

WLINK

User Manual

---Apply to WL-R320 Series 4G+/4G Router

V1.2

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

Jan, 2023



Copyright © Shenzhen WLINK Technology Company Limited 2012 ~ 2023

Without our written approval, anyone can't extract, copy whole or part of content of this file and can't spread out in any format.

Caution

Due to product updates or functional upgrading, we may renew the content of this file, and this file only for reference. All statement, information, suggestion etc. in this file does not compose any form of guarantee and we WLINK reserves the right of final explanation.

Version History

Updates between document versions are cumulative. The latest document version contains all updates made to previous version.

Data	Document Version	Software Version	Note
2023-1-17	V1.2	V7.2.1112	Improve GUI, Add link backup
2021-10-30	V1.1	V5.1.1030	Improve GUI
2021-5-30	V1.0	V4.1.0530	

Shenzhen WLINK Technology Company Limited

Add 2A, F5 Building, TCL International E City, No.1001 Zhongshanyuan Rd.,
Nanshan Dist., Shenzhen, 518052, China

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

Service Email support@wlink-tech.com

Tel 86-755-86089513

Fax 86-755-26059261

1 Contents

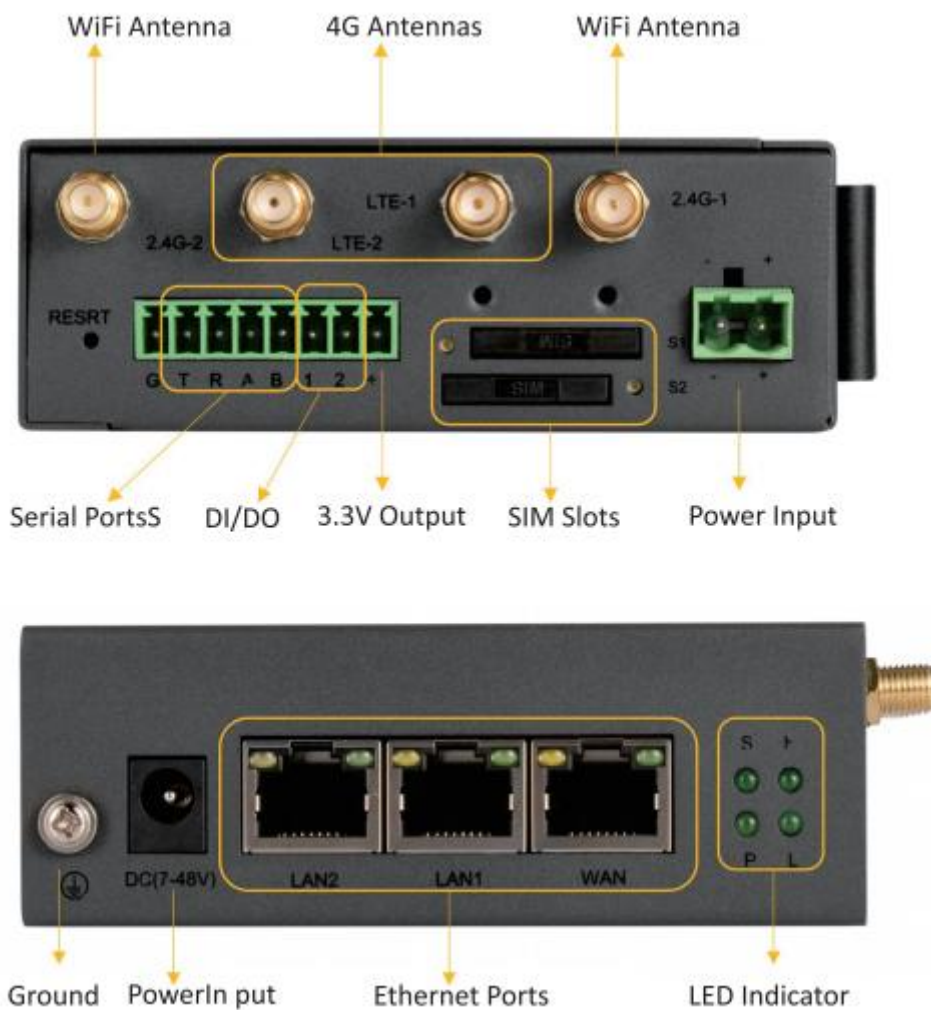
1 Contents	3
2 Hardware Introduction	5
2.1 Interface	5
2.2 LED Status	6
2.3 Dimension	6
2.4 How to Install	7
3 Router Configuration	10
3.1 Local Configure	10
3.2 Dashboard	11
3.3 Utilization	11
3.4 Interface	12
3.5 Network	13
3.6 VPN Setting	32
3.7 Wireless Setting	39
3.8 Station	42
3.9 Application	45
3.10 System	51
3.11 Debug	56
3.12 Development(SDK)	59
3.13 Default Factory Configuration	59
4 Configuration Instance	60
4.1 Link Backup	60
4.2 Lock Band	62
4.3 LTE SMS	63

4.4 DDNS	64
4.5 GNSS	65
4.6 Remote IO	69
4.7 OpenVPN(TAP Mode)	73
4.8 IPSec Setting	77
4.9 Station Setting	80

2 Hardware Introduction

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.

2.1 Interface



 **NOTE**

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

Table 2-1 Router Interface

Port	Instruction	Remark
SIM	Support 1.8/3V automatic detection.	Two SIM as default
Antenna Connectors	SMA connector, 50Ω. LTE1 as Main, LTE2 as 4G Aux. Wi-Fi1, Wi-Fi2 and GNSS Optional.	
LAN1	10/100Base-TX, MDI/MDIX self-adaptio	
LAN2	10/100Base-TX, MDI/MDIX self-adaption	LAN as Default
WAN	10/100Base-TX, MDI/MDIX self-adaption	LAN as Default
TTL/RS232	Gnd, Tx, Rx	RS232 as default
RS485	A, B	
GPIO	2 GPIOs	
Reset	Reset button, (press on button at least 5 seconds)	
PWR	1xDC Power connector 1x Terminal Block(2 Pins)	7~48VDC

2.2 LED Status

Table 2-2 Router LED indicator Status

silk-screen	Indicator		Note
System(S)	Blue	Slow Blinking (1s)	System Auto-check
		Quick Blinking (0.5s)	Dialing
		Solid light	4G/3G online
Power(P)	Orange	Solid light	Power on
		light off	Power off or power fault
High(H)	Green	Solid light	Good Signal(CSQ≥-19)
Low(L)	Red	Solid light	Weak Signal(CSQ<-18)

2.3 Dimension

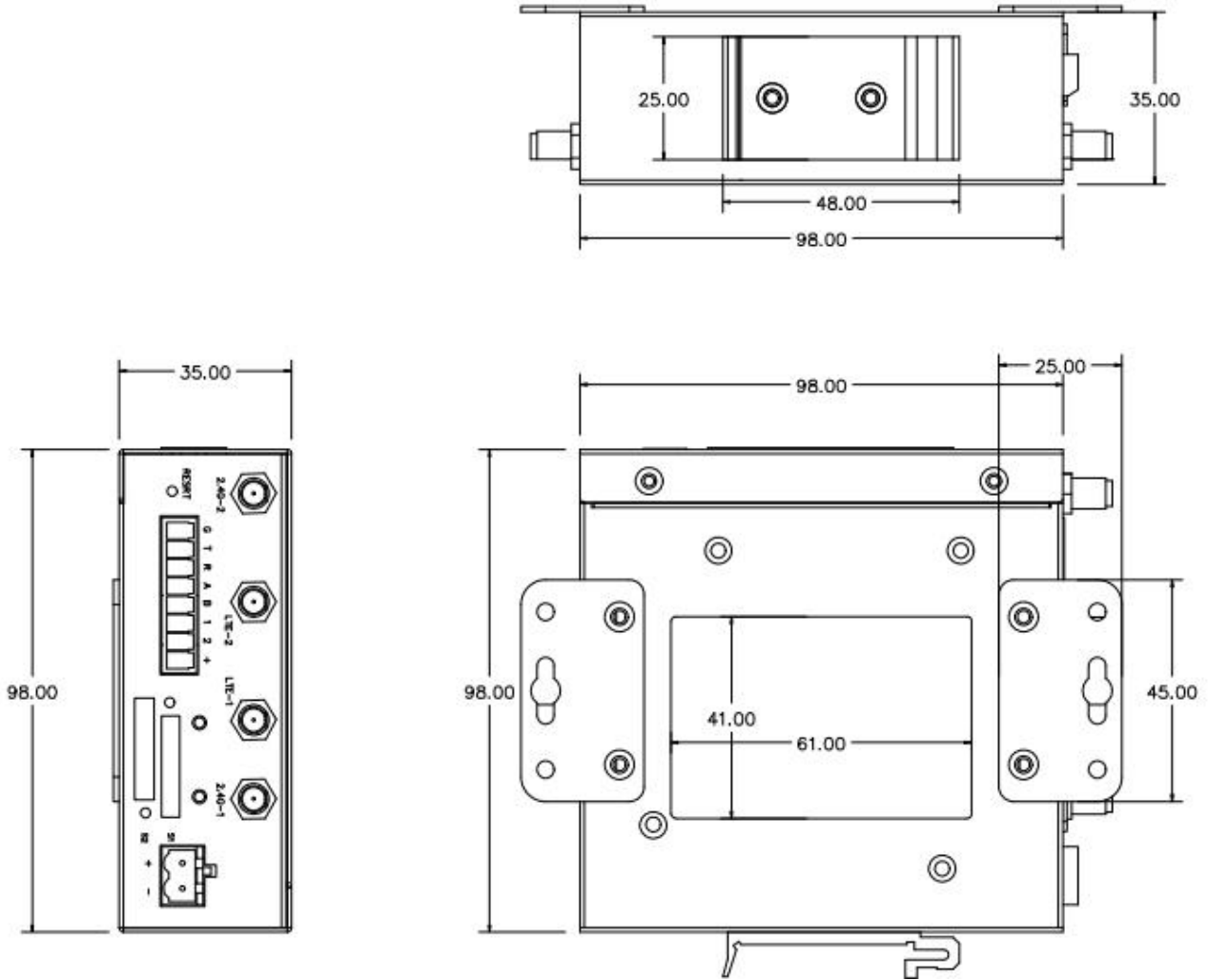
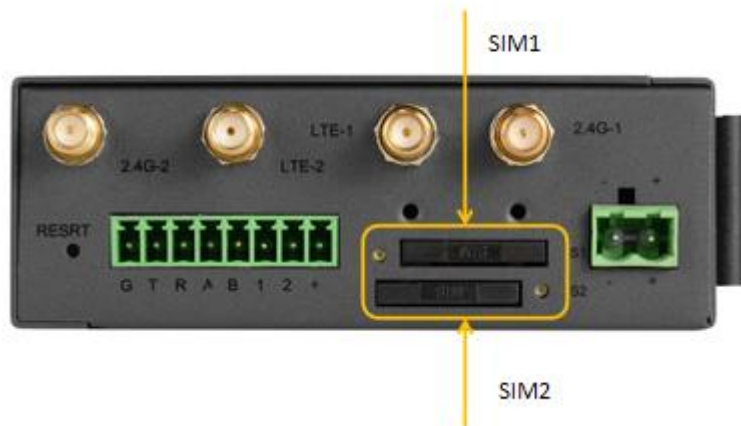


Figure 2-2 R320 Series Router Dimension

2.4 How to Install

1.4.1 SIM/UIM card install

Please insert the dual SIM cards before configure the router.





Before connecting, please disconnect any power resource of router

1.4.2 Ethernet Cable Connection

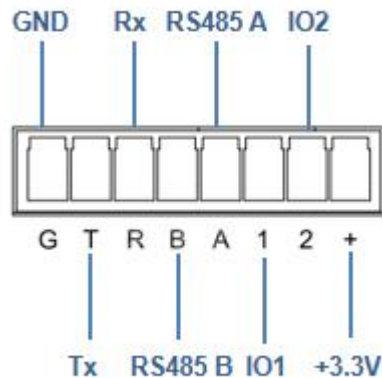
Connect the router with a computer by an Ethernet cable for GUI configuration, or transit by a switch.

1.4.3 Power Supply Connection

Voltage input range +9~48VDC, 5.5mm DC interface and 2Pins terminal block are alternative.

1.4.4 Serial Port and GPIO Connection

WL-R320 supports one RS232 and one RS485 ports as default. It might be requested serial port for TTL when placed order. The serial port feature supports TCP/UDP client/server as optional, also supports Modbus protocol.



1.4.6 Review

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



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

3 Router Configuration

WL-R320 Series routers support GUI. 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.

3.1 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 192.168.8.1, 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,192.168.8.xxx(XXX can be any number between 2~254)

Step 3 Run an Internet Explorer and visit “<http://192.168.8.1/>”, to enter identify page.

The default username is admin and password is admin168. User should modify the login password.

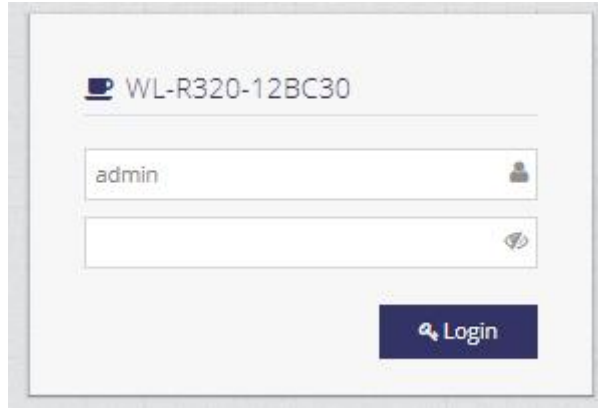
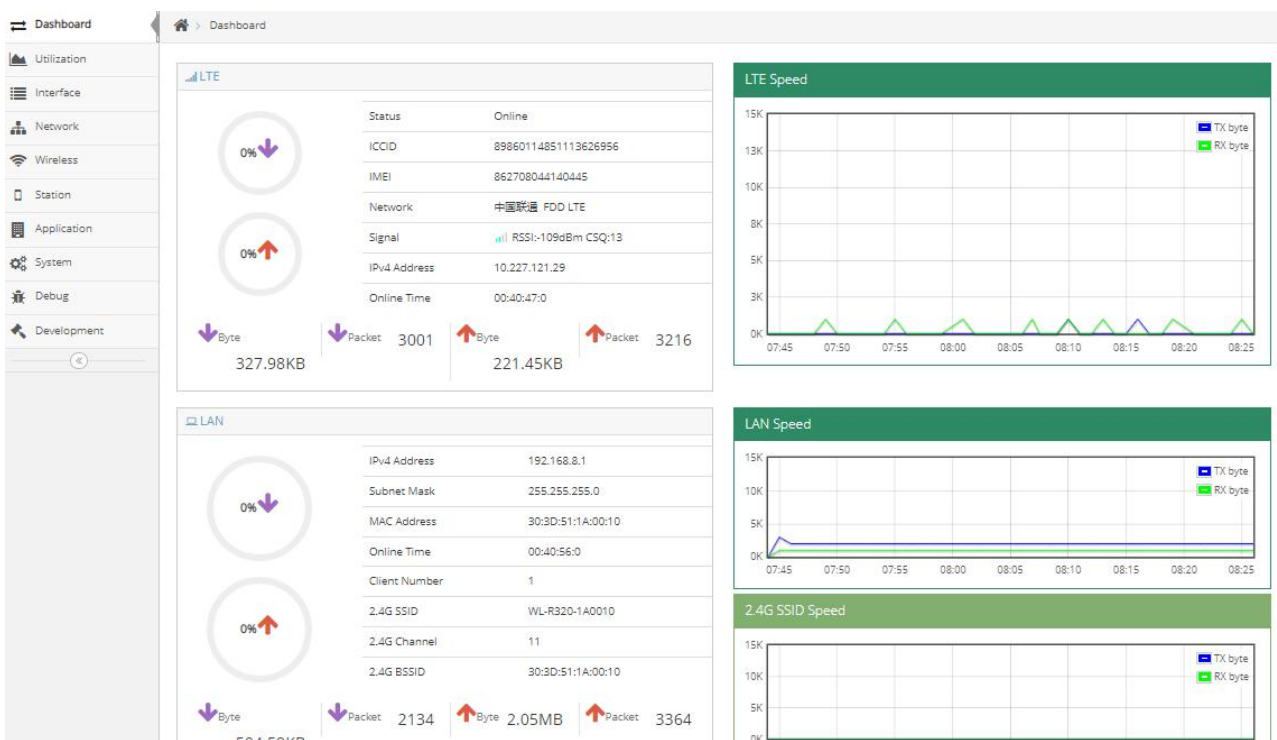


Figure 2-2 User Identify Interface

----END

2.2 Dashboard

Check routers information such as status, 4G/WAN speed, after login router. Especially, suggest change the password according to the prompts because of security requirement.



