User Manual

---Apply to WL-G510 Series Industrial 4G/3G Router

V1.0

http://www.wlink-tech.com

March, 2018

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.

Shenzhen WLINK Technology Company Limited

Add： 3F, Yiben Building, Chaguang Road, Xili, Nanshan Dist., China, 518000

Web： http://www.wlink-tech.com

Service Email： support@wlink-tech.com

Tel： 86-755-86089513

Fax： 86-755-26059261

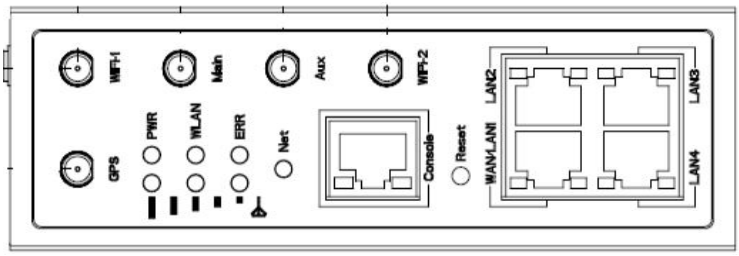
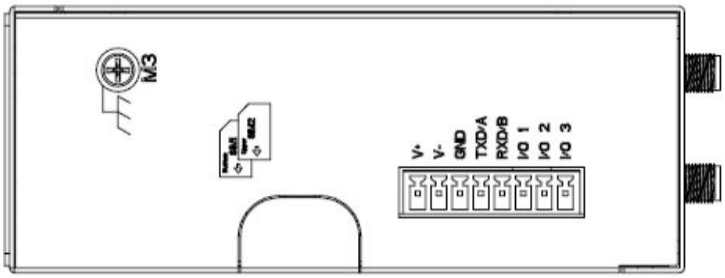
Contents

1 Hardware Installation

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

1.1 Panel

Table 1-1 WL-G510 Structure

WLINK Tech.	G510 series
Front	
Top	

NOTE

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

Table 1-2 Router Interface

Port	Instruction	Remark
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection.	

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

1.2 LED Status

Table 1-3 Router LED indictor Status

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

NOTE

There are some difference in the LED indicator of the router with expanded Wi-Fi, GPS function and single module dual SIM.

1.3 Dimension

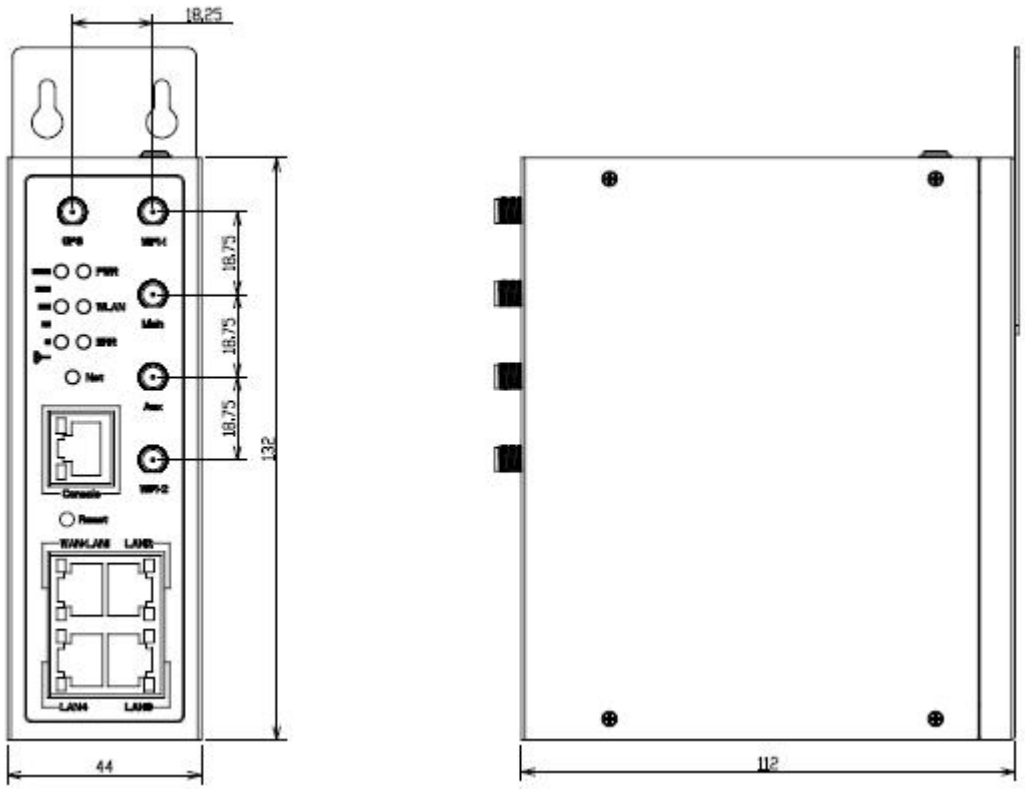
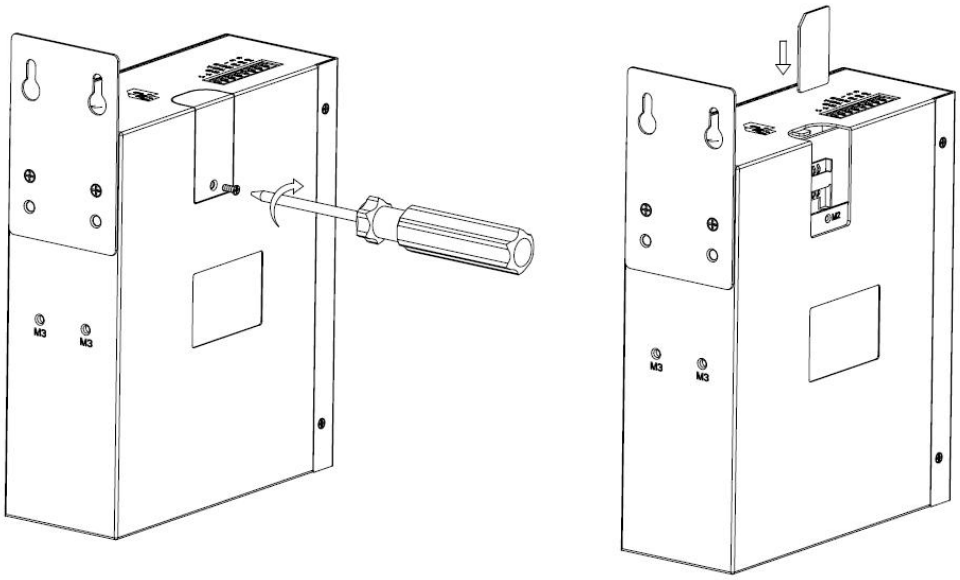


Figure 1-2 G510 Series Router Dimension

1.4 How to Install

1.4.1 SIM/UIM card install

Please insert the dual SIM cards before configure the router.



CAUTION

Before connecting, please disconnect any power resource of router

1.4.2 Ethernet Cable Connection

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

1.4.3 4G and Wi-Fi Antenna Plug

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

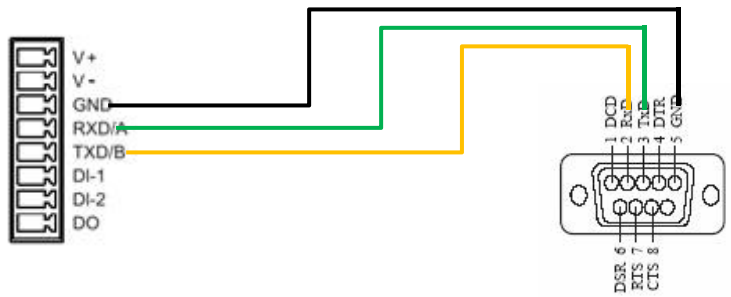
NOTE

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

1.4.4 Serial Port (Terminal block) Connection

The serial port supports alternative RS232/RS485 port, and RS232 port as default. It might be requested serial port for RS485 when place order. The serial port feature supports TCP/UDP client/server as optional, also supports Modbus protocol. You may check the feature in Serial App of Advanced Network UI. Below is RS232 connection sequence as reference.

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



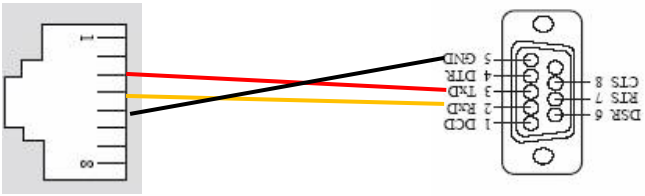
CAUTION

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

1.4.5 Console Port Connection

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

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



1.4.6 Power Supply

Plug in power adaptor.Voltage input range:+7.5~32VDC. (Extended models: 7.5~ 48VDC)

1.4.7 Review

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

CAUTION

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

Notice:

Step 1 Check the antenna connection.

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

Step 3 Power on the industrial Router

----END

2 Router Configuration

WL-G510 Series routers support GUI and CLI configuration. This chapter introduce GUI configuration via Ethernet port, if need CLI configuration guide, please contact our technical support department by email: support@wlink-tech.com.

2.1 Local Configure

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

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 2-3 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 2-4 User Identify Interface

----END

2.2 Status

Check routers status after login router.

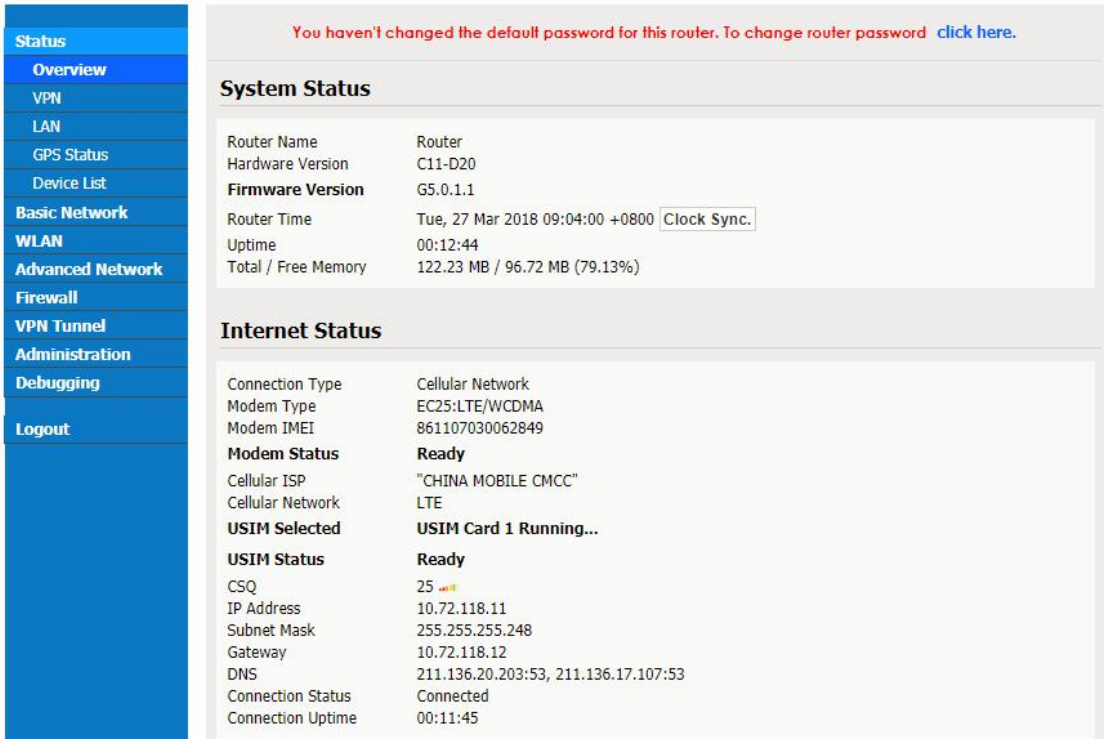


Figure 2-5 Router Status GUI

NOTE

After login, router status will be show as below, then you should change the password according to the prompts.

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

3.2.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface

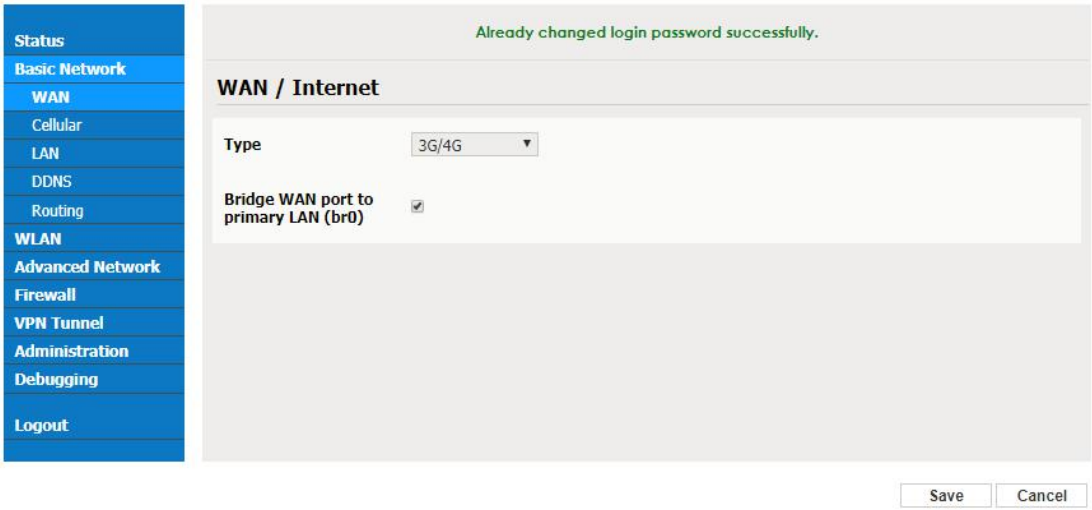


Figure 3-1 WAN Setting GUI

Table 3-1 WAN Setting Instruction

Parameter	Instruction
Type	Support 3G/4G, PPPoE, DHCP, Static IP
Bridge WAN to LAN	Configure WAN port as LAN port

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

----End

3.2.2 Cellular Network Configure

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

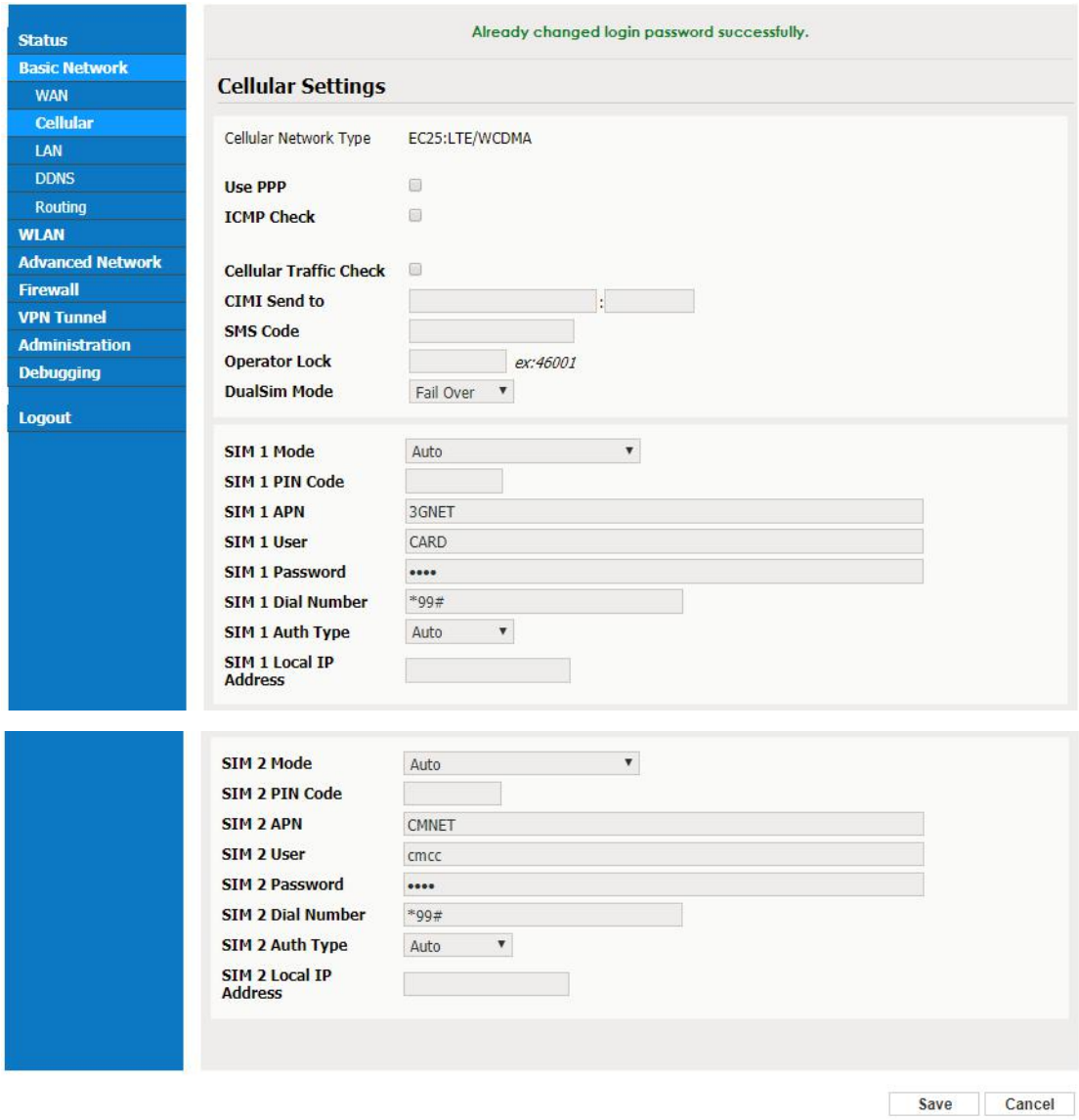


Figure 3-2 Cellular Setting GUI

Parameter	Instruction
Use PPP	ECM dialup as default. PPP optional.
ICMP check	If enable ICMP check and setup a reachable IP address as destination IP, the router will reconnect/reboot once ICMP check failed.
Cellular Traffic Check	The router will reconnect/reboot once there's no Rx/Tx data.
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock a specified operator for the router by MCC/MNC code.

