Bivocom®

Industrial Gigabit Cellular Gateway

5G/4G

TG465 Series User Guide

Note: interfaces of hardware(4G&5G) for different model will be different.

Copyright

Trademark

FEDERAL COMMUNICATION COMMISSION (FCC) STATEMENT

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 25cm between the radiator& your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

HQ: 27-28th Floor, F14 Building, Software Park #3, Xiamen, China

Assembly Center: 6th Floor, 18# building, AnRen industrial park, No. 1068, Jimei North Ave, Jimei, Xiamen, China

Tel.: +86-15880262905

Email: support@bivocom.com

sales@bivocom.com

www.bivocom.com

CE FC

EU DECLARATION OF CONFORMITY

Hereby, **XIAMEN BIVOCOM TECHNOLOGIES CO., LTD.**declares that the radio equipment type TG465 is in compliance with Directive2014/53/EU.

About This Guide

Thank you for choosing Bivocom Industrial 5G/4G Gigabit IoT Gateway TG465 Series.

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

This manual is compatible with below models

Model	Description
TG465-NR	Industrial Edge Gateway with 5G/NR Sub-6
TG465-LF	Industrial Edge Gateway with 4G/LTE

Table of Contents

1. Introduction

1.1 Overview

The TG465 is a powerful and intelligent next generation IoT Gateway built-in with ARM CPU, GPU and NPU. It's designed for mission-critical IoT applications that demands advanced connectivity, edge computing, enhanced security, AI and machine learning, improved energy efficiency. It finds great utility in sectors such as industry 4.0, telecom sites, smart city, smart grid, renewable energy, transportation, etc.

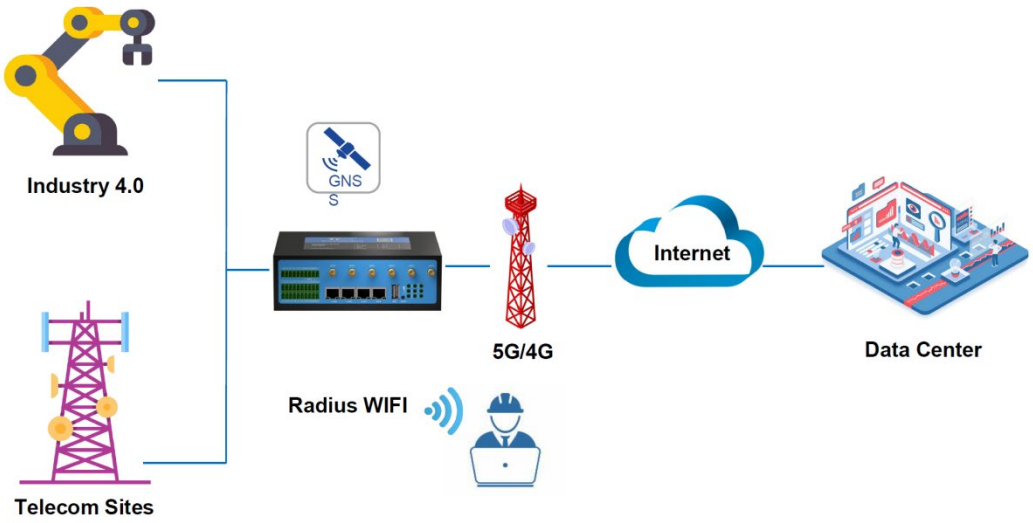
The TG465 offers an embedded environment with OpenWRT-based Linux OS, enabling IoT developers to program and install their own applications using Python, C/C++ directly on the hardware via SDK. Additionally, it provides a flexible secondary development option through the Ubuntu programming environment.

The TG465 has wide range of interfaces and I/Os, allowing seamless connectivity with various equipment, controllers, and sensors. It facilitates data transfer to the cloud server via a 5G/4G LTE cellular network. It also supports crucial industrial protocols like MQTT broker/client, Modbus RTU/TCP, JSON, TCP/UDP, OPC UA, IEC101/104, and VPN, ensuring efficient and secure IoT data connectivity between field devices and the cloud server.

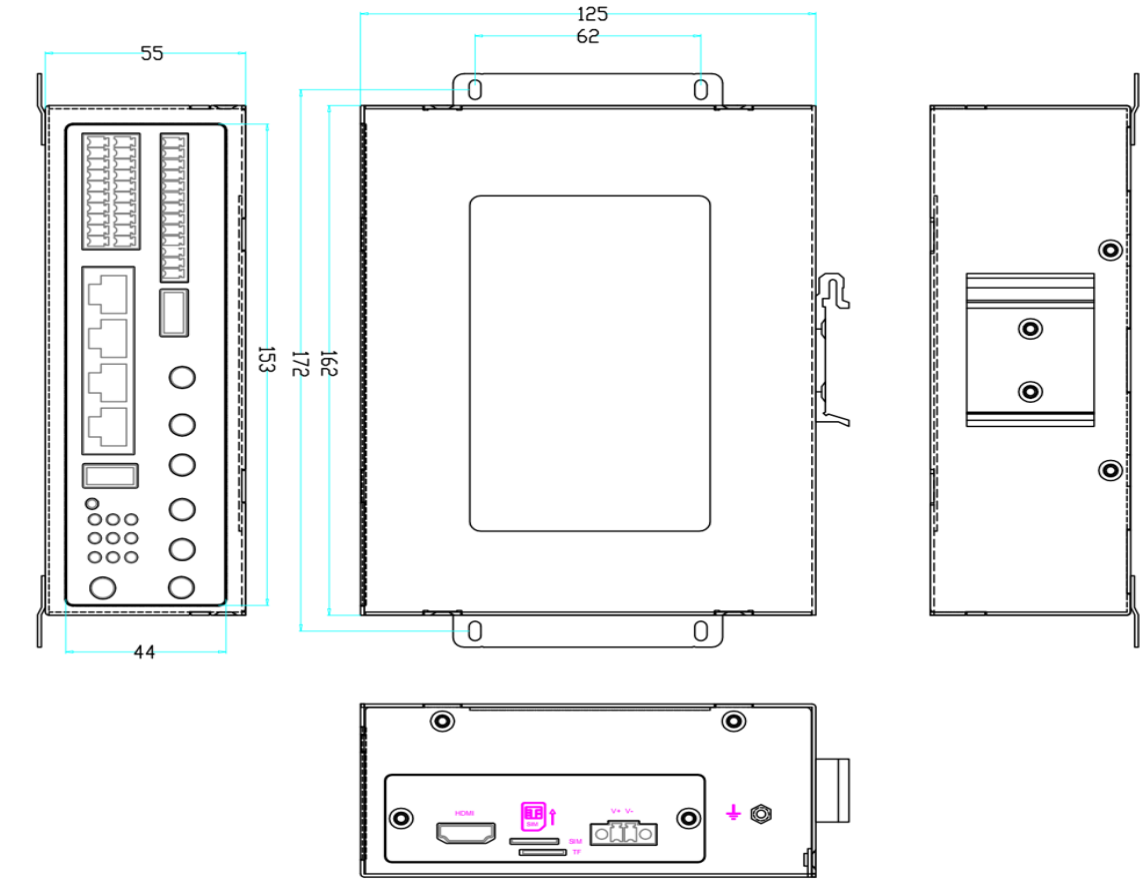
1.2 Applications

The TG465 facilitates quick access to high-speed internet and ensures secure and reliable data transmission. It has found widespread applications in smart pole scenarios, including smart cities, municipal areas, parks, highways, tunnels, scenic areas, industrial parks, and themed towns.

Typical application as below.



1.3 Dimensions



1.4 Physical Characteristics

Physical Characteristics	
Housing	Metal, IP30
Dimensions	162x125x55mm (6.38 x 4.92 x 2.16in), Antenna and other accessories not included
Weight	TG465: 799g (1.76lbs), without accessories.

2. Getting Started

2.1 Package Checklist

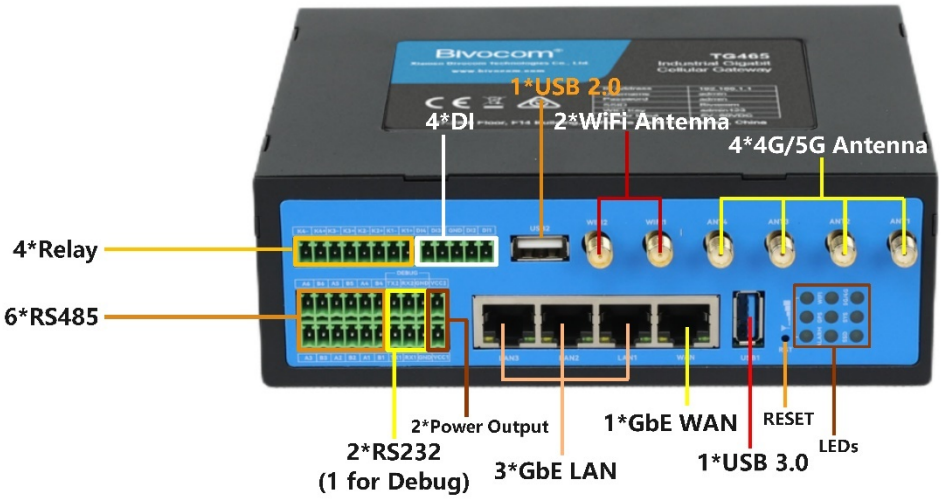
The following components are included in your TG465 package.

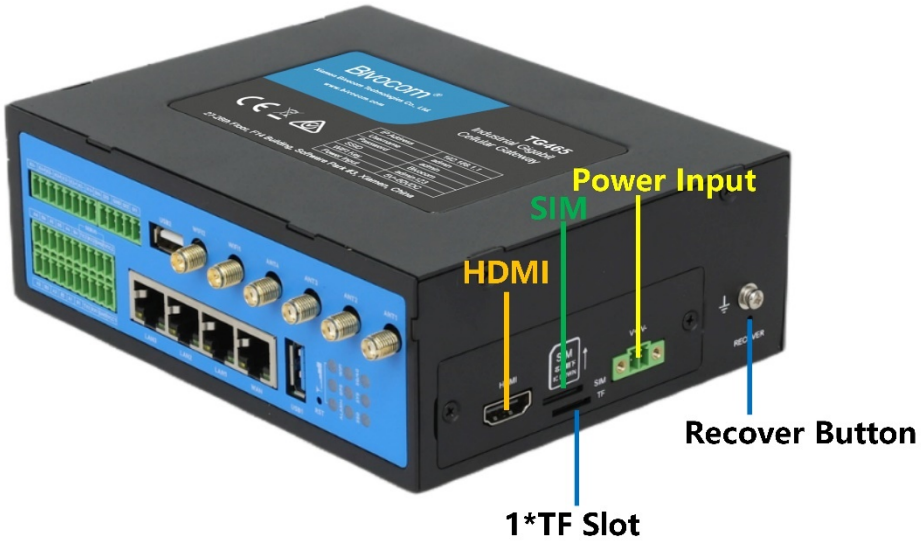
Check the list before installation. If you find anything missing, please feel free to contact Bivocom.

1. TG465 Gateway	1PCS	
2. Power Adapter(DC 12V/1.5A, EU/US/UK/AU plug optional)		1PCS
3. Mag-mount Cellular Antenna (SMA Male, 1 meter, 5dBi)		5G Version:4 PCS 4G Version:2 PCS
4. RS232 Cable (DB9 Female, 1 meter)	1PCS	
5. Ethernet Cable (1 meter)	1PCS	
6. 10-Pin Terminal Block	3PCS	
7. 2-Pin Terminal Block	1PCS	
8. DIN-Rail Mount Kits	1PCS	

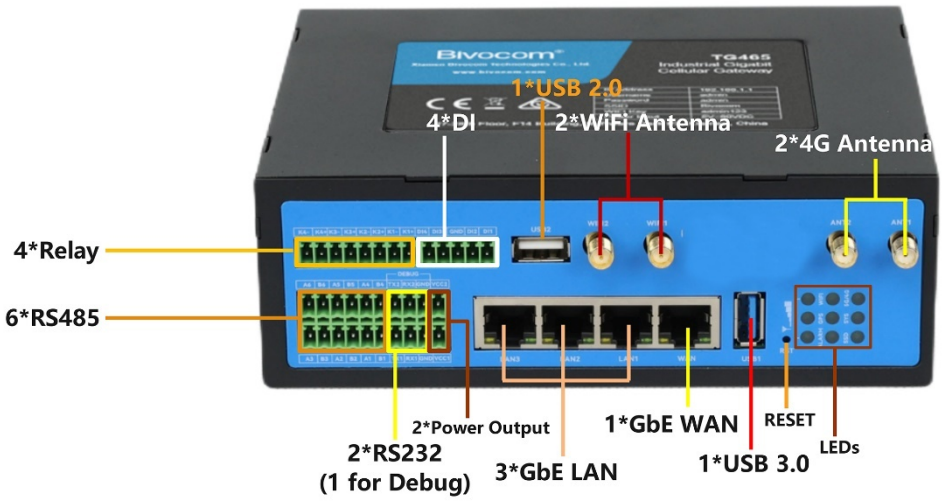
2.2 Installation

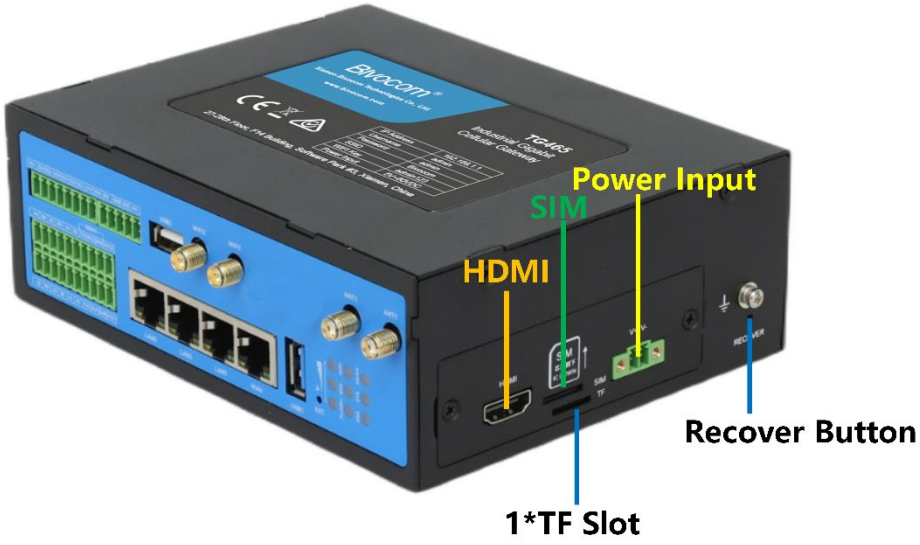
TG465-NR(5G Version) Hardware interfaces instruction:





TG465-LF(4G Version) Hardware interfaces instruction:





2.2.1 SIM/UIM Card

TG465 supports Micro SIM(3FF) only, so if you're using a Nano SIM card, you may need to use a Nano SIM to Micro SIM adapter.

