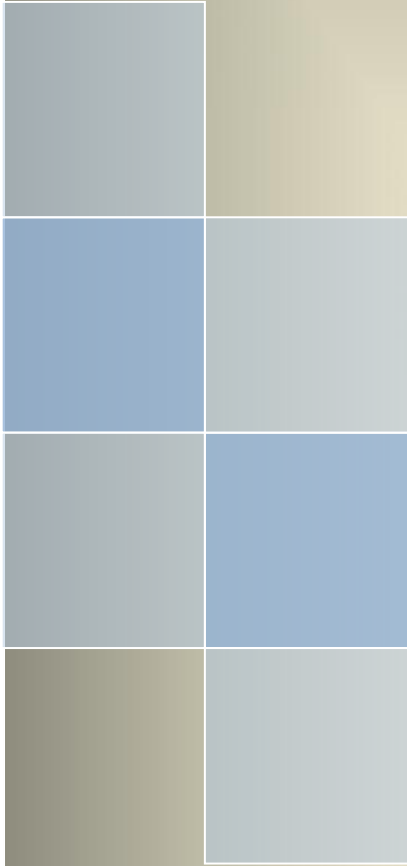


WLINK

User Manual

---Apply to WL-R200 Series Industrial 4G/3G Router



Copyright © Shenzhen WLINK Technology Company Limited 2012 ~ 2018

Without our written approval, Anyone can't extract, copy whole or part of content of this file and can't spread out in any format.

Caution

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

Shenzhen WLINK Technology Company Limited

Add: 3F, Yiben Building, Chaguang Road, Xili, Nanshan District, China, 518054

Web: <http://www.wlink-tech.com>

Service Email: support@wlink-tech.com

Tel: 86-755-86089513

Fax: 86-755-26059261

Contents

1 Product Introduction.....	4
1.1 Product overview.....	4
1.2 Model introduction.....	4
1.3 Product Appearance.....	6
1.4 Typical Application Diagram.....	6
1.5 Features.....	7
2 Hardware Installation.....	8
2.1 Panel:.....	8
2.2 LED Status.....	9
2.3 Dimension.....	10
2.4 How to Install.....	10
3 Router Configuration.....	12
3.1 Local Configure.....	12
3.2 Basic Configuration.....	13
3.3 WLAN Setting.....	20
3.4 Advanced Network Setting.....	24
3.5 Firewall.....	32
3.6 VPN Tunnel.....	34
3.7 System Management.....	43

3.8 Debugging Setting.....	51
3.9 “RST” Button for Restore Factory Setting.....	54
3.10 Appendix (For GPS, Captive Portal &OpenVPN only).....	54

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

Optional Model List							
Model	LTE 4G	3G	Interface	WiFi	GPS	DL	UL
WL-R200L	FDD LTE 2600/2100/1800/900/800MHz	UMTS 800/850/900/1900/2100MHz	1xLAN 1xWAN			100M	50M
WL-R200L-w	FDD LTE 2600/2100/1800/900/800MHz	UMTS 800/850/900/1900/2100MHz	1xLAN 1xWAN	✓		100M	50M
WL-R200L-g	FDD LTE 2600/2100/1800/900/800MHz	UMTS 800/850/900/1900/2100MHz	1xLAN 1xWAN		✓	100M	50M
WL-R200LZ	FDD LTE: 2600/2100/1900/1700/900//850/700MHz TDD LTE: B38	UMTS 2100/1900/850/900MHz	1xLAN 1xWAN			FDD:100M TDD:60M	FDD:50M TDD:60M
WL-R200LZ-w	FDD LTE: 2600/2100/1900/1700/900//850/700MHz TDD LTE: B38	UMTS 2100/1900/850/900MHz	1xLAN 1xWAN	✓		FDD:100M TDD:60M	FDD:50M TDD:60M
WL-R200LZ-g	FDD LTE: 2600/2100/1900/1700/900//850/700MHz TDD LTE: B38	UMTS 2100/1900/850/900MHz	1xLAN 1xWAN		✓	FDD:100M TDD:60M	FDD:50M TDD:60M
WL-R200H		HSPA+ 2100/1900/850MHz	1xLAN 1xWAN			21M	5.76M
WL-R200H-w		HSPA+ 2100/1900/850MHz	1xLAN 1xWAN	✓		21M	5.76M
WL-R200H-g		HSPA+ 2100/1900/850MHz	1xLAN 1xWAN		✓	21M	5.76M
WL-R200H2		HSPA 2100/1900/900/850MHz	1xLAN 1xWAN			14M	5.76M
WL-R200H2-w		HSPA 2100/1900/900/850MHz	1xLAN 1xWAN	✓		14M	5.76M
WL-R200H2-g		HSPA 2100/1900/900/850MHz	1xLAN 1xWAN		✓	14M	5.76M
WL-R200U		HSUPA 2100/1900/900/850MHz	1xLAN 1xWAN			7.2M	5.76M
WL-R200U-w		HSUPA 2100/1900/900/850MHz	1xLAN 1xWAN	✓		7.2M	5.76M
WL-R200U-g		HSUPA 2100/1900/900/850MHz	1xLAN 1xWAN		✓	7.2M	5.76M
WL-R200E		EVDO 800/MHz	1xLAN 1xWAN			3.1M	1.8M
WL-R200E-w		EVDO 800MHz	1xLAN 1xWAN	✓		3.1M	1.8M
WL-R200E-g		EVDO 800MHz	1xLAN 1xWAN		✓	3.1M	1.8M

Note:
1. If need Special frequency band, pls consult wlink sale person
2. Please specify before order if need VPN or OpenVPN

1.3 Product Appearance

Table 1-2 WLINK Router Appearance

Series	R200	R200—W(G)	R520-g	R520-d
Appearance				
Ports	1*LAN 1*WAN	1*LAN + 1*WAN + GPS or WLAN(11n 1T1R)	1*WAN + 4*LAN + GPS or WLAN(11n 1T1R)	1*WAN + 4*LAN + single module/dual SIM, dual module/dual SIM
Product category	Single port router	Single port Wi-Fi (GPS) router	Multi-port Wi-Fi router	multi-port double-link router

1.4 Typical Application Diagram

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

For example, in economic area, R200 Series Router connect server by IPSec & GRE to ensure data security, tiny design makes it could installed into ATM machine. All these technology ensured safe and reliable data transmission, and minimize the probability of network disconnection, and maximize the usability of economic business like ATM, POS .etc.

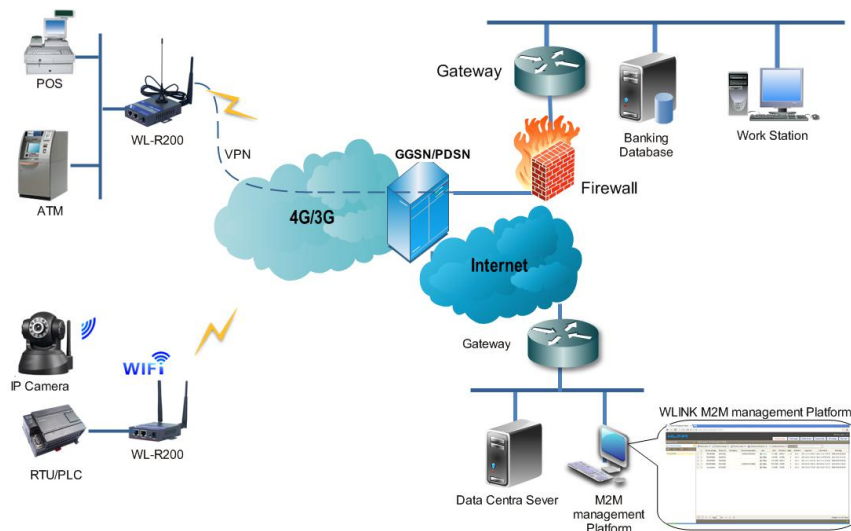


Figure 1-1 Network Topology

WLINK industrial router is based on mobile wireless public network or private network, build wireless data channel in mature network, to lower down the cost of wireless data transmission and technique.

1.5 Features

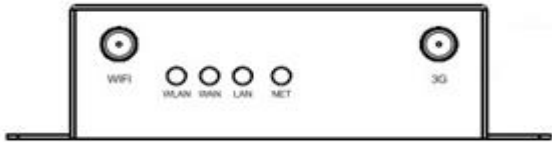

- Various cellular module optional, LTE/HSPA+/EVDO/CDMA2000 optional
- Support IEEE802.11b/g/n Wi-Fi AP function, extended support to Wi-Fi terminal, WDS bridging, support WEP, WPA/WPA2 Personal/Enterprise, TKIP/AES, etc., Authenticated encryption mode
- Support virtual data and private network (APN/VPDN)
- 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 customer's demand

2 Hardware Installation

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

2.1 Panel:

Table 1-1 WLR200 -Structure

WLINK Tech.	R200 series
Front	
Rear	



NOTE

There are some different for Antenna interface and indicator light for the expanded Wi-Fi, GPS series.

Table 2-1 Router Interface

Port	Instruction	Remark
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection	
3G	3G antenna, SMA connector, 50Ω	
WIFI	Wi-Fi antenna, SMA connector, 50Ω	Optional

Port	Instruction	Remark
LAN	10/100Base-TX, MDI/MDIX self-adaption,	R200: 1*LAN
WAN	10/100Base-TX, MDI/MDIX self-adaption	R200 serial port and WAN port multiplex
RST	Reset button,(press on button 5 seconds)	
PWR	Power connector	5 ~ 26V DC
WAN/CON	Four pin serial port, suitable for collection device with RS-232 or RS-485 interface, for wireless data transmission, CON for debug test.	R20 serial port and WAN port multiplex

2.2 LED Status

Table 2-2 Router LED indicator Status

silk-screen	Indicator		Note
NET	Color	Green	Strong Signal
		Orange	Normal Signal
		Red	Weak Signal
	Status	Quick Blinking (0.5s)	Dialing
		Slow Blinking (2s)	3G online
		Solid light	4G online
WLAN	Green	Solid light	WLAN port open, but no data sending.
	Green	Blinking quickly	Data is in transmitting
	Green	Extinguished	WLAN port isn't opened
LAN	Green	Solid light	Connection ok
	Green	Blinking	Data Sending
	Green	Extinguished	Not connection



NOTE

There are some difference among the LED indicator of expanded Wi-Fi, GPS function and single module/double SIM, double module/double SIM series products.

2.3 Dimension

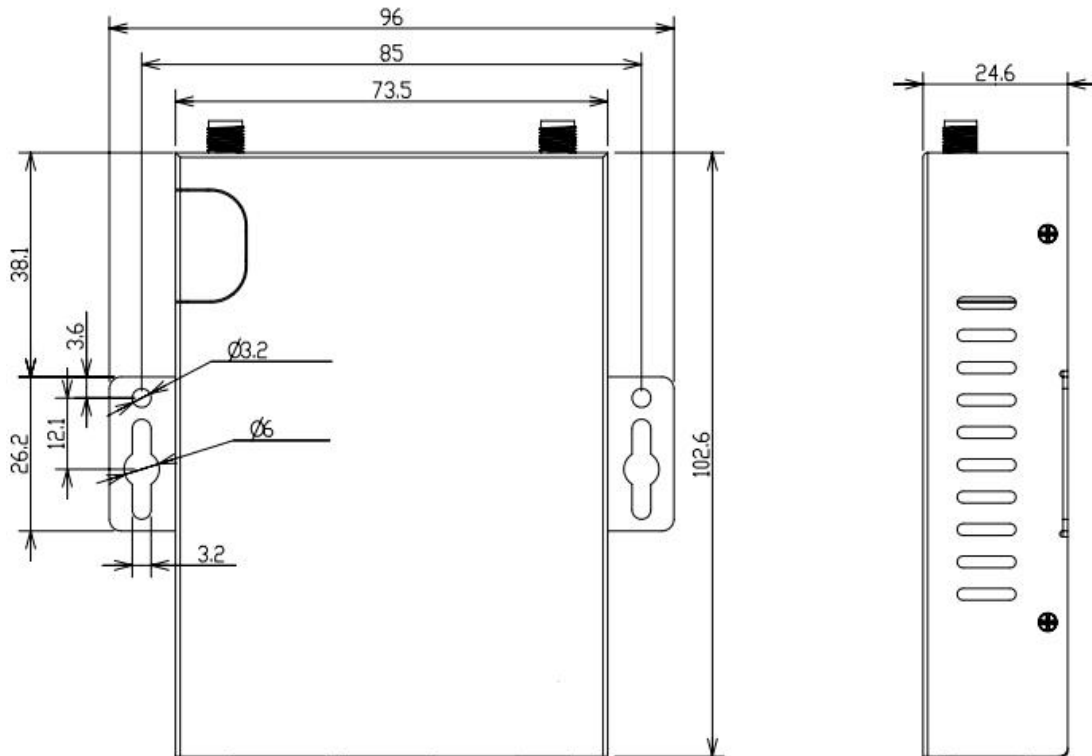


Figure 2-2 WL-R200 Series Router Dimension Figure

2.4 How to Install

2.4.1 SIM/UIM card install

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



Before connecting, please disconnect any power resource of router

2.4.2 Ethernet Cable Connection

Use the Ethernet cable to connect the cellular Router to 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. One end connect to computer serial port, the other end connects the console port of the router



Before connecting, please disconnect any power resource of router

2.4.4 Power Supply

In order to get high reliability, WLINK Series Router adapt supports wide voltage input range: +5V~+36VDC, support hot plug and complex application environment.

2.4.5 Review

After insert the SIM/UIM card, connect Ethernet cable and necessary antenna, connect power cable.



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

Notice:

- Step 1 Check 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 input “http://192.168.1.1”, to enter identify page.

User should use the default user name and password when log in for the first time



Figure 3-4 User Identify Interface

---END

3.2 Basic Configuration



NOTE

Different software version have different web configuration interface, below take R520 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.

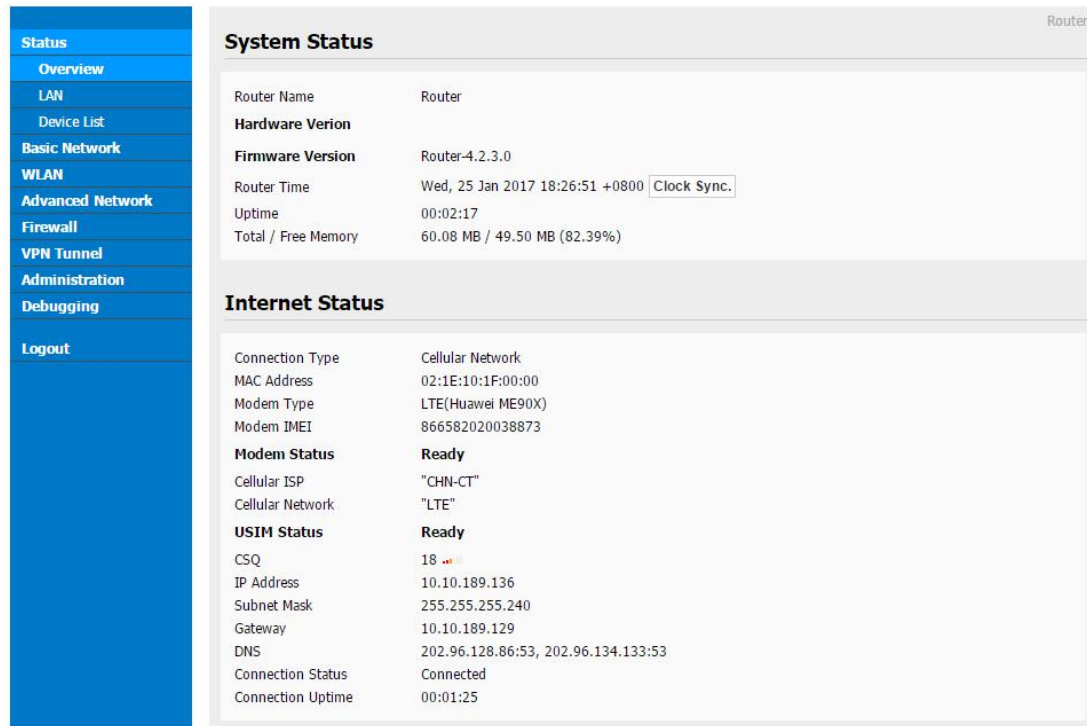


Figure 3-5 Router Status GUI

3.2.1 WAN Setting

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



Figure 3-1 WAN Setting GUI

Table 3-1 WAN Setting Instruction

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

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.

