F8926-GW LoRaWAN Gateway User Manual	Document Version	Pages
	V1.0.0	
	Model：F8926-GW	Total: 77

F8926-GW LoRaWAN Gateway User Manual

Model	Category
F8926-GW-W	LoRa+WCDMA+WIFI Router
F8926-GW-FL	LoRa+LTE FDD+WIFI Router
F8926-GW-L	LoRa+LTE+WIFI Router

Four-Faith Corporation

Add：11th Floor, A-06 Area, No.370, Chengyi Street, Jimei,
Xiamen, Fujian, China.

Tel：+86 592-5907276 Fax: +86 592-5912735

Web: en.four-faith.com

Files Revised Record

Date	Version	Remark	Author
2019.2.19	V1.0.0	Initial version	Jim

Copyright Notice

All contents in the files are protected by copyright law, and all copyrights are reserved by Xiamen Four-Faith Communication Technology Co., Ltd. Without written permission, all commercial use of the files from Four-Faith are forbidden, such as copy, distribute, reproduce the files, etc., but non-commercial purpose, downloaded or printed by individual (all files shall be not revised, and the copyright and other proprietorship notice shall be reserved) are welcome.

Trademark Notice

Four-Faith、四信、 、 、 are all registered trademarks of Xiamen Four-Faith Communication Technology Co., Ltd., illegal use of the name of Four-Faith, trademarks and other marks of Four-Faith is forbidden, unless written permission is authorized in advance.

WAN/
LAN
LAN
System
WiFi
Online
LoRa
SIM/UIM
Power

Contents

Chapter 1 Product Introduction

1.1 Overview

F8926-GW is a wireless data transmission gateway based on standard LoRaWAN protocol, and it applicable to the terminal and NS which meets standard LoRaWan protocol. It can be connected to LoRaWAN terminals in various application nodes, collects useful information and sends the data to cloud server through wireless 3G/4G cellular network or wired ethernet port.

The product uses the high-performance industrial-grade 32-bits CPU and wireless module, with the embedded real-time operating system as the software support platform. It provides 1*LAN/WAN, 1*LAN, 1*Console, 1*WIFI, 1*USIM, 3*antenna interfaces and DC power supply. And it supports wireless configuration, management and online update.

1.2 Features & Benefits

Industrial-grade Design

- High performance industrial-grade 32-bits CPU
- High performance industrial-grade wireless communication module
- High performance industrial-grade multi-channel LoRaWAN RF chip
- Support low power mode
- Metal housing, IP30 metal casting

Stability & Reliability

- WDT design
- Complete anti-drop mechanism ensures device always online
- Ethernet interface with built-in 1.5KV electromagnetic isolation protection
- RS232/RS485 interface with built-in 1.5KV electromagnetic isolation protection
- SIM/UIM card interface with built-in 15KV ESD protection
- Built-in reverse phase protection, over voltage protection and lightning protection
- Antenna lightning protection

Standard & Easy-To-Use

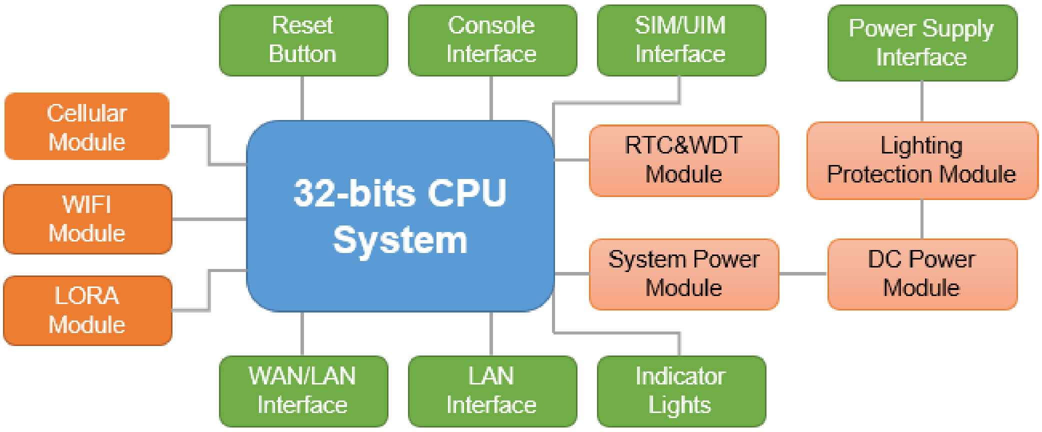
- Standard RS232 (or RS485/RS422), ethernet and WIFI interfaces
- Standard WAN/LAN port (support standard PPPOE protocol)
- Automatically enter into transmission status after power-on
- Powerful central management software

- Multiple working mode are available
- Convenient system configuration and maintenance interface

Powerful Functions

- Support static IP, DHCP, L2TP, PPTP, PPPOE and 2.5G/3G/4G connection types
- Support cellular and wired-WAN dual link intelligent switching backup
- Support VPN client (PPTP, L2TP, OPENVPN, IPSEC and GRE) (only for the VPN version)
- Support VPN server (PPTP, L2TP, OPENVPN, IPSEC and GRE) (only for the VPN version)
- Support remote management, such as SYSLOG, SNMP, TELNET, SSHD and HTTPS
- Support local and remote online upgrade
- Support NTP, embedded RTC
- Support multiple DDNS
- Support MAC address clone
- WIFI support 802.11b/g/n protocol, and can set AP, AP Client, Relay, Relay bridge or WDS mode
- WIFI support WEP, WPA and WPA2 encryption types
- WIFI support RADIUS authentication and MAC address filter
- Support many online or offline trigger modes, include short message, phone call, serial message and network message methods
- Support APN/VPDN
- Support DHCP server and DHCP client
- Support TCP/IP, UDP, FTP and HTTP network protocols
- Support SPI firewall, VPN, access control and URL filter functions
- Support wireless data transmission by LoRa

1.3 Hardware Block Diagram



1.4 Specifications

CHARACTERISTICS	
Network Structure	Simple Star Network Topology and support repeater mode
LoRaWAN Protocol	Class A, Class B*, Class C
Band	EU433, CN470-510, CN779-787, EU863-870, US902-928, AU915-928, AS923, KR920-923
Outdoor	3.5km
Output Power	23±2dBm@LoRa
Sensitivity	-142dbm@LoRa; -72dBm@WIFI
Bandwidth	125kHz \ 250kHz \ 500kHz
Upstream Channel	8
Downstream Channel	1
Communication Rate	ADR
Work Mode	Support full duplex or half-duplex
Server Report Method	Support 3G/4G or wired-ethernet
Management	Management and upgrade by WIFI
ANTENNA	
Cellular	1*Standard SMA female antenna interface, characteristic impedance: 50Ω
LoRa	1*Standard SMA female antenna interface, characteristic impedance: 50Ω
WIFI	1*Standard SMA male antenna interface, characteristic impedance: 50Ω
POWER SUPPLY	
Standard	12V/1.5A
Range	DC 9~36V
POWER CONSUMPTION	
Stand By	Average Current⩽145mA@12V
Communication	TXD ≤ 450mA@12V RXD ≤ 390mA@12V
PHYSICAL PROPERTIES	
Dimensions	157.0x97.0x25.0 mm (excluding antennas and mountings)
Weight	510g (excluding antennas, accessories and POE power)
Shell	IP30
OTHERS	
Operating Temperature	-35~+75^{o}C
Storage Temperature	-40~+85^{o}C
Relative Humidity	95% (non-condensing)
Certifications	CE*

Chapter 2 Installation

2.1 General Packing List

F8926-GW must be installed correctly and the installation must be conducted by a qualified engineer recognized by Four-Faith.

- *Warning:*

1. Power off before installation

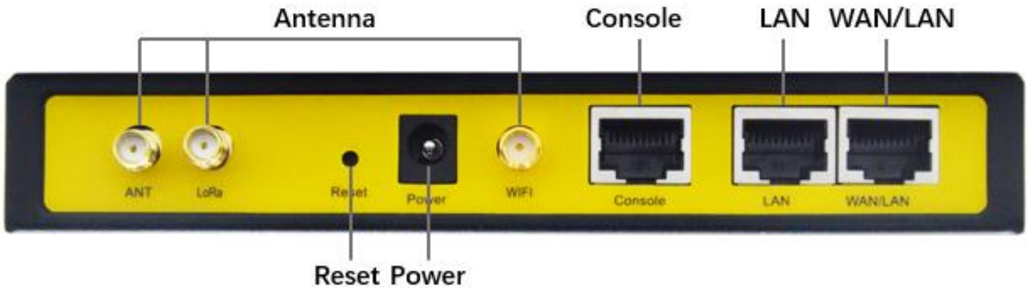
2. Don’t remove the cover, power interface and antenna interface

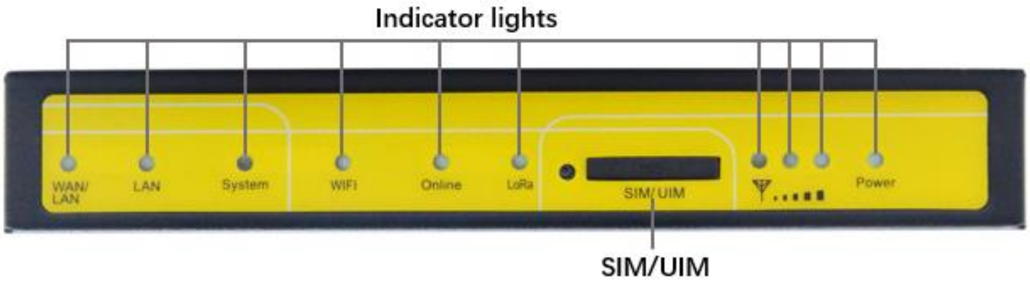
Before you install the F8926-GW, please check the package contents and make sure it completely.

Item	Qty	Remark
F8926-GW	1	
3G/4G cellular SMA male antenna	1	
WIFI SMA female antenna	1	
LoRa SMA male antenna	1	
Power adapter	1	
Network cable	1	
User manual CD	1	
Console cable	1	Optional
QC passed card	1	
Warranty card	1	

Form 2-1 F8926-GW packing list

2.2 Product Overview





2.3 Installation & Connection

2.3.1 Product Installation

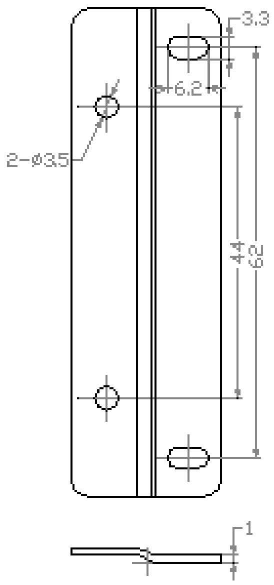
1. Drill 2 holes of ø35mm diameter, 3~4mm depth according to the position of the bracket.

◆ *Requirement:*

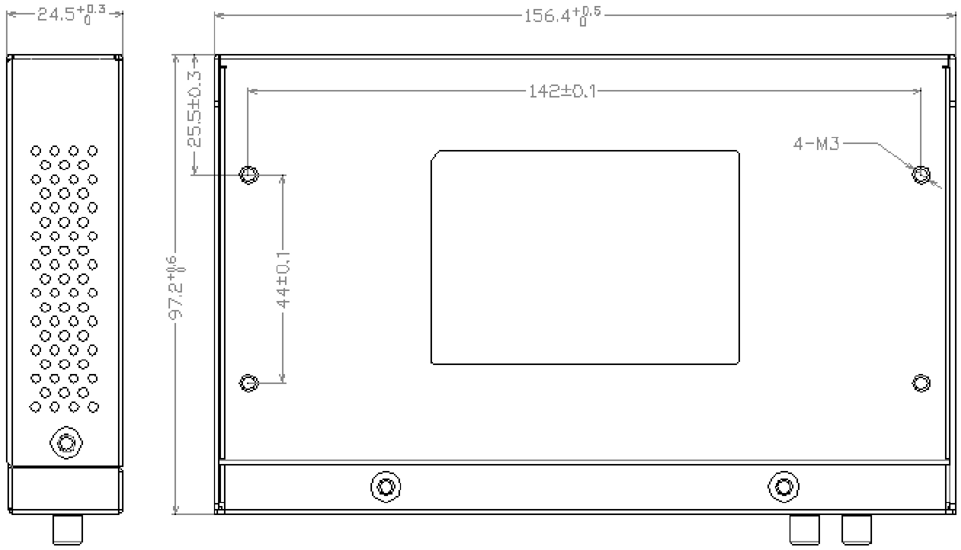
1. the wall should be flat;

2. must be in an open area

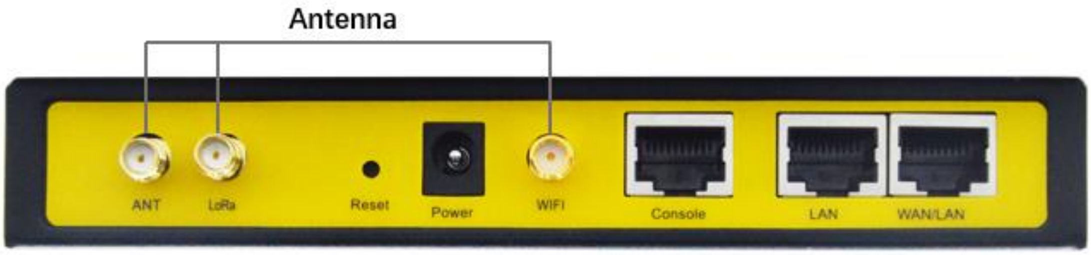
3. make sure no shield within 5 meters



2. Tighten the screws and fix the gateway on the bracket, then install the antenna.



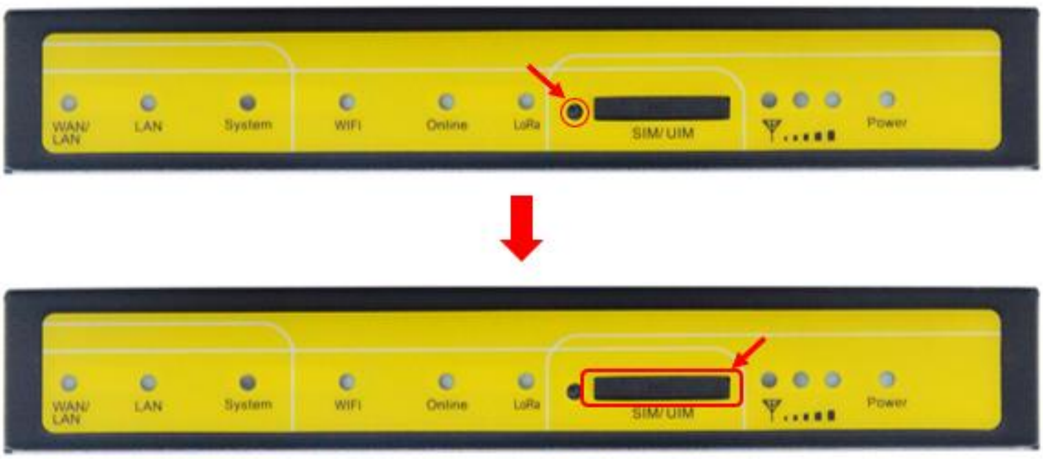
2.3.2 Antenna Installation



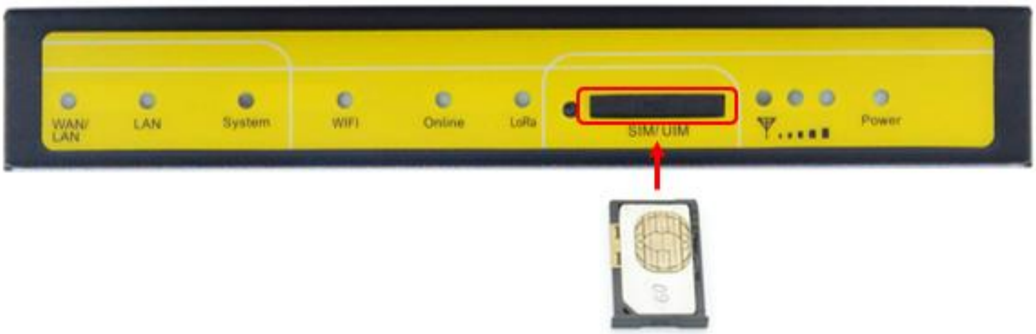
After F8926-GW is installed on the bracket, then install all antennas (4G,WIFI and LoRa), make sure all antennas are tightened to get best signal.

2.3.2 SIM/UIM Card Installation

1. Press the button beside the SIM/UIM card slot, then the SIM/UIM card slot will popup automatically.



2. Put the SIM/UIM card into the card slot, and then insert it into the SIM/UIM interface



2.3.3 Network cable connection

Get the network cable in the package, then one side connect to the LAN port of F8926-GW, and the other side connect to the ethernet port of another network device. The network cable connection line sequence 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

2.3.4 Console cable connection

Get the console cable in the package, then one side connect to the console port of F8926-GW, and the other side connect to PC.

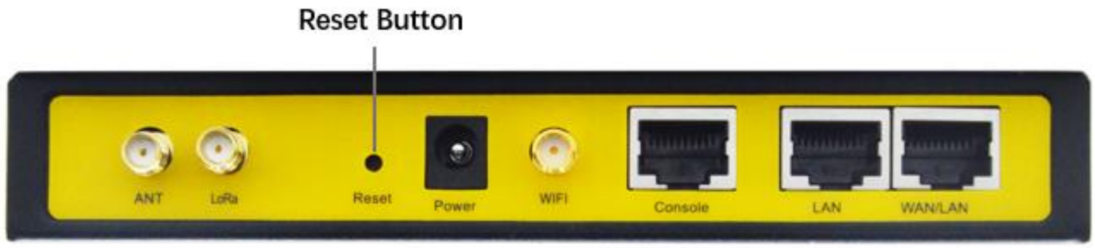
2.4 LED Indicators

The F8926-GW provides the following led indicators: include Power, System, Online, LoRa, WAN/LAN, LAN, WIFI, Signal Strength. All LED indicators description are as below:

LED	Indication	Status	Description
Power	Power Status	On	Power on
		Off	Power off
System	System Status	Flash	System work properly
		Off	System work improperly
Online	Online Status	On	Online
		Off	Offline
LoRa	LoRa Status	On	LoRa connect normal
		Off	LoRa connect abnormal
WAN/LAN	WAN/LAN Status	On	Connected
		Off	Not connected
		Flash	Communicating
LAN	LAN Status	On	Connected
		Off	Not connected
		Flash	Communicating
WIFI	WIFI Status	On	WIFI on
		Off	WIFI off

3G/4G Signal Strength	Signal 1/2/3	Turn on one light	Weak (less than -90dbm)
		Turn on two lights	Medium (-70dbm~-90dbm)
		Turn on three lights	Good (greater than -70dbm)

2.5 Reset Button



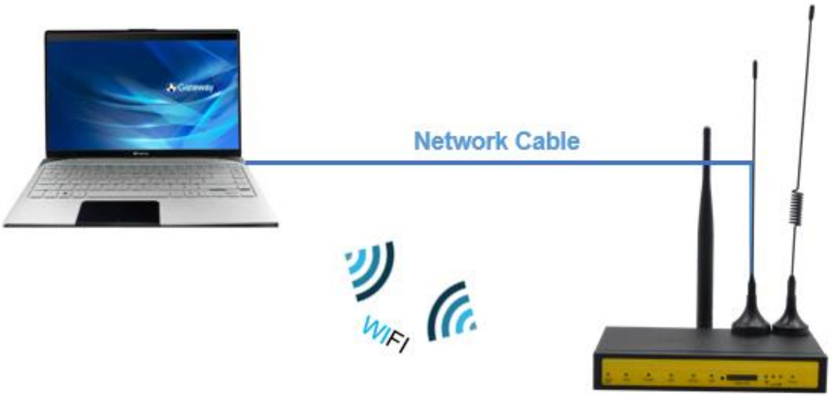
If you want to reset the system, please press the “Reset Button” 15 seconds slightly, then it will restore the configuration parameters factory, and it will reboot automatically after 5 seconds.

Chapter 3 Configuration

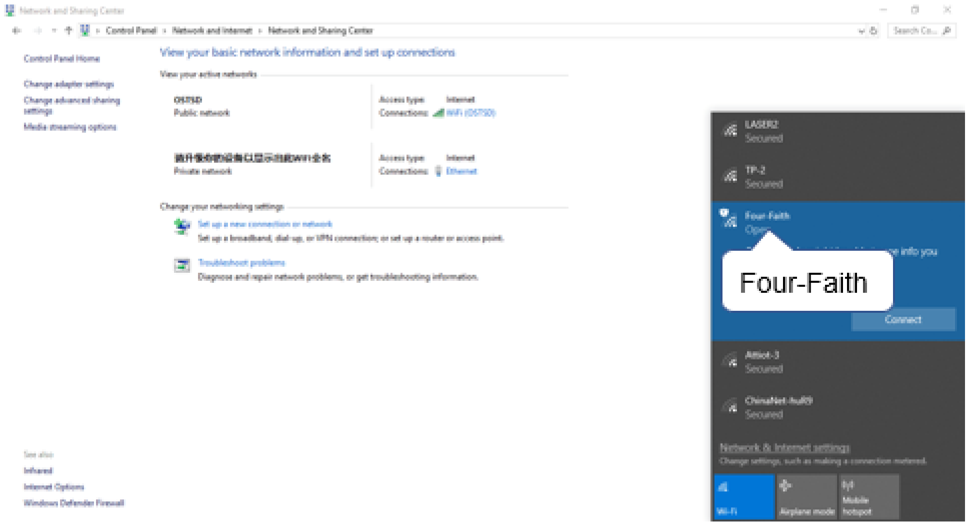
This chapter explains how to access to Web GUI of F8926-GW to complete device configuration.

3.1 Connect with the F8926-GW

Before configuration, you can connect the base station with a PC by WIFI or network cable.



- Connect the base station by **WIFI** (based on WIN10 operator system);



View your basic network information and set up connections

View your active networks

OSTSD Public network	Access type: Internet Connections: WiFi (OSTSD)
[illegible] Private network	Access type: Internet Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

LASER2
Secured

TP-2
Secured

Four-Faith
Open

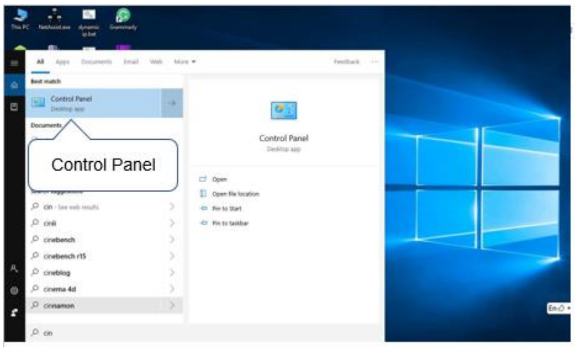
Attiot-3
Secured

ChinaNet-hufi9
Secured

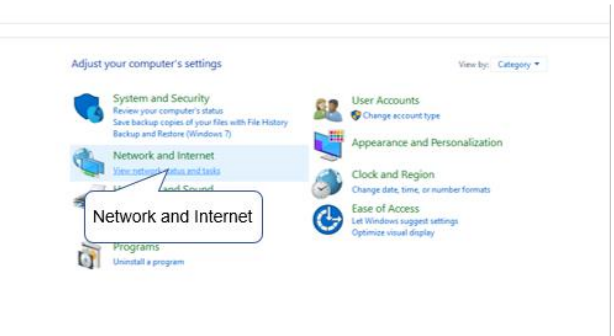
Network & Internet settings
Change settings, such as making a connection metered.

1 Connect the open hotspot “Four-Faith”, and then click the “Connect” button to connect it.

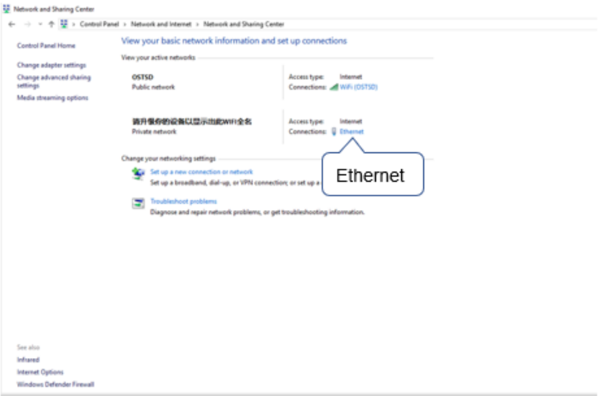
- ◆ Connect the base station by **network cable** (based on WIN10 operator system)



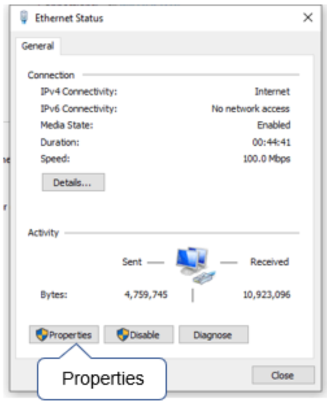
1 Click the "Search Box" to search "Control Panel", and then open it


Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Network and Internet
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

2 Find the "Network and Internet" item, and then click the "View network status and tasks"

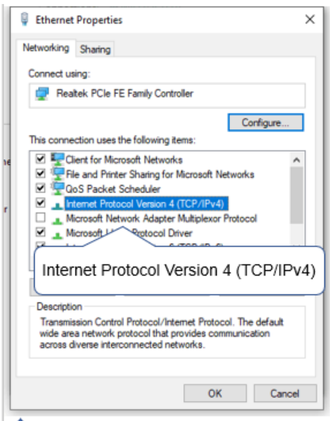

Network and Sharing Center
Control Panel › Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
Access type: Internet
Connections: Wi-Fi (OSTSD)
Access type: Internet
Connections: Ethernet
Change your networking settings
Set up a new connection or network
Troubleshoot problems
Ethernet
See also
Infrared
Internet Options
Windows Defender Firewall

3 Jump to this page, and click the "Ethernet"



IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:44:41
Speed: 100.0 Mbps
Bytes: Sent 4,759,745 Received 10,923,096

4 Click "Properties" to enter into IP configure UI



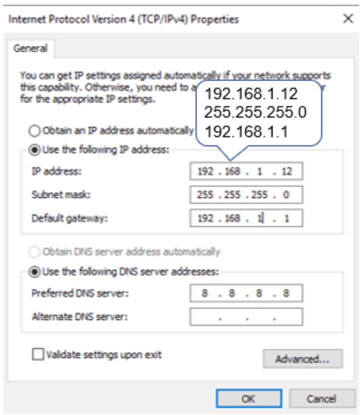
Connect using: Realtek PCIe FE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description: Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

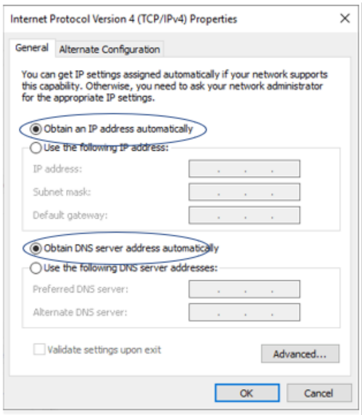
5 Double click the "Internet Protocol Version 4(TCP/IPv4)" to configure IP information



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 . 12
  - 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: 8 . 8 . 8 . 8
  - Alternate DNS server: . . .
- □ Validate settings upon exit

6 Method 1: assign a static IP address manually within the subnet of F8L10GW



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:
- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:
- □ Validate settings upon exit

7 Method 2: click the "obtain an IP address automatically" to assign an IP address automatically

3.2 Access to configuration pages

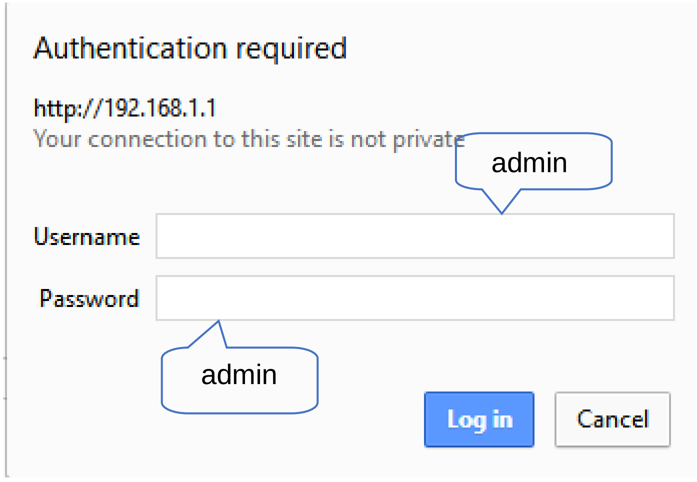
Four-Faith LoRaWAN base station provides web configuration management. You can access to the configuration pages fellow these steps:

1. Open browser (such as google, IE or others)
2. Input “**192.168.1.1**” in the search bar, and then it will enter into the configuration login page when connect F8926-GW correctly. If you are the first time configure the base station, please use the default settings by Four-Faith.

   IP: 192.168.1.1

   Username: admin

   Password: admin



Authentication required

http://192.168.1.1

Your connection to this site is not private

Username: admin

Password: admin

3. Click the **“Log in”** button, and then you can access to device configuration management

3.3 Web Configuration

There are 11 main pages in the web configuration tool, include Setup, Wireless, Services, VPN, Security, Access Restrictions, NAT, QoS, Applications, Admin and Status.