Before installing the SIM card, power off the router. Align the SIM with its chipset facing downward and insert it firmly along the guide rails until an audible click confirms secure locking. For removal, prepare a standard eject tool (e.g., SIM eject pin), insert it into the release mechanism, maintain firm pressure until an audible click indicates disengagement

and partial ejection, then fully extract the card along the insertion path.

Warning: Never install SIM/UIM card when router is powered on.

2.2.2 Interfaces connection

TG465 support 2 RS232 serial ports, 1 RS232_2 works as console port, which can be used for firmware upgrade, system log checking, debug, etc, 1 RS232_1 can be used for communicating and data collecting.

TG465 include 6 RS485, 4x Relay (K1, K2, K3, K4), 4x DI(DI_1, DI_2, DI_3, DI_4), 2 x 12V DC Output power supply, 2x USB(1xUSB2.0, 1xUSB3.0), 1x HDMI(Option), 1x TF Slot(up to 64GB).

There are 4 Relays, K1/K2/K3/K4, they are mainly used to control switching circuits, 4XDI are mainly used to detect high or low-level output(PREVP) voltage.

Relay Interface (K1, K2, K3, K4)

Relay Feature	Control the external switch
Load capacity	Maximum Voltage switch: 30VDC/250VAC Maximum Current switch: 5A

DI Interface (DI1, DI2, DI3, DI4)

DI Feature	Detect the slave device status
Input Range	Logic 1: wet contact 5-30VDC, or dry contact close. Logic 0: wet contact 0-3VDC, or dry contact open.

RS485 Cable (RS485_1~6)

Color of cable	TG465 Gateway
Red	(A)
Black	(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 5-60VDC 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 TG465(SMA female port), make sure it is screwed tightly to ensure the strength of signal.

2.3 LED Indicators

TG465 Series Gateway provides 8 LED indicators, as following.

Indicator	Status	Content
Power	On	Powered On
	Off	Powered Off
ALARM	ON	SIM/UIM doesn’t insert or broken, weak signal
	Blink every 1s	Cellular module doesn’t been detected
SYS	Blink	System works perfect
	Off	System doesn’t work

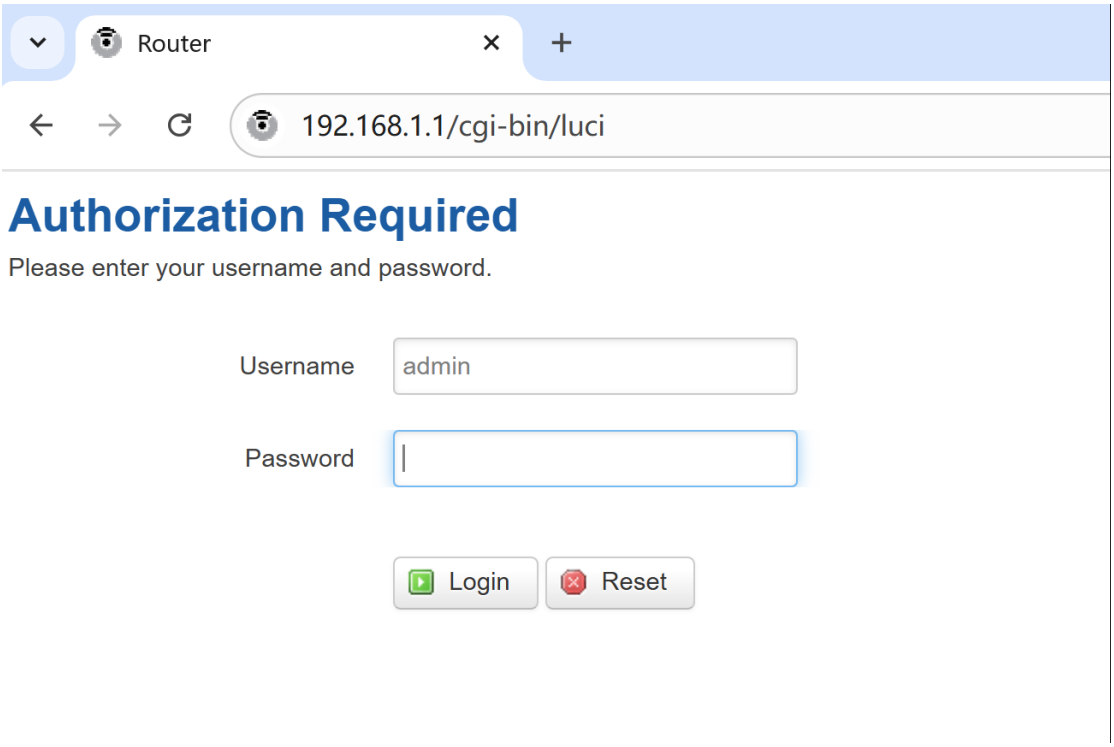
4G/5G	On	Connected to 4G/5G Network
	Off	Not connect to 4G/5G Network
WiFi	On	WiFi enabled
	Off	WiFi disabled
GPS	On	Gateway got GPS data successfully
	Off	Gateway failed in getting GPS data

3. Configuration and Management

The TG465 series devices support dual operating system configurations with OpenWRT and Ubuntu OS. This manual specifically focuses on the OpenWRT OS implementation and configuration guidelines. For technical documentation and development resources pertaining to Ubuntu OS deployment, please consult the Bivocom Support Team to obtain the dedicated Ubuntu development package and corresponding integration materials.

Use an Ethernet cable to connect the LAN port of TG465 to your laptop, or use your laptop or mobile phone to connect to WIFI hotspot ‘Bivocom’ of TG465, login with password: admin123, normally your laptop will get an IP address from TG465 DHCP as 192.168.1.xx, otherwise please manually configure your laptop IP to 192.168.1.100.

Open browser, enter 192.168.1.1 to enter into to login page, enter username: admin, and password: admin, to go to configuration page.

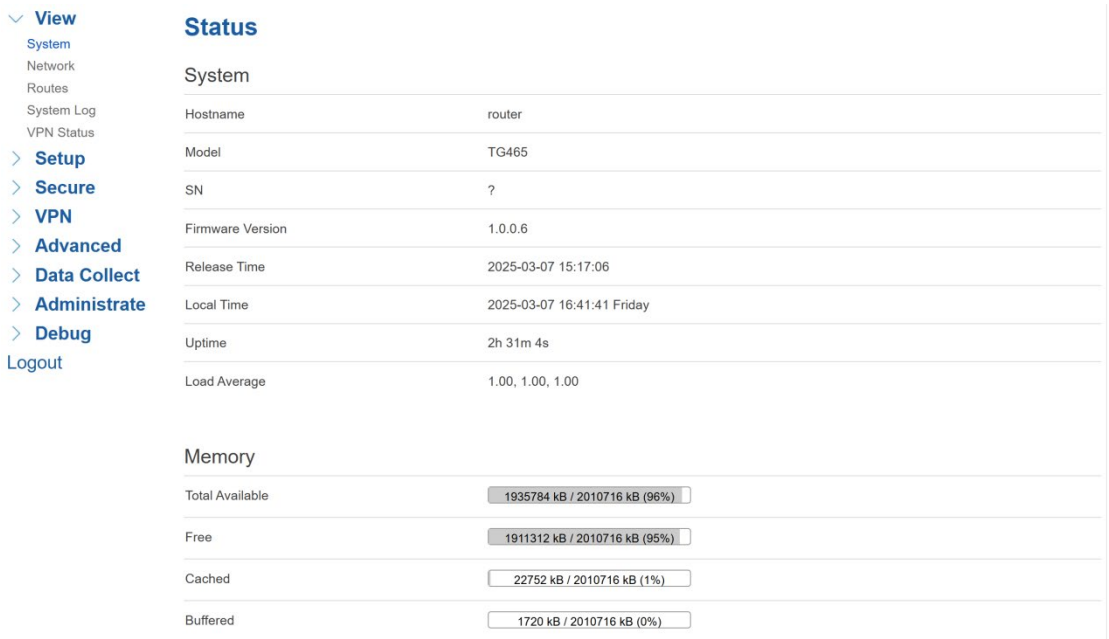


3.1 View

To check the following system information.

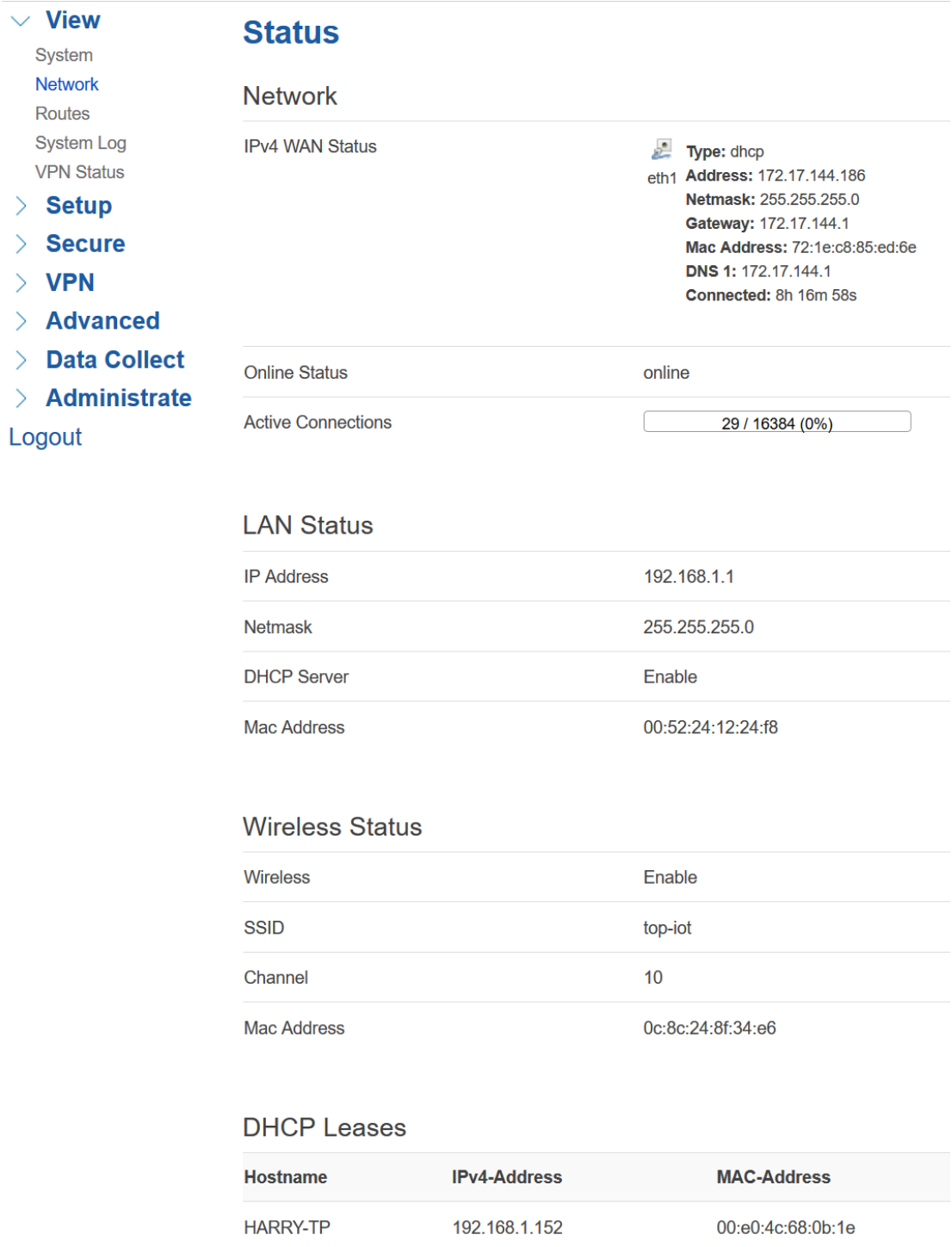
3.1.1 System

Display system related information.



3.1.2 Network

Display WAN, LAN, WiFi, DHCP network information.



3.1.3 Routing Tables

Display routing tables.

