown

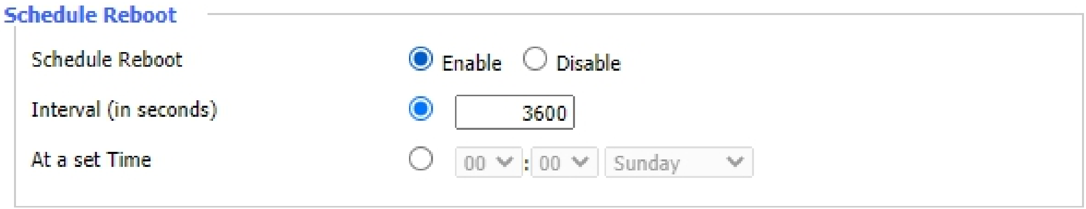


Schedule Boot&Shutdown

Schedule Boot&Shutdown	● Enable ○ Disable
Match	● Day ○ Weekday ○ Days ○ Weekdays
Shutdown Time	00 : 00
Shutdown Date	* - 01 Sunday - Sunday
Boot Time	00 : 00
Boot Date	* - 01 Sunday - Sunday

The user can set the time to turn on or off

Schedule reboot



Schedule Reboot

Schedule Reboot	● Enable ○ Disable
Interval (in seconds)	● 3600
At a set Time	○ 00 : 00 Sunday

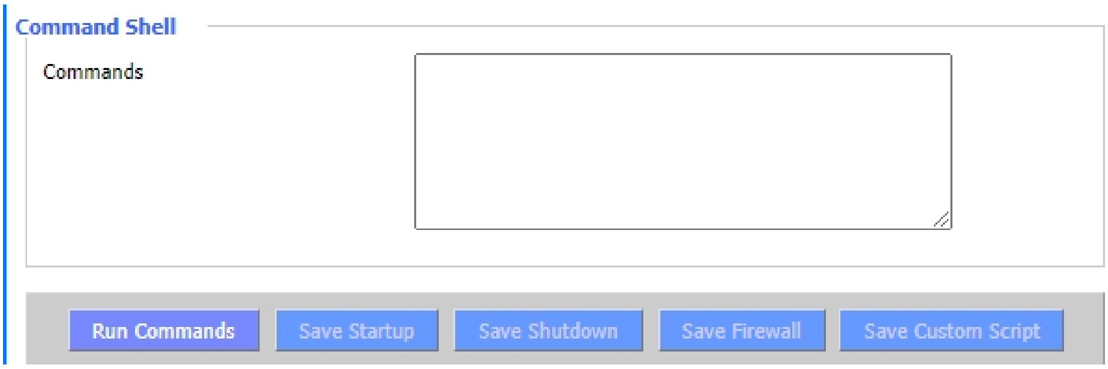
You can set timed restart routing

warning:

Choose when to restart the 5G industrial CPE. In the management tab, the Cron option must be enabled.

3.3.10.3 Command

Command Shell： 您可以通过 Web 界面运行命令行。将您的命令填入文本区域并且点击运行命令按钮提交



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

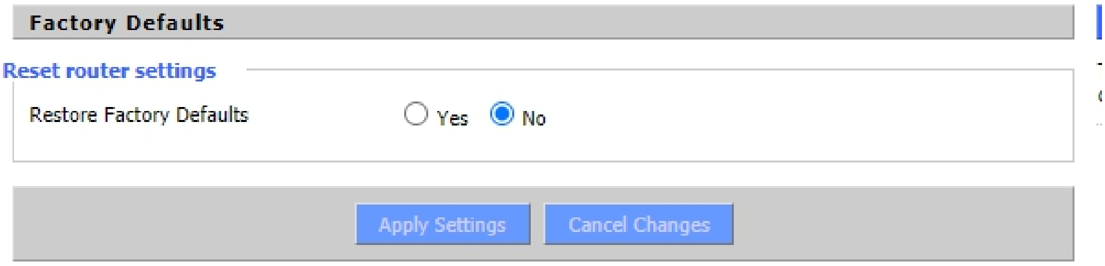
Save startup：You can save some command lines that are executed when starting the 5G industrial CPE. Enter the command (only one command line) into the text area, and then click Save as a startup command.

Save shutdown：You can save some command lines that are executed when the 5G industrial CPE is closed. Enter the command (only one command line) into the text area, and then click Save as shutdown command.

Save firewall： Every time the firewall is started, 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 instructions are stored in the /tmp/custom.sh file. You can receive it to run or use cron to call it. Enter the script command (only one command line) into the text area, and click Save as a custom command.

3.3.10.4 Factory Defaults



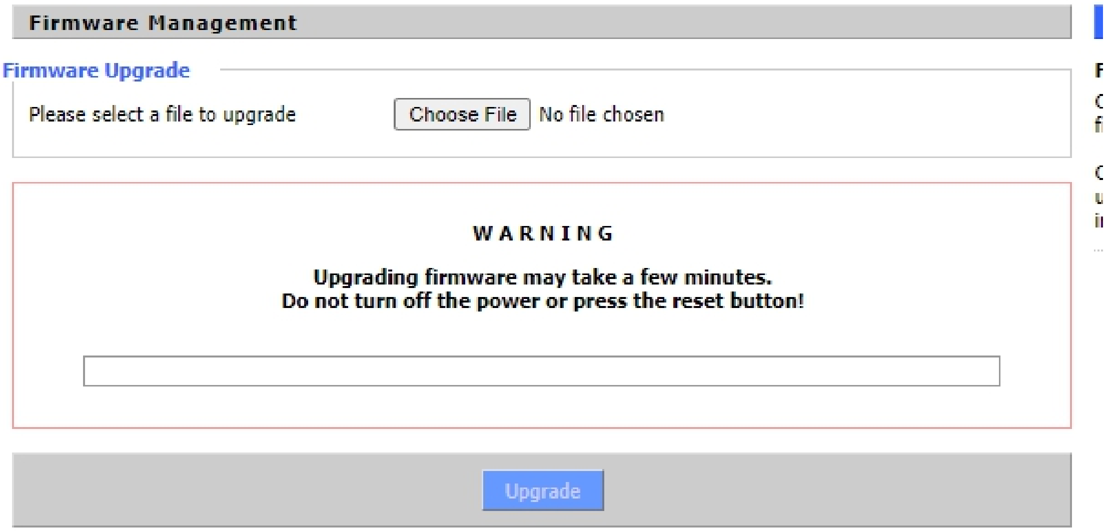
Factory Defaults

Reset router settings

Restore Factory Defaults ○ Yes ● No

Restore factory defaults Click the "Yes" button and save the settings, reset all configurations to factory defaults. When you restore to the default settings, all the settings you made will be lost. The default configuration of this feature is "No".

