



User Manual

---Apply to WL-G530 Series Industrial 5G Router

V1.0

<http://www.wlink-tech.com>

Nov, 2020



Contents

1.1	1
1 Hardware Installation.....	4
1.1 Panel.....	4
1.2 LED Status.....	5
1.3 Dimension.....	6
1.4 How to Install.....	6
2 Router Configuration.....	9
2.1 Local Configure.....	9
2.2 Status.....	10
2.3 Tool Column.....	12
2.4 Basic Network.....	14
2.5 WLAN Setting.....	23
2.6 Advanced Network Setting.....	26
2.7 Firewall.....	35
2.8 VPN Tunnel.....	37
2.9 Administration.....	47
2.10 "Reset" Button for Restore Factory Setting.....	61
3 Configuration Instance.....	63
3.1 Port Forwarding.....	63
3.2 IP Passthrough.....	64

3.3 Captive Portal.....	66
3.4 GPS Settings.....	69

1 Hardware Installation

This chapter is mainly for installation introduction, there would be some difference between the scheme and real object. But the difference won't have any influence to products performance.

1.1 Panel

Table 1-1 WL-G530 Structure

WLINK Tech.	G530 series
Front	
Side	



NOTE

There are some difference on Antenna interface and indicator light for the device with extended Wi-Fi, GPS features.

Table 1-2 Router Interface

Port	Instruction	Remark
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection.	
Main	5G-1~5G-5 antenna, SMA connector, 50Ω.	

Port	Instruction	Remark
GPS	GPS antenna, SMA connector, 50Ω.	Optional
Wi-Fi	2.4G Wi-Fi, 5G Wi-Fi. dual-band antennas, RP-SMA connector	
LAN0~LAN4	10/100/1000Base-TX, MDI/MDIX self-adaption.	
Reset	Reset button, (press on button at least 5 seconds)	
PWR	Power connector	7.5~32VDC
IO Interface	5xPins	
Terminal Block	1xRS232, 1xRS485, 1xDC Power	

1.2 LED Status

Table 1-3 Router LED indicator Status

silk-screen	status		Indication
Signal	Signal	Constant light	LED1: weak (CSQ0~10). LED2: good (CSQ11~19) LED3: strong (CSQ20~31)
	Signal 1	Blink	dialing
		Constant light	online
PWR	Constant Light		System power operation.
WLAN	Constant light		WLAN enable, but no data communication.
	Blinking quickly		Data in transmitting
	Light off		WLAN disable
ERR	Light off		System operation and 5G/4G online.
	Constant Light(Red)		System fail indicator. It indicates SIM card/ module fail.
LAN	Green	Constant light	Connected.
	Green	Blinking	Data in transmitting.
	Green	Light off	Disconnection.

1.3 Dimension

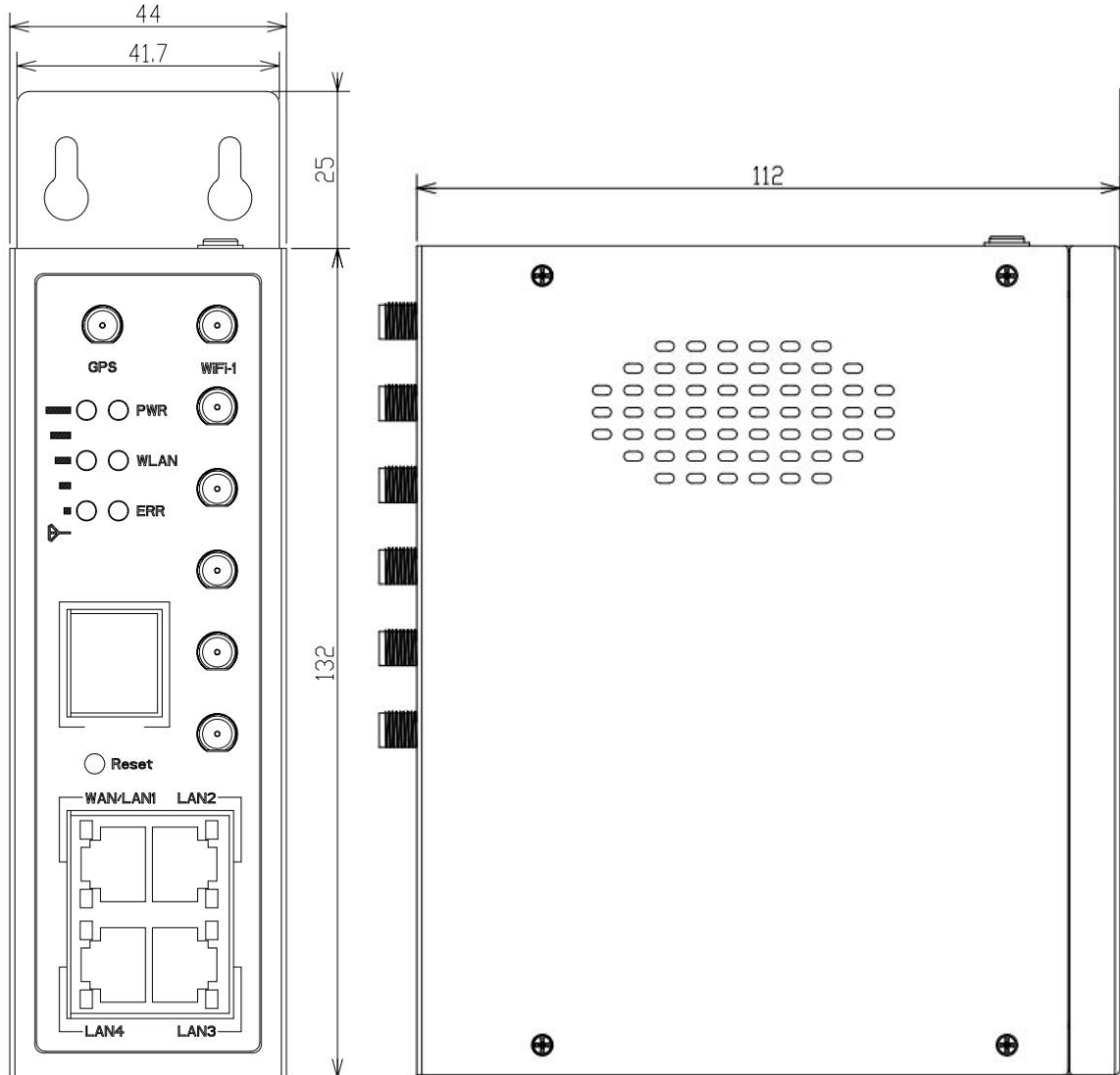
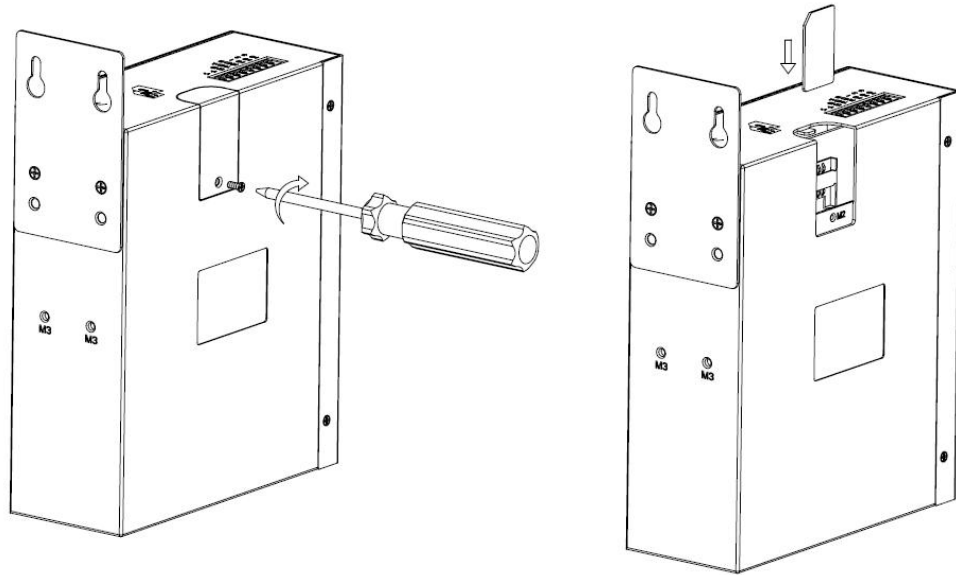


Figure 1-2 G530 Series Router Dimension

1.4 How to Install

1.4.1 SIM/UIM card install

Please insert the dual SIM cards before configure the router.



CAUTION

Before connecting, please disconnect any power resource of router

1.4.2 Ethernet Cable Connection

Connect the router with a computer by an Ethernet cable for GUI configuration, or transit by a switch.

1.4.3 5G and Wi-Fi Antenna Plug

Connect the two magnetic 5G antennas to 5G-1 to 5G-5 interfaces, and the four paddle shape Wi-Fi antennas to Wi-Fi interfaces.



NOTE

Wi-Fi antenna supports dual-band 2.4G and 5G bands.

1.4.6 Power Supply

Voltage input range: +7.5~32VDC. (Extended models: 7.5~ 48VDC)

1.4.7 Review

After insert the SIM/UIM card and connect Ethernet cable and antenna, connect power supply adaptor or power cable.



CAUTION

Please connect the antenna before power on, otherwise the signal maybe poor because of impedance mismatching.

Notice:

- Step 1 Check the antenna connection.
- Step 2 Check SIM/UIM card, confirm SIM/UIM card is available.
- Step 3 Power on the industrial Router

----END

2 Router Configuration

WL-G530 Series routers support GUI and CLI configuration. This chapter introduce GUI configuration via Ethernet port, if need CLI configuration guide, please contact our technical support department by email: support@wlink-tech.com.

2.1 Local Configure

The router supports to be configured by local Ethernet port, you could specify a static IP or set as DHCP. The default IP address is 192.168.1.1 , subnet mask is 255.255.255.0, please refer to following.

- Step 1 Click “start > control panel”, find “Network Connections” icon and double click it to enter, select “Local Area Connection” corresponding to the network card on this page. Refer to the figure below.



Figure 2-1 Network Connection

- Step 2 Obtain a IP address automatically or set up IP address,192.168.1.xxx(XXX can be any number between 2~254)
- Step 3 Run an Internet Explorer and visit “<http://192.168.1.1/>”, to enter identify page.

User should use the default user name and password when log in for the first time



Figure 2-2 User Identify Interface

----END

2.2 Status

Check routers information such as status, traffic Stats and device list after login router. Especially, suggest change the password according to the prompts because of security requirement.

You haven't changed the default password for this router. To change router password [click here](#).

The UI will display "already changed login password successfully" after router reboot.

Already changed login password successfully.

2.2.1 Overview

The overview GUI will be display router system information, Ethernet ports status, VPN connection status, LAN information, 5G connection information and WLAN information,

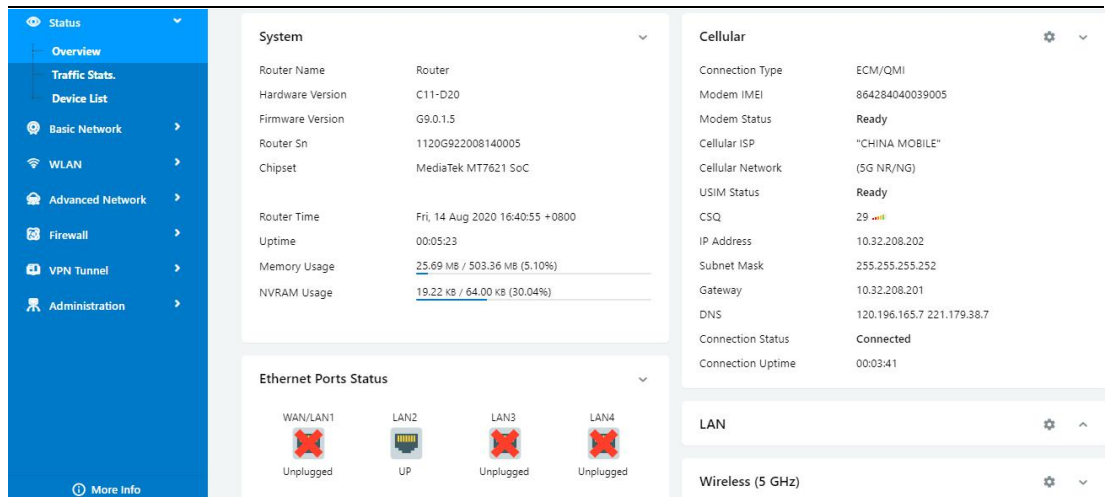


Figure 2-3 Router Status GUI

2.2.2 Traffic Stats.

Click Status->Traffic Stats. to enter the traffic stats.GUI.to check Cellular/WAN traffic in real-time.

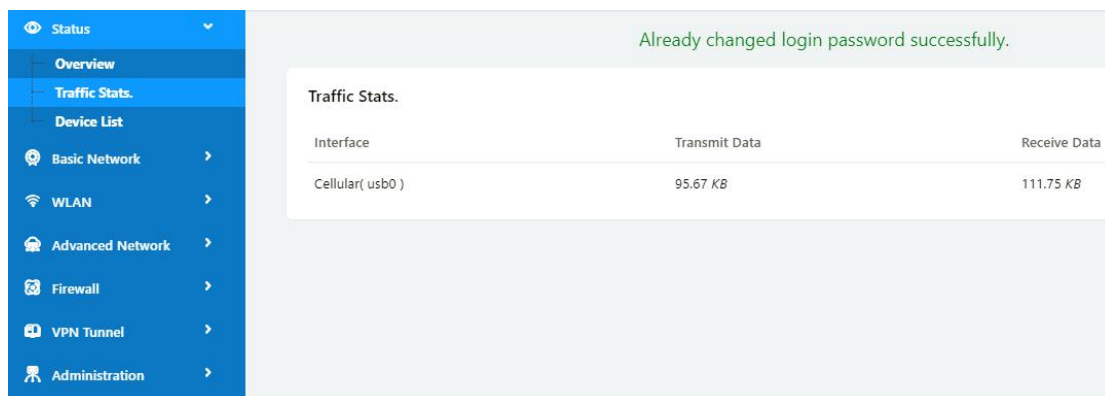


Figure 2-4 Traffic Stats. GUI

2.2.3 Device List

Click Status->Device List to enter the device list GUI.to check the connected devices information in the list.

