F3938 Router User Manual

Xiamen Four-faith Communication Technology Co., Ltd.

Addr: 3rd Floor, No.44, Guan Ri Road,
Software Park,Xiamen, China
Customer Hotline: 400-8838 -199
Tel: +86-592-5907276
Fax: +86-592-5912735
Web: en.four-faith.com

Files Revised Record

Date	Version	Remark	Author
2015-3-25	V1.00	Initial version	Jency
2016-1-19	V1.10	Modified	wusc

COPYRIGHT NOTICE

BRANDS NOTICE

Contents

Chapter 1 Brief Introduction of Product

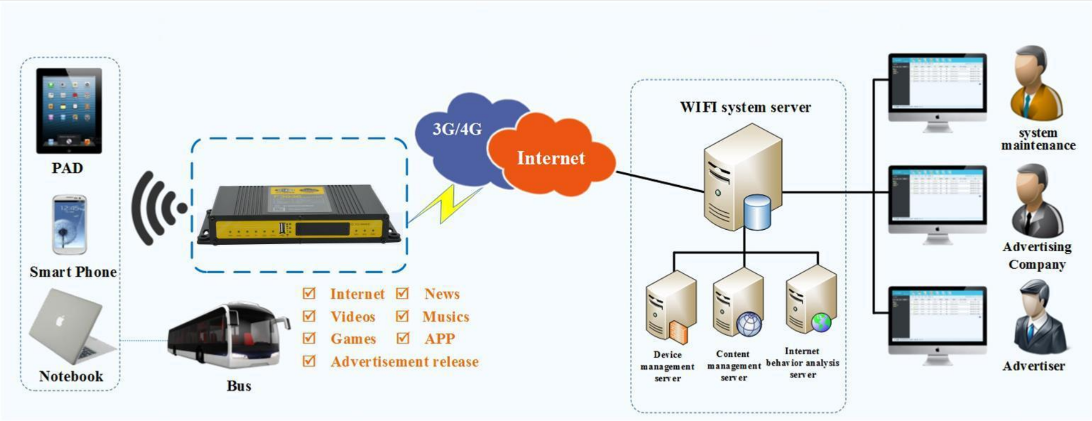
1.1 General

F3938 series is a set of wireless communicate serve to internet of things, take advantage of wireless public network to provide Wireless long-distance data transmission, multimedia information release and storage capabilities for users.

It integrates a industrial High-powered 32bits dual core CPU and industrial wireless modules, base on embedded RTOS software platform, and one RS232(or RS485/RS422), one Lan, one Wan, 2 WiFi interfaces. It can connect to serial port, Ethernet and WIFI devices at the same time, implement the transparent data transmission and routing functions.

F3938 has been already widely used in public transportation,tourism, finance and medical industries, such as urban public transport, customized bus, bus stations, tour bus, long-distance passenger bus, tourist attractions, bank, hospital and so on.

1.2 Application Topology



1.3 Features and Benefits

Design for Vehicle Application

- high-performance components
- Vehicle power supply design, support under-voltage, over-voltage, over-current, reverse connection, short circuit, surge protection
- Wide Power range: DC 9~36V
- Wide Operating Temperature(-35~+75ºC)
- Aviation plug for power input
- Metal shell, high heat radiating and anti collision performance
- Shockproof design, suitable for vehicle vibrating environment
- Security structure design for TF/SIM card
- Support backup power supply connection

Stability and Reliability

- Support double power supply systems(Vehicle power supply/UPS power supply for standby)
- System delay to power on during the vehicle starts, to avoid the surge impulse damage
- System delay to power off in case of outages, to protect storage equipment against damage
- Support hardware and software WDT to ensure the stability of the system
- Support auto recovery mechanism, including online detect, auto redial when offline to make router always online
- Data storage with SSD, ensure the data security and stability on high speed read and write
- Ethernet port: 1.5KV magnetic isolation protection
- RS232/RS485/RS422 port: 15KV ESD protection
- SIM/UIM port: 15KV ESD protection
- Antenna port: lightning protection(optional)

Standard and Convenience

- Support all kinds of the Intelligent WIFI terminals
- Smart data terminal, enter communication state automatically when

powered

- Provides standard wired network and wireless 3G/4G network
- Small size device, rapid establishment of wireless network
- Provide powerful business platform for equipment management, content management and release, report management, user behavior statistics analysis, authority management, alarm management, and other functions

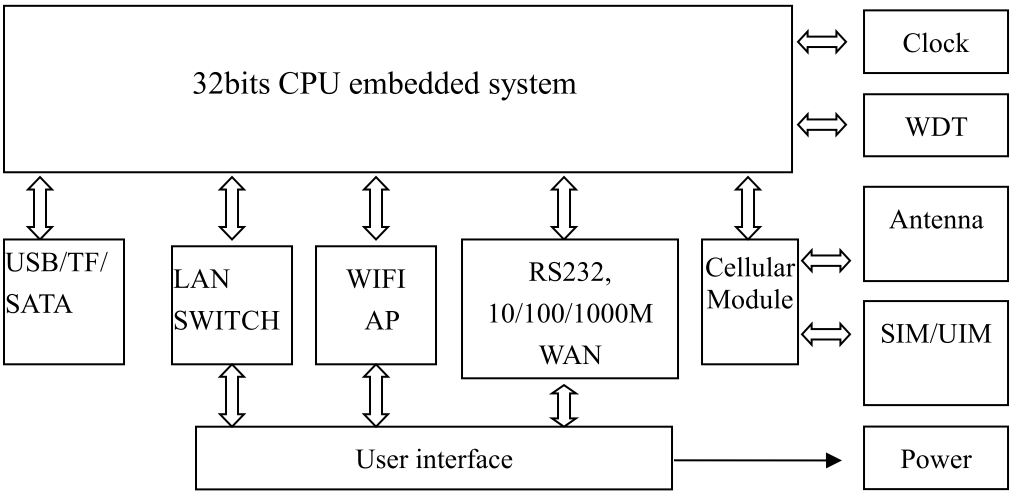
High-performance

- Support website redirection, local captive portal, remote captive portal
- Support various authentication ways, including mobile phone number authentication, WeChat authentication, Twitter authentication, Google authentication ,Facebook authentication and without authentication.
- Support 2.4G&5.8G dual-band WIFI
- Support USB3.0, downward compatibility with USB2.0
- Support WIFI channel hopping for anti-interference
- Support English SSID
- Support SSD(Solid State Disk) and TF card for local storage
- WIFI TX power is configurable for optimized wireless coverage
- Support WEB server. Supports PHP, XML, and database storage(optional)
- Support WIFI inspector
- Support black/white list of URL, account, IP address, MAC address
- Support traffic statistics. Support monitoring of device traffic, user traffic and online duration monitoring.
- Support user's surfing behavior record, local PV/UV statistics and transmit these data to server at real time for data statistics analysis.
- Support real time log auditing based on user's URL access
- Local information contains advertisement, news, APP, video, music, etc. Support various video formats and streaming media delivery
- Local information update support whole update and incremental update, support grouping update, support break-point resume and outage resume, support A/B backup, support update via 3G/4G, FTP, station WIFI(optional) and U disk upgrades
- Support remote firmware upgrade, including upgrade on single device, devices in patch and automatic upgrade(optional), support break-point resume, outage resume, U disk upgrades

- Support remote terminal parameters configuration, can be a single, batch configuration, custom configuration, at the same time support online/offline equipment configuration and U disk field configuration
- Support monitoring device status at real time, including CPU, memory, signal strength, network status, storage and alarm
- Supports completed functionality of router
- Support SPI firewall, access restriction, URL filter, QoS, NAT, etc
- Support NTP, schedule reboot and schedule boot/shutdown with in built RTC
- Support various WAN connection types, including static IP, DHCP, PPPoE, 3G / 4G, etc
- Support 3G/4G network and Ethernet WAN for backup(optional)
- Support VPN client and VPN server(PPTP, L2TP, OPENVPN, IPSEC and GRE(only VPN version supports)
- Support the GPS/beidou positioning function (optional)

1.4 Working Principle

The principle chart of the router is as following:



1.5 Product Specifications

Cellular Specification

Item	Content

Cellular Module	High-performance industrial cellular module (optional single module, double module or no module)
Standard	Can support: TDD-LTE/FDD-LTE/EVDO/WCDMA/TD-SCDMA/CDMA1X/GPRS/EDGE Optional support:single-mode,multi-mode or All network communication
Bandwidth	FDD LTE(DL:100Mbps,UL:50Mbps) TDD LTE(DL:68Mbps,UL:17Mbps) CDMA2000 1X EVDO Rev A (DL:3.1Mbps,UL:1.8Mbps) WCDMA(DL:42Mbps,UL:5.76Mbps) TD-SCDMA(DL:4.2Mbps,UL:2.2Mbps)
TX power	<24dBm
RX sensitivity	<-109dBm

GPS Specification

Item	Content
GPS Module	Industrial GPS module(optional beidou module)
Receiver Type	50-channle GPS L1（1575.42MHz）C/A code SBAS: WAAS,EGNOS,MSAS,GAGAN
Max. update rate	5 Hz
Accuracy	Position: 2.5m CPE SBAS: 2.0m CPE
Sensitivity	Tracking: -160dBm Reacquisition: -160dBm Cold starts: -146dBm

WIFI Specification

Item	Content
Standard	IEEE802.11b/g/n, 2.4G, 2*2 MIMO,AP model, Station model(optional) IEEE802.11ac，5.8G, 2*2 MIMO,AP model,Station model（optional）
Bandwidth	IEEE802.11b/g: 108Mbps (max) IEEE802.11n: 300Mbps (max) IEEE802.11ac：780Mbps(max)
Security	WEP, WPA, WPA2, etc.

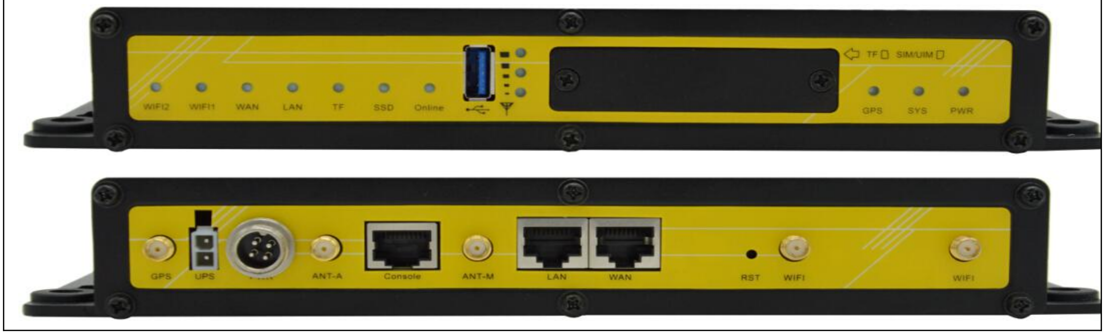
TX power	26dBm（11b），21.5dBm（11g），20dBm（11n），16dBm（11ac）
RX sensitivity	<-72dBm@54Mpbs

Hardware System

Item	Content
CPU	High-performance industrial 32bits CPU
FLASH	32MB(Extendable to 64MB)
SDRAM	512MB
SSD	128GB(optional,Extendable to 2TB)(optional)
TF	8GB/32GB (optional)

Interface Type

Item	Content
WAN	1 10/100/1000 Mbps WAN port(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
LAN	1 10/100/1000 Mbps Ethernet ports(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
Serial	1 RS232(or RS485/RS422) port, 15KV ESD protection Data bits: 5, 6 ,7, 8 Stop bits: 1, 1.5(optional), 2 Parity: none, even, odd, space(optional), mark(optional) Baud rate: 2400~115200 bps
Indicator	“PWR”、“SYS”、“SIM”、 “GPS”、“Online”、“SSD”、“TF”、“LAN”、“WAN”、“WIFI”, "Signal Strength"(Indicator according to the configuration)
Antenna	Cellular: Standard SMA female interface, 50 ohm, lighting protection(optional one, two or not) GPS:One standard SMA female interface, 50 ohm, lighting protection(optional) WIFI: Two standard SMA male interface, 50 ohm, lighting protection
SIM/UIM	Standard 3V/1.8V user card interface, 15KV ESD protection
USB	Standard USB3.0,support various of storage
TF	Standard TF card interface,support various of TF cards
Power	GX12-4 Aviation plug or 5569-4vehicle power jack, reverse-voltage and overvoltage protection
UPS	Used to connect back power supply
Reset	Press this button for 15 seconds，restore the router to its

	original factory default settings
	

Power Supply

Item	Content	
Standard Power	DC 12V/1.5A	
Power range	DC 9~36V	
Working current	3G：<850mA (12V)	4G：<950mA (12V)
Standby current	3G：<550mA (12V)	4G：<600mA (12V)

Physical Characteristics

Item	Content
Housing	Metal shell, shock proof design
Dimensions	244x139x36 mm(without antenna or installation components)
Weight	950g

Other Specification

Item	Content
Operating Temperature	-35~+75ºC（-31~+167℉）
Storage Temperature	-40~+85ºC (-40~+185℉)
Operating Humidity	95%（unfreezing)

Chapter 2 Installation Introduction

2.1 General

F3938 series ROUTER must be installed correctly to make it work properly. Currently, the installation must be in the guidance of qualified person who is confirmed by our company.

- **Warning:**
  - Forbid to install the router when powered!

2.2 Encasement List

Please keep the encasement for transportation in the future. Encasement list is below:

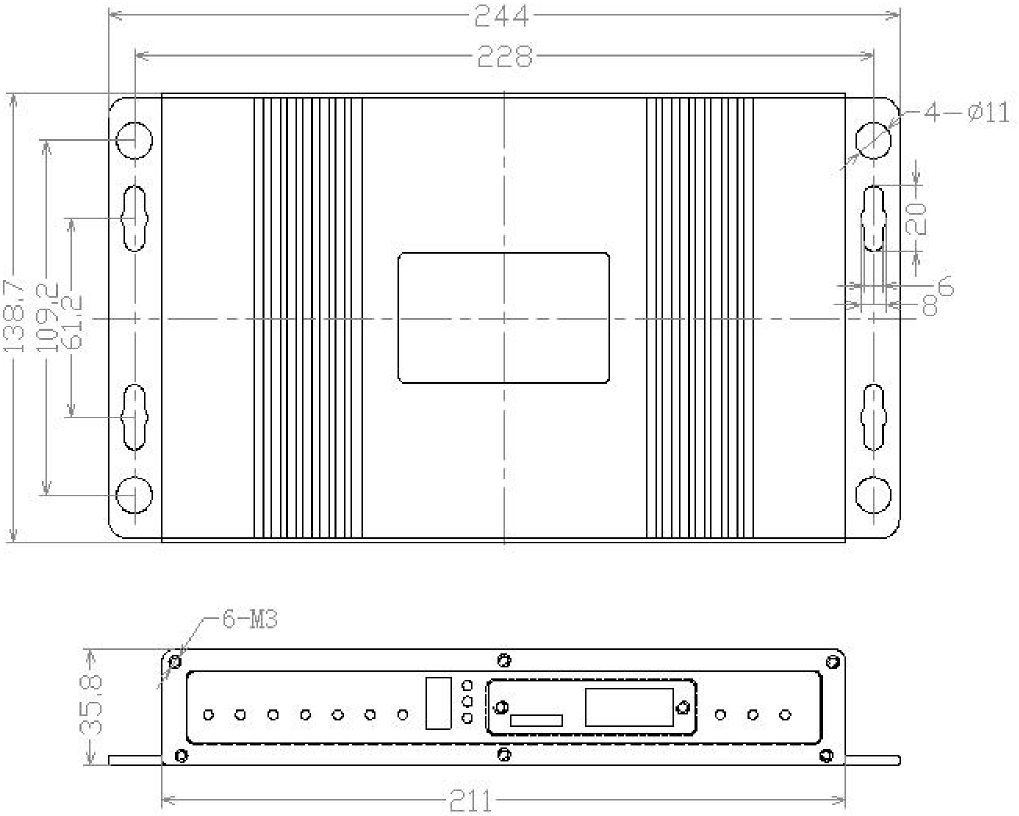
Name	Quantity	Remark
F3938 Router host	1	
Cellular antenna (Male SMA)	1(Note 1)	
GPS antenna (Male SMA)	1	optional
WIFI antenna (Female SMA)	2	
Aviation plug power cord	1	
Vehicle interface cable	1	
Manual CD	1	
UPS interface cable	1	optional
Network cable	1	
RS232 Console cable	1	optional
Power adapter	1	optional
Certification card	1	
Maintenance card	1	

Note1:Cellular antenna (Male SMA) 1 pcs for 3G comfiguration and 2 pcs for 4G comfiguration.