3.3.10.5 Firmware Upgrade



Firmware Management

Firmware Upgrade

Please select a file to upgrade No file chosen

WARNING

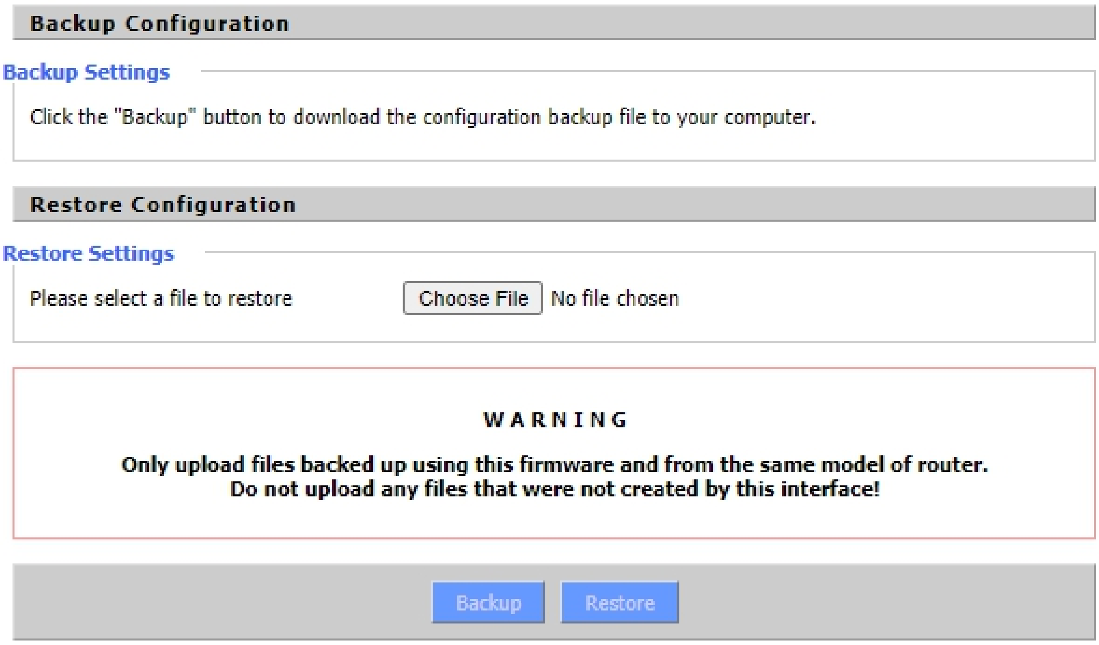
Upgrading firmware may take a few minutes.
Do not turn off the power or press the reset button!

firmware upgrade： The new firmware can be loaded onto the 5G industrial CPE.

note： When upgrading the firmware of the 5G industrial CPE, its configuration settings may be lost. Therefore, please make sure to back up the configuration information of the 5G industrial CPE before upgrading the firmware.

3.3.10.6 Backup

This page is used to backup or restore the configuration files of 5G industrial CPE.



Backup Configuration

Backup Settings

Click the "Backup" button to download the configuration backup file to your computer.

Restore Configuration

Restore Settings

Please select a file to restore No file chosen

WARNING

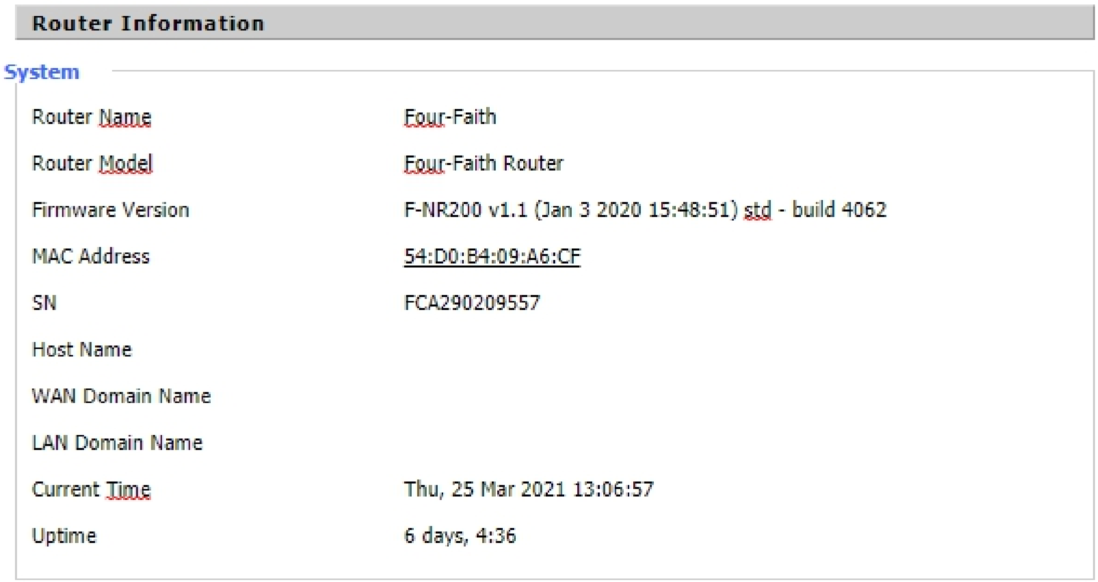
Only upload files backed up using this firmware and from the same model of router.
Do not upload any files that were not created by this interface!

If you want to back up the configuration file of the 5G industrial CPE, please click the "Backup" button. After that, follow the instructions on the screen.

If you want to restore the configuration file of the 5G industrial CPE, click the "Browse" button. After you find the backup file, follow the instructions on the screen. Select the backup file and click the "Restore" button.

3.3.11 Status

3.3.11.1 5G Industrial CPE



Router Information

System

Router Name	Four-Faith
Router Model	Four-Faith Router
Firmware Version	F-NR200 v1.1 (Jan 3 2020 15:48:51) std - build 4062
MAC Address	54:D0:B4:09:A6:CF
SN	FCA290209557
Host Name	
WAN Domain Name	
LAN Domain Name	
Current Time	Thu, 25 Mar 2021 13:06:57
Uptime	6 days, 4:36

Router name ： The name of this 5G industrial CPE can be modified in the basic settings

Router model: The model of this 5G industrial CPE is fixedly produced 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: Reflects the MAC address of the WAN, which can be modified in the setting of MAC address cloning

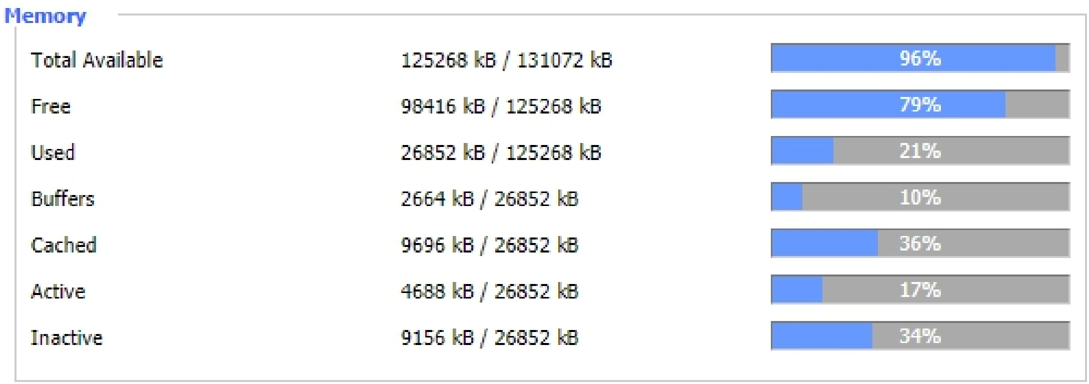
Host name: The host name of the 5G industrial CPE can be modified in the basic settings

