

Industrial Mini 5G IoT Router TR323

User Guide

Version 4.0, 09-01-2026

Thank you for choosing the Bivocom Cellular IoT Router. 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

About This Guide

Thank you for choosing Bivocom Industrial Cellular Router TR323 Series.

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

This manual is compatible with the following models

Model	Description
TR323	Industrial Mini 5G IoT Router

Table of Contents

About This Guide.....	2
Table of Contents.....	3
1. Introduction.....	6
1.1 Overview.....	6
1.2 Applications.....	6
1.3 Advantages.....	7
1.4 Dimensions.....	8
1.5 Physical Characteristics.....	8
2. Getting Started.....	8
2.1 Package Checklist.....	8
2.2 Installation.....	9
2.2.1 SIM/UIM Card.....	9
2.2.2 Interface Connection.....	10
2.2.3 Power Supply.....	11
2.2.4 Cellular Antenna.....	11
2.2.5 Wi-Fi Antenna (Optional).....	11
2.3 LED Indicators.....	12
2.4 Reset.....	12
2.5 Quick Check.....	12
3.0 Access to Web UI.....	13
3.0.1 Connect the PC to the TR323 network.....	13
3.0.2 Log in to the Web UI.....	14
3.1 View.....	15
3.1.1 System.....	15
3.1.2 Network.....	15
3.1.3 Routing Tables.....	16
3.1.4 System Log.....	17

3.1.5 VPN Status.....	17
3.2 Setup.....	18
3.2.1 WAN.....	18
3.2.2 LAN.....	20
3.2.3 Wireless (Optional).....	21
3.2.4 Wireless Client (Optional).....	23
3.2.5 Online Detection.....	23
3.2.6 Diagnostics.....	25
3.2.7 Quick Check.....	25
3.3 Security.....	26
3.3.1 DMZ Host.....	26
3.3.2 Port Forwards.....	26
3.3.3 Traffic Rules (ACL Configurations).....	28
3.3.4 Custom Settings.....	32
3.4 VPN.....	37
3.4.1 PPTP.....	37
3.4.2 L2TP.....	40
3.4.3 IPSec.....	44
3.4.4 OpenVPN.....	47
3.4.5 GRE.....	51
3.4.6 XFRP Client.....	51
3.4.7 VPN Common Issues:.....	52
3.5 Advanced.....	52
3.5.1 Send SMS.....	52
3.5.2 Static Routes.....	53
3.5.3 Net Flow.....	53
3.5.4 GPS Location (Optional).....	54
3.5.5 Dynamic DNS.....	58

3.5.6 DHCP and DNS.....	59
3.6 Data Collect.....	60
3.6.1 Basic Setting.....	60
3.6.2 Interface Setting.....	61
3.6.3 Modbus Rules Setting.....	63
3.6.4 Server Setting.....	67
3.6.5 Data Query.....	71
3.6.6 Common Application.....	71
3.7 Administrative.....	83
3.7.1 System.....	83
3.7.2 Password.....	84
3.7.3 Time Setting.....	84
3.7.4 Log Settings.....	85
3.7.5 Backup and Reset.....	86
3.7.6 Firmware Upgrade.....	87
3.7.7 Manual Reboot.....	88
3.7.8 Schedule Reboot.....	88
3.8 Debug.....	89
3.8.1 Data Packet Capture.....	89
3.8.2 Serial Debug.....	89
3.9 Logout.....	91
3.10 FAQ.....	91

1. Introduction

1.1 Overview

The TR323 is a compact industrial 5G/4G IoT router engineered for high-speed, low-latency IoT, M2M and eMBB applications. Powered by Bivocom OS, it supports C/C++, Python (Optional) and Node-RED (Optional) for secondary development.

It features 2 Gigabit Ethernet ports, 1-RS232 debug port and 2-RS485 ports, with optional 2.4 GHz Wi-Fi and GNSS. It seamlessly delivers field data to the cloud via cellular networks and supports MQTT, Modbus RTU/TCP, JSON, plus customizable protocols including BACnet IP/MSTP*, OPC UA*, IEC 101/104/61850*, etc. Equipped with WireGuard, OpenVPN, IPsec, PPTP, L2TP VPN and VXLAN, it provides robust data security and virtual networking. Combined with Bivocom DMP*, it enables centralized remote device management.

Dual-SIM redundancy ensures reliable connectivity for critical industrial projects, while integrated GNSS* supports remote asset tracking.

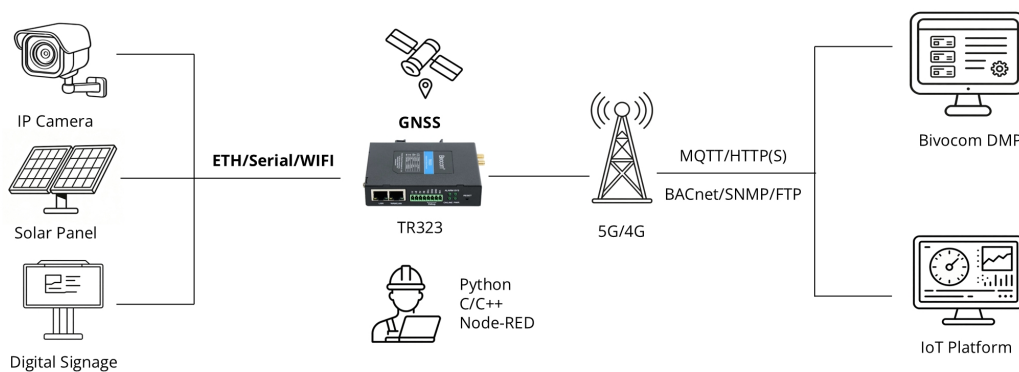


1.2 Applications

The TR323 Series Router uses a cellular network to connect network and serial devices to the management center for remote monitoring and control.

Typical applications are shown below.

Diagram



1.3 Advantages

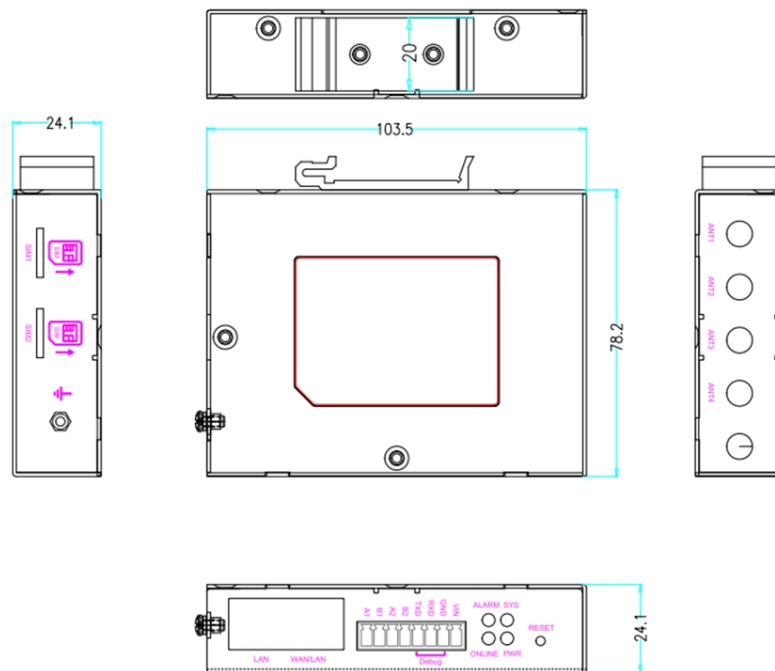
The key advantages of the TR323 Series are as follows:

- **Compact industrial 5G:** a mini 5G/4G router built for high-speed, low-latency IoT, M2M and

eMBB applications

- **Rich connectivity:** 2-RJ45 (GbE), 1-RS232 (debug) and 2-RS485 ports
- **Optional wireless:** 2.4 GHz Wi-Fi for local wireless access and GNSS for remote asset tracking
- **Dual SIM redundancy:** automatic network failover keeps critical links online
- **Secure networking:** WireGuard, OpenVPN, IPsec, PPTP, L2TP VPN and VXLAN protect data in transit
- **Wide protocol support:** MQTT, Modbus RTU/TCP, JSON, BACnet IP/MSTP*, OPC UA* and IEC 101/104/61850*
- **Programmable:** Bivocom OS supports C/C++, Python* and Node-RED*
- **Centralized management:** remote device management through Bivocom DMP*

1.4 Dimensions



1.5 Physical Characteristics

Physical Characteristics	
IP Rating	IP30
Housing & Weight	Metal, 268g (0.59 lbs), without accessories
Dimensions	103.50 x 78.20 x 24.10 mm (4.09 x 3.07 x 0.94 in)
Mounting	DIN-Rail, Desktop

2. Getting Started

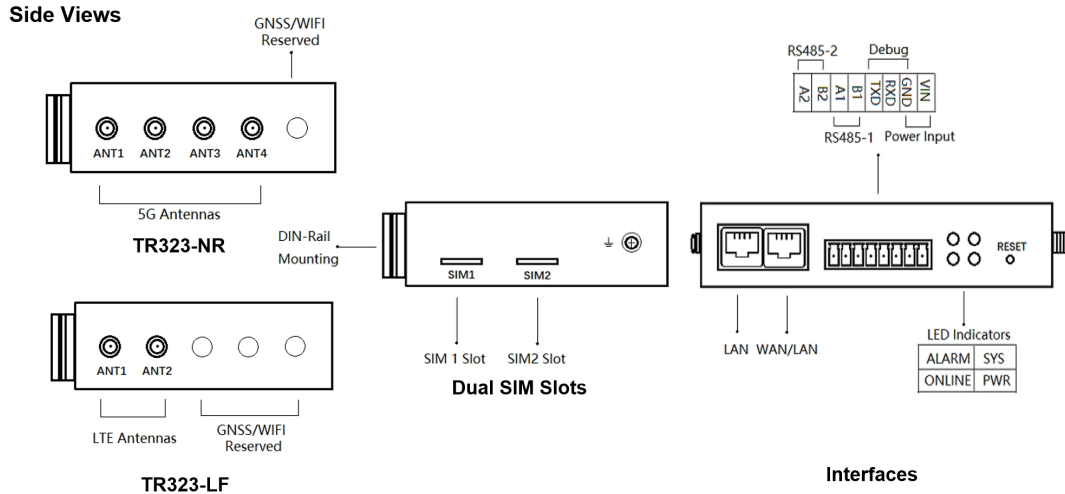
2.1 Package Checklist

- TR323 x 1
- Cellular Antenna x 4 (5G version) * Cellular Antenna x 2 (4G version)*
- DIN-Rail Mounting Kits x 1

- 8-Pin Terminal Block x 1
- Ethernet Cable x 1
- Power Adapter x 1(Optional EU/UK/AU/US/CN Type)

2.2 Installation

The following describes the TR323 ports.



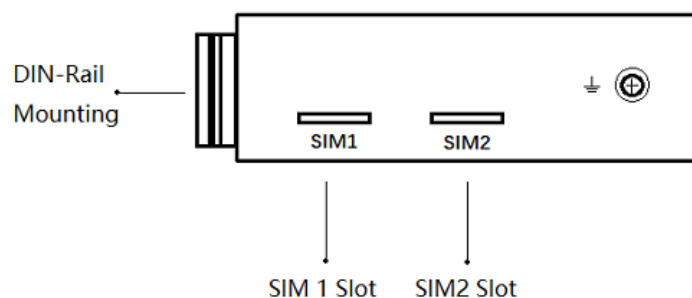
2.2.1 SIM/UIM Card

TR323 supports dual Micro-SIM cards. If a Nano-SIM card is used, a Nano-to-Micro SIM adapter must be employed; such adapters are typically included in the SIM card packaging provided by the mobile network operator.

Before installing the SIM card, power off the router. Orient the SIM card with the contact chip facing downward, align it precisely with the tray's guide rails, and insert it steadily until a distinct tactile and audible click confirms secure engagement. To remove the SIM card, use a standard SIM eject tool (e.g., a dedicated eject pin), insert it fully into the ejection port, apply consistent moderate pressure until a clear click indicates disengagement of the locking mechanism and partial ejection, then gently withdraw the card along its original insertion path.



Warning: DO NOT install SIM/UM card when router is powered on.



2.2.2 Interface Connection

TR323 supports 1 x RS232 (Debug), 2 x RS485. The serial ports can be used for firmware upgrade, system log checking, or as serial ports for data transmission.

