

Bivocom[®]

Programmable 5G/4G CAN FD/CAN Vehicle Gateway VG465 Series User Guide



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, No. C07 Building, 3rd Software Park, Xiamen, China 361000

Tel.: +86-592-6090 133

Fax: +86-592-6211727

Email: support@bivocom.com

sales@bivocom.com

www.bivocom.com



EU DECLARATION OF CONFORMITY

Hereby, **Xiamen Bivocom Technologies Co., Ltd.** declares that the radio equipment type VG465 is in compliance with Directive 2014/53/EU.

About This Guide

Thank you for choosing Bivocom Programmable 5G/4G CAN FD/CAN Gateway VG465 Series.

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

This manual is compatible with below models

Model	Description
VG465-NR	Industrial CAN FD/CAN Gateway with 5G/NR
VG465-LF	Industrial CAN FD/CAN Gateway with 4G/LTE

Table of Contents

Copyright	1
Trademark	1
Disclaimer	2
About This Guide	2
Table of Contents	4
1. Introduction	6
1.1 Overview	6
1.2 Applications	6
1.3 Dimensions	7
1.4 Physical Characteristics	8
2. Getting Started	8
2.1 Package Checklist	8
2.2 Installation	8
2.2.1 SIM/UIM Card	9
2.2.2 Interfaces connection	10
2.2.3 Power Supply	10
2.2.4 Cellular Antenna	10
2.3 LED Indicators	10
3. Configuration and Management	11
3.1 View	12
3.1.1 System	12
3.1.2 Network	13
3.1.3 Routing Tables	14
3.1.4 System Log	14
3.1.5 VPN Status	15
3.2 Setup	15
3.2.1 WAN	15
3.2.2 LAN	17
3.2.3 Wireless	18
3.2.4 Online Detection	20
3.2.5 Diagnostics	22
3.3 Security	23
3.3.1 DMZ Host	24
3.3.2 Port Forwarding	24
3.3.3 Traffic Rules	25
3.3.4 Custom Settings	27
3.4 VPN	27
3.4.1 PPTP	27
3.4.2 L2TP	29
3.4.3 OpenVPN	32

3.4.4 IPsec	33
3.5 Advanced	34
3.5.1 Static Routing	34
3.5.2 Net Flow	35
3.5.3 GPS Location	35
3.5.4 DHCP and DNS	36
3.6 Data Collect	36
3.6.1 Basic Setting	36
3.6.2 Interface Setting	37
3.6.3 Modbus Rules Setting	38
3.6.4 CAN FD/CAN Setting	40
3.6.5 Server Setting	41
3.7 Administrate	42
3.7.1 System	42
3.7.2 Password	43
3.7.3 Time Setting	44
3.7.4 Log Settings	45
3.7.5 Backup and Reset	46
3.7.6 Firmware Upgrade	47
3.7.7 Remote Management	48
3.7.8 Manual Reboot	49
3.7.9 Schedule Reboot	50

1. Introduction

1.1 Overview

The VG465 is an innovative and smart 5G/4G edge gateway designed for automotive companies to diagnose vehicle Electronic Control Units (ECUs) remotely. Powered by an ARM A55 Quad-core 64-bit processor and boasting 8GB of RAM, along with 64GB of FLASH storage, this device is primed to meet the demands of remote monitoring of in-vehicle networking.

Featuring a user-friendly LCD screen, 6 programmable buttons, and a robust set of connectivity options — including 3 RJ45 gigabit Ethernet ports, CAN FD/CAN 2.0B, WiFi, Bluetooth, and GPS — the VG465 offers seamless integration and operation. It also includes 2 RS232 ports (with 1 dedicated for debugging), 1 USB 2.0, 1 USB 3.0, and a TF slot supporting up to 32GB of data storage.

With a wide power input range of 5-60VDC, the VG465 is equipped to handle the rigors of vehicle applications. Its operating system, based on OpenWrt Linux, supports C/C++ and Python SDKs for streamlined development. Alternatively, it can run on Ubuntu with Docker container support.

