SheRink Industrial Router

Contents

1. Product Introduction..... 3

1.1 Product overview..... 3

1.2 Model introduction..... 3

1.3 Product Appearance..... 4

1.4 Typical Application Diagram..... 4

1.5 Features..... 5

2. Hardware Installation..... 6

2.1 Panel..... 6

2.2 LED Status..... 7

2.3 Dimension..... 7

2.4 How to Install..... 8

3. Router Configuration.....9

3.1 Local Configure.....9

3.2 Basic Configuration..... 10

3.3 Advanced Network Setting.....16

3.4 Firewall..... 25

3.5 VPN Tunnel.....26

3.6 Administration.....35

3.7 Debugging Setting..... 43

3.8 “RST” Button for Restore Factory Setting..... 44

3.9 Appendix.....45

1 Product Introduction

1.1 Product overview

SheRink 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..

SheRink 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, SheRink 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

SheRink 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.

Model	4G	3G	Interface	WiFi	4G
R1L1H	FDD 2600/2100/1900/1800/900/800MHz	HSPA+/HSPA/HSDPA 850/900/1900/2100MHz	1xLAN 1xRS-232	No	Yes
R1L1	FDD 2600/2100/1800/900/800MHz	HSPA+/HSPA/HSDPA 800/850/900/1900/2100MHz	1xLAN 1xRS-232	No	Yes
R1L1F	FDD:1800/2100/2600MHz TDD:1900/2300/2600MHz	HSPA+/HSPA/HSDPA 2100/1900/850/900MHz	1xLAN 1xRS-232	No	Yes
R1L1H2	FDD:700/850/1700/1900MHz	DC-HSPA+/HSPA/HSDPA 2100/1900/850/900MHz	1xLAN 1xRS-232	No	Yes
R1L1-H	-	HSPA+ 2100/1900/850MHz	1xLAN 1xRS-232	No	No
R1L1-H2	-	HSPA+ 2100/1900/900/850MHz	1xLAN 1xRS-232	No	No
R1L1-H232	-	HSPA+ 900/2100MHz or 850/1900MHz	1xLAN 1xRS-232	No	No
R1L1-H485	-	HSPA+ 900/2100MHz or 850/1900MHz	1xLAN 1xRS-485	No	No
R1L1E	-	EVDO 800MHz	1xLAN 1xRS-232	No	No

1.3 Product Appearance

Table 1-1 SheRink Router Appearance

Series	R1	R2	R20	R52
Appearance				
Ports	1xLAN 1xRS-232/RS485	2xLAN/1xLAN+ 1xWAN GPS or WLAN	2xLAN(deafult) + dual SIM GPS, WLAN	1xWAN, 4xLAN + single module / dual SIM or dual module / dual SIM
Product category	Single port router	Dual-port WiFi router	Multi-port WiFi router	Multi- functional WiFi router

1.4 Typical Application Diagram

SheRink 4G/3G Router widely used in Telecom, economic, advertisement, traffic, environment protection business area. For example, in economic area, R100 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.