The TR323 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 Router
Blue	2(RX)	TX
Brown	3(TX)	RX
Black	5(GND)	GND

RS485 Interface (2xRS485)

Color of Cable	TR323 Router
A (Red)	A1/A2
B (Black)	B1/B2

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 5-35 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 GND.

2.2.4 Cellular Antenna

The TR323 provides 4 for TR323-NR (5G version) and 2 for TR323-LF (4G version), TR323-RC (5G Redcap)cellular antenna ports. Screw the SMA male antennas to TR323 (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 TR323(SMA male port), make sure it is screwed tightly to ensure the strength of signal.

2.3 LED Indicators

TR323 Series Router provides 4xLED indicators, as follows.

Indicator	Status	Content
PWR	On	Powered On

	Off	Powered Off
SYS	Blink	System works
	Off	System doesn't work
ONLINE	On	Router accesses to Internet
	Off	Router doesn't access to Internet
Alarm	On	● SIM/UIM Card is not insert correctly or broken ● Antenna signal is too weak
	1 Blink Per Second	Cellular module was not registered to Router
	2 Blinks Per Second	Router can't access to Internet
	Off	Router doesn't have any alarm

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 TR323 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**

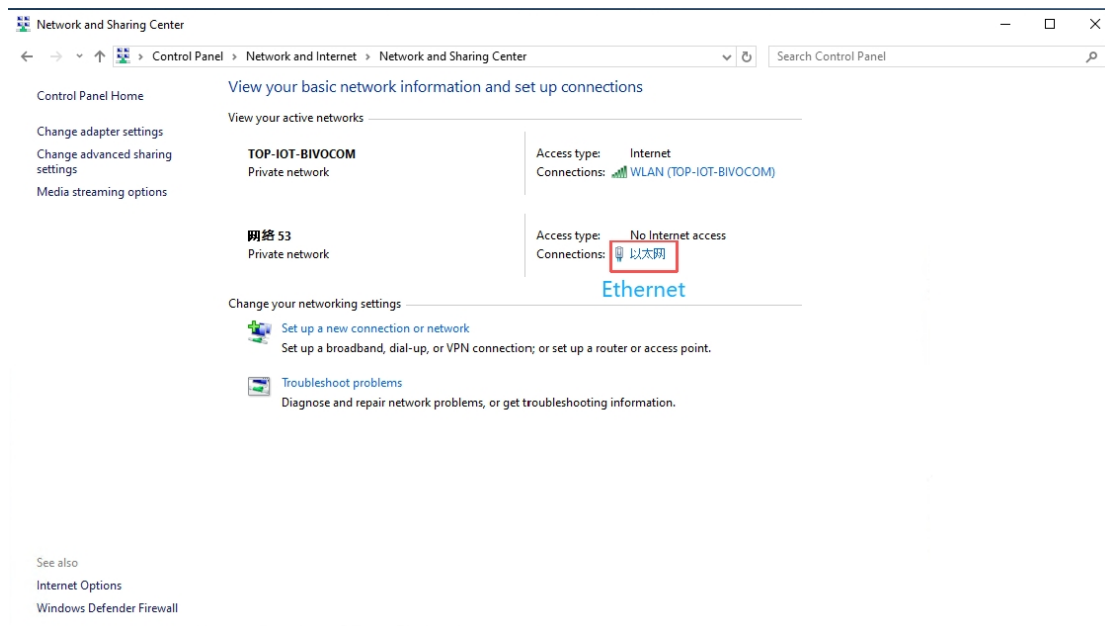
Password: **admin**

IP Address: **192.168.1.1**

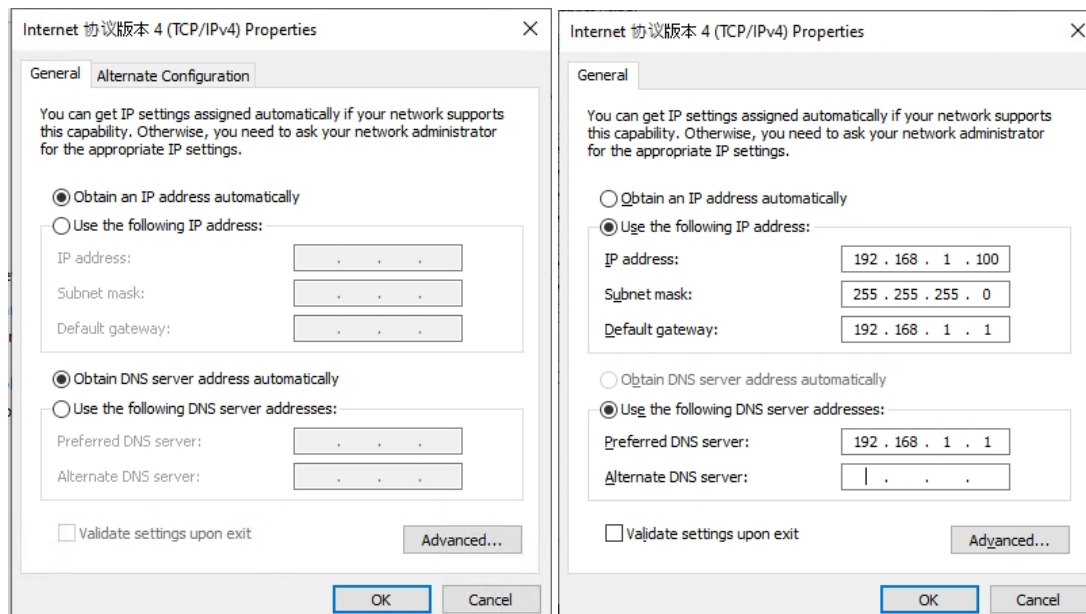
3.0.1 Connect the PC to the TR323 network

1. Using an Ethernet cable, connect one end of the Ethernet cable to the LAN port on TR323 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 TR323.

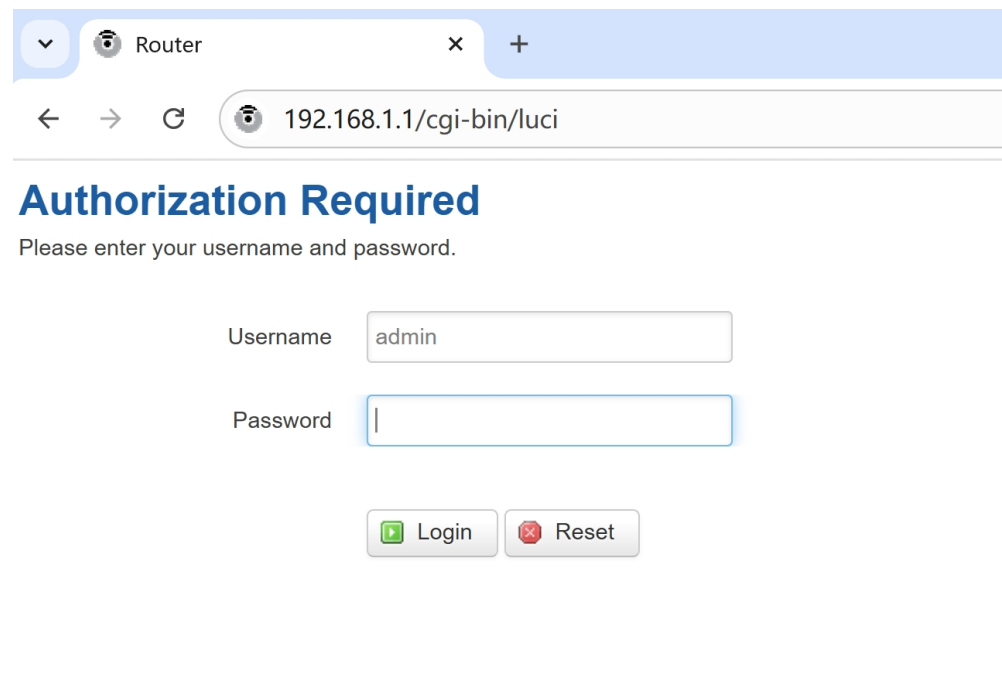


4. Alternatively, connect a laptop to the TR323 Wi-Fi hotspot named "Bivocom_xxxx" and log in with the default password "admin123".

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.



Router

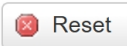
192.168.1.1/cgi-bin/luci

Authorization Required

Please enter your username and password.

Username

Password

 Login  Reset

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 TR323 information like SN, Firmware version, Memory usage, etc.

Status

System

Hostname	router
Model	BIVOCOM323
SN	26051800057
Firmware Version	53.1.0.28
Release Time	2025-08-08 10:54:47
Local Time	2026-09-21 09:56:38 Monday
Uptime	0h 1m 29s
Load Average	0.54, 0.25, 0.10

Memory

Total Available	220180 kB / 253836 kB (86%)
Free	201860 kB / 253836 kB (79%)
Cached	13888 kB / 253836 kB (5%)
Buffered	4432 kB / 253836 kB (1%)

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.

View

System

Network

Routes

System Log

VPN Status

Setup

Secure

VPN

Advanced

Data Collect

Administrate

Logout

Status

Network

IPv4 WAN Status

eth2

Type: dhcp
Address: 172.17.1.228
Netmask: 255.255.0.0
Gateway: 172.17.144.1
Mac Address: 00:52:24:17:2d:3b
DNS 1: 172.17.144.1
Connected: 2h 13m 14s

Online Status

online

Active Connections

80 / 16384 (0%)

LAN Status

IP Address

192.168.1.1

Netmask

255.255.255.0

DHCP Server

Enable

Mac Address

00:52:24:17:2d:3b

Wireless Status

Wireless

Enable

SSID

top-iot_2d3c

Channel

auto

Encryption

wpa2psk-aes

Mac Address

00:0c:43:26:60:40

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
DESKTOP-RKDCFB	192.168.1.204	50:9a:4c:14:19:2a	9h 45m 18s

3.1.3 Routing Tables

Display ARP list and active routing tables.

- View
 - System
 - Network
 - Routes
 - System Log
 - VPN Status
 - Setup
 - Secure
 - VPN
 - Advanced
 - Data Collect
 - Administrative
- Logout

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.1.244	4c:34:88:87:e3:a8	br-lan
192.168.1.10	00:00:00:00:00:00	br-lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
wan	10.191.11.20/30	0.0.0.0	0
lan	192.168.1.0/24	0.0.0.0	0
wan	0.0.0.0/0	10.191.11.22	0

Active IPv6-Routes

Network	Target	IPv6-Gateway	Metric
loopback	0:0:0:0:0:0:0:0	0:0:0:0:0:0:0:0	FFFFFFFF

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.

- View
 - System
 - Network
 - Routes
 - System Log
 - VPN Status
 - Setup
 - Secure
 - VPN
 - Advanced
 - Data Collect
 - Administrative
- Logout

System Log

[Clear Log](#) [Save Log](#) [Refresh Log](#)

```
Mar 16 18:14:46 diald[1297]: AT+CGPADDR*M
Mar 16 18:14:46 diald[1297]: *M +CGPADDR: 1,10.191.11.21*M +CGPADDR: 2,0.0.0.0,0.0.0.0,0.0.0.0,0.0.0.0,0.0.0.0*M +CGPADDR: 3,0.0.0.0*M +CGP
Mar 16 18:14:46 diald[1297]: address is 10.191.11.21
Mar 16 18:14:56 dcd[2981]: Server Address is: 192.168.1.10
Mar 16 18:14:59 dcd[2981]: Failed to connect server 192.168.1.10, port 9001, wait 20s and retry
Mar 16 18:15:00 dcd[2981]: Start to collect data
Mar 16 18:15:00 dcd[2981]: get di data
Mar 16 18:15:00 dcd[2981]: get relay data
Mar 16 18:15:00 dcd[2981]: Start to send collected data [1]
Mar 16 18:15:01 diald[1297]: AT+PSRAT*M
Mar 16 18:15:02 diald[1297]: *M +PSRAT: "CDMA"*M "FDD LTE"*M *M OK*M
Mar 16 18:15:02 diald[1297]: AT+COPS?*M
Mar 16 18:15:02 diald[1297]: *M +COPS: 0,0,"CHN-CT",7*M *M OK*M
Mar 16 18:15:02 diald[1297]: AT+CSQ*M
Mar 16 18:15:02 diald[1297]: *M +CSQ: 26,99*M *M OK*M
Mar 16 18:15:02 diald[1297]: AT+QCRMCALL?*M
Mar 16 18:15:03 diald[1297]: *M +QCRMCALL: 1, V4*M *M OK*M
Mar 16 18:15:03 diald[1297]: AT+CGPADDR*M
Mar 16 18:15:03 diald[1297]: *M +CGPADDR: 1,10.191.11.21*M +CGPADDR: 2,0.0.0.0,0.0.0.0,0.0.0.0,0.0.0.0,0.0.0.0*M +CGPADDR: 3,0.0.0.0*M +CGP
Mar 16 18:15:03 diald[1297]: address is 10.191.11.21
Mar 16 18:15:03 diald[1297]: Server Address collect
```

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.

