Programmable AIoT Gateway

TG465 Series

User Guide
Version 4.0, 09-01-2026

Thank you for choosing the Bivocom Cellular IoT Gateway. Please read this guide carefully before use; it will help you install, configure and manage the device safely and efficiently.

Trademark

Bivocom 佰沃恩

“Bivocom 佰沃恩” are proprietary registered trademarks of Bivocom. All unapproved exploitation of these marks is forbidden. Any other trade names referenced belong to the trademark holders themselves.

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 accuracy, completeness of the information published.

Copyright © XIAMEN BIVOCOM TECHNOLOGIES CO., LTD. All rights reserved.

HQ: 27–28/F, Building F14, Software Park Phase III, Xiamen, 361022, China

Factory: 6/F, Building No.18, Anren Industrial Park, No.1068 Jimei North Avenue, Jimei District, Xiamen, 361023, China

W: www.bivocom.com P: +86 158 8026 2905

E: sales@bivocom.com E: support@bivocom.com

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 B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the

following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

About This Guide

Thank you for choosing Bivocom Industrial Cellular Gateway TG465 Series.

Read this user guide thoroughly before configuring and installing the device.

This manual is compatible with the following models

Model	Description
TG465	Programmable AIoT Gateway

Table of Contents

FEDERAL COMMUNICATION COMMISSION (FCC) STATEMENT 2
About This Guide 3
Table of Contents 4
1. Introduction 7
1.1 Overview 7
1.2 Applications 7
1.3 Advantages 8
1.4 Dimensions 9
1.5 Physical Characteristics 9
2. Getting Started 9
2.1 Package Checklist 9
2.2 Installation 10
2.2.1 SIM/UIM Card 11
2.2.2 Interface Connection 11
2.2.3 Power Supply 12
2.2.4 Cellular Antenna 12
2.2.5 Wi-Fi Antenna (Optional) 12
2.3 LED Indicators 12
2.4 Reset 14
2.5 Quick Check 14
3.0 Access to Web UI 14
3.0.1 Connect the PC to the TG465 network 14
3.0.2 Log in to the Web UI 15
3.1 View 16
3.1.1 System 16
3.1.2 Network 17

3.1.3 Routing Tables 18
3.1.4 System Log 19
3.1.5 VPN Status 19
3.2 Setup 20
3.2.1 WAN 20
3.2.2 LAN 22
3.2.3 Wireless (Optional) 23
3.2.4 Wireless Client (Optional) 25
3.2.5 Online Detection 25
3.2.6 Diagnostics 27
3.2.7 Quick Check 27
3.3 Security 28
3.3.1 DMZ Host 28
3.3.2 Port Forwards 28
3.3.3 Traffic Rules (ACL Configurations) 30
3.3.4 Custom Settings 34
3.4 VPN 39
3.4.1 PPTP 39
3.4.2 L2TP 42
3.4.3 IPSec 46
3.4.4 OpenVPN 49
3.4.5 GRE 53
3.4.6 XFRP Client 53
3.4.7 VPN Common Issues: 54
3.5 Advanced 54
3.5.1 Send SMS 54
3.5.2 Static Routes 55
3.5.3 DI DO 55

3.5.4 Net Flow 57
3.5.5 GPS Location (Optional) 57
3.5.6 Dynamic DNS 61
3.5.7 DHCP and DNS 62
3.6 Data Collect 63
3.6.1 Basic Setting 64
3.6.2 Interface Setting 65
3.6.3 Modbus Rules Setting 67
3.6.4 IO Setting 71
3.6.5 Server Setting 73
3.6.6 Data Query 76
3.6.7 Common Application 77
3.7 Administrate 108
3.7.1 System 108
3.7.2 Password 109
3.7.3 Time Setting 109
3.7.4 Log Settings 110
3.7.5 Backup and Reset 111
3.7.6 Firmware Upgrade (OpenWRT only) 112
3.7.7 Manual Reboot 113
3.7.8 Schedule Reboot 113
3.8 Debug 114
3.8.1 Data Packet Capture 114
3.8.2 Serial Debug 114
3.9 Logout 116
3.10 FAQ 116

1. Introduction

1.1 Overview

The TG465 is a high-performance IoT gateway featuring ARM CPU, GPU and NPU for edge and AI computing. It provides flexible memory and storage options: 2 GB DDR4 RAM (8 GB optional) and 16 GB eMMC flash (128 GB optional), with an NVMe M.2 slot for AI accelerator and SSD expansion. Ideal for mission-critical IIoT applications: BESS, Telecom sites, power, smart traffic light, etc.

Preloaded with Bivocom OS (Ubuntu optional), the gateway supports SDK-based secondary development via Node-RED, Python, C/C++ and Docker for flexible custom application deployment.

Equipped with rich industrial interfaces including 4×GbE RJ45, 1×RS232, 6×RS485, 4×DI, 4×Relay, 2×power output, 1×USB3.0, 1×USB2.0, 1×TF slot, HDMI port and Wi-Fi 6, it easily connects to diverse field devices.

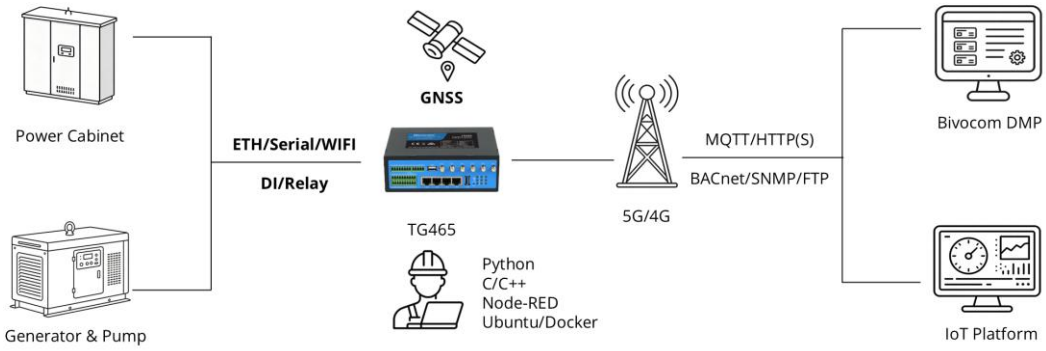
It supports 5G/4G LTE and mainstream industrial protocols such as MQTT, Modbus RTU/TCP, JSON, TCP/UDP, OPC UA*, DNP3*, IEC101/104* and SNMP. Combined with VPN encryption, it delivers efficient, stable and secure end-to-end IoT data transmission.



1.2 Applications

The TG465 Series Gateway uses a cellular network to connect network and serial devices to the management center for remote monitoring and control.

Typical applications are shown below.

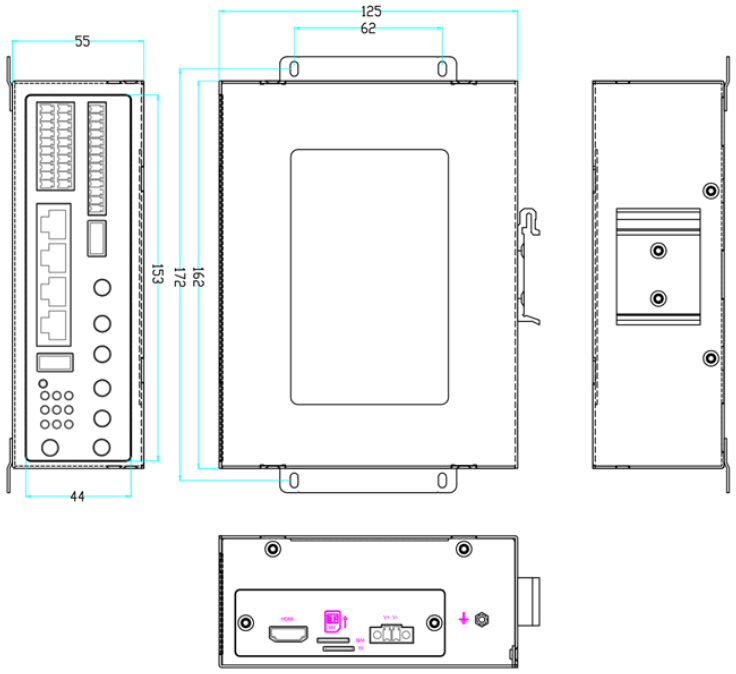


1.3 Advantages

The key advantages of the TG465 Series are as follows:

- **High-performance edge computing:** Rockchip RK3568J quad-core Cortex-A55 CPU with GPU and NPU for AI and edge workloads
- **Flexible memory and storage:** 2 GB DDR4 RAM (8 GB optional), 16 GB eMMC flash (128 GB optional) and an NVMe M.2 slot
- **Rich interfaces:** 4-GbE, 2-RS232 (1 debug), 6-RS485, 4-DI, 4-Relay, 2-DC power output, USB 3.0, USB 2.0, 1-TF slot, HDMI and Wi-Fi 6
- **Optional cellular:** 5G NR, 5G RedCap and 4G LTE, with optional dual SIM for failover
- **Programmable:** Bivocom OS supports C/C++, Python, Node-RED, Docker and Ubuntu*
- **Wide protocol support:** MQTT, Modbus RTU/TCP, JSON, TCP/UDP, OPC UA*, DNP3*, IEC 101/104* and SNMP
- **Centralized management:** Bivocom DMP* enables centralized remote device management

1.4 Dimensions



1.5 Physical Characteristics

Physical Characteristics	
IP Rating	IP30
Housing & Weight	Metal, 799g (1.76 lbs), without accessories
Dimensions	162x125x55 mm (6.38 x 4.92 x 2.16 in)
Mounting	Desktop, DIN-Rail

2. Getting Started

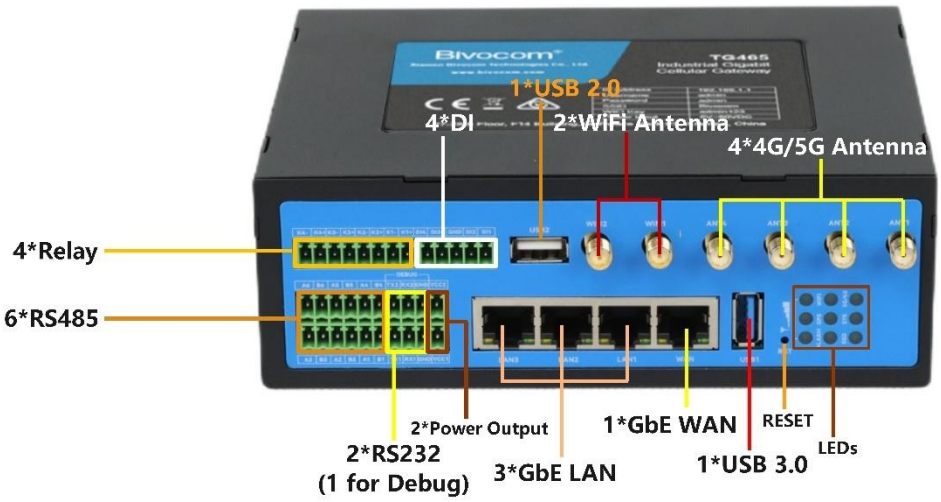
2.1 Package Checklist

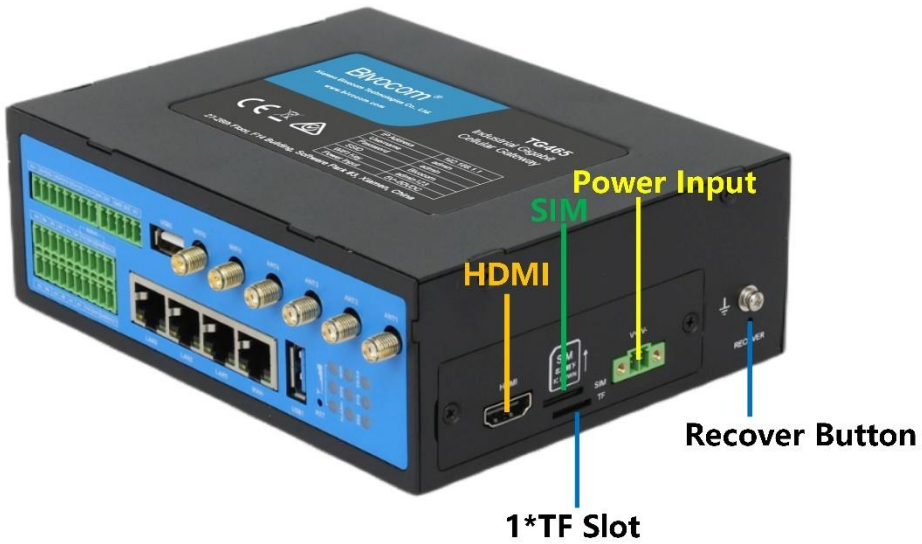
- TG465 Unit x 1
- Cellular Antenna x 4
- Wi-Fi Antenna x 2
- DIN-Rail mounting kit x 1
- Ethernet Cable x 1

- 2-Pin Terminal Block x 1
- 10-Pin Terminal Block x 3
- Power Adapter x 1 (Optional EU/UK/AU/US/CN Type)

2.2 Installation

The following describes the TG465 ports.





2.2.1 SIM/UIM Card

TG465 supports Micro SIM/UIM only, so if you're using Normal SIM or Nano SIM card, you may need to use a Nano SIM to Micro SIM adapter, and switch Normal SIM to Micro SIM.

Before inserting the SIM card, make sure the gateway is powered off. Place the SIM card in the SIM slot, use the SIM card ejector tool to insert the SIM card into the gateway, and make sure it is fully seated.

Warning: DO NOT install SIM/UIM card when gateway is powered on.

2.2.2 Interface Connection

TG465 supports 2xRS232 (1-Debug, 1-Shared via RS485), 6xRS485, 4xDI, 4xRelay. The serial ports can be used for firmware upgrade, system log checking, or as serial ports for data transmission.

The TG465 uses industrial terminal block interfaces. The console cable supplied with the device has a female connector at one end and stripped wires at the other; the signal assignment is defined below.

RS232 Cable(with DB9 female connector and stripping cable)

Color of Cable	Corresponding DB9-Female Pin No.	Corresponding Pin No. of Gateway
Blue	2(RX)	TX1/TX2 (Debug)
Brown	3(TX)	RX/RX2 (Debug)
Black	5(GND)	GND

RS485 Cable

Color of Cable	TG465 Gateway
A (Red)	A1~A6
B (Black)	B1~B6

Relay Interface (Relay1, Relay2, Relay3, Relay4)

Relay Feature	Control the External Switch
Load capacity	Maximum Voltage switch: 30 VDC/220VAC Maximum Current switch: 5A

DI Interface (DI1, DI2, DI3, DI4)

DI Feature	Detect the Slave Device Status
Input Range	Logic 1: wet contact 0-3 VDC, or dry contact close. Logic 0: wet contact 5-30 VDC, or dry contact open.

2.2.3 Power Supply

Use the standard Bivocom power adapter (12 VDC/1.5A). If you supply power from another source, make sure the voltage stays within 5-60 VDC and is stable. When using Bivocom power adapter, please make sure you connect the cable to the right pin, red cable connects to VIN+, and black cable connects to VIN-.

2.2.4 Cellular Antenna

The TG465 provides 4 for TG465-NR and 2 for TG465-LF, TG465-RC cellular antenna ports. Screw the SMA male antennas to TG465 (SMA female ports), make sure they are screwed tightly to ensure the strength of signal.

2.2.5 Wi-Fi Antenna (Optional)

Screw the SMA female Wi-Fi antenna to TG465(SMA male port), make sure it is screwed tightly to ensure the strength of signal.

2.3 LED Indicators

TG465 Series Gateway provides 9xLED indicators, as follows.

Indicator	Status	Content

Power	On	Powered On
	Off	Powered Off
Signal Strength	1 Lights	Signal weak
	2 Lights	Signal Medium
	3 Lights	Signal Strong
System	Blink	System works
	Off	System doesn't work
Online	On	Gateway accesses to Internet
	Off	Gateway doesn't access to Internet
Alarm	On	● SIM/UIM Card is not insert correctly or broken ● Antenna signal is too weak
	1 Blink Per Second	Cellular module was not registered to Gateway
	2 Blinks Per Second	Gateway can't access to Internet
	Off	Gateway doesn't have any alarm
Wi-Fi	On	Wi-Fi Enabled
	Off	Wi-Fi Disabled
WAN	On	WAN is connected
	Off	WAN is not connected
LAN	LAN1 Blink	LAN1 works
	LAN2 Blink	LAN2 works
	LAN3 Blink	LAN3 works

	LAN4 Blink	LAN4 works
	Off	LAN is not connected

2.4 Reset

Press the Reset button to restore the factory defaults. This resolves problems caused by incorrect configuration, such as being unable to access the Internet, log in or manage the device.

Use a needle object (such as paper clip) to insert into hole of 'Reset', hold until all the LED indicators turn off.

2.5 Quick Check

Once the installation has been completed, carry out the verification steps below:

· The power cable is plugged in correctly, and the PWR light is on.

- The network wire is linked to the PC's Ethernet port.
- The PC's IP address falls within the same subnet as the device.
- The Web UI can be accessed through browser (http://192.168.1.1).
- Log in successfully using the default account admin/admin.

3.0 Access to Web UI

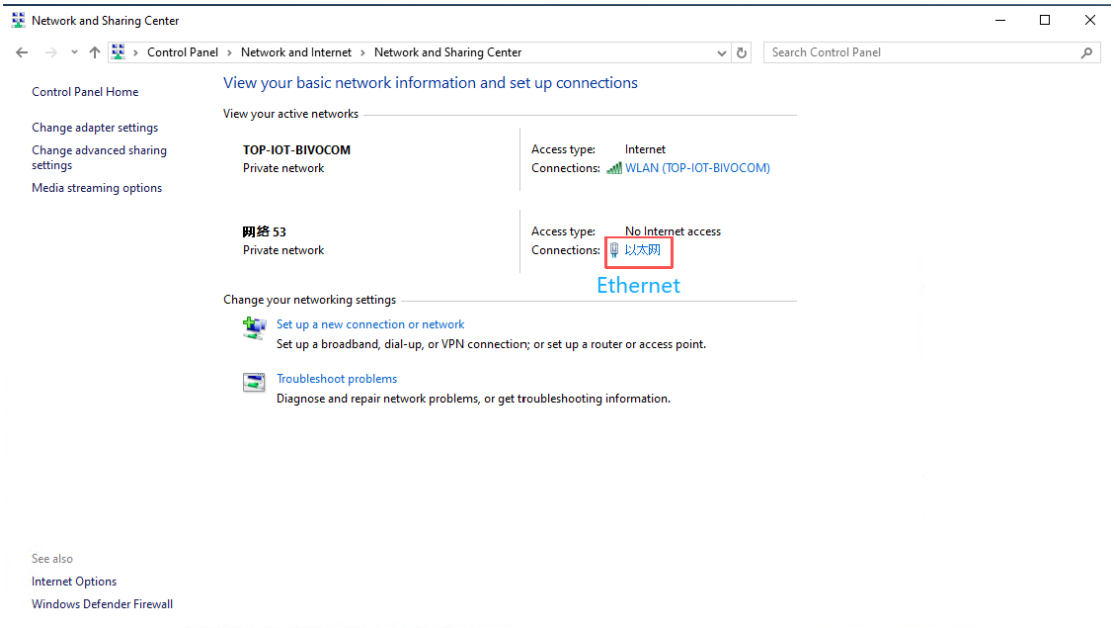
The TG465 provides an intuitive, easy-to-use Web UI for configuration and management. The sections below describe the features and settings of each menu item in the Web UI. The screenshots were taken on Windows 10 and are for reference only.

Username: **admin**
Password: **admin**
IP Address: **192.168.1.1**

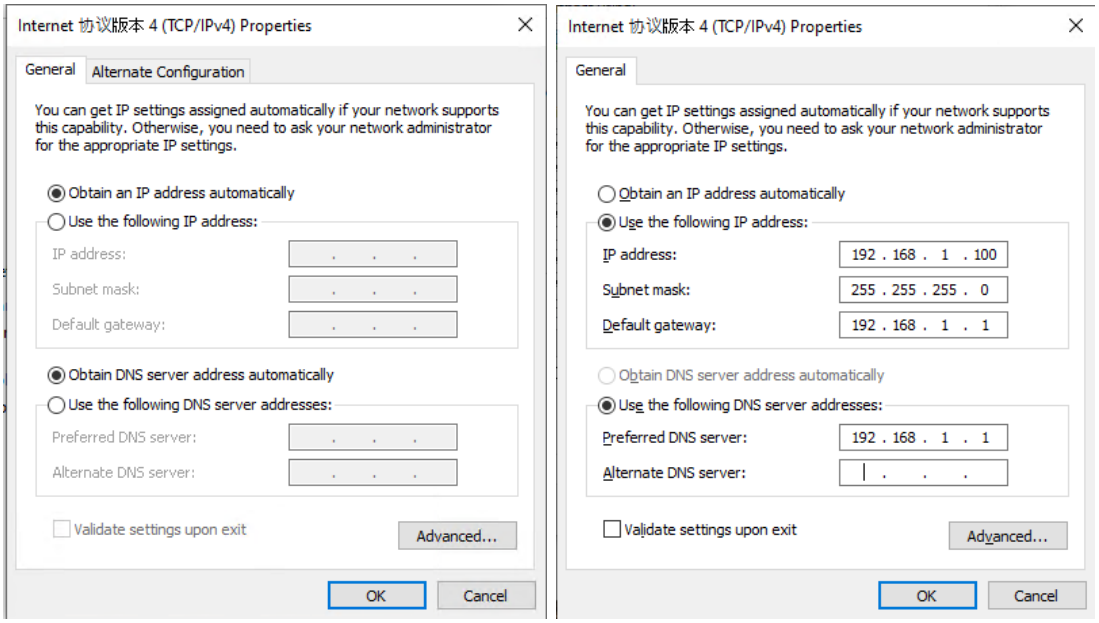
3.0.1 Connect the PC to the TG465 network

1. Using an Ethernet cable, connect one end of the Ethernet cable to the LAN port on TG465 unit and the other end to a LAN port on a PC.

2. Open "Control Panel" → "Network and Internet" → "Network and Sharing Center", click "Ethernet".



3. Enter "Properties" → "Internet Protocol Version 4 (TCP/IPv4) ", set "Obtain an IP address automatically" or "Use the following IP address", then input a static IP (192.168.1.100, for example) manually within the same subnet of the TG465.



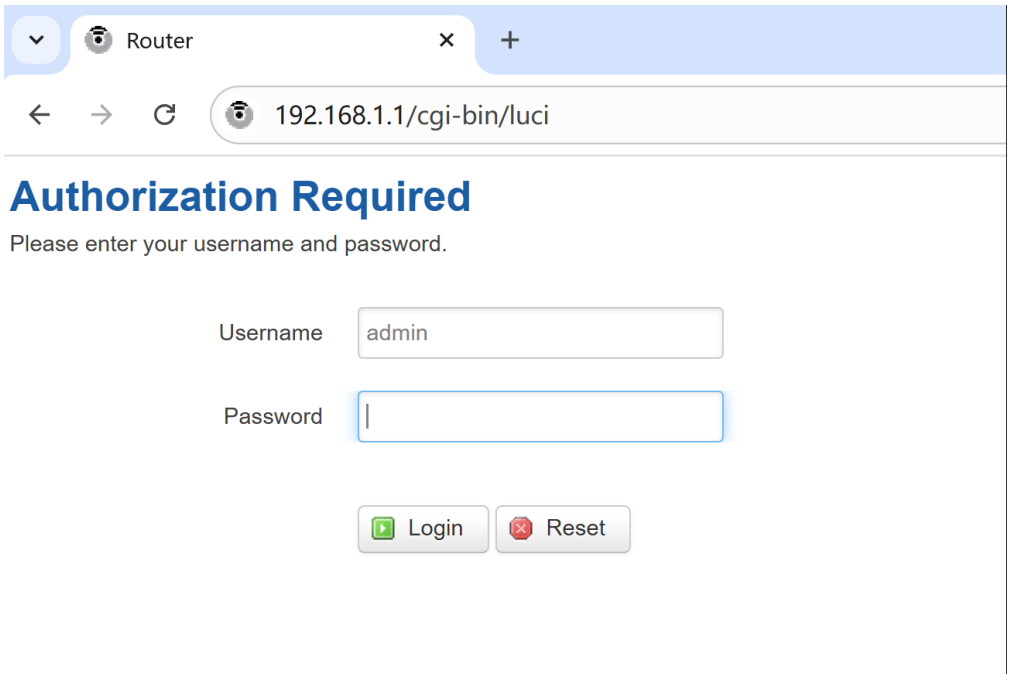
4. Alternatively, connect a laptop to the TG465 Wi-Fi hotspot named "Bivocom_xxxx" and log in with the default password "admin123".

3.0.2 Log in to the Web UI

Enter http://192.168.1.1 in the address bar of a PC browser. Log in with the default username and password, both of which are "admin", and then click Login.

NOTE: To protect the device and your data, Bivocom strongly recommends changing the

password to a strong one after the first login.

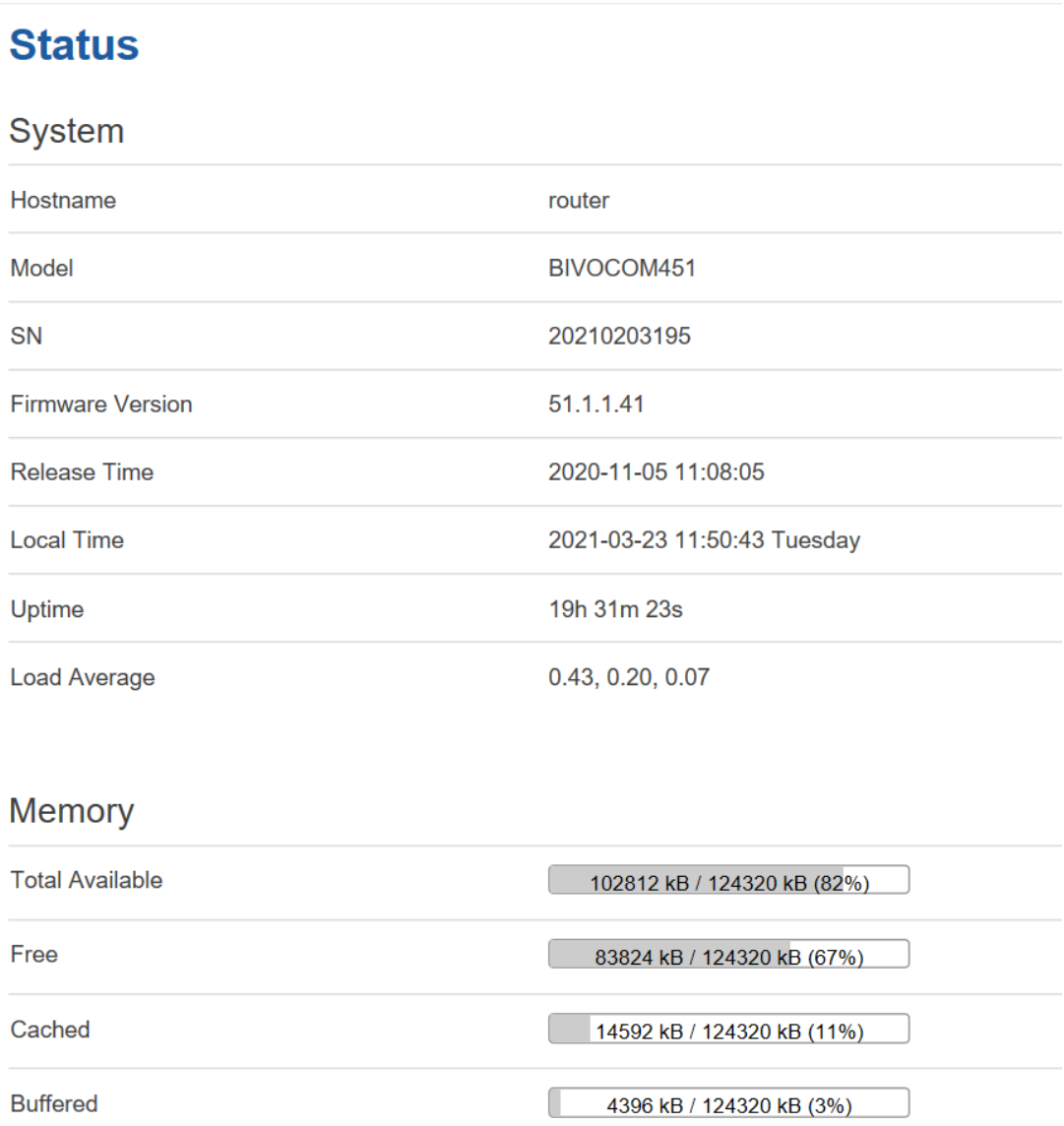


3.1 View

View page shows the basic system information including System, Network, Routes, System Log, VPN Status. The following details are shown:

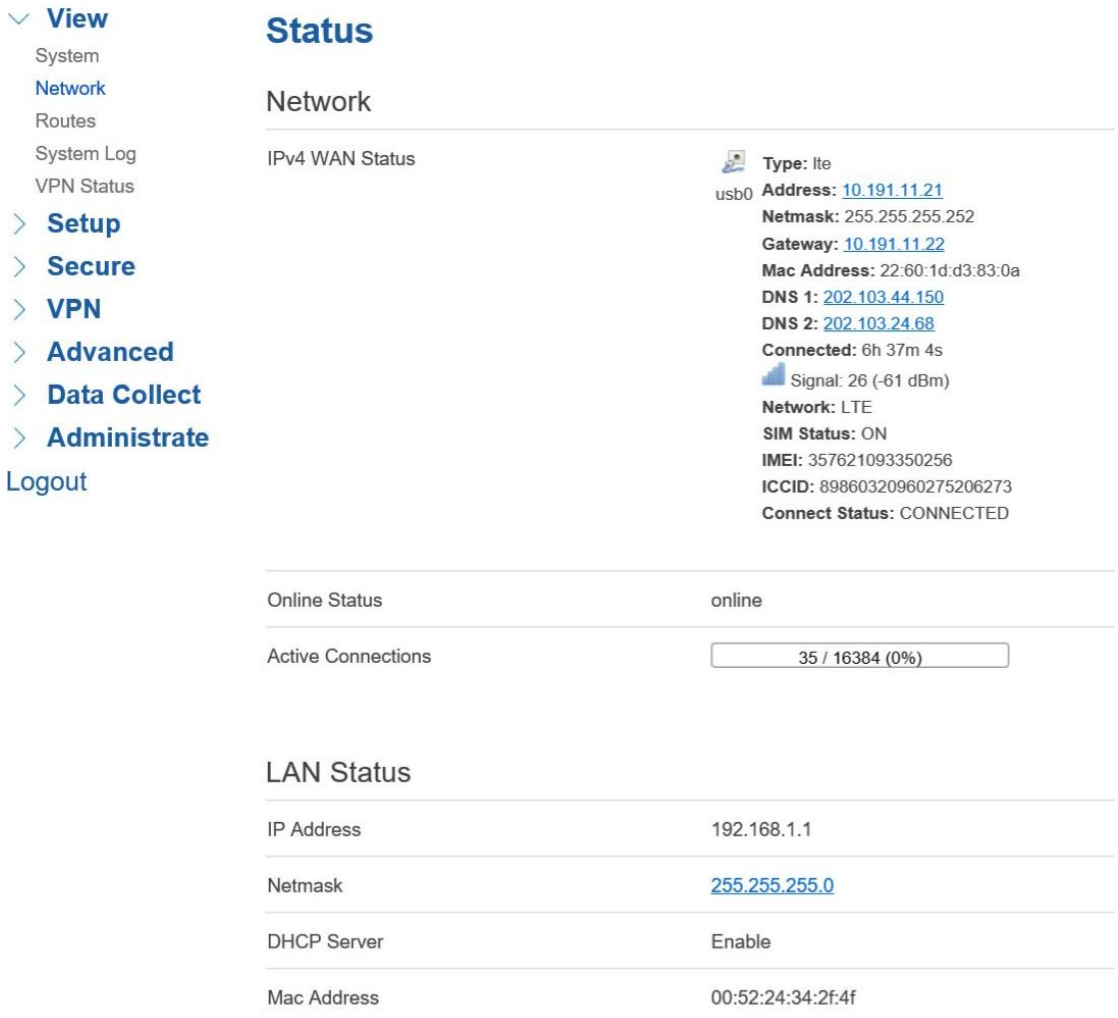
3.1.1 System

System page shows you an overview of TG465 information like SN, Firmware version, Memory usage, etc.



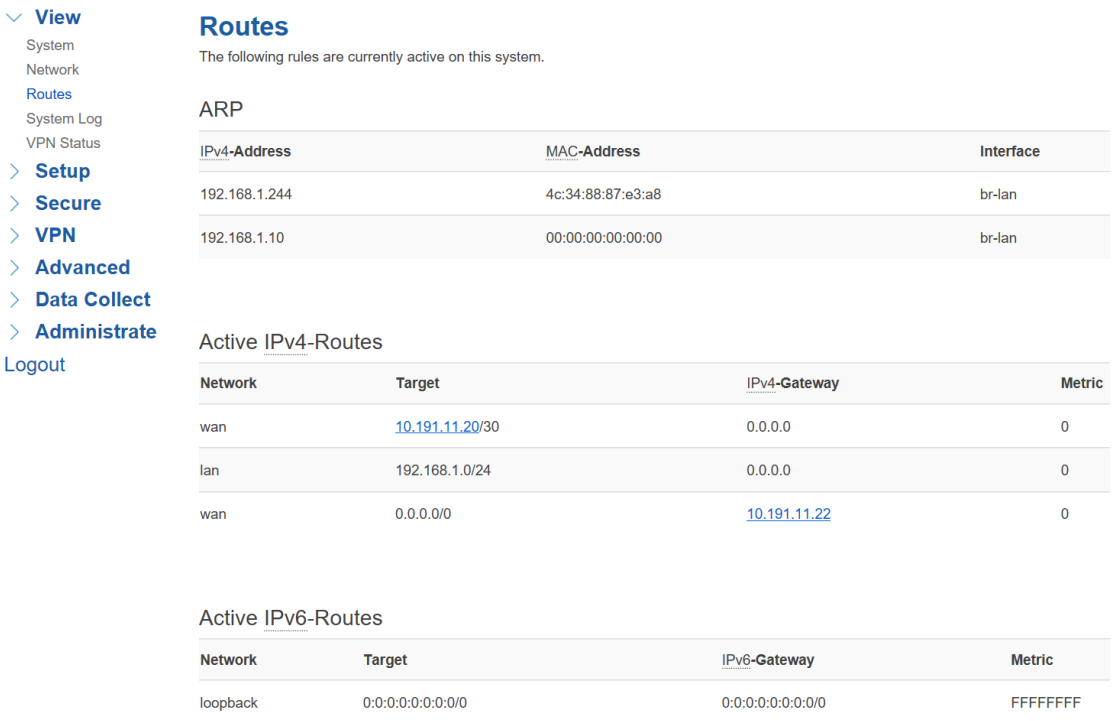
3.1.2 Network

The Network page displays the current WAN status, such as the network type, IP address and connection status. It also shows the LAN status, wireless status and DHCP leases.



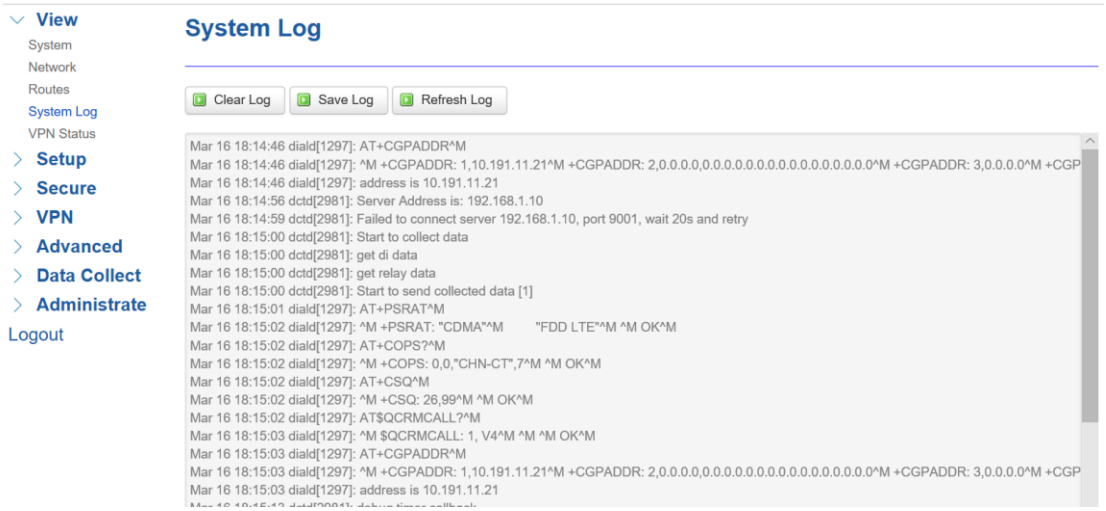
3.1.3 Routing Tables

Display ARP list and active routing tables.



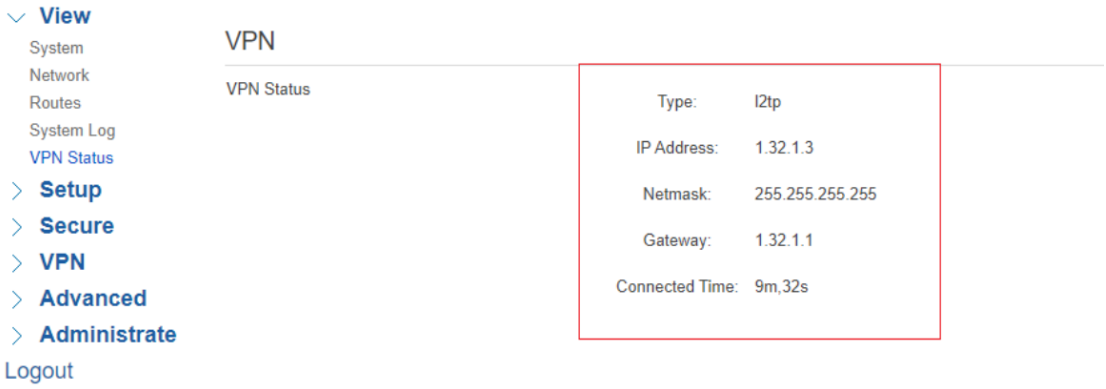
3.1.4 System Log

System log page continuously prints the current running status syslog. It is useful for troubleshooting when there are some features working not as expected. System log page provides three buttons, "Clear Log" will empty current printed log, "Save Log" will save current printed log as a file, and "Refresh Log" which prints out the latest log.



