Quick Start Guide

---Apply to WL-ODU310 Outdoor 4G+/4G Router

V1.5
http://www.wlink-tech.com
Jan, 2025

Contents

Hardware Installation

Packing Contents

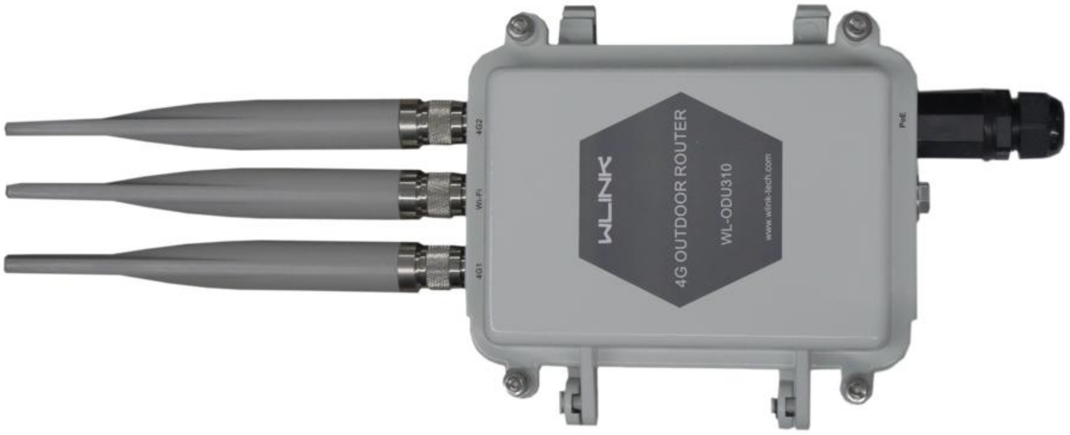
Mount Kits

WL-ODU310

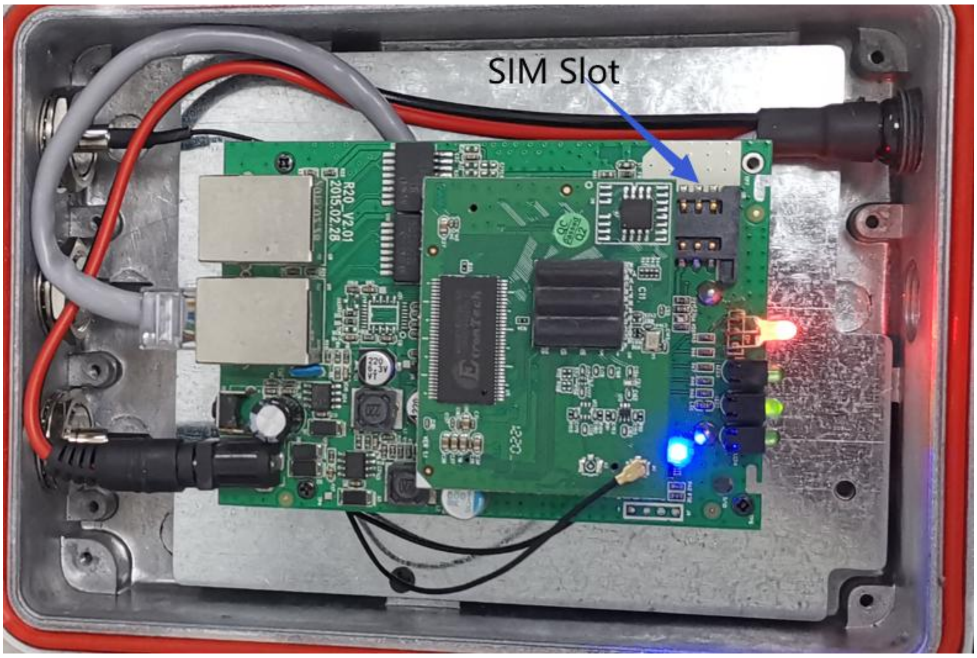
4G/Wi-Fi Antennas

PoE Power Adapter

Antenna Installation

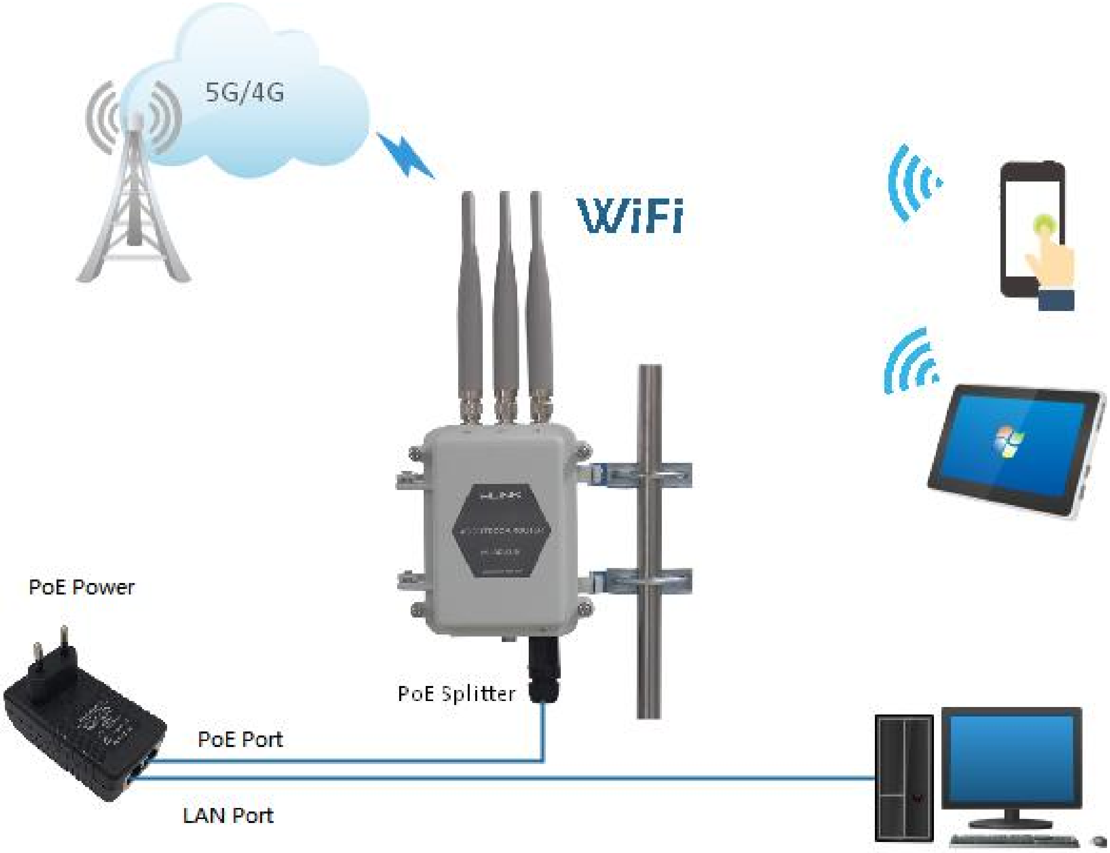


SIM Installation

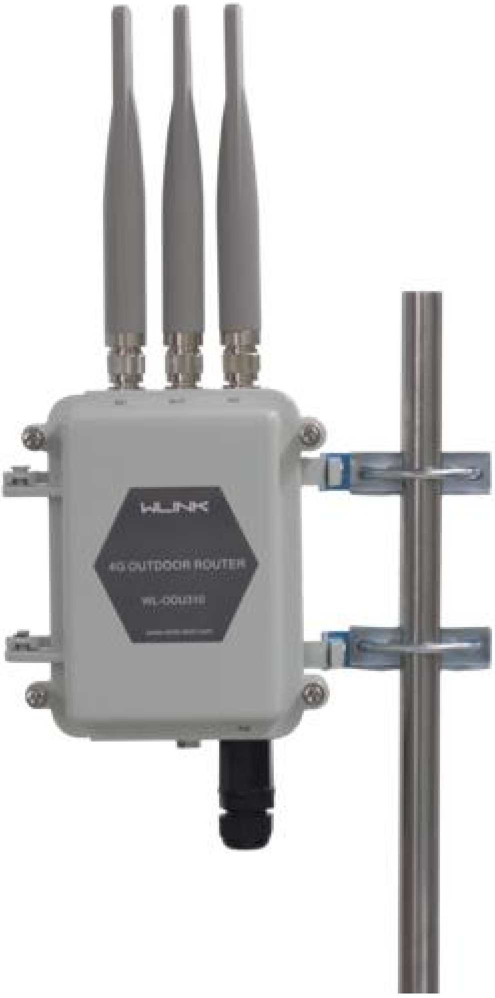


Power on Router

Connect PoE(passive) port via RJ45 Cable between WL-ODU310 and Wlink power adapter. Connect LAN port of Power adapter to PC to configure the router.



Mount Kits Installation



LED Status Indication

silk-screen	Indicator		Note
NET	Color	Green	Good Signal
		Red	Poor Signal
	Status	Quick Blinking (0.5s)	Offline
		Slow Blinking (1.5s)	3G online
		Solid light	4G online

Configuration

Login

To access and configure certain features of the WL-ODU310, one needs to log in to the WL-ODU310. Connect one Ethernet cable to PoE interface of device and PoE adapter, and connect other Ethernet cable between LAN of PoE adapter and PC.

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.

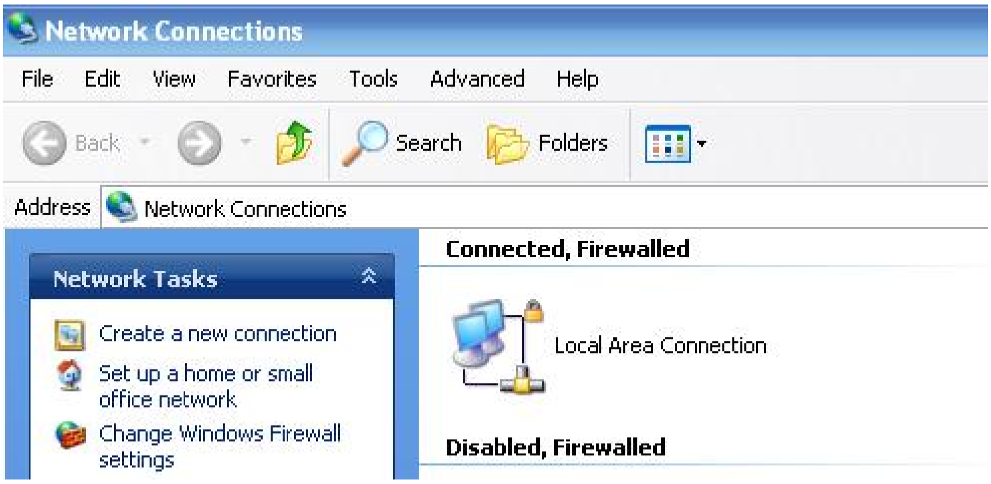
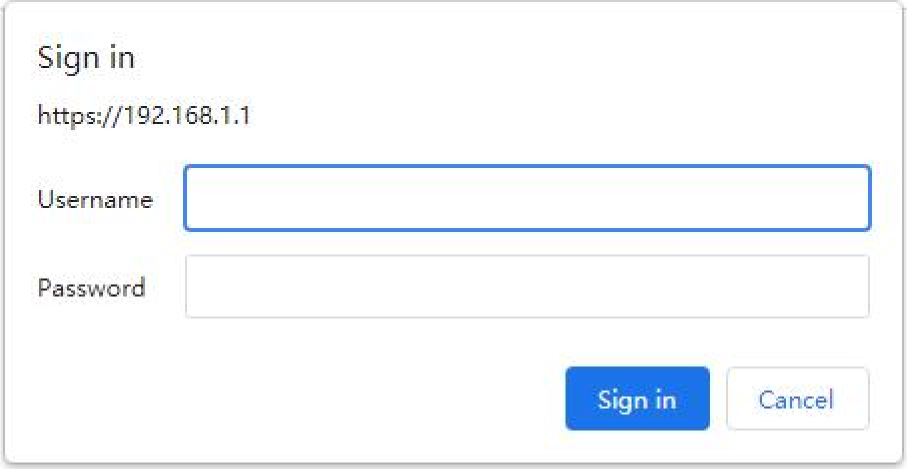


Figure 2-1 Network Connection

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 .Enter the default IP Address as http://192.168.1.1 the login page will open as shown in the figure below.



