Bivocom®

Industrial Cellular Edge Gateway TG462 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

Xiamen Bivocom Technologies Co., Ltd.
Addr: Unit 1504, No. A1 Building, 3rd Software Park, Xiamen, China 361000
Tel.: +86-592-6090 133
Fax: +86-592-6211727
Email: support@bivocom.com
sales@bivocom.com
www.bivocom.com

About This Guide

Thank you for choosing Bivocom Industrial Cellular Edge Gateway TG462 Series.

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

This manual is compatible with below models

Model	Description
TG462	Industrial Edge Gateway
TG462S	Industrial Edge Gateway with Touch screen

Table of Contents

1. Introduction

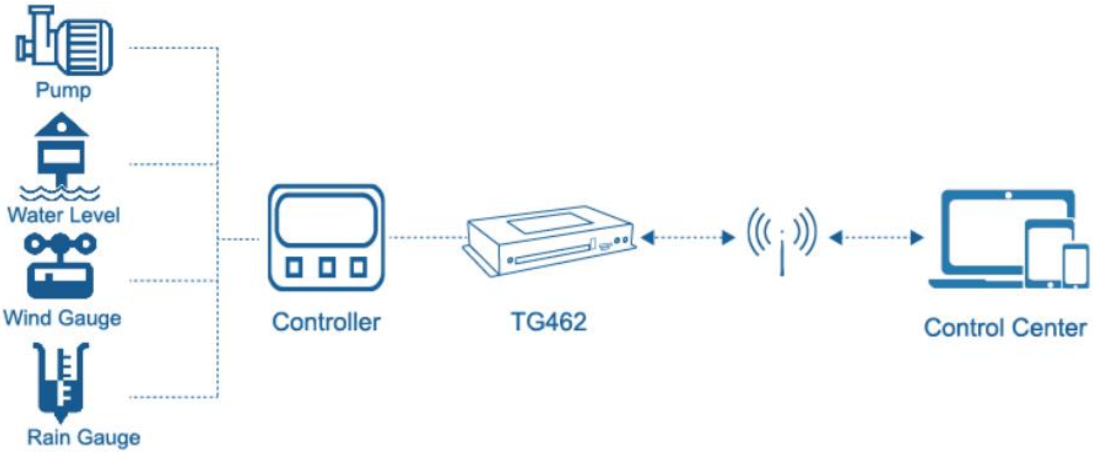
1.1 Overview

TG462/TG462S Industrial cellular Edge Gateways are designed for connecting diverse types of field sensors and equipment to cloud via LTE/3G cellular network, which is suitable for IIoT and M2M applications that require secure and rugged LTE connectivity in harsh environment, such as water&waste water, gas&oil, industry 4.0, smart city, vending machines, etc.

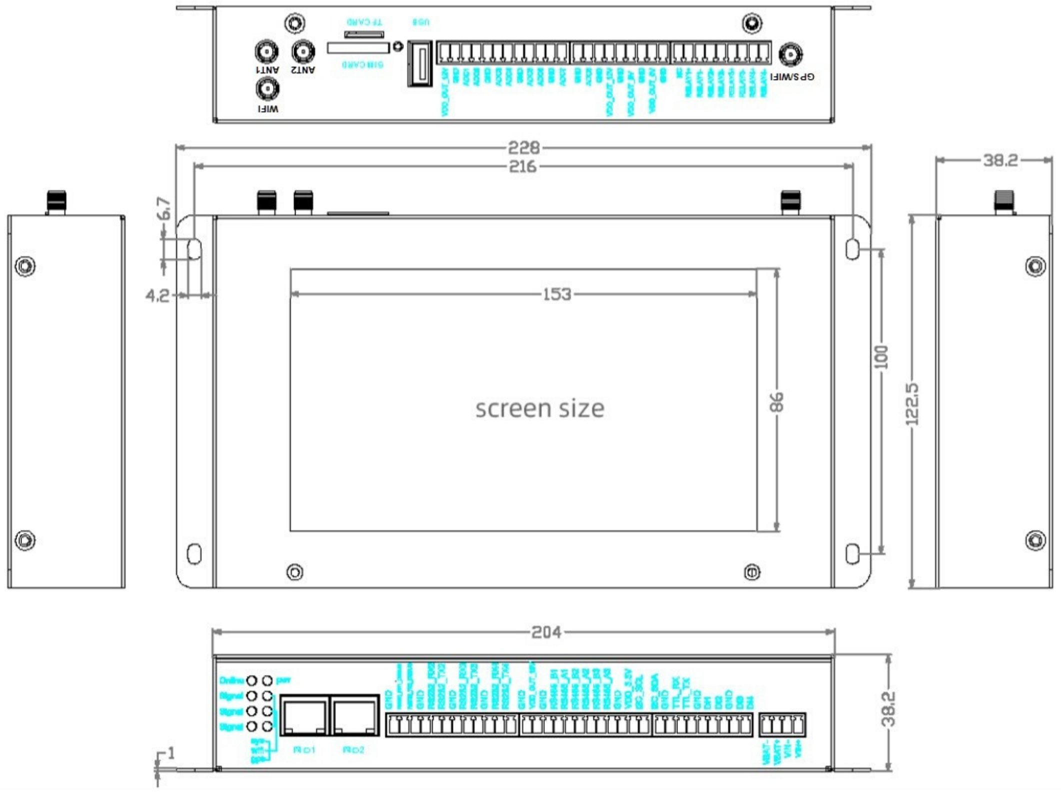
With rich interfaces, includes Ethernet ports, RS232/RS485, digital inputs, analog inputs, relay outputs, I2C, power output, USB, GPS, WIFI, etc., The TG462/TG462S Edge Gateways allow users to integrate legacy systems with modern sensors. With high-performance 32-bit ARM-based CPU, Modbus RTU/TCP, MQTT, TCP/IP, and customized protocols, as well as up to 1G flash and 32G micro SD local data storage, enables users to collect, store and process data at IoT edge network. Besides, TG462S embedded with a 7inch HD TFT touch screen provides a better user experience for field data display and maintenance.

1.2 Applications

TG462 Series Edge Gateways utilizes cellular network to connect your edge devices and controller devices to your center for remote monitoring and control.
Typical application as below.



1.3 Dimensions



1.4 Physical Characteristics

Physical Characteristics	
Housing	Metal, IP30
Dimensions	228×122.5×38.2mm(8.97x4.82x1.50in), Antenna and other accessories not included
Weight	TG462: 850g(1.87lbs), TG462S: 900g(1.98lbs), without accessories.

2. Getting Started

2.1 Package Checklist

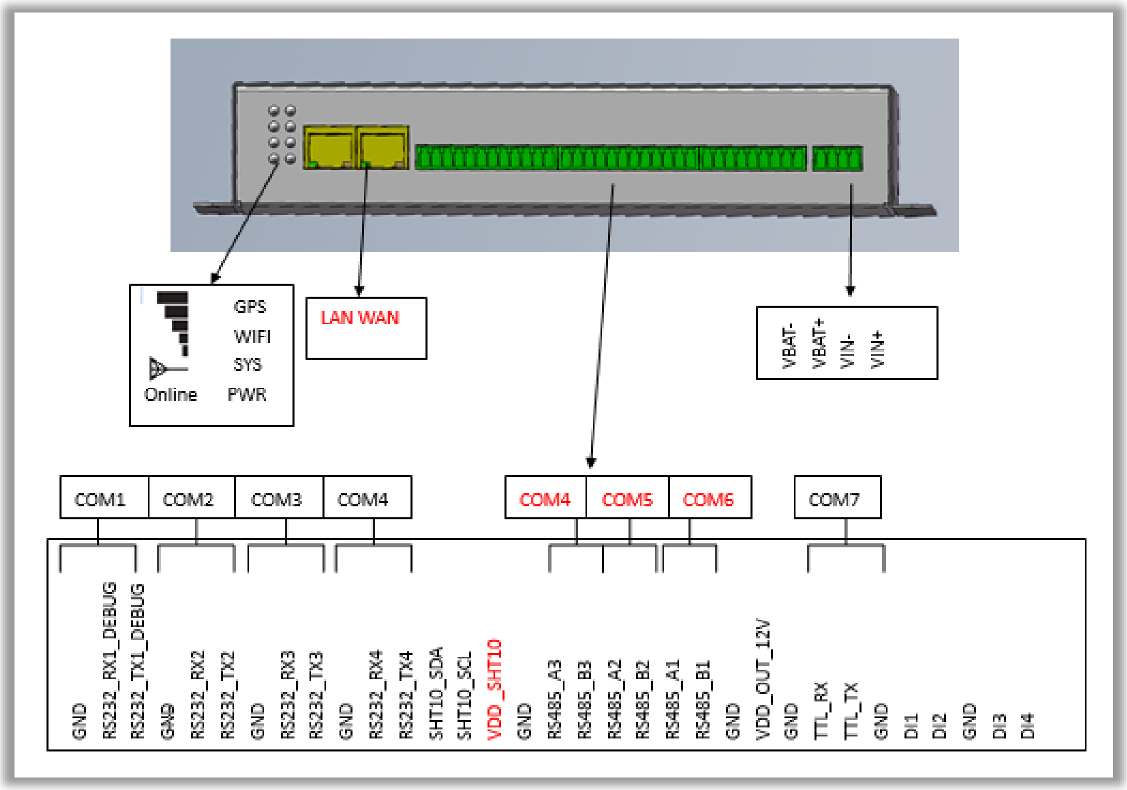
The following components are included in your TG462 package.
Check the list before installation. If you find anything missing, Please feel free to contact Bivocom.

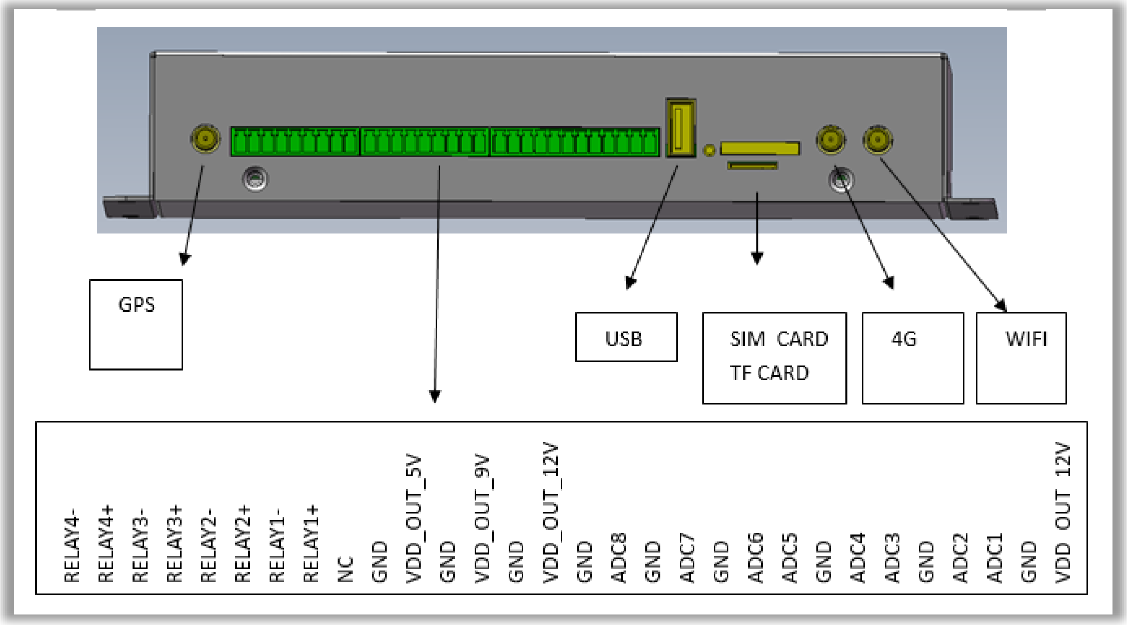
1 x TG462/TG462S Gateway
1 x Power Adapter (DC 12V/1.5A, EU/US/UK/AU plug optio)

2 x Mag-mount Cellular Antenna (SMA Male, 1 meter, 5dBi)
1 x RS232 Cable (DB9 Female, 1 meter)
1 x Ethernet Cable (1 meter)
3 x 12-Pin Terminal Block
3 x 9-Pin Terminal Block
1 x 4-Pin Terminal Block (Power)
1 x Quick Start Guide (Printed)*

2.2 Installation

Hardware interfaces instruction:





2.2.1 SIM/UIM Card

TG462 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 Interfaces connection

TG462 support a RS232 (com1) serial port as console port, which can be used for firmware upgrade, system log checking, debug, etc.
TG462 include 3 RS232 (com1, com2, com3), and 3 RS485 (com4, com5, com6, while com4 can be used as RS232 as well.), 1x I2C, 1x TTL, 4x DI, 8x ADC (12 bit AD, support 4~20mA current or 0-5V voltage signal input), 4x Relay, 5x power supply.

TG462 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	TG462 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 TG462(SMA female port), make sure it is screwed tightly to ensure the strength of signal.