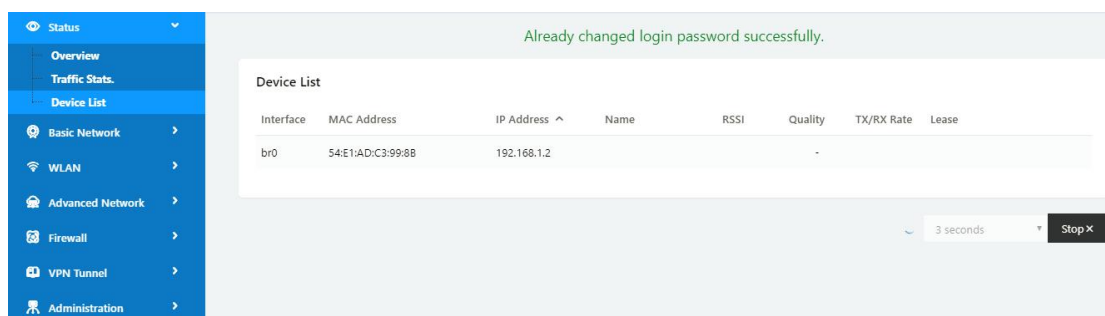


Figure 2-5 Device List GUI

2.3 Tool Column



Figure 2-6 Tool Column GUI

2.3.2 Tools

2.3.2.1 Ping

Click Tools->Ping to enter ping test GUI. Used to test the reachability of a host on an Internet IP network and to measure the round-trip time for messages sent from the originating host to a destination server.

2.3.2.2 Trace

Click Tools->Trace to enter trace test GUI. diagnostic tool for displaying the route and measuring transit delays of packets across an Internet IP network.

2.3.2.3 WOL

Click Tools-> WOL to enter WOL(Wake On Lan) GUI. Used to wake up those connected devices via WOL protocol. Click left mouse button to wake up the device.

Wake On Lan

MAC Address	IP Address	Status	Name ^
54:E1:AD:C3:99:8B	192.168.1.2	Active (In ARP)	

Click to wake up

MAC Address List

Wake Up ^ Refresh

2.3.2.4 Log

Click Tools-> Log to enter Log GUI. Use to check logs in GUI, download GUI and send logs to server.

Logs

View

Download Log File

FindQ

» Logging Configuration

2.3.2.5 Capture

Click Tools-> Capture to enter capture data GUI. Use to capture LAN/WAN data packet to analyse what happen in the router.

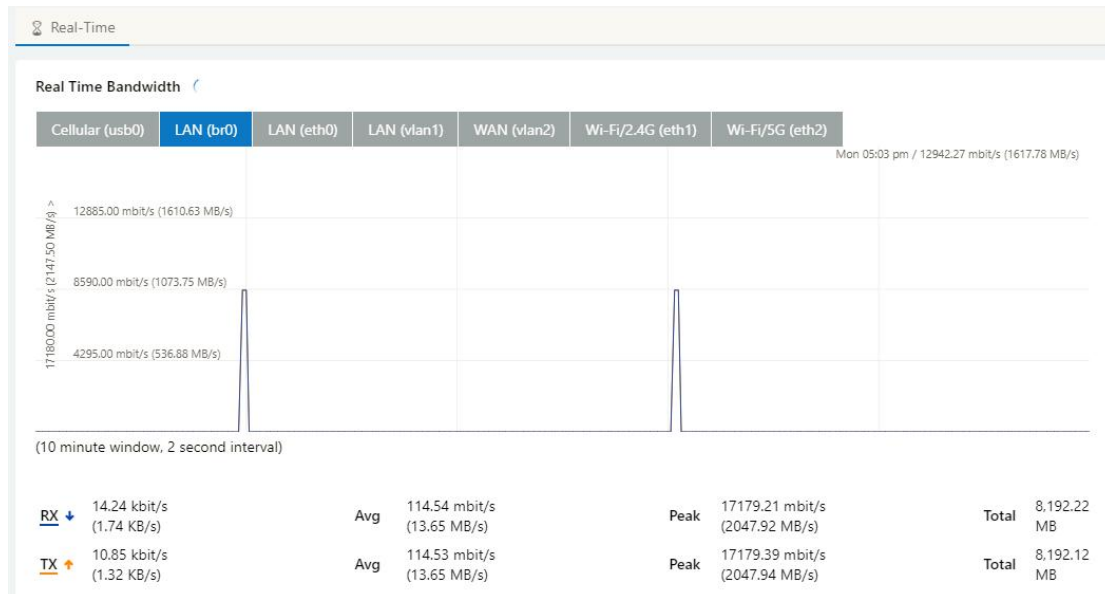
Capture

Time1 15 minutes Start

Network LAN

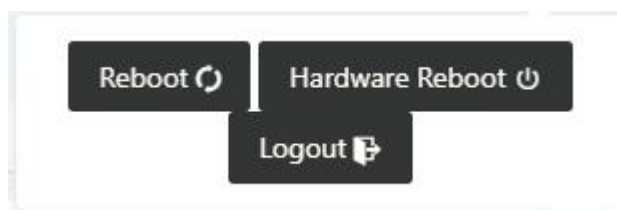
2.3.3 Bandwidth

Click Bandwidth to enter bandwidth graphic GUI. Used to check cellular/LAN/Wi-Fi real-time bandwidth.



2.3.4 System

Click system to choose software reboot, hardware reboot and logout GUI.



2.4 Basic Network

2.4.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface.

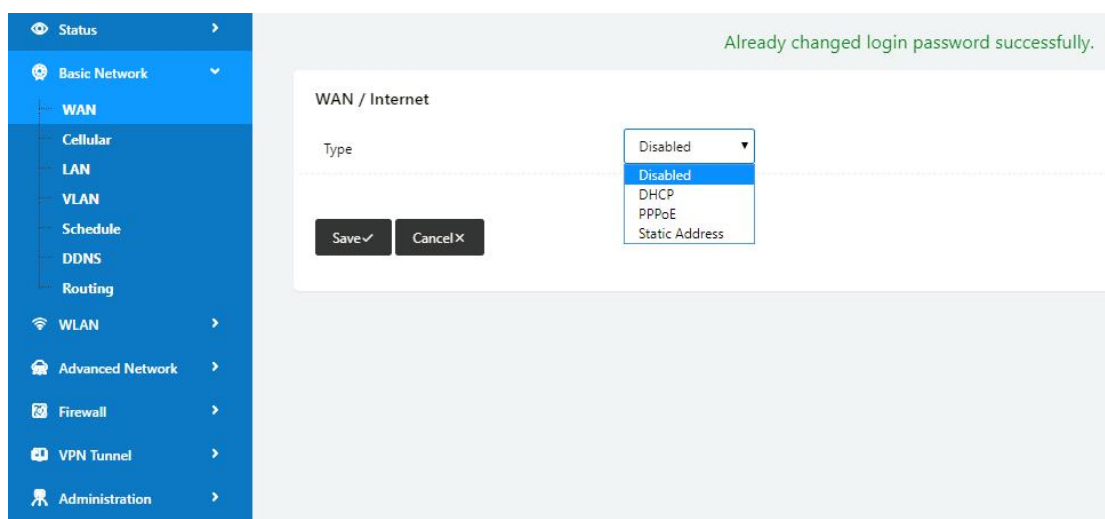


Table 2-1 WAN Setting Instruction

Parameter	Instruction
Type	Support DHCP, PPPoE, Static IP address

Step 2 After setting, please click “save” to finish, the device will reboot.

----End

2.4.2 Cellular Setting

Step 1 Basic Network-> Cellular, you can modify relevant parameter according to the application.

The screenshot displays the 'Cellular Settings' page in the router's web interface. On the left, a blue sidebar contains navigation options: Status, Basic Network (selected), WAN, Cellular (highlighted), LAN, VLAN, Schedule, DDNS, Routing, WLAN, Advanced Network, Firewall, VPN Tunnel, and Administration. The main content area is titled 'Cellular Settings' and features a toggle for 'Enable Modem' which is turned on. Below this are three tabs: 'Basic Settings', 'SIM 1', and 'SIM 2'. The 'Basic Settings' tab is active, showing several configuration options: 'Use PPP' (checkbox), 'ICMP Check' (checkbox), 'Cellular Traffic Check' (checkbox), 'CIMI Send to' (two input fields), 'SMS Code' (input field), 'Operator Lock' (input field with example 'ex:46001'), and 'DualSim Mode' (dropdown menu set to 'Fail Over'). At the bottom of this section are 'Save' and 'Cancel' buttons. The 'SIM 1' tab is also visible, showing fields for 'SIM 1 Mode' (dropdown set to 'Auto'), 'SIM 1 PIN Code', 'SIM 1 APN' (set to '3GNET'), 'SIM 1 User' (set to 'CARD'), 'SIM 1 Password' (masked with dots), 'SIM 1 Dial Number' (set to '*99#'), 'SIM 1 Auth Type' (dropdown set to 'Auto'), and 'SIM 1 Local IP Address'.

Table 2-2 WAN Setting Instruction

Parameter	Instruction
Enable Modem	Enable/Disable 5G mode.
Use PPP	ECM dialup as default. PPP optional.
ICMP check	If enable ICMP check and setup a reachable IP address as destination IP, the router will reconnect/reboot once ICMP check failed.
Cellular Traffic Check	The router will reconnect/reboot once there's no Rx/Tx data.
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock a specified operator for the router by MCC/MNC code.
Dual SIM Mode	<p>【Fail Over】 Two SIM cards mutual backup. Once SIM1 failed, it'll switch to SIM2 and work on SIM2, and vice versa.</p> <p>【SIM1 Only】 Only SIM1 works.</p> <p>【SIM2 Only】 Only SIM2 works.</p> <p>【Backup】 SIM1 is the primary SIM. Once SIM1 failed, it'll switch to SIM2 and work on SIM2 for a specified period of time, then it switches back to SIM1.</p>
Connect Mode	<p>【Auto】 The router will automatically connect to 3G/5G networks and give priority to 5G.</p> <p>【LTE】 Router will connect to 5G only.</p> <p>【3G】 Router will connect to 3G only.</p>
Pin Code	Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen.
APN	APN is provided by local ISP, usually CDMA/EVDO networks do not need this parameter.
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth. Type	Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional.
SIM Local IP Address	Fix SIM IP. The feature is available if carrier can provide this service.



NOTE ICMP Check and Cellular Traffic Check are alternative.

【ICMP Check】

Enable ICMP, Router will automatically check whether the defined IP address is reachable per 60s. If the IP address is unreachable and ICMP check is timeout at the first time, it will check 2 times every 3 seconds. If the third time is still failed, the router will redial.

The ICMP Check IP is a public IP or company server IP address.

ICMP Check	<input checked="" type="checkbox"/>
Check IP	8.8.8.8
Check IP (Optional)	4.4.4.4
Interval	60 (seconds)
Retries	3 (Times)
Fail Action	Reboot System ▼

【Cellular Traffic Check】

【Check Mode】 there are Rx(Receive), Tx(Transmission) and Rx/Tx check modes.

【Rx】Router will check the 3G/LTE cellular receiver traffic. If no receiver traffic within the defined check interval, the router will implement the specified action reconnect or reboot.

Cellular Traffic Check	<input checked="" type="checkbox"/>
Check Mode	Rx ▼
Check Interval	10 (minutes) Range: 1 ~ 1440
Fail Action	Cellular Reconnect ▼

Step 2 After Setting, please click “save” icon.

----End

2.4.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface

Already changed login password successfully.

Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440

1
Add +

Save ✓
Cancel ✕

Table 2-3 LAN Setting Instruction

Parameter	Instruction
Bridge	Supports 4 LAN IP address for br0 to br3 interface. If need to support VLAN, please go to VLAN GUI.
Router IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease
IP Pool	IP address range within LAN
Lease	The valid time, unit as minute
Add	Add LAN IP address, supports 4 LAN IP addresses.

Step 2 After setting, please click “save” to finish, the device will reboot.

----End

2.4.4 VLAN

Step 1 Basic Network->VLAN to enter the VLAN setting page.

Table 2-4 LAN Setting Instruction

Parameter	Instruction
VID	VLAN ID number. The VID range is from 1 to 15.
WAN/LAN1~LAN4	Defined LAN ports in different Bridge.
Tagged	Enable to make router can encapsulate and de-encapsulate the VLAN tag.
Bridge	Route interface br0, br1, br2, br3 and WAN

Step 2 Please Click “Save” to finish.

----End

2.4.5 Schedule

Step 1 Basic Network->Schedule to enter the Schedule setting page.

Parameters	Instruction
modem	The router dial-up to network via modem
wan	The router dial-up to network via WAN (DHCP, PPPOE, Static IP) port.
ICMP Check	When the ICMP Check fails, the switching action between Link1 and Link2 will be triggered.