ARP

IPv4-Address	MAC-Address	Interface
192.168.1.100	1c:39:47:3f:28:1d	br-lan

Active IPv4-Routes

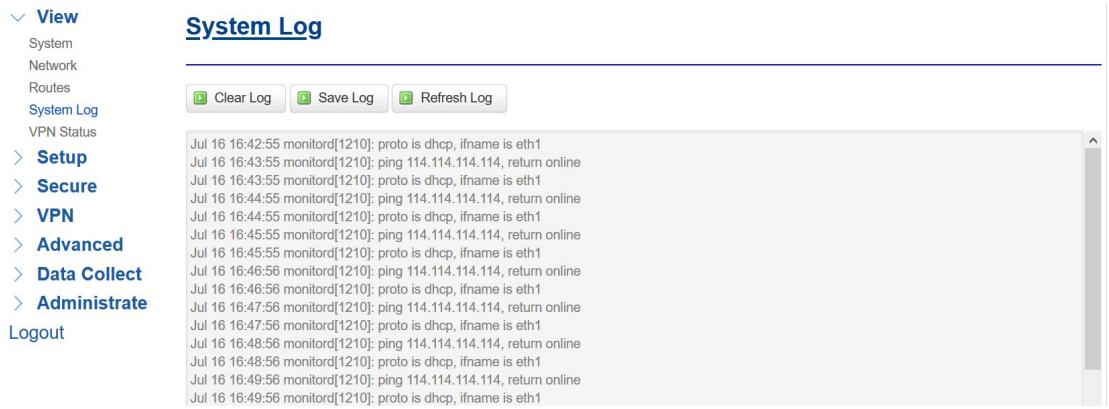
Network	Target	IPv4-Gateway	Metric
lan	192.168.1.0/24	0.0.0.0	0

Active IPv6-Routes

Network	Target	IPv6-Gateway	Metric
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0/0	00000000
(eth2)	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
lan	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
(ra0)	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
wan	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF

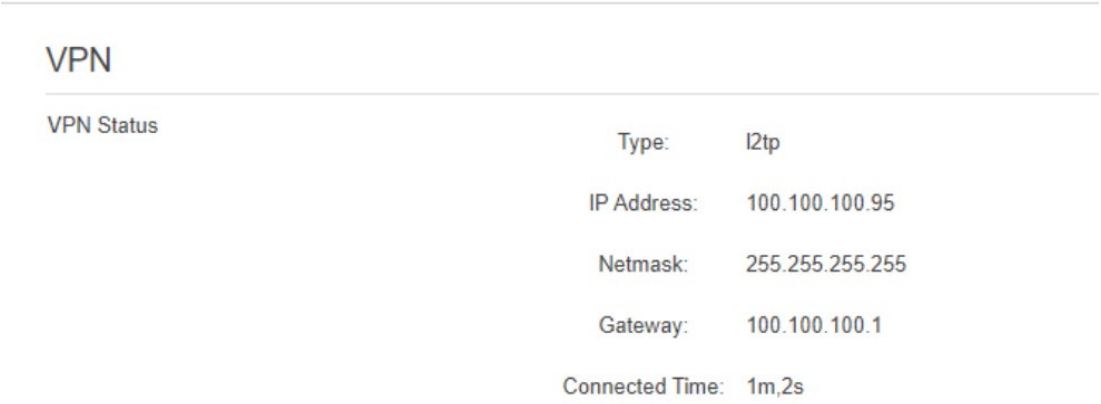
3.1.4 System Log

Display system log.



3.1.5 VPN Status

Display VPN status.



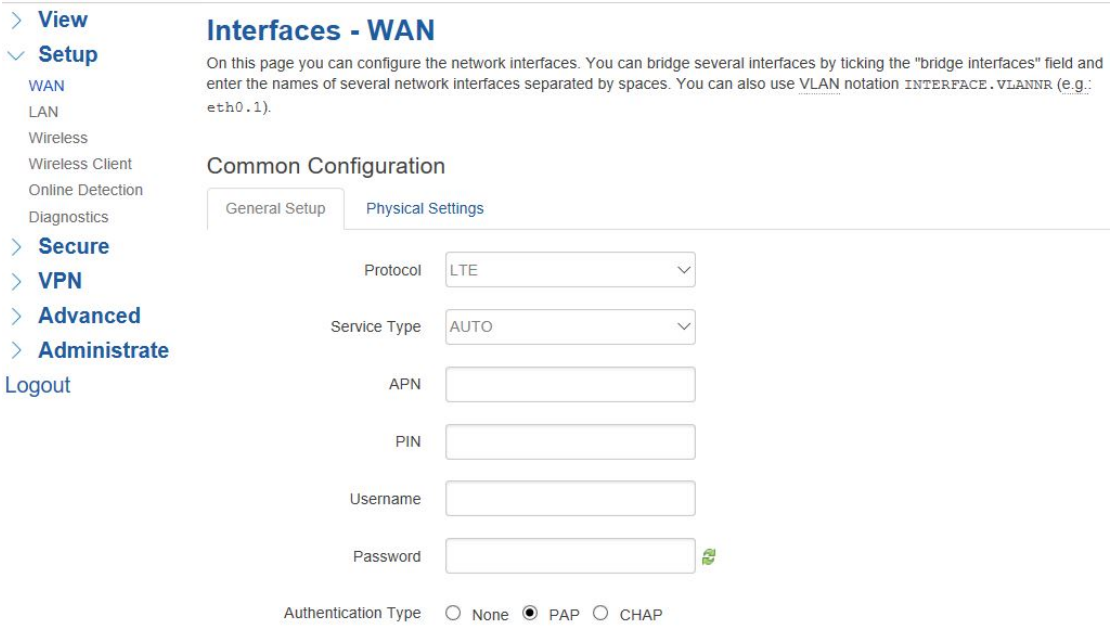
3.2 Setup

Main menu of this page includes, WAN, LAN, Wireless, Online Detection, Diagnostics.

3.2.1 WAN

WAN supports DHCP/Static IP/PPPoE/5G/LTE connection mode.

Choose the mode you need, and configure the related parameters, then click ‘Save&Apply’, after a while, you should able to connect to the internet.



1) Server Type

Type of network, the default value is AUTO, you can keep it or choose your own preference.

2) APN

Different carrier might have different APN, please ask your carrier if you have no idea of what your APN is.

3) PIN

PIN code of SIM card, please use it carefully, or the SIM card may be locked.

4) PAP/CHAP Username

Only for private network SIM card, if you're using public network SIM card, just keep it as null.

5) PAP/CHAP Password

Only for private network SIM card, if you're using public network SIM card, just keep it as null.

6) Call Center No.

When you're using SIM card, different carrier may have different call center Number, please ask your carrier for this info if you have questions.

7) Authentication Type

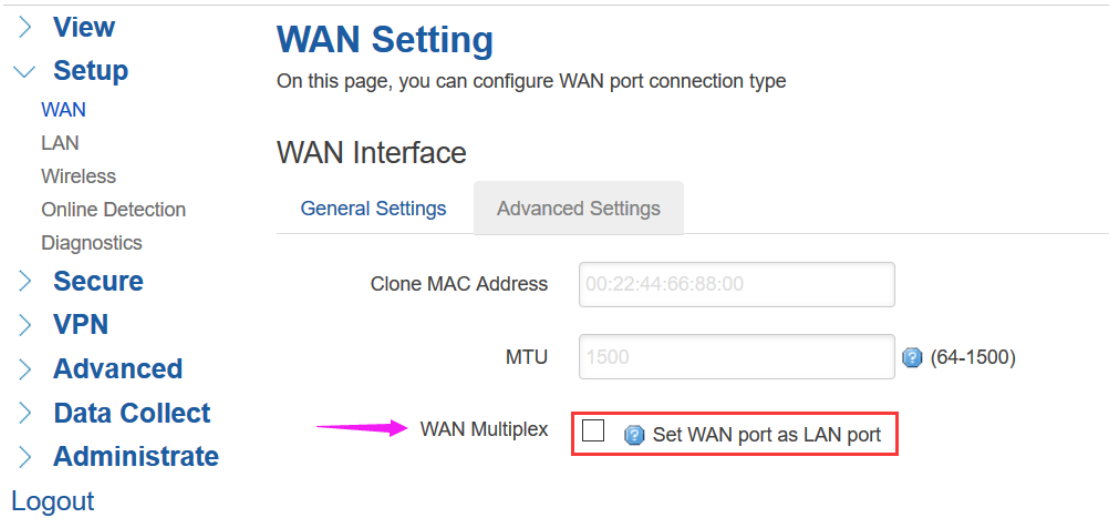
If there have username and password, you need to choose authentication type.

- PAP, Plaintext Authentication
- CHAP, Handshake authentication

You need to choose the authentication type according to carrier's network, or you may fail to dial up.

8) WAN Used As LAN

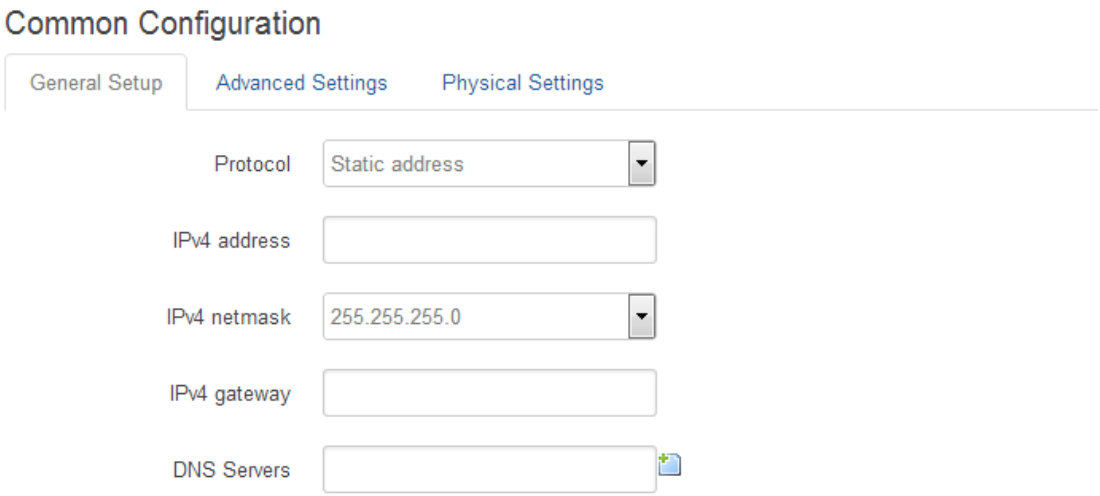
When you use 5G/4G/3G cellular network to access internet, you can change the WAN to act as a LAN port.



3.2.2 LAN

Menu of LAN are mainly for configuring IP address of router, enabling DHCP server, and assign the IP address.

The meaning of the parameters are as follows.



1) IPv4 Address

To configure IP address of LAN port.

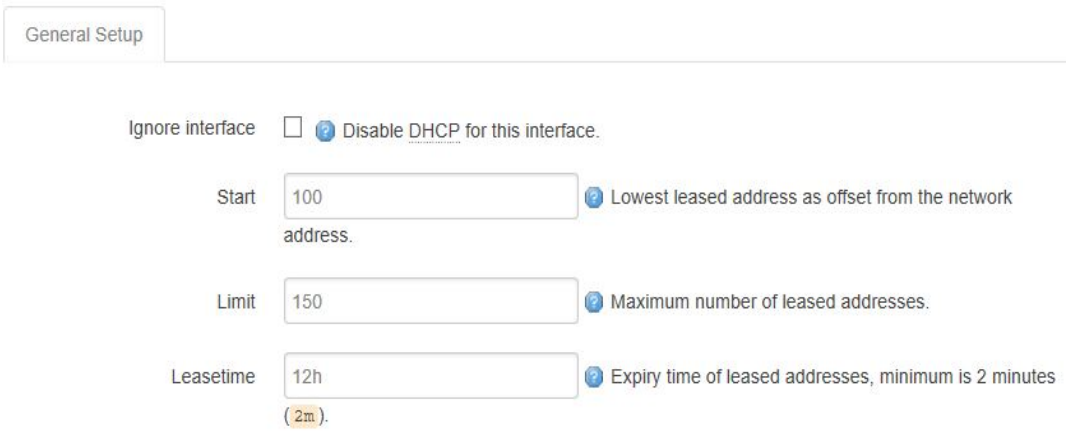
2) IPv4 Netmask

The netmask of LAN port IP address.

3) IPv4 Gateway

Specify the next-hop routing gateway.

4) DHCP 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.

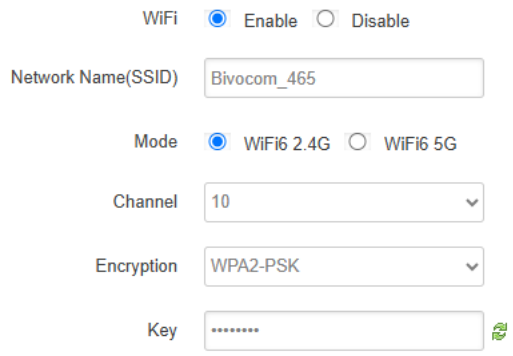
- **Lease time**

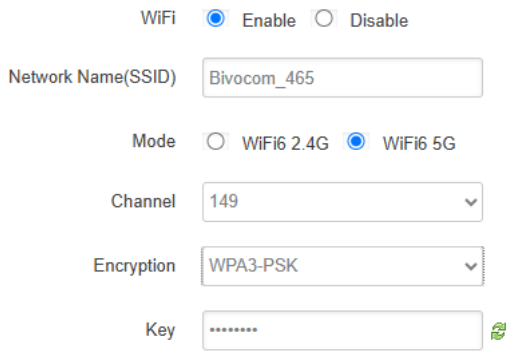
Time of assigning the IP address.

3.2.3 Wireless (Option)

Menu of wireless are mainly for configuring the SSID, work mode, password, etc.

Note, WiFi is not be included in standard TG465, please ask Bivocom representative when place the order.





- **WIFI6 2.4G**

Click ‘WiFi6 2.4G’ button to enable the WIFI 2.4G function.

1) Network Name（SSID）

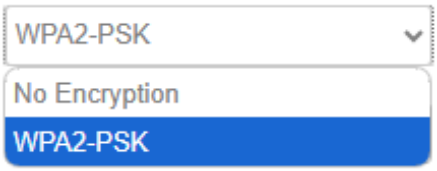
WIFI network name.

2) Channel

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

3) Encryption

You can only choose below types if the mode is set as WiFi 2.4G.



4) Key

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

- **WIFI6 5G**

Click ‘WiFi6 5G’ button to enable the WIFI 5G function.