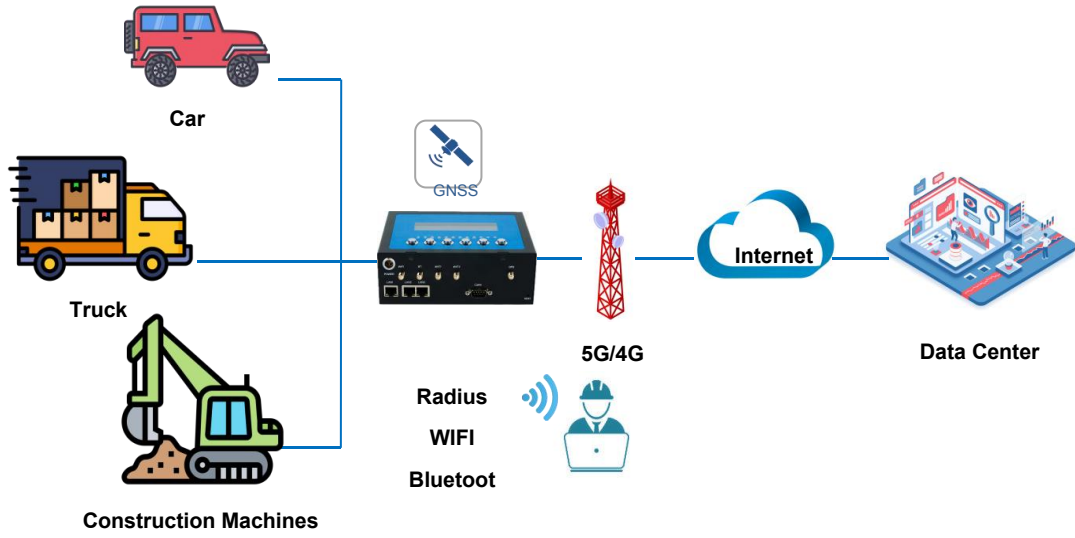
Moreover, the VG465 comes with a rich array of protocols including MQTT broker/client, Modbus RTU/TCP, JSON, TCP/UDP, SNMP, OPC UA, IEC 101/104, and VPN. These protocols allow for versatile and secure communication, tailor-made to meet your monitoring needs.

1.2 Applications

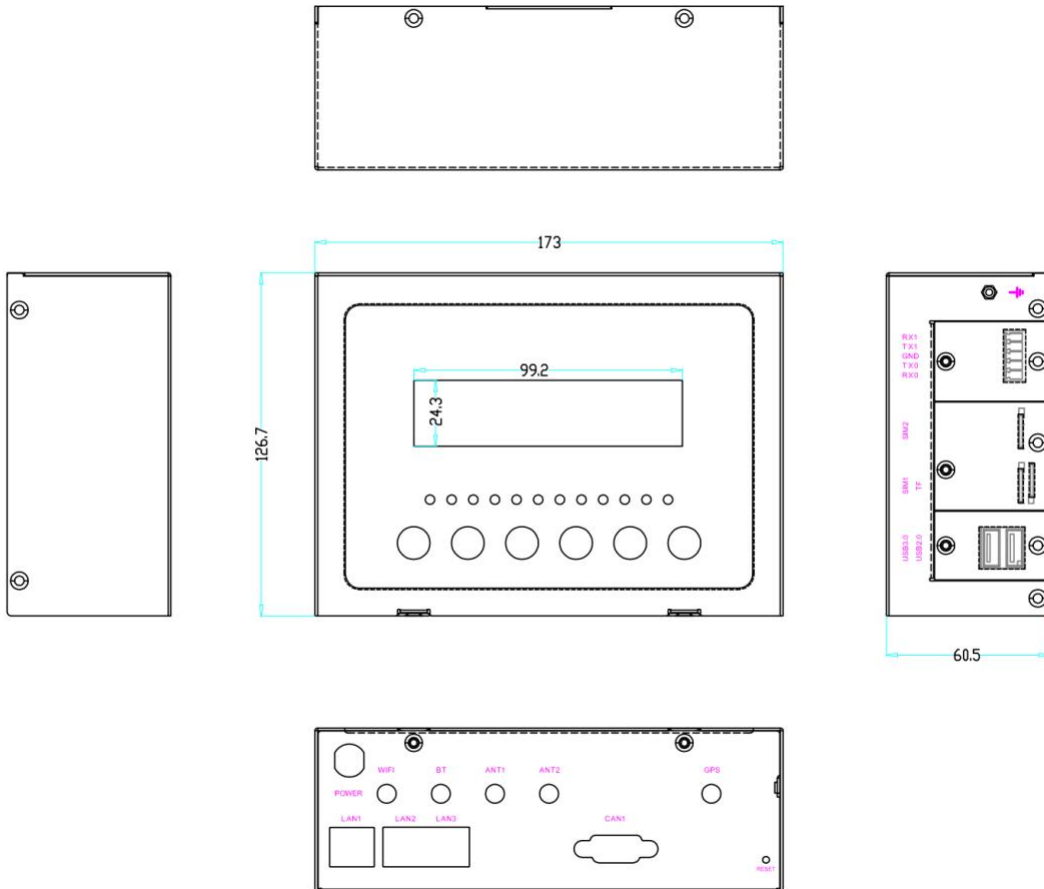
The VG465 supports engineer to collect CAN/CAN FD data from ECU and log the data to a file, which can help to analyse or diagnose the state of car, include Anti-lock Braking System, chassis, engine, etc.

Typical application as below.