2.3 Utilization

The Utilization GUI will be display router system information such as CPU, Memory information

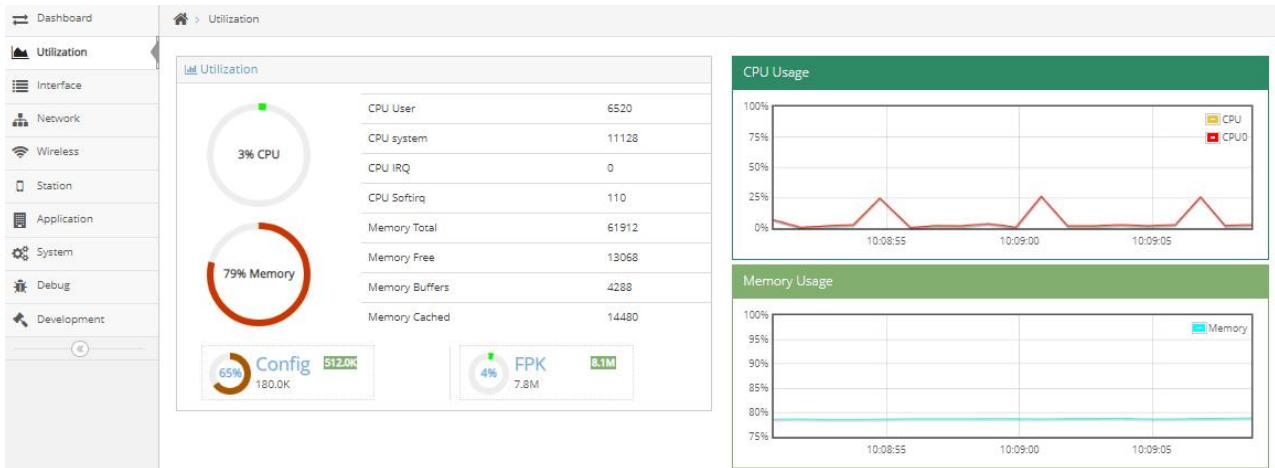


Figure 2-3 Resource GUI

2.4 Interface

The interface GUI will display network interface status such as 4G information, LAN and Switch Status including ISP name, network type, signal, band, SIM IP address and 4G online time.

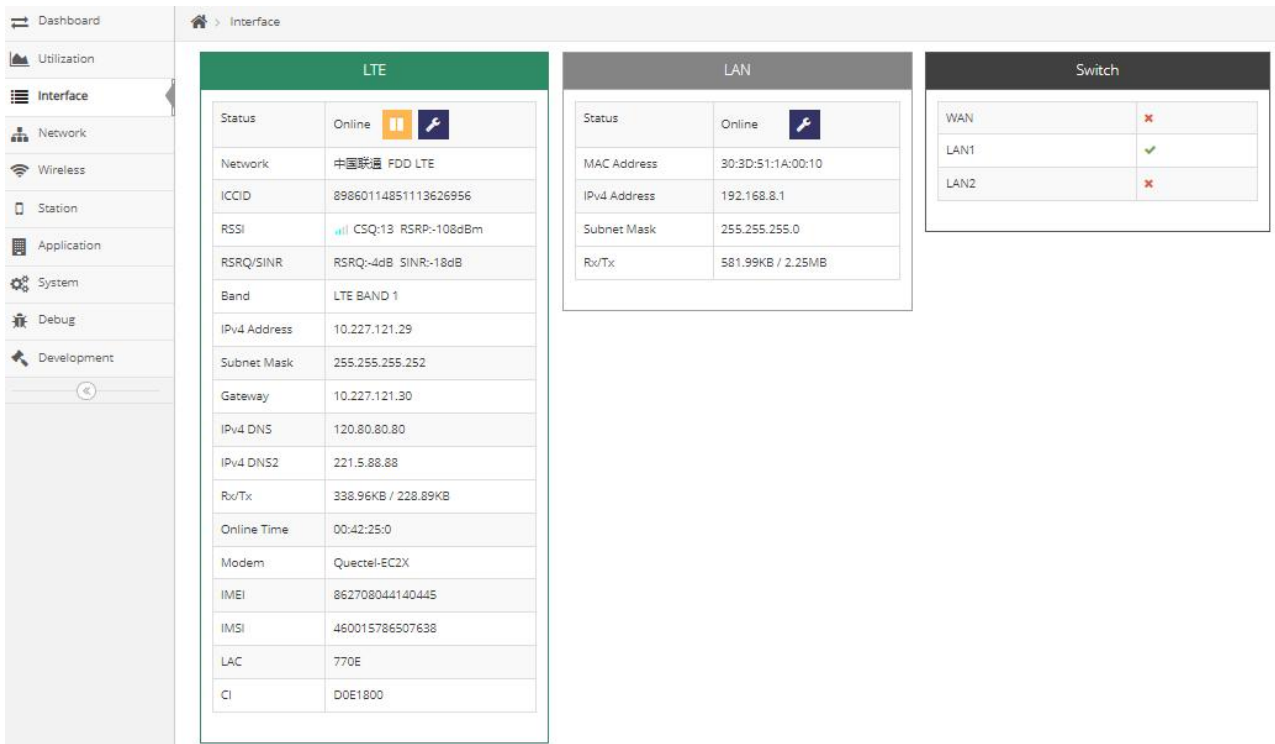


Figure 2-4 Interface. GUI

2.5 Network

2.5.1 LTE Setting

Step 1 Network>LTE to enter LTE Status GUI. It supports to disable 4G connection by Status button.

🏠 > Network > LTE			
Status	UP 	IP Address	10.42.212.49
Operator	中国移动	Network	TDD LTE
RSSI	 -59dBm	IMEI	862506040853791
Live Time	00:00:10:0	ICCID	89860000192127678193
Rx/Tx	8.85KB / 8.61KB	IMSI	460077121812838

Step 2 Network>LTE to Network Mode setting GUI as following.


APN Setting

APN Custom

APN

Username

Password 

IP Type 

Authentication 

Dial Number

Dial CID

Parameter	Instruction	Default
APN Custom	Auto APN will be enable when APN Custom switch is Off. The router will recognize the access point name(APN)automatically. Regarding to private SIM card, please enable APN Custom button to configure SIM information such as APN, Username and Password.	Off
APN	APN is provided by local ISP	internet
Username	SIM card user name is provided by ISP	
Password	SIM card password is provided by ISP	
IP Type	IP/IPv4v6/IPv6 optional.	Null
Authentication	Select Auto/NONE/PAP/Chap/PAP/CHAP authentication as requested	
Dial Number	4G/3G connection service code	*99#
Dial CID	Connect to the specified cellular ID. CID number is provided by local carrier.	

Cellular Attach Setting

Attach Mode

GPS

[Modem Settings](#)

Parameter	Instruction	Default
Attach Mode	【Auto】 The router will automatically connect to 4G/3G networks and give priority to 4G. 【LTE(4G)】 Router will connect to 4G only. 【WCDMA/TDSCDMA/EVDO】 Router will connect to 3G only. 【CDMA/GSM】 Router will connect to 2G only.	Auto
GPS	The GPS is built-in 4G module.The GPS feature will be related to model and hardware.	Off
Modem Settings	Supports Lock IMEI, Lock IMSI, Lock PIN and Lock Band.	Null

Parameter	Instruction	Default
	Supports no SIM Card,PLMN and Signal for testing as requested.	Need



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

Network Status Setting

Network Status

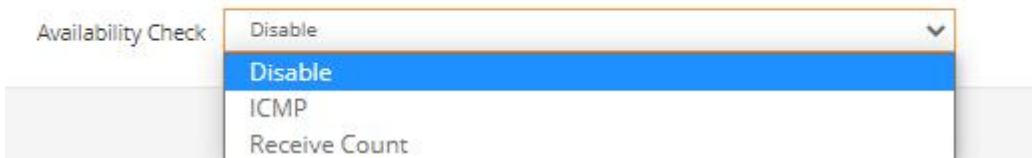
IPv4 Mode

IPv4 Masquerade(NAT)

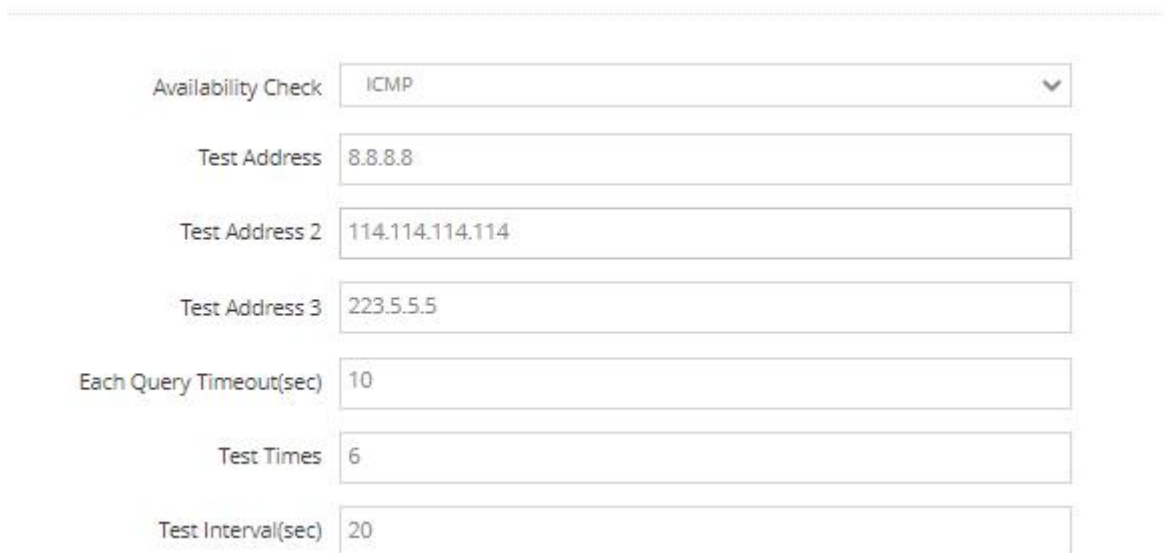
TTL

Parameter	Instruction	Default
Dial Mode	<p>【Advise】The router will automatically dial-up 4G/3G by ECM protocol.</p> <p>【PPP】 The router will automatically dial-up 4G/3G by PPP protocol.</p> <p>【DHCP】 The router will automatically dial-up 4G/3G by DHCP protocol.</p> <p>【Static IP】 The router will automatically dial-up 4G/3G and obtain SIM IP as ISP requested.</p>	Advise
MTU	Maximum Transmission Unit on Cellular network.	1500
LCP Echo Interval	LCP(link control protocol) check interval	10
LCP Echo Times	LCP check Times. If no replace, the PPP will reconnect.	12
PPP Option	PPP debugging information	debug
Custom DNS	Configure DNS server IP address	Disable
IP Masquerade(NAT)	Replace internal ip address to SIM IP address when sent data.	Enable

Network Availability Check Setting



Parameter	Instruction	Default
Availability Check	Disable, ICMP Check and Receive Count Optional	Disable



Parameter	Instruction	Default
Availability Check	Disable, ICMP Check and Receive Count Optional	Disable
ICMP	Configure 3 destination IP address to check check the Cellular connection available.	
Test Address	Reachable destination IP address1	
Test Address2	Reachable destination IP address1	12
Test Address3	PPP debugging information	debug
Each Query Timeout(sec)	Configure DNS server IP address	10
Test Times	ICMP times	6
Test Interval(sec)	ICMP Interval	20

Availability Check	Receive Count
Duration(sec)	20
Test Times	30
Request packets	1

Parameter	Instruction	Default
Receive Count	Disable, ICMP Check and Receive Count Optional	Disable
Duration(sec)	Configure 3 destination IP address to check check the Cellular connection available.	20
Test Times	Reachable destination IP address1	30
Request packets	Reachable destination IP address1	1

Step 3 After Setting, please click “Apply” icon.

----End

2.5.2 LTE SMS Setting

Step 1 Network>LTE SMS to enter LTE SMS GUI.

Parameter	Instruction	Default
SMS Function	SMS Function Enable/Disable Optional.	Disable
HE Agent	Enable SMS command inquiry by HE command line mode.	Disable
Command Contact	Specify the acceptable phone number. If null, the router will accept anyone phone number without limitation.	Null
Command Prefix	SMS command identify. The router will implement message command with correct prefix.	Null

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



Configuration Instance

Please check LTE SMS Configuration in the chapter 3 as reference.

----End

2.5.3 LTE Backup SIM

Step 1 Network>LTE Backup SIM to enter Setting GUI.

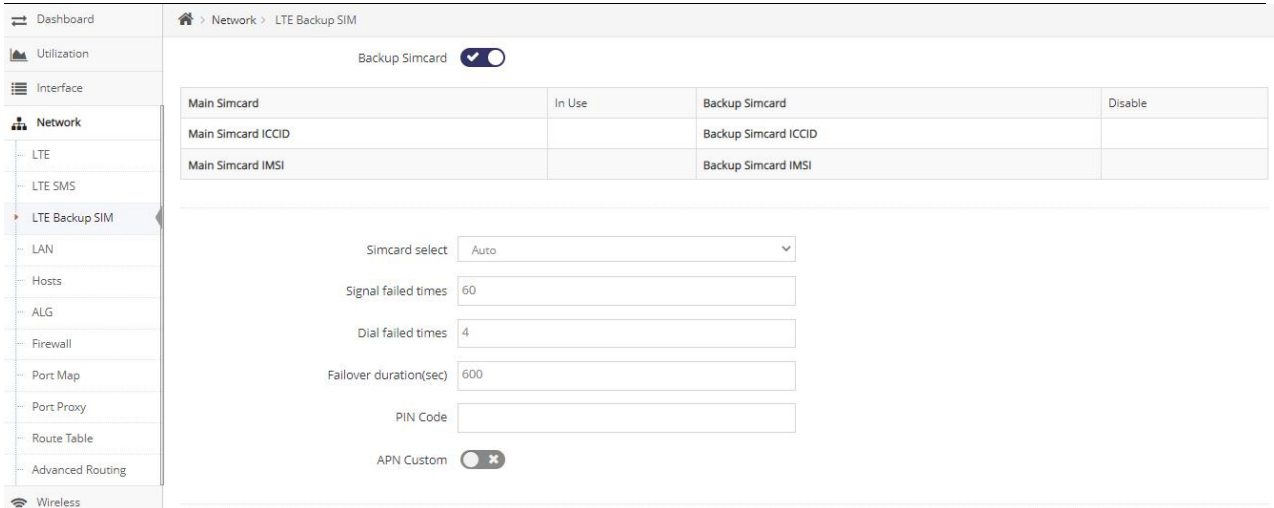


Table 2-1 LAN Setting Instruction

Parameter	Instruction	Default
Backup SIM	Enable Backup Simcard	Disable
Simcard Select	Auto, Main Simcard, Backup Simcard optional	Auto
Signal failed times	Router will switch to backup Sim card once detect signal failure times exceeds the defined times.	60times
Dial failed times	It will switch to backup Sim card once dail-up failure times exceeds the defined times.	4times
Failover duration(sec)	The router will work on the backup Sim card time(sec)	600s
PIN Code	Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen.	86400
APN Custom	Auto APN will be enable when APN Custom switch is Off. The router will recognize the access point name(APN)automatically. Regarding to private SIM card, please enable APN Custom button to configure SIM information such as APN, Username and Password.	Off

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

---End

2.5.4 LAN Setting

Step 1 Network>LAN to enter below GUI.

Table 2-2 LAN Setting Instruction

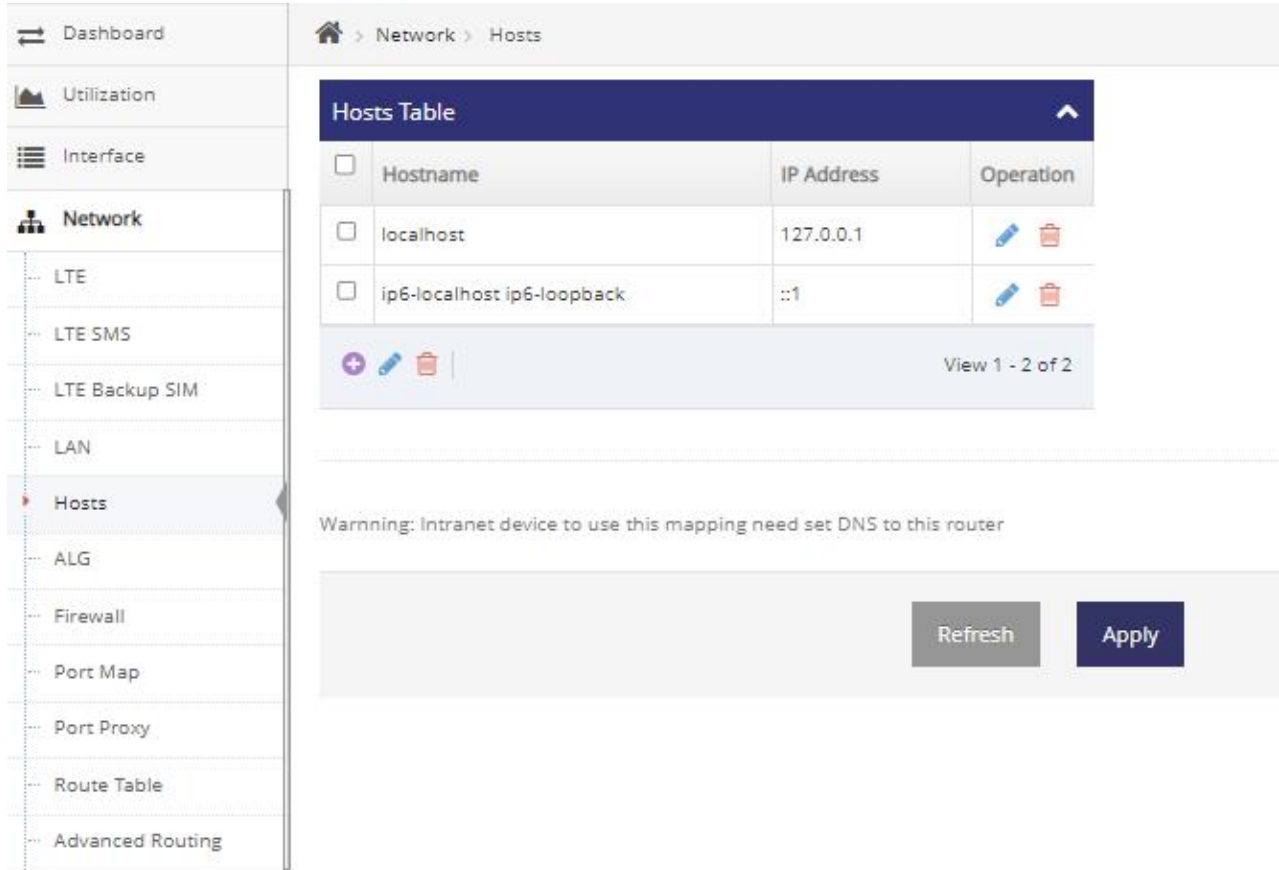
Parameter	Instruction	Default
IP Address	Router IP address, default IP is 192.168.8.1	192.168.8.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0	255.255.255.0
Address2	Add LAN address	Disable
Address3	Add LAN address	Disable
DHCP Server	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease	Enable
Start IP Address	DHCP IP pool start IP address	192.168.8.2
End IP Address	DHCP IP pool end IP address	192.168.8.250
Lease	The valid time, unit as sec	86400
Assign Gateway	Specified the gateway IP address	Null
Assign DNS	Specified the DNS server IP address	Null
Assign DNS2	Specified the DNS server IP address	Null

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

----End

2.5.5 Hosts

Step 1 Network->Host to enter the Hosts setting GUI.