WAN: The domain name of the WAN port can be modified in the basic settings

LAN: The domain name of the LAN port is fixedly generated by the system and cannot be modified

Current time: system local time

Up time: Time when the system is powered on



Memory

Total Available	125268 kB / 131072 kB	96%
Free	98416 kB / 125268 kB	79%
Used	26852 kB / 125268 kB	21%
Buffers	2664 kB / 26852 kB	10%
Cached	9696 kB / 26852 kB	36%
Active	4688 kB / 26852 kB	17%
Inactive	9156 kB / 26852 kB	34%

Total available: All available RAM size (that is, physical memory minus some reserved bits and the binary code size of the kernel)

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

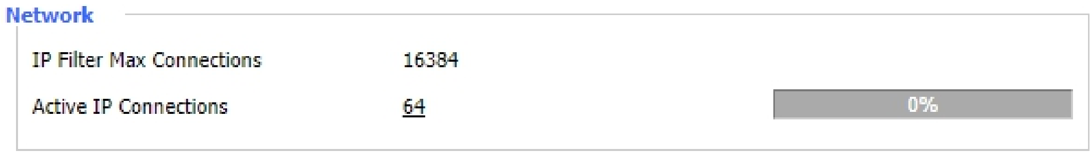
Used : Used memory, all available memory minus free memory

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

Cached : The size of the memory used by the cache memory

Active : The size of the buffer or cache page file in active use

Inactive : Infrequently used buffer or cache page file size

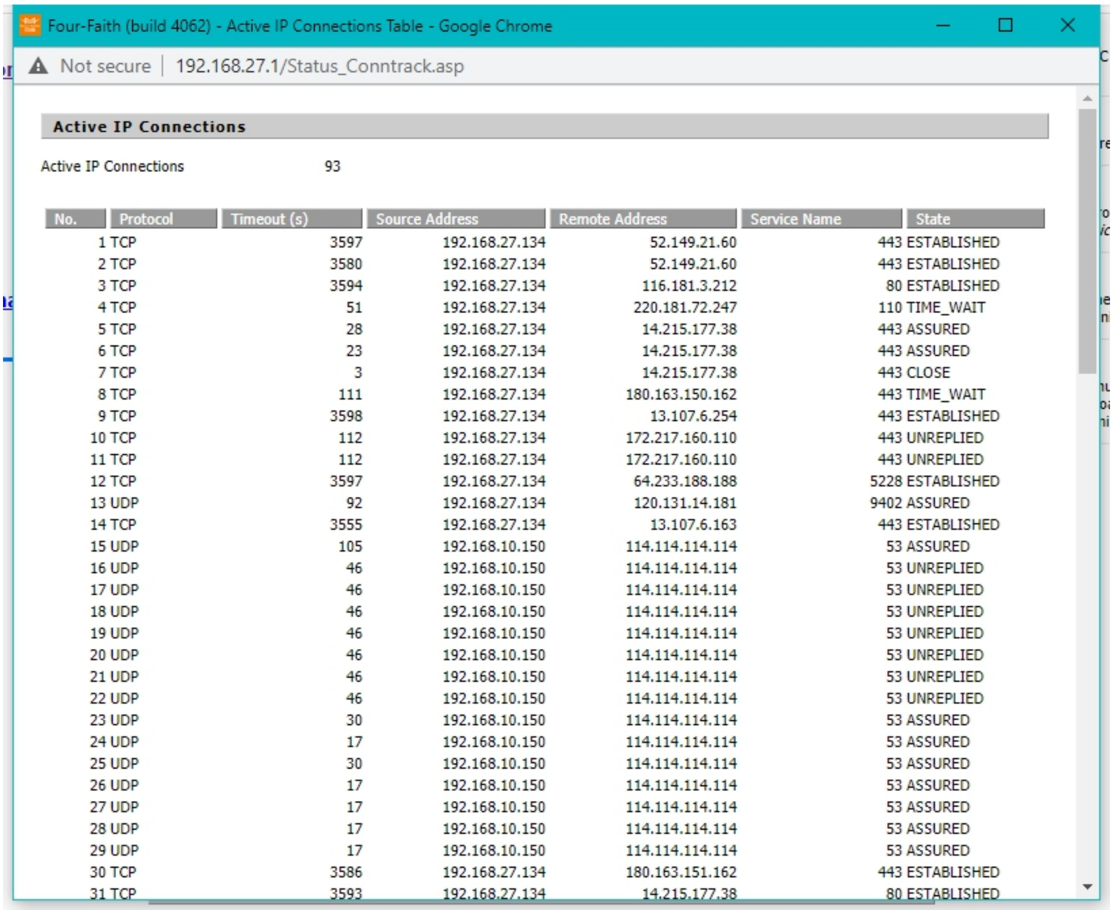


Network

IP Filter Max Connections	16384	
Active IP Connections	64	0%

IP filter maximum connections: default 4096, manageable

Active IP connections: Real-time detection of the number of IP connections that the system is active, if you click it, you can see the following



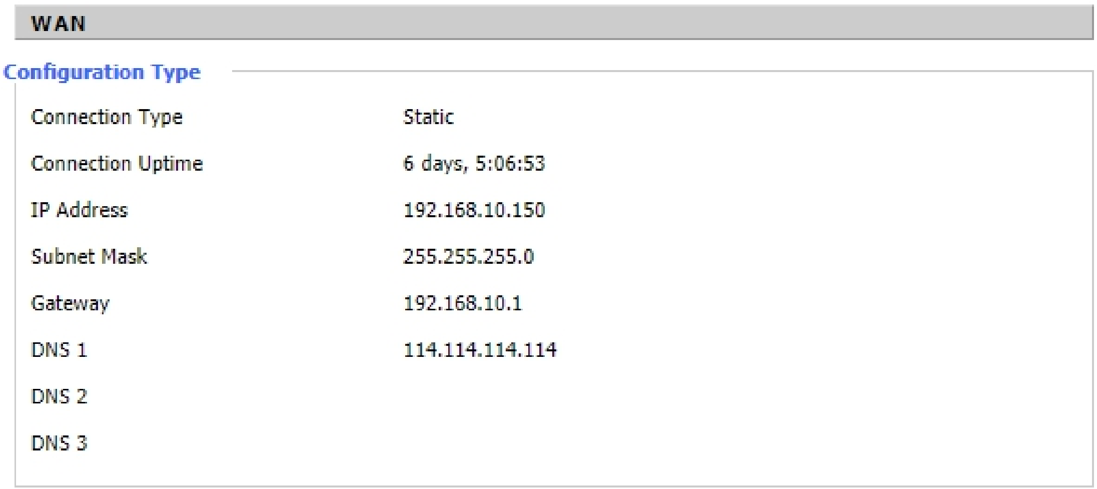
Four-Faith (build 4062) - Active IP Connections Table - Google Chrome
Not secure | 192.168.27.1/Status_Conntrack.asp

