



Collie

(GL-X300B)

USER MANUAL

Table of Contents

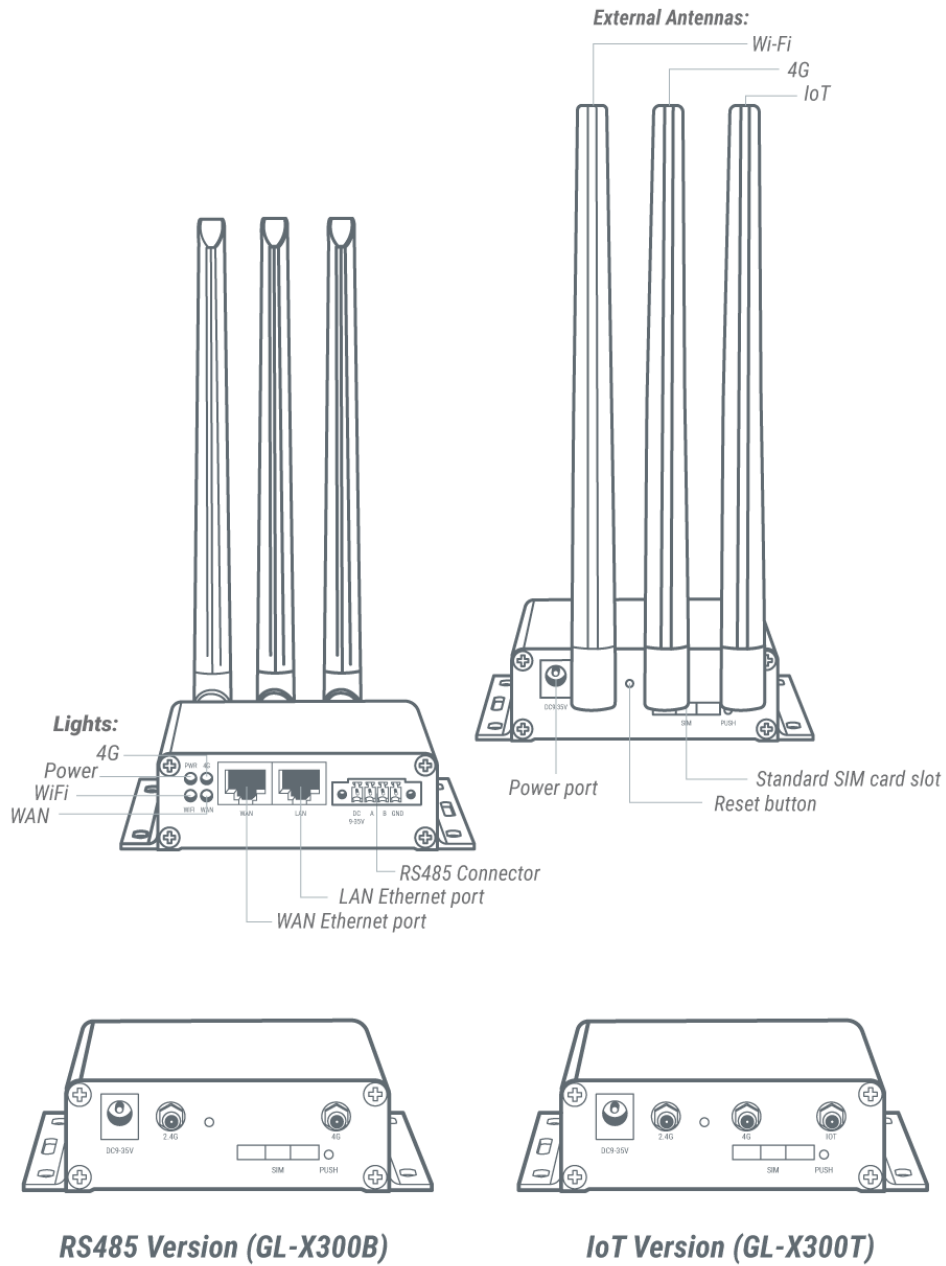
1. Getting Started with GL.iNet Collie.....	1
1.1. Power on.....	2
1.2. Connect.....	3
(1) Connect via LAN.....	3
(2) Connect via Wi-Fi	4
1.3. Access the Web Admin Panel.....	4
1) Language Setting	4
2) Admin Password Setting	5
3) Admin Panel.....	6
2. INTERNET	7
2.1. Cable.....	8
(1) DHCP	9
(2) Static.....	10
(3) PPPoE.....	10
2.2. Repeater.....	11
2.3. 3G/4G Modem.....	12
AT Command	14
3. WIRELESS	15
4. CLIENTS.....	17
5. UPGRADE.....	18
5.1. Online Upgrade.....	18
5.2. Upload Firmware	19
(1) Official OpenWrt/LEDE firmware.....	20
(2) Compile your own firmware	20
5.3. Auto Upgrade	20
6. FIREWALL	21
6.1. Port Forwards	22
6.2. Open Ports on Router	23
6.3. DMZ.....	23
7. VPN.....	24
8. RS485	27

8.1.	Config.....	27
8.2.	Socket (RS485 to TCP/UDP).....	28
8.3.	MQTT.....	32
9.	APPLICATIONS.....	35
9.1.	Plug-ins.....	35
9.2.	Remote Access.....	36
	Cloud Management.....	37
	DDNS.....	37
9.3.	Captive Portal.....	38
10.	MORE SETTINGS	38
10.1.	Admin Password.....	38
10.2.	LAN IP	39
10.3.	Time Zone	40
10.4.	MAC Clone.....	41
10.5.	Custom DNS Server.....	42
10.6.	Network Mode.....	43
10.7.	Revert Firmware	44

1. Getting Started with GL.iNet Collie

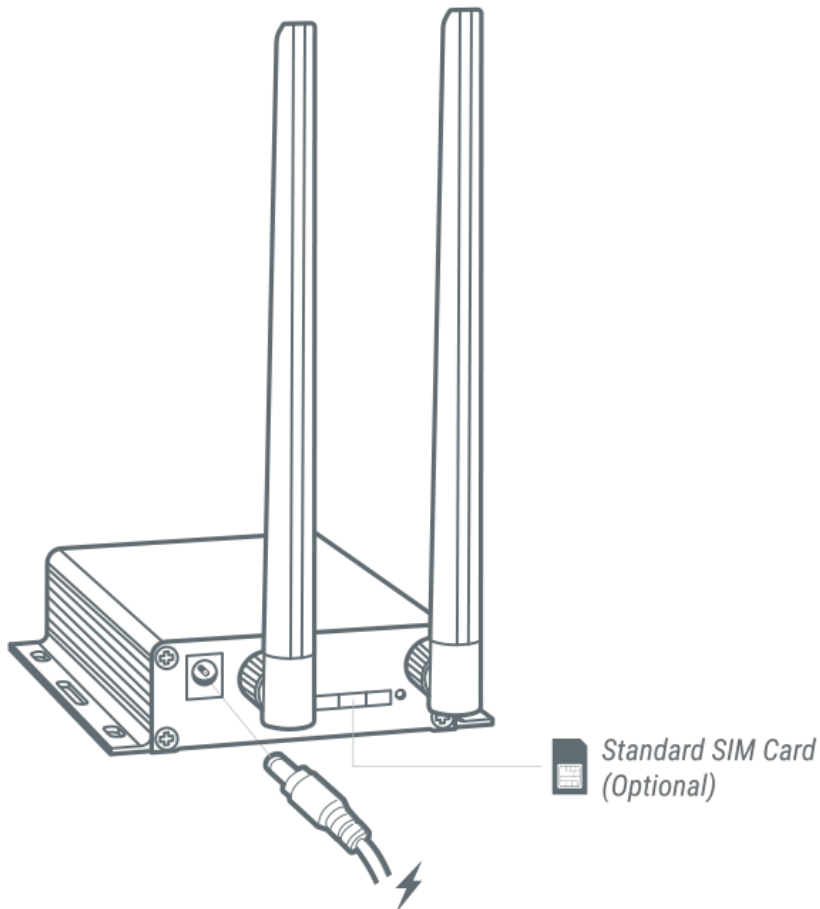
Model:

GL-X300B



1.1. Power on

Plug the power cable into the power port of the router. Make sure you are using a standard **DC 12V/1.0 A** power adapter. Otherwise it may cause malfunction.



*Note: Hot plug for SIM card is **not** supported. If you want to use, please insert SIM card before powering on the router.*

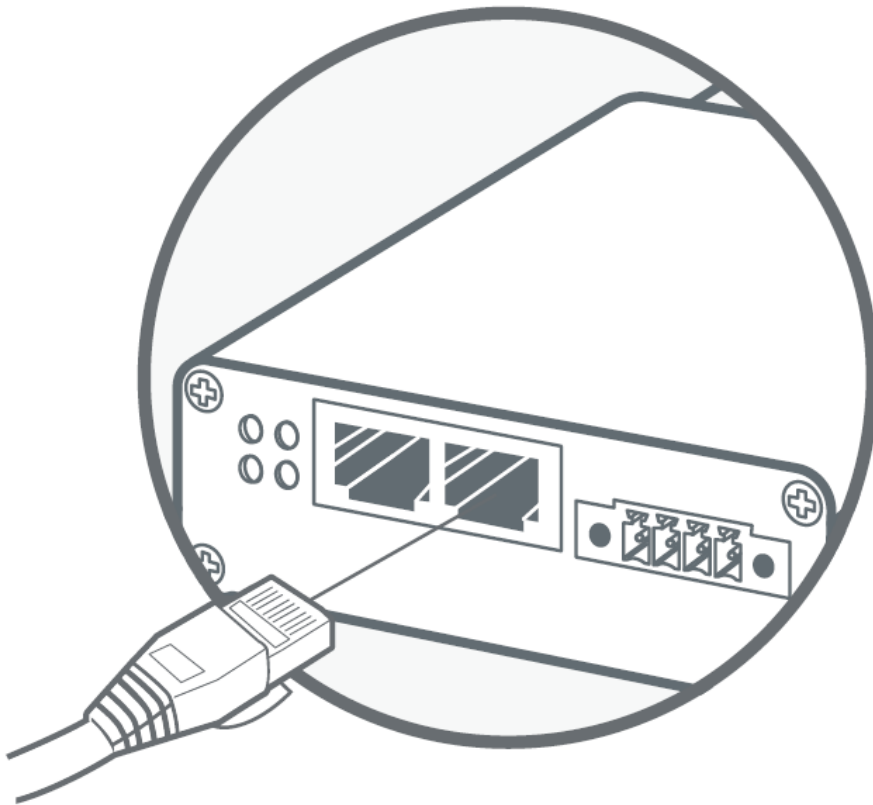
1.2. Connect

You can connect to the router via Ethernet cable or Wi-Fi.

Note: This step only connects your devices to the local area network (LAN) of the router. You cannot access the Internet currently. In order to connect to the Internet, please finish the setup procedures below and then follow [Internet](#) to set up an Internet connection.

(1)Connect via LAN

Connect your device to the LAN port of the router via Ethernet cable.



