

G6500 EDGE Computing Gateway User Manual





Table of Contents

Copyright.....	2
Trademark.....	2
Disclaimer.....	2
About This Guide.....	3
Table of Contents.....	4
1. Introduction.....	6
1.1 Overview.....	6
1.2 Applications.....	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 SIM/UID Card.....	9
2.2.2 6-Pin Terminal Block and Console Cable.....	9
2.2.3 USB Port.....	10
2.2.4 Relay Interface (K0+ K0-, K1+ K1-).....	10
2.2.5 Digital Input (DI0, DI1).....	10
2.2.3 Power Supply.....	10
2.2.4 Cellular Antenna.....	10
2.2.5 WIFI Antenna.....	10
2.3 LED Indicators.....	10
2.4 Reset.....	11
3. Configuration and Management.....	12
3.0 Getting start Web UI.....	12
3.0.1 Connect your PC to G6500 network.....	12
3.0.1 Login the WebUI.....	12
3.1 View.....	13
3.1.1 System.....	13
3.1.2 Network.....	13
3.1.3 Routing Tables.....	14
3.1.4 System Log.....	15
3.1.5 VPN Status.....	15
3.2 Setup.....	16
3.2.1 WAN.....	16
3.2.2 LAN.....	18
3.2.3 Wireless.....	19
3.2.4 Wireless Client.....	21
3.2.5 Online Detection.....	22

3.2.6 Diagnostics.....	24
3.3 Security.....	24
3.3.1 DMZ Host.....	24
3.3.2 Port Forwarding.....	25
3.3.3 Traffic Rules.....	26
3.3.4 Custom Settings.....	28
3.4 VPN.....	28
3.4.1 PPTP.....	28
3.4.2 L2TP.....	30
3.4.3 OpenVPN.....	34
3.4.4 IPSec.....	35
3.4.5 GRE.....	37
3.5 Advanced.....	37
3.5.1 Send SMS.....	37
3.5.2 Static Routing.....	38
3.5.3 DI DO.....	38
3.5.4 Net Flow.....	39
3.5.5 GPS Location.....	40
3.5.6 BS Location (Option).....	41
3.5.7 Dynamic DNS.....	42
3.4.8 SNMP.....	43
3.5.9 DHCP and DNS.....	44
3.6 Data Collect.....	45
3.6.1 Basic Setting.....	45
3.6.2 Interface Setting.....	45
3.6.3 Modbus Rules Setting.....	46
3.6.4 IO Setting.....	47
3.6.5 Server Setting.....	48
3.7 Administrate.....	49
3.7.1 System.....	49
3.7.2 Password.....	50
3.7.3 Time Setting.....	50
3.7.4 Log Settings.....	52
3.7.5 Backup and Reset.....	53
3.7.6 Firmware Upgrade.....	53
3.7.7 Remote Management.....	54
3.7.8 Manual Reboot.....	56
3.7.9 Schedule Reboot.....	56
3.8 Logout.....	56



1. Introduction

1.1 Overview

G6500 Series Gateway is a type of industrial 802.11/b/g/n cellular gateway, which adopts high-powered industrial 32-bits CPU, with multi-layer software detection and hardware protection mechanism to ensure reliability and stability of the device. It supports worldwide carrier 4G/3G/2G cellular network FDD-LTE, TDD-LTE, and WCDMA, EVDO, TD-SCDMA, EDGE, CDMA 1X and GPRS. With rich VPN protocols (IPSEC, PPTP, L2TP and OpenVPN) to ensure the security of data transmission, and rich interfaces, such as 4x LAN ports, 1x WAN port, 1x USB port, 2x Relay(Optional), 1x RS232(Or RS485), 1x RS485, 2x DI(Digital Input), 1x CAN(Optional), Dual SIM(Single module, option) and Dual SIM(Dual Module, option), GPS(Optional) and WIFI, etc.

G6500 Series Gateway enables users to quickly access the Internet, to ensure secure and reliable data transmission. It's ideal for IOT (Internet of Things) and M2M(Machine to Machine) applications, and has been widely used in many applications, such as Intelligent Transportation, Smart Grid, Vending Machine, Agricultural Irrigation, Environmental Protection, Industrial Automation, Energy Saving, Smart Home, etc.

1.2 Applications

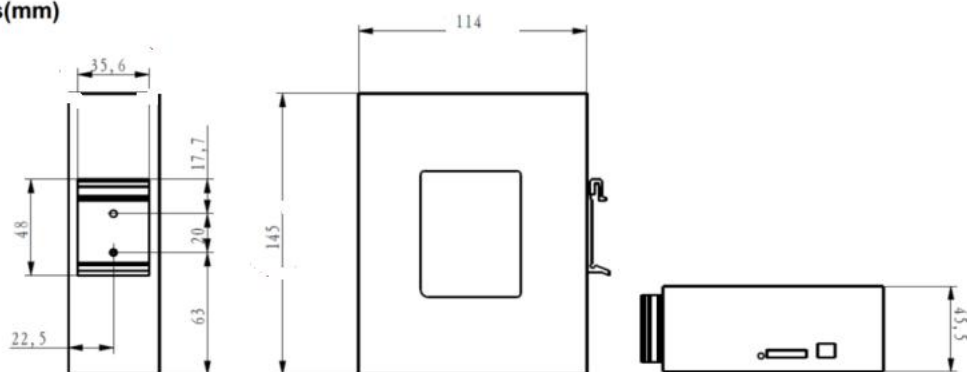
G6500 Series Gateway utilizes cellular network to connect your network devices and serial port devices to your center for remote monitoring and control.

