User Manual

---Apply to WL-G510 Series Industrial 4G Router

V4.0

http://www.wlink-tech.com

Jan, 2026

Caution

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

Version History

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

Data	Document Version	Software Version	Note
2026-1-30	V4.0	G5.0.1.5-250226-175022.trx	Improved WAN MAC Address
2024-12-16	V3.9	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	V3.7	G5.0.1.5-230116-113230.trx	Improve Configuration Restore. Add Configuration Instances.
2022-1-5	V3.6	G5.0.1.5-211103-170736	Added two OpenVPN tunnel Amended GUI Spelling.
2021-2-3	V3.5	G5.0.1.5-210106-165114	Improve SIM tray in hardware Added IKE2 and TR069
2020-3-1	V3.4	G5.0.1.5-200225-155218	Add IPsec Domain name. Add Configuration Instance
2019-7-2	V3.3	G5.0.1.5-190522-165655	Improved M2M Setting
2019-2-1	V3.1	G5.0.1.5-190116-175745	

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

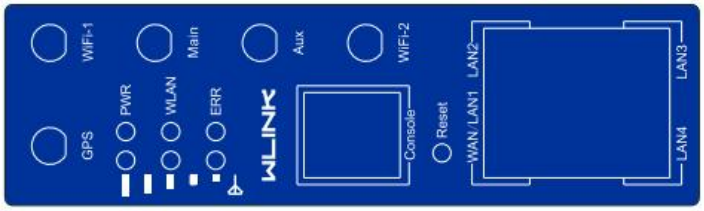
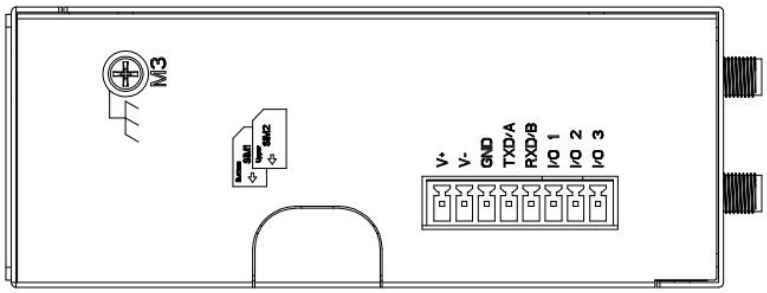
Contents

1 Hardware Installation

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-G510 Structure

WLINK Tech.	G510 series
Front	
Top	

NOTE

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

Table 1-2 Router Interface

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

Port	Instruction	Remark
Aux	LTE MIMO antenna	
GPS	GPS antenna, SMA connector, 50Ω.	
Wi-Fi1	Wi-Fi dual-band antenna, SMA connector	
Wi-Fi2	Wi-Fi dual-band antenna, SMA connector	
LAN	10/100/1000Base-TX，MDI/MDIX self-adaption.	
WAN/LAN	10/100/1000Base-TX，MDI/MDIX self-adaption.	Default as LAN
Reset	Reset button, (press on button at least 5 seconds)	
PWR	Power connector	7.5～32VDC
I/O	DI-1 and DI-2 are digital input, and DO is digital output.	
Console	RJ45-DB9 cable for CLI configuration.	

1.2 LED Status

Table 1-3 Router LED indictor Status

silk-screen	status		Indication
Signal	Signal	Constant light	LED1: weak (CSQ0~10). LED2: good (CSQ11~19) LED3: strong (CSQ20~31)
	Signal 1	Blink	dialing
		Constant light	online
PWR	Constant Light		System power operation.
WLAN	Constant light		WLAN enable, but no data communication.
	Blinking quickly		Data in transmitting
	Light off		WLAN disable
ERR	Light off		System operation and LTE/3G online.
	Constant Light(Red)		System fail indicator. It indicates SIM card/ module fail.
LAN	Green	Constant light	Connected.
	Green	Blinking	Data in transmitting.
	Green	Light off	Disconnection.

1.3 Dimension

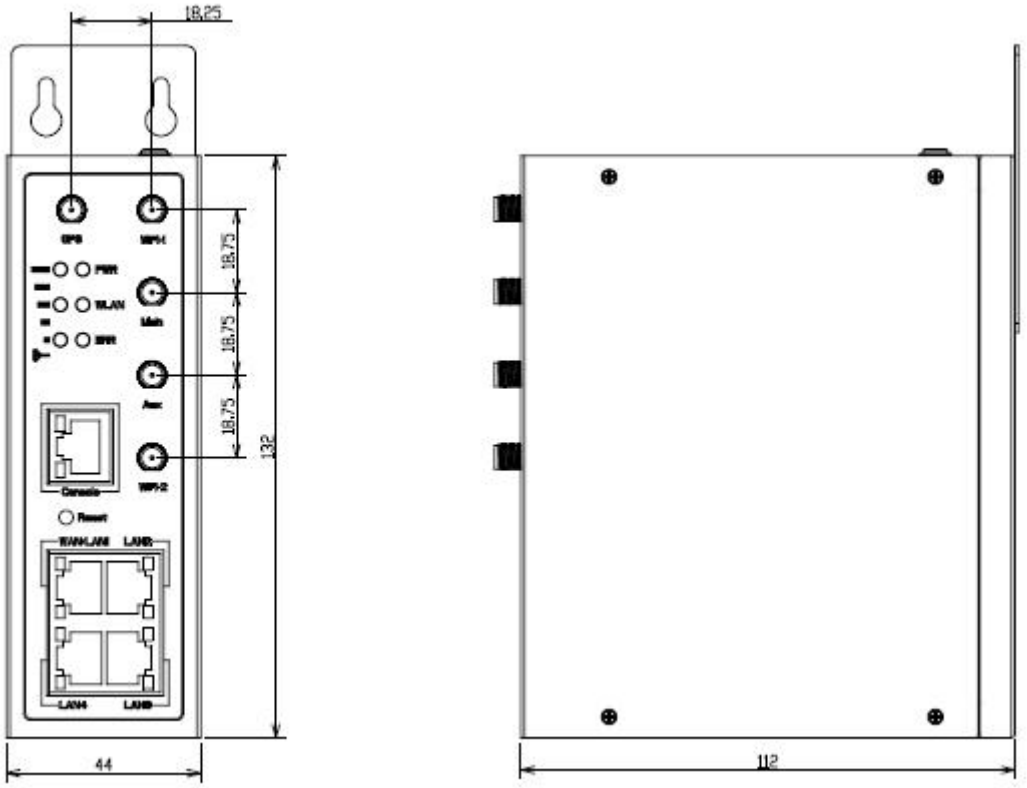
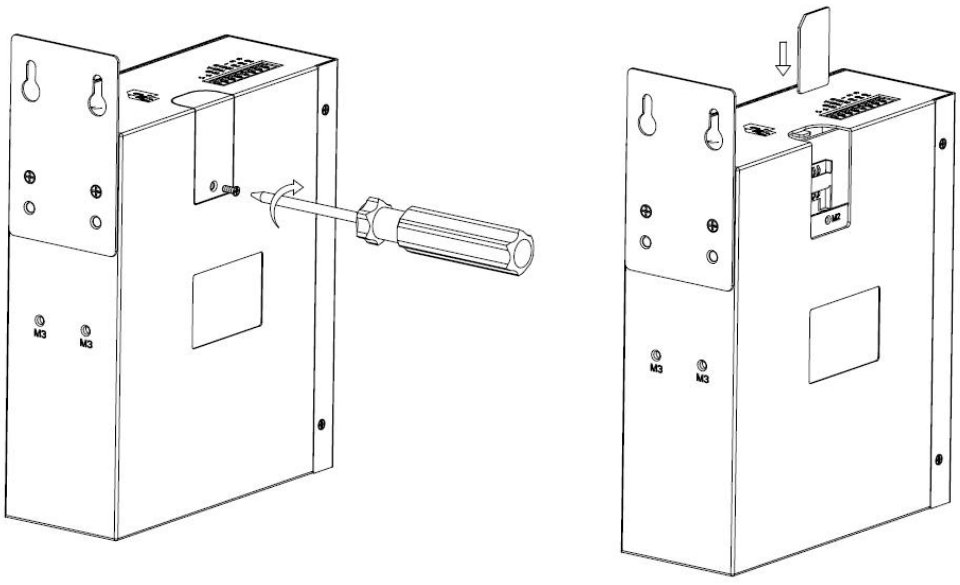


Figure 1-2 G510 Series Router Dimension

1.4 How to Install

1.4.1 SIM/UIM card install

Please insert the dual SIM cards before configure the router.



CAUTION

Before connecting, please disconnect any power resource of router

1.4.2 Ethernet Cable Connection

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

1.4.3 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.

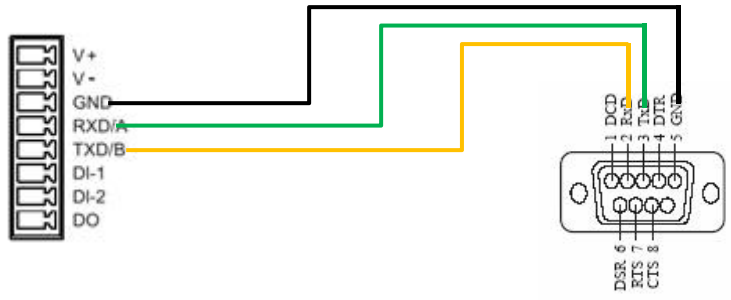
NOTE

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	V+	Power V+, Anti reverse
2	V-	Power V-
3	GND	GND for RS232 communication
4	RXD/A	RS232 RXD, 57600bps as default
5	TXD/B	RS232 TXD, RS485 optional
6	DI-1	Digital Input, Dry Contact
7	DI-2	Digital Input, Dry Contact
8	DO	Short to GND



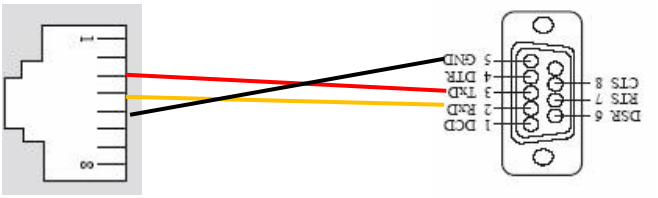
CAUTION

The serial port will be unavailable in WL-G510 standalone GPS model.

1.4.5 Console Port Connection

Connect the router to a computer by an RJ45-DB9 cable for CLI configuration and router system debugging.

Pin	Instruction	Remark
1	CTS	Input
2	RTS	Output
3	RXD	Input
4	TXD	Output
5	GND	GND
6	DSR	Input
7	DCD	Output
8	DTR	Output



1.4.6 Power Supply

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

1.4.7 Review

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

CAUTION

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

Notice:

Step 1 Check the antenna connection.

Step 2 Check SIM/UIM card, confirm SIM/UIM card is available.

Step 3 Power on the industrial Router

----END

2 Router Configuration

WL-G510 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.

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

2.2.1 Overview

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

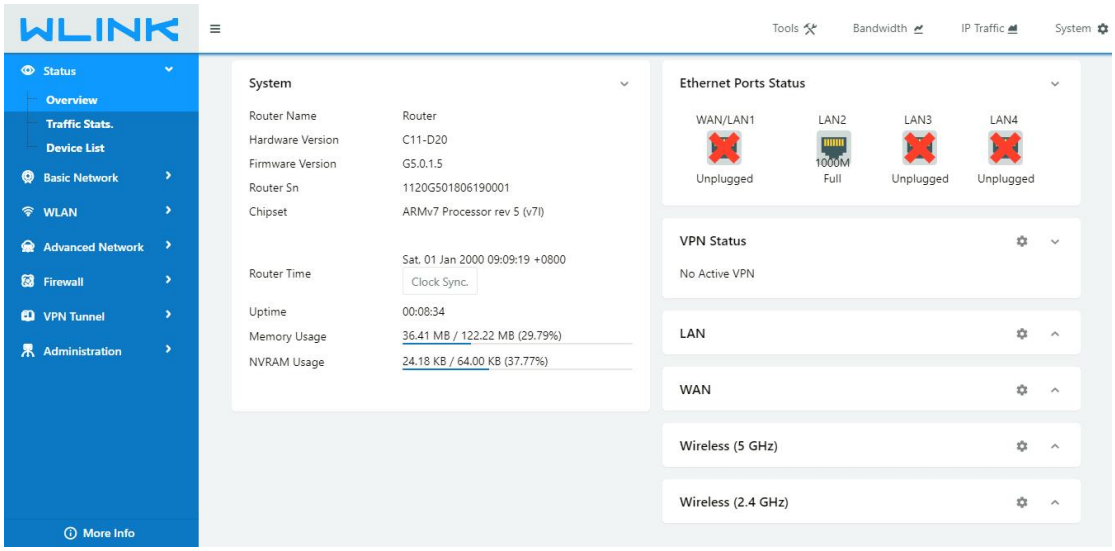


Figure 2-3 Router Status GUI

2.2.2 Traffic Stats.

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

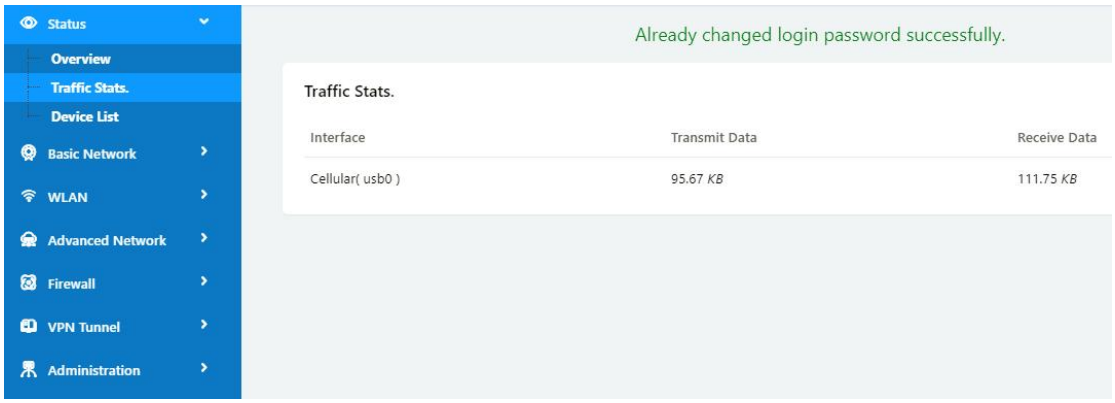


Figure 2-4 Traffic Stats. GUI

2.2.3 Device List

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

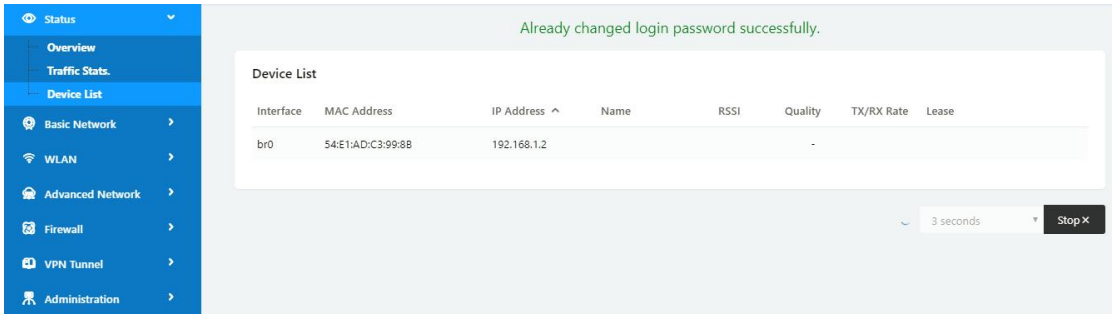


Figure 2-5 Device List GUI

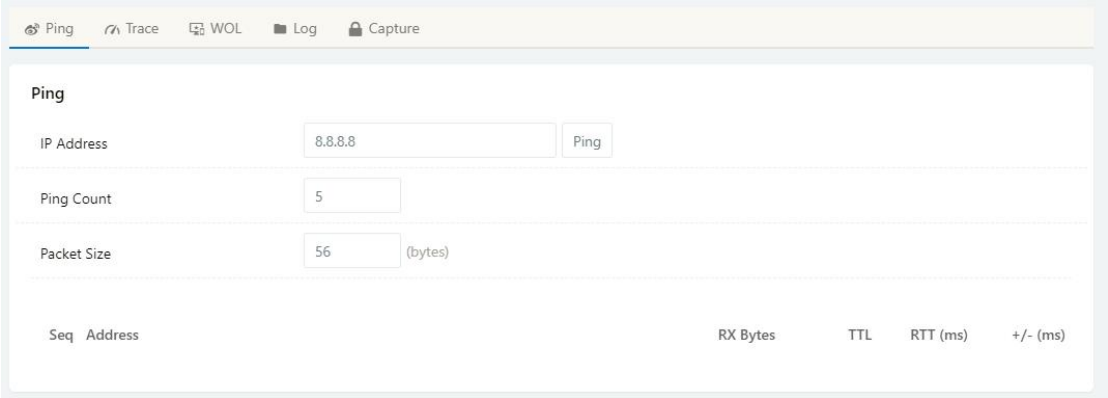
2.3 Tool Column

Figure 2-6 Tool Column GUI

2.3.2 Tools

2.3.2.1 Ping

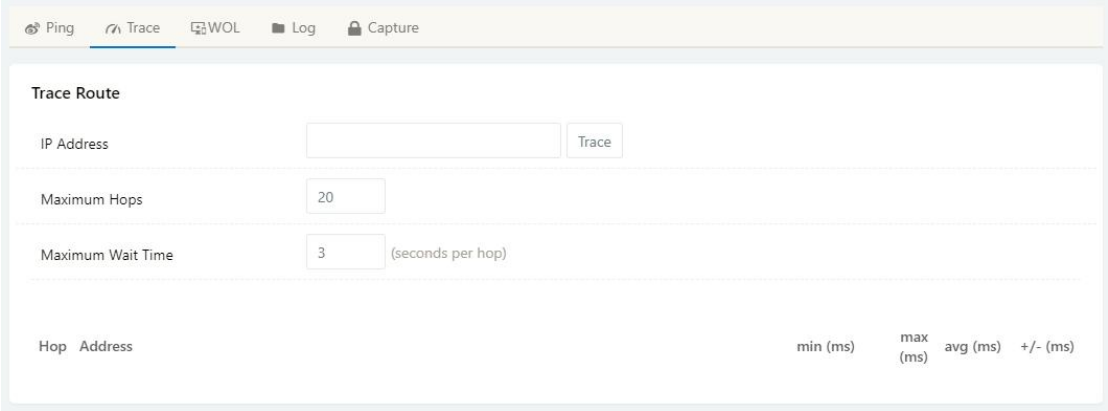
Click Tools->Ping to enter ping test GUI. Used to test the reachability of a host on an Internet IP network and to measure the round-trip time for messages sent from the originating host to a destination server.



Parameter	Instruction
IP Address	Target IP address to perform the ping test
Ping Count	Number of ping tests to be performed for each address
Packet Size	Packet size for ping test

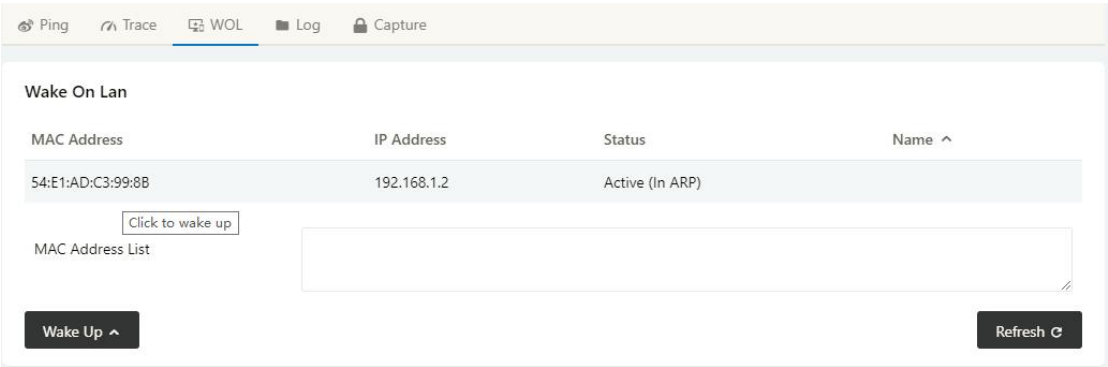
2.3.2.2 Trace

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



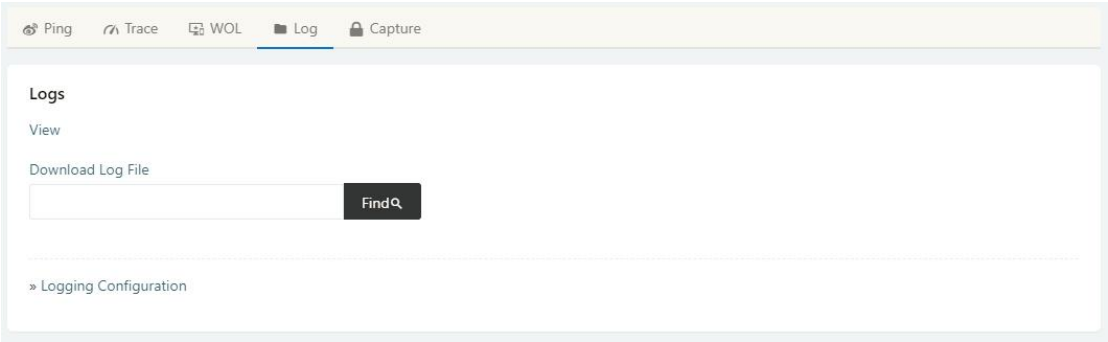
2.3.2.3 WOL

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



2.3.2.4 Log

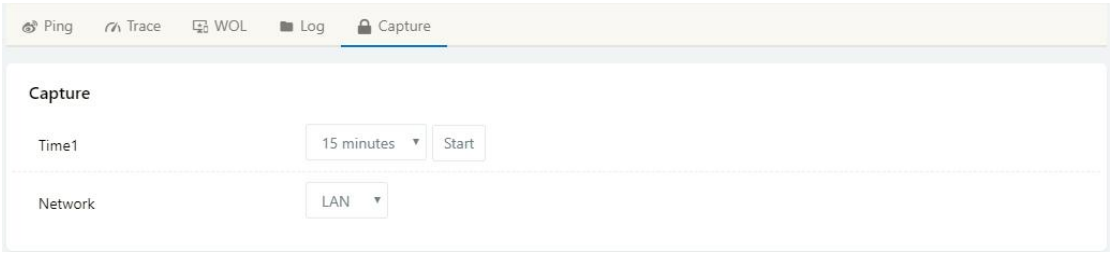
Click Tools-> Log to enter Log GUI. Use to check logs in GUI, download GUI and send logs to server.



Parameter	Instruction
View	Click View to check the router's live log
Download Log File	Click to Download a log file, RAM space is limited and only about 3 minutes of log content is cached, so if need more content, please use the log tool to get more content.

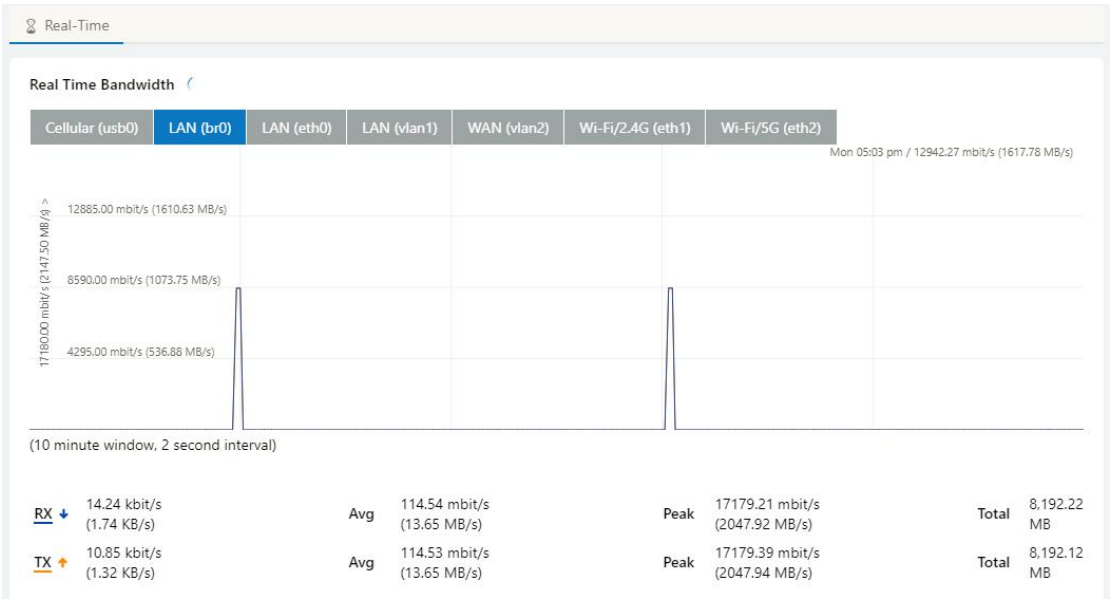
2.3.2.5 Capture

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



2.3.3 Bandwidth

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



2.3.4 System

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

2.4 Basic Network

2.4.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface.

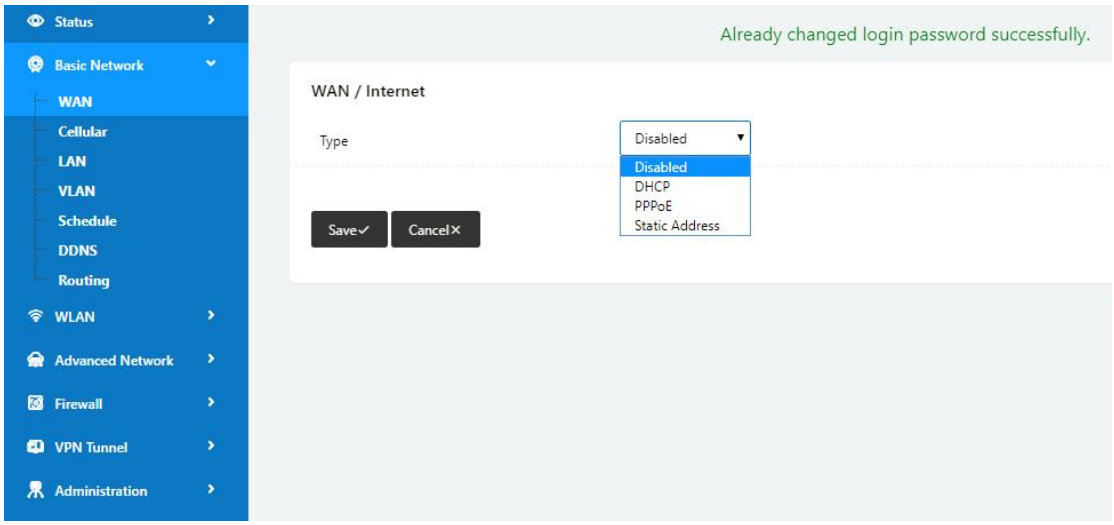


Table 2-1 WAN Setting Instruction

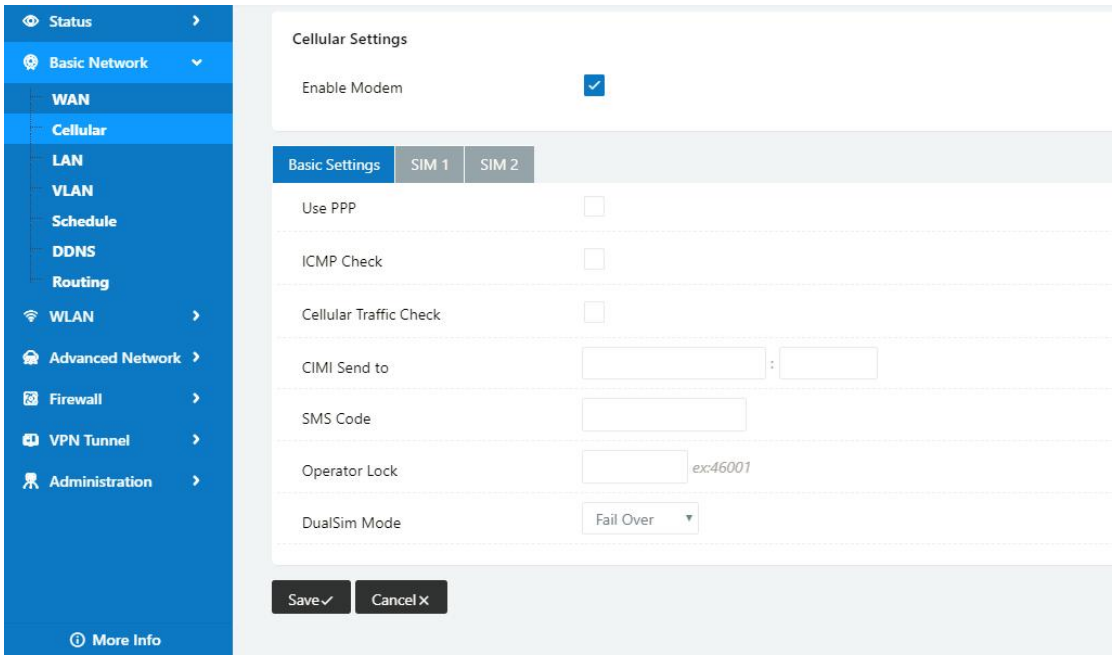
Parameter	Instruction
Disabled	Turn off the WAN Ethernet port
DHCP	WAN port automatically get an IP address
PPPoE	WAN port to get network via PPPOE dial-up
Static Address	WAN port to get network via a static IP address

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

----End

2.4.2 Cellular Setting

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



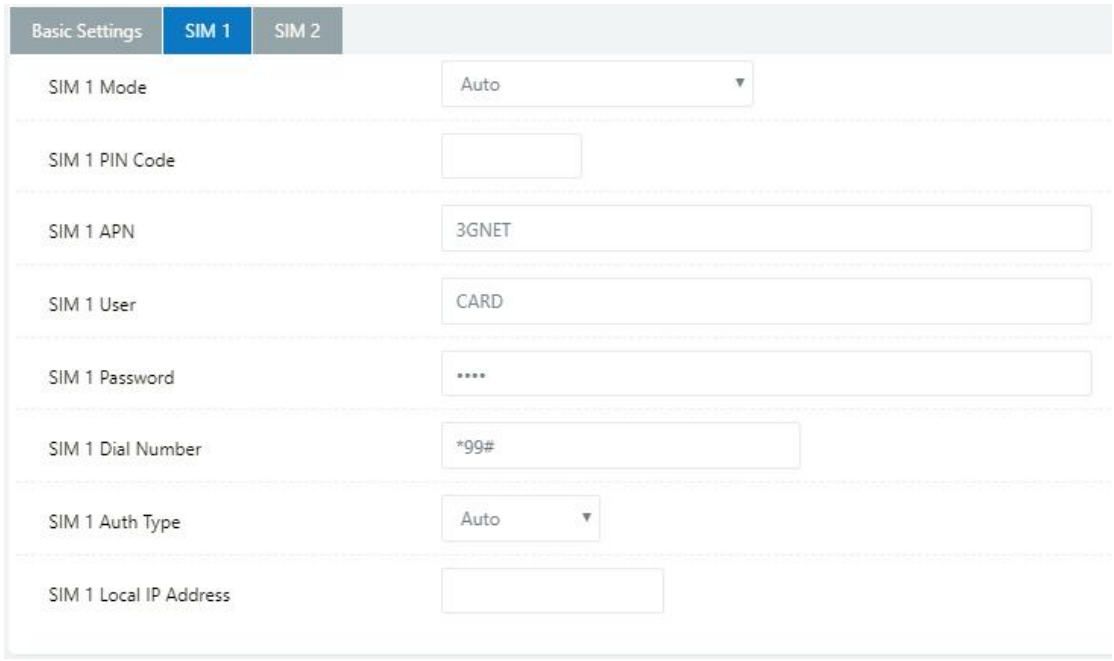


Table 2-2 WAN Setting Instruction

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.

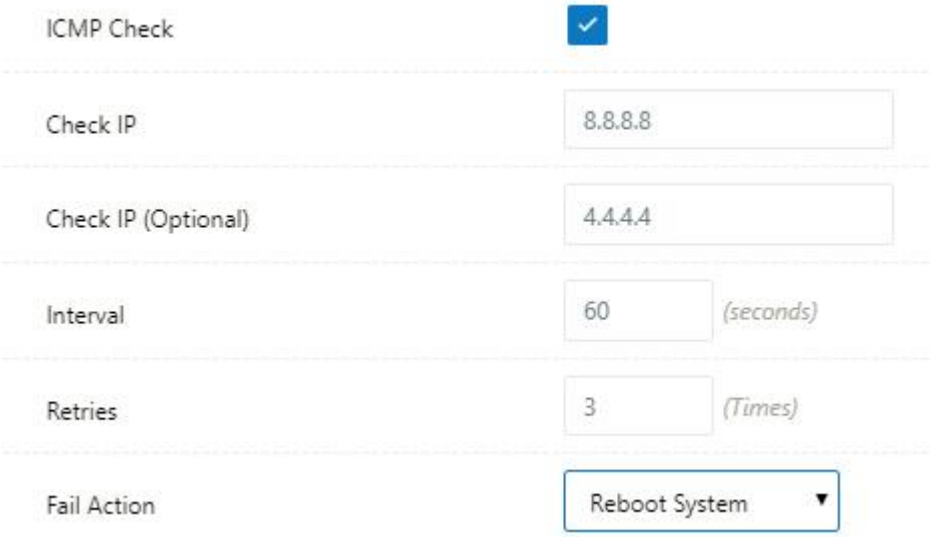
Parameter	Instruction
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock a specified operator for the router by MCC/MNC code.
Dual SIM Mode	【Fail Over】Two SIM cards mutual backup. Once 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.
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.

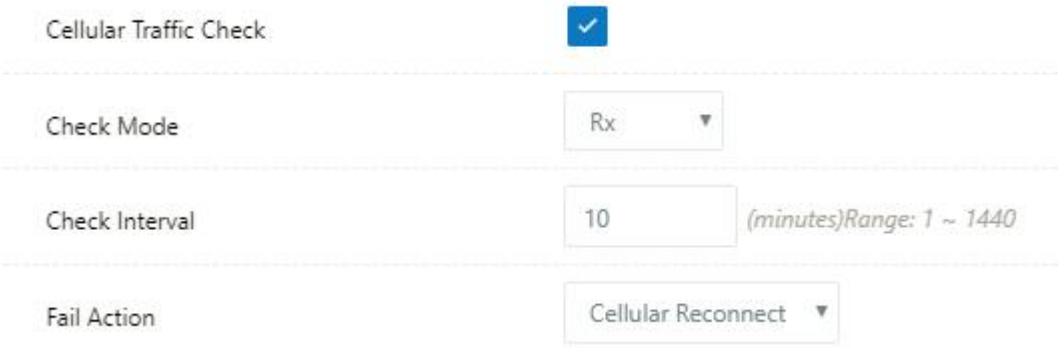
The ICMP Check IP is a public IP or company server IP address.



【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.



