WLINK

User Manual

---Apply to WL-R130 Series 4G/3G Router

V1.0
http://www.wlink-tech.com
Jan, 2024

Copyright © Shenzhen WLINK Technology Company Limited 2012 ～ 2024

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.

Important Notice

Due to the nature of cellular/wireless communications, transmission and reception of data can never be guaranteed, Especially the cellular signal quality is not good on the site. Data may be delayed, corrupted (i.e., have errors) or be totally lost, WLINK accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data. Wlink accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data.

Furthermore, 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.

Safety Precautions

- The router generates radio frequency (RF) power. When using the router, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Don't use the router in places where cellular products are prohibited.
- Make sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance,etc.
- Make sure plug an available SIM card in the router. Don't power on the router without SIM card for long time if router worked on 5G/4G mode.
- An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router.
- Always keep the antenna with minimum safety distance of 30 cm or more from human body. Do not put the antenna inside metal box, containers, etc.

Various Signs

The manual also uses a variety of eye-catching signs to indicate the places to which special attention should be paid in operation. The significance of these signs are as follows.

CAUTION	Caution indication, used to reminder and warning during product operation and testing.
NOTE	Note indication, use to complement the additional descriptions.
Configuration Instance	Configuration instance indication, use to show configuration instance as reference.

Version History

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

Data	Document Version	Firmware Version	Description
2024-1-5	V1.0	Rm.0.2.5-240105-152307.bin	Released.

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

Contents

1 Overview 6

1.1 Key Features 6

1.2 Specifications 6

2 Hardware Introduction 9

2.1 WL-R130 Panel 9

2.2 Dimension 10

2.3 LED Indicator 10

2.4 Ethernet Connection 11

2.5 Serial Port Connection 11

2.6 Power Supply 11

2.7 Review 11

3 Router Configuration 13

3.1 Local Configure 13

3.2 Status 14

3.3 Overview 14

3.4 Traffic Stats. 15

3.5 Device List 15

3.6 Tool Column 15

3.7 Basic Network 18

3.8 WLAN Setting 27

3.9 Advanced Network Setting 29

3.10 Firewall 38

3.11 VPN Tunnel 40

3.12 Administration 56

4 Configuration Instance 64

4.1 VLAN 64

4.2 WAN Backup (WAN as Main, Cellular Backup) 66

4.3 Port Forwarding 68

4.4 Port Redirecting 69

4.5 IP Passthrough 70

4.6 GPS Settings 72

4.7 Firewall 75

4.8 VPN Tunnel 76

1 Overview

WLINK R130 is a compact and versatile 4G LTE router router tailored for industrial applications. It is engineered to meet diverse interface requirements, featuring a configuration that includes 1xLAN, 1xRS232, and 1xRS485 ports. The R130 is equipped with a 32-bit industrial grade processor, ruggedized enclosure and powerful internal components to handle temperature extremes, dust and moisture and terminal block for secure power supply, ensuring reliability and efficiency in demanding environments.

The R130 supports a wide range of standard network protocols such as ICMP, TCP, UDP, Telnet, SSH, FTP, HTTP, HTTPS, as well as IPV4 and IPv6, ensuring seamless integration into existing network infrastructures. Additionally, it offers robust VPN support, including PPTP/L2TP, GRE, IPSec, OpenVPN, DMVPN, WireGuard, and Zerotier, providing secure and reliable connectivity options.

With its RS232 and RS485 interfaces, the R130 is an ideal solution for serial communication with Meter/Sensor/Controller, supporting Serial port to IP features, Modbus RTU/TCP protocol, and MQTT protocol uploading.

Especially, the R130 is eSIM supported, making it easier to switch from one carrier to others.

1.1 Key Features

Dual SIM redundancy for continuous cellular connections, supports 2G/3G/4G.
WAN link management: cellular WAN/Ethernet WAN/WLAN WAN backup.
VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE/Wireguard
Supports Modbus router (Modbus RTU/ASCII to Modbus TCP).
Supports GPS (optional), provides real time location and tracking.
Auto reboot via SMS/Timing.
Supports WLINK M2M management platform.
Flexible Management methods: Web/CLI/SNMP/WLINK M2M Platform.
Firmware upgrade via Web/CLI/USB/SMS/WLINK M2M management Platform.
Various interfaces: RS232/RS485/Ethernet.
Wide range input voltages from 7.5 to 32 VDC and extreme operating temperature.

1.2 Specifications

Cellular

Number of antennas: 2

Connector: SMA, female
SIM slot: 2 (3.0V & 1.8V)
Standards: 5G Redcap/ LTE-A/LTE/LTE CAT1
HSPA/WCDMA/UMTS
EDGE/GPRS

Ethernet Interface

Number of ports: 1x 10/100Mbps
Magnet isolation protection: 1.5 KV

GPS Interface (Optional)

Number of antennas: 1
Connector: SMA Female with 50 ohms impedance
GPS Sensitivity: -160dBm
GPS Accuracy: 2.5m CEP
Update Rate: 1Hz@5Hz
Time to First Fix: Cold Status 27s, Hot status 1s.
Protocol: NMEA-0183 2.3V

Serial Interface

Number of ports: 1xRS232, 1xRS485
Connector: 3.5mm RP female socket
Baud rate: 300bps to 115200bps
RS232: TxD, RxD,GND
RS485: A (Data+), B (Data-), GND

Software (Basic features of WLINKOS)

Network protocols: PPP, TCP, UDP, ICMP, HTTP, HTTPs, DNS, NTP, SMTP, Telnet, SSH2, DDNS, etc.
VPN tunnel: IPsec, OpenVPN, GRE, PPTP/L2TP, Wireguard, Zerotier
Serial port: Transparent, TCP Client/Server, UDP, Modbus RTU
Management: Web, CLI, SMS, WLINK M2M Platform

Consumption

Voltage: DC +7.5~32V (standard 12V/1A power adapter)
SIM/R-UIM Card: 1.8V/3V
Idle: 110mA@+12VDC
Online: 170mA@+12VDC

Other

Galvanized metal with grounding Screw
Dimension: 103mm x 73.5mm x 25.5mm (not including antenna)
Weight: 225g (not including accessories)

Operation temperature: -30~+75℃

Store temperature: -40~+85℃

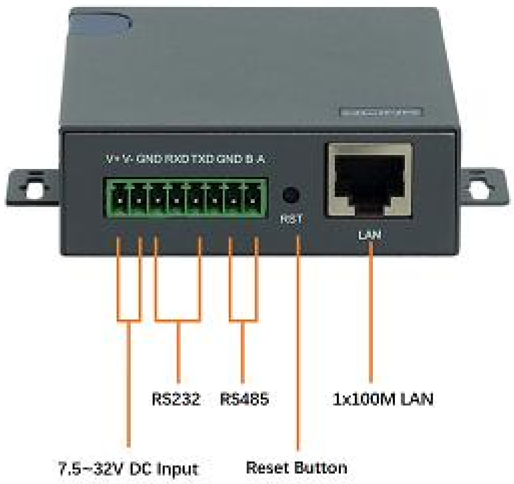
Related humidity: 0~95% (non-condensing)

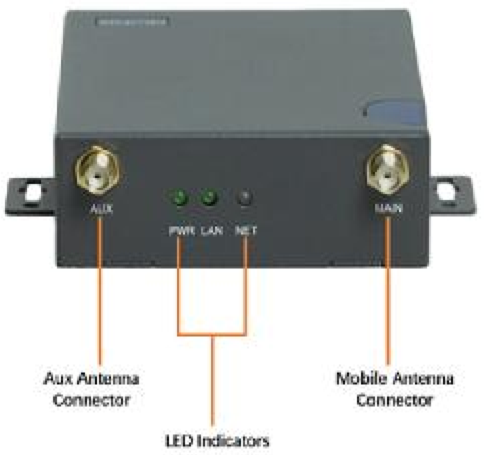
Guarantee: two years

2 Hardware Introduction

This chapter is mainly for hardware 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 WL-R130 Panel

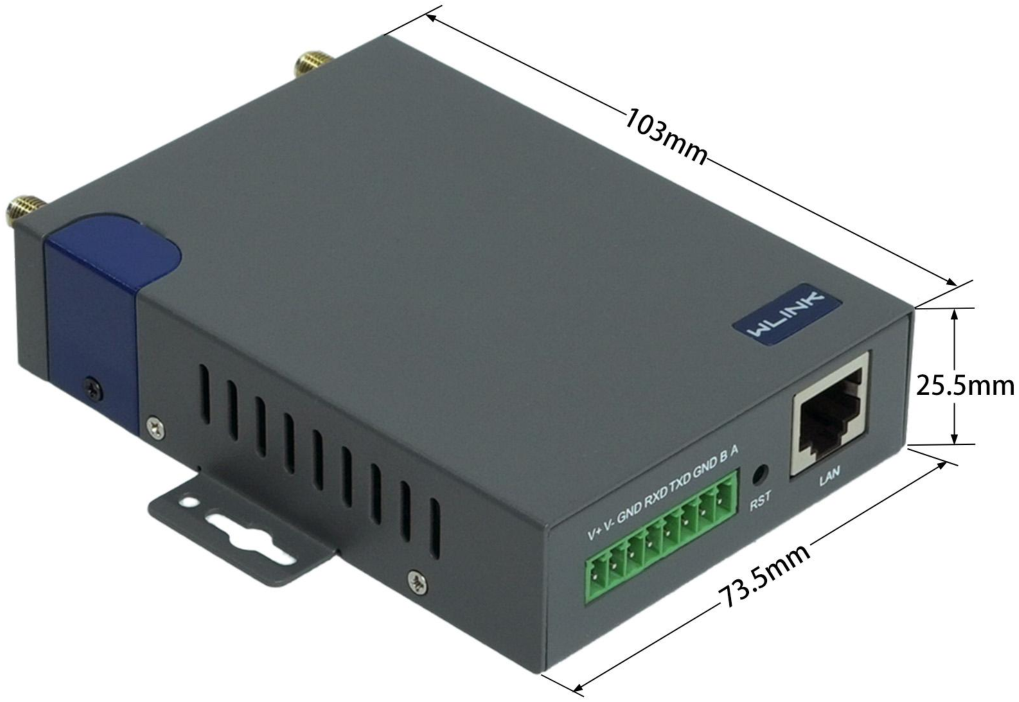

V+ V- GND RXD TXD GND B A
RST
LAN
RS232
RS485
1x100M LAN
7.5~32V DC Input
Reset Button


AUX
PWR LAN NET
MAIN
Aux Antenna Connector
Mobile Antenna Connector
LED Indicators

Interface	Description	Note
Main	4G Main SMA Antenna Connector, 50Ω	
Aux/GPS	4G Aux SMA Antenna Connector, 50Ω.	GPS Optional.
Reset	Reset router to default setting.	Press 5s for Reset
LAN	10/100M Base-TX，MDI/MDIX Self-adaptation	
SIM Cover	Protect SIM cards.	One SIM slot

Terminal Block	8Pin Bock. Power interface, RS232, RS485	Included power interfaces.

2.2 Dimension


103mm
25.5mm
73.5mm
WLINK
V+ V- GND RXD TXD GND B A
RST
LAN

2.3 LED Indicator

silk-screen	color	status	Indication
NET	Red		Pool Signal
	Green		Strong Signal

		Solid light	4G Online
		Slow Blink (1.5s)	3G Online
		Quick Blink (0.5s)	Offline
LAN	Green	Solid light	Plugged
	Green	Blinking	Data Sending
	Green	Dark	Unplugged
PWR	Green	Solid light	Router OS is running.

2.4 Ethernet Connection

Connect an Ethernet cable to the port marked ETH0 or ETH1 at the front of the R130 Router, and connect the other end of the cable to your computer.

2.5 Serial Port Connection

The serial port supports RS232 and RS485 ports as default.The serial port feature supports TCP/UDP client/server as optional, also supports Modbus protocol. You may check the feature in Serial App of Advanced Network UI.

2.6 Power Supply

Voltage input range: +7.5~32VDC.

CAUTION

WL-R130 supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly.

2.7 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

3 Router Configuration

WL-R130 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.

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 192.168.1.1, 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.

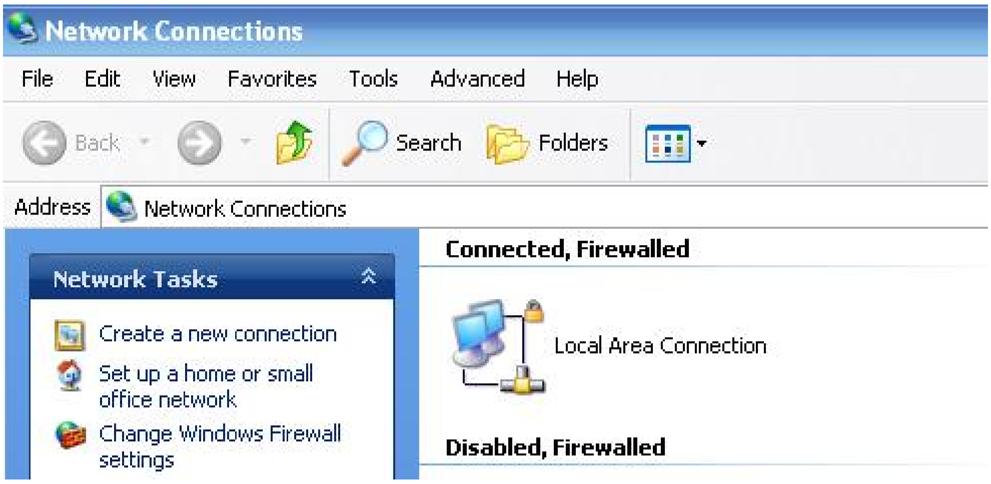
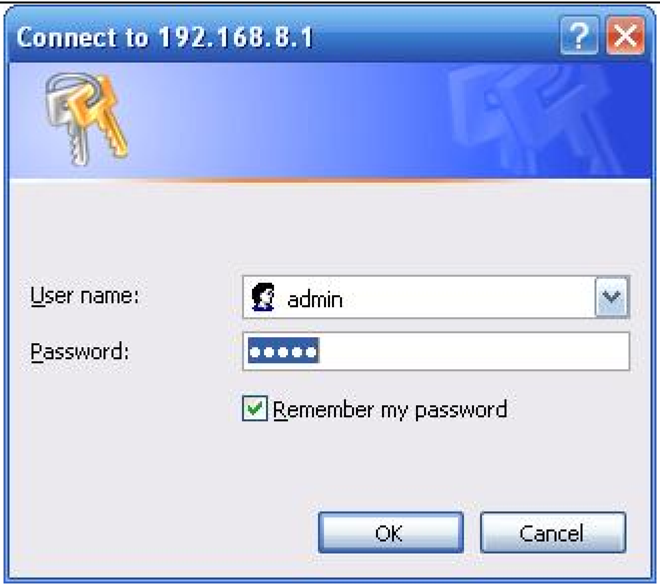

Network Connections
File
Edit
View
Favorites
Tools
Advanced
Help
Back
Search
Folders
Address
Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
Connected, Firewalled
Local Area Connection
Disabled, Firewalled

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


Connect to 192.168.8.1
OK
Cancel

User name: admin

Password: •••••

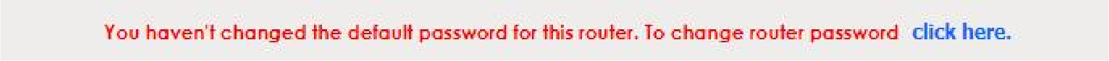
☑ Remember my password

Figure 2-2 User Identify Interface

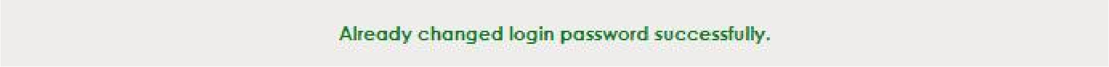
----END

3.2 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.

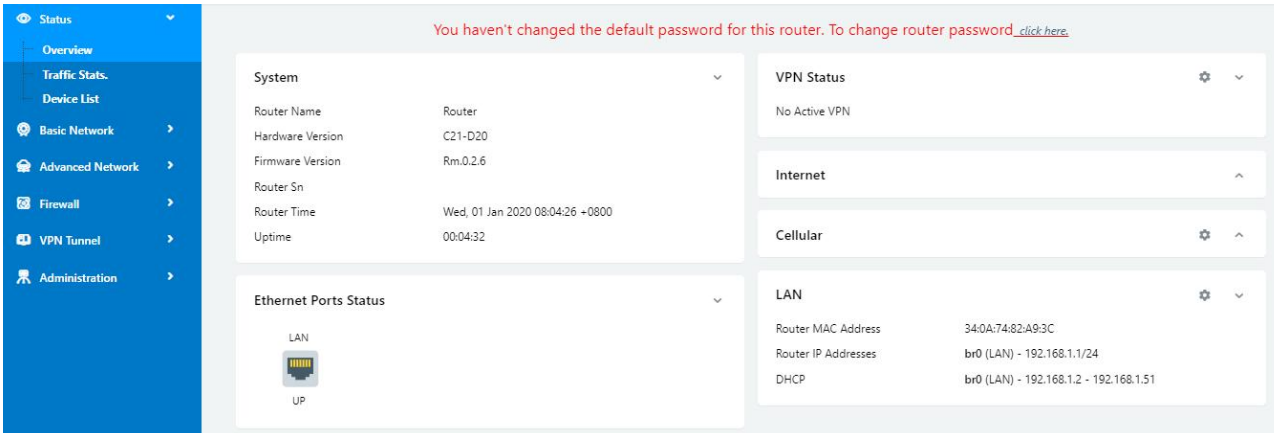

You haven't changed the default password for this router. To change router password click here.

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


Already changed login password successfully.

3.3 Overview

The overview GUI will be display router system information, Ethernet ports status, VPN connection status, LAN information, 4G connection information.


Status
Overview
Traffic Stats.
Device List
Basic Network
Advanced Network
Firewall
VPN Tunnel
Administration
Internet
Cellular
LAN
UP

You haven't changed the default password for this router. To change router password click here.

System

Router Name Router
Hardware Version C21-D20
Firmware Version Rm.0.2.6
Router Sn
Router Time Wed, 01 Jan 2020 08:04:26 +0800
Uptime 00:04:32

VPN Status

No Active VPN

Ethernet Ports Status

LAN

Router MAC Address 34:0A:74:82:A9:3C
Router IP Addresses br0 (LAN) - 192.168.1.1/24
DHCP br0 (LAN) - 192.168.1.2 - 192.168.1.51

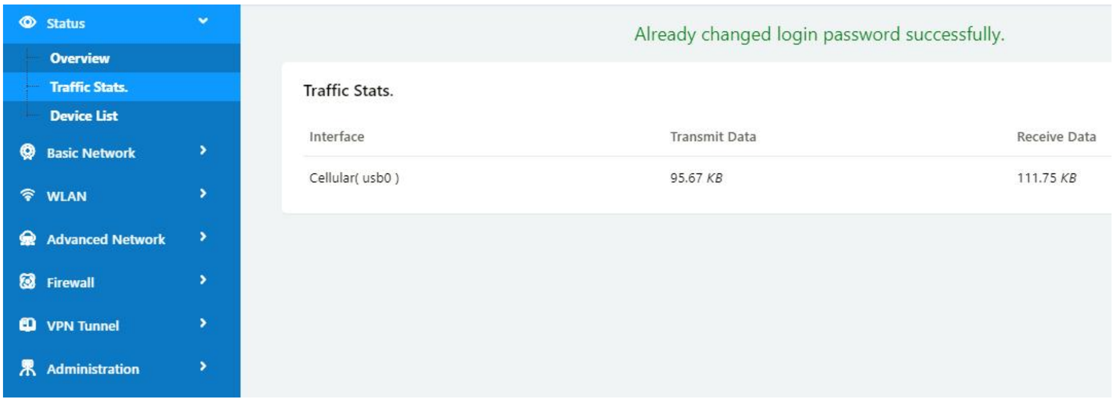
Figure 2-3 Router Status GUI

NOTE

One Ethernet Port Icon for WL-R100 and WL-R130.
Two Ethernet Port Icons for WL-R200 and WL-R210.
Five Ethernet Port Icons for WL-R520.

3.4 Traffic Stats.

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


Status
Overview
Traffic Stats.
Device List
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration

Already changed login password successfully.

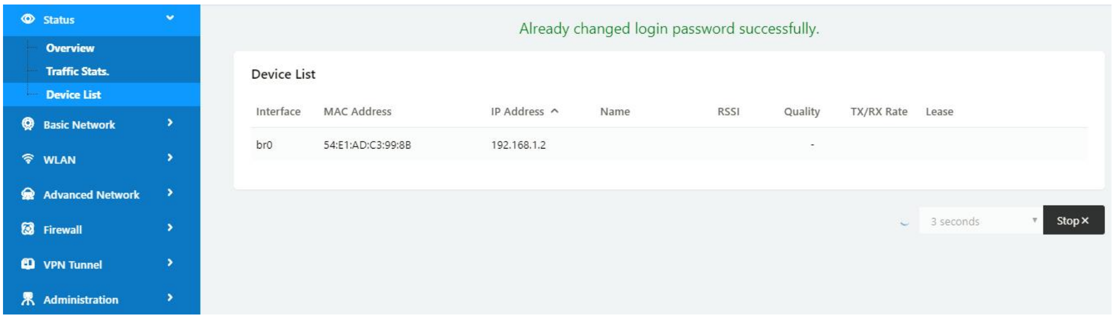
Traffic Stats.

Interface	Transmit Data	Receive Data
Cellular(usb0)	95.67 *KB*	111.75 *KB*

Figure 2-4 Traffic Stats. GUI

3.5 Device List

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


Status
Overview
Traffic Stats.
Device List
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
3 seconds
Stop ×

Already changed login password successfully.

Device List

Interface	MAC Address	IP Address ^	Name	RSSI	Quality	TX/RX Rate	Lease
br0	54:E1:AD:C3:99:8B	192.168.1.2			-		

Figure 2-5 Device List GUI

3.6 Tool Column

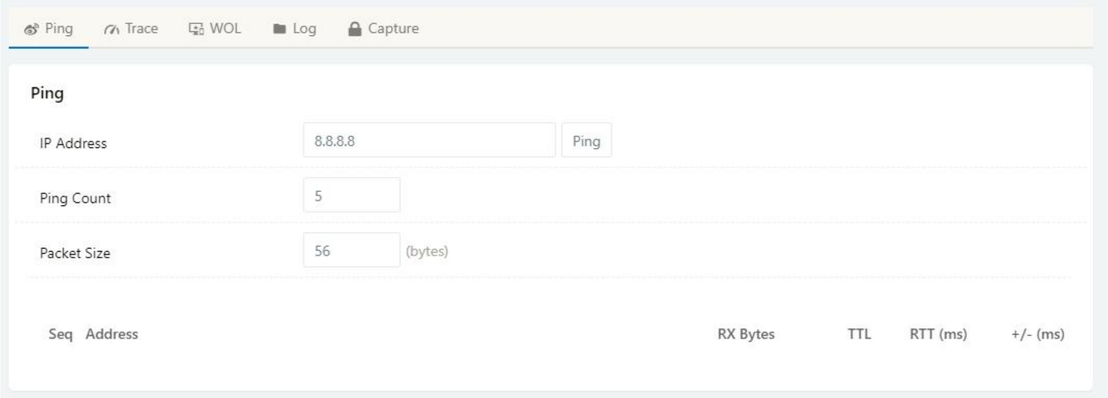
Tools
Bandwidth
IP Traffic
System

Figure 2-6 Tool Column GUI

3.6.1 Tools

3.6.1.1 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.



Ping

IP Address: 8.8.8.8 [Ping]

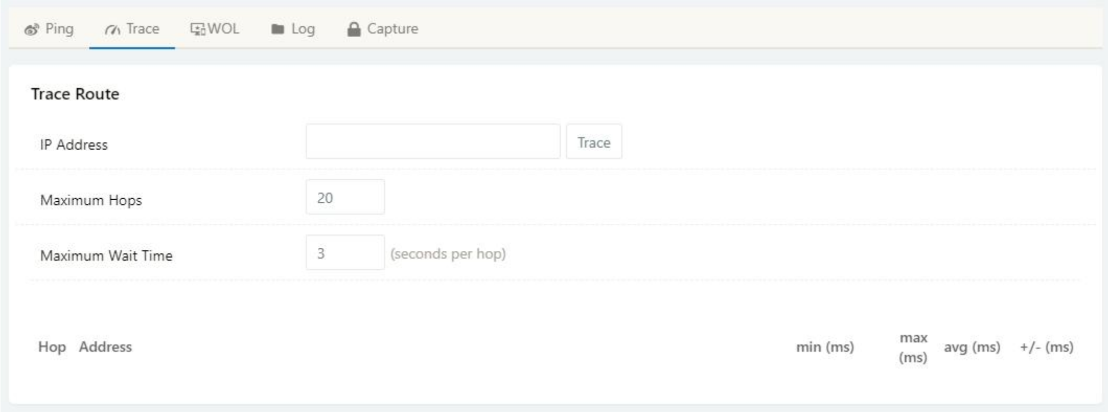
Ping Count: 5

Packet Size: 56 (bytes)

Seq	Address	RX Bytes	TTL	RTT (ms)	+/- (ms)

3.6.1.2 Trace

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



Trace Route

IP Address: [Trace]

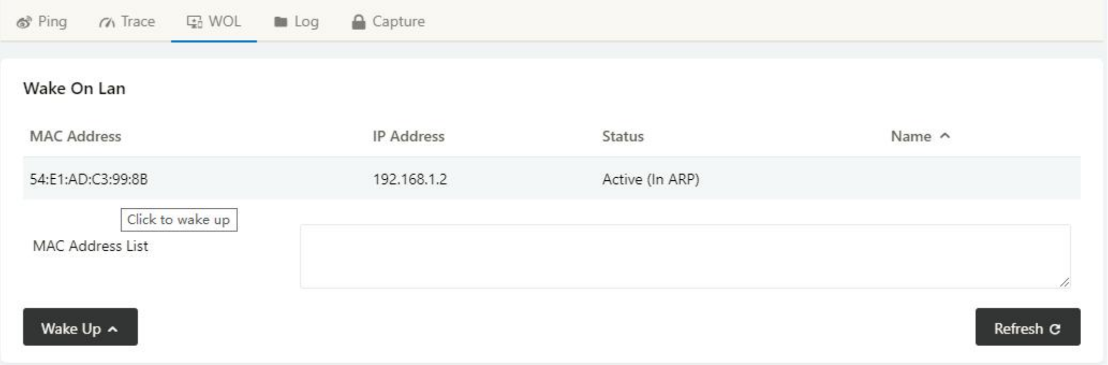
Maximum Hops: 20

Maximum Wait Time: 3 (seconds per hop)

Hop	Address	min (ms)	max (ms)	avg (ms)	+/- (ms)

3.6.1.3 WOL

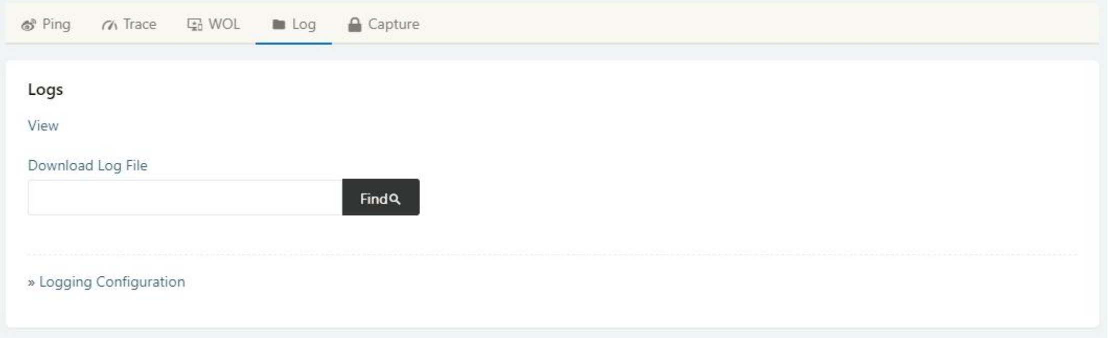
Click Tools-> WOL to enter WOL(Wake On Lan) GUI. Used to wake up those connected devices via WOL protocol. Clock left mouse button to wake up the device.


Ping
Trace
WOL
Log
Capture
Wake On Lan
Click to wake up
MAC Address List
Wake Up
Refresh

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

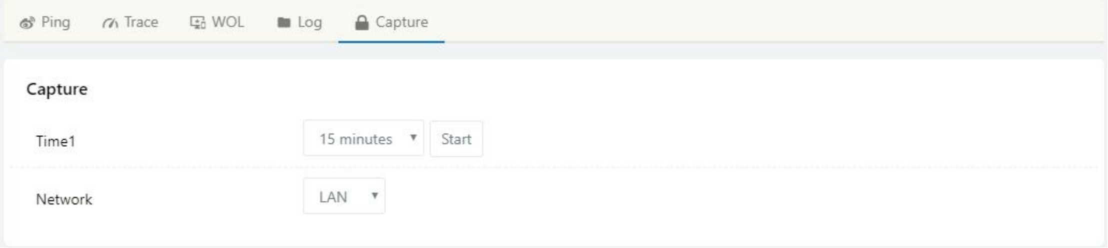
3.6.1.4 Log

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


Ping
Trace
WOL
Log
Capture
Logs
View
Download Log File
Find
» Logging Configuration

3.6.1.5 Capture

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

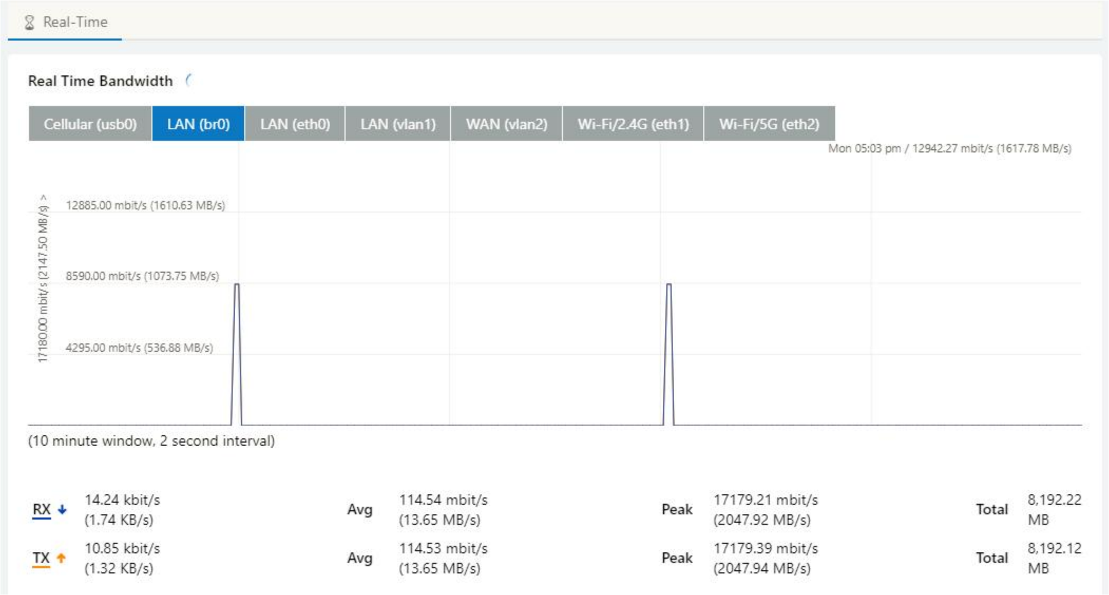

Ping
Trace
WOL
Log
Capture
Capture
Start

Time1: 15 minutes

Network: LAN

3.6.2 Bandwidth

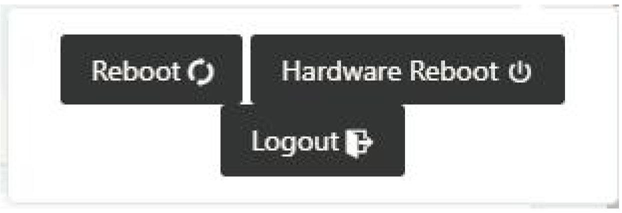
Click Bandwidth to enter bandwidth graphic GUI. Used to check cellular/LAN/Wi-Fi real-time bandwidth.


Real-Time
Real Time Bandwidth
Cellular (usb0)
LAN (br0)
LAN (eth0)
LAN (vlan1)
WAN (vlan2)
Wi-Fi/2.4G (eth1)
Wi-Fi/5G (eth2)
Mon 05:03 pm / 12942.27 mbit/s (1617.78 MB/s)
12885.00 mbit/s (1610.63 MB/s)
8590.00 mbit/s (1073.75 MB/s)
4295.00 mbit/s (536.88 MB/s)
17180.00 mbit/s (2147.50 MB/s)
(10 minute window, 2 second interval)

RX ↓	14.24 kbit/s (1.74 KB/s)	Avg	114.54 mbit/s (13.65 MB/s)	Peak	17179.21 mbit/s (2047.92 MB/s)	Total	8,192.22 MB
TX ↑	10.85 kbit/s (1.32 KB/s)	Avg	114.53 mbit/s (13.65 MB/s)	Peak	17179.39 mbit/s (2047.94 MB/s)	Total	8,192.12 MB

3.6.3 System

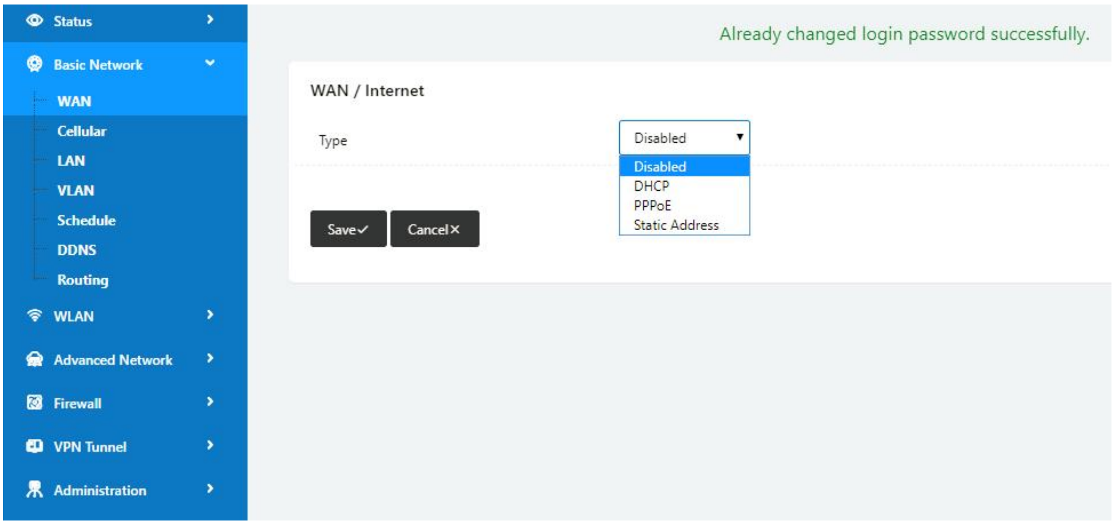
Click system to choose software reboot, hardware reboot and logout GUI.


Reboot
Hardware Reboot
Logout

3.7 Basic Network

3.7.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface.


Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Disabled
DHCP
PPPoE
Static Address
Save
Cancel

Already changed login password successfully.

WAN / Internet

Type: Disabled

Table 2-1 WAN Setting Instruction

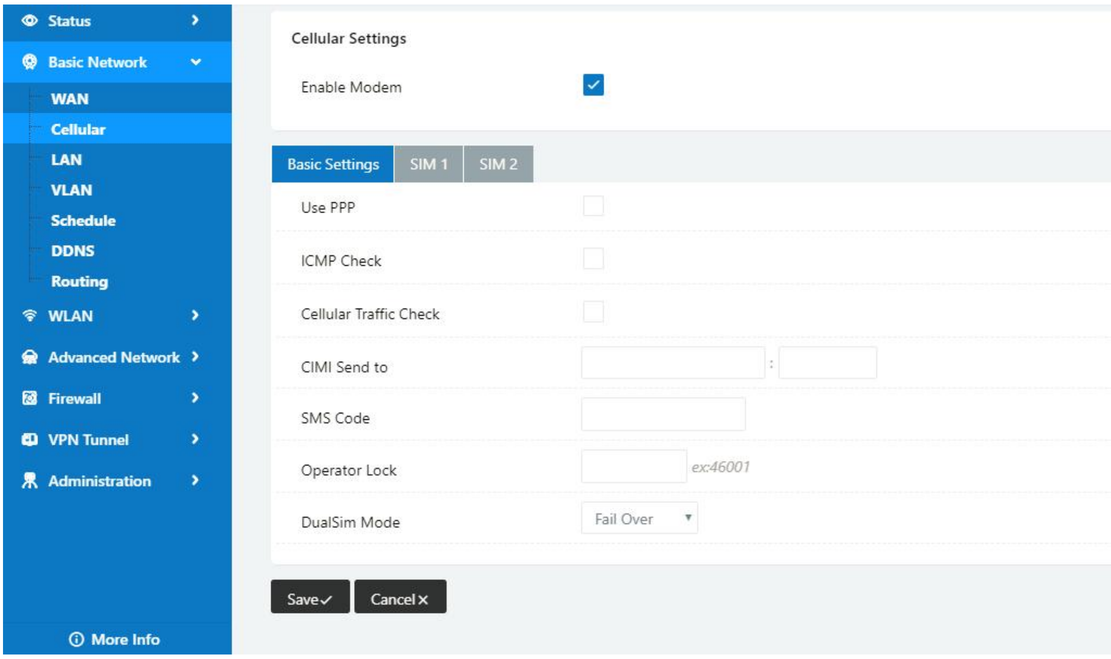
Parameter	Instruction
Type	Support DHCP, PPPoE, Static IP address

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

----End

3.7.2 Cellular Setting

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


Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Basic Settings
SIM 1
SIM 2
Save✓
Cancel✕

Cellular Settings

Enable Modem ☑

Use PPP ☐

ICMP Check ☐

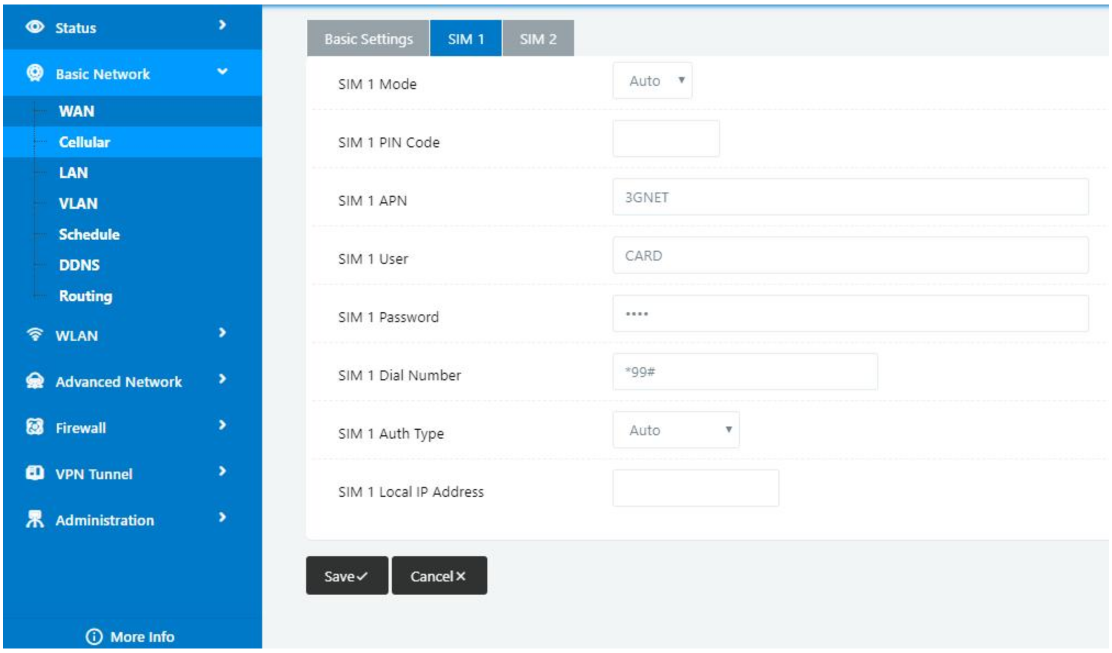
Cellular Traffic Check ☐

CIMI Send to :

SMS Code

Operator Lock ex:46001

DualSim Mode Fail Over


Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Basic Settings
SIM 1
SIM 2
Save✓
Cancel✕

SIM 1 Mode Auto

SIM 1 PIN Code

SIM 1 APN 3GNET

SIM 1 User CARD

SIM 1 Password ••••

SIM 1 Dial Number *99#

SIM 1 Auth Type Auto

SIM 1 Local IP Address

CAUTION

WL-R100 supports single SIM.
WL-R130 supports dual-SIM as default.
WL-R200/R520 supports dual-SIM as optional.
WL-R210 supports dual-SIM as default.
WL-R230 supports dual-SIM as default.