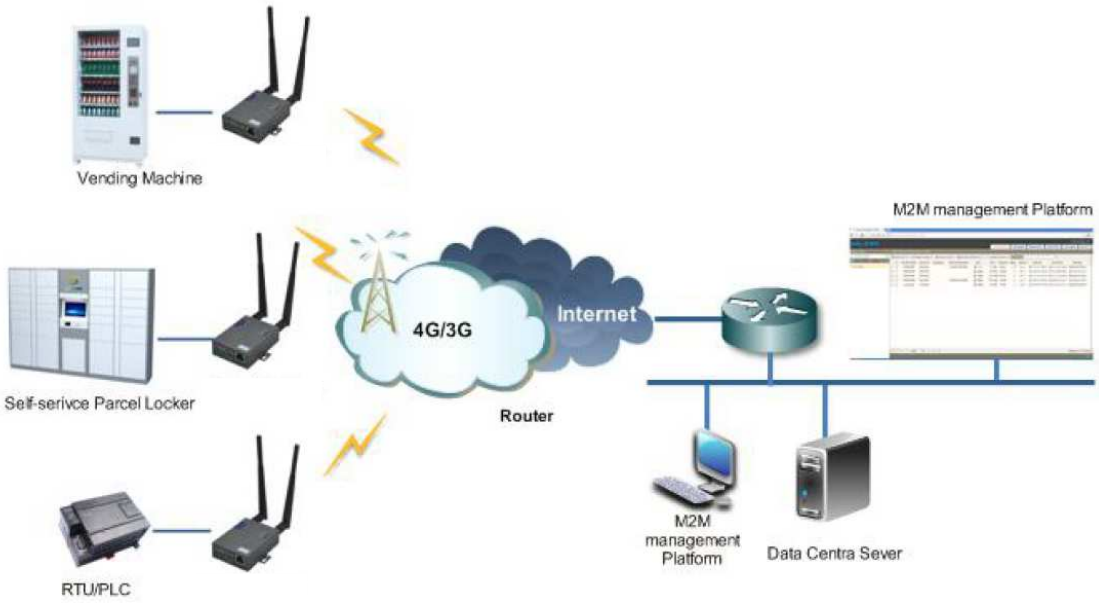


Figure 1-1 Network Topology

SheRink 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 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, advanced VPN function

- Provide friendly user interface, use normal web internet explorer to easily configure and manage, long-distance configure Telnet/SSH.

- Optional IPv6 protocol stack

- Optional support M2M terminal management platform

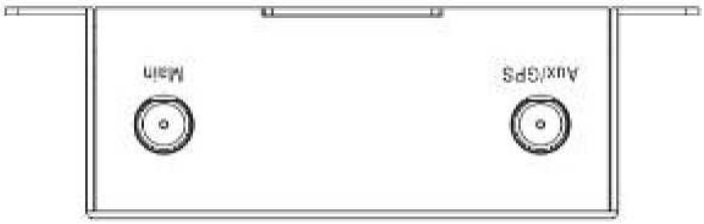
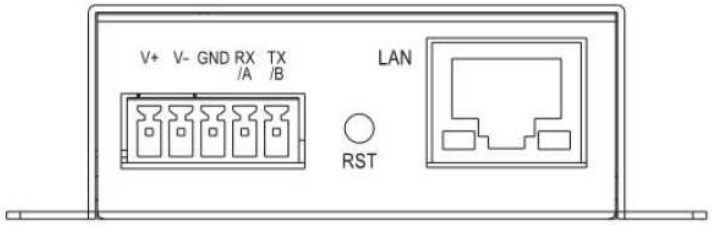
- WDT watchdog design, keep system stable

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 R1 –Structure

	R1 series
Front	
Rear	

There are some different for Antenna interface and indicator light for the expanded GPS series.

Table 2-1 Router Interface

Port	Instruction
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection
Main	4G/3G antenna, SMA connector, 50Ω

Port	Instruction
Aux/GPS	4G Aux Antenna or GPS Antenna, SMA connector, 50Ω
LAN	10/100Base-TX，MDI/MDIX self-adaption,
RST	Reset button,(press on button 5 seconds)
PWR	Power connector
COM	Three pins serial port, suitable for collection device with RS-232 or RS-485 interface, for wireless data transmission.

2.2 LED Status

silk-screen	color	status	Indication
NET	Green		Strong Signal
	Orange		Normal Signal
	Red		Weak Signal
		Solid light	Connected 4G successfully
		Blinking quickly(0.5s)	Dialing
LAN	Green	Solid light	Connected
	Green	Blinking	Data Sending
	Green	Dark	Not connected
PWR	Green	Solid light	Router OS is running.