3.1.5 VPN Status

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



3.2 Setup

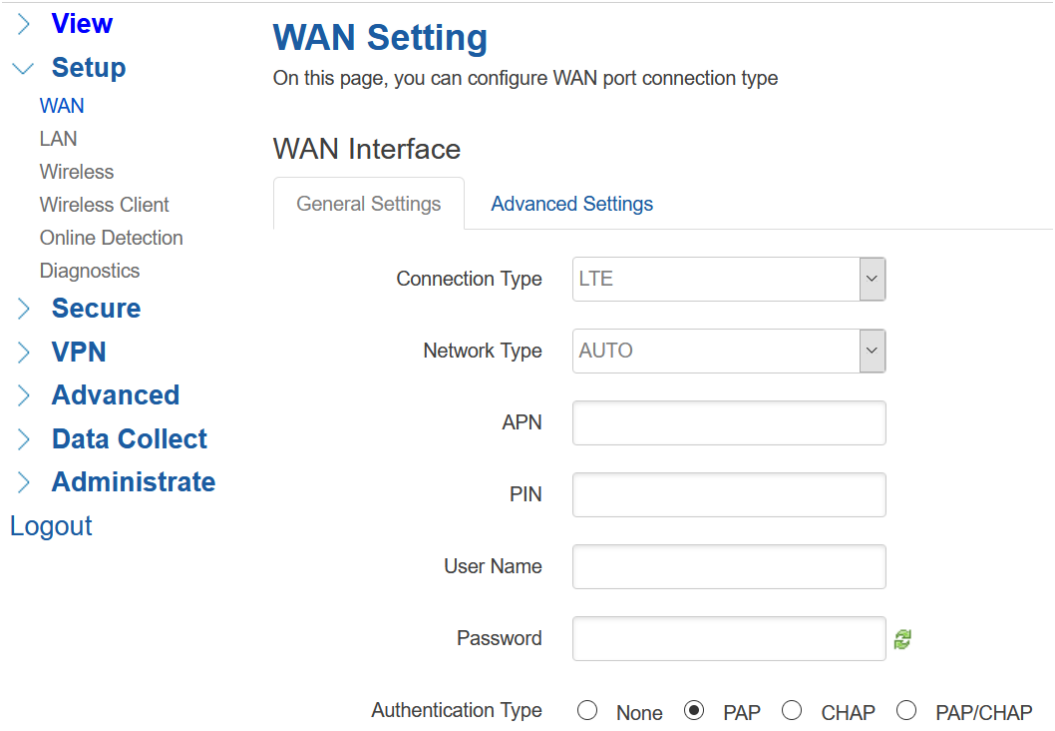
The Setup page includes the WAN, LAN, Wireless, Wireless Client, Online Detection and Diagnostics menus, which are used to configure the corresponding features.

3.2.1 WAN

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

WAN	
Item	**Description**
Static IP	Set a static IP address to connect to the upper network through the WAN port.
DHCP	Obtain an IP address from the upstream DHCP device (such as a gateway) through the WAN port.
PPPoE	Obtain a network connection through the PPPoE protocol. The carrier normally provides the username and password when the network service is purchased.
3G	Dial up a 3G cellular connection when using a 3G SIM card. The APN, username and password may be required by the SIM card provider.
LTE	Dial up a 4G/LTE cellular connection when using a 4G SIM card. The APN, username and password may be required by the SIM card provider.

Unmanaged	Disables the WAN connection; the device then operates in switch mode.



NOTE

1) PIN is the identified password of SIM card. DO NOT input PIN code if not enabled, it will lock the SIM card if set incorrect PIN.

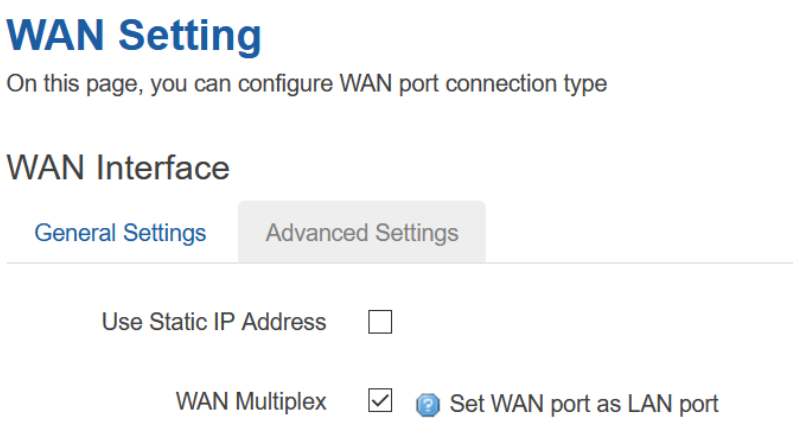
2) PAP/CHAP, Username/password will be requested when you are using a private network SIM card, if you're using public network SIM card, just keep it as null.

3) Select Dial Number when using a 3G connection. The dial number varies by carrier; contact your carrier if you are unsure.

4) WAN Used As LAN

When using LTE/3G connection type to access internet, which means the WAN port is available to change it to a LAN port.

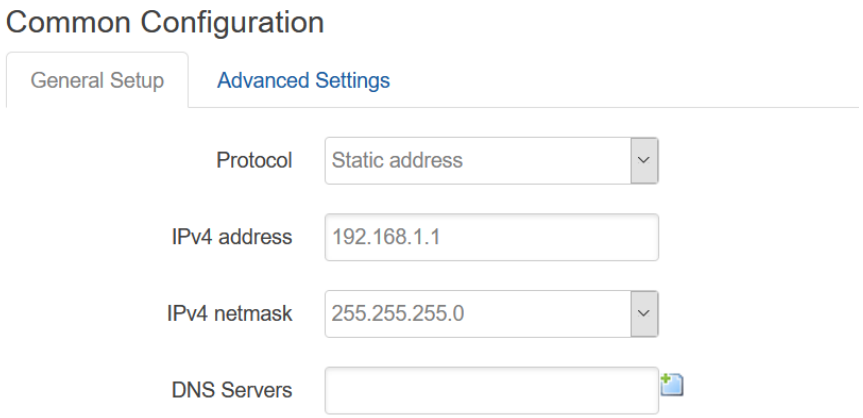
"Advanced Settings" menu provides this option



3.2.2 LAN

The LAN menu is mainly for configuring IP address of TG465, 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.

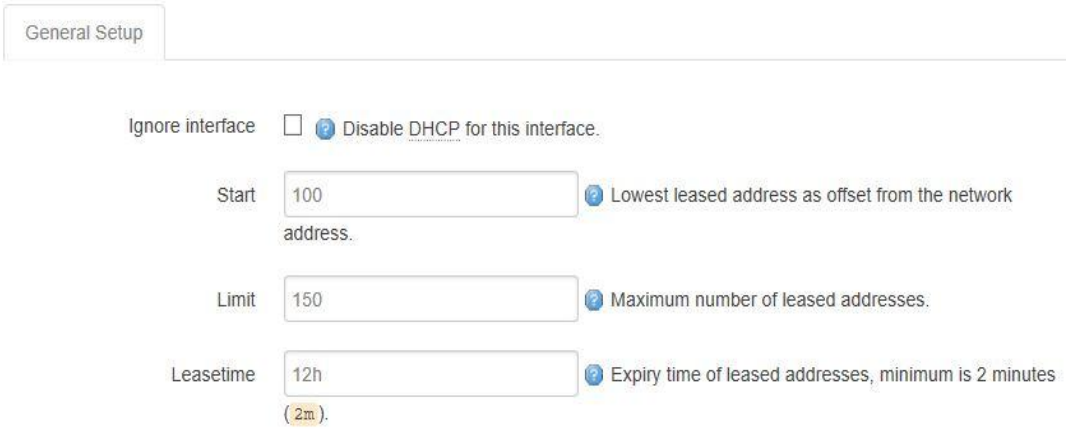
DNS Server

To specify the DNS server, leaving it blank uses the upstream network DNS by default.

Advanced Settings

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

- **Lease time**

Lease duration (the time for which the IP address is assigned).

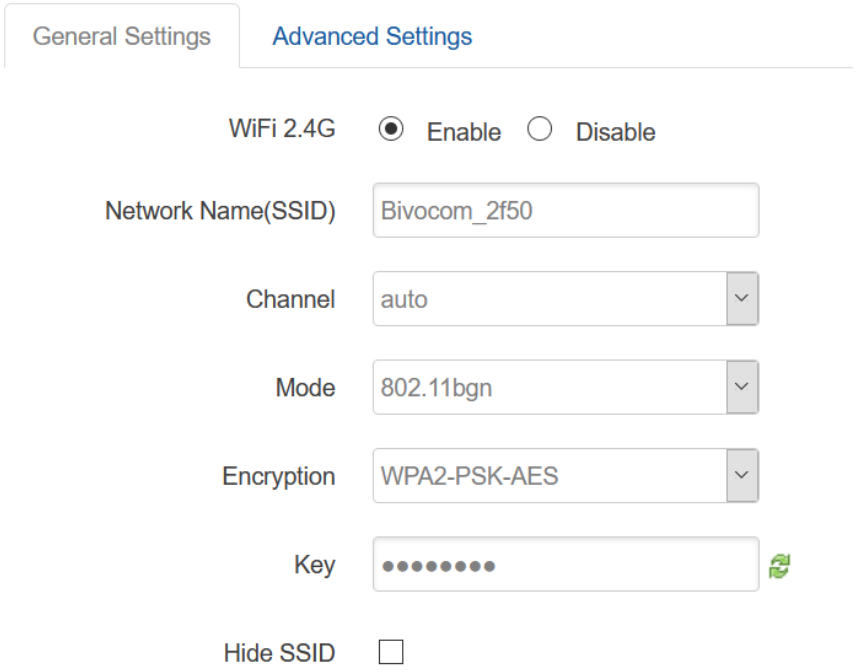
3.2.3 Wireless (Optional)

The Wireless menu is mainly for configuring the Wi-Fi, SSID, mode, encryptions, etc.

Wireless Setting

On this page, we can configure Wireless general or advanced parameters

Interface Configuration



Wireless (Optional)	
Item	**Description**
Wi-Fi 2.4G	Provide Enable or Disable option for the Wi-Fi function switch.
Network Name (SSID)	Wi-Fi network name setting.
Channel	Support 1-13 channels or auto options, default value is auto, channel can be changed automatically.
Mode	Supports the 802.11b, 802.11g, 802.11bg and 802.11bgn modes, which determine the maximum Wi-Fi speed: up to 11 Mbps for 802.11b, 54 Mbps for 802.11g and 300 Mbps for 802.11bgn.
Encryption	Configure the way of encryption, select from No Encryption, WPA2-AES-RADIUS, WPA2-PSK-AES, WPA-PSK-AES. While for RADIUS option, it provides for configuring RADIUS Auth Server address, shared key, etc.

Key	Wi-Fi password, users need to enter it to access the internet. The minimum length of password is 8 bytes.
Hide SSID	When Hide SSID is enabled, SSID is invisible, and users need to enter the SSID to share the Wi-Fi.

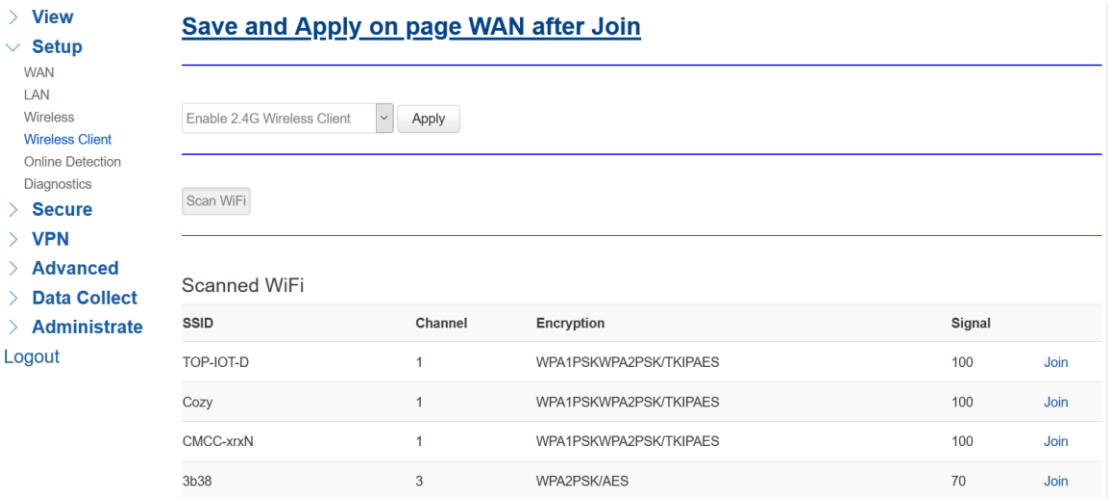
NOTE:

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 (Optional)

Wireless Client menu provides a way to connect to a local Wi-Fi hotspot, this setting related to WAN setting when you select Static IP or DHCP connection type.

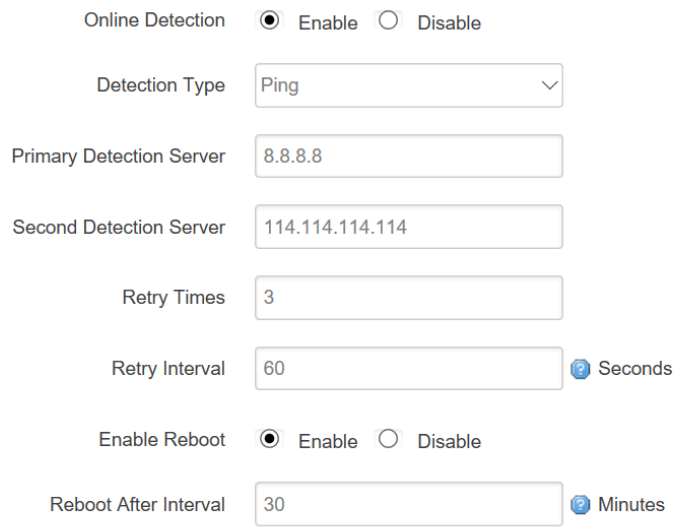
Enable wireless client and apply it, it will list all Wi-Fi hotspots which can be detected. Join one of them, will ask you input the password if hotspot request.



3.2.5 Online Detection

The online-detection feature checks the network connection status periodically, if there has issue of connection, gateway will auto reconnect. If it fails to reconnect after times of trial, gateway will reboot automatically to try to recover the network.

Online Detection



Online Detection	
Item	**Description**
Detection Type	There are 3 types: ping, traceroute and DNS.
Primary Detection Server	It can be an IP address or a Domain Name.
Second Detection Server	If primary detection server fails, then gateway will auto detect the second detection server.
Retry Times	Set the maximum number of retries to detect the network connection failure.
Retry Interval	Set the online detection interval time to ensure network connection.
Enable Reboot	Enable reboot device after maximum retry times.
Reboot After Interval	Set the reboot interval after maximum retry times.

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 is cached, it may show the gateway is online even it is offline.

Common Issues:

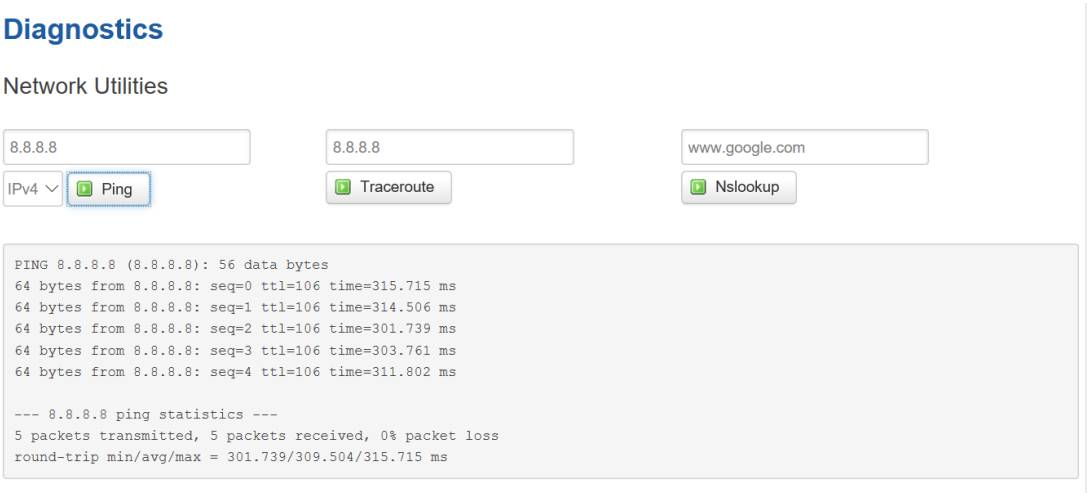
- Network Status shows as Offline: Check if SIM card and antennas are installed well, fill the correct APN setting if necessary, check current SIM card status with operator/SIM provider.
- Device Keeps Rebooting Every 30 minutes/Often Re-dial even with Good Signal: Change **Online Detection** IP addresses to the one can ping without issue if using private network (4G/Wire network).

3.2.6 Diagnostics

Diagnostics feature allows users to 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 gateway is online or not. While nslookup is used to analyze a domain.



1) Ping

Click Ping to check whether an IP address responds, as shown below.

2) Traceroute

Click Traceroute; the response is similar to the example below.

3) Nslookup

Click NSLookup; the response is similar to the example below.

3.2.7 Quick Check

- SIM card, antennas are well installed when using LTE mode

- APN and Username/Password shall be entered according to the requirements of SIM provider

- The IP addresses in Online Detection need to be changed if using private network SIM cards, it will stay in Offline status if left unchanged and keep rebooting every 30 minutes (default

interval) due to Online Detection failure.

- Online indicator will light when Online Detection succeed

- Wi-Fi AP and STA shouldn't be enabled at the same time

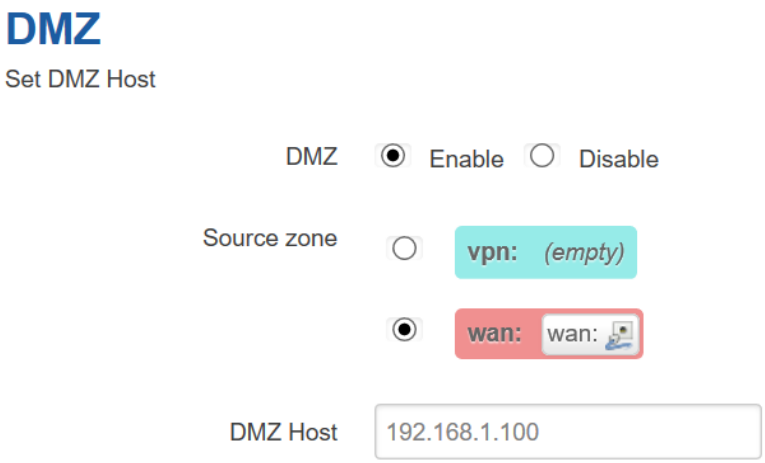
- Web UI address will be changed to the new LAN IPv4 address, ensure PC stays in DHCP mode or in the same subnet.

3.3 Security

The Security menu is for configuring the firewall, to ensure the security of accessing to the Internet, and implement the port forwarding, access control, data packet filtering, and other functions.

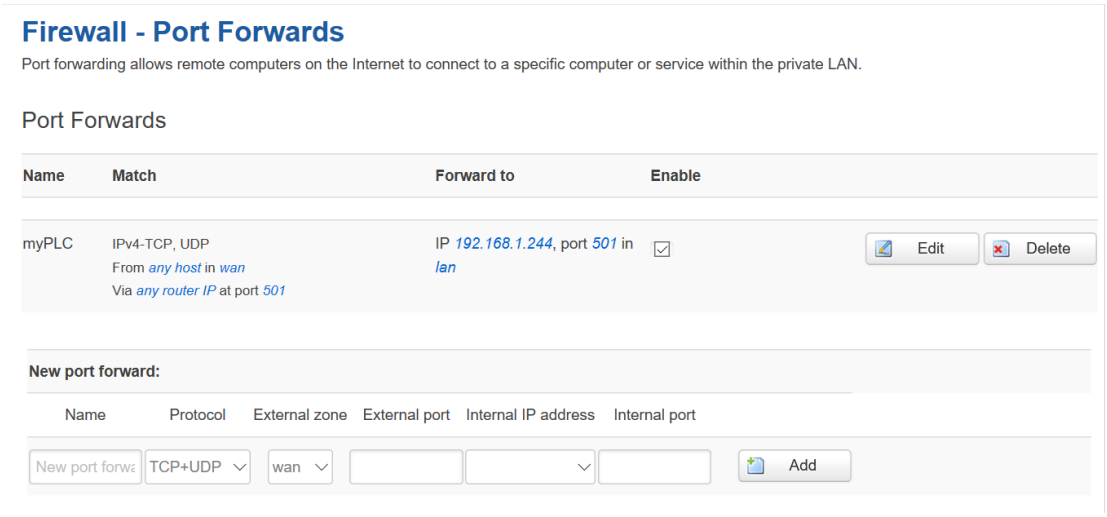
3.3.1 DMZ Host

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



3.3.2 Port Forwards

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



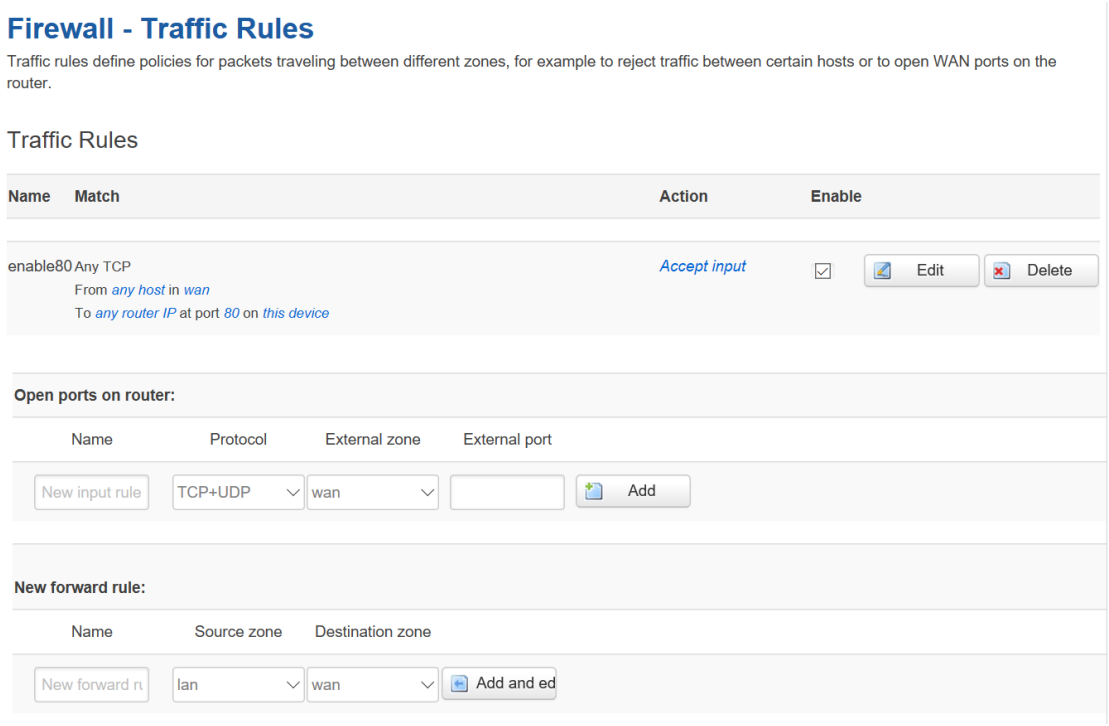
Port Forwards	
Item	**Description**
Name	The name of the rule being created.
Protocol	Select from TCP, UDP, and TCP/UDP.
External Zone	The source zone which can access local IP addresses, select from WAN and VPN
External port	Enter the TCP/UDP port to which incoming packets are forwarded.
Internal IP address	The destination IP address that traffic from the external zone is forwarded to.
Internal port	The destination port after port forwarding. The external and internal ports are normally the same, but they can differ.

After configuring the above, click **Add**, then a new rule will be added, and click **Save & Apply**, to have the rule take effect. Click **Edit** button to enter detail settings page.

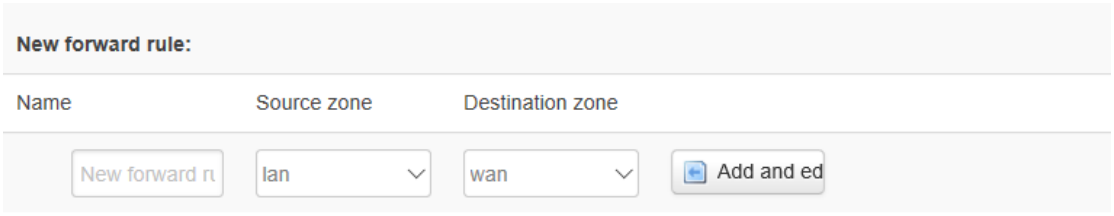
Port Forwards Details	
Item	**Description**
Source zone	Select from LAN, WAN and VPN (if connected)
Source MAC address	Specify the MAC address which can access local network.
Source IP address	The source IP address should be able to access local network
Source port	Input the TCP or UDP port through which incoming packets are forwarded.
External IP address	Only match incoming traffic directed at the given IP address.
External port	Match incoming traffic directed at the given destination port or port range on this host
Internal zone	Select from LAN,WAN and VPN (if connected) that needs to be forwarded to
Internal IP address	Enter the IP address to which packets are forwarded after being received on the incoming interface.
Internal port	Enter the destination TCP/UDP port (s) for forwarded packets.
Enable NAT Loopback	It enables local devices to reach the forwarded service via the external IP, solving the hairpin routing issue.
Extra arguments	Passes additional arguments to iptables. Use with care.

3.3.3 Traffic Rules (ACL Configurations)

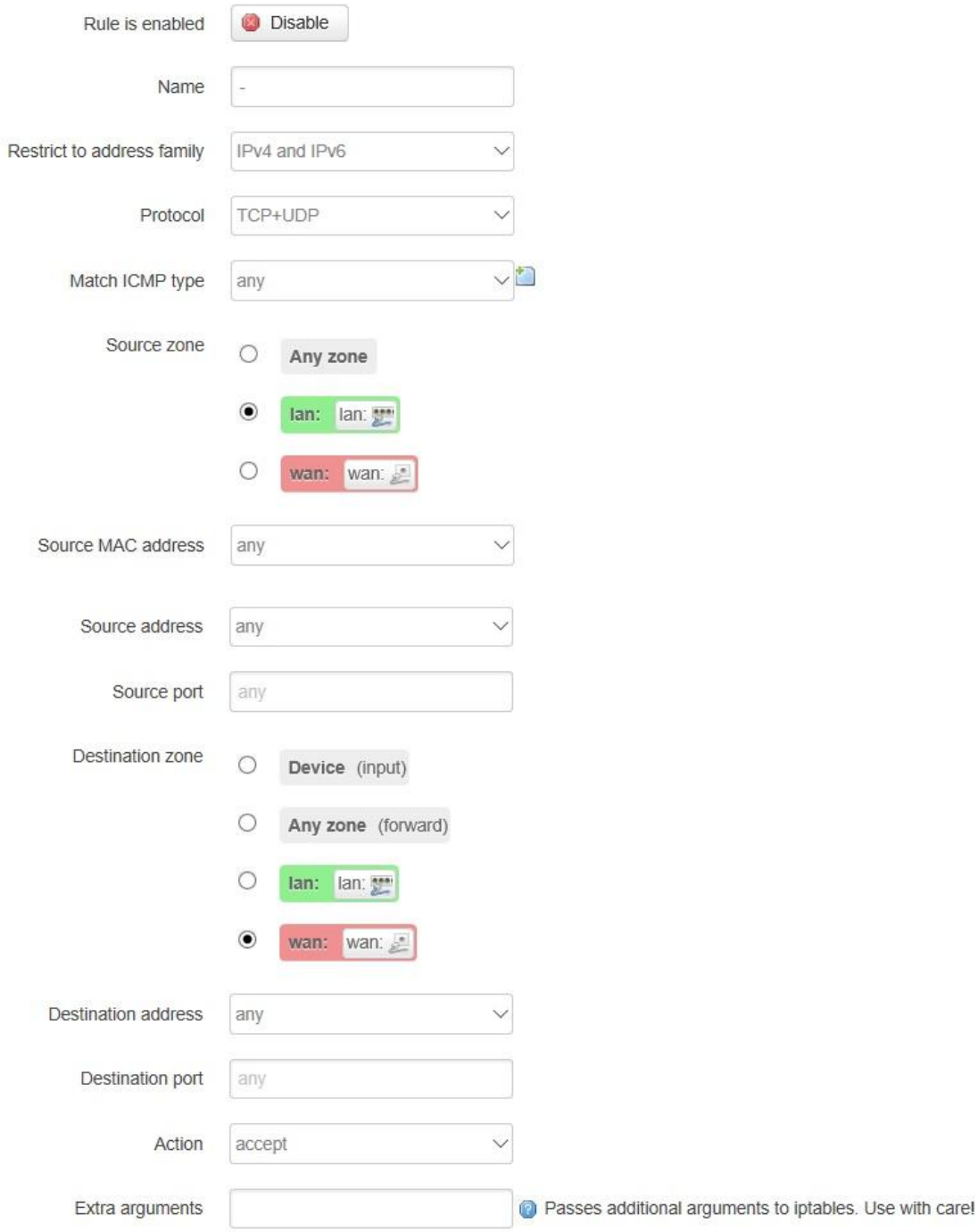
Traffic rules are used for firewall settings such as opening ports on the gateway. For example, to allow remote access to the gateway configuration page, open port 80.



In addition, Traffic rules can be used to create some access control rules, it can be from LAN to WAN, or WAN to LAN.



Click Add and Edit to access more detailed matching conditions.


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!

Traffic Rules (ACL)	
Item	**Description**
Name	The name of the ACL rule being created.
Restrict to address family	Select from IPv4 and IPv6, IPv4 Only, and IPv6 Only
Protocol	Select from TCP, UDP, TCP+UDP and ICMP
Match ICMP type	Select from any, echo-reply, destination-unreachable, network-unreachable, host-unreachable, protocol-unreachable, port-unreachable, fragmentation-needed, source-route-failed, network-unknown, host-unknown, network-prohibited, host-prohibited, TOS-network-unreachable, TOS-host-unreachable, communication-prohibited, host-precedence-violation, precedence-cutoff, source-quench
Source zone	Select from LAN, WAN, VPN (if connected) and Any Zone
Source MAC address	Specify the MAC address to be forwarded and controlled.
Source address	Source network address
Source port	Source network port
Destination zone	Select from LAN, WAN, VPN (if connected), Device (input), and Any Zone (forward)
Destination address	Select any, or specify the IP address
Destination port	Specify the port, a port range, or any.
Action	Select from accept (Allow data packet to go through), drop (Drop data packet), reject (Drop data packet, and return an unreachable data packet) and don't track (No action).
Extra arguments	Passes additional arguments to iptables. Use with care.

3.3.4 Custom Settings

Custom firewall rules can also be added. Because these rules are iptables entries, this is recommended only for advanced users who are familiar with the iptables command. Add new rules below the existing ones and do not delete the existing rules.

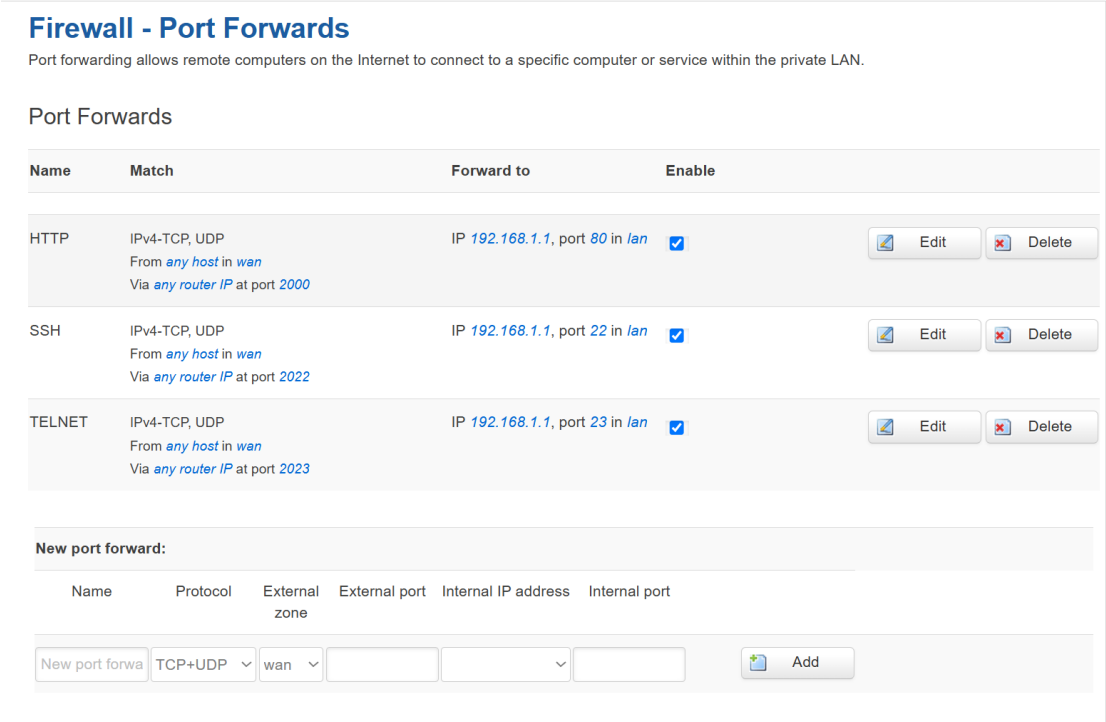
Scenario 1: Remote Access Web UI/CLI

Objective: Remote access Web UI/CLI (telnet/SSH)

Prerequisites: remotely accessible, telnet/SSH enabled

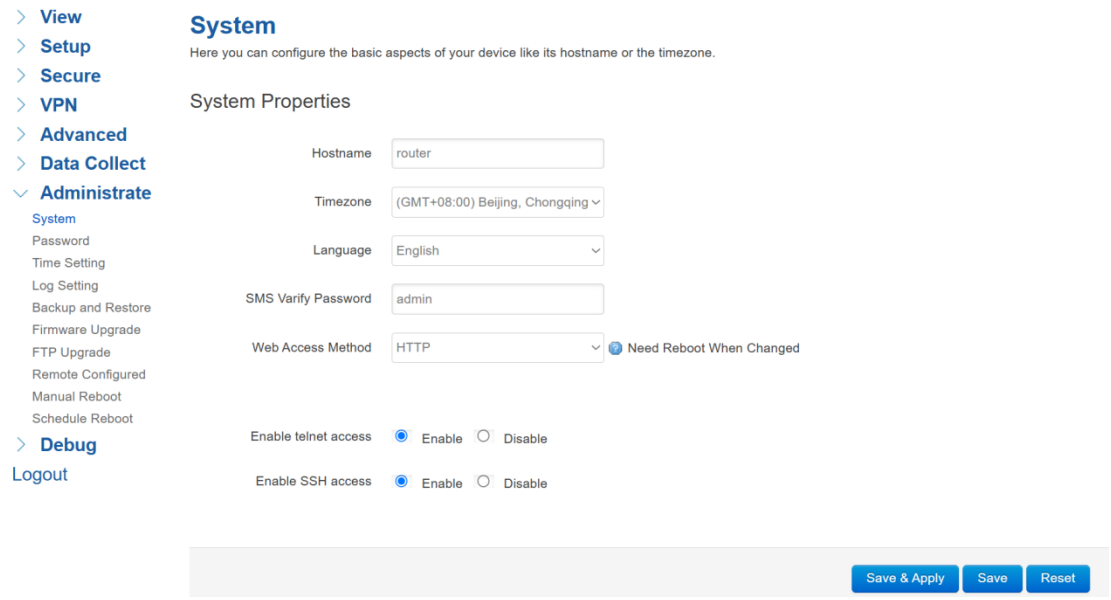
Configuration Steps:

1. Go to Secure > Port Forwards page to Enter the External Port (2000/2022/2023) of WAN IP (172.17.5.75) to the Internal Port (Web UI:80/SSH:22/telnet:23) of LAN IP (192.168.1.1) address.



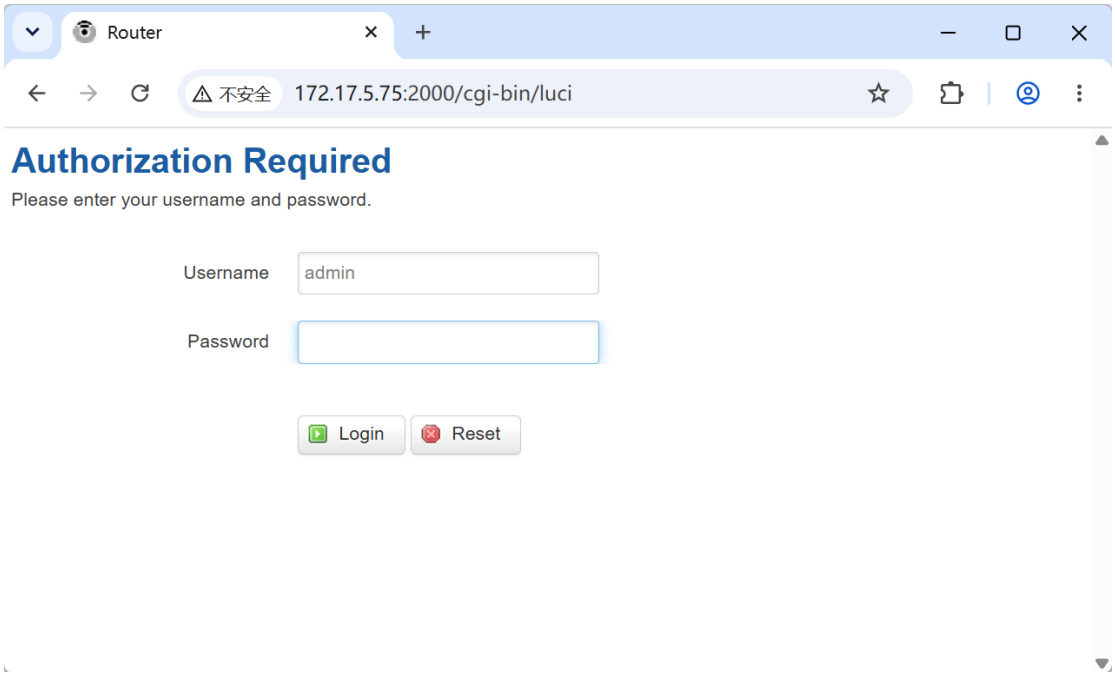
2. Click **Add** > **Save & Apply** button.