2.3 Installation and Cable Connection

Overall dimensions:

The dimensions below. (unit: mm)



Installation of antenna:

Screw the SMA male pin of the cellular antenna to the female SMA interface of the router with sign "ANT-M","ANT-A"or "ANT".

Screw the SMA male pin of the GPS antenna to the female SMA interface of the router with sign "GPS".

Screw the SMA female pin of the WIFI antenna to the male SMA interface of the router with sign "WIFI".

Warning: The cellular antenna, The GPS antenna and the WIFI antenna can not be connected wrongly. And the antennas must be screwed tightly, or the signal quality of antenna will be influenced!

Installation of SIM/UIM card:

Firstly power off the router, and press the out button of the SIM/UIM card outlet with a needle object. Then the SIM/UIM card sheath will flick out at once. Put SIM/UIM card into the card sheath (Pay attention to put the side which has metal point outside), and insert card sheath back to the SIM/UIM card outlet.

Warning: Forbid to install SIM/UIM card when powered!

Installation of cable:

Insert one end of the network cable into the switch interface with sign "Local Network", and insert the other end into the Ethernet interface of user's device. The signal connection of network direct cable is as follows:

RJ45-1	RJ45-2
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

Insert the RJ45 end of the console cable into the RJ45 outlet with sign "console", and insert the DB9F end of the console cable into the RS232 serial interface of user's device.

The signal connection of the console cable is as follows:

RJ45	DB9F
1	8
2	6
3	2
4	1
5	5
6	3
7	4
8	7

The signal definition of the DB9F serial communication interface is as follows:

Pin	RS232 signal name	The direction for Router
1	DCD	output
2	RXD	output
3	TXD	input
4	DTR	input
5	GND	
6	DSR	output
7	RTS	input
8	CTS	output

2.4 Power

Usually, F3938 is applied in the complex environment。In order to improve the stability and adapt to different applications, the advanced power technology is designed. The system should be supply with DC 12V/1.5A by power adapter or the power range DC 9~36V. If users use other power supply, the stability must be satisfied(the ripple is less than 300mV, the Instantaneous voltage less than 36V),and make sure that the power is more than 12W.
We recommend user to use the standard DC 12V/1.5A power.

2.5 Indicator Lights Introduction

The router provides following indicator lights: “PWR”, “SYS”, “SIM”, “GPS”, “Online”, “SSD”, “TF”, “LAN”, “WAN”, “WIFI”, “Signal Strength”.

Indicator Light	State	Introduction
PWR	ON	Router is powered on
	OFF	Router is powered off or in the shutdown period of schedule boot & shutdown
SYS	BLINK	System works properly
	OFF	System does not work
SIM	ON	Router identification to SIM card
	OFF	Router has not identification to SIM card
GPS	ON/ BLINK	GPS interface connected/is searching satellites
	OFF	GPS interface does not connected
Online	ON	Router has logged on network
	OFF	Router hasn’t logged on network

SSD	ON/ BLINK	Router identification to hard disk/ Router reading or writing hard disk data
	OFF	Router has not identified to hard disk
TF	ON/ BLINK	Router identification to TF card/ Router reading or writing TF card
	OFF	Router has not identification to TF card
LAN	ON / BLINK	The corresponding interface of switch is connected /communicating
	OFF	The corresponding interface of switch is not connected
WAN	ON/ BLINK	The interface of WAN is connected /communicating
	OFF	The interface of WAN is not connected
WIFI	ON	WIFI is active
	OFF	WIFI is not active
Signal Strength	One Light ON	Signal strength is weak
	Two Lights ON	Signal strength is medium
	Three Lights ON	Signal strength is good

2.6 Reset Button Introduction

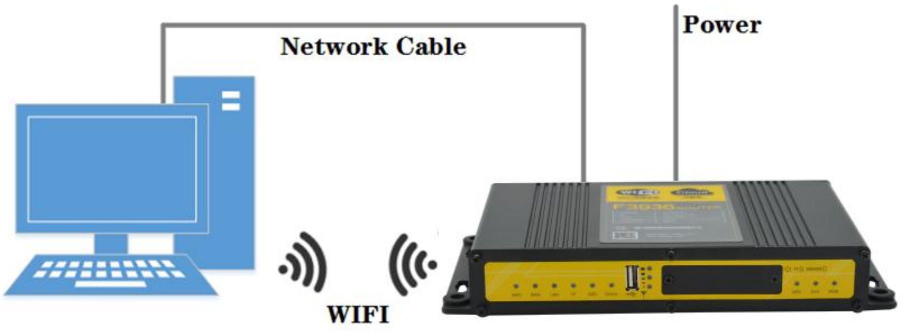
The router has a “Reset” button to restore it to original factory default settings. When user press the “Reset” button for up to 15s until SYS light blinking fast, the router will restore to original factory default settings and restart automatically.

Chapter 3 Configuration and Management

This chapter describes that how to configure and manage the router.

3.1 Configuration Connection

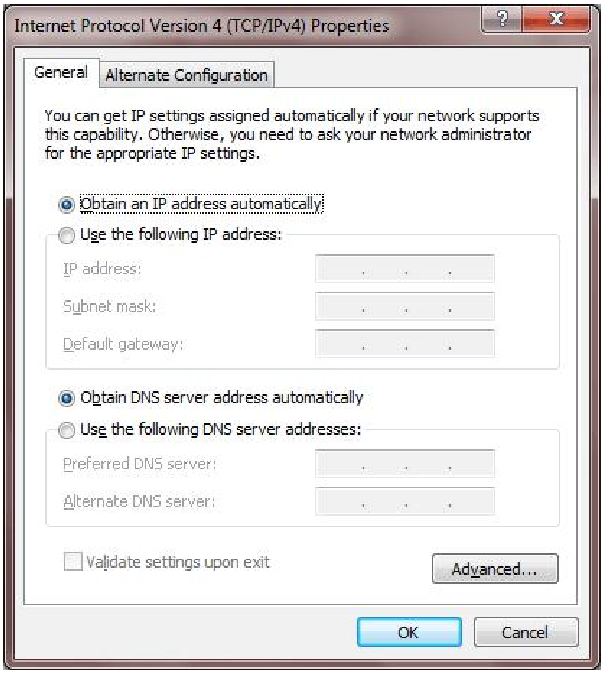
Before configuration, you should connect the router to the PC by the provided Ethernet cable or WIFI to configure the router. Connect one side of the Ethernet cable to the router LAN port, and the other side to PC ETH port. If you connect by WIFI, connect to SSID “FOUR-FAITH_XXXX”(XXXX stands for the last four letters of the default Wireless MAC address in the router) without password.



3.2 Login the Router Web GUI

3.2.1 Configure the PC IP address(There are two ways)

(1) Obtain an IP address automatically



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

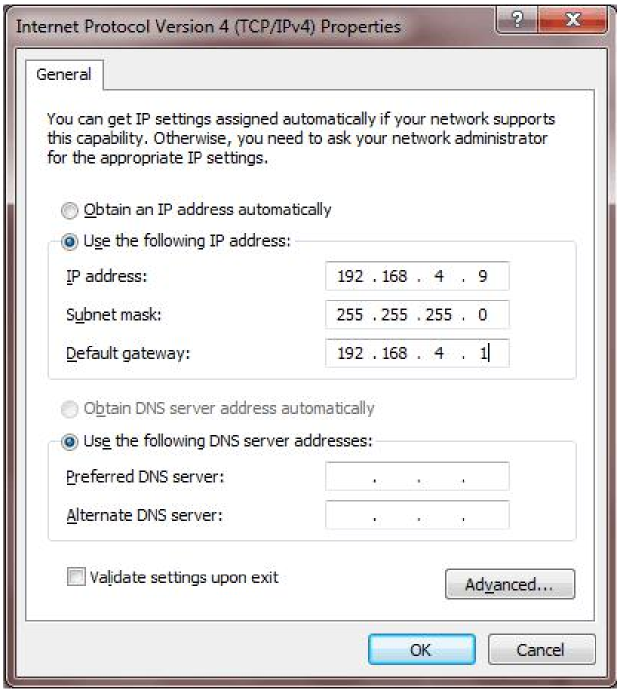
● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

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

□ Validate settings upon exit

(2) Use a given IP address

Configure the PC IP address as 192.168.4.9 (or other IP address in the same subnet), subnet mask as 255.255.255.0 and default gateway as 192.168.4.1. Configure the DNS server as the local DNS server.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 4 . 9
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 4 . 1

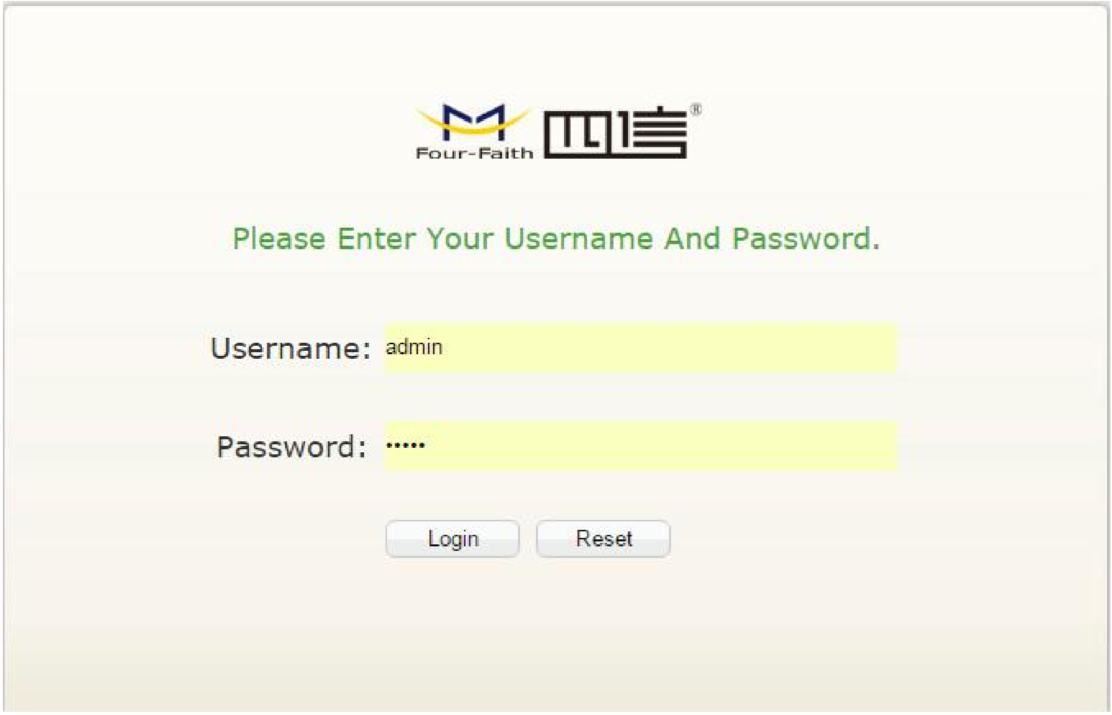
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

3.2.2 Login the router Web GUI

The main functions of each menu are described in this chapter. You can access the router Web GUI through the web browser on the PC. Main menus are as below: Status, Network, Firewall, VPN Setting, Advanced Setting and Management. Click the main menu and you will see the sub menu.

Start IE explorer or other web browser, input the router default IP address 192.168.4.1:90 and press the enter button to access router login Web GUI. You will get the following prompt box to remind you to enter the router default login username and password when you access the Web GUI for the first time.

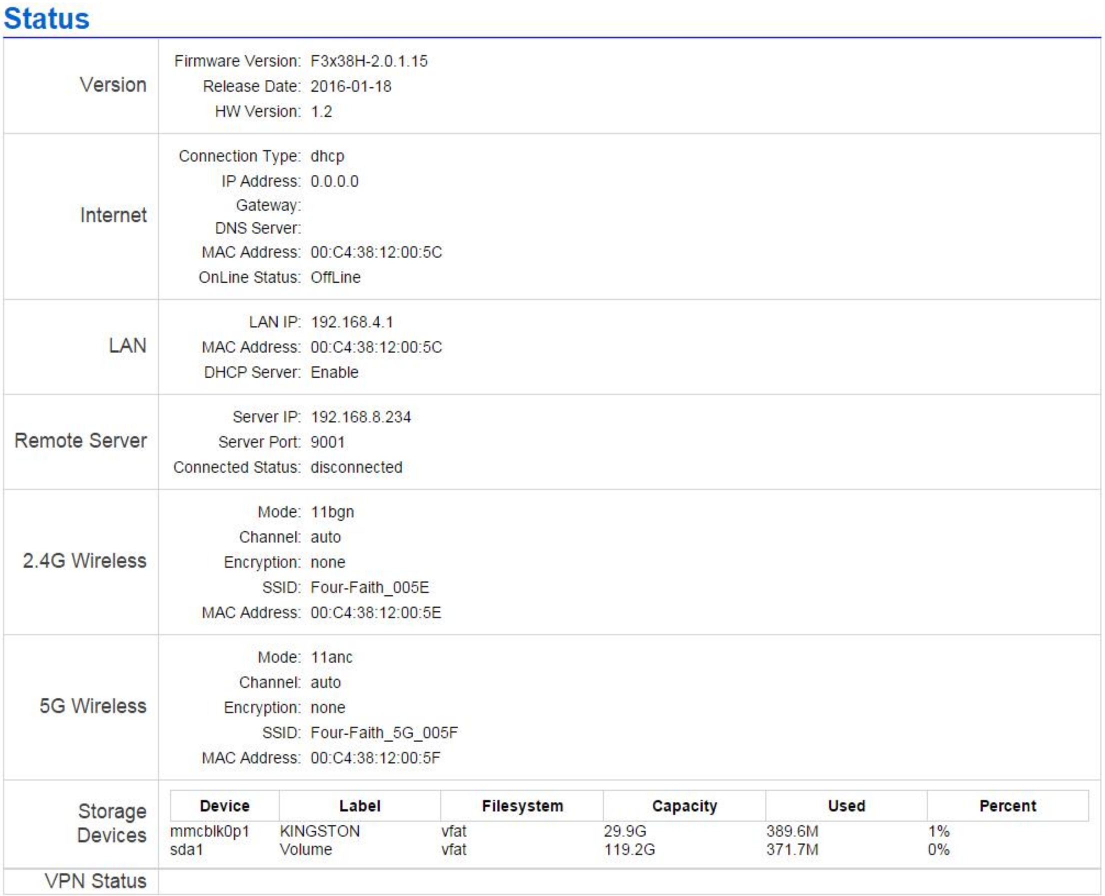


Please Enter Your Username And Password.

Username: admin

Password: •••••

Then you will enter the Status page.



Status

Version	Firmware Version: F3x38H-2.0.1.15 Release Date: 2016-01-18 HW Version: 1.2
Internet	Connection Type: dhcp IP Address: 0.0.0.0 Gateway: DNS Server: MAC Address: 00:C4:38:12:00:5C OnLine Status: OffLine
LAN	LAN IP: 192.168.4.1 MAC Address: 00:C4:38:12:00:5C DHCP Server: Enable
Remote Server	Server IP: 192.168.8.234 Server Port: 9001 Connected Status: disconnected
2.4G Wireless	Mode: 11bgn Channel: auto Encryption: none SSID: Four-Faith_005E MAC Address: 00:C4:38:12:00:5E
5G Wireless	Mode: 11anc Channel: auto Encryption: none SSID: Four-Faith_5G_005F MAC Address: 00:C4:38:12:00:5F
Storage Devices	
VPN Status	

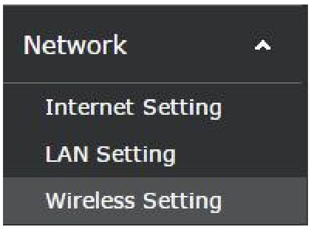
Storage Devices

Device	Label	Filesystem	Capacity	Used	Percent
mmcblk0p1	KINGSTON	vfat	29.9G	389.6M	1%
sda1	Volume	vfat	119.2G	371.7M	0%

3.3 Management and Configuration

3.3.1 Network

The first sub menu in “Network” menu is “Internet Setting”. And you can change the Internet setting according to the instructions. Click “Save & Apply” button and the changes will take effect. Click “Save” button to save the settings but the changes don’t take effect. Click “Reset” button to cancel changes.



