FOUR FAITH

F-G100 Series Smart Gateway

USER MANUAL

V2.0.1

Xiamen Four-Faith Communication Technology Co., Ltd.

Copyright Notice

Trademark Notice

Content

1. F-G100 Introduction

1.1 Overview

Four-Faith Industrial Gateway F-G100 is an intelligent 3G/4G gateway to provide the necessary M2M applications for all types of terminals.

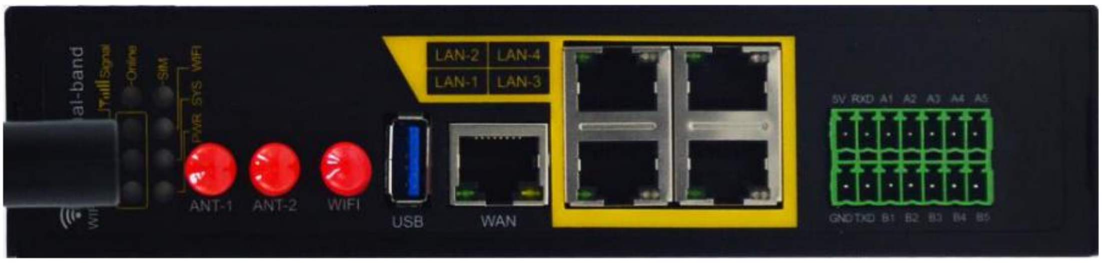
It adopts high-powered industrial 32-bits CPU and is embedded with real time operating system. It supports RS232 (or RS485/RS422), Ethernet and WIFI port that can conveniently and transparently connect the device to a cellular network, allowing you to connect to your existing serial, Ethernet and WIFI devices with only basic configuration.

It has been widely used on M2M fields, such as self-service terminal industry, intelligent transportation, smart grid, smart home, industrial automation, intelligent building, public security, fire protection, environment protection, telemetry, finance, POS, water supply, meteorology, remote sensing, digital medical, military, space exploration, agriculture, forestry, petrochemical and other fields etc..

1.2 Packing List

Parameter	Quantity	Remarks
Router	1	With SIM Slot
Cellular antenna(Male SMA)	2	1m cable
WIFI antenna(Female SMA)	2	Stick,20cm
Power Adapter	1	1m or 1.5m
Ethernet Cable	1	
Serial Port Cable	1	
Power Connection Terminal	1	2 pins
IO Connection Terminal	2	3 pins
Serial Connection Terminal	2	7 pins
Certification card	1	
Maintenance card	1	
DIN Rail	1	Router installation way, can remove
Fixed Plate	2	Optional, router installation way
CD	1	Optional
Warranty Card	1	

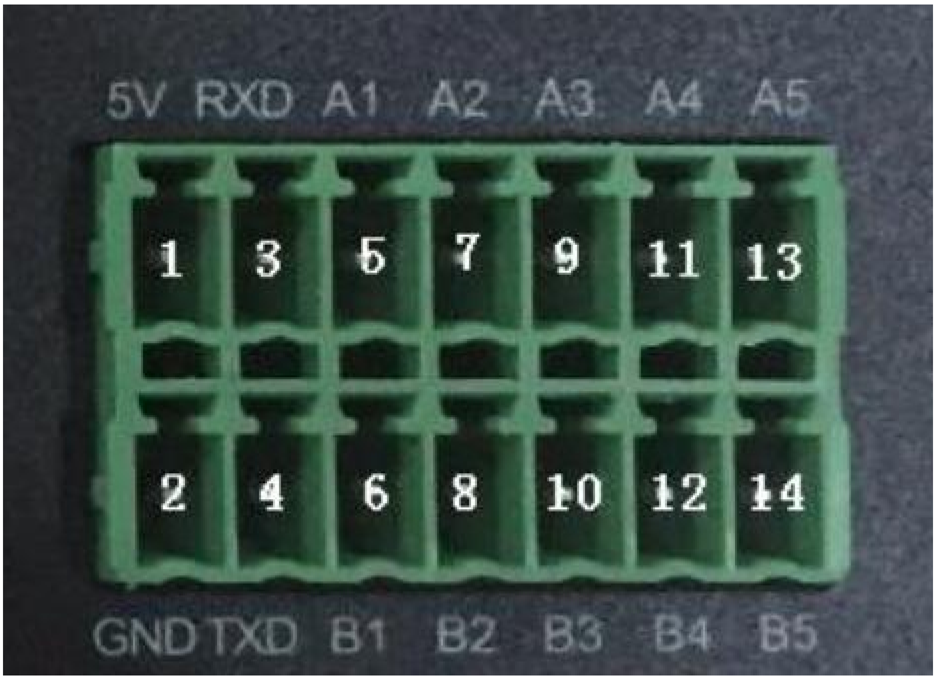
1.3 Panel Introduction



LAN/ WAN port for Ethernet cable connecction. Insert Ethernet cable to any of 4 LAN ports.

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

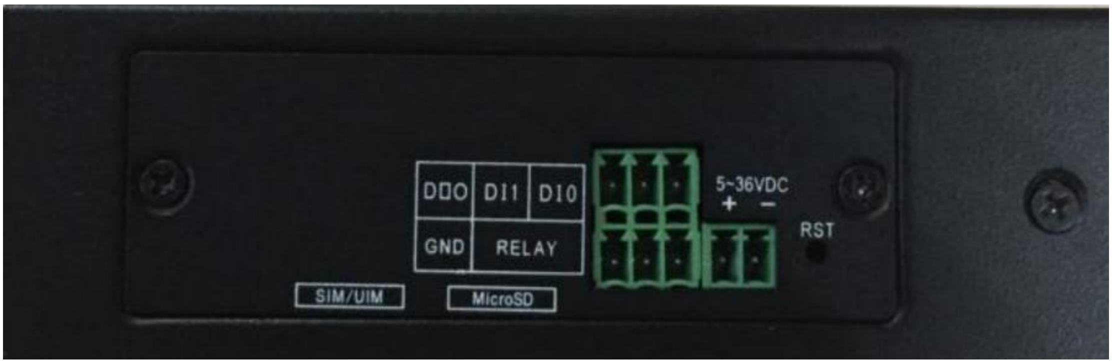
RS232/RS485 connection for serial device.



Pin	Definition	Description	Input/Output
1	5V	5V source(1W)	Output
2	GND	Power GND, GND for rs232	Output&Input
3	RXD	Receive Data for RS232,com1	Input
4	TXD	Send Data for RS232, com1	Output
5	A1	RS485,com1	Input&Output

6	B1	RS485,com1	Input&Output
7	A2	RS485,com2	Input&Output
8	B2	RS485,com2	Input&Output
9	A3	RS485,com3	Input&Output
10	B3	RS485,com3	Input&Output
11	A4	RS485,com4	Input&Output
12	B4	RS485,com4	Input&Output
13	A5	RS485, com5	Input&Output
14	B5	RS485, com5	Input&Output

Power interface and IO interface



Pin	Description	Input/Output
DO0	Digital Output 0	Output
DI1	Digital Input 1	Input
DI0	Digital Input 0	Input
GND	GND for DI &DO & Relay	Input &Output
RELAY	Relay output	Output
+	Power input +	Input
-	Power input -	Input

Note:

1. Please connect GND with - for digital input, digital output and relay output.
2. There is no voltage reading if using multiple meter to check digital output and relay output. DO0 and RELAY are dry connect(open or close status) but RELAY is dry connect with GND to power GND.

1.4 LED Status

Parameter	On/Blinking	Off	Remarks
PWR	Router is powered	Power isn't powered	
SYS	Router is running well	Router is not running	On means blinking
WIFI	WIFI is enable	WIFI is disable	
SIM	SIM card is inserted	SIM card is not inserted	
Signal	3 means good signal; 2 means not good enough ;	No Signal	

	1 means bad signal		
Online	Router has wan IP	Router cannot access internet	On doesn’t means can access internet
WAN	WAN port is connected /communication	WAN port is not connected	On means blinking
LAN-1~LAN-4	LAN port is connected / communication	LAN port is not connected	On means blinking

Note:

1. It may be different for different firmware version(two sim version may be different).

2.PWR and SYS led lights must be on(blinking) if router is running well. There must have issues for router if PWR or SYS is off (not blinking)

3.In some cases, router Online LED is on but router cannot access internet, such as private APN SIM card or SIM/WAN network cannot access internet.

1.5 Reset Button

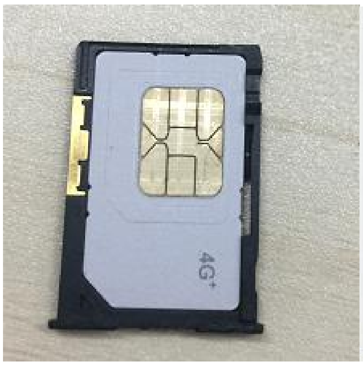
F-G100 has a reset button, RST, can make F-G100 to be factory default. Using something sharp like a pen to press RST for about 15 seconds until F-G100 all LED lights to be off. (Off status will be last for about 10s then on again)

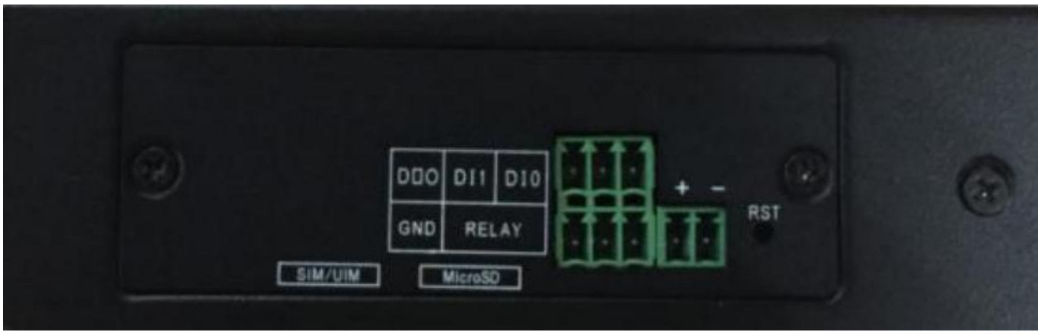
1.6 SIM Card Installation

Need to make sim card chip outside, like picture.

And reverse SIM tray, make it face down(SIM will be WIS), check picture.

Can screw the sheet to cover SIM card for safety issue.



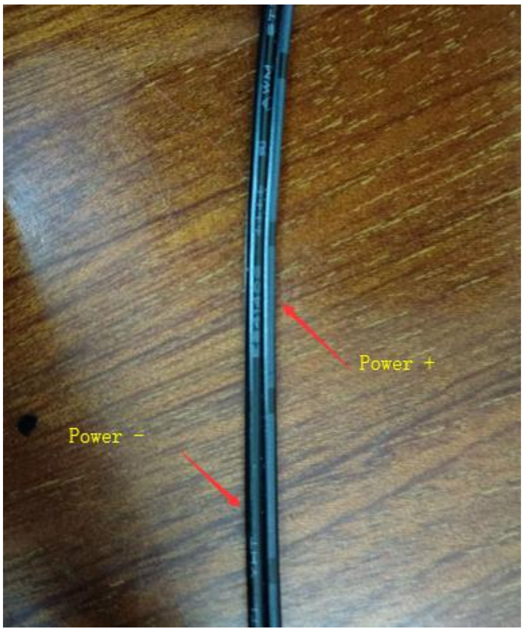


1.7 Antenna Connection

Suggest to connect all antennas to get better signal and make router working better, also suggest to place cellular antennas to something icon, such as router box. Must connect ANT-1 for sim card internet.
Note: It must to connect ANT-1 if using SIM card internet.

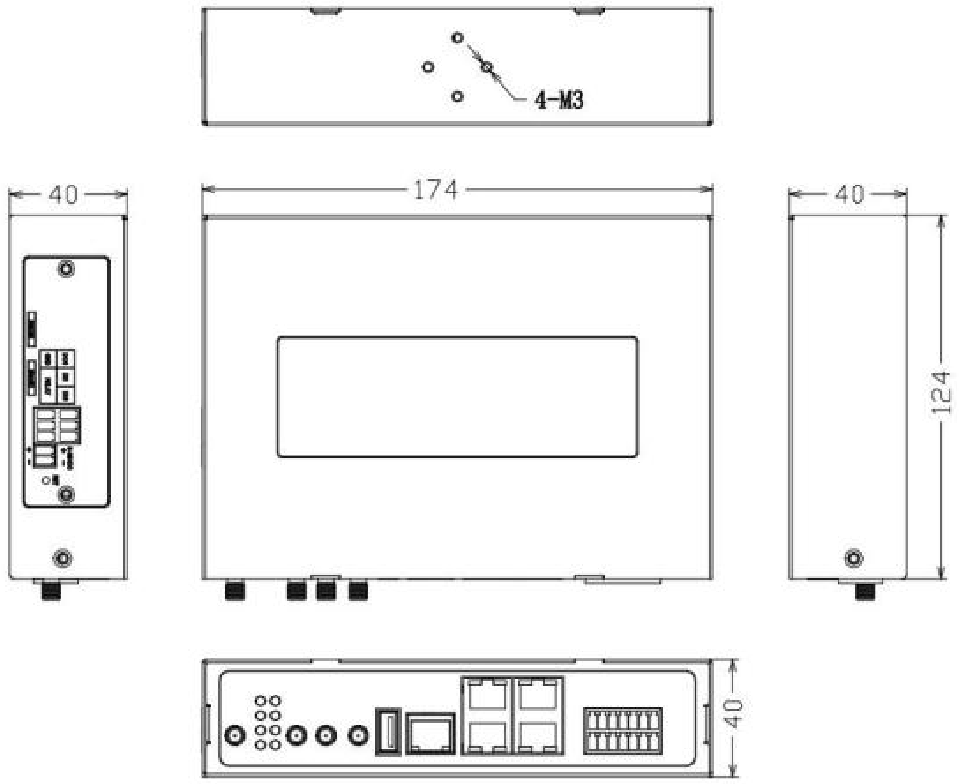
1.8 Power Cable Connection

Power cable has two cables, one cable is black with white, this is power pin, need to connect to left of power terminal; another cable is black with words, this is GND pin, need to connect to right of power terminal.
Suggest to use standard power adapter provided to power F-G100, to provide a stable power environment. Also can use 9~36VDC power to power it directly. Please make sure ripple is not more than 300mV and instantaneous voltage is not more than 36VDC if using 9~36VDC power.

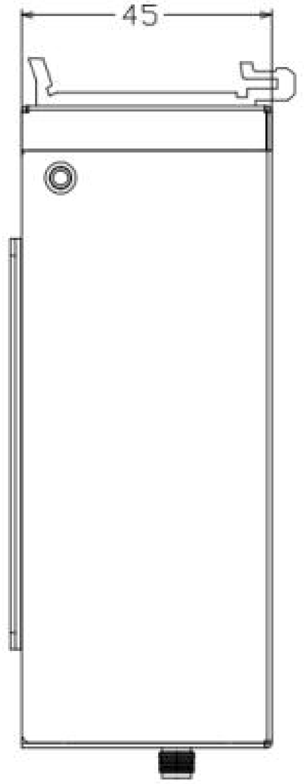


1.9 Installation

F-G100 size:

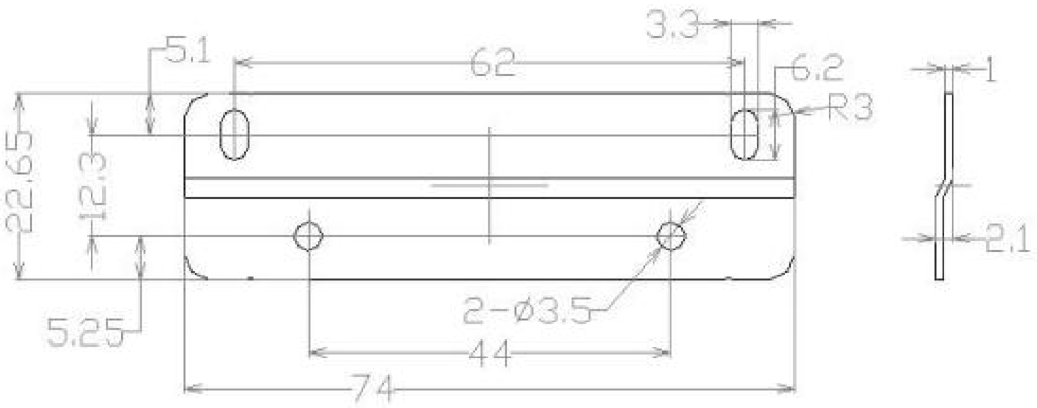


DIN Rail:



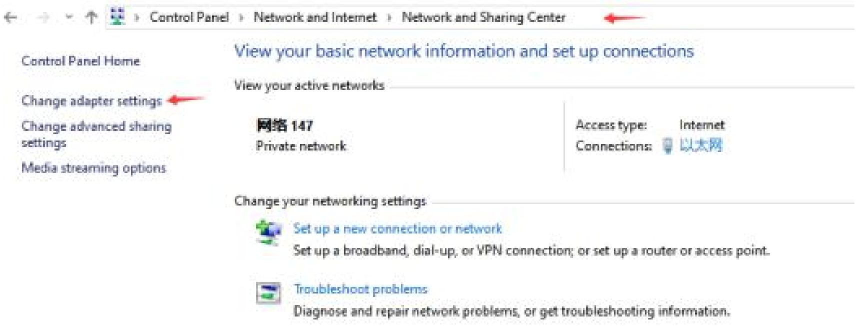
Fixed Plate:

Screw specification for installation is M3*5MM countersunk head screws(black).



1.10 Connection For Configuration

Make PC Ethernet port connect with F-G100 LAN port(any LAN port). Can connect via WIFI if PC doesn't have Ethernet port.
Make PC to get IP automatically from F-G100.


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

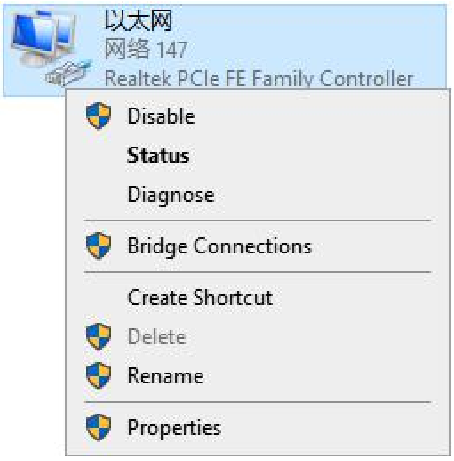
网络 147
Private network

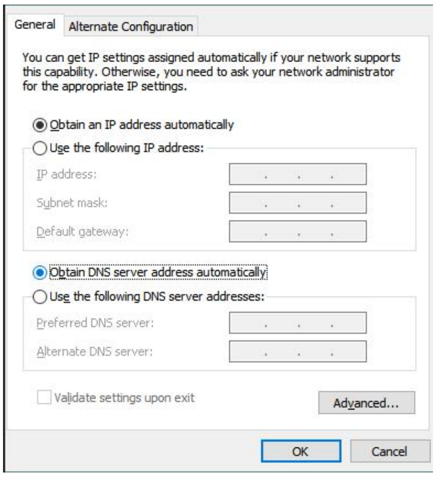
Access type: Internet
Connections: 以太网

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.




General | Alternate Configuration

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

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

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

□ Validate settings upon exit

Note: May need disable laptop firewall or put configure link

3. Web Configuration

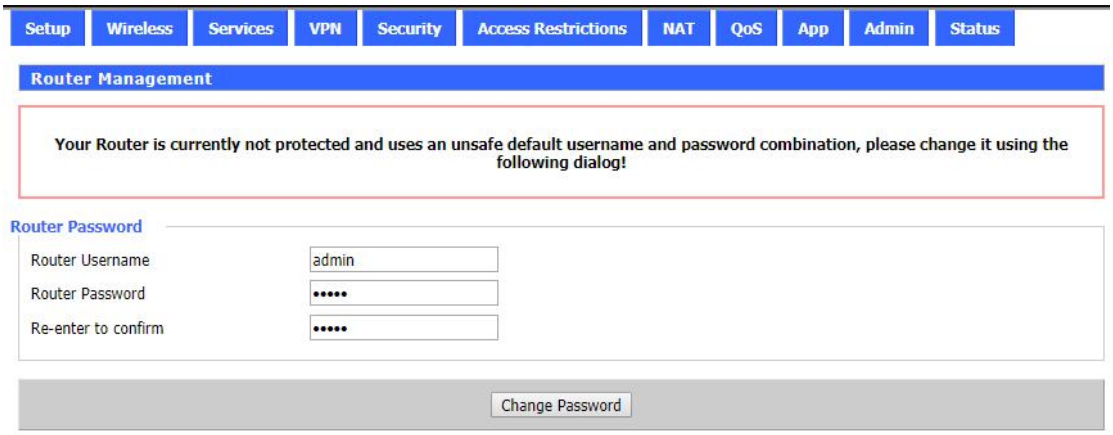
Open web browser with 192.168.4.1 to access router web configure page. First page you will see is change password page.

Router user name is admin, password is admin by default.

Click Change Password button if no need to change; fill the user name and password as you want if need to change password.

It needs to fill user name and password next time for login, default user name is admin, password is admin.

Note: please remember user name and password , no other way to enter router configure page except press reset button (router will loss configuration) to reset router to factory default if you forget user name and password later.



Router Management

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

Router Password

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

There have Setup, Wireless, Service, VPN, Security, Access Restrictions, NAT, QoS, App, Admin, Status main menu for router configuration.

Here is summary for every main menu:

Setup: make router online/ddns/ add static routing; make Vlan.

Wireless: Set WIFI SSID/ set WIFI password.

Services: Open log/ Enable USB/ Enable FTP

VPN: Configure PPTP/L2TP/IPsec/ Openvpn/ GRE server/Client;

Security: Disable firewall.

Access Restrictions: set WAN access policy/ URL filter/MAC filter/Package filter

NAT: Port Forwarding/ DMZ/Virtual IP

QoS: set QoS

App: set communication gateway

Admin: Set router to connect cloud platform/upgrade firmware/set factory default/backup and restore configuration file

Status: check router status.

3.1 Setup

Setup includes Basic Setup, DDNS,MAC Address Clone, Advanced Routing, Vlans, and Networking sub-menu.

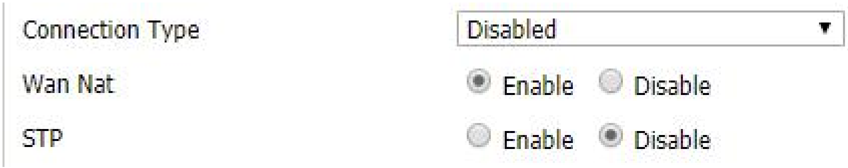
3.1.1 Basic Setup

WAN Connection Type

Connection Type

Parameter	Description	Remarks
Disable	Disable router for internet connection including	
Static IP	Router use wan port for internet access and set wan port with a fixed IP	
Automatic Configuration - DHCP	Router use wan port for internet access and get wan IP automatically	
Dhcp-4G	Router will use dhcp way for dail up	Default way
PPPoE	ADSL way to make router online	
3G/UMTS4G/LTE	Router will use ppp way for dail up	

Disable

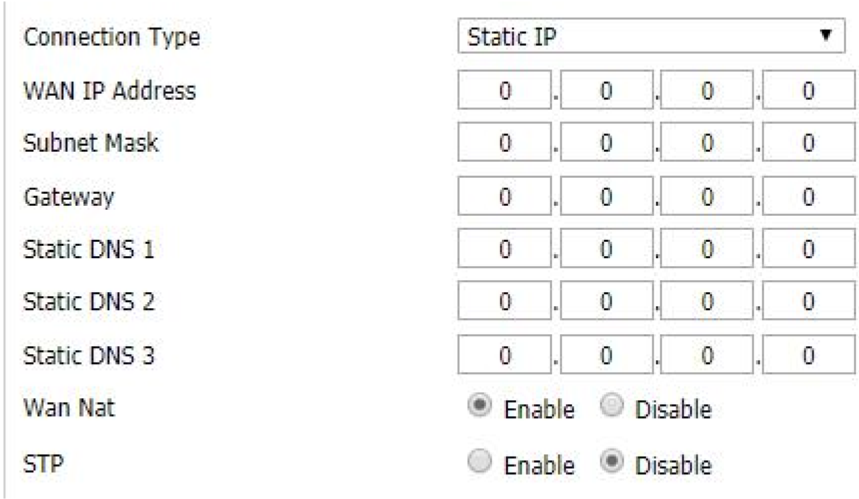


Connection Type	Disabled ▼
Wan Nat	● Enable ○ Disable
STP	○ Enable ● Disable

Wan Nat: WAN to LAN NAT. Need to enable WAN Nat to make traffic pass to router LAN.

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

Static IP



Connection Type	Static IP ▼
WAN IP Address	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0
Gateway	0 . 0 . 0 . 0
Static DNS 1	0 . 0 . 0 . 0
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
Wan Nat	● Enable ○ Disable
STP	○ Enable ● Disable

WAN IP Address: Set a WAN IP from above router or ISP.

Subnet Mask: sub-mask for above wan ip address.

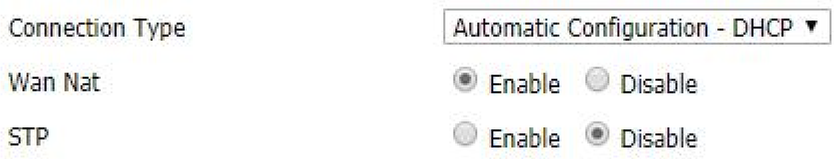
Gateway: Gateway IP for above wan ip address.

Static DNS 1/Static DNS 2/Static DNS 3: DNS IP, use customer own DNS IP or ISP DNS IP.

Wan Nat: Same with Wan Nat under Disable.

STP:Same with Wan Nat under Disable.

Automatic Configuration - DHCP



Connection Type: Automatic Configuration - DHCP ▼

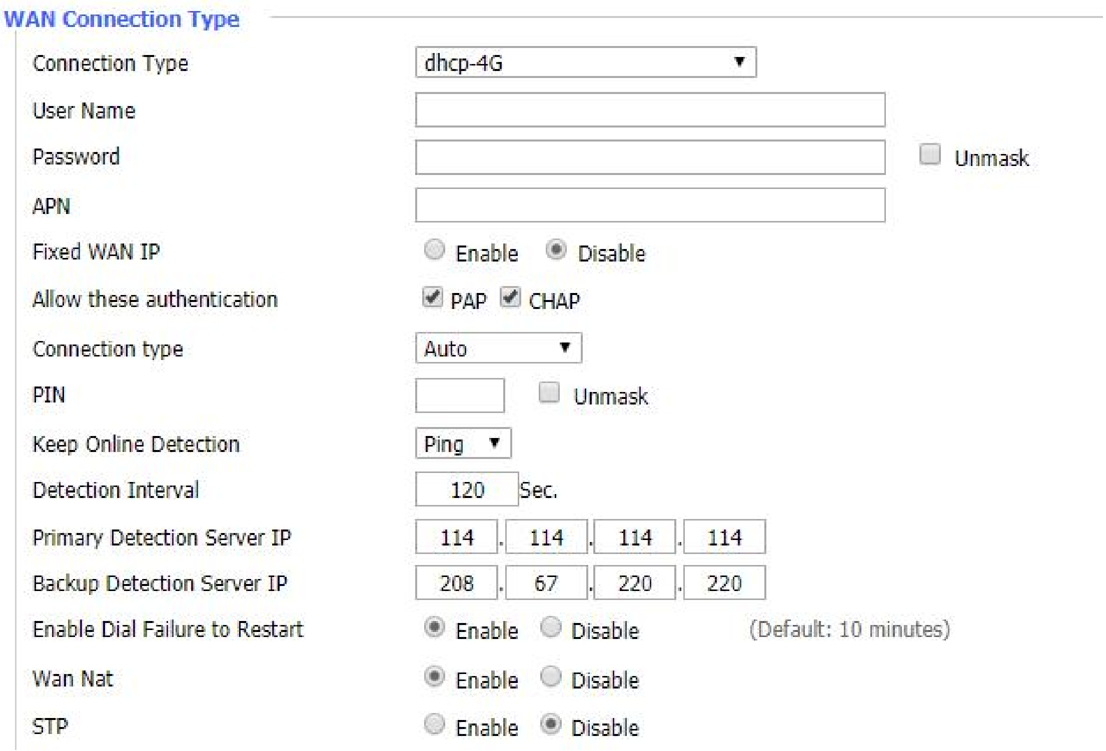
Wan Nat: ● Enable ○ Disable

STP: ○ Enable ● Disable

Wan Nat: Same with Wan Nat under Disable.

STP:Same with Wan Nat under Disable.

Dhcp-4G



WAN Connection Type

Connection Type: dhcp-4G ▼

User Name:

Password: □ Unmask

APN:

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

User Name: SIM card user name, get from ISP.

Password: SIM card password , get from ISP.

APN:SIM card APN, get from ISP.

Fixed WAN IP: A fixed wan IP if sim car has.

Allow those authentication: PAP or CHAP, chosen depends on ISP authentication, usually choose both by default.

Connection type:

Parameter	Description	Remarks
Auto	Will choose network type automatically	By default
Force 3G	Make router force to use 3G	
Force 2G	Make router force to use 2G	
Prefer 3G	Router will choose 3G to use first	
Prefer 2G	Router will choose 2G to use first	
Only WCDMA	Router can only use WCDMA (3g) network	
Force 4G	Make router force to use 4G	
2G->4G	Router will communicate with ISP, via 2G auxiliary , then jump to 4G network	

4G->2G	Router will communicate with ISP, via 4G auxiliary, then jump to 2G network	
3G->4G	Router will communicate with ISP, via 3G auxiliary, then jump to 4G network	
4G->3G	Router will communicate with ISP, via 4G auxiliary, then jump to 3G network	
EVDO	Router can only use EVDO (2g) network	

Note: Connection type may be different for different model and different module inside.

PIN: SIM card pin code.

Keep Online Detection：

Parameter	Description	Remarks
None	No keep online detection	
Ping	Ping detection server ip to do keep online detection	By Default
Route	Route to detection server ip to do keep online detection	
TCP	TCP connection to detection server IP and port to do keep online check	

Detection Interval: ping/route/tcp way for detection check interval.

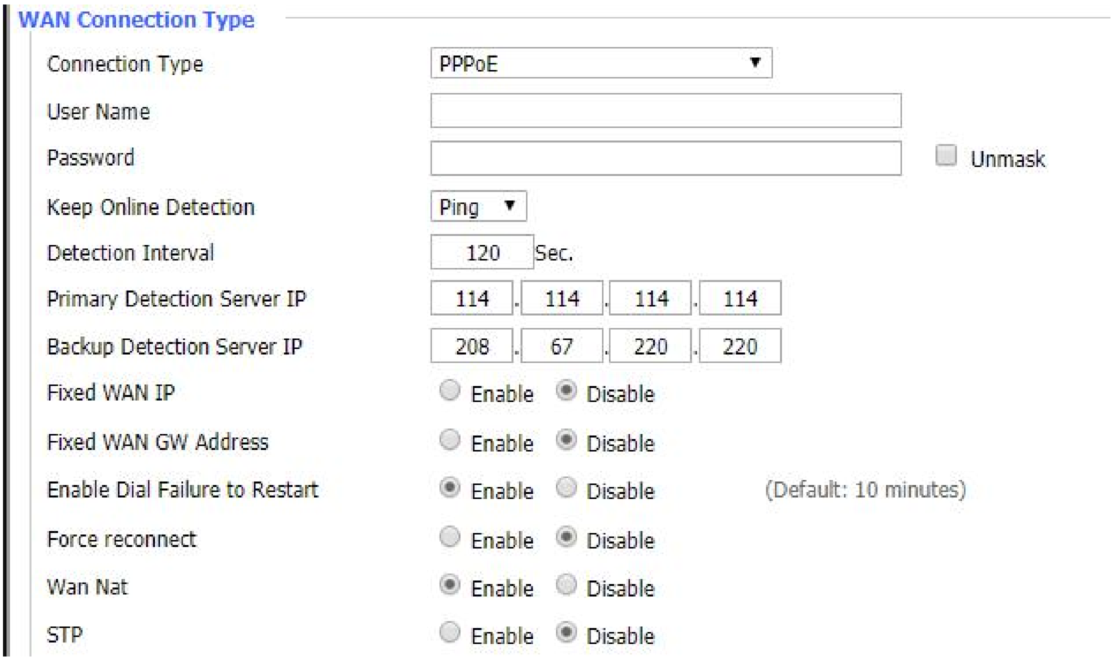
Primary Detection Server IP/Backup Detection Server IP: A detection server IP that SIM can reach, will use primary one first, then use backup one, primary IP should be different from backup IP.

Enable Dail Failure to Restart:

WAN Nat:Same with Wan Nat under Disable.

STP:Same with STP under Disable.