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

----End

2.4.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface

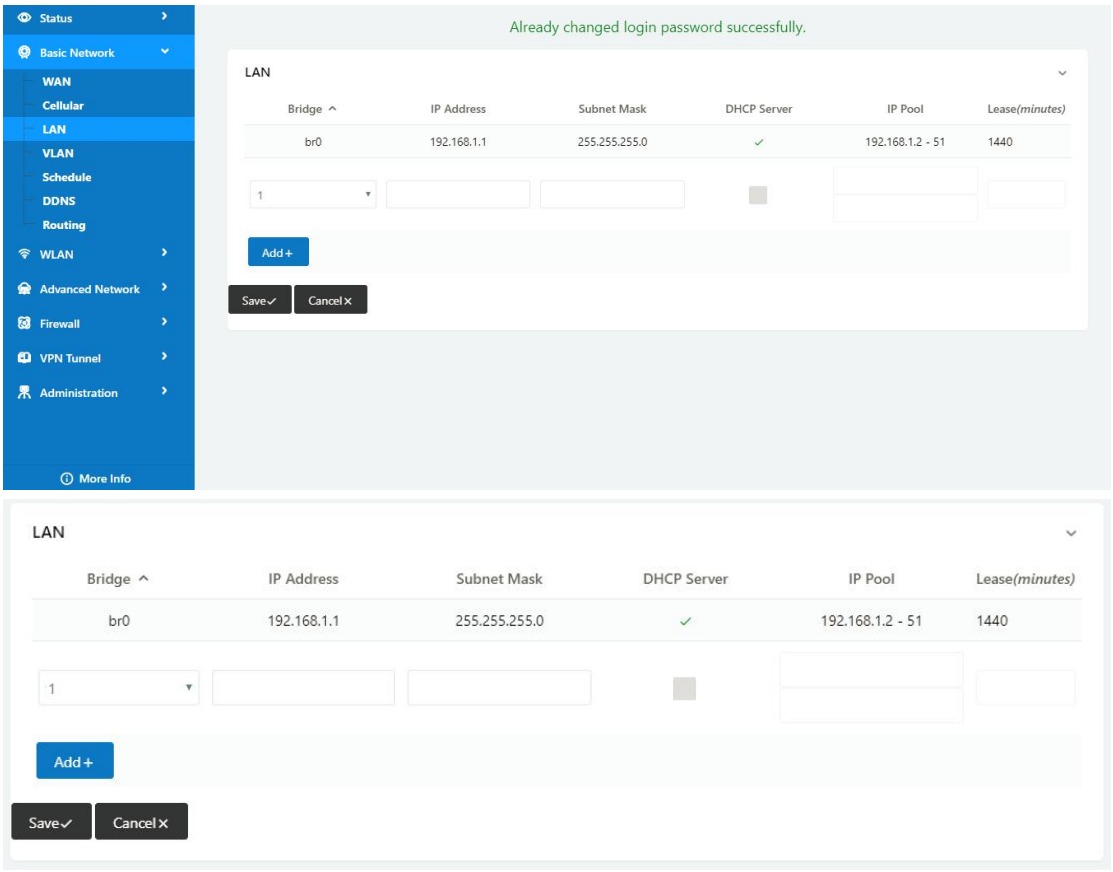


Table 2-3 LAN Setting Instruction

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

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

----End

2.4.4 **VLAN**

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

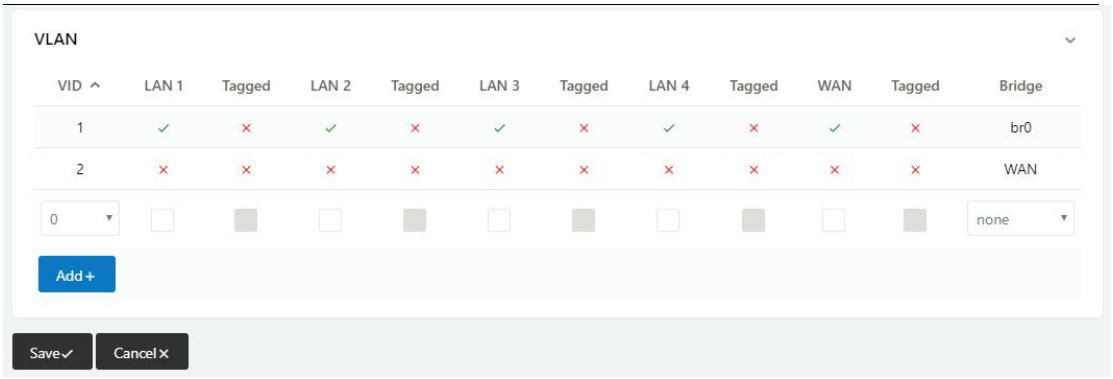


Table 2-4 LAN Setting Instruction

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

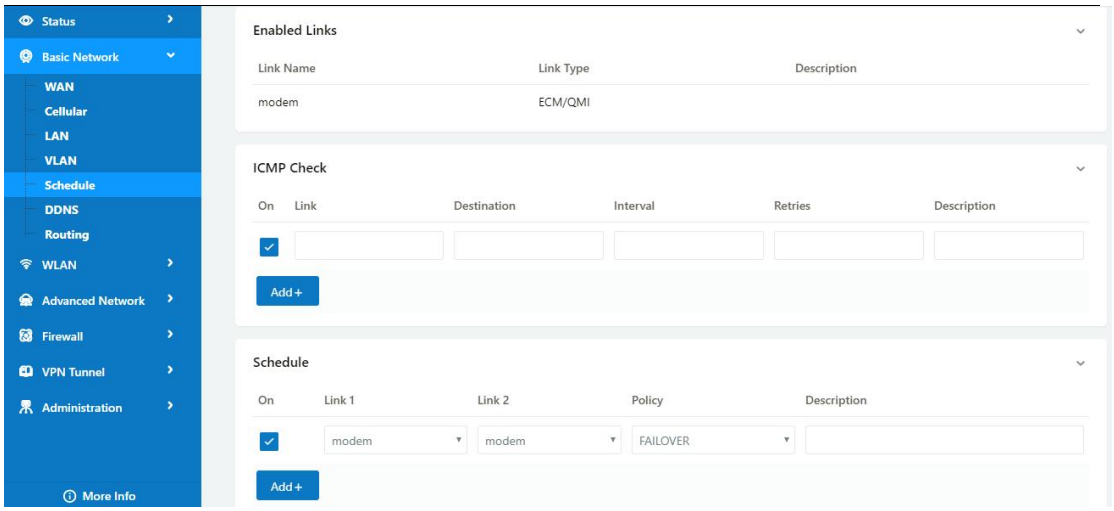
Configuration Instance

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

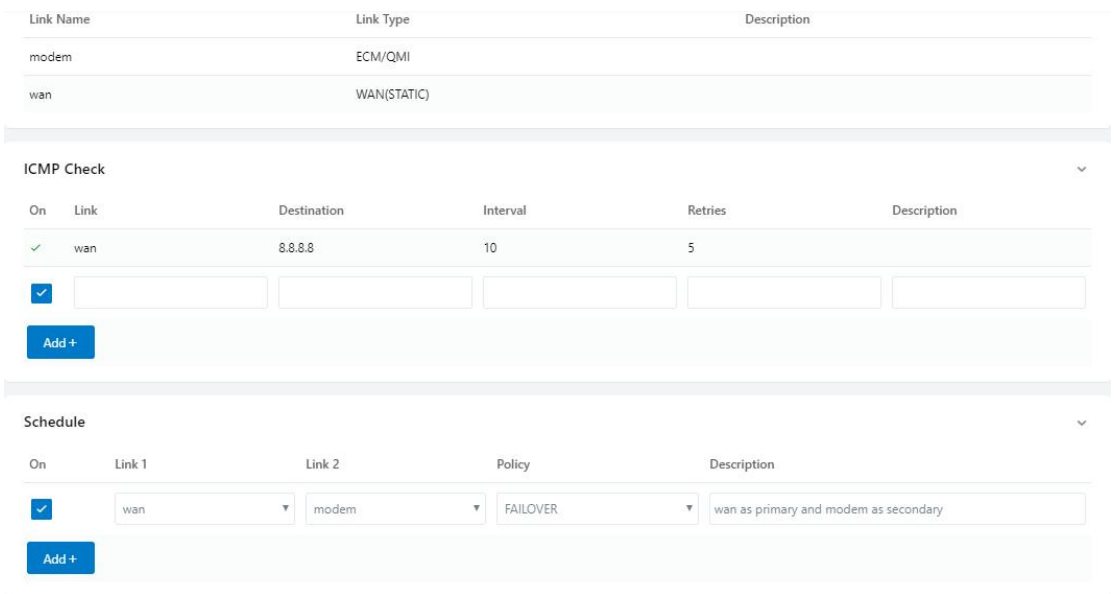
----End

2.4.5 Schedule

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

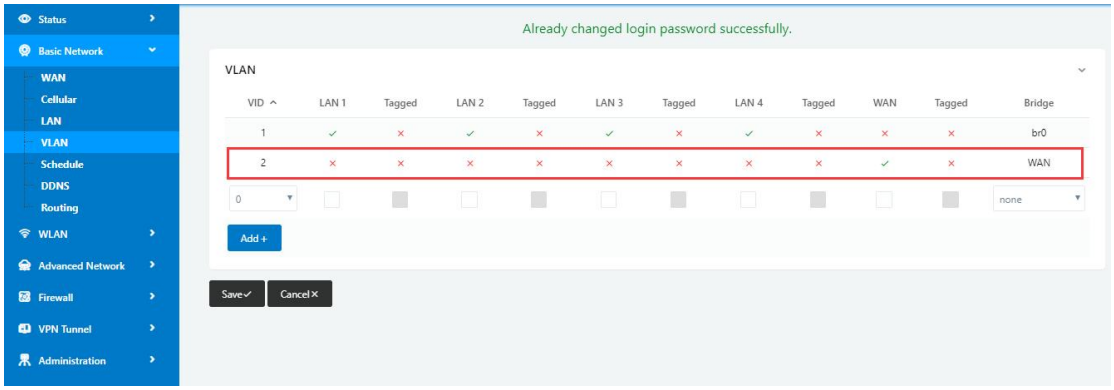


Parameters	Instruction
modem	The router dial-up to network via modem
wan	The router dial-up to network via WAN (DHCP, PPPOE, Static IP) port.
ICMP Check	When the ICMP Check fails, the switching action between Link1 and Link2 will be triggered.
Link1	The Primary link
Link2	The Secondary link
BACKUP	Link1 and Link2 mutual backup. Link1 is the primary link. Once Link1 is failed, it will switch to Link2 and work on Link2. Once Link1 recovers, it will switch back to Link1.
FAILOVER	Link1 is the primary link, Link2 is the backup link. Once Link1 is failed, it will switch to Link2 and work on Link2.



NOTE

The VLAN should be configured with WAN and 4G backup together. Please define WAN port as bridge WAN interface in the VLAN GUI as below.



Step 2 Please Click “Save“ to finish.

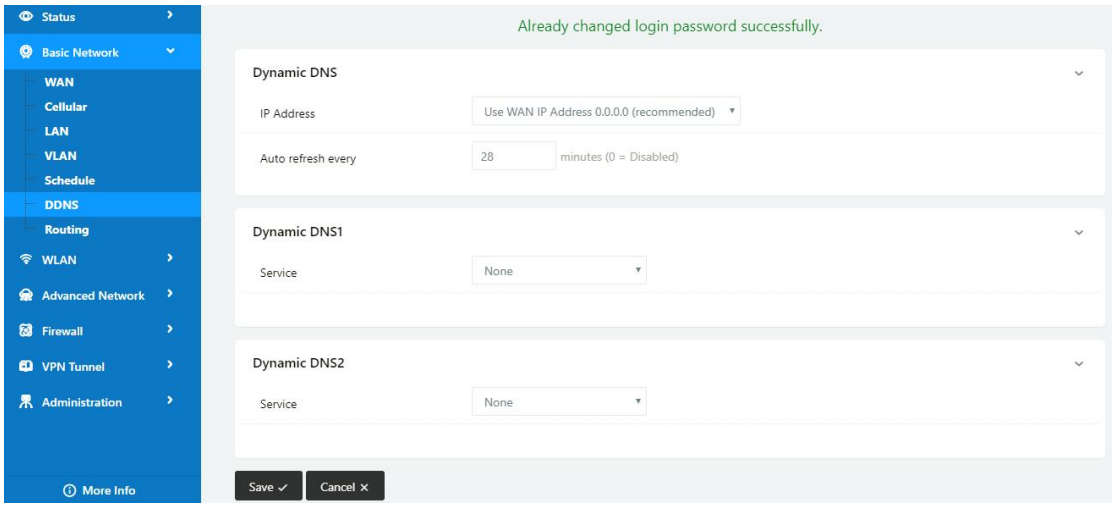
Configuration Instance

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

----End

2.4.6 Dynamic DNS Setting

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



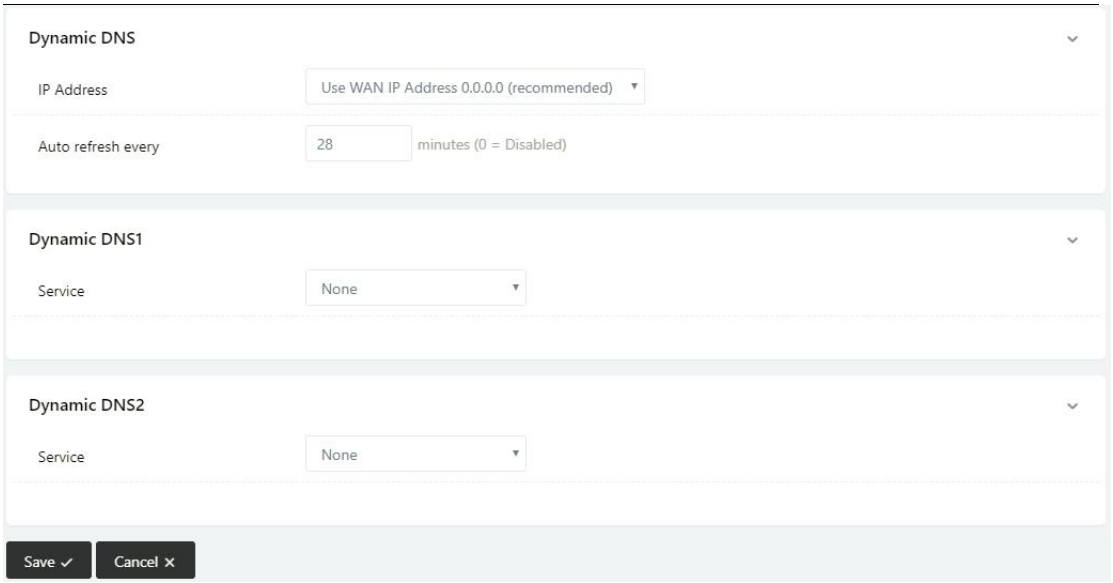


Table 2-5 DDNS Setting Instruction

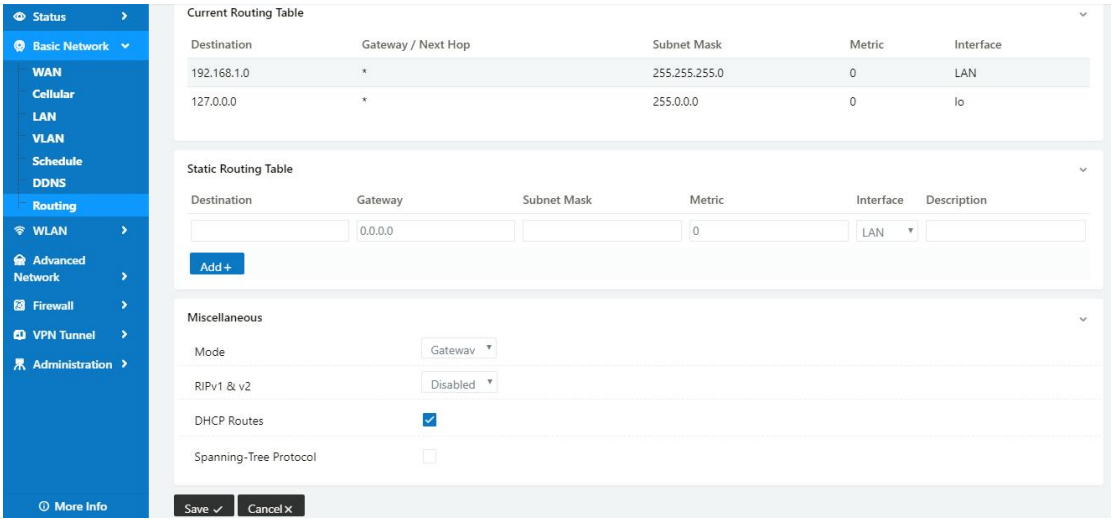
parameter	Instruction
IP address	Default is standard DDNS protocol, for customized protocol, please contact Wlink engineer. Usually, use default IP 0.0.0.0
Auto refresh time	Set the interval of the DDNS client obtains new IP, suggest 240s or above
Service provider	Select the DDNS service provider that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

Step 2 Please Click “Save“ to finish.

----End

2.4.7 **Routing Setting**

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



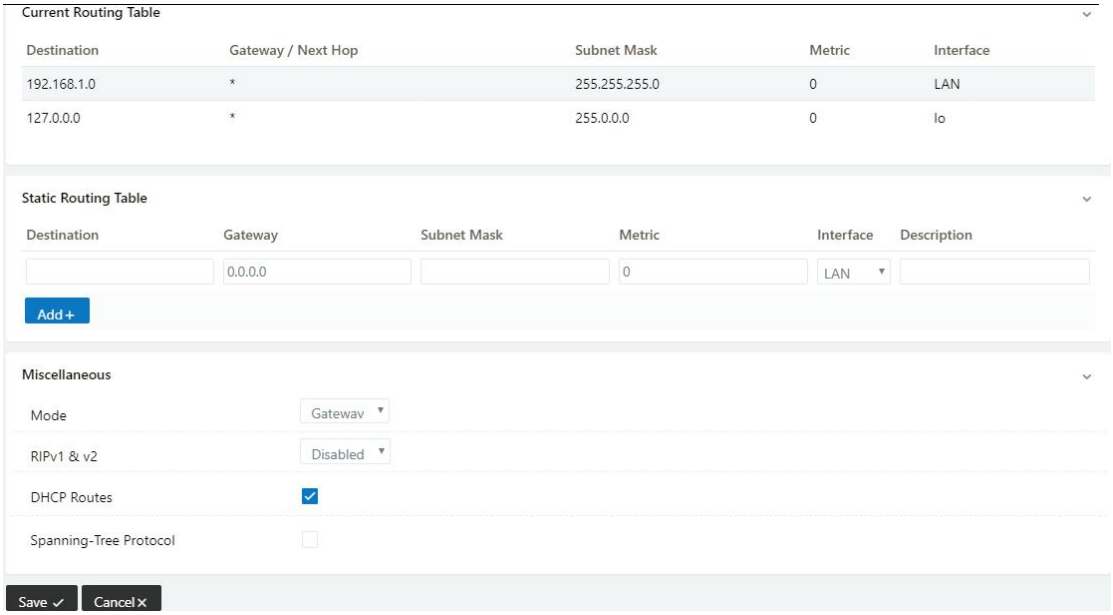


Table 2-6 Routing Setting Instruction

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

Step 2 Please Click " Save " to finish.

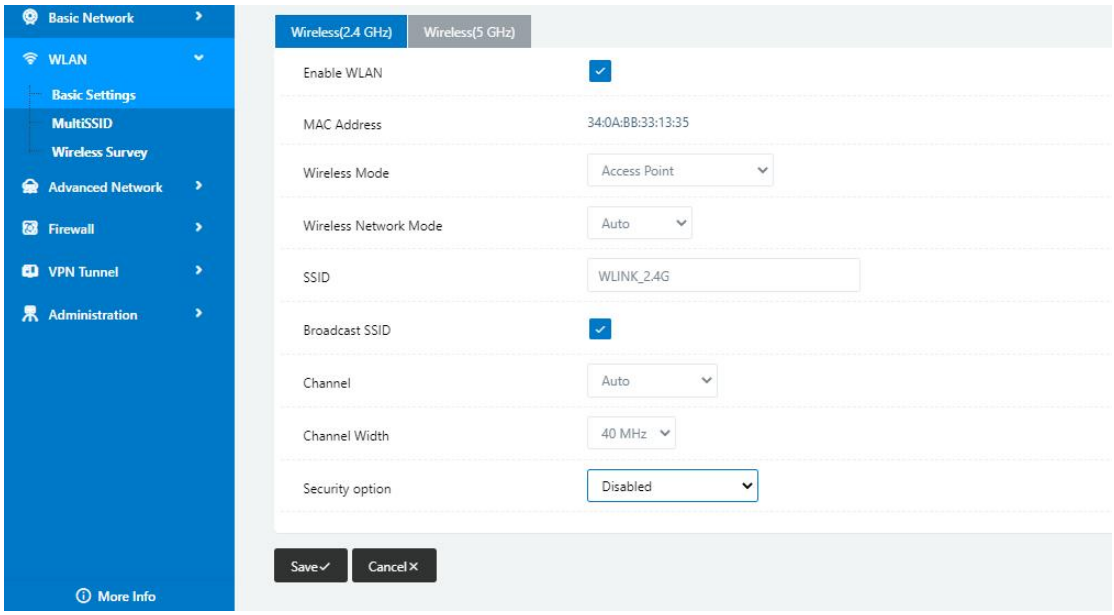
----End

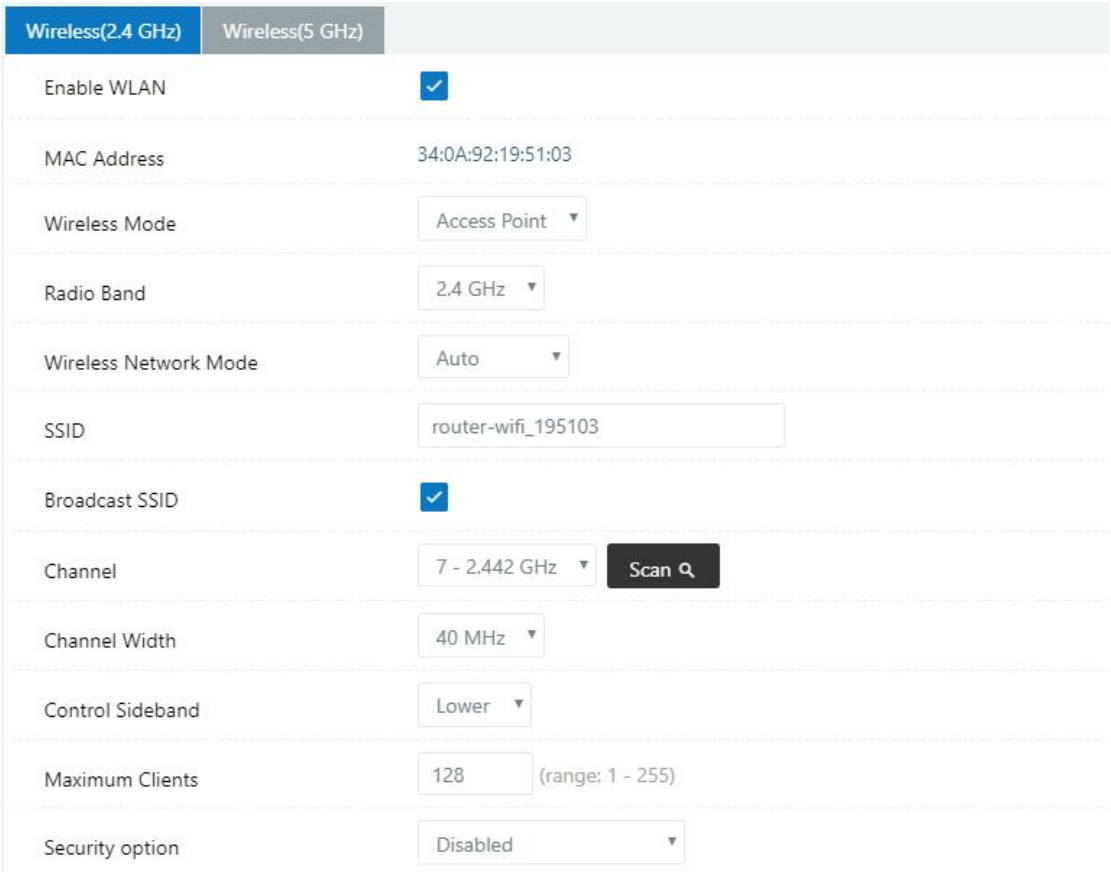
2.5 WLAN Setting

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

2.5.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter


Basic Network
WLAN
Basic Settings
MultiSSID
Wireless Survey
Advanced Network
Firewall
VPN Tunnel
Administration
More Info
Wireless(2.4 GHz)
Wireless(5 GHz)
Enable WLAN
MAC Address
34:0A:BB:33:13:35
Wireless Mode
Access Point
Wireless Network Mode
Auto
SSID
WLINK_2.4G
Broadcast SSID
Channel
Auto
Channel Width
40 MHz
Security option
Disabled
Save
Cancel


Wireless(2.4 GHz)
Wireless(5 GHz)
Enable WLAN
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
Channel
7 - 2.442 GHz
Scan
Channel Width
40 MHz
Control Sideband
Lower
Maximum Clients
128
(range: 1 - 255)
Security option
Disabled

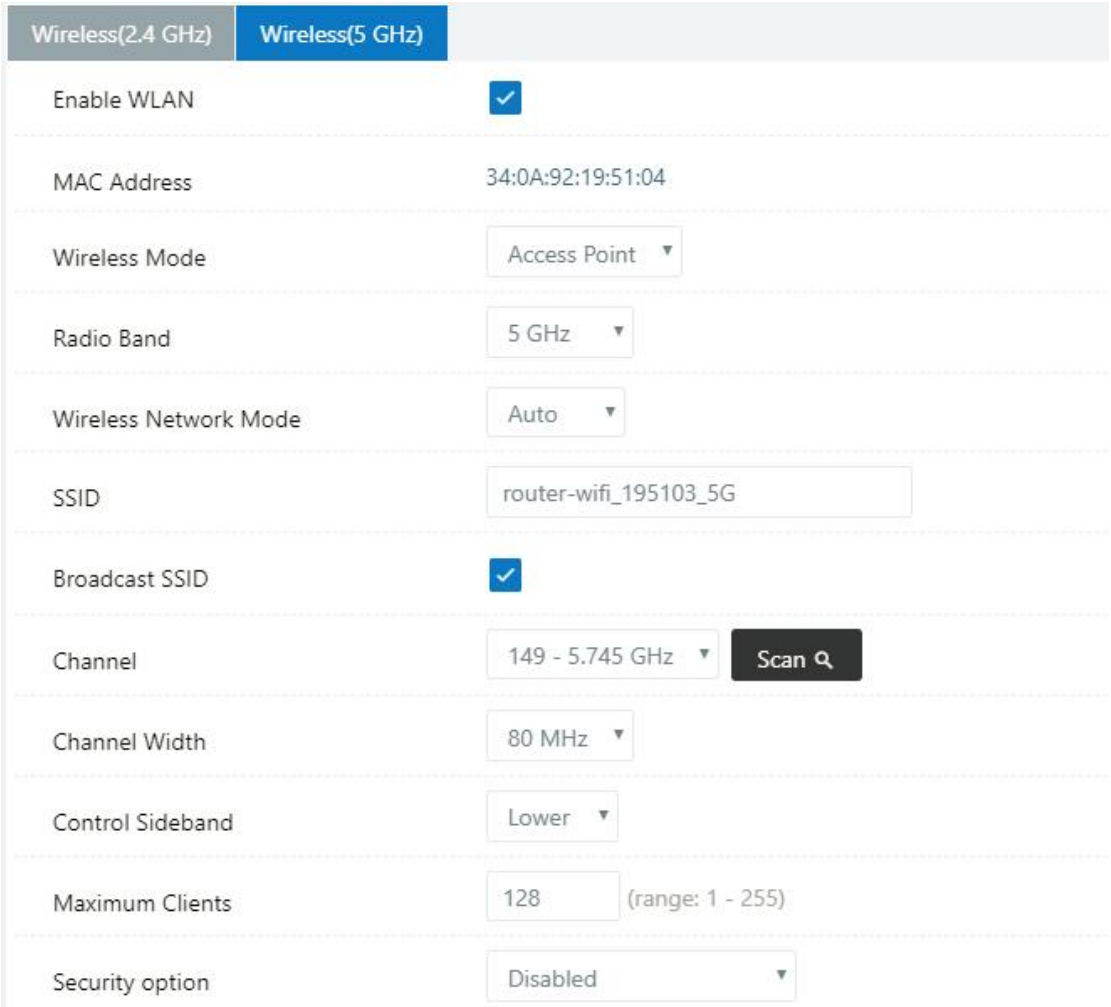


Table 2-7 Basic of WLAN Setting Instruction

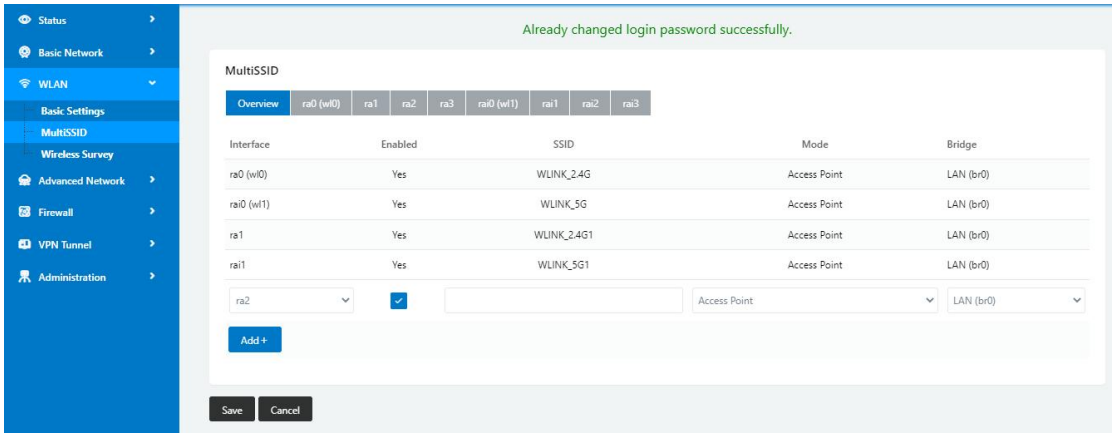
Parameter	Instruction
Radio Mode	2.4G+5G mode as default. Support 2.4G, 5G modes optional. 2.4G+5G model, Wi-Fi bandwidth for 683Mbps 2.4G model, Wi-Fi bandwidth for 300Mbps 5G model, Wi-Fi bandwidth for 866Mbps
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP mode.
Wireless Network 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

2.5.2 MultiSSID

Step 1 WLAN->MultiSSID to configure relative parameter.



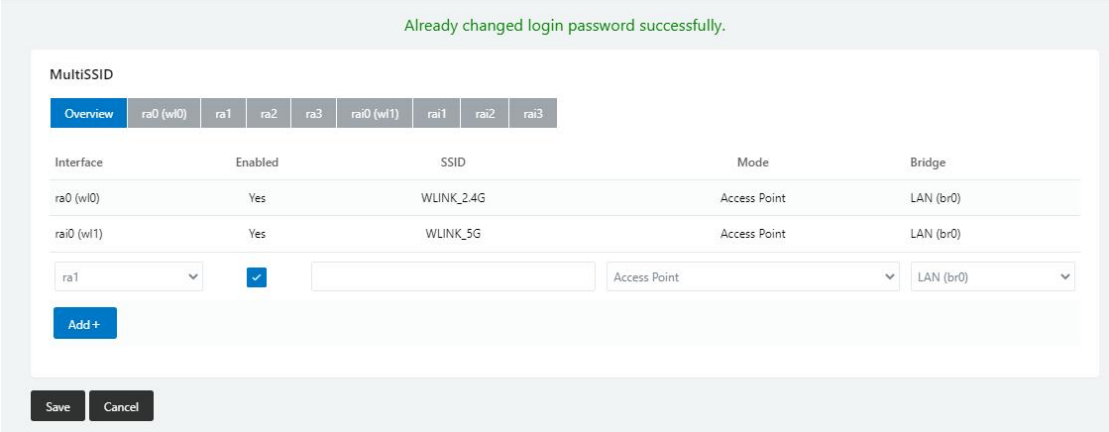


Table 2-8 MultiSSID of WLAN Setting Instruction

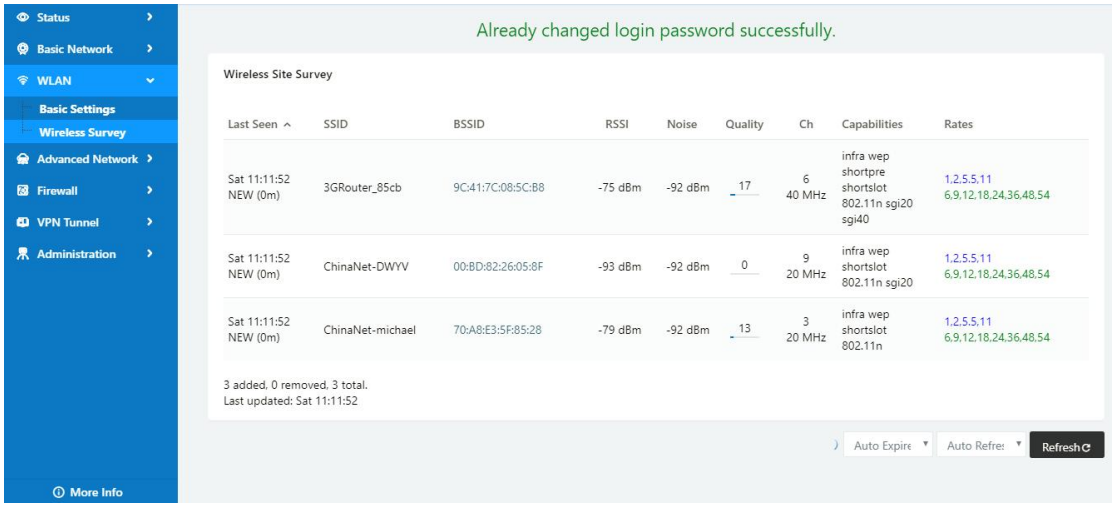
Parameter	Instruction
Overview	SSID List including Interface, Status, SSID name, mode.
Interface	Ra0~3 for 2.4G interface. Rai0~3 for 5G Wi-Fi interface
SSID	Support 4 SSID for 2.4G and 5G Wi-Fi.
Mode	Support Access Point, Wireless Client and Wireless Ethernet Bridge options.
Bridge	Bridge LAN(Br0) interface as default.
Channel	The channel of wireless network, suggest keep the default

Step 2 Please click “Save” to finish.

----End

2.5.3 Wireless Survey

Click WLAN> Wireless Survey to survey the near wireless sites information.



2.6 Advanced Network Setting

2.6.1 Port Forwarding

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

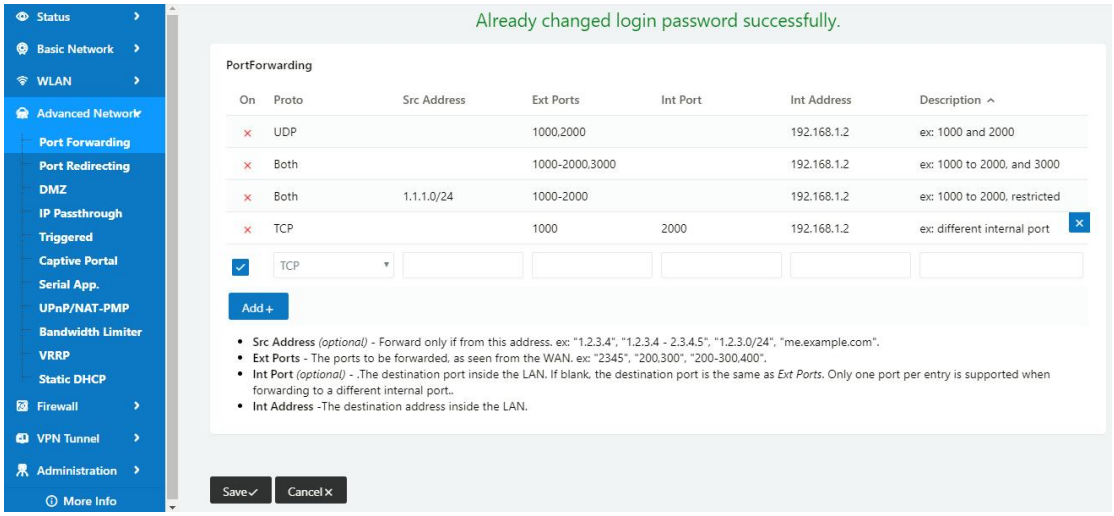


Table 2-9 Port Forwarding Instruction

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.

Configuration Instance

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

----End

2.6.2 Port Redirecting

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

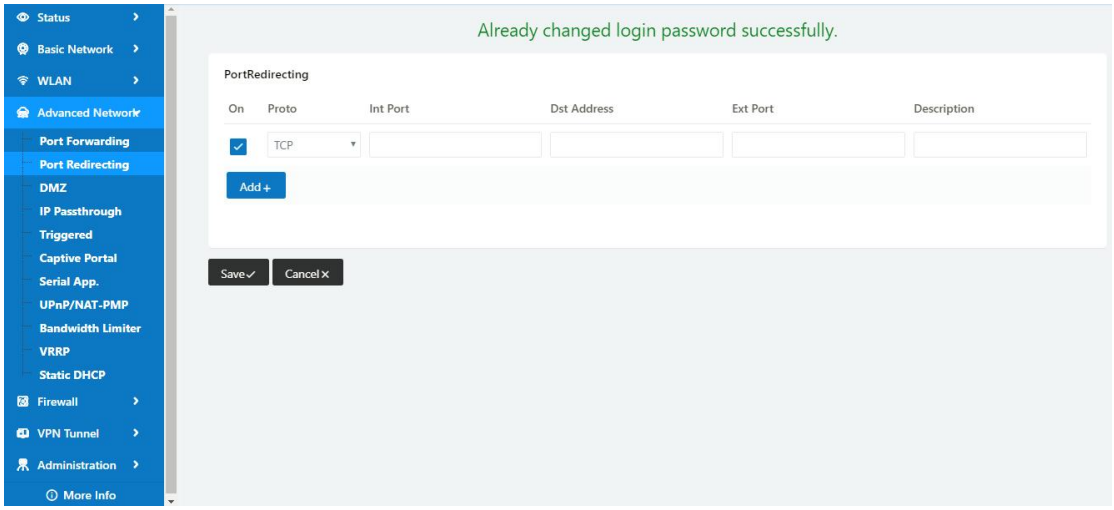


Table 2-10 Port Redirecting Instruction

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.

Parameter	Instruction
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

2.6.3 DMZ Setting

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

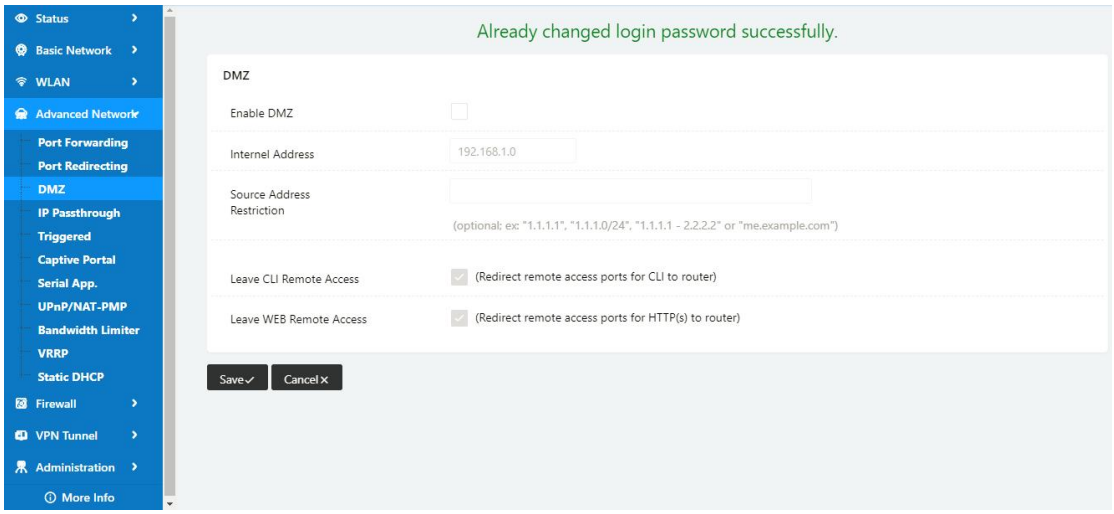


Table 2-11 DMZ Instruction

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

2.6.4 IP Passthrough Setting

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

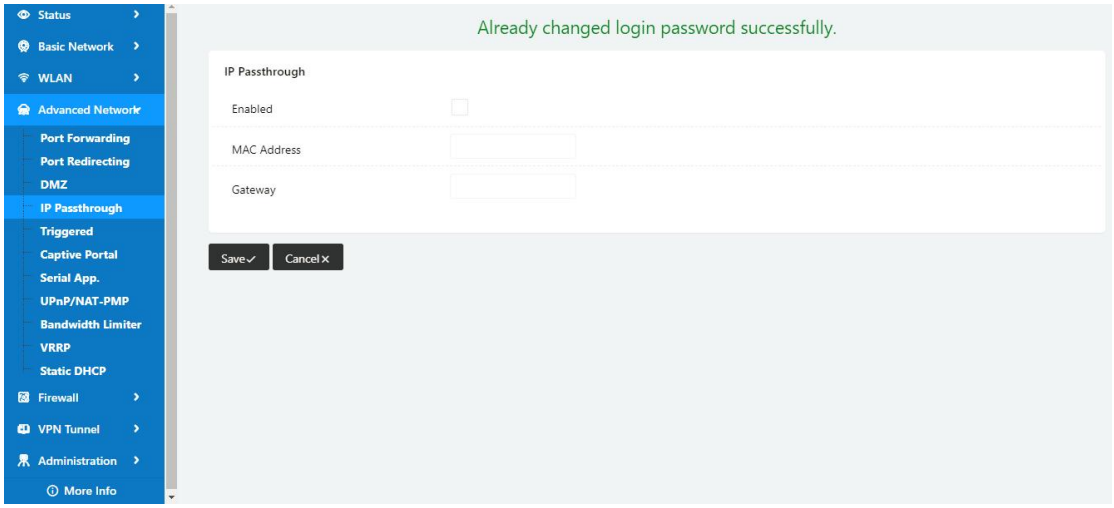


Table 2-12 IP Passthrough Instruction

parameter	Instruction
Enable	Enable IP Passthrough
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.
Gateway	If WL-G510 connect to multiple device, input other device gateway. 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

2.6.5 Triggered Setting

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

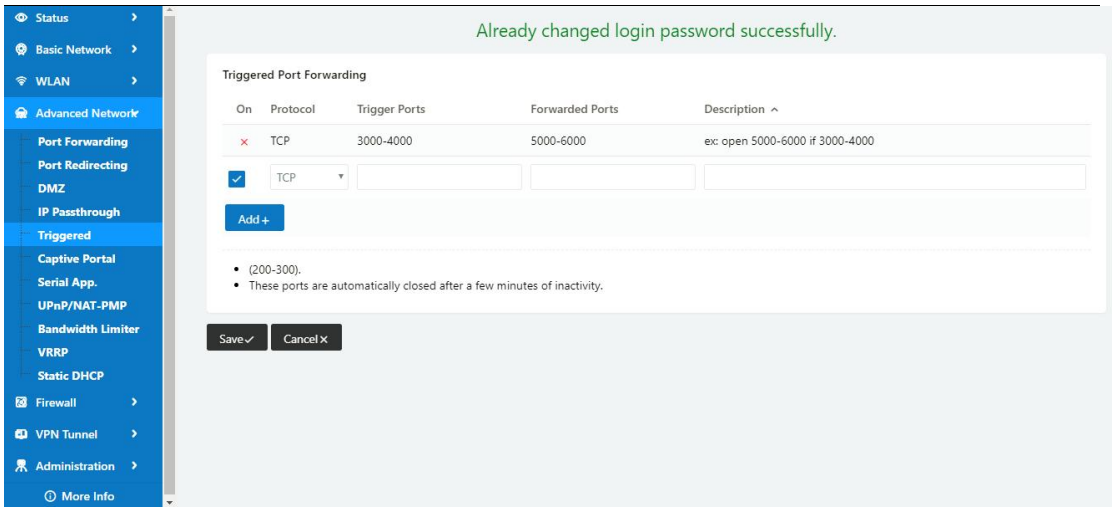


Table 2-13 Triggered Instruction

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

2.6.6 Captive Portal

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

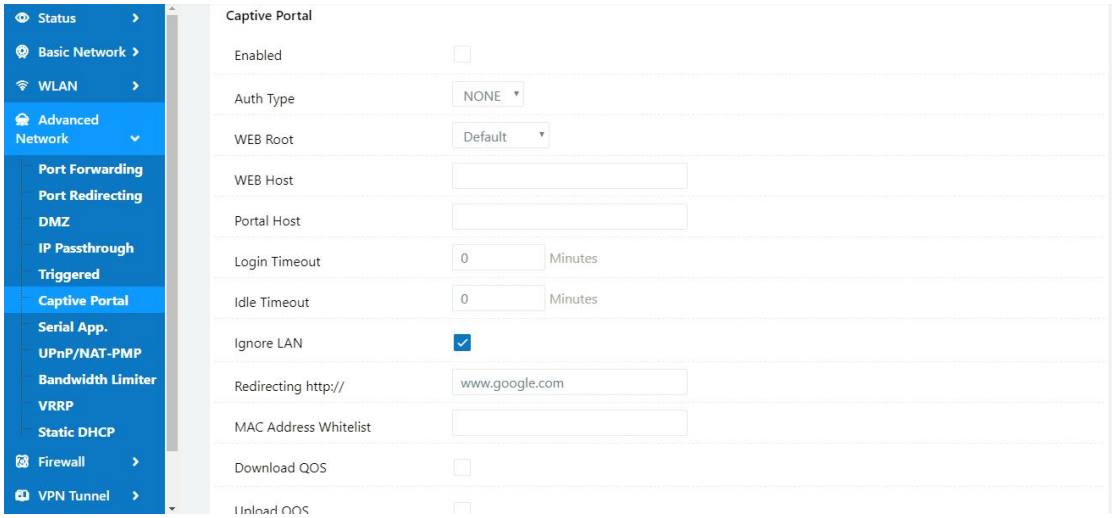


Table 2-14 Captive Portal Instruction

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.
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.