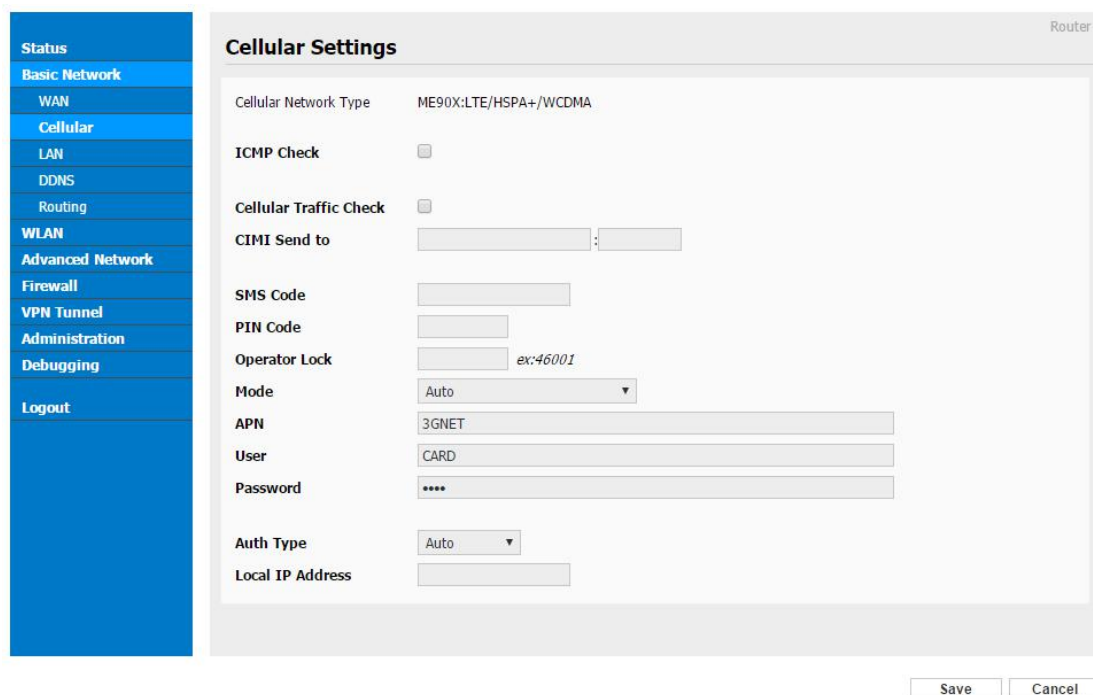


Figure 3-2 Cellular Settings GUI

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.
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.

Parameter	Instruction
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	<ul style="list-style-type: none"> ● 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
Local IP Add	Assigned SIM IP from operator.



【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	<input checked="" type="checkbox"/>
Check IP	<input type="text" value="8.8.8.8"/>
Check IP (Optional)	<input type="text" value="4.4.4.4"/>
Interval	<input type="text" value="60"/> (seconds)
Retries	<input type="text" value="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.

---End

3.2.3 LAN Setting

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

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 GUI.

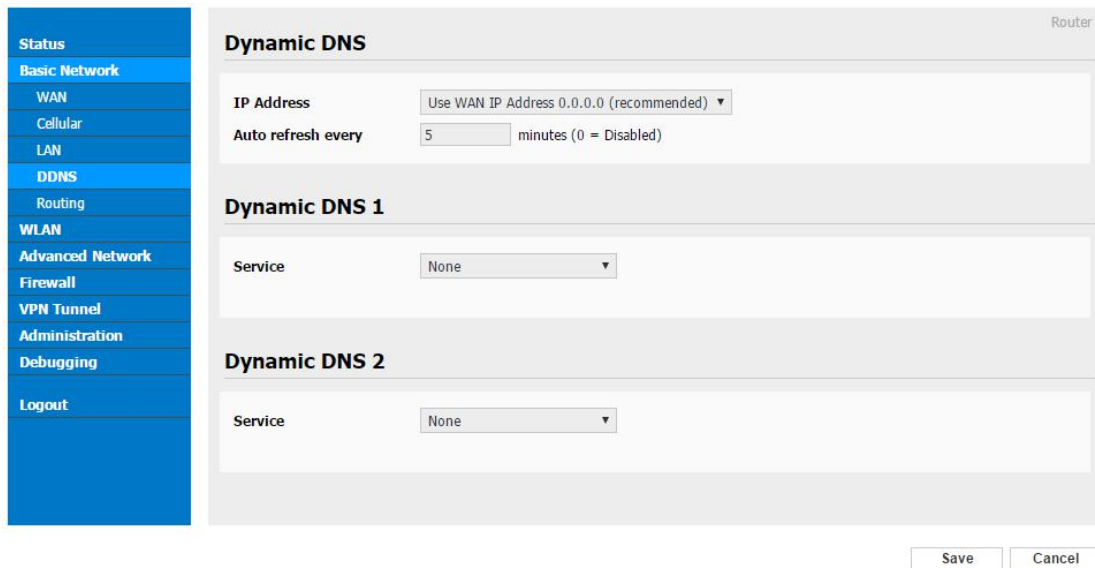


Figure 3-4 Dynamic DNS Setting

Table 3-4 DDNS Setting Instruction

parameter	Instruction
IP address	Default is standard DDNS protocol, for customized protocol, please contact WLINK engineer. use default IP 0.0.0.0 as usually.
Auto refresh time	Set the interval of the DDNS client obtains new IP, suggest 5mins 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.

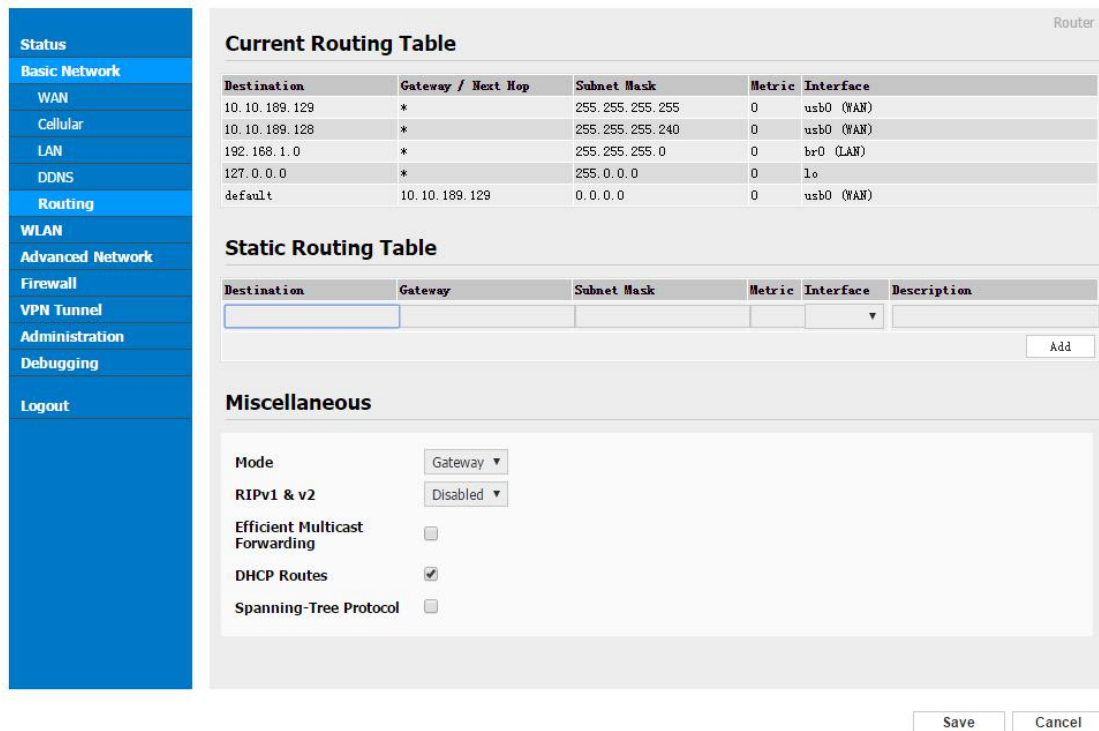


Figure 3-5 Routing Setting

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
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

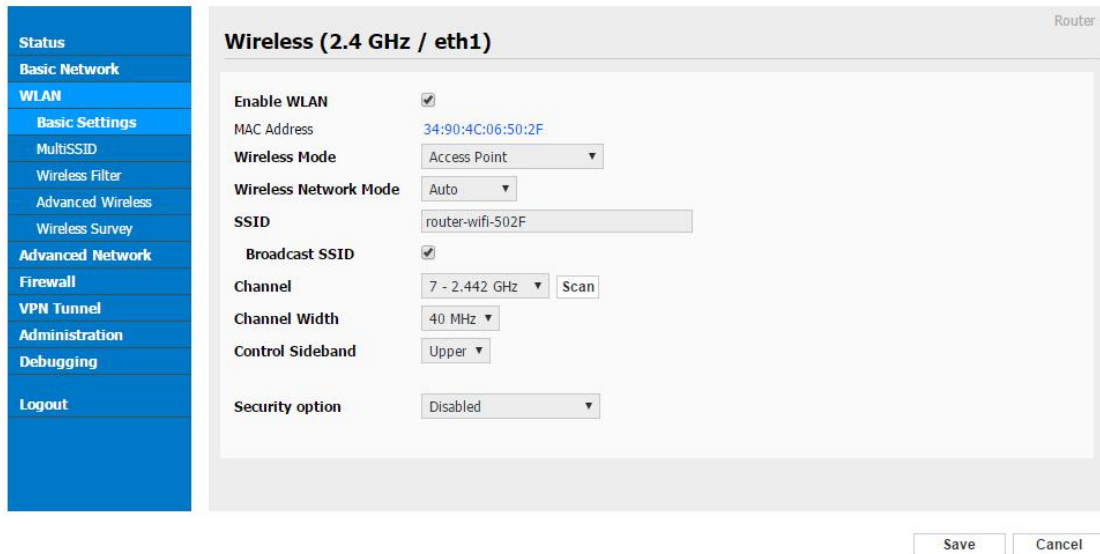


Figure 3-6 WLAN Basic Settings GUI

Table 3-6 Basic Setting Instruction

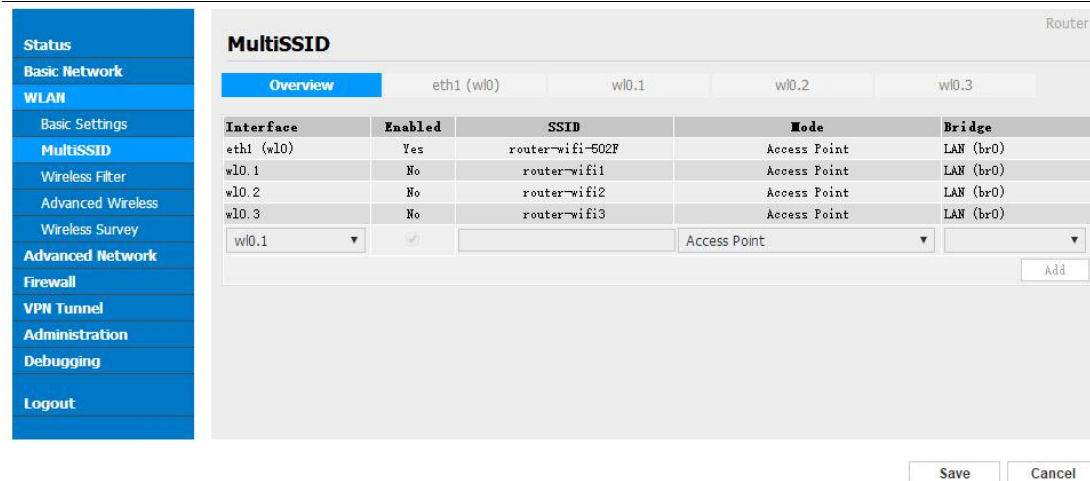
Parameter	Instruction
Enable wireless	Enable or Disable the Wireless
Wireless mode	Support AP, AP+WDS, Bridge, Client, WDS
Wireless Network protocol	Support Auto, IEEE 11b/g/n optional
SSID	The default is router, can be modified as per application.
Channel	The channel of wireless network, suggest keep the default
Channel Width	20MHZ and 40MHZ alternative
Security	Support various encryption method

Step 2 Please click “Save” to finish.

----End

3.3.2 Wireless Filter Setting

Step 1 Single click “WLAN > MultiSSID”.



3.3.3 Wireless Filter Setting

Step 1 Single click “WLAN > Wireless Filter”.

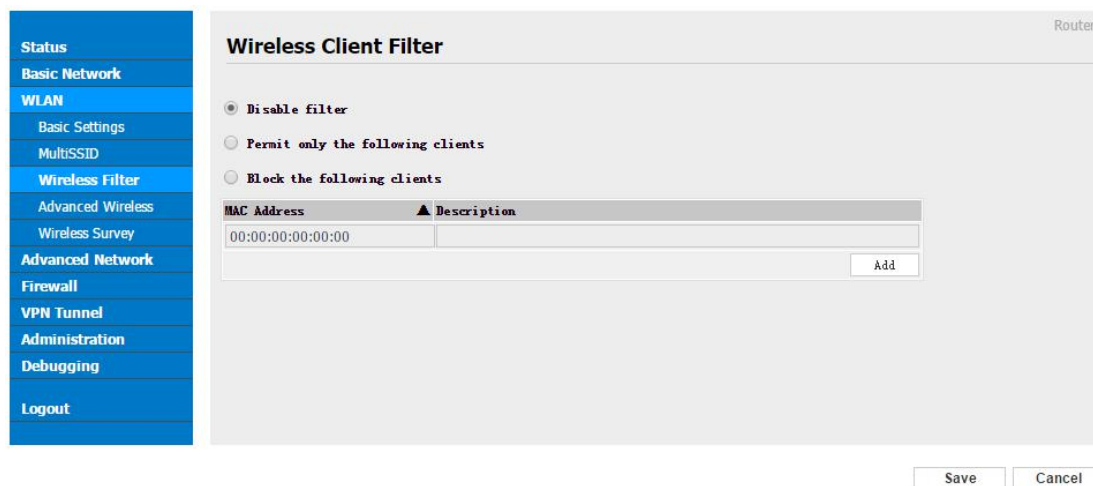


Figure 3-7 Wireless Client Filter Setting GUI

The Wireless Filter enable to set the permitted client or prohibit the specific client to connect the WiFi, However, this feature is invalid for wired connection application.