3. Go to **Administrate** > **System** page, enable SSH and telnet access.

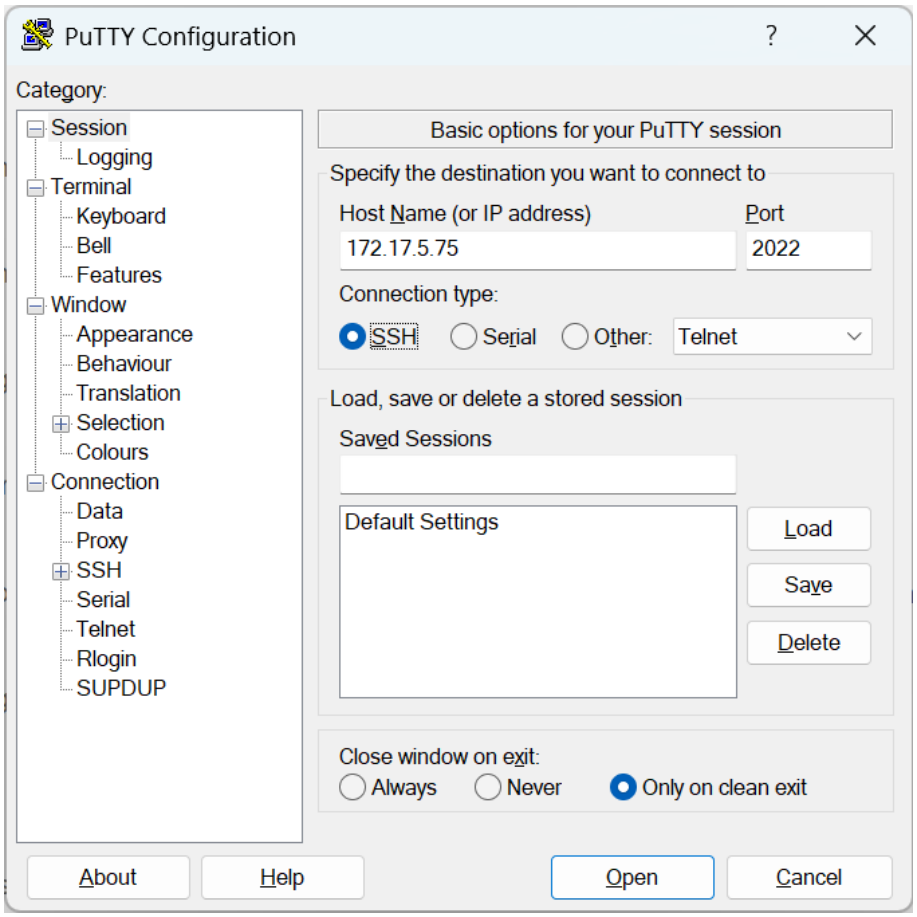


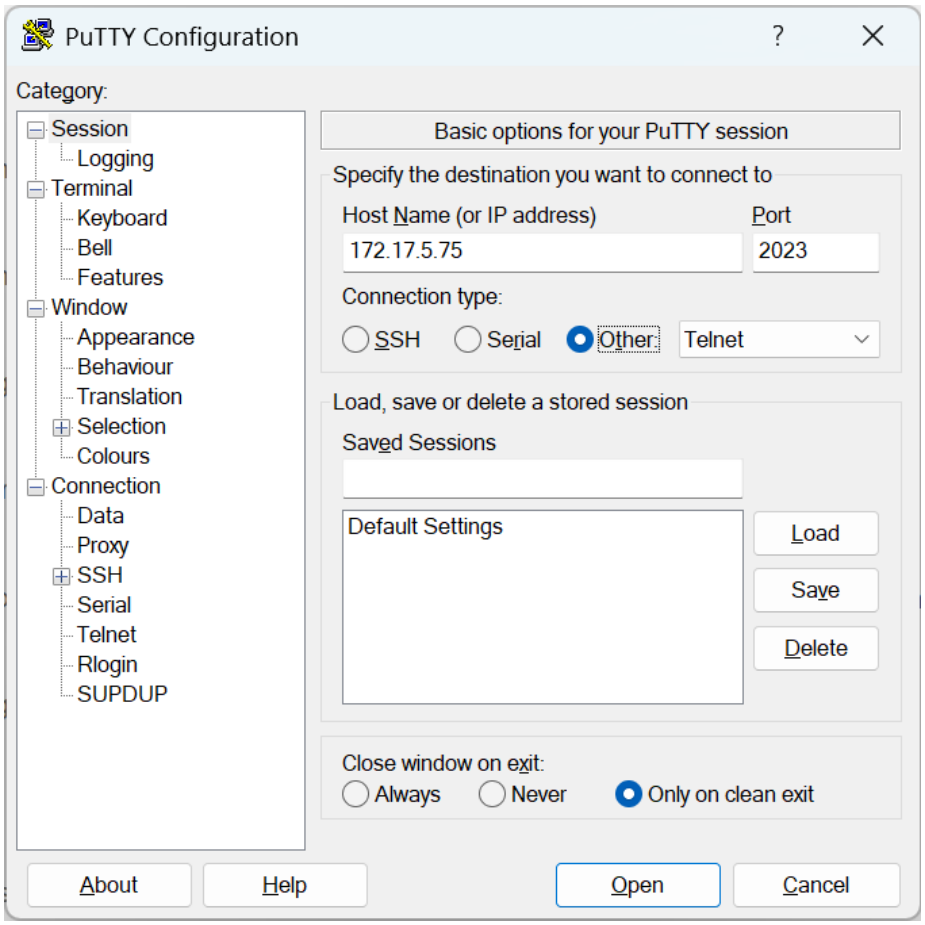
Verification Method:

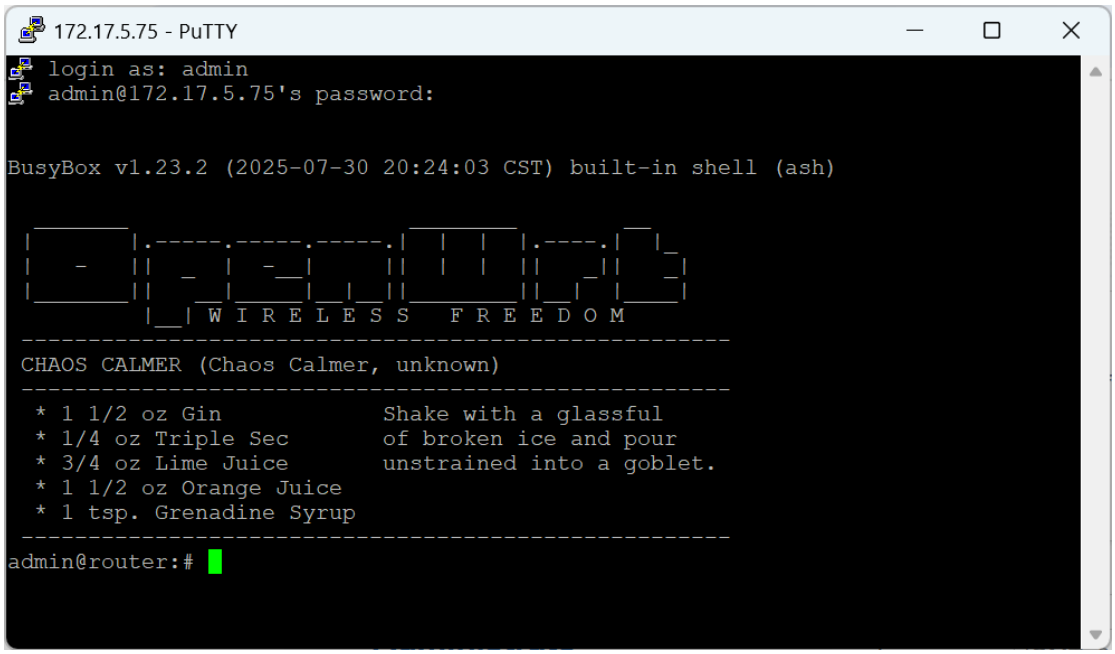
1. Open browser on remote PC, fill in http://172.17.5.75:2000 to access Web UI.http://172.17.5.75:2000/



2. Use Putty to SSH (172.17.5.75:2022)/telnet (172.17.5.75:2023) access CLI.


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
172.17.5.75
2022
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

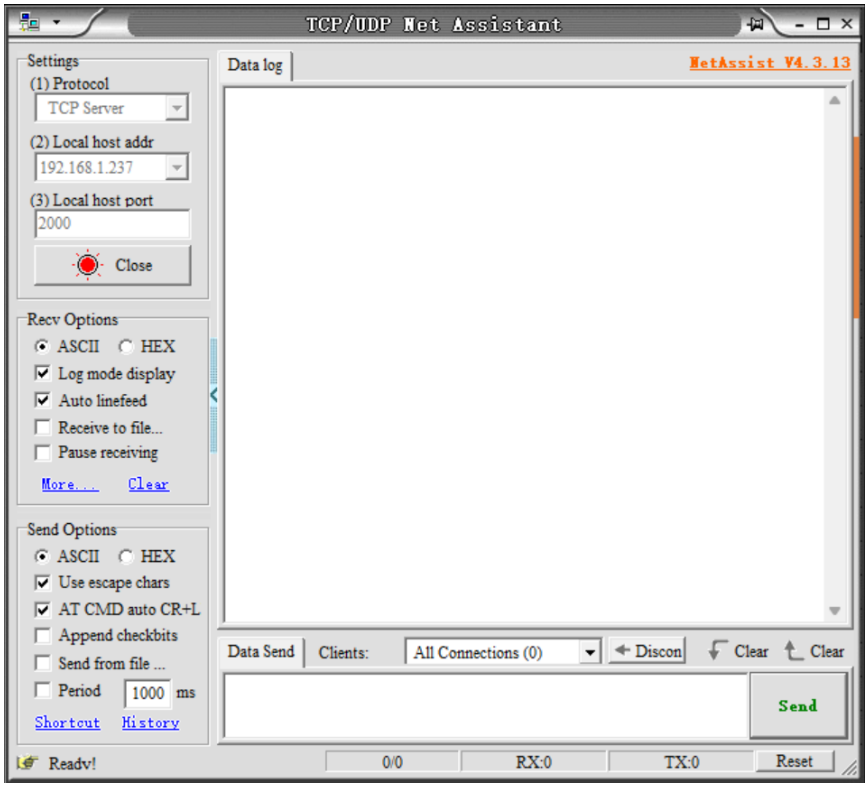

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
172.17.5.75
2023
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel



Scenario 2: Remote Access Internal Device

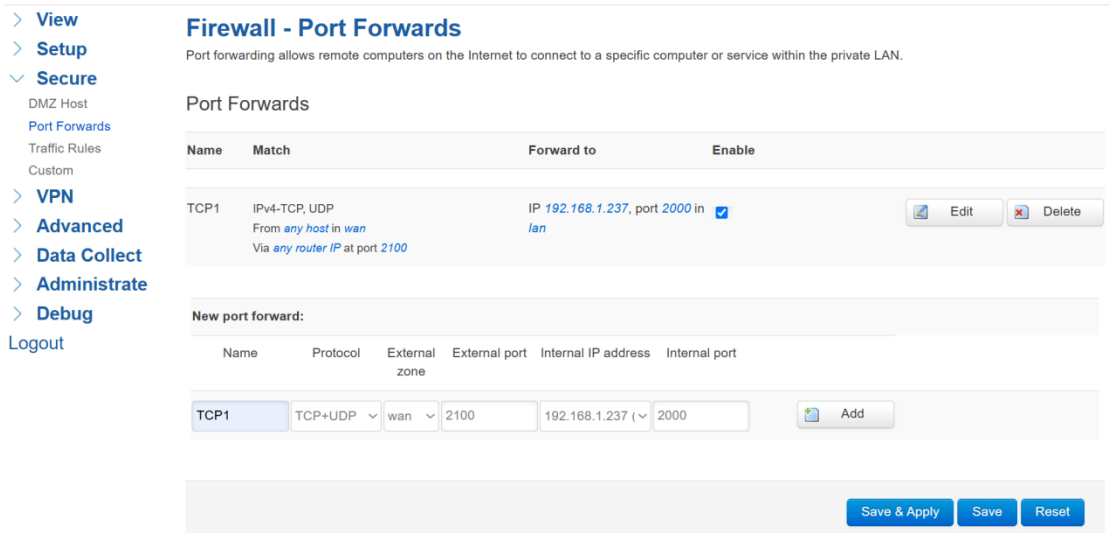
Objective: Remote access LAN devices through WAN IP address

Prerequisites: External WAN IP address is available to be accessed, service is running on the specific port of LAN IP devices, for example running TCP server on PC at port 2000



Configuration Steps:

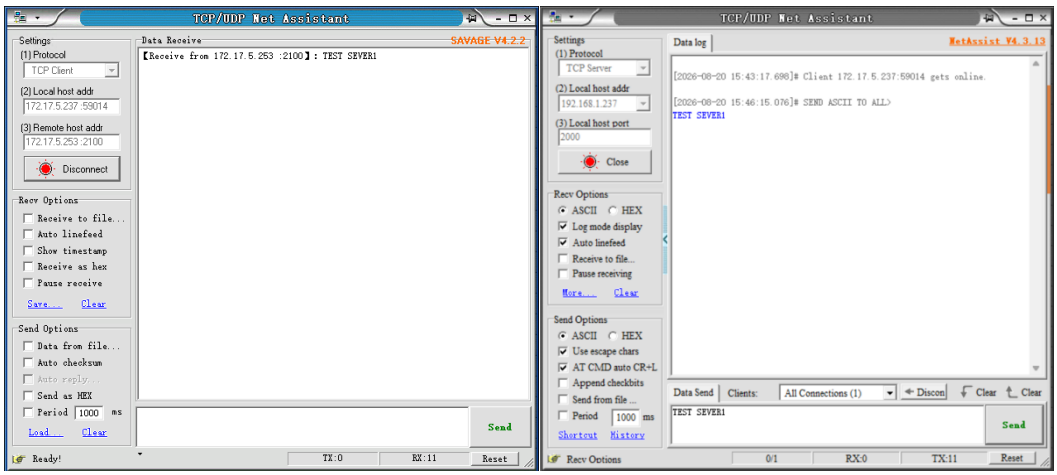
1. Go to **Secure** > **Port Forwards** page to input the **External Port** (2100) of WAN IP (172.17.5.253) to the **Internal Port** (2000) of LAN IP (192.168.1.237) address.



2. Click **Add** > **Save & Apply** button.

Verification Method:

1. Go to remote PC to verify WAN IP communication.
2. Open NetAssistant tool on remote PC to run TCP Client and connect to TCP server running on internal PC (192.168.1.237).
3. Send messages to TCP server, check the data log.



Common Errors:

- Network connection issue: Go to **Setup** > **Diagnostics** page, ping the remote IP address, use remote PC to ping the WAN IP address. Ensure SIM is well inserted and connected to the Internet.
- Firewall blocking: Check firewall configurations of both PC.

3.4 VPN

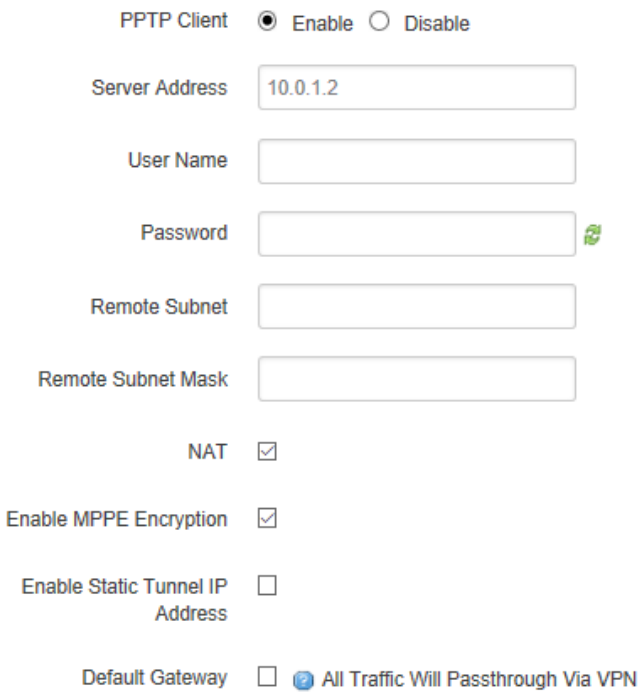
VPN is used to establish a virtual private channel, and all the data in this channel will be encrypted to ensure data security during transmission.

TG465 supports several types of VPN: PPTP, L2TP, IPSec, OpenVPN and GRE.

3.4.1 PPTP

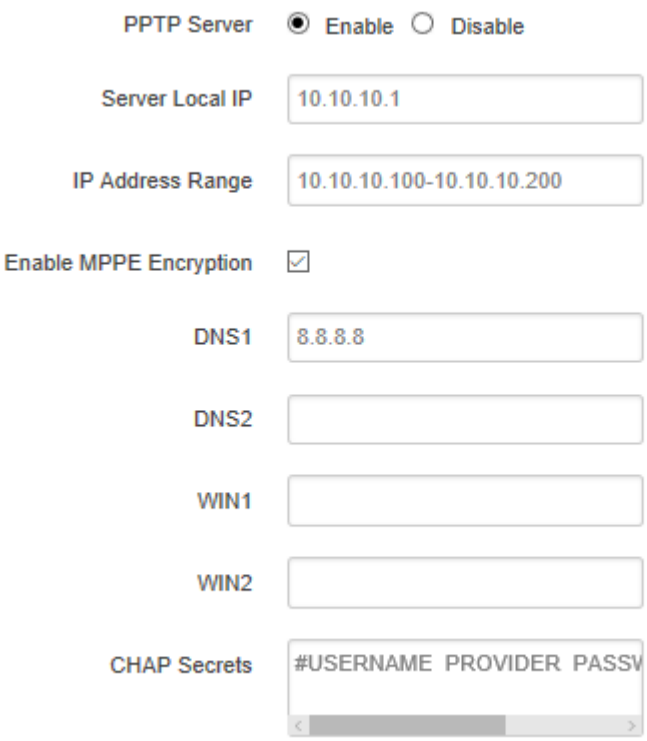
You can configure either the PPTP client or the PPTP server, but not both at the same time; using both may cause unexpected issues.

1) PPTP Client



PPTP Client	
Item	**Description**
Server Address	To enter the IP address or Domain Name of PPTP server.
Username / Password	Enter the username and password provided by the server.
Remote Subnet	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.
Remote Subnet Mask	Enter the remote subnet mask; it is normally 255.255.255.0.
NAT	All packets come from ppp0 and their source IP address is replaced with the IP address of ppp0.
Enable MPPE Encryption	Enable MPPE encryption.
Enable Static Tunnel IP Address	Enabling this option fixes the PPTP tunnel IP address.
Default Gateway	Click Default Gateway to establish a default route under ppp0; all data then uses this route.

2) PPTP Server



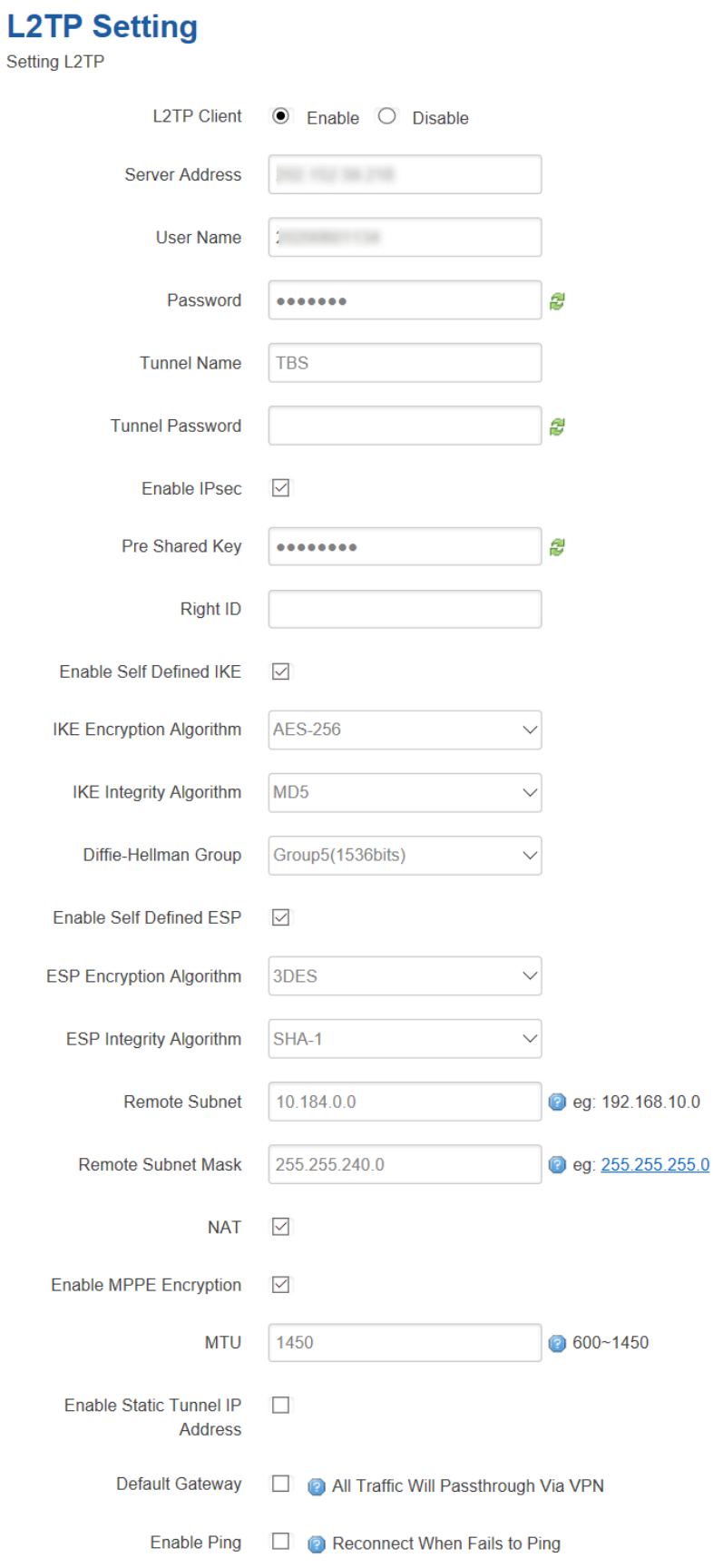
PPTP Server	
Item	**Description**
Server Local IP	The local IP address of the current device.
IP Address Range	Defines the tunnel IP address range for PPTP clients.
Enable MPPE Encryption	Enable MPPE encryption.
NAT	Enable NAT traversal.
DNS1/DNS2	Enter the assigned DNS server address.
WINS1/WINS2	Enter the WINS server address.
CHAP Secrets	Create a username and password under CHAP Secrets using the following format: Username<space>*<space>password<space>* For example, a username of Test with the password test123 is entered as follows,

	Test * test123 *
Client Subnet	Set the client subnet if communication with a device on the peer subnet is required.

3.4.2 L2TP

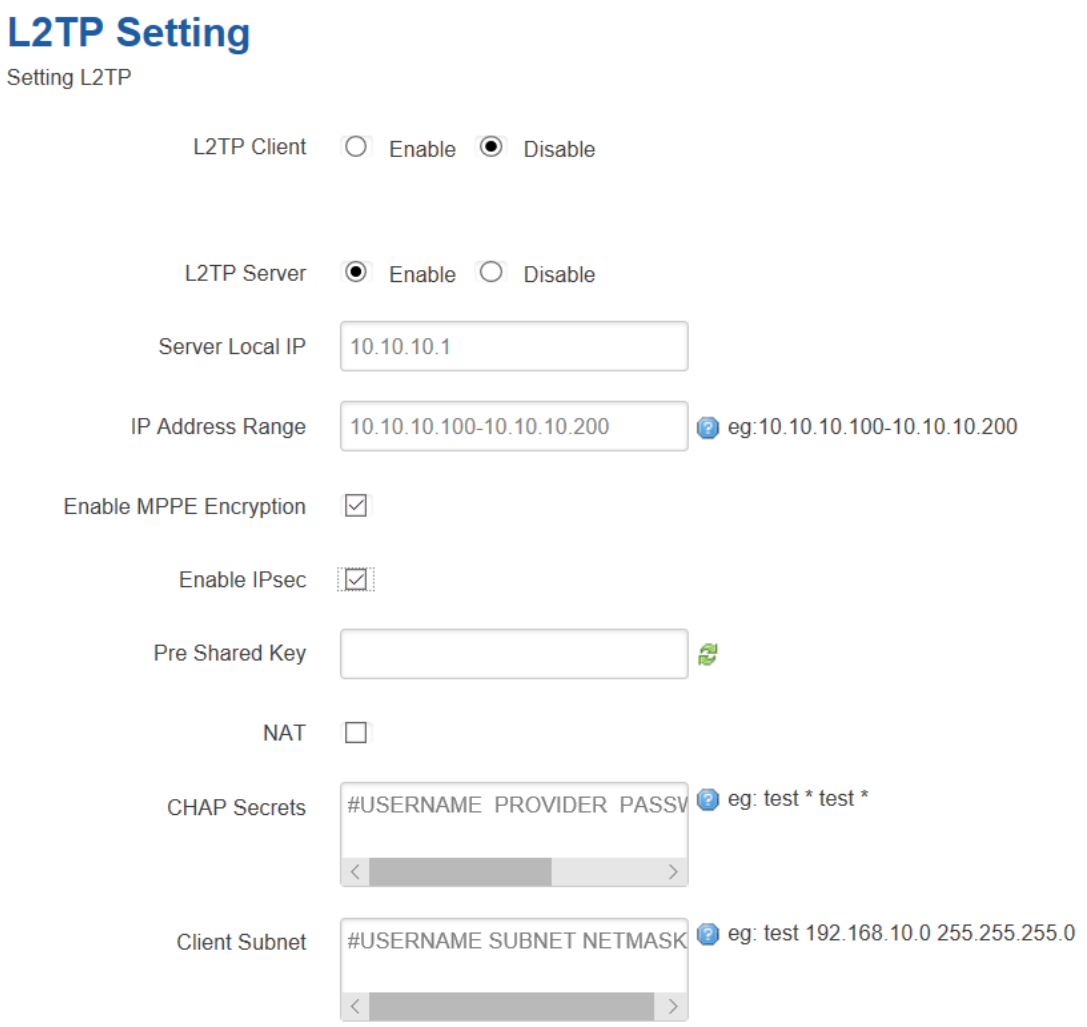
You can also configure either the L2TP client or the L2TP server, but not both at the same time, as that may cause unexpected issues.

1) L2TP Client



L2TP Client	
Item	**Description**
Server Address	To enter the IP address or Domain Name of L2TP server.
Username / Password	Enter the username and password provided by the server.
Tunnel Name	Enter the name of current tunnel
Tunnel Password	The password of L2TP tunnel
Enable IPsec	Enable IPsec encryption.
Pre Shared Key	Enter the pre-shared key provided by the IPsec server.
Right ID	The Right ID of IPsec
Enable Self Defined IKE	Enable IKE parameters provided by the IPsec server
Enable Self Defined ESP	Enable ESP parameters provided by the IPsec server
Remote Subnet	Enter the IP address of the remote subnet
Remote Subnet Mask	Enter the remote netmask that L2TP protects
NAT	Enable NAT traversal.
Enable MPPE Encryption	Enable MPPE encryption.
MTU	Set the maximum transmission unit. Range: 600-1450
Enable Static Tunnel IP Address	Set a static tunnel IP of L2TP client
Default Gateway	This enables all data to pass through the VPN

L2TP Server


L2TP Setting
Setting L2TP
L2TP Client
Enable
Disable
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
Enable IPsec
Pre Shared Key
NAT
CHAP Secrets
#USERNAME PROVIDER PASSV
eg: test * test *
Client Subnet
#USERNAME SUBNET NETMASK
eg: test 192.168.10.0 255.255.255.0

L2TP Server	
Item	**Description**
Server Local IP	The local IP address of the current device.
IP Address Range	Defines the tunnel IP address range for L2TP clients.
Enable MPPE Encryption	Enable MPPE encryption.
Enable IPsec	Enable IPsec encryption.
Pre Shared Key	Enter the pre-shared key provided by the IPsec server.
NAT	Enable NAT traversal.
CHAP Secrets	Create a username and password under CHAP Secrets using the following format: Username<space>*<space>password<space>* For example, a username of Test with the password test123 is entered as follows, Test * test123 *
Client Subnet	Set the client subnet if communication with a device on the peer subnet is required.

3.4.3 IPSec

IPsec (Internet Protocol Security) is a protocol suite that secures IP communications by providing encryption, source authentication, data integrity, and replay protection. It operates in two modes – transport (encrypts only the payload) and tunnel (encrypts the entire IP packet) – and is primarily used to build secure VPNs for remote user access and site-to-site connectivity over untrusted networks, making it a widely adopted standard for network-layer security.

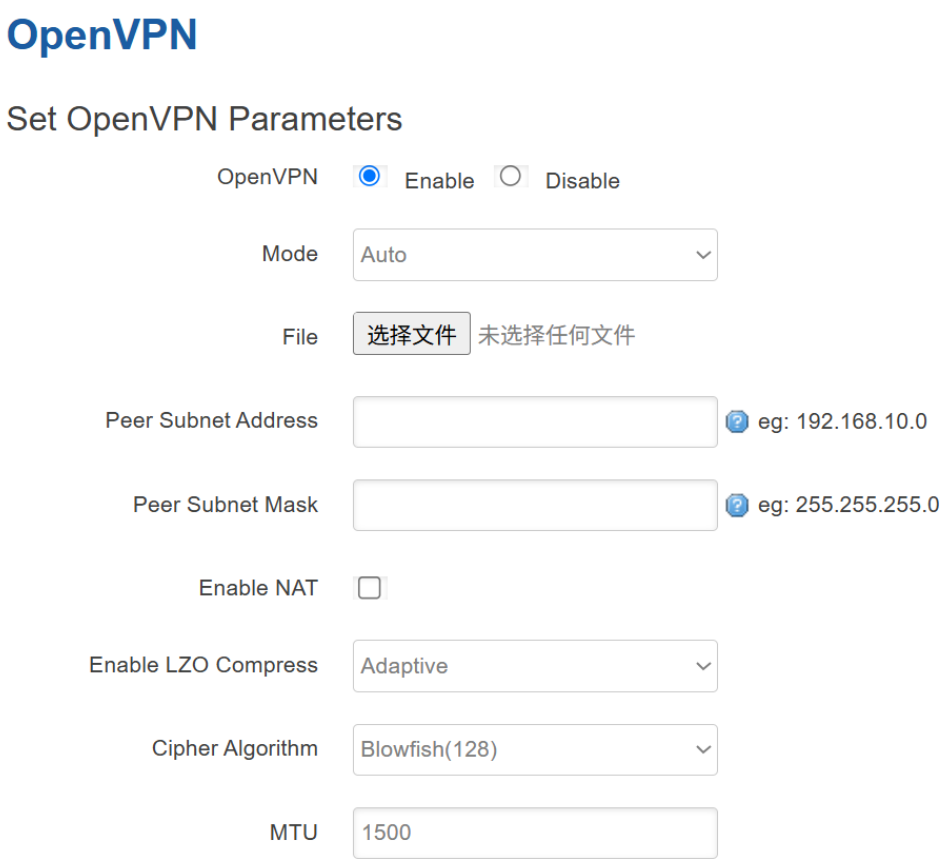
IPSec	(•) Enable ( ) Disable
Peer Address	%any
Negotiation Method	Main
Tunnel Type	Site To Site
Local Subnet	192.168.4.0/24
Peer Subnet	192.168.5.0/24
IKE Encryption Algorithm	AES-128
IKE Integrity Algorithm	SHA-1
Diffie-Hellman Group	Group14(2048bits)
IKE Life Time	28800
Authentication Type	Pre-shared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

IPsec	
Item	**Description**
Peer Address	IP address or domain name of the remote VPN gateway.
Negotiation Method	Select from IKEv1 exchange mode: Main (6-packet, secure) and Aggressive (3-packet, faster).
Tunnel Type	Defines the tunnel endpoints: Site-to-Site (gateway-to-gateway), Site-to-Host (gateway-to-client), Host-to-Site (client-to-gateway), or Host-to-Host (client-to-client).
Local Subnet	Enter the local subnet IP address behind the local endpoint
Peer Subnet	Enter the remote subnet IP address behind the remote endpoint
IKE Encryption Algorithm	Select from "3DES", "AES128", "AES192" and "AES256"
IKE Integrity Algorithm	Select from "MD5", " SHA1", "SHA2-256" and "SHA2-512"
Diffie-Hellman Group	DH group, select from Group 1 (768bits), Group 2 (1024bits), Group 5 (1536bits) and Group 14 (2048bits).
IKE Life Time	Lifetime of the IKE SA before re-keying
Enable NAT	Enable NAT traversal.
Authentication Type	Credential method, e.g., pre-shared key or public key (certificates).
Pre-shared Key	Shared secret string used for mutual authentication.
Local Identifier	Identity (IP, FQDN, or user@realm) sent to the peer.
Peer Identifier	Expected identity of the remote peer for verification.
ESP Encryption Algorithm	Select from "3DES", "AES128", "AES192" and "AES256"
ESP Integrity Algorithm	Select from "MD5", " SHA1", "SHA2-256" and "SHA2-512"

DPD Timeout	Maximum time to wait for a DPD response before declaring peer dead.
DPD Detection Period	Interval between consecutive DPD probe messages.
DPD Action	Action upon DPD failure (e.g., Restart, Clear, Hold or None).
Reboot Enable	Reboot device when Fails to Establish IPsec connection.

3.4.4 OpenVPN

OpenVPN is a versatile VPN solution that creates secure, encrypted tunnels over the internet, enabling both remote user access and site-to-site network connections. It uses strong SSL/TLS cryptography to protect data privacy and integrity, supports flexible authentication methods (including certificates and credentials), and runs on all major operating systems. Its ability to operate over both TCP and UDP helps it traverse firewalls and NAT, making it a reliable and widely adopted tool for secure private networking. Bivocom TG465 provides auto mode and manual mode for configuration file uploading.



OpenVPN (Auto Mode)	
Item	**Description**
File	Click to upload the Client configuration ovpn file which includes settings and certificates
Peer Subnet Address	Enter the peer route IP address.
Peer Subnet Mask	Enter the remote netmask protected by OpenVPN.
Enable NAT	Enable NAT traversal.
Enable LZO Compress	Select to enable or disable LZO to compress data
Cipher Algorithm	Select from Blowfish (128), NONE, DES (128), 3DES (192), AES (128), AES (192), AES (256)
MTU	The maximum transmission unit. Range: 128-1500.

OpenVPN

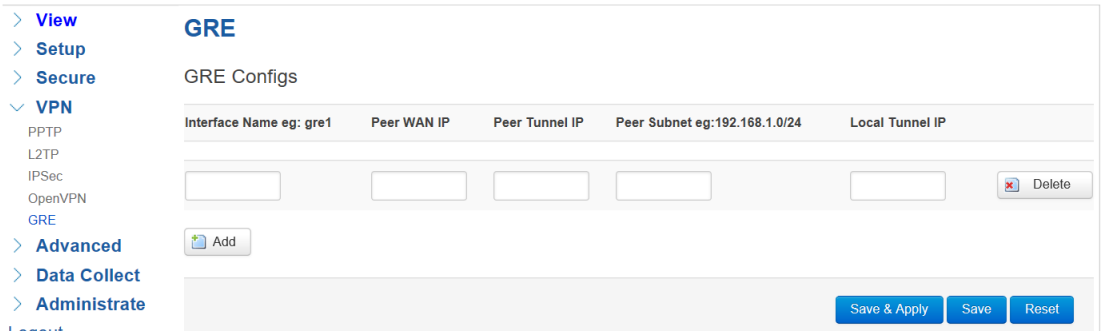
Set OpenVPN Parameters

OpenVPN	(•) Enable ( ) Disable
Mode	Manual
Topology	Subnet
Role	Client
Protocol	UDP
Port	1194
Device Type	TUN
OpenVPN Server	
Authentication Type	Certificate
CA	选择文件 未选择任何文件
Public Certificate	选择文件 未选择任何文件
Private Key	选择文件 未选择任何文件
DH	选择文件 未选择任何文件
TLS Authentication Key	选择文件 未选择任何文件
Peer Subnet Address	eg: 192.168.10.0
Peer Subnet Mask	eg: 255.255.255.0
Enable NAT	☐
Enable LZO Compress	Adaptive
Cipher Algorithm	Blowfish(128)
MTU	1500

OpenVPN (Manual Mode)	
Item	**Description**
Topology	Select the topology: 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.
Role	Select from server and client mode if in subnet topology.
Protocol	Select the protocol, UDP or TCP (default: UDP).
Port	Enter the port assigned to OpenVPN (default: 1194).
Device Type	Select the device type: TUN (layer 3 data encapsulation) or TAP (layer 2 data encapsulation).
OpenVPN Server	When you choose server in Role, you need to enter an IP address or domain name of server.
Authentication Type	If topology is subnet, authentication type is certificate. If it is point-to-point, you can choose none, certificate or static secret. Certificates need to be uploaded if chose Certificate as Authentication Type.
Peer Subnet Address	Enter the peer route IP address.
Peer Subnet Mask	Enter the remote netmask protected by OpenVPN.
Enable NAT	Enable NAT traversal.
Enable LZO Compress	Select to enable or disable LZO to compress data
Cipher Algorithm	Select from Blowfish (128), NONE, DES (128), 3DES (192), AES (128), AES (192), AES (256)
MTU	The maximum transmission unit. Range: 128-1500.