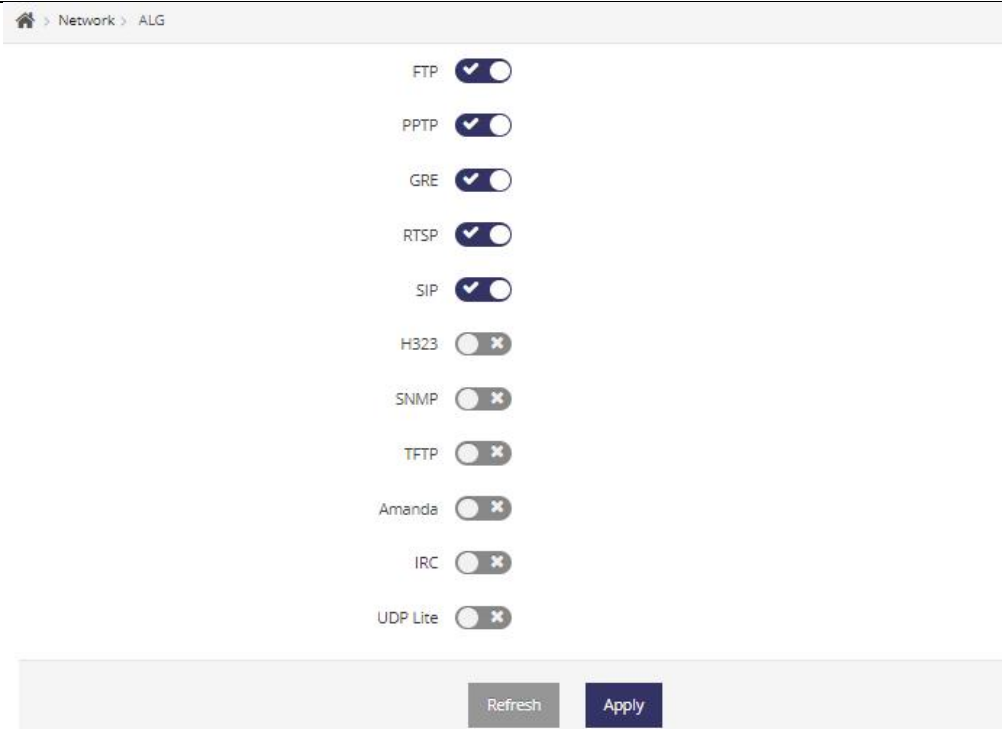


Step 2 Please Click “ Apply “ to finish.

----End

2.5.6 ALG

Step 1 Basic Network->ALG to enter the application layer gateway setting GUI.



Step 2 Please Click “ Apply “ to finish.

----End

2.5.7 Firewall

Step 1 Network->Firewall to enter the Firewall setting page.

- Dashboard
- Utilization
- Interface
- Network**
 - Connection
 - LTE
 - LTE SMS
 - LTE Backup SIM
 - WAN
 - WISP(2.4G)
 - LAN
 - Hosts
 - ALG
 - Firewall**
 - Port Map
 - Port Proxy
 - Route Table
 - Advanced Routing
- VPN

Home > Network > Firewall

Interface: LTE

Status:

ICMP Access: X

Telnet Access: X

SSH Access: X

WEB Access: X

ICMP Through:

NAT Through:

Default Action: Extranet access is prohibited

Action Rule Table

<input type="checkbox"/>	Name(unique)	Extranet Address	Intranet Address	Protocol	Intranet Port	Action	Operation
<div style="display: flex; justify-content: space-between; align-items: center;"> No records to view </div>							

Refresh
Apply

Home > Network > Firewall

Interface: LTE

Status:

ICMP Access:

Telnet Access:

SSH Access:

WEB Access:


ICMP Through:

NAT Through:

Default Action: Drop

Action Rule Table						
<input type="checkbox"/>	Name(unique)	Extranet Address	Intranet Address	Protocol	Intranet Port	Operation
No records to view						

Refresh Apply

Click  to add firewall rules. The maximum rule count is 30.

Add Record
✕

Name(unique)

Extranet Address

Intranet Address

Protocol TCP ▼

Intranet Port

Action Drop ▼

Submit
Cancel

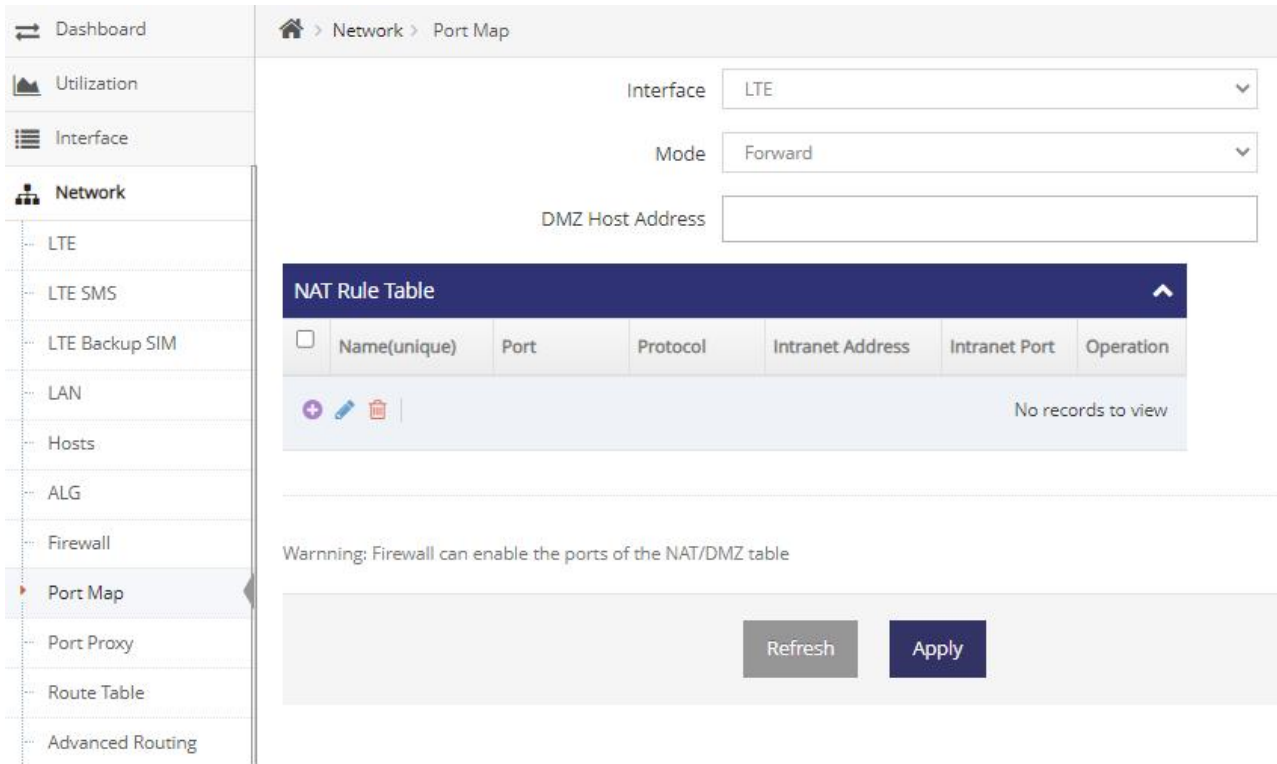
Parameter	Instruction	Default
Interface	WAN/LTE/VPN interface Options	WAN
Status	Enable/Disable Options	ON
ICMP Access	Indicate the ordinal of the list.	OFF
Telnet/SSH/WEB Access	Enable/Disable Telnet/SSH/WEB remote access	Disable
ICMP Through	Enable/Disable ICMP Through	Enable
NAT Through	Configure external port of router which can be accessed by other hosts from internet.	Enable
Default Action	Accept/Drop Options	Drop
Name(unique)	Indicate the ordinal of the list.	Null
Extranet Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Intranet Address	The destination address inside the LAN.	Null
Protocol	TCP, UDP and ALL options	Null
Intranet Port	The destination port inside the LAN.	Null
Action	Accept and Drop	


Step 2 Please Click “Apply” to finish.

----End

2.5.8 Port Map

Step 1 Basic Network->Port Map routing to enter setting page.



Click  to add port mapping rules. The maximum rule count is 30.

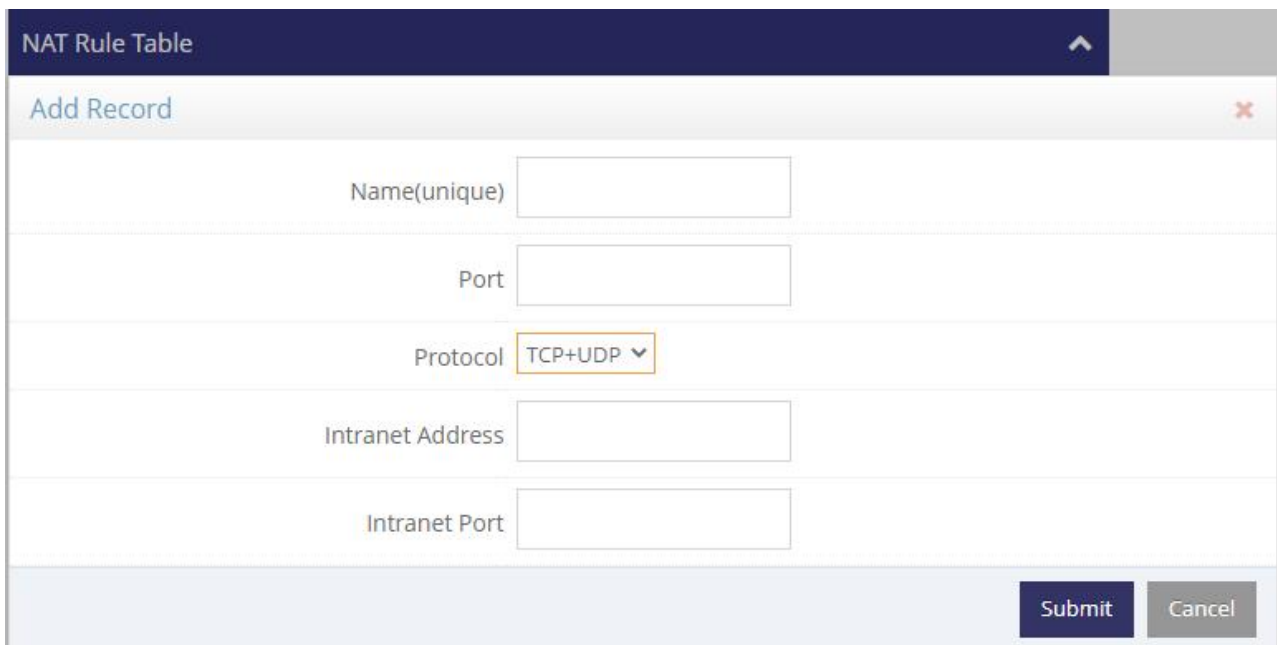


Table 2-3 Port Map Setting Instruction

Parameter	Instruction	Default
Interface	LTE/VPN interface Options	LTE

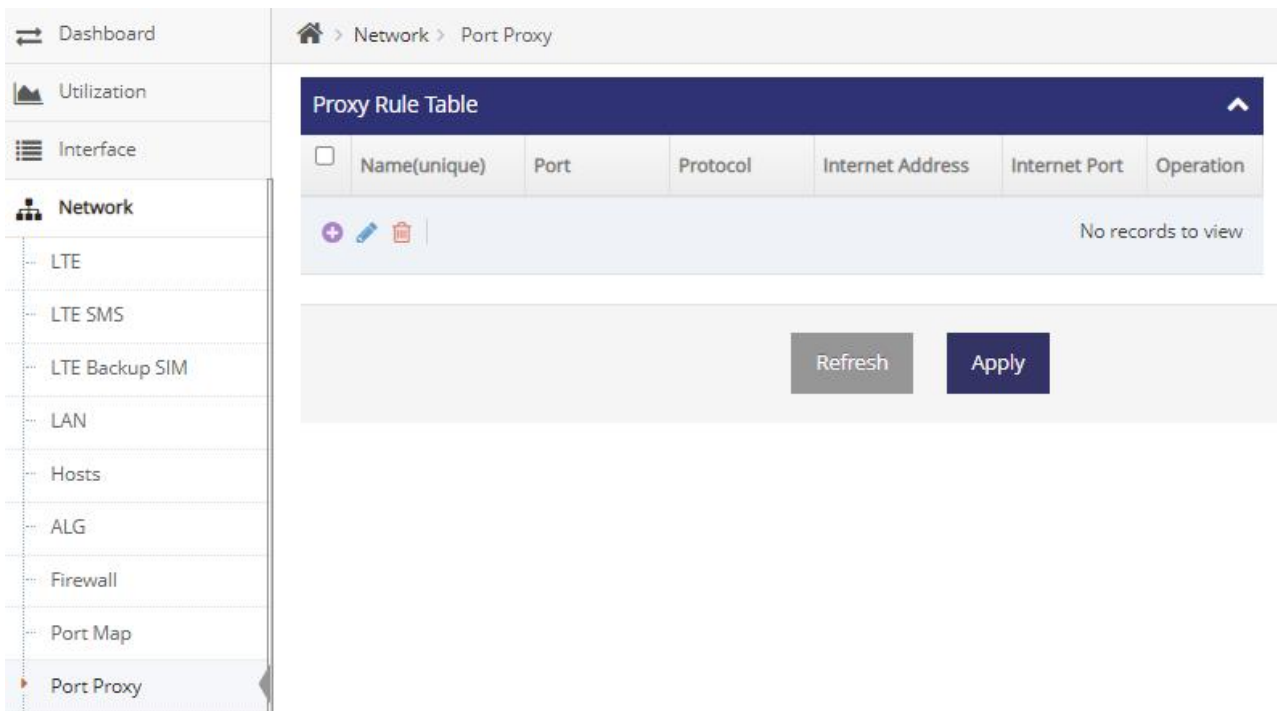
Parameter	Instruction	Default
Mode	Forward/DNAT Options	Forward
DMZ Host Address	The destination IP address inside the LAN. The DMZ will be available after configured host IP address.	Null
Name(unique)	Indicate the ordinal of the list.	Null
Port	Configure external port of router which can be accessed by other hosts from internet.	Null
Protocol	UDP, TCP, Both UDP/TCP Options	UDP+TCP
Intranet Address	The destination address inside the LAN.	Null
Intranet Port	The internal port of router's LAN	Null

Step 2 Please Click "Apply" to finish.

----End

2.5.9 Port Proxy

Step 1 Network->Port Proxy to enter the setting page.



Add Record
✕

Name(unique)

Port

Protocol TCP+UDP ▼

Internet Address

Internet Port

Submit
Cancel

Table 2-4 Port Map Setting Instruction

Parameter	Instruction	Default
Name(unique)	Indicate the ordinal of the list.	Null
Port	Configure external port of router which can be accessed by other hosts from internet.	Null
Protocol	UDP, TCP, Both UDP/TCP Options	UDP+TCP
Intranet Address	The destination address inside the LAN.	Null
Intranet Port	The internal port of router's LAN	Null



NOTE

The feature is suitable for those device without gateway IP address. However, the device need to connect internet. The WL-R320 will provide port proxy for the device. Then WL-R320 will transfer device data to internet.

Step 2 Please Click "Apply" to finish.

----End

2.5.10 Routing Table

Step 1 Network->Routing Table to enter the setting page.