Sign in

https://192.168.1.1

Username

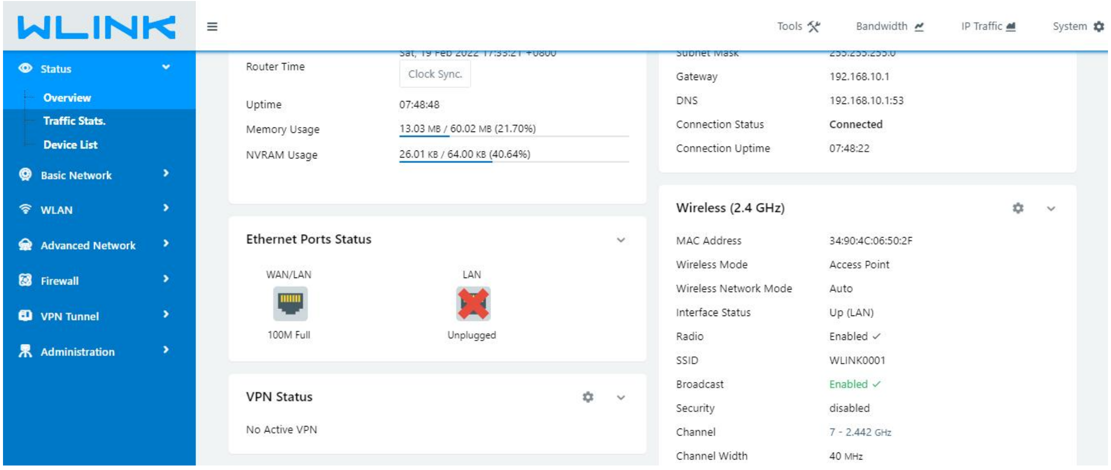
Password

User name: admin

Password: admin

Overview

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



Router Time Sat, 19 Feb 2022 17:33:21 +0800

Uptime 07:48:48

Memory Usage 13.03 MB / 60.02 MB (21.70%)

NVRAM Usage 26.01 KB / 64.00 KB (40.64%)

Ethernet Ports Status

WAN/LAN 100M Full

LAN Unplugged

VPN Status

No Active VPN

Subnet Mask 255.255.255.0

Gateway 192.168.10.1

DNS 192.168.10.1:53

Connection Status **Connected**

Connection Uptime 07:48:22

Wireless (2.4 GHz)

MAC Address 34:90:4C:06:50:2F

Wireless Mode Access Point

Wireless Network Mode Auto

Interface Status Up (LAN)

Radio Enabled ✓

SSID WLINK0001

Broadcast Enabled ✓

Security disabled

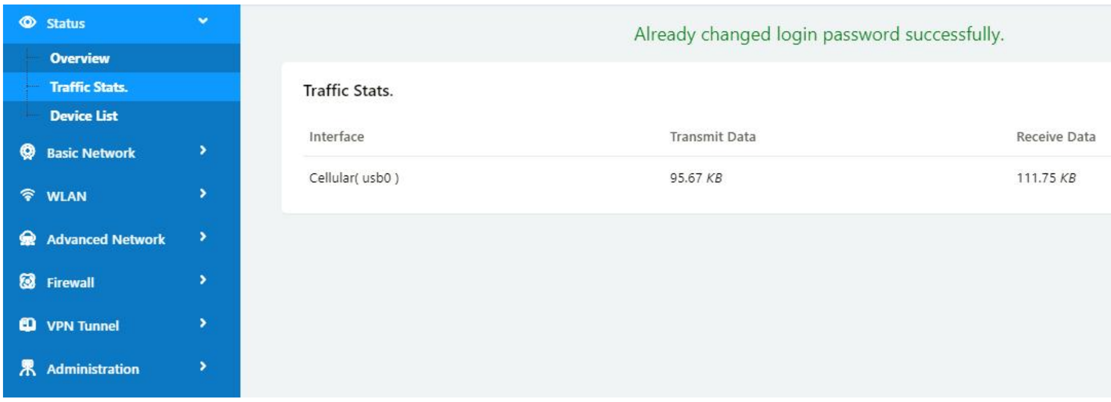
Channel 7 - 2.442 GHz

Channel Width 40 MHz

Figure 2-2 Router Status GUI

Traffic Stats.

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



Already changed login password successfully.

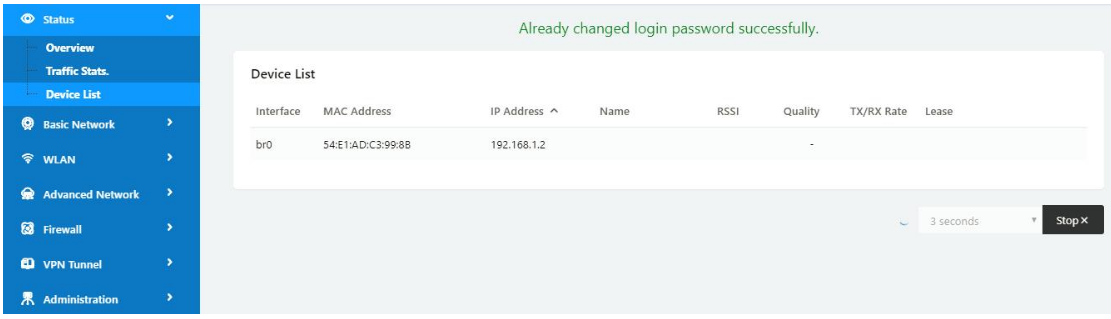
Traffic Stats.

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

Figure 2-3 Traffic Stats. GUI

Device List

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



Already changed login password successfully.

Device List

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

Figure 2-4 Device List GUI

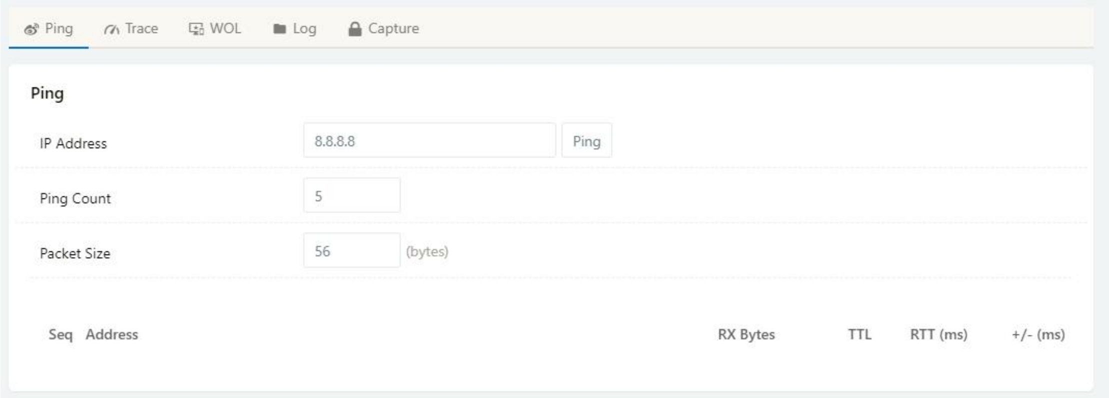
Tool Column

Tools
Bandwidth
IP Traffic
System

Figure 2-5 Tool Column GUI

Ping

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



Ping

IP Address 8.8.8.8 Ping

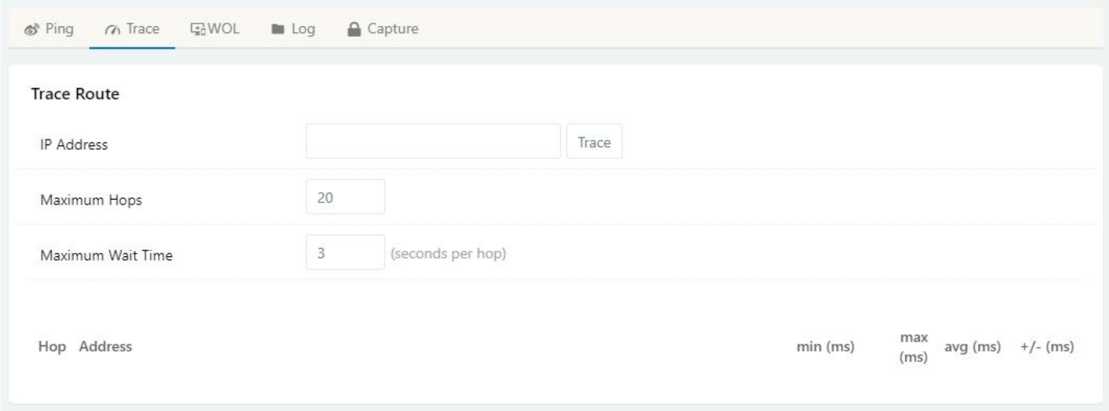
Ping Count 5

Packet Size 56 (bytes)

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

Trace

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



Trace Route

IP Address Trace

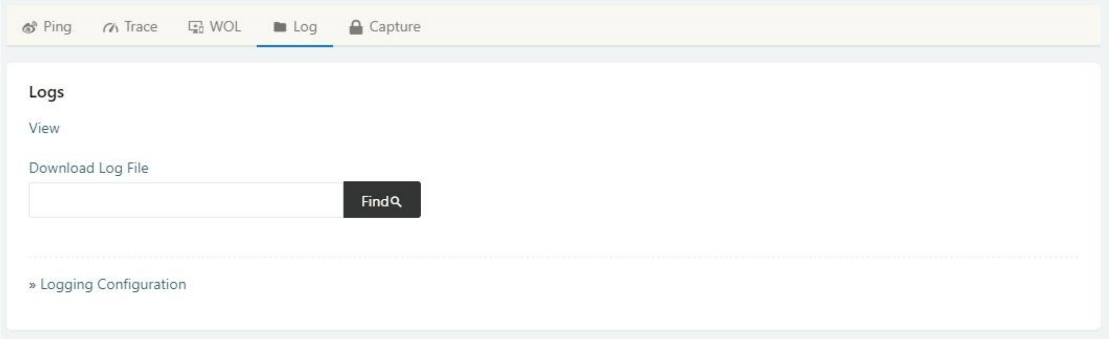
Maximum Hops 20

Maximum Wait Time 3 (seconds per hop)