2.3 LED Indicators

TG462 Series Gateway provides 8 LED indicators, as following.

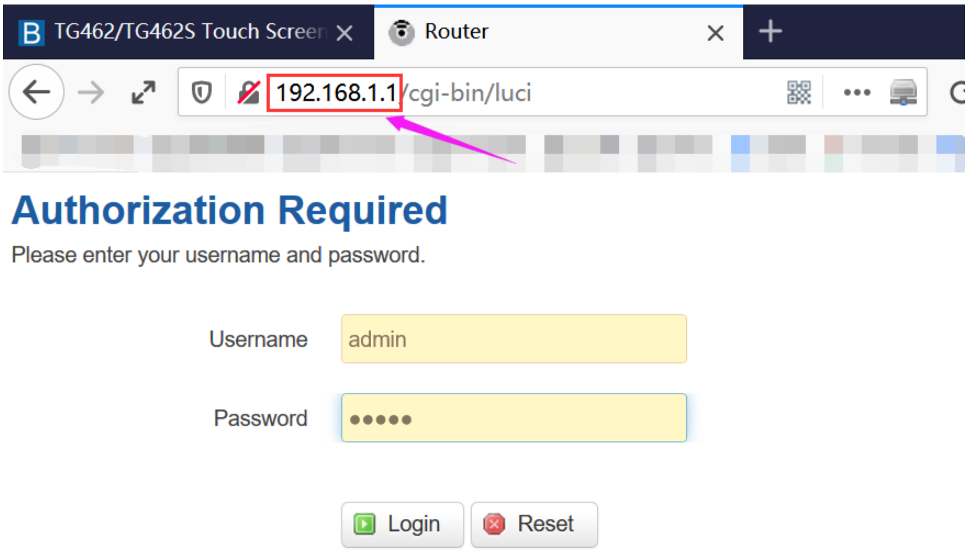
Indicator	Status	Content
Power	On	Powered On
	Off	Powered Off
Signal	1 Lights	Signal weak

Strength	2 Lights	Signal Middium
	3 Lights	Signal Strong
System	Blink	System works perfect
	Off	System doesn’t work
GPS	On	GPS attached the location
	Off	GPS not attached the location
Online	On	Router accesses to Internet
	Off	Router doesn’t access to Internet
Wifi	On	Wifi enabled
	Off	Wifi disabled
WAN	On	WAN is connected
	Off	WAN is not connected
LAN	Blink	LAN works
	Off	LAN is not connected

3. Configuration and Management

Use an Ethernet cable to connect the LAN port of TG462 to your laptop, or use your laptop or mobile phone to connect to WIFI hotspot ‘Bivocom’ of TG462, login with password: admin123, normally your laptop will get an IP address from TG462 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.



Authorization Required

Please enter your username and password.

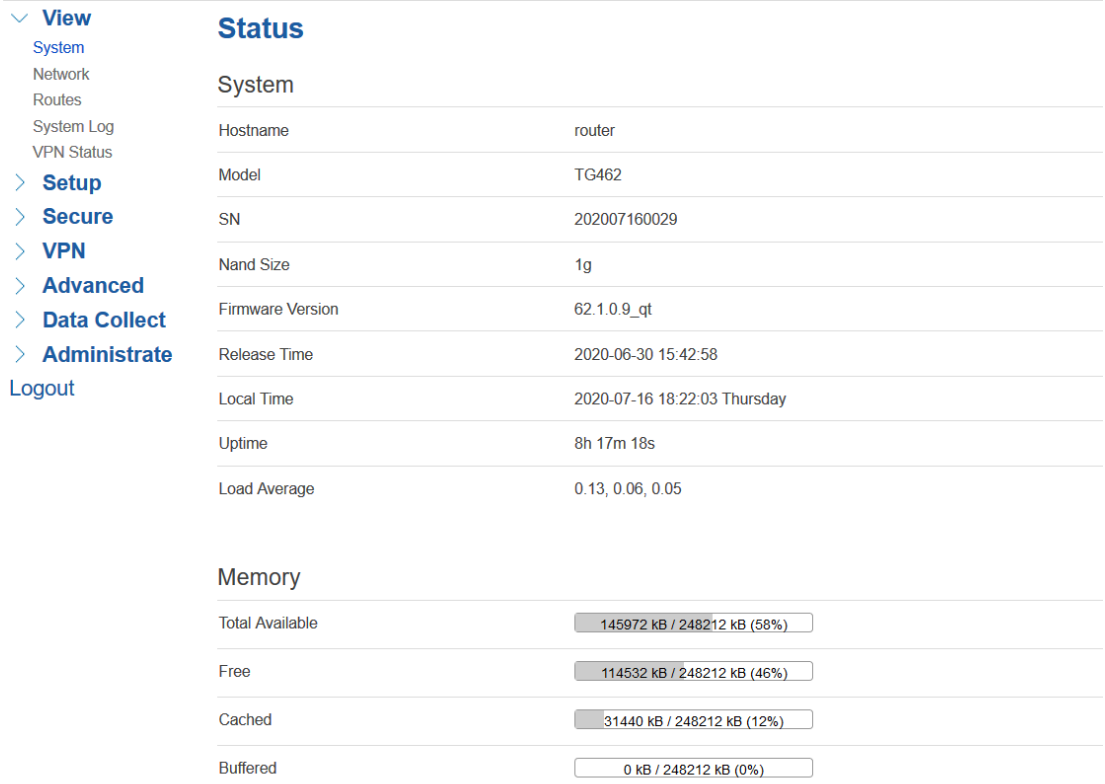
Username	admin
Password	•••••

3.1 View

To check the following system information.

3.1.1 System

Display system related information.



Status

System

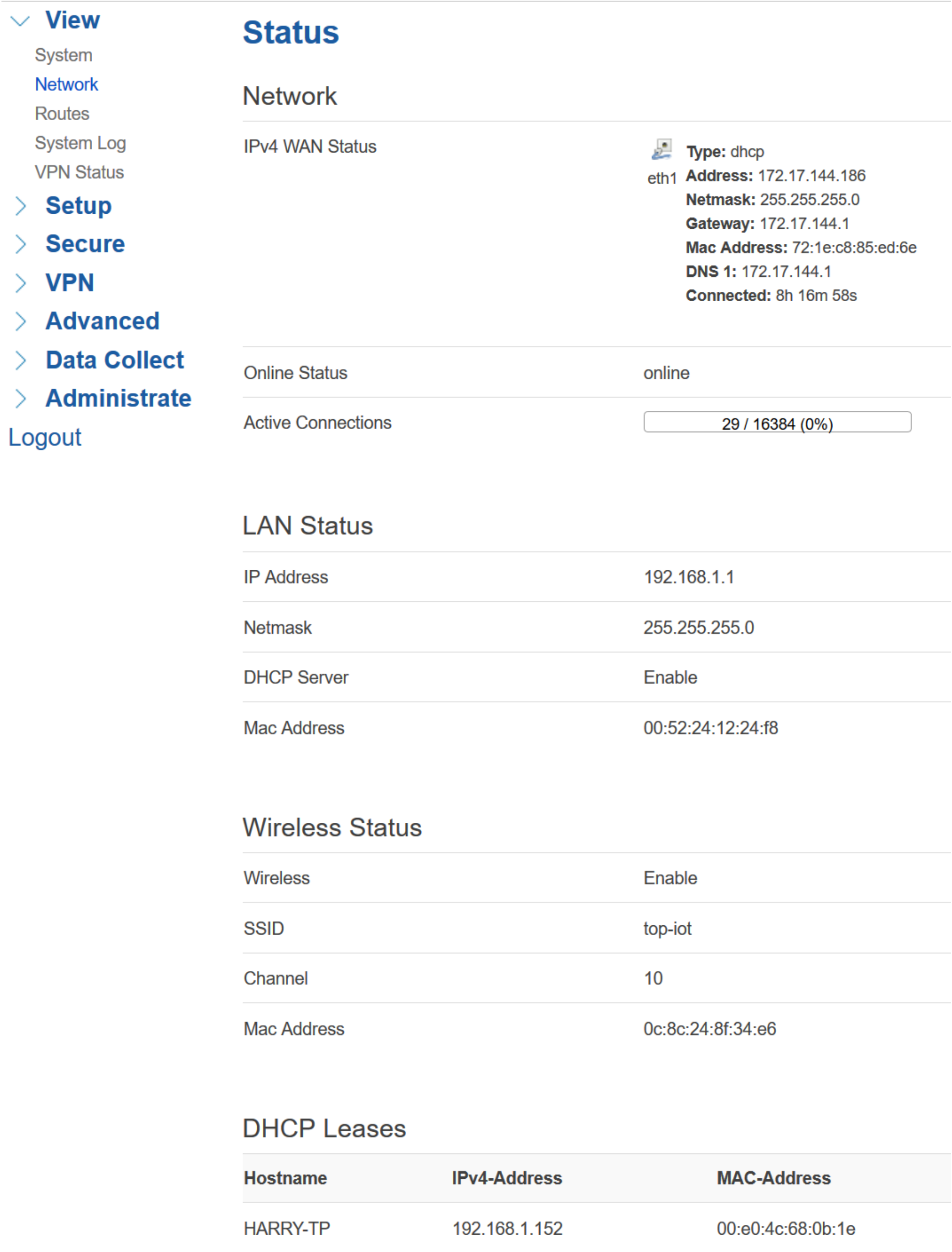
Hostname	router
Model	TG462
SN	202007160029
Nand Size	1g
Firmware Version	62.1.0.9_qt
Release Time	2020-06-30 15:42:58
Local Time	2020-07-16 18:22:03 Thursday
Uptime	8h 17m 18s
Load Average	0.13, 0.06, 0.05

Memory

Total Available	145972 kB / 248212 kB (58%)
Free	114532 kB / 248212 kB (46%)
Cached	31440 kB / 248212 kB (12%)
Buffered	0 kB / 248212 kB (0%)

3.1.2 Network

Display WAN, LAN, WiFi, DHCP network information.



Status

Network

IPv4 WAN Status	eth1 **Type:** dhcp **Address:** 172.17.144.186 **Netmask:** 255.255.255.0 **Gateway:** 172.17.144.1 **Mac Address:** 72:1e:c8:85:ed:6e **DNS 1:** 172.17.144.1 **Connected:** 8h 16m 58s
Online Status	online
Active Connections	29 / 16384 (0%)

LAN Status

IP Address	192.168.1.1
Netmask	255.255.255.0
DHCP Server	Enable
Mac Address	00:52:24:12:24:f8

Wireless Status

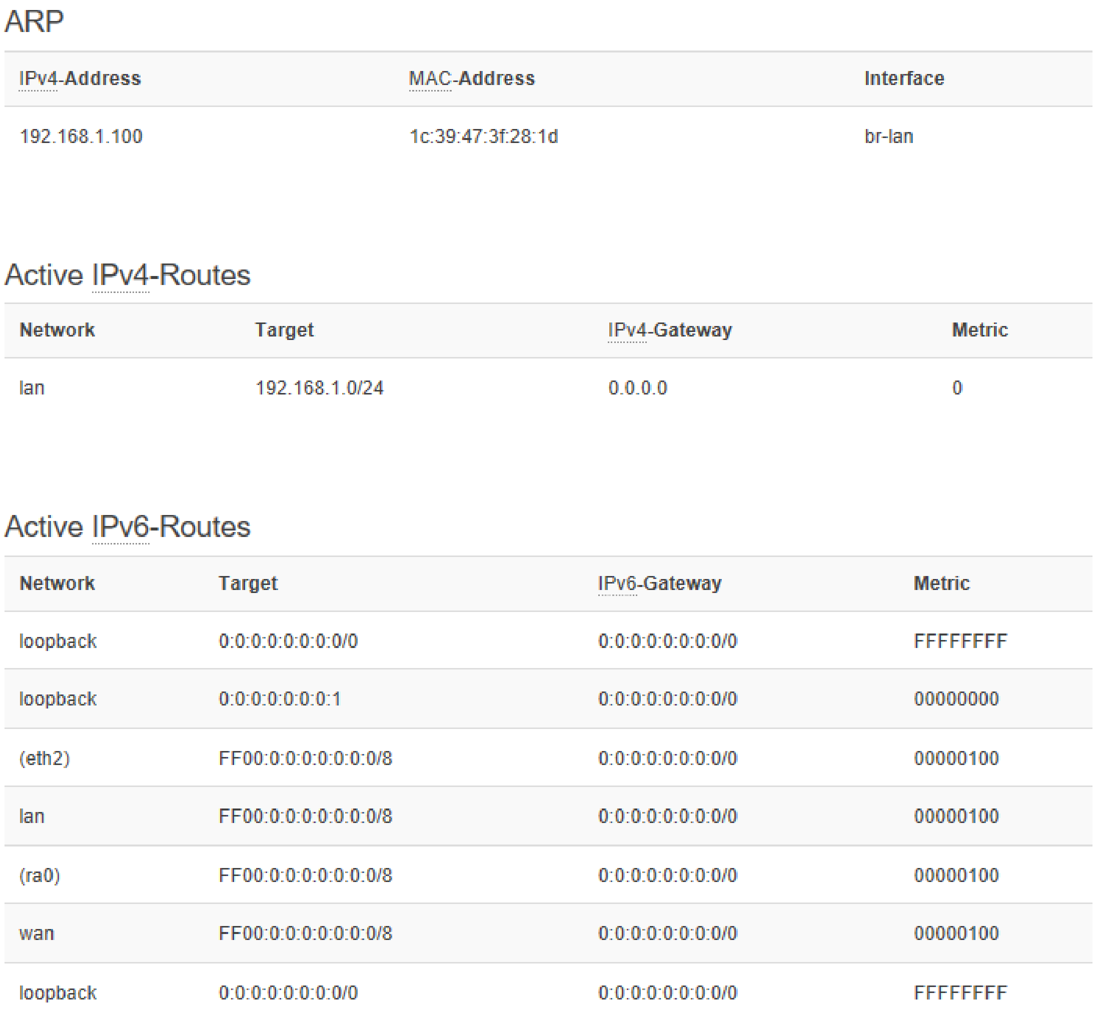
Wireless	Enable
SSID	top-iot
Channel	10
Mac Address	0c:8c:24:8f:34:e6

