WLINK

User Manual

---Apply to WL-R210 Series Industrial 4G/3G Router

V2.3
http://www.wlink-tech.com
Jan, 2020

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：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 Product Introduction

1.1 Product overview

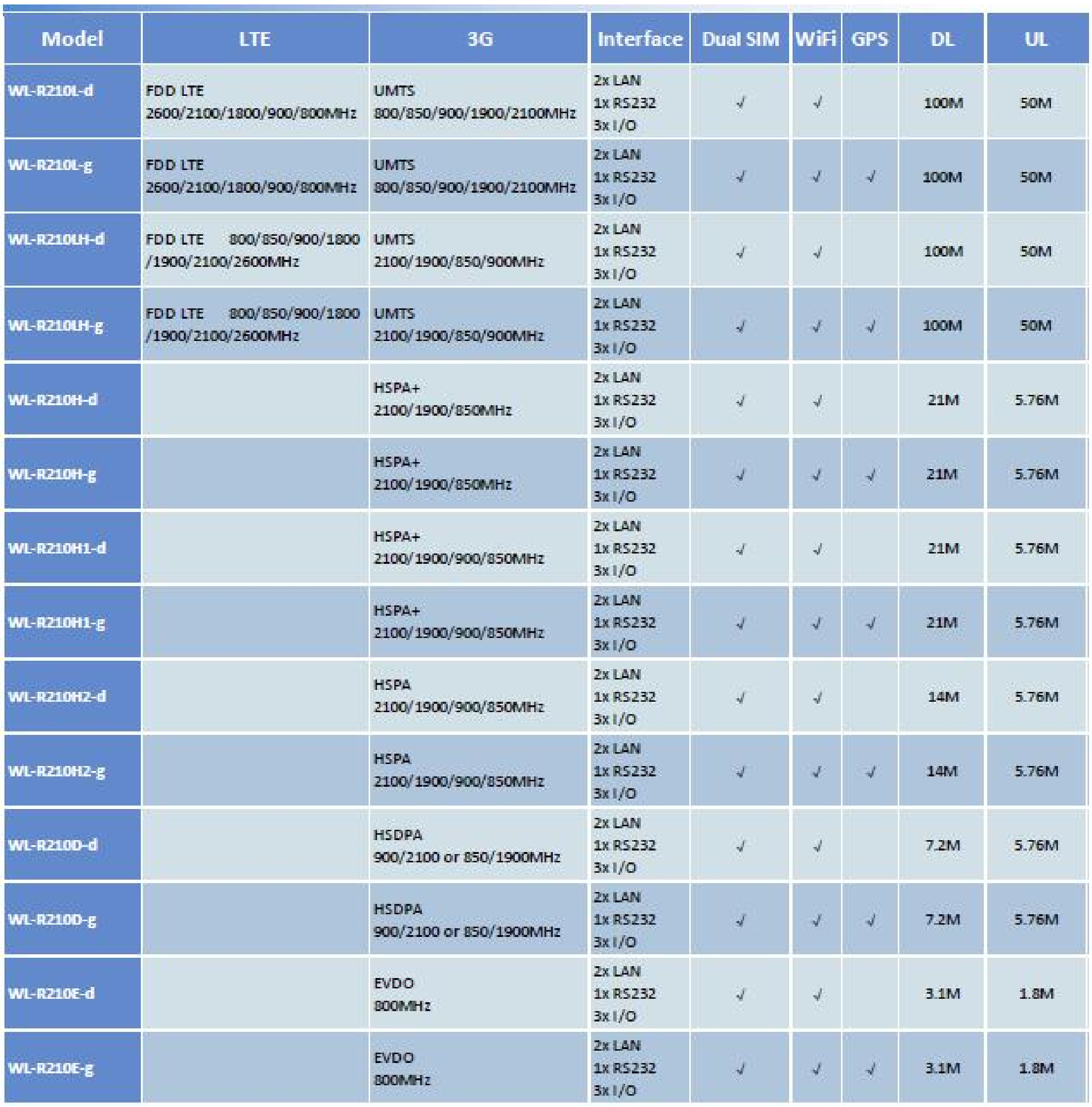
WLINK industrial Router is based on industrial grade design, built-in high-powered 32bit MIPS processor, and multi-band 4G/3G communication module, support WCDMA,HSPA+, 4G FDD/TDD etc., provide quick and convenient internet access or private network transmission to customer, provide wire-line network or wireless WLAN share high speed access, meanwhile, customized high security VPN (Open VPN, IPSec, SSL), to construct safe channel, widely used in financial, electric power, environment, oil, transportation, security, etc..

WLINK industrial series router provide GUI, optional CLI configuration interface, customer can configure by IE explore or Telnet/SSH, various configuration method, concise and friendly interface make configuring and managing of all router terminal easier, meanwhile, WLINK provide M2M terminal management platform to manage all router terminal with remote management. User can monitor all terminals which connected to platform successfully by this platform, provide long-distance control, parameter configuration, and long-distance upgrade service.

1.2 Model introduction

WLINK industrial grade router series have single module / single SIM card, single module / double SIM card, double module / double SIM card design, support multi-band frequency WCDMA, HSPA+, 4G FDD/TDD etc., and downward compatibility to GPRS、EDGE、CDMA 1x, etc., optional GPS module Expansion positioning function, to suit different requirement and different network environment of different operators. Our Router series have many model for option, below is the product model indications in detail, for more optional models, please consult local distributors /resellers.

Table 1-1 Router partial model table



Model	LTE	3G	Interface	Dual SIM	WiFi	GPS	DL	UL
WL-R210L-d	FDD LTE 2600/2100/1800/900/800MHz	UMTS 800/850/900/1900/2100MHz	2x LAN 1x RS232 3x I/O	√	√		100M	50M
WL-R210L-g	FDD LTE 2600/2100/1800/900/800MHz	UMTS 800/850/900/1900/2100MHz	2x LAN 1x RS232 3x I/O	√	√	√	100M	50M
WL-R210LH-d	FDD LTE 800/850/900/1800 /1900/2100/2600MHz	UMTS 2100/1900/850/900MHz	2x LAN 1x RS232 3x I/O	√	√		100M	50M
WL-R210LH-g	FDD LTE 800/850/900/1800 /1900/2100/2600MHz	UMTS 2100/1900/850/900MHz	2x LAN 1x RS232 3x I/O	√	√	√	100M	50M
WL-R210H-d		HSPA+ 2100/1900/850MHz	2x LAN 1x RS232 3x I/O	√	√		21M	5.76M
WL-R210H-g		HSPA+ 2100/1900/850MHz	2x LAN 1x RS232 3x I/O	√	√	√	21M	5.76M
WL-R210H1-d		HSPA+ 2100/1900/900/850MHz	2x LAN 1x RS232 3x I/O	√	√		21M	5.76M
WL-R210H1-g		HSPA+ 2100/1900/900/850MHz	2x LAN 1x RS232 3x I/O	√	√	√	21M	5.76M
WL-R210H2-d		HSPA 2100/1900/900/850MHz	2x LAN 1x RS232 3x I/O	√	√		14M	5.76M
WL-R210H2-g		HSPA 2100/1900/900/850MHz	2x LAN 1x RS232 3x I/O	√	√	√	14M	5.76M
WL-R210D-d		HSDPA 900/2100 or 850/1900MHz	2x LAN 1x RS232 3x I/O	√	√		7.2M	5.76M
WL-R210D-g		HSDPA 900/2100 or 850/1900MHz	2x LAN 1x RS232 3x I/O	√	√	√	7.2M	5.76M
WL-R210E-d		EVDO 800MHz	2x LAN 1x RS232 3x I/O	√	√		3.1M	1.8M
WL-R210E-g		EVDO 800MHz	2x LAN 1x RS232 3x I/O	√	√	√	3.1M	1.8M

1.3 Product Appearance

Table 1-2 WLINK Router Appearance

Series	R100	R200	R210	R520
Appearance				
Ports	1*LAN 1*RS232	2*LAN/ 1*LAN+ 1*WAN GPS or WLAN(11n 1T1R)	2*LAN(Default) +Dual SIM GPS, WLAN Optional	1*WAN + 4*LAN + single module/dual SIM, dual module/dual SIM
Product category	Single port router	Dual port Wi-Fi router	Multi-port Wi-Fi router	Multi-functional Wi-Fi router

1.4 Typical Application Diagram

WLINK 4G/3G Router are widely used in Telecom, economic, advertisement, traffic, environment protection business area.

For example, in economic area, WL-R210 Series Router connect server by IPSec & GRE to ensure data security, tiny design makes it easily installed into ATM machine. All these technology ensure safe and reliable data transmission, and minimize the probability of network disconnection, and maximize the usability of economic business like ATM, POS .etc.

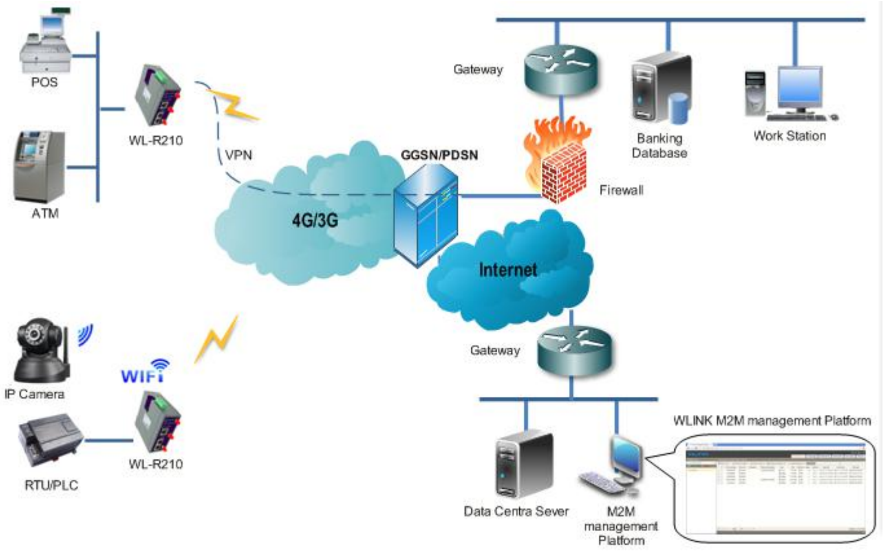


Figure 1-1 Network Topology

1.5 Features

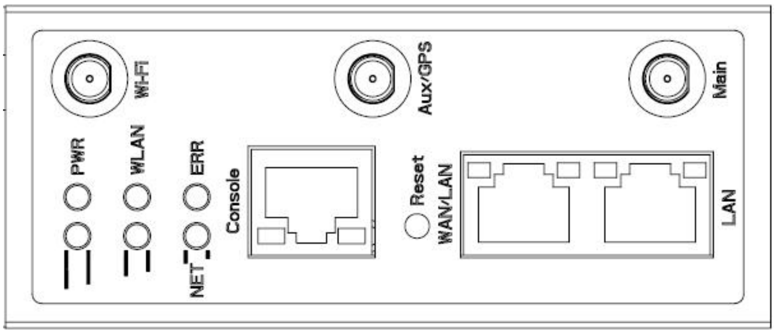
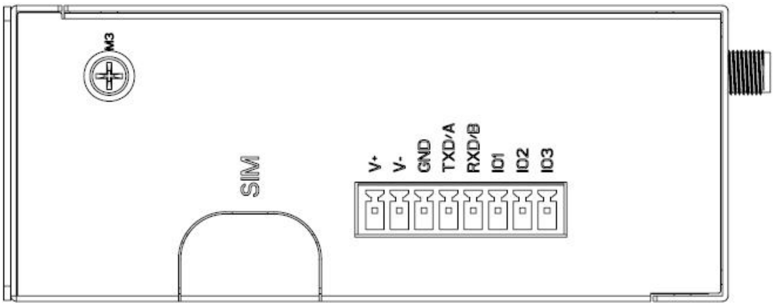
- Various cellular module optional, LTE/HSPA+/EVDO/CDMA2000 optional
- Support IEEE802.11b/g/n Wi-Fi AP function, extended support to Wi-Fi terminal, WDS bridging, support WEP, WPA/WPA2 Personal/Enterprise, TKIP/AES, etc., Authenticated encryption mode
- Support virtual data and private network（APN/VPDN）
- Optional support RS-232/RS-485 interface data transparent transmission and protocol conversion
- Support on-demand dialing, include timing on/off-line, voice or SMS control on/off-line, data trigger online or link idle offline
- Support TCP/IP protocol stack, support Telnet, HTTP, SNMP, PPP, PPPoE, etc., network protocol
- Support VPN Client（PPTP, L2TP）,optional support Open VPN, IPSec, HTTPs, SSH, etc. advanced VPN function
- Provide friendly user interface, use normal web internet explorer to easily configure and manage, long-distance configure Telnet/SSH + CLI
- Optional IPv6 protocol stack
- Optional support M2M terminal management platform
- WDT watchdog design, keep system stable
- Customization as per customer’s demand
- Protection level IP20

2 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.

2.1 Panel

Table 2-1 WL-R210 Structure

WLINK Tech.	R210 series
Front	 Wi-Fi Aux/GPS Main PWR WLAN ERR NET Console Reset WAN/LAN LAN
Top	 M3 SIM V+ V- GND TXD/A RXD/B IO1 IO2 IO3

NOTE

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

Table 2-2 Router Interface

Port	Instruction	Remark
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection.	
Main	3G/LTE antenna, SMA connector, 50Ω.	
Aux/GPS	Optional for LTE MIMO antenna or GPS antenna ,SMA connector, 50Ω.	Optional
Wi-Fi	Wi-Fi antenna, SMA connector,	Optional
LAN	10/100Base-TX，MDI/MDIX self-adaption.	
WAN/LAN	10/100Base-TX，MDI/MDIX self-adaption.	Default as LAN
Reset	Reset button,(press on button at least 5 seconds)	
PWR	Power connector	+7.5～32V DC
I/O	1/O 1 and 2 is digital input, and I/O 3 is digital output.	
Console	RJ45-DB9 cable for CLI configuration.	

2.2 LED Status

Table 2-3 Router LED indictor Status

silk-screen	status		Indication
Signal	Signal LED	Solid Light	LED1 indicates signal is weak (CSQ0~10). LED2 indicates signal is good (CSQ11~19. LED3 indicates signal is strong (CSQ20~31)
	LED 1	Quick Blinking	Dialing
		Solid Light	4G Online
		Slow Blinking	3G Online
PWR	Solid Light		System power operation.
WLAN	Solid light		WLAN enable, but no data communication.
	Quick Blinking		Data in transmitting
	Dark		WLAN disable
ERR	Dark		System operation and LTE/3G online.
	Solid Light (Red)		System fail indicator such as SIM card/ module fail.
LAN	Green	Solid light	Connected

silk-screen	status		Indication
	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/double SIM.

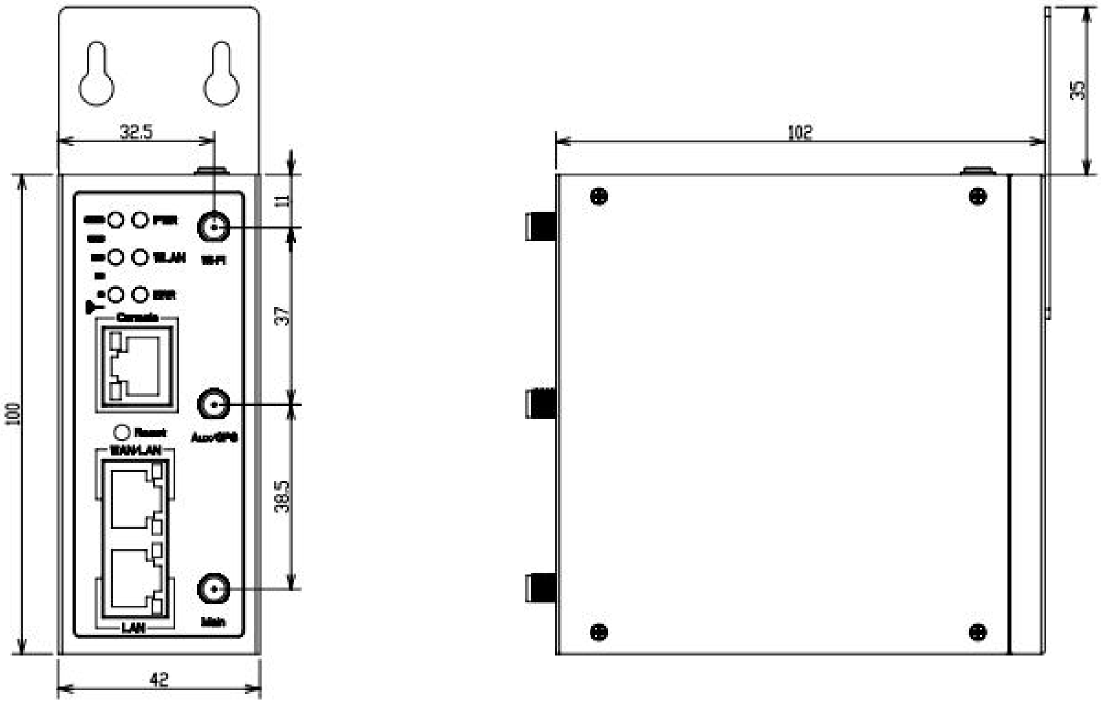


Figure 2-2 R210 Series Router Dimension

2.3 How to Install

2.4.1 SIM/UIM card install

If use dual SIM/UIM card router, you need insert dual SIM before configure it. After inserting, please follow below steps to connect the router.

CAUTION

Before connecting, please disconnect any power resource of router

2.4.2 Ethernet Cable Connection

Use an Ethernet cable to connect the cellular Router with computer directly, or transit by a switch.

2.4.3 Serial Port Connection

If you want to connect the router via serial port to laptop or other devices, you should prepare a serial port or RJ45 cable, this cable is optional available from WLINK. One end connect to computer serial port, the other end connects to the console port of the router

CAUTION

Before connecting, please disconnect any power resource.

2.4.4 Power Supply

In order to get high reliability, WLINK Series Router power adapt supports wide voltage input range from +7.5V to 32VDC, support hot plug and complex application environment.

2.4.5 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

3 Router Configuration

This Chapter introduces the parameter configuration of the router, the router can be configured via web internet explorer, Firefox, or chrome. Here we take GUIs 7 system and Internet Explorer 9.0 as sample.

3.1 Local Configure

The router supports to be configured by local Ethernet port, you could specify a static IP or DHCP get IP for your computer. 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.

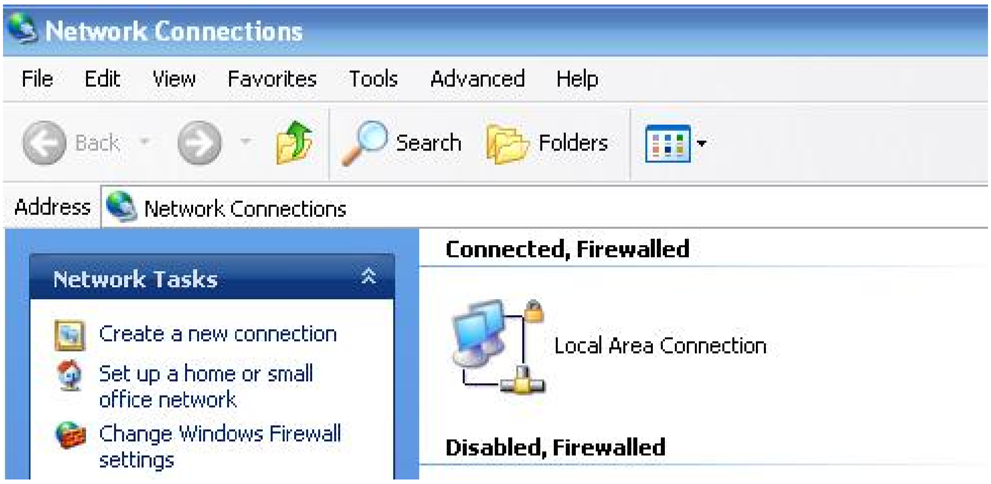
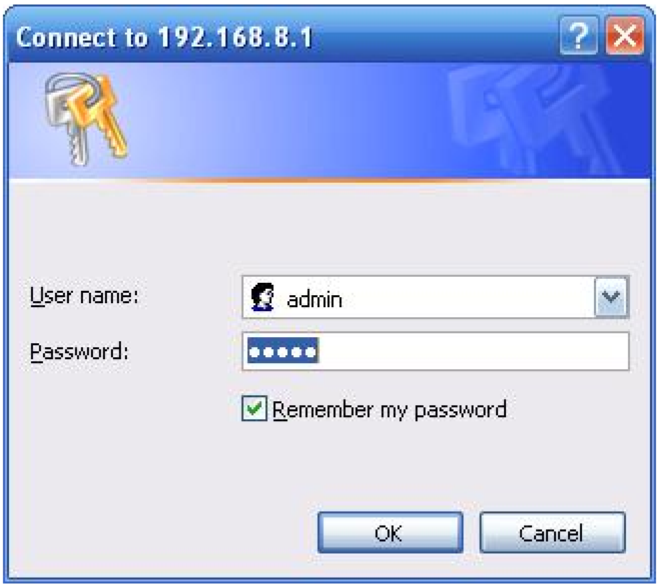


Figure 3-3 Network Connection

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



User name: admin

Password: ●●●●●

☑ Remember my password

Figure 3-4 User Identify Interface

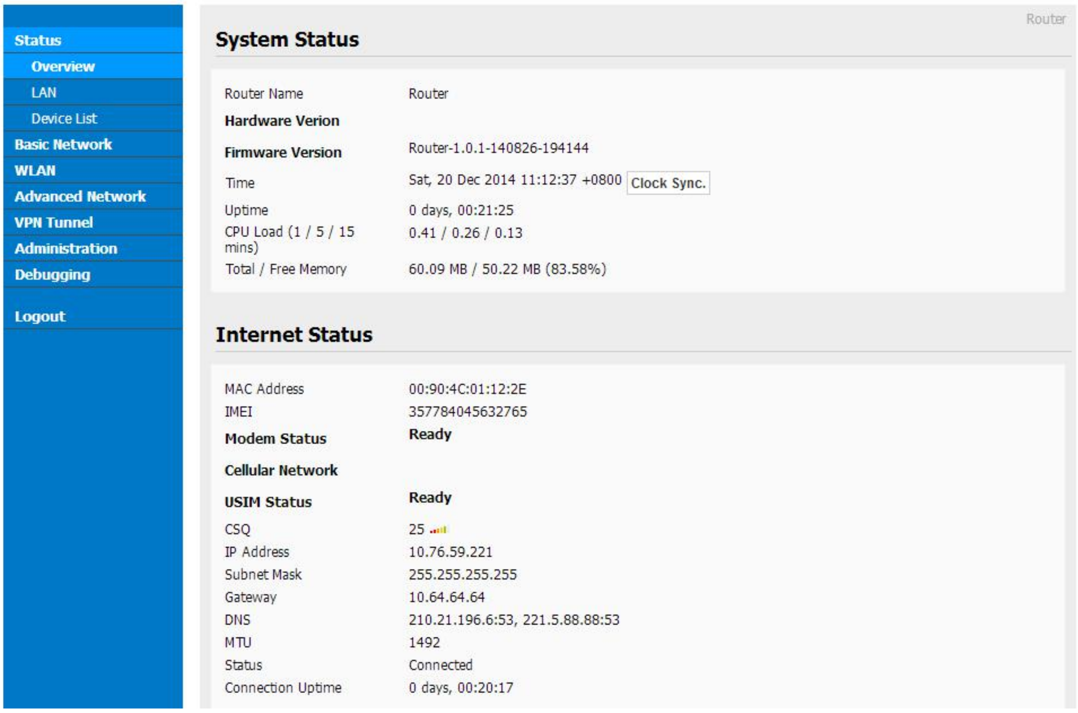
----END

3.2 Basic Configuration

NOTE

Different software version have different web configuration interface, here take R210 2.6.0.1 version as example.

After visit the WEB interface, you can check the current status of Router, or modify router configuration via web interface, below is the introduction for the common setting.



System Status

Router Name Router

Hardware Verion

Firmware Version Router-1.0.1-140826-194144

Time Sat, 20 Dec 2014 11:12:37 +0800

Uptime 0 days, 00:21:25

CPU Load (1 / 5 / 15 mins) 0.41 / 0.26 / 0.13

Total / Free Memory 60.09 MB / 50.22 MB (83.58%)

Internet Status

MAC Address 00:90:4C:01:12:2E

IMEI 357784045632765

Modem Status Ready

Cellular Network

USIM Status Ready

CSQ 25

IP Address 10.76.59.221

Subnet Mask 255.255.255.255

Gateway 10.64.64.64

DNS 210.21.196.6:53, 221.5.88.88:53

MTU 1492

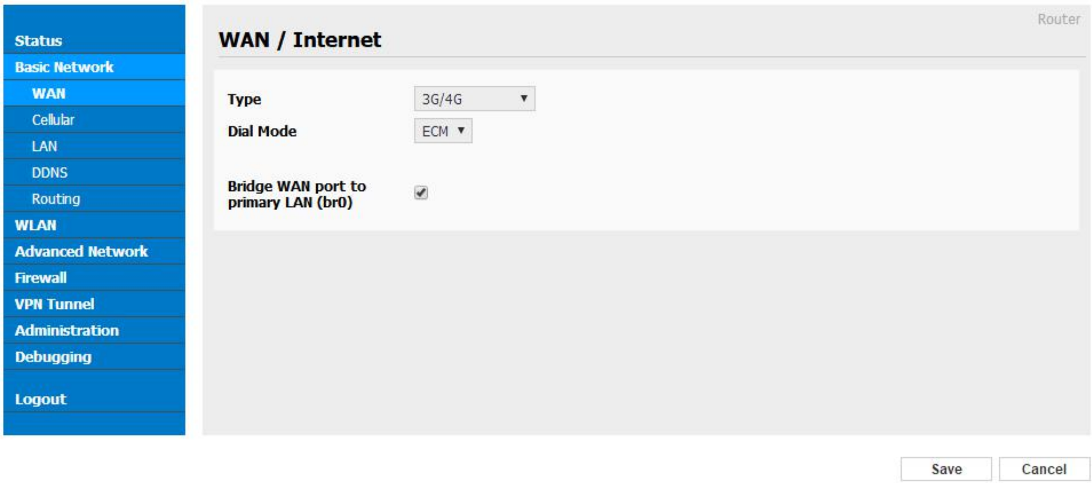
Status Connected

Connection Uptime 0 days, 00:20:17

Figure 3-5 Router Status GUI

3.2.1 **WAN Setting**

Step 1 Single Click “ Basic Network>WAN” to enter below interface



WAN / Internet

Type 3G/4G

Dial Mode ECM

Bridge WAN port to primary LAN (br0) ☑

Figure 3-1 WAN Setting GUI

Table 3-1 WAN Setting Instruction

Parameter	Instruction
Type	Support 3G/4G, PPPoE, DHCP, Static IP

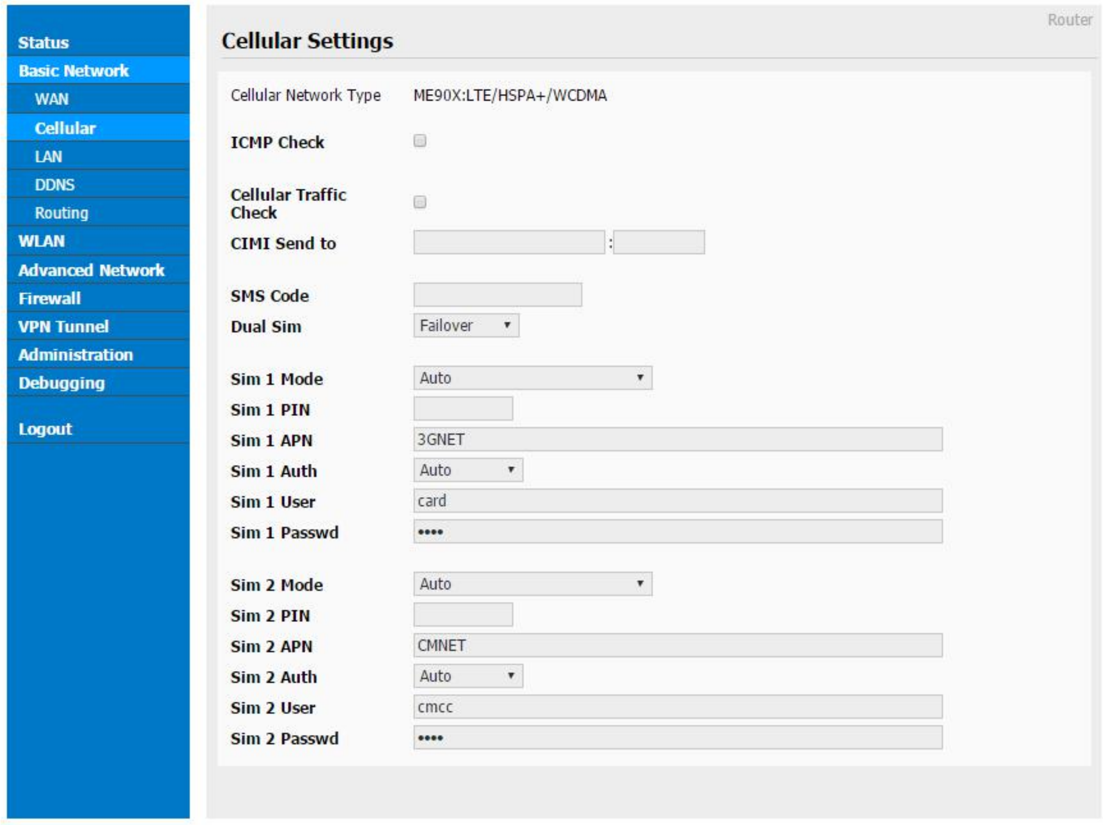
Parameter	Instruction
Dial Mode	ECM/PPP optional. Suggest ECM for 4G router
Bridge WAN to LAN	Configure WAN port as LAN port

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

----End

3.2.2 **Cellular Network Configure**

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



Cellular Settings

Cellular Network Type ME90X:LTE/HSPA+/WCDMA

ICMP Check □

Cellular Traffic Check □

CIMI Send to :

SMS Code

Dual Sim Failover

Sim 1 Mode Auto

Sim 1 PIN

Sim 1 APN 3GNET

Sim 1 Auth Auto

Sim 1 User card

Sim 1 Passwd ••••

Sim 2 Mode Auto

Sim 2 PIN

Sim 2 APN CMNET

Sim 2 Auth Auto

Sim 2 User cmcc

Sim 2 Passwd ••••

Figure 3-2 Dual SIM GUI

Table 3-2 Cellular Setting Parameter Instruction

Parameter	Instruction
ICMP check	To enable or disable ICMP check rules. Enable the ICMP check and setup a reachable IP address as destination IP. Once ICMP check failed, router will reconnect/reboot system as optional.
Cellular Traffic Check	There is Rx/Tx as options. Once no Rx/Tx data, router will router will reconnect/reboot system as options.

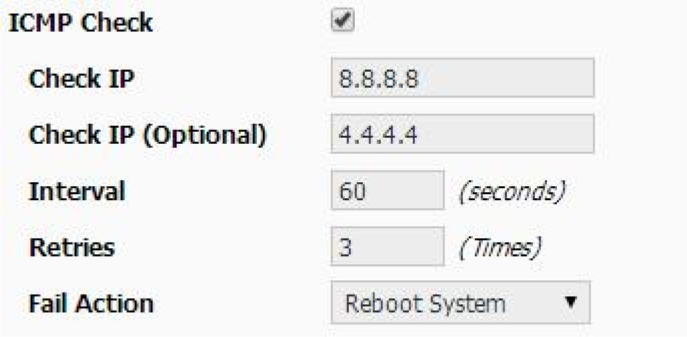
Parameter	Instruction
CIMI Send	Send CIMI to defined IP and port by TCP protocol.
SMS Code	Remotely control router by SMS. Router just identify the correct SMS code as configured.
Pin Code	Some SIM cards are locked with a Personal Identification Number (PIN) code to prevent misuse if they are lost or stolen.
Operator Lock	Lock router for a specified operator via MCC/MNC code.
Connect Mode	● Auto.Router will automatically connect 3G/4G network and keep 4G in prior. ● LTE. Router will connect 4G only. ● 3G. Router will connect 3G only.
APN	APN, provided by local ISP, usually CDMA/EVDO network do not need this parameter.
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth Type	Support PAP/Chap/MS-Chap/MS-Chapv2

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.