*Plug the cable connecting
to your computer into LAN port*

(2)Connect via Wi-Fi

Search for the SSID of the router in your device and input the default password: **goodlife**.

Note: The SSID was printed on the bottom label of the router with the following format:

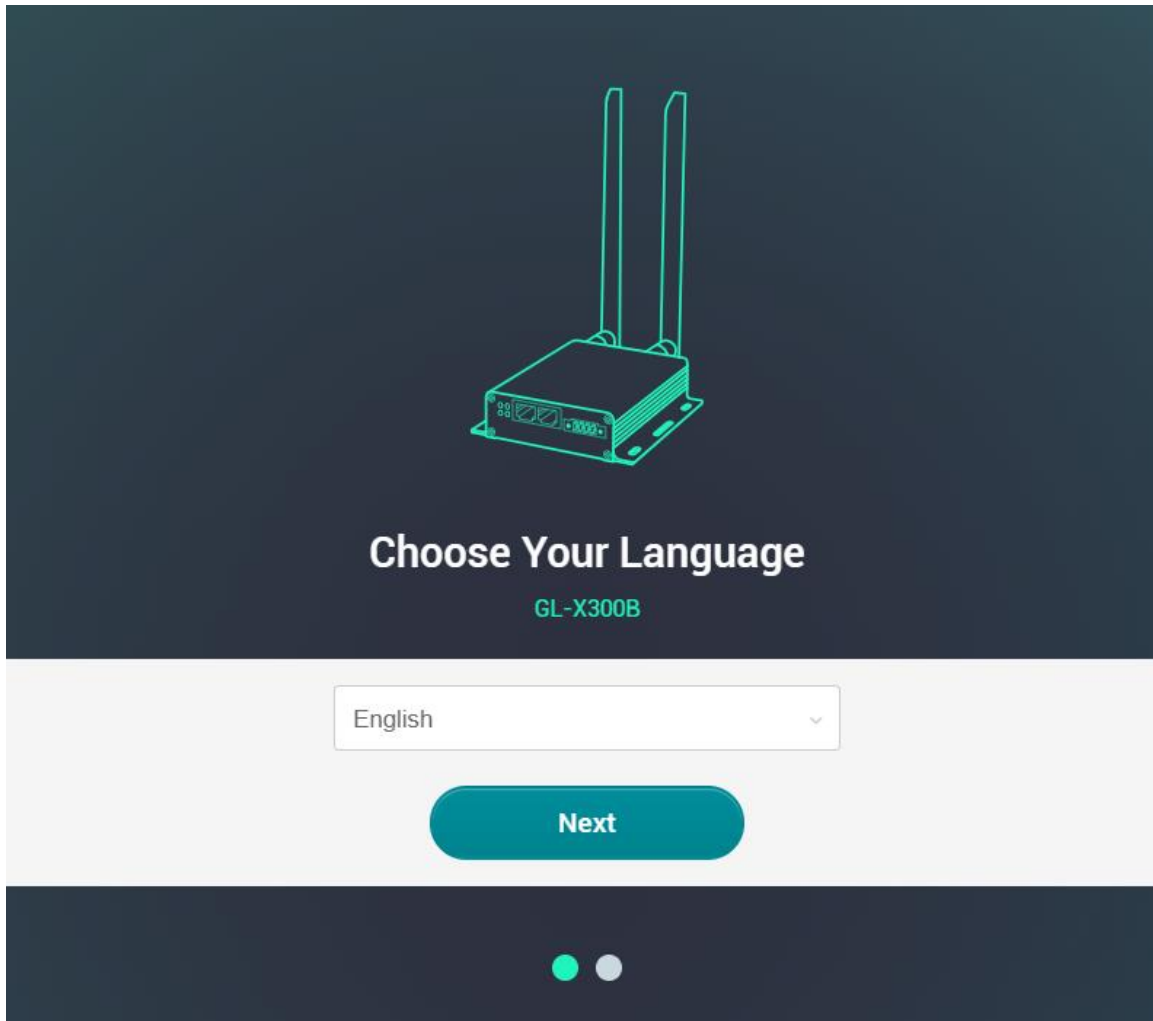
- **GL-X300B-XXX**

1.3. Access the Web Admin Panel

Open a web browser (we recommend Chrome, Firefox) and visit <http://192.168.8.1>. You will be directed to the initial setup of the web Admin Panel.

1) Language Setting

You need to choose the display language of the Admin Panel. Currently, our routers support **English**, 简体中文, 繁體中文, **Deutsch**, **Français**, **Español**, **Italiano**, 日本語 and 한국어.



2) Admin Password Setting

There is no default password for the Admin Panel. You have to set your own password, which must be at least 5 characters long. Then, click Submit to proceed.

Set Up Your Admin Password

New Password At least 5 characters

Confirm Password Must be identical to above

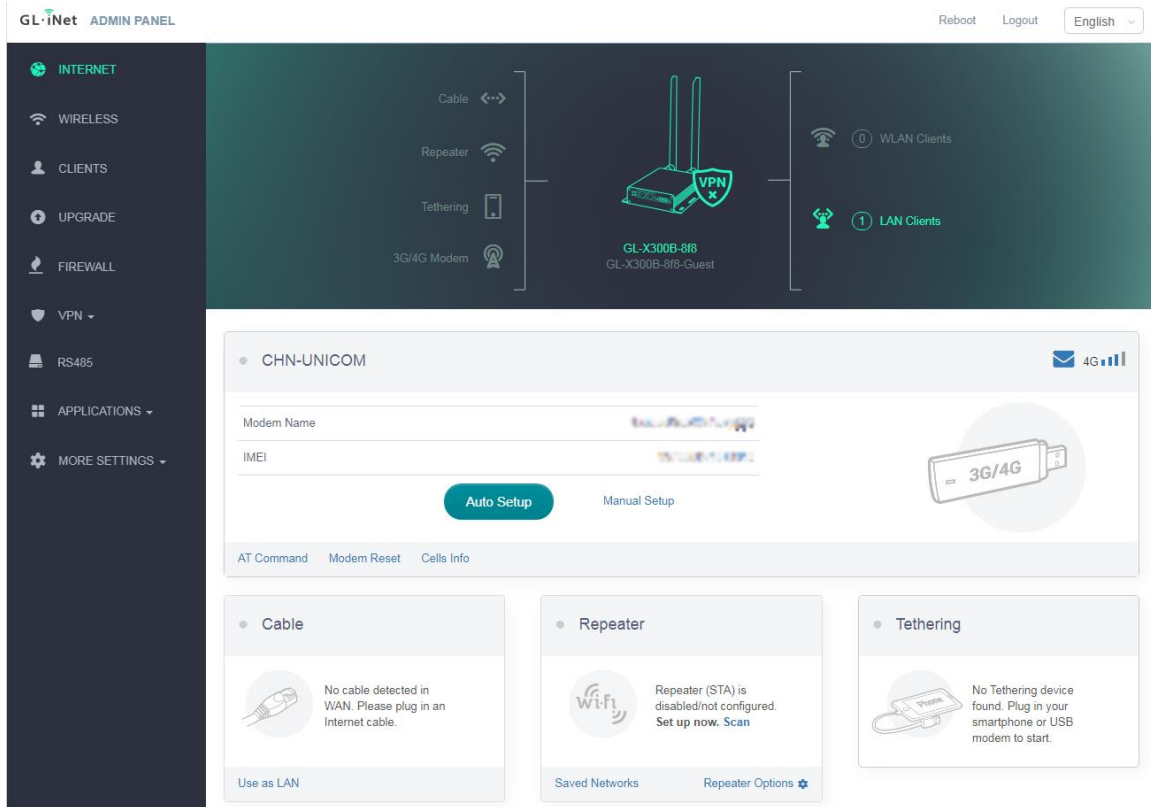
Your admin password will be used for configuring everything on the Admin Panel of your router. It is EXTREMELY important to keep it safe.

[Back](#) [Submit](#)

Note: This password is for this web Admin Panel and the embedded Linux system. It will not change your Wi-Fi password.

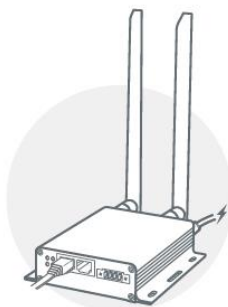
3) Admin Panel

After the initial setup, you will enter the web Admin Panel of the router. It allows you to check the status and manage the settings of the router.



2. INTERNET

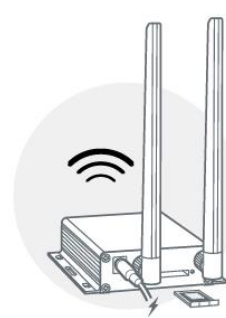
There are total 3 types of connection method that you can use to access the Internet: **Cable, Repeater, 3G/4G Modem.**



1 Cable

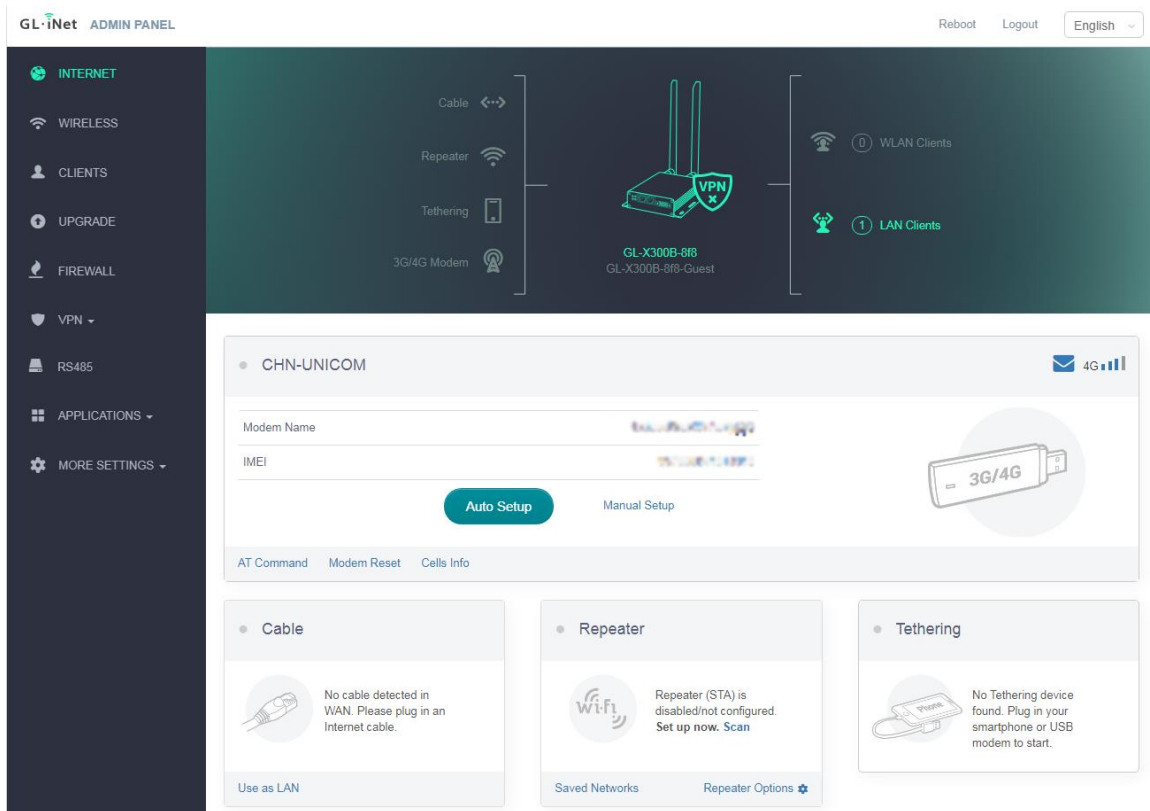


2 Repeater



3 3G/4G Modem

Click INTERNET to create an Internet connection.