Link1	The Primary link
Link2	The Secondary link
BACKUP	Link1 and Link2 mutual backup. Link1 is the primary link. Once Link1 is failed, it will switch to Link2 and work on Link2. Once Link1 recovers, it will switch back to Link1.
FAILOVER	Link1 is the primary link, Link2 is the backup link. Once Link1 is failed, it will switch to Link2 and work on Link2.

Link Name	Link Type	Description
modem	ECM/QMI	
wan	WAN(STATIC)	

ICMP Check

On	Link	Destination	Interval	Retries	Description
<input checked="" type="checkbox"/>	wan	8.8.8.8	10	5	
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Schedule

On	Link 1	Link 2	Policy	Description
<input checked="" type="checkbox"/>	wan	modem	FAILOVER	wan as primary and modem as secondary
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>



The VLAN should be configured with WAN and 5G backup together. Please define WAN port as bridge WAN interface in the VLAN GUI as below.

Already changed login password successfully.

VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	br0
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WAN
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none

Step 2 Please Click "Save" to finish.

----End

2.4.6 Dynamic DNS Setting

Step 1 Basic Network->DDNS to enter the DDNS setting page.

Dynamic DNS

IP Address: Use WAN IP Address 0.0.0.0 (recommended)

Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None

Save Cancel

Table 2-5 DDNS Setting Instruction

parameter	Instruction
IP address	Default is standard DDNS protocol, for customized protocol, please contact Wlink engineer. Usually, use default IP 0.0.0.0
Auto refresh time	Set the interval of the DDNS client obtains new IP, suggest 240s or above
Service provider	Select the DDNS service provider that listed.

Step 2 Please Click "Save" to finish.

----End

2.4.7 Routing Setting

Step 1 Basic Network->Routing to enter the DDNS setting GUI.

Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
192.168.1.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo

Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
	0.0.0.0		0	LAN	

Miscellaneous

Mode: Gateway

RIPv1 & v2: Disabled

DHCP Routes: ☒

Spanning-Tree Protocol: ☐

Save Cancel

Table 2-6 Routing Setting Instruction

Parameter	Instruction
Destination	Router can reach the destination IP address.
Gateway	Next hop IP address which the router will reach
Subnet Mask	Subnet mask for destination IP address
Metric	Metrics are used to determine whether one particular route should be chosen over another.
Interface	Interface from router to gateway.

Parameter	Instruction
Description	Describe this routing name.

Step 2 Please Click “ Save “ to finish.

----End

2.5 WLAN Setting

It's mainly for router which support Wi-Fi, you can modify and configure WLAN parameter through Web GUI, below is the common setting.

2.5.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter

Wireless(2.4 GHz)	Wireless(5 GHz)
Enable WLAN	<input checked="" type="checkbox"/>
MAC Address	34:0A:92:19:51:03
Wireless Mode	Access Point ▼
Radio Band	2.4 GHz ▼
Wireless Network Mode	Auto ▼
SSID	router-wifi_195103
Broadcast SSID	<input checked="" type="checkbox"/>
Channel	7 - 2.442 GHz ▼ Scan 🔍
Channel Width	40 MHz ▼
Control Sideband	Lower ▼
Maximum Clients	128 (range: 1 - 255)
Security option	Disabled ▼

Wireless(2.4 GHz)	Wireless(5 GHz)
Enable WLAN	<input checked="" type="checkbox"/>
MAC Address	34:0A:92:19:51:04
Wireless Mode	Access Point ▼
Radio Band	5 GHz ▼
Wireless Network Mode	Auto ▼
SSID	router-wifi_195103_5G
Broadcast SSID	<input checked="" type="checkbox"/>
Channel	149 - 5.745 GHz ▼ Scan 🔍
Channel Width	80 MHz ▼
Control Sideband	Lower ▼
Maximum Clients	128 (range: 1 - 255)
Security option	Disabled ▼

Table 2-7 Basic of WLAN Setting Instruction

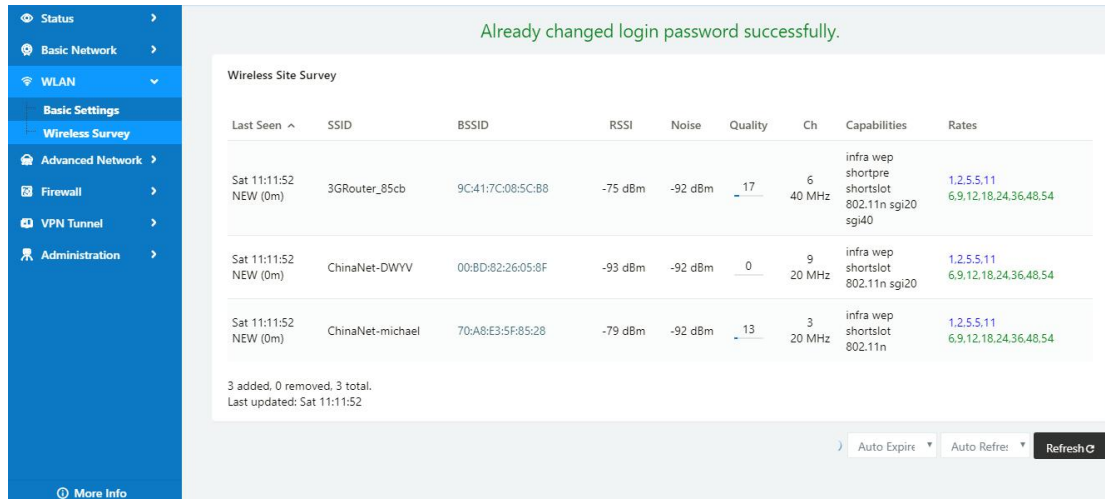
Parameter	Instruction
Radio Mode	2.4G+5G mode as default. Support 2.4G, 5G modes optional. 2.4G+5G model, Wi-Fi bandwidth for 683Mbps 2.4G model, Wi-Fi bandwidth for 300Mbps 5G model, Wi-Fi bandwidth for 866Mbps
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP mode and Client Optional.
Wireless Network protocol	Support Auto/b/g/n optional for 2.4G. Support Auto/A/N optional for 5G.
SSID	The default is router, can be modified as per application.
Channel	The channel of wireless network, suggest keep the default
Channel Width	20MHz and 40MHz alternative for 2.4G. 20MHz, 40MHz and 80MHz alternative for 5G.
Security	Support various encryption method as requested.

Step 2 Please click "Save" to finish.

----End

2.5.2 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.



2.6 Advanced Network Setting

2.6.1 Port Forwarding

Step 1 Advanced Network > Port Forwarding to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

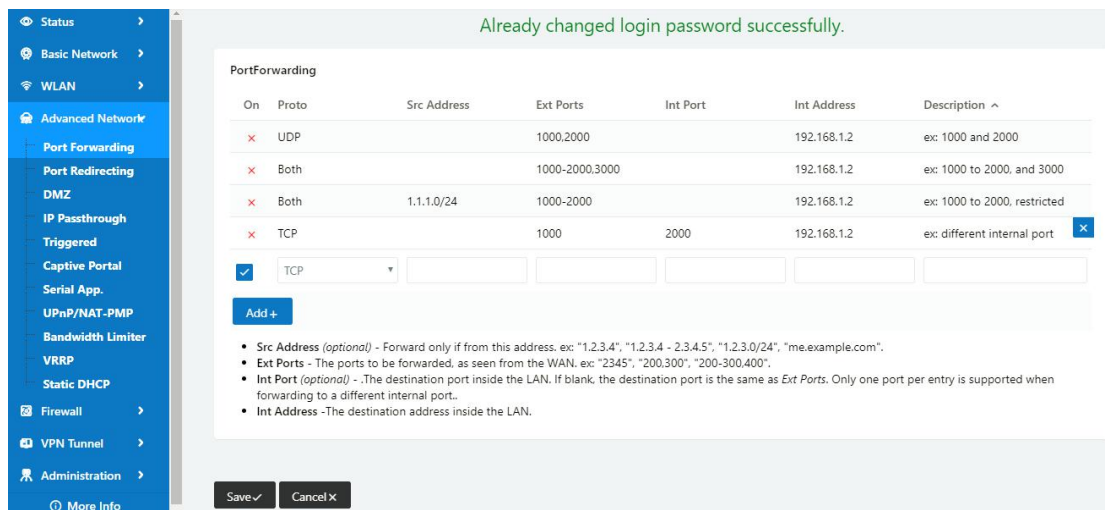


Table 2-8 Port Forwarding Instruction

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Src. Address	Source IP address. Forward only if from this address.

Parameter	Instruction
Ext. Ports	External ports. The ports to be forwarded, as seen from the WAN.
Int. Port	Internal port. The destination port inside the LAN. If blank, the destination port is the same as Ext Ports. Only one port per entry is supported when forwarding to a different internal port.
Int. Address	Internal Address. The destination address inside the LAN.
Description	Remark the rule

Step 2 Please click "save" to finish

----End

2.6.2 Port Redirecting

Step 1 Advanced Network > Port Redirecting to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

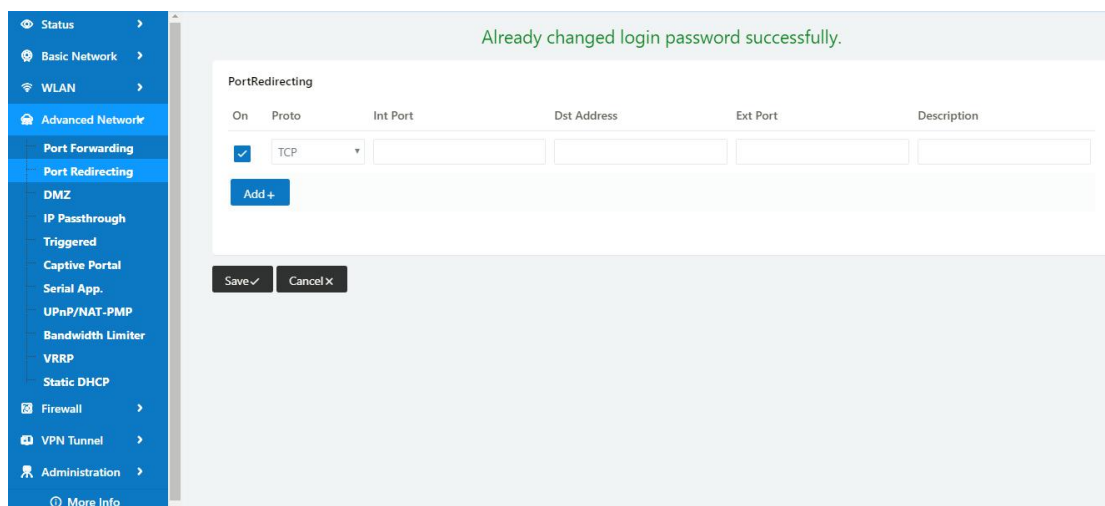


Table 2-9 Port Redirecting Instruction

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Int Port	Internal port.
Dst. Address	The redirecting IP address.
Ext. Ports	External port for redirection.
Description	Remark the rule

Step 2 Please click "save" to finish

----End

2.6.3 DMZ Setting

Step 1 Advanced Network> DMZ to check or modify the relevant parameter.

Table 2-10 DMZ Instruction

parameter	Instruction
Destination Address	The destination address inside the LAN.
Source Address Restriction	If no IP address inside, it will allow all IP address to access. If define IP address, it will just allow the defined IP address to access.
Leave Remote Access	

Step 2 Please click "save" to finish

----End

2.6.4 IP Passthrough Setting

Step 1 Advanced Network> IP Passthrough to check or modify the relevant parameter.

Table 2-11 IP Passthrough Instruction

parameter	Instruction
Enable	Enable IP Passthrough
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.
Gateway	If WL-G530 connect to multiple device, input other device gateway. The device might access to router GUI.

Step 2 Please click "save" to finish

----End

2.6.5 Triggered Setting

Step 1 Advanced Network> Triggered to check or modify the relevant parameter.

Table 2-12 Triggered Instruction

parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.
Note	Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic.

Step 2 Please click "save" to finish.

----End

2.6.6 Captive Portal

Step 1 Advanced Network> Triggered to check or modify the relevant parameter.

Table 2-13 Captive Portal Instruction

Parameter	Instruction
Enable	Enable Captive portal feature.
Auth Type	Reserved.
Web Root	Choose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router's Flash. Ex-storage: Captive portal file is in extended storage such as SD card.

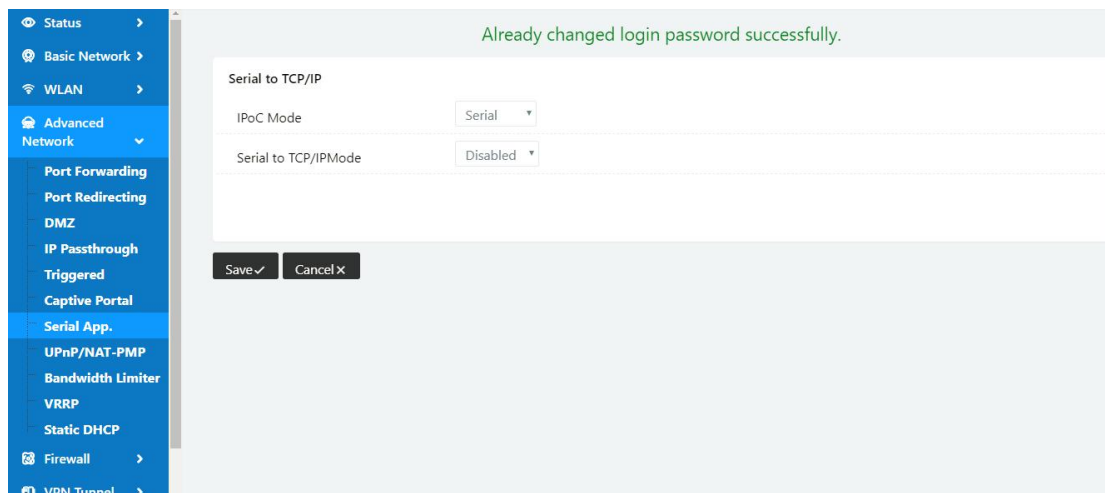
Parameter	Instruction
Web Host	Configure domain name for the captive portal access. For example, Configure as wlink.tech.com, we might directly access to captive portal page in the website as wlink.tech.com
Portal Host	Reserved.
Logged Timeout	Maximum time user has connectivity. User need to re-login Captive Portal page after defined time.
Idle Timeout	Maximum time user has connectivity if no network activity from Wi-Fi User.If User need to re-login Captive page to surf internet.
Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.
Redirecting	Router will redirect to the defined link after accepting the terms and conditions on the Captive Portal page.
MAC Whitelist	No captive portal page for Wi-Fi device.
Download QoS	Enable to apply the Download and Upload per user limits.
Upload Qos	Maximum download speed available to each user.