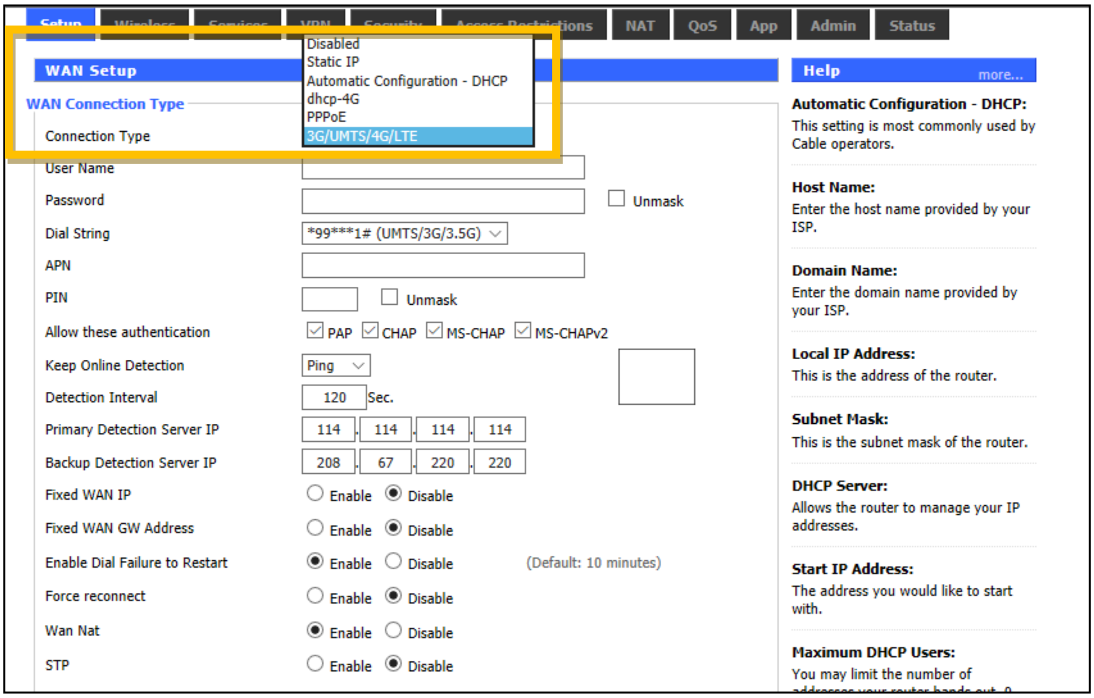
3.3.1 Setup

In this module, you can according system directions to change the basic settings of F8926-GW.

Warning: Click the “Save” button only save current settings, you need click the “Apply Settings” to make it effect. And if you don’t want save changes, click the “Cancel Changes” will realize it.

3.3.1.1 Basic Setup

- **WAN Setup**



WAN Setup

WAN Connection Type

Connection Type	3G/UMTS/4G/LTE	
User Name		
Password		□ Unmask
Dial String	*99***1# (UMTS/3G/3.5G)	
APN		
PIN		□ Unmask
Allow these authentication	☑ PAP ☑ CHAP ☑ MS-CHAP ☑ MS-CHAPv2	
Keep Online Detection	Ping	
Detection Interval	120 Sec.	
Primary Detection Server IP	114 . 114 . 114 . 114	
Backup Detection Server IP	208 . 67 . 220 . 220	
Fixed WAN IP	○ Enable ● Disable	
Fixed WAN GW Address	○ Enable ● Disable	
Enable Dial Failure to Restart	● Enable ○ Disable	(Default: 10 minutes)
Force reconnect	○ Enable ● Disable	
Wan Nat	● Enable ○ Disable	
STP	○ Enable ● Disable	

Help more...

Automatic Configuration - DHCP:
This setting is most commonly used by Cable operators.

Host Name:
Enter the host name provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

Local IP Address:
This is the address of the router.

Subnet Mask:
This is the subnet mask of the router.

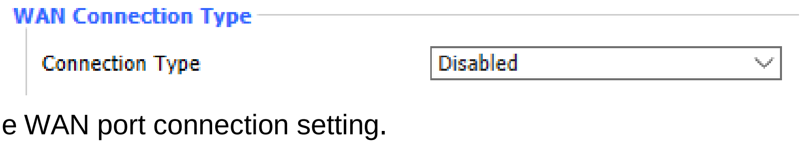
DHCP Server:
Allows the router to manage your IP addresses.

Start IP Address:
The address you would like to start with.

Maximum DHCP Users:
You may limit the number of

There are 6 WAN connection types, include: Disable, Static IP, Automatic Configuration - DHCP, PPPOE, 3G/UMTS/4G/LTE and DHCP-4G.

Mode 1: Disable



WAN Connection Type

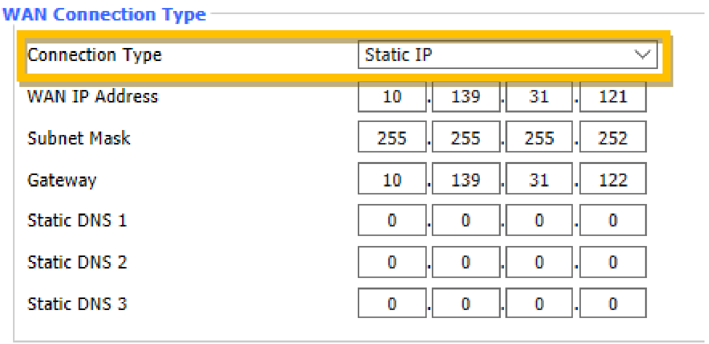
Connection Type	Disabled

Disable the WAN port connection setting.

Mode 2: Static IP

Select the **“Static IP”** connection type, this page will auto refresh and then show the configuration parameters as follow:

Warning: you need prepare a public IP address.



WAN Connection Type

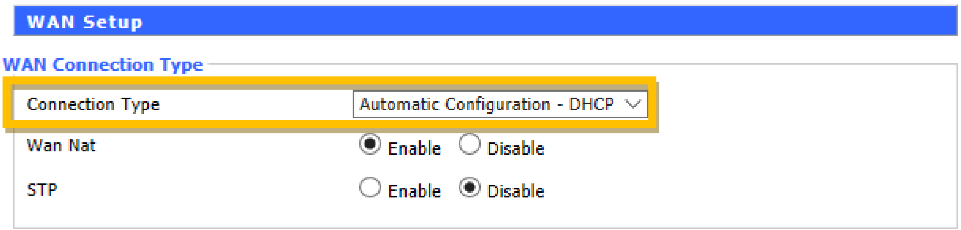
Connection Type	Static IP
WAN IP Address	10 . 139 . 31 . 121
Subnet Mask	255 . 255 . 255 . 252
Gateway	10 . 139 . 31 . 122
Static DNS 1	0 . 0 . 0 . 0
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0

Parameters	Option	Description
WAN IP Address	-	Public IP address
Subnet Mask	-	Subnet mask parameter
Gateway	-	Gateway parameter
Static DNS1	-	Static domain name server 1
Static DNS2	-	Static domain name server 2
Static DNS3	-	Static domain name server 3

Mode 3: Automatic Configuration – DHCP (default)

Select the **"Automatic Configuration - DHCP"** connection type, this page will auto refresh and then show the configuration parameters as follow:

Warning: device will dynamic assignment the IP address to WAN port in this mode.



WAN Setup

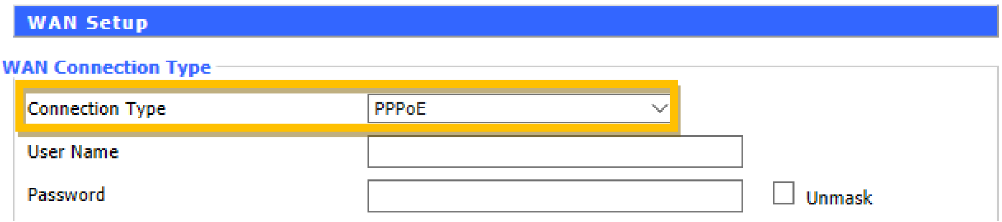
WAN Connection Type

Connection Type	Automatic Configuration - DHCP
Wan Nat	● Enable ○ Disable
STP	○ Enable ● Disable

Mode 4: PPPoE

Select the **"PPPoE"** connection type, this page will auto refresh and then show the configuration parameters as follow:

Warning: you need to fill in the username and password to take it effect.



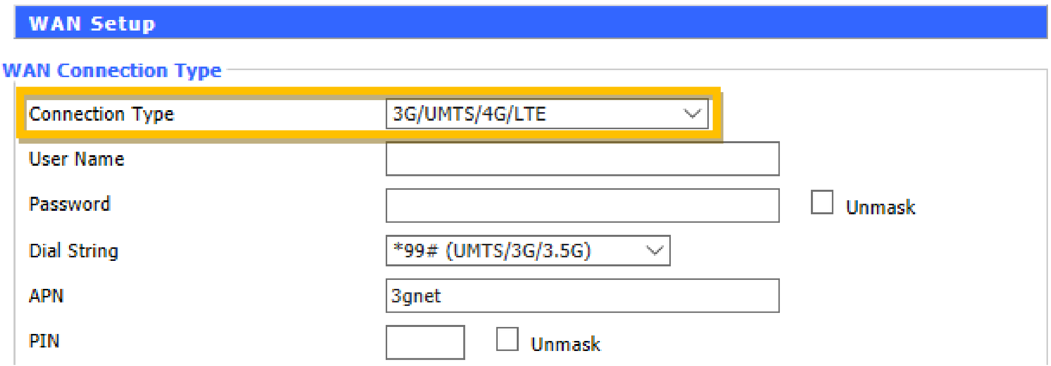
WAN Setup

WAN Connection Type

Connection Type	PPPoE
User Name	
Password	□ Unmask

Mode 5: 3G/UMTS/4G/LTE

Select the **"3G/UMTS/4G/LTE"** connection type, this page will auto refresh and then show the configuration parameters as follow:



WAN Setup

WAN Connection Type

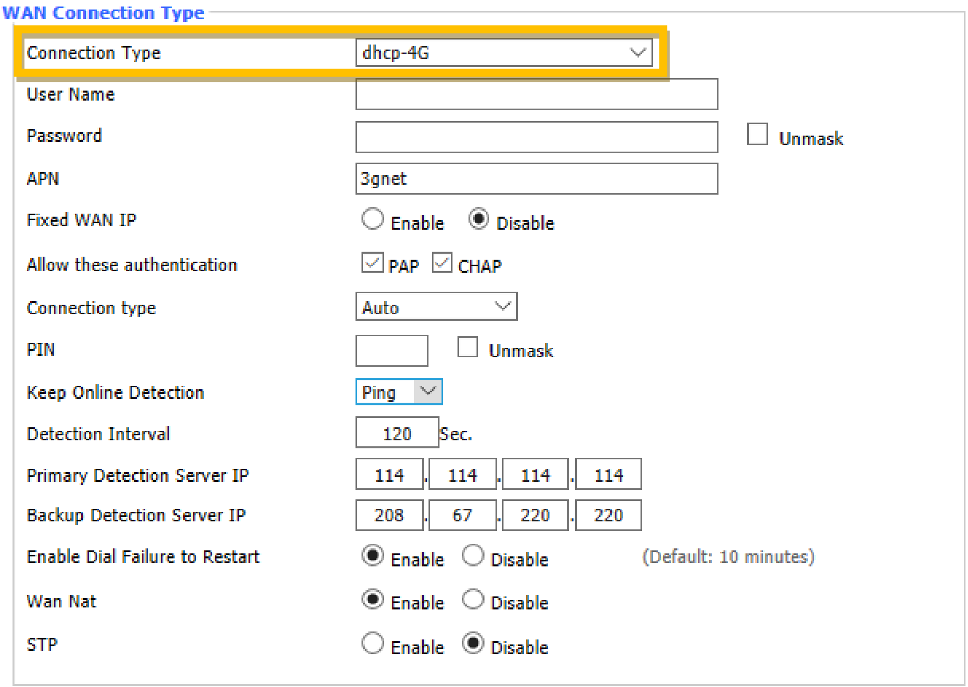
Connection Type	3G/UMTS/4G/LTE	
User Name		
Password		□ Unmask
Dial String	*99# (UMTS/3G/3.5G)	
APN	3gnet	
PIN		□ Unmask

Parameters	Option	Description
User Name	-	Input user name
Password	-	Input password
Dail String	-	Call to operator's number
APN	-	Access point name
PIN	-	PIN number

Mode 6: DHCP-4G

Select the **"dhcp-4G"** connection type, this page will auto refresh and then show the configuration parameters as follow:

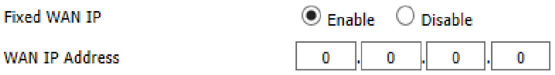
Warning: In this mode, the IP address of WAN port assigned by dhcp-4G (default).



WAN Connection Type

Connection Type	dhcp-4G	
User Name		
Password		□ Unmask
APN	3gnet	
Fixed WAN IP	○ Enable ● Disable	
Allow these authentication	☑ PAP ☑ CHAP	
Connection type	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	
Enable Dial Failure to Restart	● Enable ○ Disable	(Default: 10 minutes)
Wan Nat	● Enable ○ Disable	
STP	○ Enable ● Disable	

Parameters	Option	Description
User Name	-	Sim card account assigned by operator
Password	-	Sim card account assigned by operator
APN	-	APN number assigned by operator

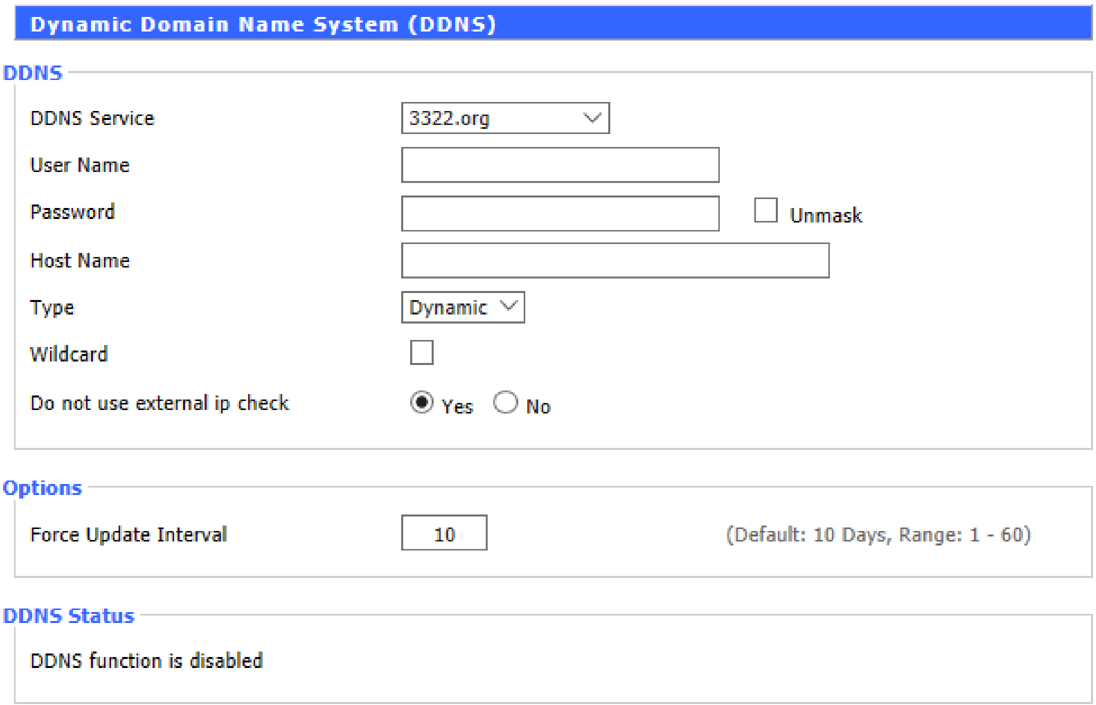
Fixed WAN IP	Enable	Turn on fixed WAN IP address function. And then fill in the WAN IP address  Fixed WAN IP ● Enable ○ Disable WAN IP Address 0 . 0 . 0 . 0
	Disable	Turn off this function
Allow these authentication	PAP	PAP authentication
	CHAP	CHAP authentication
Connection type	Auto	Automatically select operator network according deployment position
	Force-4G	Only works on 4G network
	Force-3G	Only works on 3G network
	Force-2G	Only works on 2G network
	Prefer-3G	3G network prefer select
	Prefer-2G	2G network prefer select
	Only 3G/2G	Support 2G/3G network
	Only 4G/3G/2G	Support 2G/3G/4G network
PIN	-	Sim card pin number
Keep Online Detection	None	Disable keep online detection function
	Ping	Send ping packets to detect whether connection is normal. In this mode, the “Detection Interval”, “Primary Detection Server IP” and “Backup Detection Server IP” must be configured correctly
	Router	Use router method to detect whether connection is normal. In this mode, the “Detection Interval”, “Primary Detection Server IP” and “Backup Detection Server IP” must be configured correctly
Detection Interval	-	Time interval between two detection, unit is second
Primary Detection Server IP	-	Response the primary detection server IP address of F8926-GW when detect data packets online. This configuration item takes effect when “**Keep Online Detection**” set **“Ping”** or **“Router”** mode
Backup Detection Server IP	-	Response the backup detection server IP address of F8926-GW when detect data packets online. This configuration item takes effect when “**Keep Online Detection**” set **“Ping”** or **“Router”** mode
Enable Dial Failure to Restart	Enable	Turn on restart the device when dial-up failure function
	Disable	Turn off restart the device when dial-up failure

		function
Wan Nat	Enable	Turn on NAT forwarding of WAN port function
	Disable	Turn off NAT forwarding of WAN port function
STP	Enable	Turn on STP protocol. STP (Spanning Tree Protocol) can be applied to the loop network
	Disable	Turn off STP protocol

3.3.1.2 DDNS

DDNS (Dynamic Domain Name Server): Map the router’s dynamic IP address to a fixed domain name server. So you can access the router by domain name, although the IP address may change.

F8926-GW supports many kinds of DDNS server, such as DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO and DynSIP. Also, you can customize it.



Dynamic Domain Name System (DDNS)

DDNS

DDNS Service: 3322.org

User Name:

Password: □ Unmask

Host Name:

Type: Dynamic

Wildcard: □

Do not use external ip check: ● Yes ○ No

Options

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

DDNS Status

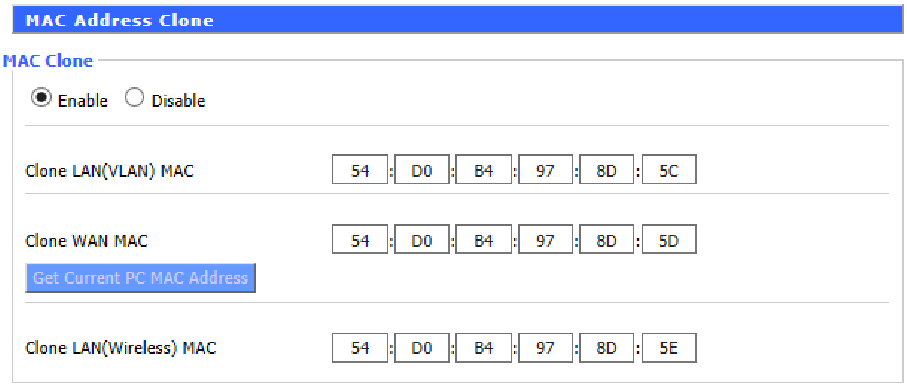
DDNS function is disabled

Parameters	Option	Description
User Name	-	The user name registered in the DDNS server, maximum 64 characters
Password	-	The password registered in the DDNS server, maximum 32 characters
Host Name	-	The host name registered in the DDNS server
Type	-	According to server types
Wildcard	-	Default OFF. If you select “ON”, it means “.host.3322.org” equal to “host.3322.org”
Do not use external IP check	-	Turn on or off external IP check function
Force Update Interval	-	Default 10 days.

DDNS Status	-	Show the current connection status

3.3.1.3 MAC Address Clone

You maybe need to register your MAC address requested by ISP. If you don’t want to register your MAC again, you can clone router’s MAC for ISP.



MAC Address Clone

MAC Clone

● Enable ○ Disable

Clone LAN(VLAN) MAC	54 : D0 : B4 : 97 : 8D : 5C
Clone WAN MAC	54 : D0 : B4 : 97 : 8D : 5D
Clone LAN(Wireless) MAC	54 : D0 : B4 : 97 : 8D : 5E

You can clone 3 parts MAC address: LAN port MAC clone, WAN port MAC clone and wireless MAC clone. There is 2 points need to be note:

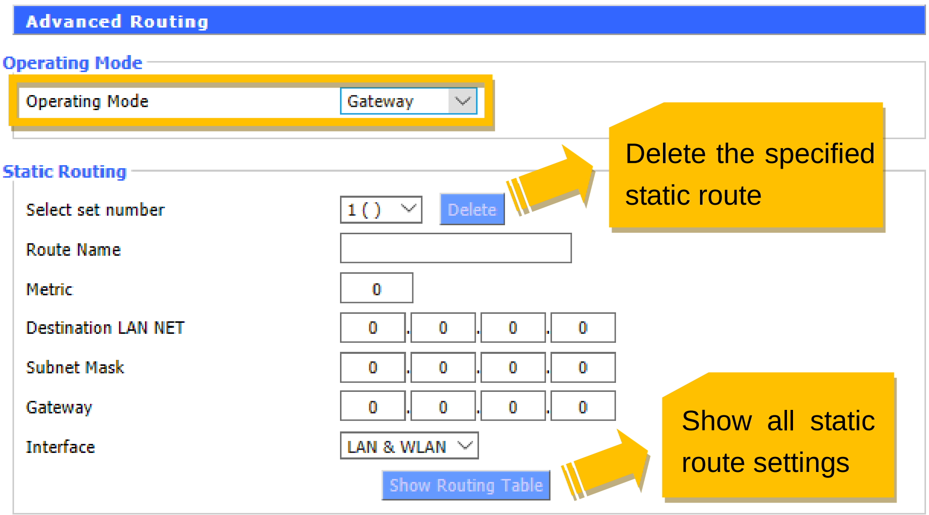
1. *MAC address is 48-bits, the first byte should be even, cannot be set to a multicast address;*
2. *Because of wireless network card and LAN network card conbine with br0 bridge, so the MAC address of the bridge br0 is determined by the smaller value of the MAC address of the LAN network card and the MAC address of wireless network card.*

3.3.1.4 Advanced Routing

In this page, you can set operate mode and static routing parameters. For most users, the “Gateway” mode is recommended.

Mode 1: Gateway

Select the **“Gateway”** mode, this page will auto refresh and then show the configuration parameters as follow:



Advanced Routing

Operating Mode

Operating Mode	Gateway

Static Routing

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

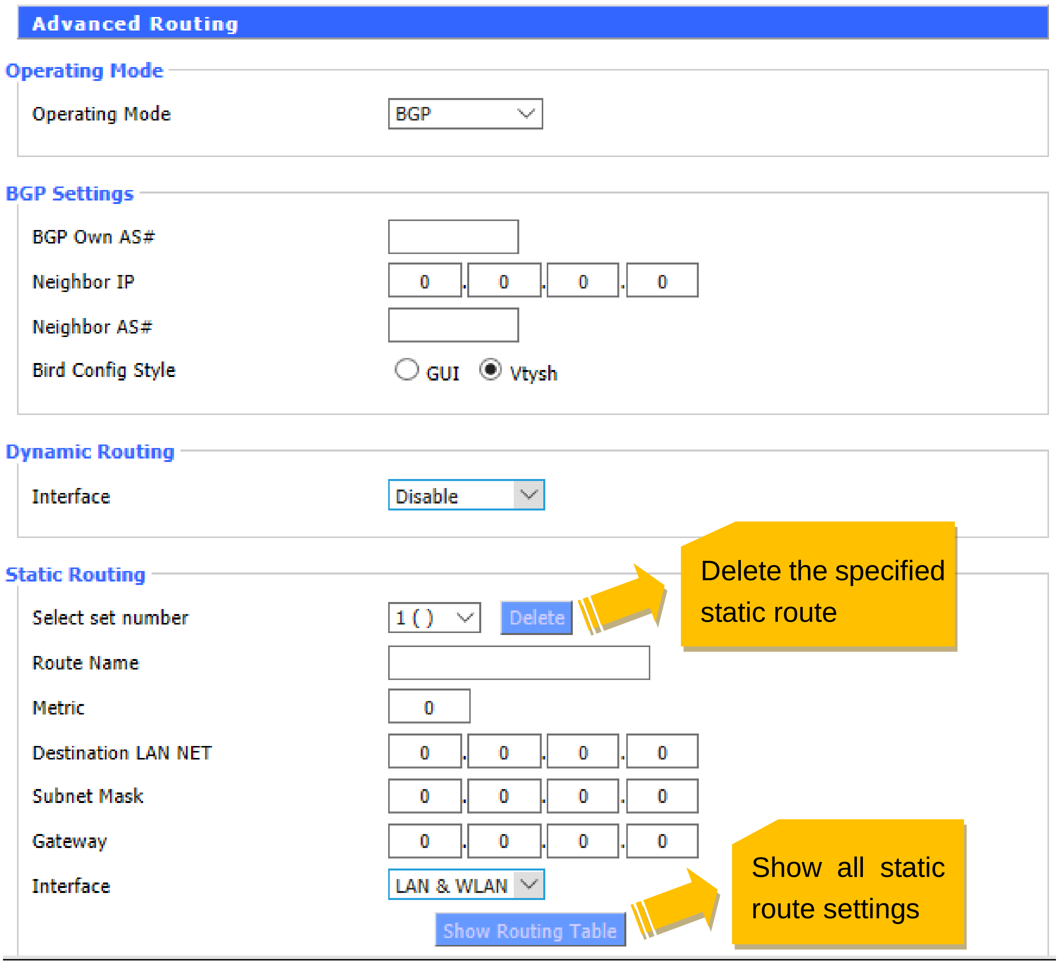
Delete the specified static route

Show all static route settings

Parameters	Option	Description
Select set number	-	You can set static route number (1-50)
Router Name	-	Customize the router name, up to 25 characters
Metric	-	The unit of measure for routing between source and destination address
Destination LAN NET	-	The destination network address or host address
Subnet Mask	-	The subnet mask of router
Gateway	-	The gateway of router
Interface	LAN & WAN	According the position of IP address, you can select suitable interface
	LAN	
	ANY	
	3G	
	IPSEC	

Mode 2: BGP

Select the **"BGP"** mode, this page will auto refresh and then show the configuration parameters as follow:



Advanced Routing

Operating Mode
- Operating Mode: BGP

BGP Settings
- BGP Own AS#:
- Neighbor IP: 0 . 0 . 0 . 0
- Neighbor AS#:
- Bird Config Style: ○ GUI ● Vtysh

Dynamic Routing
- Interface: Disable

Static Routing
- Select set number: 1 ( ) Delete
- 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

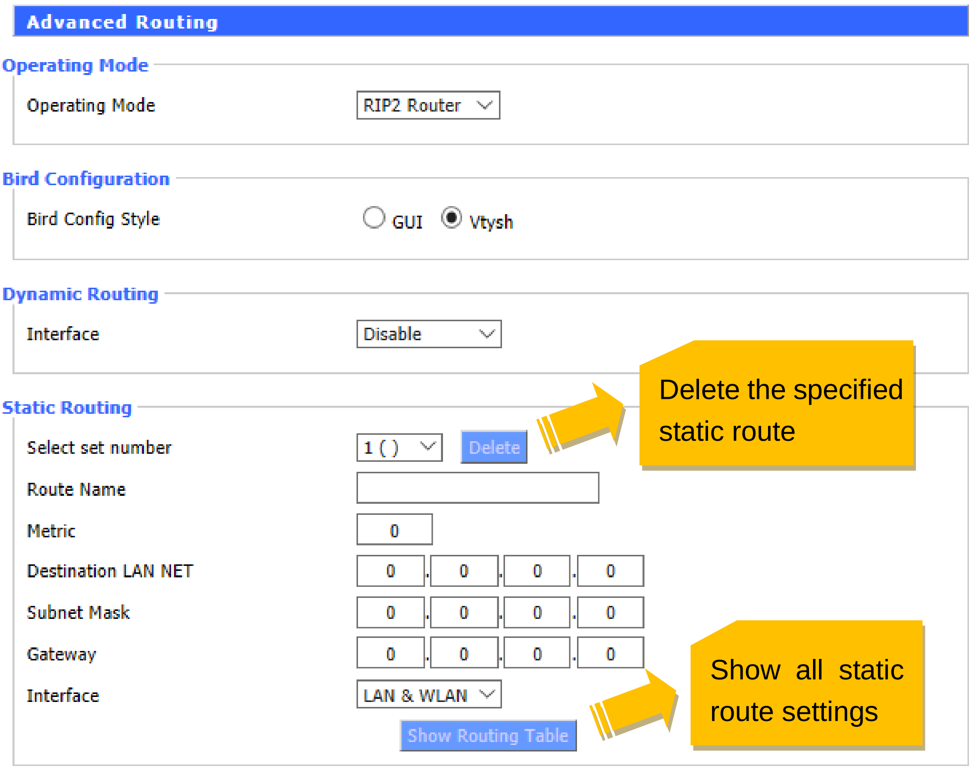
Delete the specified static route

Show all static route settings

Section	Parameters	Option	Description
BGP Settings	BGP Own AS#	-	Own AS number
	Neighbor IP#	-	Neighbor IP address
	Neighbor AS#	-	Neighbor AS number
	Bird Config Style	GUI Vtysh	GUI or vtysh command configure
Dynamic Routing	Interface	Disable WAN LAN & WAN Both	Select dynamic route interface
Static Routing	Select set number	-	You can set static route number (1-50)
	Router Name	-	Customize the router name, up to 25 characters
	Metric	-	The unit of measure for routing between source and destination address
	Destination LAN NET	-	The destination network address or host address
	Subnet Mask	-	The subnet mask of router
	Gateway	-	The gateway of router
	Interface	LAN & WAN LAN ANY 3G IPSEC	According the position of IP address, you can select suitable interface

Mode 3: RIP2 Router

Select the **"RIP2 Router"** mode, this page will auto refresh and then show the configuration parameters as follow:



Advanced Routing

Operating Mode

Operating Mode: RIP2 Router

Bird Configuration

Bird Config Style: ○ GUI ● Vtysh

Dynamic Routing

Interface: Disable

Static Routing

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

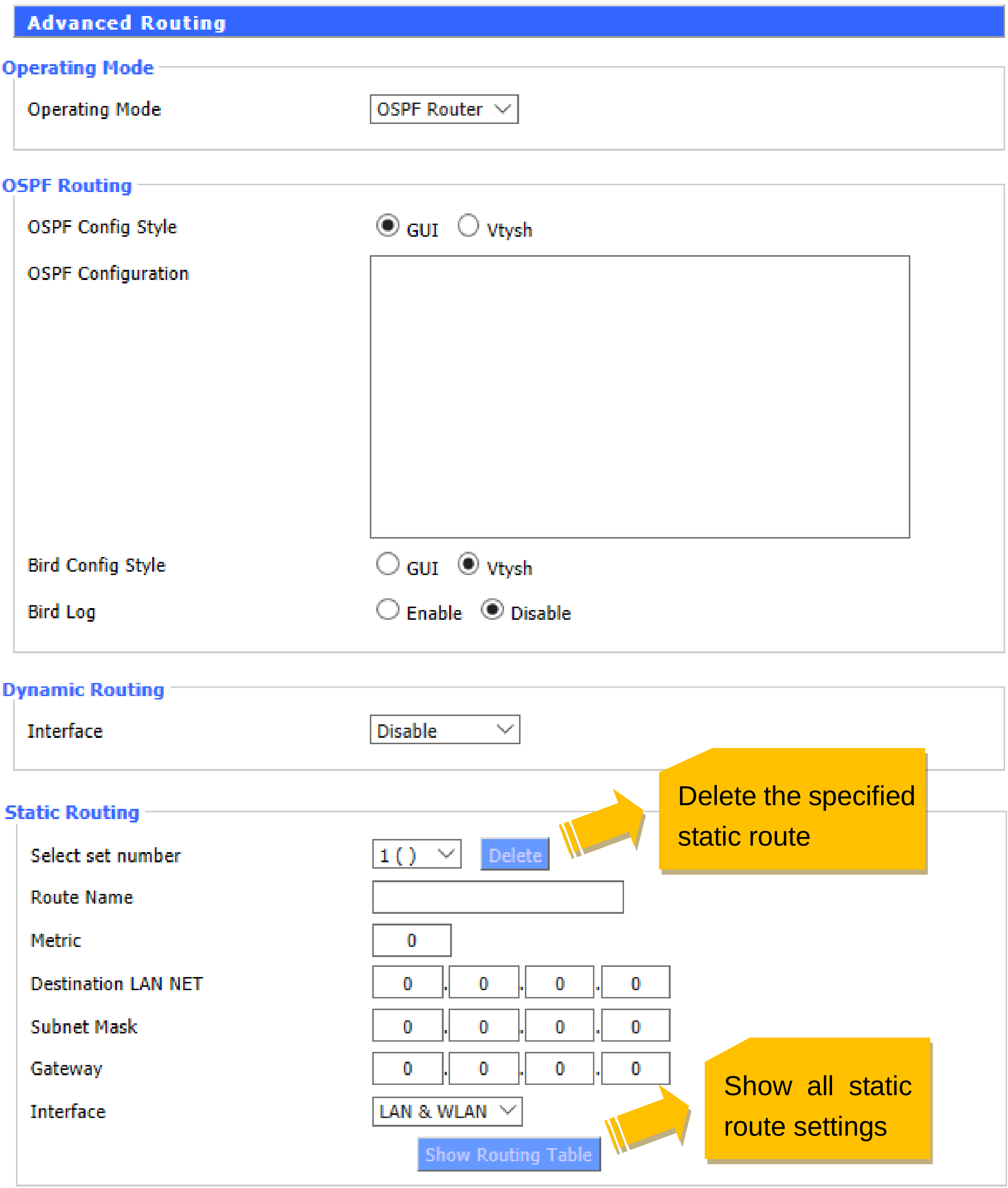
Delete the specified static route

Show all static route settings

Section	Parameters	Option	Description
Bird Configuration	Bird Config Style	GUI Vtysh	GUI or vtysh command configure
Dynamic Routing	Interface	Disable WAN LAN & WAN Both	Select dynamic route interface
Static Routing	Select set number	-	You can set static route number (1-50)
	Router Name	-	Customize the router name, up to 25 characters
	Metric	-	The unit of measure for routing between source and destination address
	Destination LAN NET	-	The destination network address or host address
	Subnet Mask	-	The subnet mask of router
	Gateway	-	The gateway of router
	Interface	LAN & WAN LAN ANY 3G IPSEC	According the position of IP address, you can select suitable interface

Mode 4: OSPF Router

Select the **"OSPF Router"** mode, this page will auto refresh and then show the configuration parameters as follow:



Advanced Routing

Operating Mode

Operating Mode: OSPF Router

OSPF Routing

OSPF Config Style: ● GUI ○ Vtysh

OSPF Configuration:

Bird Config Style: ○ GUI ● Vtysh

Bird Log: ○ Enable ● Disable

Dynamic Routing

Interface: Disable

Static Routing

Select set number: 1 ( ) Delete

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

Show Routing Table

Delete the specified static route

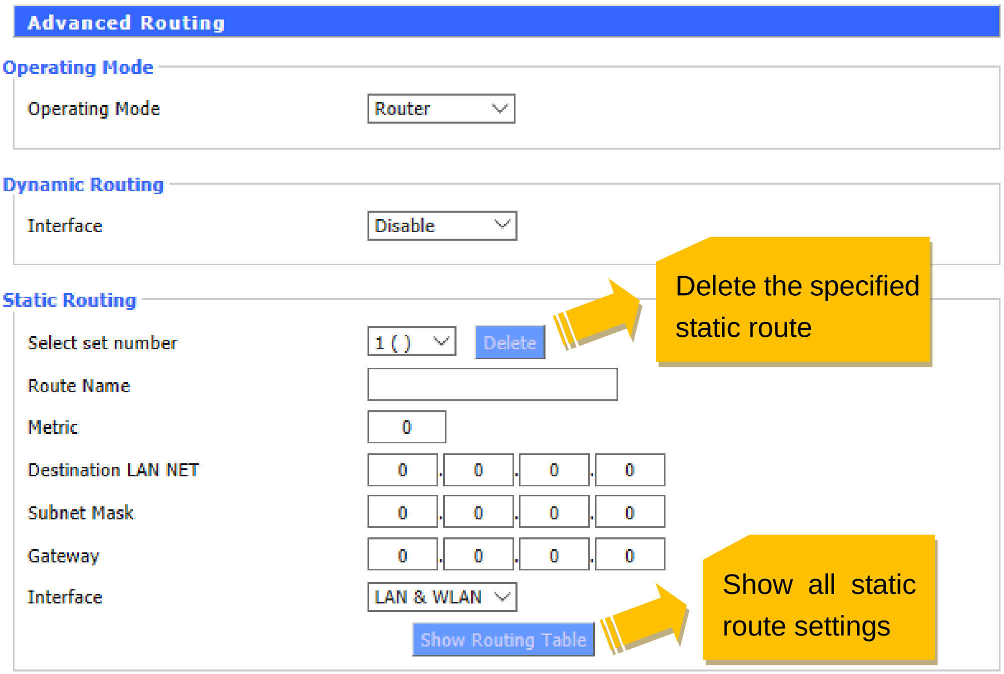
Show all static route settings

Section	Parameters	Option	Description
OSPF Routing	**OSPF Config Style**	GUI	GUI or vtysh command configure
		Vtysh	
	OSPF Configuration		OSPF configuration
	Bird Config Style	GUI	GUI or vtysh command configure
		Vtysh	
	Bird Log	Enable	Enable bird log
		Disable	Disable bird log

Dynamic Routing	**Interface**	Disable WAN LAN & WAN Both	Select dynamic route interface
Static Routing	**Select set number**	-	You can set static route number (1-50)
	Router Name	-	Customize the router name, up to 25 characters
	Metric	-	The unit of measure for routing between source and destination address
	Destination LAN NET	-	The destination network address or host address
	Subnet Mask	-	The subnet mask of router
	Gateway	-	The gateway of router
	Interface	LAN & WAN LAN ANY 3G IPSEC	According the position of IP address, you can select suitable interface

Mode 5: Router

Select the **"Router"** mode, this page will auto refresh and then show the configuration parameters as follow:



Advanced Routing

Operating Mode

Operating Mode: Router

Dynamic Routing

Interface: Disable

Static Routing

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

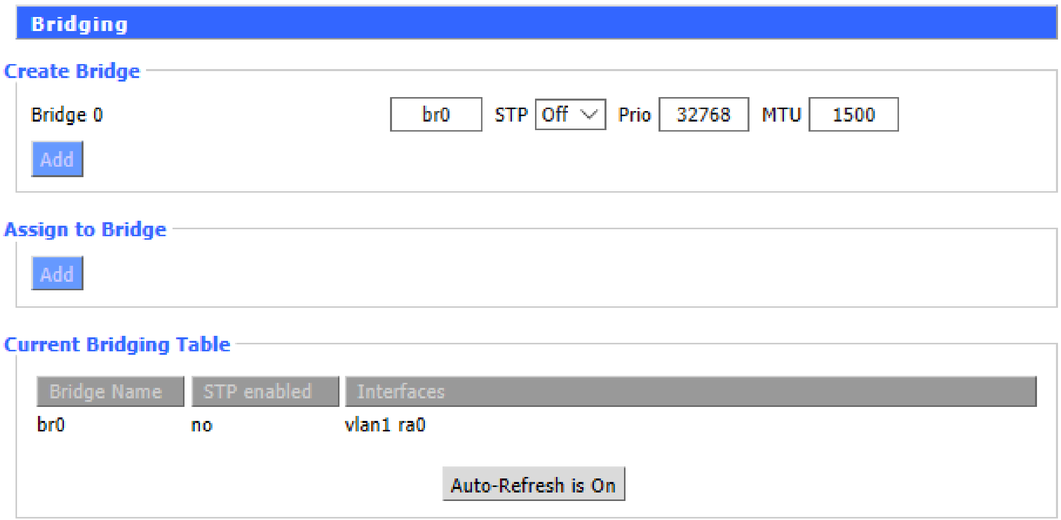
Interface: LAN & WLAN

Delete the specified static route

Show all static route settings

Section	Parameters	Option	Description
Dynamic Routing	**Interface**	Disable WAN LAN & WAN Both	Select dynamic route interface
Static Routing	**Select set number**	-	You can set static route number (1-50)
	Router Name	-	Customize the router name, up to 25 characters
	Metric	-	The unit of measure for routing between source and destination address
	Destination LAN NET	-	The destination network address or host address
	Subnet Mask	-	The subnet mask of router
	Gateway	-	The gateway of router
	Interface	LAN & WAN LAN ANY 3G IPSEC	According the position of IP address, you can select suitable interface

3.3.1.5 Networking

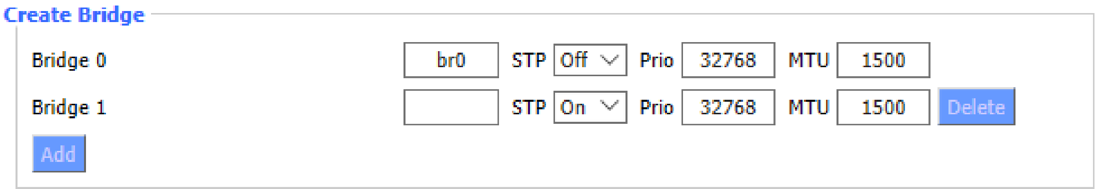


Bridge Name	STP enabled	Interfaces
br0	no	vlan1 ra0

Parameters	Option	Description
Create Bridge	Bridge No.	You can create a new bridge. The smallest number has the highest priority
Assign to Bridge	-	Allow you specify any interface in an established bridge
Current Bridging Table	-	Show all current bridge list

Question: How to create a new bridge?

Step 1. Click the “Add” button to a new bridge on the “Create Bridge”, and it will show bridge parameters as follow:

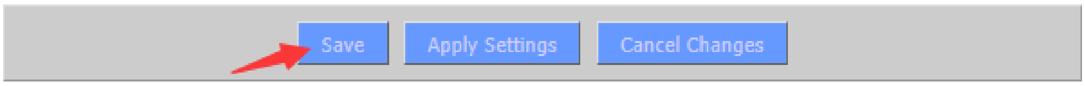


Create Bridge

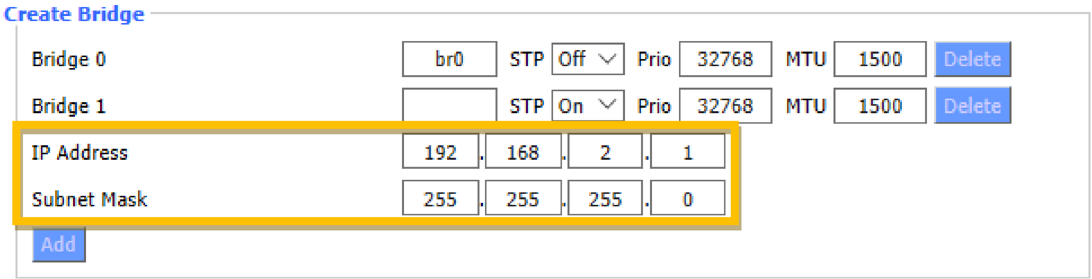
Bridge 0	br0	STP	Off	Prio	32768	MTU	1500	
Bridge 1		STP	On	Prio	32768	MTU	1500	Delete

- br0: the name of bridge
- STP: enable or disable STP
- Prio: The priority of STP. The smaller the number, the highest the level.
- MTU: Maximum transmission unit. Default 1500.

Step 2. Click the “Save” button to save the bridge configuration.



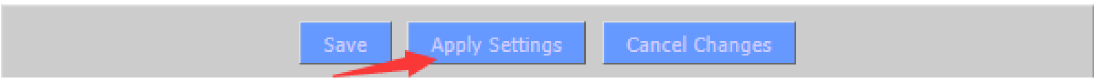
Step 3. And then in the “Create Bridge” section, it will show network configure information as follow: (input the IP address and subnet mask of bridge)



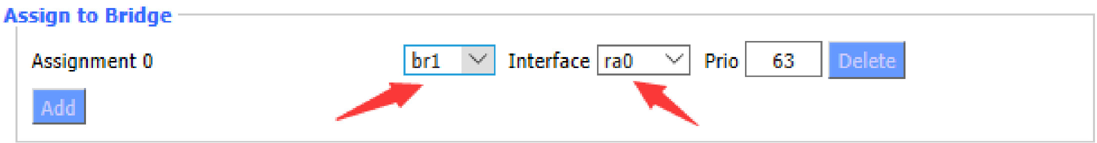
Create Bridge

Bridge 0	br0	STP	Off	Prio	32768	MTU	1500	Delete
Bridge 1		STP	On	Prio	32768	MTU	1500	Delete
IP Address	192	168	2	1				
Subnet Mask	255	255	255	0				

Step 4. Click the “Apply Settings” button to take this bridge effect.



Step 5. Now the bridge was built successfully. You can assign the different interfaces to this bridge, such as you can assign the ra0 interface (wireless) to br1 as follow:

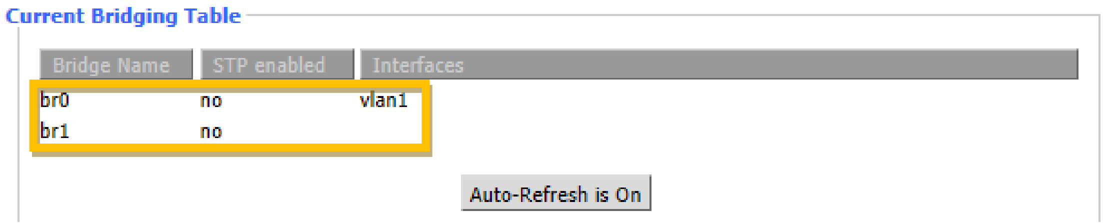


Assign to Bridge

Assignment 0	br1	Interface	ra0	Prio	63	Delete

Notice: the main function of bridge is used for LAN port, the WAN interface should not be bound.

Step 6. If bind successful, it will show on the “Current Bridging Table” as follow:



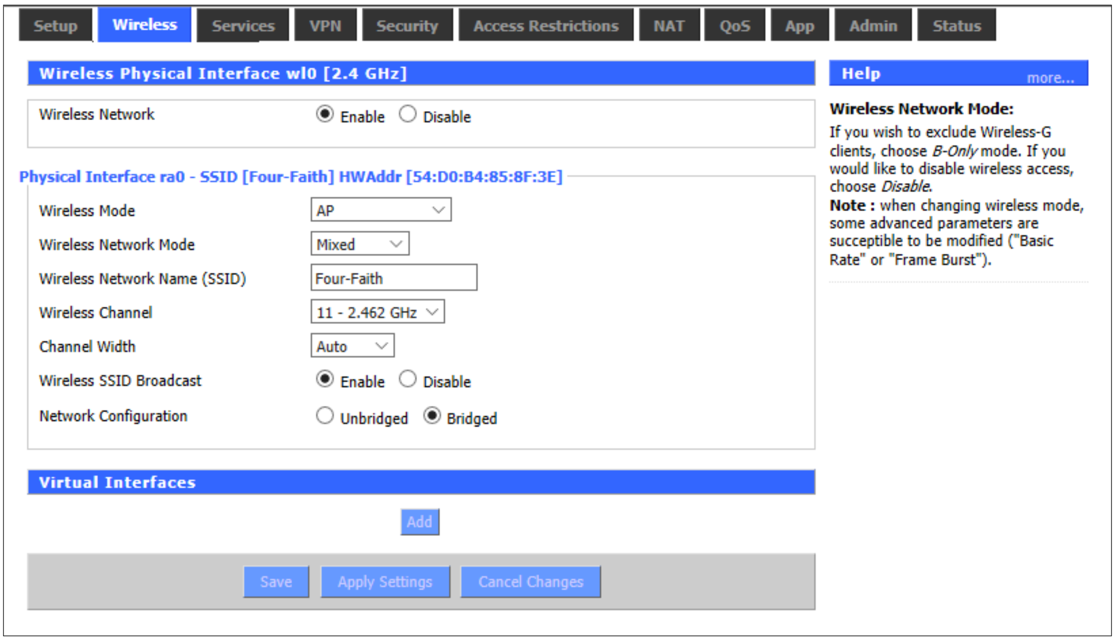
Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan1
br1	no	

3.3.2 Wireless

3.3.2.1 Basic Settings

You can configure WIFI parameters here. WIFI mainly used to upgrade device firmware.



Wireless Physical Interface wl0 [2.4 GHz]

Wireless Network ● Enable ○ Disable

Physical Interface ra0 - SSID [Four-Faith] HWAddr [54:D0:B4:85:8F:3E]

Wireless Mode: AP

Wireless Network Mode: Mixed

Wireless Network Name (SSID): Four-Faith

Wireless Channel: 11 - 2.462 GHz

Channel Width: Auto

Wireless SSID Broadcast ● Enable ○ Disable

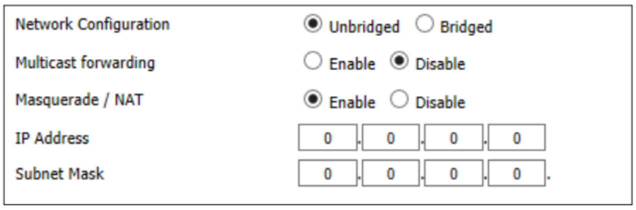
Network Configuration ○ Unbridged ● Bridged

Virtual Interfaces

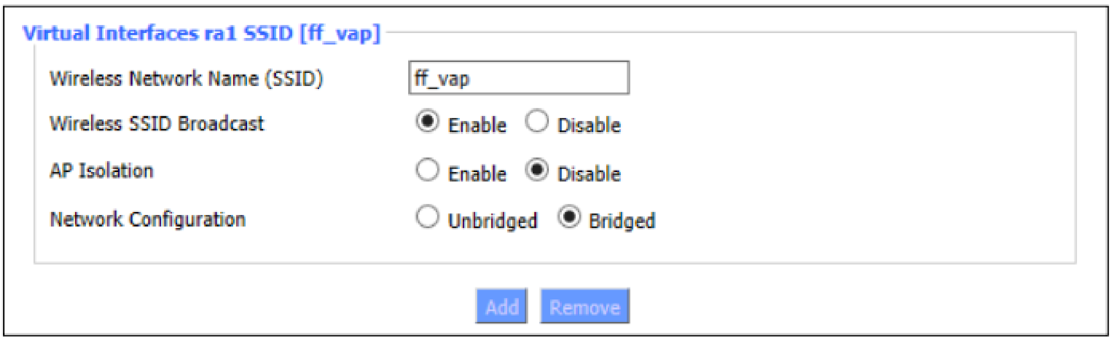
Help more...

Wireless Network Mode:
If you wish to exclude Wireless-G clients, choose *B-Only* mode. If you would like to disable wireless access, choose *Disable*.
Note : when changing wireless mode, some advanced parameters are succeptible to be modified ("Basic Rate" or "Frame Burst").

Parameters	Option	Description
Wireless Network	Enable	Turn on wifi
	Disable	Turn off wifi
Wireless Mode	AP	Convert wired network into wireless signal
	client	Receive wireless signal from other wireless routers and then convert it into wired network. PC only connect it through network cable
	ad-hoc	P2P connection, as virtual AP, and other PC can directly connect and share the network through it
	relay	Relay is a transmission path between two switching centers
	relay bridge	Wireless transmission can bridge the communication between two or more networks
Wireless Network Mode	Hybrid	Support 802.11b/g/n standard devices
	Bg-mix	Support 802.11b and 802.11g standard devices
	NG-mix	Support 802.11g and 802.11n standard devices

	B Only	Only support 802.11b standard devices
	G Only	Only support 802.11g standard devices
	Only N	Only support 802.11n standard devices
Wireless Network Name (SSID)	-	You can edit wireless network name here
Wireless Channel	-	There are 1-13 channels available. In the environment of multiple wireless devices, please try to avoid using the same channels as other devices
Channel Width	-	20MHZ and 40MHZ are available
Wireless SSID Broadcast	Enable	Broadcast SSID
	Disable	Hide SSID
Network Configuration	Bridged	In general, select bridged. The bridge is connected to F8926-GW
	Unbridged	when no bridge is connected to F8926-GW, and the IP address needs to be manually configured:  Network Configuration ● Unbridged ○ Bridged Multicast forwarding ○ Enable ● Disable Masquerade / NAT ● Enable ○ Disable IP Address 0 . 0 . 0 . 0 Subnet Mask 0 . 0 . 0 . 0

Click the “Add” button in “**Virtual Interfaces**” bar to add virtual interface, as fellow:



Virtual Interfaces ra1 SSID [ff_vap]

Wireless Network Name (SSID) ff_vap

Wireless SSID Broadcast ● Enable ○ Disable

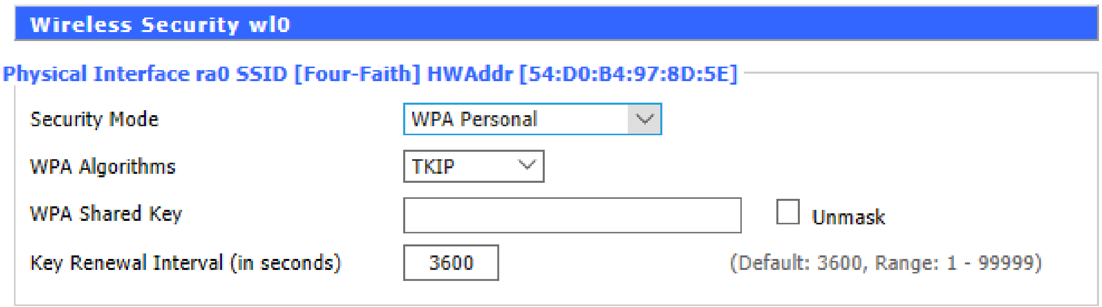
AP Isolation ○ Enable ● Disable

Network Configuration ○ Unbridged ● Bridged

3.3.2.2 Wireless Security

It has 7 wireless security modes. Default disable it. If you want to change the wireless security mode, please click the **“Apply Settings”** button to take it effect.

Mode 1: WPA Personal



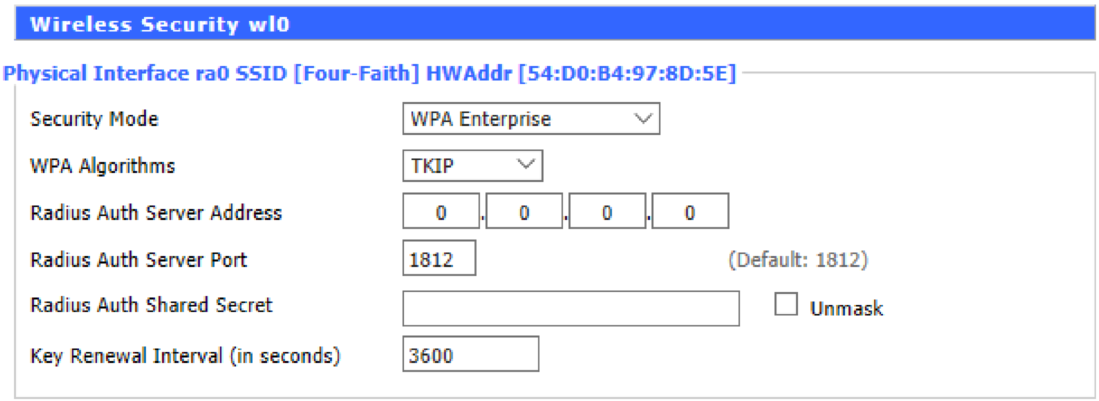
Wireless Security wl0

Physical Interface ra0 SSID [Four-Faith] HWAddr [54:D0:B4:97:8D:5E]

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

Parameters	Option	Description
WPA Algorithms	TKIP	TKIP algorithm, dynamic encryption
	AES	AES algorithm, dynamic encryption
	TKIP+AES	Both TKIP and AES algorithm
WPA Shared Key	-	8-36 characters, combine with letters and numbers
Key Renewal Interval (in seconds)	-	1-99999. Secret key update time interval, default 3600

Mode 2: WPA Enterprise



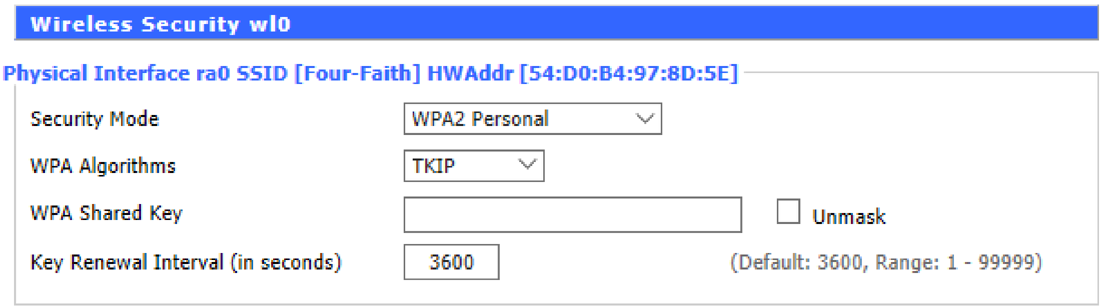
Wireless Security wl0

Physical Interface ra0 SSID [Four-Faith] HWAddr [54:D0:B4:97:8D:5E]

Security Mode	WPA Enterprise	
WPA Algorithms	TKIP	
Radius Auth Server Address	0 . 0 . 0 . 0	
Radius Auth Server Port	1812	(Default: 1812)
Radius Auth Shared Secret		□ Unmask
Key Renewal Interval (in seconds)	3600	

Parameters	Option	Description
WPA Algorithms	TKIP	TKIP algorithm, dynamic encryption
	AES	AES algorithm, dynamic encryption
	TKIP+AES	Both TKIP and AES algorithm
Radius Auth Server Address	-	Input the IP address of radius server
Radius Auth Server Port		Input the network port of radius server
Radius Auth Shared Secret		Shared secret key between router and radius server
Key Renewal Interval (in seconds)	-	1-99999. Secret key update time interval, default 3600

Mode 3: WPA2 Personal



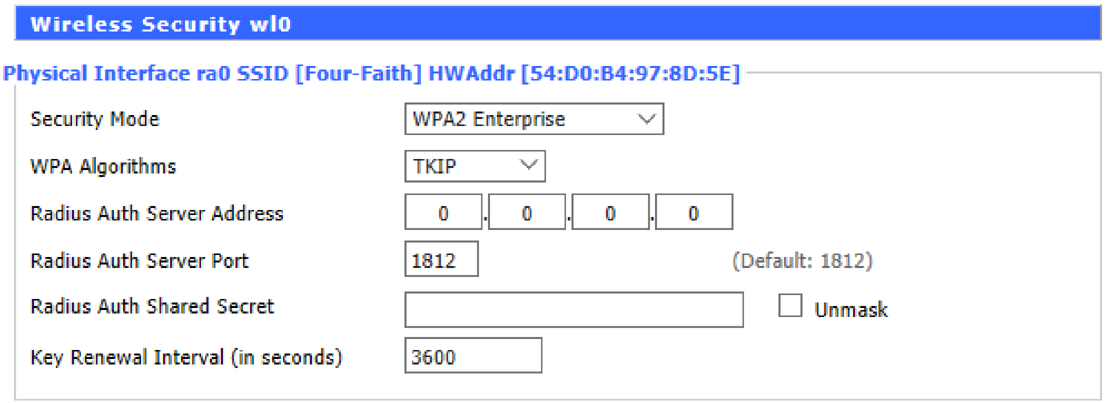
Wireless Security wl0

Physical Interface ra0 SSID [Four-Faith] HWAddr [54:D0:B4:97:8D:5E]

Security Mode	WPA2 Personal	
WPA Algorithms	TKIP	
WPA Shared Key		□ Unmask
Key Renewal Interval (in seconds)	3600	(Default: 3600, Range: 1 - 99999)

Parameters	Option	Description
WPA Algorithms	TKIP	TKIP algorithm, dynamic encryption
	AES	AES algorithm, dynamic encryption
	TKIP+AES	Both TKIP and AES algorithm
WPA Shared Key	-	8-36 characters, combine with letters and numbers
Key Renewal Interval (in seconds)	-	1-99999. Secret key update time interval, default 3600

Mode 4: WPA2 Enterprise



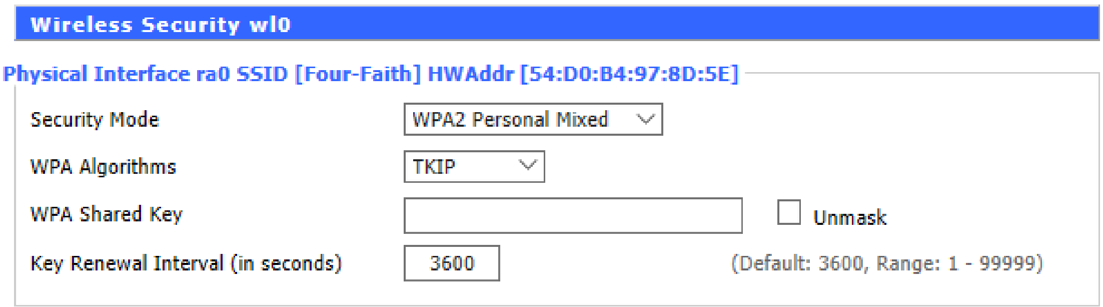
Wireless Security wl0

Physical Interface ra0 SSID [Four-Faith] HWAddr [54:D0:B4:97:8D:5E]