ICMP Check ☑

Check IP 8.8.8.8

Check IP (Optional) 4.4.4.4

Interval 60 (seconds)

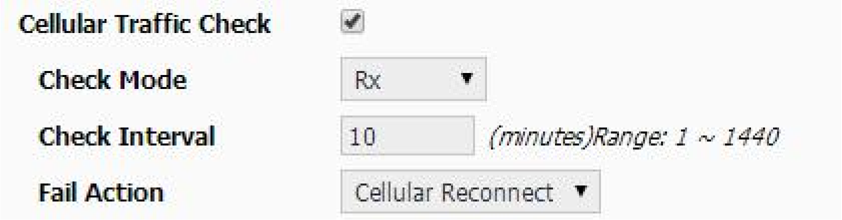
Retries 3 (Times)

Fail Action Reboot System ▼

【Cellular Traffic Check】

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

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



Cellular Traffic Check ☑

Check Mode: Rx

Check Interval: 10 (minutes)Range: 1 ~ 1440

Fail Action: Cellular Reconnect

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

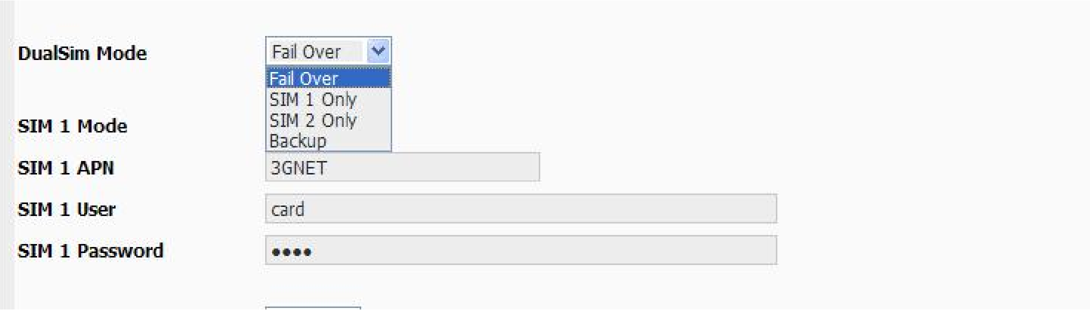
【SIM Mode】

【Fail Over】SIM card mutual backup. Once SIM card is failed, it will switch to the SIM2 and work on SIM2. Once SIM2 is failed, it will switch back to SIM1.

【SIM1 Only】Just SIM1 is available.

【SIM2 Only】Just SIM2 is available.

【Backup】SIM1 is the primary SIM. Once SIM1 is failed, it will switch to SIM2 and work on SIM2 within the defined time. Once the time is over, it will switch back to SIM1.



DualSim Mode: Fail Over

SIM 1 Mode

SIM 1 APN: 3GNET

SIM 1 User: card

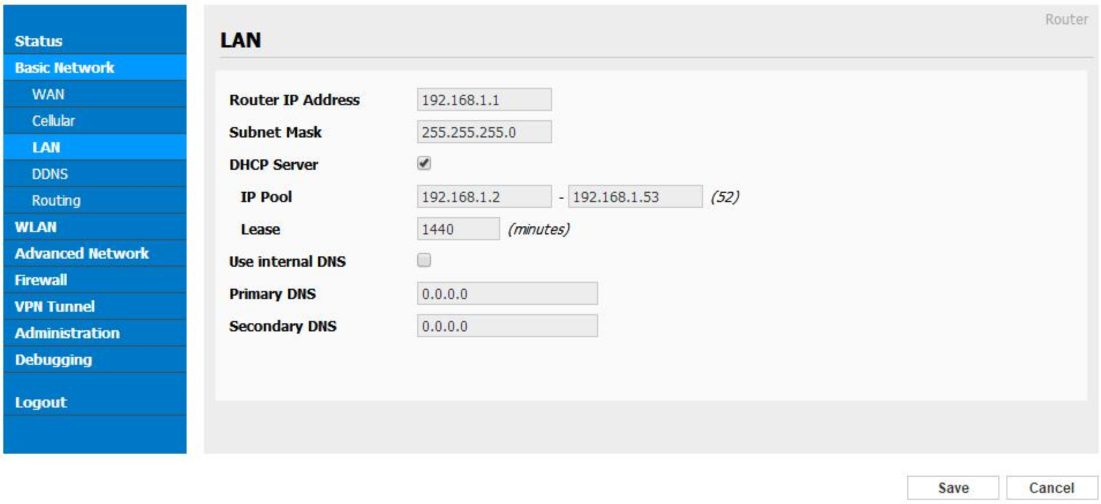
SIM 1 Password: ••••

Step 3 After Setting, please click “save” icon.

----End

3.2.3 **LAN Setting**

Step 1 Single Click “ Basic Network>LAN” to enter below interface



LAN

Router IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

DHCP Server: ☑

IP Pool: 192.168.1.2 - 192.168.1.53 (52)

Lease: 1440 (minutes)

Use internal DNS: □

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Figure 3-3 LAN Setting GUI

Table 3-3 LAN Setting Instruction

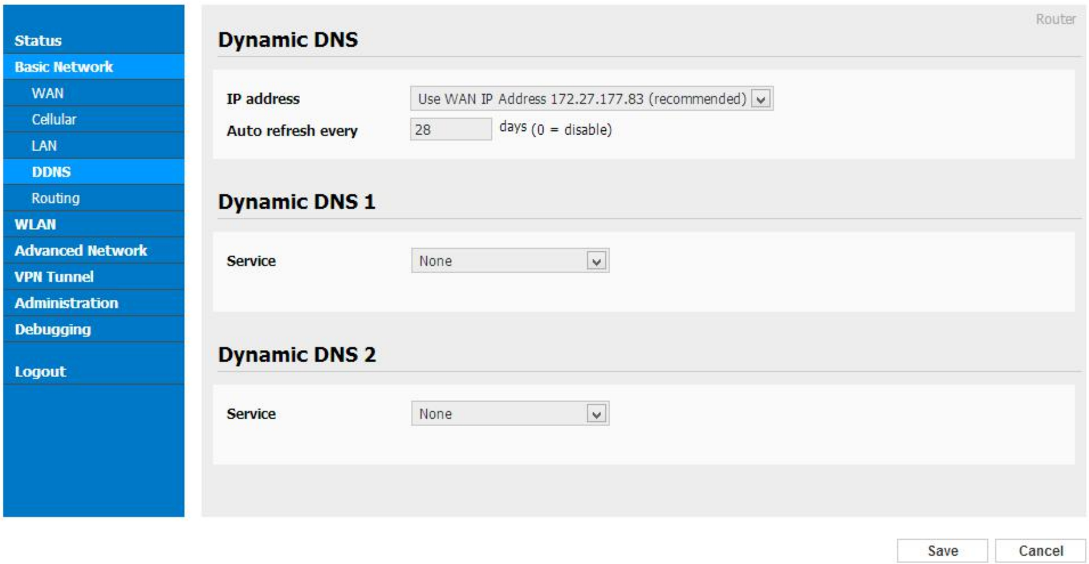
Parameter	Instruction
Router IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease
IP Address Range	IP address range within LAN
Lease	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 Single click “Basic Network->DDNS to enter the DDNS setting page.



Dynamic DNS

IP address: Use WAN IP Address 172.27.177.83 (recommended)

Auto refresh every: 28 days (0 = disable)

Dynamic DNS 1

Service: None

Dynamic DNS 2

Service: None

Figure 3-4 Dynamic DNS Setting

Table 3-4 DDNS Setting Instruction

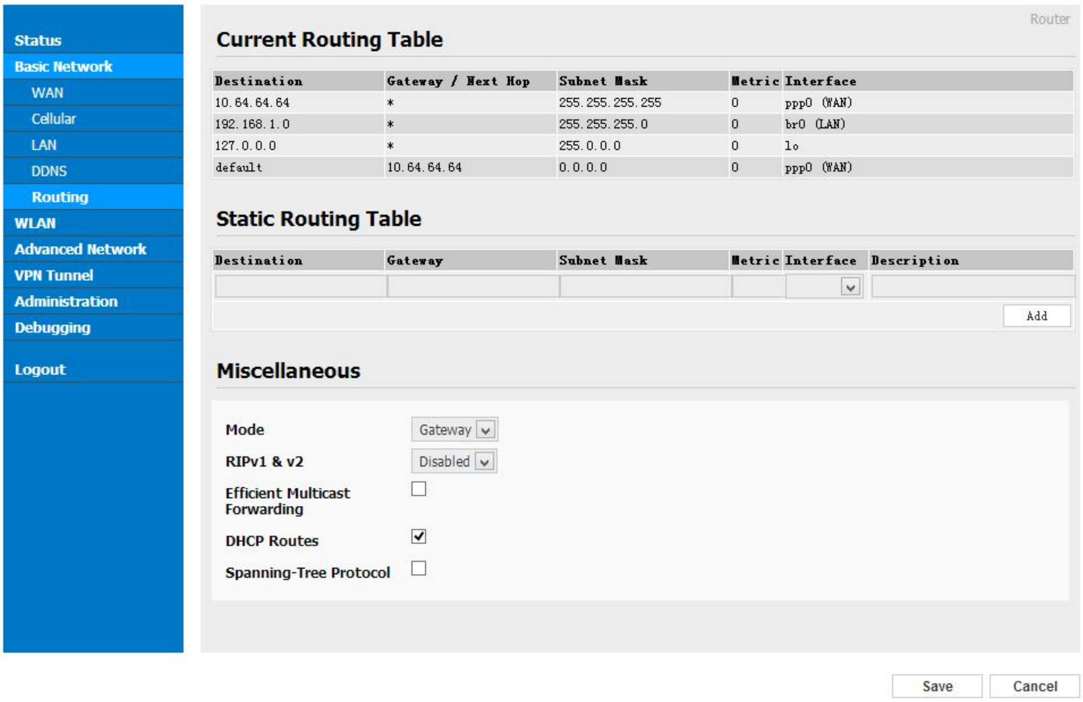
parameter	Instruction
IP address	Default is standard DDNS protocol, for customized protocol, please contact Wlink engineer. Usually, use default IP 0.0.0.0
Auto refresh time	Set the interval of the DDNS client obtains new IP, suggest 240s or above
Service provider	Select the DDNS service provider that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

Step 2 Please Click “Save“ to finish.

----End

3.2.5 Routing Setting

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



Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
10.64.64.64	*	255.255.255.255	0	ppp0 (WAN)
192.168.1.0	*	255.255.255.0	0	br0 (LAN)
127.0.0.0	*	255.0.0.0	0	lo
default	10.64.64.64	0.0.0.0	0	ppp0 (WAN)

Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description

Miscellaneous

Mode: Gateway

RIPv1 & v2: Disabled

Efficient Multicast Forwarding: □

DHCP Routes: ☑

Spanning-Tree Protocol: □

Figure 3-5 Routing Setting

Table 3-5 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.

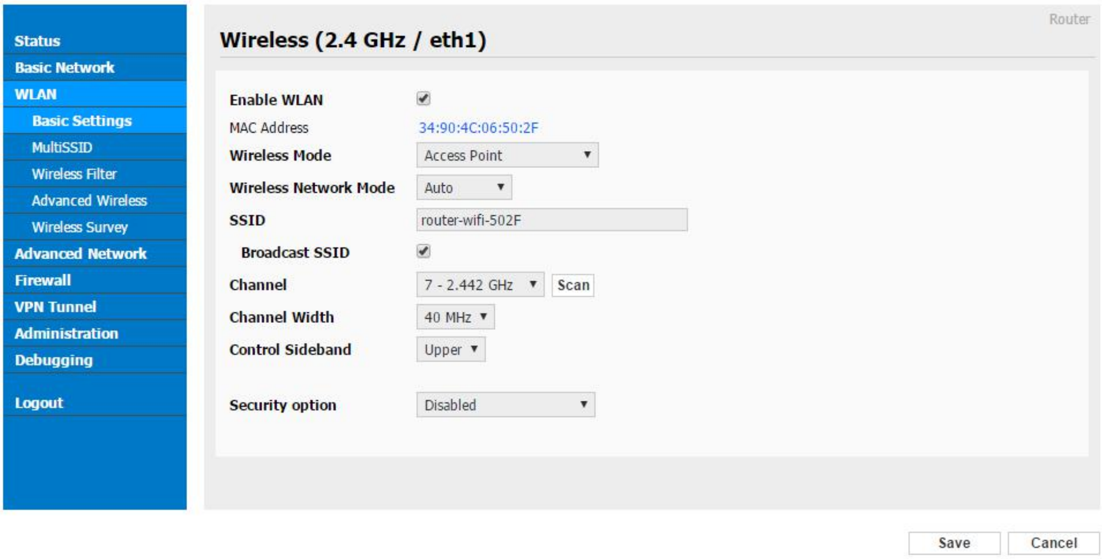
Step 2 Please Click " Save " to finish.

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 Click "WLAN->Basic Setting" to configure relative parameter



Wireless (2.4 GHz / eth1)

Enable WLAN ☑
MAC Address 34:90:4C:06:50:2F
Wireless Mode Access Point
Wireless Network Mode Auto
SSID router-wifi-502F
Broadcast SSID ☑
Channel 7 - 2.442 GHz
Channel Width 40 MHz
Control Sideband Upper
Security option Disabled

Figure 3-6 WLAN Basic Settings GUI

Table 3-6 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

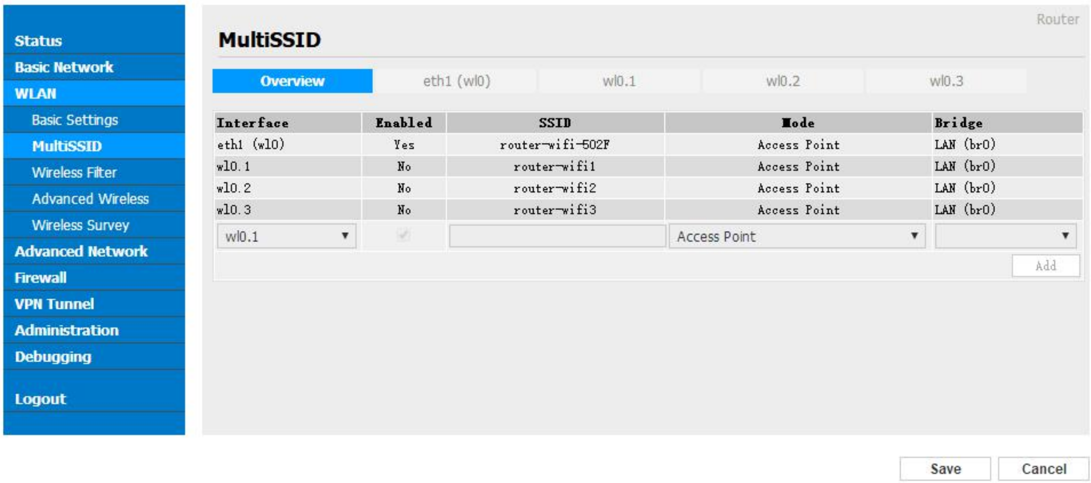
Parameter	Instruction
Channel Width	20MHZ and 40MHZ alternative
Security	Support various encryption method

Step 2 Please click “Save” to finish.

----End

3.3.2 **MultiSSID**

Step 1 Single click “WLAN > MultiSSID”.

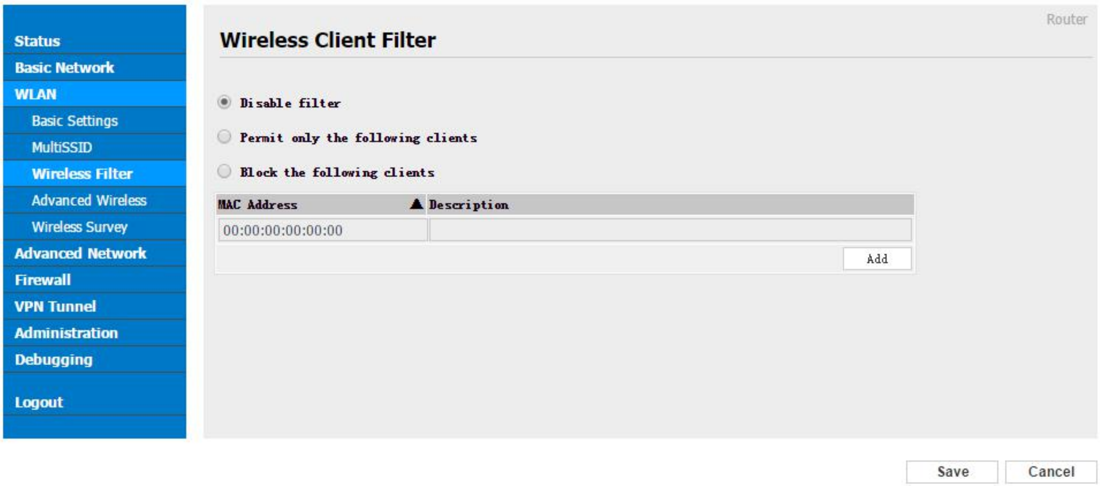


MultiSSID

Interface	Enabled	SSID	Mode	Bridge
eth1 (wl0)	Yes	router-wifi-502F	Access Point	LAN (br0)
wl0.1	No	router-wifi1	Access Point	LAN (br0)
wl0.2	No	router-wifi2	Access Point	LAN (br0)
wl0.3	No	router-wifi3	Access Point	LAN (br0)
wl0.1 ▼	✓		Access Point ▼	▼

3.3.3 **Wireless Filter Setting**

Step 1 Single click “WLAN > Wireless Filter”.



Wireless Client Filter

● Disable filter

○ Permit only the following clients

○ Block the following clients

MAC Address ▲	Description
00:00:00:00:00:00	

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 3-7 "Wireless Client Filter" Setting Instruction

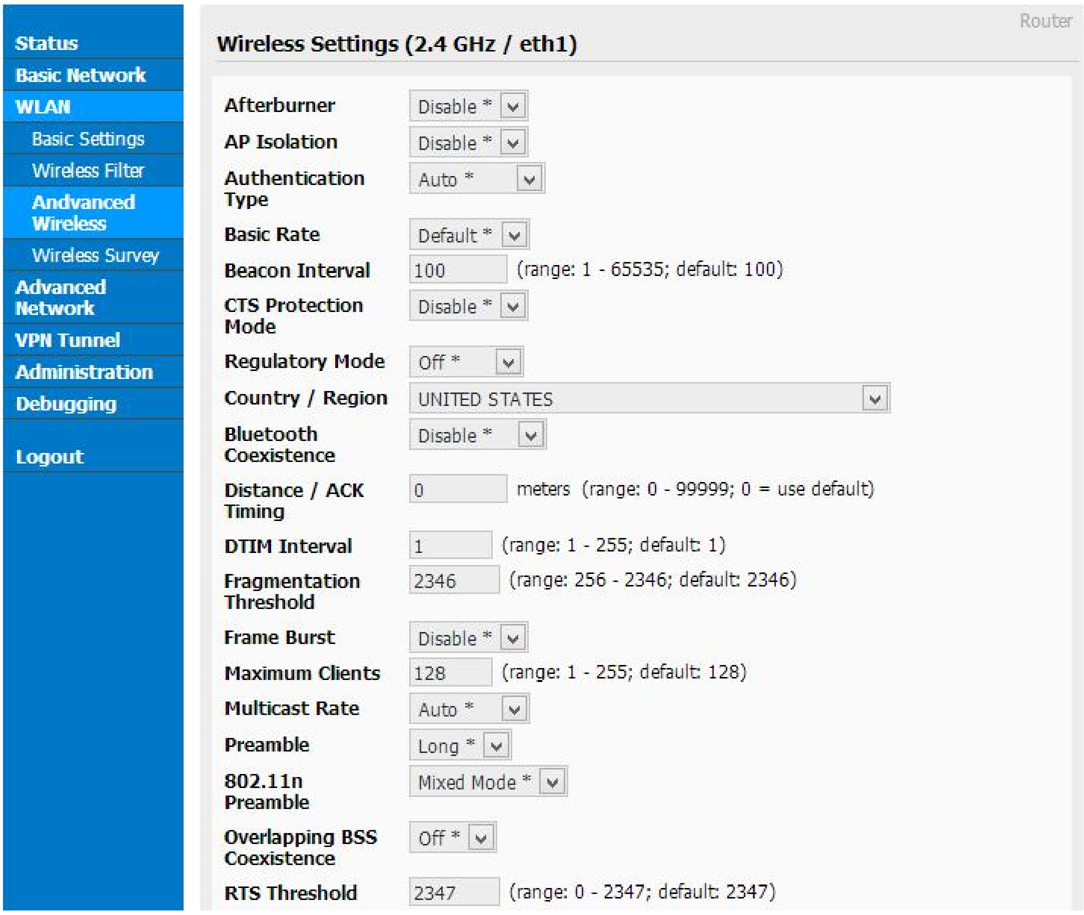
Parameter	Instruction
Disable Filter	Choose to disable
Permit on the following client	Only allow the listed MAC address to connect to router by wireless
Block the follow Client	Prevent the listed MAC address to connect to router by wireless

Step 2 Please click "save" to finish

----End

3.3.4 Advanced Wireless Setting

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



Wireless Settings (2.4 GHz / eth1)

Afterburner	Disable *	
AP Isolation	Disable *	
Authentication Type	Auto *	
Basic Rate	Default *	
Beacon Interval	100	(range: 1 - 65535; default: 100)
CTS Protection Mode	Disable *	
Regulatory Mode	Off *	
Country / Region	UNITED STATES	
Bluetooth Coexistence	Disable *	
Distance / ACK Timing	0	meters (range: 0 - 99999; 0 = use default)
DTIM Interval	1	(range: 1 - 255; default: 1)
Fragmentation Threshold	2346	(range: 256 - 2346; default: 2346)
Frame Burst	Disable *	
Maximum Clients	128	(range: 1 - 255; default: 128)
Multicast Rate	Auto *	
Preamble	Long *	
802.11n Preamble	Mixed Mode *	
Overlapping BSS Coexistence	Off *	
RTS Threshold	2347	(range: 0 - 2347; default: 2347)

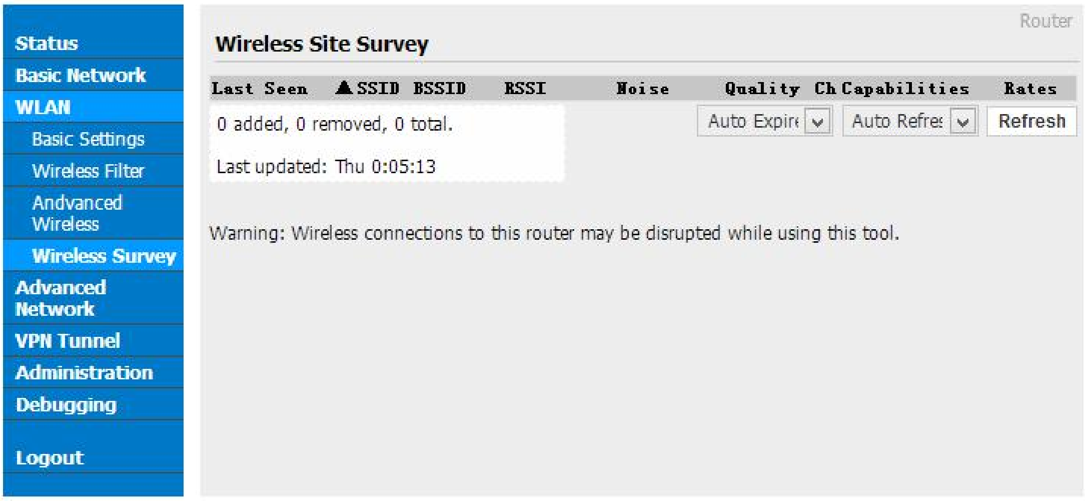
Figure 3-8 Advanced Wireless Setting GUI

Step 2 Please click ”save” to finish.

----End

3.3.5 Wireless Survey

Step 1 Please click “WLAN> Wireless Survey” to check survey.



0 added, 0 removed, 0 total.

Last updated: Thu 0:05:13

Warning: Wireless connections to this router may be disrupted while using this tool.

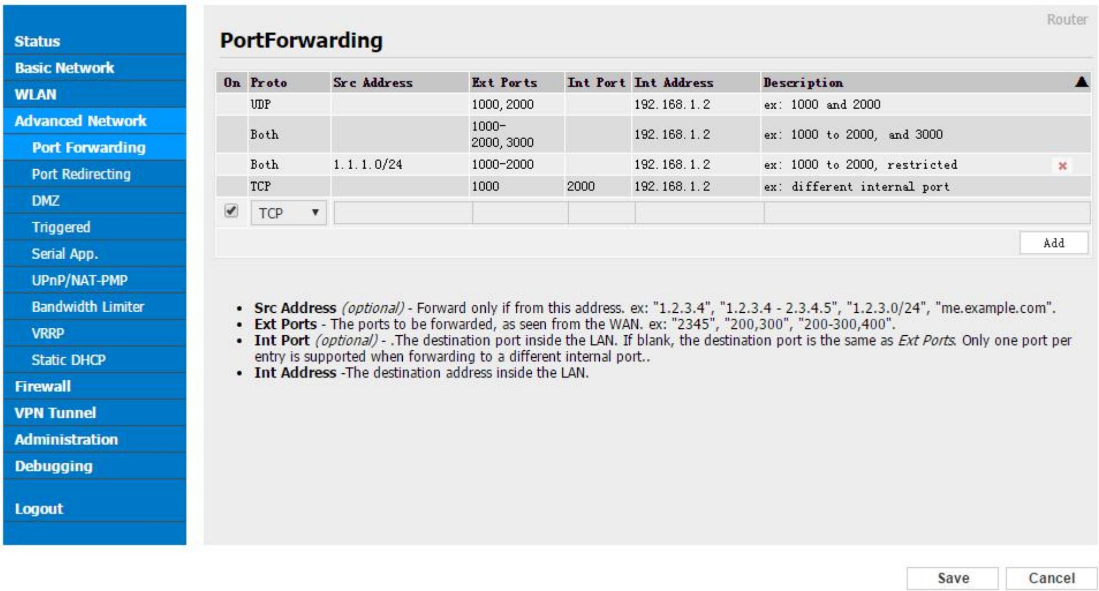
Figure 3-9 Wireless Survey Setting GUI

----End

3.4 Advanced Network Setting

3.4.1 Port Forwarding

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



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.

Figure 3-10 Port Forwarding GUI

Table 3-8 “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 Please click “Advanced Network > Port Redirecting” to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

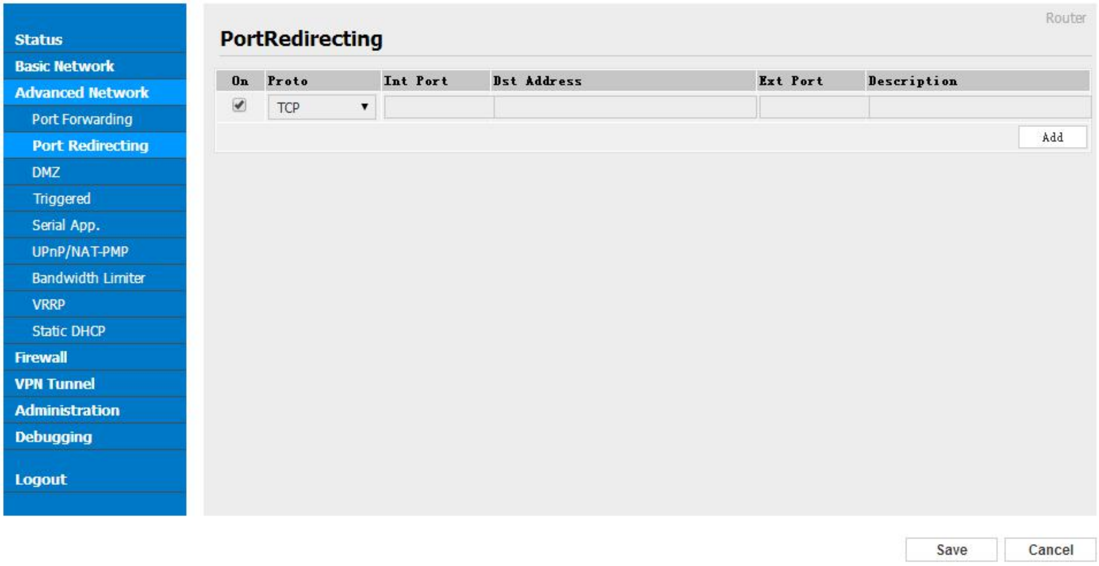


Figure 3-11 Port Forwarding GUI

Table 3-9 "Port Redirecting" Instruction

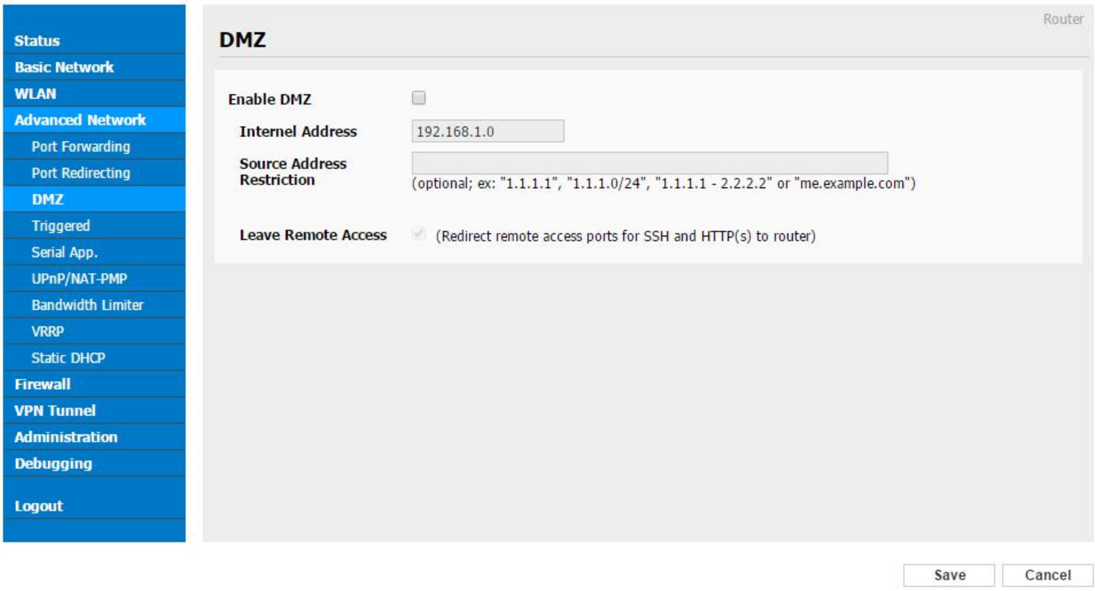
Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Int Port	Internal port.
Dst. Address	The redirecting IP address.
Ext. Ports	External port for redirection.
Description	Remark the rule

Step 2 Please click ”save” to finish

----End

3.4.3 **DMZ Setting**

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



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 Remote Access ☑ (Redirect remote access ports for SSH and HTTP(s) to router)

