

WLINK

User Manual

---Apply to WL-G520 Series 4G+/4G Router

V3.5

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

Feb, 2025



Copyright © Shenzhen WLINK Technology Company Limited 2012 ~ 2025

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

Caution

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

Version History

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

| Data | Document Version | Firmware Version | Description |
|------------|------------------|----------------------------|---|
| 2024-12-16 | V3.5 | G5.0.1.5-241211-174212.trx | Added 4G modules driver. |
| 2024-3-16 | V3.8 | G5.0.1.5-240318-093438.trx | Improve PL2303GC Driver |
| 2023-1-6 | V3.3 | G5.0.1.5-230116-113230.trx | Improve Configuration Restore. Add Configuration Instances. |
| 2022-1-2 | V3.2 | G5.0.1.5-211103-170736.trx | Added two OpenVPN tunnel, Improved UI http/https timeout. |
| 2021-7-19 | V3.1 | G5.0.1.5-210719-155351.trx | Improved SIM tray in hardware, Added IKE2 and TR069 |
| 2020-4-2 | V3.0 | G5.0.1.5-200317-162210.trx | WL-G520 UI3.0 |

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

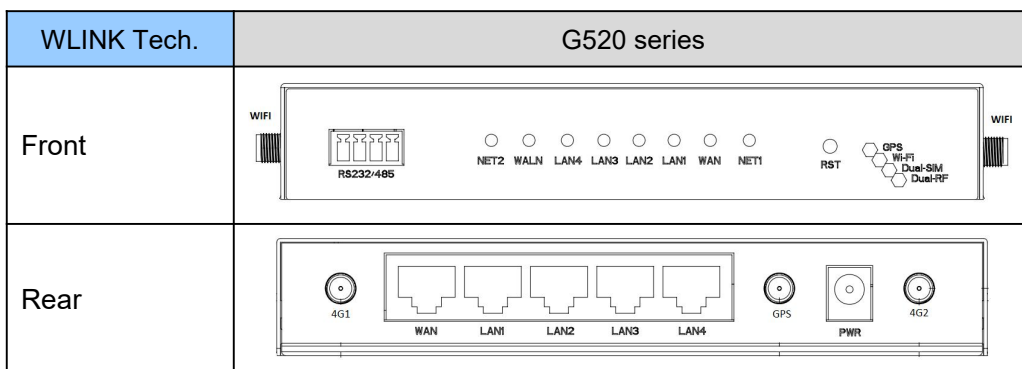
| | |
|---|----|
| 1 Hardware Installation | 4 |
| 1.1 Panel | 4 |
| 1.2 LED Status | 6 |
| 1.3 Dimension | 6 |
| 1.4 How to Install | 7 |
| 2 Router Configuration | 9 |
| 2.1 Local Configure | 9 |
| 2.2 Status | 10 |
| 2.3 Overview | 10 |
| 2.4 Traffic Stats | 11 |
| 2.5 Device List | 11 |
| 2.6 Tool Column | 12 |
| 2.7 Basic Network | 14 |
| 2.8 WLAN Setting | 24 |
| 2.9 Advanced Network Setting | 26 |
| 2.10 Firewall | 35 |
| 2.11 VPN Tunnel | 37 |
| 2.12 Administration | 47 |
| 3 Configuration Instance | 55 |
| 3.1 VLAN | 55 |
| 3.2 WAN Backup (WAN as Main, Cellular Backup) | 57 |
| 3.3 Port Forwarding | 59 |
| 3.4 IP Passthrough | 61 |
| 3.5 Captive Portal | 63 |
| 3.6 GPS Settings | 66 |
| 3.7 Firewall | 69 |
| 3.8 VPN Tunnel | 70 |

1 Hardware Installation

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

1.1 Panel

Table 1-1 WL-G520 Structure



NOTE

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

Table 1-2 Router Interface

| Port | Instruction | Remark |
|-----------|--|--------|
| USIM | Plug type SIM Slot, support 1.8/3V/5V automatic detection. | |
| 4G | LTE antenna, SMA connector, 50Ω. | |
| GPS | LTE MIMO antenna/GPS optional | |
| Wi-Fi1 | Wi-Fi dual-band antenna, RP-SMA connector | |
| Wi-Fi2 | Wi-Fi dual-band antenna, RP-SMA connector | |
| LAN1~LAN4 | 100/1000Base-TX, MDI/MDIX self-adaption. | |

| Port | Instruction | Remark |
|-----------|--|------------------|
| WAN | 100/1000Base-TX, MDI/MDIX self-adaption. | Default as LAN |
| Reset | Reset button, (press on button at least 5 seconds) | |
| PWR | Power connector | 7.5~32VDC |
| DC | V+ and V- | |
| RS232/485 | Rx, Tx and GND | RS232 as default |

1.2 LED Status

Table 1-3 Router LED indicator Status

| silk-screen | Indicator | | Note |
|-------------|-----------|-----------------------|--------------------------------------|
| NET | Color | Green | Good Signal |
| | | Red | Poor Signal |
| | Status | Quick Blinking (0.5s) | Offline |
| | | Slow Blinking (1.5s) | 3G online |
| | | Solid light | 4G online |
| WLAN | Green | Solid light | WLAN port open, but no data sending. |
| | Green | Blinking quickly | Data is in transmitting |
| | Green | Extinguished | WLAN port isn't opened |
| LAN | Green | Solid light | Connection OK |
| | Green | Blinking | Data Sending |
| | Green | Extinguished | Not connection |

1.3 Dimension

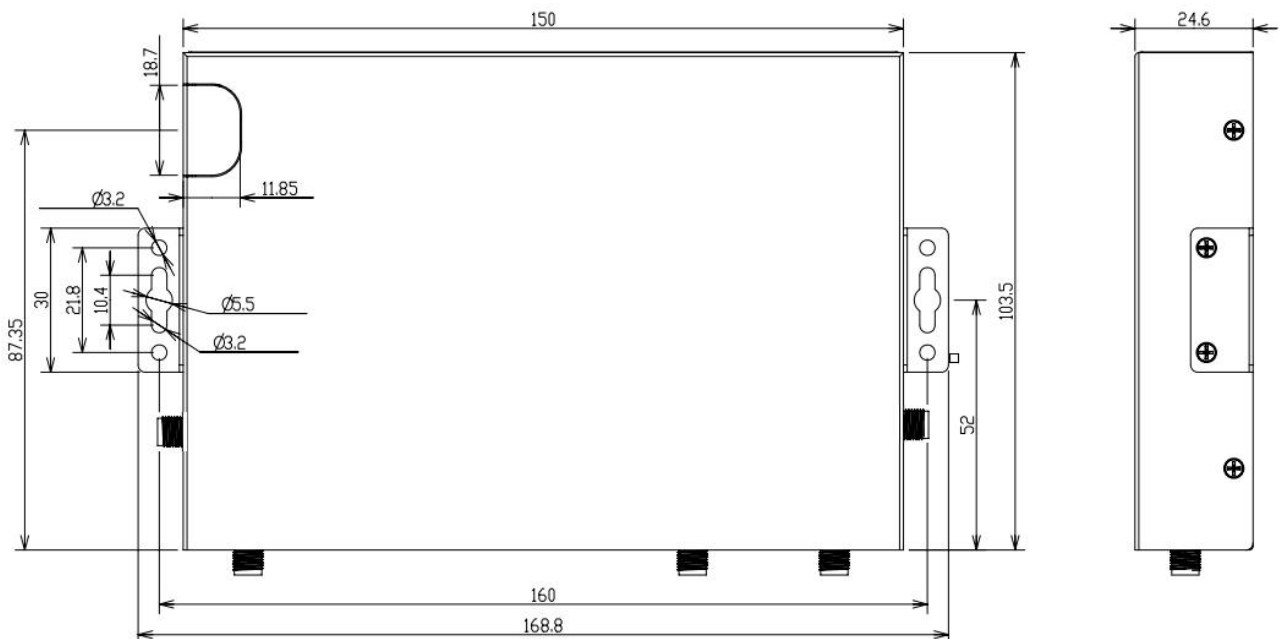
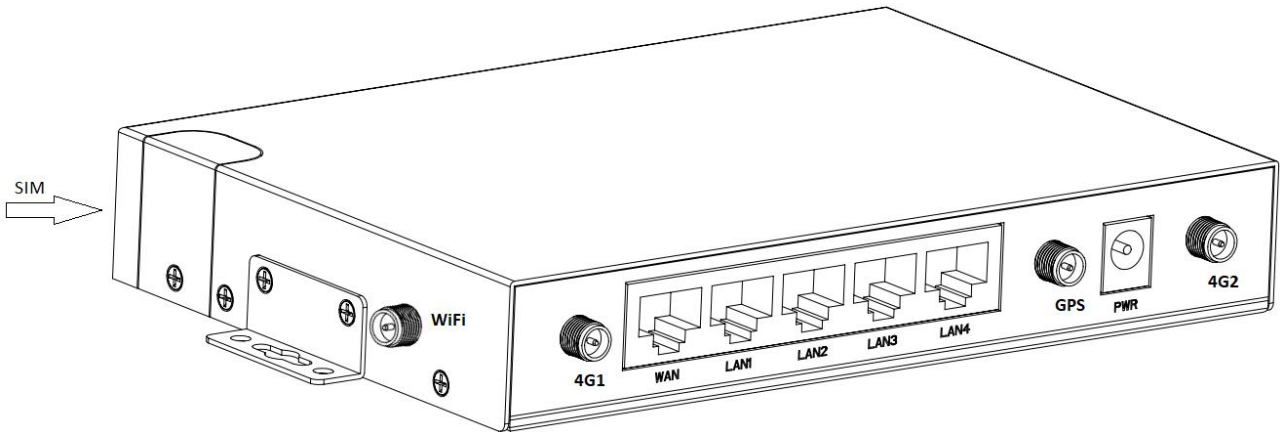


Figure 1-2 G520 Series Router Dimension

1.4 How to Install

1.4.1 SIM/UIM card install

Please insert the dual SIM cards before configure the router.



Before connecting, please disconnect any power resource of router

1.4.2 Ethernet Cable Connection

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

1.4.3 4G and Wi-Fi Antenna Plug

Connect the two magnetic 4G antennas to Main and Aux interfaces, and the two paddle shape Wi-Fi antennas to Wi-Fi1 and Wi-Fi2 interfaces.

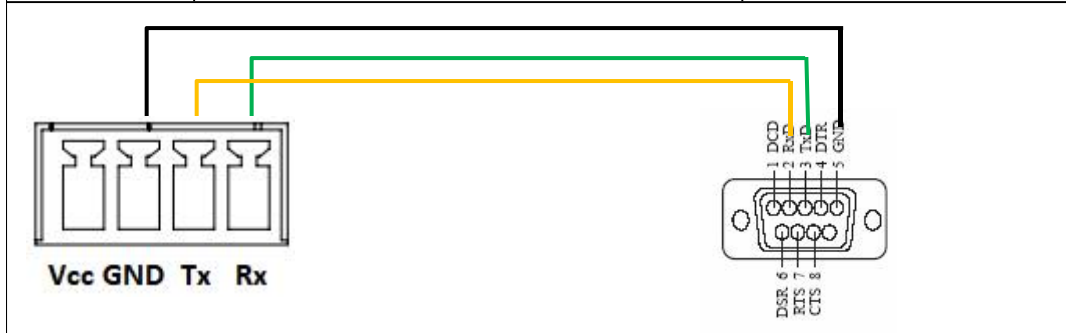


Wi-Fi antenna supports dual-band 2.4G and 5G band.

1.4.4 Serial Port (Terminal block) Connection

The serial port supports alternative RS232/RS485 port, and RS232 port as default. It might be requested serial port for RS485 when place order. 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. Below is RS232 connection sequence as reference.

| Pin | Instruction | Remark |
|-----|-------------|--------------------------------|
| 1 | Vcc | 3.3V output |
| 2 | GND | GND for RS232 communication |
| 5 | TXD/B | RS232 TXD, RS485 optional |
| 4 | RXD/A | RS232 RXD, 57600bps as default |



The serial port will be unavailable in WL-G520 standalone GPS model.

1.4.5 Power Supply

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

1.4.6 Review

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



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

Notice:

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

----END

2 Router Configuration

WL-G520 Series routers support GUI and CLI configuration. This chapter introduce GUI configuration via Ethernet port, if need CLI configuration guide, please contact our technical support department by email: support@wlink-tech.com.

2.1 Local Configure

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

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



Figure 2-1 Network Connection

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

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



Figure 2-2 User Identify Interface

----END

2.2 Status

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

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

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

Already changed login password successfully.

2.3 Overview

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

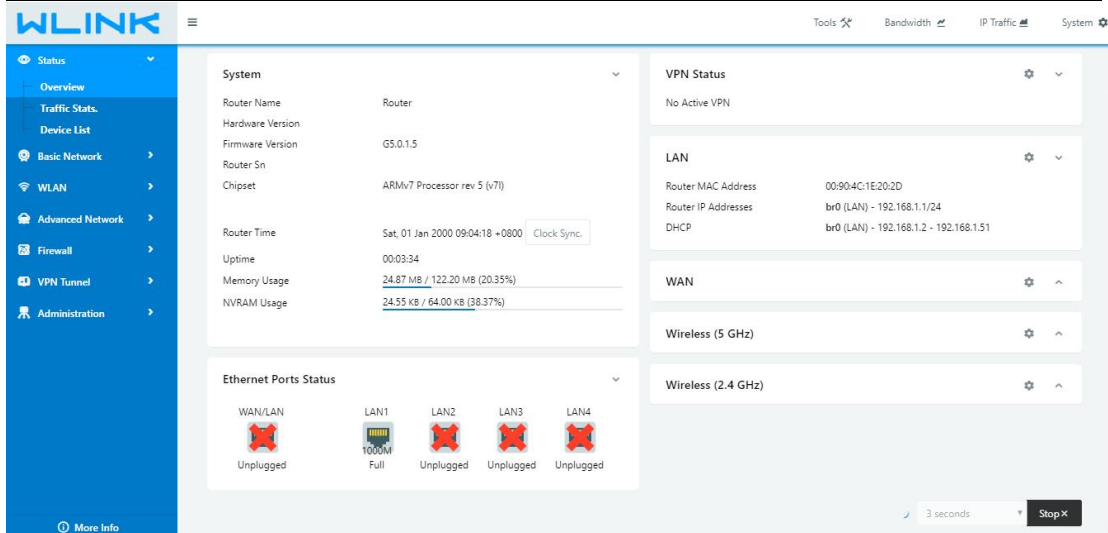


Figure 2-3 Router Status GUI

2.4 Traffic Stats.

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

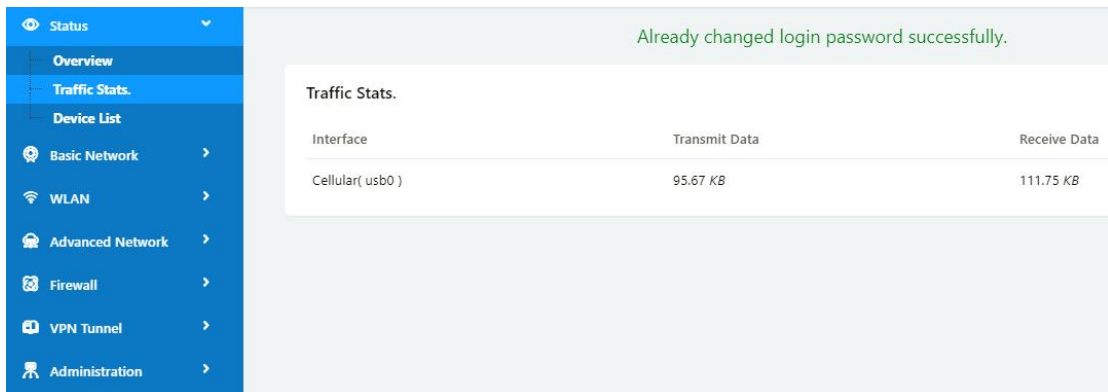


Figure 2-4 Traffic Stats. GUI

2.5 Device List

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

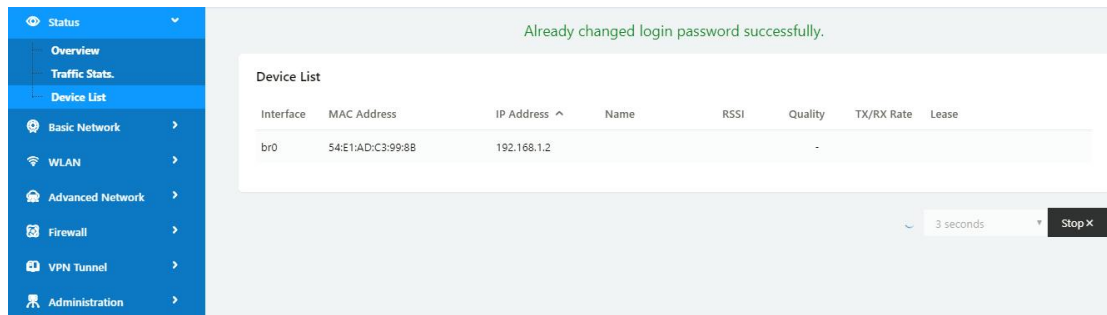


Figure 2-5 Device List GUI

2.6 Tool Column

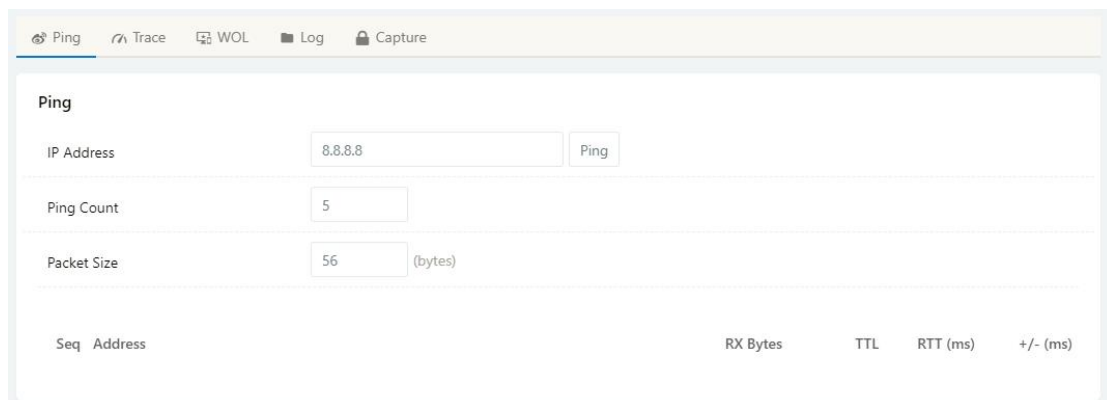


Figure 2-6 Tool Column GUI

2.6.1 Tools

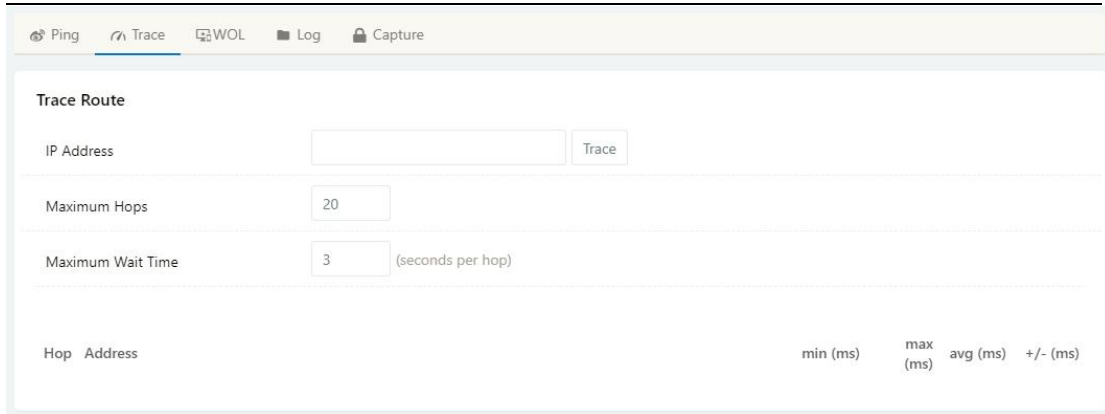
2.6.1.1 Ping

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.



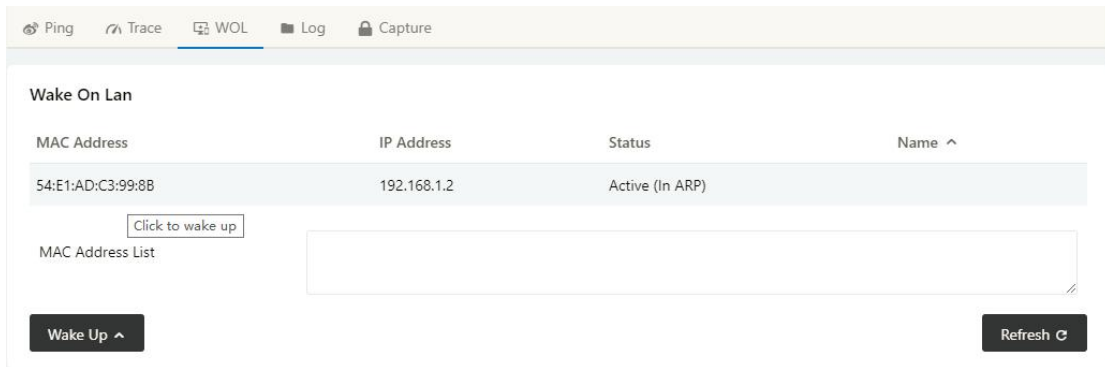
2.6.1.2 Trace

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



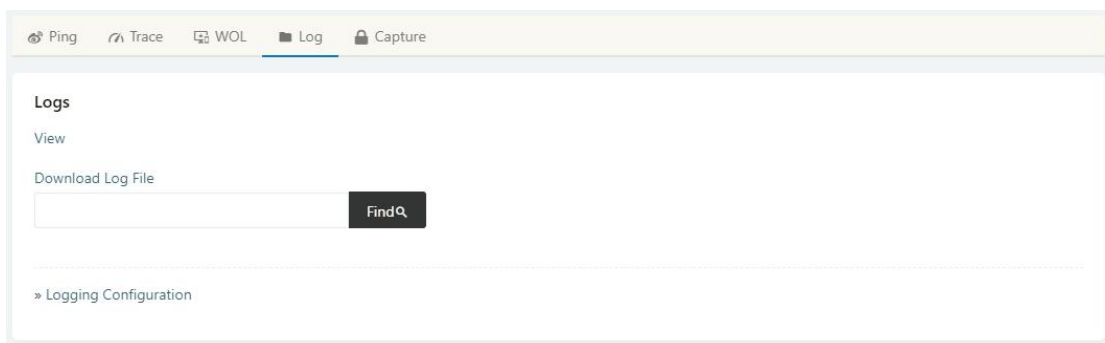
2.6.1.3 WOL

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



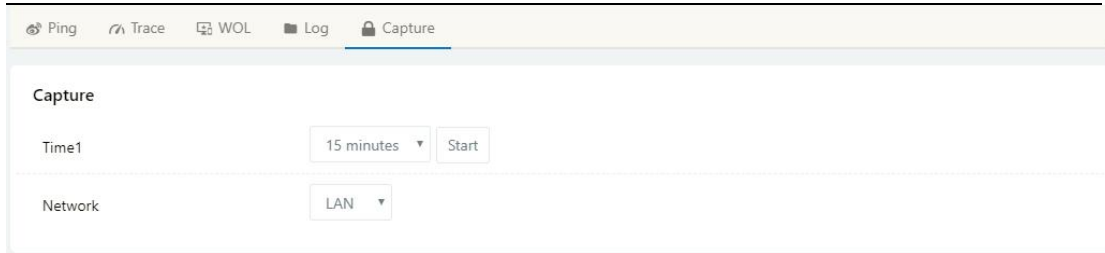
2.6.1.4 Log

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



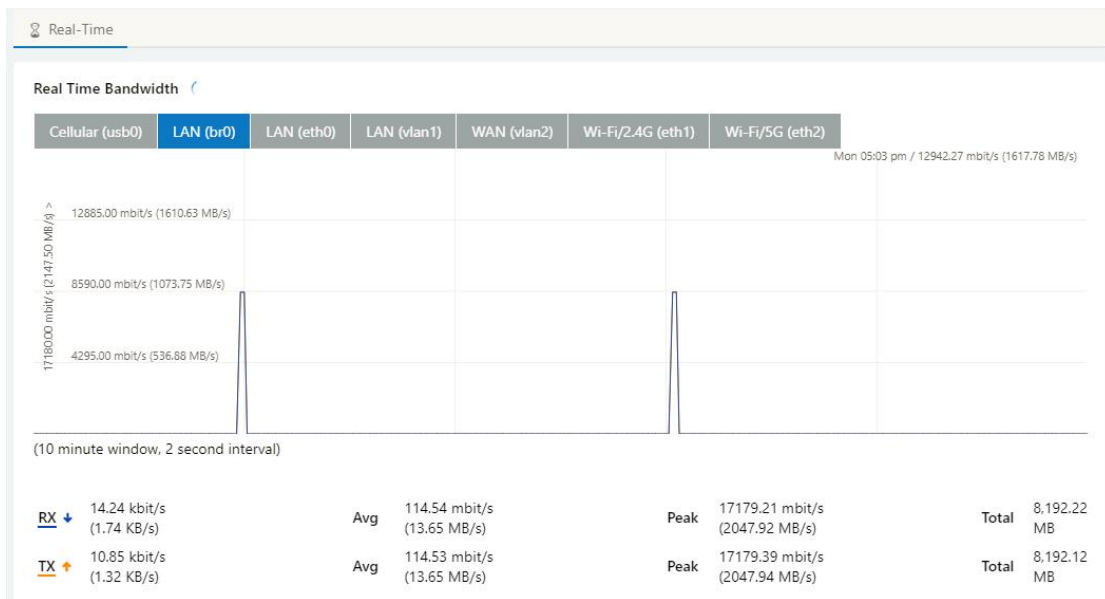
2.6.1.5 Capture

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



2.6.2 Bandwidth

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



2.6.3 System

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



2.7 Basic Network

2.7.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface.