1) Network Name（SSID）

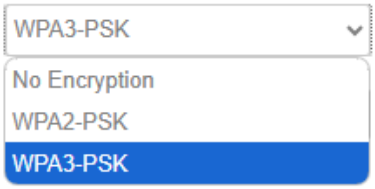
WIFI network name.

2) Channel

Support 149-165 channels, default value is auto, channel can be changed automatically.

3) Encryption

You can only choose below types if the mode is set as WiFi 5G.



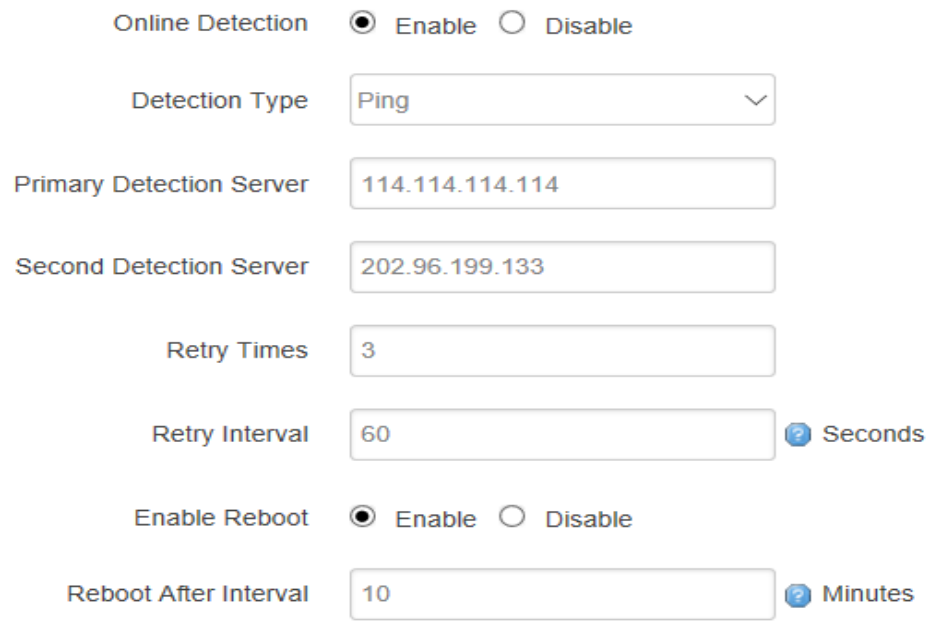
4) Key

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

3.2.4 Online Detection

Online detection will auto check the internet connection status of the router, if there has issue of connection, router will auto reconnect. If it fails to reconnect after times of trial, router will reboot, to ensure getting online.

The meaning of the parameters are as follows.



1) Detection Type

There are 3 types: ping, traceroute and DNS.

- **Ping**

Router will ping an IP address or DNS, 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 show 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 detections.

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.

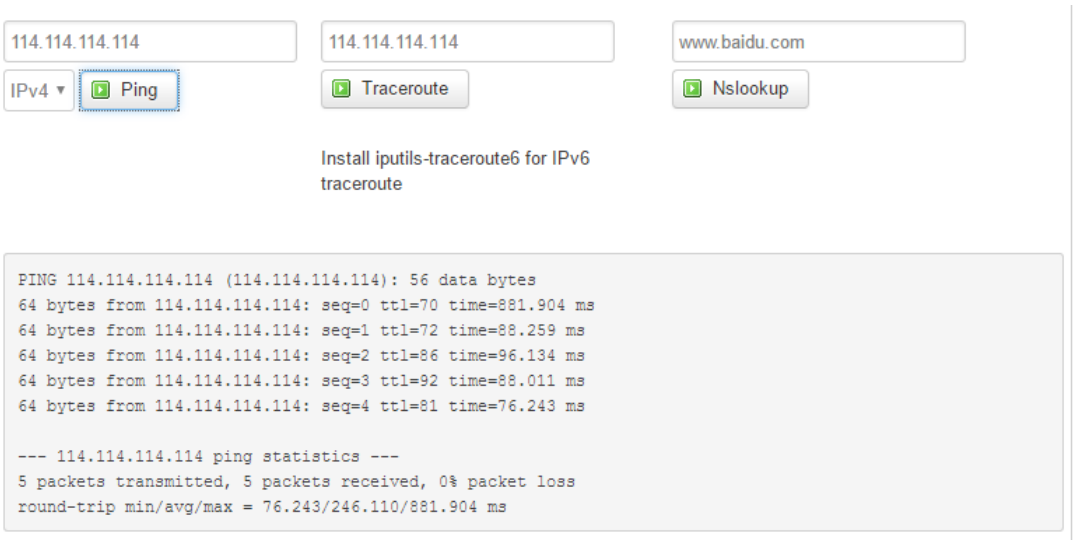
3.2.5 Diagnostics

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.

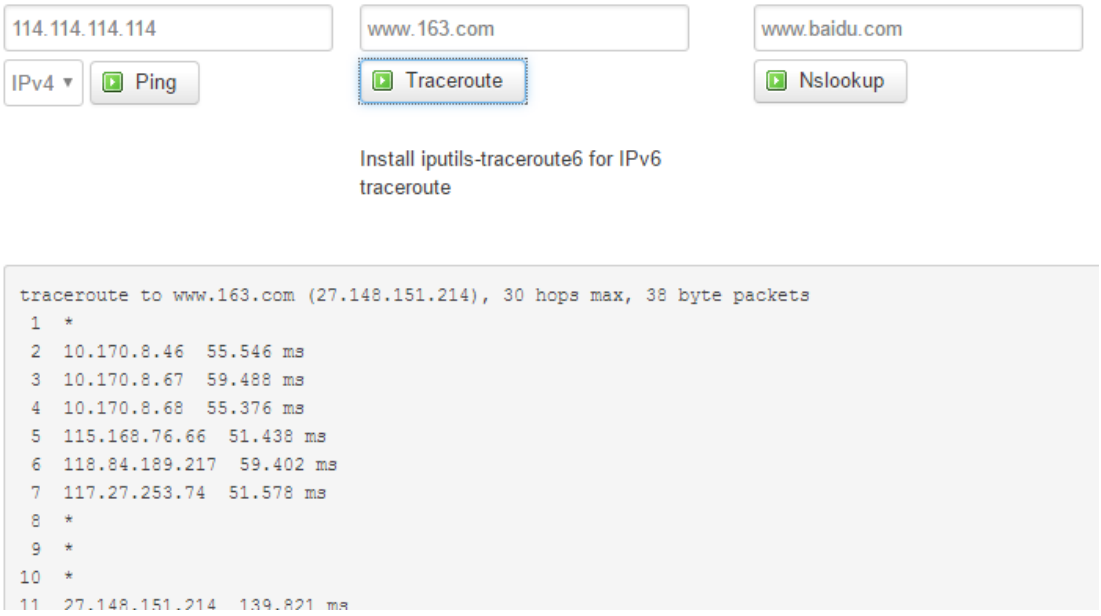
1) Ping

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



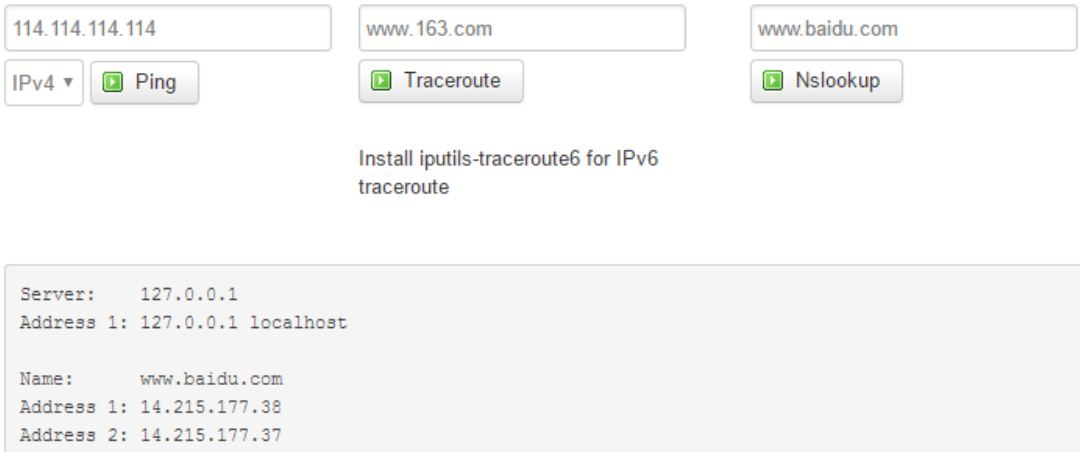
2) Traceroute

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



3) Nslookup

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

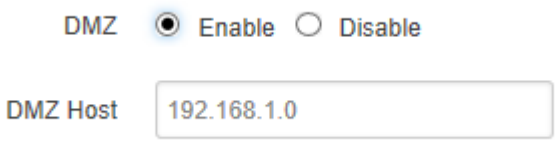


3.3 Security

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.



1) DMZ

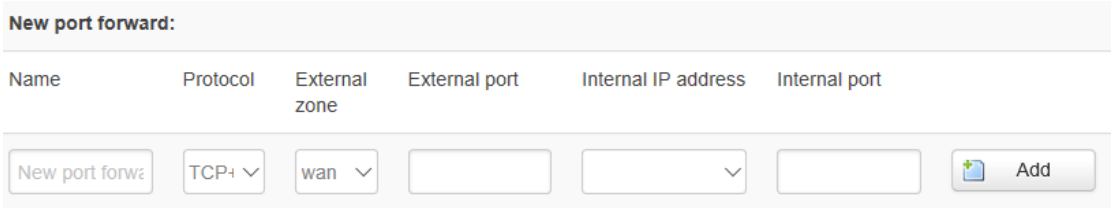
You can enable or disable the DMZ.

2) DMZ Host

An IP address of a host of LAN you want to map.

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.

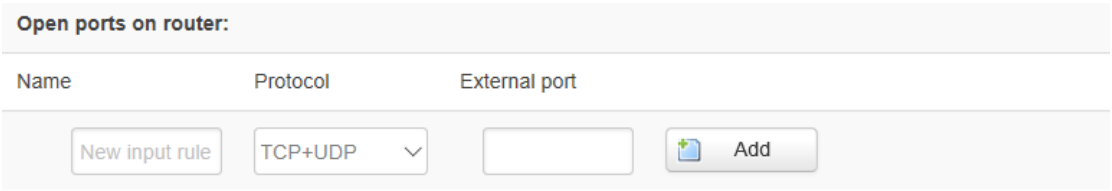
5) Internal Port

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.

3.3.3 Traffic Rules

Traffic rules is used for opening some router ports, such as remote access the configuration page of router, you can open port 80; for remote SSH connection, you can open port 22.



1) Name

You can name the rule yourself.

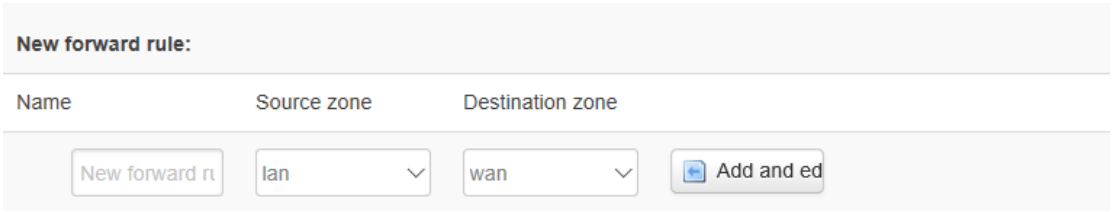
2) Protocol

Choose the protocol of you want to forward can be TCP, UDP, or TCP/UDP.

3) External Port

Choose the port you want to open.

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



1) Name

You can name the rule yourself.

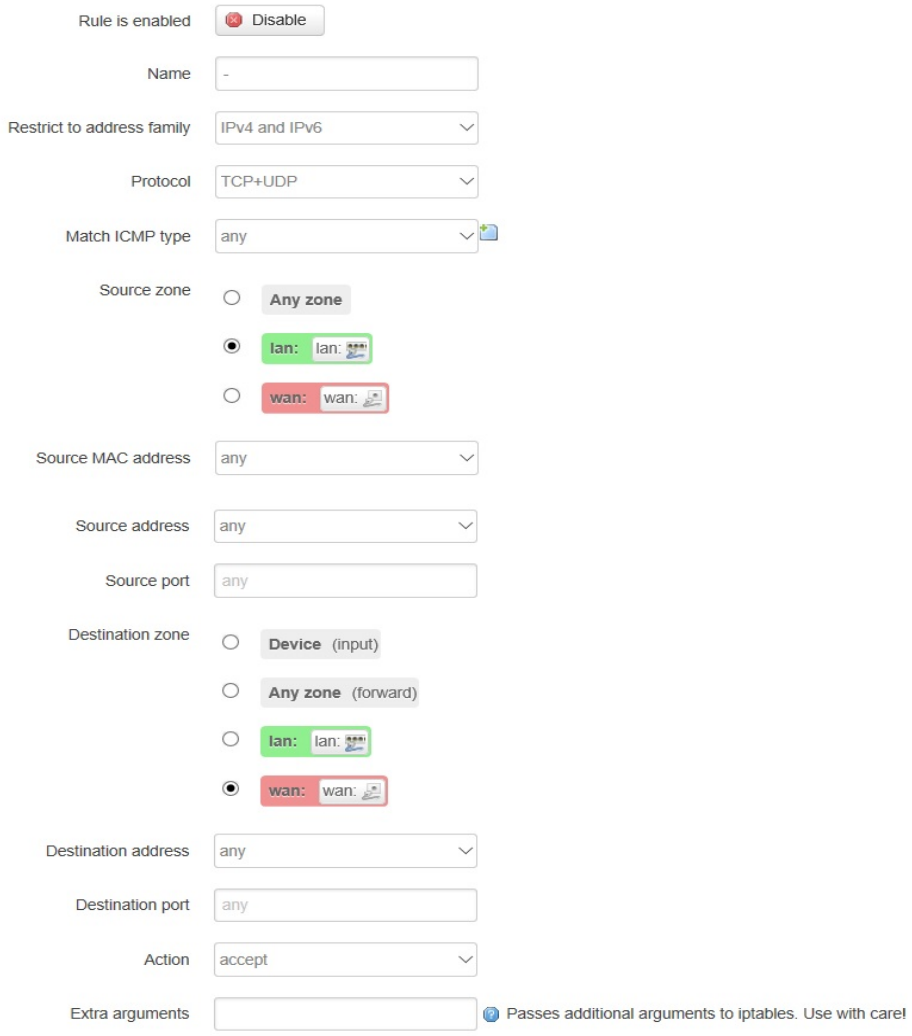
2) Source Zone

You can choose where to start the data packet.