View

System
Network
Routes
System Log
VPN Status

> Setup
> Secure
> VPN
> Advanced
> Administrative

Logout

VPN

VPN Status

Type: l2tp
IP Address: 1.32.1.3
Netmask: 255.255.255.255
Gateway: 1.32.1.1
Connected Time: 9m,32s

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", "5G" (LTE for 4G version), "Unmanaged" connection types. and the default type is 5G.

> View

> Setup

WAN
LAN
Wireless
Wireless Client
Online Detection
Diagnostics

> Secure

> VPN

> Advanced

> Data Collect

> Administrative

> Debug

Logout

WAN Setting

On this page, you can configure WAN port connection type

WAN Interface

General Settings

Advanced Settings

Connection Type 5G

Network Type AUTO

APN

PIN

User Name

Password

Authentication Type ☒ None ☐ PAP ☐ CHAP ☐ PAP/CHAP

SIM2 APN

SIM2 PIN

SIM2 Username

SIM2 Password

SIM2 Authentication Type ☒ None ☐ PAP ☐ CHAP ☐ PAP/CHAP

Save & Apply

Save

Reset

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.
5G/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

WAN Setting

On this page, you can configure WAN port connection type

WAN Interface

General Settings

Advanced Settings

Clone MAC Address

00:52:24:36:6d:48

MTU

1500

 (64-1500)

WAN Multiplex



Set WAN port as LAN port

3.2.2 LAN

The LAN menu is mainly for configuring IP address of TR323, set the IP address range of DHCP server, or disable DHCP.

1) Common Configuration

Common Configuration

General Setup	Advanced Settings
Protocol	Static address
IPv4 address	192.168.1.1
IPv4 netmask	255.255.255.0
DNS Servers	

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

General Setup		
Ignore interface ☐ ? Disable DHCP for this interface.		
Start	100	? Lowest leased address as offset from the network address.
Limit	150	? Maximum number of leased addresses.
Leasetime	12h	? Expiry time of leased addresses, minimum is 2 minutes (2m).

- **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

General Settings

Advanced Settings

WiFi 2.4G ☒ Enable ☐ Disable

Network Name(SSID)

Channel

Mode

Encryption

Key

Hide SSID ☐

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.

[View](#)
[Setup](#)

WAN
LAN
Wireless
Wireless Client
Online Detection
Diagnostics

[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
[Administrate](#)
[Logout](#)

Save and Apply on page WAN after Join

Enable 2.4G Wireless Client
Apply

Scan WiFi

Scanned WiFi

SSID	Channel	Encryption	Signal	
TOP-IOT-D	1	WPA1PSKWPA2PSK/TKIPAES	100	Join
Cozy	1	WPA1PSKWPA2PSK/TKIPAES	100	Join
CMCC-xrxN	1	WPA1PSKWPA2PSK/TKIPAES	100	Join
3b38	3	WPA2PSK/AES	70	Join

3.2.5 Online Detection

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

Online Detection

Online Detection ☒ Enable ☐ Disable

Detection Type

Primary Detection Server

Second Detection Server

Retry Times

Retry Interval  Seconds

Enable Reboot ☒ Enable ☐ Disable

Reboot After Interval  Minutes

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 router 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 router 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 router is online or not. While nslookup is used to analyze a domain.

Diagnostics

Network Utilities

```

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=106 time=315.715 ms
64 bytes from 8.8.8.8: seq=1 ttl=106 time=314.506 ms
64 bytes from 8.8.8.8: seq=2 ttl=106 time=301.739 ms
64 bytes from 8.8.8.8: seq=3 ttl=106 time=303.761 ms
64 bytes from 8.8.8.8: seq=4 ttl=106 time=311.802 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 301.739/309.504/315.715 ms
  
```

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.

DMZ

Set DMZ Host

DMZ ☒ Enable ☐ Disable

Source zone ☐ vpn: (empty) ☒ wan: wan: 

DMZ Host 192.168.1.100

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.

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable
myPLC	IPv4-TCP, UDP From <i>any host</i> in <i>wan</i> Via <i>any router IP</i> at port <i>501</i>	IP <i>192.168.1.244</i> , port <i>501</i> in <i>lan</i>	☒

 Edit  Delete

New port forward:

Name	Protocol	External zone	External port	Internal IP address	Internal port
New port forward	TCP+UDP	wan			

 Add

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 router. For example, to allow remote access to the router configuration page, open port 80.

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable
enable80	Any TCP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> at port <i>80</i> on <i>this device</i>	Accept input	☒

Open ports on router:

Name	Protocol	External zone	External port
New input rule	TCP+UDP	wan	

Add

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

Add and edit

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

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

Add and edit

Click Add and Edit to access more detailed matching conditions.

Rule is enabled Disable

Name

Restrict to address family

Protocol

Match ICMP type

Source zone

☐ Any zone

☒ lan: lan: 

☐ wan: wan: 

Source MAC address

Source address

Source port

Destination zone

☐ Device (input)

☐ Any zone (forward)

☐ lan: lan: 

☒ wan: wan: 

Destination address

Destination port

Action

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.

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	
HTTP	IPv4-TCP, UDP From <i>any host</i> in <i>wan</i> Via <i>any router IP</i> at port 2000	IP 192.168.1.1, port 80 in <i>lan</i>	☒	Edit Delete
SSH	IPv4-TCP, UDP From <i>any host</i> in <i>wan</i> Via <i>any router IP</i> at port 2022	IP 192.168.1.1, port 22 in <i>lan</i>	☒	Edit Delete
TELNET	IPv4-TCP, UDP From <i>any host</i> in <i>wan</i> Via <i>any router IP</i> at port 2023	IP 192.168.1.1, port 23 in <i>lan</i>	☒	Edit Delete

New port forward:

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

2. Click **Add > Save & Apply** button.
3. Go to **Administrate > System** page, enable SSH and telnet access.

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

> Administrate

System

Password

Time Setting

Log Setting

Backup and Restore

Firmware Upgrade

FTP Upgrade

Remote Configured

Manual Reboot

Schedule Reboot

> Debug

Logout

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Hostname	router
Timezone	(GMT+08:00) Beijing, Chongqing
Language	English
SMS Verify Password	admin
Web Access Method	HTTP Need Reboot When Changed
Enable telnet access	☒ Enable ☐ Disable
Enable SSH access	☒ Enable ☐ Disable