Figure 3-12 DMZ GUI

Table 3-10 “DMZ” Instruction

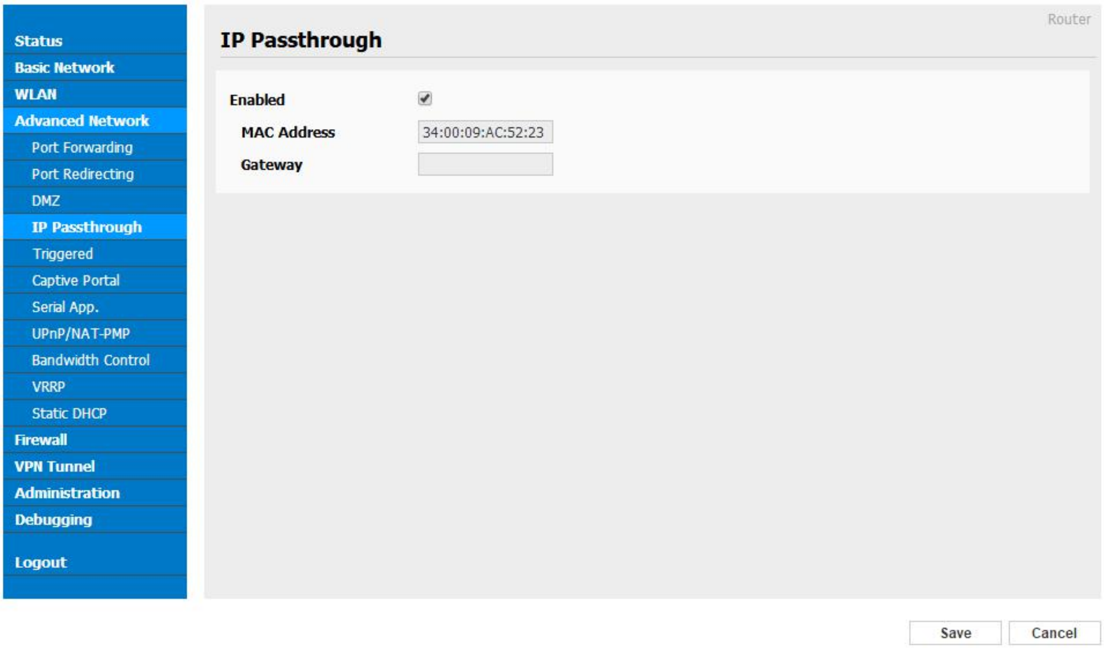
parameter	Instruction
Destination Address	The destination address inside the LAN.
Source Address Restriction	If no IP address inside, it will allow all IP address to access. If define IP address, it will just allow the defined IP address to access.
Leave Remote Access	

Step 2 Please click ”save” to finish

----End

3.4.4 IP Passthrough Setting

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



IP Passthrough

Enabled ☑

MAC Address 34:00:09:AC:52:23

Gateway

Figure 3-13 IP Passthrough GUI

Table 3-11 “IP Passthrough” Instruction

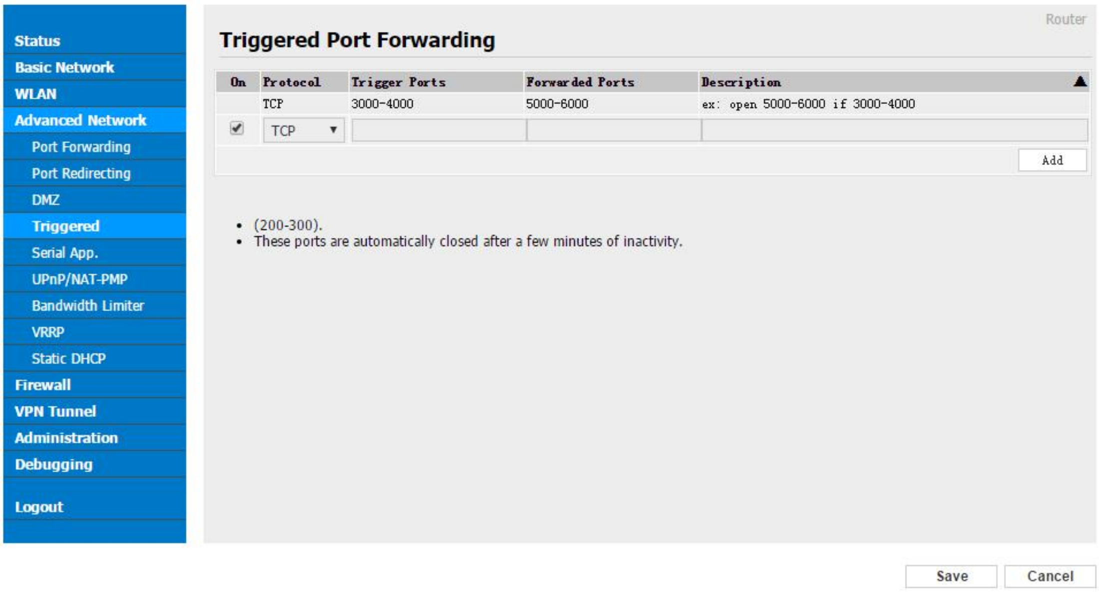
parameter	Instruction
Enable	Enable IP Passthrough
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.
Gateway	If WL-R210 connect to multiple device, input other device gateway. The device might access to router GUI.

Step 2 Please click ”save” to finish

----End

3.4.5 **Triggered Setting**

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



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.

Figure 3-14 Triggered GUI

Table 3-12 "Triggered" Instruction

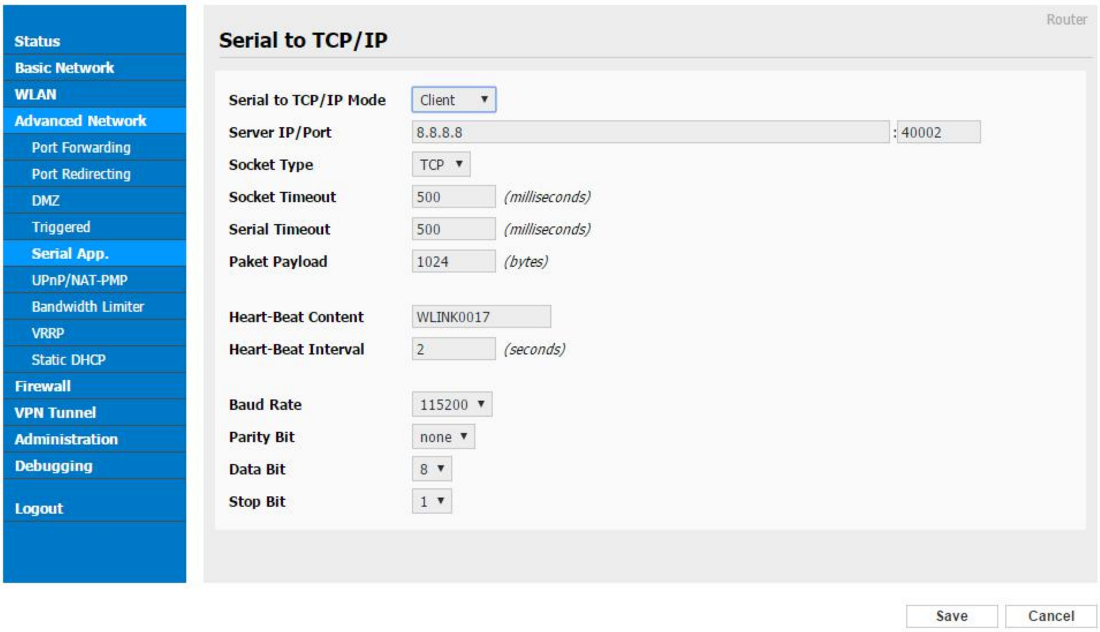
parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.
Note	Port triggering opens an incoming port when your computer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

Step 2 Please click "save" to finish.

----End

3.4.6 Serial App. Setting

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



Serial to TCP/IP

Serial to TCP/IP Mode: Client

Server IP/Port: 8.8.8.8 : 40002

Socket Type: TCP

Socket Timeout: 500 (milliseconds)

Serial Timeout: 500 (milliseconds)

Paket Payload: 1024 (bytes)

Heart-Beat Content: WLINK0017

Heart-Beat Interval: 2 (seconds)

Baud Rate: 115200

Parity Bit: none

Data Bit: 8

Stop Bit: 1

Figure 3-15 Serial App Setting GUI

Table 3-13 “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

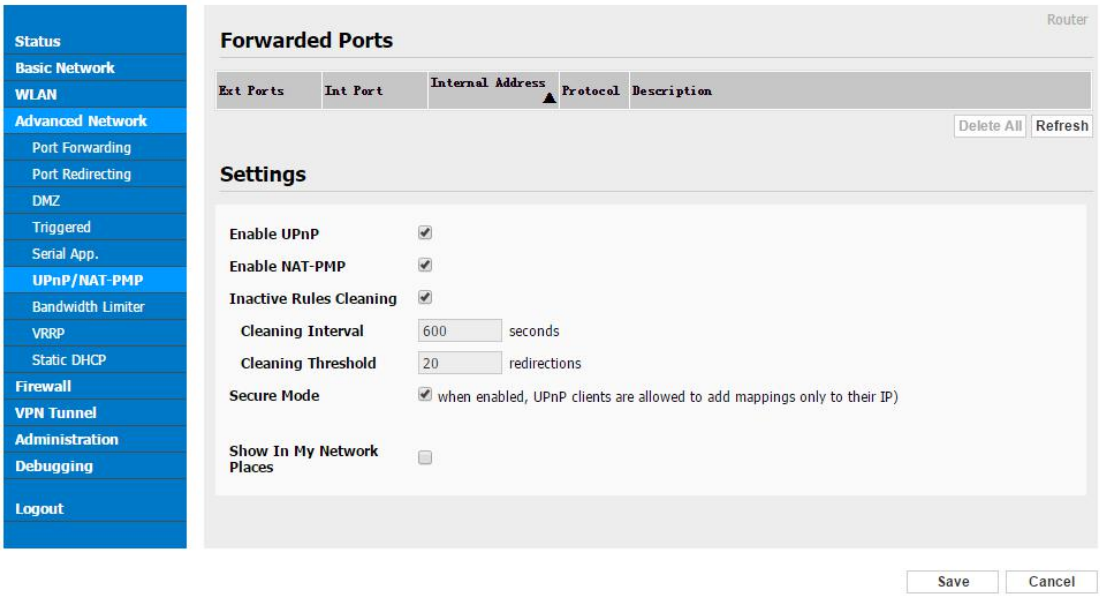
PINs		DB9(male)
V+		
V-		
GND	----	5
RX	----	3
TX	----	2
DI-1		
DI-2		
DI-3		

Step 2 Please click ”save” to finish.

----End

3.4.7 **UPnp/NAT-PMP Setting**

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



Forwarded Ports

Ext Ports	Int Port	Internal Address	Protocol	Description

Settings

Enable UPnP ☑

Enable NAT-PMP ☑

Inactive Rules Cleaning ☑

Cleaning Interval 600 seconds

Cleaning Threshold 20 redirections

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

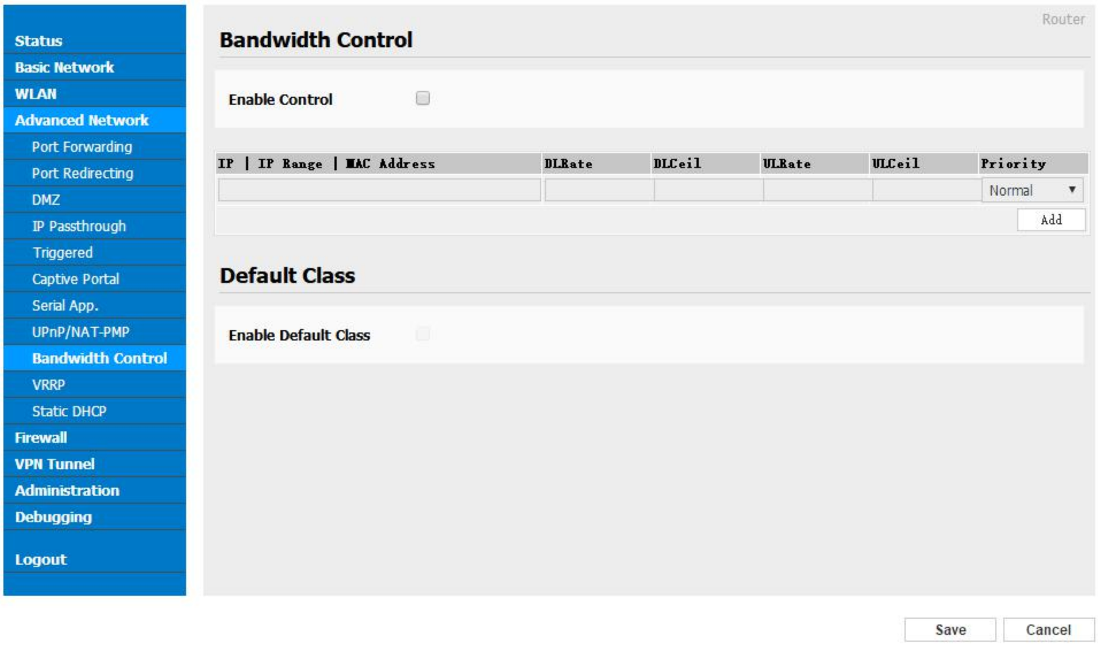
Show In My Network Places □

Figure 3-16 UPnp/NAT-PMP Setting GUI

Step 2 Please click ”save” to finish.

3.4.8 **Bandwidth Control Setting**

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



Bandwidth Control

Enable Control □

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

Default Class

Enable Default Class □

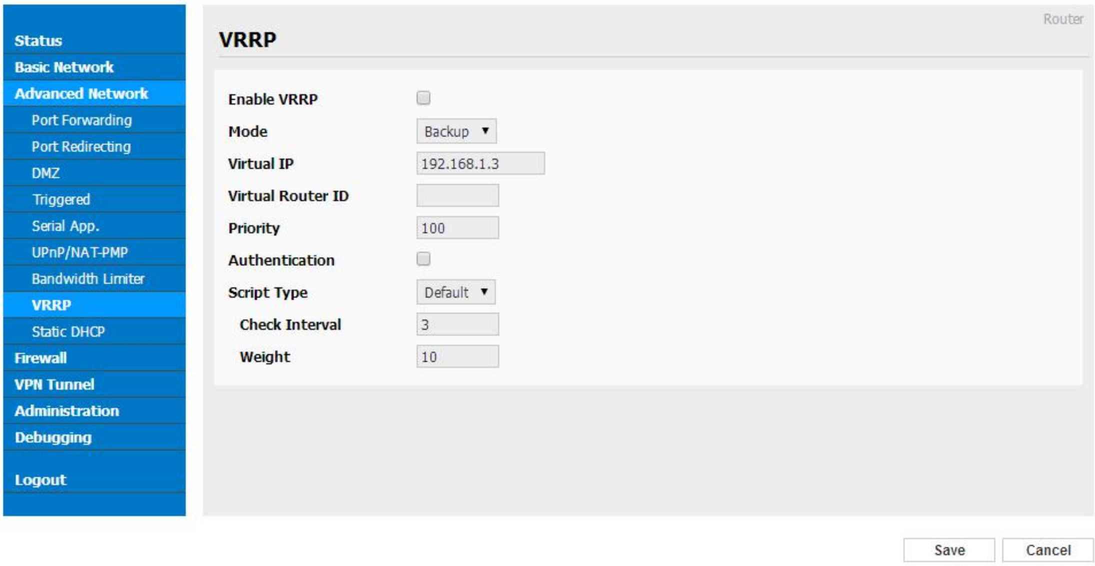
Figure 3-17 Bandwidth Control Setting GUI

Step 2 Please click ”save” to finish.

----End

3.4.9 **VRRP Setting**

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



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

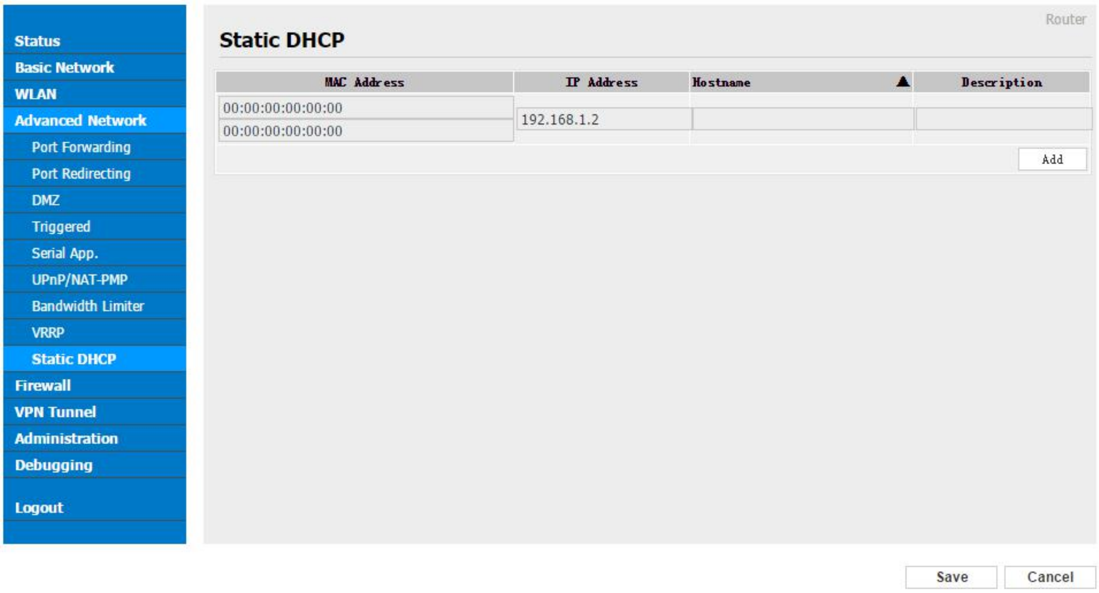
Figure 3-18 VRRP Setting GUI

Step 2 Please click ”save” to finish.

----End

3.4.10 Static DHCP Setting

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



Static DHCP

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

Figure 3-19 Static DHCP Setting GUI

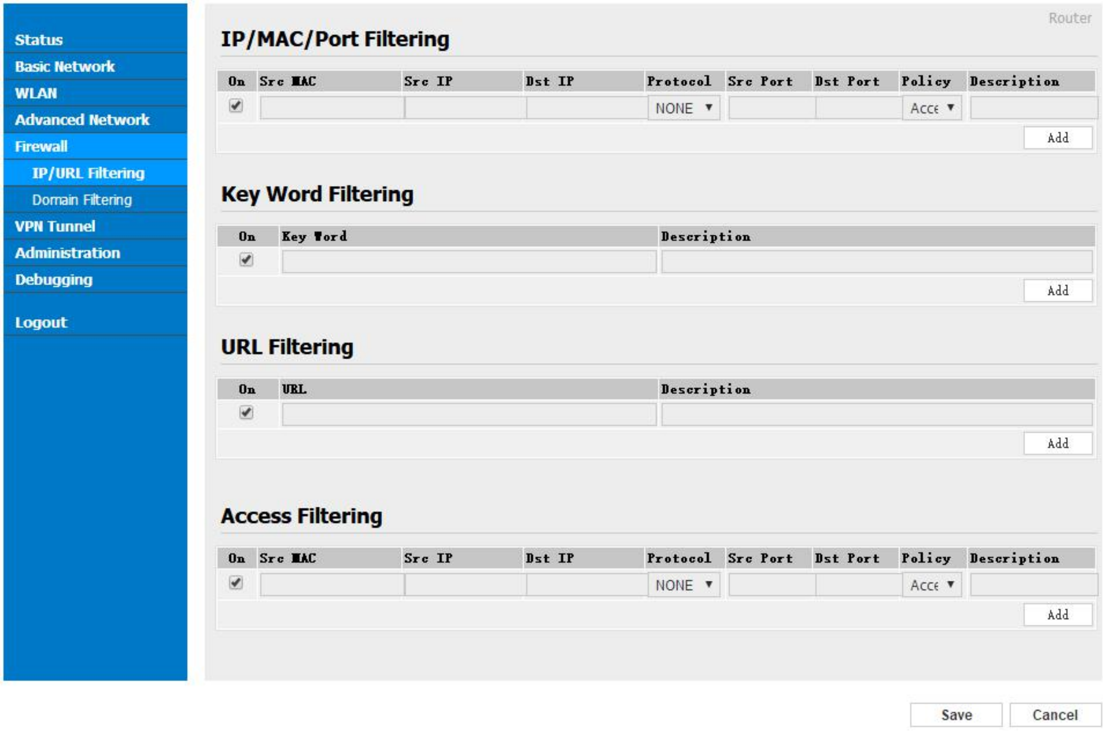
Step 2 Please click ”save” to finish.

----End

3.5 Firewall

3.5.1 IP/URL Filtering

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



IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NONE			Acce	

Key Word Filtering

On	Key Word	Description
☑		

URL Filtering

On	URL	Description
☑		

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NONE			Acce	

Table 3-14 "IP/URL Filtering" Instruction

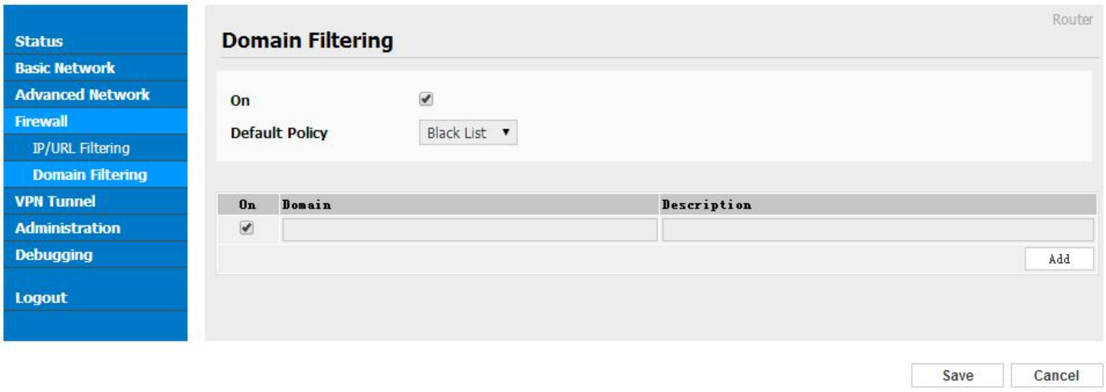
Parameter	Instruction
IP/MAC/Port Filtering	Support IP address, MAC address and port filter. Accept/Drop options for filter policy.
Key Word Filtering	Support key word filter.
URL Filtering	Support URL filter.
Access Filtering	Support Access Filter.

Step 2 Click "save" to finish. If need more information, please check the page68 for Firewall/ACL configuration instance.

---End

3.5.2 Domain Filtering

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



Domain Filtering

On ☑

Default Policy Black List

On	Domain	Description
☑		

Figure 3-20 Domain Filtering Setting GUI

Table 3-15 “GRE” Instruction

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

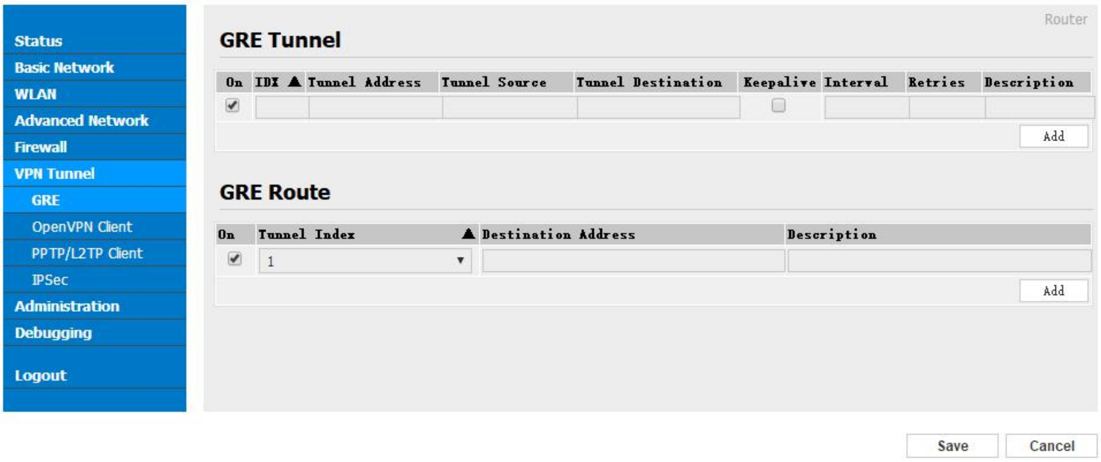
Step 2 Please click ”save” to finish.

----End

3.6 VPN Tunnel

3.6.1 GRE Setting

Step 1 Please click “VPN Tunnel> GRE” to check or modify the relevant parameter.



GRE Tunnel

On	IDX ▲	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
☑					□			

GRE Route

On	Tunnel Index ▲	Destination Address	Description
☑	1		

Figure 3-21 GRE Setting GUI

Table 3-16 “GRE” Instruction

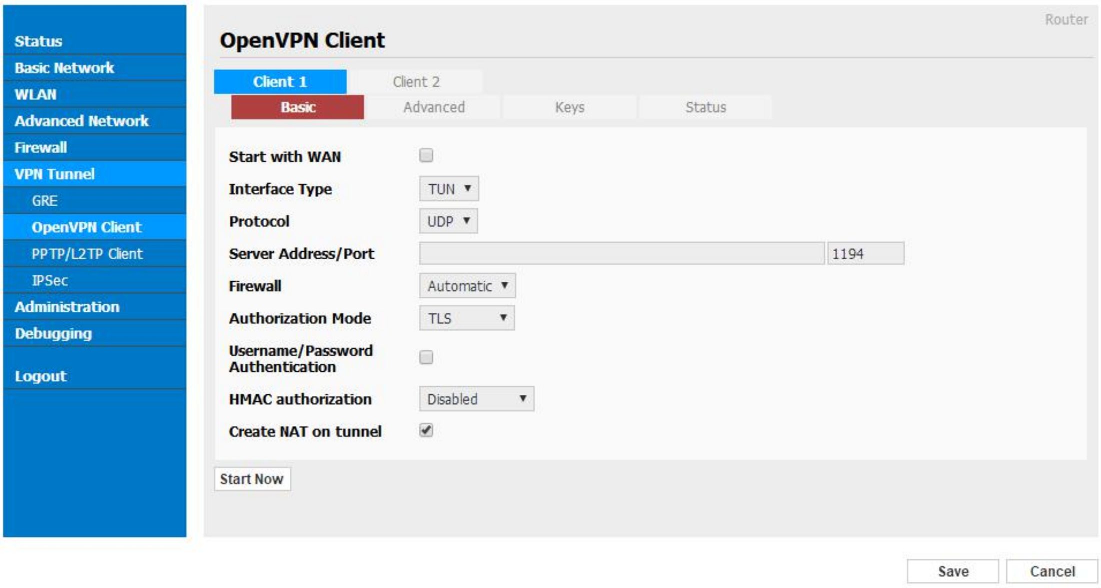
Parameter	Instruction
IDE	GRE tunnel number
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.
Tunnel Source	Router’s 3G/WAN IP address.
Tunnel Destination	GRE Remote IP address. Usually a public IP address
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.
Interval	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 Please click “VPN Tunnel> OpenVPN Client” to check or modify the relevant parameter.



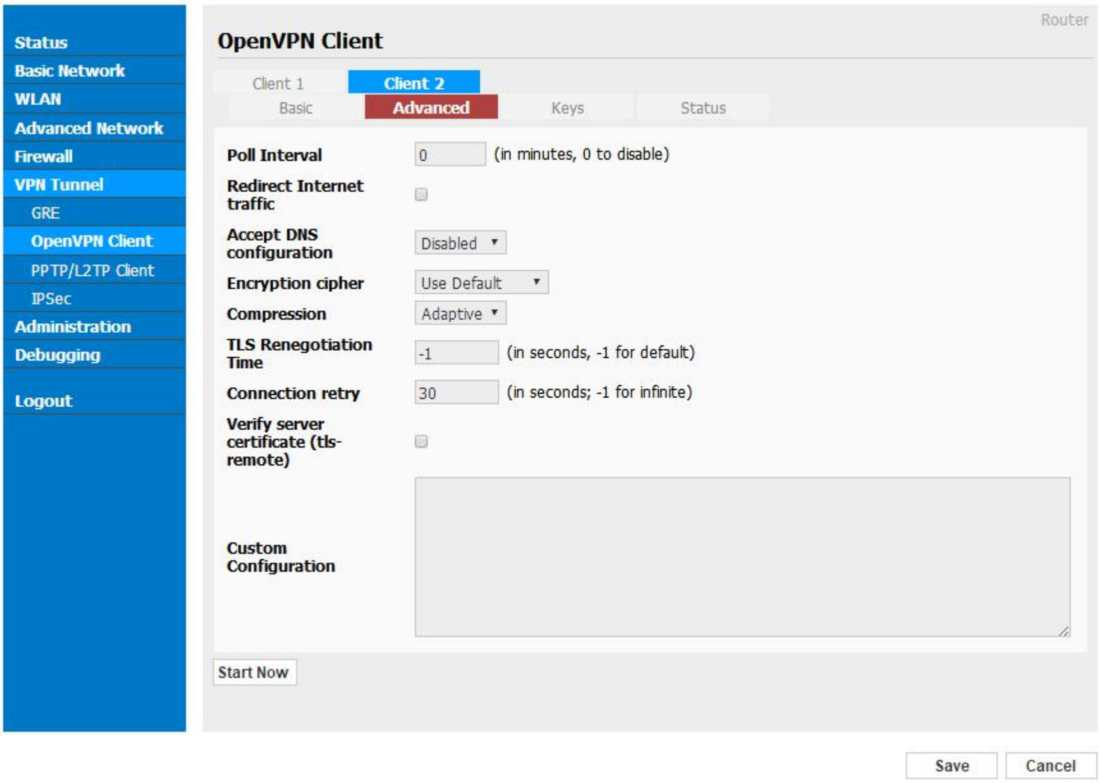
OpenVPN Client

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

Figure 3-22 OpenVPN Setting GUI

Table 3-17 “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.



OpenVPN Client

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)

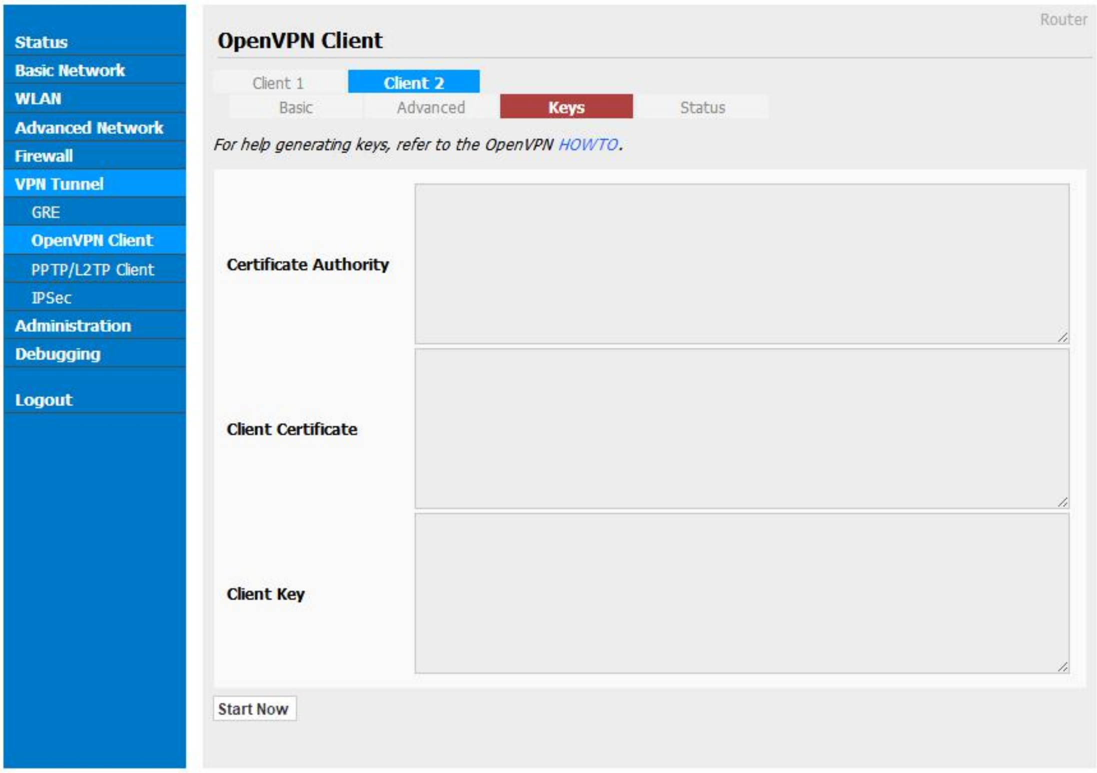
Connection retry: 30 (in seconds; -1 for infinite)

Verify server certificate (tls-remote): □

Custom Configuration:

Parameter	Instruction
Poll Interval	Openvpn client check router’s status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.