Table 2-2 Router LED indictor Status

2.3 Dimension

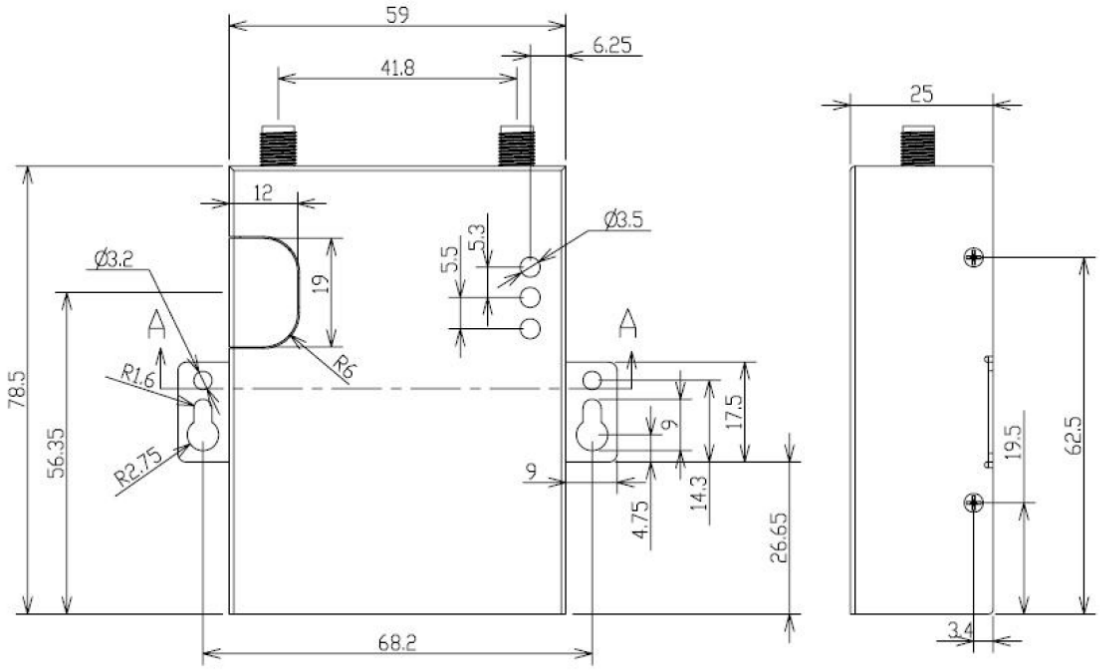


Figure 2-2 R1 Series Router Dimension Figure

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, this cable is optional. One end connect to computer serial port, the other end connects the RX/TX and GND of the router

! ! ! Before connecting, please disconnect any power resource of router

2.4.4 Power Supply

In order to get high reliability, SheRink Series Router adapt supports wide voltage input range: +7.5V～+32VDC, 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

3. Router Configuration

This Chapter introduces the parameter configuration of the router, the router can be configured via IE, Firefox, or Chrome.