Applicatio



1.3 Dimensions



1.4 Physical Characteristics

Physical Characteristics	
Housing	Metal, IP30
Dimensions	173x126.7x60.5mm (6.81 x 4.96 x 2.38in), Antenna and other accessories not included
Weight	VG465: 1051g (2.32lbs), without accessories.

2. Getting Started

2.1 Package Checklist

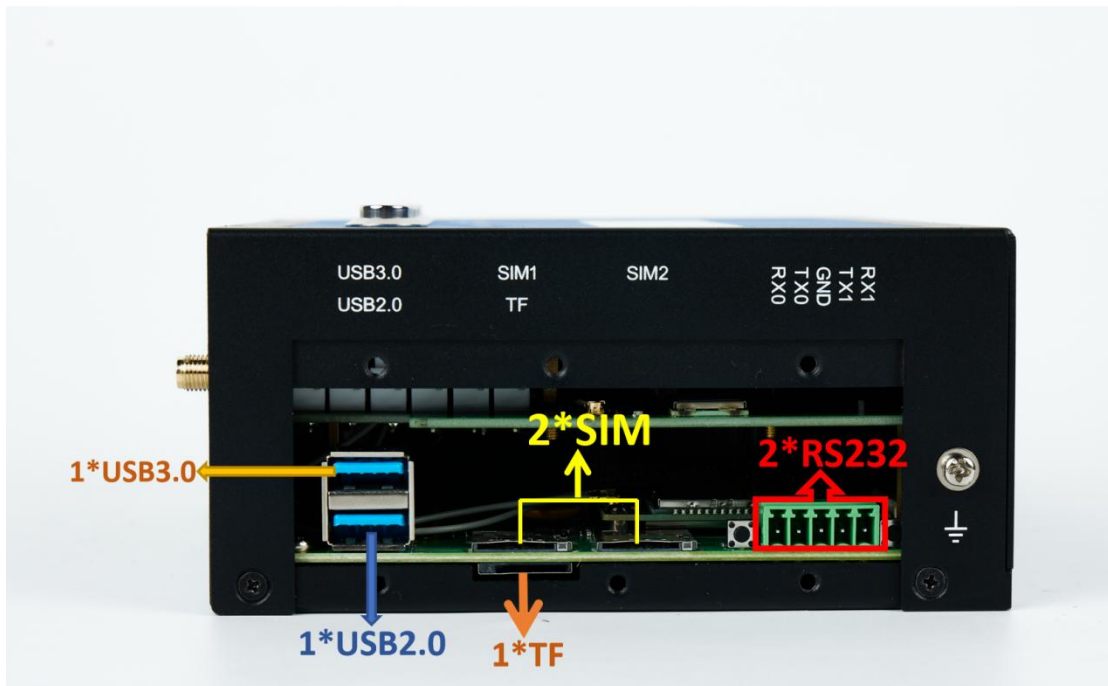
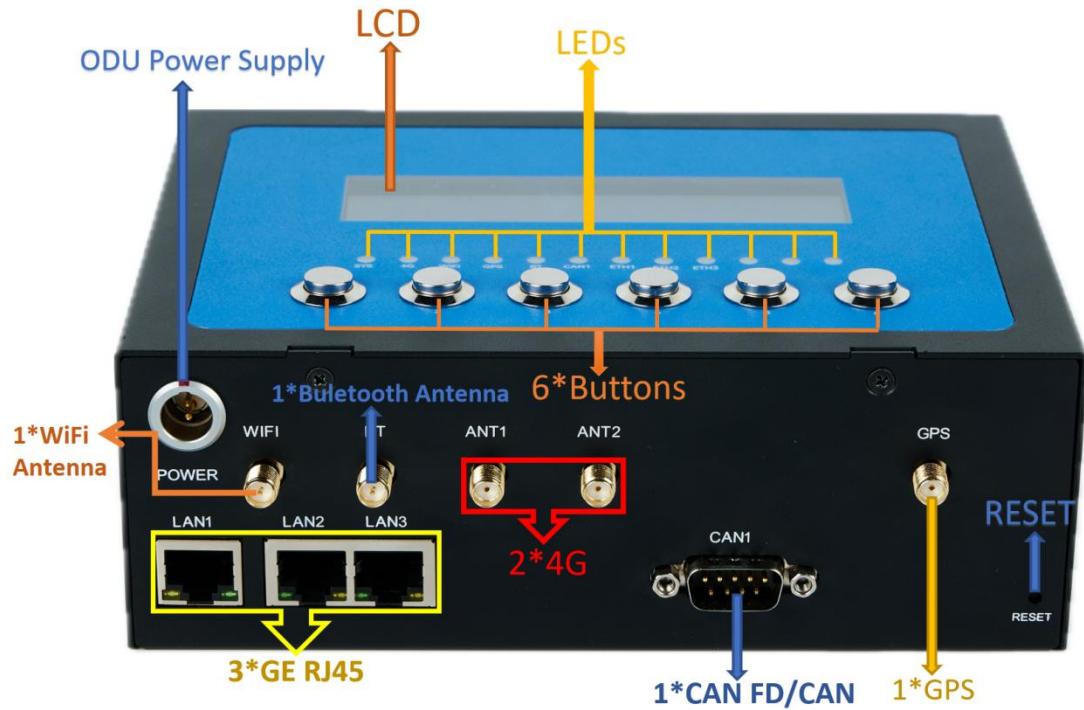
The following components are included in your VG465 package.

