



Industrial 5G/4G IoT Gateway TG453 Series User Guide



Note: interfaces of hardware for different models (5G and 4G version, GNSS) will be different.

Copyright

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

Trademark

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

Disclaimer

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

Global Technical & Sales Support

Bivocom

Xiamen Bivocom Technologies Co., Ltd.

Addr: Unit 1402-2, No. 39, Xixi Shanwei Road, Software Park #3,
Xiamen, China

Tel.: +86 158 8026 2905

Fax: +86 592 6211727

Email: support@bivocom.com

sales@bivocom.com

www.bivocom.com

About This Guide

Thank you for choosing Bivocom Industrial 5G/4G LTE IoT Gateway TG453 Series.

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

This manual is compatible with below models

Model	Description
TG453-NR	Industrial 5G IoT Gateway
TG453-LF	Industrial 4G LTE IoT Gateway

Note: please contact Bivocom team to choose the version of hardware you need for your IoT application, as different interfaces on hardware will have different part number, such as, dual sim, with/without GPS/GNSS, etc.

Table of Contents

Copyright	2
Trademark	2
Disclaimer	2
About This Guide	3
Table of Contents	4
1. Introduction	6
1.1 Overview	6
1.3 Dimensions:	7
1.4 Physical Characteristics	7
2. Getting Started	7
2.1 Package Checklist	7
2.2 Installation	8
2.2.1 Insert SIM/UIM Card	8
2.2.2 Interfaces connection	9
2.2.3 Power Supply	12
2.2.4 Cellular Antenna	12
2.2.5 WIFI Antenna	13
2.3 LED Indicators	13
3. Configuration and Management	14
3.1 View	14
3.1.1 System	14
3.1.2 Network	15
3.1.3 Routes	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	22
3.2.4 Online Detection	25
3.2.5 Diagnostics	26
3.3 Secure	28
3.3.1 DMZ Host	28
3.3.2 Port Forwarding	29
3.3.3 Traffic Rules	29
3.3.4 Custom	32
3.4 VPN	32
3.4.1 PPTP	32
3.4.2 L2TP	35

3.4.3 IPsec	37
3.4.3 OpenVPN	39
3.5 Advanced	40
3.5.1 Static Routing	40
3.5.2 Net Flow	40
3.5.3 GPS Location(Optional)	41
3.5.4 DHCP and DNS	42
3.6 Data Collect	42
3.6.1 Basic Setting	42
3.6.2 Interface Setting	42
3.6.3 Modbus Rules Setting	43
3.6.4 Server Setting	45
3.7 Administrate	45
3.7.1 System	46
3.7.2 Password	46
3.7.3 Time Setting	47
3.7.4 Log Settings	48
3.7.5 Backup and Restore	49
3.7.6 Router Upgrade	50
3.7.7 Remote Configured	51
3.7.8 Manual Reboot	53
3.7.9 Schedule Reboot	53
3.8 Logout	54

1. Introduction

1.1 Overview

The TG453 is a compact 5G NR IoT gateway designed for IoT, M2M, and eMBB applications requiring higher speed, lower latency data transmission, and capacity of basic edge computing. It provides OpenWRT based Linux OS embedded environment that allows developers and engineers to program and install their own application based on Python, C/C++ to the hardware themselves.

The TG453 gateway has 5-Gigabit ethernet ports, 1-RS232, 2-RS485 to connect to diverse field equipment and sensors, transferring the data to the cloud server via 5G/4G LTE cellular network. It comes with industrial protocols, such as MQTT, Modbus RTU/TCP, JSON, TCP/UDP and VPN to provide you an efficient and secure IoT data connectivity between field devices and cloud server. The TG453 gateway has option of dual sim/dual module for failover/load balance, providing robust and reliable wireless and wired connectivity for your mission-critical industrial applications, such as EV charging station, solar power, smart pole, smart cities, smart office, smart buildings, smart traffic light, digital signage advertising, vending machines, ATM, etc.

TG453 Series IoT Gateways utilizes cellular network to connect your edge devices and controller devices to your center for remote monitoring and control. Typical application as below.



Image 1: Diagram of TG453 Applications

1.3 Dimensions:

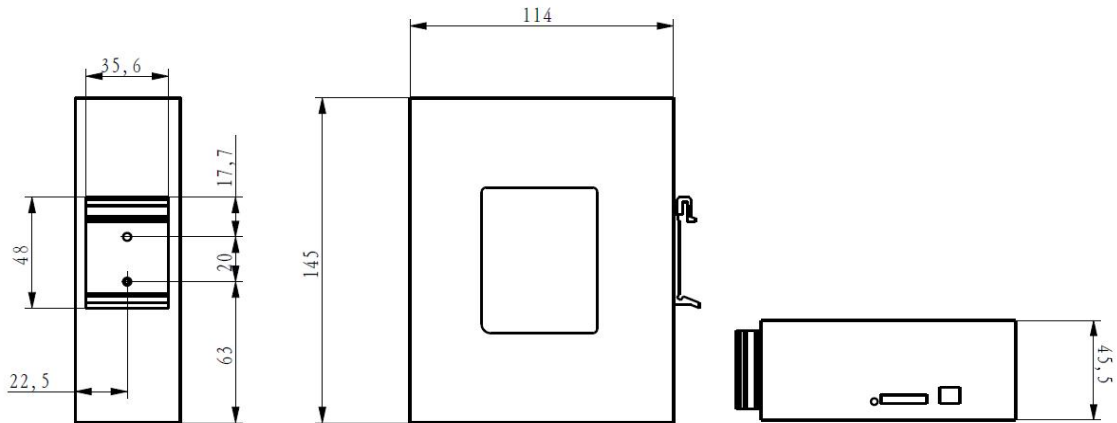


Image 2: dimensions of TG453 of different side views

1.4 Physical Characteristics

Physical Characteristics	
Housing	Metal, IP30
Dimensions	145 x 114 x 45mm (5.71 x 4.49 x 1.77in), Antenna and other accessories are not included
Weight	630g(1.39lbs), without accessories

2. Getting Started

2.1 Package Checklist

The following components are included in your standard TG453 package.

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

1. TG453 Gateway 1PCS
2. Power Adapter 1PCS
(DC 12V/1.5A, EU/US/UK/AU plug optional)
3. Cellular Antenna
5G version: 4PCS
4G version: 2PCS
4. WIFI Antenna 2PCS
5. RS232 Cable 1PCS
(DB9 Female, 1 meter)
6. Ethernet Cable(1 meter) 1PCS

- 7. 8-Pin Terminal Block 1PCS
- 8. 2-Pin Terminal Block 1PCS
- 9. DIN-Rail Mount Kits 1PCS

2.2 Installation

2.2.1 Insert SIM/UIM Card

TG453 supports normal SIM/UIM only, so if you're using a Micro SIM or Nano SIM card, you will have to use a Micro SIM or Nano SIM to Normal SIM adapter, which normally comes with your SIM card package.

Before you insert the SIM card, make sure your router is powered off, then use a needle object(such as a pen) to push the button near the SIM tray(see page below), it will flick out immediately. Put the SIM card to SIM tray with chipset upside, insert it to router and make sure it's tightly matched.