Table 3-7 “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.

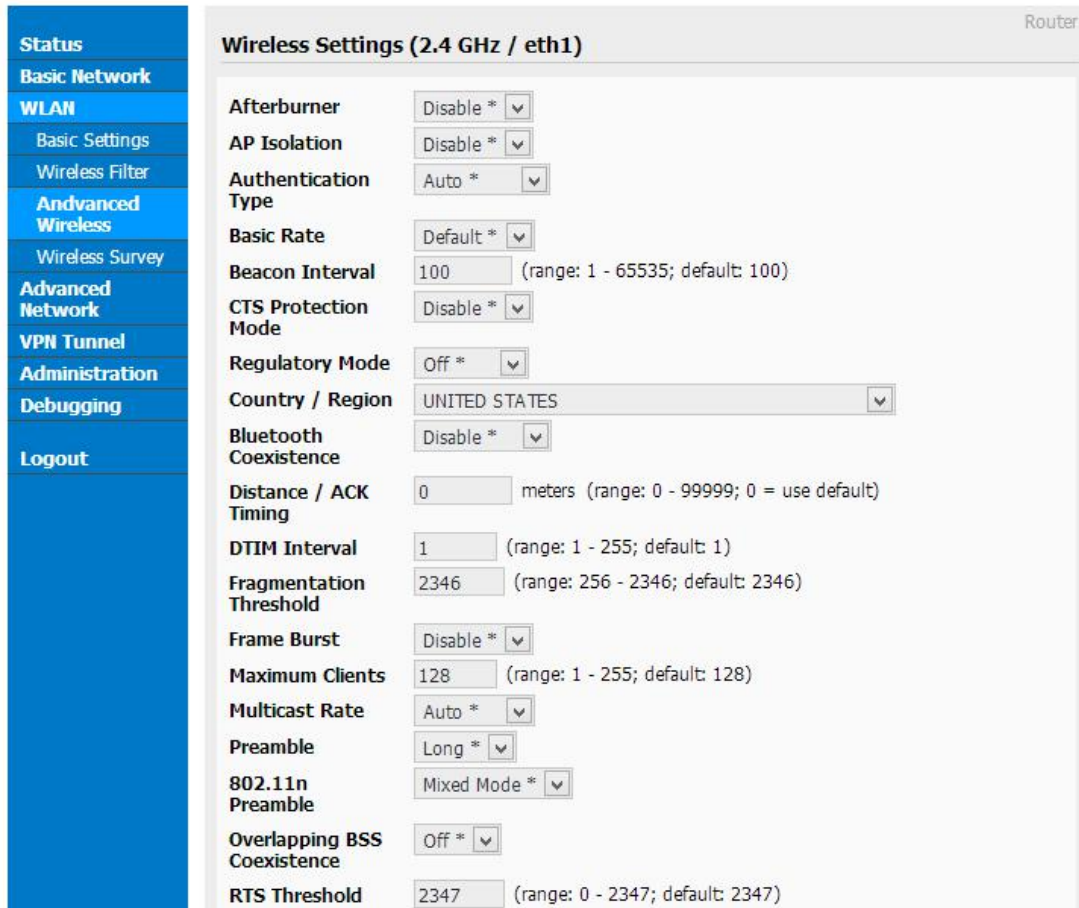


Figure 3-8 Advanced Wireless Setting GUI

Step 2 Please click “save” to finish.

----End

3.3.5 Wireless Survey

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

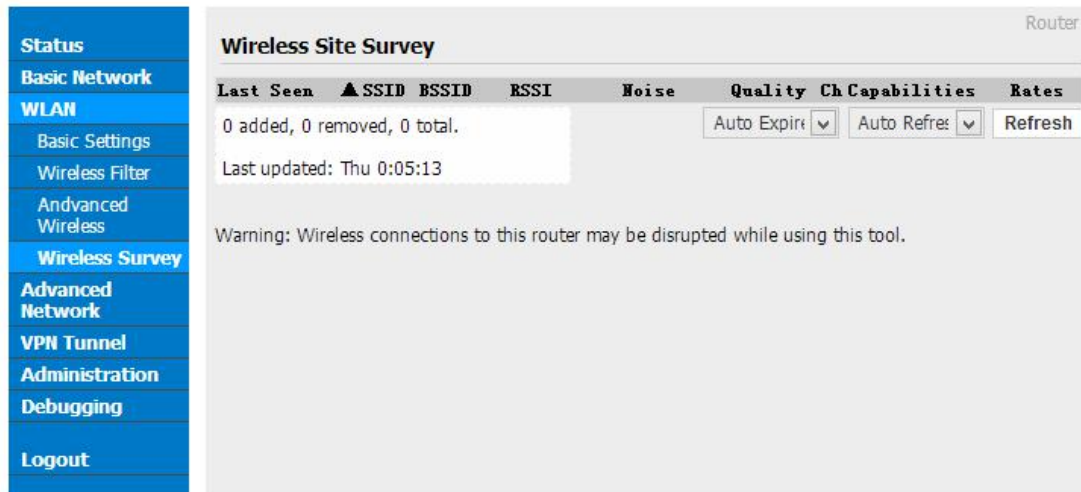


Figure 3-9 Wireless Survey Setting GUI

----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.

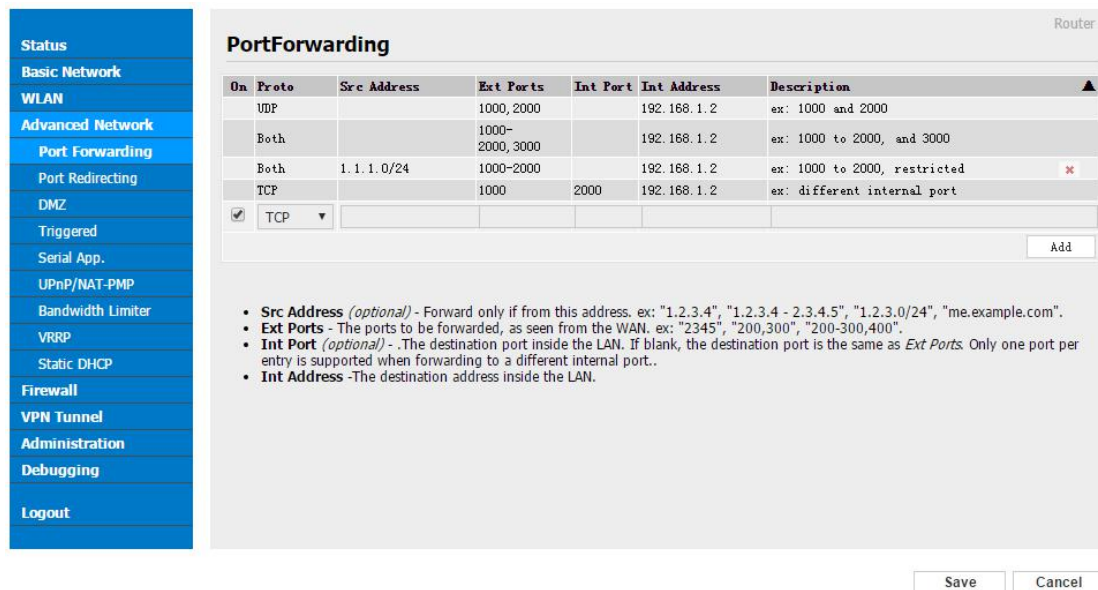


Figure 3-10 Port Forwarding GUI

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.

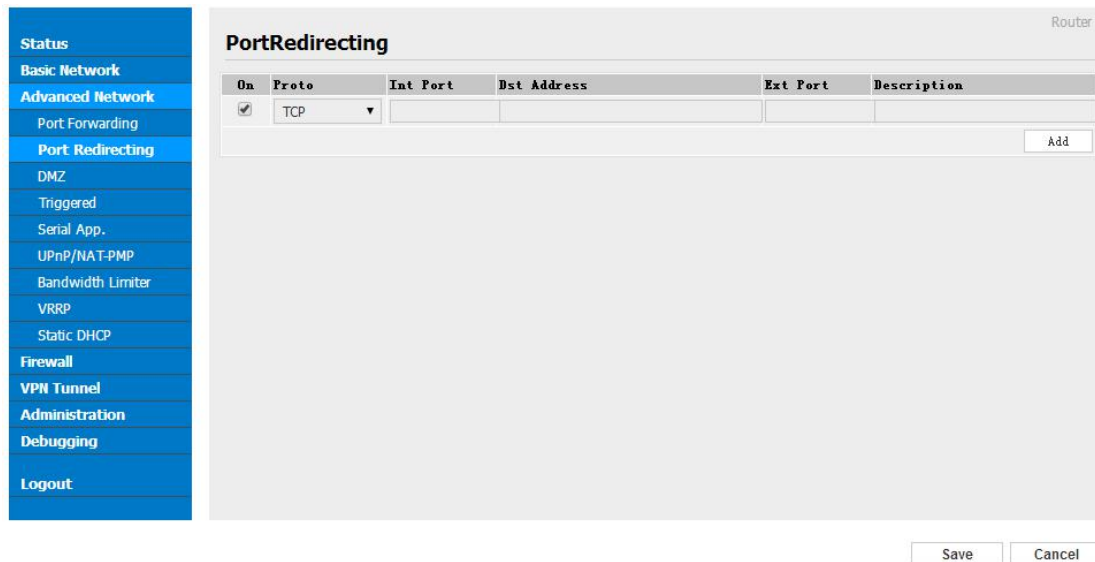


Figure 3-11 Port Forwarding GUI

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.

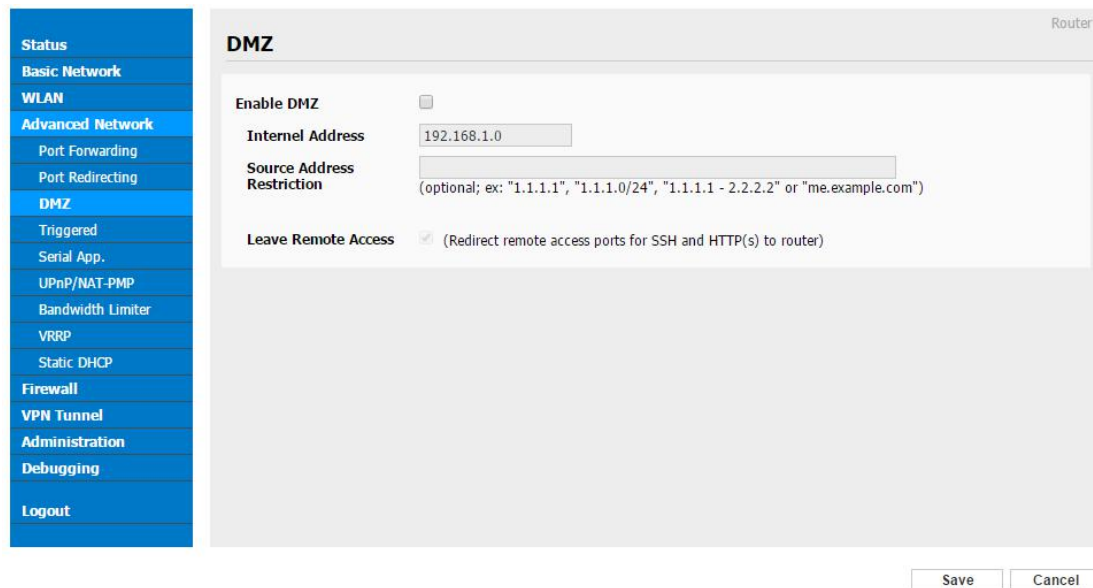


Figure 3-12 DMZ GUI

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.

parameter	Instruction
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.

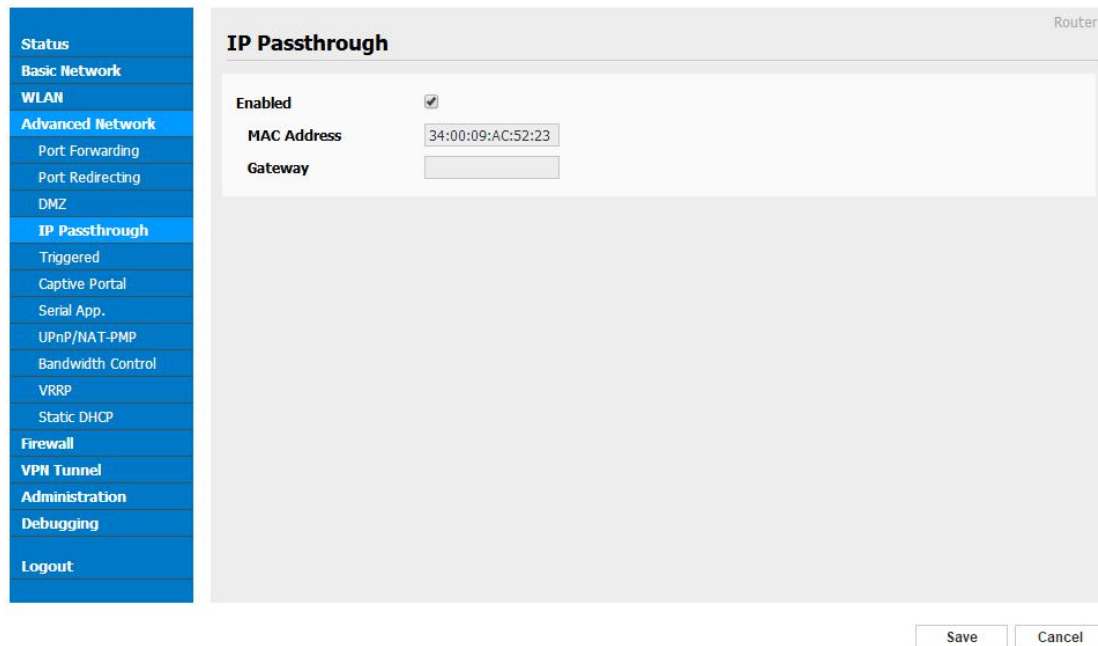


Figure 3-13 IP Passthrough GUI

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

Step 2 Please click "save" to finish

----End

3.4.5 Triggered Setting

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

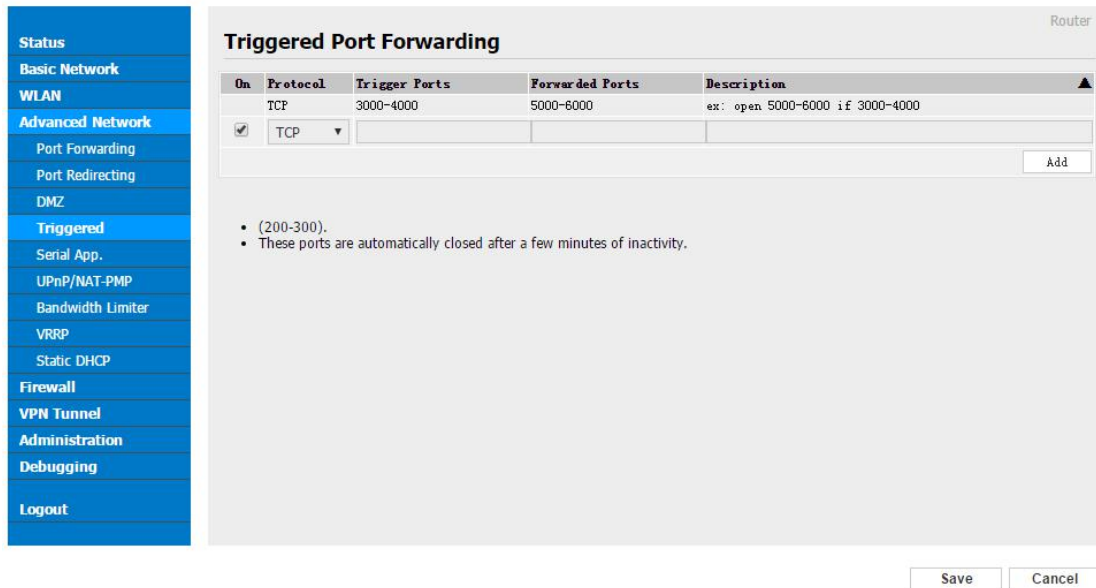


Figure 3-14 Triggered GUI

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.

