User Manual

---Apply to WL-G230 Series Industrial 5G Router

V1.4

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	Firmware Version	Note
2026-1-23	V1.4	Gm.0.2.8-260123-112838.bin	Improved 5G module drivers.
2025-2-20	V1.3	Gm.0.2.7-250207-135951.bin	Improved 5G band Locker, M2M platform, OpenVPN Client.
2024-3-20	V1.2	Gm.0.2.6-240318-171238.bin	Add Wireguard VPN, IPv6 features.
2023-1-6	V1.1	Gm.0.2.2-221202-164017	Improve Configuration Restore. Add Configuration Instances.
2022-3-15	V1.0	Gx.0.2.1-220326-105136	

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

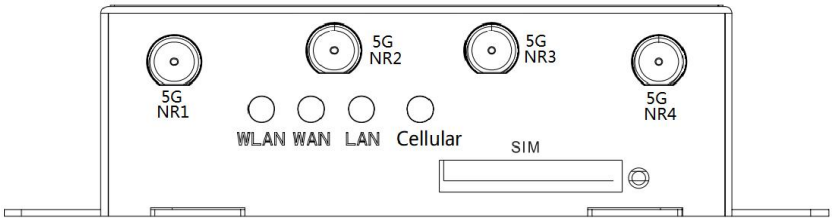
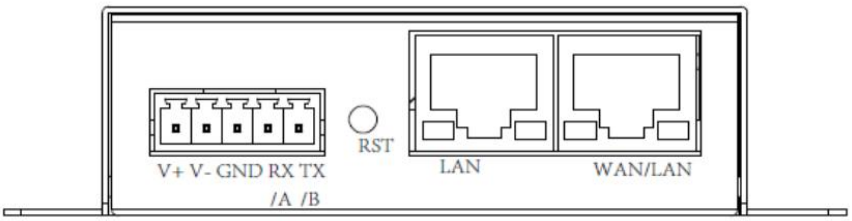
Contents

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-G230 Structure

WLINK Tech.	G230 series
Front	
Back	

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
SIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection.	
5G Antennas	5G NR1~5G NR4 antenna, SMA connector, 50Ω.	

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

1.2 LED Status

Table 1-3 Router LED indicator Status

silk-screen	Indicator		Note
Cellular	Color	Green	Good Signal
		Red	Poor Signal
	Status	Quick Blinking (0.5s)	Offline
		Slow Blinking (1.5s)	5G Dialing
		Solid light	5G online
WLAN	Constant light		WLAN enable, but no data communication.
	Blinking quickly		Data in transmitting
	Light off		WLAN disable
LAN/WAN	Green	Constant light	Connected.
	Green	Blinking	Data in transmitting.
	Green	Light off	Disconnection.

1.3 Dimension

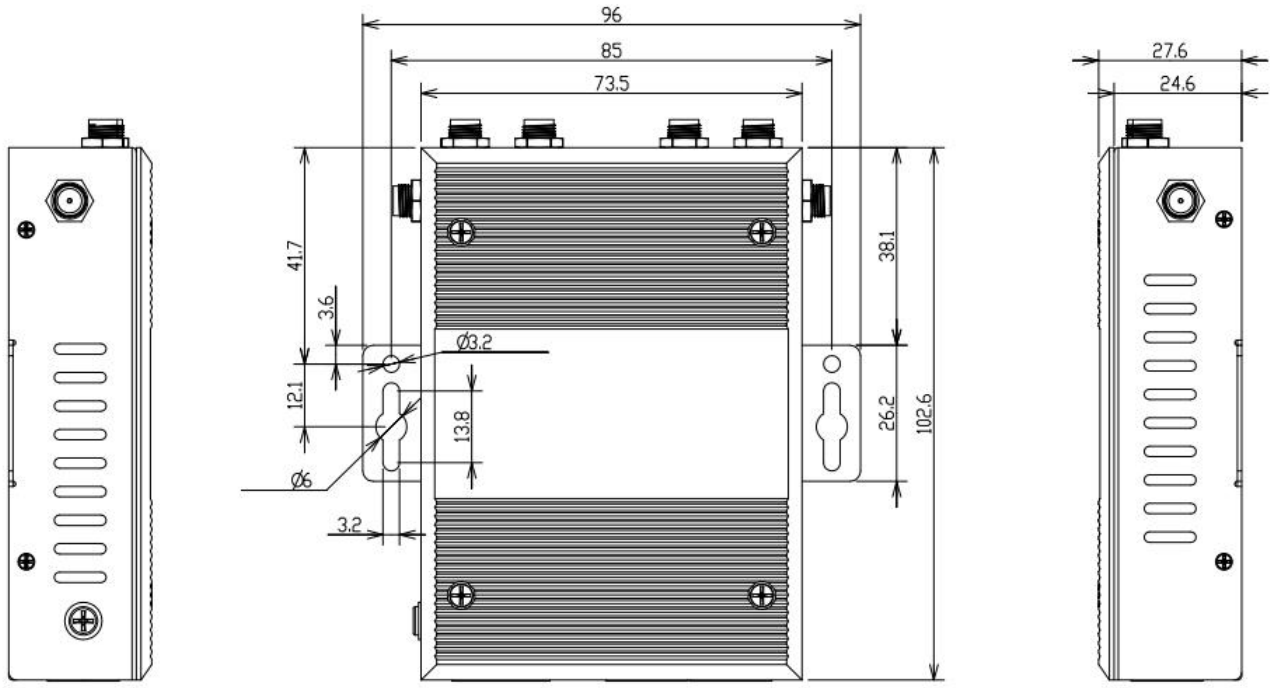
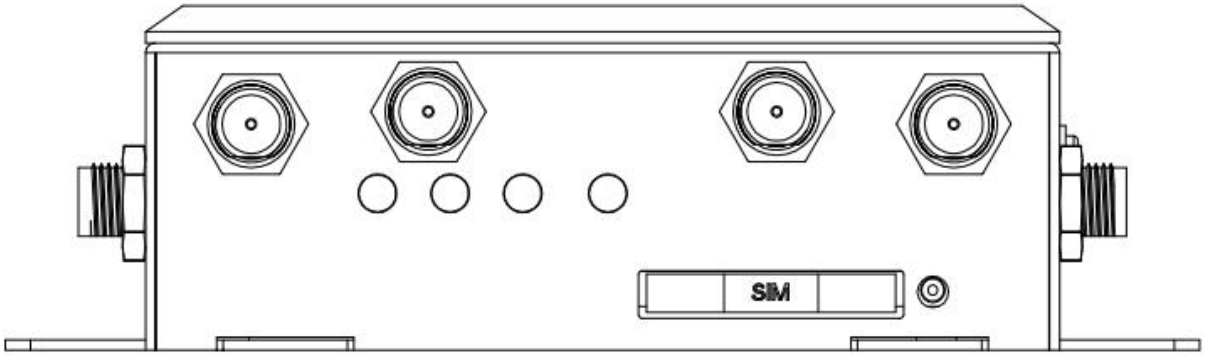


Figure 1-2 G230 Series Router Dimension

1.4 How to Install

1.4.1 SIM/UIM card install

Put the SIM card onto SIM tray and plug tray into slot before configured the router.



CAUTION

Before connecting, please disconnect any power resource of router

1.4.2 Ethernet Cable Connection

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

1.4.3 5G and Wi-Fi Antenna Plug

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

NOTE

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

1.4.6 Power Supply

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

1.4.7 Review

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

CAUTION

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

Notice:

Step 1 Check the antenna connection.

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

Step 3 Power on the industrial Router

----END

2 Router Configuration

WL-G230 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.

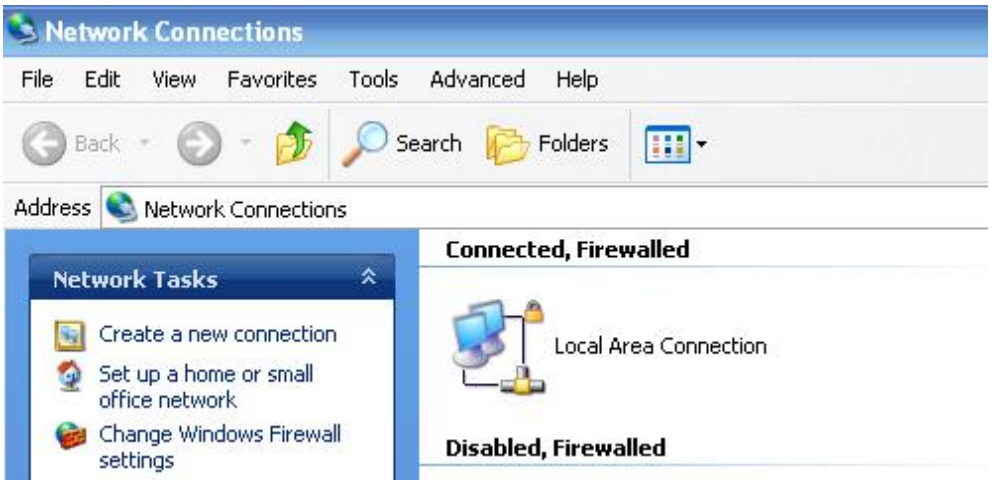


Figure 2-1 Network Connection

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

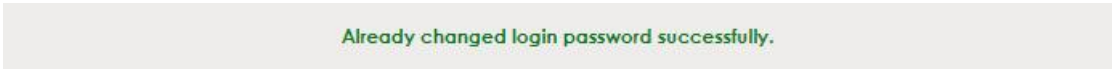
Figure 2-2 User Identify Interface

----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, 5G connection information and WLAN information,

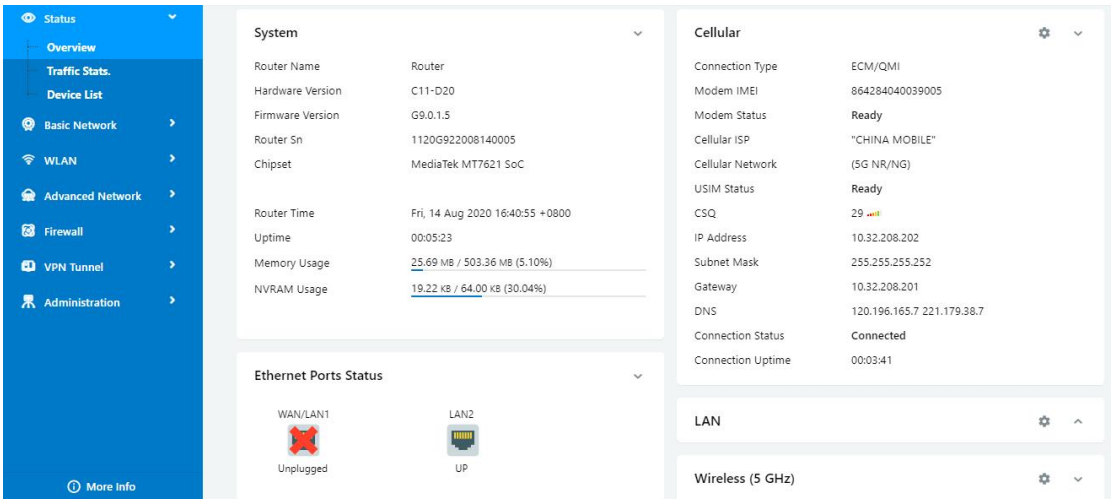


Figure 2-3 Router Status GUI

2.2.2 Traffic Stats.

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

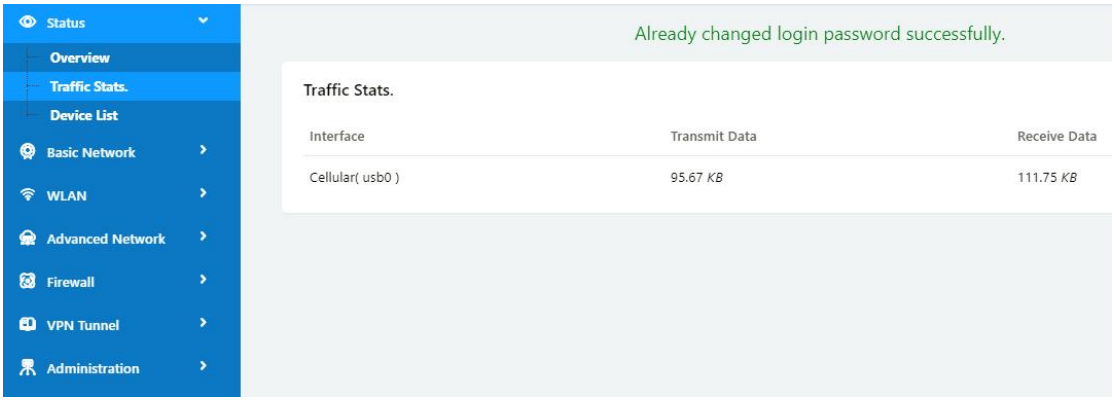


Figure 2-4 Traffic Stats. GUI

2.2.3 Device List

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

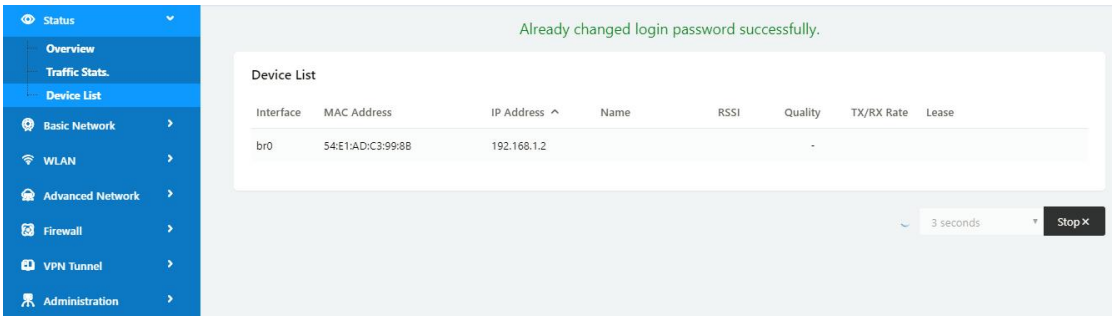


Figure 2-5 Device List GUI

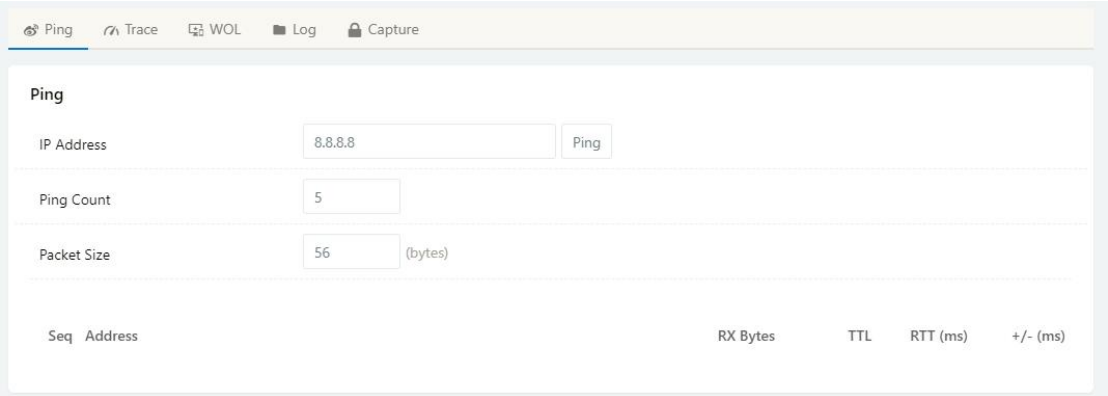
2.3 Tool Column

Figure 2-6 Tool Column GUI

2.3.2 Tools

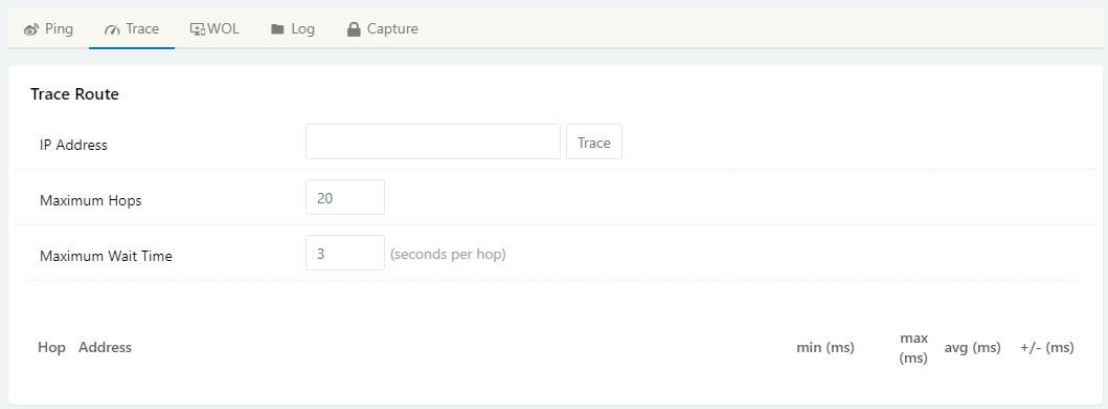
2.3.2.1 Ping

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



2.3.2.2 Trace

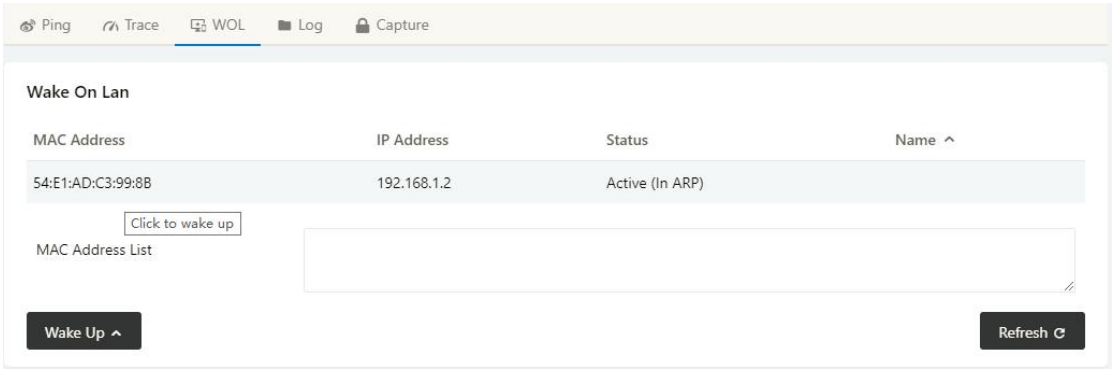
Click Tools->Trace to enter trace test GUI. diagnostic tool for displaying the route and measuring transit delays of packets across an Internet IP network.



2.3.2.3 WOL

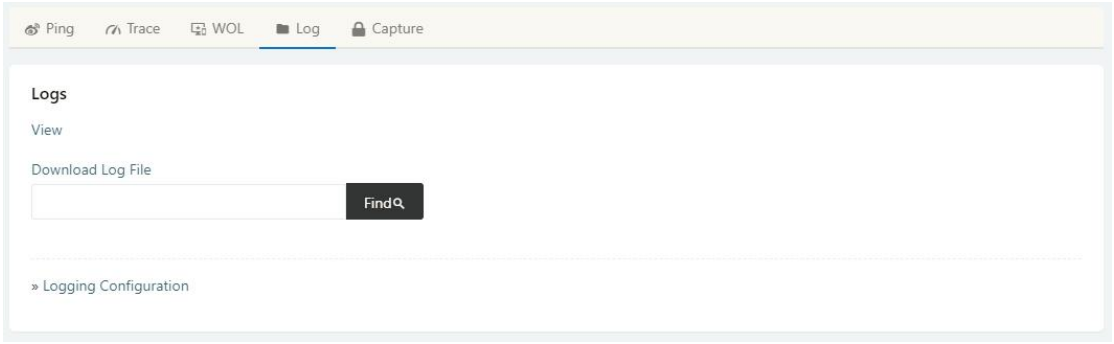
Click Tools-> WOL to enter WOL(Wake On Lan) GUI. Used to wake up those connected devices via WOL protocol.

Clock left mouse button to wake up the device.



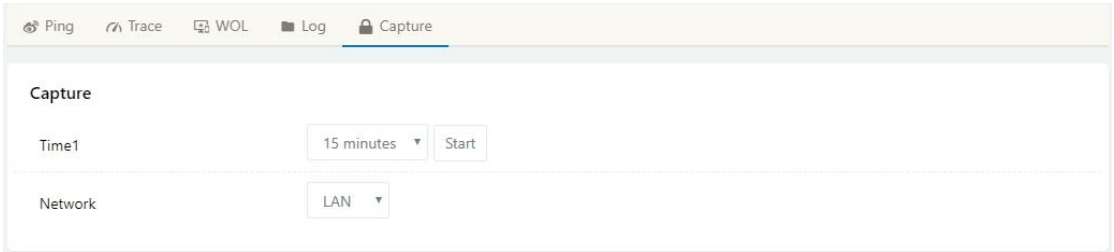
2.3.2.4 Log

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



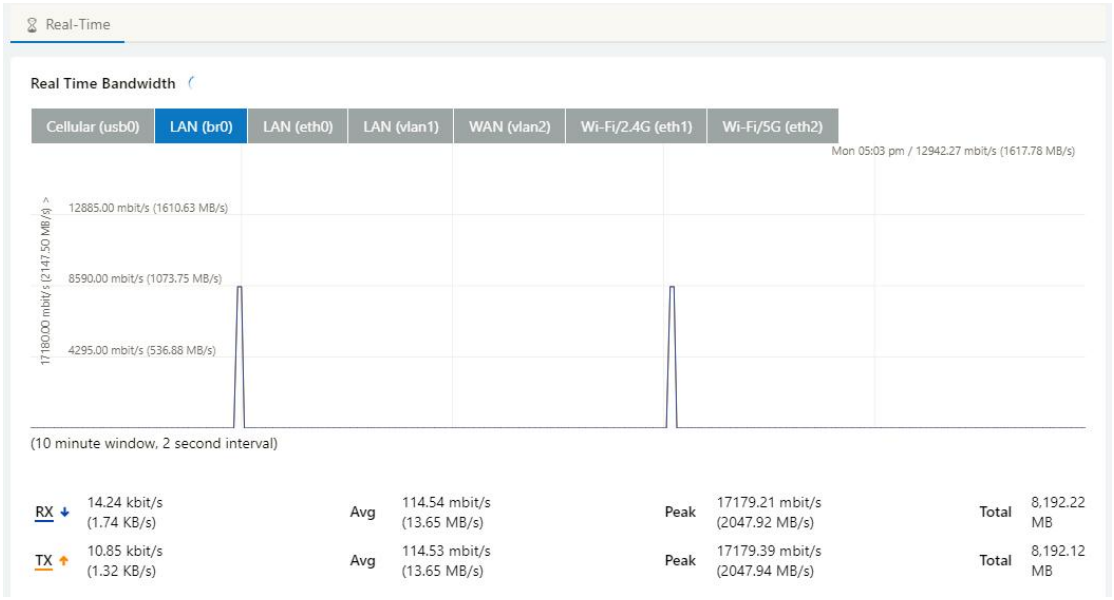
2.3.2.5 Capture

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.

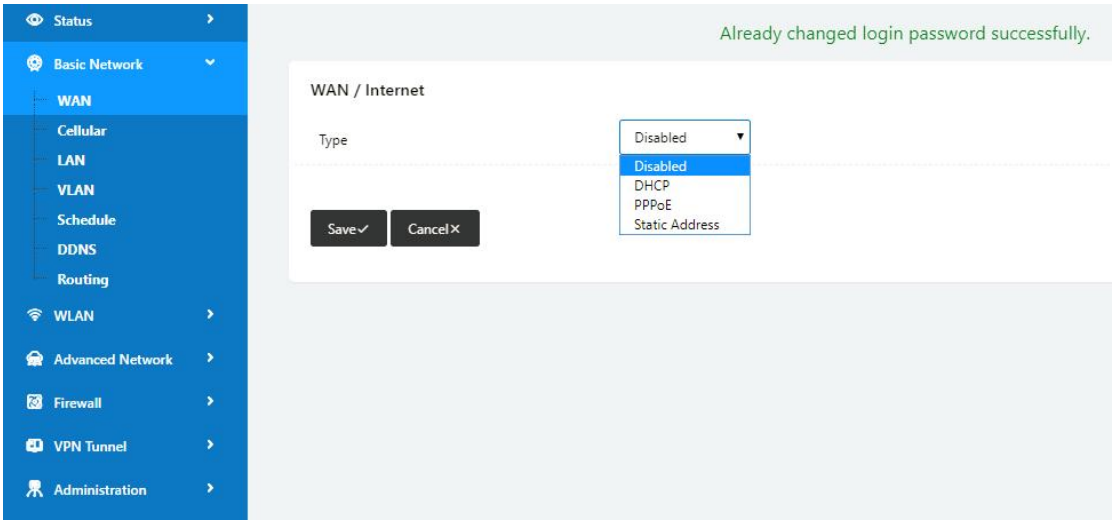


Table 2-1 WAN Setting Instruction

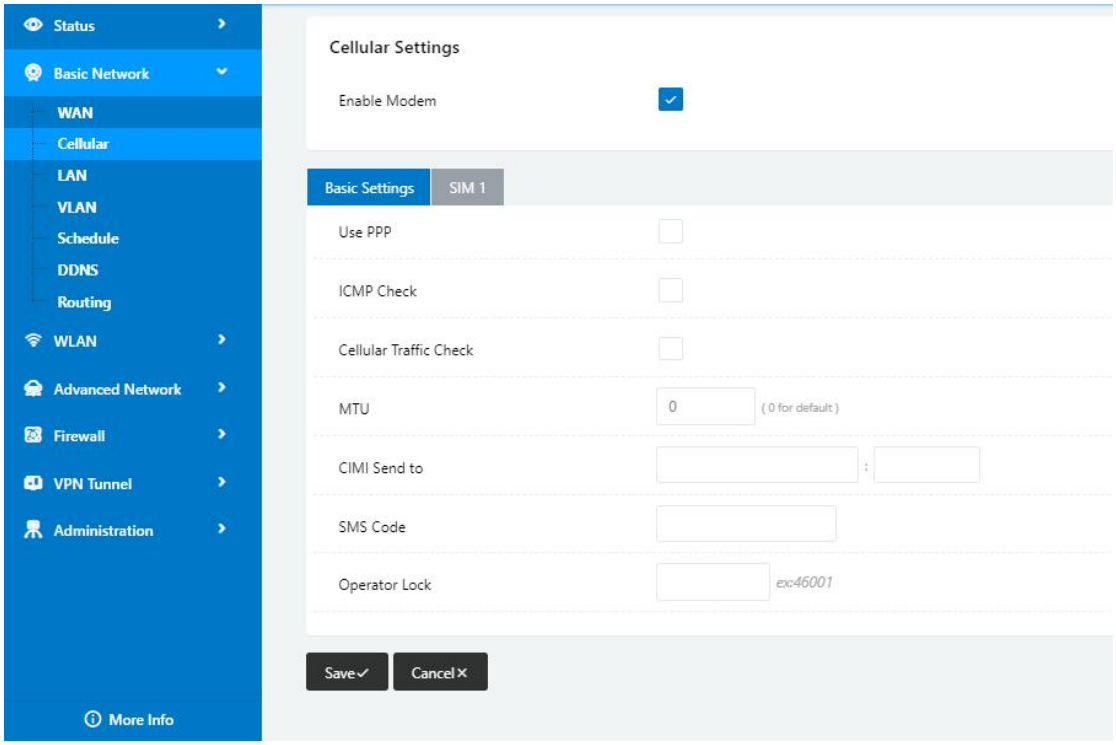
Parameter	Instruction	Default
Type	Support DHCP, PPPoE, Static IP address	Disable

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.



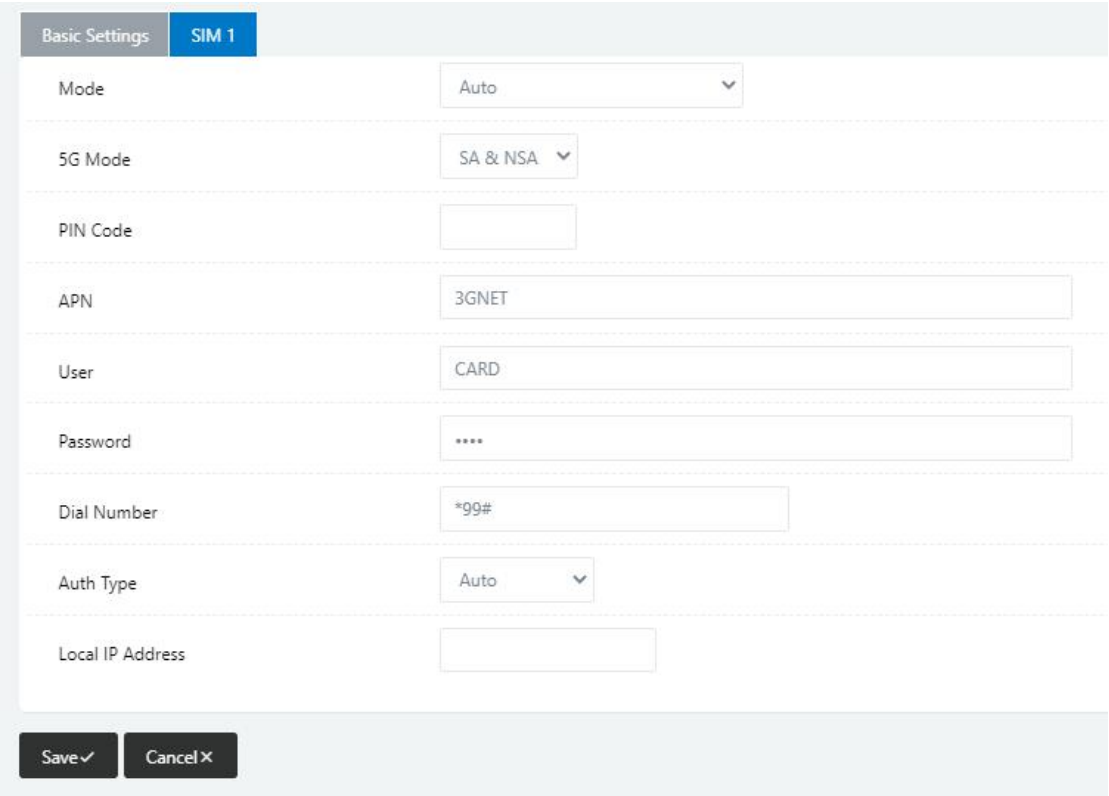


Table 2-2 WAN Setting Instruction

Parameter	Instruction	Default
Enable Modem	Enable/Disable 5G mode.	Enable
Use PPP	ECM dialup as default. PPP is suitable for 4G connection only.	Disable
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.	
MTU	MTU configurable. 0 as default for MTU 1500	
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.	
Mode	【Auto】The router will automatically connect to 3G/4G/5G networks and give priority to 5G. 【5G NR】Router will connect to 5G only. 【LTE】Router will connect to 4G only.	

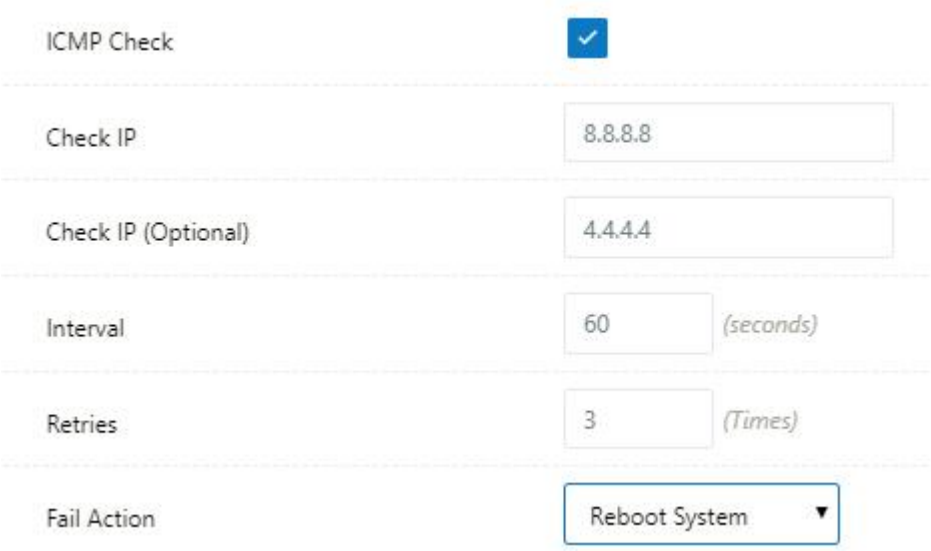
Parameter	Instruction	Default
	【3G】Router will connect to 3G only.	
5G Mode	SA, NSA, SA/NSA optional.	
Pin Code	Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen.	
APN	APN is provided by local ISP, usually CDMA/EVDO networks do not need this parameter.	
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.

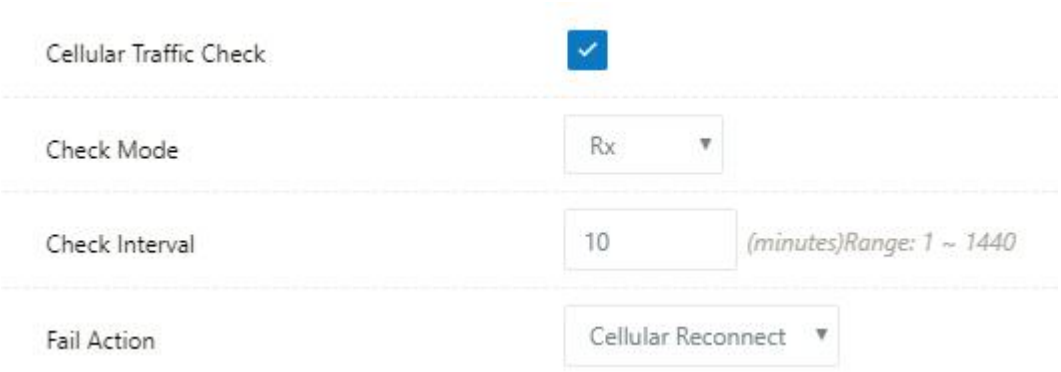
The ICMP Check IP is a public IP or company server IP address.



【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

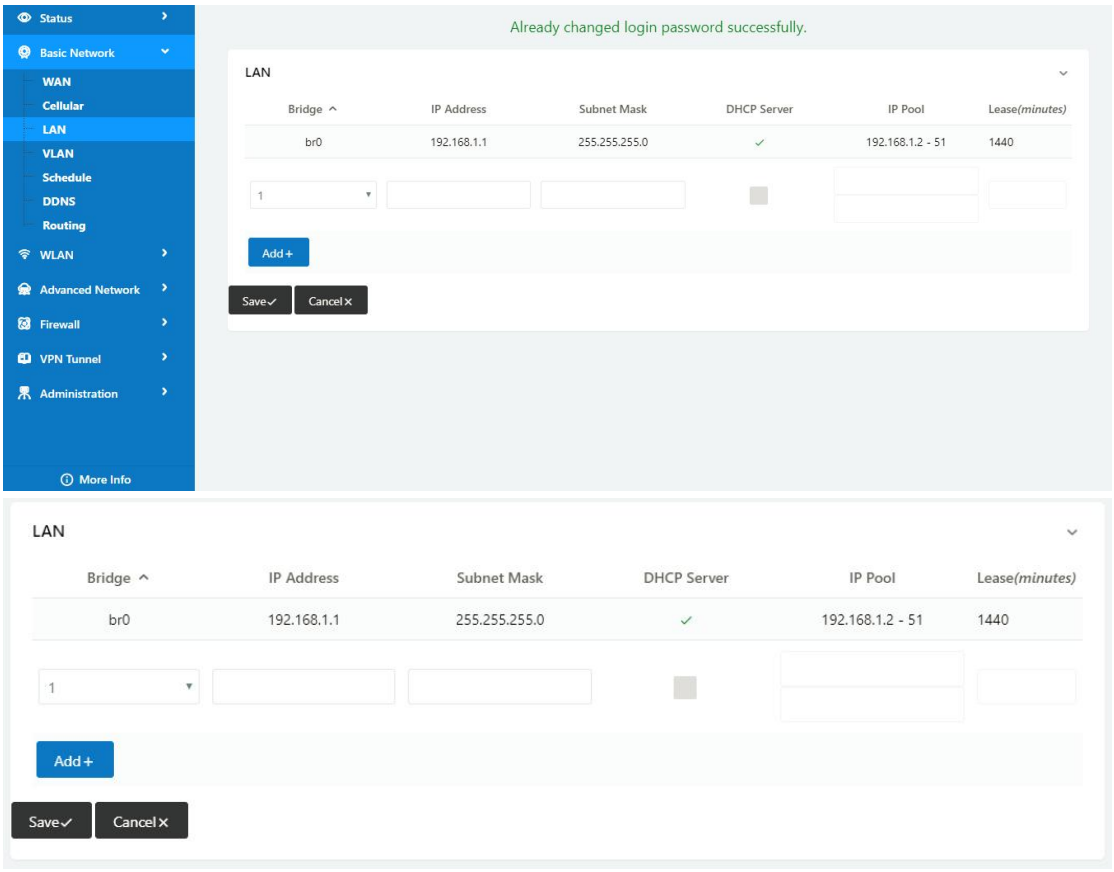


Table 2-3 LAN Setting Instruction

Parameter	Instruction	Default
Bridge	Supports 4 LAN IP address for br0 to br3 interface. If need to support VLAN, please go to VLAN GUI.	

Parameter	Instruction	Default
Router IP Address	Router IP address, default IP is 192.168.1.1	192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0	255.255.255.0
DHCP	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease	Enable
IP Pool	IP address range within LAN	192.168.1.2—51
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.

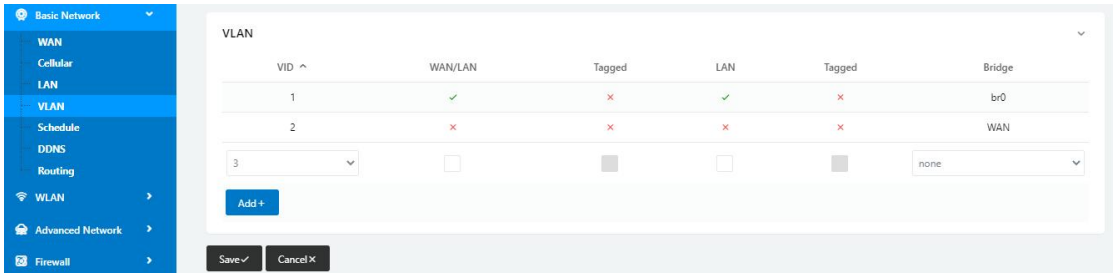


Table 2-4 LAN Setting Instruction

Parameter	Instruction	Default
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.

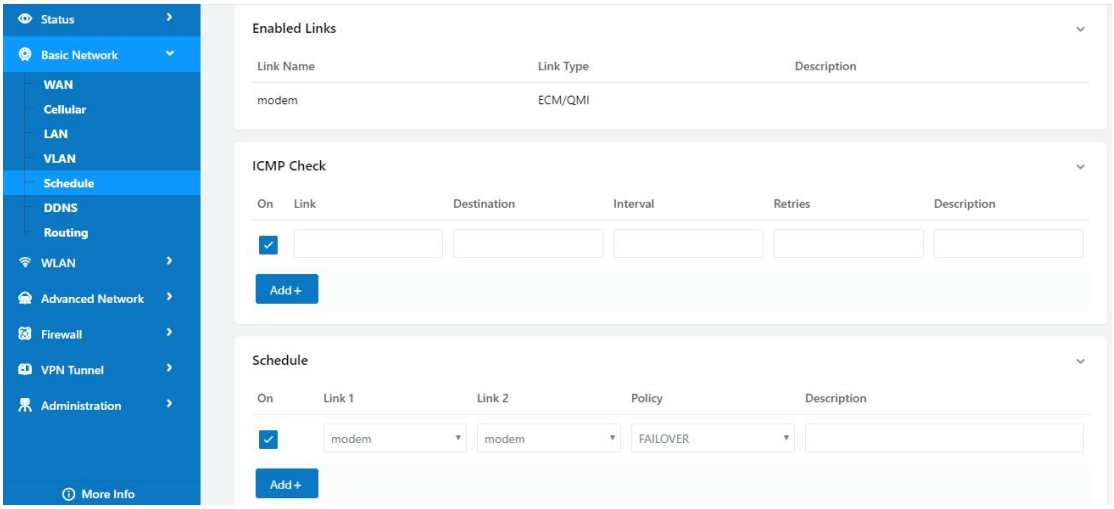
Configuration Instance

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

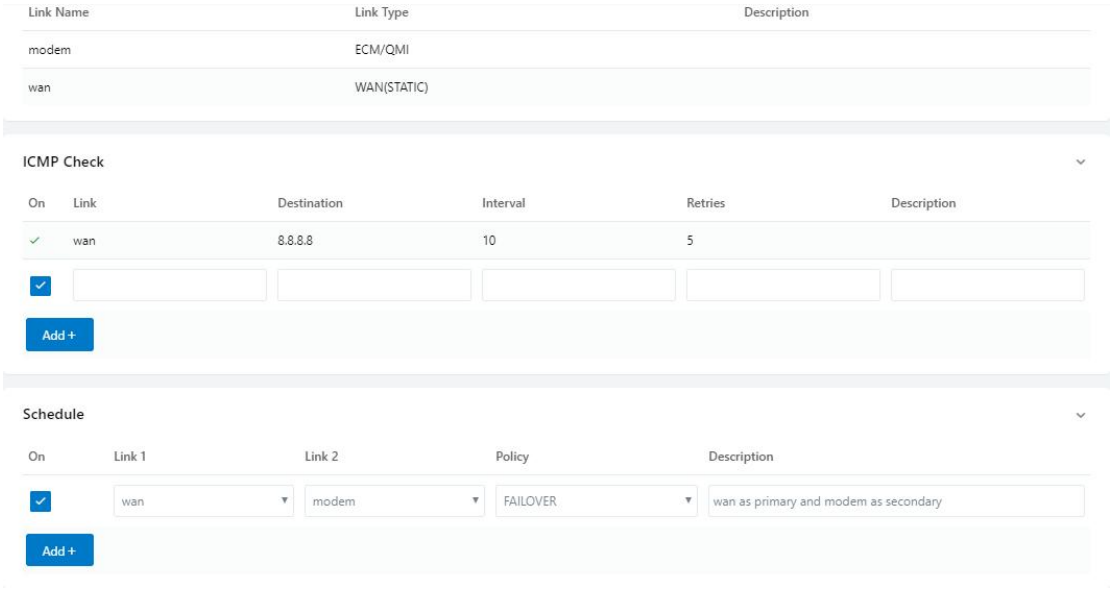
----End

2.4.5 Schedule

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

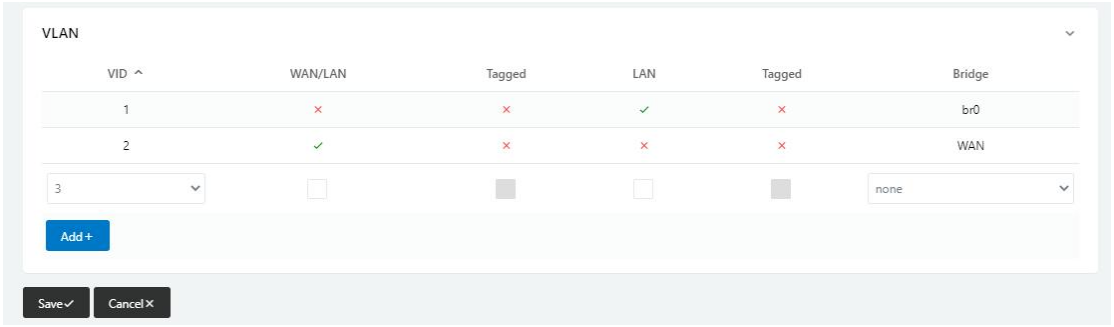


Parameters	Instruction	Default
modem	The router dial-up to network via modem	
wan	The router dial-up to network via WAN (DHCP, PPPOE, Static IP) port.	
ICMP Check	When the ICMP Check fails, the switching action between Link1 and Link2 will be triggered.	
Link1	The Primary link	
Link2	The Secondary link	
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 5G 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.