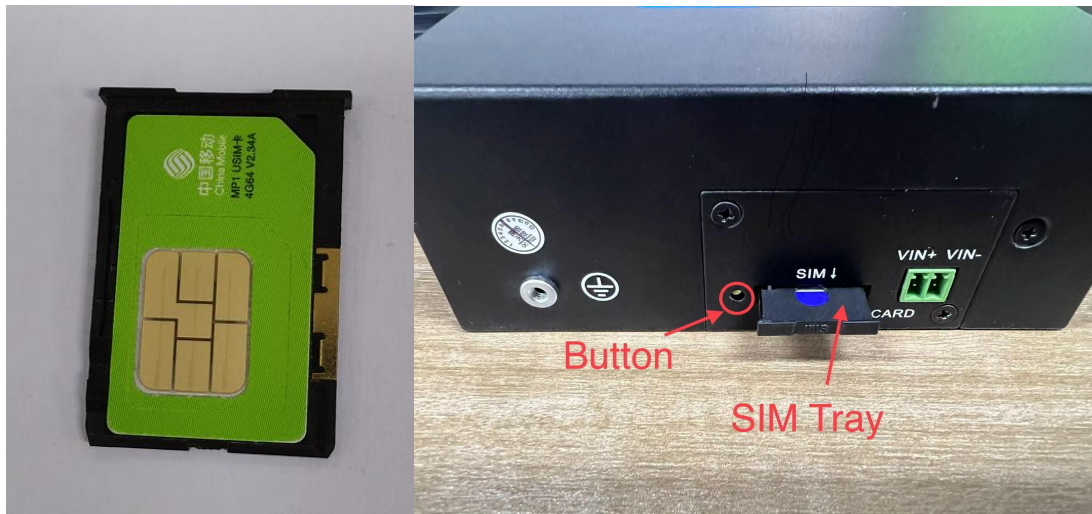


Image 3: SIM card and SIM tray installation

Warning: DON NOT install and swap SIM/UIM card when router is powered on.

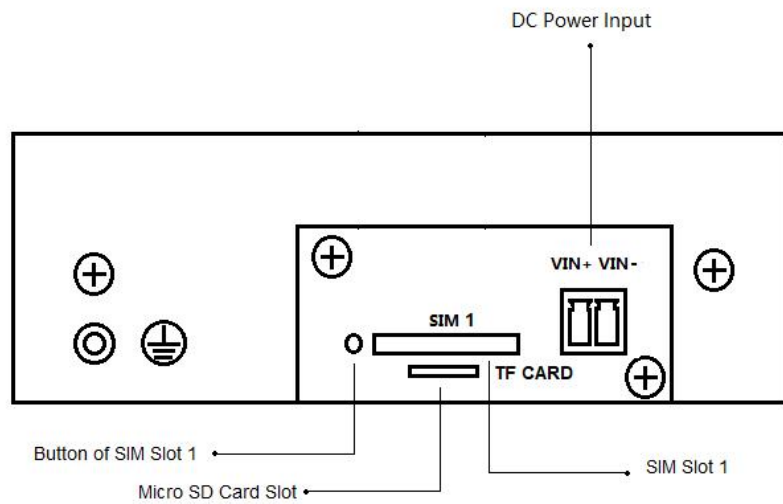


Image 4: Side view of TG453 with single SIM

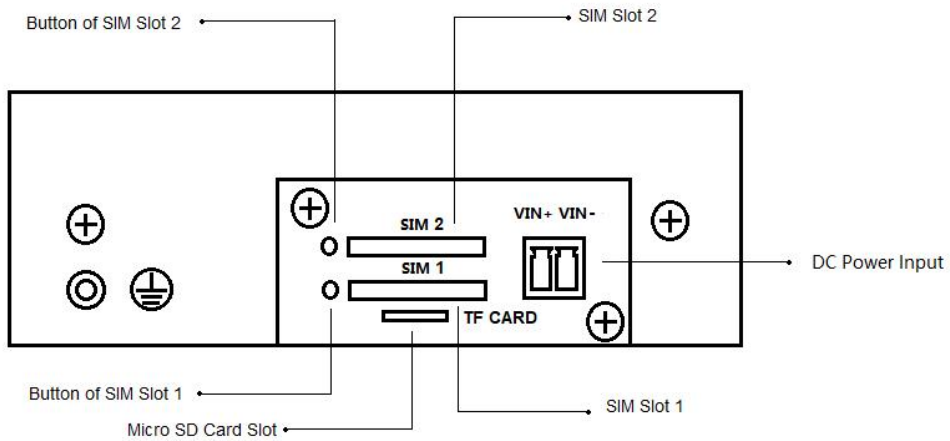


Image 5: Side view of TG453 with dual SIM

Note: standard package only supports single SIM, dual SIM is an optional feature.

2.2.2 Interfaces connection

Hardware Interfaces Instruction (standard TG453-NR and TG453-LF as an example)

Before we start to install and configure the TG453, let's have a quick view of the interfaces of it.(image 6-7 and table 1)