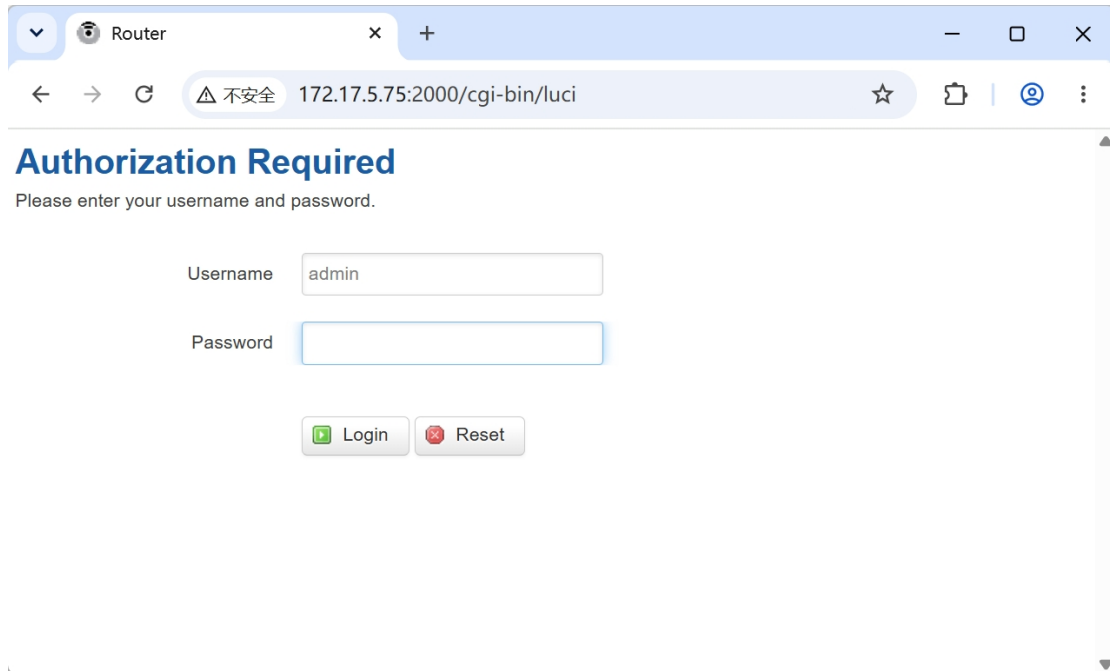
Save & Apply

Save

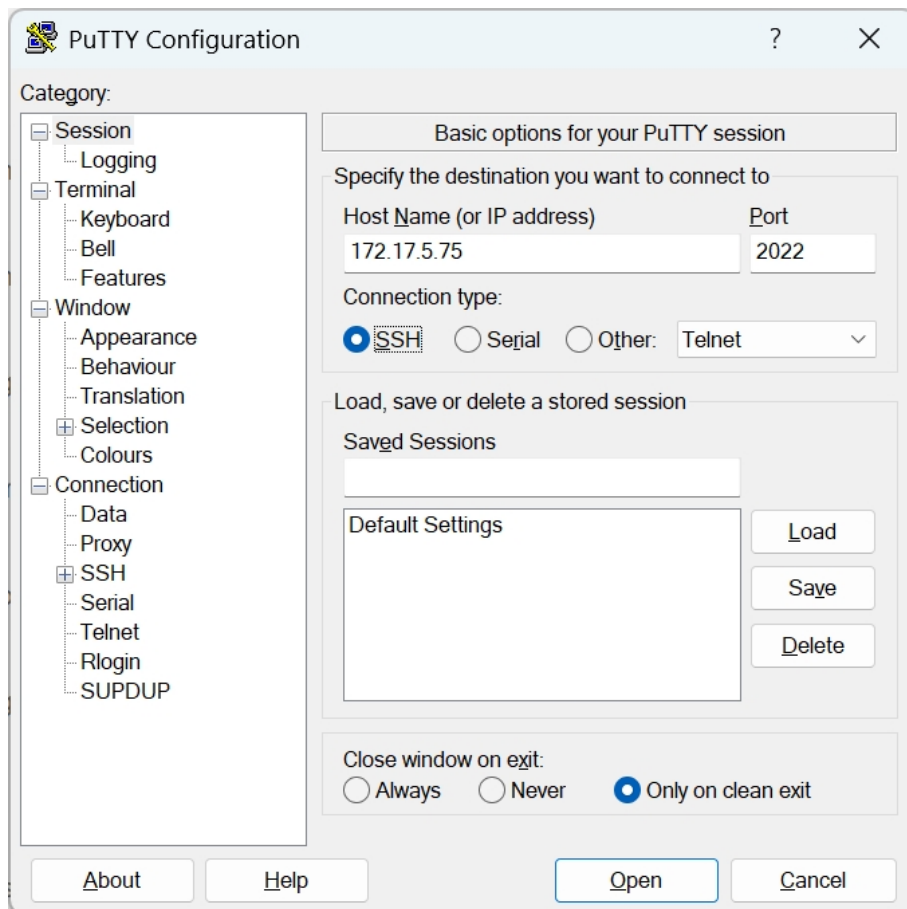
Reset

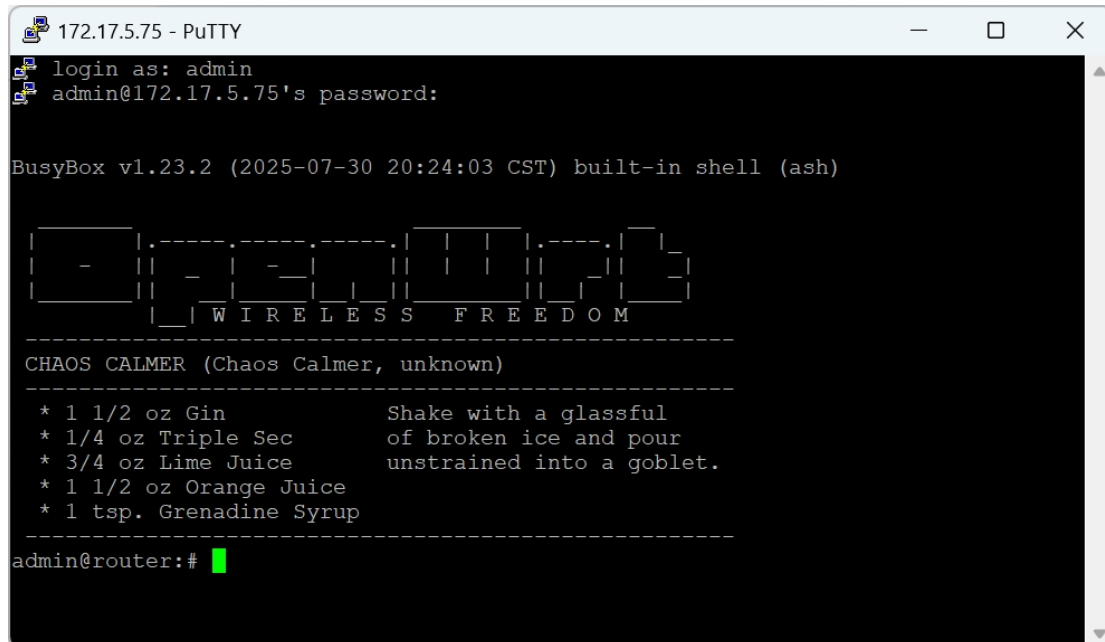
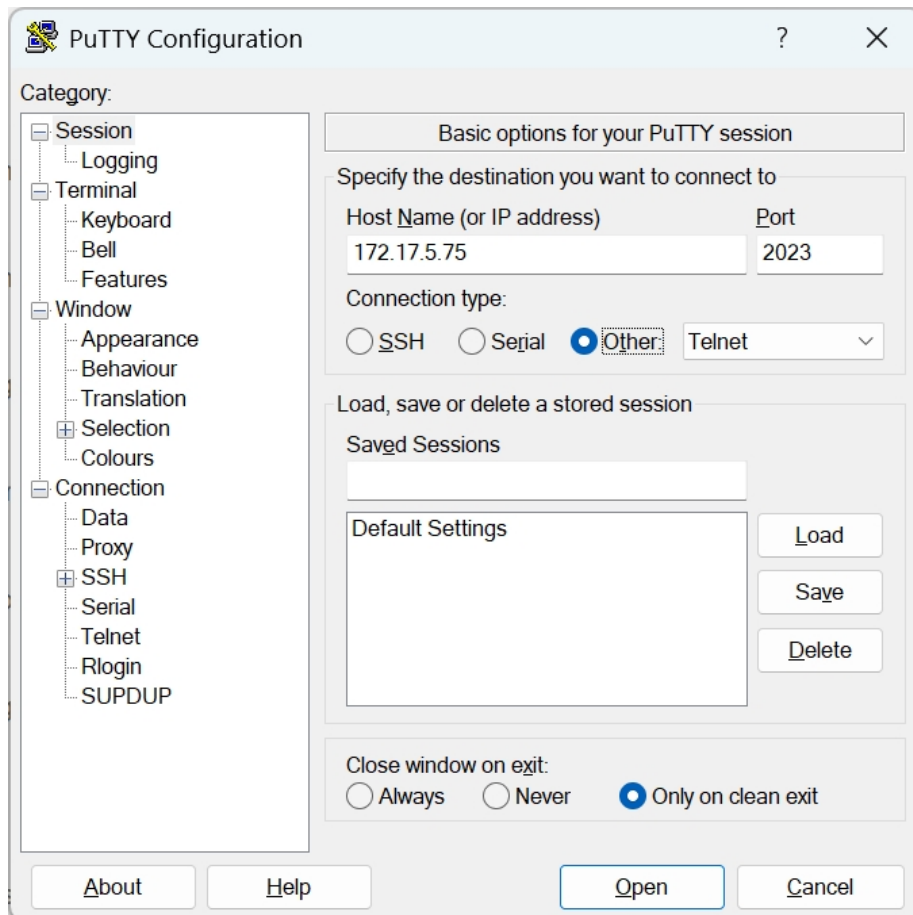
Verification Method:

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.

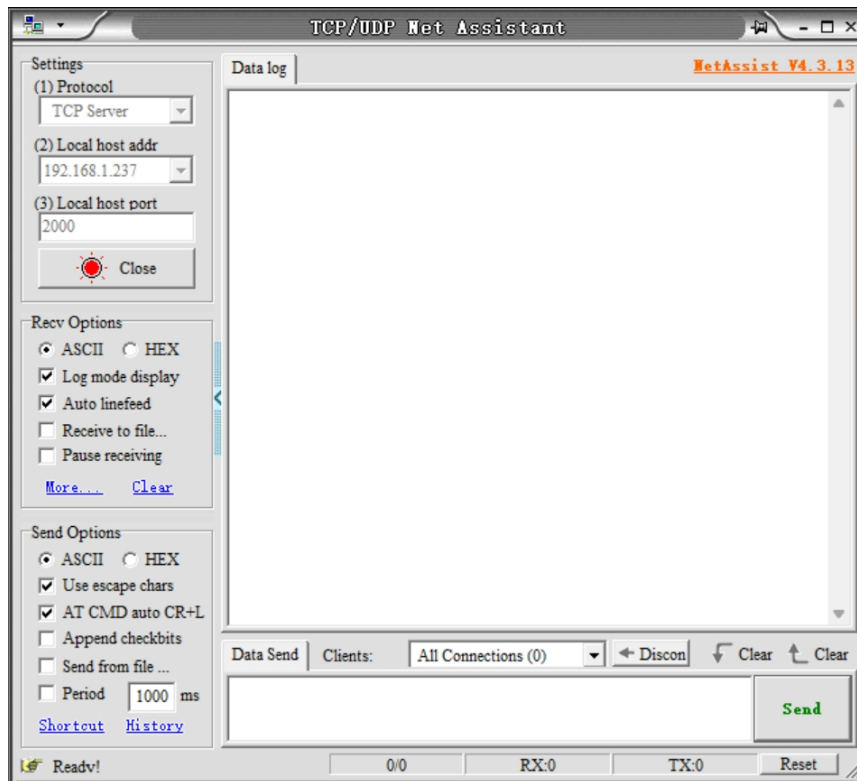




Scenario 2: Remote Access Internal Device

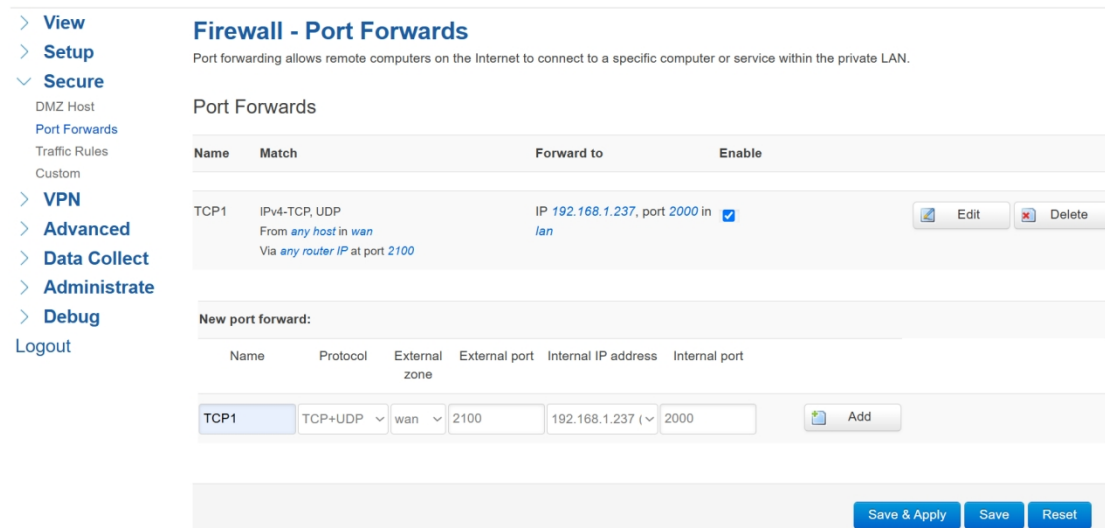
Objective: Remote access LAN devices through WAN IP address

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:

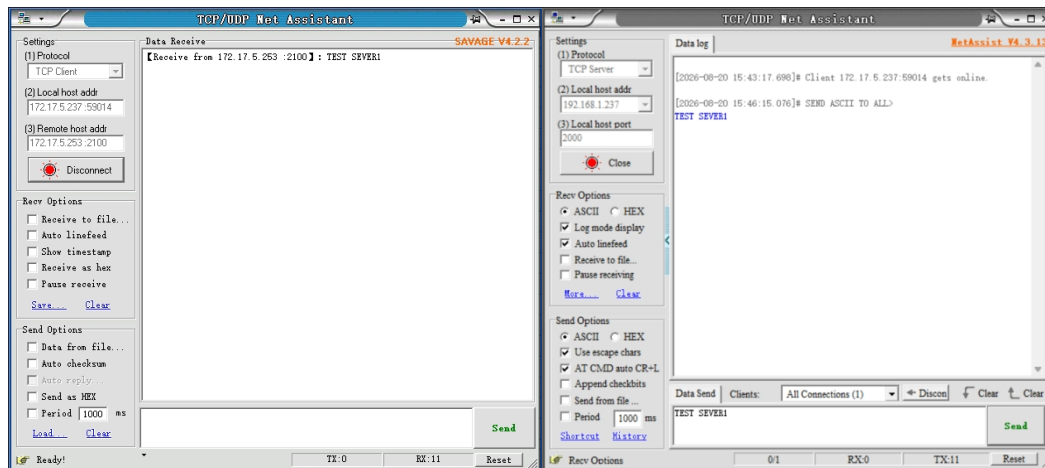
1. Go to **Secure > Port Forwards** page to input the **External Port** (2100) of WAN IP (172.17.5.253) to the **Internal Port** (2000) of LAN IP (192.168.1.237) address.



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.

TR323 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 ☒ Enable ☐ Disable

Server Address

User Name

Password 

Remote Subnet

Remote Subnet Mask

NAT ☒

Enable MPPE Encryption ☒

Enable Static Tunnel IP Address ☐

Default Gateway ☐  All Traffic Will Passthrough Via VPN

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 Router	Click Default Gateway to establish a default route under ppp0; all data then uses this route.

2) PPTP Server

PPTP Server ☒ Enable ☐ Disable

Server Local IP

IP Address Range

Enable MPPE Encryption ☒

DNS1

DNS2

WIN1

WIN2

CHAP Secrets

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 Setting

Setting L2TP

L2TP Client	☒ Enable ☐ Disable
Server Address	192.168.10.10
User Name	admin@10.10.10.10
Password	12345678 
Tunnel Name	TBS
Tunnel Password	12345678 
Enable IPsec	☒
Pre Shared Key	12345678 
Right ID	
Enable Self Defined IKE	☒
IKE Encryption Algorithm	AES-256
IKE Integrity Algorithm	MD5
Diffie-Hellman Group	Group5(1536bits)
Enable Self Defined ESP	☒
ESP Encryption Algorithm	3DES
ESP Integrity Algorithm	SHA-1
Remote Subnet	10.184.0.0  eg: 192.168.10.0
Remote Subnet Mask	255.255.240.0  eg: 255.255.255.0
NAT	☒
Enable MPPE Encryption	☒
MTU	1450  600~1450
Enable Static Tunnel IP Address	☐
Default Gateway	☐  All Traffic Will Passthrough Via VPN
Enable Ping	☐  Reconnect When Fails to Ping

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 Router	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

IP Address Range  eg: 10.10.10.100-10.10.10.200

Enable MPPE Encryption ☒

Enable IPsec ☒

Pre Shared Key 

NAT ☐

CHAP Secrets  eg: test * test *

< >

Client Subnet  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

Negotiation Method

Tunnel Type

Local Subnet

Peer Subnet

IKE Encryption Algorithm

IKE Integrity Algorithm

Diffie-Hellman Group

IKE Life Time

Authentication Type

Pre-shared Key

Local Identifier

Peer Identifier

ESP Encryption Algorithm

ESP Integrity Algorithm

DPD Timeout  seconds

DPD Detection Period  seconds

DPD Action

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 (router-to-router), Site-to-Host (router-to-client), Host-to-Site (client-to-router), 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 TR323 provides auto mode and manual mode for configuration file uploading.