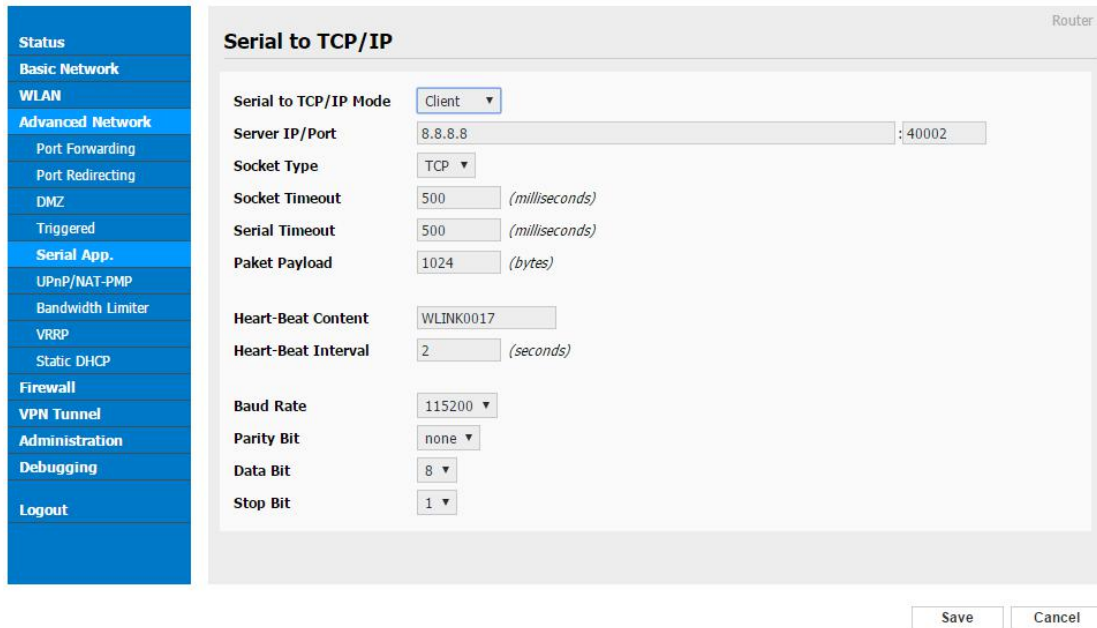


Figure 3-15 Serial App Setting GUI

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

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.

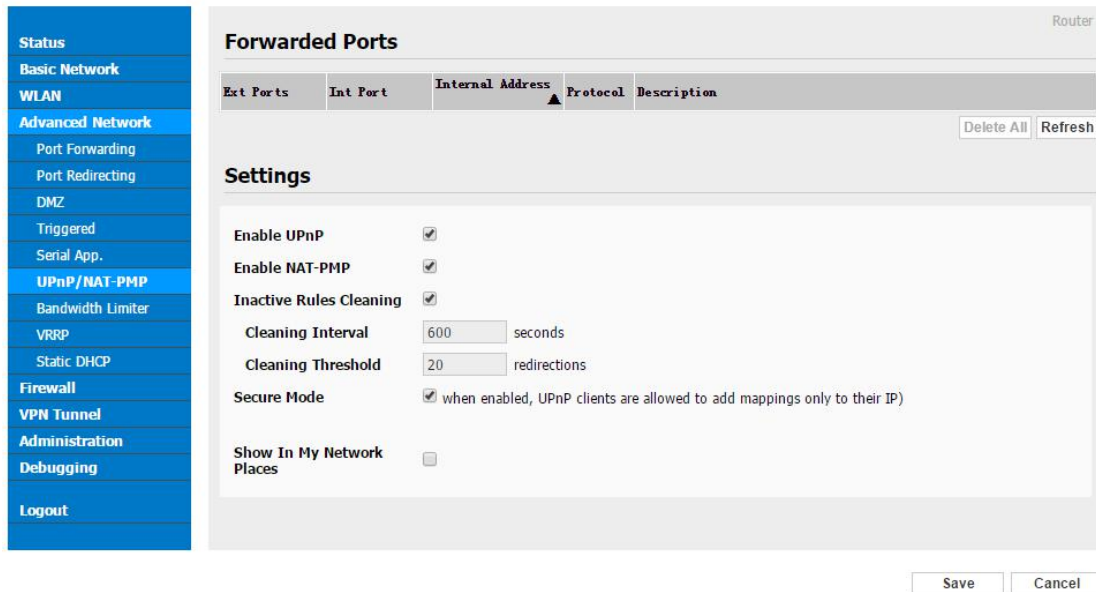


Figure 3-16 UPnp/NAT-PMP Setting GUI

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.

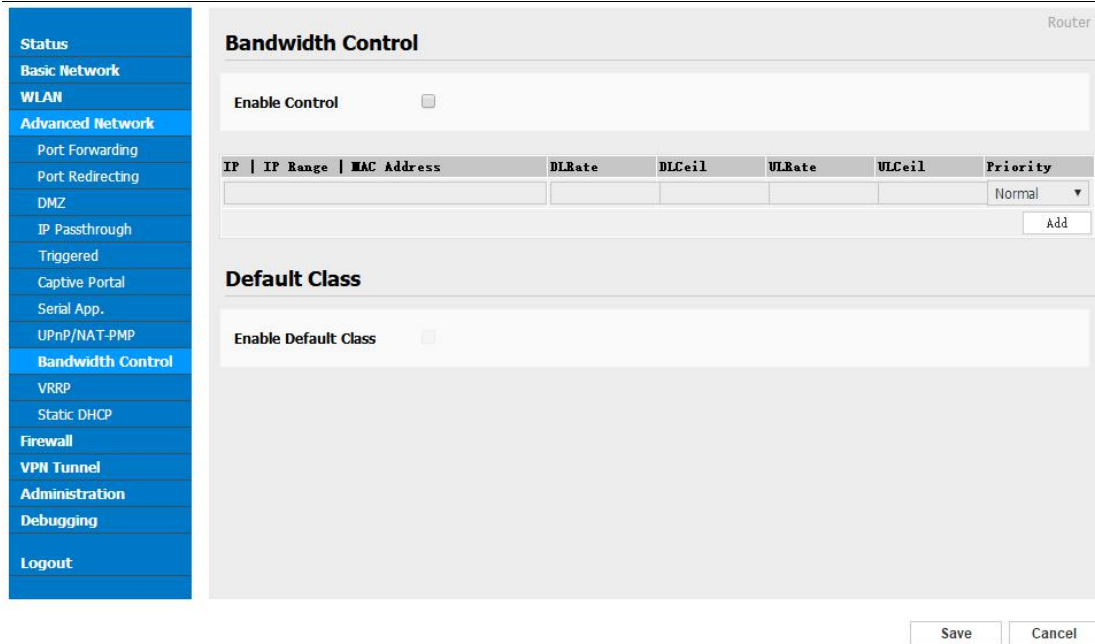


Figure 3-17 Bandwidth Control Setting GUI

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.

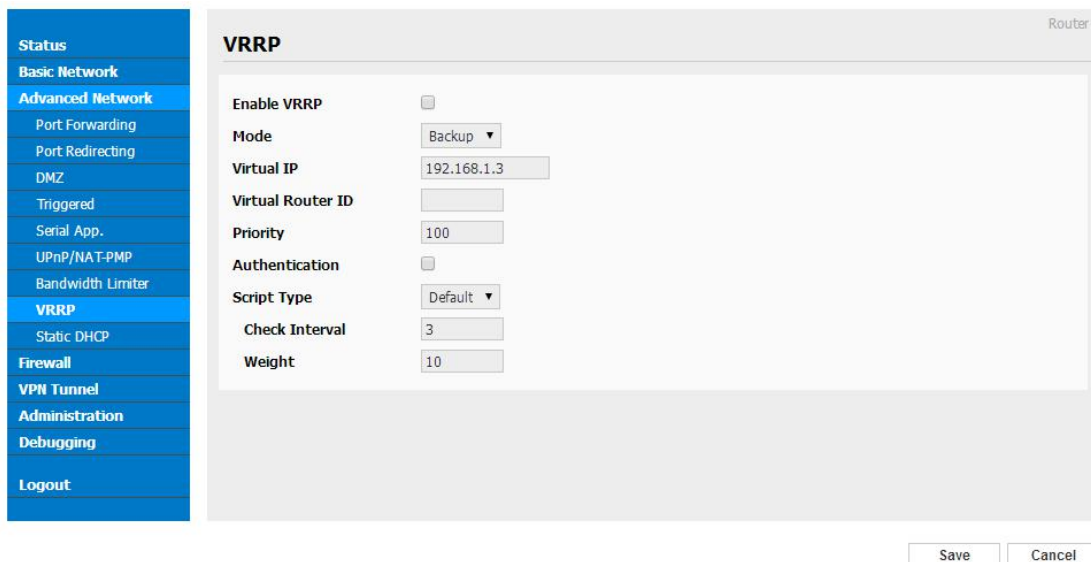


Figure 3-18 VRRP Setting GUI

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.

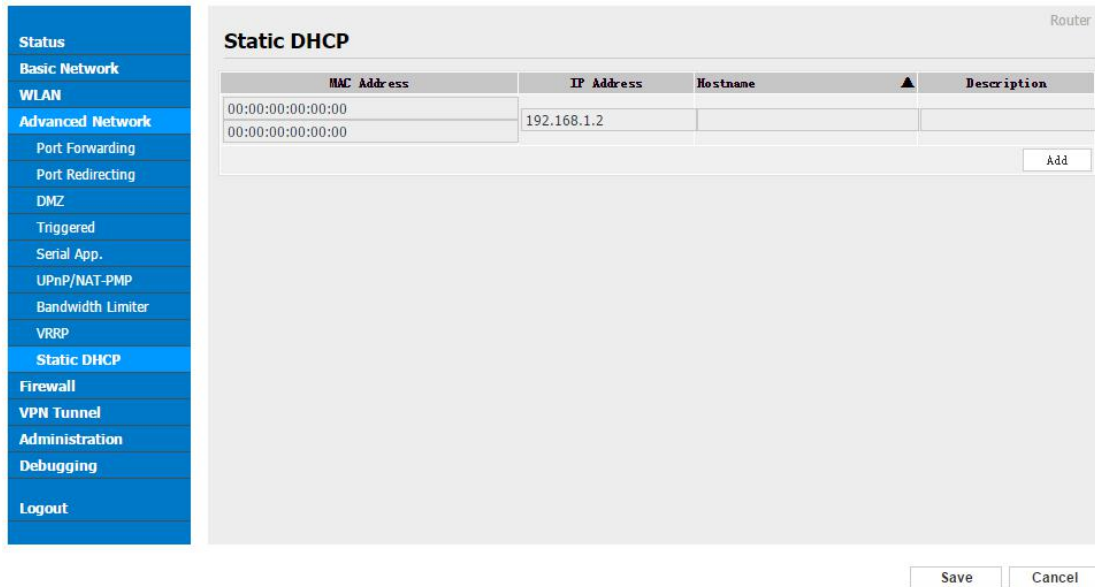


Figure 3-19 Static DHCP Setting GUI

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.

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 Please click “save” to finish.

3.5.2 Domain Filtering

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



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.



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.

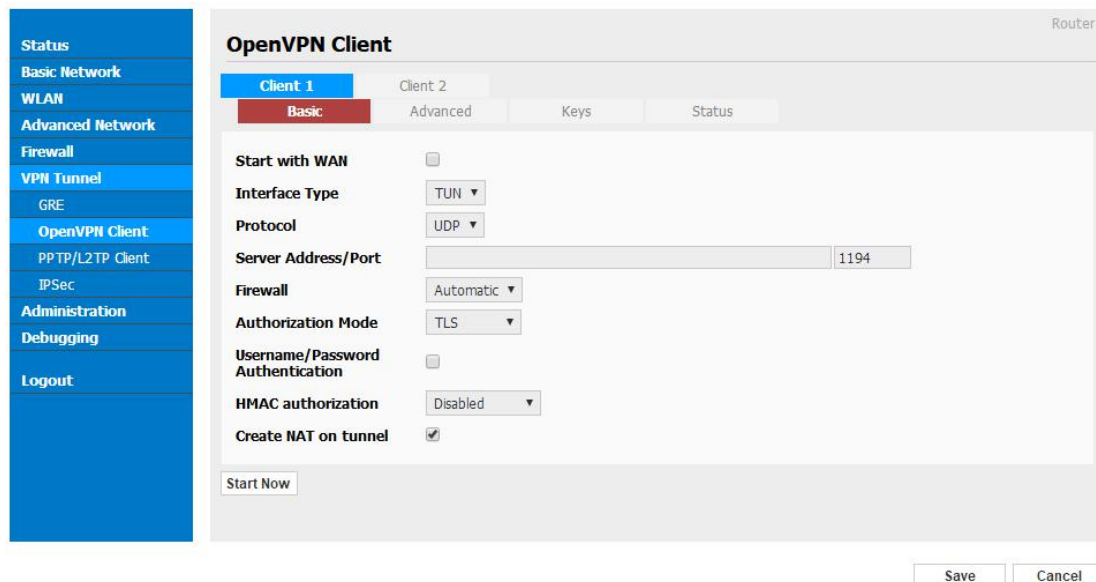
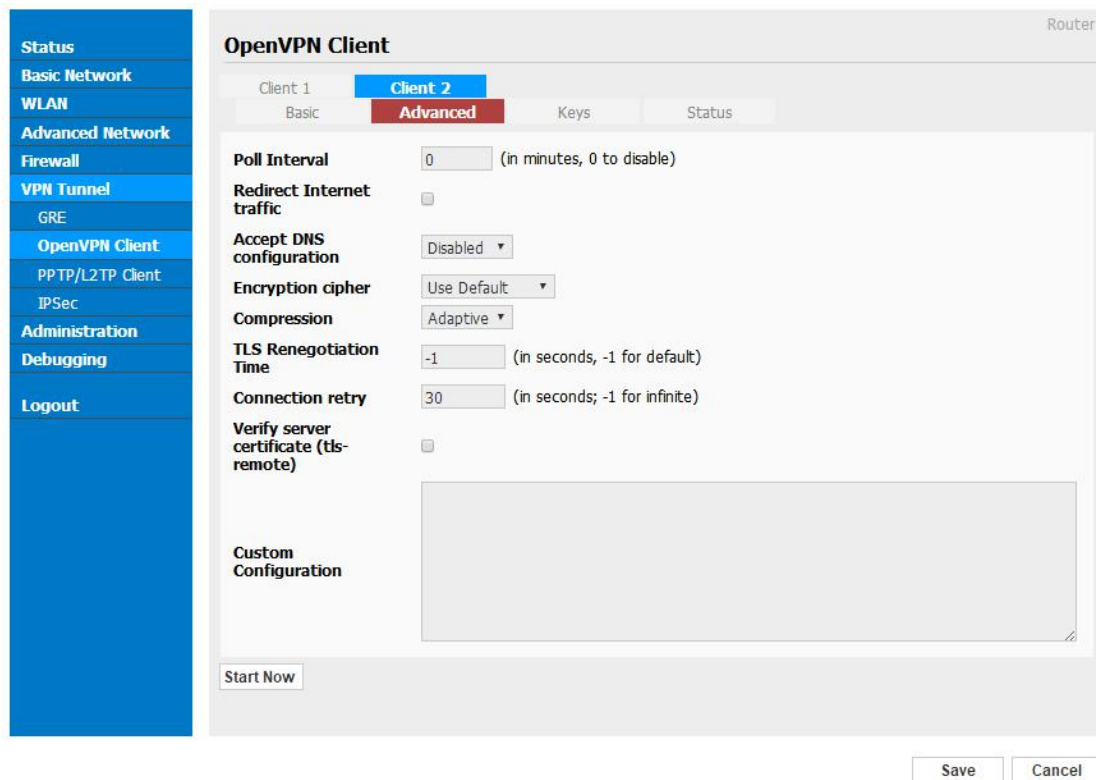