Home > Network > Routing Table

Route Table								
<input type="checkbox"/>	Name(unique)	IP Address	Subnet Mask	Gateway	Interface	Network Device	Metric	Operation
<input type="checkbox"/>	System Rules	192.168.10.0	255.255.255.0	0.0.0.0	WAN	eth0.2	0	
<input type="checkbox"/>	System Rules	192.168.8.0	255.255.255.0	0.0.0.0	LAN	lan	0	
<input type="checkbox"/>	System Rules	127.0.0.0	255.255.255.0	0.0.0.0	Not Specified	lo	0	
<input type="checkbox"/>	System Rules	8.8.8.8	255.255.255.255	192.168.10.1	WAN	eth0.2	0	
<input type="checkbox"/>	System Rules	0.0.0.0	0.0.0.0	192.168.10.1	WAN	eth0.2	0	

|
 << < | 1 / 1 | > >> 20 ▾ View 1 - 5 of 5

Refresh

Add Record ✕

Name(unique)

IP Address

Subnet Mask

Gateway

Interface Not Specified ▾

Metric

Submit
Cancel

Table 2-5 Router Setting Instruction

Parameter	Instruction	Default
Name(unique)	Indicate the ordinal of the list.	Null
IP Address	Router can reach the destination IP address.	Null
Subnet Mask	Subnet mask for destination IP address	Null
Gateway	Next hop IP address which the router will reach.	Null
Interface	Interface from router to gateway.	Null

Parameter	Instruction	Default
Metric	The metric value acts as a measurement of priority. If a packet about to be routed matches two or more rules, the one with the lower metric is applied. Metric value range 0~255.	Null

Step 3 Please Click “Apply” to finish.

----End

2.5.11 Advanced Routing

Step 1 Basic Network->Advanced routing to enter setting page.

Home > Network > Advanced Routing

Packet Mark List

<input type="checkbox"/>	Name(unique)	Mark ID	Source IP	Dest IP	Protocol	Source Port	Dest Port	Operation
« < 1 / 0 > » 10 No records to view								

Routing Rule List

<input type="checkbox"/>	Name(unique)	Source Address	Subnet Mask	Source Interface	Mark ID	Table ID	Pref	Operation
« < 1 / 0 > » 10 No records to view								

Routing Table List

<input type="checkbox"/>	Name(unique)	Table ID	Dest Address	Subnet Mask	Gateway	Interface	Metric	Operation
« < 1 / 0 > » 10 No records to view								



Advanced Routing Features used to configure routing based on packet Mark, source addresses or ports. It will include 3 steps configuration as following.

- 1) Packet Mark. Mark the packet in the Packet Mark list. It will provide Mark ID.
- 2) Routing rule. Specify source address or Mark ID. It will provide routing Table ID.
- 3) Add Routing. Add a routing rule to the routing table specified by the routing table id, requiring that data accessing the specified IP address or IP address segment is sent to the specified next hop address via the specified interface.

Commonly, the source address is widely used for applications. It just need to configure routing rule and

configure routing table.

Add Record
✕

Name(unique)

Source Address

Subnet Mask

Source Interface Not Specified ▼

Mark ID

Table ID

Pref

Submit
Cancel

Table 2-6 Source Address Routing Setting Instruction

Parameter	Instruction	Default
Name(unique)	Indicate the ordinal of the list.	Null
Source Address	Allow the specified subnet IP address/IP segment data to specify the destination IP or interface.	Null
Subnet Mask	Subnet mask for destination IP address	Null
Source Interface	Specify source address interface.	Not specified
Mark ID	Mark ID is created in Mark ID list. Source address without the Mark ID.	Null
Table ID	Create routing table ID and Add the table ID in routing table list. Table ID value range 100~250.	Null
Pref	Controls the order of IP rules. Rules with a lower priority value will be checked first.	Null

Add Record ✕

Name(unique)

Table ID

Dest Address

Subnet Mask

Gateway

Interface Not Specified ▼

Metric

Submit
Cancel

Table 2-7 Source Address Routing Setting Instruction

Parameter	Instruction	Default
Name(unique)	Indicate the ordinal of the list.	Null
Table ID	Input the Table ID as the same as in Routing Rule list	Null
Dest Address	Routing can reach the destination IP address.	Null
Subnet Mask	Subnet mask for destination IP address	Null
Gateway	Next hop IP address which the routing will reach.	Null
Interface	Interface from router to gateway.	Not specified
Metric	The metric value acts as a measurement of priority. If a packet about to be routed matches two or more rules, the one with the lower metric is applied. Metric value range 0~255.	Null

Step 2 Please Click "Apply" to finish.

---End

2.6 VPN Setting

2.6.1 IPSec Setting

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

Dashboard > VPN > IPSEC Connection

IPSEC Client

Connection Status	Online	Peer Address	222.248.230.163
Local <-> Peer	10.18.92.217<=>222.248.230.163	Local Network <-> Peer Network	192.168.8.0/24<=>192.168.31.0/24
Online Time	56 seconds ago	Rx/Tx(byte)	0/0

Peer Address: 222.248.230.163

Peer Network: 192.168.31.0

Peer Network Mask: 255.255.255.0

Peer Identify Type: IP

Local Identify Type: IP

Aggressive Mode:

Password: *****

IKE Version: IKEv1

IKE Authentication: MD5

Step 2 Please click "Apply" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

---End

2.6.2 OpenVPN Client Setting

Step 1 VPN > Openvpn client to check or modify the relevant parameter.

Topology

Server Address

Device

Protocol

Port

Cipher

LZO Compress

Auth Type

HMAC Signature Check

IP Masquerade(NAT)

Default Route

Custom DNS

Keepalive Interval(sec)

Keepalive Timeout(sec)

OpenVPN Custom Options(Separated by semicolons)

Table 2-8 OpenVPN Client Instruction

Parameter	Instruction	Default
Technology	Subnet/Point-to-point options	Subnet
Server Address	The Openvpn server public IP address and port.	Null
Device Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.	TUN
Protocol	UDP and TCP optional.	
Port	The Openvpn server port.	
Cipher	Encryption Cipher as requested. Null as Auto	Null

Parameter	Instruction	Default
LZO Compress	Disable/Adaptive/Yes/No options	No
Auth. Type	Certificate and Username/password options	Certificate
HMAC Signature	Disable/TLS options	Disable

Step 2 Please click "Apply" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

---End

2.6.3 OpenVPN Server Setting

Step 1 VPN > Openvpn Server to check or modify the relevant parameter.

Home > VPN > OpenVPN Server

Status

Refresh
Apply

Certificate Authority(CA) Certificate	<input type="text" value="No File"/>	Choose	Generate
Certificate Authority(CA) Private Key	<input type="text" value="No File"/>	Choose	Generate
Server Certificate	<input type="text" value="No File"/>	Choose	Generate
Server Private Key	<input type="text" value="No File"/>	Choose	Generate
Diffie Hellman Parameters	<input type="text" value="No File"/>	Choose	Generate

Client Certificate List(0)

Client Name	Certificate	Private Key	Operation
No records to view			

Status

Topology: Subnet

Device: TUN

Protocol: UDP

Port: 1194

Cipher:

LZO Compress: Disable

Tunnel Subnet: 10.0.0.0

Tunnel Subnet Mask: 255.255.255.0

Tunnel DNS:

Tunnel DNS2:

Client to Client:

Client Duplication:

Auth Type: Certificate

HMAC Signature Check: Disable

Keepalive Interval(sec): 10

Keepalive Timeout(sec): 120

OpenVPN Custom Options(Separated by semicolons)

Table 2-9 OpenVPN Client Instruction

Parameter	Instruction	Default
Technology	Subnet/Point-to-point options	Subnet
Server Address	The Openvpn server public IP address and port.	Null
Device Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.	TUN
Protocol	UDP and TCP optional.	
Port	The Openvpn server port.	
Cipher	Encryption Cipher as requested. Null as Auto	Null
LZO Compress	Disable/Adaptive/Yes/No options	No
Auth. Type	Certificate and Username/password options	Certificate
HMAC Signature	Disable/TLS options	Disable

Step 2 Please click "Apply" to finish.



The OpenVPN server supports to generate certificate for testing. We suggest generate certificate from third party server.

----End

2.6.4 L2TP Client Setting

Step 1 VPN > L2TP Client to check or modify the relevant parameter.

Application > L2TP Client

Status

Connection Status	Down	Server IP Address
Local IP Address		Remote IP Address
Subnet Mask		Gateway
DNS		DNS2
Rx/Tx(byte)	/	Live Time

Server Address

Server Port

Username

Password

Tunnel Auth Mode

IP Masquerade(NAT)

Default Route

Custom DNS

Custom IP Address

MTU

LCP Echo Interval

LCP Echo Times

PPP Option

Step 1 Please click "Apply" to finish.

----End

2.6.5 PPTP Client Setting

Step 1 VPN > PPTP client to check or modify the relevant parameter.

Application > PPTP Client

Status

Connection Status	Down	Server IP Address
Local IP Address		Remote IP Address
Subnet Mask		Gateway
DNS		DNS2
Rx/Tx(byte)	/	Live Time

Server Address

Username

Password

MPPE Encryption MPPE MPPE State Encryption

IP Masquerade(NAT)

Default Route

Custom DNS

Custom IP Address

MTU

LCP Echo Interval

LCP Echo Times

PPP Option

Step 2 Please click "Apply" to finish.

---End

2.6.6 GRE

Step 1 Application > GRE client to check or modify the relevant parameter.

Status

Connection Status	Down	Peer IP Address
Local IP Address		Remote IP Address
Subnet Mask		Gateway
DNS		DNS2
Rx/Tx(byte)	/	Live Time

Extern Interface

Peer Address

Local IP Address

Remote IP Address

TTL

IP Masquerade(NAT)

Default Route

Route Table

	Rule Name	Target Address	Target Mask
+	No records to view		

Custom DNS

Step 2 Please click "Apply" to finish.

----End

2.7 Wireless Setting

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

2.7.1 SSID Setting

Step 1 Wireless->SSID Setting to configure relative parameter.

Home > Wireless > 2.4G SSID

Status

SSID

Security Mode

WPA Mode

Password

Hide SSID

Isolate Clients

Clients ACL

Step 2 Wireless->SSID Setting to ACL relative parameter.

Home > Wireless > 2.4G SSID

Clients ACL

ACL Type Black List White List

Station List						
<input type="checkbox"/>	MAC	Hostname	IP Address	Live Time	RSSI	Operation
+ Edit Delete Scan						No records to view

Step 3 Wireless->SSID Setting to Channel relative parameter.

Mode

Band Width

Country

Channel

Beacon

DTIM

STBC

Short GI

Tx Power

Step 4 Please click "Apply" to finish.

----End

2.7.2 AP Client

Step 1 Wireless->AP Client to enter the setting page.

2.4G AP Client

Status	DOWN 	MAC
Peer		Peer MAC
RSSI		Channel
Rx/Tx	0B / 0B	Rate

Scan

Peer SSID

Peer SSID2

Peer SSID3

Lock Strong Signal

Lock BSSID

Security Mode

Hidden SSID

Parameter	Instruction	Default
2.4G AP Client	Wi-Fi Client ON/OFF	OFF
Peer SSID	Defined the available SSID to connect. Supports 3 SSIDs as Options.	Null
Lock Strong Signal	The Wi-Fi client will always connect the strongest signal SSID.	Null
Lock BSSID	The Wi-Fi client will always connect the Basic Service Set Identifier(BSSID)	Null
Hidden SSID	Supprts to connect hidden SSID. It's necessary to define the channel of hidedd SSID.	Null

Step 2 Please click “Apply” to finish.

----End

2.7.3 Clients

Step 1 Wireless->Clients to enter the client list page.

Online Number(1) ^						
Hostname	MAC Address	IP Address	Live Time	Rx/Tx	RSSI	Operation
HUAWEI_Mate_20-da5235c086	12:B5:09:6B:23:28	192.168.8.67	00:00:04	0B / 0B	-68dBm	Knock

----End

2.8 Station

2.8.1 Access Control

Step 1 Station Control > Access Control to check or modify the relevant parameter.

Home > Station > Access Control

Status

ACL Rule											
<input type="checkbox"/>	Rule Name	Action	Dest	Protocol	Port	Start Date	End Date	Start time	End time	Week	Operation
No records to view											

Configure access control for the entire network, need click <apply> to save and apply

Refresh

Apply

Add Record

Rule Name

Source

Type

Action

Dest&Domain&Keyword

Dest Port

Time Settings

Start Date

End Date

Start time

End time

Week Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Submit

Cancel

Table 2-10 Access Control Instruction

Parameter	Instruction	Default
Rule Name	Indicate the ordinal of the list.	Null
Source Address	Specify the station device IP, MAC and IP segment.	Null

Parameter	Instruction	Default
	If configure multiple IP addresses with comma(,) as separator.	
Type	Support UDP/TCP/Domain/keyword filter	TCP
Action	Drop, Accept and Return options	Drop
Destination Address	Indicate the ordinal of the list.	Null
Protocol	All, UDP, TCP options	All
Time Setting	Define access control available time.	Disable

Step 2 Please click "Apply" to finish



- 1) It will accept/drop the destination address and content(keyword/domain name) from router.
- 2) It will accept/drop the whitelist/blacklist.



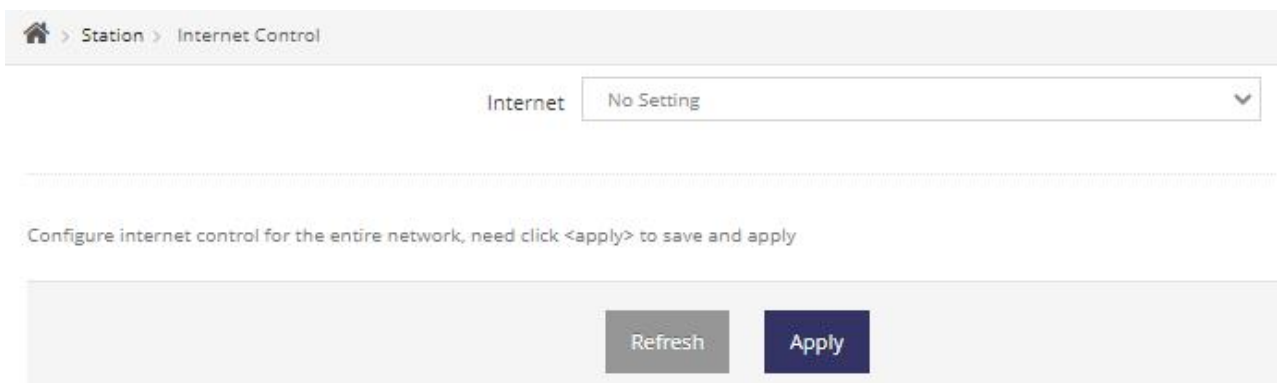
Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.8.2 Internet Control

Step 1 Station Control > Internet Control enter the setting GUI.



Step 2 Please click "Apply" to finish

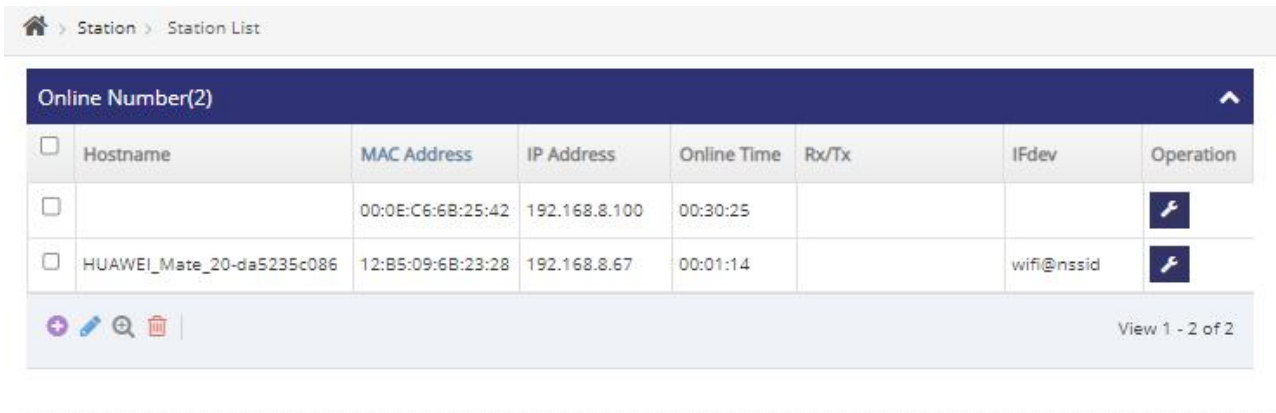


It will support to control internet access authority and time management

----End

2.8.3 Station List

Step 1 Station Control > Station List to enter the GUI to check station list. We may check the device list in the station.



The <delete> here will clear the station of all configure

Step 2 Please click "Apply" to finish.