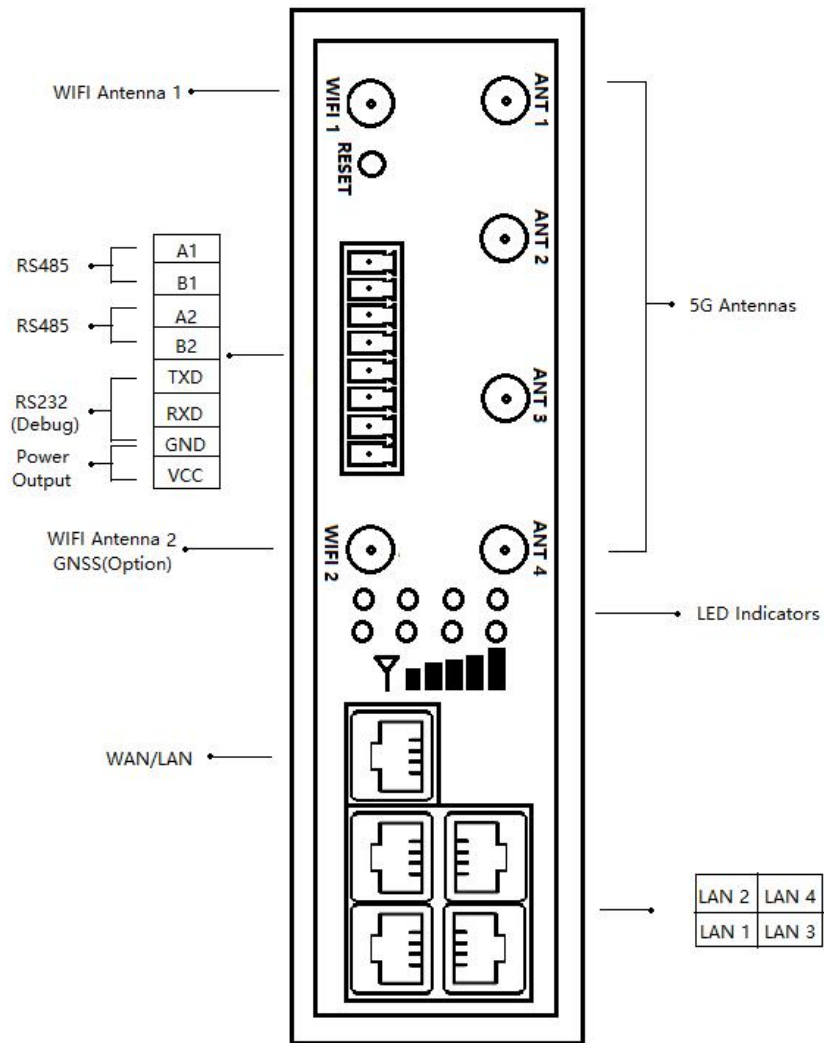


Image 6: TG453-NR 5G version Interfaces

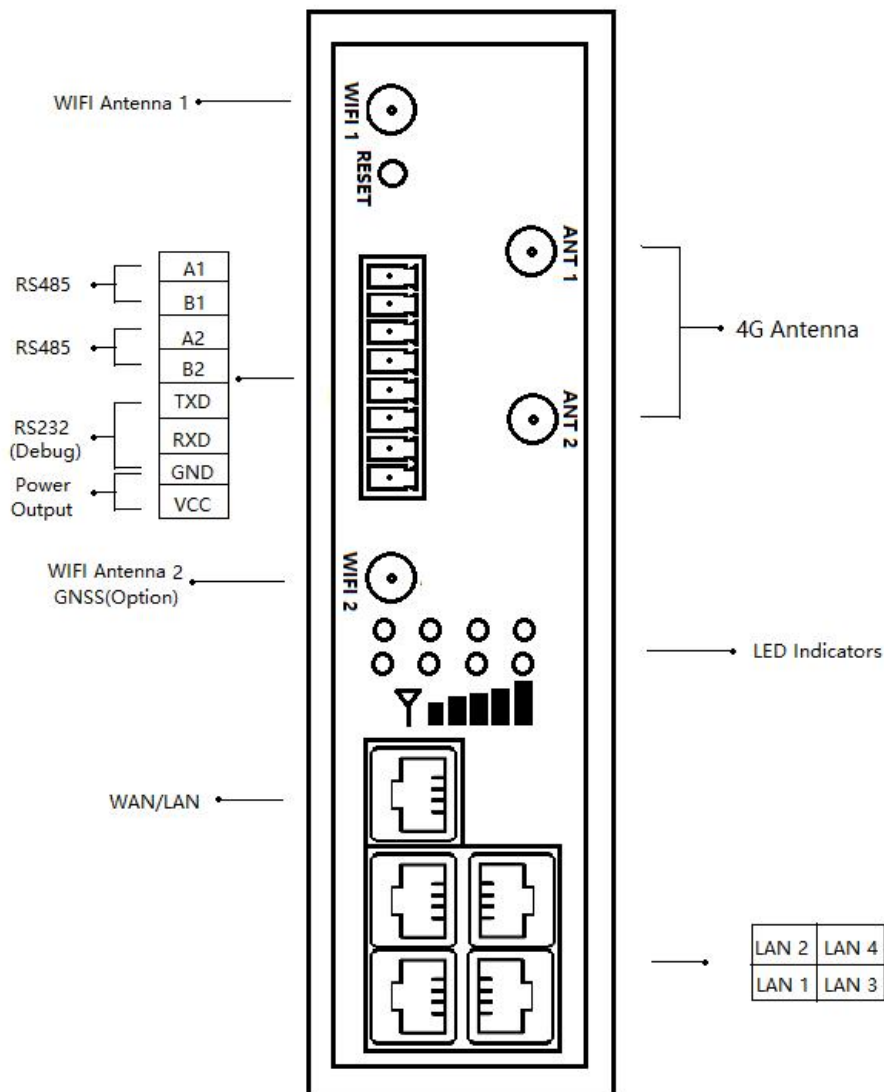


Image 6: TG453-LF 4G version Interfaces

1) Definition for I/O

No.	Item	Description
1	A1	RS485 port, used for connecting to sensors, controllers
2	B1	
3	A2	
4	B2	
5	TXD1	RS232 port, used for debug
6	RXD1	
7	GND	
8	VCC1	DC power output(12VDC output, current 1A), Built-in overcurrent protection, for external devices DC power input

Table 1: I/O of TG453

TG453 support 1x RS232(Debug only) and 2x RS485 serial ports, which can be used for IoT sensors/controllers, firmware upgrade, system log checking, debug, etc.

Besides, TG453 also comes with 1x DC power output, which is used to supply DC power for field sensors.

TG453 designed with industrial terminal block interface, and the RS232 cable in this package with ends of female connector and stripping cable, the signal of console cable is defined as below.(Table 2)

RS232 Cable(with DB9 female connector and stripping cable)

Color of cable	Corresponding DB9-Female Pin No.	Corresponding Pin No. of Router (See I/O 1)
Blue	2 (RX)	3(TX)
Brown	3 (TX)	4(RX)
Black	5 (GND)	5(GND)

Table 2: definition of RS232 cable

RS485 Cable (not included in package)

Color of cable	TG453 Router
Red	1(A)
Black	2(B)

Table 3: definition of RS485

2.2.3 Power Supply

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

2.2.4 Cellular Antenna

TG453 provides 4 cellular antennas(TG453-NR, 5G version), which comes with SMA male connector, screw the SMA male antenna to TG453(SMA female port, ANT 1-4, image 6), make sure it is screwed tightly to ensure the strength of signal.

2.2.5 WIFI Antenna

TG453 provides 2 WIFI antennas which comes with SMA female connector, screw the antenna to 2 TG453 WIFI ports(male), make sure it's screwed tightly to ensure the strenght of signal.(image 6)

2.3 LED Indicators

TG453 Series Gateway provides 8 LED indicators, as following.

Indicator	Status	Content
Power	On	Powered On
	Off	Powered Off
Signal Strength	1 Lights	Weak signal strength
	2 Lights	Middium signal strenght
	3 Lights	Strong signal strenght
Online	On	Gateway accesses to Internet
	Off	Gateway doesn't access to Internet
Alarm	On	<ul style="list-style-type: none"> ● SIM/UIM Card is not insert corectly or broken ● Antenna signal is too weak
	1 Blink Per Second	Cellular module was not registered to Gateway
	2 Blinks Per Second	Gateway can't access to Internet
	Off	Gateway doesn't have any alarm
WIFI	On	WIFI Enabled
	Off	WIFI Disabled
WAN	On	WAN is connected
	Off	WAN is not connected
LAN	LAN1 Blink	LAN1 works
	LAN2 Blink	LAN2 works
	LAN3 Blink	LAN3 works
	LAN4 Blink	LAN4 works

	Off	LAN is not connected
--	-----	----------------------

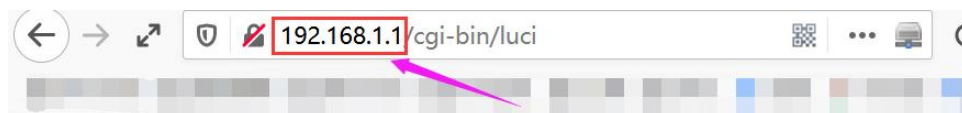
Table 4: Definition of LED indicators

3. Configuration and Management

To enter into the web config UI, there are 2 ways: Via Ethernet port and WIFI hotspot.

Use an Ethernet cable to connect the LAN port of TG453 to your laptop, or use your laptop or mobile phone to connect to WIFI hotspot 'Bivocom' of TG453, login with password of WIFI: admin123, normally your laptop will get an IP address from TG453 DHCP as 192.168.1.xx, otherwise please manually configure your laptop IP to 192.168.1.100.

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



Authorization Required

Please enter your username and password.

Username

Password

After enter into the web config page, you'll see a list of menu on left side, as below.

3.1 View

To check the following system information.

3.1.1 System

Display system related information, such as firmware version, local time, SN, uptime, etc.