PPPoE



WAN Connection Type

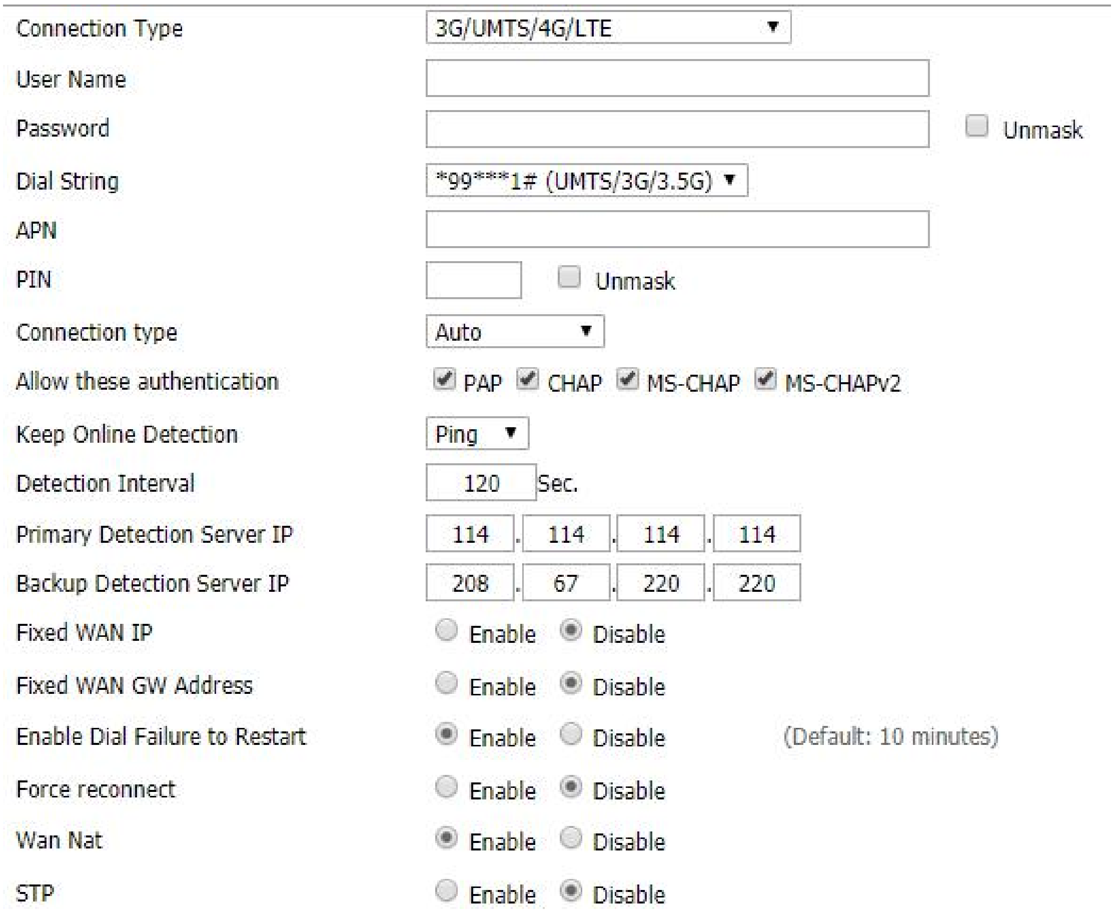
Connection Type	PPPoE ▼	
User Name		
Password		□ Unmask
Keep Online Detection	Ping ▼	
Detection Interval	120 Sec.	
Primary Detection Server IP	114 . 114 . 114 . 114	
Backup Detection Server IP	208 . 67 . 220 . 220	
Fixed WAN IP	○ Enable ● Disable	
Fixed WAN GW Address	○ Enable ● Disable	
Enable Dial Failure to Restart	● Enable ○ Disable	(Default: 10 minutes)
Force reconnect	○ Enable ● Disable	
Wan Nat	● Enable ○ Disable	
STP	○ Enable ● Disable	

User Name: User name for ADSL.

Password: Password for ADSL.

Others are same with dhcp-4G.

3G/UMTS/4G/LTE



Connection Type	3G/UMTS/4G/LTE ▼	
User Name		
Password		□ Unmask
Dial String	*99***1# (UMTS/3G/3.5G) ▼	
APN		
PIN	□ Unmask	
Connection type	Auto ▼	
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	

Dail String : a dial number for PPP dail-up, usually *99***1# or *99#.

Others are same with dhcp-4G.

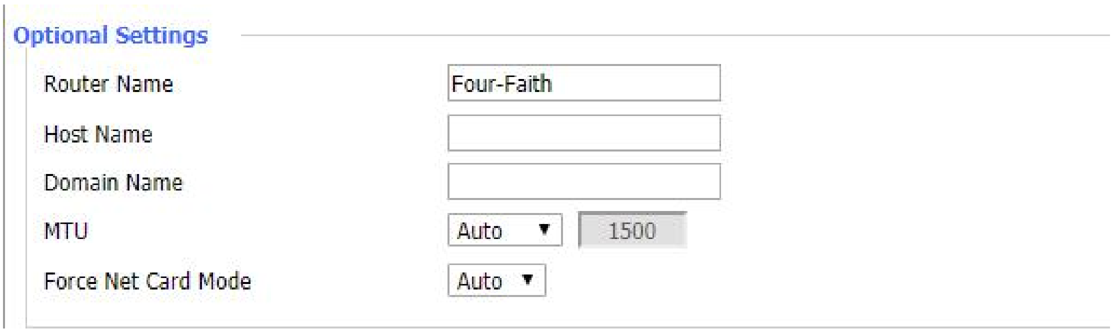
Optional Settings

Router Name: Router name.

Host Name/Domain Name: Some ISP will need host name and domain name to identify router, leave as empty for most cases.

MTU:auto (1500) and manual (1200-1492 in PPPOE/PPTP/L2TP mode, 576-16320 in other modes)

Force Net Card Mode: Usually as Auto.

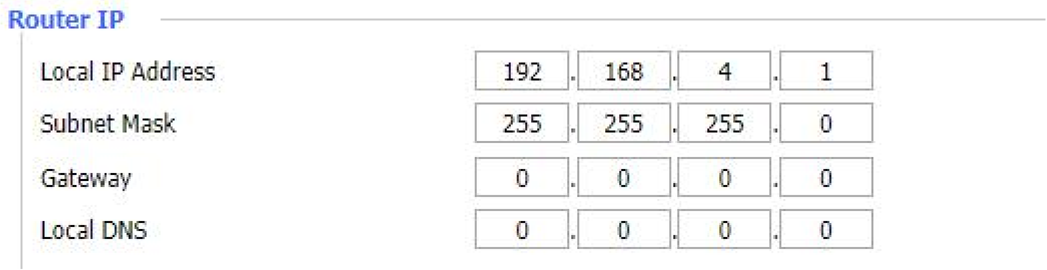


Optional Settings

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

Router IP

Local IP Address: Router IP, 192.168.4.1 by default.
Subnet Mask: Router LAN network sub-net mask, 255.255.255.0 by default.
Gateway: Router gateway, 0.0.0.0 means gateway IP will be router IP.
Local DNS: Router DNS IP, 0.0.0.0 means router will use DNS from ISP by default.



Router IP

Local IP Address 192 . 168 . 4 . 1
Subnet Mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
Local DNS 0 . 0 . 0 . 0

Network Address Server Settings(SHCP)

DHCP Type:

Parameter	Description	Remarks
DHCP Server	Assign IP to LAN devices, LAN will get IP from router automatically	Default enabled; LAN devices including LAN port users and WIFI users, same as followings
DHCP Forwarder	Used to forward the DHCP packets directly	

DHCP Server

Start IP Address: DHCP server start IP address, LAN IP will start with this IP. Cannot be 192.168.1.1 as it is router IP. Default will begin with 100.

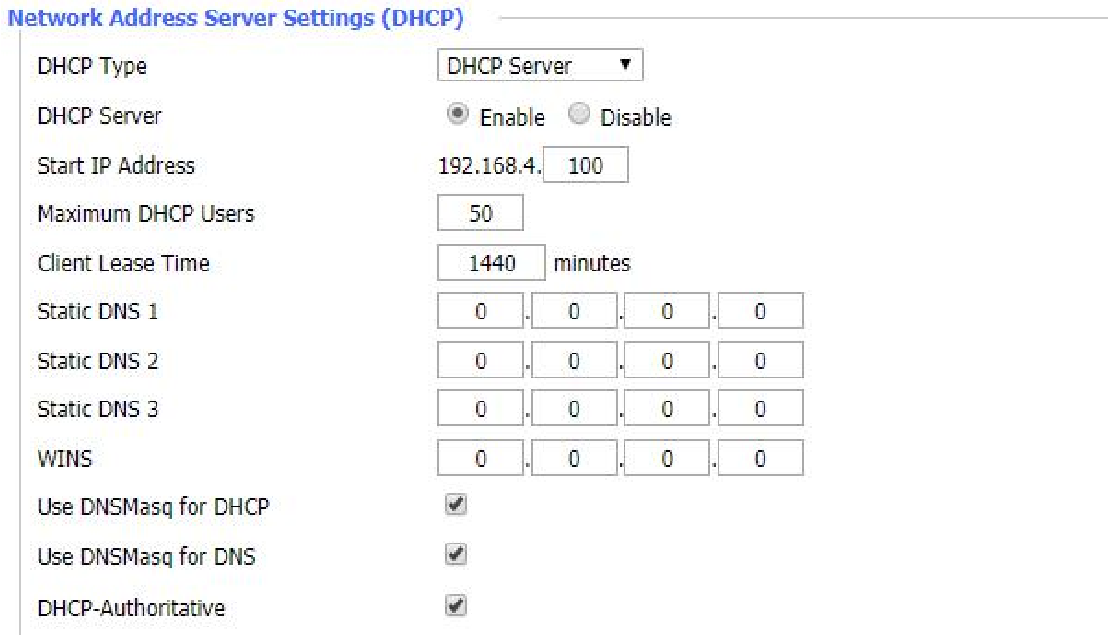
Maximum DHCP Users: Maximum LAN user number, default is 50 users.

Client Lease Time: Client Lease Time is the time that LAN users allowed to connect to router with current dynamic IP address. Unit is minute, default is 1440 minute.

Static DNS 1/Static DNS 2/Static DNS 3：DNS IP, use customer own DNS IP or ISP DNS IP. Default as 0.0.0.0, means user SIM card DNS.

WINS：Windows Internet Name Service.

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

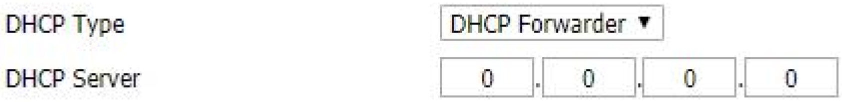


Network Address Server Settings (DHCP)

DHCP Type	DHCP Server ▼
DHCP Server	● Enable ○ Disable
Start IP Address	192.168.4. 100
Maximum DHCP Users	50
Client Lease Time	1440 minutes
Static DNS 1	0 . 0 . 0 . 0
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
WINS	0 . 0 . 0 . 0
Use DNSMasq for DHCP	☑
Use DNSMasq for DNS	☑
DHCP-Authoritative	☑

DHCP Forwarder

DHCP Server： set DHCP server IP, F-G100 will forward DHCP data from/to this server IP.



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

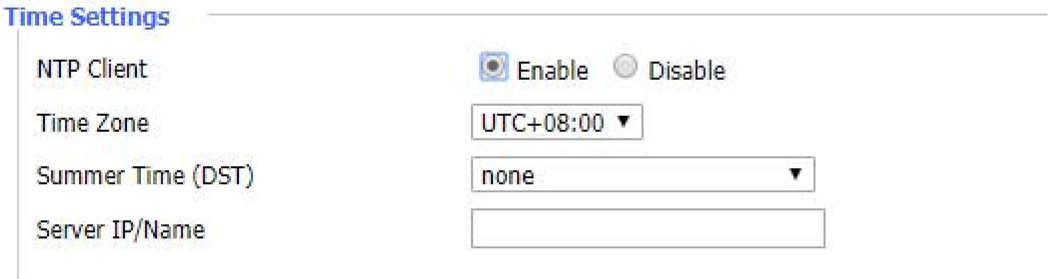
Time Settings

NTP Client: enable means router get time from NTP server; disable means router will use router RTC time.

Time Zone: Choose time zone.

Summer Time(DST):Set summer time or not.

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

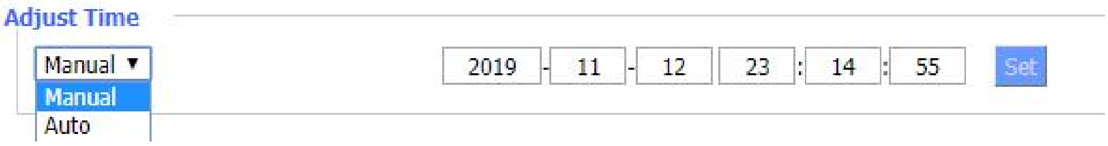


Time Settings

NTP Client	● Enable ○ Disable
Time Zone	UTC+08:00 ▼
Summer Time (DST)	none ▼
Server IP/Name	

Adjust Time

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



Adjust Time

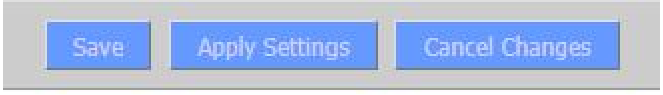
Manual ▼ 2019 - 11 - 12 23 : 14 : 55

Save: Click to save changes or settings.

Apply Settings: Click to apply changes or settings, changes or settings will work after clicking this button.

Cancel Changes: Click to delete changes or settings.

Note: Save , Apply Settings and Cancel Changes these three buttons are same function.

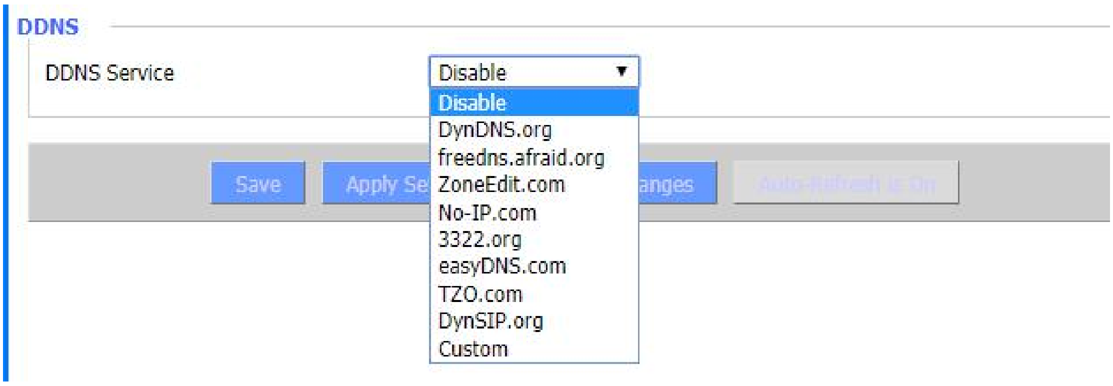


3.1.2 DDNS

DDNS means dynamic domain name service. Will be used for public but dynamic IP, to fix dynamic IP to a domain name.

DDNS Service: Support DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP and Custom for DDNS services. Can choose custom to use if used DDNS service is not in the list.

Different DDNS services have similar parameters, just use 3322 to be an example for DDNS service.


DDNS

DDNS Service: Disable

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

Password: password for the user name, up to 32 characters.

Host Name: users register in DDNS server, no limit.

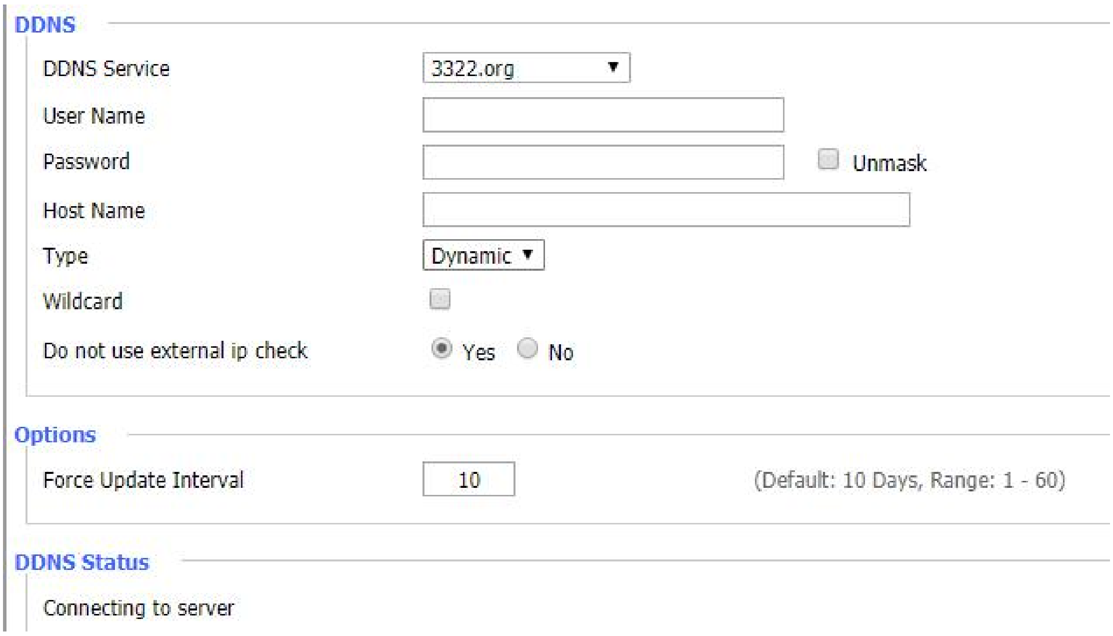
Type: depends on the server.

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

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

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

DDNS Status: shows DDNS connection status.



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)

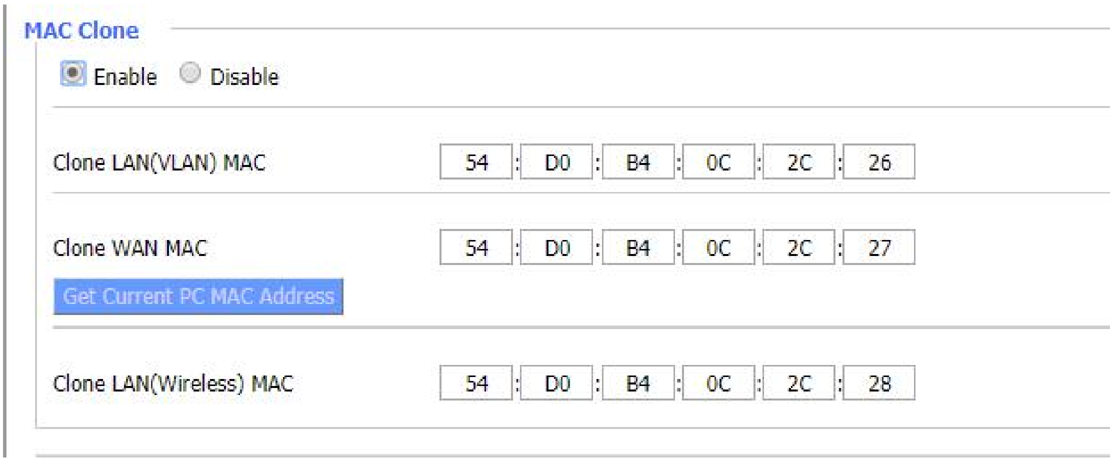
DDNS Status

Connecting to server

3.1.3 MAC Address Clone

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

Clone MAC address can be done for three parts: Clone LAN MAC, Clone WAN MAC, Clone Wireless MAC.



MAC Clone

● Enable ○ Disable

Clone LAN(VLAN) MAC: 54 : D0 : B4 : 0C : 2C : 26

Clone WAN MAC: 54 : D0 : B4 : 0C : 2C : 27

Clone LAN(Wireless) MAC: 54 : D0 : B4 : 0C : 2C : 28

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

3.1.4 Advanced Routing

Operating Mode

Parameter	Description	Remarks
Gateway	Choose Gateway if this Router is host users' Internet connection	

BGP	Choose BGP if need to use BGp	
RIP2 Router	Choose RIP2 Router if need to use RIP	
OSPF Router	Choose OSPF router if need to use OSPF	
Router	Choose Router if another router exists on their network	

Note: There may be different options for different version.

Select set number: 1-50

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

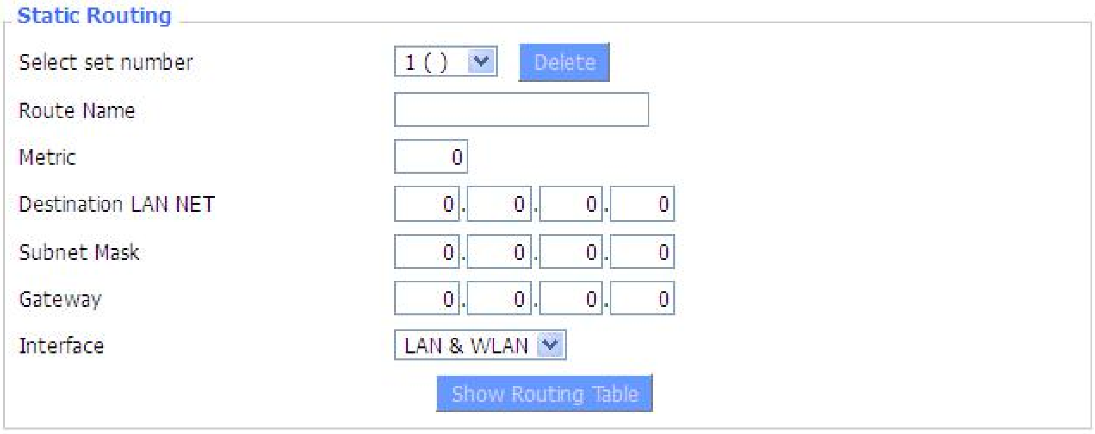
Metric: 0-9999

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

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

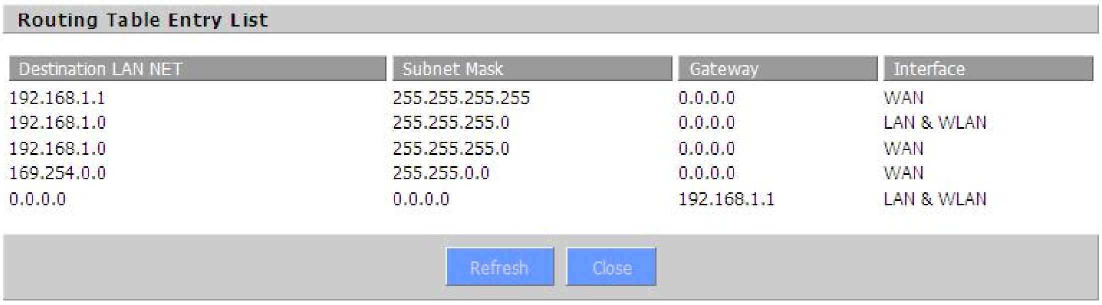
Gateway: IP address of the gateway device that allows for contact between the Router and the network or host.

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



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

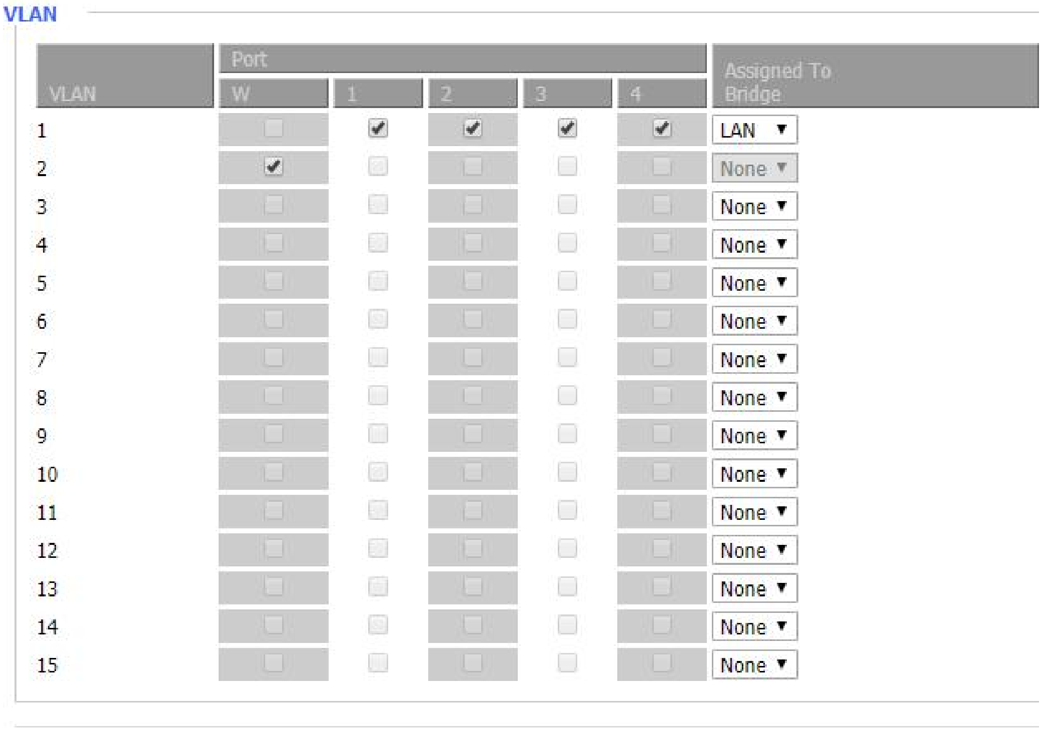
Show Routing Table



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

3.1.5 VlANs

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



VLAN

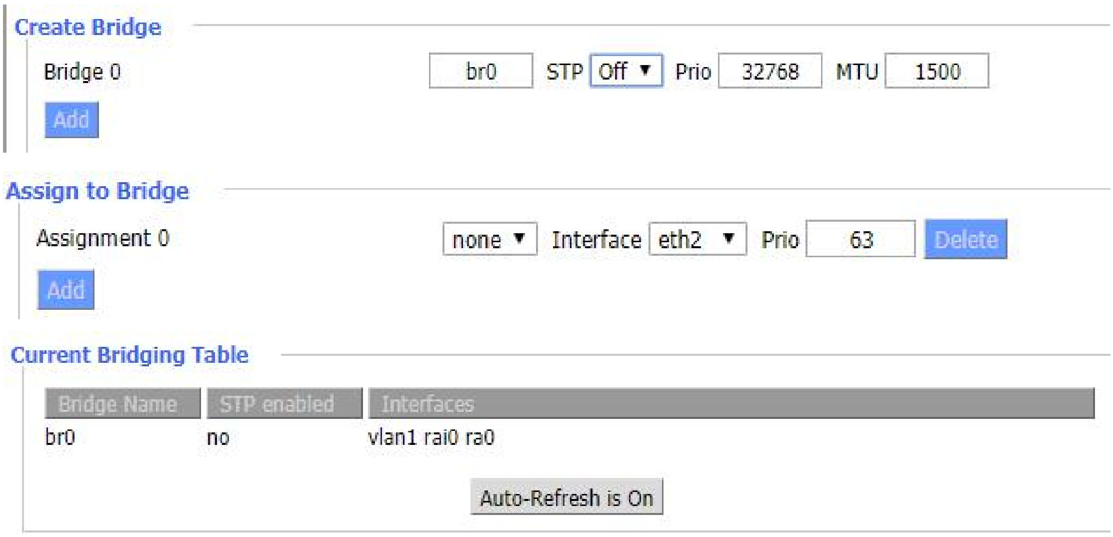
VLAN	Port					Assigned To Bridge
	W	1	2	3	4	
1	□	☑	☑	☑	☑	LAN ▾
2	☑	□	□	□	□	None ▾
3	□	□	□	□	□	None ▾
4	□	□	□	□	□	None ▾
5	□	□	□	□	□	None ▾
6	□	□	□	□	□	None ▾
7	□	□	□	□	□	None ▾
8	□	□	□	□	□	None ▾
9	□	□	□	□	□	None ▾
10	□	□	□	□	□	None ▾
11	□	□	□	□	□	None ▾
12	□	□	□	□	□	None ▾
13	□	□	□	□	□	None ▾
14	□	□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

3.1.6 Networking

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

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

Current Bridging Table: shows current bridging table.



Create Bridge

Bridge 0 — br0 — STP Off ▾ — Prio 32768 — MTU 1500

Assign to Bridge

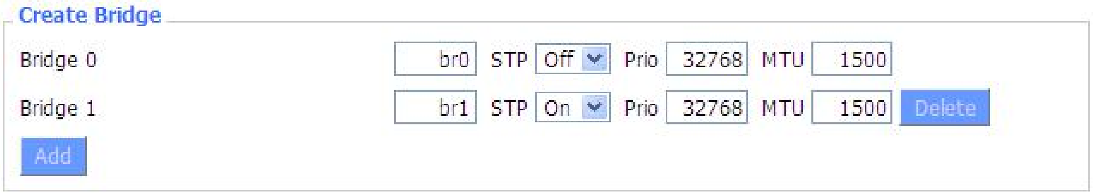
Assignment 0 — none ▾ — Interface eth2 ▾ — Prio 63

Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan1 rai0 ra0

Create steps as below:

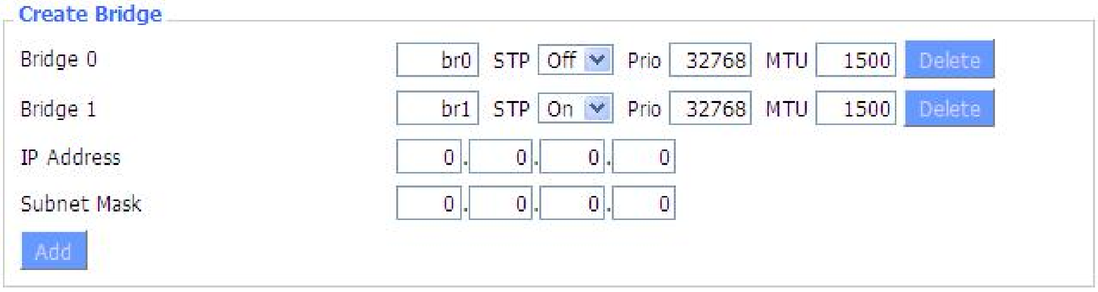
Click 'Add' to create a new bridge, configuration is as below:



Create Bridge

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

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

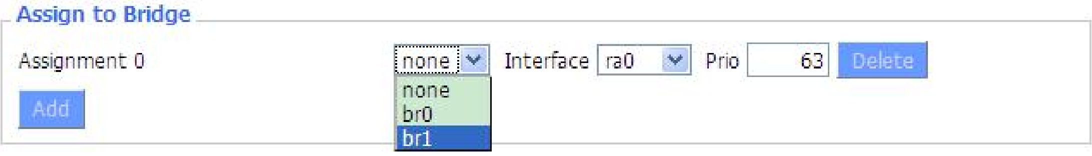


Create Bridge

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

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

Note: Only create a bride can apply it.



Assign to Bridge

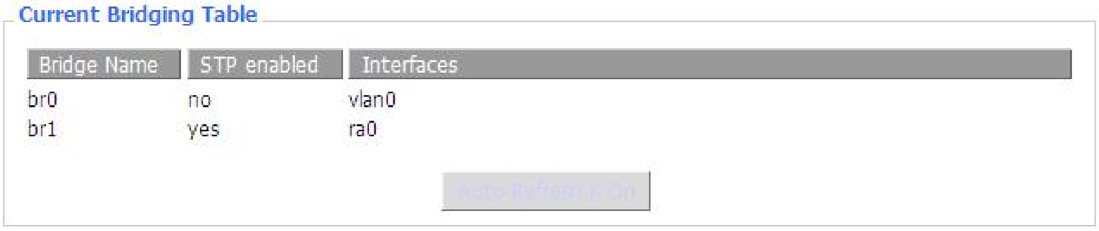
Assignment 0	none	Interface	ra0	Prio	63	Delete

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

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

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

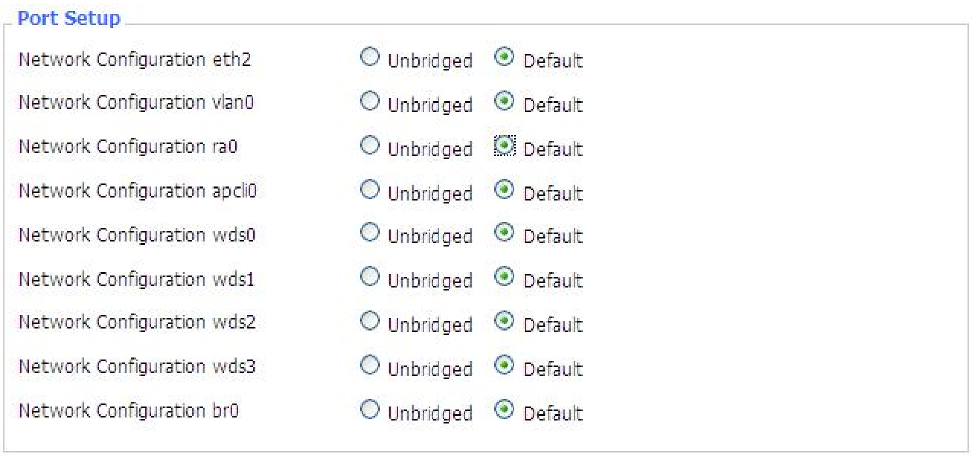
If bind success, bridge binding list in the list of current bridging table is as below:



Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0
br1	yes	ra0

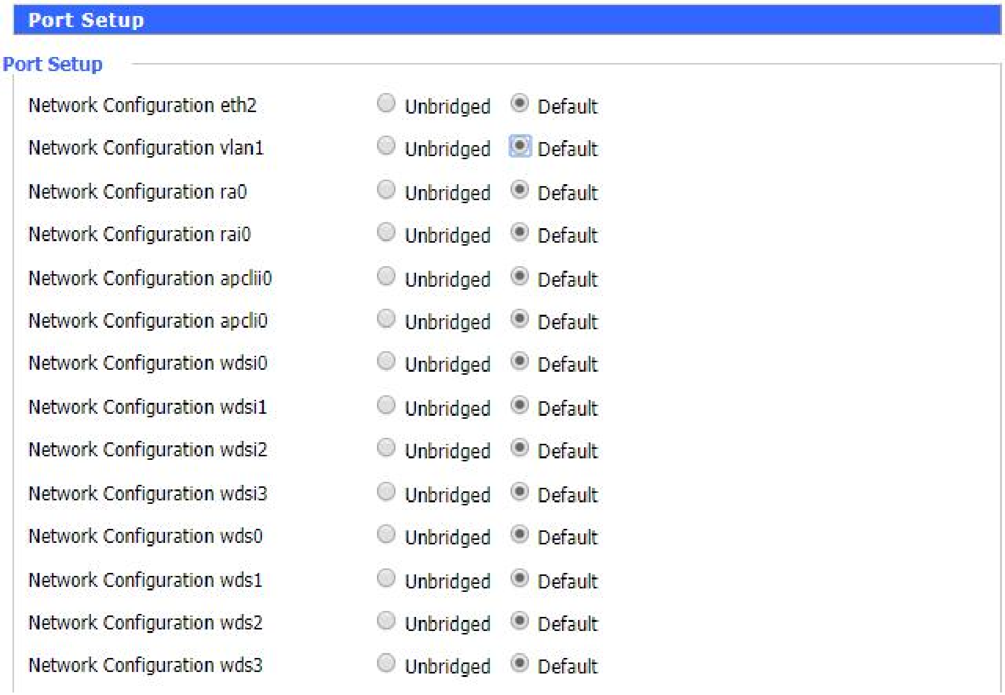
To make br1 bridge has the same function with DHCP assigned address, users need to set multiple DHCP function, see the introduction of multi-channel DHCPD:



Port Setup

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

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



Port Setup

Port Setup

Network Configuration eth2	○ Unbridged ● Default
Network Configuration vlan1	○ Unbridged ● Default
Network Configuration ra0	○ Unbridged ● Default
Network Configuration rai0	○ Unbridged ● Default
Network Configuration apclii0	○ Unbridged ● Default
Network Configuration apcli0	○ Unbridged ● Default
Network Configuration wdsi0	○ Unbridged ● Default
Network Configuration wdsi1	○ Unbridged ● Default
Network Configuration wdsi2	○ Unbridged ● Default
Network Configuration wdsi3	○ Unbridged ● Default
Network Configuration wds0	○ Unbridged ● Default
Network Configuration wds1	○ Unbridged ● Default
Network Configuration wds2	○ Unbridged ● Default
Network Configuration wds3	○ Unbridged ● Default

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

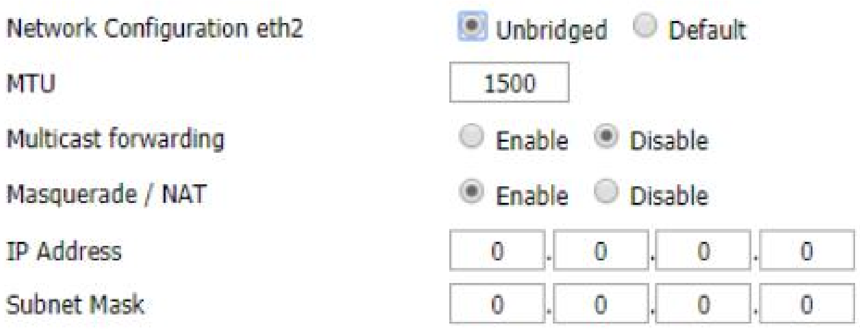
MTU: maximum transfer unit

Multicast forwarding: enable or disable multicast forwarding

Masquerade/NAT: enable or disable Masquerade/NAT

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

Subnet Mask: set subnet mask.