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

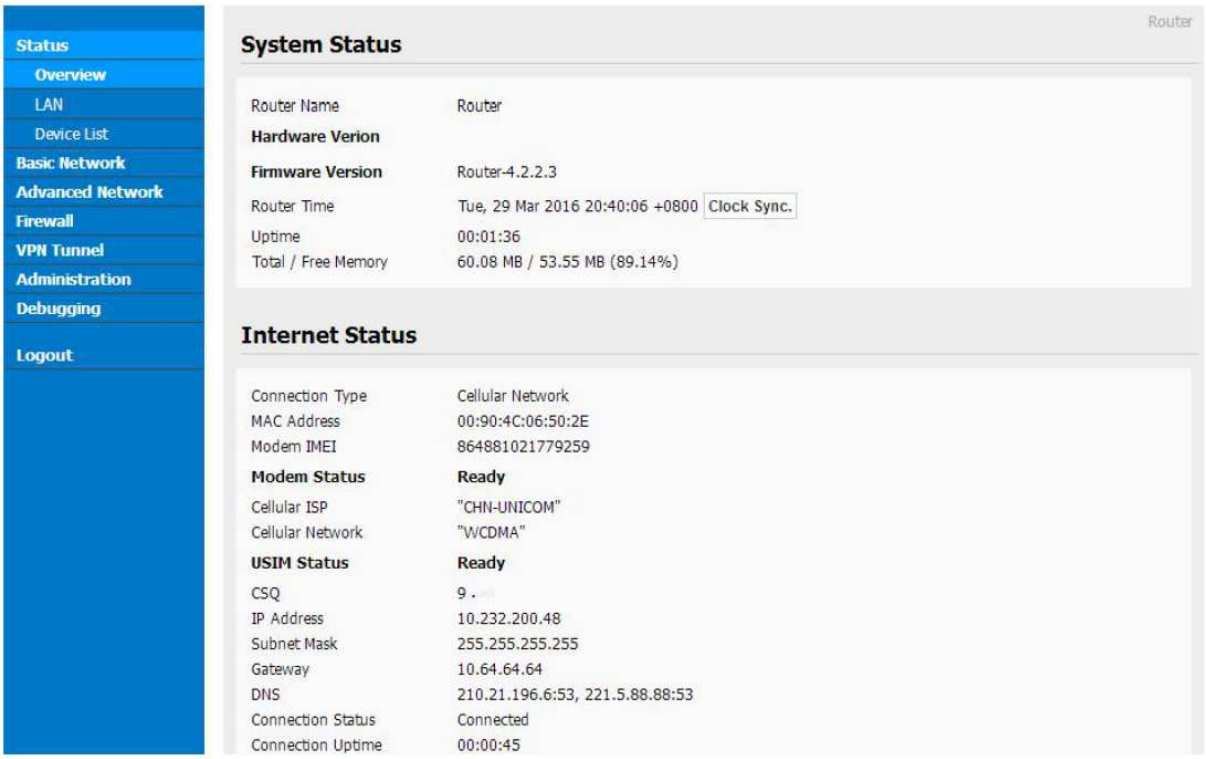
Step 2 Obtain a IP address automatically or set up IP address,192.168.1.xxx(XXX can be any number between 2～254)

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

Figure 3-4 User Identify Interface

3.2 Basic Configuration

Different software version has different web configuration interface, below take WL-R100 as example. After access 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.