Security Mode	WPA2 Enterprise	
WPA Algorithms	TKIP	
Radius Auth Server Address	0 . 0 . 0 . 0	
Radius Auth Server Port	1812	(Default: 1812)
Radius Auth Shared Secret		□ Unmask
Key Renewal Interval (in seconds)	3600	

Parameters	Option	Description
WPA Algorithms	TKIP	TKIP algorithm, dynamic encryption
	AES	AES algorithm, dynamic encryption
	TKIP+AES	Both TKIP and AES algorithm
Radius Auth Server Address	-	Input the IP address of radius server
Radius Auth Server Port		Input the network port of radius server
Radius Auth Shared Secret		Shared secret key between router and radius server
Key Renewal Interval (in seconds)	-	1-99999. Secret key update time interval, default 3600

Mode 5: WPA2 Personal Mixed



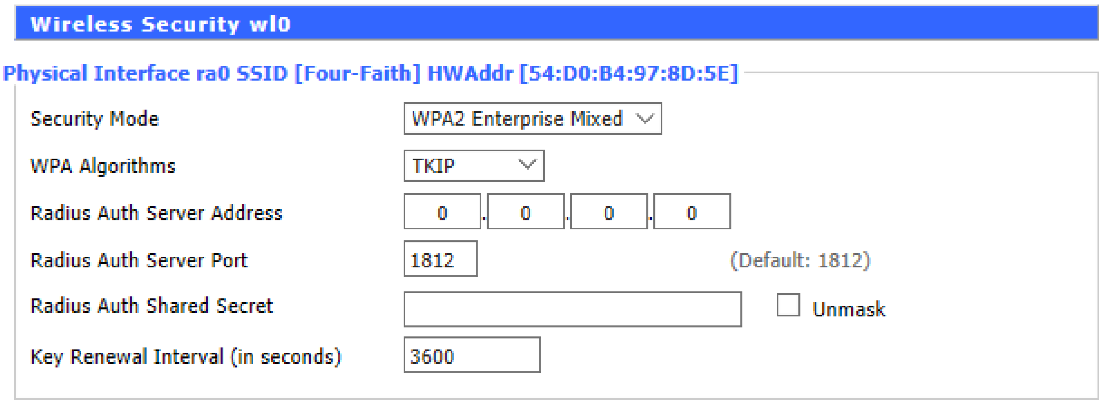
Wireless Security wl0

Physical Interface ra0 SSID [Four-Faith] HWAddr [54:D0:B4:97:8D:5E]

Security Mode	WPA2 Personal Mixed	
WPA Algorithms	TKIP	
WPA Shared Key		□ Unmask
Key Renewal Interval (in seconds)	3600	(Default: 3600, Range: 1 - 99999)

Parameters	Option	Description
WPA Algorithms	TKIP	TKIP algorithm, dynamic encryption
	AES	AES algorithm, dynamic encryption
	TKIP+AES	Both TKIP and AES algorithm
WPA Shared Key	-	8-36 characters, combine with letters and numbers
Key Renewal Interval (in seconds)	-	1-99999. Secret key update time interval, default 3600

Mode 6: WPA2 Enterprise Mixed



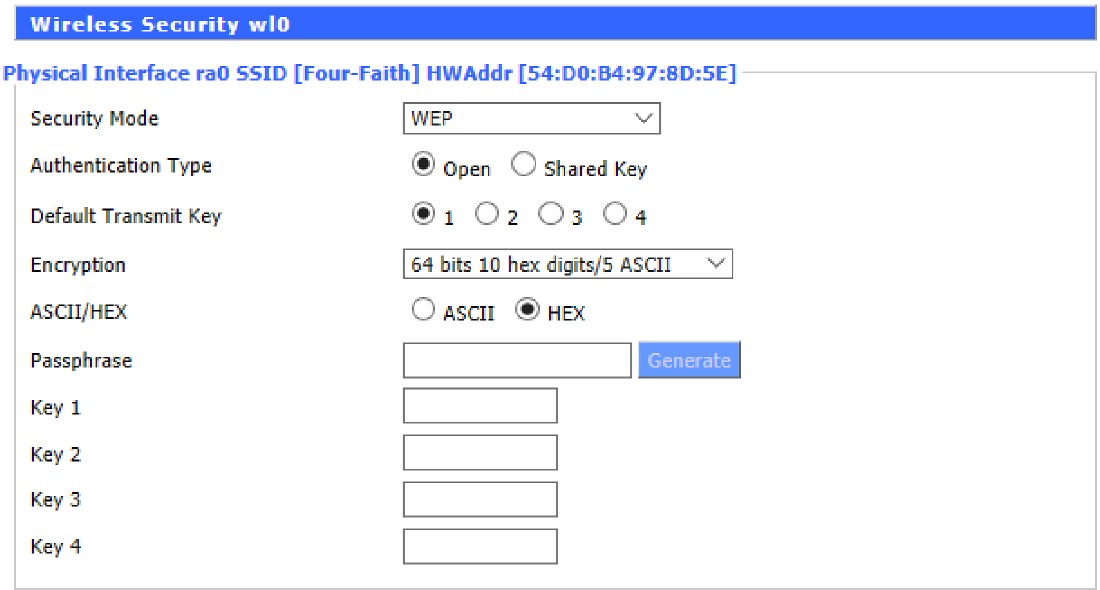
Wireless Security wl0

Physical Interface ra0 SSID [Four-Faith] HWAddr [54:D0:B4:97:8D:5E]

Security Mode	WPA2 Enterprise Mixed	
WPA Algorithms	TKIP	
Radius Auth Server Address	0 . 0 . 0 . 0	
Radius Auth Server Port	1812	(Default: 1812)
Radius Auth Shared Secret		□ Unmask
Key Renewal Interval (in seconds)	3600	

Parameters	Option	Description
WPA Algorithms	TKIP	TKIP algorithm, dynamic encryption
	AES	AES algorithm, dynamic encryption
	TKIP+AES	Both TKIP and AES algorithm
Radius Auth Server Address	-	Input the IP address of radius server
Radius Auth Server Port		Input the network port of radius server
Radius Auth Shared Secret		Shared secret key between router and radius server
Key Renewal Interval (in seconds)	-	1-99999. Secret key update time interval, default 3600

Mode 7: WEP



Wireless Security wl0

Physical Interface ra0 SSID [Four-Faith] HWAddr [54:D0:B4:97:8D:5E]

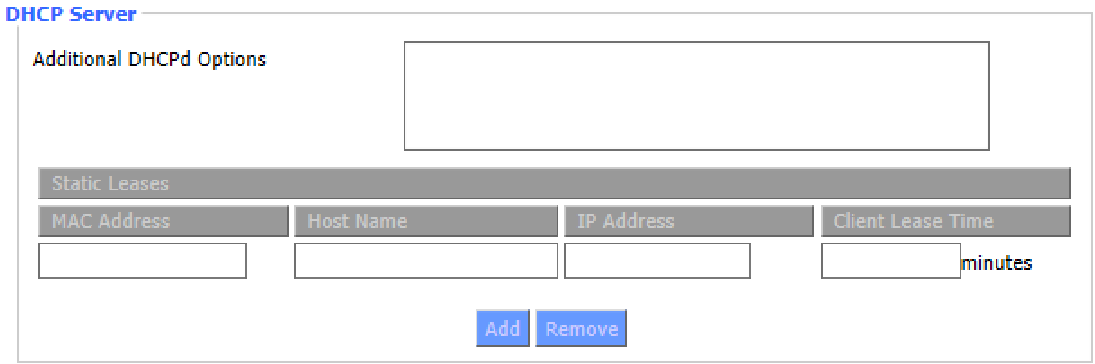
Security Mode	WEP
Authentication Type	● Open ○ Shared Key
Default Transmit Key	● 1 ○ 2 ○ 3 ○ 4
Encryption	64 bits 10 hex digits/5 ASCII
ASCII/HEX	○ ASCII ● HEX
Passphrase	Generate
Key 1	
Key 2	
Key 3	
Key 4	

Parameters	Option	Description
Authentication Type	Open	Open secret key
	Shard Key	Shared secret key
Default Transmit Key	1	You can select one of the keys as the transport encryption key
	2	
	3	
	4	
Encryption	64 bits 10 hex digits / 5 ASCII	Every secret key is 10-bits hex characters or 5-bits ASCII characters
	128 bits 26 hex digits / 13 ASCII	Every secret key is 26-bits Dec characters or 5-bits ASCII characters
ASCII / HEX	ASCII	Secret key is ASCII code
	HEX	Secret key is HEX code
Passphrase	-	Generate the secret key. Combine with letters and characters
Key 1	-	Secret key 1
Key 2	-	Secret key 2
Key 3	-	Secret key 3
Key 4	-	Secret key 4

3.3.3 Services

◆ DHCP Server

DHCP service is assign IP address to your local devices. You can enter into this menu and then configure it.



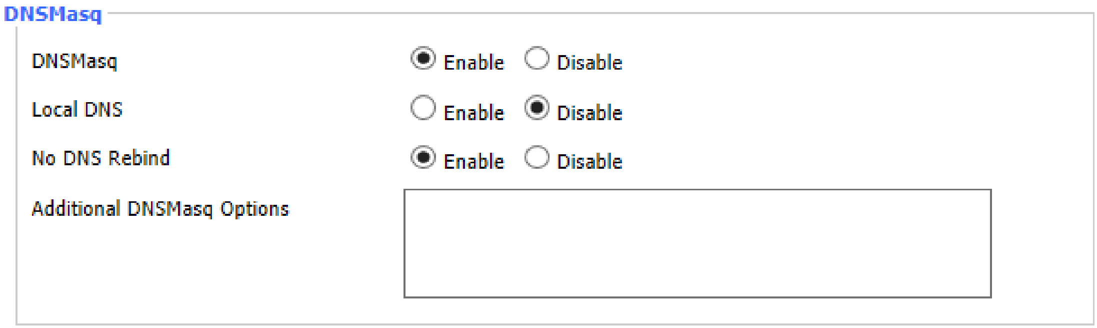
DHCP Server

Additional DHCPd Options

Static Leases			
MAC Address	Host Name	IP Address	Client Lease Time
			minutes

◆ DNSMasq

DNSMasq is local DNS server. It will resolve all hosts which the names of DNS entries forwarded and cached from the DHCP routers and the remote DNS server.



DNSMasq

DNSMasq ● Enable ○ Disable

Local DNS ○ Enable ● Disable

No DNS Rebind ● Enable ○ Disable

Additional DNSMasq Options

Parameters	Option	Description
DNSMasq	Enable	Turn on this service
	Disable	Turn off this service
Local DNS	Enable	Enable local DNS service
	Disable	Disable it
No DNS Rebind	Enable	It is a security method, can prevent attacker to access the web interface of router
	Disable	Disable it

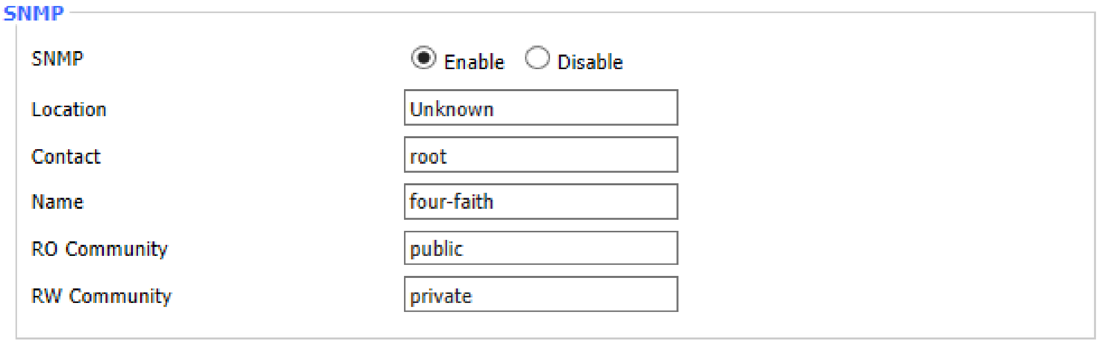
Additional DNSMasq Options	-	You can set extra options, such as:
		dhcp-host = AB:CD:EF:11:22:33, 192.168.0.10, myhost, myhost.domain, 12h;
		dhcp-lease-max = 2;
		dhcp-range = 192.168.0.110, 192.168.0.111, 12h

◆ SNMP

SNMP (Simple Network Management Protocol) is a widely used network management protocol.

SNMP Agent can monitor current network status by collecting hardware or software process information of network devices (such as concentrator, router and so on).

MIB is a data structure can be used to define some options from devices.



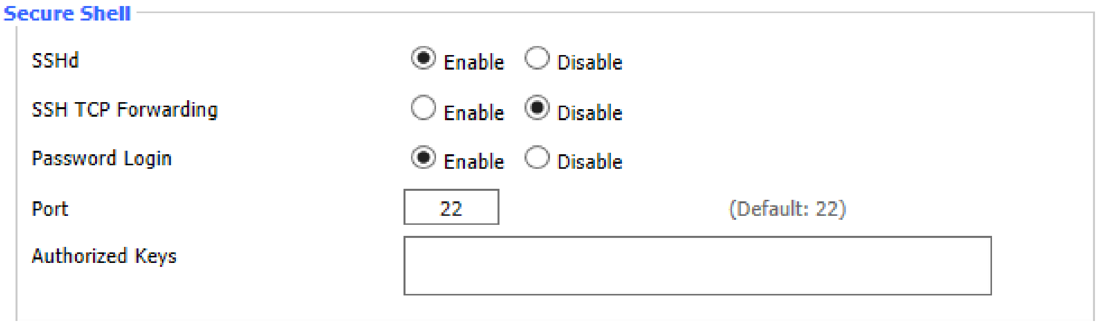
SNMP

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

Parameters	Option	Description
SNMP	Enable	Turn on this service
	Disable	Turn off this service
Location	-	User defined. The identification of the location of the device
Contact	-	User defined. It should be consistent with client
Name	-	User defined. It should be consistent with client
RO Community	-	User defined. It should be consistent with client, read only permission
RW Community	-	User defined. It should be consistent with client, read and write permission

◆ SSHD

You can remote access your router by SSH client when you are enable the SSHD service.



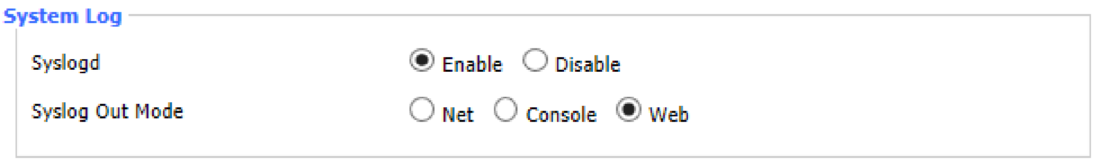
Secure Shell

SSHd	● Enable ○ Disable
SSH TCP Forwarding	○ Enable ● Disable
Password Login	● Enable ○ Disable
Port	22 (Default: 22)
Authorized Keys	

Parameters	Option	Description
SSHD	Enable	Turn on this service
	Disable	Turn off this service

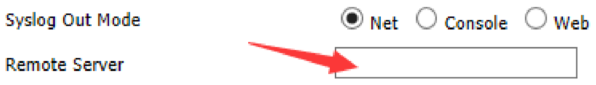
SSH TCP Forwarding	Enable	Support TCP forwarding function
	Disable	Disable TCP forwarding function
Password Login	Enable	Login with password
	Disable	Login without password
Port	-	Setting SSHD port, default 22
Authorized Keys	-	Use the system user name and password by default

- **System Log**


System Log

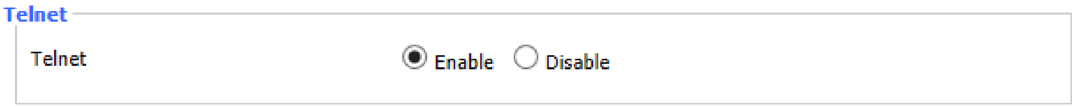
Syslogd ● Enable ○ Disable

Syslog Out Mode ○ Net ○ Console ● Web

Parameters	Option	Description
Syslogd	Enable	Turn on this service
	Disable	Turn off this service
Syslog Out Mode	Net	Log out by network, you need fill in the IP address of remote server  Syslog Out Mode ● Net ○ Console ○ Web Remote Server
	Console	Log out by console
	Web	Log out by web GUI

- **Telnet**

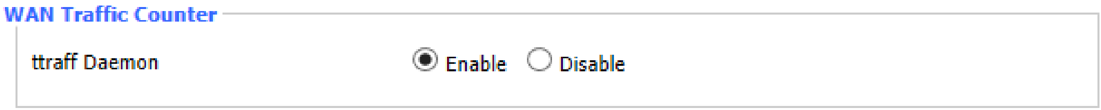
Telnet is a terminal simulation protocol that usually used to network which based on TCP/IP. It can log in remote device and run the program by PC.


Telnet

Telnet ● Enable ○ Disable

- **WAN Traffic Counter**

Traffic statistics function.

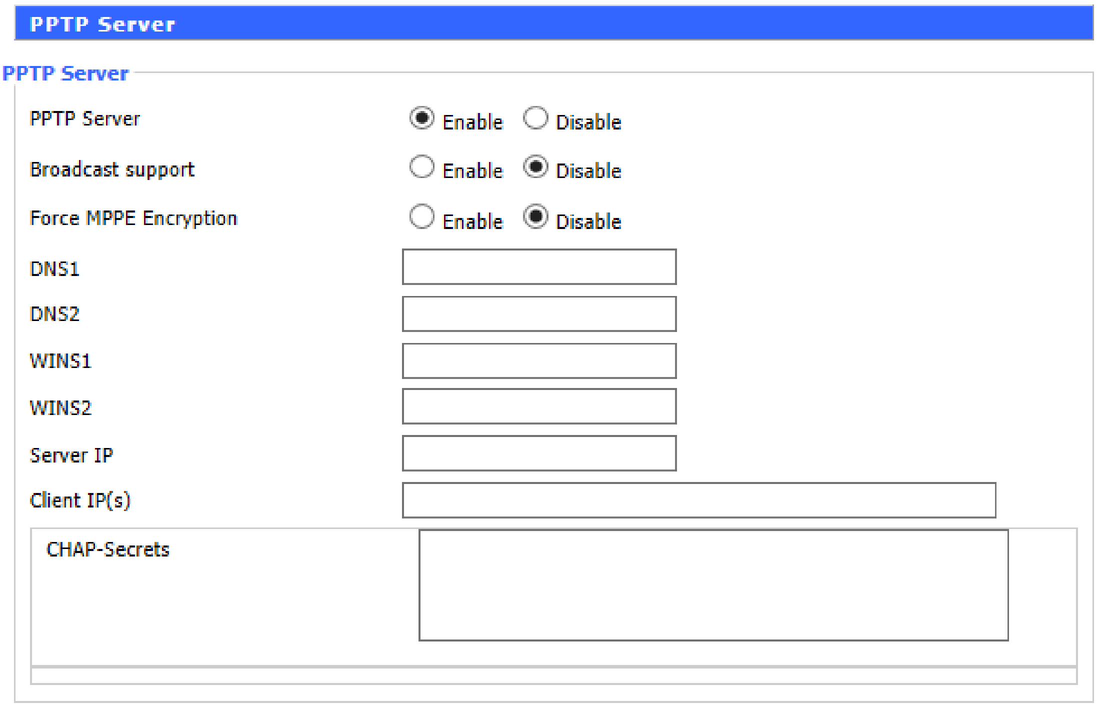

WAN Traffic Counter

ttraff Daemon ● Enable ○ Disable

3.3.4 VPN

3.3.4.1 PPTP

◆ **PPTP Server**



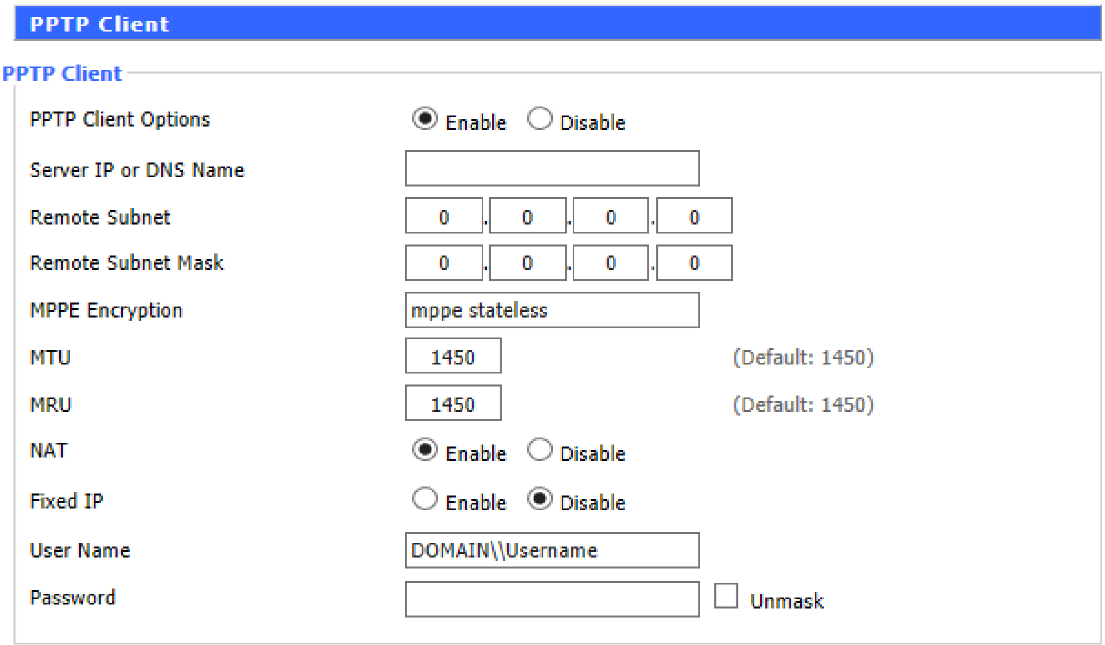
PPTP Server

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	

Parameters	Option	Description
PPTP Server	Enable	Turn on PPTP server
	Disable	Turn off PPTP server
Broadcast support	Enable	PPTP server support broadcast function
	Disable	PPTP server non-support broadcast function
Force MPPE Encryption	Enable	Force data MPPE encryption of PPTP server
	Disable	Disable MPPE encryption function
DNS1	-	First DNS
DNS2	-	Second DNS
WINS1	-	First WINS
WINS2	-	Second WINS
Sever IP	-	Input the router’s IP address as the address of PPTP server. It should not be the same as the LAN port
Client IP(s)	-	The IP address assigned to the client. Format is: xxx.xxx.xxx.xxx-xxx
CHAP-Secrets	-	The client’s username and password. Format is: user * password *

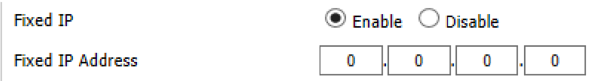
◆ PPTP Client



PPTP Client

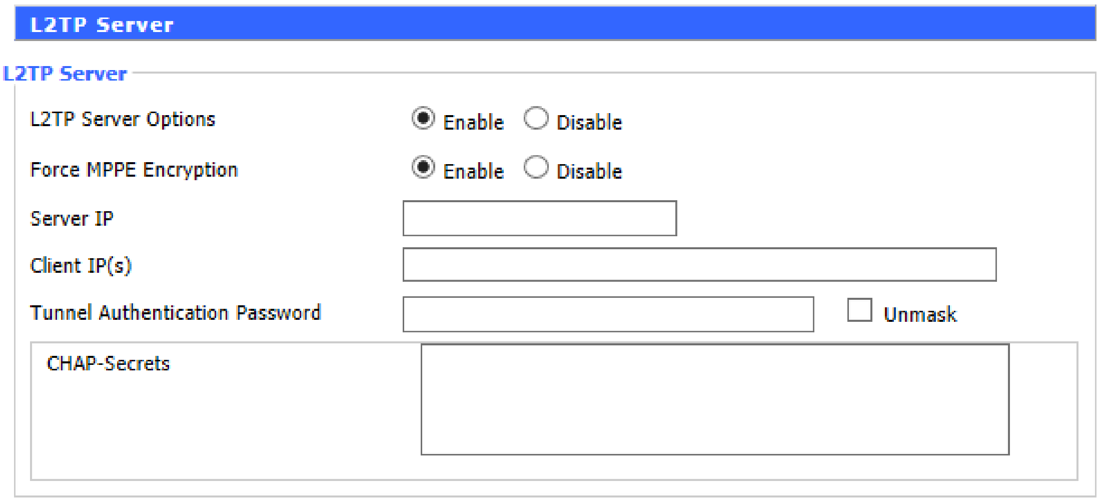
PPTP Client

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 stateless	
MTU	1450	(Default: 1450)
MRU	1450	(Default: 1450)
NAT	● Enable ○ Disable	
Fixed IP	○ Enable ● Disable	
User Name	DOMAIN\\Username	
Password		□ Unmask

Parameters	Option	Description
PPTP Client Options	Enable	Turn on PPTP client
	Disable	Turn off PPTP client
Server IP or DNS Name	-	The IP address or DNS name of PPTP server
Remote Subnet	Enable	The subnet of PPTP server
Remote Subnet Mask	-	The subnet mask of PPTP server
MPPE Encryption	-	Support MPPE encryption or not
MTU	-	The maximum transmission unit. Range: 0-1500
MRU	-	The maximum receive unit. Range: 0-1500
NAT	Enable	Turn on network address translation function
	Disable	Turn off network address translation function
Fixed IP	Enable	You need input fixed IP address.  Fixed IP ● Enable ○ Disable Fixed IP Address 0 . 0 . 0 . 0
	Disable	Dynamic assign IP address
User Name	-	The allowed username of PPTP server
Password		The corresponding password of PPTP server

3.3.4.2 L2TP

◆ **L2TP Server**



L2TP Server

L2TP Server

L2TP Server Options ● Enable ○ Disable

Force MPPE Encryption ● Enable ○ Disable

Server IP

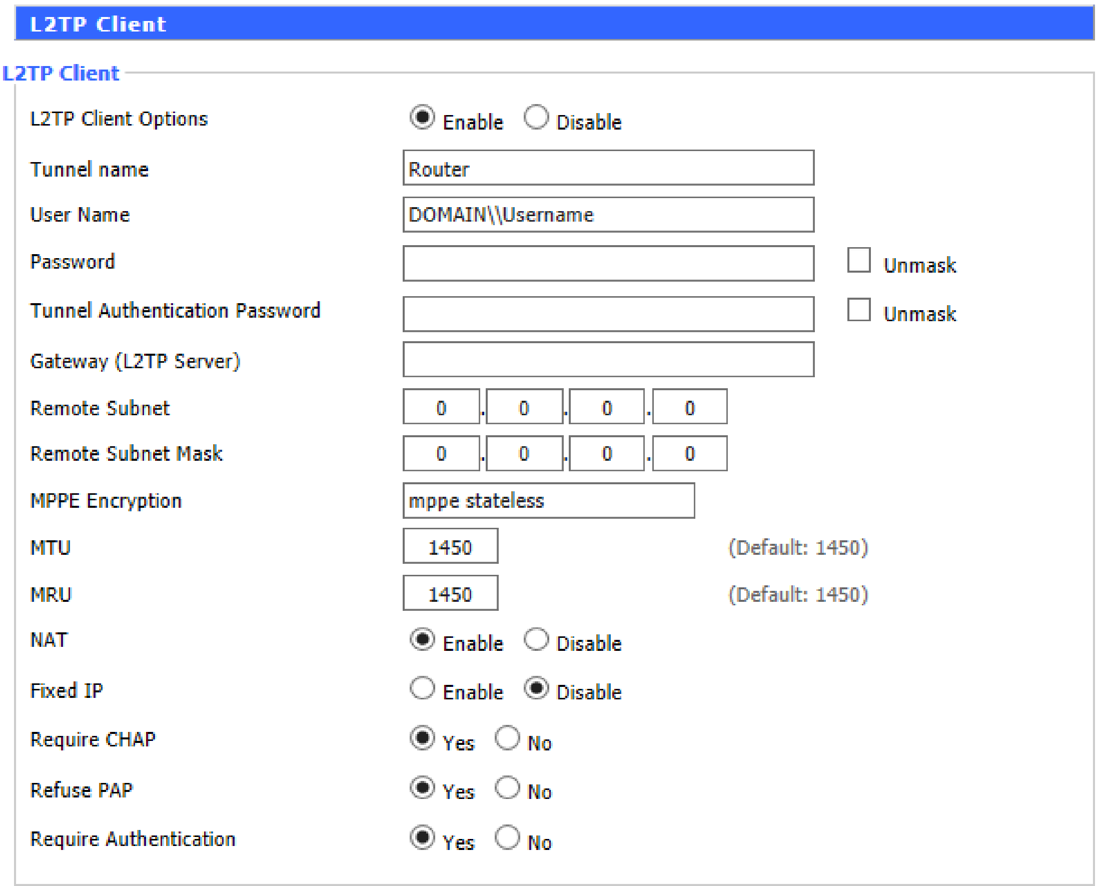
Client IP(s)

Tunnel Authentication Password □ Unmask

CHAP-Secrets

Parameters	Option	Description
L2TP Server Options	Enable	Turn on L2TP server
	Disable	Turn off L2TP server
Force MPPE Encryption	Enable	Force data MPPE encryption of L2TP server
	Disable	Disable MPPE encryption function
Sever IP	-	Input the router’s IP address as the address of L2TP server. It should not be the same as the LAN port
Client IP(s)	-	The IP address assigned to the client. Format is: xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx
Tunnel Authentication Password	-	The tunnel authentication key
CHAP-Secrets	-	The client’s username and password. Format is: user * password *

◆ **L2TP Client**

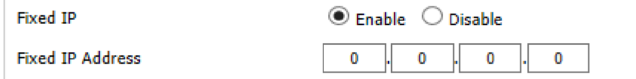


L2TP Client

L2TP Client

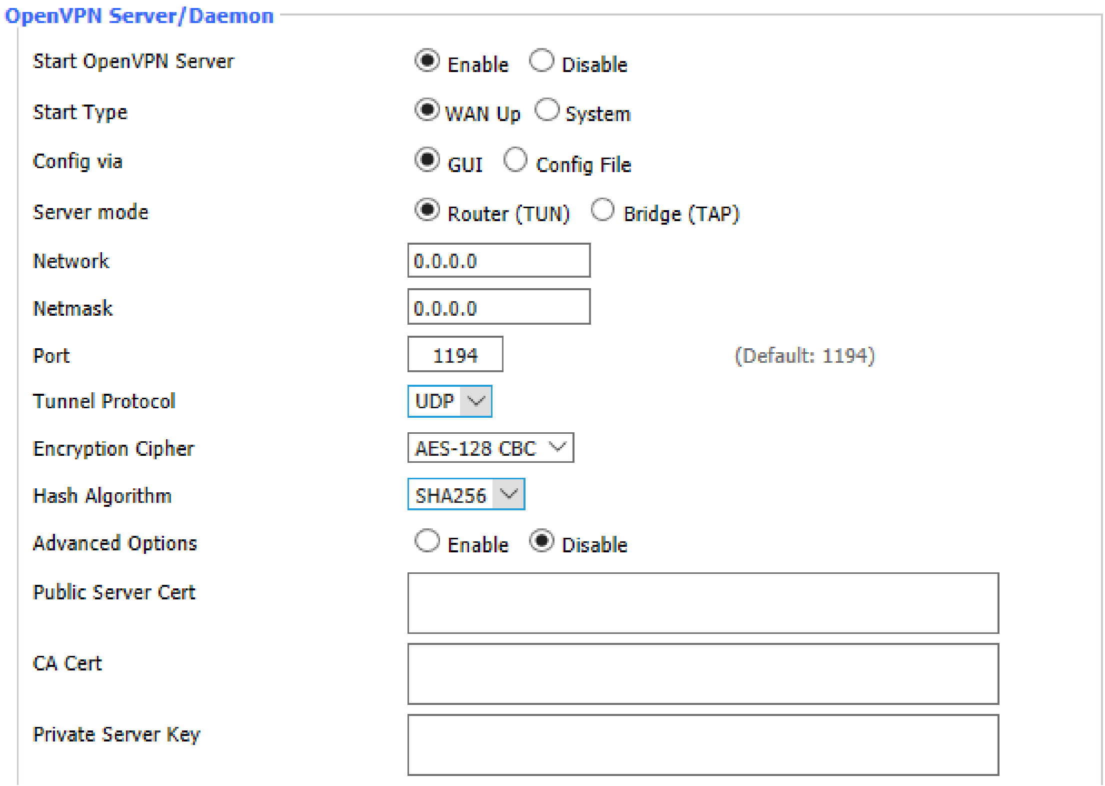
L2TP Client Options	● Enable ○ Disable	
Tunnel name	Router	
User Name	DOMAIN\\Username	
Password		□ Unmask
Tunnel Authentication Password		□ Unmask
Gateway (L2TP Server)		
Remote Subnet	0 . 0 . 0 . 0	
Remote Subnet Mask	0 . 0 . 0 . 0	
MPPE Encryption	mppe stateless	
MTU	1450	(Default: 1450)
MRU	1450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

Parameters	Option	Description
L2TP Client Options	Enable	Turn on L2TP client
	Disable	Turn off L2TP client
Tunnel Name	-	The allowed tunnel name of L2TP server
User Name	-	The allowed username of L2TP server
Password	-	The corresponding password of L2TP server
Tunnel Authentication Password	-	The allowed tunnel authentication password of L2TP server
Gateway (L2TP Server)	-	The IP address or DNS name of L2TP server
Remote Subnet	Enable	The subnet of L2TP server
Remote Subnet Mask	-	The subnet mask of L2TP server
MPPE Encryption	-	Support MPPE encryption or not
MTU	-	The maximum transmission unit. Range: 0-1500
MRU	-	The maximum receive unit. Range: 0-1500
NAT	Enable	Turn on network address translation function
	Disable	Turn off network address translation function
Fixed IP	Enable	You need input fixed IP address.