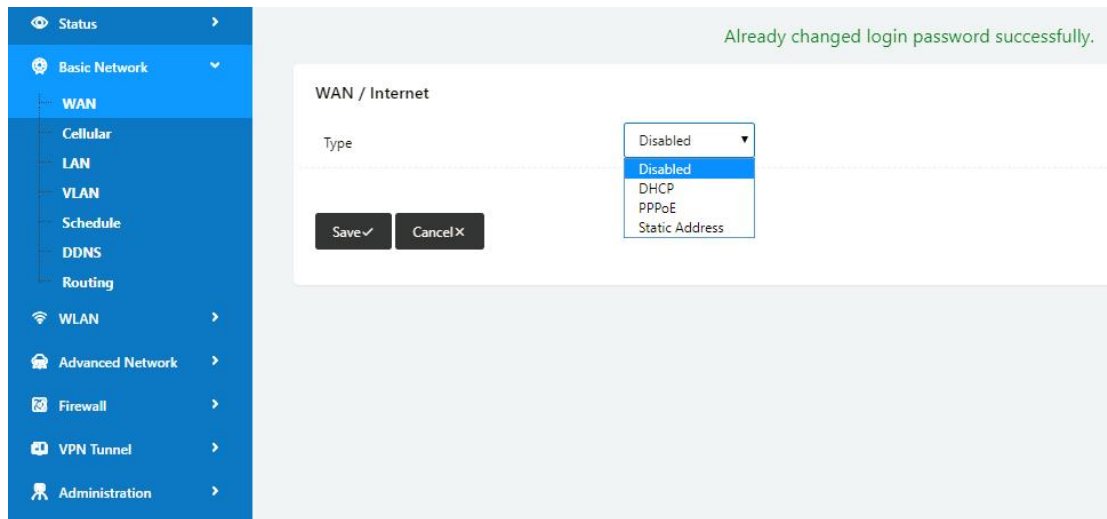


Table 2-1 WAN Setting Instruction

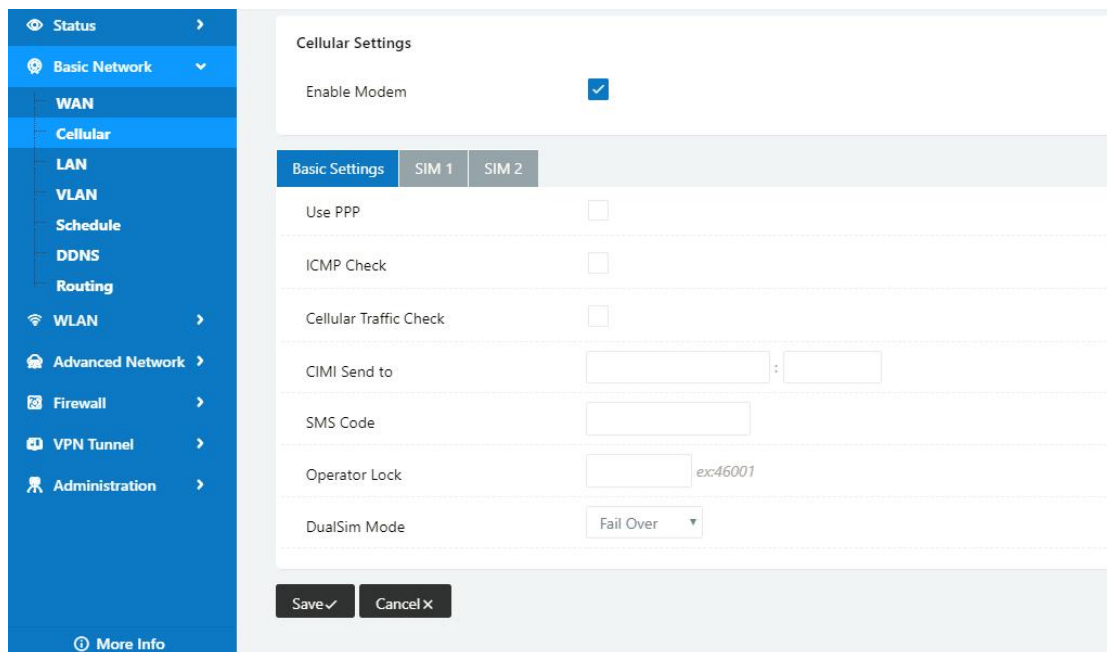
| Parameter | Instruction |
|-----------|--|
| Type | Support DHCP, PPPoE, Static IP address |

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

----End

2.7.2 Cellular Setting

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



| Basic Settings | SIM 1 | SIM 2 |
|------------------------|----------------------|-------|
| SIM 1 Mode | Auto ▼ | |
| SIM 1 PIN Code | <input type="text"/> | |
| 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 | <input type="text"/> | |

Table 2-2 WAN 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 | <p>【Fail Over】 Two SIM cards mutual backup. Once SIM1 failed, it'll switch to SIM2 and work on SIM2, and vice versa.</p> <p>【SIM1 Only】 Only SIM1 works.</p> <p>【SIM2 Only】 Only SIM2 works.</p> <p>【Backup】 SIM1 is the primary SIM. Once SIM1 failed, it'll switch to SIM2 and work on SIM2 for a specified period of time, then it switches back to SIM1.</p> |

| Parameter | Instruction |
|----------------------|--|
| Connect Mode | <p>【Auto】 The router will automatically connect to 3G/4G networks and give priority to 4G.</p> <p>【LTE】 Router will connect to 4G only.</p> <p>【3G】 Router will connect to 3G only.</p> |
| Pin Code | Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen. |
| APN | APN is provided by local ISP, usually CDMA/EVDO networks do not need this parameter. |
| User | SIM card user name is provided by ISP |
| Password | SIM card password is provided by ISP |
| Auth. Type | Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional. |
| SIM Local IP Address | Fix SIM IP. The feature is available if carrier can provide this service. |



NOTE ICMP Check and Cellular Traffic Check are alternative.

【ICMP Check】

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

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

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

【Cellular Traffic Check】

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

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

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

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

----End

2.7.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface

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 | |
| 1 | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Add +

Save ✓ Cancel X

| LAN | | | | | | |
|----------|----------------------|----------------------|--------------------------|----------------------|----------------------|----------------------|
| Bridge ^ | IP Address | Subnet Mask | DHCP Server | IP Pool | Lease(minutes) | |
| br0 | 192.168.1.1 | 255.255.255.0 | ✓ | 192.168.1.2 - 51 | 1440 | |
| 1 | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Add +

Save ✓ Cancel X

Table 2-3 LAN Setting Instruction

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

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

----End

2.7.4 VLAN

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

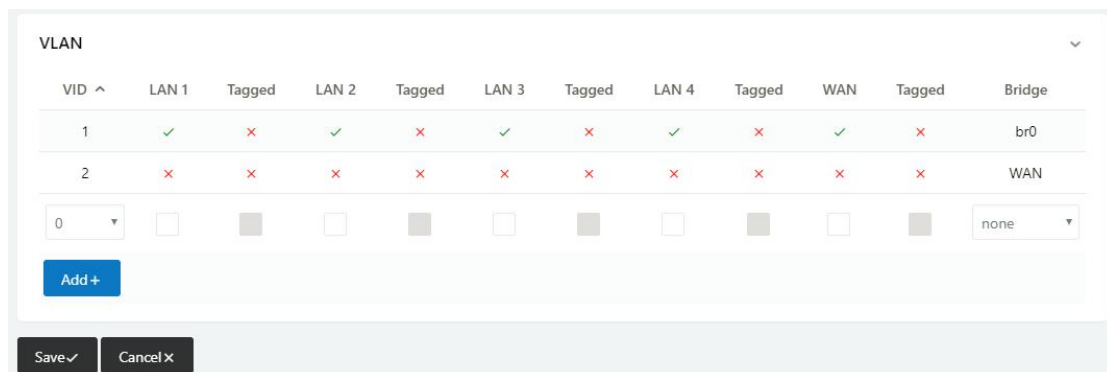


Table 2-4 LAN Setting Instruction

| Parameter | Instruction |
|----------------|--|
| VID | VLAN ID number. The VID range is from 1 to 15. |
| 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.

----End

2.7.5 VLAN

Step 3 Basic Network->VLAN to enter the VLAN setting page.

| VID ^ | LAN 1 | Tagged | LAN 2 | Tagged | LAN 3 | Tagged | LAN 4 | Tagged | WAN | Tagged | Bridge |
|-------|-------|--------|-------|--------|-------|--------|-------|--------|-----|--------|--------|
| 1 | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | br0 |
| 2 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | WAN |

0 none

Add+

Save ✓ Cancel ✗

Table 2-5 LAN Setting Instruction

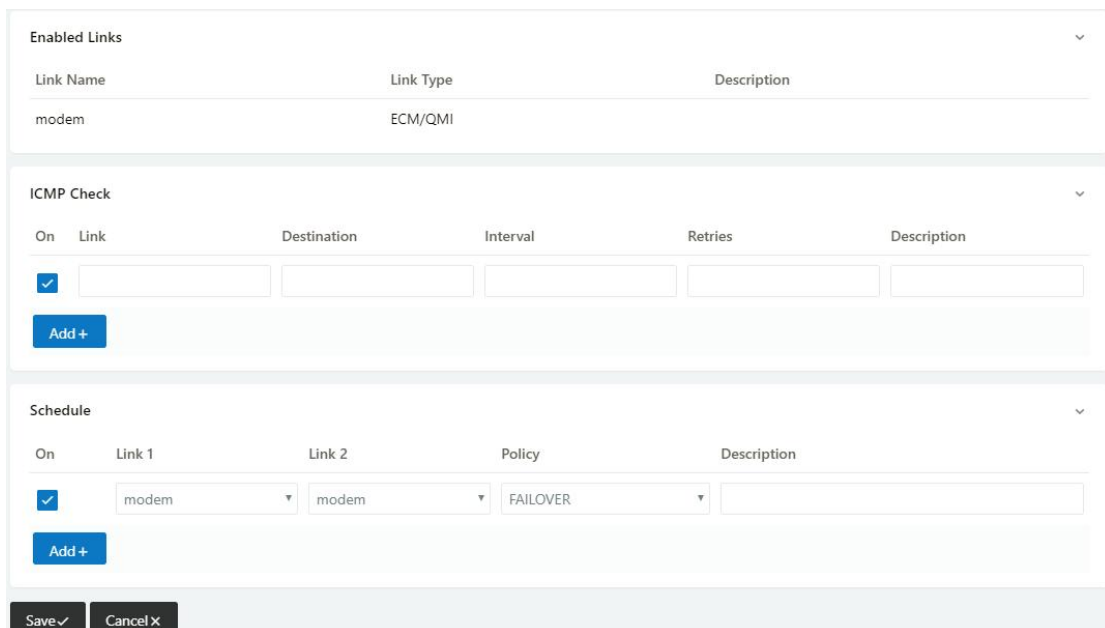
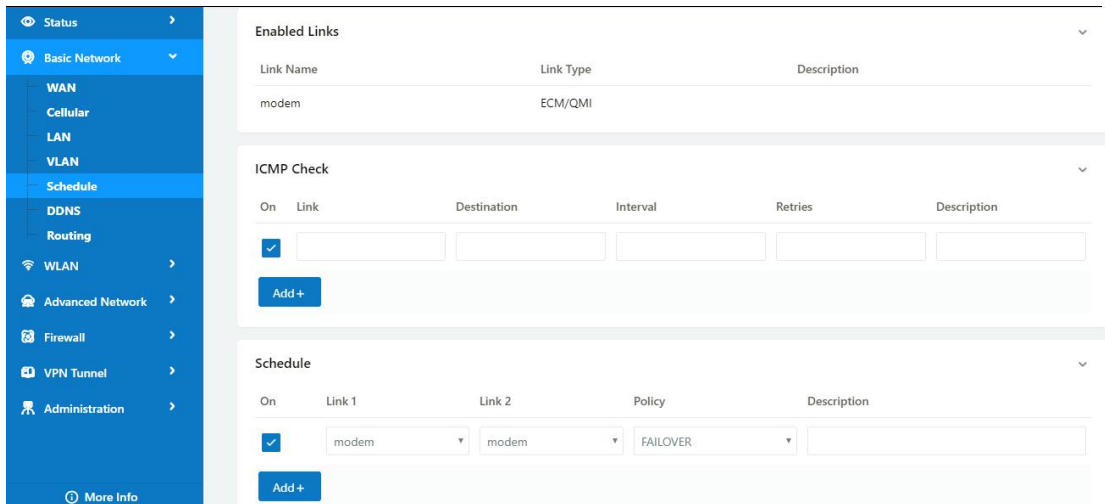
| Parameter | Instruction |
|----------------|--|
| VID | VLAN ID number. The VID range is from 1 to 15. |
| LAN1~LAN4, WAN | LAN |
| Tagged | Enable to make router can encapsulate and de-encapsulate the VLAN tag. |
| Bridge | Routers interface br0, br1, br2, br3 and WAN |

Step 4 Please Click “Save” to finish.

----End

2.7.6 Schedule

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



Step 2 Please Click “Save” to finish.

----End

2.7.7 Dynamic DNS Setting

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

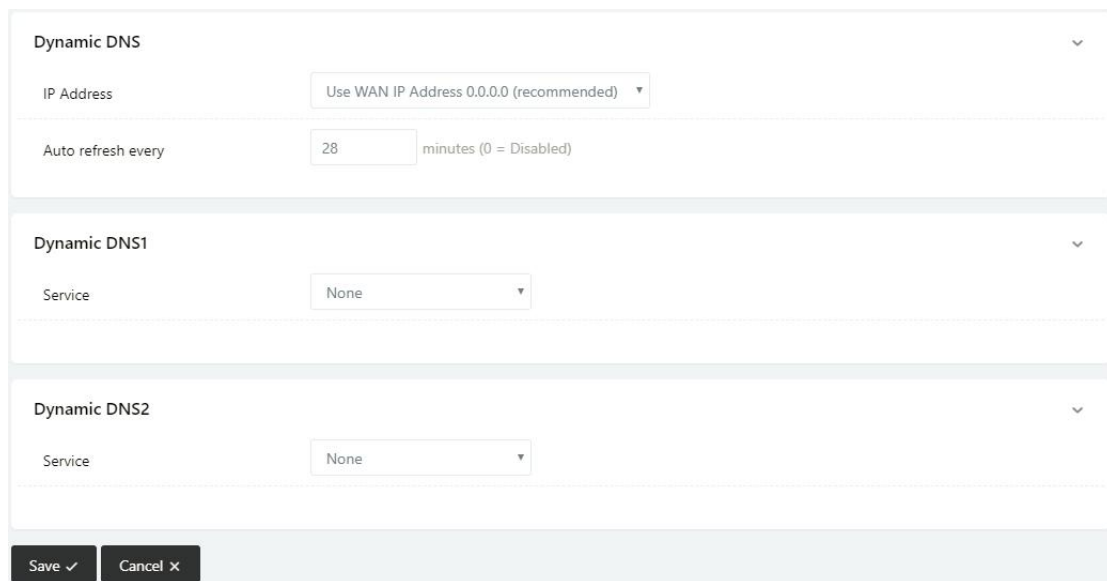
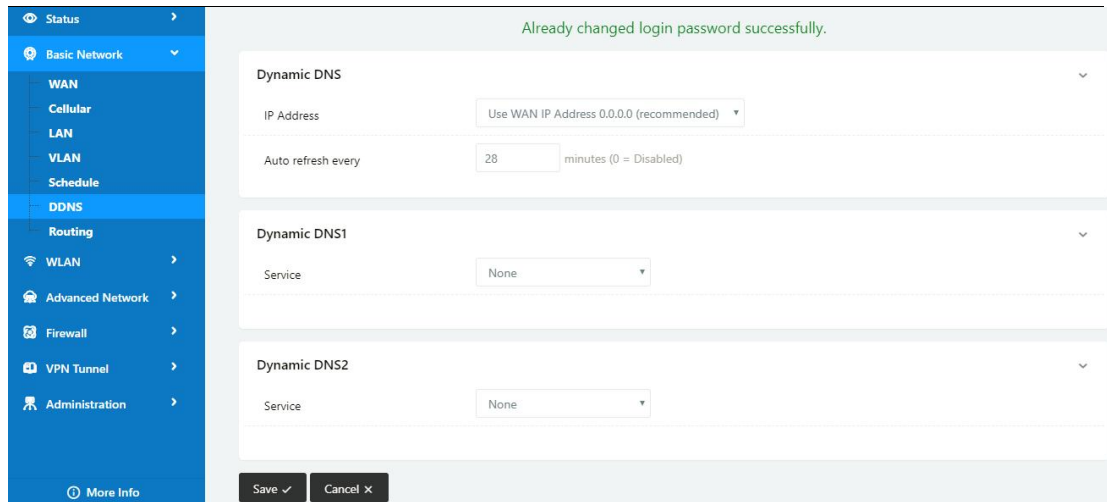


Table 2-6 DDNS Setting Instruction

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

Step 2 Please Click “Save” to finish.

----End

2.7.8 Routing Setting

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

Table 2-7 Routing Setting Instruction

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

Step 2 Please Click “ Save “ to finish.

----End

2.8 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.

2.8.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter

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

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

Table 2-8 Basic of WLAN Setting Instruction

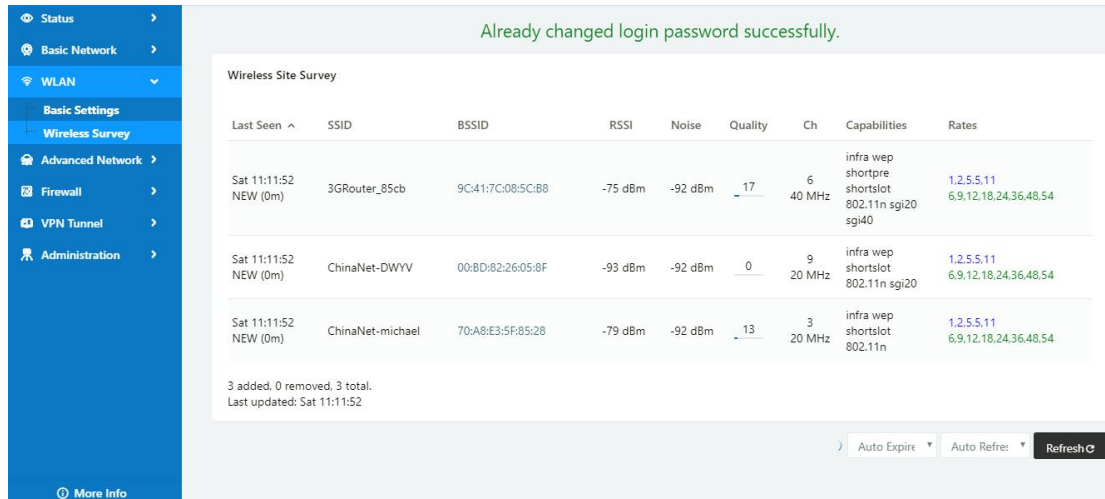
| Parameter | Instruction |
|---------------------------|---|
| Radio Mode | 2.4G+5G mode as default. Support 2.4G, 5G modes optional. 2.4G+5G model, Wi-Fi bandwidth for 683Mbps 2.4G model, Wi-Fi bandwidth for 300Mbps 5G model, Wi-Fi bandwidth for 866Mbps |
| Enable wireless | Enable or Disable the Wireless |
| Wireless mode | Support AP mode. |
| 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 80MHz alternative for 2.4G. |
| Security | Support various encryption method as requested. |

Step 2 Please click “Save” to finish.

----End

2.8.2 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.



2.9 Advanced Network Setting

2.9.1 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.

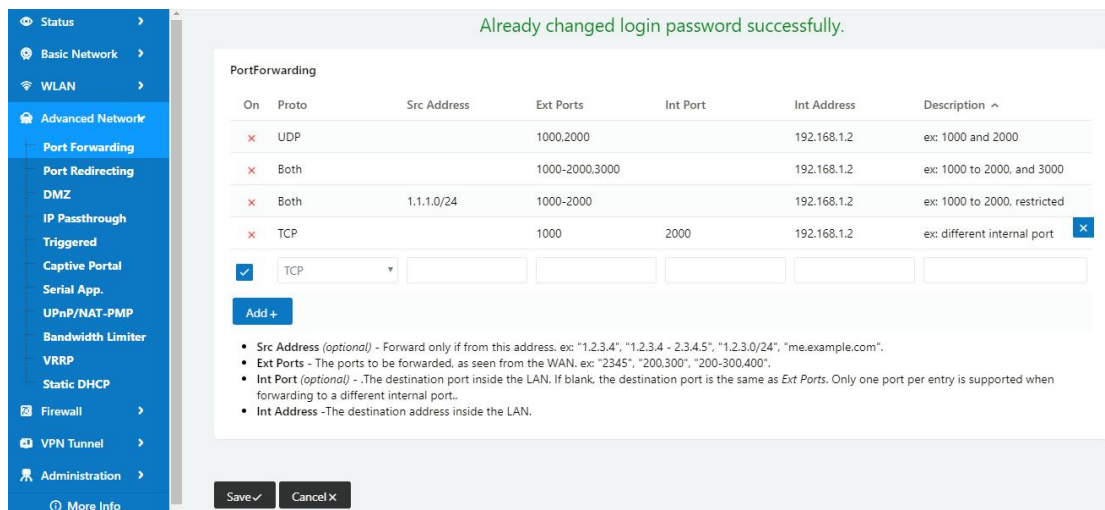


Table 2-9 Port Forwarding Instruction

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

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

Step 2 Please click "save" to finish

----End

2.9.2 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.

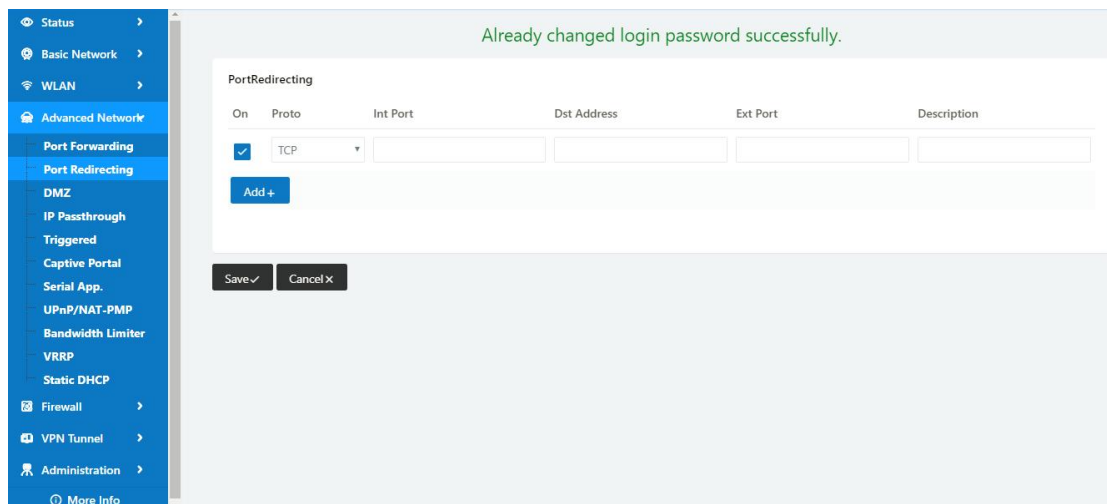


Table 2-10 Port Redirecting Instruction

| 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.