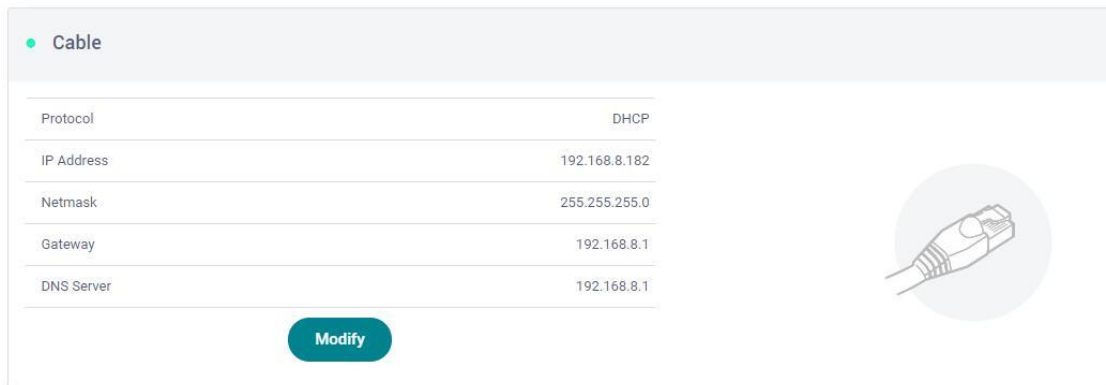
2.1. Cable

Connect the router to the modem or main router via Ethernet cable to access the Internet.

Before plugging the Ethernet cable into the WAN port of the router, you can click Use as LAN to set the WAN port as a LAN port. That is useful when you are using the router as a [repeater](#). As a result, you can have one more LAN port.

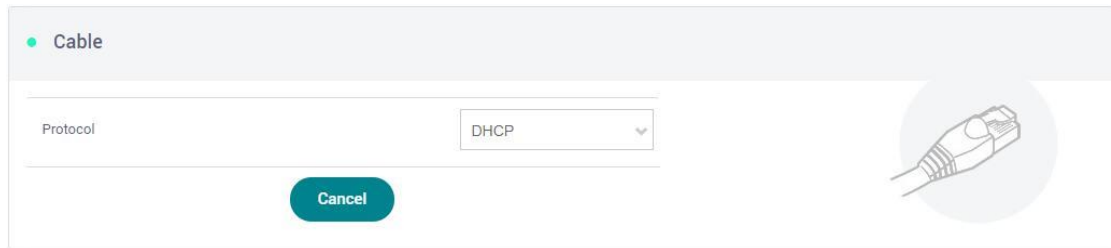


Plug the Ethernet cable into the WAN port of the router. The information of your connection will be shown on the Cable section. DHCP is the default protocol. You can click Modify to change the protocol.



(1)DHCP


DHCP is the default and most common protocol. It doesn't require any manual configuration.



• Cable

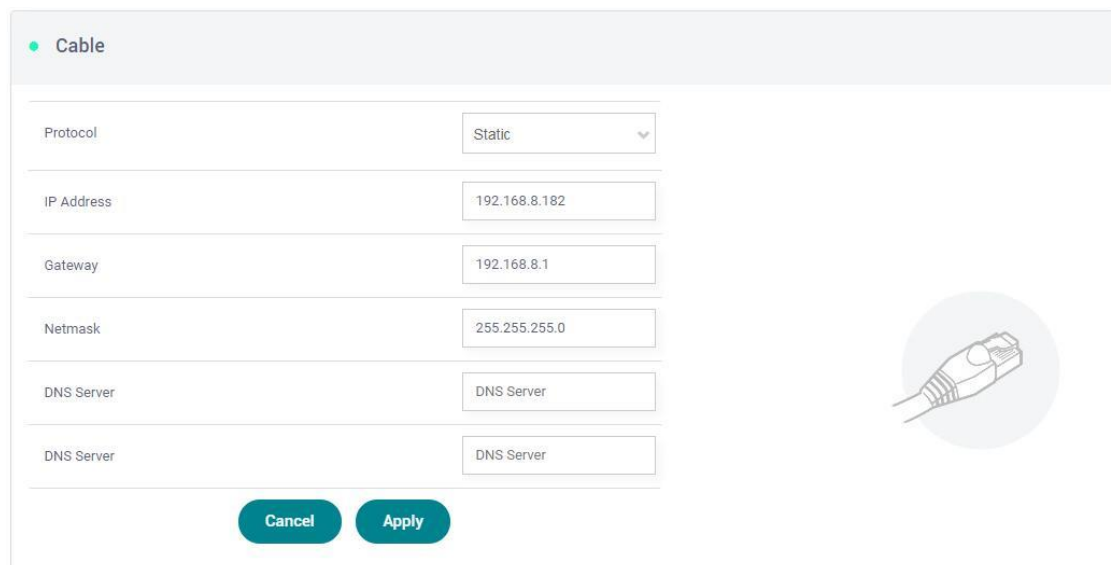
Protocol DHCP

Cancel



(2)Static

Static is required if your Internet Service Provider (ISP) has provided a fixed IP address for you or you want to configure the network information such as IP address, Gateway, Netmask manually. Change it according to your needs and then click Apply.



• Cable

Protocol Static

IP Address 192.168.8.182


Gateway 192.168.8.1

Netmask 255.255.255.0

DNS Server DNS Server

DNS Server DNS Server

Cancel Apply



(3)PPPoE

PPPoE is required by many Internet Service Providers (ISP). Generally, your ISP will give you a modem and provide you a username and password that you needed when you are creating the Internet connection.

Under PPPoE protocol, enter your username and password, then click Apply.

Cable

Protocol

PPPoE

User Name


User Name

Password

Password

Cancel

Apply

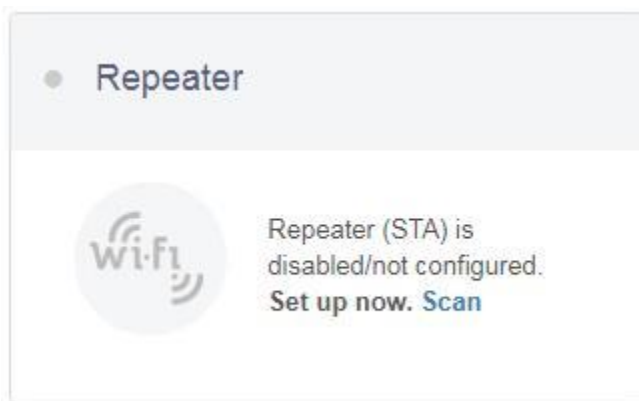


2.2. Repeater

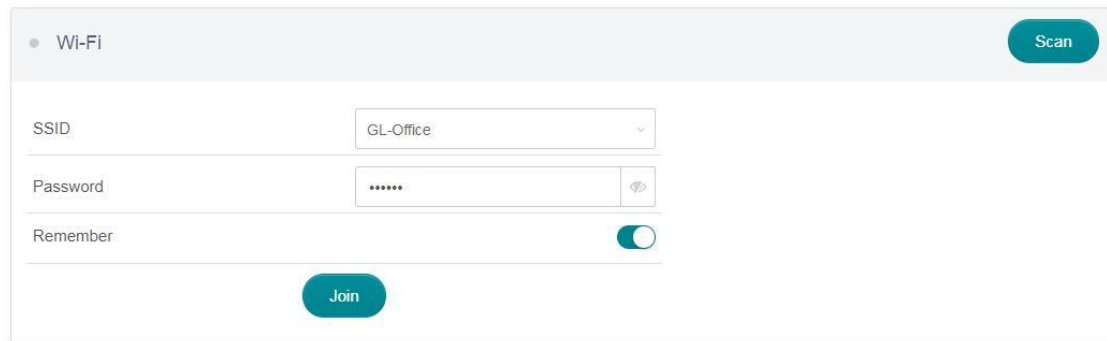
Using Repeater means connecting the router to another existing wireless network, e.g. when you are using free Wi-Fi in a hotel or cafe.

It works in WISP (Wireless Internet Service Provider) mode by default, which means that the router will create its own subnet and act as a firewall to protect you from the public network.

In Repeater section, click Scan to search for the available wireless networks nearby.



Choose a SSID from the drop-down list and enter its password. You can also enable the Remember button to save the current chose wireless network. Finally, click Join.

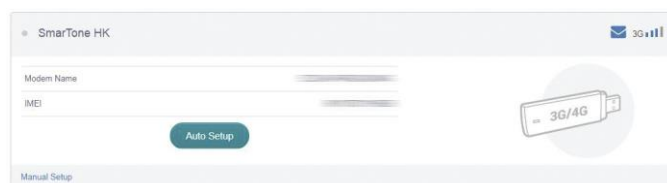


The image shows a Wi-Fi configuration interface. At the top left, there is a tab labeled "Wi-Fi". At the top right, there is a "Scan" button. Below the tab, there are three input fields: "SSID" with a dropdown menu showing "GL-Office", "Password" with a masked input (*****), and "Remember" with a toggle switch that is currently turned on. At the bottom center, there is a "Join" button.

2.3. 3G/4G Modem

Collie has a built-in 3G/4G modem which you can insert your SIM card directly. Please insert the SIM card before powering on the router. Then, you should find the name of your carrier, click Auto Setup to create the connection.

Note: Some 3G/4G modems will be recognized as Tethering connection.



The image shows a 3G/4G Modem configuration interface. At the top left, there is a tab labeled "SmarTone HK". At the top right, there is a "3G/4G" status indicator. Below the tab, there are two input fields: "Modem Name" and "IMEI". Below these fields, there is an "Auto Setup" button. To the right of the "Auto Setup" button, there is an illustration of a 3G/4G modem. At the bottom left, there is a "Manual Setup" link.

You can also click Manual Setup to set up manually.

In General, you can set up by the three basic parameters below. Click Apply to connect.


- **Device:** Please choose **/dev/cdc-wdm0 (qmi)** or **/dev/ttyUSB3**.
- **Service Type:** Indicate the service of your SIM card.
- **APN:** Confirm with your SIM card carrier.

SmarTone HK
3G

Device
/dev/ttyUSB3
Service
LTE/UMTS/GPRS
APN

AT Command
Advanced
Modem Reset

Cancel
Apply



Advanced Settings:

- Dial Number:** Generally, it is a default value and you don't need to set it manually. However, if you have this info, please input it.
- Pincode, Username and Password:** Generally, these are not necessary for an unlocked SIM card. However, if you have a locked SIM card, please consult your service provider.