Step 2 Please click "save" to finish.

----End

2.6.7 Serial App. Setting

Step 1 Advanced Network> Serial App to check or modify the relevant parameter.



Serial to TCP/IP

IPoC Mode

Serial

Serial to TCP/IP Mode

Client

Server IP/Port

8.8.8.8

:

40002

Socket Type

TCP

Socket Timeout

500

(milliseconds)

Serial Timeout

500

(milliseconds)

Packet Payload

1024

(bytes)

Heart-Beat Content

Heart-Beat Interval

2

(seconds)

Port Type

RS485/RS232

Cache Enable

☒

Debug Enable

☐

Baud Rate

57600

Parity Bit

none

Data Bit

8

Stop Bit

1

Save

Cancel

Table 2-14 Serial App Instruction

Parameter	Instruction
Serial to TC/IP mode	Support Disable, Server and Client mode. Such as Client.
Server IP/Port	IP address and domain name are acceptable for Server IP
Socket Type	Support TCP/UDP protocol
Socket Timeout	Router will wait the setting time to transmit data to serial port.
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that is less the Packet payload. If the last package equals to the Packet payload, Serial port will transmit it immediately. The default setting is 500ms.
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.
Heart-beat Content	Send heart beat to the defined server to keep router online. Meantime, it's convenient to monitor router from server.
Heart beat Interval	Heart beat interval time

Parameter	Instruction
Baud Rate	115200 as default
Parity Bit	None as default
Data Bit	8bit as default
Stop Bit	1bit as default



Serial port connection

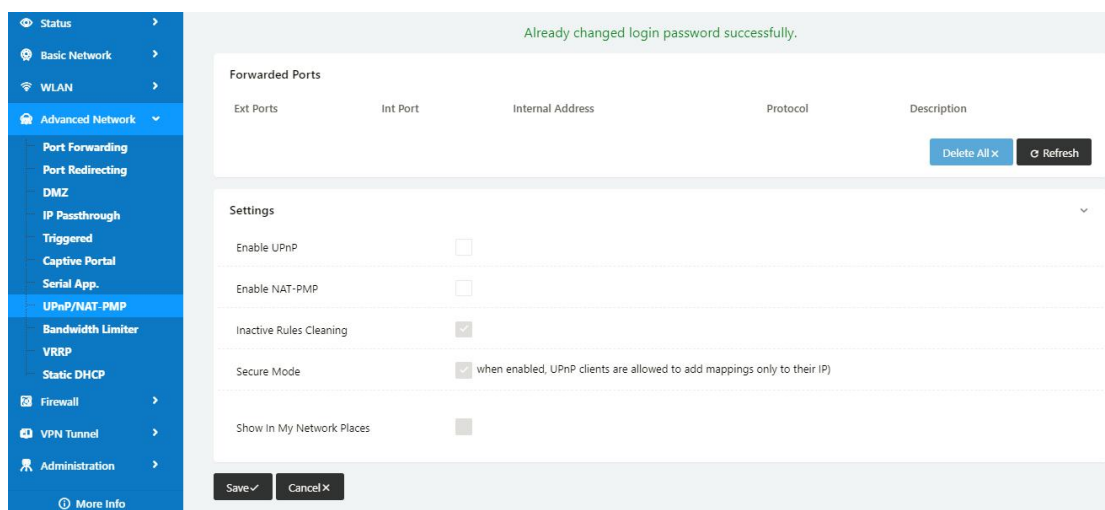
PINs		DB9(male)
V+		
V-		
GND	----	5
RX	----	3
TX	----	2
DI-1		
DI-2		
DO		

Step 2 Please click "save" to finish.

----End

2.6.8 UPnp/NAT-PMP Setting

Step 1 Advanced Network> Upnp/NAT-PMP to check or modify the relevant parameter.



Step 2 Please click "save" to finish.

----End

2.6.9 Bandwidth Control Setting

Step 1 Advanced Network> Bandwidth Control to check or modify the relevant parameter.

Table 2-15 Bandwidth Control Instruction

Max Available Download	Speed limit for router.
Max Available Upload	Speed limit for router.
IP/ IP Range/ MAC Address	Limit devices speed for specified IP/IP Range/ MAC Address.
DL Rate	Mix Download rate
DL ceil	Max download rate
UL Rate	Mix Upload rate
UL ceil	Max upload rate
Priority	The priority of a specific user.
Default Class	If no specified IP/MAC, the download and upload limit for total speed for all of device.

Step 2 Please click "save" to finish.

----End

2.6.10 VRRP Setting

Step 1 Advanced Network> VRRP to check or modify the relevant parameter.

Step 2 Please click "save" to finish.

----End

2.6.11 Static DHCP Setting

Step 1 Advanced Network> Static DHCP to check or modify the relevant parameter.

Step 2 Please click "save" to finish.

----End

2.7 Firewall

2.7.1 IP/URL Filtering

Step 1 Firewall> IP/URL Filtering to check or modify the relevant parameter.

Status

Basic Network

WLAN

Advanced Network

Firewall

IP/URL Filtering

Domain Filtering

VPN Tunnel

Administration

More Info

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NOH			Acce	
Add +								

Key Word Filtering

On	Key Word	Description
<input checked="" type="checkbox"/>		
Add +		

URL Filtering

On	URL	Description
<input checked="" type="checkbox"/>		
Add +		

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NOH			Acce	
Add +								

Key Word Filtering

On	Key Word	Description
<input checked="" type="checkbox"/>		
Add +		

URL Filtering

On	URL	Description
<input checked="" type="checkbox"/>		
Add +		

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>				NOH			Acce	
Add +								

Save ✓ Cancel ✕

Table 2-16 IP/URL Filtering Instruction

Parameter	Instruction
IP/MAC/Port Filtering	Support IP address, MAC address and port filter. Accept/Drop options for filter policy.
Key Word Filtering	Support key word filter.
URL Filtering	Support URL filter.
Access Filtering	Support Access Filter.

Step 2 Please click "save" to finish.

---End

2.7.2 Domain Filtering

Step 1 Firewall> Domain Filtering to check or modify the relevant parameter.

Table 2-17 Domain Filtering Instruction

Parameter	Instruction
Default Policy	Support black list and white list
Local IP Address	Local IP address for LAN.
Domain	Support Domain filter.

Step 2 Please click "save" to finish.

----End

2.8 VPN Tunnel

2.8.1 GRE Setting

Step 1 VPN Tunnel> GRE to check or modify the relevant parameter.

Table 2-18 GRE Instruction

Parameter	Instruction
IDx	GRE tunnel number
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.
Tunnel Source	Router's 3G/WAN IP address.
Tunnel Destination	GRE Remote IP address. Usually a public IP address
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.
Interval	Keep alive interval time.
Retries	Keep alive retry times. After retry times, GRE tunnel will be re-established.
Description	

Step 2 Please click "save" to finish.

----End

2.8.2 OpenVPN Client Setting

Step 1 VPN Tunnel> OpenVPN Client to check or modify the relevant parameter.

The screenshot shows the 'OpenVPN Client' configuration page. On the left is a blue sidebar menu with options: Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel (selected), GRE, OpenVPN Client (active), PPTP/L2TP Client, IPSec, and Administration. The main content area is titled 'OpenVPN Client' and has tabs for 'Client 1' and 'Client 2'. Below the tabs are sub-tabs: 'Basic', 'Advanced', 'Keys', and 'Status'. The 'Basic' tab is active, showing settings for 'VPN Client #1 (Stopped)'. The settings include: 'Start with WAN' (checkbox), 'Interface Type' (dropdown set to 'TUN'), 'Protocol' (dropdown set to 'UDP'), 'Server Address' (text input with '1194' in a box), 'Firewall' (dropdown set to 'Automatic'), 'Authorization Mode' (dropdown set to 'TLS'), 'Username/Password Authentication' (checkbox), 'HMAC authorization' (dropdown set to 'Disabled'), and 'Create NAT on tunnel' (checkbox checked). At the bottom is a 'Start Now' button.

OpenVPN Client

Client 1

Client 2

Basic

Advanced

Keys

Status

VPN Client #1 (Stopped)

Start with WAN

Interface Type

TUN

Protocol

UDP

Server Address

1194

Firewall

Automatic

Authorization Mode

TLS

Username/Password Authentication

HMAC authorization

Disabled

Create NAT on tunnel

Start Now

Save

Cancel

Table 2-19 Basic of OpenVPN Instruction

Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 5G/3G/WAN port.
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.
Protocol	UDP and TCP optional.
Server Address	The Openvpn server public IP address and port.
Firewall	Auto, External only and Custom are optional
Authorization Mode	TLS, Static key and Custom are optional.
User name/Password	As the configuration requested.

Parameter	Instruction
Authentication	
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.

Basic Advanced Keys Status

VPN Client #1 (Stopped)

Poll Interval (in minutes, 0 to disable)

Redirect Internet traffic ☐

Accept DNS configuration

Encryption cipher

Compression

TLS Renegotiation Time (in seconds, -1 for default)

Connection retry (in seconds; -1 for infinite)

Verify server certificate (tls-remote) ☐

Custom Configuration

Start Now

Table 2-20 Advanced of OpenVPN Instruction

Parameter	Instruction
Poll Interval	Openvpn client check router's status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As the configuration requested.
Encryption	As the configuration requested.
Compression	As the configuration requested.
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.
Connection Retry Time	Openvpn retry to connection interval.
Verify server certificate	As the configuration requested.
Custom Configuration	As the configuration requested.

Basic Advanced **Keys** Status

VPN Client #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

Client Certificate

Client Key

Start Now

Table 2-21 Keys of OpenVPN Instruction

Parameter	Instruction
Certificate Authority	Keep certificate as the same as server
Client Certificate	Keep client certificate as the same as server
Client Key	Keep client key as the same as server

OpenVPN Client

Client 1 Client 2

Basic Advanced **Keys** Status

VPN Client #1 (Stopped)

Client is not running or status could not be read.

Refresh Status

Start Now

Table 2-22 Status of OpenVPN Instruction

Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 2 Please click "save" to finish.

----End

2.8.3 PPTP/L2TP Client Setting

Step 1 VPN Tunnel> VPN Client to check or modify the relevant parameter.

VPN Tunnel

L2TP/PPTP Basic

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
<input checked="" type="checkbox"/>	L2TP					<input type="checkbox"/>	<input type="checkbox"/>	
Add +								

L2TP Advanced

On	Name	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>		
Add +							

PPTP Advanced

On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>	<input type="checkbox"/>	
Add +							

Schedule

On	Name 1	Name 2	Policy	Description
<input checked="" type="checkbox"/>			FAILOVER	
Add +				

Table 2-23 PPTP/L2TP Basic Instruction

parameter	Instruction
On	VPN enable
Protocol	VPN Mode for PPTP and L2TP
Name	VPN Tunnel name
Server Address	VPN Server IP address.
User name	As the configuration requested.
Password	As the configuration requested.
Firewall	Firewall For VPN Tunnel
Local IP	Defined Local IP address for tunnel

Table 2-24 L2TP Advanced Instruction

On	L2TP Advanced enable
Name	L2TP Tunnel name
Accept DNS	As the configuration requested.
MTU	MTU is 1450bytes as default
MRU	MRU is 1450bytes as default
Tunnel Auth.	L2TP authentication Optional as the configuration requested.
Tunnel Password	As the configuration requested.

Custom Options	As the configuration requested.
----------------	---------------------------------

Table 2-25 PPTP Advanced Instruction

On	PPTP Advanced enable
Name	PPTP Tunnel name
Accept DNS	As the configuration requested.
MTU	MTU is 1450bytes as default
MRU	MRU is 1450bytes as default
MPPE	As the configuration requested
MPPE Stateful	As the configuration requested
Customs	As the configuration requested

Table 2-26 SCHEDULE Instruction

On	VPN SCHEDULE feature enable
Name1	VPN tunnel name
Name2	VPN tunnel name
Policy	Support VPN tunnel backup and failover modes optional
Description	As the configuration requested

Step 2 Please click "save" to finish.

---End

2.8.4 IPSec Setting

Already changed login password successfully.

IPSec

IPSec 1 | IPSec 2 | Schedule

Group Setup | Basic Setup | Advanced Setup

Enable IPSec ☐

IPSec Extensions Normal ▾

Local Security Gateway Interface 3G Cellular ▾

Local Security Group Subnet/Netmask 192.168.1.0/24 ex. 192.168.1.0/24

Local Security Firewalling ☒

Remote Security Gateway IP/Domain

Remote Security Group Subnet/Netmask 10.0.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☒

Save ✓ Cancel ✕

2.8.4.1 IPSec Group Setup

Step 1 IPSec> Group Setup to check or modify the relevant parameter.