3) Destination Zone

You can choose where to forward the data packet.

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 consist of iptables, we suggest users that 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

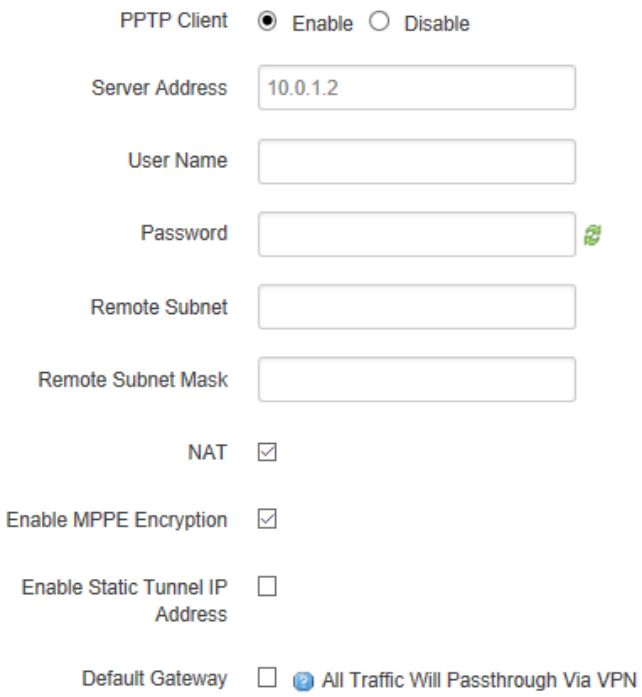
VPN is used to establish a virtual private channel, and all the data in this channel will be encrypted to ensure that data security during transmission.

TG465 support VPN: PPTP, L2TP, OpenVPN and IPSec. PPTP/L2TP are layer 2 VPN, and OpenVPN is VPN based on SSL, while IPSec layer 3 VPN. PPTP/L2TP are more convenient to use, while OpenVPN and IPSec is more complex, as they need complex certification management, meanwhile, they offer more secured encrypted data.

3.4.1 PPTP

You can configure either PPTP client or PPTP server, but not both of them at the same time, as 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 username 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.

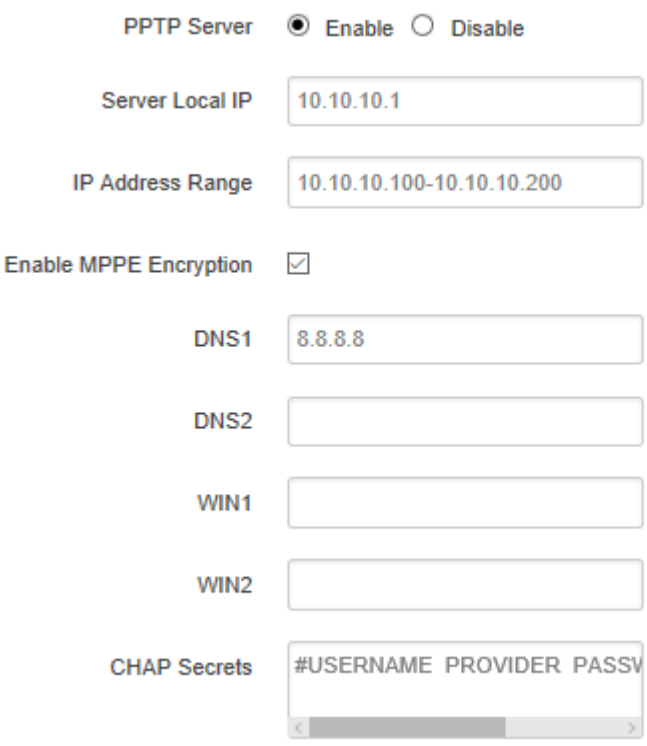
7. Enable MPPE Encryption.

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 a username and password under CHAP Secrets, format as below,

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

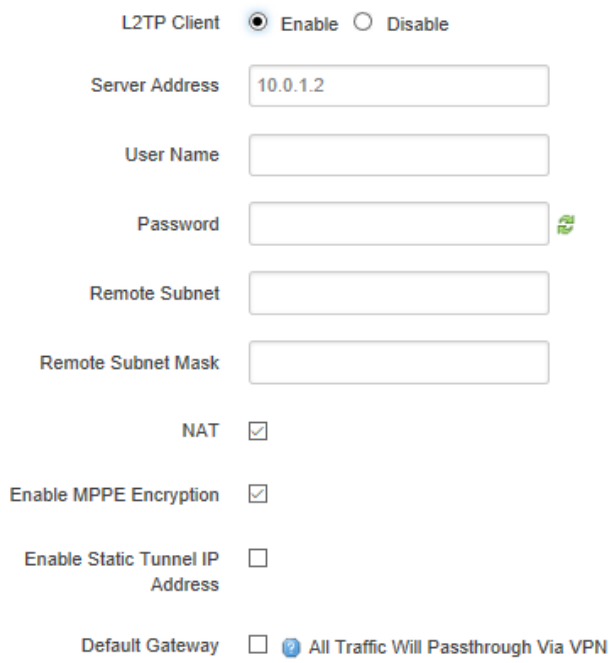
For example, if you want to create a username: test, password: test, it is as below,

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 username 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.

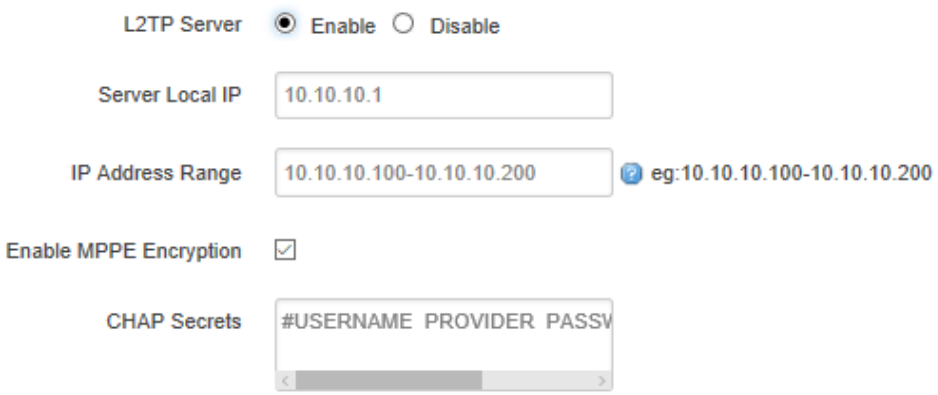
7. Enable MPPE Encryption.

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

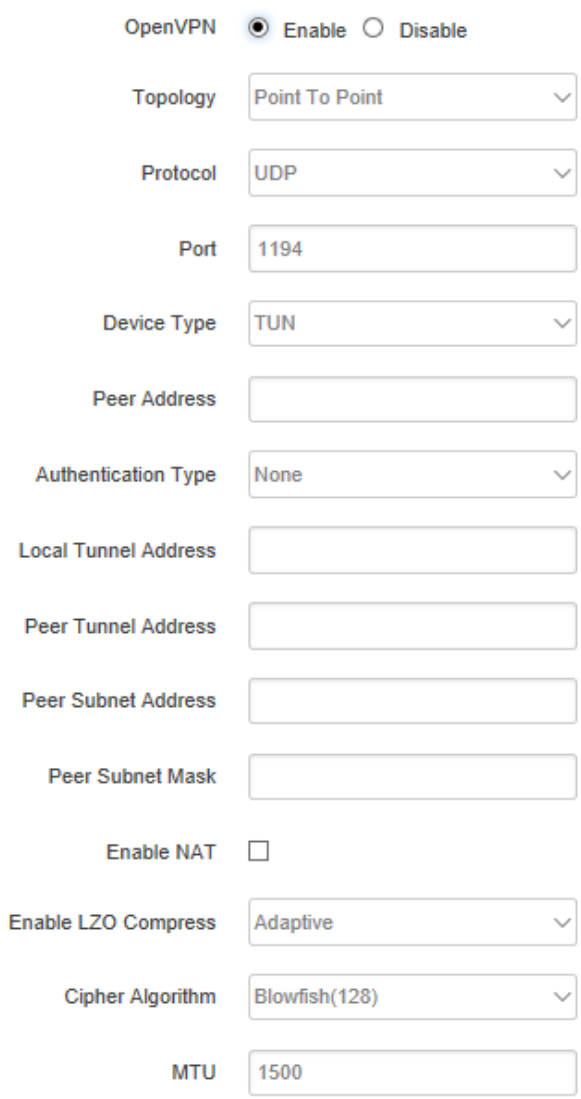
To create a username and password under CHAP Secrets, format as below,

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 Role, you need to enter an IP address or domain name of server.

8) Authentication Type

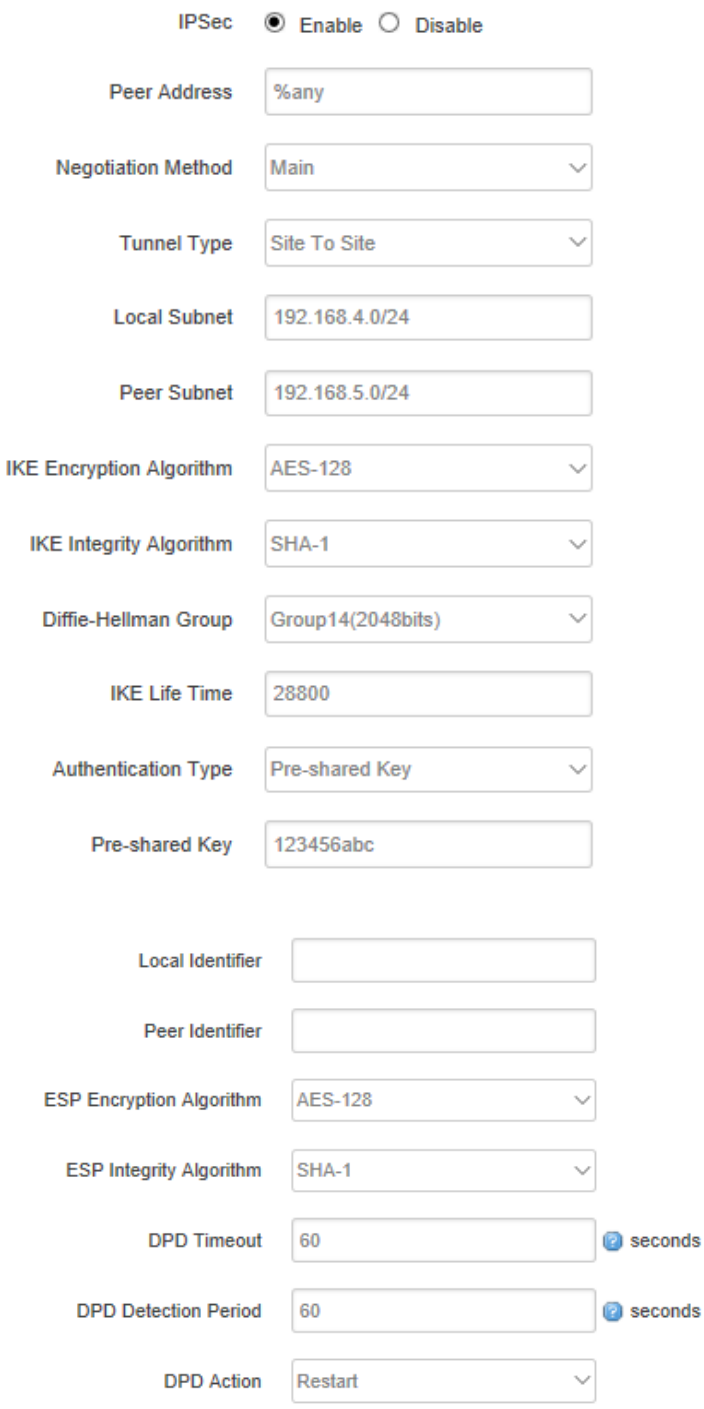
If topology is subnet, authentication type is certification. If it is point to point, you can choose none, certificate or static secret.

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 lifetime.

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.

3.5 Advanced

You can set up some advanced functions here.

3.5.1 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.