Active IP Connections

Active IP Connections 93

No.	Protocol	Timeout (s)	Source Address	Remote Address	Service Name	State
1	TCP	3597	192.168.27.134	52.149.21.60	443	ESTABLISHED
2	TCP	3580	192.168.27.134	52.149.21.60	443	ESTABLISHED
3	TCP	3594	192.168.27.134	116.181.3.212	80	ESTABLISHED
4	TCP	51	192.168.27.134	220.181.72.247	110	TIME_WAIT
5	TCP	28	192.168.27.134	14.215.177.38	443	ASSURED
6	TCP	23	192.168.27.134	14.215.177.38	443	ASSURED
7	TCP	3	192.168.27.134	14.215.177.38	443	CLOSE
8	TCP	111	192.168.27.134	180.163.150.162	443	TIME_WAIT
9	TCP	3598	192.168.27.134	13.107.6.254	443	ESTABLISHED
10	TCP	112	192.168.27.134	172.217.160.110	443	UNREPLIED
11	TCP	112	192.168.27.134	172.217.160.110	443	UNREPLIED
12	TCP	3597	192.168.27.134	64.233.188.188	5228	ESTABLISHED
13	UDP	92	192.168.27.134	120.131.14.181	9402	ASSURED
14	TCP	3555	192.168.27.134	13.107.6.163	443	ESTABLISHED
15	UDP	105	192.168.10.150	114.114.114.114	53	ASSURED
16	UDP	46	192.168.10.150	114.114.114.114	53	UNREPLIED
17	UDP	46	192.168.10.150	114.114.114.114	53	UNREPLIED
18	UDP	46	192.168.10.150	114.114.114.114	53	UNREPLIED
19	UDP	46	192.168.10.150	114.114.114.114	53	UNREPLIED
20	UDP	46	192.168.10.150	114.114.114.114	53	UNREPLIED
21	UDP	46	192.168.10.150	114.114.114.114	53	UNREPLIED
22	UDP	46	192.168.10.150	114.114.114.114	53	UNREPLIED
23	UDP	30	192.168.10.150	114.114.114.114	53	ASSURED
24	UDP	17	192.168.10.150	114.114.114.114	53	ASSURED
25	UDP	30	192.168.10.150	114.114.114.114	53	ASSURED
26	UDP	17	192.168.10.150	114.114.114.114	53	ASSURED
27	UDP	17	192.168.10.150	114.114.114.114	53	ASSURED
28	UDP	17	192.168.10.150	114.114.114.114	53	ASSURED
29	UDP	17	192.168.10.150	114.114.114.114	53	ASSURED
30	TCP	3586	192.168.27.134	180.163.151.162	443	ESTABLISHED
31	TCP	3593	192.168.27.134	14.215.177.38	80	ESTABLISHED

3.3.11.2 WAN



WAN

Configuration Type

Connection Type	Static
Connection Uptime	6 days, 5:06:53
IP Address	192.168.10.150
Subnet Mask	255.255.255.0
Gateway	192.168.10.1
DNS 1	114.114.114.114
DNS 2	
DNS 3	

Connection type: including 7 ways: disable, static IP, auto configuration-DHCP, PPPOE, PPTP, L2TP, 3G/UMTS.

Connected time: the time that has been connected, if not connected, it will ask "unavailable"

IP address: the IP address obtained from the 5G industrial CPEWAN port

Subnet mask: the subnet mask obtained from the 5G industrial CPEWAN port

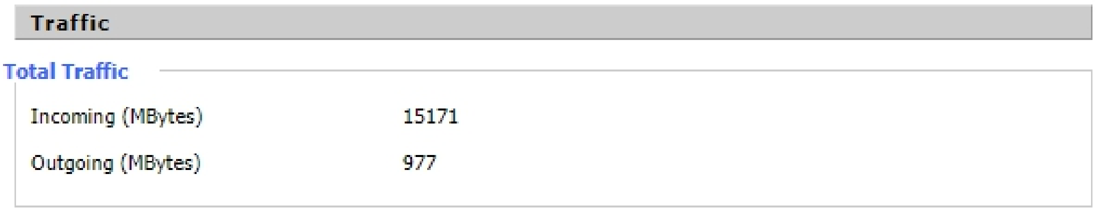
Gateway: The gateway obtained from the 5G industrial CPEWAN port

DNS1, DNS2, DNS3: the first DNS, the second DNS, and the third DNS obtained from the 5G industrial CPEWAN port

Lease remaining time: the remaining time occupied by obtaining the IP address in DHCP mode

DHCP release: release the DHCP address

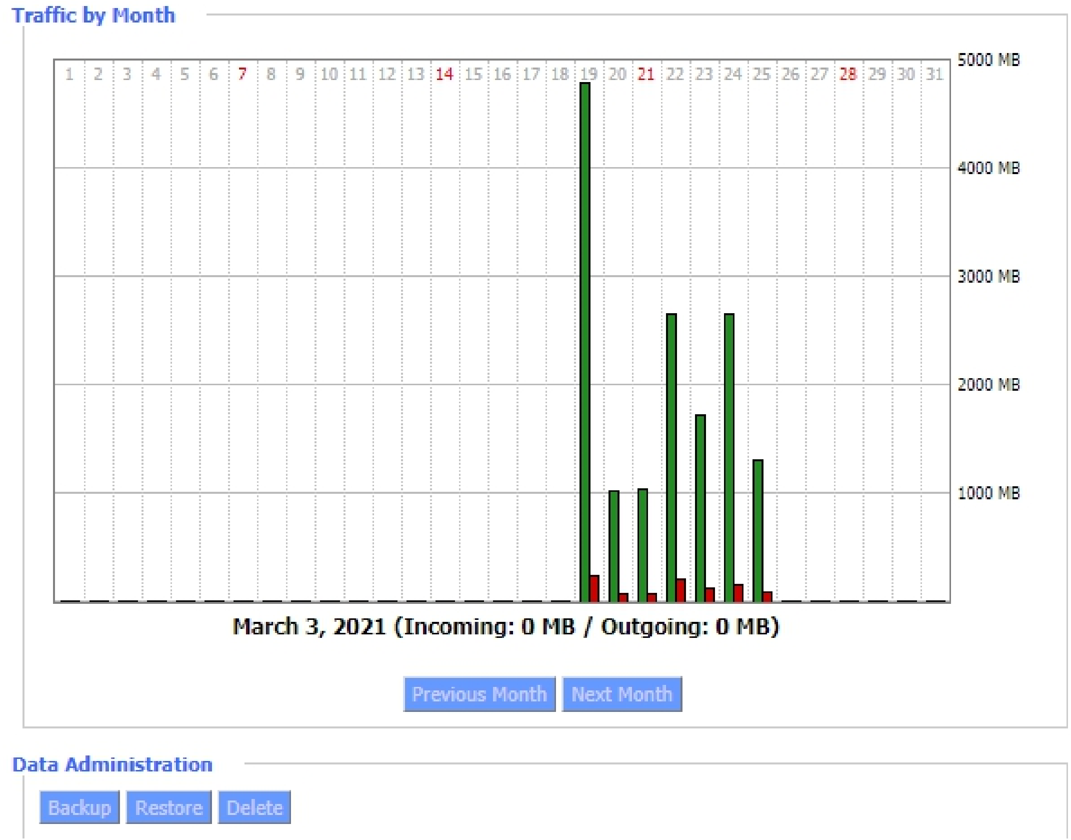
DHCP renewal: renew the IP address obtained through DHCP, the default renewal is 1 day