Configuration Instance

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

----End

2.6.7 Serial App. Setting

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

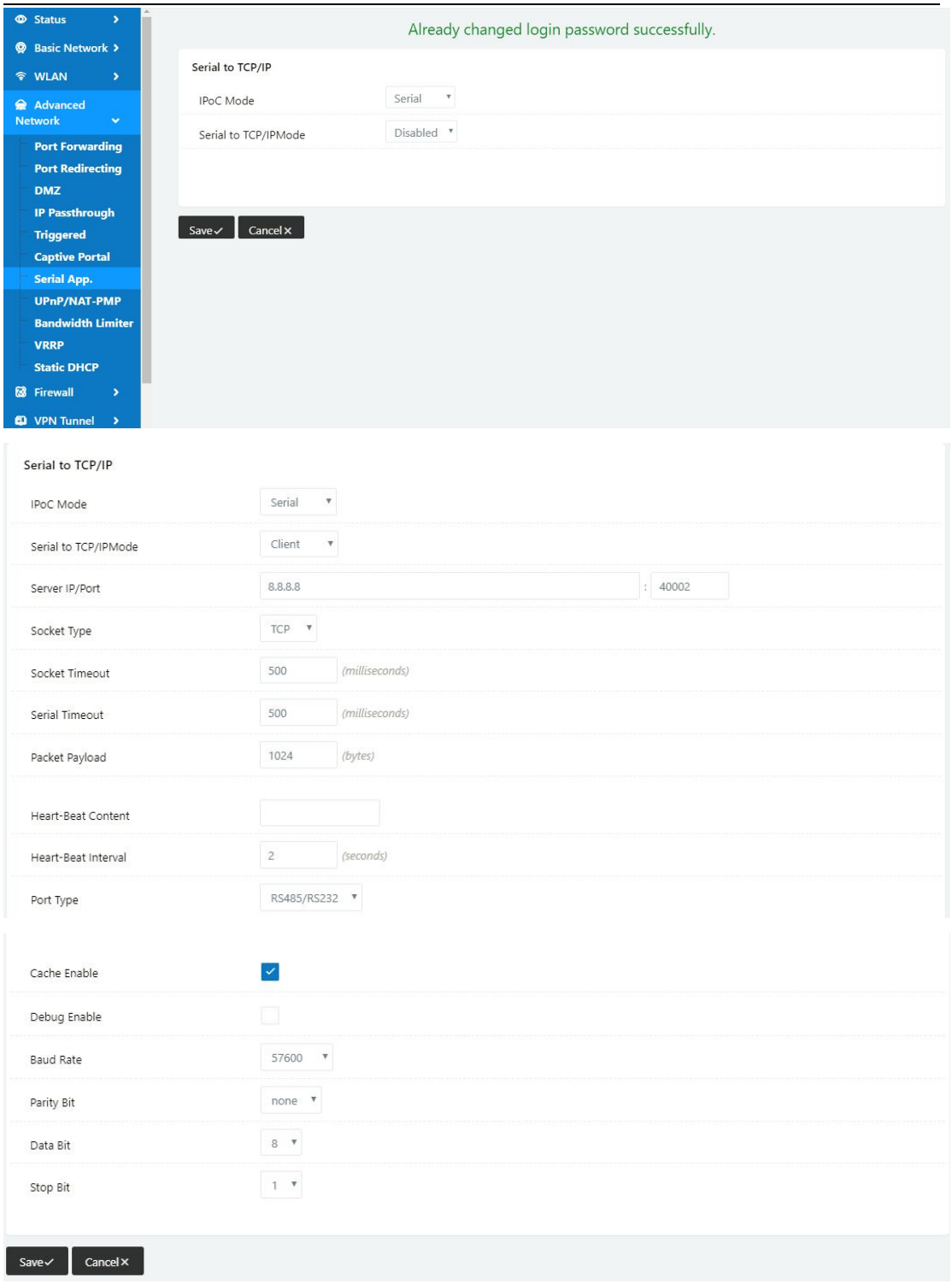


Table 2-15 Serial App Instruction

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

Parameter	Instruction
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

Serial port connection

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

Step 2 Please click "save" to finish.

----End

2.6.8 AT over IP Setting

Step 3 Advanced Network> AT over IP to check or modify the relevant parameter.

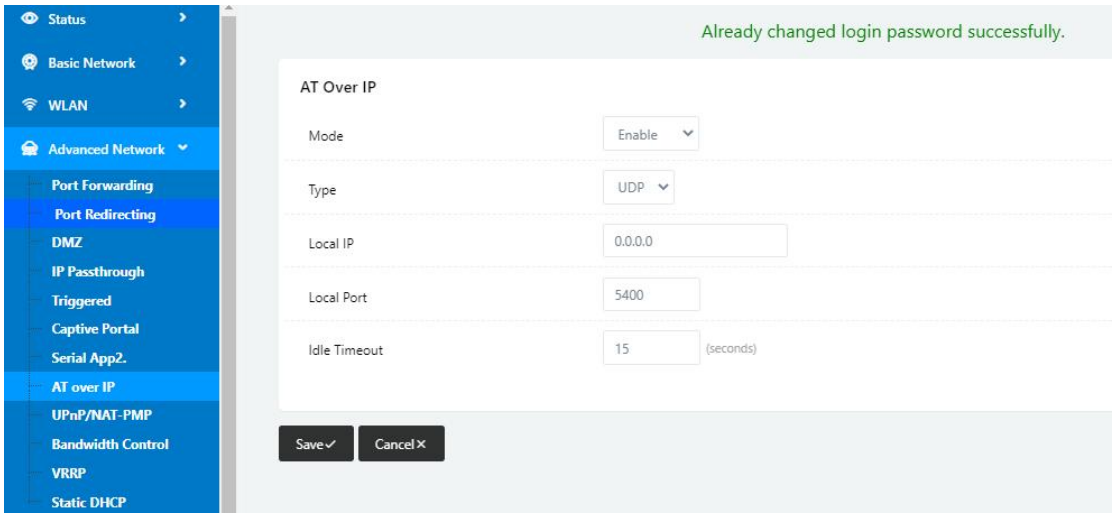


Table 2-16 AT over IP Instruction

Parameter	Instruction
Mode	Disable/Enable optional. Disable as default.
Type	UPD/TCP optional.
Local IP	Input the router local IP address. The feature will act as server mode.
Local Port	Input router local IP and port.
Idle Timeout	The connection will be released after the idle time.

NOTE

Input AT command after connected successfully. The router will reply AT command from 4G/3G modem.

----End

2.6.9 GPS Setting

Step 4 Advanced Network> GPS to check or modify the relevant parameter.

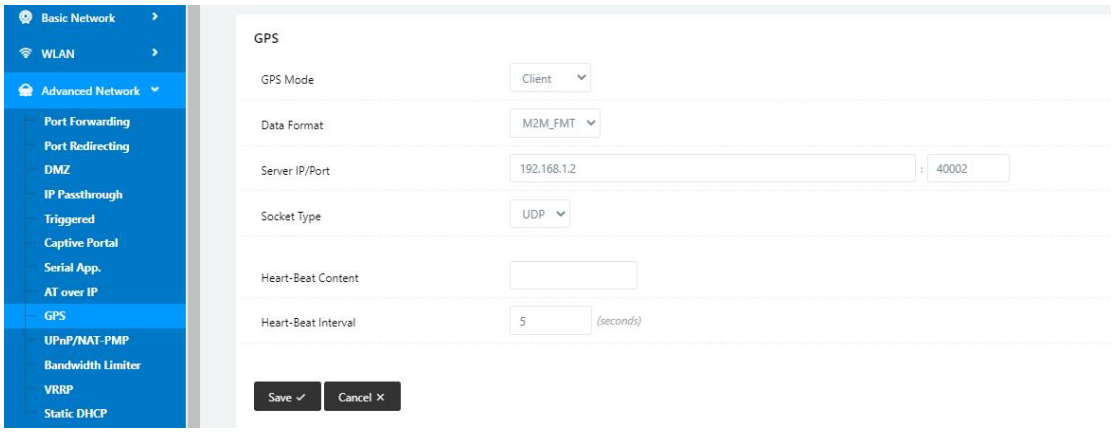


Table 2-17 AT over IP Instruction

Parameter	Instruction
Mode	Disable/Client/Server optional. Disable as default.
Data Format	NMEA/M2M_FMT optional. MNEA data format for standard GPS(GNSS) data. M2M_FMAT data format for simple GPS data in order to save data traffic.
Server IP/Port	IP address and domain name are acceptable for Server IP.
Socket Type	UDP/TCP optional
Heart-Beat Content	The router will send heart-beat to server when configured M2M_FMT Data Format.
Heart-Beat Interval	Heart-beat interval

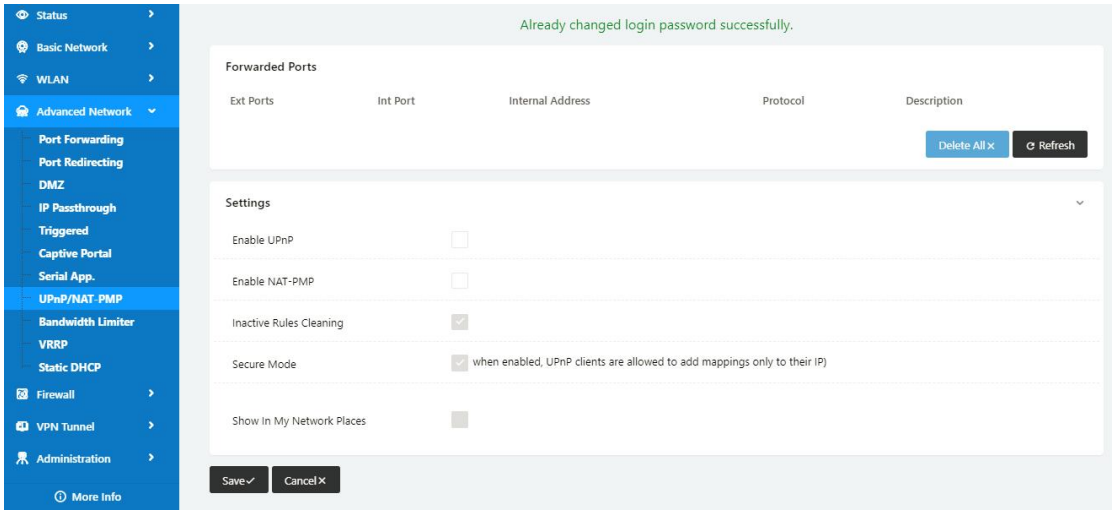
NOTE

The M2M_FMT format will be in the configuration instance.

----End

2.6.10 UPnp/NAT-PMP Setting

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



Step 2 Please click ”save” to finish.

----End

2.6.11 Bandwidth Control Setting

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

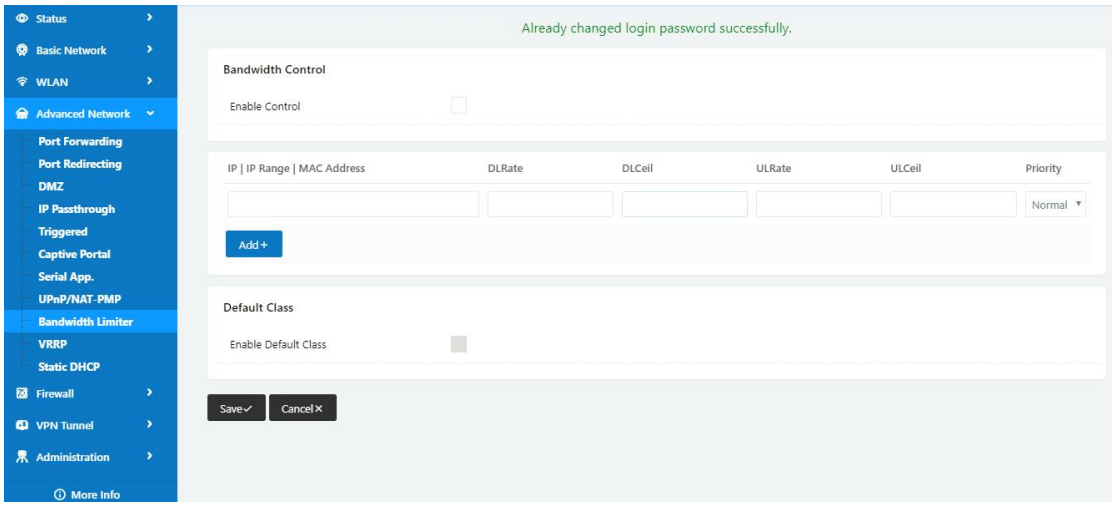


Table 2-18 Bandwidth Control Instruction

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

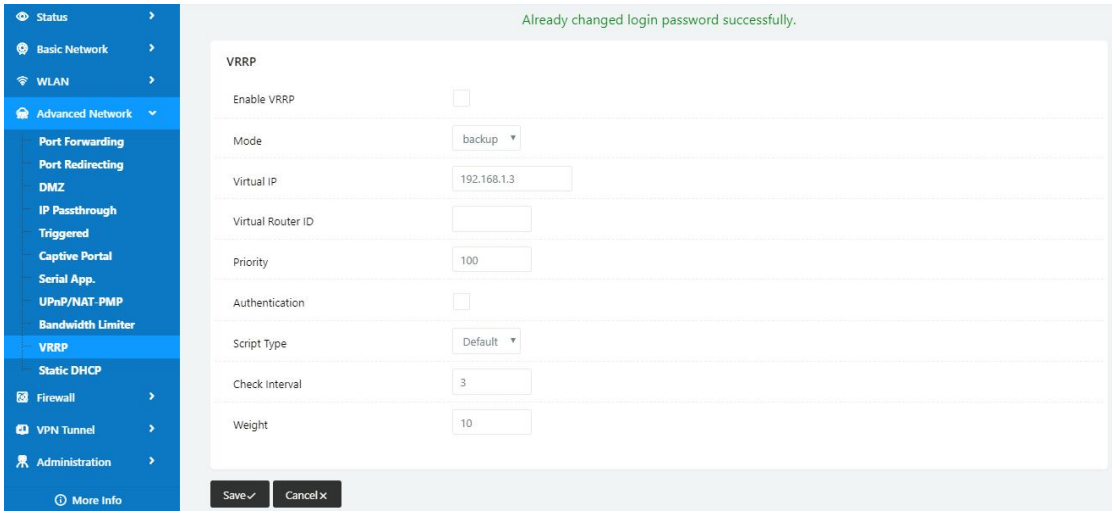
	total speed for all of device.

Step 2 Please click ”save” to finish.

----End

2.6.12 VRRP Setting

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



Parameter	Instruction
Mode	Backup / Master
Virtual IP	Virtual IP for VRRP function, master and backup routers need to be set to the same
Virtual Router ID	Virtual IP for VRRP function, master and backup routers need to be set to the same
Priority	Priority for VRRP function, the master router should be higher than the backup router, e.g. configure the master router to 100 and the backup router to 99
Authentication	Master and backup routers need to be configured the same
Script Type	Default: No network detection ICMP: ICMP detection for network connection
IP Address	Destination IP address for ICMP detection
Check Interval	ICMP interval, seconds
Weight	ICMP times

Step 2 Please click ”save” to finish.

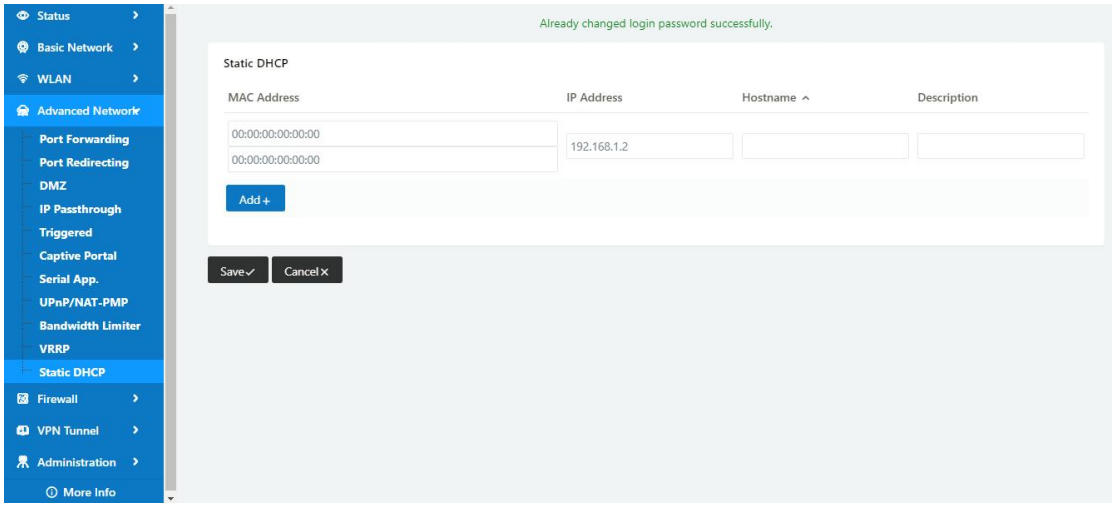
Configuration Instance

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

----End

2.6.13 Static DHCP Setting

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



Parameter	Instruction
MAC Address	6-byte, 48-bit format
IP Address	The router will assign the LAN IP to the corresponding MAC address
Hostname	Custom fillable
Description	Custom fillable

Application:

Configure a computer's WIFI Ethernet & RJ45 cable Ethernet MAC address here, and the IP address 192.168.1.2, then every time this computer is connected to the router, the router will only assign the LAN IP 192.168.1.2 to this computer

Step 2 Please click ”save” to finish.

----End

2.7 Firewall

2.7.1 IP/URL Filtering

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

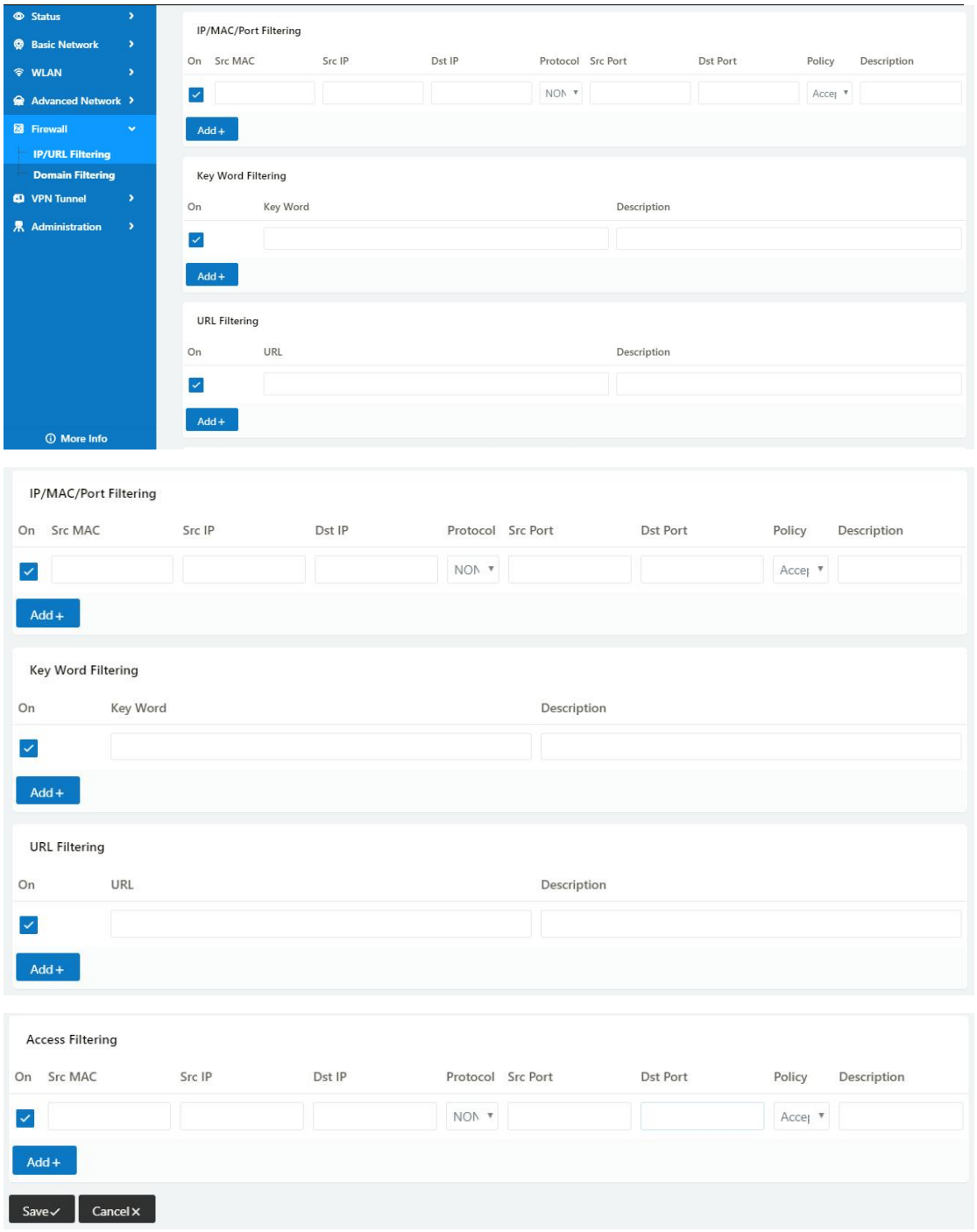


Table 2-19 IP/URL Filtering Instruction

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

Step 2 Please click ”save” to finish.

---End

2.7.2 Domain Filtering

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

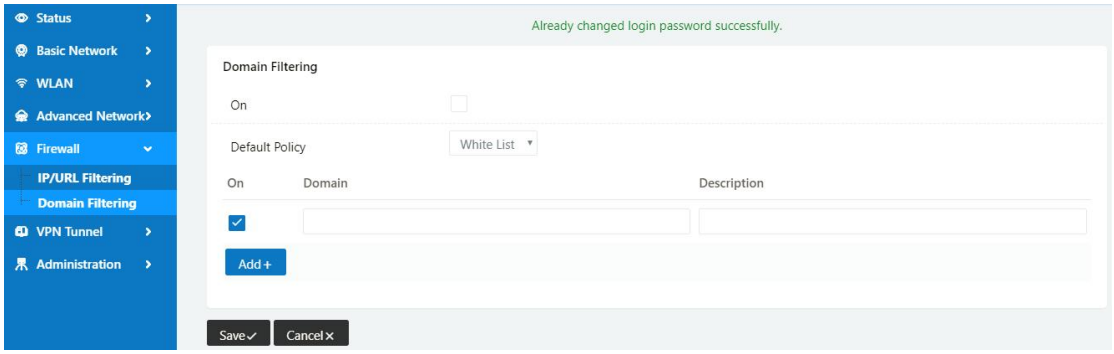


Table 2-20 Domain Filtering Instruction

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

Step 2 Please click ”save” to finish.

----End

2.8 VPN Tunnel

2.8.1 GRE Setting

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

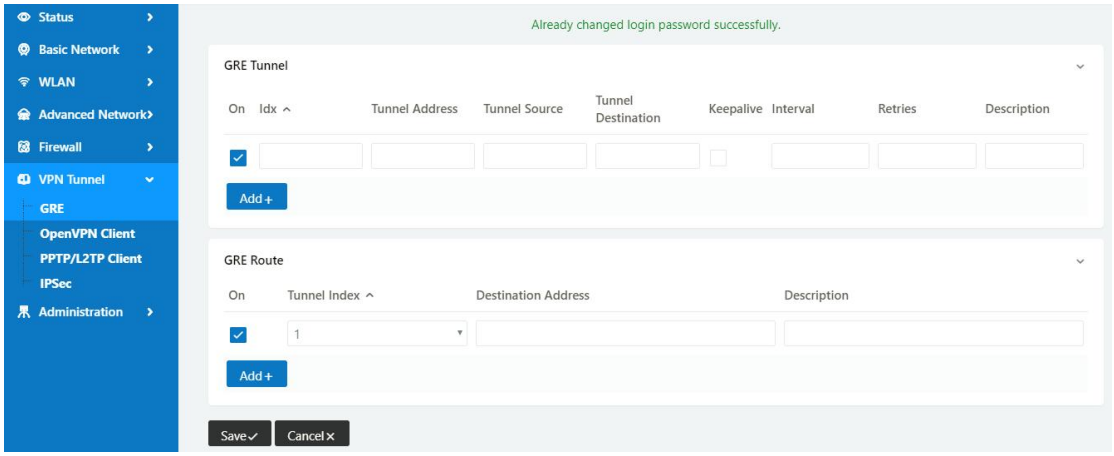


Table 2-21 GRE Instruction

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.

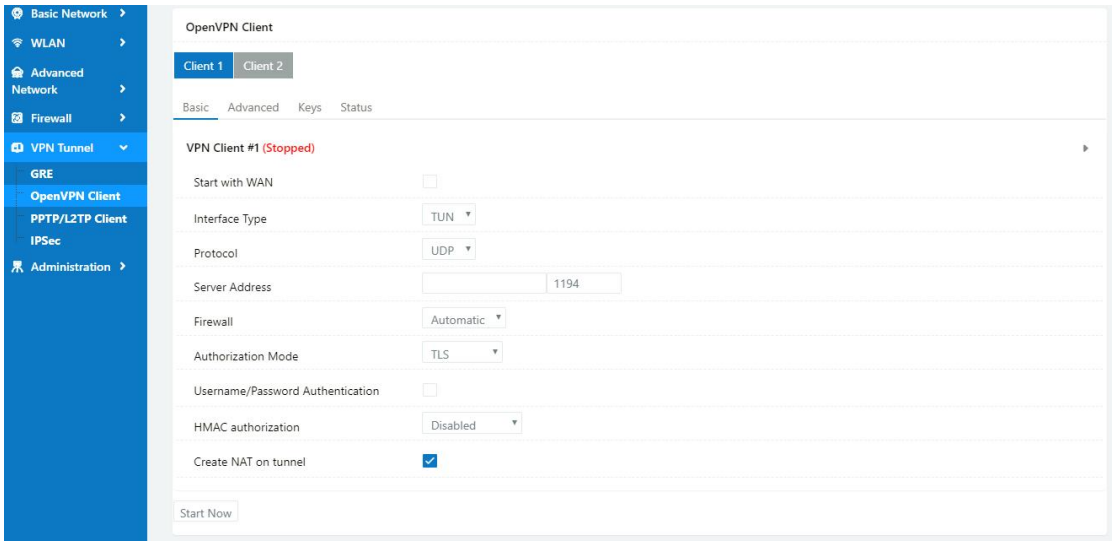
Configuration Instance

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

----End

2.8.2 OpenVPN Client Setting

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



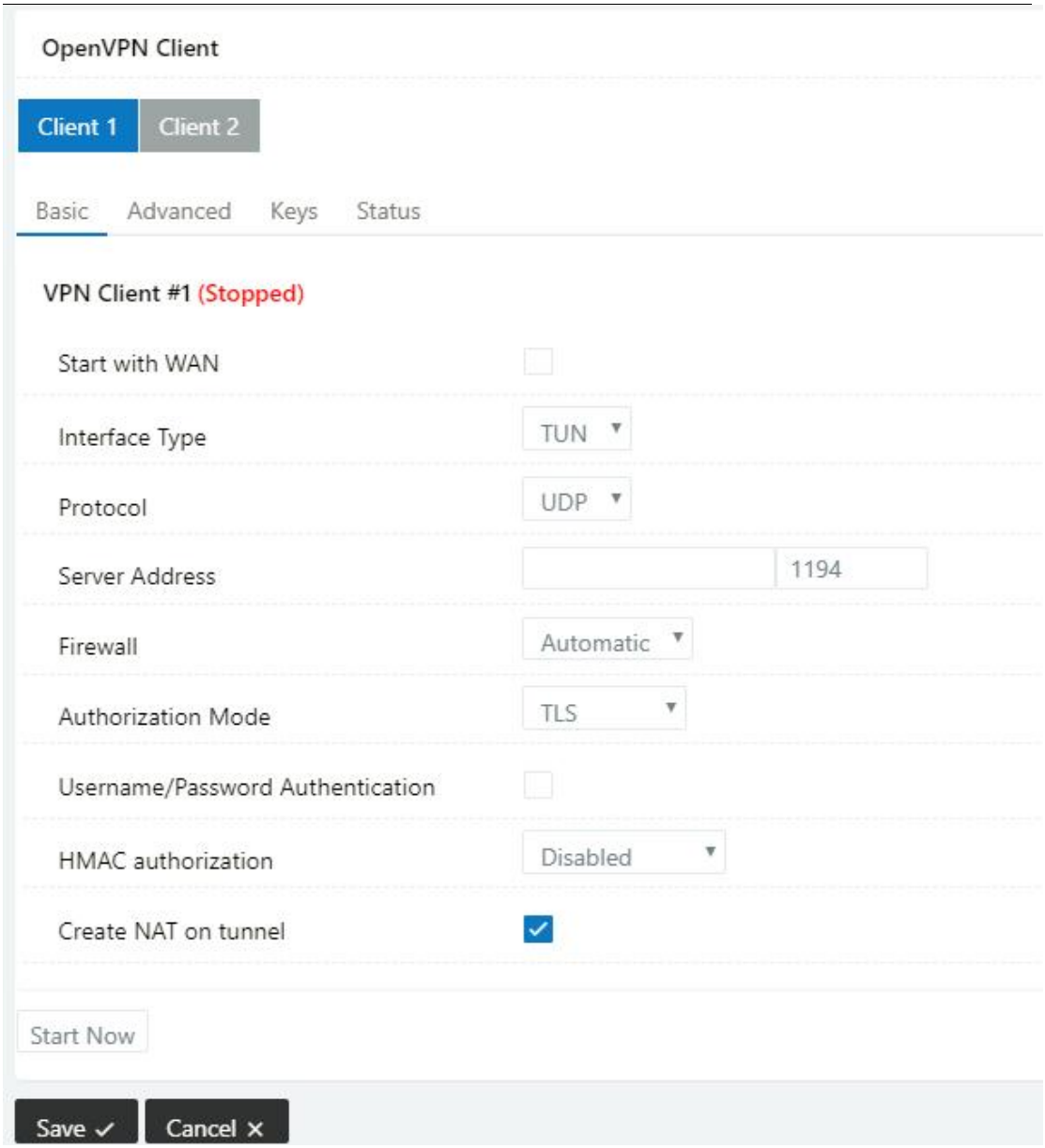


Table 2-22 Basic of OpenVPN Instruction

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.

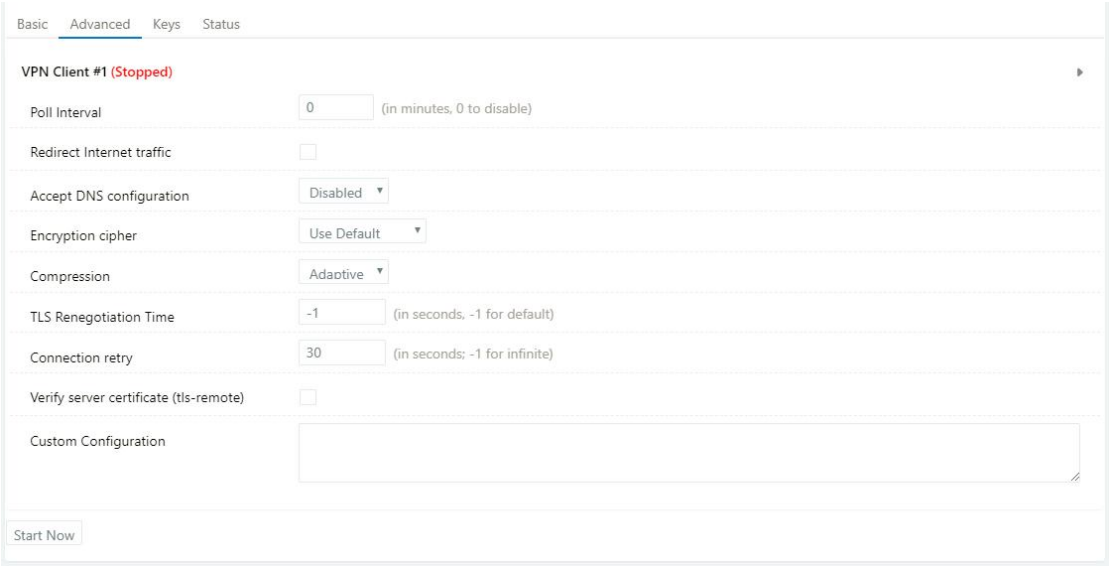


Table 2-23 Advanced of OpenVPN Instruction

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.

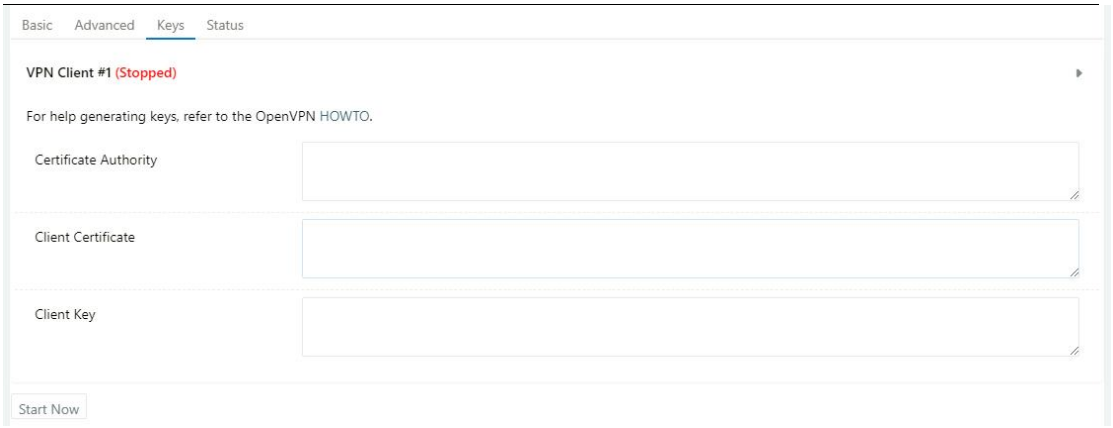


Table 2-24 Keys of OpenVPN Instruction

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

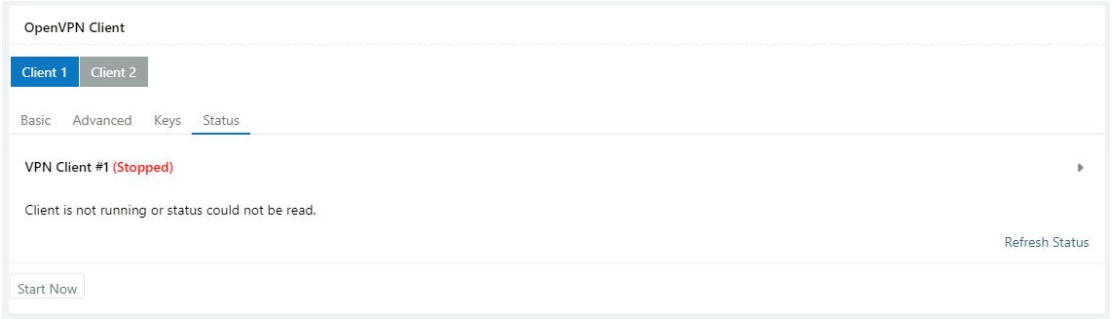


Table 2-25 Status of OpenVPN Instruction

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

2.8.3 PPTP/L2TP Client Setting

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

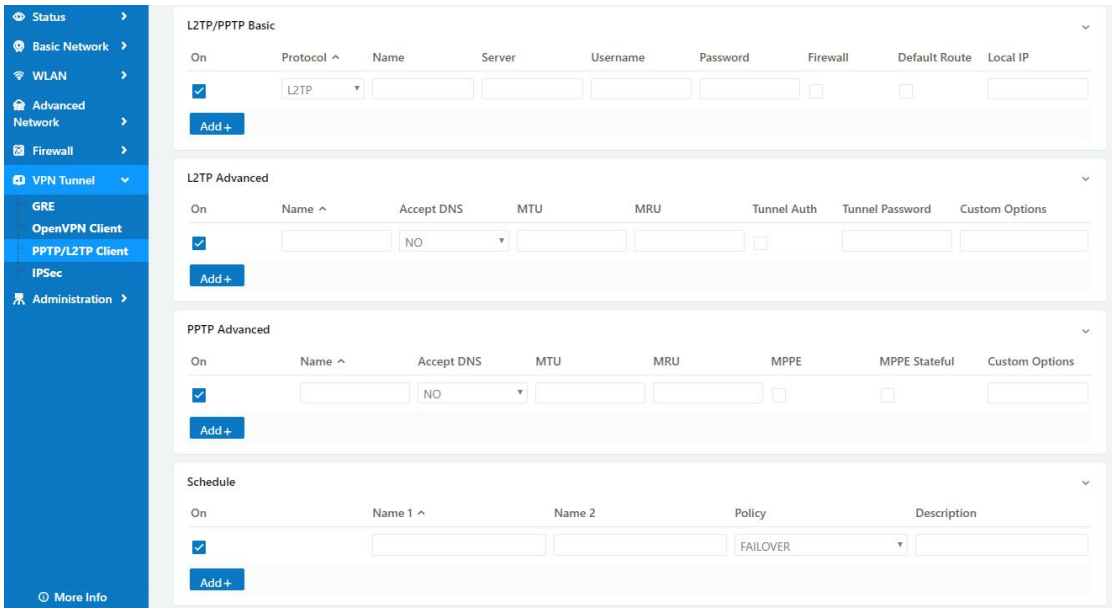


Table 2-26 PPTP/L2TP Basic Instruction

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 2-27 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	As the configuration requested.