3.3.1.1 Internet Setting

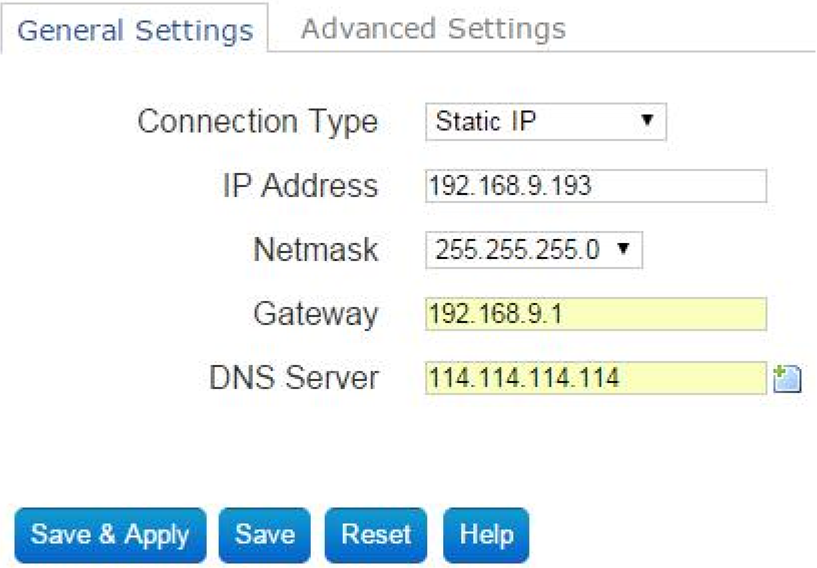
Configure “WAN Connection type” to make the router connect to the Internet. And you can get the parameters from the ISP.

WAN Connection Type:

Select the corresponding Internet connection type the ISP provides. WAN connection type includes Static IP, DHCP, PPPoE, 3G connection and LTE connection.

Mode One: Static IP

Use this mode if you subscribe optical network or other wired network and configure the IP address, netmask, gateway, DNS server provided by the ISP.



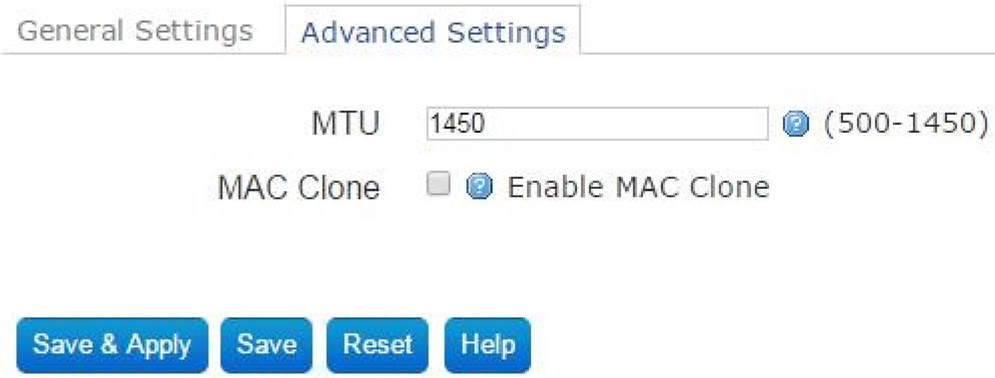
Connection Type: Static IP
IP Address: 192.168.9.193
Netmask: 255.255.255.0
Gateway: 192.168.9.1
DNS Server: 114.114.114.114

IP Address: IP address assigned by the ISP or one you set by your own

Netmask: Netmask assigned by the ISP or one you set by your own

Gateway: Gateway assigned by the ISP or one you set by your own

DNS Server: IP address assigned by the ISP or one you set by your own. Click “+” button to add more.



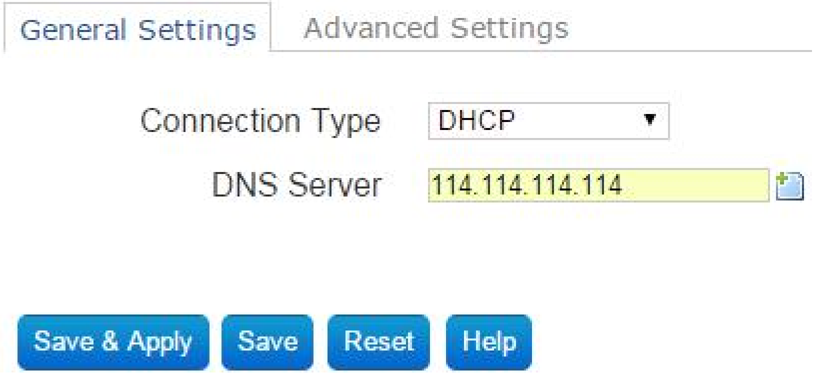
MTU: 1450 (500-1450)
MAC Clone: □ Enable MAC Clone

MTU: Set the appropriate MTU value to make full use of internet throughout.

MAC Clone: The selection enable MAC Clone.

Mode Two: DHCP

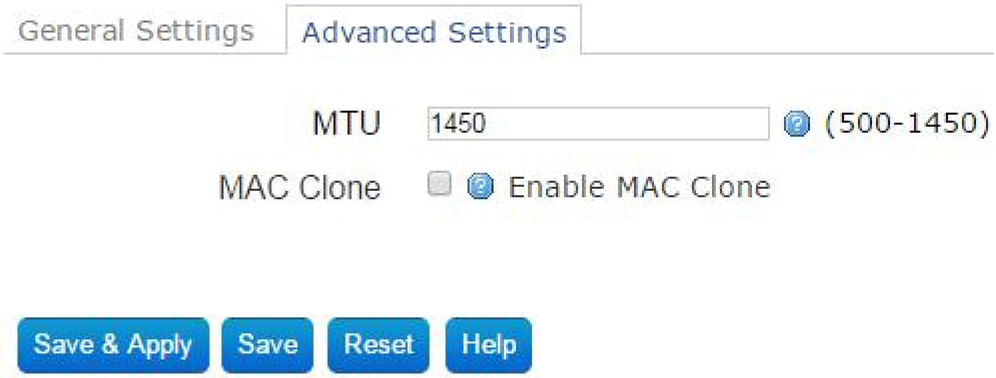
DHCP is the default WAN connection type.



Connection Type: DHCP

DNS Server: 114.114.114.114

Router obtains the WAN IP address by DHCP and you can set the static DNS server.



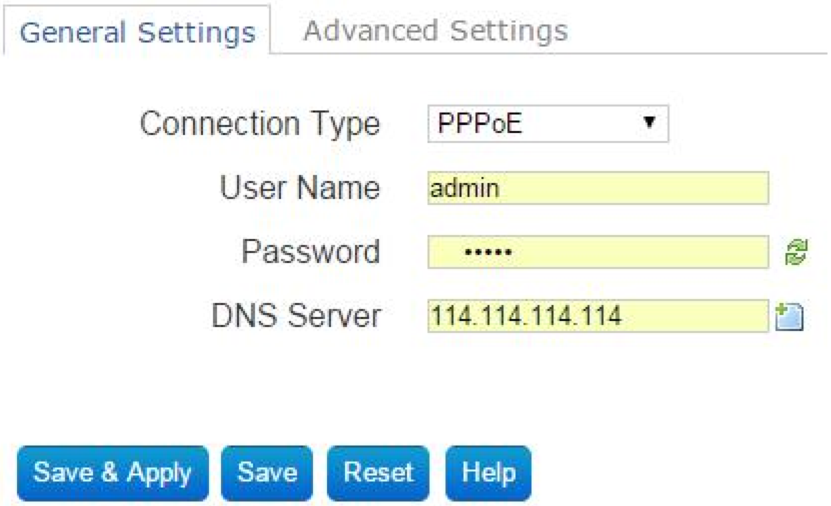
MTU: 1450 (500-1450)

MAC Clone: □ Enable MAC Clone

The advanced setting of this mode is the same with static IP mode

Mode Three: PPPOE

Use this mode if you subscribe ADSL broadband service. Configure username and password provided by the ISP.

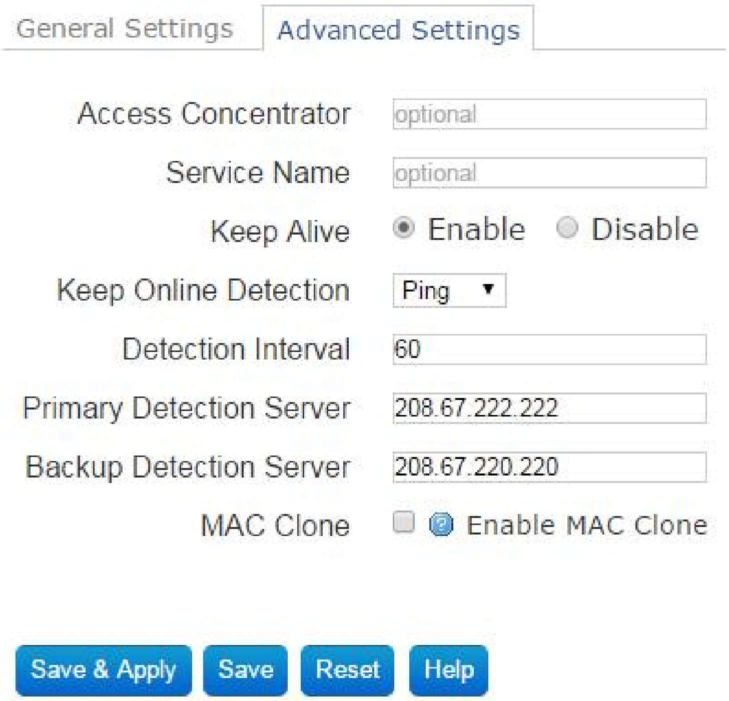


Connection Type: PPPoE

User Name: admin

Password: •••••

DNS Server: 114.114.114.114



Access Concentrator: optional

Service Name: optional

Keep Alive: ● Enable ○ Disable

Keep Online Detection: Ping

Detection Interval: 60

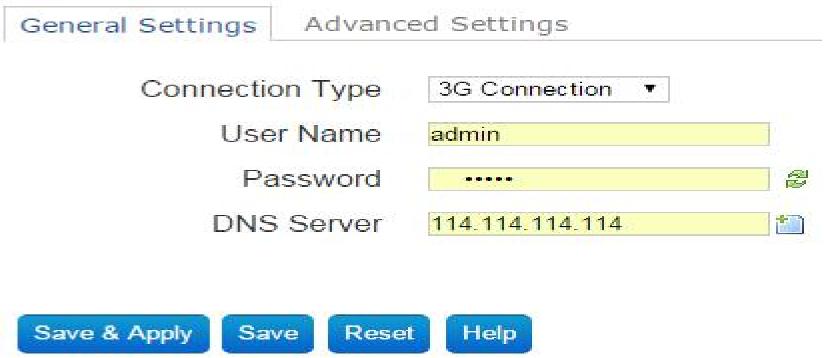
Primary Detection Server: 208.67.222.222

Backup Detection Server: 208.67.220.220

MAC Clone: □ Enable MAC Clone

Access Concentrator and **Server Name**, are optional. The other options will be explained below.

Mode Four: 3G Connection

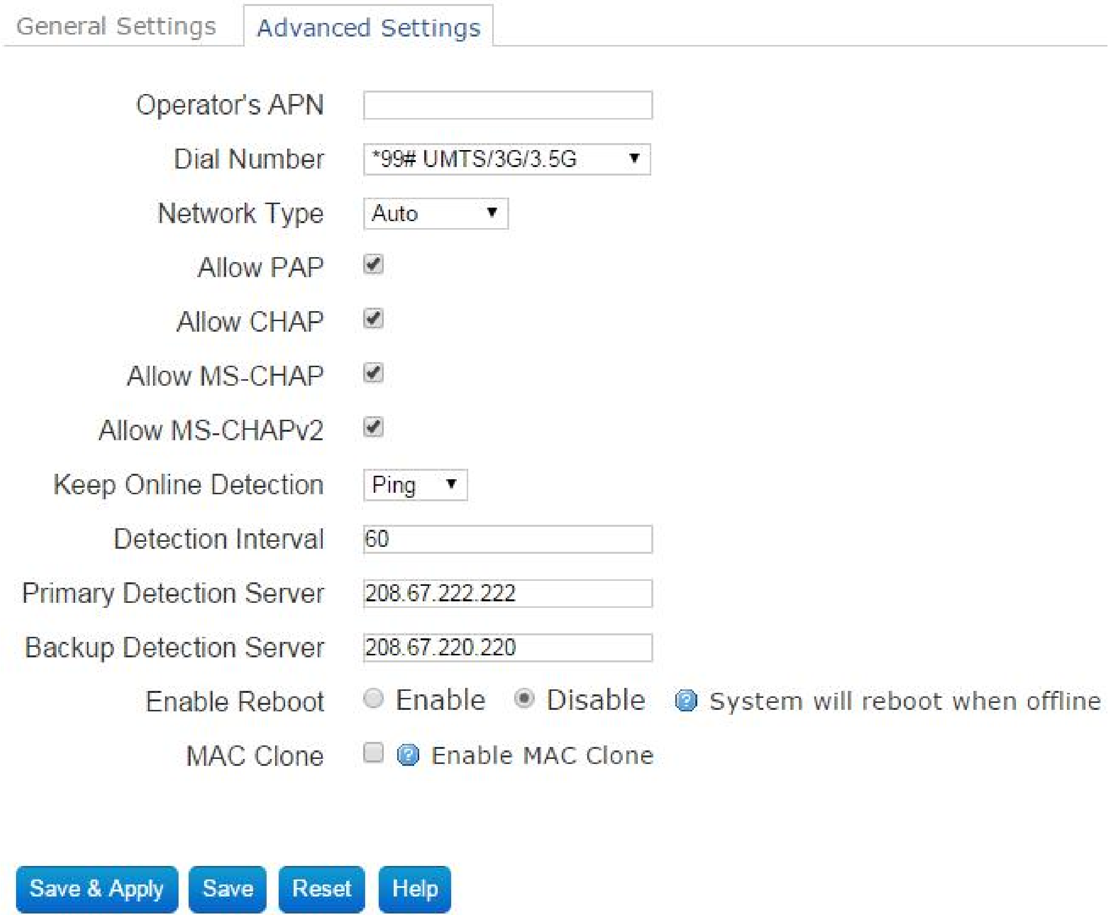


Connection Type: 3G Connection ▼

User Name: admin

Password: •••••

DNS Server: 114.114.114.114



Operator's APN:

Dial Number: *99# UMTS/3G/3.5G ▼

Network Type: Auto ▼

Allow PAP ☑

Allow CHAP ☑

Allow MS-CHAP ☑

Allow MS-CHAPv2 ☑

Keep Online Detection: Ping ▼

Detection Interval: 60

Primary Detection Server: 208.67.222.222

Backup Detection Server: 208.67.220.220

Enable Reboot ○ Enable ● Disable System will reboot when offline

MAC Clone □ Enable MAC Clone

User Name: login the Internet

Password: login the Internet

Dial Number: dial number of users' ISP

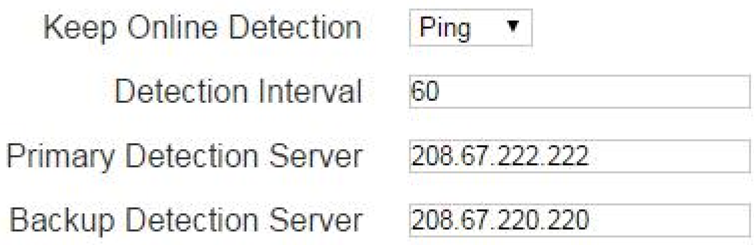
Operator's APN: access point name of users' ISP

Network Type:

Network Type: Auto ▼

Network type includes Auto, Force 3G, Force 2G, Prefer 3G, Prefer 2G, 3G/2G, Force 4G and 4G/3G/2G.

Keep Online Detection



Keep Online Detection: Ping
Detection Interval: 60
Primary Detection Server: 208.67.222.222
Backup Detection Server: 208.67.220.220

This function is used to detect whether the Internet connection is active. if users set it, router will detect the Internet connection automatically. The router will redial immediately to make the obtain active connection When it detects the connection is inactive.

Keep Online Connection Type:

None: No online detection

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

Route: Detect connection with route method. When choosing this method, you should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

PPP: Detect connection with PPP method. When choosing this method. You should also configure "Detection Interval" item.

Detection Interval:

Time interval between two detection , and unit is second.

Primary Detection Server:

The server used to response to the router’s detection packet. This item is only valid for method "Ping" and "Route".

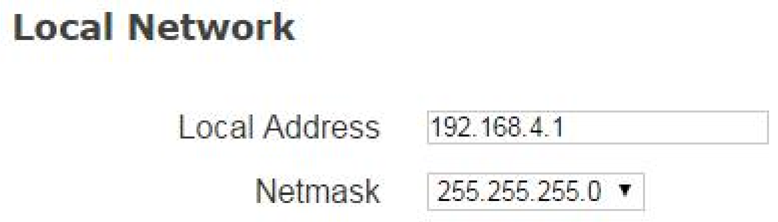
Backup Detection Server:

The backup server used to response to the router’s detection packet. This item is only valid for method "Ping" and "Route".