NOTE

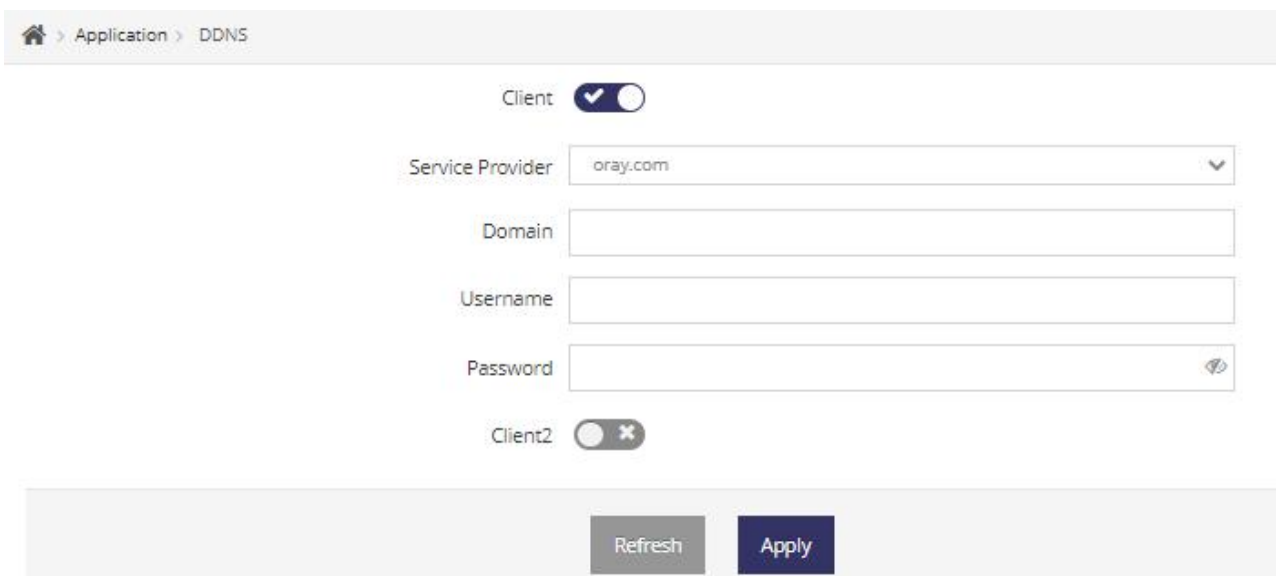
- 1) It will support to control and manage the specified devices to access to internet.
- 2) It will support accept/drop the specified devices destination address and content(keyword/domain name).

----End

2.9 Application

2.9.1 DDNS

Step 1 Application > DDNS to check or modify the relevant parameter.



Step 2 Please click "Apply" to finish.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

----End

2.9.2 Dynamic Routing

Step 1 Application > Dynamic Routing to check or modify the relevant parameter.

Step 2 Please click "Apply" to finish.

----End

2.9.3 GNSS(Optional)

Step 1 Application > GNSS to check or modify the relevant parameter.

Home > Application > GNSS

Status

Source 4G GPS

State Searching

UTC 15:28:34:11:13:2022

LON/LAT 0.000000, 0.000000

Elevation 0.00m

Speed 0.00km/h

Direction 0.000

Declination 0.000

Number Of Satellite 0

Map Preview

Client

Client2

Local Server

Step 2 Please click "Apply" to finish.



GNSS feature is optional according to customer requirements. It supports two clients mode and one server mode. When the GNSS located successfully, the GNSS information will be display in the GUI. WL-R320 supports UDP/TCP/MQTT protocol to send GNSS data in the client mode and supports UDP/TCP protocol to send GNSS data in the server mode.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

---End

2.9.4 VRRP

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

The screenshot shows the VRRP configuration page. At the top, there is a breadcrumb: Home > Application > HA(VRRP). The configuration fields are as follows:

- Status:
- Virtual IP: 192.168.8.254/24
- Device Group ID: 1
- Mode: Master
- Priority: 100
- Advert(sec): 1
- Preempt:
- Auth: 1234

At the bottom, there are two buttons: 'Refresh' and 'Apply'.

Table 2-11 VRRP Filtering Instruction

Parameter	Instruction	Default
Status	Enable/Disable options	OFF
Virtual IP	Drop, Accept and Return options	Drop
Device Group ID	Specify which VRRP group of this router belong to.	Null
Mode	Master/backup option	Master
Priority	Enter the priority value from 1 to 255. The larger value has higher priority.	100
Advert(Sec)	Advertisement interval, unit as sec	1
Preempt	Enable preemption on the router and configure its preemption delay in a specific VRRP group.	OFF
Auth.	Master and backup mode router authentication key	1234

Step 2 Please click "Apply" to finish.

---End

2.9.5 Remote IO

Step 1 Application > Remote IO to check or modify the relevant parameter.

Home > Application > Remote IO

Current IO Status g1=00;g2=01;

G1

G2

SMS Monitoring Center

Center Number

Center2 Number

Center3 Number

Client

Client2

GPIO Value Format

Item	Value	Indication
GPIO number	g1	g1 for GPIO1(G1) port g2 for GPIO2(G2) port g3 for G3 port(Reserved)
First Digit	1	Output(DO)
	0	Input(DI)
Second Digit	1	High Level(3.3v)
	0	Low Level(0v)
Separator sign	;	

Step 2 Please click "Apply" to finish.



The remote IO feature support to remotely control IO by SMS and TCP protocol, and support IO status to report server by SMS and TCP protocol.



Configuration Instance

Please check lock bank configuration in the chapter 3 as reference.

---End

2.9.6 TTL/RS232

Step 1 Application > TTL/R232 to check or modify the relevant parameter. Serial #1 for RS232 port and Serial #2 for RS485 port as default.

Table 2-12 Serial Port Instruction

Parameter	Instruction	Default
Status	ON/OFF Options	ON
Mode	GNSS, Command Line, Modbus, MQTT, Transport Forwarding Options. Transport Forwarding for example as below.	Command Line
Convert	ON/OFF Options. RS232/RS485 for ON status. Two	ON

Parameter	Instruction	Default
	serial port for TTL/TTL, please choose OFF status.	
Server Address	The Openvpn server public IP address and port.	
Baud rate	1200~230400 Options	57600
Flow Control	Disable/Hard/Soft options	Disable
Parity	Disable/Odd/Even	Disable
Data Bit	Data bit 5,6,7,8 options	8
Stop Bit	Stop bit 1,2 options	1
Active Packet	Disable/Idle/Time options	Disable
Center Address	Supports 3 data server synchronously. IP address and domain name are acceptable for Server IP	OFF
Protocol	Data server port	Null
Port	TCP/UDP options	TCP



NOTE Customize Register Packet

Registration Packet

Packet Size(Byte)

Time between Packets(ms)

Prefix of Packet

Suffix of Packet

Keepalive Packet

Step 2 Please click "Apply" to finish.

----End

2.9.7 L2TP Client

2.10 System

2.10.1 Device

Step 1 System > Device to check or modify the relevant parameter.

System > Device

Device Name	WL-R320-12BC30	Modify
MAC Address	00:03:7F:12:BC:30	
Current Time	12:20:09 (06/19/2022)	Copy from computer
Time Source	NTP Server	
Run Time	03:59:46	
System Reboot		

Operation Mode

Language Settings Restore to factory will not change its setting

Time Zone

NTP [Sync](#)

NTP Server

NTP Server2

NTP Server3

NTP Service

[Refresh](#) [Apply](#)

Step 2 Please click "Apply" to finish.

----End

2.10.2 Configure

Step 1 System > Configure to check or modify the relevant parameter.

System > Configure

Configure Version 8

[Backup Configure](#) [Default Configure](#)

Restore Configure [Choose](#)

Step 2 Please click "Apply" to finish.

----End

2.10.3 Software

Step 1 System > Software to check or modify the relevant parameter.

Home > System > Software

Firmware

Firmware Version: 4.3.5-053022

Upgrade: [Choose](#)

Upgrade Online

[Check new version](#)

Software Repositories

[Enter Repositories](#)

Software List

Software Number(0)					
Name	Size	Version	Author	Introduction	Operation
Clear Installed Software and Default Configure					

Step 2 Please click "Apply" to finish.

---End

2.10.4 Password

Step 1 System > Password to check or modify the relevant parameter.

System > Password

Username

Old Password

New Password

Repeat New Password

Step 2 Please click "Apply" to finish.

---End

2.10.5 Auto Reboot

Step 1 System > Auto Reboot to check or modify the relevant parameter.

System > Auto Reboot

Reboot Mode

Minimum running time(sec)

None Client duration(sec)

Point Reboot Time

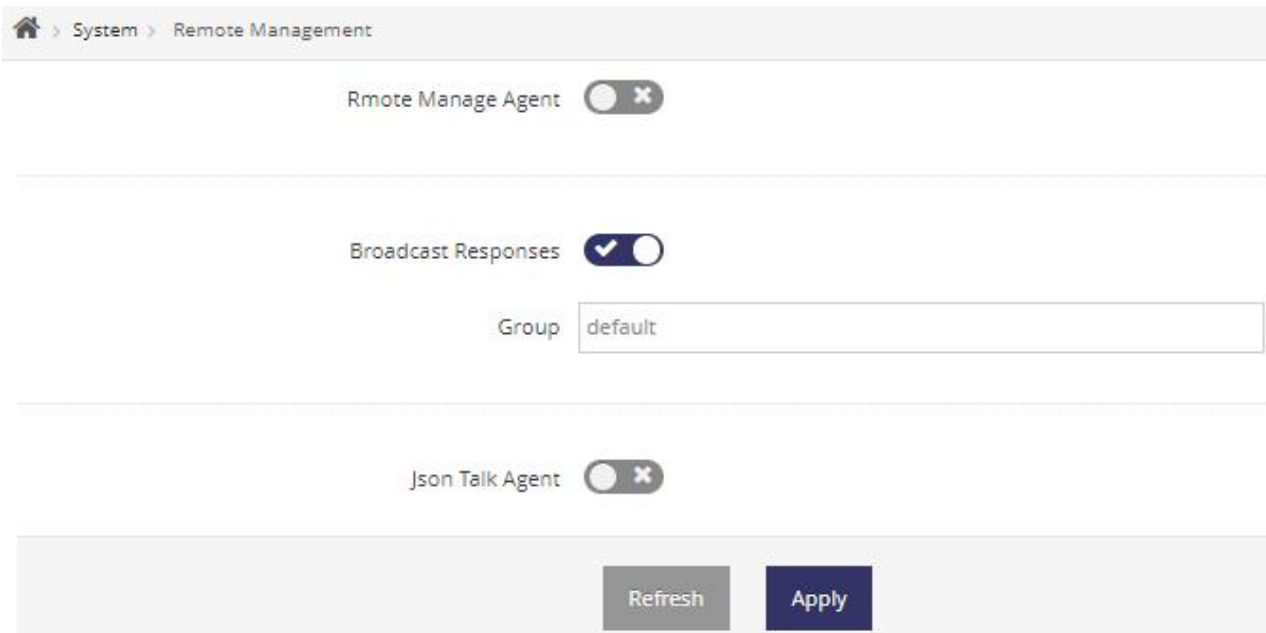
Maximum running time(sec)

Step 2 Please click "Apply" to finish.

---End

2.10.6 Manage Server

Step 1 System > Manage Server to check or modify the relevant parameter.

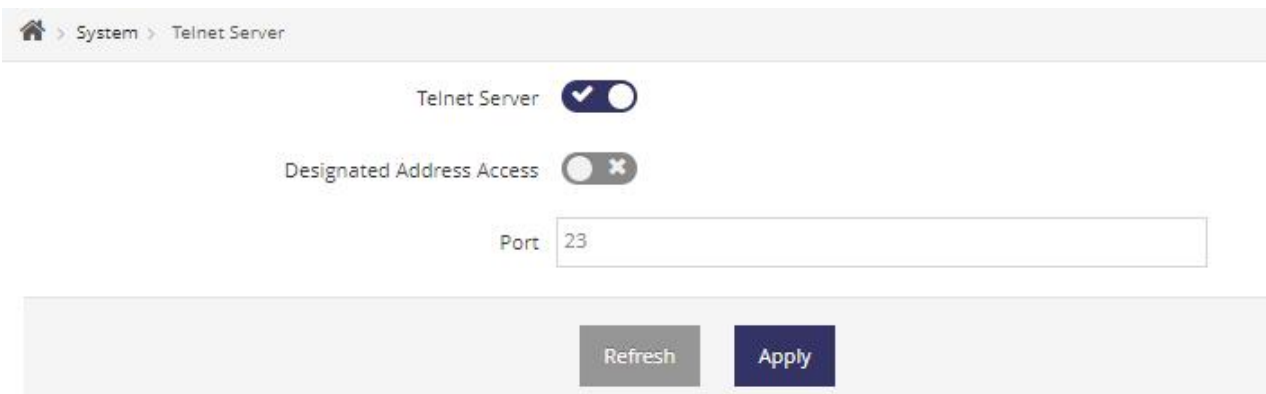


Step 2 Please click "Apply" to finish.

---End

2.10.7 Telnet Server

Step 1 System > Telnet Server to check or modify the relevant parameter.

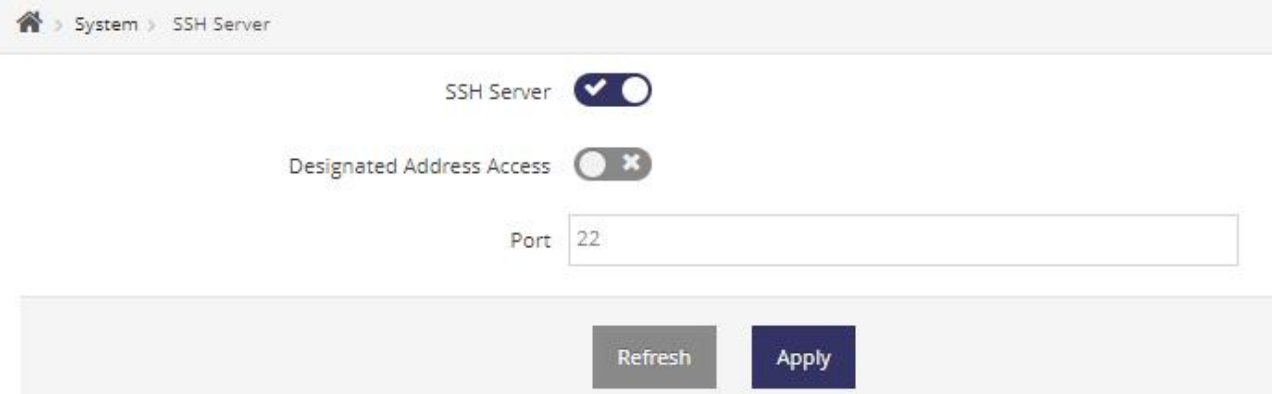


Step 2 Please click "Apply" to finish.

---End

2.10.8 SSH Server

Step 1 System > SSH Server to check or modify the relevant parameter.

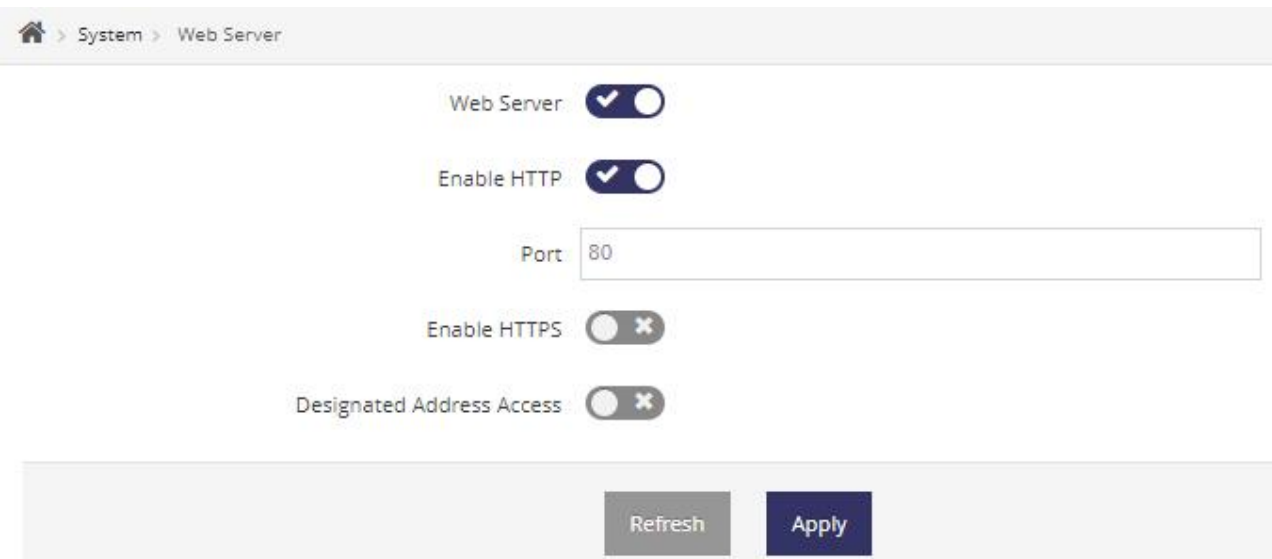


Step 2 Please click "Apply" to finish.

---End

2.10.9 Web Server

Step 1 System > Web Server to check or modify the relevant parameter.