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

1. VG465 Gateway	1PCS
2. Cellular Antenna	5GVersion:4 PCS 4GVersion:2 PCS
3. WiFi Antenna	1PCS
4. Bluetooth Antenna	1PCS
5. GPS Antenna	1PCS
6. Ethernet Cable (1 meter)	1PCS
7. 5-Pin Terminal Block	3PCS
8. RS232 Cable(DB9 Female, 1 meter)	1PCS

2.2 Installation

Hardware interfaces instruction:



2.2.1 SIM/UIM Card

VG465 supports Micro SIM/UIM only, so if you're using Normal SIM or Nano SIM card, you may need to use a Nano SIM to Micro SIM adapter, and switch Normal SIM to Micro

SIM.

Make sure your router is powered off, put the SIM/UIM card to SIM card slot, insert it to gateway and press it until it was locked. If you want to plug out your SIM/UIM card, also need to make sure your router is powered off, then gently press the protruding part of the sim card, it will flick out immediately.

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

2.2.2 Interfaces connection

VG465 support 2 RS232 serial ports, 1 RS232_2 works as console port, which can be used for firmware upgrade, system log checking, debug, etc, 1 RS232_1 can be used for communicating and data collecting.

VG465 has 1 CAN FD/CAN port(DB9 Male Connector), which can support CAN FD or CAN data collecting.

CAN1 DB9 Male Connector(CAN FD/CAN)

PIN	Function
2	CAN1_L, CAN FD channel 1 Low
7	CAN1_H, CAN FD channel 1 High

2.2.3 Power Supply

The power supply of VG465 is 2 pin EGG.1B.Male connector, we suggest you power cord for it with 2 pin FGG 1B Female connector. Bivocom's standard power supply is 1.5A/12VDC. If you have to use your own power supply, make sure the power range is 5-60VDC and it is stable enough(Ripple shall be less than 300mV, and Instantaneous voltage shall not larger than 60V), meanwhile, power shall over 4W.

2.2.4 Cellular Antenna

Screw the SMA male antenna to VG465(SMA female port), make sure it is screwed tightly to ensure the strength of signal.

2.3 LED Indicators

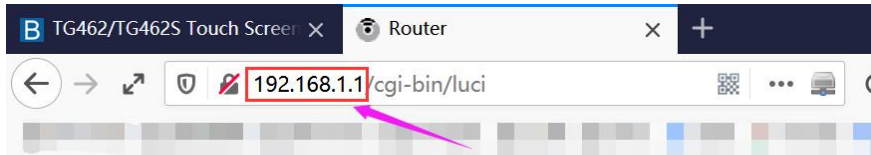
VG465 Series Gateway provides 8 LED indicators, as following.

Indicator	Status	Content
SYS	Blink	System works perfect
	Off	System doesn't work
BT	ON	Bluetooth enabled
	Off	Bluetooth disabled
GPS	On	Gateway got GPS data successfully
	Off	Gateway failed in getting GPS data
CAN1	On	CAN FD/CAN Function works
	Off	CAN FD/CAN Function doesn't work
WiFi	On	WiFi enabled
	Off	WiFi disabled
ETH1	On	ETH1 connected
	Off	ETH1 disconnected
ETH2	On	ETH2 connected
	Off	ETH2 disconnected
ETH3	On	ETH2 connected
	Off	ETH2 disconnected

3. Configuration and Management

Use an Ethernet cable to connect the LAN port of VG465 to your laptop, or use your laptop or mobile phone to connect to WIFI hotspot 'Bivocom' of VG465, login with password: admin123, normally your laptop will get an IP address from VG465 DHCP as 192.168.1.xx, otherwise please manually configure your laptop IP to 192.168.1.100.

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



Authorization Required

Please enter your username and password.

Username

Password

3.1 View

To check the following system information.

3.1.1 System

Display system related information.