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

Status

System

Hostname	router
Model	TG453
SN	20220730843
Firmware Version	53.1.0.15
Release Time	2022-06-24 11:08:42
Local Time	2022-11-30 14:30:39 Wednesday
Uptime	0h 1m 45s
Load Average	0.24, 0.12, 0.05

Memory

Total Available	230524 kB / 253928 kB (90%)
Free	215908 kB / 253928 kB (85%)
Cached	10972 kB / 253928 kB (4%)
Buffered	3644 kB / 253928 kB (1%)


3.1.2 Network

Display WAN, LAN, WiFi, DHCP network information.

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

Status

Network

IPv4 WAN Status	 Type: dhcp eth2.2 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-RKDCFBI	192.168.1.204	50:9a:4c:14:19:2a	9h 45m 18s

3.1.3 Routes

Display routing tables.

ARP

IPv4-Address	MAC-Address	Interface
172.17.144.1	00:52:24:89:2d:03	eth2.2
172.17.144.77	1c:a0:b8:80:95:ae	eth2.2
192.168.1.204	50:9a:4c:14:10:2a	br-lan
172.17.1.188	a4:55:90:81:4e:47	eth2.2
172.17.144.21	00:e0:4c:38:26:0c	eth2.2
192.168.1.10	00:00:00:00:00:00	br-lan
172.17.1.232	00:00:00:00:00:00	eth2.2
172.17.0.146	00:00:00:00:00:00	eth2.2

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
wan	0.0.0.0/0	172.17.144.1	0
wan	172.17.0.0/16	0.0.0.0	0
wan	172.17.144.1	0.0.0.0	0
lan	192.168.1.0/24	0.0.0.0	0

Active IPv6-Routes

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

3.1.4 System Log

Display system log.

View

- System
- Network
- Routes
- System Log
- VPN Status

Setup

Secure

VPN

Advanced

Data Collect

Administrate

Logout

System Log

```
Dec 21 13:52:00 dctd[1163]: Start to collect data
Dec 21 13:52:00 dctd[1163]: get adc data
Dec 21 13:52:00 dctd[1163]: get di data
Dec 21 13:52:00 dctd[1163]: get relay data
Dec 21 13:52:00 dctd[1163]: Start to send collected data, type[1]
Dec 21 13:52:05 dctd[1163]: debug timer callback
Dec 21 13:52:06 dctd[1163]: Server Address is: 192.168.1.10
Dec 21 13:52:09 dctd[1163]: Failed to connect server 192.168.1.10, port 9001, wait 20s and retry
```

3.1.5 VPN Status

Display VPN status.

Bivocom TG453 supports IPsec, PPTP, L2TP, OpenVPN, GRE protocols, after it's successfully connected to your VPN server, it'll display some info as below, such as,

Type, Connect Status, Uptime, Subnet Mask, etc.

VPN

VPN Status	Type:	openvpn
	IP Address:	10.10.10.1
	Netmask:	255.255.255.255
	Gateway:	10.10.10.2
	Connected Time:	21m,53s

View
System
Network
Routes
System Log
VPN Status
Setup
Secure
VPN
Advanced
Administrate
Logout

3.2 Setup

Main menu of this page includes, [WAN](#), [LAN](#), [Wireless](#), [Online Detection](#), [Diagnostics](#).

3.2.1 WAN

1) Connection Type

WAN supports DHCP/Static IP/PPPoE/3G/4G/5G connection type.

Choose the mode you need to configure the related parameters, then you can connect to the internet.

Let's take cellular type(5G) as an example.

WAN Setting

On this page, you can configure WAN port connection type

WAN Interface

General Settings | Advanced Settings

Connection Type: 5G

Network Type: Static IP, DHCP, PPPoE, 3G, 5G, Unmanaged

APN: [input field]

PIN: [input field]

User Name: [input field]

Password: [input field]

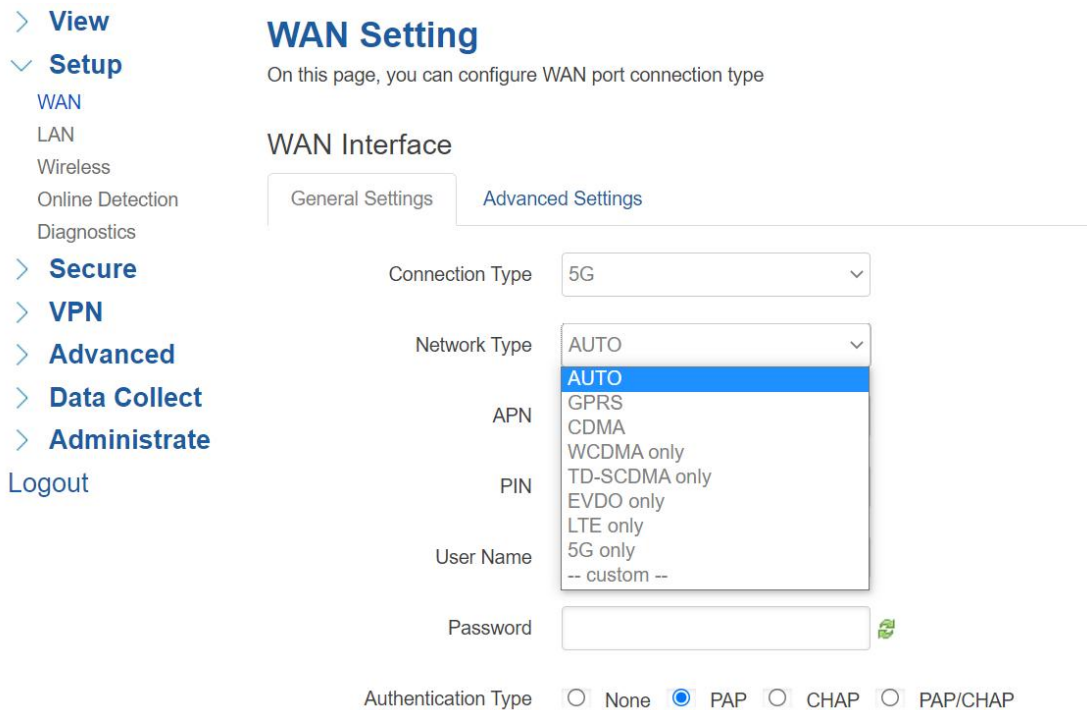
Authentication Type: None PAP CHAP PAP/CHAP

Save & Apply Save Reset

View
Setup
WAN
LAN
Wireless
Online Detection
Diagnostics
Secure
VPN
Advanced
Data Collect
Administrate
Logout

2) Network Type

Type of network, the default value is AUTO, you can keep it as default or choose your own preference, such as 5G only, LTE only or 3G only, etc.



The screenshot shows the 'WAN Setting' configuration page. On the left is a navigation menu with options: View, Setup (selected), WAN, LAN, Wireless, Online Detection, Diagnostics, Secure, VPN, Advanced, Data Collect, and Administrate. Below the menu is a 'Logout' link. The main content area is titled 'WAN Setting' and includes a subtitle: 'On this page, you can configure WAN port connection type'. Below this is the 'WAN Interface' section with two tabs: 'General Settings' (active) and 'Advanced Settings'. The 'General Settings' tab contains several fields: 'Connection Type' (set to 5G), 'Network Type' (dropdown menu), 'APN', 'PIN', 'User Name', and 'Password'. The 'Network Type' dropdown menu is open, showing options: AUTO (highlighted), GPRS, CDMA, WCDMA only, TD-SCDMA only, EVDO only, LTE only, 5G only, and -- custom --. Below the fields is the 'Authentication Type' section with radio buttons for None, PAP (selected), CHAP, and PAP/CHAP.