DHCP Leases

Hostname	IPv4-Address	MAC-Address
HARRY-TP	192.168.1.152	00:e0:4c:68:0b:1e

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

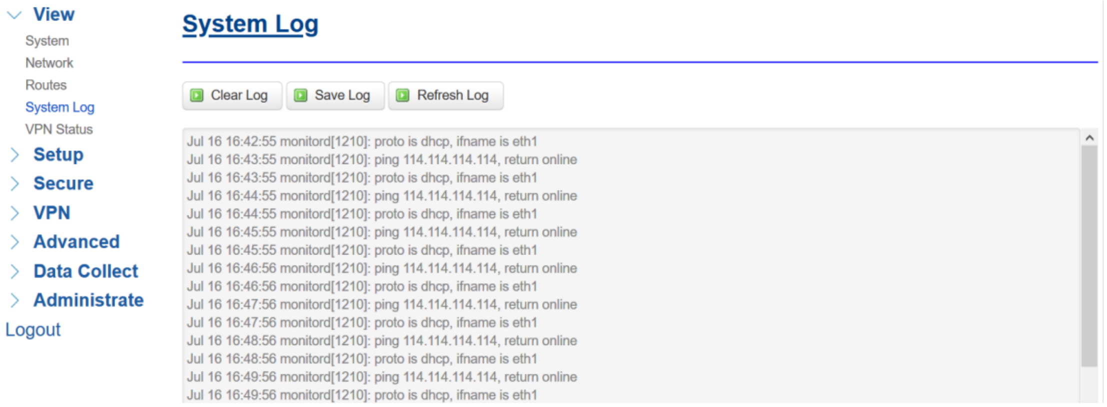
Network	Target	IPv4-Gateway	Metric
lan	192.168.1.0/24	0.0.0.0	0

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

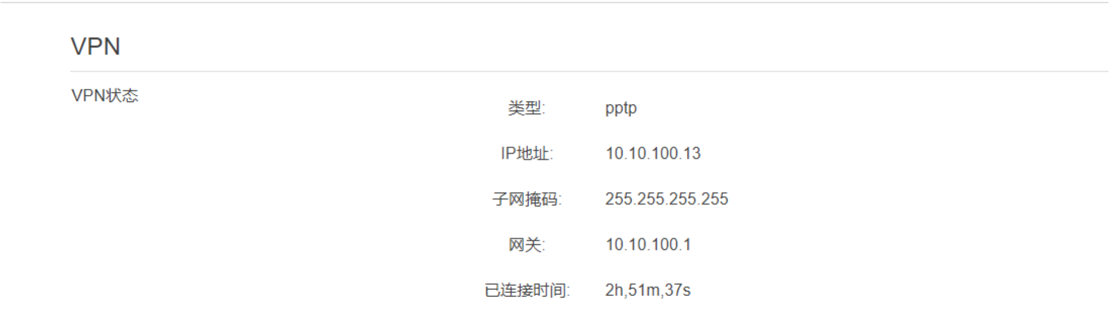
Display system log.



```
Jul 16 16:42:55 monitord[1210]: proto is dhcp, ifname is eth1
Jul 16 16:43:55 monitord[1210]: ping 114.114.114.114, return online
Jul 16 16:43:55 monitord[1210]: proto is dhcp, ifname is eth1
Jul 16 16:44:55 monitord[1210]: ping 114.114.114.114, return online
Jul 16 16:44:55 monitord[1210]: proto is dhcp, ifname is eth1
Jul 16 16:45:55 monitord[1210]: ping 114.114.114.114, return online
Jul 16 16:45:55 monitord[1210]: proto is dhcp, ifname is eth1
Jul 16 16:46:56 monitord[1210]: ping 114.114.114.114, return online
Jul 16 16:46:56 monitord[1210]: proto is dhcp, ifname is eth1
Jul 16 16:47:56 monitord[1210]: ping 114.114.114.114, return online
Jul 16 16:47:56 monitord[1210]: proto is dhcp, ifname is eth1
Jul 16 16:48:56 monitord[1210]: ping 114.114.114.114, return online
Jul 16 16:48:56 monitord[1210]: proto is dhcp, ifname is eth1
Jul 16 16:49:56 monitord[1210]: ping 114.114.114.114, return online
Jul 16 16:49:56 monitord[1210]: proto is dhcp, ifname is eth1
```

3.1.5 VPN Status

Display VPN status.



VPN

VPN状态

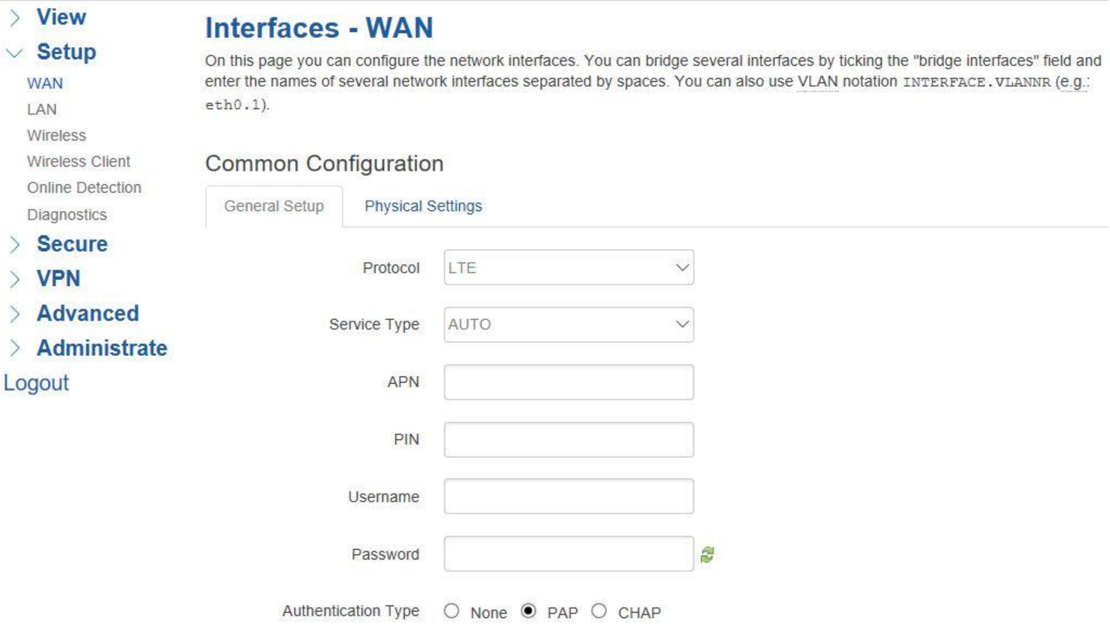
类型:	pptp
IP地址:	10.10.100.13
子网掩码:	255.255.255.255
网关:	10.10.100.1
已连接时间:	2h,51m,37s

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/3G/LTE connection mode.
Choose the mode you need, then click ‘Switch Connection Mode’ and configure the related parameters, then you can connect to the internet.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Protocol	LTE
Service Type	AUTO
APN	
PIN	
Username	
Password	
Authentication Type	○ None ● PAP ○ CHAP

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

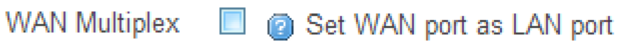
If there have username and password, you need to choose authentication type.

- 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 4G/3G/2G cellular network to access internet, you can change the WAN to act as a LAN port.



WAN Multiplex □ ? Set WAN port as LAN port

3.2.2 LAN

3.2.3 Wireless (Option)

3.2.4 Online Detection

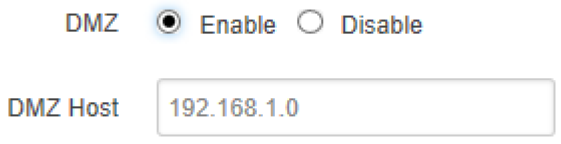
3.2.5 Diagnostics

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.



DMZ ● Enable ○ Disable

DMZ Host 192.168.1.0

1) DMZ

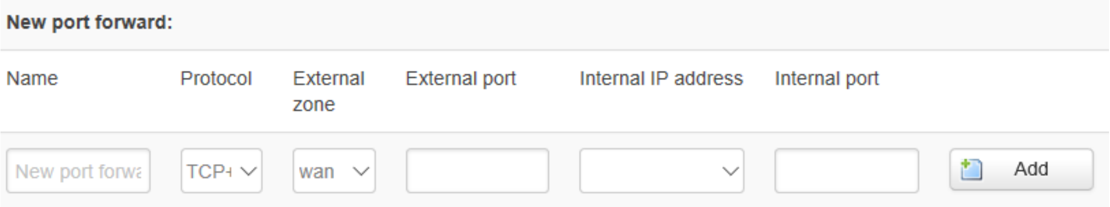
You can enable or disable the DMZ.

2) DMZ Host

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

3.2.2 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.



New port forward:

Name	Protocol	External zone	External port	Internal IP address	Internal port	
New port forwa	TCP+	wan				Add

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.

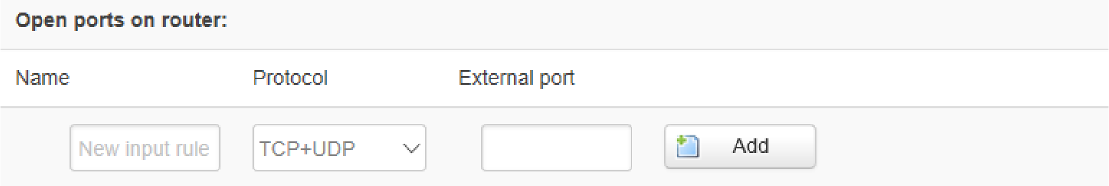
5) Internal Port

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.



Open ports on router:

Name	Protocol	External port	
New input rule	TCP+UDP		Add

1) Name

You can name the rule yourself.

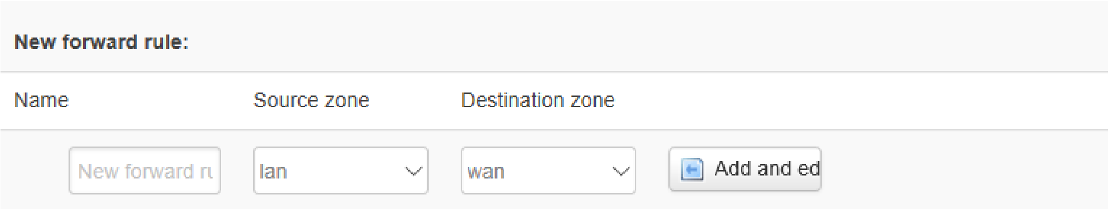
2) Protocol

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.


New forward rule:

Name	Source zone	Destination zone
New forward ru	lan	wan

1) Name

You can name the rule yourself.