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

Log

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



Logs

View

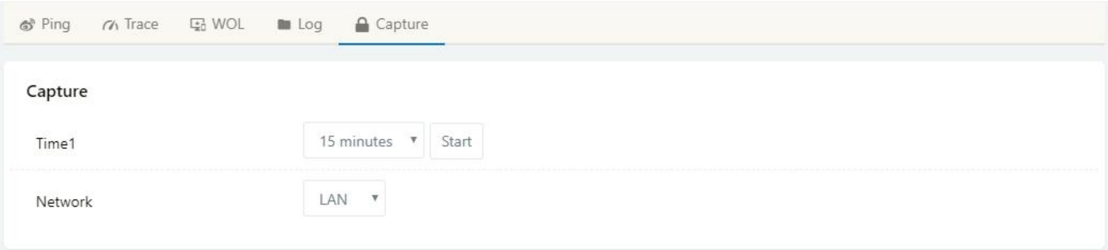
Download Log File

Find

» Logging Configuration

Capture

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



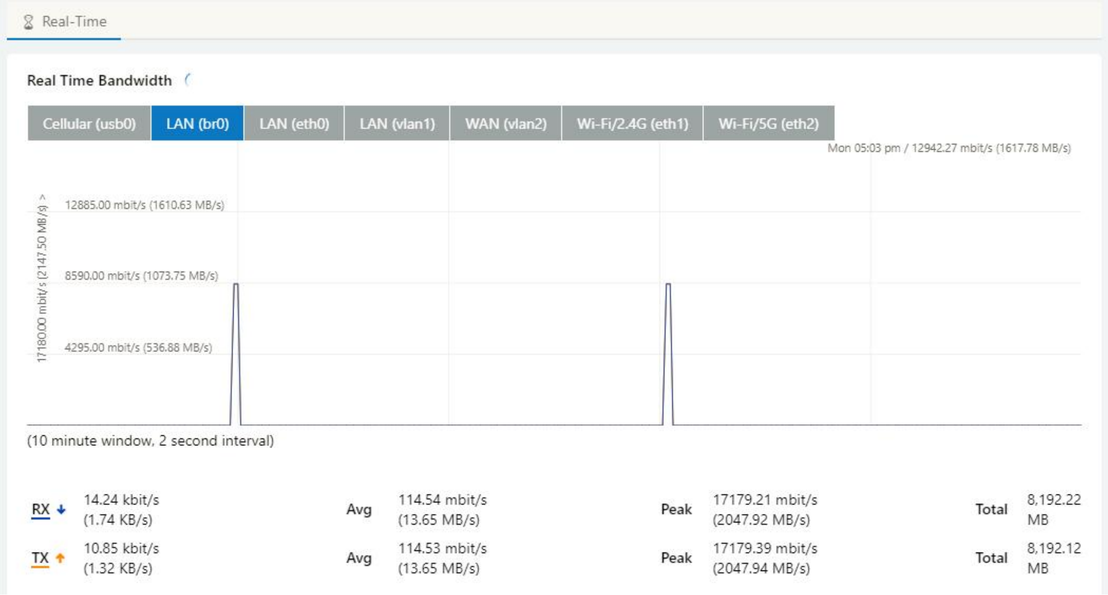
Capture

Time1 15 minutes ▾ Start

Network LAN ▾

Bandwidth

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

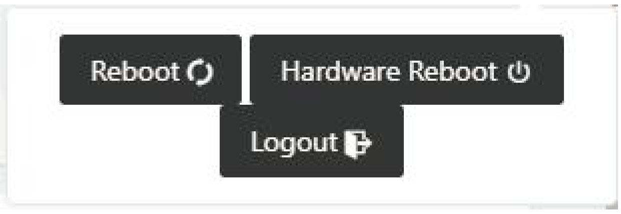

Real-Time
Real Time Bandwidth
Cellular (usb0)
LAN (br0)
LAN (eth0)
LAN (vlan1)
WAN (vlan2)
Wi-Fi/2.4G (eth1)
Wi-Fi/5G (eth2)
Mon 05:03 pm / 12942.27 mbit/s (1617.78 MB/s)
17180.00 mbit/s (2147.50 MB/s) ^
12885.00 mbit/s (1610.63 MB/s)
8590.00 mbit/s (1073.75 MB/s)
4295.00 mbit/s (536.88 MB/s)

(10 minute window, 2 second interval)

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

System

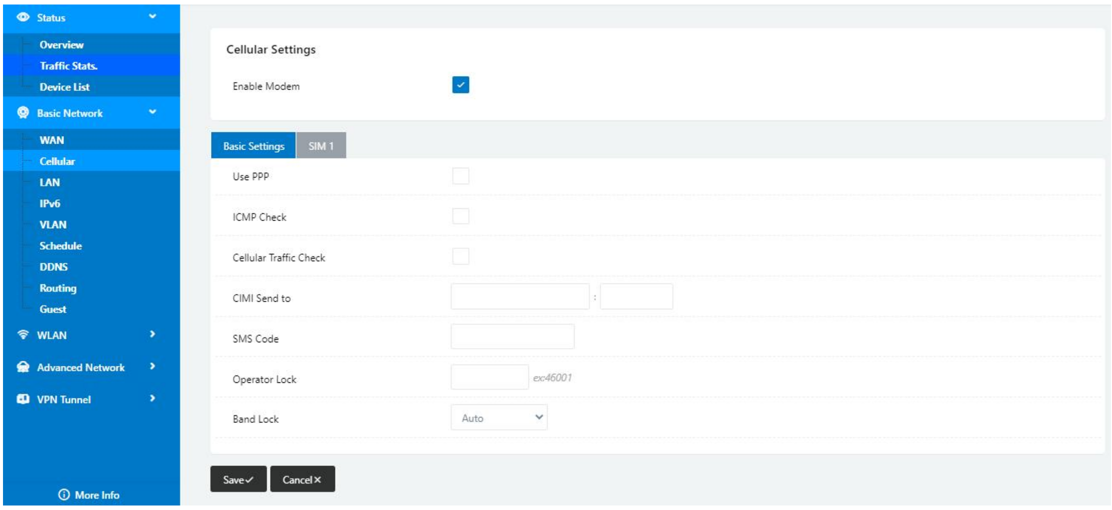
Click system to choose software reboot, hardware reboot and logout GUI.



Basic Network

Cellular Setting

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



Cellular Settings

Enable Modem ☑

Use PPP □

ICMP Check □

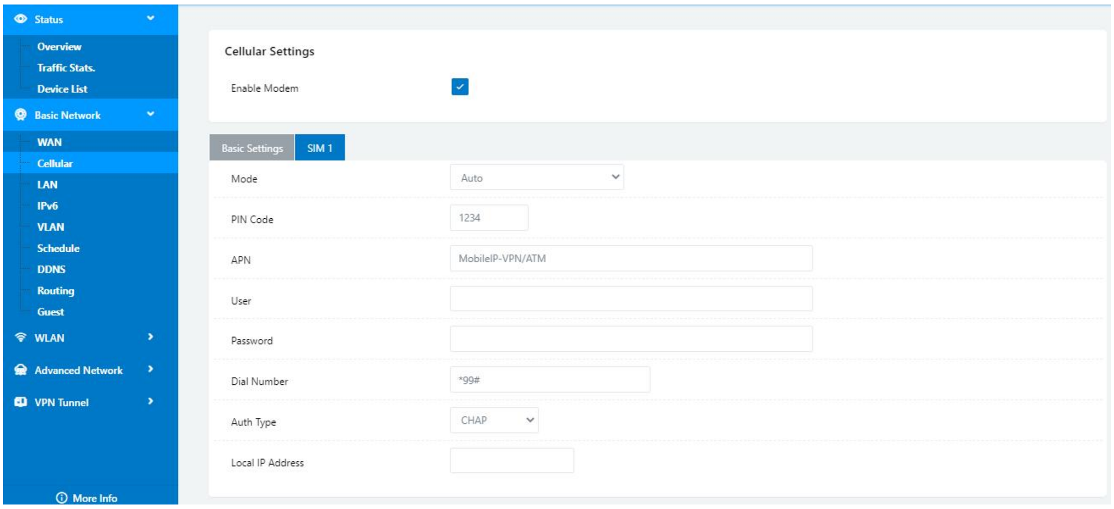
Cellular Traffic Check □

CIMI Send to :

SMS Code

Operator Lock ex46001

Band Lock Auto



Cellular Settings

Enable Modem ☑

Mode Auto

PIN Code 1234

APN MobileIP-VPN/ATM

User

Password

Dial Number *99#

Auth Type CHAP

Local IP Address

Table 2-1 Cellular Setting Instruction

Parameter	Instruction
Enable Modem	Enable/Disable 4G mode.
Use PPP	ECM dialup as default. PPP optional.
ICMP check	If enable ICMP check and setup a reachable IP address as destination IP, the router will reconnect/reboot once ICMP check failed.

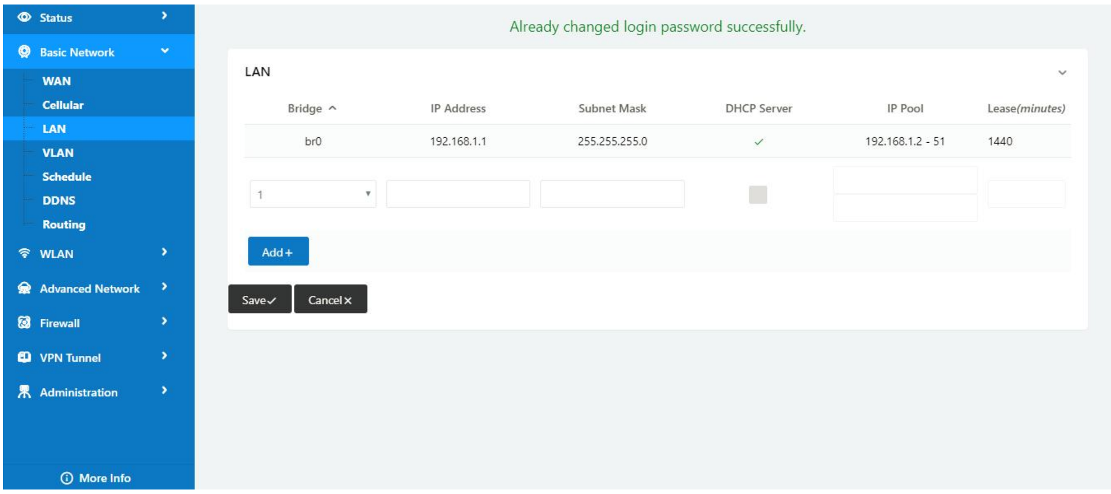
Parameter	Instruction
Cellular Traffic Check	The router will reconnect/reboot once there's no Rx/Tx data.
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock a specified operator for the router by MCC/MNC code.
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.

Step 2 After Setting, please click "save" icon.

----End

LAN Setting

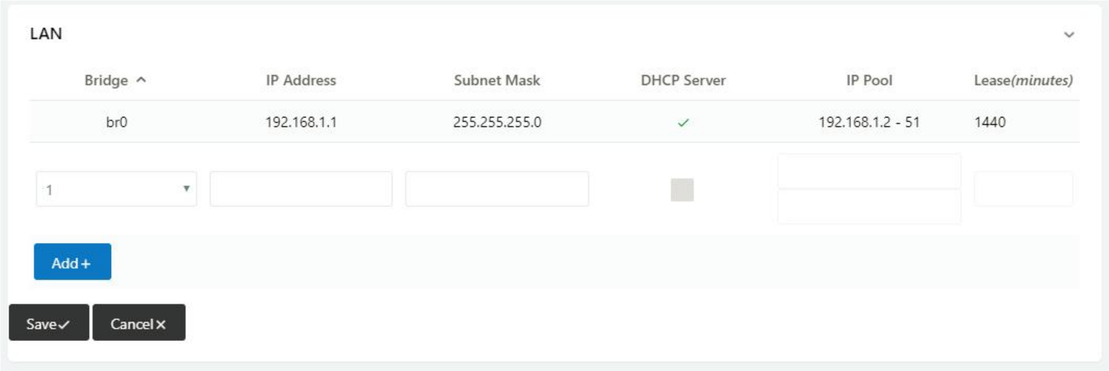
Step 1 Basic Network>LAN to enter below interface



Already changed login password successfully.