Group Setup | Basic Setup | Advanced Setup

Enable IPSec ☐

IPSec Extensions Normal ▾

Local Security Gateway Interface 3G Cellular ▾

Local Security Group Subnet/Netmask 192.168.1.0/24 ex. 192.168.1.0/24

Local Security Firewalling ☒

Remote Security Gateway IP/Domain

Remote Security Group Subnet/Netmask 10.0.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☒

Table 2-27 IPSec Group Setup Instruction

parameter	Instruction
IPSec Extensions	Support Standard IPSec, GRE over IPSec, L2TP over IPSec
Local Security Interface	Defined the IPSec security interface
Local Subnet/Mask	IPSec local subnet and mask.
Local Firewall	Forwarding-firewalling for Local subnet

parameter	Instruction
Remote IP/Domain	IPsec peer IP address/domain name.
Remote Subnet/Mask	IPSec remote subnet and mask.
Remote Firewall	Forwarding-firewalling for Remote subnet

Step 2 Please click "save" to finish.

2.8.4.2 IPSec Basic Setup

Step 1 IPSec >Basic Setup to check or modify the relevant parameter.

Group Setup	Basic Setup	Advanced Setup
Keying Mode IKE with Preshared Key ▼		
Phase 1 DH Group Group 2 - modp1024 ▼		
Phase 1 Encryption 3DES (168-bit) ▼		
Phase 1 Authentication MD5 HMAC (96-bit) ▼		
Phase 1 SA Life Time 28800 seconds		
Phase 2 DH Group Group 2 - modp1024 ▼		
Phase 2 Encryption 3DES (168-bit) ▼		
Phase 2 Authentication MD5 HMAC (96-bit) ▼		
Phase 2 SA Life Time 3600 seconds		
Preshared Key <input type="text"/>		

Table 2-28 IPSec Basic Setup Instruction

parameter	Instruction
Keying Mode	IKE preshared key
Phase 1 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPsec setting.
Phase 1 Encryption	Support 3DES, AES-128, AES-192, AES-256

parameter	Instruction
Phase 1 Authentication	Support HASH MD5 and SHA
Phase 1 SA Life Time	IPSec Phase 1 SA lifetime
Phase 2 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.
Phase 2 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase 2 Authentication	Support HASH MD5 and SHA
Phase 2 SA Life Time	IPSec Phase 2 SA lifetime
Preshared Key	Preshared Key

Step 2 Please click "save" to finish.

2.8.4.3 IPSec Advanced Setup

Step 1 IPSec >Advanced Setup to check or modify the relevant parameter.

Group Setup	Basic Setup	Advanced Setup
		Aggressive Mode <input type="checkbox"/>
		Compress(IP Payload Compression) <input type="checkbox"/>
		Dead Peer Detection(DPD) <input type="checkbox"/>
		ICMP Check <input type="checkbox"/>
		IPSec Custom Options 1 <input type="text"/>
		IPSec Custom Options 2 <input type="text"/>
		IPSec Custom Options 3 <input type="text"/>
		IPSec Custom Options 4 <input type="text"/>

Table 2-29 IPSec Advanced Setup Instruction

parameter	Instruction
Aggressive Mode	Default for main mode
ID Payload Compress	Enable ID Payload compress
DPD	To enable DPD service
ICMP	ICMP Check for IPSec tunnel
IPSec Custom Options	IPSec advanced setting such as left/right ID.

Step 2 Please click "save" to finish.

----End

2.9 Administration

2.9.1 Identification Setting

Step 1 Please click "Administrator> Identification" to enter the GUI, you may modify the router name, Host name and Domain name according to self-requirement.

Router Identification

Router Name

Hostname

Domain Name

Table 2-30 Router Identification Instruction

Parameter	Instruction
Router name	Default is router, can be set maximum 32 character
Host name	Default is router, can be set maximum 32 character

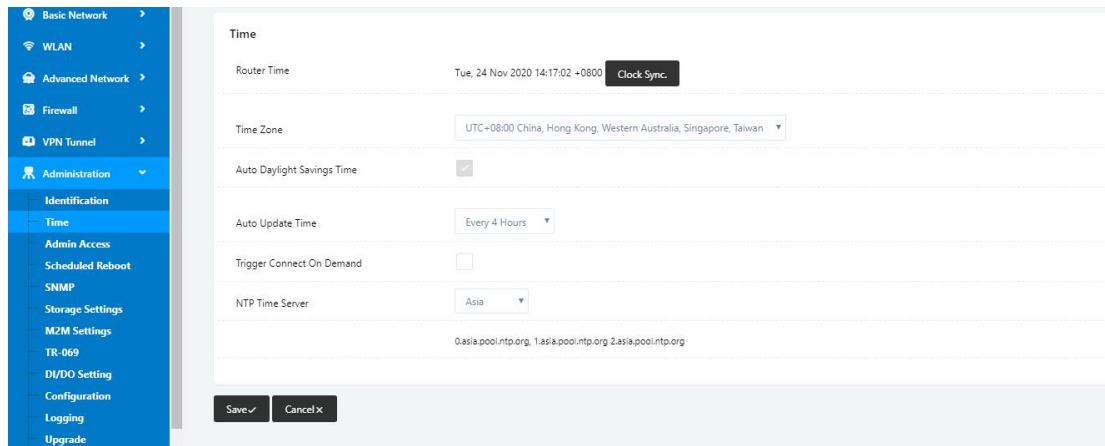
Parameter	Instruction
Domain name	Default is empty, support maximum up to 32 character, it is the domain of WAN, no need to configure for most application.

Step 2 Please click "save" to finish

----End

2.9.2 Time Setting

Step 1 Please click “Administrator> time” to check or modify the relevant parameter.




If the device is online but time update is fail, please try other NTP Time Server.

Step 2 Please click “save to finish.

----End

2.9.3 Admin Access Setting

Step 1 Please click “Administrator>Admin” to check and modify relevant parameter.

In this page, you can configure the basic web parameter, make it more convenient for usage. Please note the “password” is the router system account password.

Step 2 Please click save icon to finish the setting

----End

2.9.4 Schedule Reboot Setting

Step 1 Please click “Administrator>Schedule Reboot” to check and modify relevant parameter.

Step 2 Please click save icon to finish the setting

----End

2.9.5 SNMP Setting

Step 1 Please click “Administrator>SNMP” to check and modify relevant parameter.

SNMP Settings

Enable SNMP ☐

Port

Remote Access ☐

Allowed Remote IP Address
(optional; e.g. "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2")

System Name

Location

Contact

RO Community

RW Community

SNMPv3 Authentication Type

SNMPv3 Privacy Type

Step 2 Please click save icon to finish the setting

----End

2.9.6 Storage Setting

Step 1 Please click “Administrator>Storage Setting” to check and modify relevant parameter.

Storage settings

Storage Total:16.00 MB Free:15.50 MB

Upload new file

No file chosen

Current file list

File name	File size	File operation
sms.list	408	<input type="button" value="X"/> <input type="button" value="Download"/>

Step 2 Please click save icon to finish the setting

----End

2.9.7 M2M Access Setting (Apply to M2M Management Platform installation application only)

Step 1 Please click “Administrator>M2M Access” to check and modify relevant parameter.

Already changed login password successfully.

- Status
- Basic Network
- WLAN
- Advanced Network
- Firewall
- VPN Tunnel
- Administration
- Identification
- Time
- Admin Access
- Scheduled Reboot
- SNMP
- Storage Settings
- M2M Settings
- DI/DO Setting
- Configuration
- Logging
- Upgrade

More Info

m2m

M2M Enabled ☐

Fail Action Restart M2M

Device ID

M2M Server/Port : 8000

Heartbeat Intval 60 (seconds)

Heartbeat Retry 10 (Range:10-1000)

Named-Pipe Enabled Remote Connect

Named-Pipe Server Port 8002 (Range:1024-65535)

Named-Pipe Status Offline

Named-Pipe Address 0.0.0.0

Save Cancel

Step 2 Please click save iron to finish the setting

----End

2.9.8 TR-069 Setting

Step 3 Please click "Administrator>TR-069 Setting" to check and modify relevant parameter.

- Basic Network
- WLAN
- Advanced Network
- Firewall
- VPN Tunnel
- Administration
- Identification
- Time
- Admin Access
- Scheduled Reboot
- SNMP
- Storage Settings
- M2M Settings
- TR-069
- DI/DO Setting
- Configuration
- Logging
- Upgrade

TR069

Enabled ☐

Enable Periodic Transmission ☐

Username openacs

Password openacs

URL http://192.168.1.110:8080/openacs/acs

Save Cancel

Step 4 Please click save iron to finish the setting

----End

2.9.9 DI/DO Setting

Step 1 Please click “Administrator>DI/DO Setting” to check and modify relevant parameter.

DI Setting

Enabled ☒ Port1 ☒ Port2 ☐

Port1Mode

Filter (*100ms)

SMS Alarm ☐

DO Setting

Enabled ☐ Port1 ☐ Port2 ☐

Save Cancel

2.9.7.1 DI Configure

DI Setting

Enabled ☒ Port1 ☒ Port2 ☐

Port1Mode

Filter (*100ms)

SMS Alarm ☐

DO Setting

Enabled ☐ Port1 ☒ Port2 ☐

Alarm Source ☐ SMS Control ☐

Alarm Action

Power On Status

Keep On (*100ms)

Table 2-31 DI Instruction

Parameter	Instruction
Enable	Enable DI. Port1 is for I/O1 and Port2 is I/O2. Both I/O1 and I/O2 are DI ports
Mode	Selected from OFF, ON and EVENT_COUNTER modes. OFF Mode: DI from high level(3.3v~5V) to low level(0V), it will trigger alarm. ON Mode: DI from low level(0V) to high level(3.3v~5V), it will trigger alarm. EVENT_COUNTER Model: Enter EVENT_COUNTER mode.
Filter	Software filtering is used to control switch bounces. Input (1~100)*100ms. Under OFF and ON modes, WL-G530 detects pulse signal and compares with first pulse shape and last pulse shape. If both are the same level, WL-G530 will trigger alarm. Under EVENT_COUNTER mode, if first pulse shape and last pulse shape are not the same level, WL-G530 will trigger alarm according to Counter Action setting.
Counter Trigger	Available when DI under Event Counter mode Input from 0 to 100. (0=will not trigger alarm) It will trigger alarm when counter reaches this value. After triggering alarm, DI will keep counting but no trigger alarm again.
Counter Period	It's a reachable IP address. Once the ICMP check is failed, GRE will be established again.
Counter Recover	it will re-count after counter trigger alarm. The value is 0~30000(*100ms). 0 means no counter.
Counter Action	HI_TO_LO and LO_TO_HI is available when DI under Event Counter mode. In Event Counter mode, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When LO_TO_HI is selected, the counter value increase when the attached switch is pushed. When HI_TO_LO is selected, the counter value increases when the switch is pushed and released.
Counter Start	Available when DI under EVENT_COUNTER mode. Start counting when enable this feature.
SMS Alarm	The alarm SMS will send to specified phone group. Each phone group include up to 2 phone numbers.
SMS Content	70 ASCII Char Max
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

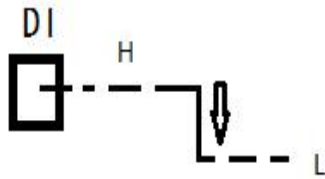
Step 2 Please click "save" to finish.



NOTE

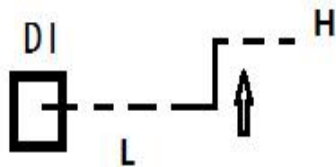
OFF Mode

DI from high level 3.3~5V to low level 0V will be triggered.



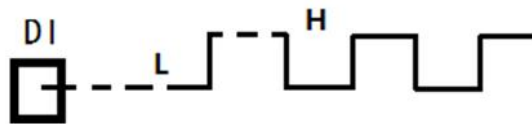
ON Mode

Data input from low level 0V to high level 3.3~5V will be triggered.



EVENT_COUNTER Model

The counted number of pulses will be triggered.



2.9.7.2 DO Configure

DO Setting

Enabled ☒

Alarm Source

DI Control ☒
SMS Control ☒

Alarm Action

ON

Power On Status

OFF

Keep On

1

(*100ms)

SMS Trigger Content

70 ASCII Max

SMS Reply Content

70 ASCII Max

SMS admin Num1

SMS admin Num2

Backup

Save ✓

Cancel ✕

Table 2-32 DO Instruction

Parameter	Instruction
Enable	1 DO as selected
Alarm Source	<p>Digital output initiates according to different alarm source. Select from DI Alarm, SMS Control and M2M Control. Selections can be one or more.</p> <p>DI Alarm: Digital Output triggers the related action when there is alarm from Digital Input.</p> <p>SMS Control: Digital Output triggers the related action when receiving SMS from the number in phone book.</p> <p>M2M Control: it's not ready.</p>
Alarm Action	<p>Digital Output initiates when there is an alarm. Selected from "OFF", "ON", "Pulse".</p> <p>OFF: Open from GND when triggered.</p> <p>ON: Short contact with GND when triggered.</p> <p>Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.</p>
Power on Status	<p>Specify the digital Output status when power on. Selected from OFF and ON.</p> <p>OFF: low level(0V).</p> <p>ON: high level(4.8-5.0V)</p>
Keep On	<p>Available when digital output Alarm On Action/Alarm Off Action status is ON, input the Digital Output keep on status time. Input from 0 to 255 seconds. (0=keep on until the next action)</p>
Delay	<p>Available when enable Pulse in Alarm On Action/Alarm Off Action. The first pulse will be generated after a "Delay" .</p>

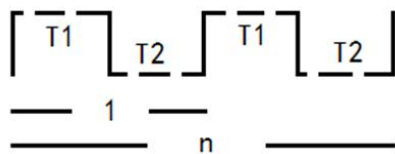
Parameter	Instruction
	Input from 0 to 30000ms. (0=generate pulse without delay)
Low	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Input from 1 to 30000 ms.
High	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Input from 1 to 30000 ms.
Output	Available when enable Pulse in Alarm On Action/Alarm Off Action. The number of pulses, input from 0 to 30000. (0 for continuous pulse output)
SMS Trigger Content	Available when enable SMS Control in Alarm Source. Input the SMS content to enable "Alarm On Action" by SMS (70 ASCII II char max).
SMS Reply Content	Input the SMS content, which will be sent after DO was triggered. (70 ASCII II char max).
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 3 Please click "save" to finish.



