Bivocom®

Industrial Cellular WIFI Router
TR321 Series User Guide

Copyright

Trademark

BIVOCOM logo is a registered trademark of Xiamen Bivocom Technologies Co., Ltd. All other trademarks belong to their respective vendors or manufactures.

Disclaimer

Product specifications and information in this document are subject to change without any notice, and BIVOCOM reserves the right to improve and change this user guide at any time. Users should take full responsibility for their application of products, and Xiamen Bivocom Technologies Co., Ltd. disclaims all warranties and liability for the accurateness, completeness of the information published.

Global Technical &Sales Support

Bivocom

Xiamen Bivocom Technologies Co., Ltd.
Addr: Unit 1402, No. C07 Building, 3rd Software Park, Xiamen, China 361000
Tel.: +86-592-6211770
Fax: +86-592-6211727
Email: support@bivocom.com
sales@bivocom.com
www.bivocom.com

About This Guide

Thank you for choosing Bivocom Industrial Cellular Router TR321 Series.

Please thoroughly read this user guide before you configure and install the device.

This manual is compatible with below models

Model	Description
TR321-W	Industrial WCDMA ROUTER
TR321-LF	Industrial LTE/WCDMA ROUTER
TR321-M	Industrial CAT-M & NBIoT ROUTER

Table of Contents

1. Introduction

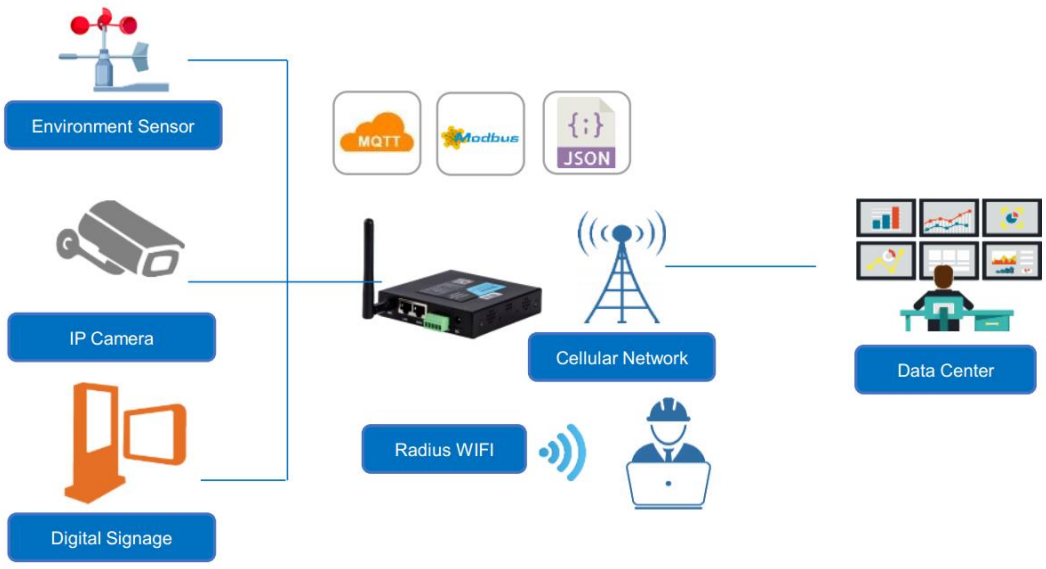
1.1 Overview

TR321 Series Router is a type of compact industrial wireless router, designed to fully meet the needs of industrial standards and industrial users. It adopts high-powered industrial 32-bits CPU, multi-layer software detection and hardware protection mechanism to ensure reliability and stability of the device. It supports worldwide carrier 4G/3G cellular network FDD-LTE, TD-LTE, and WCDMA, EVDO, TD-SCDMA, EDGE, CDMA 1X and GPRS, CAT-M, NBIoT. With rich VPN protocols(IPSEC、PPTP、L2TP etc.) to ensure the security of data transmission, and rich interfaces, such as RS232 (or RS485/RS422), Ethernet Port, and WIFI(Option), etc.

TR321 Series Router enables users to quickly access the Internet, to ensure secure and reliable data transmission. It's ideal for IOT (Internet of Things) and M2M(Machine to Machine) applications, and has been widely used in many applications, such as Intelligent Transportation, Smart Grid, Vending Machine, Agricultural Irrigation, Environmental Protection, Industrial Automation, Energy Saving, Smart Home, etc.

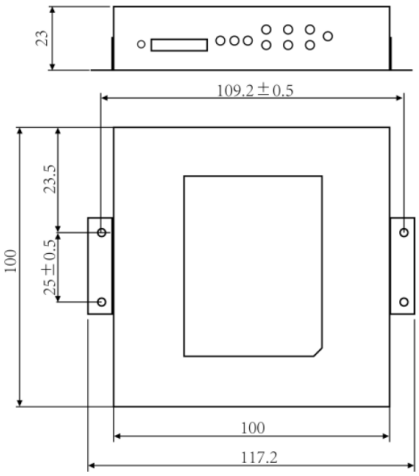
1.2 Applications

TR321 Series Router utilizes cellular network to connect your network devices and serial port devices to your center for remote monitoring and control.
Typical application as below.

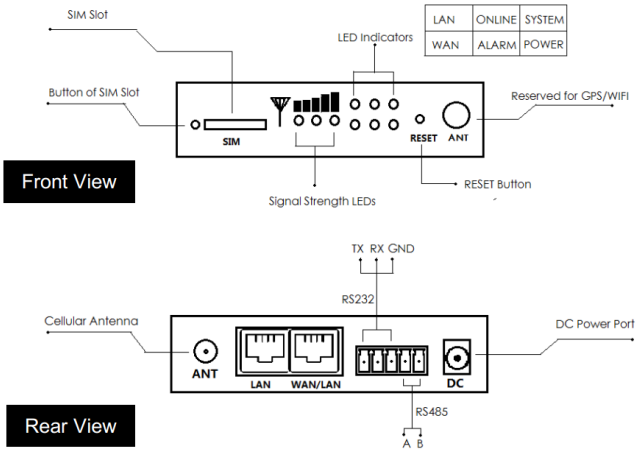


1.3 Dimensions

Dimensions(mm)



Side Views



1.4 Physical Characteristics

Physical Characteristics	
Housing	Metal, IP30
Dimensions	100x100x23mm(3.94x3.94x0.91 inches), Antenna and other accessories not included
Weight	320g(0.71lbs)

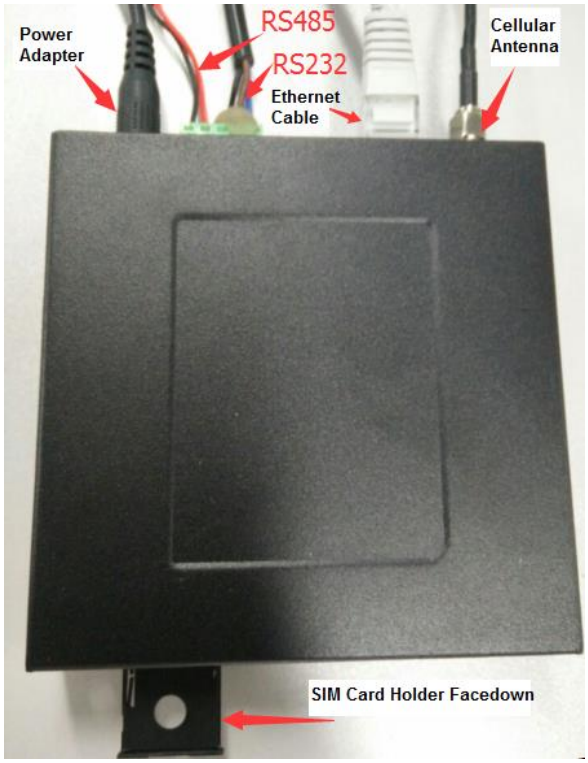
2. Getting Started

2.1 Package Checklist

The following components are included in your TR321 package.
Check the list before installation. If you find anything missing, Please feel free to contact Bivocom.

- TR321 Router Host
- Power Adapter(1.5A/12VDC)
- Cellular Antenna(Male SMA)
- Console Cable(RS232)
- Ethernet Cable(1 meter)
- 5-Pin Terminal Block

2.2 Installation



2.2.1 SIM/UIM Card

TR321 supports normal SIM/UIM only, so if you're using a Micro SIM or Nano SIM card, you may need to use a Micro SIM or Nano SIM to Normal SIM adapter.

Make sure your router is powered off, then use a needle object(such as a pen) to push the button near the SIM/UIM card holder, it will flick out immediately. Put the SIM/UIM card to card holder with chipset upside, insert it to router and make sure it's tightly matched.
Warning: Never install SIM/UIM card when router is powered on.

2.2.2 5-Pin Terminal Block and Console Cable

TR321 supports RS232 and RS485 serial port, which can be used for firmware upgrade, system log checking, or acts as serial port of a DTU(Please refer to Bivocom TD210 Series DTU).
TR321 designed with industrial terminal block interface, and the cable in this package with ends of female connector and stripping cable, the signal of console cable is defined as below,

RS232 Cable(with DB9 female connector and stripping cable)

Color of cable	Corresponding DB9-Female Pin No.	Corresponding Pin No. of Router (Pin 1 closes to power jack, Pin 5 closes to ethernet port)
Blue	2（RX）	1(TX)
Brown	3（TX）	2(RX)
Black	5（GND）	3(GND)

RS485 Cable

Color of cable	TR321 Router
Red	4(A)
Black	5(B)

2.2.3 Power Supply

We suggest you use Bivocom standard power adapter (1.5A/12VDC). If you have to use your own power supply, make sure the power range is 5-35VDC and it is stable enough(Ripple shall be less than 300mV, and Instantaneous voltage shall not larger than 35V), meanwhile, power shall over 4W.

2.2.4 Cellular Antenna

Screw the SMA male antenna to TR321(SMA female port), make sure it is screwed tightly to ensure the strength of signal.

2.3 LED Indicators

TR321 Series Router provides 7 LED indicators, as following.

Indicator	Status	Content
Power	On	Powered On
	Off	Powered Off
Signal Strength	1 Lights	Signal weak
	2 Lights	Signal Middium
	3 Lights	Signal Strong
System	Blink	System works perfect
	Off	System doesn't work
Online	On	Router accesses to Internet
	Off	Router doesn't access to Internet
Alarm	On	● SIM/UIM Card is not insert corectly or broken ● Antenna signal is too weak
	1 Blink Per Second	Cellular module was not registered to router
	2 Blinks Per Second	Router can't access to Internet
	Off	Router doesn't have any alarm
WAN	On	WAN is connected

	Off	WAN is not connected
LAN	Blink	LAN works
	Off	LAN is not connected

2.4 Reset

You can press the Reset button to reset settings to factory defaults to solve the problem of incorrect configuration that makes you couldn't access to internet, login and management, etc.
Use a needle object(such as pen) to insert into hole of 'Reset', hold until all the LED indicators turn off.

3. Configuration and Management

3.0 Getting start Web UI

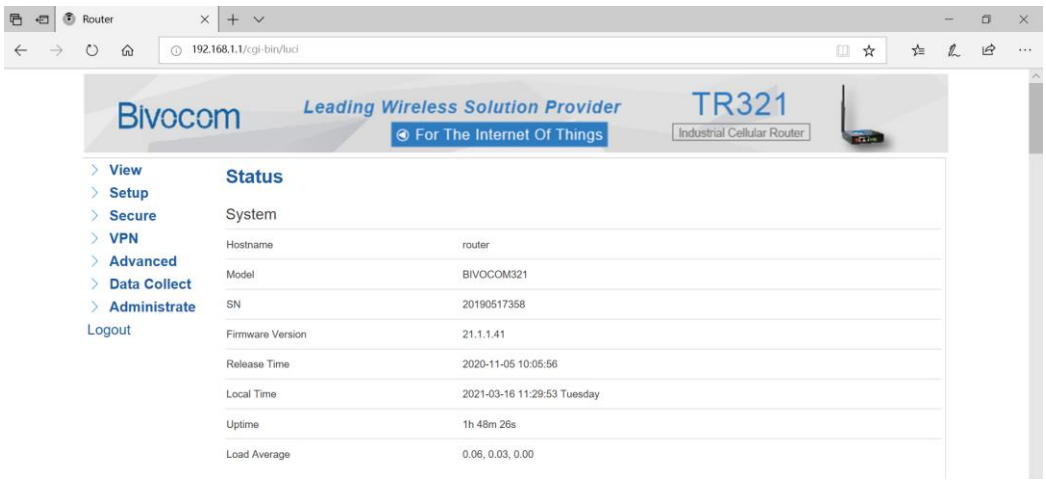
TR321 provide visible and easy-to-use WebUI for configuration setting and management. Below sections indicate each menu items feature introduce and setting on WebUI.

3.0.1 Connect your PC to TR321 network.

- Using an Ethernet cable, connect one end of the Ethernet cable to the LAN port on TR321 unit and the other end to a LAN port on a PC.
- Or use your laptop to connect to WIFI hotspot 'Bivocom_xxxx' from TR321, login with default password: "admin123".
- If your PC is configured to automatically get an IP address, it will obtain the IP address from the TR321 DHCP. Otherwise, make sure your PC can connect to the network 192.168.1.0 (255.255.255.0).

3.0.1 Login the WebUI

Enter 192.168.1.1 into the address bar of your PC web browser. Login with user name and password both "admin" as default. A web page with menu items will guide you start the configuration.

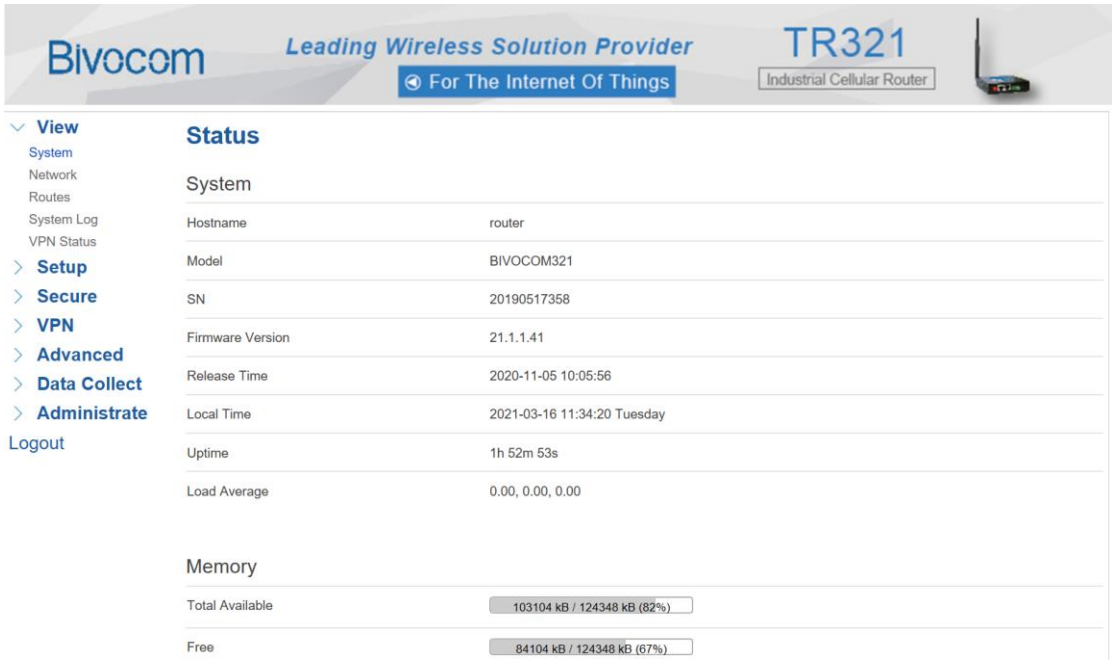


3.1 View

View page shows the basic system information including System, Network, Routes, System Log, VPN Status. Checking the following details information.