Traffic

Total Traffic

Incoming (MBytes)	15171
Outgoing (MBytes)	977



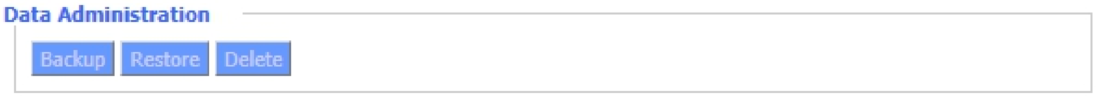
March 3, 2021 (Incoming: 0 MB / Outgoing: 0 MB)

Total traffic: Statistics of the traffic used since the last power outage is divided into two directions: download and upload

Monthly traffic: MB of traffic unit counted in one month

Last month: Check the traffic of the last month

Next month: Check the traffic of the next month

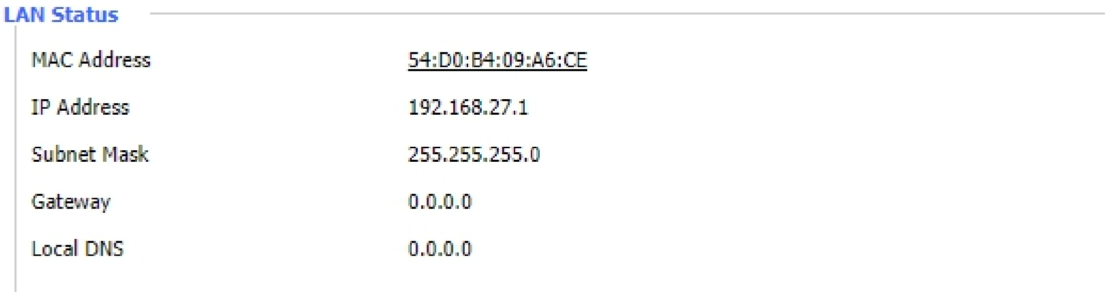


Backup: backup data traffic statistics

Restore: restore data traffic statistics

Delete: delete data traffic statistics

3.3.11.3 LAN



MAC Address	54:D0:B4:09:A6:CE
IP Address	192.168.27.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

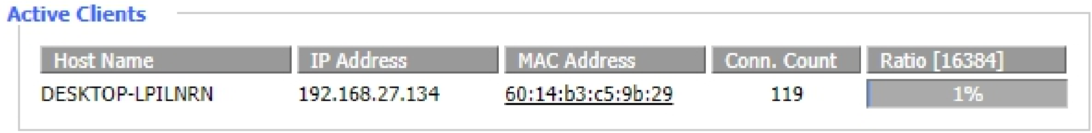
MAC address: the MAC address of the LAN port

IP address: the 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



Active Clients

Host Name	IP Address	MAC Address	Conn. Count	Ratio [16384]
DESKTOP-LPILNRN	192.168.27.134	60:14:b3:c5:9b:29	119	1%

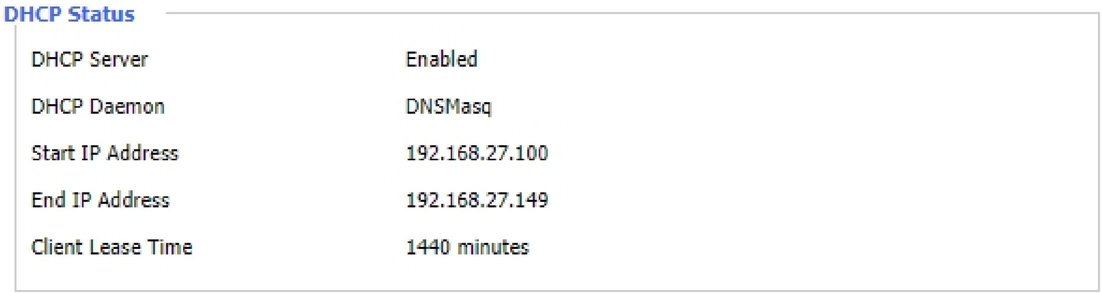
Host name: the host name of the LAN port client

IP address: the IP address of the client

MAC address: the MAC address of the client

Number of connections: the number of connections generated by the client

Proportion: Percentage of 4096 connections



DHCP Status

DHCP Server	Enabled
DHCP Daemon	DNSMasq
Start IP Address	192.168.27.100
End IP Address	192.168.27.149
Client Lease Time	1440 minutes

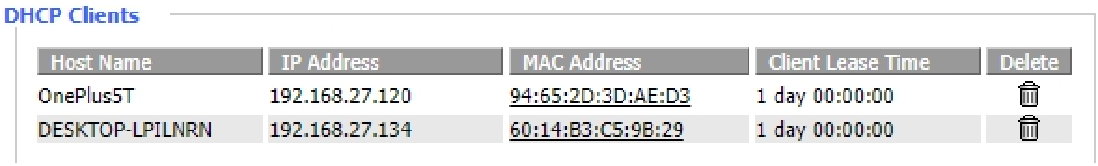
DNCP server: Whether to enable the DHCP server

DHCP daemon: The protocol distribution used by DHCP mainly includes DNSMasq and DHCPd

Start IP address: the start IP address of the DHCP client

End IP address: the end IP address of the DHCP client

Client lease time: DHCP client lease time



DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time	Delete
OnePlus5T	192.168.27.120	94:65:2D:3D:AE:D3	1 day 00:00:00	🗑
DESKTOP-LPILNRN	192.168.27.134	60:14:B3:C5:9B:29	1 day 00:00:00	🗑