Typical application as below.



1.3 Dimensions

Dimensions(mm)



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 not included.
Weight	630g(1.39lbs)

2. Getting Started

2.1 Package Checklist

The following components are included in your G6500 package.

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

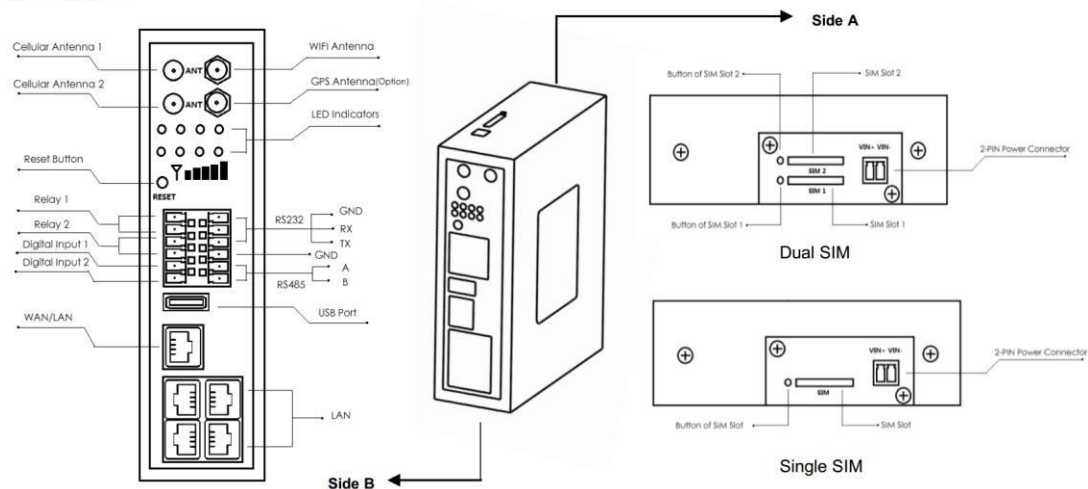
- G6500 Gateway Host
- Power Adapter(DC 12V/1.5A)
- WIFI Antenna(Female SMA)
- 2xCellular Antennas (Male SMA)
- Console Cable(RS232)
- Ethernet Cable(1 meter)
- 2x6-Pin Terminal Block
- 1x2-Pin Terminal Block
- DIN-rail mounting



2.2 Installation

G6500 ports instruction.

Side Views





2.2.1 SIM/UIM Card

G6500 supports normal SIM/UIM only, so if you're using a Micro SIM or Nano SIM card, you may need to use a Micro SIM or Nano SIM to Normal SIM adapter.

Make sure your device is powered off, then use a needle object(such as a pen) to push the button near the SIM/UIM card holder, it will flick out immediately. Put the SIM/UIM card to card holder with chipset upside, insert it and make sure it's tightly matched.

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

2.2.2 6-Pin Terminal Block and Console Cable

G6500 supports RS232 and RS485 serial port, which can be used for firmware upgrade, system log checking, or acts as serial port for data transmission.

G6500 is designed with industrial terminal block interface, and the cable in this package with ends of female connector and stripping cable, the signal of console cable is defined as below,

RS232 Cable(with DB9 female connector and stripping cable)

Color of cable	Corresponding DB9-Female Pin No.	Corresponding Pin No. of Gateway
Blue	2(RX)	TX
Brown	3(TX)	RX
Black	5(GND)	GND

RS485 Cable

Color of cable	TR341 Router
Red	5(A)
Black	6(B)

2.2.3 USB Port

Interface standard	USB2.0
Usage	For data storage, BLE dongle, and upgrade

2.2.4 Relay Interface (K0+ K0-, K1+ K1-)

Range	Supports max. 5A output, supports 220V AC, 30V DC
Usage	To control the power supply of peripherals

2.2.5 Digital Input (DI0, DI1)

Input range	DC 0~30V(0~2V is low level, about 2V is high level)
Usage	To detect status of peripherals

2.2.3 Power Supply

We suggest you use our standard power adapter (1.5A/12VDC). If you have to use your own power supply, make sure the power range is 5-35VDC and it is stable enough(Ripple shall be less than 300mV, and Instantaneous voltage shall not larger than 35V). When using our power adapter, please make you connect the cable to the right pin, red cable is for VIN+, and black cable is for VIN-, as below, or it may cause damage.

2.2.4 Cellular Antenna

Screw the 2 SMA male antennas to G6500(SMA female port), make sure it is screwed tightly to ensure the strength of signal.

2.2.5 WIFI Antenna

Screw the SMA female WIFI antenna to G6500(SMA male port), make sure it is screwed tightly to ensure the strength of signal.

2.3 LED Indicators

G6500 Series Gateway provides LED indicators, as following.