Parameter	Instruction
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.



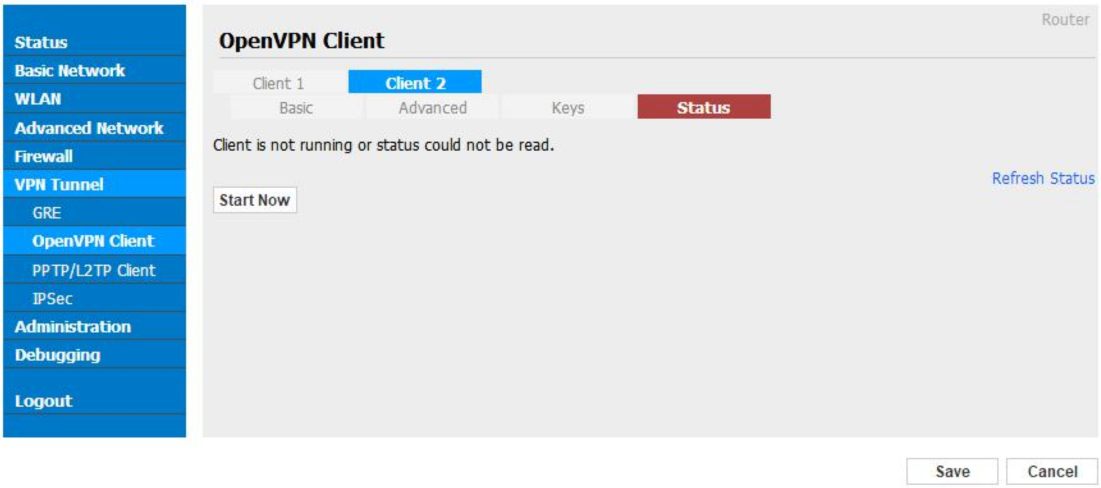
For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

Client Certificate

Client Key

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



OpenVPN Client

Client is not running or status could not be read.

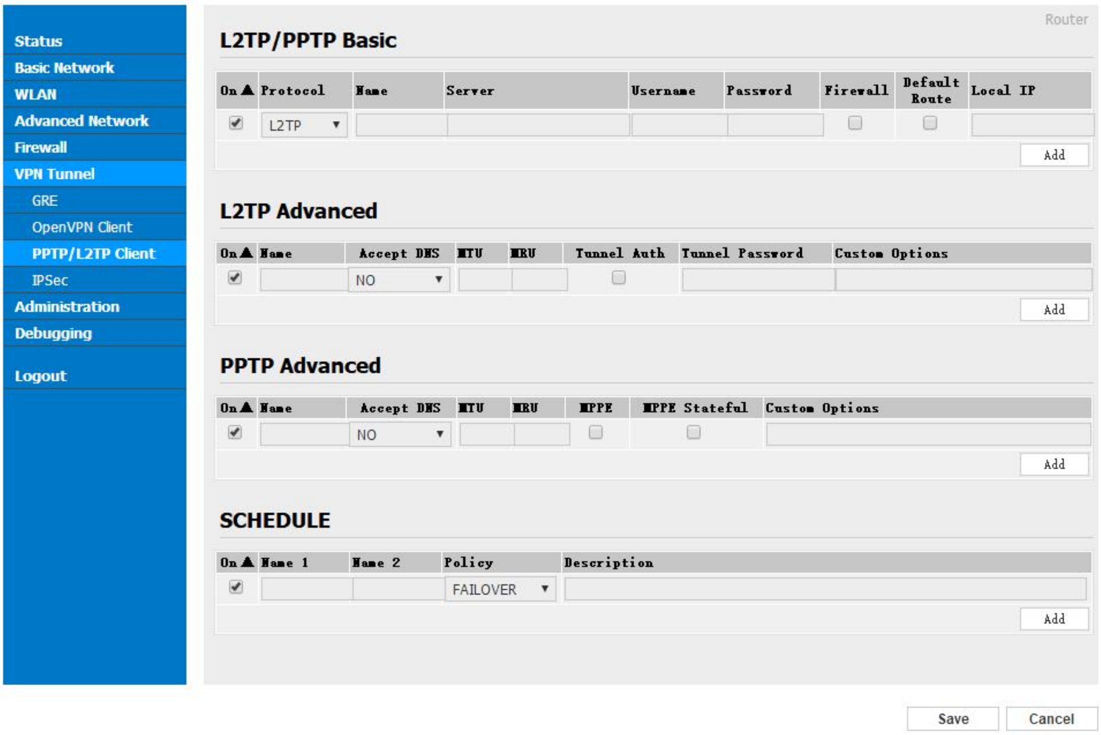
Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 2 Please click ”save” to finish.

----End

3.6.3 VPN Client Setting

Step 1 Please click “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					☐	☐	

L2TP Advanced

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

PPTP Advanced

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

SCHEDULE

On▲	Name 1	Name 2	Policy	Description
☑			FAILOVER	

Table 3-18 “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 3-19 “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 3-20 “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

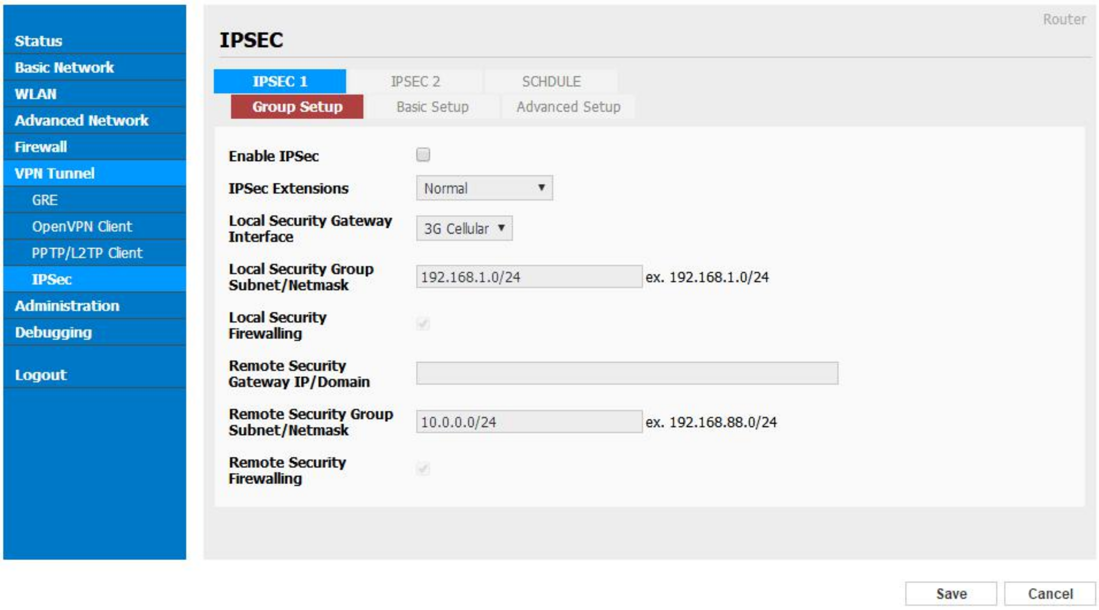
Table 3-21 “SCHEDULE” Instruction

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



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 ☑

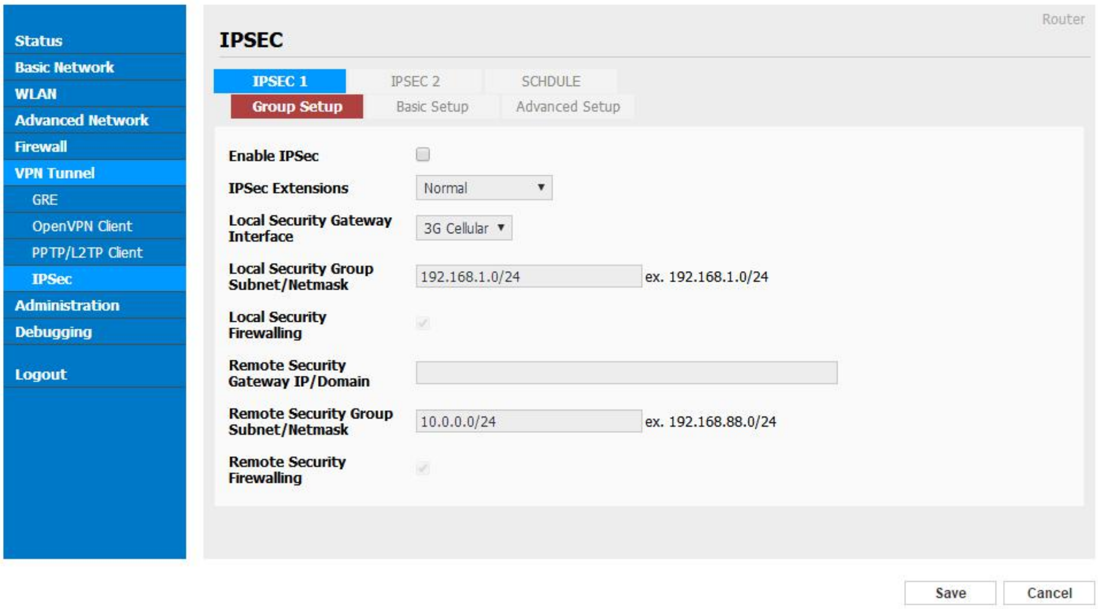
Remote Security Gateway IP/Domain:

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

Remote Security Firewalling ☑

3.5.3.1 IPSec Group Setup

Step 1 Please click “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 ☑

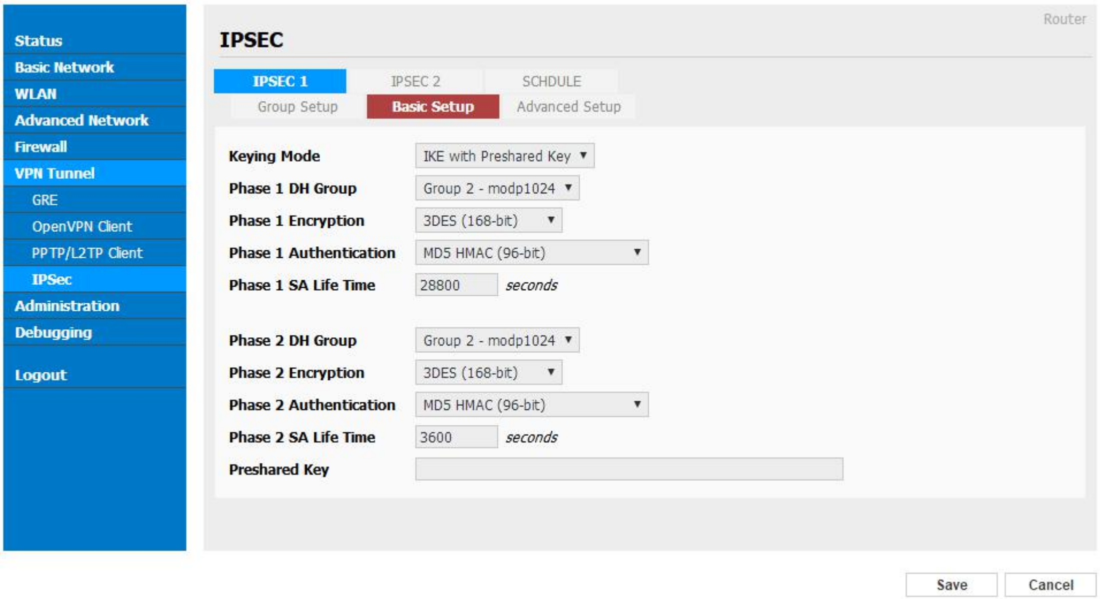
Table 3-22 “ IPSec Group Setup” Instruction

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 Please click “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:

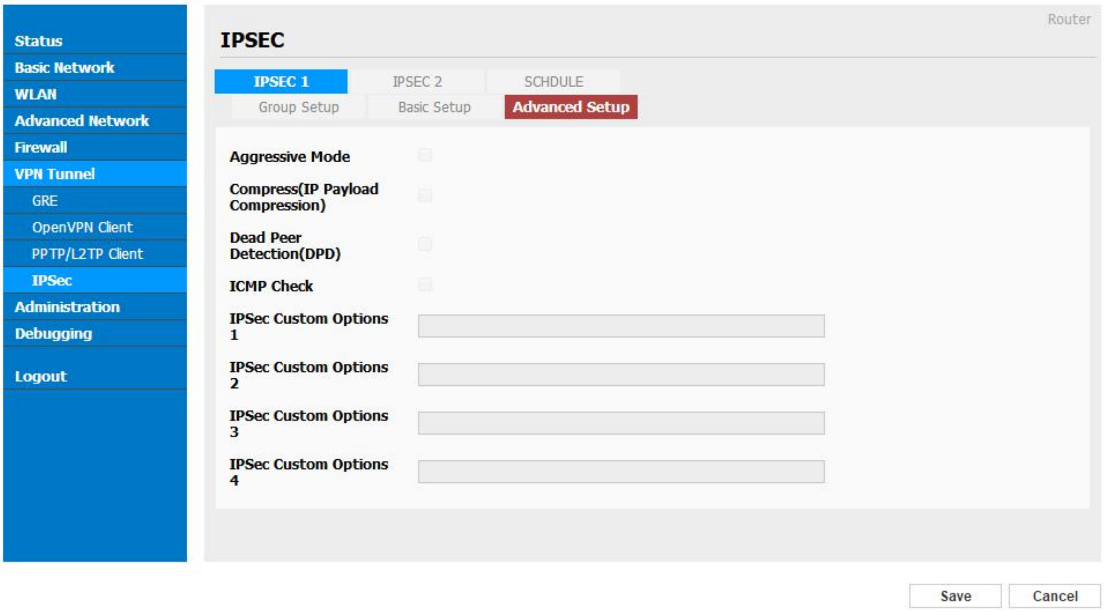
Table 3-23 " IPSec Basic Setup" Instruction

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 Please click "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 3-24 " 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.

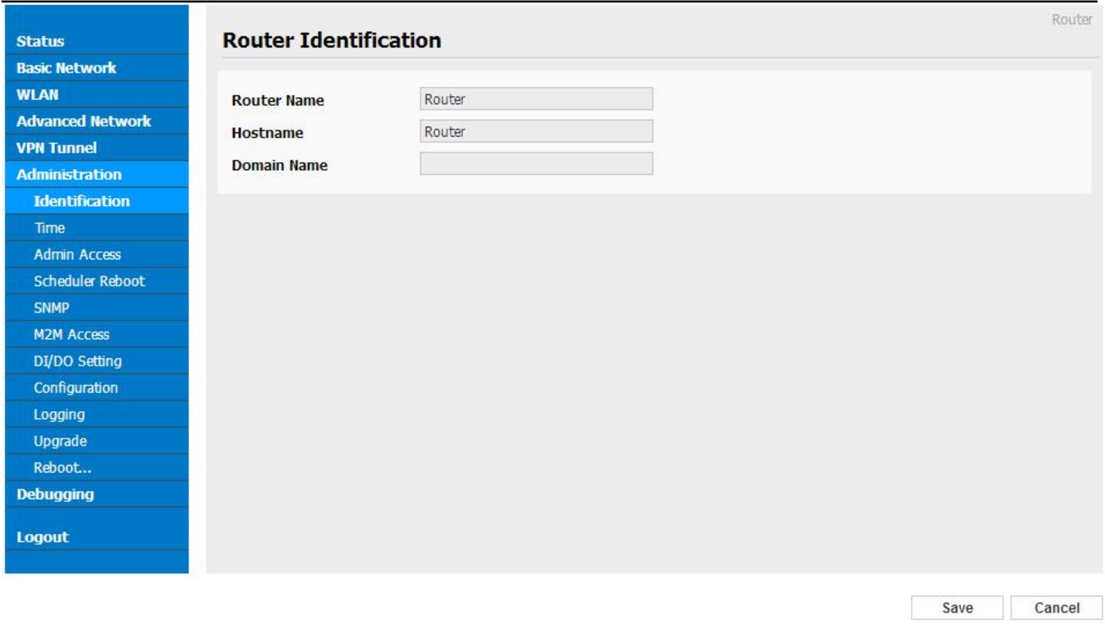
Step 2 Please click "save" to finish.

----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.



Router Identification

Router Name: Router

Hostname: Router

Domain Name:

Figure 3-23　Router Identification GUI

Table 3-25　"Router Identification" Instruction

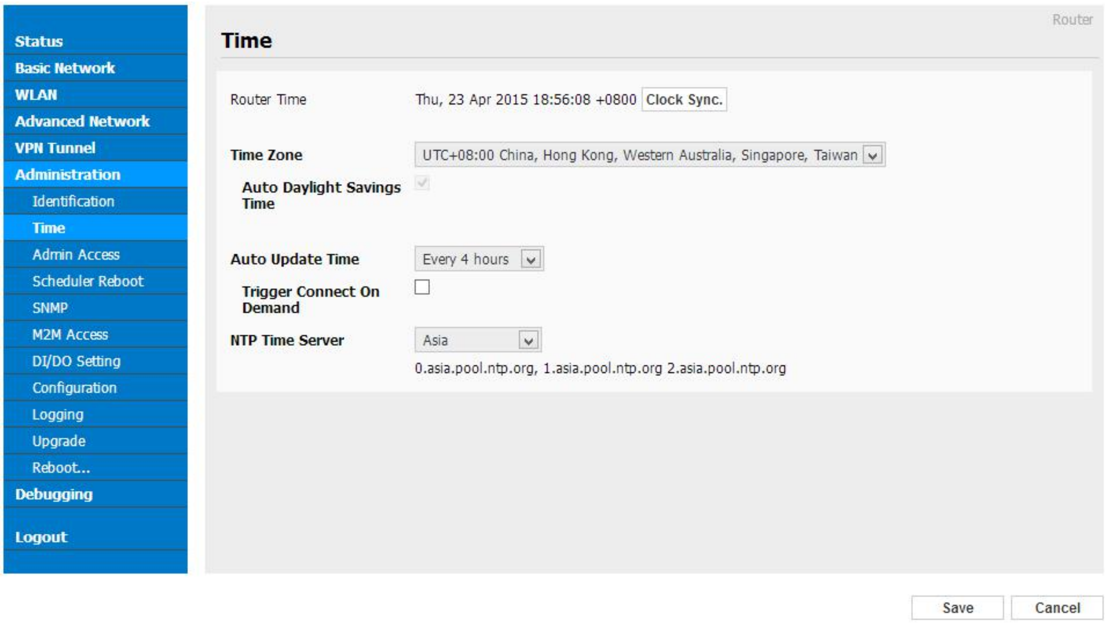
Parameter	Instruction
Router name	Default is router, can be set　maximum 32 character
Host name	Default is router, can be set　maximum 32 character
Domain name	Default is empty, support maximum up to 32 character, it is the domain of WAN, no need to configure for most application.

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.



Time

Router Time Thu, 23 Apr 2015 18:56:08 +0800

Time Zone UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan

Auto Daylight Savings Time ☑

Auto Update Time Every 4 hours

Trigger Connect On Demand □

NTP Time Server Asia

0.asia.pool.ntp.org, 1.asia.pool.ntp.org 2.asia.pool.ntp.org

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

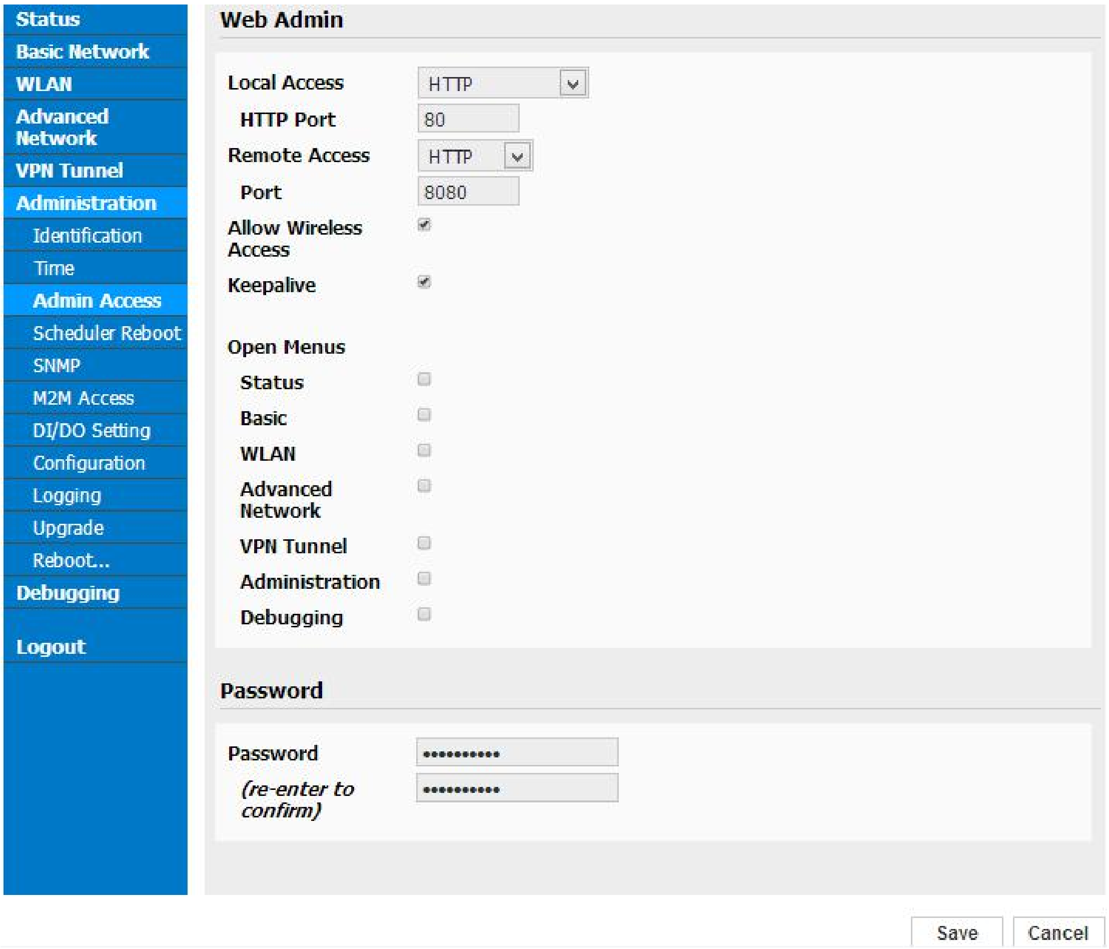
Step 1 Please click “Administrator>Admin” to check and modify relevant parameter.

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



Web Admin

Local Access	HTTP
HTTP Port	80
Remote Access	HTTP
Port	8080
Allow Wireless Access	☑
Keepalive	☑

Open Menus

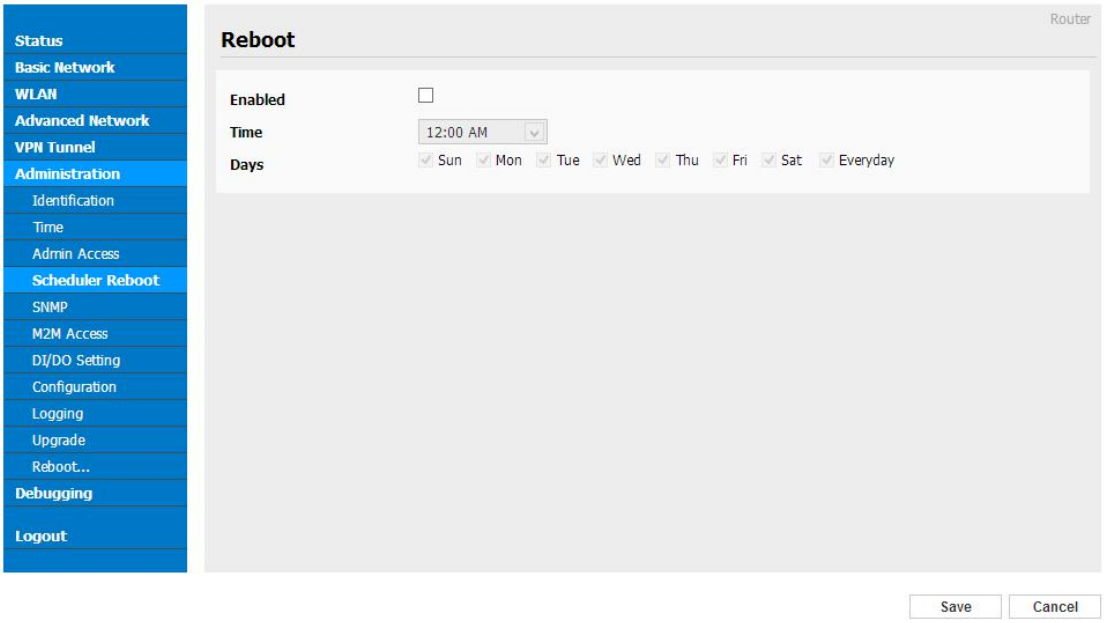
Status	□
Basic	□
WLAN	□
Advanced Network	□
VPN Tunnel	□
Administration	□
Debugging	□

Password

Password	••••••••••
(re-enter to confirm)	••••••••••

3.7.4 Schedule Reboot Setting

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



Reboot

Enabled □

Time 12:00 AM

Days ✓ Sun ✓ Mon ✓ Tue ✓ Wed ✓ Thu ✓ Fri ✓ Sat ✓ Everyday

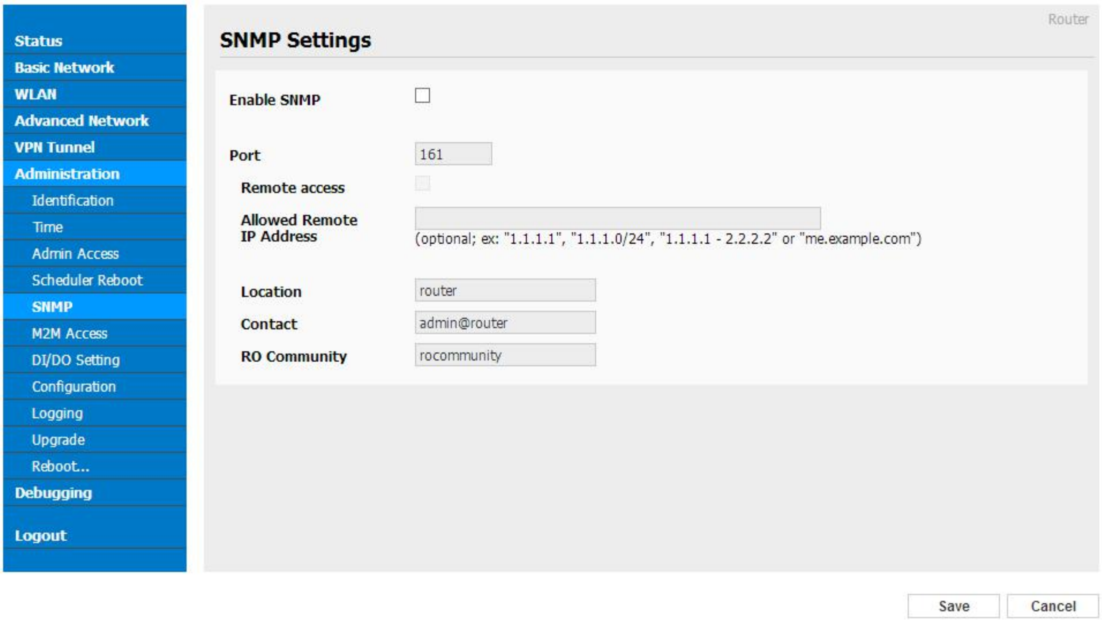
Figure 3-26 Scheduler Reboot Setting GUI

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.



SNMP Settings

Enable SNMP □

Port 161

Remote access □

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

Location router

Contact admin@router

RO Community rocommunity

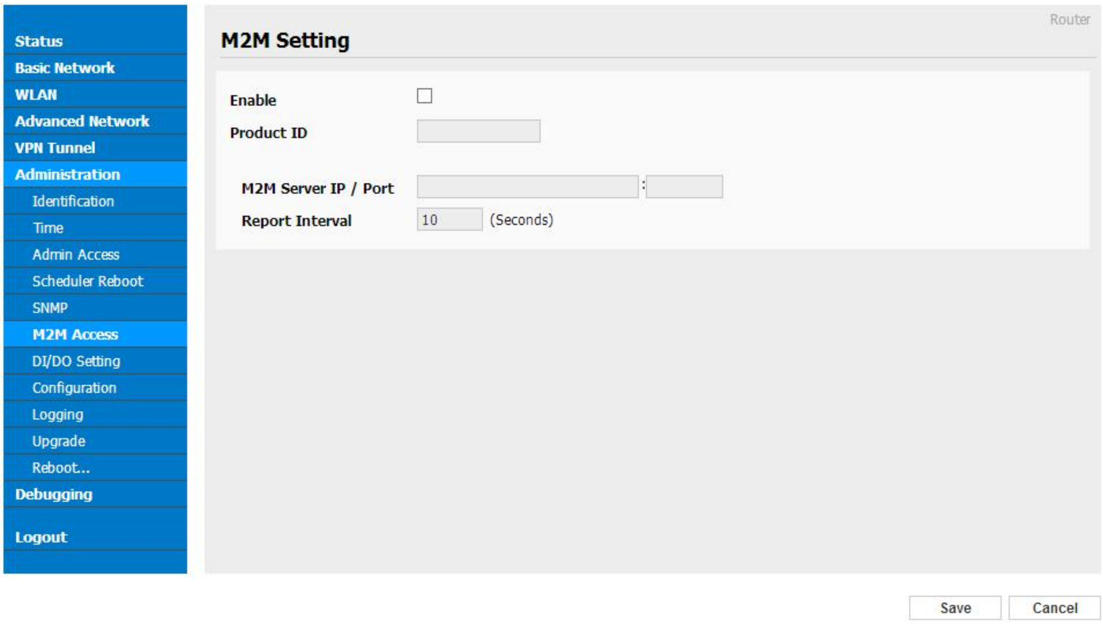
Figure 3-27 SNMP Setting GUI

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.