OpenVPN

Set OpenVPN Parameters

OpenVPN ☒ Enable ☐ Disable

Mode

File 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

Cipher Algorithm

MTU

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.

> View

> Setup

> Secure

> VPN

PPTP

L2TP

IPSec

OpenVPN

GRE

> Advanced

> Data Collect

> Administrate

GRE

GRE Configs

Interface Name eg: gre1	Peer WAN IP	Peer Tunnel IP	Peer Subnet eg:192.168.1.0/24	Local Tunnel IP	
					Delete

Add

Save & Apply Save Reset

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.

> View

> Setup

> Secure

> VPN

PPTP

L2TP

IPSec

OpenVPN

XFRP Client

> Advanced

> Data Collect

> Administrate

> Debug

Logout

XFRP Client

Enable XFRP
☒ Enabled
☐ Disabled

XFRP Server Address

XFRP Server Port

This section contains no values yet

Add

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

TR323 provides a window for sending text messages to certain numbers with configurable contents.

Send Short Message

Phone Number

Please Input The Content

Send

Reset

3.5.2 Static Routes

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

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric
	Host-IP or Network	if target is a network		
lan		255.255.255.2		0
Delete				

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 Net Flow

The traffic meter of the TR323 collects traffic statistics for the WAN port and provides a traffic overflow alarm. Traffic statistics are retained when the router is powered off, and counting resumes from the last recorded value the next time the router is powered on.

Net Flow

Traffic Meter

Current Day Flow	Current Month Flow
0.0G	0.0G

Net Flow

Net Flow ☒ Enable ☐ Disable

Limit Enabled ☐ [Effective for LTE or 3G](#)

Clear Day Flow [Clear Day Flow](#)

Clear Month Flow [Clear Month Flow](#)

[Save & Apply](#)[Save](#)[Reset](#)

3.5.4 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.

- > View
- > Setup
- > Secure
- > VPN
- > **Advanced**

Send SMS
Static Routes
DI DO
Oray
Net Flow
GPS Location
BS Location
Dynamic DNS
SNMP
DHCP and DNS

- > **Data Collect**
- > **Administrate**
- > **Debug**
- Logout

GPS Location

GPS Location ☒ Enable ☐ Disable

GPS Source ☒ External ☐ Dongle ☐ N303-5Q

Output Mode [Output To Network](#)

Server Address [192.168.1.100](#)

Server Port [9010](#)

Report Mode [Pure TCP](#)

User Defined Register Packet [Max 128 Bytes ASCII](#)

User Defined Heartbeat Packet [Max 128 Bytes ASCII](#)

Report Interval [60](#) [Seconds](#)

Heartbeat Interval [30](#) [Seconds](#)

GPS Info -

Connection Status -

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 router location, default value is 60 seconds.
Heartbeat Interval	Set the interval for client to send heart beat packet to server after router 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, TR323 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).

[View](#)
[Setup](#)
[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
[Administrate](#)
[Debug](#)
[Logout](#)

Location

Location ☒ Enable ☐ Disable

Signal Source ☒ External ☐ Dongle

External Model

Output Mode

Server Address

Server Port

Report Mode

User Defined Register Packet [?](#) Max 128 Bytes ASCII

User Defined Heartbeat Packet [?](#) Max 128 Bytes ASCII

Report Interval [?](#) Seconds

Heartbeat Interval [?](#) Seconds

Location Info

Connection Status

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.

[View](#)
[Setup](#)
[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
[Administrate](#)
[Debug](#)
[Logout](#)

Interface Setting

COM1/RS485 COM2/RS485 COM3/RS232

Enabled ☐ Enable ☒ Disable

TCP Device Setting

TCP Device1 TCP Device2 TCP Device3 TCP Device4 TCP Device5

Enabled ☐ Enable ☒ Disable

GPS Device

Must Enable GPS On Page Advanced/GPS Location First

GPS ☒ Enable ☐ Disable

Factor Name [?](#) Longitude and Latitude

Alias Name

Reporting Center [?](#) eg:1-2-3-4-5

[Save & Apply](#)
[Save](#)
[Reset](#)

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.

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

> Administrate

> Debug

Logout

Server Setting

Server1 Settings

Server2 Settings

Server3 Settings

Server4 Settings

Server5 Settings

Enabled ☒ Enable ☐ Disable

Protocol

Encapsulation Type

Server Address

Server Port

Heartbeat Interval Seconds, 0 means Default Heartbeat

MQTT Public Topic

MQTT Subscribe Topic

MQTT Username

MQTT Password

Client ID

Enable TLS/SSL ☐

Enable Self Defined Variable ☐

Connection Status **CONNECTED**

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 router and subscribe topic on other devices are the same.

3.5.5 Dynamic DNS

If the public IP address assigned to the router 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 router, no matter how often the IP address changes.

DDNS ☒ Enable ☐ Disable

Service Type

User Name

User Password 

Host Name

- **Service Type**

The router 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.

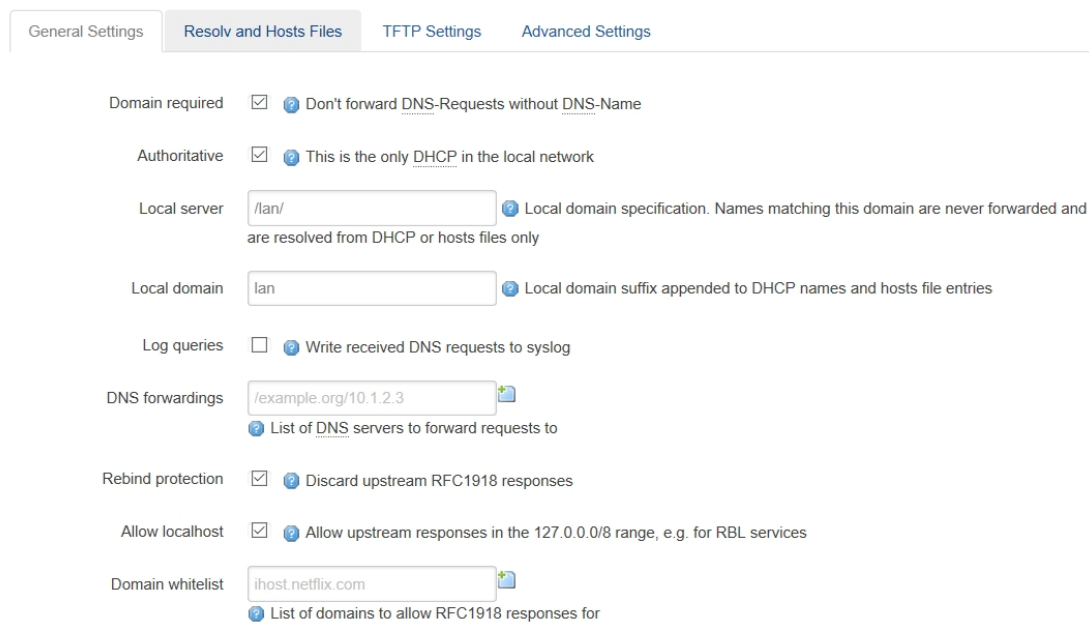
3.5.6 DHCP and DNS

The TR323 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.

DHCP and DNS

Dnsmasq is a combined [DHCP-Server](#) and [DNS-Forwarder](#) for [NAT](#) firewalls

Server Settings



Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
----------	--------------	-------------	---------------------

Collecting data...

Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configuration where only hosts with a corresponding lease are served.

Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
----------	-------------	--------------	-------------------

This section contains no values yet

 Add

Save & Apply Save Reset

3.6 Data Collect

Data Collect settings are for TR323 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.

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Basic Setting

Data Collect ☒ Enable ☐ Disable

Collect Period  Seconds

Report Period  Seconds

Enable Cache ☒  Cache History Data

Cache Days  day

Cache Path  Path Where Data Is Stored

Send Minute Data ☐

Send Hour Data ☐

Send Day Data ☐

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~COM2), Modbus TCP base on Ethernet LAN, GPS Device.

Serial Ports Setting (2xRS485)

Interface Setting

COM1/RS485

COM2/RS485

Enabled ☒ Enable ☐ Disable

Baudrate 9600

Databit 8

Stopbit 1

Parity None

Frame Interval 200 ms

COM Protocol Modbus RTU

Command Interval 1 ms

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 Device Setting

TCP Device1
TCP Device2
TCP Device3
TCP Device4
TCP Device5

Enabled
☒ Enable
☐ Disable

IP Address

Port

Frame Interval
 ms

COM Protocol
Modbus TCP

Command Interval
 ms

Connection Status
CONNECTED

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

Must Enable GPS On Page Advanced/GPS Location First

GPS ☒ Enable ☐ Disable

Factor Name [?](#) Longitude and Latitude

Alias Name

Reporting Center [?](#) eg:1-2-3-4-5

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 TR323 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

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

IO Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Modbus Rules Setting

Modbus Rules

Configure import and export

Order	Device ID	Interface	Factor Name	Device Num	Function Code	Start Address	Count	Data Type	Reporting Center	Enable	
H1	1	COM1	Temp	1	3	1	1	unsigned 11 1 6Bits AB		☒	Edit Delete

New Modbus Rule

Order	Device ID	Interface	Factor Name	Device Num	Function Code	Start Address	Count	Data Type	Reporting Center
		COM1		0~255	0~255	addr[byte]	1~120	Unsigned 16Bits	1-2-3-4-5

Add

Save & Apply

Save

Reset

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

[View](#)
[Setup](#)
[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
 Basic Setting
 Interface Setting
Modbus Rules Setting
 IO Setting
 Server Setting
 Data query
[Administrative](#)
[Debug](#)
 Logout

Modbus Rules Setting

Modbus Rules

Configure import and export

Order	Device ID	Interface	Factor Name	Device Num	Function Code	Start Address	Count	Data Type	Reporting Center	Enable	
H1	1	COM1	Temp	1	3	1	1	unsigned 11 6Bits AB		☒	Edit Delete

New Modbus Rule

Order	Device ID	Interface	Factor Name	Device Num	Function Code	Start Address	Count	Data Type	Reporting Center	
		COM1		0~255	0~255	addr[byte]	1~120	Unsigned 16Bits	1-2-3-4-5	Add

[Save & Apply](#)
[Save](#)
[Reset](#)

[View](#)
[Setup](#)
[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
 Basic Setting
 Interface Setting
Modbus Rules Setting
 IO Setting
 Server Setting
 Data query
[Administrative](#)
[Debug](#)
 Logout

Modbus configuration import / export

Export modbus configuration: [Export configuration](#)

Import modbus configuration: [选择文件](#) 未选择任何文件 [Import configuration](#)

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, router 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)

- > View
- > Setup
- > Secure
- > VPN
- > Advanced
- ▼ Data Collect
 - Basic Setting
 - Interface Setting
 - Modbus Rules Setting
 - IO Setting
 - Server Setting
 - Data query
- > Administrate
- > Debug
- Logout

Modbus Rules - Gen_HGM - COM1

enabled Disable

Order

Device ID Device Unique Identifier

Device Name

Belonged Interface

Factor Name Multiple Factors Are Separated By Semicolon

Alias Name Multiple Aliases Are Separated By Semicolon

Device Num 0~255

Function Code 0~255

Reply Timeout ms

Report Type 0~4

limitA

limitB

Start Address addr or addr.byte or addr.bit

Count 1~120

Data Type

Reporting Center Multiple Servers Are Separated By Minus

Unit Multiple Units Are Separated By Semicolon

Operator 0 + - * /

Accuracy 0~6

Enable Webshow ☒ After checking, you can query the collected data of the configuration item on the web page

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 (router) 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 ($\leq A$) , Greater Equal Than B ($\geq B$) , 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 Server Setting

The Server settings menu allows users to set the data-center address with multiple protocols, the standard TR323 support TCP, UDP, HTTP (s), MQTT (s), TCP Server and Modbus TCP (slave). For the data format, TR323 support different Encapsulation type, include "Transparent", "Json", and "HJ212" (special for some Environment SCADA).