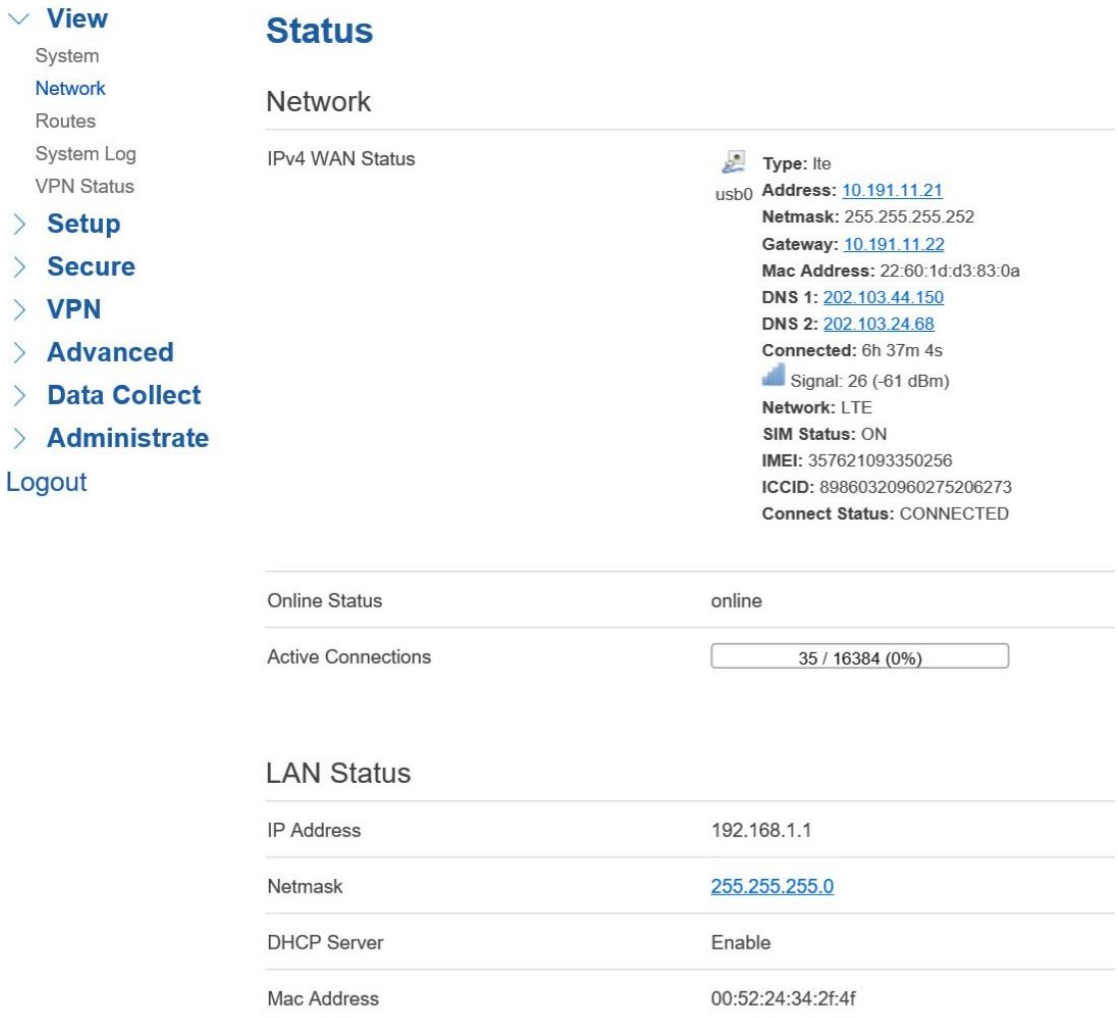
3.1.1 System

System page show you an overview of TR321 information like SN, Firmware version, Memory usage, etc.



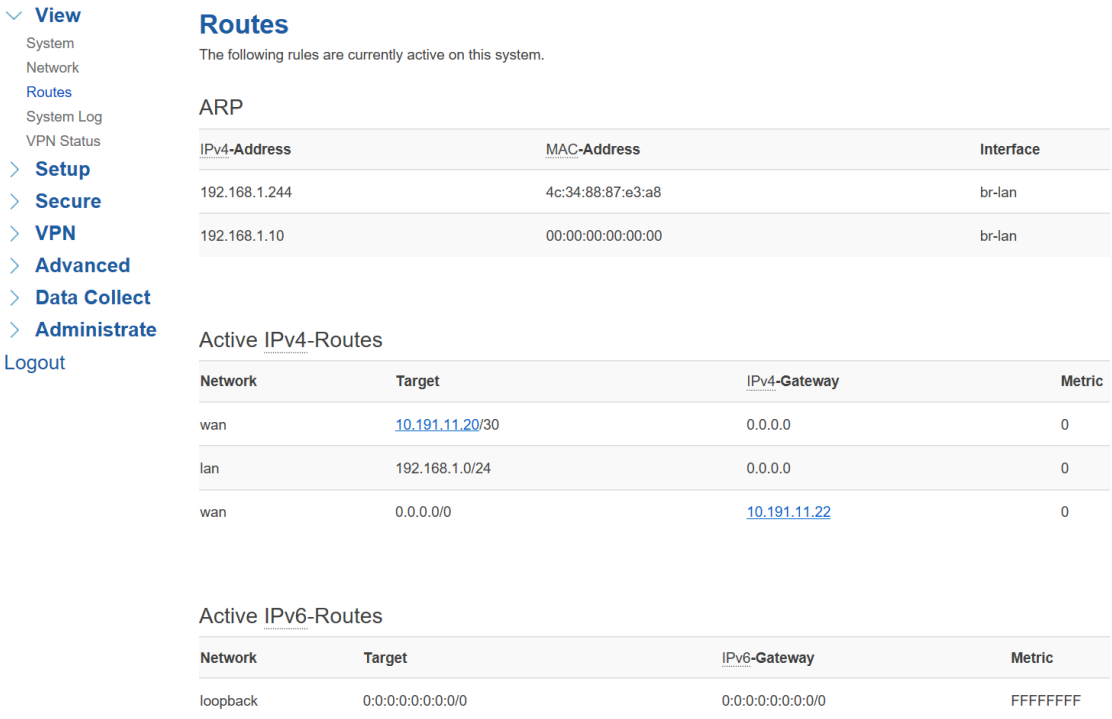
3.1.2 Network

Network page display the current WAN status, like network type, IP address, Connect Status, and so on. Also indicate the LAN Status, Wireless Status, DHCP Leases.



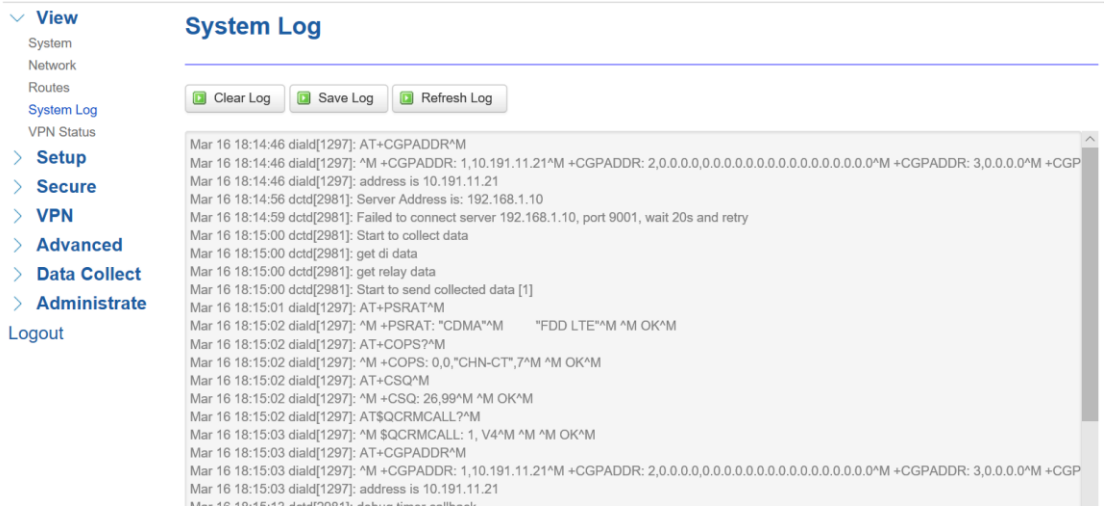
3.1.3 Routing Tables

Display ARP list and active routing tables.



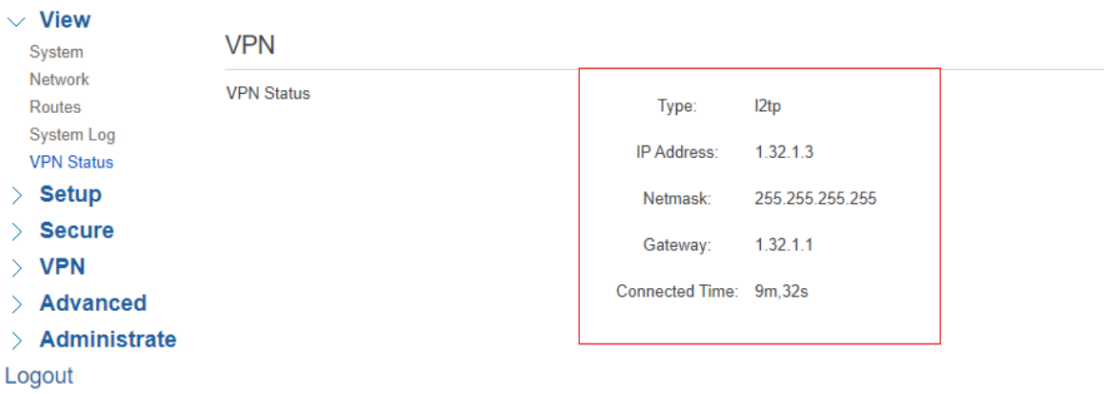
3.1.4 System Log

System log page continuous print the current running status syslog. It is useful for troubleshooting when there are some features working not as expected. System log page provide three buttons for “Clear Log” which empty current printed log, “Save Log” which saving current printed log as a file, and “Refresh Log” which asking print out latest log.



3.1.5 VPN Status

Display current VPN status. If you have setup a VPN connection, there will indicate the status, like VPN type, IP address, Connected Time, etc.



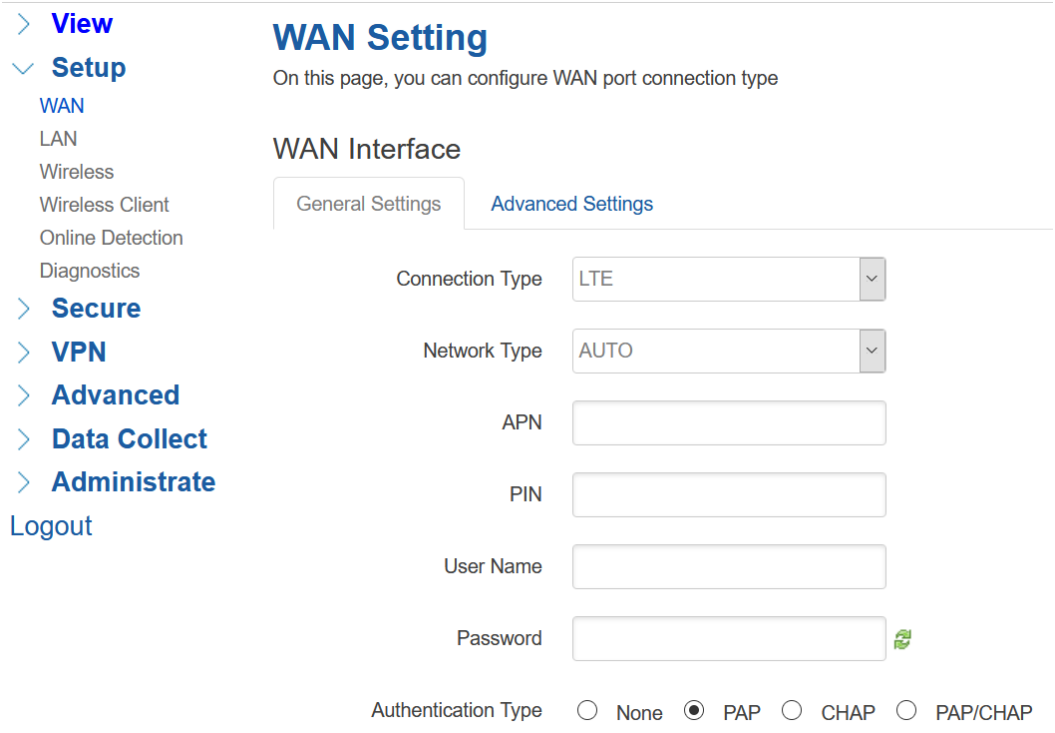
3.2 Setup

Setup page includes WAN, LAN, Wireless, Wireless Client, Online Detection, Diagnostics menus, which is for you configuring the features accordingly.

3.2.1 WAN

WAN Setting contains General Setup which provide configuration option for setting “Connection Type” and relevant items. It supports “Static IP”, “DHCP”, “PPPoE”, “3G”, “LTE”, “Unmanaged” connection types. While the default type is LTE.

- “Static IP” is for TR321 setting static IP address to connect to upper network via WAN port.
- “DHCP” is for TR321 obtain network from Upper DHCP device (like router) via WAN port.
- “PPPoE” is for getting network via PPPoE protocol, normally you will get username password from carrier when you purchase a network.
- “3G” is for dialing up 3G or NBIOT cellular network when using a 3G SIM card or a NBIOT SIM card. You may need input APN, PIN, PAC/CHAP Username Password if your SIM card provider request.
- “LTE” is for dialing up 4G/LTE cellular network when using a 4G SIM card. You may need input APN, PIN, PAC/CHAP Username Password if your SIM card provider request.
- “Unmanaged” is for disabling WAN connection.

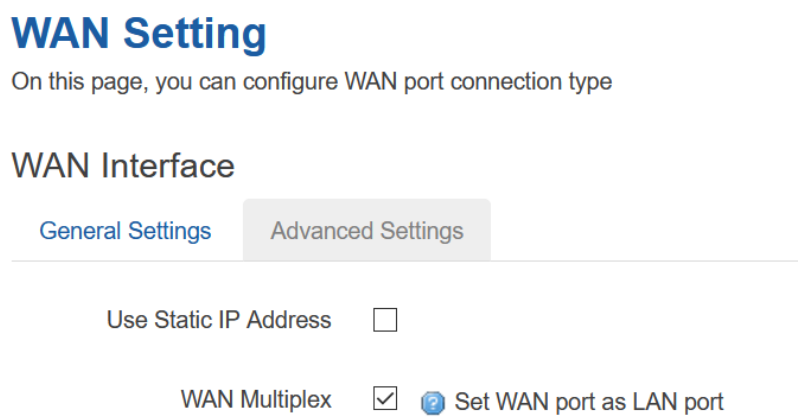


Note,

1) PAP/CHAP Username password Only when you are using a private network SIM card, if you're using public network SIM card, just keep it as null.
2) Choose Dial Number when you are using 3G type, different carriers may have different dial number, please ask your carrier for this info if you have questions.

3) WAN Used As LAN

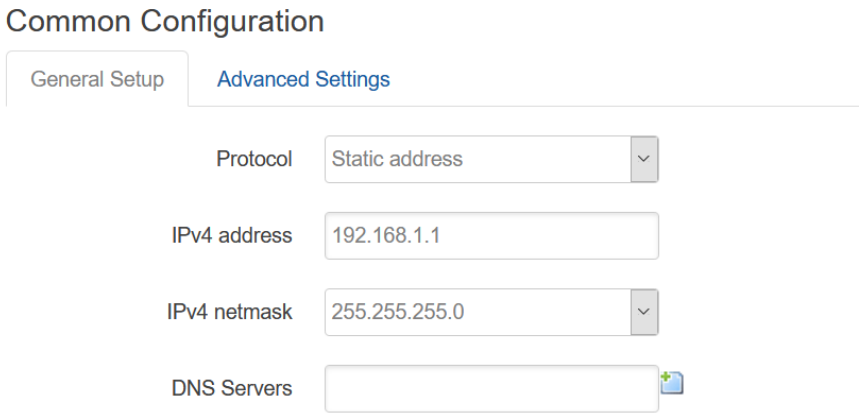
When using LTE/3G connection type to access internet, which mean WAN port is available for you change it as a LAN port.
"Advanced Settings" menu provide this option



3.2.2 LAN

Menu of LAN are mainly for configuring IP address of TR321, set the IP address range of DHCP server, or disable DHCP.

1) Common Configuration



IPv4 Address

To configure IP address of LAN port.

IPv4 Netmask

The netmask of LAN port IP address.

IPv4 Gateway

Specify the next-hop routing gateway.