		 Fixed IP ● Enable ○ Disable Fixed IP Address 0 . 0 . 0 . 0
	Disable	Dynamic assign IP address
Require CHAP	Yes	Require CHAP encryption authentication
	No	Not require CHAP encryption authentication
Refuse PAP	Yes	Refuse PAP encryption authentication
	No	Not refuse PAP encryption authentication
Require Authenticaiton	Yes	Require authentication
	No	Not require authentication

3.3.4.3 OPENVPN

- **OpenVPN Server**



OpenVPN Server/Daemon

Start OpenVPN Server ● Enable ○ Disable

Start Type ● WAN Up ○ System

Config via ● GUI ○ Config File

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

Network 0.0.0.0

Netmask 0.0.0.0

Port 1194 (Default: 1194)

Tunnel Protocol UDP

Encryption Cipher AES-128 CBC

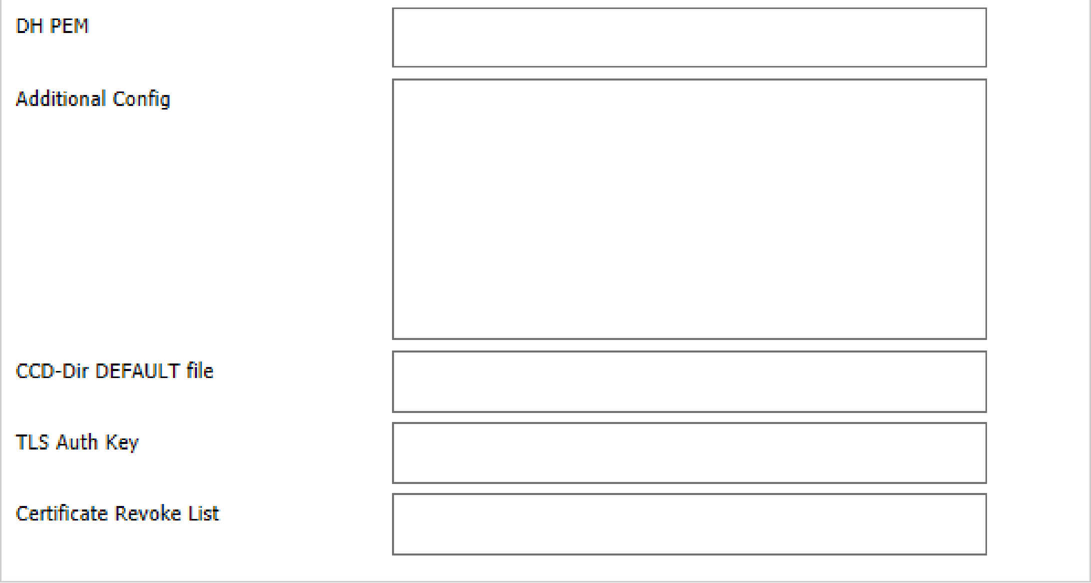
Hash Algorithm SHA256

Advanced Options ○ Enable ● Disable

Public Server Cert

CA Cert

Private Server Key



DH PEM

Additional Config

CCD-Dir DEFAULT file

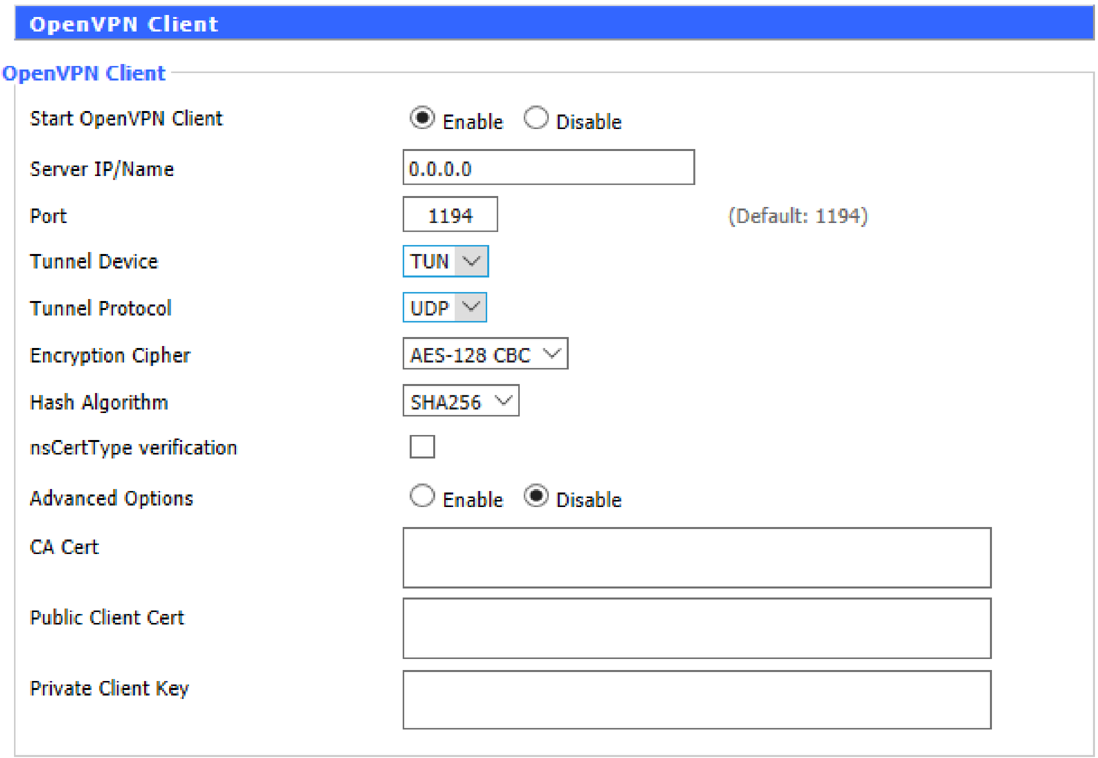
TLS Auth Key

Certificate Revoke List

Parameters	Option	Description
Start OpenVPN Server	Enable	Turn on OpenVPN Server
	Disable	Turn off OpenVPN Server
Start Type	WAN Up	Start it after online
	System	Start it when boot up
Config via	GUI	Configure it by GUI
	Config File	Configure it by config file
Server mode	Router (TUN)	Router mode
	Bridge (TAP)	Bridge mode
Network	-	The allowed network address by OpenVPN server
Netmask	-	The allowed netmask by OpenVPN server
Port	-	The listening port of OpenVPN server
Tunnel Protocol	UDP	UDP protocol
	TCP	TCP protocol
Encryption Cipher	Blowfish CBC	Blowfish encryption
	AES-128 CBC	AES-128 encryption
	AES-192 CBC	AES-192 encryption
	AES-256 CBC	AES-256 encryption
	AES-512 CBC	AES-512 encryption
Hash Algorithm	SHA1	SHA1 algorithm
	SHA256	SHA256 algorithm
	SHA512	SHA512 algorithm
	MD5	MD5 algorithm
Advanced Options	Enable	Advanced options configuration
	Disable	Disable advanced options configuration
CA Cert	-	A common CA certificate for both the server and client

Public Server Cert	-	The cert of OpenVPN server
Private Server Key	-	The key set by OpenVPN server
DH PEM	-	The PEM certification of server
Additional Config	-	Additional server configuration
CCD-Dir DEFAULT file	-	Another file path
TLS Auth Key	-	The authentication key of secure transport layer
Certificate Revoke List	-	Configure a list of revoke certificates

◆ OpenVPN Client



OpenVPN Client

OpenVPN Client

Start OpenVPN Client ● Enable ○ Disable

Server IP/Name 0.0.0.0

Port 1194 (Default: 1194)

Tunnel Device TUN

Tunnel Protocol UDP

Encryption Cipher AES-128 CBC

Hash Algorithm SHA256

nsCertType verification □

Advanced Options ○ Enable ● Disable

CA Cert

Public Client Cert

Private Client Key

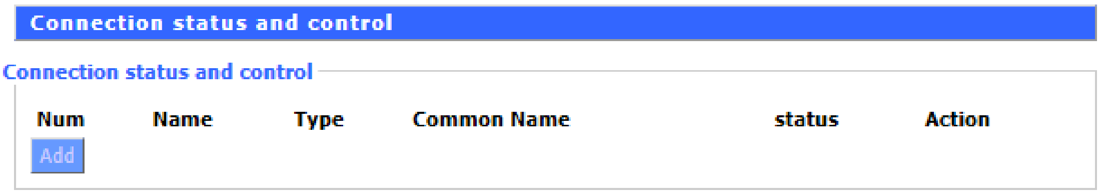
Parameters	Option	Description
Start OpenVPN Client	Enable	Turn on OpenVPN Server
	Disable	Turn off OpenVPN Server
Server IP / Name	WAN Up	Start it after online
Port	-	The listening port of OpenVPN server
Tunnel Device	TUN	Router mode
	TAP	Bridge mode
Tunnel Protocol	UDP	UDP protocol
	TCP	TCP protocol
Encryption Cipher	Blowfish CBC	Blowfish encryption
	AES-128 CBC	AES-128 encryption
	AES-192 CBC	AES-192 encryption
	AES-256 CBC	AES-256 encryption

	AES-512 CBC	AES-512 encryption
Hash Algorithm	SHA1	SHA1 algorithm
	SHA256	SHA256 algorithm
	SHA512	SHA512 algorithm
	MD5	MD5 algorithm
nsCertType verification	Enable	Support nsCertType verification
	Disable	Non-support nsCertType verification
Advanced Options	Enable	Advanced options configuration
	Disable	Disable advanced options configuration
CA Cert	-	A common CA certificate for both the server and client
Public Server Cert	-	The cert of OpenVPN client
Private Server Key	-	The key set by OpenVPN client

3.3.4.4 IPSEC

◆ **Connection status and control**

In the page of IPSEC, it shows the current IPSEC connection and its status of device.



Connection status and control

Connection status and control

Num	Name	Type	Common Name	status	Action

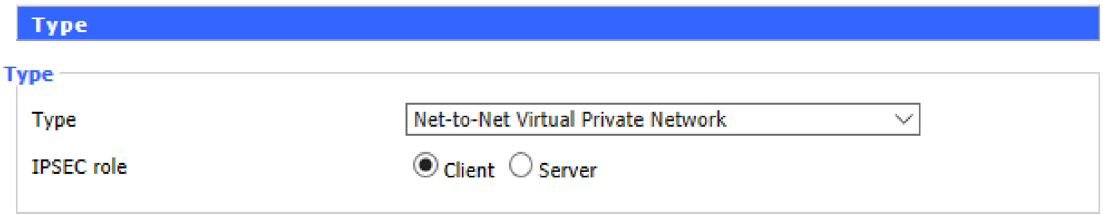
Parameters	Option	Description
Num	-	The number of IPSEC
Name	-	The name of IPSEC
Type	-	The type of IPSEC
Common Name	-	The common name of current connection
Status	Close	The connection does not make a request to the opposite
	Communicate	The connection has been requested to the opposite and is in the process of negotiation. The connection has not been established yet
	Establish	The connection has been established and the tunnel is available
Action	Delete	It will delete the connection
	Edit	Modify the configuration information for this connection
	Reconnect	Delete the current tunnel and restart the tunnel creation request
	Enable	The connection will initiate the tunnel establishment request when reboot or reconnect

		the system.

And, if click the **"Add"** button, it will warn you to create a new IPSEC connection.

◆ Add IPSEC connection or edit IPSEC connection

1. Type: Select mode and functions of IPSEC in this section, now it supports client of tunnel function, server of tunnel function and transport mode.



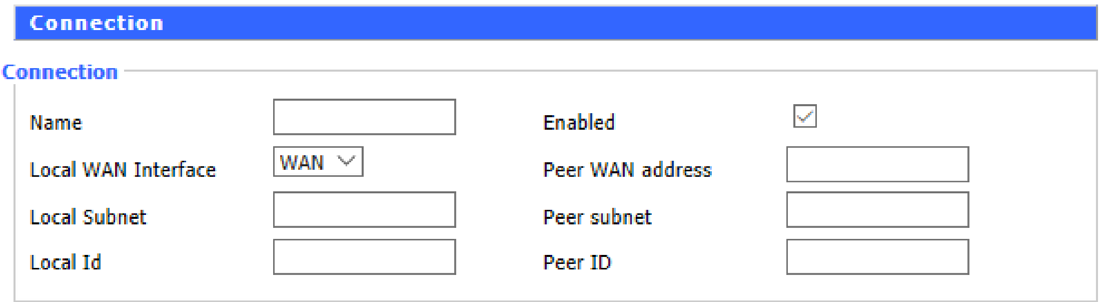
Type

Type

Type: Net-to-Net Virtual Private Network

IPSEC role: ● Client ○ Server

2. Connection: It contains basic address information of tunnel.



Connection

Connection

Name:

Enabled: ☑

Local WAN Interface: WAN

Peer WAN address:

Local Subnet:

Peer subnet:

Local Id:

Peer ID:

Name - The name used to identify the connection.

Enable - It will initiate the connection request when reboot or reconnection system;

Local WAN Interface - Local WAN IP address.

Local Subnet - The subnet mask of local device, such as 192.168.1.0/24, this option can be not fill in if in the transport mode.

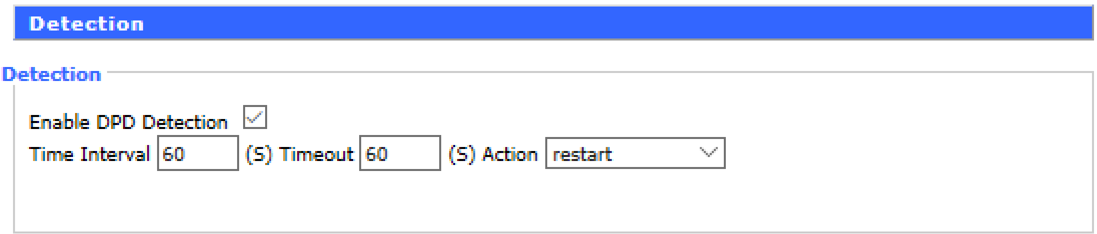
Local Id - Local identify. It can be IP address or domain name.

Peer WAN Address - The IP address of remote device. This option is not available if the tunnel mode of server is used.

Peer Subnet – The subnet mask of remote device, such as 192.168.1.0/24, this option can be not fill in if in the transport mode.

Peer Id - Remote device identify. It can be IP address or domain name.

3. Detection: The configuration information for connection detection (DPD).



Detection

Detection

Enable DPD Detection ☑

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

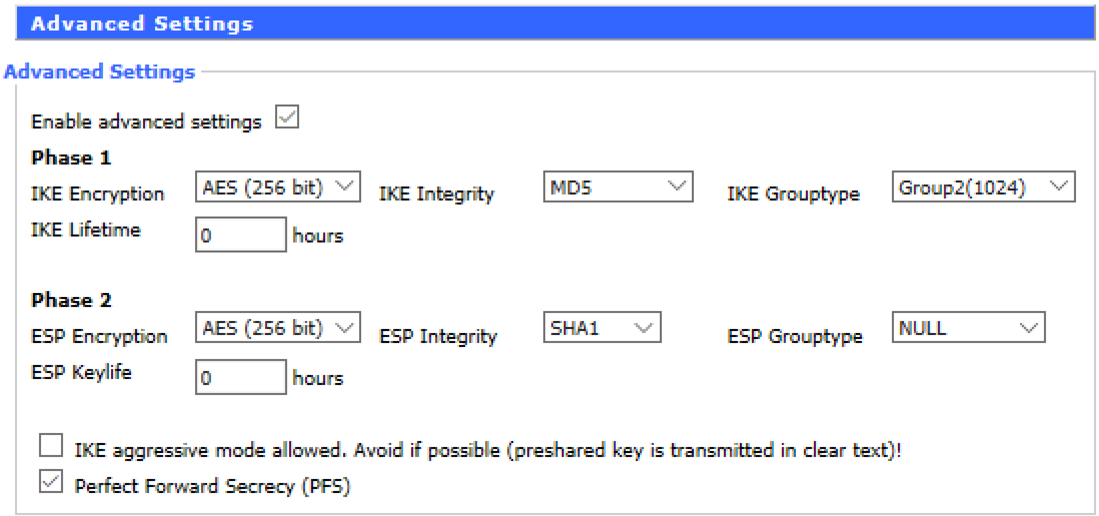
Enable DPD Detection: Whether enable this function or not, check it means enable it.

Time Interval: Set the time interval of DPD.

Timeout: Set the timeout of DPD.

Action: Set the operate mode of DPD.

4. Advanced Settings: It includes IKE, ESP and negotiation mode configuration.



Advanced Settings

Advanced Settings

Enable advanced settings ☑

Phase 1

IKE Encryption: AES (256 bit) IKE Integrity: MD5 IKE Grouptype: Group2(1024)

IKE Lifetime: 0 hours

Phase 2

ESP Encryption: AES (256 bit) ESP Integrity: SHA1 ESP Grouptype: NULL

ESP Keylife: 0 hours

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

☑ Perfect Forward Secrecy (PFS)

Enable advanced settings: Whether enable this function or not, check it means enable it.

IKE Encryption: The encryption type of IKE.

IKE Integrity: The integrity of IKE.

IKE Grouptype: The grouptype of IKE.

IKE Lifetime: The lifetime of IKE.

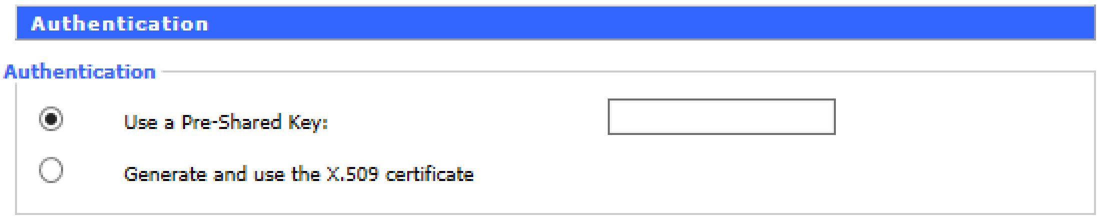
ESP Encryption: The encryption type of ESP.

ESP Integrity: The integrity of ESP.

ESP Grouptype: The grouptype of ESP.

ESP Keylife: The keylife of ESP.

5. Authentication: According requirement detail to select shared key or certificated authentication. It only supports shared key authentication.



Authentication

Authentication

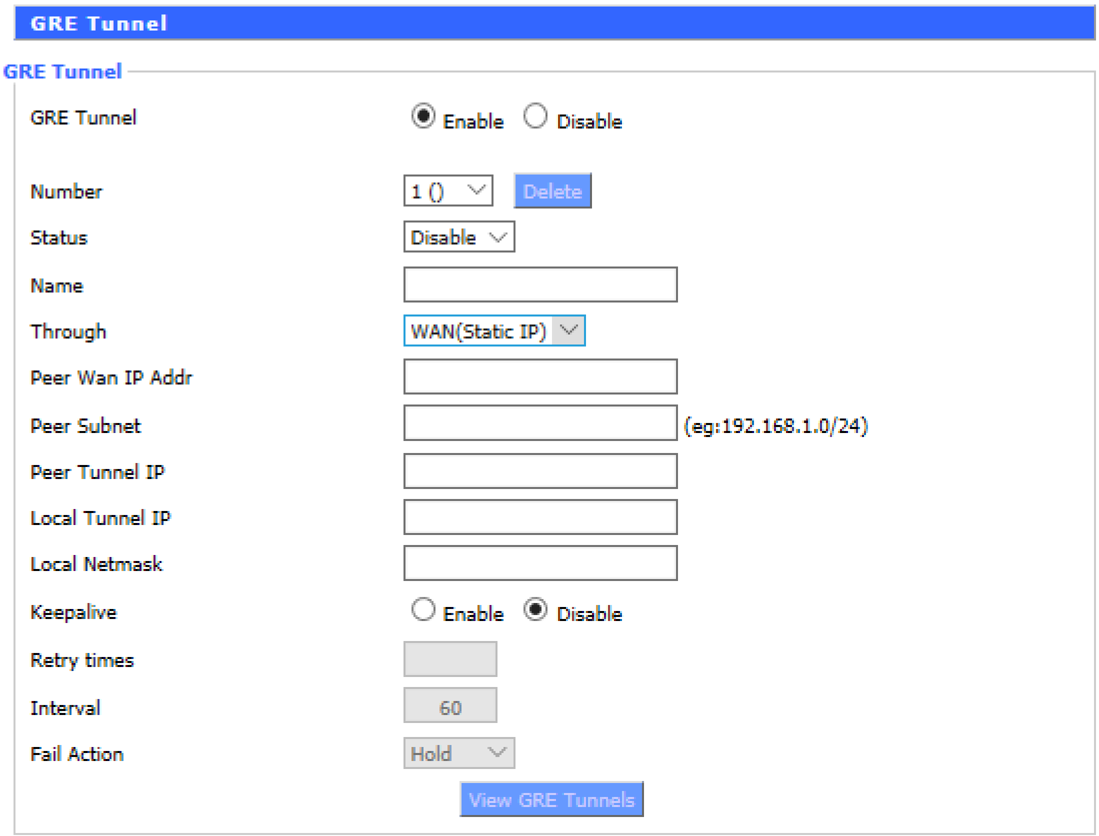
● Use a Pre-Shared Key:

○ Generate and use the X.509 certificate

3.3.4.5 GRE

GRE (Generic Routing Encapsulation) protocol can encapsulate data packets of some network layer protocols, such as IP and IPX, to enable these data packets transport in another layer of network protocol.

GRE adopts tunnel technology which is the third-layer tunnel protocol of VPN.



GRE Tunnel

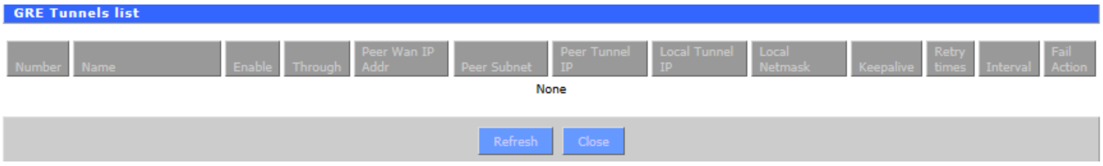
GRE Tunnel

GRE Tunnel	● Enable ○ Disable
Number	1 () Delete
Status	Disable
Name	
Through	WAN(Static IP)
Peer Wan IP Addr	
Peer Subnet	(eg:192.168.1.0/24)
Peer Tunnel IP	
Local Tunnel IP	
Local Netmask	
Keepalive	○ Enable ● Disable
Retry times	
Interval	60
Fail Action	Hold

View GRE Tunnels

Parameters	Option	Description
GRE Tunnel	Enable	Turn on GRE tunnel function
	Disable	Turn off GRE tunnel function
Number	-	The number of tunnels. Up to 12 GRE tunnels
Status	Enable	Turn on GRE tunnel
	Disable	Turn off GRE tunnel
Name	-	The name of tunnel
Through	PPP	GRE transceiver interface: PPP
	LAN	GRE transceiver interface: LAN
	WAN (Static IP)	GRE transceiver interface: WAN
Peer WAN IP Addr	-	The peer WAN port IP address of GRE
Peer Subnet	-	The peer subnet of GRE
Peer Tunnel IP	-	The peer tunnel IP address of GRE
Local Tunnel IP	-	The local tunnel IP address of GRE
Local Netmask	-	The local netmask of GRE
Keepalive	Enable	Turn on GRE keepalive function
	Disable	Turn off GRE keepalive function
Retry times	-	The maximum failure numbers of GRE keepalive
Interval	-	The data packet sending interval of GRE
Fail Action	Hold	Hold the device when failure happen
	Restart	Restart the device when failure happen

And, if you want to view the detail information of GRE, please click the **"View GRE Tunnels"** to show the current GRE information as follow:



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
None												

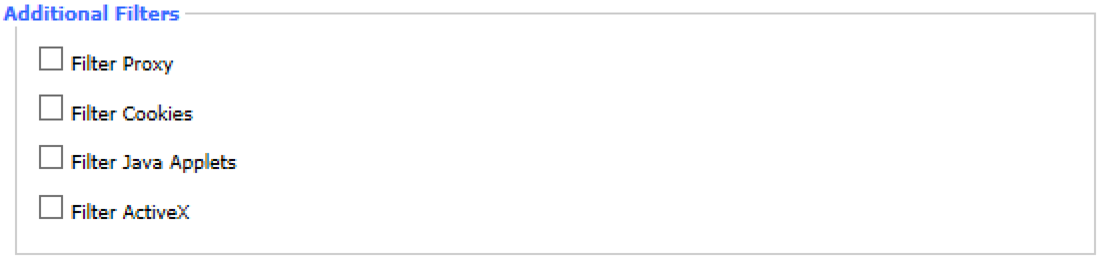
3.3.5 Security

3.3.5.1 Firewall

You can enable or disable firewall function, choose to filter specific internet data types, and prevent anonymous internet request.

It uses SPI protocol to check the incoming packets. Only enable the SPI firewall, you can use another function, such as filter proxy, prevent WAN request and so on.

- **Additional Filters**



Additional Filters

□ Filter Proxy

□ Filter Cookies

□ Filter Java Applets

□ Filter ActiveX

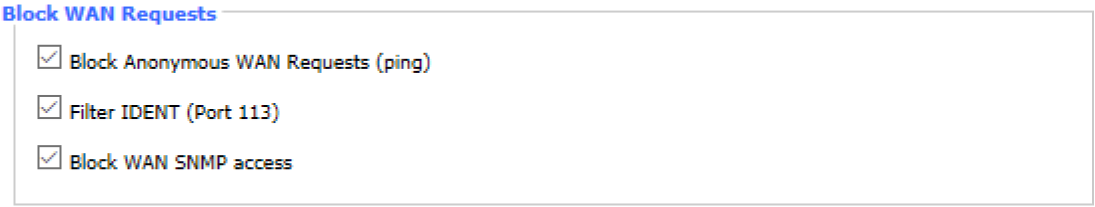
Filter Proxy: Click the check box to enable or disable this function. It will refuse any access of WAN proxy server.