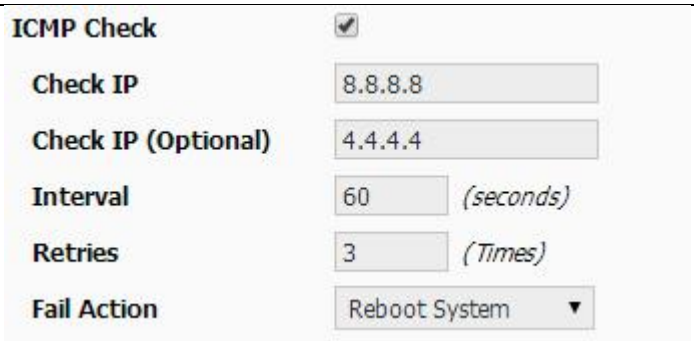
Parameter	Instruction
Dual SIM Mode	【Fail Over】Two SIM cards mutual backup. Once SIM1 failed, it'll switch to SIM2 and work on SIM2, and vice versa. 【SIM1 Only】Only SIM1 works. 【SIM2 Only】Only SIM2 works. 【Backup】SIM1 is the primary SIM. Once SIM1 failed, it'll switch to SIM2 and work on SIM2 for a specified period of time, then it switches back to SIM1.
Connect Mode	【Auto】The router will automatically connect to 3G/4G networks and give priority to 4G. 【LTE】Router will connect to 4G only. 【3G】Router will connect to 3G only.
Pin Code	Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen.
APN	APN is provided by local ISP, usually CDMA/EVDO networks do not need this parameter.
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth. Type	Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional.
SIM Local IP Address	Fix SIM IP. The feature is available if carrier can provide this service.

NOTE ICMC 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.

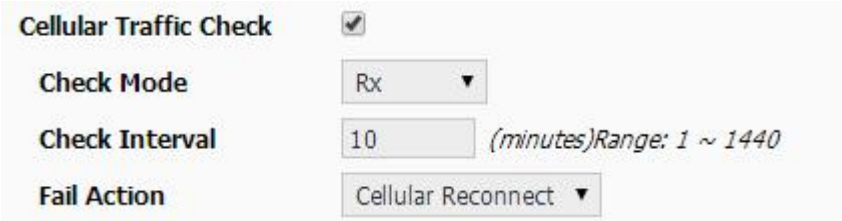
The ICMP Check IP is a public IP or company server IP address.



【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

3.2.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface

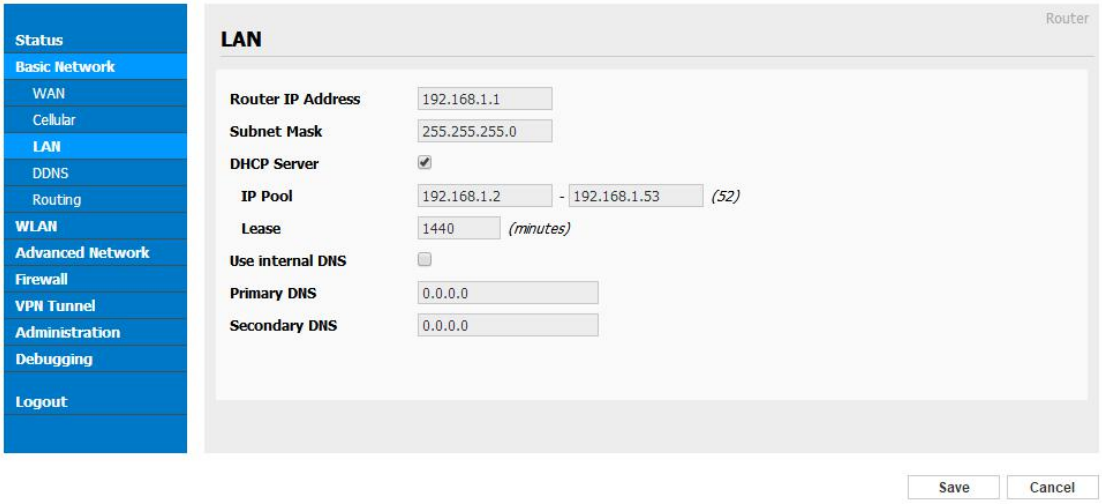


Figure 3-3 LAN Setting GUI

Table 3-2 LAN Setting Instruction

Parameter	Instruction
Router IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease
IP Address Range	IP address range within LAN
Lease	The valid time
Use Internal DNS	If click this option, router will use 3G/4G network DNS which is assigned by 3G/4G network. If not click this option, router will use custom DNS
Primary DNS	Available as customer configured
Secondary DNS	Available as customer configured

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

----End

3.2.4 Dynamic DNS Setting

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

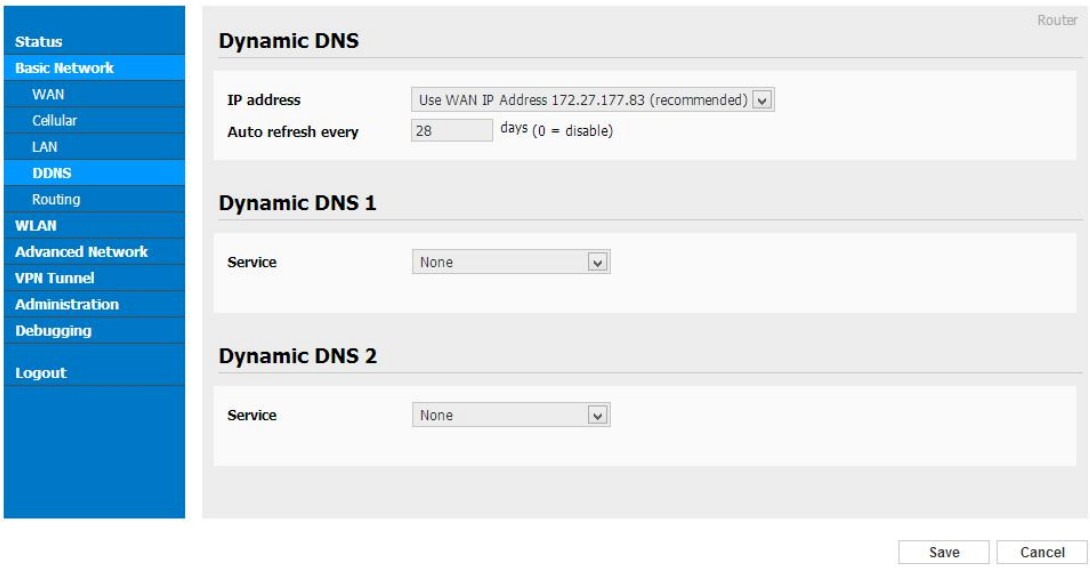


Figure 3-4 Dynamic DNS Setting

Table 3-3 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

3.2.5 Routing Setting

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

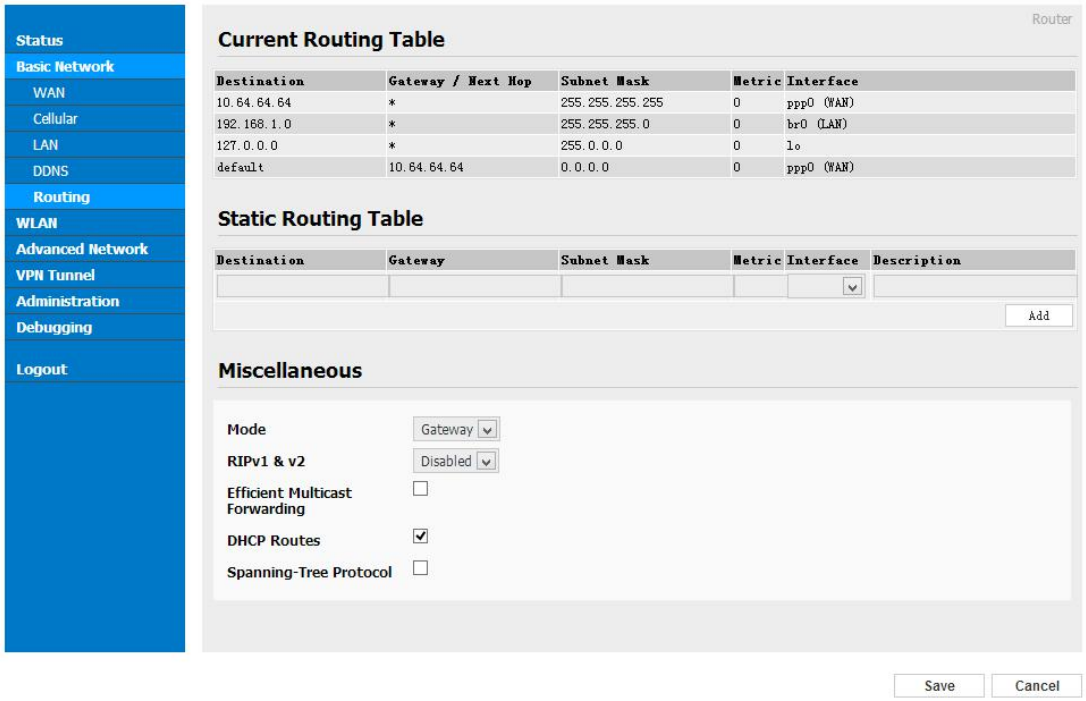


Figure 3-5 Routing Setting

Table 3-4 Routing Setting Instruction

Parameter	Instruction
Destination	Router can reach the destination IP address.
Gateway	Next hop IP address which the router will reach
Subnet Mask	Subnet mask for destination IP address

Parameter	Instruction
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.

3.3 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

3.3.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter

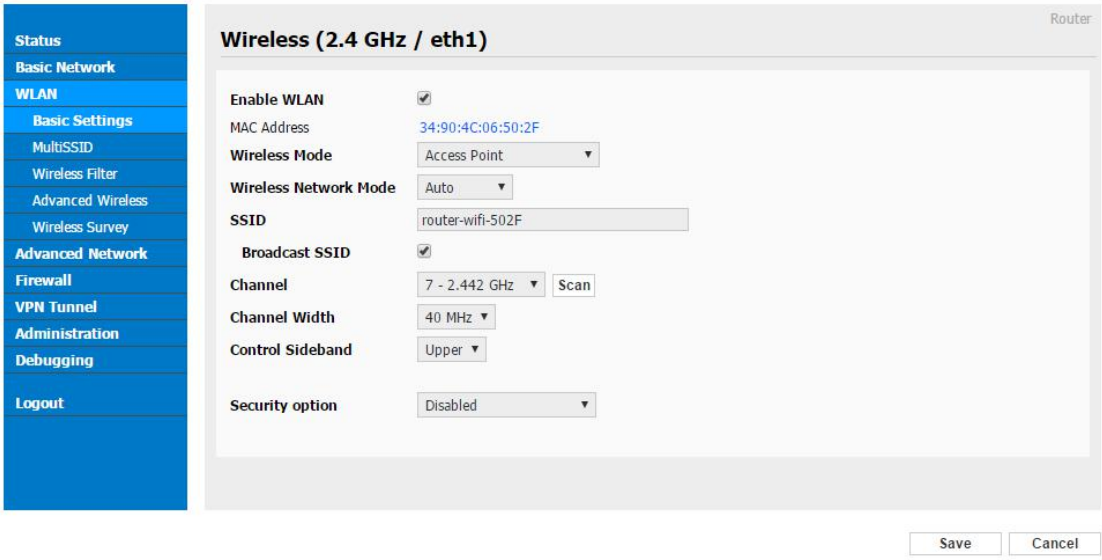


Figure 3-6 WLAN Basic Settings GUI

Table 3-5 Basic Setting Instruction

Parameter	Instruction
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP, AP+WDS, Bridge, Client, WDS
Wireless Network protocol	Support Auto, IEEE 11b/g/n optional
SSID	The default is router, can be modified as per application.
Channel	The channel of wireless network, suggest keep the default

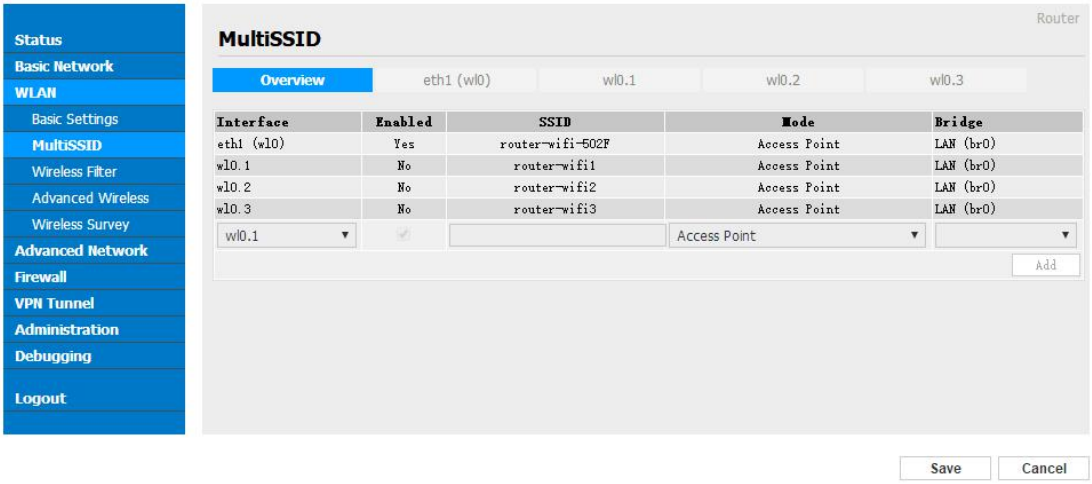
Parameter	Instruction
Channel Width	20MHZ and 40MHZ alternative
Security	Support various encryption method

Step 2 Please click “Save” to finish.

----End

3.3.2 Wireless Filter Setting

Step 1 WLAN > MultiSSID



3.3.3 Wireless Filter Setting

Step 1 WLAN > Wireless Filter

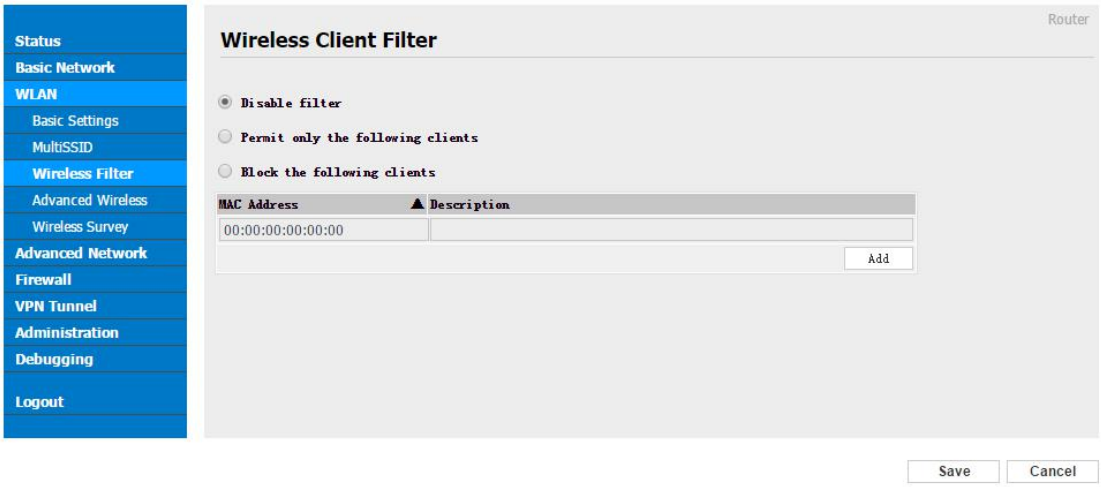


Figure 3-7 Wireless Client Filter Setting GUI

The Wireless Filter enable to set the permitted client or prohibit the specific client to

connect the WiFi, However, this feature is invalid for wired connection application.

Table 3-6 ”Wireless Client Filter” Setting Instruction

Parameter	Instruction
Disable Filter	Choose to disable
Permit on the following client	Only allow the listed MAC address to connect to router by wireless
Block the follow Client	Prevent the listed MAC address to connect to router by wireless

Step 2 Please click ”save” to finish

----End

3.3.4 Advanced Wireless Setting

Step 1 WLAN> Advanced Wireless to check or modify the relevant parameter.

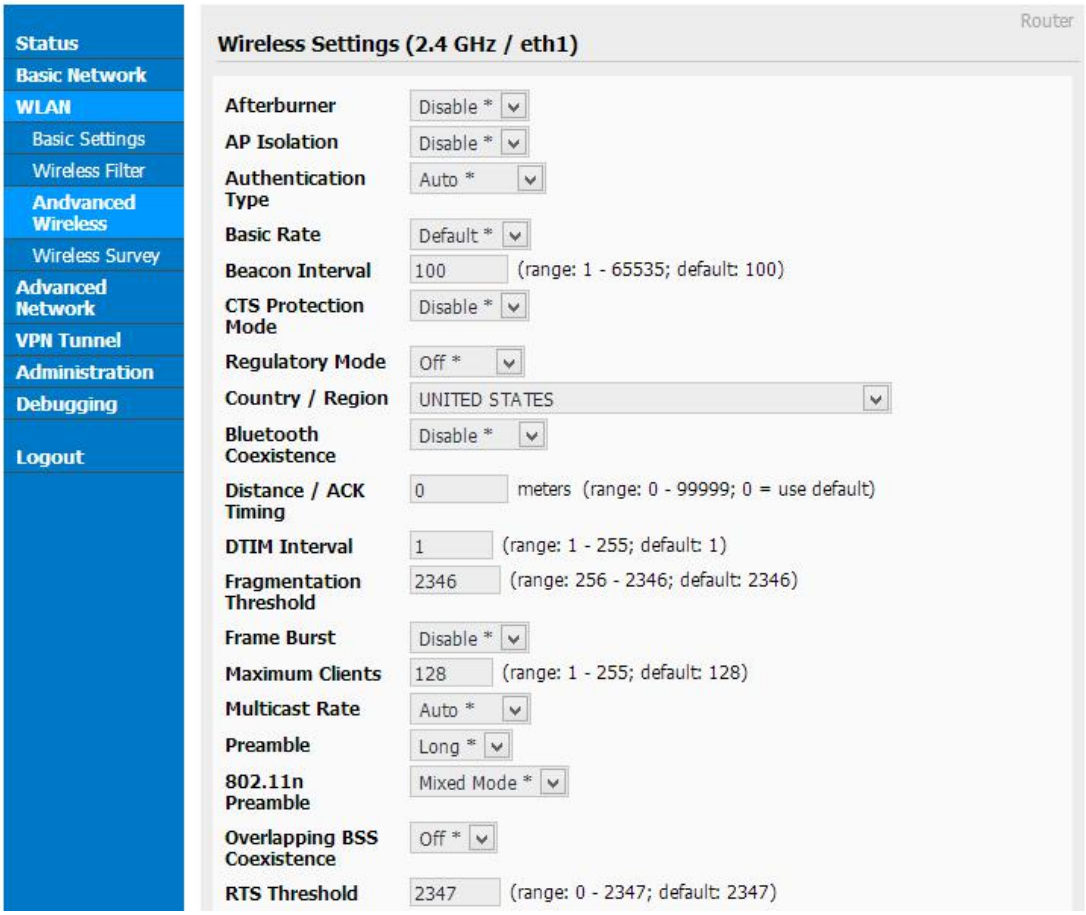


Figure 3-8 Advanced Wireless Setting GUI

Step 2 Please click ”save” to finish.

----End

3.3.5 Wireless Survey

Step 1 WLAN> Wireless Survey to check survey.

Figure 3-9 Wireless Survey Setting GUI

----End

3.4 Advanced Network Setting

3.4.1 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.