Host name: the host name of the LAN port client

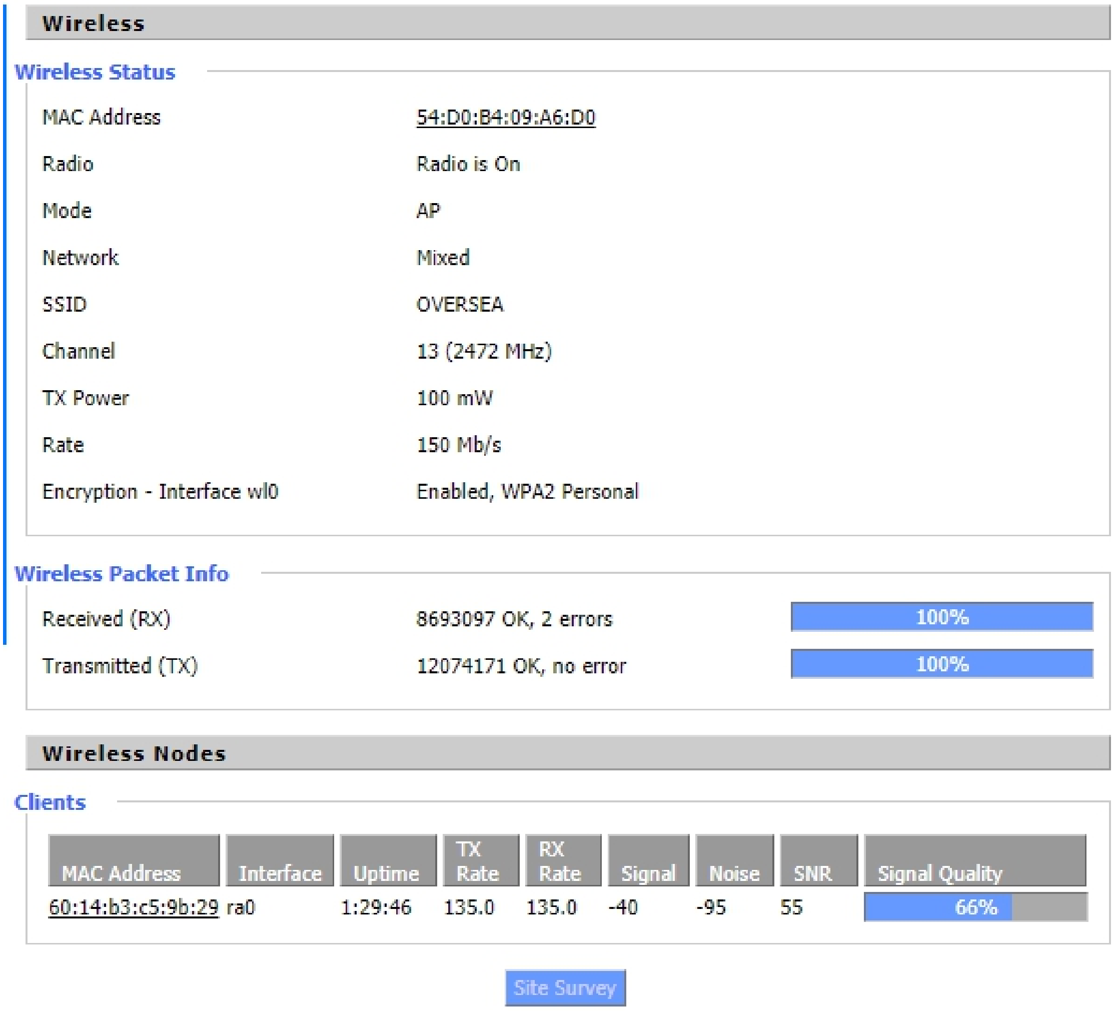
IP address: the IP address of the client

MAC address: the MAC address of the client

Client lease time: the time the client leased this IP address

Delete: Click to delete the DHCP client

3.3.11.4 Wireless



Wireless

Wireless Status

MAC Address	54:D0:B4:09:A6:D0
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	OVERSEA
Channel	13 (2472 MHz)
TX Power	100 mW
Rate	150 Mb/s
Encryption - Interface wl0	Enabled, WPA2 Personal

Wireless Packet Info

Received (RX)	8693097 OK, 2 errors	100%
Transmitted (TX)	12074171 OK, no error	100%

Wireless Nodes

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
60:14:b3:c5:9b:29	ra0	1:29:46	135.0	135.0	-40	-95	55	66%

MAC address: wireless MAC address

Wireless network: Shows whether the wireless network is turned on

Mode: wireless mode

Network: wireless network mode

SSID: The name of the wireless network

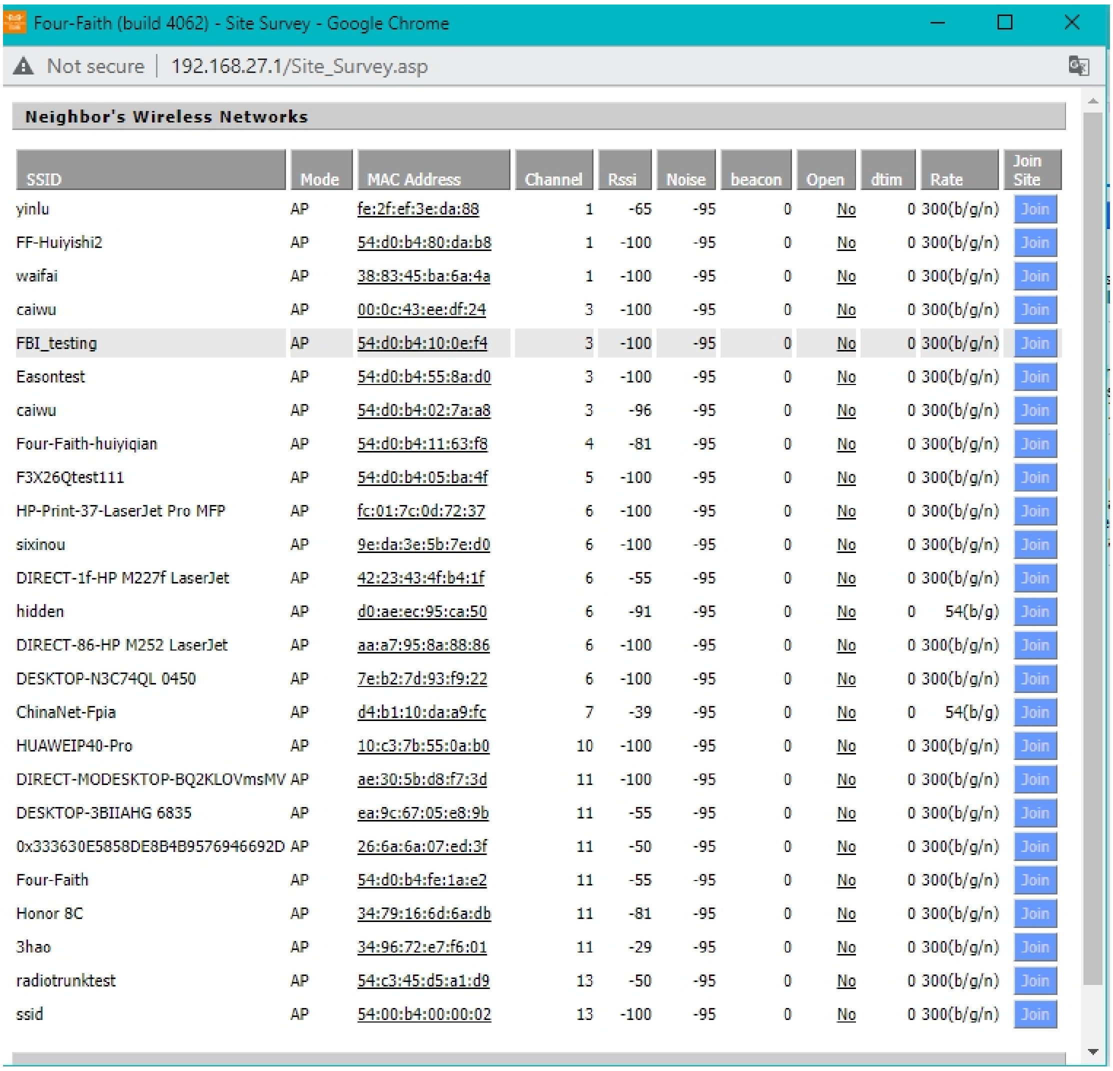
Channel: The channel of the wireless network