Indicator	Status	Content
Power	On	Powered On
	Off	Powered Off
Signal Strength	1 Lights	Signal weak
	2 Lights	Signal medium
	3 Lights	Signal Strong
System	Blink	System works
	Off	System doesn't work
Online	On	Gateway accesses to Internet
	Off	Gateway doesn't access to Internet
Alarm	On	● SIM/UIM Card is not insert correctly or broken ● Antenna signal is too weak
	1 Blink Per Second	Cellular module was not registered to Gateway
	2 Blinks Per Second	Gateway can't access to Internet
	Off	Gateway doesn't have any alarm
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

2.4 Reset

You can press the Reset button to reset settings to factory defaults to solve the problem of



incorrect configuration that makes you couldn't access to internet, login and management,



etc.

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

3. Configuration and Management

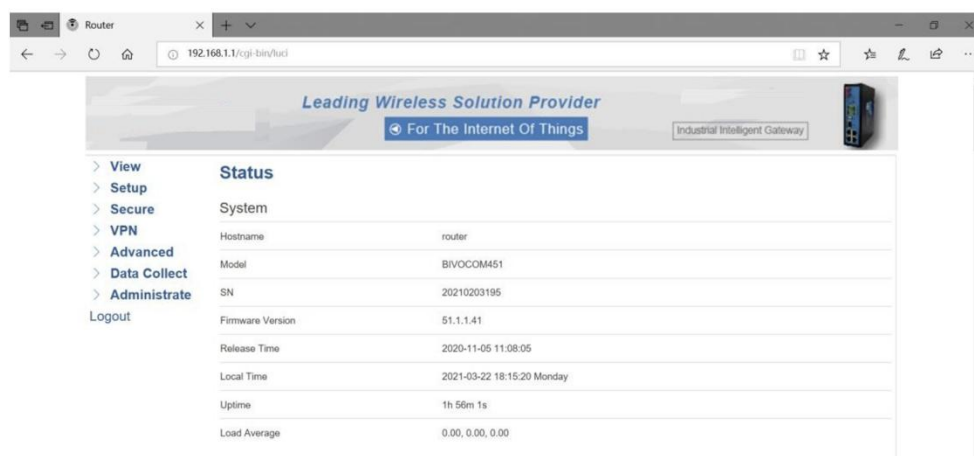
3.0 Getting start Web UI

G6500 provide visible and easy-to-use WebUI for configuration setting and management. Below sections indicate each menu items feature introduce and setting on WebUI.

3.0.1 Connect your PC to G6500 network.

- Using an Ethernet cable, connect one end of the Ethernet cable to the LAN port on G6500 unit and the other end to a LAN port on a PC.
- Or use your laptop to connect to WIFI hotspot from G6500, login with default password: "admin123".
- If your PC is configured to automatically get an IP address, it will obtain the IP address from the G6500 DHCP. Otherwise, make sure your PC can connect to the network 192.168.1.0 (255.255.255.0).

3.0.1 Login the WebUI



Enter 192.168.1.1 into the address bar of your PC web browser. Login with user name and password both "admin" as default. A web page with menu items will guide you start the configuration.



3.1 View

View page shows the basic system information including System, Network, Routes, System Log, VPN Status. Checking the following details information.

3.1.1 System

System page show you an overview of G6500 information like SN, Firmware version, Memory usage, etc.

Status

System

Hostname	router
Model	G6500
SN	20210203195
Firmware Version	51.1.1.41
Release Time	2020-11-05 11:08:05
Local Time	2021-03-23 11:50:43 Tuesday
Uptime	19h 31m 23s
Load Average	0.43, 0.20, 0.07

Memory

Total Available	102812 kB / 124320 kB (82%)
Free	83824 kB / 124320 kB (67%)
Cached	14592 kB / 124320 kB (11%)
Buffered	4396 kB / 124320 kB (3%)

3.1.2 Network



Network page display the current WAN status, like network type, IP address, Connect Status, and so on.

View

System

Network

Routes

System Log

VPN Status

Setup

Secure

VPN

Advanced

Data Collect

Administrate

Logout

Status

Network

IPv4 WAN Status

 **Type:** lte
Address: [10.191.11.21](#)
Netmask: 255.255.255.252
Gateway: [10.191.11.22](#)
Mac Address: 22:60:1d:d3:83:0a
DNS 1: [202.103.44.150](#)
DNS 2: [202.103.24.68](#)
Connected: 6h 37m 4s
 **Signal:** 26 (-61 dBm)
Network: LTE
SIM Status: ON
IMEI: 357621093350256
ICCID: 89860320960275206273
Connect Status: CONNECTED

Online Status online

Active Connections

35 / 16384 (0%)

LAN Status

IP Address	192.168.1.1
Netmask	255.255.255.0
DHCP Server	Enable
Mac Address	00:52:24:34:2f:4f



3.1.3 Routing Tables

Display ARP list and active routing tables.

Routes

The following rules are currently active on this system.

ARP

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

Active IPv4-Routes

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

Active IPv6-Routes

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

3.1.4 System Log

System log page continuously print the current running status system log. It is useful for troubleshooting when there are some features not working as expected. System log page provide three buttons for “Clear Log” which empty current printed log, “Save Log” which saving current printed log as a file, and “Refresh Log” which asking print out latest 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

```

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

```

3.1.5 VPN Status

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

VPN

VPN Status

Type:	L2tp
IP Address:	1.32.1.3
Netmask:	255.255.255.255
Gateway:	1.32.1.1
Connected Time:	9m,32s

3.2 Setup

Setup page includes WAN, LAN, Wireless, Wireless Client, Online Detection, Diagnostics menus, which is for you configuring the features accordingly.