Network Configuration eth2	● Unbridged ○ Default
MTU	1500
Multicast forwarding	○ Enable ● Disable
Masquerade / NAT	● Enable ○ Disable
IP Address	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0

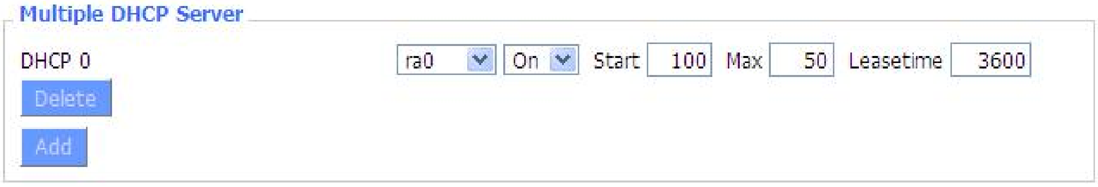
Multiple DHCP Server: using multiple DHCP service. Click 'Add' in multiple DHCP server to add a new DHCP server setting.

Can choose port or bridge (do not be configured as eth0), can choose on of off for the service.

Start means start IP address.

Max means maximum assigned DHCP clients.

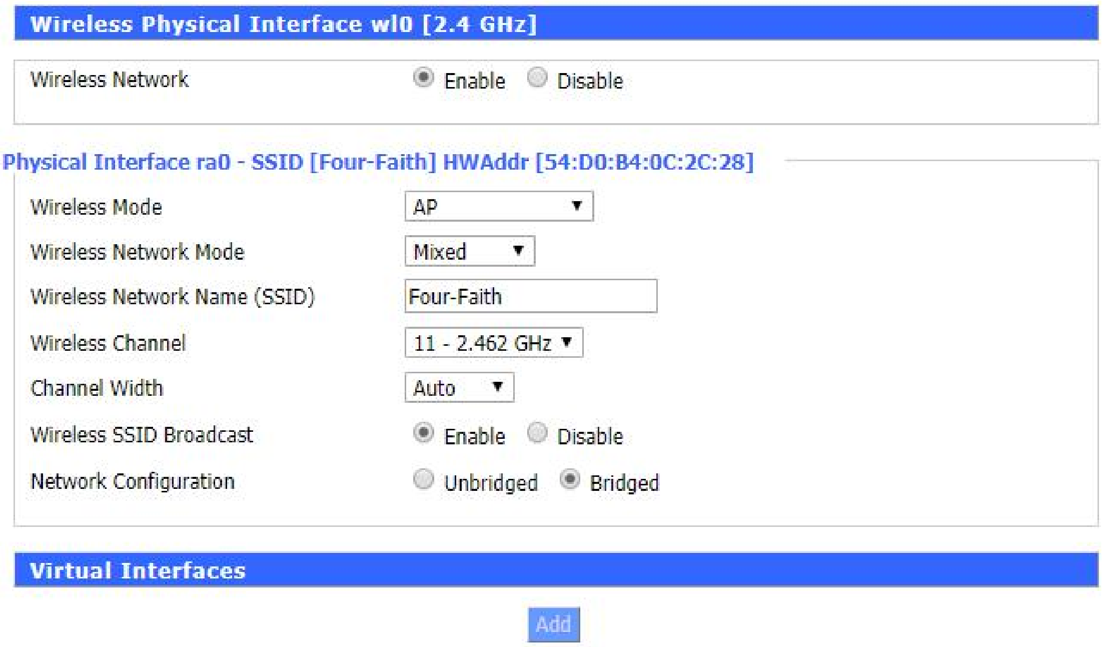
Leasetime means the client lease time, the unit is second.


Multiple DHCP Server

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

3.2 Wireless

3.2.1 Basic Settings


Wireless Physical Interface wl0 [2.4 GHz]

Wireless Network: ● Enable ○ Disable

Physical Interface ra0 - SSID [Four-Faith] HWAddr [54:D0:B4:0C:2C:28]

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

Wireless Network under 2.4G

Enable: Enable WFI radios.

Disable: Disable WIFI radios.

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

Wireless Network Mode：

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

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

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

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

G-only：Only supports the 802.11g standard wireless devices.
NG-Mixed：Support 802.11g, 802.11n wireless devices.
N-only：Only supports the 802.11g standard wireless devices.

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

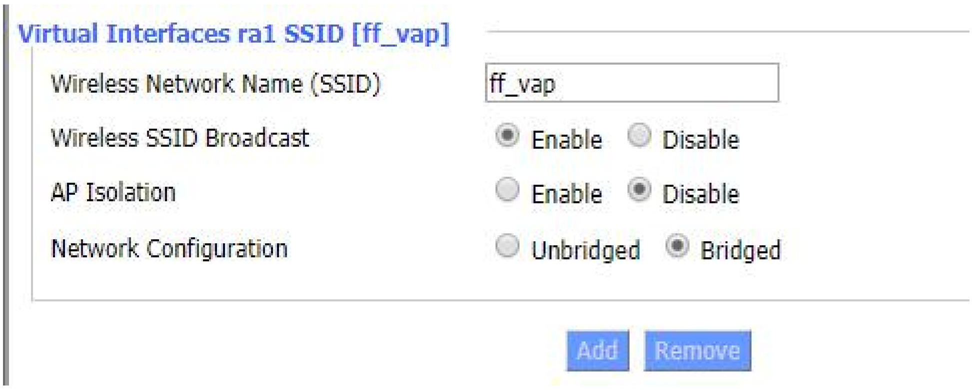
Wireless Channel：A total of 1-13 channels to choose more than one wireless device environment, please try to avoid using the same channel with other devices.

Channel Width：20MHZ and 40MHZ.

Wireless SSID Broadcast：
Enable：SSID broadcasting.
Disable：Hidden SSID.

Network Configuration：
Bridged：Bridge to the Router, under normal circumstances, please select the bridge.
Unbridged：There is no bridge to the Router, IP addresses need to manually configure.

Virtual Interfaces
To add a more wifi SSID.

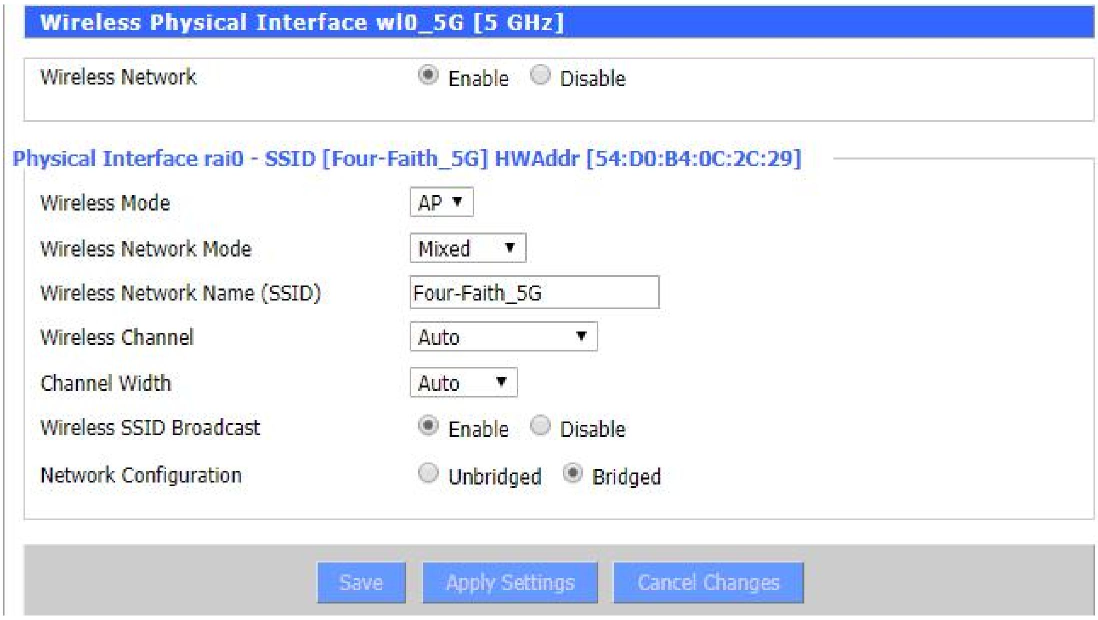


Virtual Interfaces ra1 SSID [ff_vap]

Wireless Network Name (SSID)	ff_vap
Wireless SSID Broadcast	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
Network Configuration	○ Unbridged ● Bridged

AP Isolation： This setting make all wireless clients to be isolated, and wireless clients can only access to AP internet.

5G wifi
Most parameters are same to 2.4G wifi.



Wireless Physical Interface wl0_5G [5 GHz]

Wireless Network ● Enable ○ Disable

Physical Interface rai0 - SSID [Four-Faith_5G] HWAddr [54:D0:B4:0C:2C:29]

Wireless Mode: AP

Wireless Network Mode: Mixed

Wireless Network Name (SSID): Four-Faith_5G

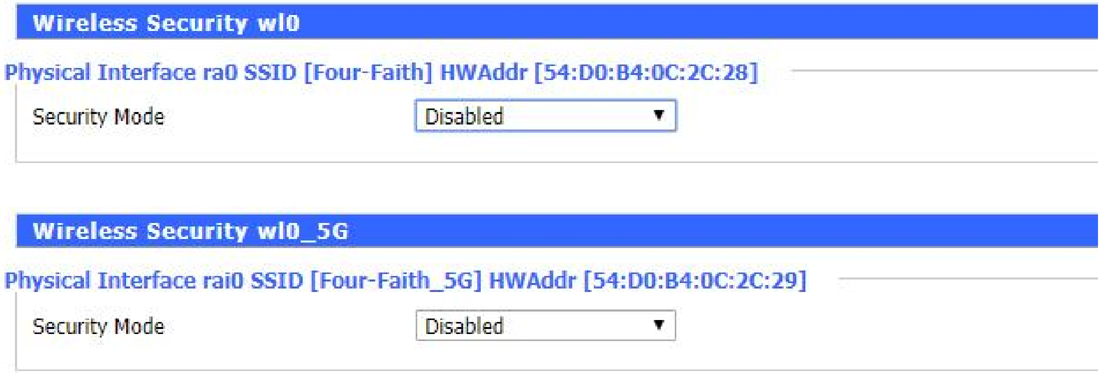
Wireless Channel: Auto

Channel Width: Auto

Wireless SSID Broadcast ● Enable ○ Disable

Network Configuration ○ Unbridged ● Bridged

3.2.2 Wireless Security



Wireless Security wl0

Physical Interface ra0 SSID [Four-Faith] HWAddr [54:D0:B4:0C:2C:28]

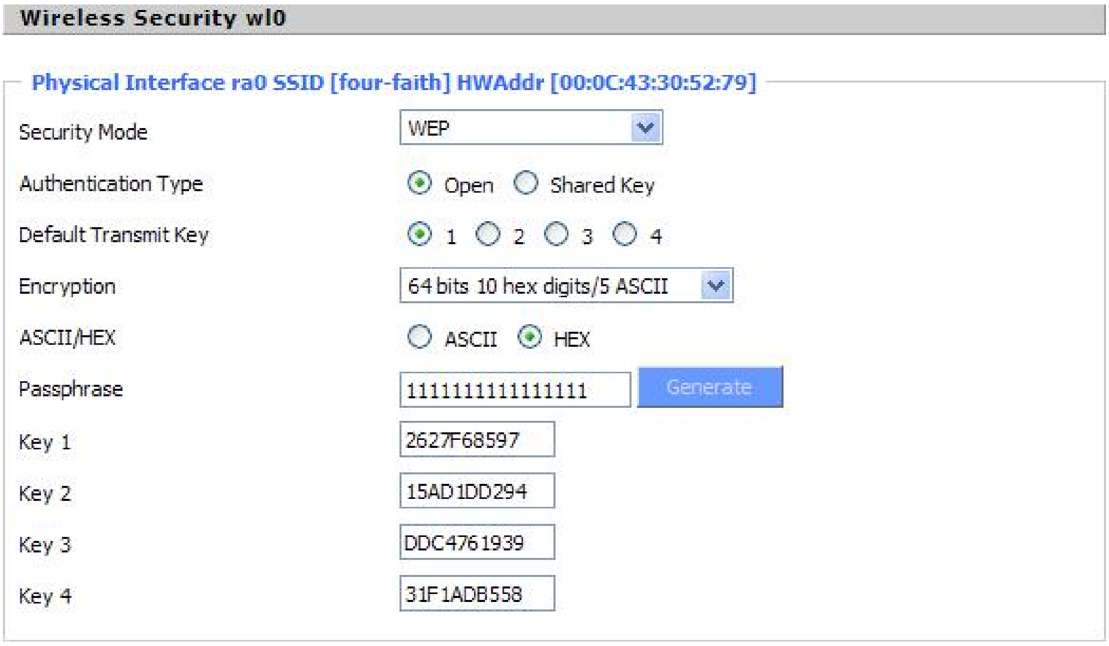
Security Mode: Disabled

Wireless Security wl0_5G

Physical Interface rai0 SSID [Four-Faith_5G] HWAddr [54:D0:B4:0C:2C:29]

Security Mode: Disabled

Wireless Security wl0 is for 2.4G.



Wireless Security wl0

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

Security Mode: WEP

Authentication Type ● Open ○ Shared Key

Default Transmit Key ● 1 ○ 2 ○ 3 ○ 4

Encryption: 64 bits 10 hex digits/5 ASCII

ASCII/HEX ○ ASCII ● HEX

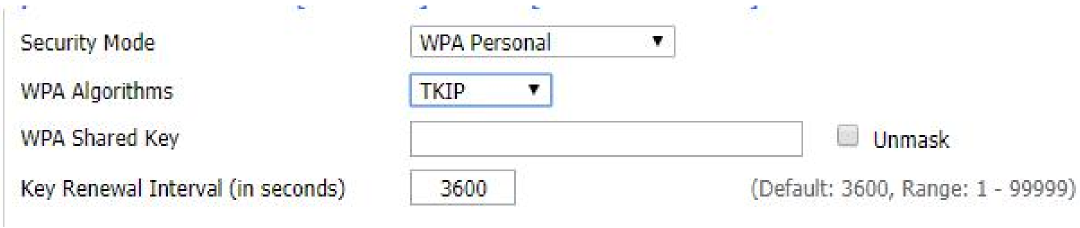
Passphrase: 111111111111111

Key 1: 2627F68597

Key 2: 15AD1DD294

Key 3: DDC4761939

Key 4: 31F1ADB558



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

WEP： Is a basic encryption algorithm is less secure than WPA.Use of WEP is discouraged due to security weaknesses, and one of the WPA modes should be used whenever possible. Only use WEP if you have clients that can only support WEP (usually older, 802.11b-only clients).

Authentication Type：Open or shared key。

Default Transmit Key：Select the key form Key 1 - Key 4 key.

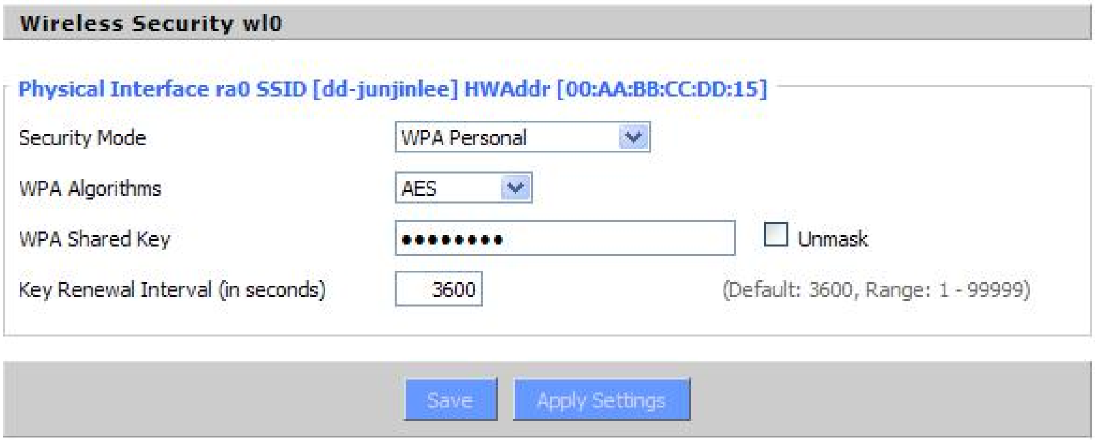
Encryption： There are two levels of WEP encryption, 64-bit (40-bit) and 128-bit. To utilize WEP, select the desired encryption bit, and enter a passphrase or up to four WEP key in hexadecimal format. If you are using 64-bit (40-bit), then each key must consist of exactly 10 hexadecimal characters or 5 ASCII charceters. For 128-bit, each key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0"-"9" and "A"-"F".

ASCII/HEX: ASCII, the keys is 5 bit ASCII characters/13bit ASCII characters.

HEX, the keys is 10bit/26 bit hex digits.

Passphrase：The letters and numbers used to generate a key.

Key1-Key4：Manually fill out or generated according to input the pass phrase.



Wireless Security wl0

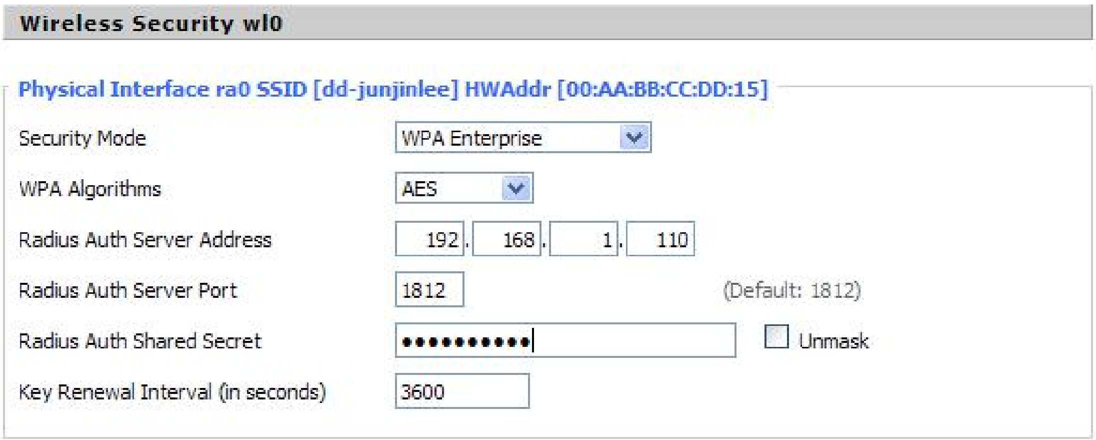
Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

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

WPA Personal/WPA2 Personal/WPA2 Person Mixed:， TKIP/AES/TKIP+AES， dynamic encryption keys. TKIP + AES, self-applicable TKIP or AES. WPA Person Mixed, allow WPA Personal and WPA2 Personal client mix.

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

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



Wireless Security wl0

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

Security Mode: WPA Enterprise

WPA Algorithms: AES

Radius Auth Server Address: 192.168.1.110

Radius Auth Server Port: 1812 (Default: 1812)

Radius Auth Shared Secret: •••••••••• □ Unmask

Key Renewal Interval (in seconds): 3600

WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed: WPA Enterprise uses an external RADIUS server to perform user authentication.

WPA Algorithms: AES/TKIP/TPIP+AES.

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

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

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

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

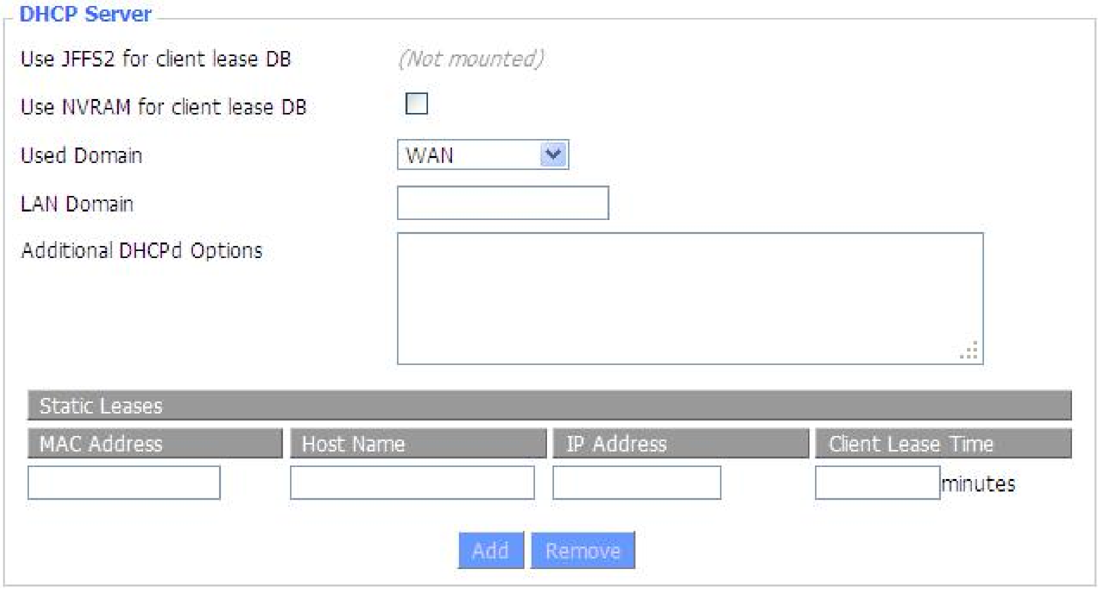
Wireless Security wl0_5G is for 5G.
Same with 2.4G WIFI.

3.3 Service

3.3.1 Service

DHCP Server

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



DHCP Server

Use JFFS2 for client lease DB: (Not mounted)

Use NVRAM for client lease DB: □

Used Domain: WAN

LAN Domain:

Additional DHCPd Options:

Static Leases

MAC Address	Host Name	IP Address	Client Lease Time
			minutes

Use NVRAM for client lease DB: users can store data to the system NVRAM area is enabled

Used domain: users can select here which domain the DHCP clients should get as their local domain. This can be the WAN domain set on the Setup screen or the LAN domain which can be set here.

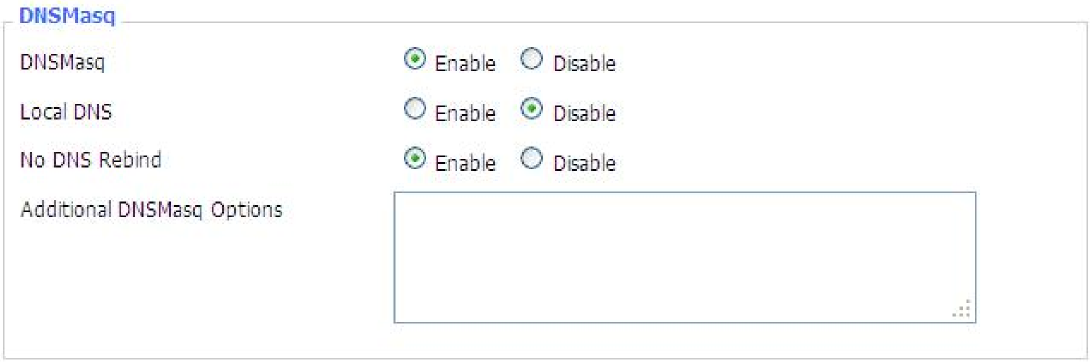
LAN Domain: users can define here their local LAN domain which is used as local domain for DNSmasq and DHCP service if chose above.

Static Leases: if users want to assign certain hosts a specific address then they can define them here. This is also the way to add hosts with a fixed address to the Router's local DNS service (DNSmasq).

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

DNSMasq

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



DNSMasq

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

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

No DNS Rebind: when enabled, it can prevent an external attacker to access the Router's internal Web interface. It is a security measure

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

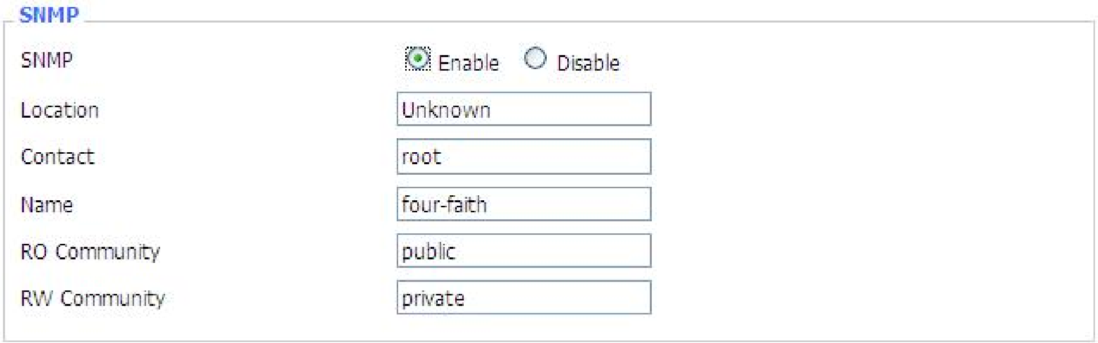
For example:

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

max lease number: dhcp-lease-max=2

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

SNMP



SNMP

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

Location: equipment location

Contact: contact this equipment management

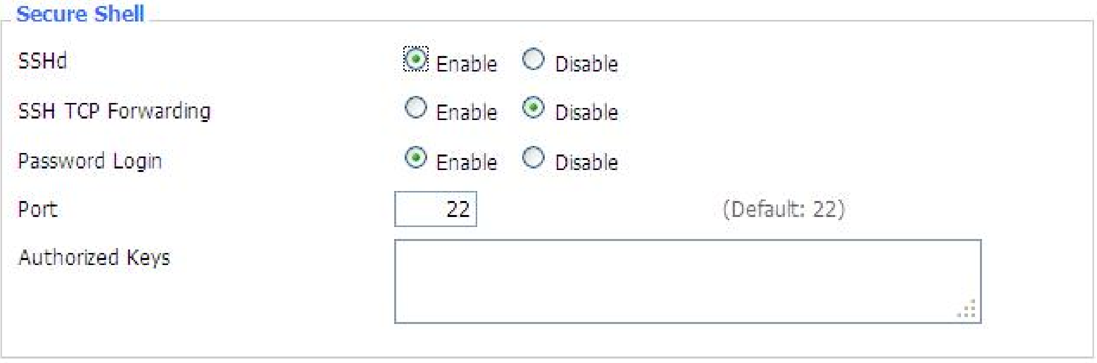
Name: device name

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

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

SSHD

Enabling SSHd allows users to access the Linux OS of their Router with an SSH client



Secure Shell

SSHd ● Enable ○ Disable

SSH TCP Forwarding ○ Enable ● Disable

Password Login ● Enable ○ Disable

Port 22 (Default: 22)

Authorized Keys

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

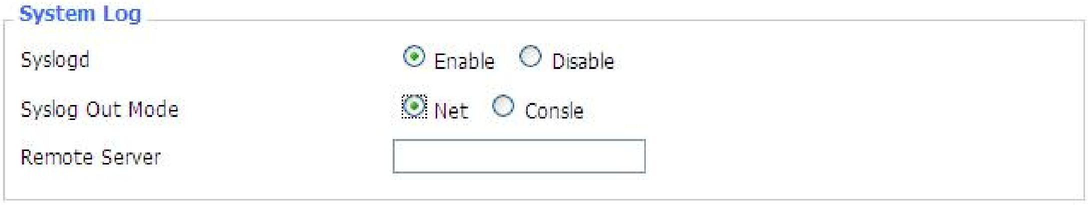
Password Login: allows login with the Router password (username is admin)

Port: port number for SSHd (default is 22)

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

System log

Enable Syslogd to capture system messages. By default they will be collected in the local file /var/log/messages. To send them to another system, enter the IP address of a remote syslog server.



System Log

Syslogd ● Enable ○ Disable

Syslog Out Mode ● Net ○ Consle

Remote Server

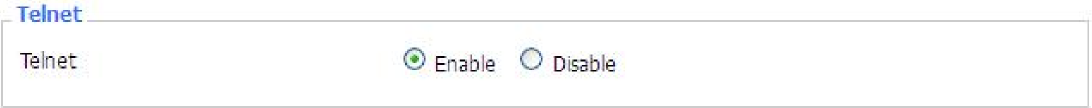
Syslog Out Mode: two log mode

Net: the log information output to a syslog server

Console: the log information output to console port

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

Telnet



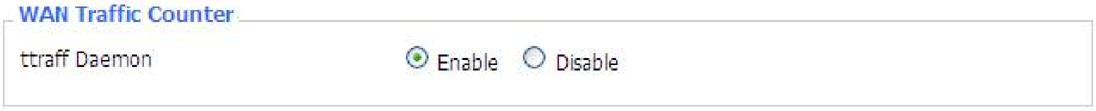
Telnet

Telnet ● Enable ○ Disable

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

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

WAN Traffic Counter



WAN Traffic Counter

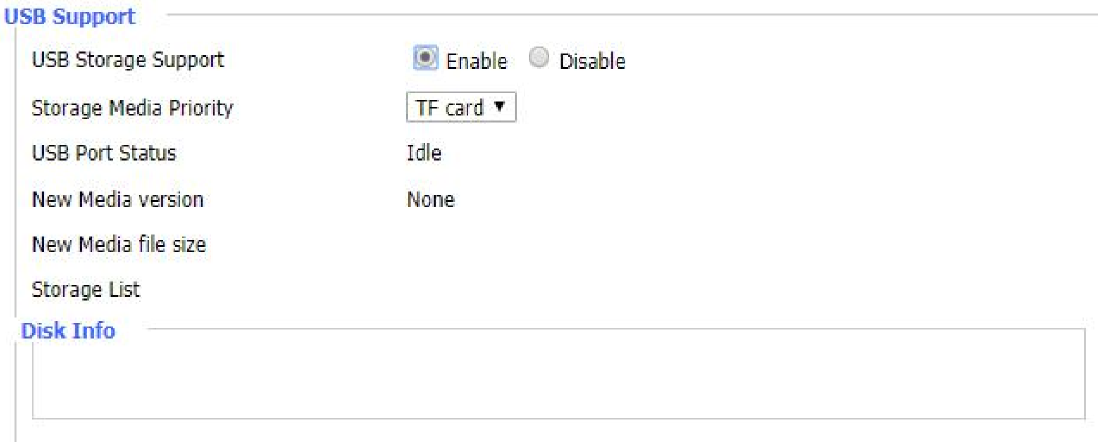
ttraff Daemon	● Enable ○ Disable

Ttraff Daemon: enable or disable wan traffic counter function

3.3.2 USB

USB part is used for TF card.

Please enable USB Storage Support, then it can detect TF card inserted.