MQTT Broker (Server)

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

IO Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Server Setting

Server1 Settings
Server2 Settings
Server3 Settings
Server4 Settings
Server5 Settings

Enabled ☒ Enable ☐ Disable

Protocol MQTT

Encapsulation Type JSON

Server Address cloud.top-iot.net

Server Port 65535

Heartbeat Interval Seconds, 0 means Default Heartbeat

MQTT Public Topic /sys/2077917031

MQTT Subscribe Topic /sys/2077917031

MQTT Username admin

MQTT Password

Client ID client01

Enable TLS/SSL ☐

Enable Self Defined Variable ☐

Connection Status CONNECTED

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 router 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

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

IO Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Server Setting

Server1 Settings

Server2 Settings

Server3 Settings

Server4 Settings

Server5 Settings

Enabled ☒ Enable ☐ Disable

Protocol

Encapsulation Type

Server Address

Server Port

User Defined Register Packet Max 128 Bytes

Use HEX Format ☐ Default is ASCII

User Defined Heartbeat Packet Max 128 Bytes

Use HEX Format ☐ Default is ASCII

Heartbeat Interval Seconds, 0 means No Heartbeat

Enable Self Defined Variable ☐

Connection Status

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 router 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

View

System
Network
Routes
System Log
VPN Status

> Setup

> Secure

> VPN

> Advanced

> Data Collect

> Administrative

> Debug

Logout

Server Setting

Server1 Settings

Server2 Settings

Server3 Settings

Server4 Settings

Server5 Settings

Enabled ☒ Enable ☐ Disable

Protocol HTTP

Encapsulation Type JSON

Http URL http://test.com/post

Server Port 6310

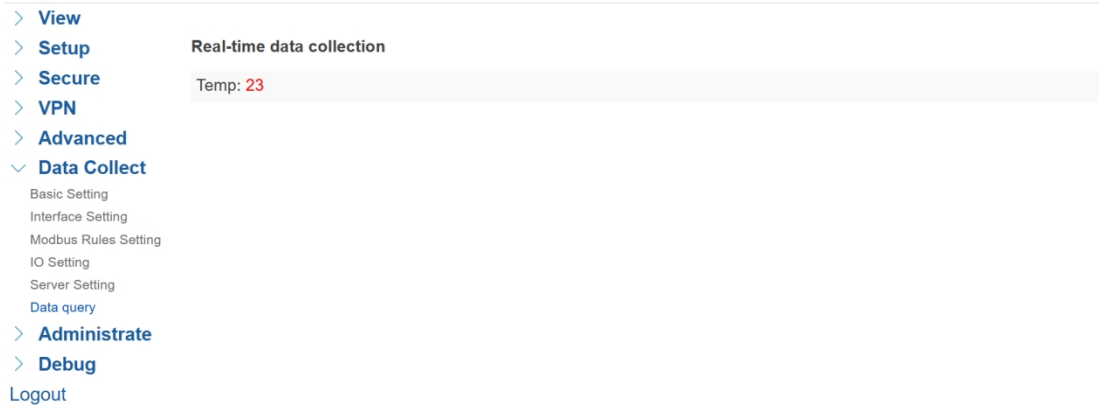
Enable Self Defined Variable ☐

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

3.6.5 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 "-".



3.6.6 Common Application

Scenario 4: Send Modbus data to MQTT

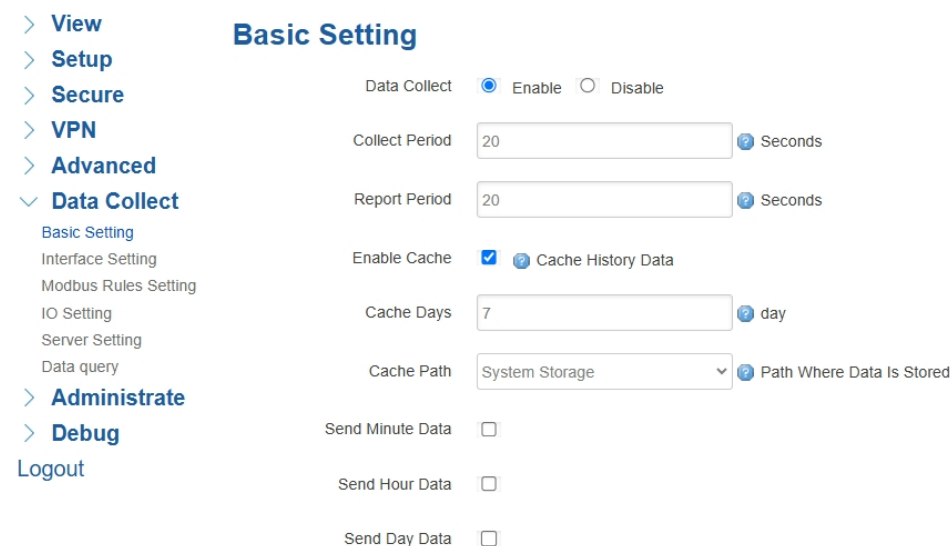
Objective: Get Modbus sensors' data and publish to MQTT broker.

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 router, responsible for collecting on-site sensor/device Modbus data and transmitting MQTT messages.

Configuration Steps:

- 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.



- 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.

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

IO Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Interface Setting

COM1/RS485_1
COM2/RS485_2
COM3/RS485_3
COM4/RS232_2
COM5/RS232_2

Enabled
☒ Enable
☐ Disable

Baudrate
9600

Databit
8

Stopbit
1

Parity
None

Frame Interval
35
ms

COM Protocol
Modbus RTU

Command Interval
1
ms

TCP Device Setting

TCP Device1
TCP Device2
TCP Device3
TCP Device4
TCP Device5

Enabled
☒ Enable
☐ Disable

IP Address
192.168.1.237

Port
9010

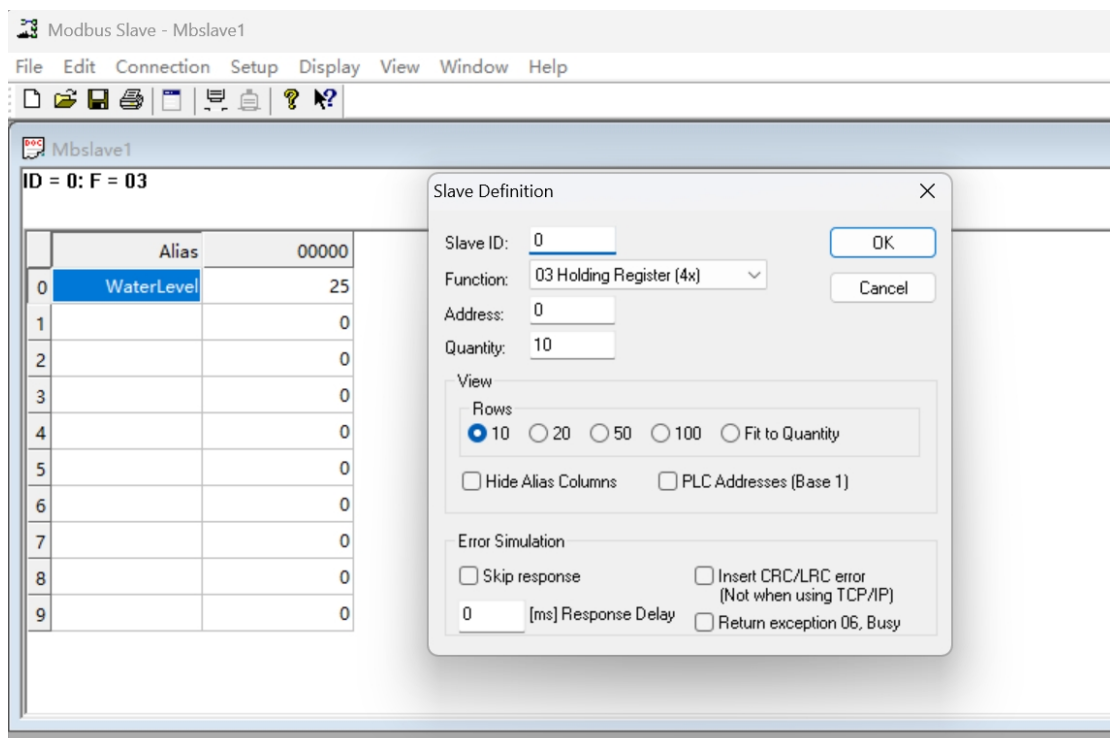
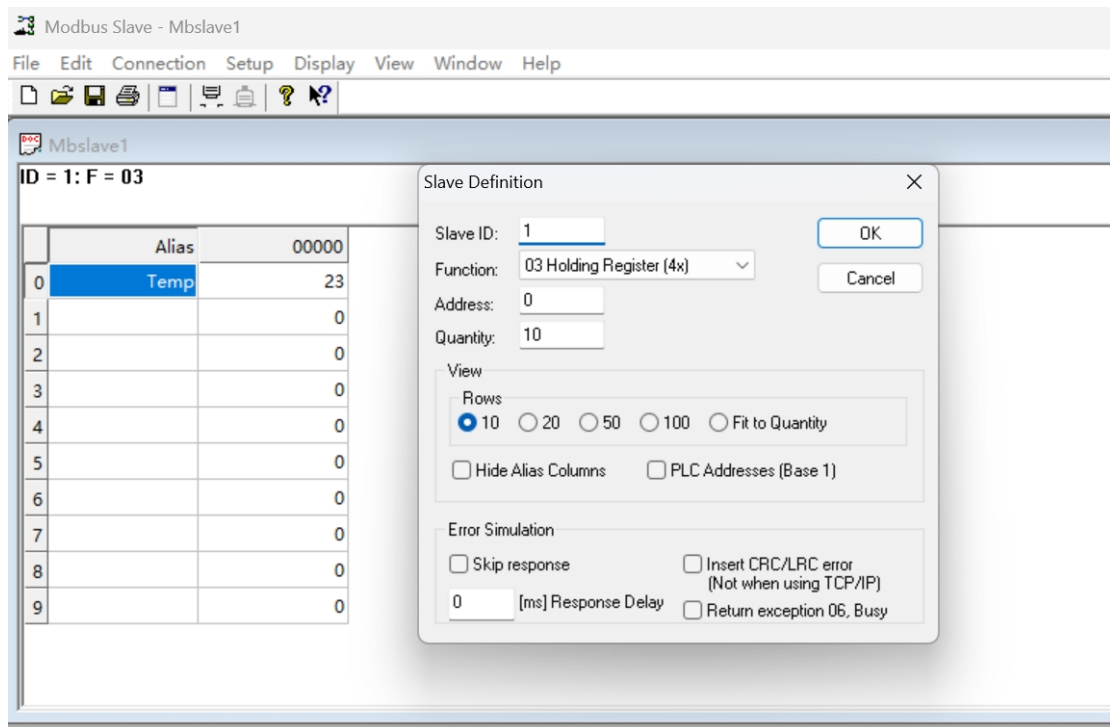
Frame Interval
10
ms

COM Protocol
Modbus TCP

Command Interval
1
ms

Connection Status
CONNECTED

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



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

[View](#)
[Setup](#)
[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
[Basic Setting](#)
[Interface Setting](#)
[Modbus Rules Setting](#)
[IO Setting](#)
[Server Setting](#)
[Data query](#)
[Administrate](#)
[Debug](#)
[Logout](#)

Modbus Rules Setting

Modbus Rules

[Configure import and export](#)

Order	Device ID	Interface	Factor Name	Device Num	Function Code	Start Address	Count	Data Type	Reporting Center	Enable	
H1	1	TCP1	Temp	1	3	1	1	unsigned 1 1 6Bits AB		☒	Edit Delete
H2	2	COM4	WaterLevel	0	3	1	1	unsigned 1 1 6Bits AB		☒	Edit Delete

New Modbus Rule

Order	Device ID	Interface	Factor Name	Device Num	Function Code	Start Address	Count	Data Type	Reporting Center
		COM4		0~255	0~255	addr[,byte[	1~120	Unsigned 16Bits	1-2-3-4-5

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

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

[View](#)
[Setup](#)
[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
[Basic Setting](#)
[Interface Setting](#)
[Modbus Rules Setting](#)
[IO Setting](#)
[Server Setting](#)
[Data query](#)
[Administrate](#)
[Debug](#)
[Logout](#)

Real-time data collection

WaterLevel: **25** Temp: **23**

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.