Figure 3-22 OpenVPN Setting GUI

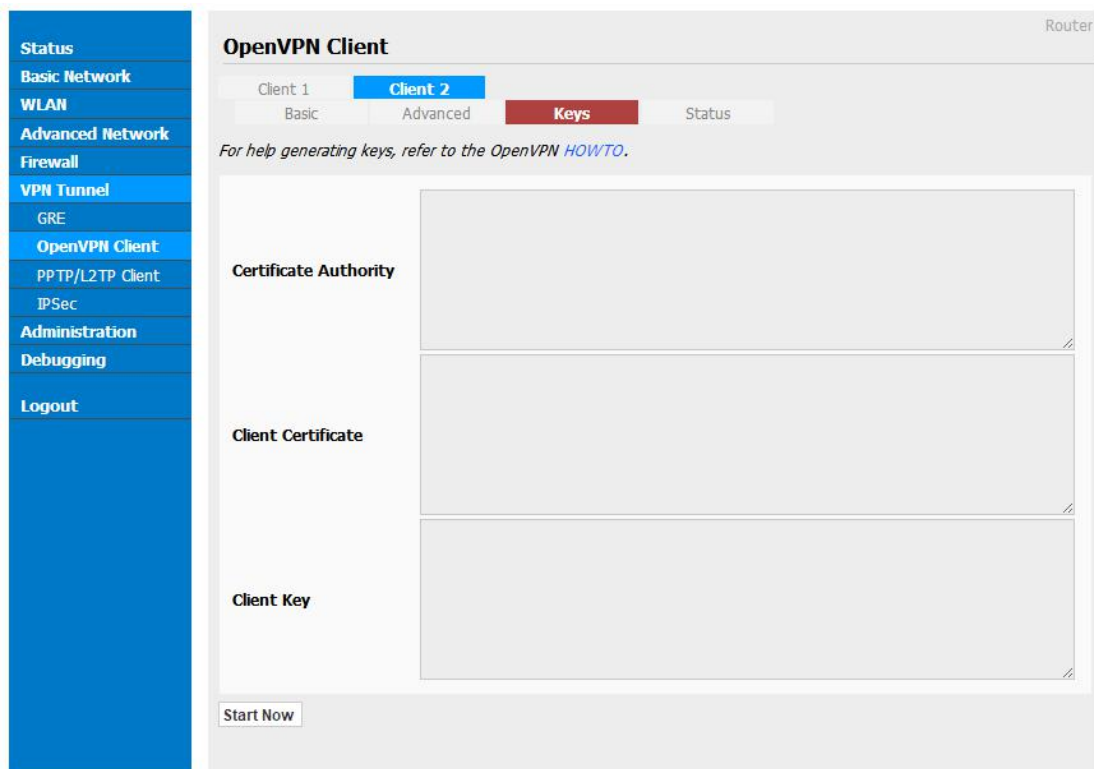
Table 3-17 “OpenVPN” Instruction

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.



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.



Parameter	Instruction
Certificate Authority	Keep certificate as the same as server
Client Certificate	Keep client certificate as the same as server
Client Key	Keep client key as the same as server

Parameter	Instruction
General Statistics	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.

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

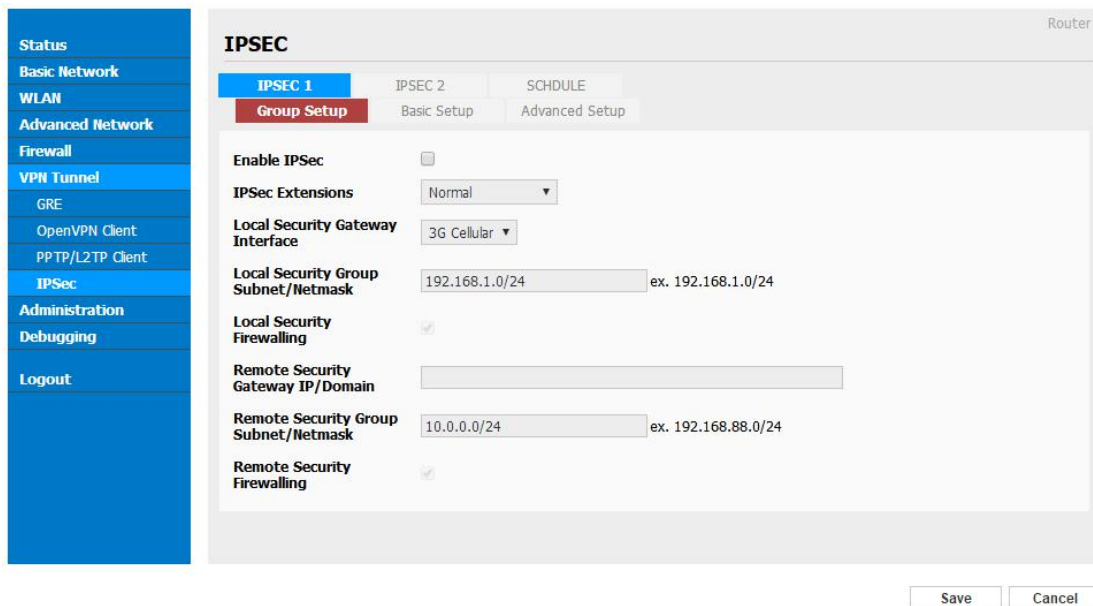
Table 3-21 "SCHEDULE" Instruction

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



3.5.3.1 IPsec Group Setup

Step 1 Please click "IPsec> Group Setup" to check or modify the relevant parameter.

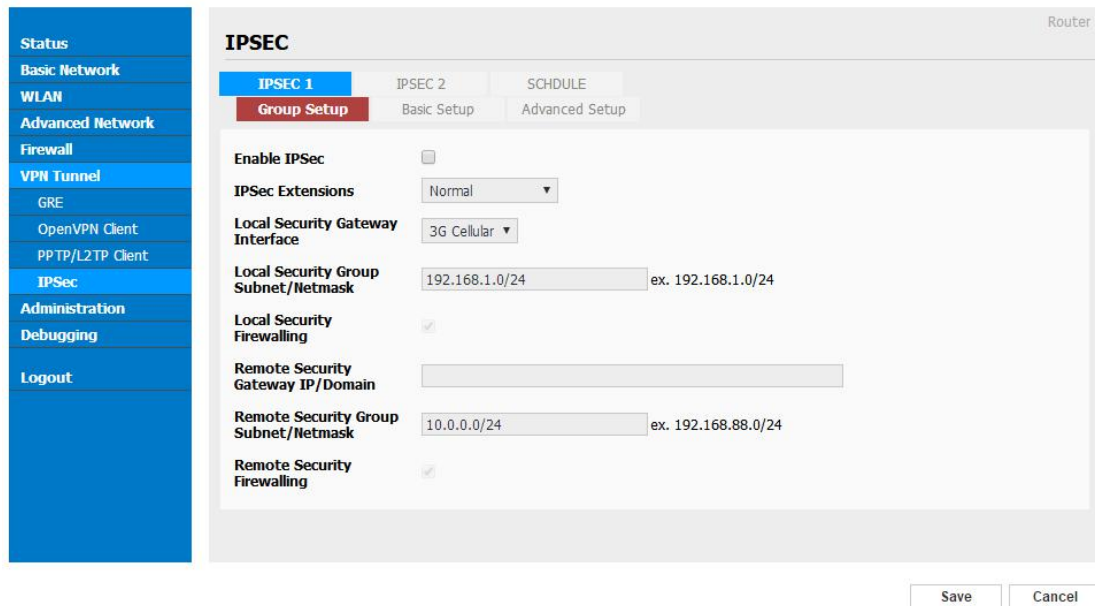


Table 3-22 “IPSec Group Setup” Instruction

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.

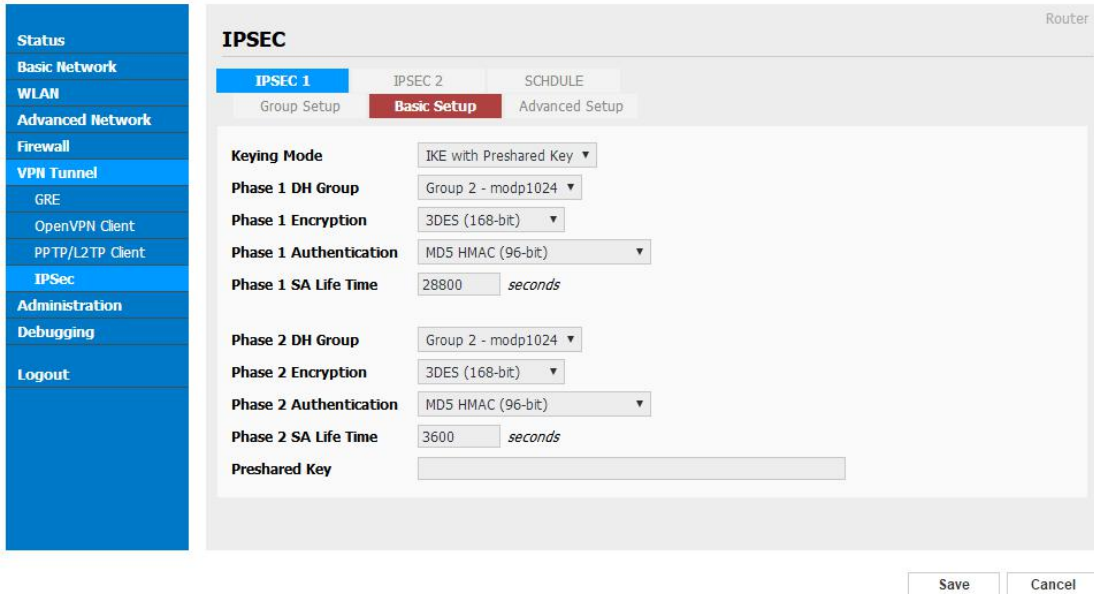


Table 3-23 “IPSec Basic Setup” Instruction

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.

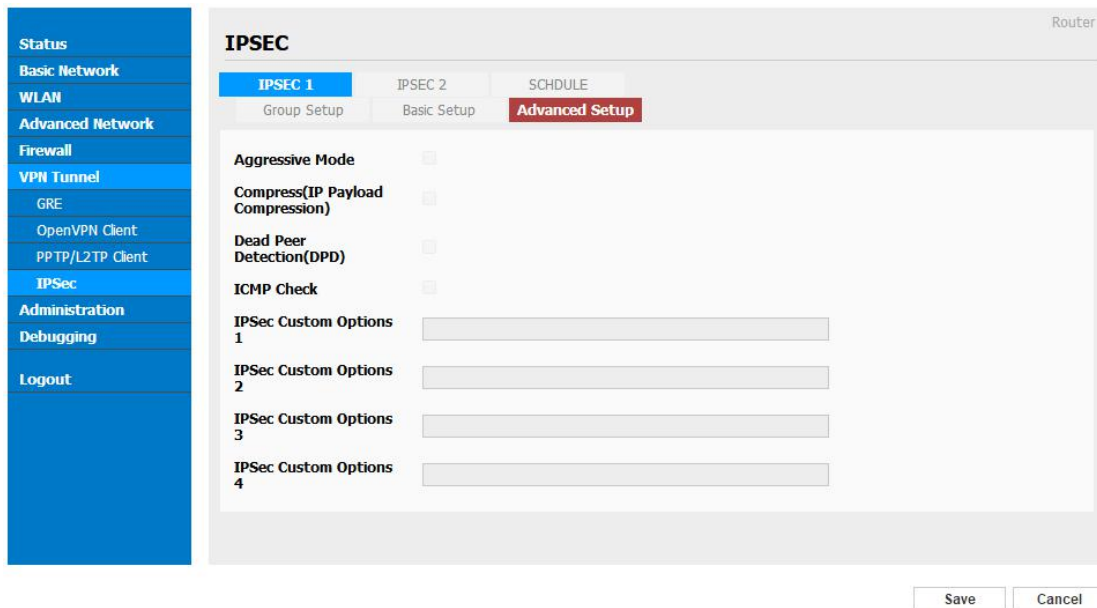


Table 3-24 “IPSec Advanced Setup” Instruction

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 System Management

3.7.1 Identification Setting

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

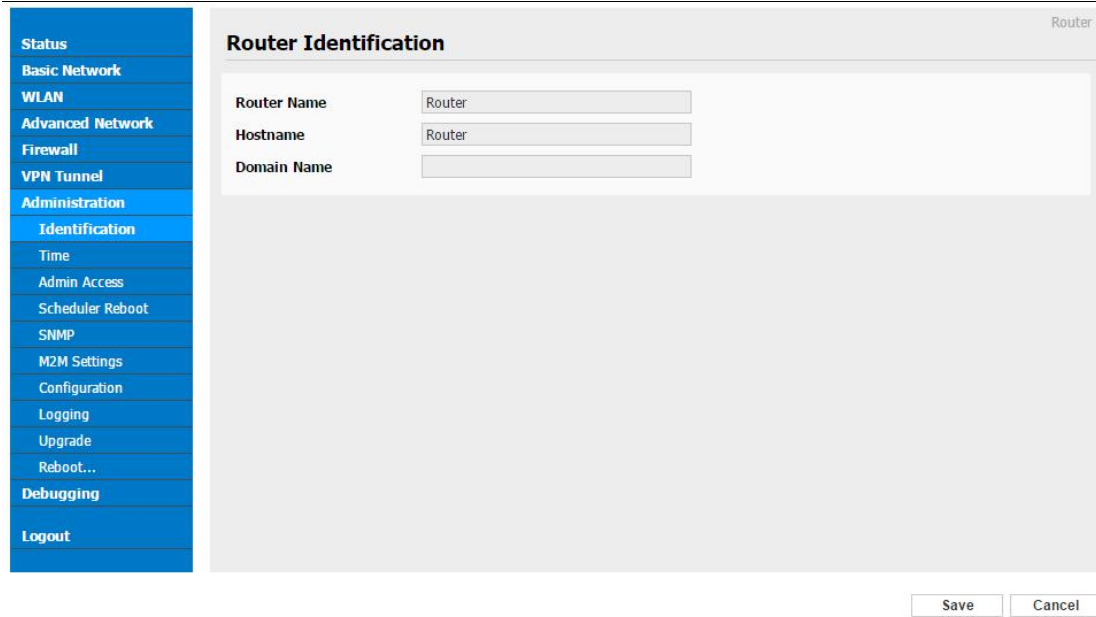


Figure 3-23 Router Identification GUI

Table 3-25 “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.