> View	Status
> Setup	System
> Secure	Hostname router
> Advanced	Model VG465
> Administrate	SN 24070530000
> Debug	Firmware Version 1.0.0.4
Logout	Release Time 2024-07-18 17:38:26
	Local Time 2024-07-18 16:20:51 Thursday
	Uptime 0h 1m 11s
	Load Average 0.72, 0.22, 0.08
	Memory
	Total Available <input type="text" value="7777224 kB / 7858808 kB (98%)"/>
	Free <input type="text" value="7750996 kB / 7858808 kB (98%)"/>
	Cached <input type="text" value="24412 kB / 7858808 kB (0%)"/>
	Buffered <input type="text" value="1816 kB / 7858808 kB (0%)"/>

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 eth1 Address: 172.17.144.186 Netmask: 255.255.255.0 Gateway: 172.17.144.1 Mac Address: 72:1e:c8:85:ed:6e DNS 1: 172.17.144.1 Connected: 8h 16m 58s
Online Status	online
Active Connections	<input type="text" value="29 / 16384 (0%)"/>

LAN Status

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

Wireless Status

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

DHCP Leases

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

3.1.3 Routing Tables

Display routing tables.

ARP

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

Active IPv4-Routes

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

Active IPv6-Routes

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

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

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

3.1.5 VPN Status

Display VPN status.

VPN

VPN Status

Type:	l2tp
IP Address:	100.100.100.95
Netmask:	255.255.255.255
Gateway:	100.100.100.1
Connected Time:	1m,2s

3.2 Setup

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

3.2.1 WAN

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

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

- > View
- > Setup
 - WAN
 - LAN
 - Wireless
 - Wireless Client
 - Online Detection
 - Diagnostics
- > Secure
- > VPN
- > Advanced
- > Administrate
- Logout

Interfaces - WAN

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

Common Configuration

General Setup | Physical Settings

Protocol	LTE
Service Type	AUTO
APN	<input type="text"/>
PIN	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>

Authentication Type: None PAP CHAP

1) Server Type

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

2) APN

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

3) PIN

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

4) PAP/CHAP Username

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

5) PAP/CHAP Password

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

6) Call Center No.

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

7) Authentication Type

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

- PAP, Plaintext Authentication
- CHAP, Handshake authentication

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

8) WAN Used As LAN

When you use 5G/4G/3G cellular network to access internet, you can change the WAN to

act as a LAN port.

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

WAN Setting

On this page, you can configure WAN port connection type

WAN Interface

General Settings | Advanced Settings

Clone MAC Address: 00:22:44:66:88:00

MTU: 1500 (64-1500)

WAN Multiplex: Set WAN port as LAN port

3.2.2 LAN

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

The meaning of the parameters are as follows.

Common Configuration

General Setup | Advanced Settings | Physical Settings

Protocol: Static address

IPv4 address: []

IPv4 netmask: 255.255.255.0

IPv4 gateway: []

DNS Servers: []

1) IPv4 Address

To configure IP address of LAN port.

2) IPv4 Netmask

The netmask of LAN port IP address.

3) IPv4 Gateway

Specify the next-hop routing gateway.

4) DHCP Settings

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 the SSID, work mode, password, etc.


WiFi Enable Disable

Network Name(SSID)

Mode WiFi6 2.4G WiFi6 5G

Channel

Encryption

Key 

1) WIFI 2.4G/5G

Click 'Enable', to enable the WIFI function.

2) Network Name (SSID)

WIFI network name.

3) Channel

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

4) Mode

Support 802.11b, 802.11g, 802.11bgn, 802.11ac.

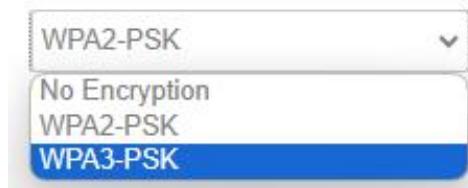
802.11b up to 11Mbps, 802.11g up to 54Mbps, 802.11n up to 300Mbps and 802.11ac up to 866Mbps.

5) Encryption

You can only choose below types if the mode is set as 802.11b or 802.11g.



If enable WiFi 5G mode, you can chose WPA3-PSK.



6) Key

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

7) Hide SSID

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

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.

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

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 shows the router is online even it is offline.

2) Primary Detection Server

It can be an IP address or a Domain Name.

3) Second Detection Server

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

4) Retry Times

You can set up retry time in case detection fails.

5) Retry Interval

The interval time between 2 detection.

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 reponse as below.