3.2.1 Cellular Network Configure

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

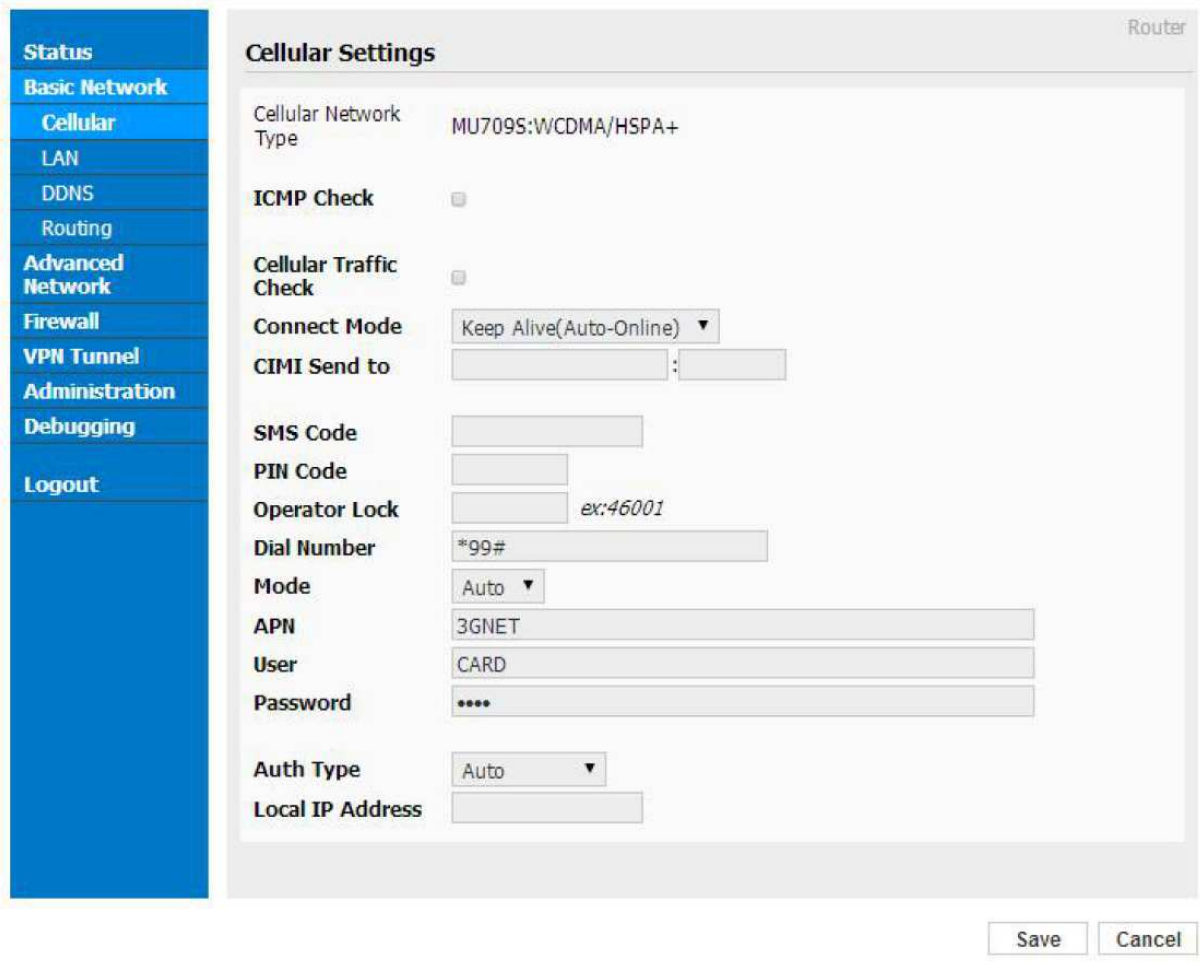


Figure 3-1 Cellular Settings GUI

Table 3-1 Cellular Setting Parameter Instruction

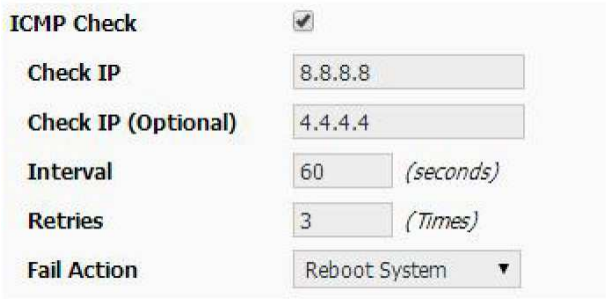
Parameter	Instruction
ICMP check	To enable or disable ICMP check rules. Enable the ICMP check and setup a reachable IP address as destination IP. Once ICMP check failed, router will reconnect/reboot system as optional..
Cellular Traffic Check	There is Rx/Tx as options. Once no Rx/Tx data, router will router will reconnect/reboot system as options.
Connect Mode	● Keep alive (Auto-online).The router will automatically connect 3G/4G network and keep online. ● Connect On Demand. Idle offline if no data from LAN to 3G/4G within defined time.

Parameter	Instruction
	● Schedule, Define online and offline time. This function need to enable NTP function, ● Call/SMS Triggered. Call/SMS trigger router online. ● Manually. Connect 3G/4G network by manual.
CIMI Send	Send CIMI to defined IP and port by TCP protocol.
SMS Code	SMS identifying code. Router just identifies the unique code to implement SMS command.
PIN Code	Unlock the SIM PIN code.
Operator Lock	Lock operators via MCC/MNC
Service Code	The default service code as *99#.
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	Defined SIM IP from operator.