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(*minutes*)
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440
1			□		



LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(*minutes*)
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440

Table 2-2 LAN Setting Instruction

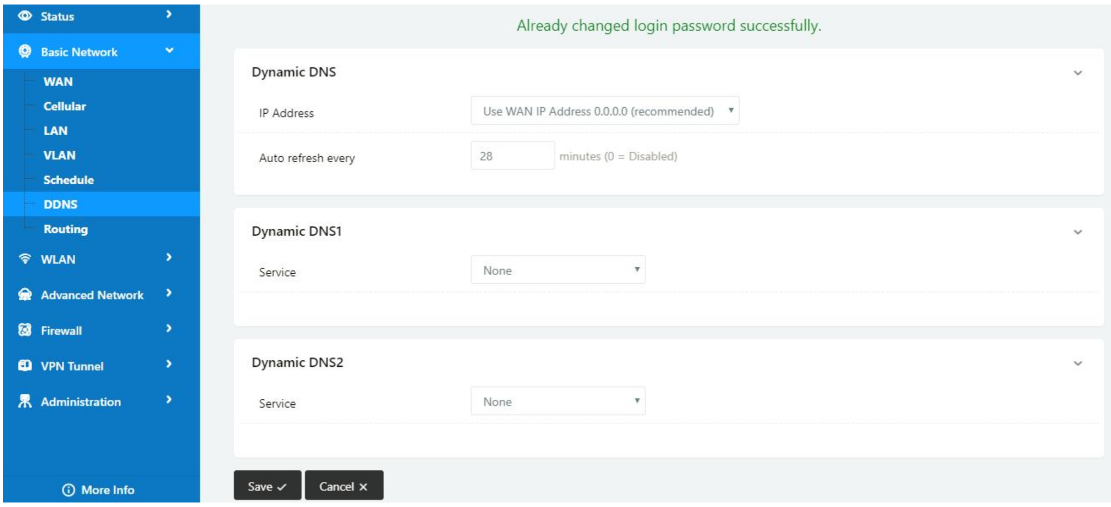
Parameter	Instruction
Bridge	Supports 4 LAN IP address for br0 to br3 interface. If need to support VLAN, please go to VLAN GUI.
Router IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service, after enable, 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

Dynamic DNS Setting

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



Already changed login password successfully.

Dynamic DNS

IP Address: Use WAN IP Address 0.0.0.0 (recommended)

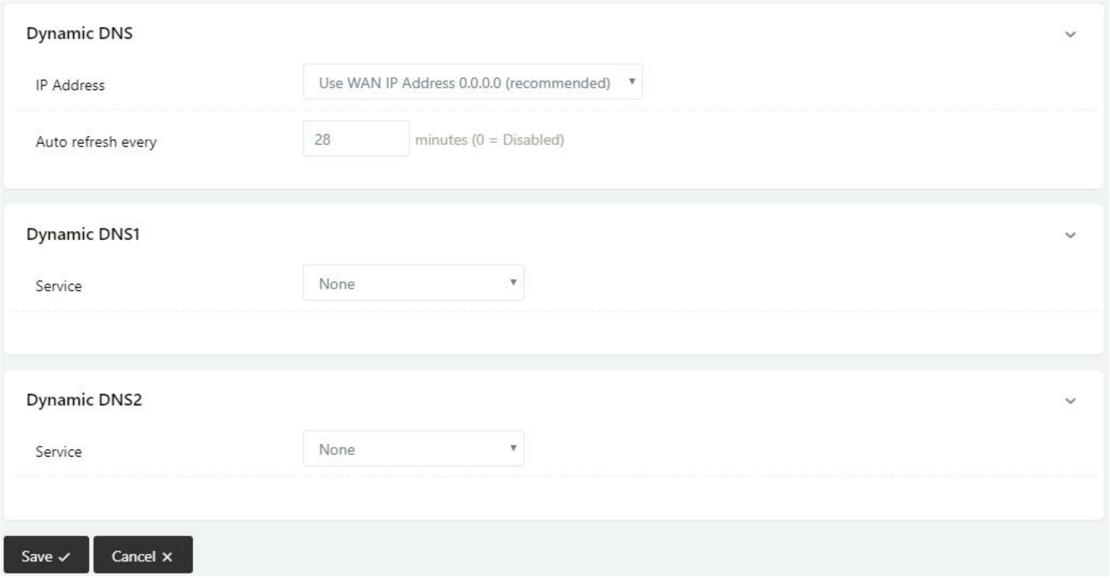
Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None



Dynamic DNS

IP Address: Use WAN IP Address 0.0.0.0 (recommended)

Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None

Table 2-3 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.

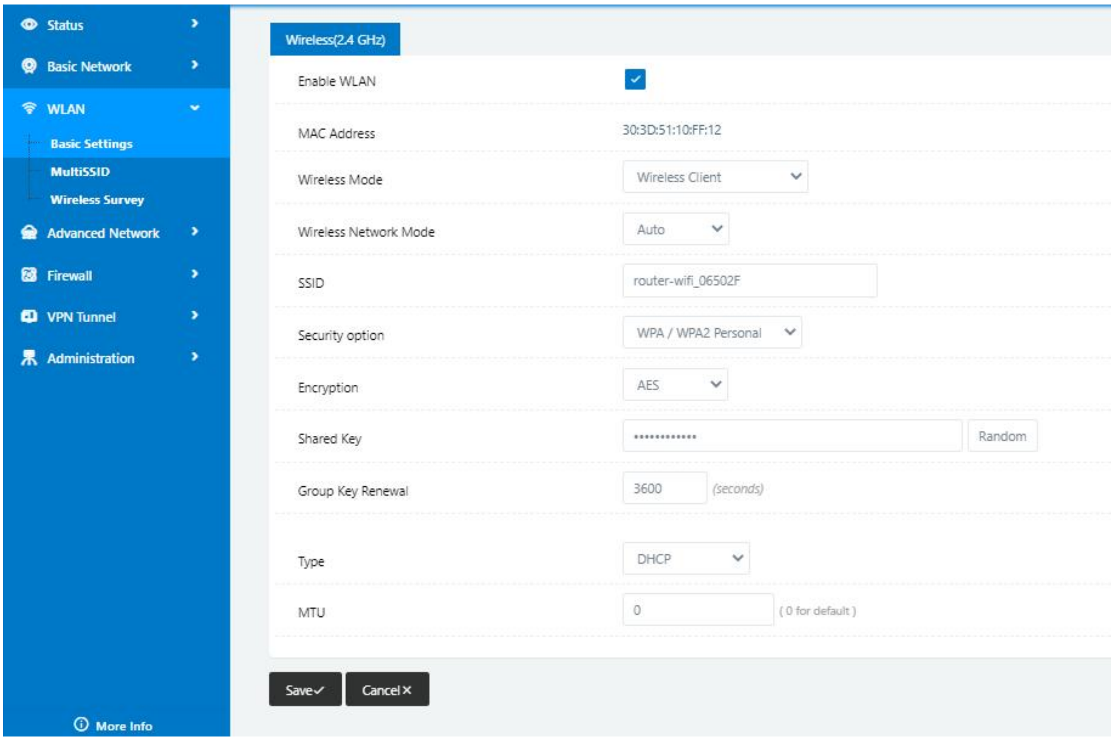
----End

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.

Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter



Enable WLAN	☑
MAC Address	30:3D:51:10:FF:12
Wireless Mode	Wireless Client
Wireless Network Mode	Auto
SSID	router-wifi_06502F
Security option	WPA / WPA2 Personal
Encryption	AES
Shared Key	••••••••••••
Group Key Renewal	3600 (seconds)
Type	DHCP
MTU	0 (0 for default)

Table 2-4 Basic of WLAN Setting Instruction

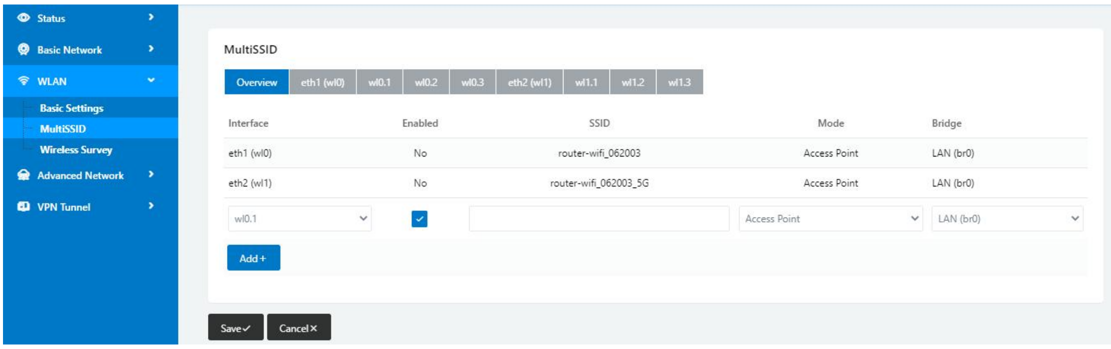
Parameter	Instruction
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP mode.
Wireless Network protocol	Support Auto/b/g/n optional for 2.4G.
SSID	The default is router, can be modified as per application.
Channel	The channel of wireless network, suggest keep the default
Channel 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

MultiSSID

Step 4 WLAN->MultiSSID Setting to configure relative parameter



MultiSSID

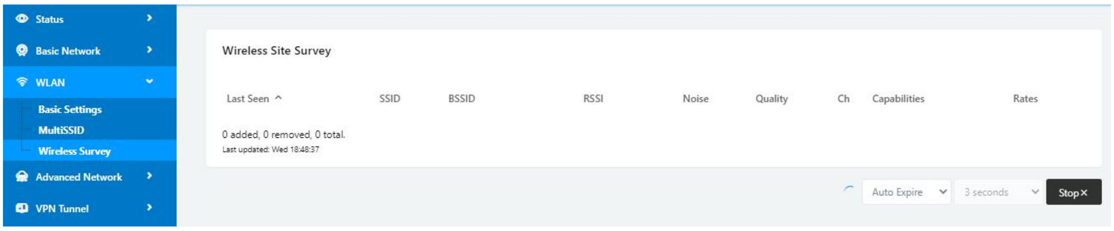
Interface	Enabled	SSID	Mode	Bridge
eth1 (wl0)	No	router-wifi_062003	Access Point	LAN (br0)
eth2 (wl1)	No	router-wifi_062003_5G	Access Point	LAN (br0)
wl0.1	☑		Access Point	LAN (br0)

Step 1 Please click “Save” to finish.

----End

Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.



Wireless Site Survey

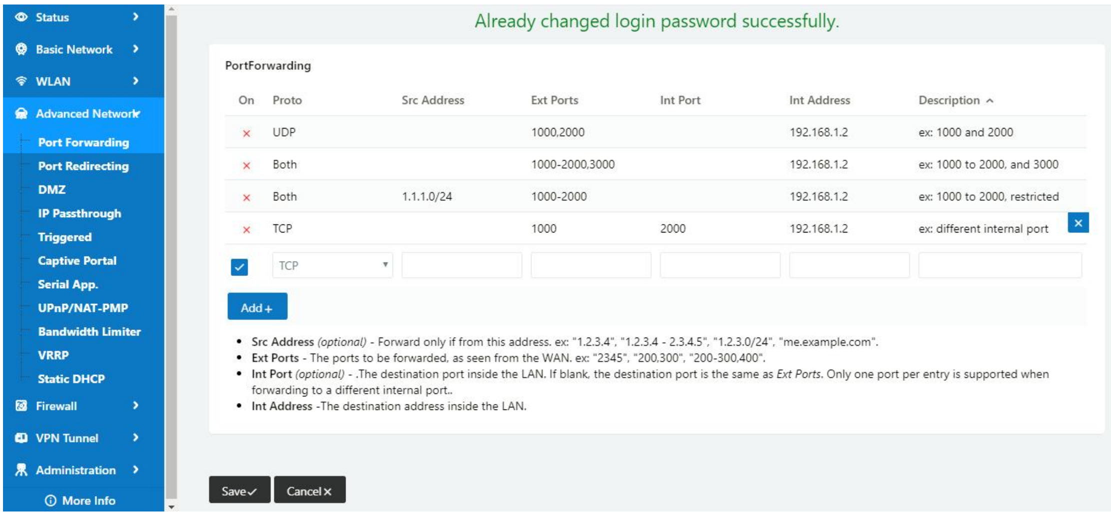
Last Seen ^	SSID	BSSID	RSSI	Noise	Quality	Ch	Capabilities	Rates

0 added, 0 removed, 0 total.
Last updated: Wed 18:48:37

Advanced Network Setting

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.