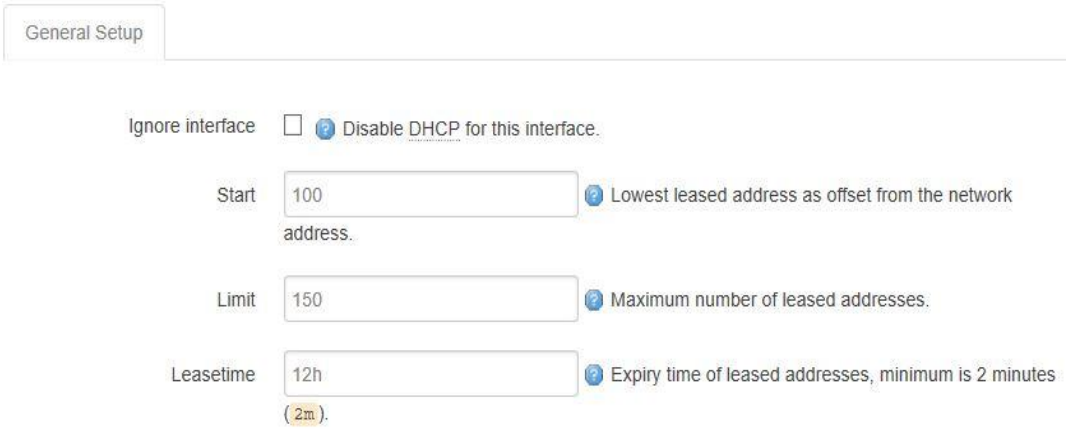
DNS Server

To specific DNS server, leave it blank as default using upper network DNS.

Advanced Settings

Specific set Override MTU, and use gateway metric. Leave it blank as default.

2) DHCP Server Settings



- **Disable DHCP**

Click to disable DHCP server.

- **Start**

Assign the IP address of DHCP server. For example, 100 means IP address starts from 192.168.1.100.

- **Limit**

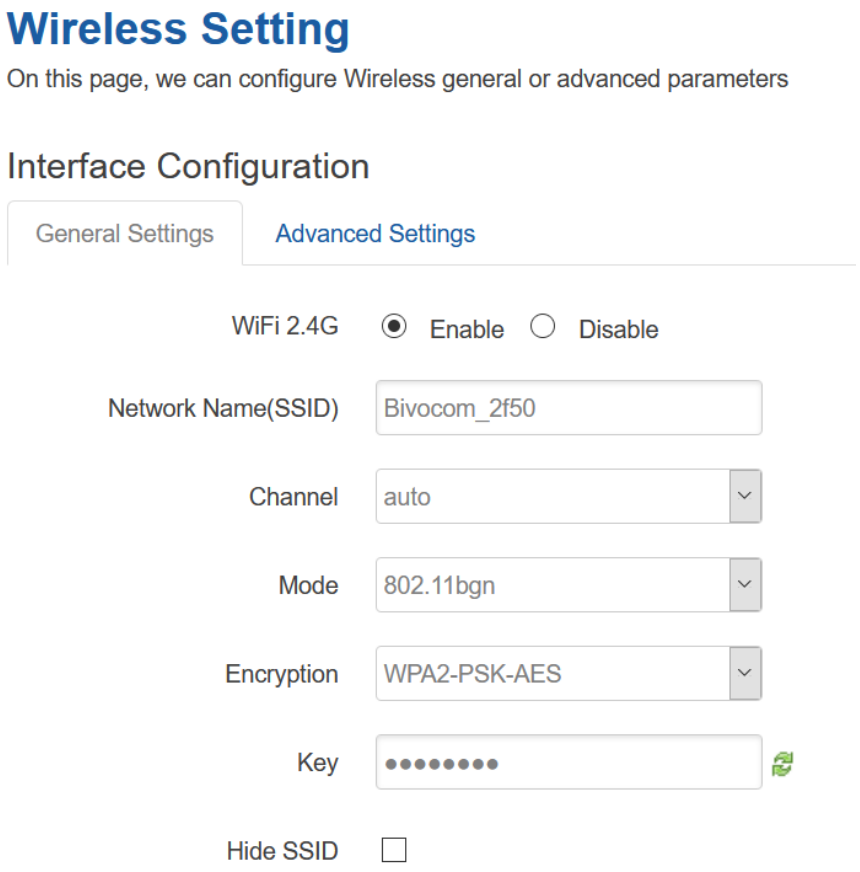
Assignable number of IP address, to ensure numbers of IP address of start and limit not exceed 250.

- **Lease time**

Time of assigning the IP address.

3.2.3 Wireless (Option)

Wireless menu is mainly for configuring the WiFi, SSID, mode, entryption, etc.



1) WIFI 2.4G

Provide Enable or Disable option for the WIFI function switch.

2) Network Name（SSID）

WIFI network name setting.

3) Channel

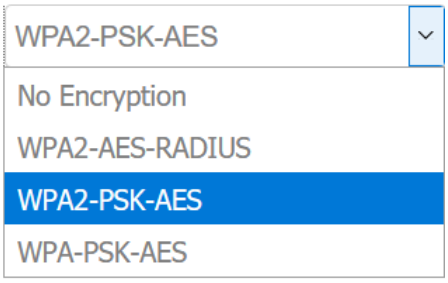
Support 1-13 channels or auto options, default value is auto, channel can be changed automatically.

4) Mode

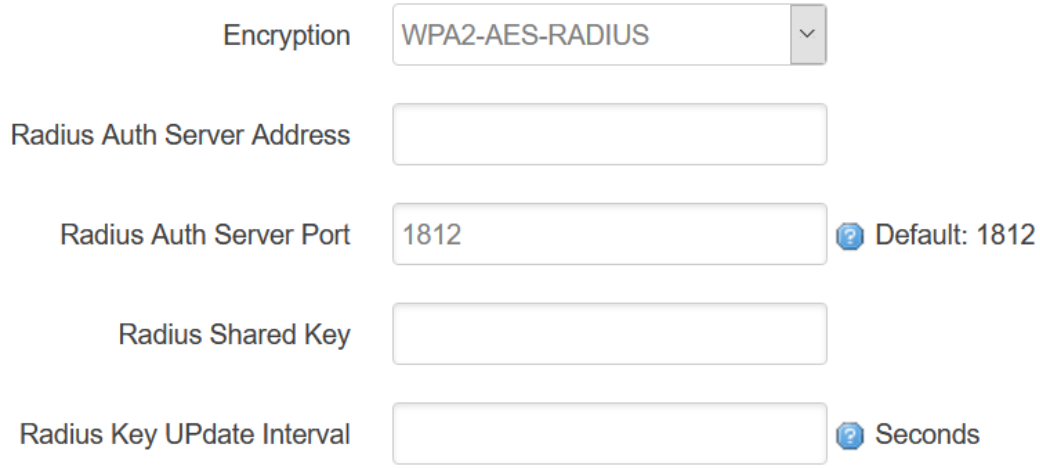
Support 802.11b, 802.11g, 802.11bg, 802.11bgn options. This may related to the maximum speed of WiFi. 802.11b up to 11Mbps, 802.11g up to 54Mbps and 802.11bgn up to 300Mbps.

5) Encryption

Configure the way of encryption,



While for RADIS option, it provide for configuring Radis Auth Server address, shared key, etc.



6) Key

Password of sharing the WIFI, user need to enter it to access the internet. The minimum length of password is 8 bytes.

7) Hide SSID

When Hide SSID enabled, SSID is invisible, and user need to enter the SSID to share the WIFI.

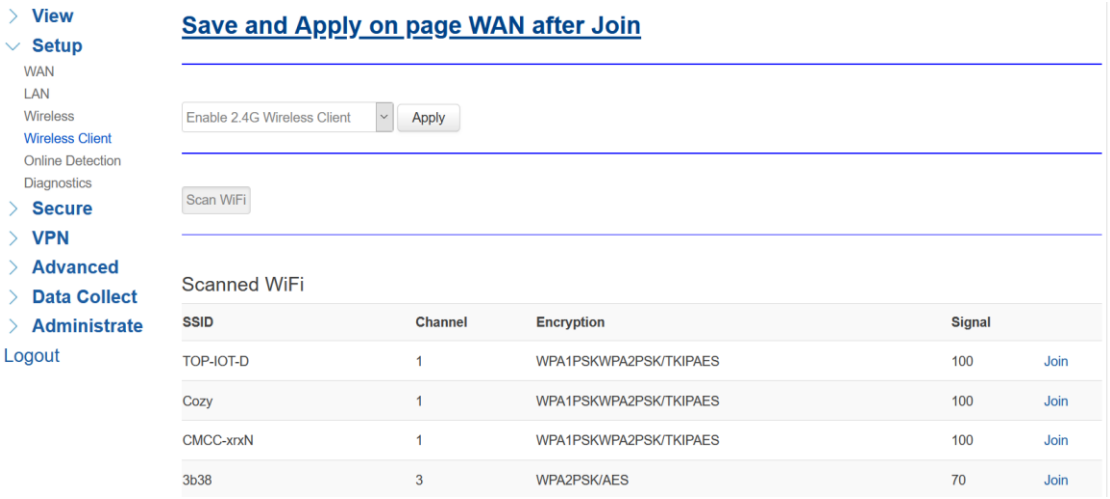
Advanced Settings related to some specific parameters setting, this is for professional users, contact Bivocom support team in case you have further questions.

3.2.4 Wireless Client

Wireless Client menu provide connecting network from local WiFi Hotspot, this setting

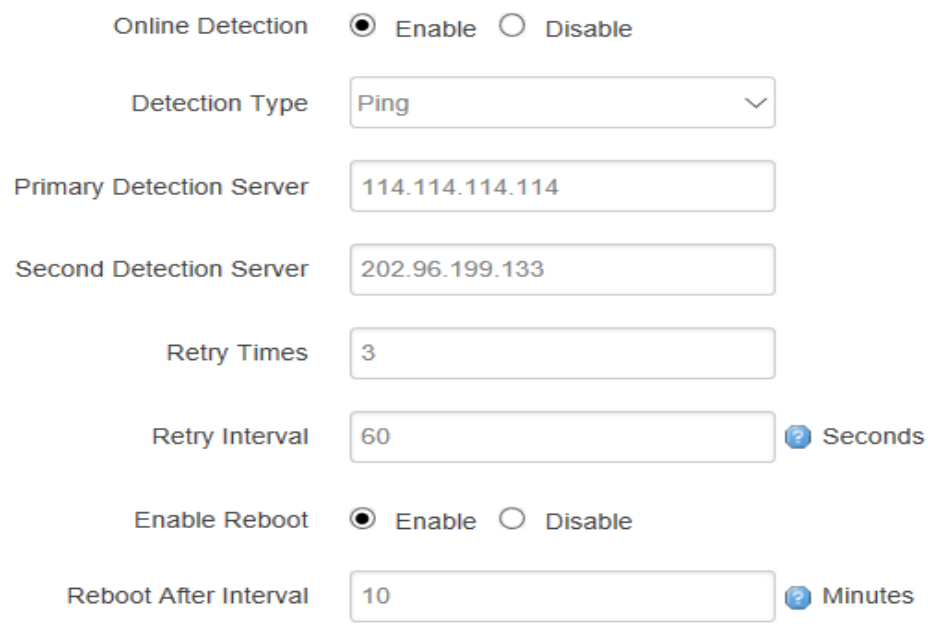
related to WAN setting when you select Static IP or DHCP connection type.

Enable wireless client and apply it, it will list all WiFi hotspots which can be detected. Join one of it, will ask you input the password if hotspot request.



3.2.5 Online Detection

Online detection feature checking the network connection status periodically, if there has issue of connection, router will auto reconnect. If it fails to reconnect after times of trial, router will reboot automatically to try to recovery the network.



1) Detection Type

There are 3 types: ping, traceroute and DNS.

- **Ping**

Router will ping an IP address periodically, if works, that means router is online.

- **Traceroute**

Traceroute will trace routing path, if achieves the target address, that means router is online.

- **DNS**

DNS will analytic a domain, if it works, that means router is online.

Note: the default setting is Ping, which is highly recommended, as traceroute will cost dataflow of SIM card, while DNS is faster, but as it has cache, it may shows the router is online even it is offline.

2) Primary Detection Server

It can be an IP address or a Domain Name.

3) Second Detection Server

If primary detection server fails, then router will auto switch to second detection server.

4) Retry Times

You can set up retry time in case detection fails.

5) Retry Interval

The interval time between 2 detection.

6) Enable Reboot

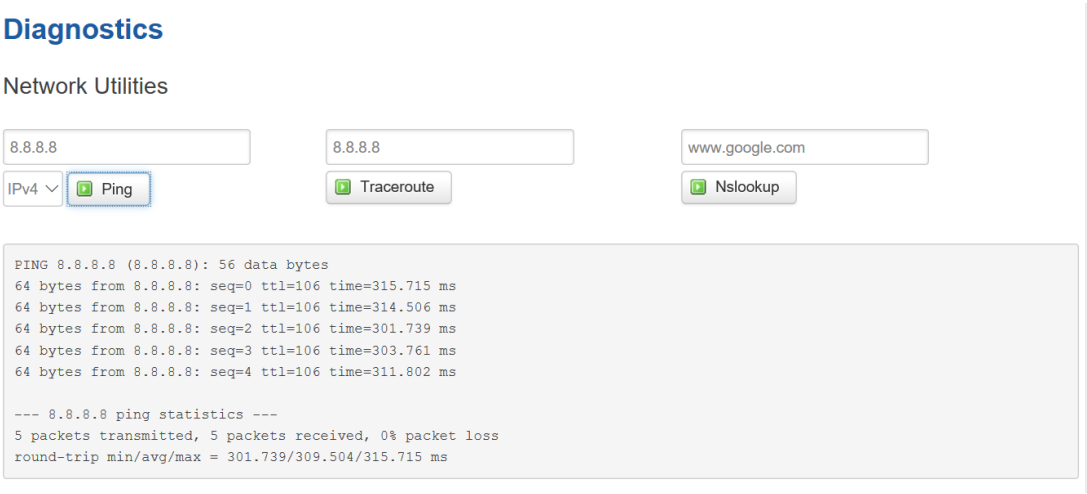
Click enable, and router will reboot within the time set if it fails to reconnect.

7) Reboot After Interval

You can specify the time for offline, to reboot the router.

3.2.6 Diagnostics

Diagnostics feature allow user check the network connection status manually.
There are 3 types of diagnostics: ping, traceroute and nslookup
Parameter of ping and traceroute can be a Domain Name or an IP address, used for checking if router is online or not. While nslookup is to analytic domain.



1) Ping

Click ping, then you can check if there is response from an IP address, as bellow.

2) Traceroute

Click traceroute, then you can see similar reponse as below.

3) Nslookup

Click nslookup, then you can see similar reponse as below.

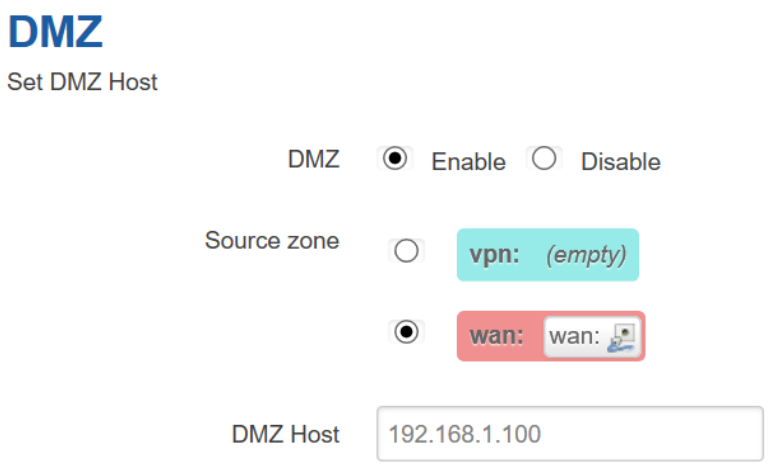
3.3 Security

Menu of Security are for configuring the firewall, to ensure the security of accessing to internet, and implement the port forwarding, access control, data packet filtering, and other functions.