M2M Setting

Enable □

Product ID

M2M Server IP / Port :

Report Interval 10 (Seconds)

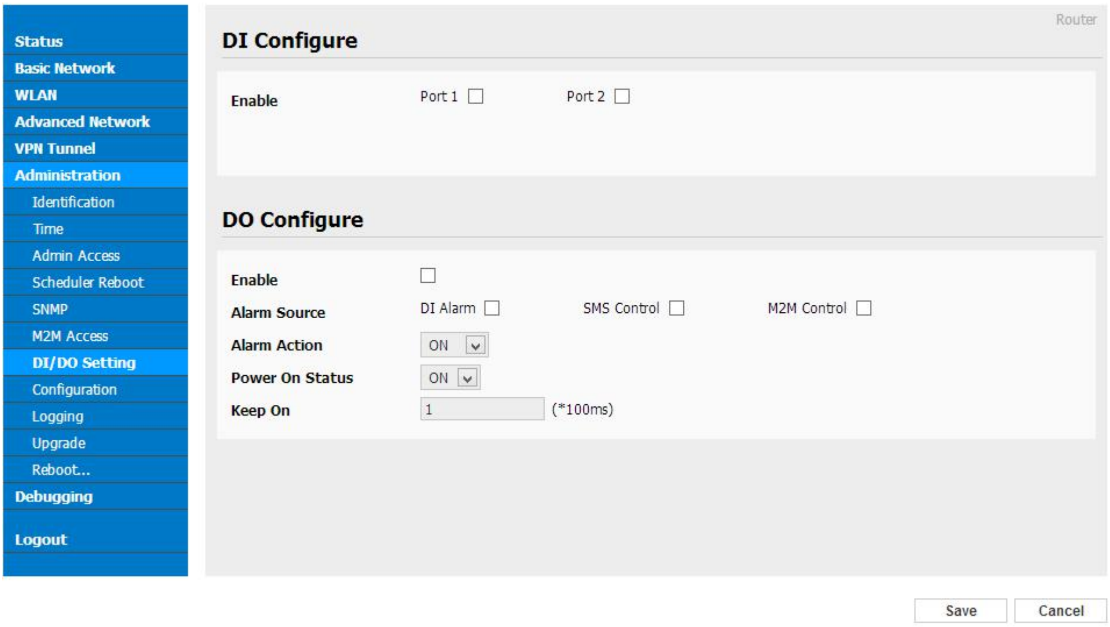
Figure 3-28 M2M Access Setting GUI

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.



DI Configure

Enable Port 1 □ Port 2 □

DO Configure

Enable □

Alarm Source DI Alarm □ SMS Control □ M2M Control □

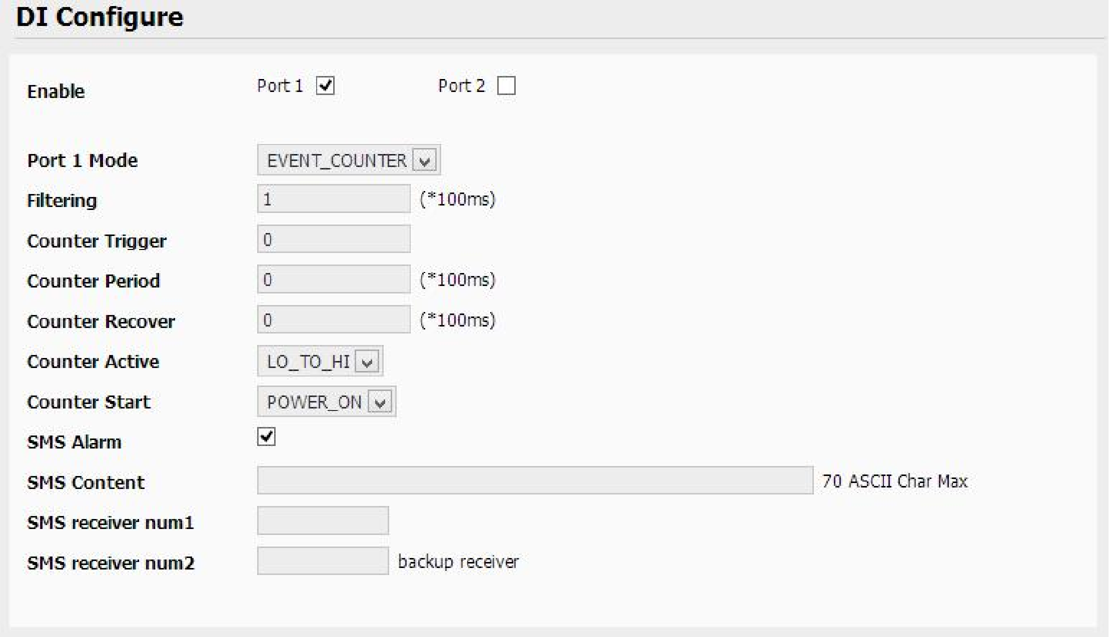
Alarm Action ON

Power On Status ON

Keep On 1 (*100ms)

Figure 3-29 DI/DO Setting GUI

3.6.7.1 DI Configure



DI Configure

Enable	Port 1 ☑ Port 2 □
Port 1 Mode	EVENT_COUNTER
Filtering	1 (*100ms)
Counter Trigger	0
Counter Period	0 (*100ms)
Counter Recover	0 (*100ms)
Counter Active	LO_TO_HI
Counter Start	POWER_ON
SMS Alarm	☑
SMS Content	70 ASCII Char Max
SMS receiver num1	
SMS receiver num2	backup receiver

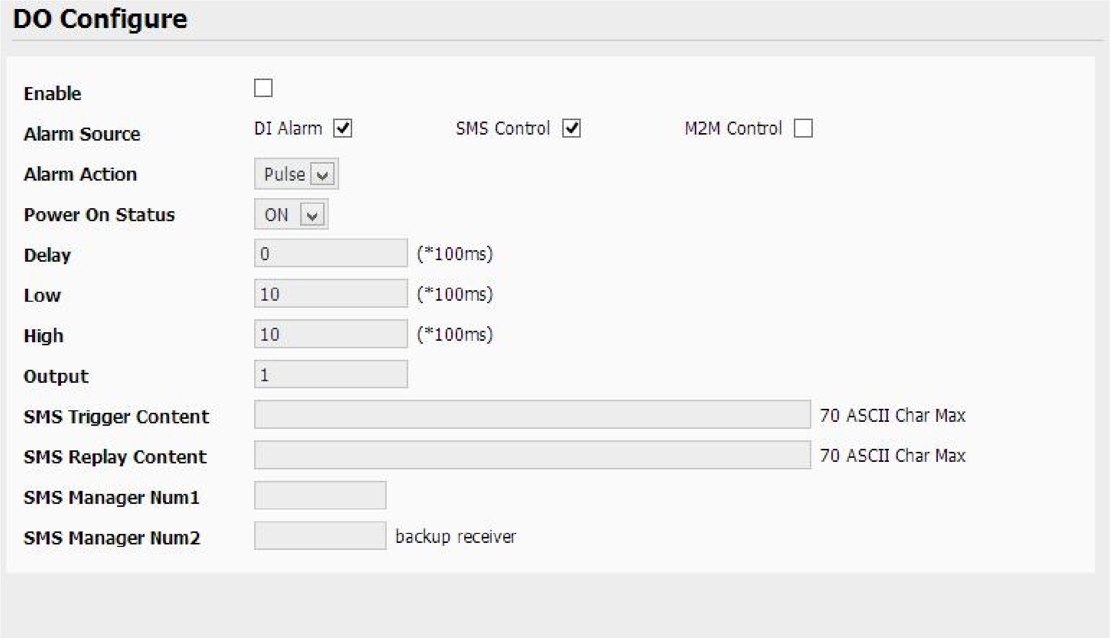
Table 3-26 "DI" Instruction

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-R210 detects pulse signal and compares with first pulse shape and last pulse shape. If both are the same level, WL-R210 will trigger alarm. Under EVENT_COUNTER mode, if first pulse shape and last pulse shape are not the same level, WL-R210 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



DO Configure

Enable	□
Alarm Source	DI Alarm ☑ SMS Control ☑ M2M Control □
Alarm Action	Pulse
Power On Status	ON
Delay	0 (*100ms)
Low	10 (*100ms)
High	10 (*100ms)
Output	1
SMS Trigger Content	70 ASCII Char Max
SMS Replay Content	70 ASCII Char Max
SMS Manager Num1	
SMS Manager Num2	backup receiver

Table 3-27 “DO” Instruction

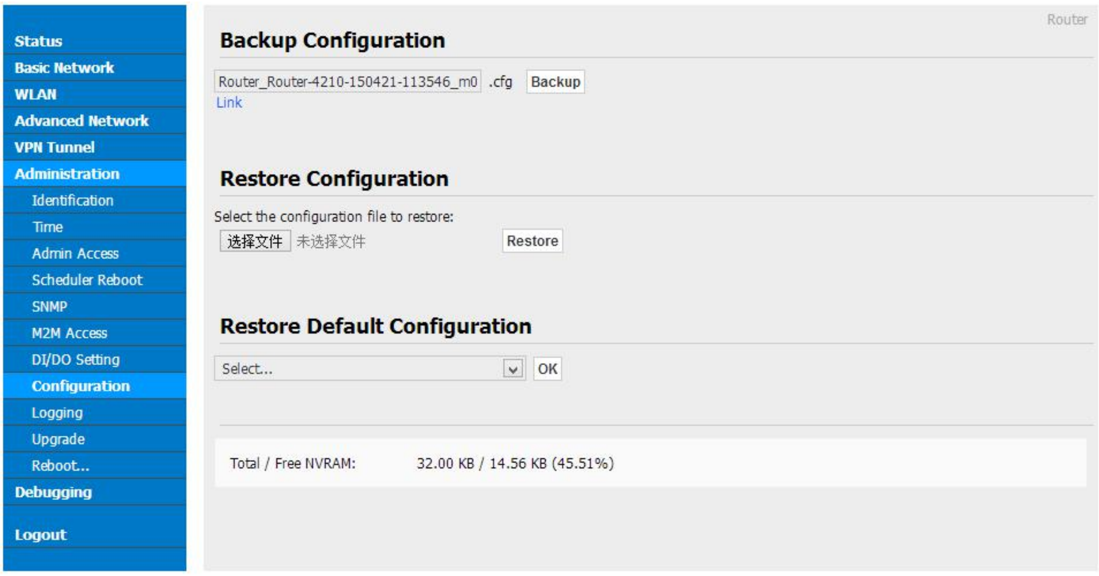
Parameter	Instruction
Enable	1 DO as selected
Alarm Source	Digital output initiates according to different alarm source. Select from DI Alarm, SMS Control and M2M Control. Selections can be one or more. DI Alarm: Digital Output triggers the related action when there is alarm from Digital Input. SMS Control: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



Backup Configuration

Router_Router-4210-150421-113546_m0 .cfg Backup
Link

Restore Configuration

Select the configuration file to restore:
选择文件 未选择文件 Restore

Restore Default Configuration

Select... OK

Total / Free NVRAM: 32.00 KB / 14.56 KB (45.51%)

Figure 3-30 Backup and Restore Configuration GUI

CAUTION

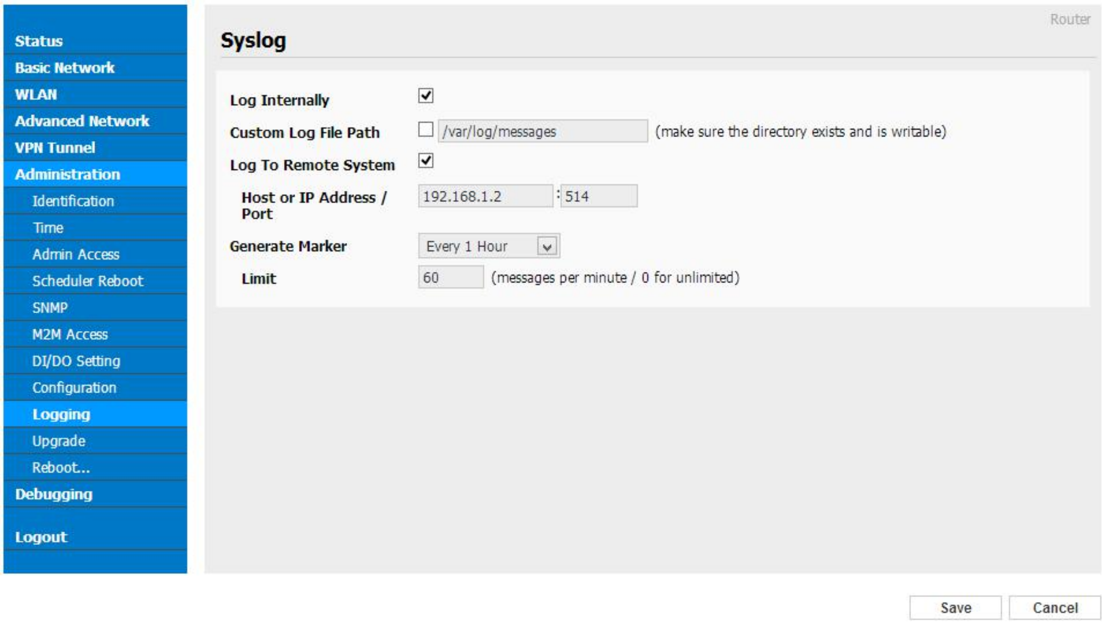
Restore Default would lose all configuration information, please be careful.

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).



Syslog

Log Internally	☑
Custom Log File Path	□ /var/log/messages (make sure the directory exists and is writable)
Log To Remote System	☑
Host or IP Address / Port	192.168.1.2 : 514
Generate Marker	Every 1 Hour
Limit	60 (messages per minute / 0 for unlimited)

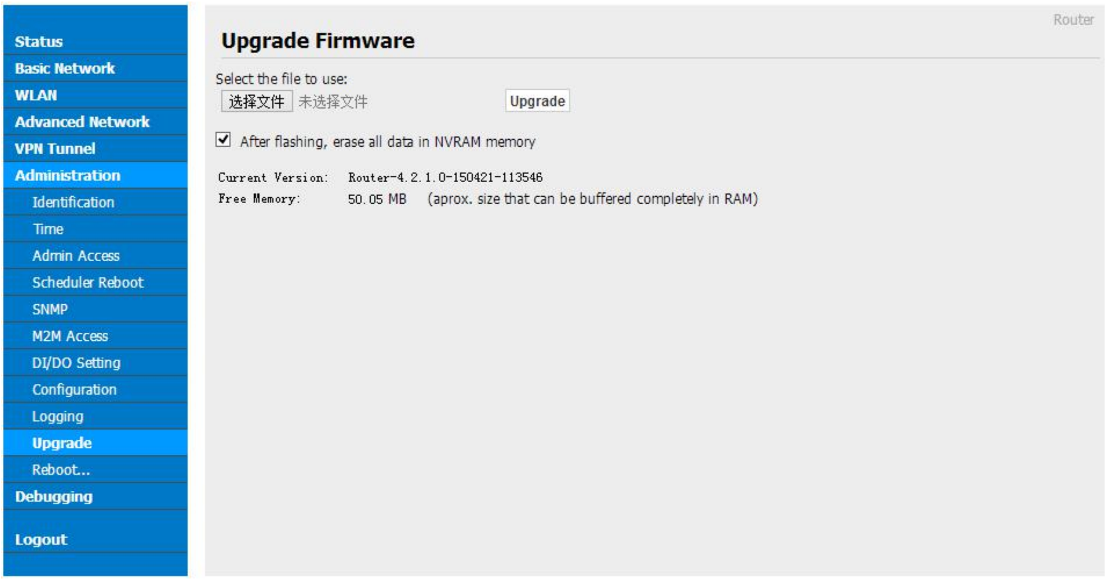
Figure 3-31 System log Setting GUI

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.



Upgrade Firmware

Select the file to use:

选择文件 未选择文件 Upgrade

☑ After flashing, erase all data in NVRAM memory

```
Current Version:  Router-4.2.1.0-150421-113546
Free Memory:      50.05 MB   (aprox. size that can be buffered completely in RAM)
```

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.

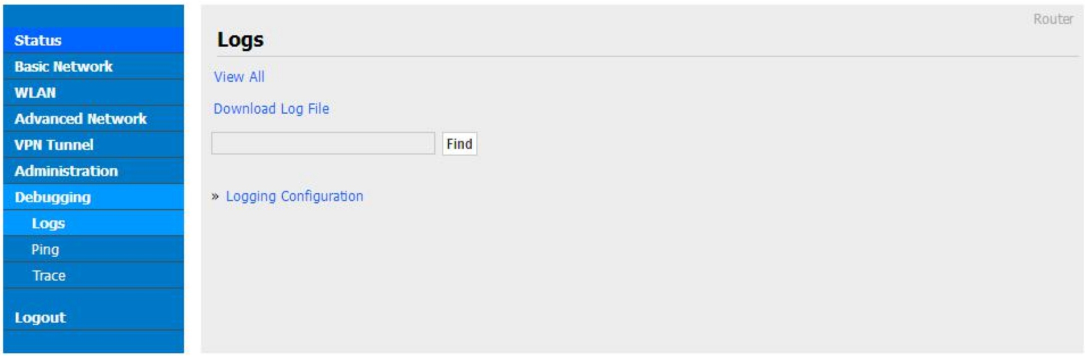
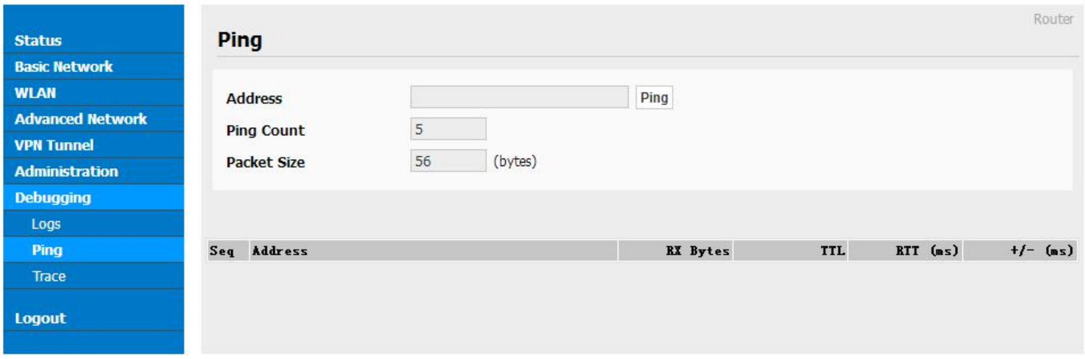


Figure 3-33 Logs GUI

----End

3.8.2 Ping Setting

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



Address
Ping Count 5
Packet Size 56 (bytes)

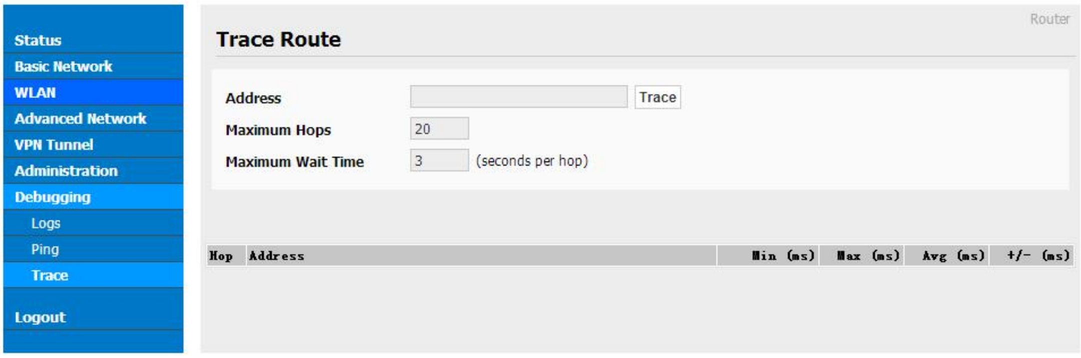
Seq	Address	RX Bytes	TTL	RTT (ms)	+/- (ms)

Figure 3-34 Ping GUI

----End

3.8.3 Trace Setting

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



Address
Maximum Hops 20
Maximum Wait Time 3 (seconds per hop)

Hop	Address	Min (ms)	Max (ms)	Avg (ms)	+/- (ms)

Figure 3-35 Trace GUI

----End

4 Configuration Instance

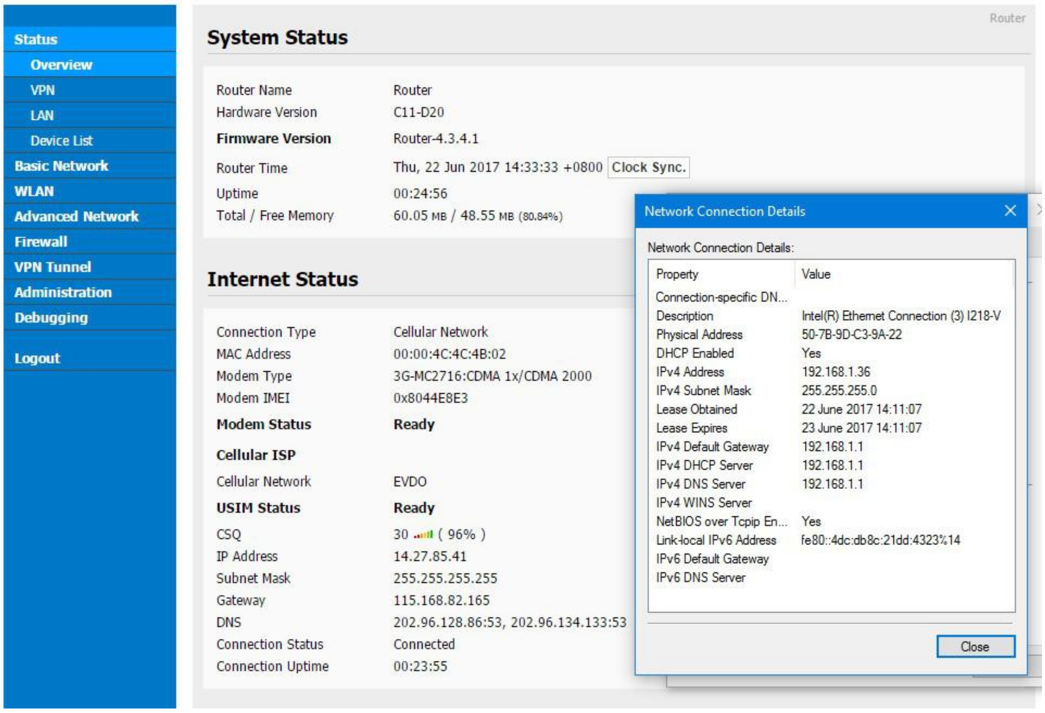
This chapter is mainly for configured test case, there would be some difference between the scheme and real object. But the difference doesn't have any influence to products performance.

4.1 Port Forwarding

1) The router online and got a public IP address 14.27.85.41

Note: It's based on SIM card carrier

2) The PC is connected to router and got IP address 192.168.1.36



System Status

Router Name	Router
Hardware Version	C11-D20
Firmware Version	Router-4.3.4.1
Router Time	Thu, 22 Jun 2017 14:33:33 +0800
Uptime	00:24:56
Total / Free Memory	60.05 MB / 48.55 MB (80.84%)

Internet Status

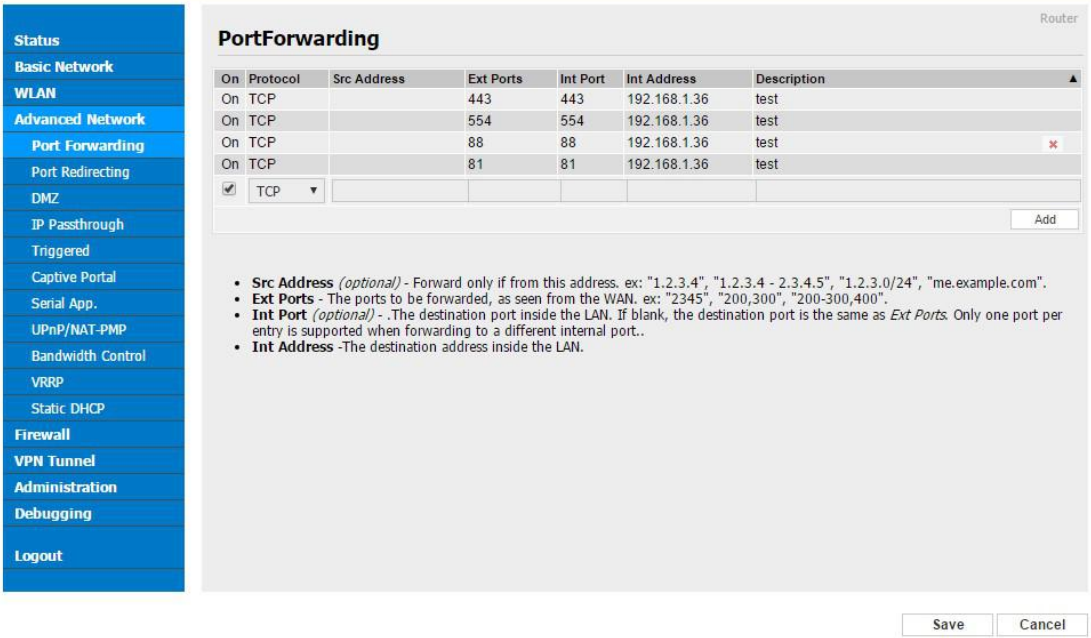
Connection Type	Cellular Network
MAC Address	00:00:4C:4C:4B:02
Modem Type	3G-MC2716:CDMA 1x/CDMA 2000
Modem IMEI	0x8044E8E3
Modem Status	**Ready**
Cellular ISP	
Cellular Network	EVDO
USIM Status	**Ready**
CSQ	30 (96%)
IP Address	14.27.85.41
Subnet Mask	255.255.255.255
Gateway	115.168.82.165
DNS	202.96.128.86:53, 202.96.134.133:53
Connection Status	Connected
Connection Uptime	00:23:55

Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) Ethernet Connection (3) I218-V
Physical Address	50-7B-9D-C3-9A-22
DHCP Enabled	Yes
IPv4 Address	192.168.1.36
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	22 June 2017 14:11:07
Lease Expires	23 June 2017 14:11:07
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::4dc:db8c:21dd:4323%14
IPv6 Default Gateway	
IPv6 DNS Server	

3) Configuration



PortForwarding

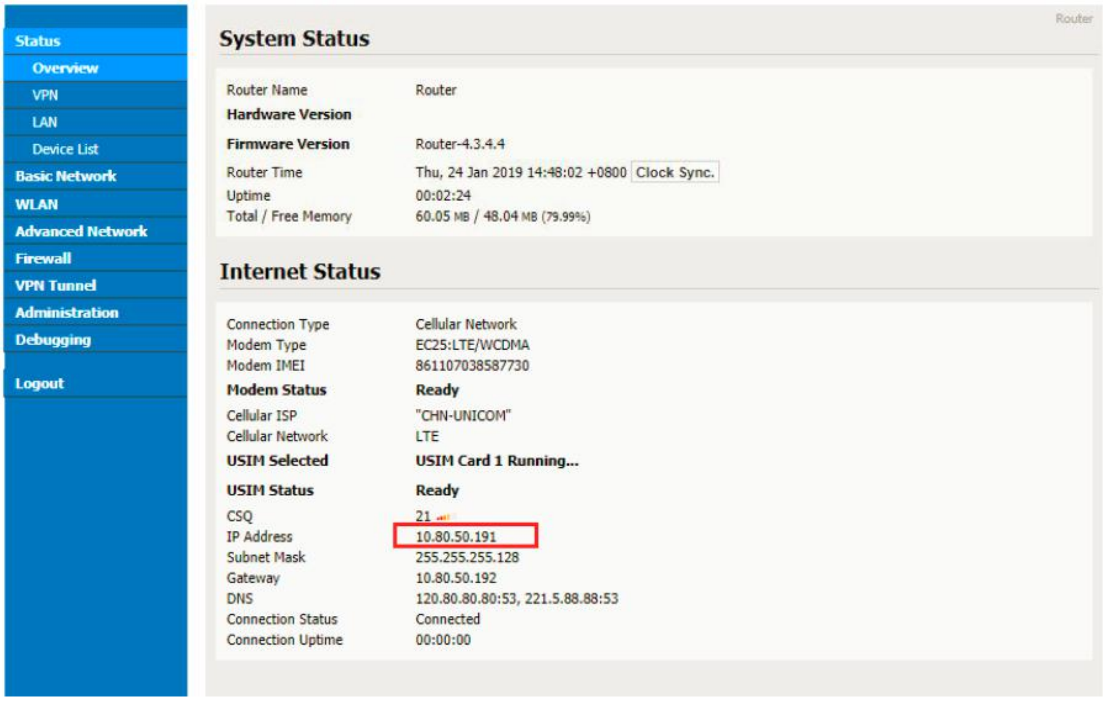
On	Protocol	Src Address	Ext Ports	Int Port	Int Address	Description
On	TCP		443	443	192.168.1.36	test
On	TCP		554	554	192.168.1.36	test
On	TCP		88	88	192.168.1.36	test
On	TCP		81	81	192.168.1.36	test
☑	TCP ▾					

- **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.