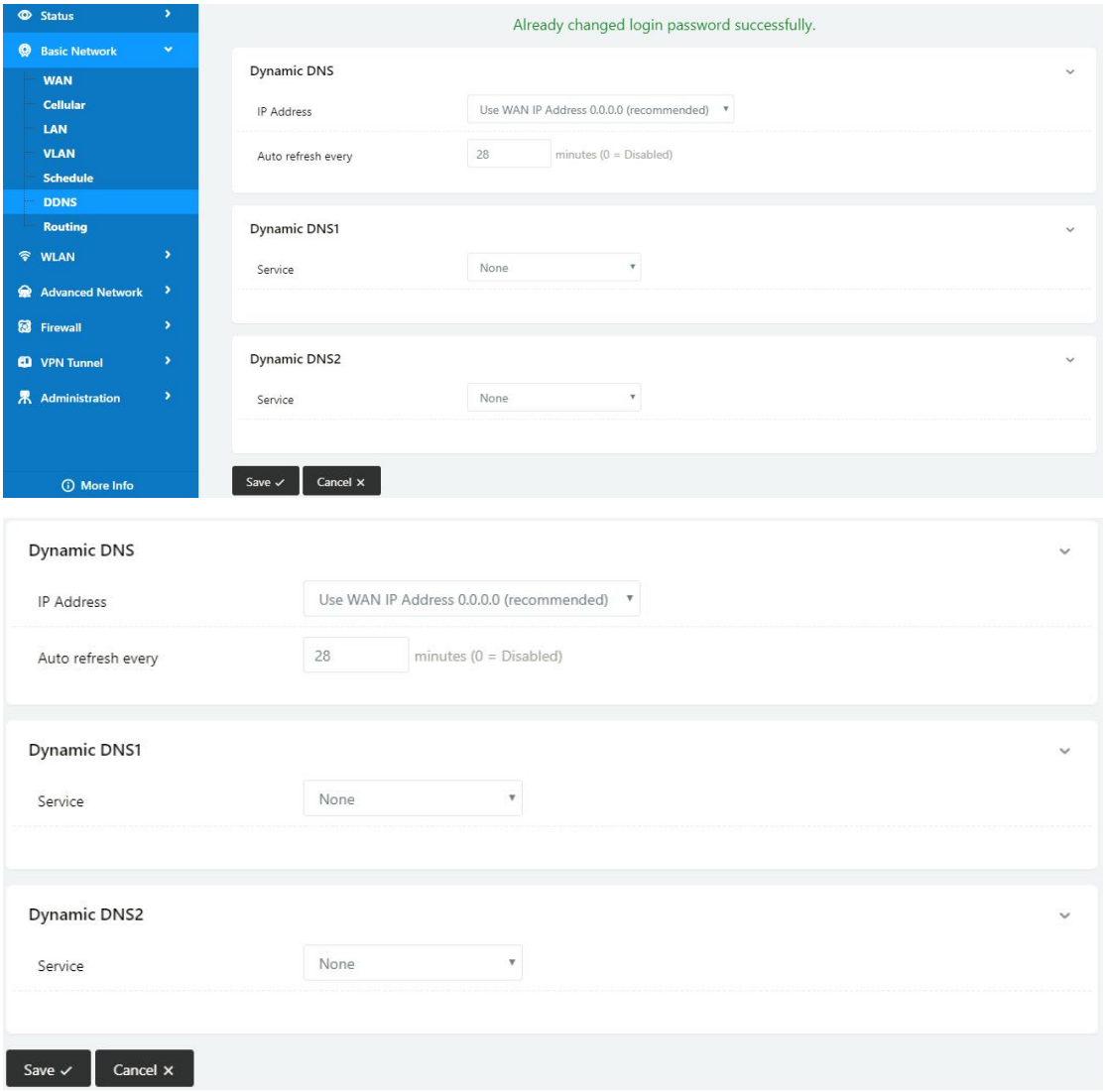


Table 2-5 DDNS Setting Instruction

parameter	Instruction	Default
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.

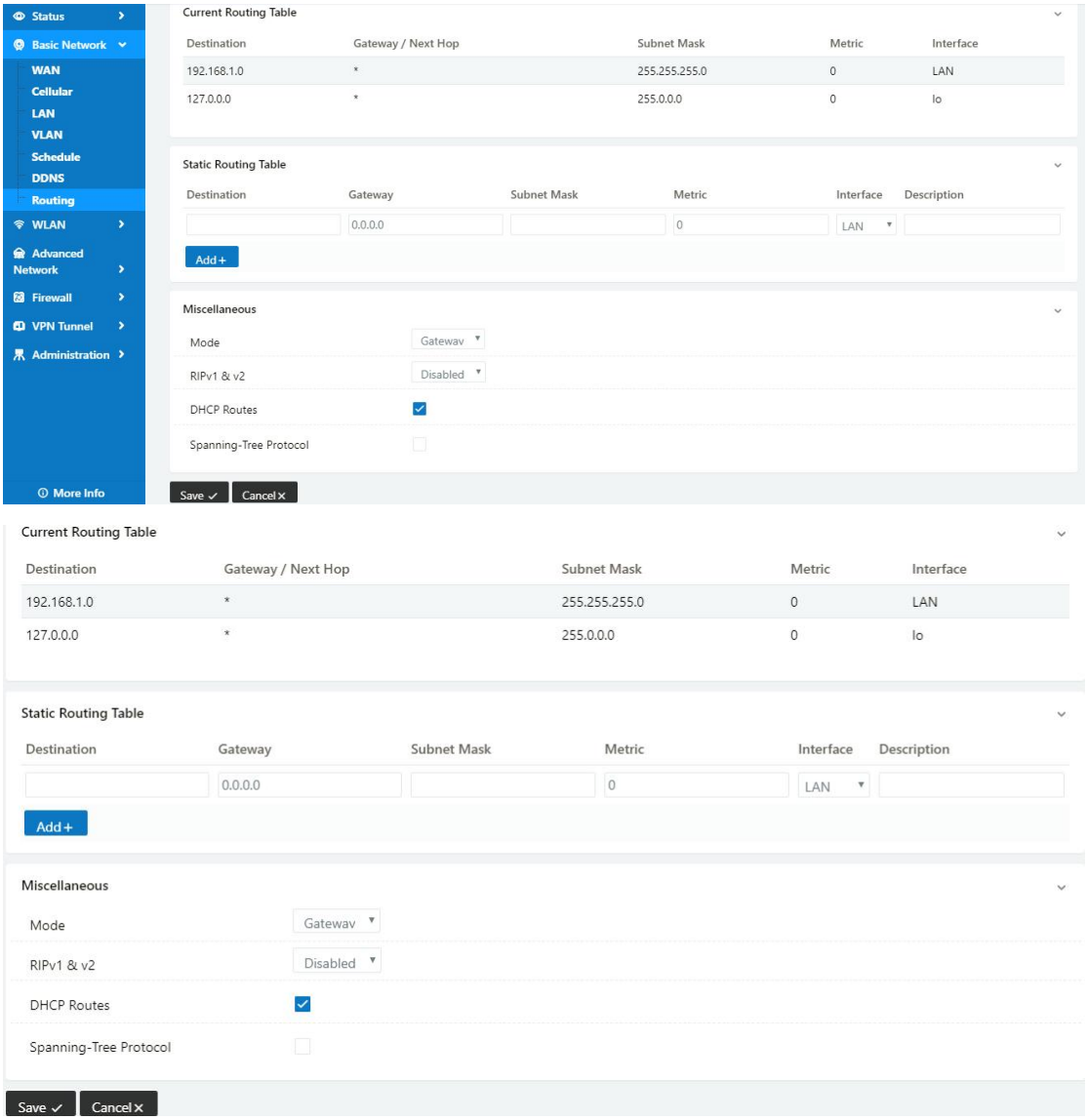


Table 2-6 Routing Setting Instruction

Parameter	Instruction	Default
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.

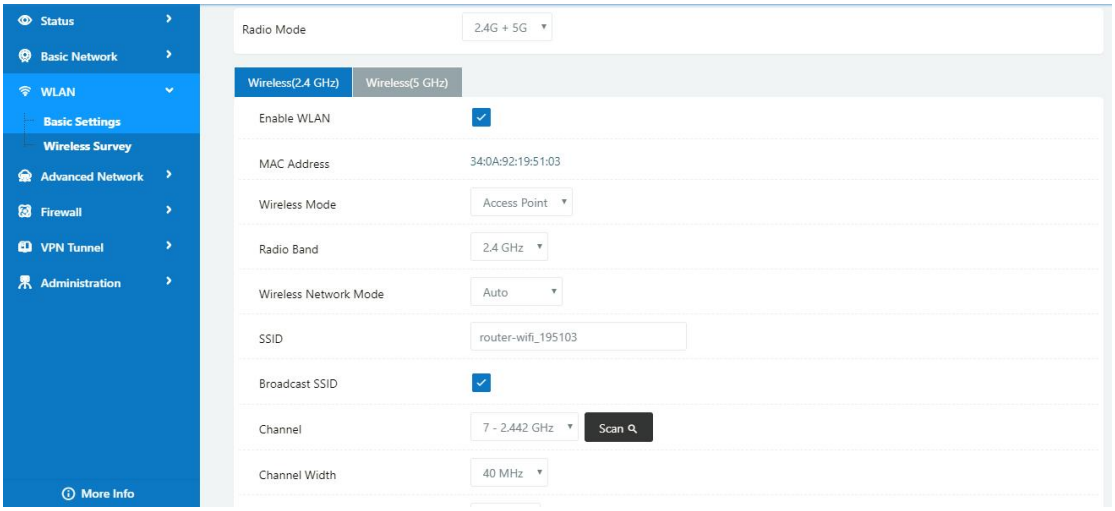
----End

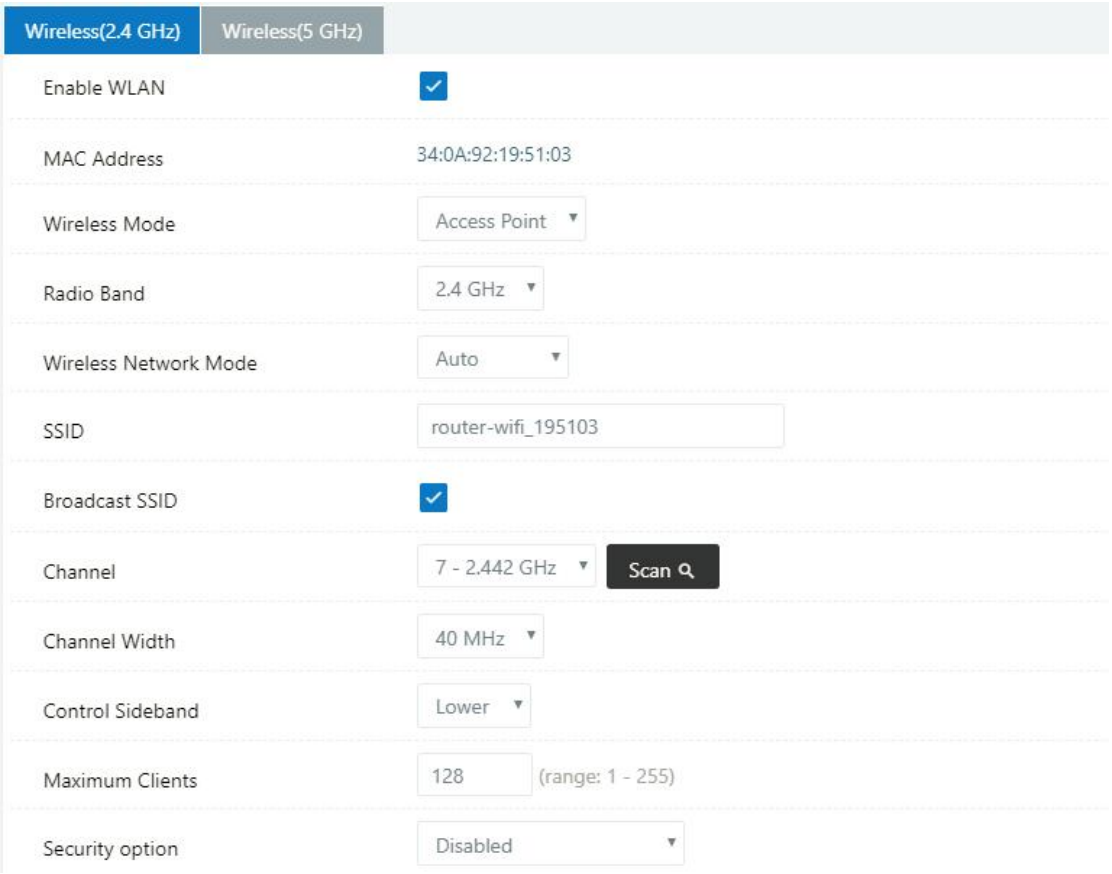
2.5 WLAN Setting

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





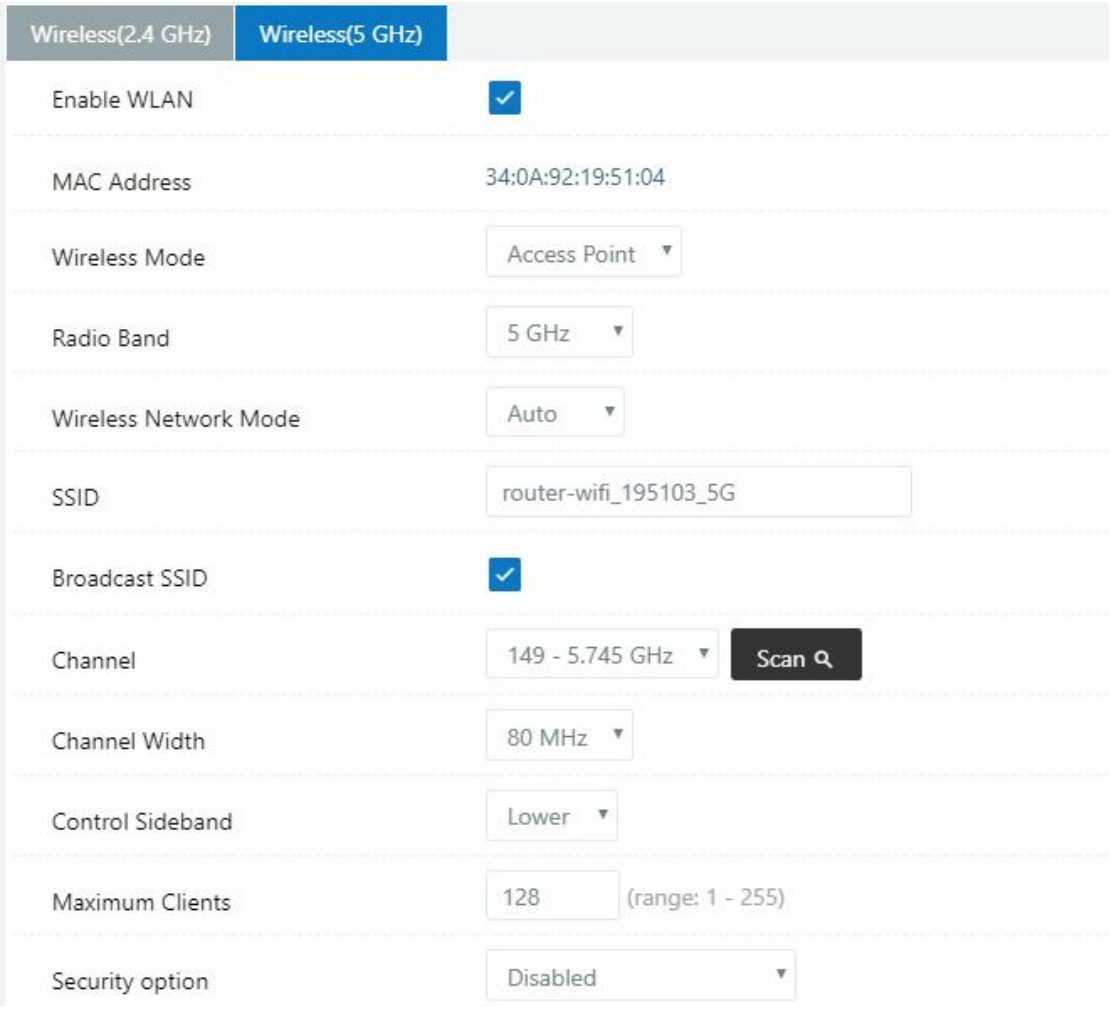


Table 2-7 Basic of WLAN Setting Instruction

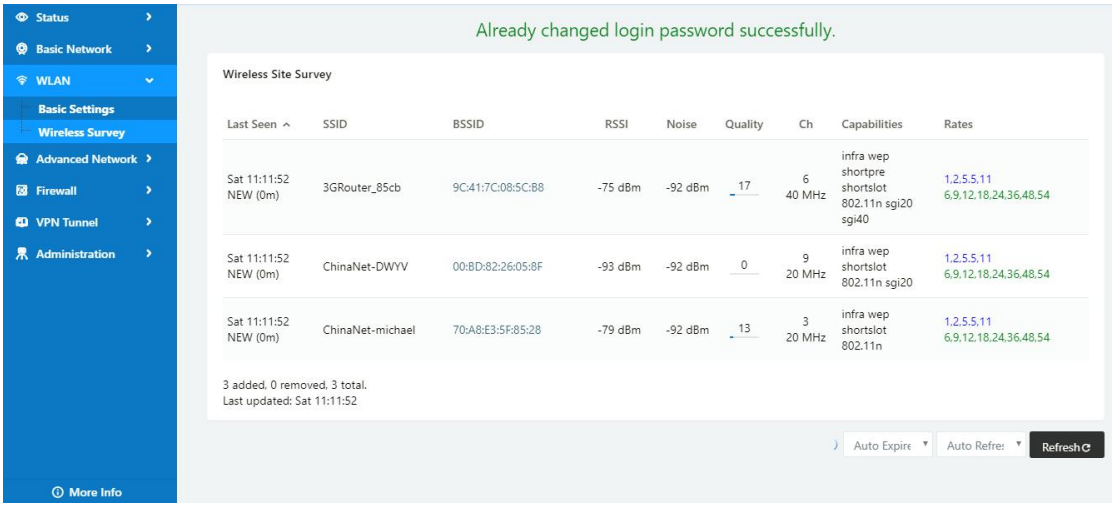
Parameter	Instruction	Default
Radio Mode	2.4G+5G mode as default. Support 2.4G, 5G modes optional. 2.4G+5G model, Wi-Fi bandwidth for 683Mbps 2.4G model, Wi-Fi bandwidth for 300Mbps 5G model, Wi-Fi bandwidth for 866Mbps	
Enable wireless	Enable or Disable the Wireless	
Wireless mode	Support AP mode and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

Step 2 Please click “Save” to finish.

----End

2.5.2 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.



2.6 Advanced Network Setting

2.6.1 Port Forwarding

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

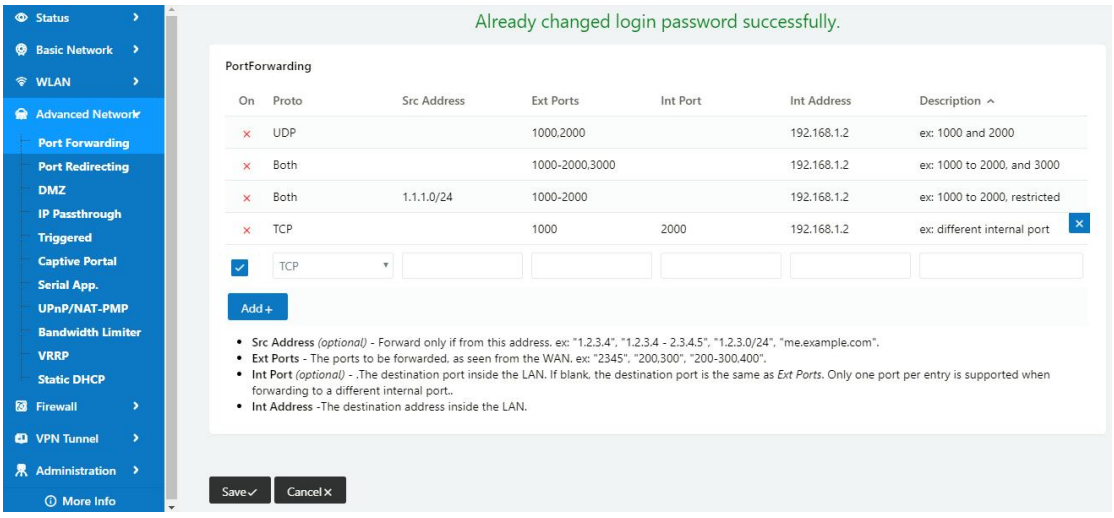


Table 2-8 Port Forwarding Instruction

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

Parameter	Instruction	Default
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.

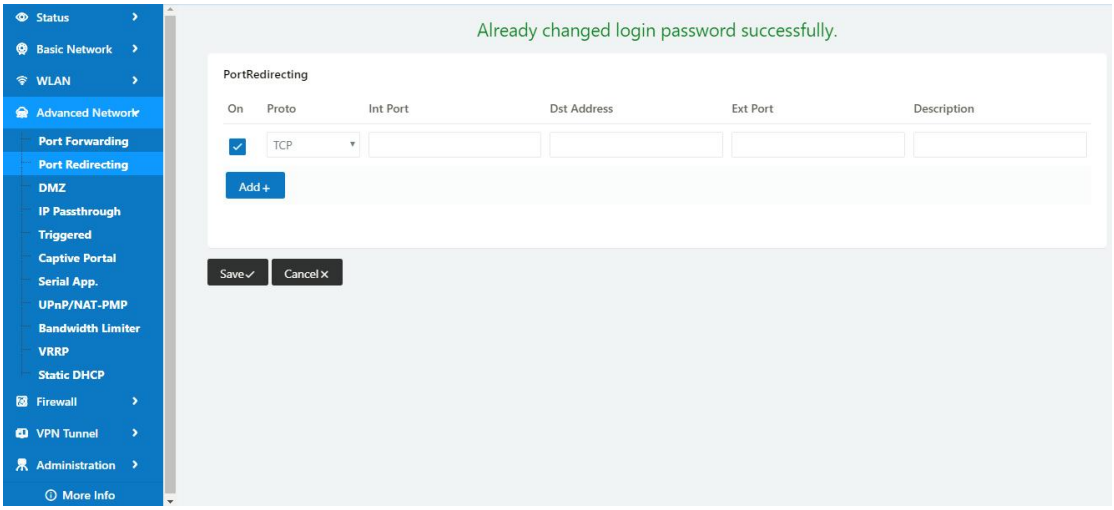


Table 2-9 Port Redirecting Instruction

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

Step 2 Please click ”save” to finish.

NOTE

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

Configuration Instance

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

----End

2.6.3 DMZ Setting

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

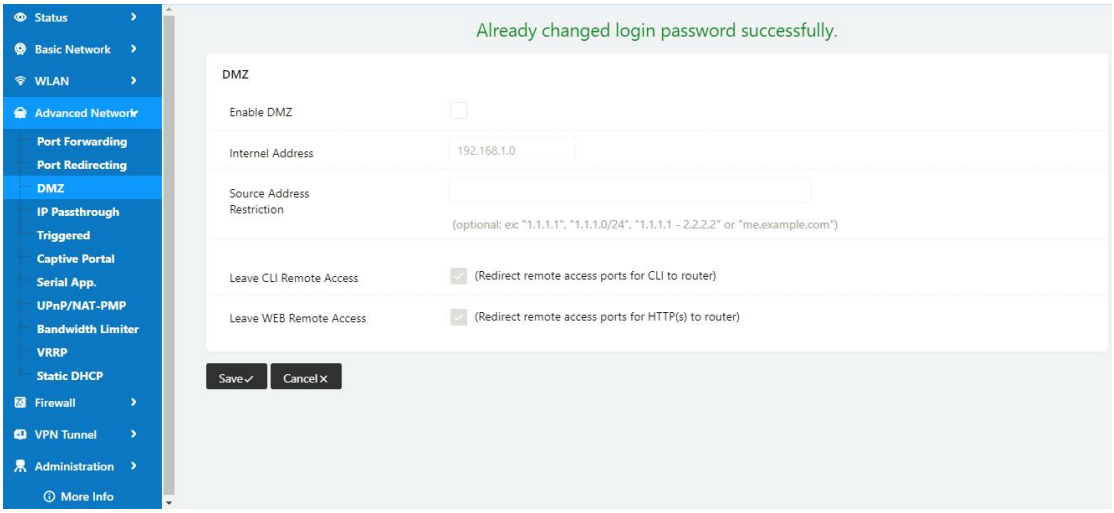


Table 2-10 DMZ Instruction

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

Step 2 Please click ”save” to finish

----End

2.6.4 IP Passthrough Setting

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

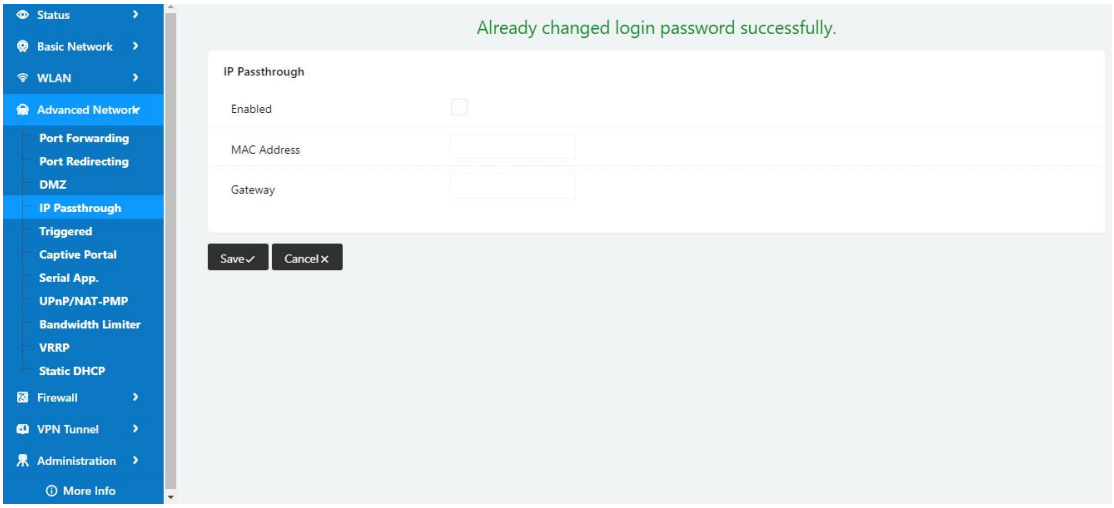


Table 2-11 IP Passthrough Instruction

parameter	Instruction	Default
Enable	Enable IP Passthrough	
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.	
Gateway	If WL-G230 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.

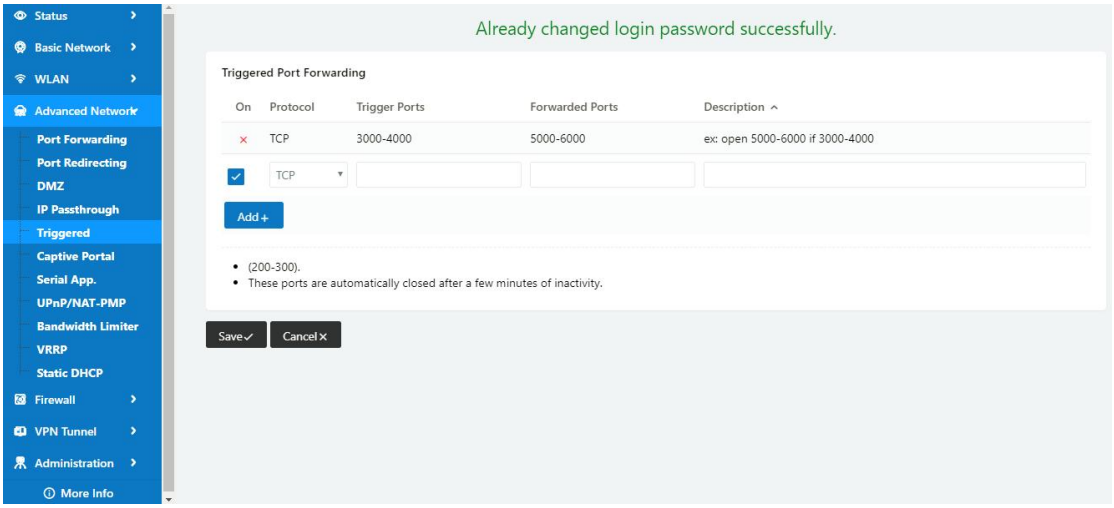


Table 2-12 Triggered Instruction

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

Step 2 Please click ”save” to finish.

----End

2.6.6 Captive Portal

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

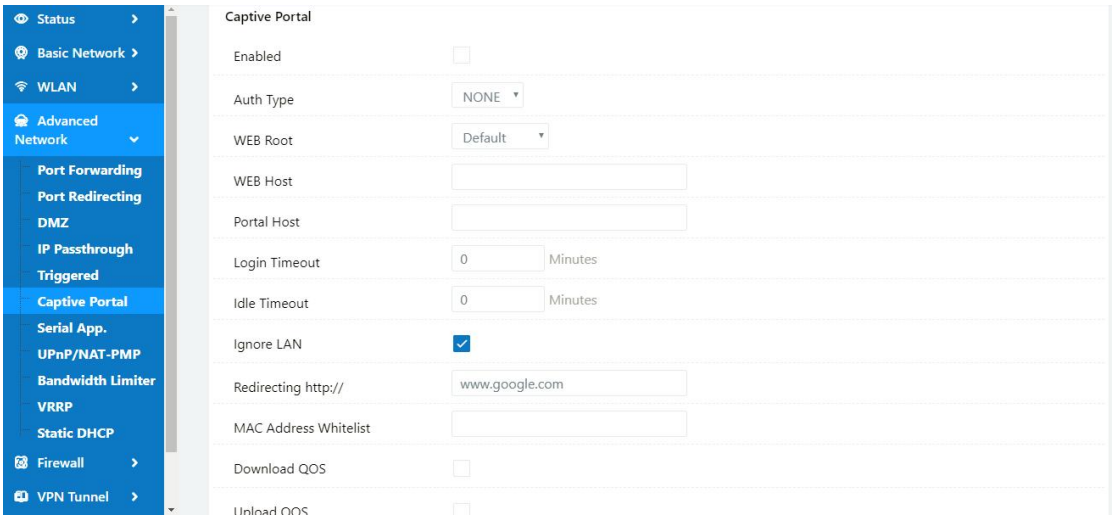


Table 2-13 Captive Portal Instruction

Parameter	Instruction	Default
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.

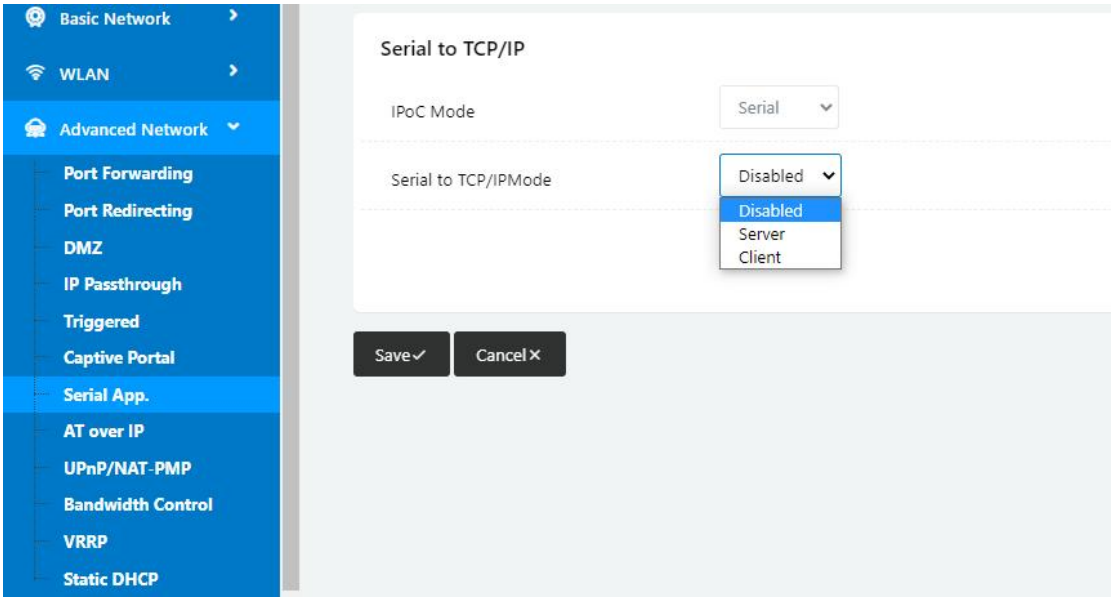
Configuration Instance

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.



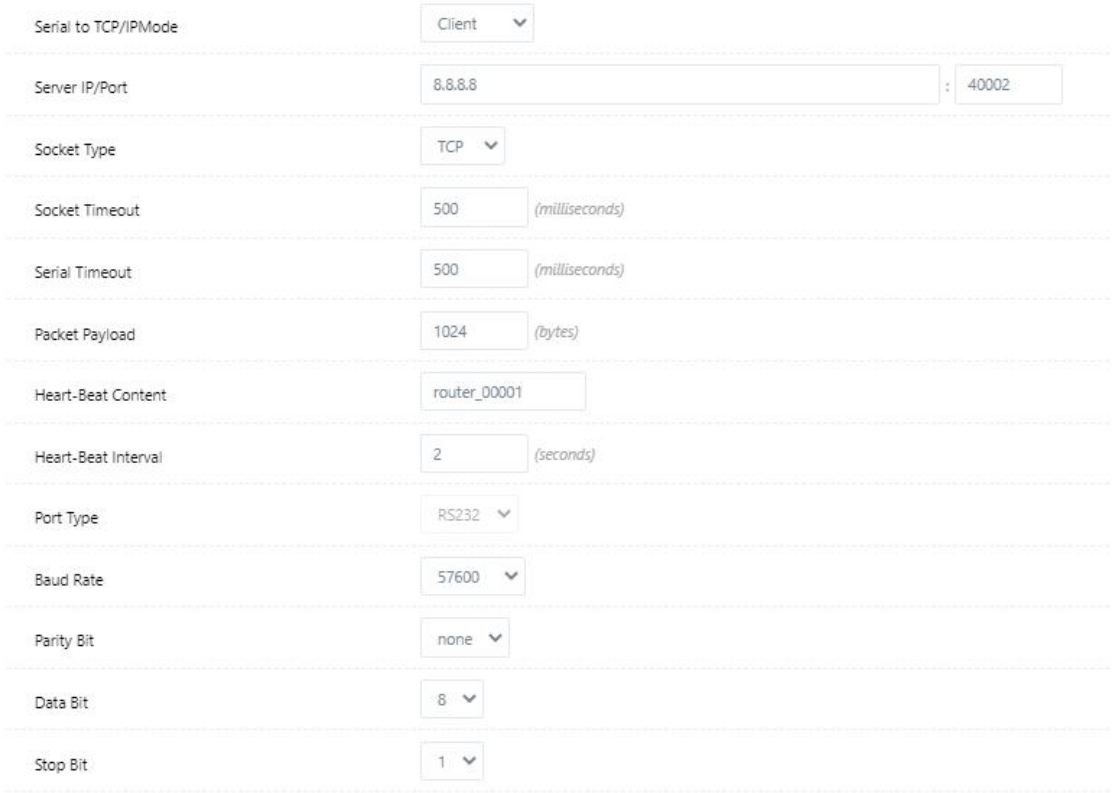


Table 2-14 Serial App Instruction

Parameter	Instruction	Default
IPoc Mode	Transparent serial port and Modbus options.	
Serial to TC/IP mode	Support Disable, Server and Client mode. Such as Client.	

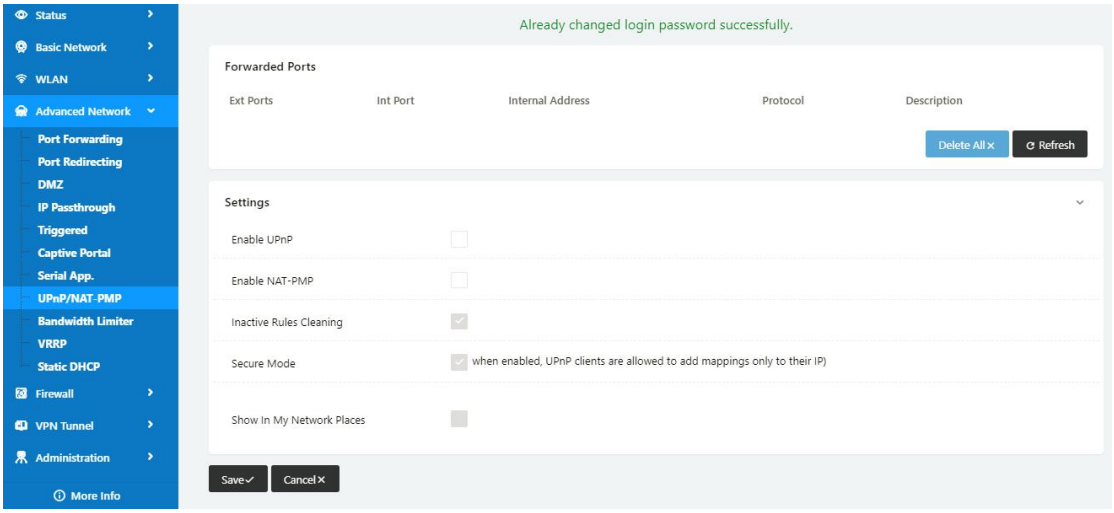
Parameter	Instruction	Default
Server IP/Port	IP address and domain name are acceptable for Server IP	
Socket Type	Support TCP/UDP protocol	
Socket Timeout	Router will wait the setting time to transmit data to serial port.	
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that is less the Packet payload. If the last package equals to the Packet payload, Serial port will transmit it immediately. The default setting is 500ms.	
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.	
Heart-beat Content	Send heart beat to the defined server to keep router online. Meantime, it's convenient to monitor router from server.	
Heart beat Interval	Heart beat interval time	
Baud Rate	115200 as default	
Parity Bit	None as default	
Data Bit	8bit as default	
Stop Bit	1bit as default	

Step 2 Please click "save" to finish.

----End

2.6.8 UPnp/NAT-PMP Setting

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



Step 2 Please click ”save” to finish.