3.3.1 DMZ Host

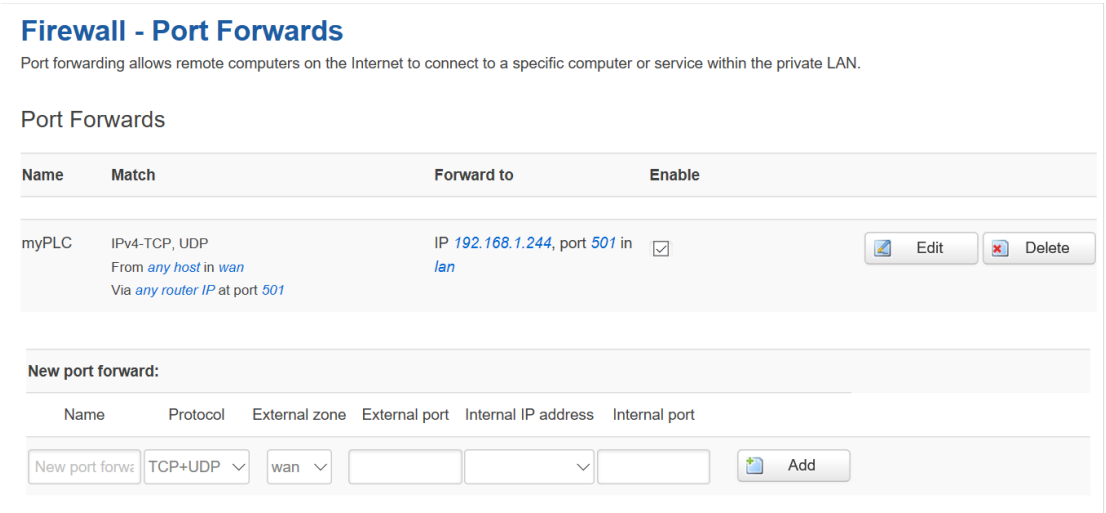
DMZ can forward the port of WAN to a host of LAN; all packet from WAN will be forwarded to specified host of LAN. It provide select source zone from VPN or WAN if there is a VPN

connection available.



3.3.2 Port Forwarding

Comparing with DMZ, Port Forwarding is for more precise control, user can forward the data packet of a port to a host of LAN, to forward different port to different host.



1) Name

You can name the rule you created.

2) Protocol

You can choose TCP, UDP, or TCP/UDP.

3) External Port

Destination port before port forwarding.

4) Internal IP Address

The Host IP address to forward.

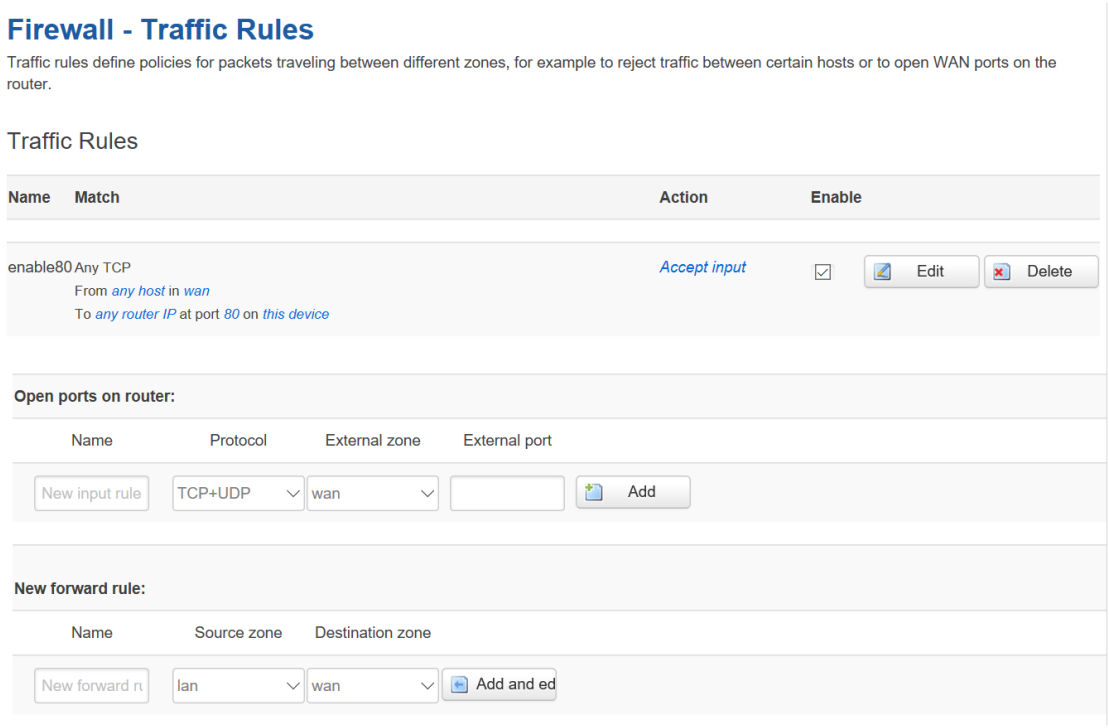
5) Internal Port

The destination port after port forwarding. Normally, external port and internal port are the same, but also can be different.

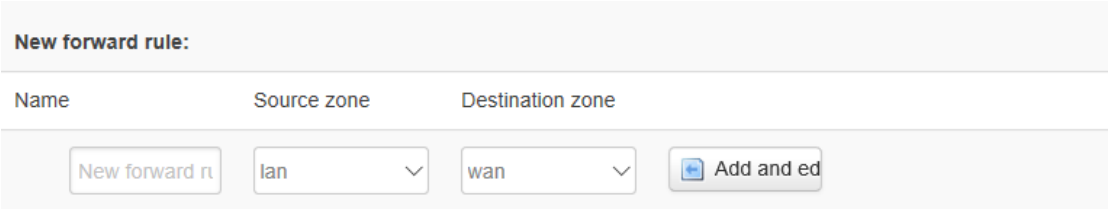
After configured above-mentioned, click ‘Add’, then a new rule will be added, and click ‘Save & Apply’, to have the rule take effect. There are more setting items when click “Edit” button.

3.3.3 Traffic Rules

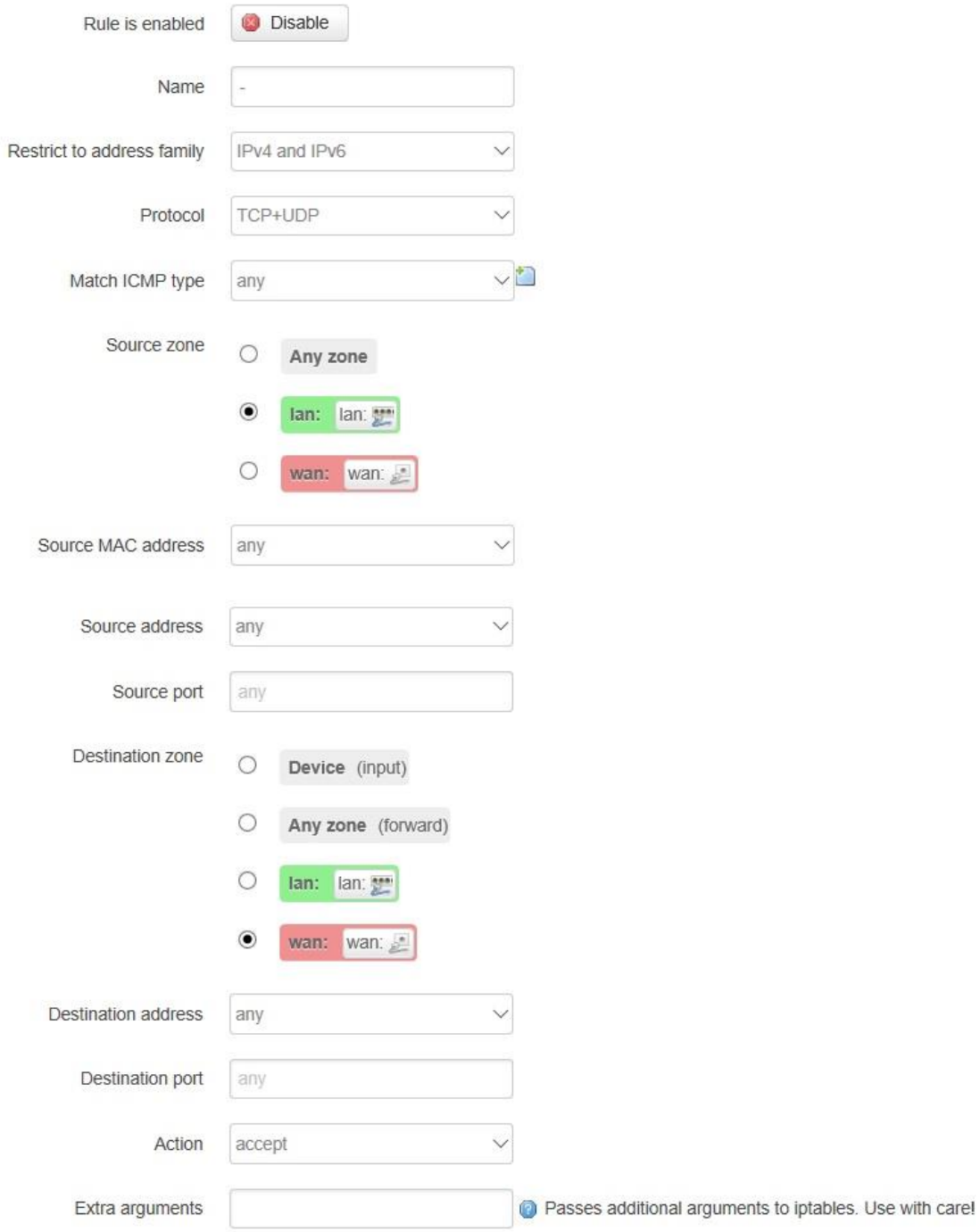
Traffic rules is used for Firewall setting like opening some ports on router, such as remote access the configuration page of router, you can open port 80.



In addition, traffic rule can be used for creating some access control rules, it can be from LAN to WAN, or WAN to LAN.



Click ‘Add and Edit’, then you can get more detailed matching condition.



1) Restrict to Address Family

You can choose IPv4, IPv6, or Pv4/IPv6.

2) Protocol

To choose the protocol you want for access control, it can TCP, UDP or TCP/UDP.

3) Source MAC Address

To choose the source MAC address of data packet.

4) Source Address

To choose the source IP address of data packet.

5) Source Port

To choose the source port of data packet.

6) Destination Address

To choose the destination IP address of data packet.

7) Destination Port

To choose the destination port of data packet.

8) Action

If the above-mentioned conditions matched, then you can choose below actions.

- **Accept**

  Allow data packet to go through.

- **Drop**

  Drop data packet

- **Reject**

  Drop data packet, and return an unachievable data packet.

- **Don’t Track**

  No action.

3.3.4 Custom Settings

Users can also customize some firewall rules themselves, as those rules is consist of iptable, we suggest only professional users who are familiar with iptables command to do this. When you add rules, please add them at the bottom of existing rules, and don’t delete them.

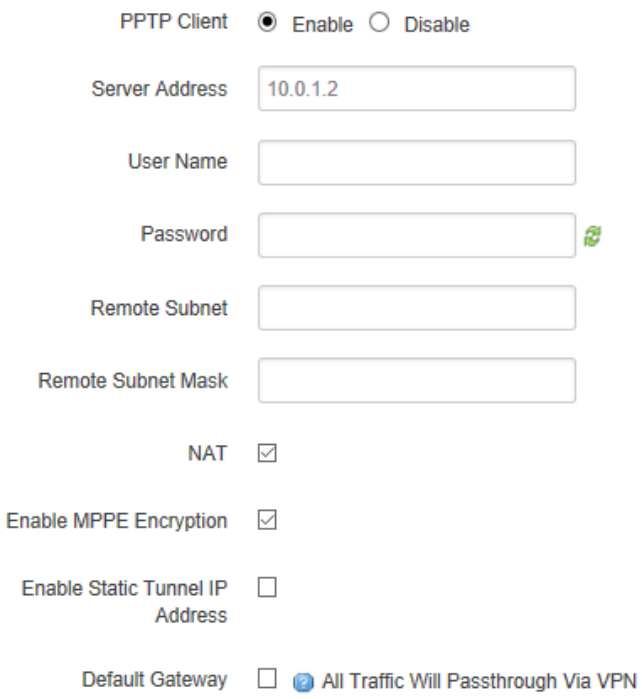
3.4 VPN

VPN is used to establish a virtual private channel, and all the data in this channel will be encrypted to ensure that data security during transmission.
TR321 support several types of VPN: PPTP, L2TP, IPSec, OpenVPN and GRE.

3.4.1 PPTP

You can configure either PPTP client or PPTP server, but it can’t use both of them at the same time, that may cause uncertain issues.

1) PPTP Client



1. PPTP Client

You can enable or disable PPTP client.

2. Server Address

To enter the IP address or Domain Name of PPTP server.

3. User Name and Password

To enter the user name and password provided by server.

4. Remote Subnet

To enter the remote subnet, for example, if LAN of PPTP server is 192.168.2.1, then you can enter remote subnet 192.168.2.0.

5. Remote Subnet Mark

To enter the remote subnet mask, normally it is 255.255.255.0.

6. NAT

If click NAT, all packets come from ppp0, and the source IP of the packets will be replaced as IP of ppp0.

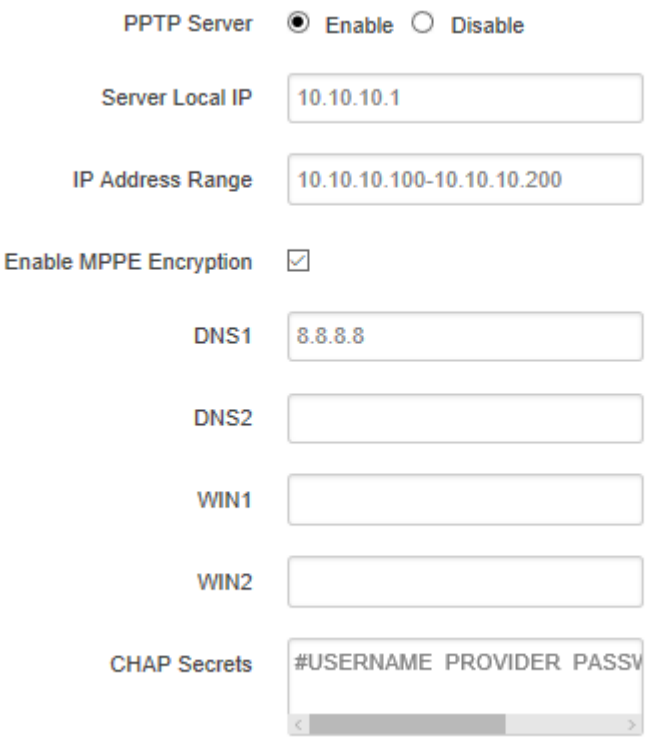
7. Enable MPPE Encryption.

You can enable MPPE encryption here.

8. Default Gateway

Click Default Gateway, then a default route will be established under ppp0, and all the data will go through this route.

2) PPTP Server



1. PPTP Server

You can enable or disable PPTP server.

2. Server Local IP

To enter the server local IP address.

3. IP Address Range

Type the range of assigned IP address.

4. Enable MPPE Encryption.

You can enable MPPE encryption here.

5. DNS1/DNS2

To enter the assigned DNS address.

6. WIN1/WIN2

To enter the WIN address.

7. CHAP Secrets

To create an username and password under CHAP Secrets, format as below,

Username<space>*<space>password<space>*

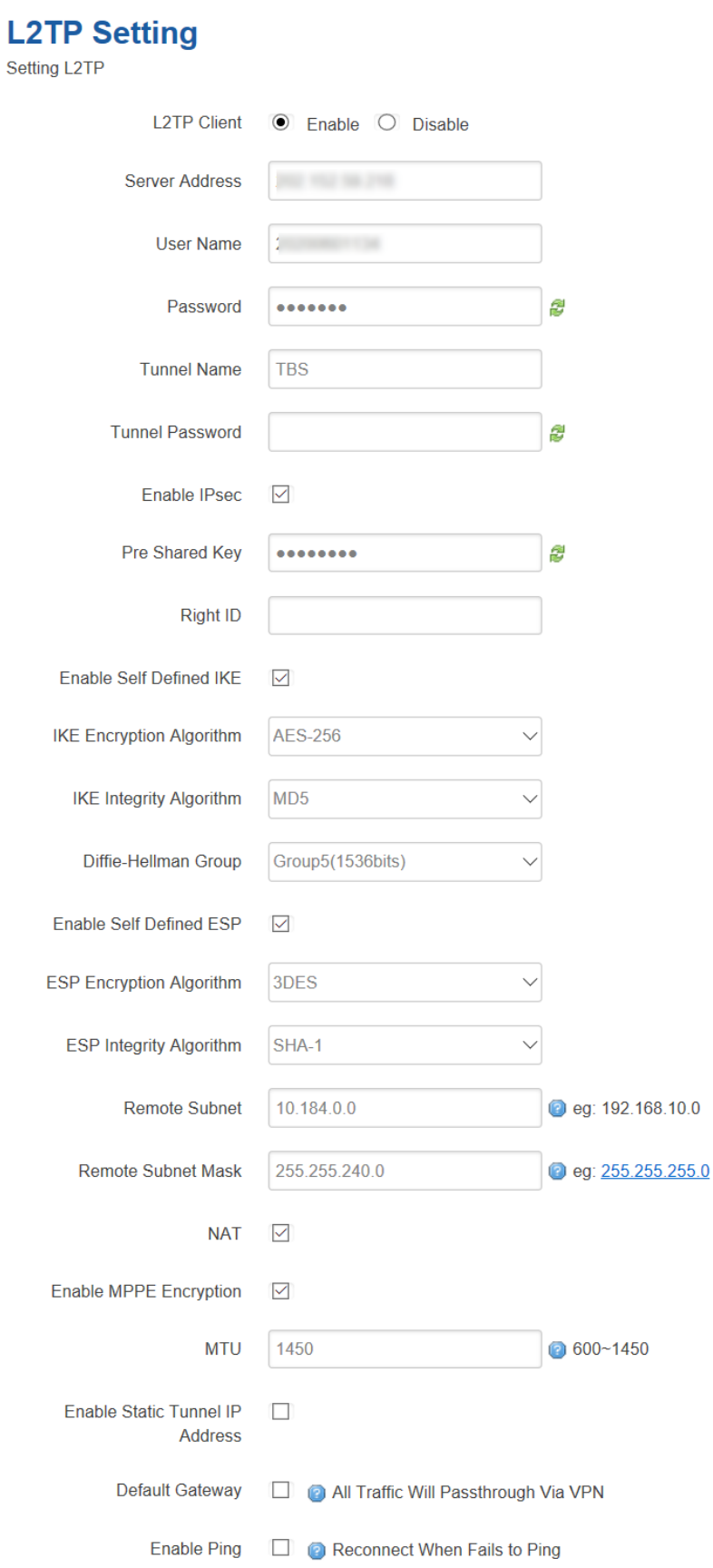
For example, if you want to create a username: test, password: test, it is as below,

Test * testing *

3.4.2 L2TP

You can also configure either L2TP client or L2TP server, but not both of them at the same time, as that may cause uncertain issues.