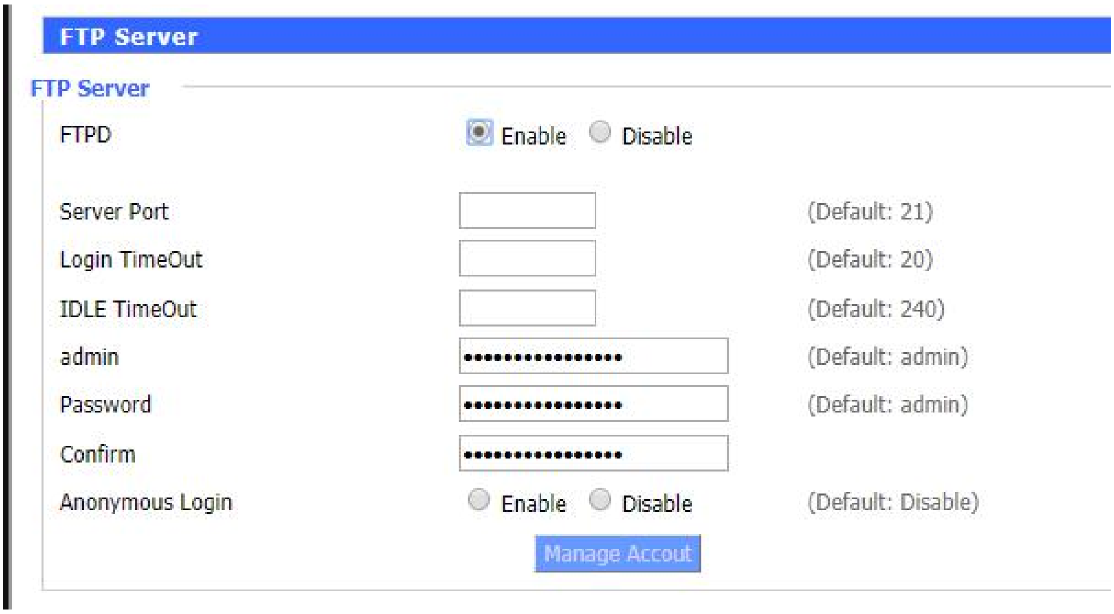
USB Support

USB Storage Support	● Enable ○ Disable
Storage Media Priority	TF card ▼
USB Port Status	Idle
New Media version	None
New Media file size	
Storage List	

Disk Info

3.3.3 FTP Server

F-G100 can support FTP server function, it is standard FTP server function.



FTP Server

FTP Server

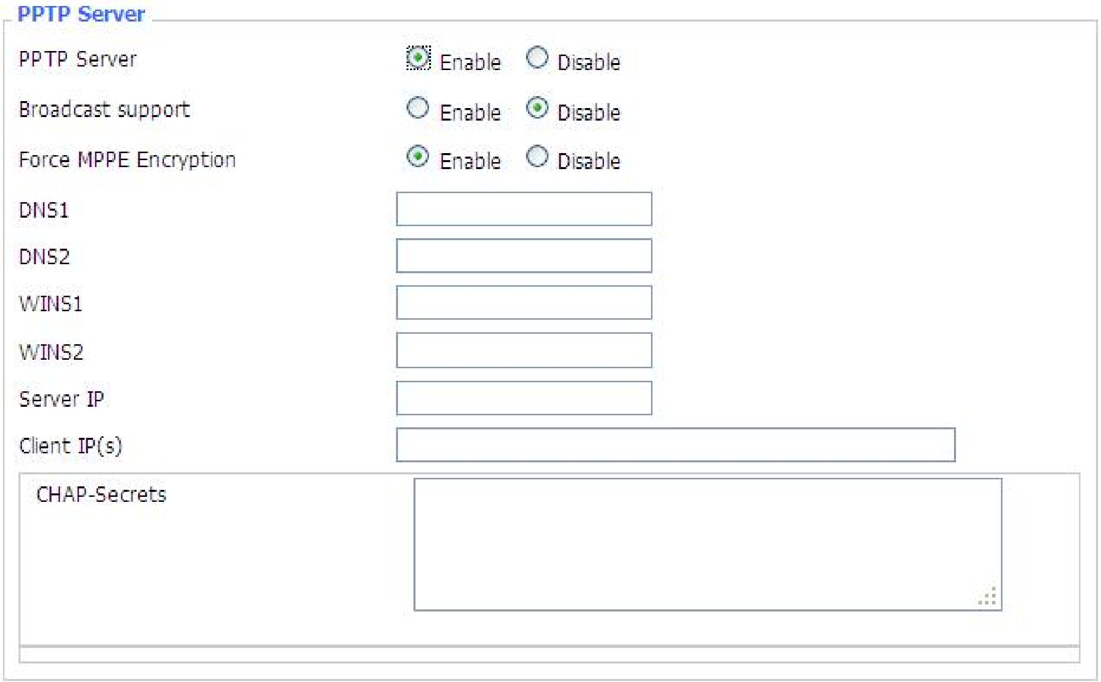
FTPD	● Enable ○ Disable	
Server Port		(Default: 21)
Login TimeOut		(Default: 20)
IDLE TimeOut		(Default: 240)
admin	••••••••••••••••	(Default: admin)
Password	••••••••••••••••	(Default: admin)
Confirm	••••••••••••••••	
Anonymous Login	○ Enable ○ Disable	(Default: Disable)

3.4 VPN

Router can be VPN server or VPN client.
VPN server needs public IP or special APN sim card, while VPN client can use normal sim card with dynamic IP.

3.4.1 PPTP

PPTP Server

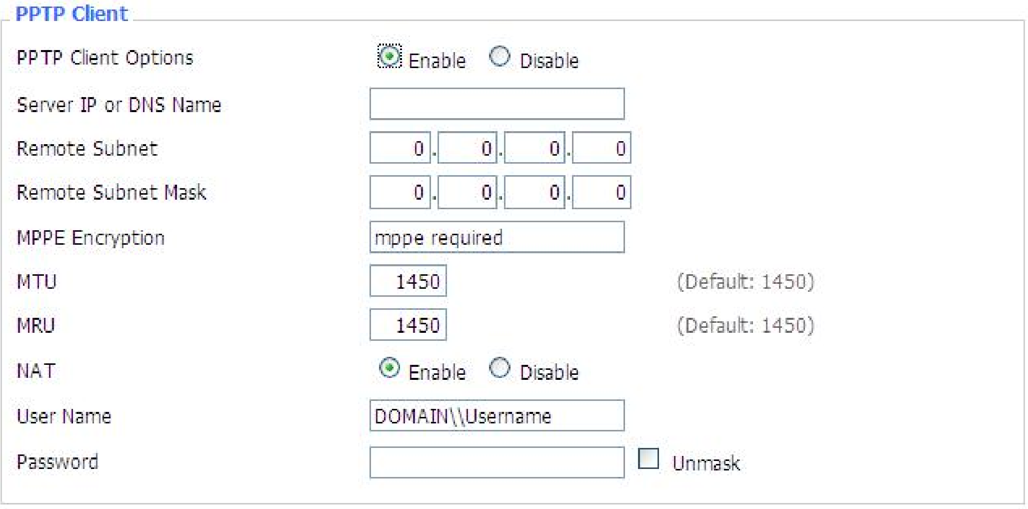


PPTP Server

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

Broadcast support: enable or disable broadcast support of PPTP server
Force MPPE Encryption: enable of disable force MPPE encryption of PPTP data
DNS1/DNS2/WINS1/WINS2: set DNS1/DNS2/WINS1/WINS2
Server IP: input IP address of the Router as PPTP server, differ from LAN address
Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx
CHAP Secrets: user name and password of the client using PPTP service
Note: client IP must be different with IP assigned by Router DHCP.
The format of CHAP Secrets is user * password *.

PPTP Client



PPTP Client

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

Server IP or DNS Name: PPTP server's IP Address or DNS Name

Remote Subnet: the network of the remote PPTP server

Remote Subnet Mask: subnet mask of remote PPTP server

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

MTU: maximum Transmission Unit

MRU: maximum Receive Unit

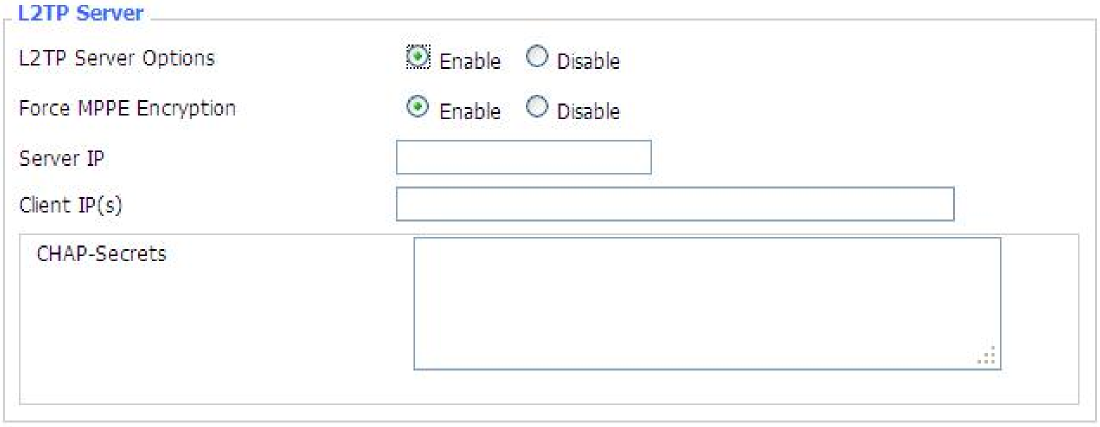
NAT: network Address Translation

User Name: user name to login PPTP Server.

Password: password to log into PPTP Server.

3.4.2 L2TP

L2TP Server



L2TP Server

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

Force MPPE Encryption: enable or disable force MPPE encryption of L2TP data

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

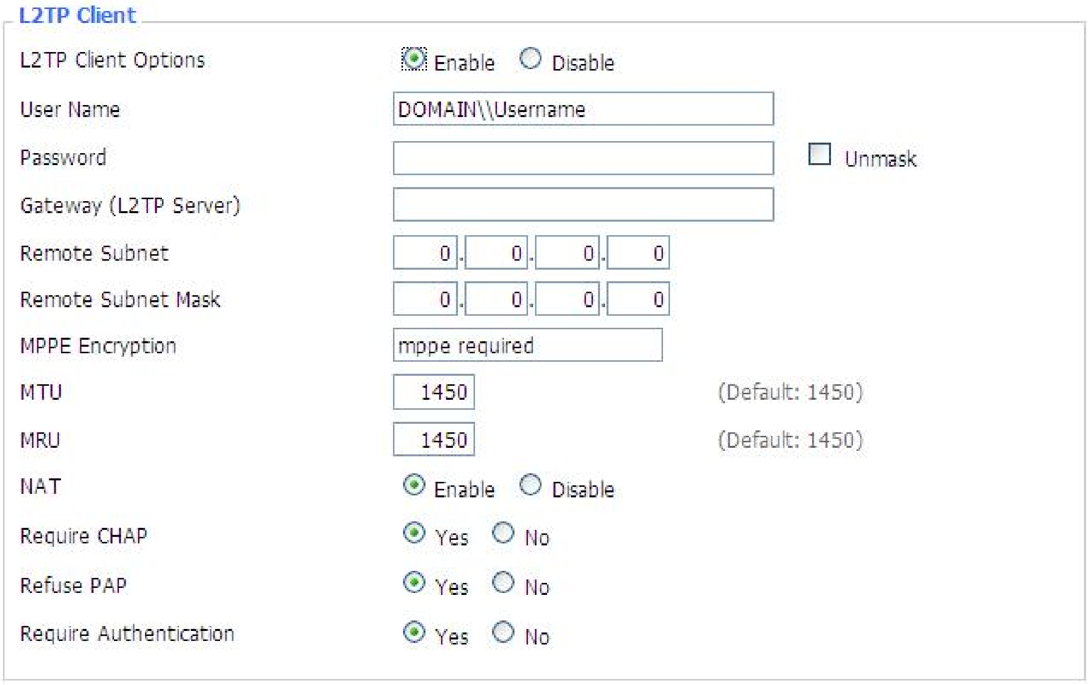
Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx

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

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

The format of CHAP Secrets is user * password *.

L2TP Client



L2TP Client

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

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

Remote Subnet: the network of remote PPTP server

Remote Subnet Mask: subnet mask of remote PPTP server

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

MTU: maximum transmission unit

MRU: maximum receive unit

NAT: network address translation

User Name: user name to login L2TP Server

Password: password to login L2TP Server

Require CHAP: enable or disable support chap authentication protocol

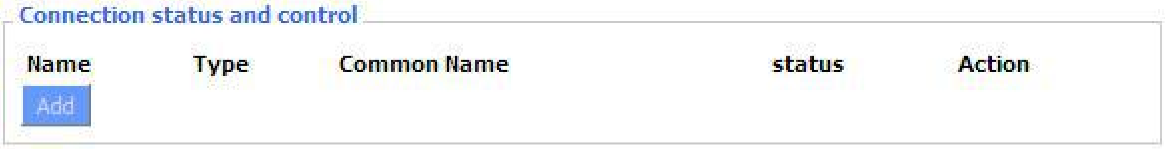
Refuse PAP: enable or disable refuse to support the pap authentication

Require Authentication: enable or disable support authentication protocol

3.4.3 IPsec

Connect Status and Control

Show IPSEC connection and status of current router on IPSEC page.



Connection status and control

Name	Type	Common Name	status	Action

Name: the name of IPSEC connection

Type: The type and function of current IPSEC connection

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

Status: connection status: closed, negotiating, establish

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

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

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

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

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

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

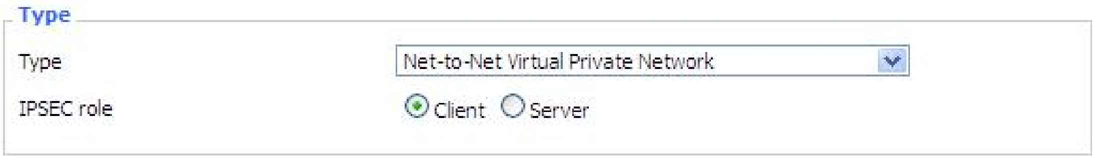
Reconnect: this action will remove current tunnel, and re-launch tunnel establish request

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

Add: to add a new IPSEC connection

Add IPSEC connection or edit IPSEC connection

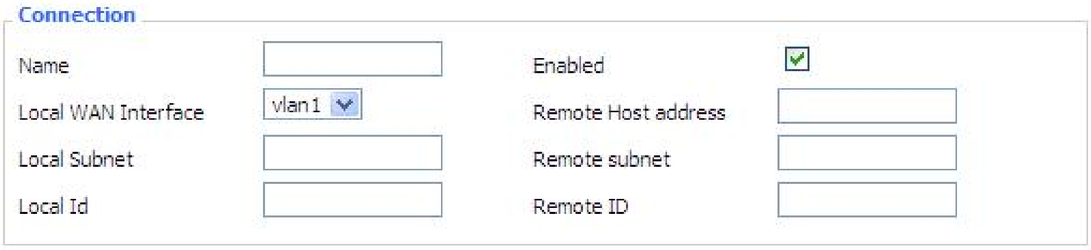
Type: to choose IPSEC mode and relevant functions in this part, supports tunnel mode client, tunnel mode server and transfer mode currently



Type

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

Connection: this part contains basic address information of the tunnel



Connection

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

Name: to indicate this connection name, must be unique

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

Local WAN Interface: local addresss of the tunnel

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

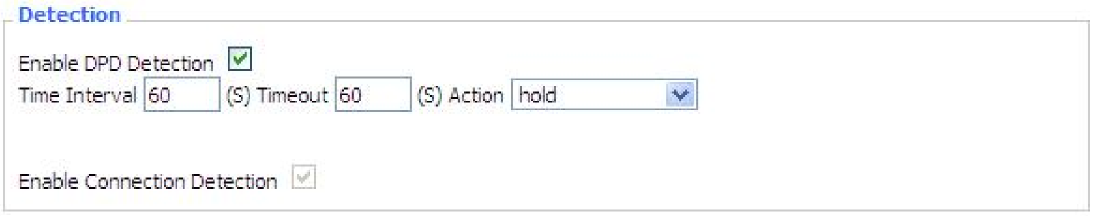
Local Subnet: IPSec local protects subnet and subnet mask, i.e. 192.168.1.0/24; this option can not fill in if using transfer mode

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

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

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

Detection: this part contains configure information of connection detection



Detection

Enable DPD Detection ☑

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

Enable Connection Detection ☑

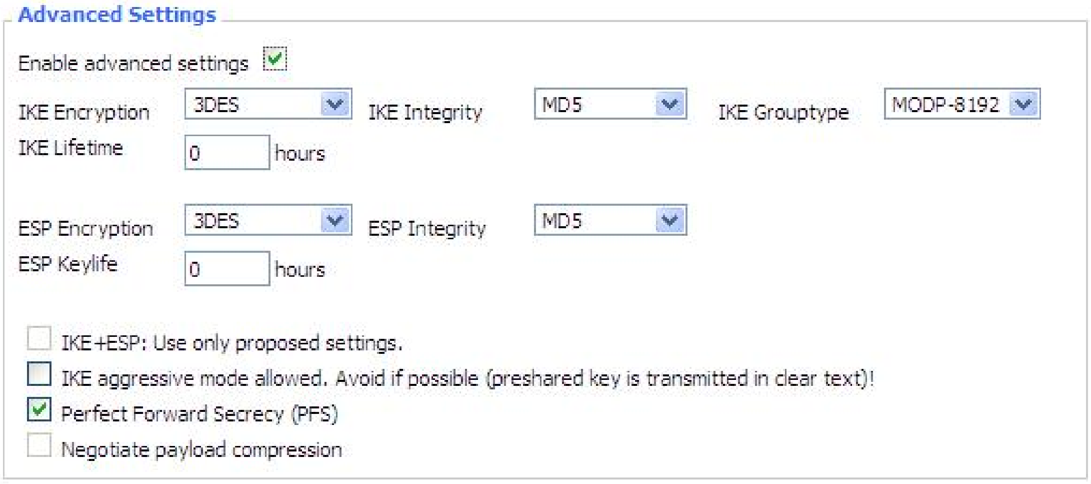
Enable DPD Detection: enable or disable this function, tick means enable

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

Timeout: set the timeout of connect detection

Action: set the action of connect detection

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



Advanced Settings

Enable advanced settings ☑

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

IKE Lifetime 0 hours

ESP Encryption 3DES ESP Integrity MD5

ESP Keylife 0 hours

□ IKE+ESP: Use only proposed settings.

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

☑ Perfect Forward Secrecy (PFS)

□ Negotiate payload compression

Enable Advanced Settings: enable to configure 1st and 2nd phase information, otherwise it will automic negotiation according to opposite end

IKE Encryption: IKE phased encryption mode

IKE Integrity: IKE phased integrity solution

IKE Grouptype: DH exchange algorithm

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

ESP Encryption: ESP encryption type

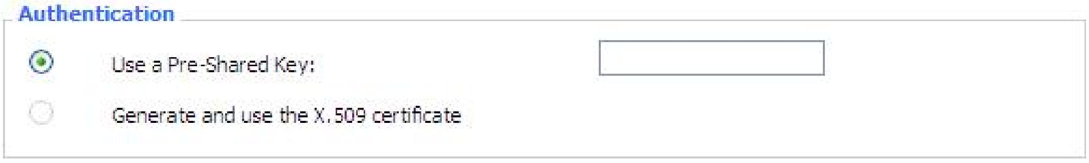
ESP Integrity: ESP integrity solution

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

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

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

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



Authentication

● Use a Pre-Shared Key:

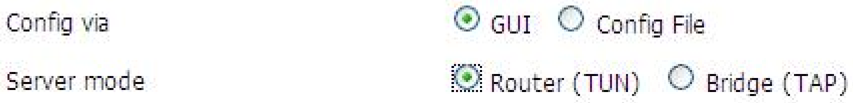
○ Generate and use the X.509 certificate

3.4.4 OPENVPN

OPENVPN Server

Start Type ○ WAN Up ● System

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



Config via ● GUI ○ Config File

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

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

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

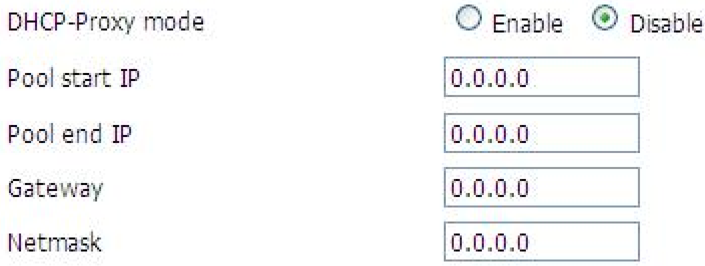
Router (TUN):

Network	0.0.0.0
Netmask	0.0.0.0

Network: network address allowed by OPENVPN server

Netmask: netmask allowed by OPENVPN server

Bridge (TAP):



DHCP-Proxy mode	○ Enable ● Disable
Pool start IP	0.0.0.0
Pool end IP	0.0.0.0
Gateway	0.0.0.0
Netmask	0.0.0.0

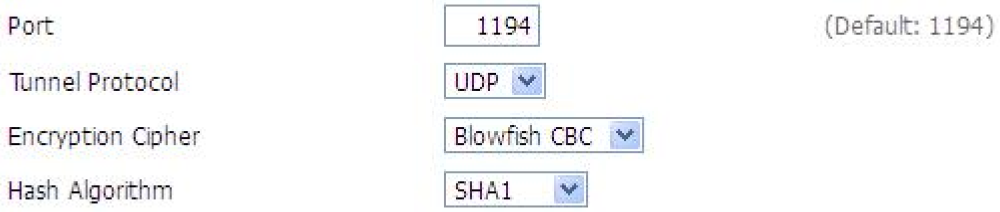
DHCP-Proxy mode: enable or disable DHCP-Proxy mode

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

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

Gateway: the gateway of the client allowed by OPENVPN server

Netmask: netmask of the client allowed by OPENVPN server



Port	1194	(Default: 1194)
Tunnel Protocol	UDP	
Encryption Cipher	Blowfish CBC	
Hash Algorithm	SHA1	

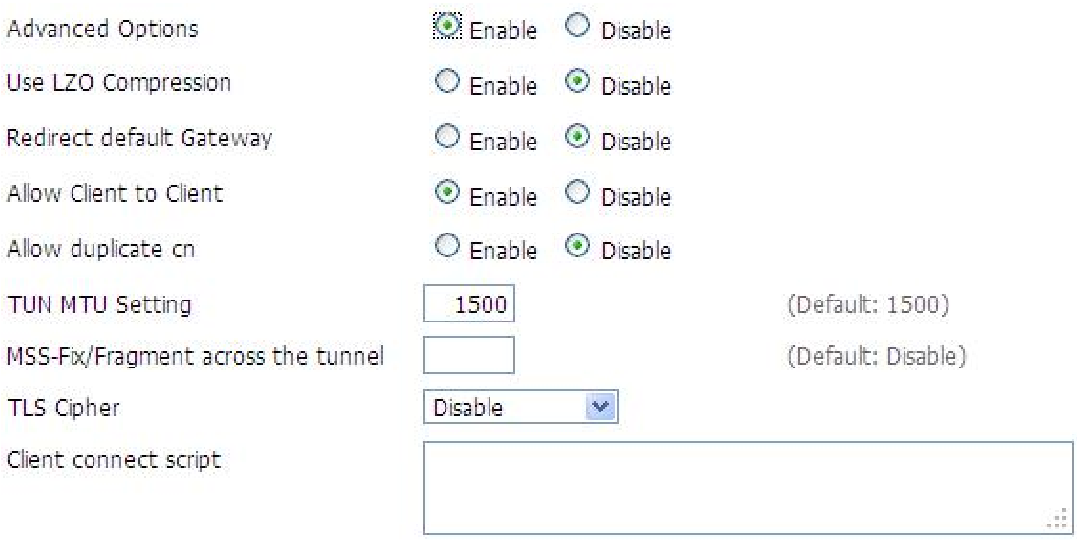
Port: listen port of OPENVPN server

Tunnel Protocol: UCP or TCP of OPENVPN tunnel protocol

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

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

Advanced Options



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

Use LZO Compression: enable or disable use LZO compression for data transfer

Redirect default Gateway: enable or disable redirect default gateway

Allow Client to Client: enable or disable allow client to client

Allow duplicate cn: enable or disable allow duplicate cn

TUN MTU Setting: set the value of TUN MTU

TCP MSS: MSS of TCP data

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

Client connect script: define some client script by user self

CA Cert

CA Cert: CA certificate

Public Server Cert

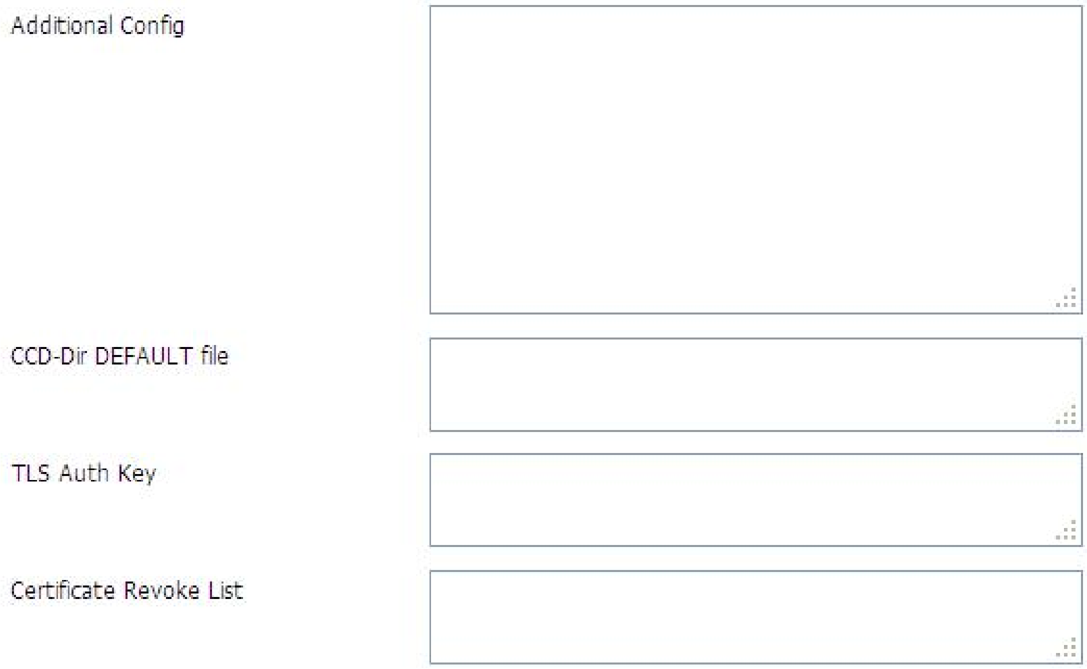
Public Server Cert: server certificate

Private Server Key

DH PEM

Private Server Key: the key seted by the server

DH PEM: PEM of the server



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

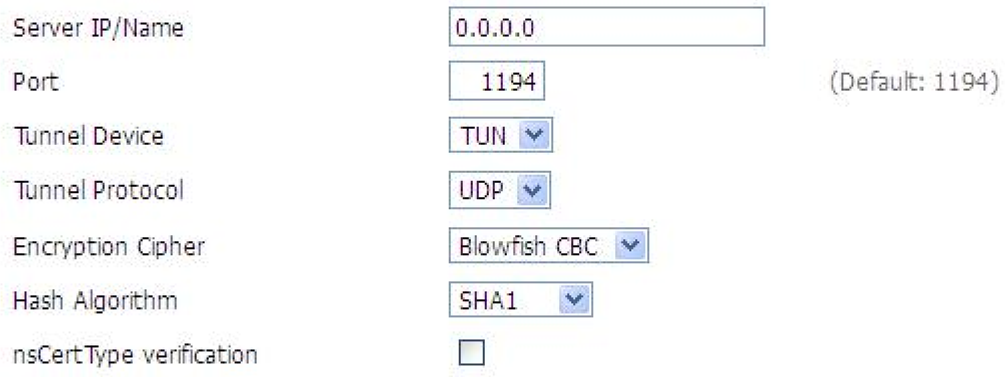
Additional Config: additional configurations of the server

CCD-Dir DEFAULT file: other file approaches

TLS Auth Key: authority key of Transport Layer Security

Certificate Revoke List: configure some revoke certificates

OPENVPN Client



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

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

Port: listen port of OPENVPN client

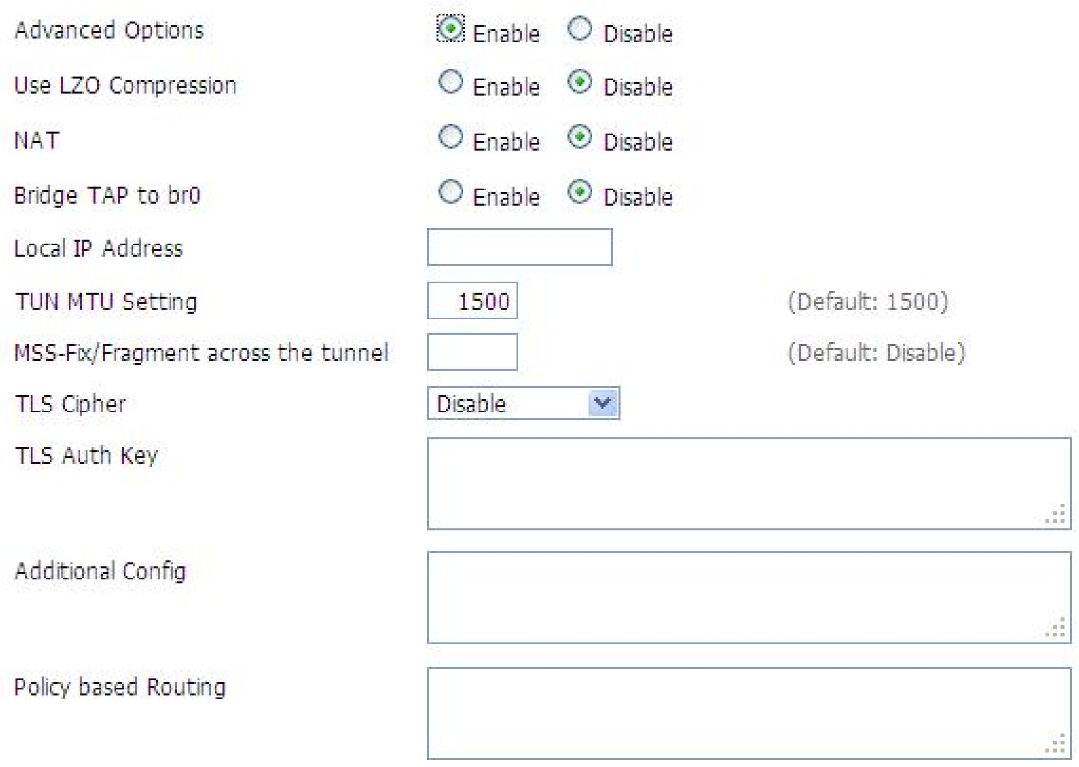
Tunnel Device: TUN----Router mode, TAP----Bridge mode

Tunnel Protocol: UDP and TCP protocol

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

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

nsCertType verification: support ns certificate type



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

Use LZO Compression: enable or disable use LZO compression for data transfer

NAT: enable or disable NAT through function

Bridge TAP to br0: enable or disable bridge TAP to br0

Local IP Address: set IP address of local OPENVPN client

TUN MTU Setting: set MTU value of the tunnel

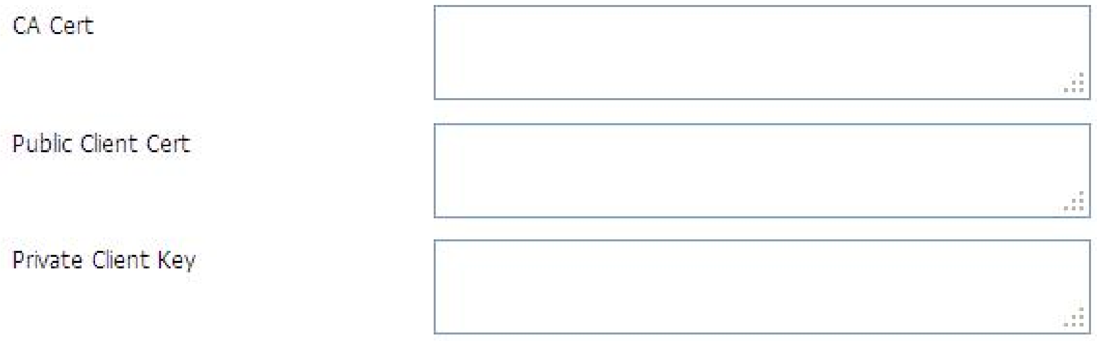
TCP MSS: mss of TCP data

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

TLS Auth Key: authority key of Transport Layer Security

Additional Config: additional configurations of OPENVPN server

Policy based Routing: input some defined routing policy



CA Cert	
Public Client Cert	
Private Client Key	

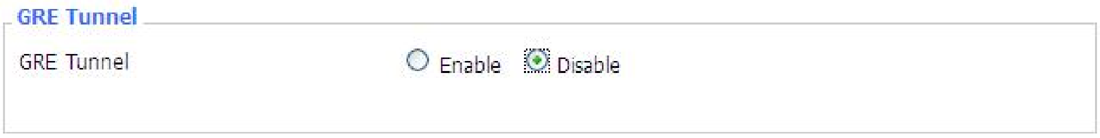
CA Cert: CA certificate

Public Client Cert: client certificate

Private Client Key: client key

3.4.5 GRE

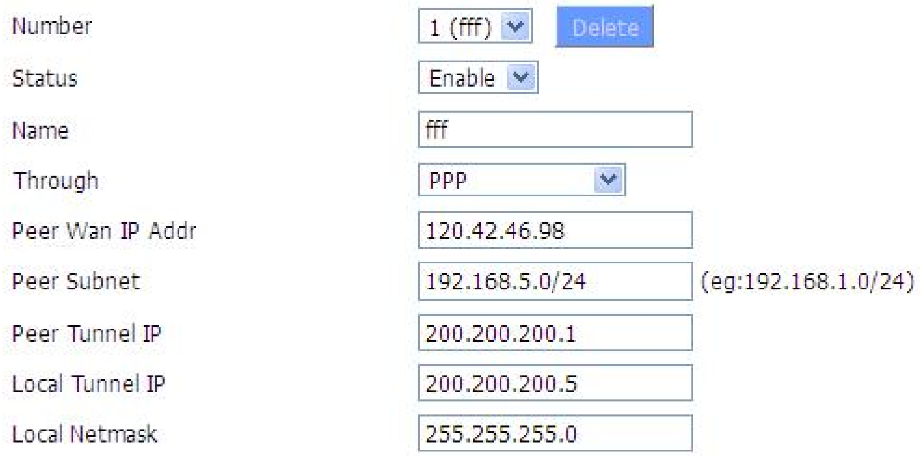
GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) protocol is a network layer protocol (such as IP and IPX) data packets are encapsulated, so these encapsulated data packets to another network layer protocol (IP)transmission. GRE Tunnel (tunnel) technology, Layer Two Tunneling Protocol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