----End

2.6.9 Bandwidth Control Setting

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

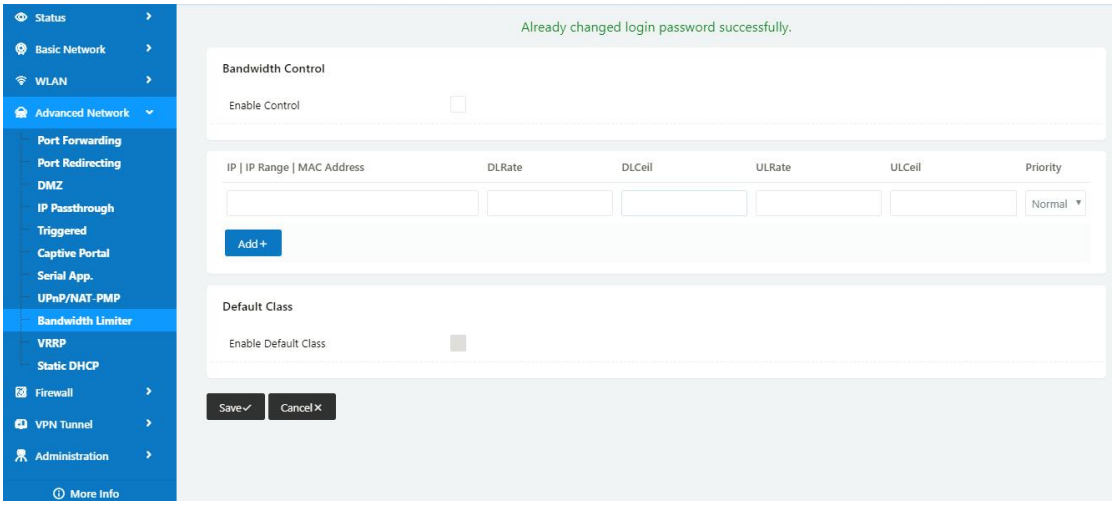


Table 2-15 Bandwidth Control Instruction

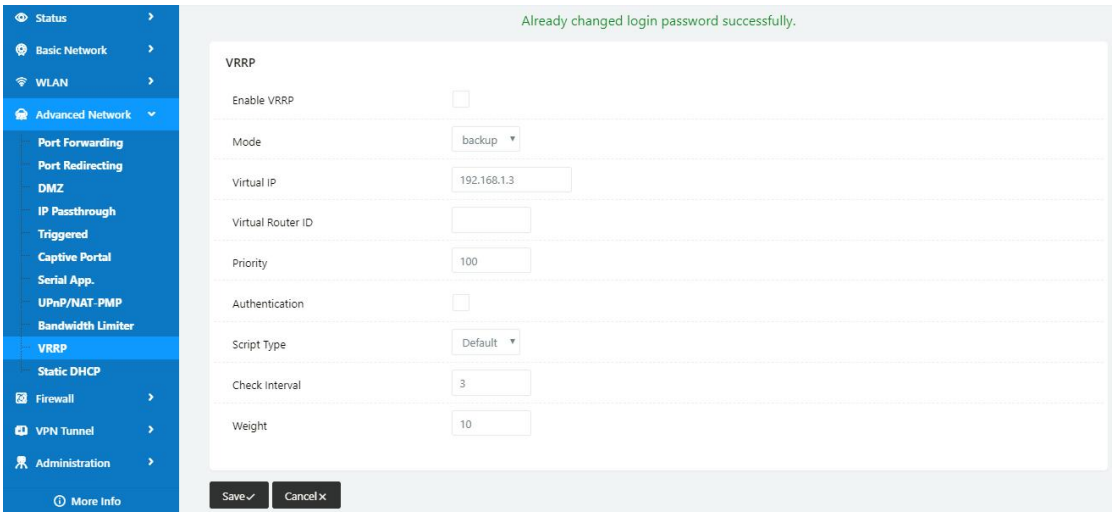
Parameter	Instruction	Default
Max Available Download	Speed limit for router.	
Max Available Upload	Speed limit for router.	
IP/ IP Range/ MAC Address	Limit devices speed for specified IP/IP Range/ MAC Address.	
DL Rate	Mix Download rate	
DL ceil	Max download rate	
UL Rate	Mix Upload rate	
UL ceil	Max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

Step 2 Please click ”save” to finish.

----End

2.6.10 VRRP Setting

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

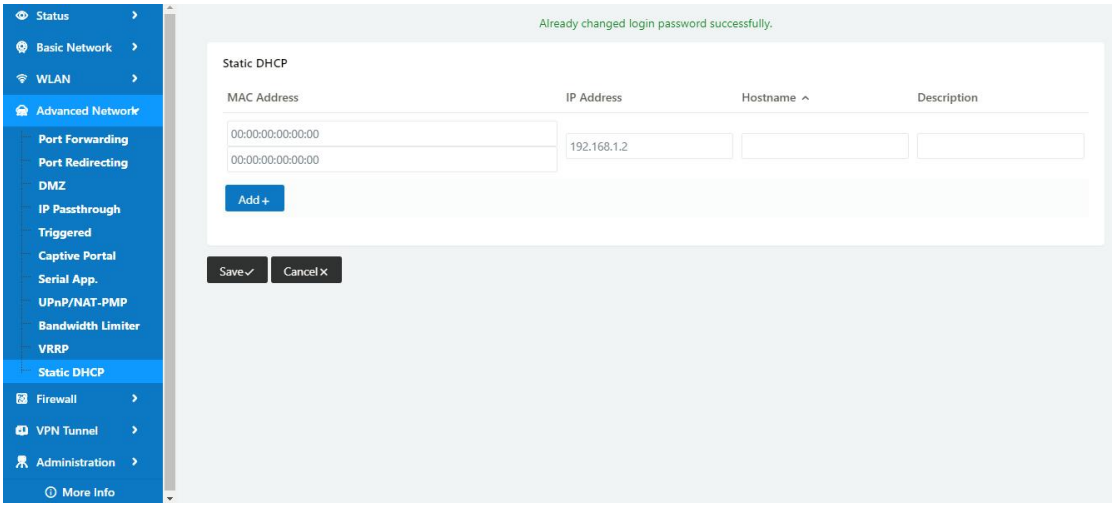


Step 2 Please click ”save” to finish.

----End

2.6.11 Static DHCP Setting

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



Step 2 Please click ”save” to finish.

----End

2.7 Firewall

2.7.1 IP/URL Filtering

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

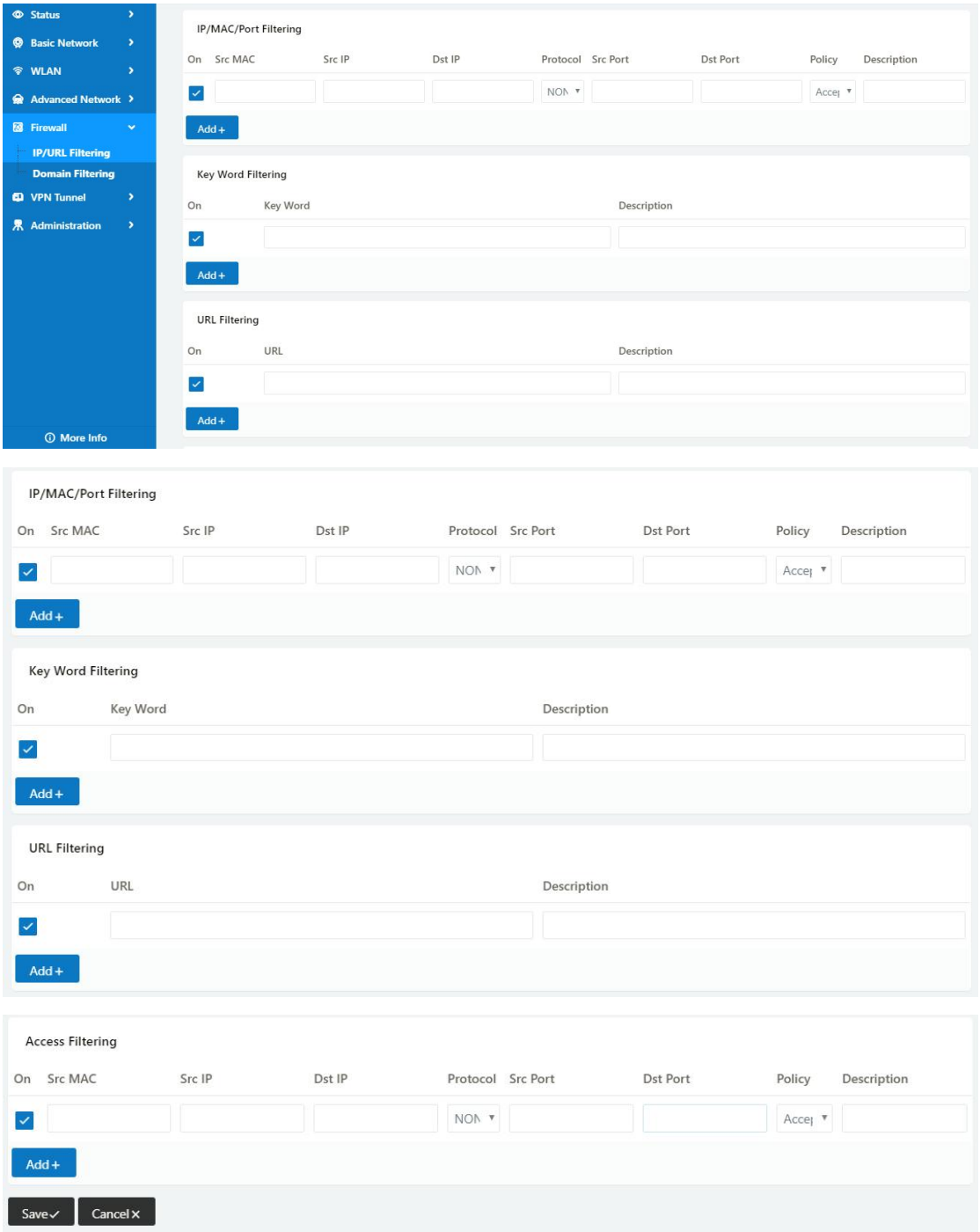


Table 2-16 IP/URL Filtering Instruction

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

Step 2 Please click ”save” to finish.

---End

2.7.2 Domain Filtering

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

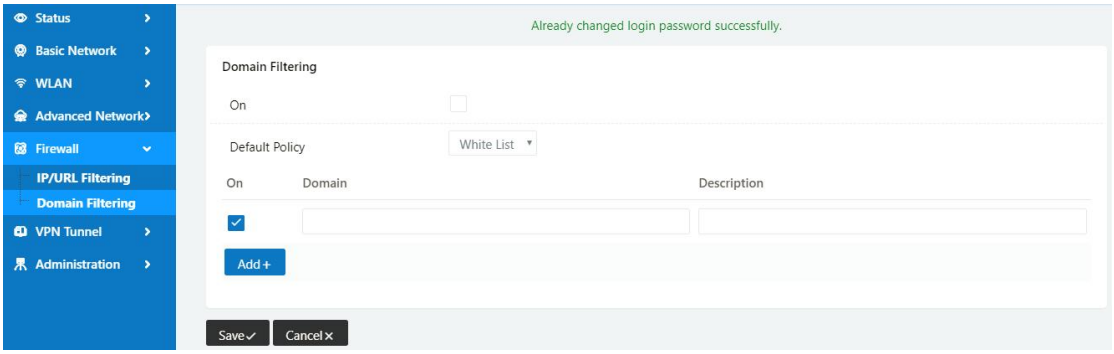


Table 2-17 Domain Filtering Instruction

Parameter	Instruction	Default
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 Wireguard Setting

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

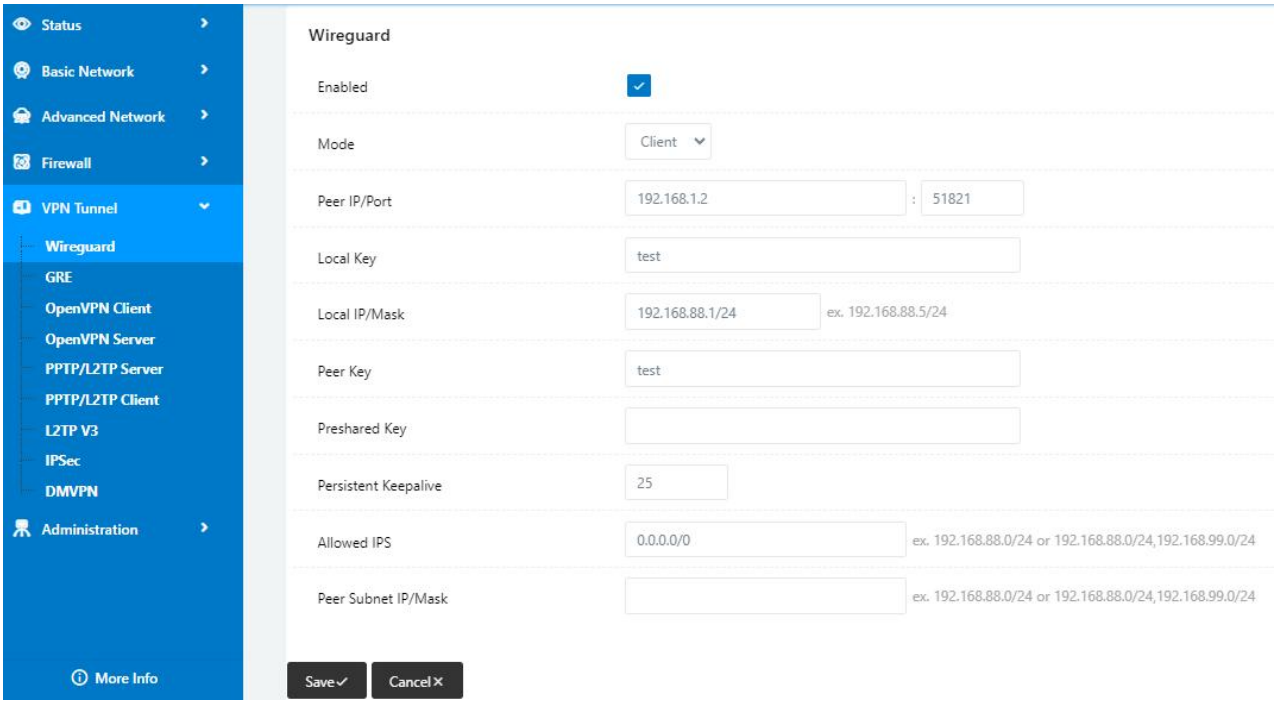


Table 2-18 Wireguard Client Instruction

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

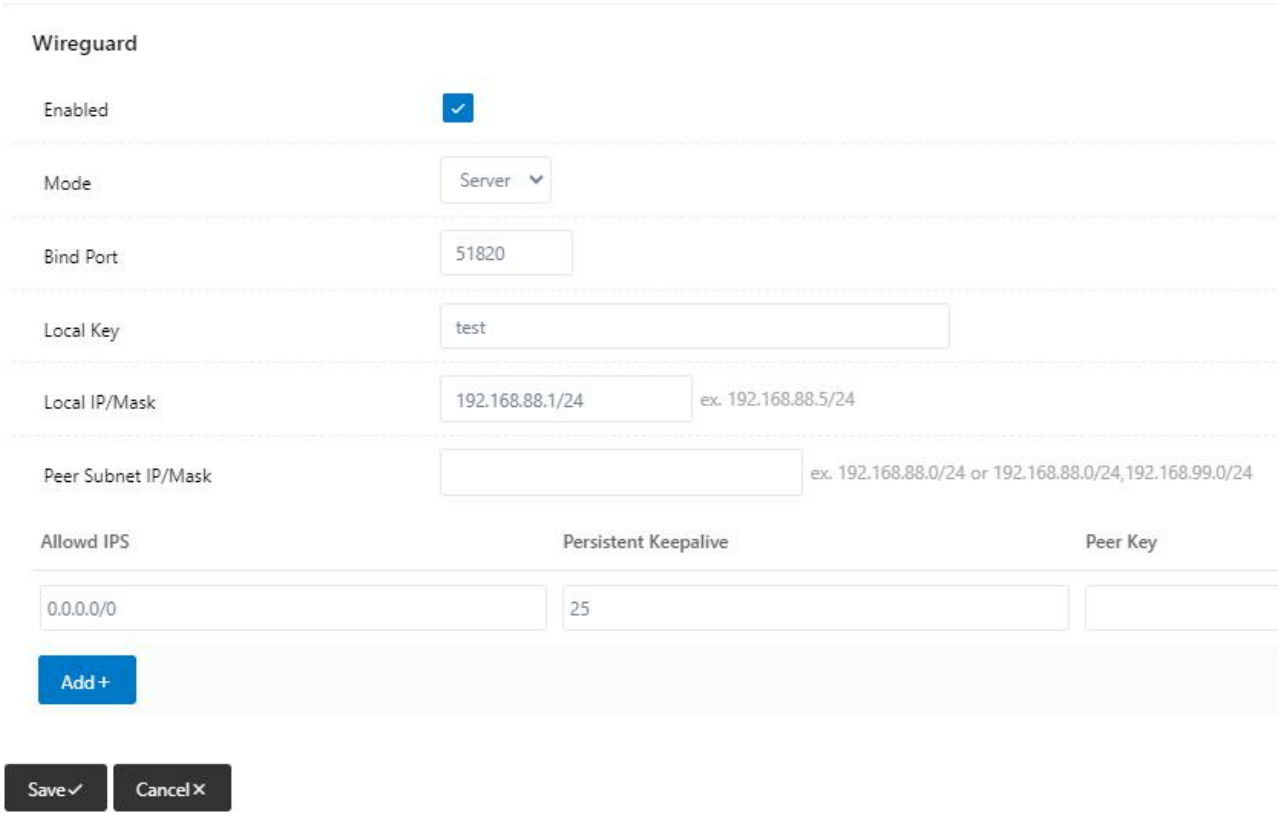


Table 2-19 Wireguard Sever Instruction

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

Step 2 Please click ”save” to finish.

Configuration Instance

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

----End

2.8.2 Zerotier Setting

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

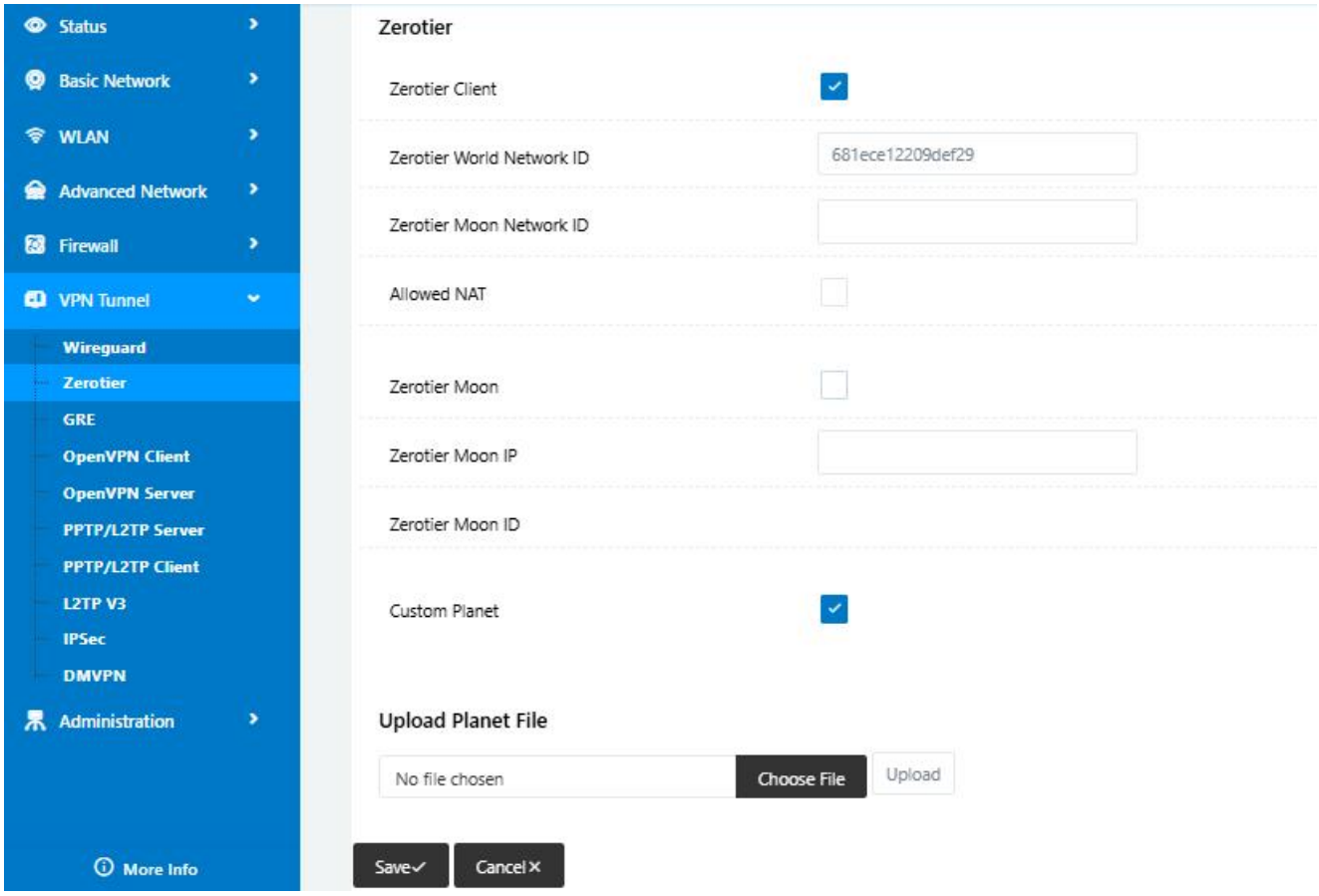


Table 2-20 Zerotier Instruction

Parameter	Instruction	Default
Enable	Enable Zerotier Client mode	Disable
Zerotier World Network ID	A unique 16-digit identifier for your ZeroTier network. Nodes must join using this ID.	Null
Zerotier Moon Network ID	ZeroTier Moon server Network ID	Null
Allowed NAT	Enable NAT in zerotier network.It function will be configured with zerotier IP management together to allow the defined zerotier clinet access.	Disable
Zerotier Moon	Private Root Servers as Moon server	Disable
Zerotier Moon IP	Moon server IP address	Null
Zerotier Moon ID	A unique 16-digit identifier for private ZeroTier network.	Null
Custom Planet	Custon Planet configuration	Disable
Allowed IPs	Allow access to other Zerotier clients. IP is the LAN segment address of other ZeroTier clients; The gateway is a VPN address of other ZeroTier clients.The IP and	Null

Parameter	Instruction	Default
	gateway must correspond to the same routing.	
Upload Planet File	Upload the updated Planet file	Null

Step 2 Please click “save” to finish.

Configuration Instance

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

----End

2.8.3 GRE Setting

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

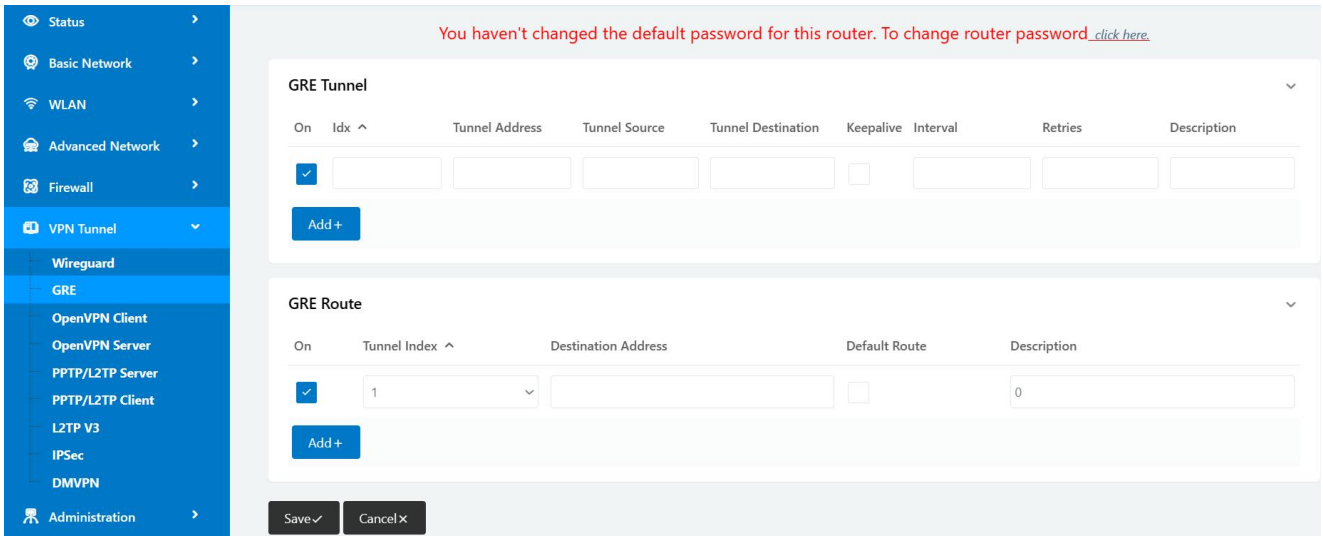


Table 2-21 GRE Instruction

Parameter	Instruction	Default
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 tunnels keep alive to keep GRE tunnel connection.	
Interval	Keep alive interval time.	
Retries	Keep alive retry times. After retrying times, GRE tunnel will be re-established.	

Parameter	Instruction	Default
Description		

Step 2 Please click “save” to finish.

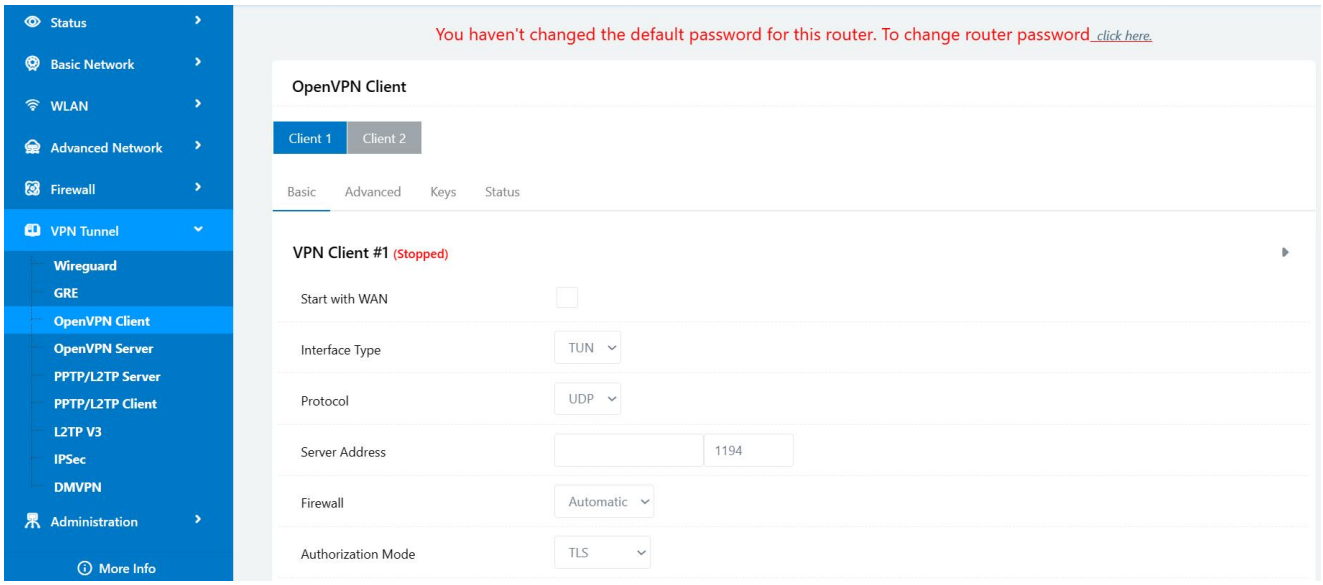
Configuration Instance

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

----End

2.8.4 OpenVPN Client Setting

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



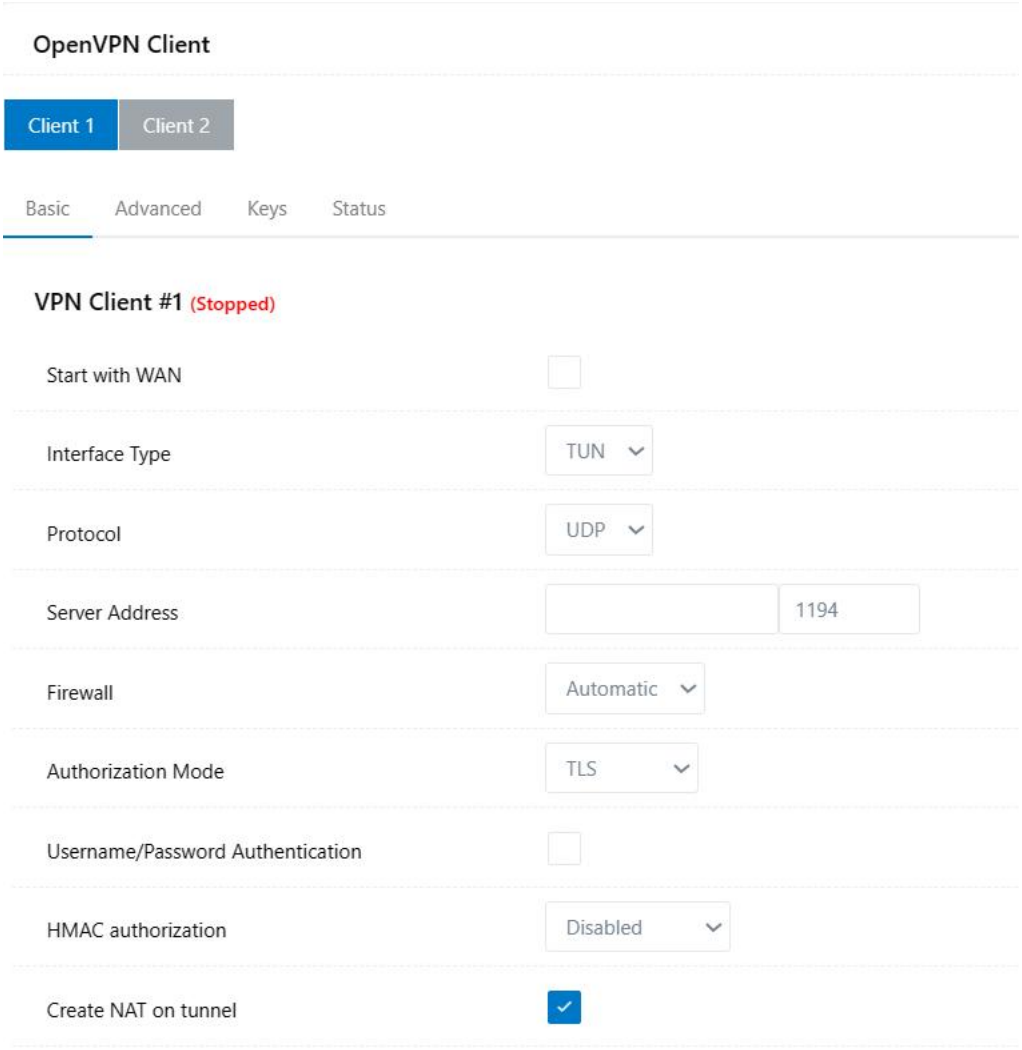


Table 2-22 Basic of OpenVPN Instruction

Parameter	Instruction	Default
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.	
Username/Password Authentication	As the configuration requested.	
HMAC authorization	As the configuration requested.	
Create NAT on tunnel	Configure NAT in OpenVPN tunnel.	

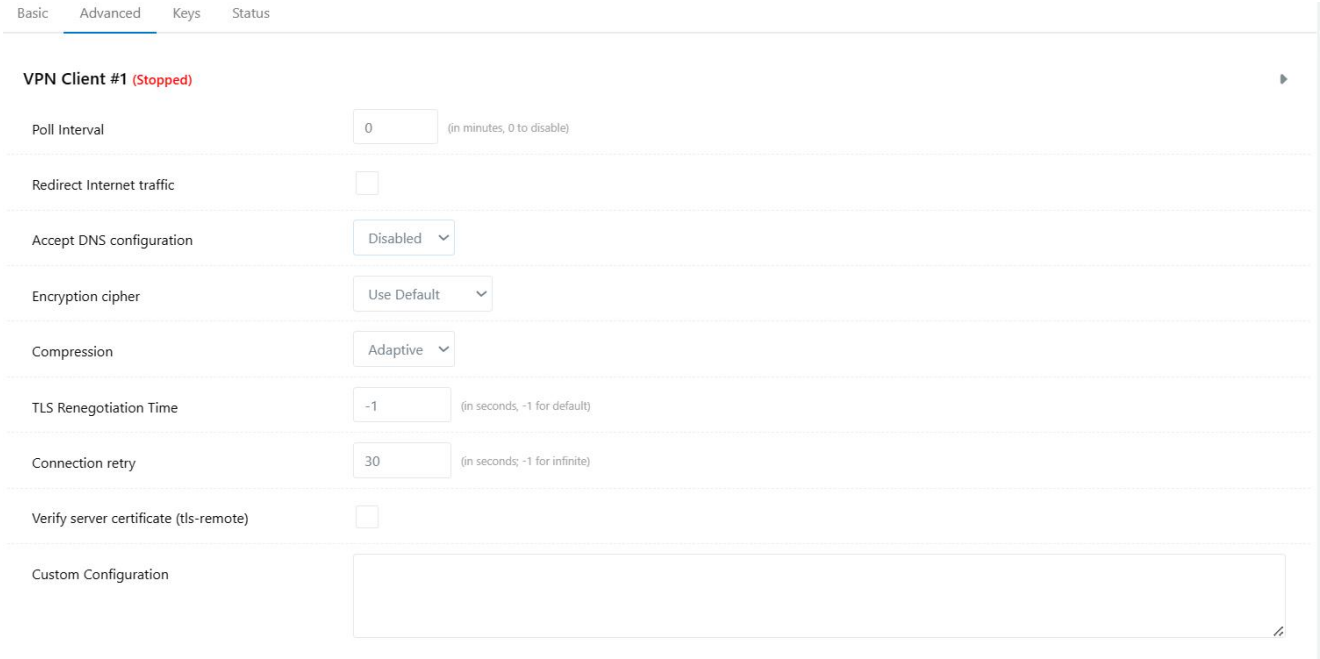


Table 2-23 Advanced of OpenVPN Instruction

Parameter	Instruction	Default
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.	

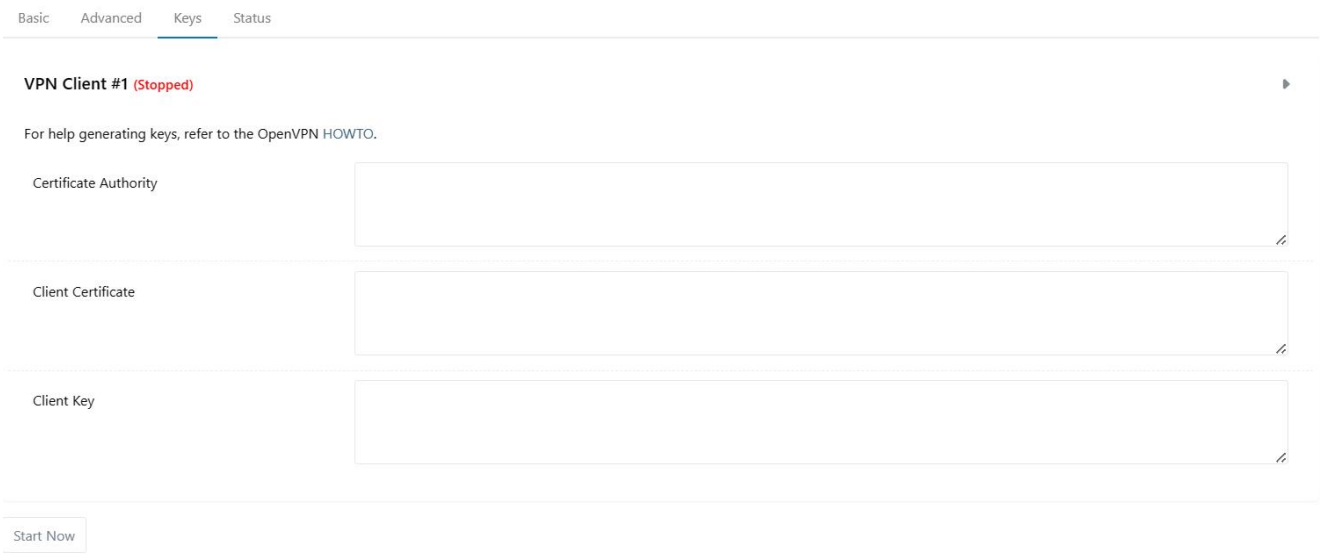


Table 2-24 Keys of OpenVPN Instruction

Parameter	Instruction	Default
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	

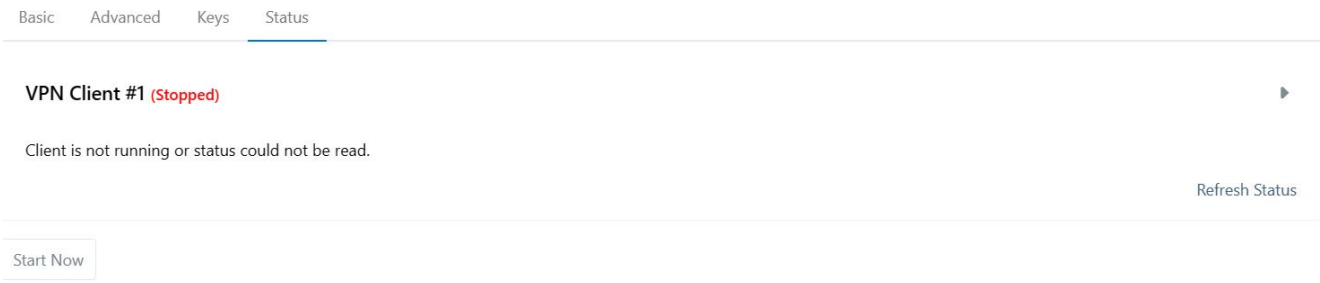


Table 2-25 Status of OpenVPN Instruction

Parameter	Instruction	Default
Status	Check OpenVPN status and data statistics.	

Step 2 Please click “save” to finish.