3.3.1.2 LAN Setting

Local Network

Configure the local area network setting



Local Network

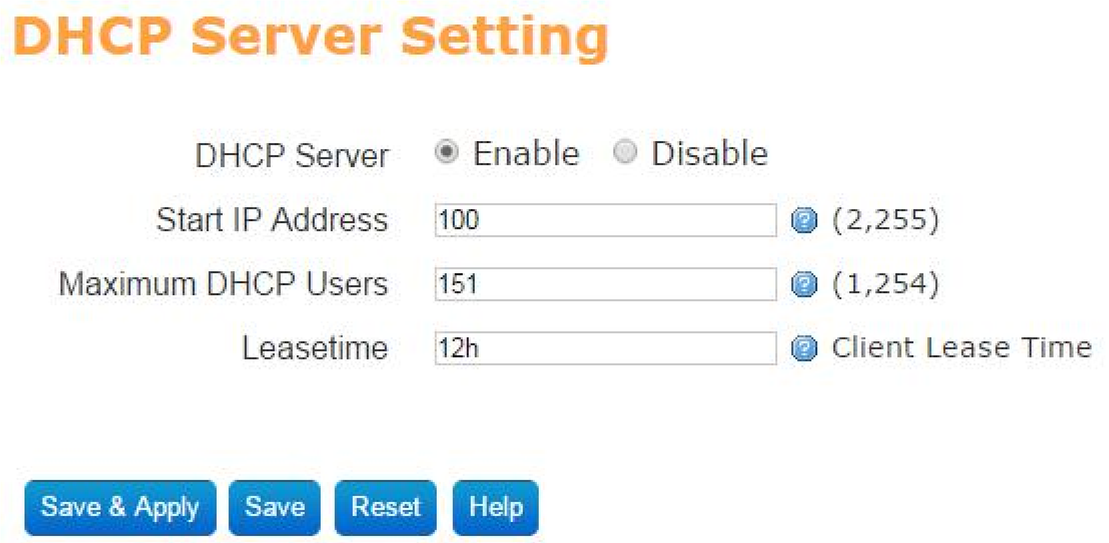
Local Address: 192.168.4.1

Netmask: 255.255.255.0 ▼

Local Address: the router IP in the local network
Netmask: Netmask assigned by the ISP or one you set by your own

DHCP Server Setting(DHCP)

These functions are used to configure dynamic host configuration protocol server setting. The F3938 router can be a DHCP server. The DHCP server provides a dynamic IP address for every pc automatically. You can configure all of computers to get IP addresses and DNS automatically while DHCP function of the router is selected, and make sure that there is only one DHCP server in the network.



DHCP Server Setting

DHCP Server: ● Enable ○ Disable

Start IP Address: 100 (2,255)

Maximum DHCP Users: 151 (1,254)

Leasetime: 12h Client Lease Time

DHCP Server: DHCP Sever is enabled by default. If users already have a DHCP server on their network or do not want a DHCP server, select disable. If the DHCP server is enabled, enter the IP address please.

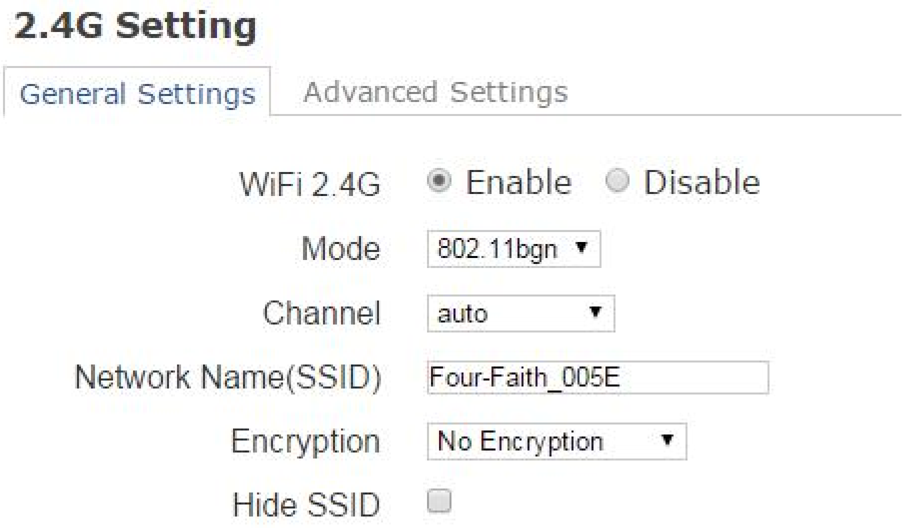
Start IP Address: Enter a numerical value for the DHCP server as the starting IP addresses. Please do not start with 192.168.1.1 (the router's own IP address). The start ip of the network must be great than or equal to 192.168.1.2, but less than 192.168.1.254. The default start IP is 192.168.1.100.

Maximum DHCP Users: Enter the maximum number of the PCs which users want to assign IP addresses to. The absolute maximum is 253 if 192.168.1.2 is users' starting IP address. The default number is 50.

Leasetime: The Leasetime is the amount of time that the dynamic IP address allowed to be used. Enter the leasetime, in minutes, so that the user could "lease" this dynamic IP address. New IP address will be assigned after the leasetime is expired.The default setting is 1440 minutes, which is one day. The configurable value ranges from 0 to 99999.

3.3.1.3 Wireless Setting

Basic Setting



2.4G Setting

WiFi 2.4G ● Enable ○ Disable

Mode 802.11bgn

Channel auto

Network Name(SSID) Four-Faith_005E

Encryption No Encryption

Hide SSID □

Enable: Enable WIFI

Disable: Disable WIFI

Wireless Mode:

802.11b: Only supports the 802.11b standard wireless devices.

802.11g: Only supports the 802.11g standard wireless devices.

802.11bg: Support 802.11b, 802.11g wireless devices.

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

Channel: There are 13 channels in total, from channel 1 to channel 13. Don’t use the same channel with other routers.

Network Name(SSID): The SSID is the network name shared in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters.

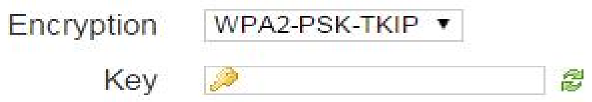
Encryption: The F3938 router contains 6 security modes in total. Encryption is disabled by default. If the mode is changed, click “Save & Apply” to make it effect immediately.

Hide SSID:

Uncheck: Broadcast SSID

Check: Hide SSID

Configure wireless network security.



Encryption WPA2-PSK-TKIP ▼

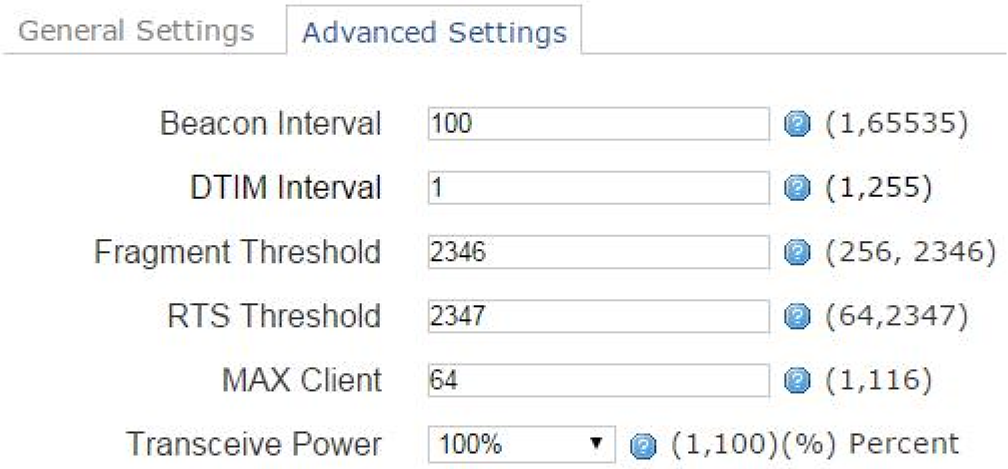
Key

WEP: WEP is a basic encryption algorithm, which is less secure than WPA. Using of WEP is discouraged due to the weaknesses security, 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).

WPA Personal/WPA2 Personal/WPA2 Person Mixed: F3938 provides 3 types of WPA security protocols,TKIP/AES/TKIP+AES,dynamic encryption keys. TKIP + AES, self-applicable TKIP or AES. WPA Person Mixed, allows WPA Personal and WPA2 Personal client mixed.

Advanced Settings:

Please be careful of these configurations, the router will degrade performance because of the incorrect configuration.



Beacon Interval	100	(1,65535)
DTIM Interval	1	(1,255)
Fragment Threshold	2346	(256, 2346)
RTS Threshold	2347	(64,2347)
MAX Client	64	(1,116)
Transceive Power	100% ▼	(1,100)(%) Percent

Beacon Interval: The default is 100. You can enter the value ranges from 1 to 65535, in milliseconds.

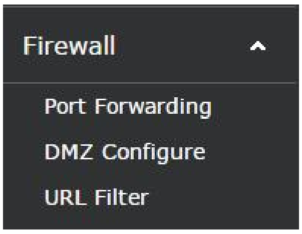
DTIM Interval: Thedefault is 1.it ranges from 1 to 255, which indicates that the interval of message transmission. The DTIM field is counted down. he rooter will inform the customer to get the broadcast and multicast messages, then the latest DTIM and DTIM interval will be sent. The clients will be waked up and get the broadcast and multicast messages from the transmitting stations.

Fragment Threshold: Keep the value 2346 by default, which ranges from 256 to 2346 Bytes. It indicates the maximum amount of data without division. You should increase Fragment Threshold when the higher packet loss rate occurs. The low fragment threshold may lead to the degrade performance. s a result, we advice you not to change fragment threshold.

RTS Threshold: Keep the value 2347 as default setting, which is range from 0 to 2347. A slight modification is allowed if you are in trouble of inconsistent data stream. The RTS/CTS mechanism will not take effect for the amount of network packets is less than preset Threshold. The router sends the RTS frame and data frame to the specific receiving station. After getting the RTS frame, The wireless terminals obtain the specific CTS frame, then transmission is starting.

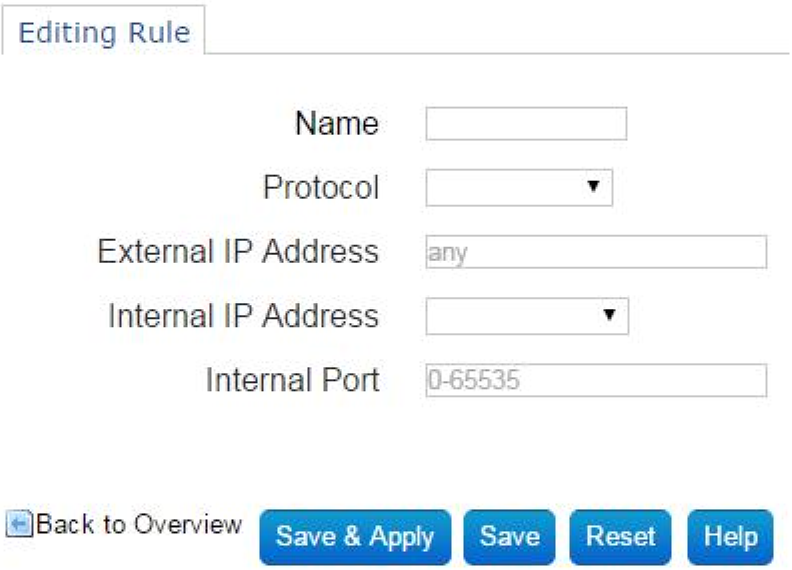
MAX Client: The maximum number of clients, 1-128.

3.3.2 Firewall



3.3.2.1 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 which use Internet access to perform functions such as video conferencing or online gaming.


Editing Rule

Name
Protocol
External IP Address: any
Internal IP Address
Internal Port: 0-65535

Names: Enter the application name in the field.

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

External IP Address: Forward only if sender matches this ip/net (example 192.168.1.0/24).

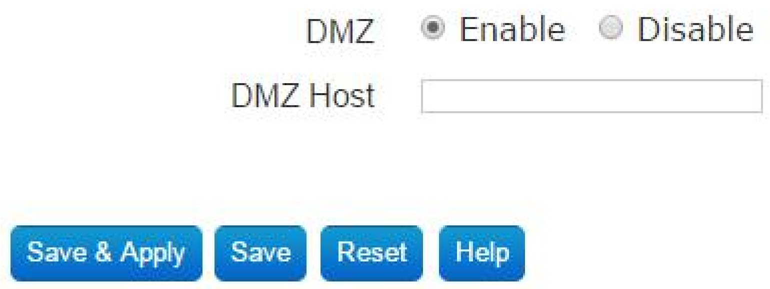
Internal IP Address: Enter the IP Address of the PC which is running the application.

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

Click “Save” or “Save & Apply”to complete modification. Click “Reset” to roll back the changes. The shortcut “Help” locates on the lower right corner of the page, click it for more details.

3.3.2.2 DMZ

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



DMZ ● Enable ○ Disable

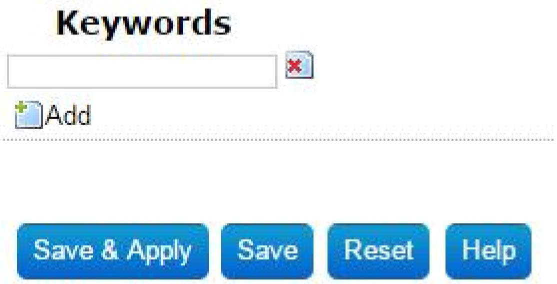
DMZ Host

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 & Apply”** or “**Save**” to save your settings. Click the “**Reset**” to cancel your changes.

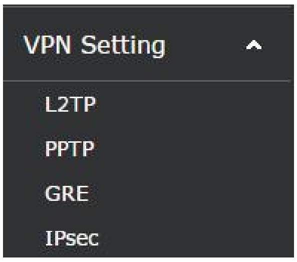
3.3.2.3 URL Filter

It filters some specific domain address. If you visit the domain address, firewall intercept it.



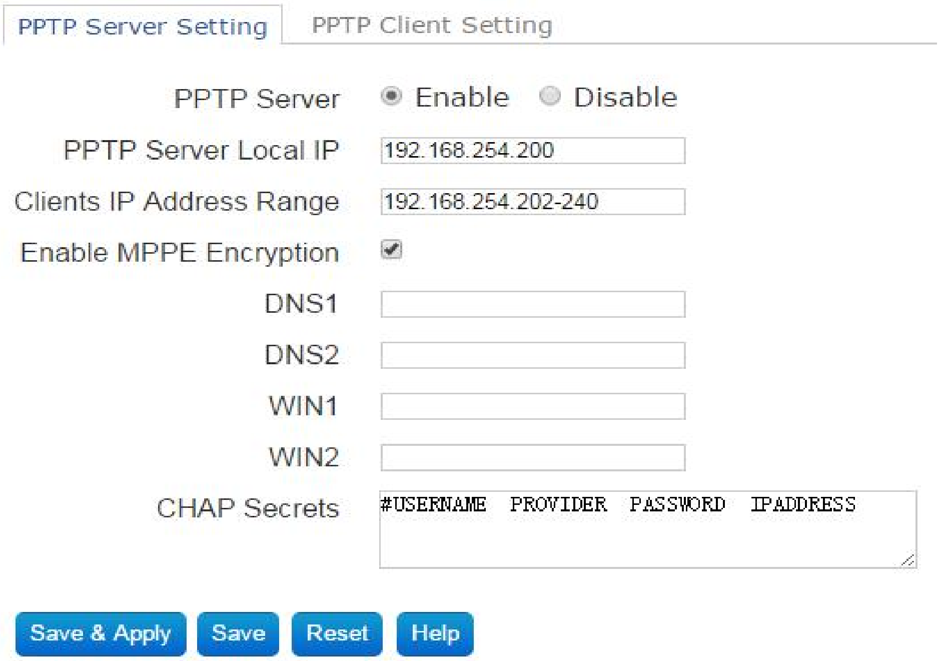
Click “Add” to add more key words.