Password	
Custom Options	As the configuration requested.

Table 2-28 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 2-29 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

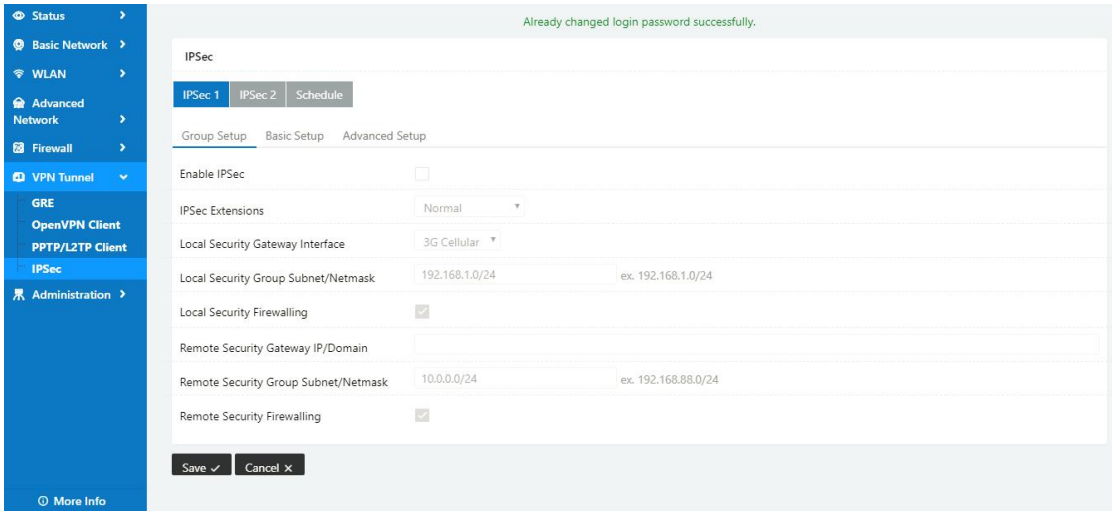
Step 2 Please click ”save” to finish.

Configuration Instance

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

---End

2.8.4 IPSec Setting



2.8.4.1 IPSec Group Setup

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

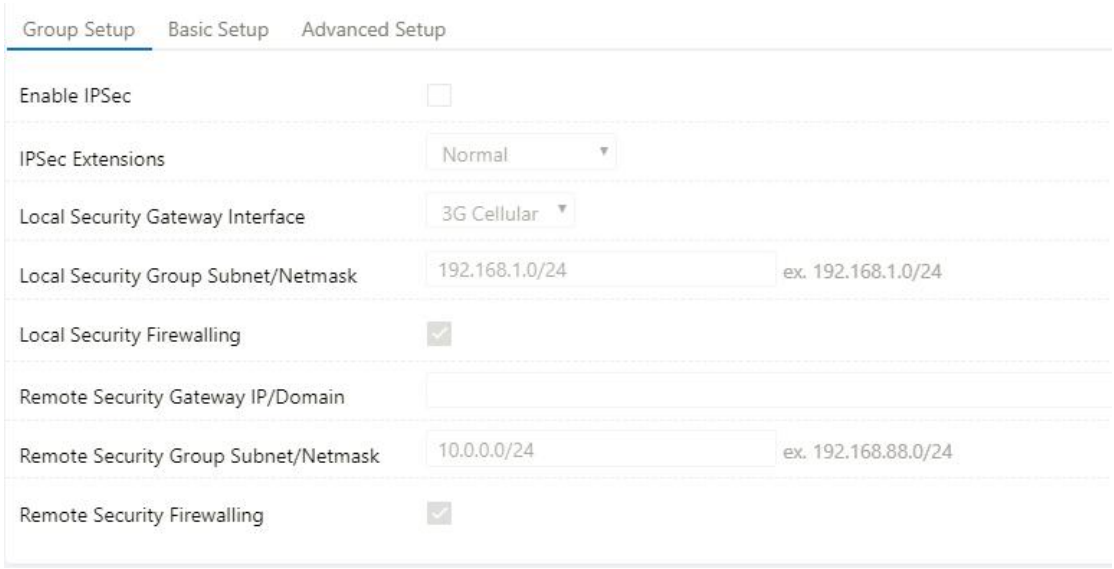


Table 2-30 IPSec Group Setup Instruction

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.

2.8.4.2 IPSec Basic Setup

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

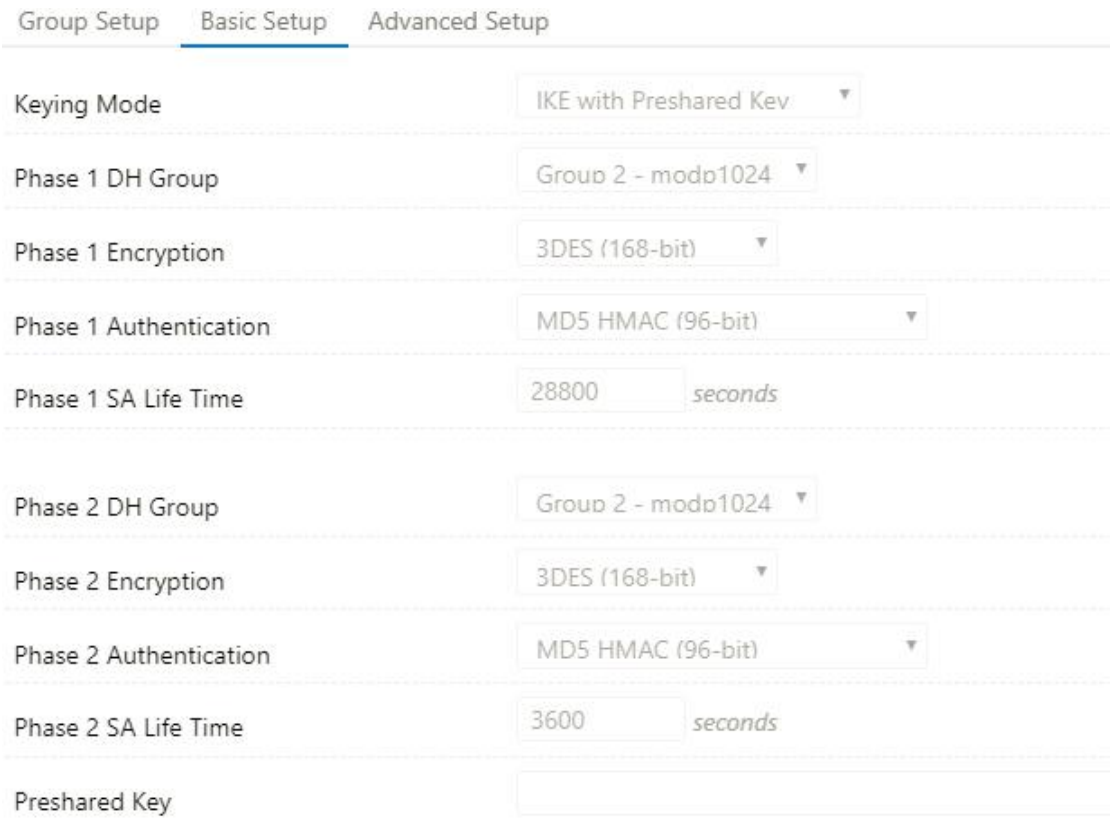


Table 2-31 IPSec Basic Setup Instruction

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.

2.8.4.3 IPSec Advanced Setup

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

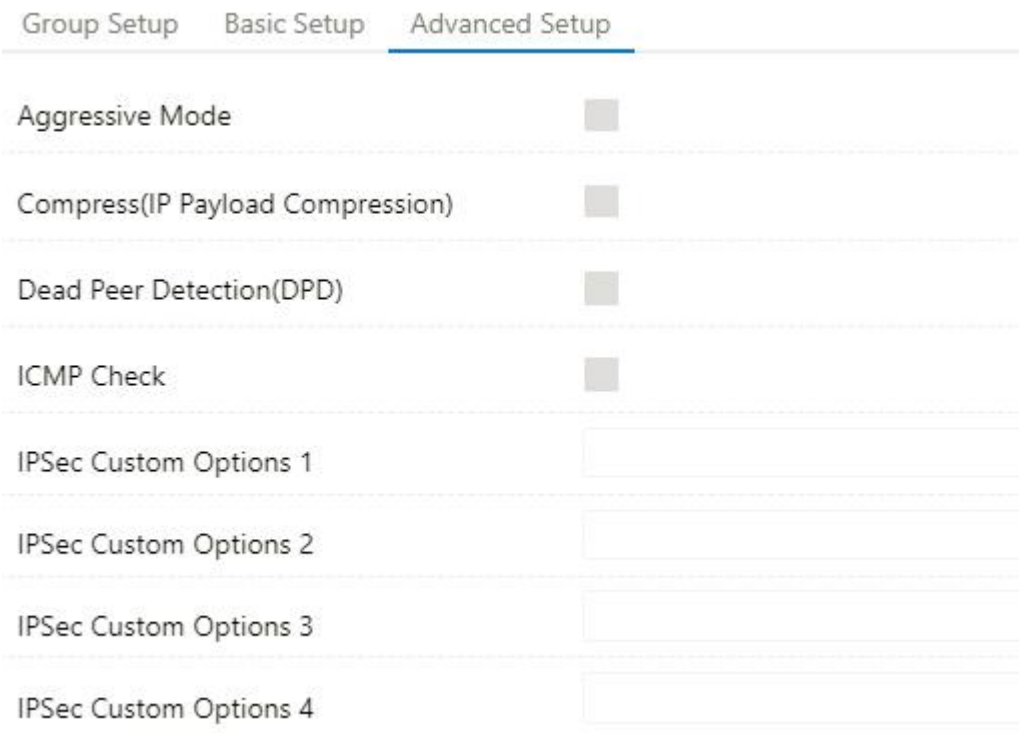


Table 2-32 IPSec Advanced Setup Instruction

parameter	Instruction
Aggressive Mode	Default for main mode

parameter	Instruction
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.

2.8.4.4 IPSec Schedule

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

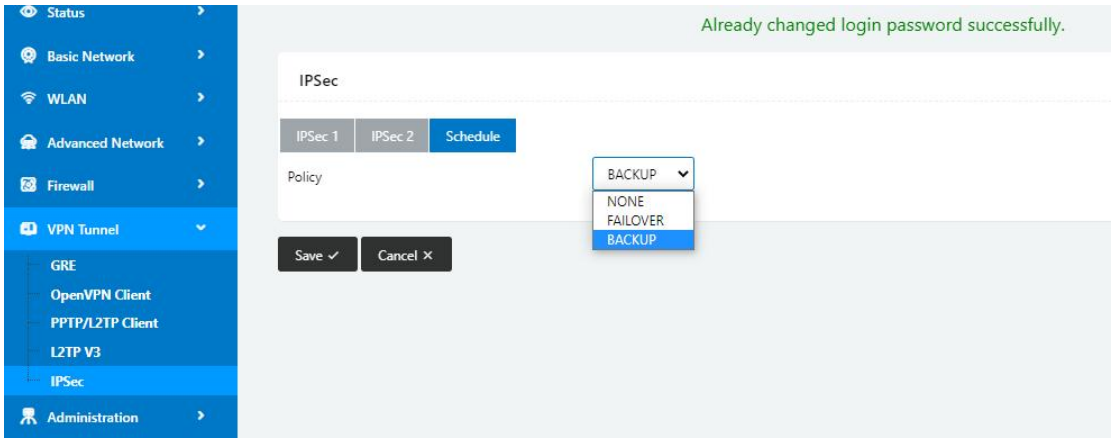


Table 2-33 IPSec Schedule Instruction

parameter	Instruction
Policy	NONE, FAILOVER and BACKUP
FAILOVER	IPSec1 tunnel and IPSec2 tunnel for failover mode. Once IPsec1 tunnel is down, the router will work on IPSec tunnel2.
BACKUP	IPSec1 tunnel and IPSec2 tunnel for backup mode. Once IPsec1 tunnel is down, the router will work on IPSec tunnel2.Once IPsec1 tunnel is up, router will work back to IPSec1 tunnel.

Configuration Instance

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

----End

2.9 Administration

2.9.1 Identification Setting

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

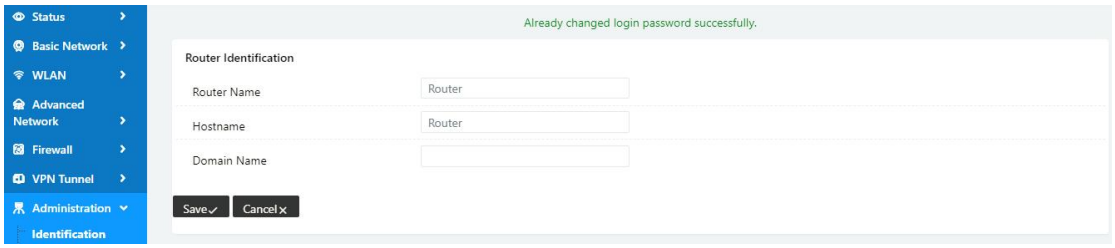


Table 2-34 Router Identification Instruction

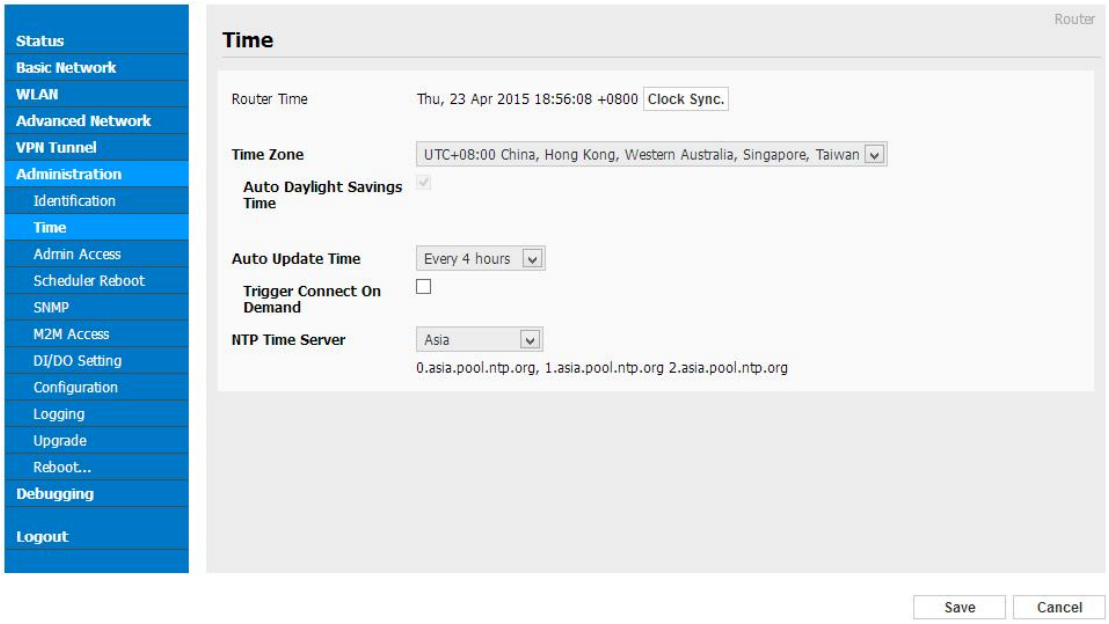
Parameter	Instruction
Router name	Default is router, can be set maximum 32 character
Host name	Default is router, can be set maximum 32 character
Domain name	Default is empty, support maximum up to 32 character, it is the domain of WAN, no need to configure for most application.

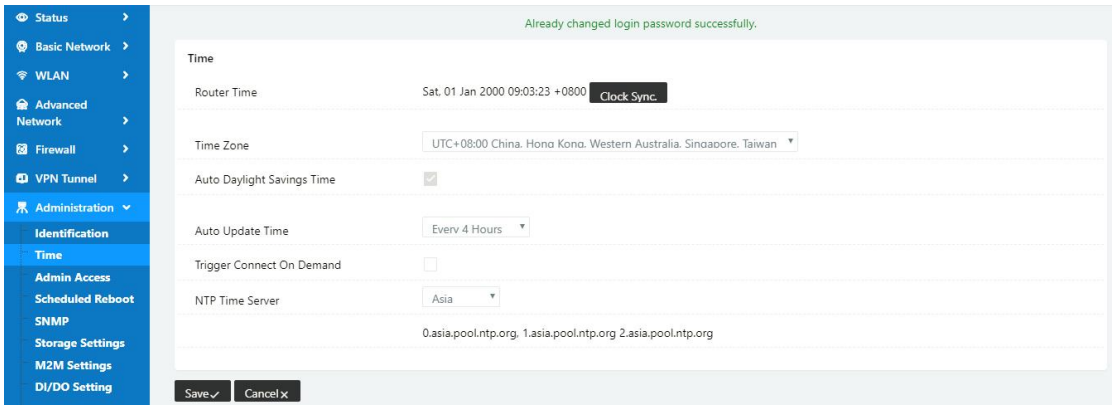
Step 2 Please click ”save” to finish

----End

2.9.2 Time Setting

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





Parameter	Instruction
Router time	The current system time of the router
Time Zone	Configurable time zones
Auto Daylight Savings Time	Automatic synchronisation for countries or regions with daylight saving time
Auto Update Time	Intervals when checking automatically through the network
Trigger Connect On Demand	Time synchronisation on demand
NTP Time Server	Configure the router to perform system timing via a designated NTP server

CAUTION

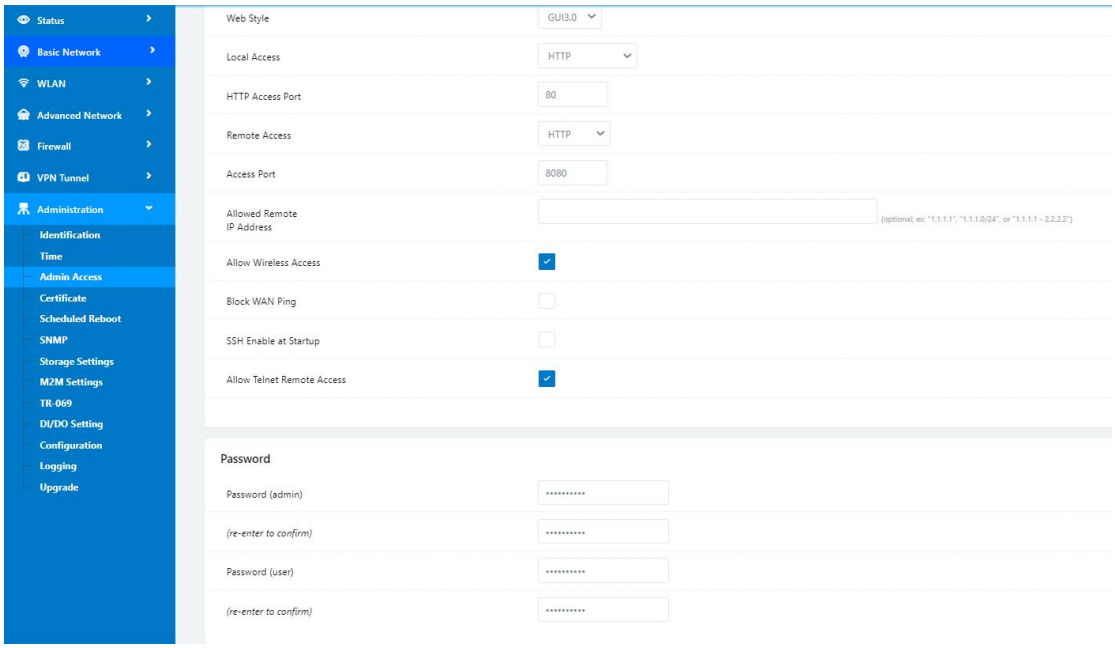
If the device is online but time update is fail, please try other NTP Time Server.

Step 2 Please click “save to finish.

----End

2.9.3 Admin Access Setting

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



Parameter	Instruction
Web Style	GUI2.0/GUI3.0
Local Access	Disabled/HTTP/HTTPS/HTTP&HTTPS, configure the type of protocol that the router GUI can be accessed by the LAN
HTTP Access Port	Configure the port on which the router GUI can be accessed by the LAN via HTTP
Remote Access	Disabled/HTTP/HTTPS, configure the type of protocol that the router GUI can be accessed by the external network
Access Port	Configure the port on which the router GUI can be accessed by the external network
Allowed Remote IP address	Whitelist IPs that allow external network access to the router GUI, with multiple IPs separated by commas
Allow Wireless Access	Whether to allow other devices to access the router GUI via WiFi
Block WAN Ping	Whether to allow the router's WAN IP address to be ping tested by an external network
SSH Enabled at Startup	Enable/Disable the SSH
Allow Telnet Remote Access	Enable/Disable external network telnet to the router
Password(admin)	The password for administrator
Password(user)	The password for guest

Step 2 Please click save iron to finish the setting

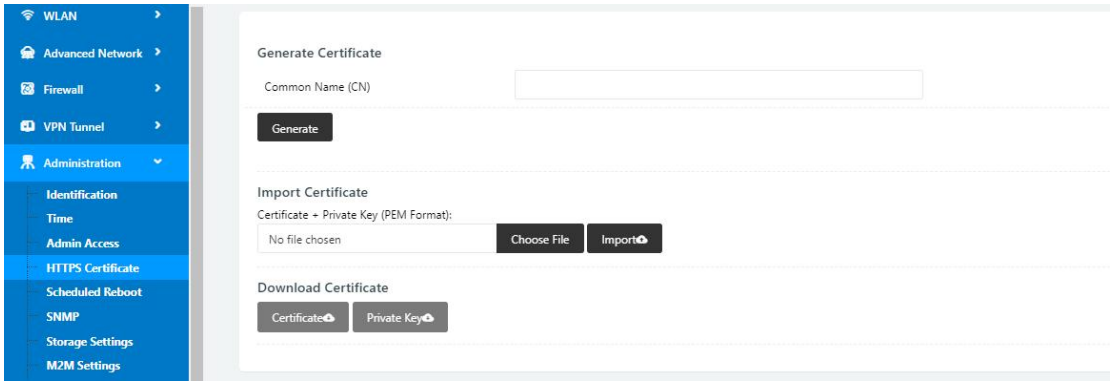
NOTE

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

----End

2.9.4 HTTPs Certificate Setting

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



Parameter	Instruction
Common Name (CN)	SSL certificate domain name
Import Certificate	Import certificate.
Download Certificate	Download certificate key and private key.

Step 2 Please click save iron to finish the setting

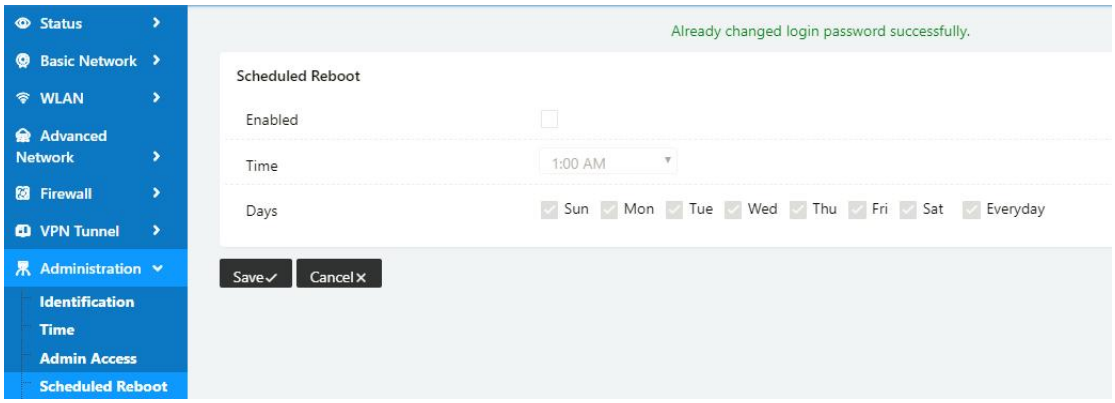
NOTE

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

----End

2.9.5 Schedule Reboot Setting

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



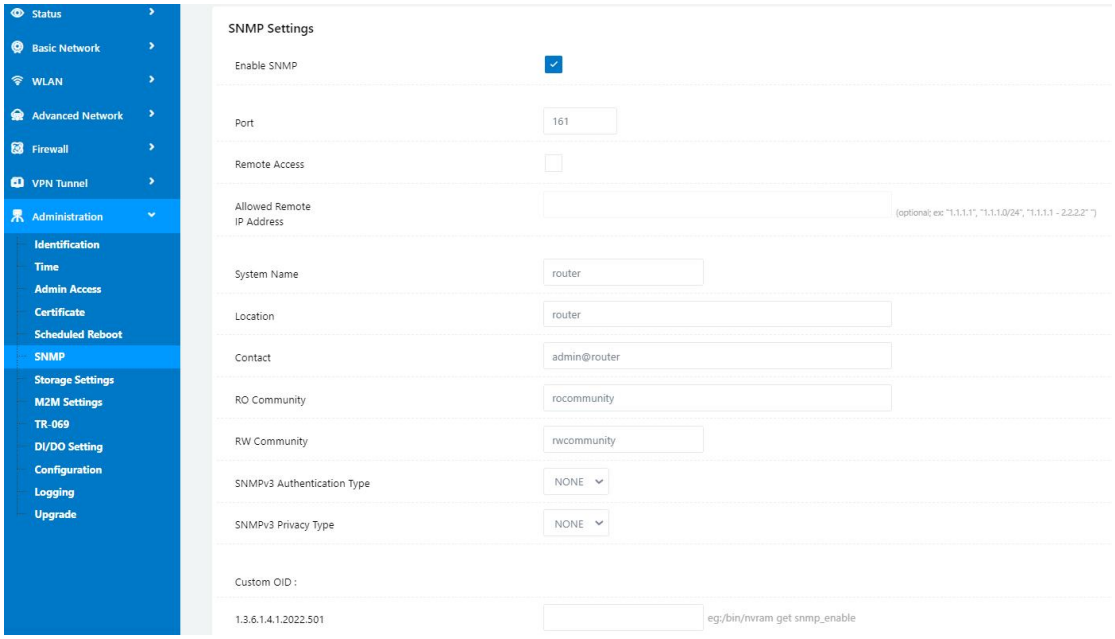
Parameter	Instruction
Enabled	Enabled/Disable
Time	Select the timed reboot point
Days	Configure the router need to reboot regularly every day or a few days a week

Step 2 Please click save iron to finish the setting

----End

2.9.6 SNMP Setting

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



Parameter	Instruction
Enable SNMP	Enable/Disable
Port	The port for SNMP communication, 161 by default

Parameter	Instruction
Remote Access	Whitelist IPs that allow external network access to the router GUI, with multiple IPs separated by commas
System Name	The system name of router in SNMP
Location	The location of router in SNMP
Contact	The contact of router in SNMP
RO community	The RO community of router in SNMP
RW community	The RW community of router in SNMP
SNMPv3 Authentication Type	NONE/MD5/SHA
SNMPv3 Privacy Type	NONE/DES/AES
Custom OID	Get router parameters by custom OID

Step 2 Please click save iron to finish the setting

----End

2.9.7 Storage Setting

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

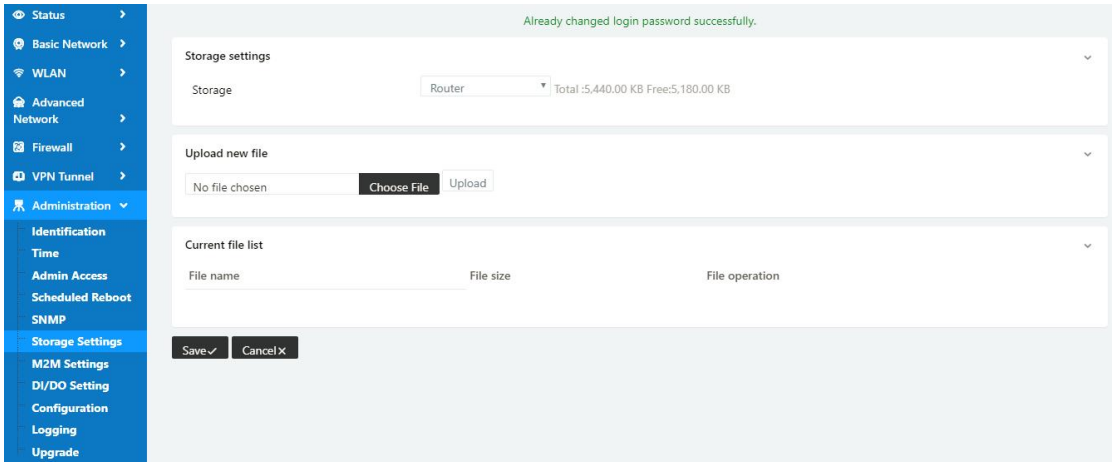


Table 2-35 Storage Instruction

Parameter	Instruction
Storage	Storage path for router and removable Device optional. The router as storage path, the volume will be Flash balance volume. The removable devices as storage path, the volume will be 16GB/32GB/128GB optional as order requested.

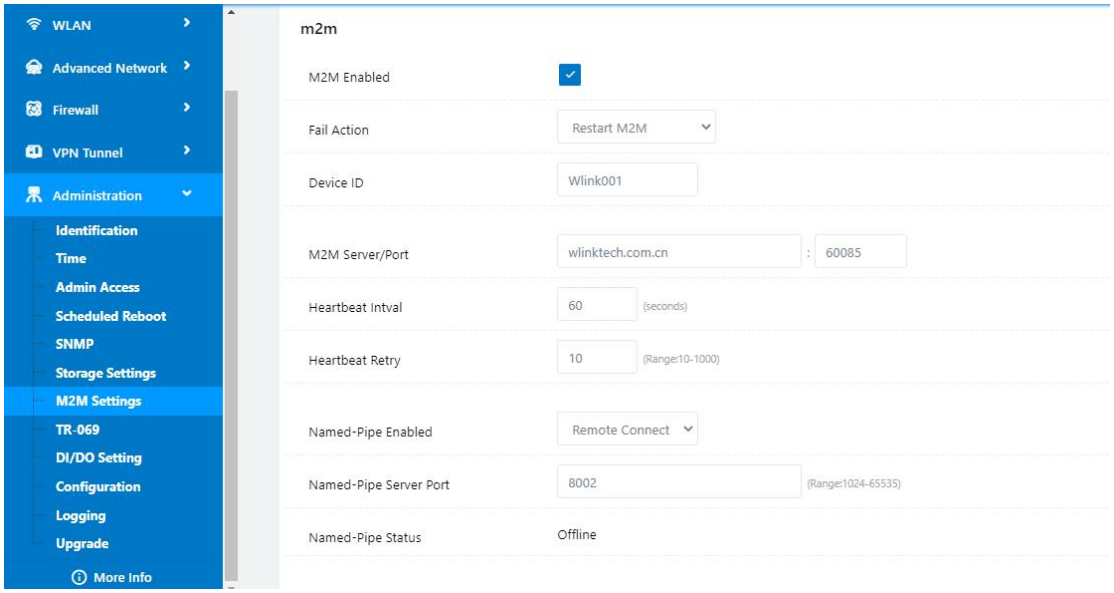
Parameter	Instruction
Upload new file	The feature is suitable for captive portal files and
Current file list	List the uploaded file in the router storage.

Step 2 Please click save iron to finish the setting

----End

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

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



Parameter	Instruction
Fail Action	Restart M2M / Reconnect network / Reboot System Actions to be performed by the router when the router fails to connect to the M2M platform
Device ID	The Device ID show on the M2M platform
M2M Server/Port	Configure the address and port for router connect to a M2M platform
Heartbeat Interval	Time interval for the router to report data to the M2M
Heartbeat Retry	Time for the next packet to reconnect to the M2M after a heartbeat packet has failed to be reported to the M2M
Named-Pipe Enabled	Remote Connect / Auto Connect type of peer-to-peer connection between the router and the M2M
Named-Pipe	The peer-to-peer connection port of M2M server

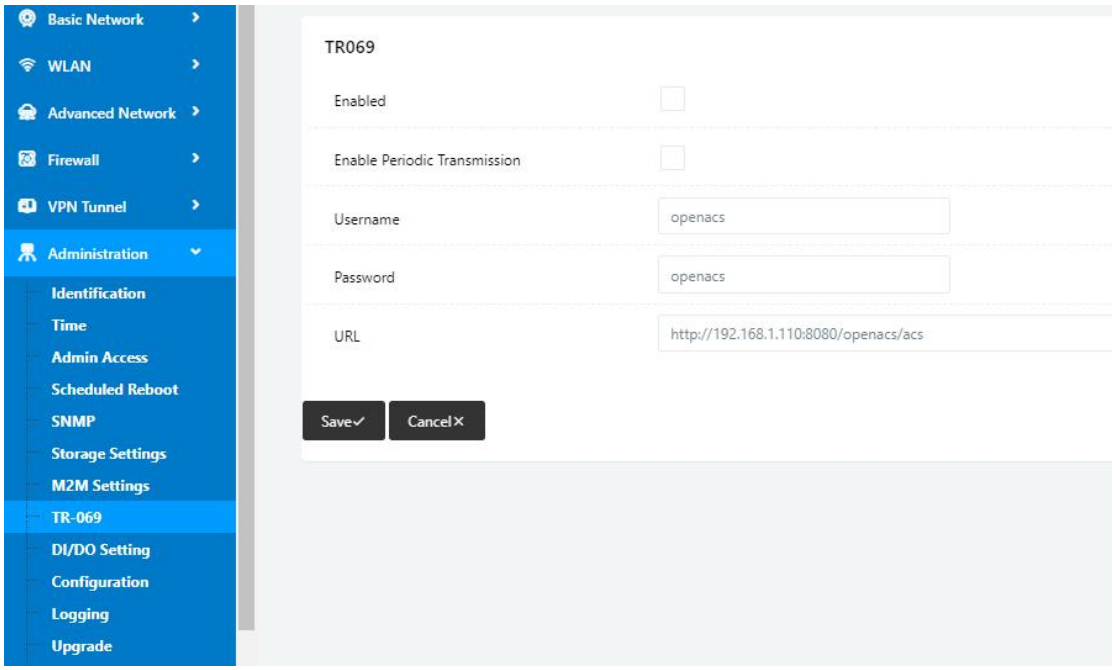
Parameter	Instruction
Server Port	
Named-Pipe Status	Offline/Online
Named-Pipe Address	After a successful connection between the peer-to-peer and the M2M server, the router will get a virtual address

Step 2 Please click save iron to finish the setting

----End

2.9.9 TR-069 Setting

Step 1 Please click “Administrator>TR-069 Setting” to check and modify relevant parameter.



Parameter	Instruction
Enabled	Enabled/Disabled
Enable Periodic Transmission	When enabled, the router will continuously sending data to the server
Sending Interval	The time interval, in seconds, for sending data continuously to the server
Username	Username used to log in to the TR069 server
Password	Password used to log in to the TR069 server

Parameter	Instruction
URL	Address of the TR069 server

Step 2 Please click save iron to finish the setting

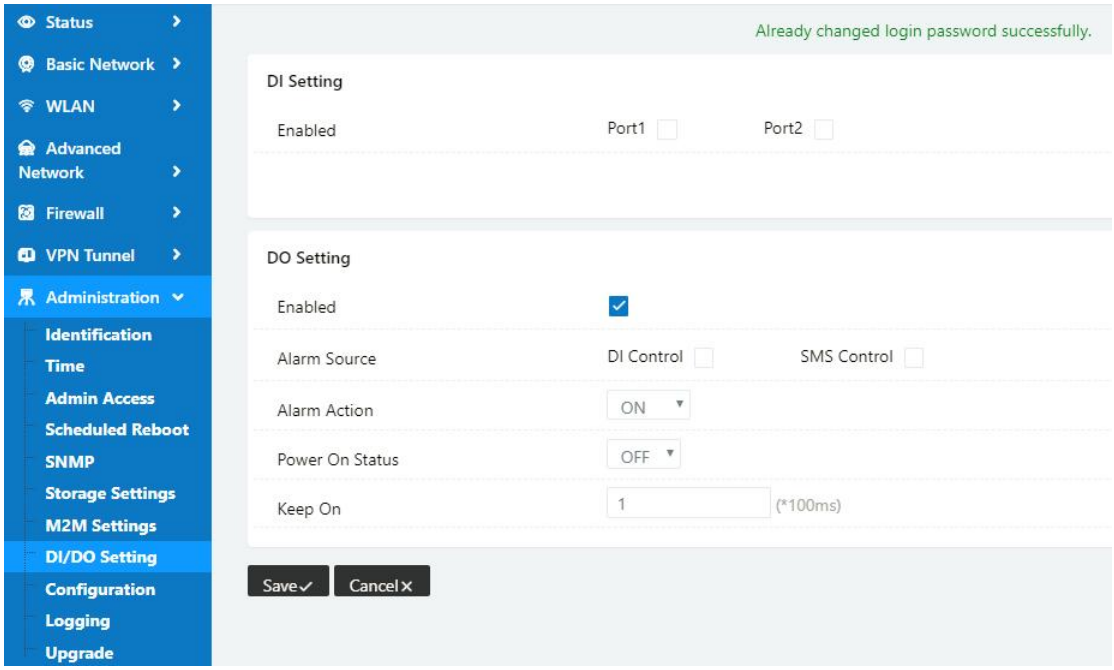
Configuration Instance

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

----End

2.1.1 DI/DO Setting

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



2.9.7.1 DI Configure

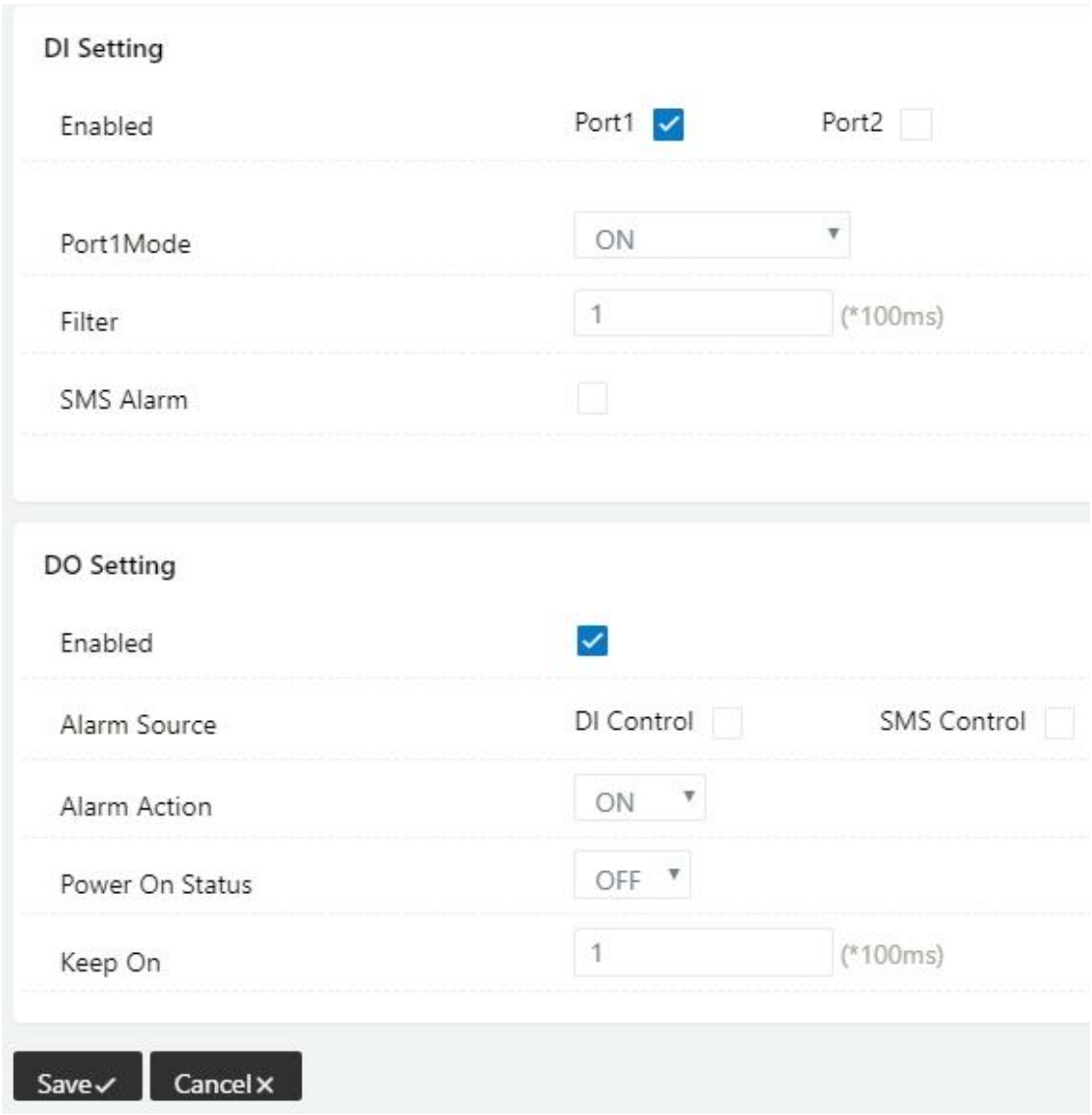


Table 2-36 DI Instruction

Parameter	Instruction
Enable	Enable DI. Port1 is for I/O1 and Port2 is I/O2. Both I/O1 and I/O2 are DI ports
Mode	Selected from OFF, ON and EVENT_COUNTER modes. OFF Mode: DI from high level(3.3v~5V) to low level(0V), it will trigger alarm. ON Mode: DI from low level(0V) to high level(3.3v~5V), it will trigger alarm. EVENT_COUNTER Model: Enter EVENT_COUNTER mode.
Filter	Software filtering is used to control switch bounces. Input (1~100)*100ms. Under OFF and ON modes, WL-G510 detects pulse signal and compares with first pulse shape and last pulse shape. If both are the same level, WL-G510 will trigger alarm.