NOTE

DO might be customized pulse width ratio: T1, T2 duration and n value.



2.9.10 Configuration Setting

Step 1 Please click " Administrator> Configuration " to do the backup setting

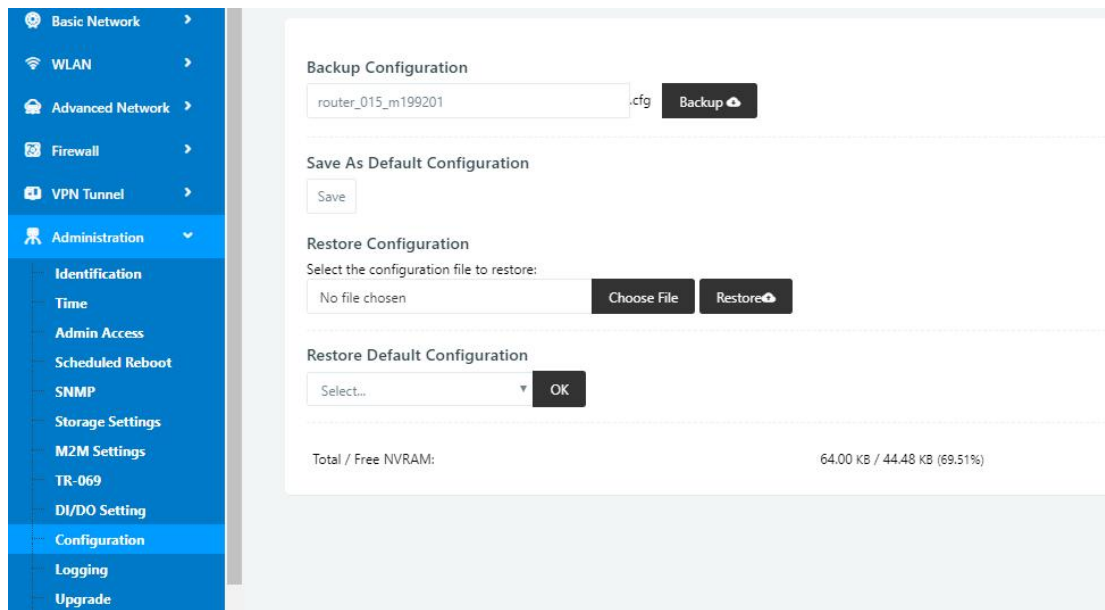


Figure 3-1 Backup and Restore Configuration GUI



Restore Default would lose all configuration information, please be careful.

Step 2 After setting the backup and restore configuration. The system will reboot automatically.

----End

2.9.11 System Log Setting

Step 1 Please click “Administrator> Logging” to start the configuration, you can set the file path to save the log (Local or remote sever).

The screenshot displays the 'Syslog' configuration page in the router's web interface. On the left, a blue sidebar lists various system settings, with 'Logging' highlighted under the 'Administration' section. The main content area has a light gray background and contains the following settings:

- Syslog**: The section title.
- Log Internally**: A checkbox that is currently checked with a blue checkmark.
- Log To Remote System**: An unchecked checkbox.
- Generate Marker**: A dropdown menu set to 'Every 1 Hour'.
- Limit**: A text input field containing '60', with a note '(messages per minute / 0 for unlimited)' to its right.

At the bottom of the configuration area, there are two buttons: 'Save' with a checkmark icon and 'Cancel' with an 'x' icon.

Figure 3-1 System log Setting GUI

Step 2 After configure, please click “Save” to finish.

----End

2.9.12 Firmware upgrade

Step 1 Please click “Administrator>firmware upgrade” to open upgrade firmware tab.

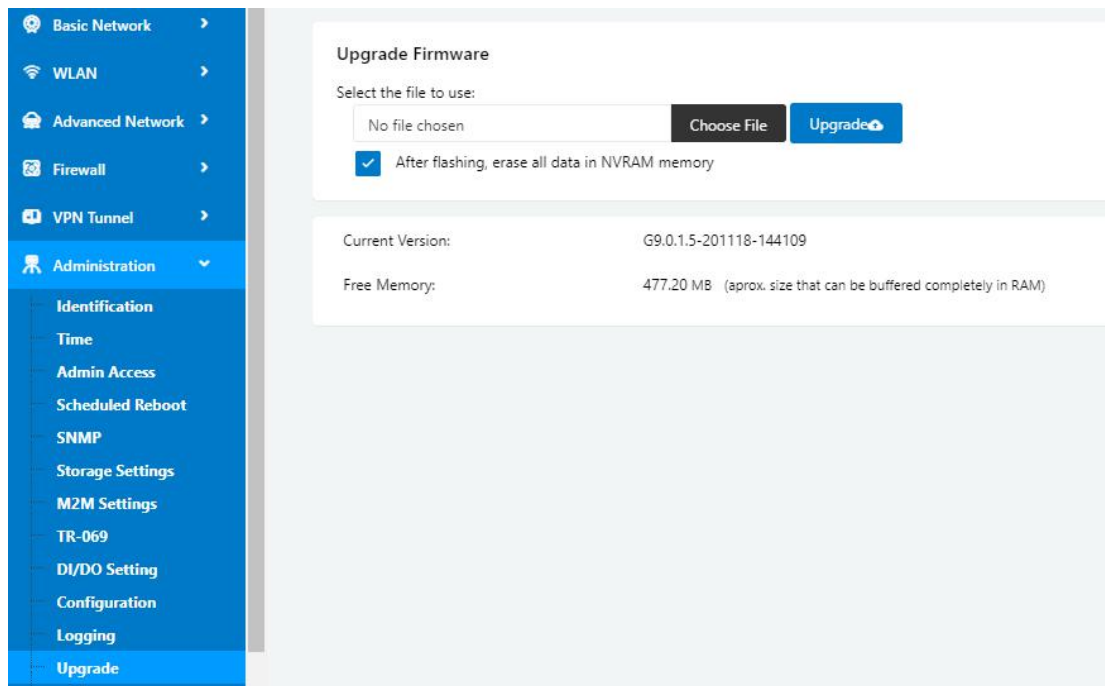


Figure 3-1 Firmware Upgrade GUI



NOTE

When upgrading, please don't cut off the power.

2.9.13 Firmware upgrade

Step 1 Please click “Administrator>firmware upgrade” to open upgrade firmware tab.

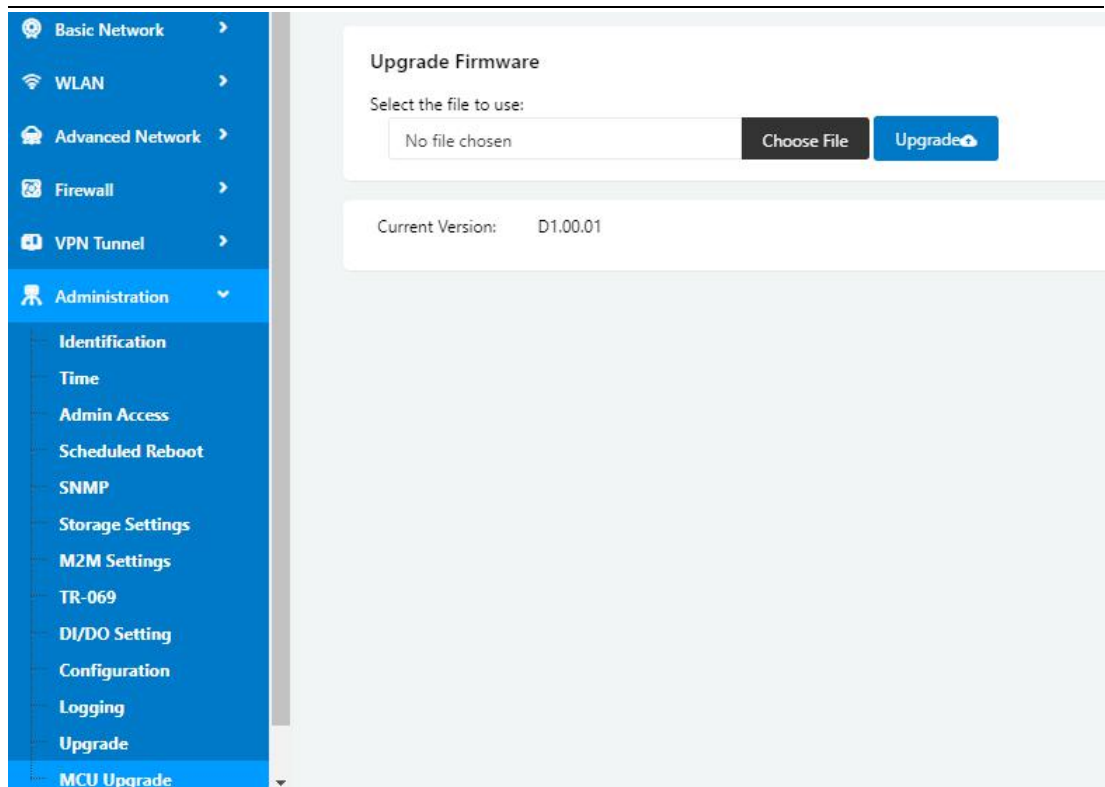


Figure 3-1 Firmware Upgrade GUI



NOTE

When upgrading, please don't cut off the power.

2.10 “Reset” Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way.

“Reset” button is near to Console port in WL-G530 panel, This button can be used when the router is in use or when the router is turned on.

Press the “RST” button and keep more than 8 seconds till the NET light stopping blink. The system will be reverted to factory.

Table 2-33 System Default Instruction

Parameter	Default setting
LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP server	Enable
User Name	admin
Password	admin



NOTE

After reboot, the previous configuration would be deleted and restore to factory settings.

3 Configuration Instance

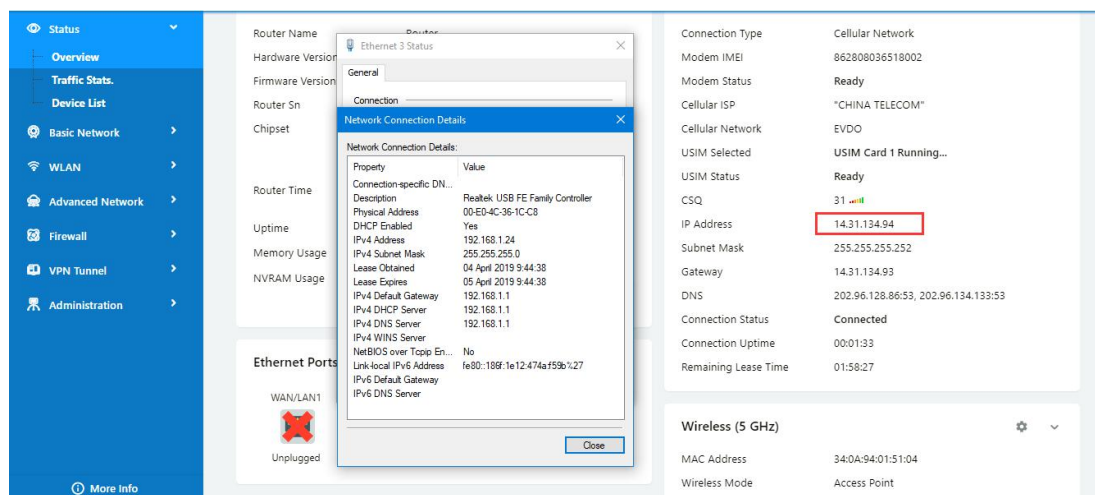
This chapter is mainly for configured test case, there would be some difference between the scheme and real object. But the difference doesn't have any influence to products performance.