Filter Cookies: Click the check box to enable or disable this function. Cookies are the data which saved in your computer. When you visit the internet, you will use it.

Filter Java Applets: Click the check box to enable or disable this function. If refuse the Java, you may not be able to open the website which programmed with Java tools.

Filter ActiveX: Click the check box to enable or disable this function. If refuse the ActiveX, you may not be able to open the website which programmed with ActiveX tools.

- **Block WAN Requests**



Block WAN Requests

☑ Block Anonymous WAN Requests (ping)

☑ Filter IDENT (Port 113)

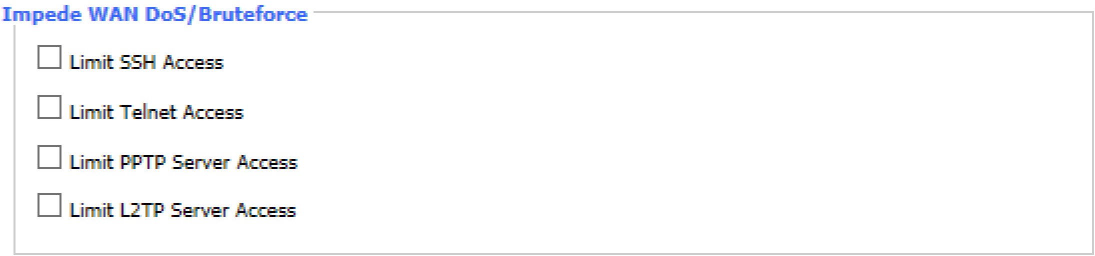
☑ Block WAN SNMP access

Block Anonymous WAN Requests (ping): Click the check box to enable or disable this function. It will prevent your network from being pinged or probed by other internet users, making it difficult to penetrate your network by external users.

Filter IDENT (Port 113): Click the check box to enable or disable this function. It will able to prevent the 113 port from being scanned by devices outside of your local network.

Block WAN SNMP access: Click the check box to enable or disable this function. It will prevent the SNMP connect request from WAN.

◆ Impede WAN DoS / Bruteforce



Impede WAN DoS/Bruteforce

□ Limit SSH Access

□ Limit Telnet Access

□ Limit PPTP Server Access

□ Limit L2TP Server Access

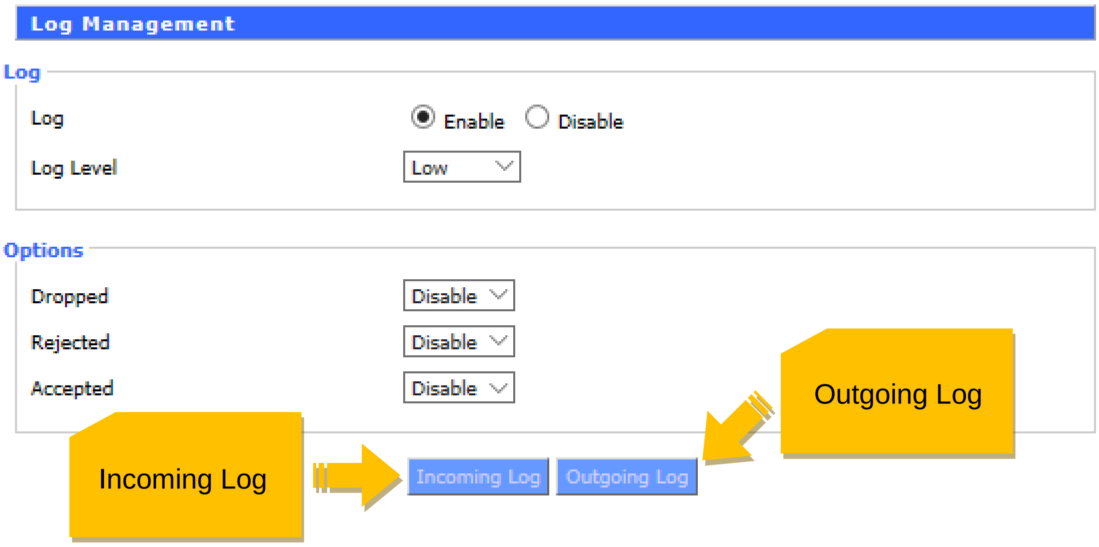
Limit SSH Access: Click the check box to enable or disable this function. It limits the SSH access request from WAN, up to 2 SSH connections per minute for the same IP address.

Limit Telnet Access: Click the check box to enable or disable this function. It limits the Telnet access request from WAN, up to 2 Telnet connections per minute for the same IP address.

Limit PPTP Server Access: Click the check box to enable or disable this function. It limits the PPTP access request from WAN, up to 2 PPTP connections per minute for the same IP address.

Limit L2TP Server Access: Click the check box to enable or disable this function. It limits the L2TP access request from WAN, up to 2 L2TP connections per minute for the same IP address.

◆ Log Management



Log Management

Log

Log	● Enable ○ Disable
Log Level	Low

Options

Dropped	Disable
Rejected	Disable
Accepted	Disable

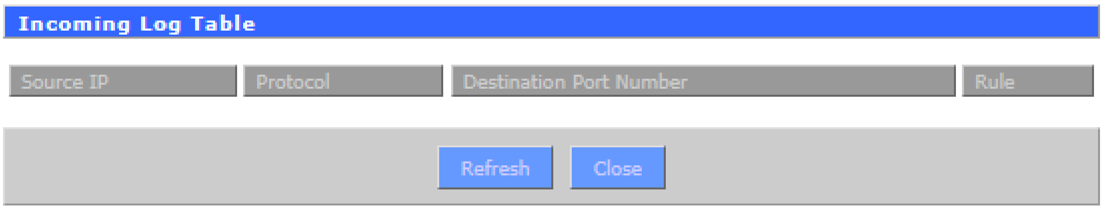
Log Level: It has Low, Medium, High types log level. The higher log level, the more logs will be recorded.

Dropped: The corresponding log will be recorded when enable it.

Rejected: The corresponding log will be recorded when enable it.

Accepted: The corresponding log will be recorded when enable it.

- **Incoming Log**

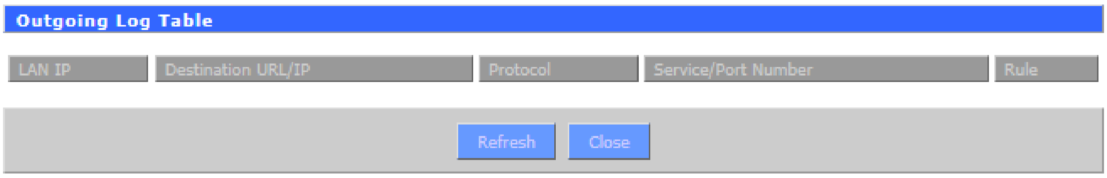


Incoming Log Table

Source IP	Protocol	Destination Port Number	Rule

Click the **"Incoming Log"** button, it will show the recent incoming temporary logs.

- **Outgoing Log**



Outgoing Log Table

LAN IP	Destination URL/IP	Protocol	Service/Port Number	Rule

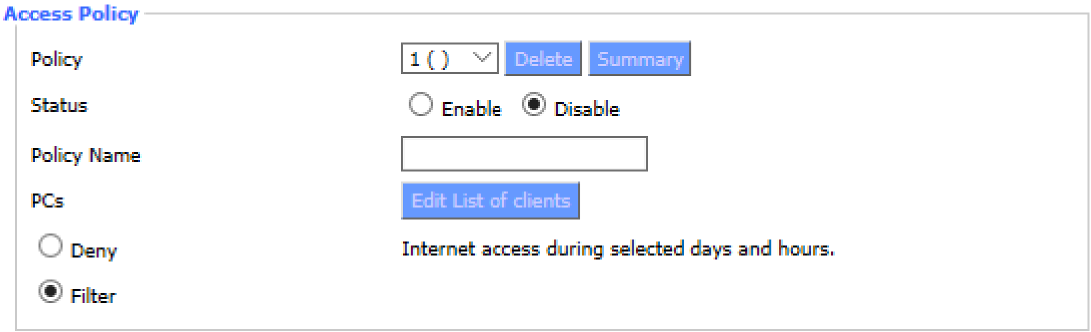
Click the **"Outgoing Log"** button, it will show the recent outgoing temporary logs.

3.3.6 Access Restrictions

3.3.6.1 WAN Access

You can prevent or allow some specific internet applications here.

- **Access Policy**



Access Policy

Policy: 1 ( )

Status: ○ Enable ● Disable

Policy Name:

PCs:

○ Deny

● Filter

Internet access during selected days and hours.

The default policy rule has 2 options: **"Deny"** and **"Filter"**.

"Deny" means specific computers will be denied access to any internet service at specific times.

"Filter" means specific computers will be denied access to specific websites at specific times.

You can set up to 10 access policy that specific computers are denied access to internet service.

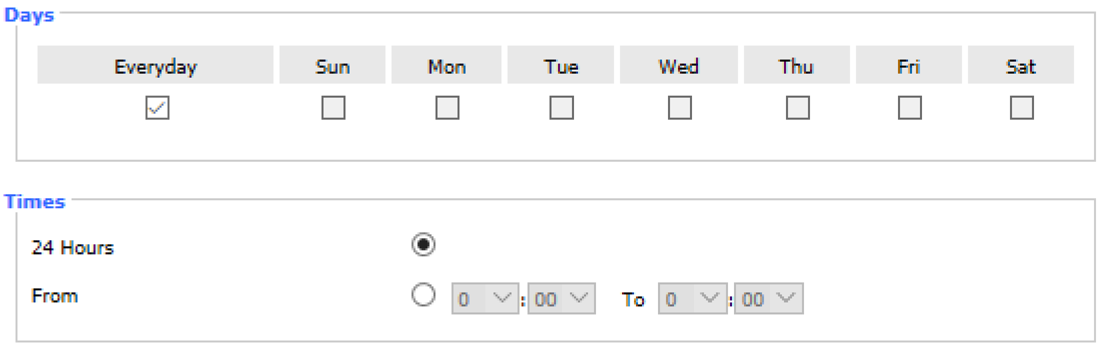
Policy: you can define up to 10 access policy. Click the **"delete"** button to delete one strategy or click the **"Summary"** button to view the strategy description.

Status: Enable or disable one strategy.

Policy Name: the name of this policy.

PCs: this function is used to edit the client list, and the policy is only valid for the PC that is in the list

◆ Date Setting



Days

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

Times

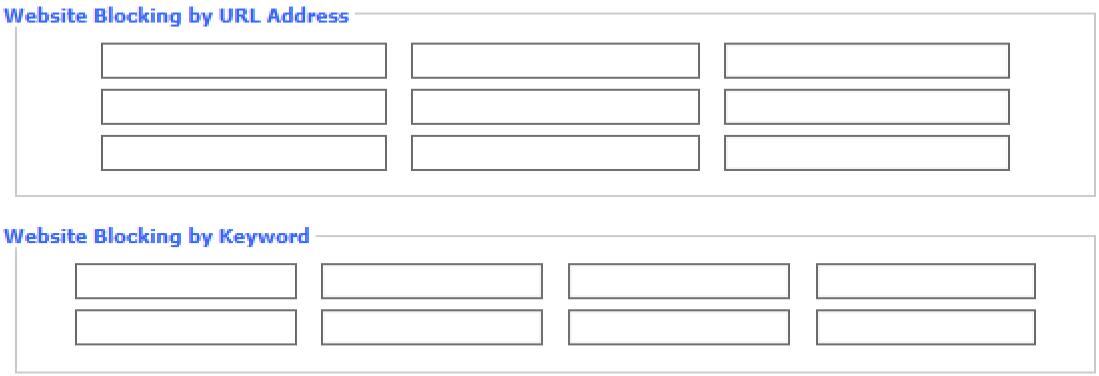
24 Hours ●

From ○ 0 : 00 To 0 : 00

Days: please select the date when your policy applied.

Times: please select the time when your policy applied.

◆ Parameters Setting



Website Blocking by URL Address

Website Blocking by Keyword

Website Blocking by URL Address: you can input URL to block access these websites.

Website Blocking by Keyword: you can input keyword which contains in some web pages to block access it.

◆ How to create a new access policy

1. Select one access policy from "Internet access policy".
2. If you want enable this policy, click the "Enable" button.
3. Fill in the policy name in the "policy name" field.
4. Click the "Edit list of clients" button, it will show "PC list" page, and then you can input the MAC or IP address of PC which applied this policy. If you want to apply this policy to a set of PCS, you can input a range of IP address. When you finish the modify, please click the "Save" button to save configurations, or click the "Cancel Changes" button to cancel it.

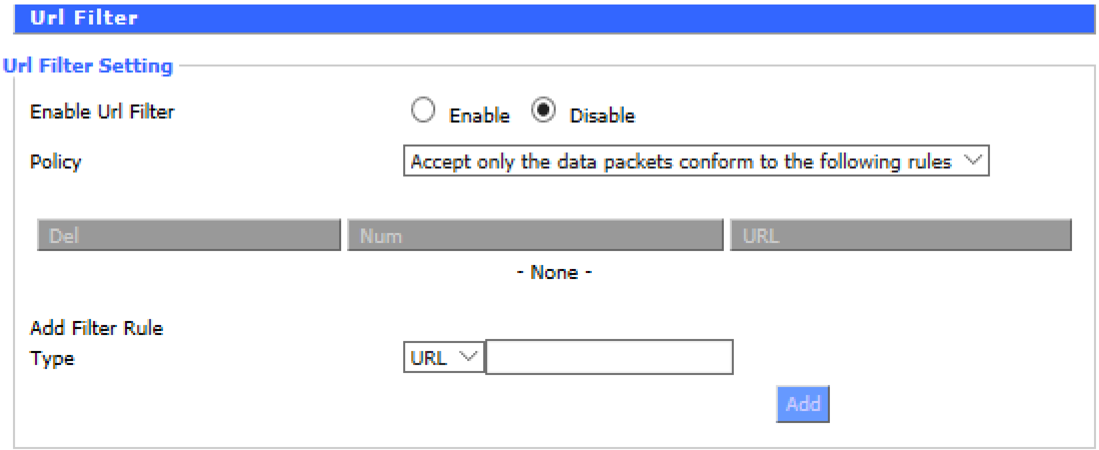
5. Make sure when this policy will take effect. Select the specific date when this policy take effect or select "Everyday", and then select the specific range of time or select "24 Hours".
6. If you want to refuse or only allow access specific URL of website, you can input URL address in the "Website Blocking by URL Address" field.
7. If you want to refuse or only allow access specific keyword of website, you can input URL address in the "Website Blocking by Keyword" field.
8. Click the "Save" button to save this policy, and then click the "Apply Settings" button to take it effect; If you want to cancel this setting, please click the "Cancel Changes" button.

Notice:

1. Default policy rule is "Filter". If you select the default policy rule is "Deny", you need edit relative policy then save it or you can save it directly. If you edit the first policy, it will become the second automatically when save it; If it is not the first one, it will save with original number.

3.3.6.2 URL Filter

You can prevent some specific clients to access specific domain name through URL filter function, such as www.sina.com.



Url Filter

Url Filter Setting

Enable Url Filter ○ Enable ● Disable

Policy: Accept only the data packets conform to the following rules

Del	Num	URL
- None -		

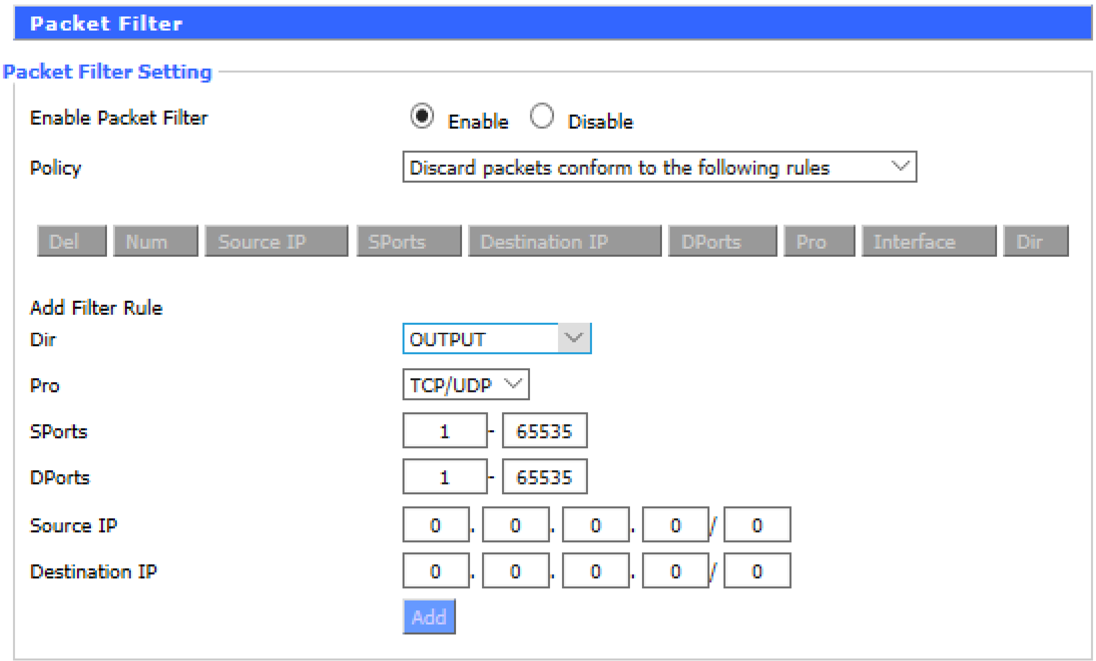
Add Filter Rule

Type: URL

Parameters	Option	Description
Enable Url Filter	Enable	Turn on Url Filter function
	Disable	Turn off Url Filter function
Policy	Accept only the data packets conform to the following rules	Allow to access the URL address which complies with the rule
	Discard packets conform to the following rules	Refuse to access the URL address which complies with the rule

3.3.6.3 Packet Filter

You can prevent some specific data packets through the router then entering the network, or prevent some specific data packets from the internet.



Packet Filter

Packet Filter Setting

Enable Packet Filter ● Enable ○ Disable

Policy: Discard packets conform to the following rules

Del	Num	Source IP	SPorts	Destination IP	DPorts	Pro	Interface	Dir

Add Filter Rule

Dir: OUTPUT

Pro: TCP/UDP

SPorts: 1 - 65535

DPorts: 1 - 65535

Source IP: 0 . 0 . 0 . 0 / 0

Destination IP: 0 . 0 . 0 . 0 / 0

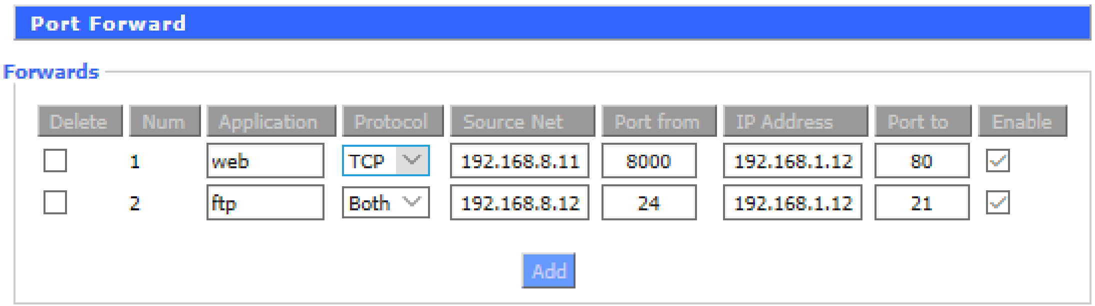
Parameters	Option	Description
Enable Packet Filter	Enable	Turn on Packet Filter function
	Disable	Turn off Packet Filter function
Policy	Accept only the data packets conform to the following rules	Allow to access the URL address which complies with the rule
	Discard packets conform to the following rules	Refuse to access the URL address which complies with the rule
Dir	Output	Data packet from WAN to LAN
	Input	Data packet from LAN to WAN
	Output / Input	All directions
Pro	TCP	TCP data packet filter
	UDP	UDP data packet filter
	ICMP	ICMP data packet filter
	TCP / UDP	TCP / UDP data packet filter
SPorts	-	The source port of data packet
DPorts	-	The destination port of data packet
Source IP	-	The source IP address of data packet
Destination IP	-	The destination IP address of data packet

3.3.7 NAT

3.3.7.1 Port Forwarding

Port forwarding can be used to setting public services of network, such as web server, ftp server or another specific internet application.

Click the **"Add"** button to add a new port forwarding rule.



Port Forward

Forwards

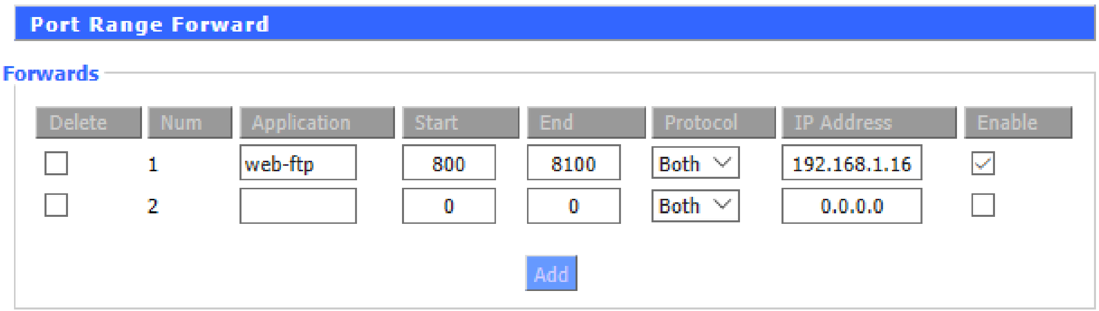
Delete	Num	Application	Protocol	Source Net	Port from	IP Address	Port to	Enable
□	1	web	TCP	192.168.8.11	8000	192.168.1.12	80	☑
□	2	ftp	Both	192.168.8.12	24	192.168.1.12	21	☑

Parameters	Option	Description
Application	-	Input the application name in this field
Protocol	TCP	TCP protocol application
	UDP	UDP protocol application
	TCP / UDP	TCP/UDP protocol application
Source Net	-	Input the source IP address of internet
Port from	-	Input the external port number
IP Address	-	The intranet IP address
Port to	-	The destination port number
Enable	-	Click the check box to enable it. Default is disable

3.3.7.2 Port Range Forwarding

Make sure some applications run normally may require forwarding specific port range. When the request for specific port range is made from internet, the router will send the data to the specific computer.

For security reasons, you may need to restrict the port forwarding to those ports which are using. If you don't want to use the port forwarding, please disable this function.



Port Range Forward

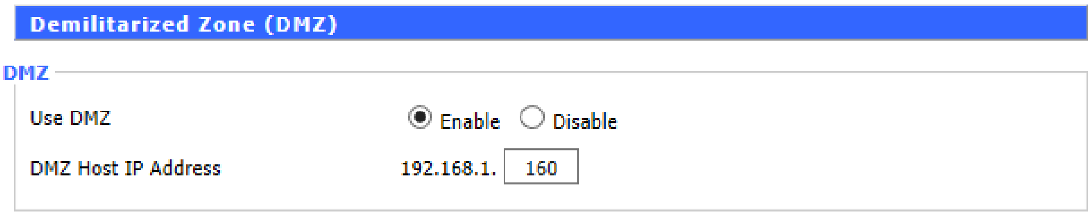
Forwards

Delete	Num	Application	Start	End	Protocol	IP Address	Enable
□	1	web-ftp	800	8100	Both	192.168.1.16	☑
□	2		0	0	Both	0.0.0.0	□

Parameters	Option	Description
Application	-	Input the application name in this field
Start	-	The start port number of port range
End	-	The end port number of port range
Protocol	TCP	TCP protocol application
	UDP	UDP protocol application
	TCP / UDP	TCP/UDP protocol application
IP Address	-	The intranet IP address
Enable	-	Click the check box to enable it. Default is disable

3.3.7.3 DMZ

DMZ (Demilitarized Zone) allows a network user to be exposed to the internet, and then provide particular service. If you want to turn on the DMZ function, please select the **"Enable"** button, and then input the IP address in the **"DMZ Host IP Address"** field.



Demilitarized Zone (DMZ)

DMZ

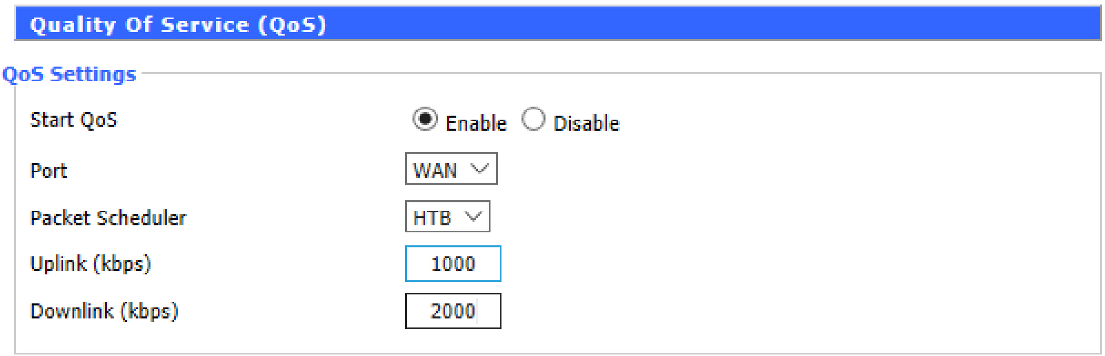
Use DMZ ● Enable ○ Disable

DMZ Host IP Address 192.168.1. 160

3.3.8 QoS

3.3.8.1 Basic

QoS allows you to limit uplink and downlink traffic and assigns priority to the specific IP address or MAC.



Quality Of Service (QoS)

QoS Settings

Start QoS ● Enable ○ Disable

Port WAN

Packet Scheduler HTB

Uplink (kbps) 1000

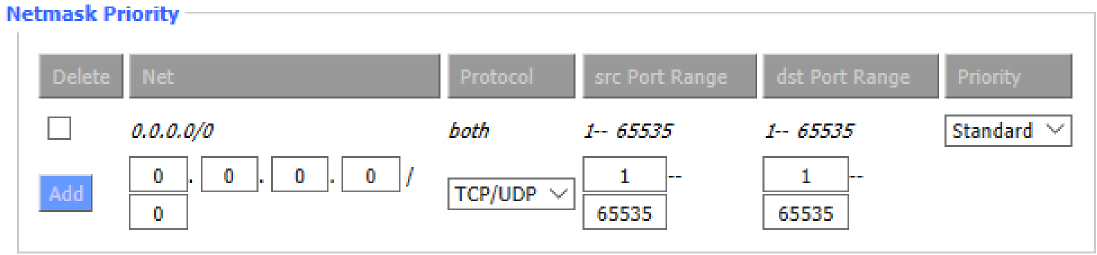
Downlink (kbps) 2000

Uplink (kbps): you can assign the uplink bandwidth in this field. In fact, it may be the 80%-90% of maximum bandwidth.

Downlink (kbps): you can assign the downlink bandwidth in this field. In fact, it may be the 80%-90% of maximum bandwidth.

3.3.8.2 Classify

◆ **Netmask Priority**

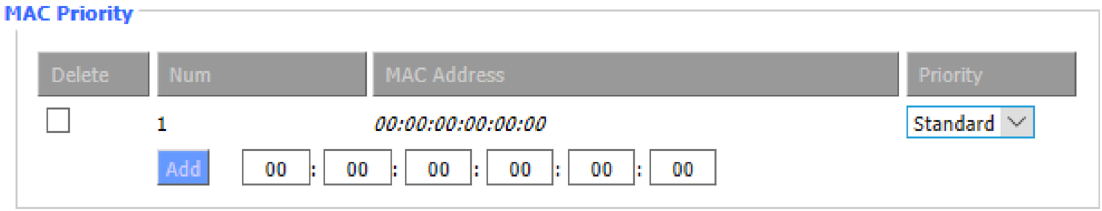


Netmask Priority

Delete	Net	Protocol	src Port Range	dst Port Range	Priority
□	*0.0.0.0/0*	*both*	*1-- 65535*	*1-- 65535*	Standard
Add	0 . 0 . 0 . 0 / 0	TCP/UDP	1 -- 65535	1 -- 65535	

Parameters	Option	Description
Priority	Exempt	At this mode, data flow only limit by hardware condition
	Premium	(75/100) * Uplink; (75/100) * Downlink
	Express	(15/100) * Uplink; (15/100) * Downlink
	Standard	(10/100) * Uplink; (10/100) * Downlink
	Bulk	1000 bit (almost 0); 1000 bit (almost 0)

◆ **MAC Priority**



MAC Priority

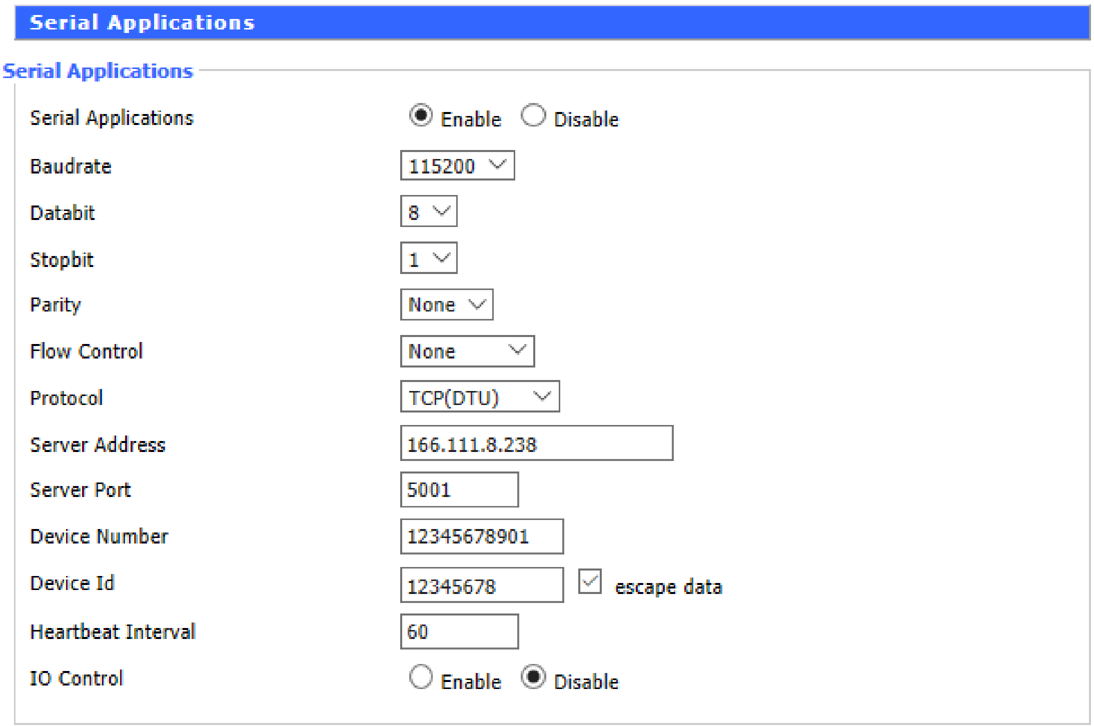
Delete	Num	MAC Address	Priority
□	1	*00:00:00:00:00:00*	Standard
	Add	00 : 00 : 00 : 00 : 00 : 00	

Parameters	Option	Description
Priority	Exempt	At this mode, data flow only limit by hardware condition
	Premium	(75/100) * Uplink; (75/100) * Downlink
	Express	(15/100) * Uplink; (15/100) * Downlink
	Standard	(10/100) * Uplink; (10/100) * Downlink
	Bulk	1000 bit (almost 0); 1000 bit (almost 0)

3.3.9 Application

3.3.9.1 Serial Applications

F8926-GW embedded serial convert to TCP/IP program. The console port can be configured to ordinary serial port.