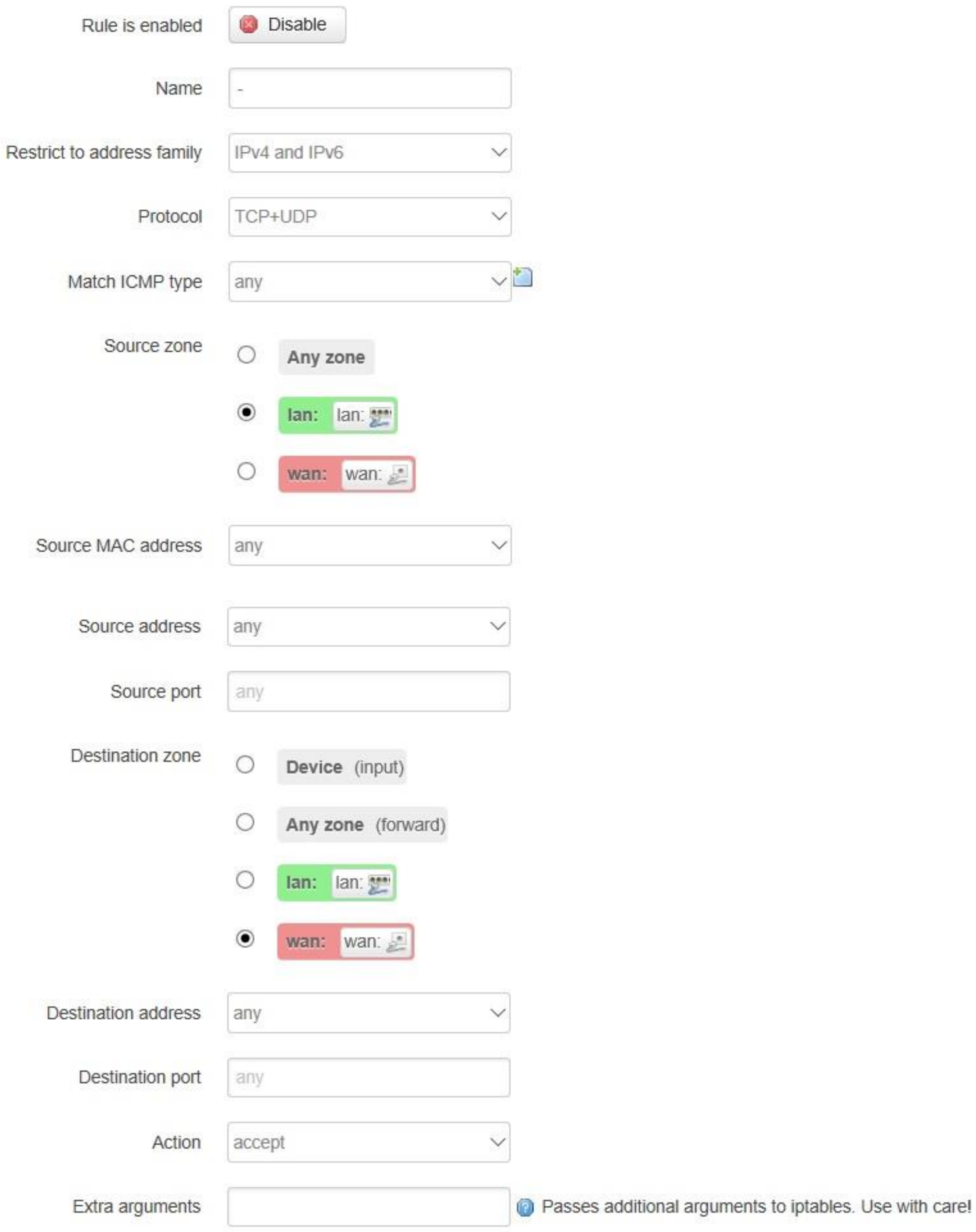
2) Source Zone

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.



Rule is enabled	Disable
Name	-
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	○ Any zone ● lan: lan: ○ wan: wan:
Source MAC address	any
Source address	any
Source port	any
Destination zone	○ Device (input) ○ Any zone (forward) ○ lan: lan: ● wan: wan:
Destination address	any
Destination port	any
Action	accept
Extra arguments	Passes additional arguments to iptables. Use with care!

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 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

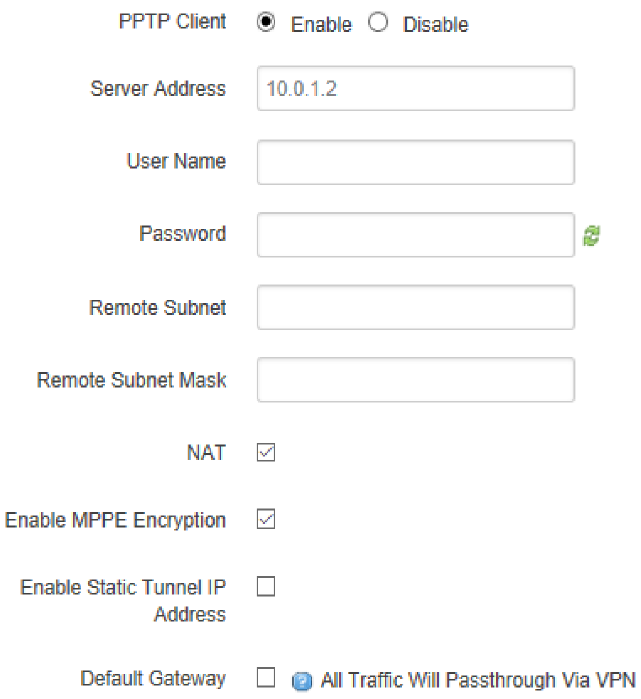
VPN is used to establish a virtual private channel, and all the data in this channel will be encrypted to ensure that data security during transmission.

TG462 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



PPTP Client	● Enable ○ Disable
Server Address	10.0.1.2
User Name	
Password	
Remote Subnet	
Remote Subnet Mask	
NAT	☑
Enable MPPE Encryption	☑
Enable Static Tunnel IP Address	□
Default Gateway	□ All Traffic Will Passthrough Via VPN

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.

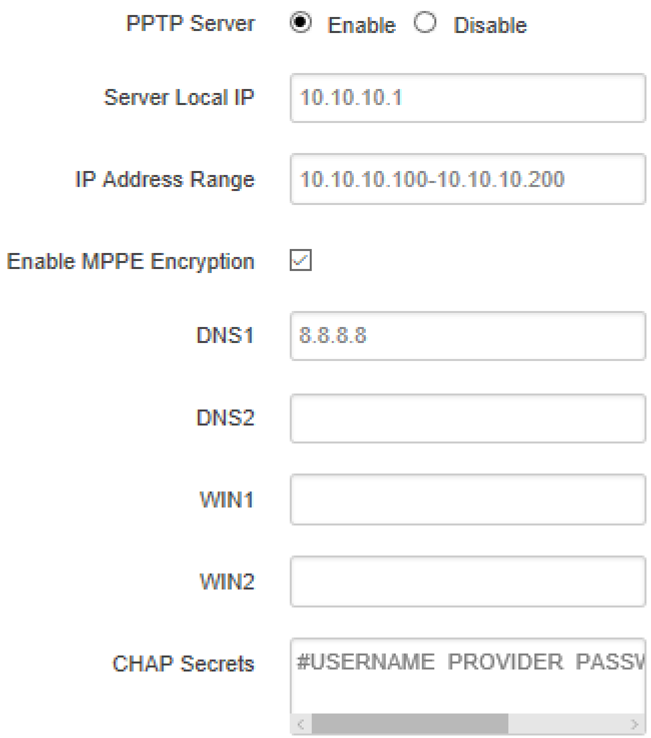
7. Enable MPPE Encryption.

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



PPTP Server ● Enable ○ Disable

Server Local IP 10.10.10.1

IP Address Range 10.10.10.100-10.10.10.200

Enable MPPE Encryption ☑

DNS1 8.8.8.8

DNS2

WIN1

WIN2

CHAP Secrets #USERNAME PROVIDER PASSV

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.

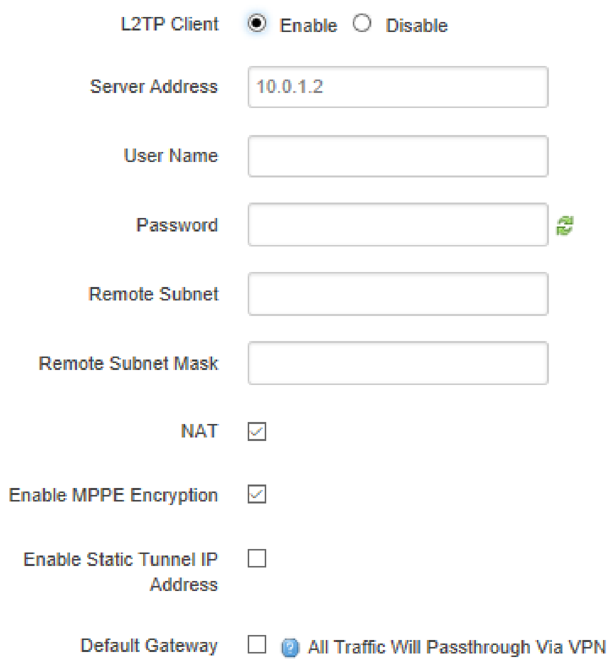
7. CHAP Secrets

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



L2TP Client ● Enable ○ Disable

Server Address: 10.0.1.2

User Name:

Password:

Remote Subnet:

Remote Subnet Mask:

NAT ☑

Enable MPPE Encryption ☑

Enable Static Tunnel IP Address □

Default Gateway □ All Traffic Will Passthrough Via VPN

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.

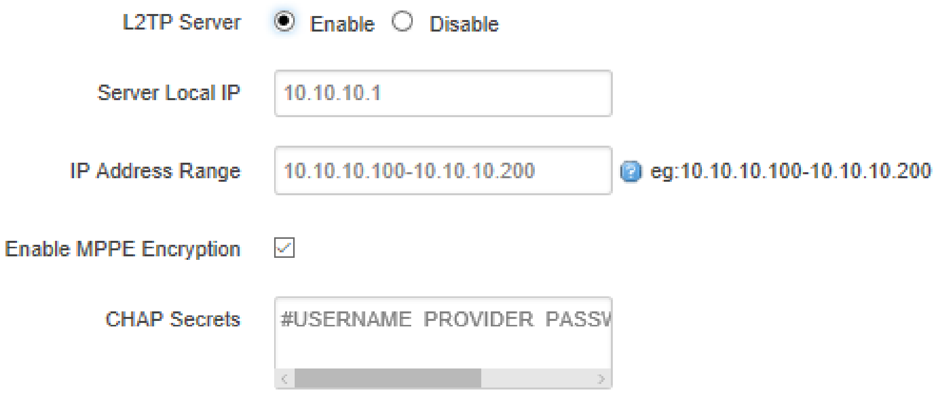
7. Enable MPPE Encryption.

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



L2TP Server ● Enable ○ Disable

Server Local IP 10.10.10.1

IP Address Range 10.10.10.100-10.10.10.200 eg:10.10.10.100-10.10.10.200

Enable MPPE Encryption ☑

CHAP Secrets #USERNAME PROVIDER PASSW

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.

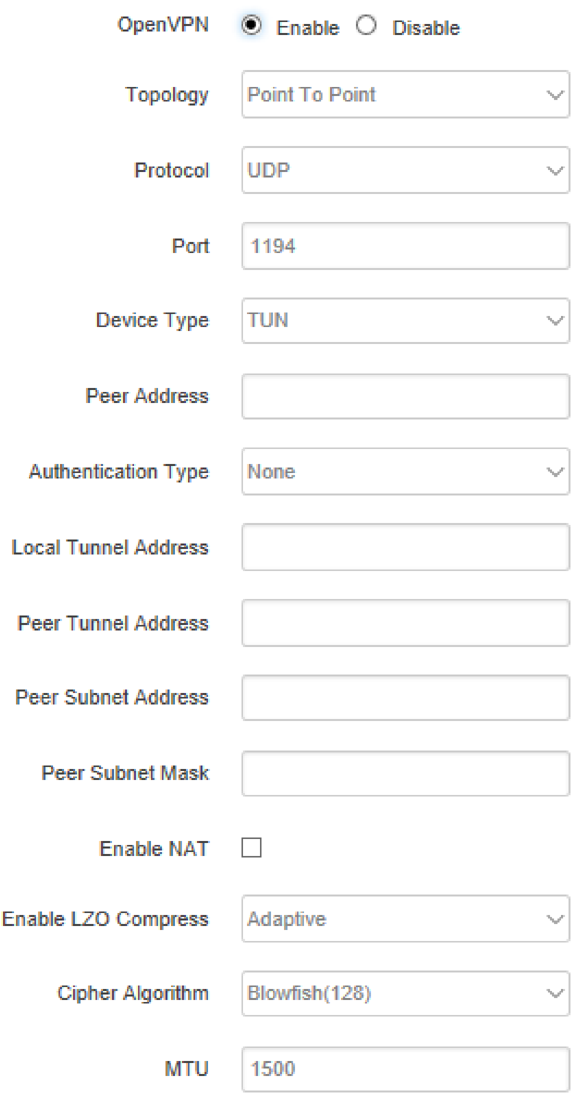
4. Enable MPPE Encryption.