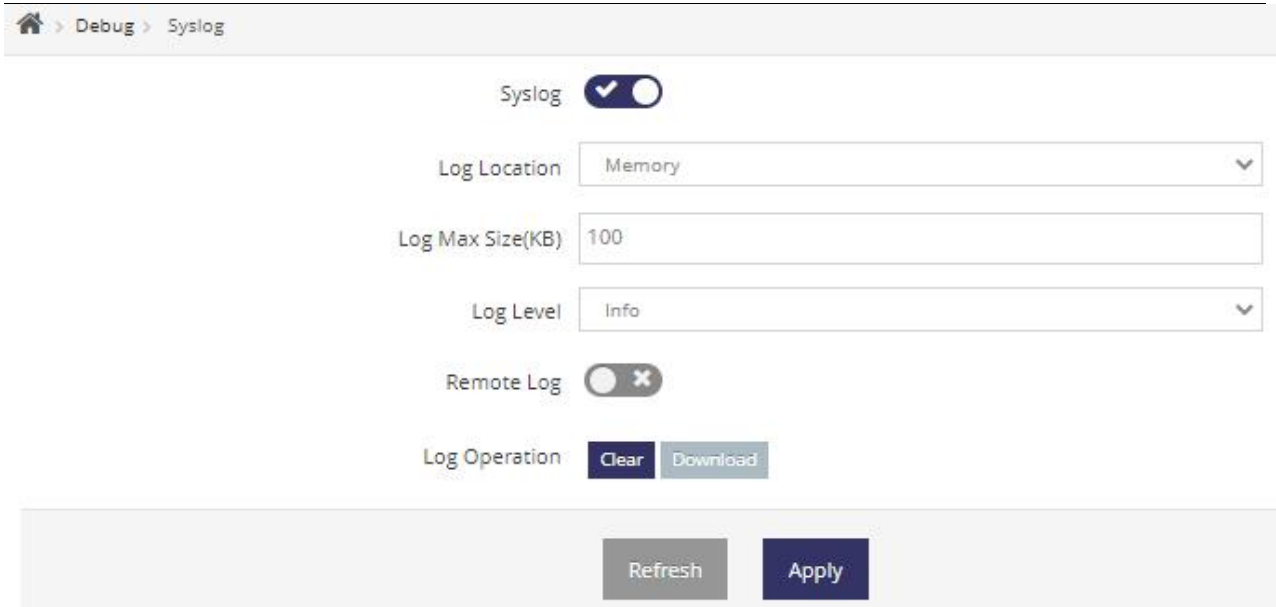
Step 2 Please click "Apply" to finish.

---End

2.11 Debug

2.11.1 Syslog

Step 1 Please click "Debug> Syslog" to enter the GUI to download logs and capture logs by local or remote.

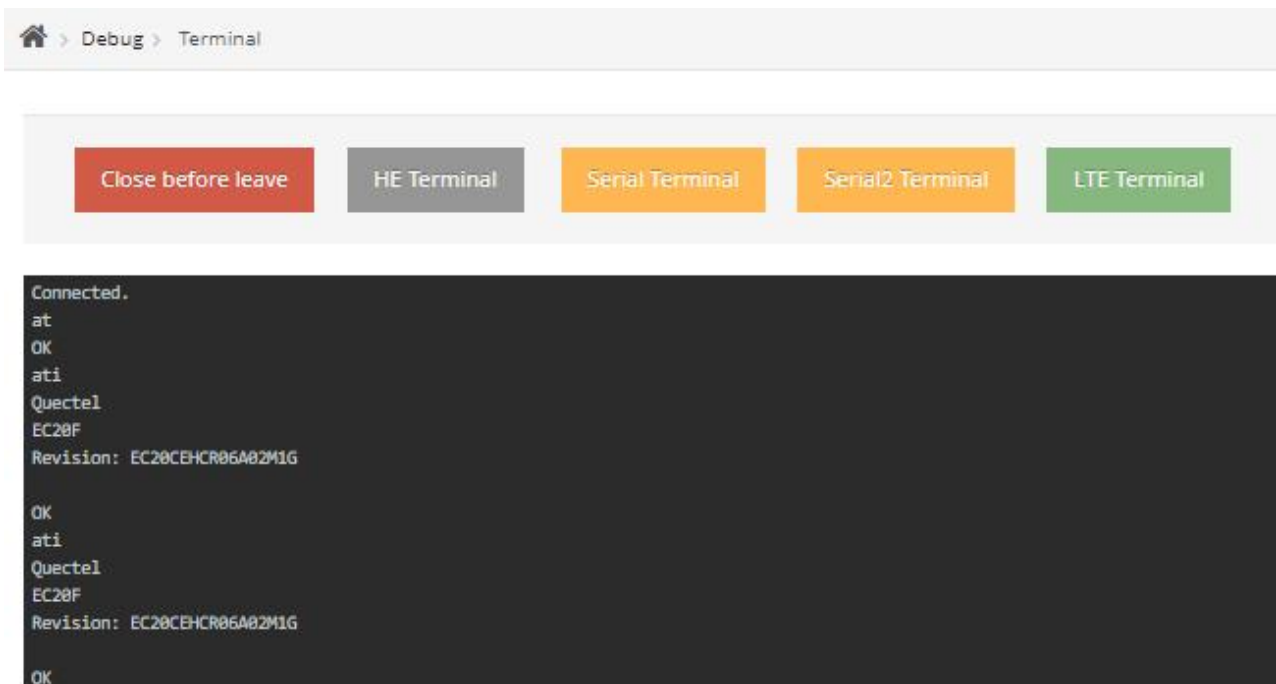


Step 2 Please click "Apply" to finish

---End

2.11.2 Terminal

Step 1 Debug > Terminal to check or modify the relevant parameter.

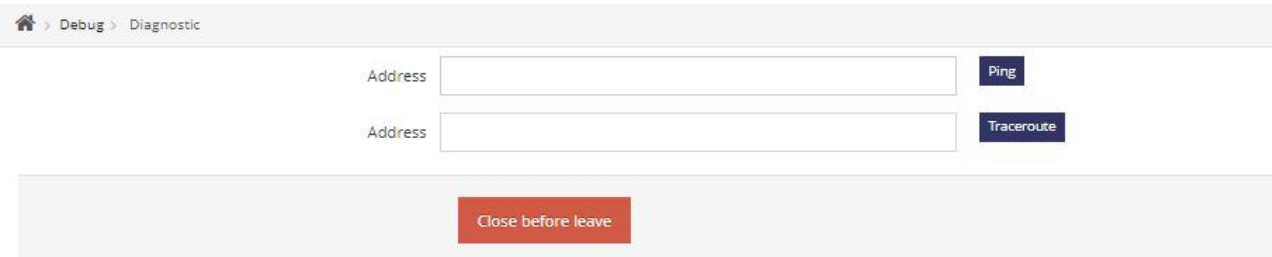


Step 2 Please click "Apply" to finish.

---End

2.11.3 Diagnostic

Step 1 Please click "Debug> Diagnostic" to enter the GUI for Ping and Traceroute.

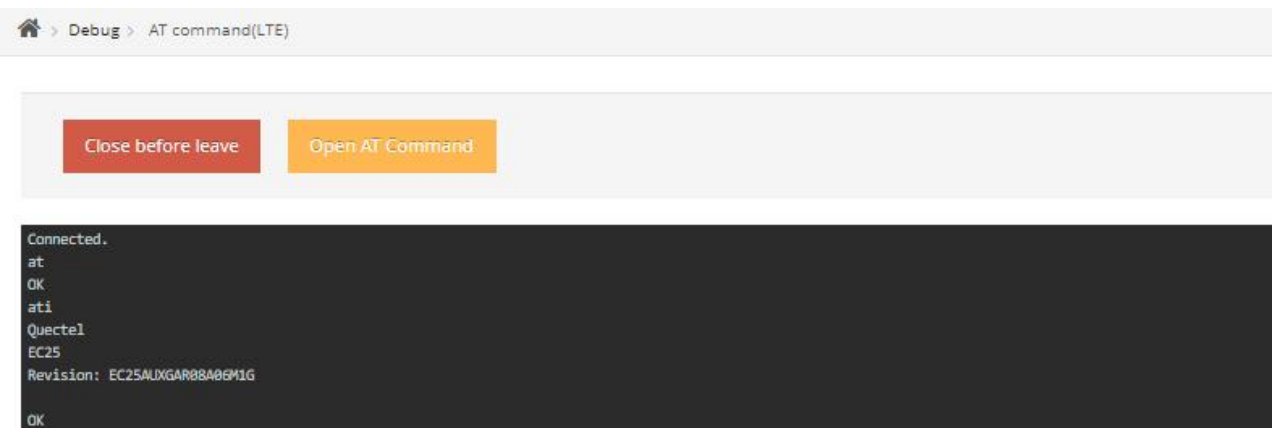


Step 2 Please click "Apply" to finish.

---End

2.11.4 AT Command(LTE)

Step 1 Please click "Debug> Diagnostic" to enter the GUI for Ping and Traceroute.



Step 2 Please click "Apply" to finish.



The 4G connection will be closed once opened AT command.

---End

2.12 Development(SDK)

Home > Development > SDK

a. How to download SDK and compile upgrade package

1. It is recommended to download this SDK after setting up the compilation environment in Ubuntu.

2. Enter the following command line to download from the Ubuntu terminal command line

```
git clone https://github.com/skinos7/tiger7.git
```

3. After waiting for the download, enter the tiger7 directory and input the following instructions to update the SDK to the latest state

```
cd tiger7
make ubuntu_preset
make pid_gBOARDID=mtk2-mt7628-d218
make update
make menu
```

4. After waiting for the update, you can input the following instructions to compile the corresponding products

```
make dep
make
```

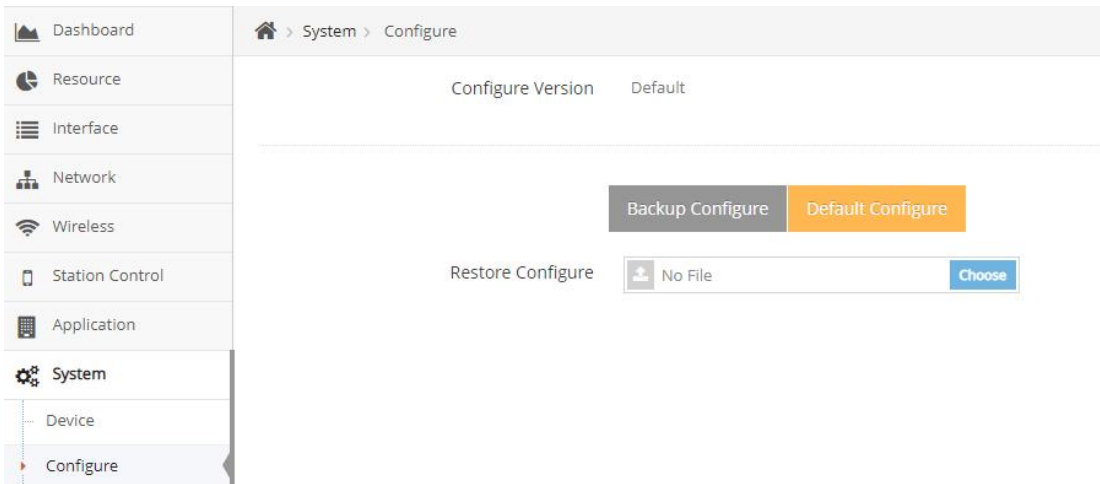
5. After waiting for the compilation, an upgrade package file ending with .zz will be generated in the ./build directory, which can be upgraded through the upgrade interface of the router

2.13 Default Factory Configuration

Three methods to default factory configuration

2.13.1 Reset in GUI

Click System--->Configure to enter Configure UI, Click Default Configure to reset router to default factory configuration.



2.13.2 Reset in SSH/Telnet

Login router via SSH/Telnet, then implement machine.default command to reset the router.

```
admin120-D17F38 login:
Password:

      EEEEEEEEE LL      FFFFFFFF
      EE        LL      FF
      EE        LL      FF
      EEEEEEEEE LL      FFFFFFFF
      EE        LL      FF
      EE        LL      FF
Ashy  EEEEEEEEE LLLLLLLLL FF

-----
Command Help
-----
@ ----- List all the project
@? ----- List all the static component
@@ ----- List all the dynamic component
<com> ----- Show component configure
<com>. ----- List all component interface
<com>:<config> ----- Get component configure attribute
<com>:<config>=<value> -- Set component configure attribute
-----
# machine.default
```

2.13.3 Reset via RST button

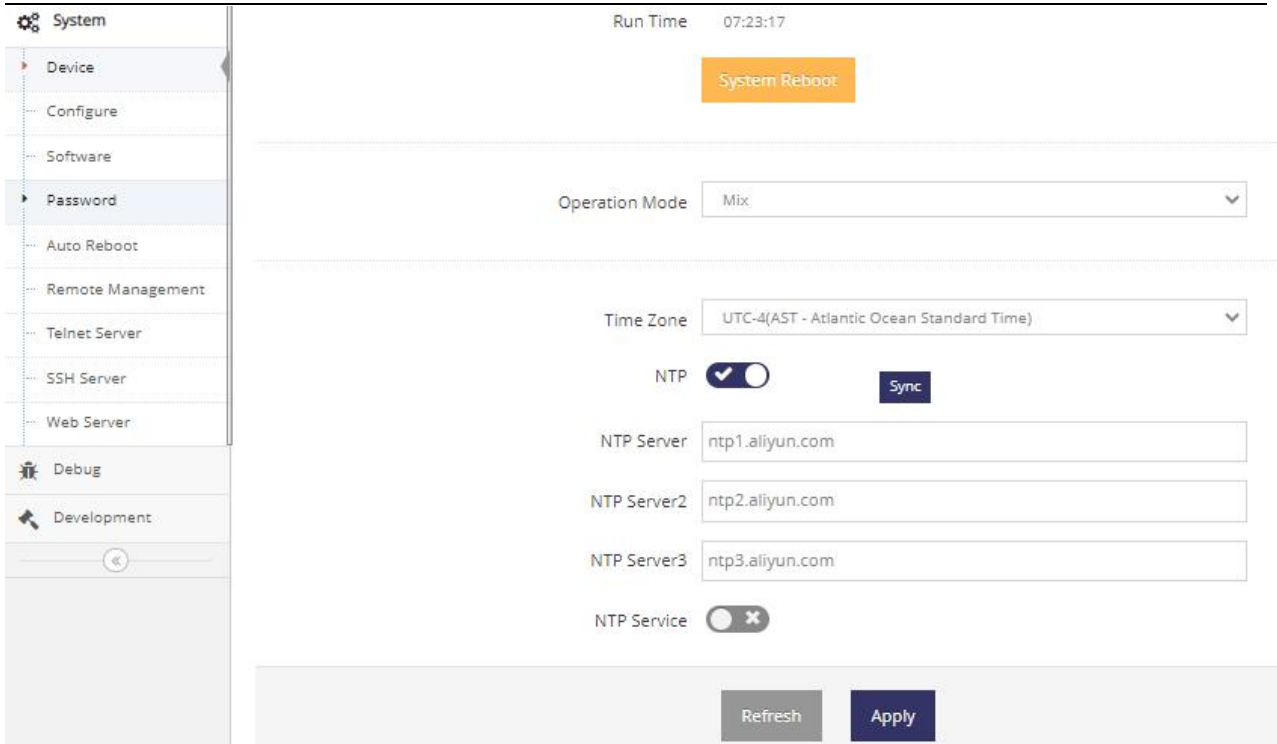
Press the RESET button for 5~8sec after the router startup and run, the router will auto reset to default factory configuration.

4 Configuration Instance

4.1 Link Backup

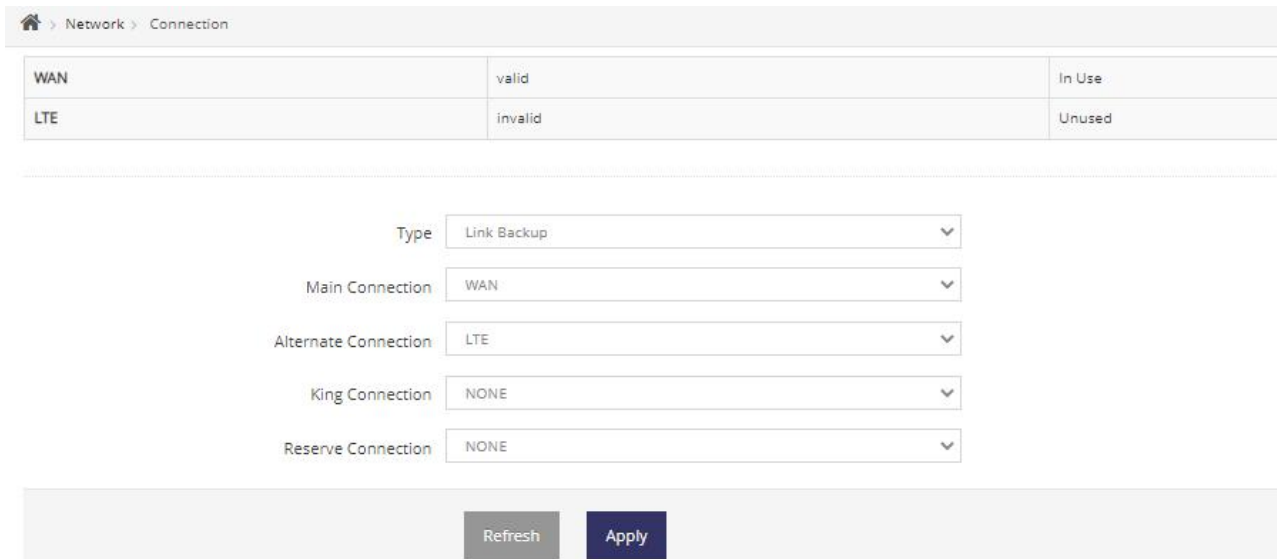
1) Operation mode

Click System---->Device GUI, Choose Mix in Operation mode.



2) Link Backup

Click Network--->Connection GUI, choose link backup mode.



The King Connection with the highest priority. The router link will switch to King Connection once the defined King Connection available.

The Reserved Connection just keep the Connection reachable.