Configuration Instance

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

----End

2.9.3 DMZ Setting

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

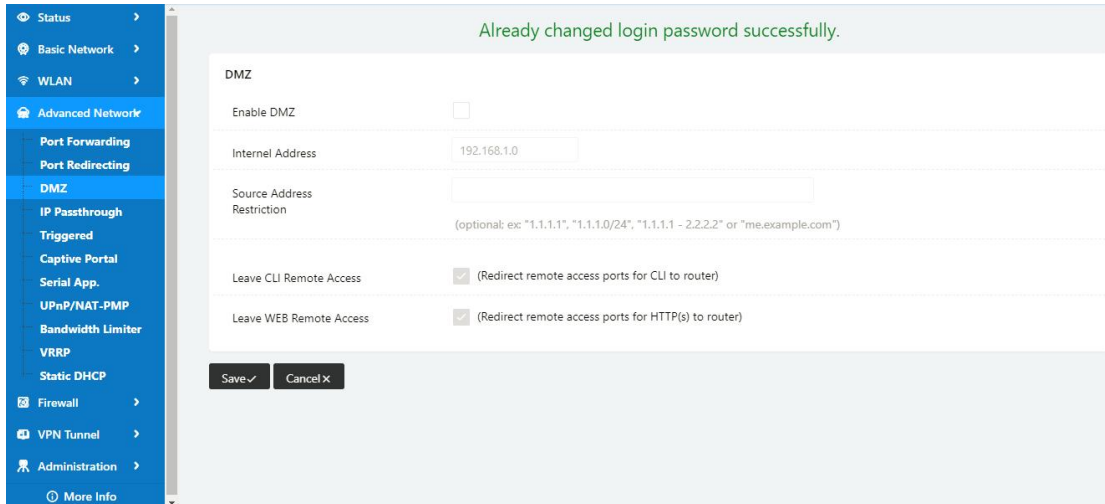


Table 2-11 DMZ Instruction

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

Step 2 Please click "save" to finish

----End

2.9.4 IP Passthrough Setting

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

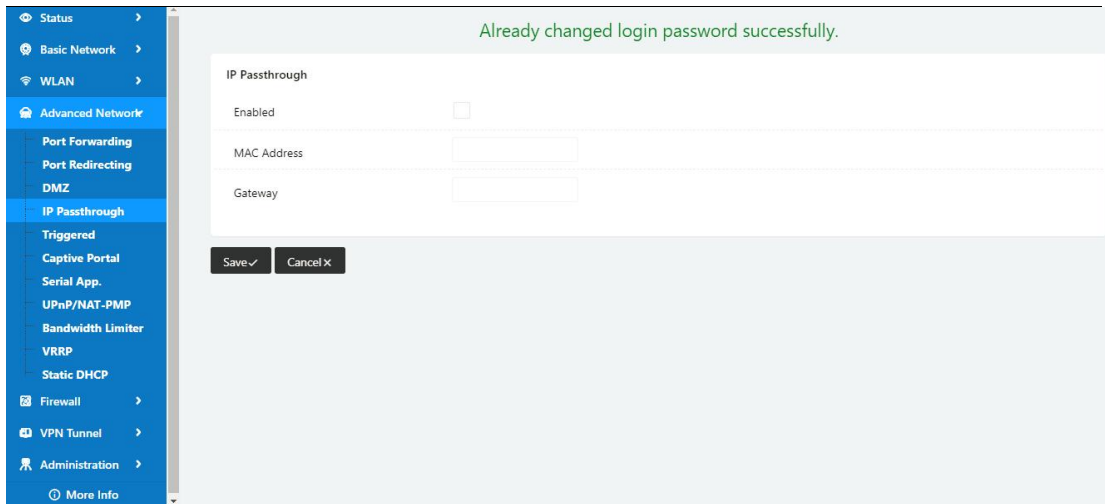


Table 2-12 IP Passthrough Instruction

| parameter | Instruction |
|-------------|---|
| Enable | Enable IP Passthrough |
| MAC Address | Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP. |
| Gateway | If WL-G520 connect to multiple device, input other device gateway. The device might access to router GUI. |

Step 2 Please click "save" to finish

----End

2.9.5 Triggered Setting

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

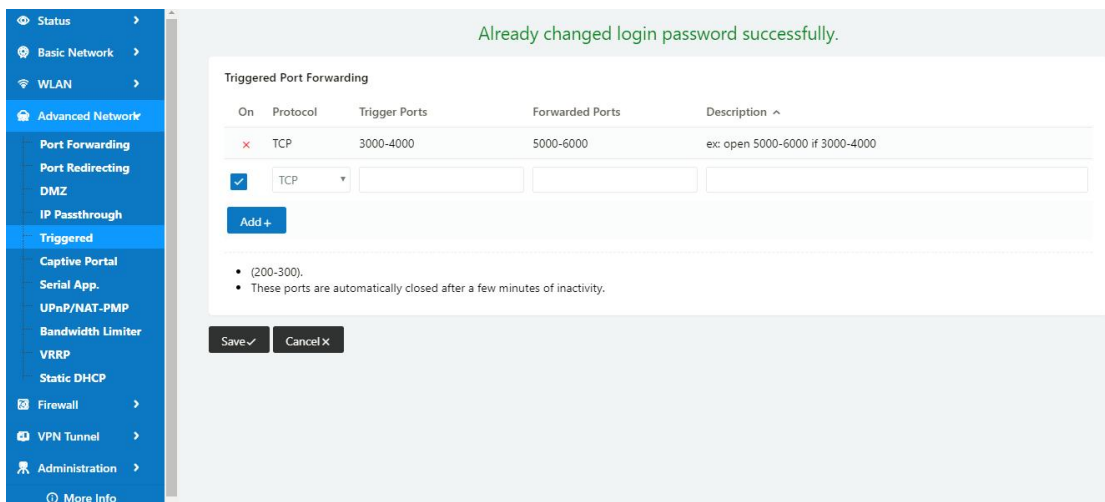


Table 2-13 Triggered Instruction

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

Step 2 Please click "save" to finish.

----End

2.9.6 Captive Portal

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

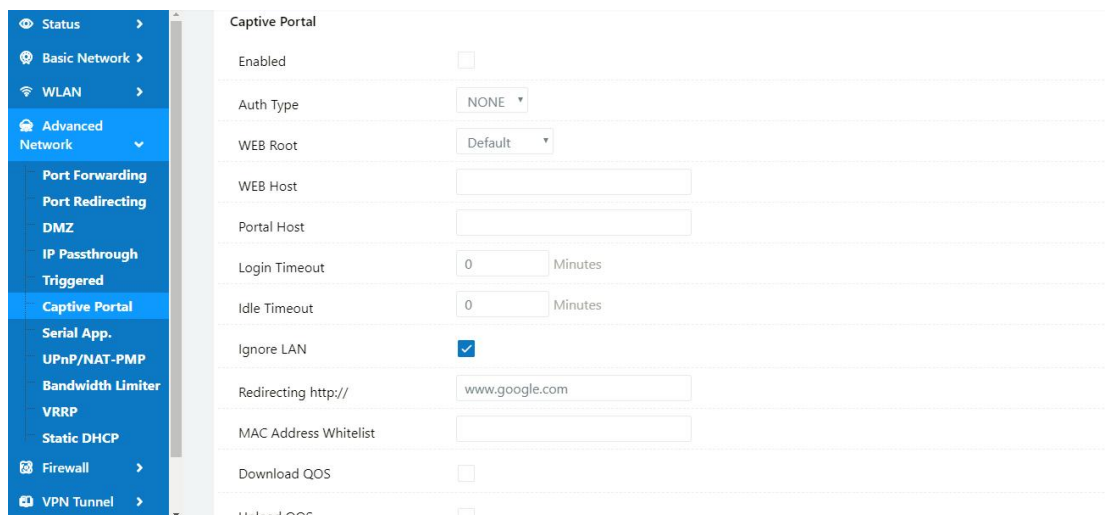


Table 2-14 Captive Portal Instruction

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

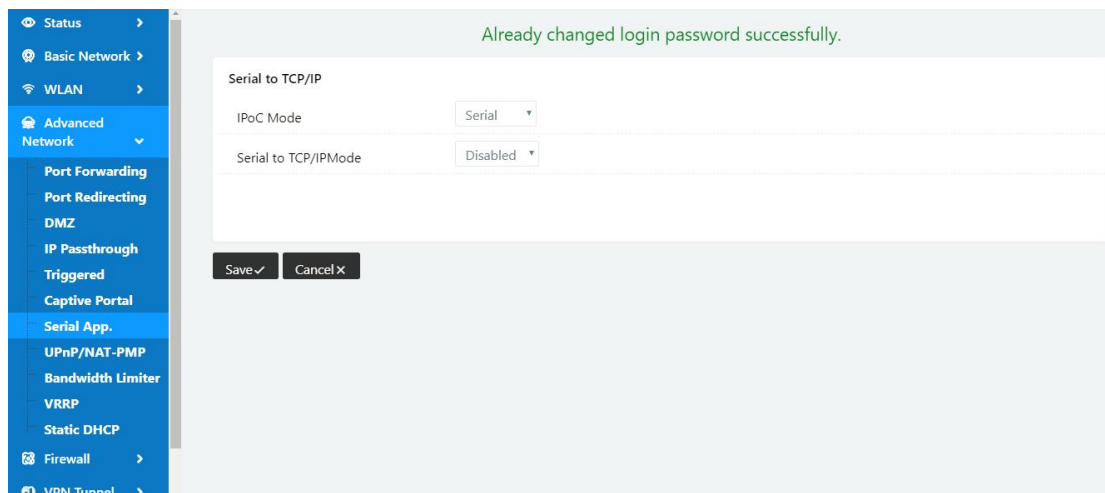
| Parameter | Instruction |
|----------------|---|
| Web Host | Configure domain name for the captive portal access. For example, Configure as wlink.tech.com, we might directly access to captive portal page in the website as wlink.tech.com |
| Portal Host | Reserved. |
| Logged Timeout | Maximum time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

Step 2 Please click "save" to finish.

----End

2.9.7 Serial App. Setting

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



Serial to TCP/IP

IPOC Mode: Serial

Serial to TCP/IP Mode: Client

Server IP/Port: 8.8.8.8 : 40002

Socket Type: TCP

Socket Timeout: 500 (milliseconds)

Serial Timeout: 500 (milliseconds)

Packet Payload: 1024 (bytes)

Heart-Beat Content:

Heart-Beat Interval: 2 (seconds)

Port Type: RS485/RS232

Cache Enable:

Debug Enable:

Baud Rate: 57600

Parity Bit: none

Data Bit: 8

Stop Bit: 1

Save ✓ Cancel ✕

Table 2-15 Serial App Instruction

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

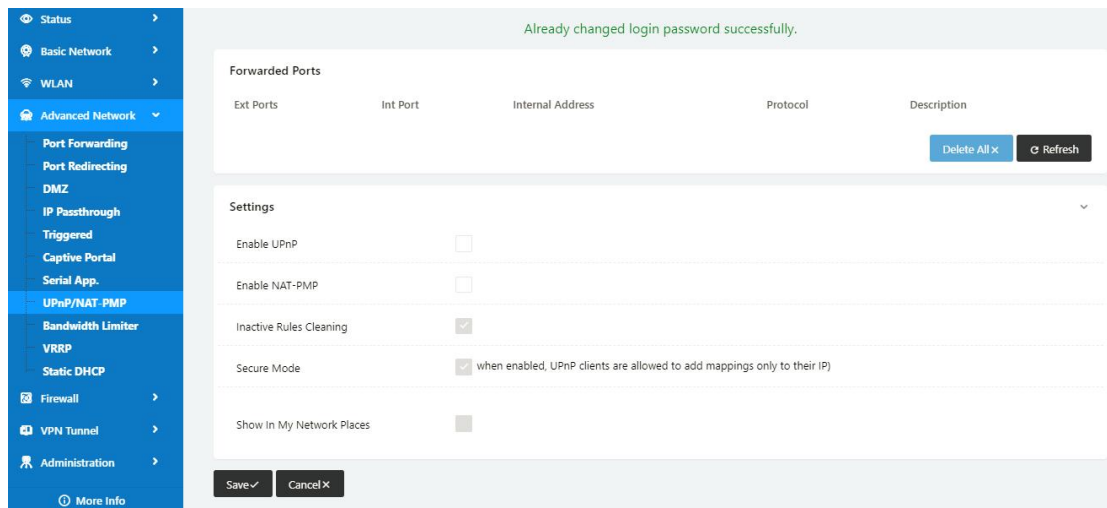
| Parameter | Instruction |
|------------|-------------------|
| Baud Rate | 115200 as default |
| Parity Bit | None as default |
| Data Bit | 8bit as default |
| Stop Bit | 1bit as default |

Step 2 Please click "save" to finish.

----End

2.9.8 UPnP/NAT-PMP Setting

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



Step 2 Please click "save" to finish.

----End

2.9.9 Bandwidth Control Setting

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

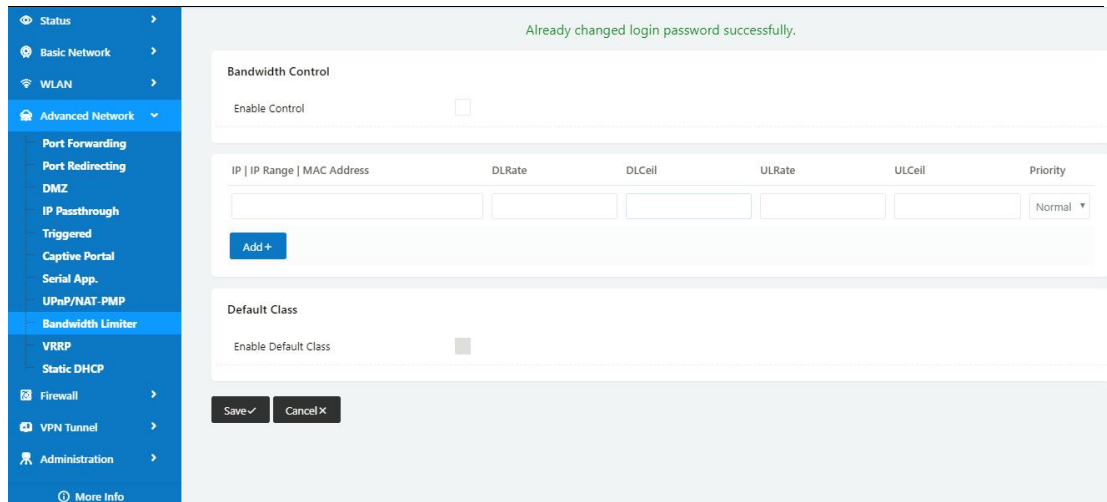


Table 2-16 Bandwidth Control Instruction

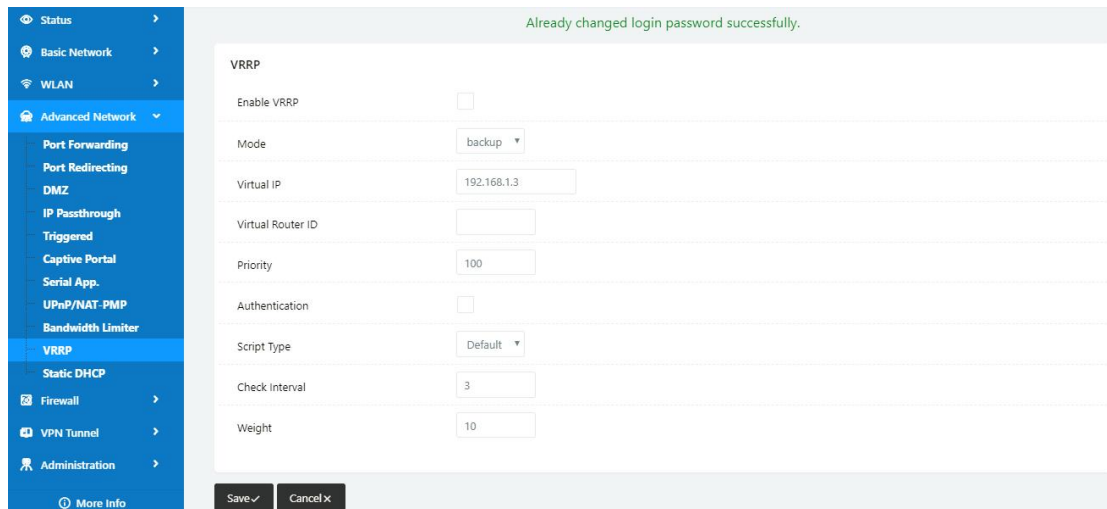
| | |
|---------------------------|--|
| Max Available Download | Speed limit for router. |
| Max Available Upload | Speed limit for router. |
| IP/ IP Range/ MAC Address | Limit devices speed for specified IP/IP Range/ MAC Address. |
| DL Rate | Mix Download rate |
| DL ceil | Max download rate |
|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

Step 2 Please click "save" to finish.

----End

2.9.10 VRRP Setting

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

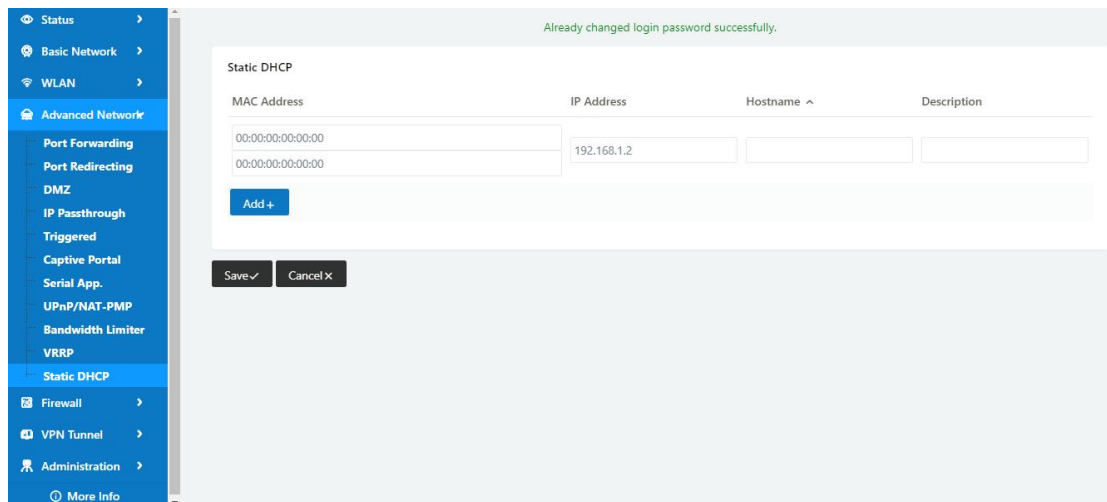


Step 2 Please click "save" to finish.

----End

2.9.11 Static DHCP Setting

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



Step 2 Please click "save" to finish.

----End

2.10 Firewall

2.10.1 IP/URL Filtering

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

Table 2-17 IP/URL Filtering Instruction

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

Step 2 Please click "save" to finish.

---End

2.10.2 Domain Filtering

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

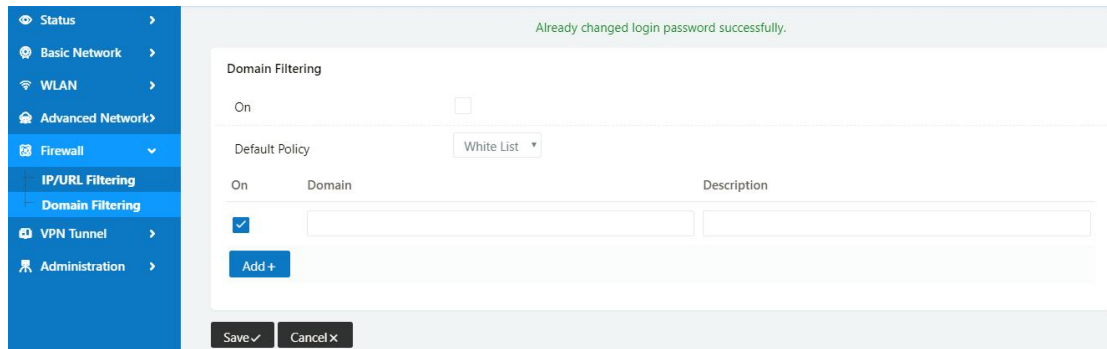


Table 2-18 Domain Filtering Instruction

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

Step 2 Please click "save" to finish.

----End

2.11 VPN Tunnel

2.11.1 GRE Setting

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

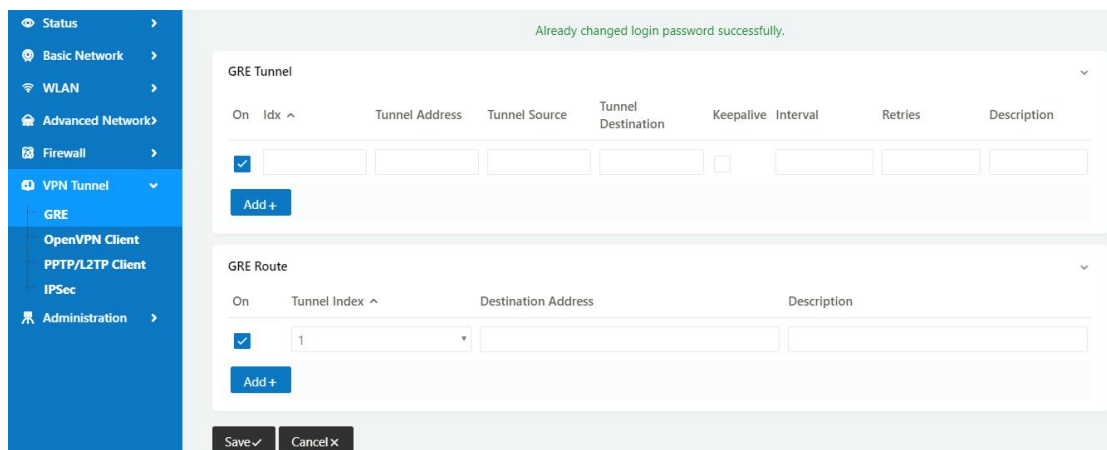


Table 2-19 GRE Instruction

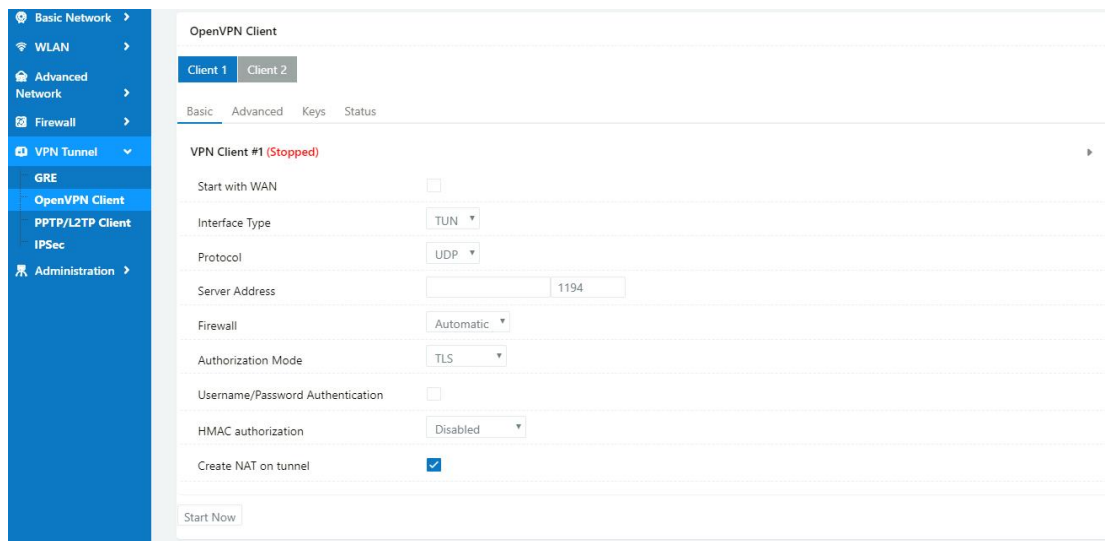
| Parameter | Instruction |
|--------------------|---|
| IDx | GRE tunnel number |
| Tunnel Address | GRE Tunnel local IP address which is a virtual IP address. |
| Tunnel Source | Router's 3G/WAN IP address. |
| Tunnel Destination | GRE Remote IP address. Usually a public IP address |
| Keep alive |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

Step 2 Please click "save" to finish.