Table 2-2 Cellular Setting Instruction

Parameter	Instruction
Enable Modem	Enable/Disable 4G 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	【Fail Over】Two SIM cards mutual backup. Once SIM1 failed, it'll switch to SIM2 and work on SIM2, and vice versa. 【SIM1 Only】Only SIM1 works. 【SIM2 Only】Only SIM2 works. 【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.
Connect Mode	【Auto】The router will automatically connect to 3G/4G networks and give priority to 4G. 【LTE】Router will connect to 4G only. 【3G】Router will connect to 3G only.
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.

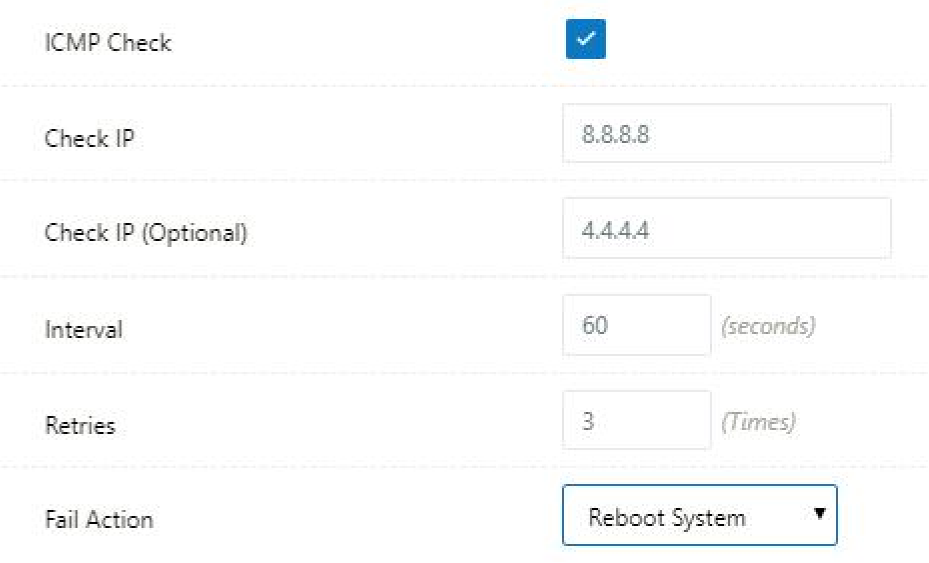
Parameter	Instruction
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth. Type	Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional.
SIM Local IP Address	Fix SIM IP. The feature is available if carrier can provide this service.

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 ☑

Check IP 8.8.8.8

Check IP (Optional) 4.4.4.4

Interval 60 (seconds)

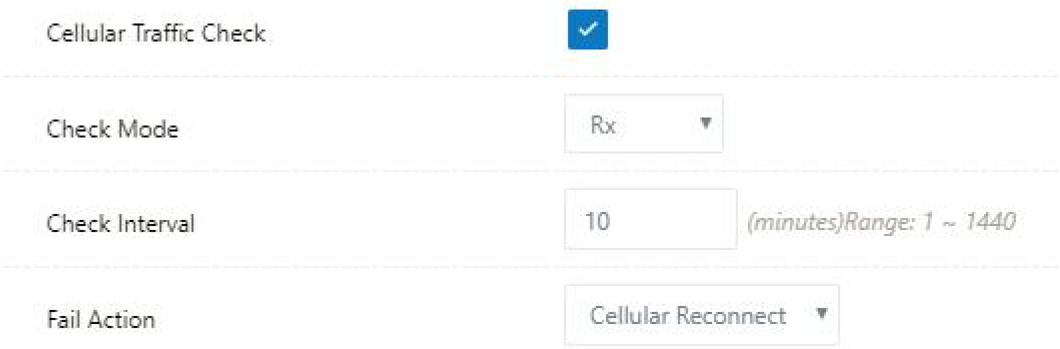
Retries 3 (Times)

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.



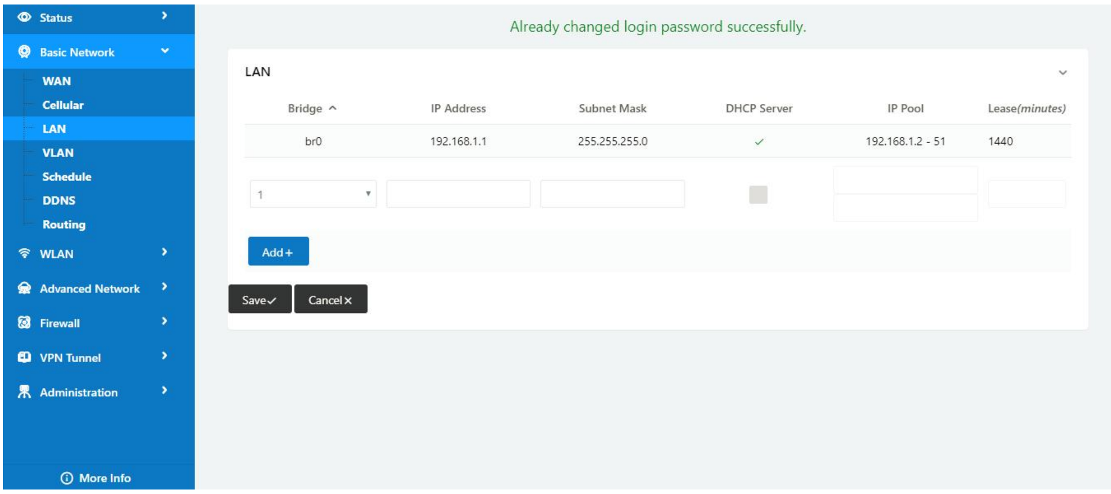
Cellular Traffic Check	☑
Check Mode	Rx
Check Interval	10 (minutes)Range: 1 ~ 1440
Fail Action	Cellular Reconnect

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

----End

3.7.3 LAN Setting

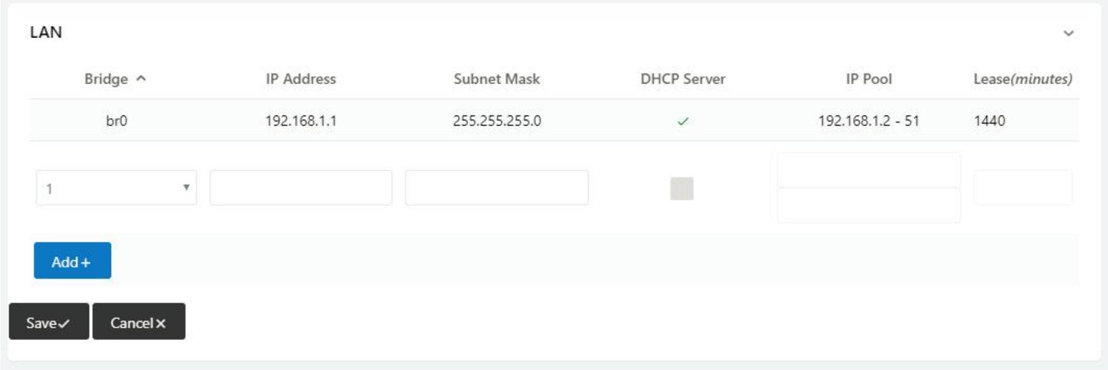
Step 1 Basic Network>LAN to enter below interface


Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Add+
Save✓
Cancel×

Already changed login password successfully.

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


Add+
Save✓
Cancel×

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

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.

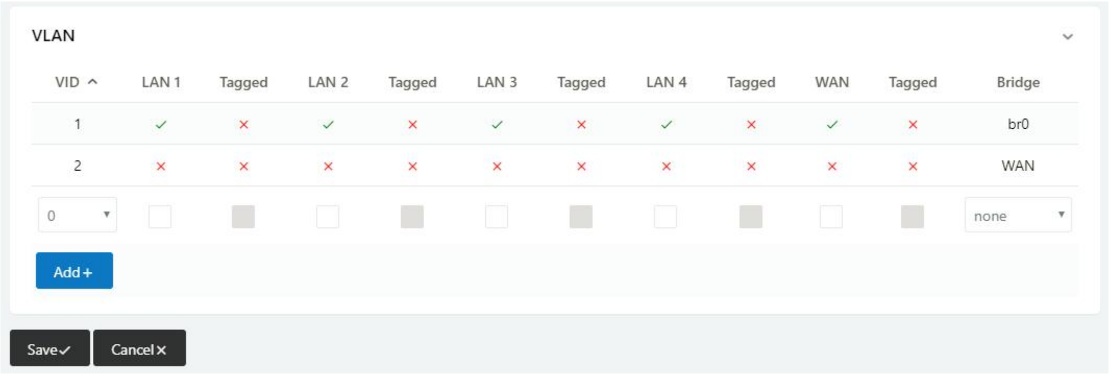
Parameter	Instruction
Router IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease
IP Pool	IP address range within LAN
Lease	The valid 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

3.7.4 VLAN

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



VLAN

VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	br0
2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	WAN
0 ▾	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	none ▾

Table 2-4 LAN Setting Instruction

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

Step 2 Please Click “Save“ to finish.

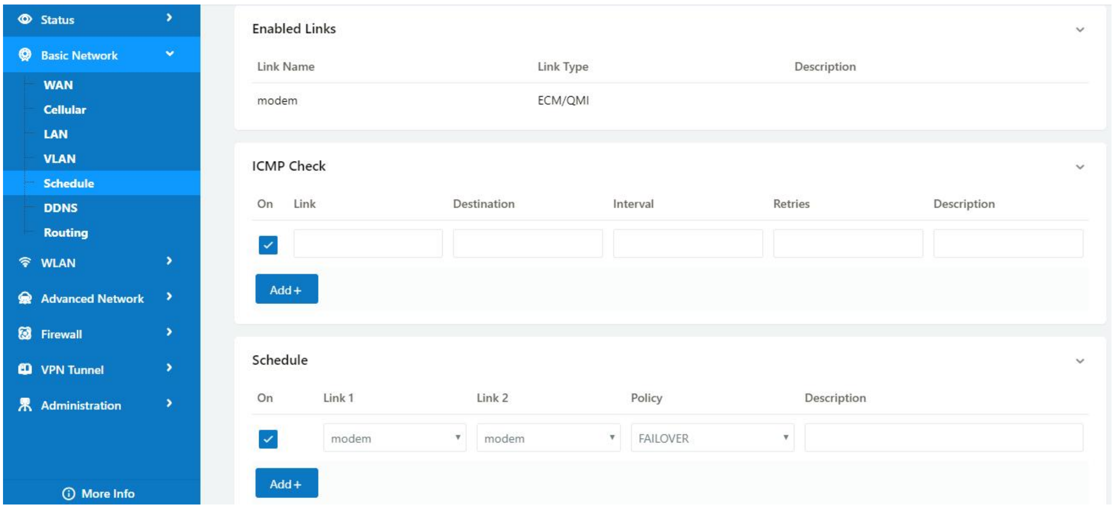
Configuration Instance

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

----End

3.7.5 Schedule

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


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

Enabled Links

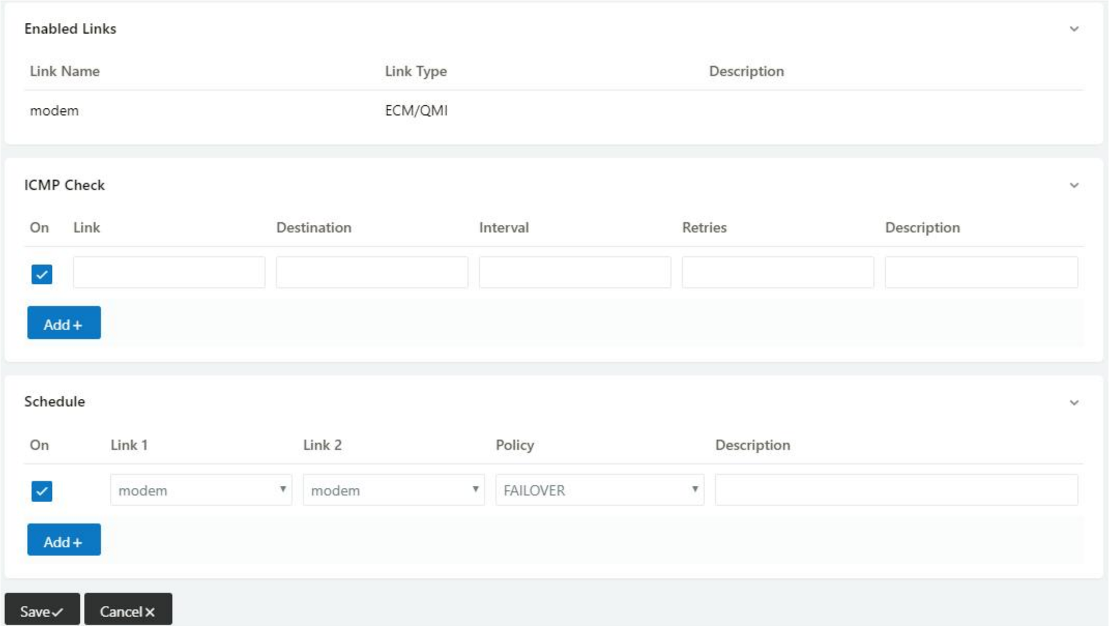
Link Name	Link Type	Description
modem	ECM/QMI	

ICMP Check

On	Link	Destination	Interval	Retries	Description
☑					

Schedule

On	Link 1	Link 2	Policy	Description
☑	modem	modem	FAILOVER	


Add +
Add +
Save✓
Cancel ✕

Enabled Links

Link Name	Link Type	Description
modem	ECM/QMI	

ICMP Check

On	Link	Destination	Interval	Retries	Description
☑					

Schedule

On	Link 1	Link 2	Policy	Description
☑	modem	modem	FAILOVER	

Step 2 Please Click “Save“ to finish.

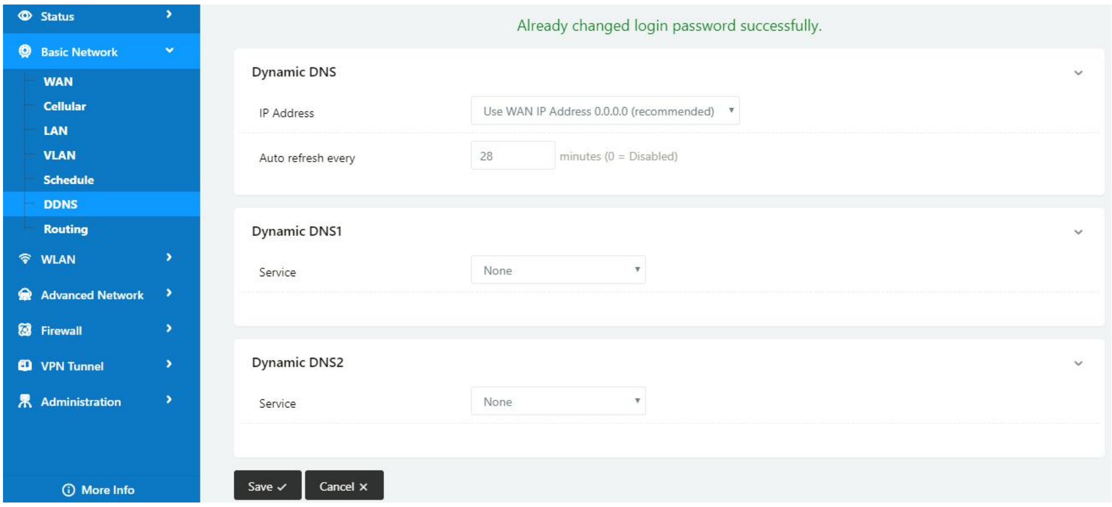
Configuration Instance

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

----End

3.7.6 Dynamic DNS Setting

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


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

Already changed login password successfully.

Dynamic DNS

IP Address: Use WAN IP Address 0.0.0.0 (recommended)

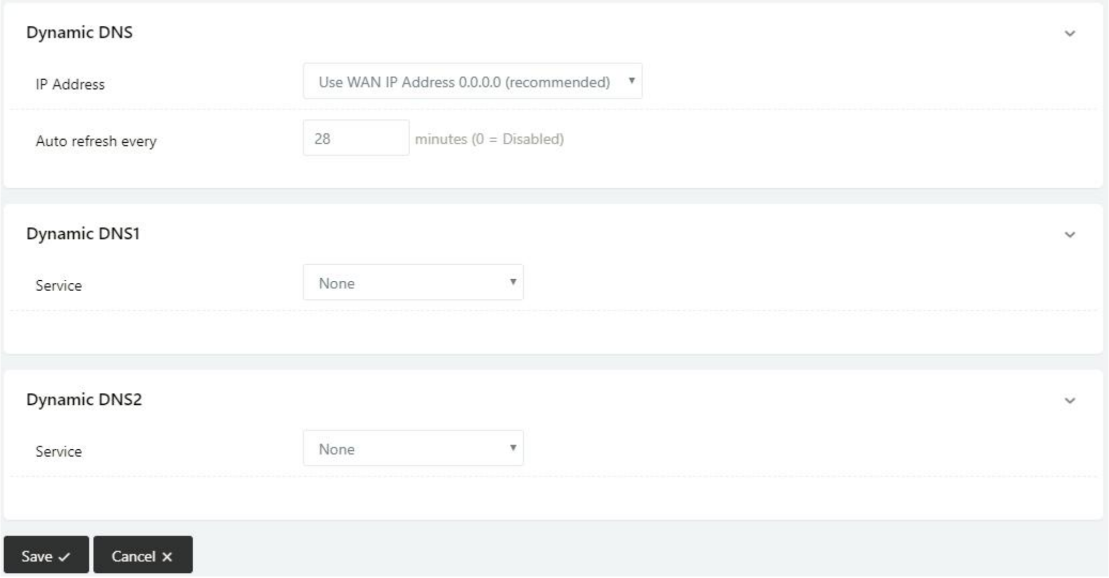
Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None


Save ✓
Cancel ✕

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

Table 2-5 DDNS Setting Instruction

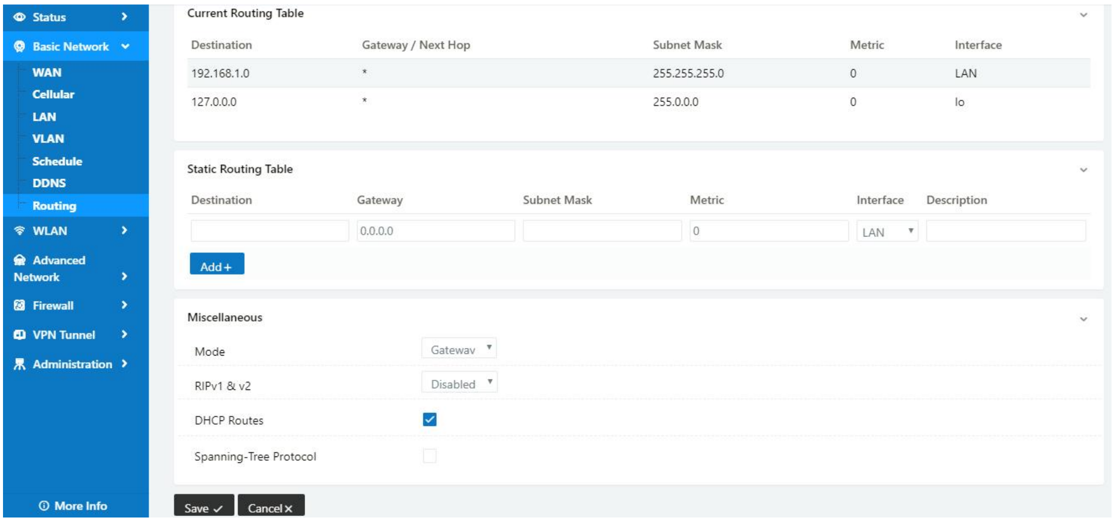
parameter	Instruction
IP address	Default is standard DDNS protocol, for customized protocol, please contact Wlink engineer. Usually, use default IP 0.0.0.0
Auto refresh time	Set the interval of the DDNS client obtains new IP, suggest 240s or above
Service provider	Select the DDNS service provider that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

Step 2 Please Click “Save“ to finish.

----End

3.7.7 Routing Setting

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


Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Add +
Save ✓
Cancel ×

Current Routing Table

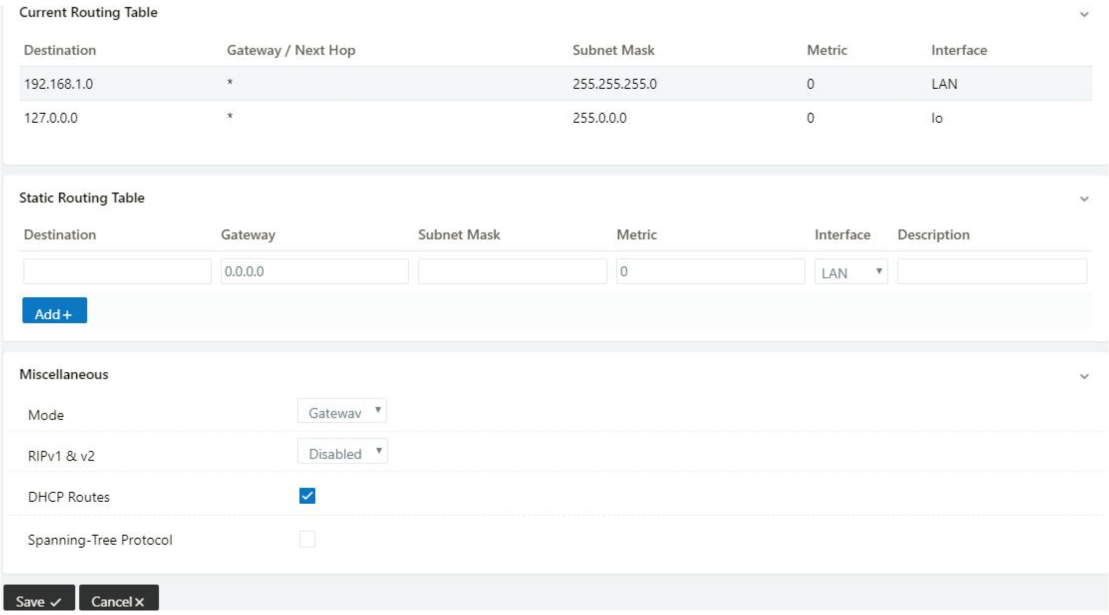
Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
192.168.1.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo

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	☐


Add +
Save ✓
Cancel ×

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	☐

Table 2-6 Routing Setting Instruction

Parameter	Instruction
Destination	Router can reach the destination IP address.
router	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 router.

Parameter	Instruction
Description	Describe this routing name.

Step 2 Please Click “ Save “ to finish.

----End

3.8 WLAN Setting

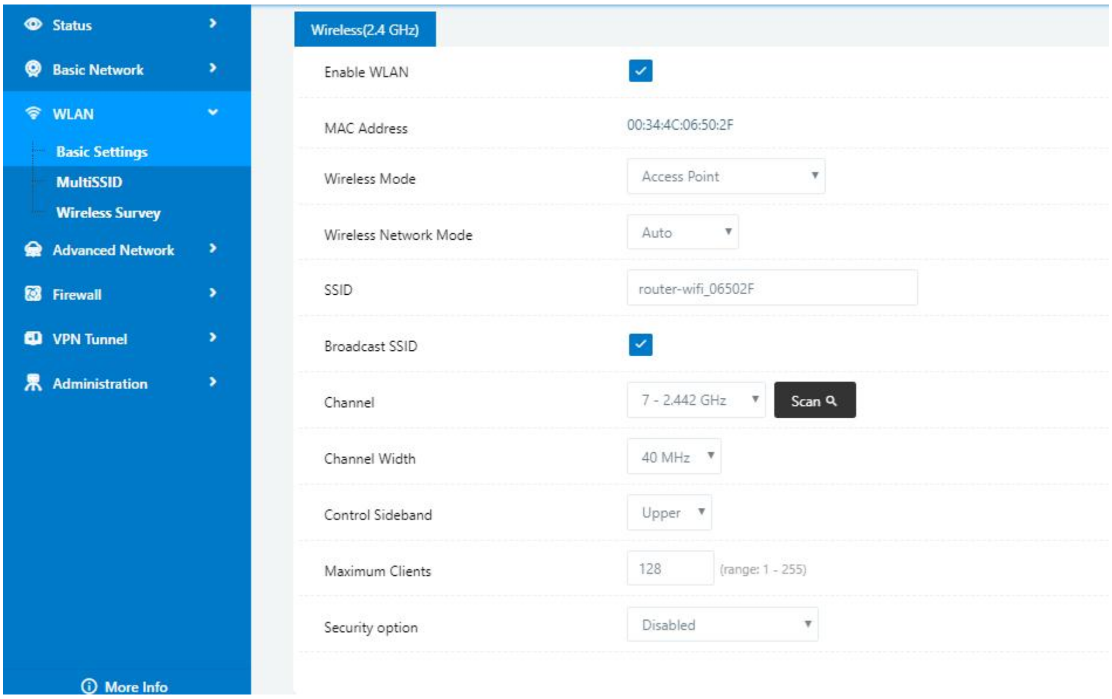
It’s mainly for router which support Wi-Fi, you can modify and configure WLAN parameter through Web GUI, below is the common setting.

CAUTION

WL-R100 doesn’t support Wi-Fi feature.
WL-R200 Wi-Fi feature is optional.
WL-R130/WL-R520 supports Wi-Fi feature as default.

3.8.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter


Status
Basic Network
WLAN
Basic Settings
MultiSSID
Wireless Survey
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Wireless(2.4 GHz)
Scan

Enable WLAN ☑
MAC Address 00:34:4C:06:50:2F
Wireless Mode Access Point
Wireless Network Mode Auto
SSID router-wifi_06502F
Broadcast SSID ☑
Channel 7 - 2.442 GHz
Channel Width 40 MHz
Control Sideband Upper
Maximum Clients 128 (range: 1 - 255)
Security option Disabled

Table 2-7 Basic of WLAN Setting Instruction

Parameter	Instruction
Radio Mode	2.4G model, Wi-Fi bandwidth for 1300Mbps

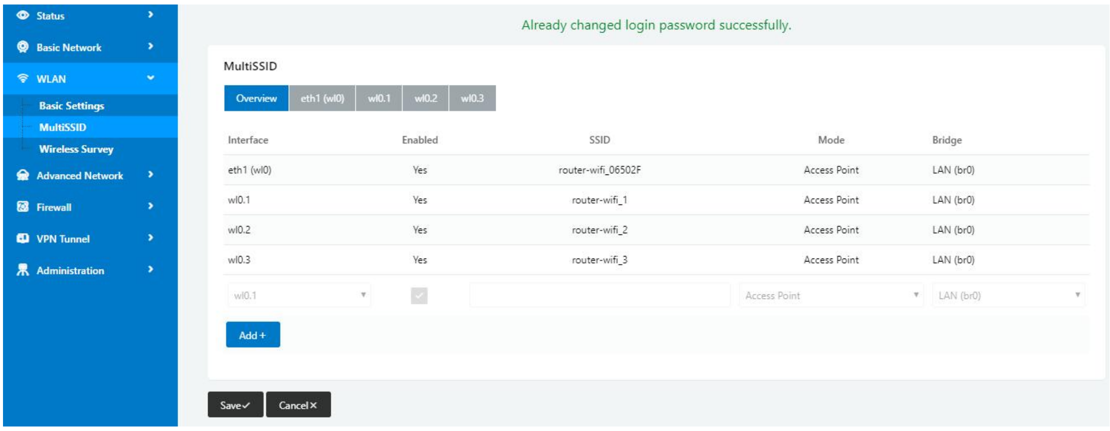
Parameter	Instruction
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP mode.
Wireless Network protocol	Support Auto/b/g/n optional for 2.4G. Support Auto/A/N optional for 2.5G.
SSID	The default is router, can be modified as per application.
Channel	The channel of wireless network, suggest keep the default
Channel Width	20MHz and 40MHz alternative for 2.4G. 20MHz, 40MHz and 80MHzalternative for 2.4G.
Security	Support various encryption method as requested.

Step 2 Please click “Save” to finish.

----End

3.8.2 MultiSSID

Step 1 WLAN> MultiSSID.


Status
Basic Network
WLAN
Basic Settings
MultiSSID
Wireless Survey
Advanced Network
Firewall
VPN Tunnel
Administration
MultiSSID
Overview
eth1 (wl0)
wl0.1
wl0.2
wl0.3
wl0.1
Access Point
LAN (br0)
Add +
Save✓
Cancel✕

Already changed login password successfully.

Interface	Enabled	SSID	Mode	Bridge
eth1 (wl0)	Yes	router-wifi_06502F	Access Point	LAN (br0)
wl0.1	Yes	router-wifi_1	Access Point	LAN (br0)
wl0.2	Yes	router-wifi_2	Access Point	LAN (br0)
wl0.3	Yes	router-wifi_3	Access Point	LAN (br0)

Step 2 Please Click “Save “ to finish.

NOTE

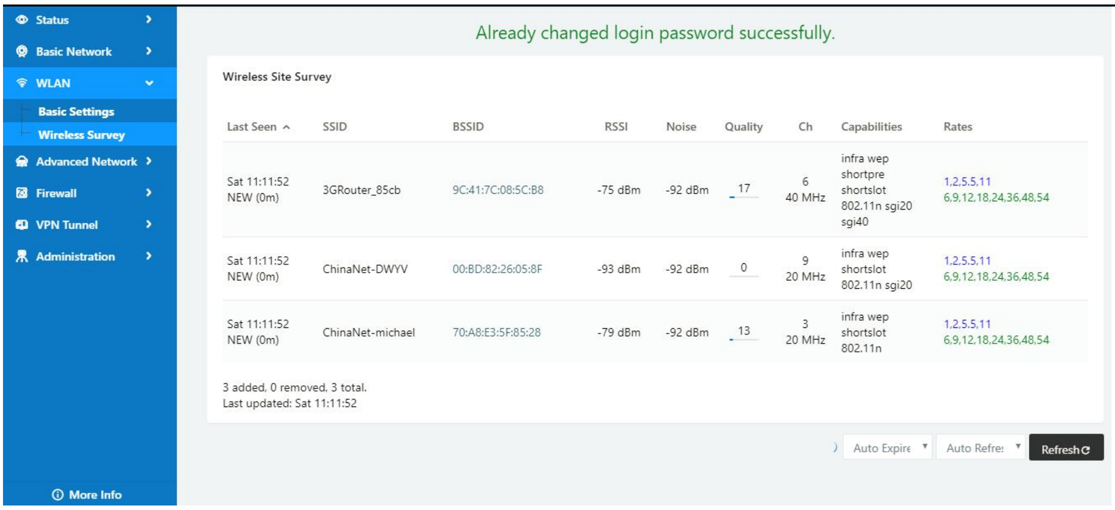
Support 4 SSIDs as Max

----End

3.8.3 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.

The Router will automatically scan neighbour SSIDs.


Status
Basic Network
WLAN
Basic Settings
Wireless Survey
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Auto Expire
Auto Refres
Refresh

Already changed login password successfully.

Wireless Site Survey

Last Seen	SSID	BSSID	RSSI	Noise	Quality	Ch	Capabilities	Rates
Sat 11:11:52 NEW (0m)	3GRouter_85cb	9C:41:7C:08:5C:B8	-75 dBm	-92 dBm	17	6 40 MHz	infra wep shortpre shortslot 802.11n sgi20 sgi40	1,2,5.5,11 6,9,12,18,24,36,48,54
Sat 11:11:52 NEW (0m)	ChinaNet-DWYV	00:BD:82:26:05:8F	-93 dBm	-92 dBm	0	9 20 MHz	infra wep shortslot 802.11n sgi20	1,2,5.5,11 6,9,12,18,24,36,48,54
Sat 11:11:52 NEW (0m)	ChinaNet-michael	70:A8:E3:5F:85:28	-79 dBm	-92 dBm	13	3 20 MHz	infra wep shortslot 802.11n	1,2,5.5,11 6,9,12,18,24,36,48,54

3 added, 0 removed, 3 total.
Last updated: Sat 11:11:52

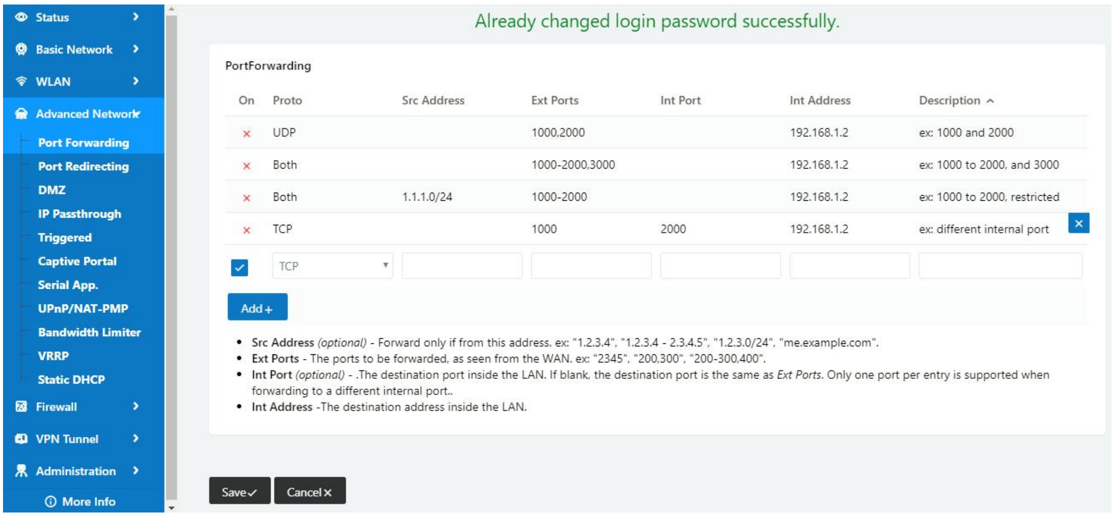
Step 2 Please Click "Stop" to change refresh by manual.

----End

3.9 Advanced Network Setting

3.9.1 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.


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Add +
Save ✓
Cancel ✕

Already changed login password successfully.

PortForwarding

On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description
✕	UDP		1000,2000		192.168.1.2	ex: 1000 and 2000
✕	Both		1000-2000,3000		192.168.1.2	ex: 1000 to 2000, and 3000
✕	Both	1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted
✕	TCP		1000	2000	192.168.1.2	ex: different internal port
☑	TCP					

- **Src Address** *(optional)* - Forward only if from this address. ex: "1.2.3.4", "1.2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.example.com".
- **Ext Ports** - The ports to be forwarded, as seen from the WAN. ex: "2345", "200,300", "200-300,400".
- **Int Port** *(optional)* - .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** -The destination address inside the LAN.

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.
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

Parameter	Instruction
	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.

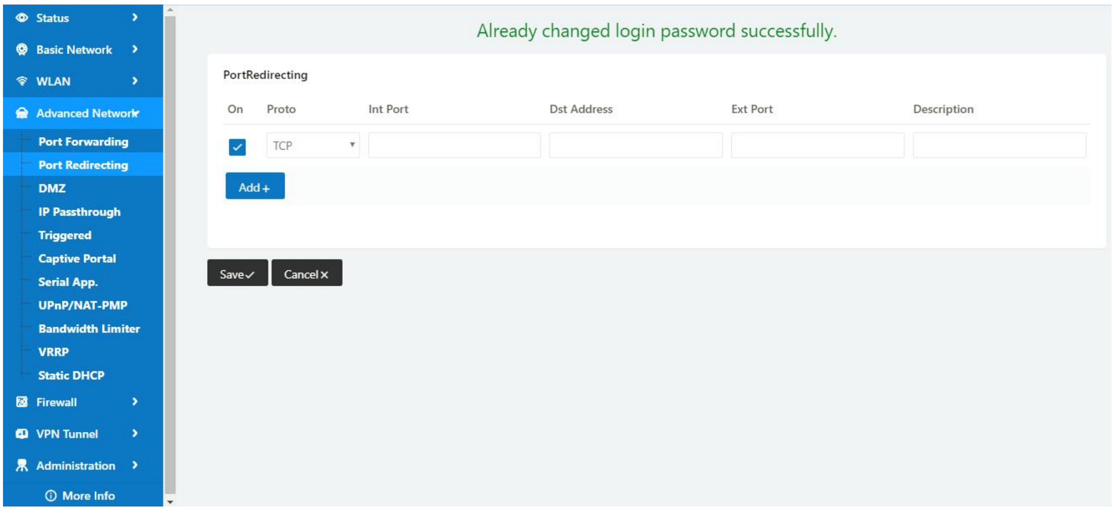
Configuration Instance

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

----End

3.9.2 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.


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Add +
Save ✓
Cancel ✕

Already changed login password successfully.

PortRedirecting

On	Proto	Int Port	Dst Address	Ext Port	Description
☑	TCP				

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.

NOTE

The Port redirecting feature will be unavailable when enable Captive Portal function.

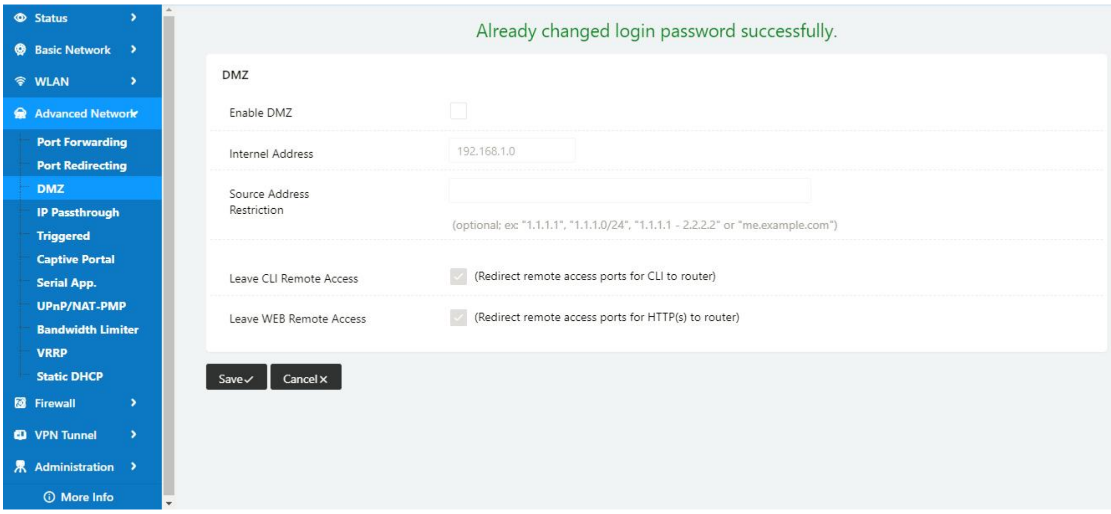
Configuration Instance

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

----End

3.9.3 DMZ Setting

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Save✓
Cancel×

Already changed login password successfully.

DMZ

Enable DMZ ☐

Internel Address 192.168.1.0

Source Address Restriction

(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com")

Leave CLI Remote Access ☑ (Redirect remote access ports for CLI to router)

Leave WEB Remote Access ☑ (Redirect remote access ports for HTTP(s) to router)

Table 2-10 DMZ Instruction

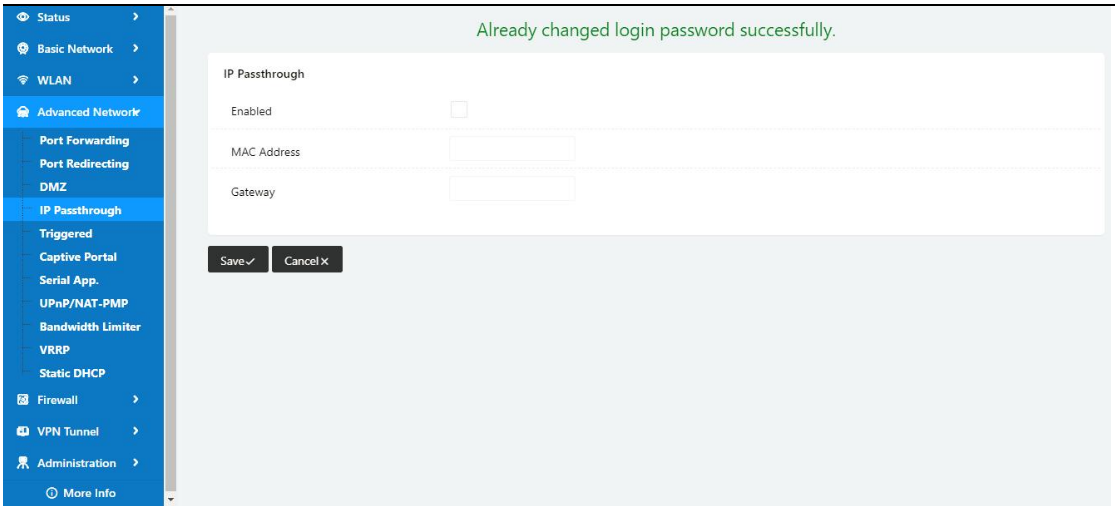
parameter	Instruction
Destination Address	The destination address inside the LAN.
Source Address Restriction	If no IP address inside, it will allow all IP address to access. If define IP address, it will just allow the defined IP address to access.
Leave Remote Access	

Step 2 Please click ”save” to finish

----End

3.9.4 IP Passthrough Setting

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Save✓
Cancel✕

Already changed login password successfully.