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

IO Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Server Setting

Server1 Settings

Server2 Settings

Server3 Settings

Server4 Settings

Server5 Settings

Enabled ☒ Enable ☐ Disable

Protocol

MQTT

Encapsulation Type

JSON

Server Address

broker.emqx.io

Server Port

1883

Heartbeat Interval

Seconds, 0 means Default Heartbeat

MQTT Public Topic

BivocomPub

MQTT Subscribe Topic

BivocomSub

MQTT Username

MQTT Password

Client ID

client0101

Enable TLS/SSL ☐

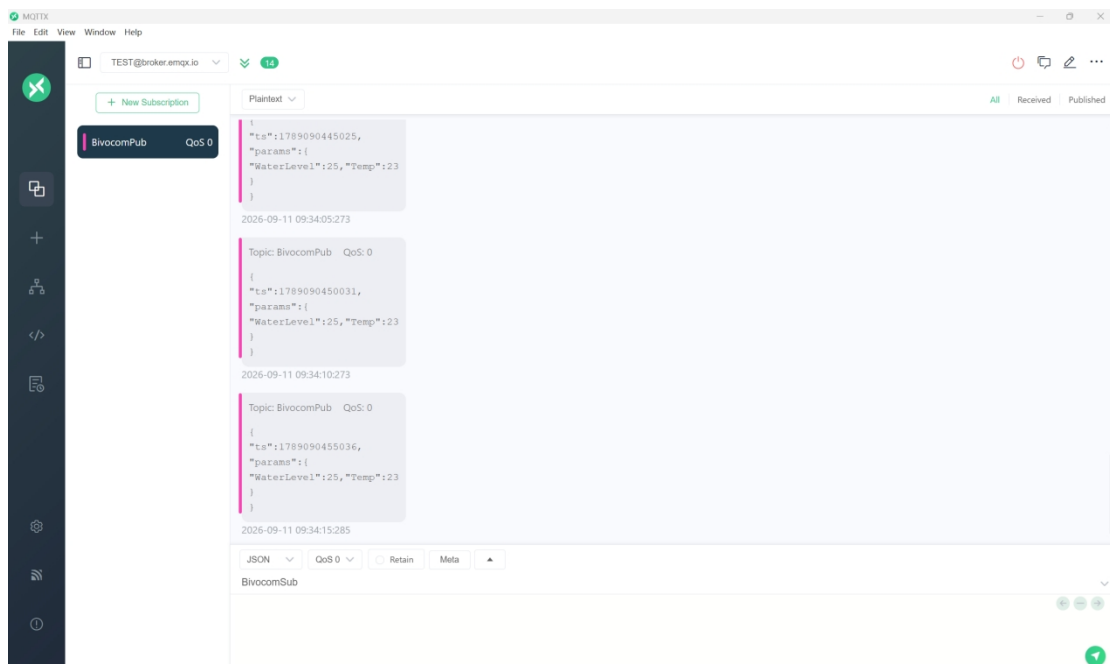
Enable Self Defined Variable ☐

Connection Status

CONNECTED

Verification Method:

1. Open MQTT client software (e.g. MQTXX) 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:

The screenshot displays the Bivocom router's web management interface. On the left, a sidebar menu includes options like View, Setup, Secure, VPN, Advanced, Data Collect, Administrate, and Debug. The main content area is divided into two sections: 'Status' and 'Diagnostics'.

Status Section:

- Network:** IPv4 WAN Status is shown. The interface type is 'dhcp' on 'eth0.2'. The IP address is 172.17.5.224, with a netmask of 255.255.255.0, gateway of 172.17.5.254, and MAC address 00:52:24:4e:10:f4. DNS 1 is 223.6.6.6, and it has been connected for 7h 55m 57s.
- Online Status:** A red box highlights the word 'online'.
- Active Connections:** A progress bar shows 51 / 16384 (0%).

Diagnostics Section:

- Network Utilities:** Includes input fields for IP addresses (8.8.8.8) and a website (www.google.com), with buttons for Ping, Traceroute, and Nslookup.
- Ping Results:** A terminal-style output shows a successful ping to 8.8.8.8 with 56 data bytes and response times around 168ms. Statistics indicate 5 packets transmitted and received with 0% packet loss.

Scenario 5: 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.

Relay Setting

Device Name	Device ID	Relay Channel	Factor Name	Reporting Center	Relay Control	Enable	
R1	01	relay1	Relay1	1	Open	☒	Edit Delete
R2	02	relay2	Relay2	1	Open	☒	Edit Delete

New Relay Channel:

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

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

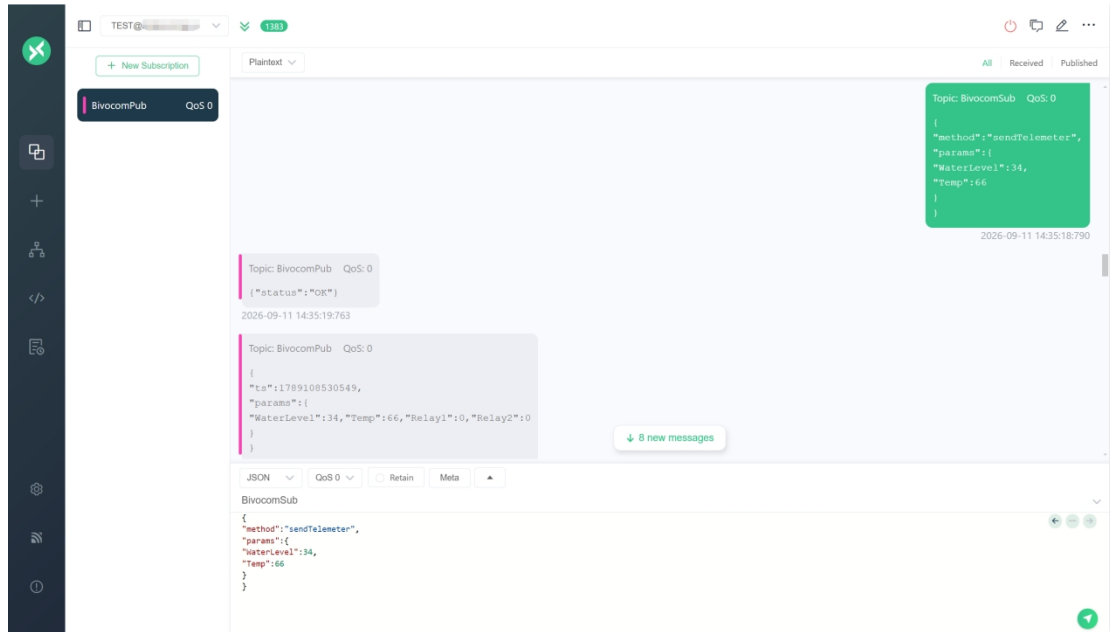
[View](#)
[Setup](#)
[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
[Basic Setting](#)
[Interface Setting](#)
[Modbus Rules Setting](#)
[IO Setting](#)
[Server Setting](#)
[Data query](#)
[Administrate](#)
[Debug](#)
[Logout](#)

Real-time data collection

WaterLevel: 25	Temp: 23	Relay1: 0	Relay2: 0
----------------	----------	-----------	-----------

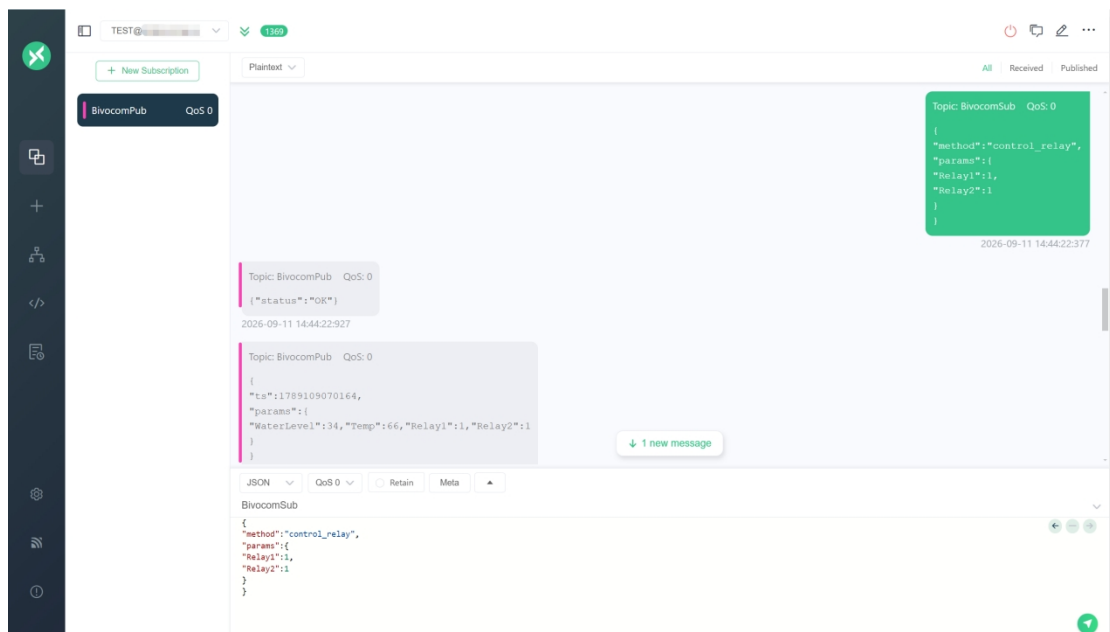
4. Connect same MQTT broker by PC, add **New Subscription** Topic (BivocomPub) the same as Bivocom router published, send controlling commands to the publish topic (BivocomSub) the same as Bivocom router subscribes. The **Factor Name** of Modbus data will be the key of controlling, device will reply 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 6: 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.

The screenshot shows the 'Basic Setting' page for 'Data Collect'. On the left is a navigation menu with options: View, Setup, Secure, VPN, Advanced, Data Collect (selected), Administrate, Debug, and Logout. Under 'Data Collect', there are sub-options: Basic Setting (selected), Interface Setting, Modbus Rules Setting, IO Setting, Server Setting, and Data query. The main content area has the following settings: 'Data Collect' is set to 'Enable' (radio button selected); 'Collect Period' is set to '5' seconds; 'Report Period' is set to '5' seconds; and 'Enable Cache' is set to 'Cache History Data' (checkbox selected). At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

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.

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

IO Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Interface Setting

COM1/RS485_1COM2/RS485_2COM3/RS485_3COM4/RS232_2COM5/RS232_2

Enabled ☒ Enable ☐ Disable

Baudrate 9600

Databit 8

Stopbit 1

Parity None

Frame Interval 35 ms

COM Protocol Transparent

Reporting Center 1-2 eg:1-2-3-4-5

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.