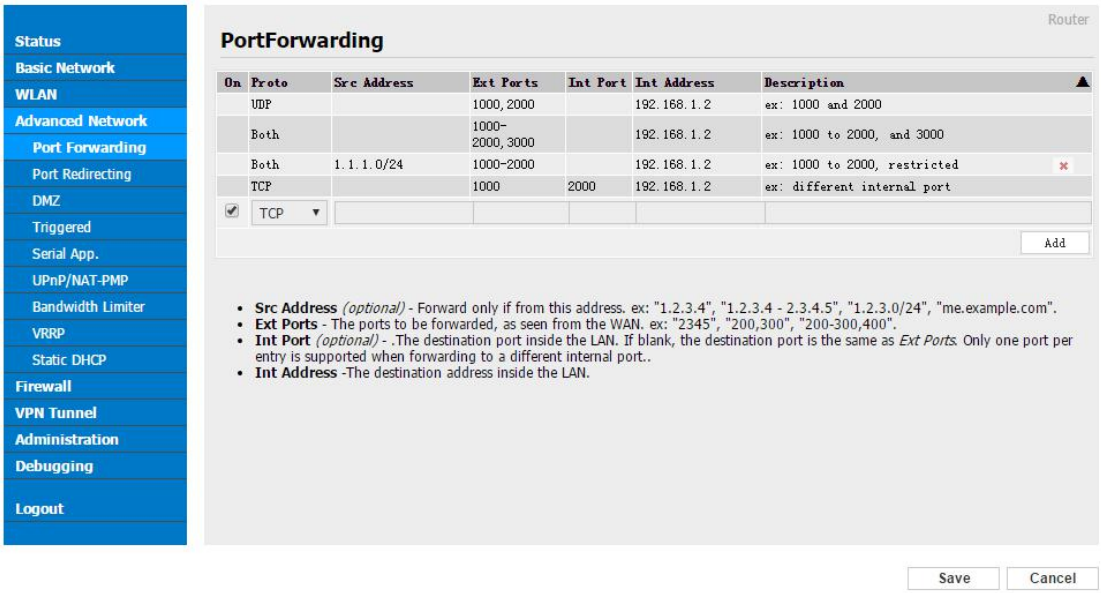


Figure 3-10 Port Forwarding GUI

Table 3-7 “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

3.4.2 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.

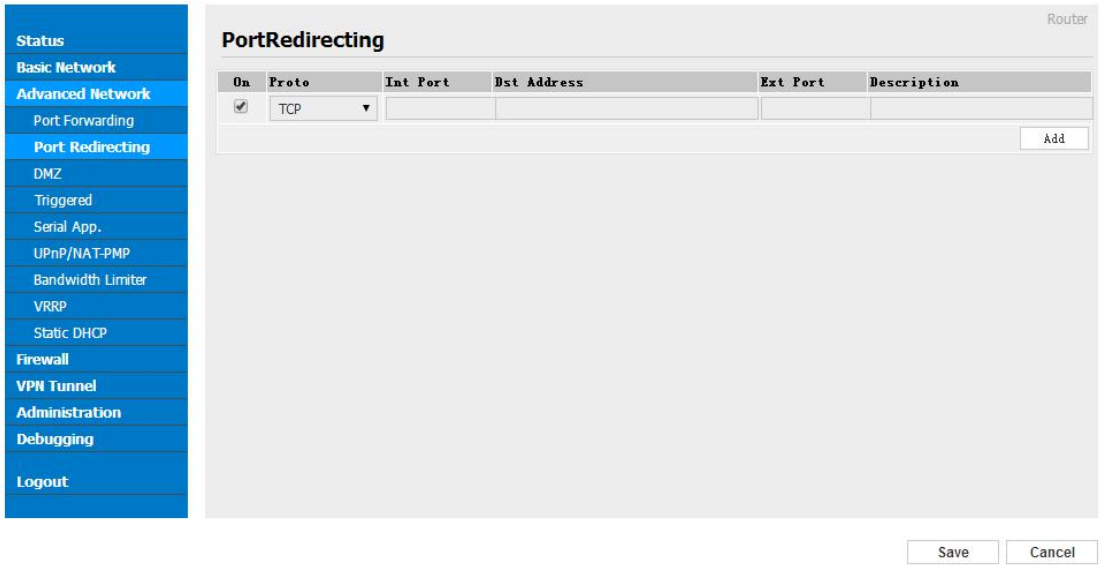


Figure 3-11 Port Forwarding GUI

Table 3-8 “Port Redirecting” Instruction

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP

Parameter	Instruction
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

----End

3.4.3 DMZ Setting

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

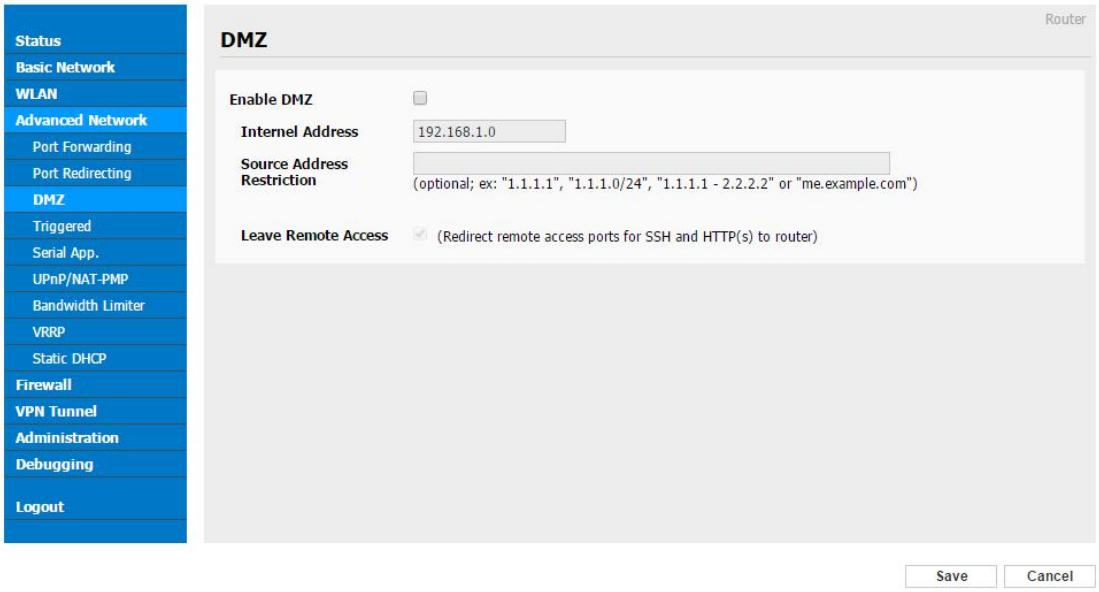


Figure 3-12 DMZ GUI

Table 3-9 “DMZ” Instruction

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

Step 2 Please click ”save” to finish

----End

3.4.4 IP Passthrough Setting

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

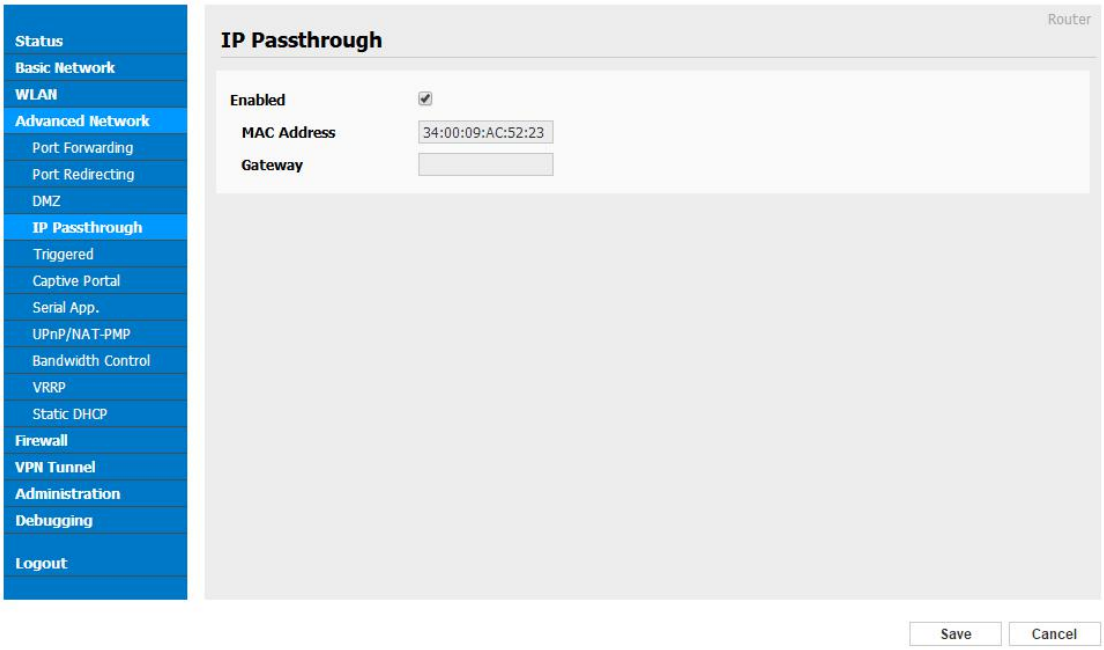


Figure 3-13 IP Passthrough GUI

Table 3-10 “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-R520 connect to multiple device, input other device gateway. The device might access to router GUI.

Step 2 Please click ”save” to finish

----End

3.4.5 Triggered Setting

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

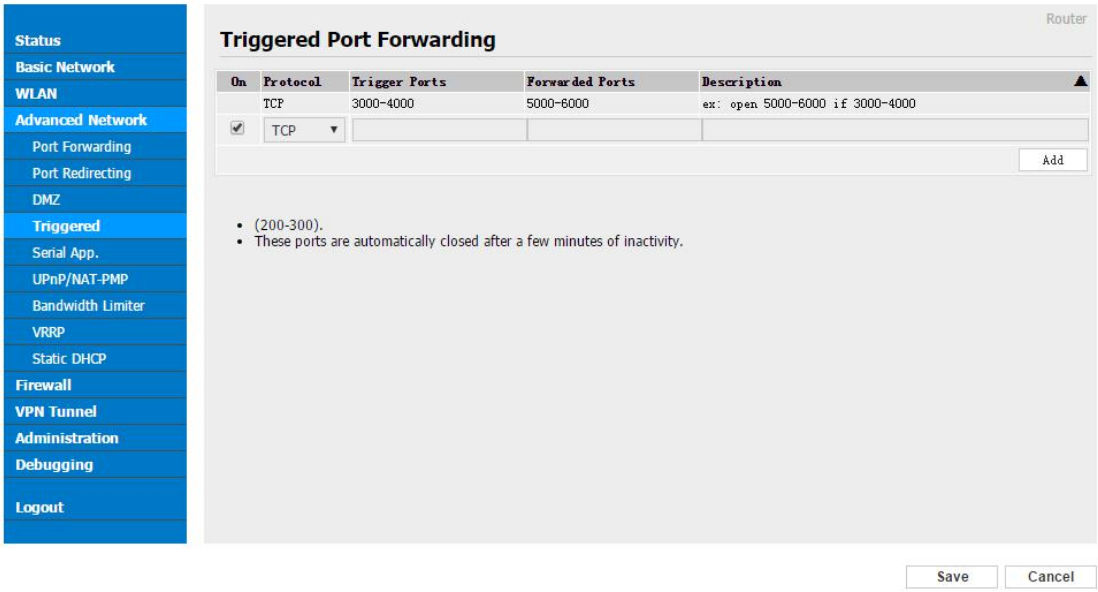


Figure 3-14 Triggered GUI

Table 3-11 “Triggered” Instruction

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

Step 2 Please click ”save” to finish.

----End

3.4.6 Serial App. Setting

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

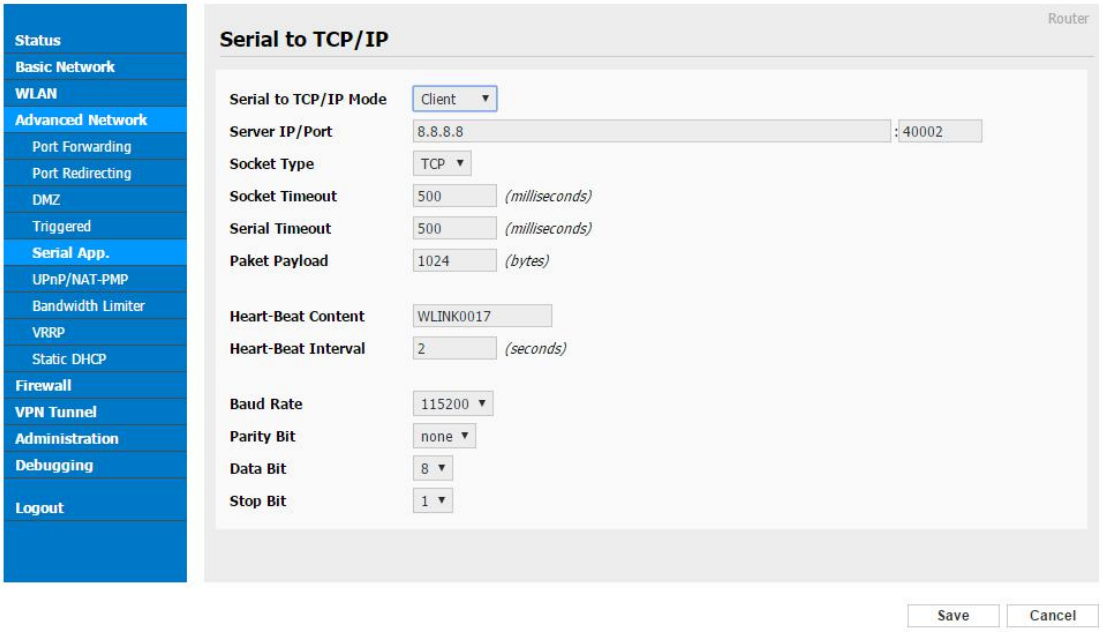


Figure 3-15 Serial App Setting GUI

Table 3-12 "Serial App" Instruction

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

NOTE

Serial port connection

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

Step 2 Please click ”save” to finish.

----End

3.4.7 UPnp/NAT-PMP Setting

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

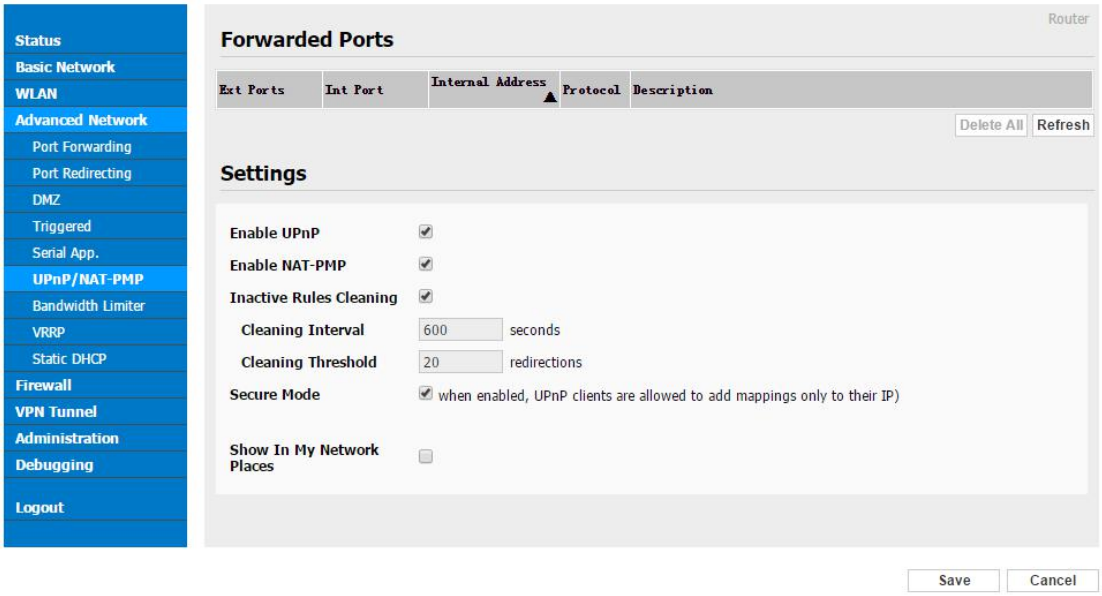


Figure 3-16 UPnp/NAT-PMP Setting GUI

Step 2 Please click ”save” to finish.

3.4.8 Bandwidth Control Setting

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

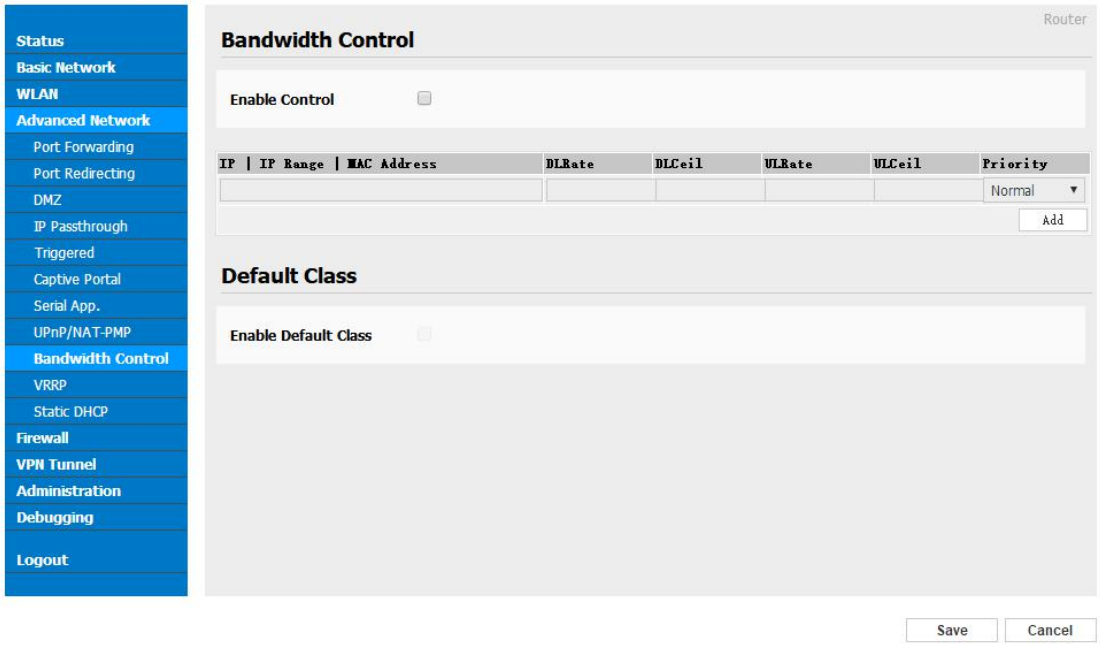


Figure 3-17 Bandwidth Control Setting GUI

Step 2 Please click ”save” to finish.