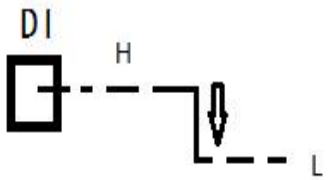
Parameter	Instruction
	Under EVENT_COUNTER mode, if first pulse shape and last pulse shape are not the same level, WL-G510 will trigger alarm according to Counter Action setting.
Counter Trigger	Available when DI under Event Counter mode Input from 0 to 100. (0=will not trigger alarm) It will trigger alarm when counter reaches this value. After triggering alarm, DI will keep counting but no trigger alarm again.
Counter Period	It's a reachable IP address. Once the ICMP check is failed, GRE will be established again.
Counter Recover	it will re-count after counter trigger alarm. The value is 0~30000(*100ms). 0 means no counter.
Counter Action	HI_TO_LO and LO_TO_HI is available when DI under Event Counter mode. In Event Counter mode, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When LO_TO_HI is selected, the counter value increase when the attached switch is pushed. When HI_TO_LO is selected, the counter value increases when the switch is pushed and released.
Counter Start	Available when DI under EVENT_COUNTER mode. Start counting when enable this feature.
SMS Alarm	The alarm SMS will send to specified phone group. Each phone group include up to 2 phone numbers.
SMS Content	70 ASCII Char Max
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 2 Please click "save" to finish.

NOTE

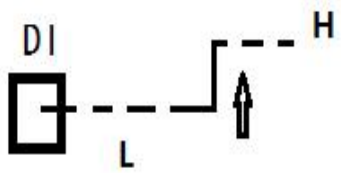
OFF Mode

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



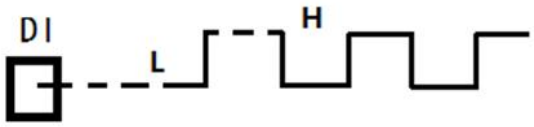
ON Mode

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



EVENT_COUNTER Model

The counted number of pulses will be triggered.



2.9.7.2 DO Configure

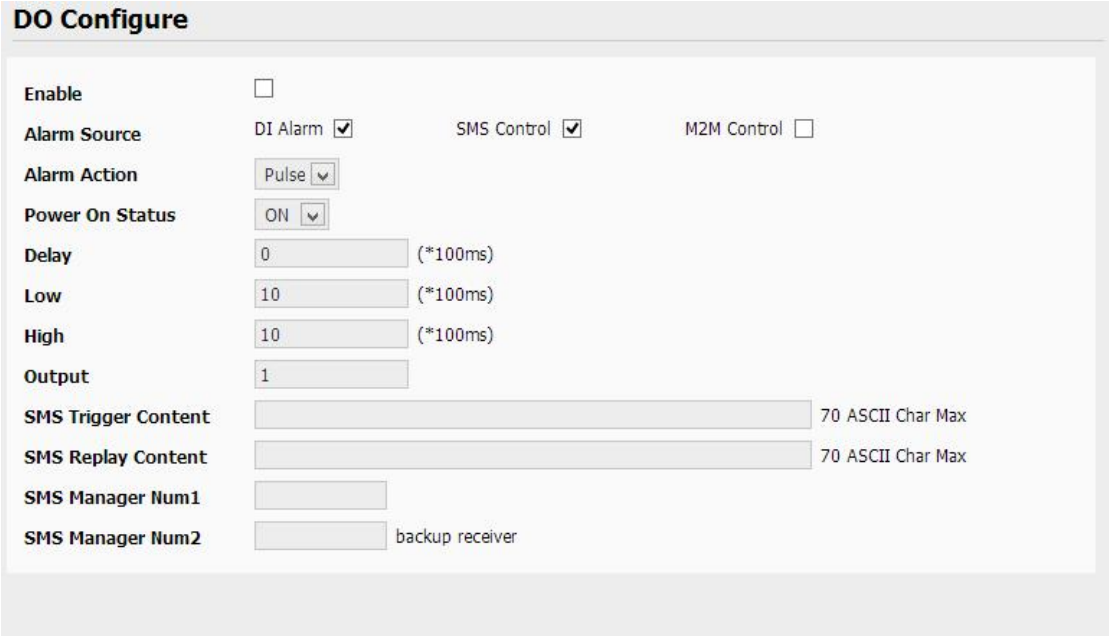


Table 2-37 DO Instruction

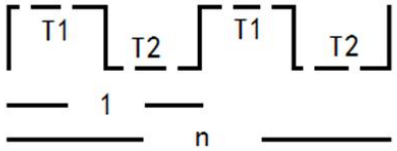
Parameter	Instruction
Enable	1 DO as selected
Alarm Source	Digital output initiates according to different alarm source. Select from DI Alarm, SMS Control and M2M Control. Selections can be one or more. DI Alarm: Digital Output triggers the related action when there is alarm from Digital Input.

Parameter	Instruction
	SMS Control: Digital Output triggers the related action when receiving SMS from the number in phone book. M2M Control: it's not ready.
Alarm Action	Digital Output initiates when there is an alarm. Selected from "OFF", "ON", "Pulse". OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.
Power on Status	Specify the digital Output status when power on. Selected from OFF and ON. OFF: how high(0V). ON: high lever(4.8-5.0V)
Keep On	Available when digital output Alarm On Action/Alarm Off Action status is ON, input the Digital Output keep on status time. Input from 0 to 255 seconds. (0=keep on until the next action)
Delay	Available when enable Pulse in Alarm On Action/Alarm Off Action. The first pulse will be generated after a "Delay". Input from 0 to 30000ms. (0=generate pulse without delay)
Low	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Input from 1 to 30000 ms.
High	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Input from 1 to 30000 ms.
Output	Available when enable Pulse in Alarm On Action/Alarm Off Action. The number of pulses, input from 0 to 30000. (0 for continuous pulse output)
SMS Trigger Content	Available when enable SMS Control in Alarm Source. Input the SMS content to enable "Alarm On Action" by SMS (70 ASIC II char max).
SMS Reply Content	Input the SMS content, which will be sent after DO was triggered. (70 ASIC II char max).
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 3 Please click "save" to finish.

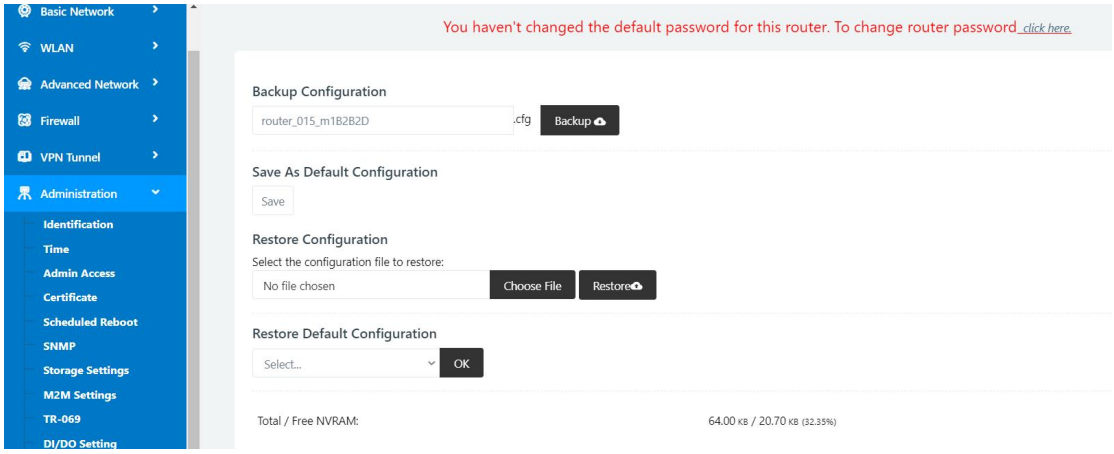
NOTE

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



2.1.2 Configuration Setting

Step 4 Please click “ Administrator> Configuration ” to do the backup setting



Parameter	Instruction
Backup Configuration	Click the Backup button to save a copy of the router's current configuration parameters
Save As Default Configuration	Save the current configuration as the router's default, even if the router is reset, it will revert to this configuration
Restore Configuration	Import a backup configuration file to modify the router's configuration parameters
Restore Default Configuration	Restore custom configuration: Restore to the custom configuration status Restore factory configuration: Clear all configuration parameters and restore the route to its factory status

Figure 3-1 Backup and Restore Configuration GUI

CAUTION

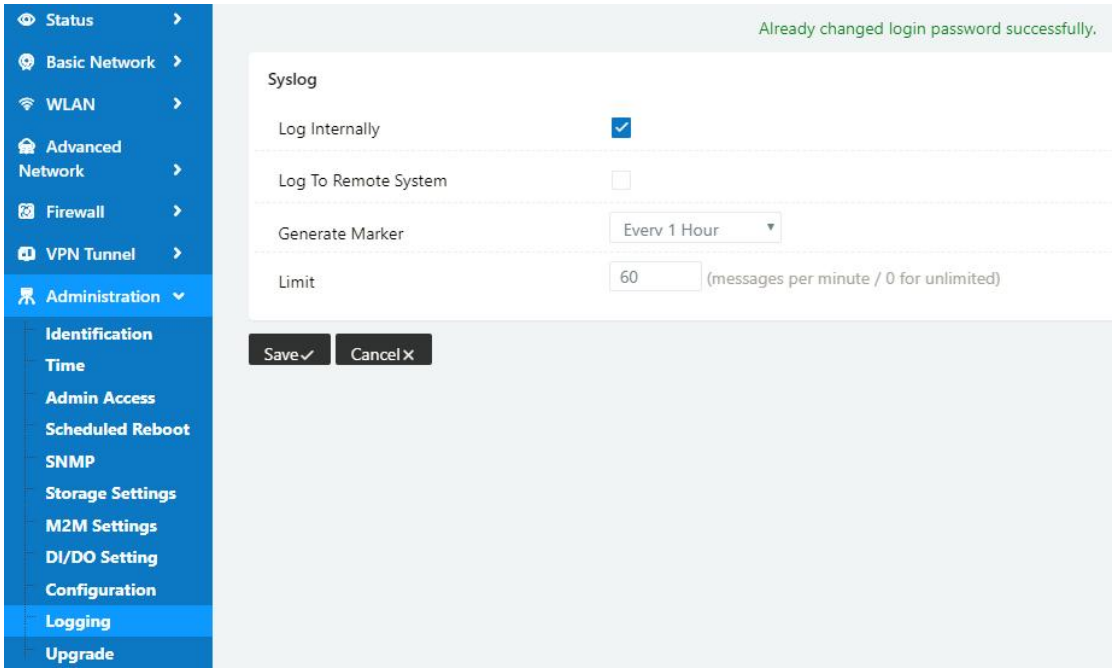
Restore Default would lose all configuration information, please be careful.

Step 5 After setting the backup and restore configuration. The system will reboot automatically.

----End

2.1.3 System Log Setting

Step 6 Please click “Administrator> Logging” to start the configuration, you can set the file path to save the log (Local or remote sever).



Parameter	Instruction
Log Internally	Enable the router to print log in Tools > Log
Log to Remote System	Enable the router to print log and send to a destination IP address
Host or IP Address / Port	Configure a destination IP and port for receive the router system log, for the log tool, please contact us
Generate Marker	The print interval of a log marker
Limit	The number of log messages the router can print per minute, set to 0 for no limit

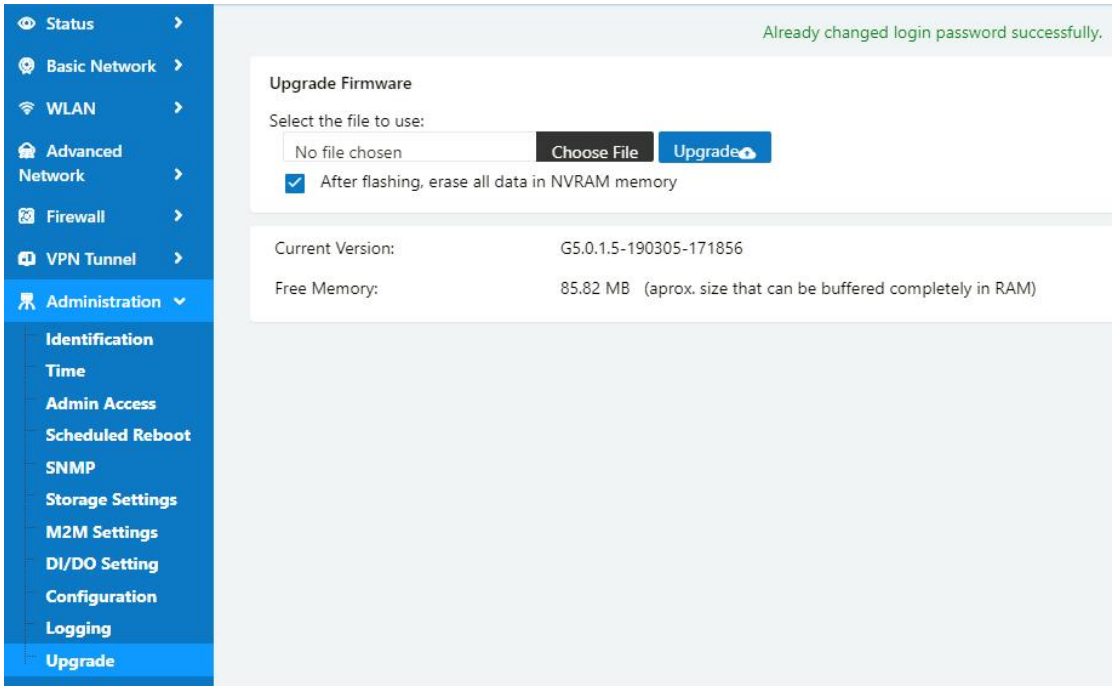
Figure 3-2 System log Setting GUI

Step 7 After configure, please click “Save” to finish.

----End

2.1.4 Firmware upgrade

Step 8 Please click “Administrator>firmware upgrade” to open upgrade firmware tab.



Parameter	Instruction
Upgrade Firmware	Select the firmware of the router you want to upgrade (please make sure the firmware is adapted to the current router before upgrading)
After flashing, erase all data in NVRAM memory	All configuration will be erased to default when clicked, Non-click will keep configuration after upgrade.
Current Version	Detailed version number of the current router firmware
Free Memory	Current space left in router RAM

Figure 3-3 Firmware Upgrade GUI

NOTE

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

2.2 “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-G510 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 2-38 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

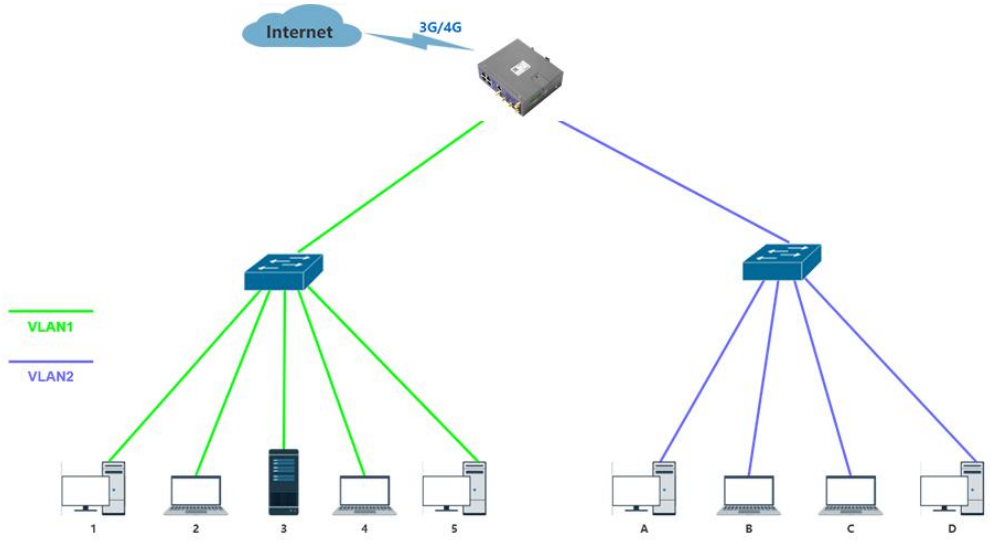
After reboot, the previous configuration would be deleted and restore to factory settings.

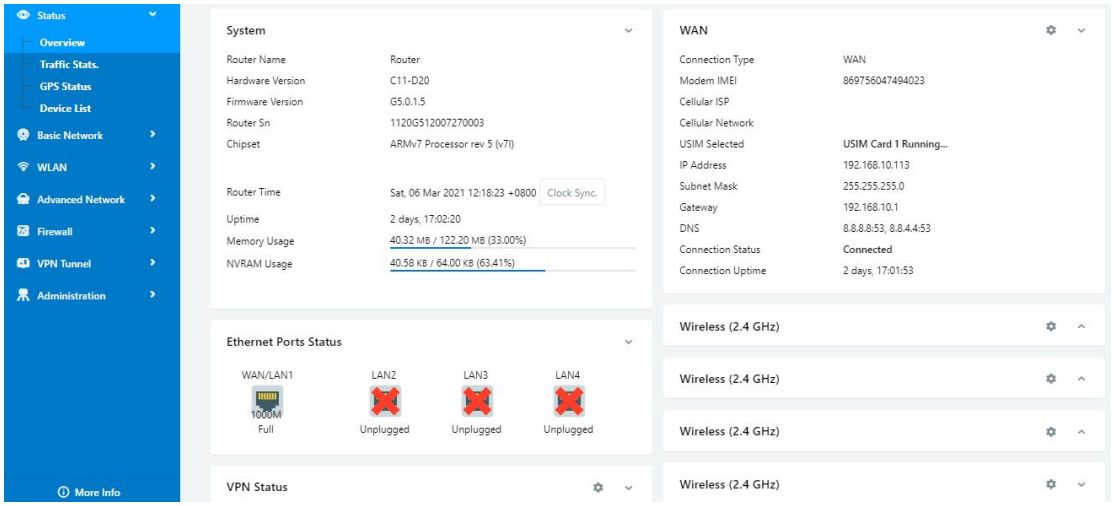
3 Configuration Instance

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.

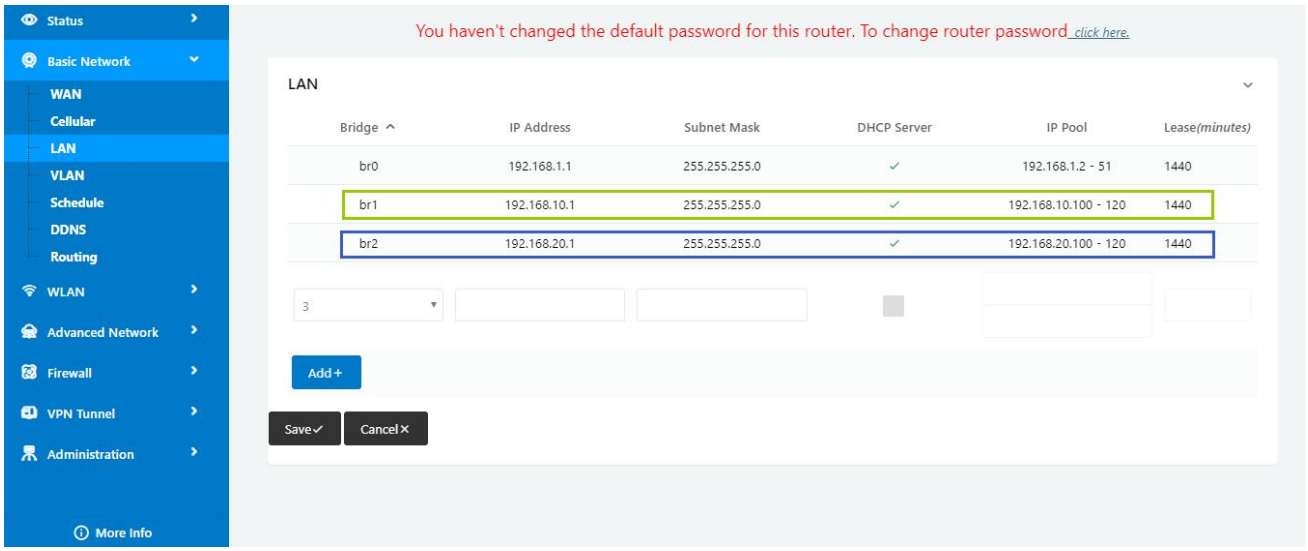
3.1 VLAN

WL-G510 supports VLAN partition based on Ethernet port (LAN1~LAN4)

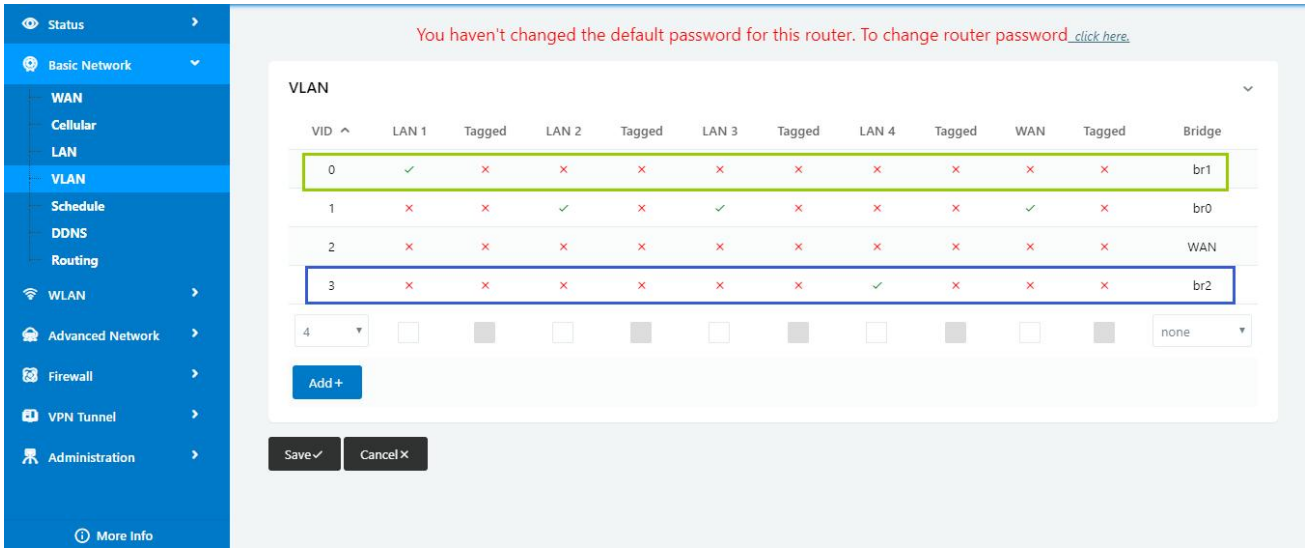




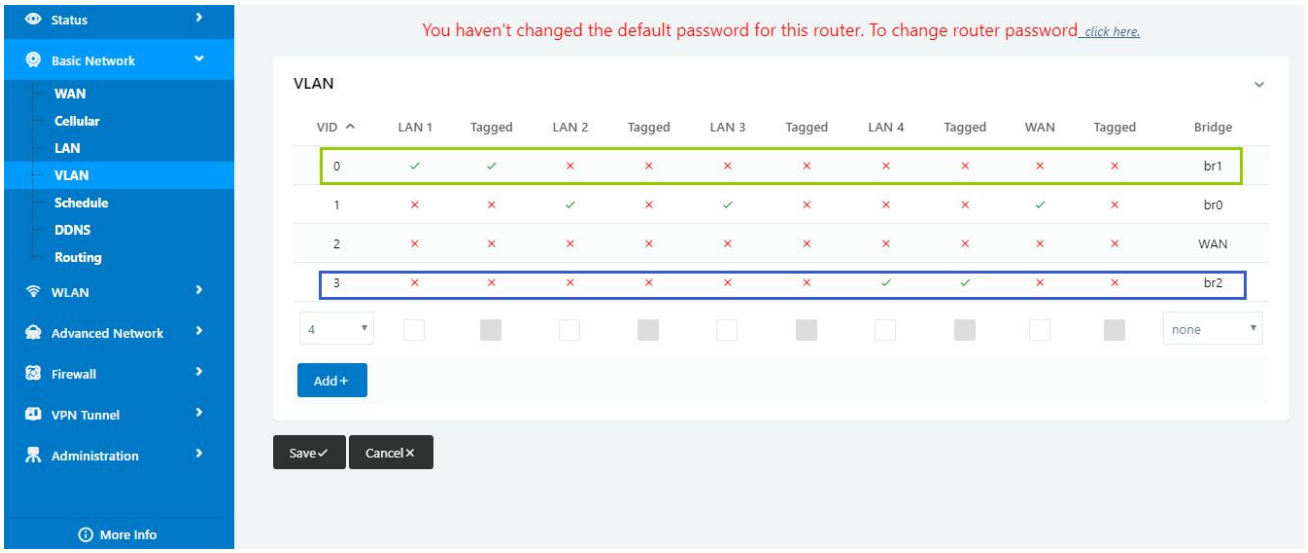
1) Configure LAN with Basic Network.



2) If untag for br1 ad 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.

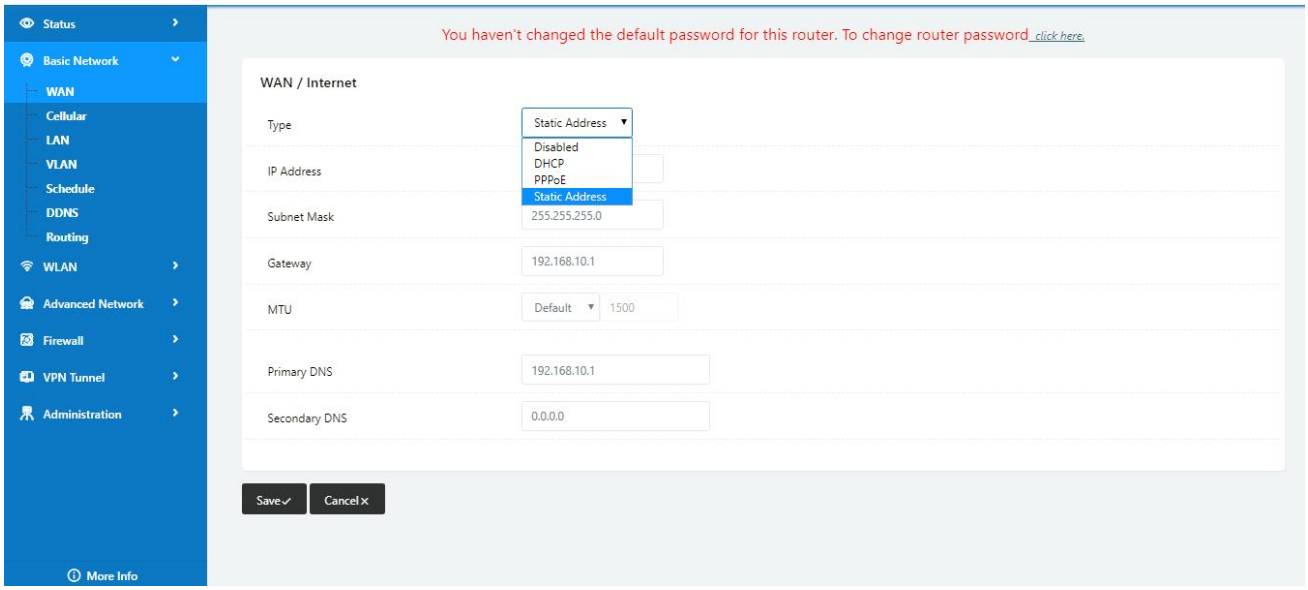


---End

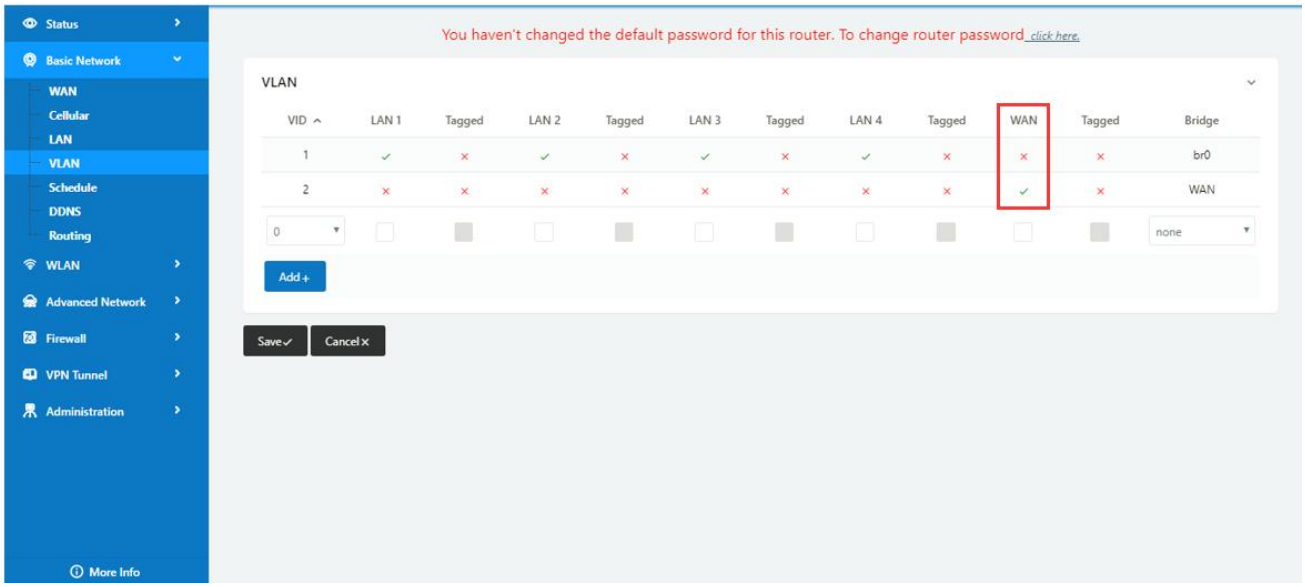
3.2 WAN Backup (WAN as Main, Cellular Backup)

The WAN and Cellular backup feature can quickly switch traffic to Cellular (link2) when WAN (link1) fails, and WL-G510 brings you a stable network experience.

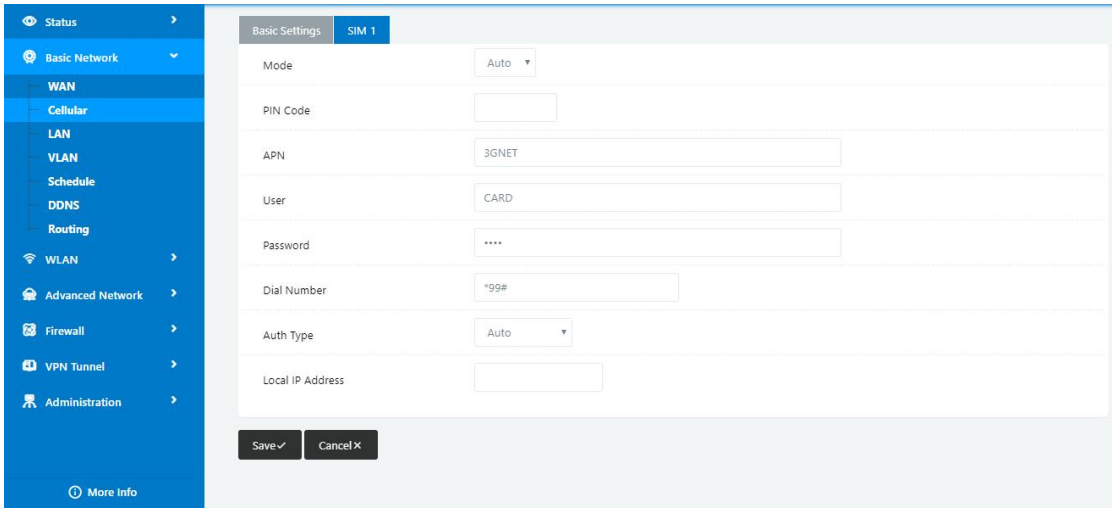
1) Navigate to Basic **Network > WAN**, you may configure the WAN parameters with your situation



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



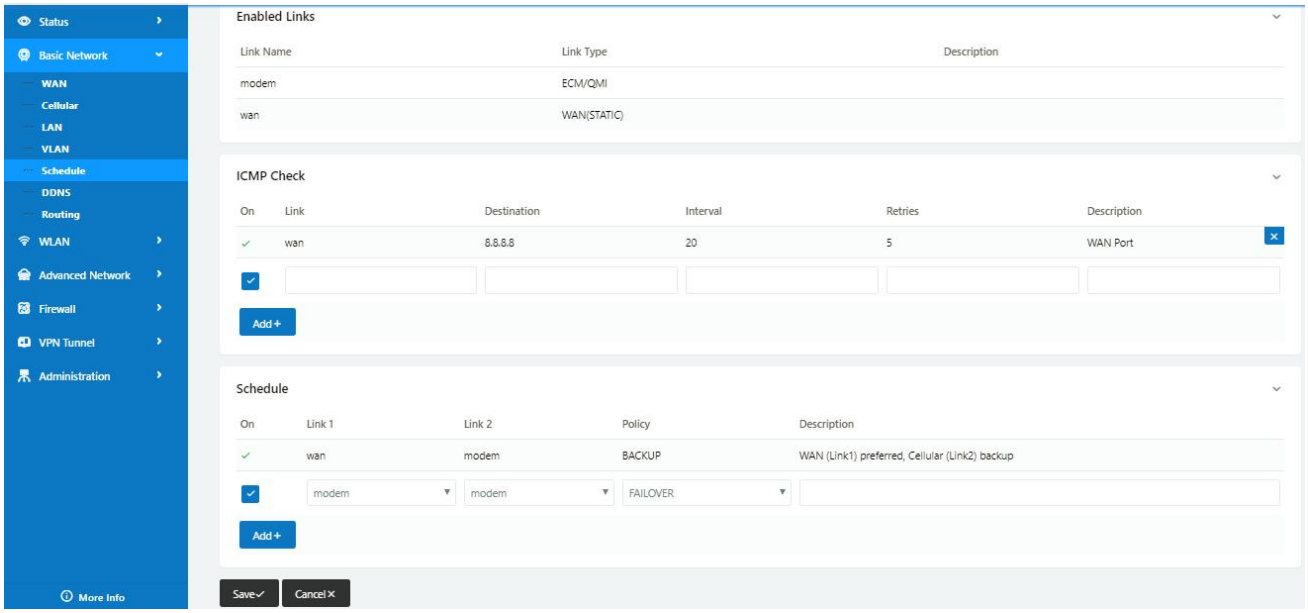
3) Navigate to **Basic network > Cellular**, configure the APN as your SIM



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

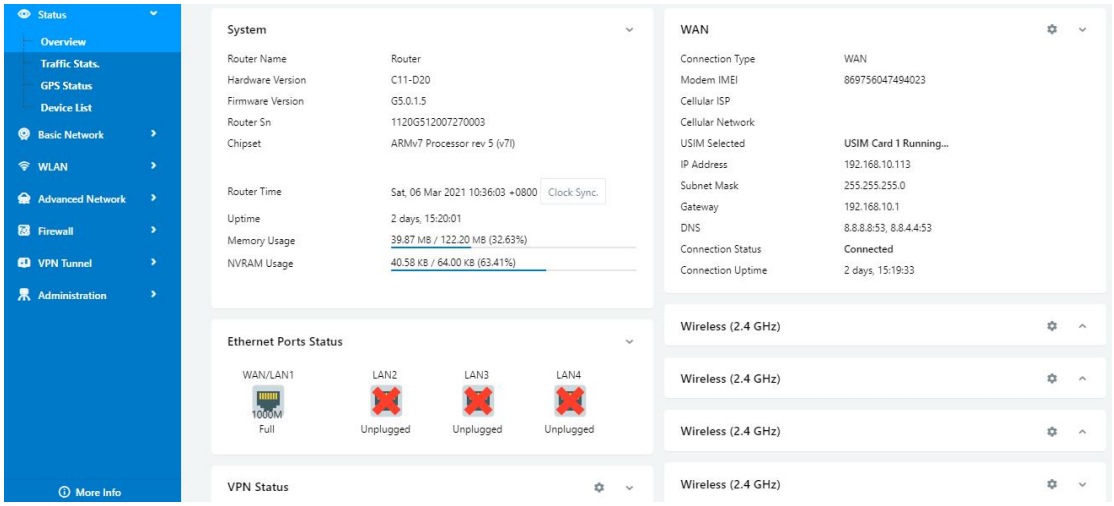
Add ICMP Check to WAN

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

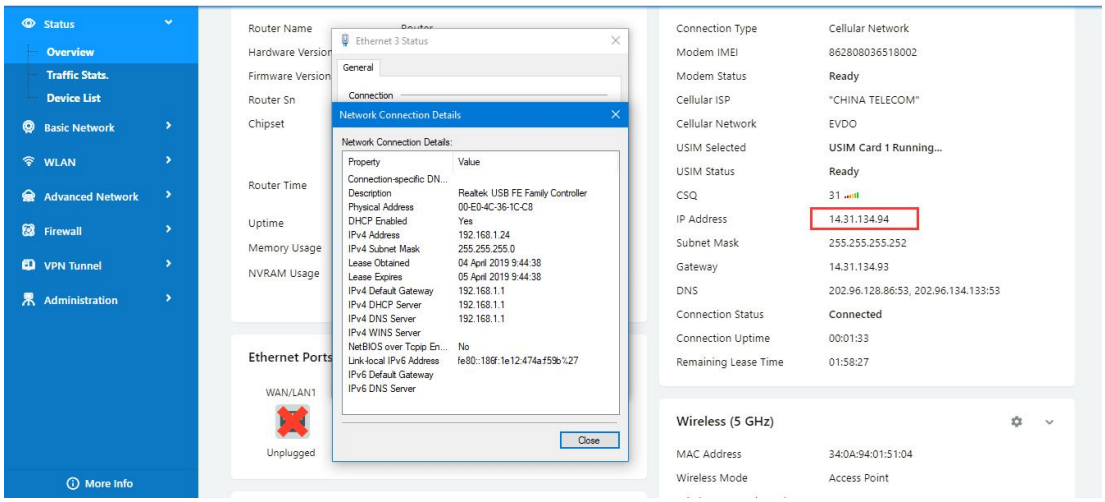
---End

3.3 Port Forwarding

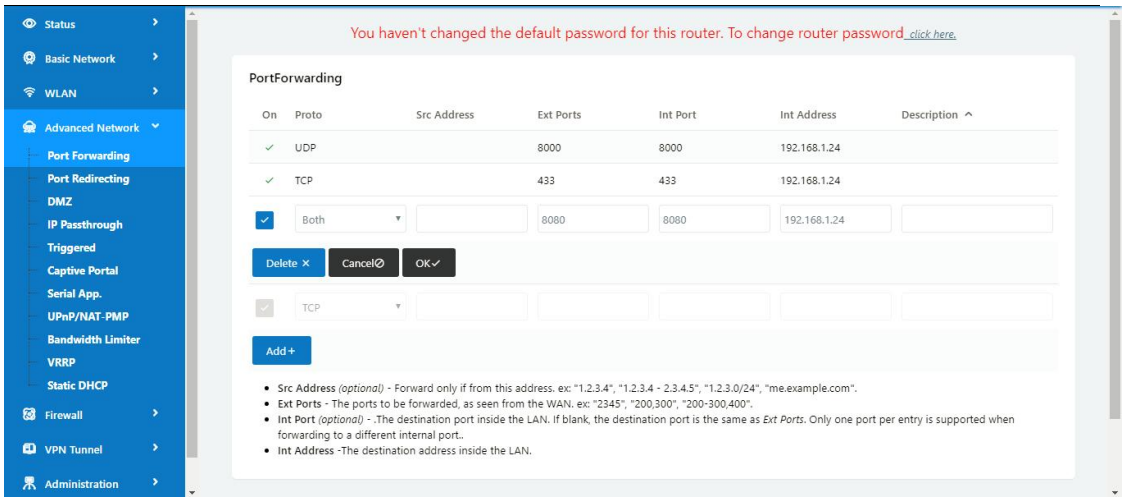
1) The router online and got a public IP address 14.31.134.94