3) APN

For standard SIM card, just keep it as blank, while if you're using SIM card with APN required, then you have to input the APN from your Telcos, and different Telcos might have different APN, please ask your Telco if you have no idea of what your APN is.

4) PIN

PIN code of SIM card, normally, just keep it as blank, so please use it carefully, or the SIM card may be locked.

5) PAP/CHAP Username

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

6) PAP/CHAP Password

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

blank.

7) Authentication Type

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

Normally, just keep it as default.

- PAP, Plaintext Authentication
- CHAP, Handshake authentication

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

8) WAN Used As LAN

When you use 5G/4G/3G/2G cellular network to access internet, you can go to "Advanced Settings" to change the WAN to act as a LAN port.

The screenshot shows the 'WAN Setting' page. On the left is a navigation menu with options: View, Setup (selected), WAN, LAN, Wireless, Online Detection, Diagnostics, Secure, VPN, Advanced, Data Collect, and Administrate. The main content area is titled 'WAN Setting' and includes the instruction: 'On this page, you can configure WAN port connection type'. Below this is the 'WAN Interface' section with two tabs: 'General Settings' and 'Advanced Settings' (selected). Under 'Advanced Settings', there are three input fields: 'Clone MAC Address' (00:22:44:66:88:00), 'MTU' (1500), and 'WAN Multiplex'. The 'WAN Multiplex' field contains an unchecked checkbox and a link 'Set WAN port as LAN port'. A red box highlights this checkbox and link, and a pink arrow points to the checkbox.

3.2.2 LAN

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

The meaning of the parameters are as follows.

1) IPv4 Address

To configure IP address of LAN port, default value is 192.168.1.1, which is also the login IP address when you want to enter into the web config page, so you can change the IP address of LAN yourself.

[View](#)
[Setup](#)
 WAN
 LAN
 Wireless
 Online Detection
 Diagnostics
[Secure](#)
[VPN](#)
[Advanced](#)
[Data Collect](#)
[Administrate](#)
 Logout

Interfaces - LAN

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

Common Configuration

General Setup | **Advanced Settings**

Protocol: Static address

IPv4 address: 192.168.1.1

IPv4 netmask: 255.255.255.0

DNS Servers:

2) IPv4 Netmask

The netmask of LAN port IP address.

3) DHCP Server

DHCP Server

General Setup

Ignore interface [Disable DHCP](#) for this interface.

Start: [Lowest leased address as offset from the network address.](#)

Limit: [Maximum number of leased addresses.](#)

Leasetime: [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 address, to ensure numbers of IP address of start and limit not exceed 250.

- **Lease time**

Time of assigning the IP address.

3.2.3 Wireless

Menu of wireless are mainly for configuring parameters of WIFI hotspot, such as, SSID, work mode, password, etc.

Note: standard package of TG453 only supports 2.4G WIFI, if you need dual band WIFI, please ask Bivocom representative for more info when place the order.

WIFI 2.4G

Click 'Enable', to enable the WIFI function.

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) Bivocom_TG453

Channel auto

Mode 802.11bgn

Encryption WPA2-PSK-AES

Key

Hide SSID

1) Network Name (SSID)

You can configure your own WIFI hotspot name.

2) Channel

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

3) Mode

Support 802.11b, 802.11g, 802.11bgn, and default value is 802.11bgn.

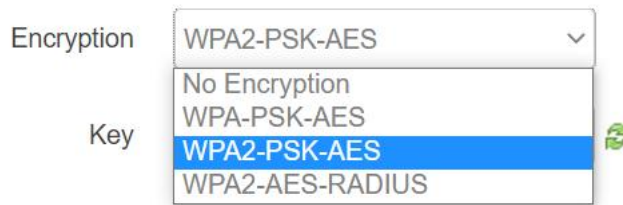
802.11b up to 11Mbps, 802.11g up to 54Mbps and 802.11n up to 300Mbps.

4) Encryption

You can choose different encryption type as below.

Encryption

Key



5) Key

Password of WIFI hotspot, user needs to input it to access the internet shared by WIFI. The minimum length of password is 8 bytes.

6) Hide SSID

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

5.8G Setting (Option)

5.8G WIFI is an optional feature, if you choose the dual band WIFI version, below are some parameters of 5.8G WIFI you'll configure.

Click 'Enable', to enable the WIFI function.

5.8G Setting

General Settings **Advanced Settings**

WiFi 5.8G Enable Disable

Mode

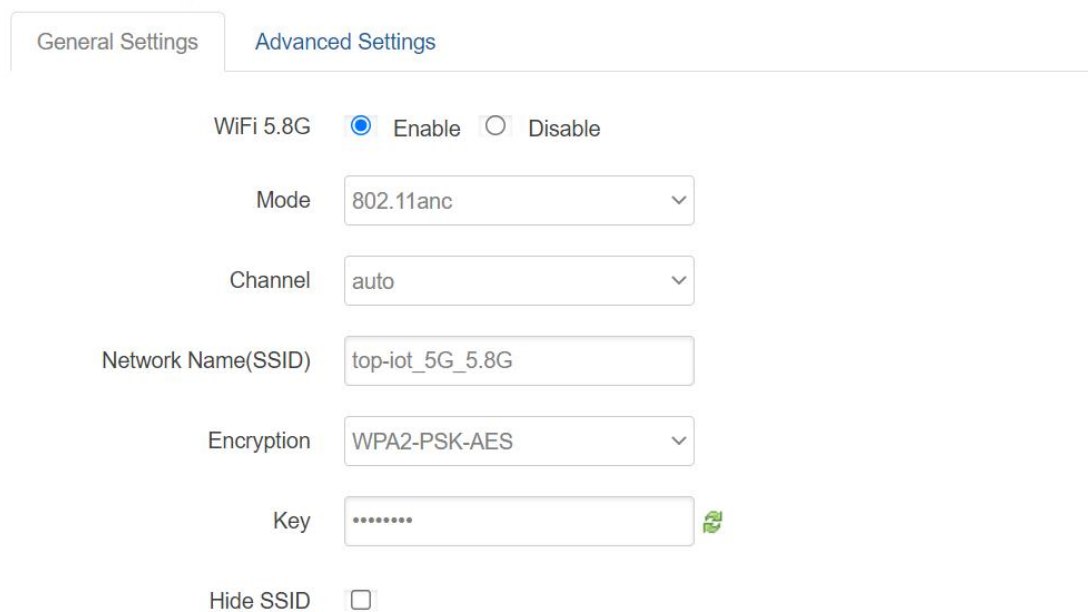
Channel

Network Name(SSID)

Encryption

Key

Hide SSID



1) Mode

Support 802.11a, 802.11an, 802.11ac and 802.11anc, and default value is 802.11anc.

2) Channel

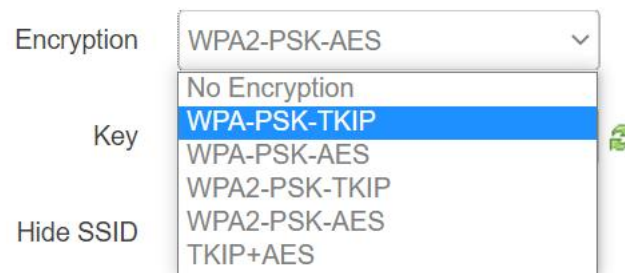
Support 149, 153, 157, 161, 165 channels, default value is auto, channel can be changed automatically.

3) Network Name (SSID)

WIFI hotspot name.

4) Encryption

You can choose different encryption type as below.