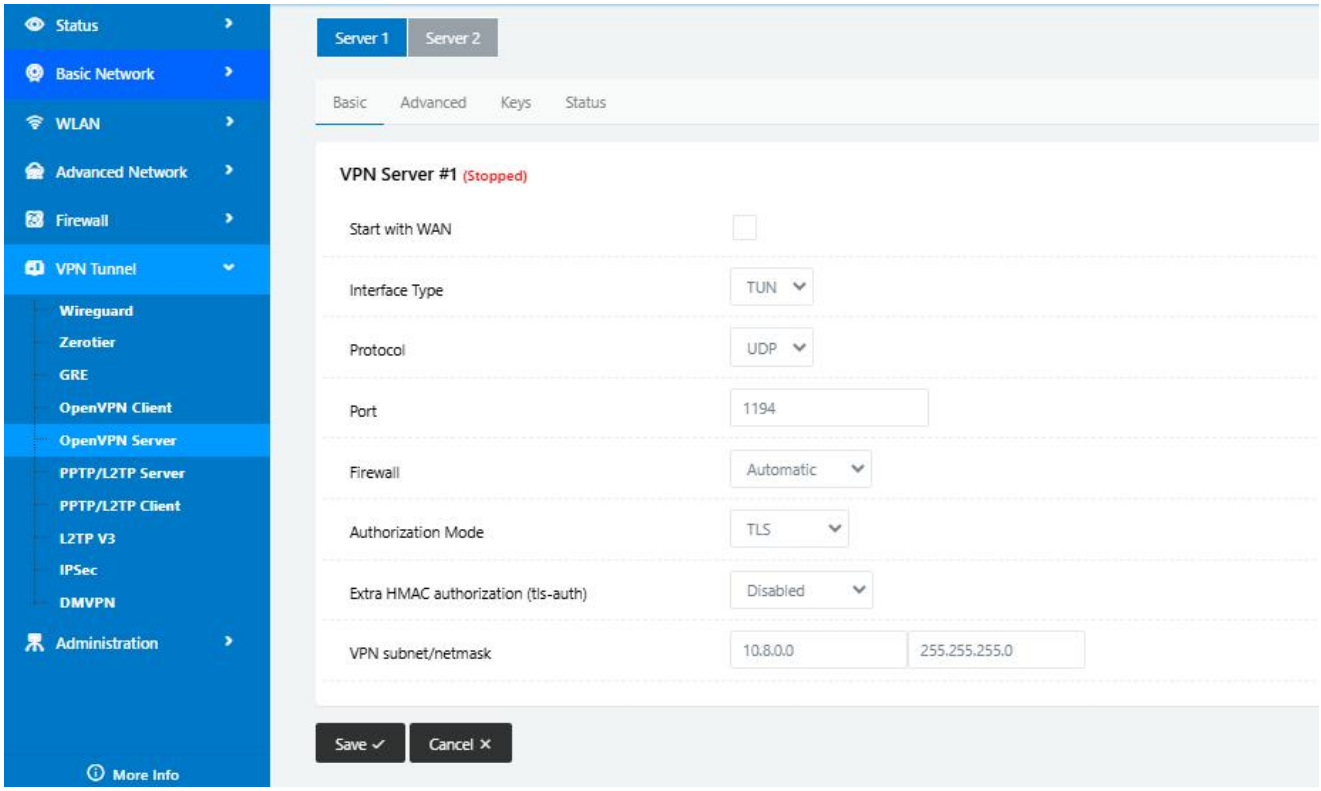
Configuration Instance

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

----End

2.8.5 OpenVPN Server Setting

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



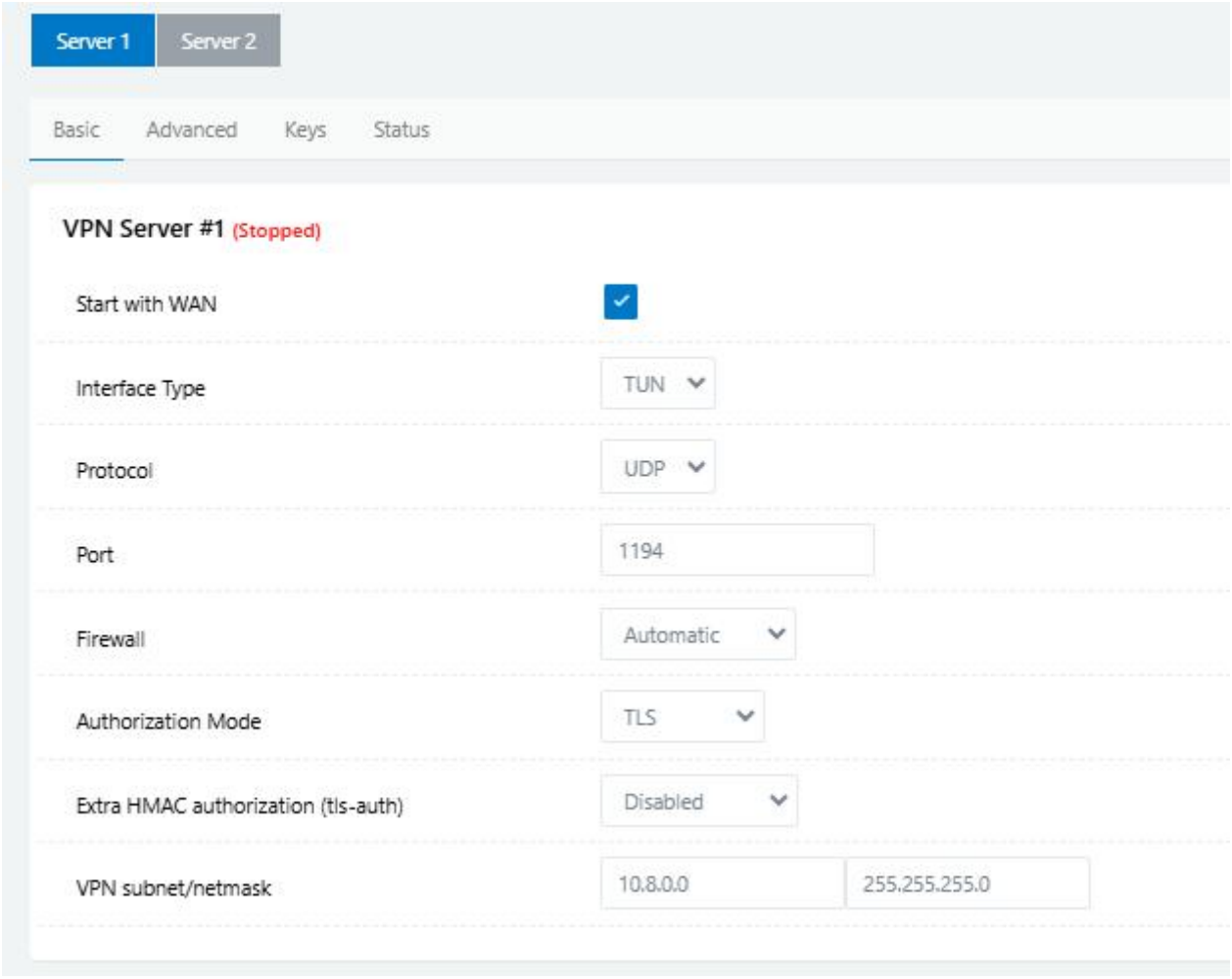


Table 2-26 Basic of OpenVPN Instruction

Parameter	Instruction	Default
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 Port	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.	
Username/Password Authentication	As the configuration requested.	
HMAC authorization	As the configuration requested. Bi-directional, Incoming, Outgoing optional.	Disable
VPN subnet/netmask	OpenVPN server subnet ip address and mask.	NULL

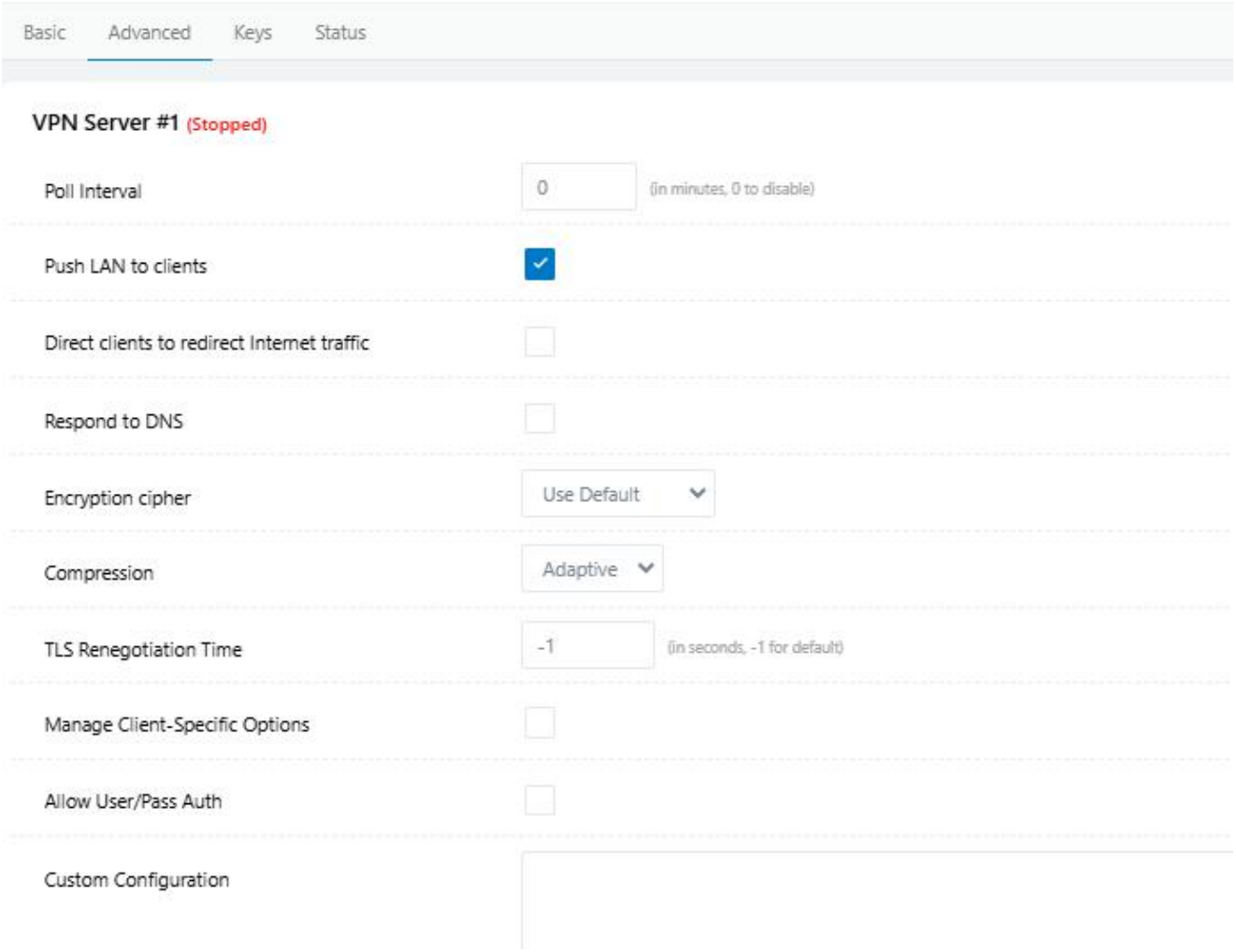


Table 2-27 Advanced of OpenVPN Instruction

Parameter	Instruction	Default
Poll Interval	OpenVPN client check router's status as interval time.	
Redirect Internet Traffic	Configure OpenVPN as default routing.	
Respond to DNS	Server respond to client DNS	Disable
Encryption	As the configuration requested.	
Compression	As the configuration requested.	
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.	
Manage Client-Specific Option	OpenVPN retry to connection interval.	
Allow User/Pass Auth	Configured the username and password for user authentication.	Disable
Custom Configuration	As the configuration requested.	

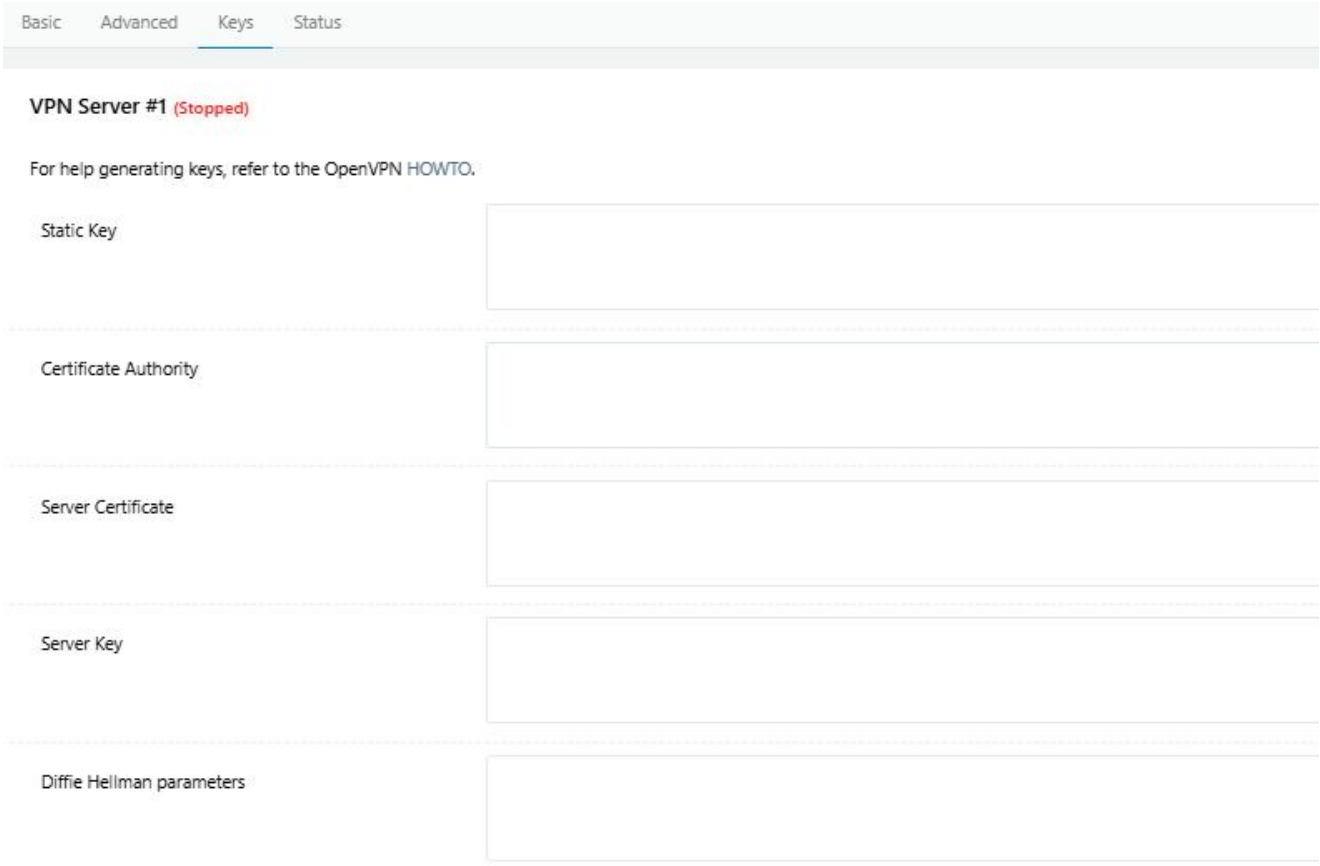


Table 2-28 Keys of OpenVPN Instruction

Parameter	Instruction	Default
Static Key	OpenVPN server	NULL
Certificate Authority	Configure Certificate Authority	NULL
Server Certificate	Configure server certificate	NULL
Server Key	Configure server key	NULL
Diffie Hellman parameters	Configure server HD	NULL

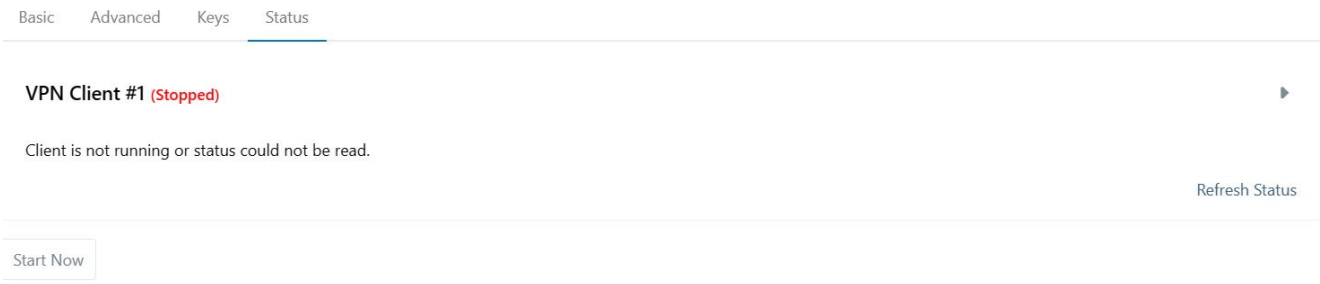


Table 2-29 Status of OpenVPN Instruction

Parameter	Instruction	Default
Status	Check OpenVPN status and data statistics.	

Step 2 Please click “save” to finish.

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

---End

2.8.6 PPTP/L2TP Sever Setting

Step 1 VPN Tunnel> PPTP/L2TP Sever to check or modify the relevant parameter.

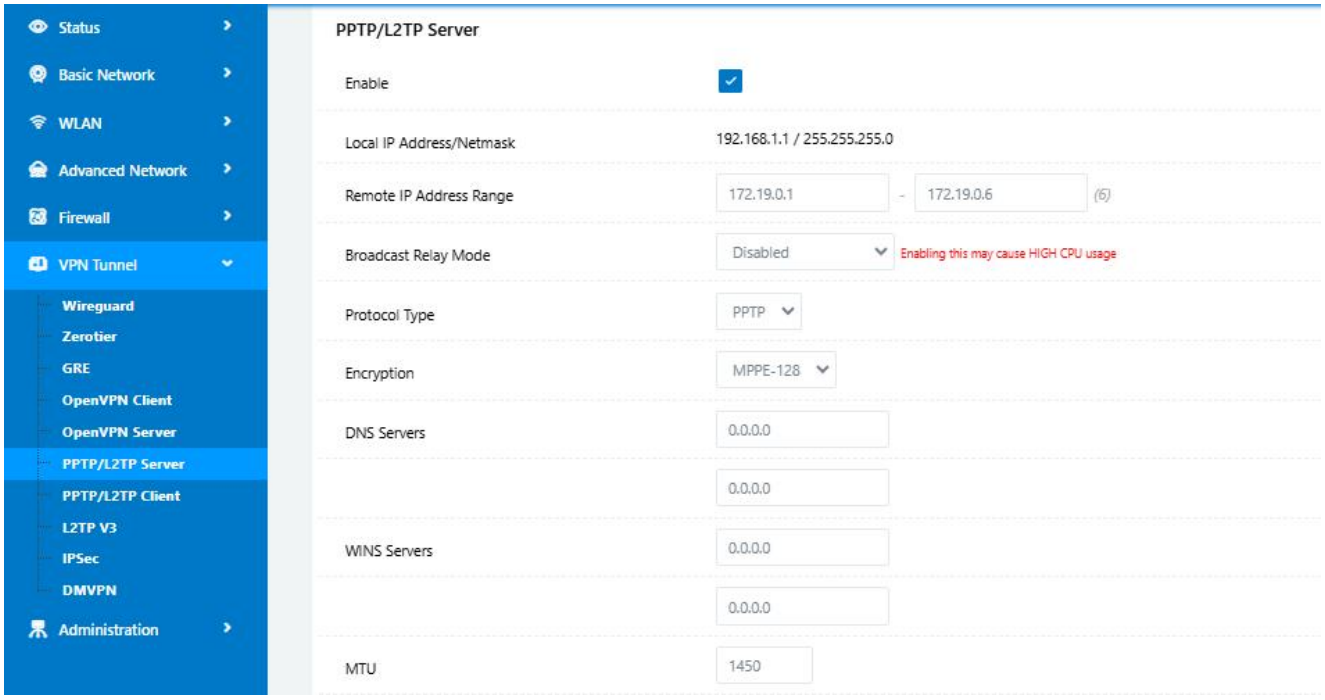


Table 2-30 PPTP/L2TP Server Basic Instruction

parameter	Instruction	Default
Enable	VPN enable	Disable
Locol IP address/Mask	Router LAN IP address. It will be configured as the LAN IP automatically.	NULL
Remote IP Add Range	Remote VPN IP address range	
Broadcast Relay mode	Broadcast relay mode as Disabled, LAN to VPN client, VPN client to LAN, Both optional	Disable
Protocol Type	PPTP/L2TP Optional	PPTP
Encryption	None/MPPE-128 optional	None
DNS Severs	VPN Domain Name Resolution Server	0.0.0.0

parameter	Instruction	Default
WINS servers	VPN Domain Name Resolution Server which is based on 机的 NetBIOS of WIN OS.	0.0.0.0
MTU	Maximum Transmission Unit(MTU) for transmission traffic	1450
MRU	Maximum Transmission Unit(MTU) for receive traffic	1450
Custom Configuration	VPN Custom Configuration	NULL
PPTP/L2TP Client List	Configure VPN name, VPN static IP and VPN client LAN IP address/Mask	NULL

Step 2 Please click “save” to finish.

Configuration Instance

---End

2.8.7 PPTP/L2TP Client Setting

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

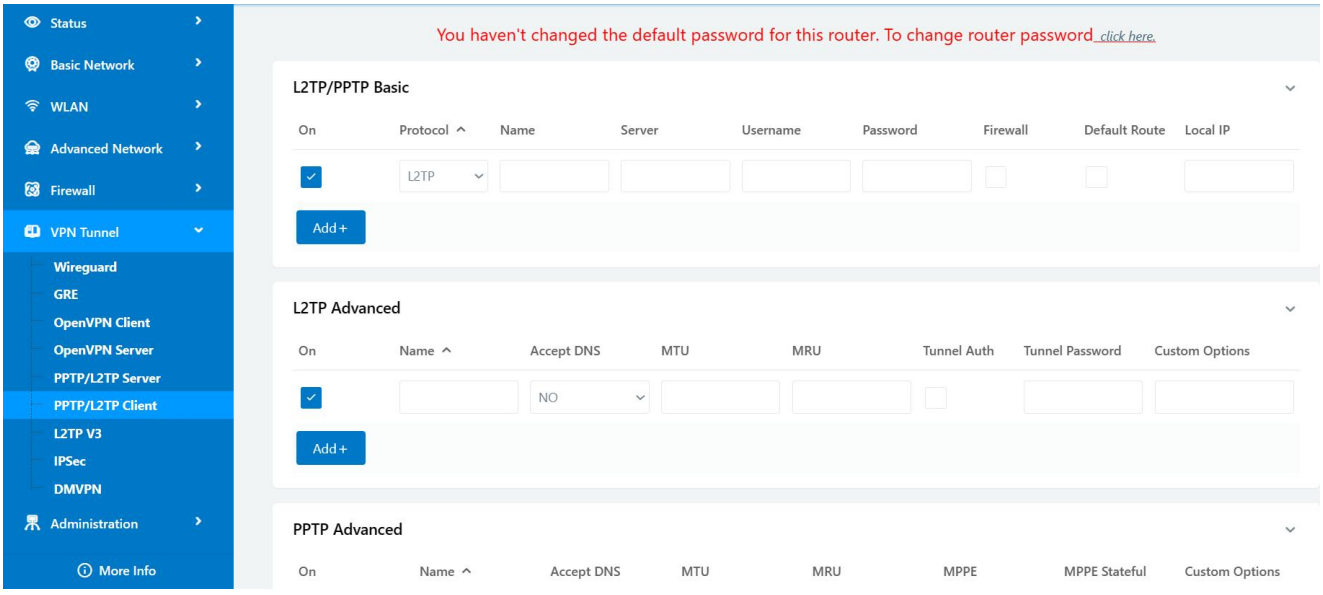


Table 2-31 PPTP/L2TP Basic Instruction

parameter	Instruction	Default
On	VPN enable	
Protocol	VPN Mode for PPTP and L2TP	
Name	VPN Tunnel name	
Server	VPN Server IP address.	

parameter	Instruction	Default
Address		
Username	As the configuration requested.	
Password	As the configuration requested.	
Firewall	Firewall For VPN Tunnel	
Local IP	Defined Local IP address for tunnel	

Table 2-32 L2TP Advanced Instruction

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

Table 2-33 PPTP Advanced Instruction

On	PPTP Advanced enable	Default
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	

On	VPN SCHEDULE feature enable	Default
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

2.8.8 L2TP V3 Setting

Step 1 VPN Tunnel> L2TP V3 to check or modify the relevant parameter.

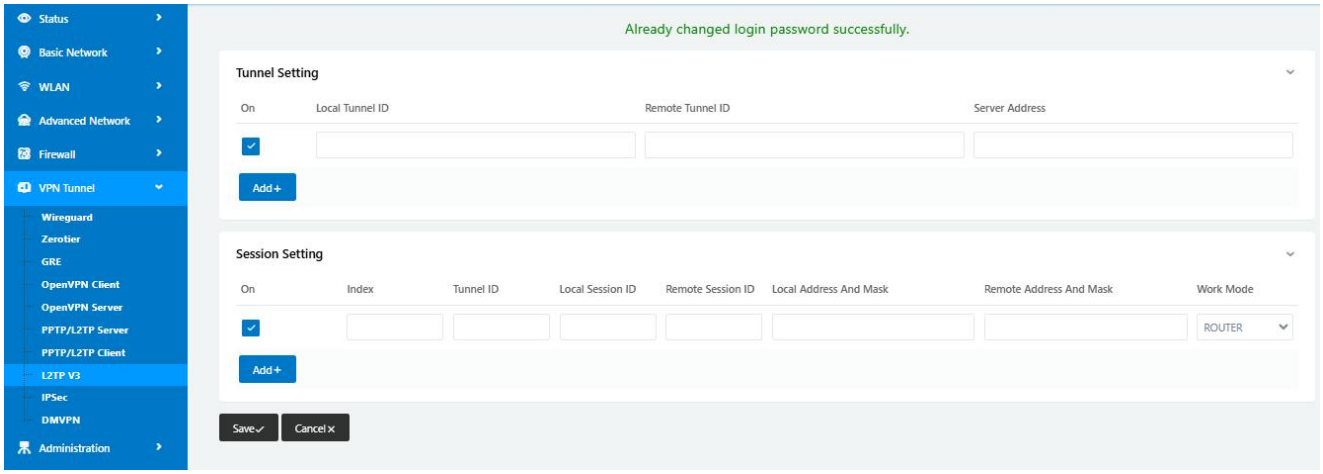


Table 2-34 L2TP V3 Basic Instruction

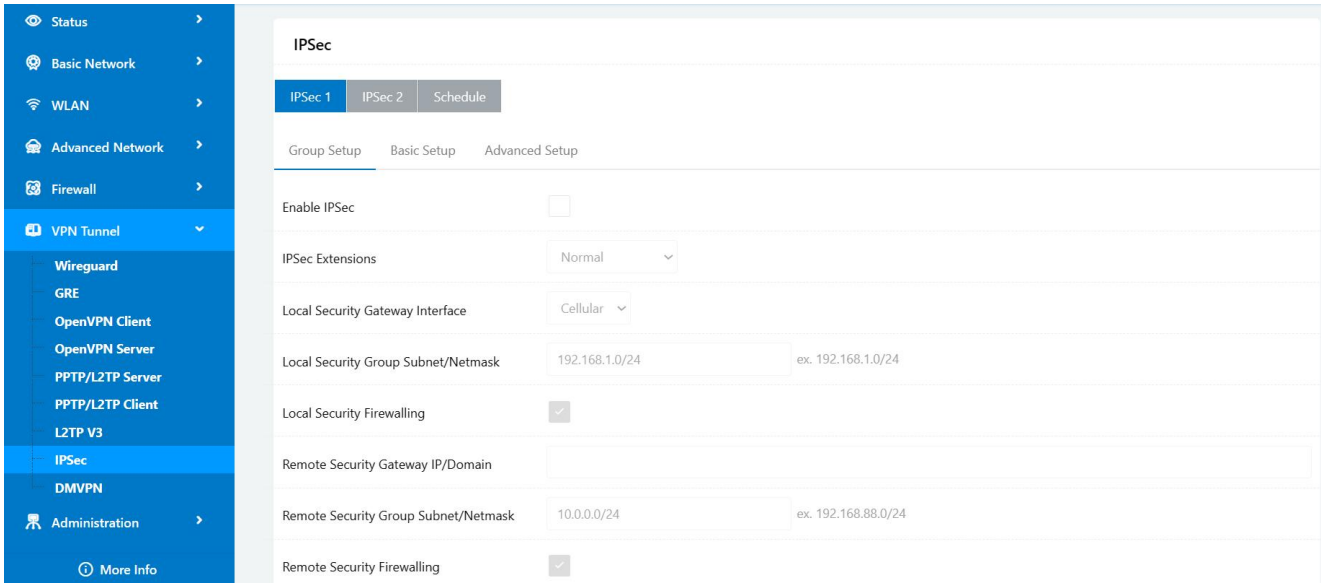
parameter	Instruction	Default
On	VPN on/off optional	OFF
Local Tunnel ID	Local VPN tunnel ID	NULL
Remote Tunnel ID	Remote VPN tunnel ID	NULL
Server Address	VPN Server IP address	NULL
Index	VPN sequence number	NULL
Tunnel ID	VPN tunnel ID	NULL
Local Session ID	Local Session ID	NULL

parameter	Instruction	Default
Remote Session ID	Local Session ID	NULL
Local IP and mask	Local tunnel IP and mask as format A.B.C.D/M	NULL
Remote IP and mask	Remote tunnel IP and mask as format A.B.C.D/M	NULL
Work Model	Router/Gateway/Bridge optional	NULL

Step 2 Please click “save” to finish.

---End

2.8.9 IPSec Setting



2.8.9.1 IPSec Group Setup

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

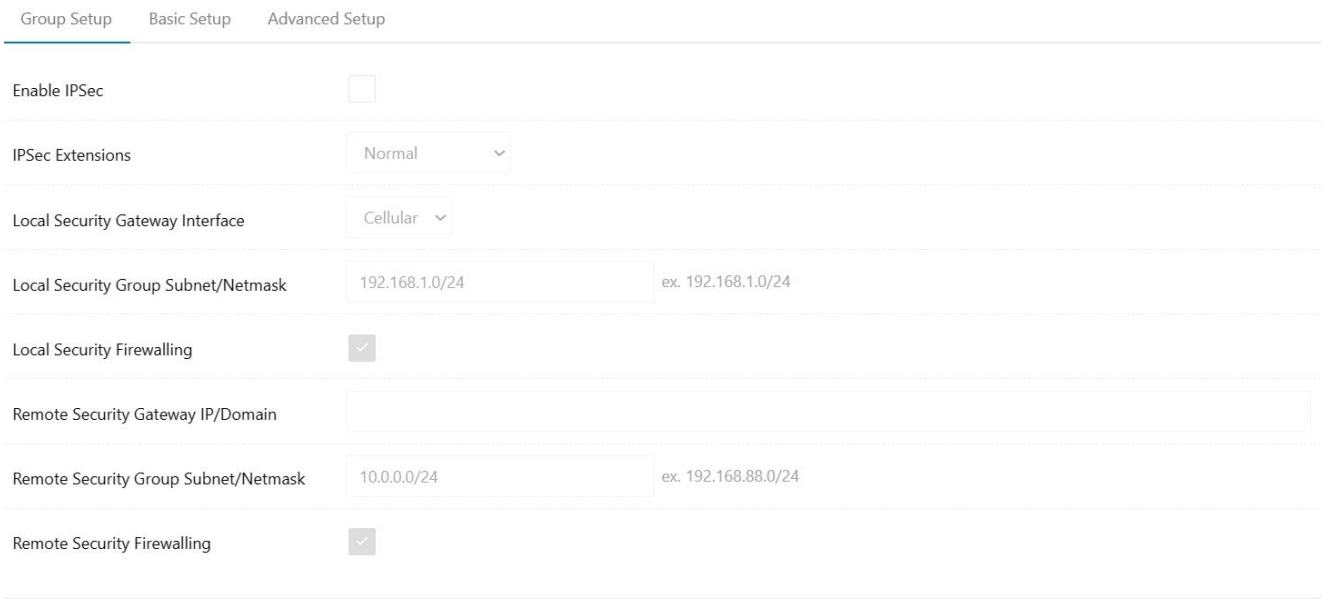


Table 2-35 IPSec Group Setup Instruction

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

Step 2 Please click “save” to finish.

---End

2.8.9.2 IPSec Basic Setup

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

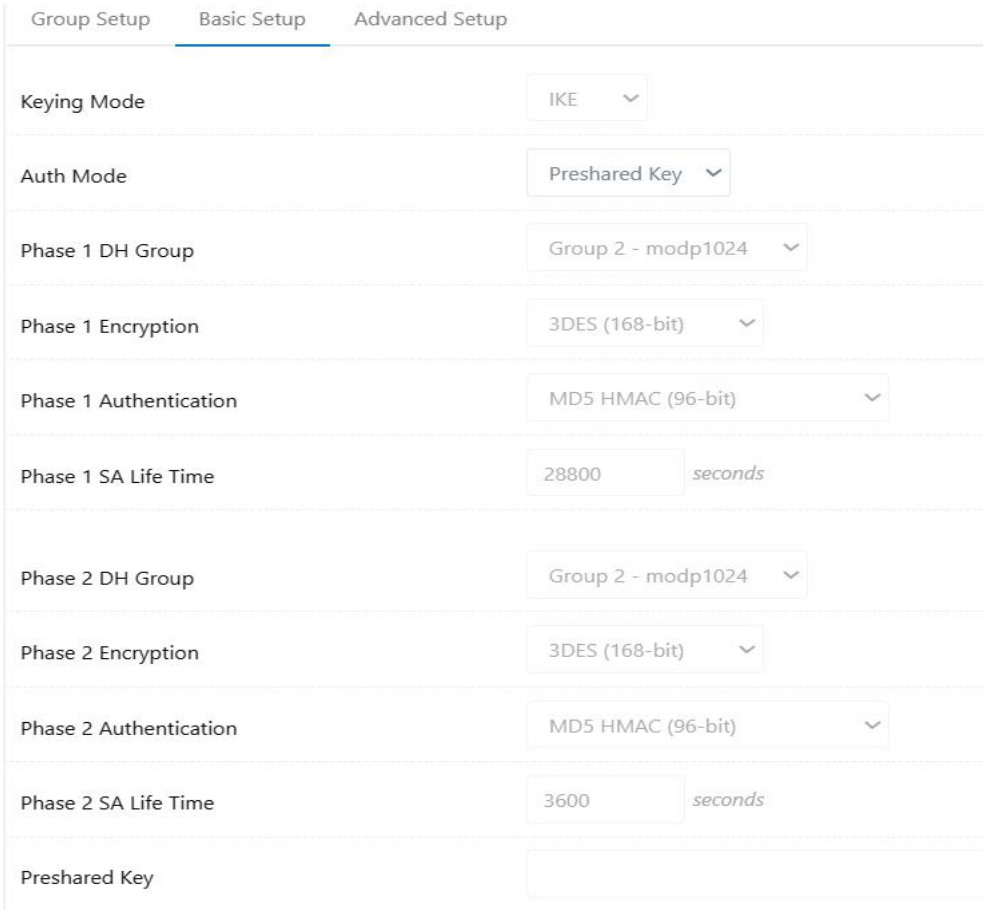


Table 2-36 IPSec Basic Setup Instruction

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

Step 2 Please click “save” to finish.

---End

2.8.9.3 IPSec Advanced Setup

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

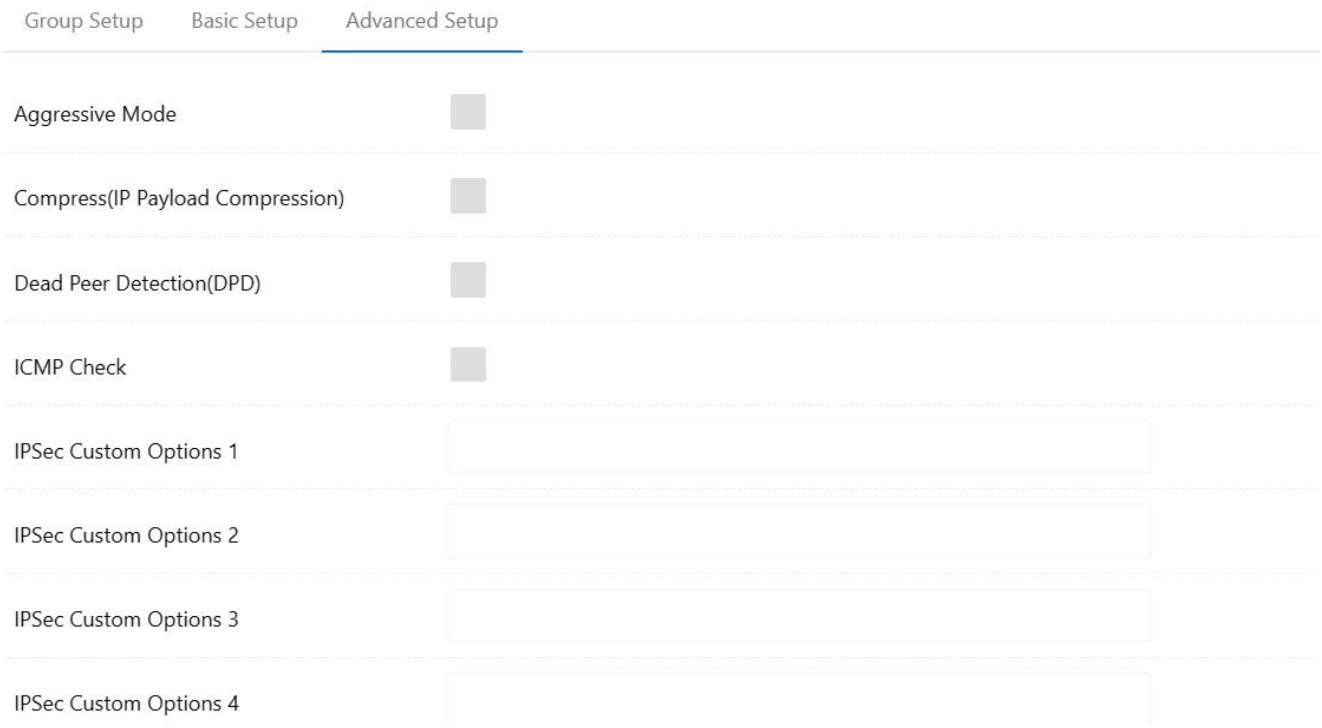


Table 2-37 IPSec Advanced Setup Instruction

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

Step 2 Please click “save” to finish.

Configuration Instance

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

----End

2.8.10 DMVPN Setting

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

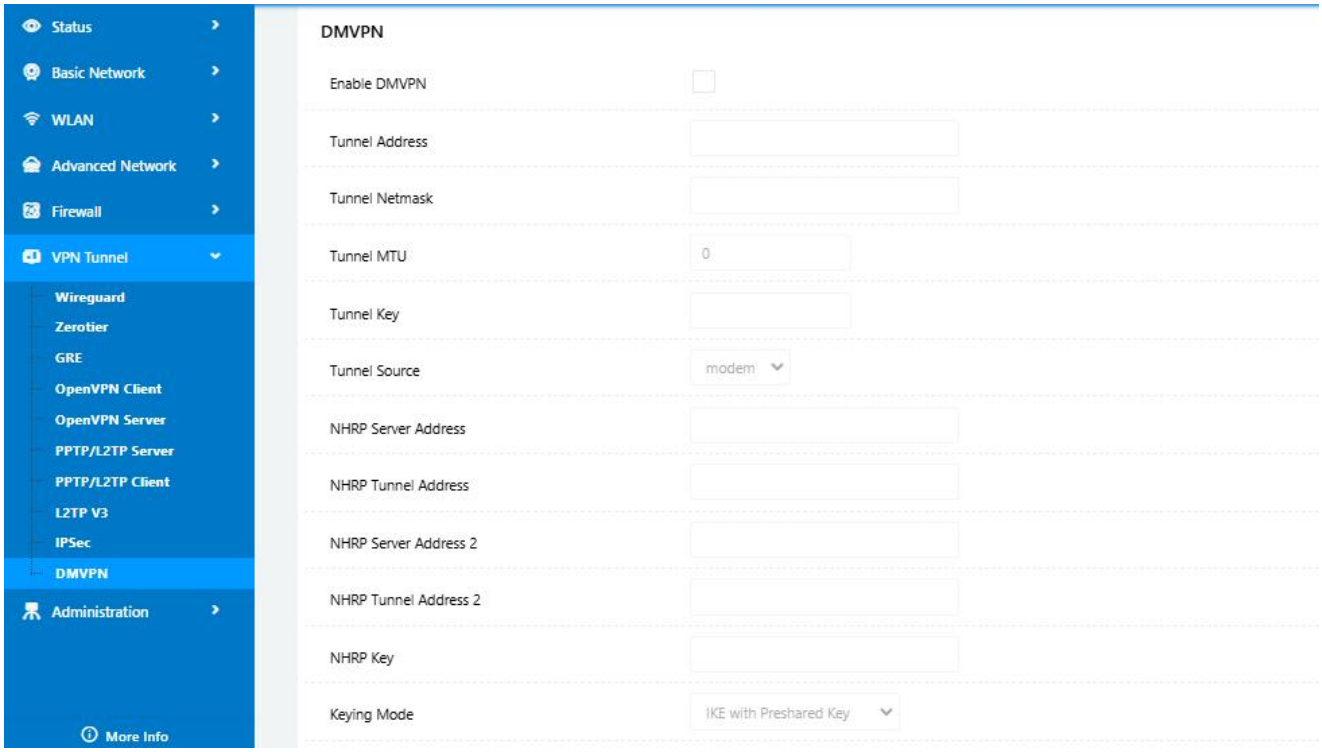


Table 2-38 DMVPN Basic Instruction

parameter	Instruction	Default
Enable	DMVPN enable/disable optional	OFF
Tunnel Address	GRE Tunnel IP address	NULL
Tunnel Mask	GRE Tunnel mask	NULL
Tunnel MTU	GRE Tunnel MTU	0
Tunnel Key	GRE Tunnel Key	NULL
Tunnel Source	Tunnel source IP address. Modem, WAN, sta, sta2 optional	NULL
NHRP Server Address	NHRP server IP address	NULL
NHRP Tunnel Address	NHRP Tunnel IP address	NULL
LNHRP Server Address2	LNHRP server IP address1	NULL
NHRP Tunnel Address2	RNHRP server IP address1	NULL
NHRP Key	NHRP Key	NULL
Keying Mode	IPsec key. IKE1 shared key and IKE2 shared key optional	

parameter	Instruction	Default
Phase 1 DH Group	Phase1 Group. Group1, 2,5 optional	
Phase 1 Encryption	3DES, AES-128/192/256 optional	
Phase 1 Authentication	MD5, SHA, SHA2 256/384/512 optional	
Phase 1 SA Life Time	Phase 1 SA Life available time	
Phase 2 DH Group	Phase1 Group. Group1, 2,5 optional	
Phase 2 Encryption	DES, AES-128/192/256 optional	
Phase 2 Authentication	MD5, SHA, SHA2 256/384/512 optional	
Phase 2 SA Life Time	Phase 2 SA Life available time	
Preshared Key	IPSec preshared key	
Dead Peer Detection(DPD)	Dead Peer Detection(DPD)	
IPSec Custom Options	IPSec Custom as requested	

Step 2 Please click “save” to finish.

---End

2.9 Administration

2.9.1 Identification Setting

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

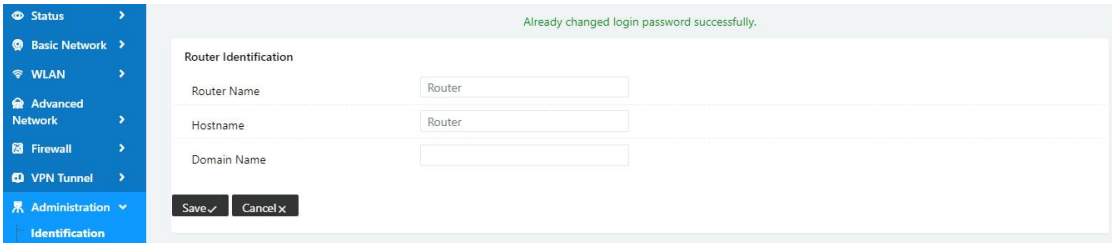


Table 2-39 Router Identification Instruction

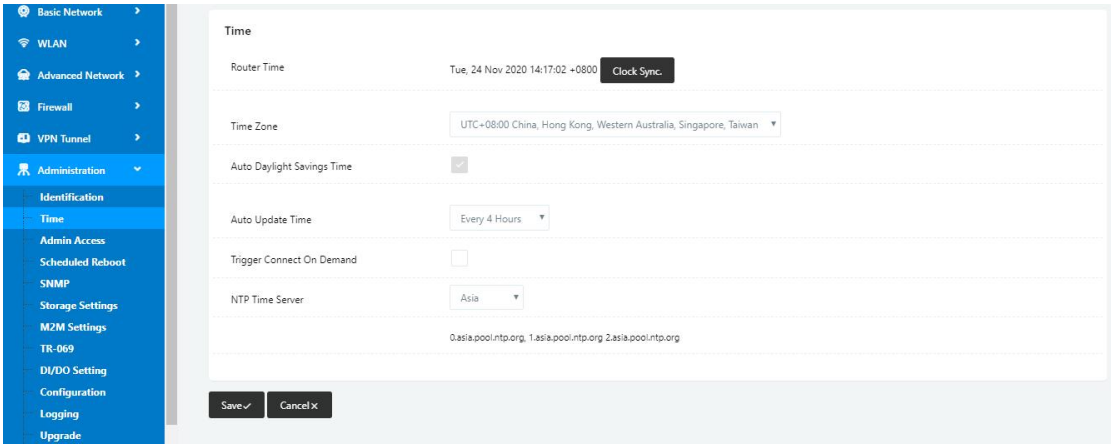
Parameter	Instruction	Default
Router name	Default is router, can be set maximum 32 character	
Host name	Default is router, can be set maximum 32 character	
Domain name	Default is empty, support maximum up to 32 character, it is the domain of WAN, no need to configure for most application.	