----End

2.11.2 OpenVPN Client Setting

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



OpenVPN Client

Client 1
Client 2

Basic
Advanced
Keys
Status

VPN Client #1 (Stopped)

Start with WAN

Interface Type TUN ▼

Protocol UDP ▼

Server Address 1194

Firewall Automatic ▼

Authorization Mode TLS ▼

Username/Password Authentication

HMAC authorization Disabled ▼

Create NAT on tunnel

Start Now

Save ✓
Cancel ✕

Table 2-20 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. |
| Firewall | Auto, External only and Custom are optional |
| Authorization Mode | TLS, Static key and Custom are optional. |
| User name/Password | As the configuration requested. |

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

Table 2-21 Advanced of OpenVPN Instruction

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

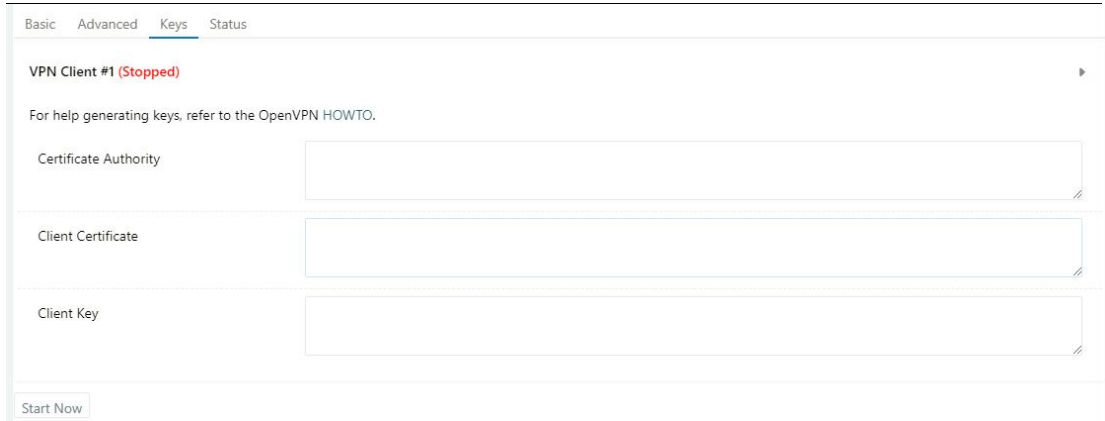


Table 2-22 Keys of OpenVPN Instruction

| 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 |

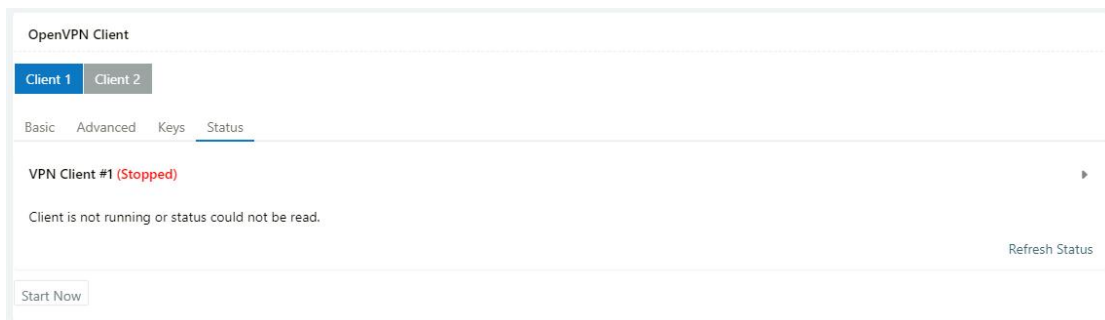


Table 2-23 Status of OpenVPN Instruction

| Parameter | Instruction |
|-----------|---|
| Status | Check Openvpn status and data statistics. |

Step 2 Please click "save" to finish.

----End

2.11.3 PPTP/L2TP Client Setting

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

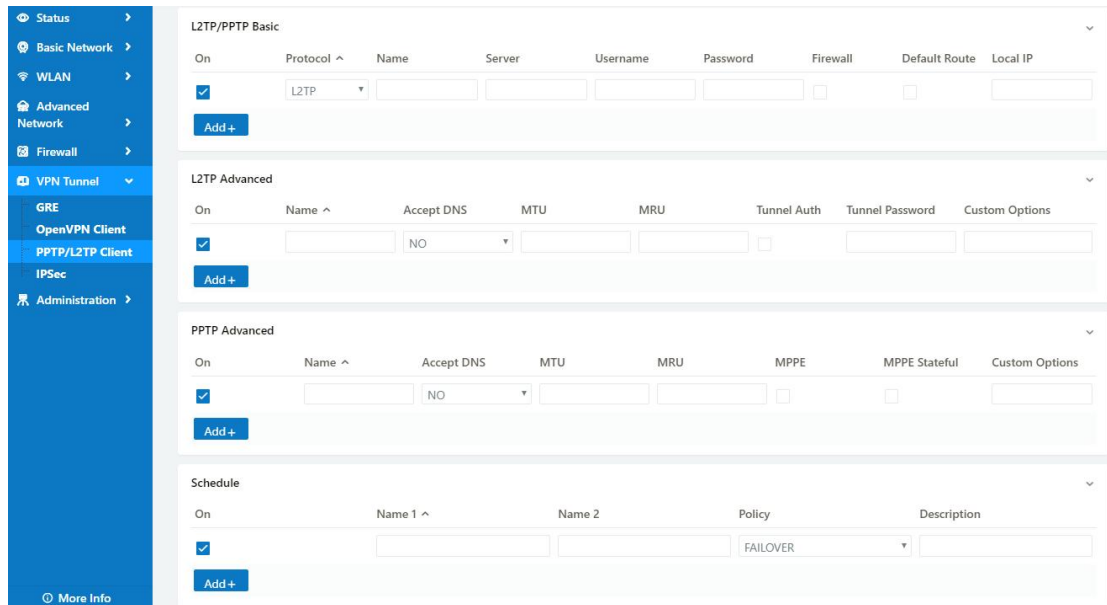


Table 2-24 PPTP/L2TP Basic Instruction

| 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 2-25 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 2-26 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 |

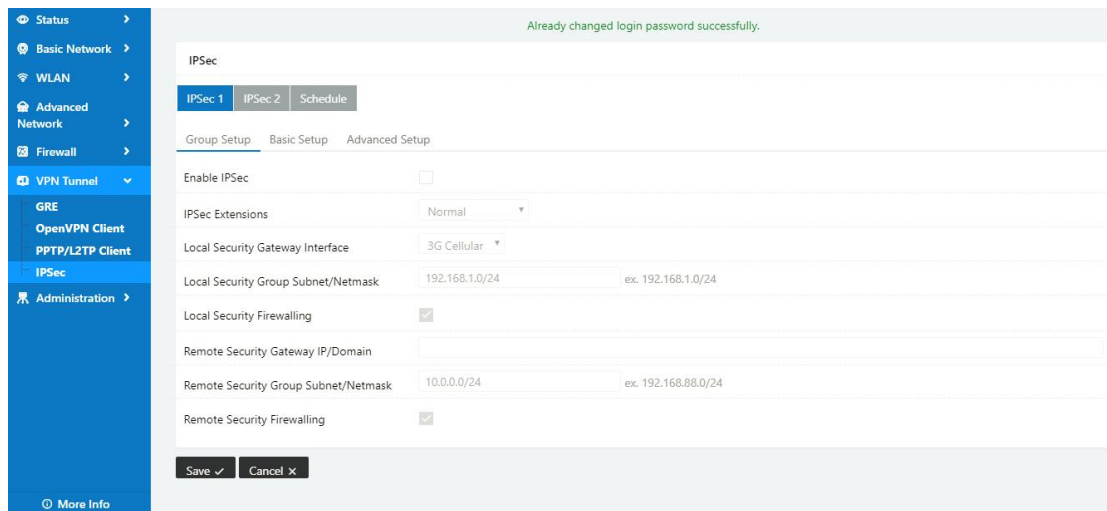
Table 2-27 SCHEDULE Instruction

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

Step 2 Please click "save" to finish.

---End

2.11.4 IPSec Setting



2.11.4.1 IPSec Group Setup

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

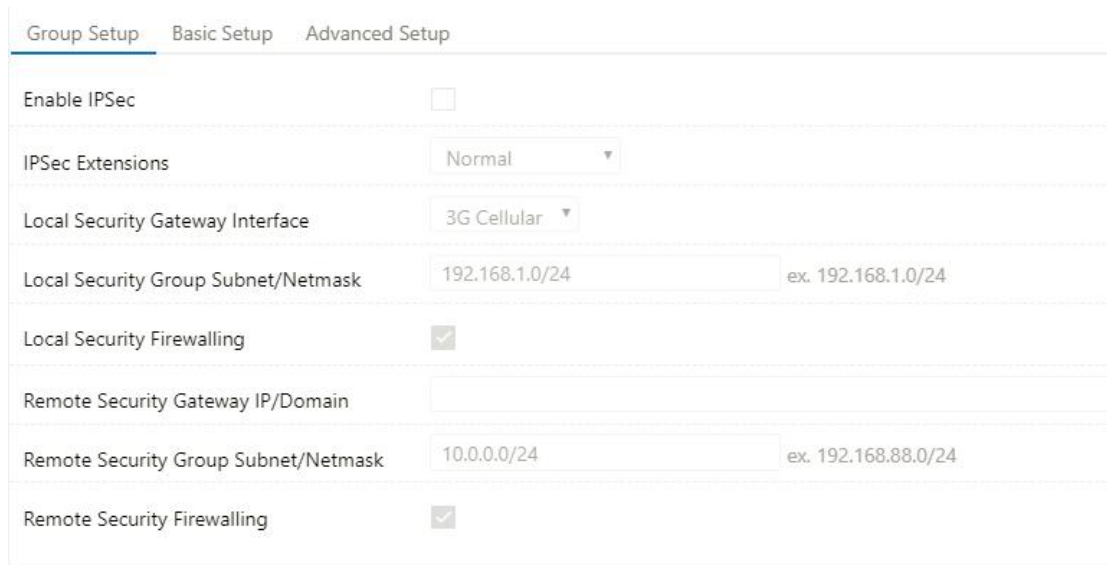


Table 2-28 IPSec Group Setup Instruction

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

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

Step 2 Please click "save" to finish.

2.11.4.2 IPSec Basic Setup

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

Group Setup **Basic Setup** Advanced Setup

Keying Mode: IKE with Preshared Key ▼

Phase 1 DH Group: Group 2 - modp1024 ▼

Phase 1 Encryption: 3DES (168-bit) ▼

Phase 1 Authentication: MD5 HMAC (96-bit) ▼

Phase 1 SA Life Time: 28800 seconds

Phase 2 DH Group: Group 2 - modp1024 ▼

Phase 2 Encryption: 3DES (168-bit) ▼

Phase 2 Authentication: MD5 HMAC (96-bit) ▼

Phase 2 SA Life Time: 3600 seconds

Preshared Key:

Table 2-29 IPSec Basic Setup Instruction

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

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

Step 2 Please click "save" to finish.

2.11.4.3 IPSec Advanced Setup

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

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

Table 2-30 IPSec Advanced Setup Instruction

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

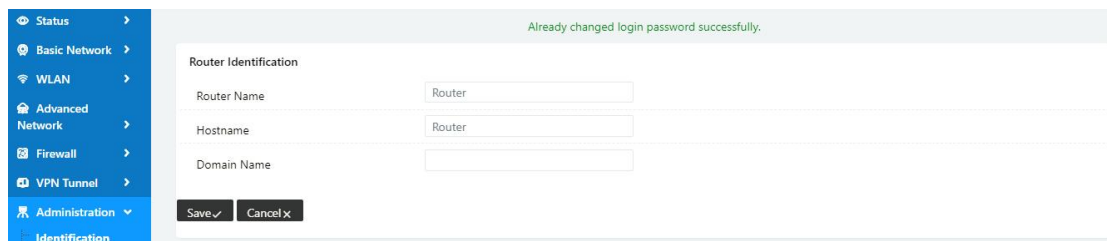
Step 2 Please click "save" to finish.

----End

2.12 Administration

2.12.1 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.



Router Identification

Router Name

Hostname

Domain Name

Table 2-31 Router Identification Instruction

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

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

Step 2 Please click "save" to finish

----End

2.12.2 Time Setting

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

The screenshot displays the 'Time' configuration page in the router's web interface. The left-hand navigation menu is expanded to show 'Administration', with 'Time' selected. The main panel shows the following settings:

- Router Time:** Sat, 01 Jan 2000 09:01:24 +0800. A 'Clock Sync.' button is present.
- Time Zone:** A dropdown menu showing 'UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan'.
- Auto Daylight Savings Time:** A checked checkbox.
- Auto Update Time:** A dropdown menu set to 'Every 4 Hours'.
- Trigger Connect On Demand:** An unchecked checkbox.
- NTP Time Server:** A dropdown menu set to 'Asia'.
- NTP Servers:** A list of servers: 0.asia.pool.ntp.org, 1.asia.pool.ntp.org, 2.asia.pool.ntp.org.

At the bottom of the configuration area, there are two buttons: 'Save ✓' and 'Cancel ✕'.



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

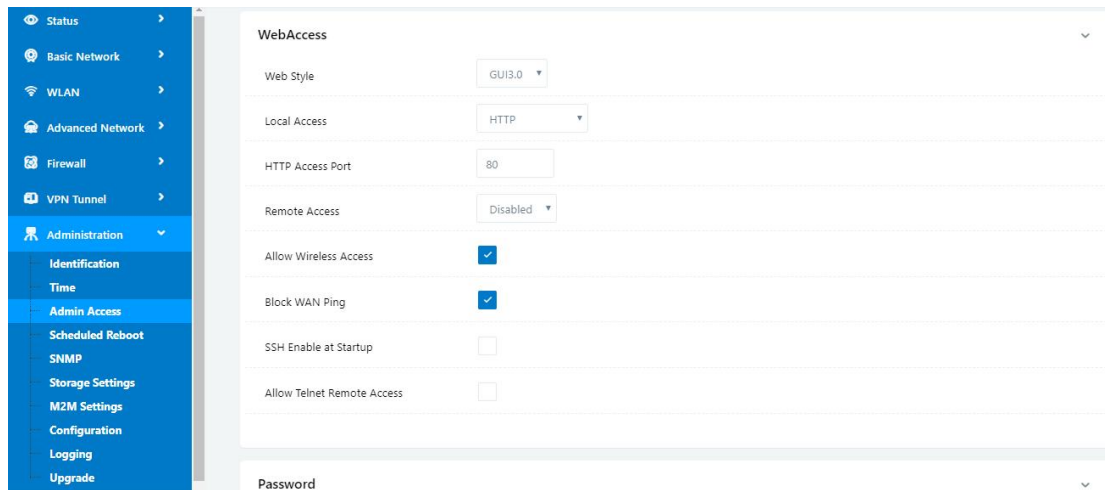
Step 2 Please click “save to finish.

----End

2.12.3 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.

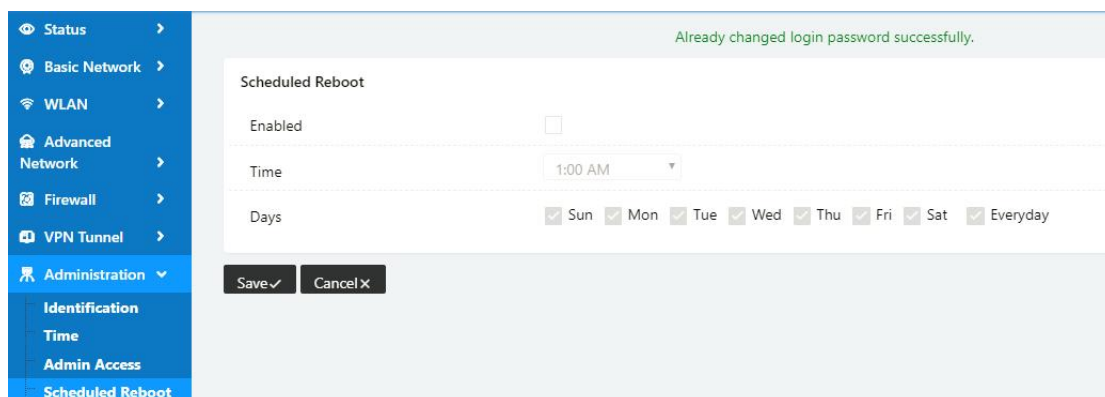


Step 2 Please click save icon to finish the setting

----End

2.12.4 Schedule Reboot Setting

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

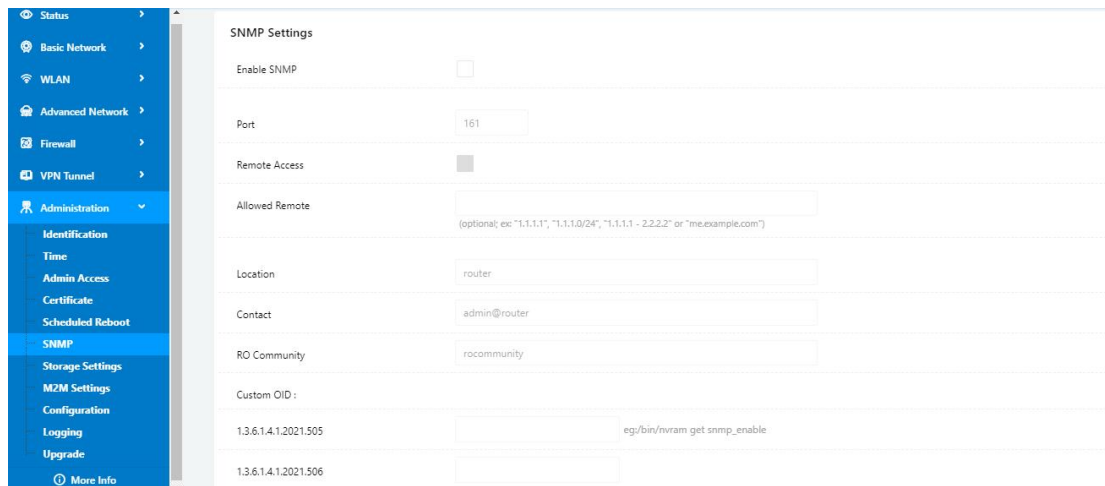


Step 2 Please click save icon to finish the setting

----End

2.12.5 SNMP Setting

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

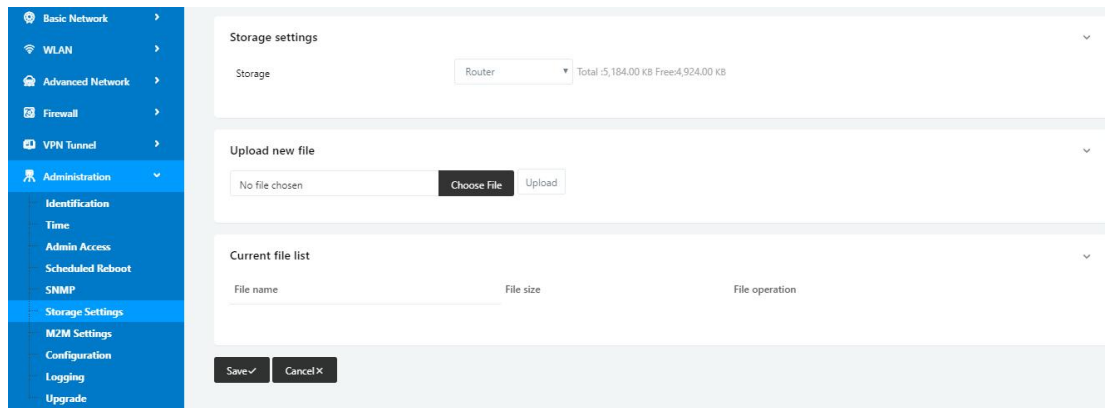


Step 2 Please click save iron to finish the setting

----End

2.12.6 Storage Setting

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



Step 2 Please click save iron to finish the setting

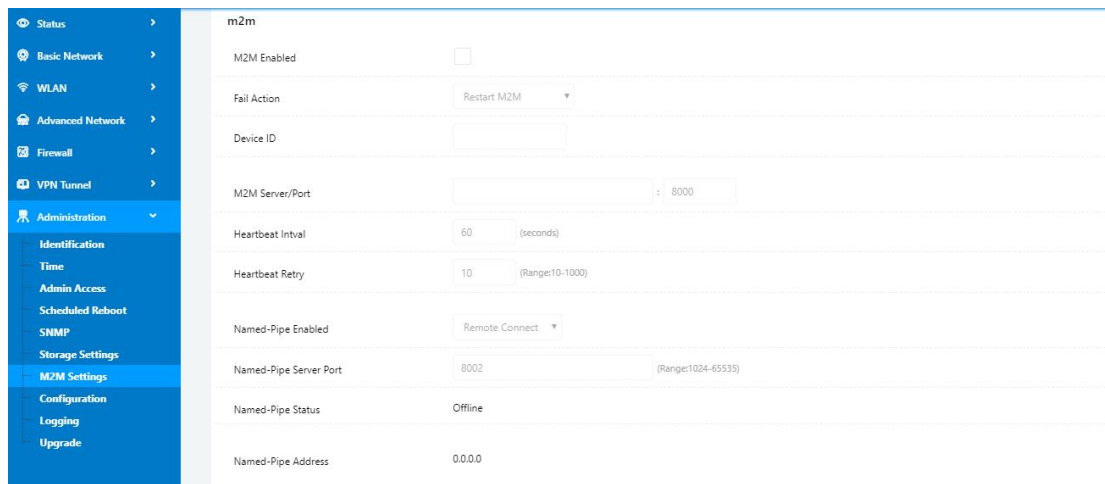


NOTE WL-G520 series router supports extra storage. The default storage path is Router

----End

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

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



Step 2 Please click save iron to finish the setting

----End

2.12.8 Configuration Setting

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

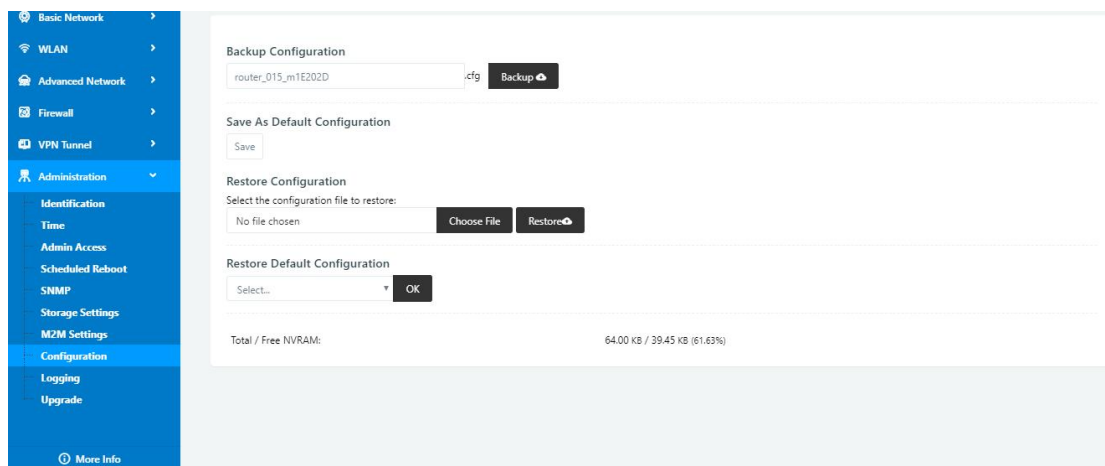


Figure 3-1 Backup and Restore Configuration GUI



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

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

----End

2.12.9 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).

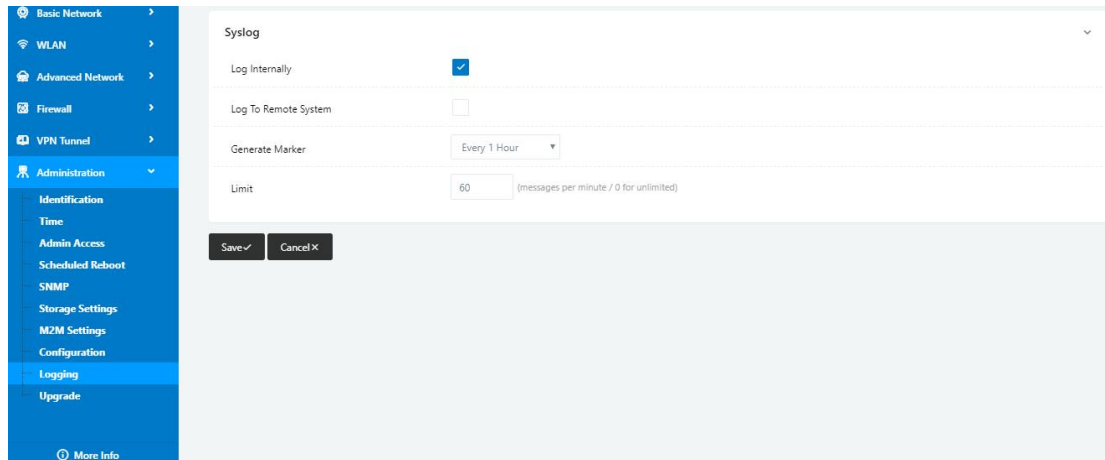


Figure 3-2 System log Setting GUI

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

----End

2.12.10 Firmware upgrade

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

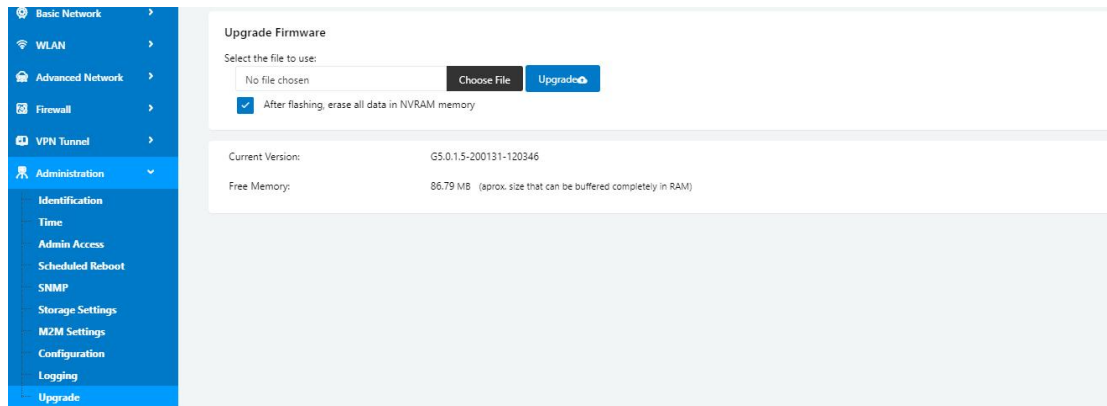


Figure 3-3 Firmware Upgrade GUI



NOTE

Please don't cut off the power during upgrade. The upgrade period will be taken about 4mins.