3.3.4 VPN



3.3.4.1 PPTP

PPTP Server



PPTP Server	● Enable ○ Disable
PPTP Server Local IP	192.168.254.200
Clients IP Address Range	192.168.254.202-240
Enable MPPE Encryption	☑
DNS1	
DNS2	
WIN1	
WIN2	
CHAP Secrets	#USERNAME PROVIDER PASSWORD IPADDRESS

PPTP Server Local IP: Enter the PPTP Server IP address, different with LAN IP address.

Clients IP Address Range: IP addresses assigned to the clients, **xxx.xxx.xxx.xxx-xxx**

Enable MPPE Encryption: Use MPPE Force Encryption.

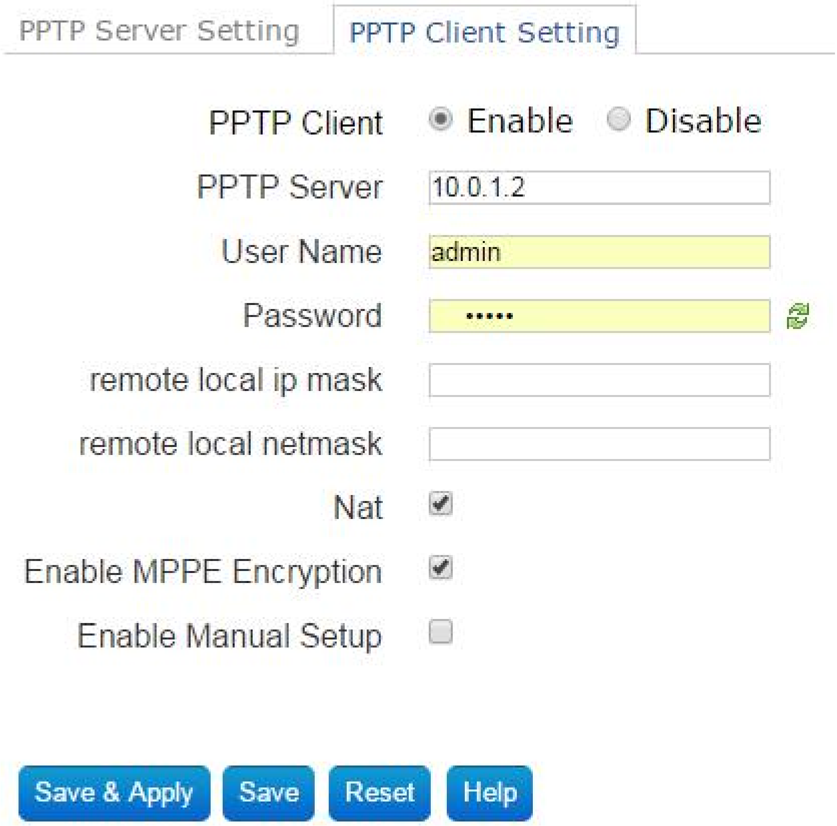
DNS1,DNS2,WINS1,WINS2: Set your first DNS, second DNS, first wins, second wins.

CHAP Secrets: The usernames and passwords of the clients.

NOTE: The Clients IP can’t be the same with the IP of DHCP, but outside of the range.

CHAP Secrets format: user blank*blank password blank*

PPTP Client



PPTP Client ● Enable ○ Disable

PPTP Server 10.0.1.2

User Name admin

Password •••••

remote local ip mask

remote local netmask

Nat ☑

Enable MPPE Encryption ☑

Enable Manual Setup □

PPTP Server: The IP address of PPTP server

User Name: The user name which is recognized by the server

Password: The password which is corresponding to user name

remote local ip mask: The remote local ip address

remote local netmask: Netmask assigned by the ISP of remote local ip;

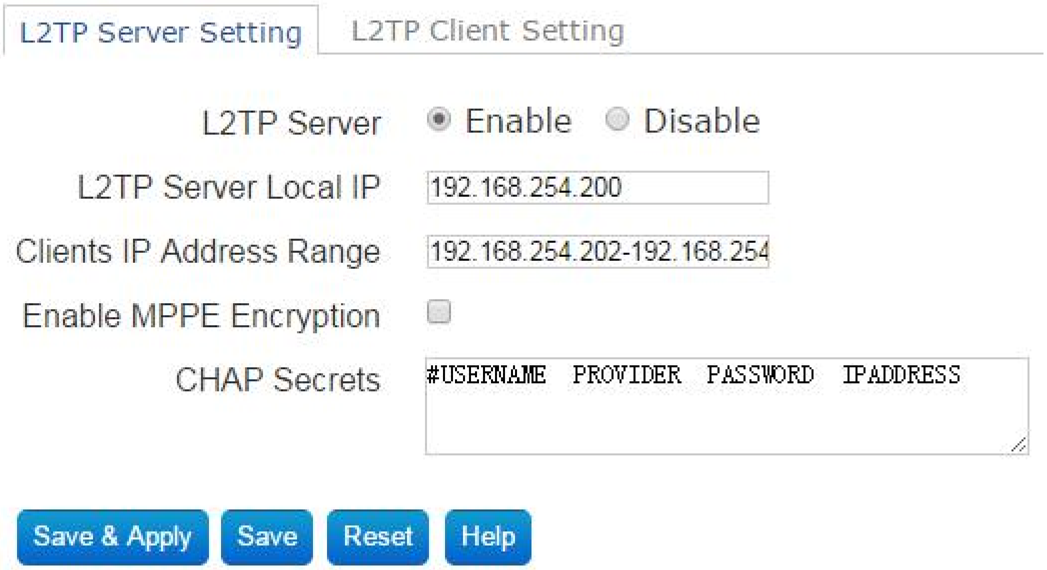
Nat: Allow network address translation

Enable MPPE Encryption: Use MPPE Force Encryption.

Enable Manual Setup: Assign the IP address manually.

3.3.4.2 L2TP

L2TP Server



L2TP Server ● Enable ○ Disable

L2TP Server Local IP 192.168.254.200

Clients IP Address Range 192.168.254.202-192.168.254

Enable MPPE Encryption □

CHAP Secrets #USERNAME PROVIDER PASSWORD IPADDRESS

L2TP Server Local IP: Enter the L2TP Server IP address, make sure that the Sever IP is different from LAN IP address.

Clients IP Address Range: IP addresses assigned to the Clinets, **xxx.xxx.xxx.xxx-xxx**

Enable MPPE Encryption：Use MPPE Force Encryption.

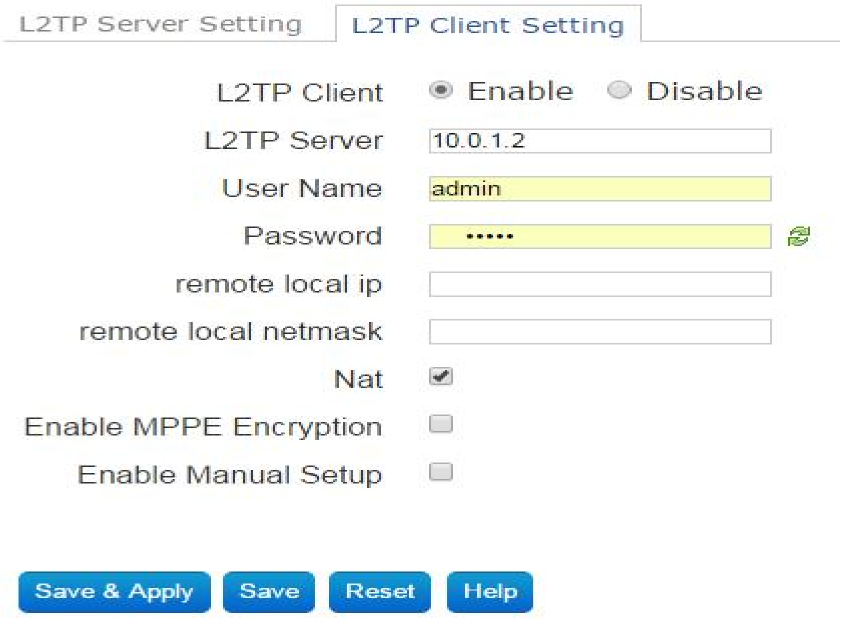
DNS1，DNS2，WINS1，WINS2：Set your first DNS, second DNS, first wins, second wins.

CHAP Secrets： The usernames and passwords of the clients.

NOTE： The Clients IP can’t be the same with the IP of DHCP, but outside of the range.

CHAP Secrets format: user blank*blank password blank*

L2TP Clinet



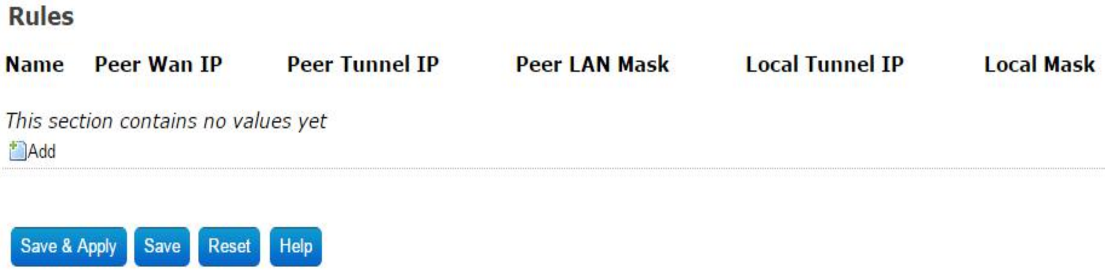
L2TP Server Setting | L2TP Client Setting

L2TP Client	● Enable ○ Disable
L2TP Server	10.0.1.2
User Name	admin
Password	•••••
remote local ip	
remote local netmask	
Nat	☑
Enable MPPE Encryption	□
Enable Manual Setup	□

L2TP Server: The IP address of L2TP server
User Name: The user name which is recognized by the server
Password: The password which is corresponding to user name
remote local ip mask: The remote local ip address
remote local netmask: Netmask assigned by the ISP of remote local ip;
Nat: Allow network address translation
Enable MPPE Encryption: Use MPPE force encryption.
Enable Manual Setup: Configure the IP address manually.

3.3.4.3 GRE

GRE (Generic Routing Encapsulation) encapsulates the network layer protocol(IP , IPX) data packets, it makes these packets can be transferred in the other network layer protocol. GRE uses tunnel technology, which is the third layer protocol of VPN(Virtual Private Network). With GRE you can setup VPN tunnel through GRE protocol. You can setup max 12 tunnels.

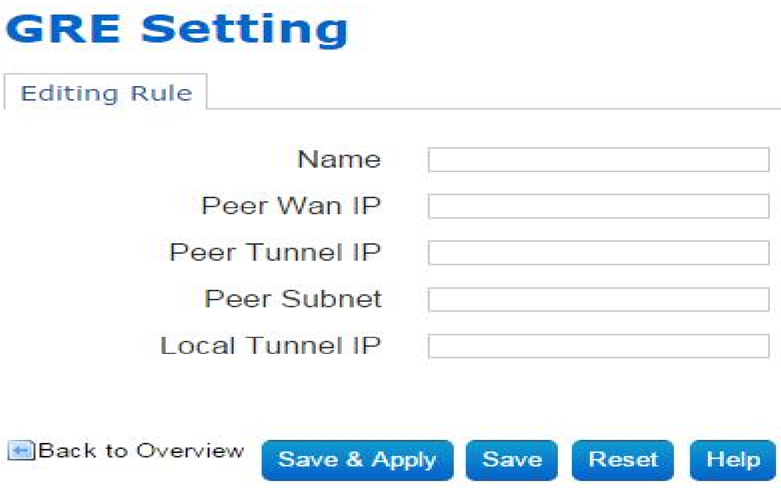


Rules

Name	Peer Wan IP	Peer Tunnel IP	Peer LAN Mask	Local Tunnel IP	Local Mask

This section contains no values yet

Click “Add” to add rules, just like below.



GRE Setting

Editing Rule

Name	
Peer Wan IP	
Peer Tunnel IP	
Peer Subnet	
Local Tunnel IP	

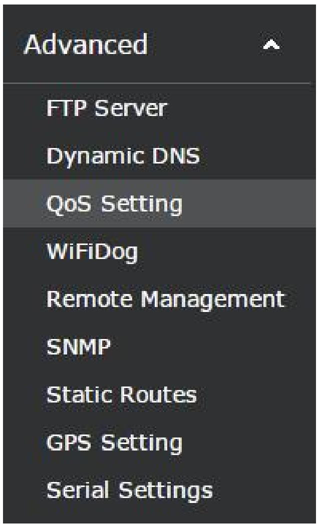
Name: The name of GRE rule

Peer Wan IP: Enter the GRE Wan IP of peer side

Peer Tunnel IP: The GRE tunnel IP of peer side

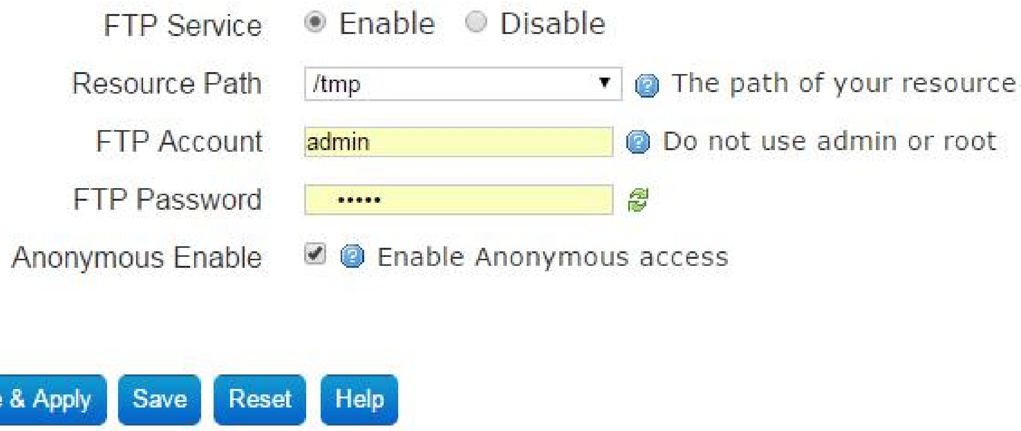
Peer Subnet: The Subnet of peer side

3.3.5 Advanced



3.3.5.1 FTP Server

In this page, you can config the FTP server setting..



FTP Service ● Enable ○ Disable

Resource Path /tmp ▾ The path of your resource

FTP Account admin Do not use admin or root

FTP Password •••••

Anonymous Enable ☑ Enable Anonymous access

FTP Service: FTP Service is enabled by default, select “Disable” if you want to disable this function.

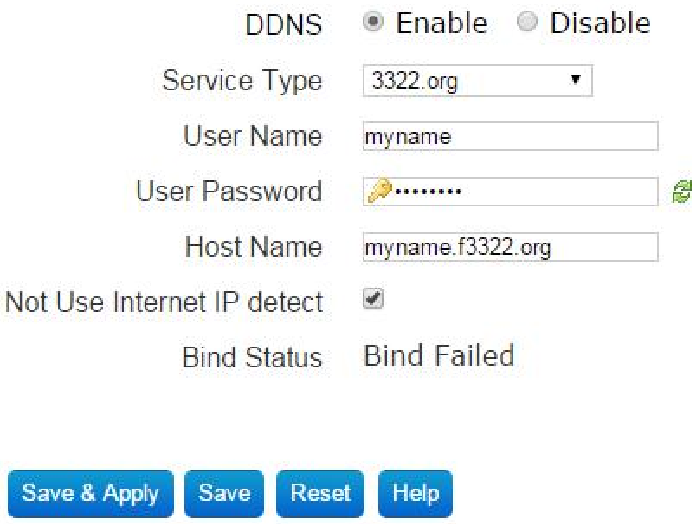
Resource Path: The path of your resource, you can select other option in the drop-down box.

FTP Account: The FTP account of the service, do not use admin or root

FTP Password: The password according to FTP Account.

3.3.5.2 Dynamic DNS

Because of the allocation of dynamic IP addresses, wan IP addresses always change when the routers connect to the internet. In that case, you should use dynamic DNS. The domain name providers allows you to register a domain name which is signing up with current ip of the routers. As a result, you can access to the latest internet IP address.



DDNS ● Enable ○ Disable

Service Type 3322.org ▾

User Name myname

User Password ••••••••

Host Name myname.f3322.org

Not Use Internet IP detect ☑

Bind Status Bind Failed

Service Type: F3938 router supports several DDNS server, such as DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP. User-defined server is allowed either.

User Name: The user name which is registered on the DDNS server. The maximum length is 64 characters.

User Password: The password according to the user name. The maximum length is 32 characters.

Host Name: The subdomain which is registered on the DDNS server. There is no limit to the length of host name.