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.



CAUTION

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

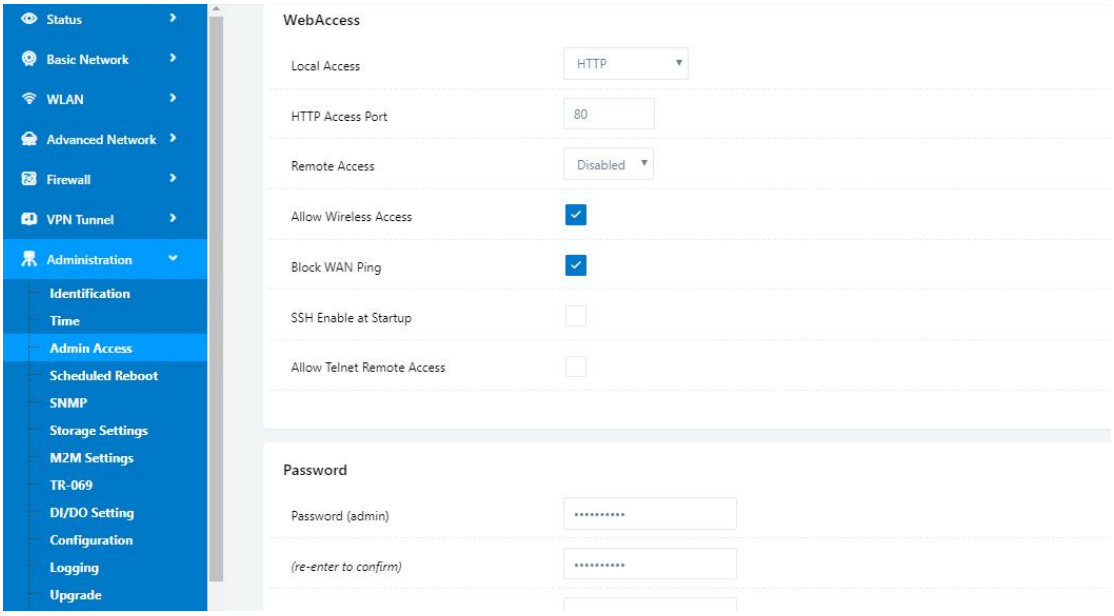
Step 2 Please click “save to finish.

----End

2.9.3 Admin Access Setting

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

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

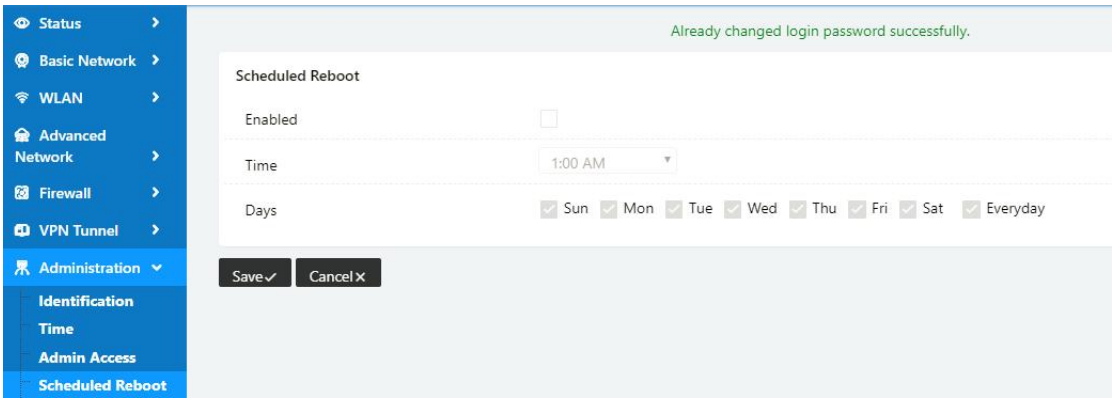


Step 2 Please click save iron to finish the setting

----End

2.9.4 Schedule Reboot Setting

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

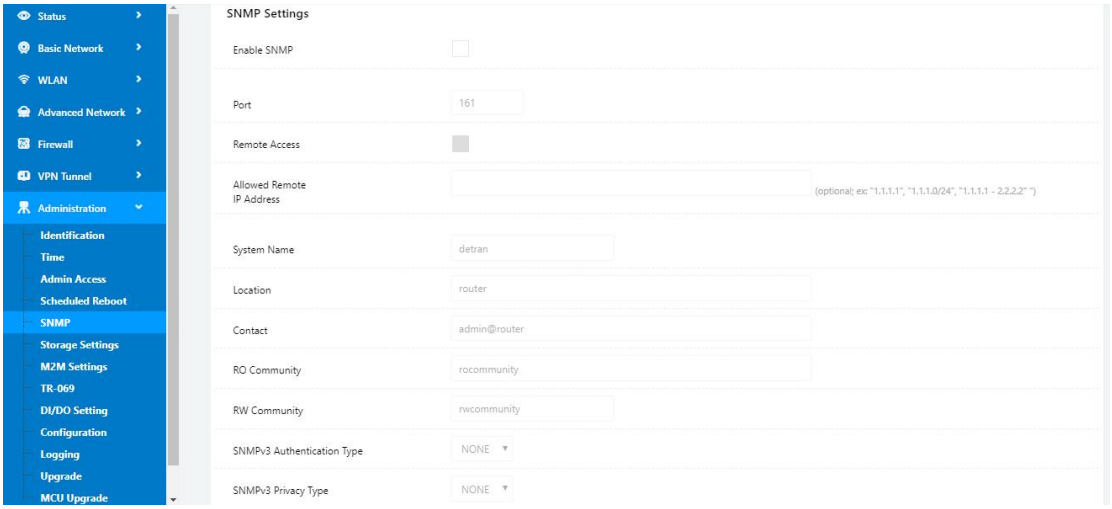


Step 2 Please click save iron to finish the setting

----End

2.9.5 SNMP Setting

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

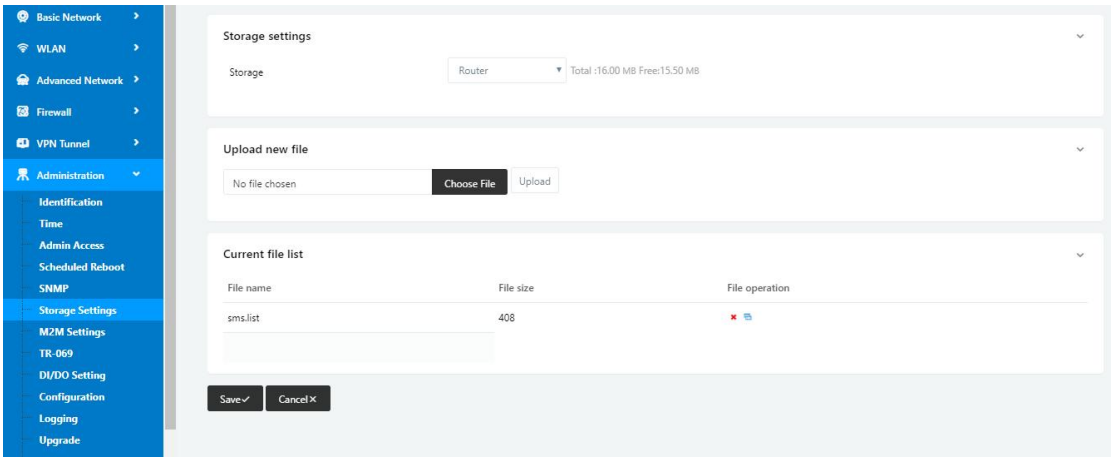


Step 2 Please click save iron to finish the setting

----End

2.9.6 Storage Setting

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

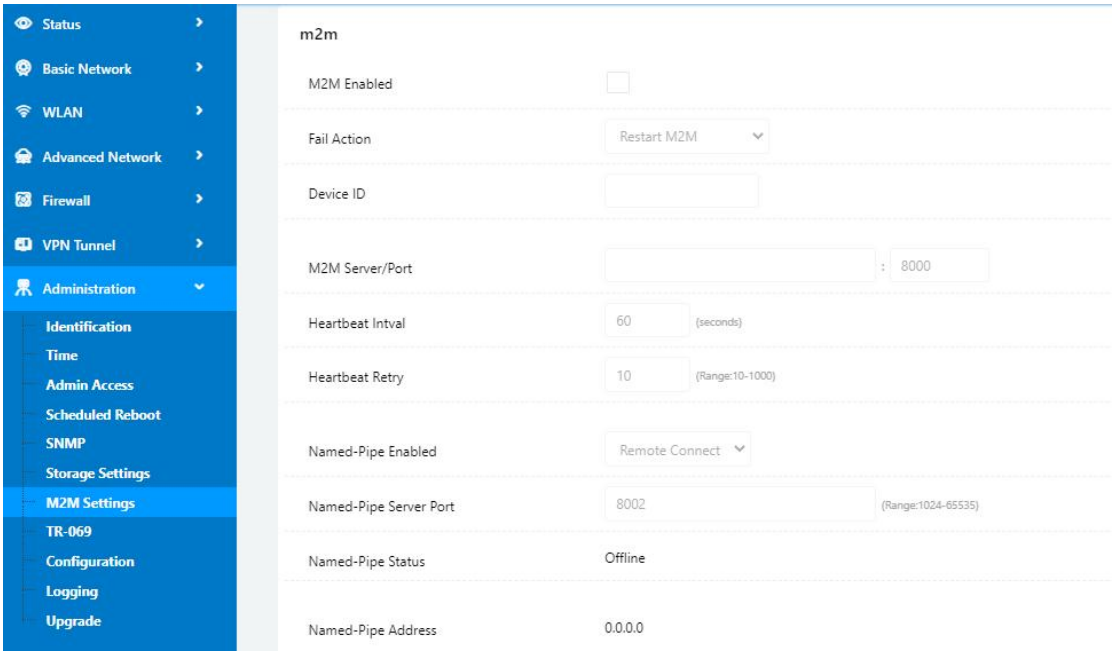


Step 2 Please click save iron to finish the setting

----End

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

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

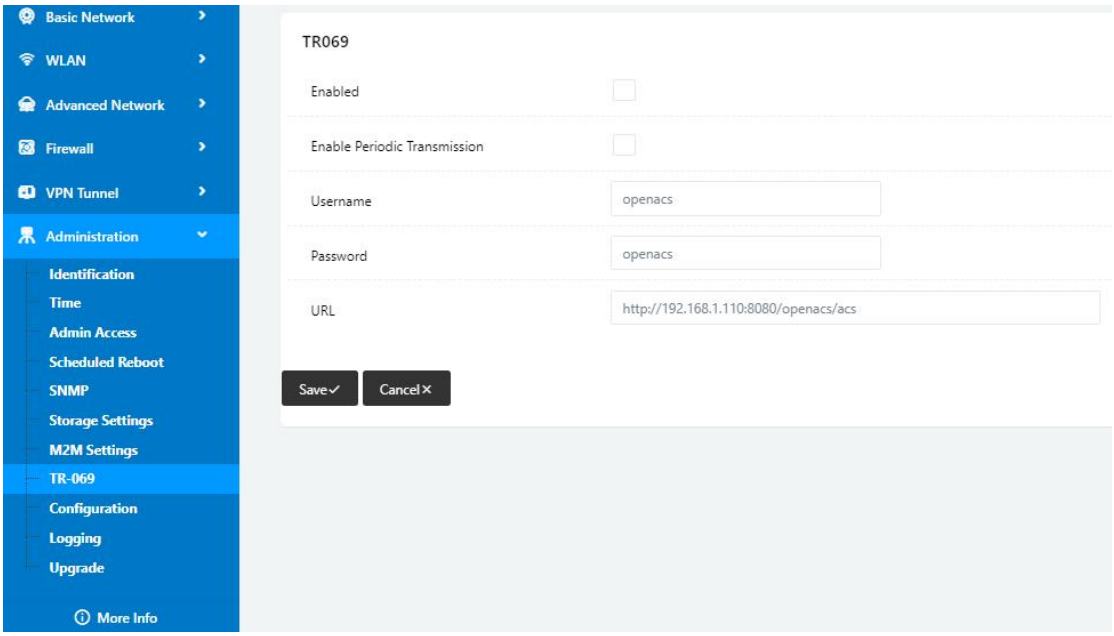


Step 2 Please click save iron to finish the setting

----End

2.9.8 TR-069 Setting

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



Step 2 Please click save iron to finish the setting

Configuration Instance

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

----End

2.9.9 Configuration Setting

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

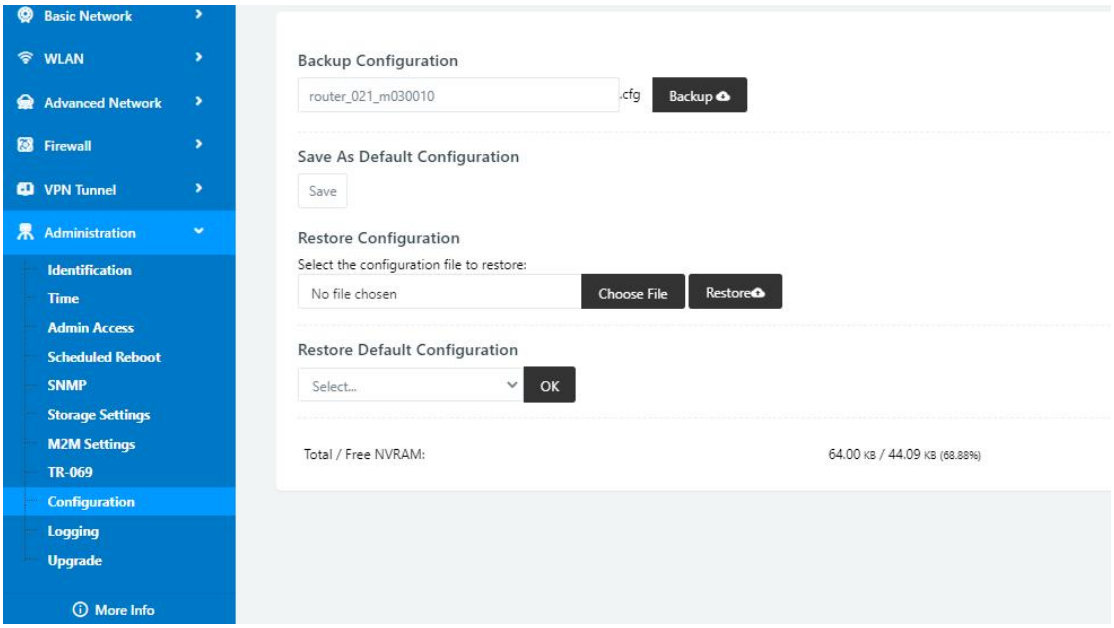


Figure 3-1 Backup and Restore Configuration GUI

CAUTION

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

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

----End

2.9.10 System Log Setting

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

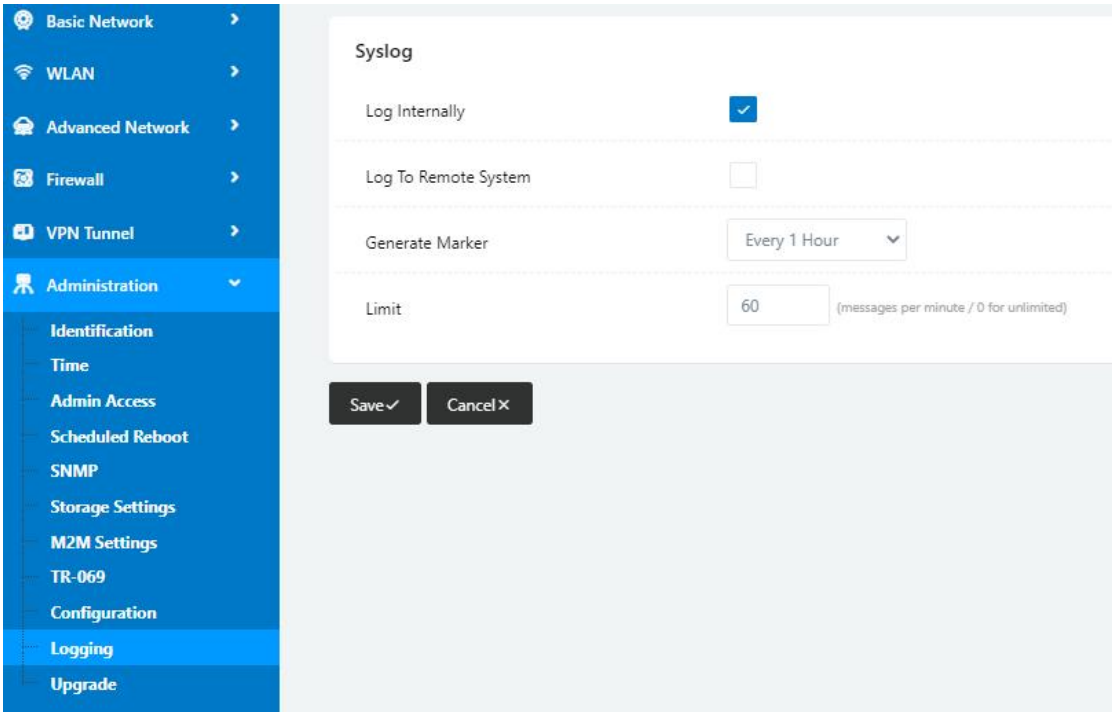


Figure 3-1 System log Setting GUI

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

----End

2.9.11 Firmware upgrade

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

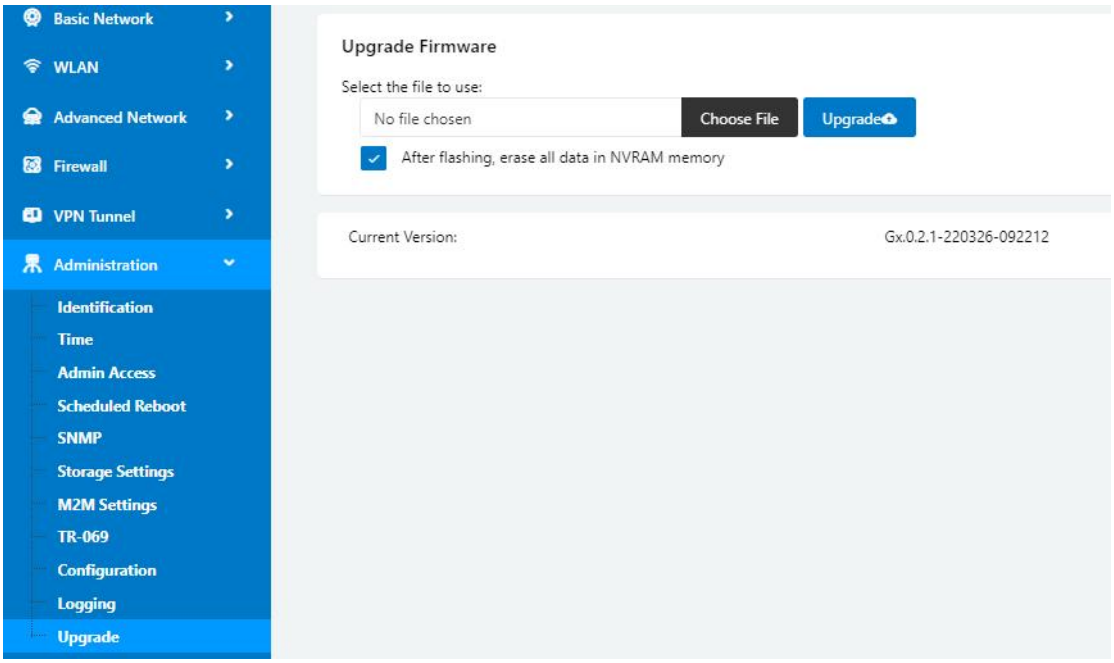


Figure 3-1 Firmware Upgrade GUI

NOTE

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

2.10 “Reset” Button for Restore Factory Setting

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

“Reset” button is near to Console port in WL-G230 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 2-40 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

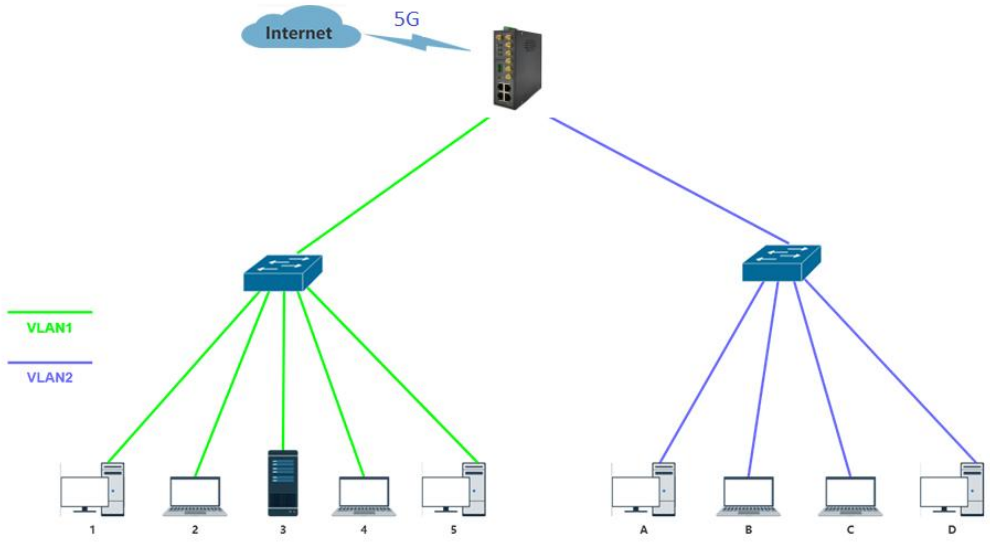
After reboot, the previous configuration would be deleted and restore to factory settings.

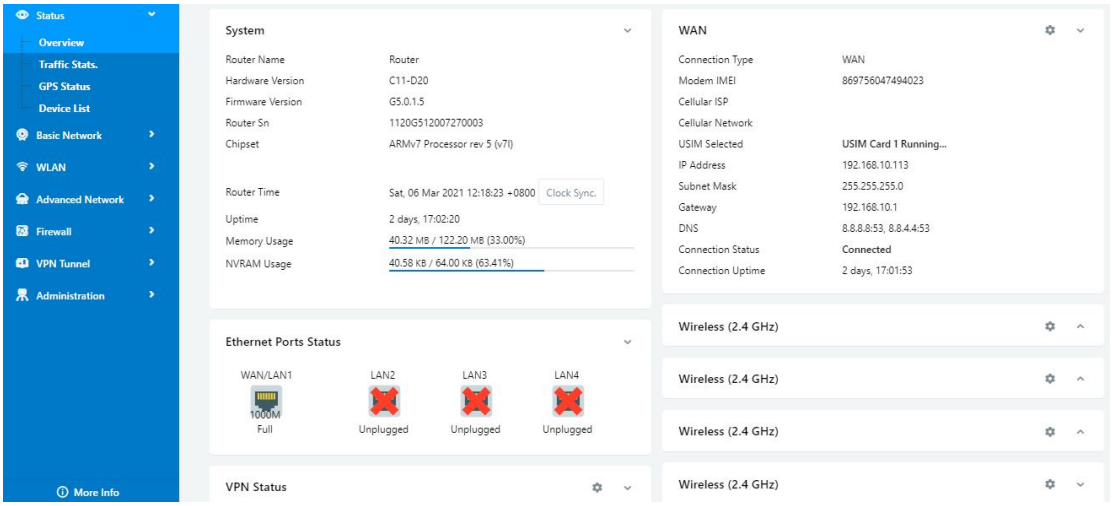
3 Configuration Instance

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.

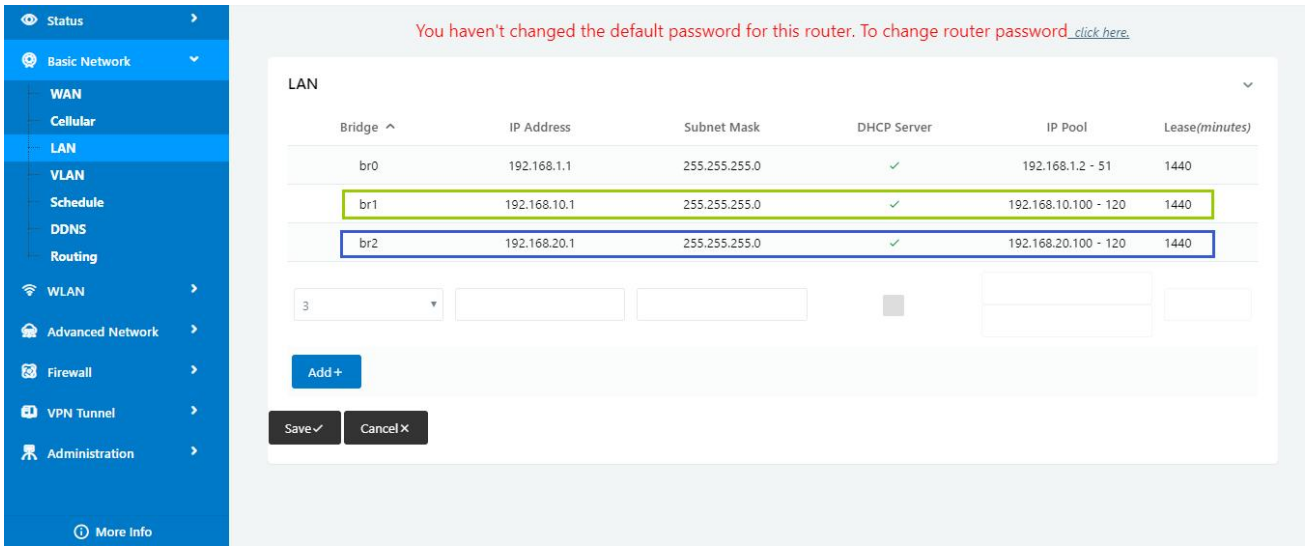
3.1 VLAN

WL-G230 supports VLAN partition based on Ethernet port (LAN1~LAN4)

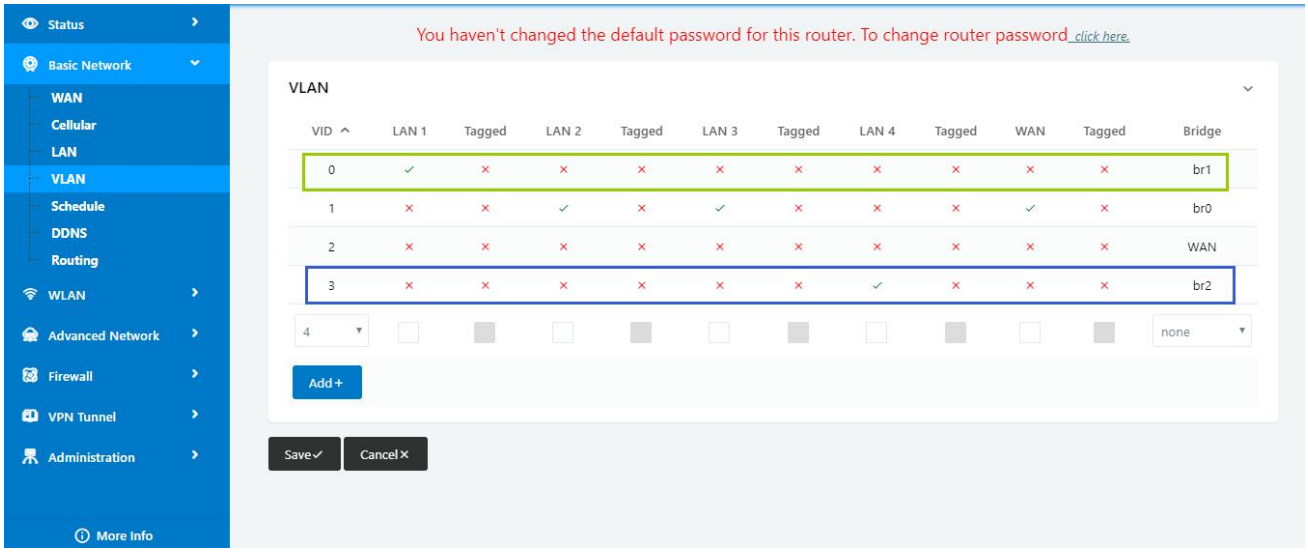




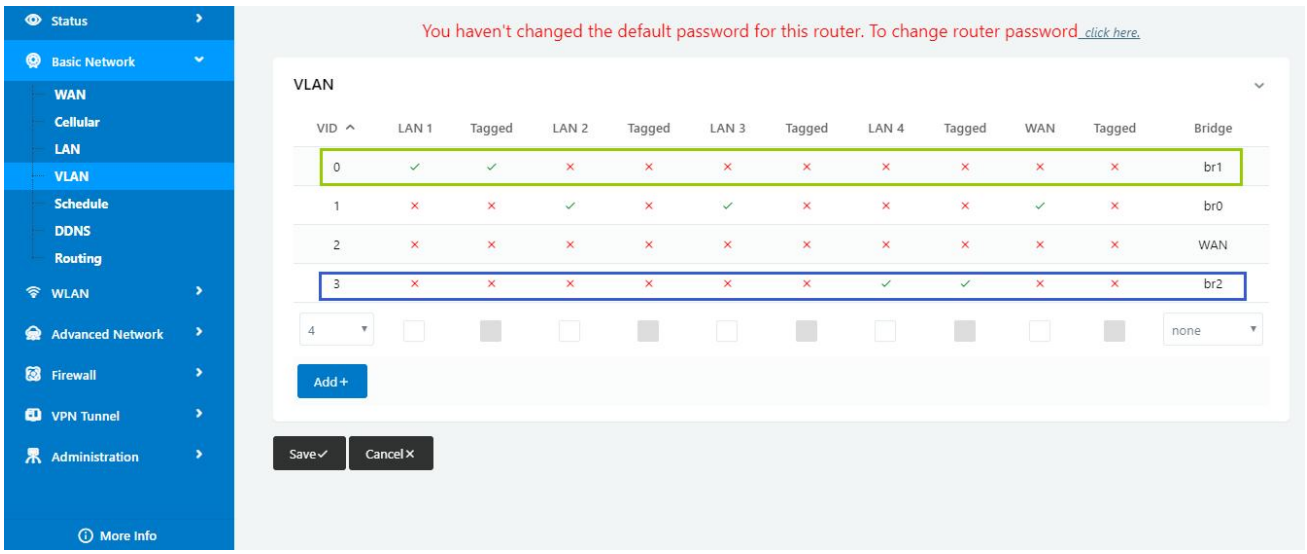
1) Configure LAN with Basic Network.



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.

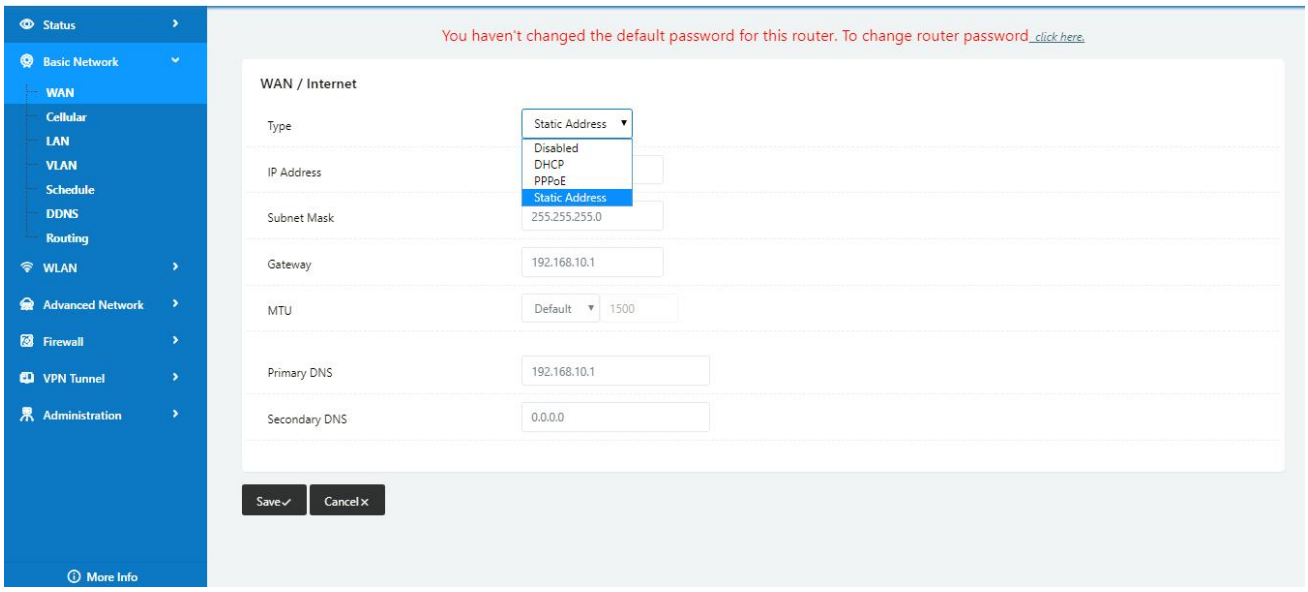


---End

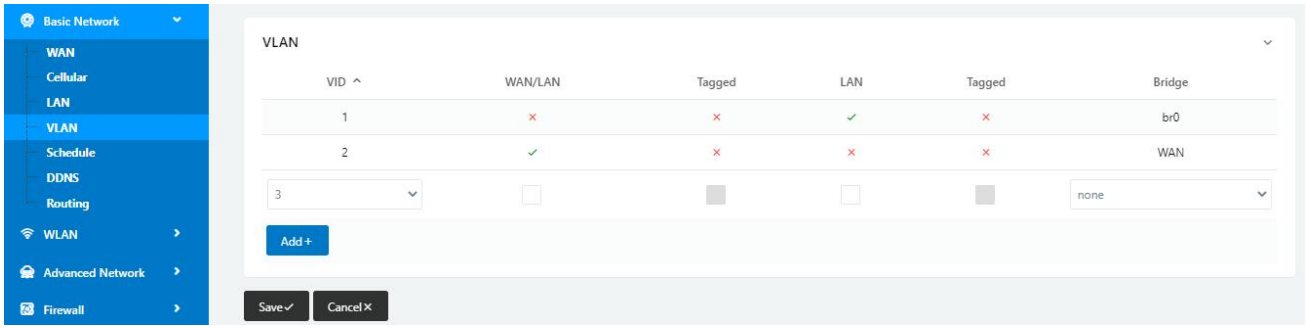
3.2 WAN Backup (WAN as Main, Cellular Backup)

The WAN and Cellular backup feature can quickly switch traffic to Cellular (link2) when WAN (link1) fails, and WL-G230 brings you a stable network experience.

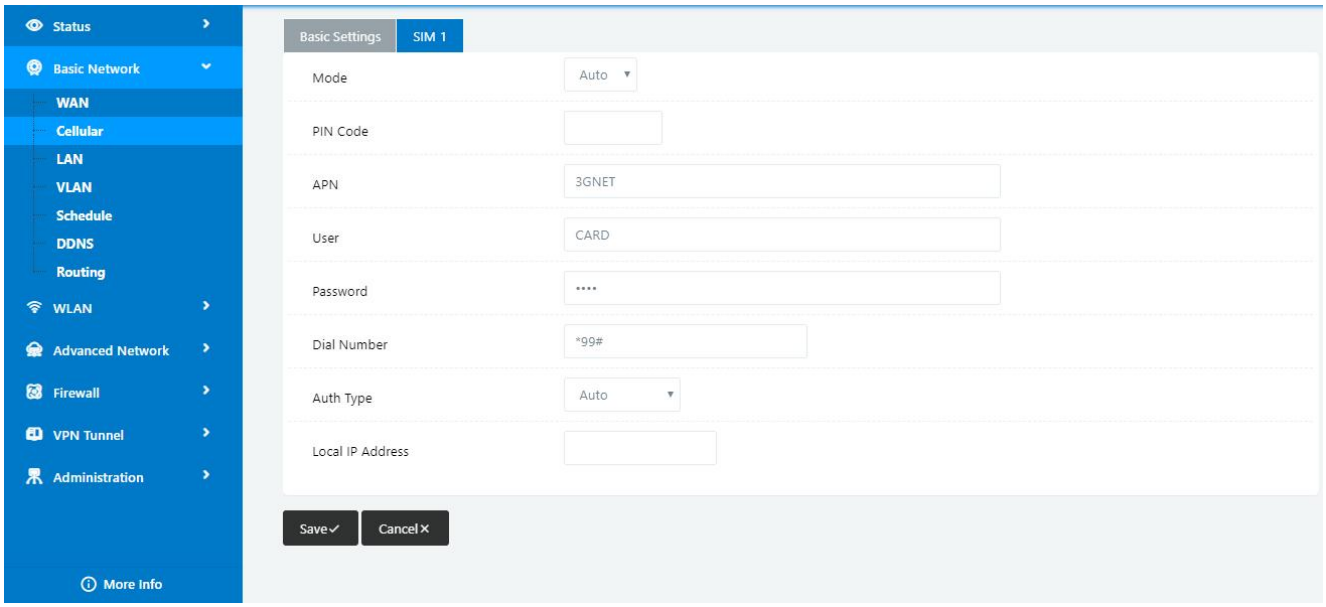
1) Navigate to Basic **Network > WAN**, you may configure the WAN parameters with your situation



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



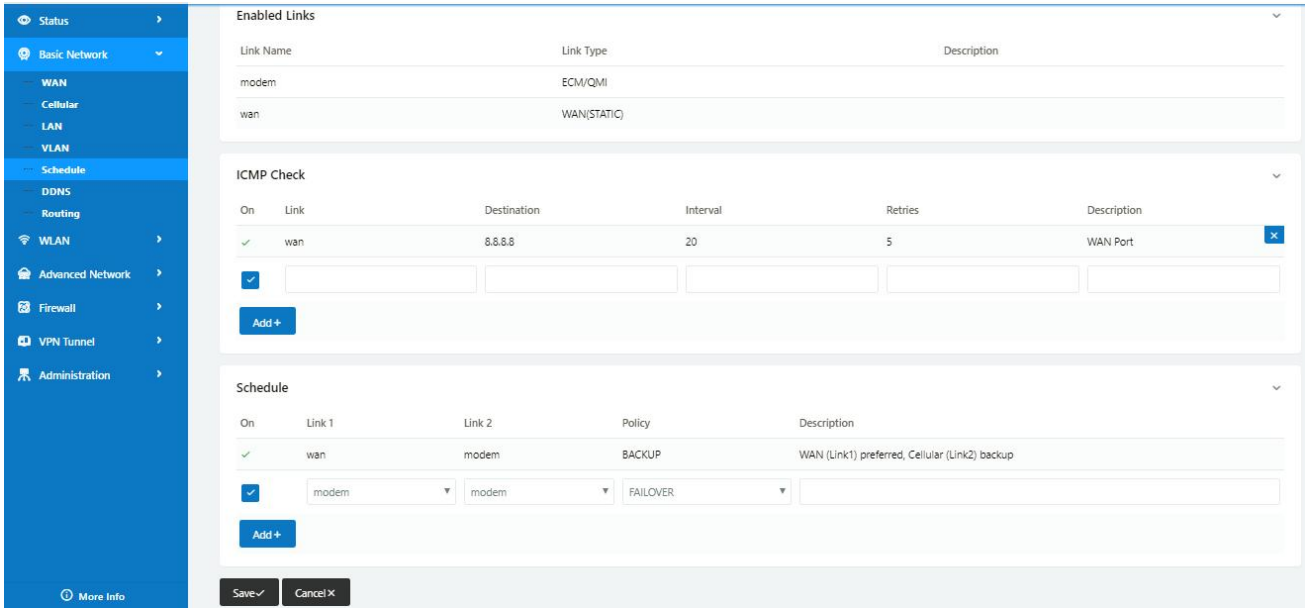
3) Navigate to **Basic network > Cellular**, configure the APN as your SIM