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

IO Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Server Setting

Server1 SettingsServer2 SettingsServer3 SettingsServer4 SettingsServer5 Settings

Enabled ☒ Enable ☐ Disable

Protocol MQTT

Encapsulation Type Transparent

Server Address bro

Server Port 1883

Heartbeat Interval Seconds, 0 means Default Heartbeat

MQTT Public Topic BivocomPub

MQTT Subscribe Topic BivocomSub

MQTT Username

MQTT Password

Client ID client0101

Enable TLS/SSL ☐

Connection Status CONNECTED

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

Basic Setting

Interface Setting

Modbus Rules Setting

IO Setting

Server Setting

Data query

> Administrate

> Debug

Logout

Server Setting

Server1 Settings

Server2 Settings

Server3 Settings

Server4 Settings

Server5 Settings

Enabled ☒ Enable ☐ Disable

Protocol

TCP

Encapsulation Type

Transparent

Server Address

172.17.5

Server Port

9000

User Defined Register Packet

Max 128 Bytes

Use HEX Format ☐

Default is ASCII

User Defined Heartbeat Packet

Max 128 Bytes

Use HEX Format ☐

Default is ASCII

Heartbeat Interval

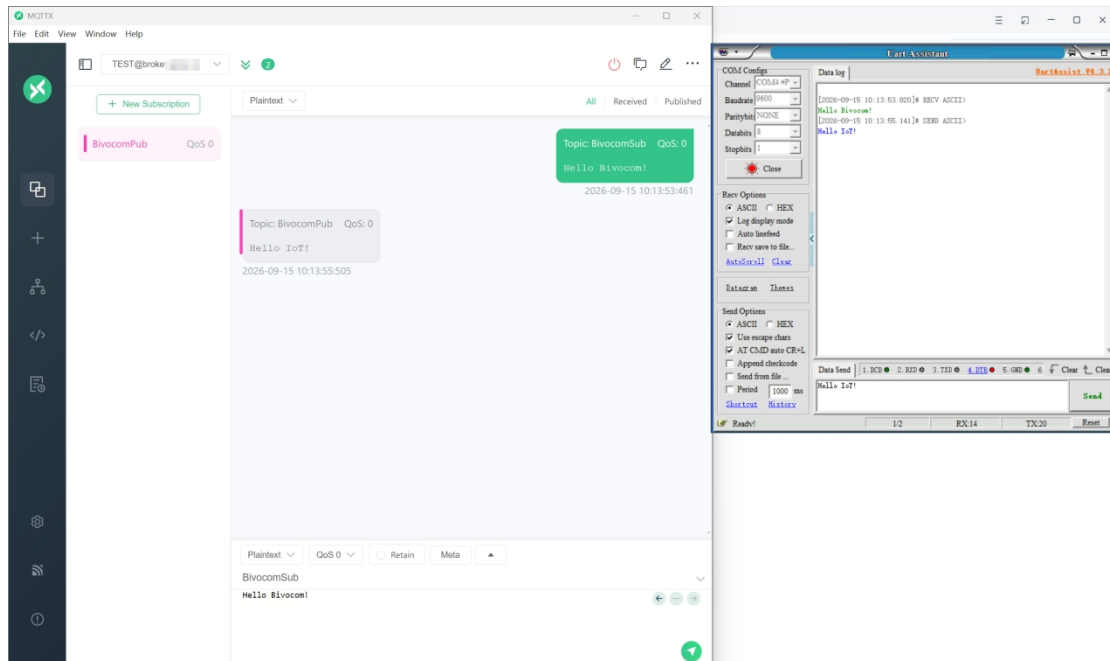
Seconds, 0 means No Heartbeat

Connection Status

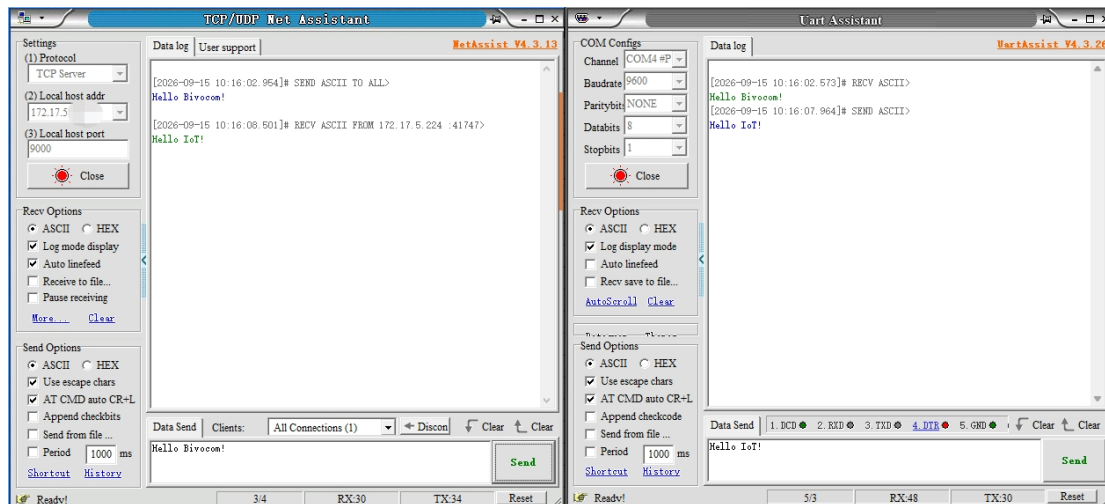
CONNECTED

- 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

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Hostname	router
Timezone	(GMT+08:00) Beijing, Chongqing
Language	English
Web Access Method	HTTP ? Need Reboot When Changed
Enable telnet access	☒ Enable ☐ Disable
Enable SSH access	☐ Enable ☒ Disable

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.
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 router.

Admin Password

Change the password of the system administrator (User `root`)

Origin Password		
Password		
Confirmation		

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 router is powered off, while for NTP, router will connect to NTP server which requires internet connection, time won't be saved once powered off. But NTP will be more accurate than RTC, and you may need to adjust the time manually if it is not accurate.

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

> Administrate

System

Password

Time Setting

Log Setting

Backup and Restore

Firmware Upgrade

Remote Configured

Manual Reboot

Schedule Reboot

> Debug

Logout

Set System Time

Current system time 2026-09-14 10:10:20

System Time Type ☒ ntp ☐ rtc

NTP Time Server

Port

Update Interval  seconds

Sync to RTC ☒

> View

> Setup

> Secure

> VPN

> Advanced

> Data Collect

> Administrate

System

Password

Time Setting

Log Setting

Backup and Restore

Firmware Upgrade

Remote Configured

Manual Reboot

Schedule Reboot

> Debug

Logout

Set System Time

Current system time 2026-09-14 10:10:20

System Time Type ☐ ntp ☒ rtc

Current RTC Time Mon Sep 14 10:10:20 2026

RTC Date  eg: 2016-01-01

RTC Time  eg: 12:00:00

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.

Output To Device

Log Size KB

Log Server

Log Server Port

Output Level

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 router as a .gz file, or reset all settings to factory defaults.

Backup / Restore

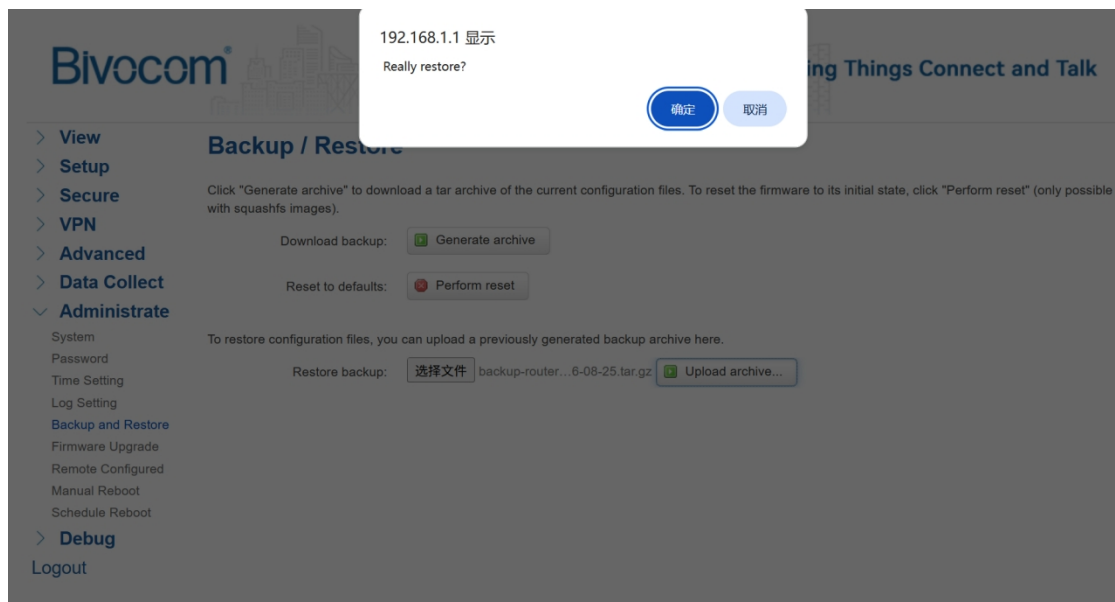
Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:

Reset to defaults:

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

Restore backup: 未选择文件。



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

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.

Flash operations

Flash new firmware image

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

Image: 未选择文件。

1) Choose and Upload Firmware Image

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

Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.

Click "Proceed" below to start the flash procedure.

Checksum: `f68983dbe5ec7f0d4bf9258e421ad53d`

Size: 9.00 MB

Configuration files will be kept.

- **Checksum**

MD5 checksum value of firmware.

- **Size**

The size of firmware.

- **Proceed**

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

3.7.7 Manual Reboot

Reboot

Reboots the operating system of your device

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

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

3.7.8 Schedule Reboot

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

Schedule Reboot

Enable Schedule Reboot ☒ Enable ☐ Disable

Schedule Type ☒ By Period ☐ By Time

Period Interval  Minutes, Min 5

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.

- > View
- > Setup
- > Secure
- > VPN
- > Advanced
- > Data Collect
- > Administrate
- > Debug
 - Data Packet Capture
 - Serial Debug

[Logout](#)

Data Packet Capture

general

Interface	Package Number	Host(IP Address)	Port	Protocol
eth0	1000	192.168.1.1	80	tcp all tcp udp icmp ip arp rarp ether

capture done!

capture will be stopped when filesize greater than 10,000,000 bytes(less 10MB)
please click stop button before downloading the file to ensure that all data is written to the file

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.

- > View
- > Setup
- > Secure
- > VPN
- > Advanced
- > Data Collect
- > Administrate
- > Debug
 - Data Packet Capture
 - Serial Debug
- Logout

Serial Debug

COM Setting

Interface	Baudrate	Databit	Stopbit	Parity	Frame Interval(ms)	Send Format	Receive Format
COM1	9600	8	1	None	200	ASCII	ASCII

```

<----->
2026-09-14 14:32:14
send 4 bytes to COM1
send data(ascii):test
read 0 bytes from COM1
<----->
2026-09-14 14:32:18
send 4 bytes to COM1
send data(ascii):test
read 0 bytes from COM1
          
```

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?

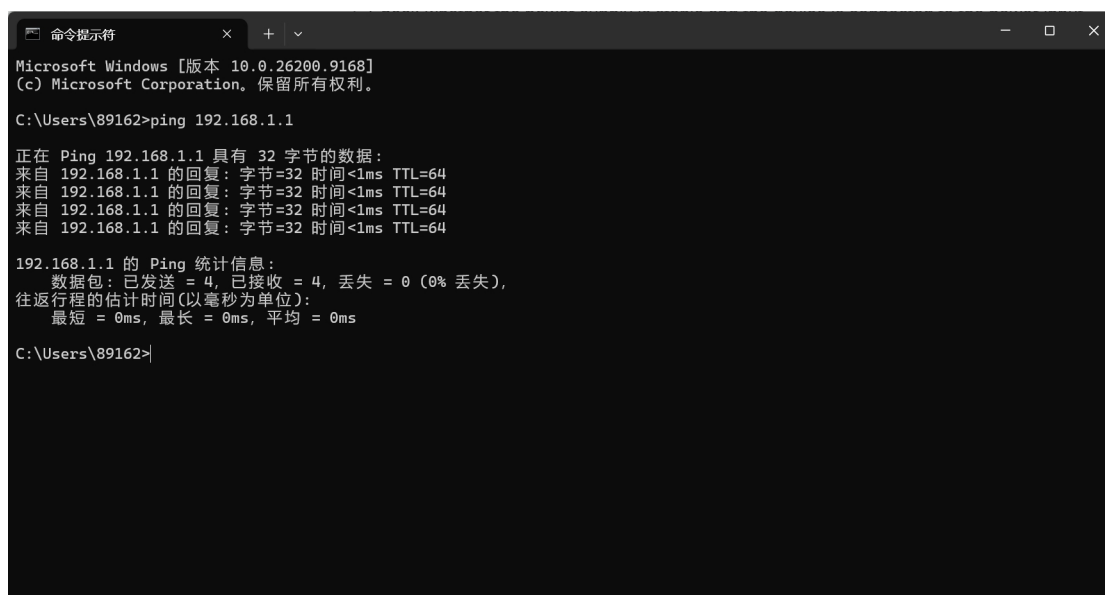
1. Check whether the SIM card is inserted into the correct slot and whether the cellular antennas are installed correctly.
2. Ensure the **WAN Connection Type** is set correctly (e.g., LTE), and the **APN** settings and **Username/Password** are configured as required by your SIM card provider.
3. Check 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).



```
命令提示符
Microsoft Windows [版本 10.0.26200.9168]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\89162>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\89162>
```

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.