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

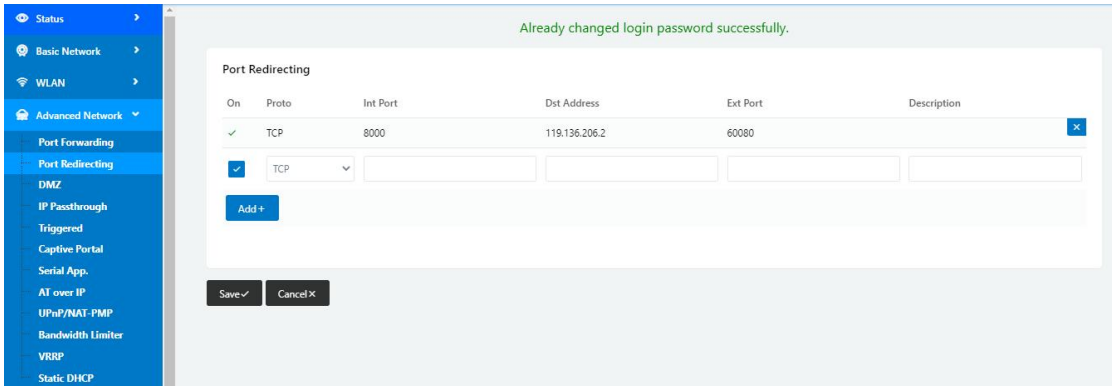


4) The PC can be accessed via 14.31.134.94:443 over Internet

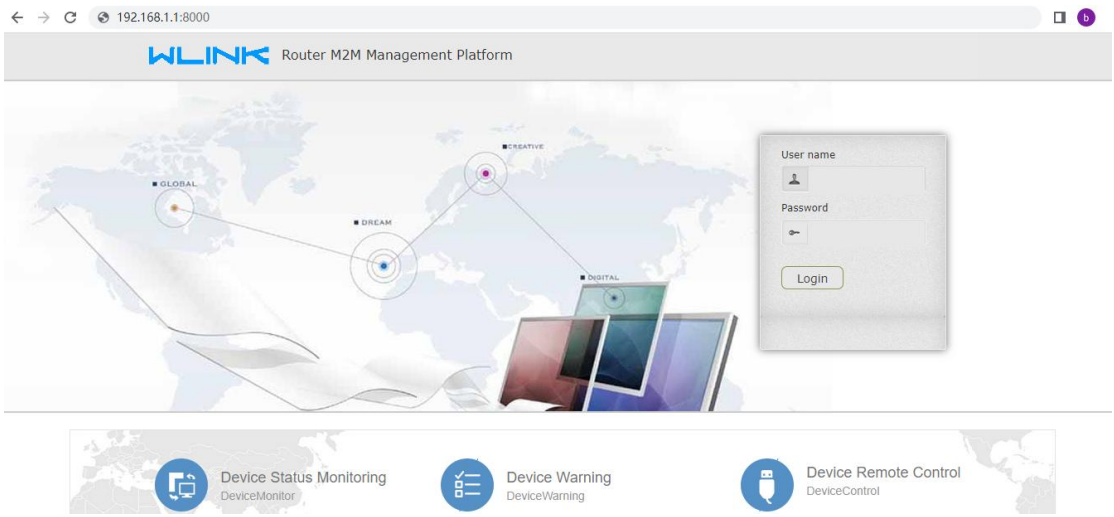
---End

3.4 Port Redirecting

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



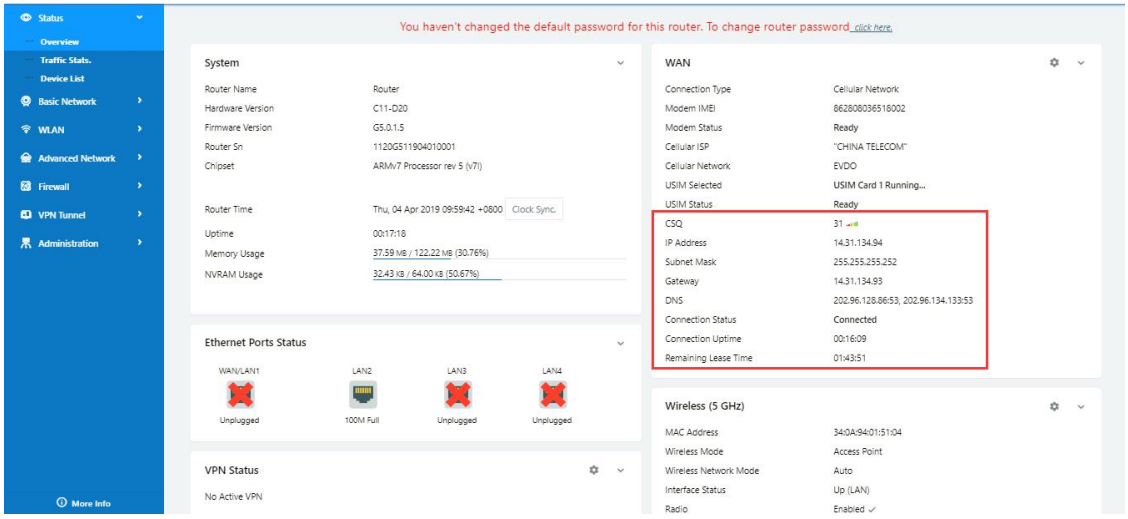
Configure Internal port as 8000, the Destination IP address as 119.136.206.2 and External port 60080(M2M Platform Server IP and Port as example). Access to 192.168.1.1:8000 in browser, the router will redirect to 119.136.206.2: 60080.



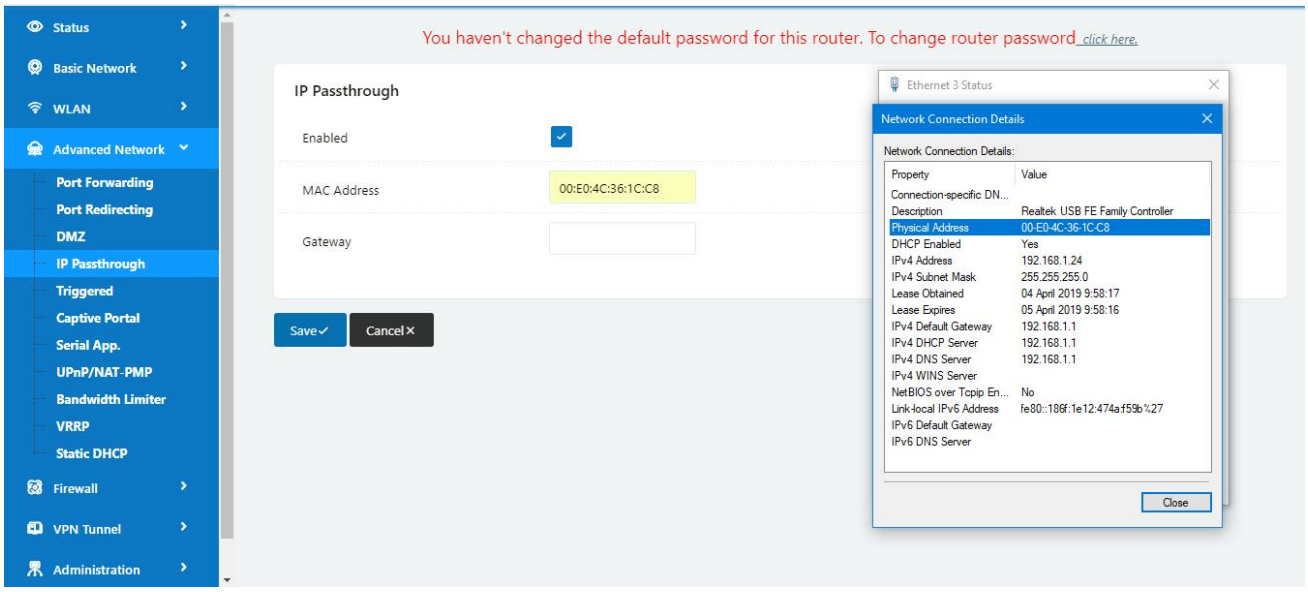
---End

3.5 IP Passthrough

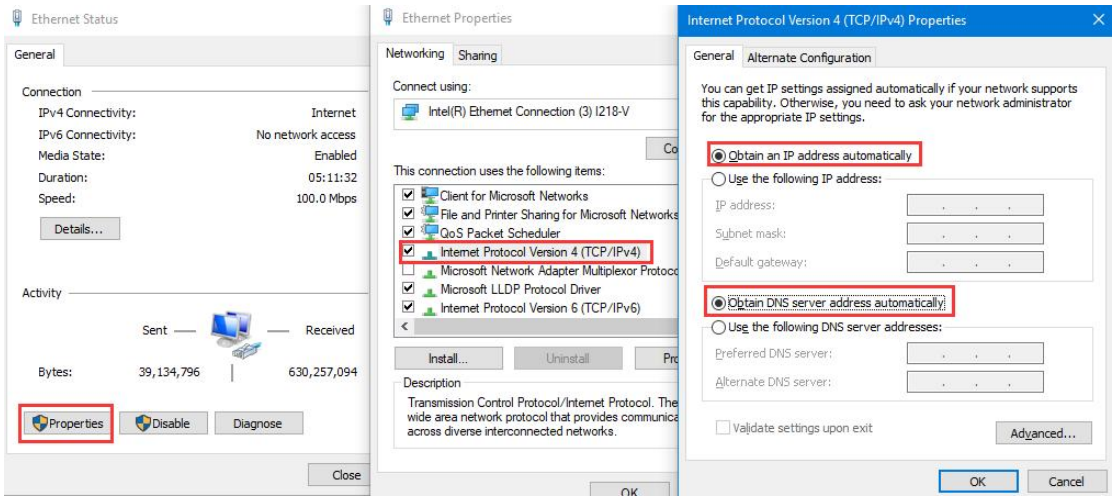
1) The router online



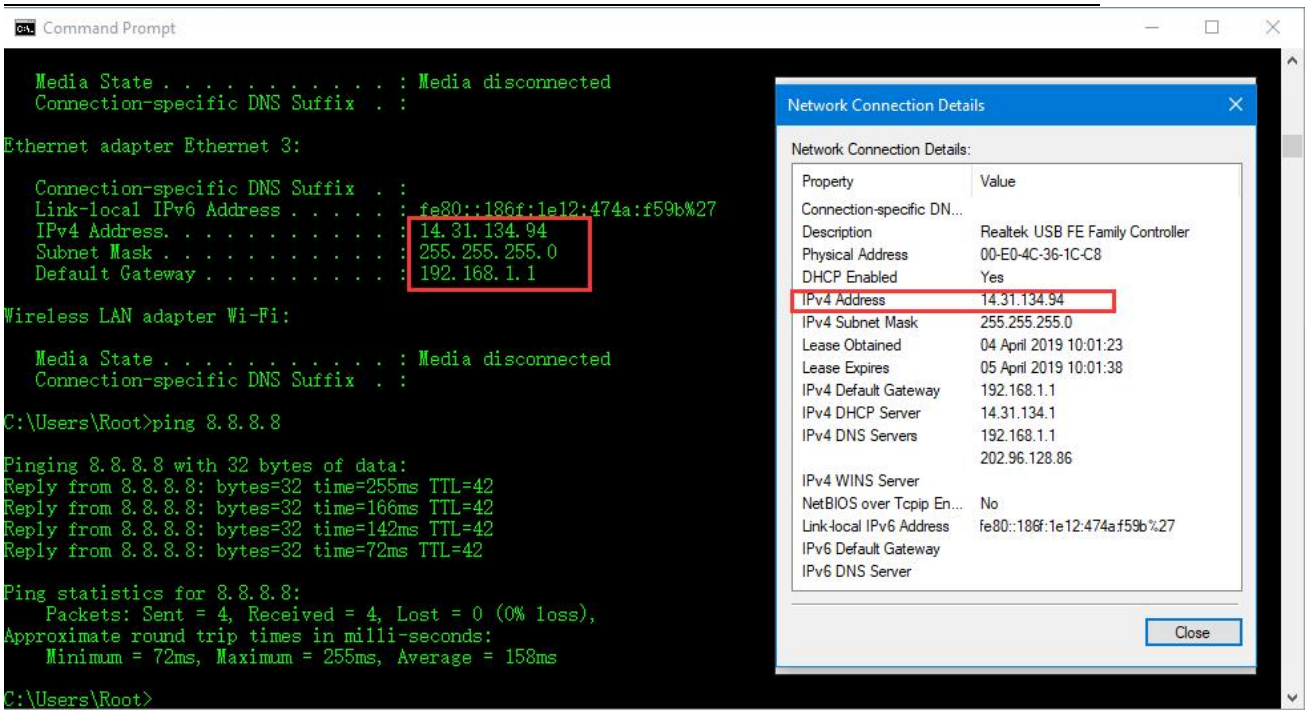
2) Configure IP passthrough destination MAC address (PC Ethernet MAC)



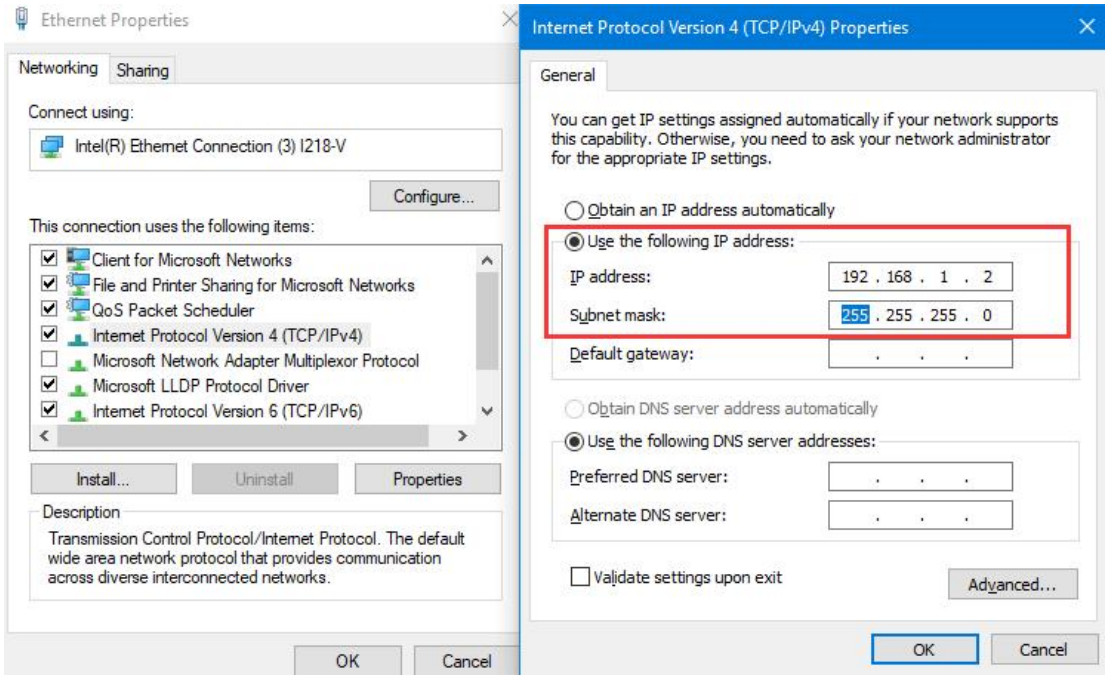
3) Set the PC to DHCP



4) Check the Ethernet status and ping test



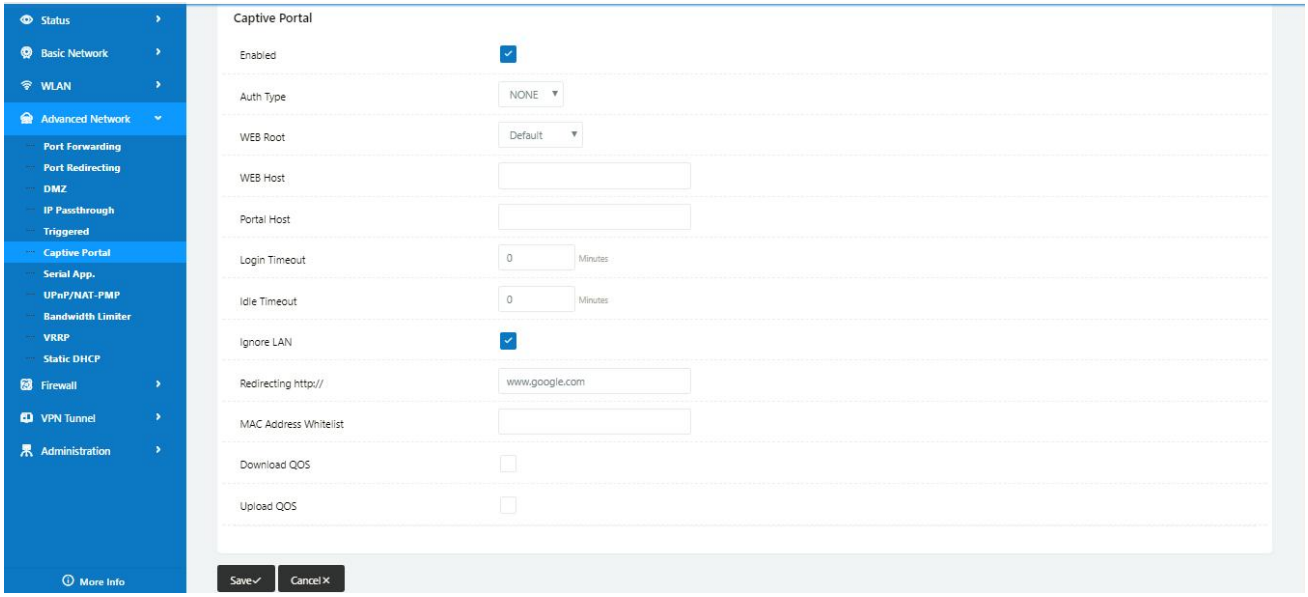
5) Set the PC Ethernet as DHCP to release the IP and access to router GUI again



---End

3.6 Captive Portal

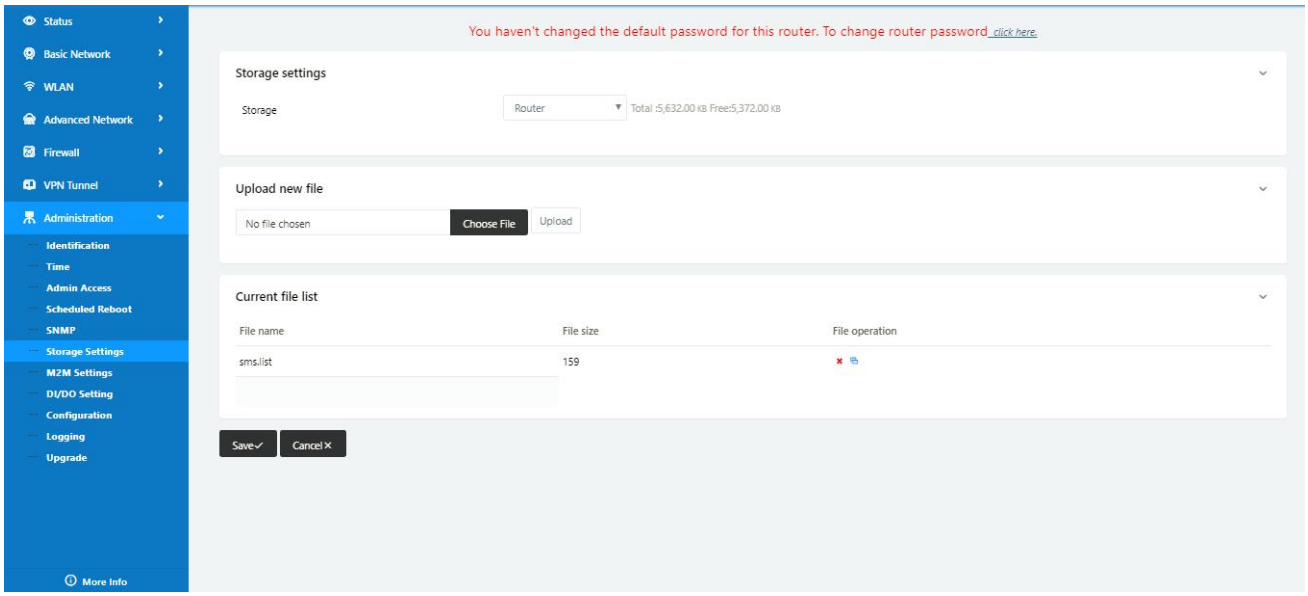
Please click “Advanced Network> Captive Portal” to check or modify the relevant parameter.



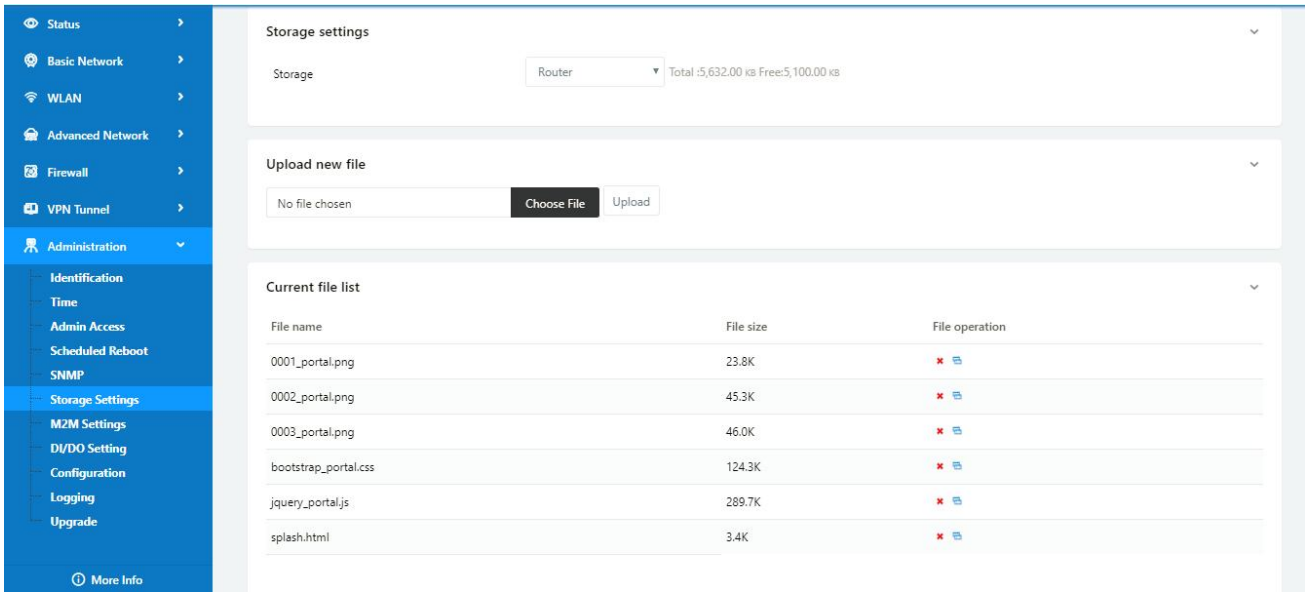
1) Upload Portal file and Splash.html by local

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.

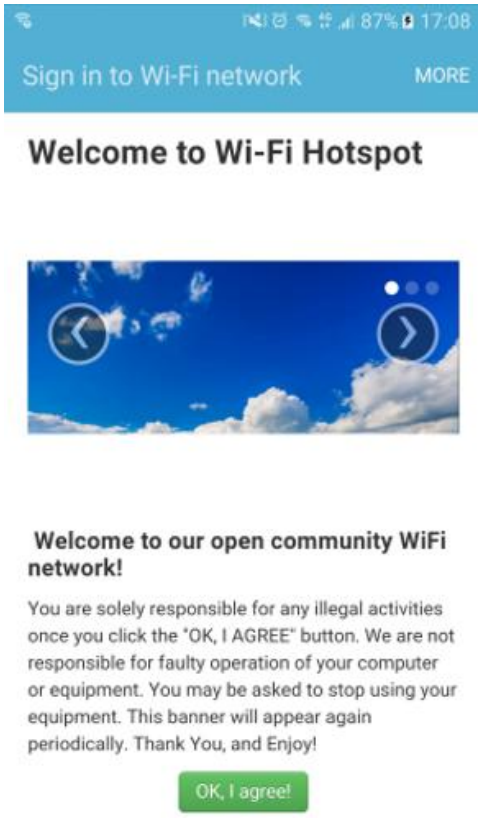


Each Ad file just supports 3 Ad portal images. Picture format is acceptable for png/jpg and image size is less than 100Kbytes and resolution is 800*600. Picture name is 0001_portal.png, 0002_portal.png and 0003_portal.png. Furthermore, please keep image names the same between portal file and splash.html.