114.114.114.114	www.163.com	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

```
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 reponse as below.

114.114.114.114	www.163.com	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 Security

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

3.3.1 DMZ Host

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

DMZ Enable Disable

DMZ Host

1) DMZ

You can enable or disable the DMZ.

2) DMZ Host

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

3.2.2 Port Forwarding

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

New port forward:

Name	Protocol	External zone	External port	Internal IP address	Internal port	
<input type="text" value="New port forward"/>	<input type="text" value="TCP"/>	<input type="text" value="wan"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

1) Name

You can name the rule you created.

2) Protocol

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

3) External Port

Destination port before port forwarding.

4) Internal IP Address

The Host IP address to forward.

5) Internal Port

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

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

3.3.3 Traffic Rules

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

Open ports on router:

Name	Protocol	External port
<input type="text" value="New input rule"/>	TCP+UDP	<input type="text"/>

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
<input type="text" value="New forward rule"/>	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 or TCP/UDP.

3) Source MAC Address

To choose the source MAC address of data packet.

4) Source Address

To choose the source IP address of data packet.

5) Source Port

To choose the source port of data packet.

6) Destination Address

To choose the destination IP address of data packet.

7) Destination Port

To choose the destination port of data packet.

8) Action

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

- **Accept**

Allow data packet to go through.

- **Drop**

Drop data packet

- **Reject**

Drop data packet, and return an unachievable data packet.

- **Don't Track**

No action.

3.3.4 Custom Settings

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

3.4 VPN

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

VG465 support VPN: PPTP, L2TP, OpenVPN and IPsec. PPTP/L2TP are layer 2 VPN, and OpenVPN is VPN based on SSL, while IPsec layer 3 VPN. PPTP/L2TP are more convenient to use, while OpenVPN and IPsec is more complex, as they need complex certification management, meanwhile, they offer more secured encrypted data.

3.4.1 PPTP


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

1) PPTP Client

PPTP Client Enable Disable

Server Address

User Name

Password 


Remote Subnet

Remote Subnet Mask

NAT

Enable MPPE Encryption

Enable Static Tunnel IP Address

Default Gateway  All Traffic Will Passthrough Via VPN

1. PPTP Client

You can enable or disable PPTP client.

2. Server Address

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

3. User Name and Password

To enter the user name and password provided by server.

4. Remote Subnet

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

5. Remote Subnet Mark

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

6. NAT

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

7. Enable MPPE Encryption.

You can enable MPPE encryption here.

8. Default Gateway

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

2) PPTP Server

PPTP Server Enable Disable

Server Local IP

IP Address Range

Enable MPPE Encryption

DNS1

DNS2

WIN1

WIN2

CHAP Secrets

1. PPTP Server

You can enable or disable PPTP server.

2. Server Local IP

To enter the server local IP address.

3. IP Address Range

Type the range of assigned IP address.

4. Enable MPPE Encryption.

You can enable MPPE encryption here.

5. DNS1/DNS2

To enter the assigned DNS address.

6. WIN1/WIN2

To enter the WIN address.

7. CHAP Secrets

To create an username and password under CHAP Secrets, format as below,
Username<space>*<space>password<space>*

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

3.4.2 L2TP


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

1) L2TP Client

L2TP Client Enable Disable

Server Address

User Name

Password 


Remote Subnet

Remote Subnet Mask

NAT

Enable MPPE Encryption

Enable Static Tunnel IP Address

Default Gateway  All Traffic Will Passthrough Via VPN

1. L2TP Client

You can enable or disable L2TP client.

2. Server Address

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

3. User Name and Password

To enter the user name and password provided by server.

4. Remote Subnet

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

5. Remote Subnet Mark

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

6. NAT

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

7. Enable MPPE Encryption.

You can enable MPPE encryption here.

8. Default Gateway

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

2) L2TP Server

L2TP Server Enable Disable

Server Local IP

IP Address Range eg:10.10.10.100-10.10.10.200

Enable MPPE Encryption

CHAP Secrets

1. L2TP Server

You can enable or disable L2TP server.

2. Server Local IP

To enter the server local IP address.

3. IP Address Range

Type the range of assigned IP address.

4. Enable MPPE Encryption.

You can enable MPPE encryption here.

5. CHAP Secrets

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

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

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

Test * test *

3.4.3 OpenVPN

OpenVPN Enable Disable

Topology

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.

3.4.4 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="s"/> seconds
DPD Detection Period	<input type="text" value="60"/> <input type="button" value="s"/> seconds
DPD Action	Restart <input type="button" value="v"/>

1) Peer Address

To enter peer IP address or Domain Name, if choose as a server, you don't need to enter it.

2) Negotiation Method

You can choose 'Main' or 'Aggressive'.

3) Tunnel Type

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

4) Local Subnet

Local subnet and mask, like 192.168.10.0/24.

5) Peer Subnet

Peer subnet and mask, like 192.168.20.0/24.

6) IKE Encryption Algorithm

IKE phase encryption method

7) IKE Lifetime

To set up IKE lifetime.

8) Local Identifier

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

9) Peer Identifier

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

10) ESP Encryption Algorithm

The encryption method of ESP.

3.5 Advanced

You can set up some advanced functions here.

3.5.1 Static Routing

Static routing is used to add a routing table entry.

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	
	Host-IP or Network	if target is a network			
lan	<input type="text"/>	255.255.255.2	<input type="text"/>	0	<input type="button" value="Delete"/>

Interface: To choose which interface you want to add routing.

Target: Can be a host IP, or subnet.

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

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

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

3.5.2 Net Flow

The traffic meter function of VG465 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

Day Limit

Month Limit

Clear Day Flow

Clear Month Flow

3.5.3 GPS Location

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.

3.5.4 DHCP and DNS

General DHCP and DNS settings base on “dnsmasq” tool on VG465. Please refer to “dnsmasq” for more information.

3.6 Data Collect

Data Collect settings is for VG465 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 acquire and report period and other related options.

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

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

3.6.2 Interface Setting

Serial Ports&TCP Ports:

Switch the hardware interfaces for data acquisition from kinds of slave devices. Including Serial ports (COM1~COM2), Modbus TCP base on Ethernet LAN.

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

Interface Setting

COM1/RS485

COM2/RS485

Enabled Enable Disable

Baudrate

Databit

Stopbit

Parity

Frame Interval ms

COM Protocol

Command Interval ms

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

Connection Status

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

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

3.6.3 Modbus Rules Setting

Modbus Rules Setting is for VG465 as a Modbus master to acquire data from slave devices base on Modbus protocol. You can configure unlimited Modbus rules on it. VG465 provide the options of definable factor name, device ID, function code, register address and count register number, please following the slave device datasheet to get those information.

- > 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"/>	<input type="button" value="Edit"/> <input type="button" value="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"/>	<input type="text" value="0-255"/>	<input type="text" value="0-255"/>	<input type="text" value="0-65535"/>	<input type="text" value="1-120"/>	Unsigned 16Bits	<input type="text" value="1-2-3-4-5"/>	<input type="button" value="Add"/>

- > 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 CAN FD/CAN Setting

1) CAN Parameters

The CAN FD/CAN interface of VG465 needs to be configured by CLI(telnet or SSH login), it supports ip link set commands. For example, setup for CAN FD:

```
admin@router:# ip link set can0 down
admin@router:# ip link set can0 type can bitrate 500000 sample-point 0.8 dbitrate 2000000 dsample-point 0.70 fd on
admin@router:# ip link set can0 up
admin@router:# ip -details link show can0
2: can0: <NOARP,UP,LOWER_UP,ECHO> mtu 72 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1024
    link/can promiscuity 0 minmtu 0 maxmtu 0
    can <FD> state ERROR-ACTIVE (berr-counter tx 0 rx 0) restart-ms 0
        bitrate 500000 sample-point 0.800
        tq 50 prop-seg 15 phase-seg1 16 phase-seg2 8 sjw 1
        mcp251xfd: tseg1 2..256 tseg2 1..128 sjw 1..128 brp 1..256 brp-inc 1
        dbitrate 2000000 dsample-point 0.700
        dtq 50 dprop-seg 3 dphase-seg1 3 dphase-seg2 3 dsjw 1
        mcp251xfd: dtseg1 1..32 dtseg2 1..16 dsjw 1..16 dbrp 1..256 dbrp-inc 1
        clock 20000000 numtxqueues 1 numrxqueues 1 gso_max_size 65536 gso_max_segs 65535
```

For standard version, we didn't setup CAN settings on WEBUI, you can only configure it by CLI. If you need to configure it on WEBUI, please contact Bivocom team to discuss the details.

2) CAN send

Use VG465 to send CAN FD/CAN data frames can use cansend program on CLI, the usage is as follows:

```
admin@router:# cansend
cansend - send CAN-frames via CAN_RAW sockets.

Usage: cansend <device> <can_frame>.

<can_frame>:
  <can_id>#{data}           for 'classic' CAN 2.0 data frames
  <can_id>#R{len}           for 'classic' CAN 2.0 data frames
  <can_id>##<flags>{data}  for CAN FD frames

<can_id>:
  3 (SFF) or 8 (EFF) hex chars
{data}:
  0..8 (0..64 CAN FD) ASCII hex-values (optionally separated by '.')
{len}:
  an optional 0..8 value as RTR frames can contain a valid dlc field
<flags>:
  a single ASCII Hex value (0 .. F) which defines canfd_frame.flags

Examples:
  5A1#11.2233.44556677.88 / 123#DEADBEEF / 5AA# / 123##1 / 213##311223344 /
  1F334455#1122334455667788 / 123#R / 00000123#R3
```

3) CAN dump

VG465 supports CAN dump, you can use it to receive CAN FD/CAN data and recording

into a file, or filtering by CAN ID.

```
admin@router:# candump -h
candump - dump CAN bus traffic.