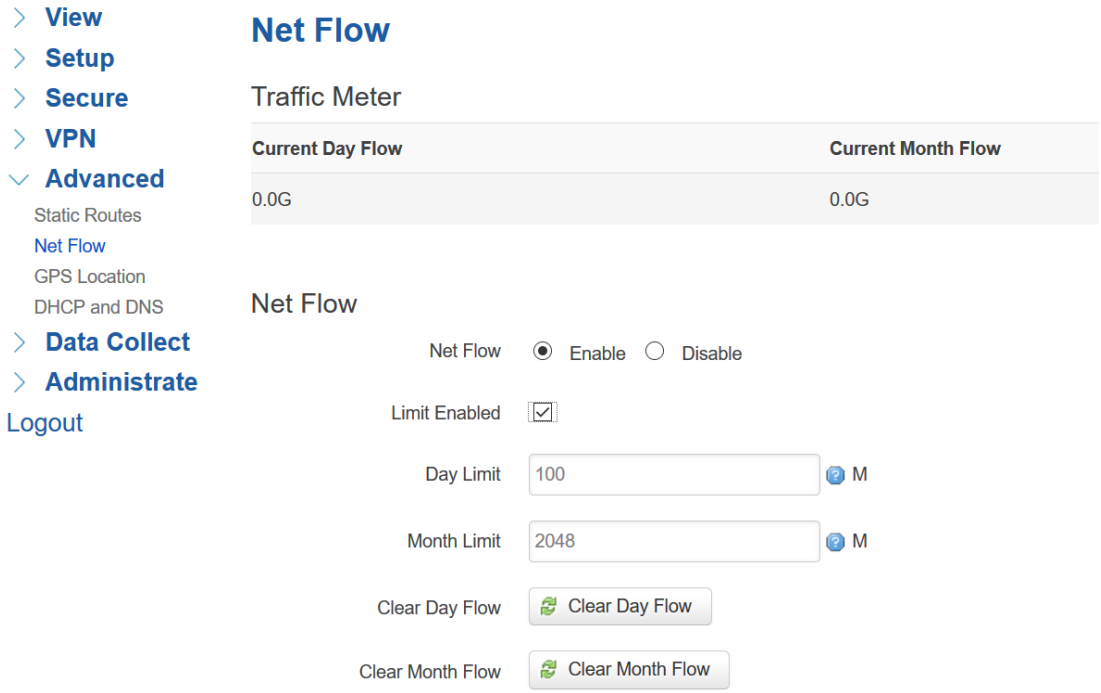
IPv4 Netmask: The netmask of subnet, if the target is host, the netmask shall be 255.255.255.255.

IPv4 Gateway: The address of next-hop gateway address.

Note: this address shall be achievable, or you'll fail to add static routing.

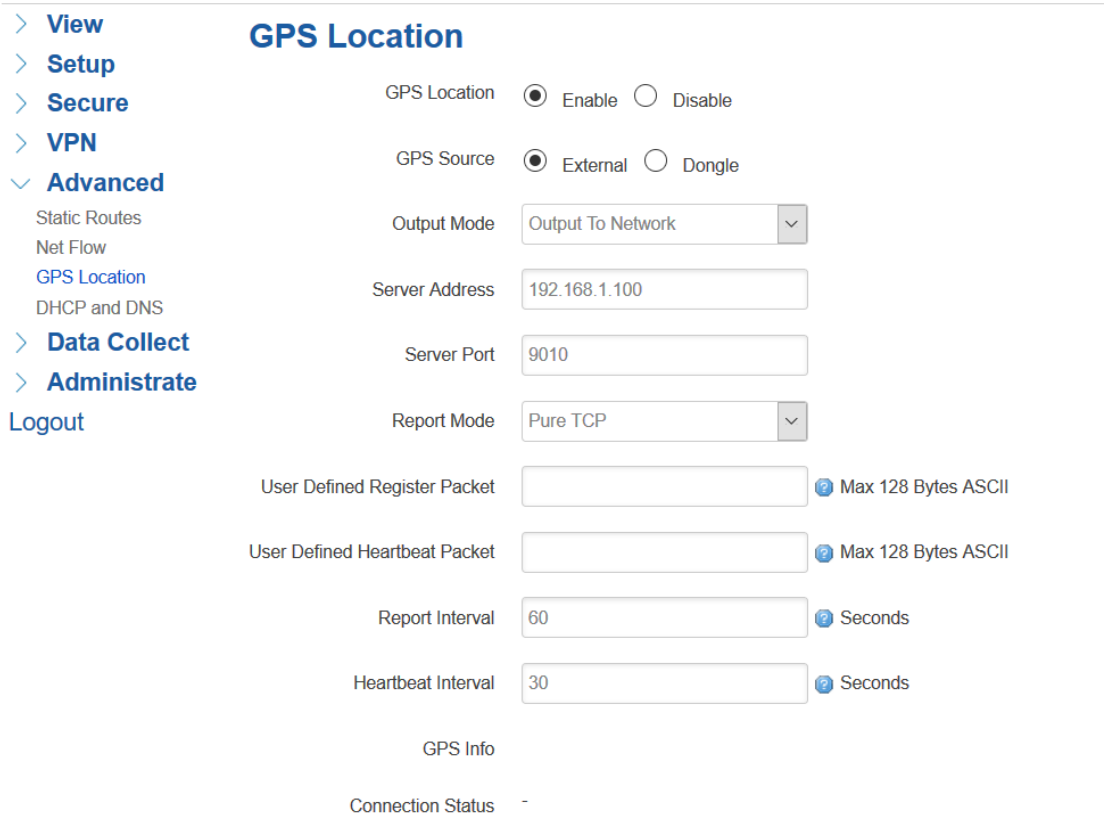
3.5.2 Net Flow

The traffic meter function of TG465 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.



3.5.3 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.



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.

3.5.4 DHCP and DNS

General DHCP and DNS settings base on “dnsmasq” tool on TG465. Please refer to “dnsmasq” for more information.

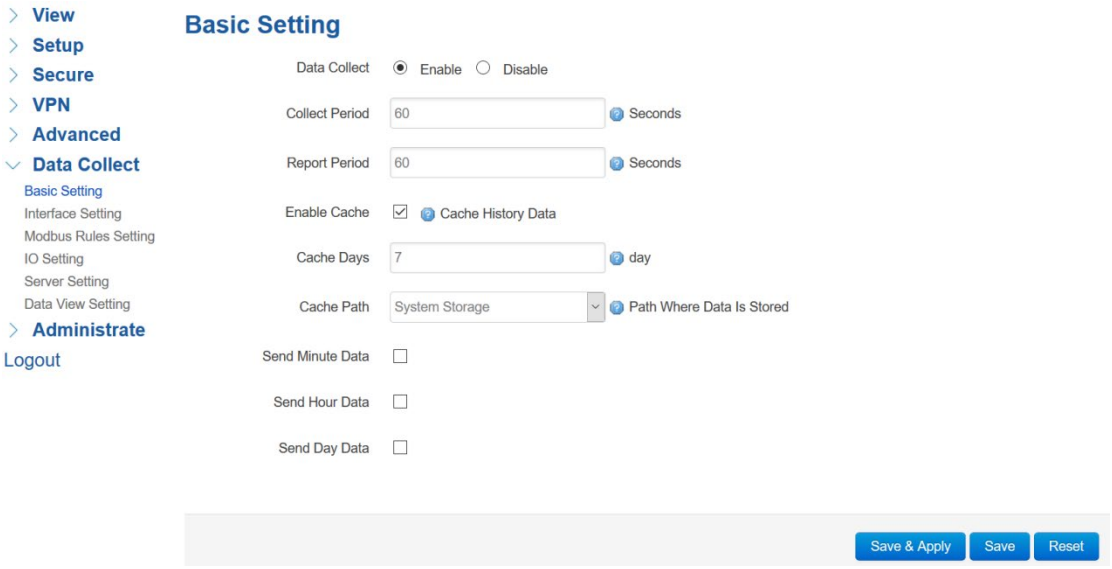
3.6 Data Collect

Data Collect settings is for TG465 acquiring data from slave devices in serial ports, Ethernet ports, IO 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.

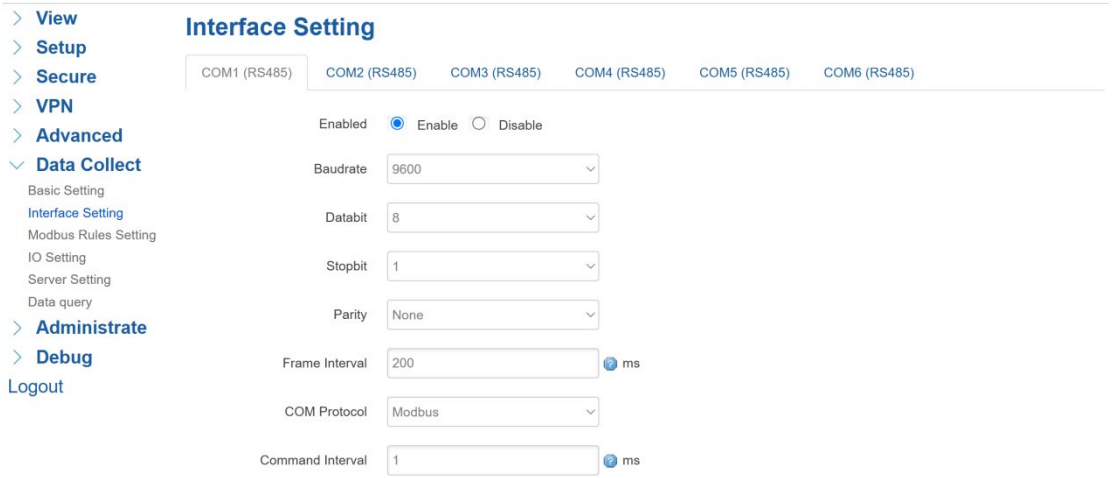
4) Enable Cache: Enable or Disable history data cache feature.

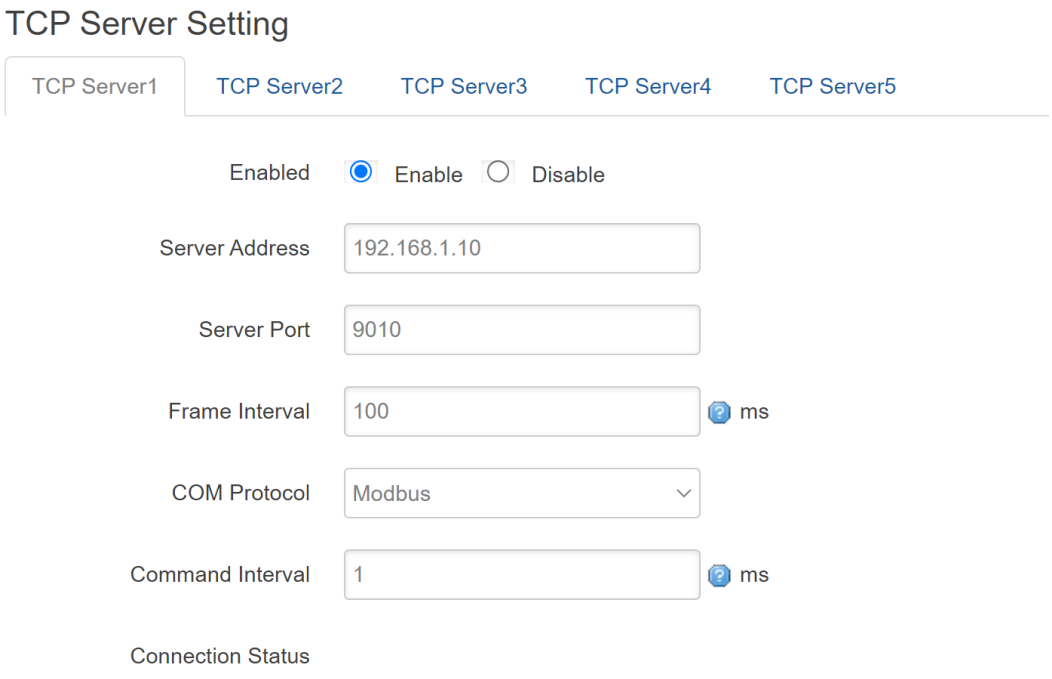
5) Related data cache setting if enable the cache feature.

3.6.2 Interface Setting

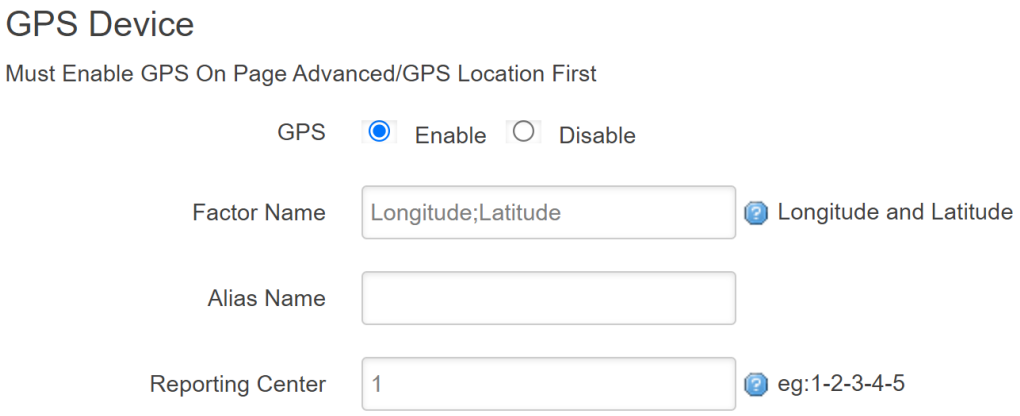
Serial Ports&TCP Ports:

Switch the hardware interfaces for data acquisition from kinds of slave devices. Including Serial ports (COM1~COM6), Modbus TCP base on Ethernet LAN.





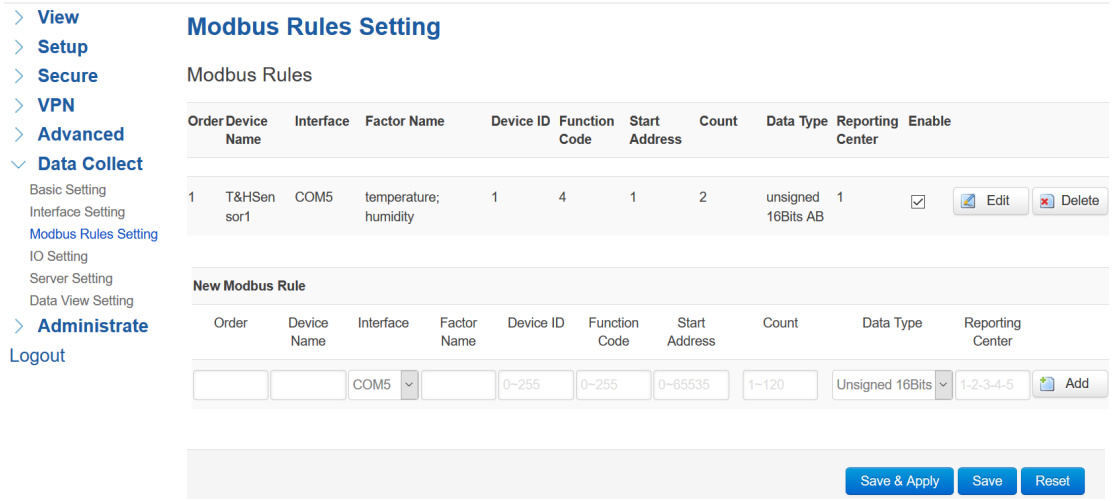
GPS Device: GPS location data can be reported to different kinds of servers, such as TCP and MQTT, if you would like to send GPS data to MQTT, need enable GPS function at Page Advanced/GPS Location First. Factor Name will be the Longitude and Latitude, separate by semicolon and set the number of Reporting Center.