Pincode

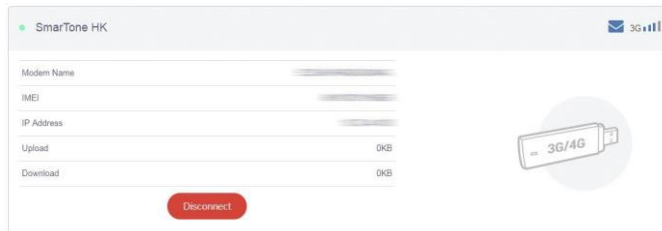
Dial number

User Name

Password

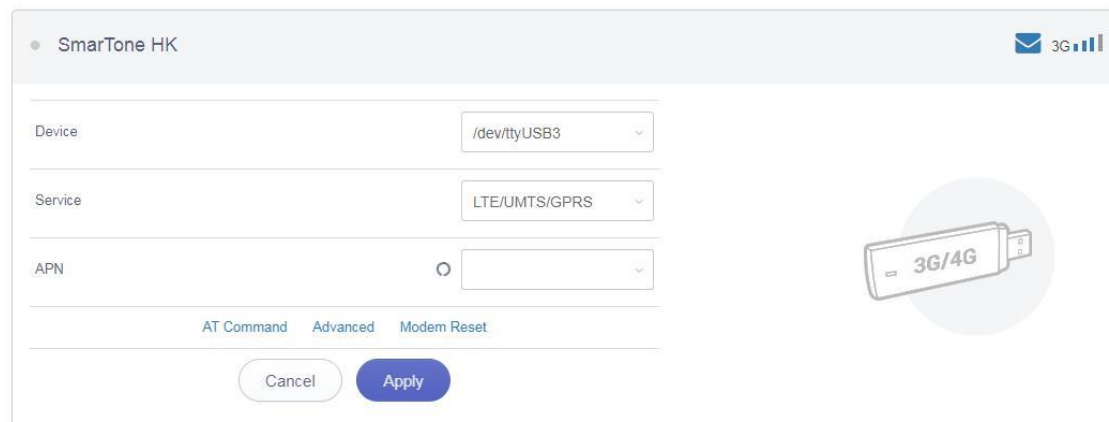
Apply

It is connected when the IP address of your SIM card shows up.



AT Command

The built-in modem supports AT command for the management and configuration of the modem. In 3G/4G Modem section, Click AT Command.



- **Shortcut:** There are several pre-configured AT commands that you can use directly. If you want to run your own AT command, choose **Manual command**.
- **AT Command:** The place where you can input AT command. For the list of AT command, please refer to the AT command manual of the built-in modem.
- **Port:** The default port for AT command is **/dev/ttyUSB2**.

• AT Command

Shortcut

Manual command

AT Command

Required

Port

/dev/ttyUSB2

Send

3. WIRELESS

In WIRELESS, you can check the current status and change the settings of the wireless network created by the router. The wireless network can be turned on or off by switching the **ON/OFF** button.

Wi-Fi Name (SSID): The name of the Wi-Fi. It is not suggested to use unicode characters such as **Chinese**.

Wi-Fi Security: The encryption method of the Wi-Fi.

Wi-Fi Key: The password of the Wi-Fi, which must be at least 8 characters long. We suggest you to change it when you receive the router.

SSID Visibility: Show or hide the SSID.

Wi-Fi Mode: Wi-Fi protocol standards. It supports 802.11/b/g/n. It is suggested to use default 802.11b/g/n or select Wi-Fi mode based on your demand.

Bandwidth: The bandwidth is the Wi-Fi channel frequency coverage range. Select 20/40MHz or 40MHz or 20MHz based on your demand.

Channel: The router will not choose the best channel itself. You need to choose a channel manually. If your router is used as a Wi-Fi repeater, the channel will be fixed according to the connected wireless network.

TX Power (dBm): It specifies the signal strength. It has 4 levels, Max, High, Medium, Low. Default setting is Max.

Channel Optimization: It will optimize your Wi-Fi signal and channel according to the Wi-Fi environment.

No Internet Connection! Find new networks to reconnect.

2.4G WiFi

2.4G Guest WiFi

GL-X300B-8f8



Wi-Fi Name (SSID)

GL-X300B-8f8

Wi-Fi Security

WPA2-PSK

Wi-Fi Key

.....

SSID Visibility

Shown

Wi-Fi Mode

802.11b/g/n

Bandwidth

20/40 MHz

Channel

6

TX Power (dBm)

Max

Modify

Channel Optimization

Copyright © 2020 GL.iNet. All Rights Reserved.

Click Modify to change the settings of the wireless network.

2.4G WiFi

2.4G Guest WiFi

GL-X300B-5a1

ON

Wi-Fi Name (SSID)	GL-X300B-5a1
Wi-Fi Security	WPA2-PSK
Wi-Fi Key ⓘ	*****
SSID Visibility	Shown
Wi-Fi Mode	802.11b/g/n
Bandwidth	20/40 MHz
Channel	9
TX Power (dBm) ⓘ	Max

Cancel

Apply

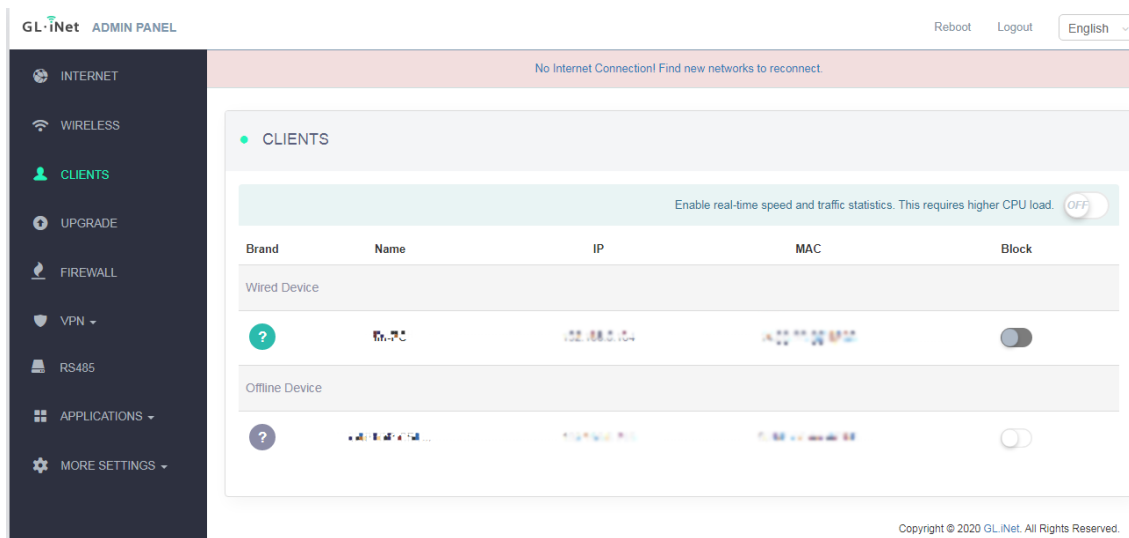
4. CLIENTS

You can manage all connected clients in CLIENTS.

You can see their name, IP, MAC address.

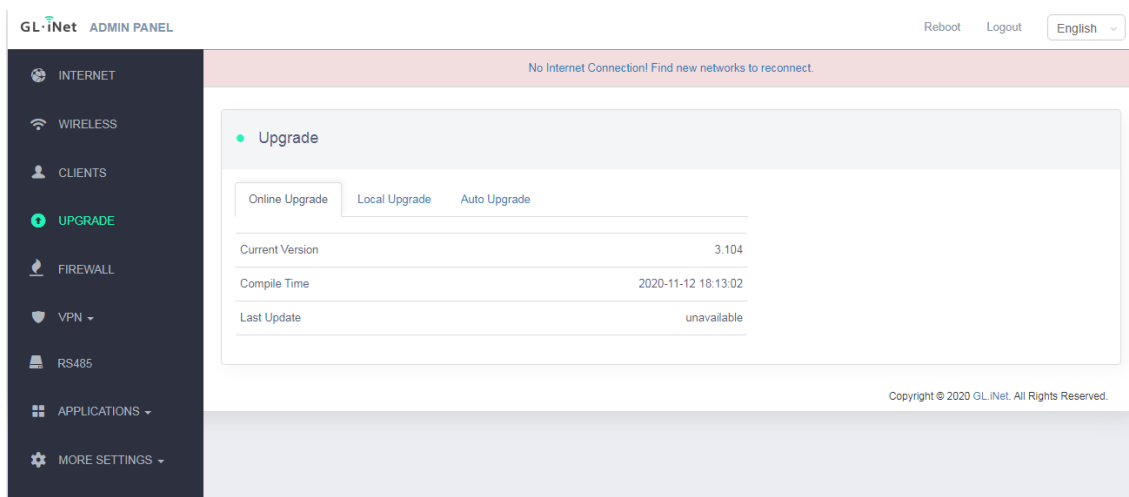
Click the button on the right to block any unwanted client.

Click the button on the right corner to enable real-time speed and traffic statistics. This requires higher CPU load.



5. UPGRADE

Click UPGRADE to check any available update and upgrade the firmware.



5.1. Online Upgrade

You can find the current firmware version here. If your router is connected to the Internet, it will check for the newer firmware version available for download.

● Upgrade

Online Upgrade

Local Upgrade

Auto Upgrade

Current Version	3.104
Compile Time	2020-06-09 13:14:20
Last Update	unavailable

*Note: It is suggested to uncheck **Keep setting** during firmware upgrade. If you keep the settings and encounter problems after the upgrade, please reset the router.*

5.2. Upload Firmware

Click Local Upgrade to upload a firmware file to the router. Simply drag and drop your firmware file to the area indicated.

● Upgrade

Online Upgrade

Local Upgrade

Auto Upgrade

↓

Select a file or drag it here.

File type includes .bin .zip .tar .gz

(1) Official OpenWrt/LEDE firmware

You can download the official firmware from our [website](#).

- Collie: <http://download.gl-inet.com/firmware/x300b/>

Find the available firmware from the folder according to your device model, and they are located in different sub-folders:

release: Official GL.iNet OpenWrt/LEDE firmware.

clean: Clean versions of OpenWrt/LEDE firmware with Luci admin page only.

testing: Beta version of GL.iNet OpenWrt/LEDE firmware.

(2) Compile your own firmware

You can compile your own firmware and flash to the router. Please refer to

<https://github.com/gl-inet/imagebuilder>

Note: If you uploaded an incompatible firmware thus bricked the router, please use Uboot to re-install the correct firmware.

5.3. Auto Upgrade

You can enable auto upgrade. The router will search for available update and upgrade automatically according to the time that you set.

● Upgrade

Online Upgrade

Local Upgrade

Auto Upgrade

Router Time

Fri Jul 17 08:28:46 UTC 2020

Enable Auto Upgrade



Auto Upgrade Time

04:00

6. FIREWALL

In FIREWALL, you can set up firewall rules like **port forwarding**, **open port** and **DMZ**.