2.12.11 “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-G520 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 2-32 System Default Instruction

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



NOTE

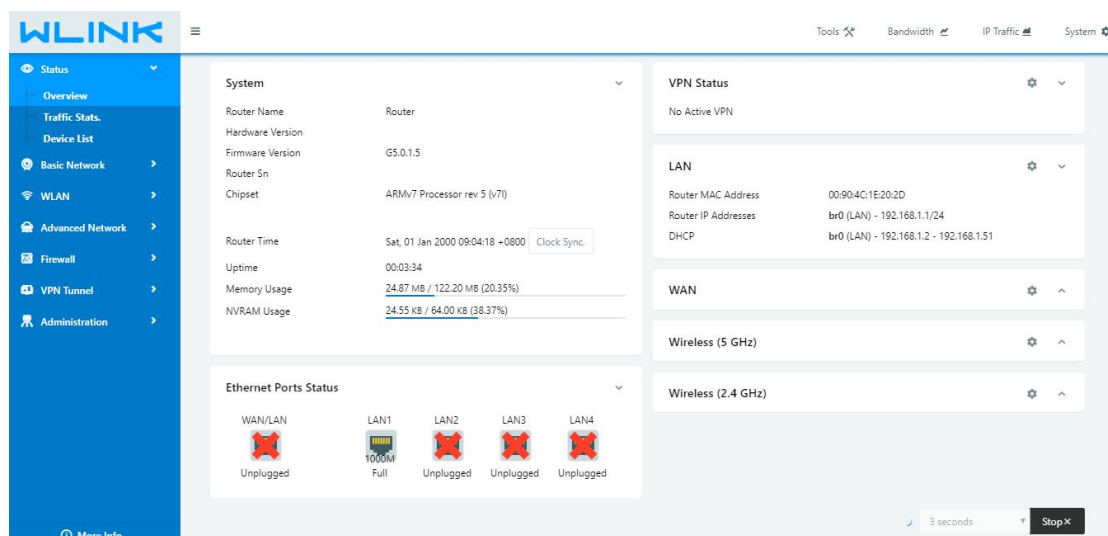
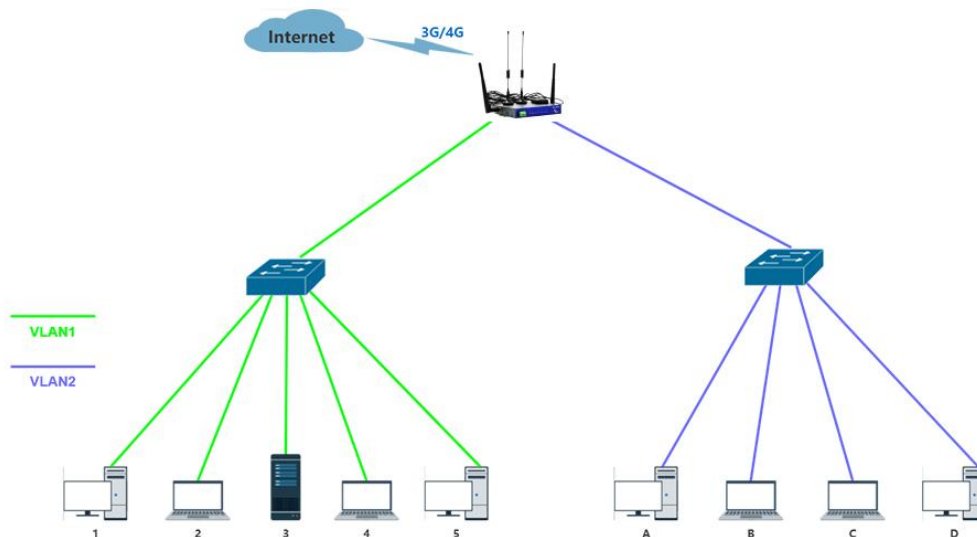
After reboot, the previous configuration would be deleted and restore to factory settings.

3 Configuration Instance

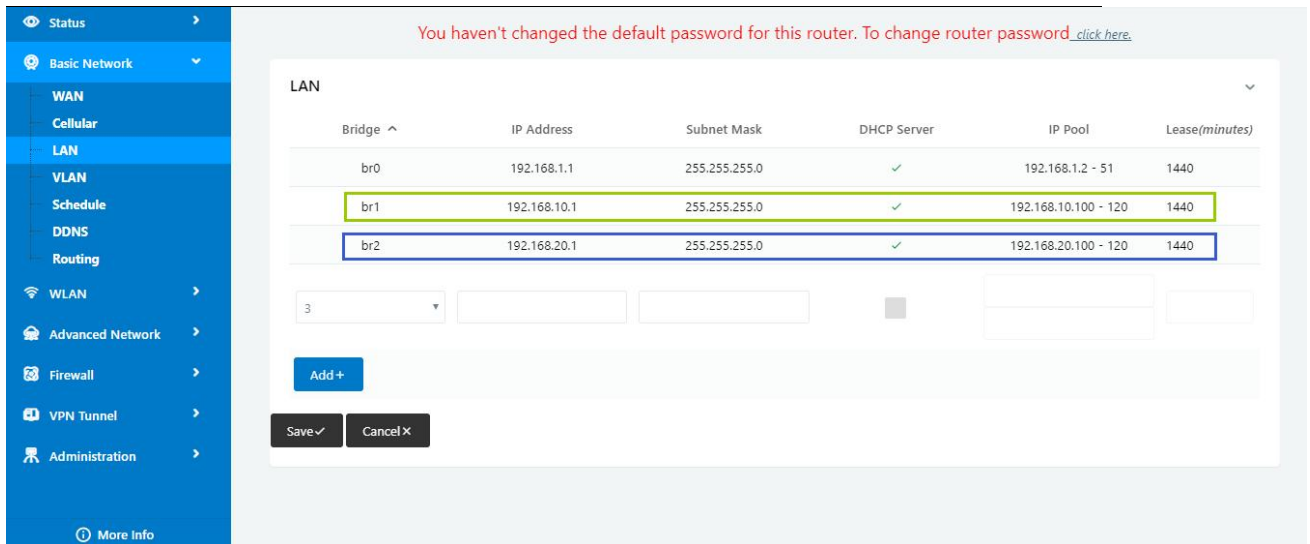
This chapter is mainly for configured test case, there would be some difference between the scheme and real object. But the difference doesn't have any influence to products performance.

3.1 VLAN

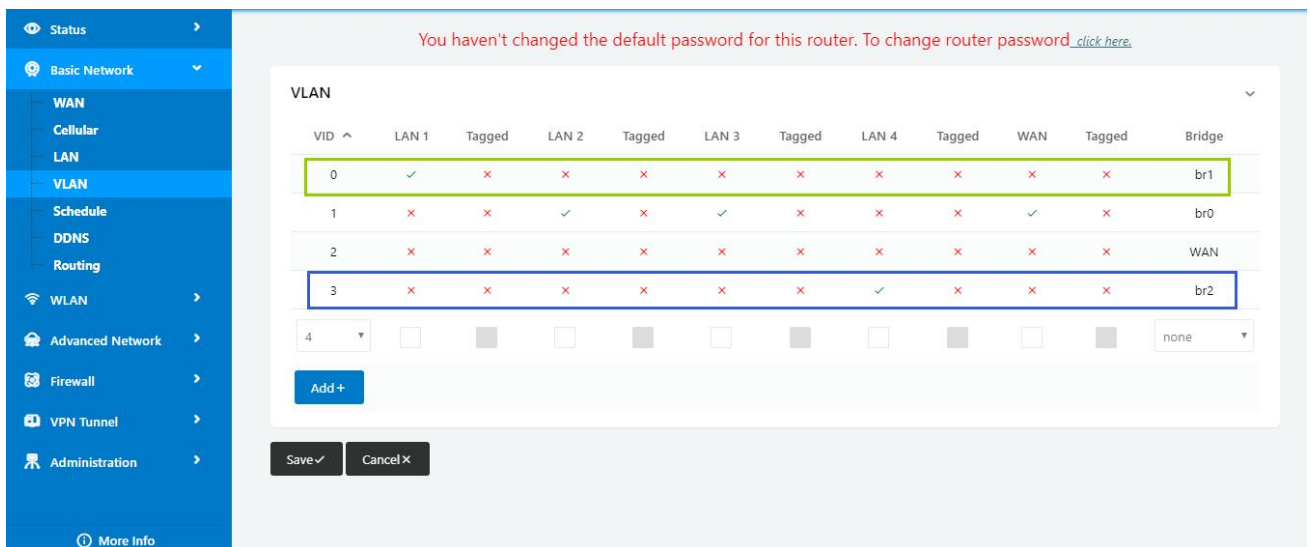
WL-G520 supports VLAN partition based on Ethernet port (LAN1~LAN5)



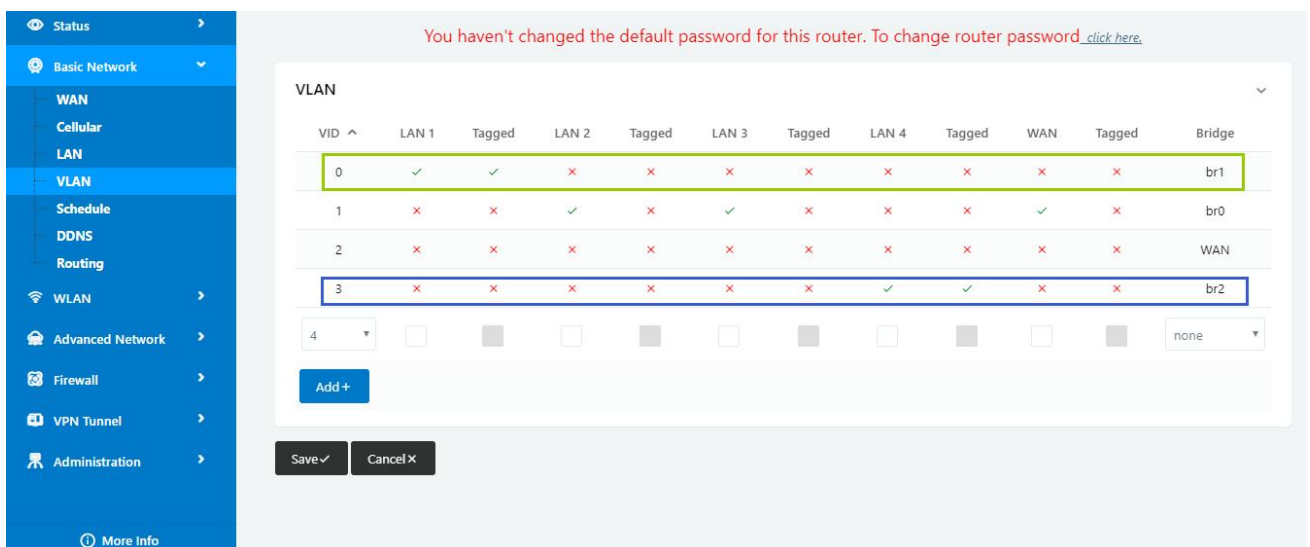
1) Configure LAN with Basic Network.



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



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

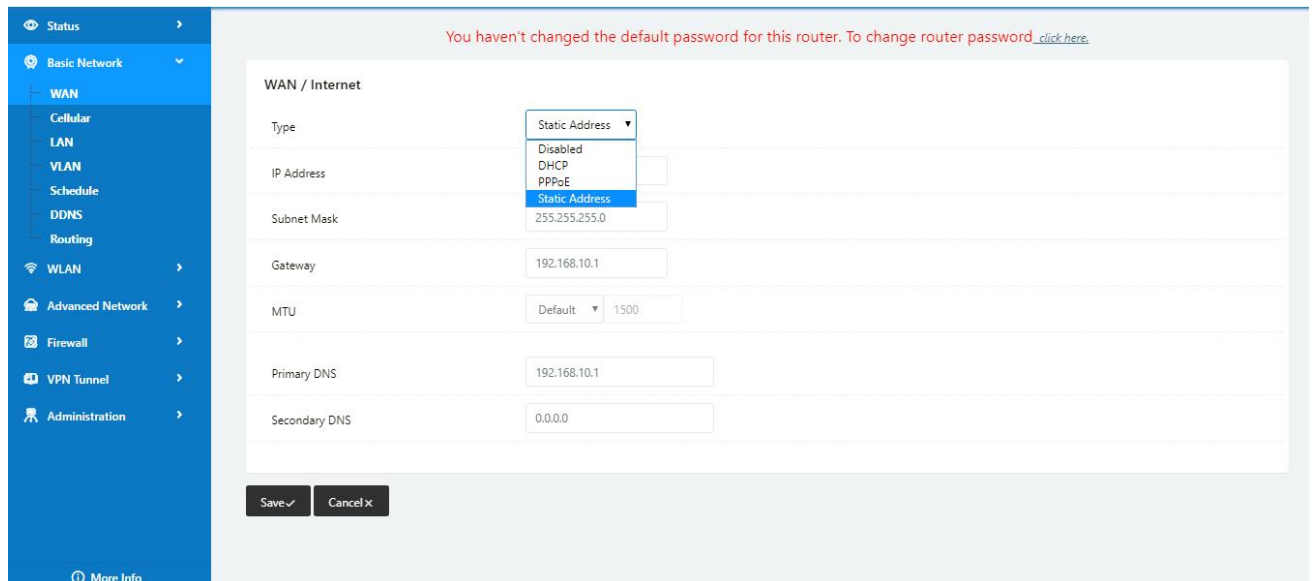


---End

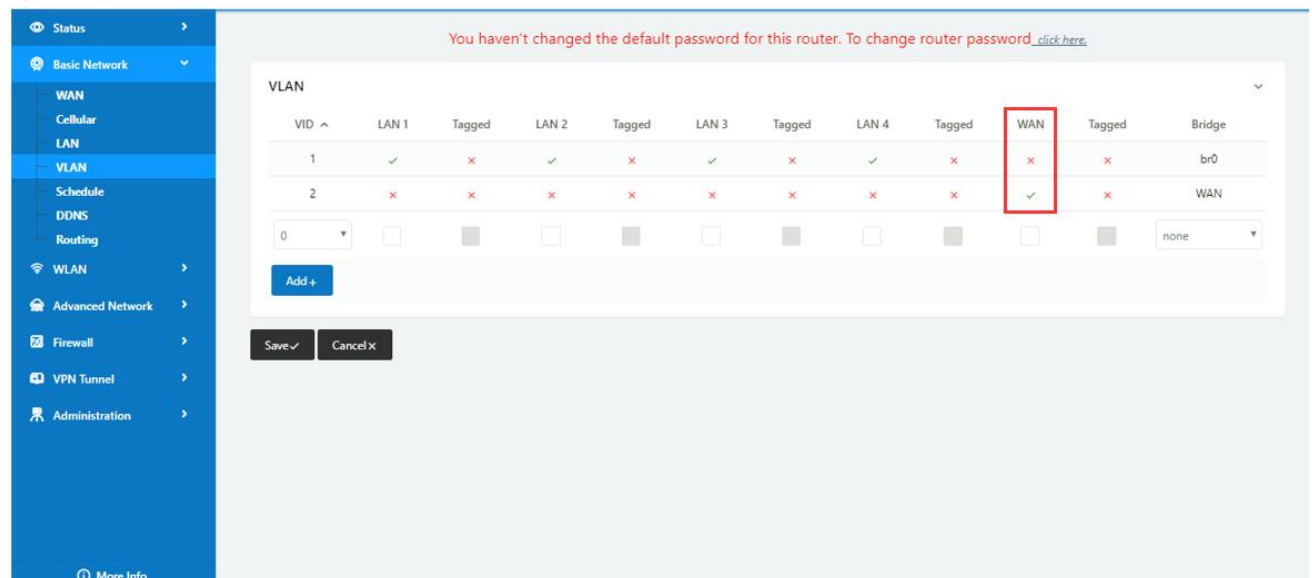
3.2 WAN Backup (WAN as Main, Cellular Backup)

The WAN and Cellular backup feature can quickly switch traffic to Cellular (link2) when WAN (link1) fails, and WL-G520 brings you a stable network experience.

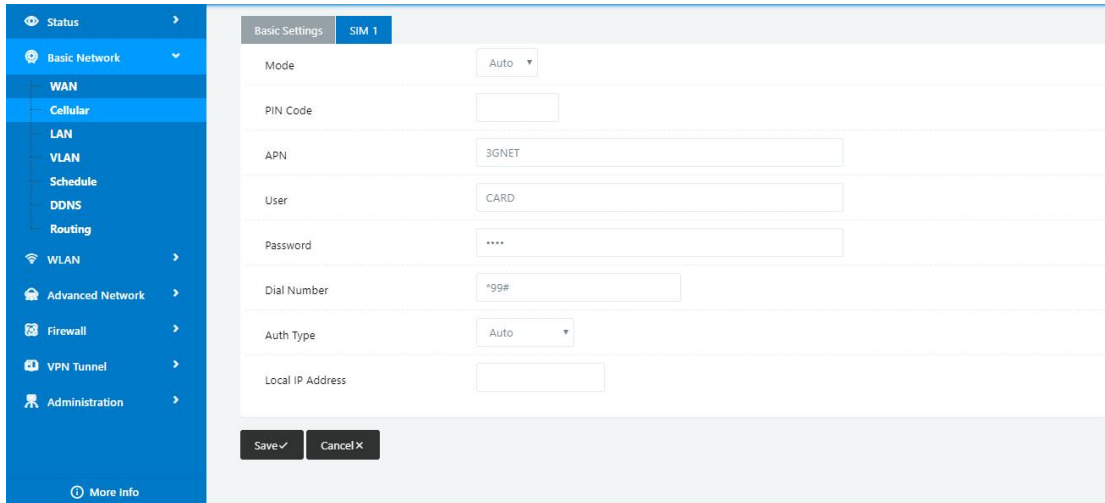
- 1) Navigate to Basic **Network** > **WAN**, you may configure the WAN parameters with your situation



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



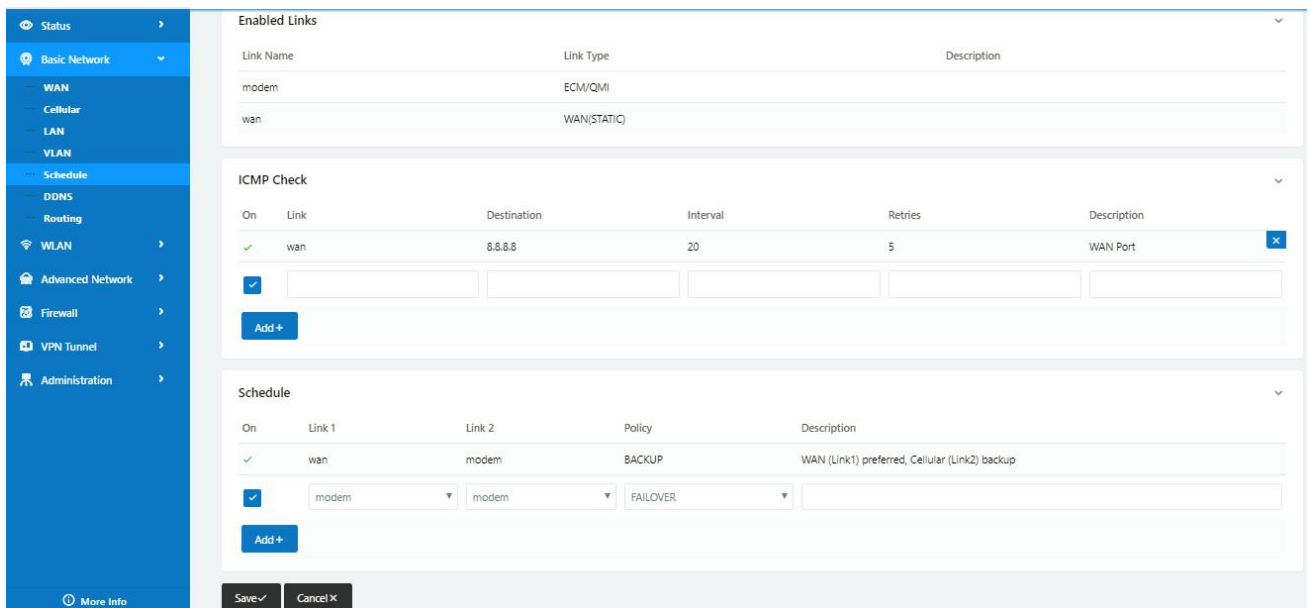
- 3) Navigate to **Basic network** > **Cellular**, configure the APN as your SIM



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

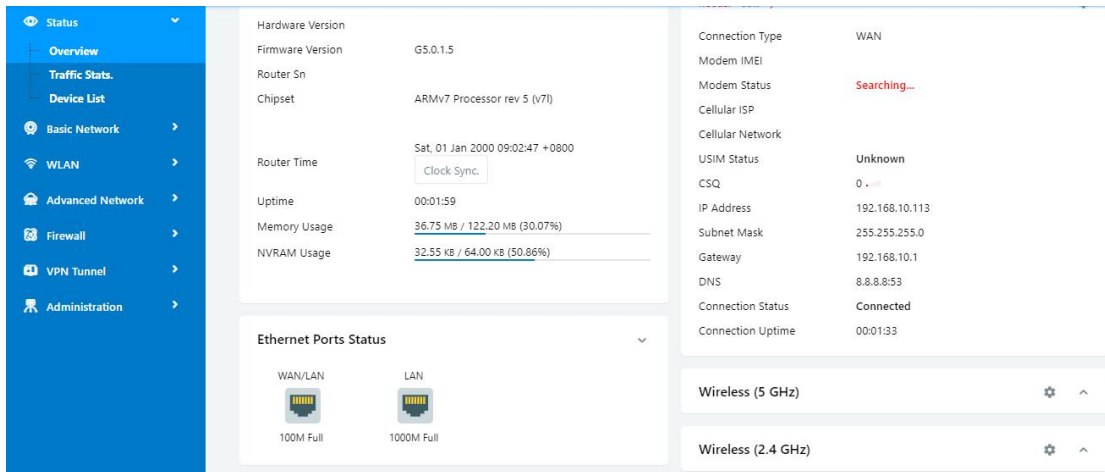
Add ICMP Check to WAN

Set the working mode (Schedule)



| 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



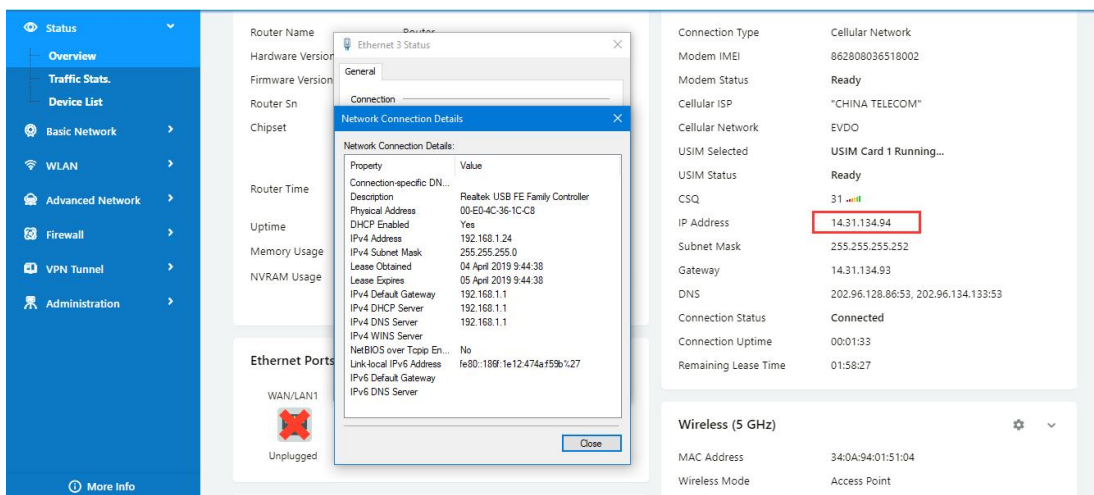
6) The system quickly switches traffic to Cellular when the WAN fails
---End