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

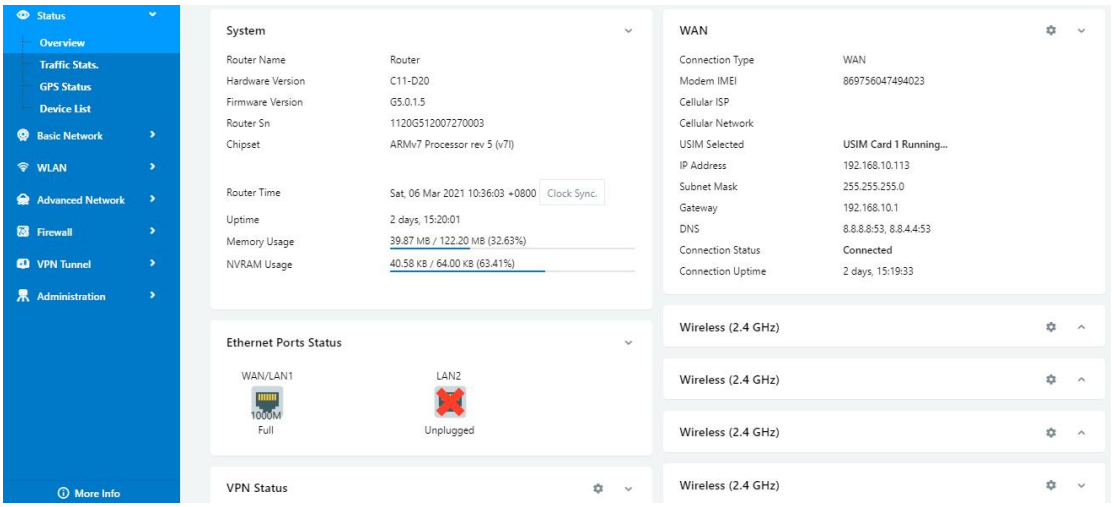
Add ICMP Check to WAN

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

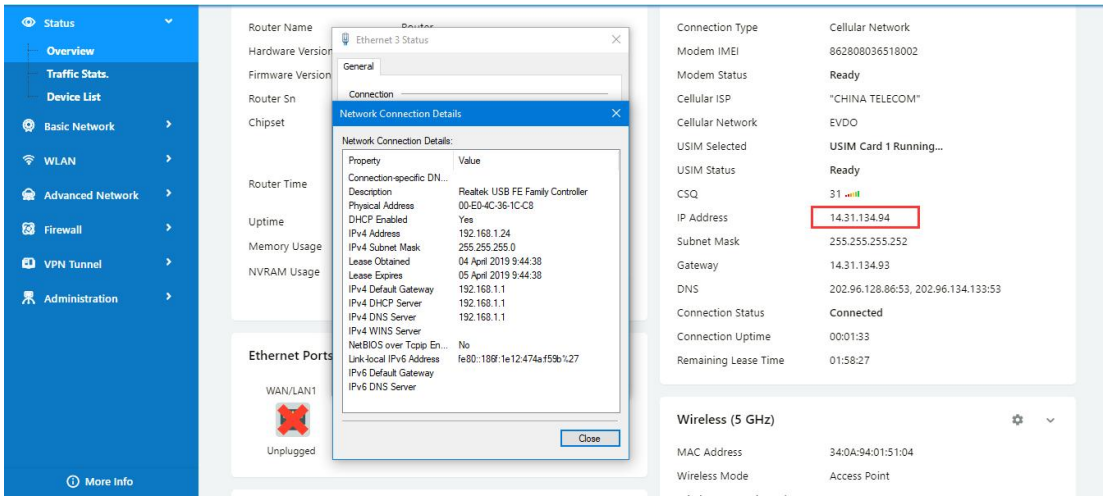
---End

3.3 Port Forwarding

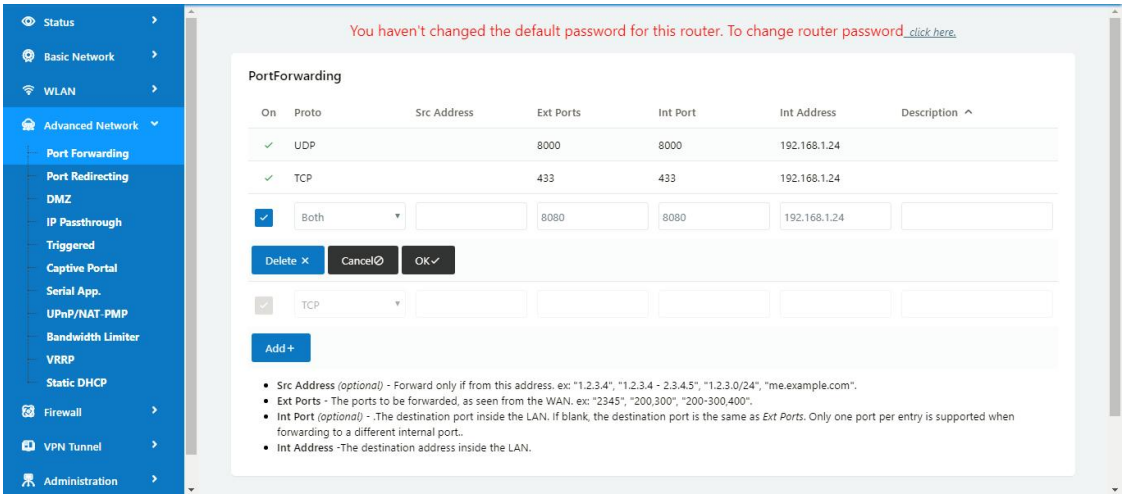
1) The router online and got a public IP address 14.31.134.94

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

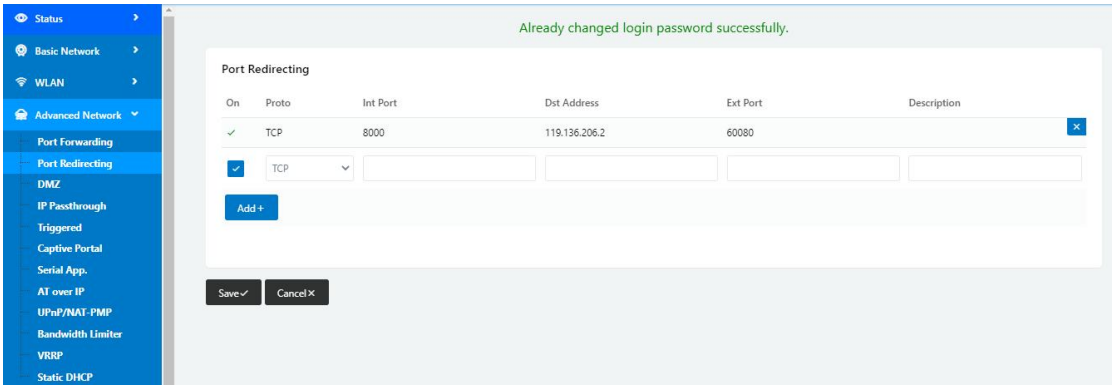


4) The PC can be accessed via 14.31.134.94:443 over Internet

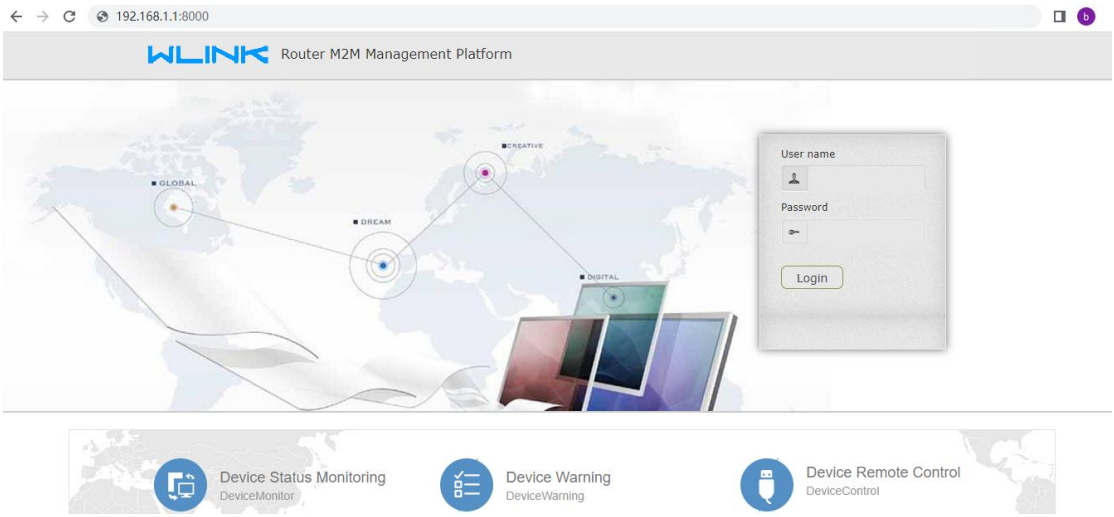
---End

3.4 Port Redirecting

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



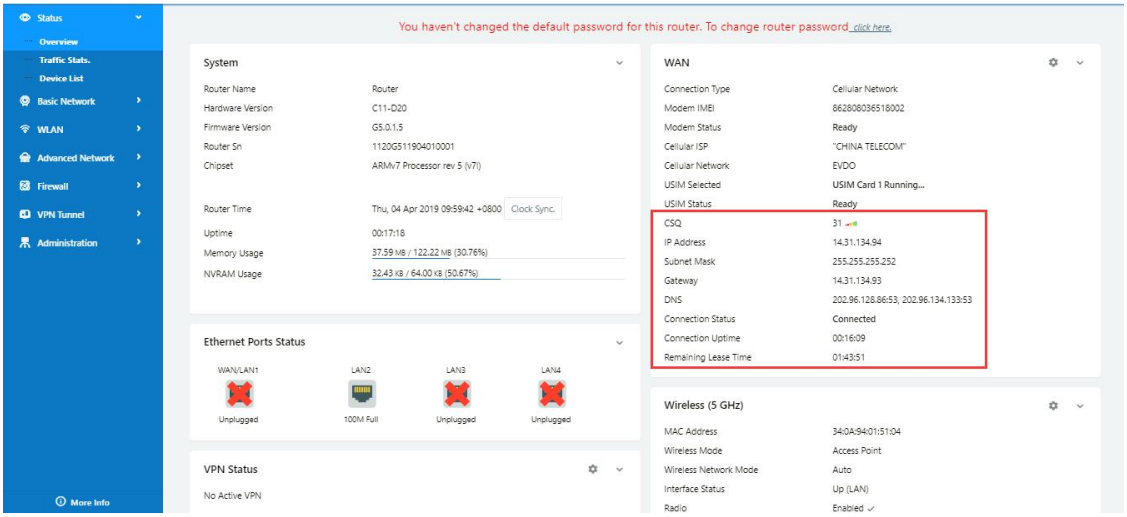
Configure Internal port as 8000, the Destination IP address as 119.136.206.2 and External port 60080(M2M Platform Server IP and Port as example). Access to 192.168.1.1:8000 in browser, the router will redirect to 119.136.206.2: 60080.



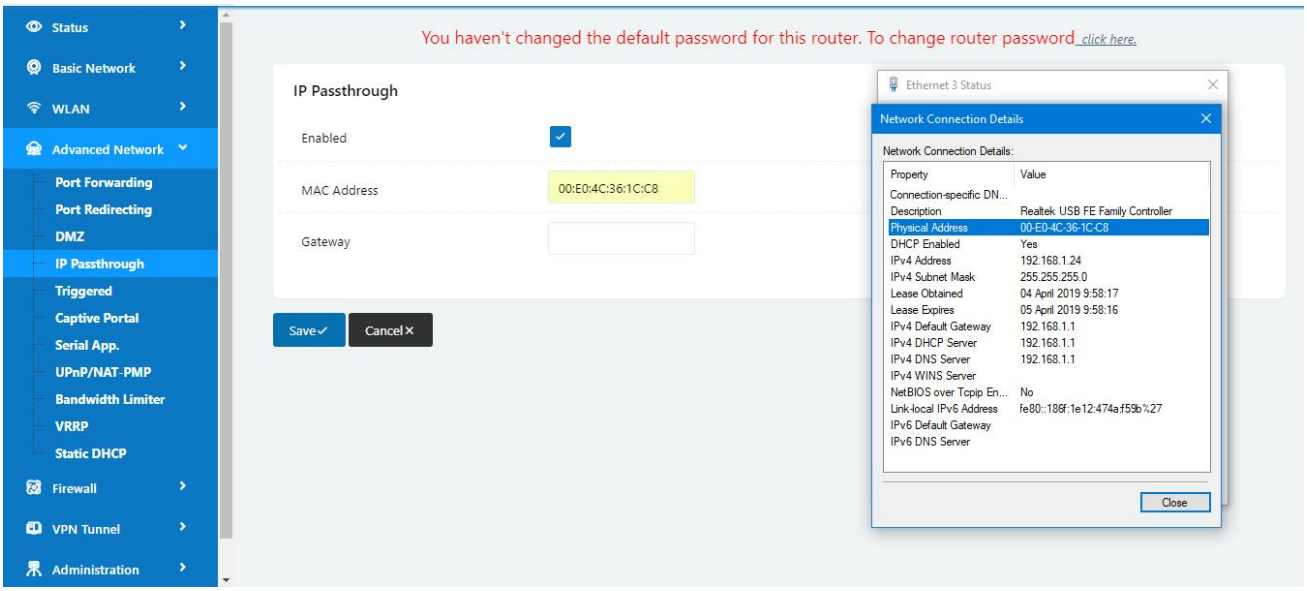
---End

3.5 IP Passthrough

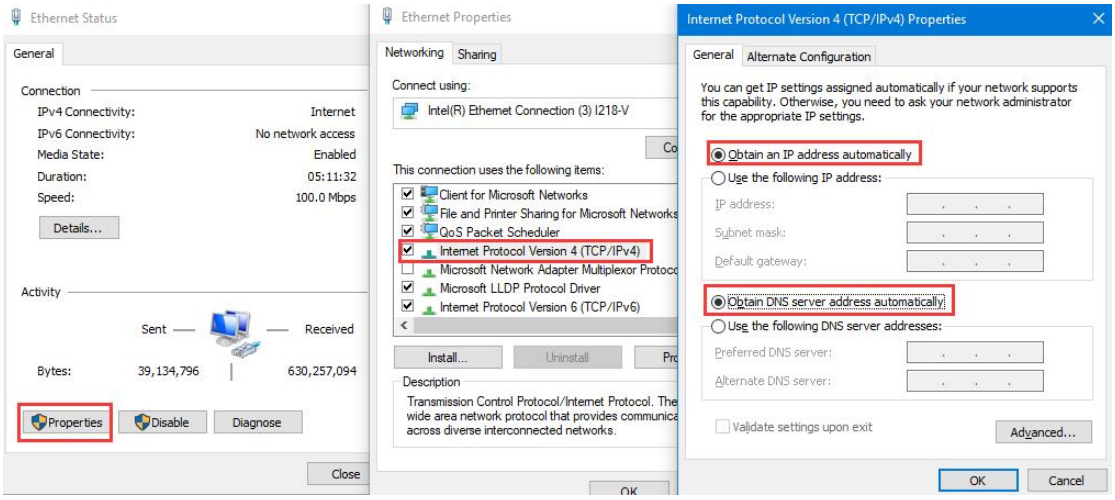
1) The router online



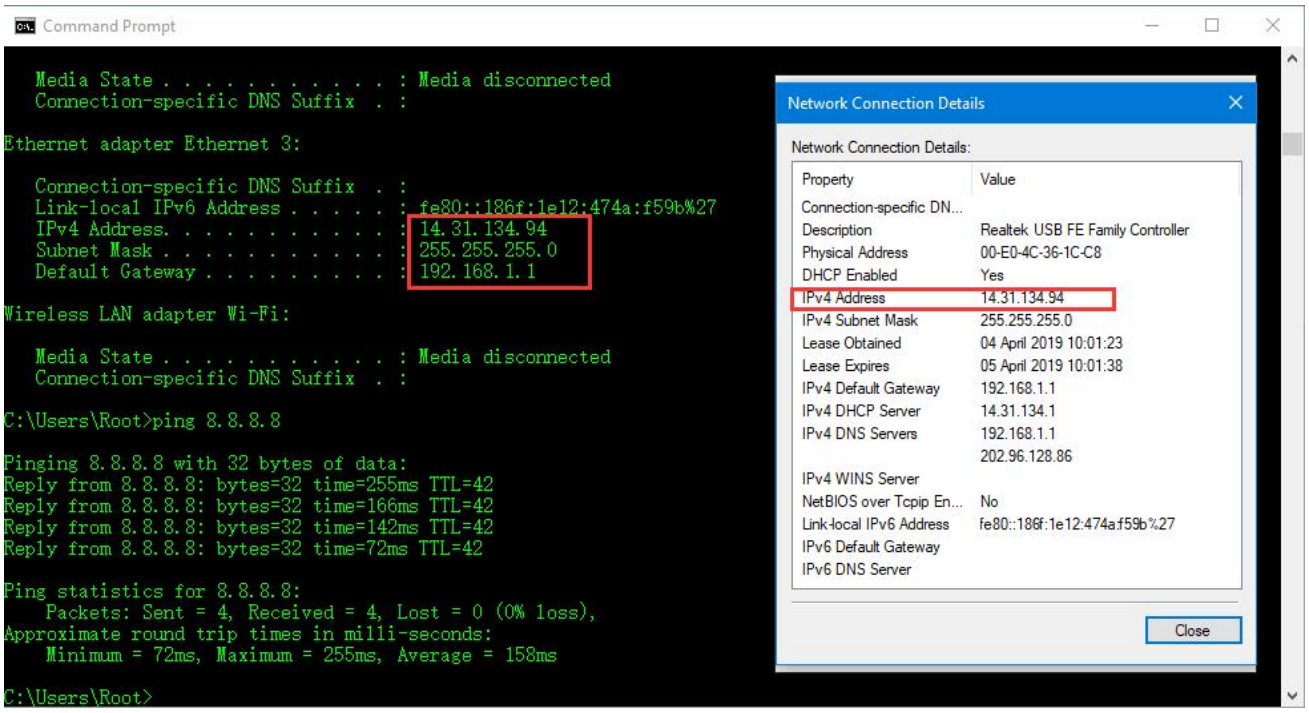
2) Configure IP passthrough destination MAC address (PC Ethernet MAC)



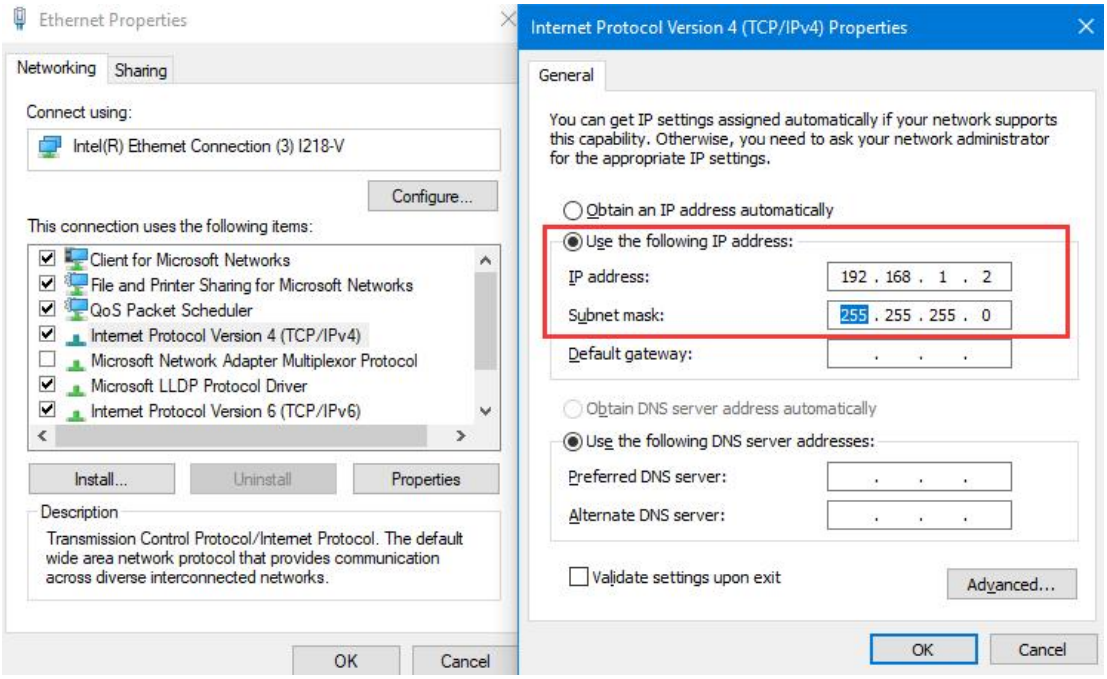
3) Set the PC to DHCP



4) Check the Ethernet status and ping test



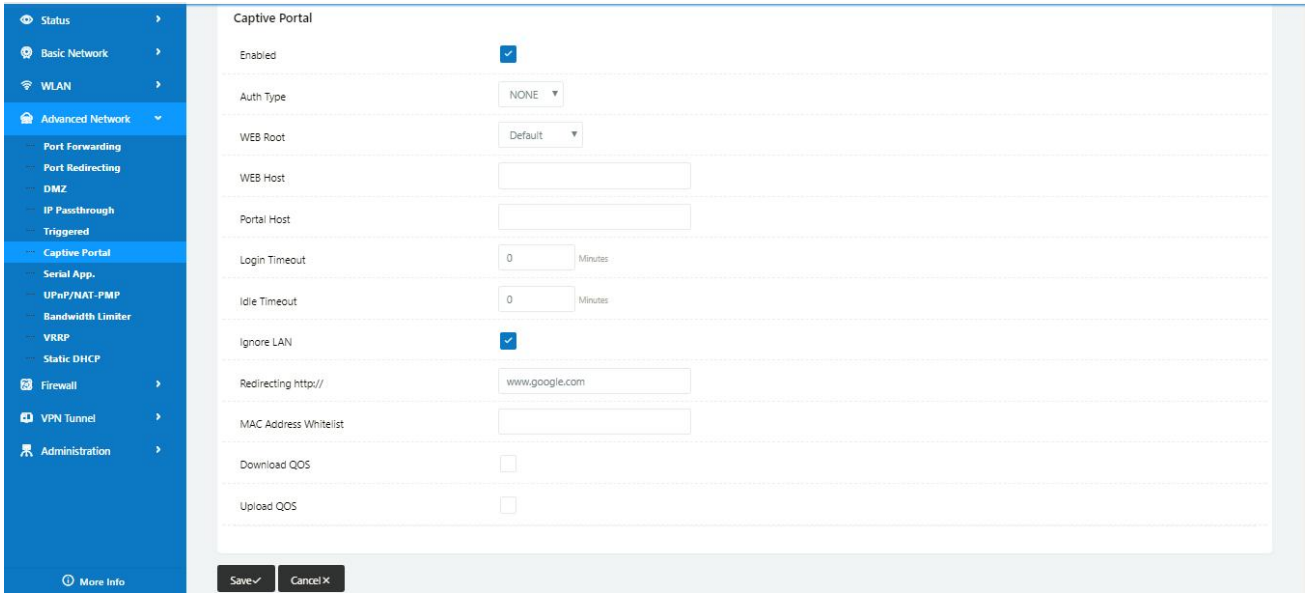
5) Set the PC Ethernet as DHCP to release the IP and access to router GUI again



---End

3.6 Captive Portal

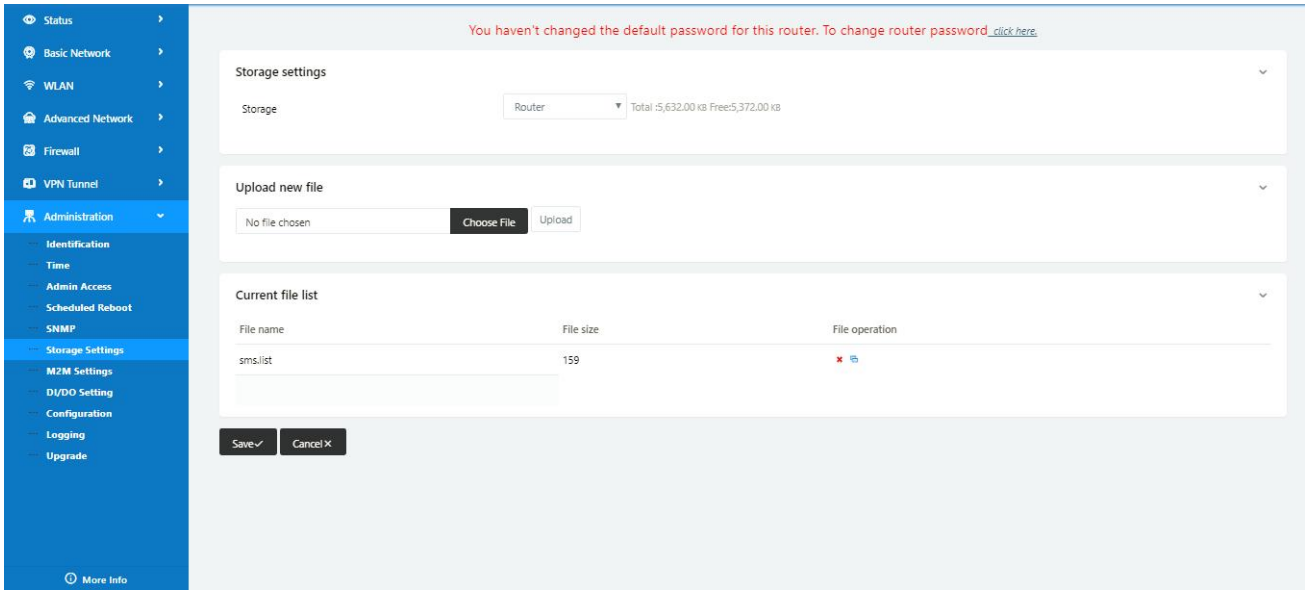
Please click “Advanced Network> Captive Portal” to check or modify the relevant parameter.



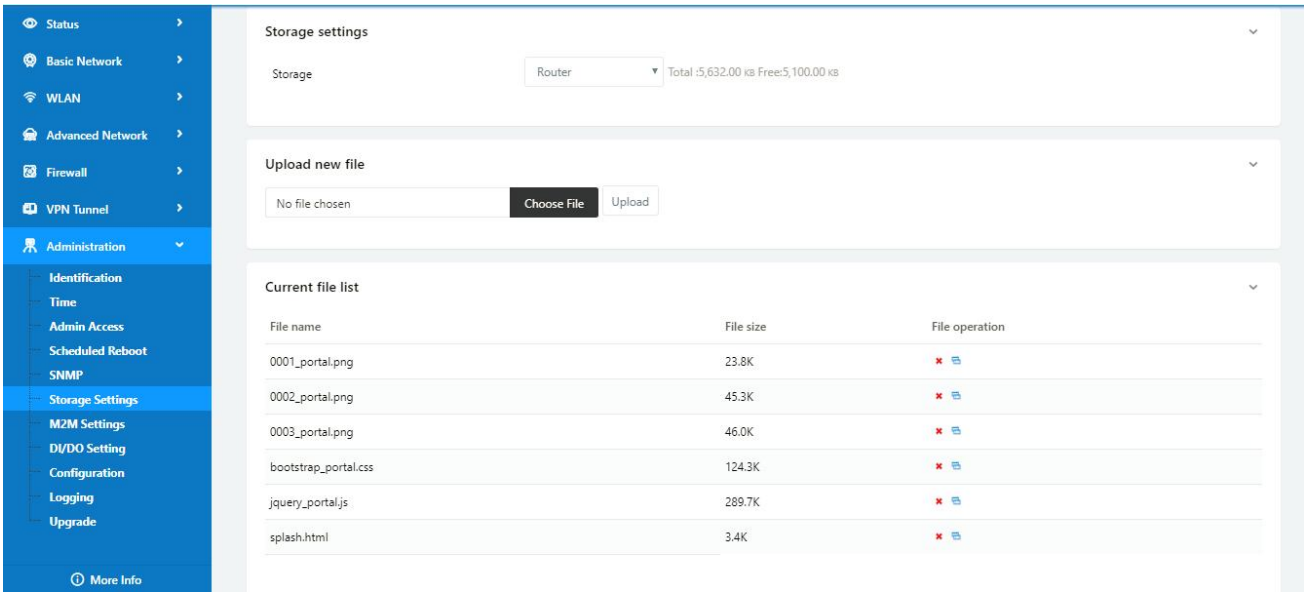
1) Upload Portal file and Splash.html by local

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.

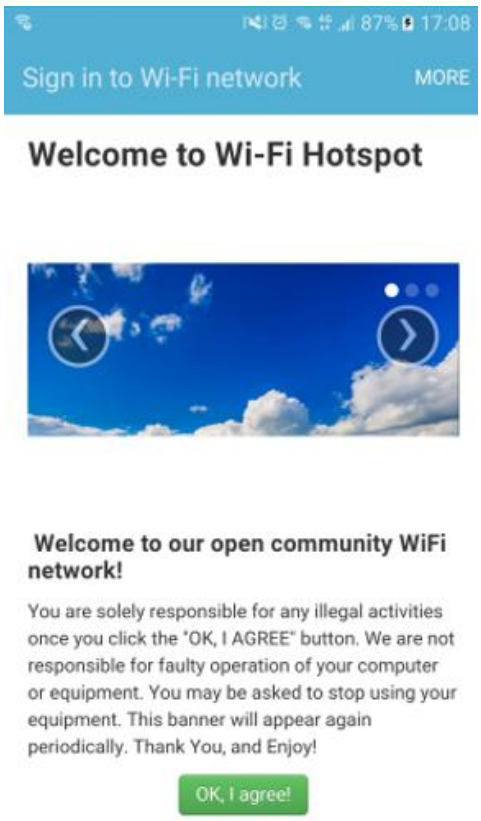


Each Ad file just supports 3 Ad portal images. Picture format is acceptable for png/jpg and image size is less than 100Kbytes and resolution is 800*600. Picture name is 0001_portal.png, 0002_portal.png and 0003_portal.png. Furthermore, please keep image names the same between portal file and splash.html.