GRE Tunnel

GRE Tunnel ○ Enable ● Disable

GRE Tunnel: enable or disable GRE function



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

Number： Switch on/off GRE tunnel app

Status： Switch on/off someone GRE tunnel app

Name： GRE tunnel name

Through： The GRE packet transmit interface

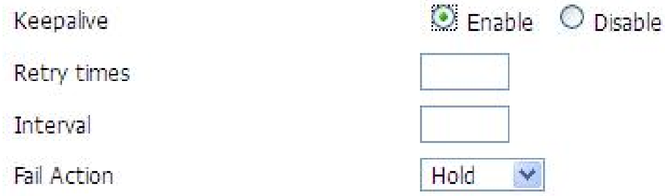
Peer Wan IP Addr： The remote WAN address

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

Peer Tunnel IP： The remote tunnel ip address

Local Tunnel IP： The local tunnel ip address

Local Netmask： Netmask of local network



Keepalive	● Enable ○ Disable
Retry times	
Interval	
Fail Action	Hold

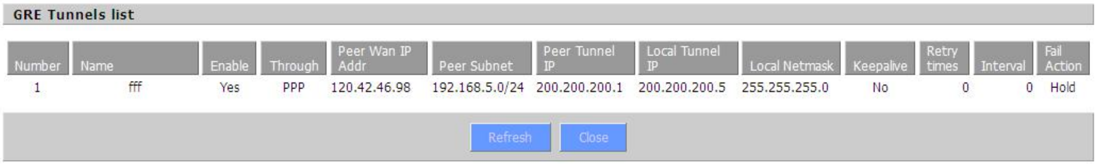
Keepalive： Enable or disable GRE Keepalive function

Retry times： GRE keepalive detect fail retries

Interval： The time interval of GRE keepalive packet sent

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

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



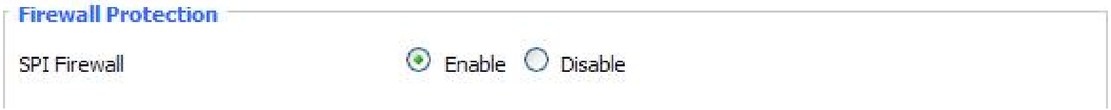
GRE Tunnels list

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

3.5 Security

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

Firewall Protection

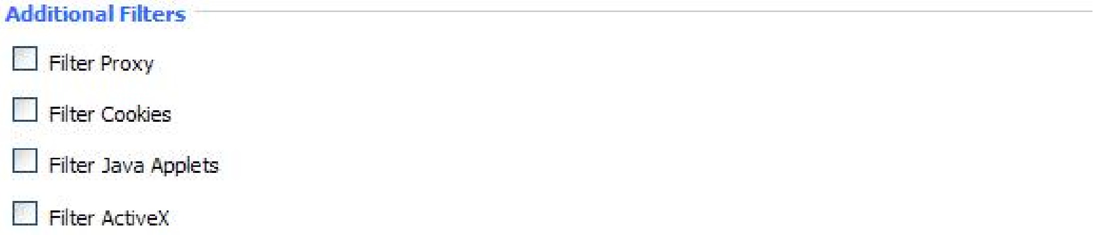


Firewall Protection

SPI Firewall ● Enable ○ Disable

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

Additional Filters



Additional Filters

□ Filter Proxy

□ Filter Cookies

□ Filter Java Applets

□ Filter ActiveX

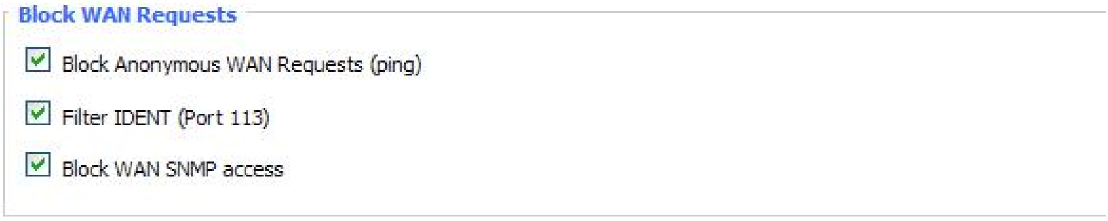
Filter Proxy: Wan proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

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

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

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

Prevent WAN Request



Block WAN Requests

☑ Block Anonymous WAN Requests (ping)

☑ Filter IDENT (Port 113)

☑ Block WAN SNMP access

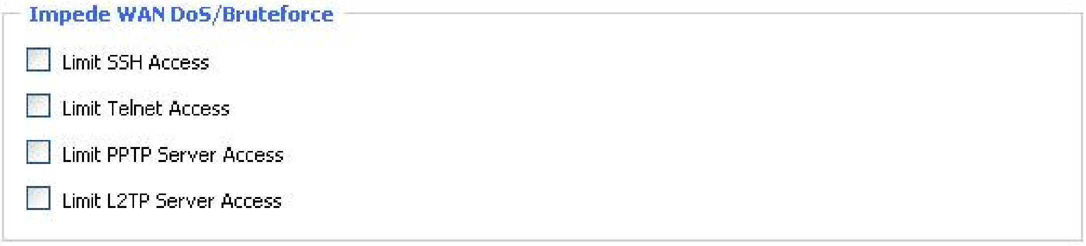
Block Anonymous WAN Requests (ping): By selecting “Block Anonymous WAN Requests (ping)” box to enable this feature, you can prevent your network from the Ping or detection of other Internet users. so that make More difficult to break into your network. The default state of this feature is enabled ,choose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

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

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

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

Impede WAN DoS/Bruteforce



Impede WAN DoS/Bruteforce

□ Limit SSH Access

□ Limit Telnet Access

□ Limit PPTP Server Access

□ Limit L2TP Server Access

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

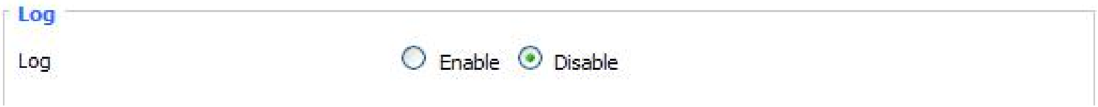
Limit Telnet Access: This feature limits the access request from the WAN by Telnet, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

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

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

Log Management

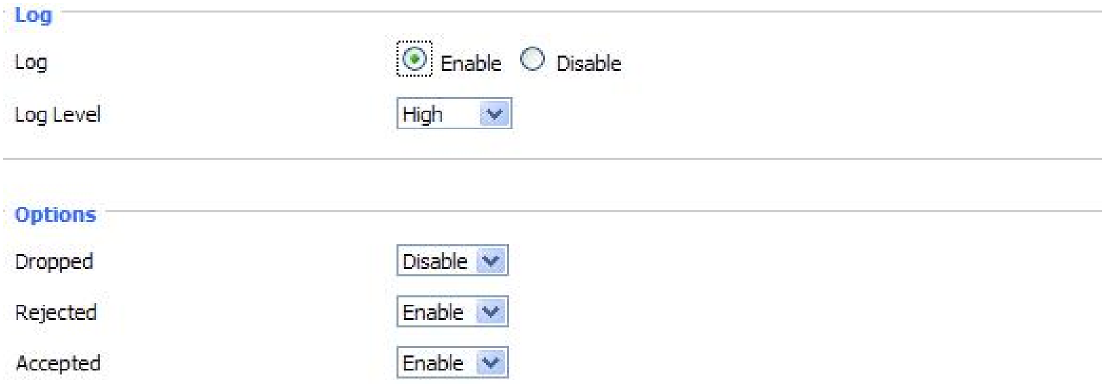
The Router can keep logs of all incoming or outgoing traffic for your Internet connection.



Log

Log ○ Enable ● Disable

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



Log

Log	● Enable ○ Disable
Log Level	High

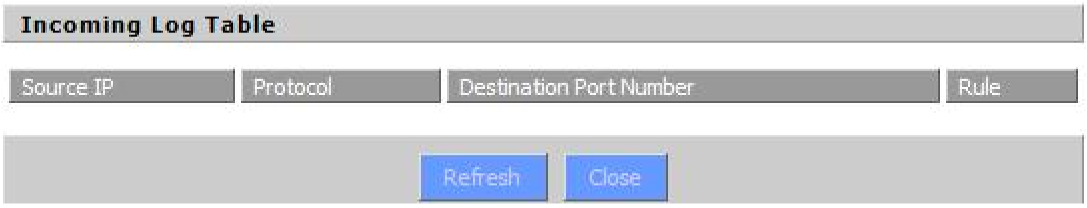
Options

Dropped	Disable
Rejected	Enable
Accepted	Enable

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

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

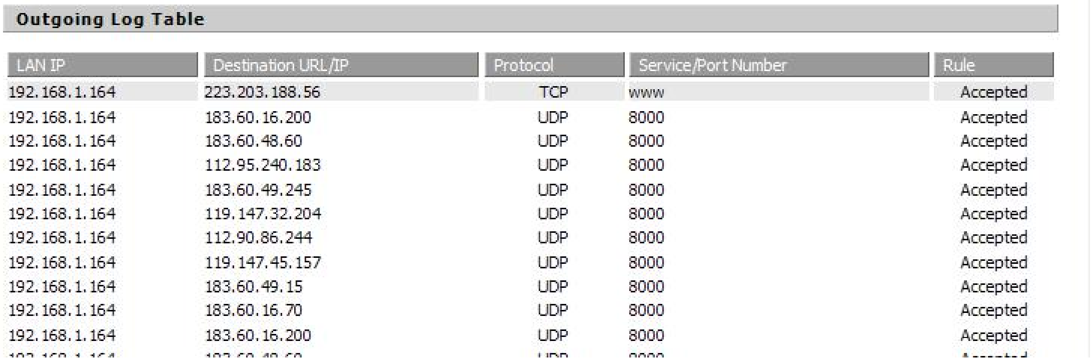
Incoming Log: To see a temporary log of the Router's most recent incoming traffic, click the Incoming Log button.



Incoming Log Table

Source IP	Protocol	Destination Port Number	Rule

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



Outgoing Log Table

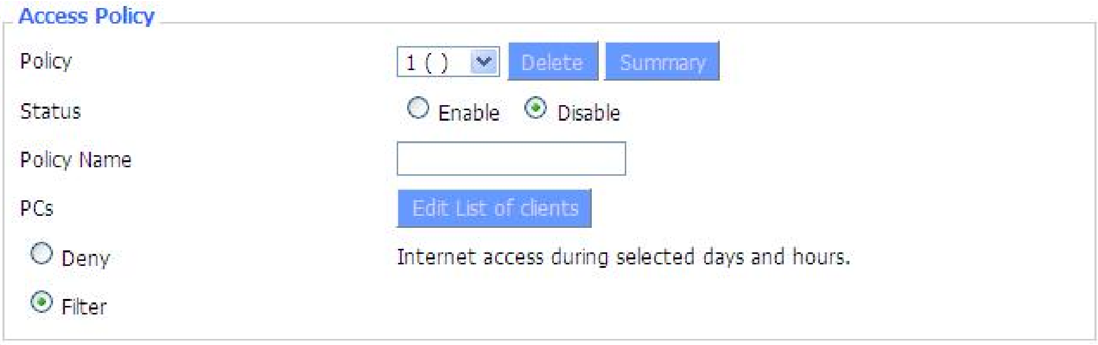
LAN IP	Destination URL/IP	Protocol	Service/Port Number	Rule
192.168.1.164	223.203.188.56	TCP	www	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted
192.168.1.164	112.95.240.183	UDP	8000	Accepted
192.168.1.164	183.60.49.245	UDP	8000	Accepted
192.168.1.164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

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

3.6 Access Restrictions

3.6.1 WAN Access

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



Policy: 1 ( )

Status: ○ Enable ● Disable

Policy Name:

PCs

○ Deny

● Filter

Internet access during selected days and hours.

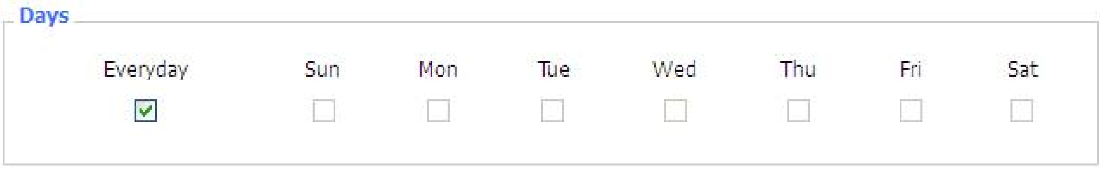
Two options in the default policy rules: "Filter" and "reject". If select "Deny”, you will deny specific computers to access any Internet service at a particular time period. If you choose to "filter"， It will block specific computers to access the specific sites at a specific time period. You can set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

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

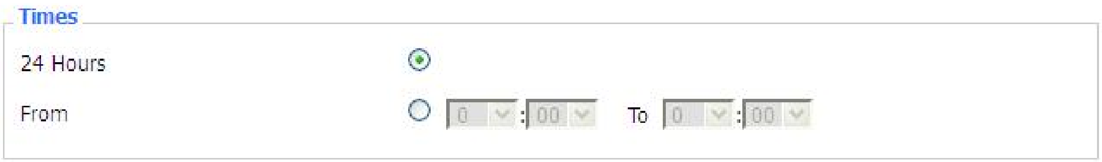
Status: Enable or disable a policy.

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

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



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

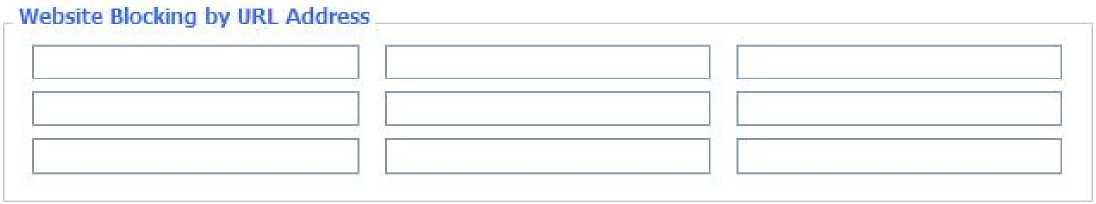


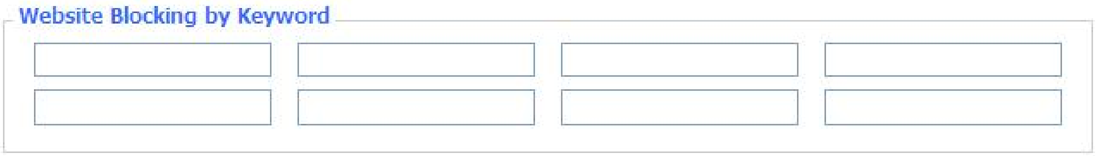
24 Hours ●

From ○ 0 : 00 To 0 : 00

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

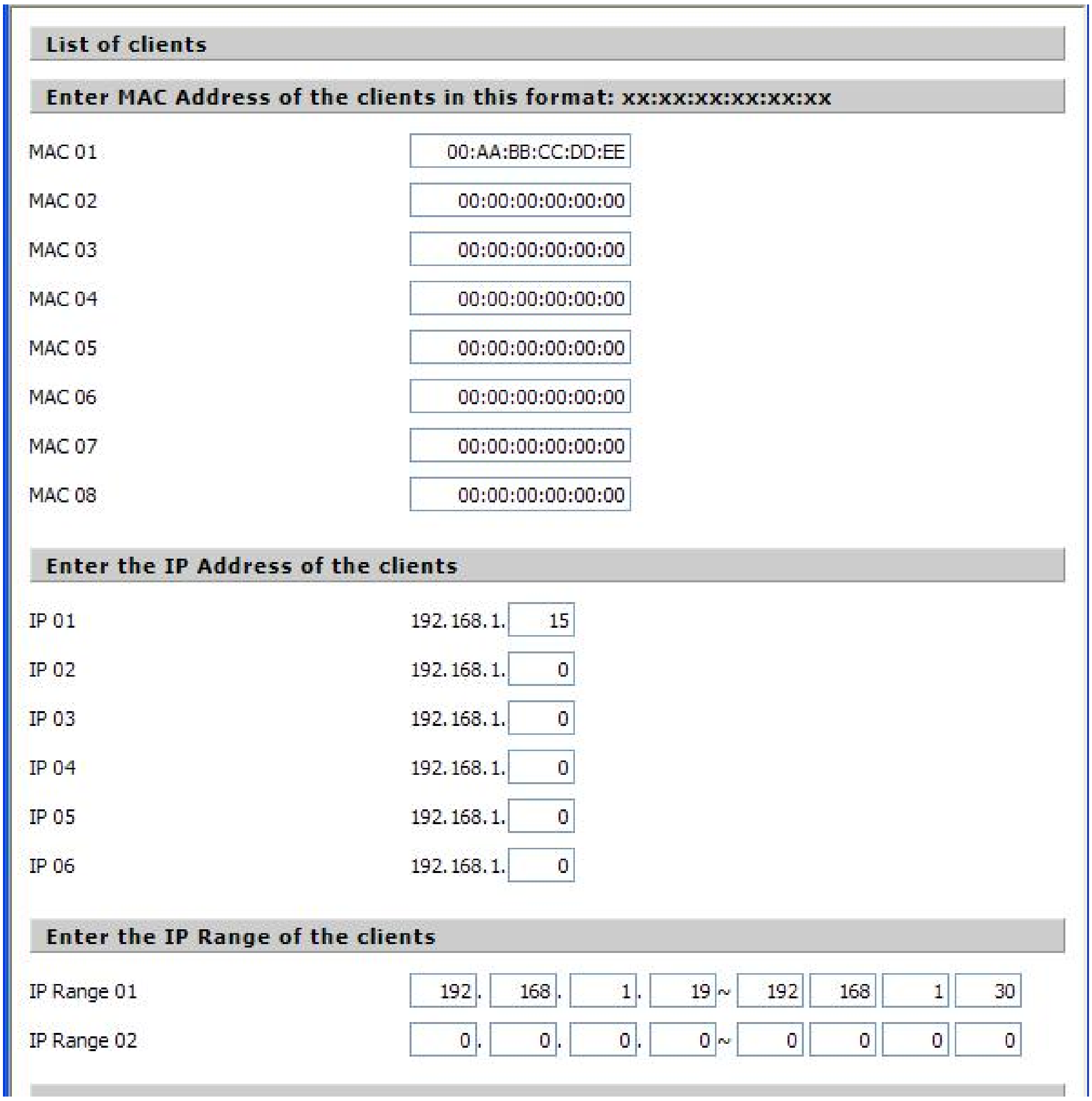
Times: Enter the time of the day you would like your policy to be applied.





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

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



List of clients

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

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

Enter the IP Address of the clients

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

Enter the IP Range of the clients

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

set up Internet access policy

1. Select the policy number (1-10) in the drop-down menu.
2. For this policy is enabled, click the radio button next to "Enable"
3. Enter a name in the Policy Name field.
4. Click the Edit List of PCs button.
5. On the List of PCs screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the IP fields. If you have a range of IP addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC addresses into the MAC fields.
6. Click the Apply button to save your changes. Click the Cancel button to cancel your unsaved changes. Click the Close button to return to the Filters screen.
7. If you want to block the listed PCs from Internet access during the designated days and time, then keep the default setting, Deny. If you want the listed PCs to have Internet filtered during the designated days and time, then click the radio button next to Filter.
8. Set the days when access will be filtered. Select Everyday or the appropriate days of the week.
9. Set the time when access will be filtered. Select 24 Hours, or check the box next to From and use the drop-down boxes to designate a specific time period.
10. Click the Add to Policy button to save your changes and active it.

11. To create or edit additional policies, repeat steps 1-9.
12. To delete an Internet Access Policy, select the policy number, and click the Delete button.

Note:

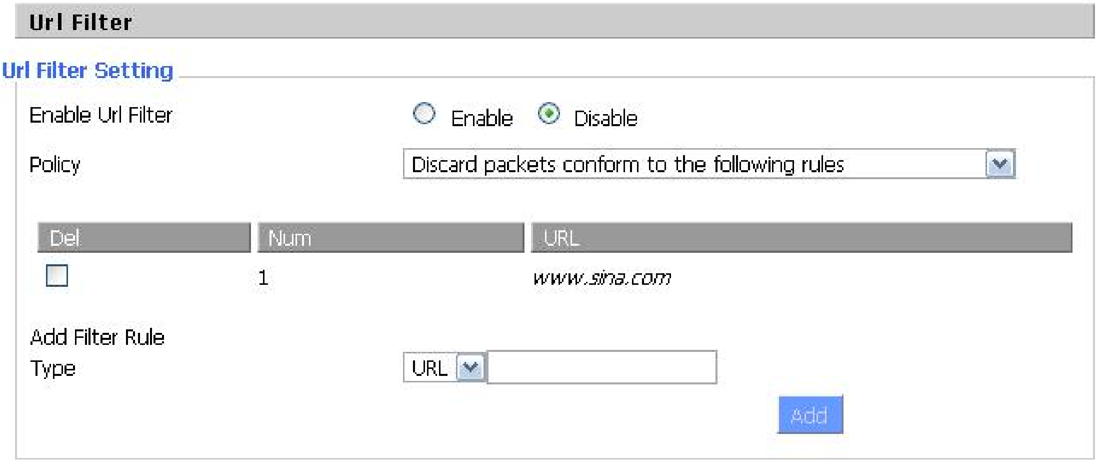
3.3.3.1 The default factory value of policy rules is "filtered". If the user chooses the default policy rules for "refuse", and editing strategies to save or directly to save the settings. If the strategy edited is the first, it will be automatically saved into the second, if not the first, keep the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

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

3.6.2 URL Filter

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

URL filtering function



Url Filter

Url Filter Setting

Enable Url Filter ○ Enable ● Disable

Policy Discard packets conform to the following rules

Del	Num	URL
□	1	www.sina.com

Add Filter Rule

Type URL

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

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

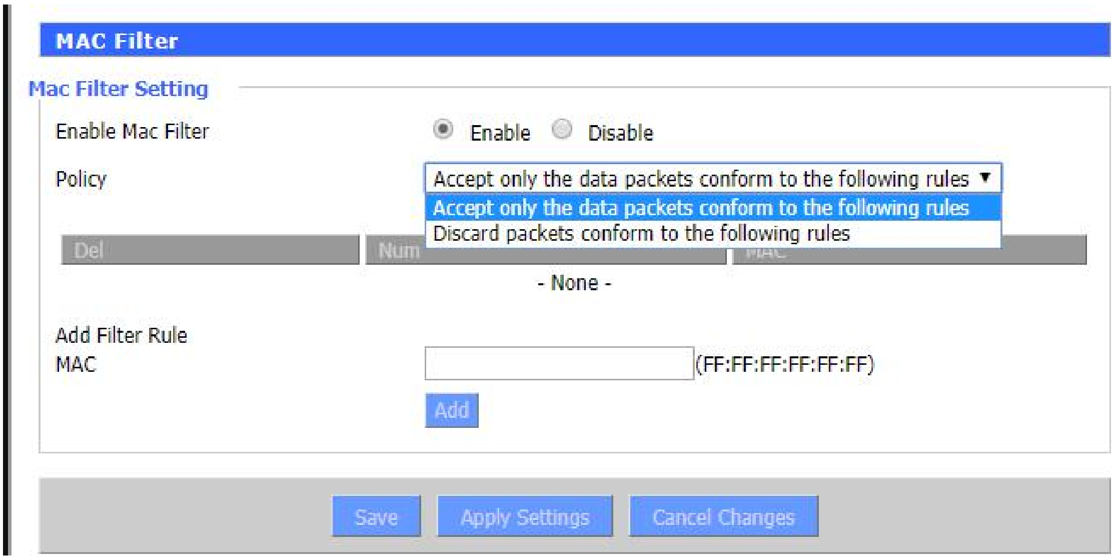
3.6.3 MAC Filter

To do internet access by device MAC.

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

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

Fill device MAC address as FF:FF:FF:FF:FF:FF, then click Add button.



MAC Filter

Mac Filter Setting

Enable Mac Filter ● Enable ○ Disable

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

Accept only the data packets conform to the following rules
Discard packets conform to the following rules
Del
Num
MAC
- None -

Add Filter Rule

MAC (FF:FF:FF:FF:FF:FF)

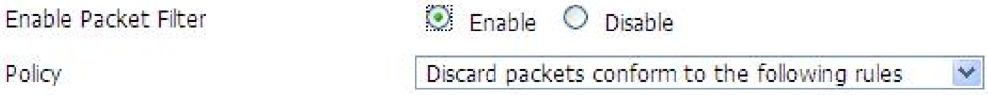
Add
Save
Apply Settings
Cancel Changes

3.6.4 Packet Filter

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

Packet Filter

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



Enable Packet Filter ● Enable ○ Disable

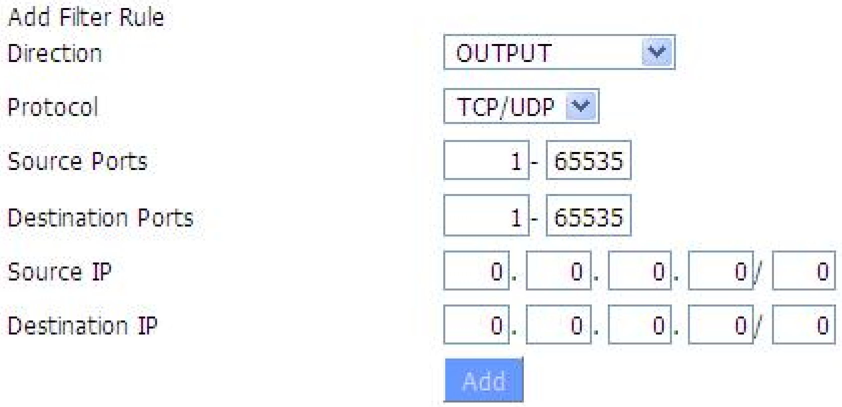
Policy: Discard packets conform to the following rules

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

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

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

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



Add Filter Rule

Direction: OUTPUT

Protocol: TCP/UDP

Source Ports: 1 - 65535

Destination Ports: 1 - 65535

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

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

Direction

input: packet from WAN to LAN
output: packet from LAN to WAN

Protocol: packet protocol type
Source Ports: packet's source port
Destination Ports: packet's destination port
Source IP: packet's source IP address
Destination IP: packet's destination IP address

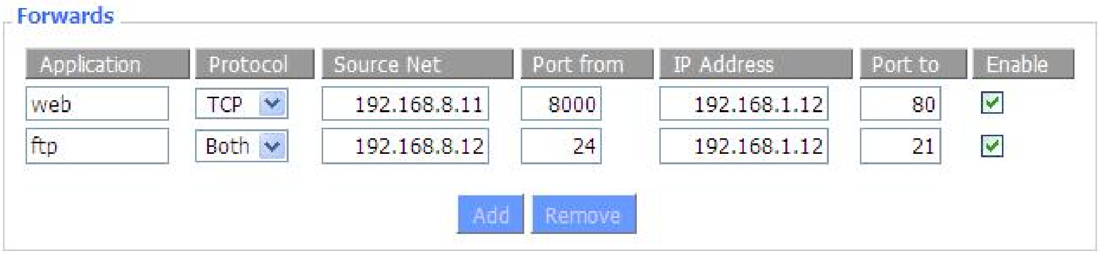
Note: "Source Port" ,"Destination Port" ,"Source IP" ,"Destination IP" could not be all empty ,you have to input at least one of these four parameters.

3.7 NAT

Port forwarding, port range forwarding, and DMZ should be used with public IP or special APN sim card or VPN.

3.7.1 Port Forwarding

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



Forwards

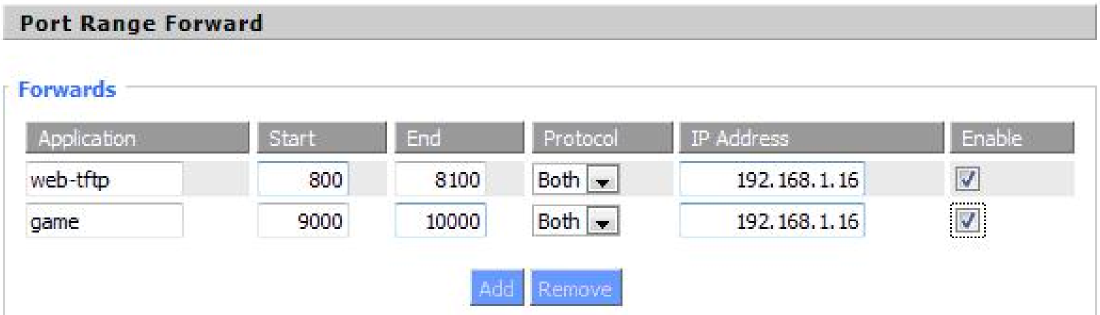
Application	Protocol	Source Net	Port from	IP Address	Port to	Enable
web	TCP	192.168.8.11	8000	192.168.1.12	80	☑
ftp	Both	192.168.8.12	24	192.168.1.12	21	☑

Application: Enter the name of the application in the field provided.
Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.
Source Net: Forward only if sender matches this ip/net (example 192.168.1.0/24).
Port from: Enter the number of the external port (the port number seen by users on the Internet).
IP Address: Enter the IP Address of the PC running the application.
Port to: Enter the number of the internal port (the port number used by the application).
Enable: Click the Enable checkbox to enable port forwarding for the application.

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

3.7.2 Port Range Forwarding

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



Port Range Forward

Forwards

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

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

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

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

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

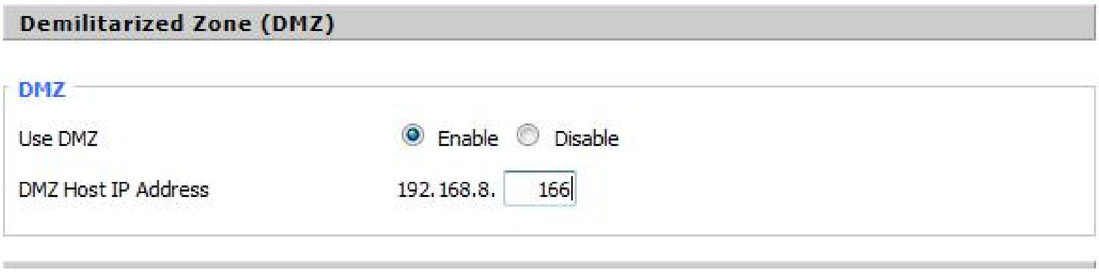
IP Address: Enter the IP Address of the PC running the application.

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

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

3.7.3 DMZ

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



Demilitarized Zone (DMZ)

DMZ

Use DMZ ● Enable ○ Disable

DMZ Host IP Address 192.168.8. 166

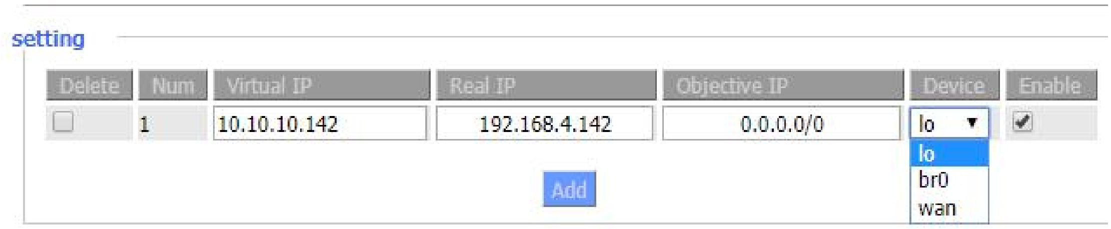
Any PC whose port is being forwarded must should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

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

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

3.7.4 Virtual IP Mapping

Virtual IP Mapping can do cases for that not show real IP from outside users.
Virtual IP: virtual IP will be showed to outside.
Real IP: device real IP.
Objective IP : destination IP when do virtual IP mapping.
Device : choose interface for virtual IP mapping.



setting

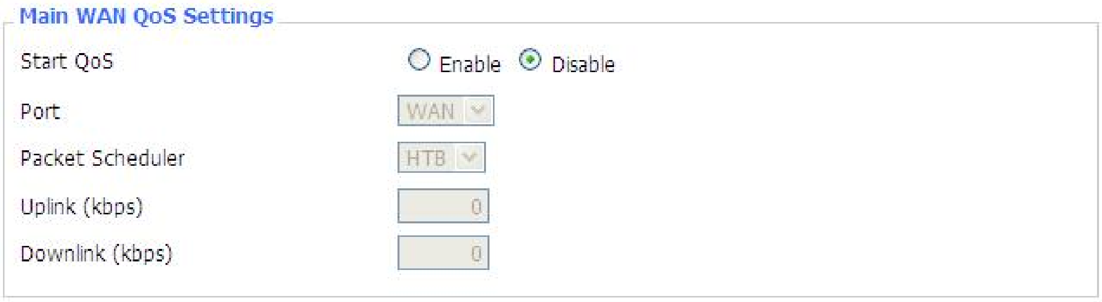
Delete	Num	Virtual IP	Real IP	Objective IP	Device	Enable
□	1	10.10.10.142	192.168.4.142	0.0.0.0/0	lo ▼	☑

3.8 QoS

3.8.1 Basic

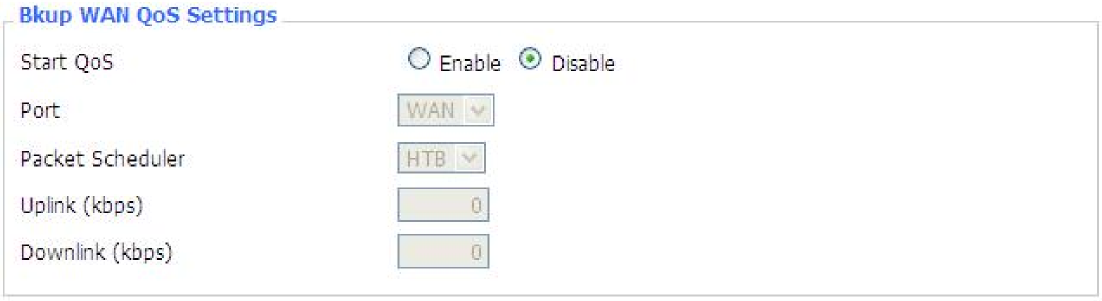
Bandwidth management prioritizes the traffic on your Router. Interactive traffic (telephony, browsing, telnet, etc.) gets priority and bulk traffic (file transfer, P2P) gets low priority. The main goal is to allow both types to live side-by side without unimportant traffic disturbing more critical things.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

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



Main WAN QoS Settings

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



Bkup WAN QoS Settings

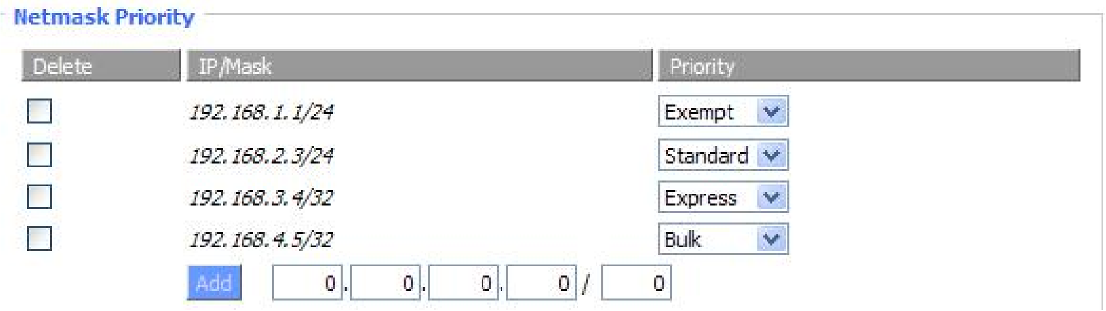
Start QoS	○ Enable ● Disable
Port	WAN
Packet Scheduler	HTB
Uplink (kbps)	0
Downlink (kbps)	0

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

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

3.8.2 Classify

Netmask Priority



Netmask Priority

Delete	IP/Mask	Priority
□	192.168.1.1/24	Exempt
□	192.168.2.3/24	Standard
□	192.168.3.4/32	Express
□	192.168.4.5/32	Bulk

You may specify priority for all traffic from a given IP address or IP Range.