IP Passthrough

Enabled ☐

MAC Address

Gateway

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.
router	If WL-Rxx router connect to multiple device, input other device router. The device might access to router GUI.

Step 2 Please click ”save” to finish.

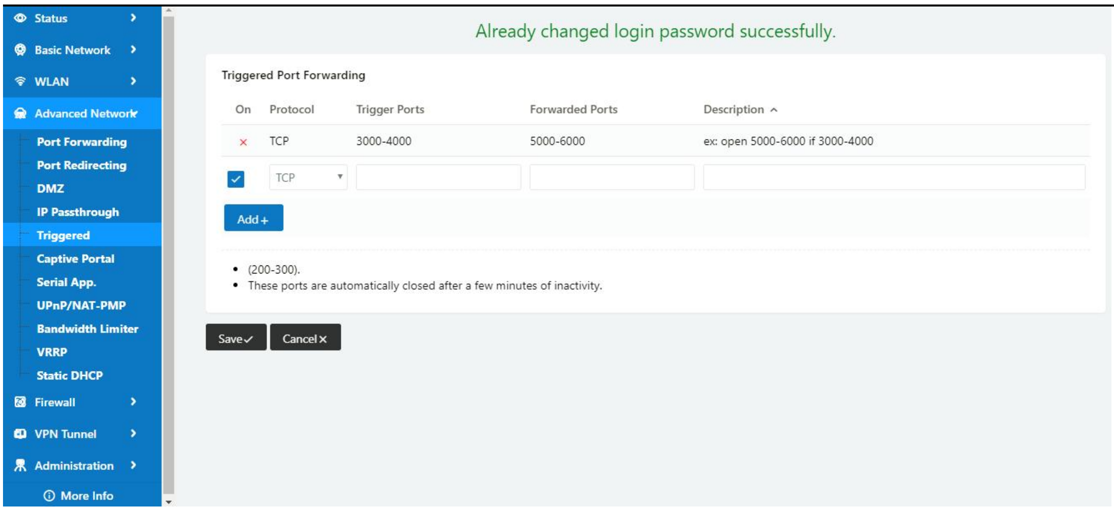
Configuration Instance

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

----End

3.9.5 Triggered Setting

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Add+
Save✓
Cancel×

Already changed login password successfully.

Triggered Port Forwarding

On	Protocol	Trigger Ports	Forwarded Ports	Description
×	TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000
☑	TCP			

- (200-300).
- These ports are automatically closed after a few minutes of inactivity.

Table 2-12　Triggered Instruction

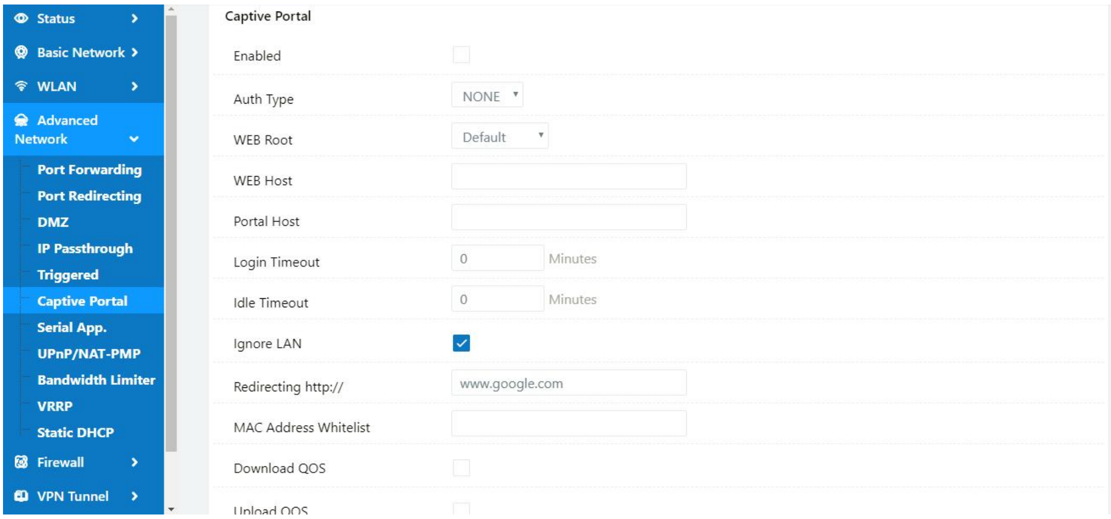
parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.
Note	Port triggering opens an incoming port when your computer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

Step 2　Please click ”save” to finish.

----End

3.9.6 Captive Portal

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel

Captive Portal

Enabled	☐
Auth Type	NONE
WEB Root	Default
WEB Host	
Portal Host	
Login Timeout	0 Minutes
Idle Timeout	0 Minutes
Ignore LAN	☑
Redirecting http://	www.google.com
MAC Address Whitelist	
Download QOS	☐
Upload QOS	☐

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.
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.

CAUTION

WL-R100 doesn't support Captive Portal feature.

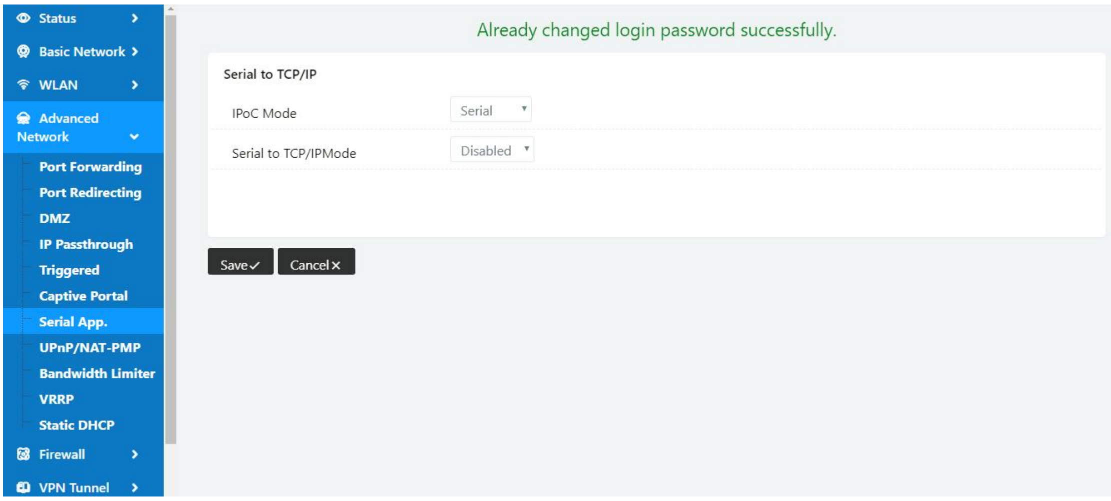
Configuration Instance

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

----End

3.9.7 Serial App. Setting

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

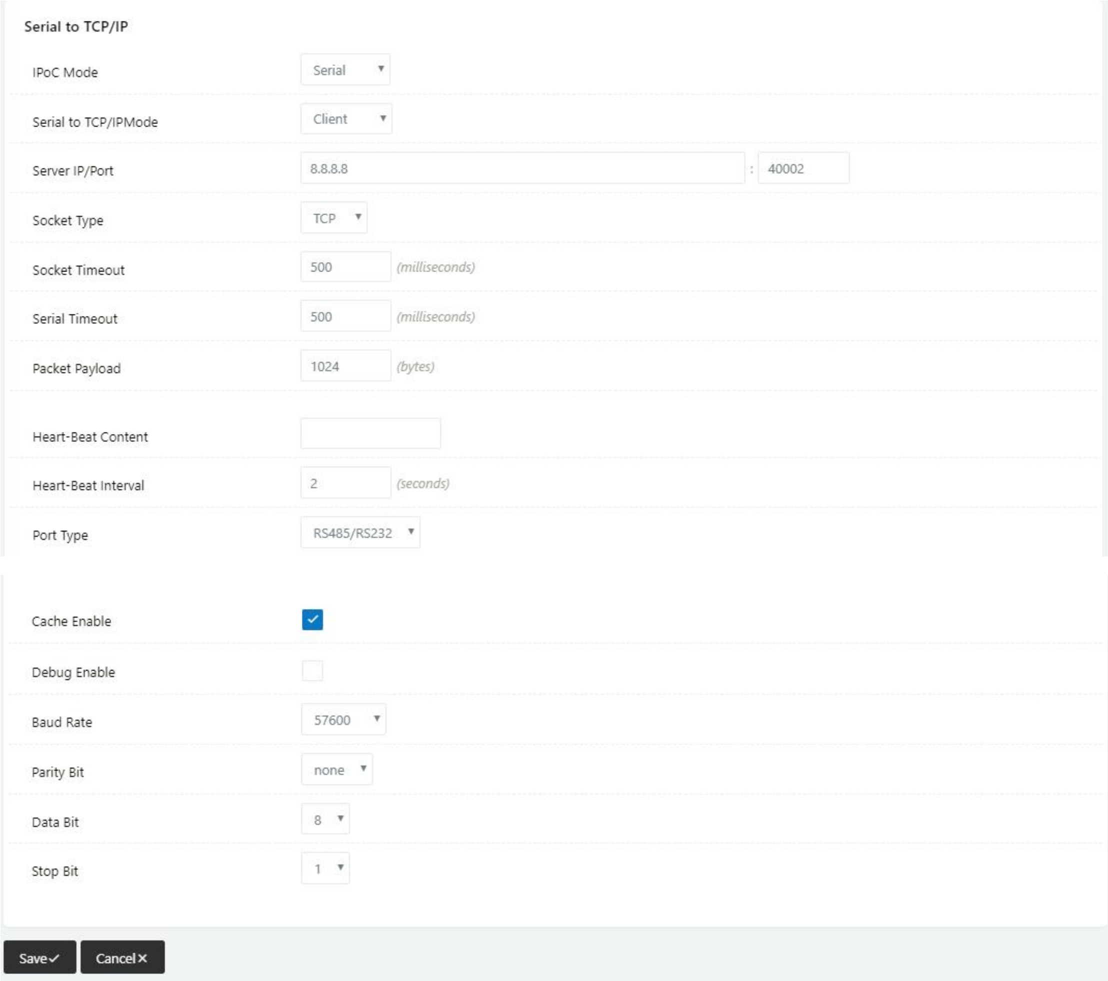

Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Save✓
Cancel×

Already changed login password successfully.

Serial to TCP/IP

IPoC Mode: Serial

Serial to TCP/IPMode: Disabled


Save✓
Cancel×

Serial to TCP/IP

IPoC Mode: Serial

Serial to TCP/IPMode: 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

Table 2-14 Serial App Instruction

Parameter	Instruction
Serial to TC/IP mode	Support Disable, Server and Client mode. Such as Client.

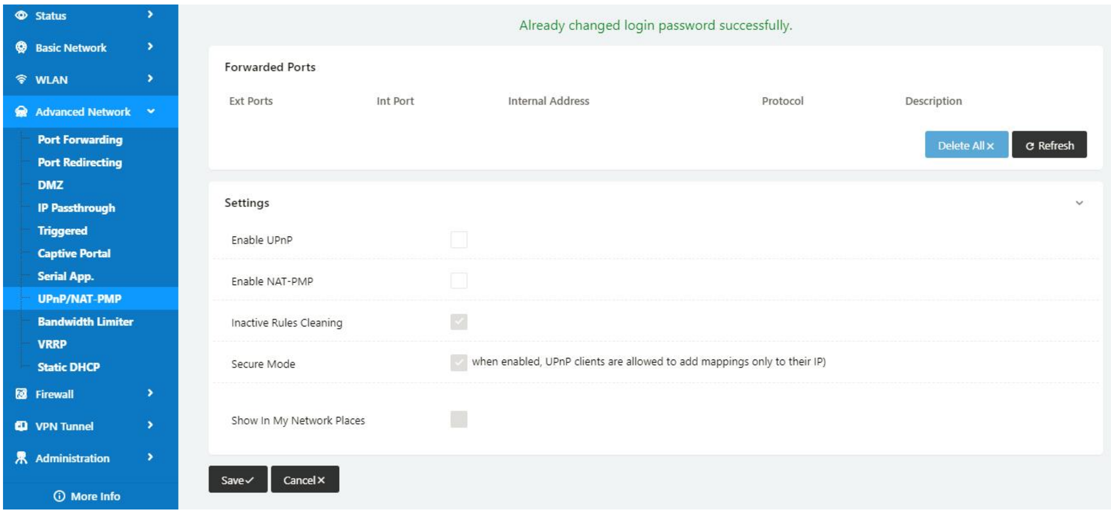
Parameter	Instruction
Server IP/Port	IP address and domain name are acceptable for Server IP
Socket Type	Support TCP/UDP protocol
Socket Timeout	Router will wait the setting time to transmit data to serial port.
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that 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
Baud Rate	115200 as default
Parity Bit	None as default
Data Bit	8bit as default
Stop Bit	1bit as default

Step 2 Please click ”save” to finish.

----End

3.9.8 UPnp/NAT-PMP Setting

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Delete All ×
Refresh
Save ✓
Cancel ×

Already changed login password successfully.

Forwarded Ports

Ext Ports	Int Port	Internal Address	Protocol	Description

Settings

Enable UPnP ☐

Enable NAT-PMP ☐

Inactive Rules Cleaning ☑

Secure Mode ☑ when enabled, UPnP clients are allowed to add mappings only to their IP)

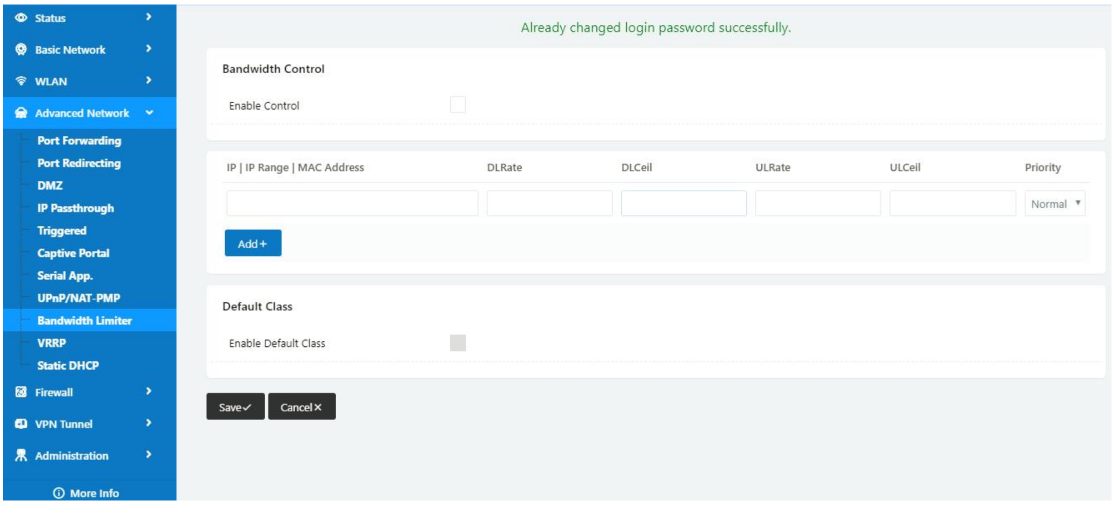
Show In My Network Places ☐

Step 2 Please click ”save” to finish.

----End

3.9.9 Bandwidth Control Setting

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Add +
Save ✓
Cancel ✕

Already changed login password successfully.

Bandwidth Control

Enable Control ☐

IP | IP Range | MAC Address	DLRate	DLCeil	ULRate	ULCeil	Priority
					Normal

Default Class

Enable Default Class ☐

Table 2-15 Bandwidth Control Instruction

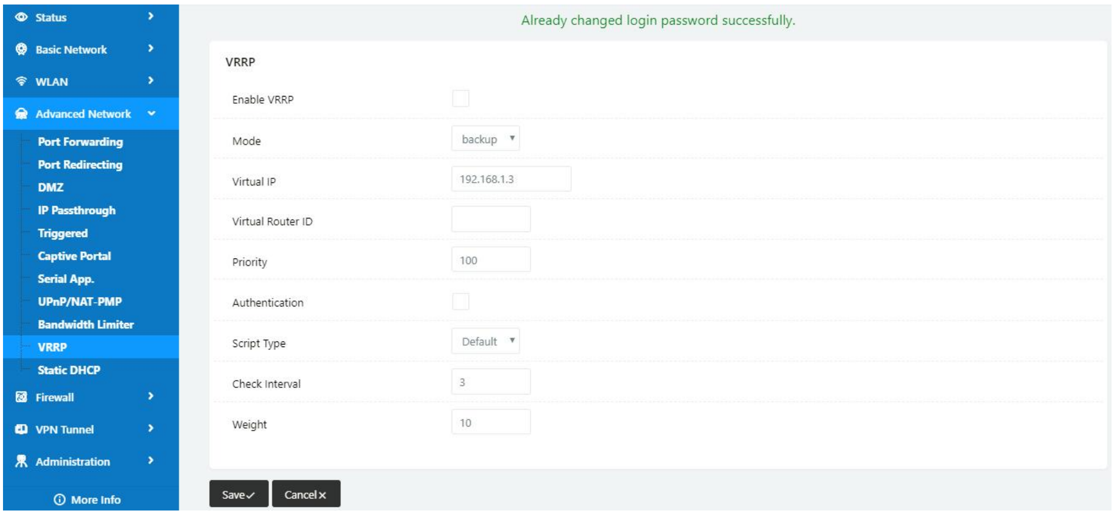
Max Available Download	Speed limit for router.
Max Available Upload	Speed limit for router.
IP/ IP Range/ MAC Address	Limit devices speed for specified IP/IP Range/ MAC Address.
DL Rate	Mix Download rate
DL ceil	Max download rate
UL Rate	Mix Upload rate
UL ceil	Max upload rate
Priority	The priority of 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

3.9.10 VRRP Setting

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Save ✓
Cancel ×

Already changed login password successfully.

VRRP

Enable VRRP ☐

Mode: backup

Virtual IP: 192.168.1.3

Virtual Router ID:

Priority: 100

Authentication ☐

Script Type: Default

Check Interval: 3

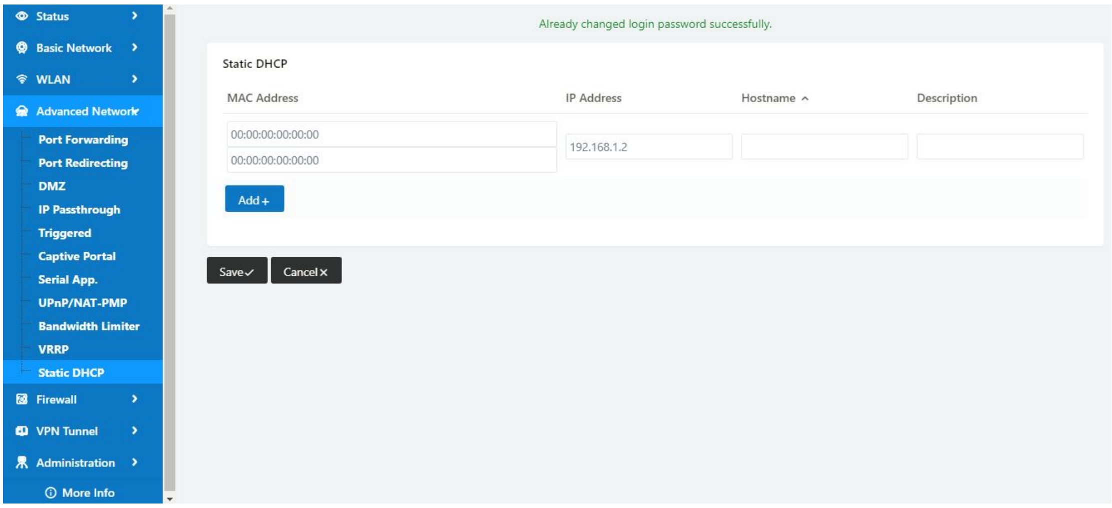
Weight: 10

Step 2 Please click ”save” to finish.

----End

3.9.11 Static DHCP Setting

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Add +
Save ✓
Cancel ×

Already changed login password successfully.

Static DHCP

MAC Address	IP Address	Hostname	Description
00:00:00:00:00:00 00:00:00:00:00:00	192.168.1.2		

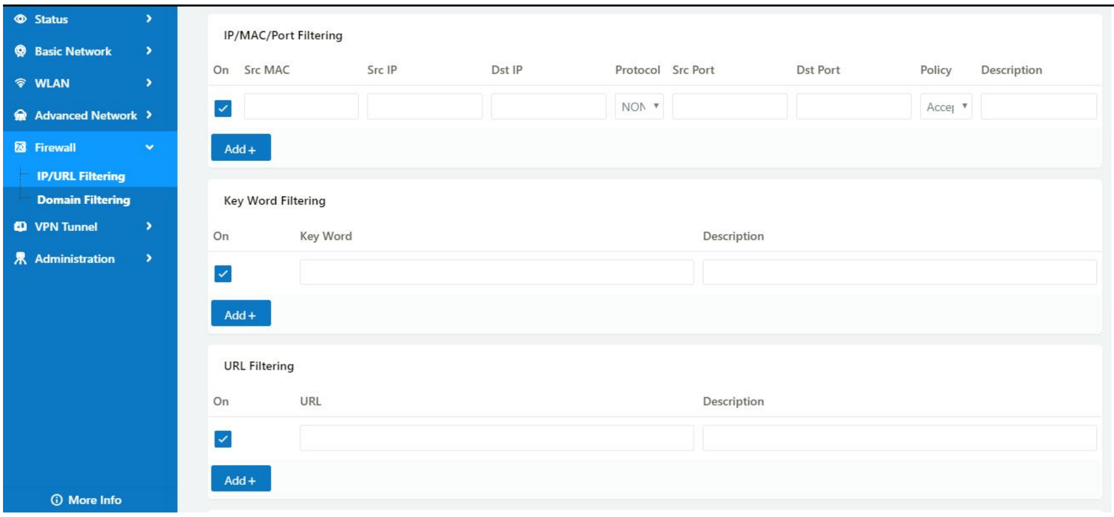
Step 2 Please click ”save” to finish.

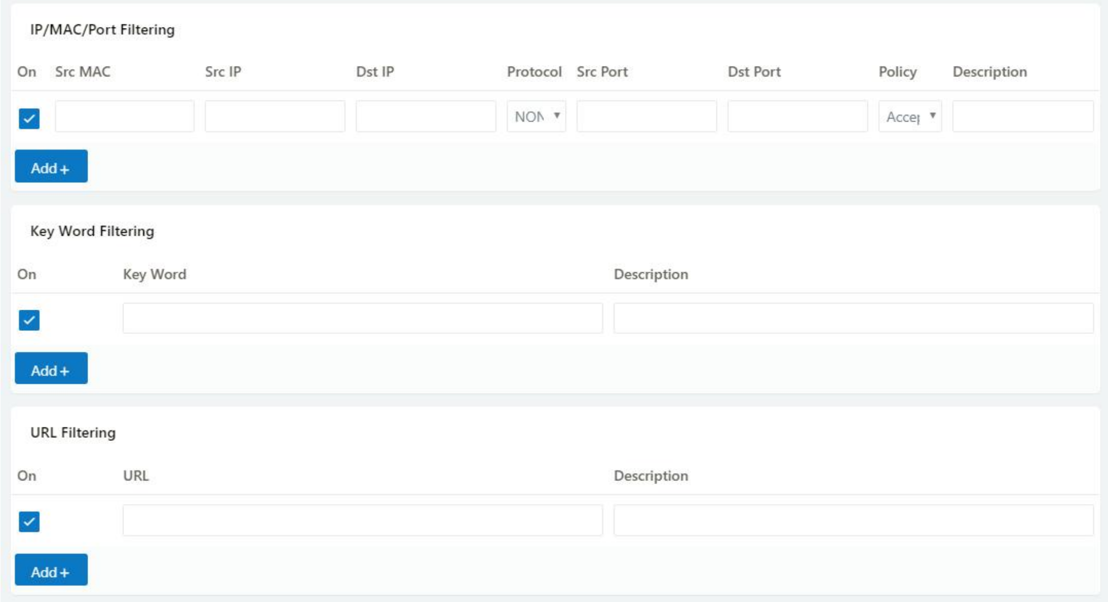
----End

3.10 Firewall

3.10.11 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
NON
Accep
Add+
Key Word Filtering
On Key Word Description
Add+
URL Filtering
On URL Description
Add+


IP/MAC/Port Filtering
On Src MAC Src IP Dst IP Protocol Src Port Dst Port Policy Description
NON
Accep
Add+
Key Word Filtering
On Key Word Description
Add+
URL Filtering
On URL Description
Add+

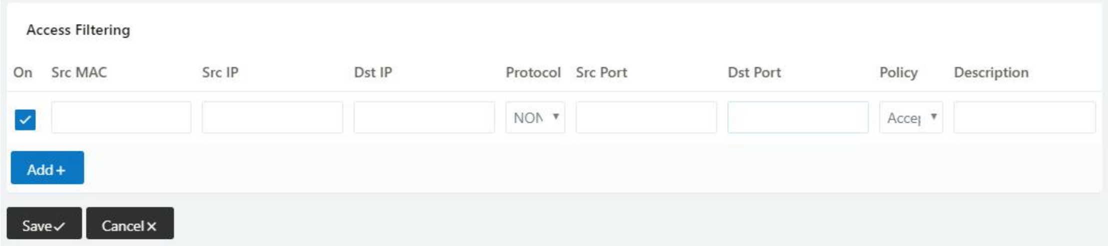

Access Filtering
On Src MAC Src IP Dst IP Protocol Src Port Dst Port Policy Description
NON
Accep
Add+
Save
Cancel

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.

NOTE

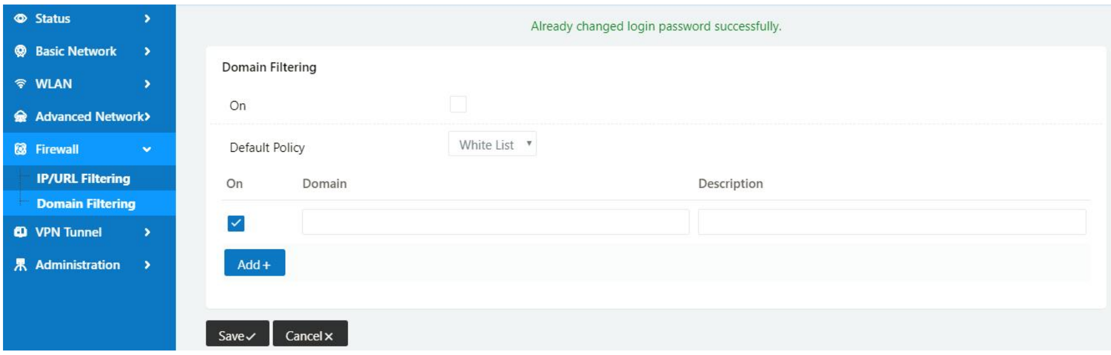
Please check Firewall rule in Configuration instance.

Step 2 Please click ”save” to finish.

---End

3.10.12 Domain Filtering

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


Status
Basic Network
WLAN
Advanced Network
Firewall
IP/URL Filtering
Domain Filtering
VPN Tunnel
Administration
Add+
Save✓
Cancel✕

Already changed login password successfully.

Domain Filtering

On ☐

Default Policy: White List

On	Domain	Description
☑		

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.

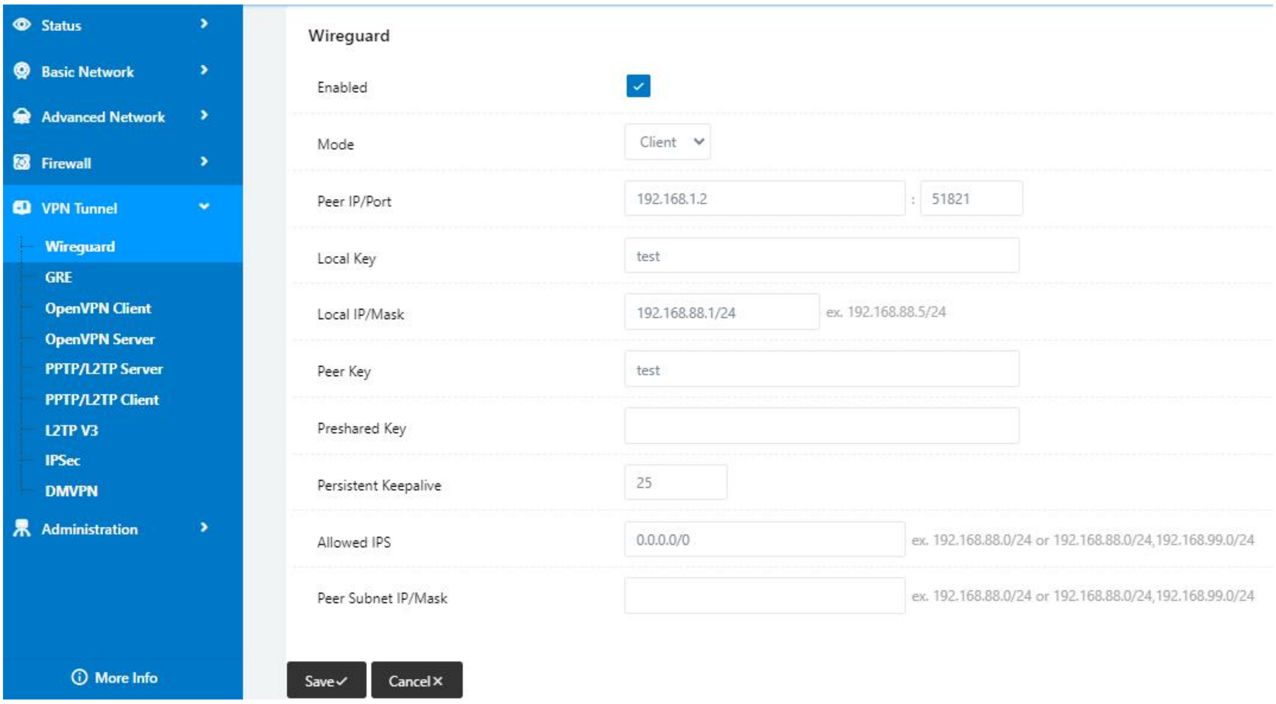
Step 2 Please click ”save” to finish.

----End

3.11 VPN Tunnel

3.11.1 Wireguard Setting

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


Status
Basic Network
Advanced Network
Firewall
VPN Tunnel
Wireguard
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration
More Info
Save✓
Cancel ×

Wireguard

Enabled ☑

Mode: Client

Peer IP/Port: 192.168.1.2 : 51821

Local Key: test

Local IP/Mask: 192.168.88.1/24 ex. 192.168.88.5/24

Peer Key: test

Preshared Key:

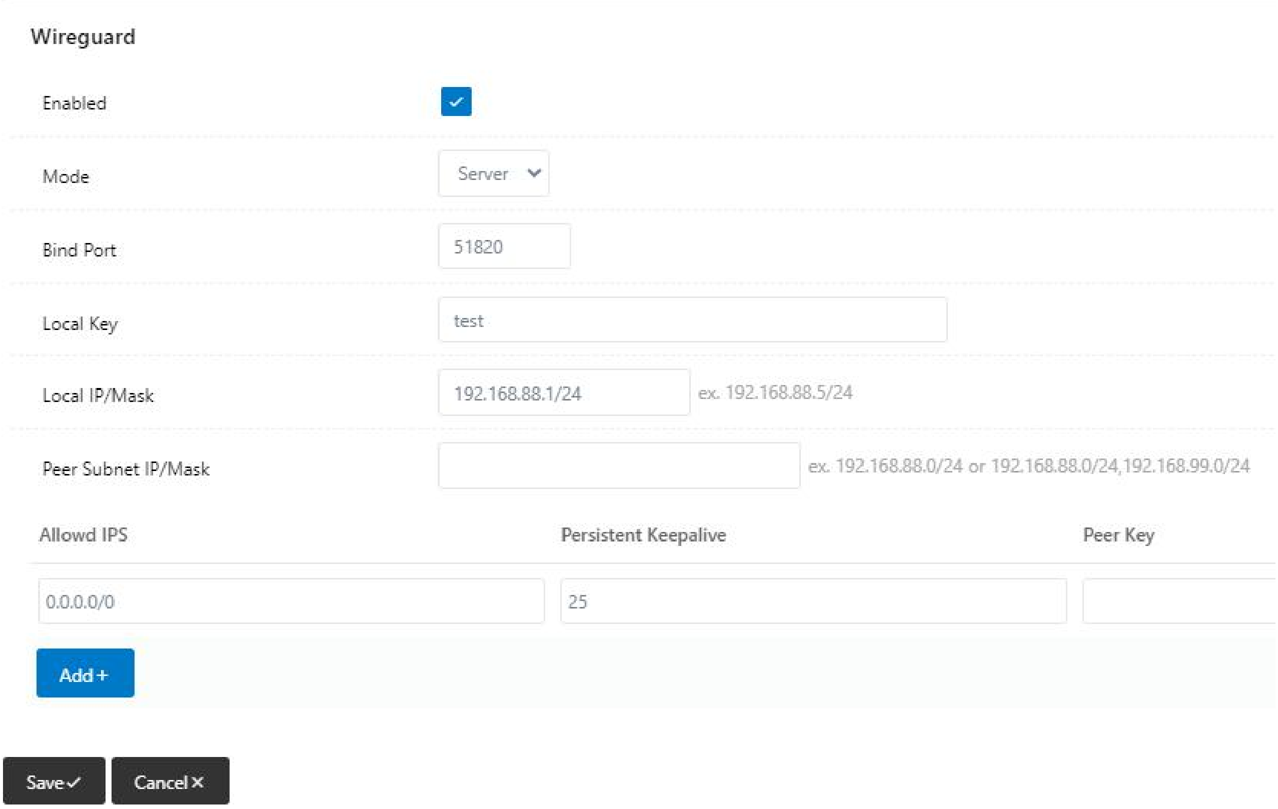
Persistent Keepalive: 25

Allowed IPS: 0.0.0.0/0 ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24

Peer Subnet IP/Mask: ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24

Table 2-18 Wireguard Client Instruction

Parameter	Instruction
Enable	Eenable Wireguard.
Model	Wireguard client and server modes optional
Peer IP/Port	Server IP and port
Local Key	VPN local key
Local IP/Mask	Wireguard VPN tunnel local IP and mask. The VPN local IP address and peer IP address are different subnet segment.
Peer Key	VPN peer key
Preshared Key	Wireguard Pre-shared key
Keepalive	Keepalive interval,unit for second
Allowed IPs	Allowed VPN subnet IP addresses
Peer Subnet IP/Mask	Wireguard VPN tunnel Peer IP and mask.


Wireguard

Enabled ☑

Mode: Server

Bind Port: 51820

Local Key: test

Local IP/Mask: 192.168.88.1/24 ex. 192.168.88.5/24

Peer Subnet IP/Mask: ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.99.0/24

Allowd IPS	Persistent Keepalive	Peer Key
0.0.0.0/0	25	

Table 2-19 Wireguard Sever Instruction

Parameter	Instruction
Enable	Eenable Wireguard.
Model	Wireguard client and server modes optional
Bind Port	Wireguard server port
Local Key	VPN local key
Local IP/Mask	Wireguard VPN tunnel local IP and mask. The VPN server local IP address and client IP address are different subnet segments.
Preshared Key	Wireguard Pre-shared key
Keepalive	Keepalive interval,unit for second
Allowed IPs	Allowed VPN subnet IP addresses
Peer Key	VPN peer key

Step 2 Please click ”save” to finish.

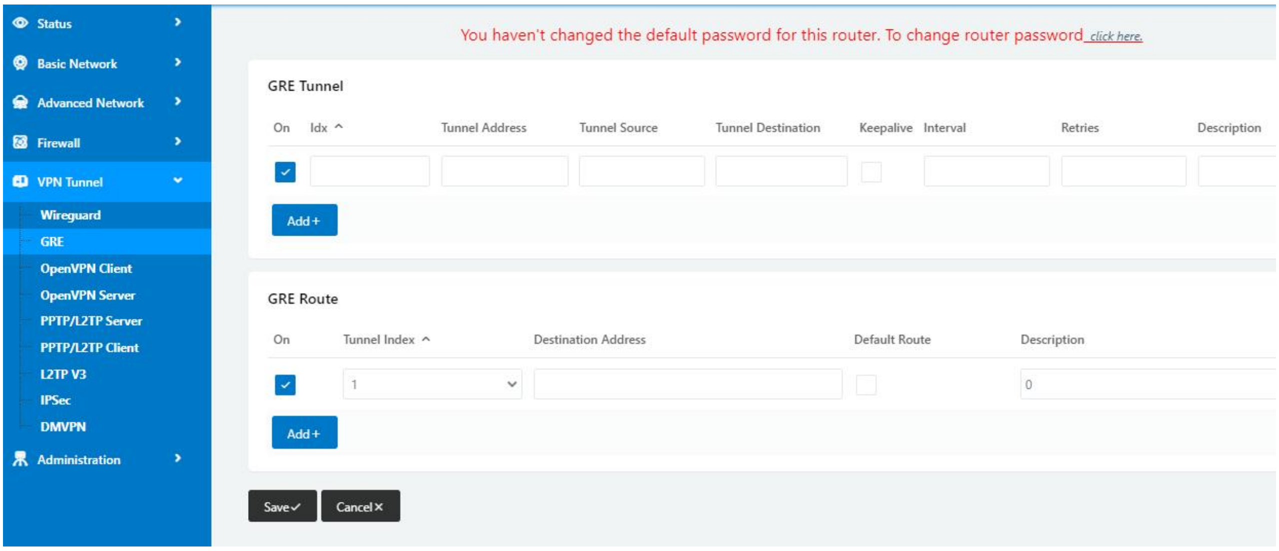
Configuration Instance

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

----End

3.11.2 GRE Setting

Step 3 VPN Tunnel> GRE to check or modify the relevant parameter.



You haven't changed the default password for this router. To change router password click here.

Status
Basic Network
Advanced Network
Firewall
VPN Tunnel
Wireguard
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration
GRE Tunnel
On
Idx
Tunnel Address
Tunnel Source
Tunnel Destination
Keepalive
Interval
Retries
Description
Add +
GRE Route
On
Tunnel Index
Destination Address
Default Route
Description
1
0
Add +
Save ✓
Cancel ✕

Table 2-20 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 4 Please click ”save” to finish.