Already changed login password successfully.

PortForwarding

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

- **Src Address** *(optional)* - Forward only if from this address. ex: "1.2.3.4", "1.2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.example.com".
- **Ext Ports** - The ports to be forwarded, as seen from the WAN. ex: "2345", "200,300", "200-300,400".
- **Int Port** *(optional)* - .The destination port inside the LAN. If blank, the destination port is the same as *Ext Ports*. Only one port per entry is supported when forwarding to a different internal port..
- **Int Address** -The destination address inside the LAN.

Table 2-5 Port Forwarding Instruction

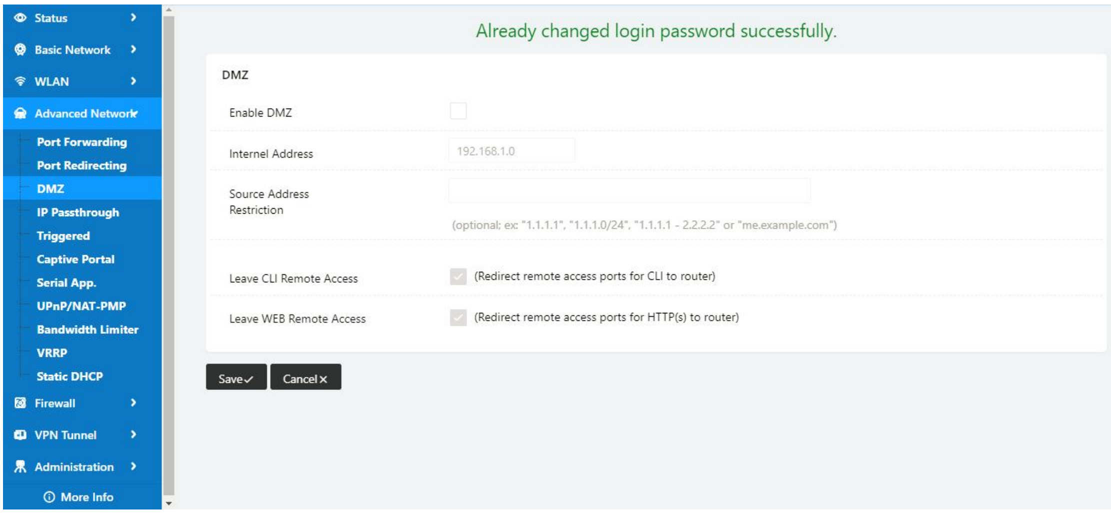
Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Src. Address	Source IP address. Forward only if from this address.
Ext. Ports	External ports. The ports to be forwarded, as seen from the WAN.
Int. Port	Internal port. The destination port inside the LAN. If blank, the destination port is the same as Ext Ports. Only one port per entry is supported when forwarding to a different internal port.
Int. Address	Internal Address. The destination address inside the LAN.
Description	Remark the rule

Step 2 Please click ”save” to finish

----End

DMZ Setting

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



Already changed login password successfully.

DMZ

Enable DMZ □

Internel Address 192.168.1.0

Source Address Restriction

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

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

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

Table 2-6 DMZ Instruction

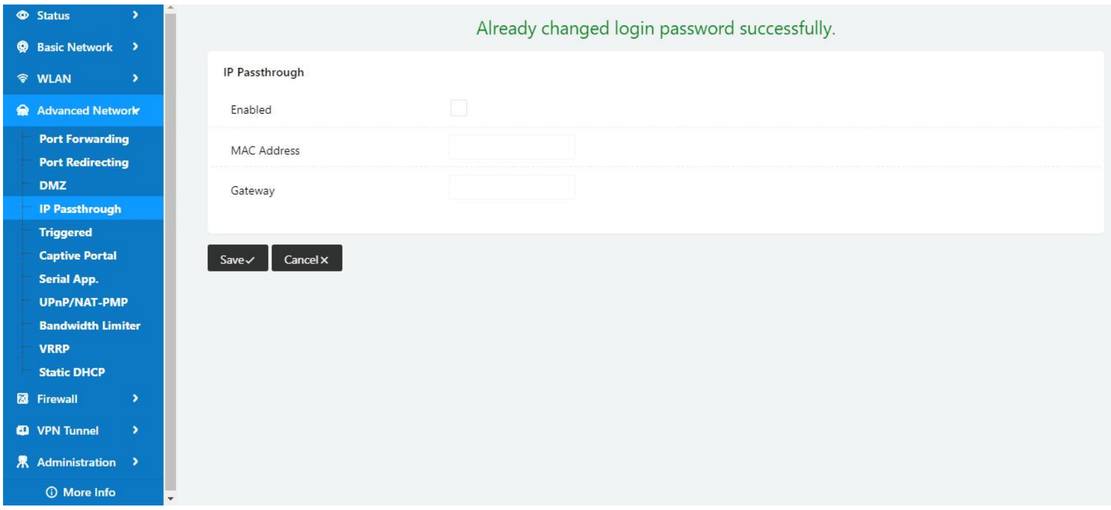
parameter	Instruction
Destination Address	The destination address inside the LAN.
Source Address Restriction	If no IP address inside, it will allow all IP address to access. If define IP address, it will just allow the defined IP address to access.
Leave Remote Access	

Step 2 Please click "save" to finish

----End

IP Passthrough Setting

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



Already changed login password successfully.

IP Passthrough

Enabled □

MAC Address

Gateway

Table 2-7 IP Passthrough Instruction

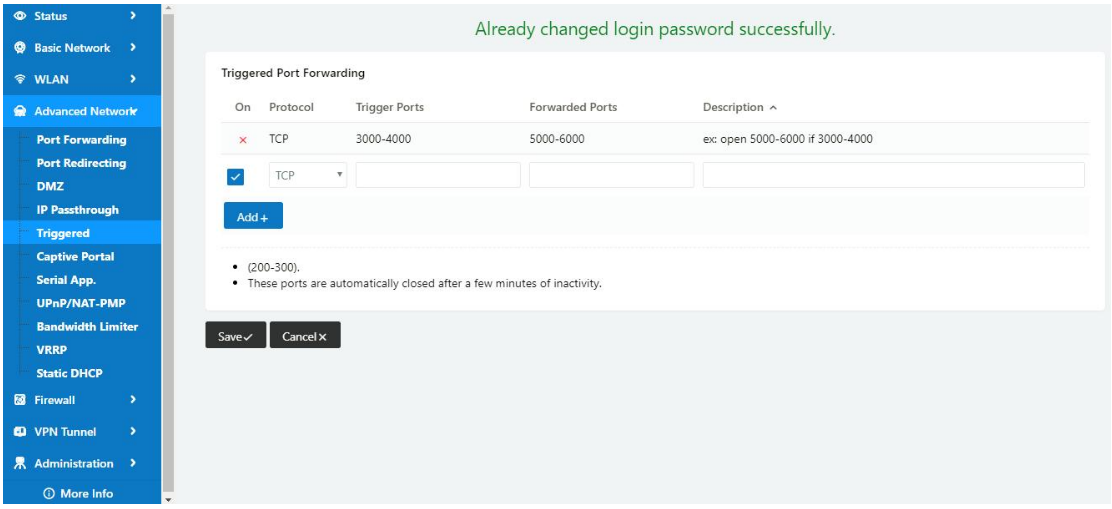
parameter	Instruction
Enable	Enable IP Passthrough
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.
Gateway	If WL-G200 connect to multiple device, input other device gateway. The device might access to router GUI.

Step 2 Please click "save" to finish

----End

Triggered Setting

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



Already changed login password successfully.

Triggered Port Forwarding

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

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

Table 2-8 Triggered Instruction

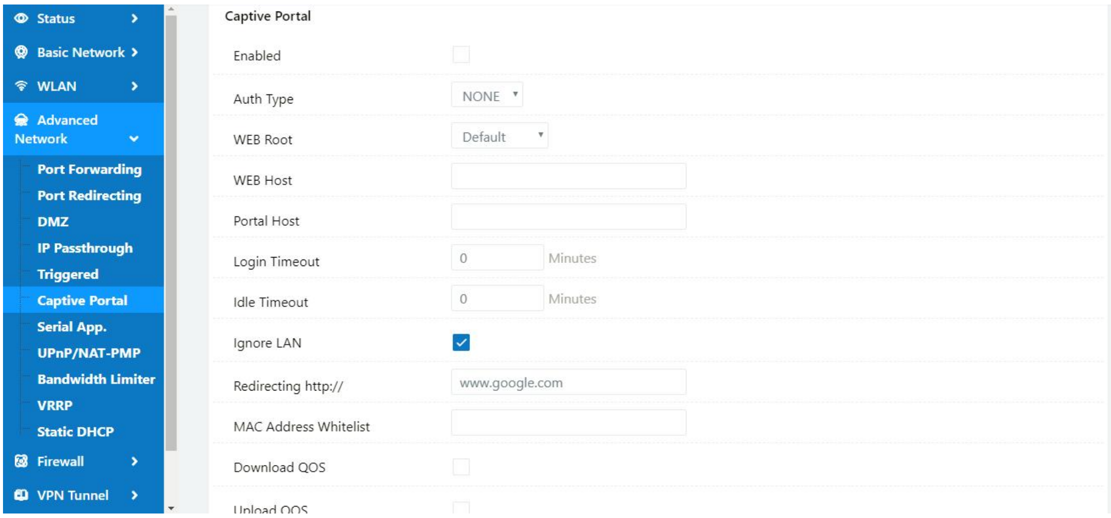
parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.
Note	Port triggering opens an incoming port when your computer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

Step 2 Please click ”save” to finish.

----End

Captive Portal

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



Captive Portal

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

Table 2-9 Captive Portal Instruction

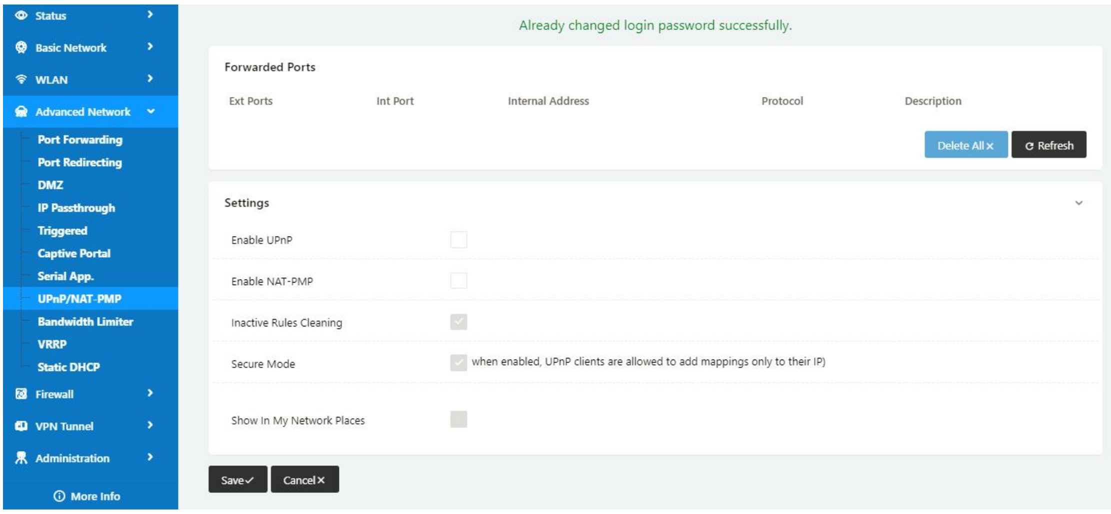
Parameter	Instruction
Enable	Enable Captive portal feature.
Auth Type	Reserved.
Web Root	Choose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router's Flash. Ex-storage: Captive portal file is in extended storage such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

----End

UPnp/NAT-PMP Setting

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



Already changed login password successfully.