3.3 Port Forwarding

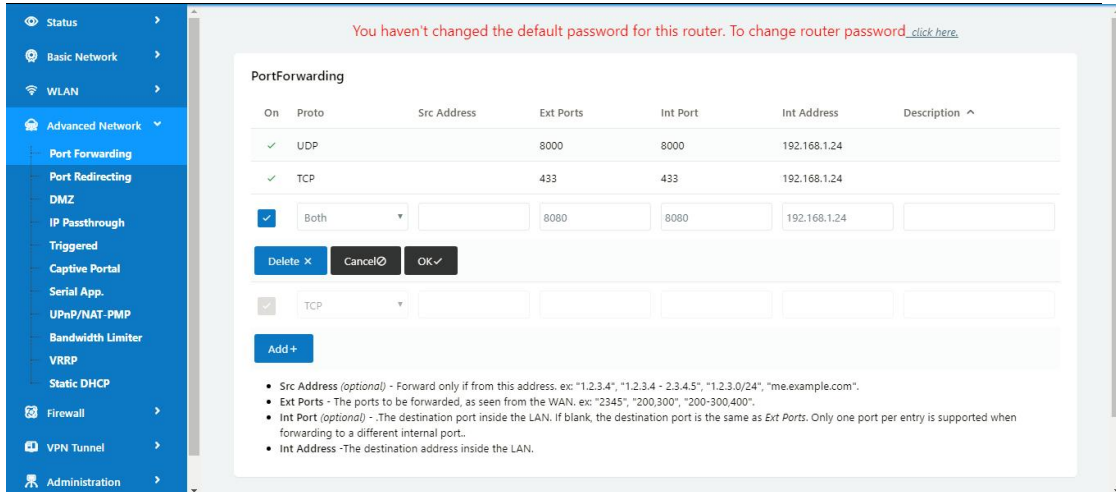
1) The router online and got a public IP address 14.31.134.94

Note: It's based on SIM card carrier

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



3) Configuration

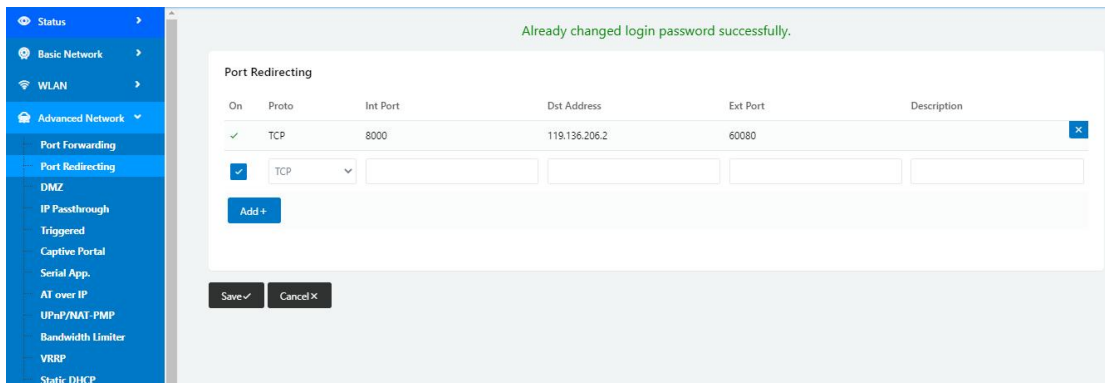


4) The PC can be accessed via 14.31.134.94:443 over Internet

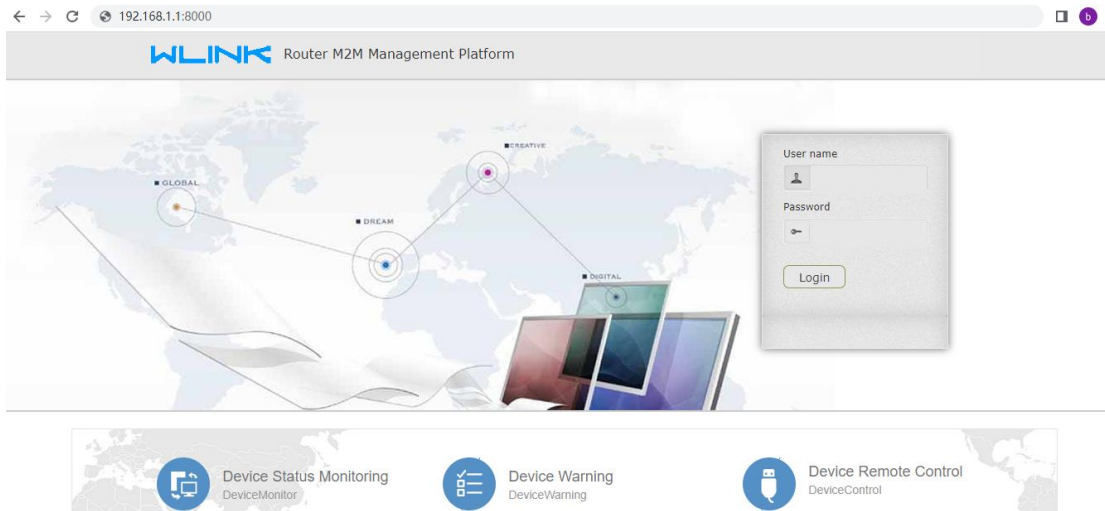
---End

3.4 Port Redirecting

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



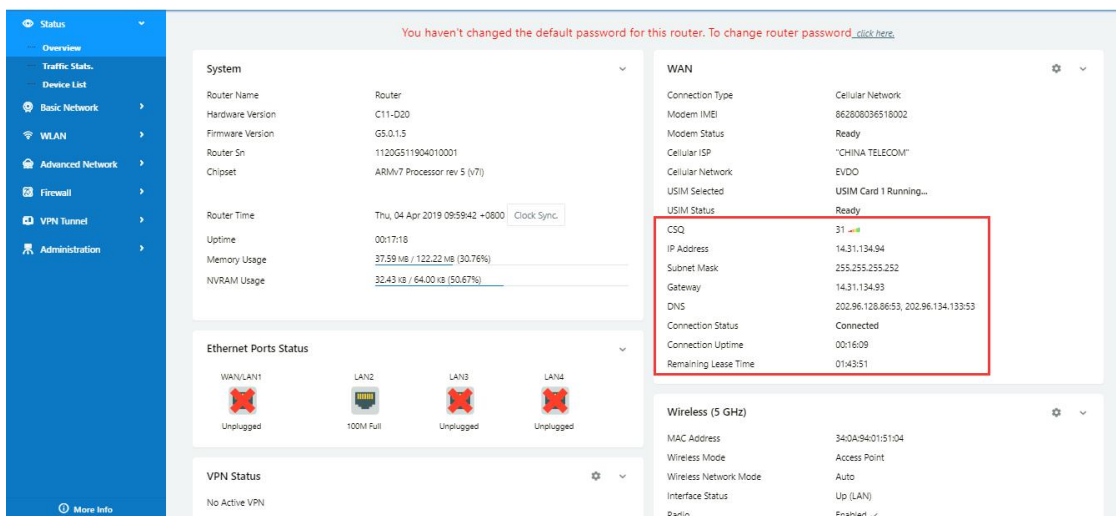
Configure Internal port as 8000, the Destination IP address as 119.136.206.2 and External port 60080(M2M Platform Server IP and Port as example). Access to 192.168.1.1:8000 in browser, the router will redirect to 119.136.206.2: 60080.



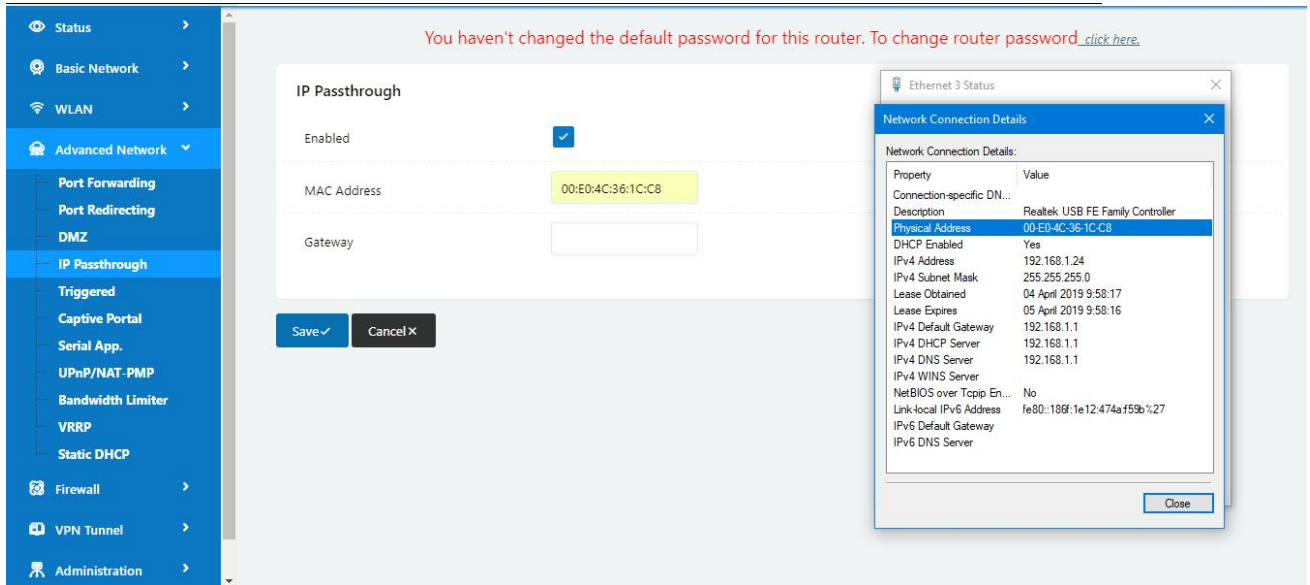
---End

3.5 IP Passthrough

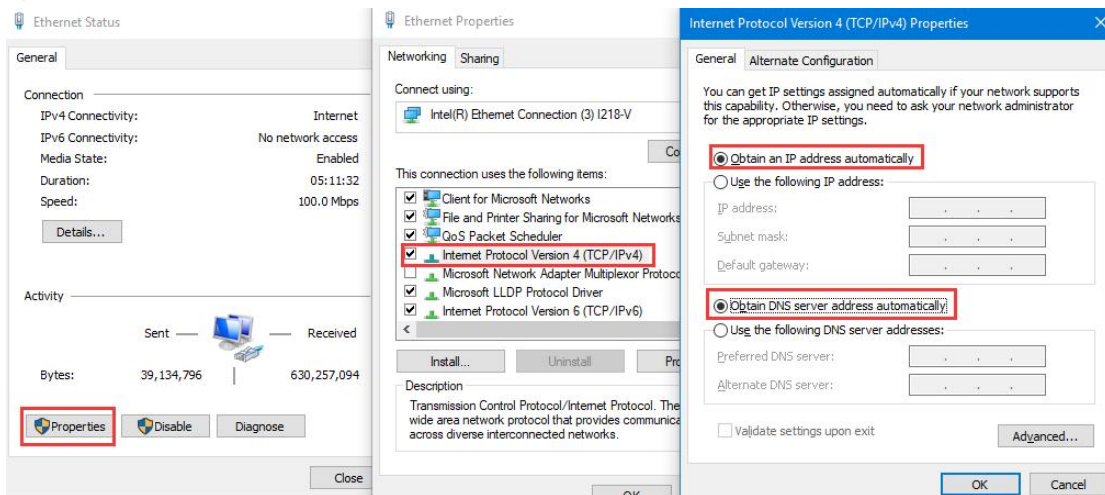
1) The router online



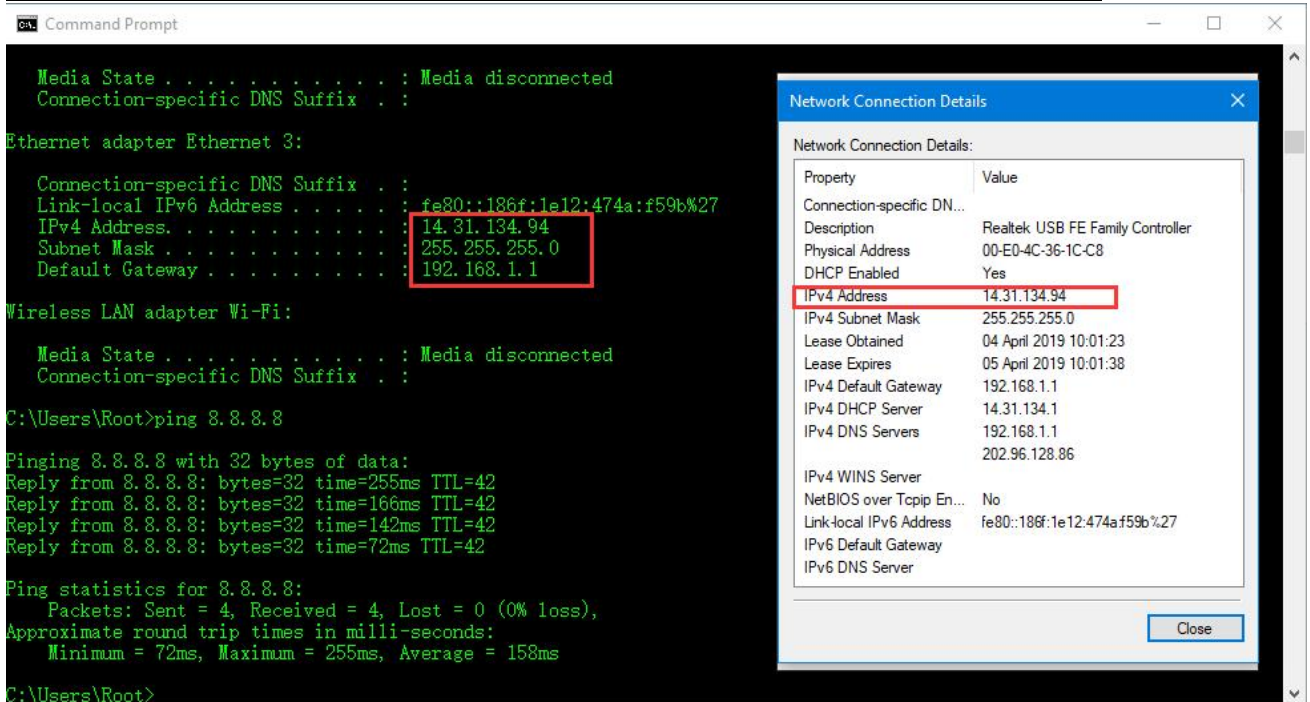
2) Configure IP passthrough destination MAC address (PC Ethernet MAC)



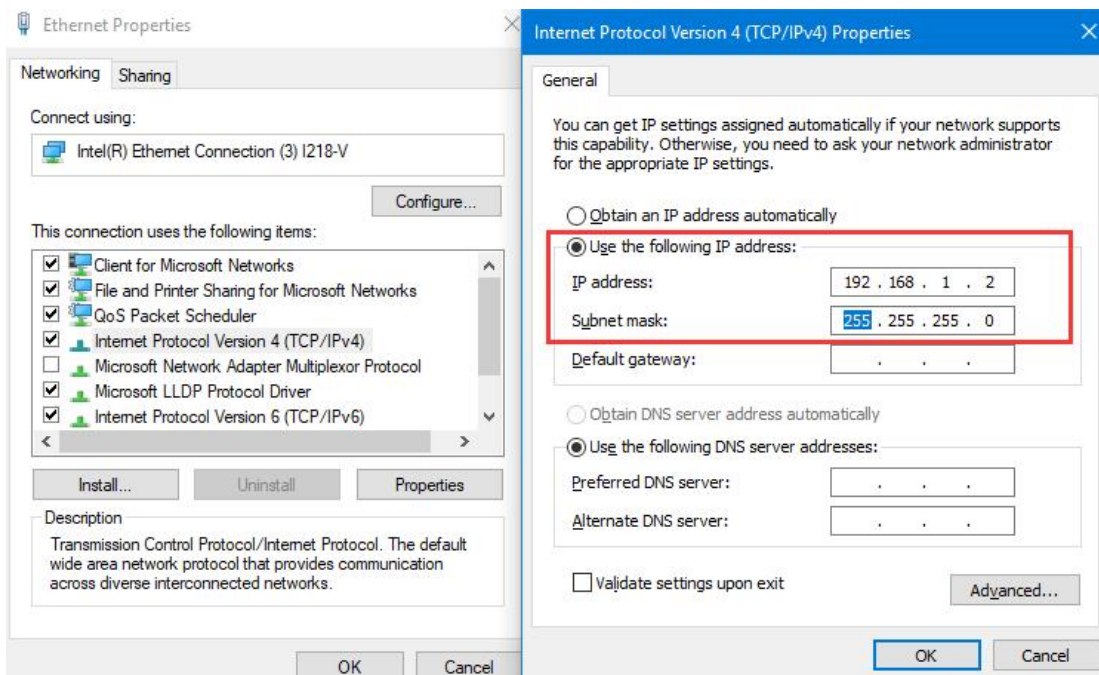
3) Set the PC to DHCP



4) Check the Ethernet status and ping test



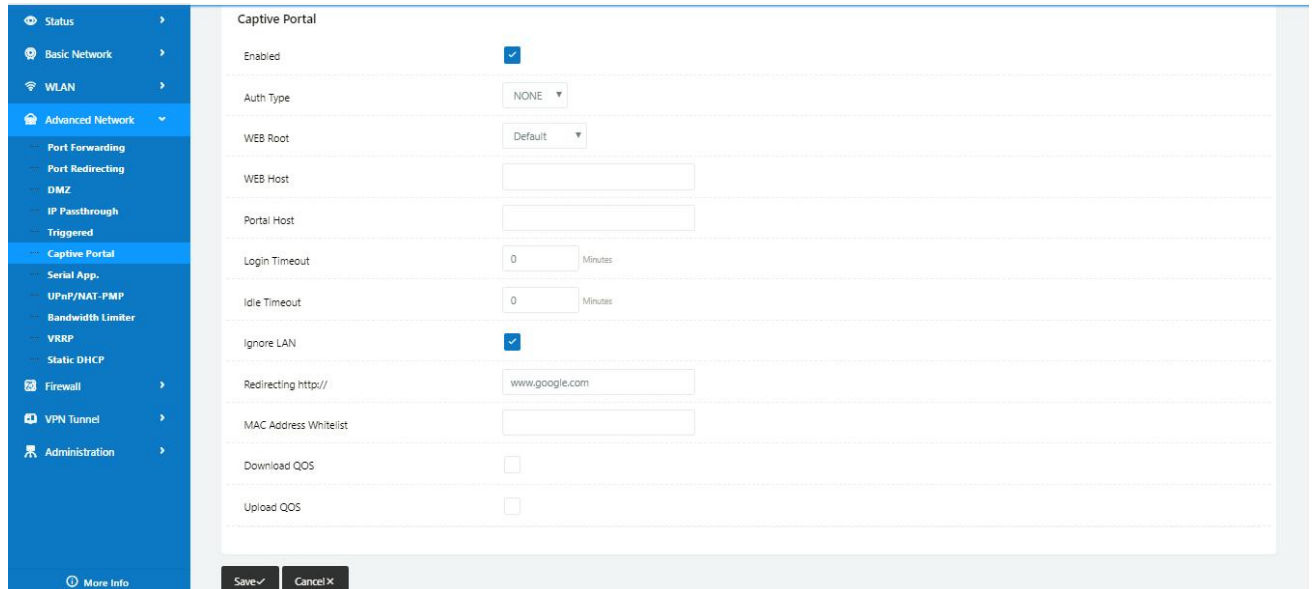
5) Set the PC Ethernet as DHCP to release the IP and access to router GUI again



---End

3.6 Captive Portal

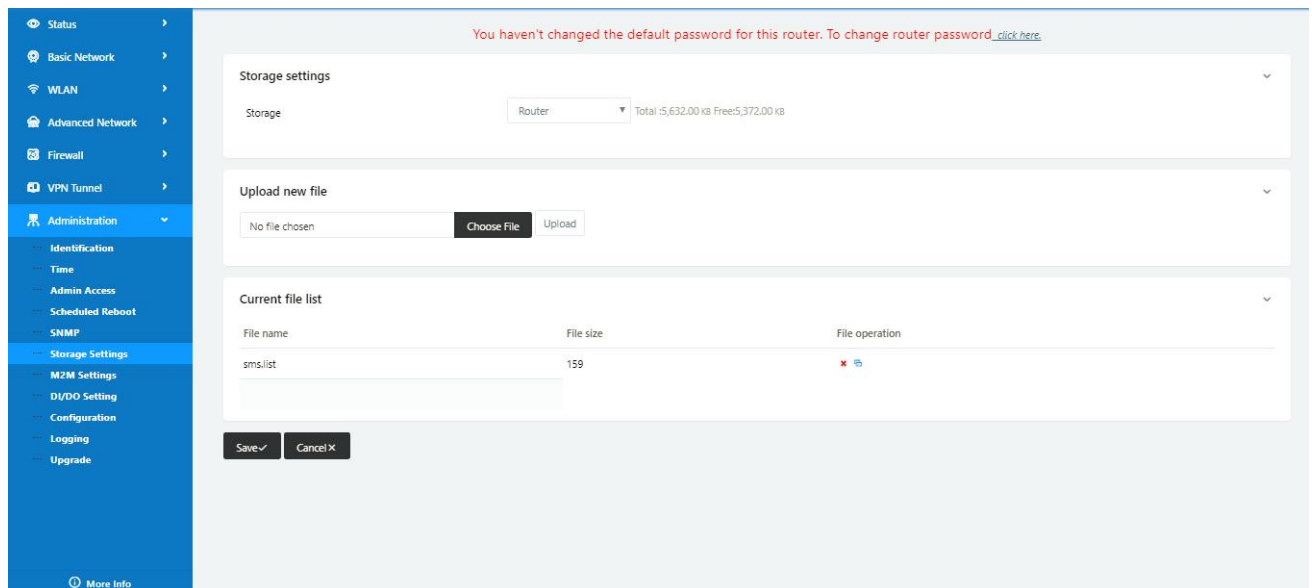
Please click “Advanced Network> Captive Portal” to check or modify the relevant parameter.



1) Upload Portal file and Splash.html by local

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

Furthermore, also might upload splash with images together.