3.1 Port Forwarding

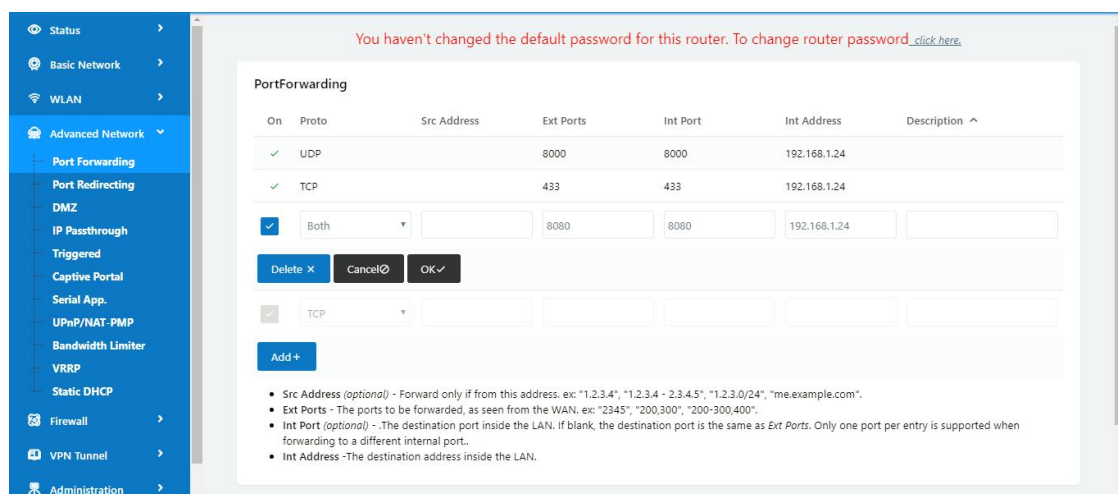
1) The router online and got a public IP address 14.31.134.94

Note: It's based on SIM card carrier

2) The PC is connected to router and got IP address 192.168.1.24



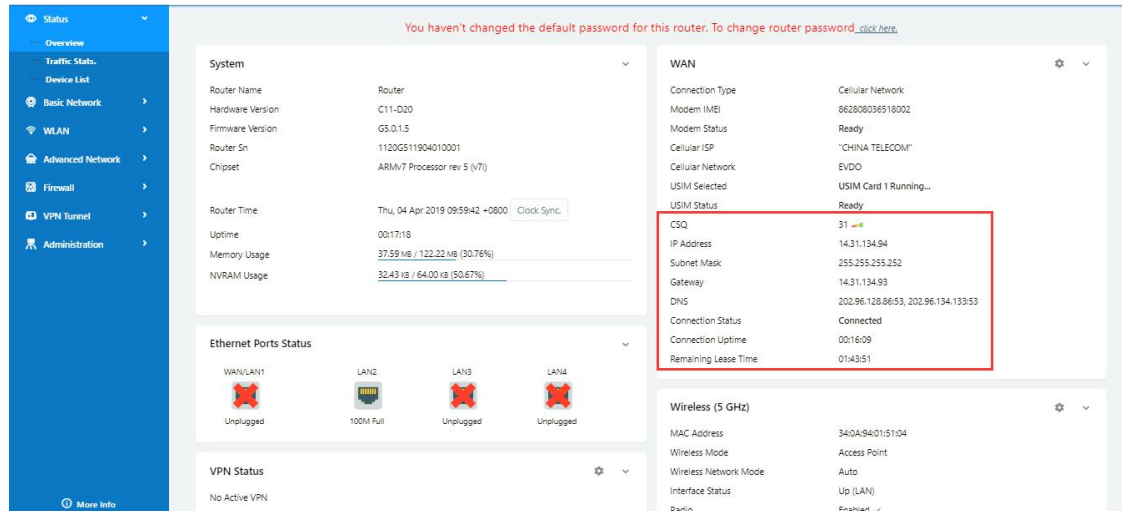
3) Configuration



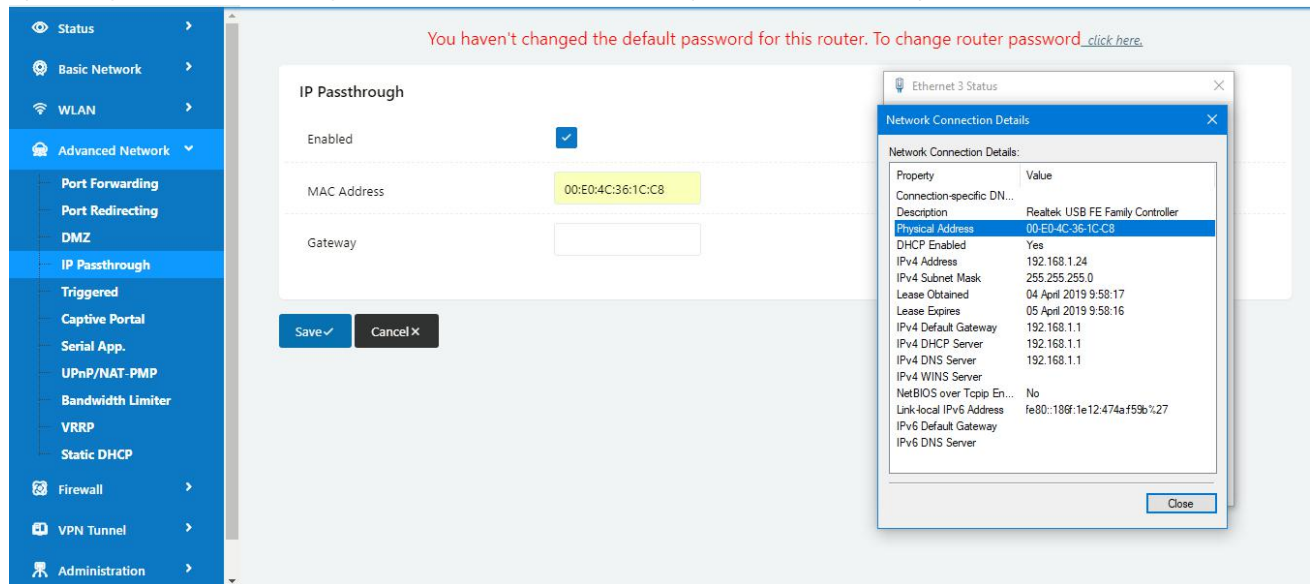
4) The PC can be accessed via 14.31.134.94:443 over Internet

3.2 IP Passthrough

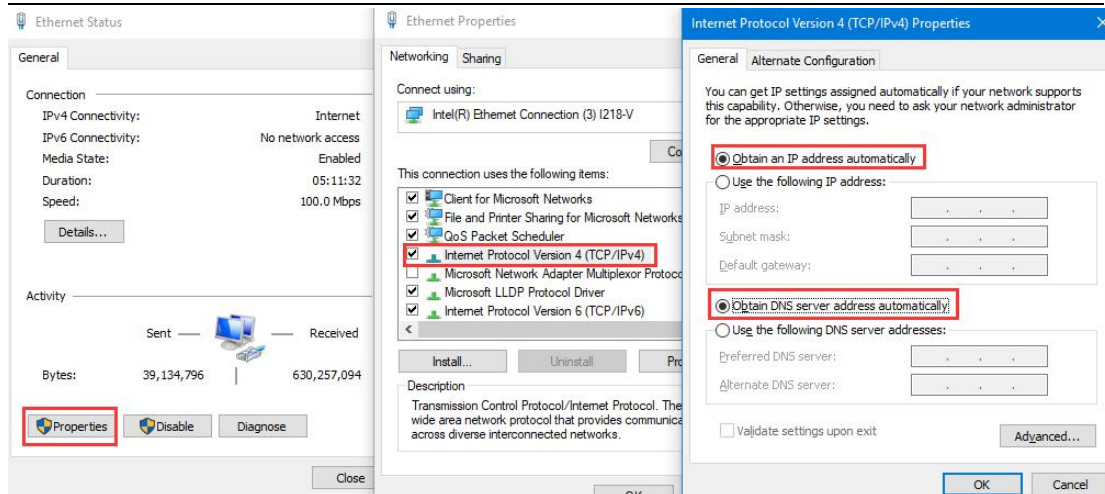
1) The router online



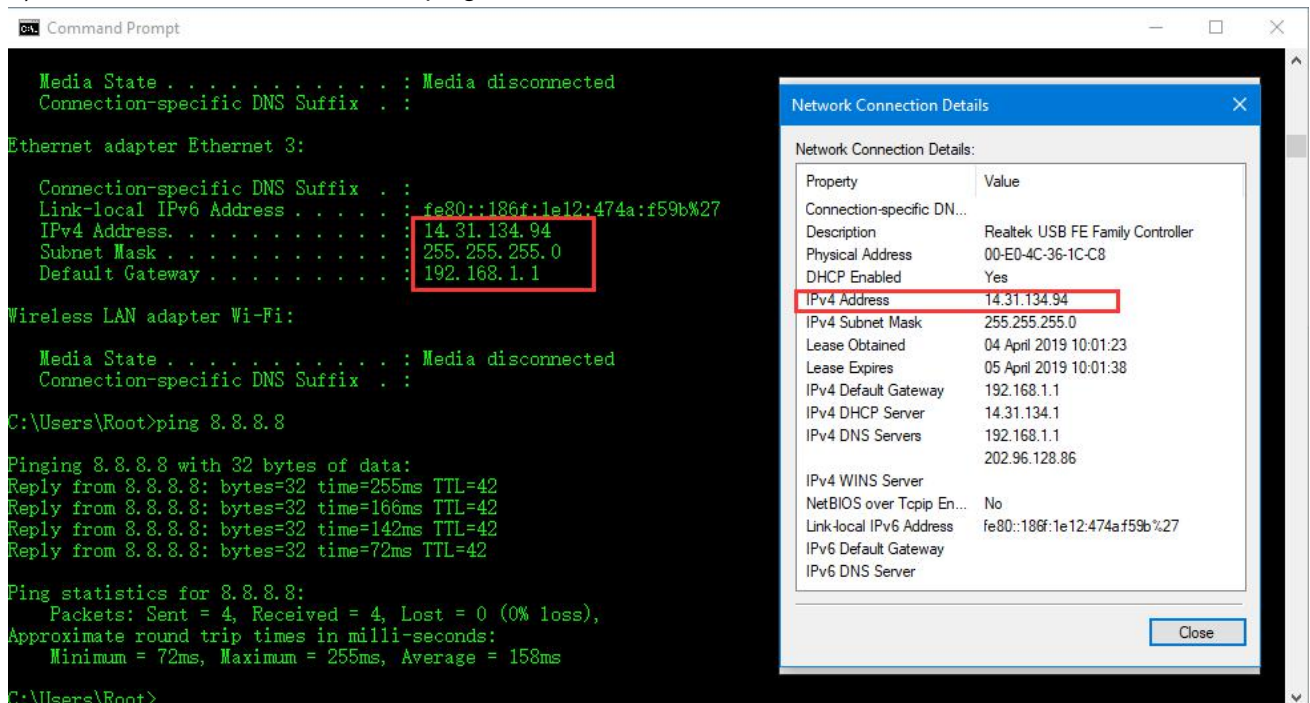
2) Configure IP passthrough destination MAC address (PC Ethernet MAC)