Forwarded Ports

Ext Ports	Int Port	Internal Address	Protocol	Description

Settings

Enable UPnP □

Enable NAT-PMP □

Inactive Rules Cleaning ☑

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

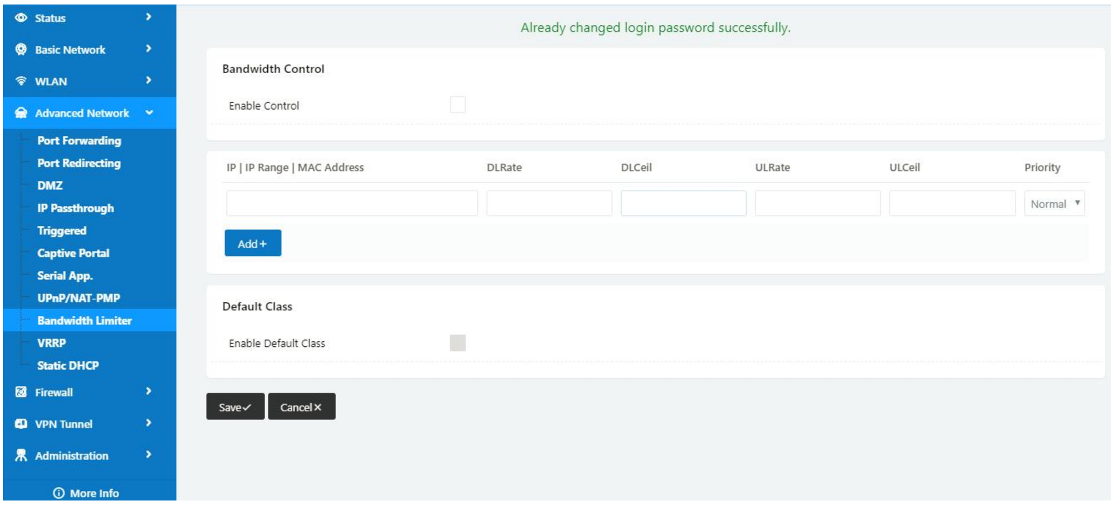
Show In My Network Places □

Step 2 Please click ”save” to finish.

----End

Bandwidth Control Setting

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



Already changed login password successfully.

Bandwidth Control

Enable Control □

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

Default Class

Enable Default Class □

Table 2-10 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.

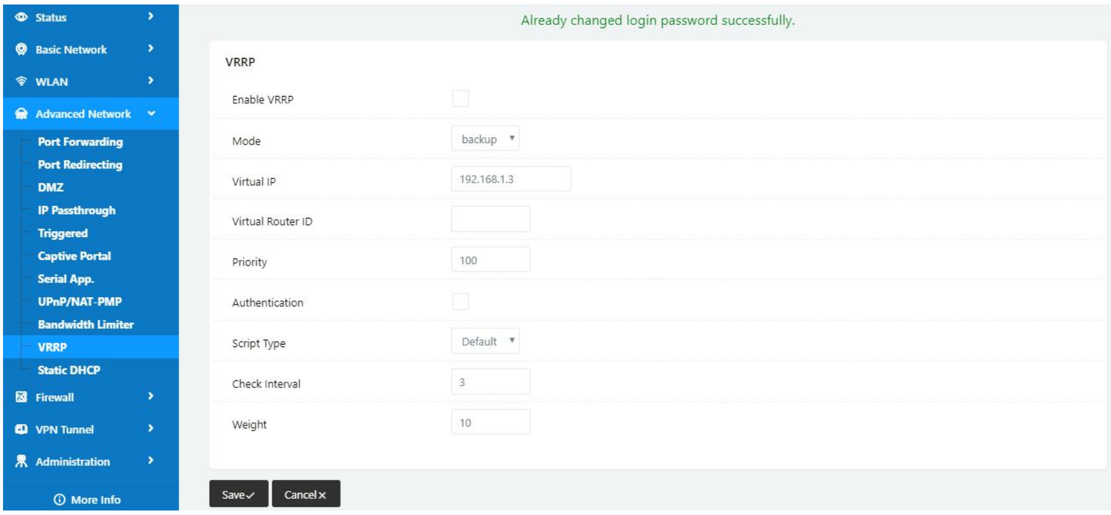
DL Rate	Mix Download rate
DL ceil	Max download rate
UL Rate	Mix Upload rate
UL ceil	Max upload rate
Priority	The priority of a specific user.
Default Class	If no specified IP/MAC, the download and upload limit for total speed for all of device.

Step 2 Please click ”save” to finish.

----End

VRRP Setting

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



Already changed login password successfully.

VRRP

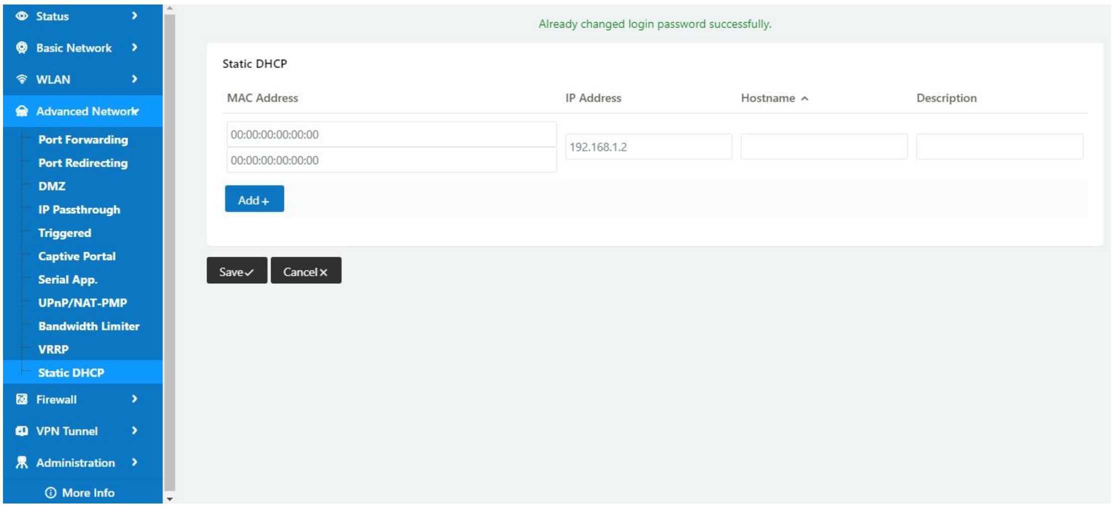
Enable VRRP	□
Mode	backup ▾
Virtual IP	192.168.1.3
Virtual Router ID	
Priority	100
Authentication	□
Script Type	Default ▾
Check Interval	3
Weight	10

Step 2 Please click ”save” to finish.

----End

Static DHCP Setting

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



Already changed login password successfully.

Static DHCP

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

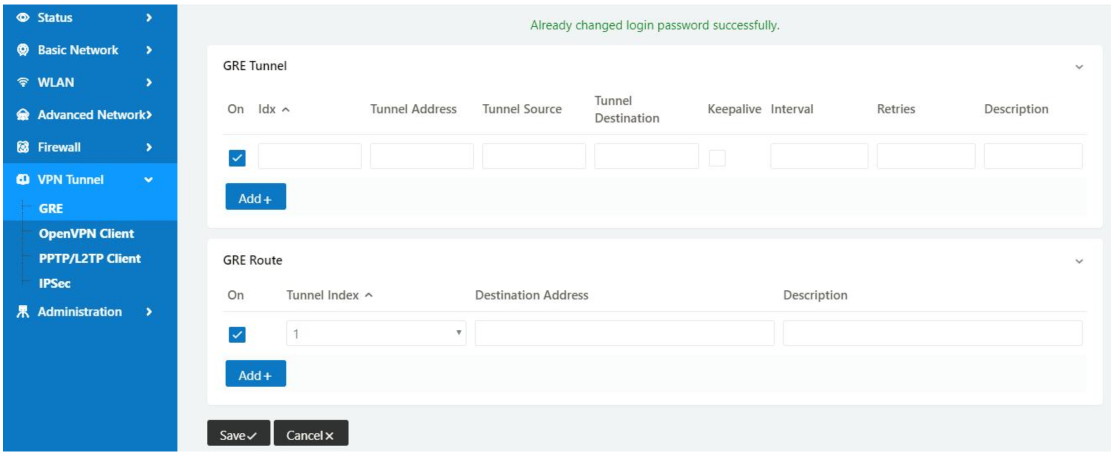
Step 2 Please click ”save” to finish.

----End

VPN Tunnel

GRE Setting

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



Already changed login password successfully.

GRE Tunnel

On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
☑					□			

GRE Route

On	Tunnel Index	Destination Address	Description
☑	1		

Table 2-11 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

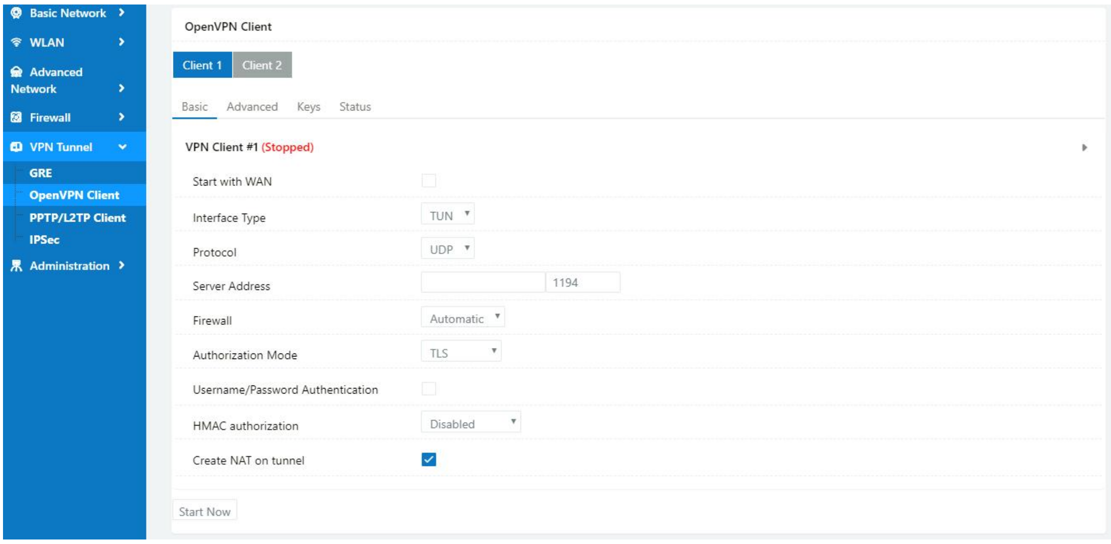
Parameter	Instruction
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.
Interval	Keep alive interval time.
Retries	Keep alive retry times. After retry times, GRE tunnel will be re-established.
Description	

Step 2 Please click ”save” to finish.