1) L2TP Client



1. **L2TP Client**

You can enable or disable L2TP client.

2. **Server Address**

To enter the IP address or Domain Name of L2TP server.

3. **User Name and Password**

To enter the user name and password provided by server.

4. **Remote Subnet**

To enter the remote subnet, for example, if LAN of L2TP server is 192.168.2.1, then you can enter remote subnet 192.168.2.0.

5. **Remote Subnet Mark**

To enter the remote subnet mask, normally it is 255.255.255.0.

6. **NAT**

If click NAT, all packets come from ppp0, and the source IP of the packets will be replaced as IP of ppp0.

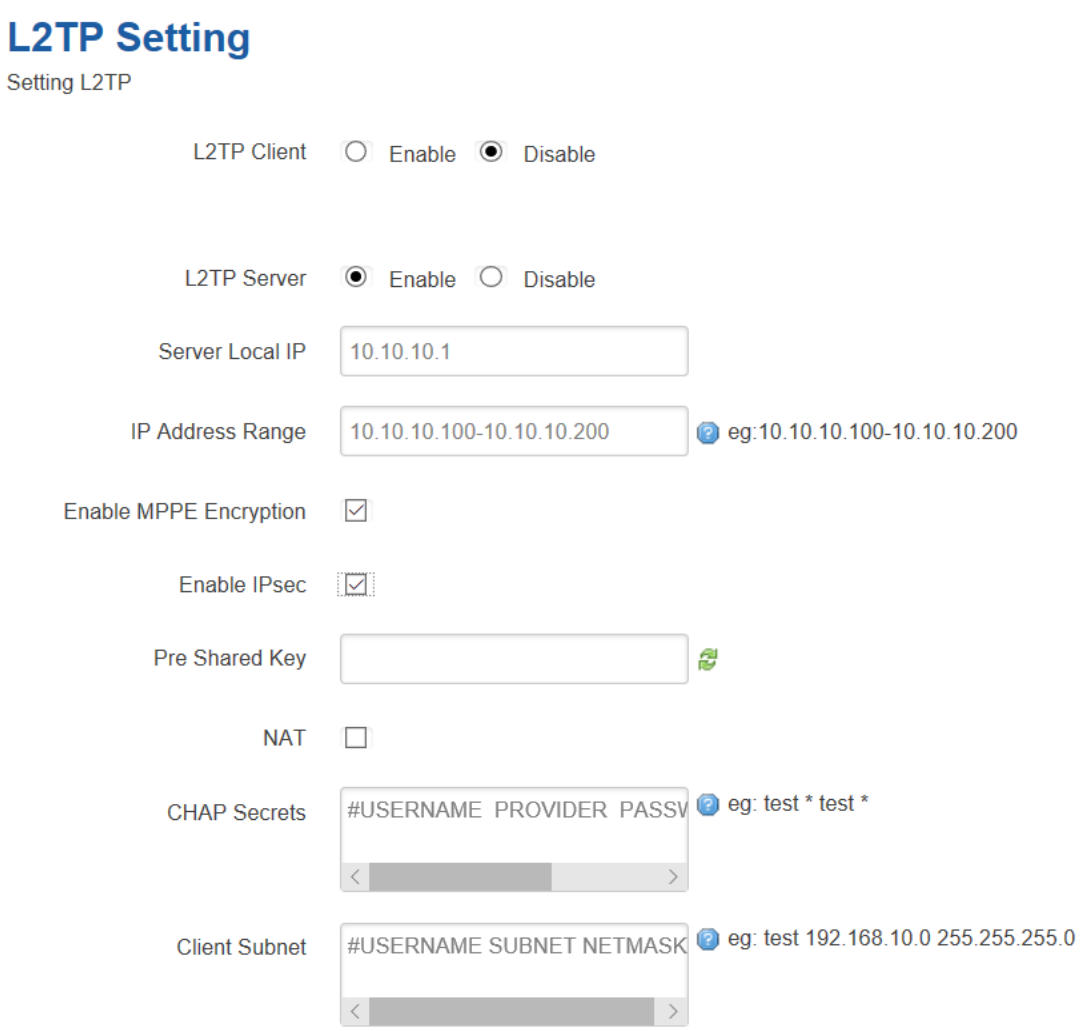
7. **Enable MPPE Encryption.**

You can enable MPPE encryption here.

8. **Default Gateway**

Click Default Gateway, then a default route will be established under ppp0, and all the data will go through this route.

2) L2TP Server



1. L2TP Server

You can enable or disable L2TP server.

2. Server Local IP

To enter the server local IP address.

3. IP Address Range

Type the range of assigned IP address.

4. Enable MPPE Encryption.

You can enable MPPE encryption here.

5. CHAP Secrets

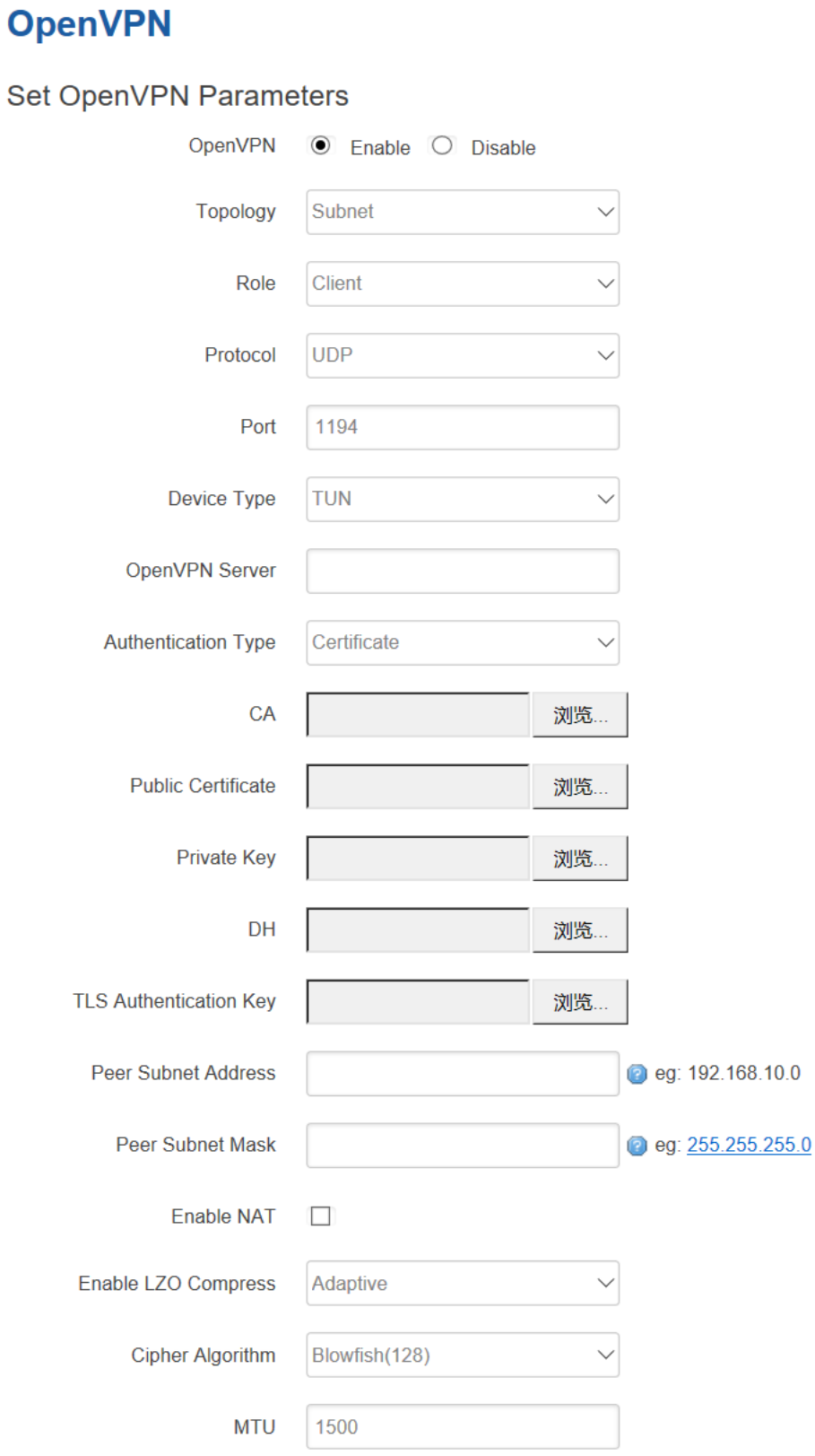
To create an username and password under CHAP Secrets, format as below,

Username<space>*<space>password<space>*

For example, if you want to create a username: test, password: test, it is as below,

Test * test *

3.4.3 OpenVPN



1) **OpenVPN**

You can enable or disable OpenVPN.

2) Topology

Choose the topology, it can be point to point or subnet

Note: For point to point, a tunnel will be established between 2 devices.

While for subnet, multi devices will be connected to one server.

3) Role

When topology is subnet, you need to choose you want it be a server or client.

4) Protocol

Choose the protocol, it can be UDP or TCP, default is UDP.

5) Port

Enter the port you want to assign to OpenVPN, default port is 1194.

6) Device Type

Choose device type, there are 2 types to choose, TUN and TAP. TUN is layer 3 data encapsulation, while TAP is layer 2 data encapsulation.

7) OpenVPN Server

When you choose server in 角色, you need to enter an IP address or domain name of server.

8) Authentication Type

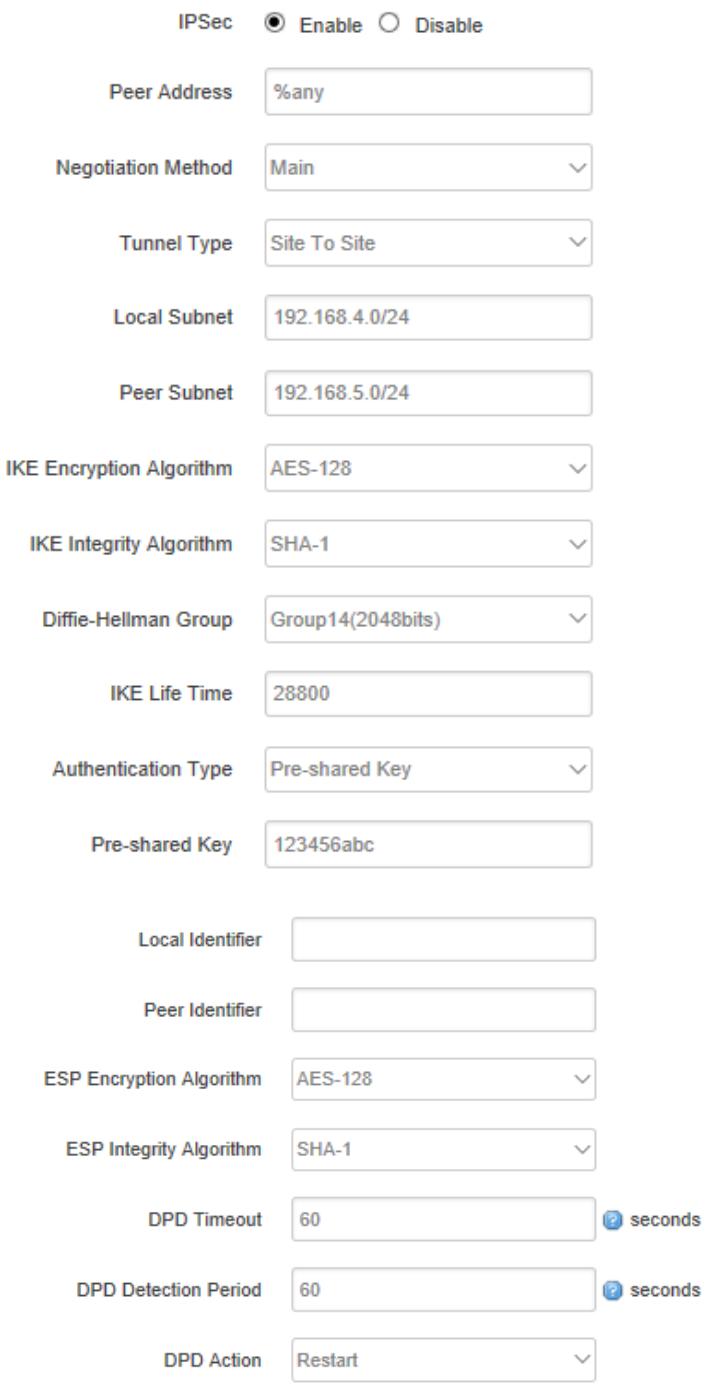
If topology is subnet, authentication type is certification. If it is point to point, you can choose none, certificate or static secret.

9) TLS Role

When topology is point to point, and authentication type is certification, you need to choose if it is server or client.

3.4.4 IPSec

On IPSEC page, system will display the IPSEC connection and status.



1) Peer Address

To enter peer IP address or Domain Name, if choose as a server, you don't need to enter it.

2) Negotiation Method

You can choose 'Main' or 'Aggressive'.

3) Tunnel Type

You can choose 'Site to Site, 'Site to Host', 'Host to Host', 'Host to Site'.

4) Local Subnet

Local subnet and mask, like 192.168.10.0/24.

5) Peer Subnet

Peer subnet and mask, like 192.168.20.0/24.

6) IKE Encryption Algorithm

IKE phase encryption method

7) IKE Lifetime

To set up IKE lifttime.

8) Local Identifier

Local identifier of channel, can be an IP address or domain name.

9) Peer Identifier

Peer identifier of channel, can be an IP address or domain name.

10) ESP Encryption Algorithm

The encryption method of ESP.

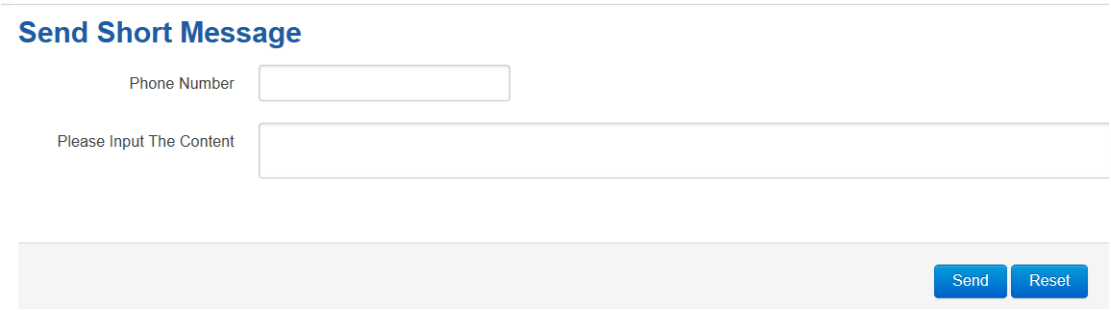
3.4.5 GRE

3.5 Advanced

Advanced menu include some advanced functions for your usage, like send SMS, traffic monitor, GPS location, SNMP, etc.