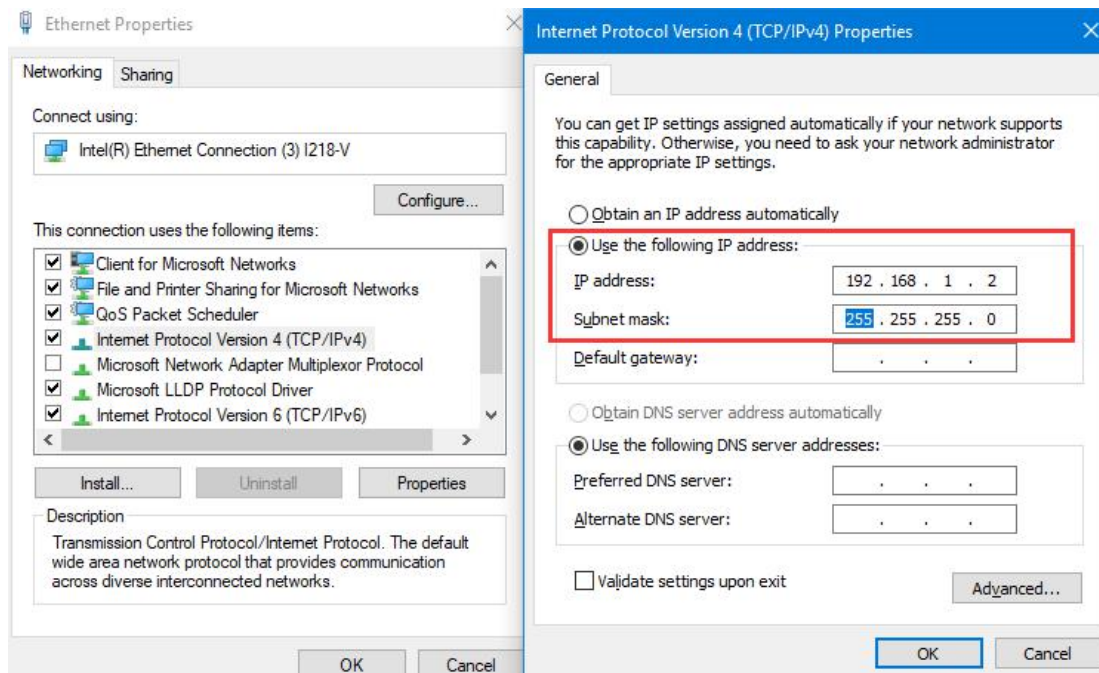
3) Set the PC to DHCP



4) Check the Ethernet status and ping test

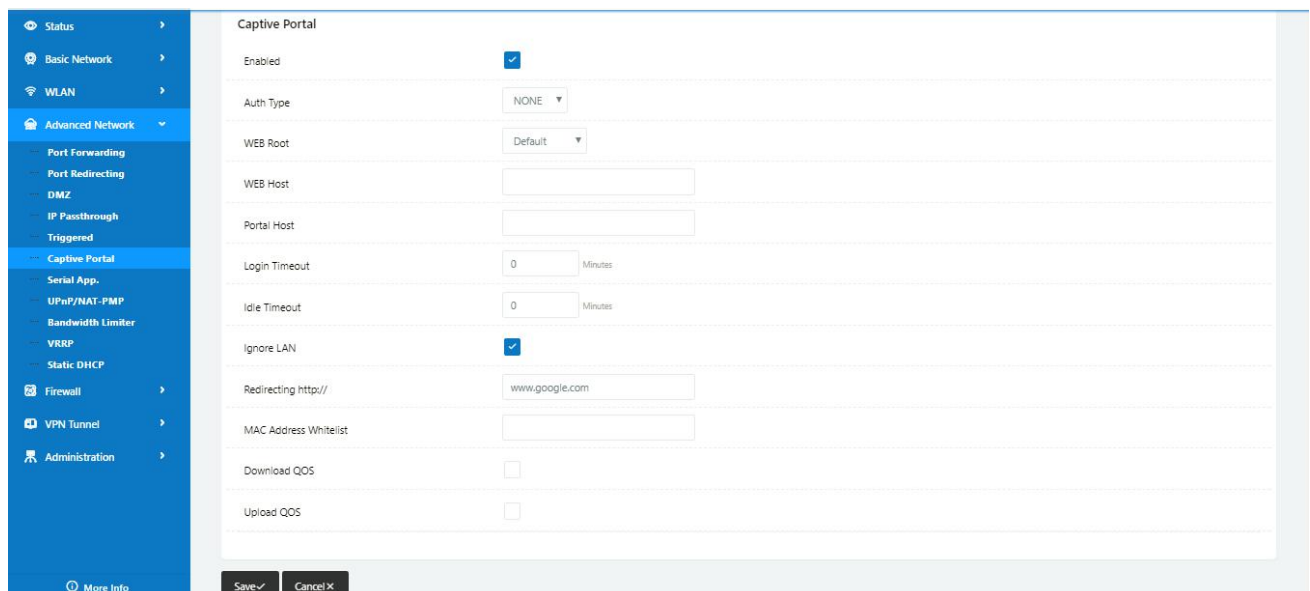


5) Set the PC Ethernet as DHCP to release the IP and access to router GUI again



3.3 Captive Portal

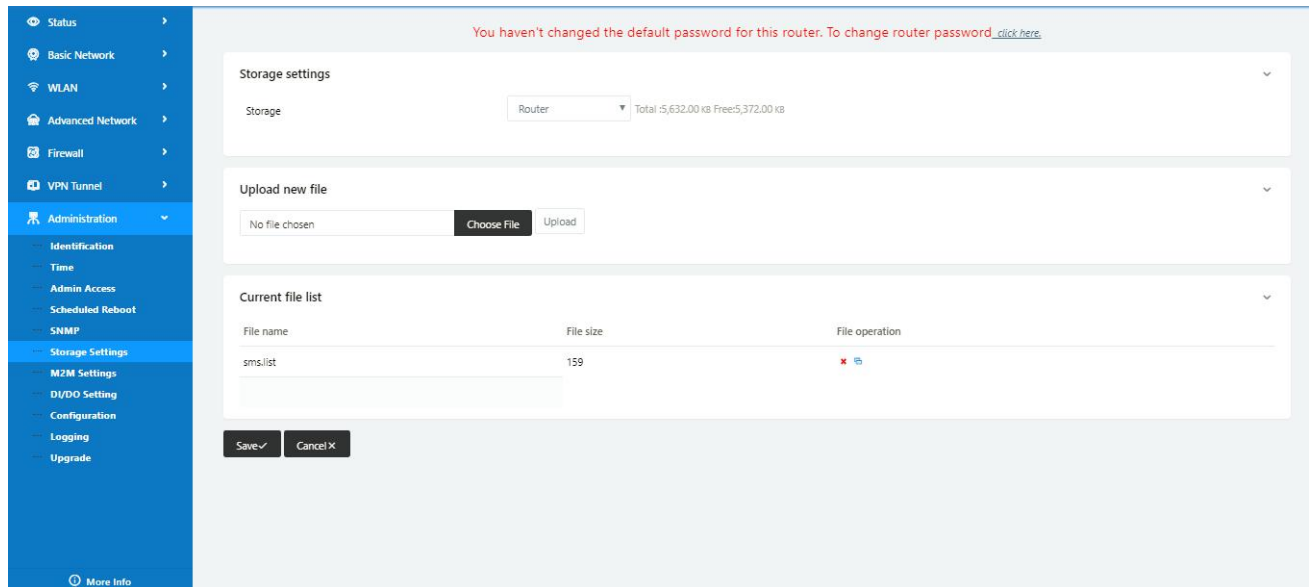
Step 1 Please click “Advanced Network> Captive Portal” to check or modify the relevant parameter.



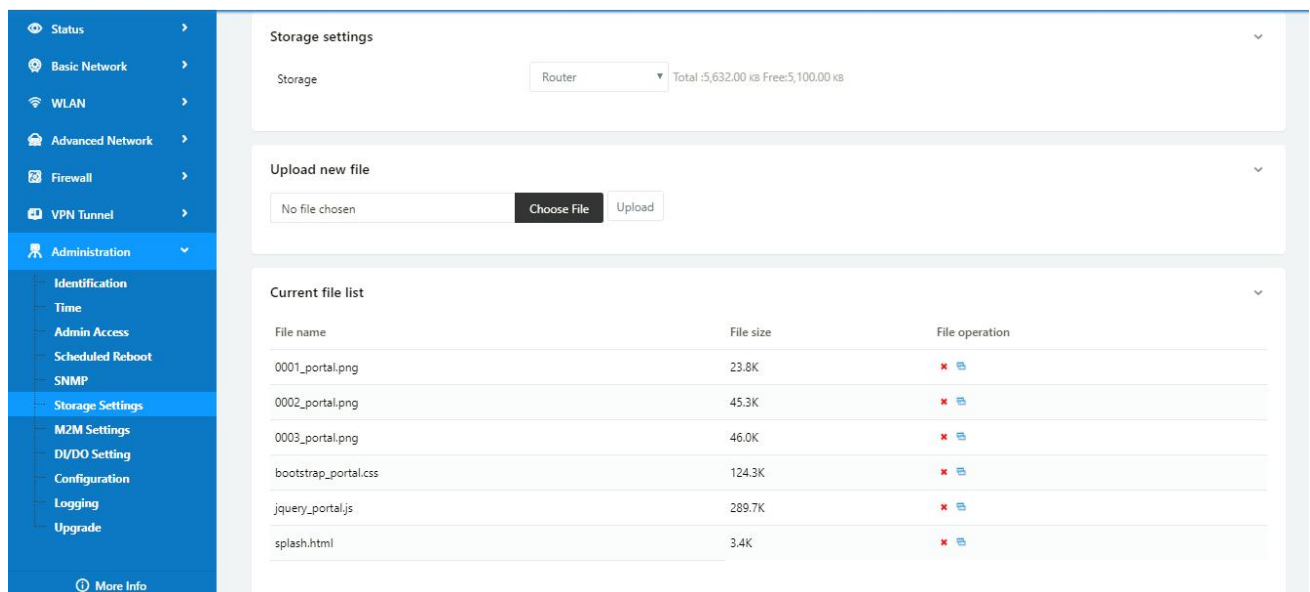
1) Upload Portal file and Splash.html by local

Upload portal images and splash.html in router for the Slider (0001_portal.png, 0002_portal.png, and 0003_portal.png) to the Router under the “Administration / Storage Settings” menu.

Furthermore, also might upload splash with images together.



Each Ad file just supports 3 Ad portal images. Picture format is acceptable for png/jpg and image size is less than 100Kbytes and resolution is 800*600. Picture name is 0001_portal.png, 0002_portal.png and 0003_portal.png. Furthermore, please keep image names the same between portal file and splash.html.



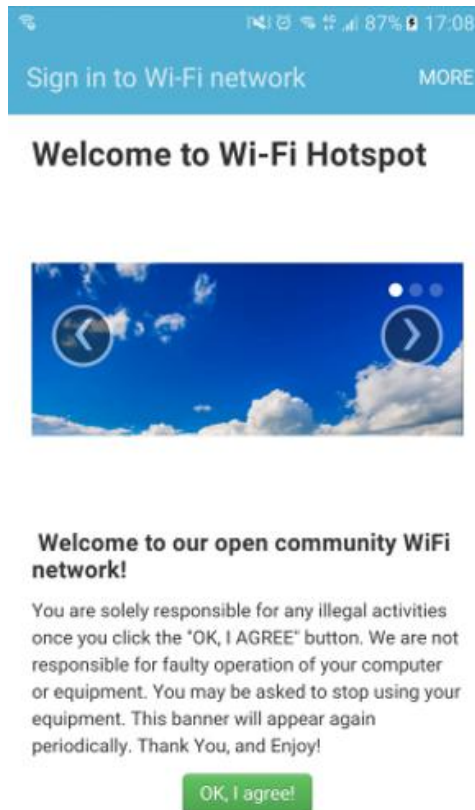
```
<!-- <hr> -->

<div id="myCarousel" class="carousel slide marketing">
  <ol class="carousel-indicators">
    <li data-target="#myCarousel" data-slide-to="0" class="active"></li>
    <li data-target="#myCarousel" data-slide-to="1"></li>
    <li data-target="#myCarousel" data-slide-to="2"></li>
  </ol>

  <div class="carousel-inner">
    <div class="item active">
      
    </div>
    <div class="item">
      
    </div>
    <div class="item">
      
    </div>
  </div>
  <a class="left carousel-control" href="#myCarousel" data-slide="prev">&lsaquo;</a>
  <a class="right carousel-control" href="#myCarousel" data-slide="next">&rsaquo;</a>
</div>

<!-- <hr> -->
```

Finally, we can see the results by connect to router WIFI



2) Modify portal file storage path

Modify portal file storage for In-storage as below.

3.4 GPS Settings

Step 1 Please click “Advanced Network> GPS” to view or modify the relevant parameter.

Figure 4-5 GPS GUI

Table 4-5 “GPS” Instruction

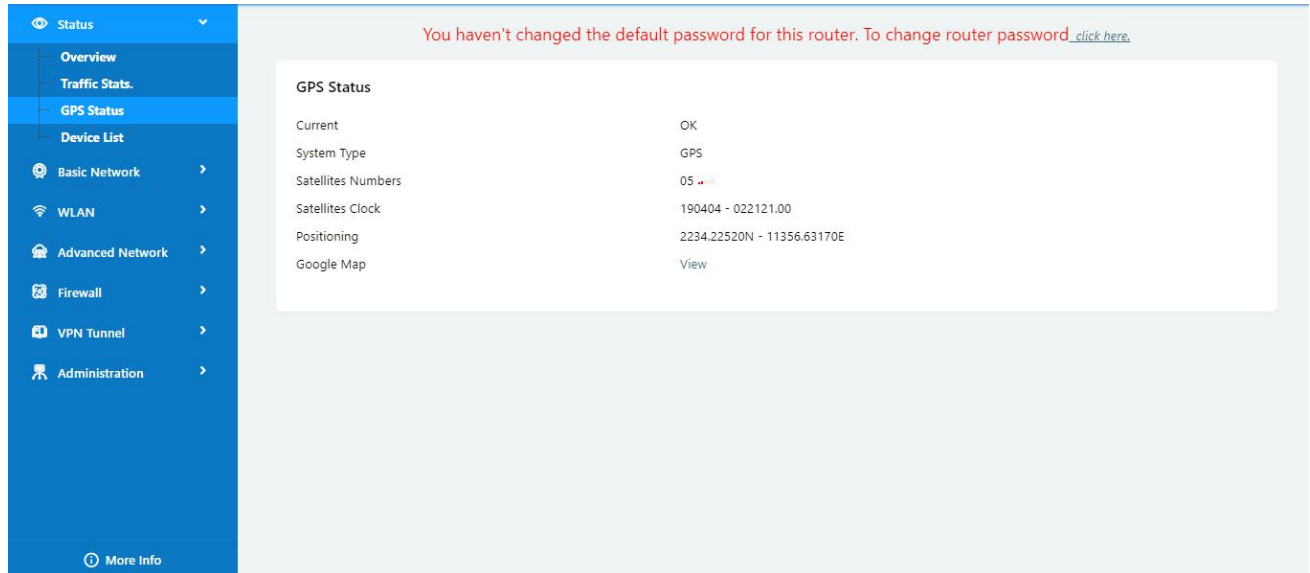
parameter	Instruction
GPS Mode	Enable/Disable
GPS Format	NMEA and M2M_FMT(WLINK)
Server IP/Port	GPS server IP and port
Heart-Beat	If choose M2M_FMT format, heart-beat ID will be packed into GPS data.

parameter	Instruction
Interval	GPS data transmit as the interval time.

Step 2 Please click “save” to finis

Step 3 Connect the GPS antenna to router GPS interface

Step 4 Check GPS Status



M2M_FMT Format as below.

1. GPS data structure.

Router ID, gps_date, gps_time, gps_use, gps_latitude, gps_NS, gps_longitude, gps_EW, gps_speed, gps_degrees, gps_FS, gps_HDOP, gps_MSL

2. Example

0001_R081850ac,150904,043215.0,06,2234.248130,N,11356.626179,E,0.0,91.5,1,1.2,97.5

3. GPS data description

Field No.	Name	Format	Example	Description
1	Router ID	String	0001_R081850ac	0001 customizable product ID. _R router indicator.

				081850ac Last 8digits of routers MAC address.
2	gps_date	yymmdd	150904	Date in year,month,day
3	gps_time	hhmmss.ss s	043215.0	UTC Time, Time of position fix.
4	gps_use	numeric	06	Satellites Used, Range 0 to 12.
5	gps_latitude	ddmm.mm mm	2234.248130	Latitude, Degrees + minutes.
6	gps_NS	character	N	N/S Indicator,N=north or S=south.
7	gps_longitude	ddmm.mm mm	11356.626179	Longitude, Degrees + minutes.
8	gps_EW	character	E	E/W indicator, E=east or W=west.
9	gps_speed	numeric	0.0	Speed over ground, units is km/h.
10	gps_degrees	numeric	91.5	Course over ground, unit is degree.
11	gps_FS	digit	1	Position Fix Status Indicator,
12	gps_HDOP	numeric	1.2	HDOP, Horizontal Dilution of Precision
13	gps_MSL	numeric	97.5	MSL Altitude, units is meter.