ICMP Check

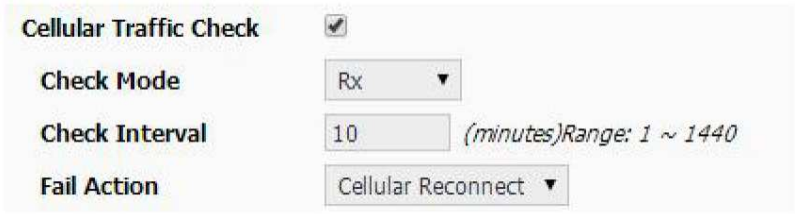
Enable ICMP, Router will automatically check whether the defined IP address is reachable per 60s. If the IP address is unreachable and ICMP check is timeout AT the first time, it will check 2 times every 3 seconds. If the third time is still failed, the router will redial.

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



Cellular Traffic Check

【Check Mode】there are Rx(Receive), Tx(Transmission) and Rx/Tx check modes.【Rx】Router will check the 3G/LTE cellular receiver traffic. If no receiver traffic within the defined check interval, the router will implement the specified action reconnect or reboot.



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

3.2.2 LAN Setting

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

Figure 3-2 LAN Setting GUI

Table 3-2 LAN Setting Instruction

Parameter	Instruction
Router IP Address	Router IP address, default IP is 192.168.1.1
Subnet Mask	Router subnet mask, default mask is 255.255.255.0
DHCP	Dynamic allocation IP service, after enable, it will show the IP address range and options of lease
IP Address Range	IP address range within LAN
Lease	The valid time