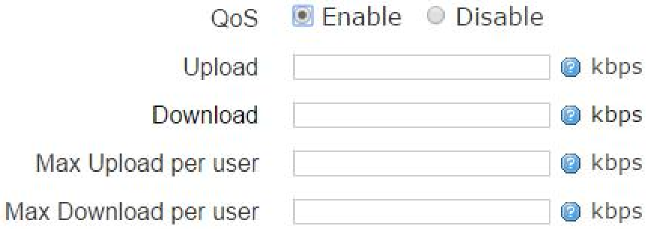
Not USE Internet IP detect: The approach to access wan IP address. Router should detect the wan IP itself when it is selected.

Bind Status: The running state of DDNS. "Bind Failed" or "Bind success"

3.3.5.3 QoS Setting

QoS function controls the upload traffic and download traffic to balance the traffic, and it also can assign priority for specific IP address or MAC.

Basic Setup



QoS ● Enable ○ Disable

Upload ________ kbps

Download ________ kbps

Max Upload per user ________ kbps

Max Download per user ________ kbps

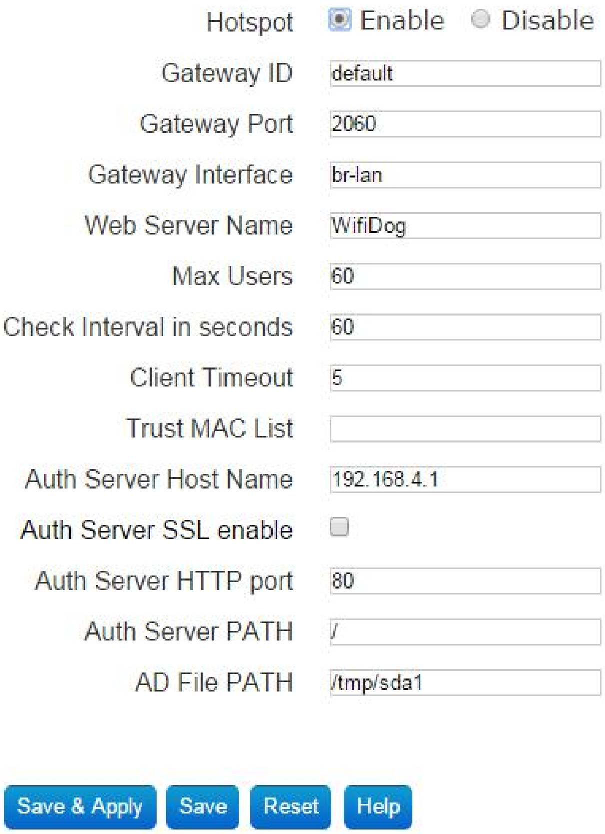
Download speed(kbit/s): In order to use bandwidth management (QoS) you must enter bandwidth values for your downlink. These are generally 80% to 90% of your maximum bandwidth.

Upload speed(kbit/s): 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.

Max Upload per user:you can enter max upload bandwidth values for per user.

Max Download per user:you can enter max download bandwidth values for per user.

3.3.5.4 WIFIDOG



Hotspot	● Enable ○ Disable
Gateway ID	default
Gateway Port	2060
Gateway Interface	br-lan
Web Server Name	WifiDog
Max Users	60
Check Interval in seconds	60
Client Timeout	5
Trust MAC List	
Auth Server Host Name	192.168.4.1
Auth Server SSL enable	□
Auth Server HTTP port	80
Auth Server PATH	/
AD File PATH	/tmp/sda1

Gateway ID: hotspot remote / local authentication server that uniquely identifies the default is default

Port: default 2060, range: 1 - 65535 Please note that no special circumstances do not arbitrarily modify

Max Users: limit the number of customers connected to the local WIFI Internet access, the default factory setting is 60

Check Interval (in sec.): Detection WIFI wireless client terminals (computers, mobile phones, etc.) and link status time interval of this station router, the default is 180 seconds

Client Timeout (minutes): detects the connection at the maximum timeout this station WIFI wireless router client terminals (computers, mobile phones, etc.) did not have the Internet to communicate, think 10 minutes by default. After this time customers need to re-authenticate login.

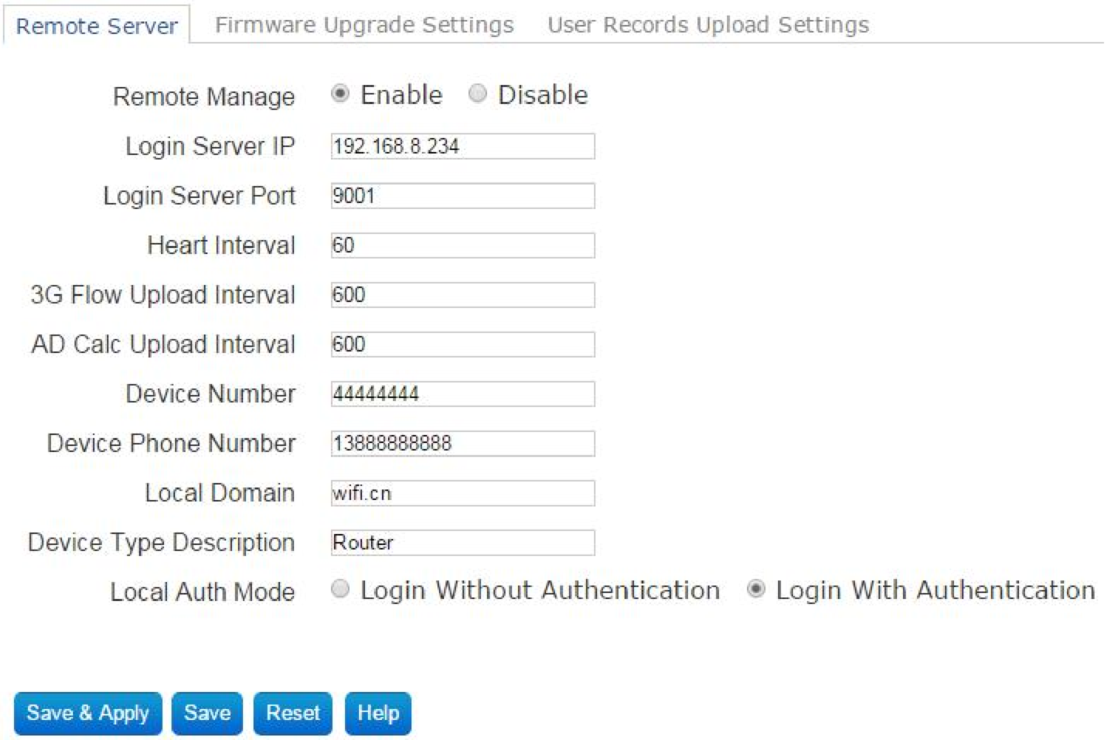
Auth Server Host Name: remote / local hotspot server host domain name or IP, if the authentication or jump in our station carried the router, please fill out this station router's LAN IP network segment

AuthServer Path: Remote / local server storage WIFI hotspot jump page advertisements path, the default is "/"

3.3.5.5 Remote Management Settings

Remote management function can manage all of the routes by the cloud platform. Users can control all devices by the cloud platform, including routine configuration, firmware upgrade and User records upload.

Remote Server:



Remote Manage ● Enable ○ Disable
Login Server IP 192.168.8.234
Login Server Port 9001
Heart Interval 60
3G Flow Upload Interval 600
AD Calc Upload Interval 600
Device Number 44444444
Device Phone Number 13888888888
Local Domain wifi.cn
Device Type Description Router
Local Auth Mode ○ Login Without Authentication ● Login With Authentication

Remote Manage:

Enable: Enable the Remote Manage function.

Disable: Disable the Remote Manage function.

Login Server IP: The IP address of cloud platform server.

Login Server Port: The port of cloud platform server

Heart Interval: The heartbeat interval to keep connection alive., 600 seconds by default

3G Flow Upload Interval: The interval of 3G flow, 600 seconds by default

Device Number: Device number is the only identification, which is a eight-digit number. Make sure that the device number is different from other devices. The defaut is 44444444.

Device Phone Number: Enter the phone number of the sim card.

Local Domain: The domain name of the router.

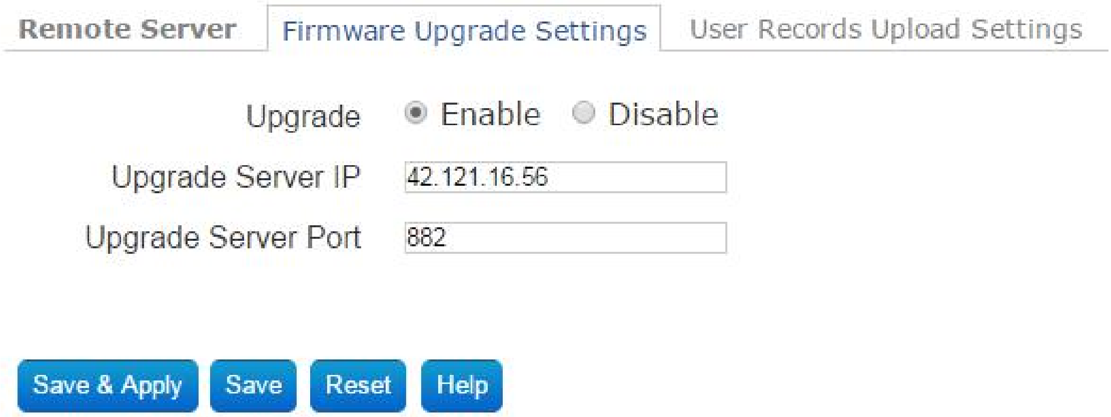
Device Type Description: The type description of the device.

Local Auth Mode:

Login With Authentication: Enable the local authentication.

Login Without Authentication: Disable the local authentication.

Firmware Upgrade Settings:



Upgrade ● Enable ○ Disable

Upgrade Server IP 42.121.16.56

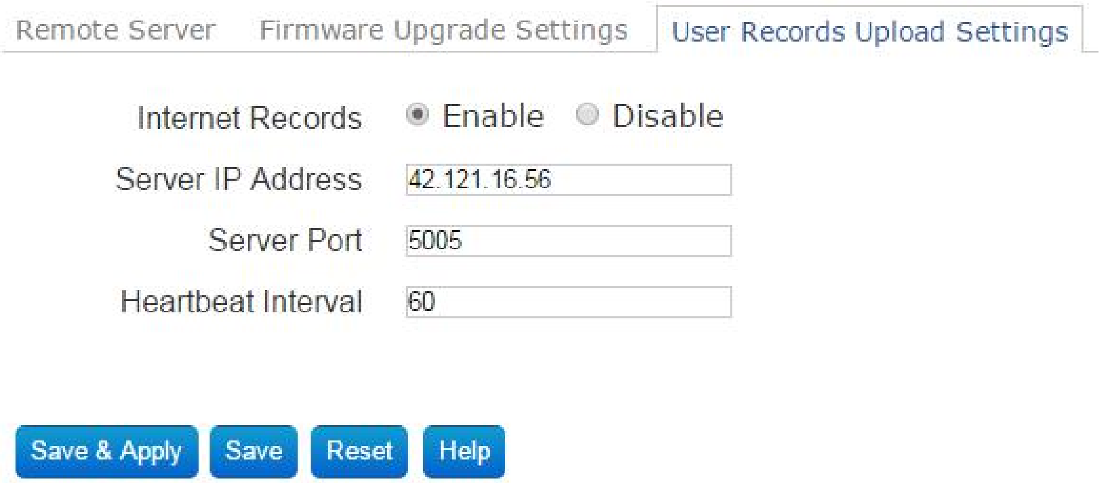
Upgrade Server Port 882

Upgrade Server IP: The remote upgrade server IP address.

Upgrade Server Port: The remote upgrade server port.

User Records Upload Settings:

This feature is used to upload user records.



Internet Records ● Enable ○ Disable

Server IP Address 42.121.16.56

Server Port 5005

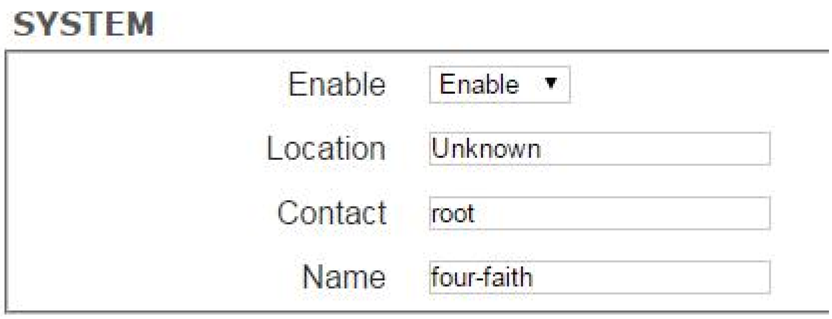
Heartbeat Interval 60

Server IP Address: The remote user records server IP address.

Server Port: The remote user records server port.

3.3.5.5 SNMP

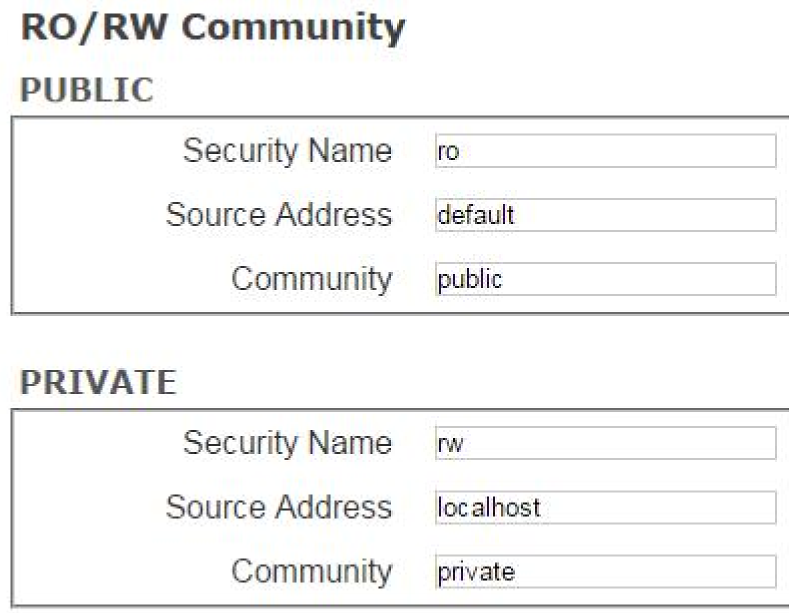
Simple **N**etwork **M**anagement **P**rotocol (**SNMP**) is a widely used protocol for monitoring the health and welfare of network equipment (eg. routers), computer equipment and even devices like UPSs.



SYSTEM

Enable	Enable ▼
Location	Unknown
Contact	root
Name	four-faith

Location: The location of the equipment.
Contact: Contact this equipment management
Name: Device name, The default name is four-faith



RO/RW Community

PUBLIC

Security Name	ro
Source Address	default
Community	public

PRIVATE

Security Name	rw
Source Address	localhost
Community	private

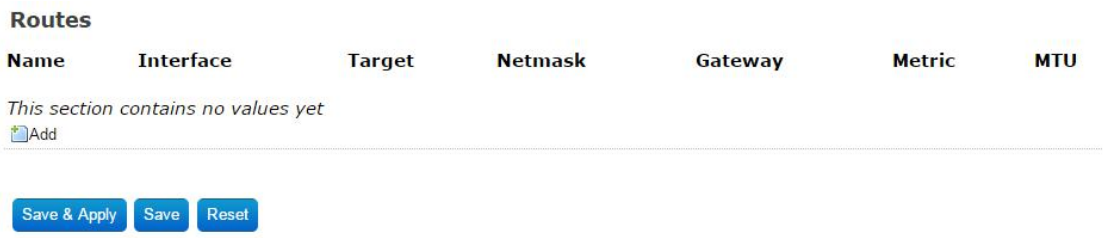
PUBLIC:
Security Name: The security name is RO, means only to read.
Source Address: The source address is default.
Community: The community is public by default

PRIVATE:

Security Name: The security name is rw, means read-write permissions
Source Address: The source address is localhost.
Community: The community is private by default

Click “Save & Apply” to make it effect and click “Save” just to save it but not apply, or you also can click “Reset” to turn to default value.