4) The PC can be accessed via 14.27.85.41:443 over Internet

4.2 IP Passthrough

1) The router online



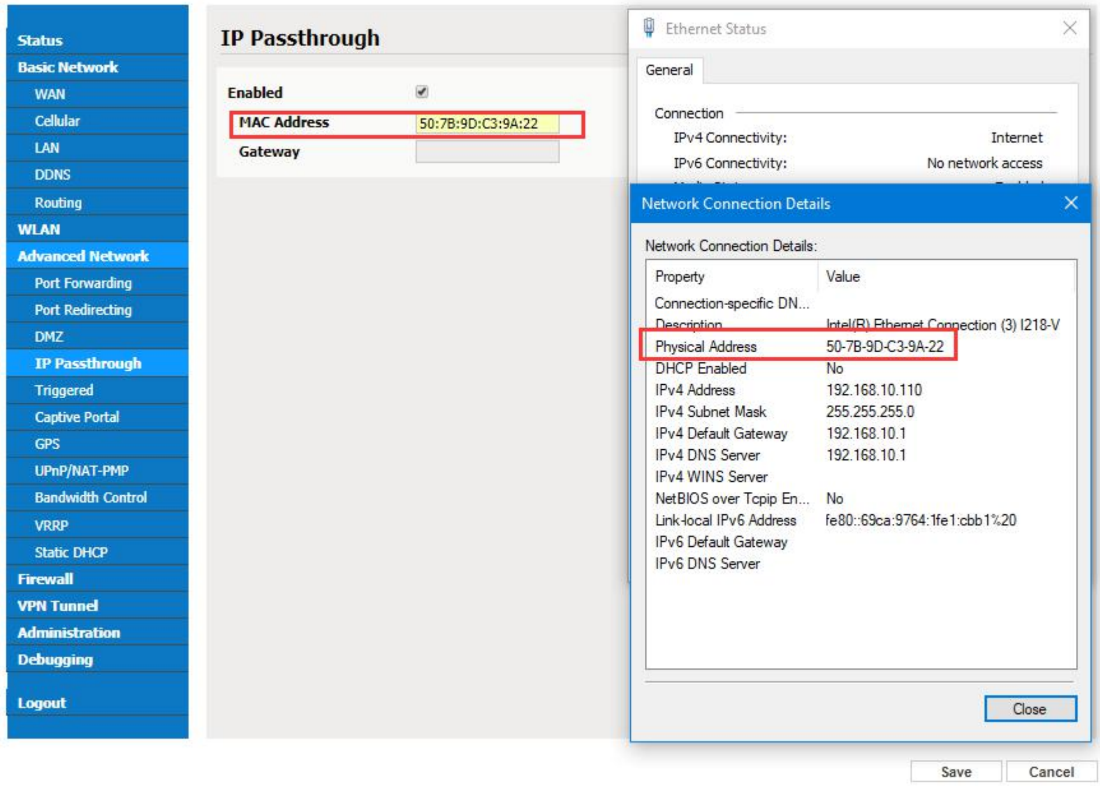
System Status

Router Name	Router
Hardware Version	
Firmware Version	Router-4.3.4.4
Router Time	Thu, 24 Jan 2019 14:48:02 +0800
Uptime	00:02:24
Total / Free Memory	60.05 MB / 48.04 MB (79.99%)

Internet Status

Connection Type	Cellular Network
Modem Type	EC25:LTE/WCDMA
Modem IMEI	861107038587730
Modem Status	**Ready**
Cellular ISP	"CHN-UNICOM"
Cellular Network	LTE
USIM Selected	**USIM Card 1 Running...**
USIM Status	**Ready**
CSQ	21
IP Address	10.80.50.191
Subnet Mask	255.255.255.128
Gateway	10.80.50.192
DNS	120.80.80.80:53, 221.5.88.88:53
Connection Status	Connected
Connection Uptime	00:00:00

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



IP Passthrough

Enabled ☑

MAC Address 50:7B:9D:C3:9A:22

Gateway

Ethernet Status

General

Connection

IPv4 Connectivity: Internet

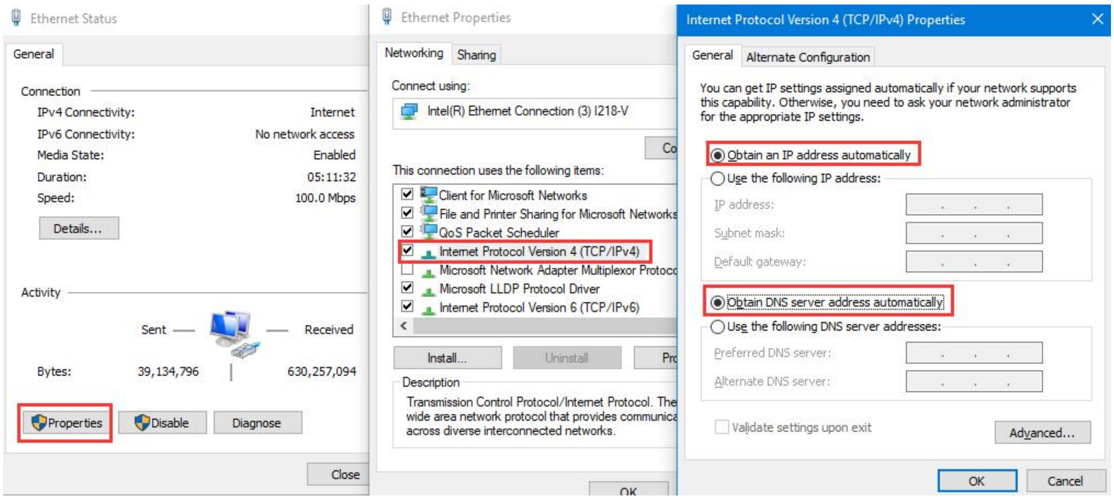
IPv6 Connectivity: No network access

Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) Ethernet Connection (3) I218-V
Physical Address	50-7B-9D-C3-9A-22
DHCP Enabled	No
IPv4 Address	192.168.10.110
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.10.1
IPv4 DNS Server	192.168.10.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	No
Link-local IPv6 Address	fe80::69ca:9764:1fe1:cbb1%20
IPv6 Default Gateway	
IPv6 DNS Server	

3) Set the PC to DHCP



Ethernet Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 05:11:32

Speed: 100.0 Mbps

Activity

Sent — Received

Bytes: 39,134,796 | 630,257,094

Ethernet Properties

Networking Sharing

Connect using:

Intel(R) Ethernet Connection (3) I218-V

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protoco
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The wide area network protocol that provides communica across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

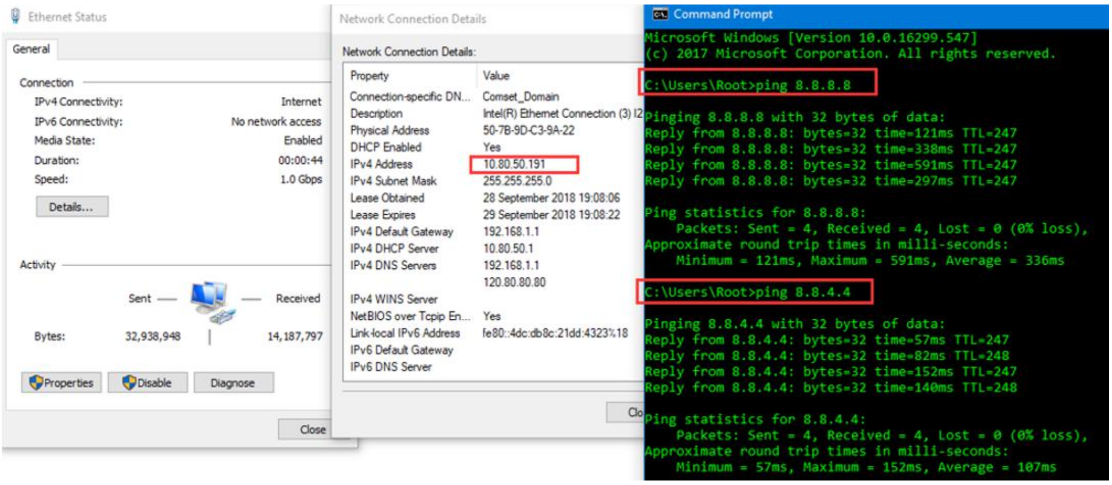
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

4) Check the Ethernet status and ping test



Ethernet Status

General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:00:44
Speed:	1.0 Gbps

Activity

	Sent	Received
Bytes:	32,938,948	14,187,797

Network Connection Details

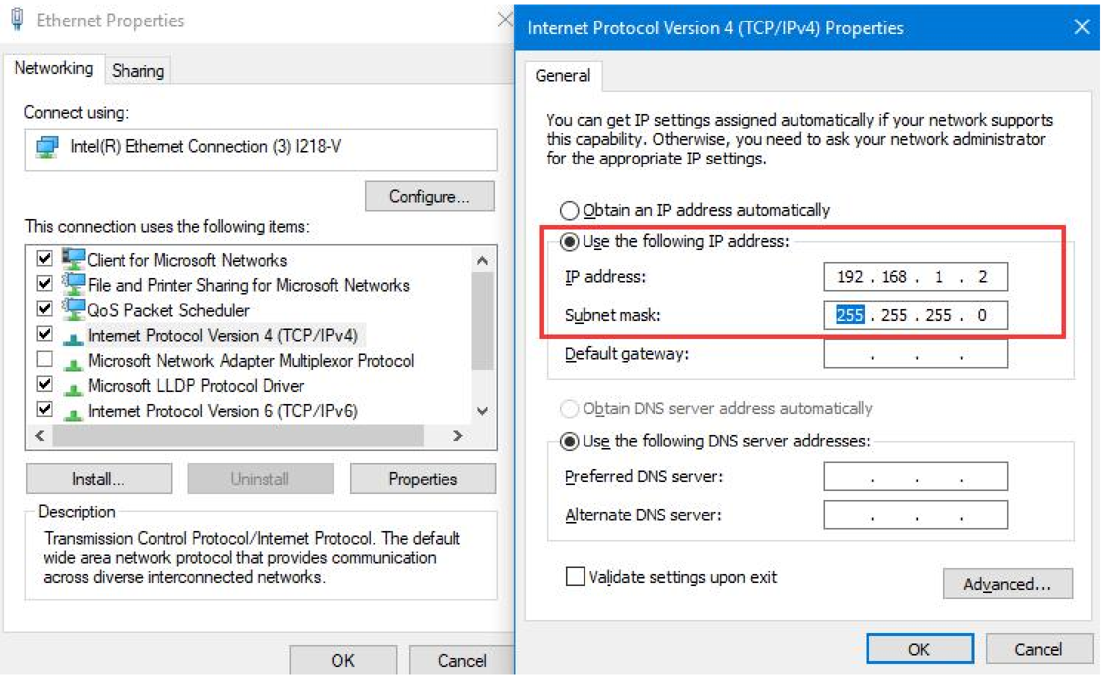
Network Connection Details:

Property	Value
Connection-specific DN...	Comset_Domain
Description	Intel(R) Ethernet Connection (3) I2
Physical Address	50-7B-9D-C3-9A-22
DHCP Enabled	Yes
IPv4 Address	10.80.50.191
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	28 September 2018 19:08:06
Lease Expires	29 September 2018 19:08:22
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	10.80.50.1
IPv4 DNS Servers	192.168.1.1 120.80.80.80
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::4dc:db8c:21dd:4323%18
IPv6 Default Gateway	
IPv6 DNS Server	

Command Prompt

```
Microsoft Windows [Version 10.0.16299.547]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Root>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=121ms TTL=247
Reply from 8.8.8.8: bytes=32 time=338ms TTL=247
Reply from 8.8.8.8: bytes=32 time=591ms TTL=247
Reply from 8.8.8.8: bytes=32 time=297ms TTL=247

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 121ms, Maximum = 591ms, Average = 336ms

C:\Users\Root>ping 8.8.4.4

Pinging 8.8.4.4 with 32 bytes of data:
Reply from 8.8.4.4: bytes=32 time=57ms TTL=247
Reply from 8.8.4.4: bytes=32 time=82ms TTL=248
Reply from 8.8.4.4: bytes=32 time=152ms TTL=247
Reply from 8.8.4.4: bytes=32 time=140ms TTL=248

Ping statistics for 8.8.4.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 152ms, Average = 107ms
```

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



Ethernet Properties

Networking | Sharing

Connect using:

Intel(R) Ethernet Connection (3) I218-V

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

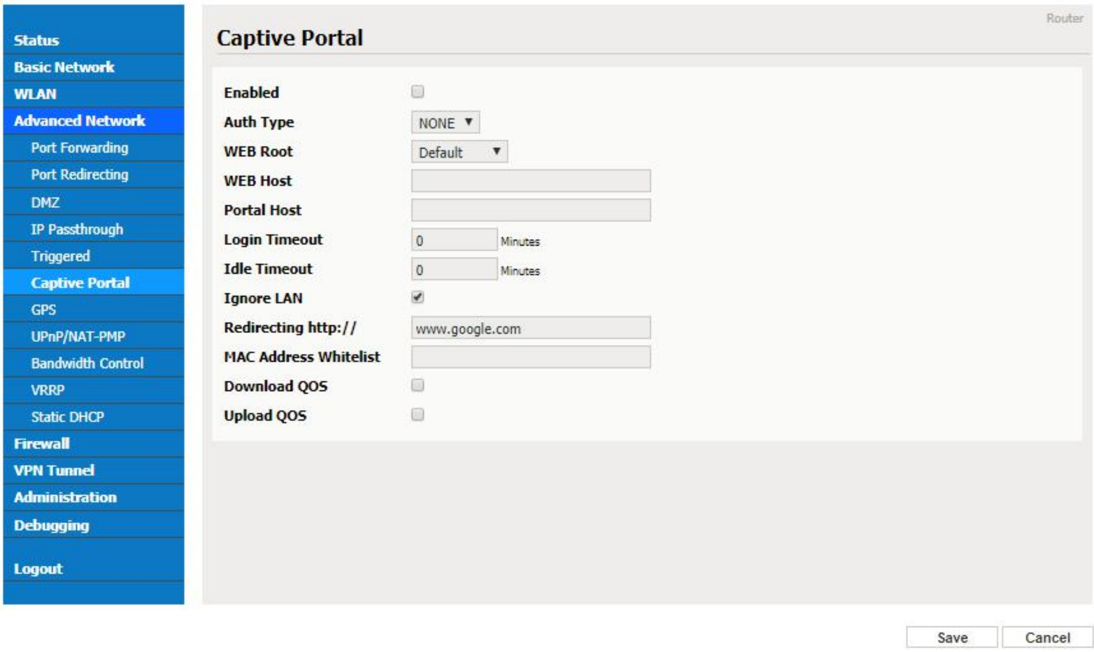
Preferred DNS server:	. . .
Alternate DNS server:	. . .

☐ Validate settings upon exit

4.3 Captive Portal

This feature is suitable for Wi-Fi captive portal

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



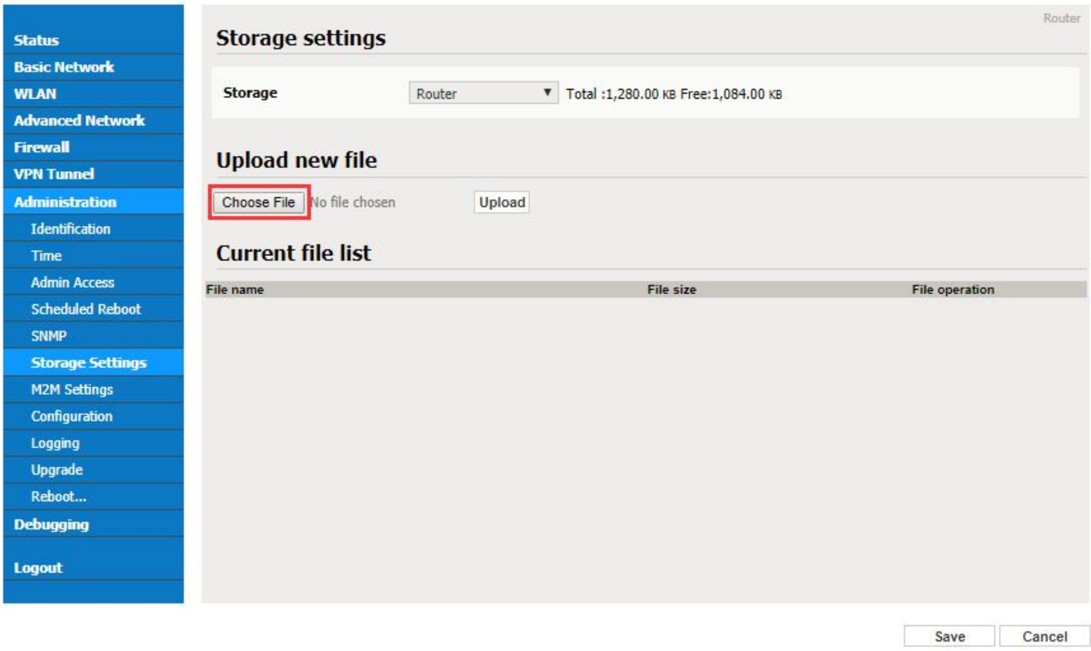
Captive Portal

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	☐

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.



Storage settings

Storage: Router — Total :1,280.00 KB Free:1,084.00 KB

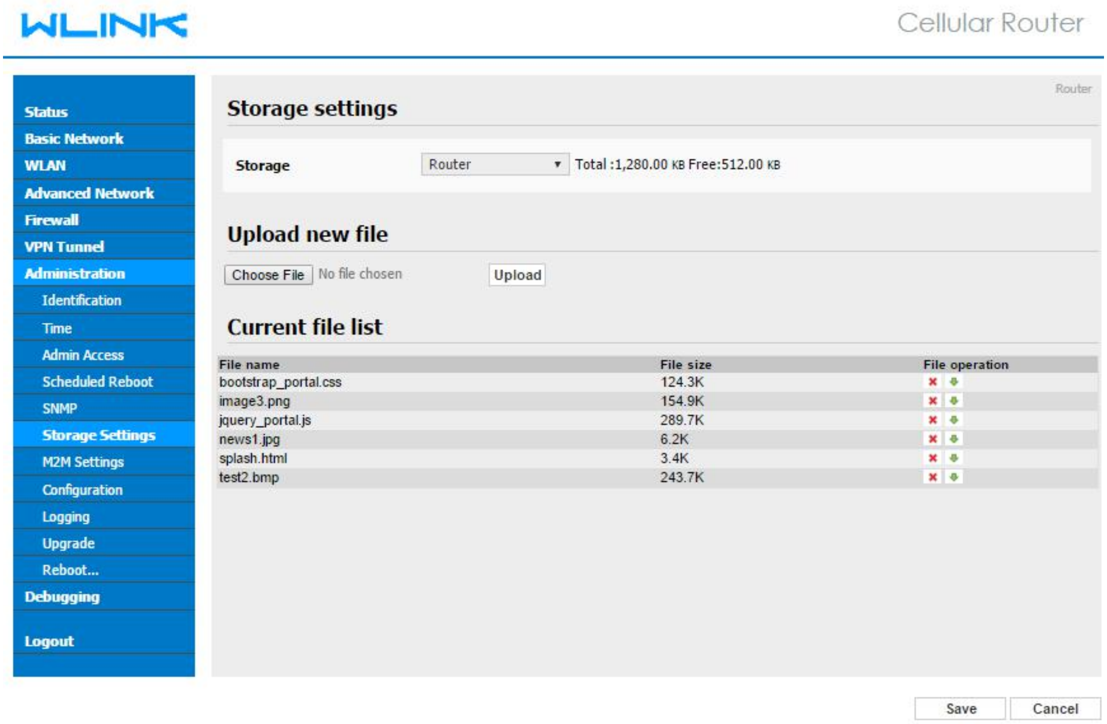
Upload new file

Choose File No file chosen Upload

Current file list

File name	File size	File operation

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.



Storage settings

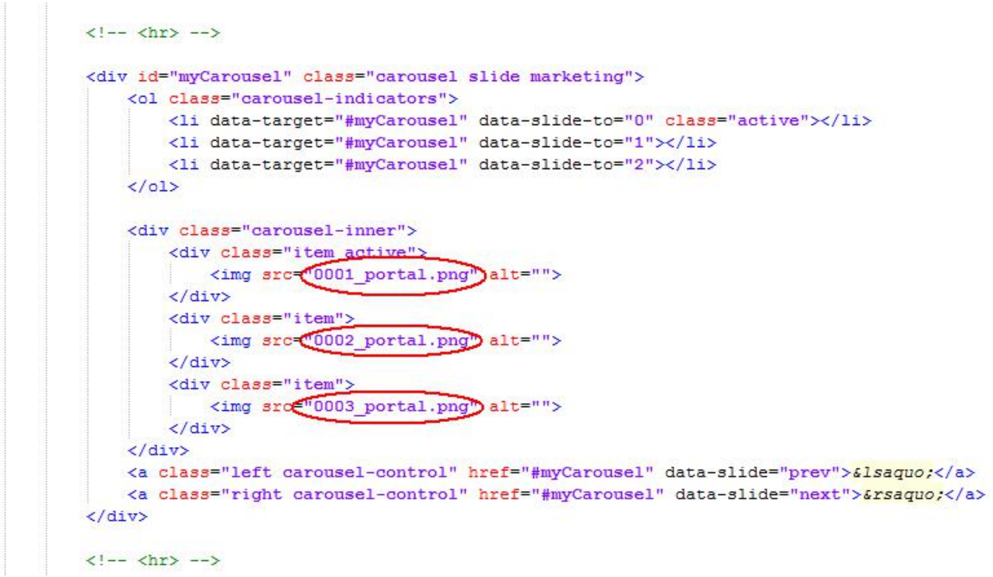
Storage: Router ▾ Total :1,280.00 KB Free:512.00 KB