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

| File name | File size | File operation |
|----------------------|-----------|-------------------------------------|
| 0001_portal.png | 23.8K | ✖ 📄 |
| 0002_portal.png | 45.3K | ✖ 📄 |
| 0003_portal.png | 46.0K | ✖ 📄 |
| bootstrap_portal.css | 124.3K | ✖ 📄 |
| jquery_portal.js | 289.7K | ✖ 📄 |
| splash.html | 3.4K | ✖ 📄 |

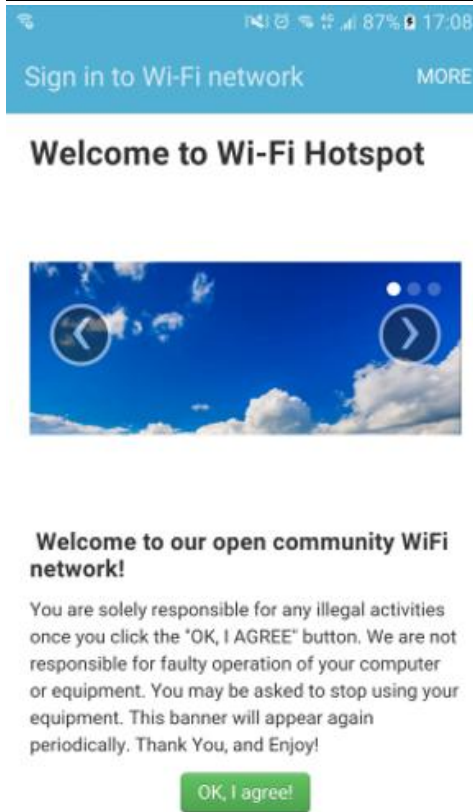
```

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

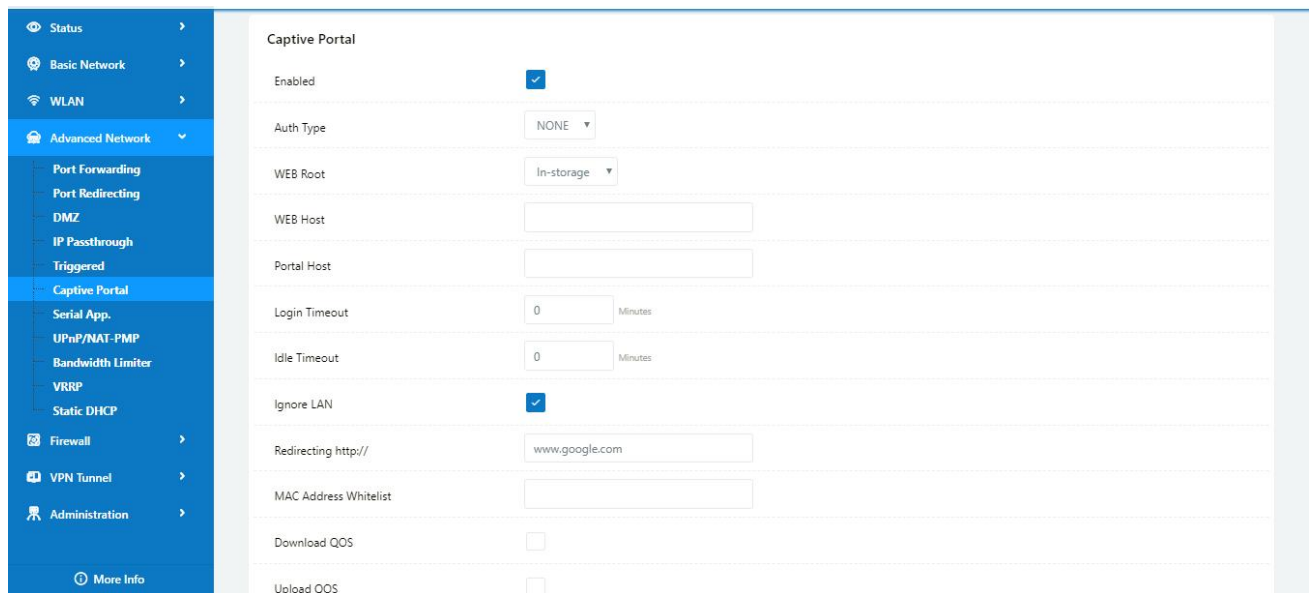
  <div class="carousel-inner">
    <div class="item active">
      
    </div>
    <div class="item">
      
    </div>
    <div class="item">
      
    </div>
  </div>
  <a class="left carousel-control" href="#myCarousel" data-slide="prev">&lsaquo;</a>
  <a class="right carousel-control" href="#myCarousel"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

```

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



- 2) Modify portal file storage path
Modify portal file storage for In-storage as below.



---End

3.7 GPS Settings

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

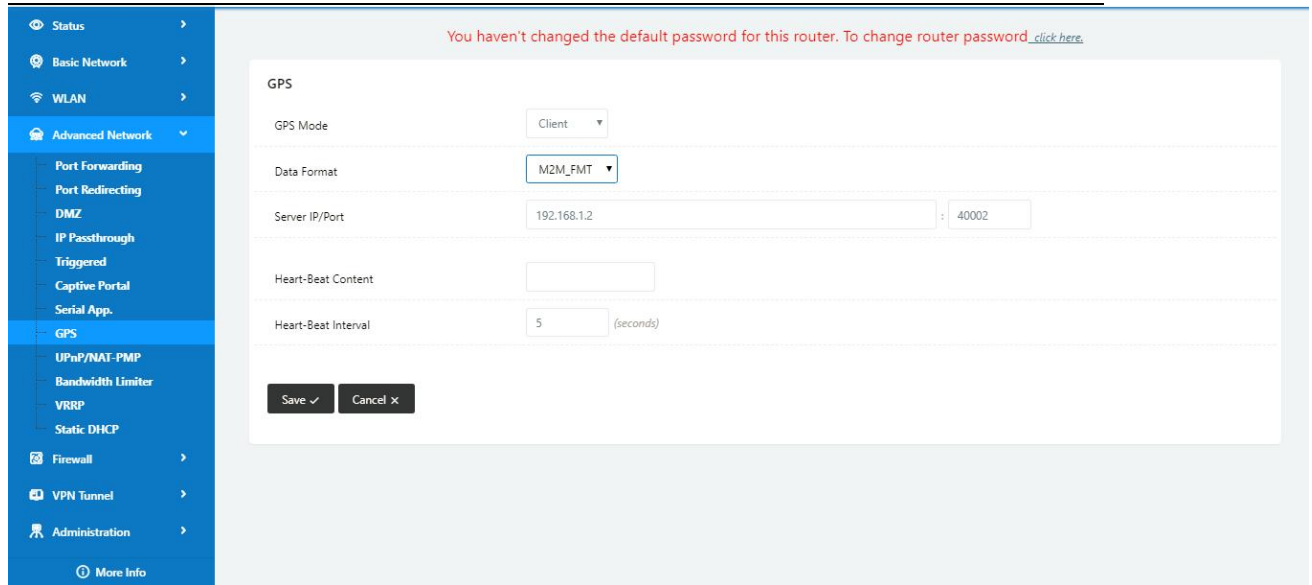


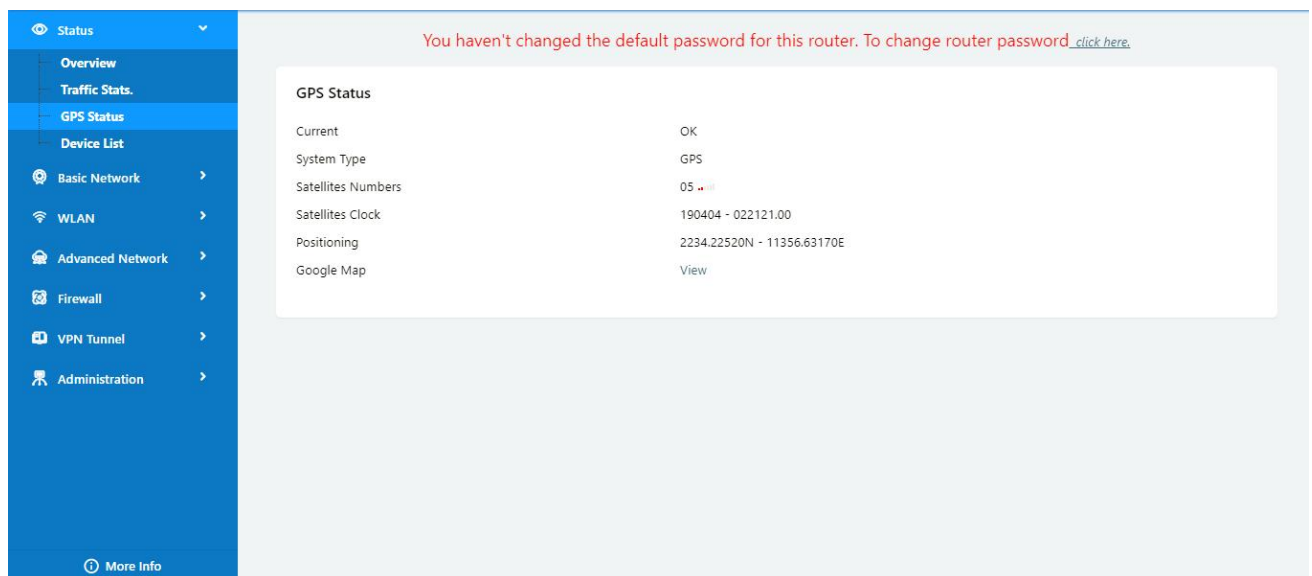
Table 4-6 “GPS” Instruction

| 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





M2M_FMT Format as below.

1. GPS data structure.

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

2. Example

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

3. GPS data description

| Field No. | Name | Format | Example | Description |
|-----------|---------------|-----------|----------------|--|
| 1 | Router ID | String | 0001_R081850ac | 0001 customizable product ID. _R router indicator. 081850ac Last 8digits of routers MAC address. |
| 2 | gps_date | yymmdd | 150904 | Date in year,month,day |
| 3 | gps_time | hhmmss.ss | 043215.0 | UTC Time, Time of position fix. |
| 4 | gps_use | numeric | 06 | Satellites Used, Range 0 to 12. |
| 5 | gps_latitude | ddmm.mm | 2234.248130 | Latitude, Degrees + minutes. |
| 6 | gps_NS | character | N | N/S Indicator,N=north or S=south. |
| 7 | gps_longitude | ddmm.mm | 11356.626179 | Longitude, Degrees + minutes. |
| 8 | gps_EW | character | E | E/W indicator, E=east or W=west. |
| 9 | gps_speed | numeric | 0.0 | Speed over ground, units is km/h. |
| 10 | gps_degrees | numeric | 91.5 | Course over ground, unit is degree. |
| 11 | gps_FS | digit | 1 | Position Fix Status Indicator, |
| 12 | gps_HDOP | numeric | 1.2 | HDOP, Horizontal Dilution of Precision |
| 13 | gps_MSL | numeric | 97.5 | MSL Altitude, units is meter. |

---End

3.8 Firewall

1) IP/MAC/Port Filtering

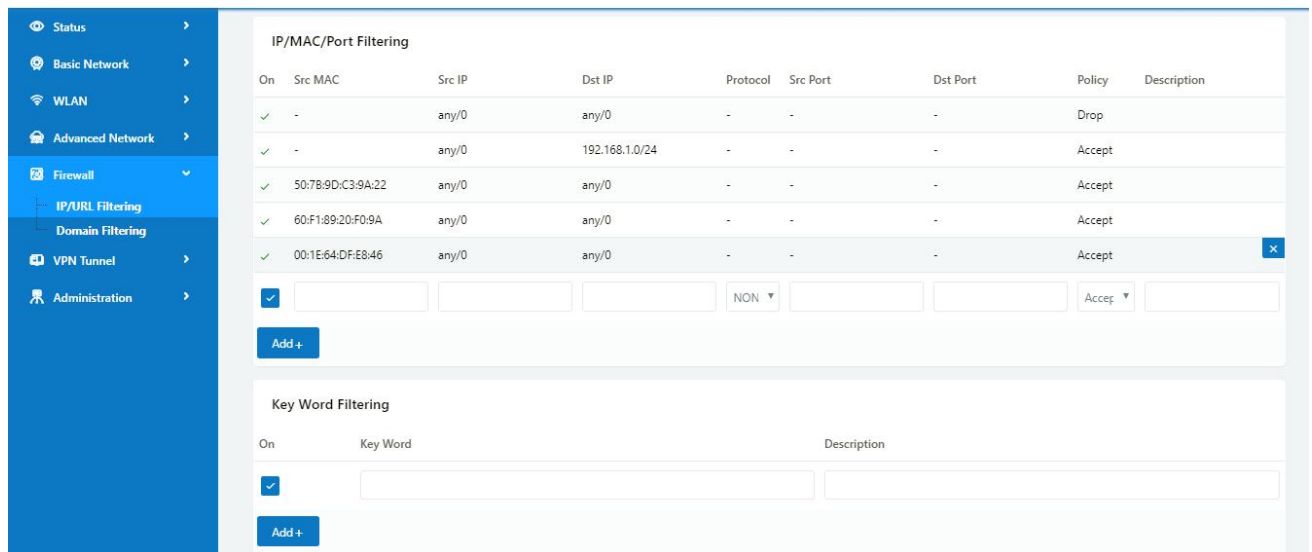
This part used to intercept packages from router's WAN/Celluar interface to Internet.

Test case:

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

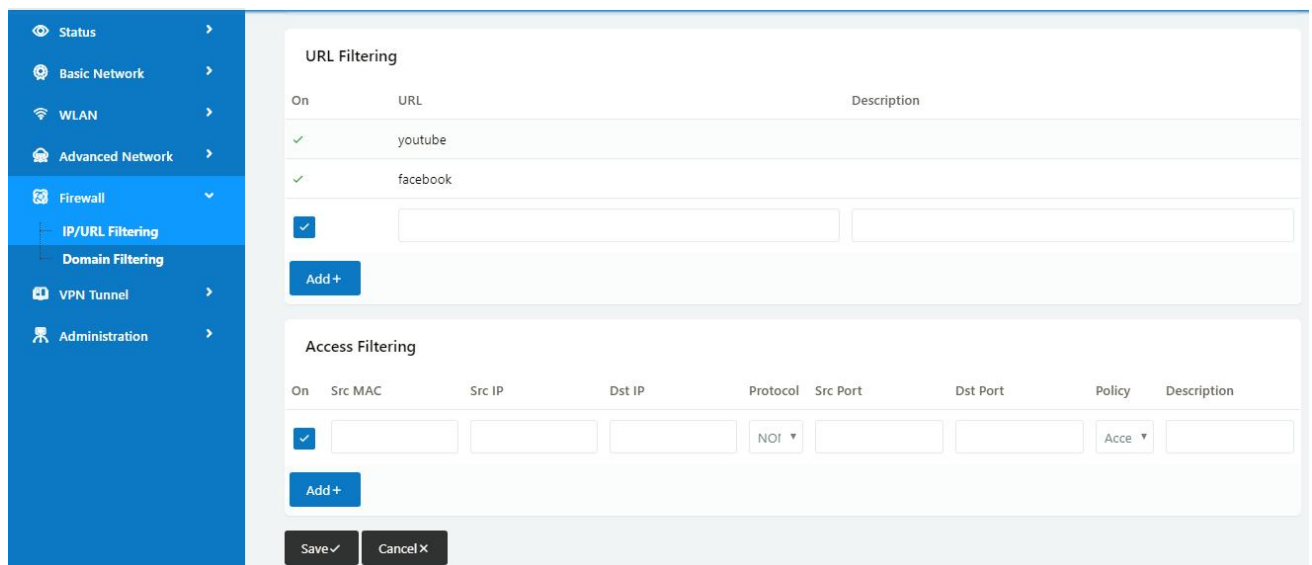
110.110.10.10

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



2) Key Word Filtering

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



3) URL Filtering

This part used to filter URL from router's WAN/Celluar interface to Internet.

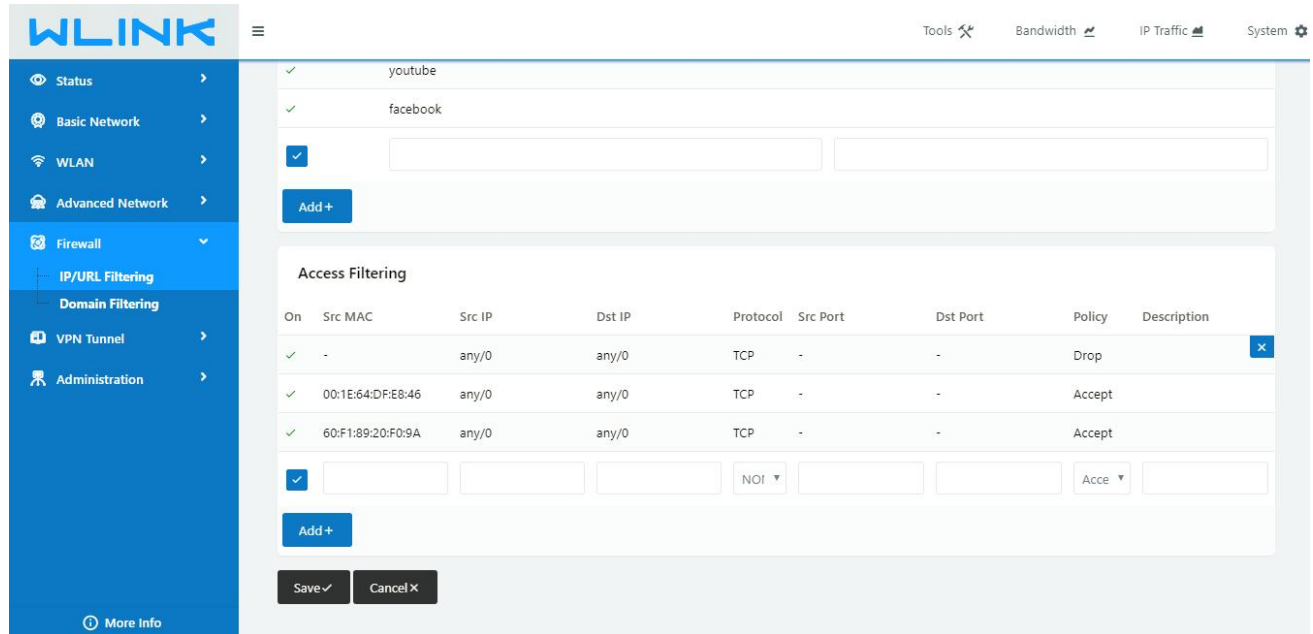
4) Access Filtering

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.