3.2.1 WAN

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

- "Static IP" is for G6500 setting static IP address to connect to upper network via WAN port.
- "DHCP" is for G6500 obtain network from Upper DHCP device (like router) via WAN port.
- "PPPoE" is for getting network via PPPoE protocol, normally you will get username password from carrier when you purchase a network.
- "3G" is for dialing up 3G or NBIOT cellular network when using a 3G SIM card or a NBIOT SIM card. You may need input APN, PIN, PAC/CHAP Username Password if your SIM card provider request.
- "LTE" is for dialing up 4G/LTE cellular network when using a 4G SIM card. You may need input APN, PIN, PAC/CHAP Username Password if your SIM card provider request.
- "Unmanaged" is for disabling WAN connection.

WAN Setting

On this page, you can configure WAN port connection type

WAN Interface

General Settings

Advanced Settings

Connection Type

Network Type

APN

PIN

User Name

Password

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

Note,

- 1) PAP/CHAP Username password Only when you are using a private network SIM card, if you're using public network SIM card, just keep it as null.
- 2) Choose Dial Number when you are using 3G type, different carriers may have different dial number, please ask your carrier for this info if you have questions.

3) WAN Used As LAN

When using LTE/3G connection type to access internet, which mean WAN port is available for you change it as a LAN port.

"Advanced Settings" menu provide this option

WAN Setting

On this page, you can configure WAN port connection type

WAN Interface

General Settings

Advanced Settings

Use Static IP Address ☐

WAN Multiplex ☒  Set WAN port as LAN port



3.2.2 LAN

Menu of LAN are mainly for configuring IP address of G6500, set the IP address range of DHCP server, or disable DHCP.

1) Common Configuration

Common Configuration

General Setup

Advanced Settings

Protocol

Static address

▼

IPv4 address

192.168.1.1

IPv4 netmask

255.255.255.0

▼

DNS Servers

+

IPv4 Address

To configure IP address of LAN port.

IPv4 Netmask

The netmask of LAN port IP address.

IPv4 Gateway

Specify the next-hop routing gateway.

DNS Server

To specific DNS server, leave it blank as default using upper network DNS.

Advanced Settings

Specific set Override MTU, and use gateway metric. Leave it blank as default.

2) DHCP Server Settings

General Setup

Ignore interface

☐ Disable DHCP for this interface.

Start

100

Lowest leased address as offset from the network address.

Limit

150

Maximum number of leased addresses.

Leasetime

12h

Expiry time of leased addresses, minimum is 2 minutes (2m).

- **Disable DHCP**

Click to disable DHCP server.

- **Start**

Assign the IP address of DHCP server. For example, 100 means IP address starts from 192.168.1.100.

- **Limit**

Assignable number of IP 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

Wireless menu is mainly for configuring the WiFi, SSID, mode, encryption, etc.

Wireless Setting

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

Interface Configuration

General Settings

Advanced Settings

WiFi 2.4G ☒ Enable ☐ Disable

Network Name(SSID)

auto

Channel

auto

Mode

802.11bgn

Encryption

WPA2-PSK-AES

Key

••••••••



Hide SSID

☐

1) WIFI 2.4G

Provide Enable or Disable option for the WIFI function switch.

2) Network Name (SSID)

WIFI network name setting.

3) Channel



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

4) Mode

Support 802.11b, 802.11g, 802.11bg, 802.11bgn options. This may related to the maximum speed of WiFi. 802.11b up to 11Mbps, 802.11g up to 54Mbps and 802.11bgn up to 300Mbps.



5) Encryption

Configure the way of encryption,

WPA2-PSK-AES

▼

No Encryption

WPA2-AES-RADIUS

WPA2-PSK-AES

WPA-PSK-AES

While for RADIS option, it provide for configuring Radius Auth Server address, shared key, etc.

Encryption	WPA2-AES-RADIUS ▼
Radius Auth Server Address	
Radius Auth Server Port	1812 Default: 1812
Radius Shared Key	
Radius Key UPdate Interval	Seconds

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.

Advanced Settings related to some specific parameters setting, this is for professional users, contact our support team in case you have further questions.

3.2.4 Wireless Client

Wireless Client menu provide connecting network from local WiFi Hotspot, this setting
YH IoT Technology Visit us: www.yhiott.com Email: service@yhiott.com

related to WAN setting when you select Static IP or DHCP connection type.

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

> View

> Setup

WAN

LAN

Wireless

Wireless Client

Online Detection

Diagnostics

> Secure

> VPN

> Advanced

> Data Collect

> Adminstrate

Logout

Save and Apply on page WAN after Join

Enable 2.4G Wireless Client

▼

Apply

Scan WiFi

Scanned WiFi

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

3.2.5 Online Detection

Online detection feature checking the network connection status periodically, if there has issue of connection, router will auto reconnect. If it fails to reconnect after times of trial, router will reboot automatically to try to recovery the network.

Online Detection

Online Detection

☒ Enable
 ☐ Disable

Detection Type

Ping

▼

Primary Detection Server

8.8.8.8

Second Detection Server

114.114.114.114

Retry Times

3

Retry Interval

60

Seconds

Enable Reboot

☒ Enable
 ☐ Disable

Reboot After Interval

30

Minutes



1) Detection Type

There are 3 types: ping, traceroute and DNS.