Transmission power: reflected power of wireless network

Rate: the reflection rate of the wireless network

Encryption-interface wl0: Whether to encrypt the wl0 interface

Site survey



Four-Faith (build 4062) - Site Survey - Google Chrome

Not secure | 192.168.27.1/Site_Survey.asp

Neighbor's Wireless Networks

SSID	Mode	MAC Address	Channel	Rssi	Noise	beacon	Open	dtim	Rate	Join Site
yinlu	AP	fe:2f:ef:3e:da:88	1	-65	-95	0	No	0	300(b/g/n)	Join
FF-Huiyishi2	AP	54:d0:b4:80:da:b8	1	-100	-95	0	No	0	300(b/g/n)	Join
waifai	AP	38:83:45:ba:6a:4a	1	-100	-95	0	No	0	300(b/g/n)	Join
caiwu	AP	00:0c:43:ee:df:24	3	-100	-95	0	No	0	300(b/g/n)	Join
FBI_testing	AP	54:d0:b4:10:0e:f4	3	-100	-95	0	No	0	300(b/g/n)	Join
Easontest	AP	54:d0:b4:55:8a:d0	3	-100	-95	0	No	0	300(b/g/n)	Join
caiwu	AP	54:d0:b4:02:7a:a8	3	-96	-95	0	No	0	300(b/g/n)	Join
Four-Faith-huiyiqian	AP	54:d0:b4:11:63:f8	4	-81	-95	0	No	0	300(b/g/n)	Join
F3X26Qtest111	AP	54:d0:b4:05:ba:4f	5	-100	-95	0	No	0	300(b/g/n)	Join
HP-Print-37-LaserJet Pro MFP	AP	fc:01:7c:0d:72:37	6	-100	-95	0	No	0	300(b/g/n)	Join
sixinou	AP	9e:da:3e:5b:7e:d0	6	-100	-95	0	No	0	300(b/g/n)	Join
DIRECT-1f-HP M227f LaserJet	AP	42:23:43:4f:b4:1f	6	-55	-95	0	No	0	300(b/g/n)	Join
hidden	AP	d0:ae:ec:95:ca:50	6	-91	-95	0	No	0	54(b/g)	Join
DIRECT-86-HP M252 LaserJet	AP	aa:a7:95:8a:88:86	6	-100	-95	0	No	0	300(b/g/n)	Join
DESKTOP-N3C74QL 0450	AP	7e:b2:7d:93:f9:22	6	-100	-95	0	No	0	300(b/g/n)	Join
ChinaNet-Fpia	AP	d4:b1:10:da:a9:fc	7	-39	-95	0	No	0	54(b/g)	Join
HUAWEIP40-Pro	AP	10:c3:7b:55:0a:b0	10	-100	-95	0	No	0	300(b/g/n)	Join
DIRECT-MODESKTOP-BQ2KLOVmsMV	AP	ae:30:5b:d8:f7:3d	11	-100	-95	0	No	0	300(b/g/n)	Join
DESKTOP-3BIIAHG 6835	AP	ea:9c:67:05:e8:9b	11	-55	-95	0	No	0	300(b/g/n)	Join
0x333630E5858DE8B4B9576946692D	AP	26:6a:6a:07:ed:3f	11	-50	-95	0	No	0	300(b/g/n)	Join
Four-Faith	AP	54:d0:b4:fe:1a:e2	11	-55	-95	0	No	0	300(b/g/n)	Join
Honor 8C	AP	34:79:16:6d:6a:db	11	-81	-95	0	No	0	300(b/g/n)	Join
3hao	AP	34:96:72:e7:f6:01	11	-29	-95	0	No	0	300(b/g/n)	Join
radiotrunktest	AP	54:c3:45:d5:a1:d9	13	-50	-95	0	No	0	300(b/g/n)	Join
ssid	AP	54:00:b4:00:00:02	13	-100	-95	0	No	0	300(b/g/n)	Join

Nearby wireless networks: display other nearby networks

SSID: The name of the neighboring wireless network

Mode: Proximity wireless working mode

MAC address: MAC address of neighboring wireless

Channel: adjacent wireless channel

Rssi: nearby wireless signal strength

Noise: nearby wireless noise

Beacon: Proximity wireless signal marker

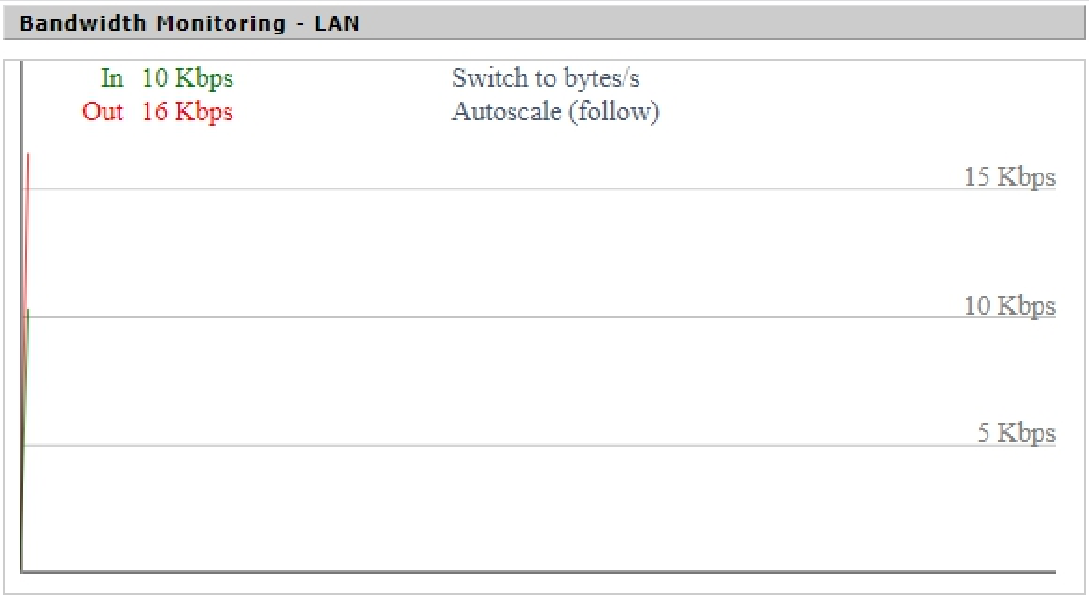
Turn on: Whether the proximity wireless is turned on

Dtim: Proximity wireless delivery and transmission instruction information

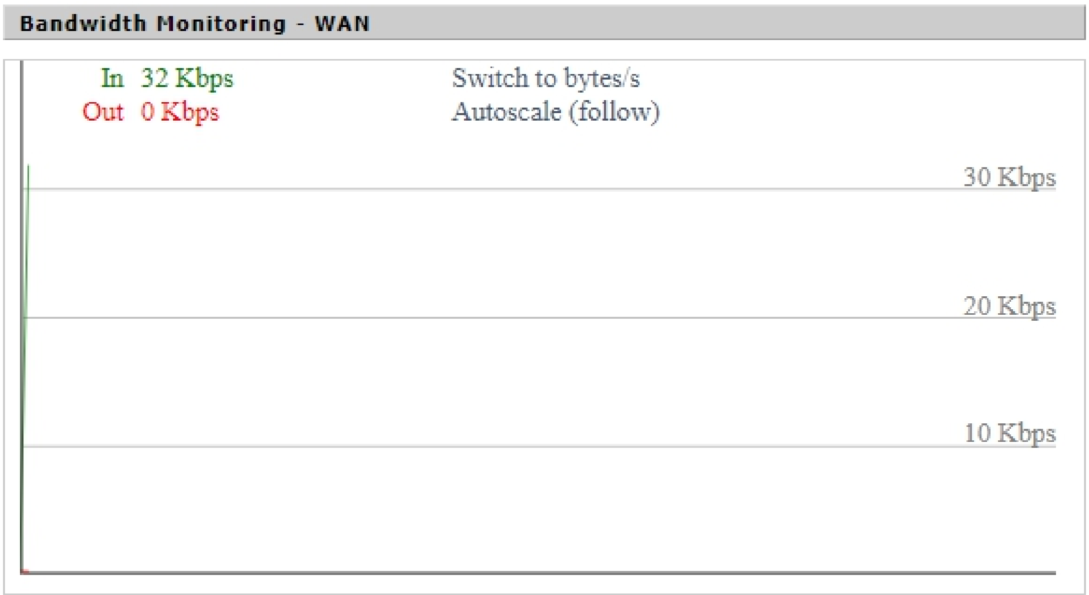
Speed: the speed of the neighboring wireless