5) Key

Password of WIFI hotspot, user needs to input it to access the internet shared by WIFI. The minimum length of password is 8 bytes.

6) Hide SSID

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

3.2.4 Online Detection

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

The meaning of the parameters are as follows.

The screenshot shows the 'Online Detection' configuration page. On the left is a navigation menu with options: View, Setup (selected), WAN, LAN, Wireless, Online Detection, Diagnostics, Secure, VPN, Advanced, Data Collect, and Administrate. The main content area is titled 'Online Detection' and contains the following settings:

- Online Detection: Enable Disable
- Detection Type: Ping (selected in a dropdown menu)
- Primary Detection Server: 114.114.114.114
- Second Detection Server: 202.96.199.133
- Retry Times: 3
- Retry Interval: 60 (with a help icon and the unit 'Seconds')
- Enable Reboot: Enable Disable
- Reboot After Interval: 30 (with a help icon and the unit 'Minutes')

1) Detection Type

There are 3 types: ping, traceroute and DNS.

- **Ping**

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

- **Traceroute**

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

- **DNS**

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

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

2) Primary Detection Server

It can be an IP address or a Domain Name configured by yourself.

3) Second Detection Server

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

4) Retry Times

You can set up retry time in case detection fails.

5) Retry Interval

The interval time between 2 detections.

6) Enable Reboot

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

7) Reboot After Interval

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

3.2.5 Diagnostics

There are 3 types of diagnostics: ping, traceroute and nslookup

Parameter of ping and traceroute can be a Domain Name or an IP address, used for checking if router is online or not. While nslookup is to analytic domain.

1) Ping

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

114.114.114.114 114.114.114.114 www.baidu.com

IPv4 ▾ **Ping** **Traceroute** **Nslookup**

Install iputils-traceroute6 for IPv6 traceroute

```

PING 114.114.114.114 (114.114.114.114): 56 data bytes
64 bytes from 114.114.114.114: seq=0 ttl=70 time=881.904 ms
64 bytes from 114.114.114.114: seq=1 ttl=72 time=88.259 ms
64 bytes from 114.114.114.114: seq=2 ttl=86 time=96.134 ms
64 bytes from 114.114.114.114: seq=3 ttl=92 time=88.011 ms
64 bytes from 114.114.114.114: seq=4 ttl=81 time=76.243 ms

--- 114.114.114.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 76.243/246.110/881.904 ms

```

2) Traceroute

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

114.114.114.114 www.163.com www.baidu.com

IPv4 ▾ **Ping** **Traceroute** **Nslookup**

Install iputils-traceroute6 for IPv6 traceroute

```

traceroute to www.163.com (27.148.151.214), 30 hops max, 38 byte packets
 1 *
 2 10.170.8.46 55.546 ms
 3 10.170.8.67 59.488 ms
 4 10.170.8.68 55.376 ms
 5 115.168.76.66 51.438 ms
 6 118.84.189.217 59.402 ms
 7 117.27.253.74 51.578 ms
 8 *
 9 *
10 *
11 27.148.151.214 139.821 ms

```

3) Nslookup

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

<input type="text" value="114.114.114.114"/>	<input type="text" value="www.163.com"/>	<input type="text" value="www.baidu.com"/>
IPv4 ▾ <input type="button" value="Ping"/>	<input type="button" value="Traceroute"/>	<input type="button" value="Nslookup"/>

Install iputils-traceroute6 for IPv6 traceroute

```
Server: 127.0.0.1
Address 1: 127.0.0.1 localhost

Name: www.baidu.com
Address 1: 14.215.177.38
Address 2: 14.215.177.37
```

3.3 Secure

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

3.3.1 DMZ Host

DMZ can forward the port of WAN to a host of LAN; all packet from WAN will be forwarded to specified host of LAN.

- > View
- > Setup
- > **Secure**
 - DMZ Host
 - Port Forwards
 - Traffic Rules
 - Custom
- > VPN
- > Advanced
- > Data Collect
- > Administrate
- Logout

DMZ

Set DMZ Host

DMZ Enable Disable

Source zone wan: wan:

DMZ Host

1) DMZ

You can enable or disable the DMZ.

2) DMZ Host

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

3.2.2 Port Forwarding

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

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
This section contains no values yet			

New port forward:

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

Add

Save & Apply Save Reset

1) Name

You can name the rule you created.

2) Protocol

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

3) External Port

Destination port before port forwarding.

4) Internal IP Address

The Host IP address to forward.

5) Internal Port

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

After configured above-mentioned, click 'Add', then a new rule will be added, and click 'Save & Apply', to have the rule take effect.

3.3.3 Traffic Rules

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

> View
 > Setup
 > Secure
 DMZ Host
 Port Forwards
 Traffic Rules
 Custom
 > VPN
 > Advanced
 > Data Collect
 > Administrate
 Logout

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
This section contains no values yet		

Open ports on router:

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

New forward rule:

Name	Source zone	Destination zone
New forward ru	lan	wan

1) Name

You can name the rule yourself.

2) Protocol

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

3) External Port

Choose the port you want to open.

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

New forward rule:

Name	Source zone	Destination zone
New forward ru	lan	wan

1) Name

You can name the rule yourself.

2) Source Zone

You can choose where to start the data packet.

3) Destination Zone

You can choose where to forward the data packet.

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

Rule is enabled

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!

1) Restrict to Address Family

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

2) Protocol

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

3) Source MAC Address

To choose the source MAC address of data packet.

4) Source Address

To choose the source IP address of data packet.

5) Source Port

To choose the source port of data packet.

6) Destination Address

To choose the destination IP address of data packet.

7) Destination Port

To choose the destination port of data packet.

8) Action

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

- **Accept**

Allow data packet to go through.

- **Drop**

Drop data packet

- **Reject**

Drop data packet, and return an unachievable data packet.

- **Don't Track**

No action.

3.3.4 Custom

Custom rules allow you to execute arbitrary iptables commands which are not covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

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

The screenshot shows a web interface for configuring firewall rules. On the left is a navigation menu with items: View, Setup, Secure (expanded), DMZ Host, Port Forwards, Traffic Rules, Custom (highlighted with a red box), VPN, Advanced, Data Collect, Administrate, and Logout. The main content area is titled "Firewall - Custom Rules" and contains the following text: "Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded." Below this is a text area with a search icon, containing the following shell script comments: "# This file is interpreted as shell script.", "# Put your custom iptables rules here, they will", "# be executed with each firewall (re-)start.", "# Internal uci firewall chains are flushed and recreated on reload, so", "# put custom rules into the root chains e.g. INPUT or FORWARD or into the", "# special user chains, e.g. input_wan_rule or postrouting_lan_rule."

3.4 VPN

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

TG453 support VPN: PPTP, L2TP, OpenVPN and IPSec. PPTP/L2TP are layer 2 VPN, and OpenVPN is VPN based on SSL, while IPSec is layer 3 VPN. PPTP/L2TP are more convenient to use, while OpenVPN and IPSec is more complex, as they need complex certification management, meanwhile, they offer more secured encrypted data.

3.4.1 PPTP


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


1) PPTP Client


PPTP Client Enable Disable

Server Address

User Name

Password 


Remote Subnet  eg: 192.168.10.0

Remote Subnet Mask  eg: 255.255.255.0

NAT

Enable MPPE Encryption

Enable Static Tunnel IP Address

Default Gateway  All Traffic Will Passthrough Via VPN

1. PPTP Client

You can enable or disable PPTP client.

2. Server Address

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

3. User Name and Password

To enter the username and password provided by server.