Serial Applications

Serial Applications

Serial Applications	● Enable ○ Disable
Baudrate	115200
Databit	8
Stopbit	1
Parity	None
Flow Control	None
Protocol	TCP(DTU)
Server Address	166.111.8.238
Server Port	5001
Device Number	12345678901
Device Id	12345678 ☑ escape data
Heartbeat Interval	60
IO Control	○ Enable ● Disable

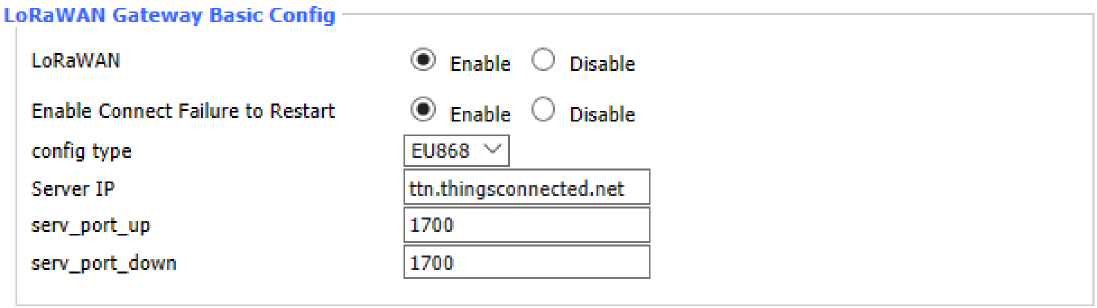
Parameters	Option	Description
Serial Applications	Enable	Turn on serial application function
	Disable	Turn off serial application function
Baudrate		The number of bytes per second transmitted by device. It can be 110, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 119200
Databit	-	Databit can be 5,6,7 or 8
Stopbit	-	It is the ending flag of data. It can be 1 or 2
Parity	None	None parity check
	Odd	Odd parity check
	Even	Even parity check
Flow Control	None	None flow control
	Hardware	Hardware flow control
	Software	Software flow control
Protocol	UDP (DTU)	Serial convert to UDP connection, include custom application layer protocols, as a four-faith IP Modem
	Pure UDP	Standard serial converts to UDP connection
	TCP (DTU)	Serial convert to TCP connection, include custom application layer protocols, as a four-faith IP Modem
	Pure TCP	Standard serial converts to TCP connection
	TCP Server	Standard TCP server connection
	TCST	Custom TCP connection
	Modbus TCP	Standard Modbus TCP

Server Address	-	The IP address or domain name of server
Server Port	-	The listening port of server
Device Number	-	11 bytes character string. It only takes effect when protocol type selects “UDP(DTU)” or “TCP(DTU)”
Device Id	-	8 bytes character string. It only takes effect when protocol type selects “UDP(DTU)” or “TCP(DTU)”
Heartbeat Interval	-	The time interval of heartbeat packets. It only takes effect when protocol type selects “UDP(DTU)” or “TCP(DTU)”

3.3.9.2 LoRaWAN Application

You can configure LoRaWAN parameters of F8926-GW here.

◆ **LoRaWAN Gateway Basic Config**



LoRaWAN Gateway Basic Config

LoRaWAN ● Enable ○ Disable

Enable Connect Failure to Restart ● Enable ○ Disable

config type EU868

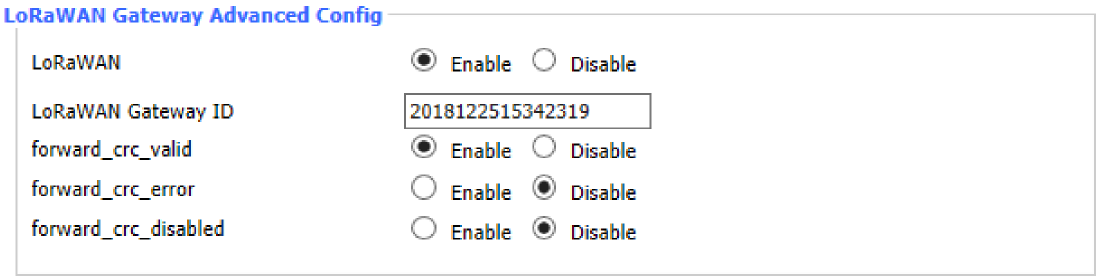
Server IP ttn.thingsconnected.net

serv_port_up 1700

serv_port_down 1700

Parameters	Options	Description
LoRaWAN	Enable	Turn on LoRaWAN function
	Disable	Turn off LoRaWAN function
Enable Connect Failure to Restart	Enable	Enable restart system when connect failure
	Disable	Disable restart system when connect failure
Config type	CN433	LoRaWAN frequency band setting: CN433
	CN470	LoRaWAN frequency band setting: CN470
	EU868	LoRaWAN frequency band setting: EU868
	US915	LoRaWAN frequency band setting: US915
	AU915	LoRaWAN frequency band setting: AU915
Server IP	-	The IP address of LoRaWAN server
Serv_port_up	-	LoRaWAN data service center program uplink port. Value range is 0-65535 and the default value is 1700.
Serv_port_down	-	LoRaWAN data service center program downlink port. Value range is 0-65535 and the default value is 1700

- ◆ **LoRaWAN Gateway Advanced Config**



LoRaWAN Gateway Advanced Config

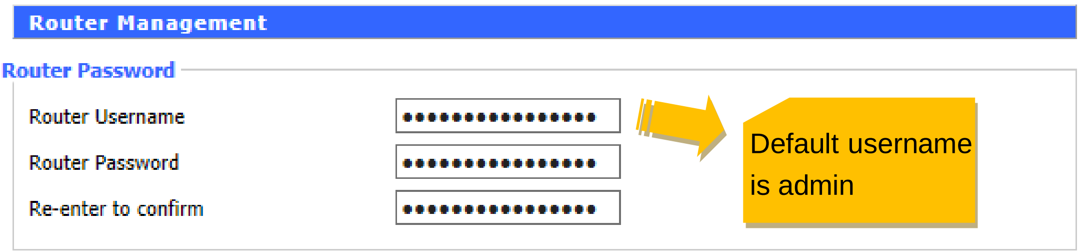
LoRaWAN	● Enable ○ Disable
LoRaWAN Gateway ID	2018122515342319
forward_crc_valid	● Enable ○ Disable
forward_crc_error	○ Enable ● Disable
forward_crc_disabled	○ Enable ● Disable

Parameters	Options	Description
LoRaWAN	Enable	Turn on LoRaWAN function
	Disable	Turn off LoRaWAN function
LoRaWAN Gateway ID	-	the unique identity of the base station, which the server can distinguish different LoRaWAN base station
Forward_crc_valid	Enable	Turn on CRC for validation (default)
	Disable	Turn off CRC for validation
Forward_crc_error	Enable	Turn on CRC for validation error function
	Disable	Turn off CRC for validation error function (default)
Forward_crc_disabled	Enable	Turn on CRC validation
	Disable	Turn off CRC validation (default)

3.3.10 Admin

3.3.10.1 Management

This page allows network administrators to manage specific F8926-GW functions to ensure access and security.



Router Management

Router Password

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

Default username is admin

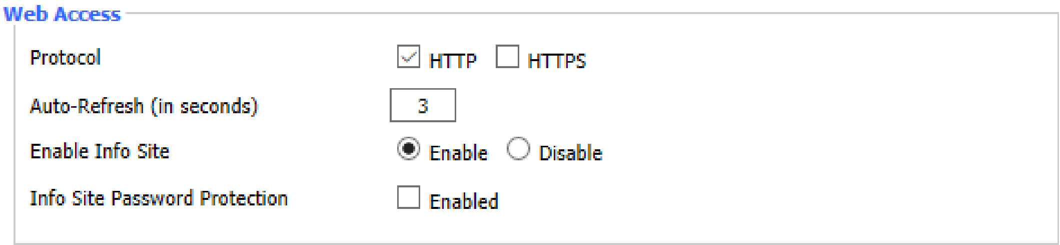
New password shall not exceed 32 characters length and shall not contain any space. Make sure the password is the same as the one you set, or the system will prompt an error.

We strongly recommend that modify the default password to ensure system security.

- ◆ **Web Access**

You can manage the base station by HTTP or HTTPS protocol, and if you select to disable this function, it should be root manually.

Also, you can enable or disable the information pages of F8926-GW, so that you can protect it by password (input correctly username and password to open it).



Web Access

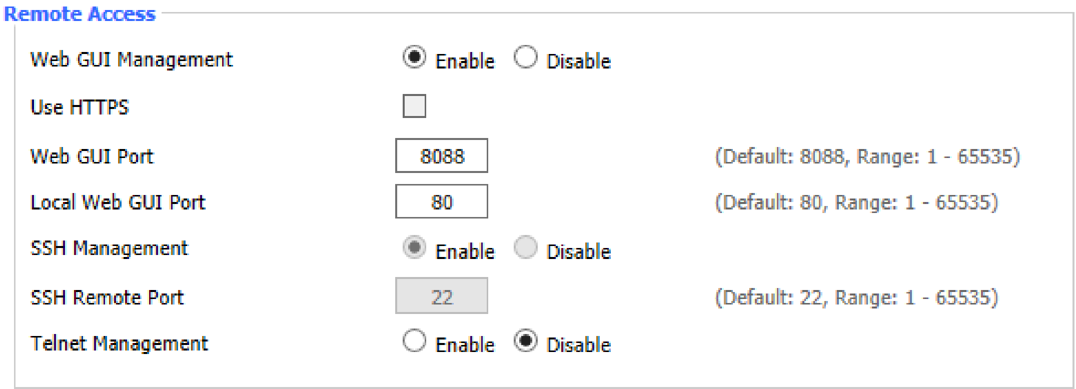
Protocol	☑ HTTP ☐ HTTPS
Auto-Refresh (in seconds)	3
Enable Info Site	● Enable ○ Disable
Info Site Password Protection	☐ Enabled

Parameters	Options	Description
Protocol	HTTP	Web access by http
	HTTPS	Web access by https
Auto-Refresh (in seconds)	-	The time interval for automatic refresh the web page. If you set 0, it means turn off this function
Enable Info Site	Enable	Enable display system information page before login
	Disable	Disable display system information page before login
Info Site Password Protection	Enabled	Enable the system information page password protection function
	None	Disable the system information page password protection function

- **Remote Access**

It allows remote manage the device through the internet.

Warning：If the remote access function is turn on, anyone who get the correctly IP address and password will change the device settings.



Remote Access

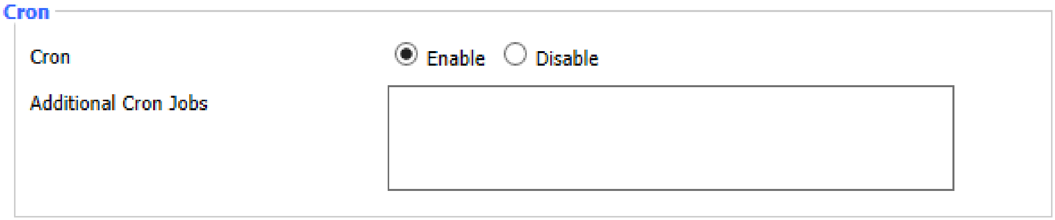
Web GUI Management	● Enable ○ Disable	
Use HTTPS	☐	
Web GUI Port	8088	(Default: 8088, Range: 1 - 65535)
Local Web GUI Port	80	(Default: 80, Range: 1 - 65535)
SSH Management	● Enable ○ Disable	
SSH Remote Port	22	(Default: 22, Range: 1 - 65535)
Telnet Management	○ Enable ● Disable	

Parameters	Options	Description
Web GUI Management	Enable	Enable remote web management function. If you don’t check the https protocol, you can input http://xxx.xxx.xxx.xxx:8088 to remote manage F8926-GW, else you need input https://xxx.xxx.xxx.xxx:8088 (x means the access IP address, and 8088 means the web access port),

	Disable	Disable remote web management function
Use HTTPS	-	Whether using https protocol access device. It will take effect when you check it
Web GUI Port	-	Specify the web access port, default 8088
Local Web GUI Port	-	Specify the local access port, default 80
SSH Management	Enable	Turn on SSH remote management function. You can get more information about SSH daemon settings in service pages
	Disable	Turn off SSH remote management function
SSH Remote Port	-	Specify the SSH remote port, default 22
Telnet Management	Enable	Turn on telnet management function
	Disable	Turn off telnet management function

◆ Cron

Cron can execute the Linux commands what you plan. You can set the command lines or scripts in that.



Cron

Cron ● Enable ○ Disable

Additional Cron Jobs

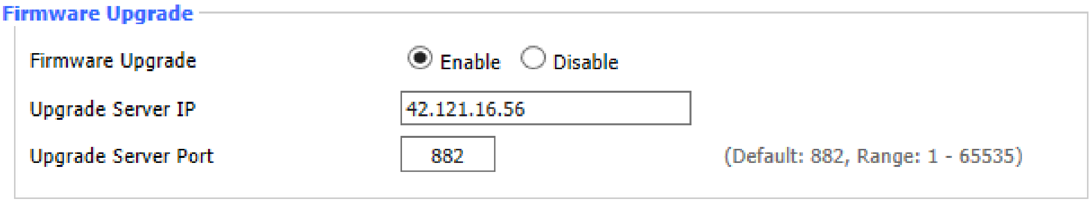
Parameters	Options	Description
Cron	Enable	Turn on Cron server
	Disable	Turn off Cron server
Additional Cron Jobs	-	Linux command lines or scripts

◆ Remote Management

This function is used for server configurations with device platform, such as device monitoring platform, WIFI advertising system, device flow monitoring and so on. To get more details can contact with our technical support.

◆ Firmware Upgrade

Remote firmware upgrade configuration.



Firmware Upgrade

Firmware Upgrade ● Enable ○ Disable

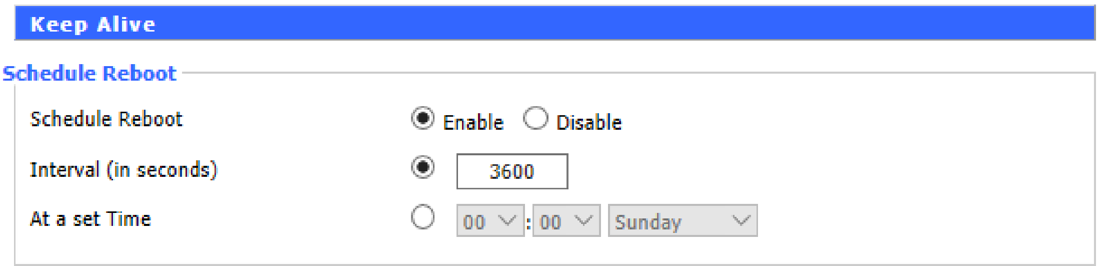
Upgrade Server IP 42.121.16.56

Upgrade Server Port 882 (Default: 882, Range: 1 - 65535)

Parameters	Options	Description
Firmware Upgrade	Enable	Turn on remote firmware upgrade function
	Disable	Turn off remote firmware upgrade function
Upgrade Server IP	-	Configure upgrade server IP address
Upgrade Server Port		Configure upgrade server port

3.3.10.2 Keep Alive

You can set schedule restart the system.



Keep Alive

Schedule Reboot

Schedule Reboot ● Enable ○ Disable

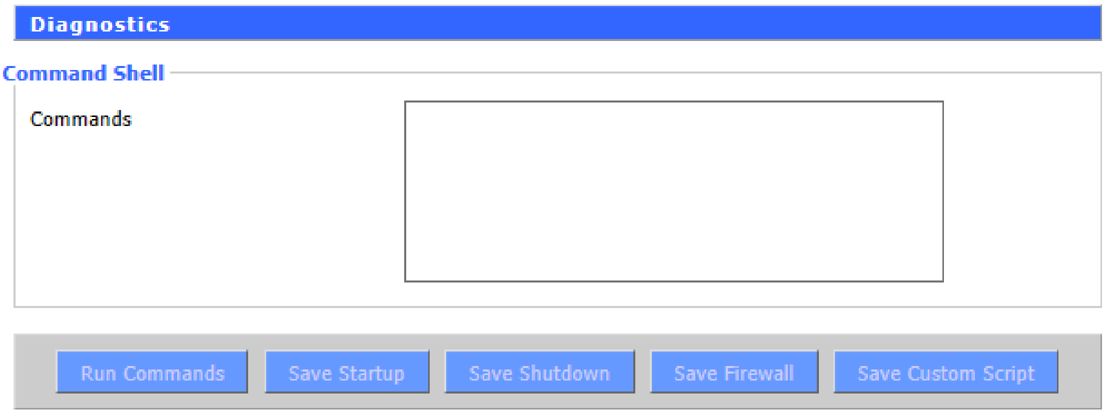
Interval (in seconds) ● 3600

At a set Time ○ 00 : 00 Sunday

Parameters	Options	Description
Schedule Reboot	Enable	Turn on schedule reboot function
	Disable	Turn off schedule reboot function
Interval (in seconds)	-	Restart the system in seconds
At a set Time		Restart the system in a specific data, everyday or every week

3.3.10.3 Commands

You can fill in the commands in this field and click the “Run commands” button to submit it.



Diagnostics

Command Shell

Commands

“Run Commands” – Run these commands.

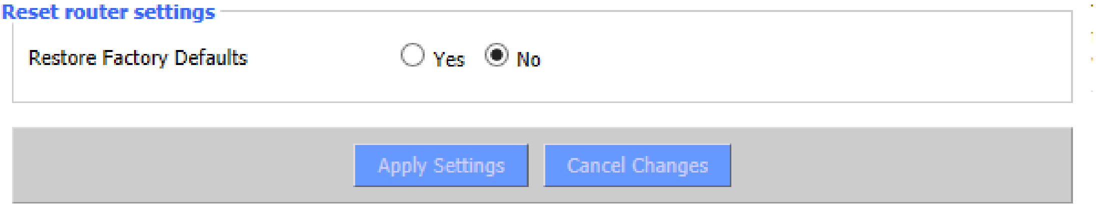
“Save Startup” – You can save these commands to startup command.

“Save Shutdown” – You can save these commands to shutdown command.

“Save Firewall” – You can save these commands to firewall command.

“Save Custom Script” – Custom commands save in /tmp/custom.sh file, you can run or use the cron to call it.

3.3.10.4 Factory Defaults

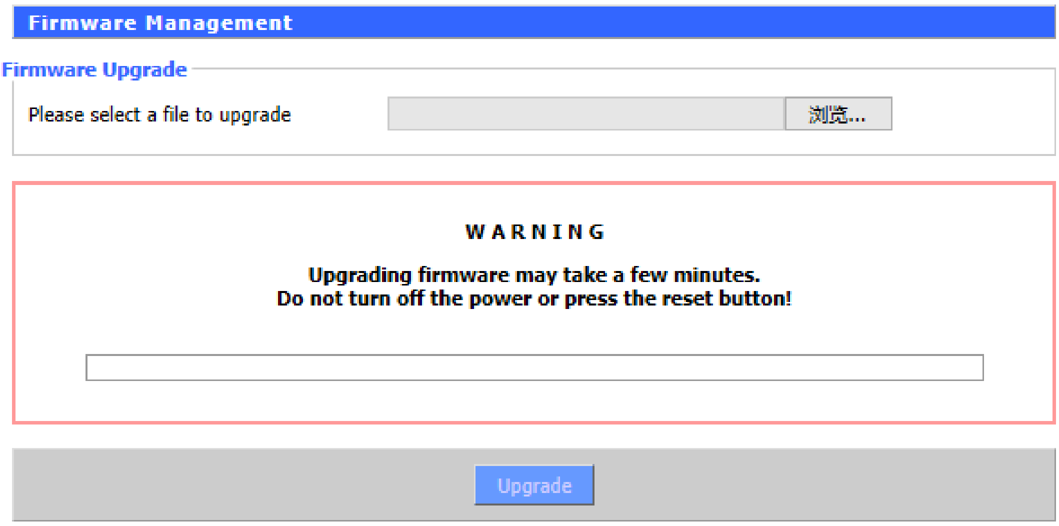


Reset router settings

Restore Factory Defaults ○ Yes ● No

In this page, you can restore device configurations. If you select **“yes”** and then click the **“Apply Setting”** button, all configurations will be cleared and restored to factory settings.

3.3.10.5 Firmware Upgrade



Firmware Management

Firmware Upgrade

Please select a file to upgrade

WARNING

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

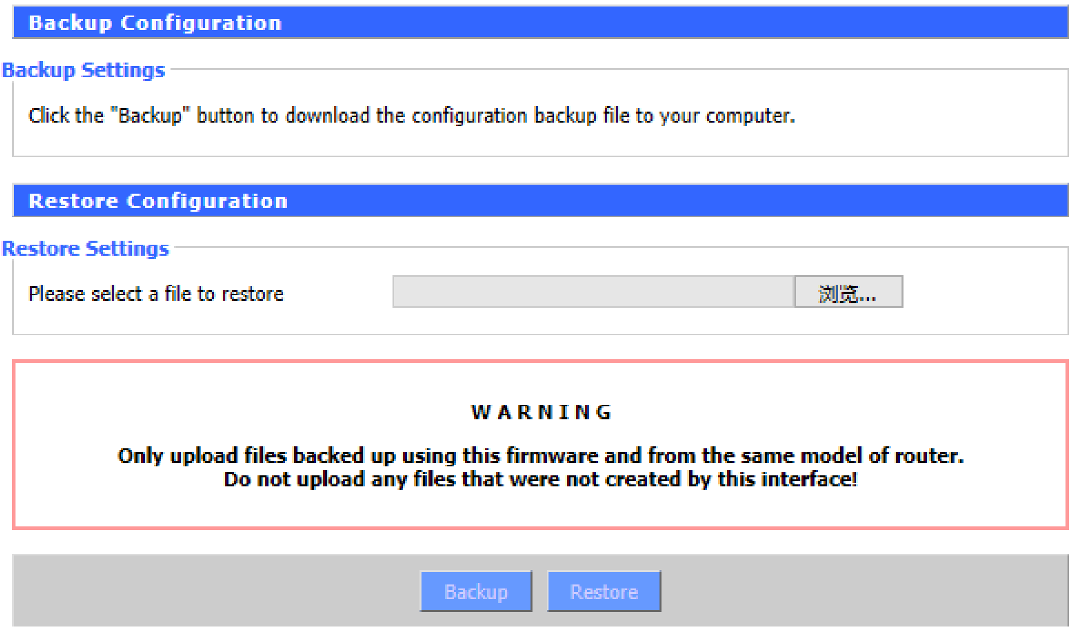
New firmware version can be found in en.four-faith.com, you can download it free, and then loading it into F8926-GW. If the device can work normally, there is no need download and upgrade new firmware version, unless new firmware version includes what new features you want.

Click the **“browse”** button and then choose the firmware file and then click the **“upgrade”** button, the device starting upgrade. It may take a few minutes, please don’t power off or reset the device.

Warning: It may be lost configurations when upgrade firmware, so you need backup current configurations before upgrade it.

3.3.10.6 Backup

This module is used to backup or restore the device configuration file.



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

WARNING

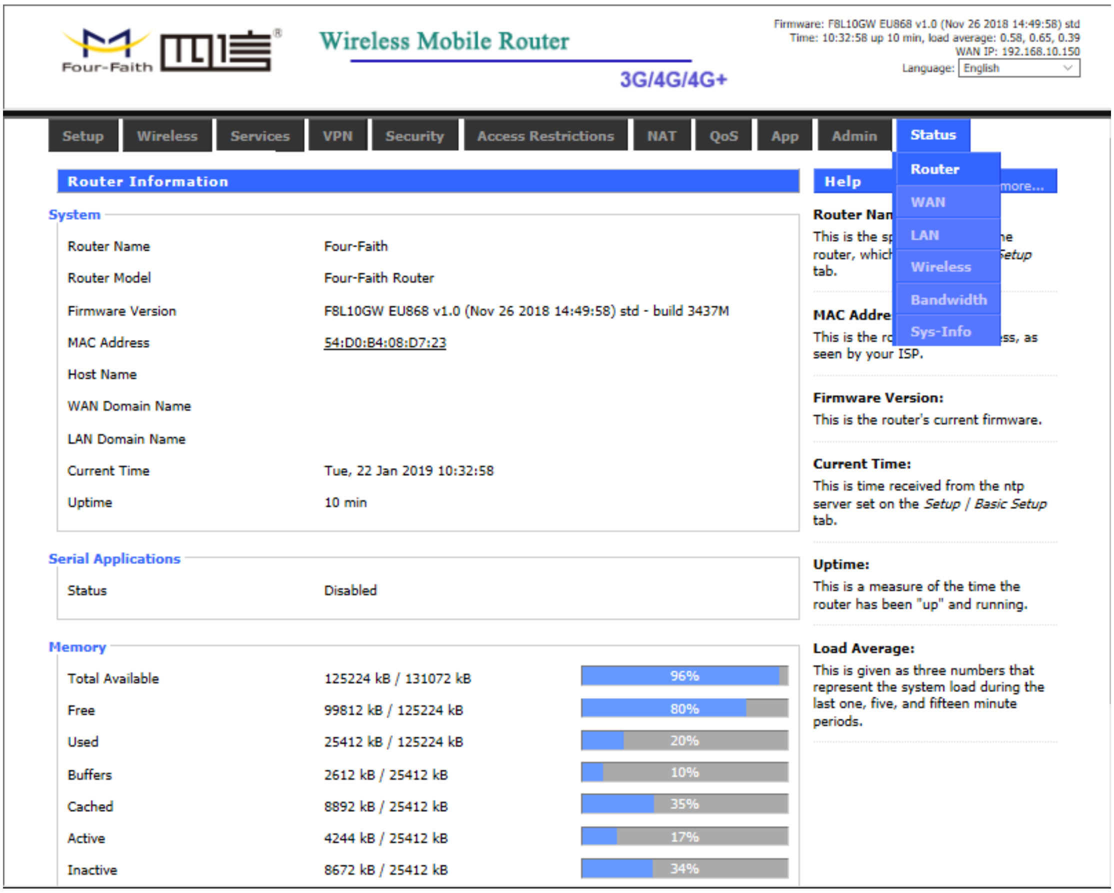
Only upload files backed up using this firmware and from the same model of router.
Do not upload any files that were not created by this interface!

If you want to backup configuration file, please click the **"Backup"** button and then follow the system directions step by step.

If you want to restore configuration file, please click the **"Browse"** button select the backup configuration file and then follow the system directions step by step. And click the **"Restore"** button to upload it.

3.3.11 Status

3.3.11.1 Router



Firmware: F8L10GW EU868 v1.0 (Nov 26 2018 14:49:58) std
Time: 10:32:58 up 10 min, load average: 0.58, 0.65, 0.39
WAN IP: 192.168.10.150
Language: English

Router Information

System

Router Name	Four-Faith
Router Model	Four-Faith Router
Firmware Version	F8L10GW EU868 v1.0 (Nov 26 2018 14:49:58) std - build 3437M
MAC Address	54:D0:B4:08:D7:23
Host Name	
WAN Domain Name	
LAN Domain Name	
Current Time	Tue, 22 Jan 2019 10:32:58
Uptime	10 min

Serial Applications

Status	Disabled

Memory

Total Available	125224 kB / 131072 kB	96%
Free	99812 kB / 125224 kB	80%
Used	25412 kB / 125224 kB	20%
Buffers	2612 kB / 25412 kB	10%
Cached	8892 kB / 25412 kB	35%
Active	4244 kB / 25412 kB	17%
Inactive	8672 kB / 25412 kB	34%

Router Nam

This is the sp he router, which *Setup* tab.

MAC Addre

This is the ro ss, as seen by your ISP.

Firmware Version:

This is the router's current firmware.

Current Time:

This is time received from the ntp server set on the *Setup* / *Basic Setup* tab.

Uptime:

This is a measure of the time the router has been "up" and running.