- **Ping**

Router will ping an IP address periodically, 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 data flow 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.

3.2.6 Diagnostics

Diagnostics feature allow user check the network connection status manually.

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

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

Diagnostics

Network Utilities



The screenshot shows the 'Network Utilities' section with three input fields and three buttons. The first field contains '8.8.8.8', the second '8.8.8.8', and the third 'www.google.com'. Below the first field is a dropdown menu set to 'IPv4' and a 'Ping' button. Below the second field is a 'Traceroute' button. Below the third field is an 'Nslookup' button. The output area shows the results of a ping command to 8.8.8.8.

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

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

1) Ping

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

2) Traceroute

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

3) Nslookup

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

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. It provide select source zone from VPN or WAN if there is a VPN



connection available.

DMZ

Set DMZ Host

DMZ ☒ Enable ☐ Disable

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

DMZ Host

3.3.2 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	
myPLC	IPv4-TCP, UDP From <i>any host</i> in <i>wan</i> Via <i>any router IP</i> at port <i>501</i>	IP <i>192.168.1.244</i> , port <i>501</i> in <i>lan</i>	☒	Edit Delete

New port forward:

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

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. There are more setting items when click "Edit" button.

3.3.3 Traffic Rules

Traffic rules is used for Firewall setting like opening some ports on router, such as remote access the configuration page of router, you can open port 80.

Firewall - Traffic Rules

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

Traffic Rules

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

Open ports on router:

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

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

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 rule	lan	wan

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

Rule is enabled Disable

Name

Restrict to address family

Protocol

Match ICMP type

Source zone

☐ Any zone

☒ lan: lan: 

☐ wan: wan: 

Source MAC address

Source address

Source port

Destination zone

☐ Device (input)

☐ Any zone (forward)

☐ lan: lan: 

☒ wan: wan: 

Destination address

Destination port

Action

Extra arguments Passes additional arguments to iptables. Use with care!

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 only professional users who 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.

G6500 support several types of VPN: PPTP, L2TP, IPSec, OpenVPN and GRE.

3.4.1 PPTP

You can configure either PPTP client or PPTP server, but it can't use both of them at the same time, 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 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) 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 Setting

Setting L2TP

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



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 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 Setting

Setting L2TP

L2TP Client ☐ Enable ☒ Disable

L2TP Server ☒ Enable ☐ Disable

Server Local IP

IP Address Range eg: 10.10.10.100-10.10.10.200

Enable MPPE Encryption ☒

Enable IPsec ☒

Pre Shared Key 

NAT ☐

CHAP Secrets eg: test * test *

Client Subnet eg: test 192.168.10.0 255.255.255.0

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

Set OpenVPN Parameters

OpenVPN ☒ Enable ☐ Disable

Topology

Role

Protocol

Port

Device Type

OpenVPN Server

Authentication Type

CA

Public Certificate

Private Key

DH

TLS Authentication Key

Peer Subnet Address eg: 192.168.10.0

Peer Subnet Mask eg: [255.255.255.0](#)

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, 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

Negotiation Method

Tunnel Type

Local Subnet

Peer Subnet

IKE Encryption Algorithm

IKE Integrity Algorithm

Diffie-Hellman Group

IKE Life Time

Authentication Type

Pre-shared Key

Local Identifier

Peer Identifier

ESP Encryption Algorithm

ESP Integrity Algorithm

DPD Timeout seconds

DPD Detection Period seconds

DPD Action

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.

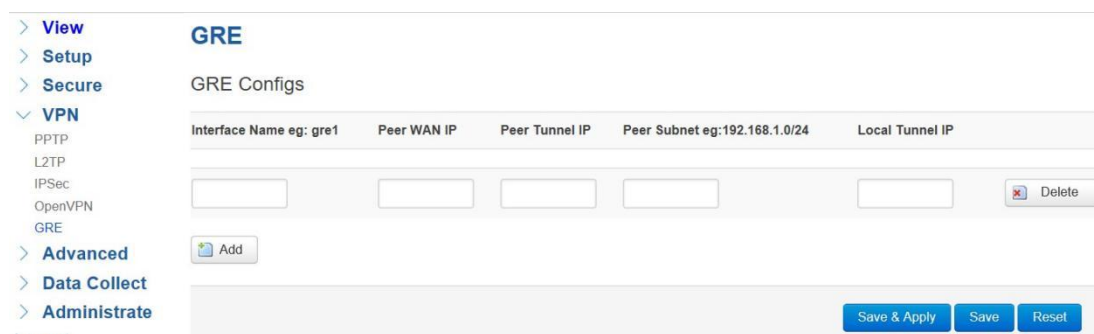
9) Peer Identifier

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

10) ESP Encryption Algorithm

The encryption method of ESP.

3.4.5 GRE



The screenshot shows the 'GRE' configuration page. On the left is a sidebar menu with options: View, Setup, Secure, VPN (selected), Advanced, Data Collect, and Administrative. Under 'VPN', there are sub-options: PPTP, L2TP, IPSec, OpenVPN, and GRE. The main area is titled 'GRE' and 'GRE Configs'. It contains a table with columns: Interface Name eg: gre1, Peer WAN IP, Peer Tunnel IP, Peer Subnet eg:192.168.1.0/24, and Local Tunnel IP. Below the table is an 'Add' button. At the bottom right are 'Save & Apply', 'Save', and 'Reset' buttons.