GL.iNet ADMIN PANEL

Reboot Logout English

No Internet Connection! Find new networks to reconnect.

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN

RS485

APPLICATIONS

MORE SETTINGS

● Firewall

Port Forwards Open Ports on Router DMZ

Port Forwarding allows remote computers to connect to a specific computer or service behind the firewall in the local LAN (such as web servers, FTP servers, etc.)

Name	Protocol	External Zone	External Ports	Internal Zone	Internal IP	Internal Ports	Status	Action
Required	TCP/UDP	wan	Required	lan	Required	Required	Enable	Add

Add a New One

Copyright © 2020 GL.iNet. All Rights Reserved.

6.1. Port Forwards

Port Forwarding allows remote computers to connect to a specific computer or service behind the firewall in the local LAN (such as web servers, FTP servers, etc.)

To set up port forwarding, click Port Forwards and input the required parameters or click Add a New One.

Firewall

Port Forwards

Open Ports on Router

DMZ

Port Forwarding allows remote computers to connect to a specific computer or service behind the firewall in the local LAN (such as web servers, FTP servers, etc.)

Name	Protocol	External Zone	External Ports ⓘ	Internal Zone	Internal IP	Internal Ports ⓘ	Status	Action
<input type="text" value="Required"/>	<div>TCP/U ▾</div>	<div>wan ▾</div>	<input type="text" value="Required"/>	<div>lan ▾</div>	<div>Required ▾</div>	<input type="text" value="Required"/>	<div>Enable ▾</div>	Add
Add a New One								

Name: The name of the rule which can be specified by the user.

Protocol: The protocol used, you can choose TCP, UDP, or both TCP and UDP.

External Zone: The zone to which hosts will be connecting.

External Ports: The numbers of external ports. You can enter a specific port number or a range of service ports (E.g. **100-300**).

Internal Zone: The zone to which the incoming connection will be redirected.

Internal IP: The IP address assigned by the router to the device which needs to be accessed remotely.

Internal Ports: The internal port number of the device. You can enter a specific port number. Leave it blank if it is same as the external port.

Status: Activate or Deactivate the rule.

6.2. Open Ports on Router

The router's services, such as web, FTP and so on, require their respective ports to be opened on the router in order to be publicly reachable.

To open a port, click Open Ports on Router and input the required parameters or click Add a New One.



Firewall

Port Forwards Open Ports on Router DMZ

The router's services, such as web, FTP and so on, require their respective ports to be opened on the router in order to be publicly reachable.

Name	Port	Protocol	Status	Action
Required	Required	TCP/UDP	Enabled	Add

Name: The name of the rule which can be specified by the user.

Port: The port number that you want to open.

Protocol: The protocol used, you can choose TCP, UDP, or both TCP and UDP.

Status: Activate or Deactivate the rule.

6.3. DMZ

DMZ allows you to expose one computer to the Internet, so that all the inbound packets will be redirected to the computer you set.

Click DMZ and enable Open DMZ. Input the internal IP address (E.g. 192.168.8.100) of your device which is going to receive all the inbound packets.

The screenshot shows the 'Firewall' section of a router's web interface, specifically the 'DMZ' tab. At the top, there are three tabs: 'Port Forwards', 'Open Ports on Router', and 'DMZ'. Below the tabs, a light blue informational box states: 'DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set.' followed by a warning icon and text: 'If you enable DMZ, your port forward and port open rules will not take effect.' Below this, there is a toggle switch for 'Open DMZ' which is currently turned off. Underneath the toggle is a label 'DMZ Host IP' followed by a dropdown menu. At the bottom center of the form is an 'Apply' button.

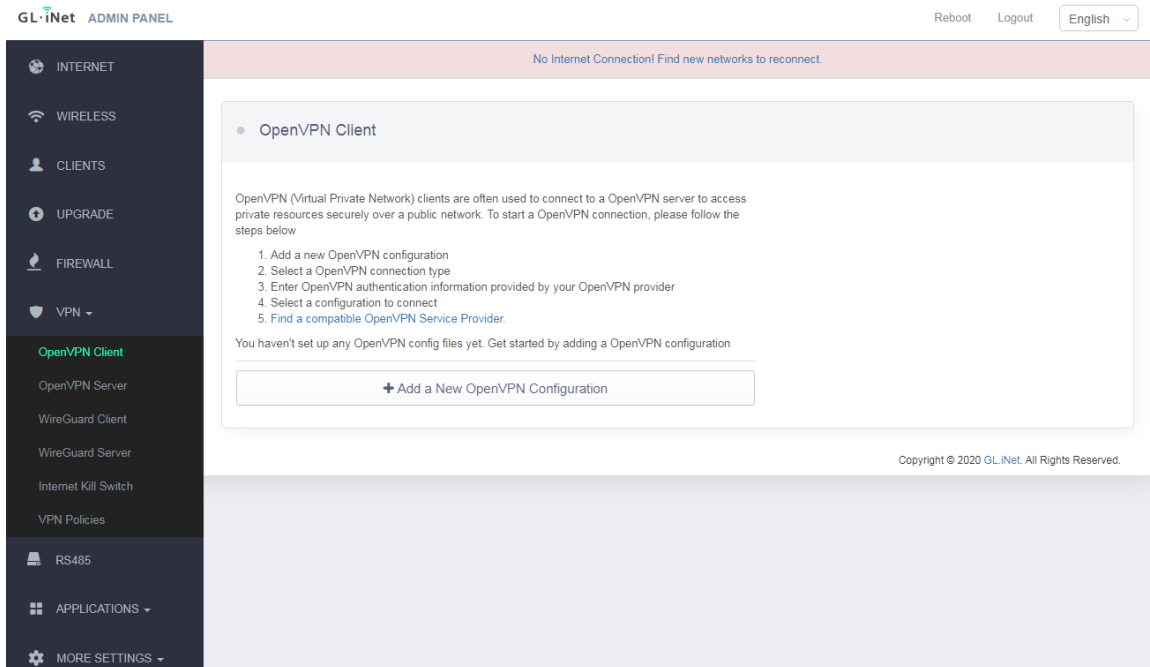
7. VPN

GL.iNet routers have pre-installed VPN server and client in **OpenVPN** and **WireGuard**.

Shadowsocks is not a default function and you need to install packages in Plugins.

Please refer to the links below for the detailed setup instruction:

- [OpenVPN](#)
- [WireGuard](#)

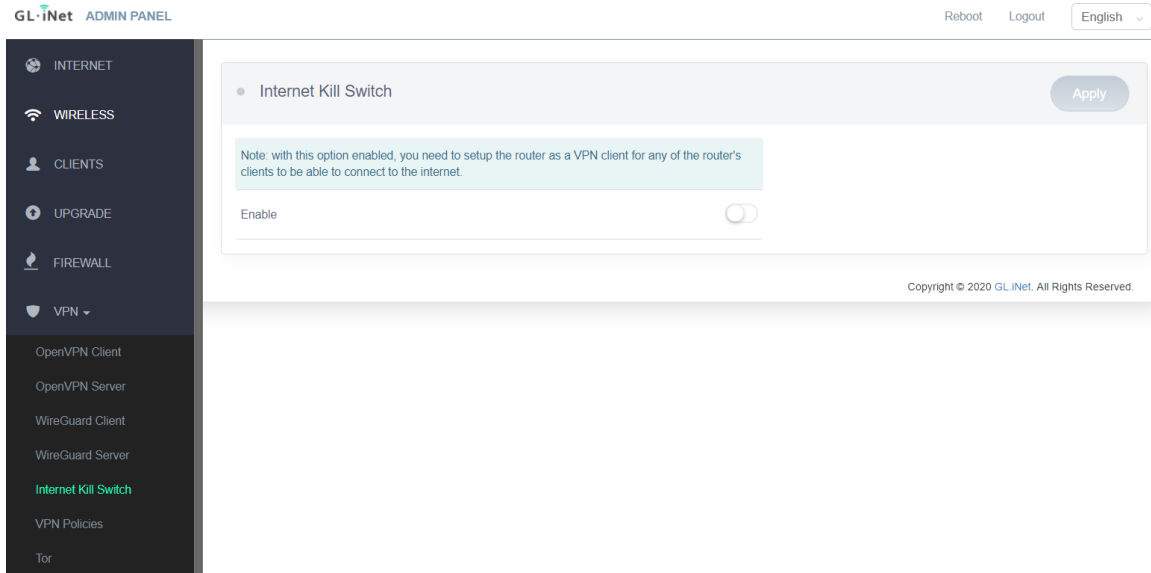


Internet Kill Switch

Starting from firmware version 3.100.

Please refer to the links below for the detailed setup instruction:

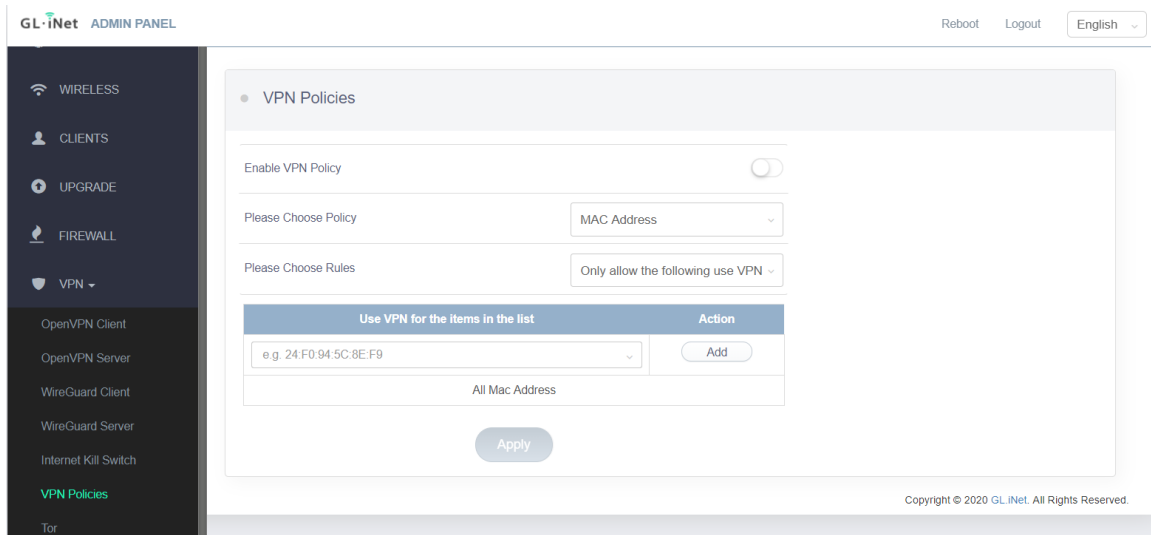
- [Internet Kill Switch](#)



Starting from firmware version 3.022, users can define **VPN routing policies**.