4. Remote Subnet

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

5. Remote Subnet Mark

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

6. NAT

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

7. Enable MPPE Encryption.

You can enable MPPE encryption here.

8. Default Gateway

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

2) PPTP Server

PPTP Server Enable Disable

Server Local IP

IP Address Range eg: 10.10.10.1-10.10.10.254

Enable MPPE Encryption

NAT

DNS1

DNS2

WIN1

WIN2

CHAP Secrets eg: test * test *

Client Subnet eg: test 192.168.10.0

1. PPTP Server

You can enable or disable PPTP server.

2. Server Local IP

To enter the server local IP address.

3. IP Address Range

Type the range of assigned IP address.

4. Enable MPPE Encryption.

You can enable MPPE encryption here.

5. DNS1/DNS2

To enter the assigned DNS address.

6. WIN1/WIN2

To enter the WIN address.

7. CHAP Secrets

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

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

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

Test * testing *

Please ask for Bivocom support if you need an example of how to set up the PPTP client and server work mode.

3.4.2 L2TP


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

1) L2TP


L2TP Client Enable Disable

Server Address


User Name


Password 

Tunnel Name

Tunnel Password 


Enable IPsec

Remote Subnet  eg: 192.168.10.0


Remote Subnet Mask  eg: 255.255.255.0

NAT

Enable MPPE Encryption

MTU  600~1450

Enable Static Tunnel IP Address

Default Gateway  All Traffic Will Passthrough Via VPN

Client

1. L2TP Client

You can enable or disable L2TP client.

2. Server Address

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

3. User Name and Password

To enter the username and password provided by server.

4. Remote Subnet

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

5. Remote Subnet Mask

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

6. NAT

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

7. Enable MPPE Encryption.

You can enable MPPE encryption here.

8. Default Gateway

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

2) L2TP Server

L2TP Server Enable Disable

Server Local IP

IP Address Range eg:10.10.10.100-10.10.10.200

Enable MPPE Encryption

Enable IPsec

NAT

CHAP Secrets eg: test * test *

Client Subnet eg: test 192.168.10.0 255.255.255.0

1. L2TP Server

You can enable or disable L2TP server.

2. Server Local IP

To enter the server local IP address.

3. IP Address Range

Type the range of assigned IP address.

4. Enable MPPE Encryption.

You can enable MPPE encryption here.

5. CHAP Secrets

To create an username and password under CHAP Secrets, format as below,
Username<space>*<space>password<space>*
For example, if you want to create a username: test, password: test, it is as below,
Test * test *

Please ask for Bivocom support if you need an example of how to set up the L2TP client and server work mode.

3.4.3 IPsec

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

IPsec Enable Disable

Peer Address	<input type="text" value="%any"/>
Negotiation Method	<input type="text" value="Main"/>
Tunnel Type	<input type="text" value="Site To Site"/>
Local Subnet	<input type="text" value="192.168.4.0/24"/>
Peer Subnet	<input type="text" value="192.168.5.0/24"/>
IKE Encryption Algorithm	<input type="text" value="AES-128"/>
IKE Integrity Algorithm	<input type="text" value="SHA-1"/>
Diffie-Hellman Group	<input type="text" value="Group14(2048bits)"/>
IKE Life Time	<input type="text" value="28800"/>
Authentication Type	<input type="text" value="Pre-shared Key"/>
Pre-shared Key	<input type="text" value="123456abc"/>

Local Identifier	<input type="text"/>
Peer Identifier	<input type="text"/>
ESP Encryption Algorithm	AES-128 <input type="button" value="v"/>
ESP Integrity Algorithm	SHA-1 <input type="button" value="v"/>
DPD Timeout	<input type="text" value="60"/> <input type="button" value="seconds"/>
DPD Detection Period	<input type="text" value="60"/> <input type="button" value="seconds"/>
DPD Action	Restart <input type="button" value="v"/>

1) Peer Address

To enter peer IP address or Domain Name, if TG453 chosen as an IPsec server, you don't need to input it.

2) Negotiation Method

You can choose 'Main' or 'Aggressive'.

3) Tunnel Type

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

4) Local Subnet

Local subnet and mask, like 192.168.10.0/24.

5) Peer Subnet

Peer subnet and mask, like 192.168.20.0/24.

6) IKE Encryption Algorithm

IKE phase encryption method

IKE Encryption Algorithm	AES-128 <input type="button" value="v"/>
IKE Integrity Algorithm	<input type="button" value="3DES"/> <input checked="" type="button" value="AES-128"/> <input type="button" value="AES-192"/> <input type="button" value="AES-256"/>

7) IKE Lifetime

To set up IKE lifetime.

8) Local Identifier

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

9) Peer Identifier

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

10) ESP Encryption Algorithm

The encryption method of ESP.

For more info about how to set up IPsec, please contact Bivocom support to get quick guide.

3.4.3 OpenVPN

OpenVPN Enable Disable

Topology

Protocol

Port

Device Type

Peer Address

Authentication Type

Local Tunnel Address

Peer Tunnel Address

Peer Subnet Address

Peer Subnet Mask

Enable NAT

Enable LZO Compress

Cipher Algorithm

MTU

1) OpenVPN

You can enable or disable OpenVPN.

2) Topology

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

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

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

3) Role

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

4) Protocol

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

5) Port

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

6) Device Type

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

7) OpenVPN Server

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

8) Authentication Type

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

9) TLS Role

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

For more info, please contact Bivocom support to get quick guide.

3.5 Advanced

You can set up some advanced functions here.

The screenshot shows the 'Routes' configuration page. The left sidebar has a menu with 'Advanced' highlighted in a red box. The main content area is titled 'Routes' and contains a table for 'Static IPv4 Routes'. The table has columns for Interface, Target, IPv4-Netmask, IPv4-Gateway, and Metric. Below the table is an 'Add' button.

3.5.1 Static Routing

Static routing is used to add a routing table entry. (Currently, it only supports IPv4)

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

Buttons: Add, Delete

Interface: To choose which interface you want to add routing, LAN or WAN.

Target: Can be a host IP, or subnet.

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

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

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

3.5.2 Net Flow

The traffic meter function of TG453 is for traffic statistics from WAN port, meanwhile, it has traffic overflow alarm function. Even if the router is powered off, the traffic statistics

will be saved, and when you power on the router, the traffic will be counted based on your last time traffic.

- > View
- > Setup
- > Secure
- > VPN
- > **Advanced**
 - Static Routes
 - Net Flow
 - GPS Location
 - DHCP and DNS
- > Data Collect
- > Administrate

Logout

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

Day Limit M

Month Limit M

Clear Day Flow

Clear Month Flow

3.5.3 GPS Location(Optional)

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

- > View
- > Setup
- > Secure
- > VPN
- > **Advanced**
 - Static Routes
 - Net Flow
 - GPS Location
 - DHCP and DNS
- > Data Collect
- > Administrate

Logout

GPS Location

GPS Location Enable Disable

GPS Source External Dongle

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

GPS Info -

Connection Status -

Server Address: The IP address of server that you want the router to report the location, which is based on TCP connection.

Server Port: The port of server.

Report Interval: The interval time for auto report of router location, default value is 60 seconds.

Note: GPS is an optional feature.

3.5.4 DHCP and DNS

General DHCP and DNS settings base on Dnsmasq tool on TG453. Please refer to Dnsmasq for more information.

3.6 Data Collect

Data Collect settings is for TG453 to acquire data from slave devices in serial ports, Ethernet ports, I/O ports, with Modbus protocol and other customized protocols.