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

3.9 App

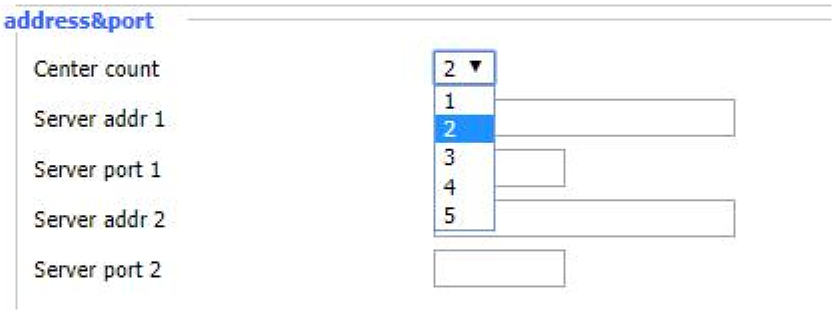
3.9.1 Communication Gateway

Communication gateway is to do communication protocol analysis, can support device communication such as PLC.

Note: FourFaith is trying to make firmware better all the time, so communication gateway part may be different for different versions.

address&port

Here is to configure 1~5 data centers(TCP server IP and port).



address&port

Center count: 2

Server addr 1

Server port 1

Server addr 2

Server port 2

Center count:

can choose from 1~5. 1 means 1 data center, 2 means 2 data centers, ….5 means 5 data centers.

Server addr n, n=1~5, to fill TCP server IP for server n.

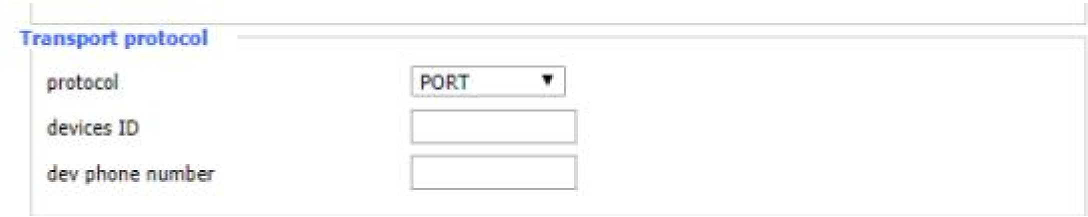
Server port n, n=1~5, to fill TCP server port for server n.

Transport protocol

Here is to configure protocol to connect data center (above data center).

protocol: 9 protocols can be chosen.

(F-G100 will be client to connect to server via described protocol)



Transport protocol

protocol	PORT ▼
devices ID	
dev phone number	

PORT

PORT is a TCP protocol but with a register packet when it connects to server. Register packet will contain device ID.

Fill devices ID and dev phone number(can be any you want), click save and apply settings buttons, then F0G100 will connect to the TCP server, it will send a register packet to server the time F-G100 connects.

protocol	PORT ▼
devices ID	
dev phone number	

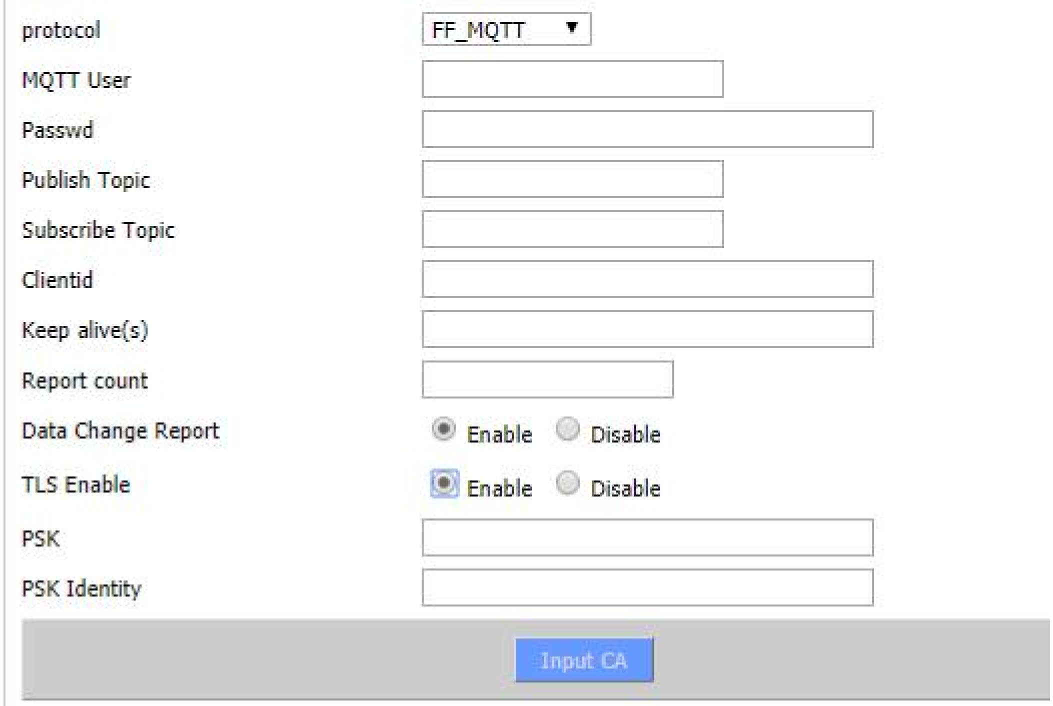
FF_MQTT

FF_MQTT means F-G100 will connect to server via MQTT protocol.

For MQTT part, F-G100 can connect to server with user name and password for mqtt, or can also load key for connection. (depends on mqtt server side)

User can configure data sending topic, data receiving topic, also can configure ID, report count.

Data Change Report enable means data will report when it changes.

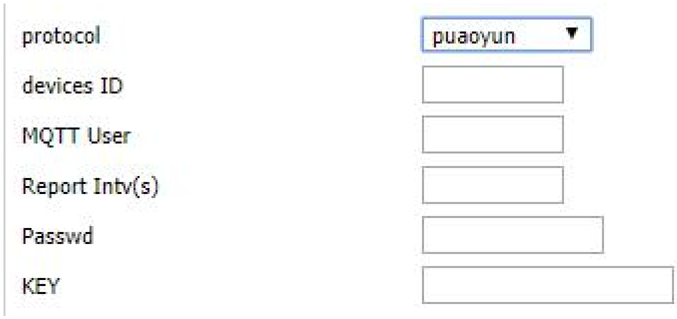


protocol	FF_MQTT ▼
MQTT User	
Passwd	
Publish Topic	
Subscribe Topic	
Clientid	
Keep alive(s)	
Report count	
Data Change Report	● Enable ○ Disable
TLS Enable	● Enable ○ Disable
PSK	
PSK Identity	

puaoyun

puaoyun means F-G100 will connect to puaoyun cloud platform (puaoyun is a IoT platform in China).

Fill needed information one by one and correctly (can get information from puaoyun IOT platform), click save and apply setting button, then F-G100 will connect to puaoyun with filled information,

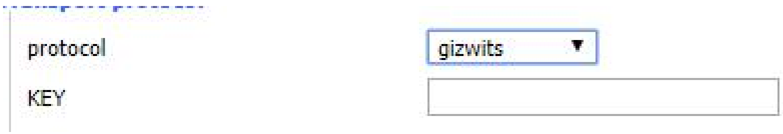


protocol	puaoyun ▼
devices ID	
MQTT User	
Report Intv(s)	
Passwd	
KEY	

gizwits

gizwits means F-G100 will connect to gizwits cloud platform(gizwits is a IoT platform in China).

Fill needed information correctly (can get information from gizwits IOT platform), click save and apply setting button, then F-G100 will connect to gizwits with filled key,

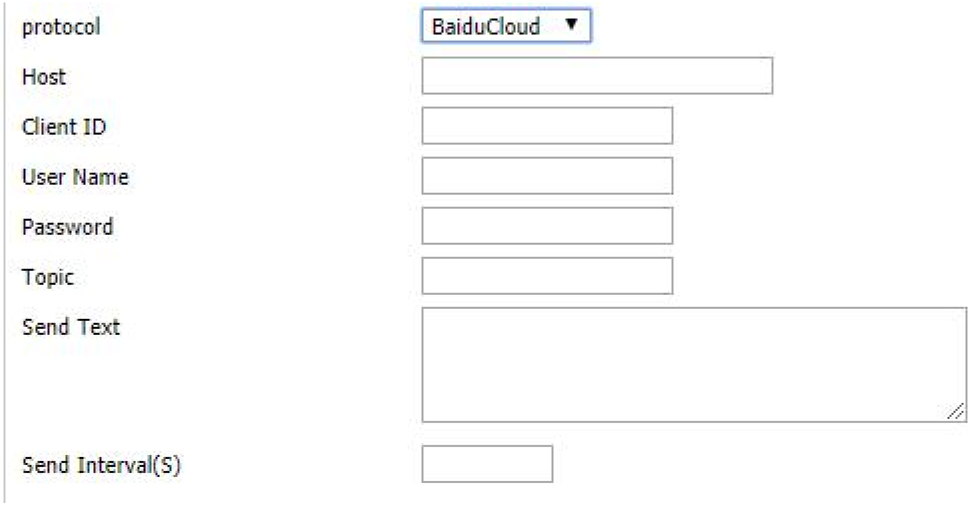


protocol	gizwits ▼
KEY	

BaiduCloud

BaiduCloud means F-G100 will connect to Baidu cloud platform (Baidu Cloud is a IoT platform in China).

Fill needed information one by one and correctly (can get information from Baidu IOT platform), click save and apply setting button, then F-G100 will connect to Baidu cloud platform with filled information.

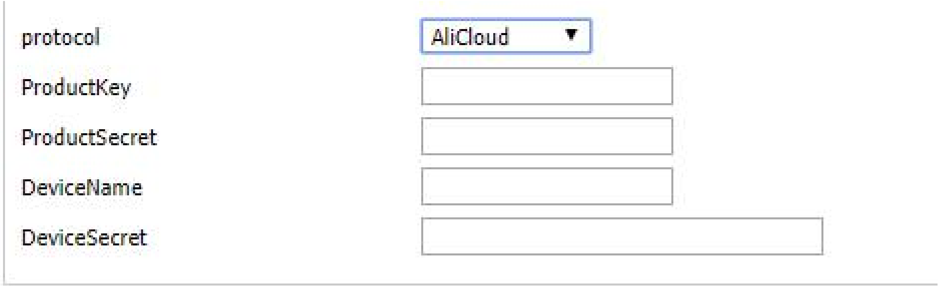


protocol	BaiduCloud ▼
Host	
Client ID	
User Name	
Password	
Topic	
Send Text	
Send Interval(S)	

AliCloud

AliCloud means F-G100 will connect to Ali cloud platform (Ali Cloud is a IoT platform in China).

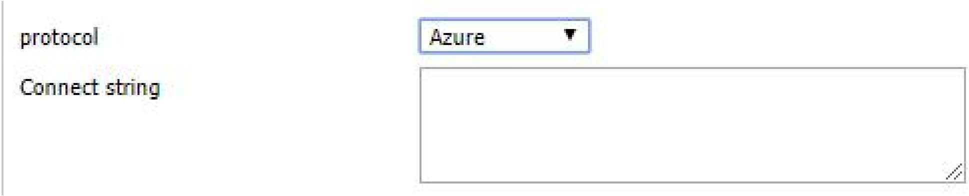
Fill needed information one by one and correctly (can get information from Ali IOT platform), click save and apply setting button, then F-G100 will connect to Ali Cloud platform with filled information



protocol	AliCloud ▼
ProductKey	
ProductSecret	
DeviceName	
DeviceSecret	

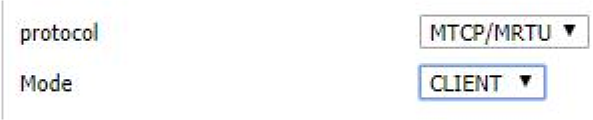
Azure

For Azure connection, F-G100 supports use connect string to connect to it. Fill connect string which got from mircosoft, click save and apply settings button, then F-G100 will connect to Azure,

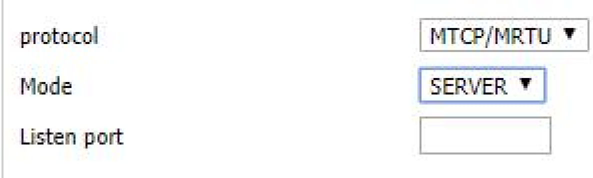


protocol	Azure ▼
Connect string	

MTCP/MRTU



protocol	MTCP/MRTU ▼
Mode	CLIENT ▼



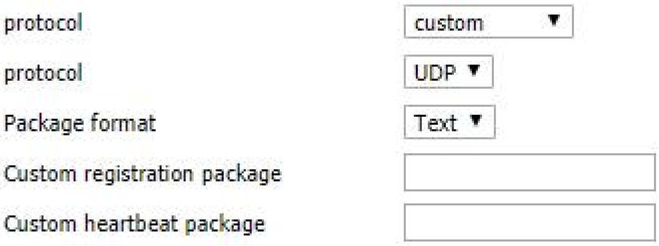
protocol	MTCP/MRTU ▼
Mode	SERVER ▼
Listen port	

Custom

F-G100 will connect to server with standard TCP or UDP(depends on tcp or udp is chosen),

There will have register packet when F-G100 connects to server, register packet is filled string for Custom registration package; there will have a heartbeat data packet to server to tell server that F-G100 connection is still up, heartbeat packet is filled string for Custom hearbeat package.

Format for register package and heat-beat package depends on format choose to be test or hex.



protocol	custom ▼
protocol	UDP ▼
Package format	Text ▼
Custom registration package	
Custom heartbeat package	

Apply protocol

Choose COM for serial port device connection, choose different COM depends on physical connection.

Choose LAN for Ethernet port device connection. LAN1, LAN2,LAN3,LAN4 doesn’t mean F-G100 physical LAN1/2/3/4. it means can connect 4 Ethernet devices, can use 4 different protocol or same protocol.

Different COM and LAN can be used at same time with different or same configuration.

COM

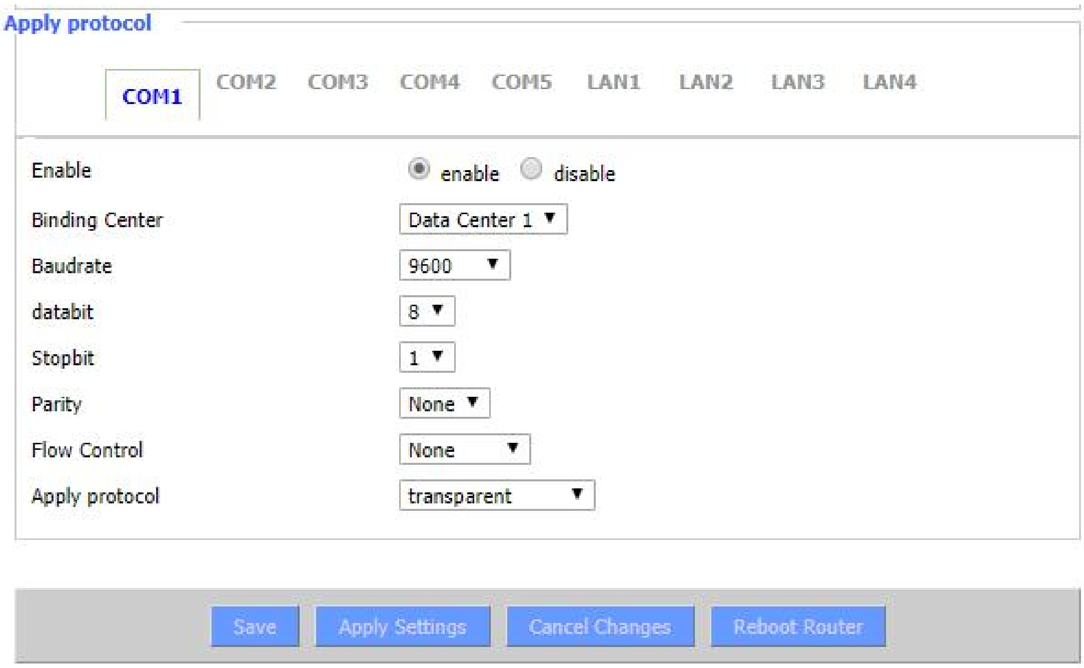
First, Enable it.

Binding Center means com data will send to the chosen data center with configuration server protocol. Can choose 1/2/3/4/5 or ALL, ALL means com data will send to all 5 servers. Disable means no need send to data center.

Baudrate (9600/19200/38400/57600/115200), databit (8/7/6/5), stopbit(2/1), parity(even /odd/none) are to set serial port parameters, configure as real device parameters.

Flow Control can be chosen as none, hardware, software, also depends on serial port device, usually use none.

Apply protocol can choose transparent or acquisition mode. transparent means com device will send to server transparently, it will be used for device which will auto send data usually; acquisition mode means F-G100 will read com device with configured protocol, check below in detail.


Apply protocol

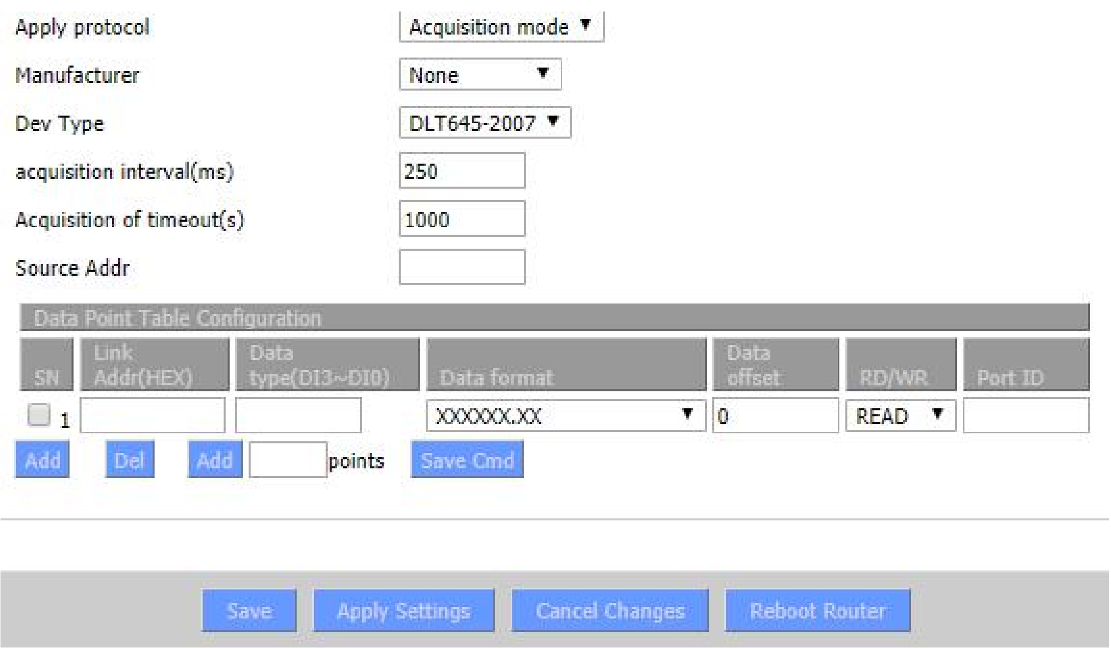
Enable	● enable ○ disable
Binding Center	Data Center 1 ▼
Baudrate	9600 ▼
databit	8 ▼
Stopbit	1 ▼
Parity	None ▼
Flow Control	None ▼
Apply protocol	transparent ▼

Manufacturer means F-G100 can support different serial port PLC, such as SIEMENS, MITSUBISHI, Schnedier, none means serial device is not from those manufacturers but has its own protocol.

Dev Type is to choose protocol/PLC type for com device.

Then can configure acquisitive parameters for serial port device connected depends on different devices and parameters. (need to know something about PLC protocol first)

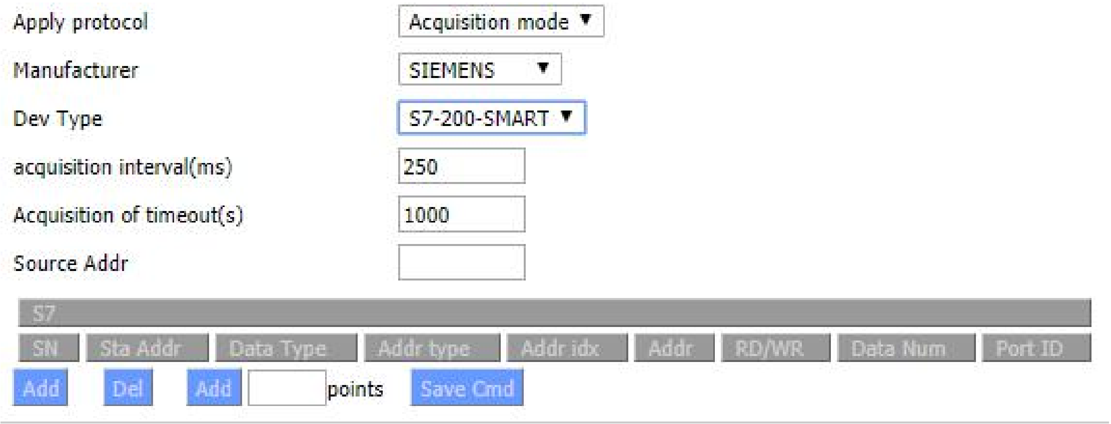
Acquisition interval means time interval to read serial port device.



Apply protocol	Acquisition mode ▼
Manufacturer	None ▼
Dev Type	DLT645-2007 ▼
acquisition interval(ms)	250
Acquisition of timeout(s)	1000
Source Addr	

Data Point Table Configuration

SN	Link Addr(HEX)	Data type(DI3~DI0)	Data format	Data offset	RD/WR	Port ID
□ 1			XXXXXX.XX ▼	0	READ ▼	



Apply protocol	Acquisition mode ▼
Manufacturer	SIEMENS ▼
Dev Type	S7-200-SMART ▼
acquisition interval(ms)	250
Acquisition of timeout(s)	1000
Source Addr	

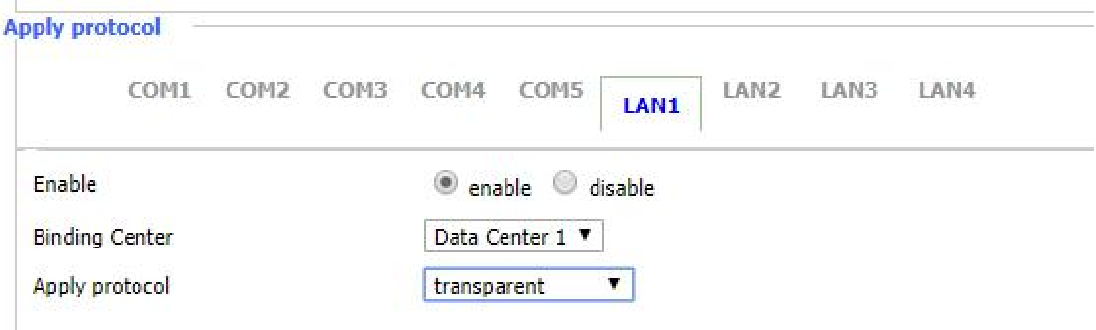
S7

SN	Sta Addr	Data Type	Addr type	Addr idx	Addr	RD/WR	Data Num	Port ID

LAN

First , Enable it.

Apply protocol can choose transparent or acquisition mode. Transparent means Ethernet device is transparent transmission; acquisition mode means F-G100 will to read Ethernet device with configuration.



Apply protocol

Enable	● enable ○ disable
Binding Center	Data Center 1 ▼
Apply protocol	transparent ▼

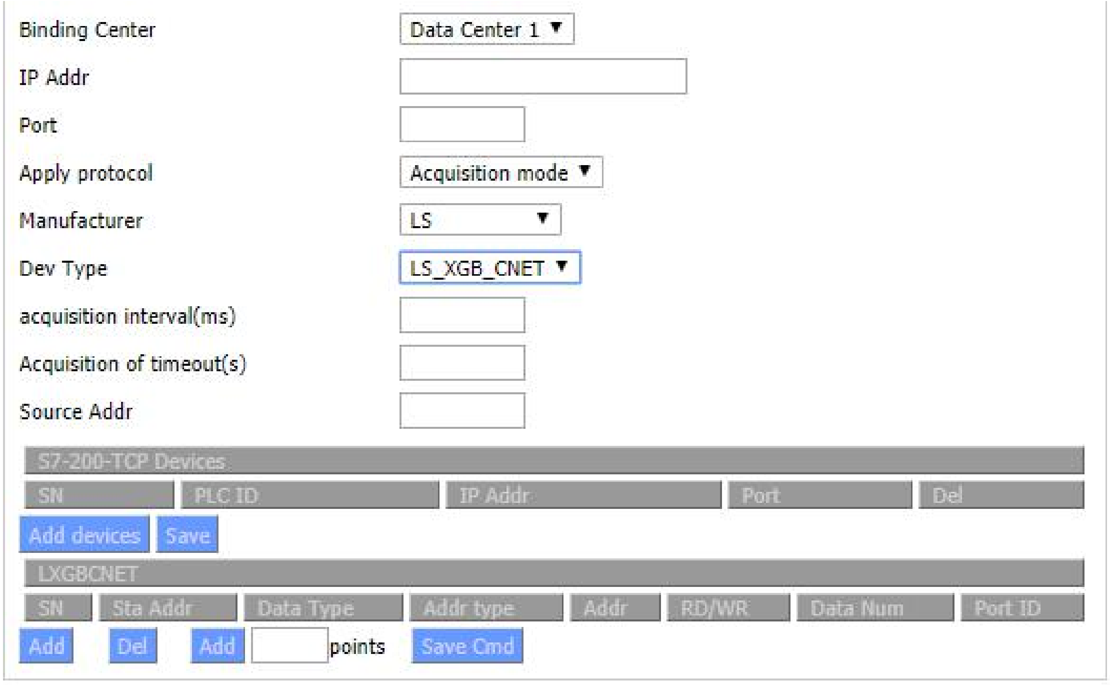
For Ethernet PLC/device, need to fill device IP and port usually to make F0G100 to communicate with PLC/device first. (there has IP and port setting when you choose different manufacturer and dev.)

Manufacturer means F-G100 can support different Ethernet PLC, such as SIEMENS, MITSUBISHI, Schnedier, none means Ethernet device is not from those manufacturers but has its own protocol.

Dev Type is to choose protocol/PLC type for Ethernet device.

Then can configure acquisitive parameters for Ethernet port device connected depends on different devices and parameters. (need to know something about PLC protocol first)

Acquisition interval means time interval to read serial port device.



Binding Center	Data Center 1 ▼
IP Addr	
Port	
Apply protocol	Acquisition mode ▼
Manufacturer	LS ▼
Dev Type	LS_XGB_CNET ▼
acquisition interval(ms)	
Acquisition of timeout(s)	
Source Addr	

S7-200-TCP Devices

SN	PLC ID	IP Addr	Port	Del

LXGBCNET

SN	Sta Addr	Data Type	Addr type	Addr	RD/WR	Data Num	Port ID

3.9.2 Baidu Iot

Baidu Iot is a special application to connect device to Baidu IoT platform .

Endpoint Address: endpoint address for Baidu IoT connection.

Device: Device name for Baidu IoT connection.

Username: Username for Baidu IoT connection.

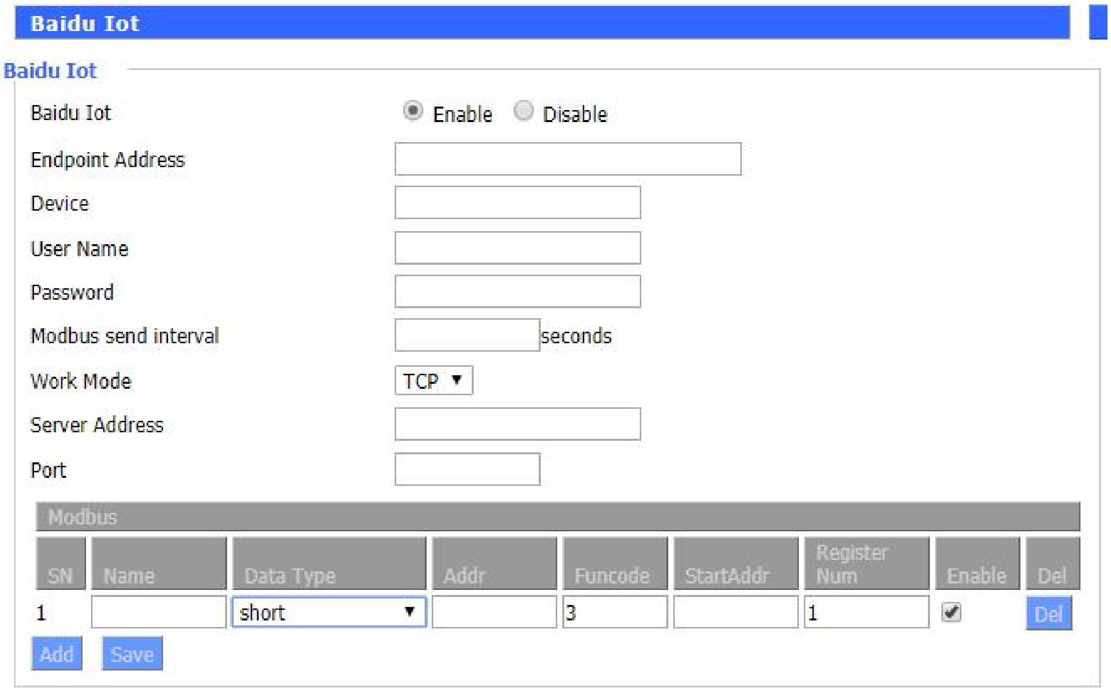
Password: Password for Baidu IoT connection.

Modbus send interval: modbus auto acquisition time interval.

Work mode: choose TCP or UDP/

Server Address: Server address for Baidu IoT connection.

Port: Server port for Baidu IoT connection.



Baidu Iot

Baidu Iot

Baidu Iot ● Enable ○ Disable

Endpoint Address

Device

User Name

Password

Modbus send interval seconds

Work Mode TCP ▼

Server Address

Port

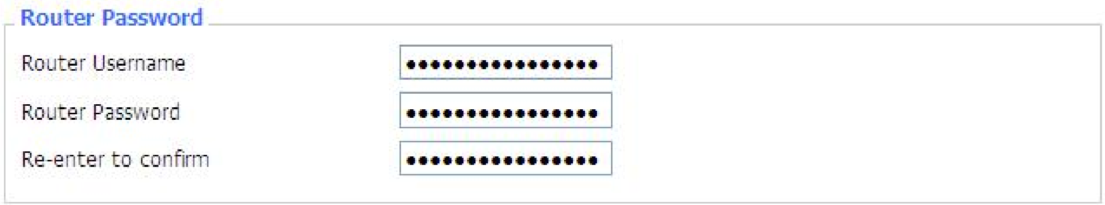
Modbus

SN	Name	Data Type	Addr	Funcode	StartAddr	Register Num	Enable	Del
1		short ▼		3		1	☑	Del

3.10 Admin

3.10.1 Management

The Management screen allows you to change the Router's settings. On this page you will find most of the configurable items of the Router code.