Please refer to the links below for the detailed setup instruction:

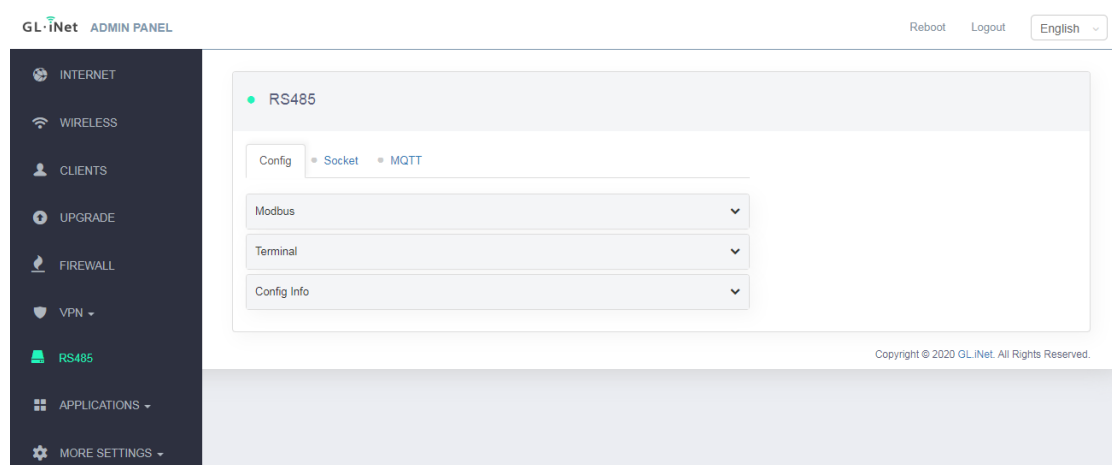
- [VPN Policies](#)



8. RS485

GL.iNet provides a simple configuration and debugging interface for RS485. We hope this simple RS485 function can meet the development and debugging of basic applications.

Including **Config** (basic configuration), **Socket** configuration, **MQTT** configuration.



8.1. Config

Config includes Modbus (Configuration), Terminal (Terminal debug), Config Info.

Modbus: This function can perform read and write operations on terminal devices that support Modbus protocol. It requires users to have a certain knowledge of Modbus protocol.

Device ID: Device ID is 01 by default mostly. When multiple terminal devices are connected and used at the same time, separate connected devices need to be set with different ID numbers.

Function Code: Function code needs to be obtained from the terminal device manual.

Reg Addr: Register address, it needs to be obtained from the terminal device manual.

Reg Len: Register length, it needs to be obtained from the terminal device manual.

Terminal: Provide X300B and RS485 terminal debugging interface, mainly used in debugging and testing phase. Support string format and hexadecimal format, support echo and time stamp display. This function can be used to debug terminal device that supports Modbus, DL/T645, DL/T698 and other protocols.

Config Info:

Device: The `/dev/ttyS0` in the interface refers to the name of the RS485 driver, and the name generally does not need to be modified.

Speed: It refers to the baud rate, which can be modified according based on the RS485 device.

Mode: Modify it to make sure it's consistent with the connected 485 terminal device (Mode info can be found on RS485 device manual).

Timeout(ms): Information receiving timeout period, set according to actual needs.

8.2. Socket (RS485 to TCP/UDP)

Socket function is RS485 to TCP/UDP, and transparent transmission. There are 3 modes: TCPC, TCPS and UDP.

Below is the topology diagram and description of each mode.

● RS485

Config
Socket
MQTT

Address

192.168.8.1

Port

502

Mode

tcps ▼

Timeout

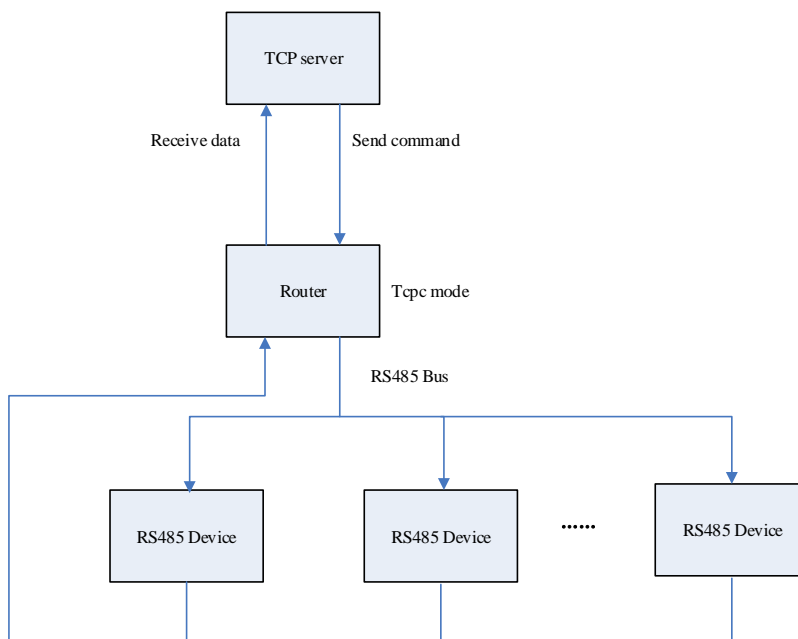
60

Cancel
Apply

Note: Above address is the server-side address.

TCPC TCP Client

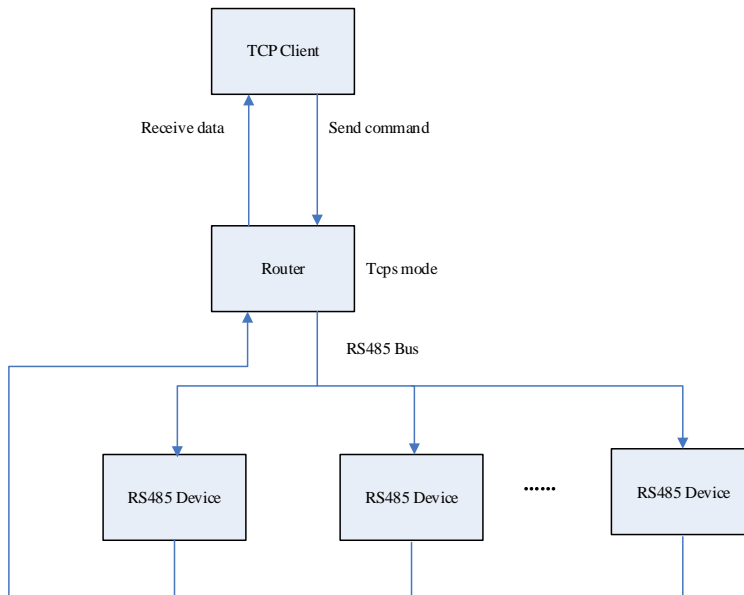
Router acts as a TCP client. After router connecting to the TCP server, the TCP server can send commands to obtain data from the RS485 terminals.



TCPS TCP Server

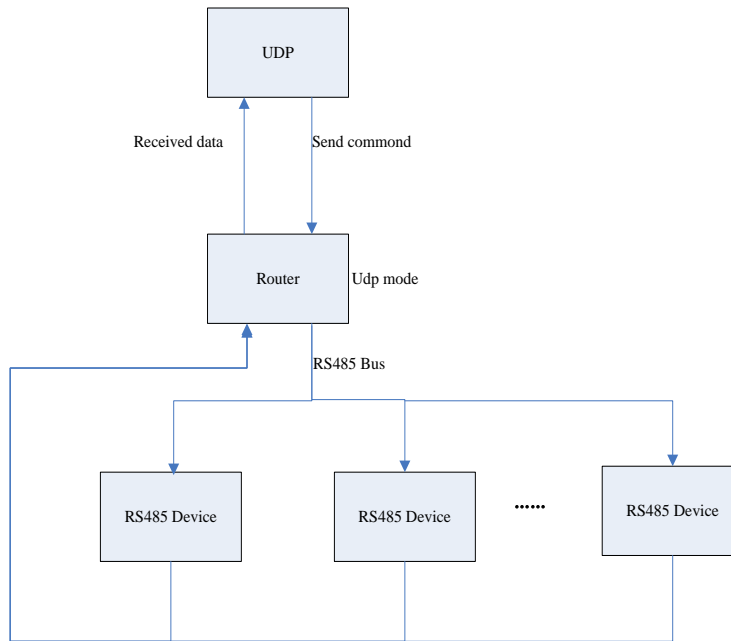
Router acts as a TCP server. After starting the server, the TCP client can connect to the router, and the TCP client can send commands to get the data of the RS485 terminals.

If it is in a local area network environment, fill in the address information of the router gateway IP. If it is in a wide area network environment, the router needs to have a public IP, and the address information should fill in the public IP.

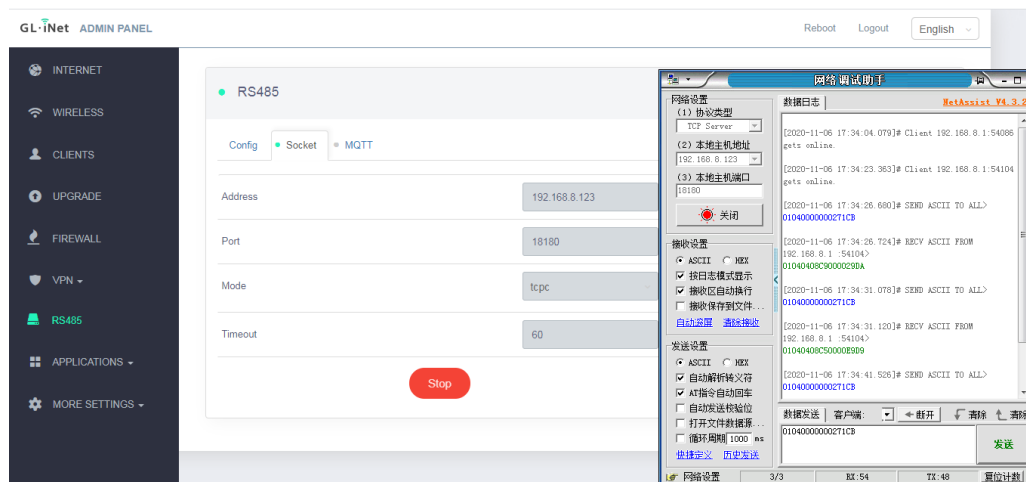


UDP

If it is in a local area network environment, fill in the address information of the router gateway IP. If it is in a wide area network environment, the router needs to have a public IP, and the address information should fill in the public IP.



Example: Set the router to TCPC, install a TCP/UDP test program on the computer, and build a test environment on the LAN for testing.



Note: The test terminal device connected to the router is a smart meter. The 01040000000271CB in the figure is a command to obtain voltage data.

Please enter the correct command according to the manual of the connected terminals. The input command is in string format, and the program will convert the command to hexadecimal and send to the terminal devices. It'll convert the obtained hexadecimal data sentence into a string format and send it to the remote server or client.

8.3. MQTT

● RS485

Config

● Socket

● MQTT

MQTT Broker Profile Settings

Broker Address

47.106.196.54

Broker Port

1883

Client ID

glinet-x300b

Qos

0

Publish

device/e4956e40b6...