Join base station: click to join the neighboring wireless network

3.3.11.5 Bandwidth


Bandwidth Monitoring - LAN

In 10 Kbps
Out 16 Kbps
Switch to bytes/s
Autoscale (follow)


Bandwidth Monitoring - WAN

In 32 Kbps
Out 0 Kbps
Switch to bytes/s
Autoscale (follow)

The real-time detection state diagram of the LAN port, the abscissa represents the time, the ordinate represents the code rat

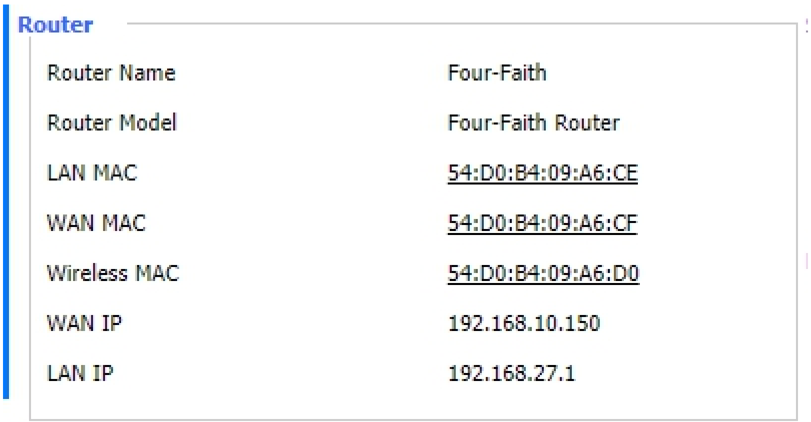
WAN port's time-to-time detection status diagram, the abscissa represents the time, the ordinate represents the code rate

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

Switch to: Click the label to select the unit (byte/second or bit/second).

Autoscale: Click on the label to select the type of graph auto-scaling.

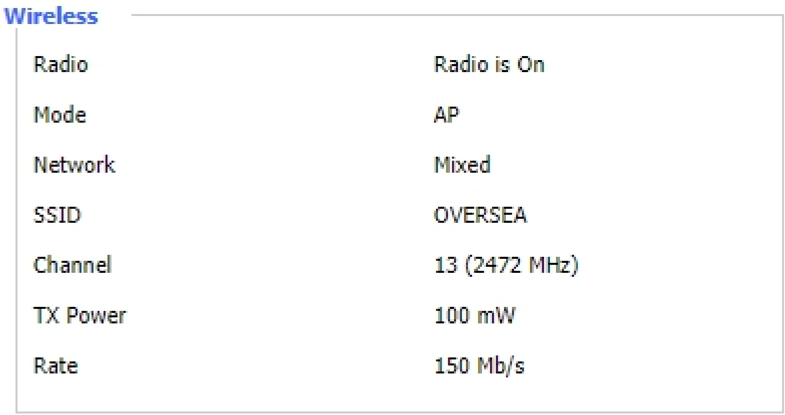
3.3.11.6 System info



Router

Router Name	Four-Faith
Router Model	Four-Faith Router
LAN MAC	54:D0:B4:09:A6:CE
WAN MAC	54:D0:B4:09:A6:CF
Wireless MAC	54:D0:B4:09:A6:D0
WAN IP	192.168.10.150
LAN IP	192.168.27.1

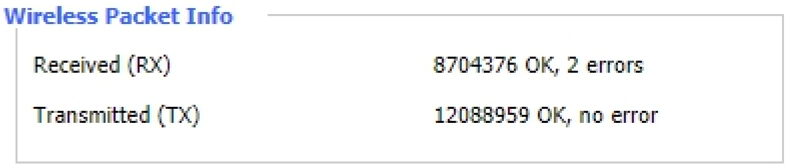
Router Name: The name of the native 5G industrial CPE
Router model: the model of the native 5G industrial CPE
LAN MAC: MAC address of the LAN port
WAN MAC: MAC address of WAN port
Wireless MAC: wireless MAC address
WAN IP: IP address of WAN port
LAN IP: IP address of the LAN port



Wireless

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	OVERSEA
Channel	13 (2472 MHz)
TX Power	100 mW
Rate	150 Mb/s

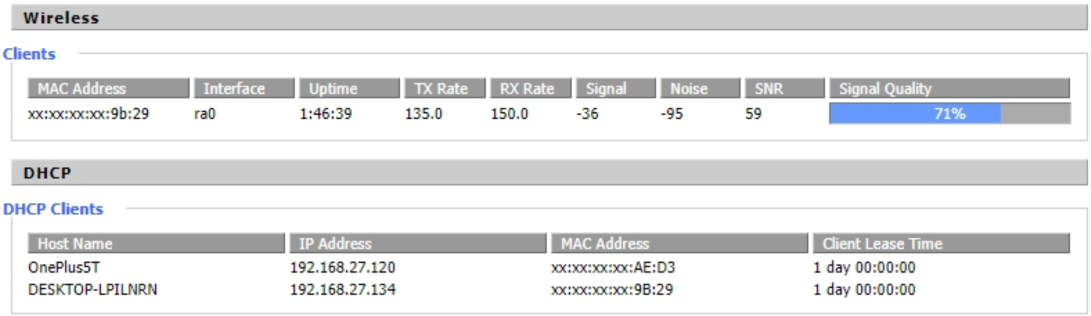
Wireless network: Shows whether the wireless network is turned on
Mode: wireless mode
Network: wireless network mode
SSID: The name of the wireless network
Channel: The channel of the wireless network
Transmission power: reflected power of wireless network
Rate: the reflection rate of the wireless network



Wireless Packet Info

Received (RX)	8704376 OK, 2 errors
Transmitted (TX)	12088959 OK, no error

Received (RX): data packet that has been received
Transmitted (TX): The data packet that has been sent



Wireless

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
xx:xx:xx:xx:9b:29	ra0	1:46:39	135.0	150.0	-36	-95	59	71%

DHCP

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time
OnePlus5T	192.168.27.120	xx:xx:xx:xx:AE:D3	1 day 00:00:00
DESKTOP-LPILNRN	192.168.27.134	xx:xx:xx:xx:9B:29	1 day 00:00:00

Host name: the host name 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 leased this IP address