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



OpenVPN	● Enable ○ Disable
Topology	Point To Point
Protocol	UDP
Port	1194
Device Type	TUN
Peer Address	
Authentication Type	None
Local Tunnel Address	
Peer Tunnel Address	
Peer Subnet Address	
Peer Subnet Mask	
Enable NAT	□
Enable LZO Compress	Adaptive
Cipher Algorithm	Blowfish(128)
MTU	1500

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

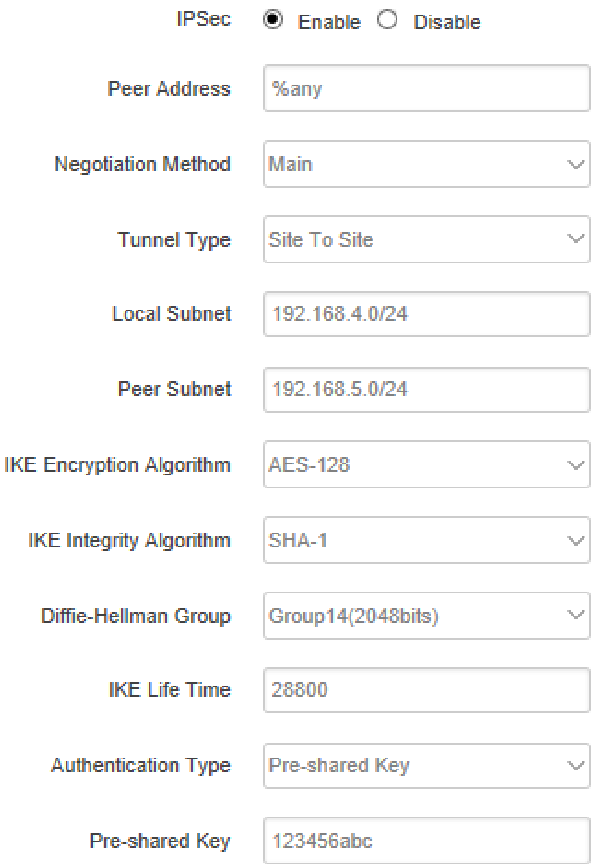
If topology is subnet, authentication type is certification. If it is point to point, you can choose none, certificate or static secret.

9) TLS Role

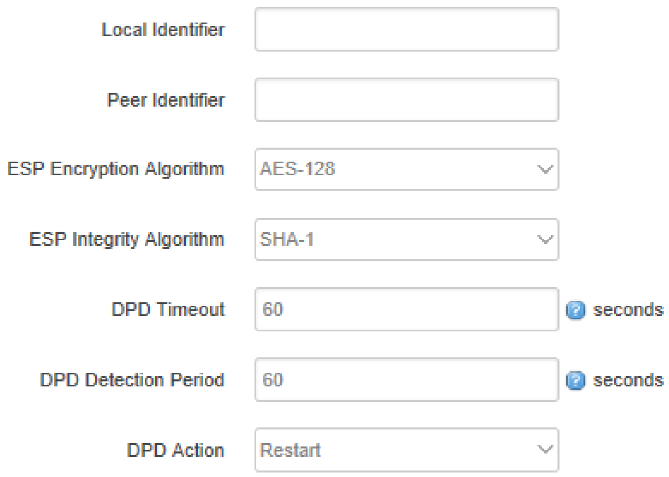
When topology is point to point, and authentication type is certification, you need to choose if it is server or client.

3.4.4 IPSec

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



IPSec	● Enable ○ Disable
Peer Address	%any
Negotiation Method	Main
Tunnel Type	Site To Site
Local Subnet	192.168.4.0/24
Peer Subnet	192.168.5.0/24
IKE Encryption Algorithm	AES-128
IKE Integrity Algorithm	SHA-1
Diffie-Hellman Group	Group14(2048bits)
IKE Life Time	28800
Authentication Type	Pre-shared Key
Pre-shared Key	123456abc



Local Identifier		
Peer Identifier		
ESP Encryption Algorithm	AES-128	
ESP Integrity Algorithm	SHA-1	
DPD Timeout	60	seconds
DPD Detection Period	60	seconds
DPD Action	Restart	

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.

3.5 Advanced

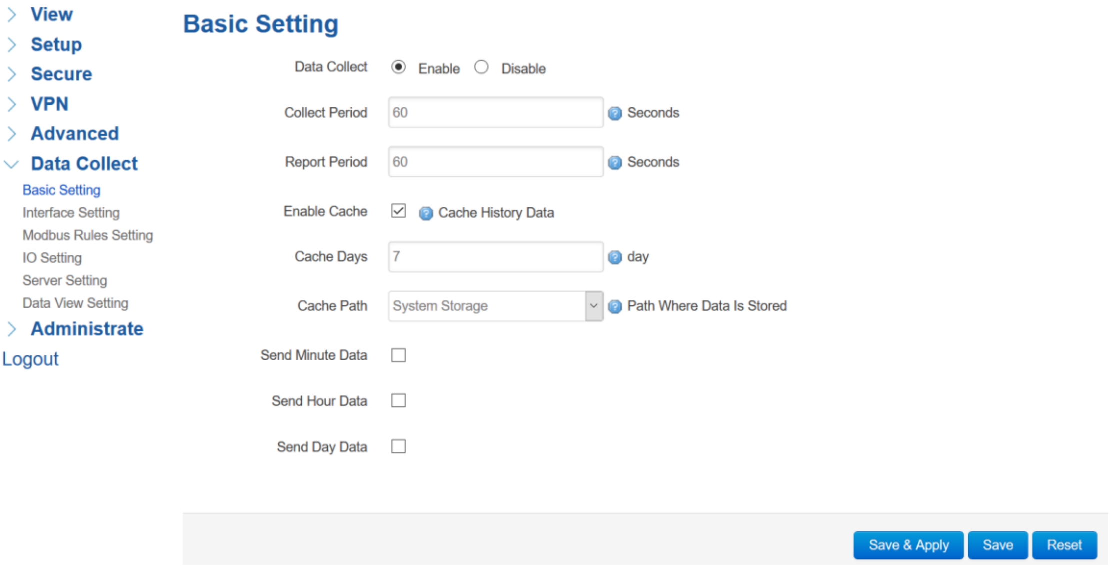
3.6 Data Collect

Data Collect settings is for TG462 acquiring data from slave devices in serial ports, Ethernet ports, IO ports, with Modbus protocol and other customized protocols.

Also support customize data display on LCD (only for TG462S).

3.6.1 Basic Setting

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



Basic Setting

Data Collect ● Enable ○ Disable

Collect Period 60 Seconds

Report Period 60 Seconds

Enable Cache ☑ Cache History Data

Cache Days 7 day

Cache Path System Storage Path Where Data Is Stored

Send Minute Data □

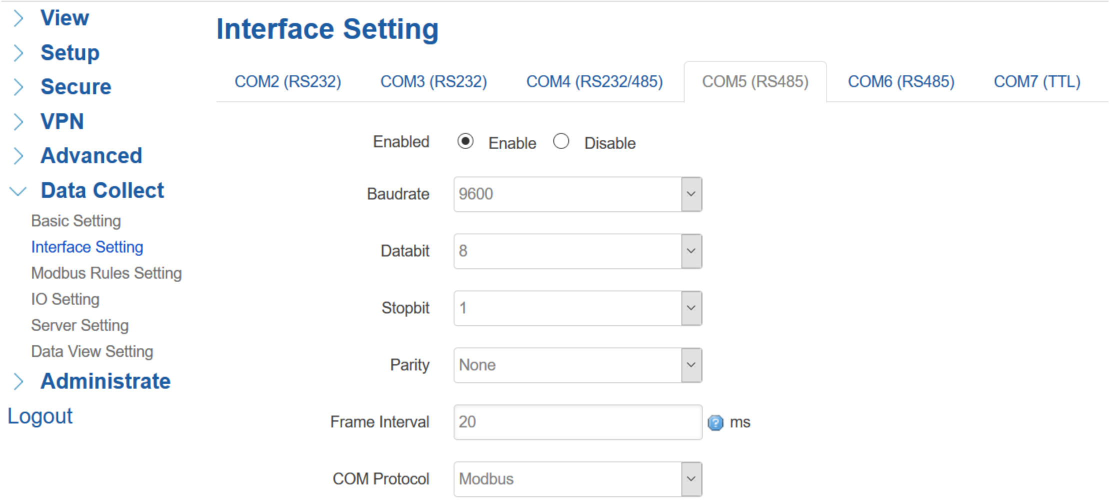
Send Hour Data □

Send Day Data □

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 (COM2~COM7), Modbus TCP base on Ethernet LAN, I2C ports.



Interface Setting

Enabled ● Enable ○ Disable

Baudrate 9600

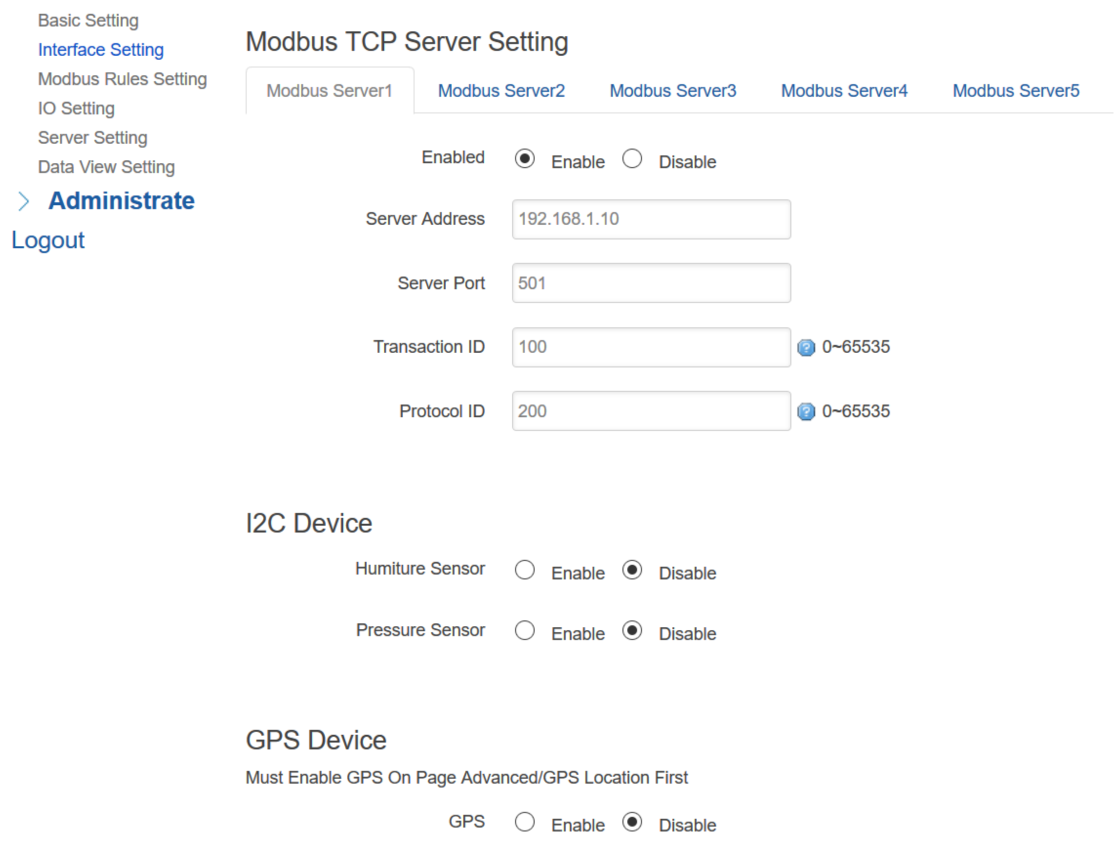
Databit 8

Stopbit 1

Parity None

Frame Interval 20 ms

COM Protocol Modbus



Modbus TCP Server Setting

Enabled ● Enable ○ Disable

Server Address: 192.168.1.10

Server Port: 501

Transaction ID: 100 0~65535

Protocol ID: 200 0~65535

I2C Device

Humiture Sensor ○ Enable ● Disable

Pressure Sensor ○ Enable ● Disable

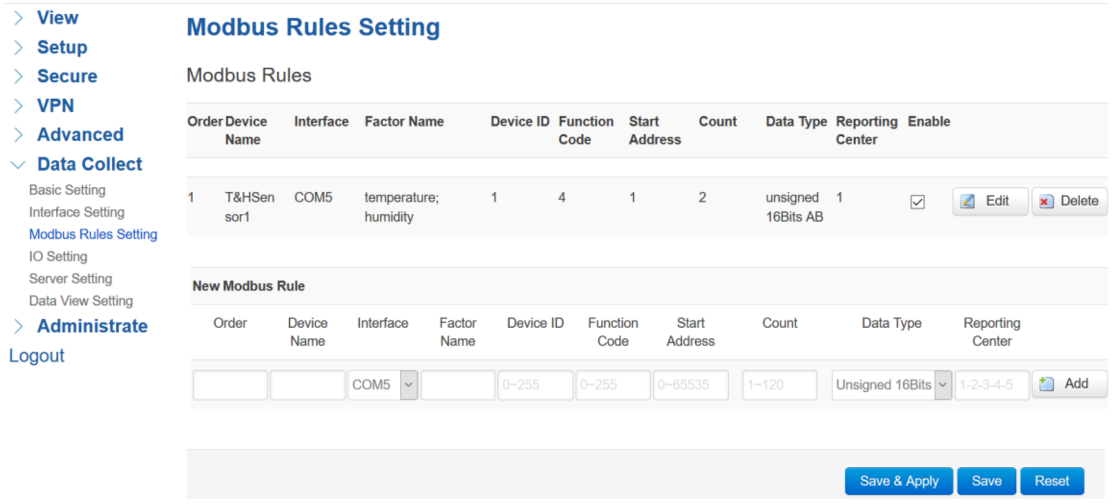
GPS Device

Must Enable GPS On Page Advanced/GPS Location First

GPS ○ Enable ● Disable

3.6.3 Modbus Rules Setting

Modbus Rules Setting is for TG462 as a Modbus master to acquire data from slave devices base on Modbus protocol. You can configure unlimited Modbus rules on it. TG462 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.