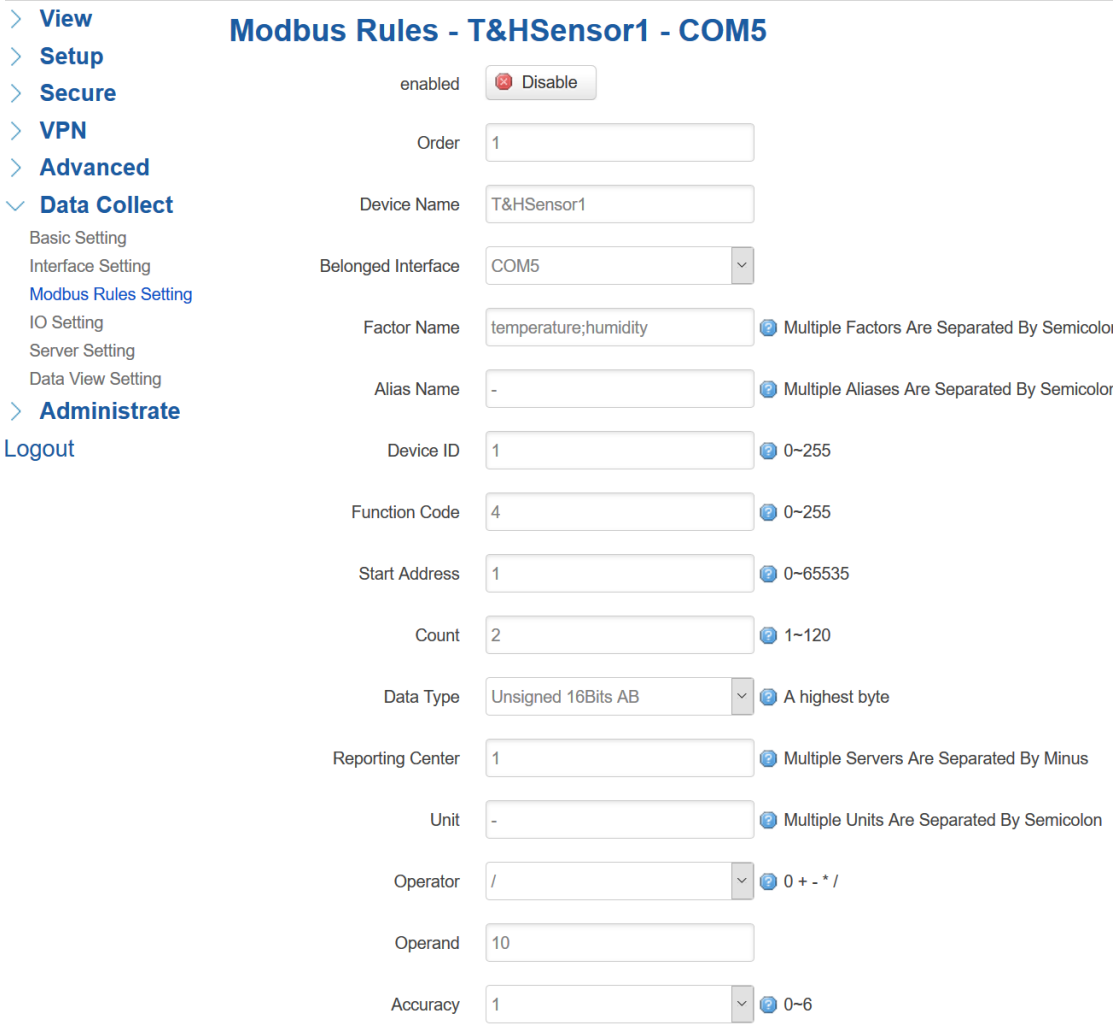


3.6.3 Modbus Rules Setting

Modbus Rules Setting is for TG465 as a Modbus master to acquire data from slave devices base on Modbus protocol. You can configure unlimited Modbus rules on it. TG465 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 the information.

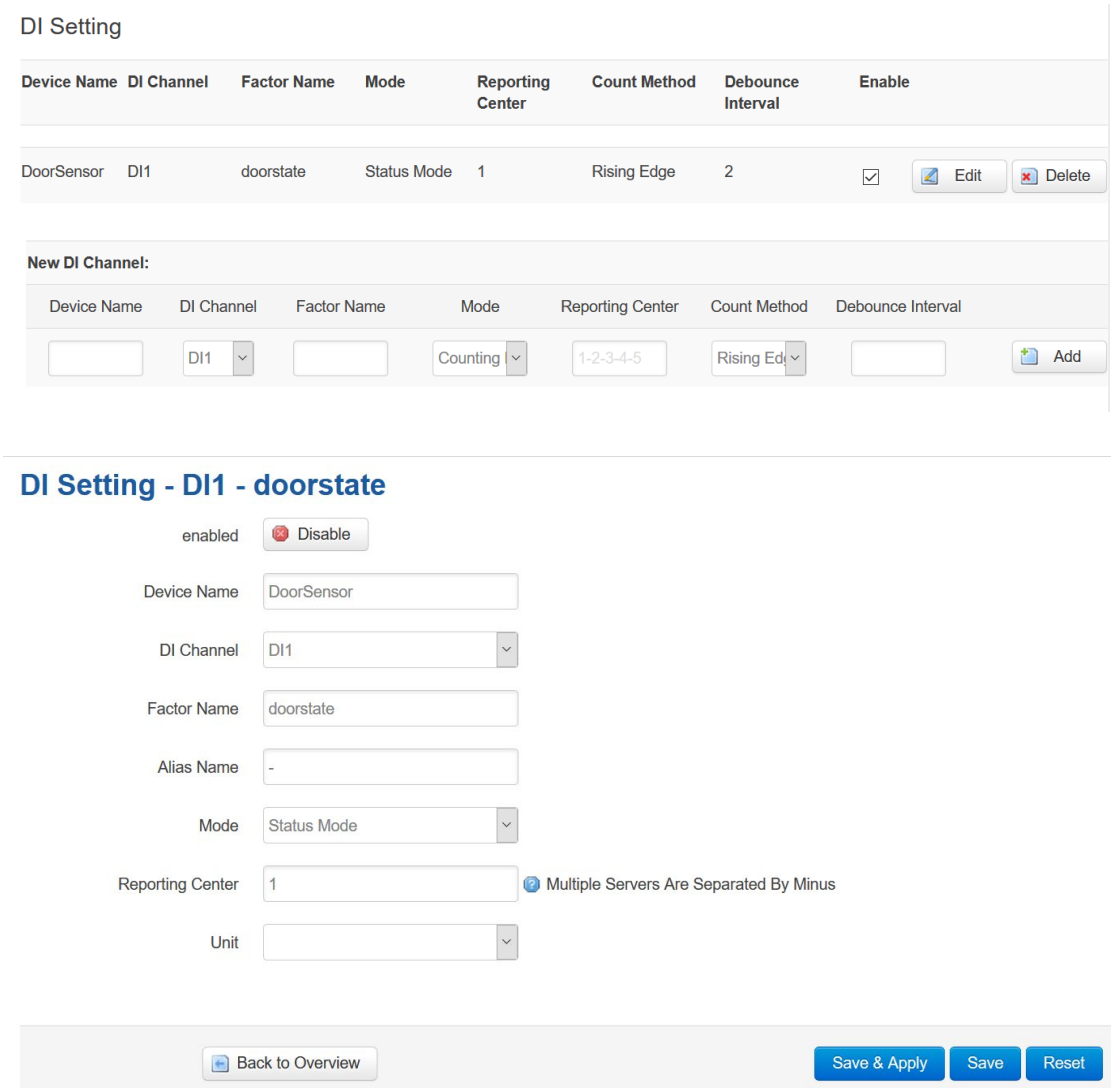




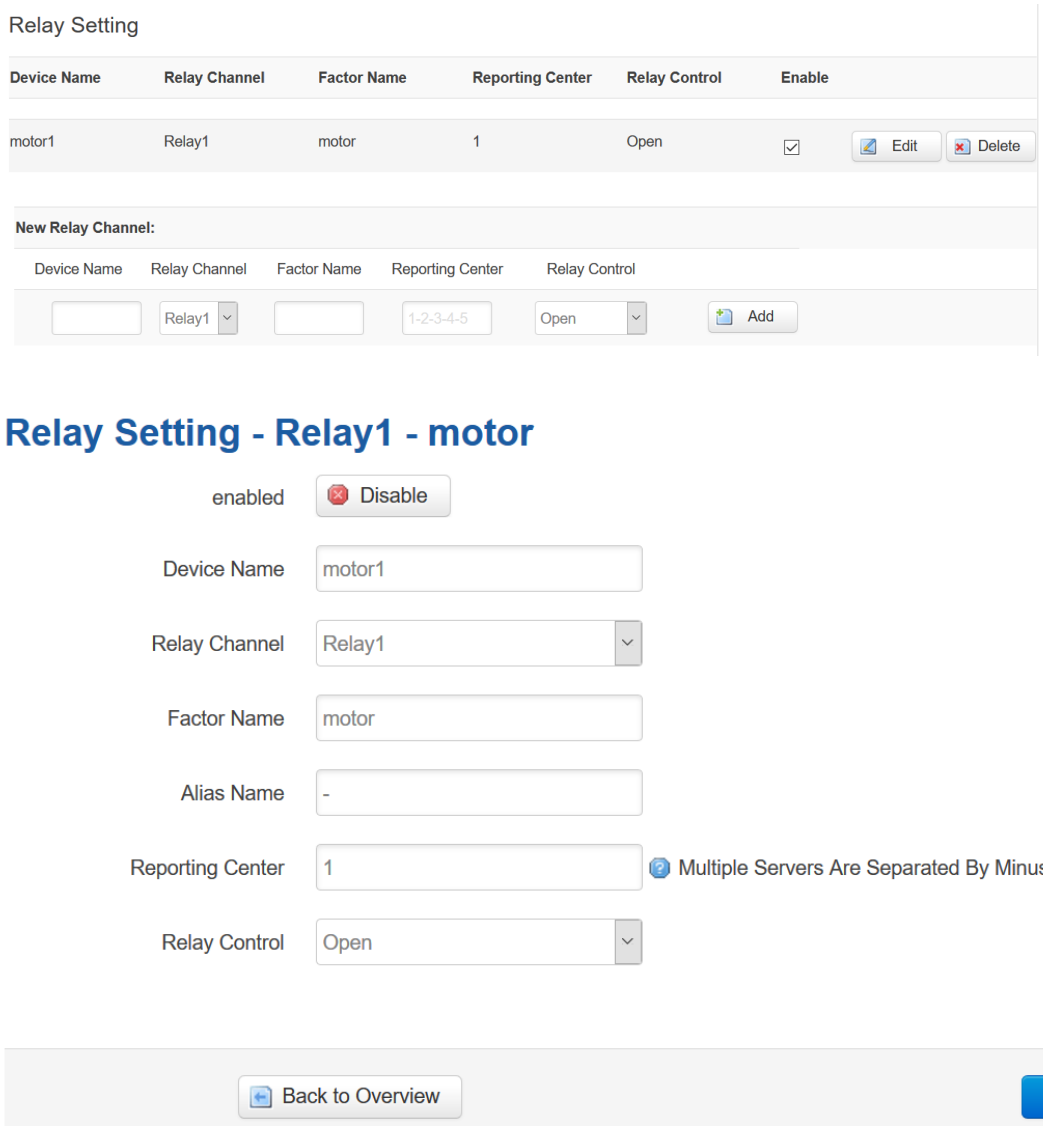
3.6.4 IO Setting

IO Setting menu is for setting DI ports, and Relay ports.