----End

OpenVPN Client Setting

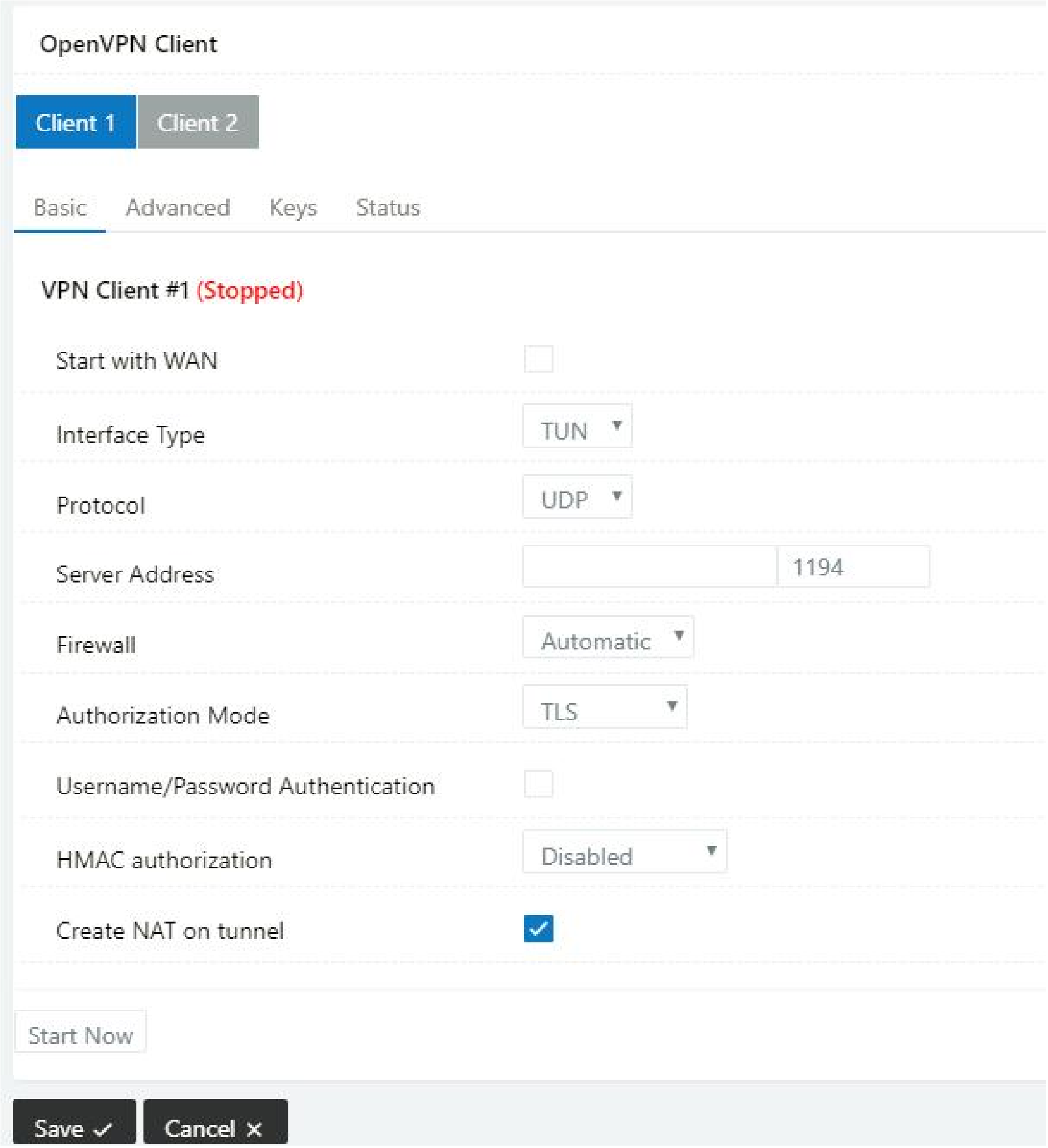
Step 1 VPN Tunnel> OpenVPN Client to check or modify the relevant parameter.



OpenVPN Client

VPN Client #1 (Stopped)

Start with WAN	□
Interface Type	TUN
Protocol	UDP
Server Address	1194
Firewall	Automatic
Authorization Mode	TLS
Username/Password Authentication	□
HMAC authorization	Disabled
Create NAT on tunnel	☑



OpenVPN Client

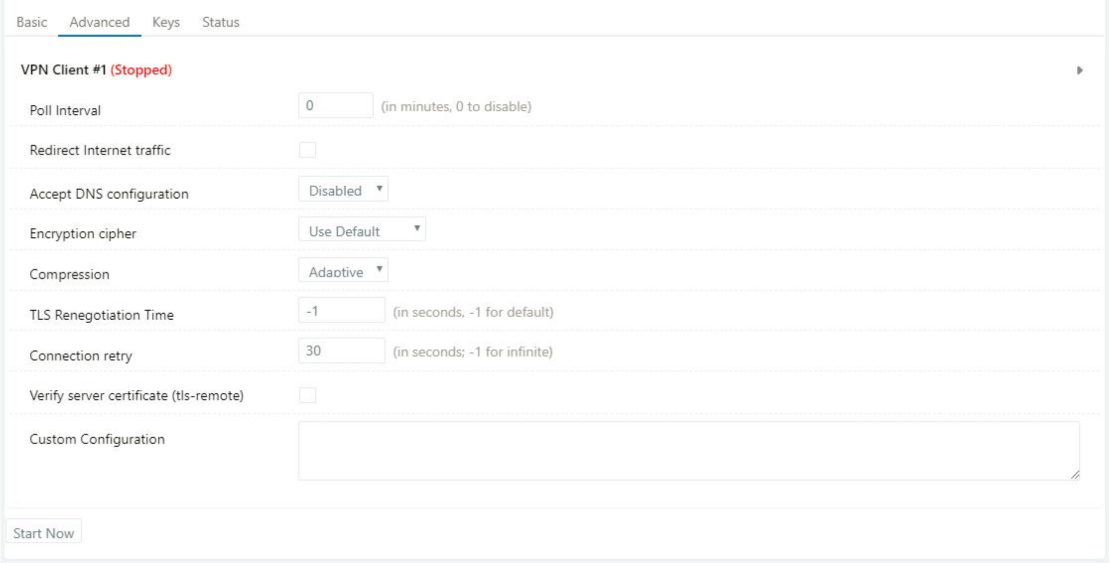
VPN Client #1 (Stopped)

Start with WAN	□
Interface Type	TUN
Protocol	UDP
Server Address	1194
Firewall	Automatic
Authorization Mode	TLS
Username/Password Authentication	□
HMAC authorization	Disabled
Create NAT on tunnel	☑

Table 2-12 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.



VPN Client #1 (Stopped)

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

Redirect Internet traffic: □

Accept DNS configuration: Disabled

Encryption cipher: Use Default

Compression: Adaptive

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

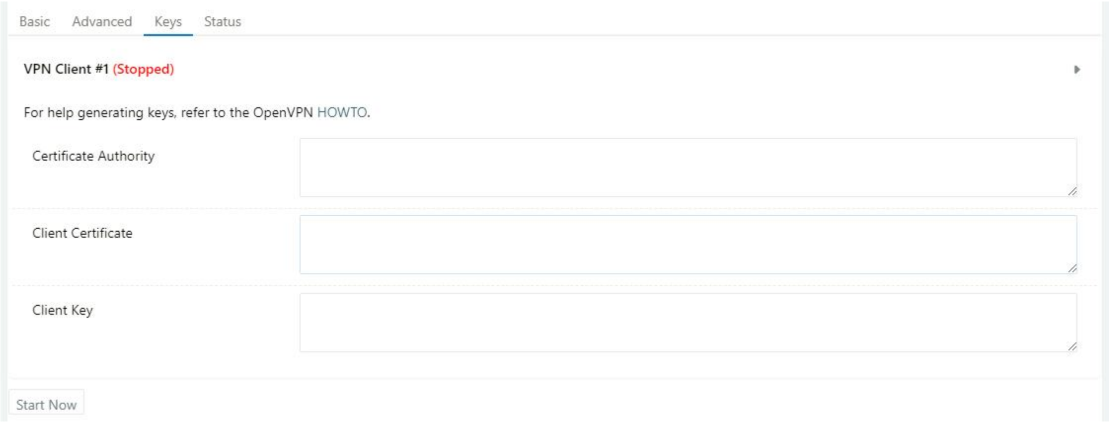
Connection retry: 30 (in seconds; -1 for infinite)

Verify server certificate (tls-remote): □

Custom Configuration:

Table 2-13 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.



VPN Client #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

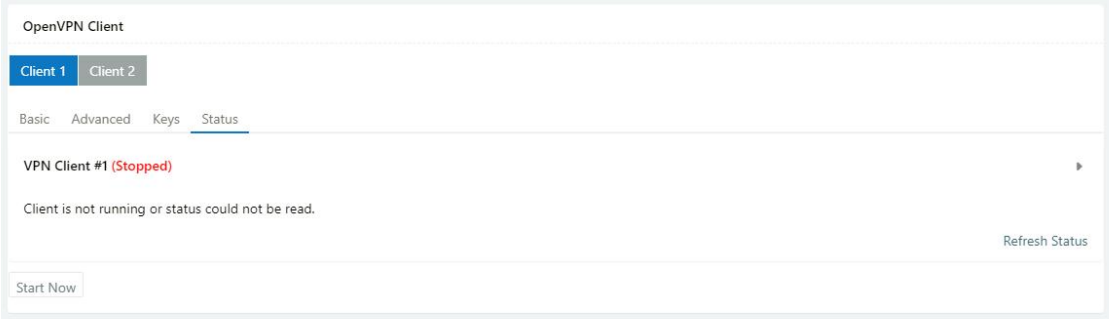
Certificate Authority

Client Certificate

Client Key

Table 2-14 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



VPN Client #1 (Stopped)

Client is not running or status could not be read.

Table 2-15 Status of OpenVPN Instruction

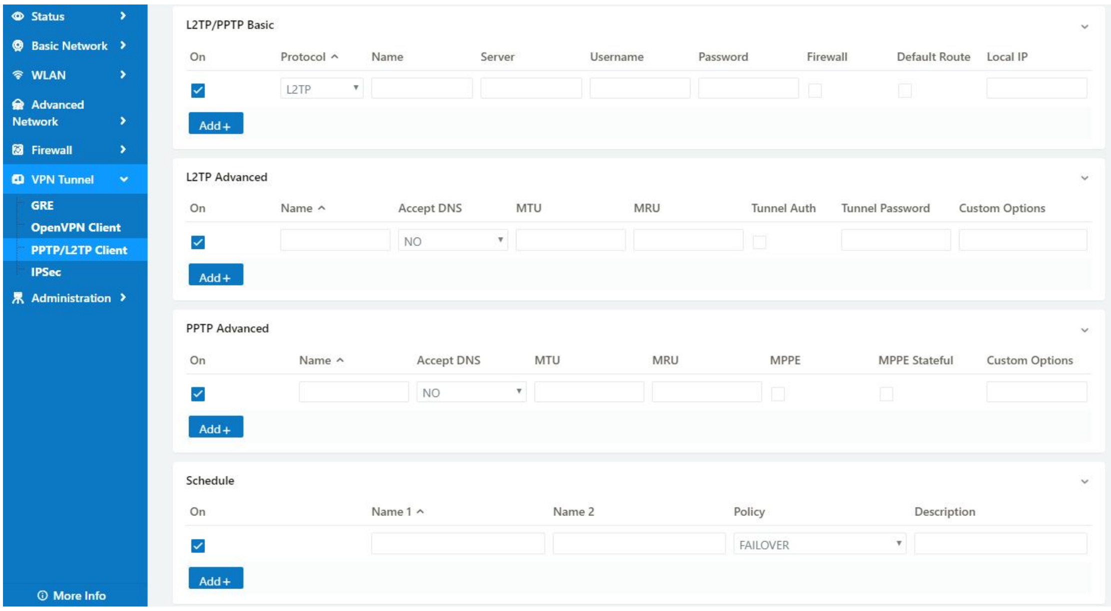
Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 2 Please click ”save” to finish.

----End

PPTP/L2TP Client Setting

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



L2TP/PPTP Basic

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
☑	L2TP					☐	☐	

Add+

L2TP Advanced

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

Add+

PPTP Advanced

On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
☑		NO			☐	☐	

Add+

Schedule

On	Name 1	Name 2	Policy	Description
☑			FAILOVER	

Add+

Table 2-16 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 2-17 L2TP Advanced Instruction

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

Custom Options	As the configuration requested.