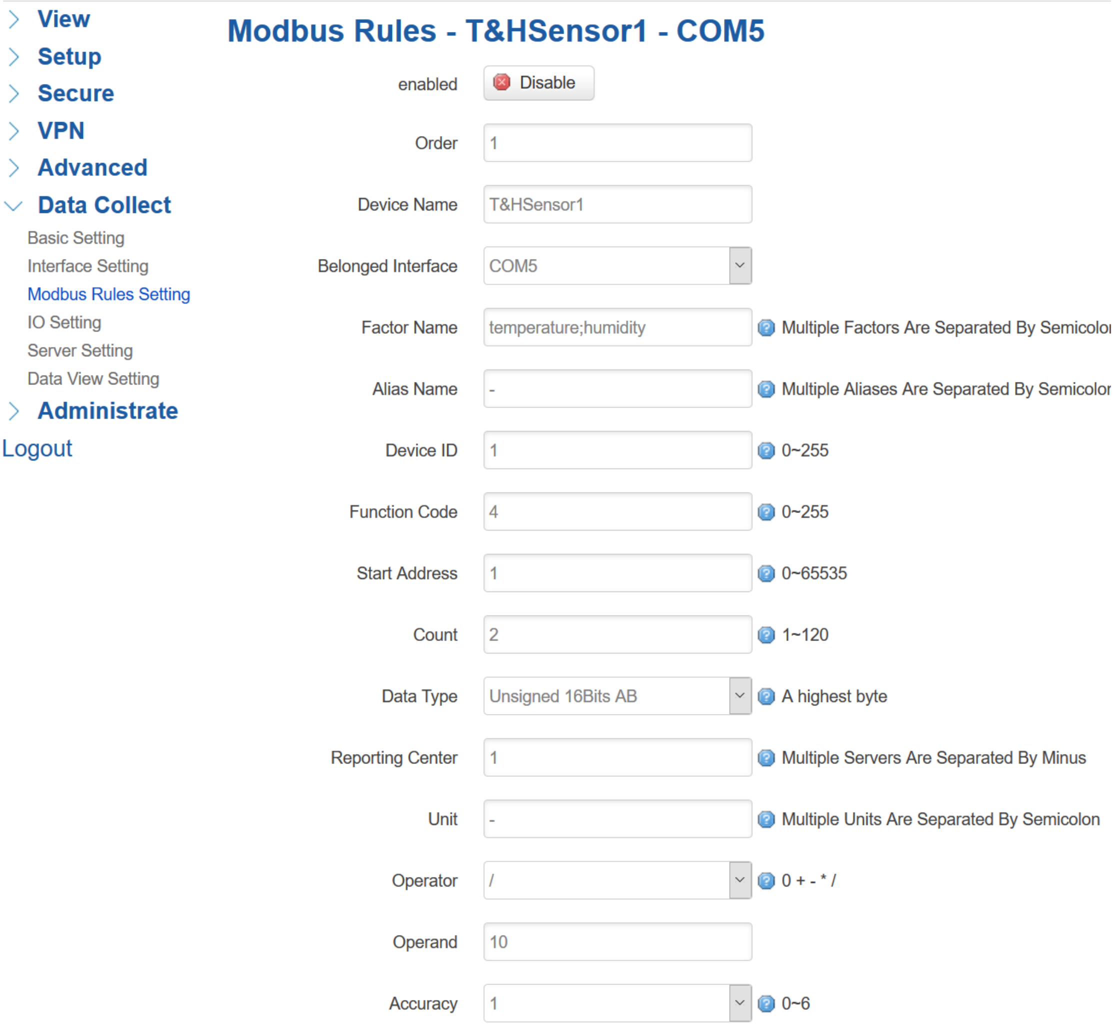
Modbus Rules Setting

Modbus Rules

Order	Device Name	Interface	Factor Name	Device ID	Function Code	Start Address	Count	Data Type	Reporting Center	Enable		
1	T&HSensor1	COM5	temperature; humidity	1	4	1	2	unsigned 16Bits AB	1	☑	Edit	Delete

New Modbus Rule

Order	Device Name	Interface	Factor Name	Device ID	Function Code	Start Address	Count	Data Type	Reporting Center	
		COM5		0~255	0~255	0~65535	1~120	Unsigned 16Bits	1-2-3-4-5	Add



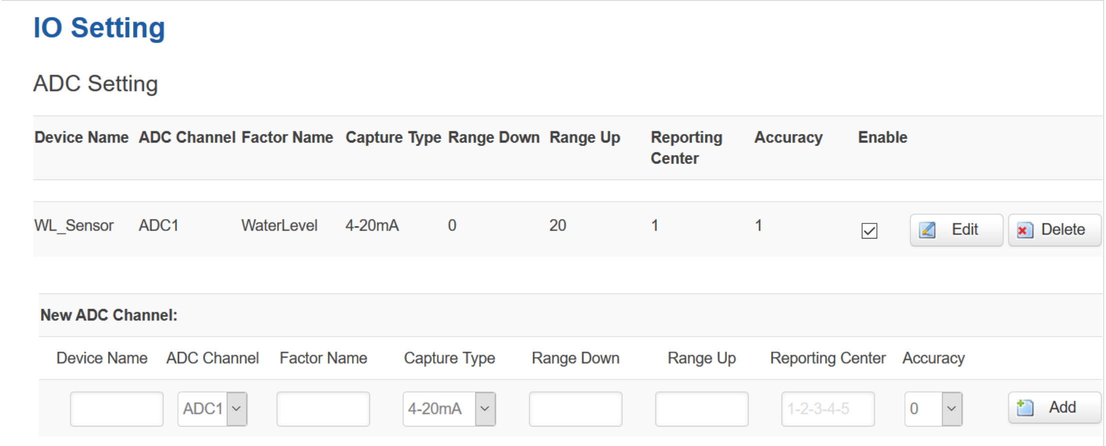
Modbus Rules - T&HSensor1 - COM5

enabled	Disable	
Order	1	
Device Name	T&HSensor1	
Belonged Interface	COM5	
Factor Name	temperature;humidity	Multiple Factors Are Separated By Semicolo
Alias Name	-	Multiple Aliases Are Separated By Semicolo
Device ID	1	0~255
Function Code	4	0~255
Start Address	1	0~65535
Count	2	1~120
Data Type	Unsigned 16Bits AB	A highest byte
Reporting Center	1	Multiple Servers Are Separated By Minus
Unit	-	Multiple Units Are Separated By Semicolon
Operator	/	0 + - * /
Operand	10	
Accuracy	1	0~6

3.6.4 IO Setting

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

1) ADC ports setting



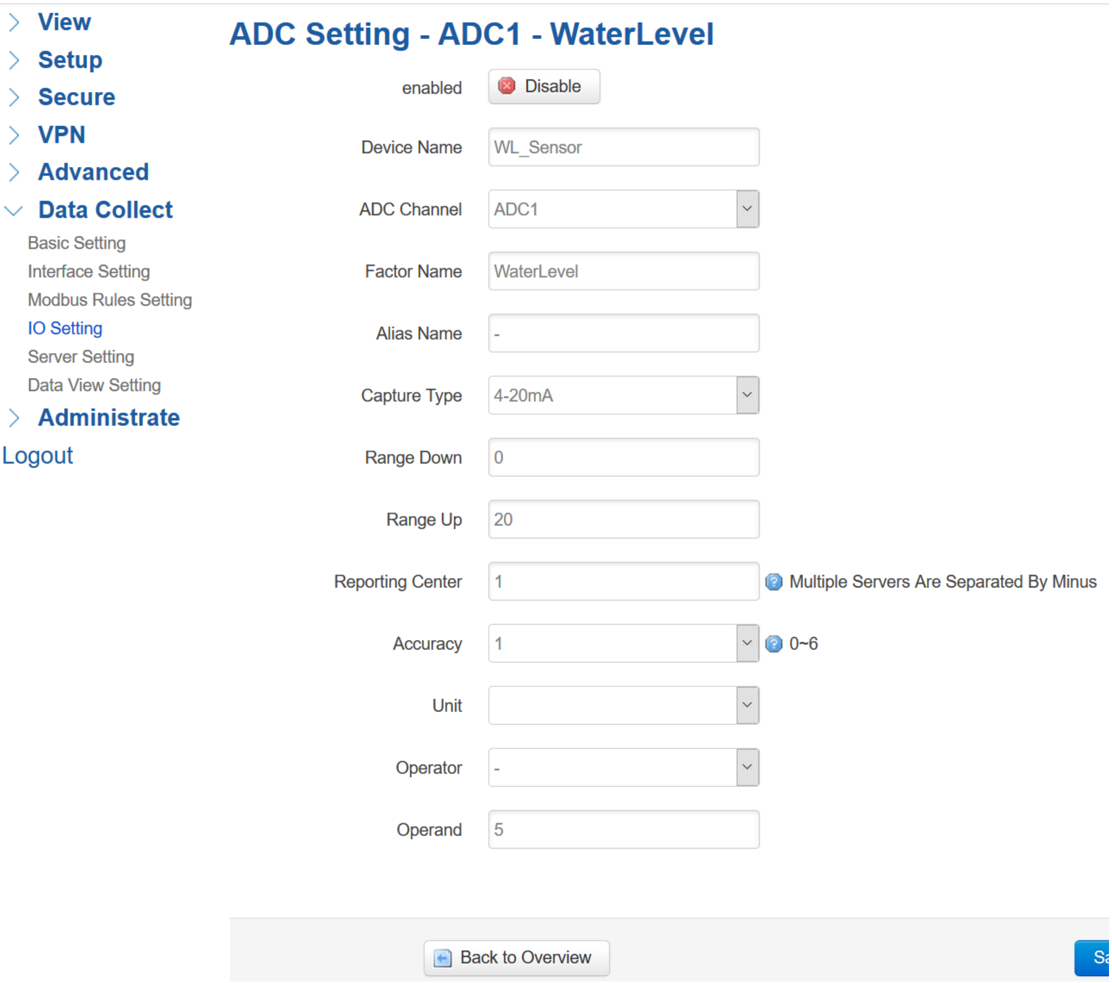
IO Setting

ADC Setting

Device Name	ADC Channel	Factor Name	Capture Type	Range Down	Range Up	Reporting Center	Accuracy	Enable		
WL_Sensor	ADC1	WaterLevel	4-20mA	0	20	1	1	☑	Edit	Delete

New ADC Channel:

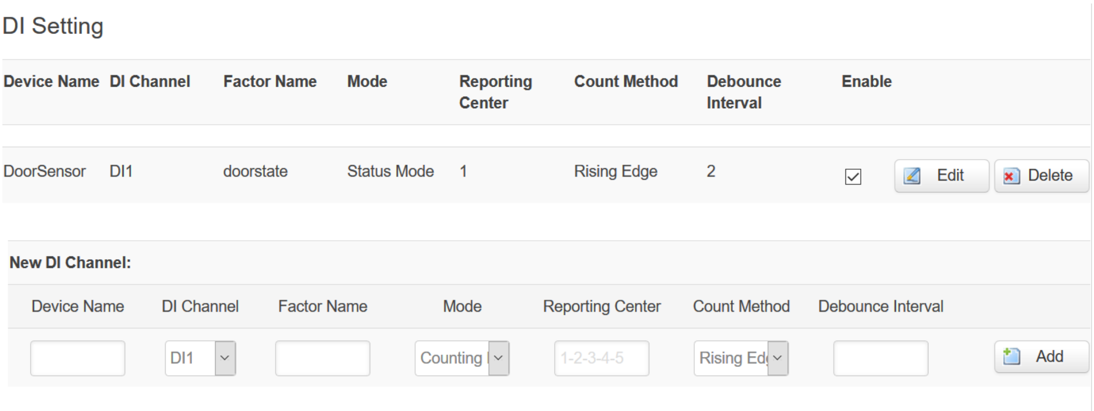
Device Name	ADC Channel	Factor Name	Capture Type	Range Down	Range Up	Reporting Center	Accuracy	
	ADC1		4-20mA			1-2-3-4-5	0	Add



ADC Setting - ADC1 - WaterLevel

enabled	Disable
Device Name	WL_Sensor
ADC Channel	ADC1
Factor Name	WaterLevel
Alias Name	-
Capture Type	4-20mA
Range Down	0
Range Up	20
Reporting Center	1 Multiple Servers Are Separated By Minus
Accuracy	1 0~6
Unit	
Operator	-
Operand	5