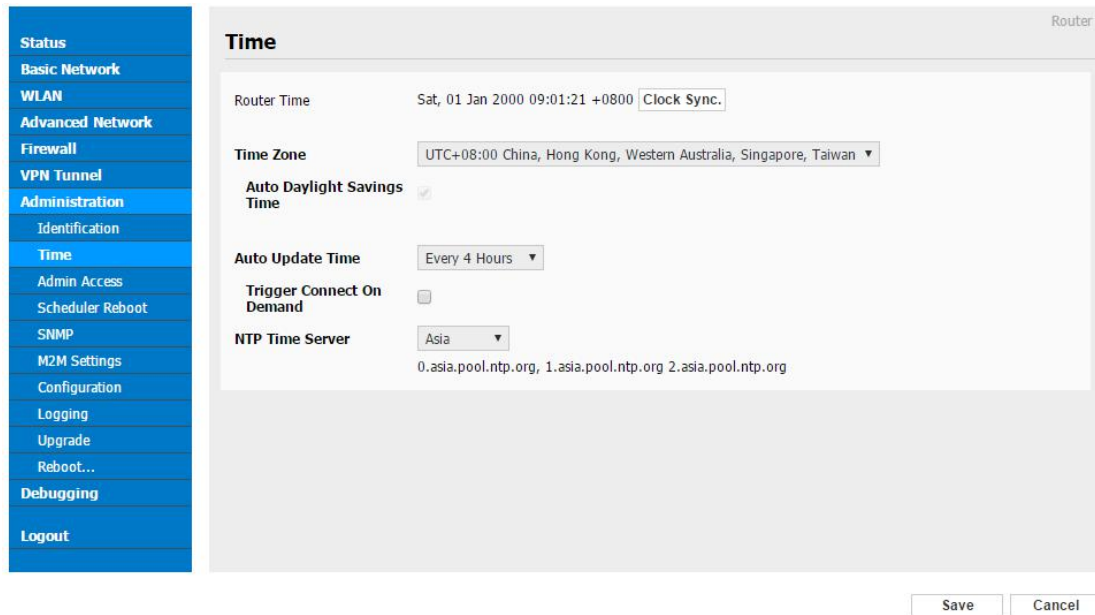


Figure 3-24 System Configuration GUI



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

Step 2 Please click “save to finish.

----End

3.7.3 Admin Access Setting

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

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

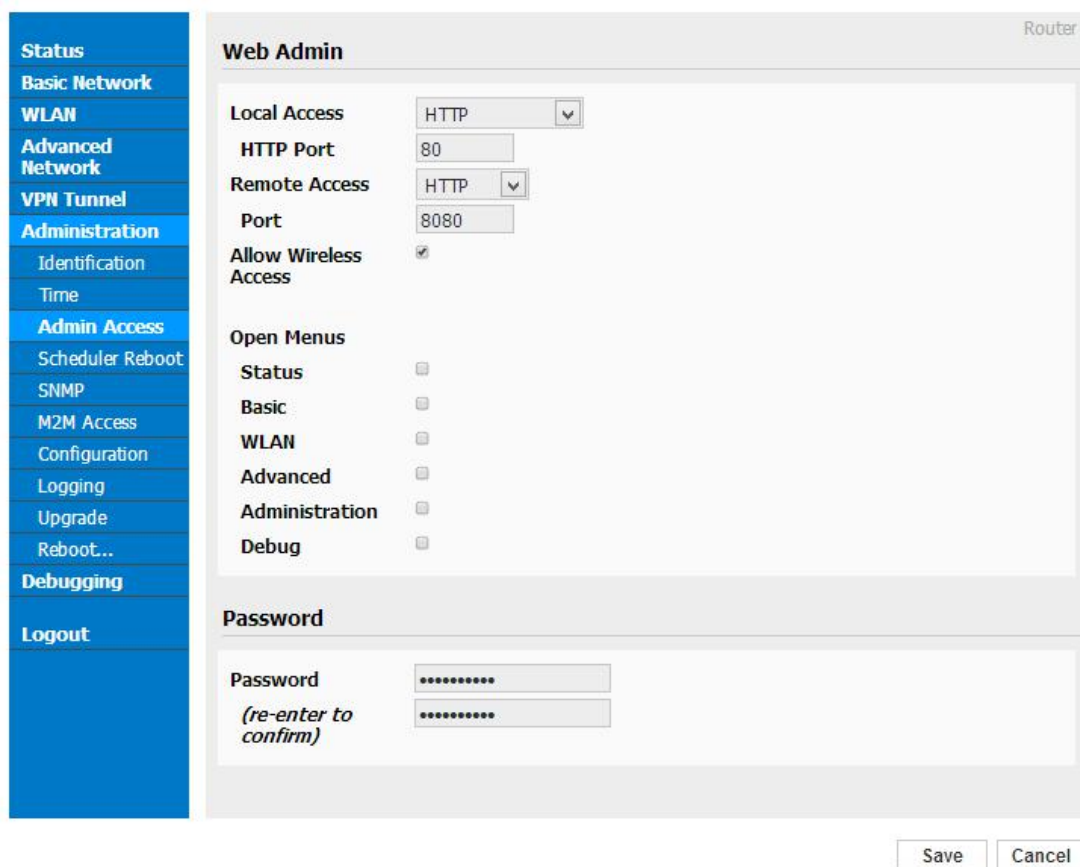


Figure 3-25 Admin Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.7.4 Schedule Reboot Setting

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

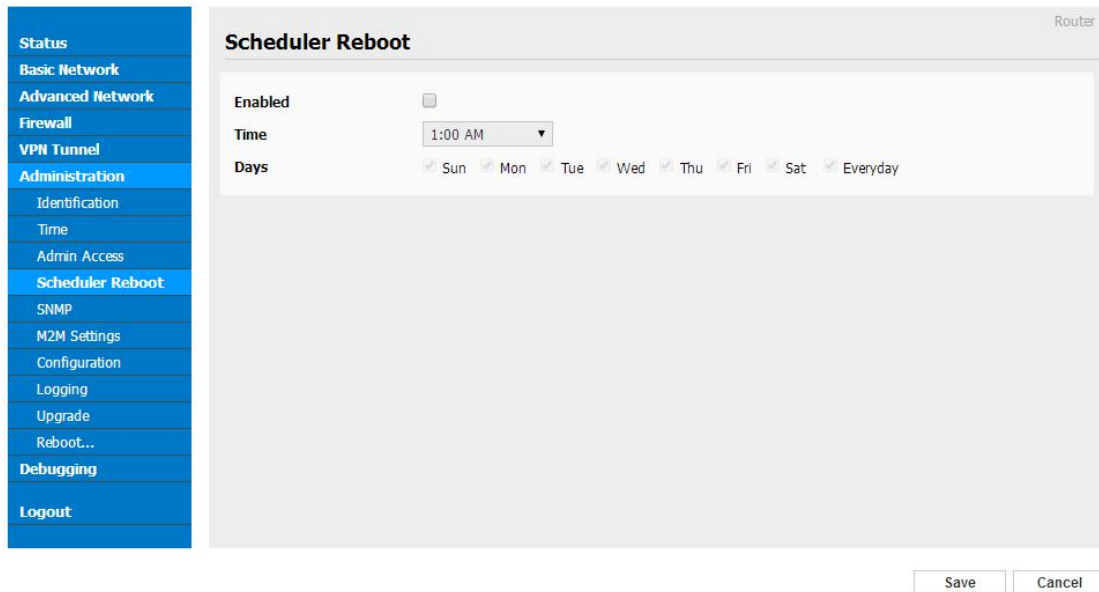


Figure 3-26 Scheduler Reboot Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.7.5 SNMP Setting

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

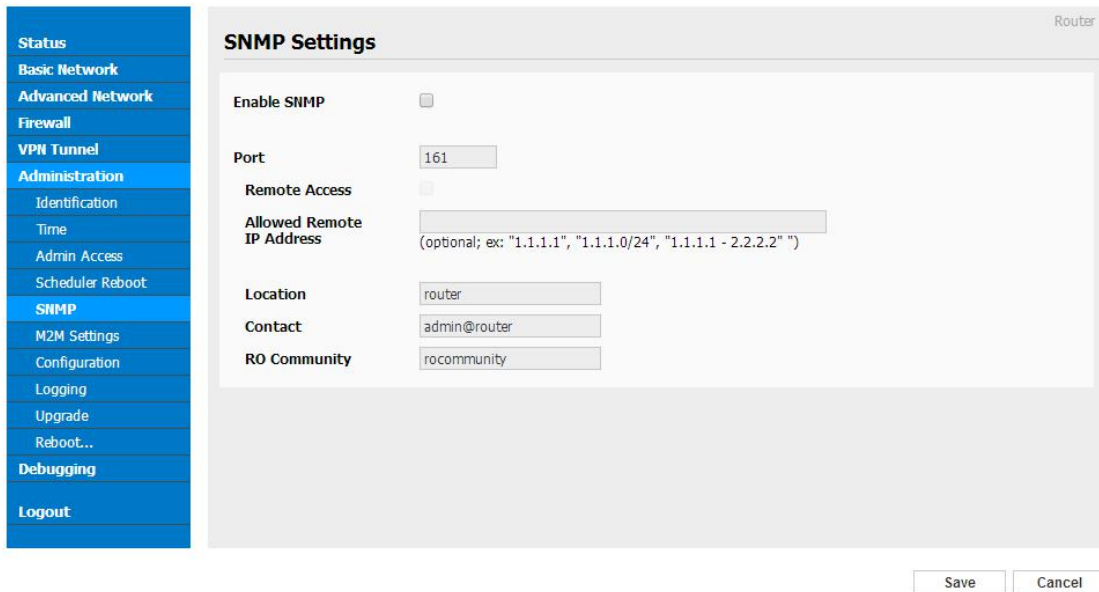


Figure 3-27 SNMP Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.7.6 M2M Access Setting

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

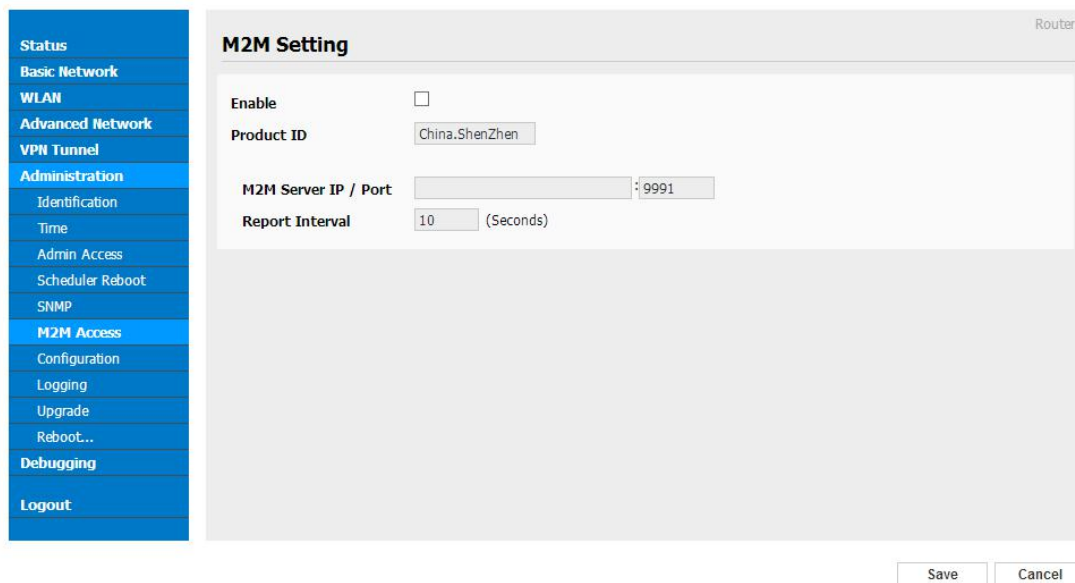


Figure 3-28 M2M Access Setting GUI

Parameter	Instruction
M2M Enable	Enable/Disable M2M feature in router.
Device ID	Identify router in M2M Platform. Max length 24bytes and Min length 7bytes visible characters.
M2M Server/Port	Configure M2M platform IP and port. The router will log in M2M platform and establish a connection between router and M2M platform. The connection protocol is UDP.
Heartbeat Interval	Router send heartbeat to M2M platform as the defined time interval to keep connection.