Table 2-18 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

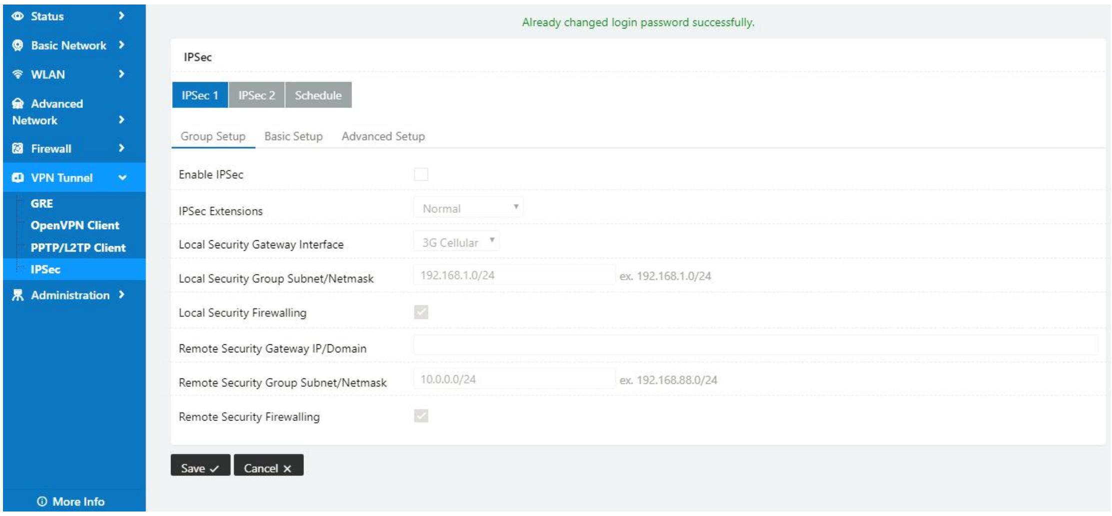
Table 2-19 SCHEDULE Instruction

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

Step 2 Please click ”save” to finish.

---End

IPSec Setting



Already changed login password successfully.

IPSec

Enable IPSec □

IPSec Extensions: Normal

Local Security Gateway Interface: 3G Cellular

Local Security Group Subnet/Netmask: 192.168.1.0/24 ex. 192.168.1.0/24

Local Security Firewalling ☑

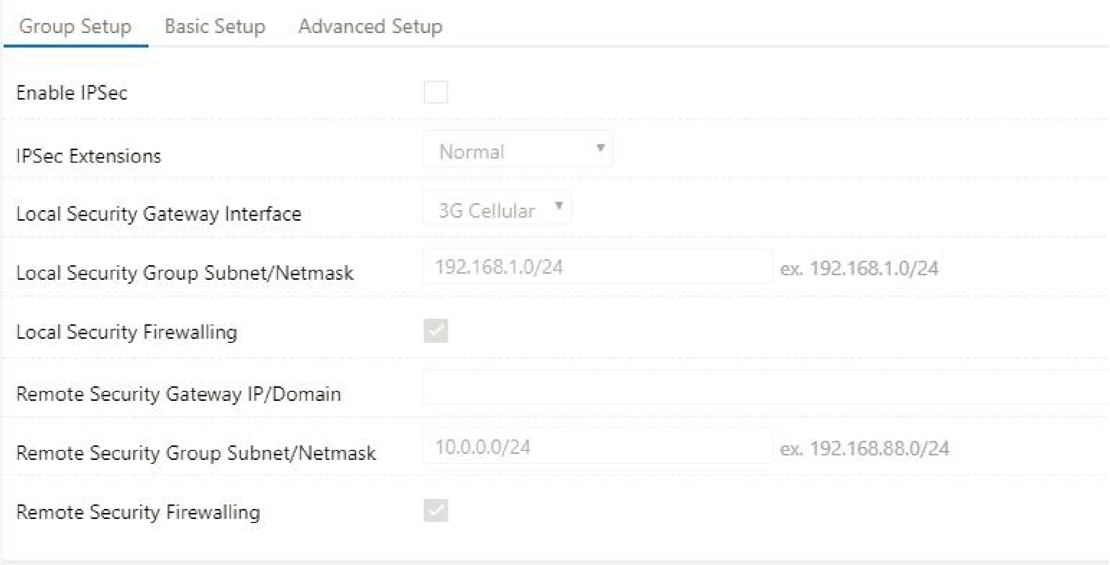
Remote Security Gateway IP/Domain:

Remote Security Group Subnet/Netmask: 10.0.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☑

IPSec Group Setup

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



Enable IPSec □

IPSec Extensions: Normal

Local Security Gateway Interface: 3G Cellular

Local Security Group Subnet/Netmask: 192.168.1.0/24 ex. 192.168.1.0/24

Local Security Firewalling ☑

Remote Security Gateway IP/Domain:

Remote Security Group Subnet/Netmask: 10.0.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☑

Table 2-20 IPSec Group Setup Instruction

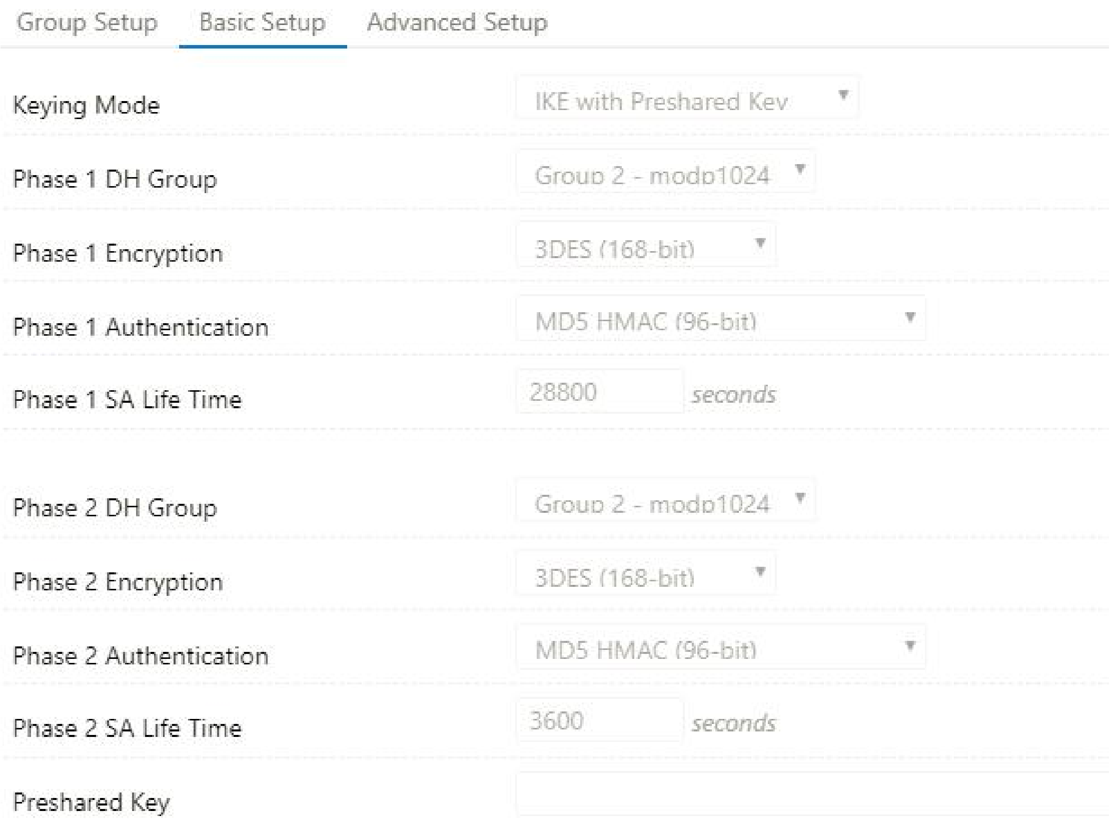
parameter	Instruction
IPSec Extensions	Support Standard IPSec, GRE over IPSec, L2TP over IPSec
Local Security Interface	Defined the IPSec security interface
Local Subnet/Mask	IPSec local subnet and mask.

parameter	Instruction
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.

IPSec Basic Setup

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



Keying Mode: IKE with Preshared Key
Phase 1 DH Group: Group 2 - modp1024
Phase 1 Encryption: 3DES (168-bit)
Phase 1 Authentication: MD5 HMAC (96-bit)
Phase 1 SA Life Time: 28800 seconds
Phase 2 DH Group: Group 2 - modp1024
Phase 2 Encryption: 3DES (168-bit)
Phase 2 Authentication: MD5 HMAC (96-bit)
Phase 2 SA Life Time: 3600 seconds
Preshared Key:

Table 2-21 IPSec Basic Setup Instruction

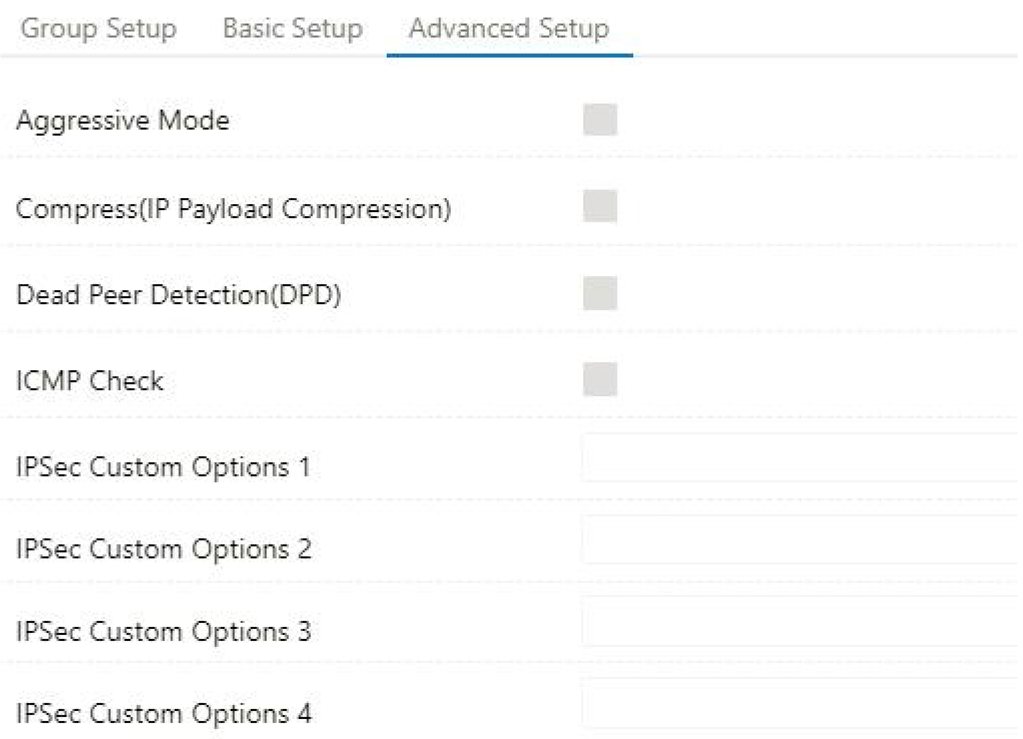
parameter	Instruction
Keying Mode	IKE preshared key
Phase 1 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.
Phase 1	Support 3DES, AES-128, AES-192, AES-256

parameter	Instruction
Encryption	
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.

IPSec Advanced Setup

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



Aggressive Mode □

Compress(IP Payload Compression) □

Dead Peer Detection(DPD) □

ICMP Check □

IPSec Custom Options 1

IPSec Custom Options 2

IPSec Custom Options 3

IPSec Custom Options 4

Table 2-22 IPSec Advanced Setup Instruction

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

Step 2 Please click ”save” to finish.

----End