3.3.5.6 Static Routes

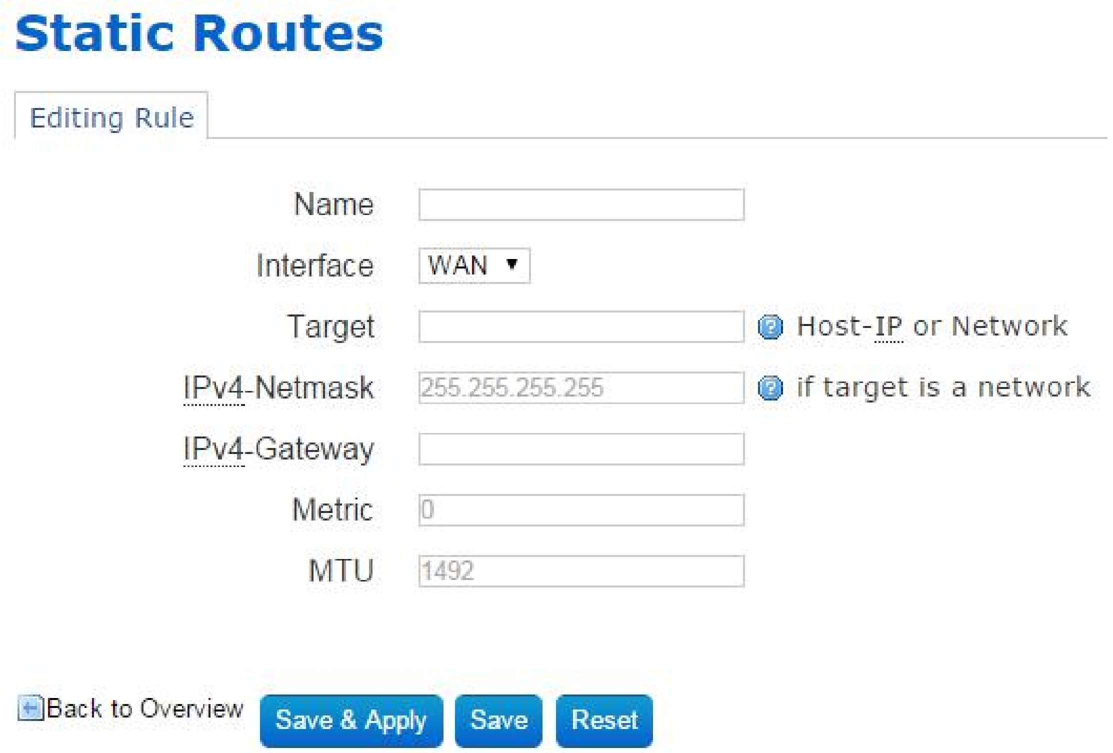


Routes

Name	Interface	Target	Netmask	Gateway	Metric	MTU

This section contains no values yet

If you want to set static routing between the router and the other network, Click “Add” on the bottom-left corner of the page, and you will see below, then edit the rule please.



Static Routes

Editing Rule

Name	
Interface	WAN ▾
Target	Host-IP or Network
IPv4-Netmask	255.255.255.255 — if target is a network
IPv4-Gateway	
Metric	0
MTU	1492

Name: Defined routing name by users, up to 25 characters

Interface: It indicates that users whether the Destination IP Address is on the LAN (internal wired and wireless networks) or the WAN (Internet). Select the appropriate interface option in the drop-down box.

Target: The destination IP address, which is the address that users want to assign a static route.

IPv4-Netmask: The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion

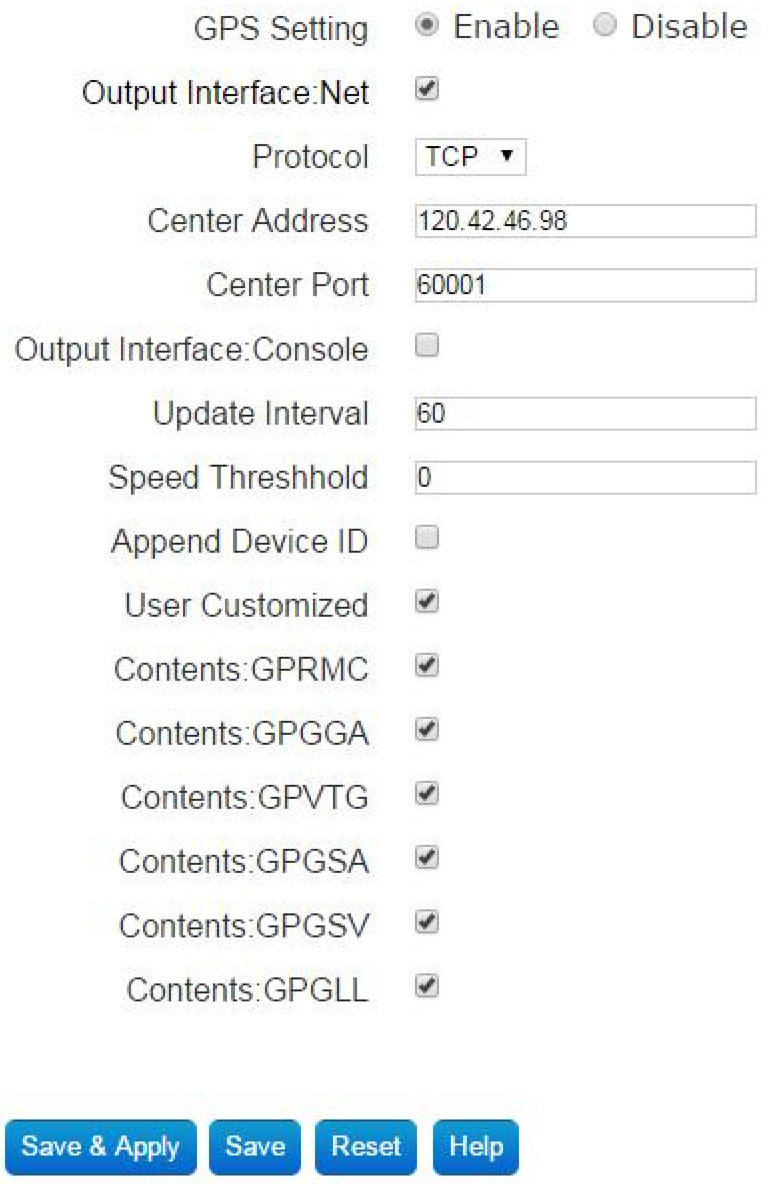
IPv4-Gateway: IP address of the gateway device that allows for contact between the router and the network or host.

Metric: 0-9999, the same as the ttl.

MTU: Maximum Transmission Unit, set the value according to the local MTU and the internet MTU, to make full use of the internet throughout.

3.3.5.7 GPS Setting

GPS setting allows you to set the GPS configuration. The user customized feature is provided.



GPS Setting	● Enable ○ Disable
Output Interface:Net	☑
Protocol	TCP
Center Address	120.42.46.98
Center Port	60001
Output Interface:Console	□
Update Interval	60
Speed Threshhold	0
Append Device ID	□
User Customized	☑
Contents:GPRMC	☑
Contents:GPGGA	☑
Contents:GPVTG	☑
Contents:GPGSA	☑
Contents:GPGSV	☑
Contents:GPGLL	☑

Gps Setting: Enable or disable GPS function.

Output Interface:

Net: This item selects the network output interface.

Console: This item selects the GPS serial port output interface.

Protocol: TCP mode or UDP mode.

Center Address: The GPS center’s IP Address or domain name.

Center Port: The GPS center’s listening port.

Update Interval: The time interval between two GPS information update, unit is second.

Speed Threshold: The GPS speed threshold of update gps information.

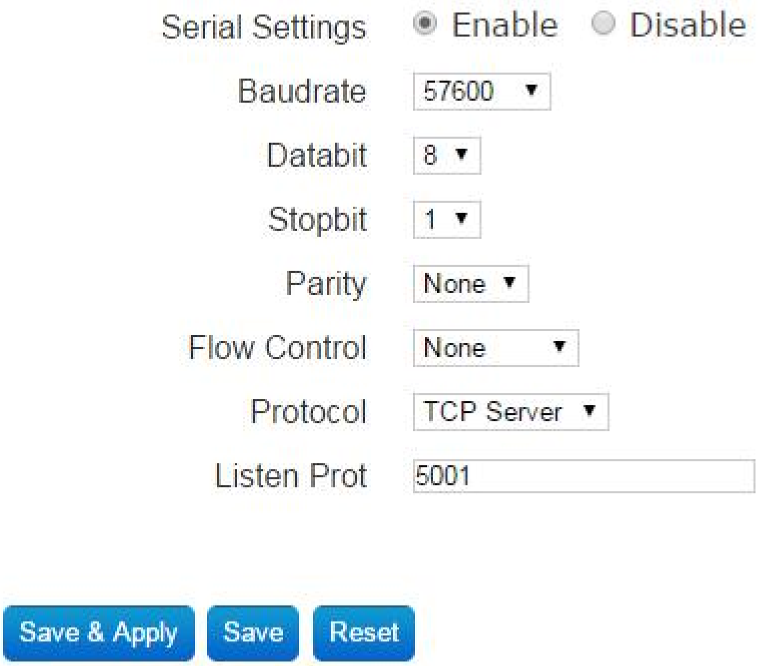
Append Device ID: The item selects the device ID.

Device ID: The device ID.

User Customized: GPS contents selection, including GPRMC, GPGGA, GPVTG, GPGSA, GPGSV, GPGLL.

3.3.5.8 Serial Setting

There is a console port on F3938 router. Normally, this port is used to debug the router. it can also be used as a serial port. The router has embedded a serial to TCP program. The data sent to the serial port is encapsulated by TCP/IP protocol stack and then is sent to the destination server. This function can work as a DTU (Data Terminal Unit).



Serial Settings	● Enable ○ Disable
Baudrate	57600 ▼
Databit	8 ▼
Stopbit	1 ▼
Parity	None ▼
Flow Control	None ▼
Protocol	TCP Server ▼
Listen Prot	5001

Baudrate: The serial port’s baudrate, there are several options, such as: 115200, 57600, 38400, 19200, 9600, 4800, 2400, etc.

Databit: The databit of the serial port

Stopbit: The stopbit of the serial port

Parity: The parity of the serial port

Flow Control: The flow control type of the serial port

Protocol: The protocol type to transmit data.

UDP(DTU) – Data transmit with UDP protocol , work as a DTU which has application protocol and hear beat mechanism.

Pure UDP – Data transmit with standard UDP protocol.

TCP(DTU) -- Data transmit with TCP protocol , work as a DTU which has application protocol and hear beat mechanism.

Pure TCP -- Data transmit with standard TCP protocol, router is the client.

TCP Server -- Data transmit with standard TCP protocol, router is the server.

TCST -- Data transmit with TCP protocol, Using a custom data

Server Address: The data service center's IP Address or domain name.

Server Port: The data service center's listening port.

Device Number: The router's phone number.

Device ID: The router's identity ID.

Heartbeat Interval: The time interval to send heart beat packet. This item is valid only when you choose UDP(DTU) or TCP(DTU) protocol type.

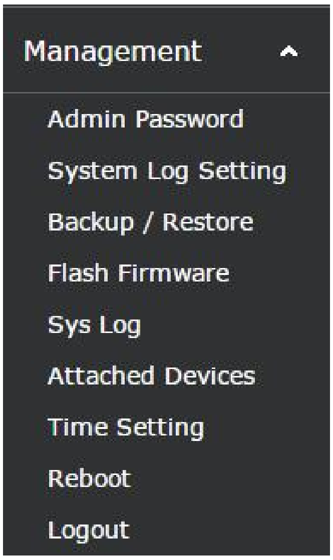
Listen Port: This item is valid when Protocol Type is "TCP Server"

Custom Heartbeat Packet : This item is valid when Protocol Type is "TCST"

Custom Registration Packets: This item is valid when Protocol Type is "TCST"

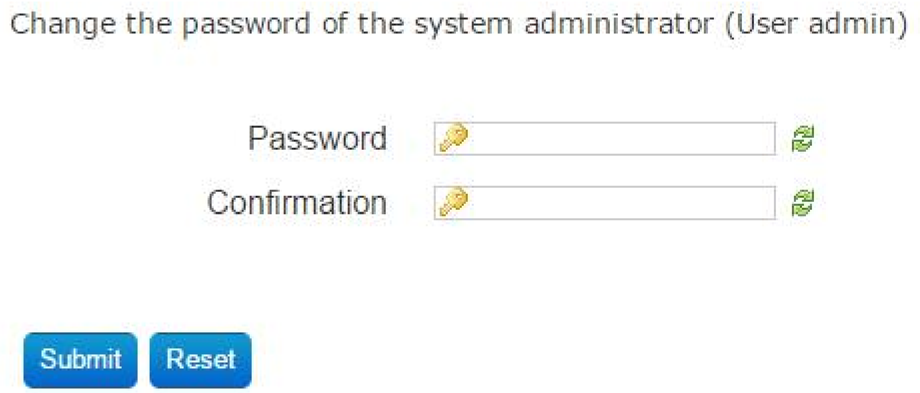
3.3.6 Management

The Management screen allows you to change the settings of the F3938 router. On this page you will find most of the configurable items of the router code.



3.3.6.1 Admin Password

In this part, user can modify the password and submit it to make it effect.



Change the password of the system administrator (User admin)

Password

Confirmation

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.

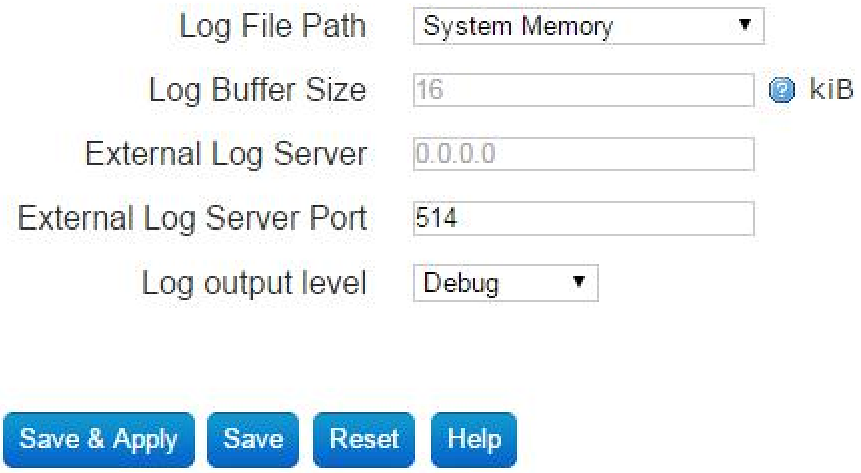
Note：

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.

3.3.6.2 System Log Setting

System Log Setting is used to modify the system log configuration.



Log File Path: System Memory

Log Buffer Size: 16 kiB

External Log Server: 0.0.0.0

External Log Server Port: 514

Log output level: Debug

Log File Path: Select the storage path in the drop-down box, which are “System memory”, “Console”,”KINGSTON(mmcblk0p1:)”,”Volume(sda1:)”, Please be attention that system log would be lost when the system is power failures if “System memory” is selected.

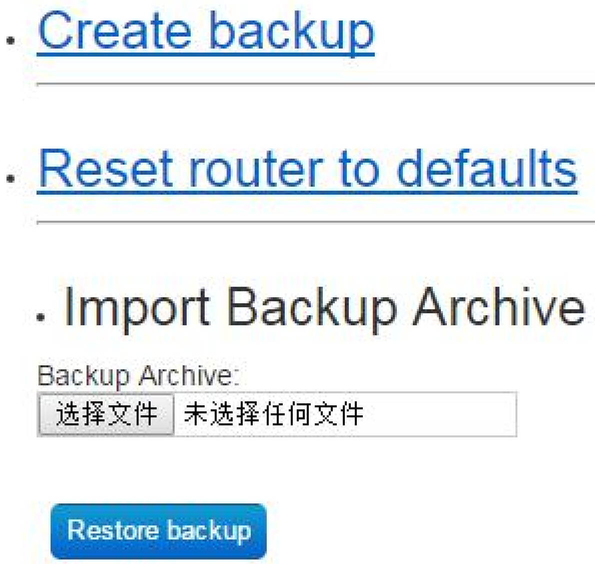
Log Buffer Size: Enter the buffer length of log file, in KB. The Log file will be clean when the data length is over the threshold you have defined.

External Log Server: If you have an external log server, enter the IP address.

Log output level: Select the debug level in the drop-down box. The debug levels contain Debug, Info, Notice, Warning, Error, Critical, Alert, Emergency. Debug is the lowest priority level while “Emergency” is the highest. Select the appropriate level. The lower the priority is, the more output. Click the “Save & Apply” to make it effect.

3.3.6.3 Backup/Restore

Backup/Restore functions, as the name, is used to backup the current configurations, and restore the settings at anytime if necessary.