3) Link Backup

Click Network--->WAN GUI, configure WAN and add Availability Check rule.

ICMP failure as configured, the router link will switch to 4G link.

Availability Check	ICMP
Test Address	208.67.222.222
Test Address 2	8.8.8.8
Test Address 3	
Each Query Timeout(sec)	5
Test Times	5
Test Interval(sec)	15

The router support to check 3 test addresses max one time.
 If ICMP is failed, the router will send ICMP as Each Query Timeout.
 If ICMP is reachable, the router will send ICMP as Test Interval.

For example.

If both 208.67.222.222 and 8.8.8.8 are unreachable, the router will check the test address 5 times as interval 5s. It will switch to 4G link. When one of 208.67.222.222 and 8.8.8.8 is reachable, it will switch back to WAN link.

4.2 Lock Band

Click Network--->LTE GUI, Modem Setting to enter Lock Band GUI.

Status	Online	IPv4 Address	10.227.121.29
Network	中国联通 FDD LTE	RSSI	CSQ:13 RSRP:-119dBm
ICCID	89860114851113626956	IMEI	862708044140445
Online Time	00:48:08:0	Rx/Tx	1.79MB / 1.19MB

APN Custom

Attach Mode: Auto

GPS

Modem Settings

Lock IMEI

Lock IMSI

Lock PIN

Lock Band

Input command to lock the corresponding band as below list.

Items	Band	Commands
1	Band1	0,1,0,1
2	Band3	0,4,0,1
3	Band5	0,10,0,1
4	Band7	0,40,0,1
5	Band8	0,80,0,1
6	Band20	0,80000,0,1

For example.

Lock band3 as below.

Lock Band

4.3 LTE SMS

Click Network --->LTE SMS Setting GUI.

The router will just accept the message command as the specified Command phone number and Prefix.

The Contact phone number 13760365619 and Prefix 123456 as example. The prefix doesn't support special characters such as @#>&^*[].

The SMS command lists as following.

Inquiry Items	SMS Command	SMS ACK	Note
4G Status	123456ifname>lte.status:status	Up/Down	
RSRP	123456ifname>lte.status:rsrp	RSRP Value	
CSQ	123456ifname>lte.status:csq	0~31	
IMEI	123456ifname>lte.status:imei	IMEI Value	
ICCID	123456ifname>lte.status:iccid	ICCDI Value	
IMSI	123456ifname>lte.status:imsi	IMSI Value	
Network Type	123456ifname>lte.status:nettype	Network Type	
Operator	123456ifname>lte.status:operator	Operator Name	
MCC/MNC	123456ifname>lte.status:plmn	MCC/MNC	
Online Time	123456ifname>lte.status:lifetime	Online Time	hh:mm:ss

SIM IP	123456ifname>lte.status:ip	SIM IP Address	
Restart	123456land>machine.restart(5)	ttrue	Restart after 5sec.

Mobile Phone Inquiry and ACK.



4.4 DDNS

Click Application-->DDNS GUI to configure DDNS.

The default update time is 600sec for domain name service.

Application > DDNS

Client

State Update Succeed

Domain IP Address 222.248.230.163

Extern IP Address 222.248.230.163

Service Provider oray.com

Domain dimmalex.wicp.net

Username dimmalex

Password

Client2

State Update Succeed

Domain IP Address 222.248.230.163

Extern IP Address 222.248.230.163

Service Provider oray.com

Domain dimmalex.site

Username dimmalex

Password

Refresh

Apply

4.5 GNSS

Click Network--->LTE GUI, Modem Setting to enable GPS feature GUI.

The screenshot shows the 'LTE' configuration page in the router's web interface. On the left is a navigation menu with options like Dashboard, Utilization, Interface, Network, LTE, LTE SMS, LTE Backup SIM, LAN, Hosts, ALG, Firewall, Port Map, Port Proxy, Route Table, and Advanced Routing. The main content area displays the following information:

Status	Online II	IPv4 Address	10.46.165.129
Network	中国联通 FDD LTE	RSSI	 CSQ:18 RSRP:-107dBm
ICCID	89860114851113626956	IMEI	865847058016203
Online Time	00:05:51:0	Rx/Tx	77.55KB / 66.82KB

Below the table, there are several controls:

- APN Custom: (disabled)
- Attach Mode:
- GPS:
- Modem Settings: [Modem Settings](#) button

Click Application-->GNSS GUI to check GPS status GUI.

The screenshot shows the 'GNSS' status page in the router's web interface. The page displays the following information:

- Status:
- Source: 4G GPS
- State: Located
- UTC: 3:1:33:11:14:2022
- LON/LAT: 113.920944, 22.574869
- Elevation: 37.60m
- Speed: 0.00km/h
- Direction: 283.700
- Declination: 286.000
- Number Of Satellite: 5
- Map Preview: [Map Preview](#) button

GPS client mode

Configure TCP server IP, port and GPS data interval. You may custom GPS data as requested such router's ID, GPS data prefix and so on.

Client

Server Address: 113.87.83.74

Protocol: TCP

Port: 40001

Report Interval: 5

Device ID:

Username:

Verification Code:

Report NMEA Header:

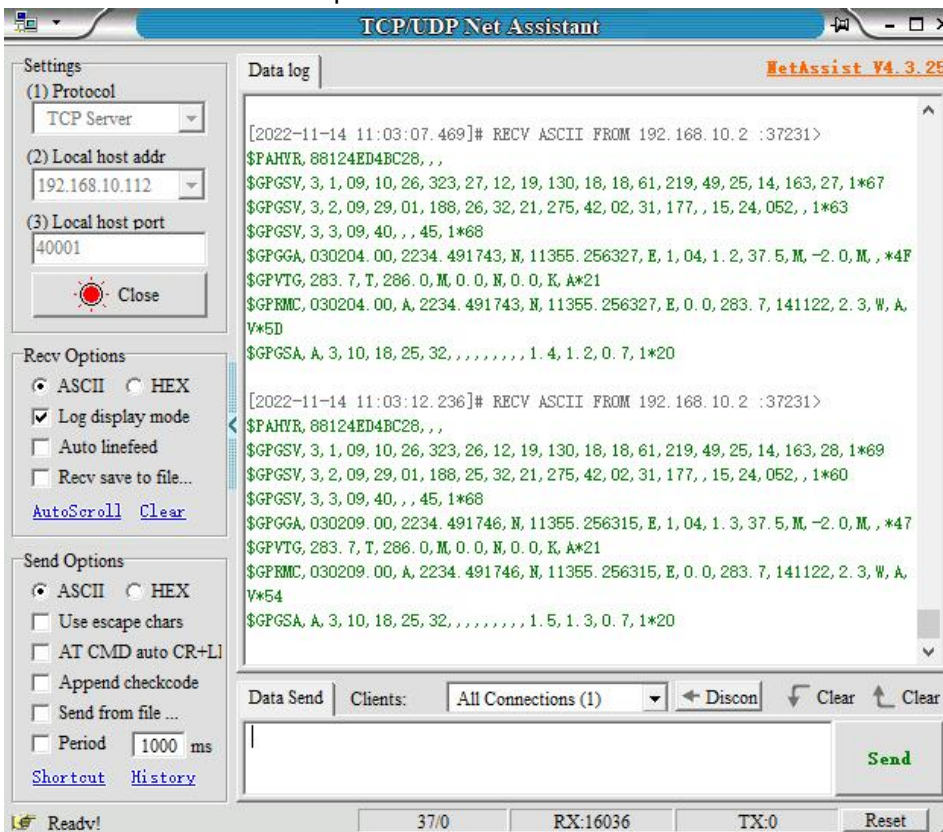
Registration Packet: Disable

Prefix of frame: Disable

Suffix of frame: Disable

Rx/Tx: 0/7408

Receive GPS data in transparent TCP server.



GPS Server mode

Configure TCP server local port and GPS data interval. You may custom GPS data as requested such router's ID, GPS data prefix and so on.

Local Server

Protocol

Port

Report Interval

Max Connections

Device ID

Username

Verification Code

Report NMEA Header

Registration Packet

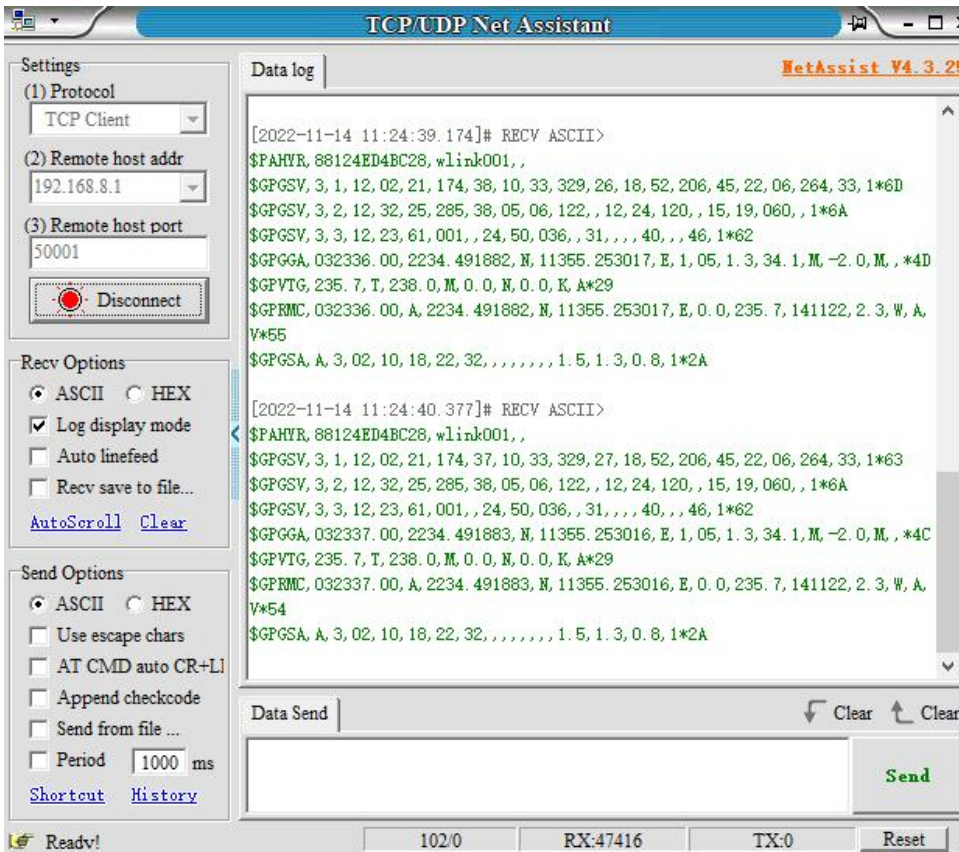
Prefix of frame

Suffix of frame

Connections List

Clients(1)			
Peer	Connection	Tx	Rx
192.168.8.100:61606	Online	10024	0

Receive GPS data in transparent TCP Client.



4.6 Remote IO

Click Application-->Remote IO GUI.

Application > Remote IO

Current IO Status g1=00;g2=01;

G1

G2

SMS Monitoring Center

Center Number

Center2 Number

Center3 Number

Client

Client2

1) TCP Login Data format

macid=88124ED18010;id=wlink0001;user=test;vcode=123456;

Network

Wireless

Station Control

Application

System

Device

Configure

Software

Password

Web Server

Telnet Server

SSH Server

Manage Server

Auto Reboot

LED/IO Control

IO Control Center

Server

Protocol

Port

Device ID

Username

Verification Code

Connection Status connecting

Rx/Tx 0/55

MQTT Server

2) GPIO Value Format

g1=11;g2=10

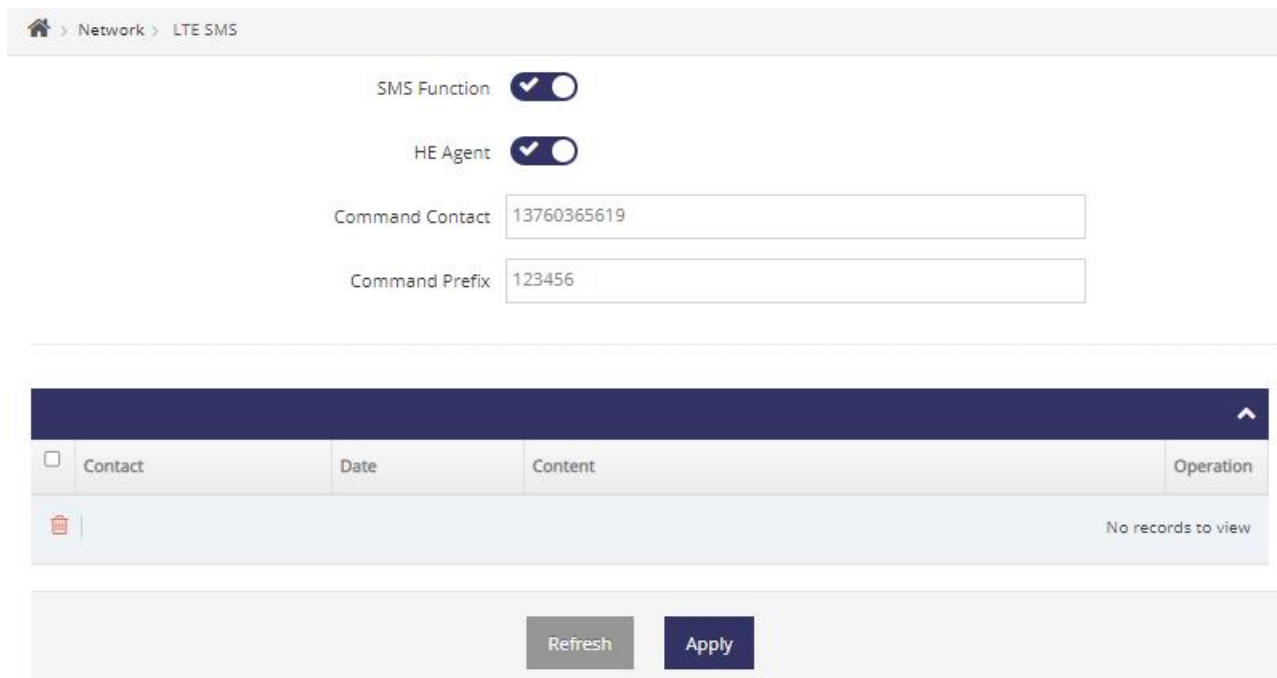
Item	Value	Indication
------	-------	------------

GPIO number	g1	g1 for GPIO1 port g2 for GPIO2 port g3 for G3 port(Reserved)
First Digit	1	Output(DO)
	0	Input(DI)
Second Digit	1	High Level(3.3v)
	0	Low Level(0v)
Separator sign	;	

3) SMS Control and Report

➤ SMS Control

Network---> LTE SMS to enable SMS function and configure the Contact phone number and command prefix code. The router will implement the command from the configured contact phone number and ignore other phone number command.



The SMS command lists as following.