3.4.5 GRE

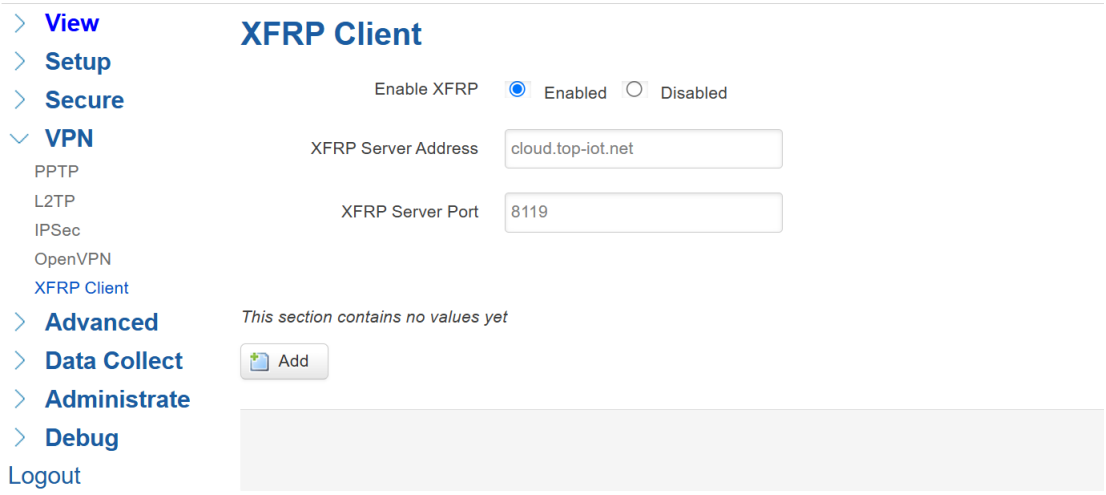
GRE (Generic Routing Encapsulation) is a tunneling protocol that encapsulates any network-layer protocol (e.g., IPv4, IPv6, multicast) over IP to create virtual point-to-point links. It enables multi-protocol transport across networks but lacks built-in encryption or authentication.



GRE	
Item	**Description**
Interface Name	Enter the name of GRE tunnel interface
Peer WAN IP	Enter the remote IP address running the GRE tunnel
Peer Tunnel IP	Set the local tunnel IP address of GRE tunnel
Peer Subnet	Enter the remote subnet IP address of GRE tunnel
Local Tunnel IP	Enter the local tunnel IP address of GRE

3.4.6 XFRP Client

XFRP Client page provides remote access via the Bivocom Device Platform (DMP), user can enable/disable or change the Server Address and Server Port to the private DMP.



3.4.7 VPN Common Issues:

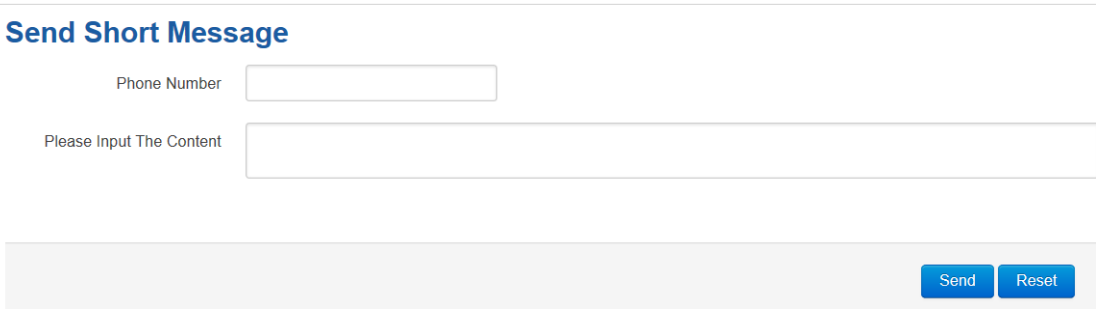
- **VPN Status** page is empty: Check the network status of device, confirm the VPN settings are correct, ensure VPN server can be reached.
- OpenVPN disconnected continually: Confirm the network stability of device, check **Keepalive**, **MTU, CA certificates** available, and ensure the **Cipher Algorithm, Device Type (TUN/TAP)** same as VPN server. Ensure the OpenVPN server version is not higher than **2.6.x** version, incompatibility issues will happen if version too high.

3.5 Advanced

The Advanced menu provides additional functions such as Send SMS, Static Routes, Net Flow, GPS location, SNMP, etc.

3.5.1 Send SMS

TG465 provides a window for sending text messages to certain numbers with configurable contents.



3.5.2 Static Routes

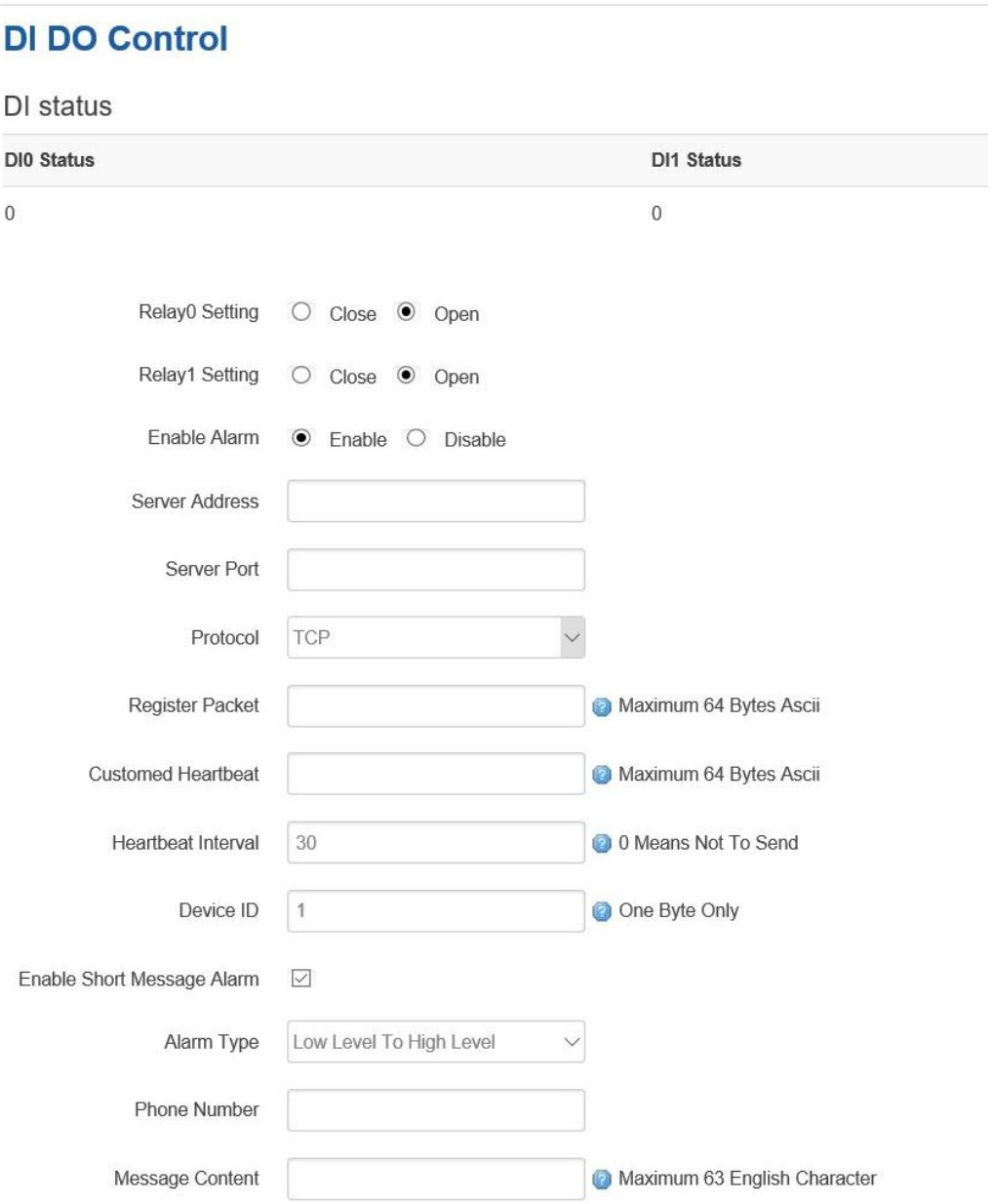
A static route is used to add a routing table entry.



Static Routes	
Item	**Description**
Interface	Select the interface that needs to be added to the routing table
Target	It 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 next-hop gateway address **Note**: This address shall be reachable, or you'll fail to add static routing.

3.5.3 DI DO

TG465 provides DI DO configuration page for setting up DI and Relay ports on TG465. It displays the real-time status of DI0 and DI1. Also supports manually changing the relay Close or Open. And support "Enable Alarm" to connect and report the status changes to a server. What's more, it supports SMS alarm to monitoring the DI status change.

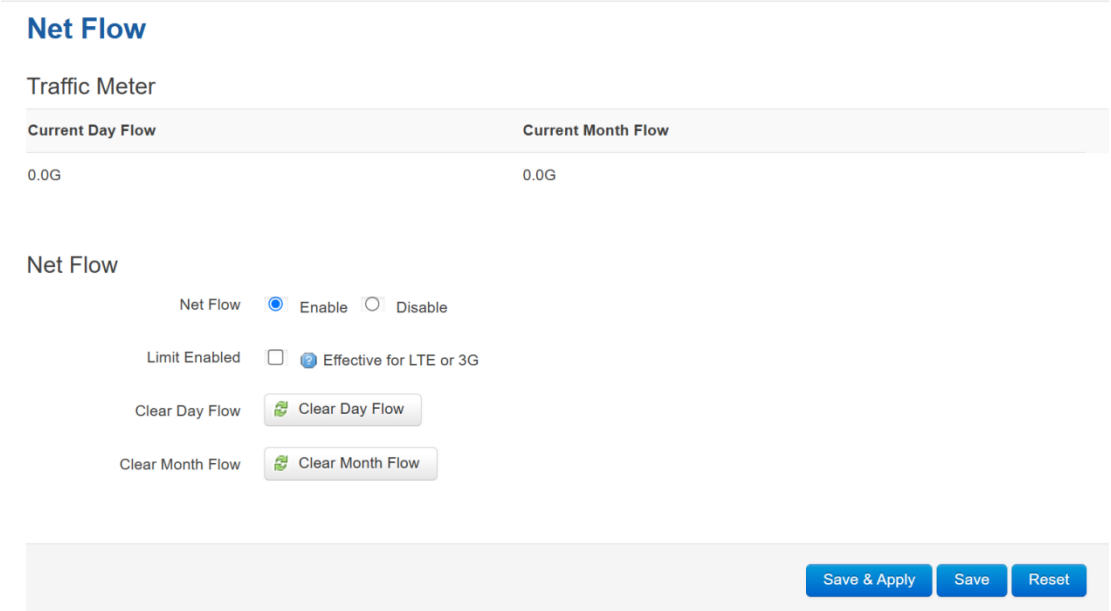


DI DO	
Item	**Description**
Server Address	Fill in the IP address or domain name
Server Port	Fill in TCP/UDP port, range is 1-65535.
Protocol	Select from TCP or UDP
Register Packet	Fill in the register packet string when connects to server

Custom Heartbeat	Heartbeat packet, maximum 64 bytes ASCII
Heartbeat Interval	Set the interval for client to send heart beat packet to server after gateway is connected to the server.
Device ID	Device ID of TG465
Enable Short Message Alarm	Enable SMS alarm
Alarm Type	Select from "Low Level to High Level" or "High Level to Low Level"
Phone Number	The phone number will receive SMS alarm
Message Content	Fill in SMS contents, maximum 63 English characters

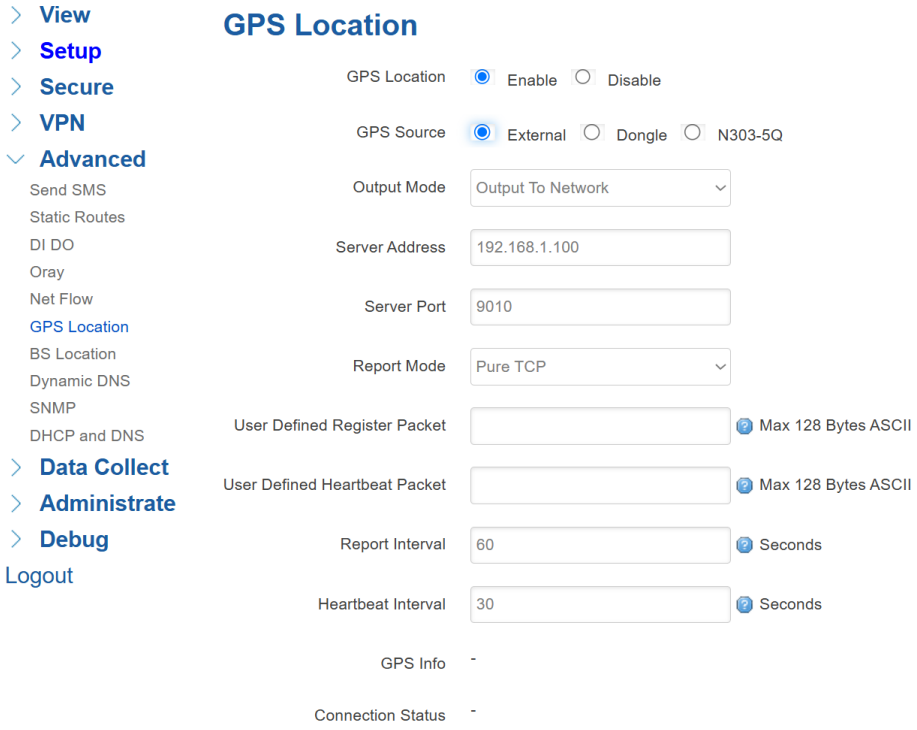
3.5.4 Net Flow

The traffic meter of the TG465 collects traffic statistics for the WAN port and provides a traffic overflow alarm. Traffic statistics are retained when the gateway is powered off, and counting resumes from the last recorded value the next time the gateway is powered on.



3.5.5 GPS Location (Optional)

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



GPS Location (Optional)	
Item	**Description**
GPS Source	External for getting GPS data from independent GPS module (Optional), while Dongle for getting GPS data from cellular module, N303-5Q is another independent GPS module (default option when select independent GPS).
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 Mode	Select from Pure TCP, Pure UDP, or with Protocol (original data)
User Defined Register Packet	Register packet when connects to server, max 128 Bytes ASCII

User Defined Heartbeat Packet	Heartbeat packet, maximum 128 bytes ASCII
Report Interval	The interval for auto reporting the gateway location, default value is 60 seconds.
Heartbeat Interval	Set the interval for client to send heart beat packet to server after gateway is connected to the server.
GPS Info	Display longitude and latitude data if GPS function works well
Connection Status	Show the current connection status with TCP/UDP server.

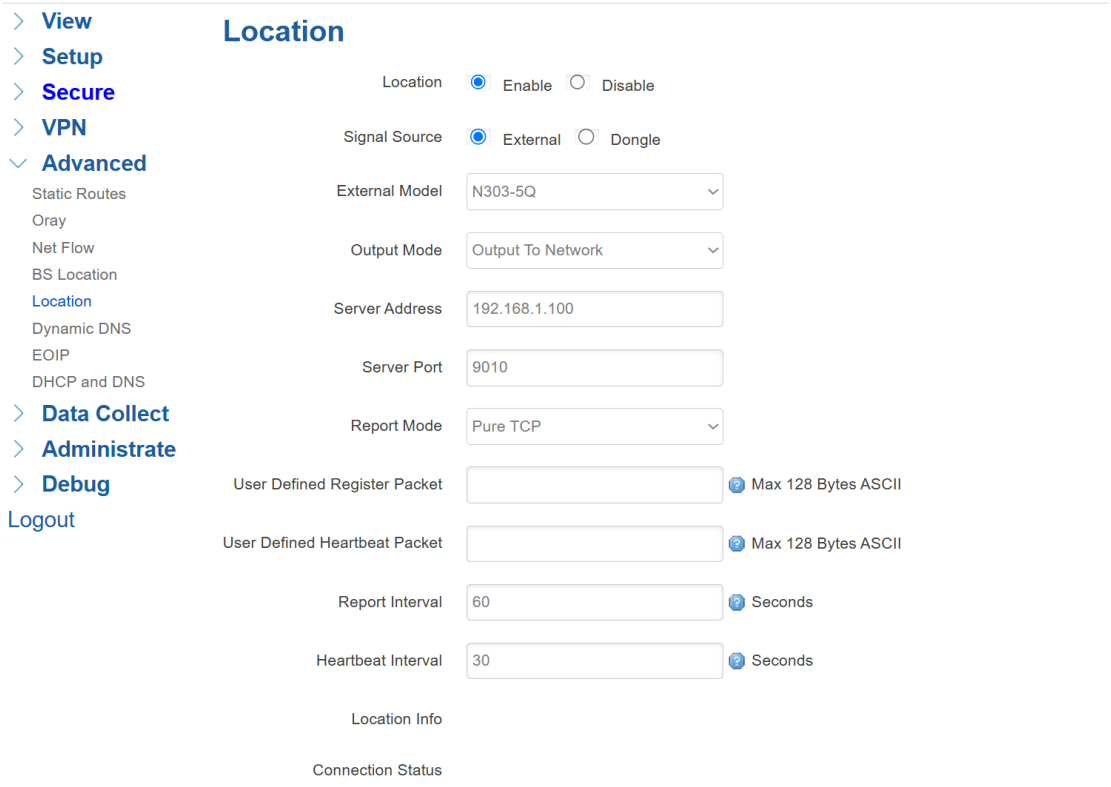
Scenario 3: Send GPS location to MQTT

Objective: Get current GPS location data and send to MQTT with other data.

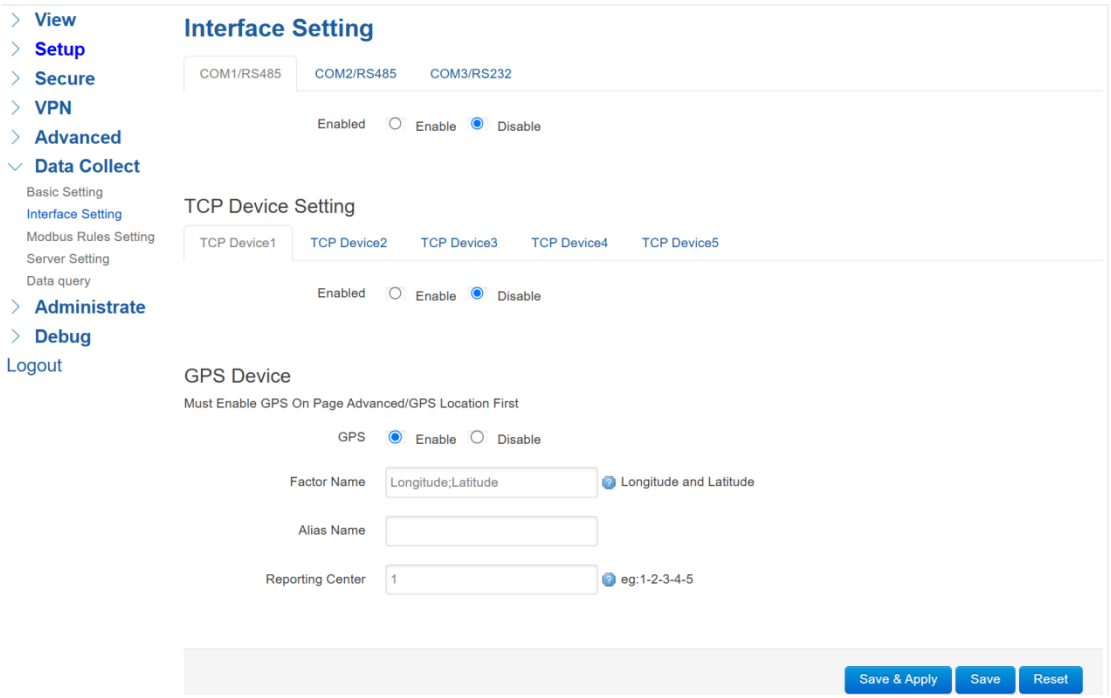
Prerequisites: GPS antenna was installed correctly, GPS Info displays current location, TG465 connected with MQTT broker, ensure device works in open area without shelter.

Configuration Steps:

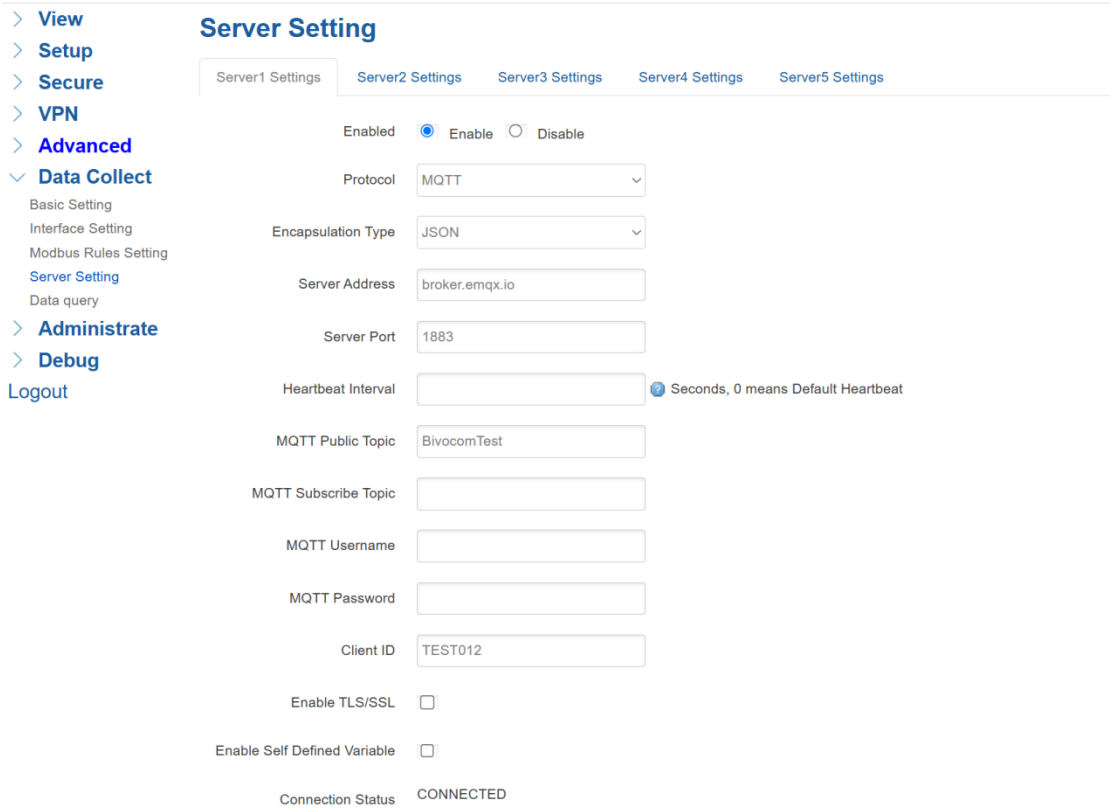
1. Go to **Advanced** > **Location** page to enable Location function, select GPS Source (depends on the hardware options, External is independent GPS module, Dongle is from cellular module GPS).



2. Ensure GPS/Location Info displays the longitude and latitude data.
3. Go to **Data Collect** > **Basic Setting** page to enable data collection.
4. Go to **Data Collect** > **Interface Setting** page to Enable GPS Device, enable **GPS Device**, fill "Longitude;Latitude" (separated by semicolon) into Factor Name, set the MQTT broker number which GPS data will report.



5. Go to **Data Collect** > **Server Setting** page to select the protocol of remote server, here we select MQTT, fill in **Server Address** (can be host IP address or domain name), set MQTT **Server Port** and **Public Topic** as it runs as remote server. **Client ID** should be unique, click **Save & Apply** after settings.

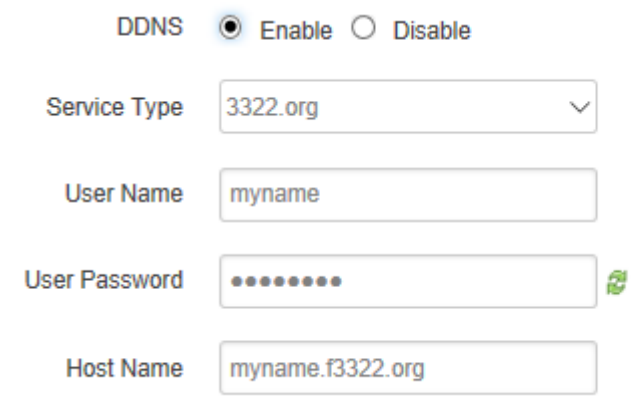


Common Issues:

No signal output to remote server: Check the installation of GPS antenna, make sure the GPS Info displays with location data. Ensure network connection works well, check if public topic sends from gateway and subscribe topic on other devices are the same.

3.5.6 Dynamic DNS

If the public IP address assigned to the gateway is dynamic and changes frequently, enable the DDNS function and register a domain name bound to that address. The domain then always resolves to the gateway, no matter how often the IP address changes.



- **Service Type**

The gateway supports several types of DDNS service, as listed below.



- **User Name**

The username you register at DDNS service provider.

- **User Password**

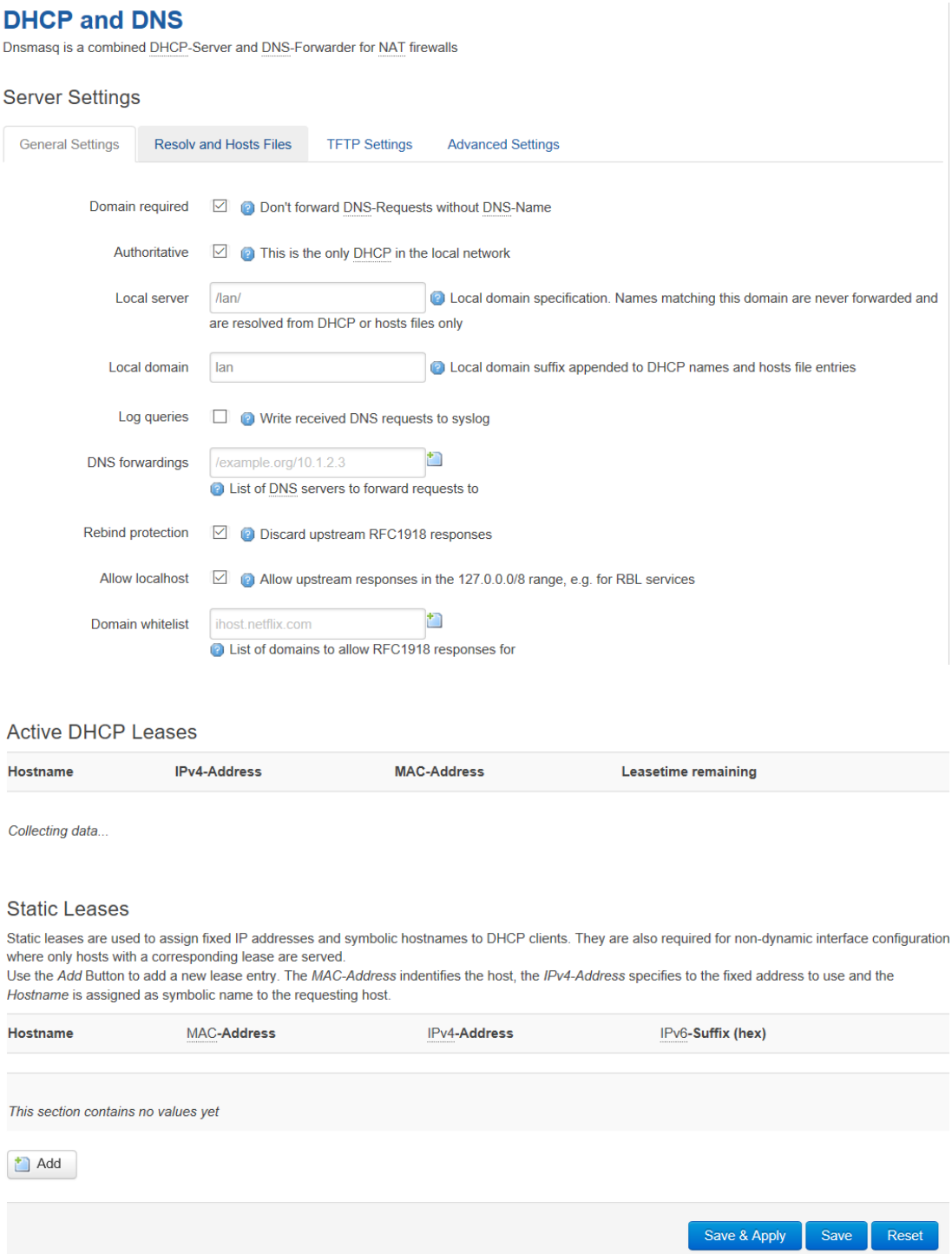
The password you set up when registering the username at DDNS service provider.

- **Host Name**

The registered domain name to bind to the IP address.

3.5.7 DHCP and DNS

The TG465 provides DHCP and DNS settings through the Dnsmasq package. The DHCP server and DNS forwarding settings can be configured if your network requires specific parameters, and static leases are also supported. In most cases, leave these settings at their default values.

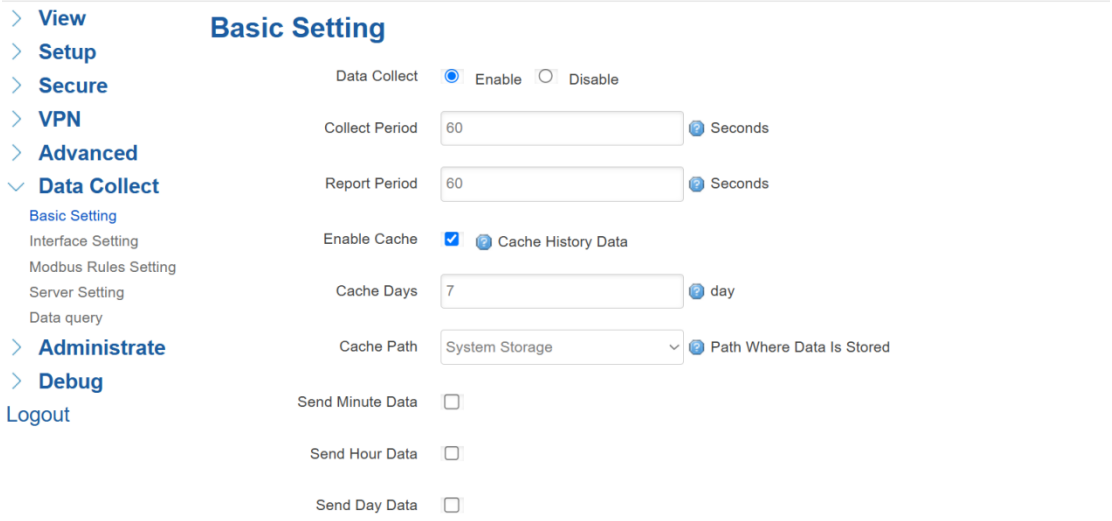


3.6 Data Collect

Data Collect settings are for TG465 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 acquisition and reporting period and other related options.

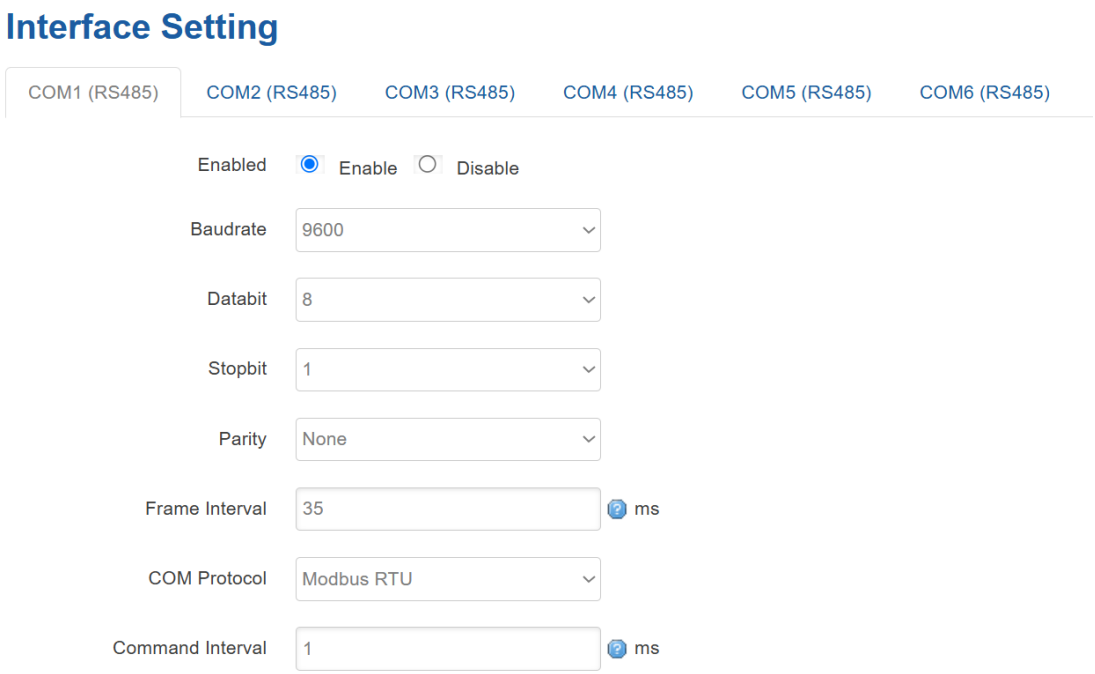


Data Collect — Basic Setting	
Item	**Description**
Collect Period	Set the period of data reporting from slave devices. Range: 1-9999 (S)
Report Period	Set the period of data reporting from slave devices. Range: 1-9999 (S)
Enable Cache	Enable or disable the historical data when network is disconnected, cached data will be re-transmitted after network recovery.
Cache Days	Set the days of historical cache data.
Cache Path	Select from System Storage or SD card/USB device (some models support)
Send Minute/Hour/Day Data	Custom cache data package, only enabled with specific firmware

3.6.2 Interface Setting

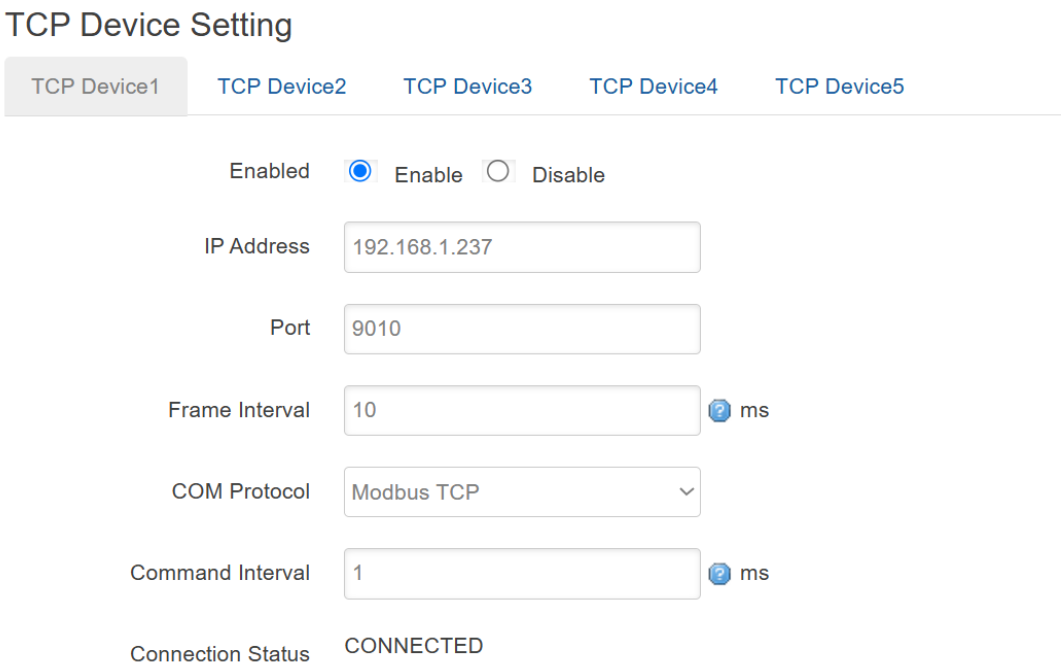
Switch the hardware interfaces for data acquisition from kinds of slave devices. Including Serial ports (COM1~COM6), Modbus TCP base on Ethernet LAN, GPS Device.

Serial Ports Setting



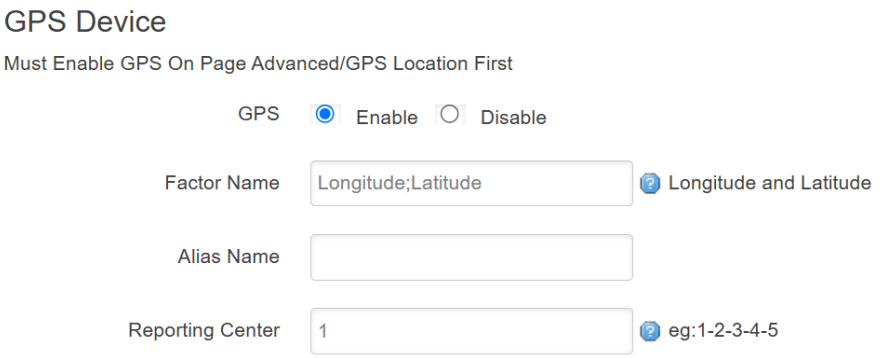
Data Collect — Serial Ports Setting	
Item	**Description**
Baud Rate	Select from "1200~230400"
Data Bits	Select from "7" and "8"
Stop Bits	Select from "1" and "2"
Parity	Select from "None", "Odd" and "Even"
Frame Interval	Set the configurable silent gap between serial frames that delimits frame boundaries.
COM Protocol	Select from "Modbus RTU" and "Transparent"(Unprocessed)
Command Interval	Idle delay after a response before the next request, allowing slave recovery and bus settling.