3.5.1 Send SMS

TR321 provide window for sending out Short Message to certain numbers with configurable content.



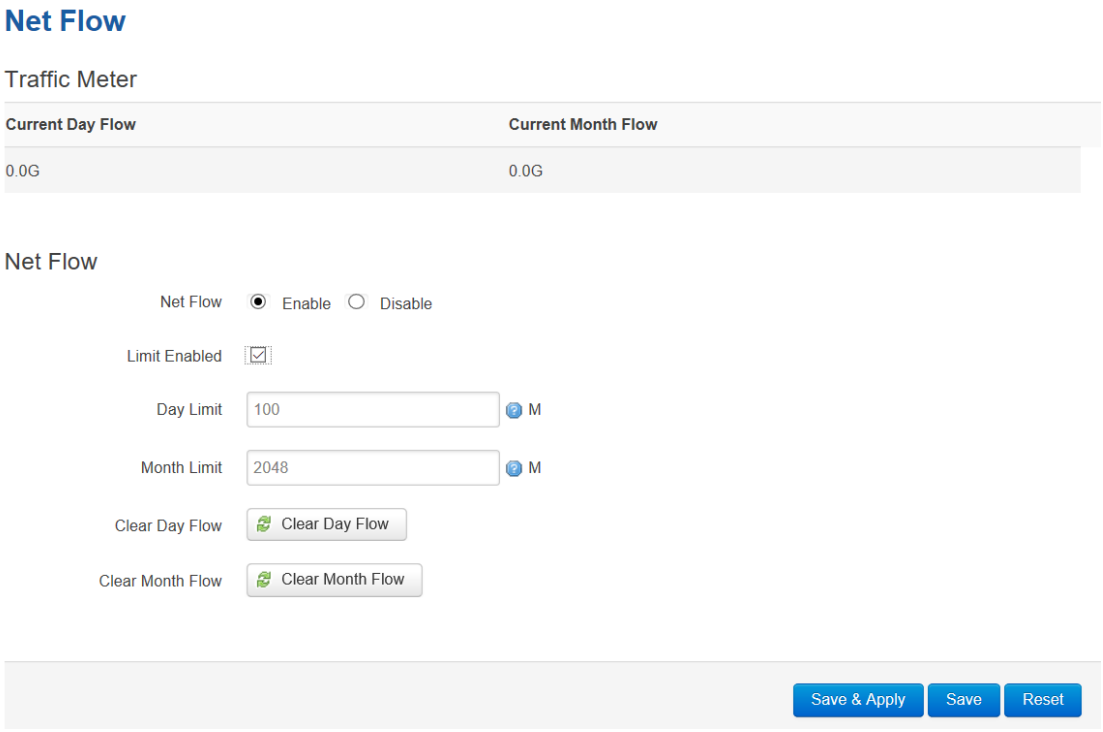
3.5.2 Static Routing

Static routing is used to add a routing table entry.

Interface: To choose which interface you want to add routing.
Target: Can be a host IP, or subnet.
IPv4 Netmask: The netmask of subnet, if the target is host, the netmask shall be 255.255.255.255.
IPv4 Gateway: The address of next-hop gateway address.
Note: this address shall be achievable, or you'll fail to add static routing.

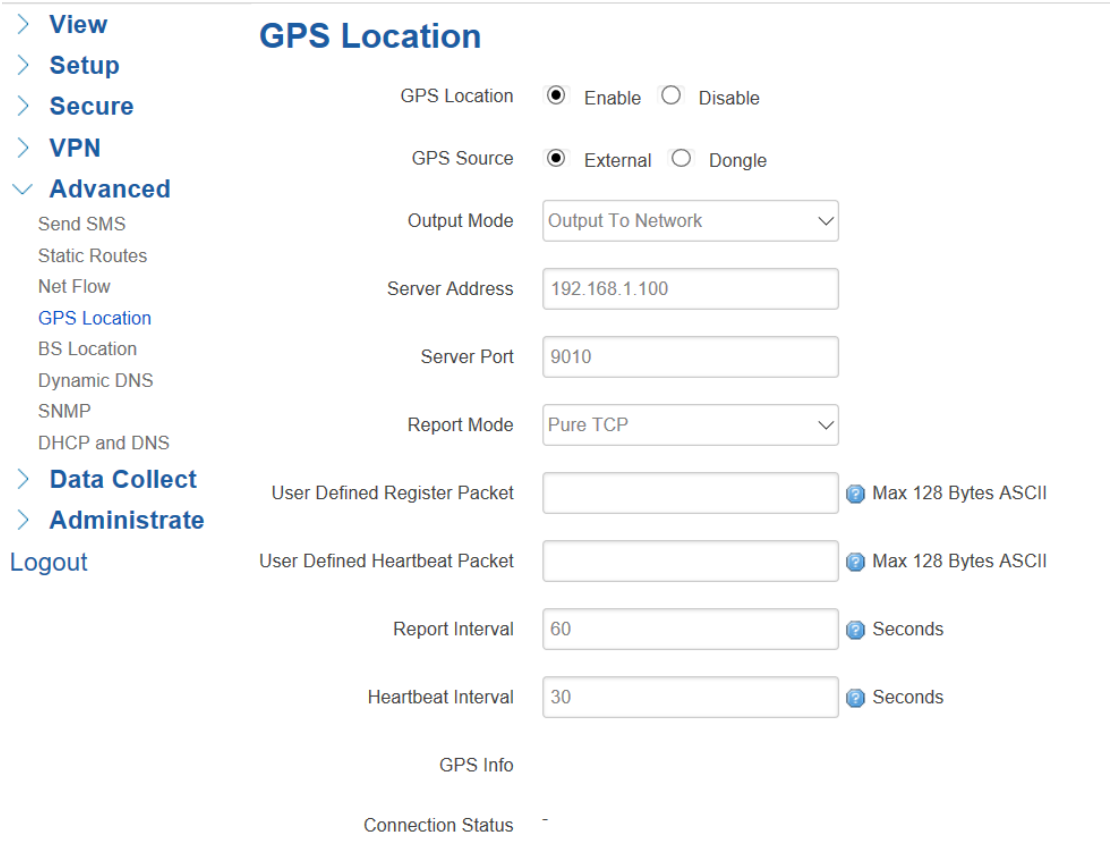
3.5.3 Net Flow

The traffic meter function of TR321 is for traffic statistics from WAN port, meanwhile, it has traffic overflow alarm function. Even if the router is powered off, the traffic statistics will be saved, and when you power on the router, the traffic will be counted based on your last time traffic.



3.5.4 GPS Location (Option)

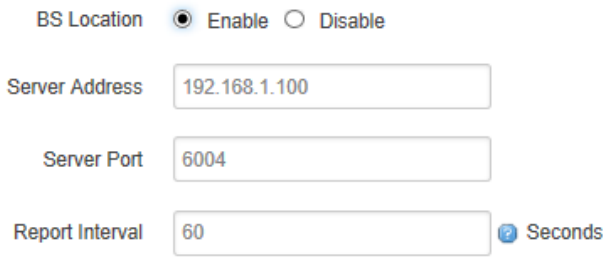
GPS location will report GPRMV information regularly, saying longitude and latitude information. And this function is used for accurate location of outdoor open area.



GPS Source: External for getting GPS data from independent GPS module (Option), while Dongle for getting GPS data from cellular module which base on Station location.
Output Mode: Output to network, or output to serial which through RS232 port.
Server Address: The IP address of server that receive GPS data if the output mode as “Output to Network”, which is based on TCP or UDP connection.
Server Port: The port of server.
Report Interval: The interval time for auto report of router location, default value is 60 seconds.

3.5.5 BS Location (Option)

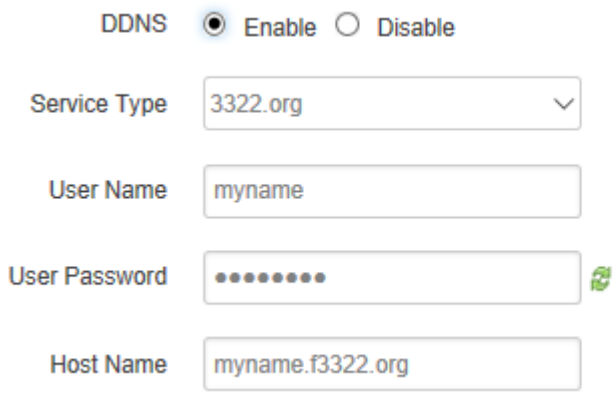
Base station location is to locate the TR321 by obtaining the nearest base station number, this function is mainly for rough location of indoor application.
Enter the server IP address and port that you want to report the location of router, then router will auto report its location to server regularly(within the interval time you set).



Server Address: The IP address of server that you want the router to report the location, which is based on TCP connection.
Server Port: The port of server.
Report Interval: The interval time for auto report of router location, default value is 60 seconds.

3.5.6 Dynamic DNS

If the assigned public IP address of router is dynamic and changes frequently, you can enable DDNS function, while allows you to register a domain to bundle with the IP address, in this case, no matter what the IP address changed, it will direct to your registered domain.



- **Service Type**

There are several types of DDNS service supported in router, as below.

- **User Name**

The username you register at DDNS service provider.

- **User Password**

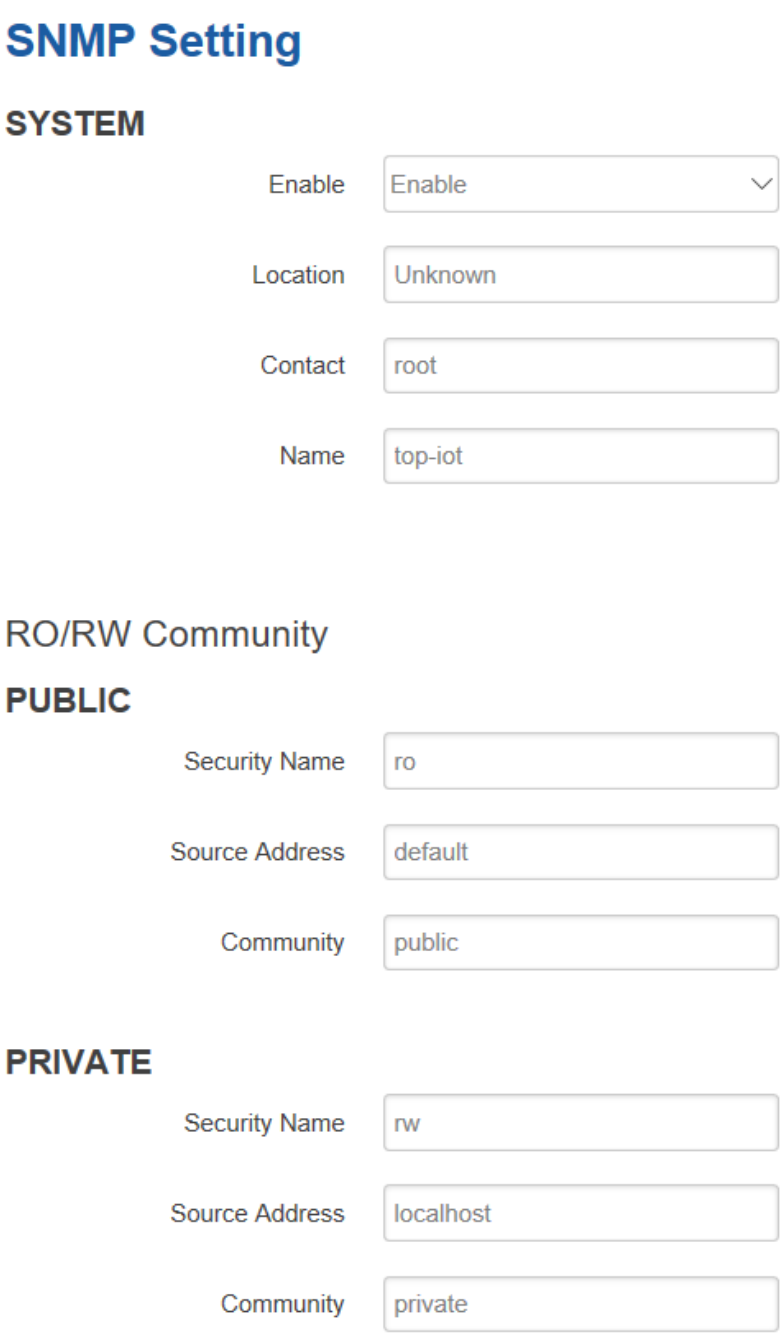
The password you set up when registering the user name at DDNS service provider.

- **Host Name**

The register domain you want to bundle.

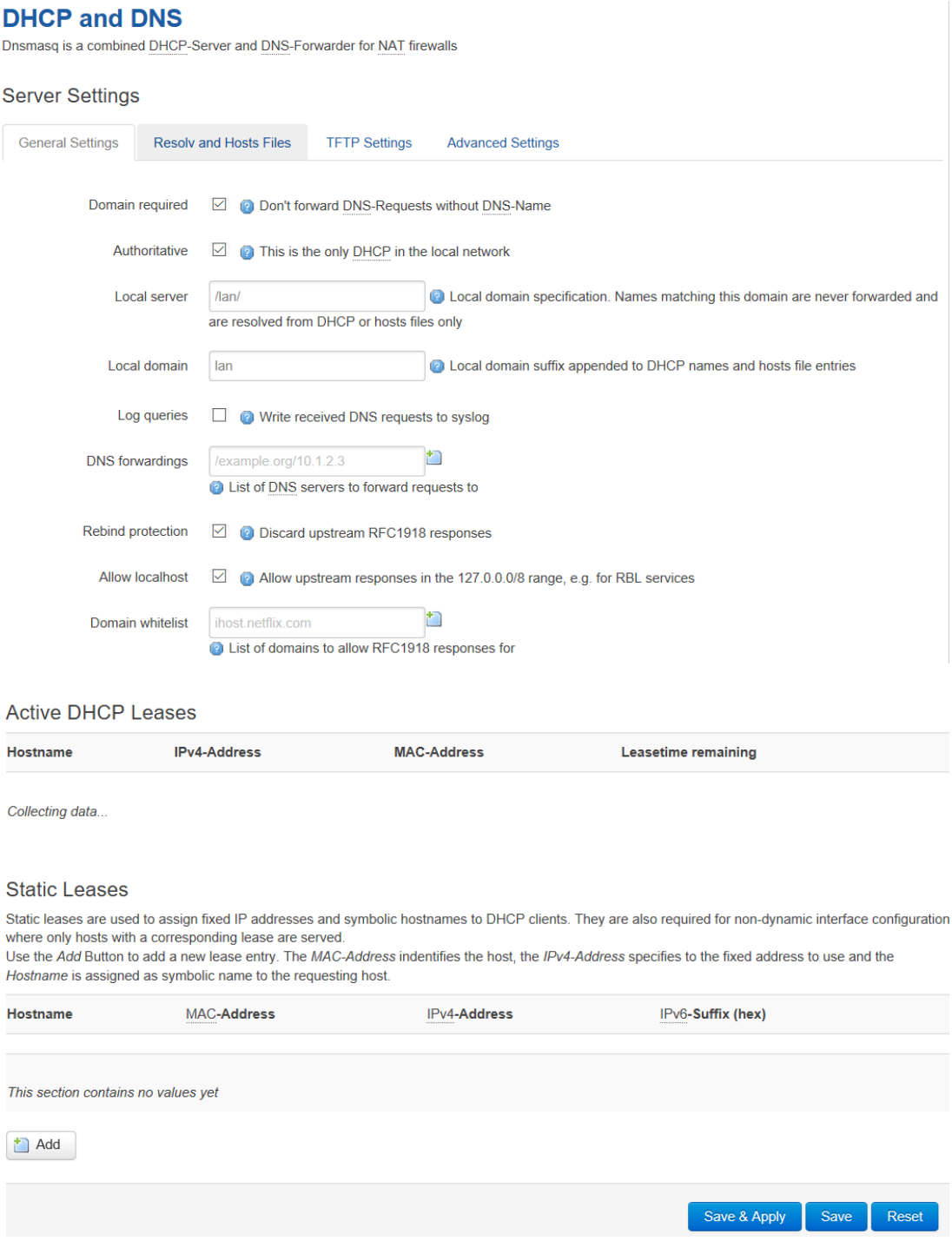
3.4.6 SNMP

TR321 router provide SNMP feature for manage the device via SNMP. Configure the relevant settings accordingly.



3.5.7 DHCP and DNS

TR321 provide DHCP and DNS setting via Dnsmasq package, it support configure DHCP server related settings and DNS forwarding setting if your network request specific parameters. Also support set static Leases. Normally leave it as default.