2) DI ports setting

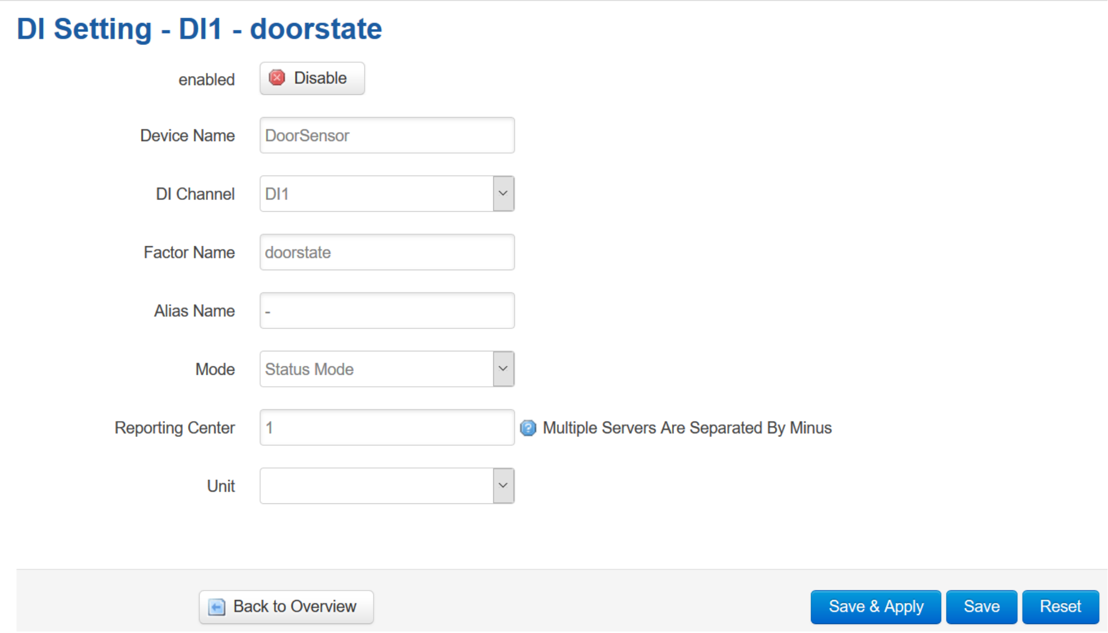


DI Setting

Device Name	DI Channel	Factor Name	Mode	Reporting Center	Count Method	Debounce Interval	Enable		
DoorSensor	DI1	doorstate	Status Mode	1	Rising Edge	2	☑	Edit	Delete

New DI Channel:

Device Name	DI Channel	Factor Name	Mode	Reporting Center	Count Method	Debounce Interval	
	DI1		Counting	1-2-3-4-5	Rising Ed		Add

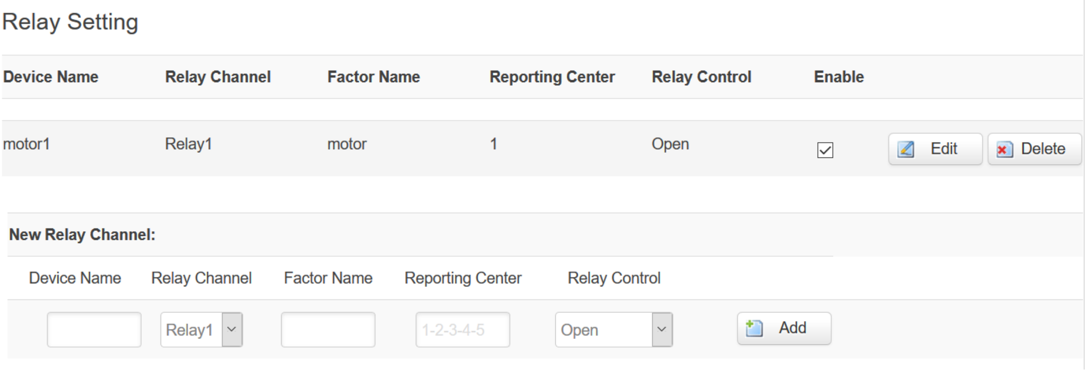


DI Setting - DI1 - doorstate

enabled	Disable
Device Name	DoorSensor
DI Channel	DI1
Factor Name	doorstate
Alias Name	-
Mode	Status Mode
Reporting Center	1
Unit	

Multiple Servers Are Separated By Minus

3) Relay Setting

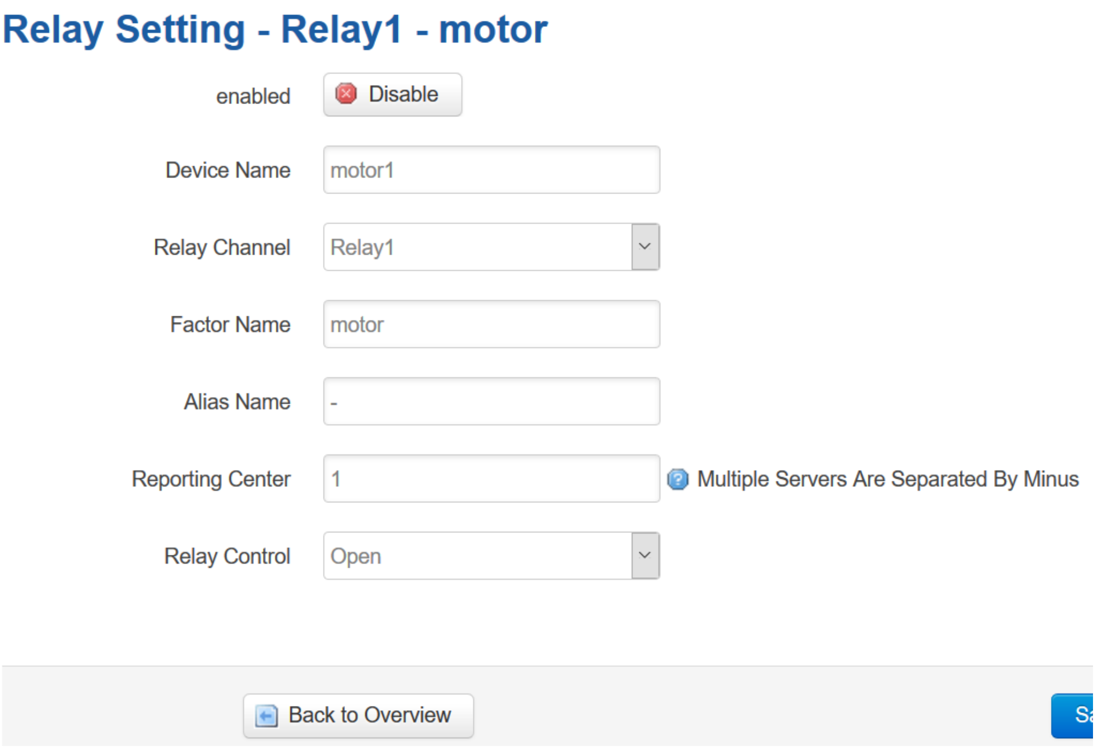


Relay Setting

Device Name	Relay Channel	Factor Name	Reporting Center	Relay Control	Enable		
motor1	Relay1	motor	1	Open	☑	Edit	Delete

New Relay Channel:

Device Name	Relay Channel	Factor Name	Reporting Center	Relay Control	
	Relay1		1-2-3-4-5	Open	Add



Relay Setting - Relay1 - motor

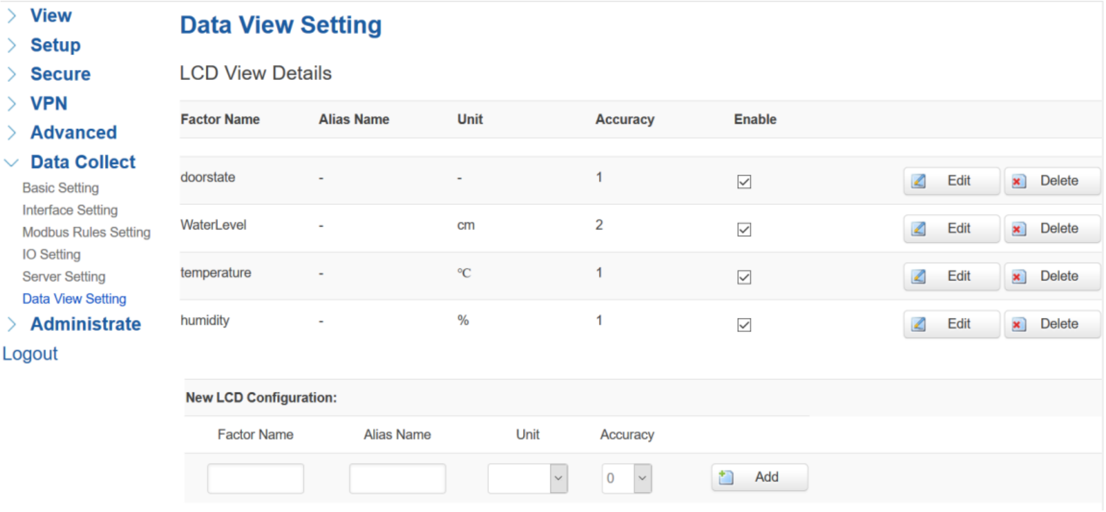
enabled	Disable
Device Name	motor1
Relay Channel	Relay1
Factor Name	motor
Alias Name	-
Reporting Center	1
Relay Control	Open

Reporting Center: Multiple Servers Are Separated By Minus

3.6.5 Server Setting

3.6.6 Data View Setting

Data View Setting menu is for configuring the items which need display on LCD. It use “**Factor Name**” as relevant key point which configured on previous steps.



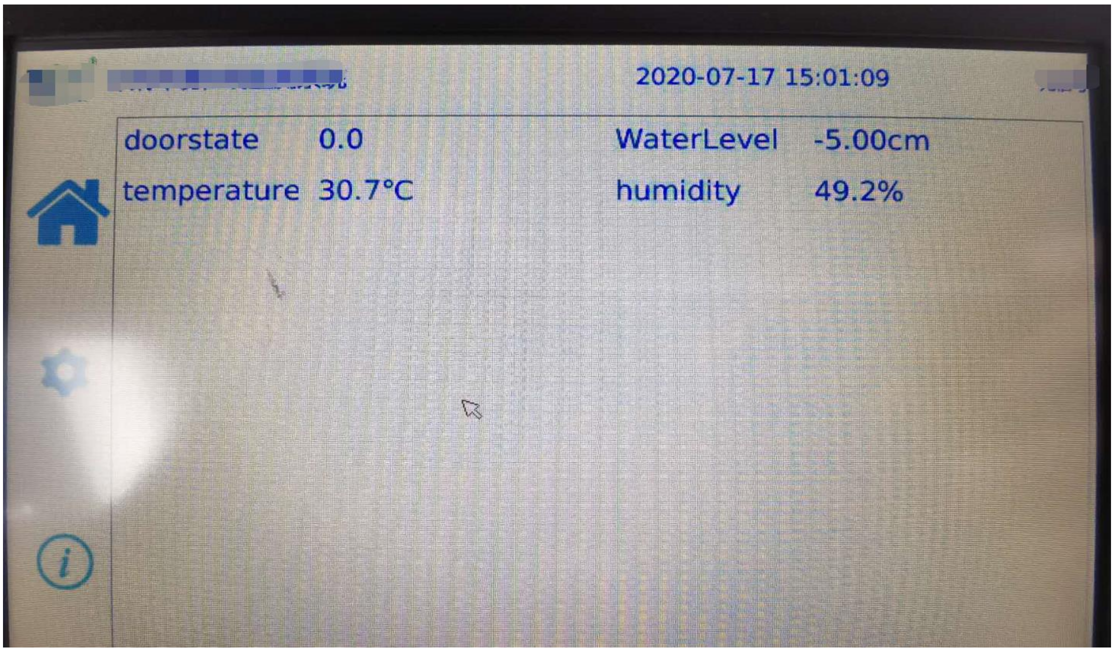
Data View Setting

LCD View Details

Factor Name	Alias Name	Unit	Accuracy	Enable		
doorstate	-	-	1	☑	Edit	Delete
WaterLevel	-	cm	2	☑	Edit	Delete
temperature	-	℃	1	☑	Edit	Delete
humidity	-	%	1	☑	Edit	Delete

New LCD Configuration:

Factor Name	Alias Name	Unit	Accuracy	
			0	Add



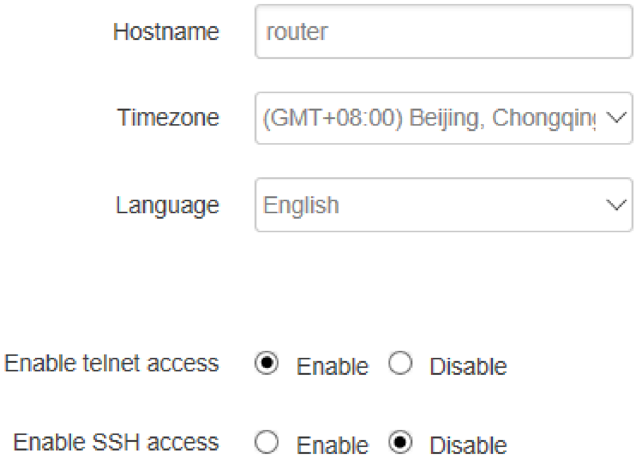
[redacted] 2020-07-17 15:01:09 [redacted]

doorstate	0.0	WaterLevel	-5.00cm
temperature	30.7°C	humidity	49.2%

Note, TG462S LCD also provide change configuration via screen by press the Setting button, while the default password is “123456”

3.7 Administrate

3.7.1 System



Hostname	router
Timezone	(GMT+08:00) Beijing, Chongqin
Language	English
Enable telnet access	● Enable ○ Disable
Enable SSH access	○ Enable ● Disable

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

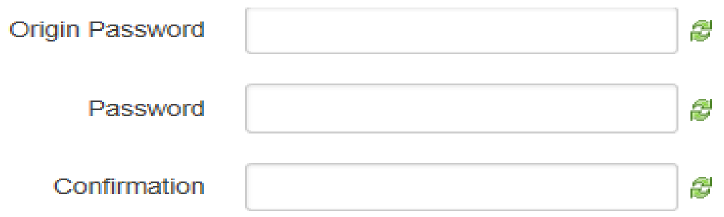
To enable the telnet server, the default function is enable.