Step 2 Please click save iron to finish the setting

----End

3.7.7 Backup Setting

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

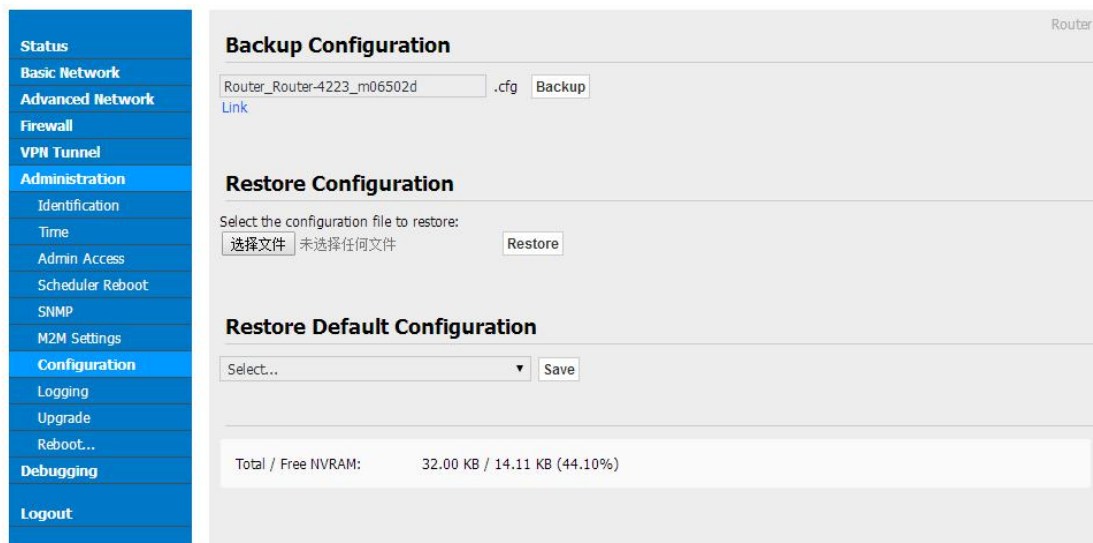


Figure 3-29 Backup and Restore Configuration GUI



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

3.7.8 System Log Setting

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

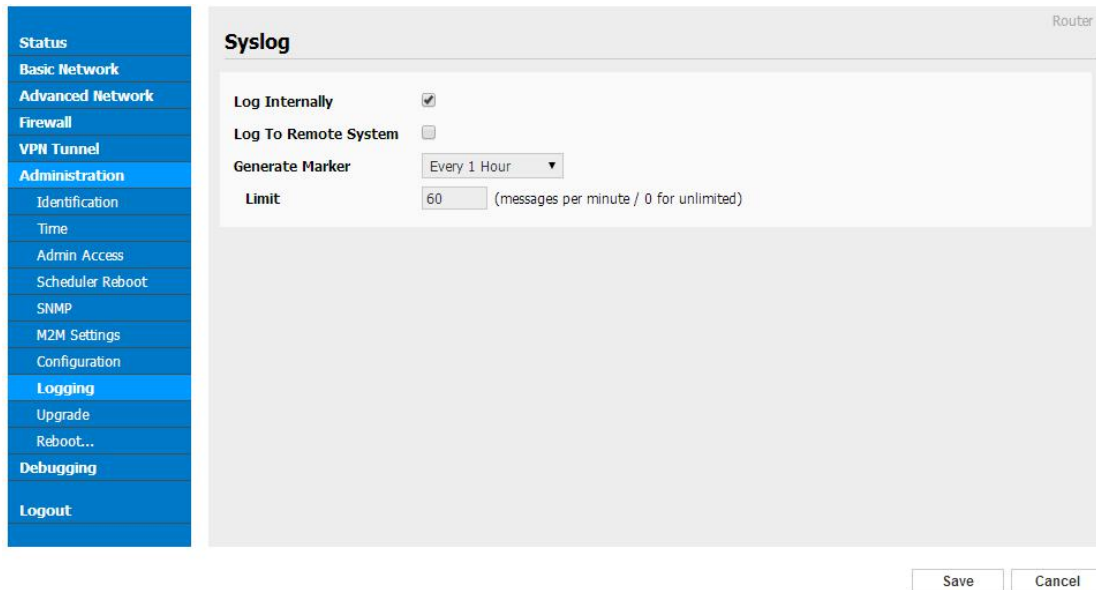


Figure 3-30 System log Setting GUI

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

----End

3.7.9 Firmware upgrade

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



Figure 3-31 Firmware Upgrade GUI



NOTE

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

3.7.10 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.

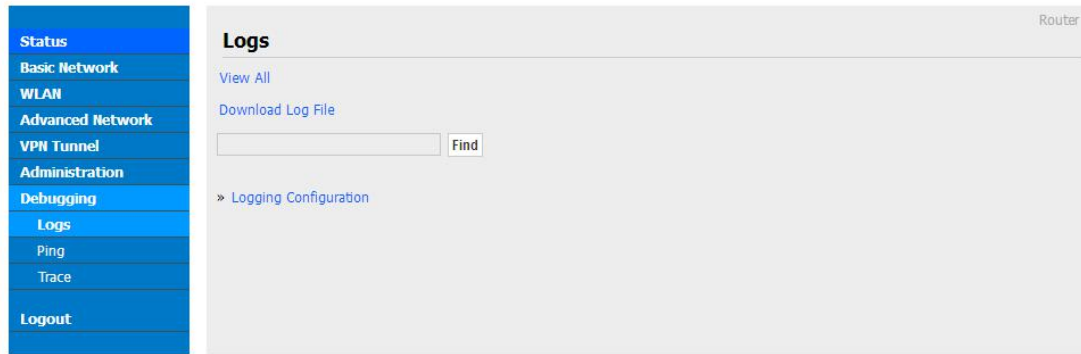


Figure 3-32 Logs GUI

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

----End

3.8.2 Ping Setting

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



Figure 3-33 Ping GUI

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

----End

3.8.3 Trace Setting

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

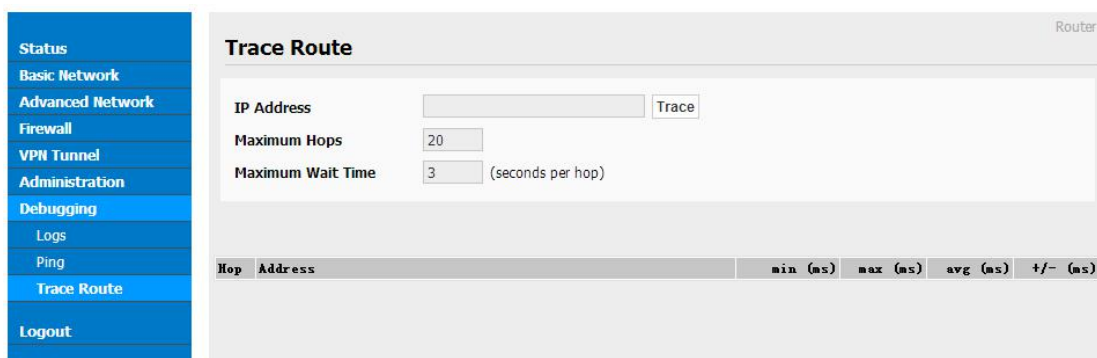


Figure 3-34 Trace GUI

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

---End

3.9 “RST” Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way. For R200 Series, “RST” button is on the left or Ethernet port, for R520 Series, the button is on the left of NET light. This button can be used when the router is in use or when the router is turned on.

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

Table 3-26 System Default Instruction

Parameter	Default setting
LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP server	Enable
User Name	admin
Password	admin



NOTE

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

3.10 Appendix (For GPS, Captive Portal & OpenVPN only)

3.10.1 GPS Setting

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

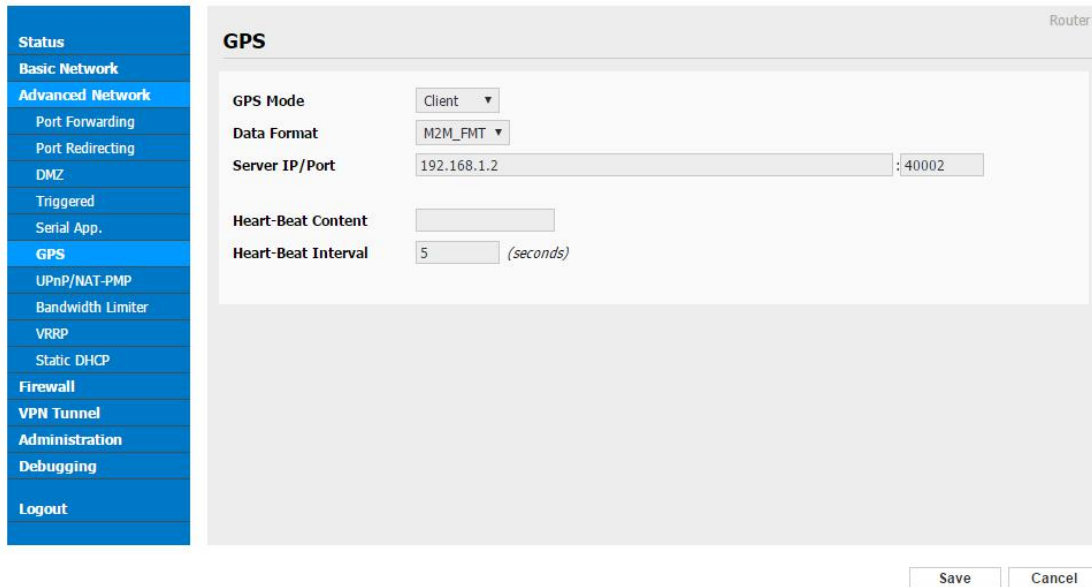


Figure 3-35 GPS Setting GUI

Table 3-27 “GPS” Instruction

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

Step 2 Please click "save" to finish



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.ss s	043215.0	UTC Time, Time of position fix.
4	gps_use	numeric	06	Satellites Used, Range 0 to 12.
5	gps_latitude	ddmm.mm mm	2234.248130	Latitude, Degrees + minutes.
6	gps_NS	character	N	N/S Indicator,N=north or S=south.
7	gps_longitude	ddmm.mm mm	11356.626179	Longitude, Degrees + minutes.
8	gps_EW	character	E	E/W indicator, E=east or W=west.
9	gps_speed	numeric	0.0	Speed over ground, units is km/h.
10	gps_degrees	numeric	91.5	Course over ground, unit is degree.
11	gps_FS	digit	1	Position Fix Status Indicator,
12	gps_HDOP	numeric	1.2	HDOP, Horizontal Dilution of Precision
13	gps_MSL	numeric	97.5	MSL Altitude, units is meter.

3.10.2 Captive Portal Setting

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

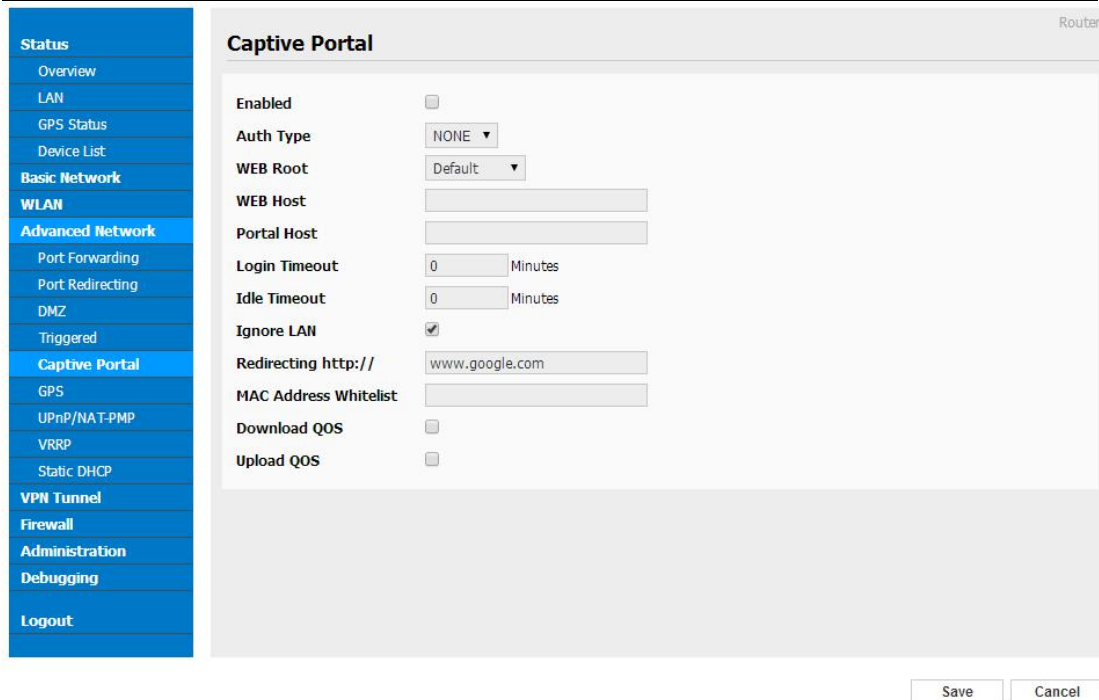


Figure 3-36 Captive Portal Setting GUI

Table 3-28 “Serial App” Instruction

Parameter	Instruction
Enable	Enable Captive portal feature.
Auth Type	Reserved.
Web Root	Choose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router’s Flash. Ex-storage: Captive portal file is in extended storage such as SD card.
Web Host	Configure domain name for the captive portal access. For example, Configure as wlink.tech.com, we might directly access to captive portal page in the website as wlink.tech.com
Portal Host	Reserved.
Logged Timeout	Maximum time user has connectivity. User need to re-login Captive Portal page after defined time.
Idle Timeout	Maximum time user has connectivity if no network activity from Wi-Fi User.If User need to re-login Captive page to surf internet.
Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.
Redirecting	Router will redirect to the defined link after accepting the terms and conditions on the Captive Portal page.

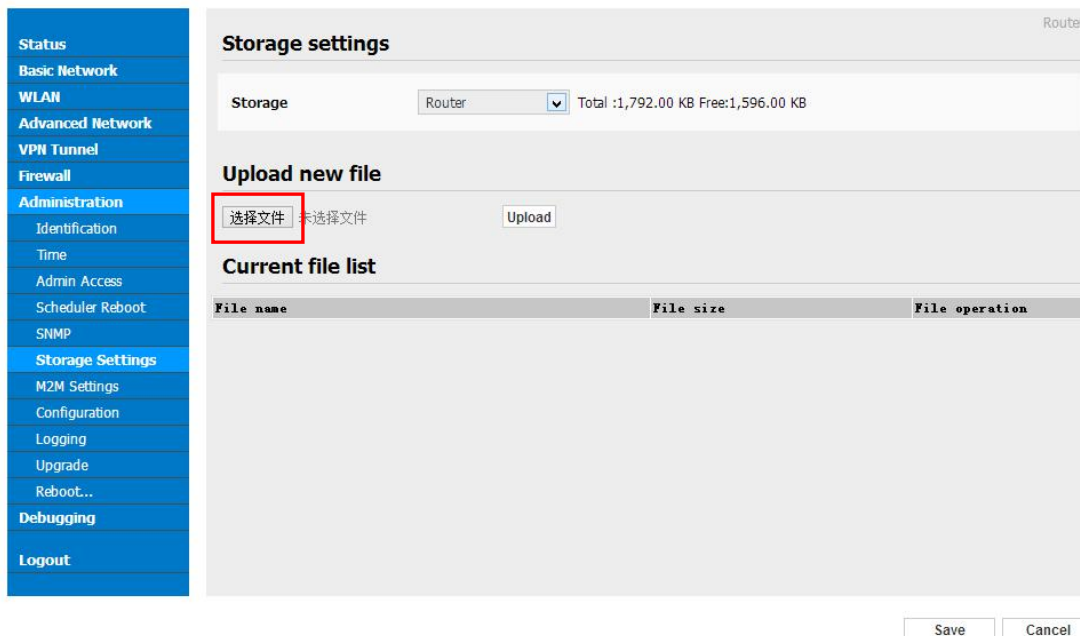
Parameter	Instruction
MAC Whitelist	No captive portal page for Wi-Fi device.
Download QoS	Enable to apply the Download and Upload per user limits.
Upload QoS	Maximum download speed available to each user.



1) Upload Portal file and Splash.html by local

Upload portal images and splash.html in router for the Slider (0001_portal.png, 0002_portal.png, and 0003_portal.png) to the Router under the “Administration / Storage Settings” menu.

Furthermore, also might upload splash with images together.



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

```

<!-- <hr> -->

<div id="myCarousel" class="carousel slide marketing">
  <ol class="carousel-indicators">
    <li data-target="#myCarousel" data-slide-to="0" class="active"></li>
    <li data-target="#myCarousel" data-slide-to="1"></li>
    <li data-target="#myCarousel" data-slide-to="2"></li>
  </ol>

  <div class="carousel-inner">
    <div class="item active">
      
    </div>
    <div class="item">
      
    </div>
    <div class="item">
      
    </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> -->
    
```

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

Identification

Time

Admin Access

Scheduled Reboot

SNMP

Storage Settings

M2M Settings

Configuration

Logging

Upgrade

Reboot...