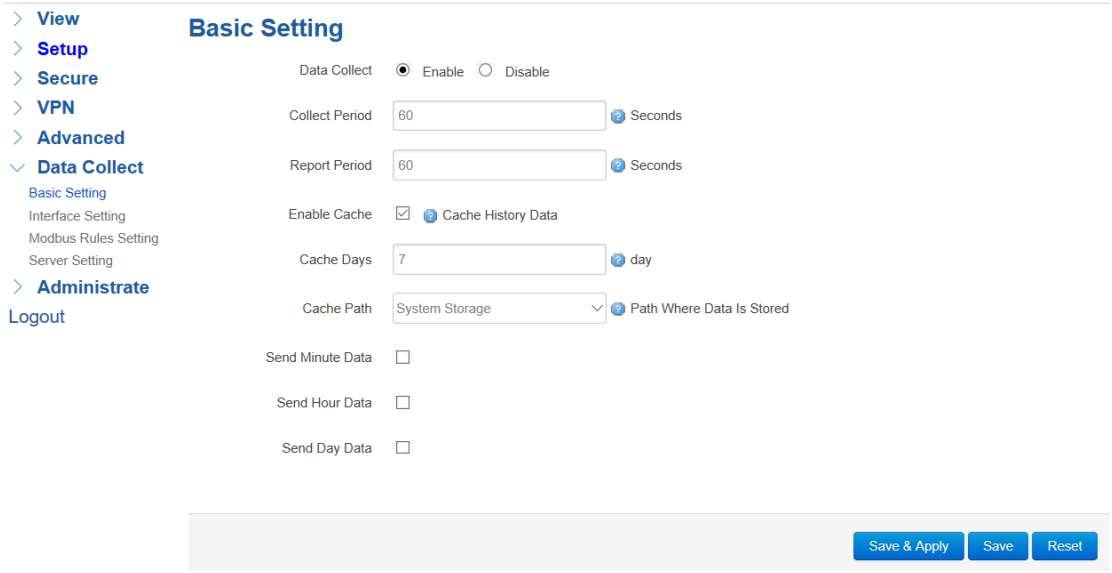


3.6 Data Collect

Data Collect settings is for TR321 acquiring data from slave devices in serial ports, Ethernet ports, with Modbus protocol and other customized protocols.

3.6.1 Basic Setting

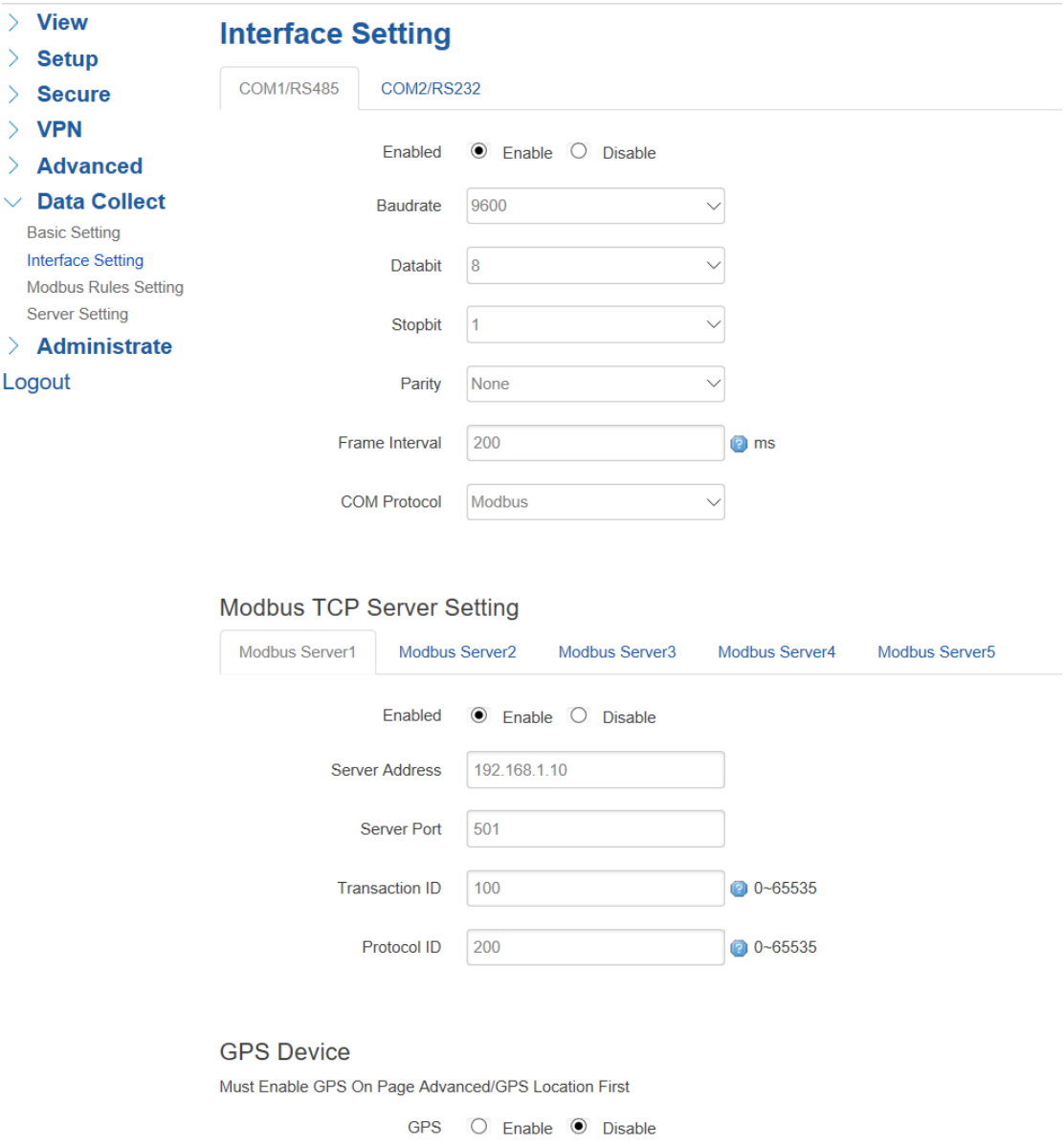
Enable or Disable the data collect feature, setting the data acquire and report period and other related options.



1) Data Collect: Enable or Disable data collect feature.
2) Collect Period: Set the period of data acquire from slave devices.
3) Report Period: Set the Period of data report to server.
4) Enable Cache: Enable or Disable history data cache feature.
5) Related data cache setting if enable the cache feature.

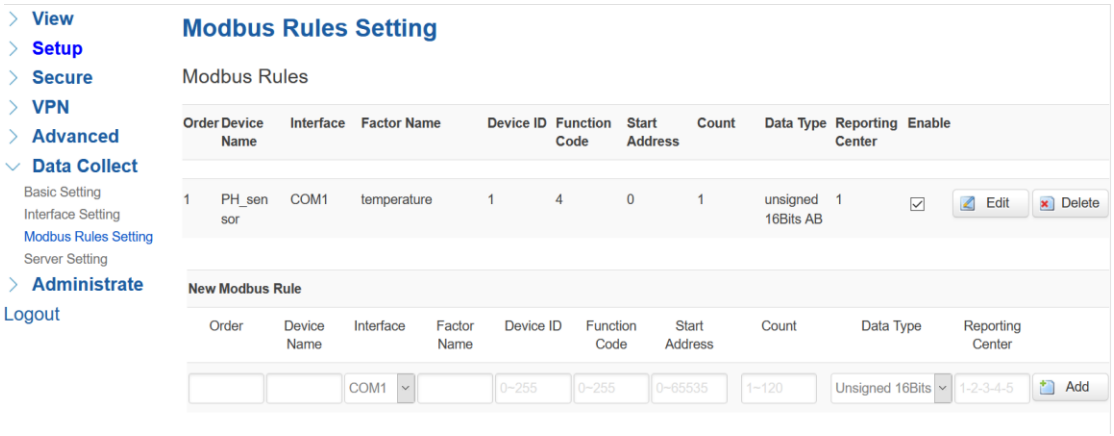
3.6.2 Interface Setting

Switch the hardware interfaces for data acquisition from kinds of slave devices. Including Serial ports (COM1~COM2), Modbus TCP base on Ethernet LAN, GPS Device.

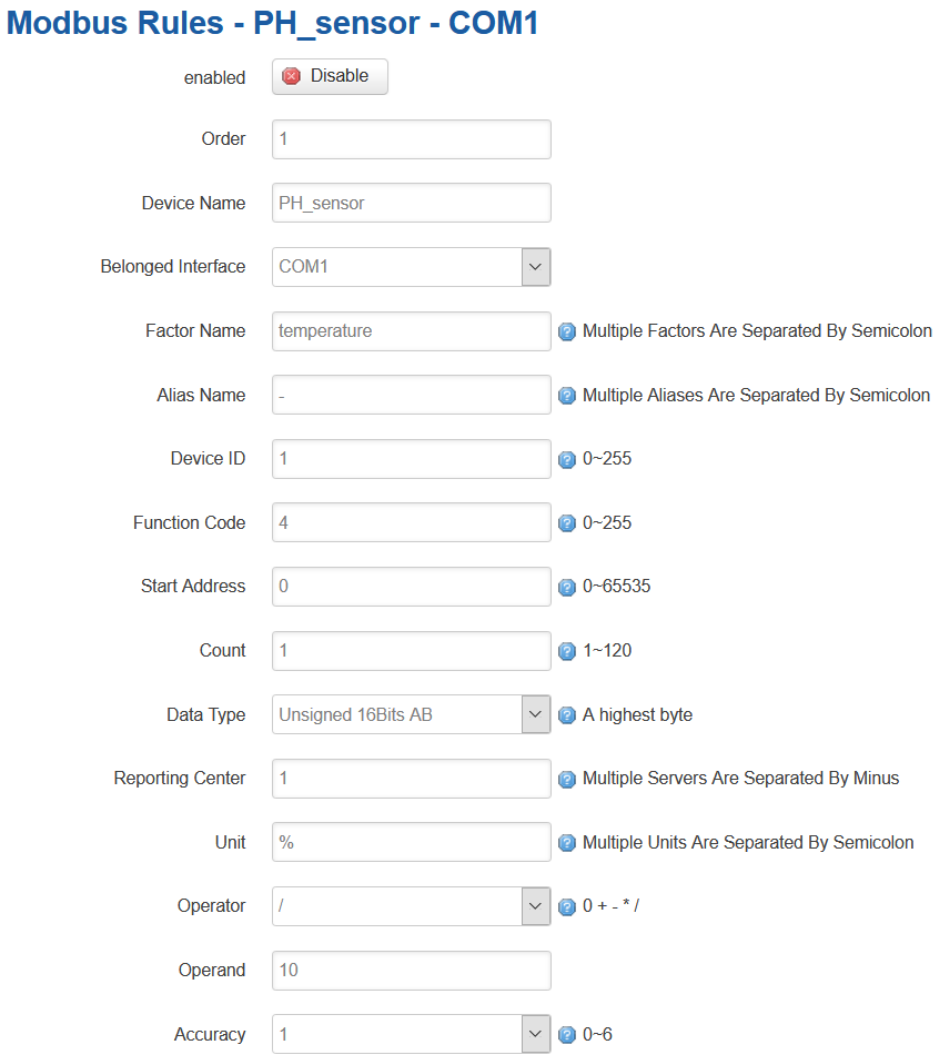


3.6.3 Modbus Rules Setting

Modbus Rules Setting is for TR321 as a Modbus master to acquire data from slave devices base on Modbus protocol. You can configure unlimited Modbus rules on it. TR321 provide the options of definable factor name, device ID, function code, register address and count register number, please following the slave device datasheet to get those information.



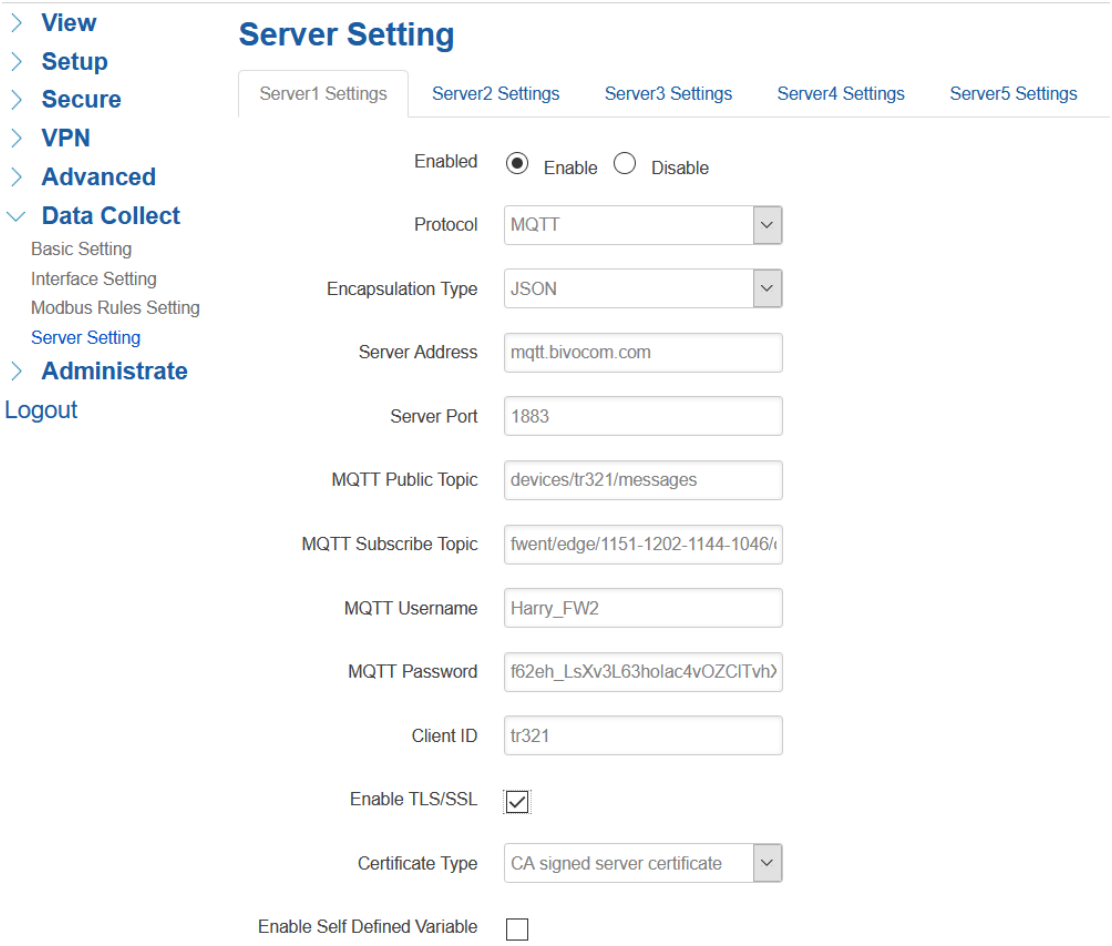
Click “Edit” button for more details setting,



3.6.4 Server Setting

Server setting menu allows user set the data center address with multiple protocols, the standard TR321 support TCP, UDP, HTTP, MQTT, and Modbus TCP. For the data format,

TR321 support different Encapsulation type, include “Transparent”, “Json”, and “HJ212” (special for some Environment SCADA). Also TR321 accept customize specific protocols for your data center.