TCP Server (Modbus TCP Slave) Setting



TCP Server (Modbus TCP Slave) Setting	
Item	**Description**
IP Address	Fill in with Host IP address
Port	Fill in the port runs TCP server/Modbus TCP
Frame Interval	Set the configurable silent gap between serial frames that delimits frame boundaries.
COM Protocol	Select from "Modbus RTU" and "Transparent"(Unprocessed)
Command Interval	Idle delay after a response before the next request, allowing slave recovery and bus settling.
Connection Status	Show the TCP connection status

GPS Device

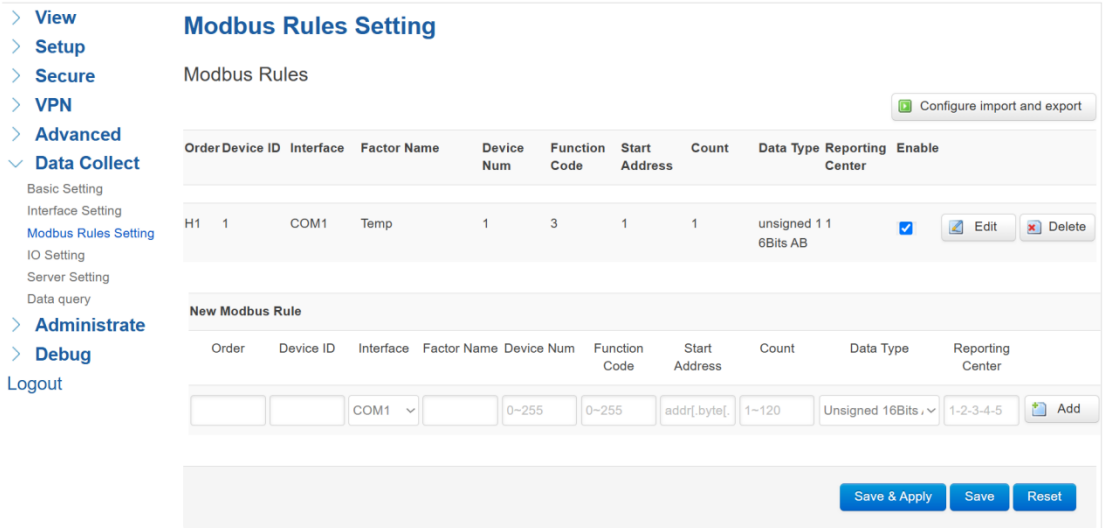


GPS Device Setting	
Item	**Description**
Factor Name	Fill in the factor name of longitude and latitude data
Alias Name	The name will be display on **Data Collect**—**Data Query** page
Reporting Center	Fill in from "1~5", different servers need to be separated by "-"

3.6.3 Modbus Rules Setting

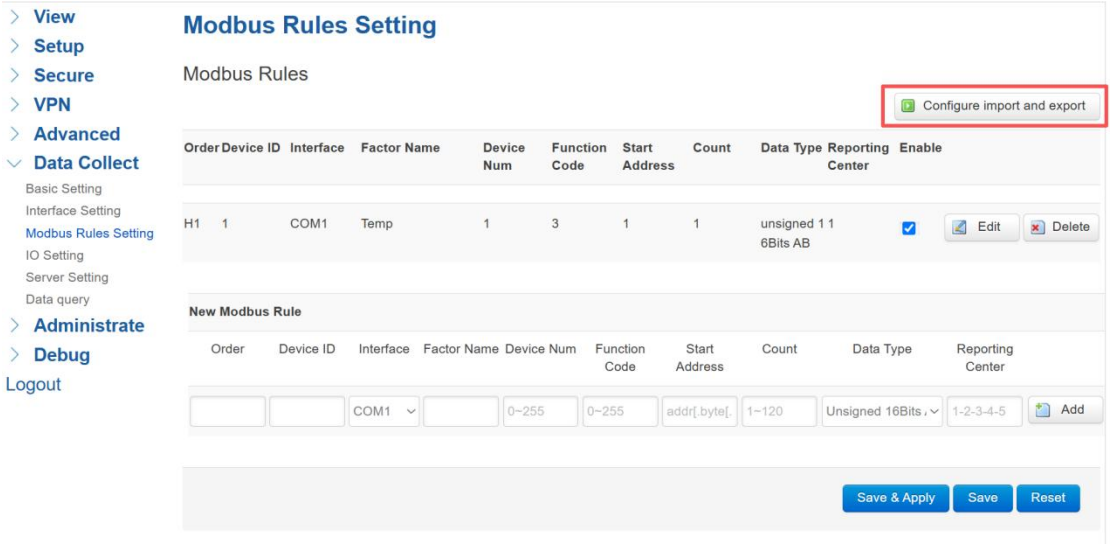
Modbus Rules Setting configures the TG465 as a Modbus master that collects data from slave devices over the Modbus protocol. The number of Modbus rules you can configure is unlimited. The factor name, device ID, function code, register address and register count are all user-definable; refer to the slave device datasheet for the correct values.

General Settings



Modbus Rules Setting (General Settings)	
Item	**Description**
Order	Fill in the rule number of Modbus rule
Device ID	Fill in the device ID of slave device
Interface	Select which interface connects to the Modbus slave device
Factor Name	Factor name will be the data name when sending to server, different data should be separated by semicolon (;)
Device Num	Same as the Modbus slave ID/address
Function Code	Fill in function code (**01, 03, 04**) according to the datasheet of Modbus slave device
Start Address	The start address of the Modbus data address that need to be collected
Count	The number of registers to be read, same as the read count
Data Type	Select from **Unsigned 16Bits AB, Unsigned 16Bits BA, Signed 16Bits AB, Signed 16Bits BA, Unsigned 32Bits ABCD, Unsigned 32Bits BADC, Unsigned 32Bits CDAB, Unsigned 32Bits DCBA, Signed 32Bits ABCD, Signed 32Bits BADC, Signed 32Bits CDAB, Signed 32Bits DCBA, Float ABCD, Float BADC, Float CDAB, Float DCBA, Bit, Byte AB, Byte BA, BCD 16Bits AB, BCD 16Bits BA, BCD 32Bits ABCD, BCD 32Bits BADC, BCD 32Bits CDAB, BCD 32Bits DCBA, String, Signed 64Bits ABCDEFGH, Signed 64Bits GHEFCDAB, Signed 64Bits BADCFEHG, Signed 64Bits HGFEDCBA, Double ABCDEFGH, Double GHEFCDAB, Double BADCFEHG** and **Double HGFEDCBA**
Reporting Center	Enter the server number that needs to receive data
Edit	Click to enter Detailed Settings
Delete	Click to delete current rule

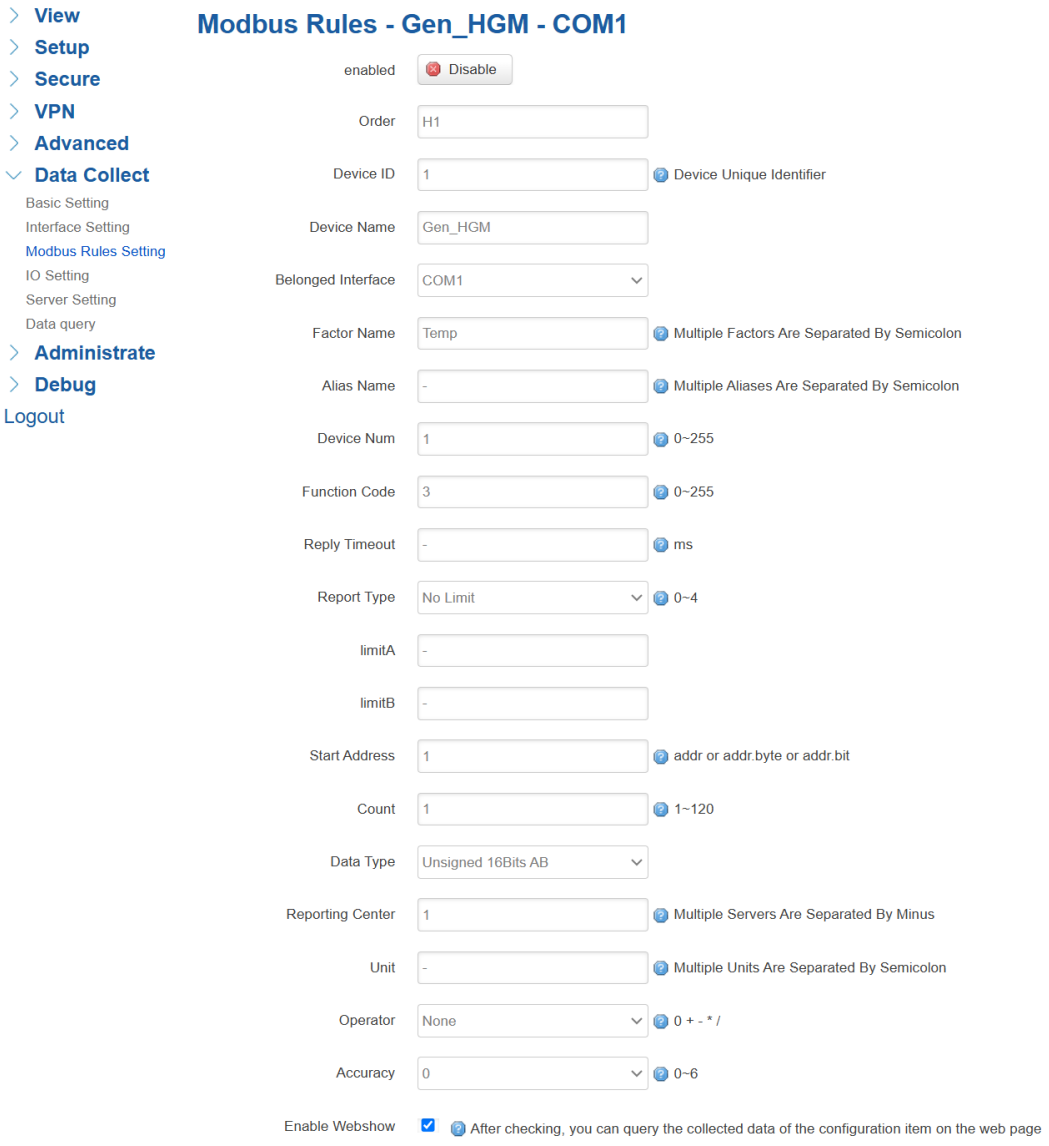
Configure import and export





Modbus configuration import / export	
Item	**Description**
Export modbus configuration	Click **Export configuration** to create current Modbus rules
Import modbus configuration	Click Choose File to upload the csv of Modbus rules, gateway will load all of the configurations and apply the Modbus settings after restarting the data-collection process.

Modbus Rule Setting (click Edit to enter detailed settings)



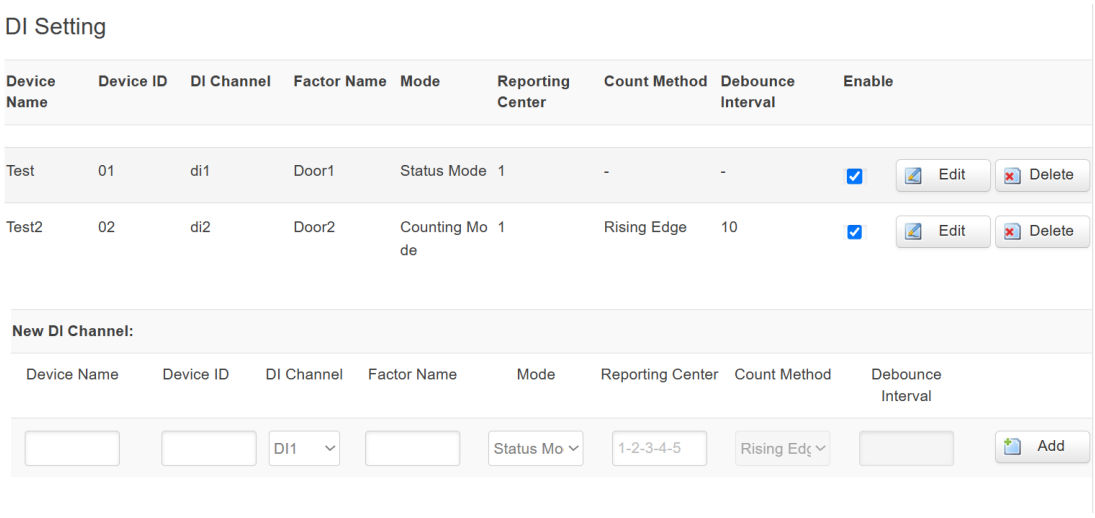
Modbus Rules Setting (Detailed Settings, Remove duplicates)	
Item	**Description**
Device Name	Fill in name of slave device for identification
Alias Name	Fill in the data name which displays on **Data query**
Reply Timeout	Set the maximum duration a master (gateway) waits for a slave's (slave sensors/devices) response; if exceeded, the transaction is considered failed.
Report Type	Set the report type of current Modbus rule, select from **No Limit** (default, always report), **Report Variable Value** (when data value changes), **Less Equal Than A (≤ A)**, **Greater Equal**

	Than B (≥ B), Between Limit A and B
limitA/B	Set data value limitation for **Report Type**
Unit	Fill in the unit for data value (V, A, W, etc.)
Operator	Operators used to perform calculations on data value. Common examples include: **+** (addition), **-** (subtraction), ***** (multiplication), **/** (division) and **Expression**.
Operation Expression	A complex arithmetic expression involves multiple operators, e.g. **(x + 10) * 10**, **x** is collected data
Accuracy	Accurate to N decimal places, select from **0-6**.
Enable Webshow	Show current Modbus rule's data on **Data query** page.

3.6.4 IO Setting

Since the TG465 provides 4 DI and 4 relay ports, it is possible to detect their status and report to server via JSON format, which take "Factor Name" as individual parameter.

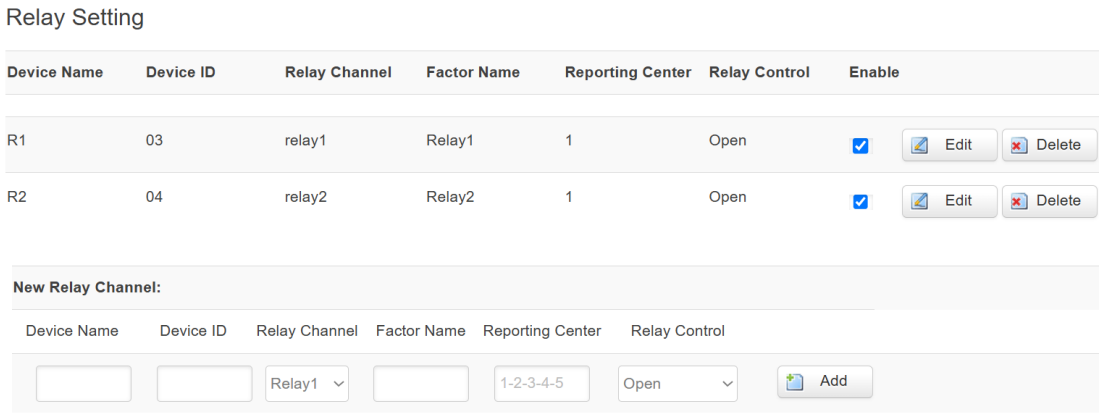
DI Setting



IO Setting (DI)	
Item	**Description**

Device Name	Fill in name of slave device for identification
Device ID	Fill in the unique ID of current device
DI Channel	Select from **DI1 ~ DI4**
Factor Name	Set the **Factor Name** of current DI channel when reporting to server
Mode	Select from **Status Mode** and **Counting Mode**
Reporting Center	Select from 1–5 server numbers, multiple servers need to be separated by "-", e.g. "1-2-3"
Count Method	Select from **Rising Edge** (0 to 1) and **Falling Edge** (1 to 0)
Debounce Interval	The configured time window during which subsequent DI (**Counting Mode**) transitions are ignored, ensuring that no additional DI count is triggered within that period. **Default value**: 10ms

Relay Setting



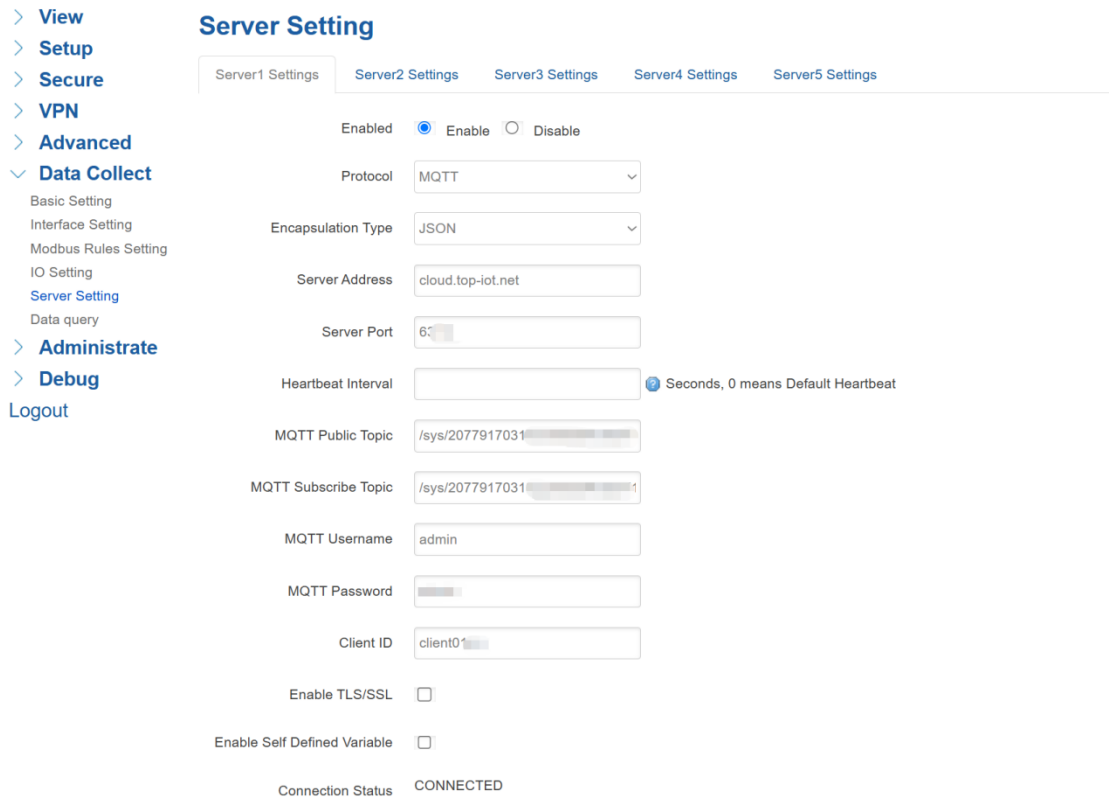
IO Setting (Relay)	
Item	**Description**
Device Name	Fill in name of slave device for identification

Device ID	Fill in the unique ID of current device
Relay Channel	Select from **Relay1 ~ Relay4**
Factor Name	Set the **Factor Name** of current DI channel when reporting to server
Reporting Center	Select from 1–5 server numbers, multiple servers need to be separated by "-", e.g. "1-2-3"
Relay Control	Select from **Open** and **Close** for the initial status of relay

3.6.5 Server Setting

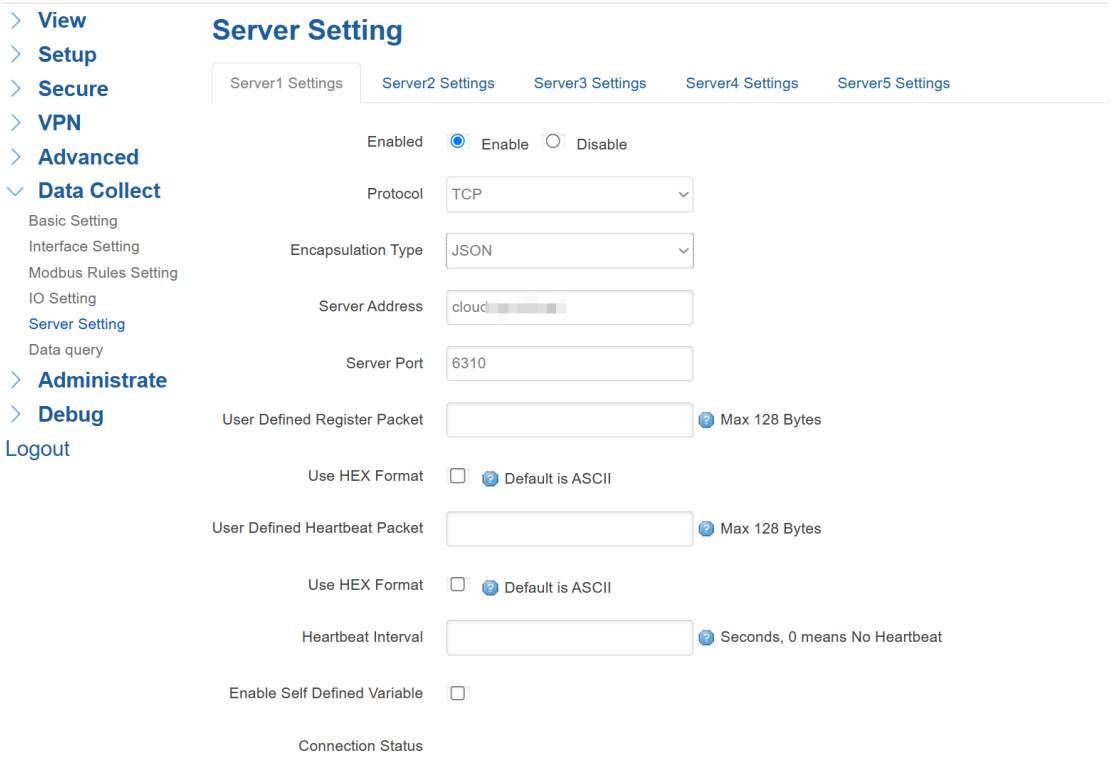
The Server settings menu allows users to set the data-center address with multiple protocols, the standard TG465 support TCP, UDP, HTTP (s), MQTT (s), TCP Server and Modbus TCP (slave). For the data format, TG465 support different Encapsulation type, include "Transparent", "Json", and "HJ212" (special for some Environment SCADA).

MQTT Broker (Server)



MQTT Broker (Server)	
Item	**Description**
Encapsulation Type	Select from JSON, Transparent, JSON_IoT (Specific for Bivocom IoT Platform) and HJ212 (Specific for some SCADA)
Server Address	Fill in the Host IP address or domain name of MQTT broker
Server Port	Set the MQTT broker port to receive data
Heartbeat Interval	Set the interval for client to send heart beat packet to server after gateway is connected to the server.
MQTT Public Topic	Set the topic name of data publishing
MQTT Subscribe Topic	Set the topic name of data receiving
MQTT Username/Password	The Username/Password for connecting to the MQTT broker
Client ID	The unique ID for connecting to the MQTT broker
Enable TLS/SSL	Enable TLS encryption for MQTT connection. Select from **CA signed server certificate** (verify with the certificate issued by Certificate Authority (CA) that pre-loaded on the device.), **One-way certificate** (upload the specific CA certificate) and **Two-way certificate** (upload the custom CA certificates, client certificates, and secret key, like.cer,.crt, or.pem) for verification.
Enable Self Defined Variable	Click to fill in specific device name and value for verification
Connection Status	Show the current connection status with MQTT broker.

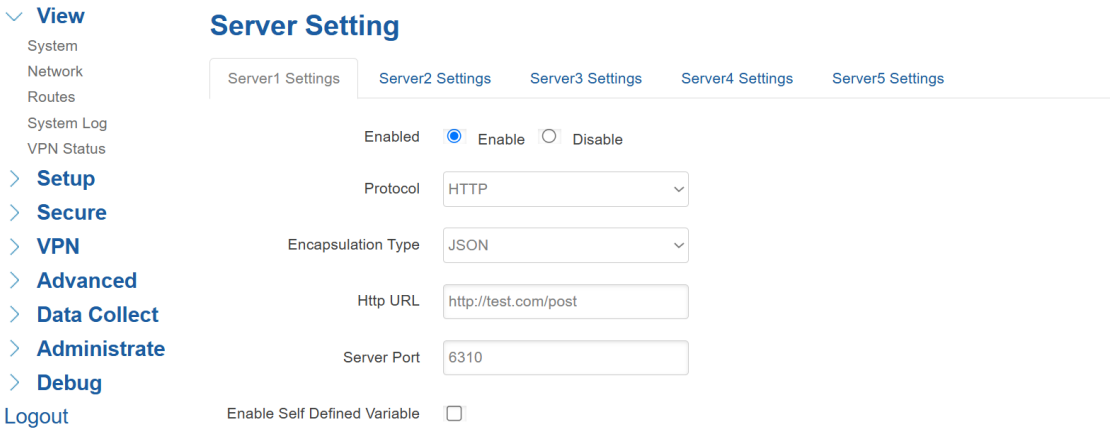
TCP/UDP Server



TCP/UDP Server	
Item	**Description**
Encapsulation Type	Select from JSON, Transparent, JSON_IoT (Specific for Bivocom IoT Platform) and HJ212 (Specific for some SCADA)
Server Address	Fill in the Host IP address or domain name of TCP/UDP server
Server Port	Set the TCP/UDP port to receive data
User Defined Register Packet	Fill in the register packet string when connects to server
User Defined Heartbeat Packet	Heartbeat packet, maximum 128 bytes ASCII
Heartbeat Interval	Set the interval for client to send heart beat packet to server after gateway is connected to the server.
Enable Self Defined Variable	Click to fill in specific device name and value for verification

Connection Status	Show the current connection status with TCP/UDP server

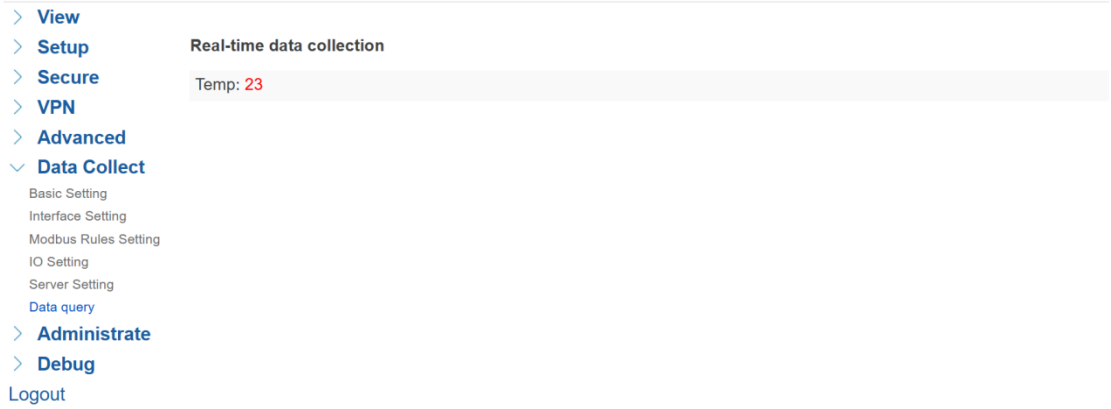
HTTP (S) Server



HTTP (S) Server	
Item	**Description**
Encapsulation Type	Select from JSON, Transparent, JSON_IoT (Specific for Bivocom IoT Platform) and HJ212 (Specific for some SCADA)
HTTP (S) URL	Fill in the **HTTP URL** of posting data, it can be HTTPS URL but without username/password authentication
Server Port	Set the HTTP (S) port to receive POST data
User Defined Register Packet	Fill in the register packet string when connects to server
User Defined Heartbeat Packet	Heartbeat packet, maximum 128 bytes ASCII
Enable Self Defined Variable	Click to fill in specific device name and value for verification

3.6.6 Data Query

Data Query page allows user to check the value of current data collecting, the data value of failed in reading will show as "-".



3.6.7 Common Application

Scenario 4: Ubuntu Secondary Development (Ubuntu OS)

Objective: Extend the TG465 gateway with your own applications by using the Ubuntu operating system and the standard Linux device interfaces that the gateway hardware exposes. This scenario describes the hardware resources that are available to developers, the device files that represent the serial, digital I/O and power-output interfaces, and the steps to log in to the device, install the GCC toolchain and compile a C program that reads the on-board DI status.

Prerequisites: A TG465 running the Ubuntu system image; a PC connected to the gateway through the LAN port, or an RS232 debug cable; and a terminal emulator such as PuTTY, or the built-in SSH and telnet clients of your operating system.

Device Role: The gateway acts as a general-purpose Ubuntu host. Its hardware interfaces are exposed to the operating system as ordinary Linux device files, so an application running on the gateway can read and control them with the standard open, read, write, close and ioctl calls, without any proprietary SDK.

Hardware Resources

The tables below list the hardware resources that are available to applications running on the gateway.

Hardware System	
Item	**Description**
CPU	Quad-core ARM Cortex-A55 running at 2.0 GHz
VPU	4K@60 fps H.265/H.264/VP9 video decoding, 1080p@60 fps H.265/H.264 video encoding, 8 MP ISP with HDR support

GPU	ARM G52 2EE
NPU	1 TOPS
DDR4	2 GB, expandable to 8 GB
eMMC	32 GB, expandable to 128 GB

Network Communication	
Item	**Description**
Ethernet Port	1 x WAN and 3 x LAN, 10/100/1000 Mbps RJ45, self-adaptive MDI/MDI-X, with 1.5 kV magnetic isolation protection
Wi-Fi 6	2T2R 802.11 a/b/g/n/ac/ax, with support for WEP, WPA and WPA2 and multiple encryption modes
Cellular (4G/5G, optional)	All-Netcom (full network support)

Interfaces	
Item	**Description**
RS232	1 x RS232, multiplexed with RS485_1, with 8 kV ESD protection
RS485	6 x RS485, with 15 kV ESD protection
DO (Relay)	4 digital outputs. Maximum switching voltage 30 VDC / 250 VAC; maximum switching current 5 A.
DI	4 optically isolated digital inputs. Logic 1: wet contact 5-30 VDC, or dry contact open. Logic 0: wet contact 0-3 VDC, or dry contact closed.
Power Output (VCC)	2 power outputs, 5-60 VDC, controlled through the device power input
HDMI	1 HDMI input, supporting displays up to 4K

USB	1 x USB 3.0 port and 1 x USB 2.0 port
TF Card	1 x TF card interface, used to store data
M.2	Internal M.2 interface supporting NVMe solid-state drives, expandable to 2 TB (optional)
SIM/UIM	Standard 1.8 V/3 V SIM/UIM interface, with 15 kV ESD protection
Antenna	Standard SMA female connector, 50 ohms
Indicator	RUN, SYSTEM, ONLINE, Wi-Fi and ALARM

Interface Device Instructions

The TG465 supports secondary development of the serial ports, the digital outputs (relay), the digital inputs and the power outputs. Under Ubuntu these interfaces are presented as device files, so they are operated with standard Linux file operations. The sections below list the device file that corresponds to each interface and give the commands used to read or change its state.

RS485 / RS232

The TG465 provides six RS485 ports, one of which is multiplexed with RS232. Each port has its own device file:

Serial Port Device Files	
Item	**Description**
RS485_1 / RS232	/dev/ttyS0
RS485_2	/dev/ttyS3
RS485_3	/dev/ttyS4
RS485_4	/dev/ttyS7
RS485_5	/dev/ttyS8
RS485_6	/dev/ttyS9

DI / DO (Relay)

The TG465 provides four digital outputs and four digital inputs. Each one corresponds to a device file:

DI and DO Device Files	
Item	**Description**
DO1 (Relay 1)	/sys/class/gpio/relay1
DO2 (Relay 2)	/sys/class/gpio/relay2
DO3 (Relay 3)	/sys/class/gpio/relay3
DO4 (Relay 4)	/sys/class/gpio/relay4
DI1	/sys/class/gpio/di1
DI2	/sys/class/gpio/di2
DI3	/sys/class/gpio/di3
DI4	/sys/class/gpio/di4

The four relays are normally open by default. To close a relay, write 1 to the value file of the corresponding device. The command below closes relay 1:

```
echo 1 > /sys/class/gpio/relay1/value
```

To read the state of DI 1, run:

```
cat /sys/class/gpio/di1/value
```

A returned value of 1 means that DI 1 is connected to GND. A returned value of 0 means that it is floating.

Power Output (VCC)

The TG465 provides two power outputs in the 5-60 VDC range. Each one corresponds to a device file:

Power Output Device Files	
Item	**Description**
Power Output 1 (VCC1)	/sys/class/gpio/pwr_vcc1

Power Output 2 (VCC2)	/sys/class/gpio/pwr_vcc2

To read the current state of power output 1, run:

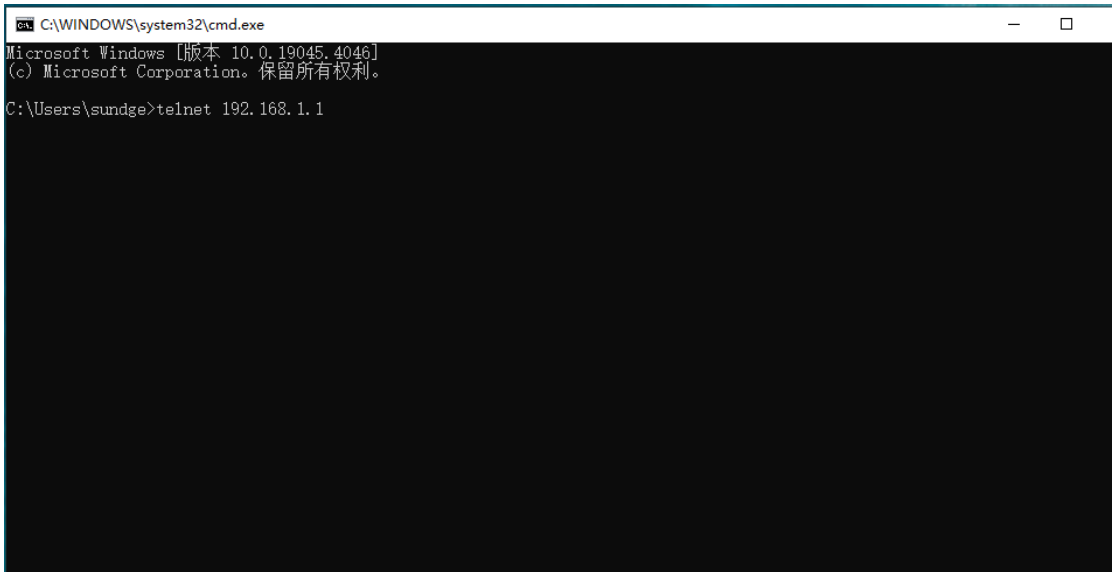
```
cat /sys/class/gpio/pwr_vcc1/value
```

A returned value of 1 indicates that VCC1 is at a high level (active) and that the power output is working normally.

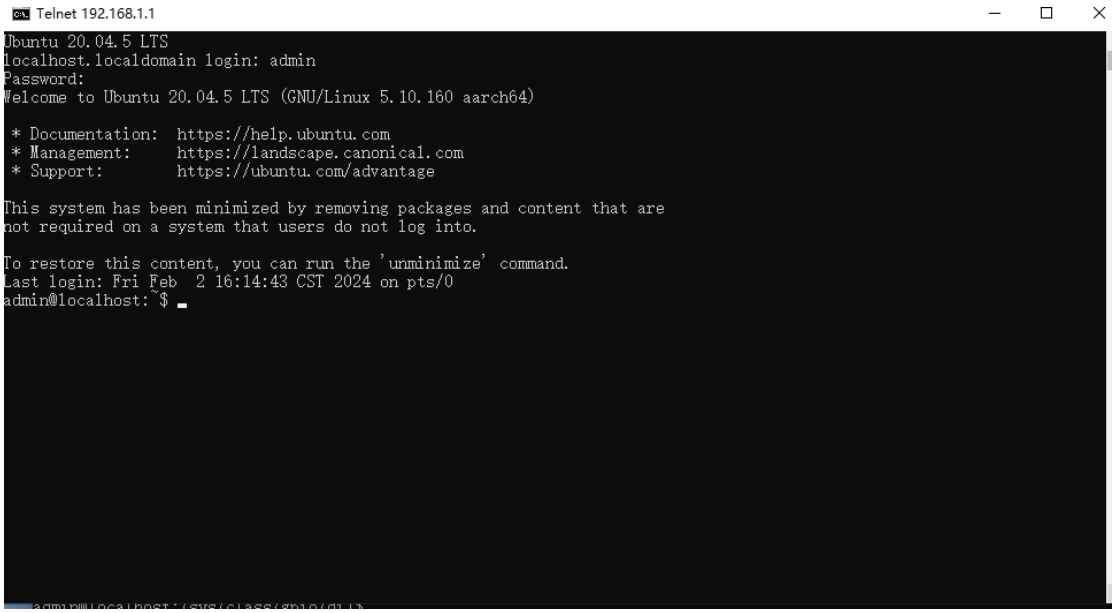
- **Ubuntu Secondary Development Demo**

Log In to the Device

1. Log in to the TG465 over telnet or SSH, or through the debug port. Use the RS232 port if you have a serial debug cable, or telnet or SSH over the Ethernet port.
2. Connect the LAN port of the gateway to your PC with an RJ45 cable, then log in. The default IP address of the gateway is 192.168.1.1, and the default username and password are root/heyroot.
3. Enter sudo -s to switch to the superuser (root) account. The default root password is heyroot.

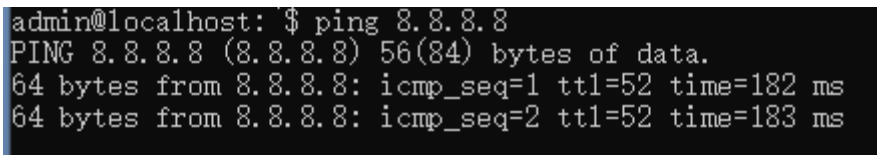






Connect the Device to the Network

The TG465 can reach the Internet either through the Ethernet WAN port or through a cellular (4G/5G) connection. Connect the WAN port to a device that has Internet access, or insert a SIM card, connect the cellular antenna and let the gateway register on the network. Once the link is up, run ping 8.8.8.8 to confirm that the gateway has Internet access.



Install the GCC Toolchain

The Ubuntu system image does not include the GCC toolchain by default. Install it with the

following commands:

```
sudo apt update

sudo apt install gcc

sudo apt install make
```

Once GCC is installed, applications can be developed in C. Python is also supported, because a Python interpreter is included in the device image by default.