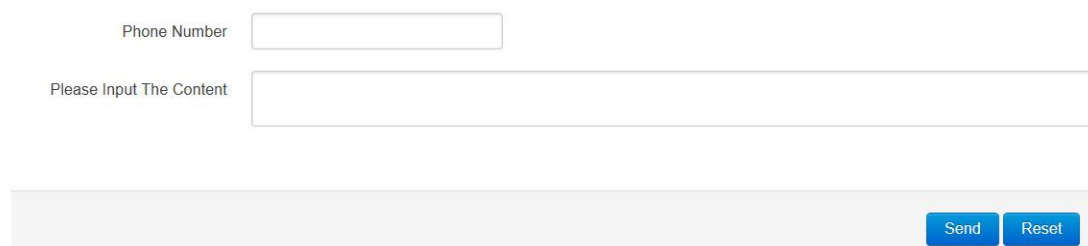
3.5 Advanced

Advanced menu include some advanced functions for your usage, like send SMS, traffic monitor, GPS location, SNMP, etc.

3.5.1 Send SMS

G6500 provide window for sending out Short Message to certain numbers with configurable content.

Send Short Message



The screenshot shows the 'Send Short Message' form. It has two input fields: 'Phone Number' and 'Please Input The Content'. At the bottom right are 'Send' and 'Reset' buttons.

3.5.2 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 ▼		255.255.255.2		0	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.

3.5.3 DI DO

G6500 provide DI DO configuration page for setting up DI and Relay ports on G6500. It displaying the real-time status of DI0 and DI1. Also support manually change the relay Close or Open. And support "Enable Alarm" to connect and report the status changes to a server. What's more, it support SMS alarm to monitoring the DI status change.

DI DO Control

DI status

DI0 Status	DI1 Status
0	0

Relay0 Setting ☐ Close ☒ Open

Relay1 Setting ☐ Close ☒ Open

Enable Alarm ☒ Enable ☐ Disable

Server Address

Server Port

Protocol

Register Packet Maximum 64 Bytes Ascii

Customed Heartbeat Maximum 64 Bytes Ascii

Heartbeat Interval 0 Means Not To Send

Device ID One Byte Only

Enable Short Message Alarm ☒

Alarm Type

Phone Number

Message Content Maximum 63 English Character

3.5.4 Net Flow

The traffic meter function of G6500 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.

Traffic Meter

Current Day Flow	Current Month Flow
0.0G	0.0G

Net Flow

Net Flow ☒ Enable ☐ Disable

Limit Enabled ☒

Day Limit M

Month Limit M

Clear Day Flow

Clear Month Flow

3.5.5 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**
 - Send SMS
 - Static Routes
 - Net Flow
 - GPS Location
 - BS Location
 - Dynamic DNS
 - SNMP
 - DHCP and DNS
- > Data Collect
- > Administrate
- Logout

GPS Location

GPS Location ☒ Enable ☐ Disable

GPS Source ☒ External ☐ Dongle

Output Mode Output To Network ▼

Server Address 192.168.1.100

Server Port 9010

Report Mode Pure TCP ▼

User Defined Register Packet ⓘ Max 128 Bytes ASCII

User Defined Heartbeat Packet ⓘ Max 128 Bytes ASCII

Report Interval 60 ⓘ Seconds

Heartbeat Interval 30 ⓘ Seconds

GPS Info

Connection Status -

GPS Source: External for getting GPS data from independent GPS module (Option), while Dongle for getting GPS data from cellular module which may not so accurate.

Output Mode: Output to network, or output to serial which through RS232 port.

Server Address: The IP address of server that receive GPS data if the output mode as “Output to Network”, which is based on TCP or UDP connection.

Server Port: The port of server.

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

3.5.6 BS Location (Option)

Base station location is to locate the G6500 by obtaining the nearest base station number, this function is mainly for rough location of indoor application.

Enter the server IP address and port that you want to report the location of router, then router will auto report its location to server regularly(within the interval time you set).

BS Location ☒ Enable ☐ Disable

Server Address 192.168.1.100

Server Port 6004

Report Interval 60 ⓘ Seconds

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.

3.5.7 Dynamic DNS

If the assigned public IP address of router is dynamic and changes frequently, you can enable DDNS function, while allows you to register a domain to bundle with the IP address, in this case, no matter what the IP address changed, it will direct to your registered domain.

DDNS ☒ Enable ☐ Disable

Service Type

User Name

User Password 

Host Name

- **Service Type**

There are several types of DDNS service supported in router, as below.

DynDNS.org
freedns.afraid.org
ZoneEdit.com
No-IP.com
3322.org
easyDNS.com
TZO.com
DynSIP.org
custom
Oray

- **User Name**

The username you register at DDNS service provider.



- **User Password**

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

- **Host Name**

The register domain you want to bundle.

3.4.8 SNMP

G6500 router provide SNMP feature for manage the device via SNMP. Configure the relevant settings accordingly.

SNMP Setting

SYSTEM

Enable	Enable
Location	Unknown
Contact	root
Name	top-iot

RO/RW Community

PUBLIC

Security Name	ro
Source Address	default
Community	public

PRIVATE

Security Name	rw
Source Address	localhost
Community	private

3.5.9 DHCP and DNS

G6500 provide DHCP and DNS setting via Dnsmasq package, it support configure DHCP server related settings and DNS forwarding setting if your network request specific parameters. Also support set static Leases. Normally leave it as default.

DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

General Settings
Resolv and Hosts Files
TFTP Settings
Advanced Settings

Domain required ☒ Don't forward DNS-Requests without DNS-Name

Authoritative ☒ This is the only DHCP in the local network

Local server Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only

Local domain Local domain suffix appended to DHCP names and hosts file entries

Log queries ☐ Write received DNS requests to syslog

DNS forwardings List of DNS servers to forward requests to

Rebind protection ☒ Discard upstream RFC1918 responses

Allow localhost ☒ Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist List of domains to allow RFC1918 responses for

Active DHCP Leases

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

Collecting data...

Static Leases

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

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

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

This section contains no values yet

Add

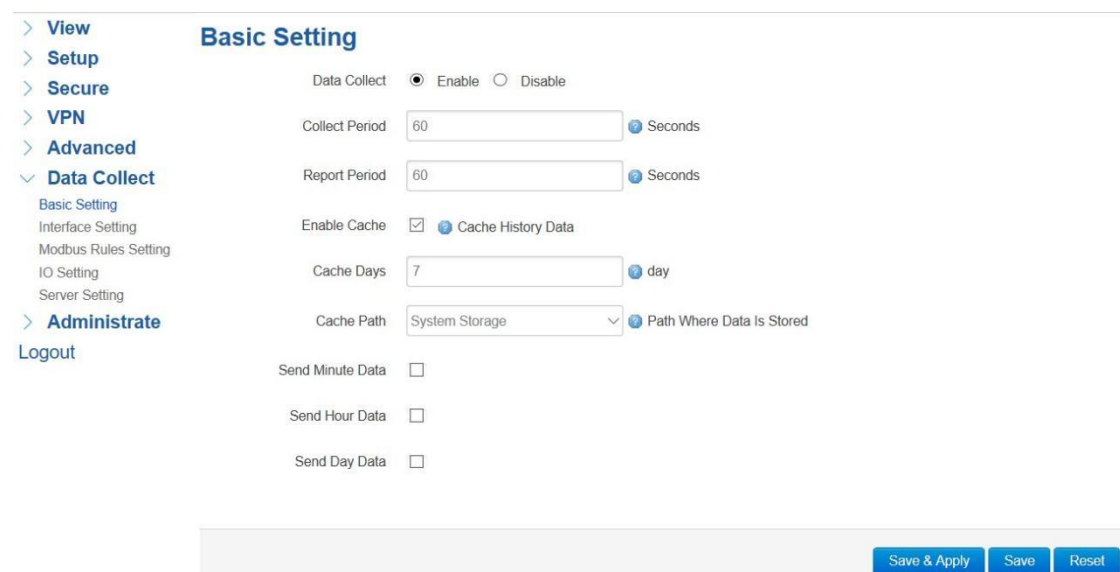
Save & Apply Save Reset

3.6 Data Collect

Data Collect settings is for G6500 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.



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

3.6.2 Interface Setting

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

Interface Setting

COM1/RS485

COM2/RS232

Enabled ☒ Enable ☐ Disable

Baudrate

Databit

Stopbit

Parity

Frame Interval ms

COM Protocol

Modbus TCP Server Setting

Modbus Server1

Modbus Server2

Modbus Server3

Modbus Server4

Modbus Server5

Enabled ☒ Enable ☐ Disable

Server Address

Server Port

Transaction ID 0~65535

Protocol ID 0~65535

GPS Device

Must Enable GPS On Page Advanced/GPS Location First

GPS ☐ Enable ☒ Disable

3.6.3 Modbus Rules Setting

Modbus Rules Setting is for G6500 as a Modbus master to acquire data from slave devices based on Modbus protocol. You can configure unlimited Modbus rules on it. G6500 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
 - Server 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	PH_sensor	COM1	temperature	1	4	0	1	unsigned 16Bits AB	1	☒	Edit Delete

New Modbus Rule

Order	Device Name	Interface	Factor Name	Device ID	Function Code	Start Address	Count	Data Type	Reporting Center	
		COM1		0~255	0~255	0~65535	1~120	Unsigned 16Bits	1-2-3-4-5	Add

Click “Edit” button for more details setting,

Modbus Rules - PH_sensor - COM1

enabled
[Disable](#)

Order

Device Name

Belonged Interface COM1

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 Unsigned 16Bits AB A highest byte

Reporting Center Multiple Servers Are Separated By Minus

Unit Multiple Units Are Separated By Semicolon

Operator / 0 + - * /

Operand

Accuracy 1 0~6

3.6.4 IO Setting

Since G6500 provide 2 DI and 2 Relay ports, it is possible to detect their status and report to server via JSON format, which take “Factor Name” as individual parameter.

IO Setting

DI Setting

Device Name	DI Channel	Factor Name	Mode	Reporting Center	Enable	
door_sensor	DI1	front_door	Status Mode	1	☒	 Edit  Delete

New DI Channel:

Device Name	DI Channel	Factor Name	Mode	Reporting Center	
	DI1 v		Status Mc v	1-2-3-4-5	 Add

Relay Setting

Device Name	Relay Channel	Factor Name	Reporting Center	Relay Control	Enable	
AC_engine	Relay1	AC_on	1	Open	☒	 Edit  Delete

New Relay Channel:

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

3.6.5 Server Setting

Server setting menu allows user set the data center address with multiple protocols, the standard G6500 support TCP, UDP, HTTP, MQTT, and Modbus TCP. For the data format, G6500 support different Encapsulation type, include "Transparent", "Json", and "HJ212" (special for some Environment SCADA). Also G6500 accept customize specific protocols for your data center.