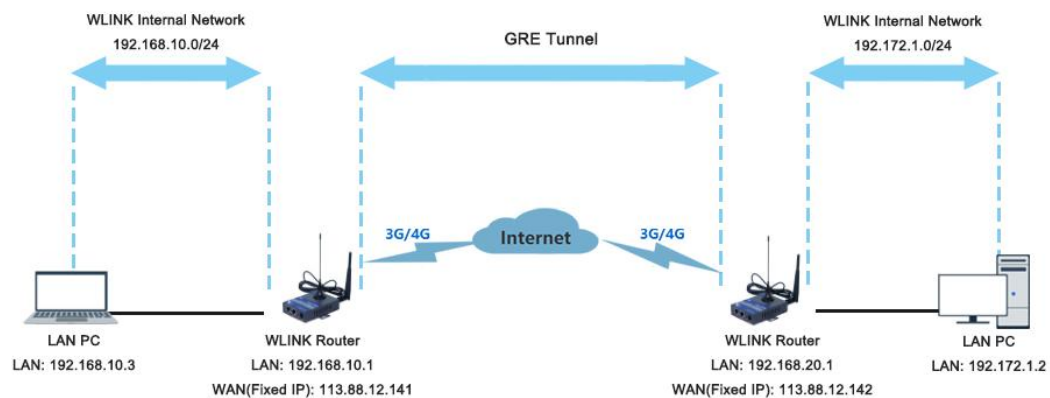


---End

3.9 VPN Tunnel

3.8.1 GRE

GRE Tunnel between WLINK Routers



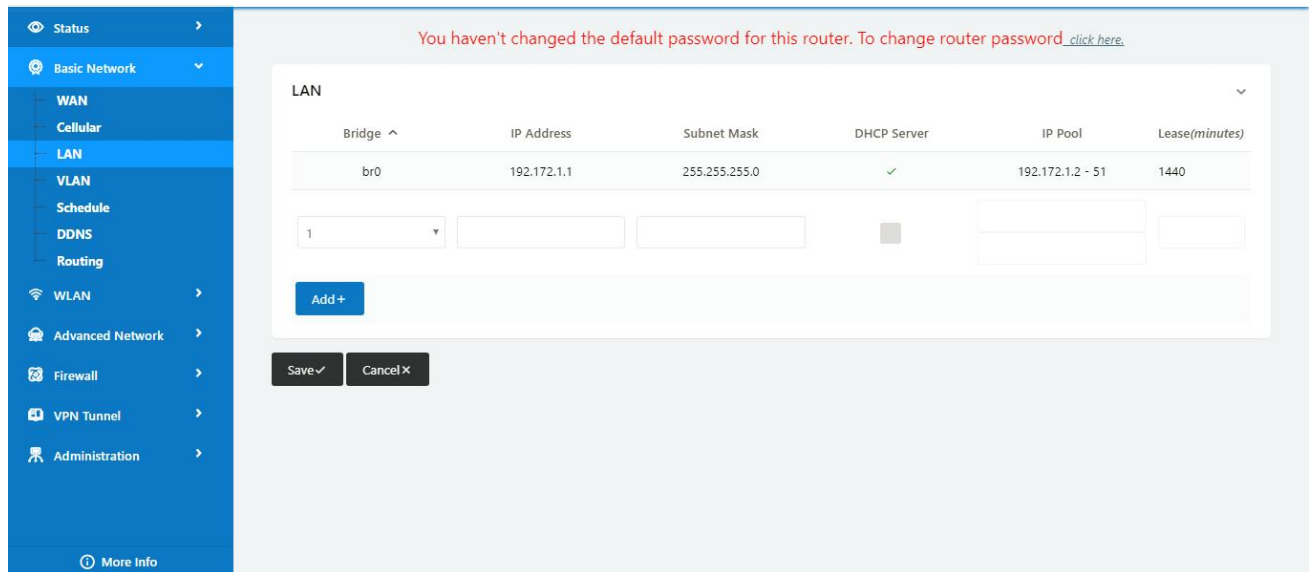
1) WL-G520(A) Config

Navigate to **Basic Network > LAN**

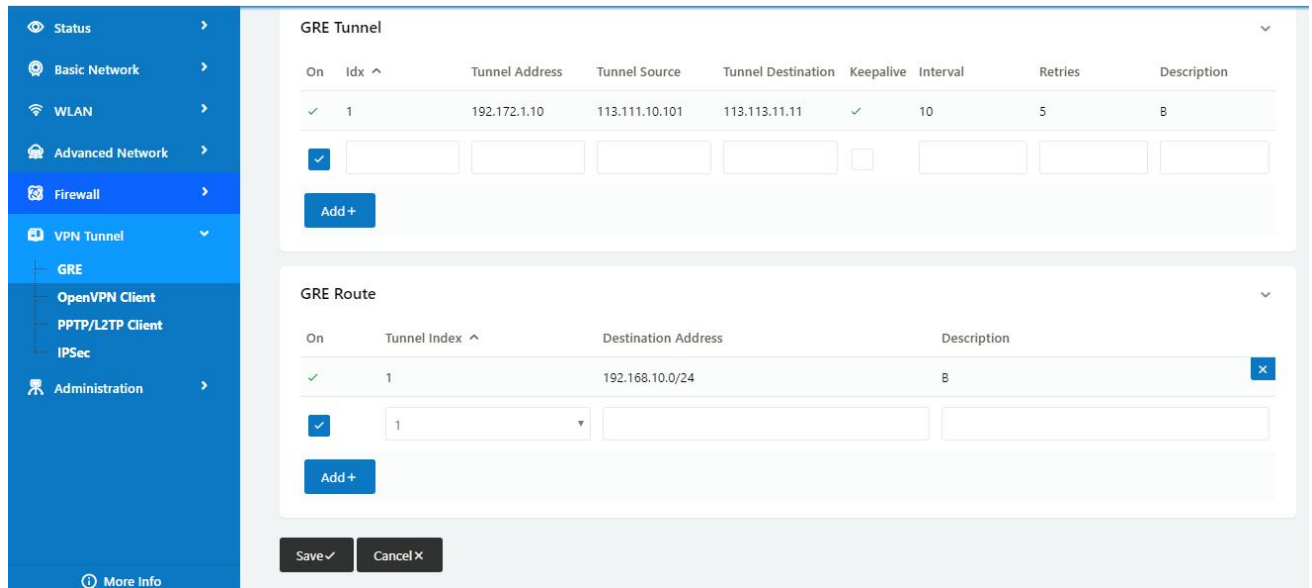
Navigate to **VPN Tunnel > GRE**

2) WL-G520(B) Config

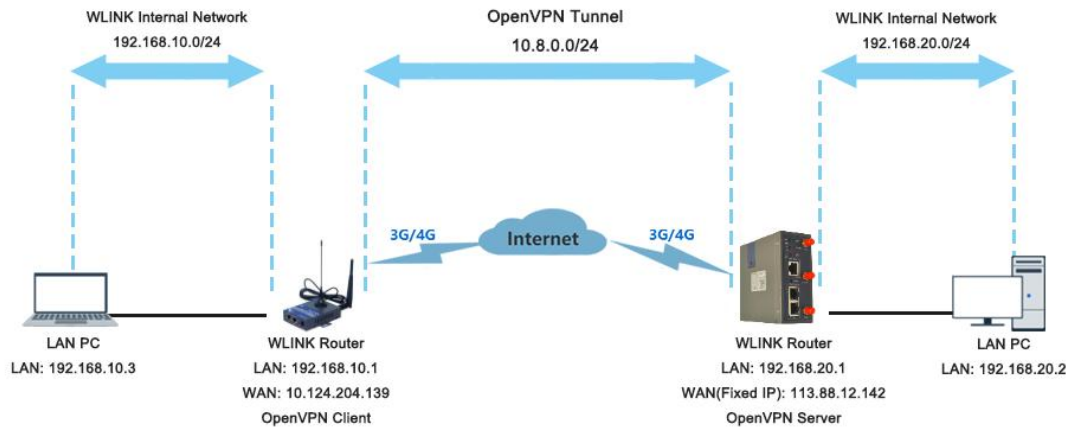
Navigate to **Basic Network > LAN**



Navigate to **VPN Tunnel > GRE**

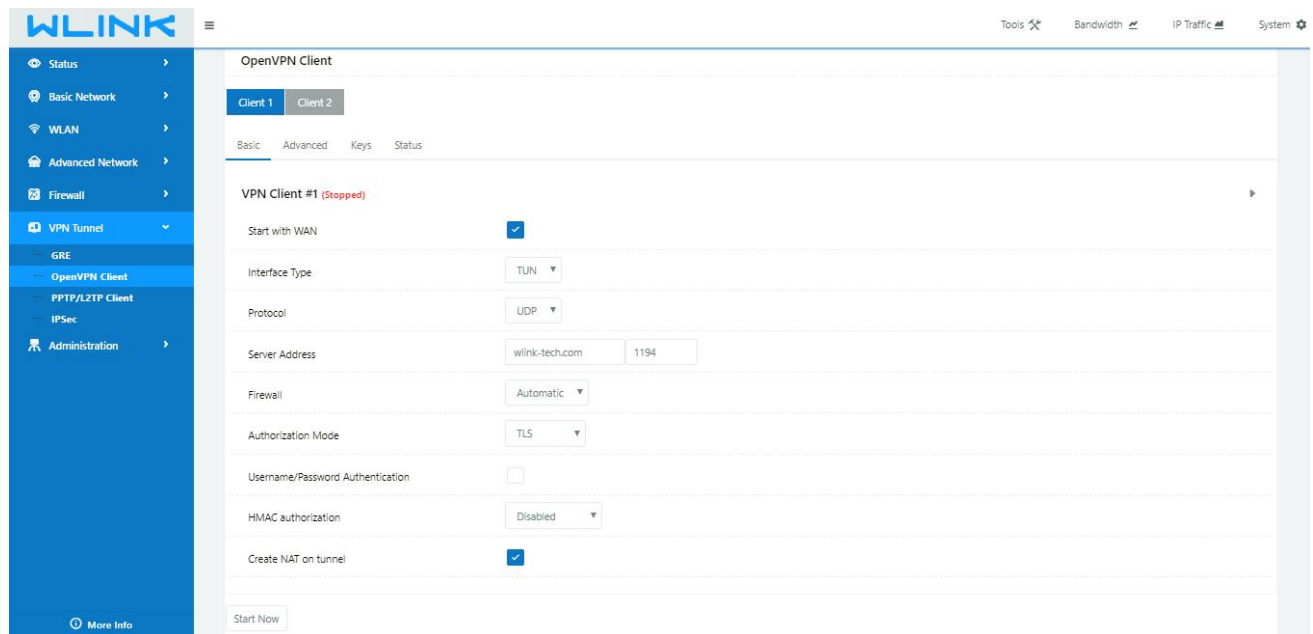


3.8.2 OpenVPN



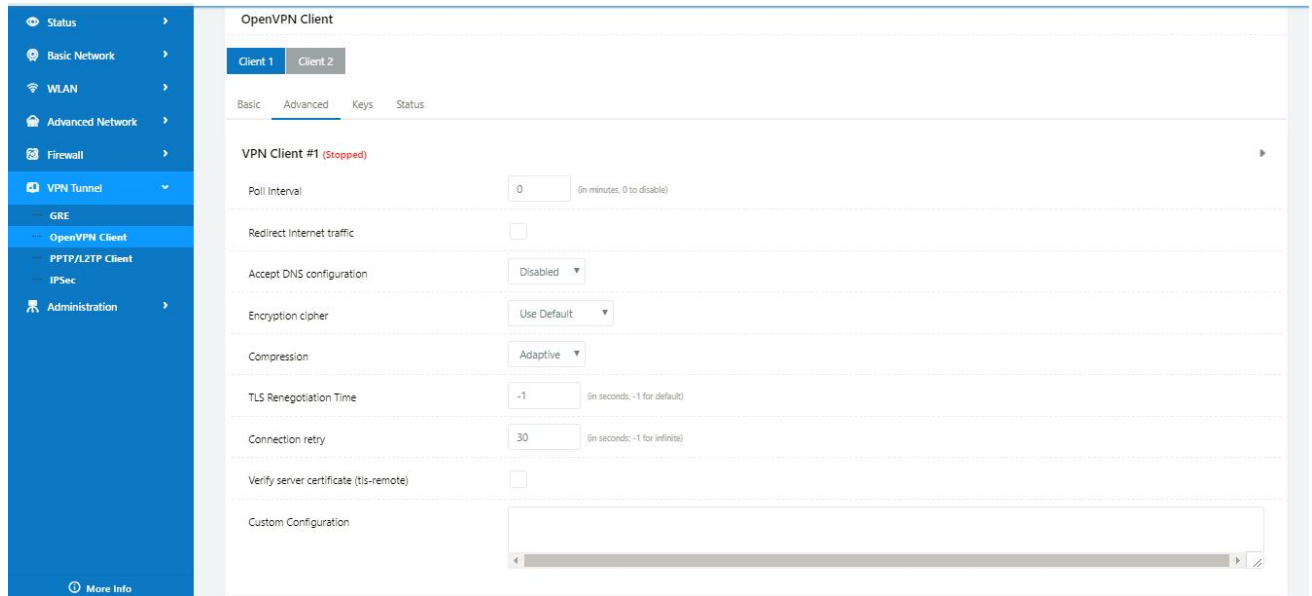
OpenVPN between WL-G520 client and Server

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

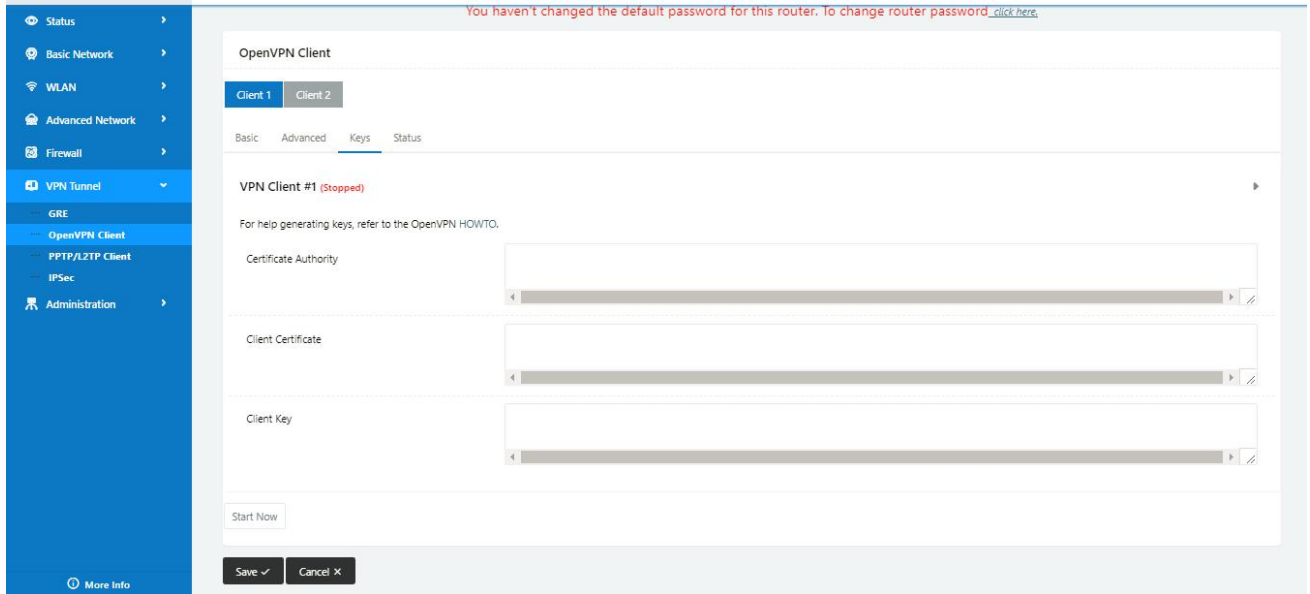


| Parameter | Instruction |
|--------------------|---|
| Start with WAN | Enable the Openvpn feature for 4G/3G/WAN port. |
| Interface Type | Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode. |
| Protocol | UDP and TCP optional. |
| Server Address | The Openvpn server public IP address and port. |
| Firewall | Auto, External only and Custom are optional |
| Authorization Mode | TLS, Static key and Custom are optional. |

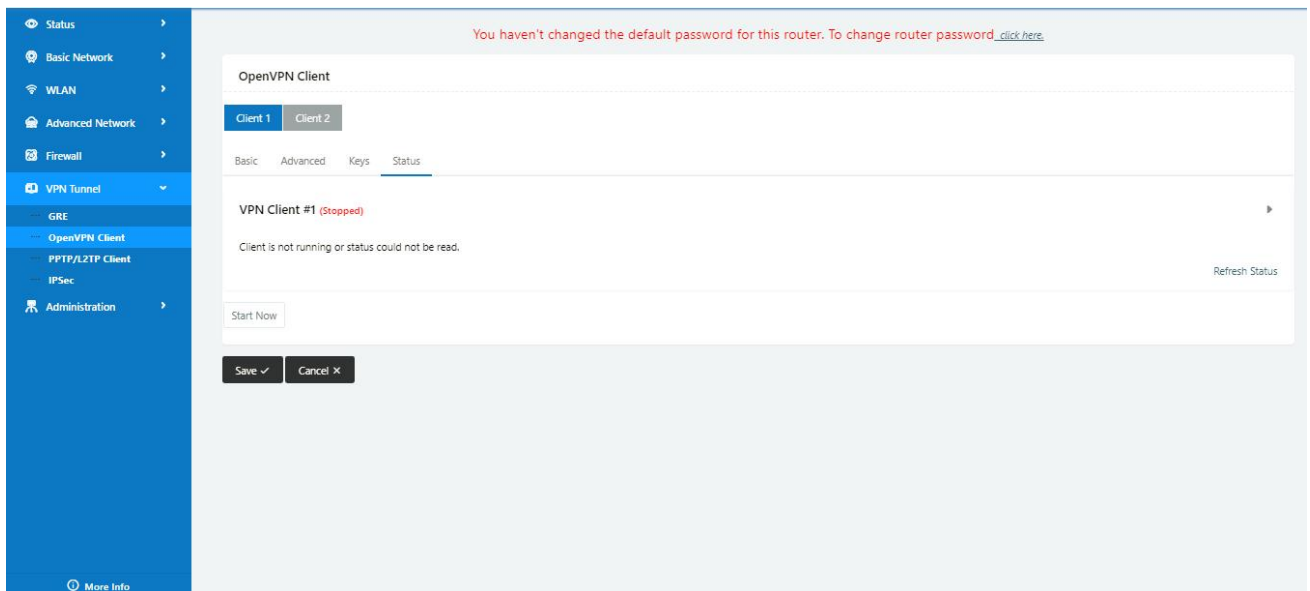
| | |
|-----------------------------------|----------------------------------|
| User name/Password Authentication | As the configuration requested. |
| HMAC authorization | As the configuration requested. |
| Create NAT on tunnel | Configure NAT in Openvpn tunnel. |



| 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. |



| 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 |



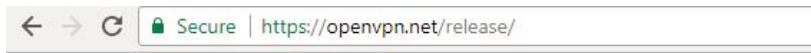
| Parameter | Instruction |
|-----------|---|
| Status | Check OpenVPN status and data statistics. |

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

 [OpenVPN Keys Guide](#)

The following 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)



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)



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 >

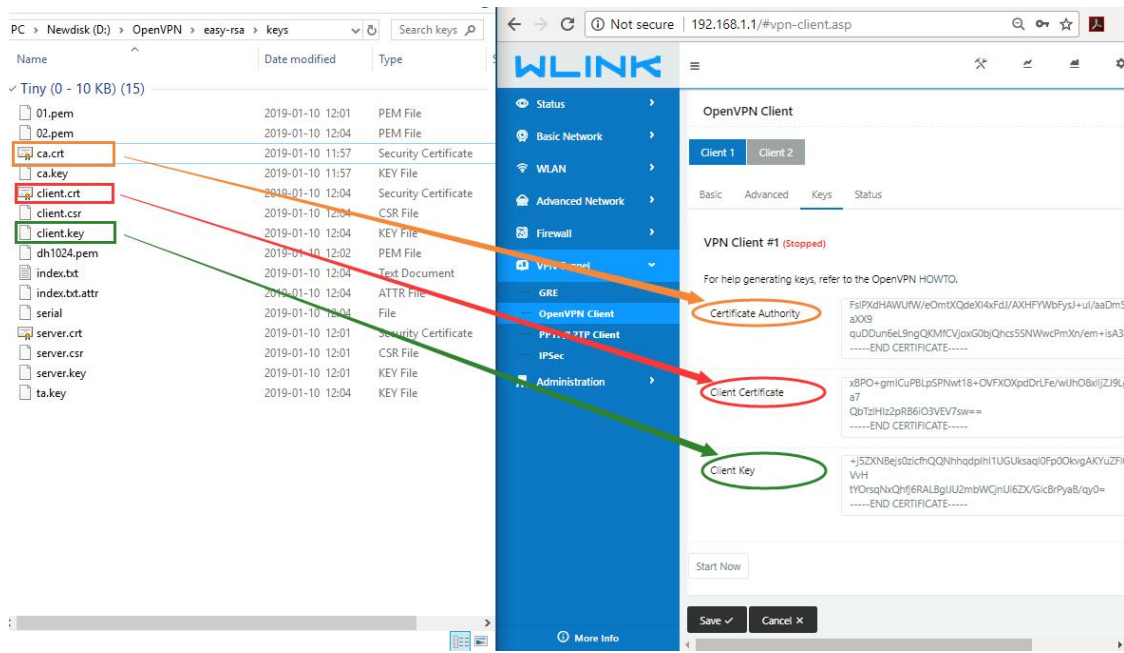
| Name | Date modified | Type | Size |
|----------------------|------------------|--------------------|------|
| keys | 2019-01-10 12:04 | File folder | |
| .rnd | 2019-01-10 12:04 | RND File | 1 KB |
| build-ca.bat | 2016-01-04 20:41 | Windows Batch File | 1 KB |
| build-dh.bat | 2016-01-04 20:41 | 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

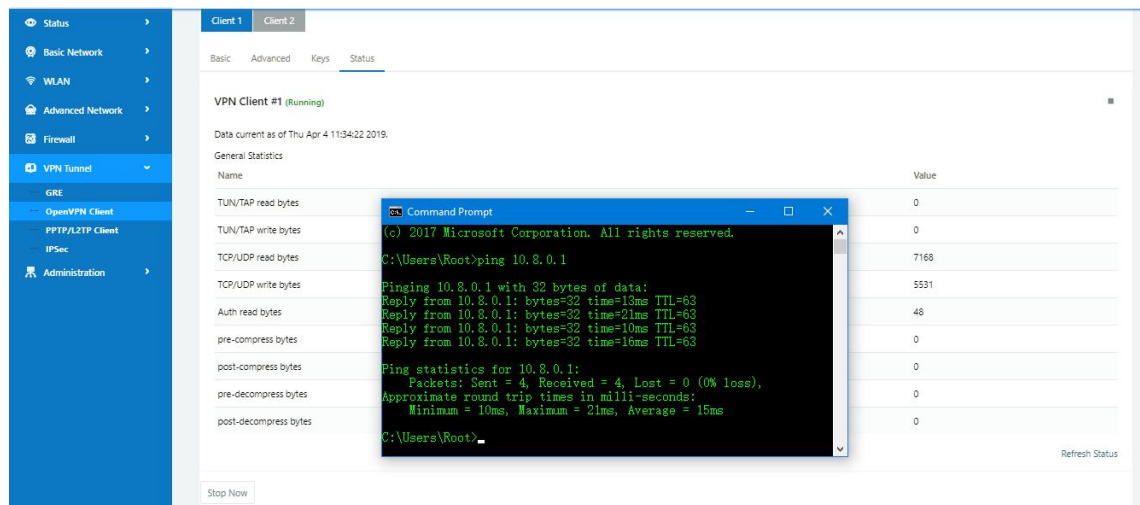
Client certificate (Generated on the server)

| 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



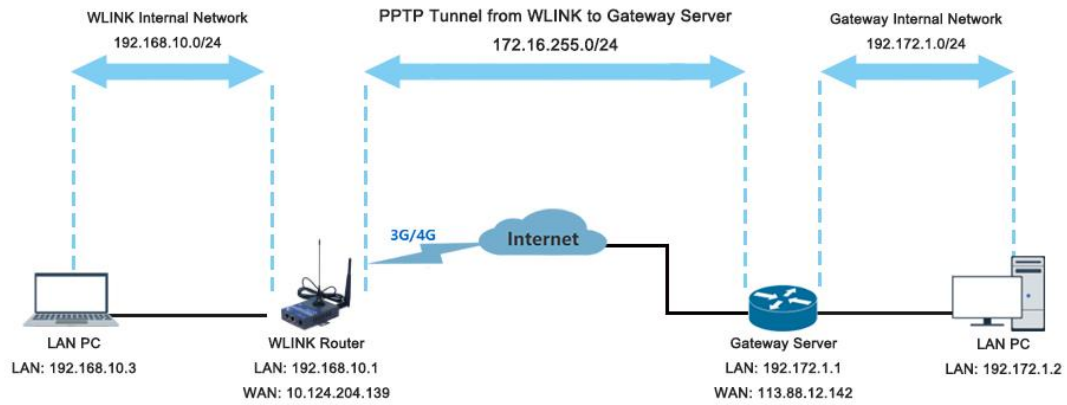
Ping test to your server when the tunnel is established



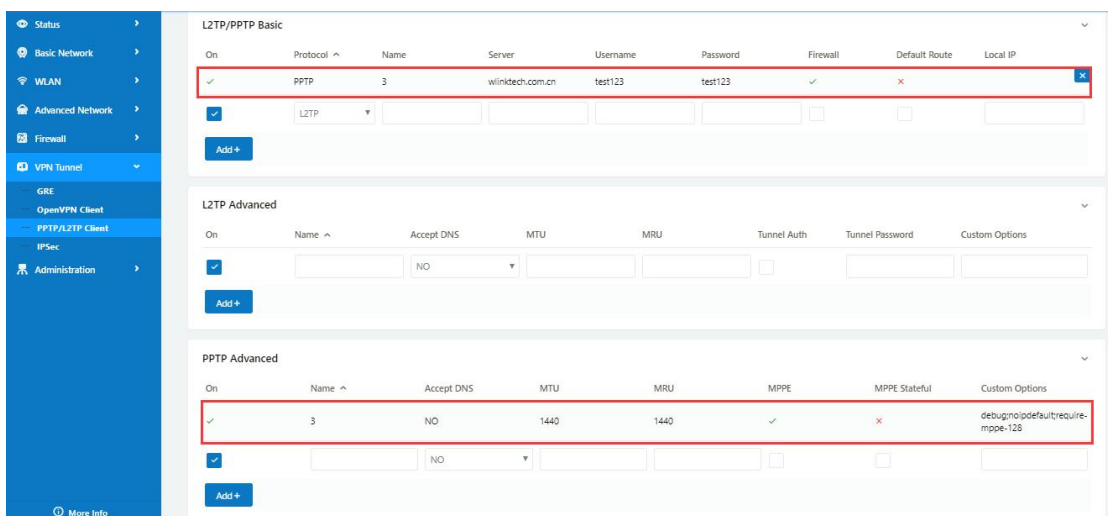
---End

3.8.3 L2TP/PPTP

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



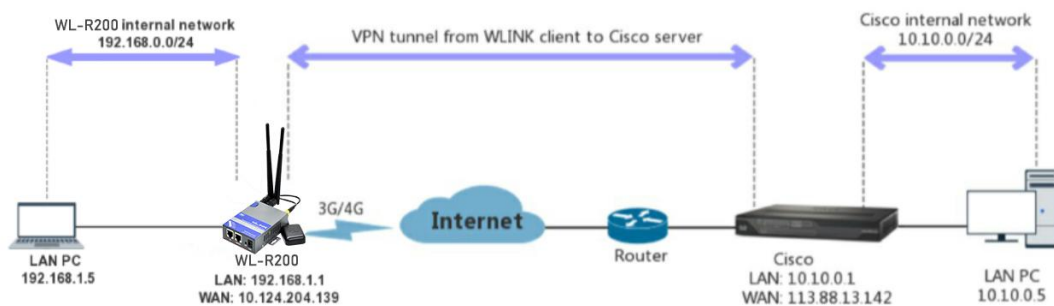
Configured as PPTP



Note: The Custom Options are based on your server
---End

3.8.4 IPSec

IPSec between WL-G520 and Cisco Router



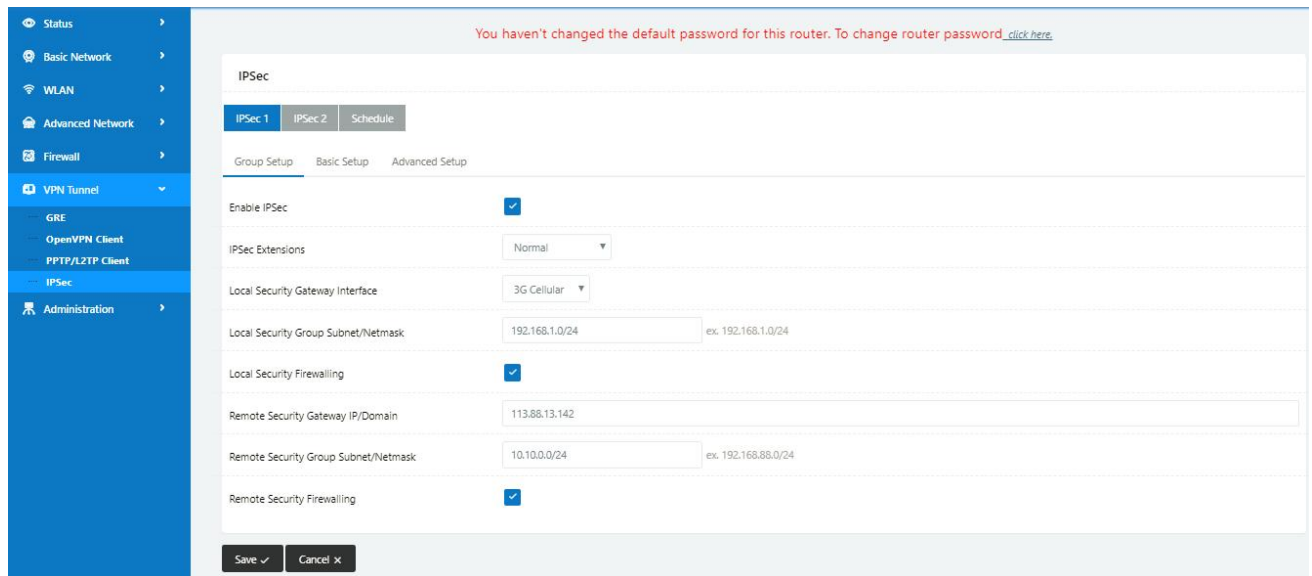
1) Cisco Config (main mode)

```
!
crypto isakmp policy 10
encr 3des
```

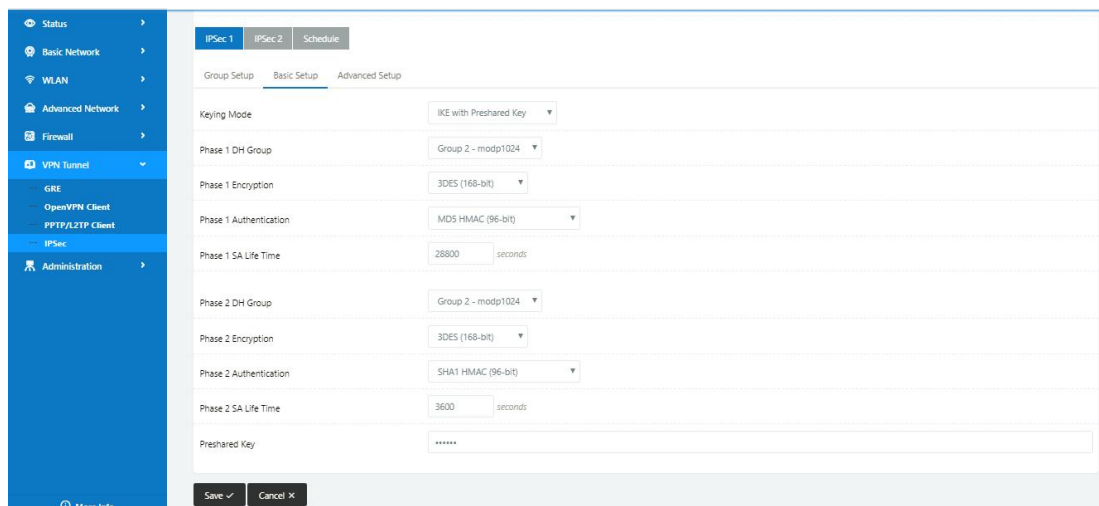
```
hash md5
authentication pre-share
group 2
crypto isakmp key test1234 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set Tran-set esp-3des esp-sha-hmac
crypto ipsec nat-transparency spi-matching
!
```

2) WLINK Config

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



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



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

| 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 | |
|-----------------------|-----------------------|
| 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 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