The example below is a complete secondary-development program. It takes the name of a GPIO device as its parameter, opens the corresponding Linux device file and prints the current value of that input.

```
#include <stdio.h>

#include <fcntl.h>

#include <stdlib.h>

#include <unistd.h>

#include <string.h>


void main(int argc, char *argv[])

{

 int fd;

 int ret;

 char path[128];

 char buff[32] = {'\0'};


 if (argc < 2) {

        printf("not enough parameter, should great 2 \n");

 return;

 }

    snprintf(path, sizeof(path), "/sys/class/gpio/%s/value", argv[1]);

 fd = open(path, O_RDONLY);

 if (fd < 0) {

        printf("Fails to open %s\n", path);

 return;
```

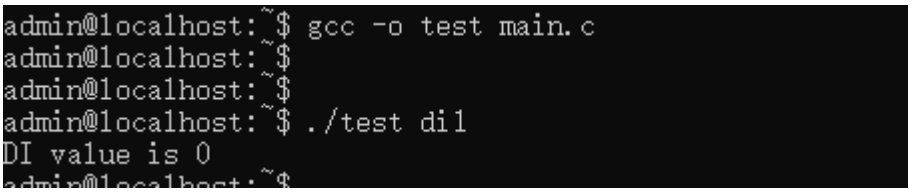
```
    }
        ret = read(fd, buff, sizeof(buff));
    if (ret <= 0) {
            printf("Fails to read\n");
    close(fd);
    return;
    }
    ret = atoi(buff);
        printf("DI value is %d\n", ret);
    close(fd);
}
```

Save the code as main.c, then compile it with:

```
gcc -o test main.c
```

This produces an executable file named test. Pass the name of the input you want to read as the first parameter, for example:

```
./test di1
```



Verification Method:

1. Run ping 8.8.8.8 from the Ubuntu shell and confirm that replies are received, which proves that the gateway has Internet access.
2. Run gcc --version and confirm that the toolchain reports its version.
3. Compile the sample program and run ./test di1. The program prints DI value is 1 or DI value is 0, matching the current state of the corresponding input.

Common Issues:

1. Cannot log in over telnet or SSH: confirm that the PC is on the same subnet as the gateway (the default address is 192.168.1.1) and that the credentials are correct (admin / admin). If no Ethernet link is available, log in through the RS232 debug port instead.
2. Permission denied when writing to a device file: switch to the root account with sudo -s and enter the root password.
3. Package installation fails: confirm that the gateway has Internet access, as described in Connect the Device to the Network, and run sudo apt update again.

4. The compiled program reports "Fails to open /sys/class/gpio/...": check that the device name passed on the command line matches one of the device files listed above, for example ./test di1, and run the program with root privileges.

Scenario 5: Install and Run Docker Containers (Ubuntu OS)

Objective: Install Docker on the TG465 gateway and run containers on it, so that applications such as MQTT brokers, data processors or custom analytics modules can be deployed to the edge as isolated, lightweight units.

Prerequisites: A TG465 running the Ubuntu system image; Internet access from the gateway; and a PC that can reach the gateway over SSH or telnet.

NOTE: The TG465 is available with two operating systems, OpenWRT and Ubuntu. Docker requires the Ubuntu system, so select Ubuntu when you order the device, and tell your Bivocom sales representative which system you need. An existing device can also be upgraded from OpenWRT to Ubuntu. Contact our technical support team for assistance.



Device Role: The gateway acts as a Docker host. Containers run in isolated user spaces on top of the gateway Ubuntu system and share its Linux kernel, while remaining independent of each other.

What Is Docker?

Docker is an open platform for developing, shipping and running applications in containers. It separates applications from the underlying infrastructure, which allows software to be delivered more quickly and lets you manage your infrastructure in the same way that you manage your applications. By adopting the Docker approach to building, testing and deploying code, you can significantly shorten the time between writing code and running it in production.



Docker requires a Linux kernel and relies on Linux-specific features such as cgroups and namespaces. The Bivocom intelligent gateway TG465 supports the Ubuntu operating system, so Docker can be installed on the gateway and used to run containers that deploy a wide range of applications.

Combining Docker with the TG465 creates a flexible and efficient edge-computing environment. By containerizing applications such as MQTT brokers, data processors or custom analytics modules, you can deploy, manage and update services as isolated, lightweight units. This approach keeps behaviour consistent across different environments, makes better use of the limited resources of edge hardware, and greatly simplifies maintenance, so the gateway can run several workloads securely at the same time and adapt quickly to new requirements.

For more information, refer to the official Docker documentation.

System Requirements

The table below lists the system requirements of Docker and shows how the TG465 meets them.

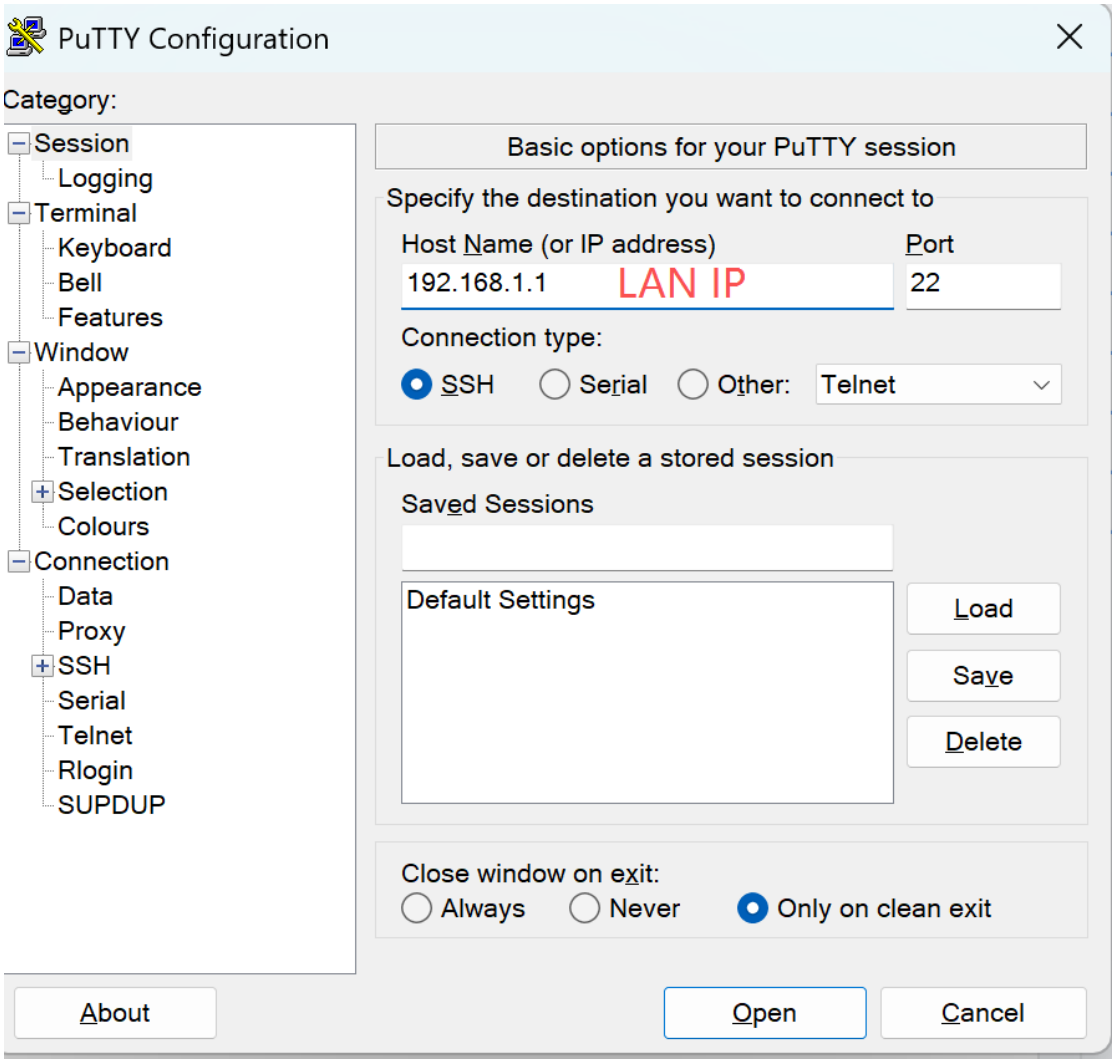
Docker System Requirements	
Item	**Description**
CPU	Linux 64-bit, x86_64 or ARM64 architecture. The TG465 is powered by a 64-bit ARM Cortex-A55 processor.
Linux Kernel	Minimum kernel 3.10; kernel 4.x or 5.x recommended. The TG465 runs Linux kernel 5.10.
Operating System	A Debian-based distribution: Debian 10+, Ubuntu 20.04+,

	CentOS 7+, Fedora 33+ or RHEL 7+. The TG465 runs Ubuntu 20.04.
RAM / Flash	2 GB of RAM and 2 GB of flash recommended. The TG465 provides 2 GB of DDR4 RAM (8 GB optional) and 32 GB of eMMC flash (128 GB optional).

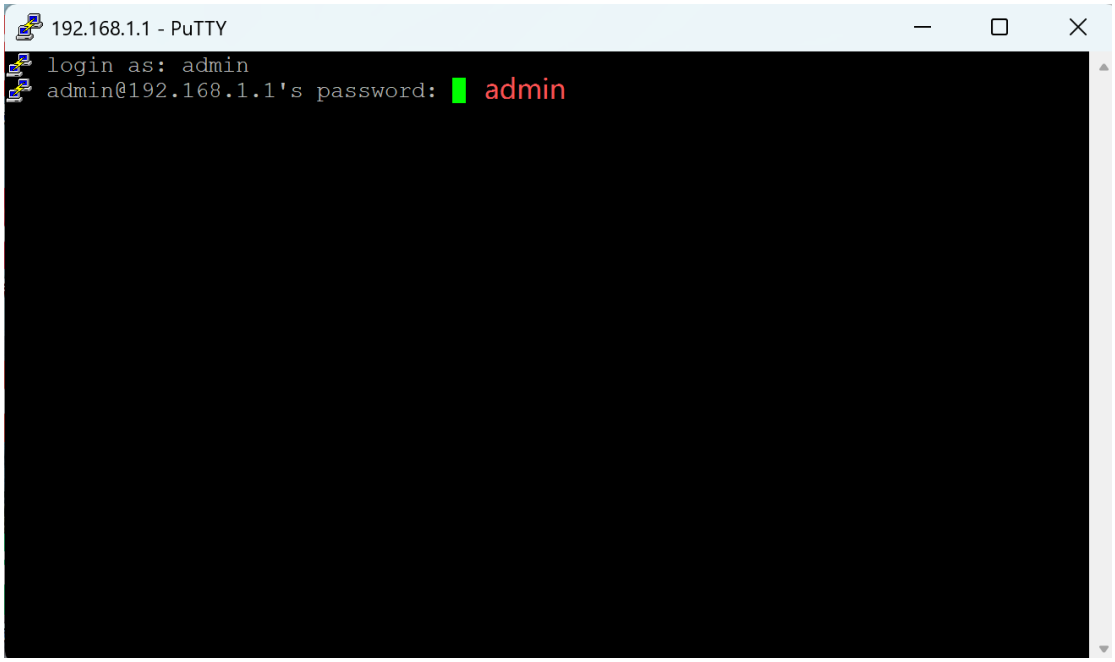
Install Docker

Log In to the Gateway

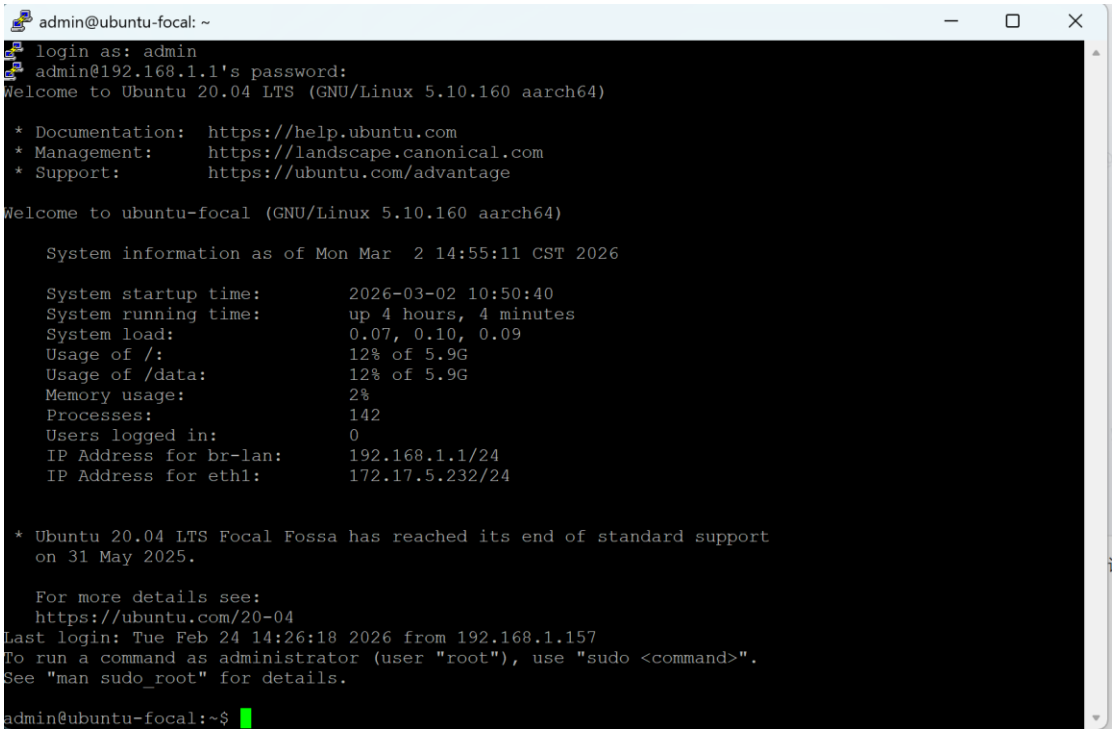
1. Open a terminal emulator such as PuTTY on your PC, then start an SSH or a telnet session to the gateway. In this example, PuTTY is used to open an SSH session.



1. Enter the username and password. The default username and password are both admin.



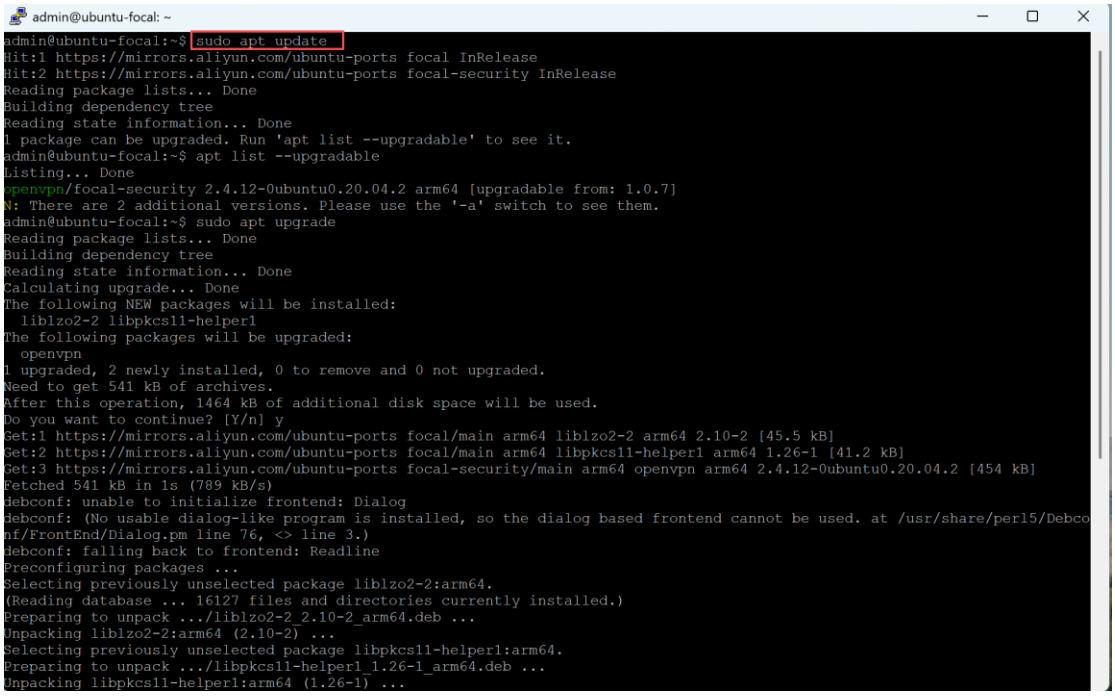
1. After you log in, the gateway presents a Linux shell.



Installation Steps

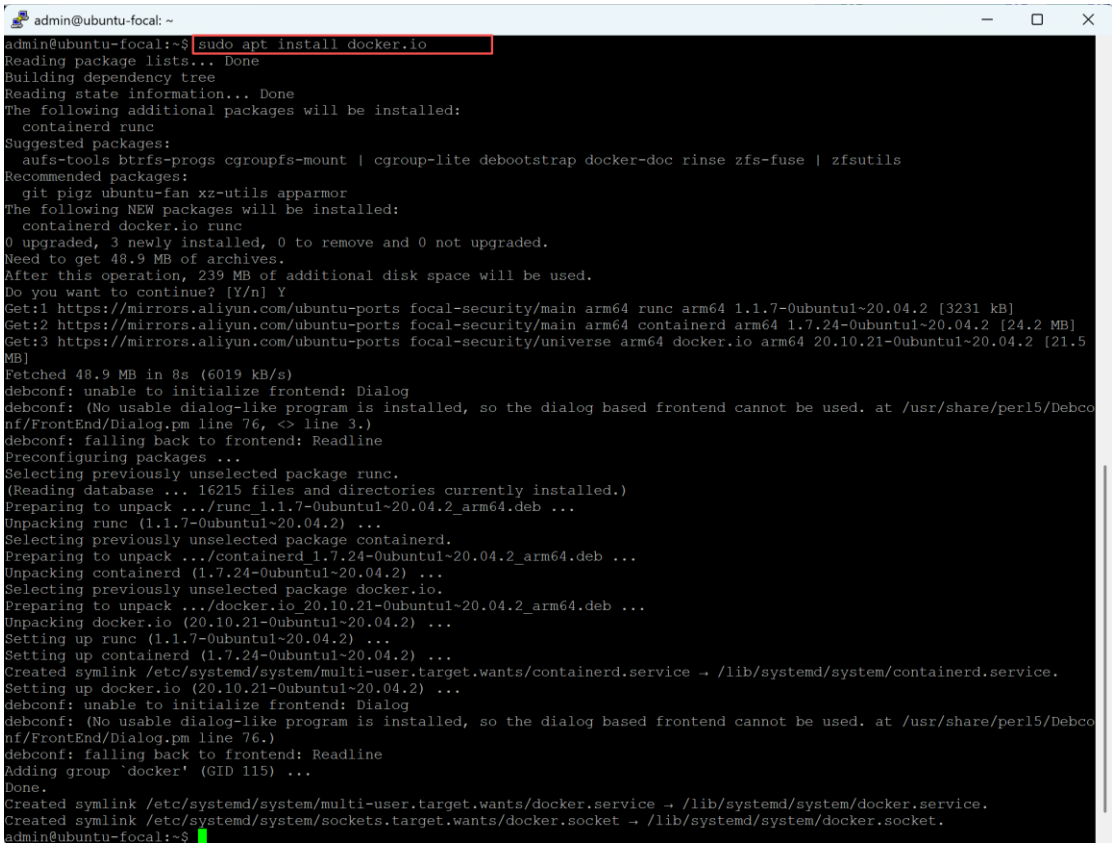
1. Update the package list.

sudo apt update



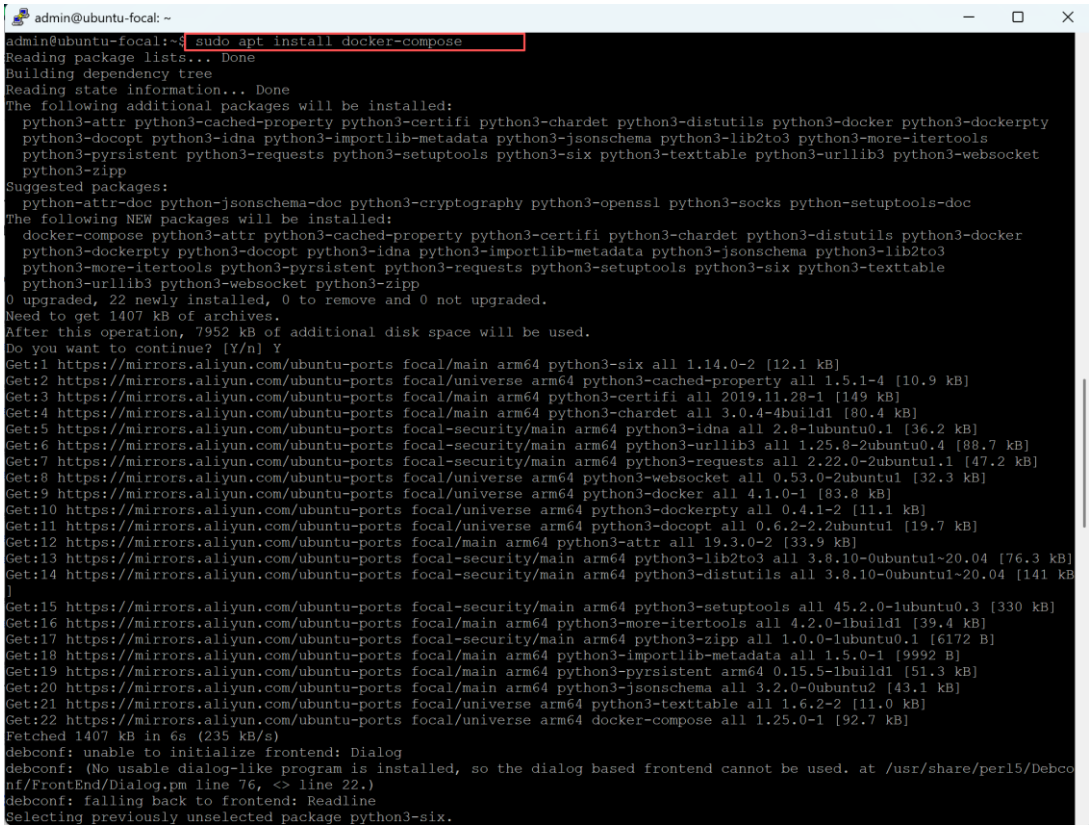
1. Install Docker from the official Ubuntu repository.

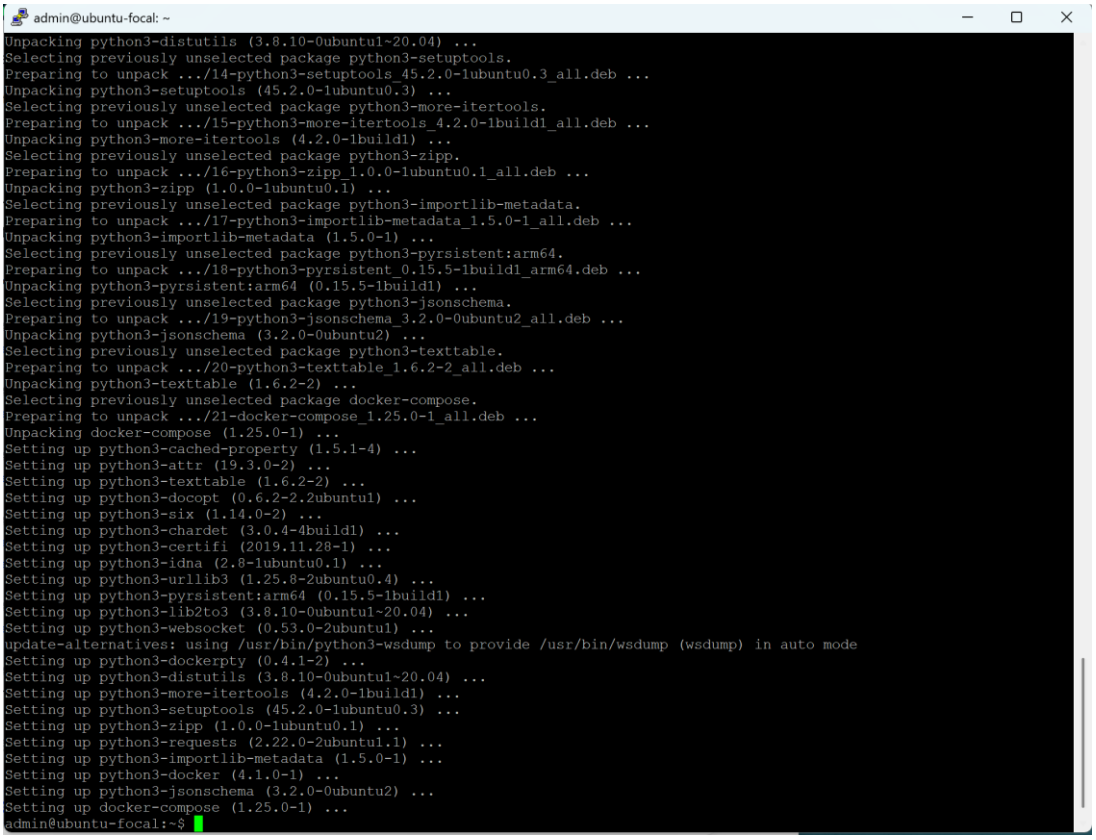
sudo apt install docker.io



1. Install the additional Docker tooling.

sudo apt install docker-compose

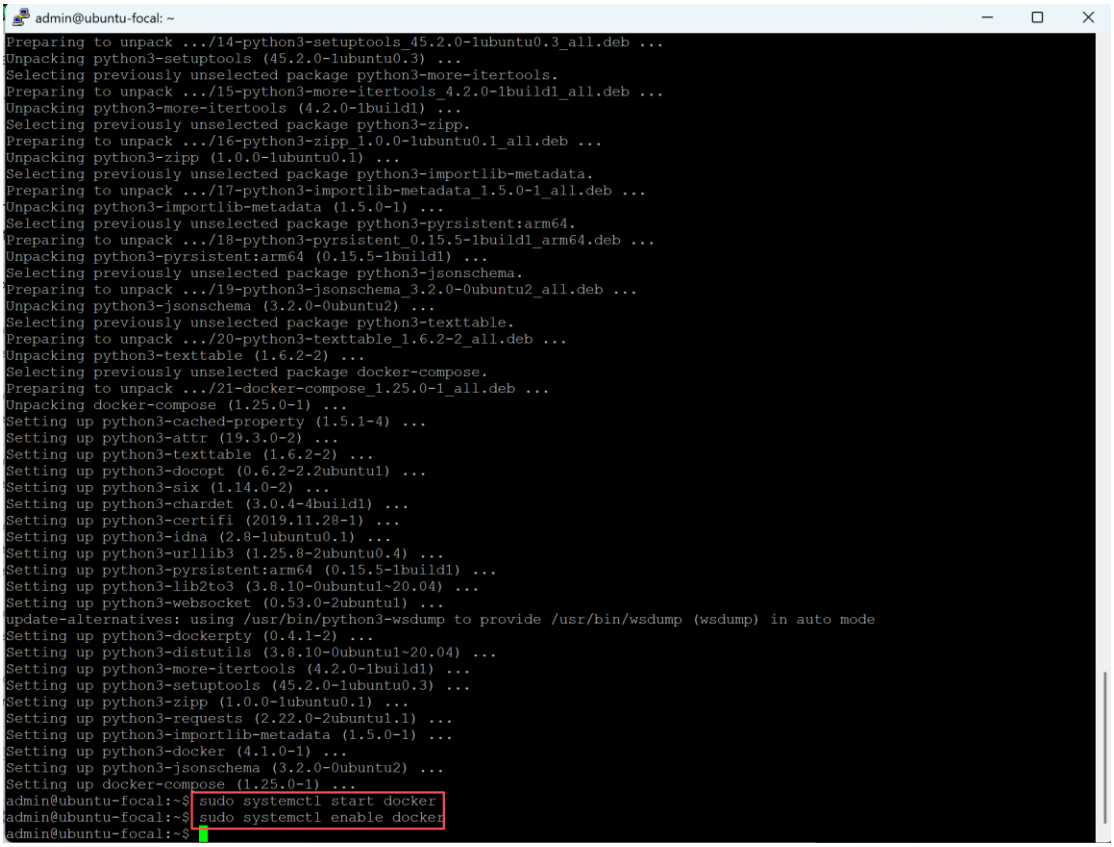




1. Start the Docker service and enable it at boot.

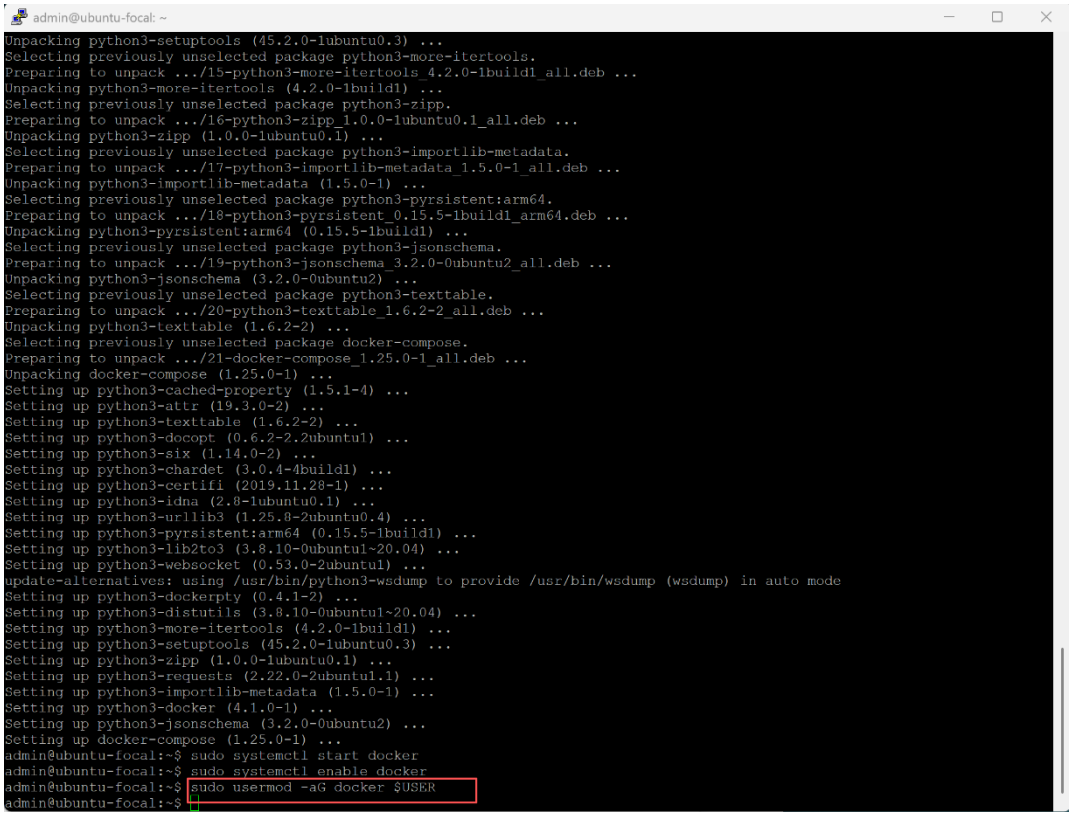
sudo systemctl start docker

sudo systemctl enable docker



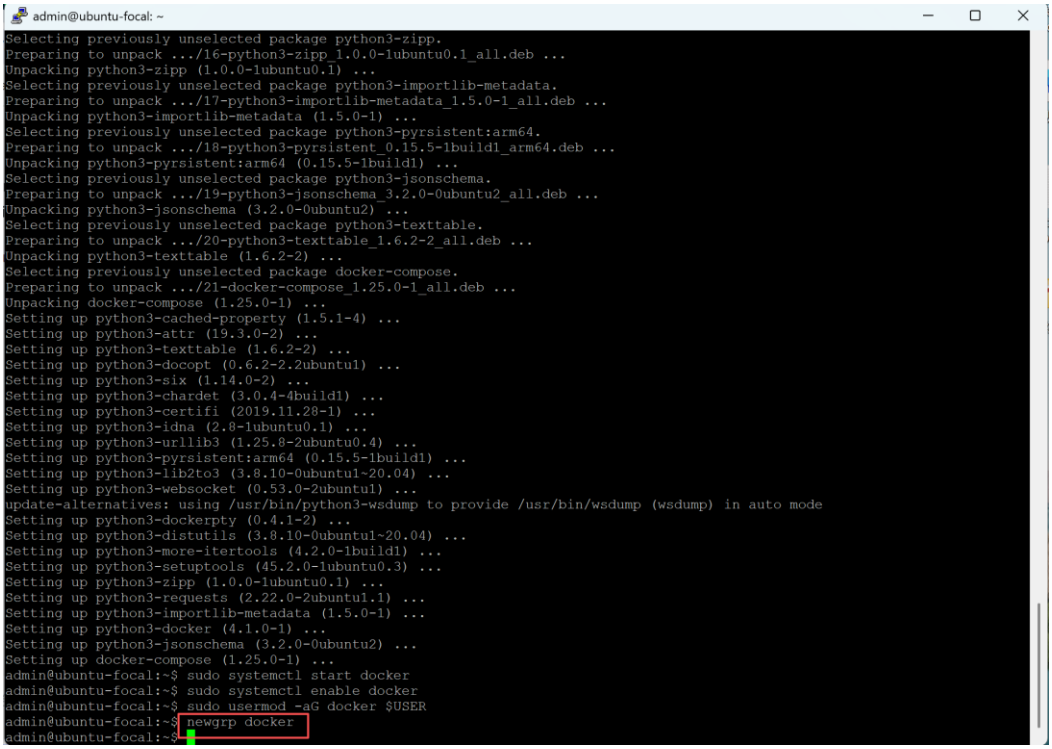
1. Add the current user to the docker group, so that Docker can be used without sudo.

sudo usermod -aG docker $USER



1. Log out and log in again, or run the following command, to apply the new group membership.

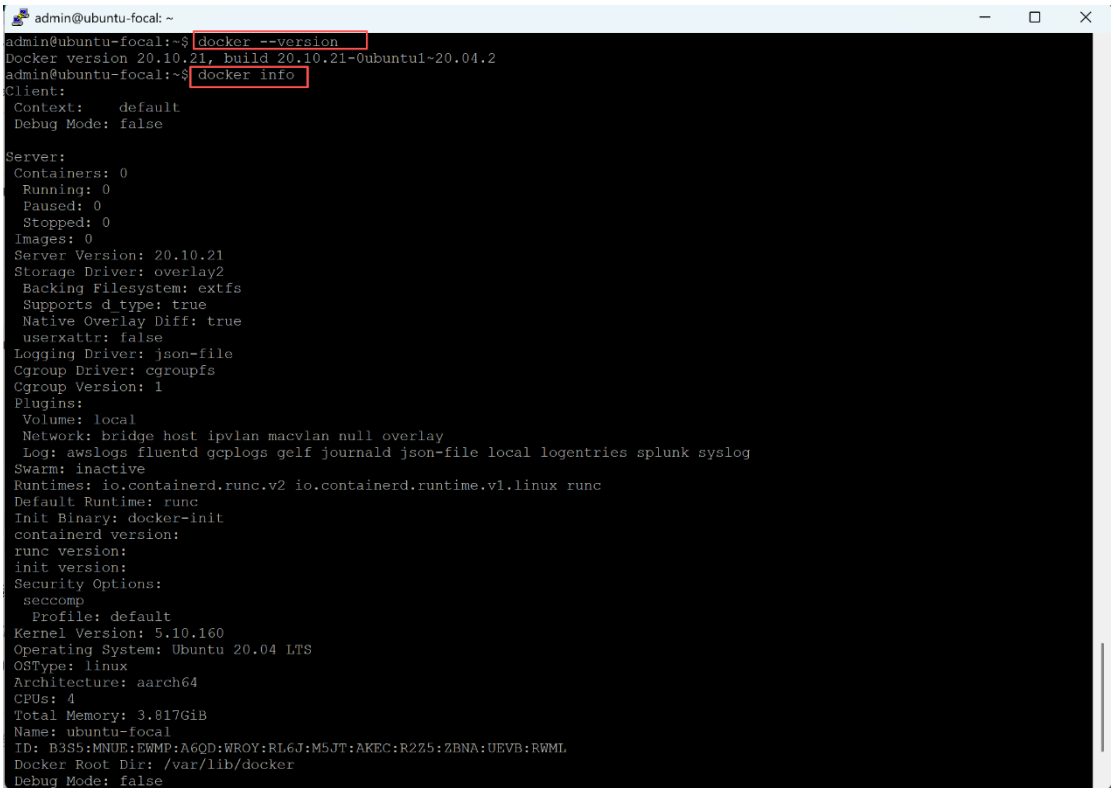
newgrp docker



1. Verify the installation.

docker --version

docker info



If the commands return version and configuration information, Docker has been installed successfully. In the example above, the installed version is 20.10.21.