1) DI ports setting

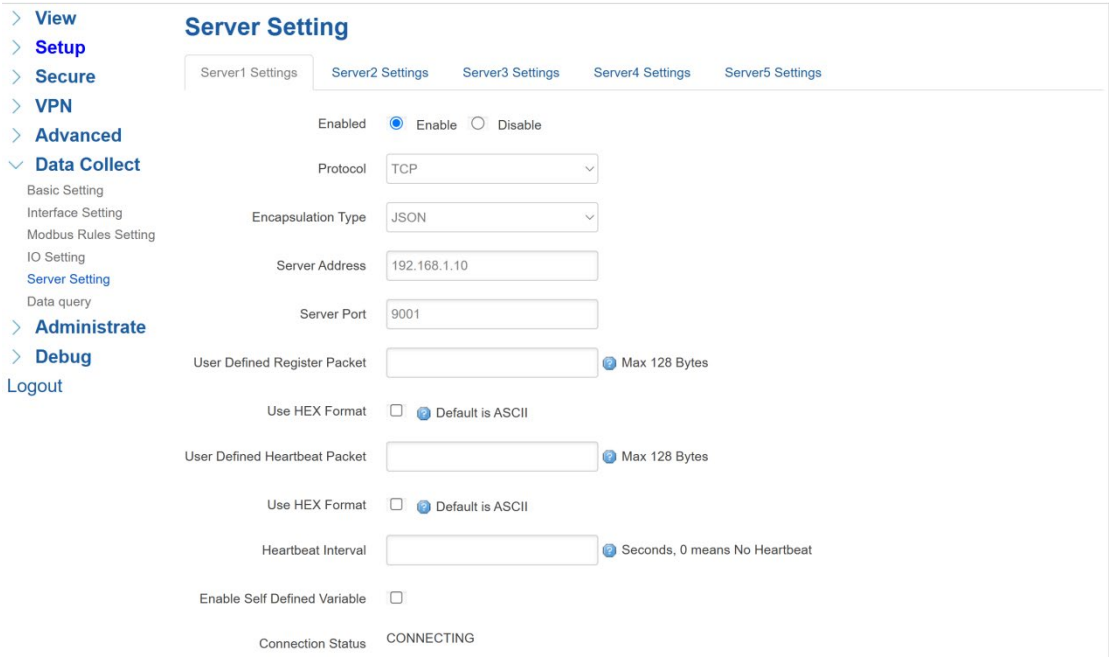


2) Relay Setting



3.6.5 Server Setting

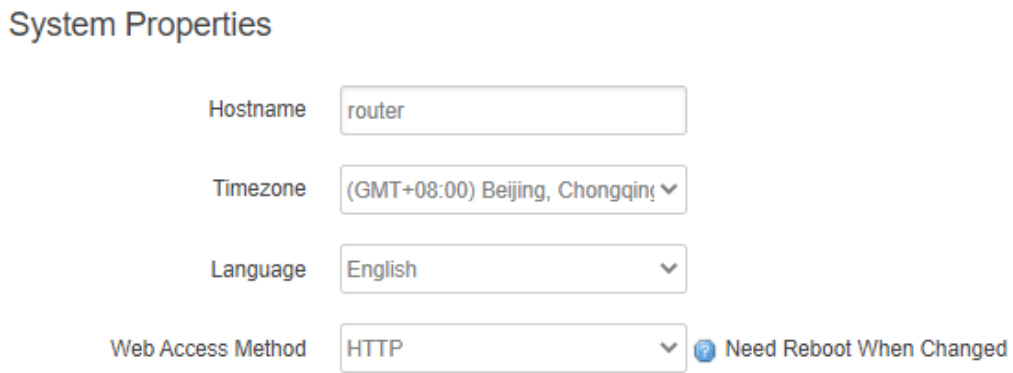
Server setting menu allows user set the data center address with multiple protocols, the standard TG465 support TCP, UDP, HTTP, MQTT, and Modbus TCP. For the data format, TG465 support different Encapsulation type, include “Transparent”, “JSON”, and “HJ212” (special for some Environment SCADA).TG465 accepts customize specific protocols for your data center too.



3.7 Administrate

In this menu, you can set up time zone, language (English and Chinese only now), time setting, firmware upgrade, etc.

3.7.1 System



1) Host Name

The host name of router, default name is router.

2) Time Zone

Set up the time zone of system, default time zone is GMT8.

3) Language

Change the language of configuration interface, default language is English.

4) Enable Telnet Access

To enable the telnet server, the default function is enabled.

5) Enable SSH Access

To enable the SSH server, the default function is disabled.

3.7.2 Password

To revise the login password of router.

1) Origin Password

You'll be required to enter your origin password before your revise your new password.

2) Password

Type the new password you want to change.

3) Confirmation

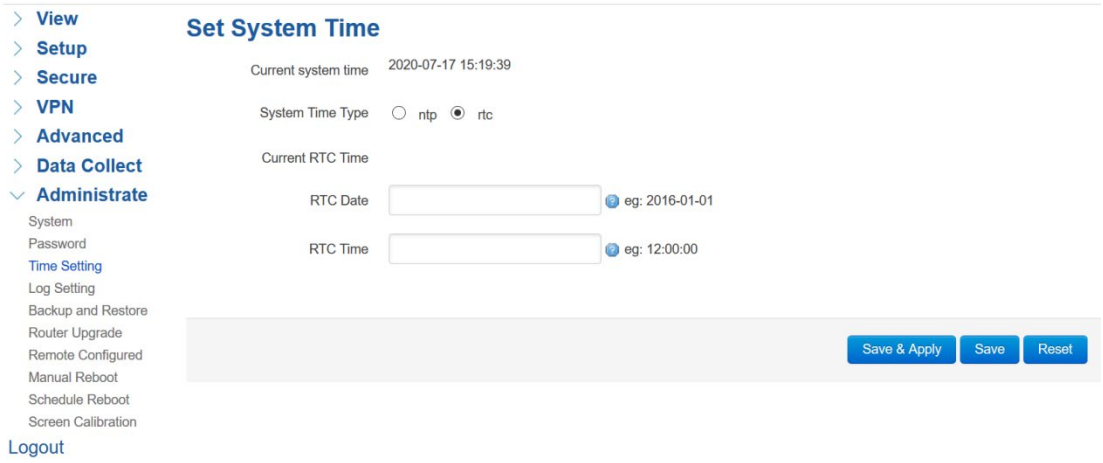
Type the new password again to confirm it.

If the new password and confirmation password you type is different, then it fails to revise the password. After password revised, router will return to login page, then you can enter your username and password.

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.

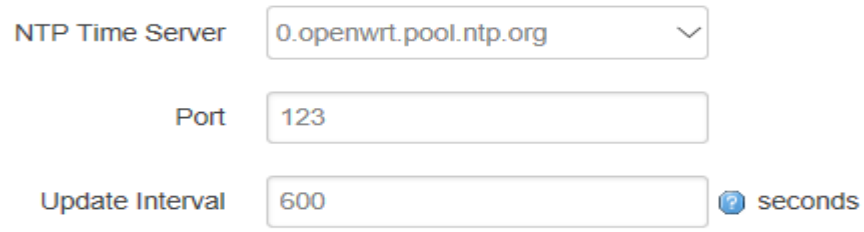
RTC Data

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 by yourself.

Port

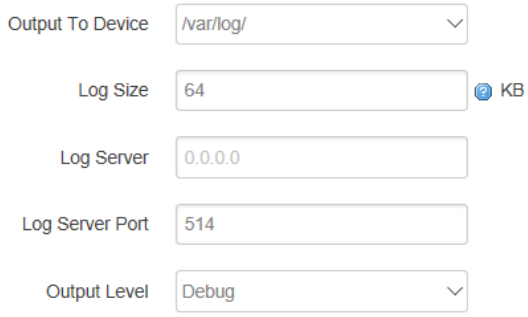
NTP time server port, default port is 123.

Update Interval

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

3.7.4 Log Settings

Log settings are 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

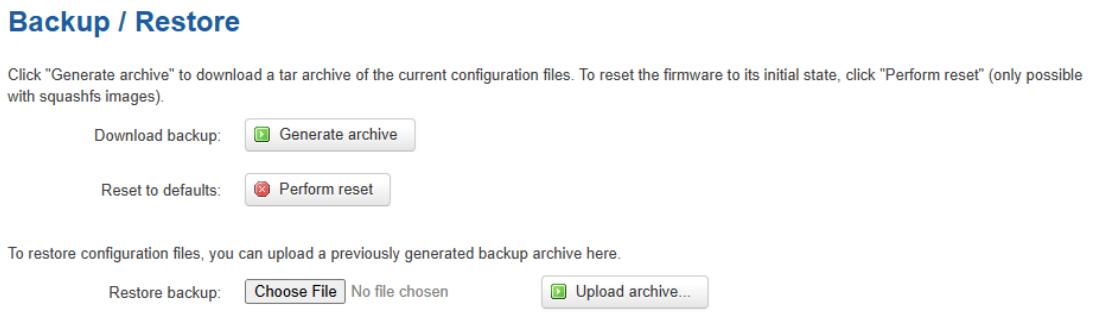
Set up the port of log server, default value is 514

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 Restore

User can either backup the configuration of router, or reset to factory defaults.



1) Download Backup

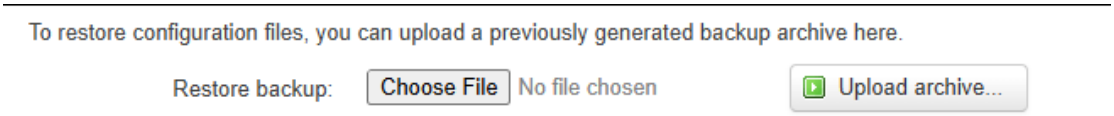
Click to generate a configuration file in format of “backup-router-2016-**-**.tar.gz”.

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.

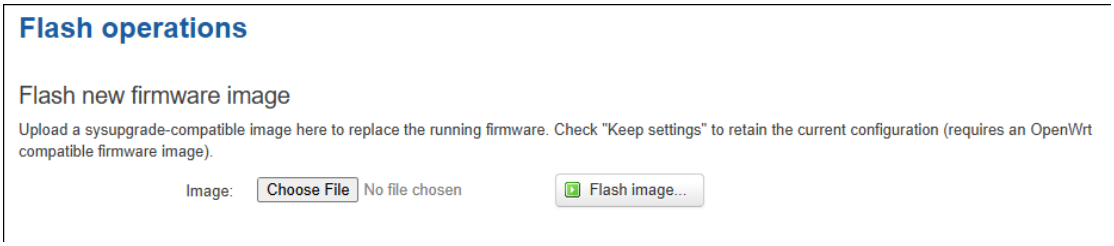
3) Restore Backup

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 Router Upgrade

Before you upgrade the firmware for router, make sure the firmware you’re planning to upload is correct. If errors occur, use serial port and connect the Ethernet cable, upgrade the firmware through u-boot.



1) Keep Settings

Click it, and system configuration will not be changed after firmware upgrade.

2) 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.

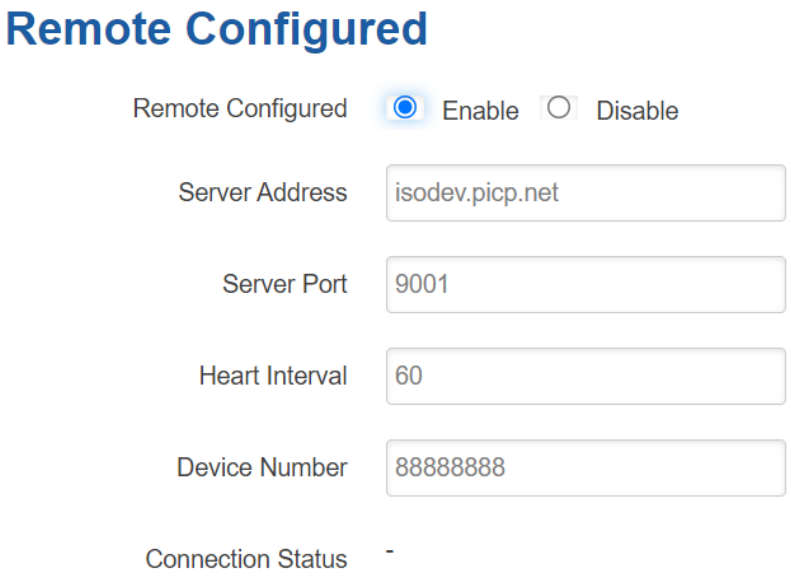
- **Proceed**

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

3.7.7 Remote Configured

Remote Configured feature allows TG465 to **work with Bivocom Device Management Platform(Option service)** 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.



1) Remote Configured

You can enable or disable this function to choose if you want to remote manage the router or not.

2) Server Address

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

3) Server Port

The specified login server port.

4) Heart Interval

The heartbeat time interval (Unit: second)

5) Device Number

Device ID of router.

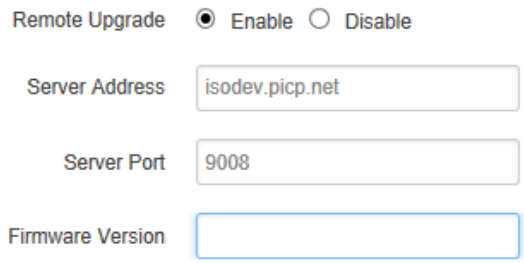
6) Device Phone Number

The phone number of SIM card insert in router.

7) Device Type

Type of the device, default is router.

You can also remote upgrade the firmware for router, as below.



8) Remote Upgrade

Click ‘Enable’ to enable remote firmware upgrade function.

9) Server Address

Type the server IP address or Domain Name for remote upgrade.

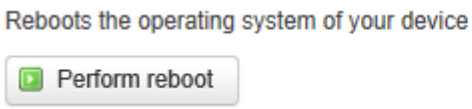
10) Server Port

Type the server port for remote upgrade.

11) Firmware Version

Type the firmware version that you want to upgrade remotely.

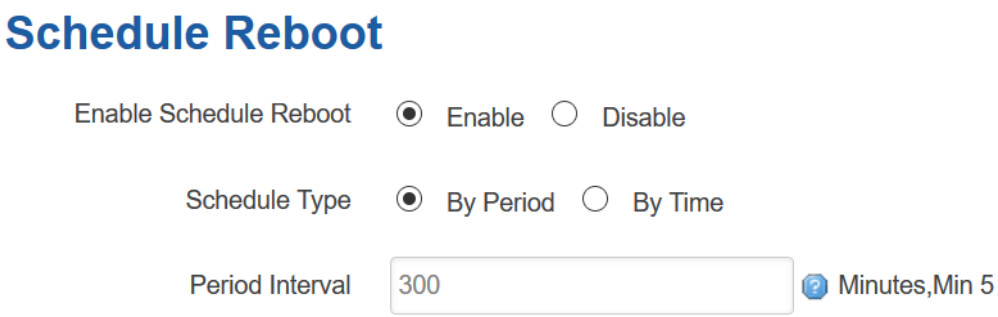
3.7.8 Manual Reboot



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 allows user to configure the period or dedicate time for device reboot.



Note: if you have any other questions about Bivocom products, please contact Bivocom support@bivocom.com.

3.8 Logout

Click the Logout menu to logout the web UI of TG465.