5) Enable SSH Access

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

3.7.2 Password

To revise the password of router.



Origin Password	
Password	
Confirmation	

1) Origin Password

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

2) Password

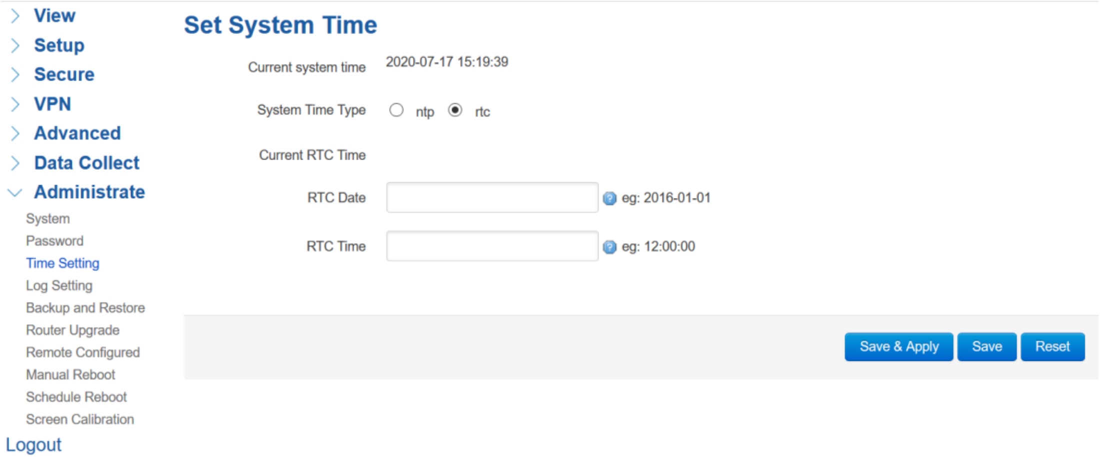
Type the new password you want to change.

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.



Set System Time

Current system time 2020-07-17 15:19:39

System Time Type ○ ntp ● rtc

Current RTC Time

RTC Date eg: 2016-01-01

RTC Time eg: 12:00:00

1) Current System Time

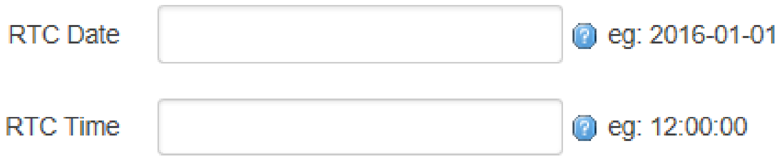
Display the time of router.

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 Date eg: 2016-01-01

RTC Time eg: 12:00:00

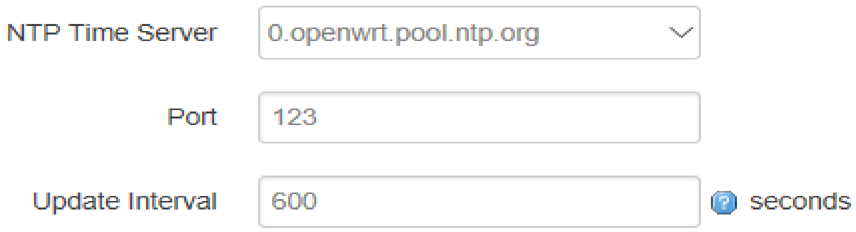
RTC Data

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: 0.openwrt.pool.ntp.org

Port: 123

Update Interval: 600 seconds

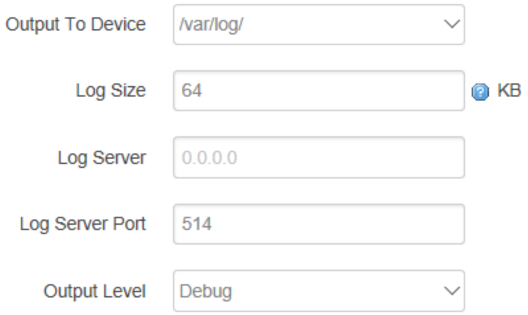
NTP Time Server
You can select the NTP time server through drop-down menu, or you can customize it yourself.

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.



Output To Device: /var/log/

Log Size: 64 KB

Log Server: 0.0.0.0

Log Server Port: 514

Output Level: Debug

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

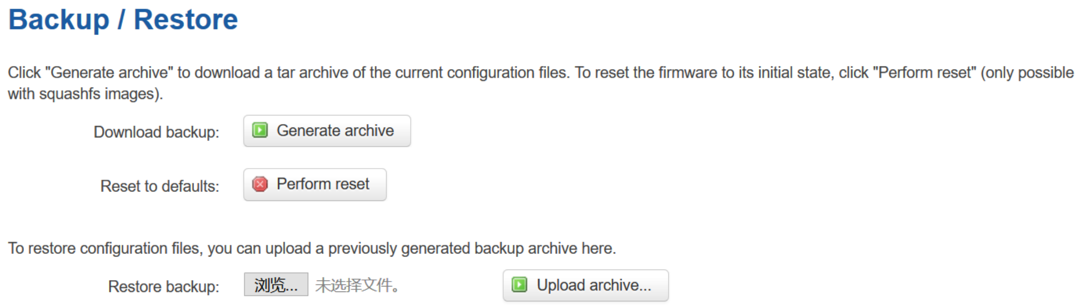
Set up the port of log server, default value is 514

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, or reset to factory defaults.



Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: 浏览... 未选择文件。 Upload archive...

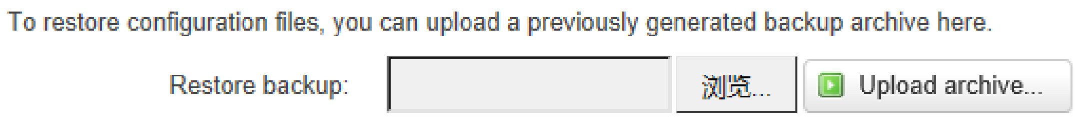
1) Download Backup

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



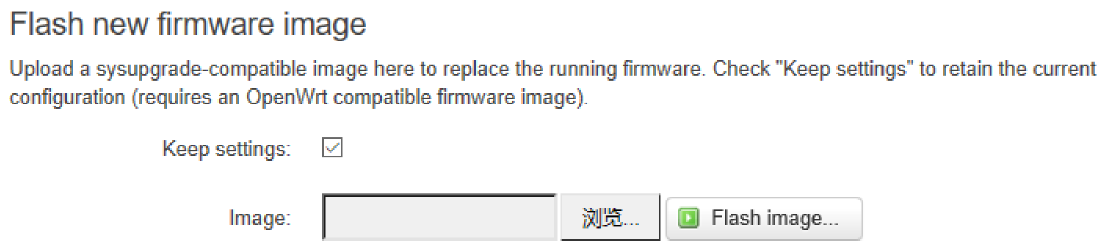
To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: 浏览... Upload archive...

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

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



Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings: ☑

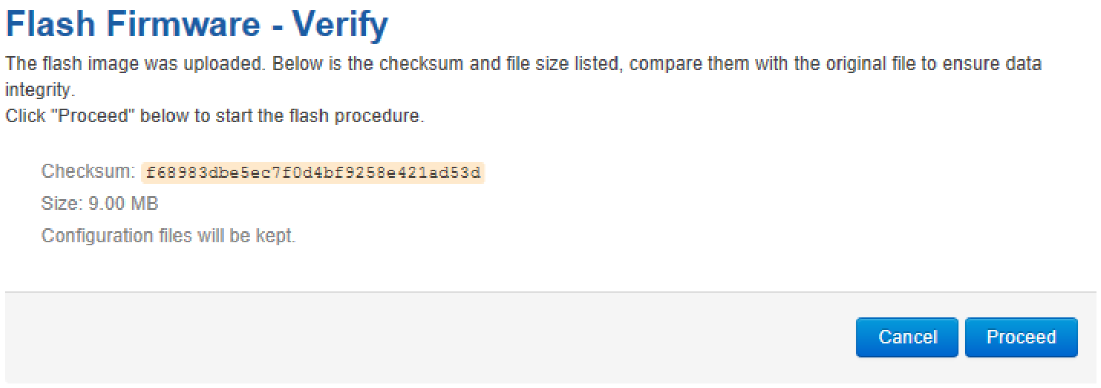
Image:

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.



Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

Checksum: f68983dbe5ec7f0d4bf9258e421ad53d

Size: 9.00 MB

Configuration files will be kept.

- **Checksum**

MD5 checksum value of firmware.

- **Size**

The size of firmware.

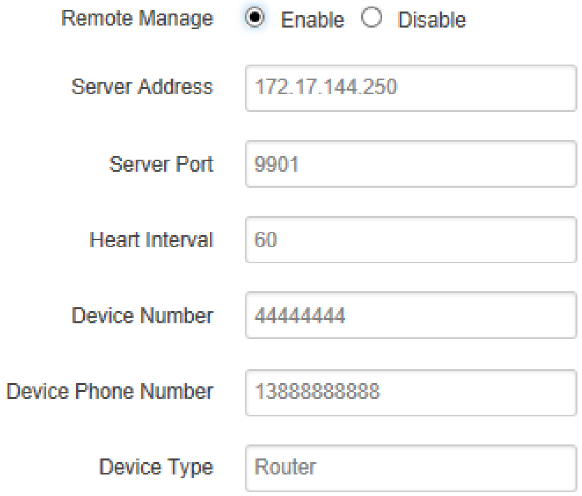
- **Proceed**

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

3.7.7 Remote Management

Remote Management feature allows TG462 **work with Bivocom Device Management Platform** 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.



Remote Manage	● Enable ○ Disable
Server Address	172.17.144.250
Server Port	9901
Heart Interval	60
Device Number	44444444
Device Phone Number	13888888888
Device Type	Router

1) Remote Manage

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 mange the router, it can be either an IP address or Domain Name.

3) Server Port

The specified login server port.

4) Heartbeat Interval

The heartbeat time interval (Unit: second)

5) Device Number

Device ID of router.

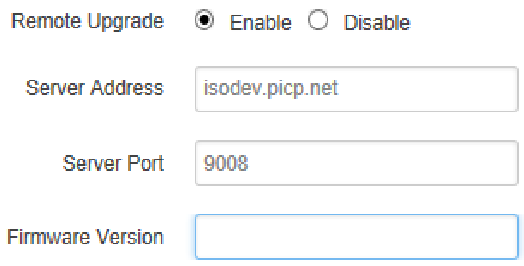
6) Device Phone Number

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.



Remote Upgrade ● Enable ○ Disable

Server Address: isodev.picp.net

Server Port: 9008

Firmware Version:

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.

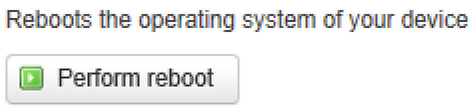
10) Server Port

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



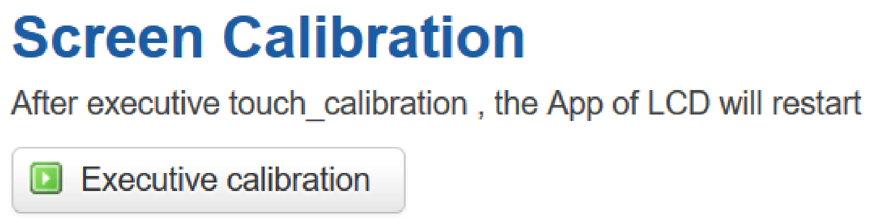
Reboots the operating system of your device

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

3.7.10 Screen Calibration

Screen Calibration allows calibrate TG462S touch LCD. After “Executive calibration”, you will be asked press the location points on LCD for touch calibration.



Screen Calibration

After executive touch_calibration , the App of LCD will restart