- Create backup
- Reset router to defaults
- Import Backup Archive

Backup Archive:

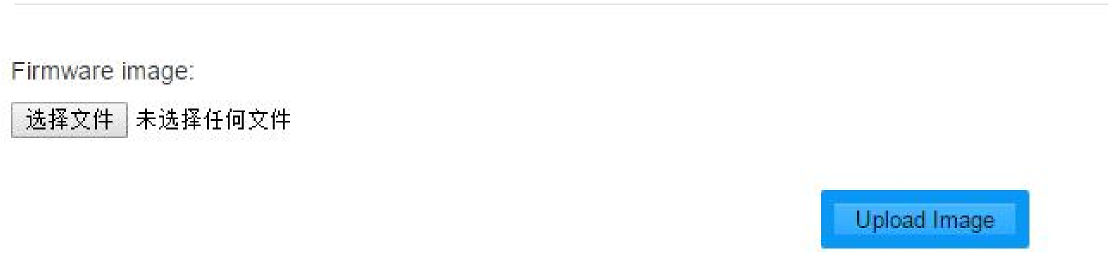
create backup: In case you need to reset the router back to the factory default settings, click “Create backup” to backup the current configurations, which maybe take several minutes. Some of configuration files, which are under the directory /lib and /ete, are compressed to backup-Four-Faith-xxxx-xx-xx.tar.gz.

Reset router to defaults: It is used to reset all configurations to their default values.

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 192.168.4.1 and the default password is “admin”.

3.3.6.4 Flash Firmware


Firmware image:

Flash Firmware: New firmware versions are posted at www.four- faith.com and can be downloaded. If the Router is not experiencing difficulties, then there is no need to download a 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 that you have backup the current router settings before you upgrade the 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 Image” button and wait until the upgrade is finished.

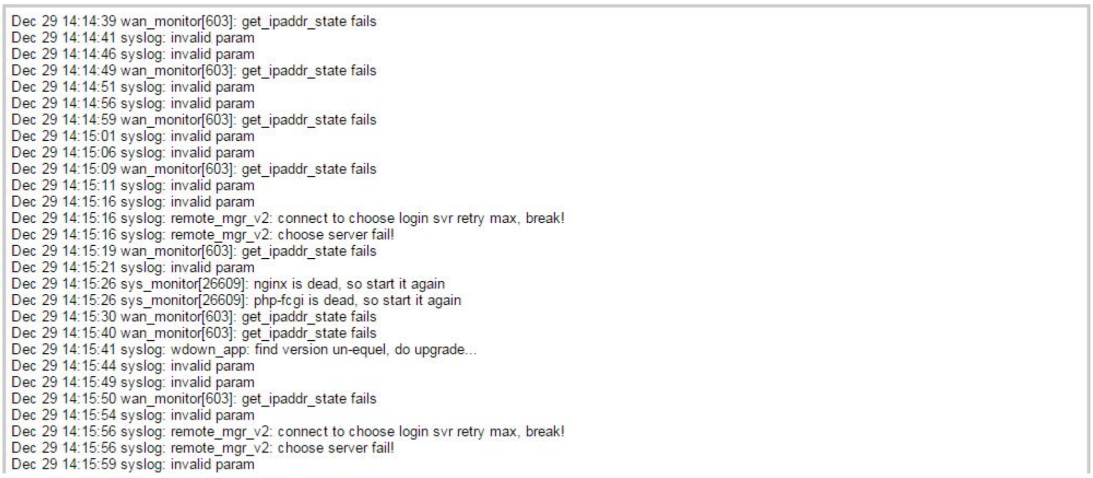
Note:

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.

3.3.6.5 Sys Log

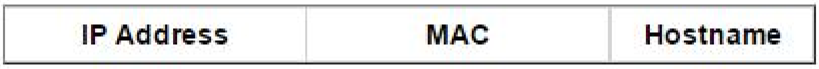
Sys Log shows the system log information to user . You can get the system running state of the router, and diagnose system problems.



```
Dec 29 14:14:39 wan_monitor[603]: get_ipaddr_state fails
Dec 29 14:14:41 syslog: invalid param
Dec 29 14:14:46 syslog: invalid param
Dec 29 14:14:49 wan_monitor[603]: get_ipaddr_state fails
Dec 29 14:14:51 syslog: invalid param
Dec 29 14:14:56 syslog: invalid param
Dec 29 14:14:59 wan_monitor[603]: get_ipaddr_state fails
Dec 29 14:15:01 syslog: invalid param
Dec 29 14:15:06 syslog: invalid param
Dec 29 14:15:09 wan_monitor[603]: get_ipaddr_state fails
Dec 29 14:15:11 syslog: invalid param
Dec 29 14:15:16 syslog: invalid param
Dec 29 14:15:16 syslog: remote_mgr_v2: connect to choose login svr retry max, break!
Dec 29 14:15:16 syslog: remote_mgr_v2: choose server fail!
Dec 29 14:15:19 wan_monitor[603]: get_ipaddr_state fails
Dec 29 14:15:21 syslog: invalid param
Dec 29 14:15:26 sys_monitor[26609]: nginx is dead, so start it again
Dec 29 14:15:26 sys_monitor[26609]: php-fcgi is dead, so start it again
Dec 29 14:15:30 wan_monitor[603]: get_ipaddr_state fails
Dec 29 14:15:40 wan_monitor[603]: get_ipaddr_state fails
Dec 29 14:15:41 syslog: wdown_app: find version un-equel, do upgrade...
Dec 29 14:15:44 syslog: invalid param
Dec 29 14:15:49 syslog: invalid param
Dec 29 14:15:50 wan_monitor[603]: get_ipaddr_state fails
Dec 29 14:15:54 syslog: invalid param
Dec 29 14:15:56 syslog: remote_mgr_v2: connect to choose login svr retry max, break!
Dec 29 14:15:56 syslog: remote_mgr_v2: choose server fail!
Dec 29 14:15:59 syslog: invalid param
```

3.3.6.7 Attached Setting

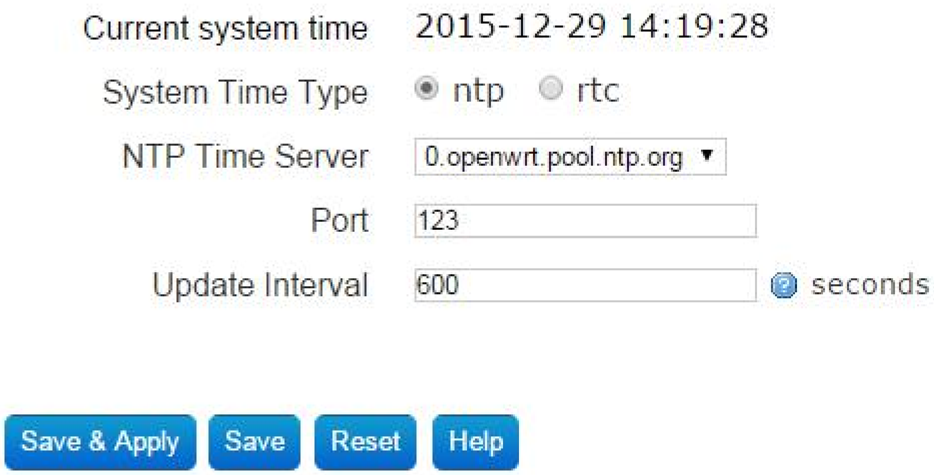
Attached Setting functions to show the attached devices in the tables, Which shows the "IP Address", "Mac", "Hostname". Click "Refresh" to update the attached device table information.



IP Address	MAC	Hostname

3.3.6.8 Time Setting

This function allows you to setting the system time.



Current system time 2015-12-29 14:19:28

System Time Type ● ntp ○ rtc

NTP Time Server 0.openwrt.pool.ntp.org ▼

Port 123

Update Interval 600 seconds

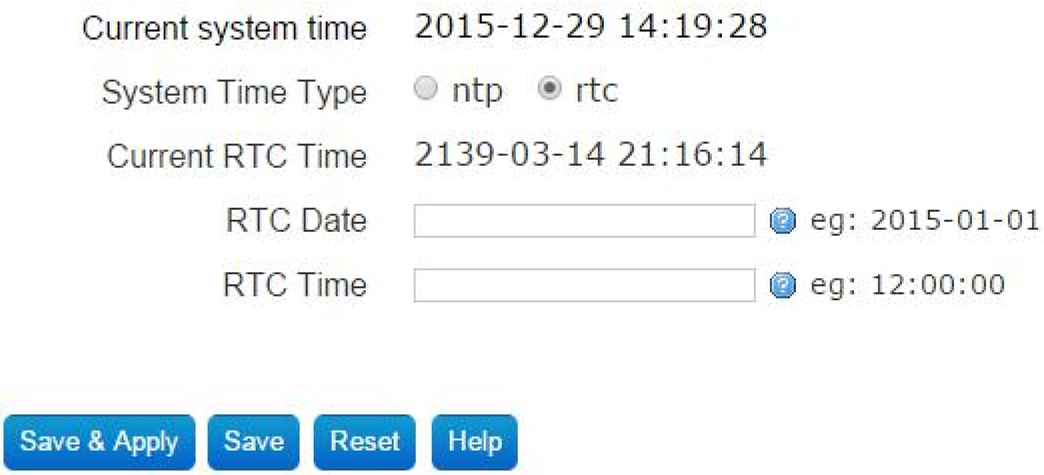
Current system time: Show the current system time.

System Time Type: The optional time type of the system are RTC and NTP. If RTC selected, the hardware RTC time is used. If ntp selected, it can synchronize to the NTP time server. As shown, The current time type is ntp.

NTP Time Server: Select the optional time server which you want to synchronize to. You also can select the custom option, and enter the time server by yourself.

Port: The listening port of the time server.

Update Interval: It specifys the interval of NTP time updating.



Current system time 2015-12-29 14:19:28

System Time Type ○ ntp ● rtc

Current RTC Time 2139-03-14 21:16:14

RTC Date eg: 2015-01-01

RTC Time eg: 12:00:00

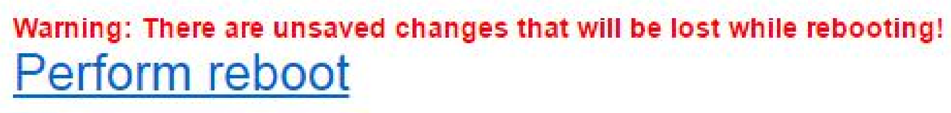
If the RTC is selected, the RTC clock time is shown as above.

RTC Date: Enter the RTC date into the field if you want to modify it. Please pay attention to the date format, separated with “-”;

RTC Time: Enter the RTC date into the field if you want to modify it. Please pay attention to the date format, separated with “:”;

3.3.6.9 Reboot

This feature is used to reboot the operating system of your device. Click the “Perform reboot” as below.



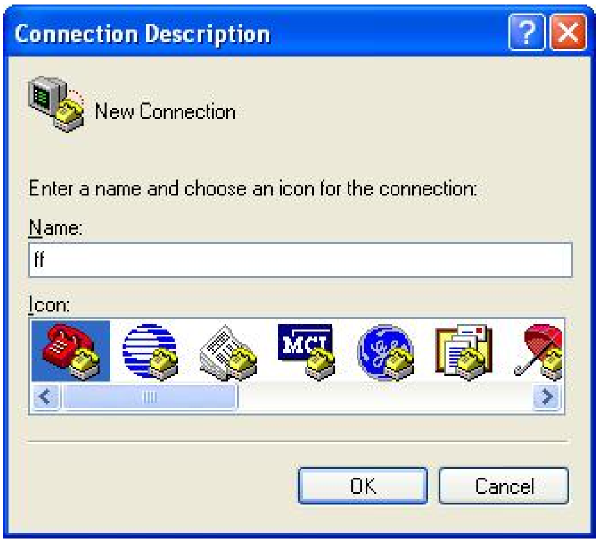
Warning: There are unsaved changes that will be lost while rebooting!

Perform reboot

3.3.7 Appendix

The following steps describe how to setup Windows XP Hyper Terminal.

1. Press “Start”→”Programs”→”Accessories”→”Communications”→”Hyper Terminal”



Connection Description

New Connection

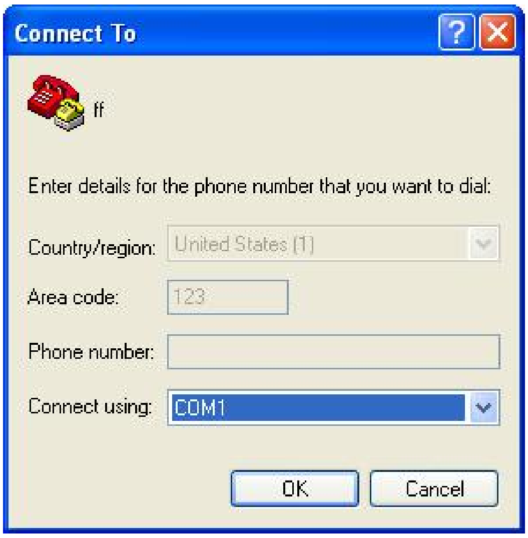
Enter a name and choose an icon for the connection:

Name: ff

Icon:

2. Input connection name, choose “OK”

3. Choose the correct COM port which connects to modem, choose “OK”



Connect To

ff

Enter details for the phone number that you want to dial:

Country/region: United States (1)

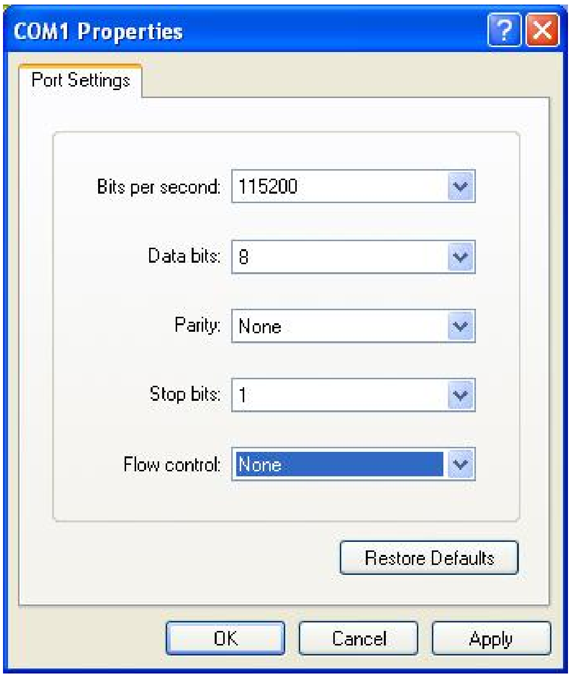
Area code: 123

Phone number:

Connect using: COM1

4. Configure the serial port parameters as following, choose “OK”

   Bits per second: 115200
   Data bits: 8
   Parity: None
   Stop bits: 1
   Flow control: None



COM1 Properties

Port Settings

Bits per second: 115200

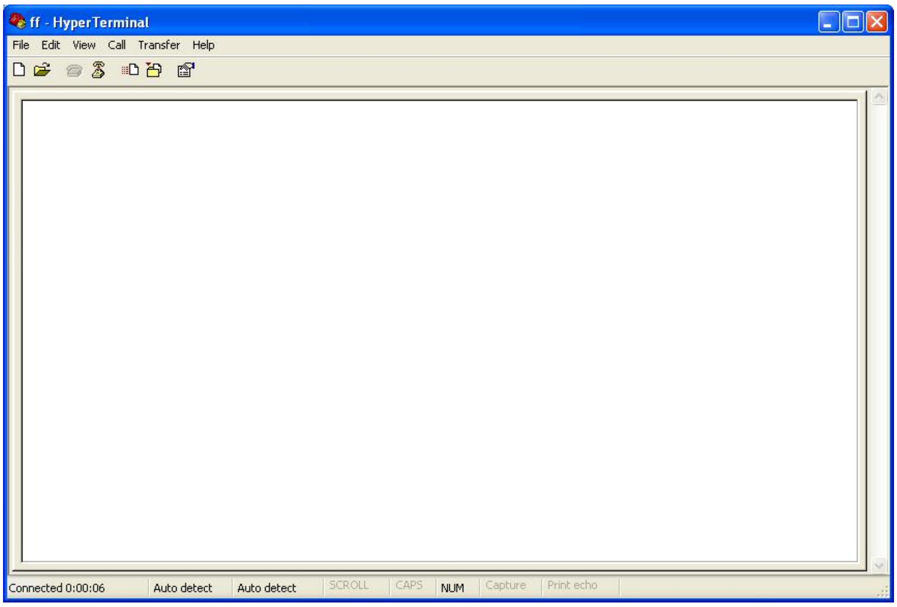
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

5. Complete Hyper Terminal operation, It runs as following


ff - HyperTerminal
File Edit View Call Transfer Help
Connected 0:00:06
Auto detect
Auto detect
SCROLL
CAPS
NUM
Capture
Print echo