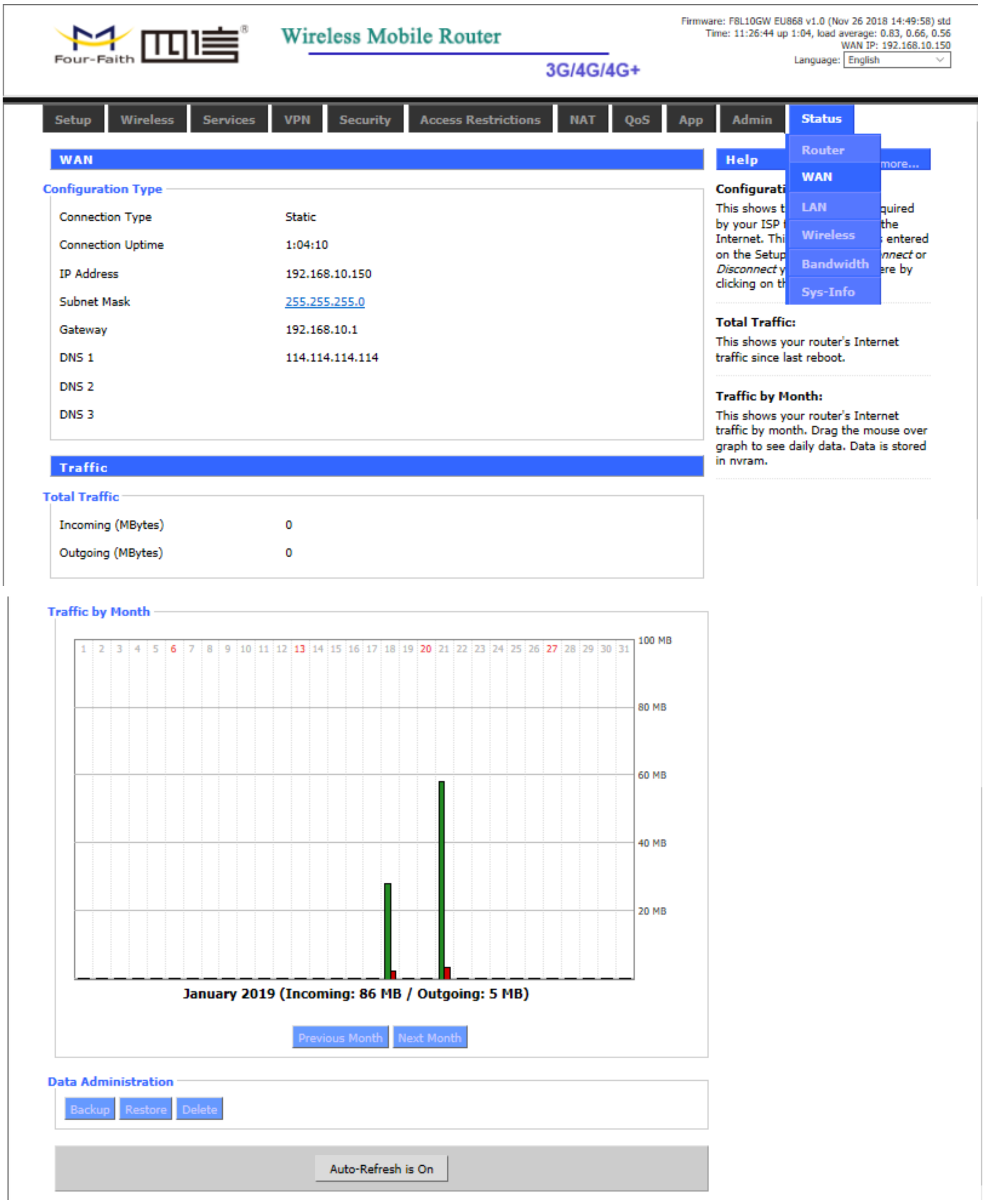
Load Average:

This is given as three numbers that represent the system load during the last one, five, and fifteen minute periods.

Item	Field	Description
System	Router Name	Show the router name of base station
	Router Model	Show the router model name of base station
	Firmware version	Show the current firmware version of base station
	MAC Address	Show the MAC address of base station
	Host Name	Show the host name of base station
	WAN Domain Name	Show the WAN port domain name of base station
	LAN Domain Name	Show the LAN port domain name of base station
	Current Time	Show the system current time of base station
	Uptime	Show the system run time of base station
Serial Application	Status	Show the serial application status of base station
Memory	Total Available	Show the available memory size of base station
	Free	Show the free memory size of base station
	Used	Show the used memory size of base station

	Buffers	Show the available buffer of base station
	Cached	Show the number of cache data
	Active	Show the active memory size of base station
	Inactive	Show the inactive memory size of base station
Network	IP Filter Max Connections	Show the IP Filter connections of base station
	Active IP Connections	Show the active IP connections of base station, if you click this link, it will show all active IP details

3.3.11.2 WAN



Firmware: F8L10GW EU868 v1.0 (Nov 26 2018 14:49:58) std
Time: 11:26:44 up 1:04, load average: 0.83, 0.66, 0.56
WAN IP: 192.168.10.150
Language: English

WAN

Configuration Type

Connection Type	Static
Connection Uptime	1:04:10
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	

Traffic

Total Traffic

Incoming (MBytes)	0
Outgoing (MBytes)	0

Traffic by Month

January 2019 (Incoming: 86 MB / Outgoing: 5 MB)

Data Administration

Configurati

This shows t quired
by your ISP the
Internet. Thi entered
on the Setup *nnect* or
Disconnect y ere by
clicking on th

Total Traffic:

This shows your router's Internet traffic since last reboot.

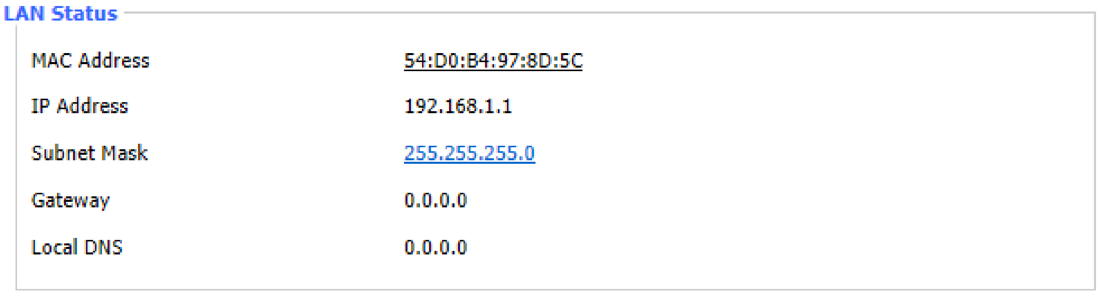
Traffic by Month:

This shows your router's Internet traffic by month. Drag the mouse over graph to see daily data. Data is stored in nvram.

Item	Parameters	Description
Configuration Type	Configuration Type	Show current connect type of base station
	Connection Uptime	Show current duration online of base station
	IP Address	Show the IP address of WAN port
	Subnet Mask	Show the subnet mask of WAN port
	Gateway	Show the gateway of WAN port
	DNS1	Show the DNS1 of WAN port
	DNS2	Show the DNS2 of WAN port
	DNS3	Show the DNS3 of WAN port
Total Traffic	Incoming	Show the incoming total traffic
	Outgoing	Show the outgoing total traffic
Data Administration	Backup	Backup the data administration configuration
	Restore	Restore the data administration configuration
	Delete	Delete the data administration configuration

3.3.11.3 LAN

- ◆ **LAN Status**

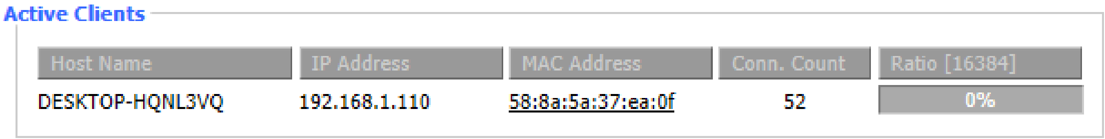


LAN Status

MAC Address	54:D0:B4:97:8D:5C
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

Item	Parameters	Description
MAC Address	-	The MAC address of LAN port
IP Address	-	The IP address of LAN port
Subnet Mask	-	The subnet mask of LAN port
Gateway	-	The gateway of LAN port
Local DNS	-	The local DNS of LAN port

- ◆ **Active Clients**



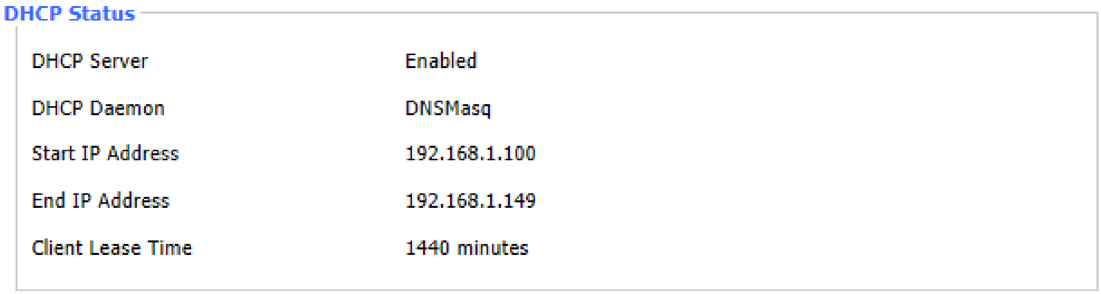
Active Clients

Host Name	IP Address	MAC Address	Conn. Count	Ratio [16384]
DESKTOP-HQNL3VQ	192.168.1.110	58:8a:5a:37:ea:0f	52	0%

Item	Parameters	Description
Host Name	-	The host name of client
IP Address	-	The IP address of client
MAC Address	-	The MAC address of client

Conn. Count	-	The number of connections generated by client
Ratio	-	Percentage of connections

- ◆ **DHCP Status**

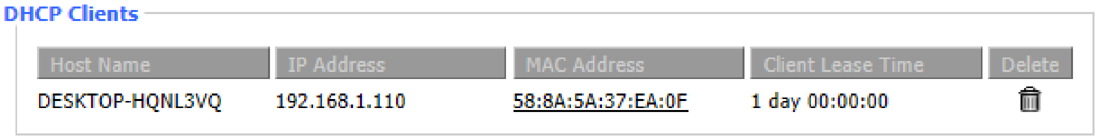


DHCP Status

DHCP Server	Enabled
DHCP Daemon	DNSMasq
Start IP Address	192.168.1.100
End IP Address	192.168.1.149
Client Lease Time	1440 minutes

Item	Parameters	Description
DHCP Server	-	The status of DHCP server
DHCP Daemon	-	The protocol of DHCP server
Start IP Address	-	The start IP address of DHCP client
End IP Address	-	The end IP address of DHCP client
Client Lease Time	-	The lease time of DHCP client

- ◆ **DHCP Clients**



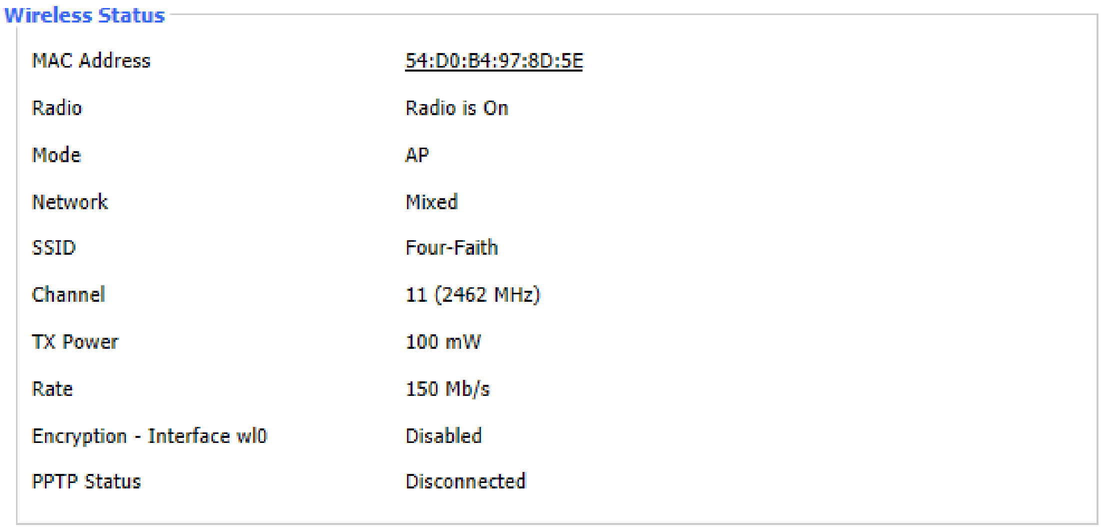
DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time	Delete
DESKTOP-HQNL3VQ	192.168.1.110	58:8A:5A:37:EA:0F	1 day 00:00:00	🗑

Item	Parameters	Description
Host Name	-	The host name of DHCP client
IP Address	-	The IP address of DHCP client
MAC Address	-	The MAC address of DHCP client
Client Lease Time	-	The lease time of DHCP client

3.3.11.4 Wireless

- ◆ **Wireless Status**

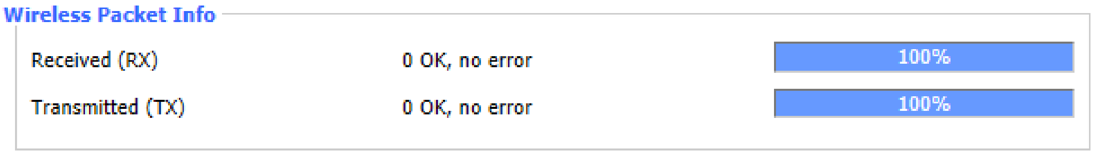


Wireless Status

MAC Address	54:D0:B4:97:8D:5E
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	Four-Faith
Channel	11 (2462 MHz)
TX Power	100 mW
Rate	150 Mb/s
Encryption - Interface wl0	Disabled
PPTP Status	Disconnected

Item	Parameters	Description
MAC Address	-	The MAC address of wireless network
Radio	-	Wireless status
Mode	-	Wireless mode
Network	-	Wireless network mode
SSID		The name of wireless network
Channel		The channel of wireless network
TX Power		The Tx power of wireless
Rate		The speed rate of wireless
Encryption - Interface wl0		Wireless encryption type
PPTP Status		PPTP status

- **Wireless Packet Info**

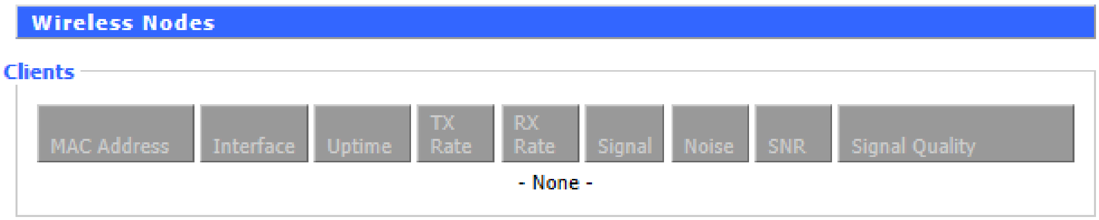


Wireless Packet Info

Received (RX)	0 OK, no error	100%
Transmitted (TX)	0 OK, no error	100%

Item	Parameters	Description
Received (RX)	-	Have been received packets
Transmitted (TX)	-	Have been transmitted packets

- **Wireless Nodes**



Wireless Nodes

Clients

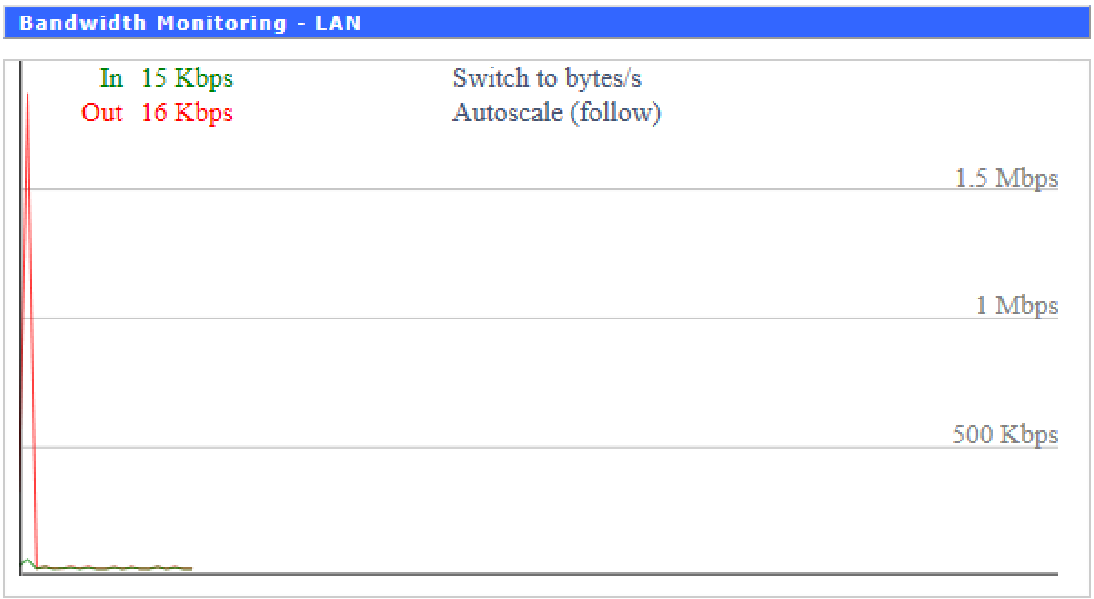
MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality

- None -

Item	Parameters	Description
MAC Address	-	The MAC address of wireless client
Interface	-	The interface of wireless client
Uptime		The uptime of wireless client
TX Rate		The TX rate of wireless client
RX Rate		The RX rate of wireless client
Signal		The signal of wireless client
Noise		The noise of wireless client
SNR		The SNR of wireless client
Signal Quality		The signal quality of wireless client

3.3.11.5 BandWidth

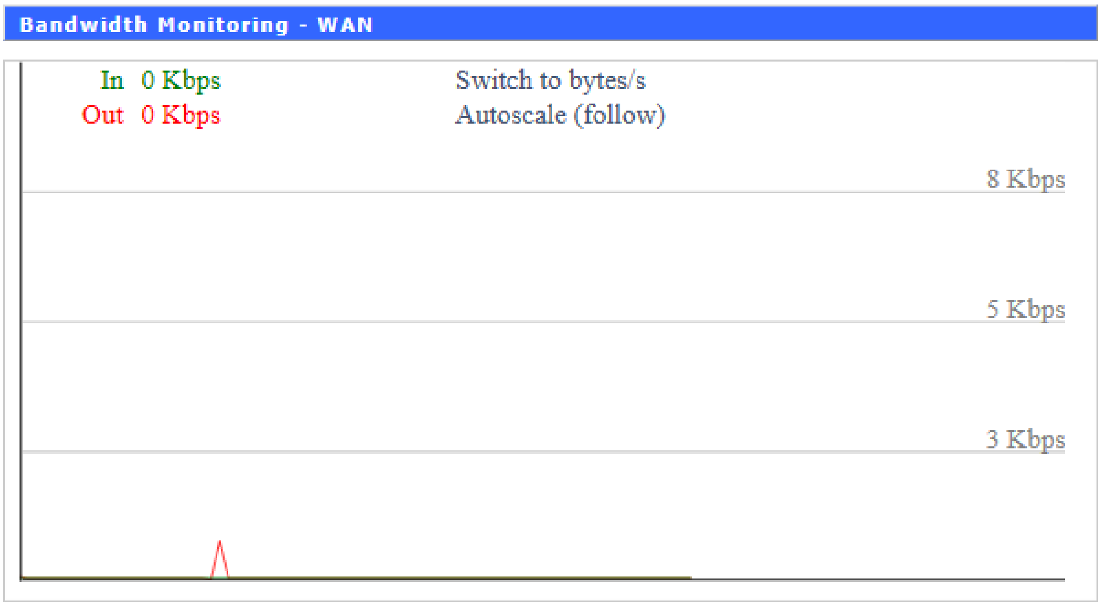
◆ **Bandwidth Monitoring - LAN**



Abscissa: Time (byte/s), you can switch to bit/s by click Switch to bytes/s

Ordinate: Speed Rate (Kbps), you can switch up or follow by click Autoscale (follow)

◆ **Bandwidth Monitoring - WAN**



Bandwidth Monitoring - WAN

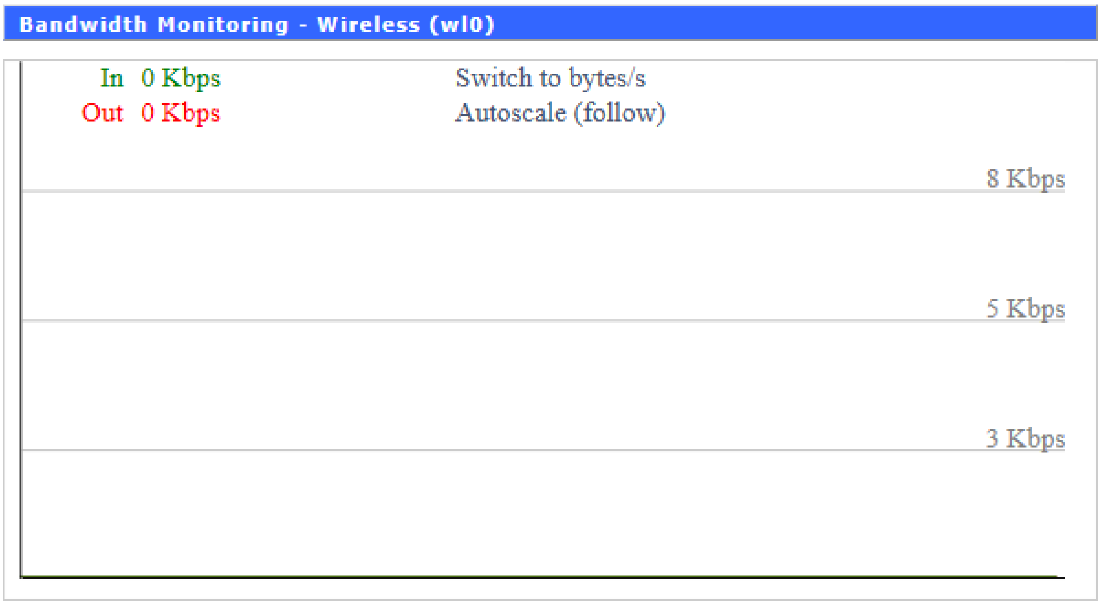
In 0 Kbps

Out 0 Kbps

Abscissa: Time (byte/s), you can switch to bit/s by click Switch to bytes/s

Ordinate: Speed Rate (Kbps), you can switch up or follow by click Autoscale (follow)

- **Bandwidth Monitoring – Wireless (wl0)**



Bandwidth Monitoring - Wireless (wl0)

In 0 Kbps

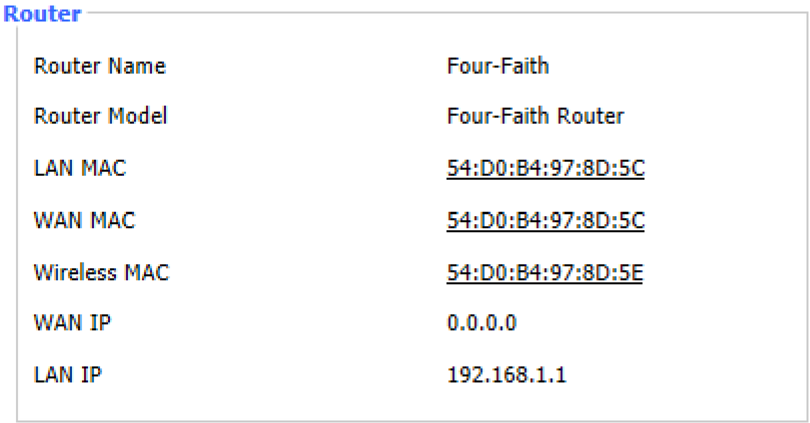
Out 0 Kbps

Abscissa: Time (byte/s), you can switch to bit/s by click Switch to bytes/s

Ordinate: Speed Rate (Kbps), you can switch up or follow by click Autoscale (follow)

3.3.11.6 System Info

- **Router**

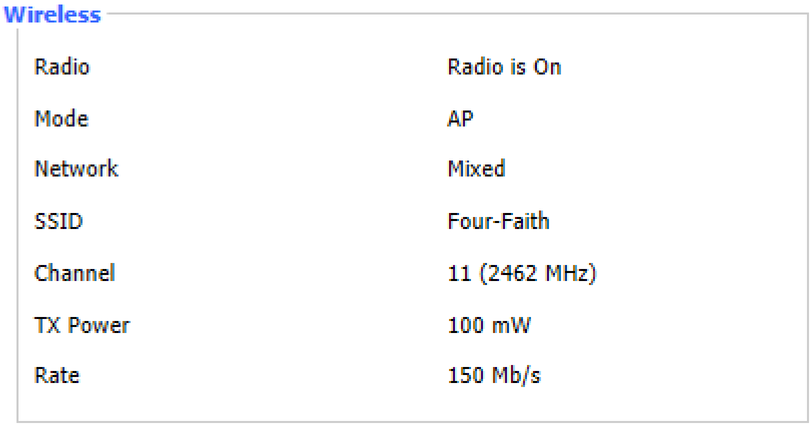


Router

Router Name	Four-Faith
Router Model	Four-Faith Router
LAN MAC	54:D0:B4:97:8D:5C
WAN MAC	54:D0:B4:97:8D:5C
Wireless MAC	54:D0:B4:97:8D:5E
WAN IP	0.0.0.0
LAN IP	192.168.1.1

Item	Parameters	Description
Router Name	-	Router's name
Router Model	-	Router's model
LAN MAC	-	The MAC address of LAN
WAN MAC	-	The MAC address of WAN
Wireless MAC	-	The MAC address of wireless
WAN IP	-	The IP address of WAN
LAN IP		The IP address of LAN

- **Wireless**

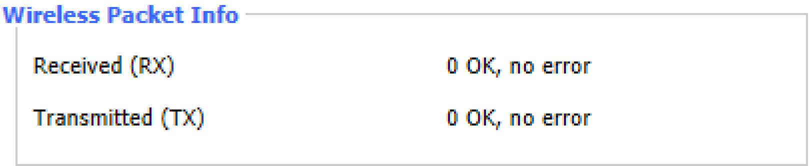


Wireless

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	Four-Faith
Channel	11 (2462 MHz)
TX Power	100 mW
Rate	150 Mb/s

Item	Parameters	Description
Radio	-	Wireless status
Mode	-	Wireless mode
Network	-	Wireless network mode
SSID		The name of wireless network
Channel		The channel of wireless network
TX Power		The Tx power of wireless
Rate		The speed rate of wireless

- **Wireless Packet Info**

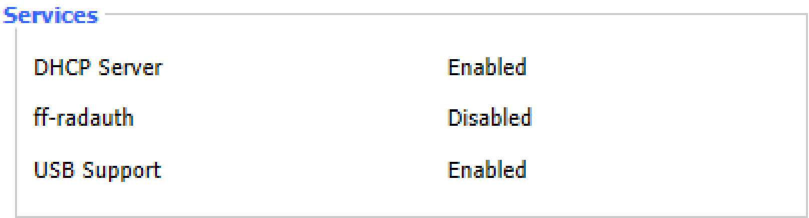


Wireless Packet Info

Received (RX)	0 OK, no error
Transmitted (TX)	0 OK, no error

Item	Parameters	Description
Received (RX)	-	Have been received packets
Transmitted (TX)	-	Have been transmitted packets

- **Service**

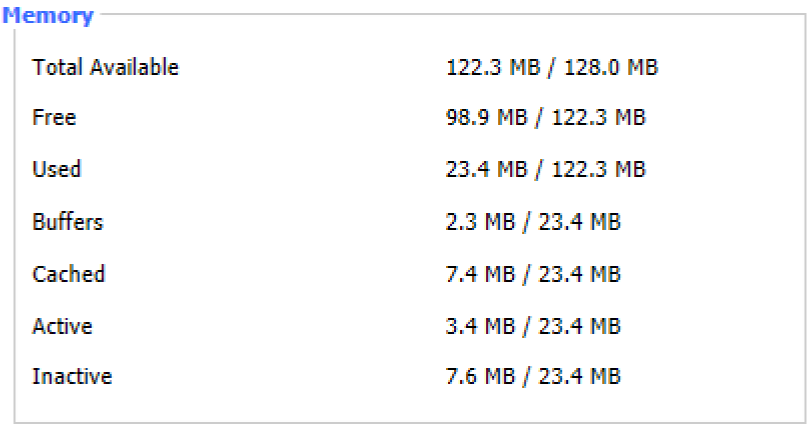


Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Enabled

Item	Parameters	Description
DHCP Server	-	Whether enable DHCP server
ff-radauth	-	Whether enable ff-radauth
USB Support	-	Whether enable USB support

- **Memory**

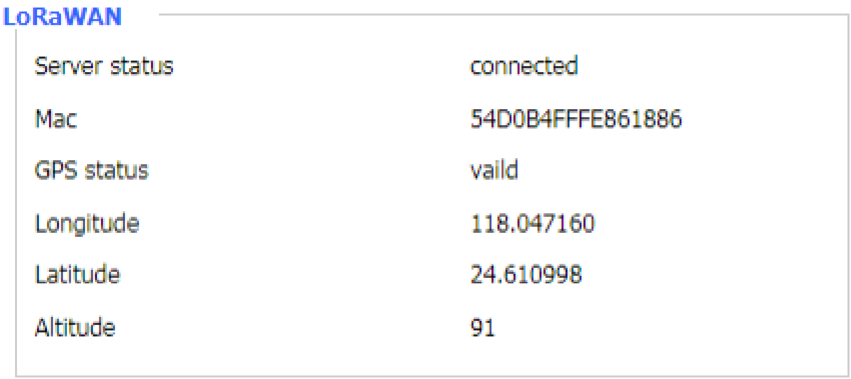


Memory

Total Available	122.3 MB / 128.0 MB
Free	98.9 MB / 122.3 MB
Used	23.4 MB / 122.3 MB
Buffers	2.3 MB / 23.4 MB
Cached	7.4 MB / 23.4 MB
Active	3.4 MB / 23.4 MB
Inactive	7.6 MB / 23.4 MB

Item	Parameters	Description
Total Available	-	All available RAM size
Free	-	Unused memory. The device will restart when it less than 500KB
Used	-	Used memory.
Buffers	-	Buffer memory
Cached	-	Cache memory
Active	-	The size of buffer or cache page file in active state
Inactive	-	The size of buffer or cache page file in inactive state

- **LoRaWAN**



LoRaWAN

Server status	connected
Mac	54D0B4FFFE861886
GPS status	vaild
Longitude	118.047160
Latitude	24.610998
Altitude	91

Item	Parameters	Description
Server status	-	Show the LoRaWAN server connection status
Mac	-	The device Mac address
GPS status	-	Show the GPS status
Longitude	-	Show current longitude of F8926-GW
Latitude	-	Show current latitude of F8926-GW
Altitude	-	Show current altitude of F8926-GW