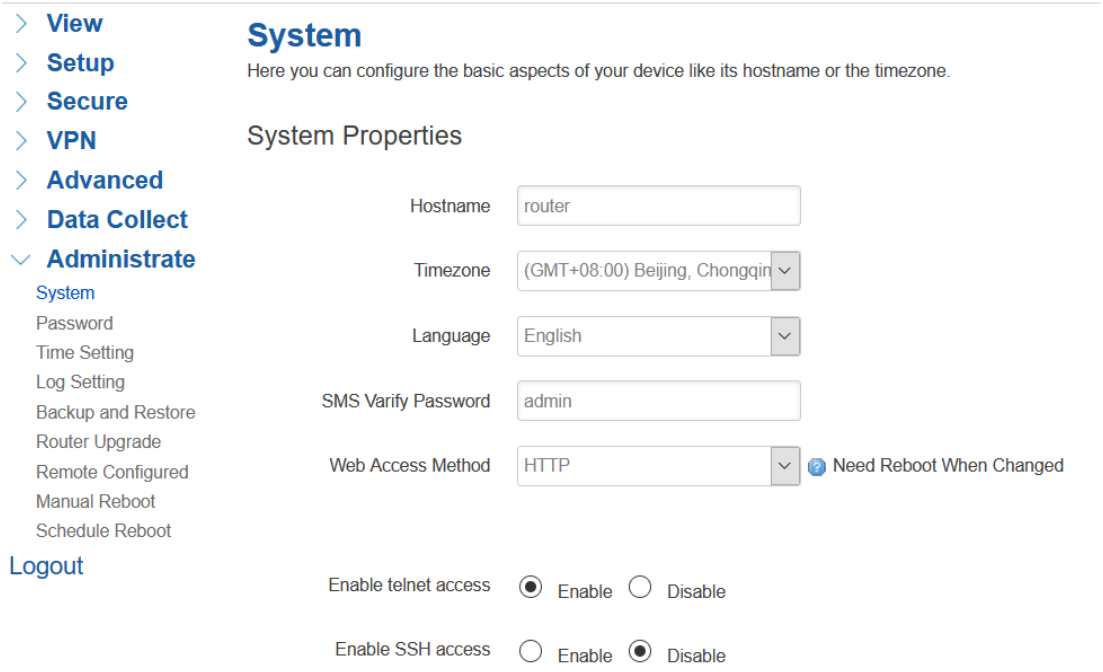


3.7 Administrate

Administrate page provide the administrator level setting for system, like password setting, Timezone setting, Backup and Reset setting, etc.

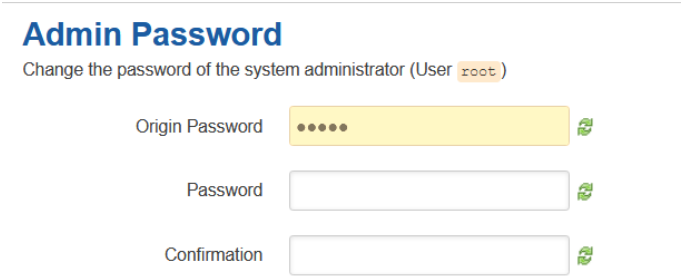
3.7.1 System

System page provide the basic system information setting like Hostname, Timezone, Language, etc.



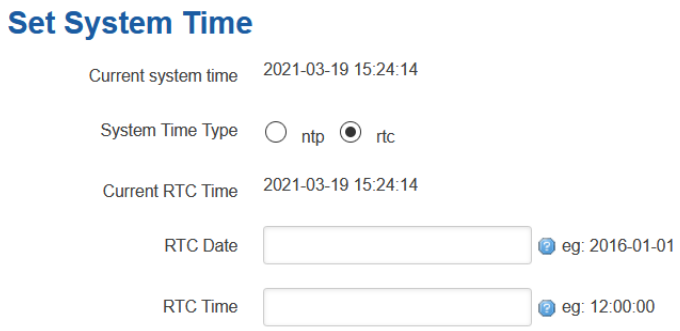
3.7.2 Password

To revise the password of router.



3.7.3 Time Setting

System time type includes RTC (Real Time Clock) and NTP (Network Time Protocol). RTC will save time even router is powered off, while for NTP, router will connect to NTP server which requires internet connection, time won't be saved once powered off. But NTP will be more accurate than RTC, and you may need to adjust the time manual if it is not accurate.



1) Current System Time

Display the time of router.

2) System Time Type

It includes NTP and RTC mentioned above, and different type has different configuration parameters

- **RTC**

You can update data and time yourself.

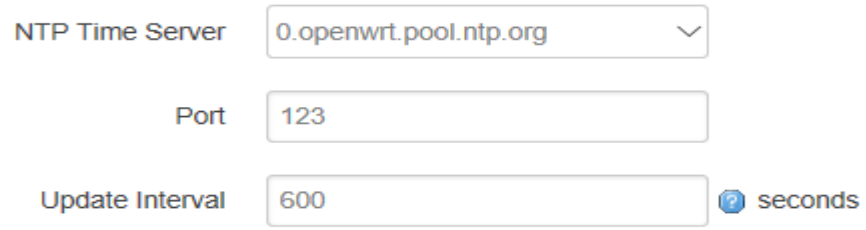
RTC Data

Format must be: 20xx-xx-xx (Year-Month-Day), or you will fail to update it.

RTC Time

Format must be xx: xx: xx (Hour-Min-Second), or you will fail to update it.

- **NTP**



NTP Time Server

You can select the NTP time server through drop-down menu, or you can customize it yourself.

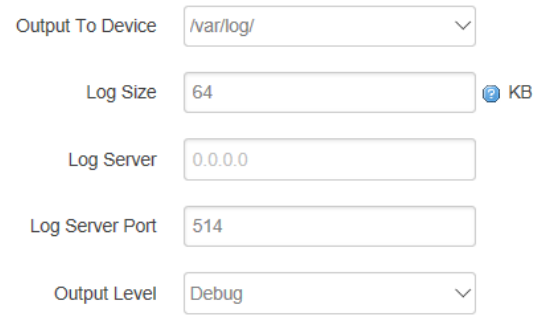
Port

NTP time server port, default port is 123.

Update Interval
How long to sync the time with NTP server, default time is 600 seconds.

3.7.4 Log Settings

Log settings is for configuring the output parameters of system log.



1) Output to Device

You can output the log to serial port, or specified file path, or external storage device, and the default path is:/var/log/

2) Log Size

Set up the size of log, default value is 64KB.

3) Log Server

Set up the IP address of log server.

4) Log Server Port

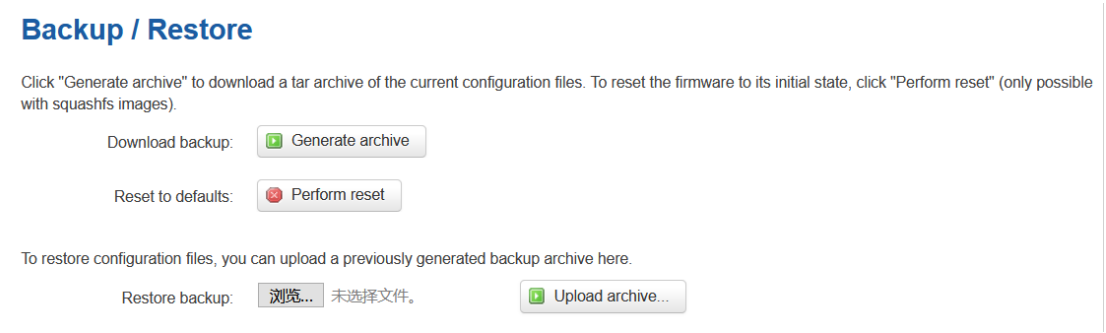
Set up the port of log server, default value is 514

5) Output Level

There are several levels supported, including ‘Debug’, ’Info’, ‘Notice’, ‘Warning’, ‘Error’, and level increased in sequence, the higher level, the less output log.

3.7.5 Backup and Reset

User can either backup the configuration of router as a .gz file, or reset all settings to factory defaults.



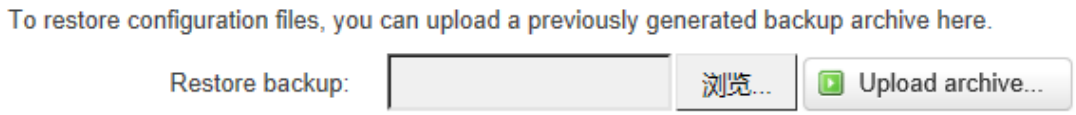
1) Download Backup

Click to generate a configuration file in format of “backup-router-2016-**-**.tar.gz”.

2) Reset to Default

Click ‘Perform Reset’, and a pop-up confirmation box with ‘Really Reset All Changes’ will display, then click ‘OK’ to reset to factory defaults.

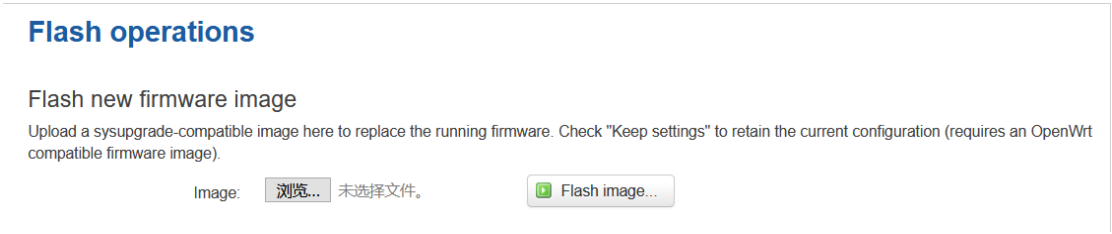
3) Restore Backup



After reset to default, you can also upload the saved configuration file to router, to recover the previous configuration. Click ‘upload archive’, select and upload the backup configuration file, and a pop-up confirmation box with ‘Really Restore’ will display, then click ‘OK’, to recover the configuration.

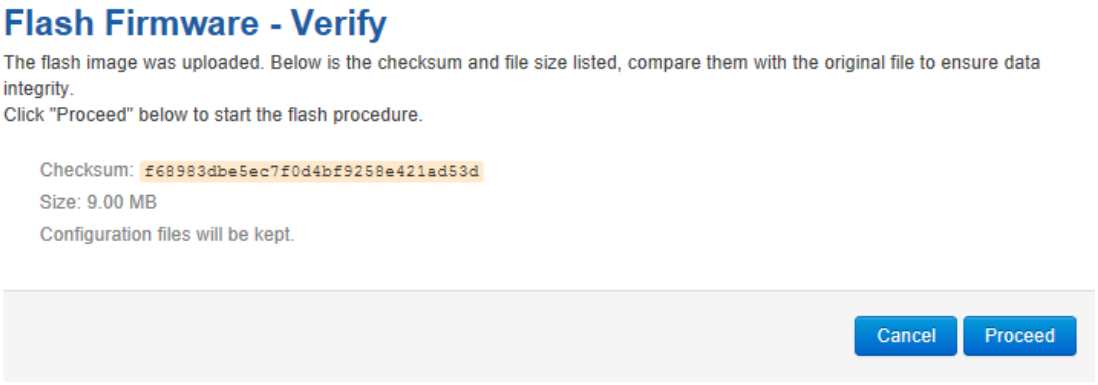
3.7.6 Firmware Upgrade

Router upgrade page provide upgrade firmware via webUI. Before upgrade the firmware for router, please ensure the firmware you’re planning to upload is correct one, otherwise that may cause device crash.



1) Choose and Upload Firmware Image

Click ‘browse’ and select the firmware, then click ‘Flash Image’, and firmware will be upload to router. Then you’ll go to below page.



- **Checksum**

MD5 checksum value of firmware.

- **Size**

The size of firmware.

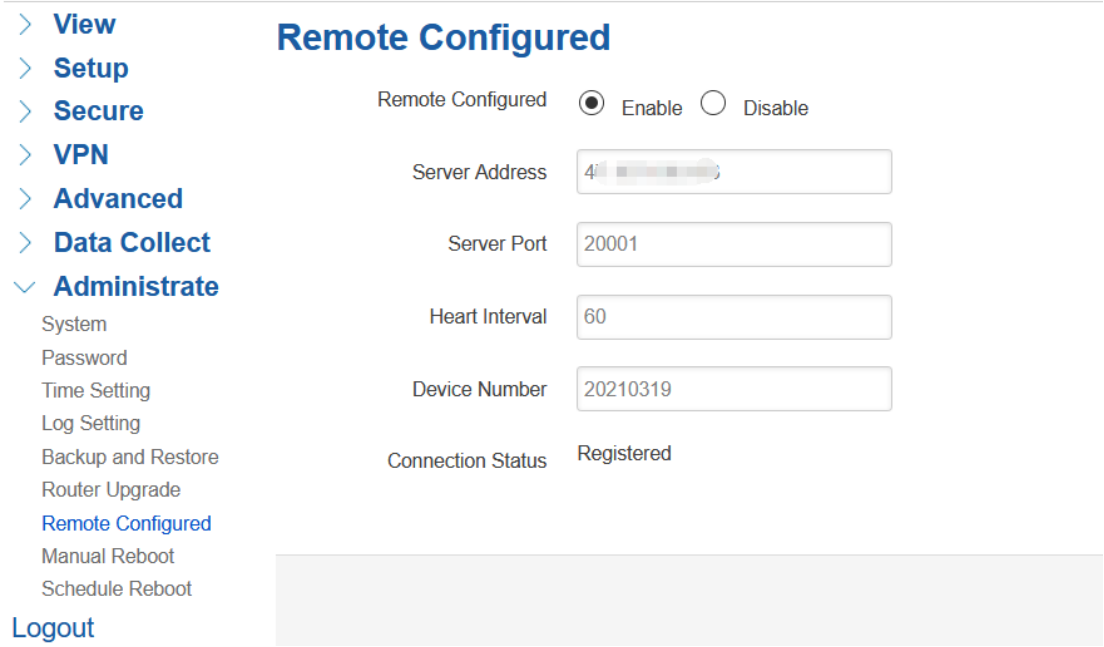
- **Proceed**

Click ‘proceed’ to start the firmware upgrade, or click ‘cancel’ to stop the firmware upgrade.

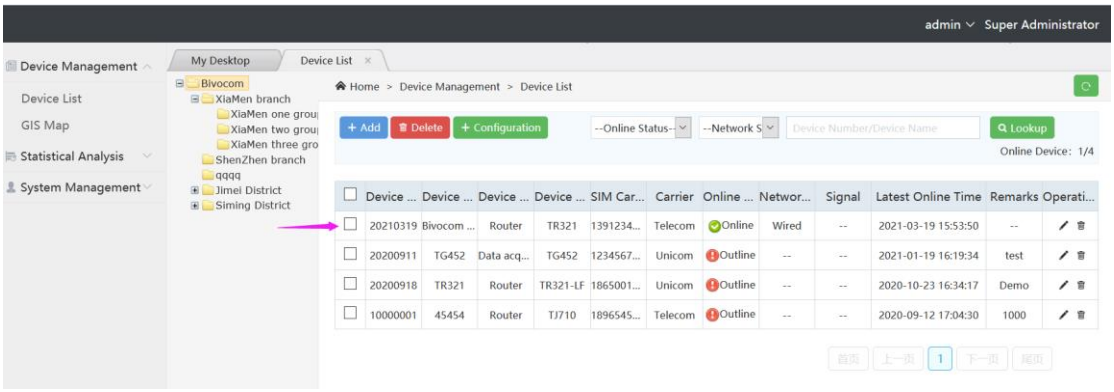
3.7.7 Remote Management

Remote Management feature allows TR321 **connect with Bivocom Device Management Platform** identify by Device Number for remote management, like firmware upgrade, configuration change, etc.

You can configure the IP address and port of remote DMP server, device number and phone number of router, etc., as below.



Once it registered, on the Bivocom Device management platform, you will see the connection status as “Online” and you can configure it via DMP webUI.



1) Server Address

Type the specified login server address you want to remote mange the router, it can be either an IP address or Domain Name.

2) Server Port

The specified login server port.

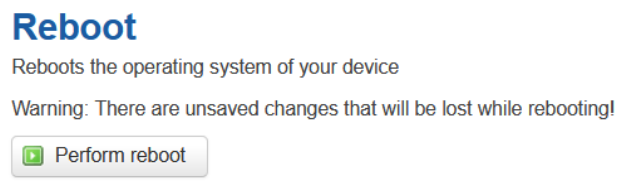
3) Heartbeat Interval

The heartbeat time interval (Unit: second)

4) Device Number

Define an individual Device ID for router and as identify on DMP.

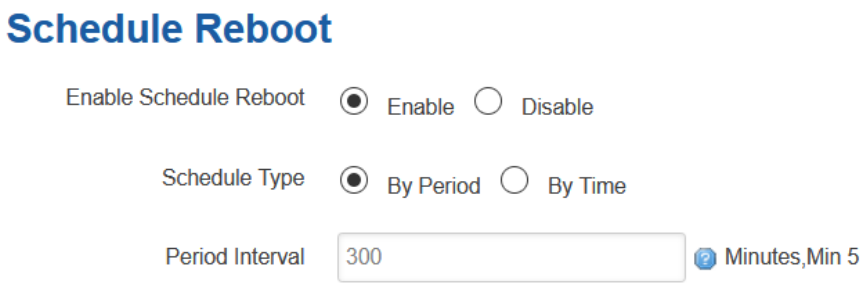
3.7.8 Manual Reboot



Click ‘Perform Reboot’, and a pop-up confirmation box with ‘Really Reboot’ will display, then click ‘OK’ to reboot the router.

3.7.9 Schedule Reboot

Schedule reboot feature allow you preset the rules of device reboot, by period interval or by a certain time point.



3.8 Logout

Click the Logout menu to logout the webUI of TR321.