Upload new file

No file chosen

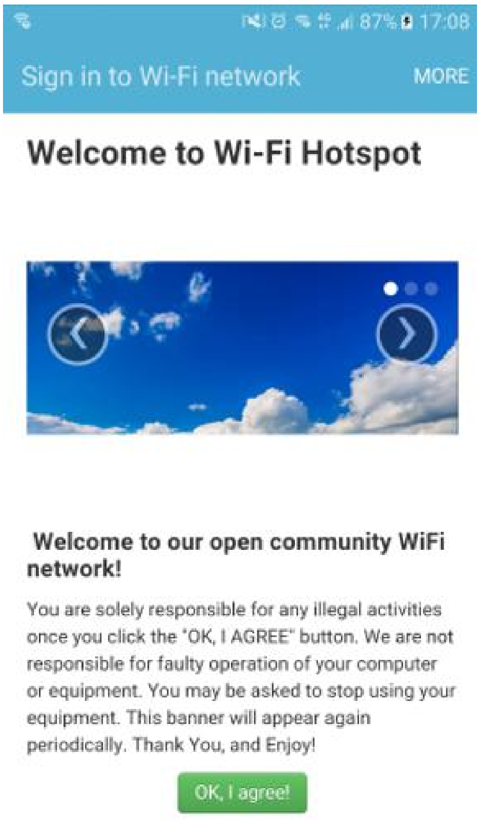
Current file list

File name	File size	File operation
bootstrap_portal.css	124.3K	✗ ↓
image3.png	154.9K	✗ ↓
jquery_portal.js	289.7K	✗ ↓
news1.jpg	6.2K	✗ ↓
splash.html	3.4K	✗ ↓
test2.bmp	243.7K	✗ ↓



```
<!-- <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



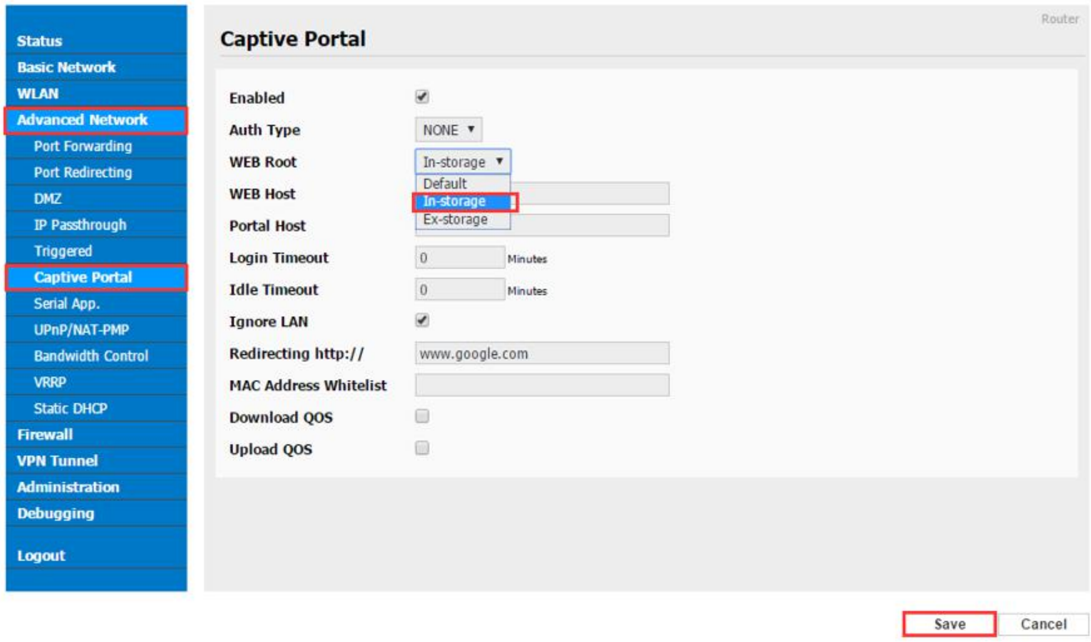
Welcome to Wi-Fi Hotspot

Welcome to our open community WiFi network!

You are solely responsible for any illegal activities once you click the "OK, I AGREE" button. We are not responsible for faulty operation of your computer or equipment. You may be asked to stop using your equipment. This banner will appear again periodically. Thank You, and Enjoy!

2）Modify portal file storage path

Modify portal file storage for In-storage as below.



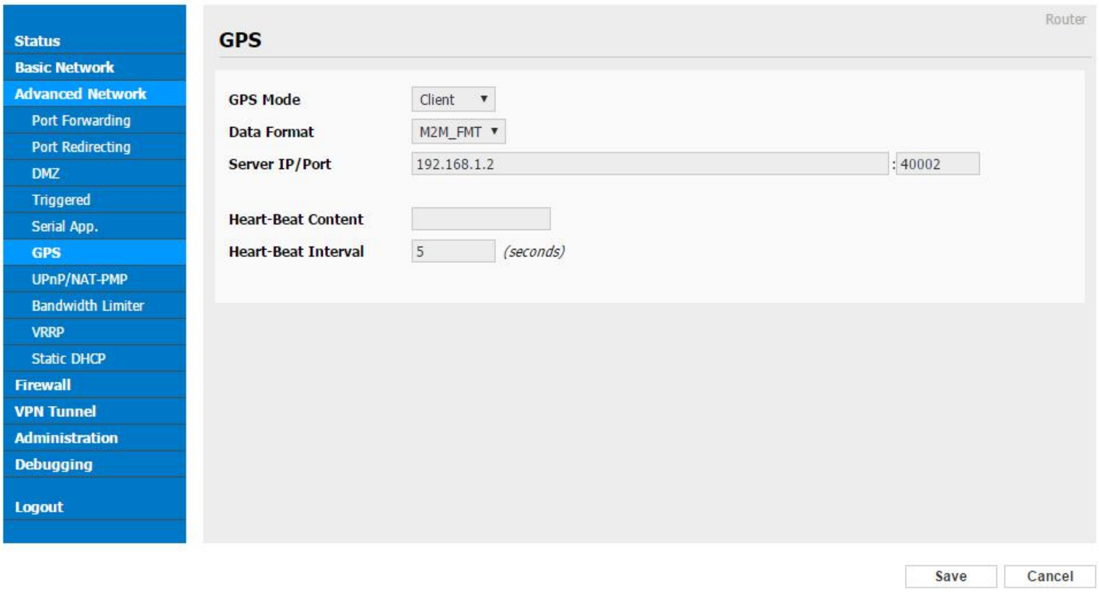
Captive Portal

Enabled	☑
Auth Type	NONE
WEB Root	In-storage (Default / In-storage / Ex-storage)
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	□

4.4 GPS Settings

The feature is requested hardware supports GPS feature.

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



GPS

GPS Mode: Client

Data Format: M2M_FMT

Server IP/Port: 192.168.1.2 : 40002

Heart-Beat Content:

Heart-Beat Interval: 5 (seconds)

Figure 4-5 GPS GUI

Table 4-5 “GPS” Instruction

	Instruction
GPS Mode	Enable/Disable
GPS Format	NMEA and M2M_FMT(WLINK)
Server IP/Port	GPS server IP and port
Heart-Beat	If choose M2M_FMT format, heart-beat ID will be packed into GPS data.
Interval	GPS data transmit as the interval time.

Step 2 Please click “save” to finis

Step 3 Connect the GPS antenna to router GPS interface

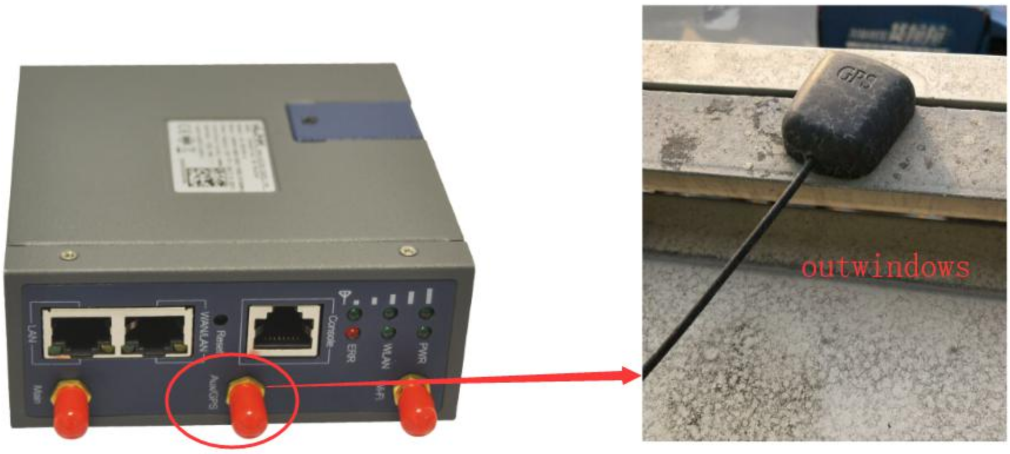
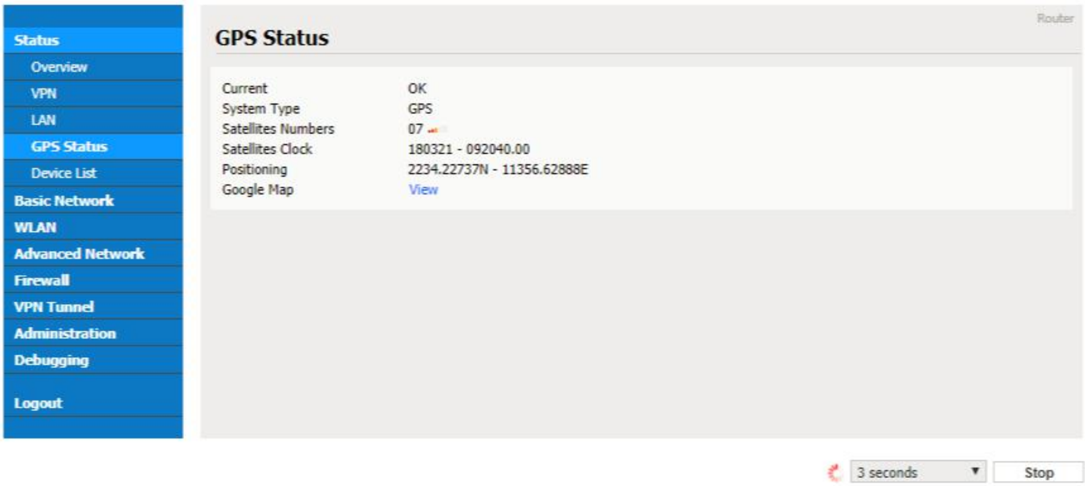


Figure 4-4 GPS Connection

Step 4 Check GPS Status



GPS Status

Current	OK
System Type	GPS
Satellites Numbers	07
Satellites Clock	180321 - 092040.00
Positioning	2234.22737N - 11356.62888E
Google Map	View

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.

4.5 Firewall

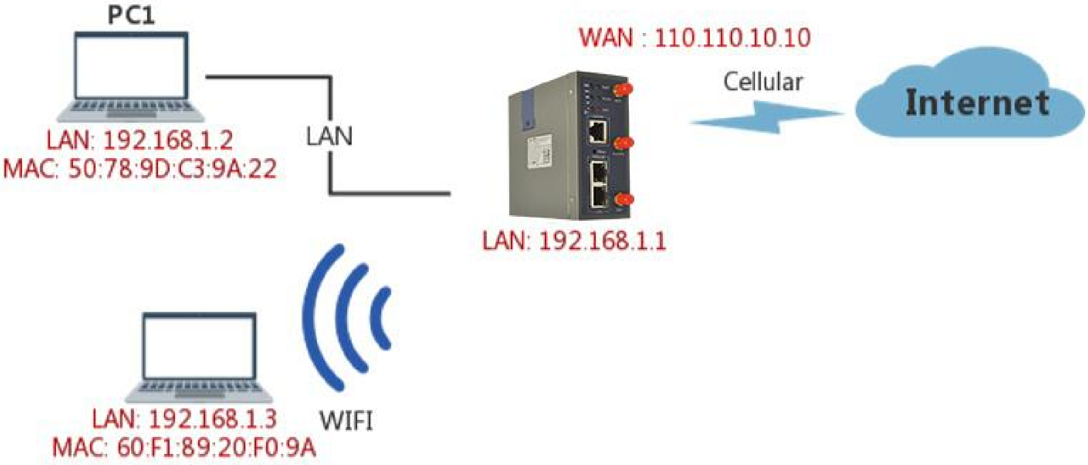


Figure 4-5 Firewall Network topology

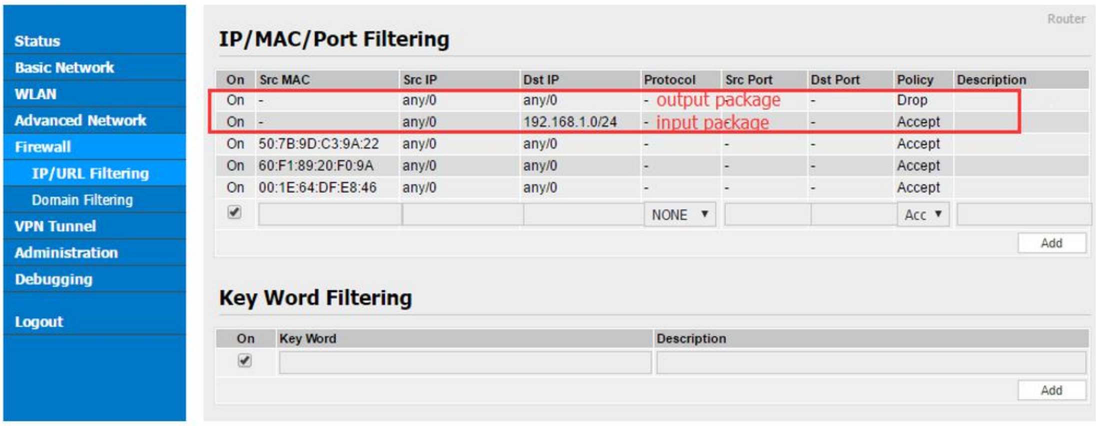
1) IP/MAC/Port Filtering

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)



IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
On	-	any/0	any/0	- output package		-	Drop	
On	-	any/0	192.168.1.0/24	- input package		-	Accept	
On	50:7B:9D:C3:9A:22	any/0	any/0	-	-	-	Accept	
On	60:F1:89:20:F0:9A	any/0	any/0	-	-	-	Accept	
On	00:1E:64:DF:E8:46	any/0	any/0	-	-	-	Accept	
☑				NONE ▾			Acc ▾	

Add

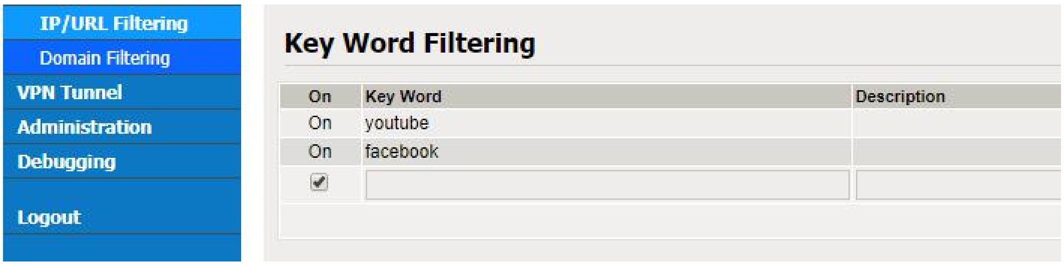
Key Word Filtering

On	Key Word	Description
☑		

Add

2) Key Word Filtering

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



Key Word Filtering

On	Key Word	Description
On	youtube	
On	facebook	
☑		

3) URL Filtering

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

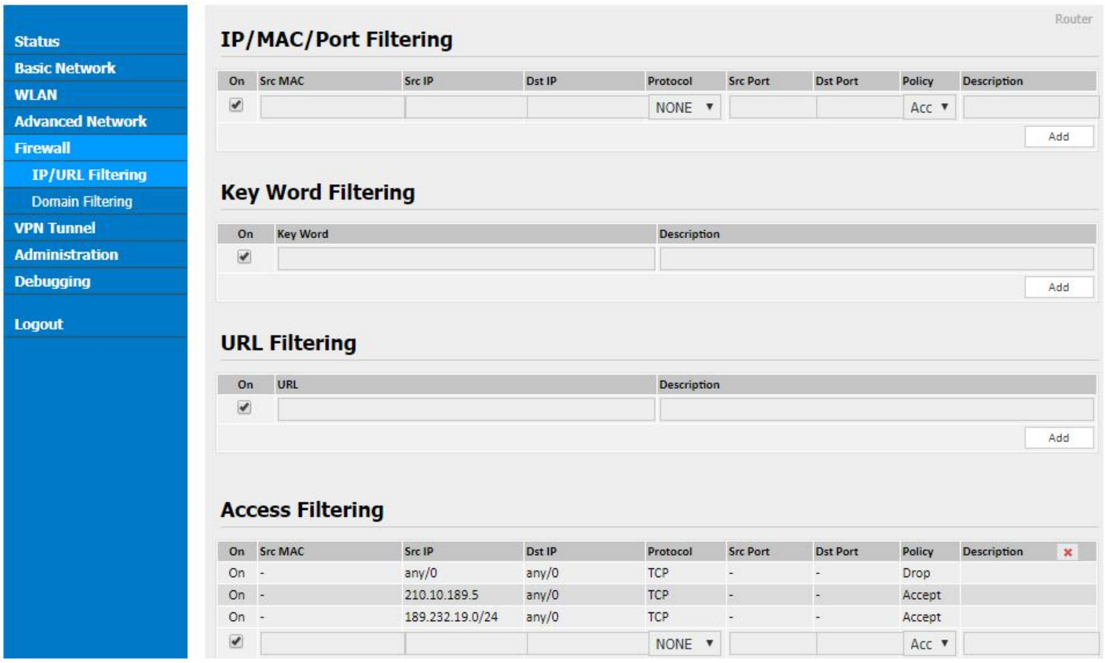
4) Access Filtering

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

Test case:

4.1) Reject all TCP access to the router.

4.2) Accept the source IP address to be accessed from Internet.



IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NONE ▼			Acc ▼	

Key Word Filtering

On	Key Word	Description
☑		

URL Filtering

On	URL	Description
☑		

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description ✖
On	-	any/0	any/0	TCP	-	-	Drop	
On	-	210.10.189.5	any/0	TCP	-	-	Accept	
On	-	189.232.19.0/24	any/0	TCP	-	-	Accept	
☑				NONE ▼			Acc ▼	

4.6 VPN Tunnel

4.6.1 GRE

GRE Tunnel between WL-R210 and WL-R200

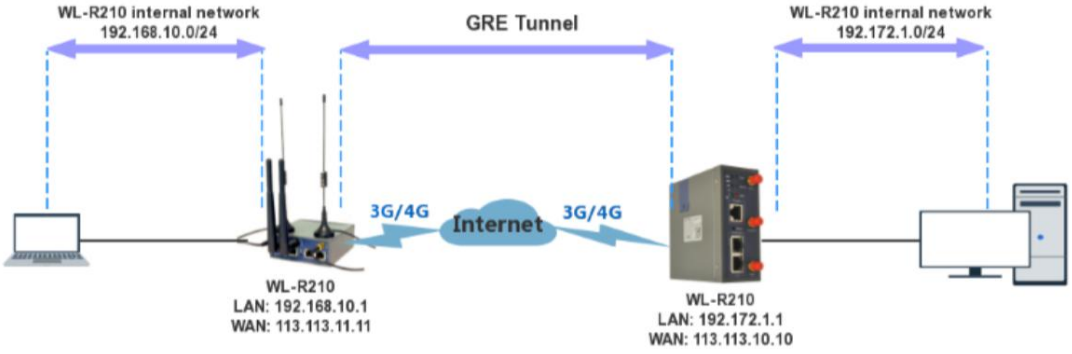
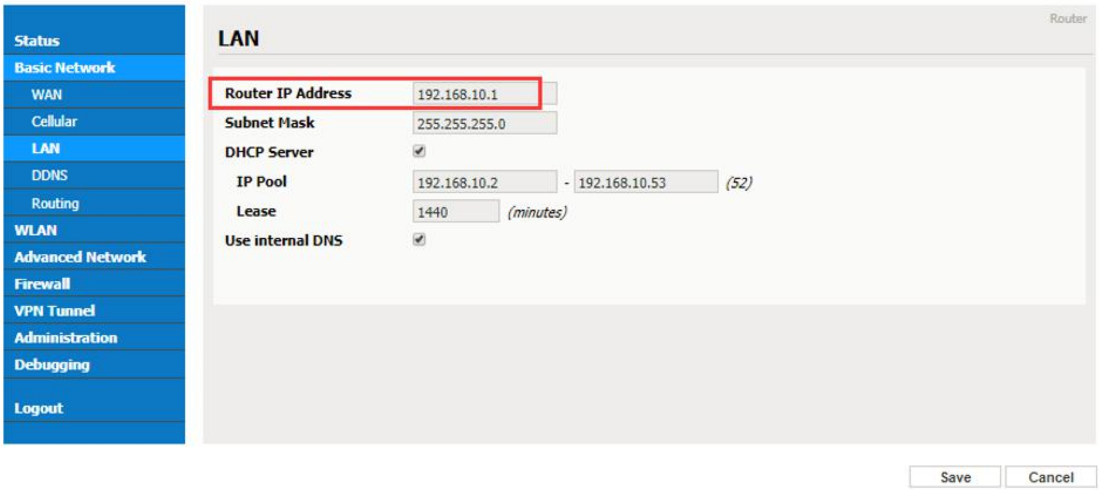


Figure 4-6-1 GRE Network topology

1) WL-R210 Config

1.1) Navigate to **Basic Network > LAN**



LAN

Router IP Address 192.168.10.1

Subnet Mask 255.255.255.0

DHCP Server ☑

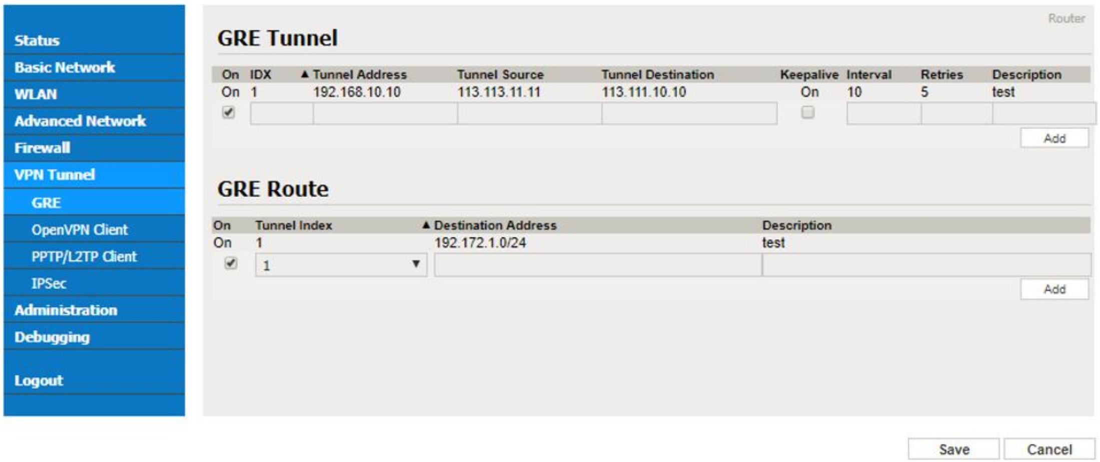
IP Pool 192.168.10.2 - 192.168.10.53 *(52)*

Lease 1440 *(minutes)*

Use internal DNS ☑

Save Cancel

1.2) Navigate to **VPN Tunnel > GRE**



GRE Tunnel

On	IDX	▲Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
On	1	192.168.10.10	113.113.11.11	113.111.10.10	On	10	5	test
☑					□			

Add

GRE Route

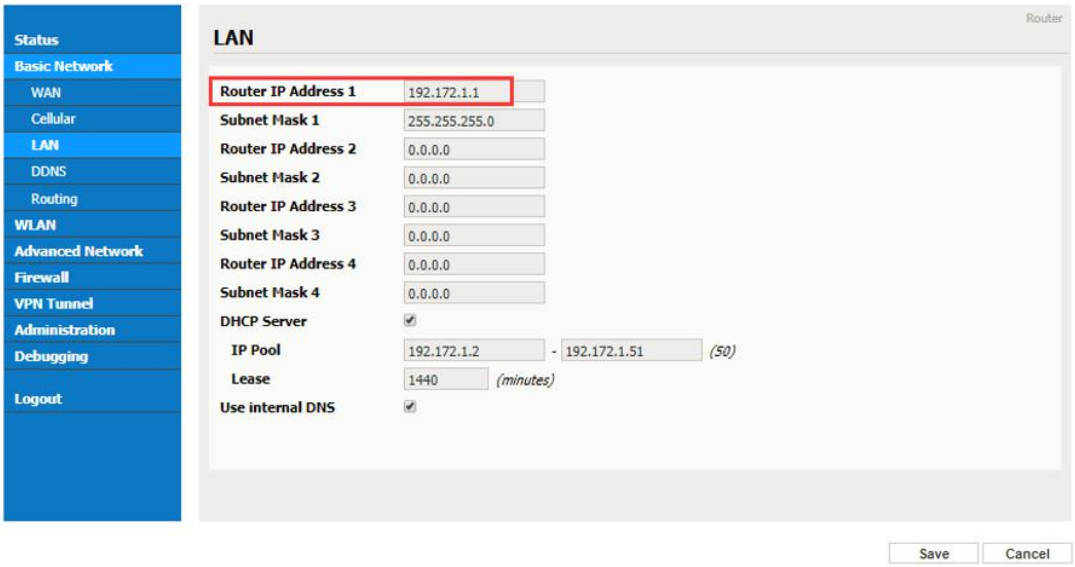
On	Tunnel Index	▲Destination Address	Description
On	1	192.172.1.0/24	test
☑	1 ▾		

Add

Save Cancel

2) WL-R210 Config

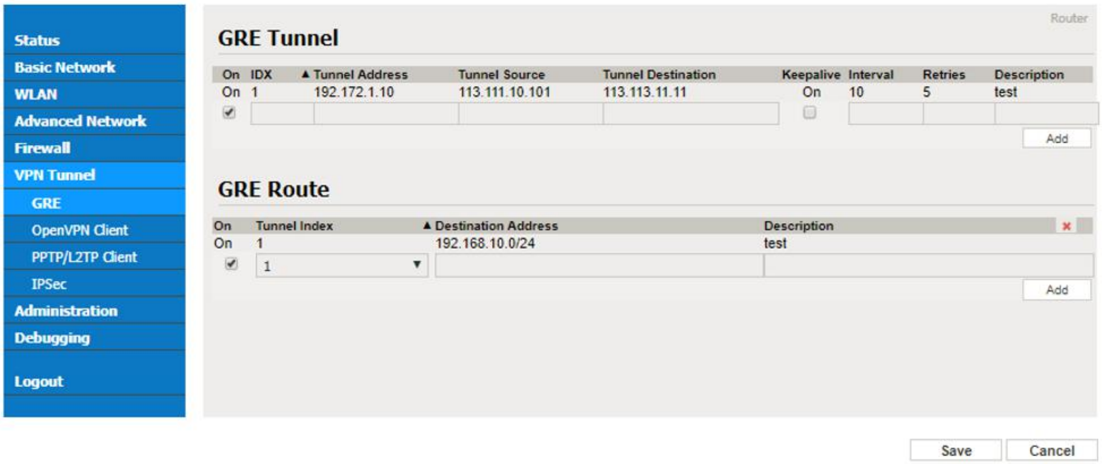
2.1) Navigate to **Basic Network > LAN**



LAN

Router IP Address 1	192.172.1.1
Subnet Mask 1	255.255.255.0
Router IP Address 2	0.0.0.0
Subnet Mask 2	0.0.0.0
Router IP Address 3	0.0.0.0
Subnet Mask 3	0.0.0.0
Router IP Address 4	0.0.0.0
Subnet Mask 4	0.0.0.0
DHCP Server	☑
IP Pool	192.172.1.2 - 192.172.1.51 *(50)*
Lease	1440 *(minutes)*
Use internal DNS	☑

2.2) Navigate to **VPN Tunnel > GRE**



GRE Tunnel

On	IDX	▲ Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
On	1	192.172.1.10	113.111.10.101	113.113.11.11	On	10	5	test
☑					☐			

GRE Route

On	Tunnel Index	▲ Destination Address	Description
On	1	192.168.10.0/24	test
☑	1 ▼		

4.6.2 OpenVPN

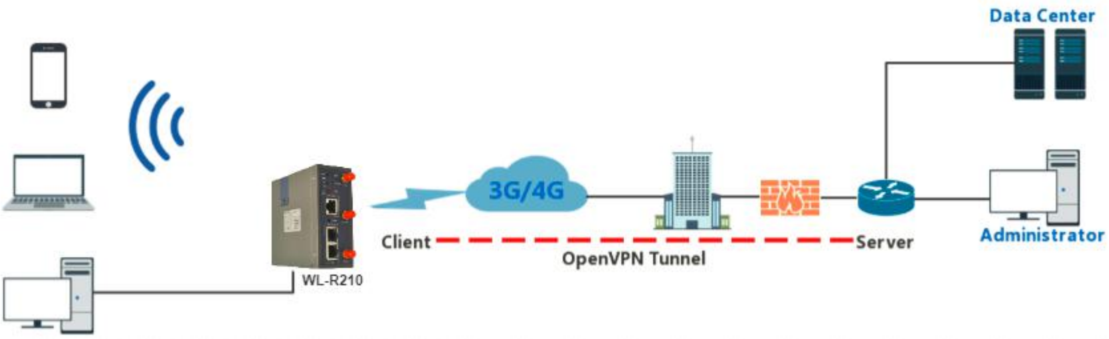
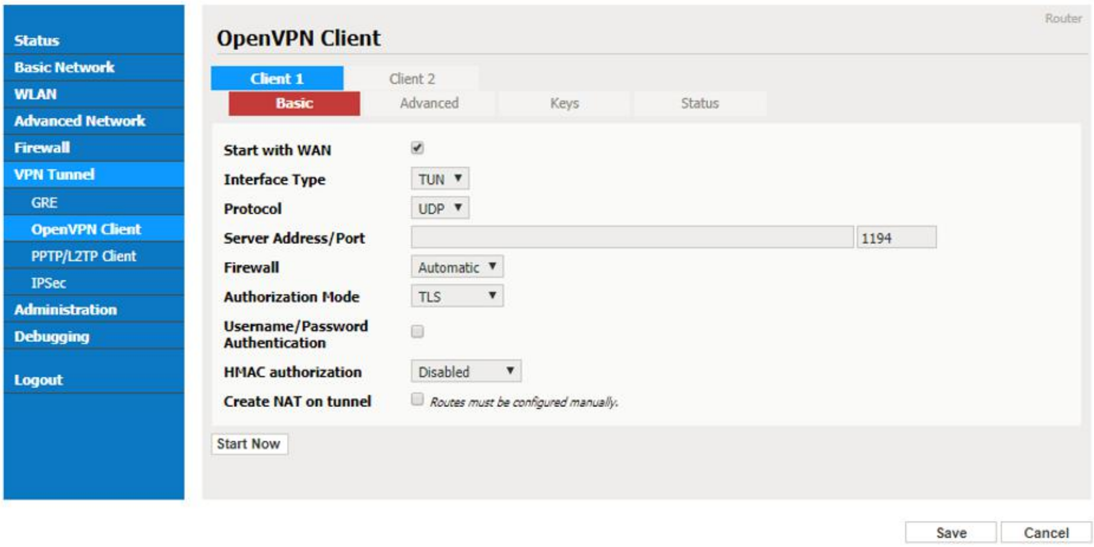


Figure 4-6-2 OpenVPN Network topology

OpenVPN between WL-R210 client and Server

Step 1 Please click “VPN Tunnel> OpenVPN Client” to check or modify the relevant parameter.

Basic



OpenVPN Client

Start with WAN ☑

Interface Type: TUN

Protocol: UDP

Server Address/Port: 1194

Firewall: Automatic

Authorization Mode: TLS

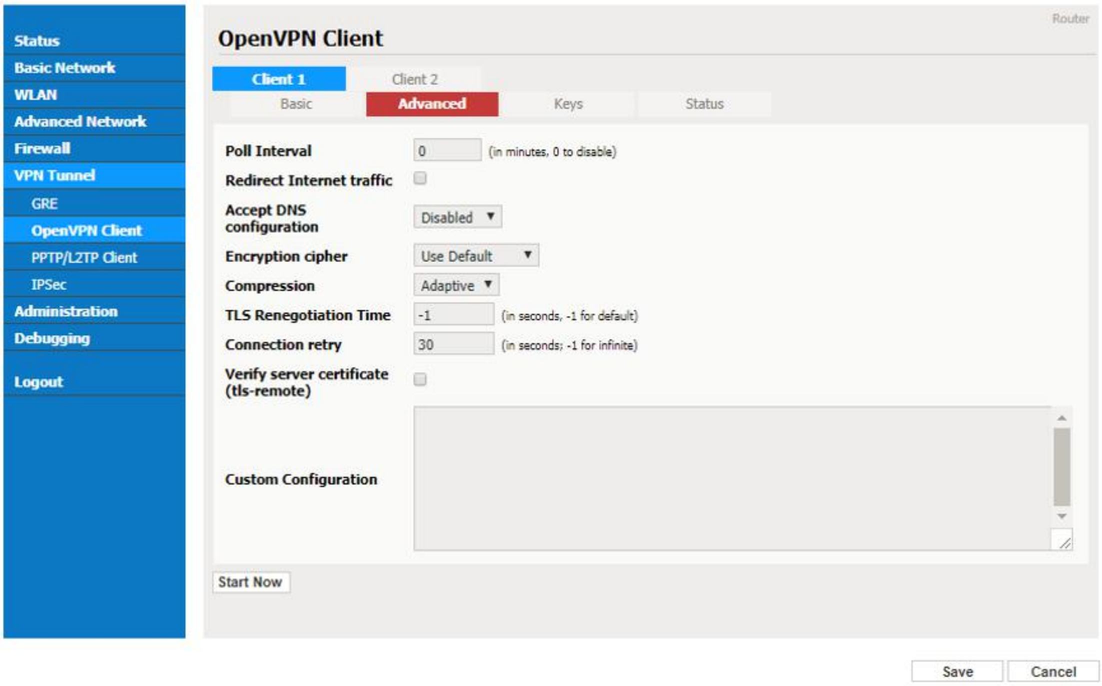
Username/Password Authentication □

HMAC authorization: Disabled

Create NAT on tunnel □ *Routes must be configured manually.*

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.

Advanced



OpenVPN Client

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)

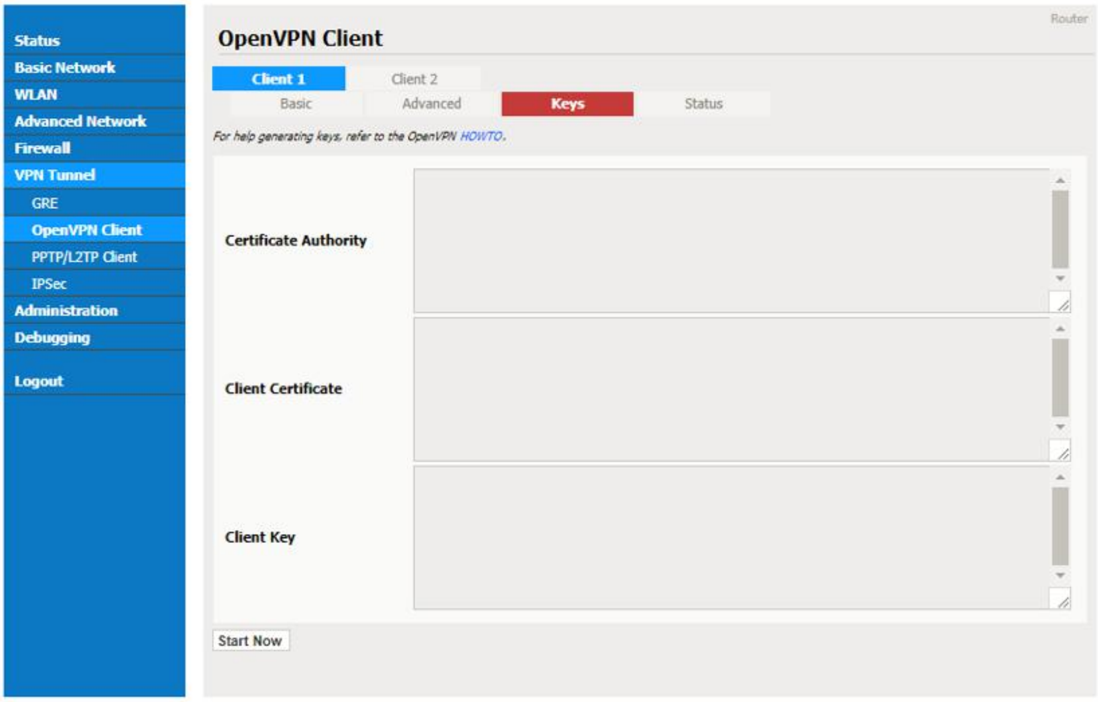
Connection retry: 30 (in seconds; -1 for infinite)

Verify server certificate (tls-remote): □

Custom Configuration:

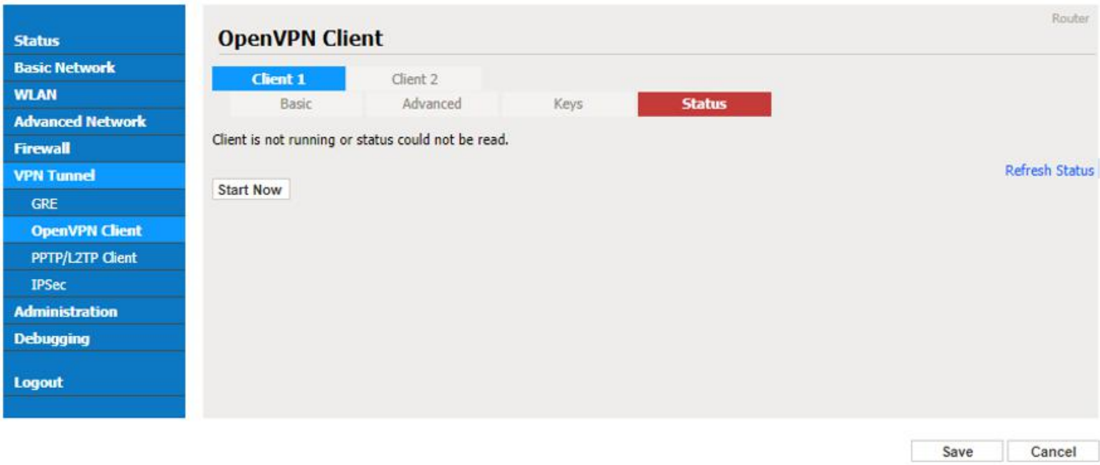
Parameter	Instruction
Poll Interval	Openvpn client check router’s status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As the configuration requested.
Encryption	As the configuration requested.
Compression	As the configuration requested.
TLS Renegotiation 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.

Keys



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

Status



Client is not running or status could not be read.

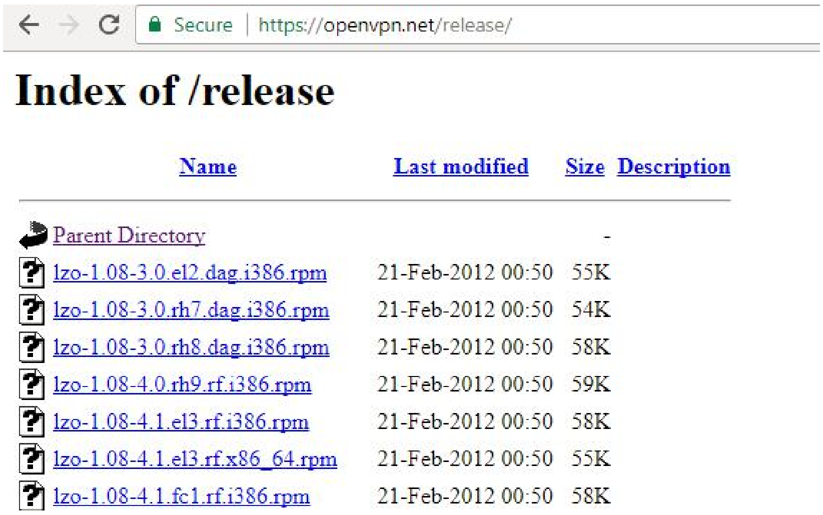
Parameter	Instruction
Status	Check OpenVPN status and data statistics.

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

OpenVPN Keys Guide

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

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

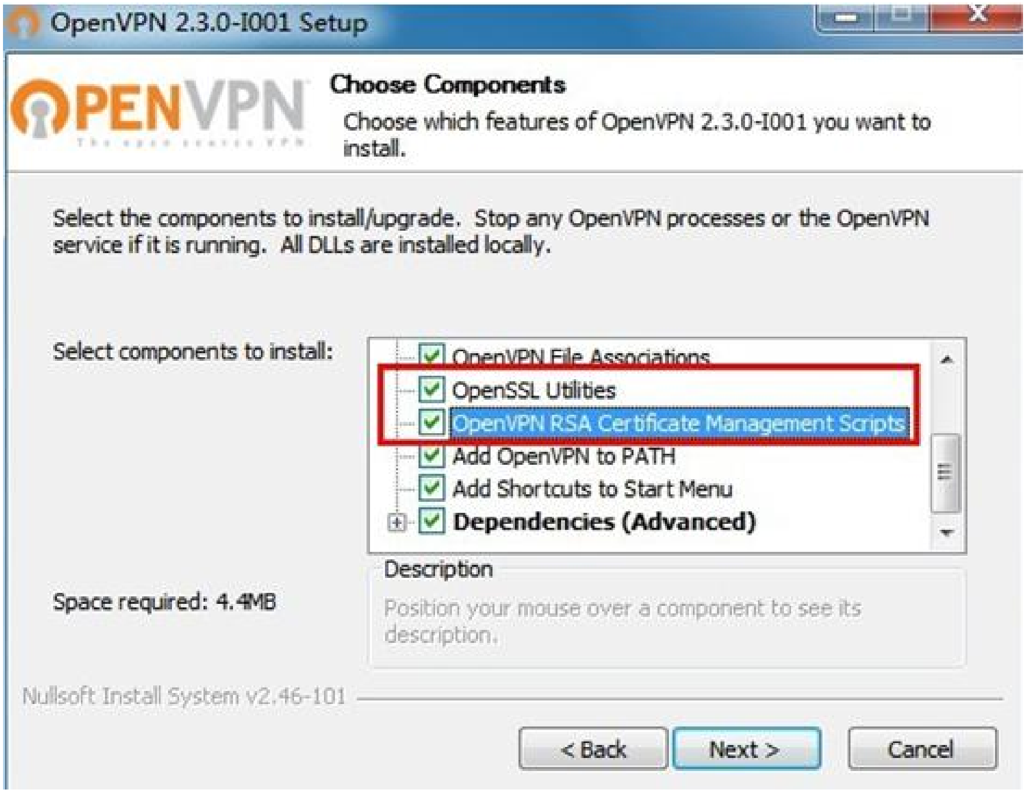


Secure | https://openvpn.net/release/

Index of /release

Name	Last modified	Size	Description
Parent Directory		-	
lzo-1.08-3.0.el2.dag.i386.rpm	21-Feb-2012 00:50	55K	
lzo-1.08-3.0.rh7.dag.i386.rpm	21-Feb-2012 00:50	54K	
lzo-1.08-3.0.rh8.dag.i386.rpm	21-Feb-2012 00:50	58K	
lzo-1.08-4.0.rh9.rf.i386.rpm	21-Feb-2012 00:50	59K	
lzo-1.08-4.1.el3.rf.i386.rpm	21-Feb-2012 00:50	58K	
lzo-1.08-4.1.el3.rf.x86_64.rpm	21-Feb-2012 00:50	55K	
lzo-1.08-4.1.fc1.rf.i386.rpm	21-Feb-2012 00:50	58K	

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



OpenVPN 2.3.0-I001 Setup

Choose Components

Choose which features of OpenVPN 2.3.0-I001 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

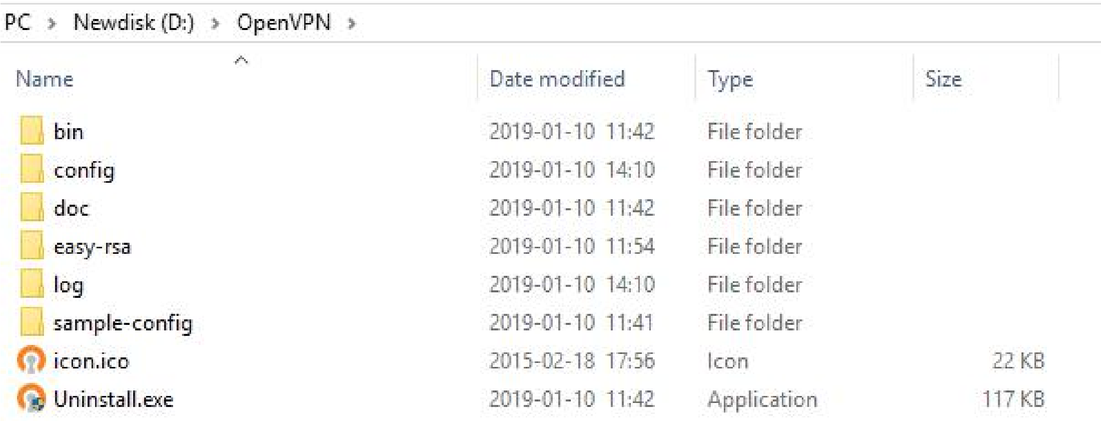
- ☑ OpenVPN File Associations
- ☑ OpenSSL Utilities
- ☑ OpenVPN RSA Certificate Management Scripts
- ☑ Add OpenVPN to PATH
- ☑ Add Shortcuts to Start Menu
- ☑ **Dependencies (Advanced)**

Space required: 4.4MB

Description

Position your mouse over a component to see its description.

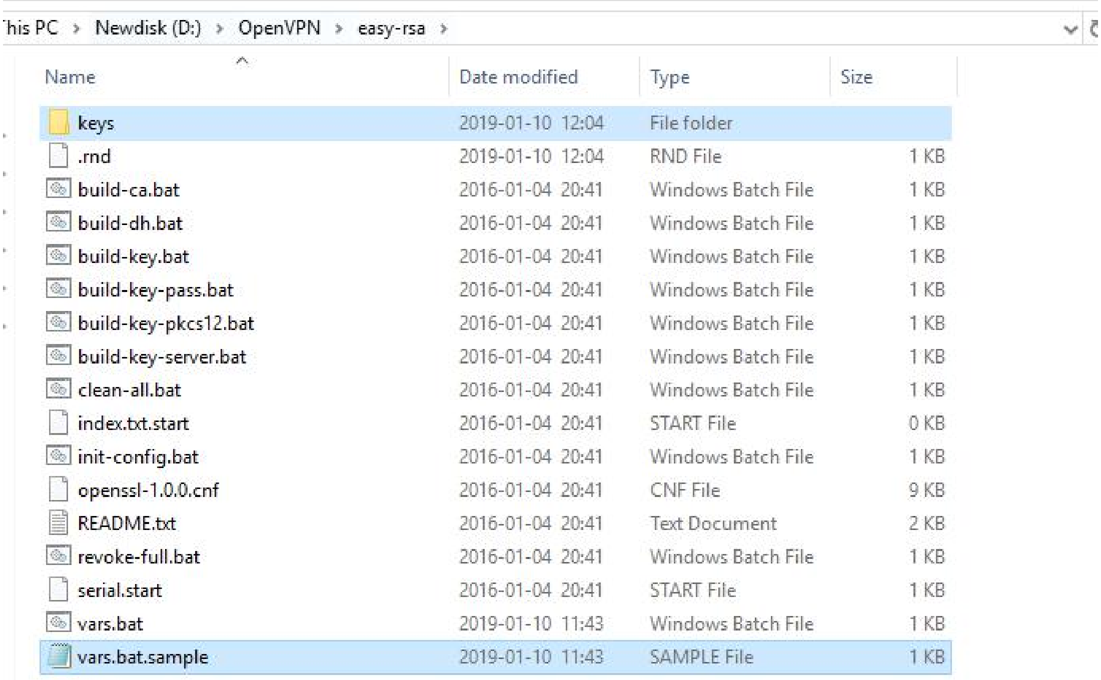
Nullsoft Install System v2.46-101



PC > Newdisk (D:) > OpenVPN >

Name	Date modified	Type	Size
bin	2019-01-10 11:42	File folder	
config	2019-01-10 14:10	File folder	
doc	2019-01-10 11:42	File folder	
easy-rsa	2019-01-10 11:54	File folder	
log	2019-01-10 14:10	File folder	
sample-config	2019-01-10 11:41	File folder	
icon.ico	2015-02-18 17:56	Icon	22 KB
Uninstall.exe	2019-01-10 11:42	Application	117 KB

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

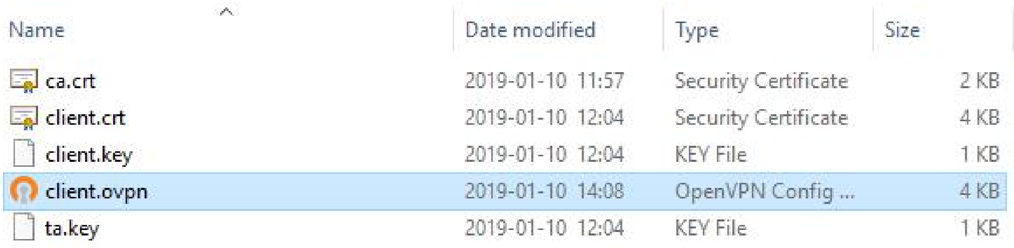


'his PC > Newdisk (D:) > OpenVPN > easy-rsa >

Name	Date modified	Type	Size
keys	2019-01-10 12:04	File folder	
.rnd	2019-01-10 12:04	RND File	1 KB
build-ca.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-dh.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pass.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pkcs12.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-server.bat	2016-01-04 20:41	Windows Batch File	1 KB
clean-all.bat	2016-01-04 20:41	Windows Batch File	1 KB
index.txt.start	2016-01-04 20:41	START File	0 KB
init-config.bat	2016-01-04 20:41	Windows Batch File	1 KB
openssl-1.0.0.cnf	2016-01-04 20:41	CNF File	9 KB
README.txt	2016-01-04 20:41	Text Document	2 KB
revoke-full.bat	2016-01-04 20:41	Windows Batch File	1 KB
serial.start	2016-01-04 20:41	START File	1 KB
vars.bat	2019-01-10 11:43	Windows Batch File	1 KB
vars.bat.sample	2019-01-10 11:43	SAMPLE File	1 KB

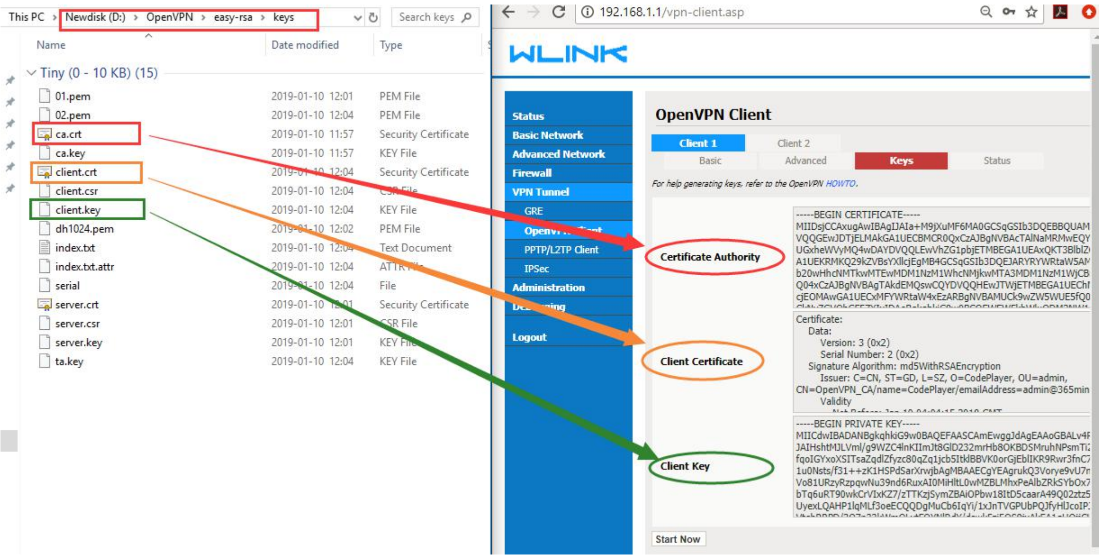
4. You may configure the client keys to WLINK OpenVPN client GUI when you create the server and client certificate in the path OpenVPN/easy-rsa/keys

4.1 Client certificate (Generated on the server)



Name	Date modified	Type	Size
ca.crt	2019-01-10 11:57	Security Certificate	2 KB
client.crt	2019-01-10 12:04	Security Certificate	4 KB
client.key	2019-01-10 12:04	KEY File	1 KB
client.ovpn	2019-01-10 14:08	OpenVPN Config ...	4 KB
ta.key	2019-01-10 12:04	KEY File	1 KB

4.1 OpenVPN>easy-rsa>keys



This PC > Newdisk (D:) > OpenVPN > easy-rsa > keys

Tiny (0 - 10 KB) (15)

Name	Date modified	Type
01.pem	2019-01-10 12:01	PEM File
02.pem	2019-01-10 12:04	PEM File
ca.crt	2019-01-10 11:57	Security Certificate
ca.key	2019-01-10 11:57	KEY File
client.crt	2019-01-10 12:04	Security Certificate
client.csr	2019-01-10 12:04	CSR File
client.key	2019-01-10 12:04	KEY File
dh1024.pem	2019-01-10 12:02	PEM File
index.txt	2019-01-10 12:04	Text Document
index.txt.attr	2019-01-10 12:04	ATTR File
serial	2019-01-10 12:04	File
server.crt	2019-01-10 12:01	Security Certificate
server.csr	2019-01-10 12:01	CSR File
server.key	2019-01-10 12:01	KEY File
ta.key	2019-01-10 12:04	KEY File

192.168.1.1/vpn-client.asp

OpenVPN Client

For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