3.6.1 Basic Setting

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

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), and Administrate. 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 is titled 'Basic Setting' and contains the following settings:

- 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:

At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

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

3.6.2 Interface Setting

TG453 has 3 serial ports, COM1(RS485), COM2(RS485) and 1 RS232 for debug, and below are some parameters to configure, for protocols, it can be configured as Modbus or transparent mode depends on your application need.

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

Logout

Interface Setting

COM1/RS485
COM2/RS485

Enabled Enable Disable

Baudrate

Databit

Stopbit

Parity

Frame Interval ms

COM Protocol

Command Interval ms

Besides, TG453 can connect up to 5 TCP servers, which means you can receive the data from remote sites in different servers, it's also a backup solution for data storage at server.

TCP Server Setting

TCP Server1
TCP Server2
TCP Server3
TCP Server4
TCP Server5

Enabled Enable Disable

Server Address

Server Port

Frame Interval ms

COM Protocol

Command Interval ms

3.6.3 Modbus Rules Setting

Modbus Rules Setting is for TG453 as a Modbus master to acquire data from slave devices base on Modbus protocol. You can configure Modbus rules on it. TG453 provides the options of definable factor name, device ID, function code, register address and count register number, please follow the slave device datasheet to get the

information.

Below is an example of getting data from temperature and humidity sensor.

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

Modbus Rules Setting

Modbus Rules

Order	Device Name	Interface	Factor Name	Device ID	Function Code	Start Address	Count	Data Type	Reporting Center	Enable	
1	T&HSensor1	COM5	temperature; humidity	1	4	1	2	unsigned 16Bits AB	1	<input checked="" type="checkbox"/>	Edit Delete

New Modbus Rule

Order	Device Name	Interface	Factor Name	Device ID	Function Code	Start Address	Count	Data Type	Reporting Center	
<input type="text"/>	<input type="text"/>	COM5	<input type="text"/>	0-255	0-255	0-65535	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 View Setting
- > Administrate
- Logout

Modbus Rules - T&HSensor1 - COM5

enabled

Order

Device Name

Belonged Interface

Factor Name Multiple Factors Are Separated By Semicolon

Alias Name Multiple Aliases Are Separated By Semicolon

Device ID 0-255

Function Code 0-255

Start Address 0-65535

Count 1-120

Data Type A highest byte

Reporting Center Multiple Servers Are Separated By Minus

Unit Multiple Units Are Separated By Semicolon

Operator 0 + - * /

Operand

Accuracy 0-6

3.6.4 Server Setting

Server setting menu allows user set the data center address with multiple protocols, the standard TG453 supports TCP, UDP, HTTP, MQTT, and Modbus TCP. For the data format, TG453 supports different Encapsulation type, include “Transparent”, “Json”, and “HJ212” (special for some Environment SCADA in China). Also TG453 accepts customized specific protocols for your data center.

> View
> Setup
> Secure
> VPN
> Advanced
✓ Data Collect
 Basic Setting
 Interface Setting
 Modbus Rules Setting
 IO Setting
 Server Setting
 Data View Setting
> Administrate
_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 **CONNECTED**

3.7 Administrate

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

3.7.1 System

System Properties

Hostname	<input type="text" value="router"/>
Timezone	<input type="text" value="(GMT+08:00) Beijing, Chongqing"/>
Language	<input type="text" value="English"/>
Web Access Method	<input type="text" value="HTTP"/>  Need Reboot When Changed

1) Host Name

The host name of router, default name is router.

2) Time Zone

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

3) Language

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

4) Enable Telnet Access

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

5) Enable SSH Access

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

3.7.2 Password

To revise the login password of router.

Origin Password	<input type="password"/>	
Password	<input type="password"/>	
Confirmation	<input type="password"/>	

1) Origin Password

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

2) Password

Type the new password you want to change.

3) Confirmation

Type the new password again to confirm it.

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

3.7.3 Time Setting

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

The screenshot shows the 'Set System Time' configuration page. On the left is a navigation menu with options: View, Setup, Secure, VPN, Advanced, Data Collect, and Administrate (expanded). Under 'Administrate', there are sub-options: System, Password, Time Setting (selected), Log Setting, Backup and Restore, Router Upgrade, Remote Configured, Manual Reboot, Schedule Reboot, and Screen Calibration. At the bottom of the menu is 'Logout'. The main content area is titled 'Set System Time' and displays the following information:

- Current system time: 2020-07-17 15:19:39
- System Time Type: Radio buttons for ntp and rtc, with rtc selected.
- Current RTC Time: A label above two input fields.
 - RTC Date: An input field with a help icon and example 'eg: 2016-01-01'.
 - RTC Time: An input field with a help icon and example 'eg: 12:00:00'.

At the bottom right of the configuration area are three buttons: 'Save & Apply', 'Save', and 'Reset'.

1) Current System Time

Display the time of router.

2) System Time Type

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

- **RTC**

You can update data and time yourself.

RTC Date  eg: 2016-01-01

RTC Time  eg: 12:00:00

RTC Data

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

RTC Time

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

- **NTP**

NTP Time Server 

Port

Update Interval  seconds

NTP Time Server

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

Port


NTP time server port, default port is 123.

Update Interval

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

3.7.4 Log Settings


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

Output To Device 

Log Size  KB

Log Server

Log Server Port

Output Level 

1) Output to Device

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

2) Log Size

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

3) Log Server

Set up the IP address of log server.

4) Log Server Port

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

5) Output Level

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

3.7.5 Backup and Restore

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

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。

1) Download Backup

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

2) Reset to Default

Click 'Perform Reset', and a pop-up confirmation box with 'Really Reset All Changes' will

display, then click 'OK' to reset to factory defaults.

3) Restore Backup

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

Restore backup:

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

3.7.6 Router Upgrade

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

Flash new firmware image

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

Keep settings:

Image:

1) Keep Settings

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

2) Choose and Upload Firmware Image

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

Flash Firmware - Verify

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

Click "Proceed" below to start the flash procedure.

Checksum: `#68983dbe5ec7f0d4bf9258e421ad53d`

Size: 9.00 MB

Configuration files will be kept.

- **Checksum**

MD5 checksum value of firmware.

- **Size**

The size of firmware.

- **Proceed**

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

3.7.7 Remote Configured

Remote Configured feature allows TG453 **work with Bivocom Device Management Platform(Option service)** for remote management, like firmware upgrade, configuration change, etc.

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

Remote Configured

Remote Configured Enable Disable

Server Address

Server Port

Heart Interval

Device Number

Connection Status -

1) Remote Configured

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

2) Server Address

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

3) Server Port

The specified login server port.

4) Heart Interval

The heartbeat time interval (Unit: second)

5) Device Number

Device ID of router.

6) Device Phone Number

The phone number of SIM card insert in router.

7) Device Type

Type of the device, default is router.

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

Remote Upgrade Enable Disable

Server Address

Server Port

Firmware Version

8) Remote Upgrade

Click 'Enable' to enable remote firmware upgrade function.

9) Server Address

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

10) Server Port

Type the server port for remote upgrade.

11) Firmware Version

Type the firmware version that you want to upgrade remotely.

3.7.8 Manual Reboot

Reboots the operating system of your device



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

3.7.9 Schedule Reboot

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

Schedule Reboot

Enable Schedule Reboot Enable Disable

Schedule Type By Period By Time

Period Interval  Minutes, Min 5

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

3.8 Logout

Click the Logout menu to logout the web UI of TG453.

Version: V1.0

November 30, 2022