----End

3.4.9 VRRP Setting

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

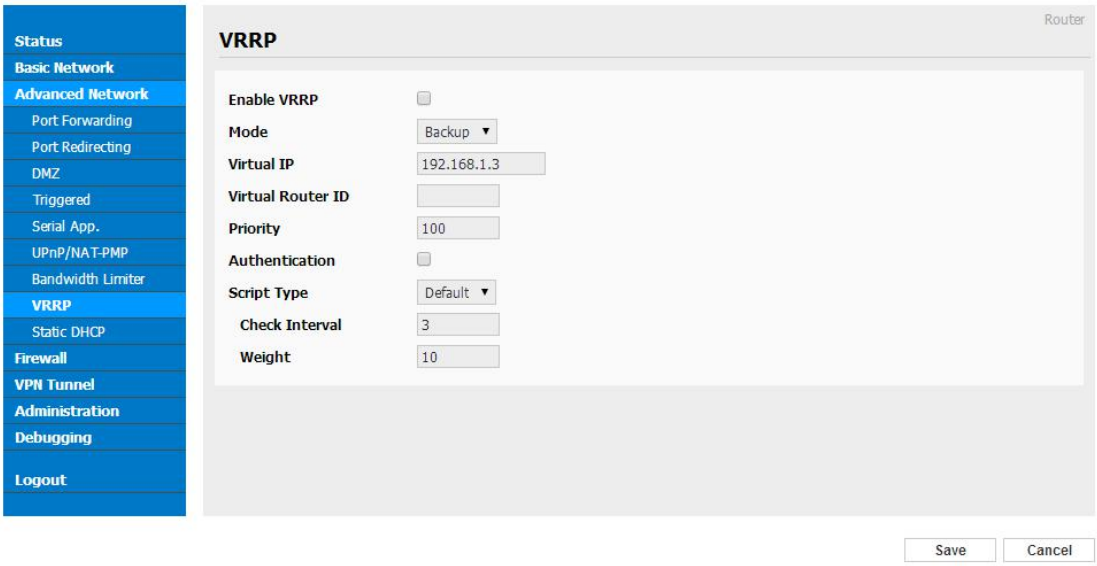


Figure 3-18 VRRP Setting GUI

Step 2 Please click ”save” to finish.

----End

3.4.10 Static DHCP Setting

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

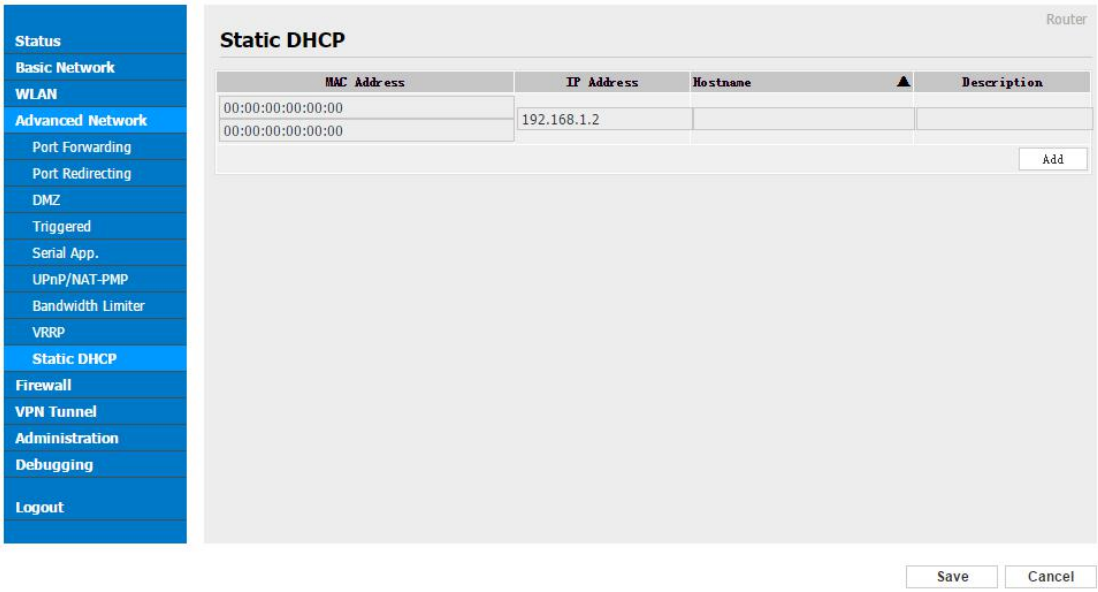


Figure 3-19 Static DHCP Setting GUI

Step 2 Please click ”save” to finish.

----End

3.5 Firewall

3.5.1 IP/URL Filtering

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

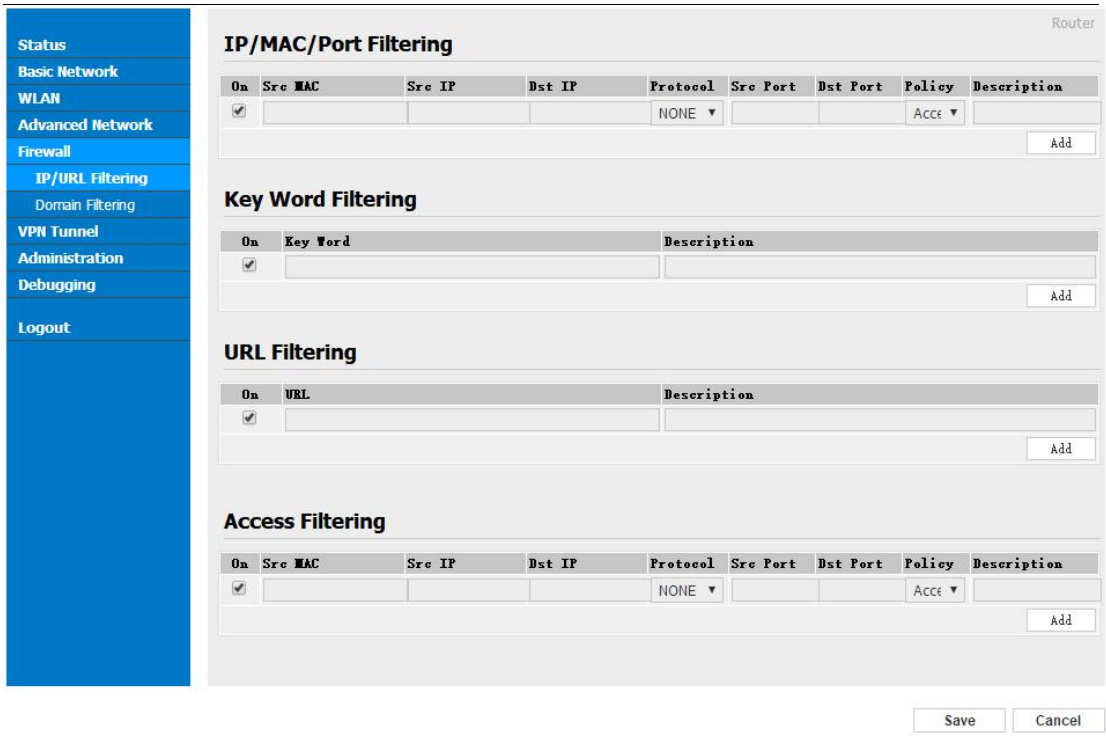


Table 3-13 “IP/URL Filtering” Instruction

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

Step 2 Please click ”save” to finish.

---End

3.5.2 Domain Filtering

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

Figure 3-20 Domain Filtering Setting GUI

Table 3-14 "GRE" Instruction

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

Step 2 Please click "save" to finish.

----End

3.6 VPN Tunnel

3.6.1 GRE Setting

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

Figure 3-21 GRE Setting GUI

Table 3-15 “GRE” Instruction

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

Step 2 Please click ”save” to finish.

----End

3.6.2 OpenVPN Client Setting

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

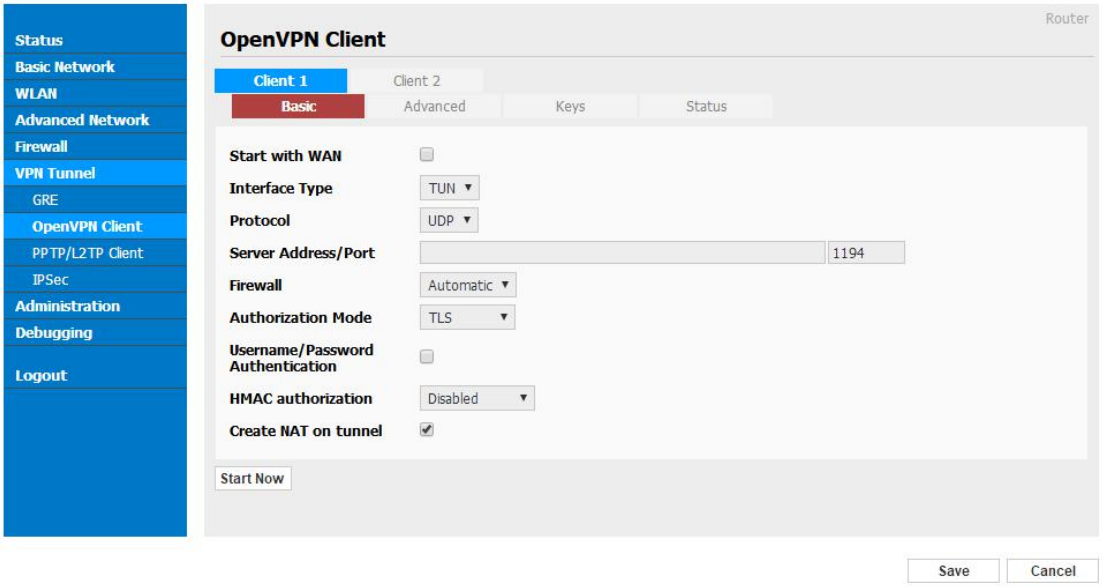
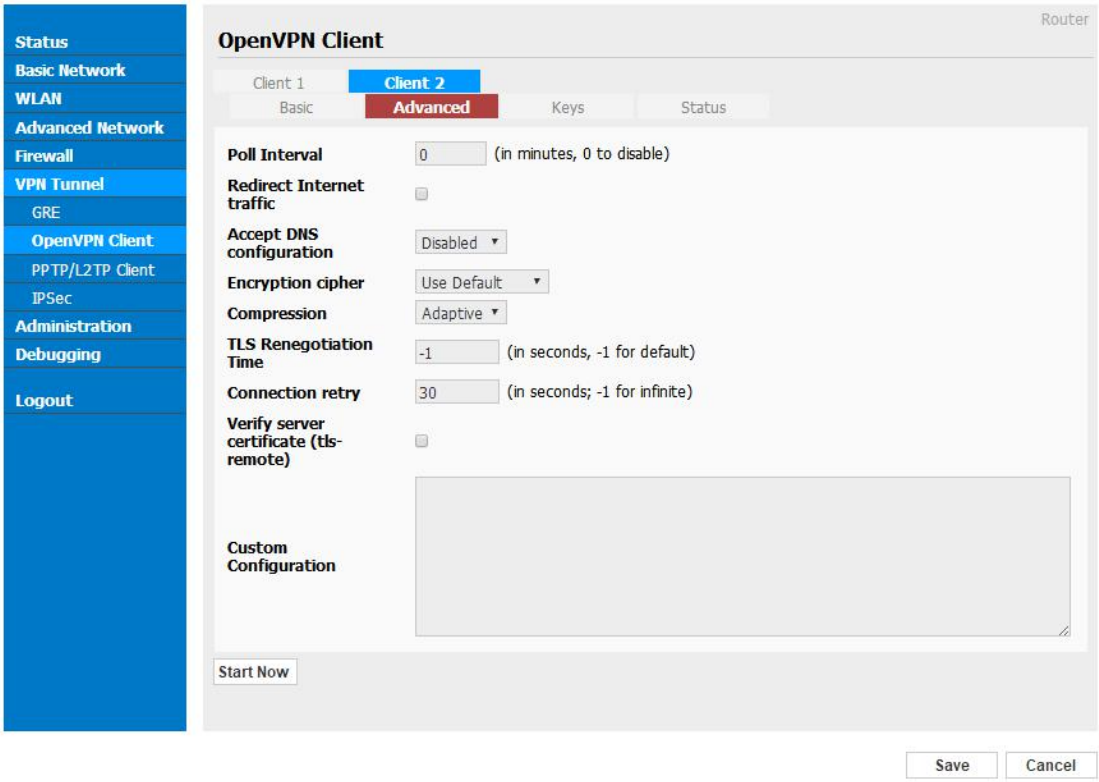


Figure 3-22 OpenVPN Setting GUI

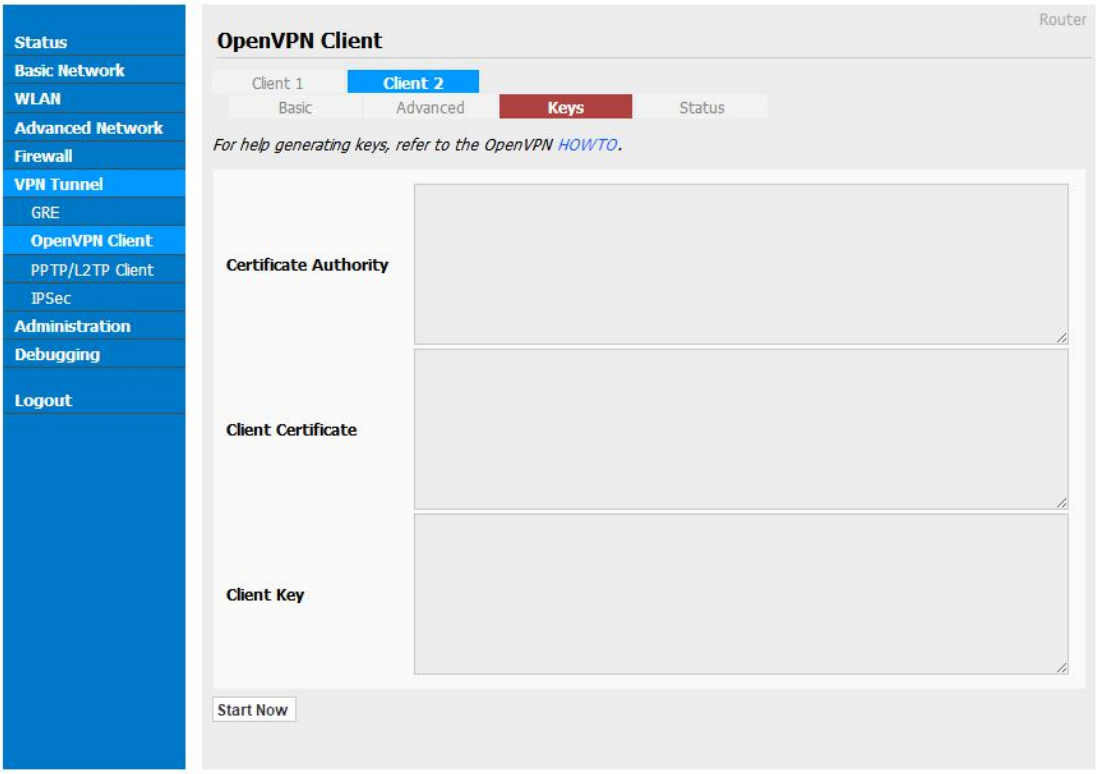
Table 3-16 “OpenVPN” Instruction

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

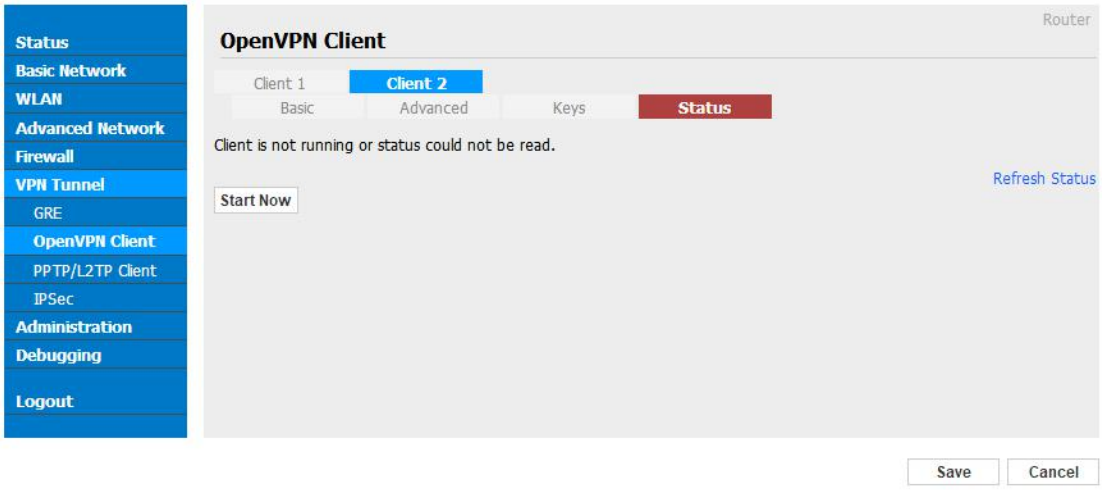


Parameter	Instruction
Poll Interval	Openvpn client check router’s status as interval time.

Parameter	Instruction
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 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



Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 2 Please click ”save” to finish.