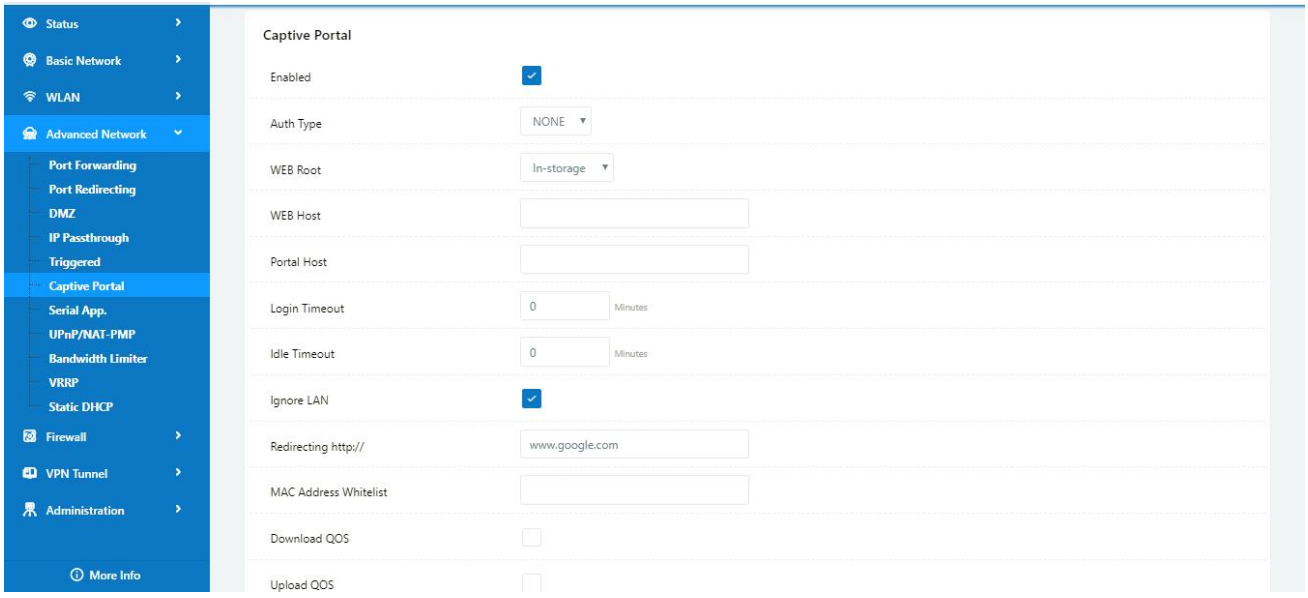

```
<!-- <hr> -->

<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">
            <img src="0001_portal.png" alt="">
        </div>
        <div class="item">
            <img src="0002_portal.png" alt="">
        </div>
        <div class="item">
            <img src="0003_portal.png" alt="">
        </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.

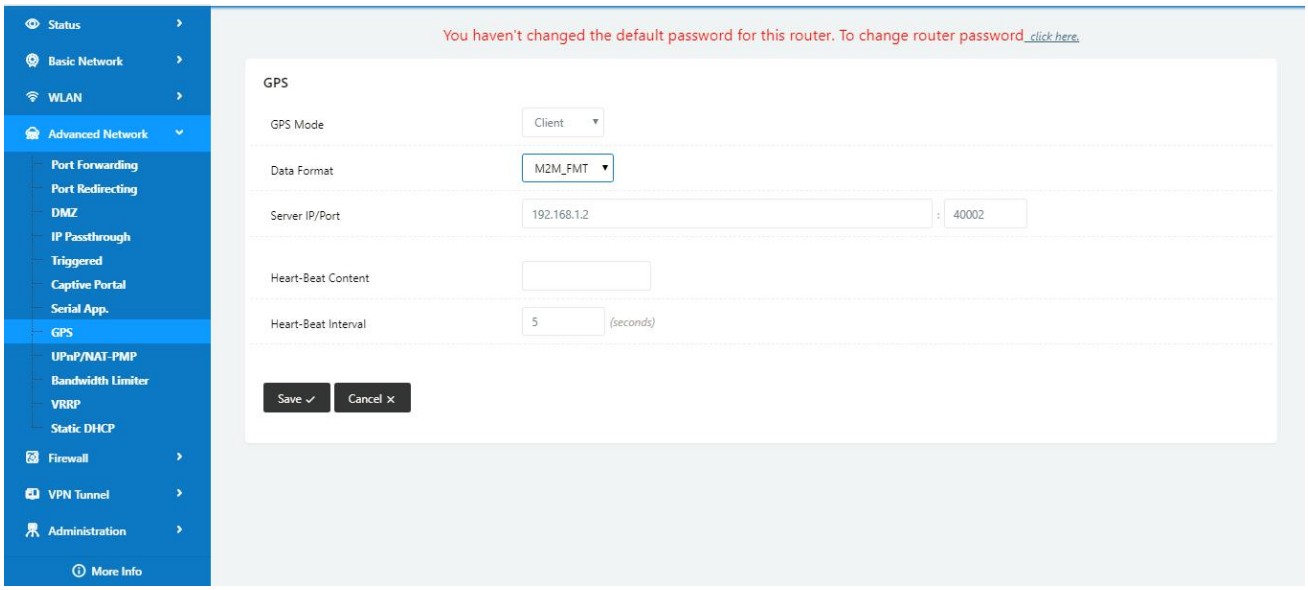


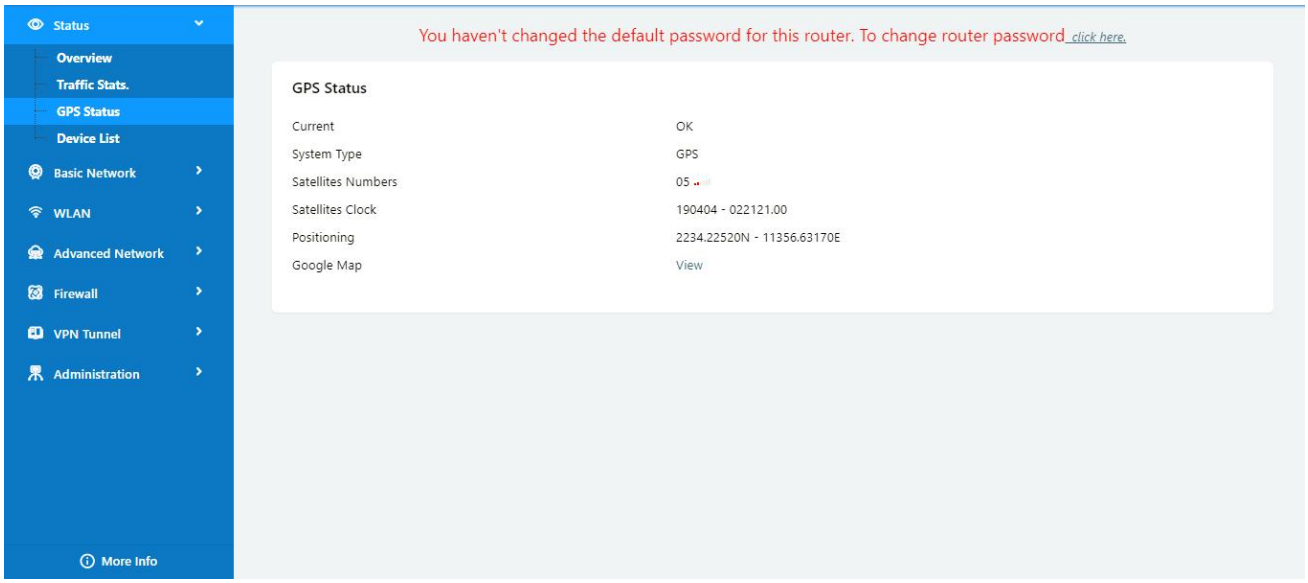
Table 4-6 “GPS” Instruction

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



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 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

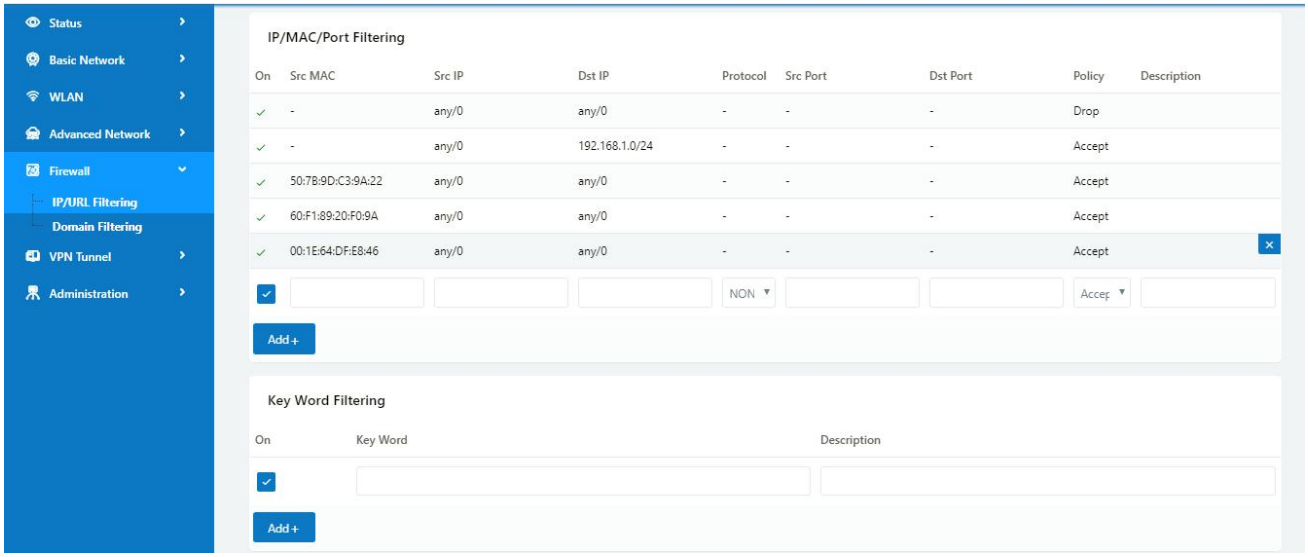
1) IP/MAC/Port Filtering

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

Test case:

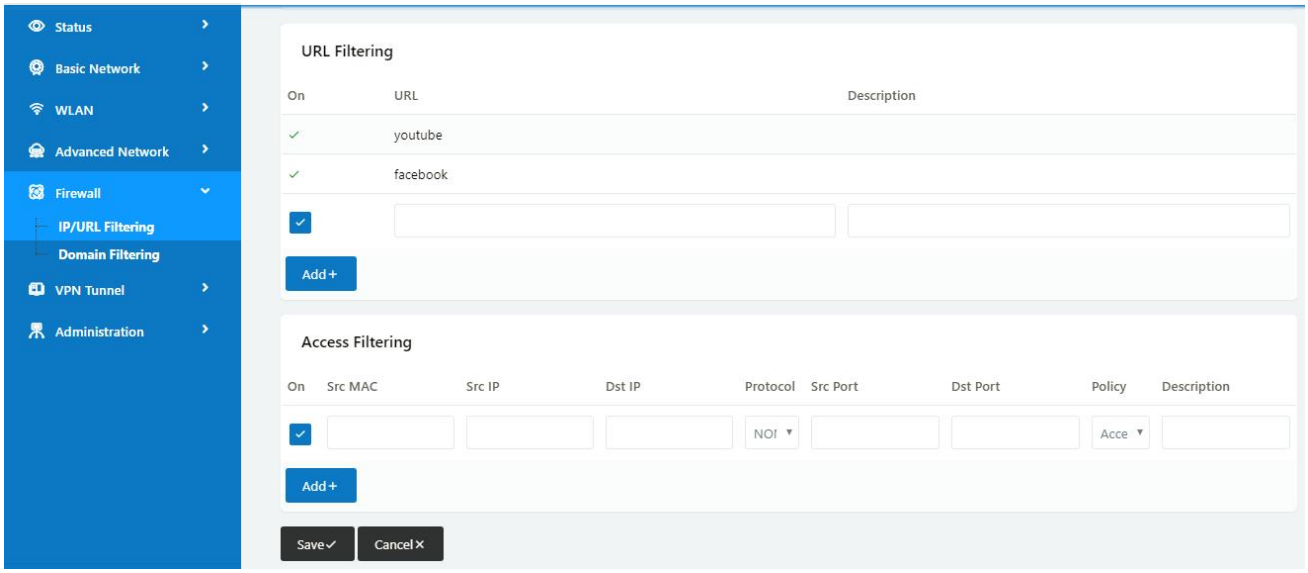
1.1 Only allow three devices (MAC/LAN/WLAN) can access to Internet via WAN: 110.110.10.10

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/Cellular interface to Internet.



3) URL Filtering

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

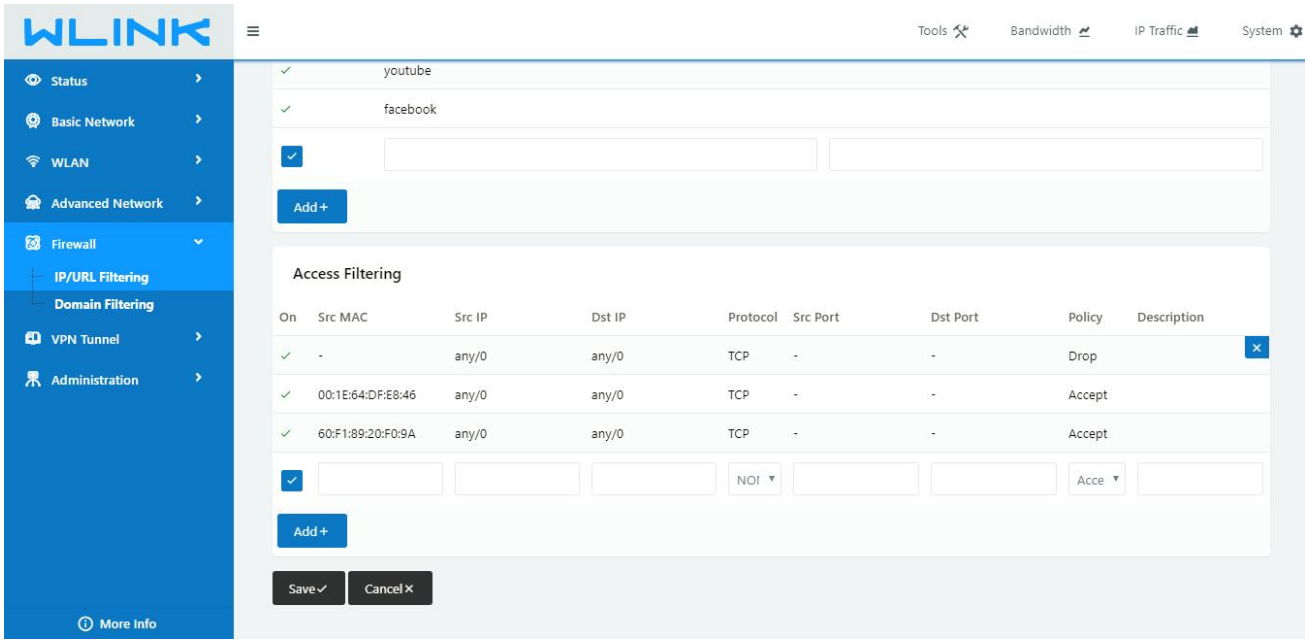
4) Access Filtering

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.

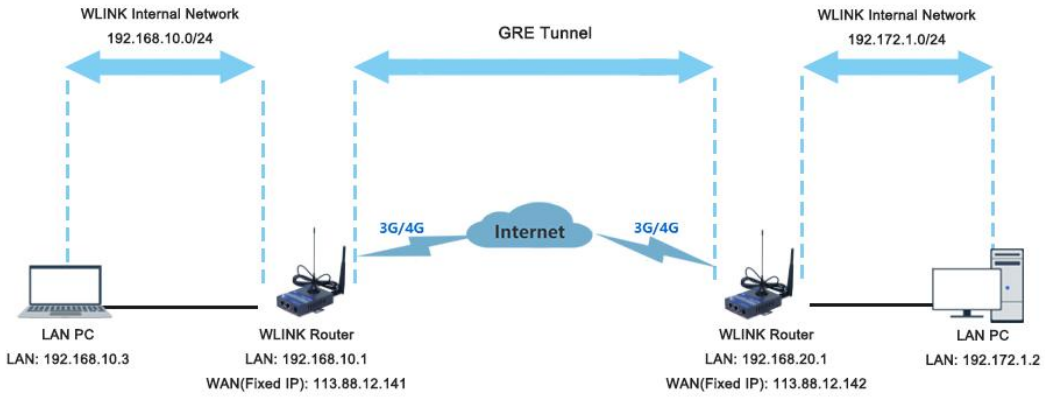


---End

3.9 VPN Tunnel

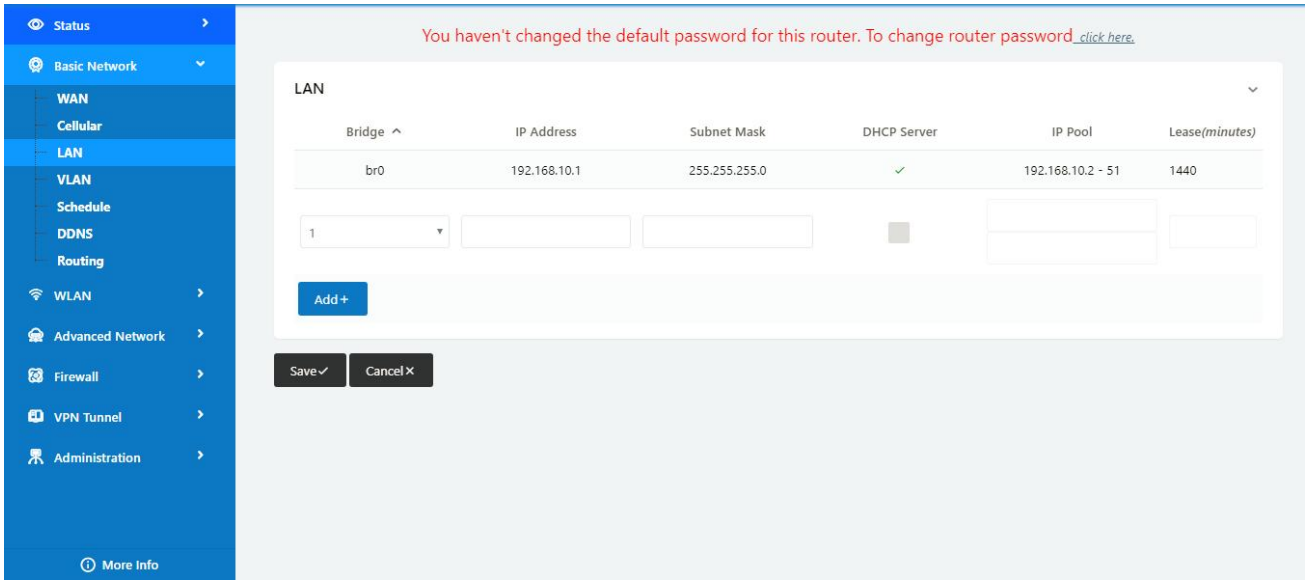
3.8.1 GRE

GRE Tunnel between WLINK Routers

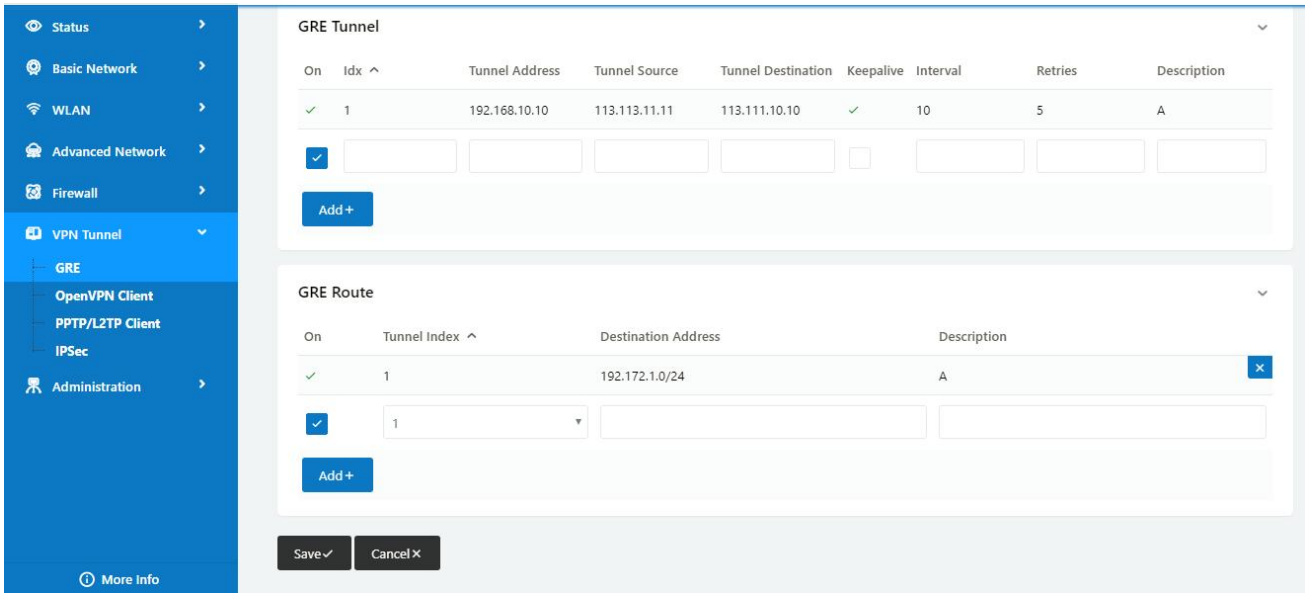


1) WL-G510(A) Config

Navigate to **Basic Network > LAN**

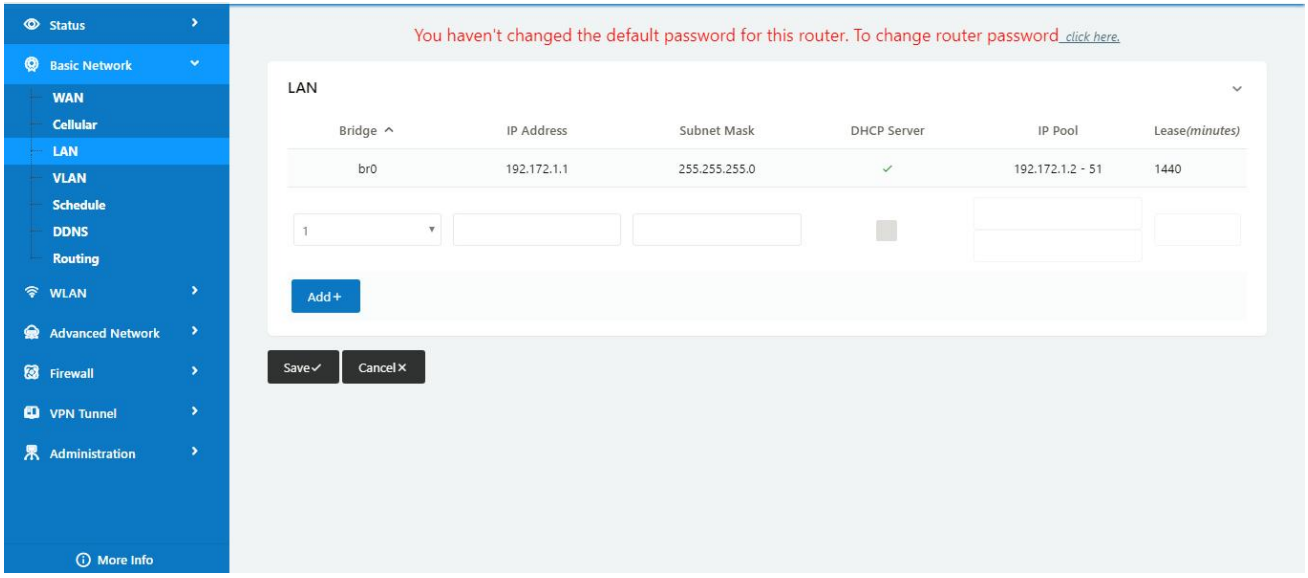


Navigate to **VPN Tunnel > GRE**

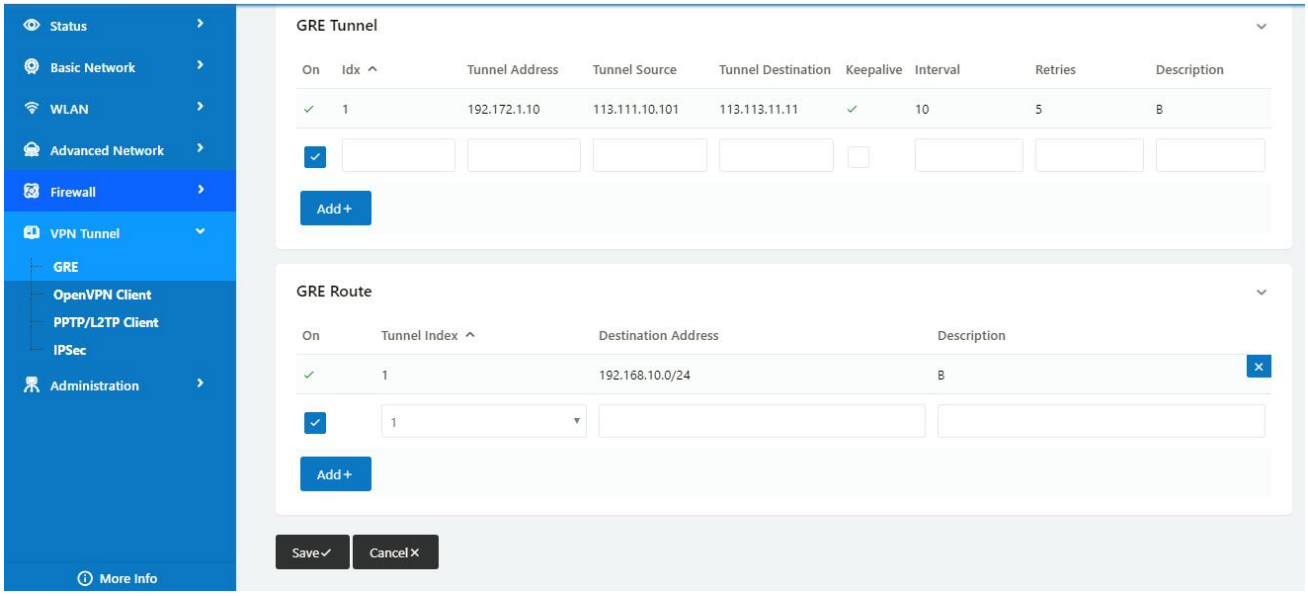


2) WL-G510(B) Config

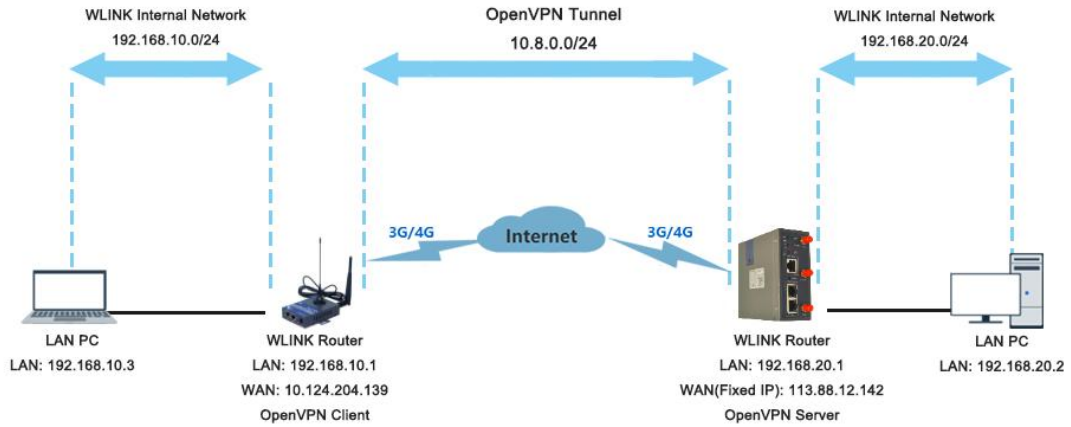
Navigate to **Basic Network > LAN**



Navigate to **VPN Tunnel > GRE**

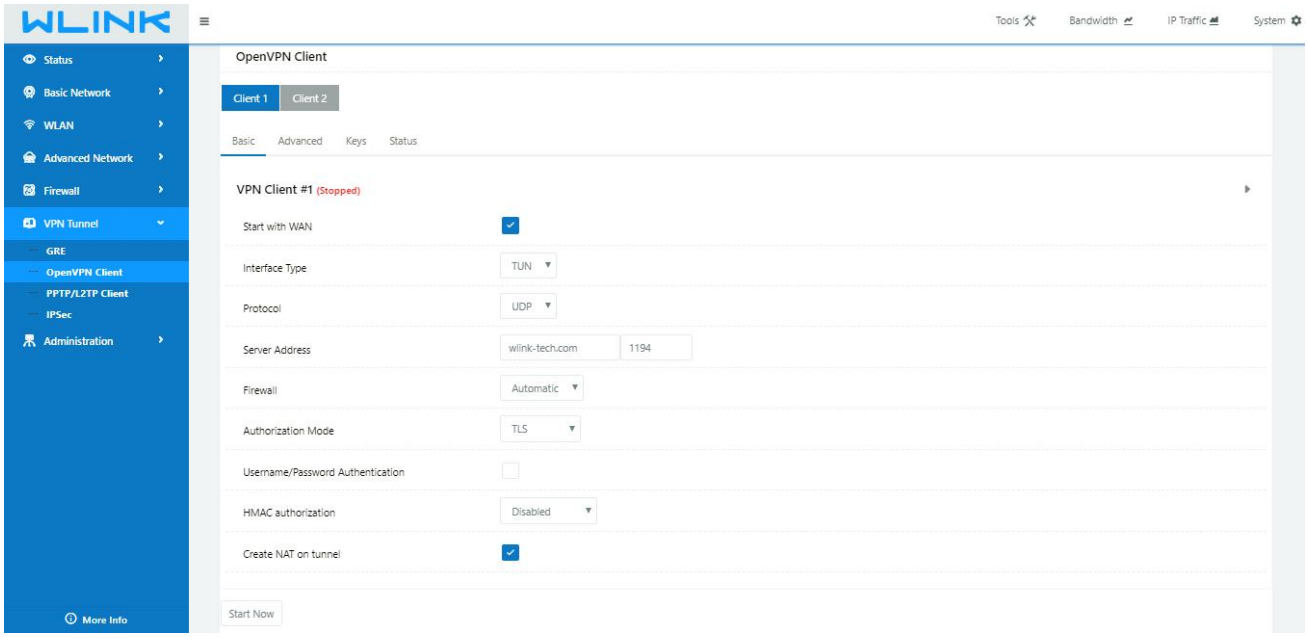


3.8.2 OpenVPN



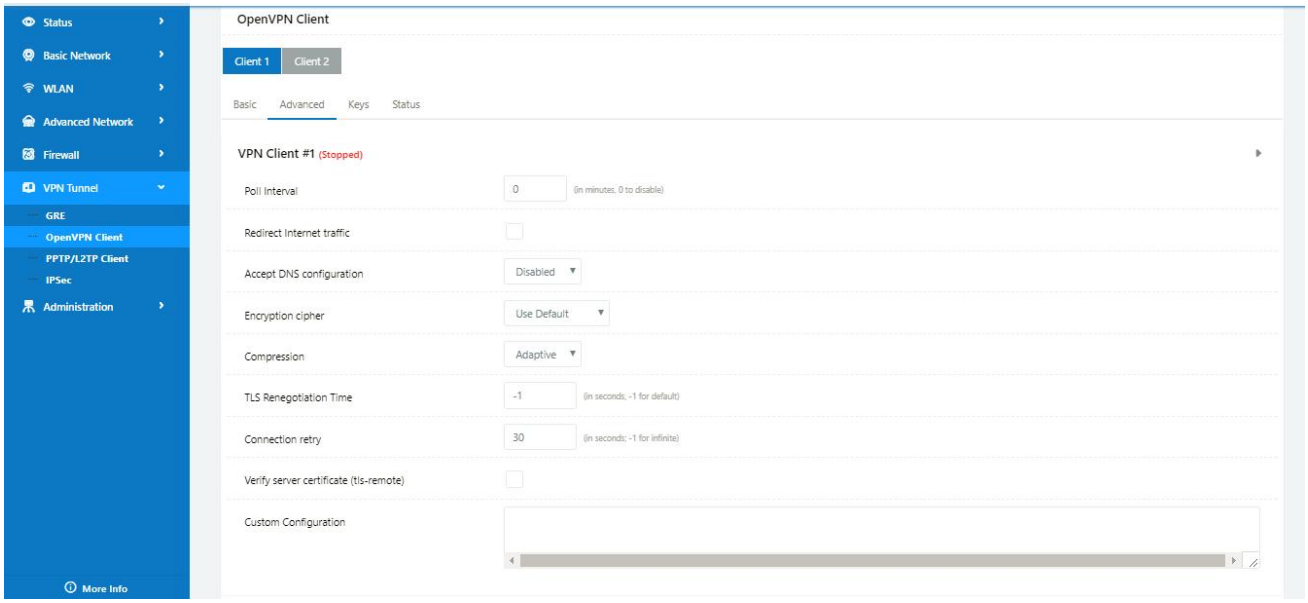
OpenVPN between WL-G510 client and Server

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

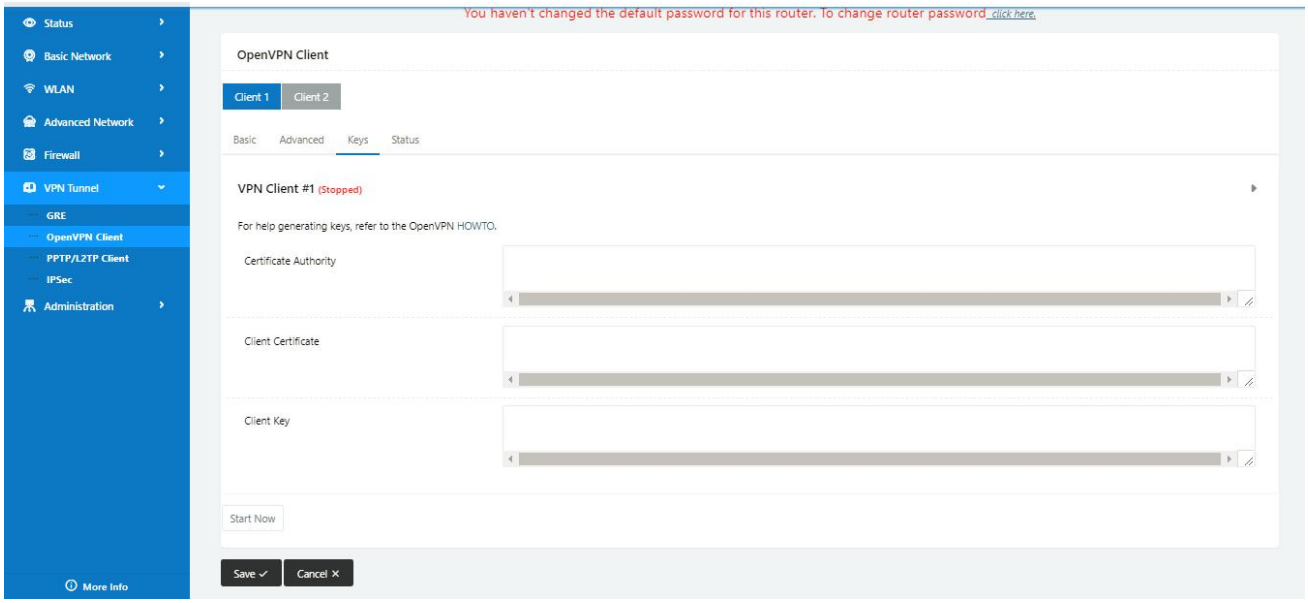


Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 4G/3G/WAN port.
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.
Protocol	UDP and TCP optional.
Server Address	The Openvpn server public IP address and port.
Firewall	Auto, External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

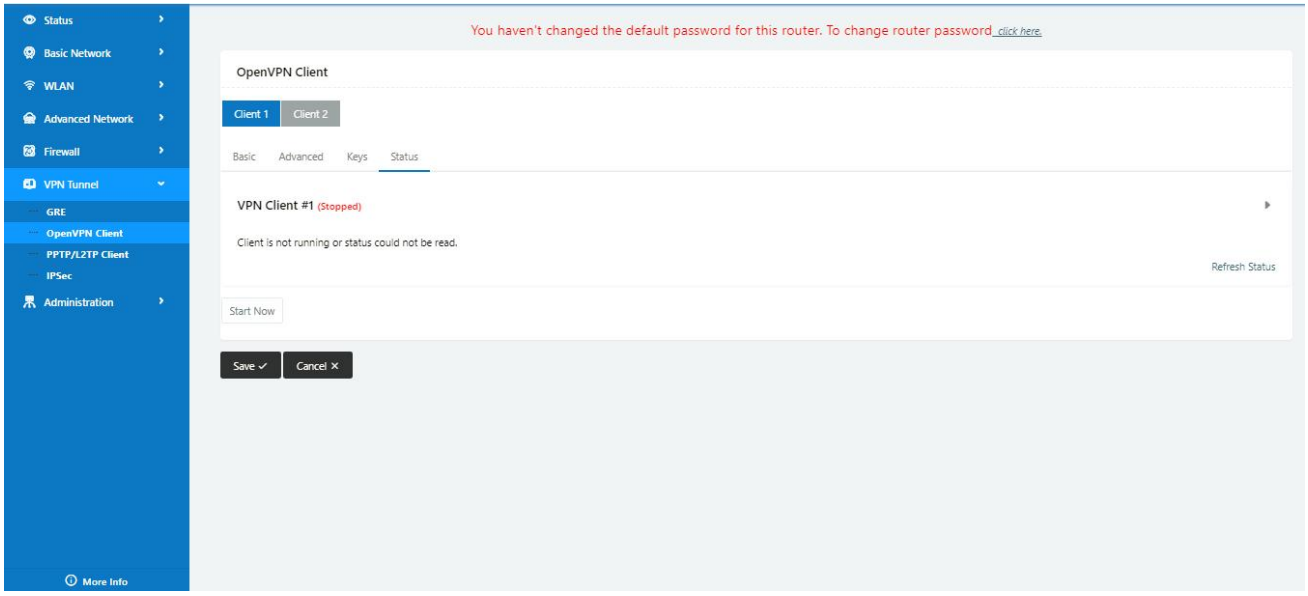
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.



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



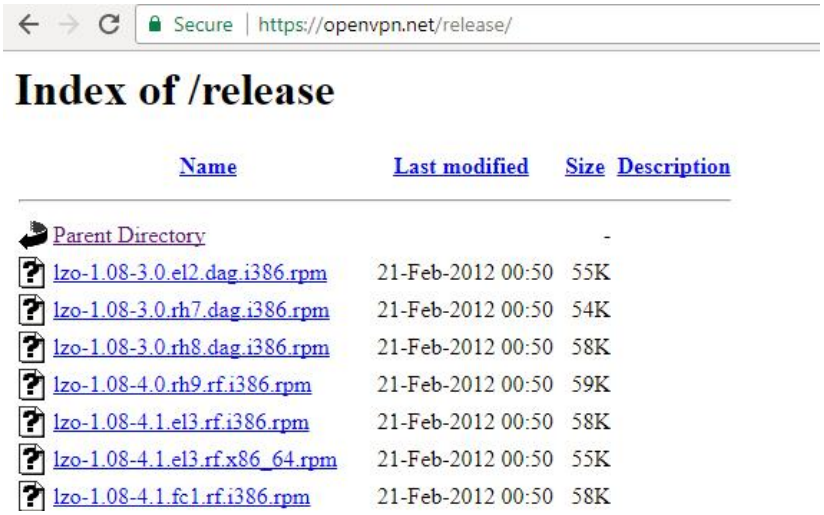
Parameter	Instruction
Status	Check OpenVPN status and data statistics.

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

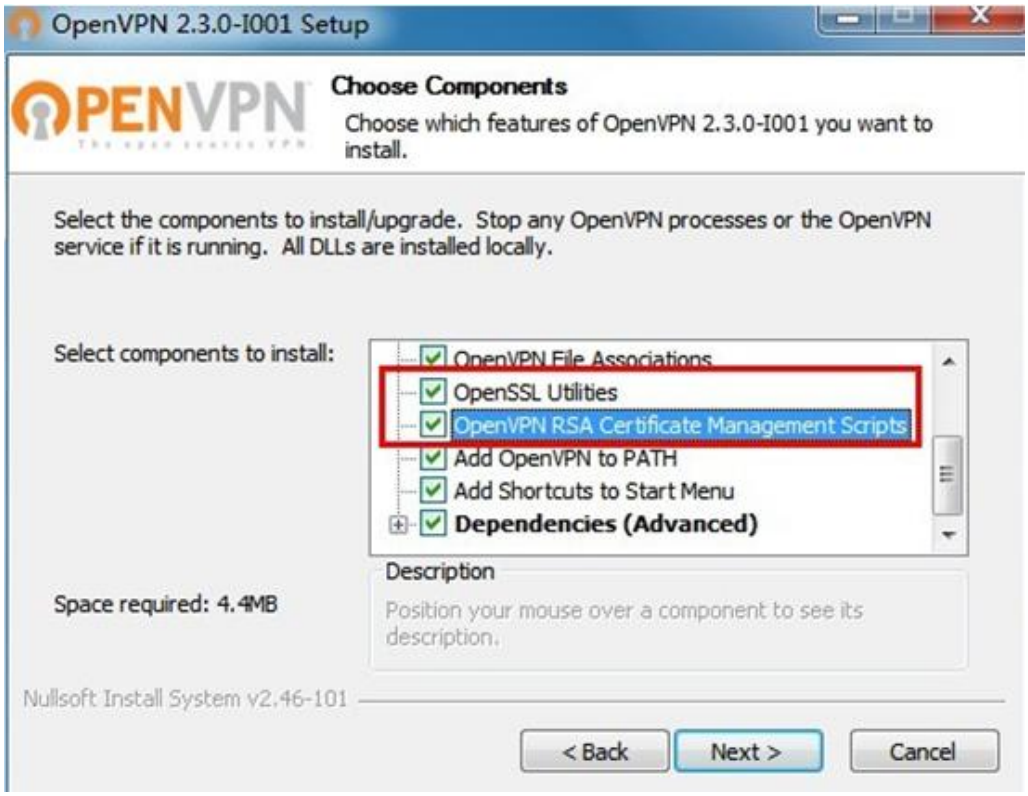
OpenVPN Keys Guide

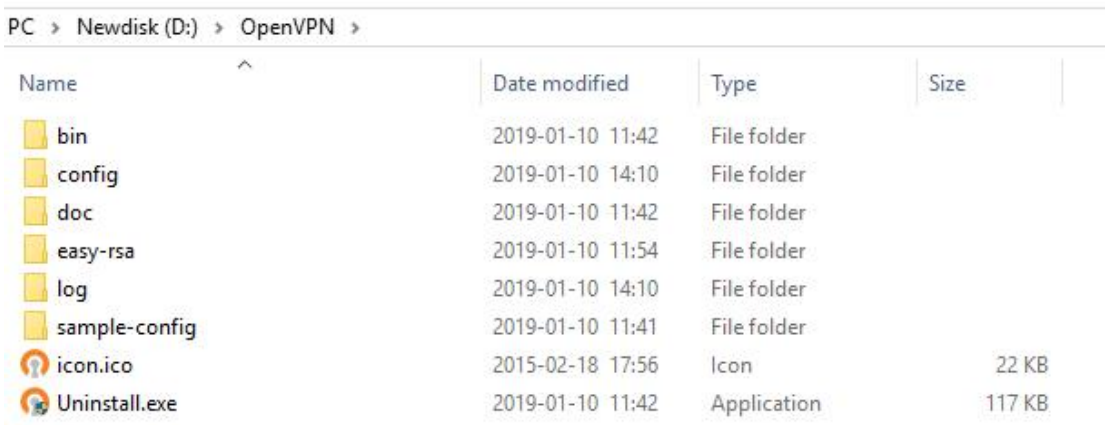
The fllowing steps are for server running on Windows 7/8/10

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

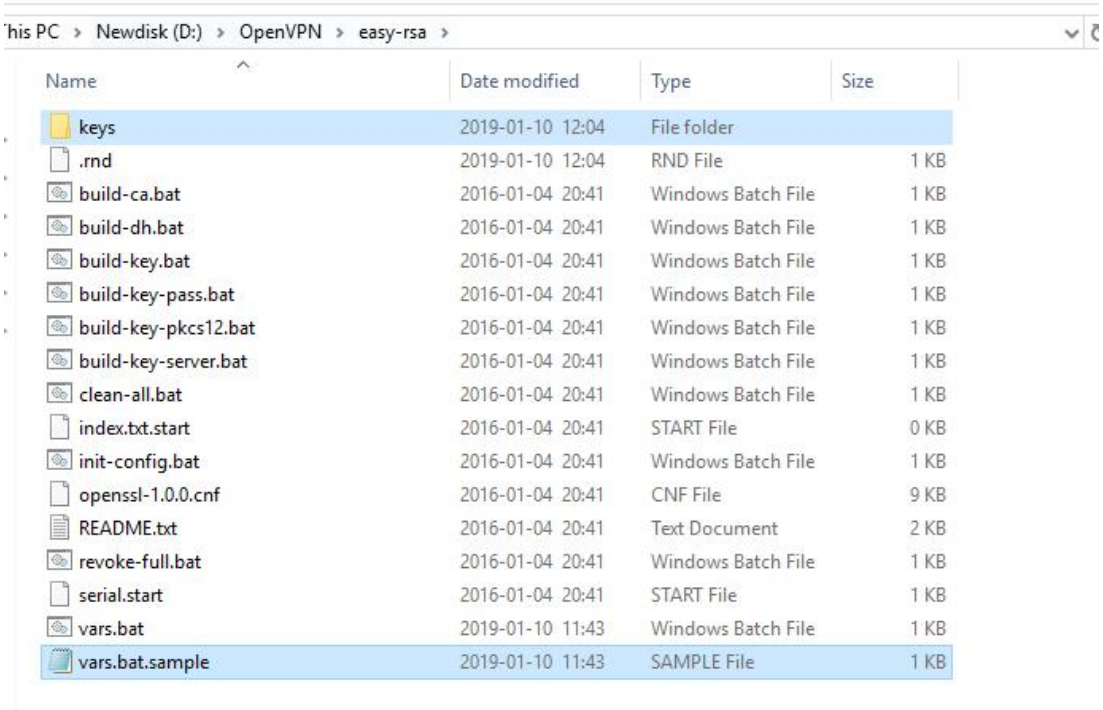


After installing OpenVPN, please find the OpenVPN folder to generate the certificate of server and client. (Access to http://openvpn.net for more information)



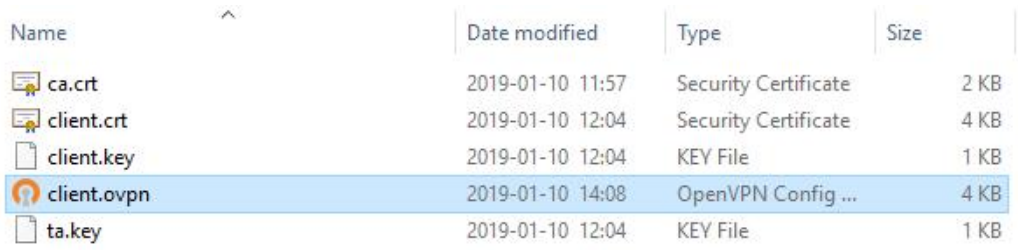


Configure “vas.bat.sample” to complete the initialization step and keys

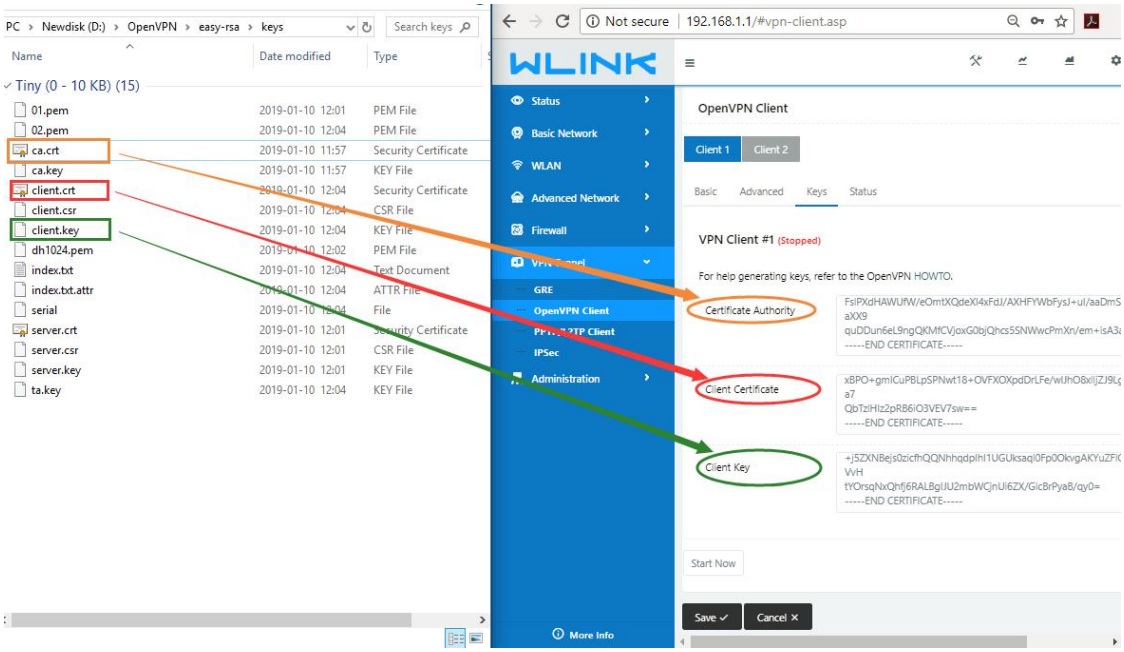


Configure the client keys to WLINK OpenVPN client GUI when you create the server and client certificate in the path OpenVPN/easy-rsa/keys

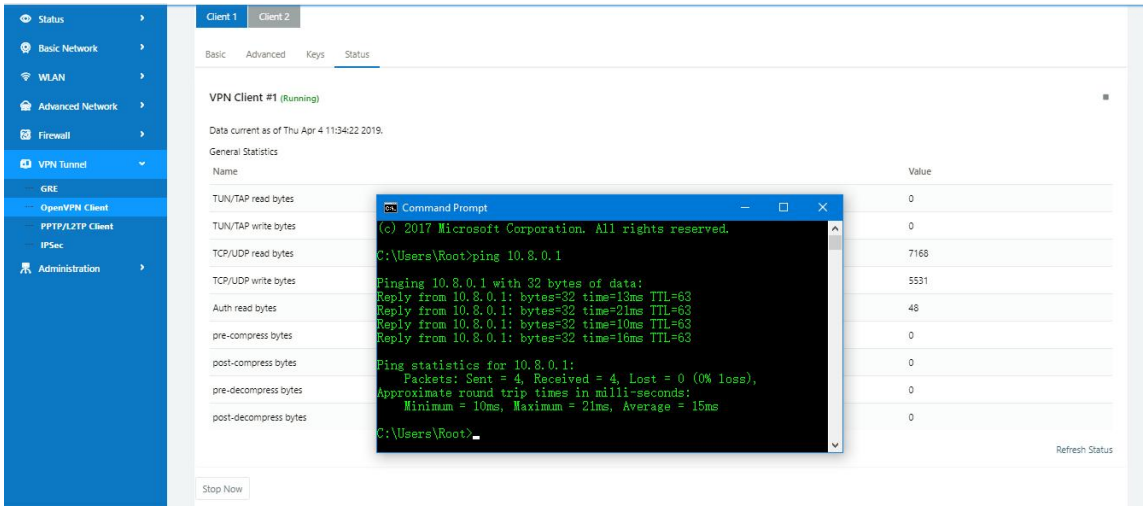
Client certificate (Generated on the server)



OpenVPN>easy-rsa>keys



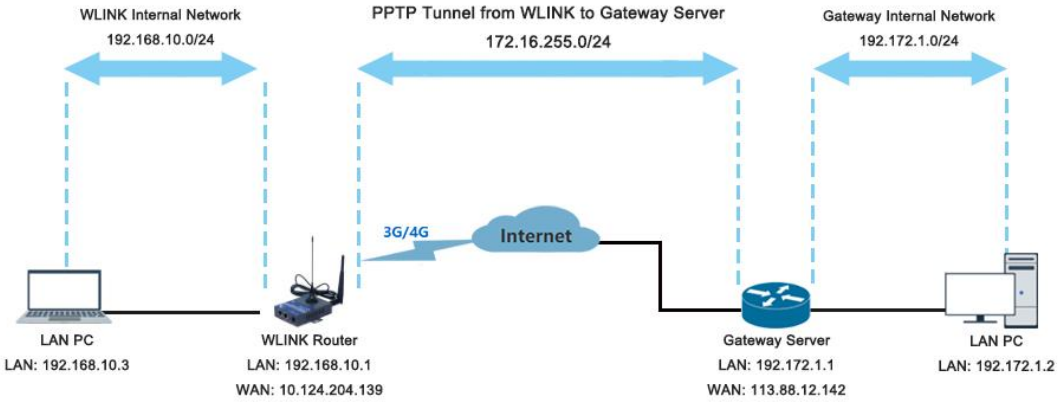
Ping test to your server when the tunnel is established



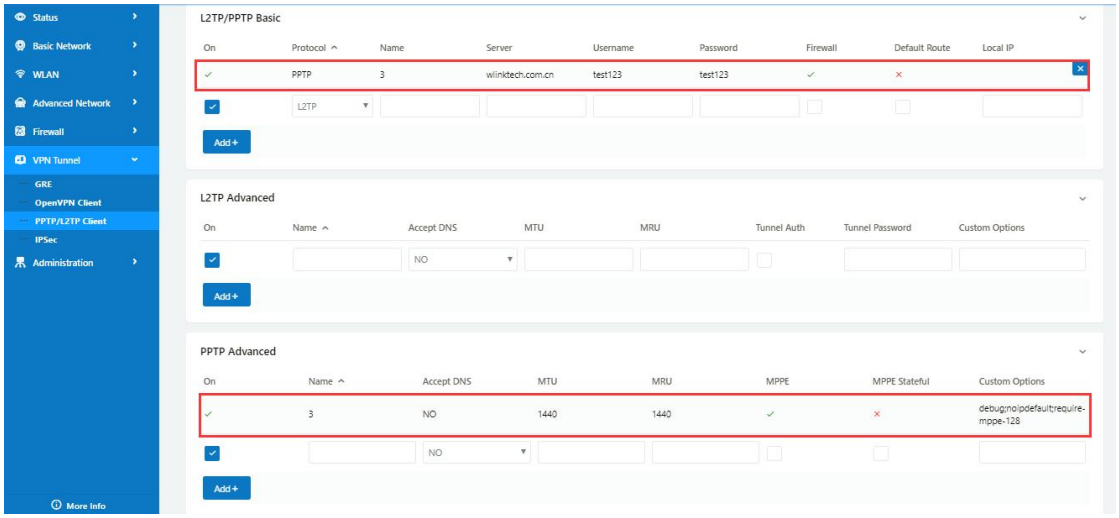
---End

3.8.3 L2TP/PPTP

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



Configured as PPTP

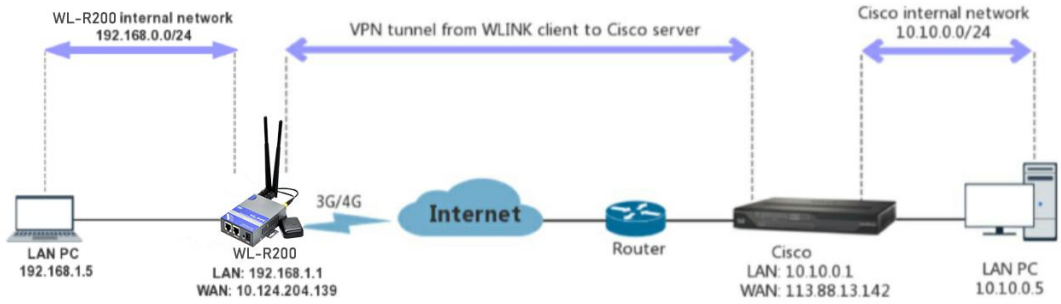


Note: The Custom Options are based on your server

---End

3.8.4 IPSec

IPSec between WLINK Router and Cisco Router



1) Cisco Config (main mode)

!

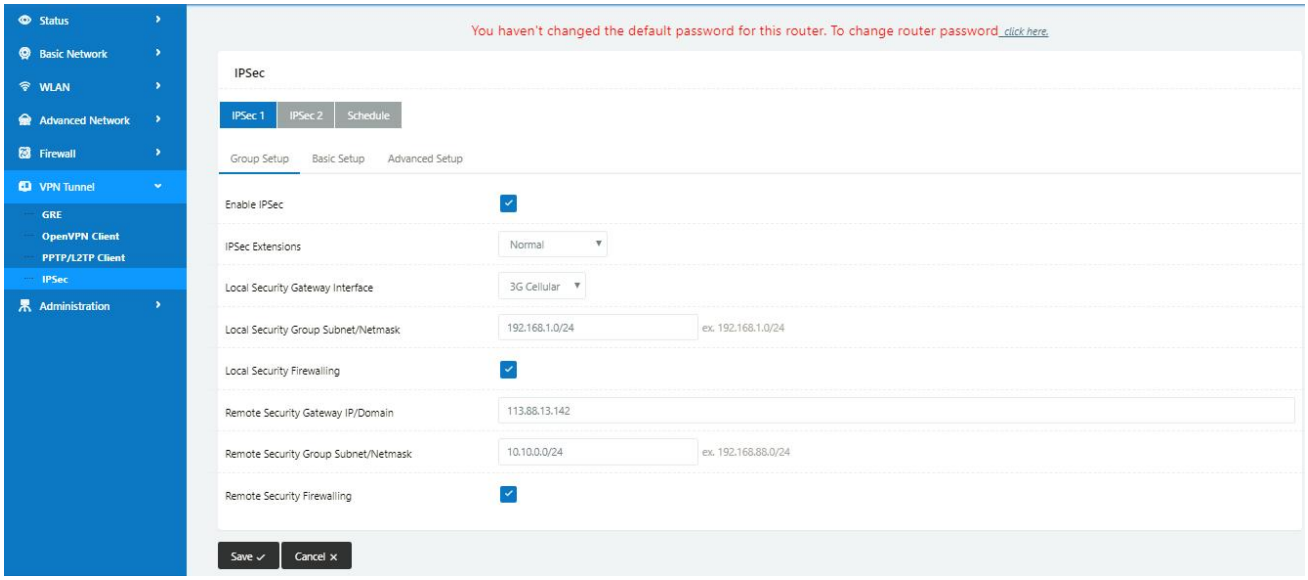
crypto isakmp policy 10

encr 3des

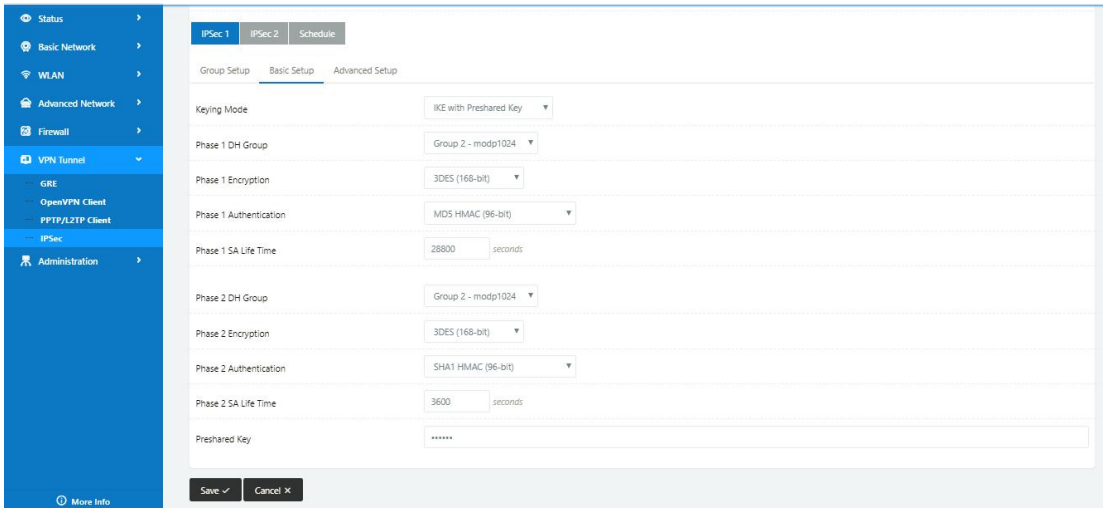
```
 hash md5
 authentication pre-share
 group 2
crypto isakmp key test1234 address 0.0.0.0    0.0.0.0
!
!
crypto ipsec transform-set Tran-set esp-3des esp-sha-hmac
crypto ipsec nat-transparency spi-matching
!
```

2) WLINK Config

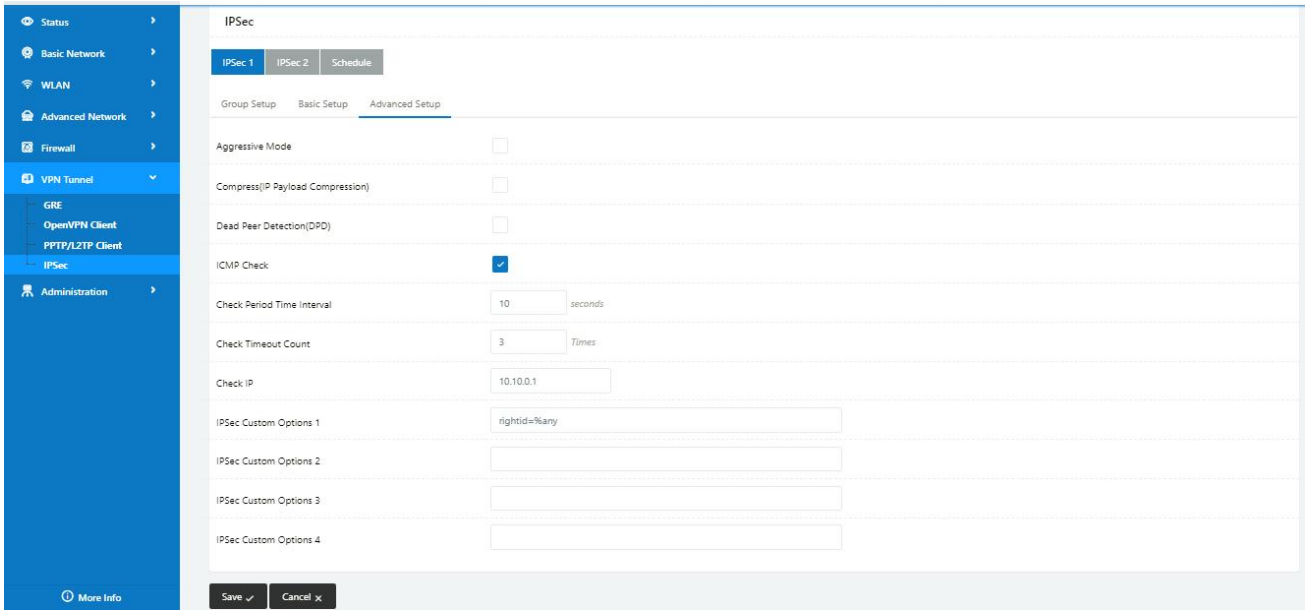
Navigate to **VPN Tunnel > IPSec > Group Setup**

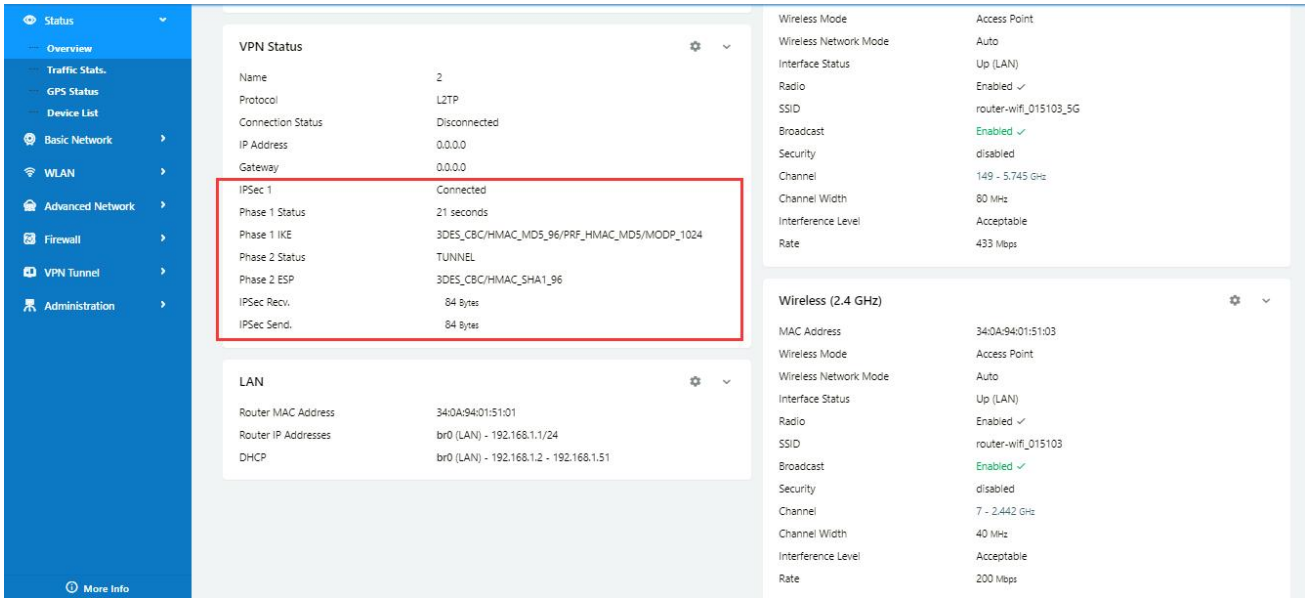


Navigate to **VPN Tunnel > IPSec > Basic Setup**



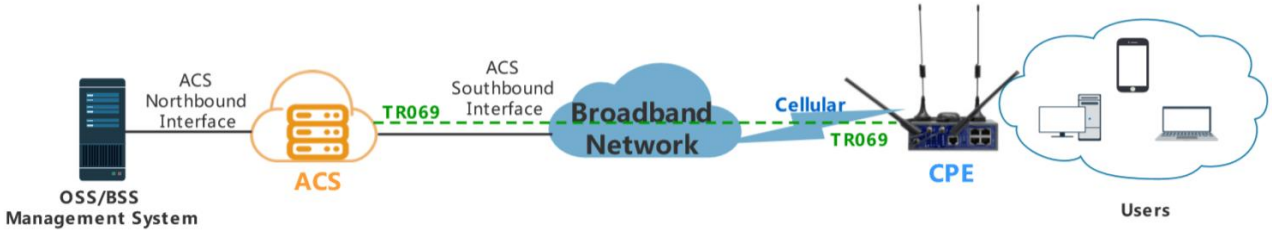
Navigate to **VPN Tunnel > IPSec > Advanced Setup**





3.10 TR-069

ACS and WL-G510 communicate through the RPC methods of TR069 protocol.

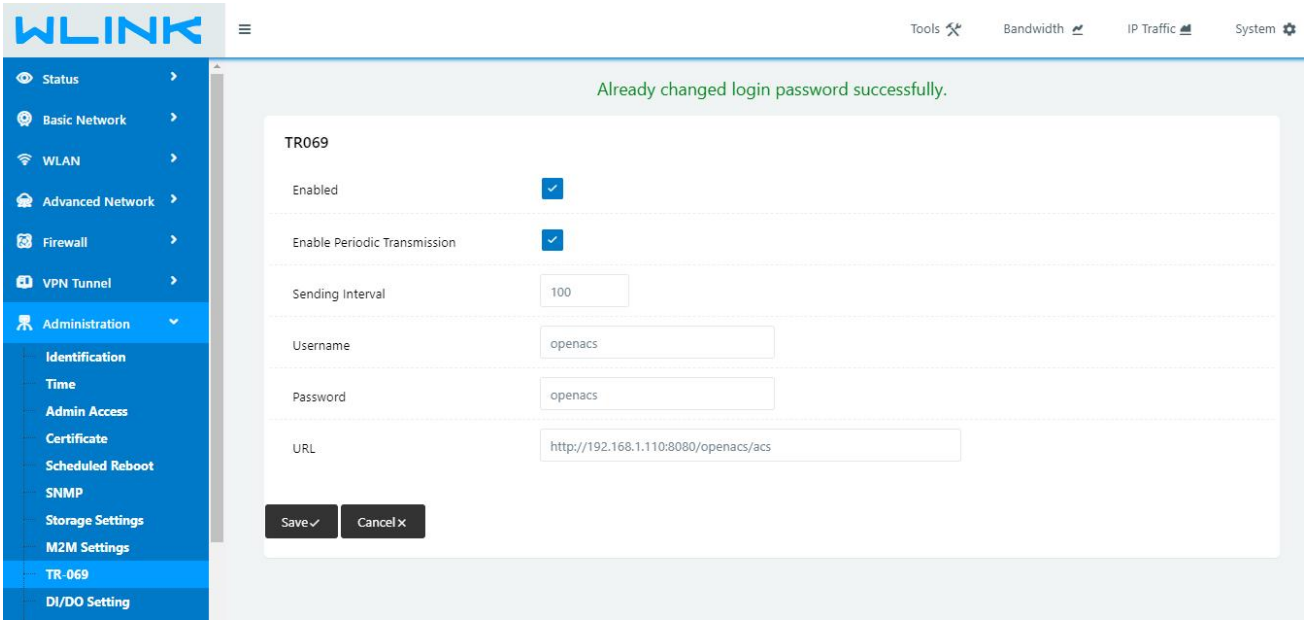


The following features are currently supported in the standard firmware for the WLINK

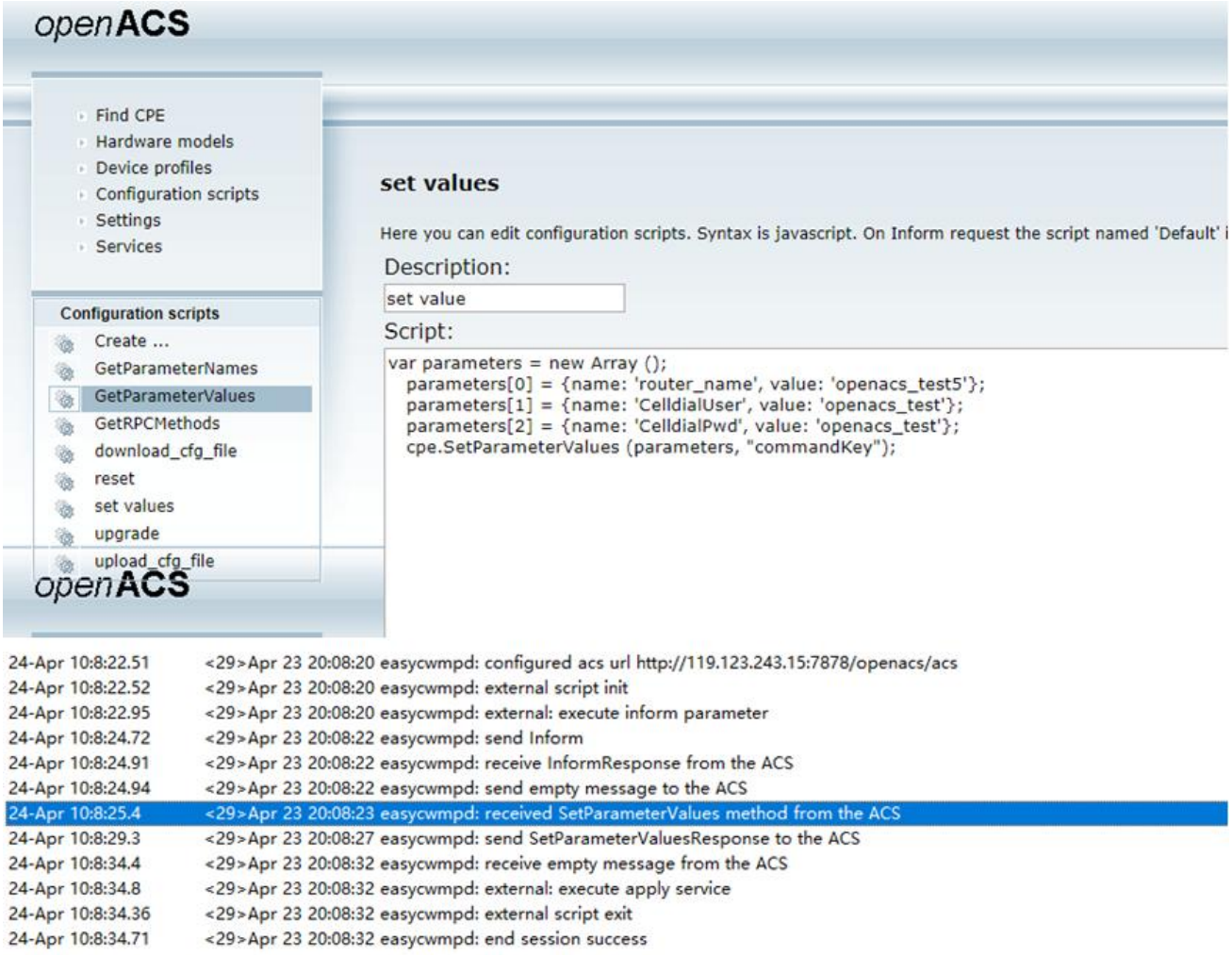
family routers

(**Note**: We also support customizing the TR069 and TR098 data-model into the firmware to support more features)

- SetParameterValues
- GetParameterValues
- Reboot
- Download
- Upload
- FactoryReset

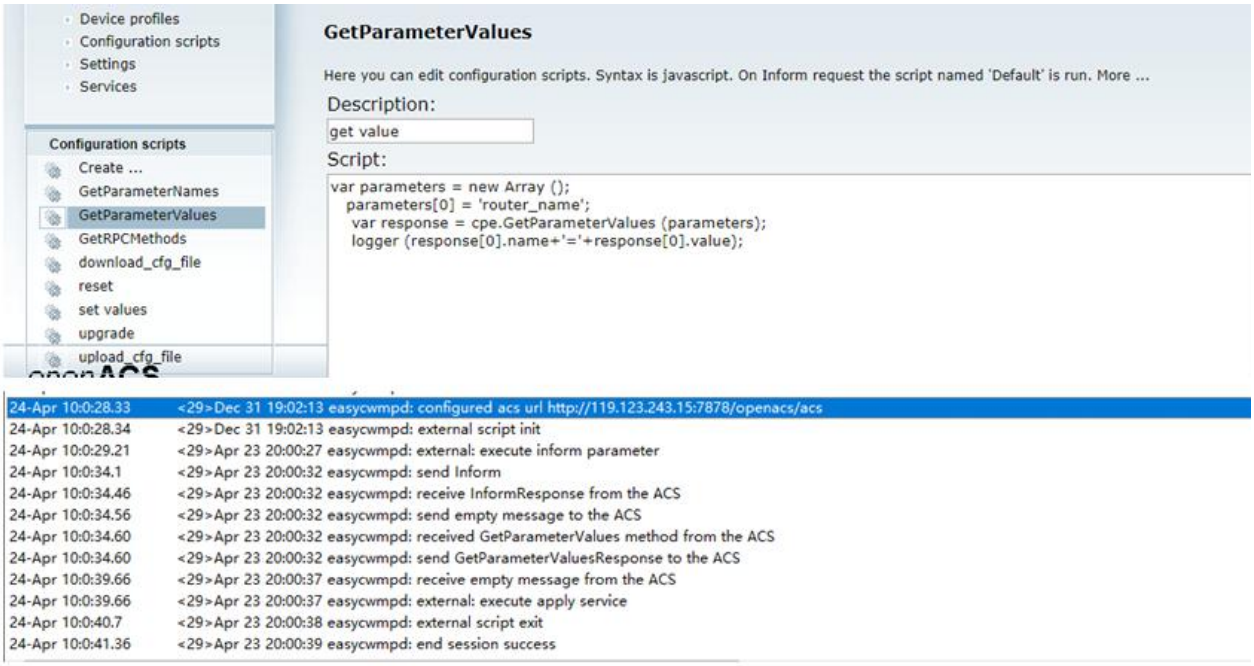


1) SetParameterValues



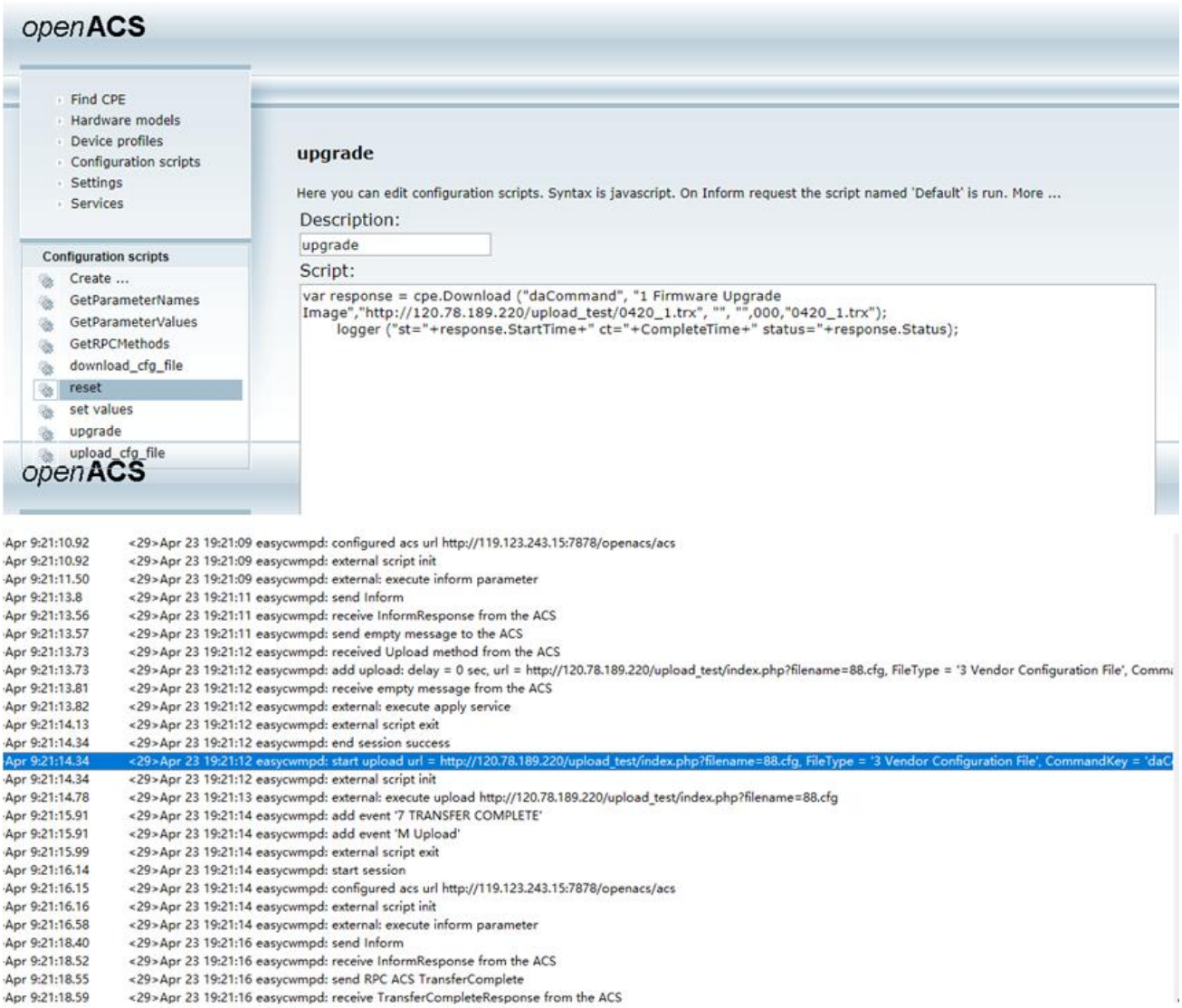