Subscribe

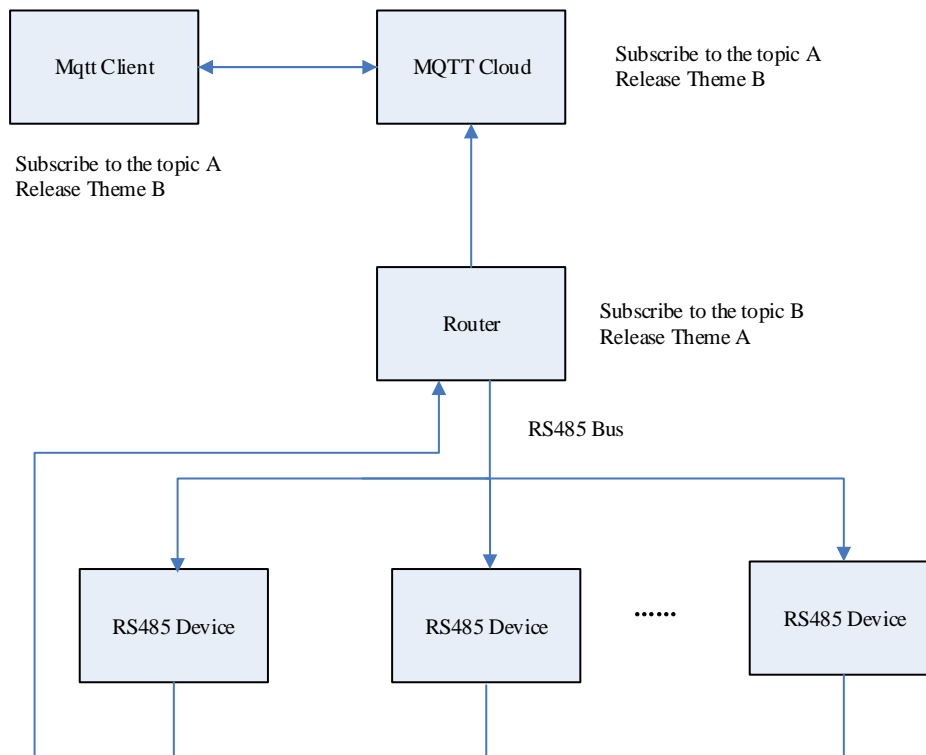
device/e4956e40b6...

More Settings

Modify

Start

This function is RS485 to MQTT. It can be used to connect to the Cloud platform. After connection, the Cloud platform or other clients that subscribe to the RS485 publishing topic will be able to obtain the data of the RS485 terminal devices.



Connect to MQTT server test: free online MQTT server
<https://www.emqx.io/cn/mqtt/public-mqtt5-broker>

接入信息

Broker: broker.emqx.io

TCP Port: 1883

Websocket Port: 8083

TCP/TLS Port: 8883

Websocket/TLS Port: 8084

Note: This server is for testing only and has no privacy protection. Any device can publish and subscribe to topics on it. Do not use in production.

Web page configuration is as follows, click **Start** after configuration.

● RS485

Config • Socket • MQTT

MQTT Broker Profile Settings

Broker Address	broker.emqx.io
Broker Port	1883
Client ID	glinetx300b
Qos	0
Publish	/glinet/rs485/data
Subscribe	/glinet/rs485/cmd

More Settings

Modify Start

Use the online MQTT client to configure the following to obtain data.

<https://www.emqx.io/cn/mqtt/mqtt-websocket-toolkit>

EMQX MQTT WebSocket Toolkit

Docs | Github

glinet@broker.emqx.io:1883

Name: glinet

Host: broker.emqx.io Port: 1883

Client ID: mqtt_7b67b62

Username: Password:

Keepalive: 60 Clean Session SSL

Connect

- INTERNET
- WIRELESS
- CLIENTS
- UPGRADE
- FIREWALL
- VPN
- APPLICATIONS
- Plug-ins**
- Remote Access
- Captive Portal
- MORE SETTINGS

Plug-ins

Update

Filter

Q Search Package

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Name	Version	Description	Action
base-files	194.2-r7897-9d401013fc	-	<div>✖ Uninstall</div>
bridge	1.5-6	-	<div>✖ Uninstall</div>
busybox	1.28.4-3	-	<div>✖ Uninstall</div>
ca-bundle	20190110-1	-	<div>✖ Uninstall</div>
ca-certificates	20190110-1	-	<div>✖ Uninstall</div>
chat	2.4.7-12	-	<div>✖ Uninstall</div>
comgt	0.32-30	-	<div>✖ Uninstall</div>
curl	7.60.0-4	-	<div>✖ Uninstall</div>

←

1

2

3

...

29

30

→

Go

Free space: 10% (1 MB)

Free space: 10% (1 MB)

1 2 3 ... 29 30 Go

9.2. Remote Access

- INTERNET
- WIRELESS
- CLIENTS
- UPGRADE
- FIREWALL
- VPN
- APPLICATIONS
- Plug-ins
- Remote Access**
- Captive Portal
- MORE SETTINGS

Cloud Management

With GoodCloud, you can manage routers in groups, check live router status, set up routers remotely, operate routers in batch and monitor connected clients etc.

Your device ID is **qg6d5b3**, Please use the ID to add this device to your cloud account. ?

Enabled GoodCloud



Apply

View Logs

Dynamic DNS

You can enable Dynamic DNS for this router and access this router remotely. [DDNS Test](#)

Note: You have to have an Internet Public IP address to use the Dynamic DNS. If this router is behind NAT, you may need to set up port forward in your ISP router. ?

Enabled DDNS ?



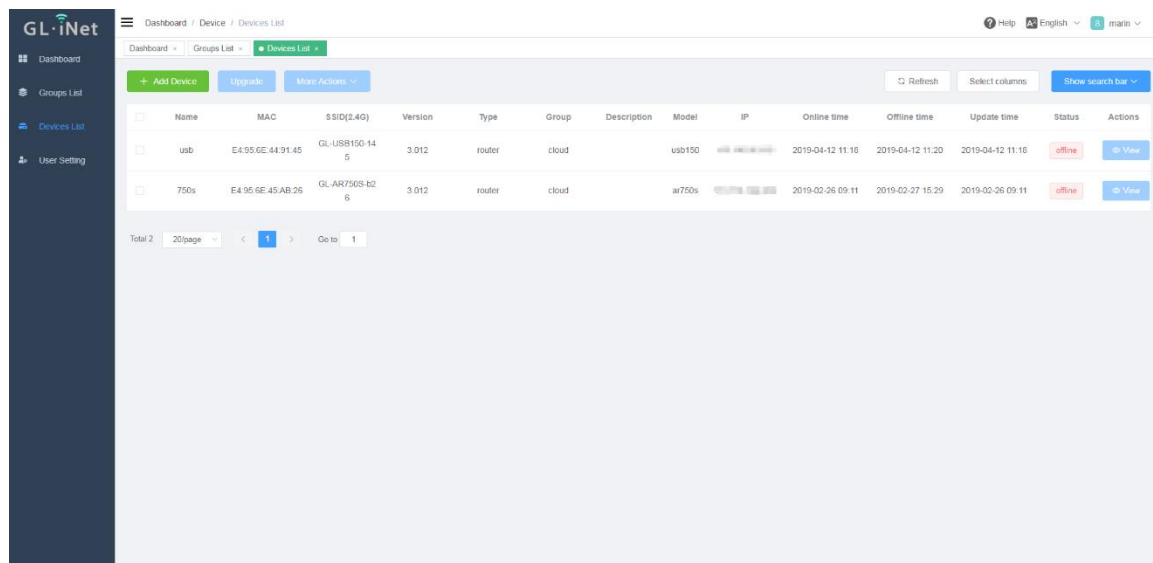
Apply

Cloud Management

GL.iNet GoodCloud cloud management services provide an easy and simple way to remotely manage routers.

In our website, you can remotely check your router status, change the password, control clients, even set email alarm when a device is online or offline.

In 3.021 version or above it is a default function, other 3.0 version need to install packages in Plug-ins.



Name	MAC	SSID(2.4G)	Version	Type	Group	Description	Model	IP	Online time	Offline time	Update time	Status	Actions
usb	E4:95:6E:44:91:45	GL-USB150-145	3.012	router	cloud		usb150		2019-04-12 11:16	2019-04-12 11:20	2019-04-12 11:16	online	View
750i	E4:95:6E:45:AB:26	GL-AR750S-b26	3.012	router	cloud		ar750s		2019-02-26 09:11	2019-02-27 15:29	2019-02-26 09:11	offline	View

For the details, please refer to [Cloud](#).

DDNS

DDNS (Dynamic Domain Name Service) is a service used to map a domain name to the dynamic IP address of a network device.

You can remotely access your router by url though this function.

In 3.021 version or above it is a default function, other 3.0 version need to install packages in Plug-ins.

For the guidance on how to set DDNS and access, please refer to [DDNS](#).

9.3. Captive Portal

You can set a **captive portal** in our routers, when newly users connect to Wi-Fi, they need to access a web page before access the internet.

Only support 3.022 version or above.

The screenshot displays the GL.iNet Admin Panel interface. On the left is a dark sidebar with navigation options: INTERNET, WIRELESS, CLIENTS, UPGRADE, FIREWALL, VPN, APPLICATIONS, Plug-ins, Remote Access, **Captive Portal** (highlighted in green), and MORE SETTINGS. The main content area has a light blue header with 'GL.iNet ADMIN PANEL' and links for 'Reboot', 'Logout', and a language dropdown set to 'English'. A red banner at the top of the main area reads 'No Internet Connection! Find new networks to reconnect.' Below this, the 'Captive Portal' settings are shown. A light blue box contains instructions: 'You can set up a captive portal to display a web page when a user connects to your Wi-Fi network. Help?' and two warning icons: 'If Guest network is disabled, captive portal function is unavailable.' and 'Opening the captival portal will cause the block function to fail.' The settings include a toggle for 'Enable captive portal' (currently off), a dropdown for 'Virtual network interface' set to 'Guest', a text input for 'Lease time minutes (1-1440)' with the value '1440', and another text input for 'Forward URL after Authorization' with the value 'Optional'. An 'Apply' button is at the bottom. A copyright notice 'Copyright © 2020 GL.iNet. All Rights Reserved.' is at the bottom right.

For the setup guidance, please refer to [Set a Captive portal](#).

10. MORE SETTINGS

10.1. Admin Password

Change the password of the web Admin Panel, which must be at least 5 characters long. You have to input your current password in order to change it.

GL.iNet ADMIN PANEL

RebootLogoutEnglish

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN

APPLICATIONS

MORE SETTINGS

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Network Mode

Admin Password

Old Password

Required

New Password

Required

Confirm Password

Required

Apply

Copyright © 2020 GL.iNet. All Rights Reserved.

10.2. LAN IP

LAN IP is the IP address that you use to connect to this router. The default IP address of GL.iNet router is 192.168.8.1. If it conflicts with the IP address of your main router, you can change it.