Router Password

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

The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.

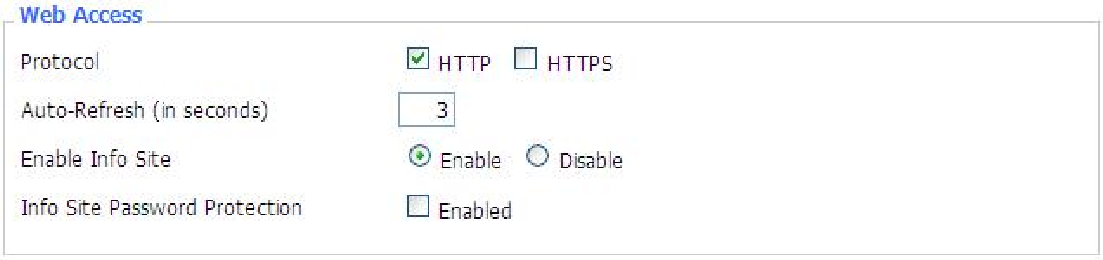
Note：

Default username is admin.

It is strongly recommended that you change the factory default password of the Router, which is admin. All users who try to access the Router's web-based utility or Setup Wizard will be prompted for the Router's password.

Web Access

This feature allows you to manage the Router using either HTTP protocol or the HTTPS protocol. If you choose to disable this feature, a manual reboot will be required.You can also activate or not the Router information web page. It's now possible to password protect this page (same username and password than above).



Web Access

Protocol ☑ HTTP □ HTTPS

Auto-Refresh (in seconds) 3

Enable Info Site ● Enable ○ Disable

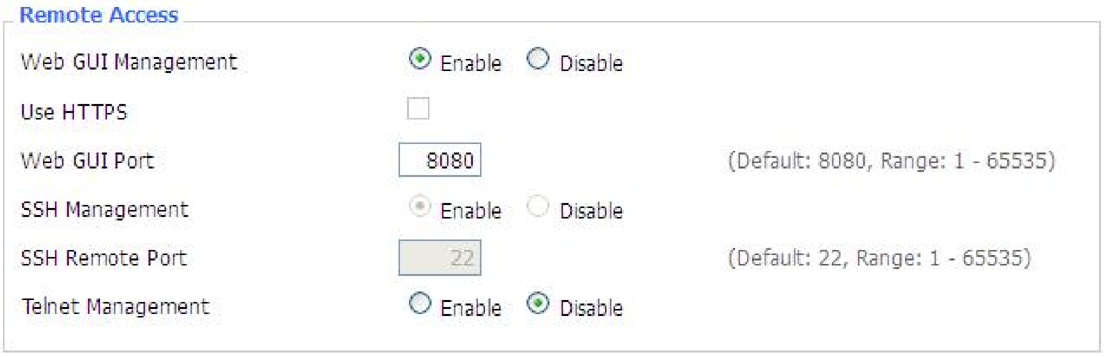
Info Site Password Protection □ Enabled

Protocol： This feature allows you to manage the Router using either HTTP protocol or the HTTPS protocol

Auto-Refresh： Adjusts the Web GUI automatic refresh interval. 0 disables this feature completely

Enable Info Site： Enable or disable the login system information page

Info Site Password Protection： Enable or disable the password protection feature of the system information page



Remote Access

Web GUI Management ● Enable ○ Disable

Use HTTPS □

Web GUI Port 8080 (Default: 8080, Range: 1 - 65535)

SSH Management ● Enable ○ Disable

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

Telnet Management ○ Enable ● Disable

Remote Access： This feature allows you to manage the Router from a remote location, via the Internet. To disable this feature, keep the default setting, Disable. To enable this feature, select Enable, and use the specified port (default is 8080) on your PC to remotely manage the Router. You must also change the Router's default password to one of your own, if you haven't already.

To remotely manage the Router, enter http://xxx.xxx.xxx.xxx:8080 (the x's represent the Router's Internet IP address, and 8080 represents the specified port) in your web browser's address field. You will be asked for the Router's password.

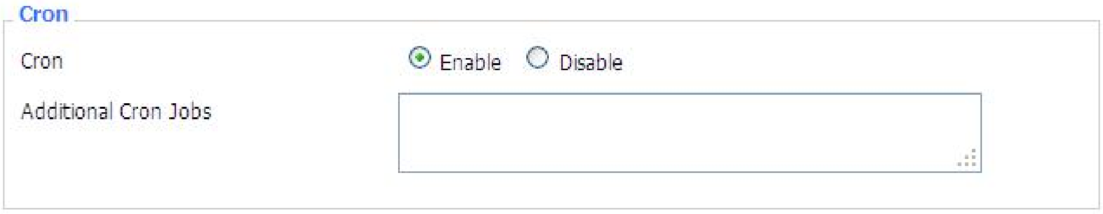
If you use https you need to specify the url as https://xxx.xxx.xxx.xxx:8080 (not all firmwares does support this without rebuilding with SSL support).

SSH Management： You can also enable SSH to remotely access the Router by Secure Shell. Note that SSH daemon needs to be enable in Services page.

Note：

> If the Remote Router Access feature is enabled, anyone who knows the Router's Internet IP address and password will be able to alter the Router's settings.

Telnet Management： Enable or disable remote Telnet function

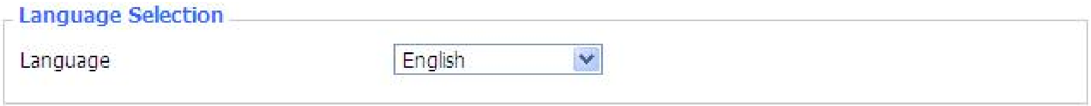


Cron

Cron ● Enable ○ Disable

Additional Cron Jobs

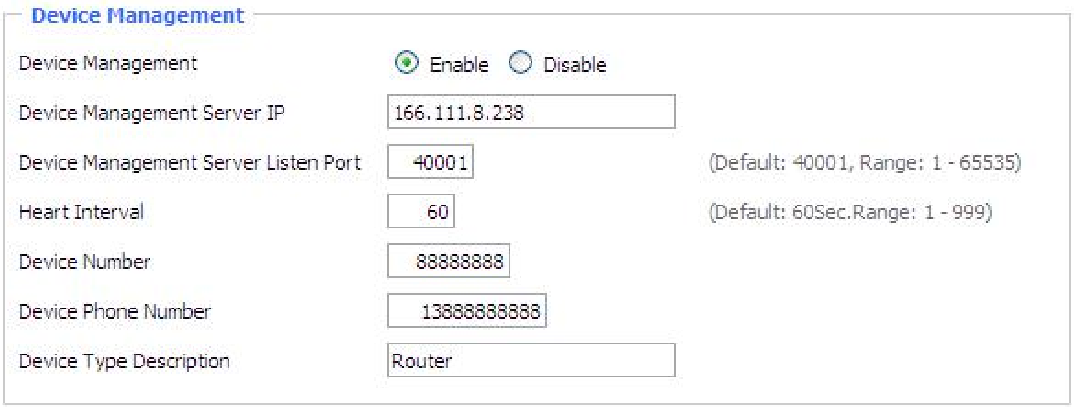
Cron： The cron subsystem schedules execution of Linux commands. You'll need to use the command line or startup scripts to actually use this.



Language Selection

Language: English

Language： Set up the Router page shows the type of language, including simplified Chinese and English.



Device Management

Device Management	● Enable ○ Disable	
Device Management Server IP	166.111.8.238	
Device Management Server Listen Port	40001	(Default: 40001, Range: 1 - 65535)
Heart Interval	60	(Default: 60Sec.Range: 1 - 999)
Device Number	88888888	
Device Phone Number	13888888888	
Device Type Description	Router	

Remote Upgrade: custom-developed remote management server for this station Router monitoring and management, configuration parameters, WIFI advertising updates.

3.10.2 Keep Alive

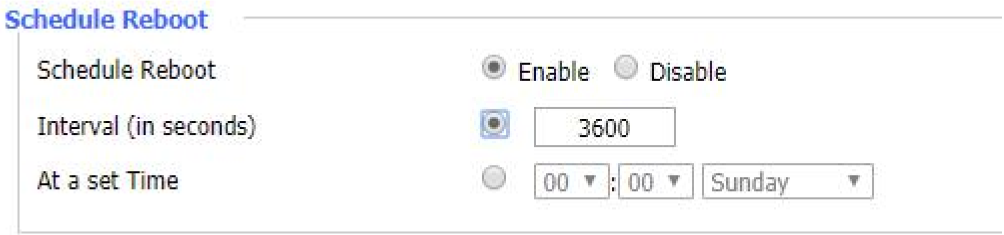
You can schedule regular reboots for the Router :

Regularly after xxx seconds.

At a specific date time each week or everyday.

Note：

For date based reboots Cron must be activated. See Management for Cron activation.

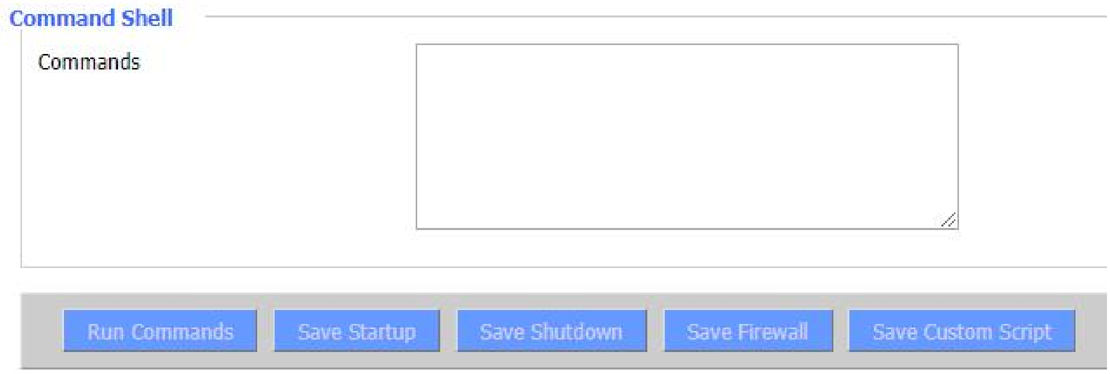


Schedule Reboot

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

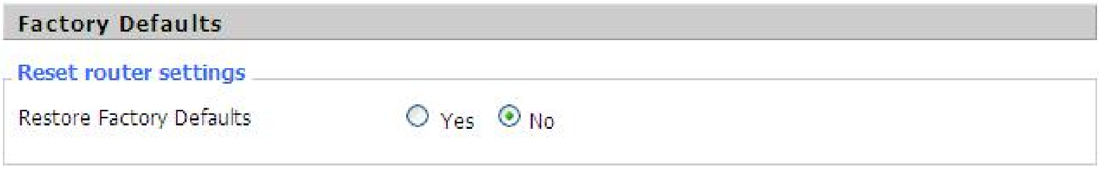
3.10.3 Commands

Commands： You are able to run command lines directly via the Web interface.



Run Command： You can run command lines via the web interface. Fill the text area with your command and click Run Commands to submit.
Startup： You can save some command lines to be executed at startup's Router. Fill the text area with commands (only one command by row) and click Save Startup.
Shutdown： You can save some command lines to be executed at shutdown's Router. Fill the text area with commands (only one command by row) and click Save Shutdown.
Firewall： Each time the firewall is started, it can run some custom iptables instructions. Fill the text area with firewall's instructions (only one command by row) and click Save Firewall.
Custom Script：Custom script is stored in /tmp/custom.sh file. You can run it manually or use cron to call it. Fill the text area with script's instructions (only one command by row) and click Save Custom Script.

3.10.4 Factory Default



Restore Factory Defaults ○ Yes ● No

Reset Router settings： Click the Yes button to reset all configuration settings to their default values. Then click the Apply Settings button.

Note：

> Any settings you have saved will be lost when the default settings are restored. After restoring the Router is accessible under the default IP address 192.168.1.1 and the default password admin.

3.10.5 Firmware Upgrade

Firmware Upgrade： New firmware versions are posted at www..com and can be downloaded. If the Router is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

Note：

> When you upgrade the Router's firmware, you lose its configuration settings, so make sure you write down the Router settings before you upgrade its firmware.

To upgrade the Router's firmware:

1. Download the firmware upgrade file from the website.

2. Click the Browse... button and chose the firmware upgrade file.

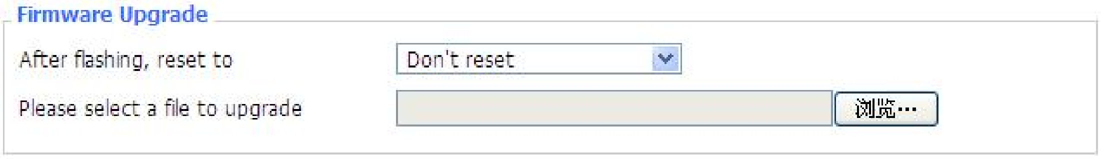
3. Click the Upgrade button and wait until the upgrade is finished.

Note：

Upgrading firmware may take a few minutes.

Do not turn off the power or press the reset button!

After flashing, reset to： If you want to reset the Router to the default settings for the firmware version you are upgrading to, click the Firmware Defaults option.



Firmware Upgrade

After flashing, reset to: Don't reset

Please select a file to upgrade

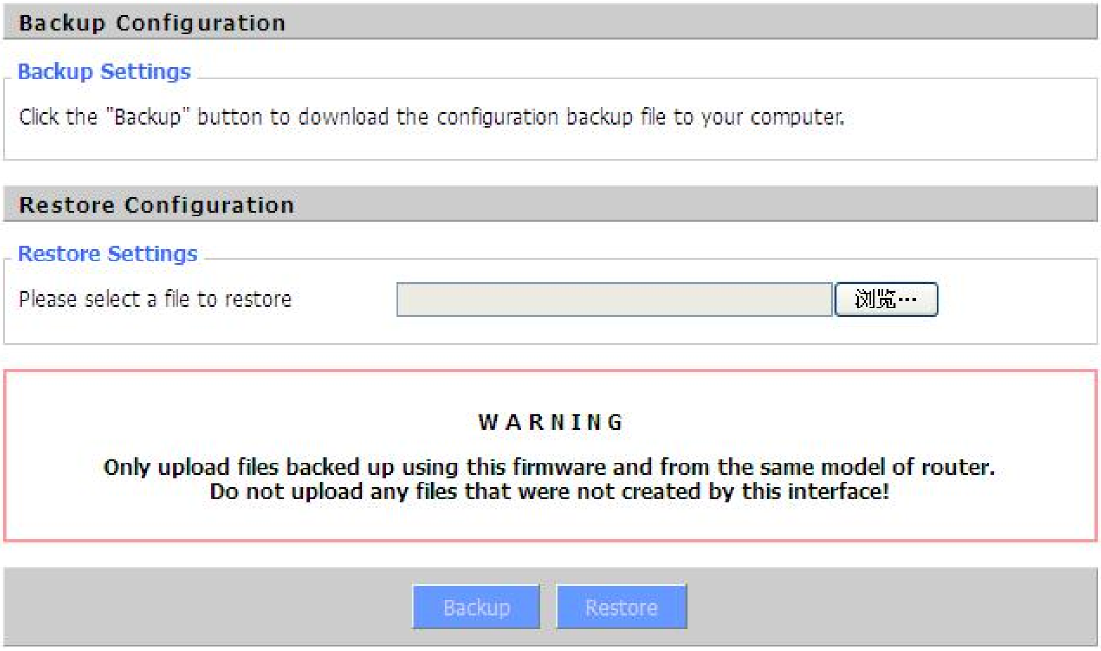
3.10.6 Backup

Backup Settings：You may backup your current configuration in case you need to reset the Router back to its factory default settings.Click the Backup button to backup your current configuration.

Restore Settings： Click the Browse... button to browse for a configuration file that is currently saved on your PC.Click the Restore button to overwrite all current configurations with the ones in the configuration file.

Note：

Only restore configurations with files backed up using the same firmware and the same model of Router.



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!

3.11 Status

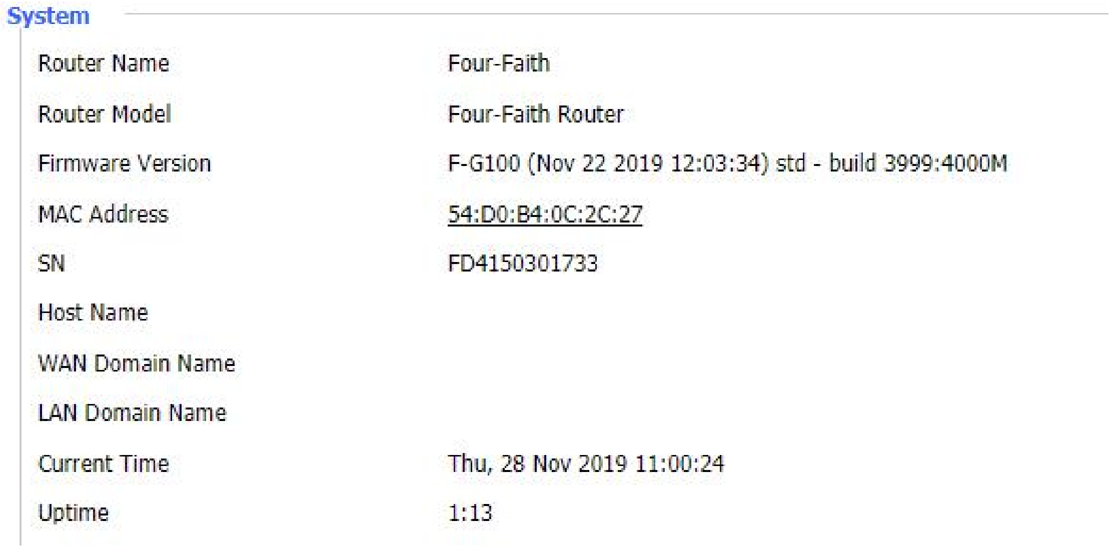
3.11.1 Router

Router Name: name of the Router, setting→basic setting to modify

Router Model: model of the Router, unavailable to modify

Firmware Version: software version information

MAC Address: MAC address of WAN, setting→Clone MAC Address to modify
Host Name: host name of the Router, setting→basic setting to modify
WAN Domain Name: domain name of WAN, setting→basic setting to modify
LAN Domain Name: domain name of LAN, unavailable to modify
Current Time: local time of the system
Uptime: operating uptime as long as the system is powered on



System

Router Name	Four-Faith
Router Model	Four-Faith Router
Firmware Version	F-G100 (Nov 22 2019 12:03:34) std - build 3999:4000M
MAC Address	54:D0:B4:0C:2C:27
SN	FD4150301733
Host Name	
WAN Domain Name	
LAN Domain Name	
Current Time	Thu, 28 Nov 2019 11:00:24
Uptime	1:13

Total Available: the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: free memory, the Router will reboot if the memory is less than 500kB

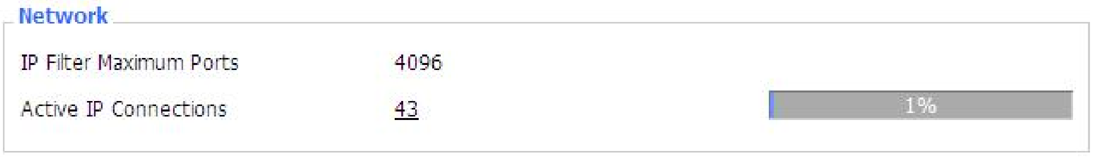
Used: used memory, total available memory minus free memory

Buffers: used memory for buffers,

Cached: the memory used by high-speed cache memory

Active: active use of buffer or cache memory page file size

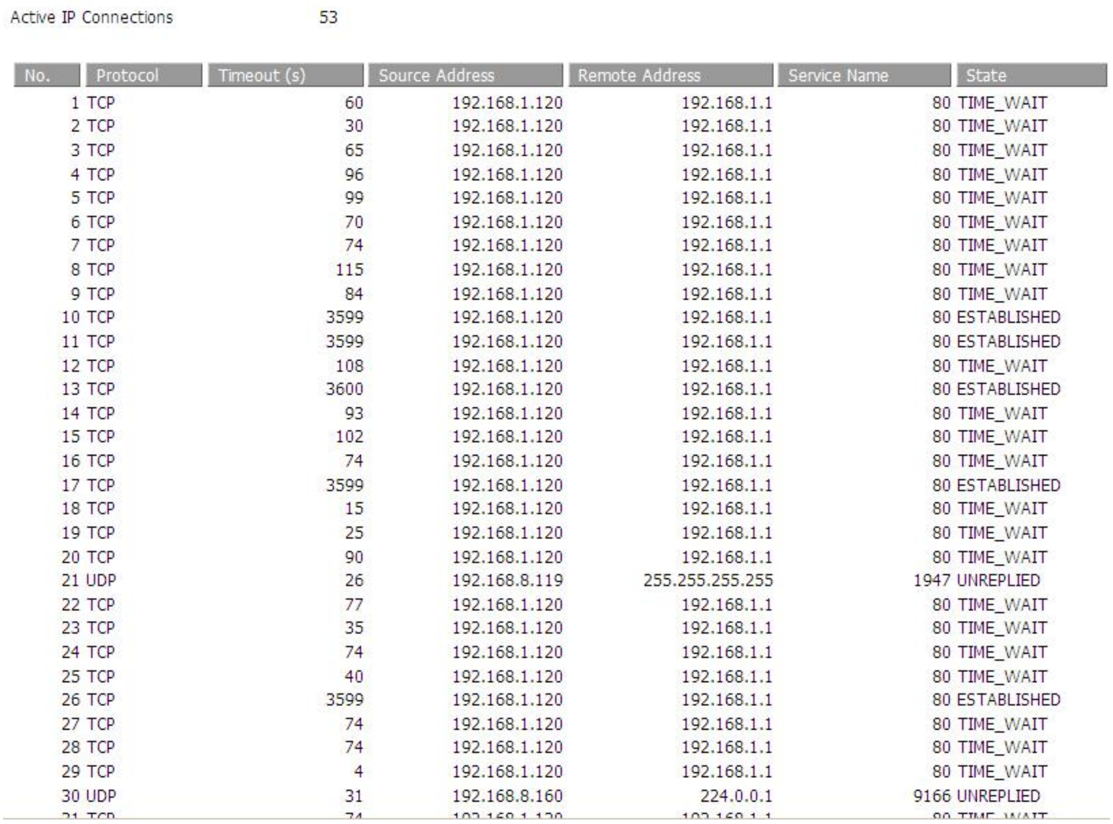
Inactive: not often used in a buffer or cache memory page file size



Network

IP Filter Maximum Ports	4096	
Active IP Connections	43	1%

IP Filter Maximum Ports: preset is 4096, available to re-management
Active IP Connections: real time monitor active IP connections of the system, click to see the table as blow:



Active IP Connections 53

No.	Protocol	Timeout (s)	Source Address	Remote Address	Service Name	State
1	TCP	60	192.168.1.120	192.168.1.1	80	TIME_WAIT
2	TCP	30	192.168.1.120	192.168.1.1	80	TIME_WAIT
3	TCP	65	192.168.1.120	192.168.1.1	80	TIME_WAIT
4	TCP	96	192.168.1.120	192.168.1.1	80	TIME_WAIT
5	TCP	99	192.168.1.120	192.168.1.1	80	TIME_WAIT
6	TCP	70	192.168.1.120	192.168.1.1	80	TIME_WAIT
7	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
8	TCP	115	192.168.1.120	192.168.1.1	80	TIME_WAIT
9	TCP	84	192.168.1.120	192.168.1.1	80	TIME_WAIT
10	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
11	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
12	TCP	108	192.168.1.120	192.168.1.1	80	TIME_WAIT
13	TCP	3600	192.168.1.120	192.168.1.1	80	ESTABLISHED
14	TCP	93	192.168.1.120	192.168.1.1	80	TIME_WAIT
15	TCP	102	192.168.1.120	192.168.1.1	80	TIME_WAIT
16	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
17	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
18	TCP	15	192.168.1.120	192.168.1.1	80	TIME_WAIT
19	TCP	25	192.168.1.120	192.168.1.1	80	TIME_WAIT
20	TCP	90	192.168.1.120	192.168.1.1	80	TIME_WAIT
21	UDP	26	192.168.8.119	255.255.255.255	1947	UNREPLIED
22	TCP	77	192.168.1.120	192.168.1.1	80	TIME_WAIT
23	TCP	35	192.168.1.120	192.168.1.1	80	TIME_WAIT
24	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
25	TCP	40	192.168.1.120	192.168.1.1	80	TIME_WAIT
26	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
27	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
28	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
29	TCP	4	192.168.1.120	192.168.1.1	80	TIME_WAIT
30	UDP	31	192.168.8.160	224.0.0.1	9166	UNREPLIED
31	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT

Active IP Connections: total active IP connections

Protocol: connection protocol

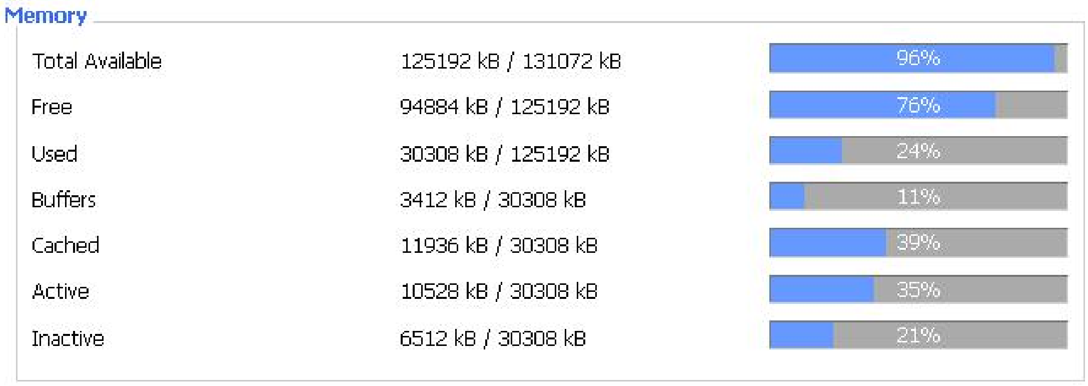
Timeouts: connection timeouts, unit is second

Source Address: source IP address

Remote Address: remote IP address

Service Name: connecting service port

Status: displayed status



Memory

Total Available	125192 kB / 131072 kB	96%
Free	94884 kB / 125192 kB	76%
Used	30308 kB / 125192 kB	24%
Buffers	3412 kB / 30308 kB	11%
Cached	11936 kB / 30308 kB	39%
Active	10528 kB / 30308 kB	35%
Inactive	6512 kB / 30308 kB	21%

Total Available: the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: free memory, the Router will reboot if the memory is less than 500kB

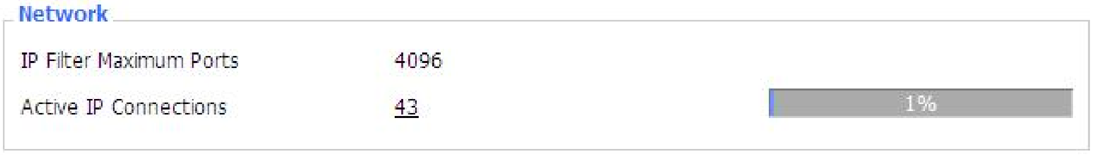
Used: used memory, total available memory minus free memory

Buffers: used memory for buffers,

Cached: the memory used by high-speed cache memory

Active: active use of buffer or cache memory page file size

Inactive: not often used in a buffer or cache memory page file size

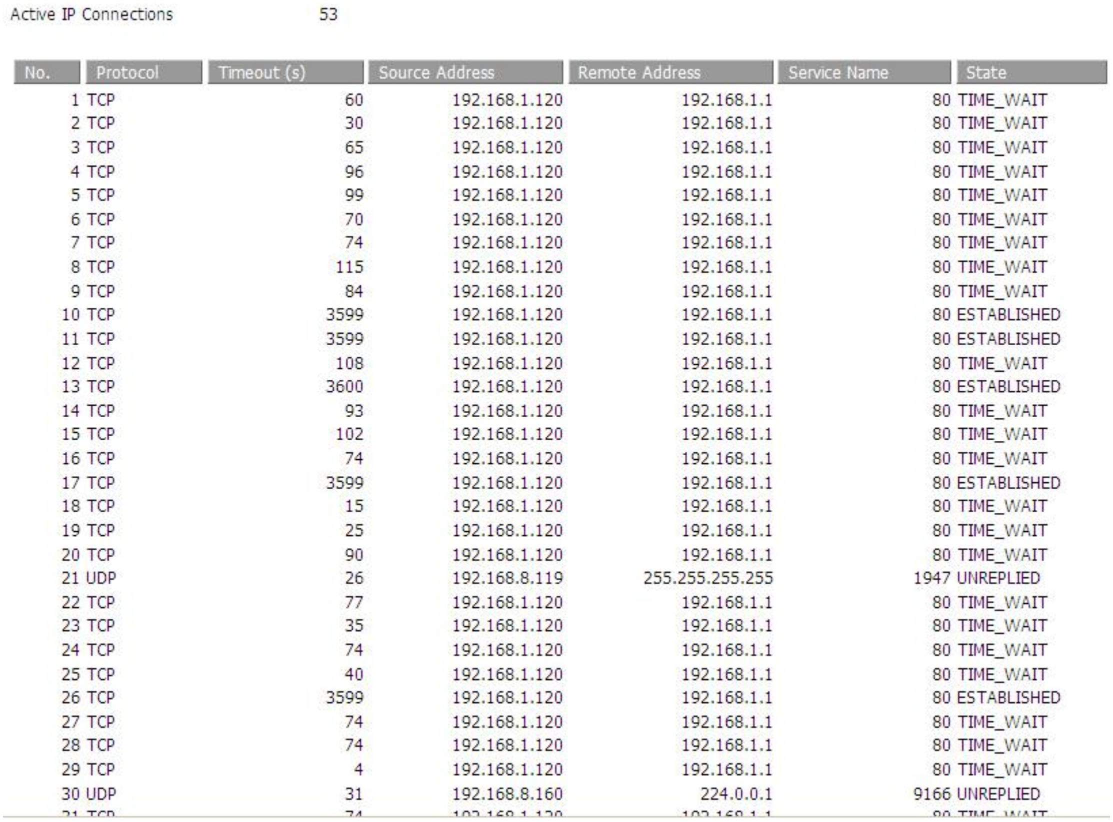


Network

IP Filter Maximum Ports	4096	
Active IP Connections	43	1%

IP Filter Maximum Ports: preset is 4096, available to re-management

Active IP Connections: real time monitor active IP connections of the system, click to see the table as blow:



Active IP Connections 53

No.	Protocol	Timeout (s)	Source Address	Remote Address	Service Name	State
1	TCP	60	192.168.1.120	192.168.1.1	80	TIME_WAIT
2	TCP	30	192.168.1.120	192.168.1.1	80	TIME_WAIT
3	TCP	65	192.168.1.120	192.168.1.1	80	TIME_WAIT
4	TCP	96	192.168.1.120	192.168.1.1	80	TIME_WAIT
5	TCP	99	192.168.1.120	192.168.1.1	80	TIME_WAIT
6	TCP	70	192.168.1.120	192.168.1.1	80	TIME_WAIT
7	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
8	TCP	115	192.168.1.120	192.168.1.1	80	TIME_WAIT
9	TCP	84	192.168.1.120	192.168.1.1	80	TIME_WAIT
10	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
11	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
12	TCP	108	192.168.1.120	192.168.1.1	80	TIME_WAIT
13	TCP	3600	192.168.1.120	192.168.1.1	80	ESTABLISHED
14	TCP	93	192.168.1.120	192.168.1.1	80	TIME_WAIT
15	TCP	102	192.168.1.120	192.168.1.1	80	TIME_WAIT
16	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
17	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
18	TCP	15	192.168.1.120	192.168.1.1	80	TIME_WAIT
19	TCP	25	192.168.1.120	192.168.1.1	80	TIME_WAIT
20	TCP	90	192.168.1.120	192.168.1.1	80	TIME_WAIT
21	UDP	26	192.168.8.119	255.255.255.255	1947	UNREPLIED
22	TCP	77	192.168.1.120	192.168.1.1	80	TIME_WAIT
23	TCP	35	192.168.1.120	192.168.1.1	80	TIME_WAIT
24	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
25	TCP	40	192.168.1.120	192.168.1.1	80	TIME_WAIT
26	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
27	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
28	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
29	TCP	4	192.168.1.120	192.168.1.1	80	TIME_WAIT
30	UDP	31	192.168.8.160	224.0.0.1	9166	UNREPLIED
31	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT

Active IP Connections: total active IP connections

Protocol: connection protocol

Timeouts: connection timeouts, unit is second

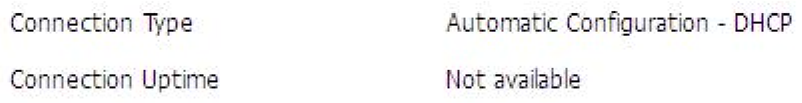
Source Address: source IP address

Remote Address: remote IP address

Service Name: connecting service port

Status: displayed status

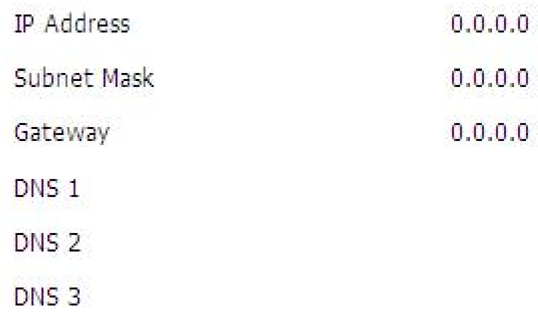
3.11.2 WAN



Connection Type	Automatic Configuration - DHCP
Connection Uptime	Not available

Connection Type: disabled, static IP, automatic configuration-DHCP, PPPOE, PPTP, L2TP, 3G/UMTS