----End

3.6.3 VPN Client Setting

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

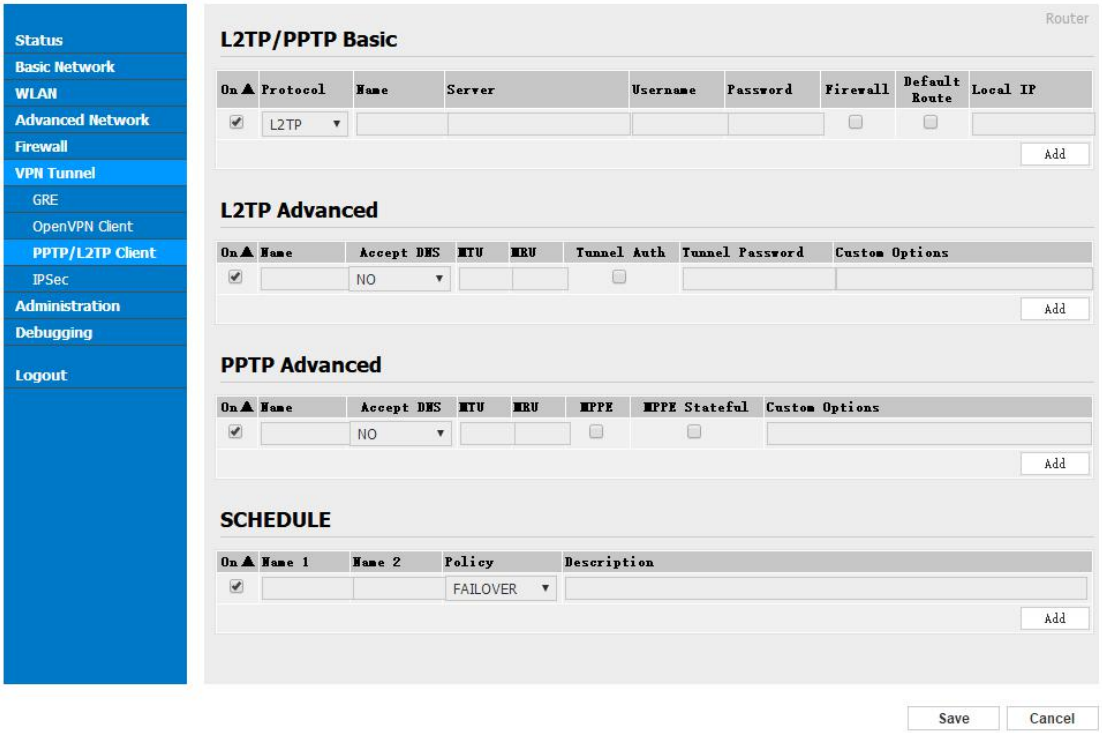


Table 3-17 “PPTP/L2TP Basic” Instruction

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 3-18 “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 3-19 “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

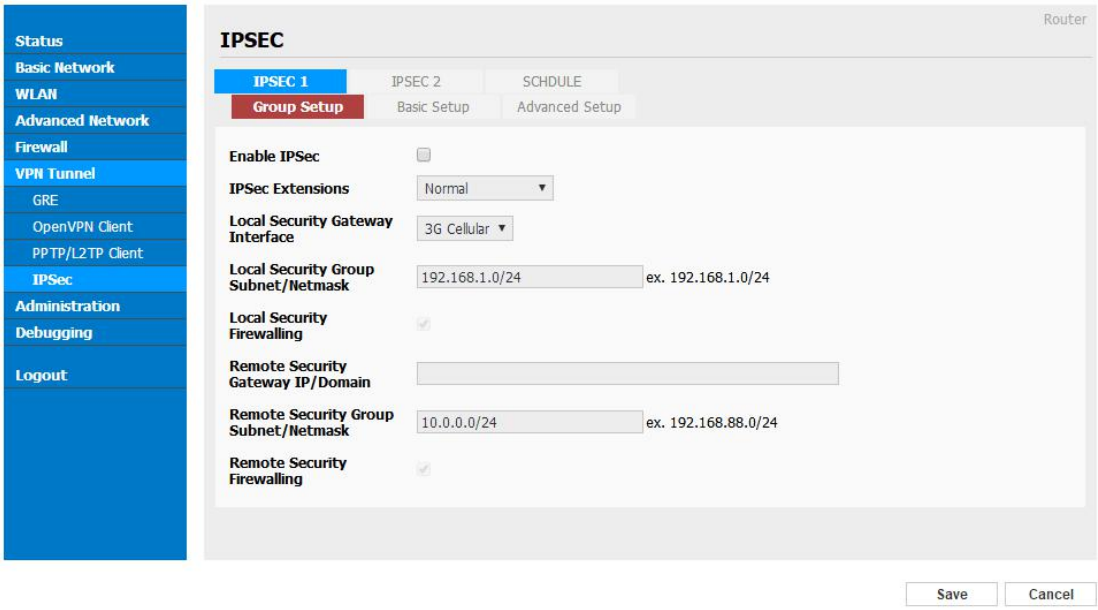
Table 3-20 “SCHEDULE” Instruction

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

3.6.4 IPSec Setting



3.5.3.1 IPSec Group Setup

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

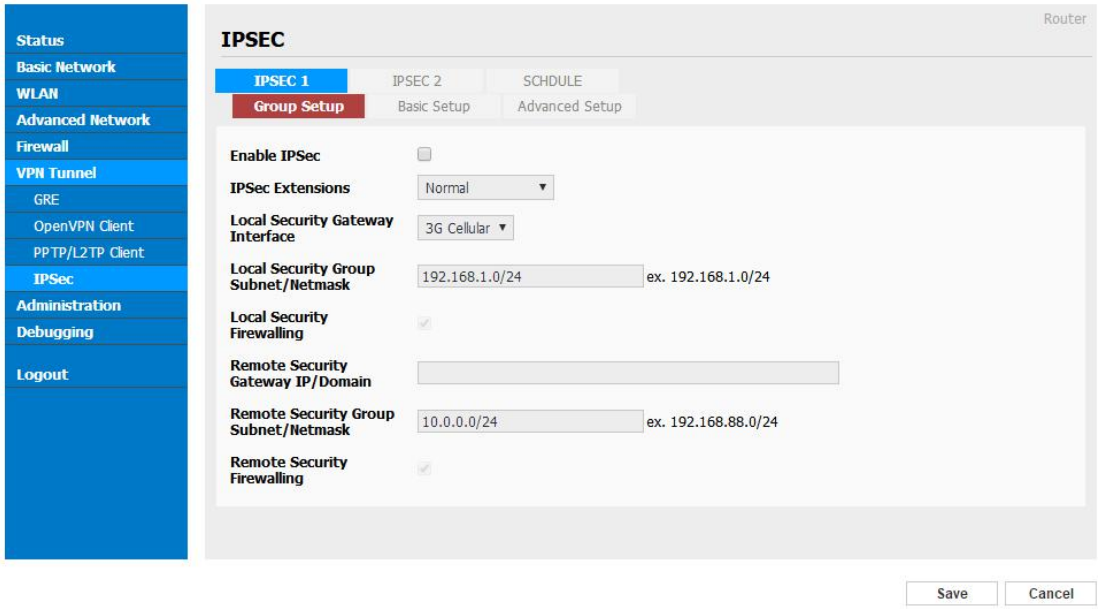


Table 3-21 " IPSec Group Setup" Instruction

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

3.5.3.2 IPSec Basic Setup

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

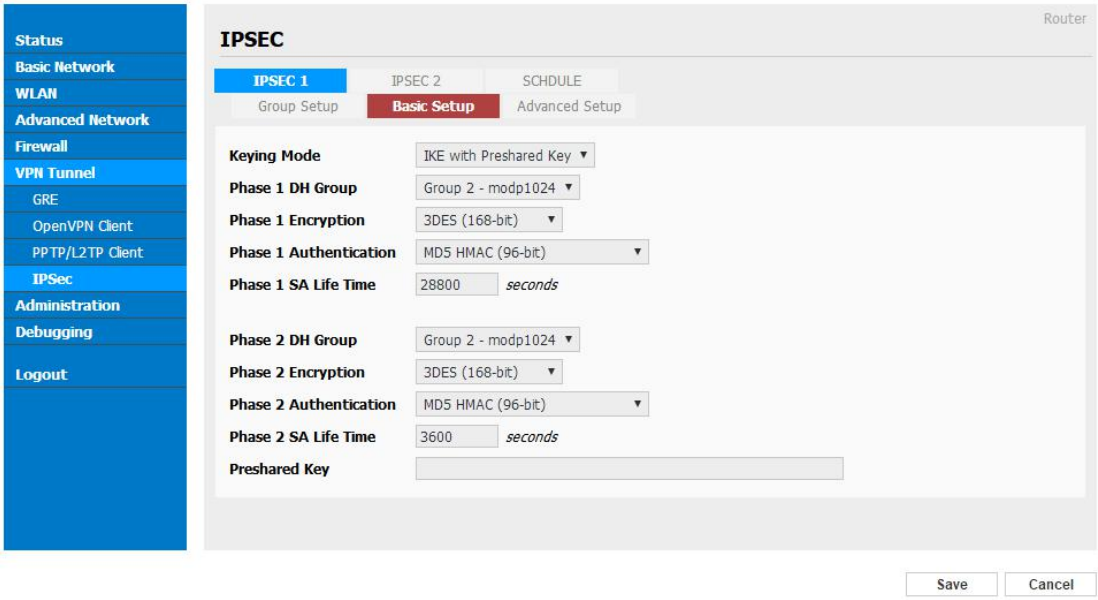


Table 3-22 " IPSec Basic Setup" Instruction

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

3.5.3.3 IPSec Advanced Setup

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

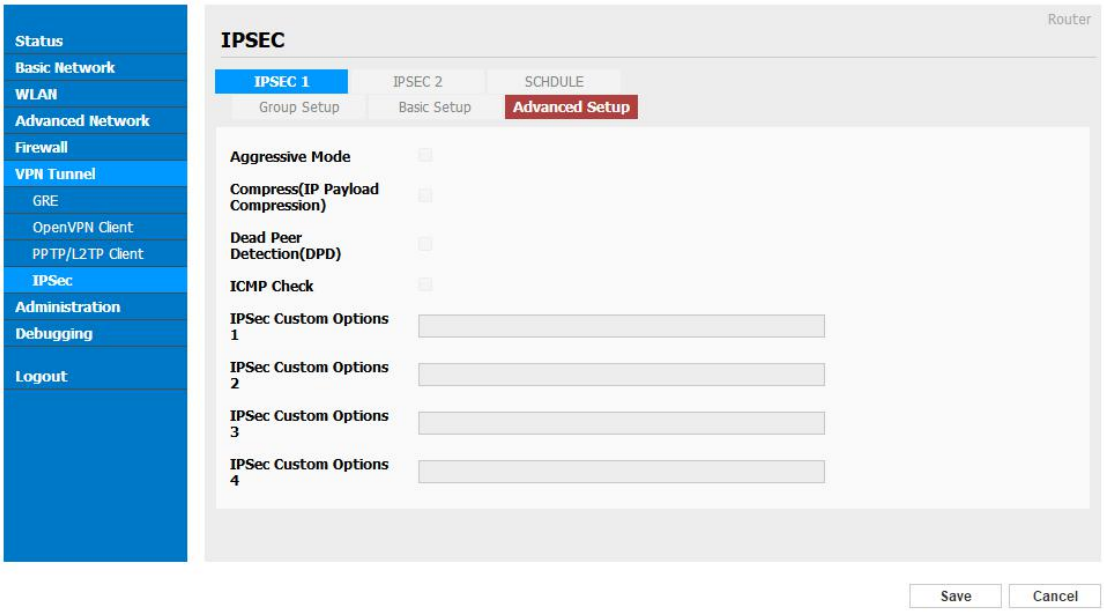


Table 3-23 " IPSec Advanced Setup" Instruction

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

3.7 Administration

3.7.1 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.

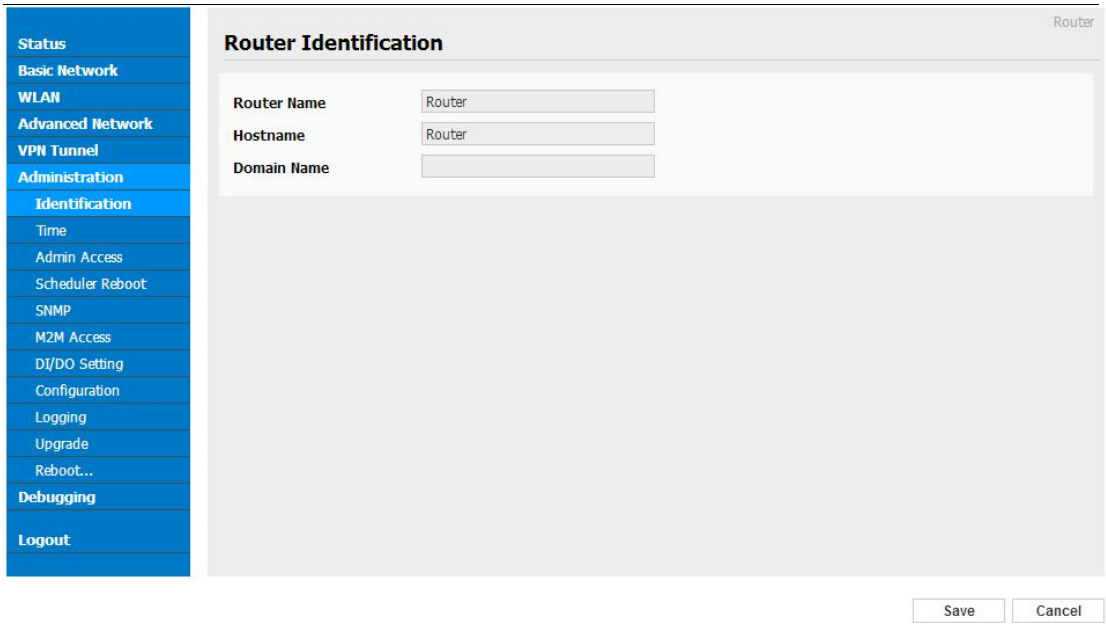


Figure 3-23 Router Identification GUI

Table 3-24 “Router Identification” Instruction

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

Step 2 Please click ”save” to finish

----End

3.7.2 Time Setting

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

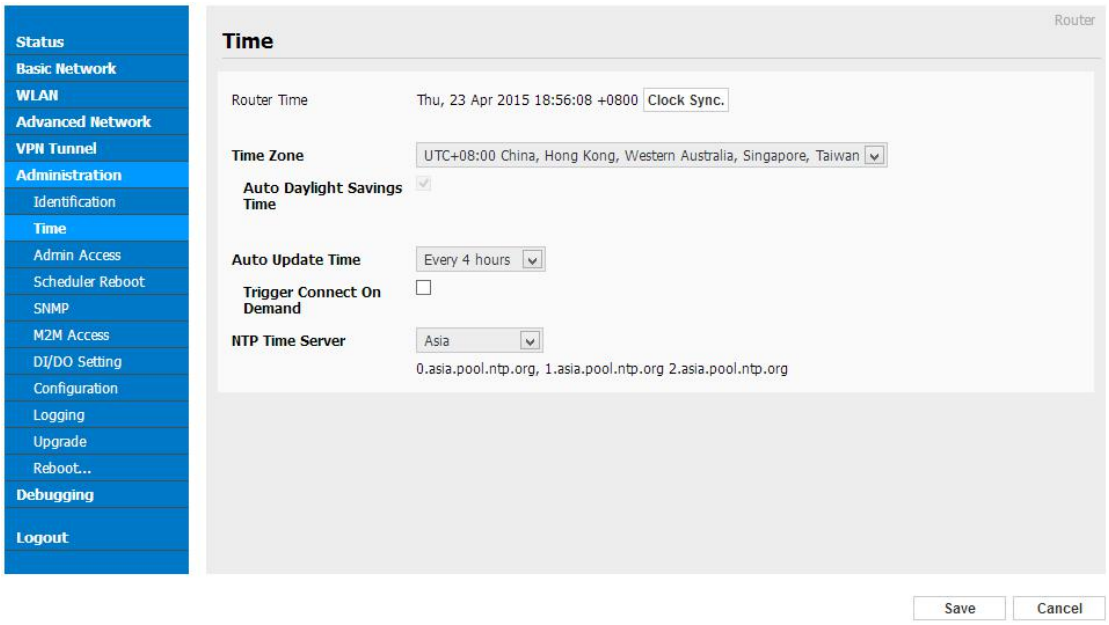


Figure 3-24 System Configuration GUI

CAUTION

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

Step 2 Please click “save to finish.

----End

3.7.3 Admin Access Setting

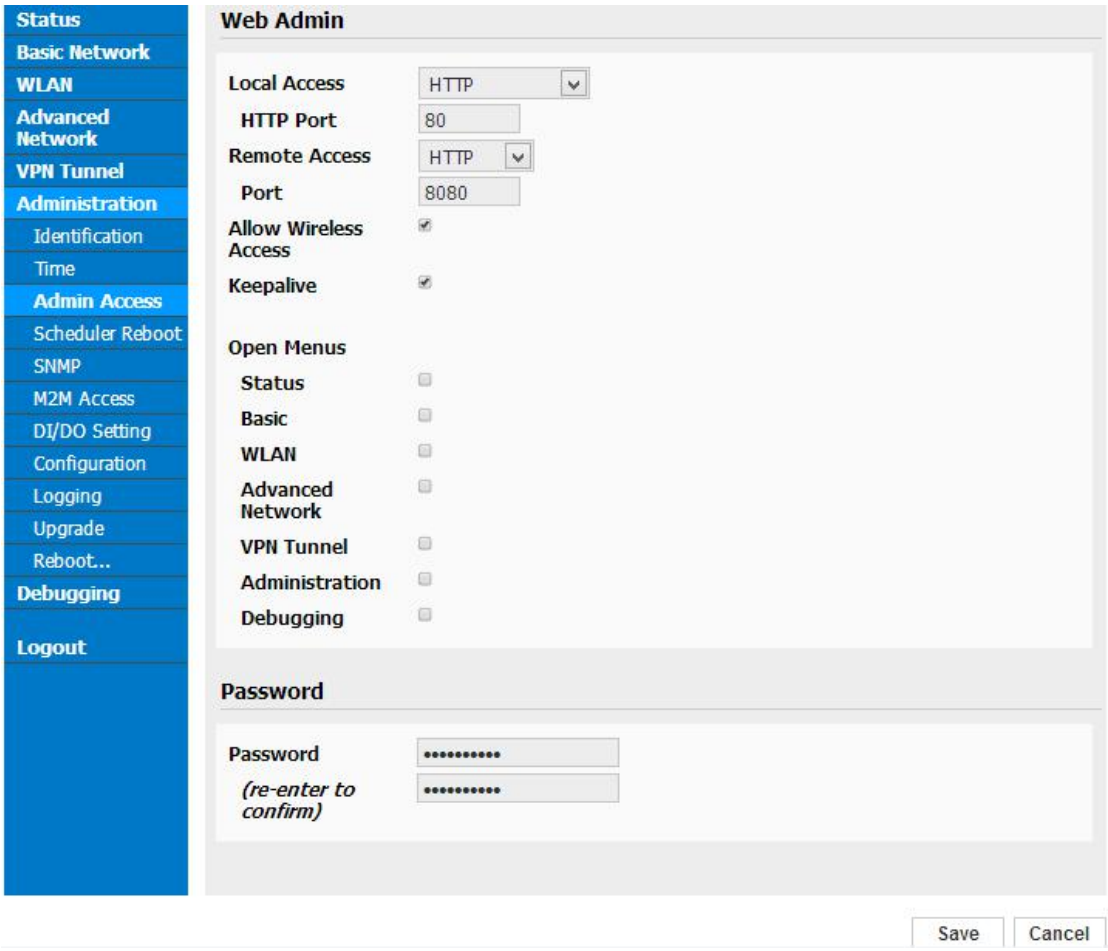
Step 1 Please click “Administrator>Admin” to check and modify relevant parameter.

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.