Run a Test Container

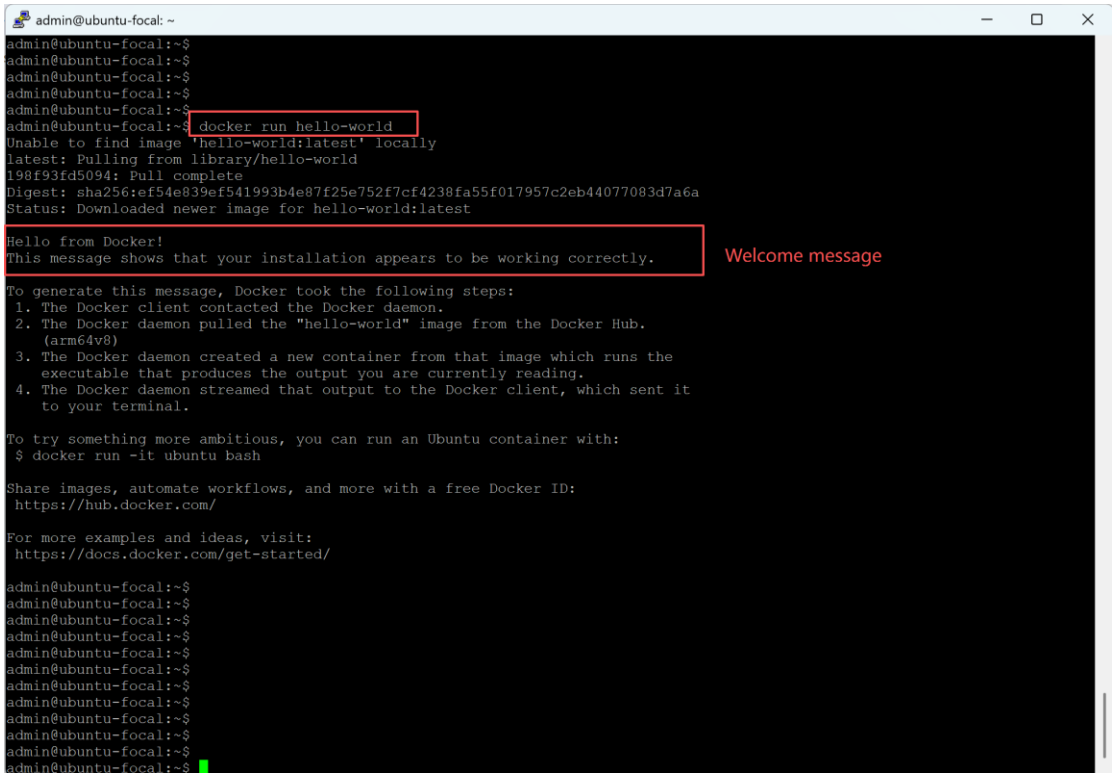
The examples below verify the basic functions of Docker after installation. They cover the common operations of pulling an image and running a container.

hello-world Image

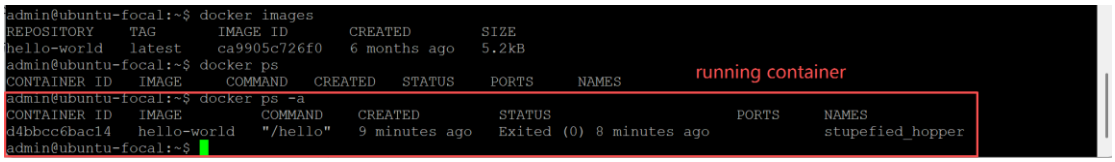
Docker provides a minimal test image called hello-world, which is used to confirm that Docker can run containers correctly.

1. Run the test image.

docker run hello-world



1. Docker pulls the hello-world image from the registry and runs the container. If the installation is correct, the container prints a welcome message.



Ubuntu Image

1. Pull the latest Ubuntu image.

docker pull ubuntu:latest



1. Start an interactive container and open a bash shell inside it.

docker run -it --rm ubuntu bash

```
admin@ubuntu-focal:~$ docker run -it --rm ubuntu bash
root@bdfe30136d45:/# cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.4 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.4 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
root@bdfe30136d45:/#
```

1. Inside the container, you can run Linux commands as usual. For example:

cat /etc/os-release # show the version of the container operating system

exit # leave the container

```
root@bdfe30136d45:/# cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.4 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.4 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
root@bdfe30136d45:/# exit
exit
admin@ubuntu-focal:~$
```

```
admin@ubuntu-focal:~$ docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED       STATUS       PORTS     NAMES
25c9a5066beb   ubuntu    "bash"    2 hours ago   Up 2 hours             relaxed_villani
admin@ubuntu-focal:~$ docker ps -a
CONTAINER ID   IMAGE         COMMAND     CREATED       STATUS                     PORTS     NAMES
25c9a5066beb   ubuntu        "bash"      2 hours ago   Up 2 hours                           relaxed_villani
d4bbcc6bac14   hello-world   "/hello"    3 hours ago   Exited (0) 3 hours ago               stupefied_hopper
admin@ubuntu-focal:~$
```

Created containers

NOTE: Docker is an open-source platform and Bivocom provides only the installation environment. The programs and applications that run inside Docker are secondary development and are outside the scope of Bivocom support, so no development or scripting guidance is provided. Refer to the official Docker documentation and research the required functionality yourself.

Verification Method:

1. Run docker --version and docker info. Both commands return version and configuration information without errors.
2. Run docker run hello-world. The container prints its welcome message, which confirms that Docker can run containers.
3. Run docker run -it --rm ubuntu bash, then run cat /etc/os-release inside the container. The command reports the version of the Ubuntu image.

Common Issues:

1. Docker reports "command not found" after installation: the shell session was opened before the package was installed. Close the session and open a new one, or run newgrp docker.
2. Docker reports "permission denied while trying to connect to the Docker daemon socket": the current user is not a member of the docker group. Run sudo usermod -aG docker $USER and log in again.
3. The image cannot be pulled: confirm that the gateway has Internet access by running ping 8.8.8.8, and check that no proxy or firewall rule blocks access to the registry.

The Docker service fails to start: run sudo systemctl status docker to inspect the service status, and confirm that the gateway is running the Ubuntu system image rather than OpenWRT.

Scenario 6: Send Modbus data to MQTT

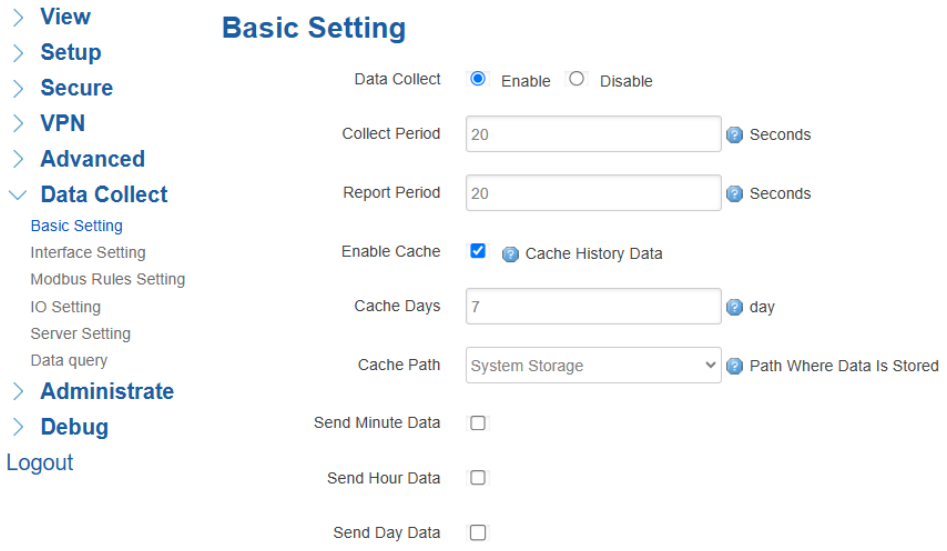
Objective: Get Modbus sensors' data and publish to MQTT broker.

Prerequisites: Ensure router connects to the internet, connect sensors (simulated by a Modbus slave in this case) to the correct interfaces, ensure sensors get suitable power supply.

Device Role: Device acts as a Modbus master gateway, responsible for collecting on-site sensor/device Modbus data and transmitting MQTT messages.

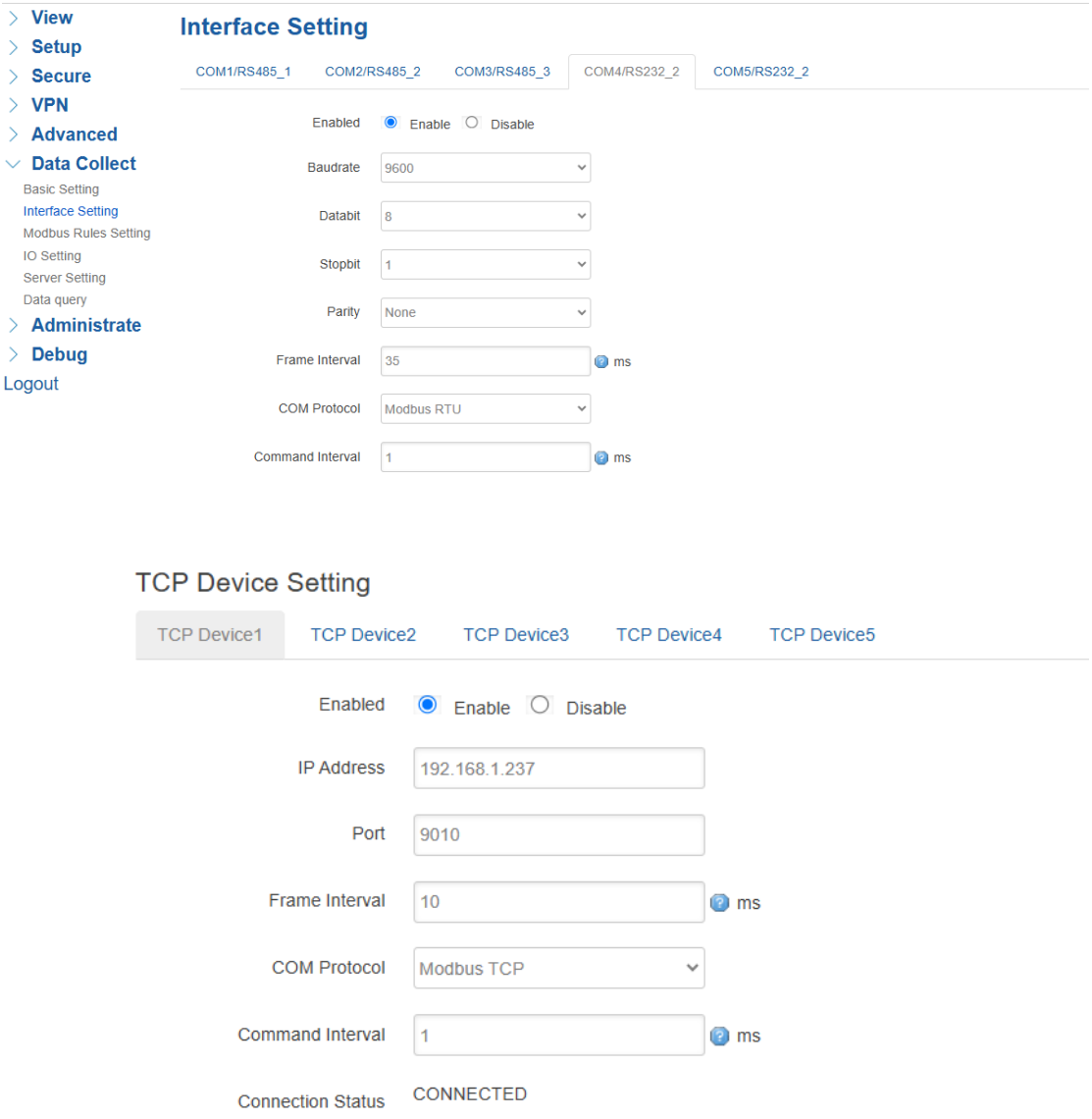
Configuration Steps:

1. Go to **Data Collect** > **Basic Setting** page to enable Data Collect function, set the **Collect Period** and **Report Period**. E.g. 20S for data collect, 20S for data reporting. User can **Enable Cache** to store the data when the network is disconnected, cached data will be resent after network reconnected.

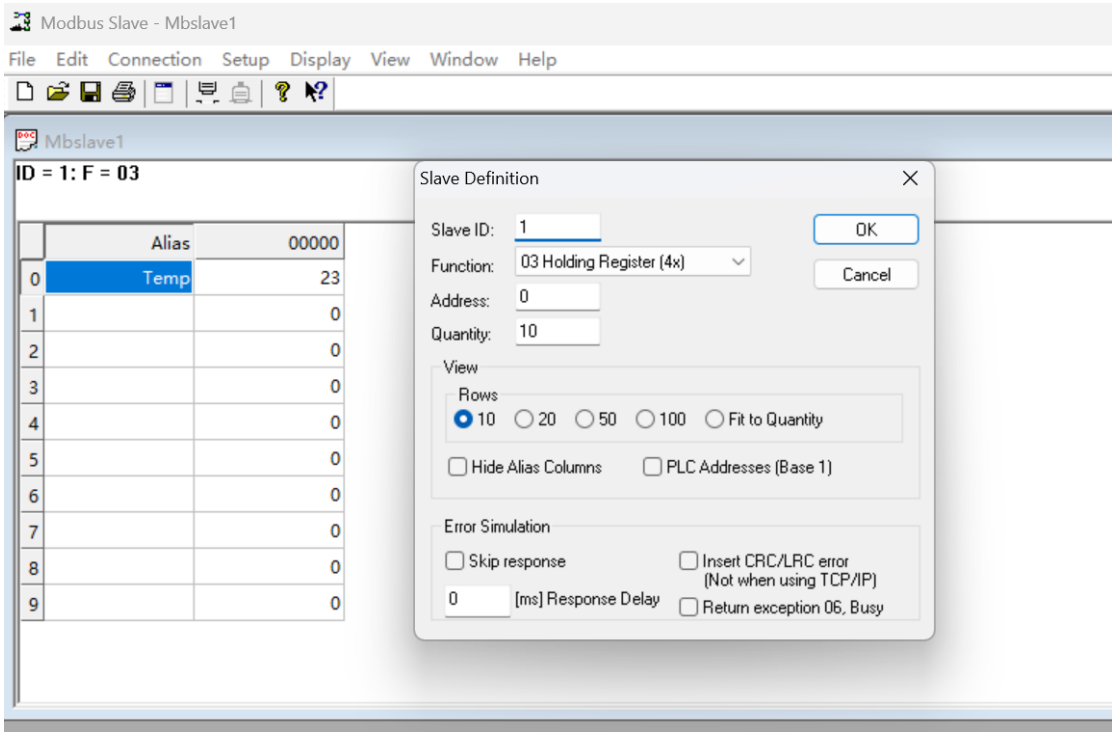


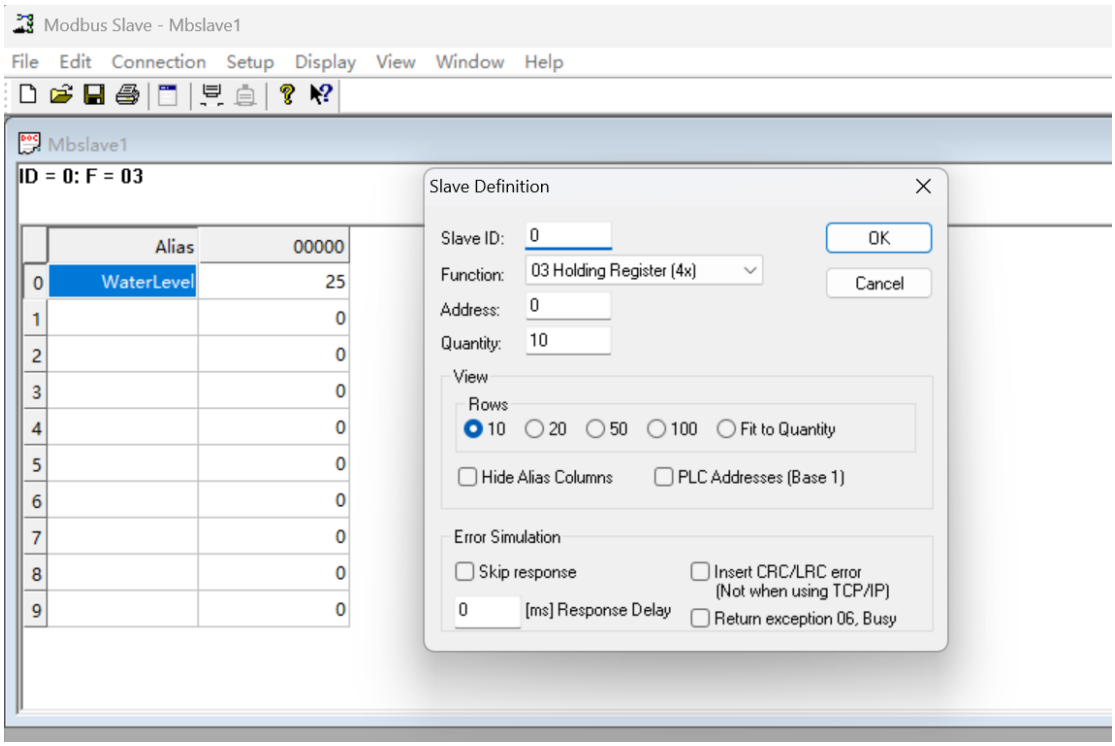
2. Go to **Interface Setting** page, set serial port parameters consistent with the sensors, select

COM Protocol as Modbus RTU according to the sensor output protocol. Configure the IP address and port when device connects with Modbus TCP slave device, select Modbus TCP as COM Protocol.

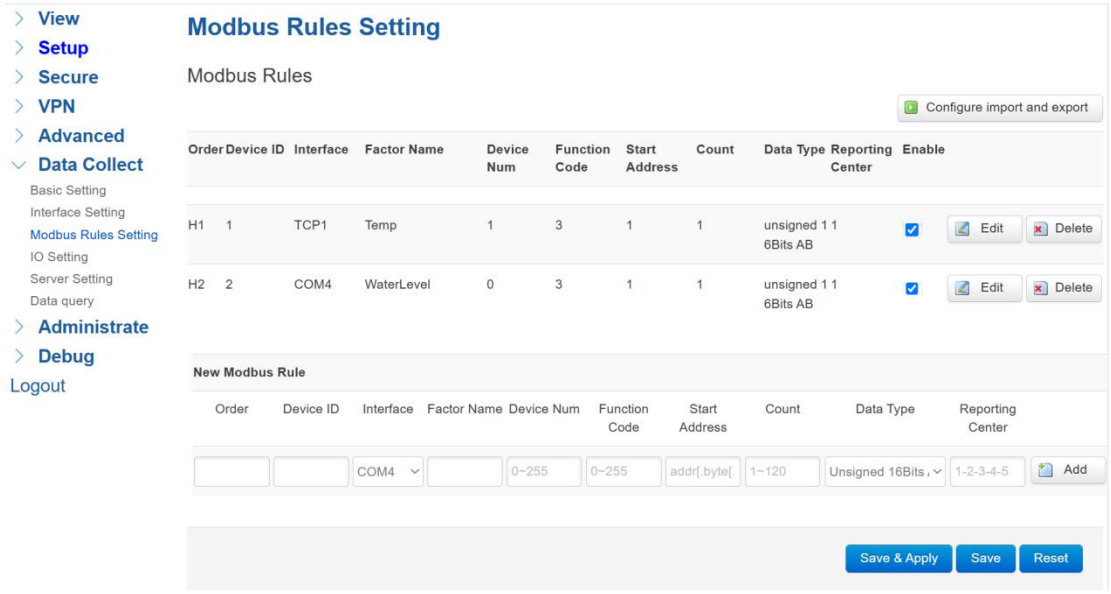


3. Confirm the Modbus slave settings of Modbus RTU/TCP sensor/device.





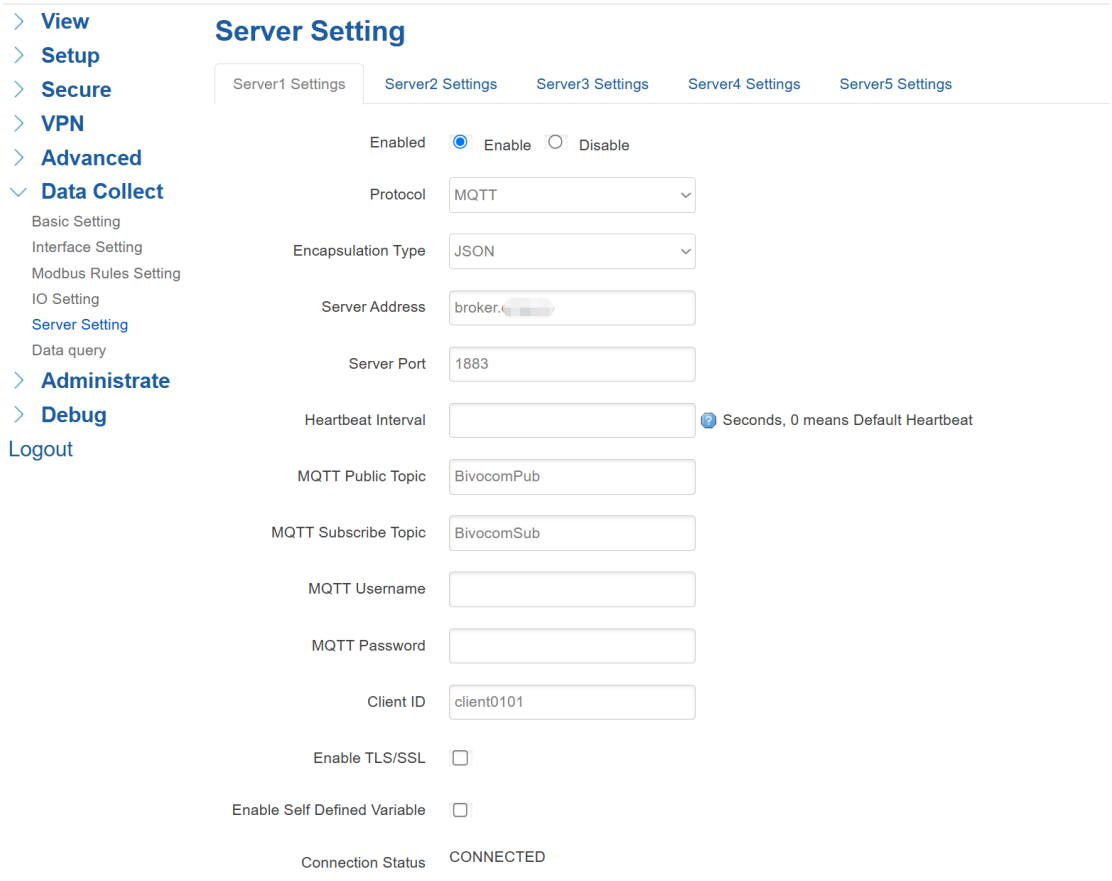
4. In **Data Collect** > **Modbus Rules Setting**, set the Modbus parameters consistent with datasheet of Modbus RTU/TCP sensor/device.



5. Check real-time data value at **Data Collect** > **Data query** page.

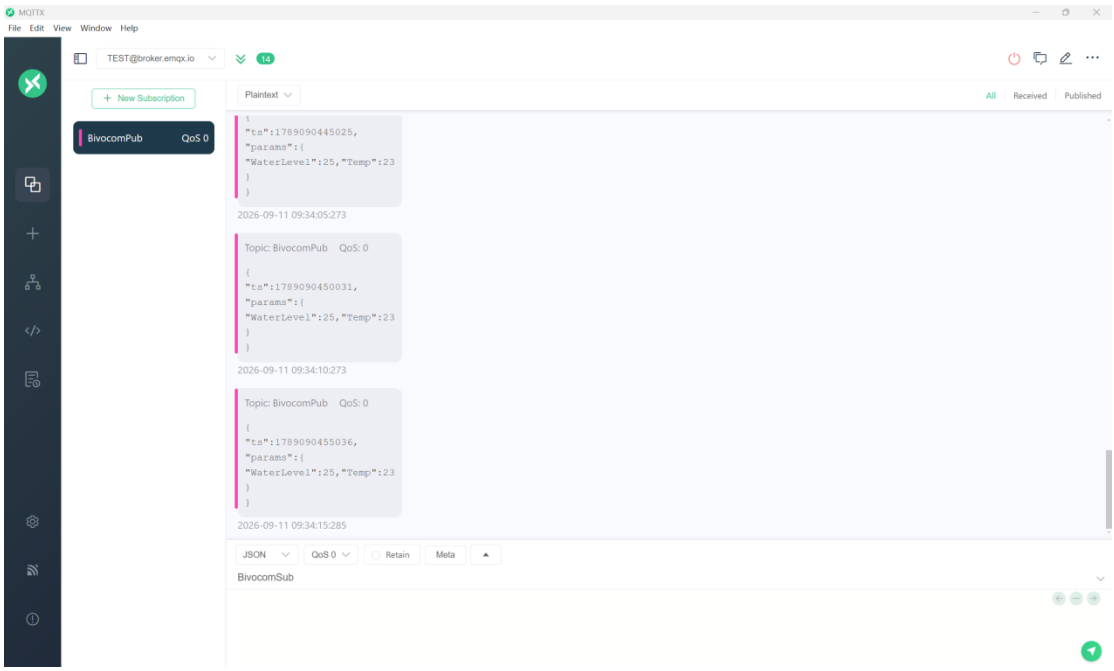


6. Go to **Data Collect** > **Server Setting**, select the protocol of server which need to receive data. Set the **Server Address** and **Server Port** as MQTT broker running, **MQTT Public Topic** is the topic name of data publish, **MQTT Subscribe Topic** is the topic name of data receiving by router. **Client ID** needs to be unique. Click **Save & Apply** button after all settings.



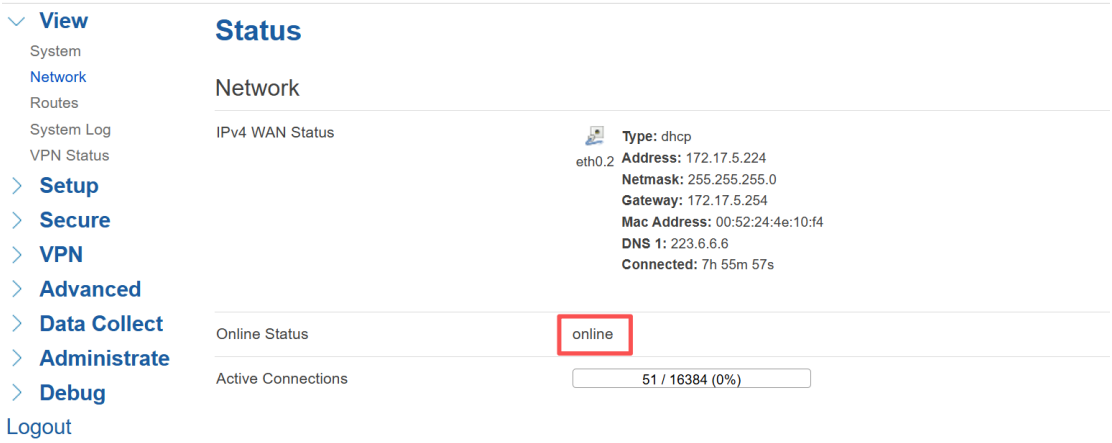
Verification Method:

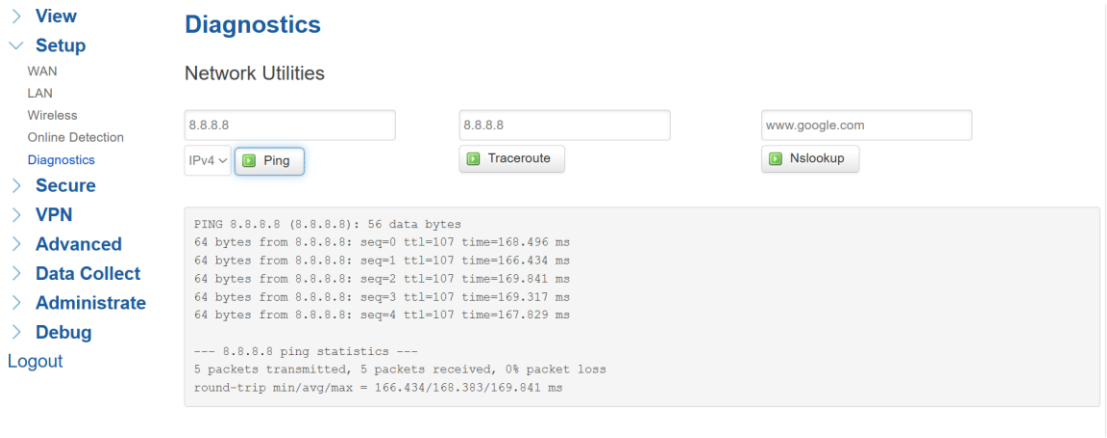
1. Open MQTT client software (e.g. MQTTX) on PC, connect to same MQTT broker, add **New Subscription** Topic "BivocomPub". After a while, JSON data will arrive from Bivocom router.



Common Issue:

- The device cannot read data from the Modbus sensor: make sure the serial port parameters match the sensor requirements, and that the Modbus rule settings (function code, slave ID, register address, register count and data type) match the sensor datasheet.
- Data can be read and displayed at Data Query page, but failed to be received by the MQTT client PC: Check the current network status at **View** > **Network** page, confirm current online status, ensure server address can be reached at **Setup** > **Diagnostics**. Confirm Modbus rule is enabled and set the right **Reporting Center** number.
- Data Value reading error:





Scenario 7: Control I/O and Change Modbus Data Remotely

Objective: Control ON/OFF for the relay and write Modbus registers data through MQTT broker.

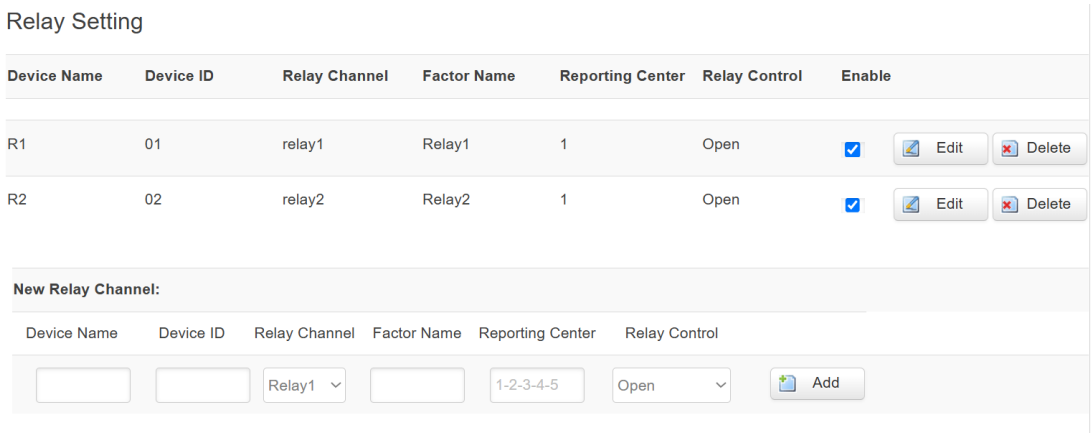
Prerequisites: Ensure router connects to the internet, connect sensors (simulated by a Modbus slave in this case) to the correct interfaces, ensure sensors get suitable power supply.

Device Role: Device acts as a protocol converter, transmit commands from MQTT broker to device, device will operate control logic as per the expected results.

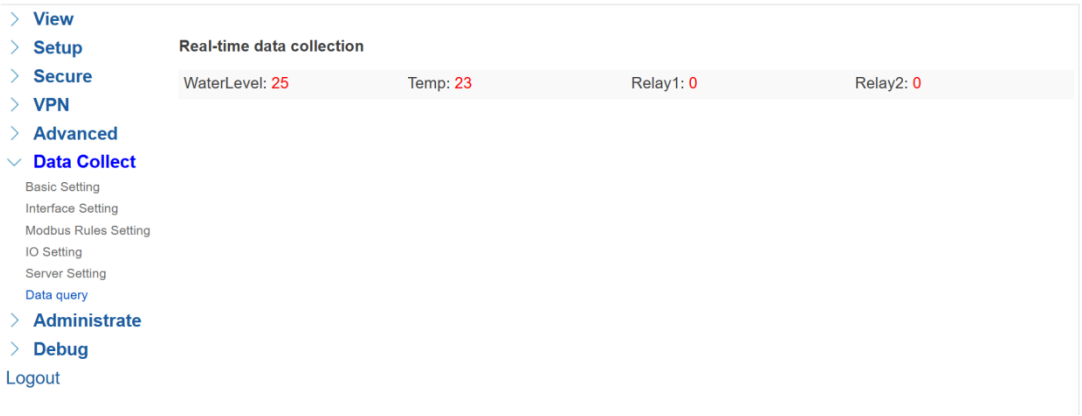
Configuration Steps:

1. Follow the configuration steps the same as **Scenario 4: Send Modbus data to MQTT**.

2. Go to **Data Collect** > **I/O Setting** page, setup the relay channels, Factor Name will be the name of data reporting and controlling.



3. Check Real-time data at **Data query**.



4. Connect same MQTT broker by PC, add **New Subscription** Topic (BivocomPub) the same as Bivocom router published, send controlling commands to the publish topic (BivocomSub) the same as Bivocom router subscribes. The **Factor Name** of Modbus data will be the key of controlling, device will reply with *{"status":"OK"}* if commands execute successfully. The format of writing Modbus registers should follow as below:

{

"method":"sendTelemeter",

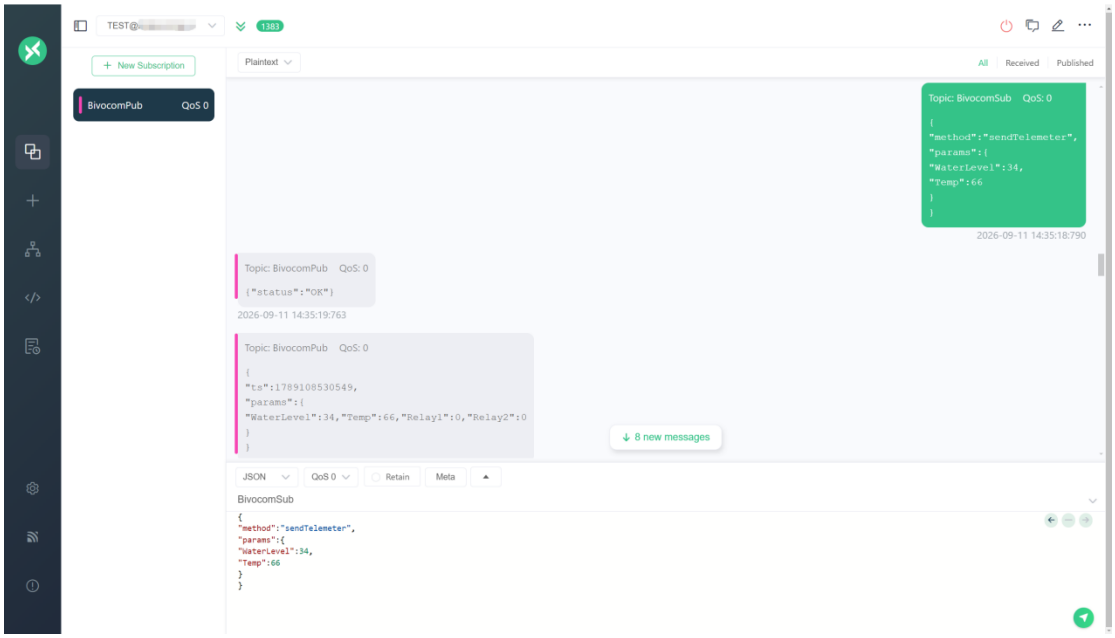
"params":{

"WaterLevel":34,

"Temp":66

}

}



5. To control relay channels remotely, fill in the factor names and use the command format shown below:

{

"method":"control_relay",

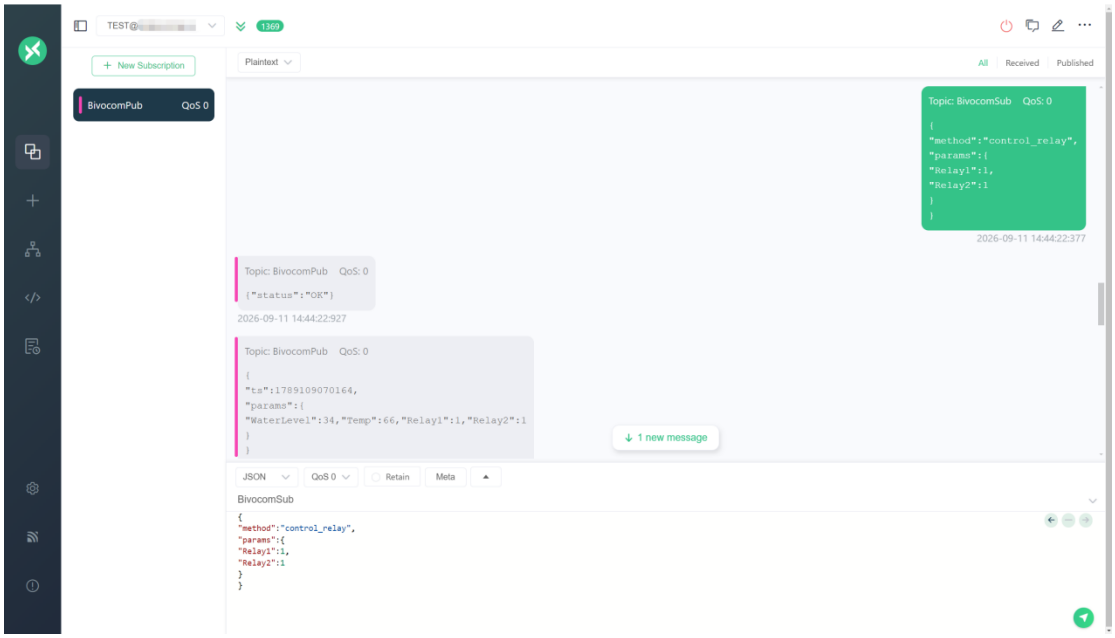
"params":{

"Relay1":1,

"Relay2":1

}

}



Common Issue:

- Device applies with *{"status":"Invalid method"}* or there is no response: Confirm the message format is correct and Factor name is the same as settings at Bivocom router.
- Relay channels value error: Ensure the Factor name consistent with the right relay channel.

Scenario 8: SCADA Communicates with Serial PLC/Sensor Remotely

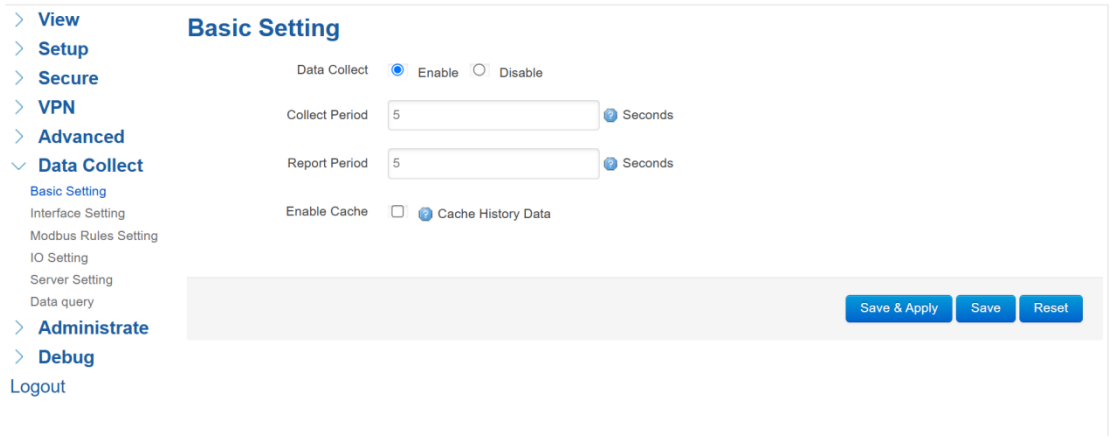
Objective: Establish two-way transparent transmission communication between SCADA and PLC/Sensor, data will be sent from SCADA to PLC/Sensor without any encapsulation protocol, response from PLC/Sensor will be sent back to SCADA transparently too.