Connection Uptime: connecting uptime; If disconnect, display Not available



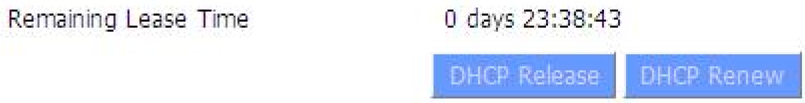
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS 1	
DNS 2	
DNS 3	

IP Address: IP address of Router WAN

Subnet Mask: subnet mask of Router WAN

Gateway: the gateway of Router WAN

DNS1, DNS2, DNS3: DNS1/DNS2/DNS3 of Router WAN



Remaining Lease Time	0 days 23:38:43

Remaining Lease Time: remaining lease time of IP address in DHCP way

DHCP Release: release DHCP address

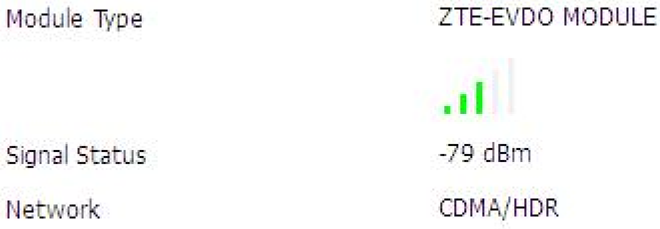
DHCP Renew: renew IP address in DHCP way, default is 1 day

Login Status	Disconnected

Login Status: connection status of WAN

Disconnection: disconnect

Connection: connect

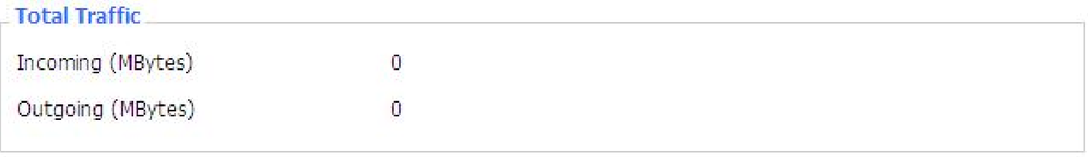


Module Type	ZTE-EVDO MODULE
Signal Status	-79 dBm
Network	CDMA/HDR

Module Type: module type in 3G/UMTS way

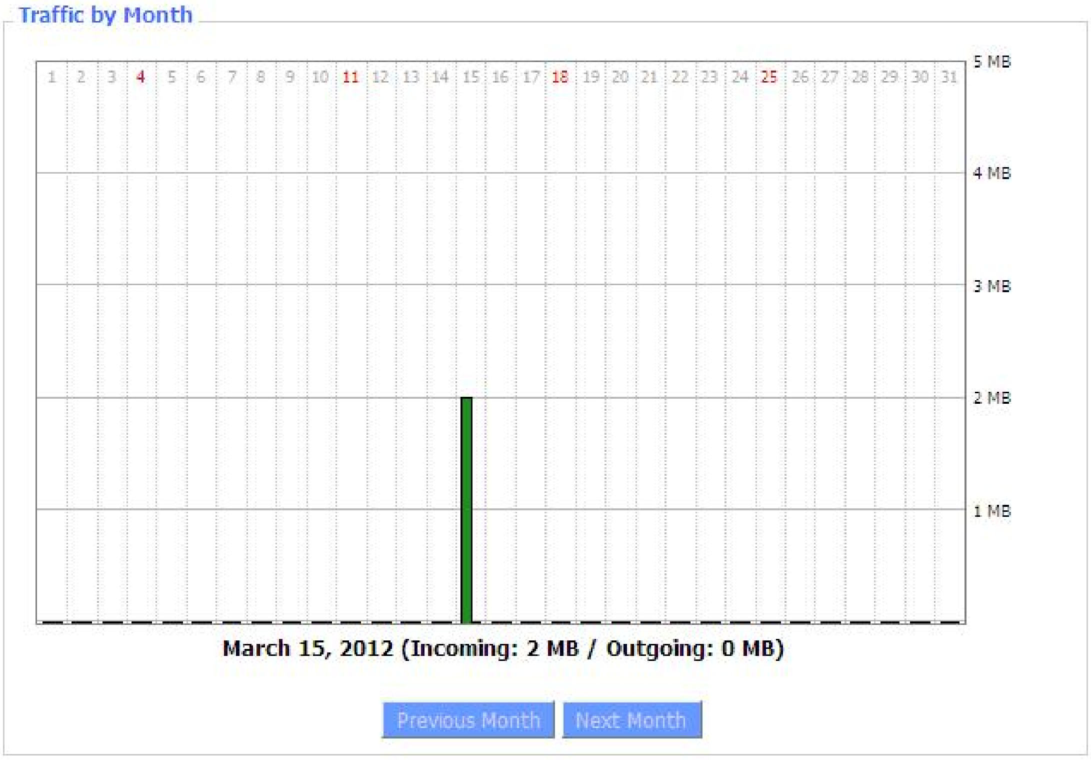
Signal Status: signal intensity of the module in 3G/UMTS way

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



Total Traffic

Incoming (MBytes)	0
Outgoing (MBytes)	0



Traffic by Month

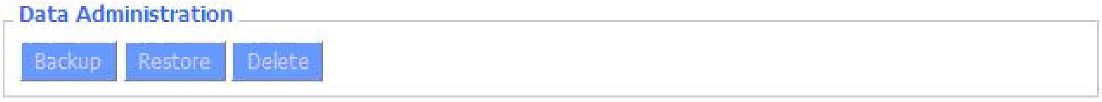
March 15, 2012 (Incoming: 2 MB / Outgoing: 0 MB)

Total Flow: flow from power-off last time until now statistics, download and upload direction

Monthly Flow: the flow of a month, unit is MB

Last Month: the flow of last month

Next Month: the flow of next month



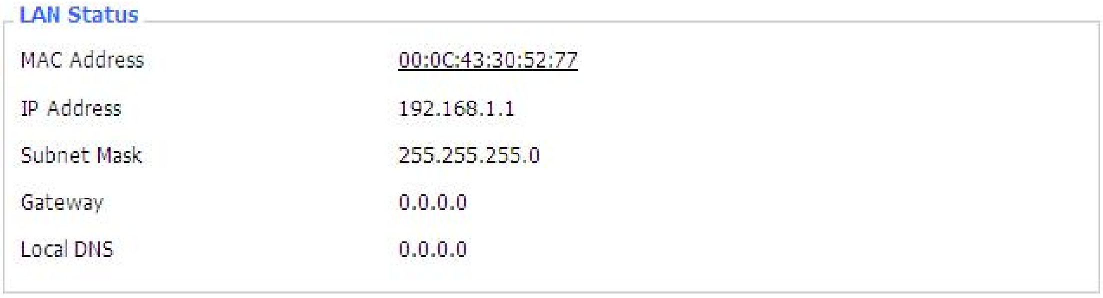
Data Administration

Backup: backup data administration

Restore: restore data administration

Delete: delete data administration

3.11.3 LAN



LAN Status

MAC Address	00:0C:43:30:52:77
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

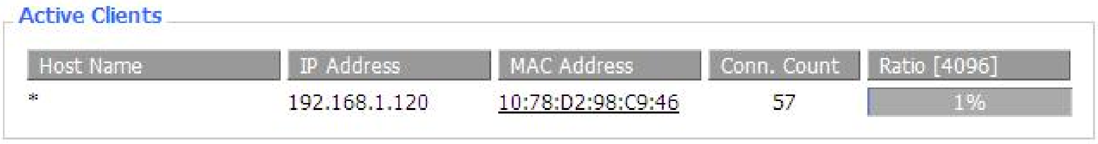
MAC Address: MAC Address of the LAN port ethernet

IP Address: IP Address of the LAN port

Subnet Mask: Subnet Mask of the LAN port

Gateway: Gateway of the LAN port

Local DNS: DNS of the LAN port



Active Clients

Host Name	IP Address	MAC Address	Conn. Count	Ratio [4096]
*	192.168.1.120	10:78:D2:98:C9:46	57	1%

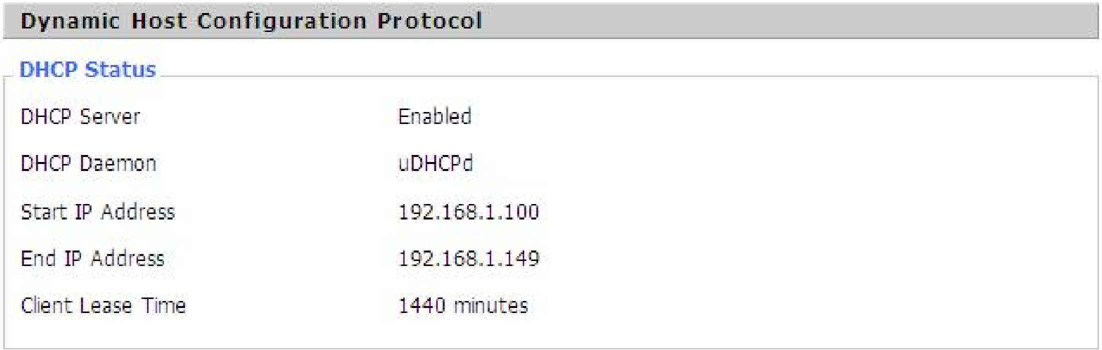
Host Name: host name of LAN client

IP Address: IP address of the client

MAC Address: MAC address of the client

Conn. Count: connection count caused by the client

Ratio: the ratio of 4096 connection



Dynamic Host Configuration Protocol

DHCP Status

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

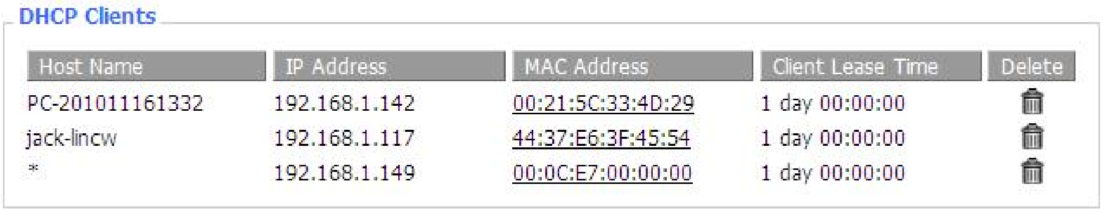
DNCP Server: enable or disable the Router work as a DHCP server

DHCP Daemon: the agreement allocated using DHCP including DNSMasq and uDHCPd

Starting IP Address: the starting IP Address of the DHCP server's Address pool

Ending IP Address: the ending IP Address of the DHCP server's Address pool

Client Lease Time: the lease time of DHCP client



DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time	Delete
PC-201011161332	192.168.1.142	00:21:5C:33:4D:29	1 day 00:00:00	🗑
jack-lincw	192.168.1.117	44:37:E6:3F:45:54	1 day 00:00:00	🗑
*	192.168.1.149	00:0C:E7:00:00:00	1 day 00:00:00	🗑

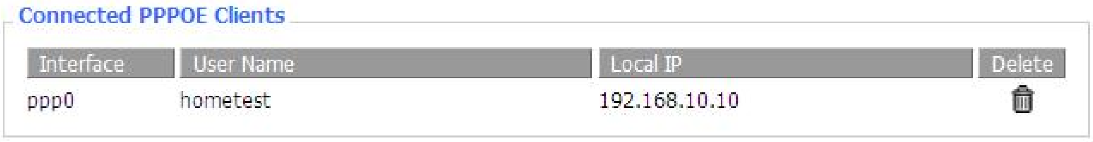
Host Name: host name of LAN client

IP Address: IP address of the client

MAC Address: MAC address of the client

Expires: the expiry the client rents the IP address

Delete: click to delete DHCP client



Connected PPPOE Clients

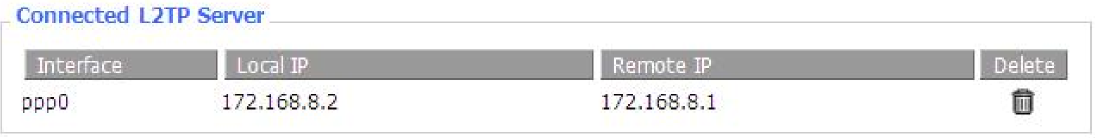
Interface	User Name	Local IP	Delete
ppp0	hometest	192.168.10.10	🗑

Interface: the interface assigned by dial-up system

User Name: user name of PPPoE client

Local IP: IP address assigned by PPPoE client

Delete: click to delete PPPoE client



Connected L2TP Server

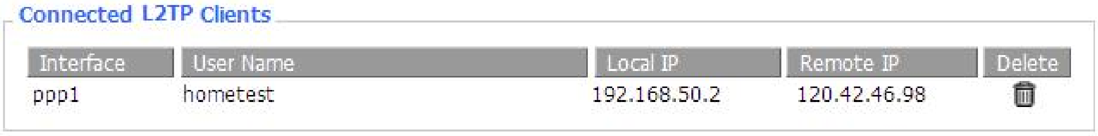
Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	🗑

Interface: the interface assigned by dial-up system

Local IP: tunnel IP address of local L2TP

Remote IP: tunnel IP address of L2TP server

Delete: click to disconnect L2TP



Connected L2TP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.50.2	120.42.46.98	🗑

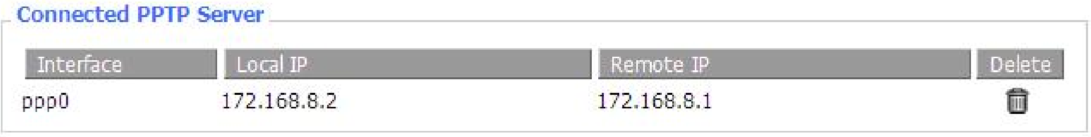
Interface: the interface assigned by dial-up system

User Name: user name of the client

Local IP: tunnel IP address of L2TP client

Remote IP: IP address of L2TP client

Delete: click to delete L2TP client



Connected PPTP Server

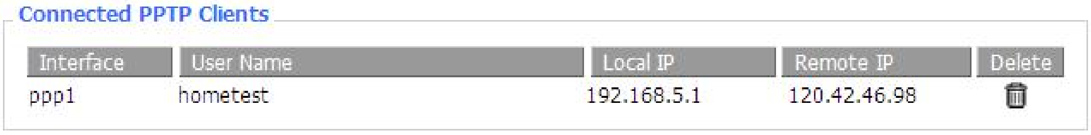
Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	🗑

Interface: the interface assigned by dial-up system

Local IP: tunnel IP address of local PPTP

Remote IP: tunnel IP address of PPTP server

Delete: click to disconnect PPTP



Connected PPTP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.5.1	120.42.46.98	🗑

Interface: the interface assigned by dial-up system

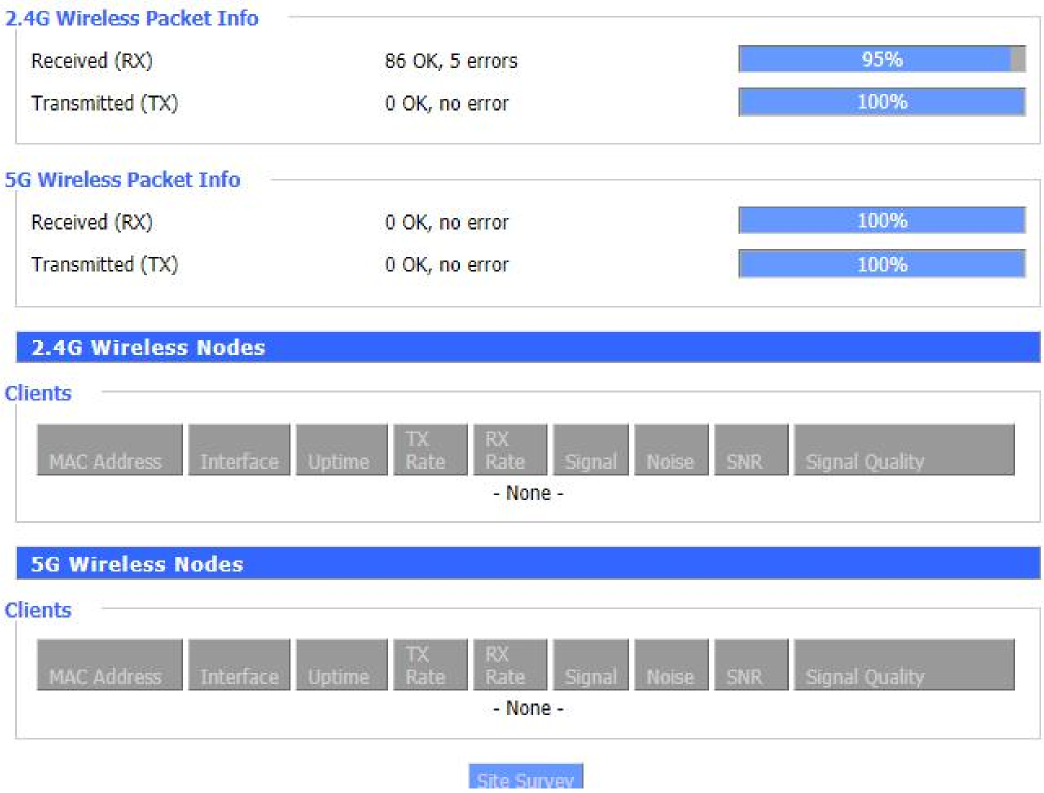
User Name: user name of the client

Local IP: tunnel IP address of PPTP client

Remote IP: IP address of PPTP client

Delete: click to delete PPTP client

3.11.4 Wireless



2.4G Wireless Packet Info

Received (RX)	86 OK, 5 errors	95%
Transmitted (TX)	0 OK, no error	100%

5G Wireless Packet Info

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

2.4G Wireless Nodes

Clients

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

- None -

5G Wireless Nodes

Clients

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

- None -

Received (RX): received data packet

Transmitted (TX): transmitted data packet

MAC Address: MAC address of wireless client

Interface: interface of wireless client

Uptime: connecting uptime of wireless client

TX Rate: transmit rate of wireless client

RX Rate: receive rate of wireless client

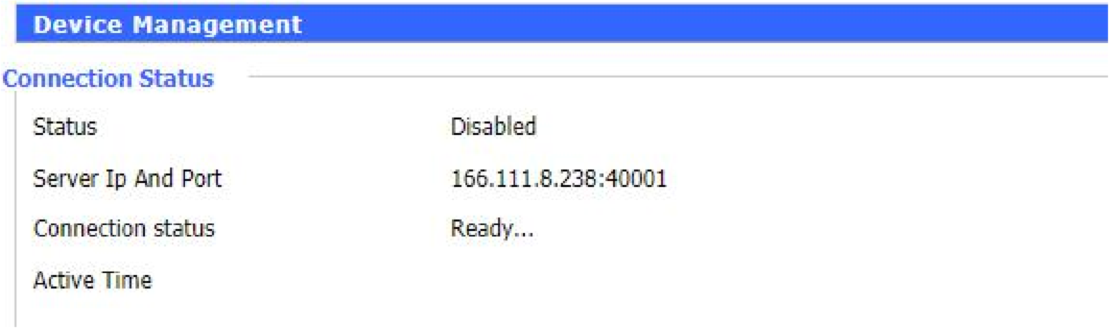
Signal: the signal of wireless client

Noise: the noise of wireless client

SNR: the signal to noise ratio of wireless client

Signal Quality: signal quality of wireless client

3.11.5 Device Management



Device Management

Connection Status

Status	Disabled
Server Ip And Port	166.111.8.238:40001
Connection status	Ready...
Active Time	

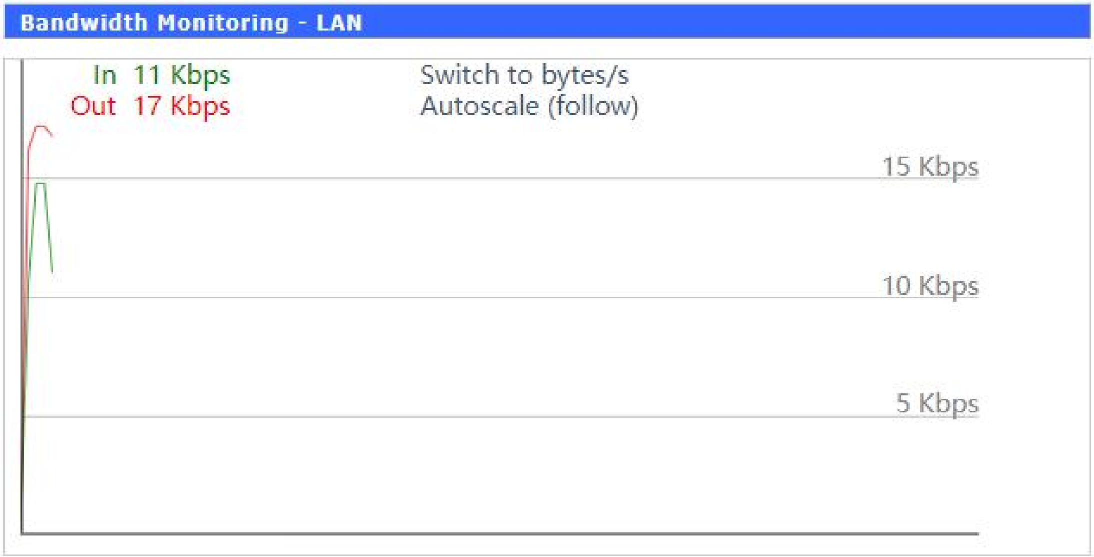
Status： Show device management status.

Server Ip And Port: Device management server IP and port.

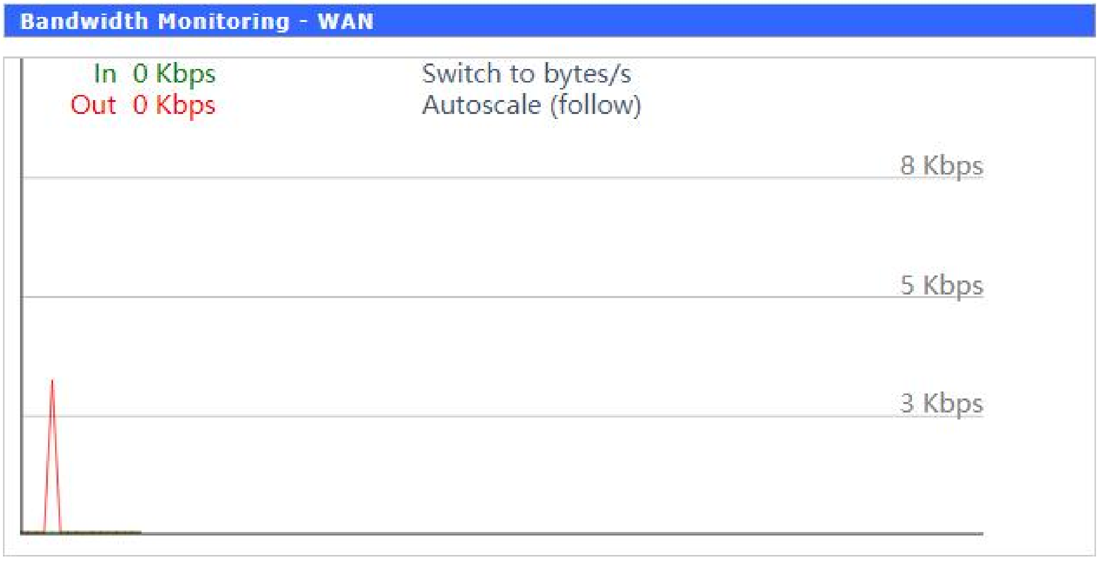
Connection Status: Device connection status to platform.

Active Time: connection time to management.

3.11.6 Bandwidth


Bandwidth Monitoring - LAN

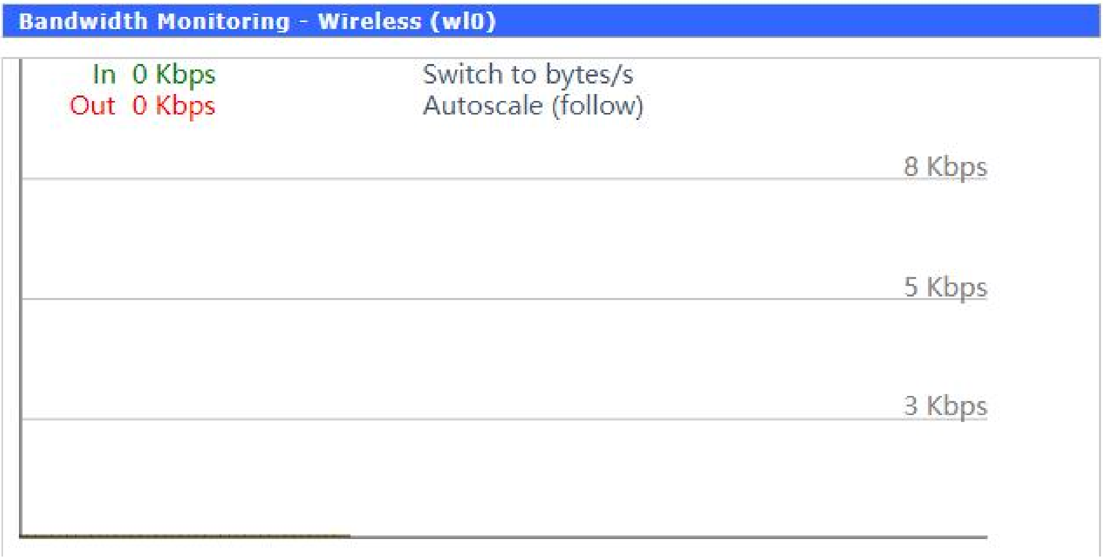
In 11 Kbps
Out 17 Kbps


Bandwidth Monitoring - WAN

In 0 Kbps
Out 0 Kbps

Bandwidth Monitoring-LAN Graph
abscissa axis: time
vertical axis: speed rate

Bandwidth Monitoring-WAN Graph
abscissa axis: time
vertical axis: speed rate

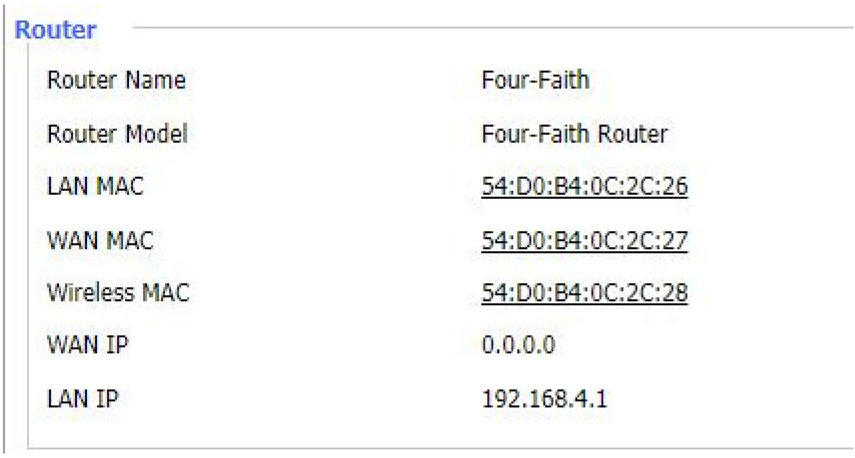


Bandwidth Monitoring-Wireless (W10) Graph

abscissa axis: time

vertical axis: speed rate

3.11.7 Sys-Info



Router

Router Name	Four-Faith
Router Model	Four-Faith Router
LAN MAC	54:D0:B4:0C:2C:26
WAN MAC	54:D0:B4:0C:2C:27
Wireless MAC	54:D0:B4:0C:2C:28
WAN IP	0.0.0.0
LAN IP	192.168.4.1

Router Name: the name of the Router

Router Model: the model of the Router

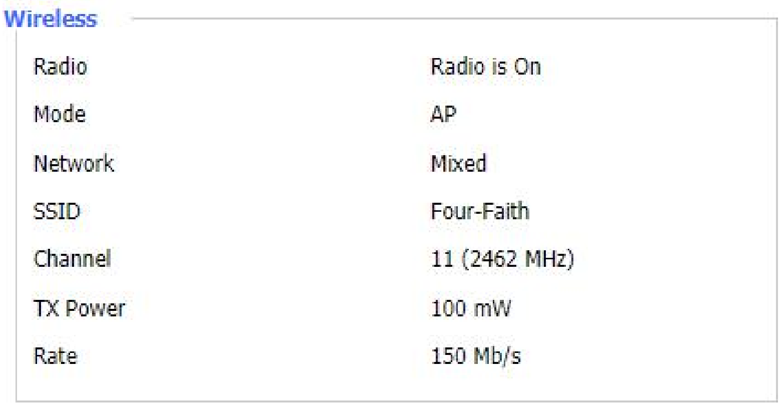
LAN MAC: MAC address of LAN port

WAN MAC: MAC address of WAN port

Wireless MAC: MAC address of the wireless

WAN IP: IP address of WAN port

LAN IP: IP address of LAN port



Wireless

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

Radio: display whether radio is on or not

Mode: wireless mode

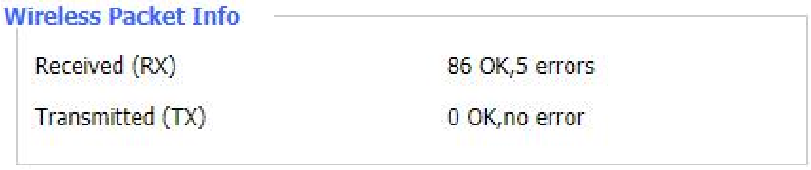
Network: wireless network mode

SSID: wireless network name

Channel: wireless network channel

TX Power: reflection power of wireless network

Rate: reflection rate of wireless network

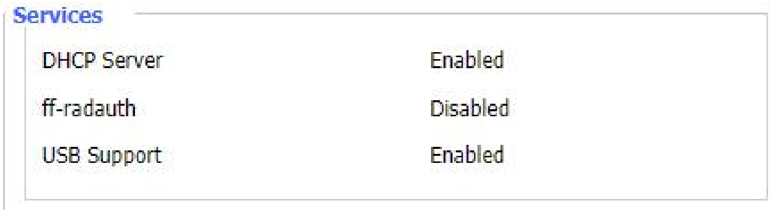


Wireless Packet Info

Received (RX)	86 OK,5 errors
Transmitted (TX)	0 OK,no error

Received (RX): received data packet

Transmitted (TX): transmitted data packet



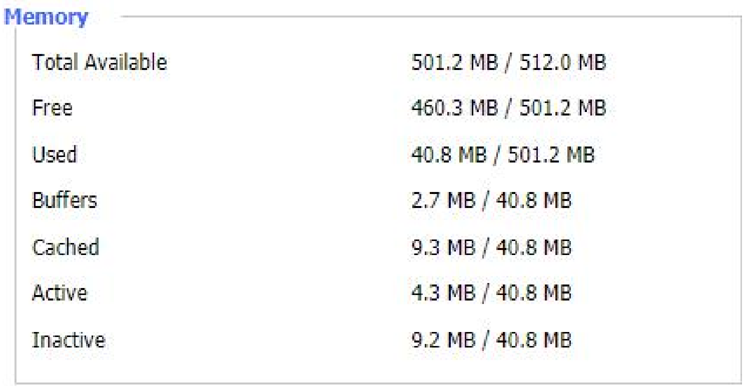
Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Enabled

DHCP Server: enabled or disabled

ff-radauth: enabled or disabled

USB Support: enabled or disabled



Memory

Total Available	501.2 MB / 512.0 MB
Free	460.3 MB / 501.2 MB
Used	40.8 MB / 501.2 MB
Buffers	2.7 MB / 40.8 MB
Cached	9.3 MB / 40.8 MB
Active	4.3 MB / 40.8 MB
Inactive	9.2 MB / 40.8 MB

Total Available: the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: free memory, the Router will reboot if the memory is less than 500kB

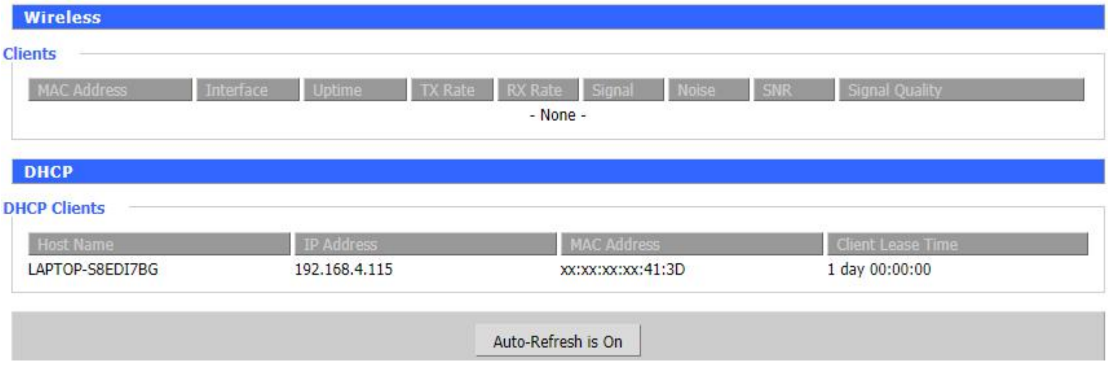
Used: used memory, total available memory minus free memory

Buffers: used memory for buffers, total available memory minus allocated memory

Cached: the memory used by high-speed cache memory

Active: Active use of buffer or cache memory page file size

Inactive: Not often used in a buffer or cache memory page file size



Wireless

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
				- None -				

DHCP

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time
LAPTOP-S8EDI7BG	192.168.4.115	xx:xx:xx:xx:41:3D	1 day 00:00:00

Wireless

MAC Address: MAC address of wireless client

Interface: interface of wireless client

Uptime: connecting uptime of wireless client

TX Rate: transmit rate of wireless client

RX Rate: receive rate of wireless client

Signal: the signal of wireless client

Noise: the noise of wireless client

SNR: the signal to noise ratio of wireless client

Signal Quality: signal quality of wireless client

DHCP

Host Name: host name of LAN client

IP Address: IP address of the client

MAC Address: MAC address of he client

Expires: the expiry the client rents the IP address