Figure 3-25 Admin Setting GUI

Step 2 Please click save iron to finish the setting

----End



3.7.4 Schedule Reboot Setting

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

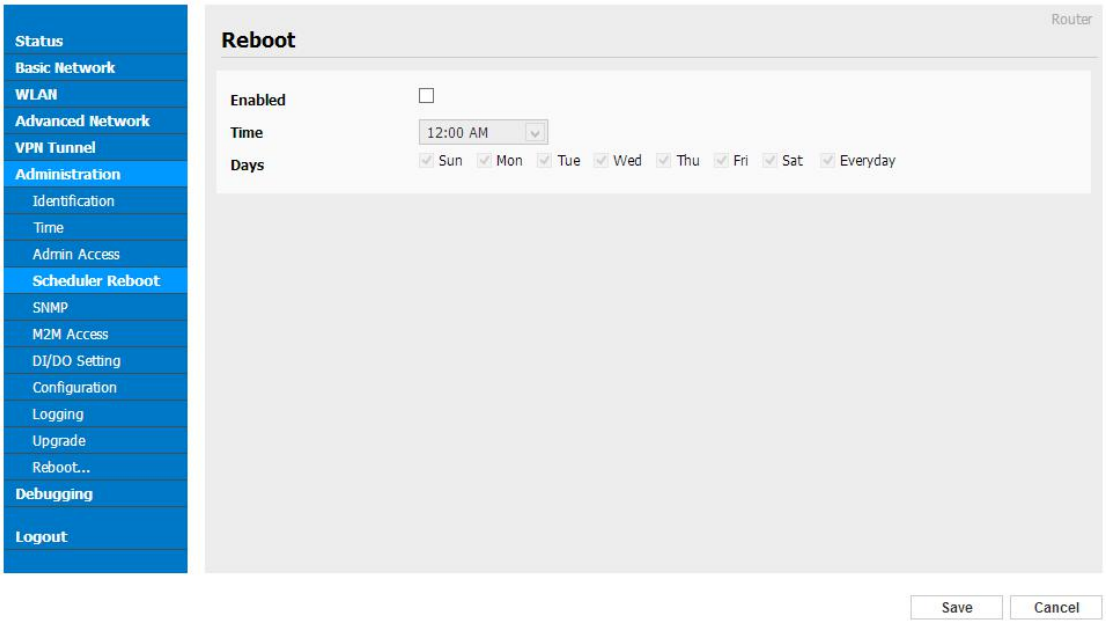


Figure 3-26 Scheduler Reboot Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.7.5 SNMP Setting

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

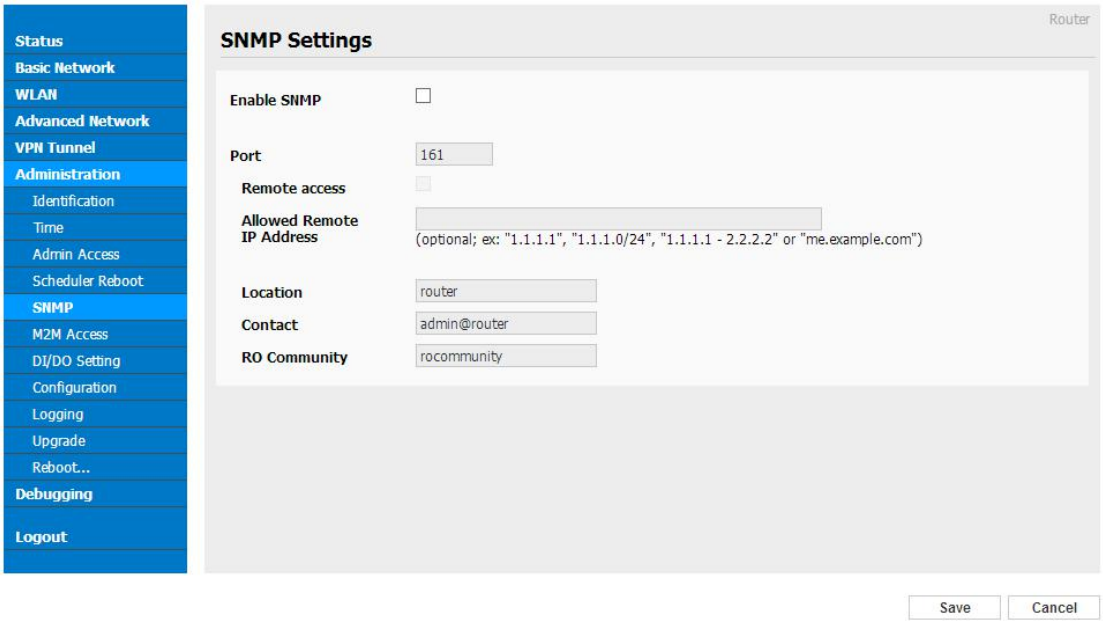


Figure 3-27 SNMP Setting GUI

Step 2 Please click save iron to finish the setting

----End

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

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

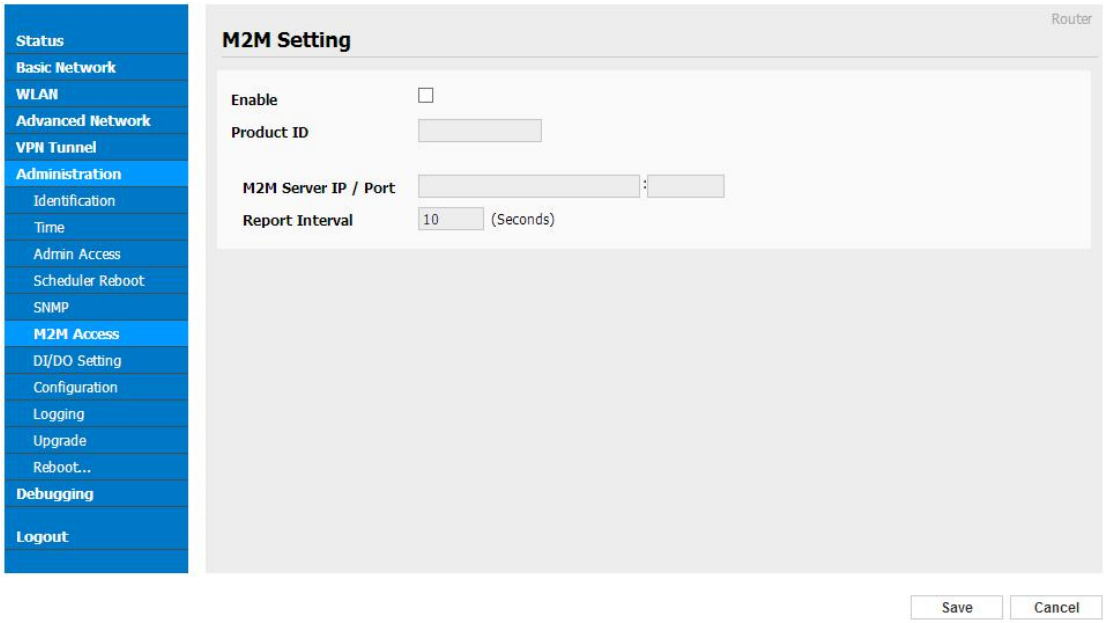


Figure 3-28 M2M Access Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.7.7 DI/DO Setting

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

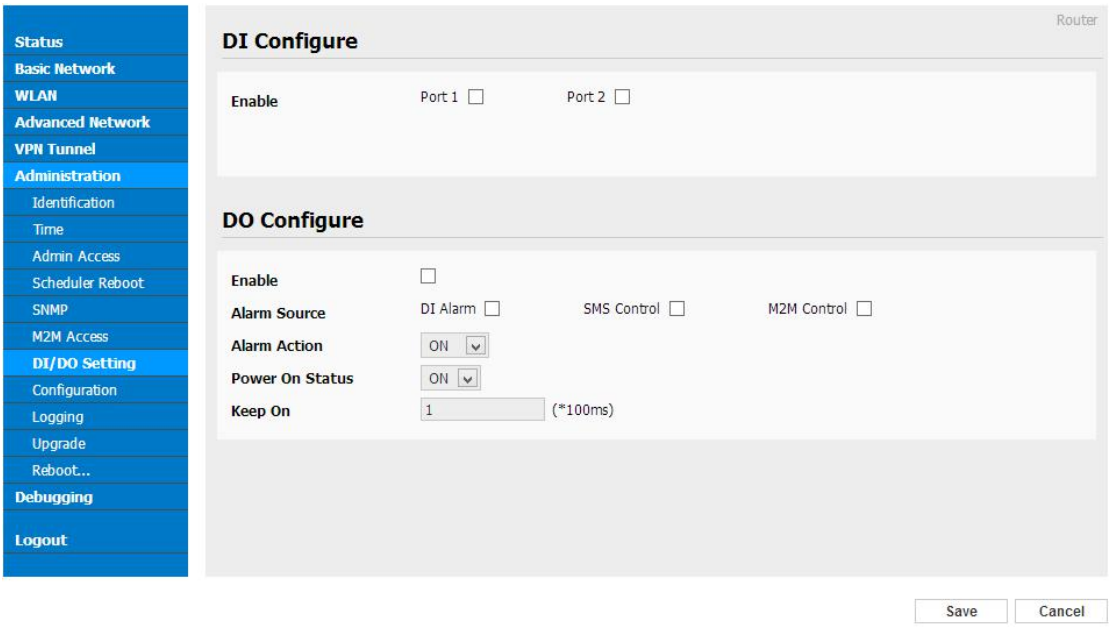


Figure 3-29 DI/DO Setting GUI

3.6.7.1 DI Configure

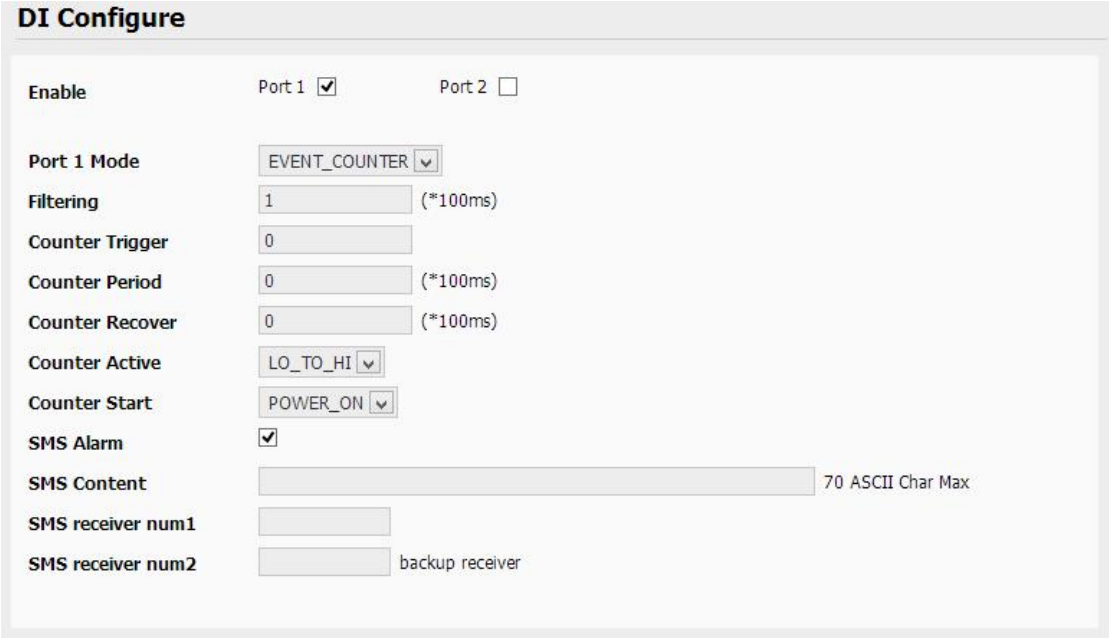


Table 3-25 "DI" Instruction

Parameter	Instruction
Enable	Enable DI. Port1 is for I/O1 and Port2 is I/O2. Both I/O1 and I/O2 are DI ports
Mode	Selected from OFF, ON and EVENT_COUNTER modes. OFF Mode: When I/O connects to GND, it will trigger alarm. ON Mode: When I/O does not connect to GND, it will trigger alarm. EVENT_COUNTER Model: Enter EVENT_COUNTER mode.
Filter	Software filtering is used to control switch bounces. Input (1~100)*100ms. Under OFF and ON modes, WL-G510 detects pulse signal and compares with first pulse shape and last pulse shape. If both are the same level, WL-G510 will trigger alarm. Under EVENT_COUNTER mode, if first pulse shape and last pulse shape are not the same level, WL-G510 will trigger alarm according to Counter Action setting.
Counter Trigger	Available when DI under Event Counter mode Input from 0 to 100. (0=will not trigger alarm) It will trigger alarm when counter reaches this value. After triggering alarm, DI will keep counting but no trigger alarm again.
Counter Period	It's a reachable IP address. Once the ICMP check is failed, GRE will be established again.
Counter Recover	it will re-count after counter trigger alarm. The value is 0~30000(*100ms). 0 means no counter.
Counter Action	HI_TO_LO and LO_TO_HI is available when DI under Event Counter mode. In Event Counter mode, the channel accepts limit or proximity

Parameter	Instruction
	switches and counts events according to the ON/OFF status. When LO_TO_HI is selected, the counter value increase when the attached switch is pushed. When HI_TO_LO is selected, the counter value increases when the switch is pushed and released.
Counter Start	Available when DI under EVENT_COUNTER mode. Start counting when enable this feature.
SMS Alarm	The alarm SMS will send to specified phone group. Each phone group include up to 2 phone numbers.
SMS Content	70 ASCII Char Max
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 2 Please click ”save” to finish.

3.6.7.1 DO Configure

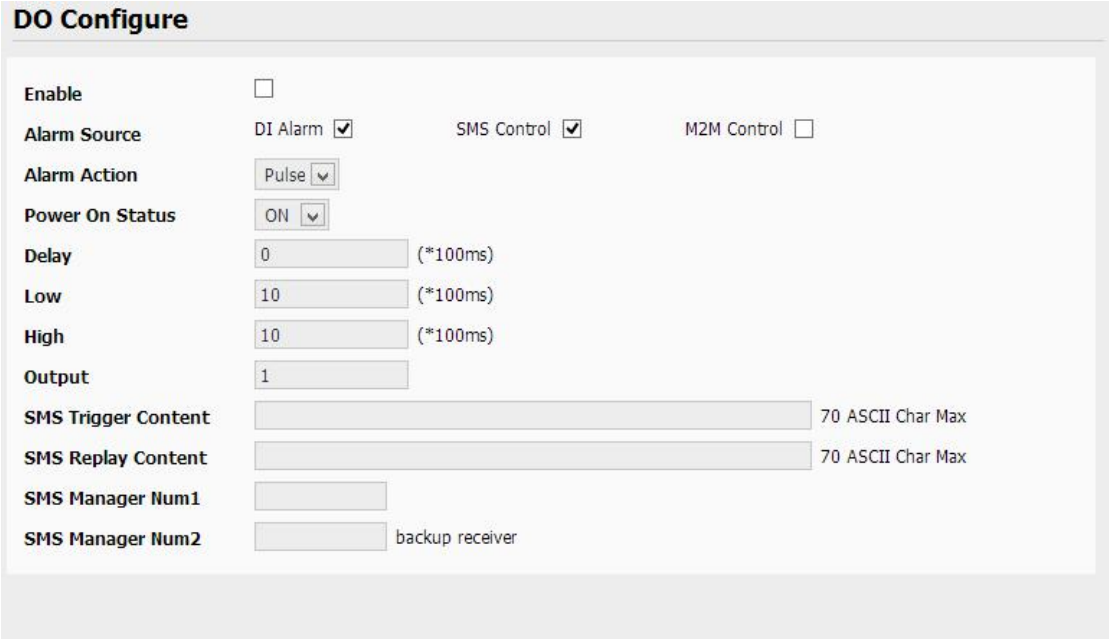


Table 3-26 “DO” Instruction

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

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

Step 3 Please click "save" to finish.

3.7.8 Configuration Setting

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

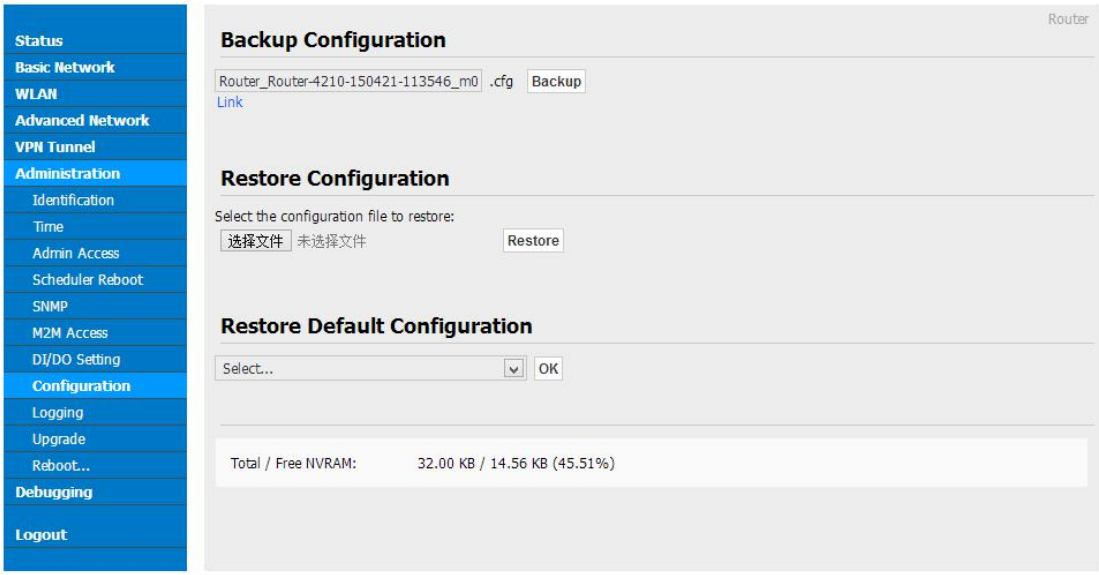


Figure 3-30 Backup and Restore Configuration GUI

CAUTION

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

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

----End

3.7.9 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).