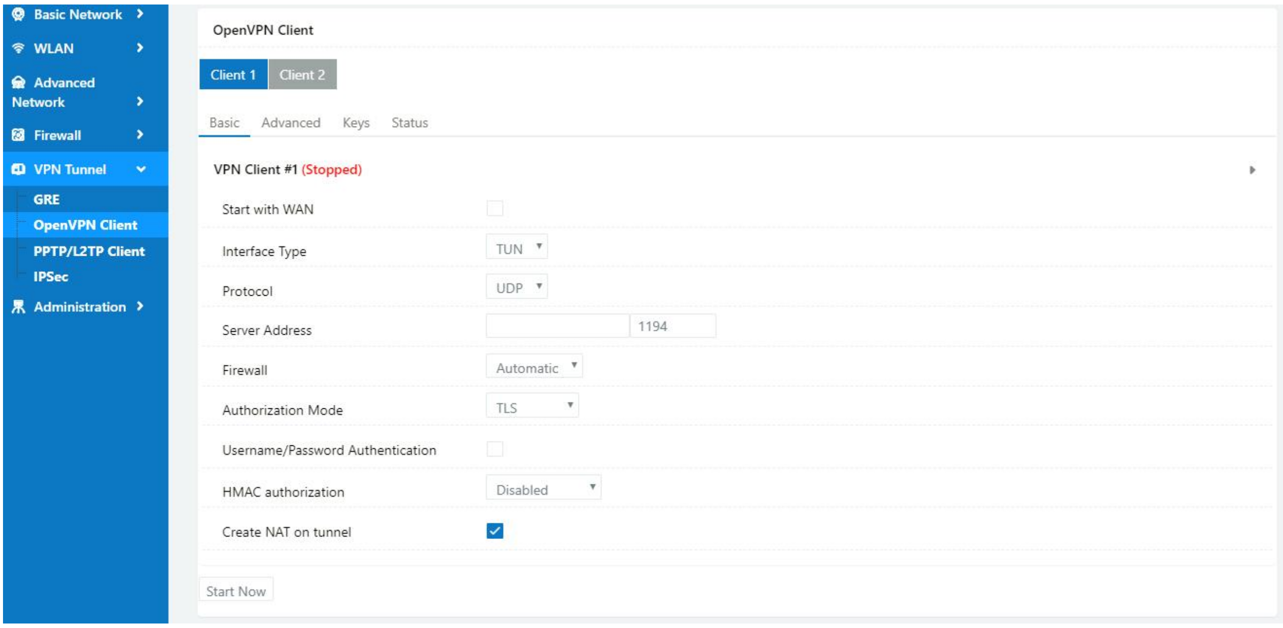
Configuration Instance

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

----End

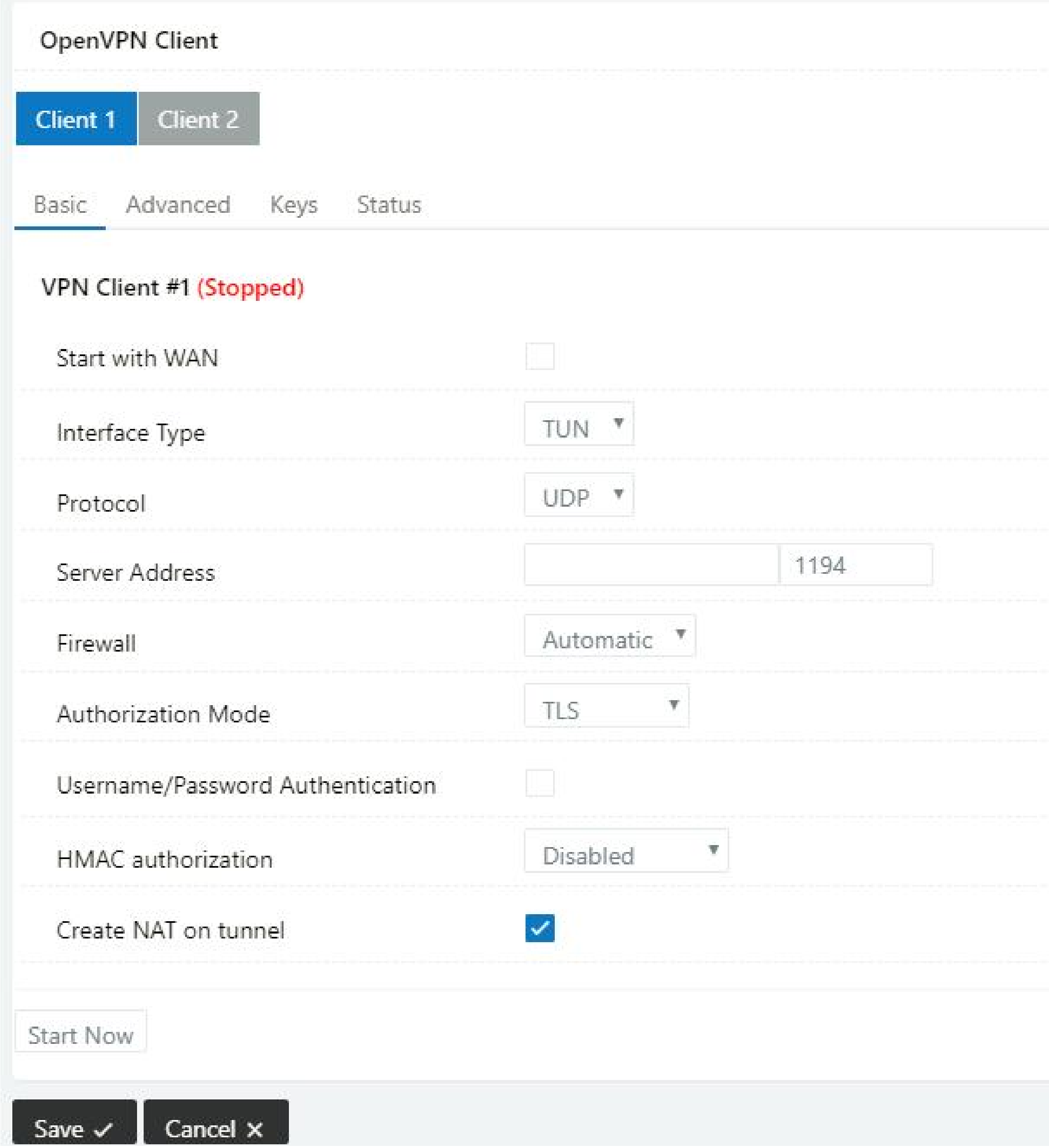
3.11.3 OpenVPN Client Setting

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


Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
OpenVPN Client
Client 1
Client 2
Basic
Advanced
Keys
Status
Start Now

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	☑



OpenVPN Client

VPN Client #1 (Stopped)

Start with WAN ☐

Interface Type: TUN

Protocol: UDP

Server Address: 1194

Firewall: Automatic

Authorization Mode: TLS

Username/Password Authentication ☐

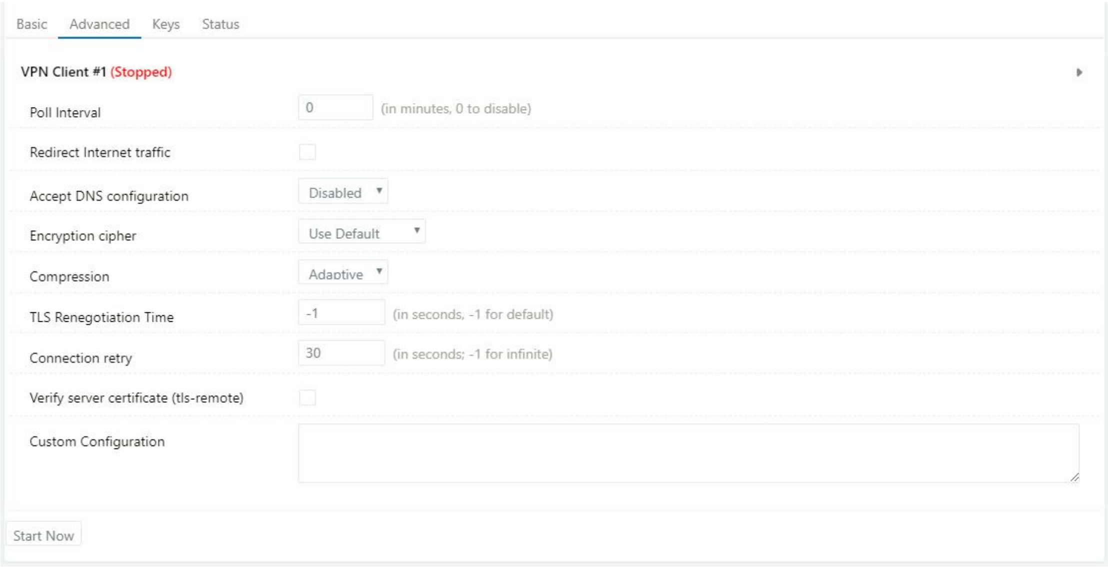
HMAC authorization: Disabled

Create NAT on tunnel ☑

Table 2-21 Basic of OpenVPN Instruction

Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 4G/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.

Parameter	Instruction
Firewall	Auto, External only and Custom are optional
Authorization Mode	TLS, Static key and Custom are optional.
User name/Password Authentication	As the configuration requested.
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.



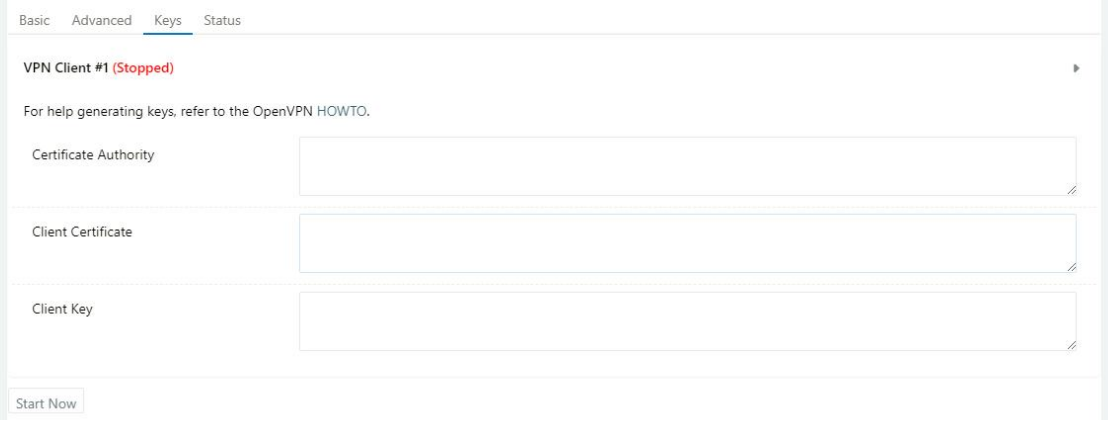
VPN Client #1 (Stopped)

Poll Interval: 0 (in minutes, 0 to disable)
Redirect Internet traffic: ☐
Accept DNS configuration: Disabled
Encryption cipher: Use Default
Compression: Adaptive
TLS Renegotiation Time: -1 (in seconds, -1 for default)
Connection retry: 30 (in seconds; -1 for infinite)
Verify server certificate (tls-remote): ☐
Custom Configuration:

Table 2-22 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.

Parameter	Instruction
Custom Configuration	As the configuration requested.

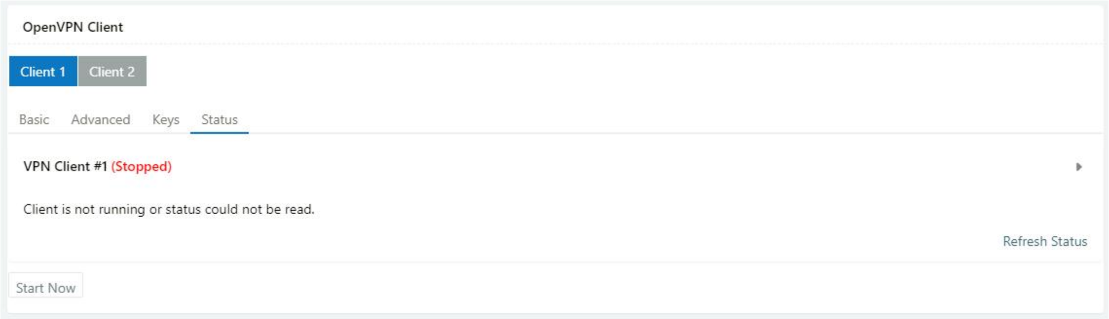

Basic
Advanced
Keys
Status
Certificate Authority
Client Certificate
Client Key
Start Now

VPN Client #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

Table 2-23 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
Refresh Status
Start Now

VPN Client #1 (Stopped)

Client is not running or status could not be read.

Table 2-24 Status of OpenVPN Instruction

Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 2 Please click ”save” to finish.

Configuration Instance

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

----End

3.11.4 PPTP/L2TP Client Setting

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

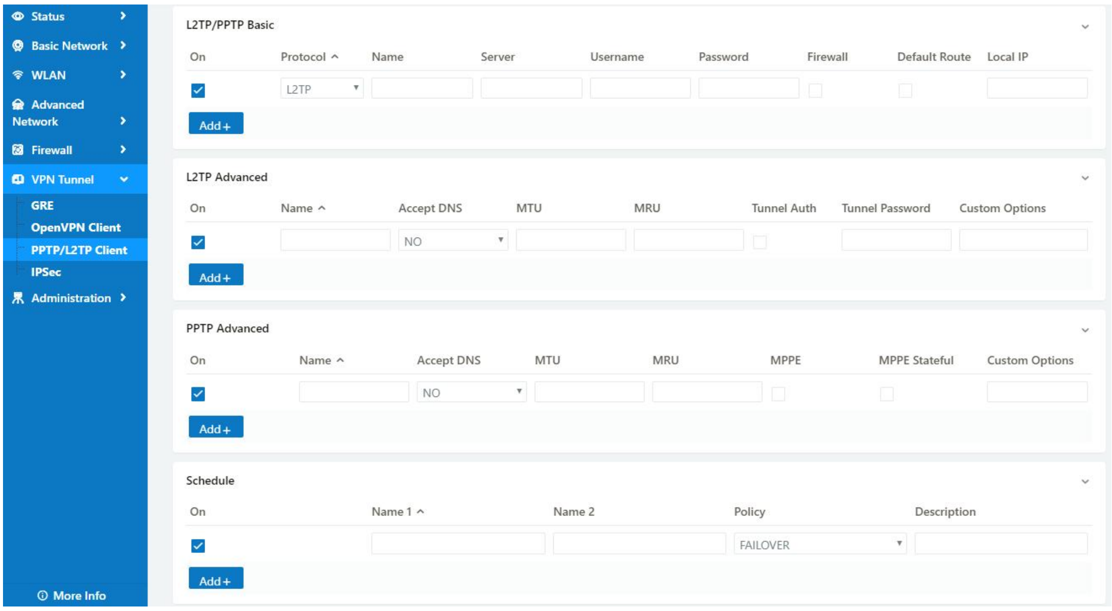

Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
L2TP/PPTP Basic
On
Protocol
Name
Server
Username
Password
Firewall
Default Route
Local IP
L2TP
Add+
L2TP Advanced
On
Name
Accept DNS
MTU
MRU
Tunnel Auth
Tunnel Password
Custom Options
NO
Add+
PPTP Advanced
On
Name
Accept DNS
MTU
MRU
MPPE
MPPE Stateful
Custom Options
NO
Add+
Schedule
On
Name 1
Name 2
Policy
Description
FAILOVER
Add+

Table 2-25 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 2-26 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 2-27 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 2-28 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

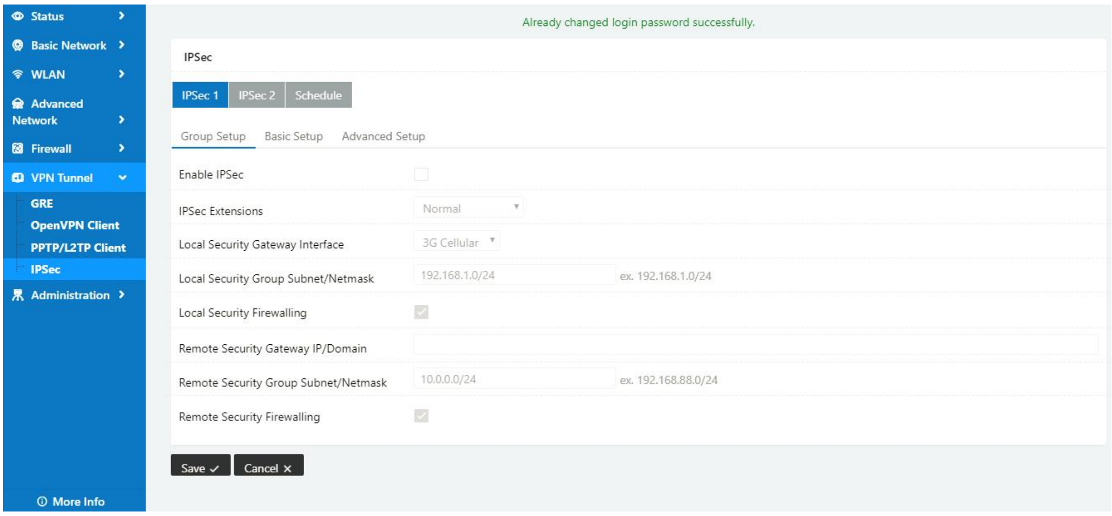
Step 2 Please click ”save” to finish.

Configuration Instance

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

---End

3.11.5 IPSec Setting

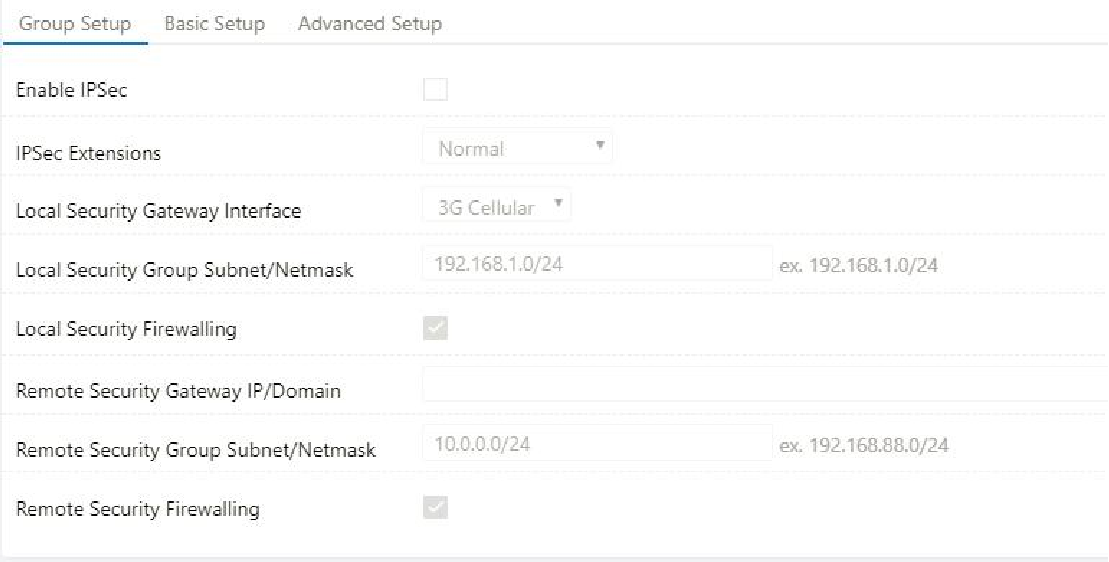

Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
IPSec
IPSec 1
IPSec 2
Schedule
Group Setup
Basic Setup
Advanced Setup
Save ✓
Cancel ×

Already changed login password successfully.

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	☑	

3.11.5.1 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 2-29 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
Remote	IPsec peer IP address/domain name.

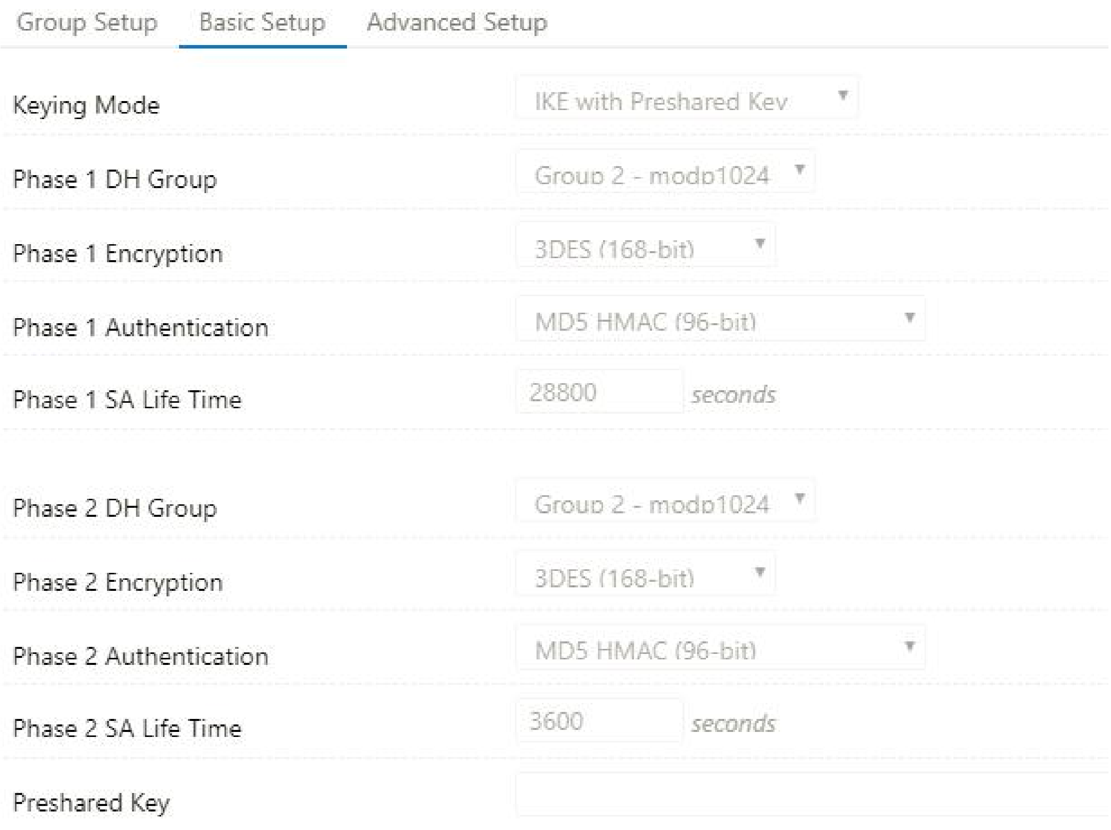
parameter	Instruction
IP/Domain	
Remote Subnet/Mask	IPSec remote subnet and mask.
Remote Firewall	Forwarding-firewalling for Remote subnet

Step 2 Please click ”save” to finish.

---End

3.11.5.2 IPSec Basic Setup

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



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:

Table 2-30 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
Phase 1	Support HASH MD5 and SHA

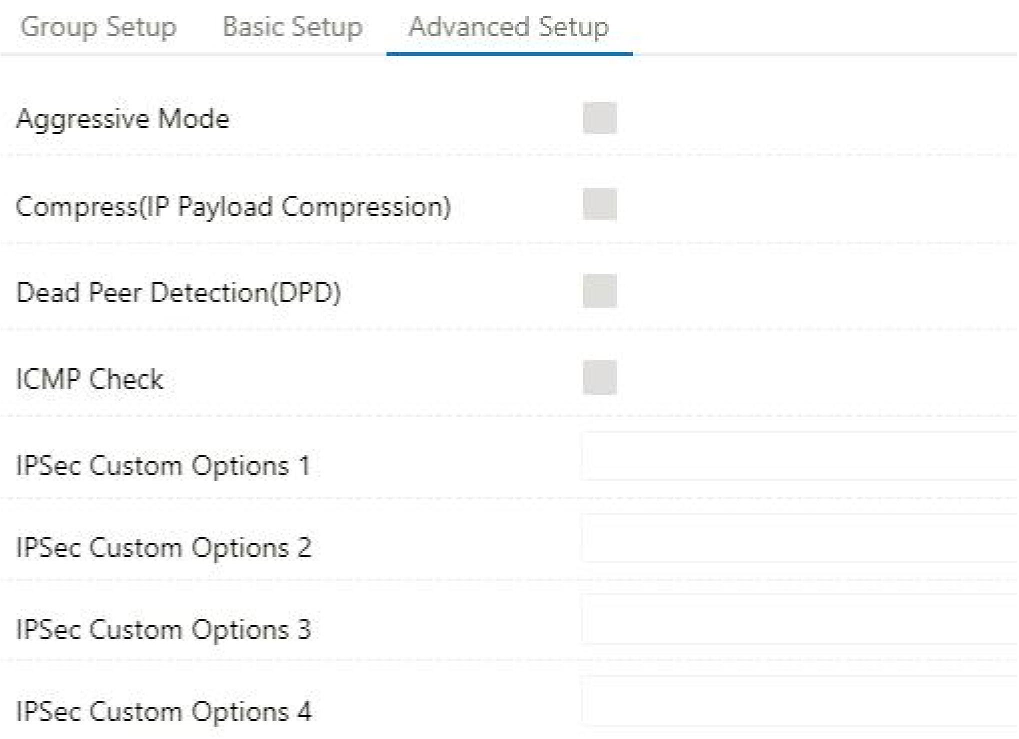
parameter	Instruction
Authentication	
Phase 1 SA Life Time	IPSec Phase 1 SA lifetime
Phase 2 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.
Phase 2 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase 2 Authentication	Support HASH MD5 and SHA
Phase 2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

Step 2 Please click ”save” to finish.

---End

3.11.5.3 IPSec Advanced Setup

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



Aggressive Mode ☐

Compress(IP Payload Compression) ☐

Dead Peer Detection(DPD) ☐

ICMP Check ☐

IPSec Custom Options 1

IPSec Custom Options 2

IPSec Custom Options 3

IPSec Custom Options 4

Table 2-31 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.

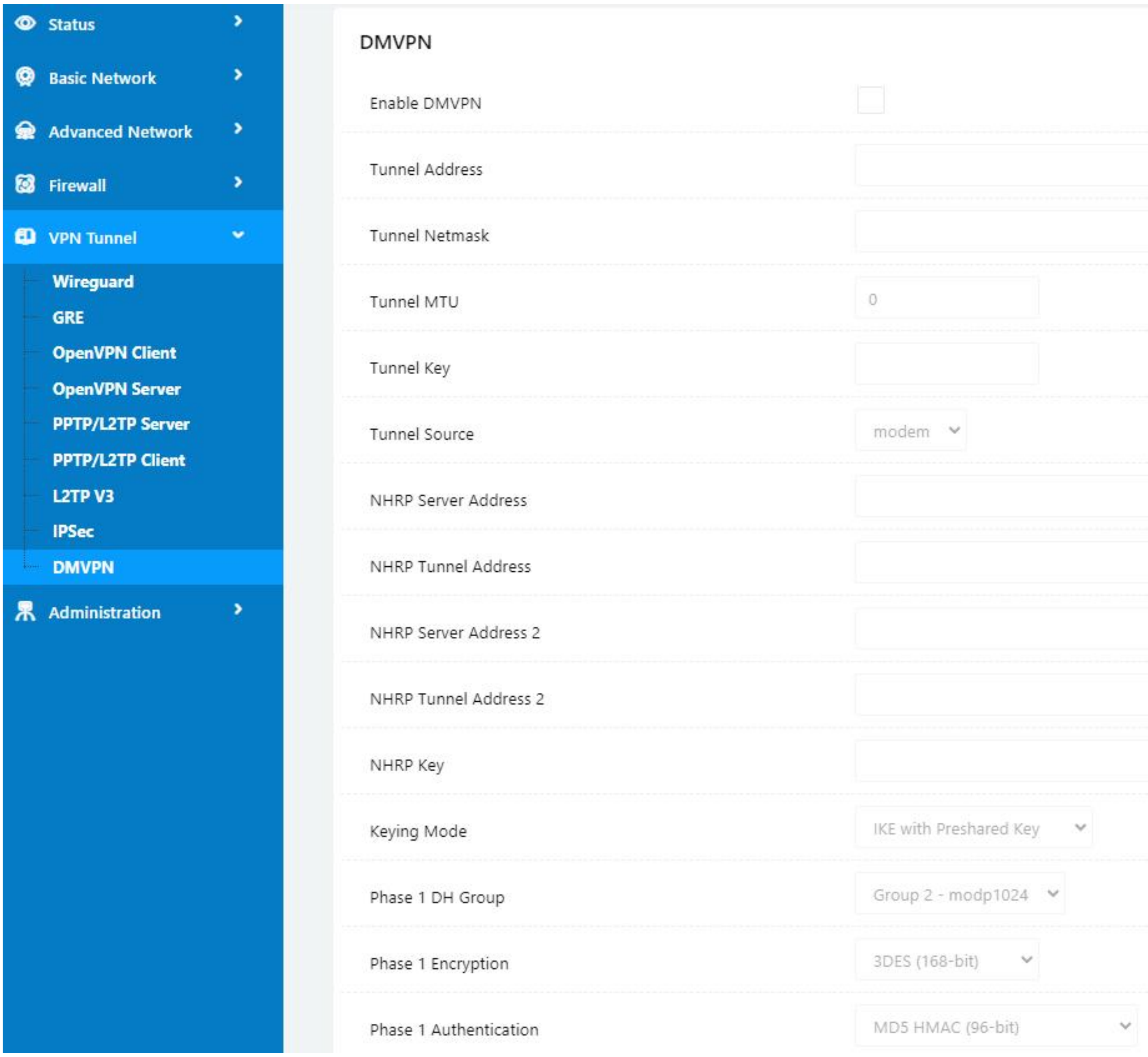
Configuration Instance

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

----End

3.11.6 DMVPN Setting

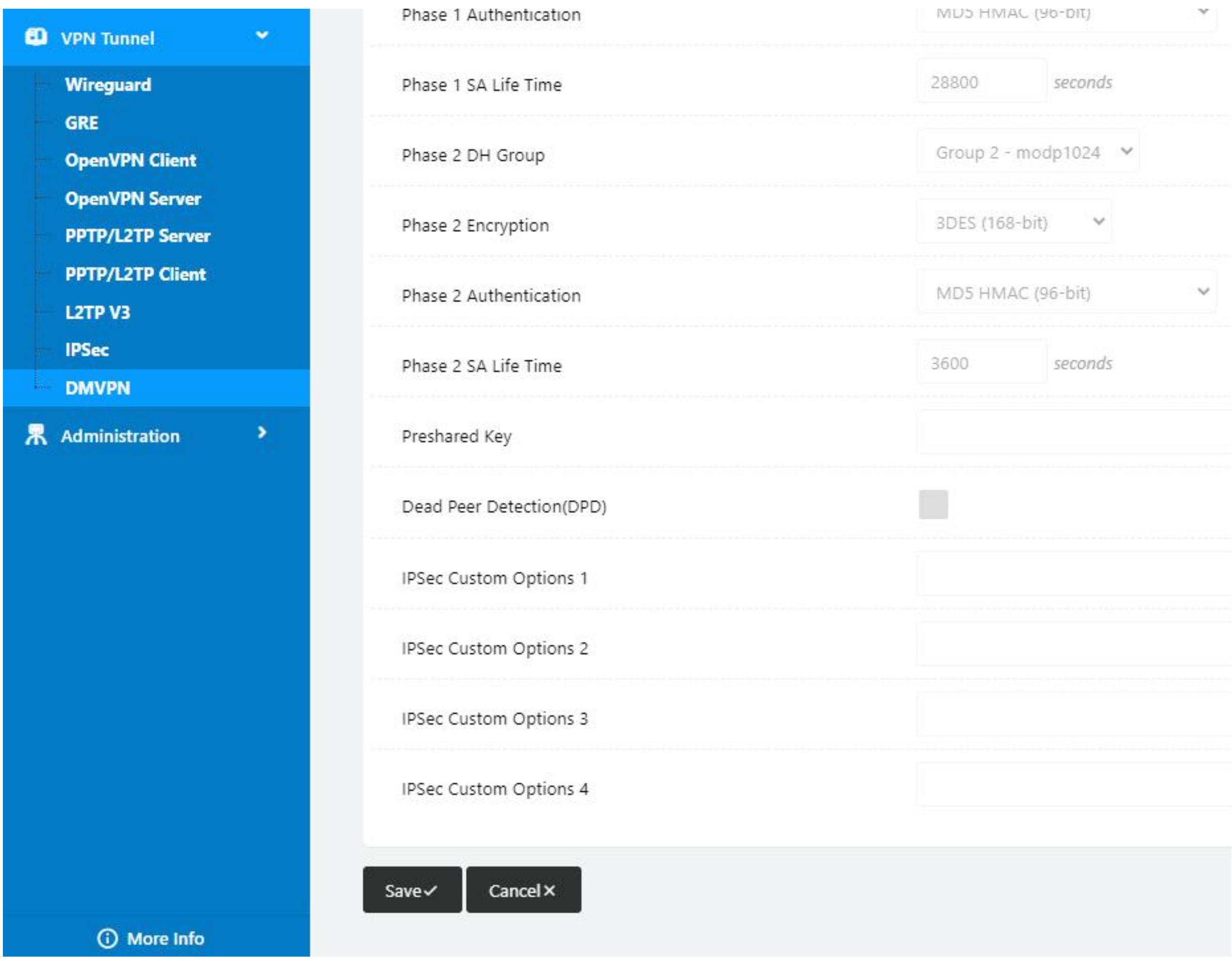
Step 1 VPN Tunnel> DMVPN to check or modify the relevant parameter.



Status
Basic Network
Advanced Network
Firewall
VPN Tunnel
Wireguard
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration

DMVPN

Enable DMVPN	☐
Tunnel Address	
Tunnel Netmask	
Tunnel MTU	0
Tunnel Key	
Tunnel Source	modem
NHRP Server Address	
NHRP Tunnel Address	
NHRP Server Address 2	
NHRP Tunnel Address 2	
NHRP Key	
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)


VPN Tunnel
Wireguard
GRE
OpenVPN Client
OpenVPN Server
PPTP/L2TP Server
PPTP/L2TP Client
L2TP V3
IPSec
DMVPN
Administration
More Info
Save✓
Cancel✕

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
Dead Peer Detection(DPD) ☐
IPSec Custom Options 1
IPSec Custom Options 2
IPSec Custom Options 3
IPSec Custom Options 4

Table 2-32 DMVPN Client Instruction

Parameter	Instruction
Enable	Eenable DMVPN
Tunnel Address	GRE tunnel address
Tunnel Mask	GRE tunnel subnet mask
Tunnel MTU	GRE tunnel MTU
Tunnel Key	GRE tunnel secret key
Tunnel Source	modem(4G/5G);WAN;STA/STA2(WIFI2.4/5.8) Optional
NHRP Server Address	NHRP Server IP address
NHRP Tunnel Address	NHRP Tunnel address
NHRP Key	NHRP Secret key
Keying Mode	IKEv1/IKEv2 optional
Phase1 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.

Parameter	Instruction
Phase1 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase1 Authentication	Support HASH MD5 and SHA
Phase1 SA Lifetime	IPSec Phase 1 SA lifetime
Phase2 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.
Phase2 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase2 Authentication	Support HASH MD5 and SHA
Phase2 SA Lifetime	IPSec Phase 2 SA lifetime
Preshared Key	IPsec preshared key
Dead Peer Detection(DPD)	Dead Peer Detection
IPSec Custom Options	IPSec custom configuration according to server.

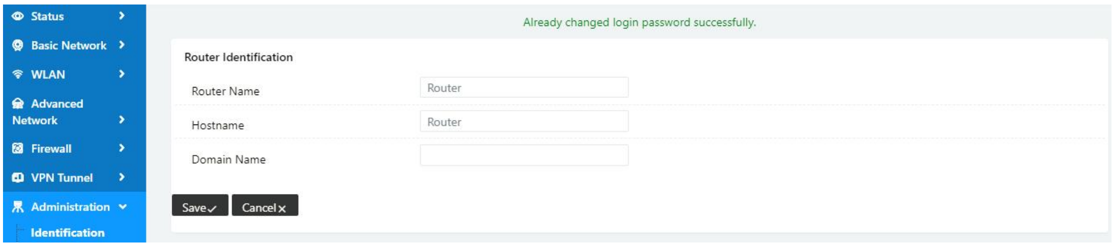
Step 2 Please click ”save” to finish.

----End

3.12 Administration

3.12.1 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.


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Identification
Save✓
Cancel✕

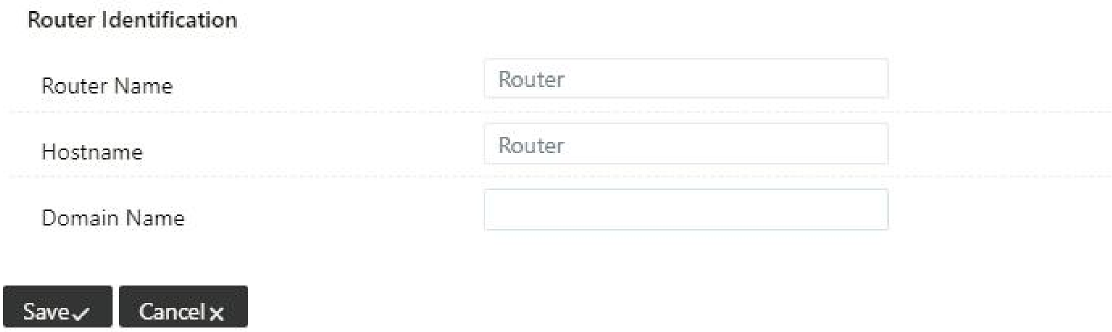
Already changed login password successfully.

Router Identification

Router Name: Router

Hostname: Router

Domain Name:


Save✓
Cancel✕

Router Identification

Router Name: Router

Hostname: Router

Domain Name:

Table 2-33 Router Identification Instruction

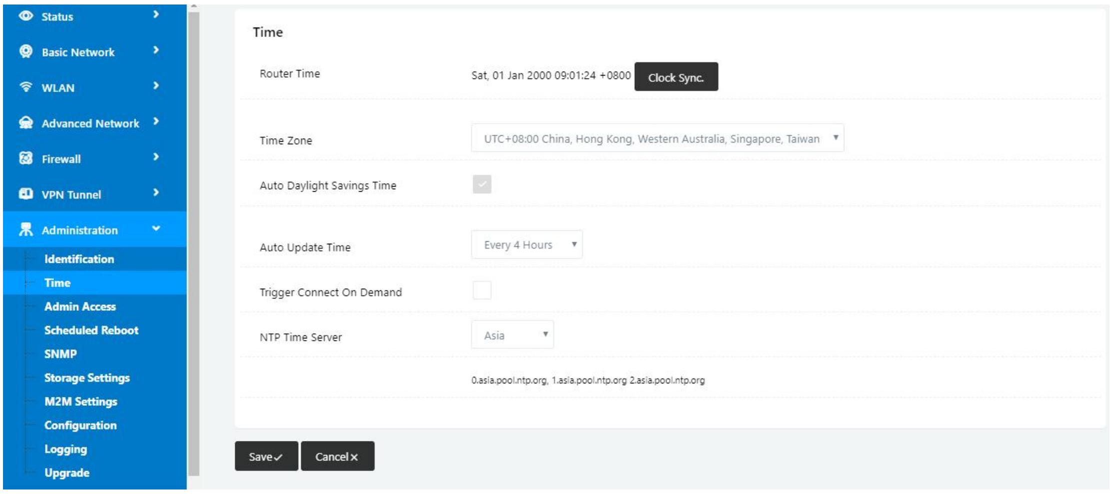
Parameter	Instruction
Router name	Default is router, can be set maximum 32 character
Host name	Default is router, can be set maximum 32 character
Domain name	Default is empty, support maximum up to 32 character, it is the domain of WAN, no need to configure for most application.

Step 2 Please click ”save” to finish

----End

3.12.2 Time Setting

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


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Identification
Time
Admin Access
Scheduled Reboot
SNMP
Storage Settings
M2M Settings
Configuration
Logging
Upgrade
Clock Sync.
Save✓
Cancel×

Time

Router Time Sat, 01 Jan 2000 09:01:24 +0800

Time Zone UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan

Auto Daylight Savings Time ☑

Auto Update Time Every 4 Hours

Trigger Connect On Demand ☐

NTP Time Server Asia

0.asia.pool.ntp.org, 1.asia.pool.ntp.org 2.asia.pool.ntp.org

CAUTION

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

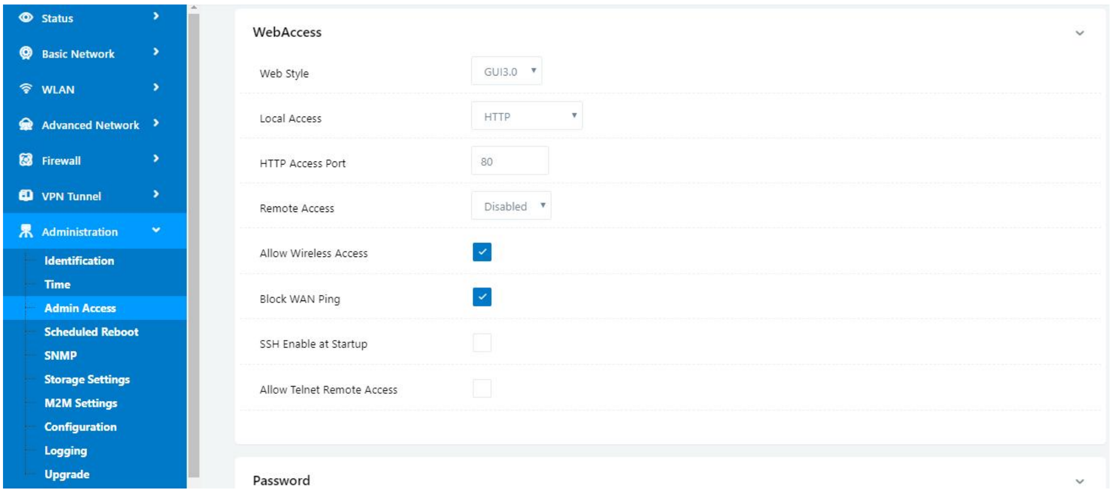
Step 2 Please click “save to finish.