```
24-Apr 10:8:22.51   <29>Apr 23 20:08:20 easycwmpd: configured acs url http://119.123.243.15:7878/openacs/acs
24-Apr 10:8:22.52   <29>Apr 23 20:08:20 easycwmpd: external script init
24-Apr 10:8:22.95   <29>Apr 23 20:08:20 easycwmpd: external: execute inform parameter
24-Apr 10:8:24.72   <29>Apr 23 20:08:22 easycwmpd: send Inform
24-Apr 10:8:24.91   <29>Apr 23 20:08:22 easycwmpd: receive InformResponse from the ACS
24-Apr 10:8:24.94   <29>Apr 23 20:08:22 easycwmpd: send empty message to the ACS
24-Apr 10:8:25.4    <29>Apr 23 20:08:23 easycwmpd: received SetParameterValues method from the ACS
24-Apr 10:8:29.3    <29>Apr 23 20:08:27 easycwmpd: send SetParameterValuesResponse to the ACS
24-Apr 10:8:34.4    <29>Apr 23 20:08:32 easycwmpd: receive empty message from the ACS
24-Apr 10:8:34.8    <29>Apr 23 20:08:32 easycwmpd: external: execute apply service
24-Apr 10:8:34.36   <29>Apr 23 20:08:32 easycwmpd: external script exit
24-Apr 10:8:34.71   <29>Apr 23 20:08:32 easycwmpd: end session success
```

2) GetParameterValues



3) Download, the router downloads the configuration parameters

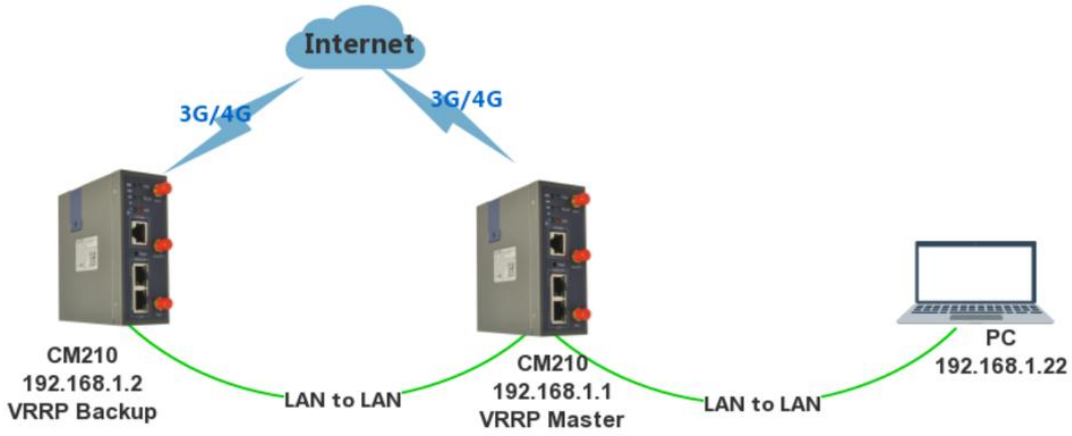
4) Upload, after uploading the router firmware, the router will automatically upgrade and restart



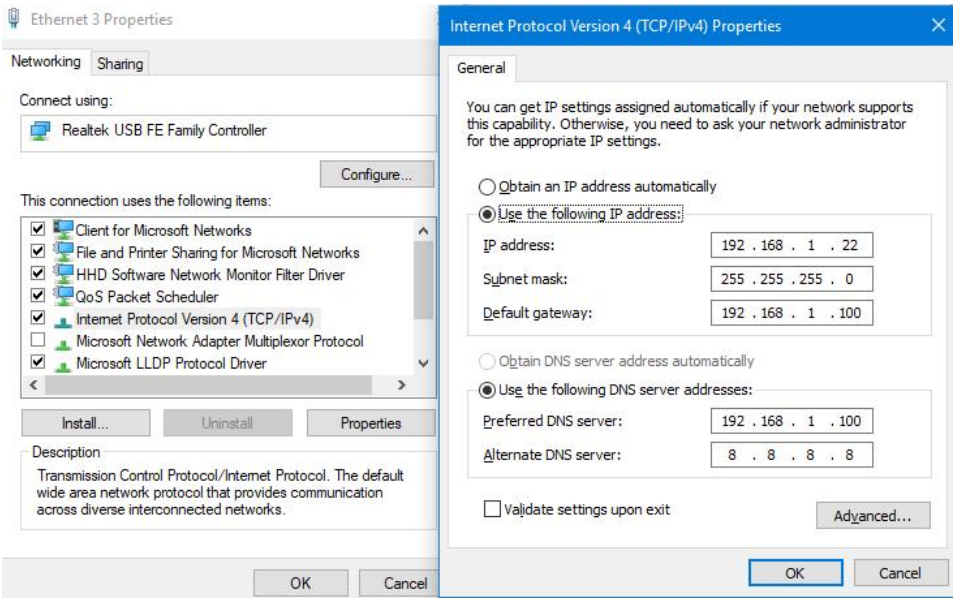
---End

3.11 VRRP

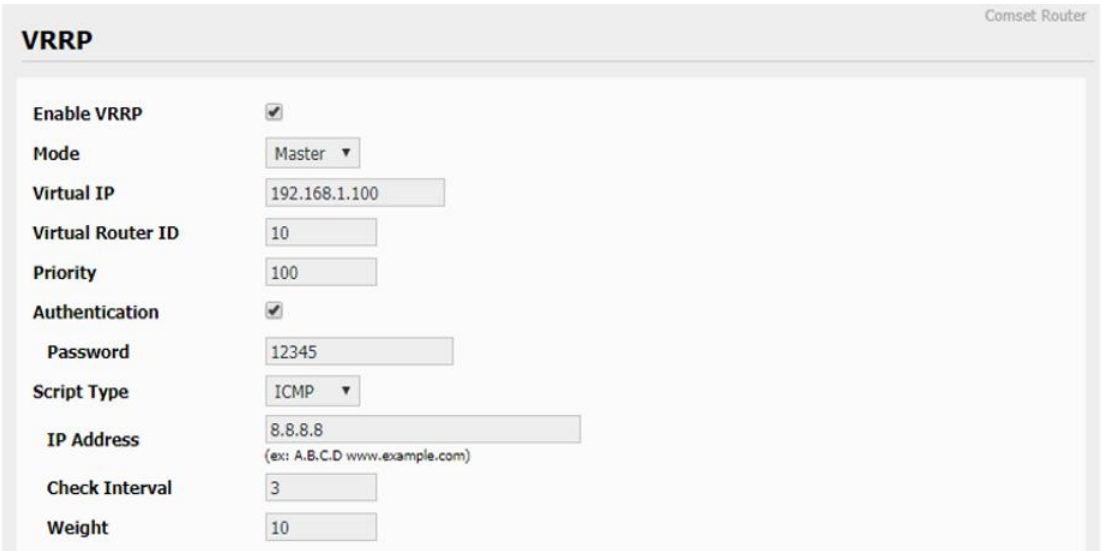
Configuring VRRP in two WLINK routers



PC Ethernet

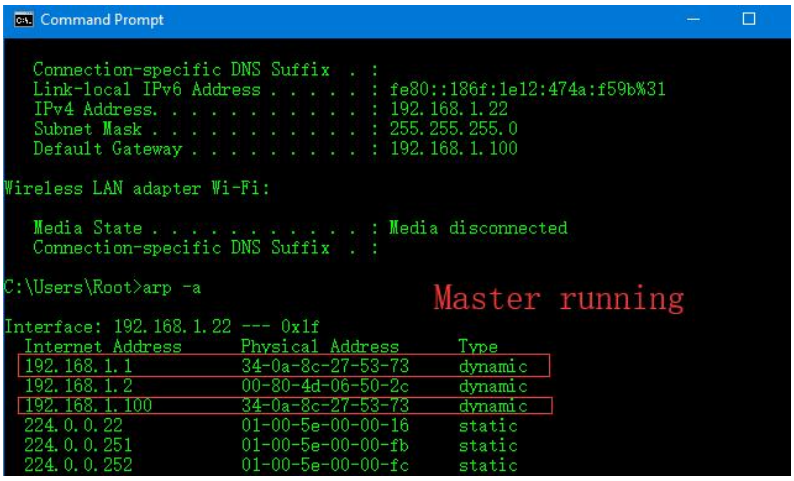


Master router config

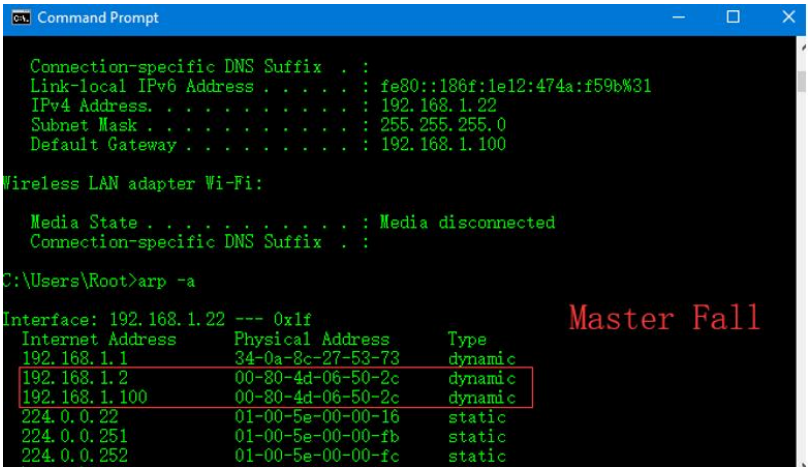


Backup router config

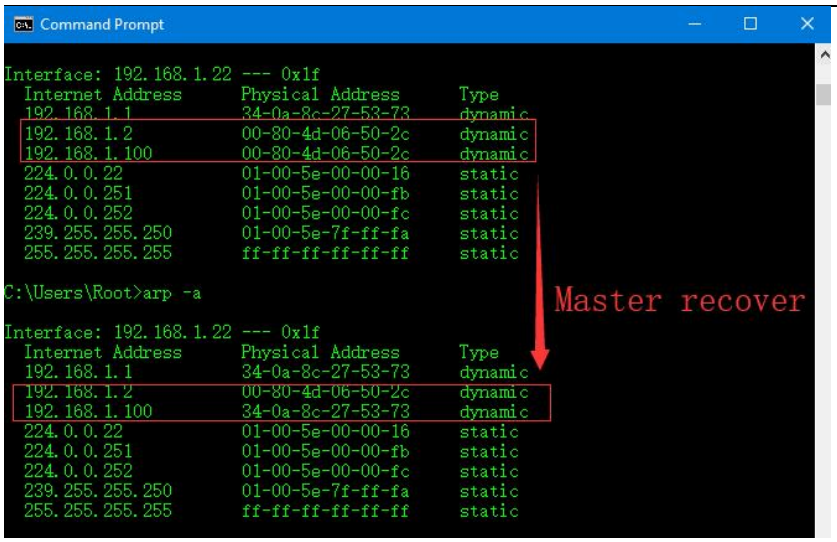
1) Normally, the master router running



2) When master router down, backup router up



3) When master router is restored


Command Prompt
Interface: 192.168.1.22 --- 0x1f
Internet Address Physical Address Type
192.168.1.1 34-0a-8c-27-53-73 dynamic
192.168.1.2 00-80-4d-06-50-2c dynamic
192.168.1.100 00-80-4d-06-50-2c dynamic
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\Root>arp -a
Master recover
Interface: 192.168.1.22 --- 0x1f
Internet Address Physical Address Type
192.168.1.1 34-0a-8c-27-53-73 dynamic
192.168.1.2 00-80-4d-06-50-2c dynamic
192.168.1.100 34-0a-8c-27-53-73 dynamic
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static