```
-----BEGIN CERTIFICATE-----
MIIDsjCCAxugAwIBAgIJAIa+M9jXuMF6MA0GCSqGSIb3DQEBBQUAM
VQQGEwJDTjELMAkGA1UECBMCR0QxCzAJBgNVBAcTAlNaMRMwEQY
UGxheWVyMQ4wDAYDVQQLEwVhZG1pbjETMBEGA1UEAxQKT3BlblZ
A1UEKRMKQ29kZVBsYXllcjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AM
b20wHhcNMTkwMTEwMDM1NzM1WhcNMjkwMTA3MDM1NzM1WjCB
Q04xCzAJBgNVBAgTAkdEMQswCQYDVQQHEwJTWjETMBEGA1UECh
cjEOMAwGA1UECxMFYWRtaW4xEzARBgNVBAMUCk9wZW5WUE5fQ0
```

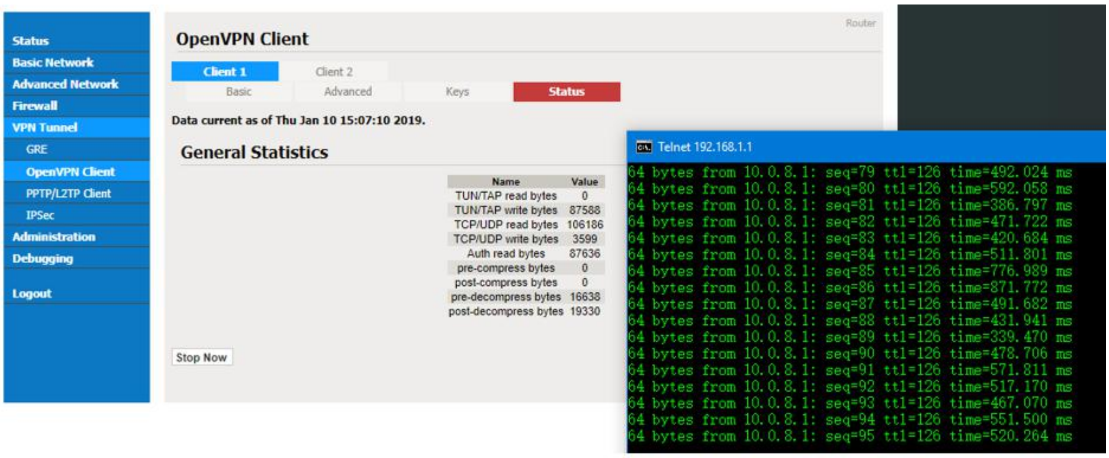
Client Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
    Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CN, ST=GD, L=SZ, O=CodePlayer, OU=admin,
CN=OpenVPN_CA/name=CodePlayer/emailAddress=admin@365min
        Validity
```

Client Key

```
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBALv4F
JAIHshtMJLVml/g9WZC4lnKIImJt8GlD232mrHb8OKBDSMruhNPsmTi
fqoIGYxoXSITsaZqdlZfyzc80qZq1jcb5ItklBBVK0orGjEblIKR9Rwr3fnC
1u0Nsts/f31++zK1HSPdSarXrwjbAgMBAAECgYEAgrukQ3Vorye9vU7r
Vo81URzyRzpqwNu39nd6RuxAI0MiHltL0wMZBLMhxPeAlbZRkSYbOx7
bTq6uRT90wkCrVIxKZ7/zTTKzjSymZBAiOPbw18ItD5caarA49Q02ztz5
UyexLQAHP1lqMLf3oeECQQDgMuCb6IqYi/1xJnTVGPUbPQJfyHlJcoIP
```

5. You may do the ping test to your server when the tunnel is established



OpenVPN Client

Data current as of Thu Jan 10 15:07:10 2019.

General Statistics

Name	Value
TUN/TAP read bytes	0
TUN/TAP write bytes	87588
TCP/UDP read bytes	106186
TCP/UDP write bytes	3599
Auth read bytes	87636
pre-compress bytes	0
post-compress bytes	0
pre-decompress bytes	16638
post-decompress bytes	19330

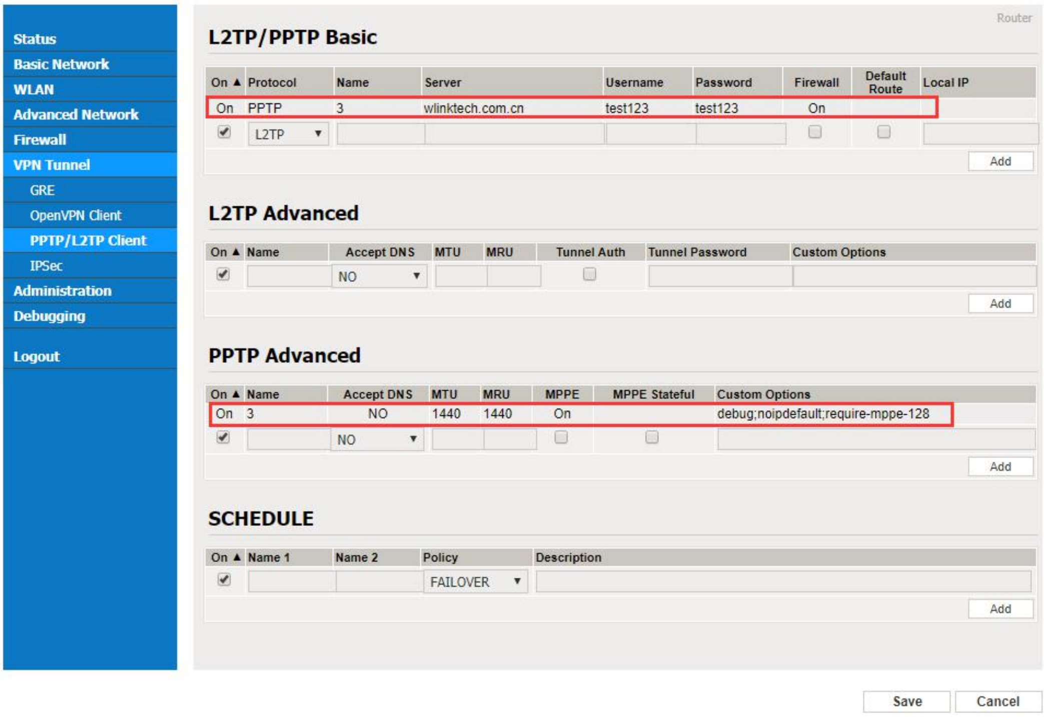
Telnet 192.168.1.1

```
64 bytes from 10.0.8.1: seq=79 ttl=126 time=492.024 ms
64 bytes from 10.0.8.1: seq=80 ttl=126 time=592.058 ms
64 bytes from 10.0.8.1: seq=81 ttl=126 time=386.797 ms
64 bytes from 10.0.8.1: seq=82 ttl=126 time=471.722 ms
64 bytes from 10.0.8.1: seq=83 ttl=126 time=420.684 ms
64 bytes from 10.0.8.1: seq=84 ttl=126 time=511.801 ms
64 bytes from 10.0.8.1: seq=85 ttl=126 time=776.989 ms
64 bytes from 10.0.8.1: seq=86 ttl=126 time=871.772 ms
64 bytes from 10.0.8.1: seq=87 ttl=126 time=491.682 ms
64 bytes from 10.0.8.1: seq=88 ttl=126 time=431.941 ms
64 bytes from 10.0.8.1: seq=89 ttl=126 time=339.470 ms
64 bytes from 10.0.8.1: seq=90 ttl=126 time=478.706 ms
64 bytes from 10.0.8.1: seq=91 ttl=126 time=571.811 ms
64 bytes from 10.0.8.1: seq=92 ttl=126 time=517.170 ms
64 bytes from 10.0.8.1: seq=93 ttl=126 time=467.070 ms
64 bytes from 10.0.8.1: seq=94 ttl=126 time=551.500 ms
64 bytes from 10.0.8.1: seq=95 ttl=126 time=520.264 ms
```

4.6.3 L2TP/PPTP

Step 1 Please click “VPN Tunnel>PPTP/L2TP Client” to view or modify the relevant parameter.

PPTP



L2TP/PPTP Basic

On ▲	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
On	PPTP	3	wlinktech.com.cn	test123	test123	On		
☑	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
On	3	NO	1440	1440	On		debug;noipdefault;require-mppe-128
☑		NO ▼			□	□	

Add

SCHEDULE

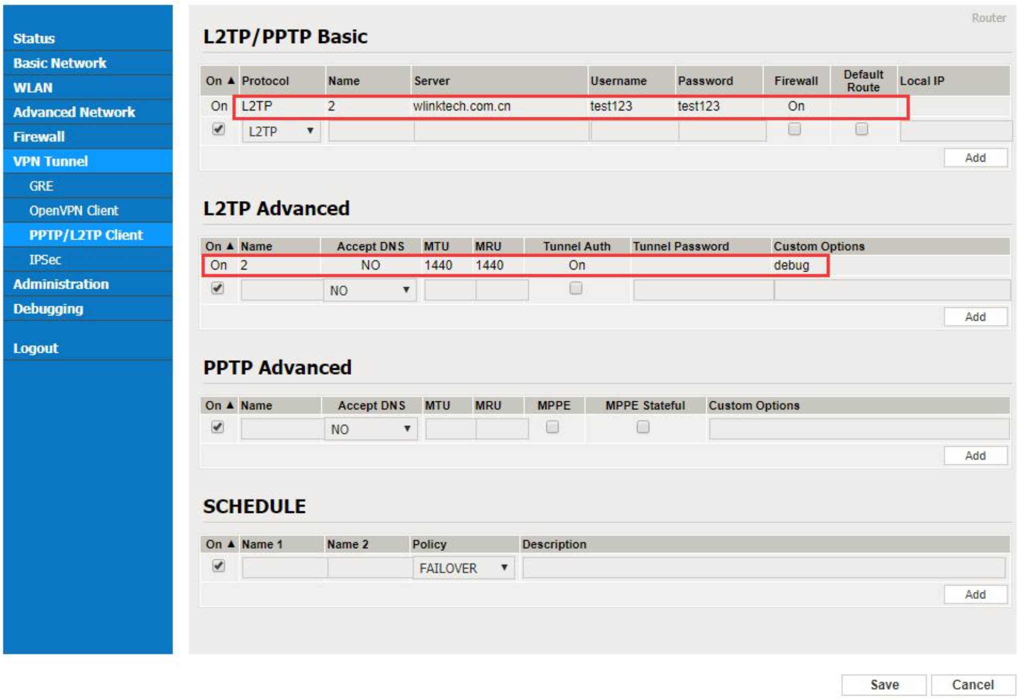
On ▲	Name 1	Name 2	Policy	Description
☑			FAILOVER ▼	

Add

Save Cancel

Note: The Custom Options based on your server

Configured test case: L2TP



L2TP/PPTP Basic

On ▲	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
On	L2TP	2	wlinktech.com.cn	test123	test123	On		
☑	L2TP ▼					□	□	

Add

L2TP Advanced

On ▲	Name	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
On	2	NO	1440	1440	On		debug
☑		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 ▼	

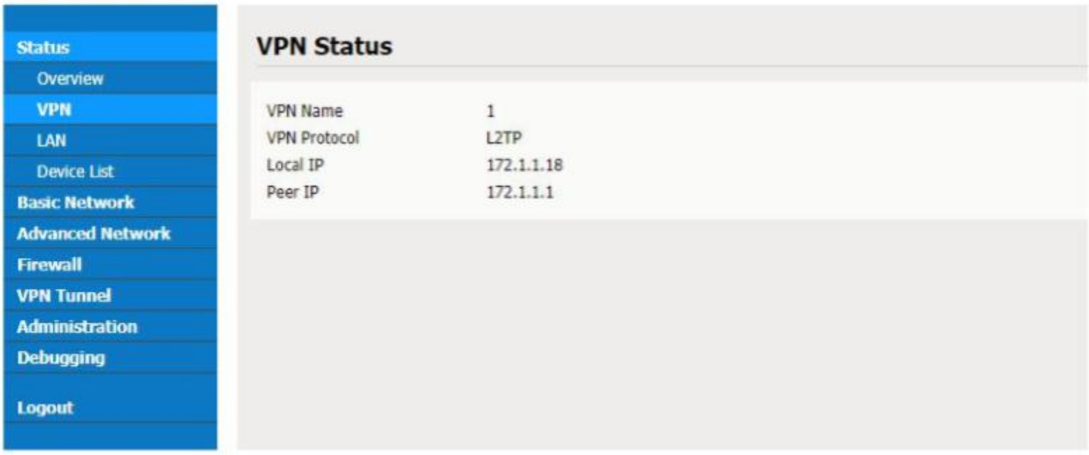
Add

Save Cancel

Note: The Custom Options based on VPN server

Step 2 Please click "Save" icon

VPN Status



VPN Status

VPN Name	1
VPN Protocol	L2TP
Local IP	172.1.1.18
Peer IP	172.1.1.1

4.6.4 IPSec

IPSec between WL-R210 and Cisco Router

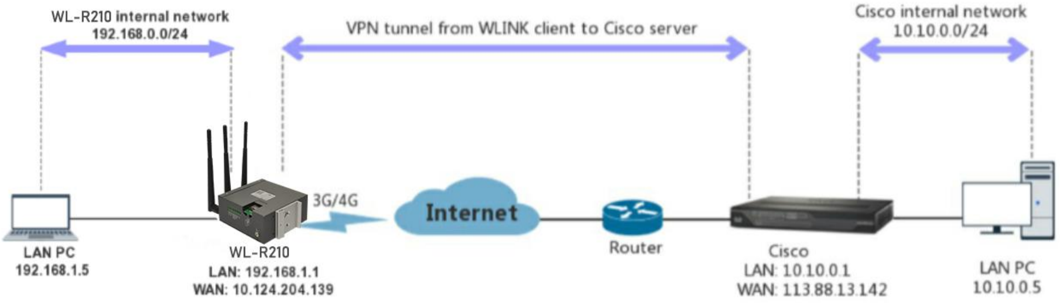


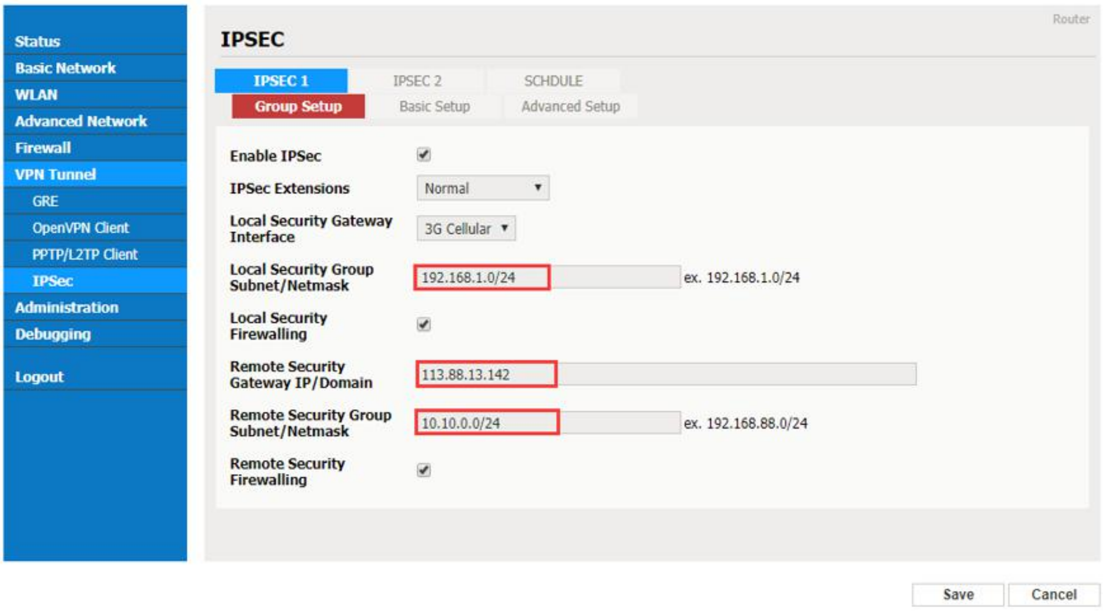
Figure 4-6-4 IPSec Network topology

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

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



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

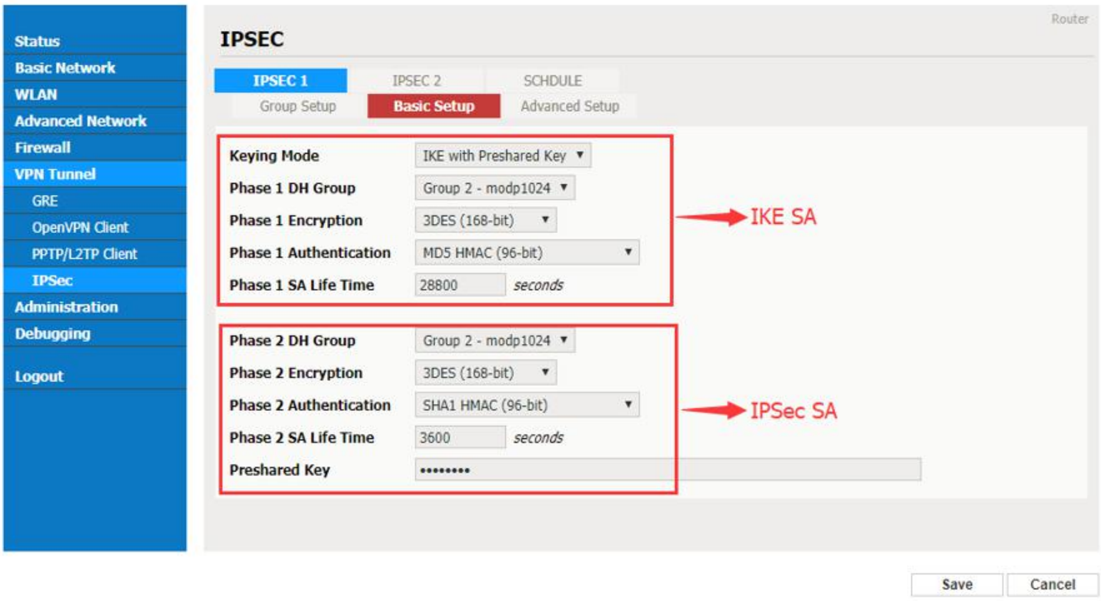
Local Security Firewalling ☑

Remote Security Gateway IP/Domain: 113.88.13.142

Remote Security Group Subnet/Netmask: 10.10.0.0/24 ex. 192.168.88.0/24

Remote Security Firewalling ☑

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



IPSEC

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

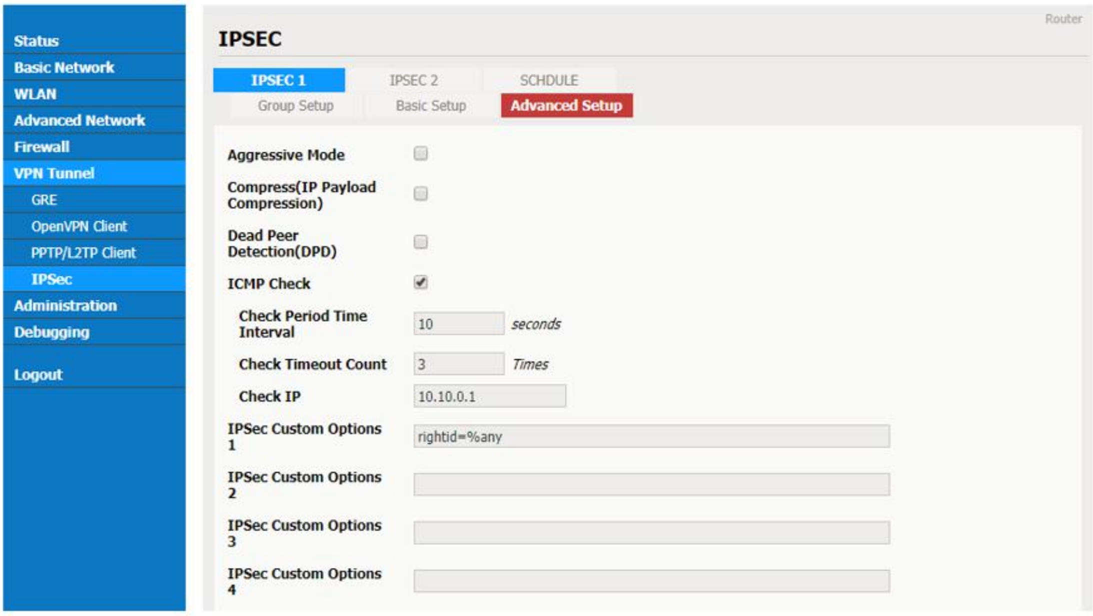
Phase 2 Encryption: 3DES (168-bit)

Phase 2 Authentication: SHA1 HMAC (96-bit)

Phase 2 SA Life Time: 3600 *seconds*

Preshared Key: ••••••••

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



IPSEC

Aggressive Mode □

Compress(IP Payload Compression) □

Dead Peer Detection(DPD) □

ICMP Check ☑

Check Period Time Interval: 10 *seconds*

Check Timeout Count: 3 *Times*

Check IP: 10.10.0.1

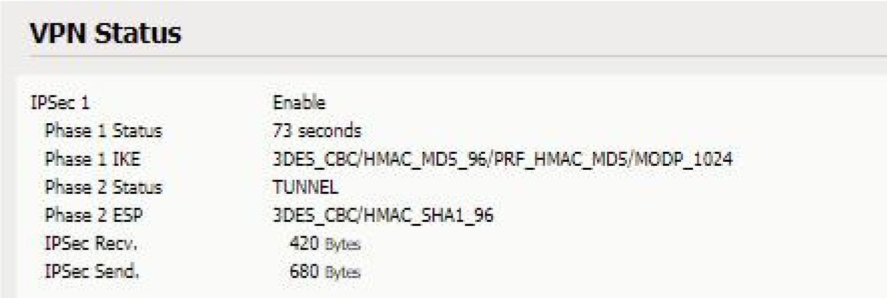
IPSec Custom Options 1: rightid=%any

IPSec Custom Options 2:

IPSec Custom Options 3:

IPSec Custom Options 4:

2.4) **Status**



VPN Status

```
IPSec 1            Enable
  Phase 1 Status   73 seconds
  Phase 1 IKE      3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
  Phase 2 Status   TUNNEL
  Phase 2 ESP      3DES_CBC/HMAC_SHA1_96
  IPSec Recv.        420 Bytes
  IPSec Send.        680 Bytes
```

--End