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Network Mode

Revert Firmware

LAN IP

Guest IP

LAN IP

GL routers use 192.168.8.1 as the default LAN IP address. This is the address you would enter into your browser's address bar to access the router admin page. You can manually setup one within these three ranges: 192.168.x.x, 172.x(16-31).x.x or 10.x.x.x

Note: The starting IP address and ending IP address must be in the range of 2-254, and the ending address should be greater than starting address.

LAN IP192.168.8.1

Start IP Address192.168.8100

End IP Address192.168.8249

Apply

Static IP Address Binding

Usually your computer's IP address is dynamically assigned by the router. If you want your computer to have a static IP address, you can manually add your computer's MAC address and the static IP address you want to use.

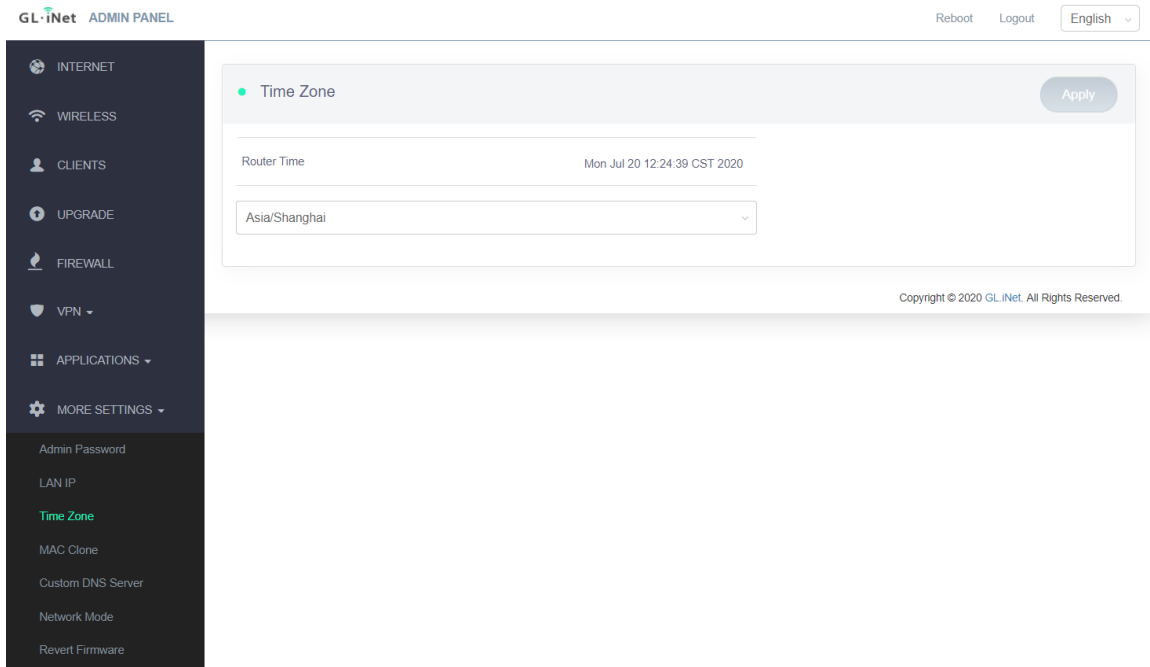
Mind the configured client has to reconnect the router to come into effect.

MAC	IP	Action
<input type="text"/>	<input type="text"/>	<div>Add</div>

Copyright © 2020 GL.iNet. All Rights Reserved.

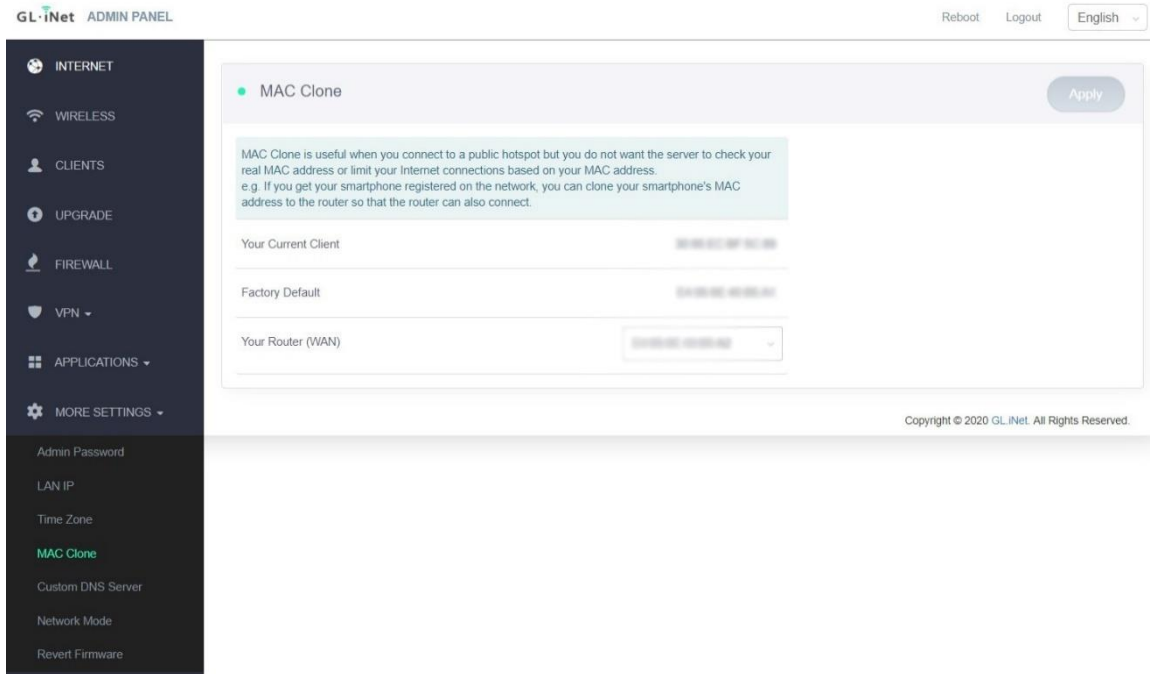
10.3. Time Zone

The time of the router's activities will be recorded according to the router time. Therefore, choosing the time zone of your location is recommended.



10.4. MAC Clone

Clone the MAC address of your current client to the router. It is used especially in hotel when the network checks your MAC address. For example, if you got your smartphone registered on the network, you can clone the MAC address of your smartphone to the router so that the router can also connect to the network.



10.5. Custom DNS Server

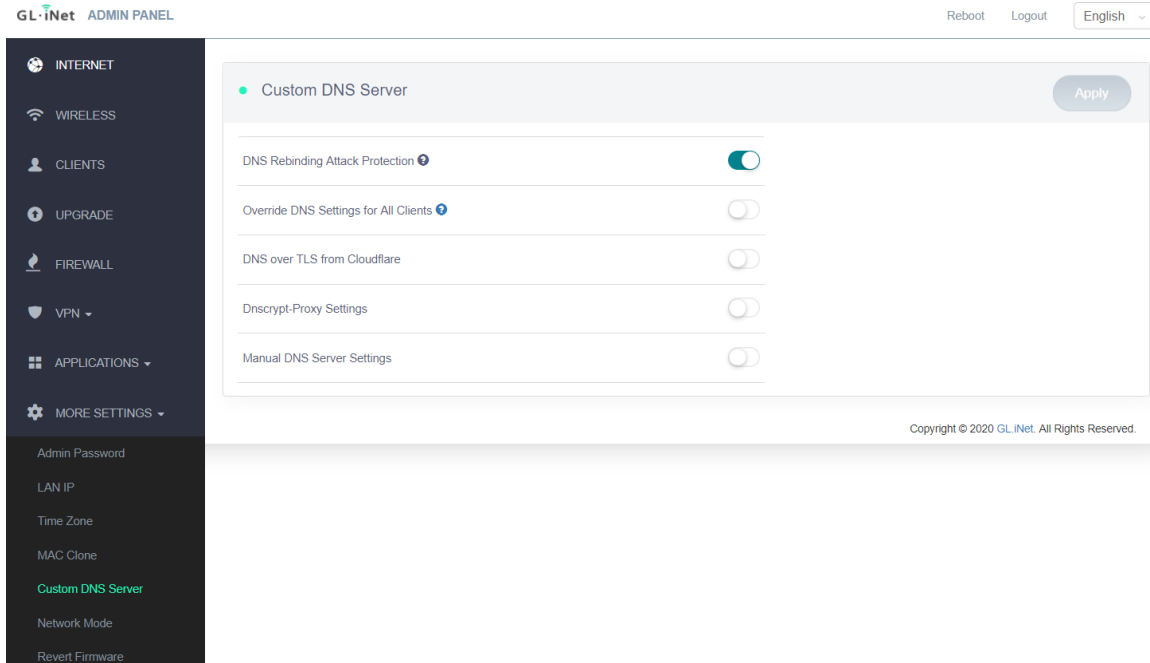
You can configure the DNS server of the router in order to prevent DNS leak or other purposes.

DNS Rebinding Attack Protection: Some network may require authentication in captive portal. Disable this option if the captive portal of your network cannot be resolved.

Override DNS Settings for All Clients: Enabling this option will capture DNS request from all connected clients.

DNS over TLS from Cloudflare: Cloudflare DNS over TLS uses the TLS security protocol for encrypting DNS queries, which helps increase privacy and prevent eavesdropping.

Manual DNS Server Settings: Input a custom DNS server manually.



10.6. Network Mode

Change the network mode to cater your usage scenario. You may need to reconnect your client device whenever you change the network mode of the router.

Be aware that you may not be able to access the web Admin Panel with the default IP 192.168.8.1 if you use the router in **Access Point**, **Extender** or **WDS** mode. If you want to access the web Admin Panel in this case, you have to use the IP address assigned by the main router to the GL.iNet router.

Router: Create your own private network. The router will act as NAT, firewall and DHCP server.

Access Point: Connect to a wired network and broadcast a wireless network.

Extender: Extend the Wi-Fi coverage of an existing wireless network.

WDS: Similar to Extender, please choose WDS if your main router supports WDS mode.

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN

APPLICATIONS

MORE SETTINGS

Admin Password

LAN IP

Time Zone


MAC Clone

Custom DNS Server

Network Mode

Revert Firmware

Network Mode



When you change the router's working mode, you may need to re-connect all your client devices.

When you use Access Point/Extender/WDS mode, you may not connect to this UI again. You can Press and hold the reset button for 4 seconds to revert back to router mode.

Mode Switch

☒ Router

☐ Access Point

☐ Extender

☐ WDS

Apply

Copyright © 2020 GL.iNet. All Rights Reserved.

10.7. Revert Firmware

Revert the router to factory default settings. All your settings, applications and data will be erased.

INTERNET

WIRELESS

CLIENTS

UPGRADE

FIREWALL

VPN ▾

APPLICATIONS ▾

MORE SETTINGS ▾

Admin Password

LAN IP

Time Zone

MAC Clone

Custom DNS Server

Network Mode

Revert Firmware

● Revert Firmware

ⓘ In case of malfunction, you can revert to factory default settings. All your current settings, applications and data will be lost. The process will take about 3 minutes. DO NOT power off the router during this process.

Revert Now

Copyright © 2020 GL.iNet. All Rights Reserved.