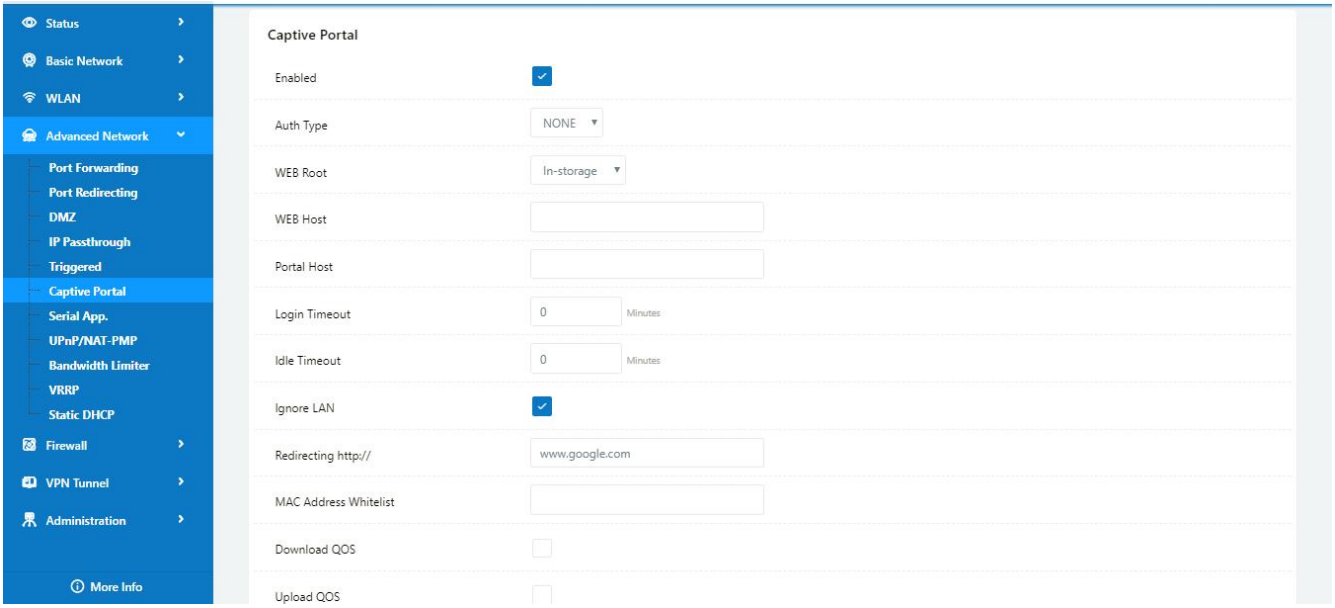

```
<!-- <hr> -->

<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.

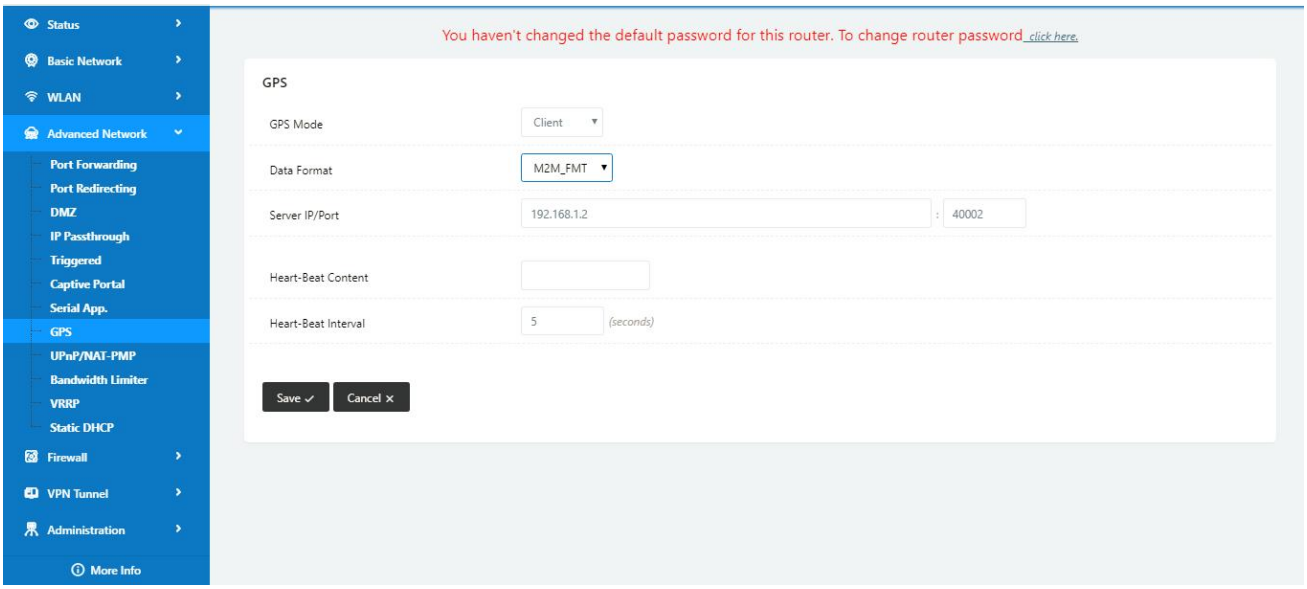


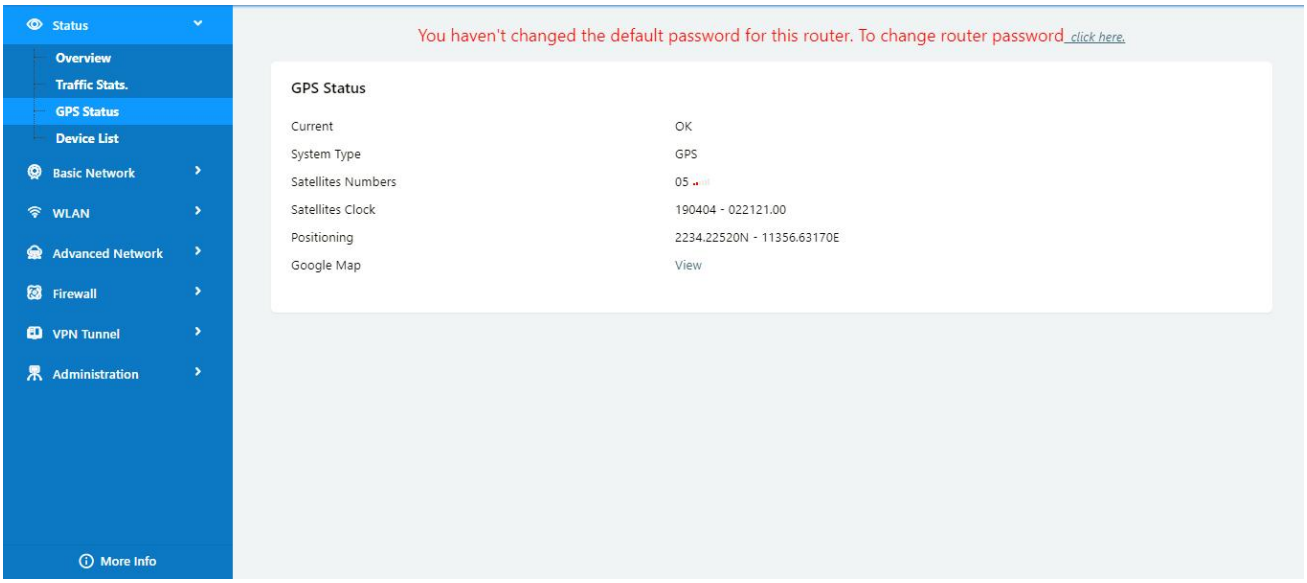
Table 4-6 “GPS” Instruction

parameter	Instruction	Default
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

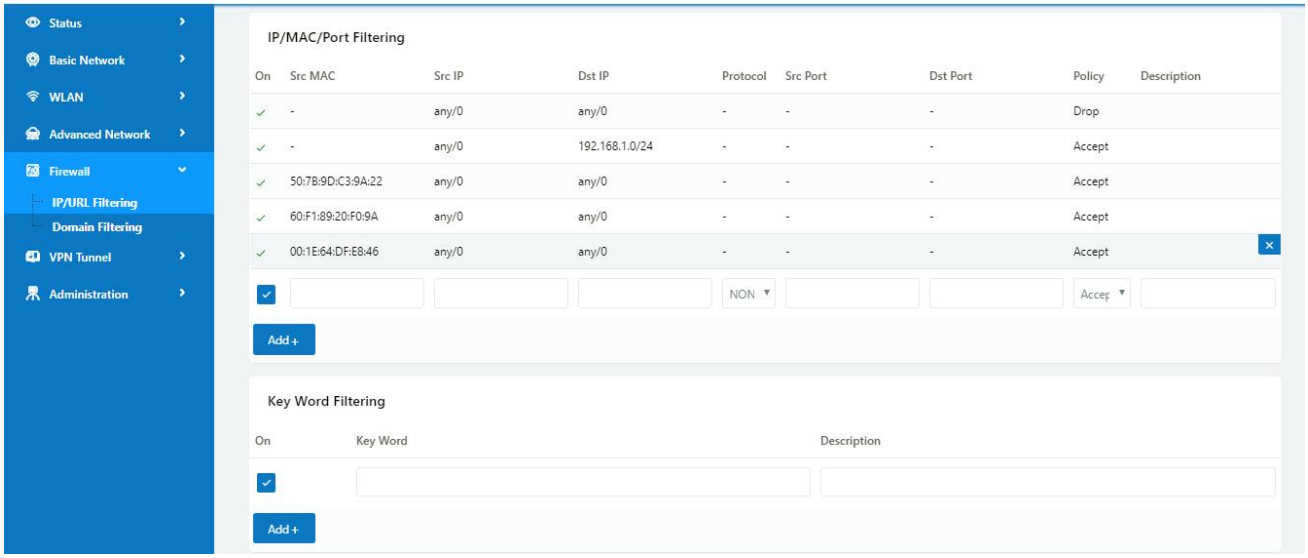
3.8 Firewall

1) IP/MAC/Port Filtering

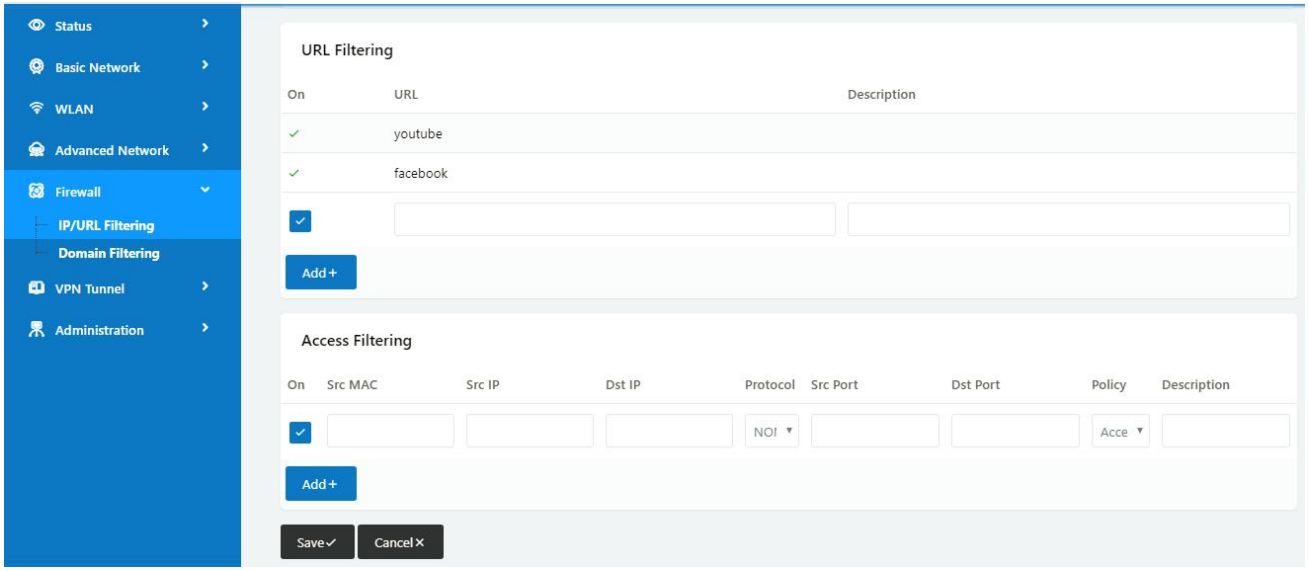
This part used to intercept packages from router's WAN/Celluar interface to Internet.

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)



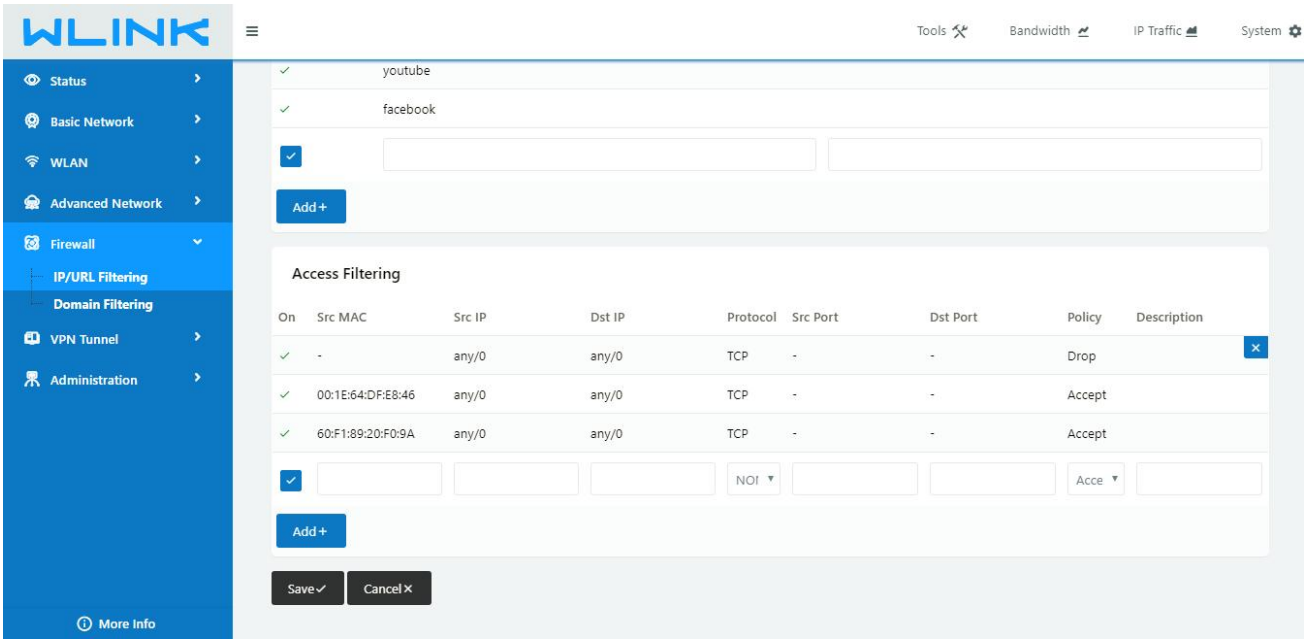
2) Key Word Filtering
This part used to filter key word packages from router's WAN/Cellular interface to Internet.



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.

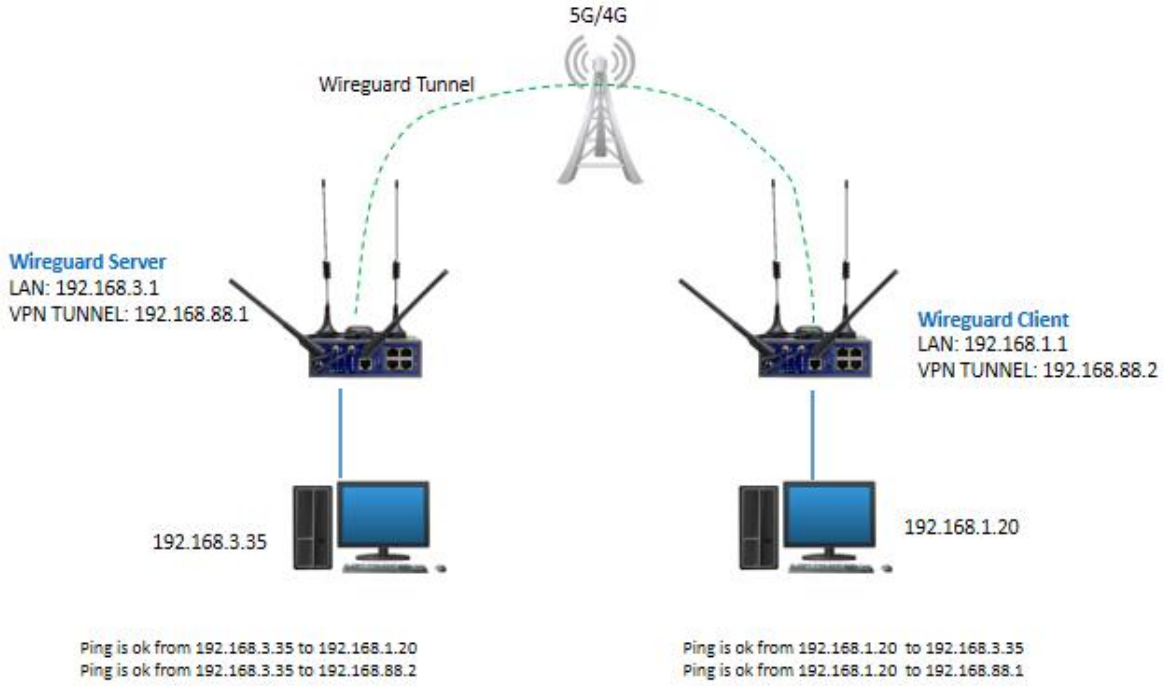


---End

3.9 VPN Tunnel

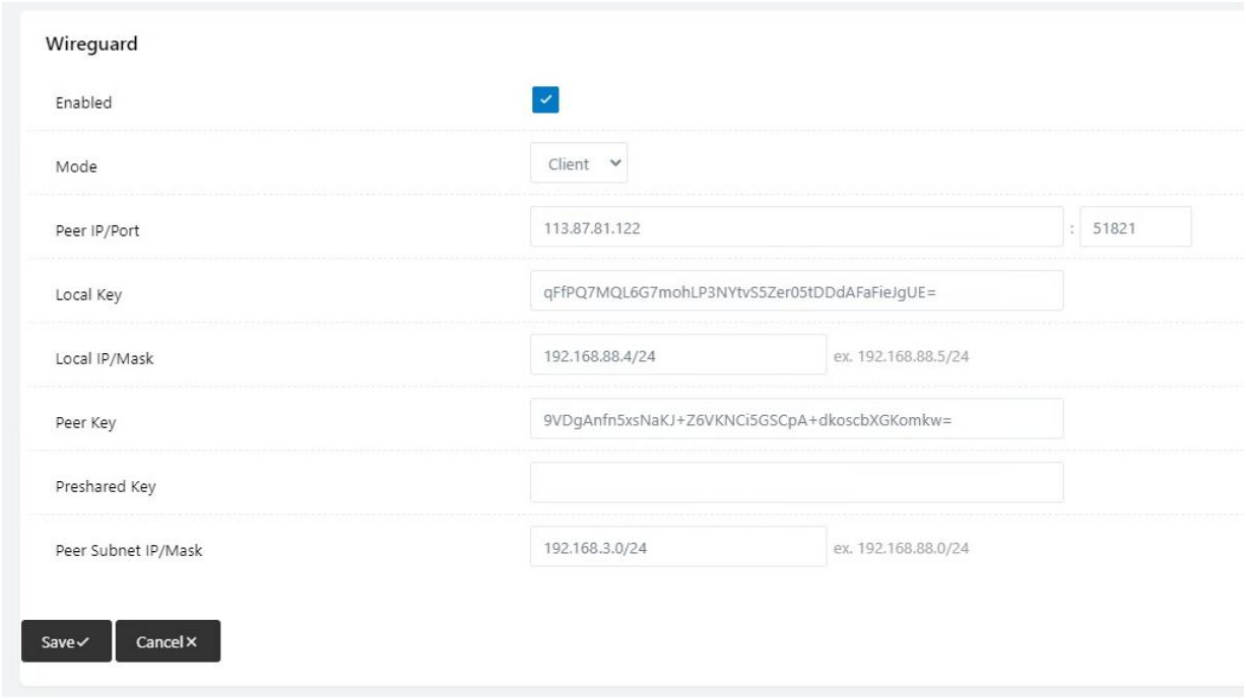
3.9.1 Wireguard VPN

Wireguard VPN between two WLINK Routers



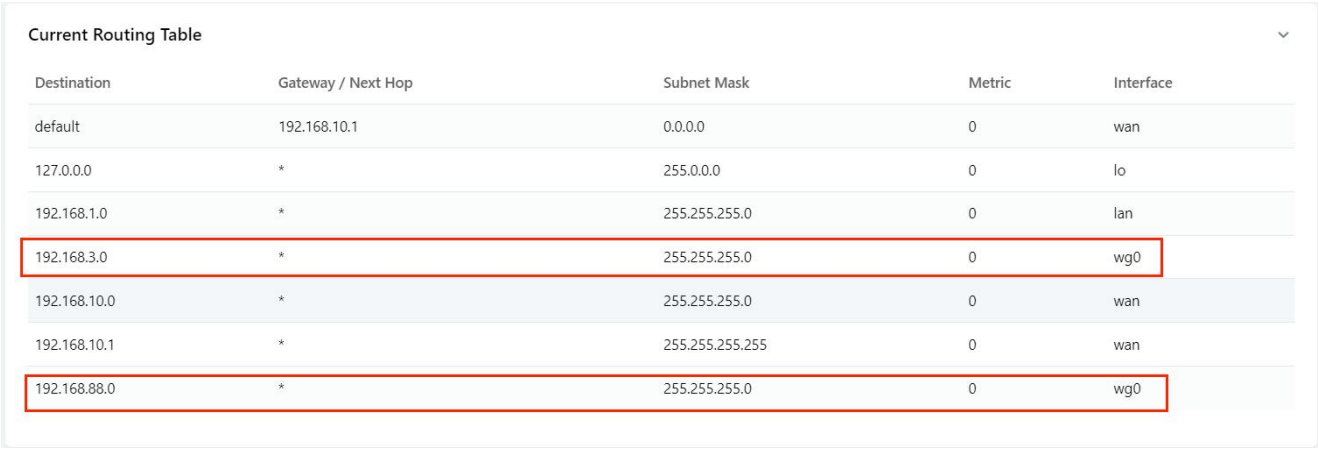
1) Wireguard VPN Client Setting

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



2) Wireguard Routing

There are two routings when Wireguard established.



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

3) Wireguard Connection Check

Check VPN connection via Ping testing.

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

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

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

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

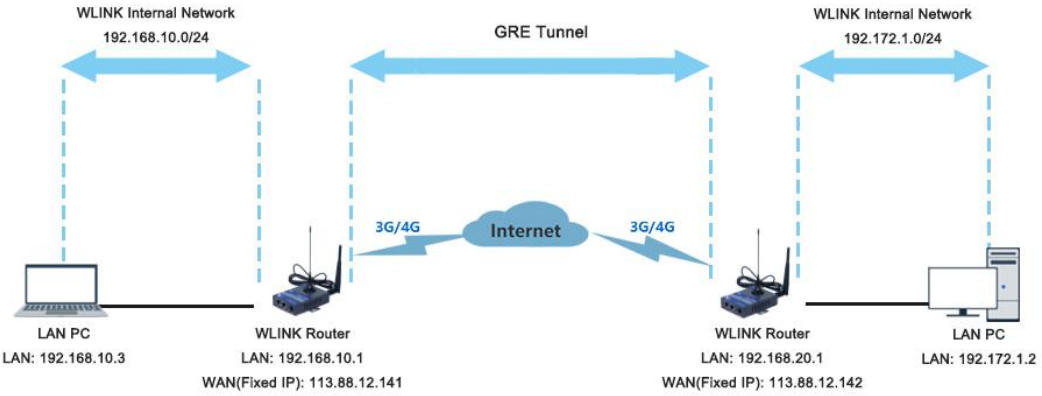
Wiregurad Peer Virtual IP

WG Server Gateway IP

WG Server LAN Host IP

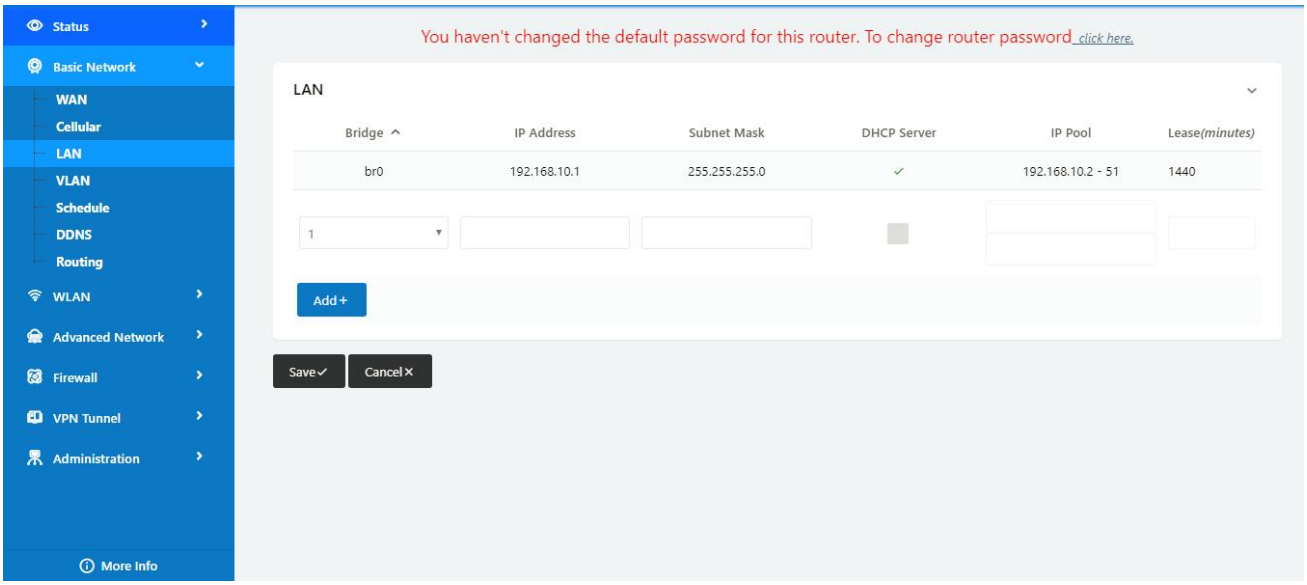
3.9.2 GRE

GRE Tunnel between WLINK Routers

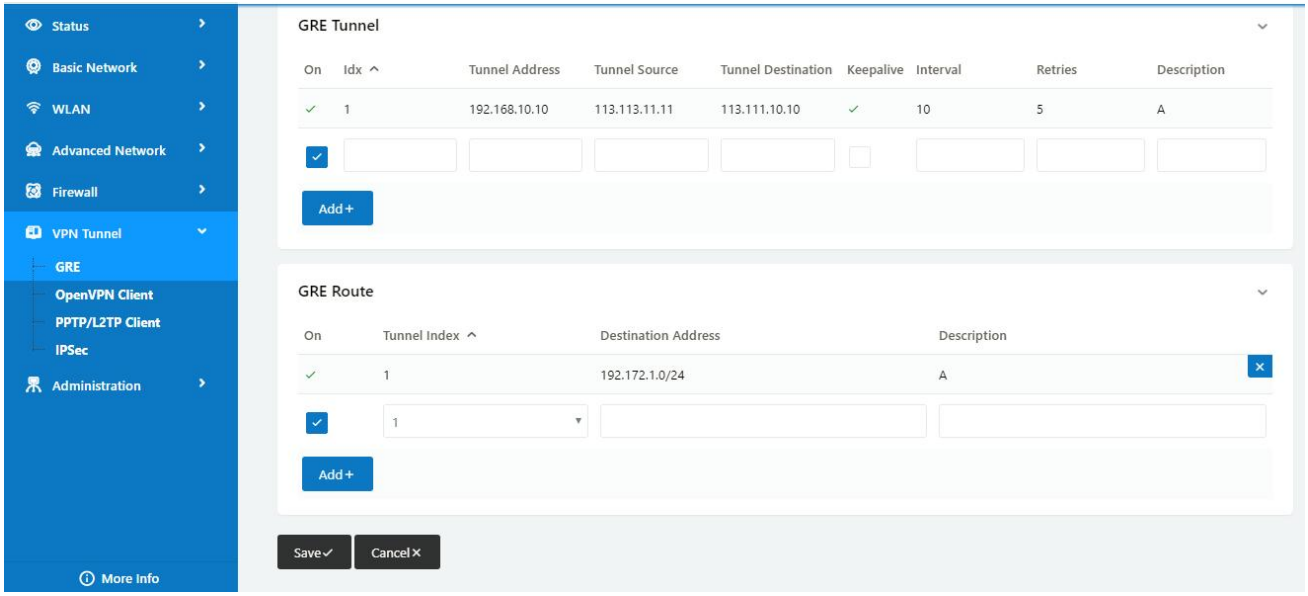


1) WL-G230(A) Config

Navigate to **Basic Network > LAN**

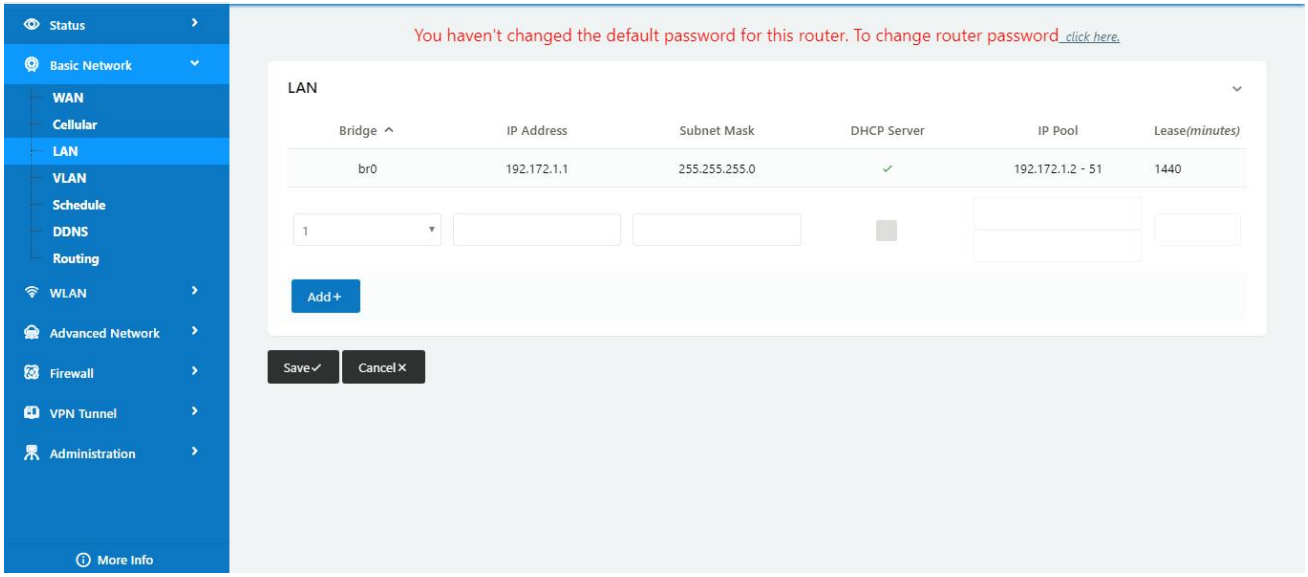


Navigate to **VPN Tunnel > GRE**

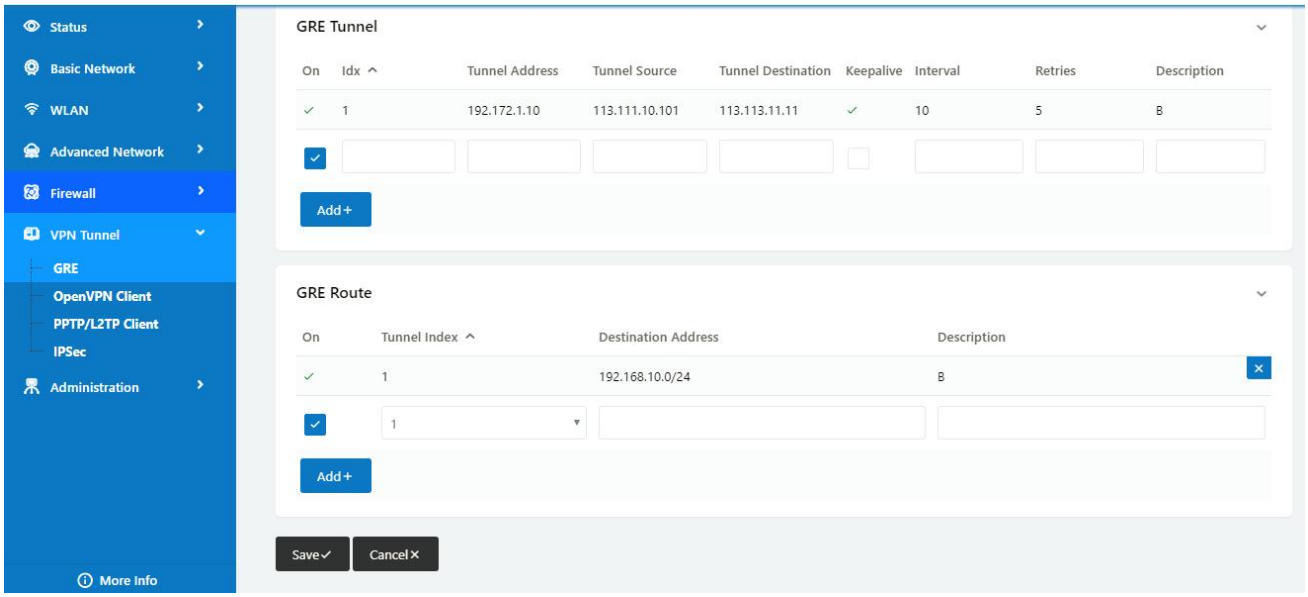


2) WL-G230(B) Config

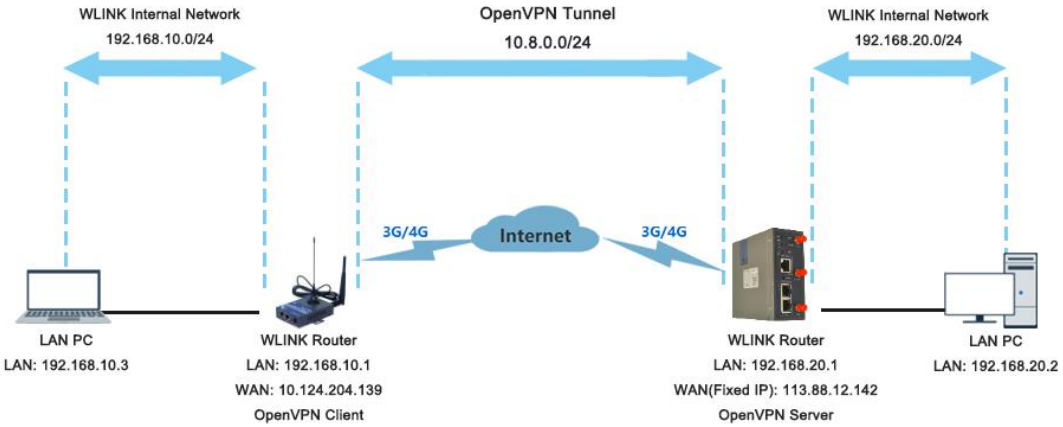
Navigate to **Basic Network > LAN**



Navigate to **VPN Tunnel > GRE**

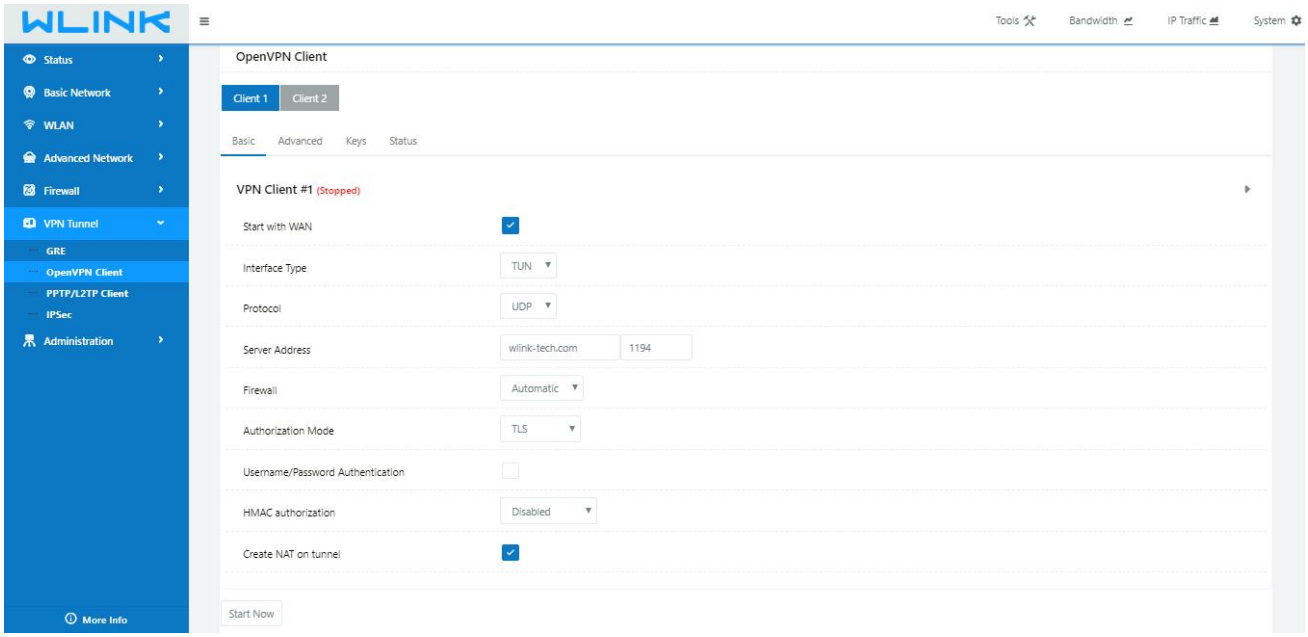


3.9.3 OpenVPN



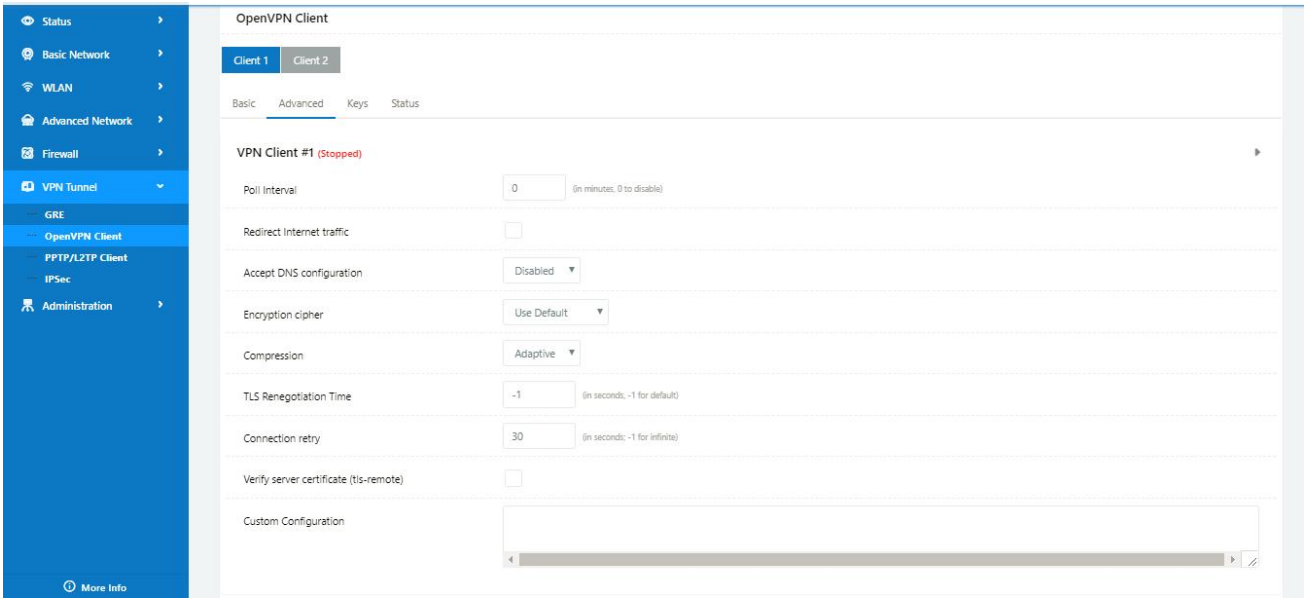
OpenVPN between WL-G230 client and Server

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

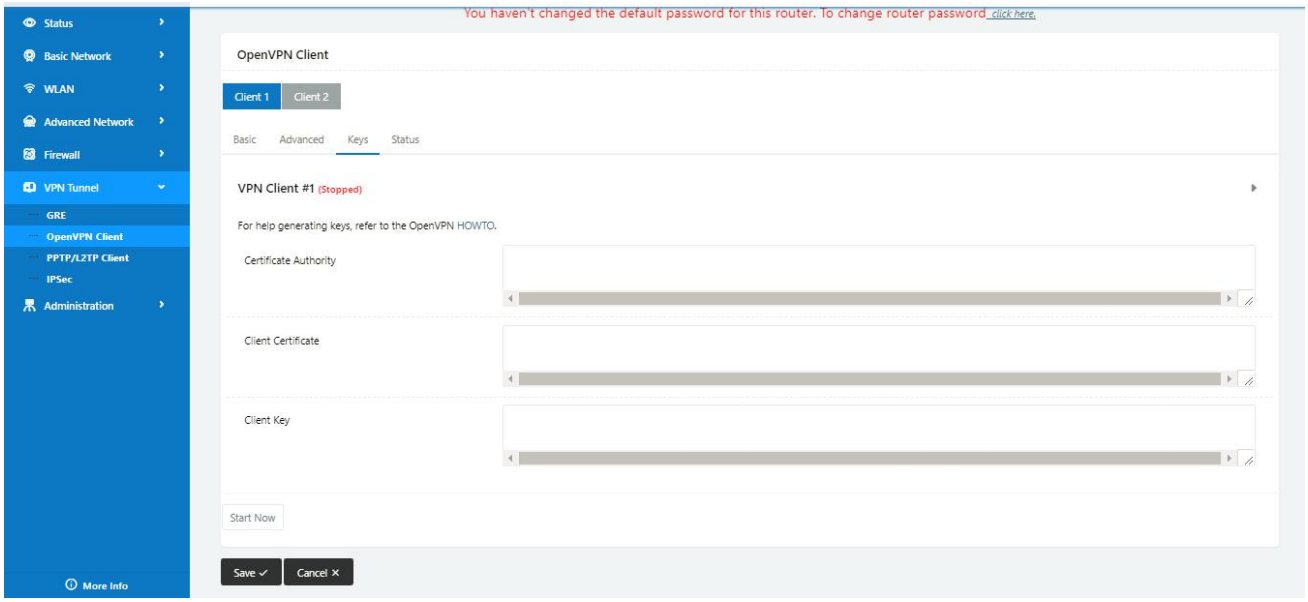


Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 4G/3G/WAN port.
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode.
Protocol	UDP and TCP optional.
Server Address	The Openvpn server public IP address and port.
Firewall	Auto, External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

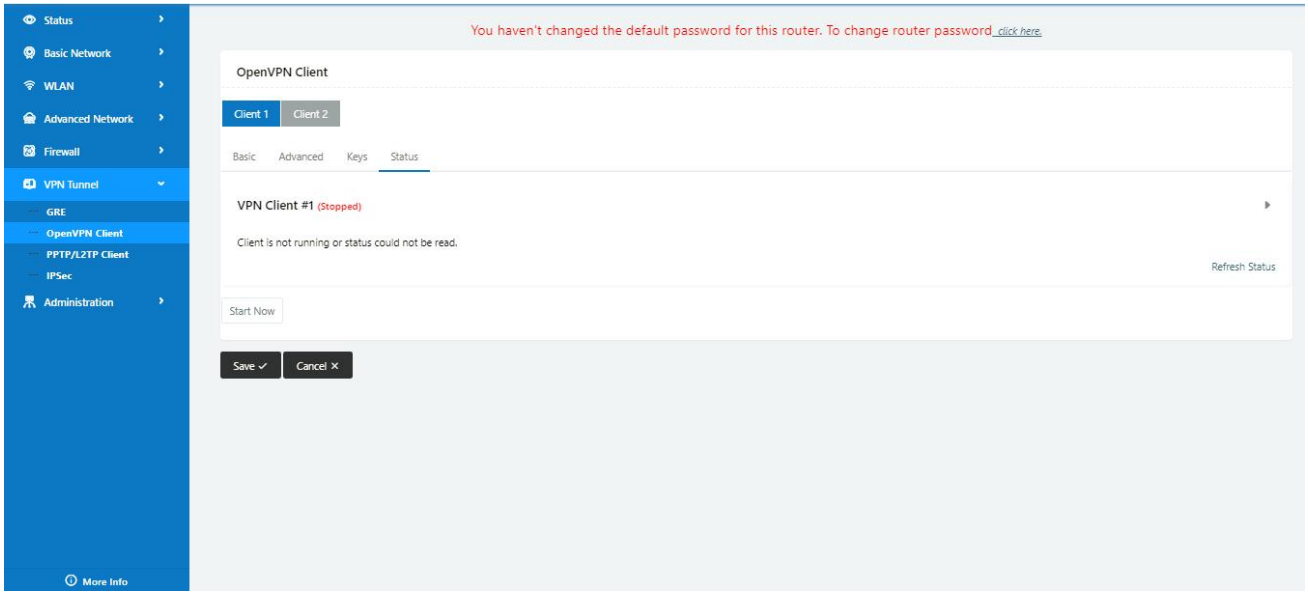
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.



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



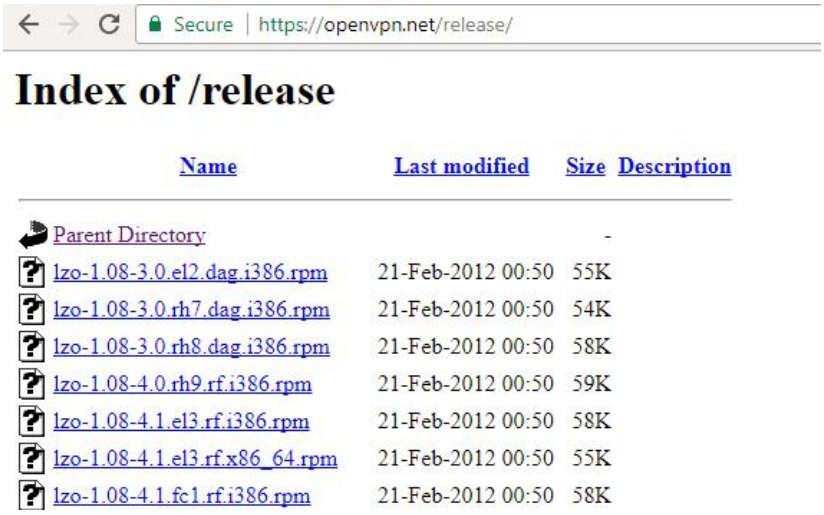
Parameter	Instruction
Status	Check OpenVPN status and data statistics.

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

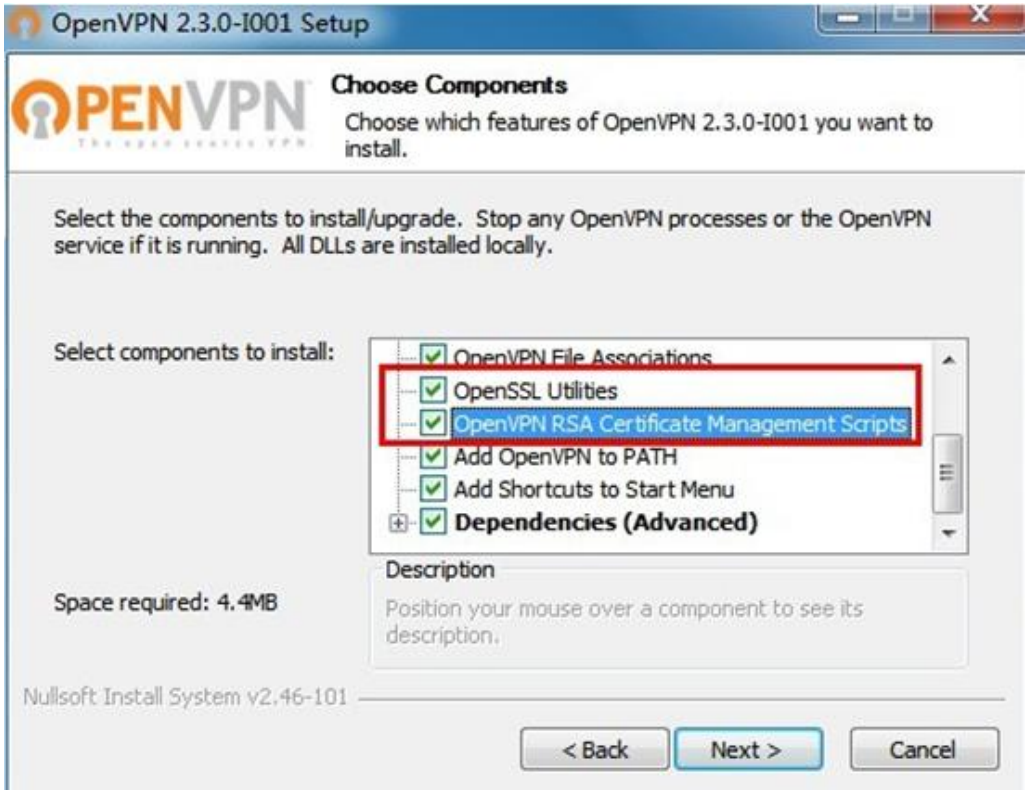
OpenVPN Keys Guide

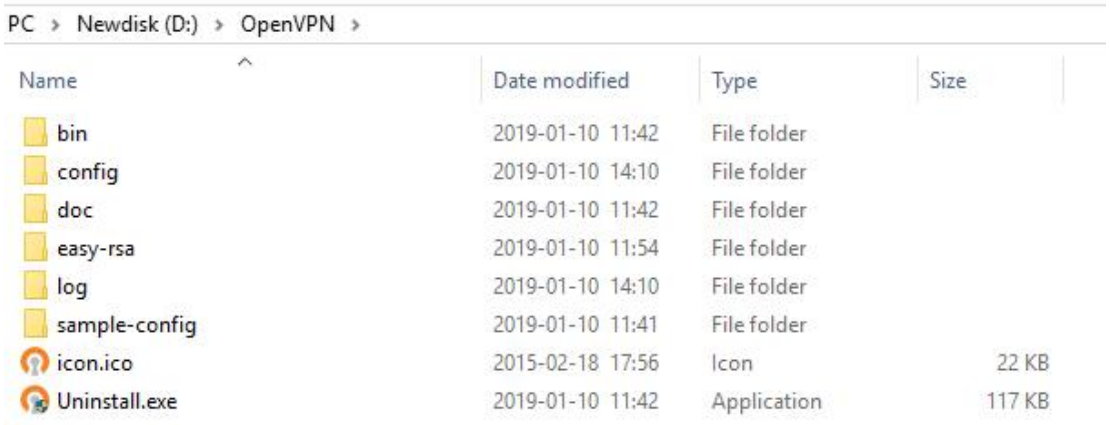
The fllowing steps are for server running on Windows 7/8/10

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

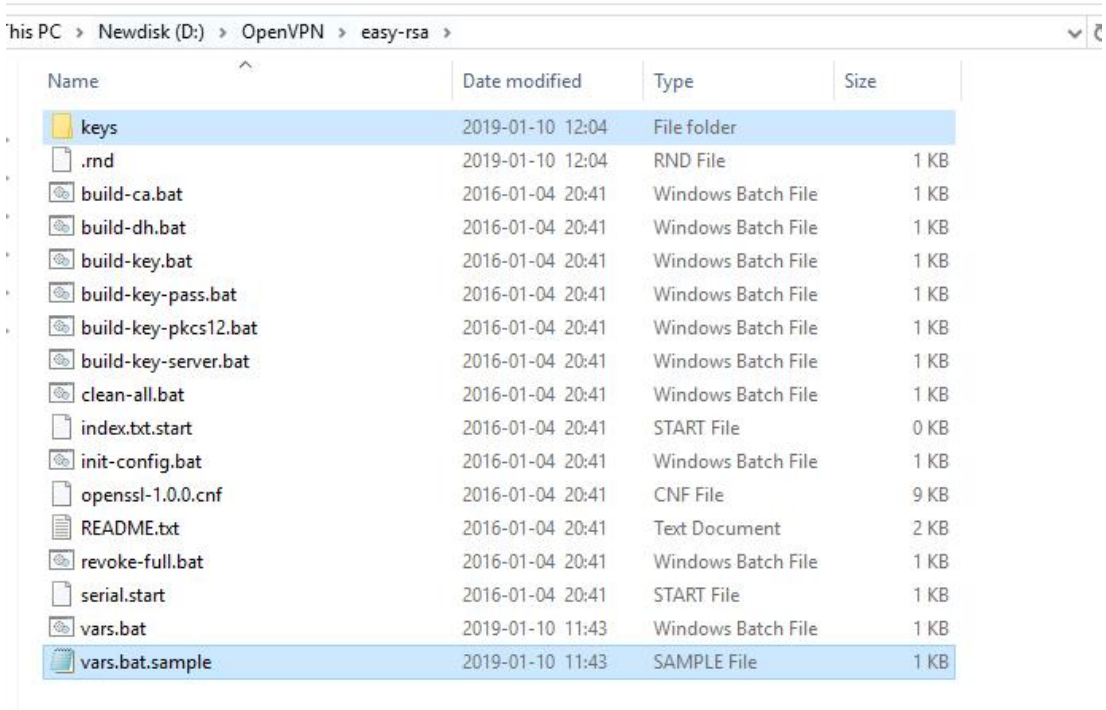


After installing OpenVPN, please find the OpenVPN folder to generate the certificate of server and client. (Access to http://openvpn.net for more information)



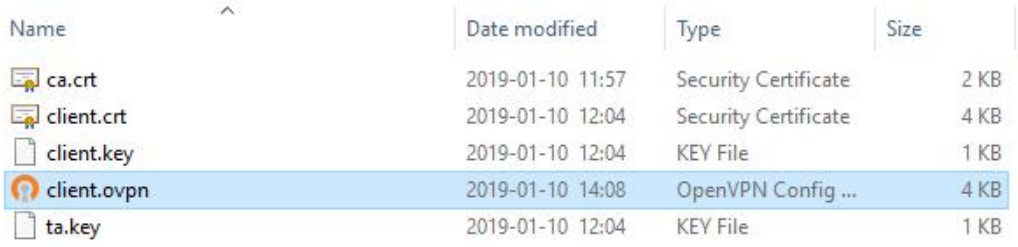


Configure “vas.bat.sample” to complete the initialization step and keys

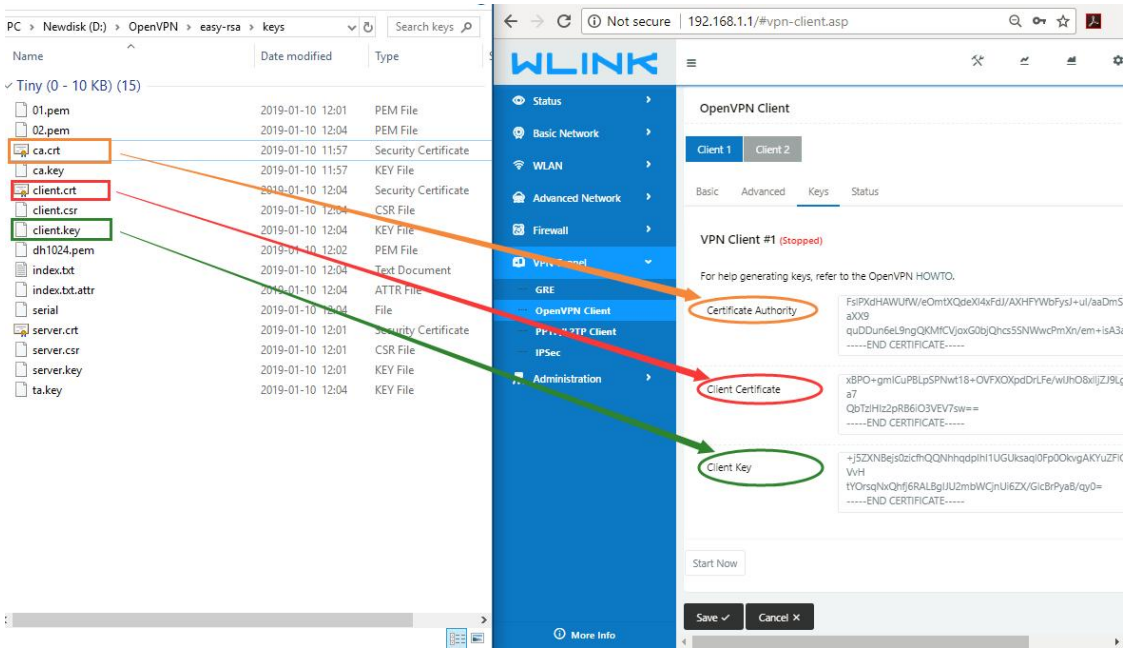


Configure the client keys to WLINK OpenVPN client GUI when you create the server and client certificate in the path OpenVPN/easy-rsa/keys

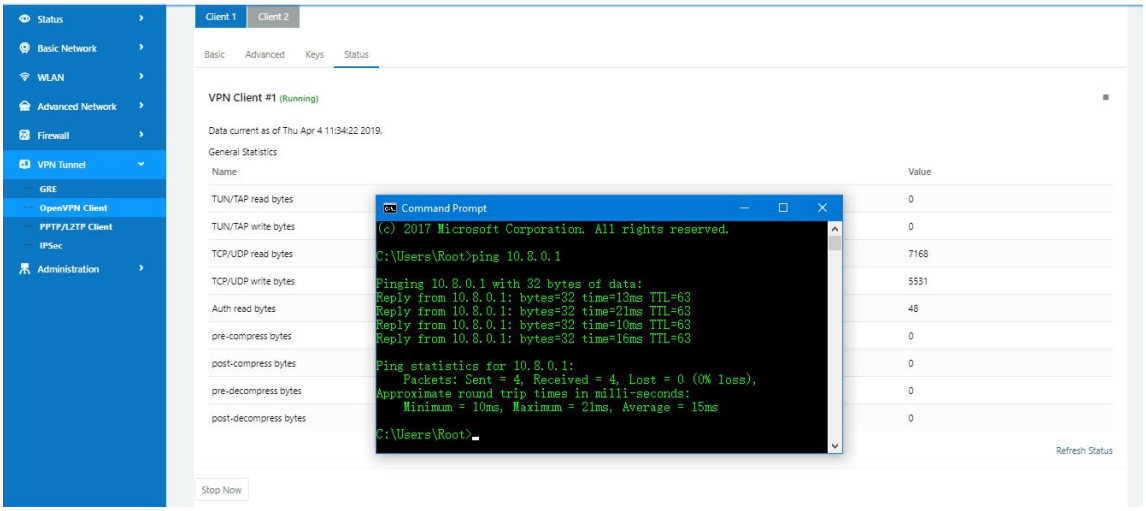
Client certificate (Generated on the server)



OpenVPN>easy-rsa>keys



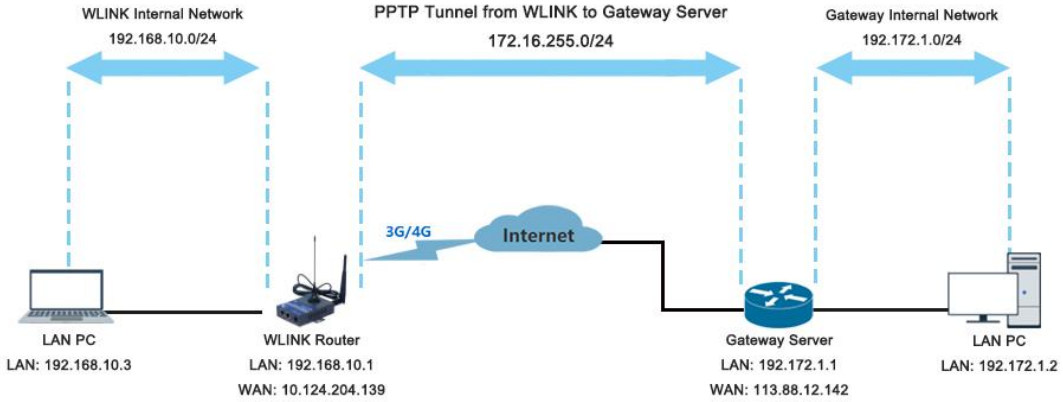
Ping test to your server when the tunnel is established



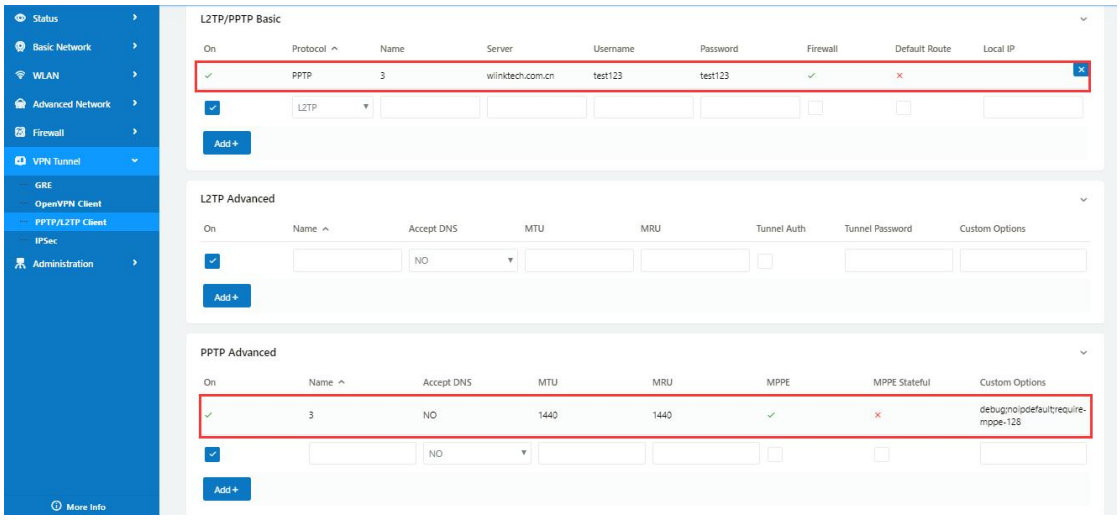
---End

3.9.4 L2TP/PPTP

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



Configured as PPTP

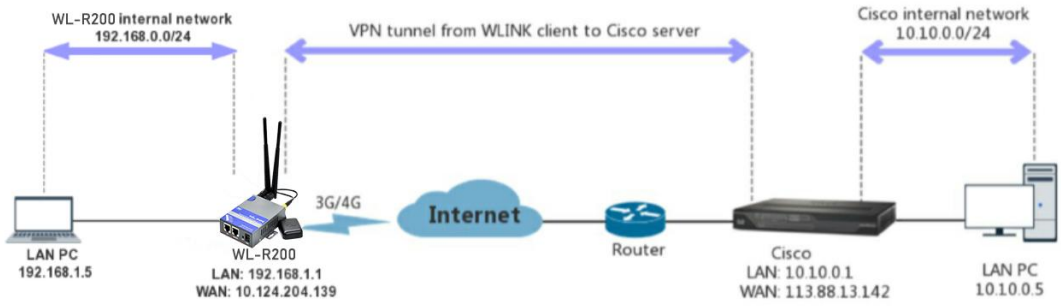


Note: The Custom Options are based on your server

---End

3.9.5 IPSec

IPSec between WLINK Router and Cisco Router



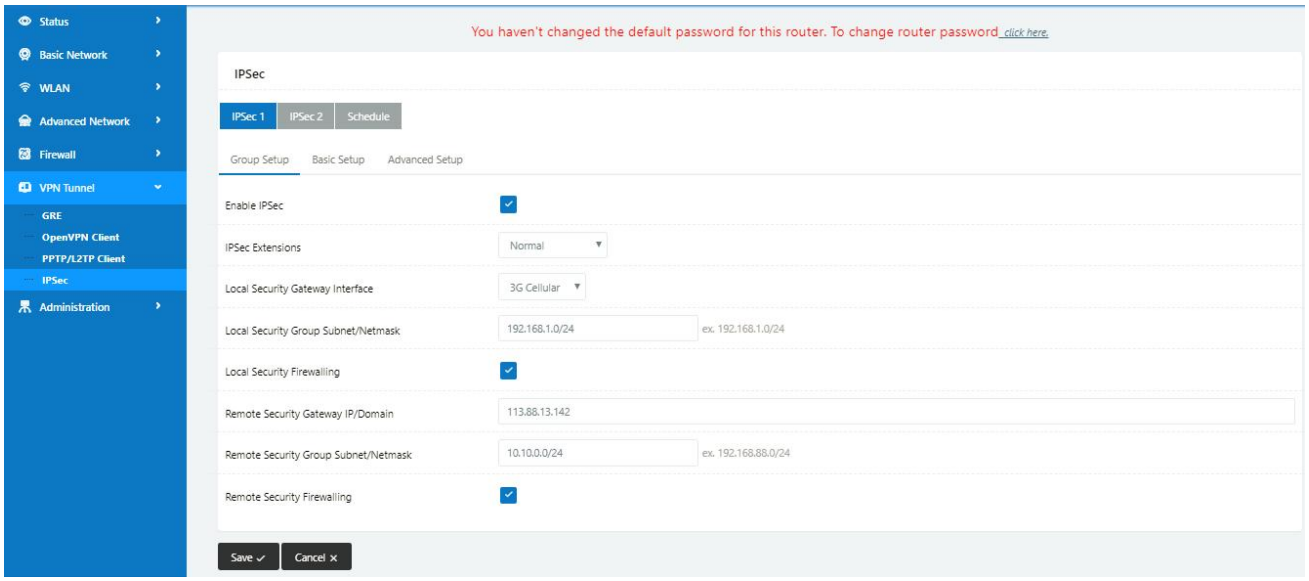
1) Cisco Config (main mode)