Debugging

Logout

Router

Storage settings

Storage Router Total :1,664.00 KB Free:1,088.00 KB

Upload new file

未选择任何文件

Current file list

File name	File size	File operation
0001_portal.png	60.7K	✖ ⬇
0002_portal.png	45.3K	✖ ⬇
0003_portal.png	46.0K	✖ ⬇
bootstrap-responsive.min_portal.css	16.5K	✖ ⬇
bootstrap-responsive_portal.css	21.6K	✖ ⬇
bootstrap.min_portal.css	103.5K	✖ ⬇
bootstrap.min_portal.js	27.8K	✖ ⬇
bootstrap_portal.css	124.3K	✖ ⬇
bootstrap_portal.js	60.1K	✖ ⬇
jquery.client_portal.js	5.9K	✖ ⬇
jquery.md5_portal.js	9.4K	✖ ⬇
jquery_portal.js	262.1K	✖ ⬇
splash.html	3.4K	✖ ⬇

```
<!-- <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">
      
    </div>
    <div class="item">
      
    </div>
    <div class="item">
      
    </div>
  </div>
  <a class="left carousel-control" href="#myCarousel" data-slide="prev">&lsaquo;</a>
  <a class="right carousel-control" href="#myCarousel" data-slide="next">&rsaquo;</a>
</div>

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

---End

2) Modify portal file storage path

Modify portal file storage for In-storage as below.


Cellular Router

Status

Basic Network

WLAN

Advanced Network

Port Forwarding

Port Redirecting

DMZ

IP Passthrough

Triggered

Captive Portal

Serial App.

UPnP/NAT-PMP

Bandwidth Control

VRRP

Static DHCP

Firewall

VPN Tunnel

Administration

Debugging

Logout

Captive Portal Router

Enabled

Auth Type

WEB Root

WEB Host

Portal Host

Ex-storage

Login Timeout Minutes

Idle Timeout Minutes

Ignore LAN

Redirecting http://

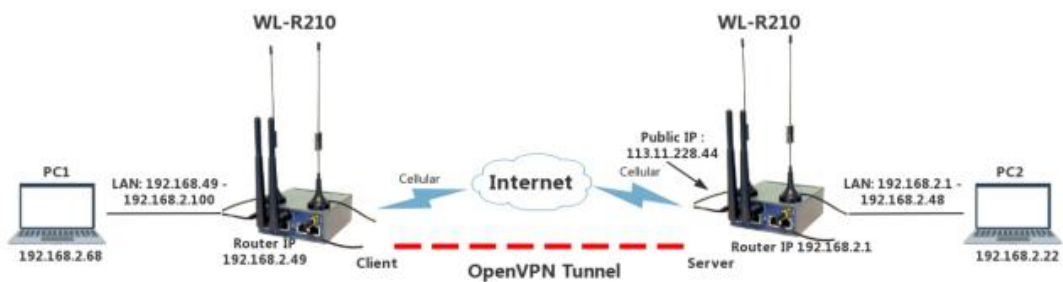
MAC Address Whitelist

Download QOS

Upload QOS

3.10.3 OpenVPN Demo (TAP Mode)

1) Network topology



2) OpenVPN Server Config Demo

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Server

OpenVPN Client

VPN Client

Administration

Debugging

Logout

Router

OpenVPN Server Configuration

Server 1

Server 2

Keys

Status

Basic

Advanced

Keys

Status

Start with WAN

Interface Type TUN ▾

Protocol UDP ▾

Port 1194

Firewall Automatic ▾

Authorization Mode TLS ▾

Extra HMAC authorization (tls-auth) Disabled ▾

VPN subnet/netmask 10.8.0.0 255.255.255.0

Start Now

Save
Cancel

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Server

OpenVPN Client

VPN Client

Administration

Debugging

Logout

Router

OpenVPN Server Configuration

Server 1

Server 2

Keys

Status

Basic

Advanced

Keys

Status

Poll Interval 0 (in minutes, 0 to disable)

Push LAN to clients

Direct clients to redirect Internet traffic

Respond to DNS

Encryption cipher Use Default ▾

Compression Adaptive ▾

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

Manage Client-Specific Options

Allow User/Pass Auth

Custom Configuration

Start Now

Save
Cancel

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Server

OpenVPN Client

VPN Client

Administration

Debugging

Logout

OpenVPN Server Configuration

Server 1
Server 2

Basic
Advanced
Keys
Status

For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

```

y2ywwp00tP1C0vX1Q0P1Pc7dxyDQWj00cH10bMv1MCAWEAA0B+1CbsjAubgnv
HQ4EFgQUH18dzrp+ZC7m08L/uQF0RWqOjhgZekZQwgZEXcZAJBgNVBAYTAklOMQswCQYDVQIQEwJH
+ZC7m08L/uQF0RWqOjhgZekZQwgZEXcZAJBgNVBAYTAklOMQswCQYDVQIQEwJH
RDELMAGAIUEBxMCU1oxDTALBgNVBAoTBFRFU1QxFDA5BgNVBAsTC29wZW52cG50
ZXN0MRAwDgYDVQDEwURVNUENBMRAwDgYDVQDEwDFYXN5UINBMR8wHQYJKoZI
hvcNAQkBFB0ZXN0QGV4YW1wbGUuY292ggkA4Se3cv19gOYwDAYDR0TBAUwAwEB
/zANBgkqhkiG9w0BAQsFAAOCAQEASbzApdBKzv7bz8WzryoX2yZ6XY3hVz9o0WJ
F73ISnDzUjKJgb5sfPUW4W3UlRtDbwLlQkQkphj30hAyGdgfQP7fxJ2JOi6Mkr
q3R53o+MXgISeN8vvtQICPbl0K5cygohFqgOoeD+JceSNUEA1U1FmJAQviupR6S
          
```

Server Certificate

```

-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAF8F53VpA0MKwB+GShyF17hN4NMNM/k10kYog+d5NEsp+Y7HY6+tn1
wNnr8dkZR8kKhpKwz9sRp5XfE8oX/Idsto6f1m8I2pLMvIs0QEbEVh53nkWwV
ofqaknbhKzB/Wcm61IpwBxeBoZARViuG1NSAQAQpk2cqW/LVA+3Yh64g0pHszd
VkgHHczTJBNjaooe7K50c2/GuhLlr+tHIP1qq0AJhBeRG9+paVjdc2vQmkVh5TA
+b/WewO41NMBO6dvJB95TsdVad8k2Qg8CWf+ox8Xt9vm8yf/U6UBLXFF5U0SFV
W9TugcABXoR0kqb1p7awbITgpHJL1gP/gwIBAg==
-----END DH PARAMETERS-----
          
```

Server Key

```

IDCBkTELMAGAIUEBhMCQ04xCzAJBgNVBAGTAkdEMQswCQYDVQQHEwJTWJENMAsG
A1UEChMEVYTVDEUMBIGA1UECkMlB3BlbnZwbmRlc3QxZDA0BgNVBAMTB1RFU1Qg
Q0ExEDA0BgNVBCKTB0Vhcz3SU0ExHzAdBgkqhkiG9w0BCQEWEHric3RAZXBhbXBs
ZS5jb22CCQDhJ7dy/X2A5JATBGNVHSUEDDAKBggrBgEFBQcDA TALBgNVHQ8EBAMC
BaAwEQYDV0R0RBAowCIIgc2VydmlvMA0GCSqGSIb3DQEBCwUAA4IBAQApmQ0VbJ7
u2rtX+SXR63BAoQ4oslWUD7/J0xbY6HldJ3/C5bH9IHx2nKrOACB2S1LfbMsCN
v4IC88aN+A4Hu5zJ8St8j5F2NEImB4MlyZ+A+uaxsp4YwD7eeOvfne1dKiq0Ld
GF5idBCif7tG5hmg4rHbLWgLC2rpeMVQranXau2b9B2/Zj3/h+qp8LJ8I2Ih0V
45Js2ZtCW90+yZwW/X60d2SKffW0yRZMDO9SnX8Gc1s8eifLdON3ZuCO4izMKyp3
VnFBHpd0u0cVvziWk0u08aj0u0u0g0c1j1m0u0p1cuzp1x0u0m0a5su0z0nHecZ4T9K
IX5YLo2Y10xNgnokJwGtoN7aMhRCdKrACaisd1t5KrgP3plywdguJhXIAMk1S9c
eLbhny/N6wKBQDIe/9uq+3klYBU4X3DO5fnNLBwVDFdbhHJZbvb+Qj0NfOYag
KI+Sula22J70hxvEvlx35Yk5yOp3UkS/f1gPI7ZPCtkkgFLrbGXIMEKQR9+z
94IYUdyzI55ciWawcPRg1YOy2Mlx8scDp0SBgFRerCzM3/VxoW+NqZTGQKBgBxp
GoZ3g/dSRx47yVbzDEHuj05yv6iqZNg8bOHLV0BwbMTBN6EAqUM97hk9wNUX/Wn
E5fgM/jJA7Ek3k1Ap6pN2/LW5fdLld3Jr40HV/eYguUa4h0PWSbYhrloxGJZbiWG
Ev/IP4uLSiZezMeqm7ZnDvg/OIPUq2IADgG+/jBAoGAZw+vJSEpyvBwnOsj83r8
          
```

Diffie Hellman parameters

3) OpenVPN Client Config Demo

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

GRE

OpenVPN Client

PP TP/L2TP Client

IPSec

Administration

Debugging

Logout

OpenVPN Client

Client 1
Client 2
Router

Basic
Advanced
Keys
Status

Start with WAN

Interface Type TUN ▼

Protocol UDP ▼

Server Address/Port 211.165.59.162 1194

Firewall Automatic ▼

Authorization Mode TLS ▼

Username/Password Authentication

HMAC authorization Disabled ▼

Create NAT on tunnel

Start Now

Save Cancel

- Status
- Basic Network
- WLAN
- Advanced Network
- Firewall
- VPN Tunnel
- GRE
- OpenVPN Client
- PPTP/L2TP Client
- IPSec
- Administration
- Debugging
- Logout

OpenVPN Client Router

Client 1 **Client 2**

Basic **Advanced** Keys Status

Poll Interval (in minutes, 0 to disable)

Redirect Internet traffic

Accept DNS configuration

Encryption cipher

Compression

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

Connection retry (in seconds; -1 for infinite)

Verify server certificate (tls-remote)

Custom Configuration

- Status
- Basic Network
- WLAN
- Advanced Network
- Firewall
- VPN Tunnel
- GRE
- OpenVPN Client
- PPTP/L2TP Client
- IPSec
- Administration
- Debugging
- Logout

OpenVPN Client Router

Client 1 **Client 2**

Basic Advanced **Keys** Status

For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

```
4qR3qQbZaYCPbG45BwskMrah/d12obRQ31X+3GCstzCmybdJhbR8tWoebdnXw+Jt
Ycvq1hixqw+8Ejy73Eeqip42E5SL7Q1kEV9K1U28oZYcO59b155KPqtAoGBAKwr
RmzplwF2jvy1isgV6W1A4vKI67sTRvOL9LXgl/vYY7ChkpaIZ8d0ZSMBH976
qc5R+3AqKB6W/+oanFp7mMHF5gkGPe01Vy34Ncu+B1F89arWBMIZ5BwignWAKDf
e1wAEHzWxfnb9z25JRZ7AHnCAzc4o4F4jYrcpHAoGAA15IOjfrdNakvTs8o1dZ
EQKAKWrb3QbhJIWajOjSho65EQFXUv9GCVkr5g39mY1tr+HZNacez9tnKfiuHaG
HhnX3fNeBREQRue8P+vQC9Udc9Bucrwq5gURZbO0oAVgE4FhVpJgcq2I7VjrZvR
uHpg1CBODY4q5L/I17Rxi=
-----END PRIVATE KEY-----
```

Client Certificate

```
CSqGSIb3DQEBJARYQdGvZdeB8eGfTcGxILmNvbYUjA0Ent3L9fYUdmM8MGA1UdIQQM
MAoGCCsGAQUFBwMCAsGA1UdDwQEAwIHgDASBgnVHREECzAJgdjbbGlnbQxMA0G
CSqGSIb3DQEBCCUAA4IBAQB9s8T8yPS6d2uwlVlymsCEEL8t5eJSuG0dvJR2ORn
ZK6T9taJVaW/Cohkx5yNlyX7Da12oyggrpxU T5FzE3LynbcCsc37ovWyhcdre
KCbJWkYFgDpzVrhob6up+R3L8TIBSCThwKt53/q+uAaWatVynqzPsYCr3J/3
hQ8oN2gdcd2Uhgwk+oO6lp23blNRwINgLYUQ0K7m9FqYlXdTuDIV72gnpdW8nX
4umRHpGWTJM2fnVEMNs45rD6ELQBbLDYDmWGAQ0/fm62B+qI9VmgusKremgDRZI
8NgdyvOv0n7WRtnWj/ZhIRF8mWhUsaIn3ai+szlX/
-----END CERTIFICATE-----
```

Client Key

```
QKIWarPuRcMjQvILzba92+69cx3rq1PMpYpHtzuxuW0X4Xh3e7r37b7ppvGTMq
bH9pFqrAbvqzoxL+Yh/9WgwwRNUdye9B96skoshDO3z86nUNVO+peNNruuySwHTk
WluJfct+L+JDEF3TEKfTbj5qNK7B9Q0C69SLfioM7mPNGMhejA4ko1BZTUJ/Pu
yJyWpCouTPYcGvxYQIOP14C7GxybQwj66cHYOBmCV1MCAwEAAsOB+TCB9jAdBgNV
HQ4EFgQUh18dzrp+ZC7m08L/uQFORWqOjwgwCYGA1UdIwSBvjCBu4AUh18dzrp
+ZC7m08L/uQFORWqOjhgZekgZQwgZEXcZAJBgNVBAYTAkNOMQswCQYDVQIExJH
RDELMAkGA1UEBMCU1oxdTALBgNVBAoTBFRFRU1QxYDFASBgnVHREECzAJgdjbbGlnbQx
ZXN0MRAwDgYDVRQQDEwURVNUJENBMRAwDgYDVRQQDEwFYN5UINBMR8wHQYJKoZI
hvcNAQkBFh0ZXN0QGV4YW1wbGUuY292tgkA4Se3cv19gOYwDAYDR0TBAUwAwEB
```

- Status
- Basic Network
- WLAN
- Advanced Network
- Firewall
- VPN Tunnel
- GRE
- OpenVPN Client**
- OpenVPN Server
- VPN Client
- IPSec
- Administration
- Debugging
- Logout

OpenVPN Client

Router

Client 1 Client 2

Basic Advanced Keys **Status**

Data current as of Sat Jan 1 09:06:05 2000.

General Statistics

Name	Value
TUN/TAP read bytes	0
TUN/TAP write bytes	0
TCP/UDP read bytes	0
TCP/UDP write bytes	70
Auth read bytes	0
pre-compress bytes	0
post-compress bytes	0
pre-decompress bytes	0
post-decompress bytes	0

Stop Now

[Refresh Status](#)

Save Cancel