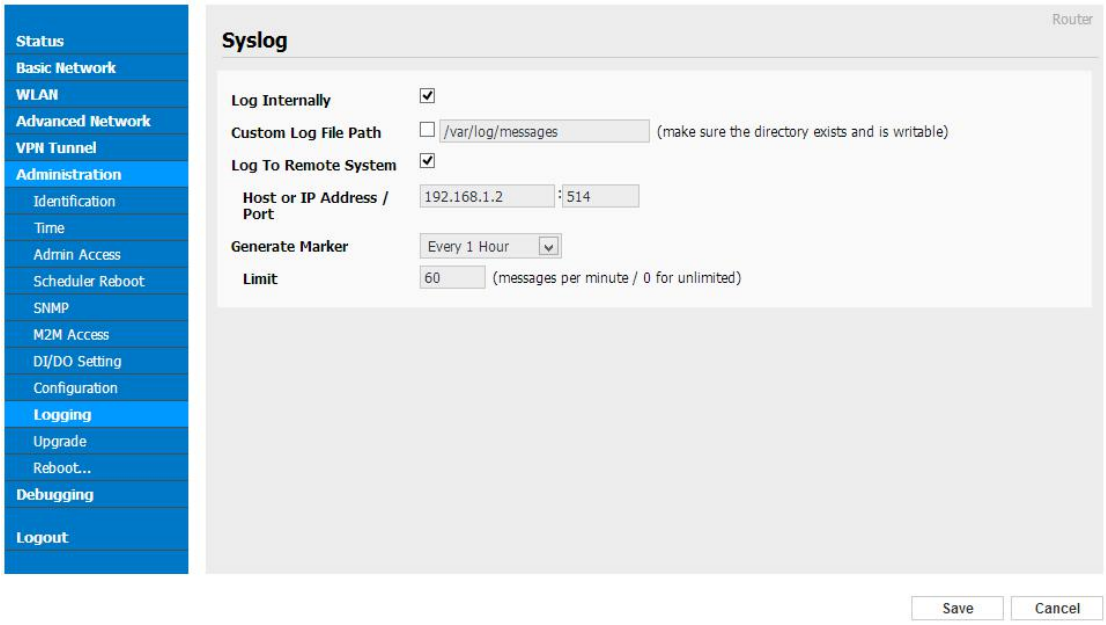


Figure 3-31 System log Setting GUI

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

----End

3.7.10 Firmware upgrade

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

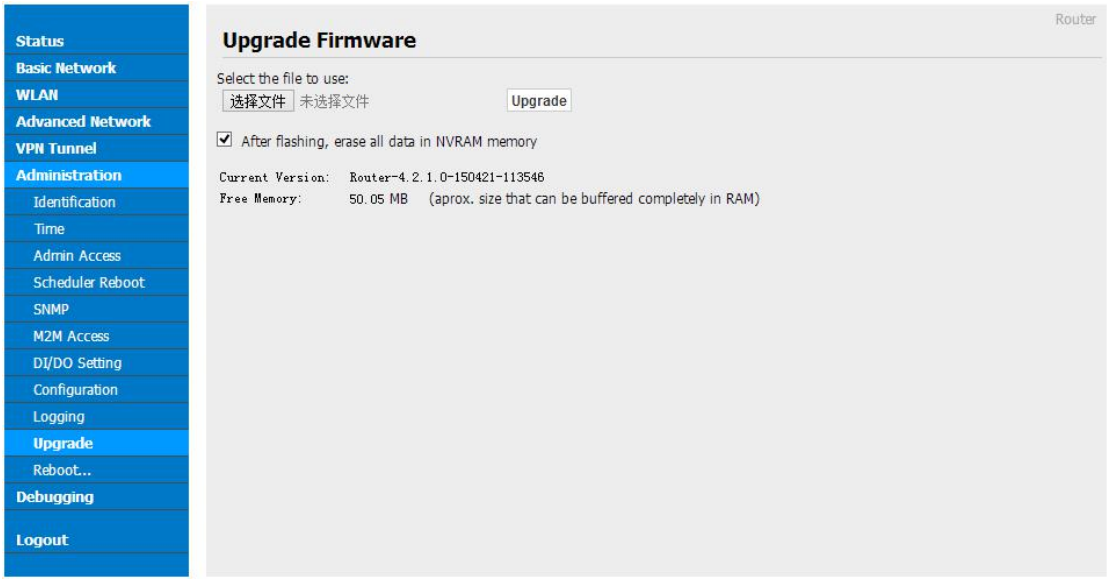


Figure 3-32 Firmware Upgrade GUI

NOTE

When upgrading, please don’t cut off the power.

3.7.11 System Reboot

Step 1 Please click “Administrator>Reboot” to restart the router. System will popup dialog to remind “Yes” or “NO” before the next step.

Step 2 If choose “yes”, the system will restart, all relevant update configuration will be effective after reboot.

----End

3.8 Debugging Setting

3.8.1 Logs Setting

Step 1 Please click “Debugging>Logs” to check and modify relevant parameter.

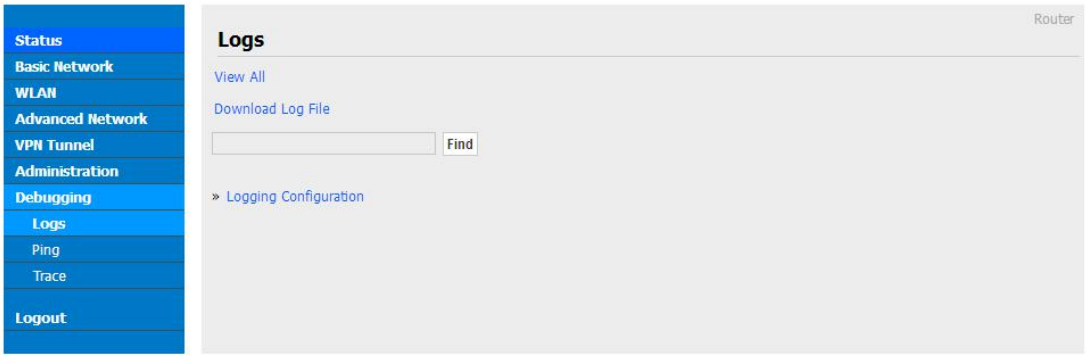


Figure 3-33 Logs GUI

----End

3.8.2 Ping Setting

Step 1 Please click “Debugging>Ping” to check and modify relevant parameter.

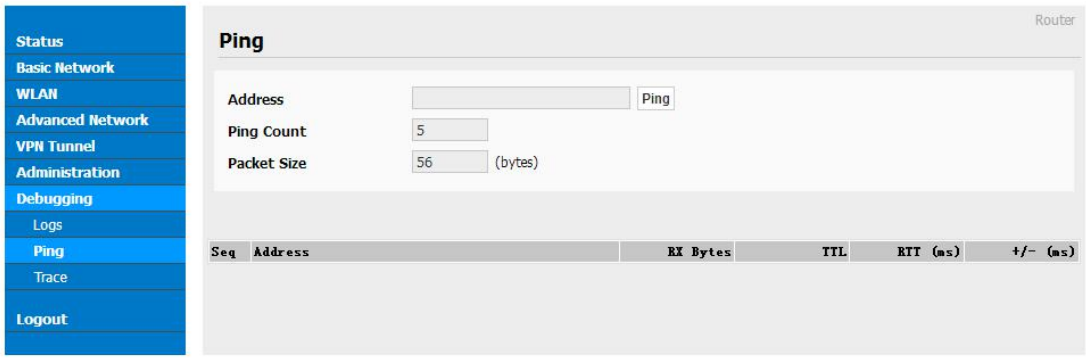


Figure 3-34 Ping GUI

----End

3.8.3 Trace Setting

Step 1 Please click “Debugging>Trace” to check and modify relevant parameter.

Figure 3-35 Trace GUI

----End

3.9 “Reset” Button for Restore Factory Setting

If you couldn’t enter web interface for other reasons, you can also use this way. “Reset” button is near to Console port in WL-G510 panel, This button can be used when the router is in use or when the router is turned on.

Press the “RST” button and keep more than 8 seconds till the NET light stopping blink. The system will be reverted to factory.

Table 3-27 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.

3.10 Appendix (For advanced optional features only)

3.10.1 GPS Setting

Step 1 Please click “Advanced Network> GPS” to view or modify the relevant parameter.

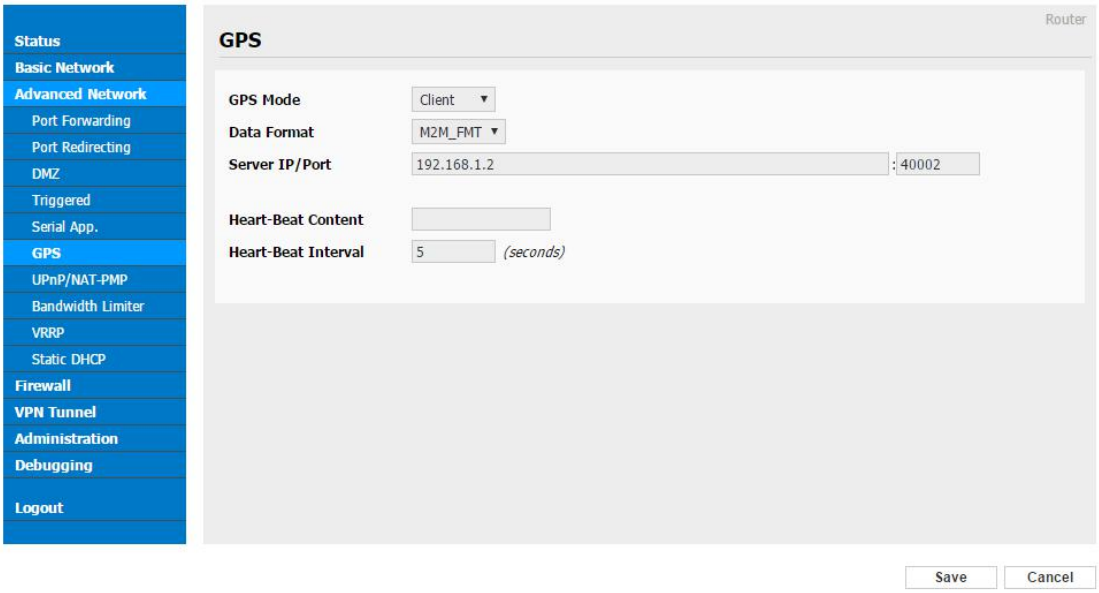


Figure 3-36 GPS Setting GUI

Table 3-28 “GPS” Instruction

parameter	Instruction
GPS Mode	Enable/Diable
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 itnto GPS data.
Interval	GPS data transmit as the interval time.

Step 2 Please click ”save” to finish

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.

3.10.2 Captive Portal Setting

Step 1 Please click “Advanced Network> Captive Portal” to check or modify the relevant parameter.

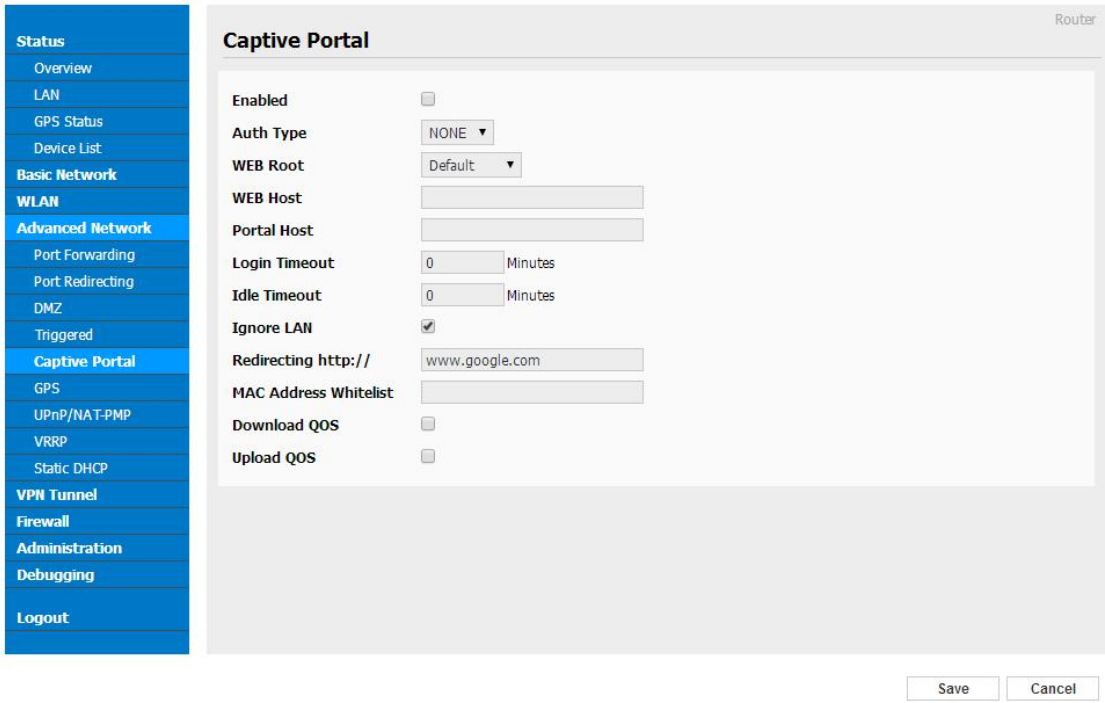


Figure 3-37 Captive Portal Setting GUI

Table 3-29 "Serial App" 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.

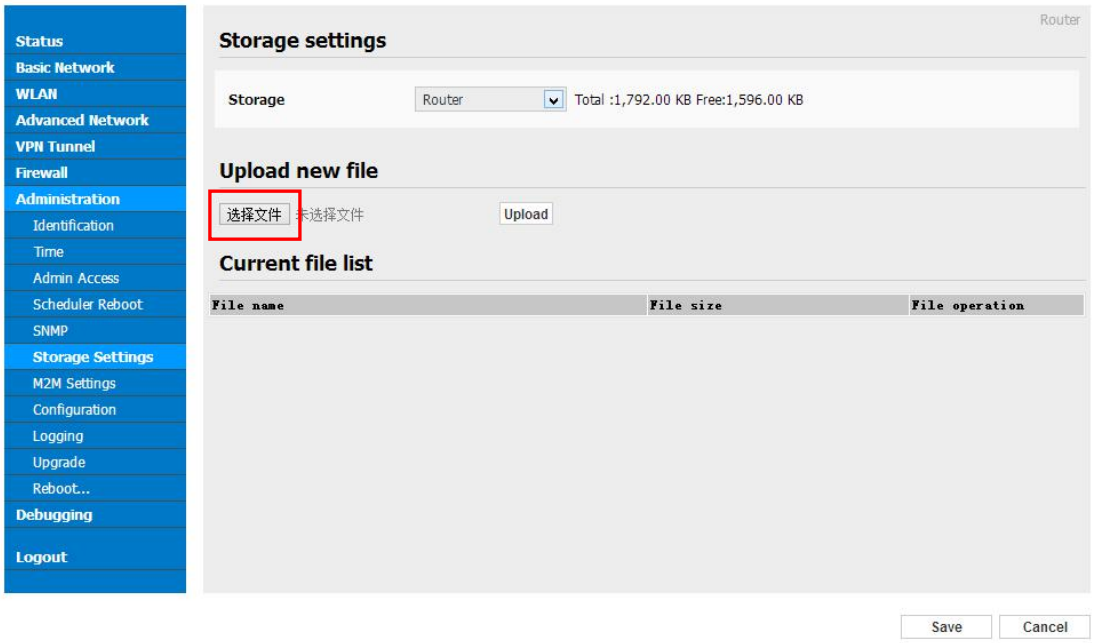
Parameter	Instruction
MAC Whitelist	No captive portal page for Wi-Fi device.
Download QoS	Enable to apply the Download and Upload per user limits.
Upload Qos	Maximum download speed available to each user.

NOTE

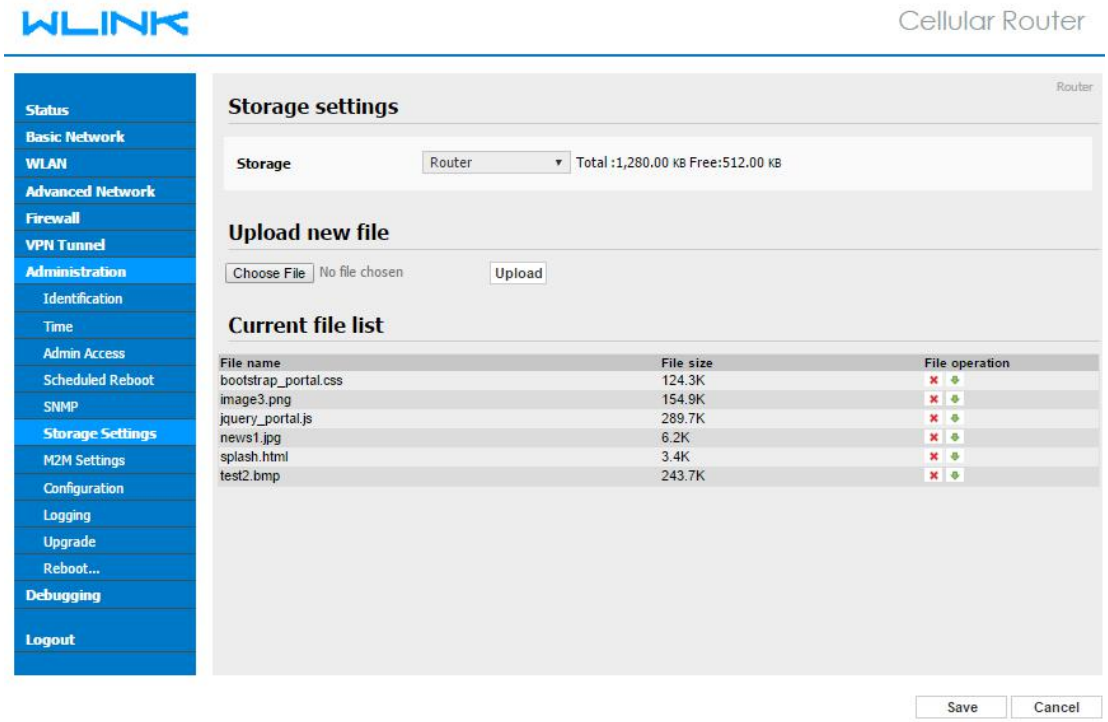
1）Upload Portal file and Splash.html by local

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.