Prerequisites: Ensure router connects to the internet, confirm the connection between Bivocom device and SCADA, connect PLC/sensor to the correct serial interface, ensure PLC/sensor get suitable power supply.

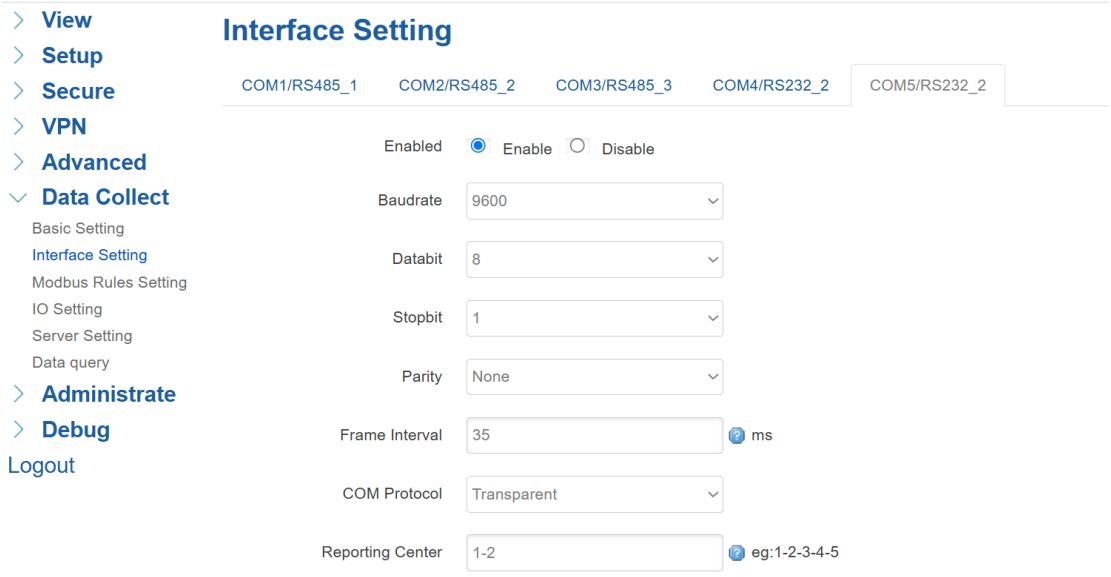
Device Role: Device acts as a transparent transmitter, create two-way communication.

Configuration Steps:

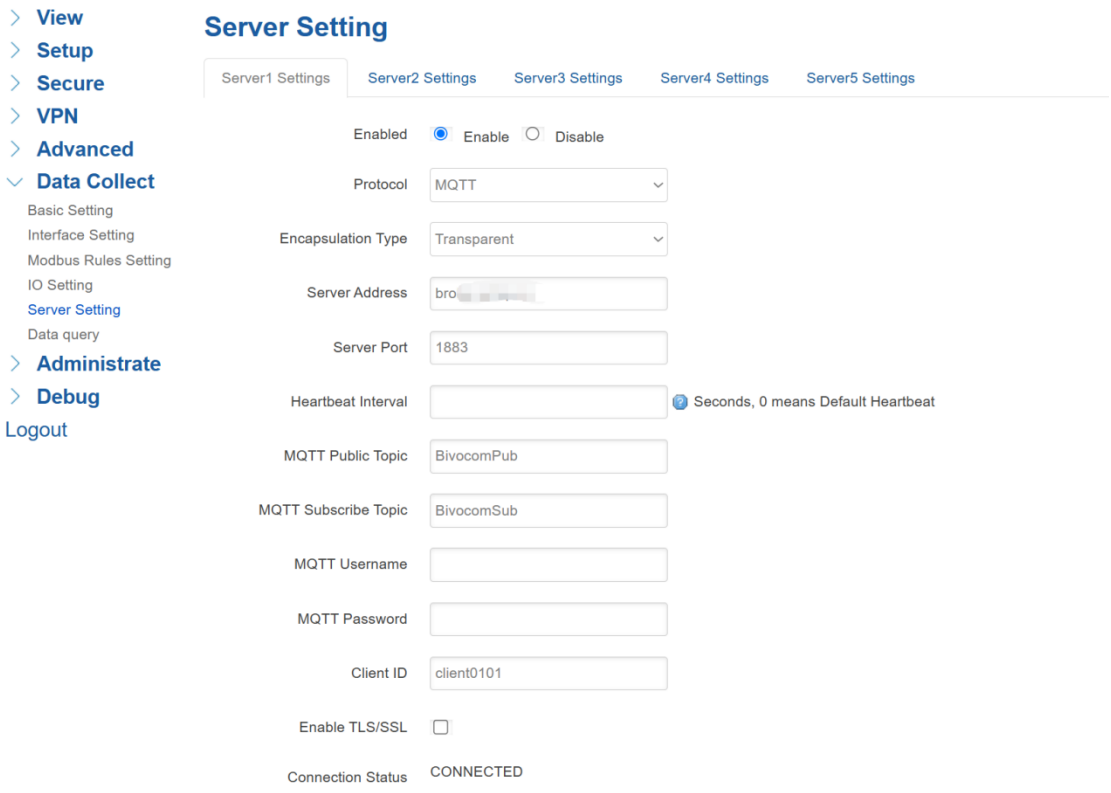
1. Enable **Data Collect** at **Basic Setting** page.

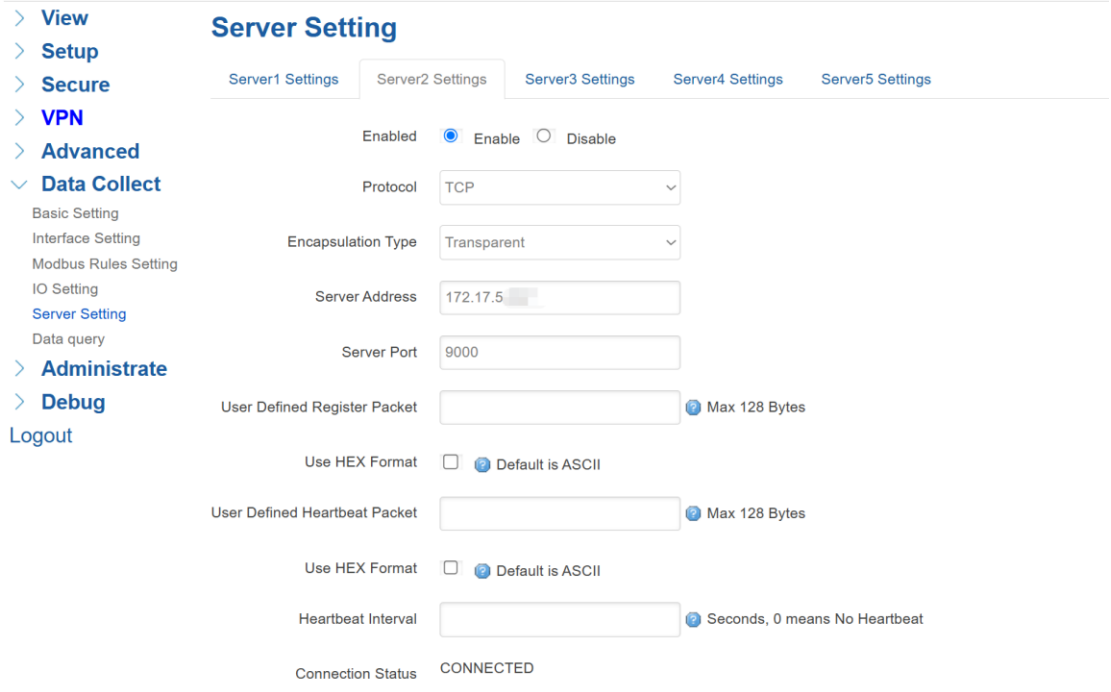


2. Set the correct serial parameters for local PLC/sensor (simulate by serial tool at this case) which connects to Bivocom device, **COM Protocol** should be **Transparent** at this scenario, **Reporting Center** should be the same as the server numbers that need to communicate with.



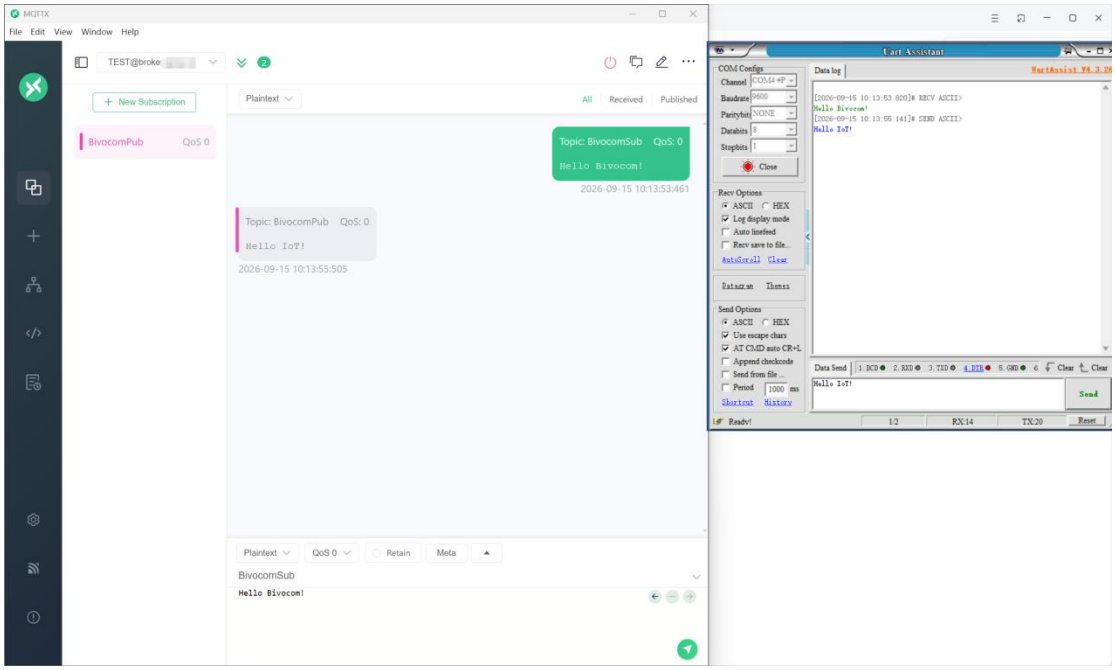
3. Go to **Data Collect** > **Server Setting** page, setup server address and protocol consistent with SCADA, we set up server 1 for MQTT broker, and server 2 for TCP server.



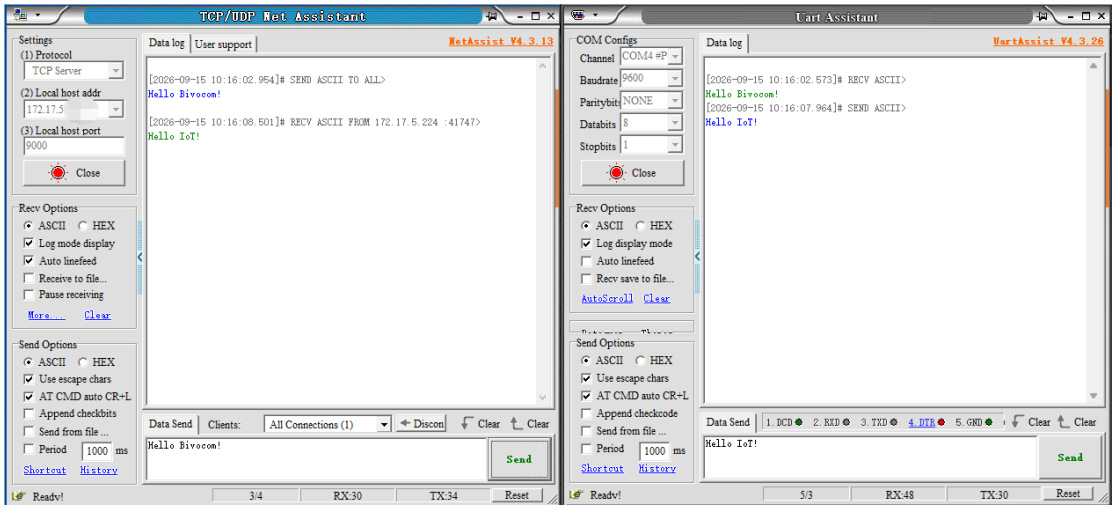


4. Send data from SCADA to PLC/Sensor, check the response from the PLC/Sensor on SCADA.

SCADA on MQTT Broker:



SCADA on TCP server:



Common Issue:

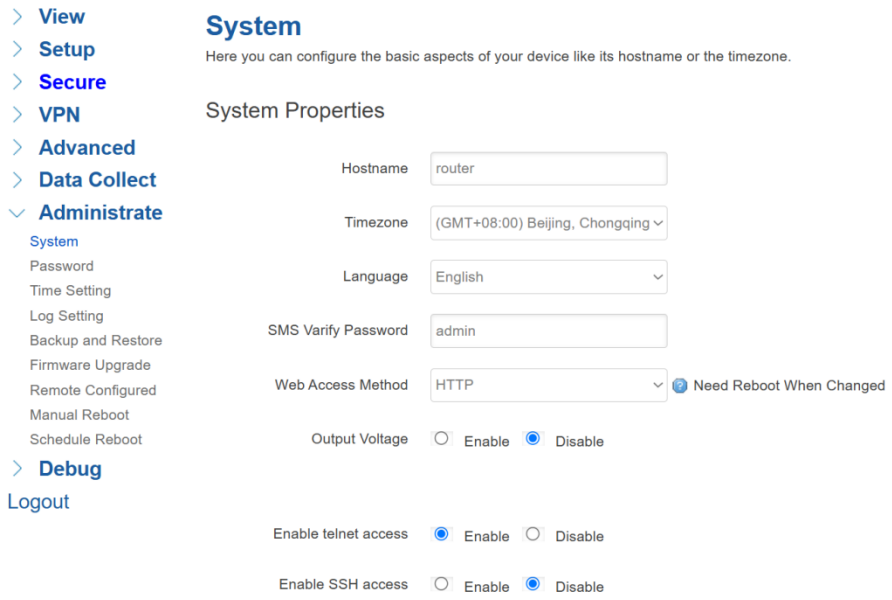
- SCADA failed to get a response from PLC/Sensor: Confirm the **Connection Status** at **Server Setting** page, check the network connection if show **Disconnected**, ensure the serial interface parameters are correct, server number is the same as SCADA.
- SCADA receives garbled characters: Check the baud rate of serial **Interface Setting**, select the correct **COM protocol** (**Transparent**).

3.7 Administrate

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

3.7.1 System

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

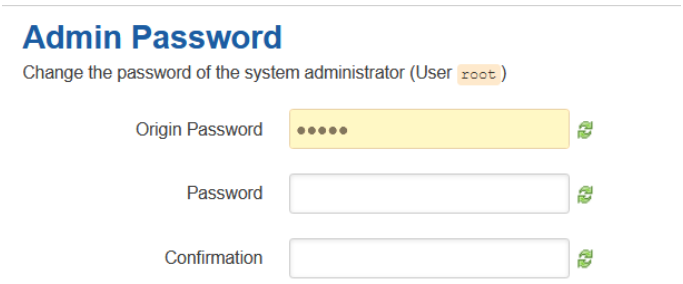


System	
Item	**Description**
Hostname	Fill in the hostname of device, new hostname will display on **View** > **System**
Timezone	Click the drop-down list to select the right time zone
Language	Select from **English** and **Chinese**
SMS Verify Password	Fill in the password when using SMS function
Web Access Method	Select from **HTTP** (default), **HTTPS** and **HTTP & HTTPS**, need reboot when setting changed.
Output Voltage	Click to enable power output function

Enable telnet/SSH access	Click to enable/disable telnet/SSH access, telnet access is enabled by default

3.7.2 Password

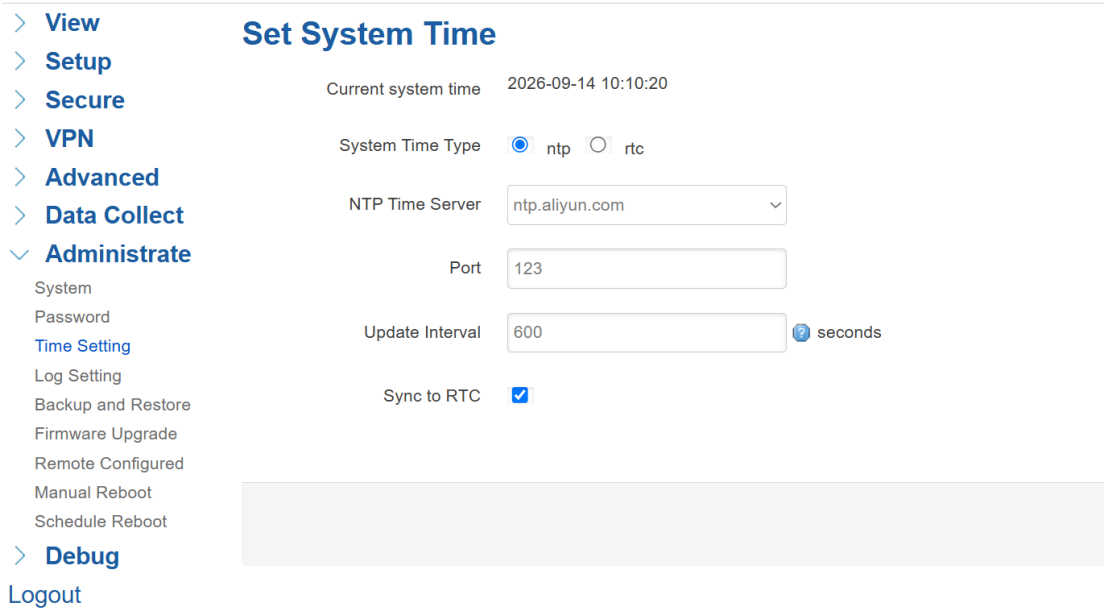
To revise the password of gateway.

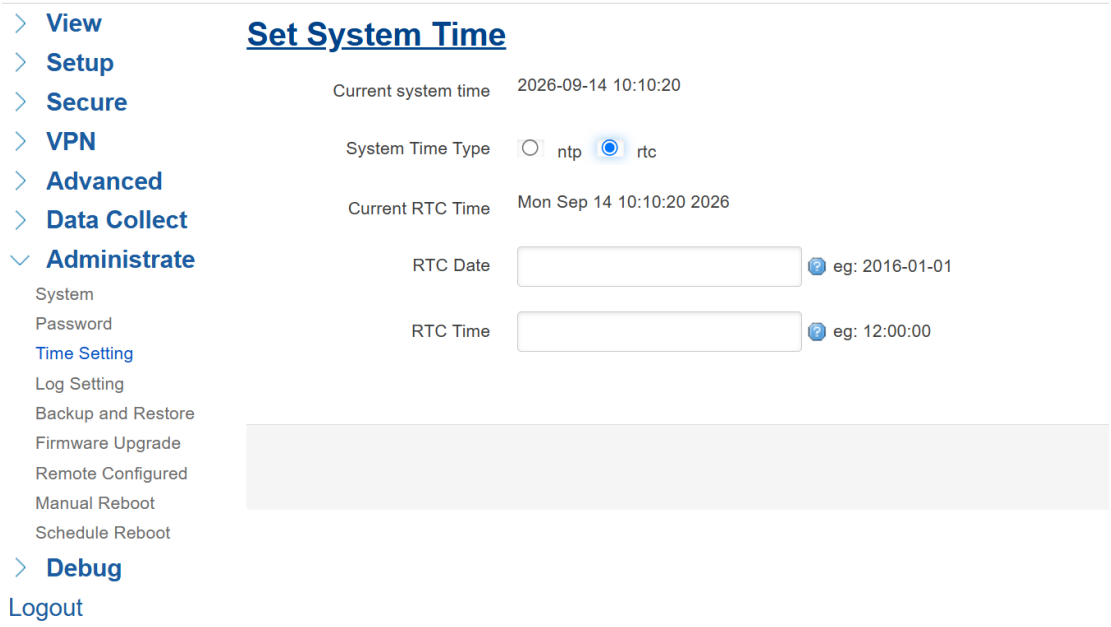


3.7.3 Time Setting

System time type includes RTC (Real Time Clock) and NTP (Network Time Protocol).

RTC will save the time even when the gateway is powered off, while for NTP, gateway 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 manually if it is not accurate.

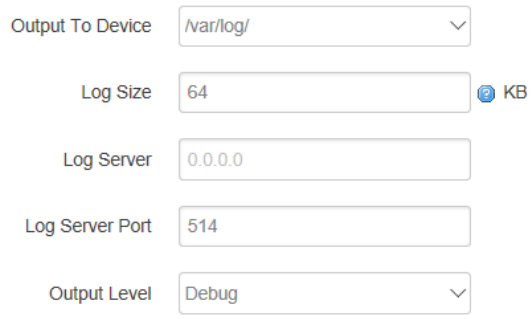




Time Setting	
Item	**Description**
Current system time	Show the current system time
System Time Type	Select from **NTP** and **RTC**
NTP Time Server	Select the **NTP server**, or fill in custom NTP server
Port	Fill in the port of NTP server, default port: 123
Update Interval	Fill in the interval of device to update from **NTP Server**
Sync to RTC	Click to synchronize time with RTC
Current RTC Time	Show the current RTC system time
RTC Date	Set RTC Date manually, e.g.: 2026-01-01
RTC Time	Set **RTC Time** manually, e.g.: 12:00:00

3.7.4 Log Settings

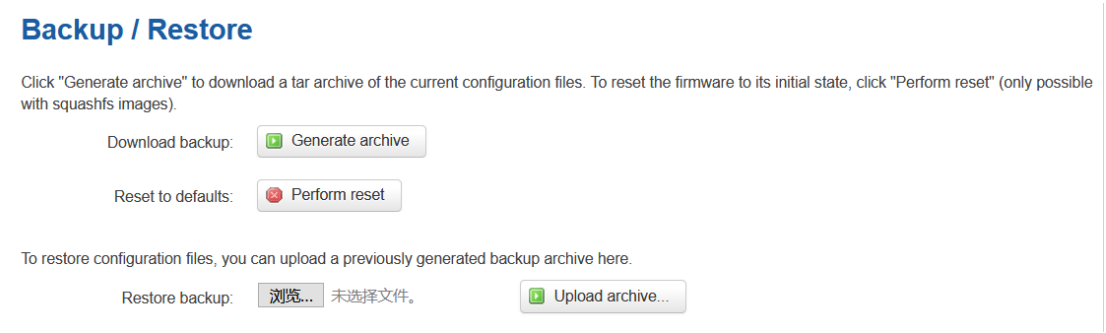
Log settings are for configuring the output parameters of system log.

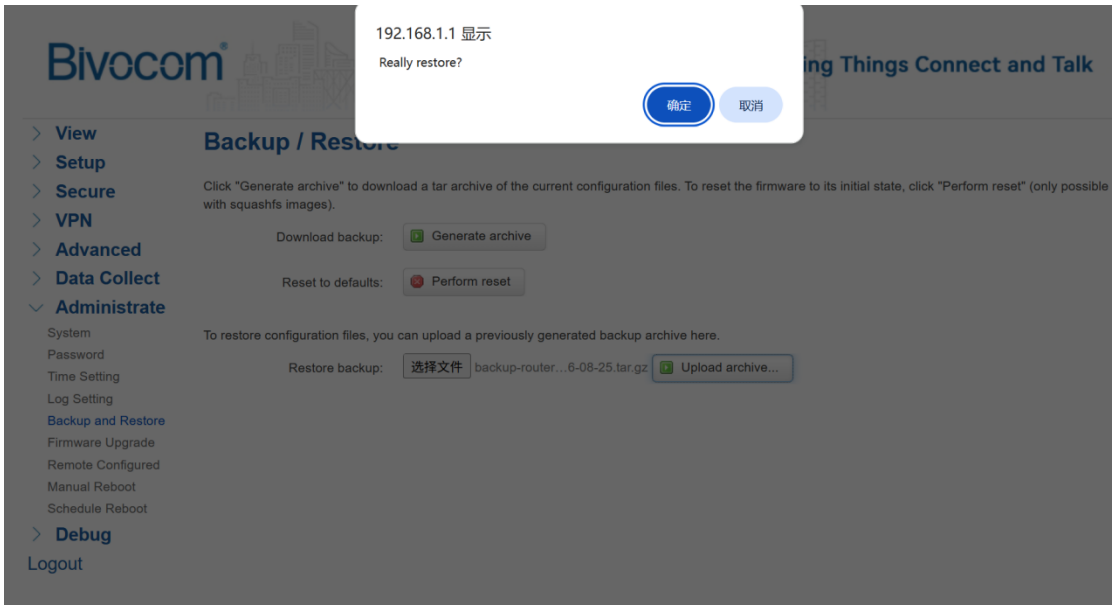


Log Setting	
Item	**Description**
Output To Device	Select the path of **System Log** storage, default path: /var/log
Log Size	Set the **System Log** size. Range: 1~30720 KB
Log Server	Fill in the **Log Server** IP address or domain name
Log Server Port	Fill in the port of **Log Server**, default port: 514
Output Level	Select from **Debug, Info, Notice, Warning** and **Error**

3.7.5 Backup and Reset

Users can either back up the configuration of gateway as a.gz file, or reset all settings to factory defaults.

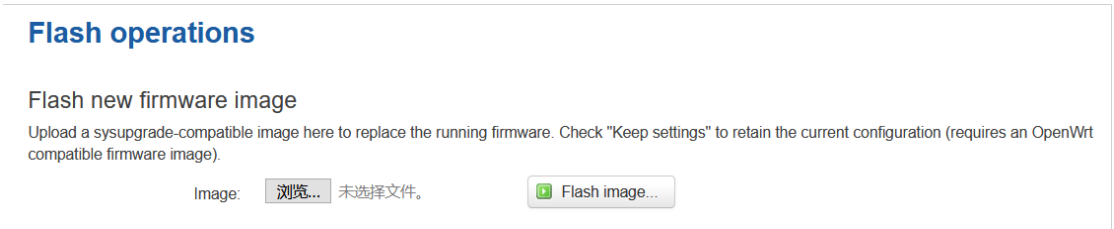




Backup and Restore	
Item	**Description**
Download backup	Click **Generate archive** button to generate a configuration file for current settings
Reset to defaults	Click **Perform reset** to factory reset for the device
Restore backup	Click **Chose File** to upload configuration file, **Upload archive**— click **OK**, device will auto reboot to load all configurations and apply

3.7.6 Firmware Upgrade (OpenWRT only)

The firmware upgrade page allows you to upgrade the firmware through the Web UI. Before upgrading, make sure the firmware file is the correct one for the device; otherwise the device may fail.



1) Choose and Upload Firmware Image

Click 'browse' and select the firmware, then click 'Flash Image', and firmware will be uploaded

to the gateway. Then you'll go to below page.



- **Checksum**

MD5 checksum value of firmware.

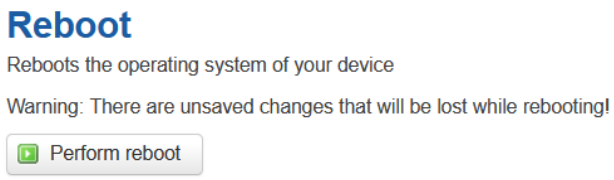
- **Size**

The size of firmware.

- **Proceed**

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

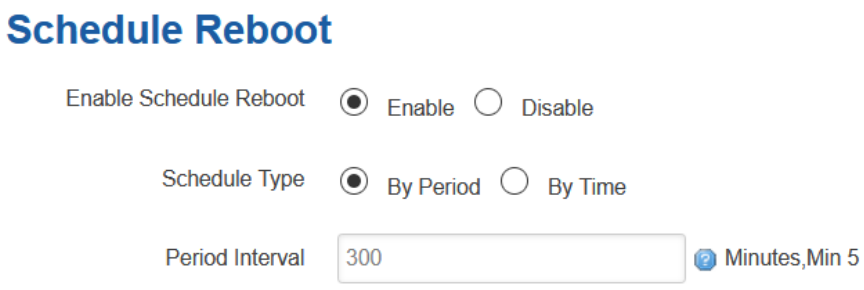
3.7.7 Manual Reboot



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

3.7.8 Schedule Reboot

The schedule reboot feature lets you preset device reboot rules by interval or at a specific time.

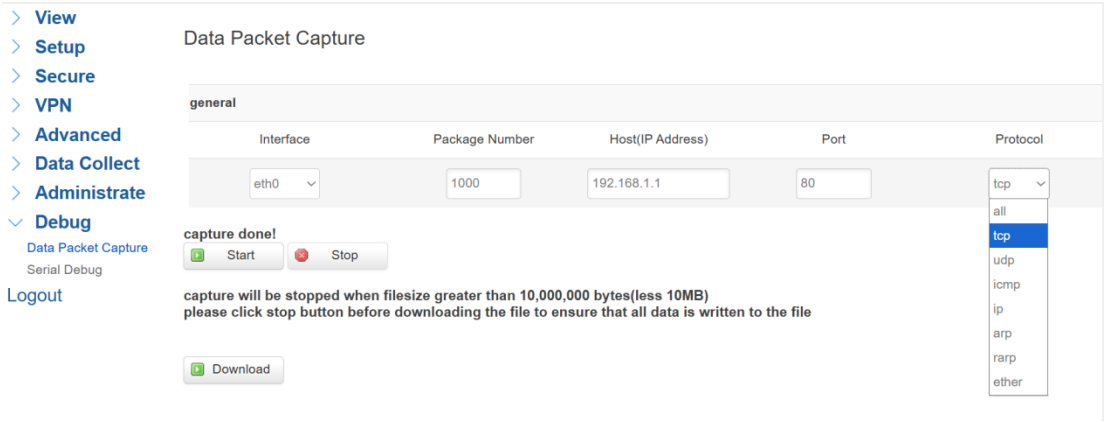


3.8 Debug

Debug page provides different tools for data capture, includes network and serial ports, which is Data Packet Capture and Serial Debug.

3.8.1 Data Packet Capture

Data Packet Capture page provides the basic tool that can capture packets by specifying the interface, IP, protocol, etc., and generate.pcap files for debugging.



Data Packet Capture	
Item	**Description**
Interface	Select the **Interface** where the data packets go through
Package Number	Set the size of packets that needs to be captured
Host (IP Address)	Set the target **Host IP/Domain** of data capture
Port	Set the target port for data capture
Protocol	Select from all, tcp, udp, icmp, ip, arp, rarp and ether, filter the protocol that should be captured

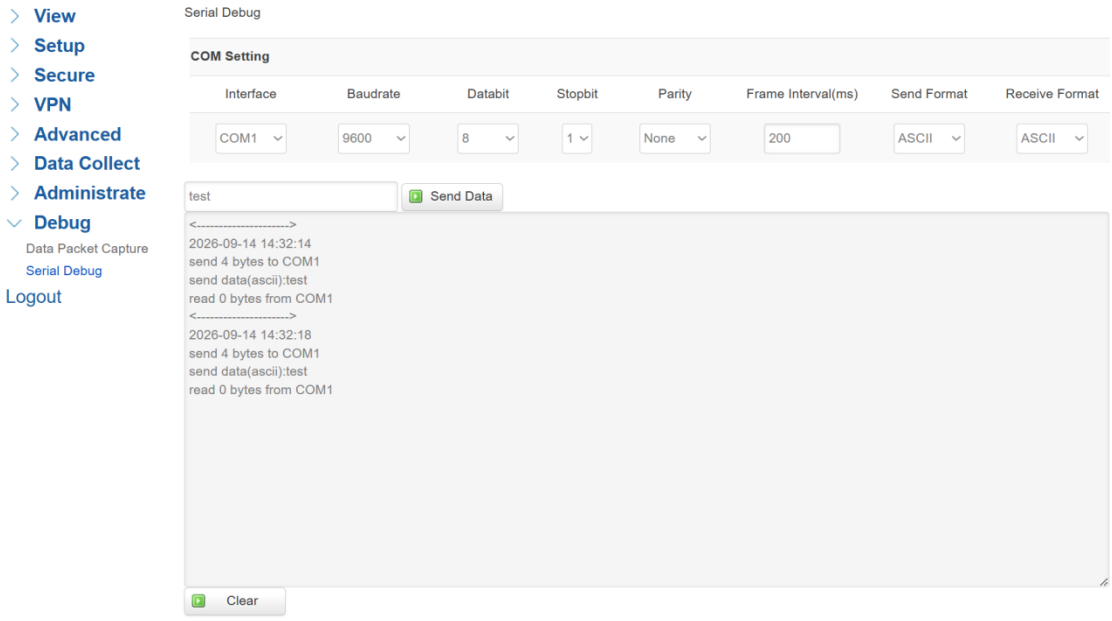
NOTE:

Capture will be stopped when file size greater than 10,000,000 bytes (less 10 MB).

3.8.2 Serial Debug

Serial Debug page provides a tool that simulates a master station to send data to and receive

corresponding replies from serial devices. The serial COM port and configuration can be specified. Sent and received data can be specified in ASCII or HEX format.



Serial Debug	
Item	**Description**
Interface	Select the target COM **Interface** that needs simulated data send
Baud Rate	Set **Baud Rate** for slave serial device/sensor
Data Bits	Set **Data Bits** for slave serial device/sensor
Stop Bits	Set **Stop Bits** for slave serial device/sensor
Parity	Set **Parity** for slave serial device/sensor
Frame Interval (ms)	Set the configurable silent gap between serial frames that delimits frame boundaries.
Send Format	Select from **ASCII** and **HEX**
Receive Format	Select from ASCII and HEX

3.9 Logout

Click the Logout menu to log out of the Web UI of device.

3.10 FAQ

Q1. What to do if the cellular network doesn't dial successfully?

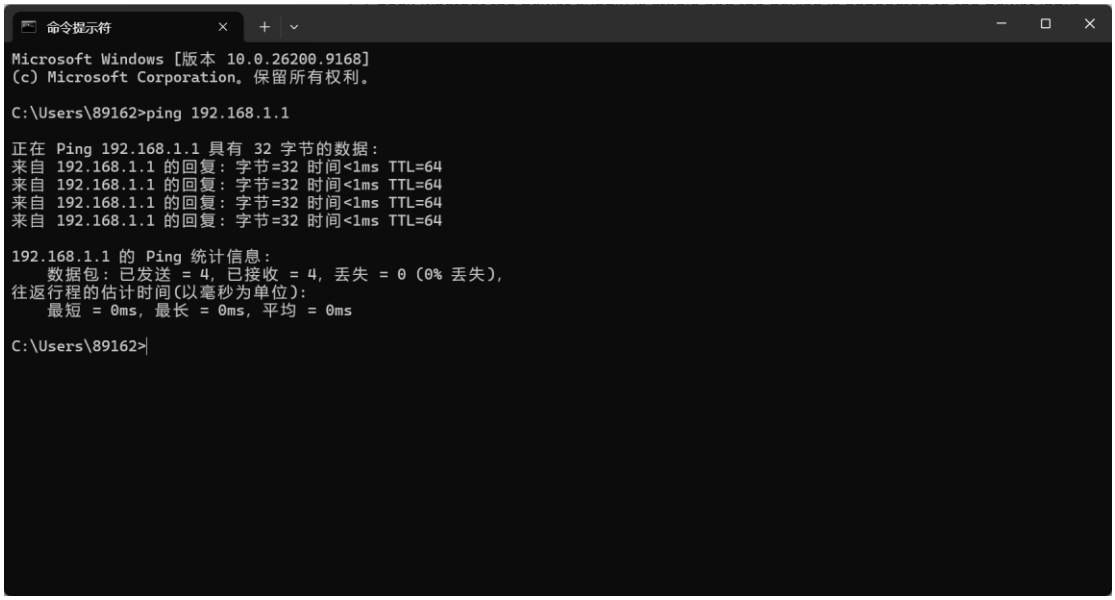
1. Check whether the SIM card is inserted into the correct slot and whether the cellular antennas are installed correctly.
2. Ensure the **WAN Connection Type** is set correctly (e.g., LTE), and the **APN** settings and **Username/Password** are configured as required by your SIM card provider.
3. Check the **View** > **Network** page in the Web UI or the signal status indicator to confirm the current signal strength.
4. Test the internet connection on the **Setup** > **Diagnostics** page by pinging 8.8.8.8 in the Web UI.
5. Remove the SIM card and insert it into a cell phone to check whether it can access the internet.
6. Restart the device and power it on after a few seconds.
7. Reset Factory Settings under **Administrate** > **Backup and Restore** > **Perform Reset**, then try again.

Q2. What to do if device keeps rebooting?

1. Check whether the power supply is stable and the device is connected to the power input correctly.
2. Ensure the IP addresses in **Setup** > **Online Detection** are reachable, and the **View** > **Network** page shows Online.
3. Check whether Administrate > Schedule Reboot is disabled.

Q3. What to do if cannot access Web UI successfully?

1. Check whether the Ethernet cable is connected to the LAN port and the LAN indicator is on steadily.
2. Ensure the PC is set to **DHCP** or a **static IP address** on the same subnet as the LAN address, and try to ping the Web UI address (e.g., ping 192.168.1.1) in Command Prompt (CMD).



3. Check the firewall settings on the PC.
4. Try another browser, such as Chrome, and try again.

Q4. What to do if forget the password of Web UI?

If you forget the Web UI password, you need to reset the device to factory settings by long-pressing the Reset button until all LED indicators turn off.

NOTE: This operation will clear all settings.

Q5. How to back up and restore current configurations to the other device?

1. Go to the **Administrate** > **Backup and Restore** page, click **Generate Archive** to save the current configurations to a file, and save it locally.
2. Switch to the other device, log in to the Web UI, upload the file to the other device, click **Upload Archive** to start the restore, and the device will reboot to load all configurations.