Usage: candump [options] <CAN interface>+
       (use CTRL-C to terminate candump)

Options:
  -t <type>      (timestamp: (a)bsolute/(d)elta/(z)ero/(A)bsolute w date)
  -H              (read hardware timestamps instead of system timestamps)
  -c              (increment color mode level)
  -i              (binary output - may exceed 80 chars/line)
  -a              (enable additional ASCII output)
  -S              (swap byte order in printed CAN data[] - marked with ``')
  -s <level>     (silent mode - 0: off (default) 1: animation 2: silent)
  -l              (log CAN-frames into file. Sets '-s 2' by default)
  -L              (use log file format on stdout)
  -n <count>     (terminate after reception of <count> CAN frames)
  -r <size>      (set socket receive buffer to <size>)
  -D              (Don't exit if a "detected" can device goes down.
  -d              (monitor dropped CAN frames)
  -e              (dump CAN error frames in human-readable format)
  -x              (print extra message infos, rx/tx brs esi)
  -T <msecs>    (terminate after <msecs> without any reception)

Up to 16 CAN interfaces with optional filter sets can be specified
on the commandline in the form: <ifname>[,filter]*

Filters:
  Comma separated filters can be specified for each given CAN interface:
  <can_id>:<can_mask>
    (matches when <received_can_id> & mask == can_id & mask)
  <can_id>~<can_mask>
    (matches when <received_can_id> & mask != can_id & mask)
  #<error_mask>
    (set error frame filter, see include/linux/can/error.h)
  [j|J]
    (join the given CAN filters - logical AND semantic)

CAN IDs, masks and data content are given and expected in hexadecimal values.
When the can_id is 8 digits long the CAN_EFF_FLAG is set for 29 bit EFF format.
Without any given filter all data frames are received ('0:0' default filter).

Use interface name 'any' to receive from all CAN interfaces.

Examples:
candump -c -c -ta can0,123:7FF,400:700,#000000FF can2,400~7F0 can3 can8

candump -l any,0~0,#FFFFFFF
       (log only error frames but no(!) data frames)
```

3.6.5 Server Setting

Server setting menu allows user set the data center address with multiple protocols, the standard VG465 support TCP, UDP, HTTP, MQTT, and Modbus TCP. For the data format, VG465 support different Encapsulation type, include "Transparent", "JSON", and "HJ212" (special for some Environment SCADA). Also VG465 accept customize 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

3.7.1 System

Hostname

Timezone

Language

Enable telnet access Enable Disable

Enable SSH access Enable Disable

1) Host Name

The host name of router, default name is router.

2) Time Zone

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

3) Language

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

4) Enable Telnet Access

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

5) Enable SSH Access

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

3.7.2 Password

To revise the password of router.

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

1) Origin Password

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

2) Password

Type the new password you want to change.

3) Confirmation

Type the new password again to confirm it.

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

3.7.3 Time Setting

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

> View
> Setup
> Secure
> VPN
> Advanced
> Data Collect
▼ Administrate
System
Password
Time Setting
Log Setting
Backup and Restore
Router Upgrade
Remote Configured
Manual Reboot
Schedule Reboot
Screen Calibration
Logout

Set System Time

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

System Time Type ntp rtc

Current RTC Time

RTC Date eg: 2016-01-01

RTC Time eg: 12:00:00

Save & Apply Save 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	<input type="text" value="0.openwrt.pool.ntp.org"/>
Port	<input type="text" value="123"/>
Update Interval	<input type="text" value="600"/> seconds

NTP Time Server

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

Port

NTP time server port, default port is 123.

Update Interval

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

3.7.4 Log Settings

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

Output To Device	<input type="text" value="/var/log/"/>
Log Size	<input type="text" value="64"/> KB
Log Server	<input type="text" value="0.0.0.0"/>
Log Server Port	<input type="text" value="514"/>
Output Level	<input type="text" value="Debug"/>

1) Output to Device

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

2) Log Size

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

3) Log Server

Set up the IP address of log server.

4) Log Server Port

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

5) Output Level

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

3.7.5 Backup and Reset

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

Backup / Restore

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

Download backup:

Reset to defaults:

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

Restore backup:

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 Firmware Upgrade

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

Flash new firmware image

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

Keep settings:

Image:

1) Keep Settings

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

2) Choose and Upload Firmware Image

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

Flash Firmware - Verify

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

Click "Proceed" below to start the flash procedure.

Checksum: `#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 Management

Remote Management feature allows VG465 **work with Bivocom Device Management Platform** for remote management, like firmware upgrade, configuration change, etc.

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

Remote Manage Enable Disable

Server Address

Server Port

Heart Interval

Device Number

Device Phone Number

Device Type

1) Remote Manage

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

2) Server Address

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

3) Server Port

The specified login server port.

4) Heartbeat Interval

The heartbeat time interval (Unit: second)

5) Device Number

Device ID of router.

6) Device Phone Number

The phone number of SIM card insert in router.

7) Device Type

Type of the device, default is router.

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

Remote Upgrade Enable Disable

Server Address

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