----End

3.12.3 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.


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

WebAccess

Web Style: GUI3.0

Local Access: HTTP

HTTP Access Port: 80

Remote Access: Disabled

Allow Wireless Access ☑

Block WAN Ping ☑

SSH Enable at Startup ☐

Allow Telnet Remote Access ☐

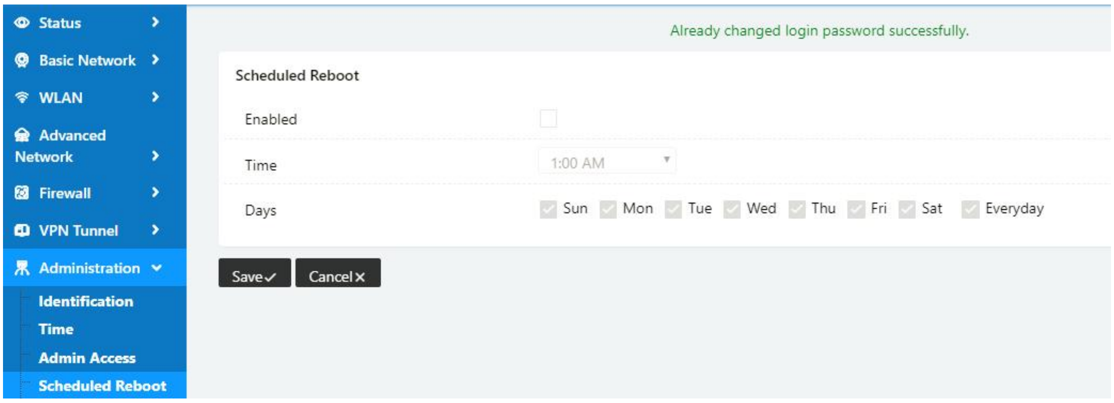
Password

Step 2 Please click save iron to finish the setting

----End

3.12.4 Schedule Reboot Setting

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


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Identification
Time
Admin Access
Scheduled Reboot
Save
Cancel

Already changed login password successfully.

Scheduled Reboot

Enabled ☐

Time: 1:00 AM

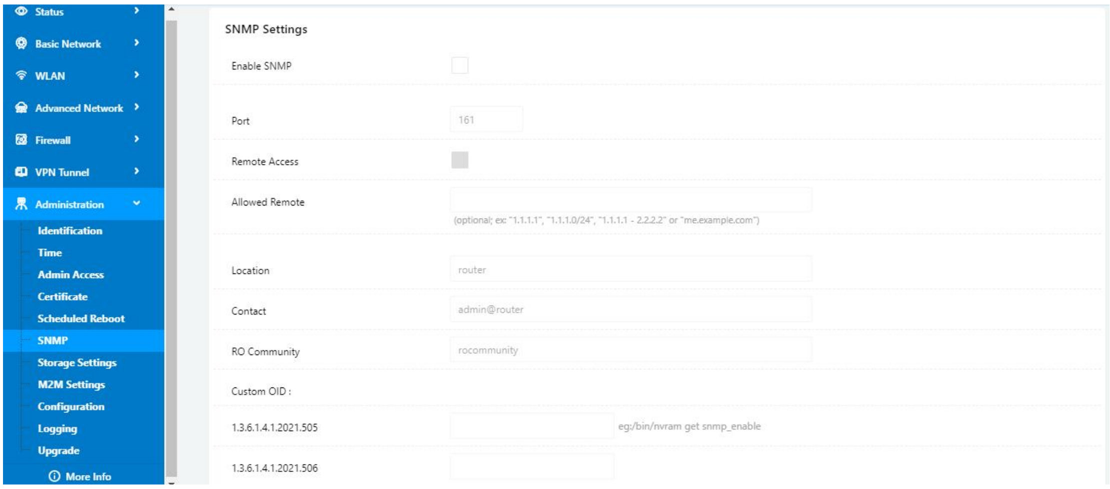
Days: ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Everyday

Step 2 Please click save iron to finish the setting

----End

3.12.5 SNMP Setting

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


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Identification
Time
Admin Access
Certificate
Scheduled Reboot
SNMP
Storage Settings
M2M Settings
Configuration
Logging
Upgrade
More Info

SNMP Settings

Enable SNMP ☐

Port 161

Remote Access ☐

Allowed Remote
(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com")

Location router

Contact admin@router

RO Community rocommunity

Custom OID :

1.3.6.1.4.1.2021.505 eg:/bin/nvram get snmp_enable

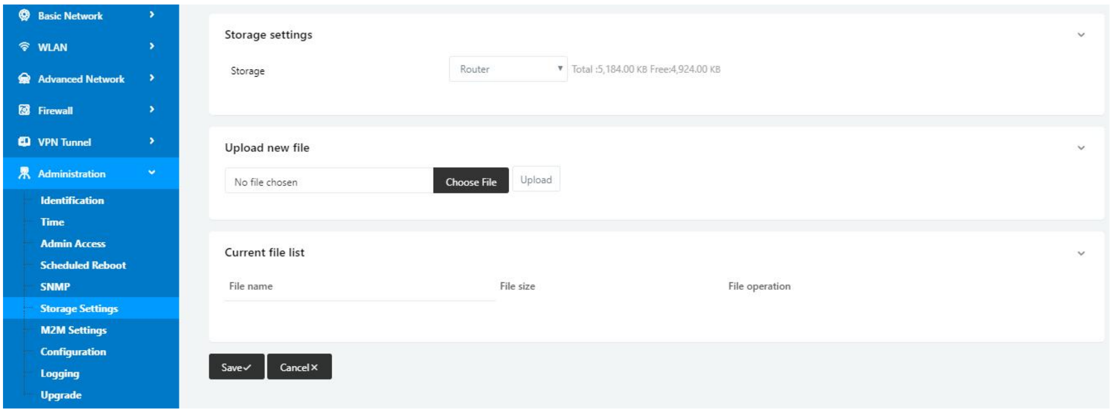
1.3.6.1.4.1.2021.506

Step 2 Please click save iron to finish the setting

----End

3.12.6 Storage Setting

Step 1 Please click “Administrator>Storage 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
Configuration
Logging
Upgrade
Choose File
Upload
Save✓
Cancel✕

Storage settings

Storage Router Total :5,184.00 KB Free:4,924.00 KB

Upload new file

No file chosen

Current file list

File name	File size	File operation

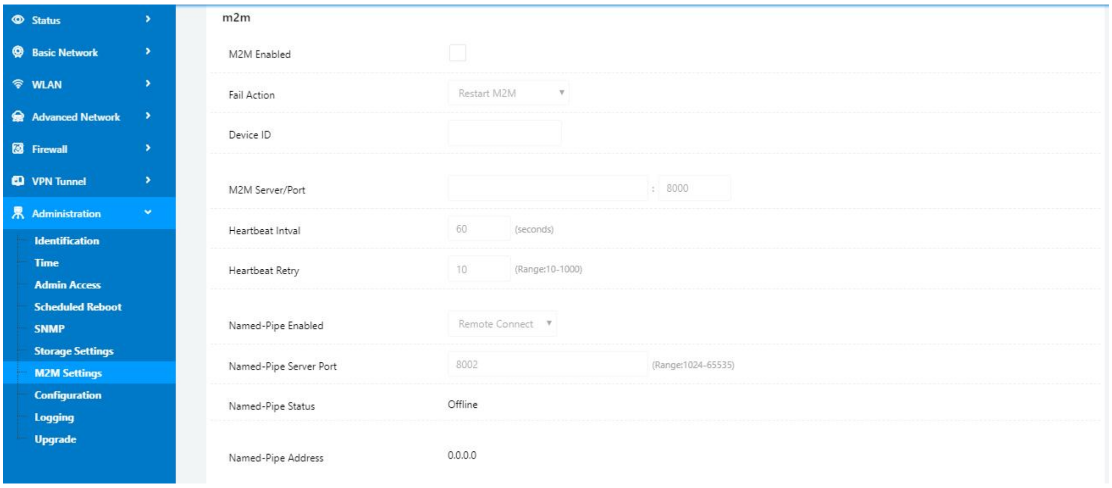
Step 2 Please click save iron to finish the setting

NOTE WL-R100/R200 series router doesn’t support extra storage. The storage path is Router as default.

----End

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

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


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

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

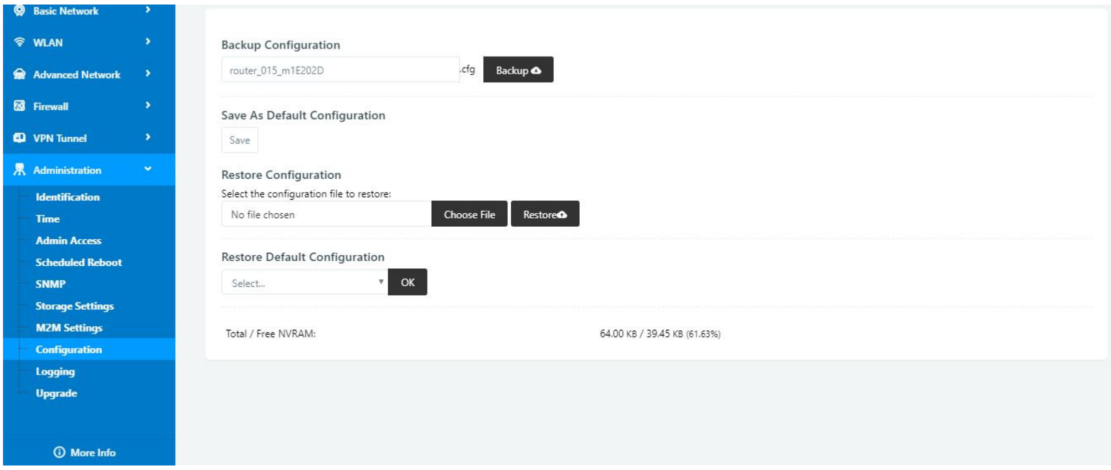
Named-Pipe Address: 0.0.0.0

Step 2 Please click save iron to finish the setting

----End

3.12.8 Configuration Setting

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


Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Identification
Time
Admin Access
Scheduled Reboot
SNMP
Storage Settings
M2M Settings
Configuration
Logging
Upgrade
More Info
Backup
Save
Choose File
Restore
OK

Backup Configuration

router_015_m1E202D.cfg

Save As Default Configuration

Restore Configuration

Select the configuration file to restore:

No file chosen

Restore Default Configuration

Select...

Total / Free NVRAM: 64.00 KB / 39.45 KB (61.63%)

Figure 3-1 Backup and Restore Configuration GUI

CAUTION

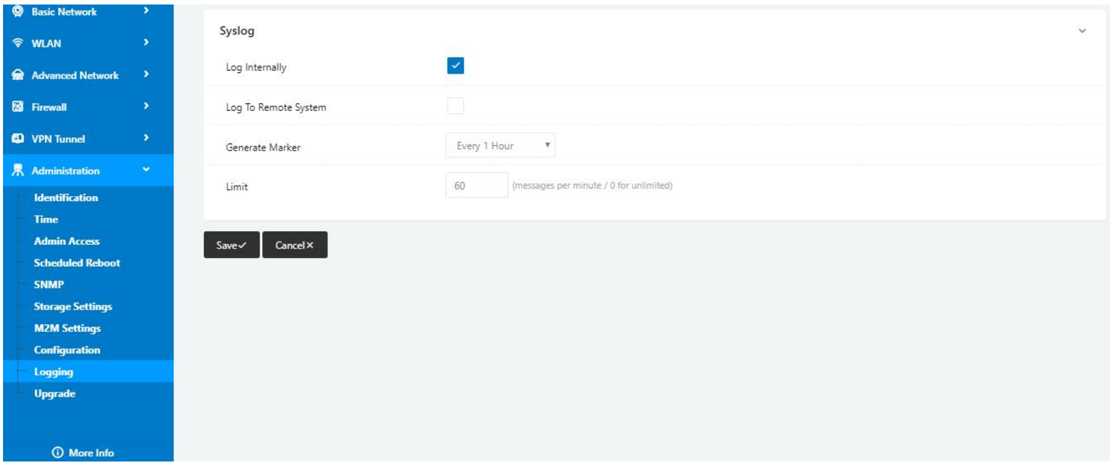
Restore Default would lose all configuration information, please be careful.

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

----End

3.12.9 System Log Setting

Step 3 Please click “Administrator> Logging” to start the configuration, you can set the file path to save the log (Local or remote sever).


Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Identification
Time
Admin Access
Scheduled Reboot
SNMP
Storage Settings
M2M Settings
Configuration
Logging
Upgrade
More Info
Save✓
Cancel✕

Syslog

Log Internally ☑

Log To Remote System ☐

Generate Marker: Every 1 Hour

Limit: 60 (messages per minute / 0 for unlimited)

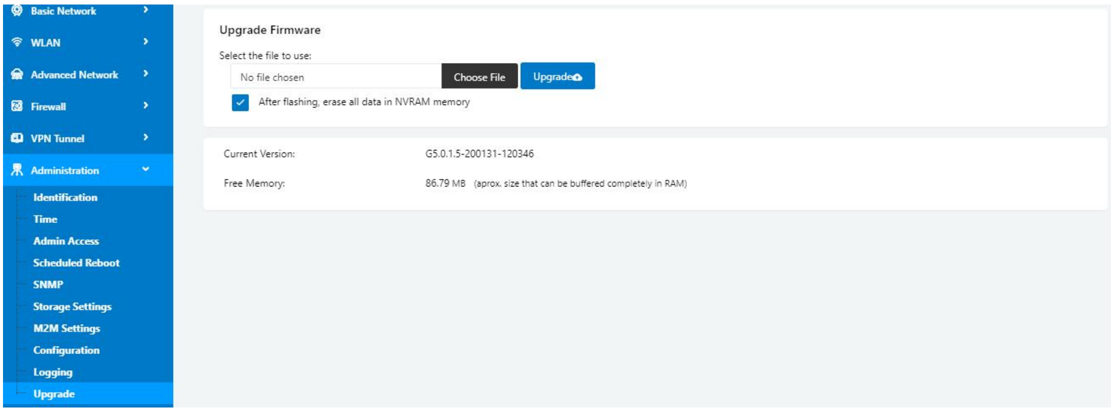
Figure 3-2 System log Setting GUI

Step 4 After configure, please click “Save” to finish.

----End

3.12.10 Firmware upgrade

Step 5 Please click “Administrator>firmware upgrade” to open upgrade firmware tab.


Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Identification
Time
Admin Access
Scheduled Reboot
SNMP
Storage Settings
M2M Settings
Configuration
Logging
Upgrade
Choose File
Upgrade

Upgrade Firmware

Select the file to use: No file chosen

☑ After flashing, erase all data in NVRAM memory

Current Version: G5.0.1.5-200131-120346

Free Memory: 86.79 MB (aprox. size that can be buffered completely in RAM)

Figure 3-3 Firmware Upgrade GUI

NOTE

Please don’t cut off the power during upgrading. The upgrade period is about 4mins.

3.12.11 “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-Rxx 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 2-34 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.

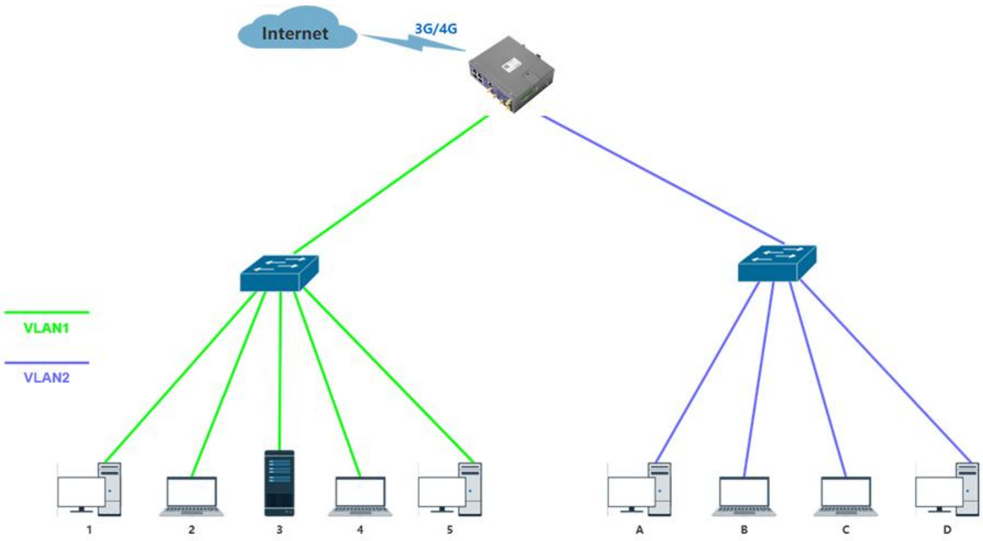
---

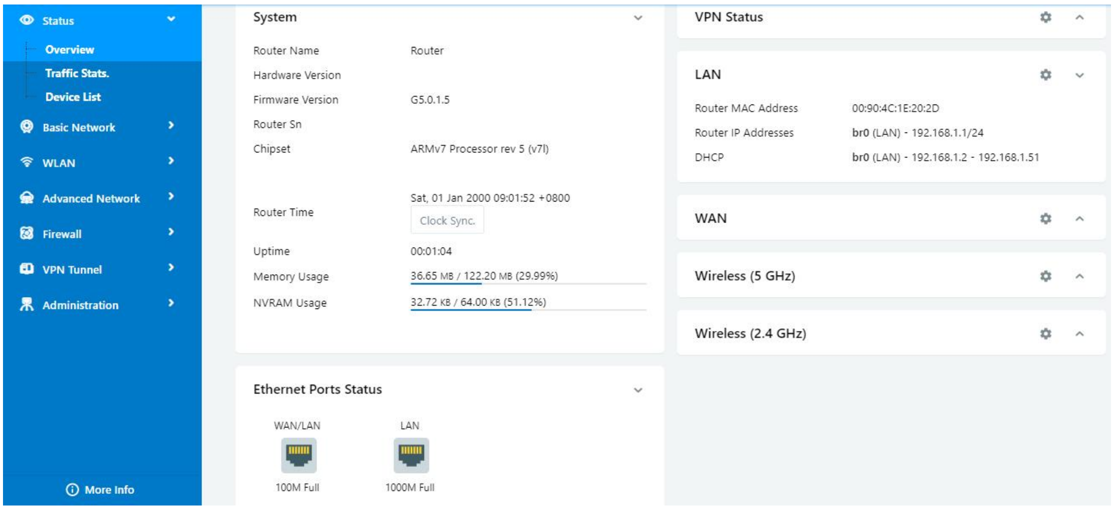
4 Configuration Instance

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.

4.1 VLAN

WL-R200/R210/R520 supports VLAN partition based on Ethernet port (LAN1~LAN5)


Internet
3G/4G
VLAN1
VLAN2
1
2
3
4
5
A
B
C
D


Status
Overview
Traffic Stats.
Device List
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Clock Sync.
VPN Status
WAN
Wireless (5 GHz)
Wireless (2.4 GHz)

System

Router Name Router
Hardware Version
Firmware Version G5.0.1.5
Router Sn
Chipset ARMv7 Processor rev 5 (v7l)
Router Time Sat, 01 Jan 2000 09:01:52 +0800
Uptime 00:01:04
Memory Usage 36.65 MB / 122.20 MB (29.99%)
NVRAM Usage 32.72 KB / 64.00 KB (51.12%)

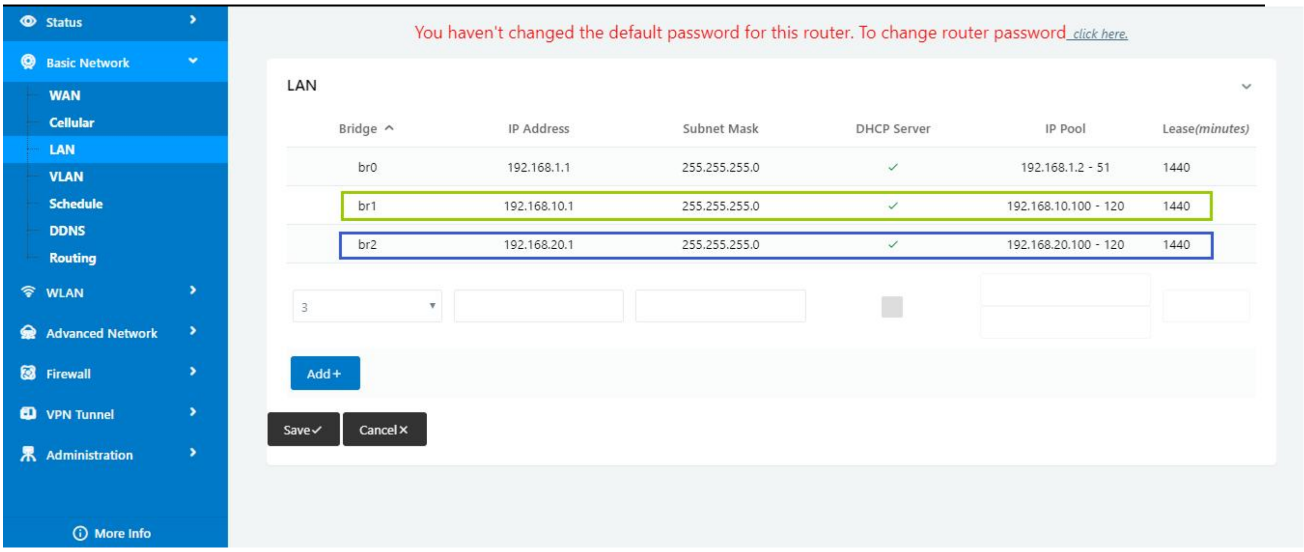
Ethernet Ports Status

WAN/LAN 100M Full
LAN 1000M Full

LAN

Router MAC Address 00:90:4C:1E:20:2D
Router IP Addresses br0 (LAN) - 192.168.1.1/24
DHCP br0 (LAN) - 192.168.1.2 - 192.168.1.51

1) Configure LAN with Basic Network.

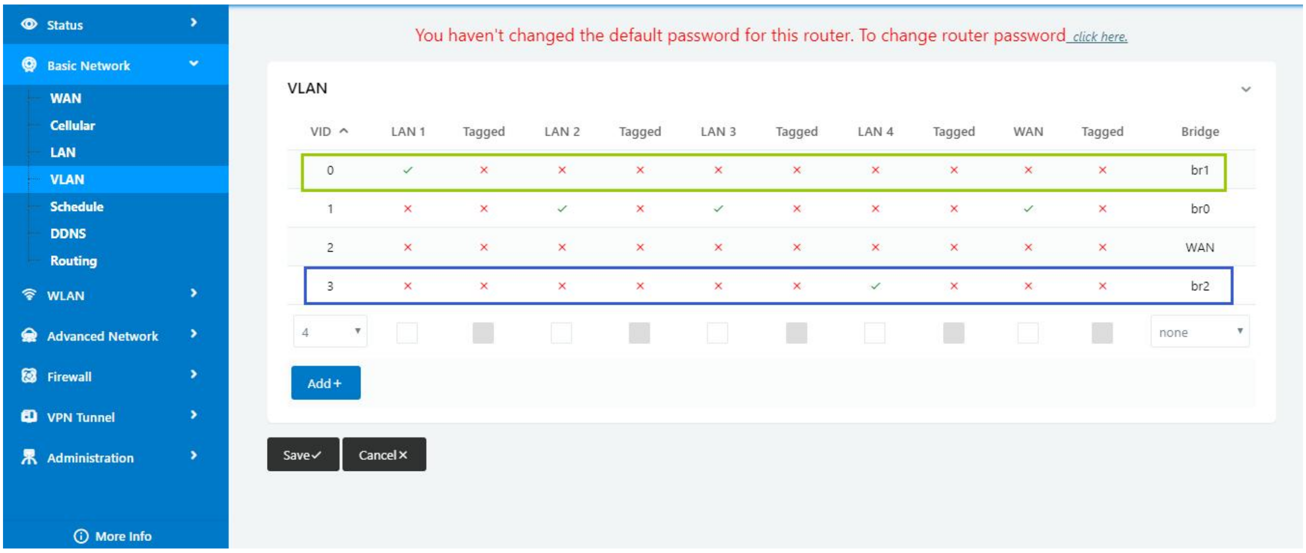

Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
3
Add +
Save ✓
Cancel ✕

You haven't changed the default password for this router. To change router password click here.

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
br1	192.168.10.1	255.255.255.0	✓	192.168.10.100 - 120	1440
br2	192.168.20.1	255.255.255.0	✓	192.168.20.100 - 120	1440

2) If untag for br1 ad br2, it won’t be accessed between SW1 and SW2.

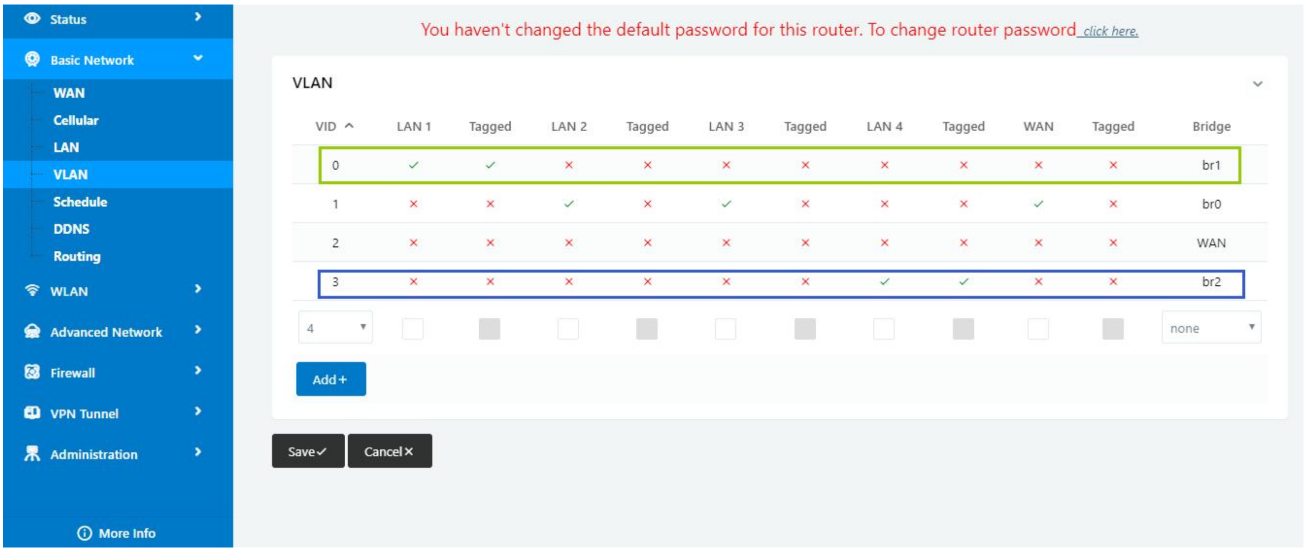

Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
4
none
Add +
Save ✓
Cancel ✕

You haven't changed the default password for this router. To change router password click here.

VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
0	✓	×	×	×	×	×	×	×	×	×	br1
1	×	×	✓	×	✓	×	×	×	✓	×	br0
2	×	×	×	×	×	×	×	×	×	×	WAN
3	×	×	×	×	×	×	✓	×	×	×	br2

3) If tag for br1 and br2, it will be accessed between sw1 and sw2.


Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
4
none
Add +
Save ✓
Cancel ✕

You haven't changed the default password for this router. To change router password click here.

VLAN

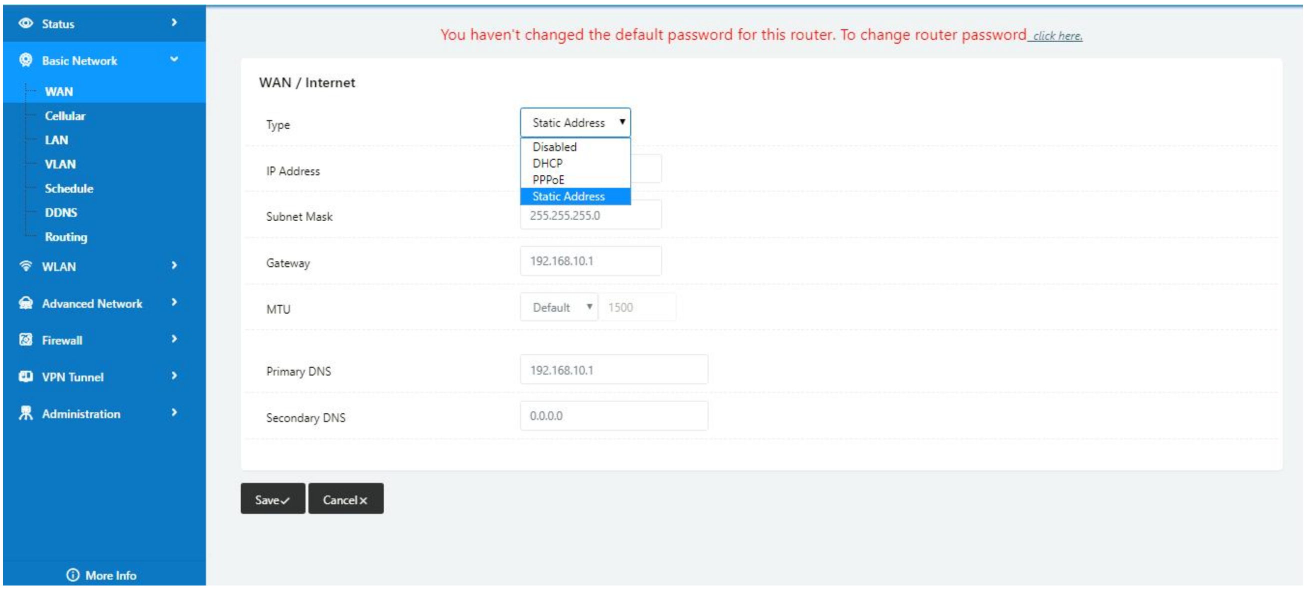
VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
0	✓	✓	×	×	×	×	×	×	×	×	br1
1	×	×	✓	×	✓	×	×	×	✓	×	br0
2	×	×	×	×	×	×	×	×	×	×	WAN
3	×	×	×	×	×	×	✓	✓	×	×	br2

---End

4.2 WAN Backup (WAN as Main, Cellular Backup)

The WAN and Cellular backup feature can quickly switch traffic to Cellular (link2) when WAN (link1) fails, and WL-Rxx brings you a stable network experience.

1) Navigate to Basic **Network > WAN**, you may configure the WAN parameters with your situation


Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Disabled
DHCP
PPPoE
Static Address
Save✓
Cancel×

You haven't changed the default password for this router. To change router password click here.

WAN / Internet

Type: Static Address

IP Address:

Subnet Mask: 255.255.255.0

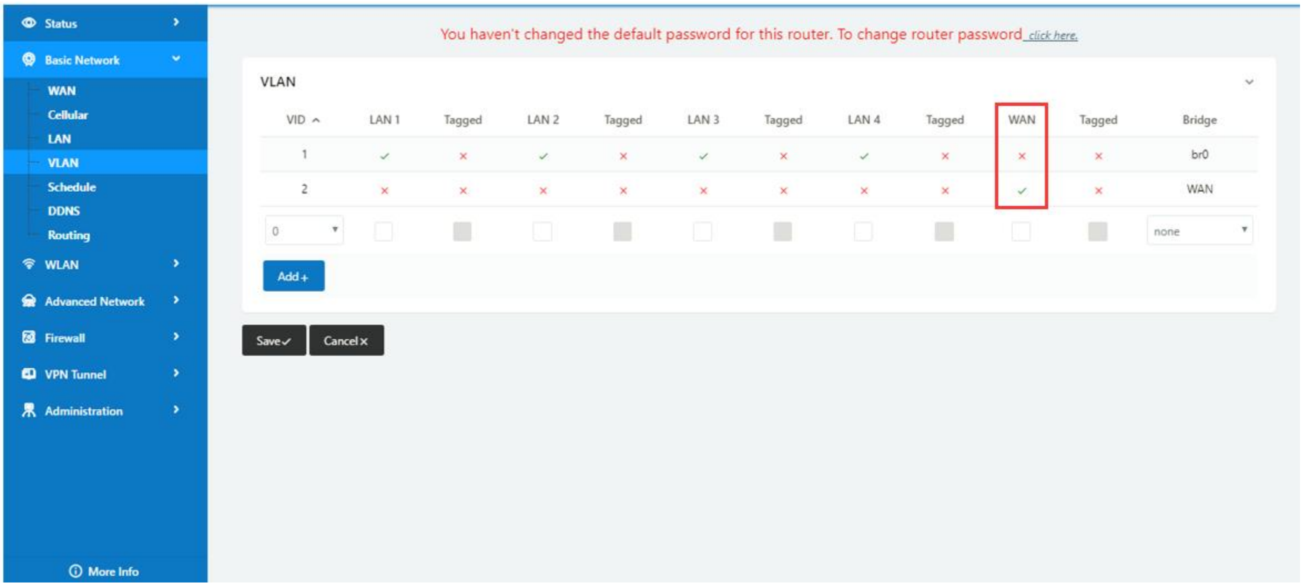
Gateway: 192.168.10.1

MTU: Default 1500

Primary DNS: 192.168.10.1

Secondary DNS: 0.0.0.0

2) Navigate to **Basic Network > VLAN**, enable the LAN1 as WAN Ethernet

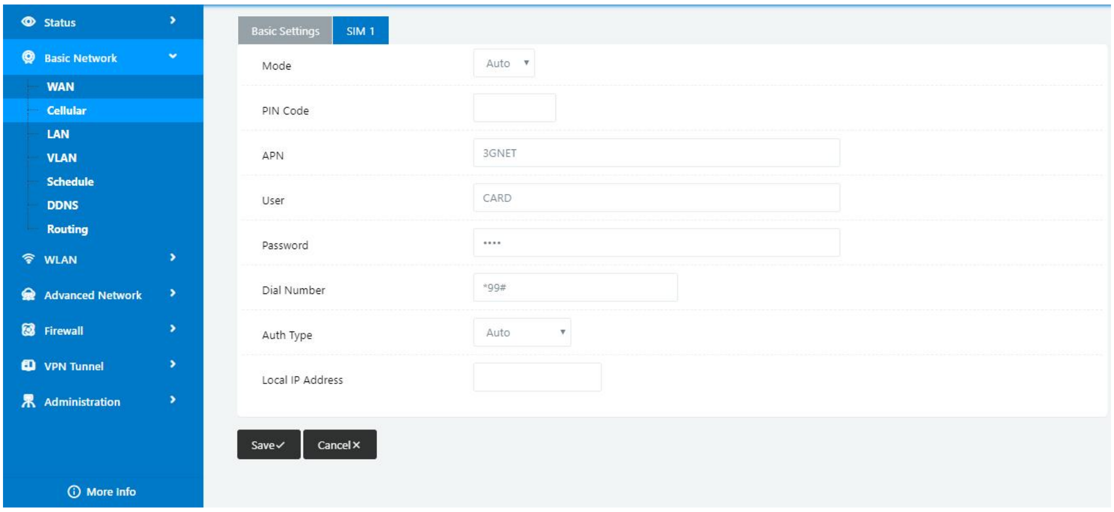

Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Add +
Save✓
Cancel×

You haven't changed the default password for this router. To change router password click here.

VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	×	✓	×	✓	×	✓	×	×	×	br0
2	×	×	×	×	×	×	×	×	✓	×	WAN
0	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	none

3) Navigate to **Basic network > Cellular**, configure the APN as your SIM

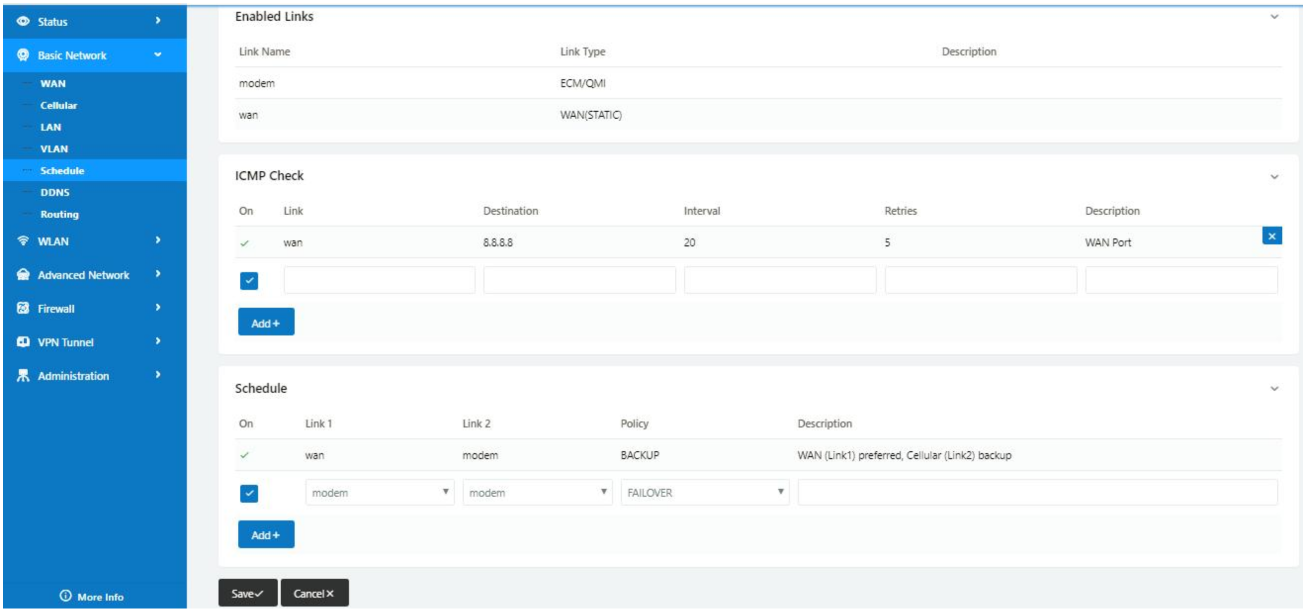

Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Basic Settings
SIM 1
Save
Cancel

Mode	Auto
PIN Code	
APN	3GNET
User	CARD
Password	····
Dial Number	*99#
Auth Type	Auto
Local IP Address	

4) Navigate to **Basic Network > Schedule**, configure WAN (Link1) preferred, Cellular backup (Link2)

Add ICMP Check to WAN

Set the working mode (Schedule)


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

Enabled Links

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

ICMP Check

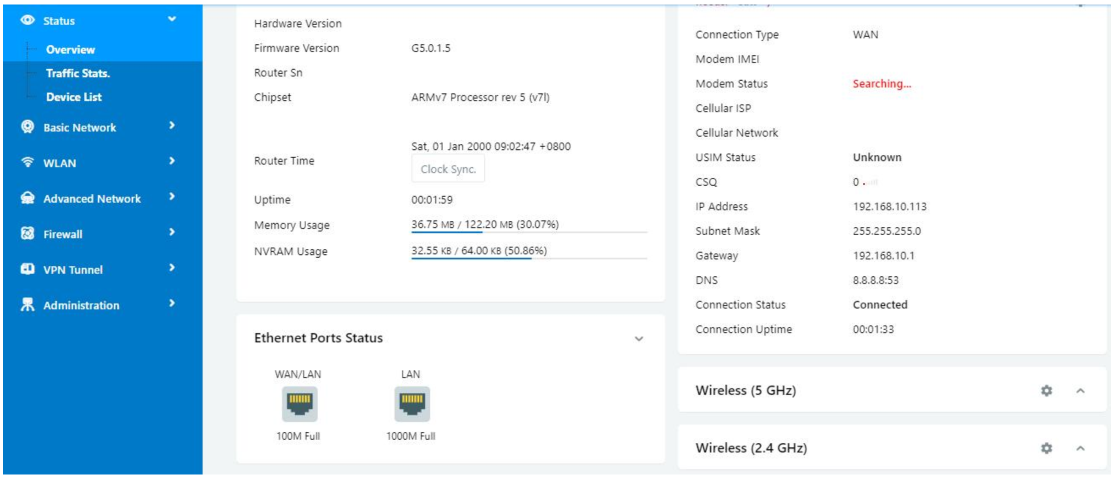
On	Link	Destination	Interval	Retries	Description
✓	wan	8.8.8.8	20	5	WAN Port
☑					

Schedule

On	Link 1	Link 2	Policy	Description
✓	wan	modem	BACKUP	WAN (Link1) preferred, Cellular (Link2) backup
☑	modem	modem	FAILOVER	

Parameters	Instruction
modem	The router dial-up to network via modem
wan	The router dial-up to network via WAN (DHCP, PPPOE, Static IP) Ethernet
ICMP Check	When the ICMP Check fails, the switching action between Link1 and Link2 will be triggered
Link1	The preferred link
Link2	The alternate link
BACKUP	Backup mode, Link1 and Link2 will remain online at the same time
FAILOVER	Failover mode, Link2 will dial-up to network when link1 fails

5) Status: WAN working


Status
Overview
Traffic Stats.
Device List
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
Clock Sync.
Ethernet Ports Status
WAN/LAN
100M Full
LAN
1000M Full
Wireless (5 GHz)
Wireless (2.4 GHz)

Hardware Version	
Firmware Version	G5.0.1.5
Router Sn	
Chipset	ARMv7 Processor rev 5 (v7l)
Router Time	Sat, 01 Jan 2000 09:02:47 +0800
Uptime	00:01:59
Memory Usage	36.75 MB / 122.20 MB (30.07%)
NVRAM Usage	32.55 KB / 64.00 KB (50.86%)

Connection Type	WAN
Modem IMEI	
Modem Status	Searching...
Cellular ISP	
Cellular Network	
USIM Status	Unknown
CSQ	0
IP Address	192.168.10.113
Subnet Mask	255.255.255.0
Gateway	192.168.10.1
DNS	8.8.8.8:53
Connection Status	Connected
Connection Uptime	00:01:33

6) The system quickly switches traffic to Cellular when the WAN fails

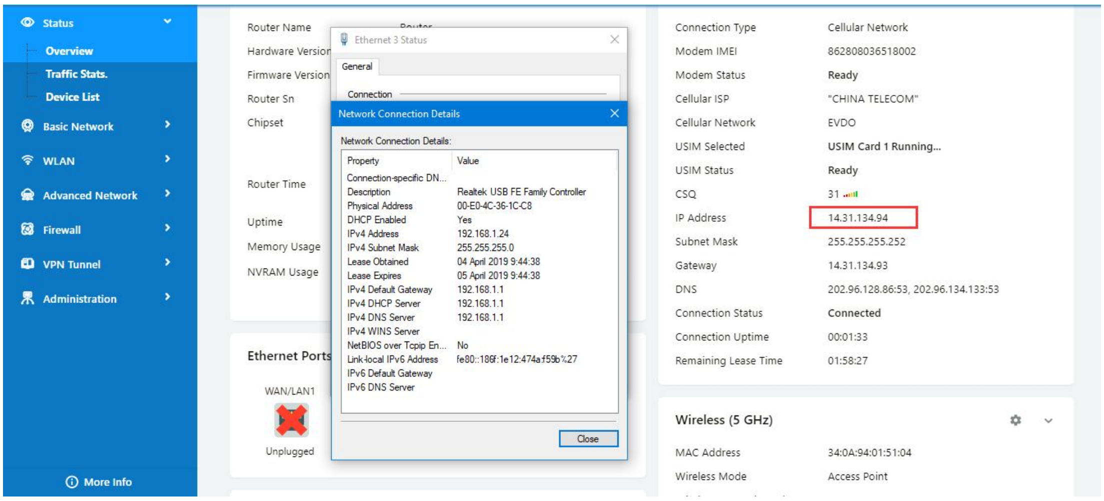
---End

4.3 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

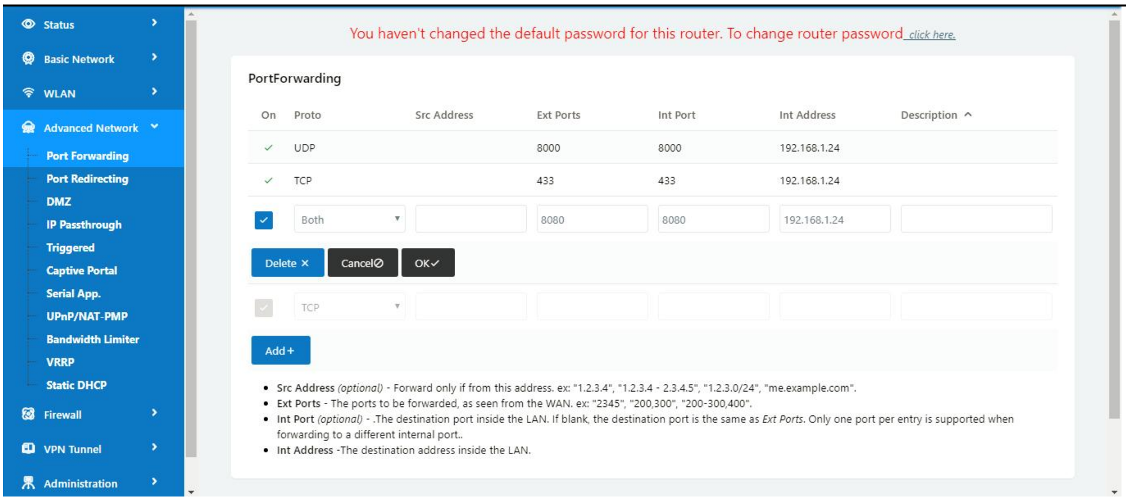

Status
Overview
Traffic Stats.
Device List
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Router Name
Hardware Version
Firmware Version
Router Sn
Chipset
Router Time
Uptime
Memory Usage
NVRAM Usage
Ethernet Ports
WAN/LAN1
Unplugged
Ethernet 3 Status
General
Connection
Network Connection Details
Close
Wireless (5 GHz)

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek USB FE Family Controller
Physical Address	00-E0-4C-36-1C-C8
DHCP Enabled	Yes
IPv4 Address	192.168.1.24
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	04 April 2019 9:44:38
Lease Expires	05 April 2019 9:44:38
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	No
Link-local IPv6 Address	fe80::186f:1e12:474a:f59b%27
IPv6 Default Gateway	
IPv6 DNS Server	

Connection Type	Cellular Network
Modem IMEI	862808036518002
Modem Status	Ready
Cellular ISP	"CHINA TELECOM"
Cellular Network	EVDO
USIM Selected	USIM Card 1 Running...
USIM Status	Ready
CSQ	31
IP Address	14.31.134.94
Subnet Mask	255.255.255.252
Gateway	14.31.134.93
DNS	202.96.128.86:53, 202.96.134.133:53
Connection Status	Connected
Connection Uptime	00:01:33
Remaining Lease Time	01:58:27
MAC Address	34:0A:94:01:51:04
Wireless Mode	Access Point

3) Configuration


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
Delete ×
Cancel⊘
OK✓
Add+

You haven't changed the default password for this router. To change router password click here.

PortForwarding

On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description
✓	UDP		8000	8000	192.168.1.24	
✓	TCP		433	433	192.168.1.24	
☑	Both		8080	8080	192.168.1.24	
☑	TCP					

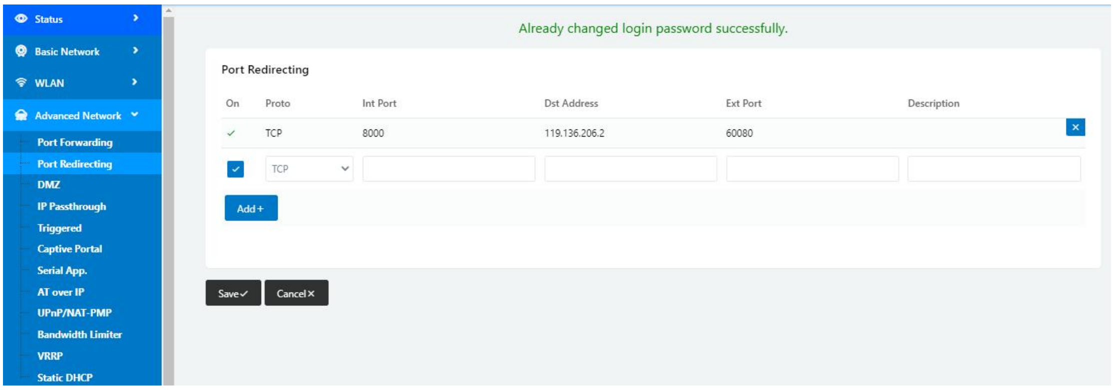
- **Src Address** *(optional)* - Forward only if from this address. ex: "1.2.3.4", "1.2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.example.com".
- **Ext Ports** - The ports to be forwarded, as seen from the WAN. ex: "2345", "200,300", "200-300,400".
- **Int Port** *(optional)* - .The destination port inside the 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** -The destination address inside the LAN.

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

---End

4.4 Port Redirecting

Please click "Advanced Network> Port Redirecting" to check or modify the relevant parameter.

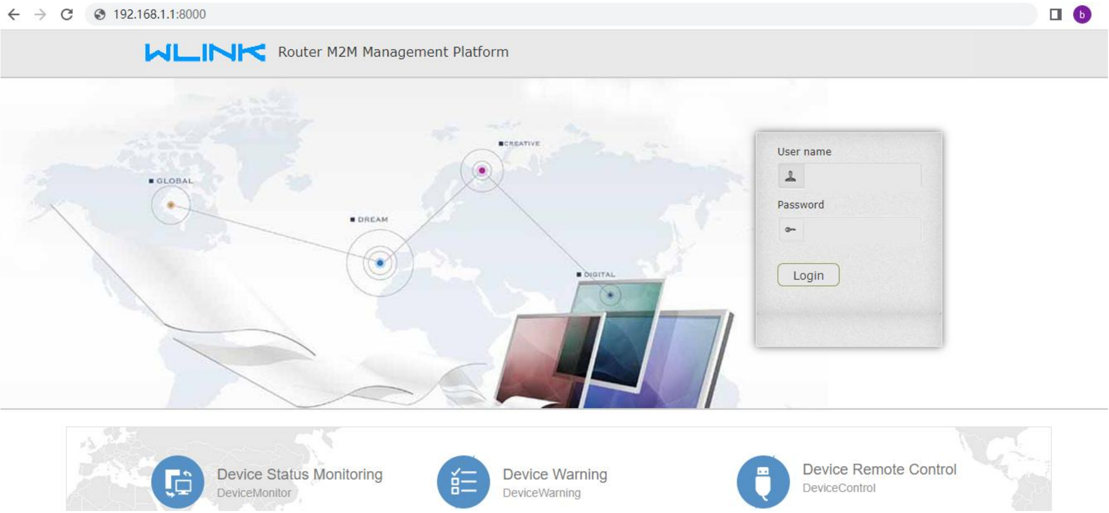

Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
AT over IP
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Add+
Save✓
Cancel×

Already changed login password successfully.

Port Redirecting

On	Proto	Int Port	Dst Address	Ext Port	Description
✓	TCP	8000	119.136.206.2	60080	
☑	TCP				

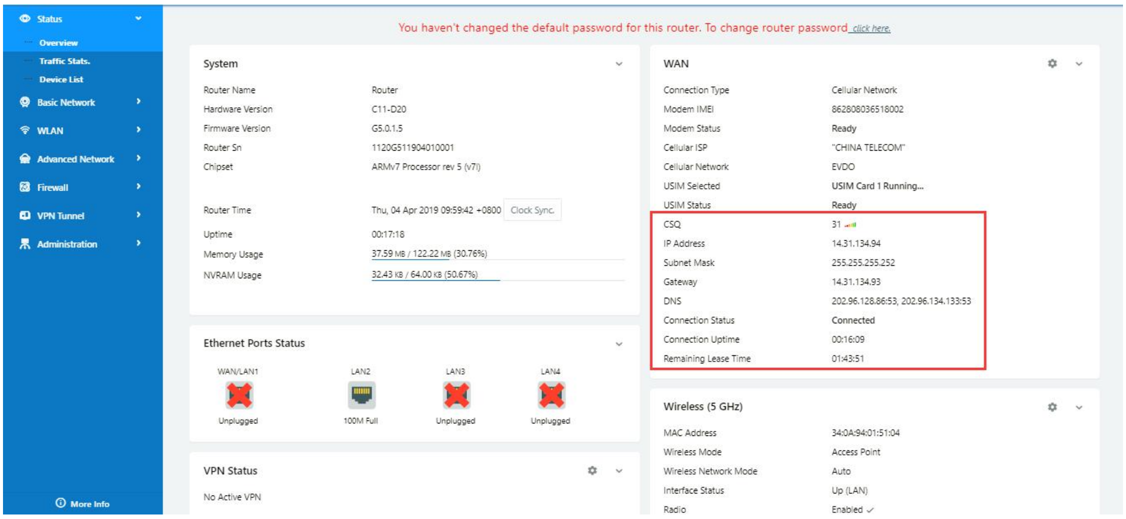
Configure Internal port as 8000, the Destination IP address as 119.136.206.2 and External port 60080(M2M Platform Server IP and Port as example). Access to 192.168.1.1:8000 in browser, the router will redirect to 119.136.206.2: 60080.


192.168.1.1:8000
Router M2M Management Platform
GLOBAL
CREATIVE
DREAM
DIGITAL
User name
Password
Login
Device Status Monitoring
DeviceMonitor
Device Warning
DeviceWarning
Device Remote Control
DeviceControl

---End

4.5 IP Passthrough

1) The router online


Status
Overview
Traffic Stats.
Device List
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info

You haven't changed the default password for this router. To change router password click here.

System

Router Name	Router
Hardware Version	C11-D20
Firmware Version	G5.0.1.5
Router Sn	1120G511904010001
Chipset	ARMv7 Processor rev 5 (v7l)
Router Time	Thu, 04 Apr 2019 09:59:42 +0800 Clock Sync.
Uptime	00:17:18
Memory Usage	37.59 MB / 122.22 MB (30.76%)
NVRAM Usage	32.43 KB / 64.00 KB (50.67%)

Ethernet Ports Status

WAN/LAN1	LAN2	LAN3	LAN4
Unplugged	100M Full	Unplugged	Unplugged

VPN Status

No Active VPN

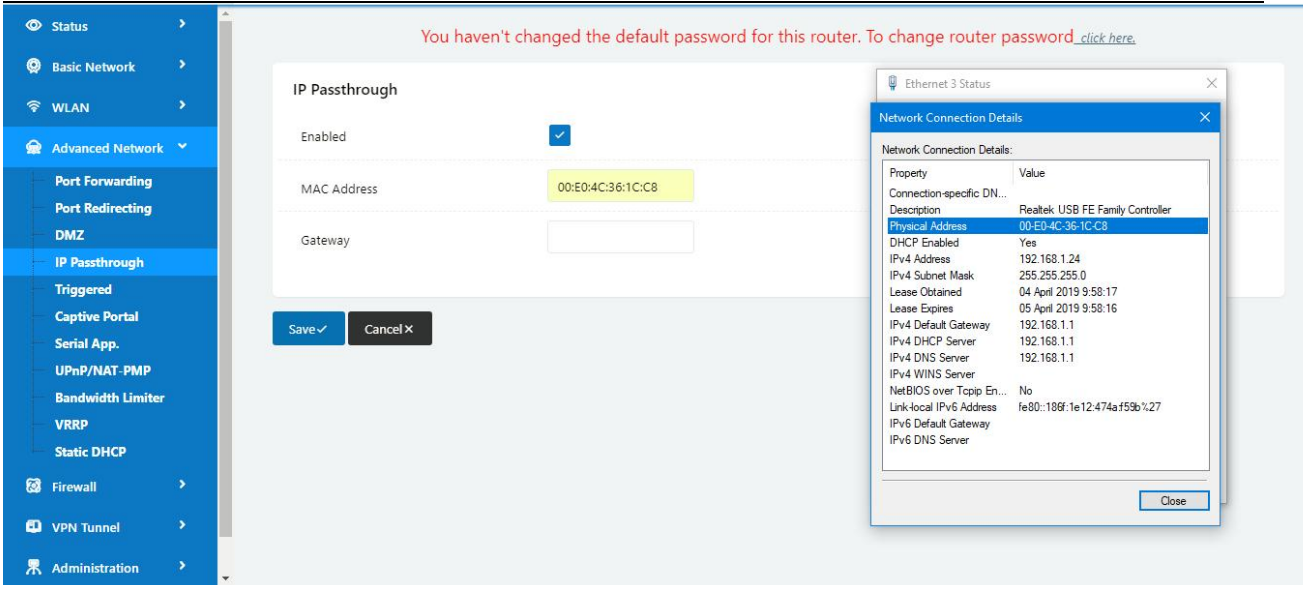
WAN

Connection Type	Cellular Network
Modem IMEI	862808036518002
Modem Status	Ready
Cellular ISP	"CHINA TELECOM"
Cellular Network	EVDO
USIM Selected	USIM Card 1 Running...
USIM Status	Ready
CSQ	31
IP Address	14.31.134.94
Subnet Mask	255.255.255.252
Gateway	14.31.134.93
DNS	202.96.128.86:53, 202.96.134.133:53
Connection Status	Connected
Connection Uptime	00:16:09
Remaining Lease Time	01:43:51

Wireless (5 GHz)

MAC Address	34:0A:94:01:51:04
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up (LAN)
Radio	Enabled ✓

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
Save ✓
Cancel ✕
Ethernet 3 Status
Close

You haven't changed the default password for this router. To change router password click here.

IP Passthrough

Enabled ☑

MAC Address 00:E0:4C:36:1C:C8

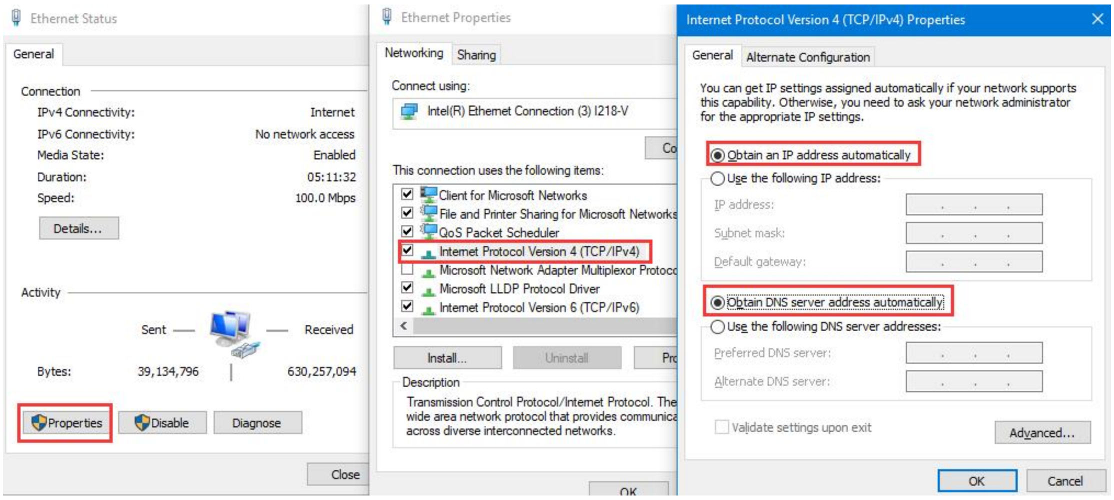
Gateway

Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek USB FE Family Controller
Physical Address	00-E0-4C-36-1C-C8
DHCP Enabled	Yes
IPv4 Address	192.168.1.24
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	04 April 2019 9:58:17
Lease Expires	05 April 2019 9:58:16
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	No
Link-local IPv6 Address	fe80::186f:1e12:474a:f59b%27
IPv6 Default Gateway	
IPv6 DNS Server	

3) Set the PC to DHCP


Ethernet Status
General
Details...
Properties
Disable
Diagnose
Close
Ethernet Properties
Networking
Sharing
Install...
Uninstall
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
Advanced...
OK
Cancel

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 05:11:32

Speed: 100.0 Mbps

Activity

Sent — Received

Bytes: 39,134,796 | 630,257,094

Connect using:

Intel(R) Ethernet Connection (3) I218-V

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The wide area network protocol that provides communica across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

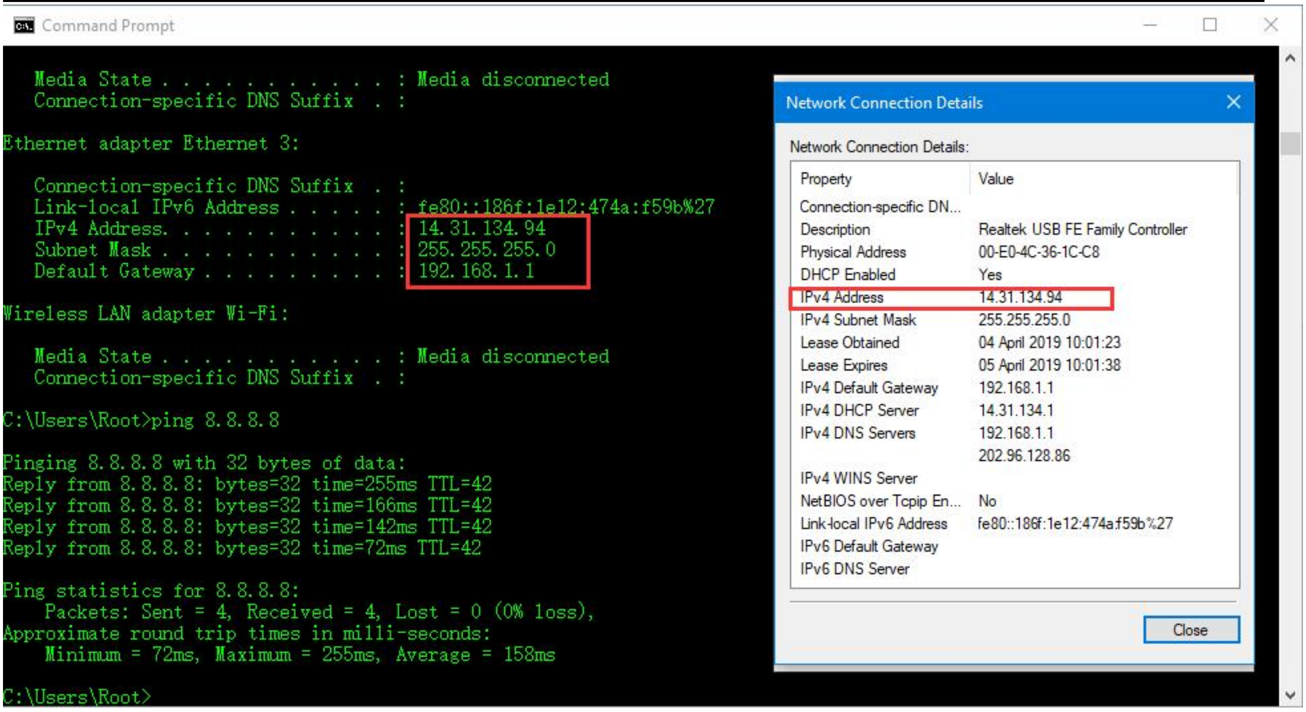
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

4) Check the Ethernet status and ping test

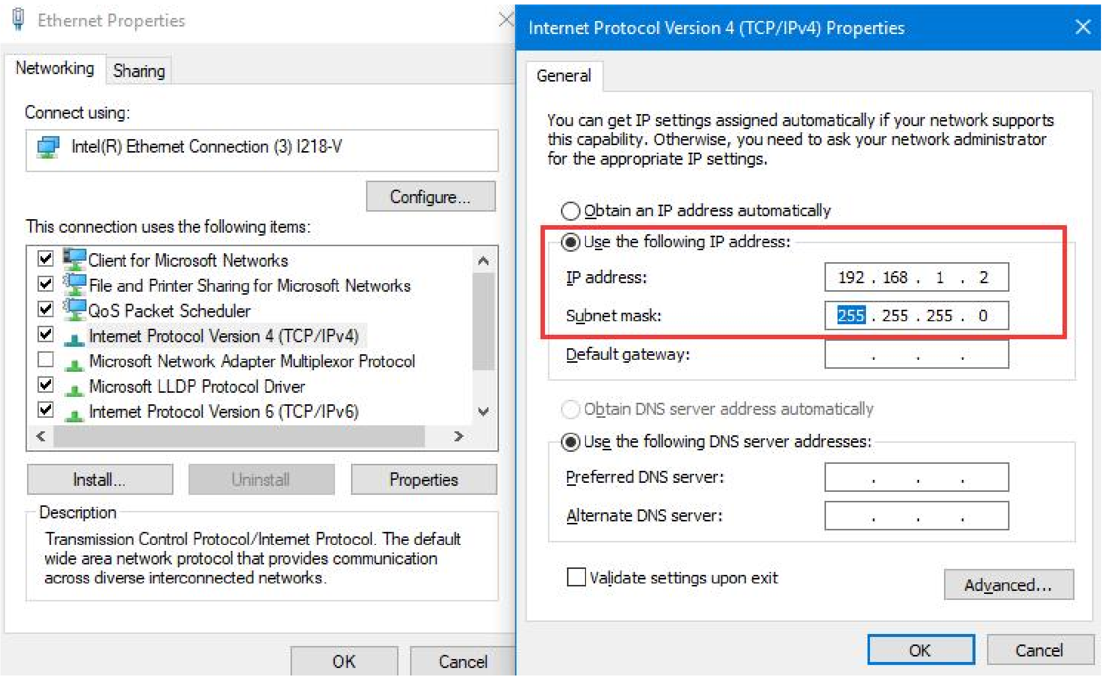


```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::186f:1e12:474a:f59b%27
   IPv4 Address. . . . . . . . . . . : 14.31.134.94
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Root>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=255ms TTL=42
Reply from 8.8.8.8: bytes=32 time=166ms TTL=42
Reply from 8.8.8.8: bytes=32 time=142ms TTL=42
Reply from 8.8.8.8: bytes=32 time=72ms TTL=42

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 72ms, Maximum = 255ms, Average = 158ms

C:\Users\Root>
```

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek USB FE Family Controller
Physical Address	00-E0-4C-36-1C-C8
DHCP Enabled	Yes
IPv4 Address	14.31.134.94
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	04 April 2019 10:01:23
Lease Expires	05 April 2019 10:01:38
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	14.31.134.1
IPv4 DNS Servers	192.168.1.1 202.96.128.86
IPv4 WINS Server	
NetBIOS over Tcpip En...	No
Link-local IPv6 Address	fe80::186f:1e12:474a:f59b%27
IPv6 Default Gateway	
IPv6 DNS Server	

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



Connect using:
Intel(R) Ethernet Connection (3) I218-V

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

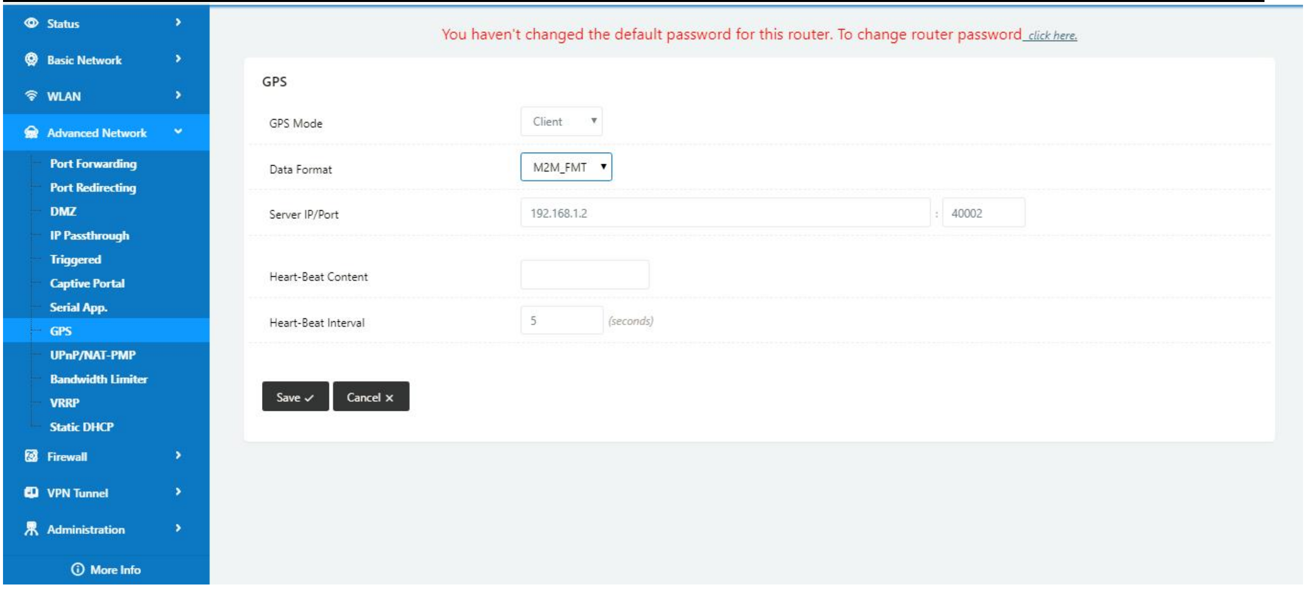
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

---End

4.6 GPS Settings

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


Status
Basic Network
WLAN
Advanced Network
Port Forwarding
Port Redirecting
DMZ
IP Passthrough
Triggered
Captive Portal
Serial App.
GPS
UPnP/NAT-PMP
Bandwidth Limiter
VRRP
Static DHCP
Firewall
VPN Tunnel
Administration
More Info
Save ✓
Cancel ×

You haven't changed the default password for this router. To change router password click here.

GPS

GPS Mode: Client

Data Format: M2M_FMT

Server IP/Port: 192.168.1.2 : 40002

Heart-Beat Content:

Heart-Beat Interval: 5 (seconds)

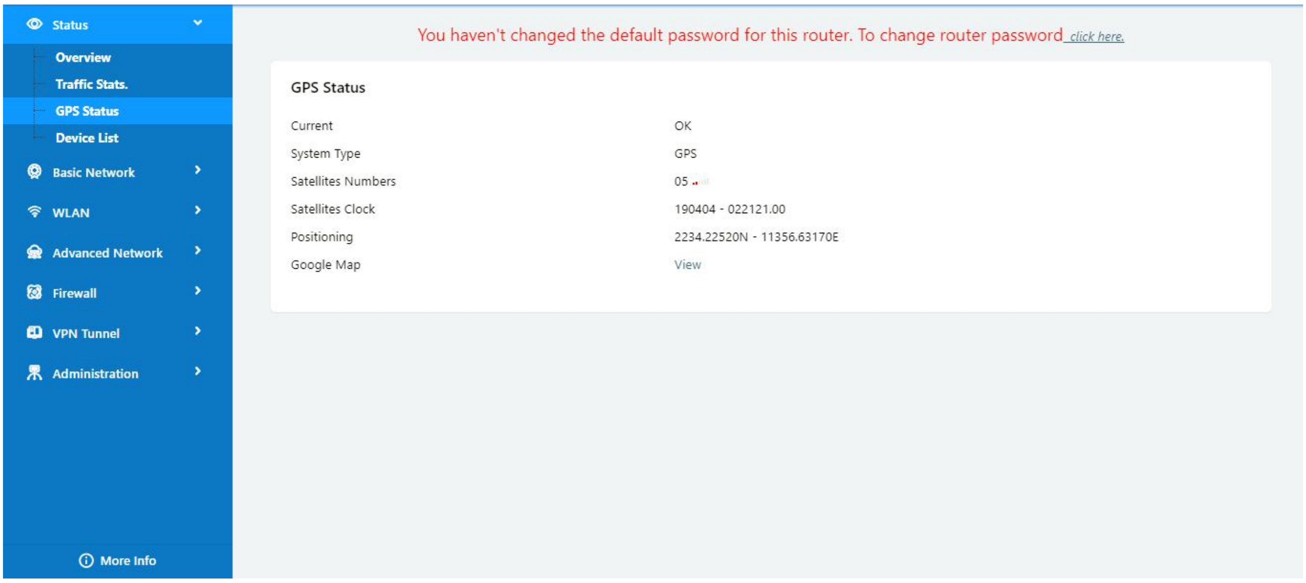
Table 4-6 "GPS" Instruction

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.
Interval	GPS data transmit as the interval time.

Step 1 Please click "save" to finis

Step 2 Connect the GPS antenna to router GPS interface

Step 3 Check GPS Status


Status
Overview
Traffic Stats.
GPS Status
Device List
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info

You haven't changed the default password for this router. To change router password click here.

GPS Status

Current: OK

System Type: GPS

Satellites Numbers: 05

Satellites Clock: 190404 - 022121.00

Positioning: 2234.22520N - 11356.63170E

Google Map: View

NOTE

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.sss	043215.0	UTC Time, Time of position fix.
4	gps_use	numeric	06	Satellites Used, Range 0 to 12.
5	gps_latitude	ddmm.mmmm	2234.248130	Latitude, Degrees + minutes.
6	gps_NS	character	N	N/S Indicator,N=north or S=south.
7	gps_longitude	ddmm.mmmm	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(Knots) over ground, units is kn/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.

---End

4.7 Firewall

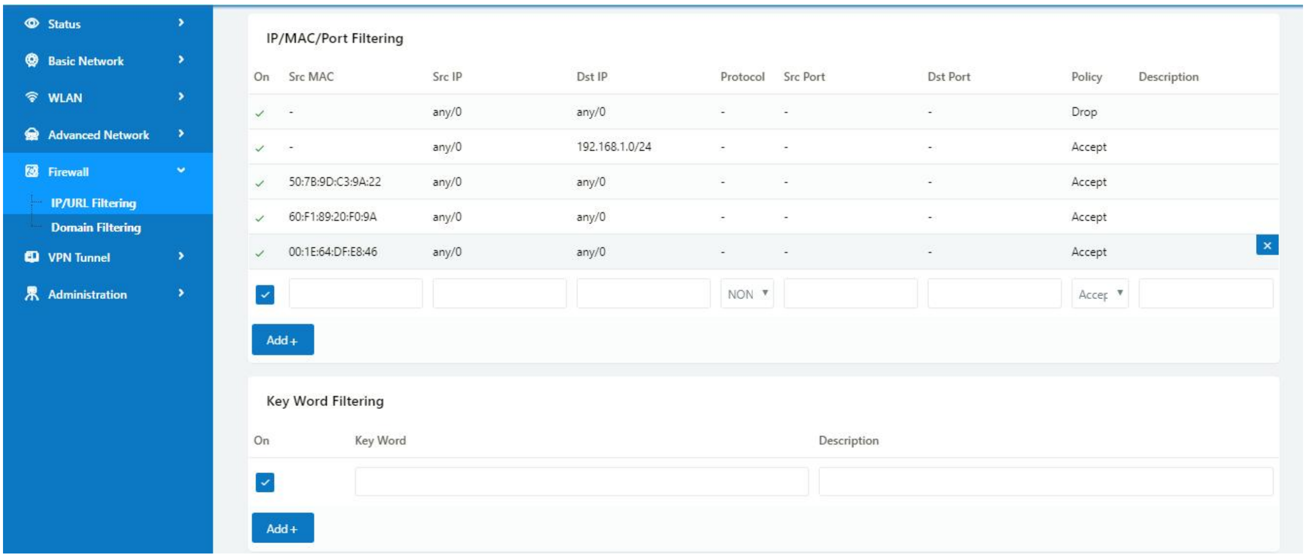
1) IP/MAC/Port Filtering

This part used to intercept packages from router’s WAN/Celluar interface to Internet.

Test case:

1.1 Only allow three devices (MAC/LAN/WLAN) can access to Internet via WAN: 110.110.10.10

1.2 Only allow three devices (MAC/LAN/WLAN) can access to the router page (192.168.1.1)


Status
Basic Network
WLAN
Advanced Network
Firewall
IP/URL Filtering
Domain Filtering
VPN Tunnel
Administration

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
✓	-	any/0	any/0	-	-	-	Drop	
✓	-	any/0	192.168.1.0/24	-	-	-	Accept	
✓	50:7B:9D:C3:9A:22	any/0	any/0	-	-	-	Accept	
✓	60:F1:89:20:F0:9A	any/0	any/0	-	-	-	Accept	
✓	00:1E:64:DF:E8:46	any/0	any/0	-	-	-	Accept	
☑				NON			Accep	

Add+

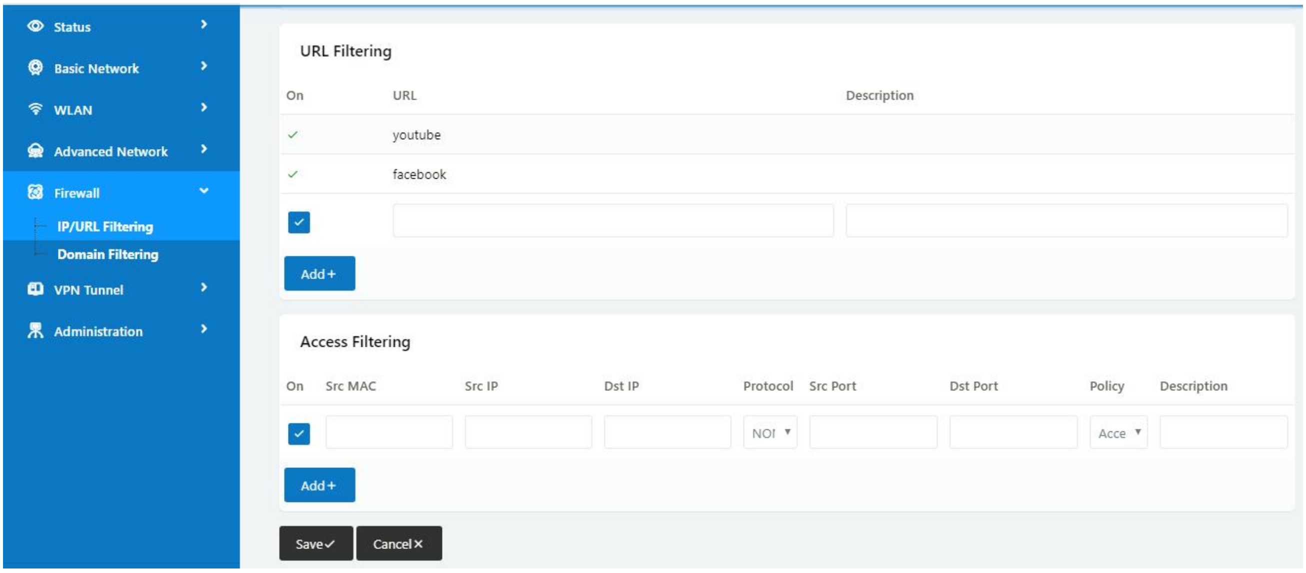
Key Word Filtering

On	Key Word	Description
☑		

Add+

2) Key Word Filtering

This part used to filter key word packages from router’s WAN/Cellular interface to Internet.


Status
Basic Network
WLAN
Advanced Network
Firewall
IP/URL Filtering
Domain Filtering
VPN Tunnel
Administration

URL Filtering

On	URL	Description
✓	youtube	
✓	facebook	
☑		

Add+

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NOI			Acce	

Add+
Save✓
Cancel×

3) URL Filtering

This part used to filter URL from router’s WAN/Cellular interface to Internet.

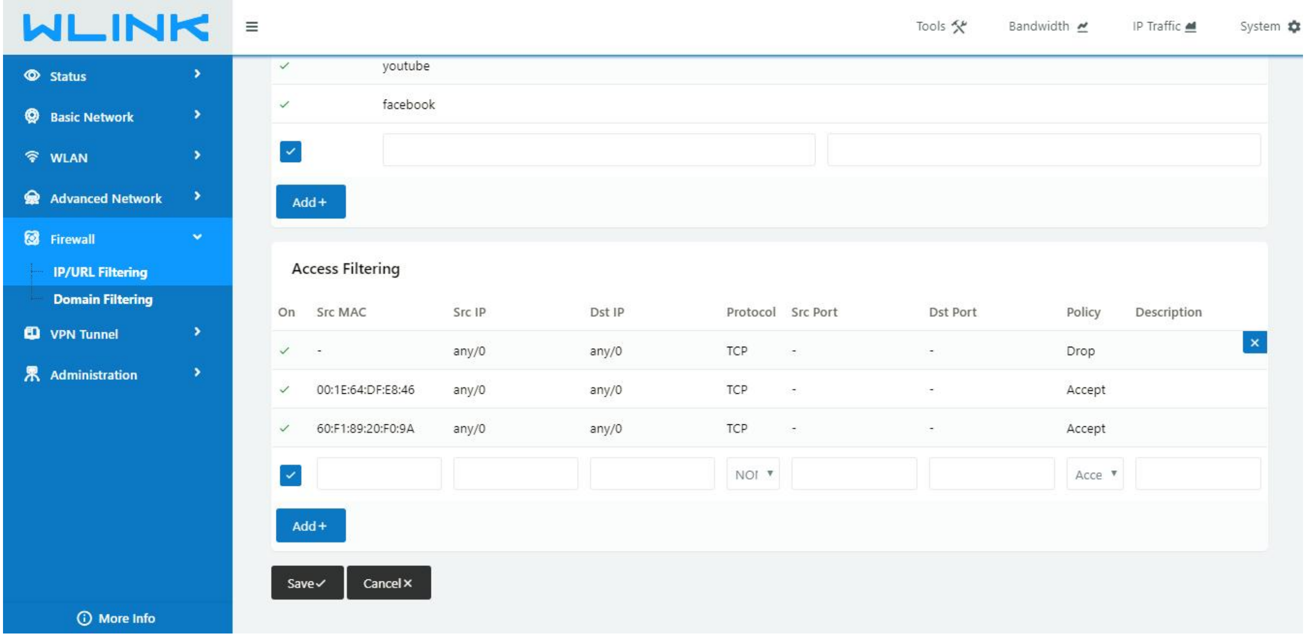
4) Access Filtering

This part used to filter packages from Internet to router’s WAN/Celluar interface.