Inquiry Items	SMS Command	SMS ACK	Note
G1 output high level	12345io>agent.modify[g1=11]	g1=11;g2=01;	
G1 input high level	12345io>agent.modify[g1=01]	g1=01;g2=01;	
G1 output low level	12345io>agent.modify[g1=10]	g1=10;g2=01;	
G1 input low level	12345io>agent.modify[g1=00]	g1=00;g2=01;	
G2 output high level	12345io>agent.modify[g2=11]	g1=00;g2=11;	
G2 output low level	12345io>agent.modify[g2=10]	g1=00;g2=10;	

➤ SMS Report

Home > Application > Remote IO

Current IO Status g1=00;g2=01;

G1

G2

SMS Monitoring Center

Center Number

Center2 Number

Center3 Number

Client

Client2

Refresh

Apply

G1 and G2 as DI mode

G1 port from low level to high level, it will trigger report as g1=01;g2=01;

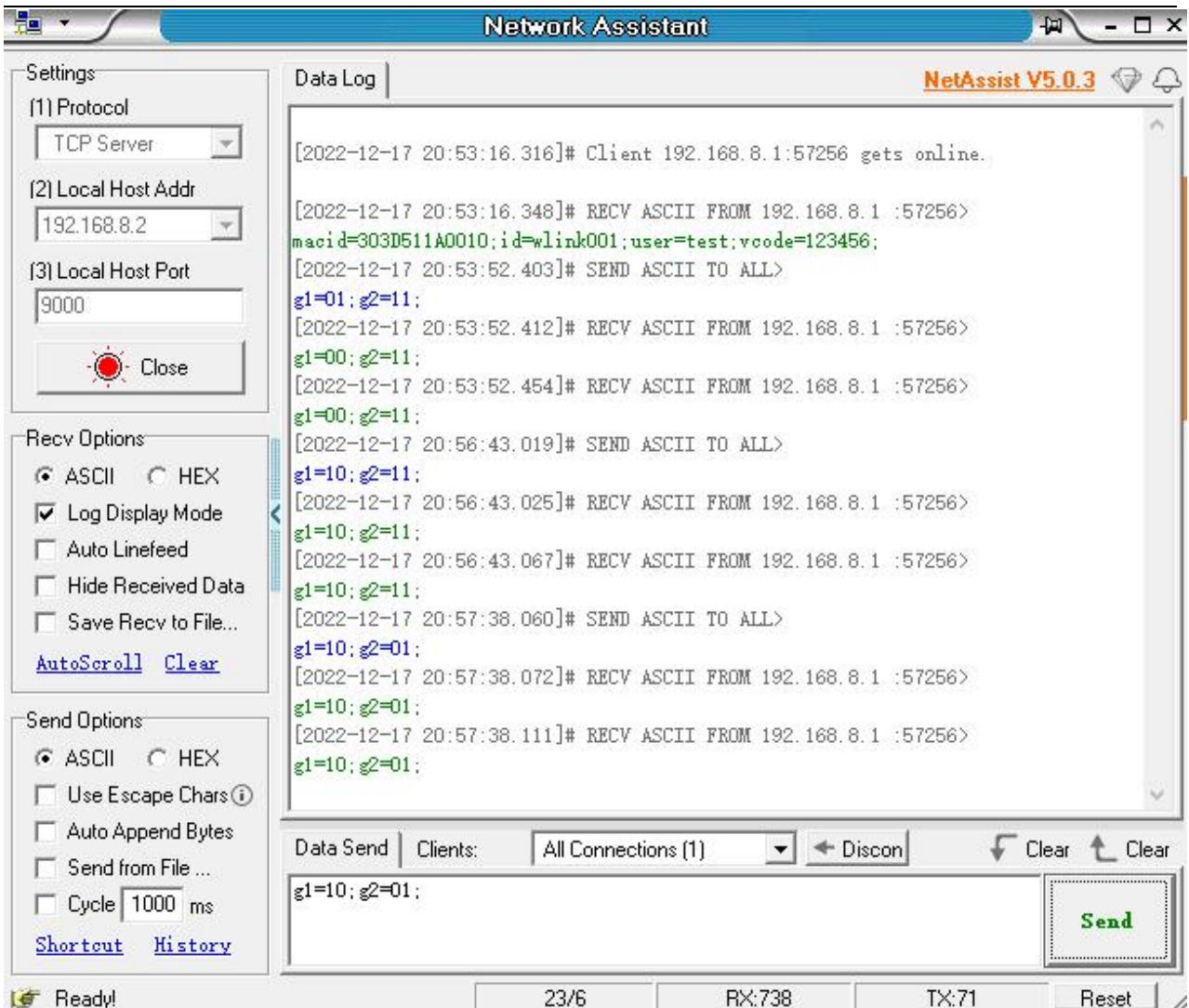
G1 port from high level to low level, it will trigger report as g1=00;g2=01;

G2 port from low level to high level, it will trigger report as g1=00;g2=01;

G2 port from high level to low level, it will trigger report as g1=00;g2=00;

4) TCP Server Demo

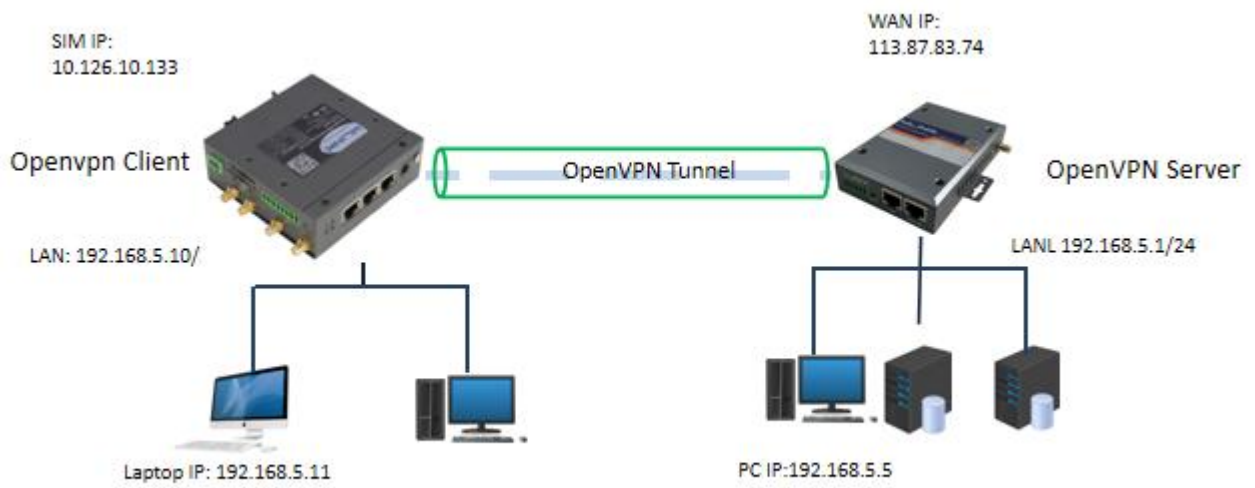
g1=10;g2=01;



Current IO Status g1=10;g2=01;

4.7 OpenVPN(TAP Mode)

OpenVPN two peers subnet IP addressed are in the same IP segment.



Configure Openvpn client according to OpenVPN server.

Topology	Subnet	▼
Server Address	113.87.83.74	
Device	TAP	▼
Protocol	UDP	▼
Port	1194	
Cipher	BF-CBC	▼
LZO Compress	Adaptive	▼
Auth Type	Certificate	▼
HMAC Signature Check	Disable	▼
Keepalive Interval(sec)	10	
Keepalive Timeout(sec)	120	
OpenVPN Custom Options(Separated by semicolons)	<input type="text"/>	

Upload OpenVPN certificate key as OpenVPN server provided.

Certificate Authority(CA)	<input type="button" value="⬇️"/> No File	<input type="button" value="Choose"/>	<input type="button" value="Download"/>	<input type="button" value="Delete"/>
Client Certificate	<input type="button" value="⬇️"/> No File	<input type="button" value="Choose"/>	<input type="button" value="Download"/>	<input type="button" value="Delete"/>
Client Private Key	<input type="button" value="⬇️"/> No File	<input type="button" value="Choose"/>	<input type="button" value="Download"/>	<input type="button" value="Delete"/>

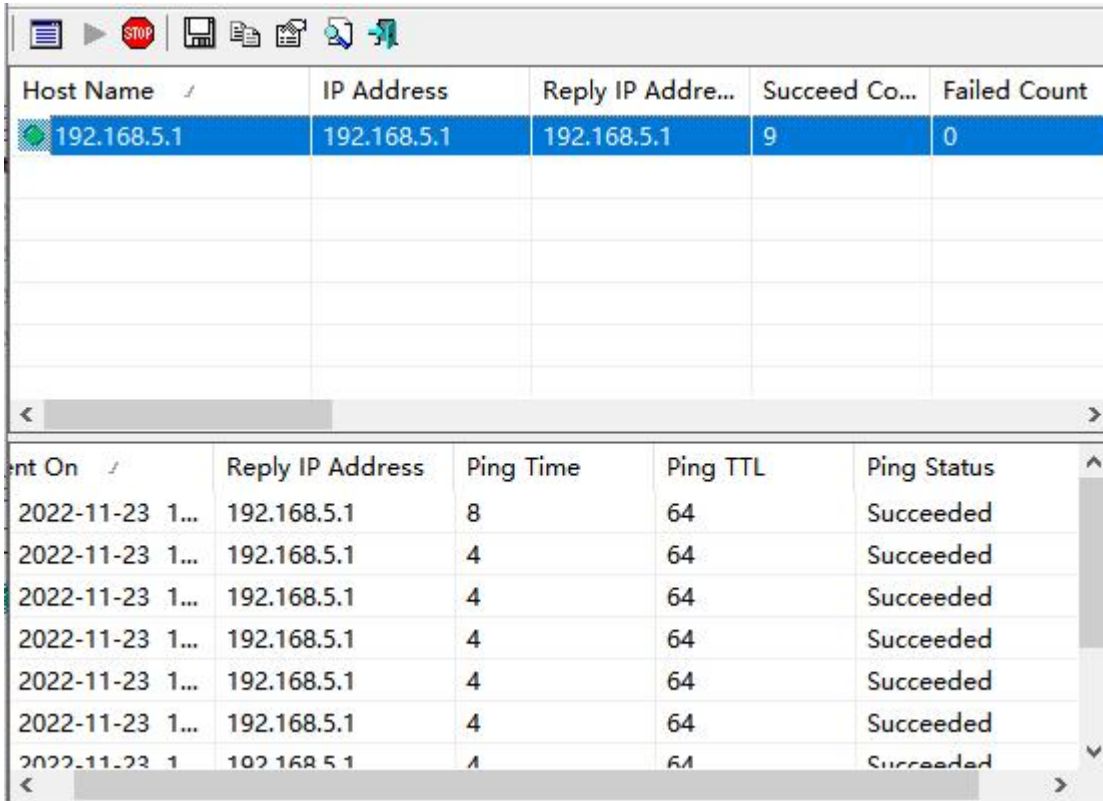
OpenVPN Status

OpenVPN client will be assigned the same segment IP address from OpenVPN server.

Status

Connection Status	Online 	Server IP Address	113.87.83.74
Local IP Address	192.168.5.3	Remote IP Address	192.168.5.3
Subnet Mask	255.255.255.0	Gateway	192.168.5.1
DNS		DNS2	
Rx/Tx(byte)	474291/13493727	Live Time	13:52:09:0

Ping Testing from laptop 192.168.5.11 to OpenVPN server 192.168.5.1



Host Name	IP Address	Reply IP Address...	Succeed Co...	Failed Count
192.168.5.1	192.168.5.1	192.168.5.1	9	0

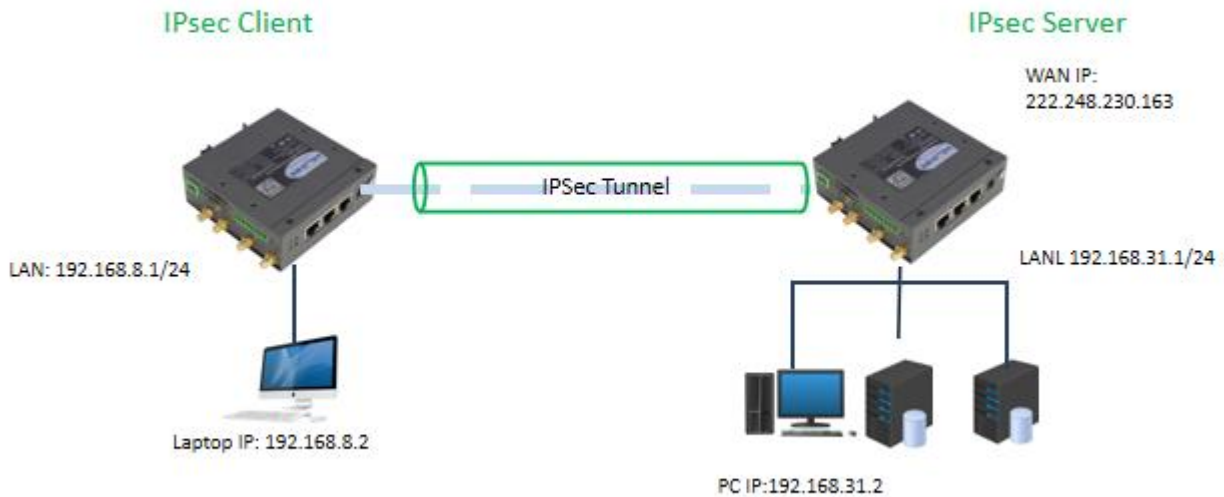
Time	Reply IP Address	Ping Time	Ping TTL	Ping Status
2022-11-23 1...	192.168.5.1	8	64	Succeeded
2022-11-23 1...	192.168.5.1	4	64	Succeeded
2022-11-23 1...	192.168.5.1	4	64	Succeeded
2022-11-23 1...	192.168.5.1	4	64	Succeeded
2022-11-23 1...	192.168.5.1	4	64	Succeeded
2022-11-23 1...	192.168.5.1	4	64	Succeeded
2022-11-23 1...	192.168.5.1	4	64	Succeeded

Ping Testing from laptop 192.168.5.11 to OpenVPN subnet PC 192.168.5.5

Host Name	IP Address	Reply IP Address...	Succeed Co...	Failed Count
DESKTOP-2B1QVF7	192.168.5.5	192.168.5.5	8	0

Sent On	Reply IP Address	Ping Time	Ping TTL	Ping Status
2022-11-23 1...	192.168.5.5	51	128	Succeeded
2022-11-23 1...	192.168.5.5	5	128	Succeeded
2022-11-23 1...	192.168.5.5	4	128	Succeeded
2022-11-23 1...	192.168.5.5	4	128	Succeeded
2022-11-23 1...	192.168.5.5	4	128	Succeeded
2022-11-23 1...	192.168.5.5	5	128	Succeeded
2022-11-23 1...	192.168.5.5	4	128	Succeeded

4.8 IPsec Setting



4.8.1 IPsec Server Mode

The router will run IPsec as server mode when didn't configure peer address.

IPSec Tunnel Table						
<input type="checkbox"/>	Name	Status	Local <-> Peer	Local Network <-> Peer Network	Encryption	Rx/Tx(byte)
<input type="checkbox"/>	connect	Online	222.248.230.163 <-> 183.9.202.143	192.168.31.0/24 <-> 192.168.8.0/24	3DES_CBC/HMAC_MD5_96	0B / 0B

View 1 - 1 of 1

Peer Address

Peer Network

Peer Network Mask

Peer Identify Type

Local Identify Type

Aggressive Mode

Password

IKE Version

IKE Authentication

IKE Encrypt

IKE DH Group

IKE Lifetime

IPSEC Protocol

IPSEC Authentication

IPSEC Encrypt

IPSEC DH Group

IPSEC Lifetime

DPD Type

DPD Delay

DPD Timeout

Configure Options

We can check IPsec Tunnel list in the table.

IPSEC Client

IPSec Tunnel Table						
Name	Status	Local <-> Peer	Local Network <-> Peer Network	Encryption	Rx/Tx(byte)	
connect	Online	222.248.230.163 <-> 119.143.94.109	192.168.31.0/24 <-> 192.168.8.0/24	3DES_CBC/HMAC_MD5_96	840B / 840B	

View 1 - 1 of 1

4.8.2 IPsec Client Mode

- Utilization
- Interface
- Network
- VPN
 - IPSEC Connection
 - OpenVPN client
 - OpenVPN Server
 - L2TP Client
 - PPTP Client
 - GRE Tunnel
- Wireless
- Station
- Application
- System
- Debug
- Development

IPSEC Client

Connection Status	Online	Peer Address	222.248.230.163
Local <-> Peer	10.7.72.2<=>222.248.230.163	Local Network <-> Peer Network	192.168.8.0/24<=>192.168.31.0/24
Online Time	50 minutes ago	Rx/Tx(byte)	0/0

Peer Address

Peer Network

Peer Network Mask

Peer Identify Type

Local Identify Type

Aggressive Mode

Password

IKE Version

IKE Authentication

IKE Encrypt

IKE DH Group

IKE Lifetime

IKE Encrypt

IKE DH Group

IKE Lifetime

IPSEC Protocol

IPSEC Authentication

IPSEC Encrypt

IPSEC DH Group

IPSEC Lifetime

DPD Type

DPD Delay

DPD Timeout

Configure Options

IPsec Status

VPN > IPSEC Connection

IPSEC Client

Connection Status	Online	Peer Address	222.248.230.163
Local <-> Peer	10.15.91.48<=>222.248.230.163	Local Network <-> Peer Network	192.168.8.0/24<=>192.168.31.0/24
Online Time	57 seconds ago	Rx/Tx(byte)	504/504

Ping Server Subnet Testing

Home > Debug > Diagnostic

Address

Address

Close before leave

```

PING 192.168.31.1 (192.168.31.1): 56 data bytes
64 bytes from 192.168.31.1: seq=0 ttl=64 time=58.249 ms
64 bytes from 192.168.31.1: seq=1 ttl=64 time=99.115 ms
64 bytes from 192.168.31.1: seq=2 ttl=64 time=73.983 ms
64 bytes from 192.168.31.1: seq=3 ttl=64 time=69.955 ms
64 bytes from 192.168.31.1: seq=4 ttl=64 time=47.336 ms
    
```

4.9 Station Setting

1) Allow one Station device IP address 192.168.8.250 to access to destination IP 163.177.151.109, TCP protocol and port 80.

Add Record ✕

Rule Name

Source

Type ▼

Action ▼

Dest&Domain&Keyword

Dest Port

Time Settings ▼

2) Refuse one Station device MAC address 00:E0:4C:68:17:E8 to access to destination IP 163.177.151.109, TCP protocol and port 80.

Add Record
✕

Rule Name

Source

Type TCP ▼

Action Drop ▼

Dest&Domain&Keyword

Dest Port

Time Settings Disable ▼

Submit
Cancel



NOTE

- Configure device MAC if need to limit only one device in the LAN.
- Configure device IP address if need to limit only one device in the LAN.
- Configure multiple devices IP addresses with comma(,) as separator if need to limit multiple devices in the LAN.
- Configure IP segment from start address to end address if limit devices with successive IP addresses.

3) Refuse 192.168.8.250, 192.168.8.224, 192.168.8.100 to access to www.google.com

Add Record
✕

Rule Name

Source

Type Domain ▼

Action Drop ▼

Dest&Domain&Keyword

Time Settings Disable ▼

Submit
Cancel

4) Refuse those IP address from 192.168.8.250 to 192.168.8.254 to access to www.google.com

Add Record ✕

Rule Name	<input type="text" value="3"/>
Source	<input type="text" value="192.168.8.250-192.168.8"/>
Type	<input type="text" value="Domain"/>
Action	<input type="text" value="Drop"/>
Dest&Domain&Keyword	<input type="text" value="www.google.com"/>
Time Settings	<input type="text" value="Disable"/>

5) It will accept/drop the whitelist/blacklist.