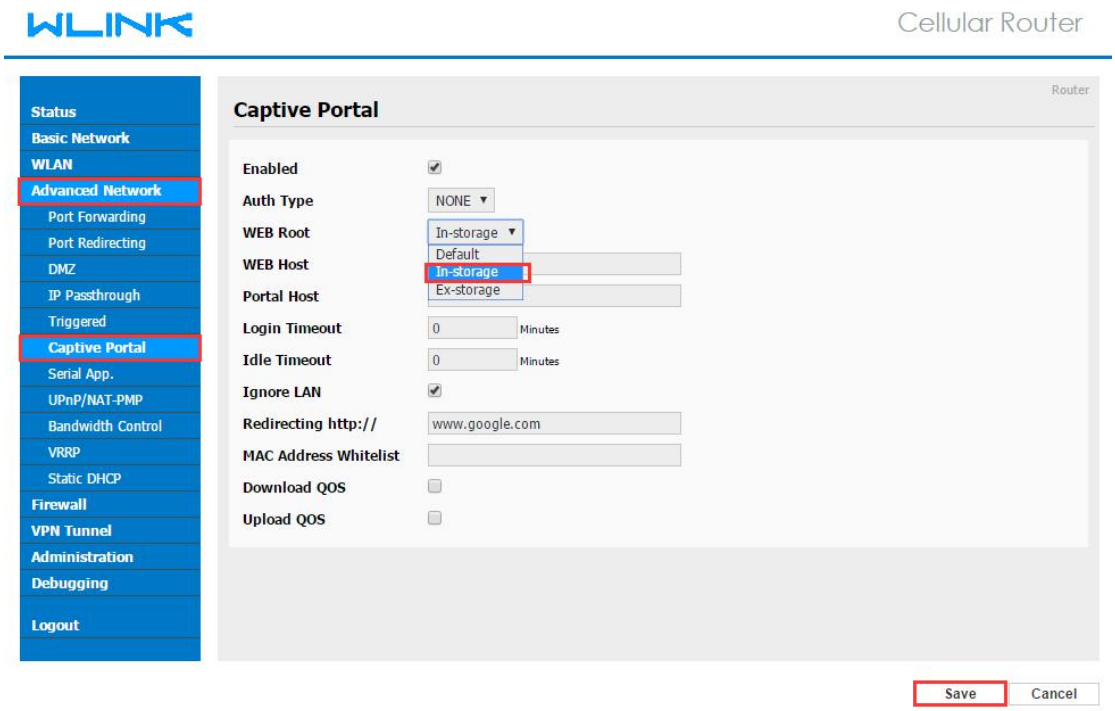



```
<!-- <hr> -->

<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> -->
```

---End

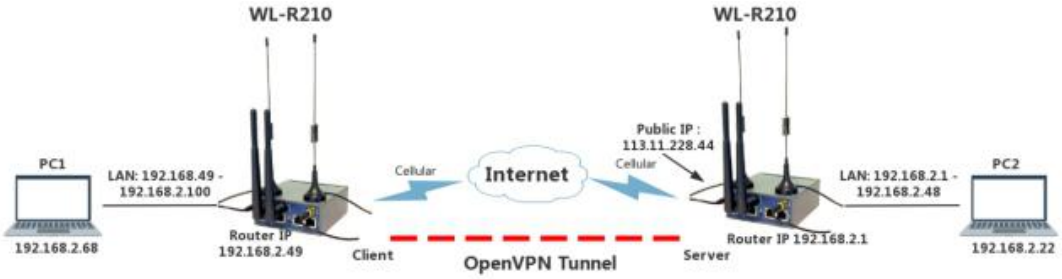
2）Modify portal file storage path

Modify portal file storage for In-storage as below.

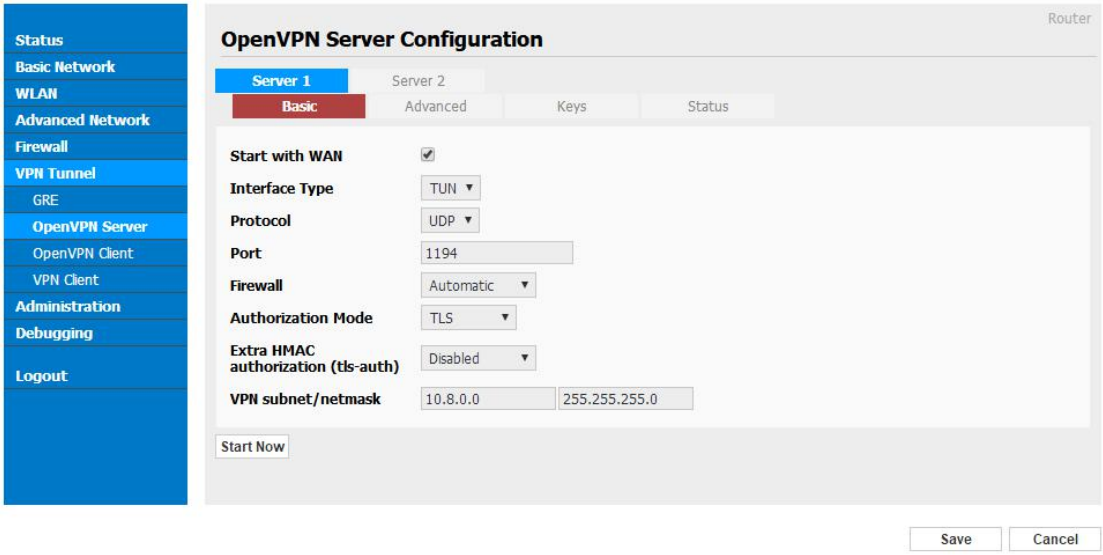


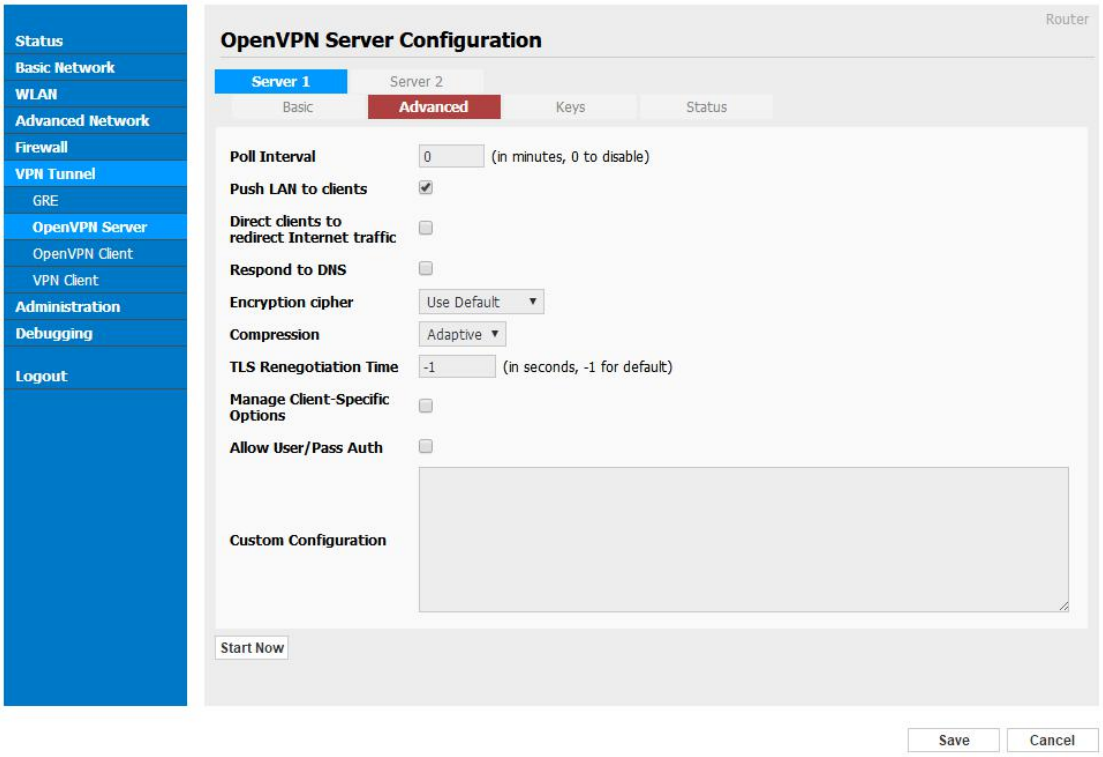
3.10.3 OpenVPN Demo (TAP Mode)

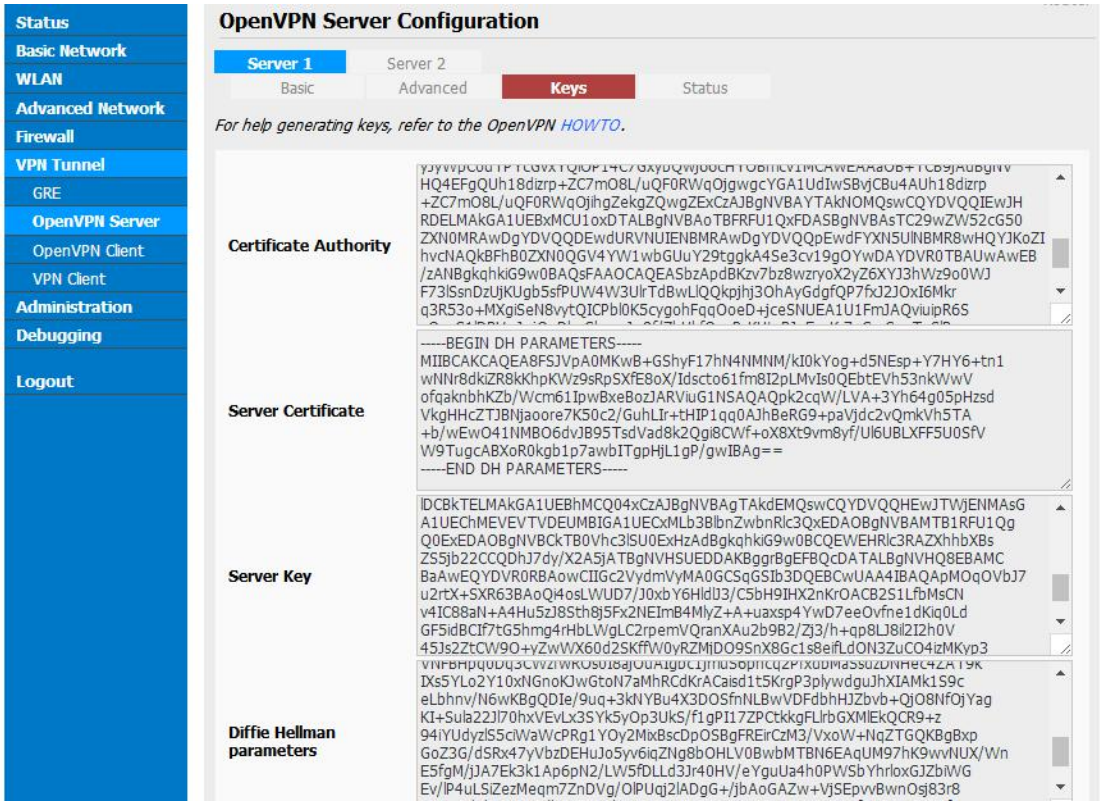
1) Network topology



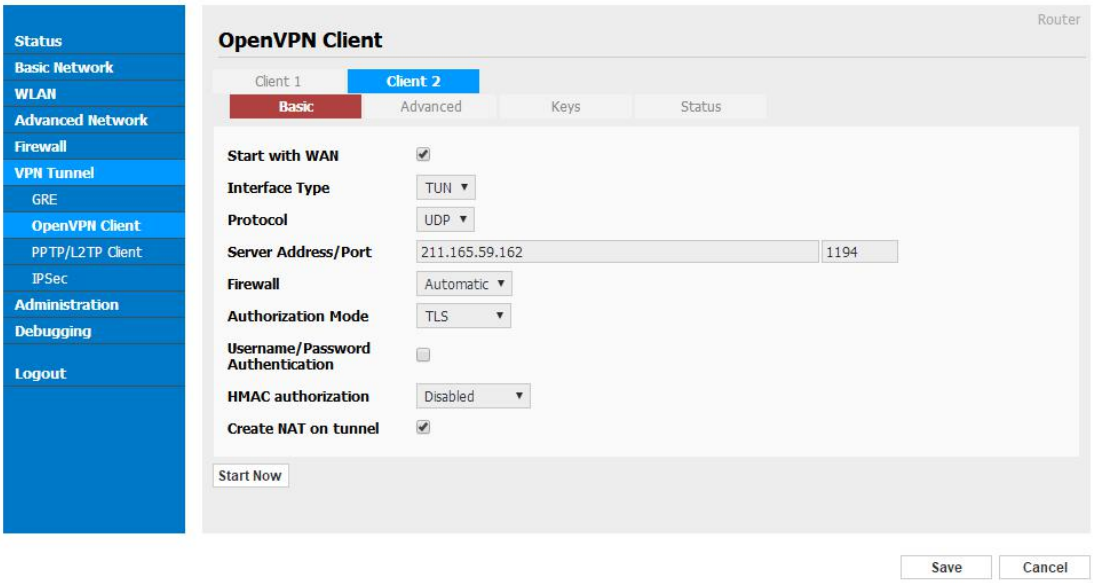
2) OpenVPN Server Config Demo

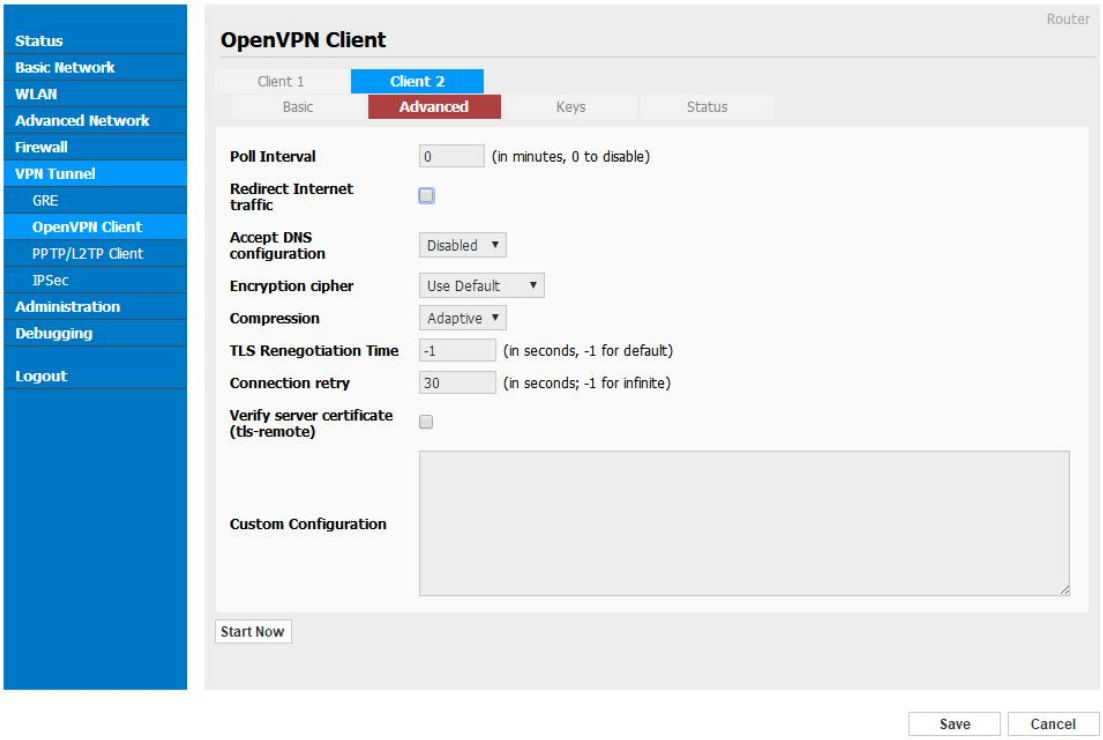

Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Server
OpenVPN Client
VPN Client
Administration
Debugging
Logout
Router
OpenVPN Server Configuration
Server 1
Server 2
Basic
Advanced
Keys
Status
Start with WAN
Interface Type
TUN
Protocol
UDP
Port
1194
Firewall
Automatic
Authorization Mode
TLS
Extra HMAC authorization (tls-auth)
Disabled
VPN subnet/netmask
10.8.0.0
255.255.255.0
Start Now
Save
Cancel

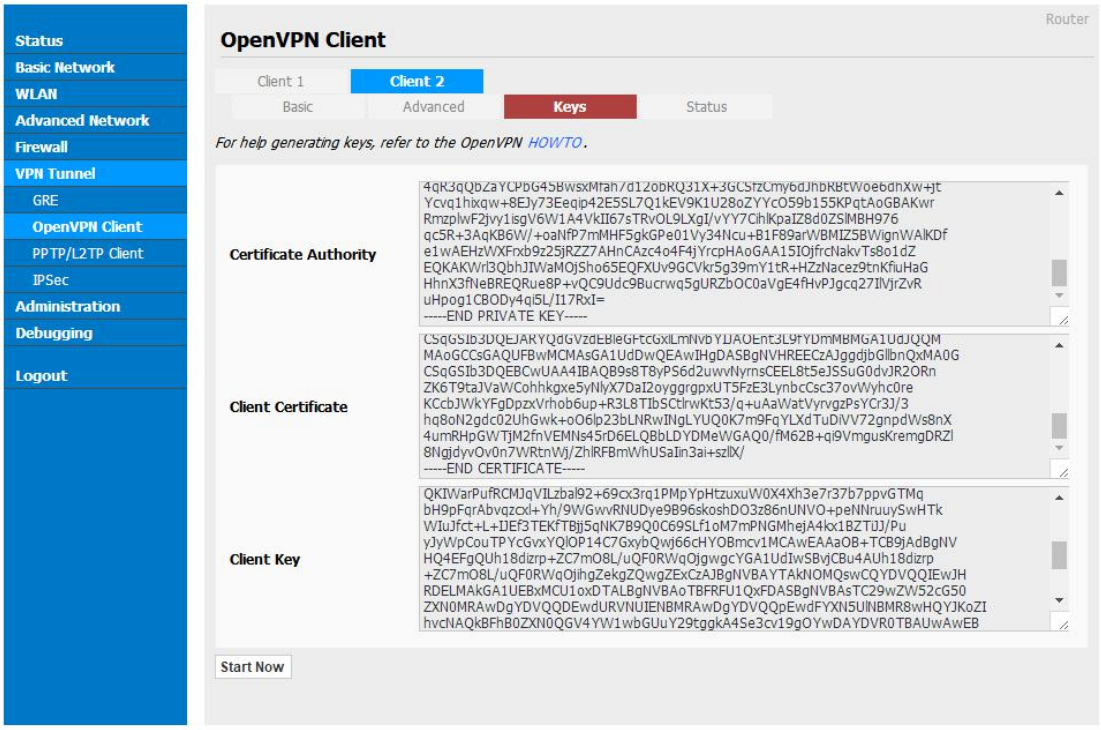

Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Server
OpenVPN Client
VPN Client
Administration
Debugging
Logout
Router
OpenVPN Server Configuration
Server 1
Server 2
Basic
Advanced
Keys
Status
Poll Interval
0
(in minutes, 0 to disable)
Push LAN to clients
Direct clients to redirect Internet traffic
Respond to DNS
Encryption cipher
Use Default
Compression
Adaptive
TLS Renegotiation Time
-1
(in seconds, -1 for default)
Manage Client-Specific Options
Allow User/Pass Auth
Custom Configuration
Start Now
Save
Cancel



3) OpenVPN Client Config Demo




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


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
Debugging
Logout
Router
OpenVPN Client
Client 1
Client 2
Basic
Advanced
Keys
Status
For help generating keys, refer to the OpenVPN HOWTO.
Certificate Authority
Client Certificate
Client Key
Start Now


Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
OpenVPN Server
VPN Client
IPSec
Administration
Debugging
Logout
Router
OpenVPN Client
Client 1
Client 2
Basic
Advanced
Keys
Status
Data current as of Sat Jan 1 09:06:05 2000.
General Statistics
Name
Value
TUN/TAP read bytes 0
TUN/TAP write bytes 0
TCP/UDP read bytes 0
TCP/UDP write bytes 70
Auth read bytes 0
pre-compress bytes 0
post-compress bytes 0
pre-decompress bytes 0
post-decompress bytes 0
Refresh Status
Stop Now
Save
Cancel