Test case:

4.1) Intercept all TCP packets accessing the router's WAN/Celluar(110.110.10.10).

4.2) Only two devices (MAC/LAN/WLAN) are allowed to be accessed from Internet packets.


WLINK
Tools
Bandwidth
IP Traffic
System
Status
Basic Network
WLAN
Advanced Network
Firewall
IP/URL Filtering
Domain Filtering
VPN Tunnel
Administration
More Info
Add+
Add+
Save✓
Cancel✕

✓	youtube
✓	facebook
☑	

Access Filtering

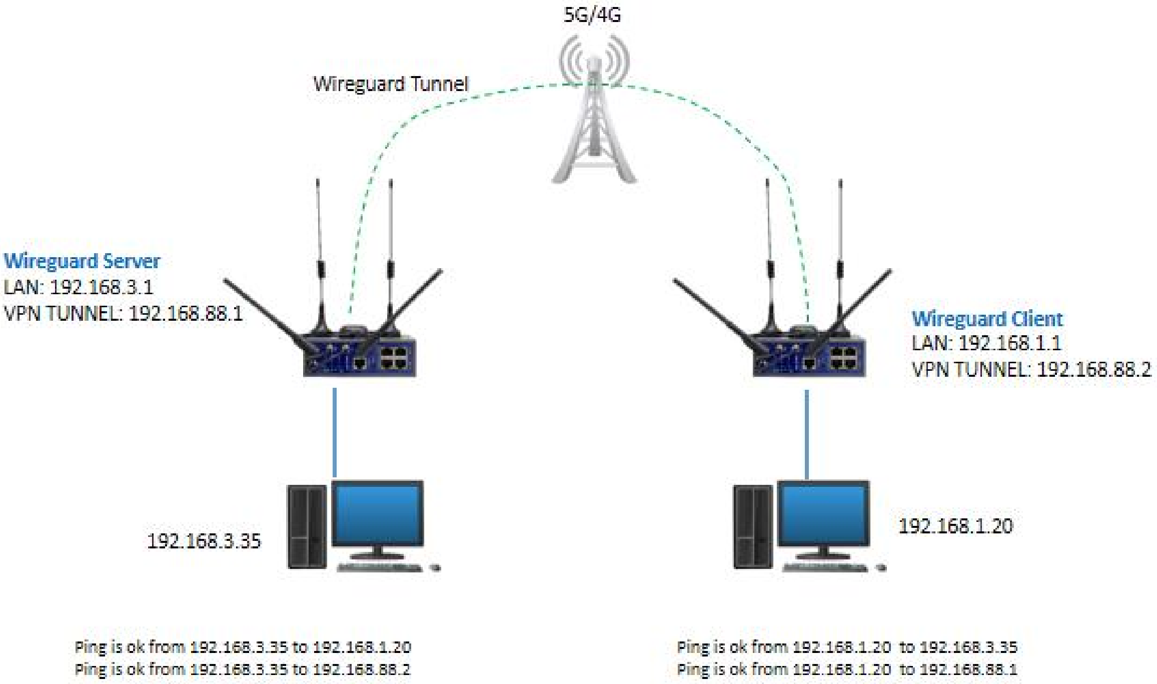
On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
✓	-	any/0	any/0	TCP	-	-	Drop	
✓	00:1E:64:DF:E8:46	any/0	any/0	TCP	-	-	Accept	
✓	60:F1:89:20:F0:9A	any/0	any/0	TCP	-	-	Accept	
☑				NOI ▾			Acce ▾	

---End

4.8 VPN Tunnel

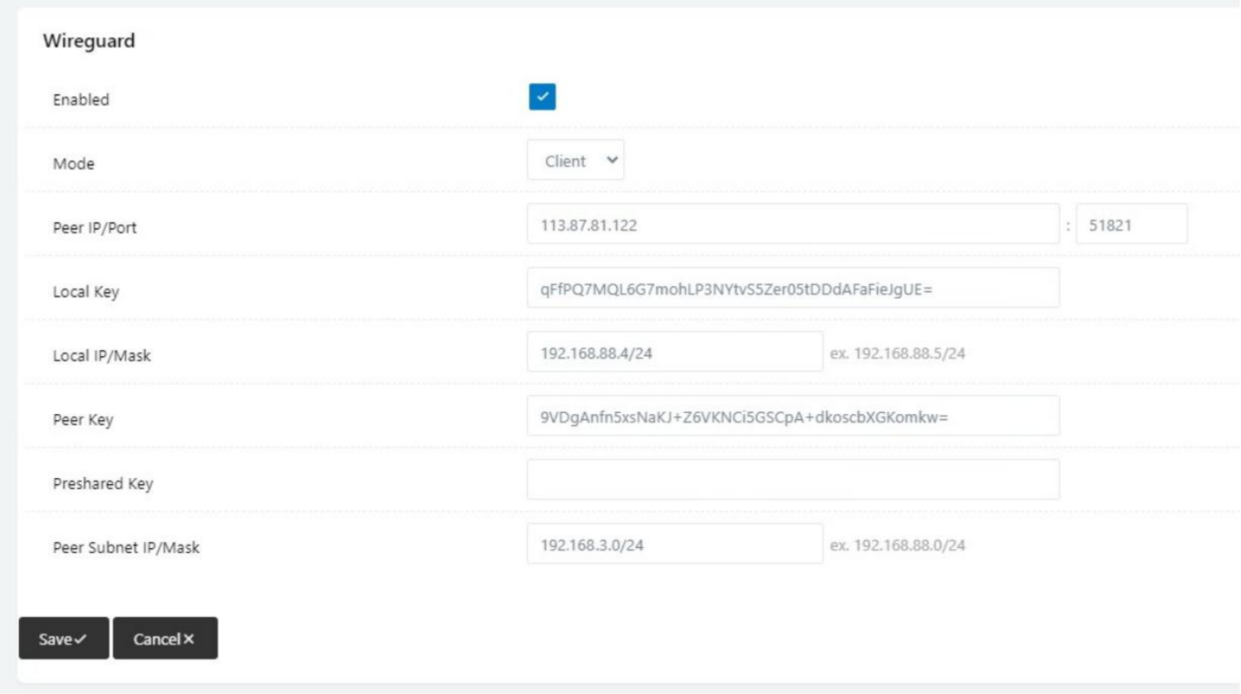
4.8.1 Wireguard VPN

Wireguard VPN between two WL-Rxx Routers


5G/4G
Wireguard Tunnel
Wireguard Server
LAN: 192.168.3.1
VPN TUNNEL: 192.168.88.1
Wireguard Client
LAN: 192.168.1.1
VPN TUNNEL: 192.168.88.2
192.168.3.35
192.168.1.20
Ping is ok from 192.168.3.35 to 192.168.1.20
Ping is ok from 192.168.3.35 to 192.168.88.2
Ping is ok from 192.168.1.20 to 192.168.3.35
Ping is ok from 192.168.1.20 to 192.168.88.1

1) Wireguard VPN Client Setting

Configure Wireguard Client as Server requested. Especially, the public Key and private key is generated by server or third party. Configure server public key in the peer key table and client private key in the local key table.



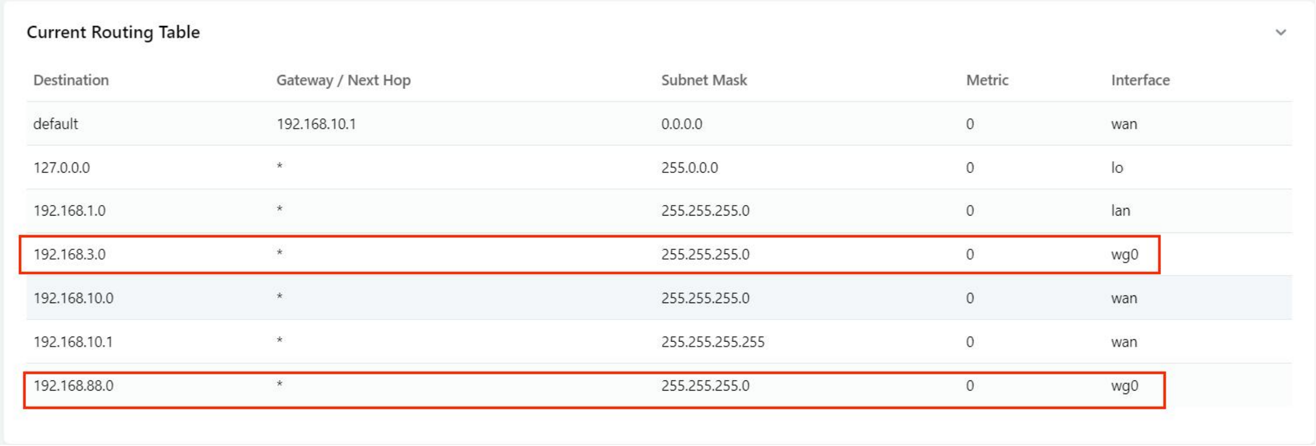
Wireguard

Enabled	☑
Mode	Client
Peer IP/Port	113.87.81.122 : 51821
Local Key	qFfPQ7MQL6G7mohLP3NYtvS5Zer05tDDdAFaFieJgUE=
Local IP/Mask	192.168.88.4/24 ex. 192.168.88.5/24
Peer Key	9VDgAnfn5xsNaKJ+Z6VKNCi5GSCpA+dkoscbXGKomkw=
Preshared Key	
Peer Subnet IP/Mask	192.168.3.0/24 ex. 192.168.88.0/24

Save✓
Cancel✕

2) Wireguard Routing

There are two routings when Wireguard established.

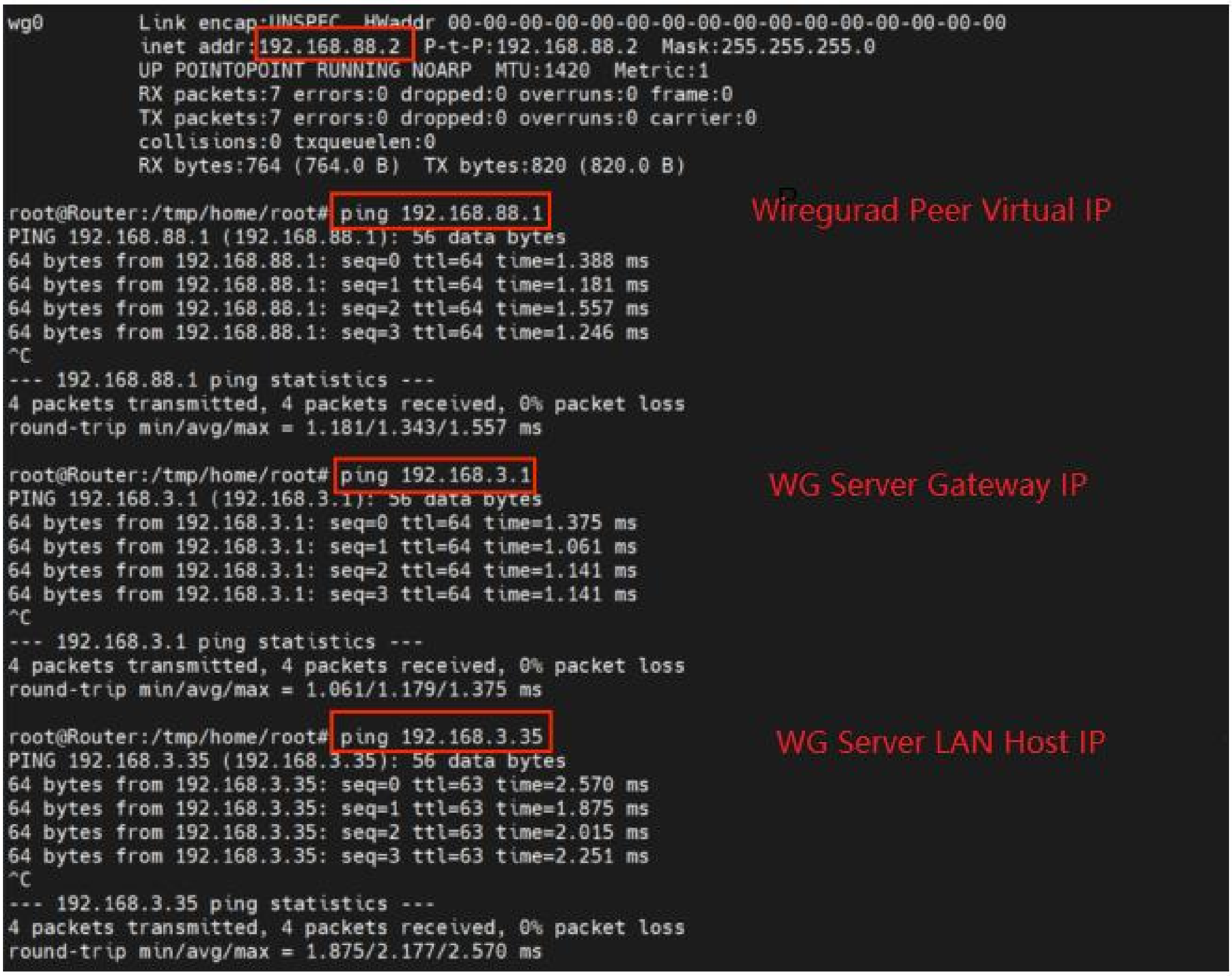


Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	192.168.10.1	0.0.0.0	0	wan
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	lan
192.168.3.0	*	255.255.255.0	0	wg0
192.168.10.0	*	255.255.255.0	0	wan
192.168.10.1	*	255.255.255.255	0	wan
192.168.88.0	*	255.255.255.0	0	wg0

3) Wireguard Connection Check

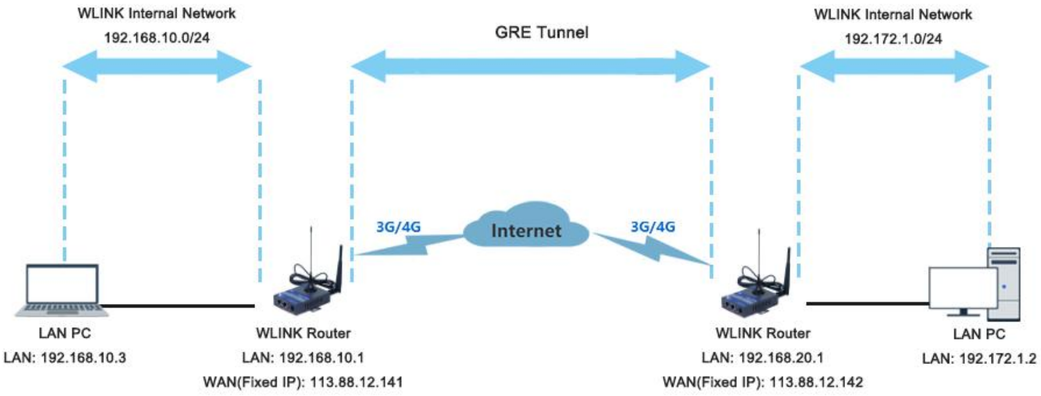
Check VPN connection via Ping testing.



```
wg0       Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.88.2  P-t-P:192.168.88.2  Mask:255.255.255.0
          UP POINTOPOINT RUNNING NOARP  MTU:1420  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:764 (764.0 B)  TX bytes:820 (820.0 B)

root@Router:/tmp/home/root# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1): 56 data bytes
64 bytes from 192.168.88.1: seq=0 ttl=64 time=1.388 ms
64 bytes from 192.168.88.1: seq=1 ttl=64 time=1.181 ms
64 bytes from 192.168.88.1: seq=2 ttl=64 time=1.557 ms
64 bytes from 192.168.88.1: seq=3 ttl=64 time=1.246 ms
^C
--- 192.168.88.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.181/1.343/1.557 ms

root@Router:/tmp/home/root# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: seq=0 ttl=64 time=1.375 ms
64 bytes from 192.168.3.1: seq=1 ttl=64 time=1.061 ms
64 bytes from 192.168.3.1: seq=2 ttl=64 time=1.141 ms
64 bytes from 192.168.3.1: seq=3 ttl=64 time=1.141 ms
^C
--- 192.168.3.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.061/1.179/1.375 ms

root@Router:/tmp/home/root# ping 192.168.3.35
PING 192.168.3.35 (192.168.3.35): 56 data bytes
64 bytes from 192.168.3.35: seq=0 ttl=63 time=2.570 ms
64 bytes from 192.168.3.35: seq=1 ttl=63 time=1.875 ms
64 bytes from 192.168.3.35: seq=2 ttl=63 time=2.015 ms
64 bytes from 192.168.3.35: seq=3 ttl=63 time=2.251 ms
^C
--- 192.168.3.35 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.875/2.177/2.570 ms
```

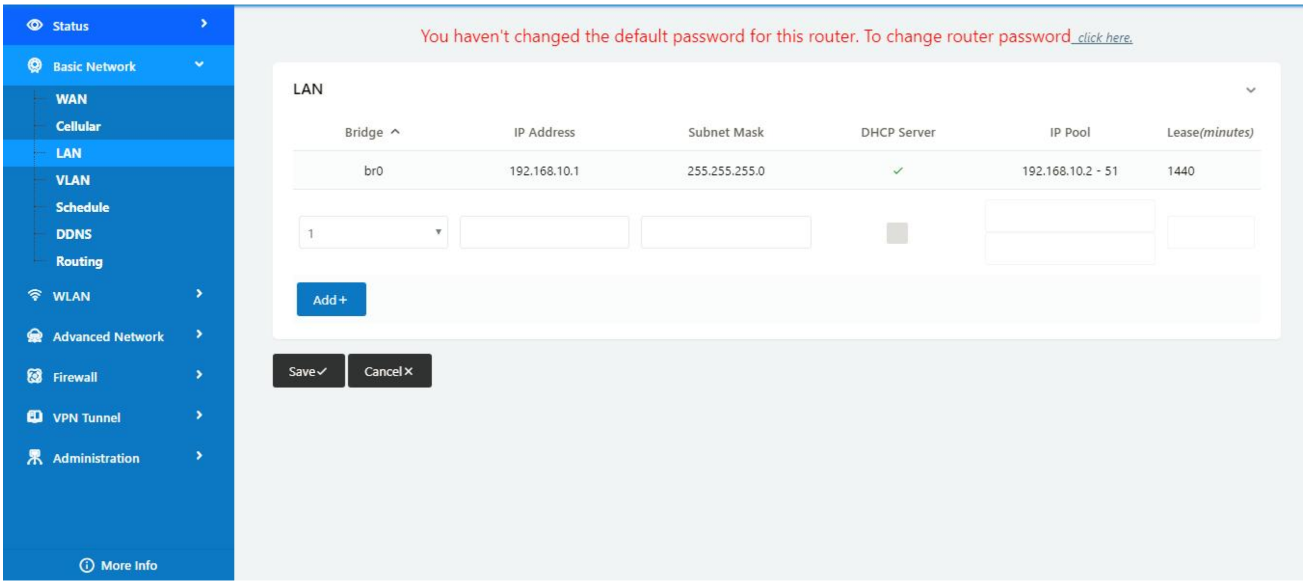
4.8.2 GRE

GRE Tunnel between two WL-Rxx Routers


WLINK Internal Network
192.168.10.0/24
GRE Tunnel
WLINK Internal Network
192.172.1.0/24
3G/4G
Internet
3G/4G
LAN PC
LAN: 192.168.10.3
WLINK Router
LAN: 192.168.10.1
WAN(Fixed IP): 113.88.12.141
WLINK Router
LAN: 192.168.20.1
WAN(Fixed IP): 113.88.12.142
LAN PC
LAN: 192.172.1.2

1) WL-R200(A) Config

Navigate to **Basic Network > LAN**

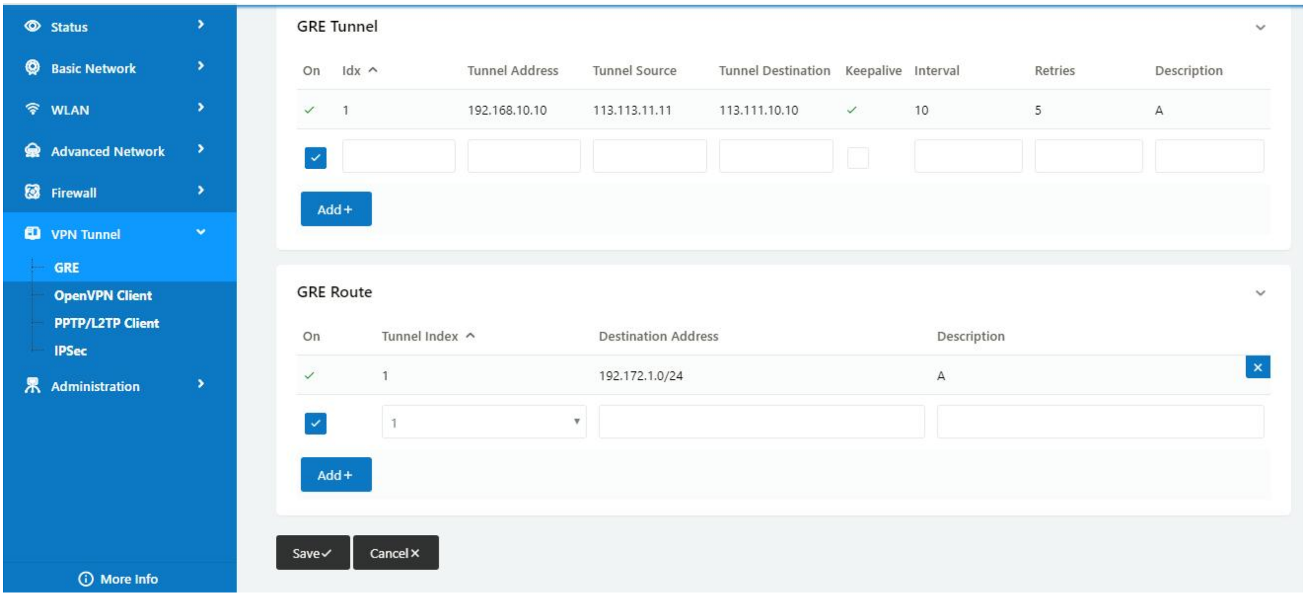

Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Add+
Save✓
Cancel✕

You haven't changed the default password for this router. To change router password click here.

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(*minutes*)
br0	192.168.10.1	255.255.255.0	✓	192.168.10.2 - 51	1440
1			☐		

Navigate to **VPN Tunnel > GRE**


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
Add+
Add+
Save✓
Cancel✕

GRE Tunnel

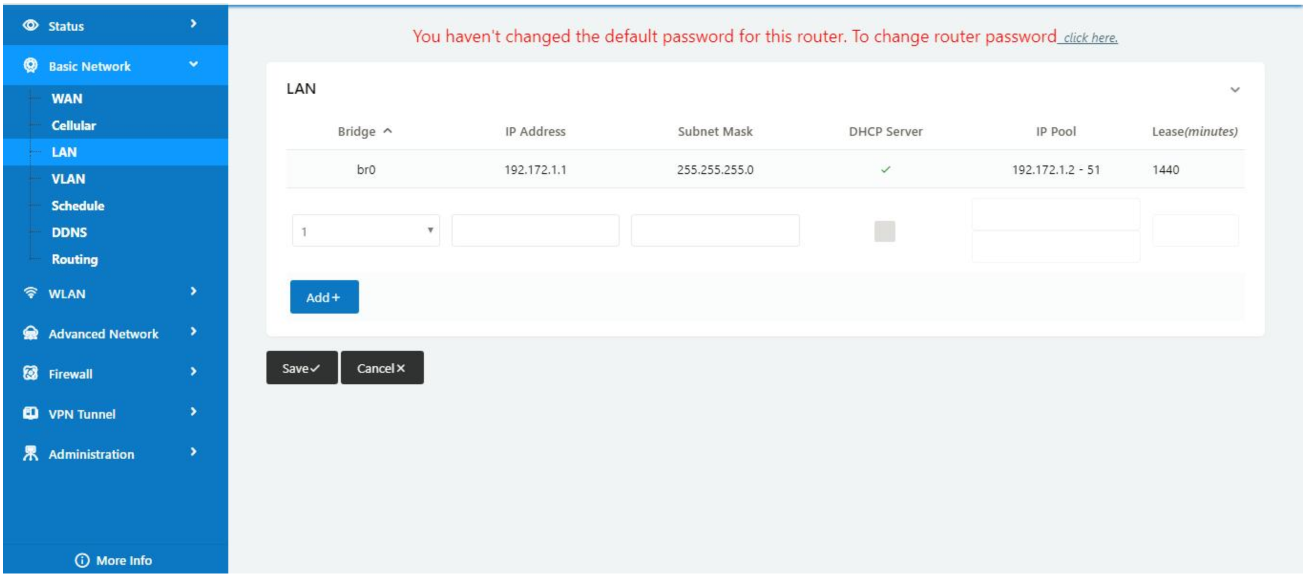
On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	1	192.168.10.10	113.113.11.11	113.111.10.10	✓	10	5	A
☑					☐			

GRE Route

On	Tunnel Index	Destination Address	Description
✓	1	192.172.1.0/24	A
☑	1		

2) WL-R200(B) Config

Navigate to **Basic Network > LAN**

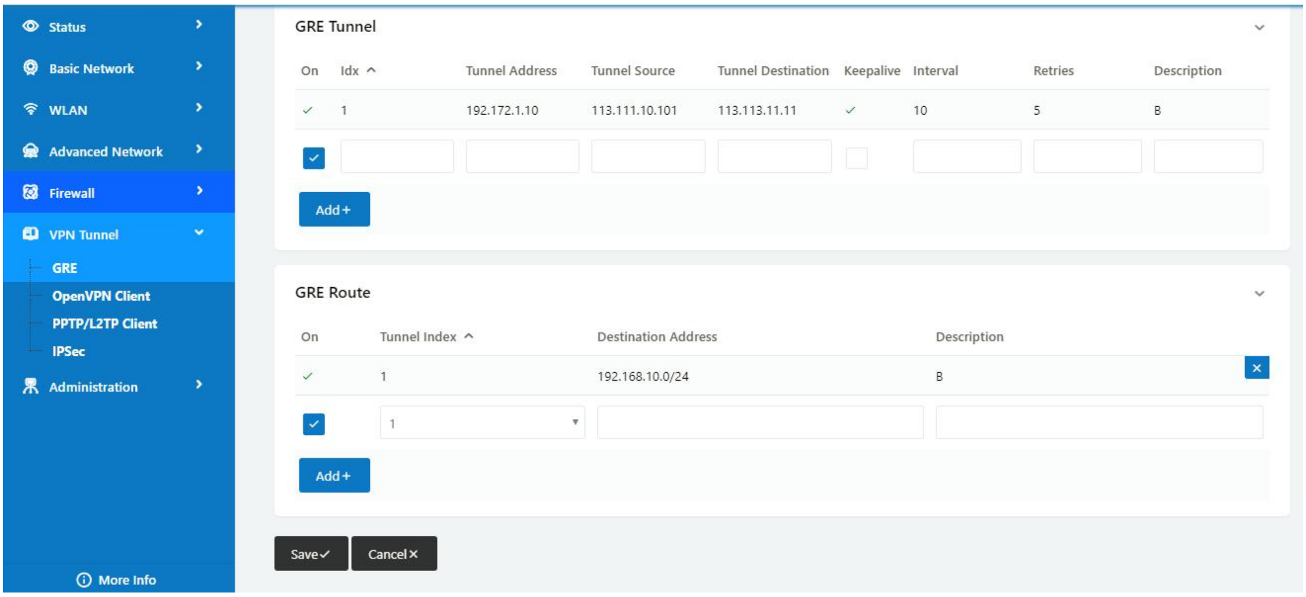

Status
Basic Network
WAN
Cellular
LAN
VLAN
Schedule
DDNS
Routing
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Add+
Save✓
Cancel✕

You haven't changed the default password for this router. To change router password click here.

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(*minutes*)
br0	192.172.1.1	255.255.255.0	✓	192.172.1.2 - 51	1440
1			☐		

Navigate to **VPN Tunnel > GRE**


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
Add+
Save✓
Cancel✕

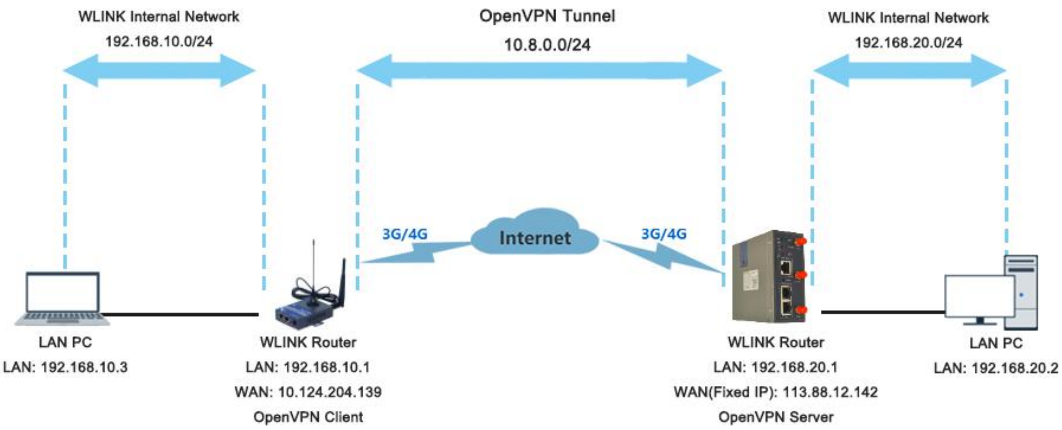
GRE Tunnel

On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	1	192.172.1.10	113.111.10.101	113.113.11.11	✓	10	5	B
☑					☐			

GRE Route

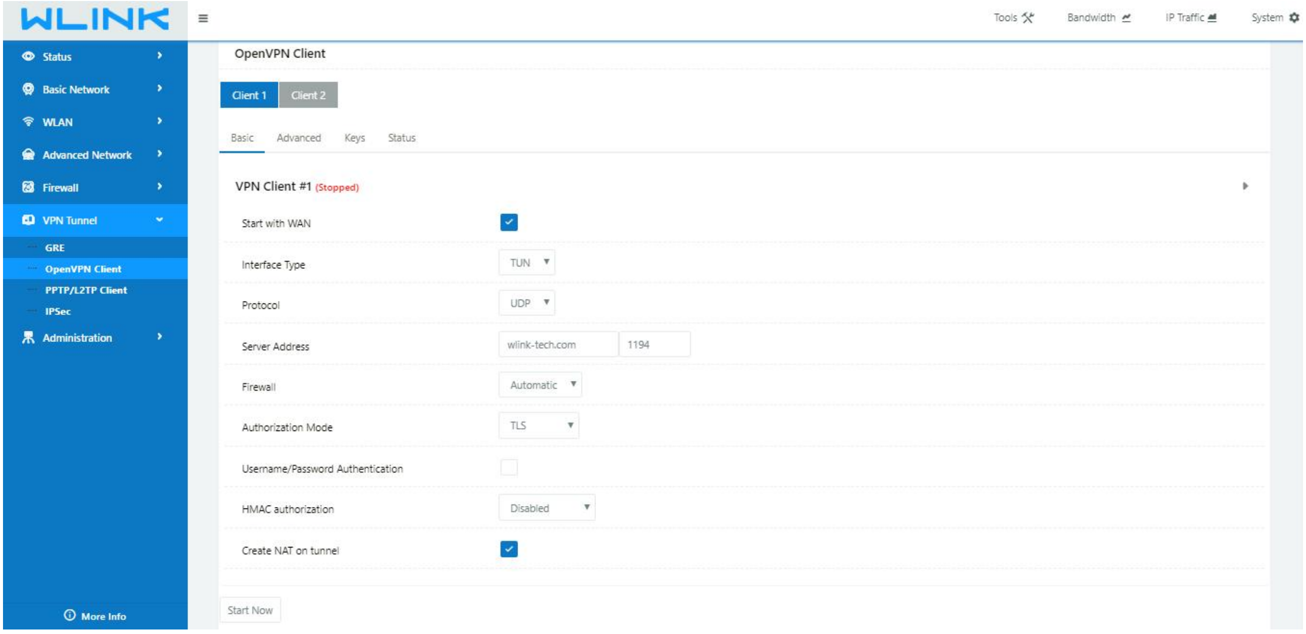
On	Tunnel Index	Destination Address	Description
✓	1	192.168.10.0/24	B
☑	1		

4.8.3 OpenVPN


WLINK Internal Network
192.168.10.0/24
OpenVPN Tunnel
10.8.0.0/24
WLINK Internal Network
192.168.20.0/24
3G/4G
Internet
3G/4G
LAN PC
LAN: 192.168.10.3
WLINK Router
LAN: 192.168.10.1
WAN: 10.124.204.139
OpenVPN Client
WLINK Router
LAN: 192.168.20.1
WAN(Fixed IP): 113.88.12.142
OpenVPN Server
LAN PC
LAN: 192.168.20.2

OpenVPN between WL-Rxx client and Server

Please click “VPN Tunnel> OpenVPN Client” to check or modify the relevant parameter.


WLINK
Tools
Bandwidth
IP Traffic
System
Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
Client 1
Client 2
Basic
Advanced
Keys
Status
Start Now

OpenVPN Client

VPN Client #1 (Stopped)

Start with WAN ☑

Interface Type TUN

Protocol UDP

Server Address wlink-tech.com 1194

Firewall Automatic

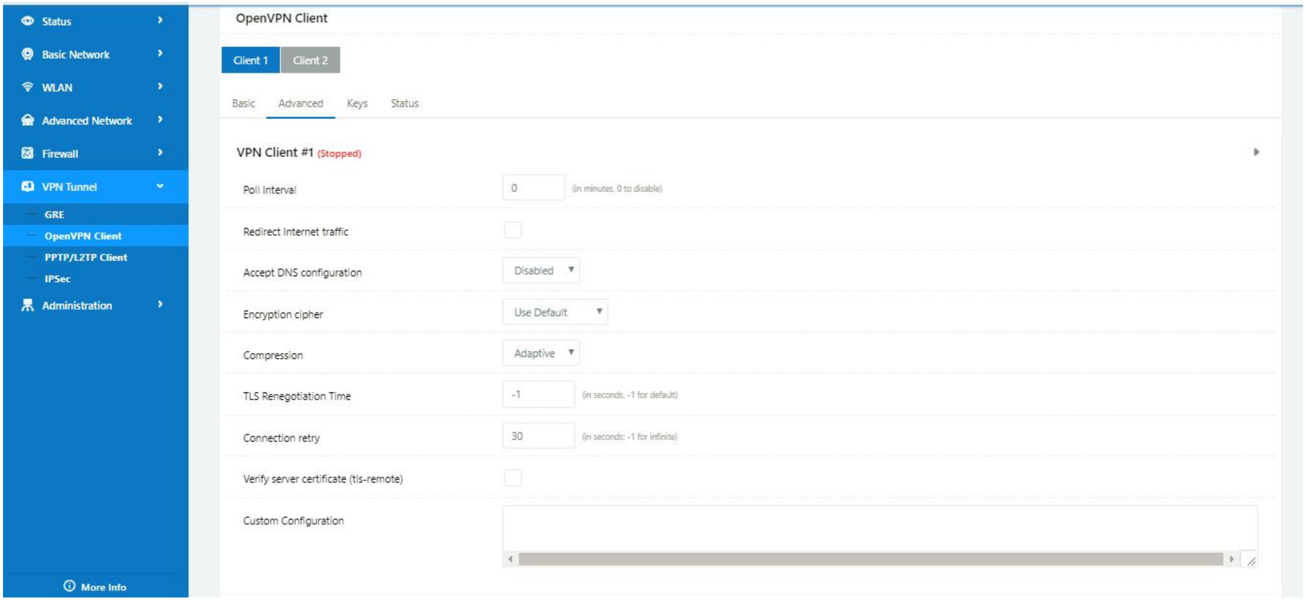
Authorization Mode TLS

Username/Password Authentication ☐

HMAC authorization Disabled

Create NAT on tunnel ☑

Parameter	**Instruction**
Start with WAN	Enable the Openvpn feature for 4G/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 Authentication	As the configuration requested.
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
OpenVPN Client
Client 1
Client 2
Basic
Advanced
Keys
Status

VPN Client #1 (Stopped)

Poll Interval: 0 (in minutes, 0 to disable)

Redirect Internet traffic: ☐

Accept DNS configuration: Disabled

Encryption cipher: Use Default

Compression: Adaptive

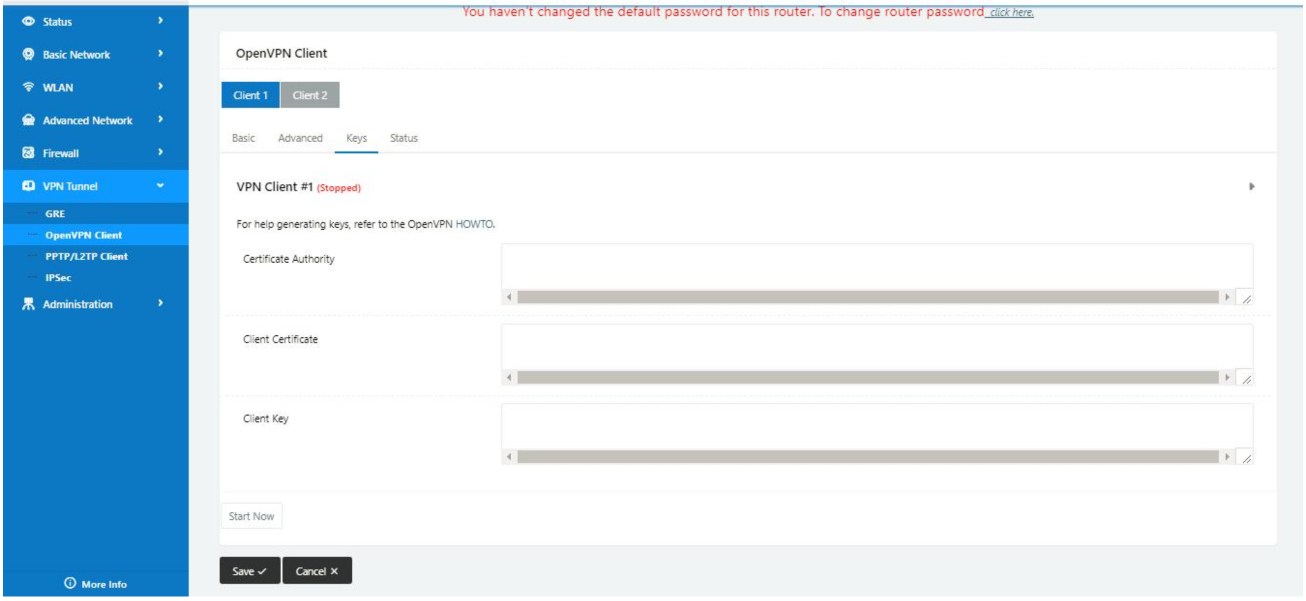
TLS Renegotiation Time: -1 (in seconds, -1 for default)

Connection retry: 30 (in seconds; -1 for infinite)

Verify server certificate (tls-remote): ☐

Custom Configuration:

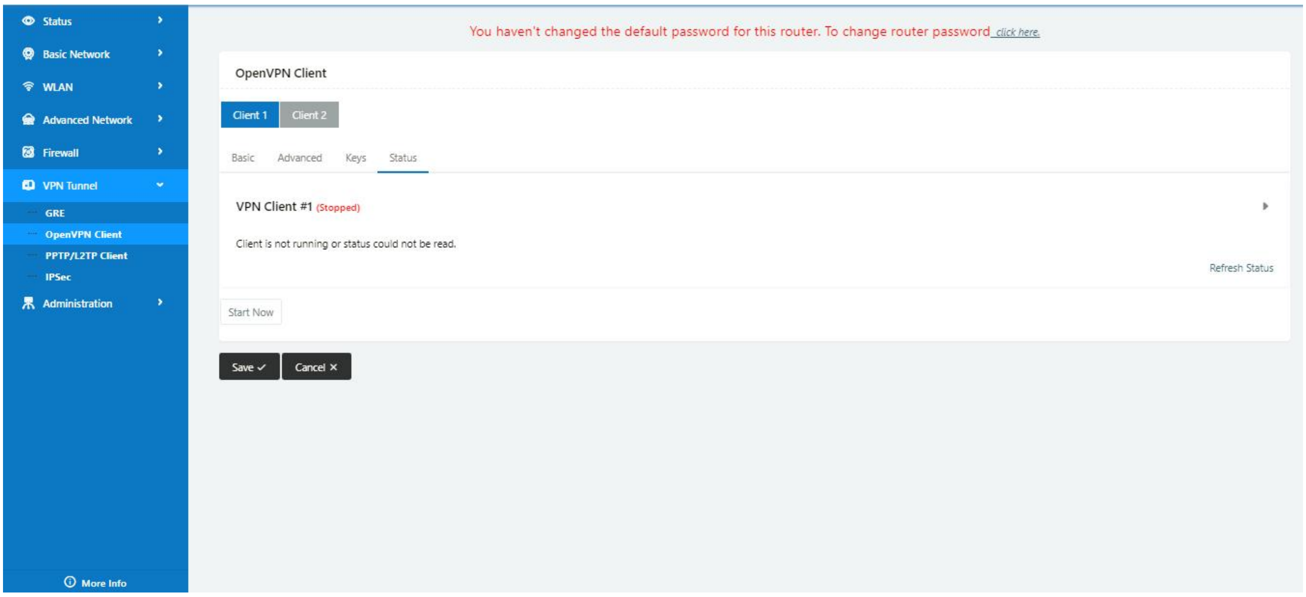
Parameter	**Instruction**
Poll Interval	Openvpn client check router’s status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As the configuration requested.
Encryption	As the configuration requested.
Compression	As the configuration requested.
TLS Renegotiation 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.