Server Setting

Server1 Settings Server2 Settings Server3 Settings Server4 Settings Server5 Settings

Enabled ☒ Enable ☐ Disable

Protocol

Encapsulation Type

Server Address

Server Port

MQTT Public Topic

MQTT Subscribe Topic

MQTT Username

MQTT Password

Client ID

Enable TLS/SSL ☒

Certificate Type

Enable Self Defined Variable ☐

3.7 Administrate

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

3.7.1 System

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

- > 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
- Logout

System

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

System Properties

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

3.7.2 Password

To revise the password of router.

Admin Password

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

Origin Password	•••••	
Password		
Confirmation		

3.7.3 Time Setting

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



Set System Time

Current system time 2021-03-19 15:24:14

System Time Type ☐ ntp ☒ rtc

Current RTC Time 2021-03-19 15:24:14

RTC Date eg: 2016-01-01

RTC Time eg: 12:00:00

1) Current System Time

Display the time of router.

2) System Time Type

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

● RTC

You can update data and time yourself.

RTC Date eg: 2016-01-01

RTC Time eg: 12:00:00

RTC Data

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

RTC Time

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

● NTP

NTP Time Server

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	/var/log/	▼
Log Size	64	KB
Log Server	0.0.0.0	
Log Server Port	514	
Output Level	Debug	▼

1) Output to Device

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

2) Log Size

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

3) Log Server

Set up the IP address of log server.

4) Log Server Port

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

5) Output Level

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

3.7.5 Backup and Reset

User can either backup the configuration of router as a .gz file, or reset all settings to factory defaults.

Backup / Restore

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

Download backup:

Reset to defaults:

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

Restore backup: 未选择文件。

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

Router upgrade page provide upgrade firmware via WebUI. Before upgrade the firmware for router, please ensure the firmware you're planning to upload is correct one, otherwise that may cause device crash.

Flash operations

Flash new firmware image

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

Image: 未选择文件。

1) Choose and Upload Firmware Image

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

Flash Firmware - Verify

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

Click "Proceed" below to start the flash procedure.

Checksum: **f68983dbe5ec7f0d4bf9258e421ad53d**

Size: 9.00 MB

Configuration files will be kept.

- **Checksum**

MD5 checksum value of firmware.

- **Size**

The size of firmware.

- **Proceed**

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

3.7.7 Remote Management

Remote Management feature allows G6500 **connect with our IoT Management Platform** identify by Device Number 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.

- > View
- > Setup
- > Secure
- > VPN
- > Advanced
- > Data Collect
- > **Administrative**
 - System
 - Password
 - Time Setting
 - Log Setting
 - Backup and Restore
 - Router Upgrade
 - Remote Configured
 - Manual Reboot
 - Schedule Reboot
- Logout

Remote Configured

Remote Configured ☒ Enable ☐ Disable

Server Address

Server Port

Heart Interval

Device Number

Connection Status Registered

Once it registered, on the Device management platform, you will see the connection status as “Online” and you can configure it via DMP WebUI.

admin > Super Administrator

Device Management

My Desktop

Device List

Device List

GIS Map

Statistical Analysis

System Management

Bivocom

XiaMen branch

XiaMen one group

XiaMen two group

XiaMen three group

ShenZhen branch

qqqq

Jimei District

Siming District

Home > Device Management > Device List

+ Add

+ Delete

+ Configuration

--Online Status--

--Network S--

Device Number/Device Name

Lookup

Online Device: 1/4

☐	Device ...	Device ...	Device ...	Device ...	SIM Car...	Carrier	Online ...	Networ...	Signal	Latest Online Time	Remarks	Operati...
☐	20210319	Bivocom ...	Router	TR321	1391234...	Telecom	Online	Wired	--	2021-03-19 15:53:50	--	
☐	20200911	TG452	Data acq...	TG452	1234567...	Unicom	Outline	--	--	2021-01-19 16:19:34	test	
☐	20200918	TR321	Router	TR321-LF	1865001...	Unicom	Outline	--	--	2020-10-23 16:34:17	Demo	
☐	10000001	45454	Router	TJ710	1896545...	Telecom	Outline	--	--	2020-09-12 17:04:30	1000	

首页

上一页

1

下一页

尾页

1) 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.

2) Server Port

The specified login server port.

3) Heartbeat Interval

The heartbeat time interval (Unit: second)



4) Device Number

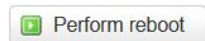
Define an individual Device ID for router and as identify on DMP.

3.7.8 Manual Reboot

Reboot

Reboots the operating system of your device

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

 Perform reboot

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 feature allow you preset the rules of device reboot, by period interval or by a certain time point.

Schedule Reboot

Enable Schedule Reboot ☒ Enable ☐ Disable

Schedule Type ☒ By Period ☐ By Time

Period Interval  Minutes, Min 5

3.8 Logout

Click the Logout menu to logout the webUI of G6500.