```
!
crypto isakmp policy 10
  encr 3des
  hash md5
```

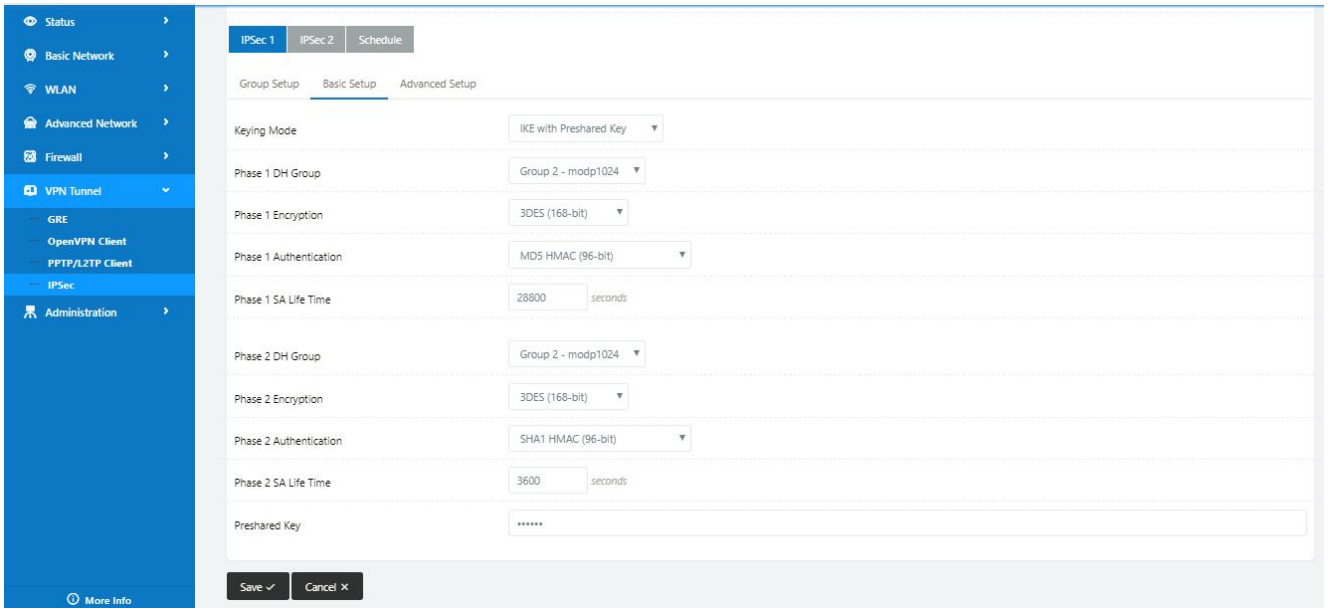
```
 authentication pre-share
 group 2
crypto isakmp key test1234 address 0.0.0.0    0.0.0.0
!
!
crypto ipsec transform-set Tran-set esp-3des esp-sha-hmac
crypto ipsec nat-transparency spi-matching
!
```

2) WLINK Config

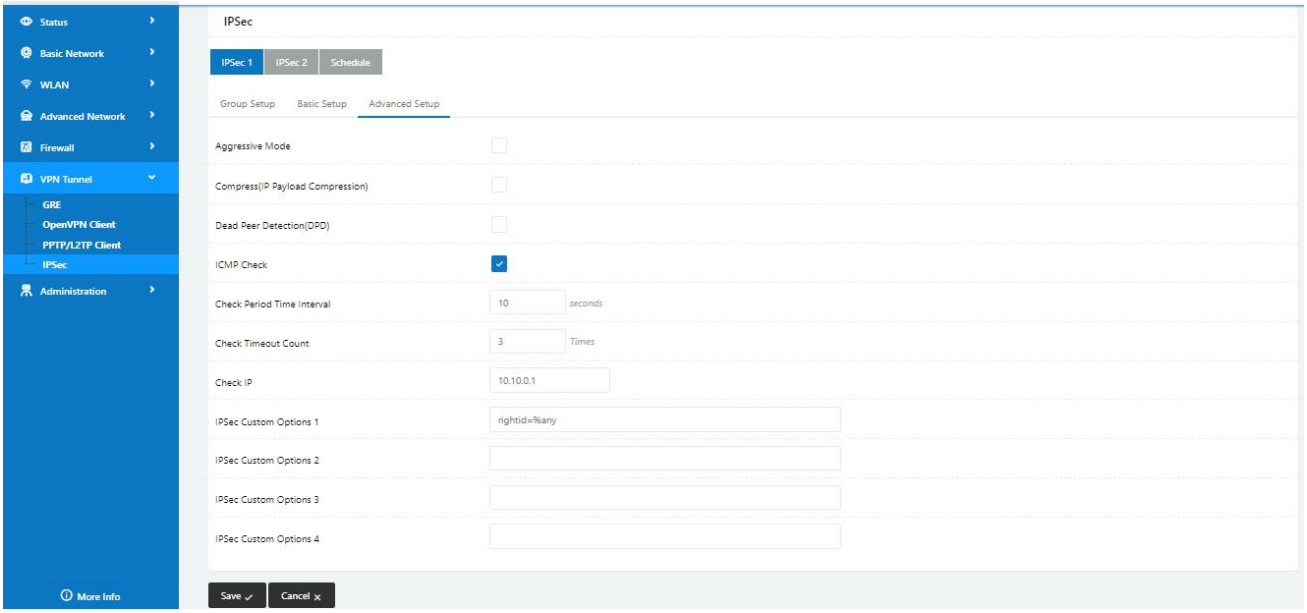
Navigate to **VPN Tunnel > IPSec > Group Setup**

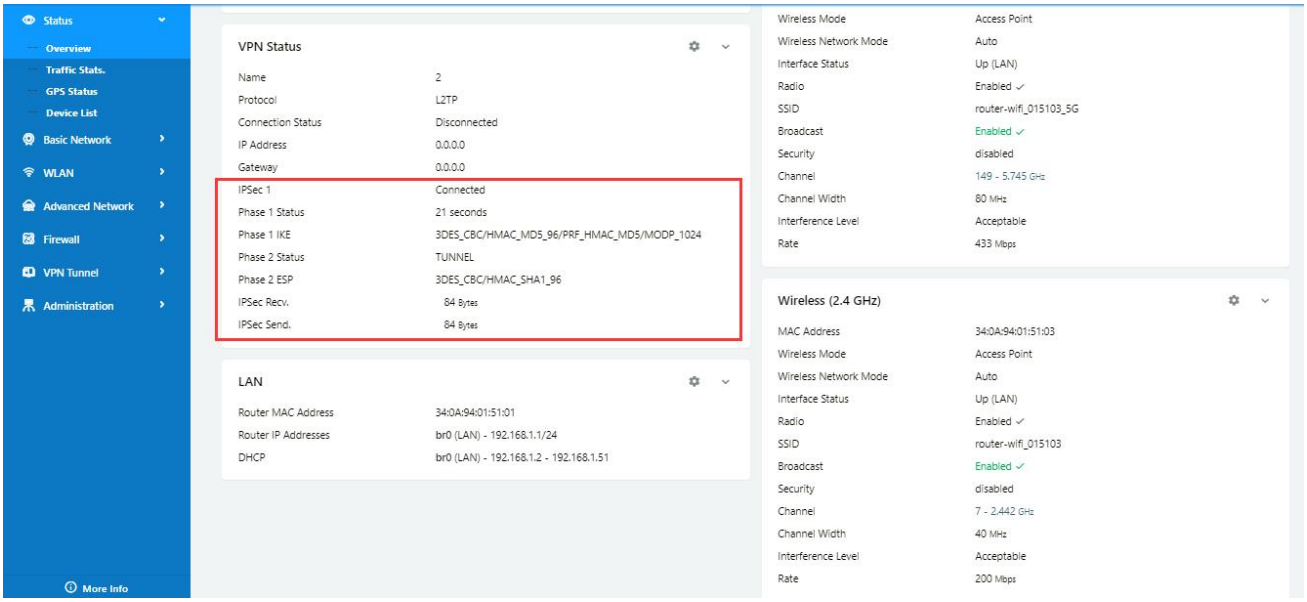


Navigate to **VPN Tunnel > IPSec > Basic Setup**



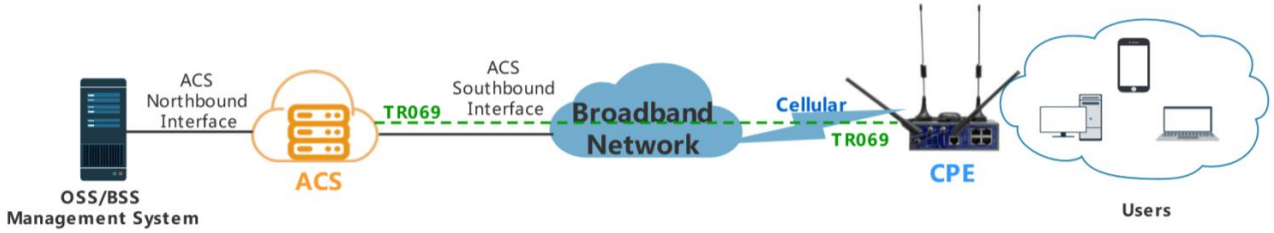
Navigate to **VPN Tunnel > IPSec > Advanced Setup**





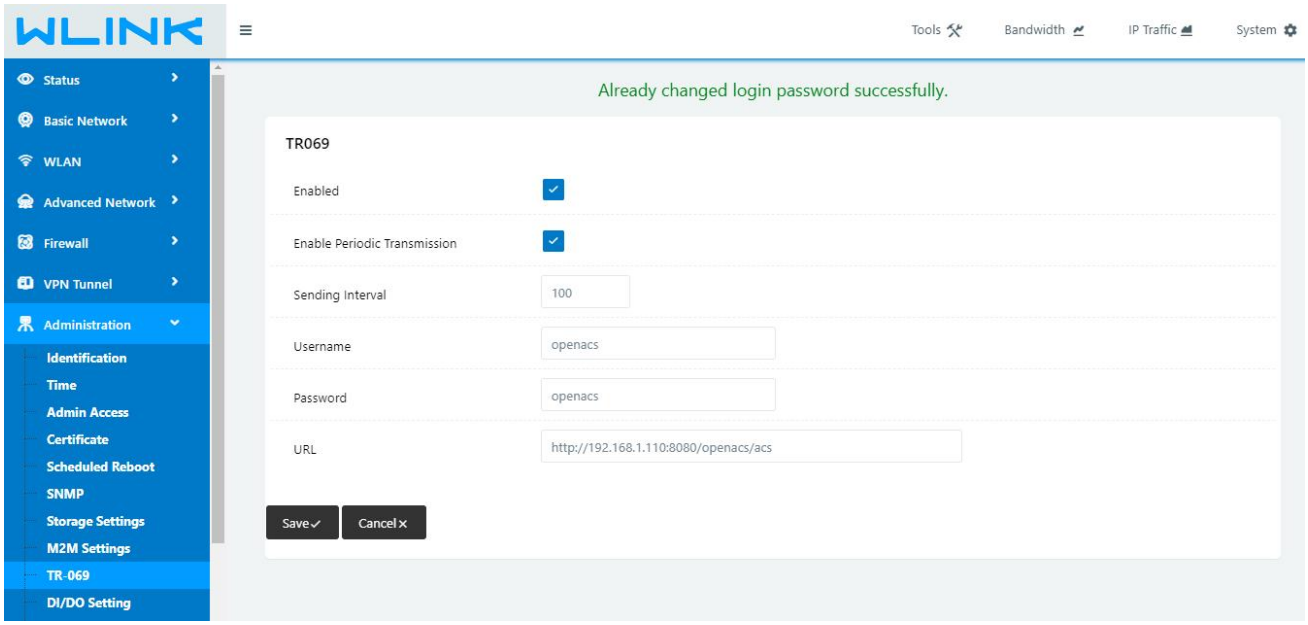
3.10 TR-069

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

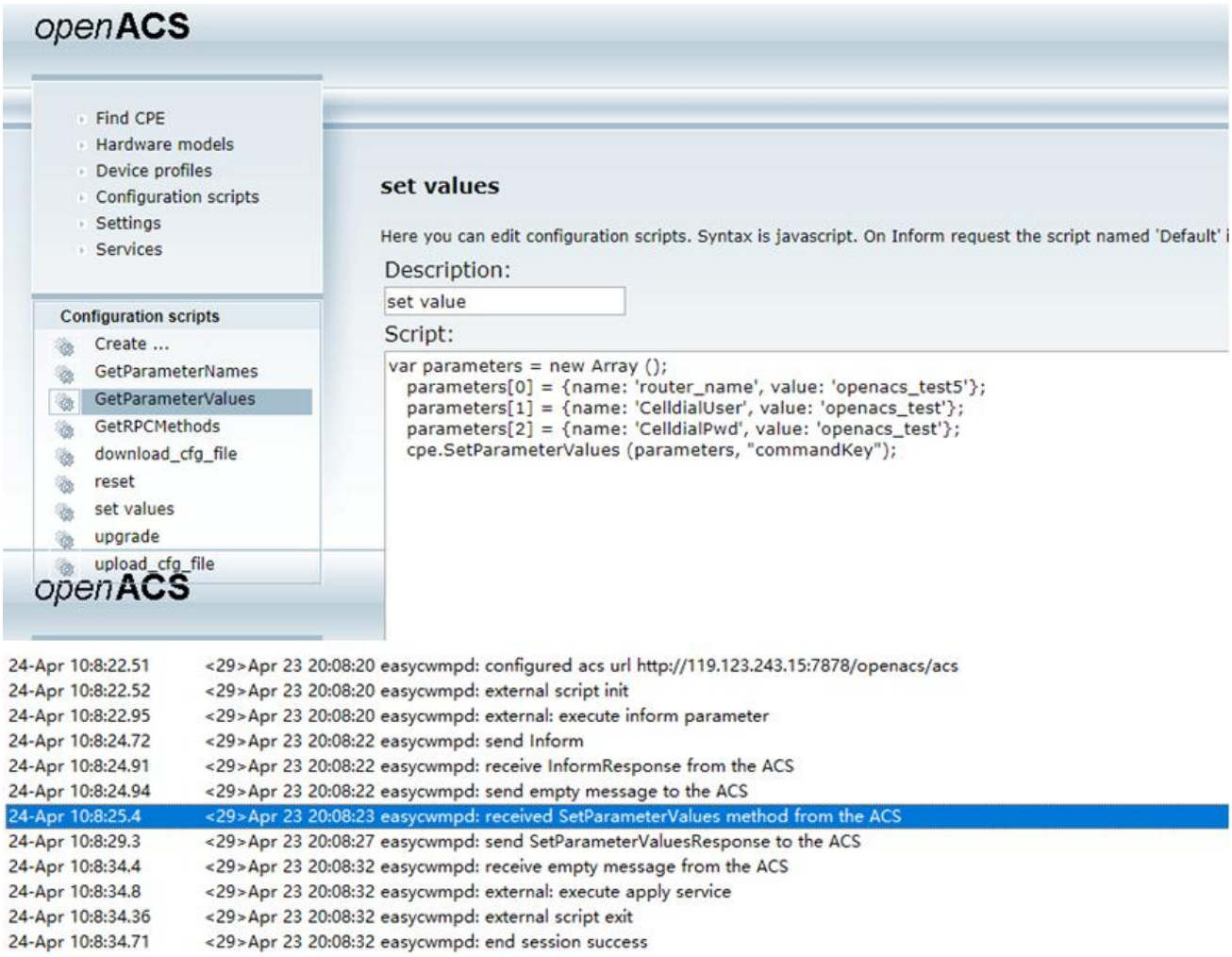


The following features are currently supported in the standard firmware for the WLINK family routers (**Note**: We also support customizing the TR069 and TR098 data-model into the firmware to support more features)

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

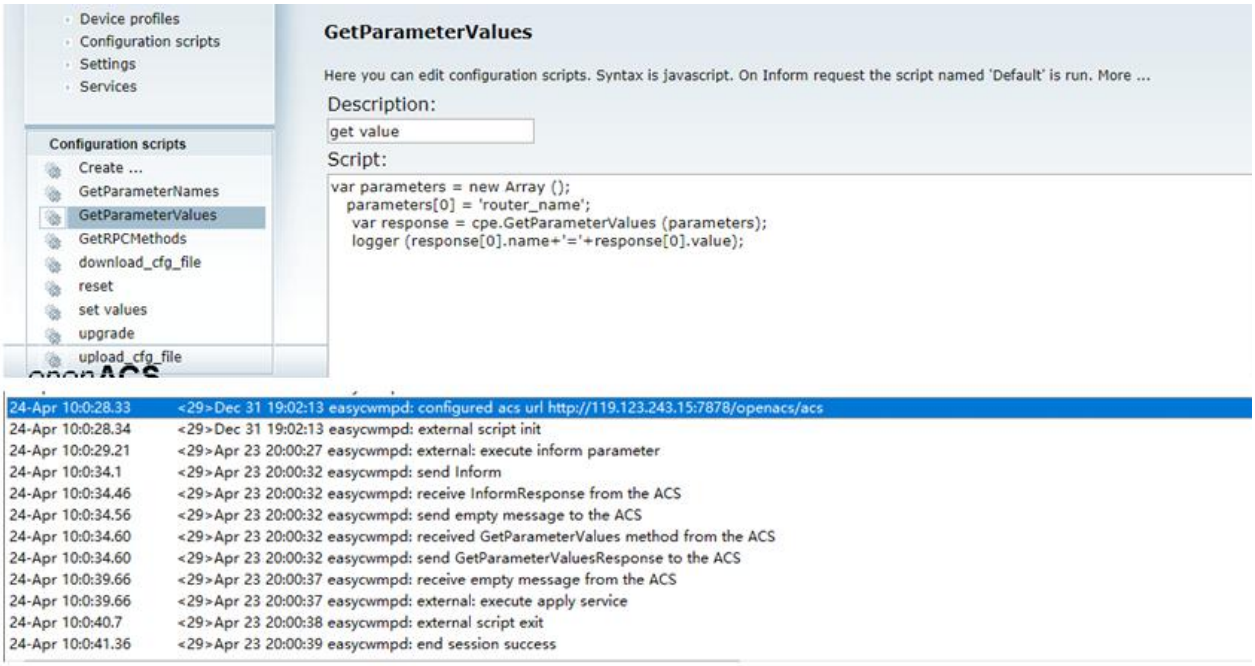


1) SetParameterValues

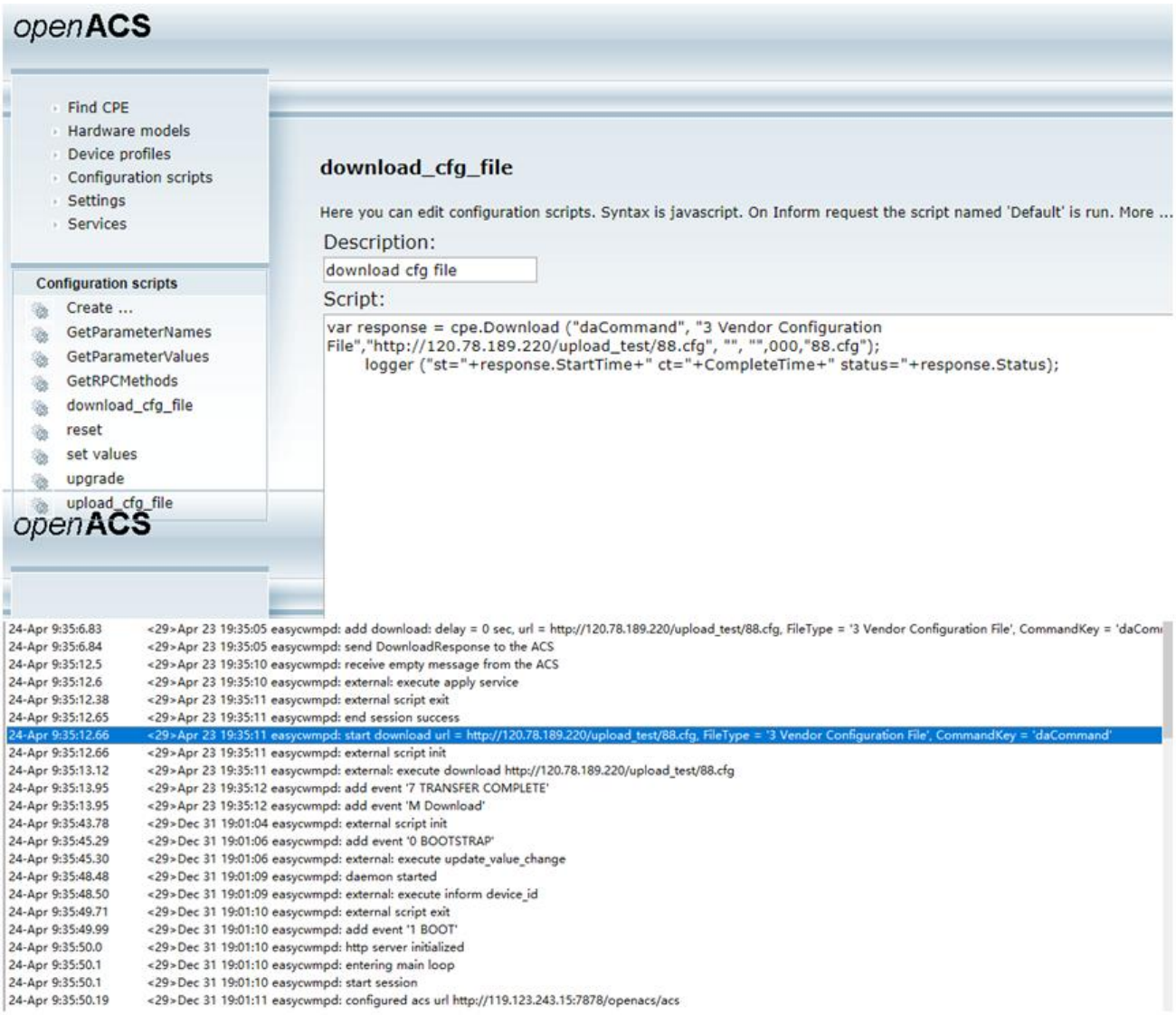



```
24-Apr 10:8:22.51   <29>Apr 23 20:08:20 easycwmpd: configured acs url http://119.123.243.15:7878/openacs/acs
24-Apr 10:8:22.52   <29>Apr 23 20:08:20 easycwmpd: external script init
24-Apr 10:8:22.95   <29>Apr 23 20:08:20 easycwmpd: external: execute inform parameter
24-Apr 10:8:24.72   <29>Apr 23 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
```

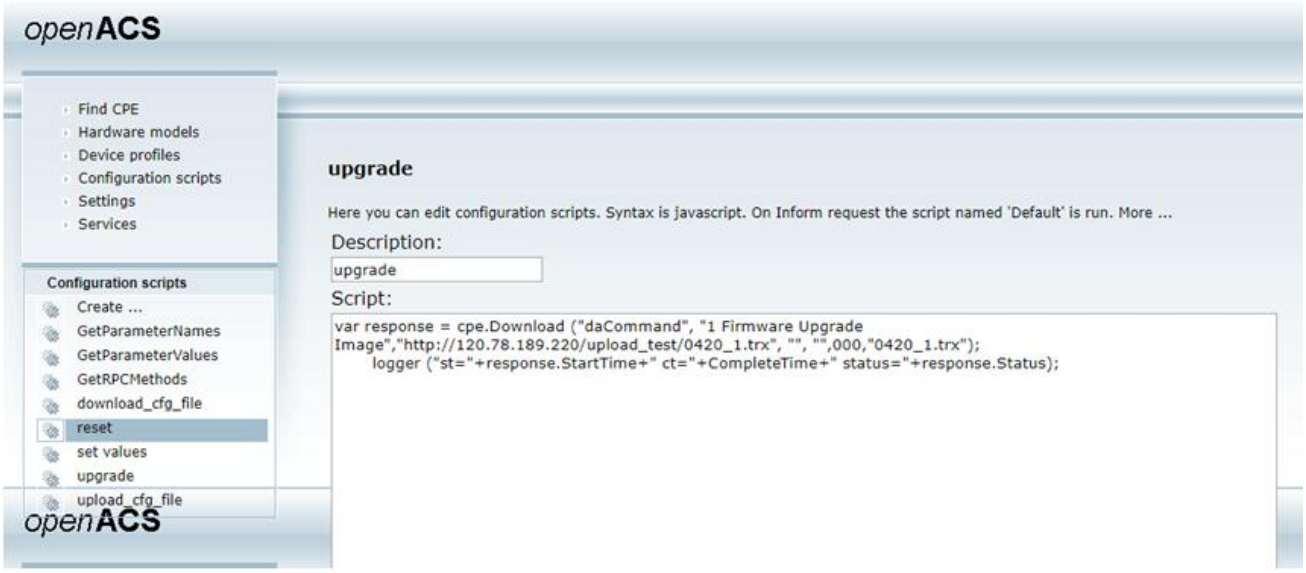
2) GetParameterValues

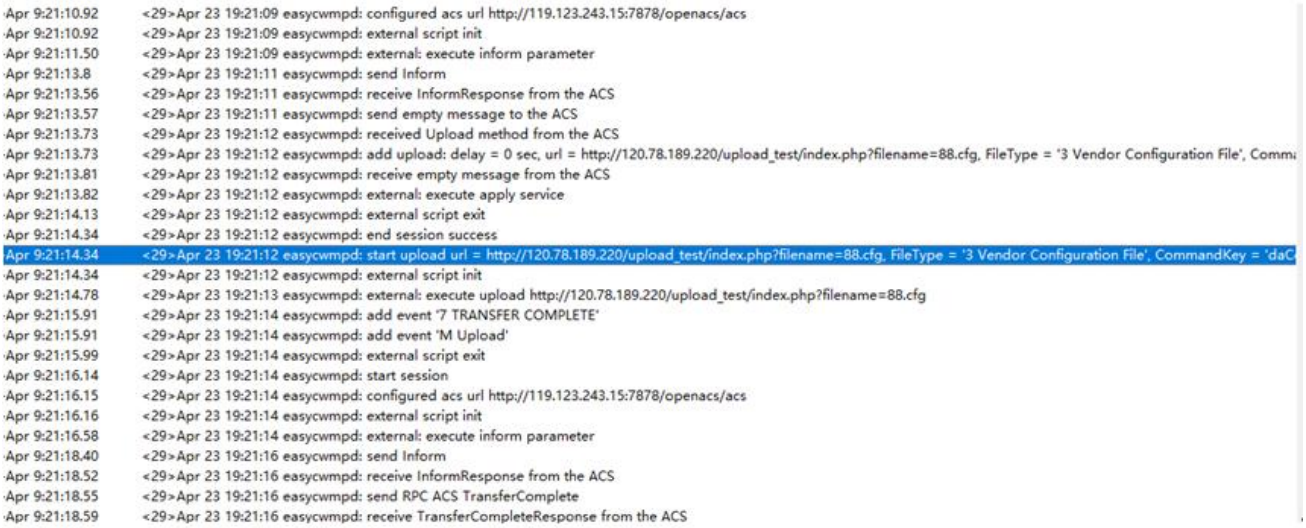


3) Download, the router downloads the configuration parameters


openACS
Find CPE
Hardware models
Device profiles
Configuration scripts
Settings
Services
Configuration scripts
Create ...
GetParameterNames
GetParameterValues
GetRPCMethods
download_cfg_file
reset
set values
upgrade
upload_cfg_file
openACS
download_cfg_file
Here you can edit configuration scripts. Syntax is javascript. On Inform request the script named 'Default' is run. More ...
Description:
download cfg file
Script:
var response = cpe.Download ("daCommand", "3 Vendor Configuration File","http://120.78.189.220/upload_test/88.cfg", "", "",000,"88.cfg");
logger ("st="+response.StartTime+" ct="+CompleteTime+" status="+response.Status);
24-Apr 9:35:6.83 <29>Apr 23 19:35:05 easycwmpd: add download: delay = 0 sec, url = http://120.78.189.220/upload_test/88.cfg, FileType = '3 Vendor Configuration File', CommandKey = 'daCom
24-Apr 9:35:6.84 <29>Apr 23 19:35:05 easycwmpd: send DownloadResponse to the ACS
24-Apr 9:35:12.5 <29>Apr 23 19:35:10 easycwmpd: receive empty message from the ACS
24-Apr 9:35:12.6 <29>Apr 23 19:35:10 easycwmpd: external: execute apply service
24-Apr 9:35:12.38 <29>Apr 23 19:35:11 easycwmpd: external script exit
24-Apr 9:35:12.65 <29>Apr 23 19:35:11 easycwmpd: end session success
24-Apr 9:35:12.66 <29>Apr 23 19:35:11 easycwmpd: start download url = http://120.78.189.220/upload_test/88.cfg, FileType = '3 Vendor Configuration File', CommandKey = 'daCommand'
24-Apr 9:35:12.66 <29>Apr 23 19:35:11 easycwmpd: external script init
24-Apr 9:35:13.12 <29>Apr 23 19:35:11 easycwmpd: external: execute download http://120.78.189.220/upload_test/88.cfg
24-Apr 9:35:13.95 <29>Apr 23 19:35:12 easycwmpd: add event '7 TRANSFER COMPLETE'
24-Apr 9:35:13.95 <29>Apr 23 19:35:12 easycwmpd: add event 'M Download'
24-Apr 9:35:43.78 <29>Dec 31 19:01:04 easycwmpd: external script init
24-Apr 9:35:45.29 <29>Dec 31 19:01:06 easycwmpd: add event '0 BOOTSTRAP'
24-Apr 9:35:45.30 <29>Dec 31 19:01:06 easycwmpd: external: execute update_value_change
24-Apr 9:35:48.48 <29>Dec 31 19:01:09 easycwmpd: daemon started
24-Apr 9:35:48.50 <29>Dec 31 19:01:09 easycwmpd: external: execute inform device_id
24-Apr 9:35:49.71 <29>Dec 31 19:01:10 easycwmpd: external script exit
24-Apr 9:35:49.99 <29>Dec 31 19:01:10 easycwmpd: add event '1 BOOT'
24-Apr 9:35:50.0 <29>Dec 31 19:01:10 easycwmpd: http server initialized
24-Apr 9:35:50.1 <29>Dec 31 19:01:10 easycwmpd: entering main loop
24-Apr 9:35:50.1 <29>Dec 31 19:01:10 easycwmpd: start session
24-Apr 9:35:50.19 <29>Dec 31 19:01:11 easycwmpd: configured acs url http://119.123.243.15:7878/openacs/acs

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





---End