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
OpenVPN Client
Client 1
Client 2
Basic
Advanced
Keys
Status
VPN Client #1 (Stopped)
Certificate Authority
Client Certificate
Client Key
Start Now
Save ✓
Cancel ✕

You haven't changed the default password for this router. To change router password click here.

For help generating keys, refer to the OpenVPN HOWTO.

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


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
OpenVPN Client
Client 1
Client 2
Basic
Advanced
Keys
Status
VPN Client #1 (Stopped)
Refresh Status
Start Now
Save ✓
Cancel ✕

You haven't changed the default password for this router. To change router password click here.

Client is not running or status could not be read.

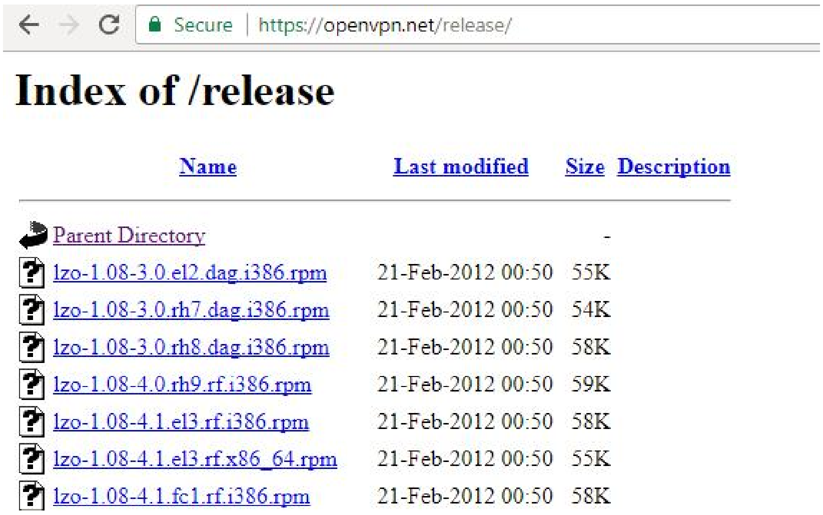
Parameter	Instruction
Status	Check OpenVPN status and data statistics.

Click “save” and “start now” to enable OpenVPN when you have done all the client config.

OpenVPN Keys Guide

The fllowing steps are for server running on Windows 7/8/10

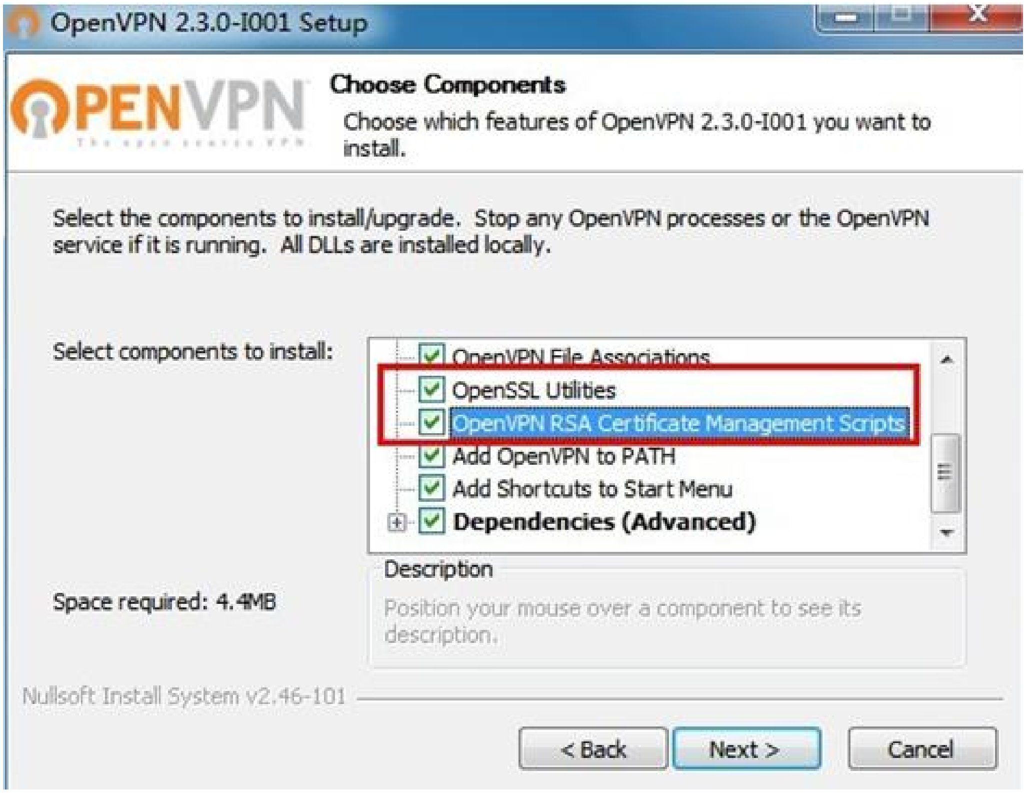
Access to (http://openvpn.net/release/) and download the file “openvpn-2.3.0-install.exe” (or higher)


Secure | https://openvpn.net/release/

Index of /release

Name	Last modified	Size	Description
Parent Directory		-	
lzo-1.08-3.0.el2.dag.i386.rpm	21-Feb-2012 00:50	55K	
lzo-1.08-3.0.rh7.dag.i386.rpm	21-Feb-2012 00:50	54K	
lzo-1.08-3.0.rh8.dag.i386.rpm	21-Feb-2012 00:50	58K	
lzo-1.08-4.0.rh9.rf.i386.rpm	21-Feb-2012 00:50	59K	
lzo-1.08-4.1.el3.rf.i386.rpm	21-Feb-2012 00:50	58K	
lzo-1.08-4.1.el3.rf.x86_64.rpm	21-Feb-2012 00:50	55K	
lzo-1.08-4.1.fc1.rf.i386.rpm	21-Feb-2012 00:50	58K	

After installing OpenVPN, please find the OpenVPN folder to generate the certificate of server and client. (Access to http://openvpn.net for more information)


OpenVPN 2.3.0-I001 Setup

Choose Components

Choose which features of OpenVPN 2.3.0-I001 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

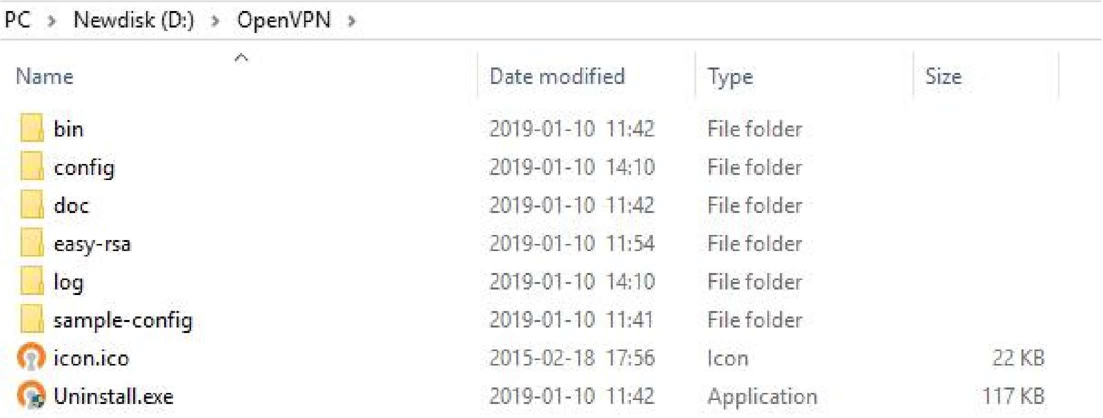
- ☑ OpenVPN File Associations
- ☑ OpenSSL Utilities
- ☑ OpenVPN RSA Certificate Management Scripts
- ☑ Add OpenVPN to PATH
- ☑ Add Shortcuts to Start Menu
- ☑ **Dependencies (Advanced)**

Space required: 4.4MB

Description

Position your mouse over a component to see its description.

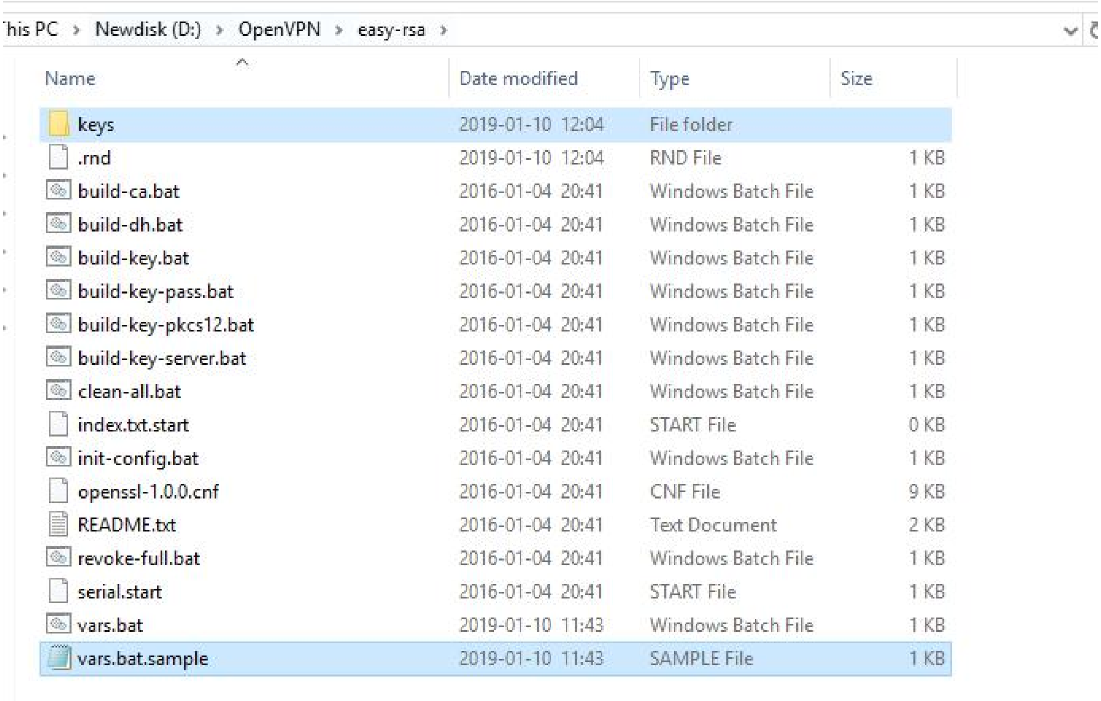
Nullsoft Install System v2.46-101



PC › Newdisk (D:) › OpenVPN ›

Name	Date modified	Type	Size
bin	2019-01-10 11:42	File folder	
config	2019-01-10 14:10	File folder	
doc	2019-01-10 11:42	File folder	
easy-rsa	2019-01-10 11:54	File folder	
log	2019-01-10 14:10	File folder	
sample-config	2019-01-10 11:41	File folder	
icon.ico	2015-02-18 17:56	Icon	22 KB
Uninstall.exe	2019-01-10 11:42	Application	117 KB

Configure “vas.bat.sample” to complete the initialization step and keys

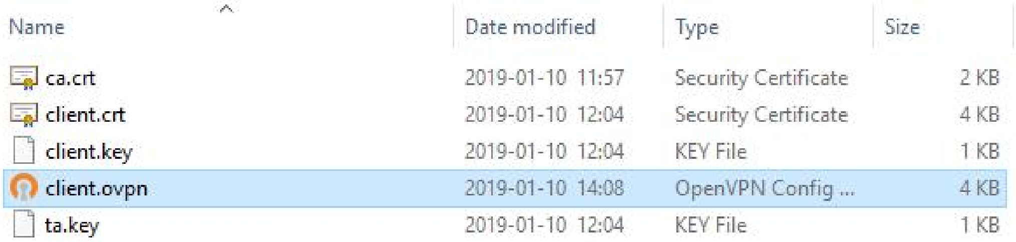


his PC › Newdisk (D:) › OpenVPN › easy-rsa ›

Name	Date modified	Type	Size
keys	2019-01-10 12:04	File folder	
.rnd	2019-01-10 12:04	RND File	1 KB
build-ca.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-dh.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pass.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pkcs12.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-server.bat	2016-01-04 20:41	Windows Batch File	1 KB
clean-all.bat	2016-01-04 20:41	Windows Batch File	1 KB
index.txt.start	2016-01-04 20:41	START File	0 KB
init-config.bat	2016-01-04 20:41	Windows Batch File	1 KB
openssl-1.0.0.cnf	2016-01-04 20:41	CNF File	9 KB
README.txt	2016-01-04 20:41	Text Document	2 KB
revoke-full.bat	2016-01-04 20:41	Windows Batch File	1 KB
serial.start	2016-01-04 20:41	START File	1 KB
vars.bat	2019-01-10 11:43	Windows Batch File	1 KB
vars.bat.sample	2019-01-10 11:43	SAMPLE File	1 KB

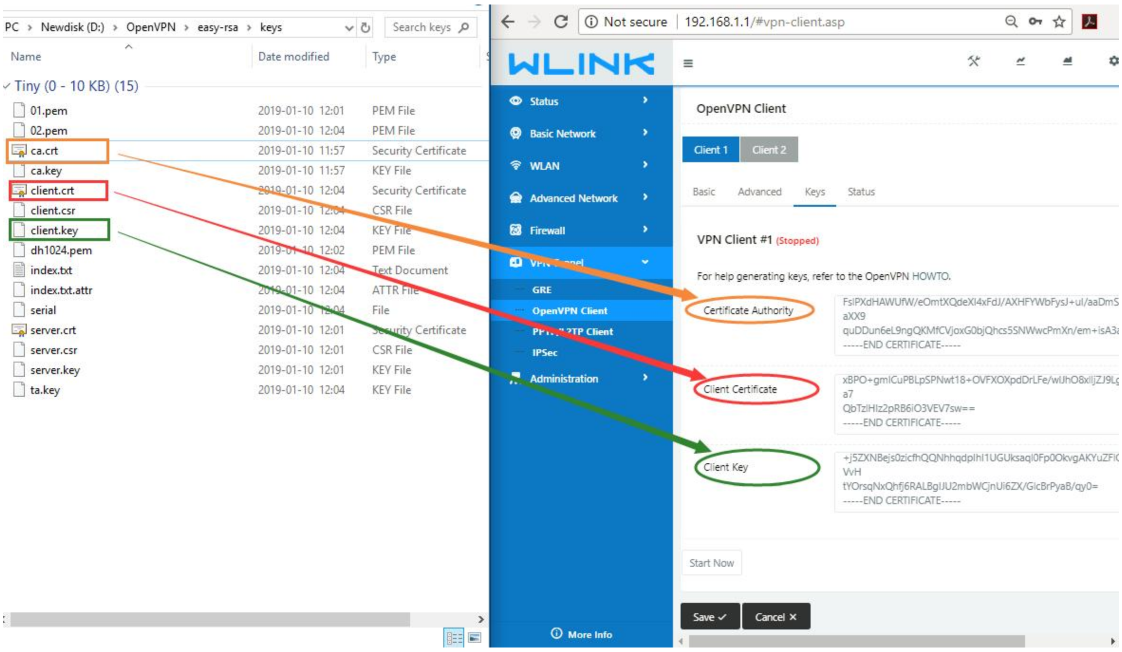
Configure the client keys to WLINK OpenVPN client GUI when you create the server and client certificate in the path OpenVPN/easy-rsa/keys

Client certificate (Generated on the server)



Name	Date modified	Type	Size
ca.crt	2019-01-10 11:57	Security Certificate	2 KB
client.crt	2019-01-10 12:04	Security Certificate	4 KB
client.key	2019-01-10 12:04	KEY File	1 KB
client.ovpn	2019-01-10 14:08	OpenVPN Config ...	4 KB
ta.key	2019-01-10 12:04	KEY File	1 KB

OpenVPN>easy-rsa>keys


PC › Newdisk (D:) › OpenVPN › easy-rsa › keys
Search keys
Not secure
192.168.1.1/#vpn-client.asp
WLINK
Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
Client 1
Client 2
Basic
Advanced
Keys
Status
Start Now
Save ✓
Cancel ✕

Tiny (0 - 10 KB) (15)

Name	Date modified	Type
01.pem	2019-01-10 12:01	PEM File
02.pem	2019-01-10 12:04	PEM File
ca.crt	2019-01-10 11:57	Security Certificate
ca.key	2019-01-10 11:57	KEY File
client.crt	2019-01-10 12:04	Security Certificate
client.csr	2019-01-10 12:04	CSR File
client.key	2019-01-10 12:04	KEY File
dh1024.pem	2019-01-10 12:02	PEM File
index.txt	2019-01-10 12:04	Text Document
index.txt.attr	2019-01-10 12:04	ATTR File
serial	2019-01-10 12:04	File
server.crt	2019-01-10 12:01	Security Certificate
server.csr	2019-01-10 12:01	CSR File
server.key	2019-01-10 12:01	KEY File
ta.key	2019-01-10 12:04	KEY File

OpenVPN Client

VPN Client #1 (Stopped)

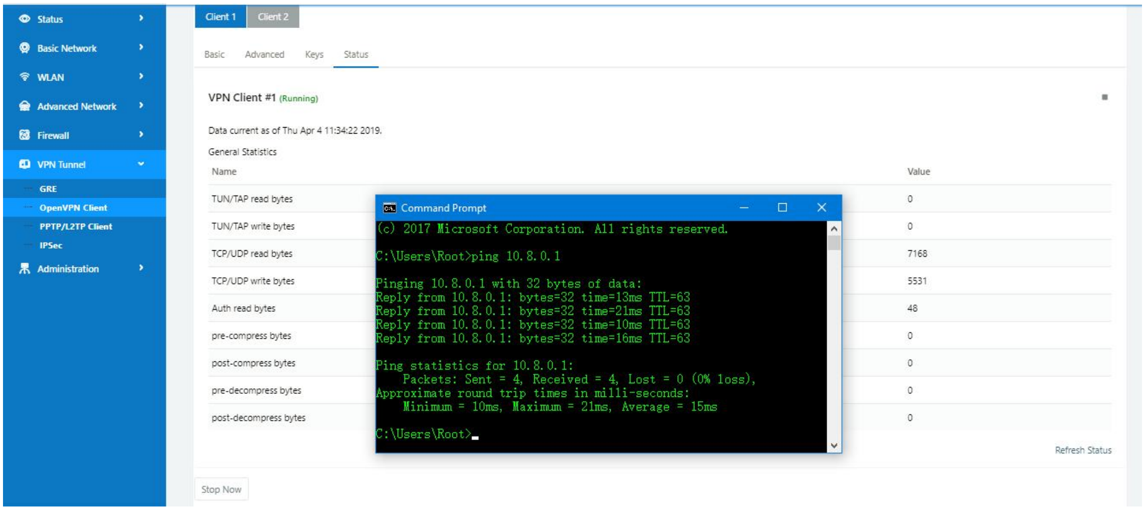
For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority
```
FsIPXdHAWUfW/eOmtXQdeXI4xFdJ/AXHFYWbFysJ+ul/aaDmS
aXX9
quDDun6eL9ngQKMfCVjoxG0bjQhcs5SNWwcPmXn/em+isA3a
-----END CERTIFICATE-----
```

Client Certificate
```
xBPO+gmICuPBLpSPNwt18+OVFXOXpdDrLFe/wUhO8xlljZJ9L
a7
QbTzlHlz2pRB6iO3VEV7sw==
-----END CERTIFICATE-----
```

Client Key
```
+j5ZXNBejs0zicfhQQNhhqdplhl1UGUksaql0Fp0OkvgAKYuZFI
VvH
tYOrsqNxQhfj6RALBgIJU2mbWCjnUi6ZX/GlcBrPyaB/qy0=
-----END CERTIFICATE-----
```

Ping test to your server when the tunnel is established


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
Client 1
Client 2
Basic
Advanced
Keys
Status
Command Prompt
Refresh Status
Stop Now

VPN Client #1 (Running)

Data current as of Thu Apr 4 11:34:22 2019.

General Statistics

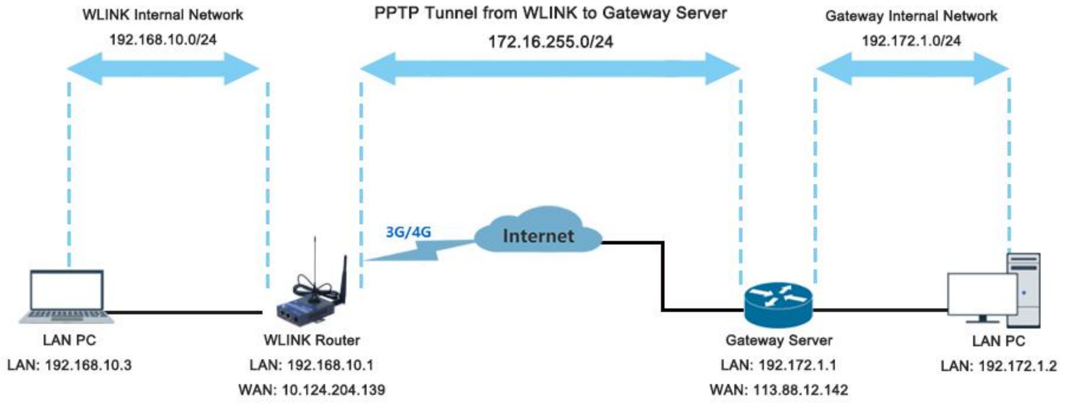
Name	Value
TUN/TAP read bytes	0
TUN/TAP write bytes	0
TCP/UDP read bytes	7168
TCP/UDP write bytes	5531
Auth read bytes	48
pre-compress bytes	0
post-compress bytes	0
pre-decompress bytes	0
post-decompress bytes	0

```
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Root>ping 10.8.0.1

Pinging 10.8.0.1 with 32 bytes of data:
Reply from 10.8.0.1: bytes=32 time=13ms TTL=63
Reply from 10.8.0.1: bytes=32 time=21ms TTL=63
Reply from 10.8.0.1: bytes=32 time=10ms TTL=63
Reply from 10.8.0.1: bytes=32 time=16ms TTL=63

Ping statistics for 10.8.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 21ms, Average = 15ms

C:\Users\Root>
```

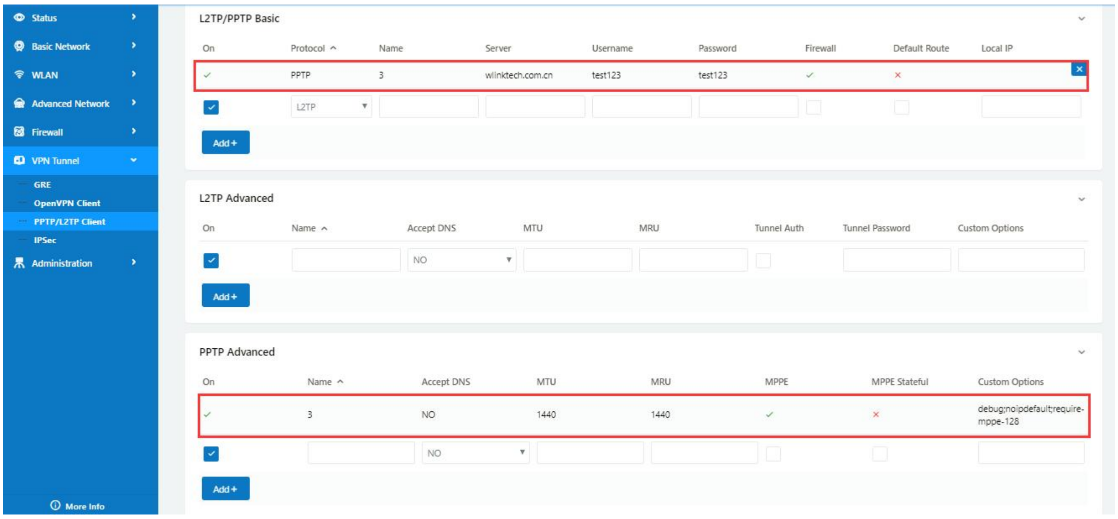
---End

4.8.4 L2TP/PPTP

Please click “VPN Tunnel>PPTP/L2TP Client” to view or modify the relevant parameter.


WLINK Internal Network
192.168.10.0/24
PPTP Tunnel from WLINK to Gateway Server
172.16.255.0/24
Gateway Internal Network
192.172.1.0/24
3G/4G
Internet
LAN PC
LAN: 192.168.10.3
WLINK Router
LAN: 192.168.10.1
WAN: 10.124.204.139
Gateway Server
LAN: 192.172.1.1
WAN: 113.88.12.142
LAN PC
LAN: 192.172.1.2

Configured as PPTP


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
Add +
Add +
Add +

L2TP/PPTP Basic

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
✓	PPTP	3	wlinktech.com.cn	test123	test123	✓	✗	
☑	L2TP					☐	☐	

L2TP Advanced

On	Name	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
☑		NO			☐		

PPTP Advanced

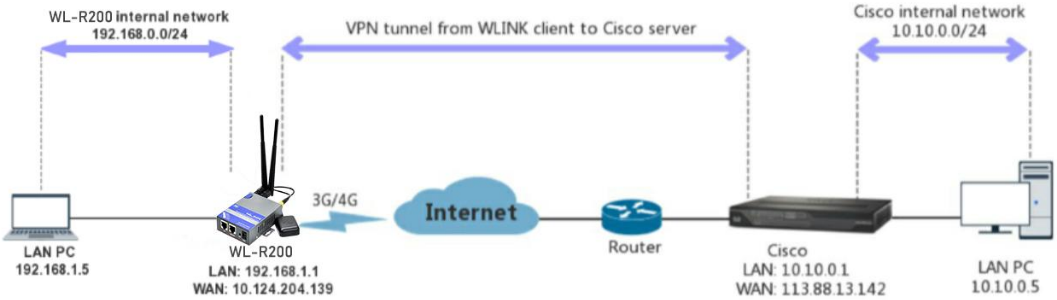
On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
✓	3	NO	1440	1440	✓	✗	debug;noipdefault;require-mppe-128
☑		NO			☐	☐	

Note: The Custom Options are based on your server

---End

4.8.5 IPSec

IPSec between WL-R200 and Cisco Router


WL-R200 internal network
192.168.0.0/24
VPN tunnel from WLINK client to Cisco server
Cisco internal network
10.10.0.0/24
3G/4G
Internet
LAN PC
192.168.1.5
WL-R200
LAN: 192.168.1.1
WAN: 10.124.204.139
Router
Cisco
LAN: 10.10.0.1
WAN: 113.88.13.142
LAN PC
10.10.0.5

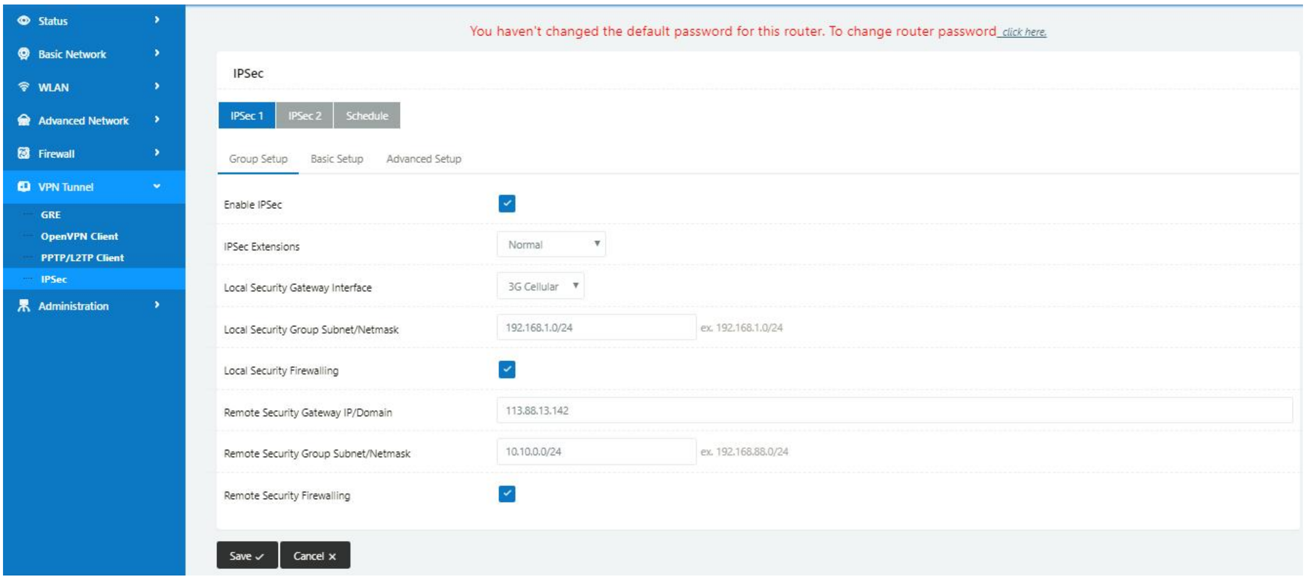
1) Cisco Config (main mode)

```
!
crypto isakmp policy 10
```

```
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key test1234 address 0.0.0.0    0.0.0.0
!
!
crypto ipsec transform-set Tran-set esp-3des esp-sha-hmac
crypto ipsec nat-transparency spi-matching
!
```

2) WLINK Config

Navigate to **VPN Tunnel > IPSec > Group Setup**


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
IPSec 1
IPSec 2
Schedule
Group Setup
Basic Setup
Advanced Setup
Save ✓
Cancel ✕

You haven't changed the default password for this router. To change router password click here.

IPSec

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

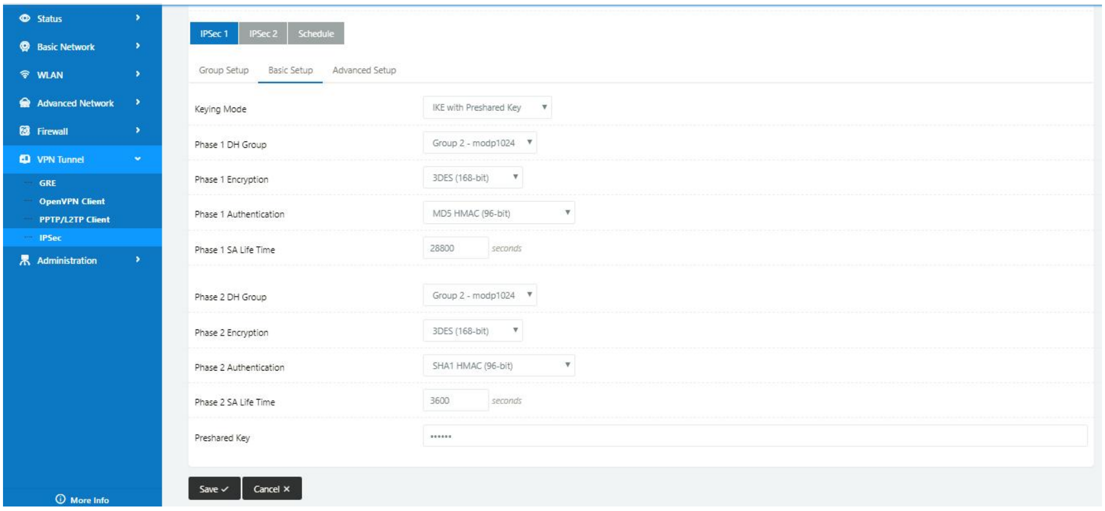
Local Security Firewalling ☑

Remote Security Gateway IP/Domain: 113.88.13.142

Remote Security Group Subnet/Netmask: 10.10.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☑

Navigate to **VPN Tunnel > IPSec > Basic Setup**


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
IPSec 1
IPSec 2
Schedule
Group Setup
Basic Setup
Advanced Setup
Save ✓
Cancel ✕

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

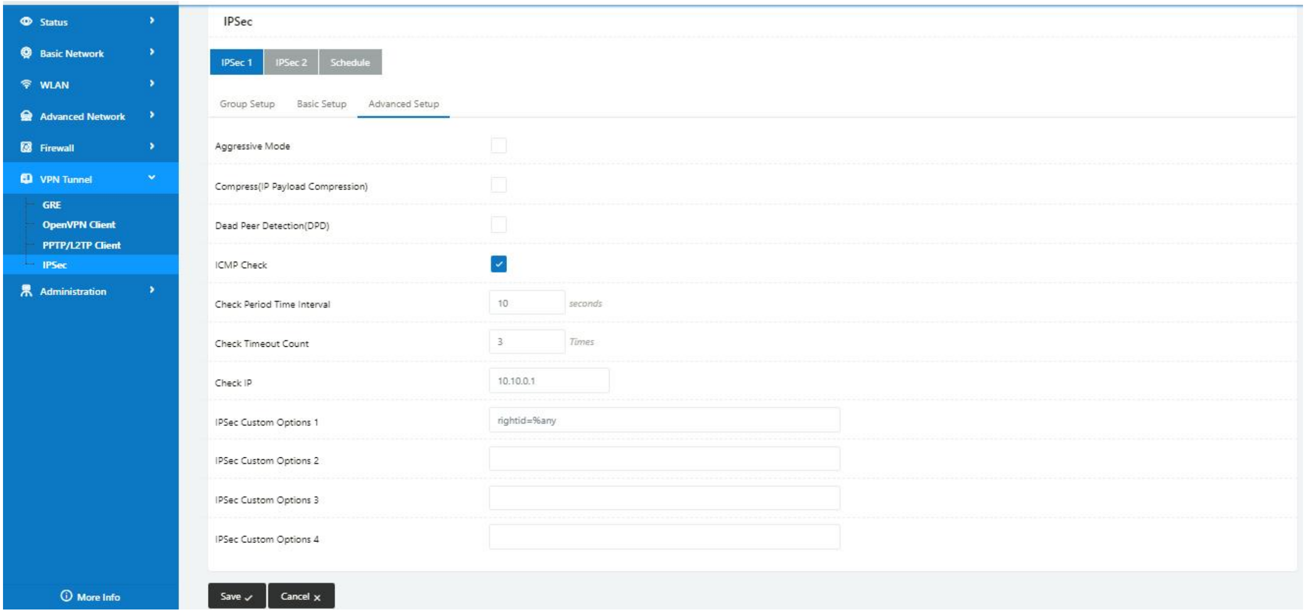
Phase 2 Encryption: 3DES (168-bit)

Phase 2 Authentication: SHA1 HMAC (96-bit)

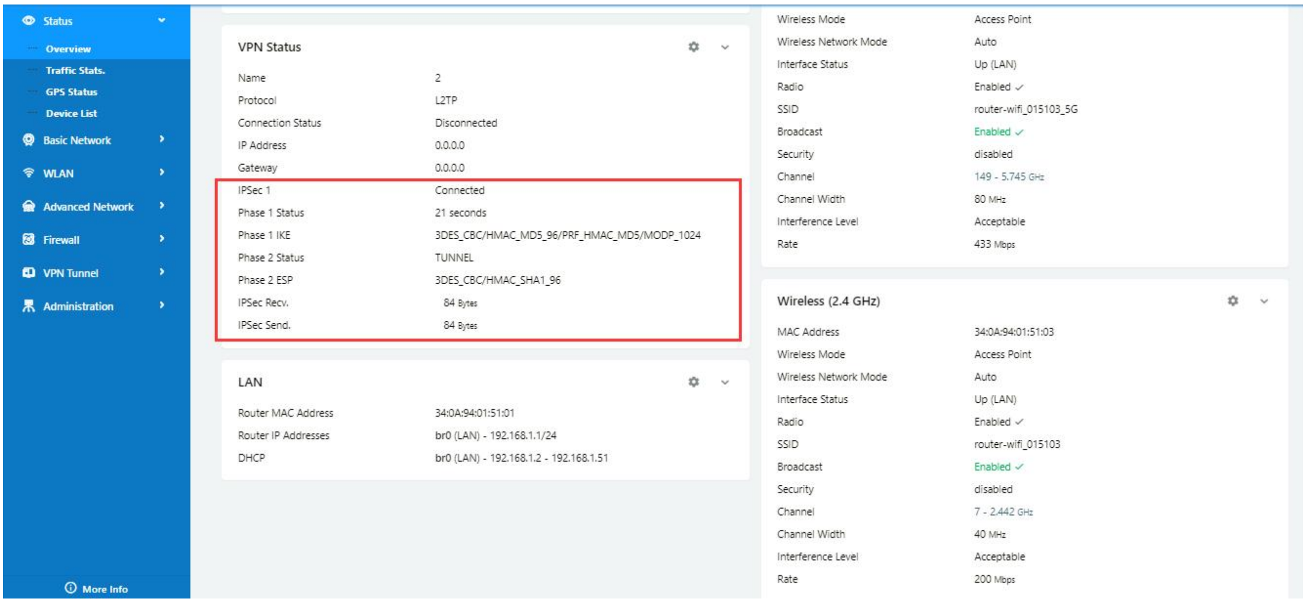
Phase 2 SA Life Time: 3600 seconds

Preshared Key: ••••••

Navigate to **VPN Tunnel > IPSec > Advanced Setup**


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
More Info
IPSec
IPSec 1
IPSec 2
Schedule
Group Setup
Basic Setup
Advanced Setup
Save
Cancel

Aggressive Mode	☐
Compress(IP Payload Compression)	☐
Dead Peer Detection(DPD)	☐
ICMP Check	☑
Check Period Time Interval	10 seconds
Check Timeout Count	3 Times
Check IP	10.10.0.1
IPSec Custom Options 1	rightid=%any
IPSec Custom Options 2	
IPSec Custom Options 3	
IPSec Custom Options 4	


Status
Overview
Traffic Stats.
GPS Status
Device List
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
Administration
More Info

VPN Status

Name	2
Protocol	L2TP
Connection Status	Disconnected
IP Address	0.0.0.0
Gateway	0.0.0.0
IPSec 1	Connected
Phase 1 Status	21 seconds
Phase 1 IKE	3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
Phase 2 Status	TUNNEL
Phase 2 ESP	3DES_CBC/HMAC_SHA1_96
IPSec Recv.	84 Bytes
IPSec Send.	84 Bytes

LAN

Router MAC Address	34:0A:94:01:51:01
Router IP Addresses	br0 (LAN) - 192.168.1.1/24
DHCP	br0 (LAN) - 192.168.1.2 - 192.168.1.51

Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up (LAN)
Radio	Enabled ✓
SSID	router-wifi_015103_5G
Broadcast	Enabled ✓
Security	disabled
Channel	149 - 5.745 GHz
Channel Width	80 MHz
Interference Level	Acceptable
Rate	433 Mbps

Wireless (2.4 GHz)

MAC Address	34:0A:94:01:51:03
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up (LAN)
Radio	Enabled ✓
SSID	router-wifi_015103
Broadcast	Enabled ✓
Security	disabled
Channel	7 - 2.442 GHz
Channel Width	40 MHz
Interference Level	Acceptable
Rate	200 Mbps

---End