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

3.2.3 Dynamic DNS Setting

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

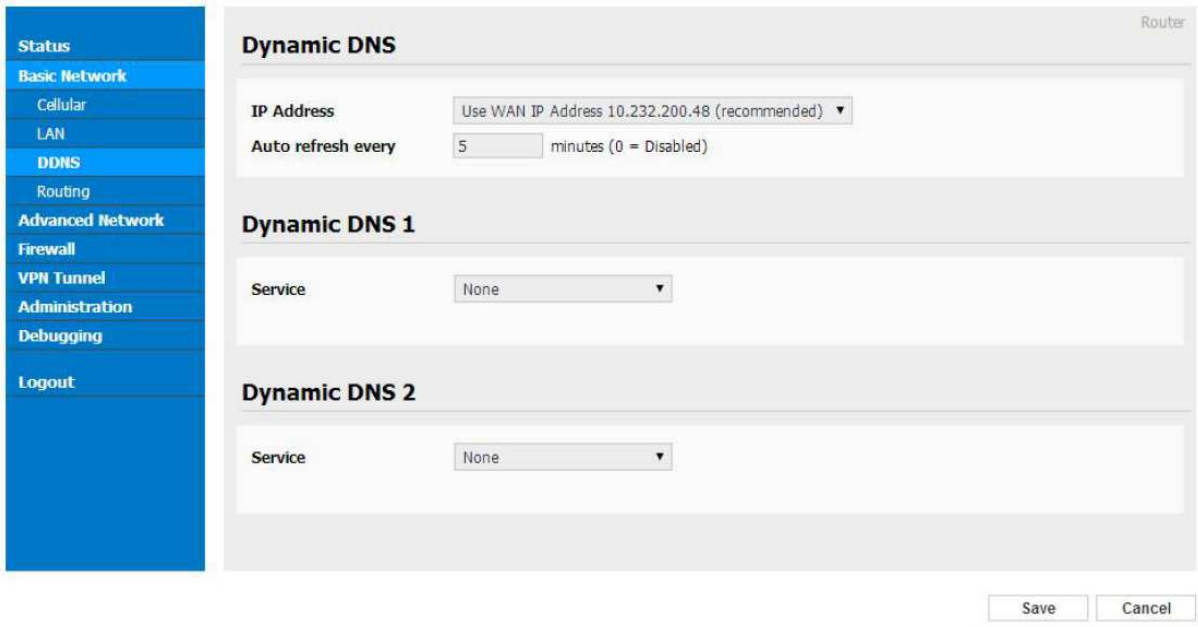


Figure 3-3 Dynamic DNS Setting

Table 3-3 DDNS Setting Instruction

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

Step 2 Please Click “Save“ to finish.

3.2.4 Routing Setting

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

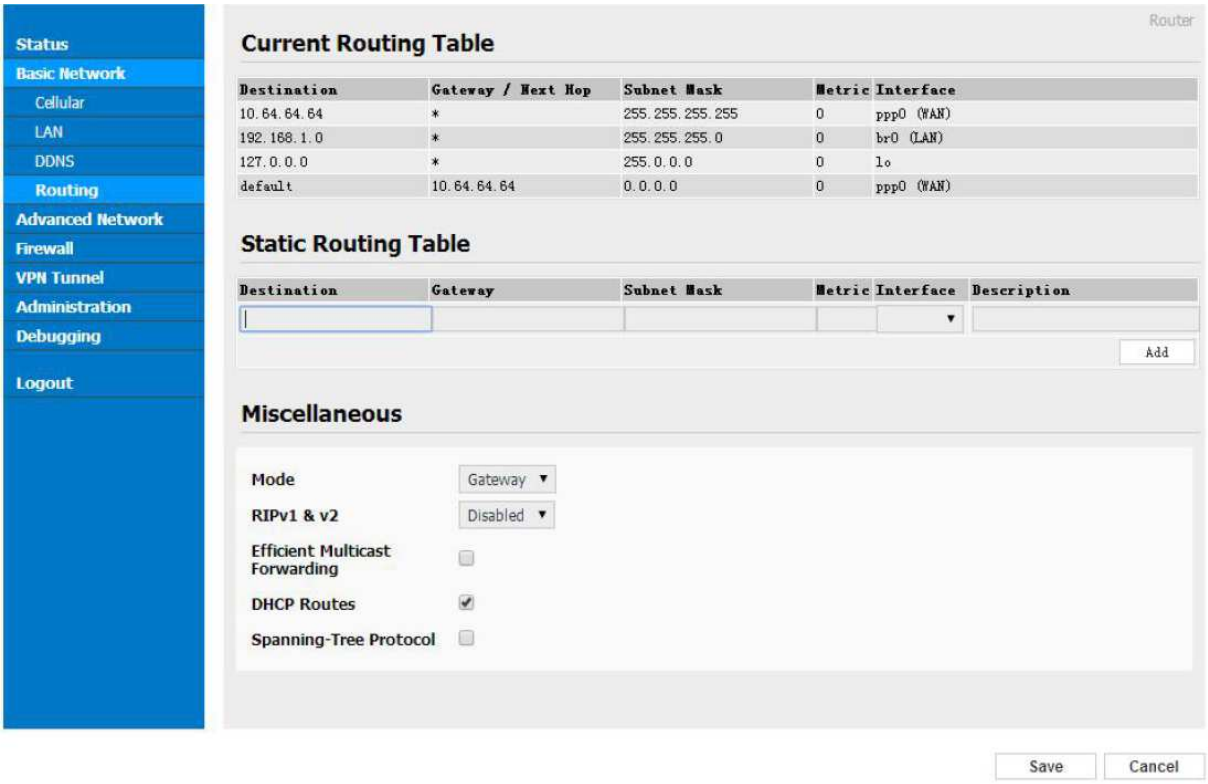


Figure 3-4 Routing Setting

Table 3-4 Routing Setting Instruction

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

3.3.1 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.

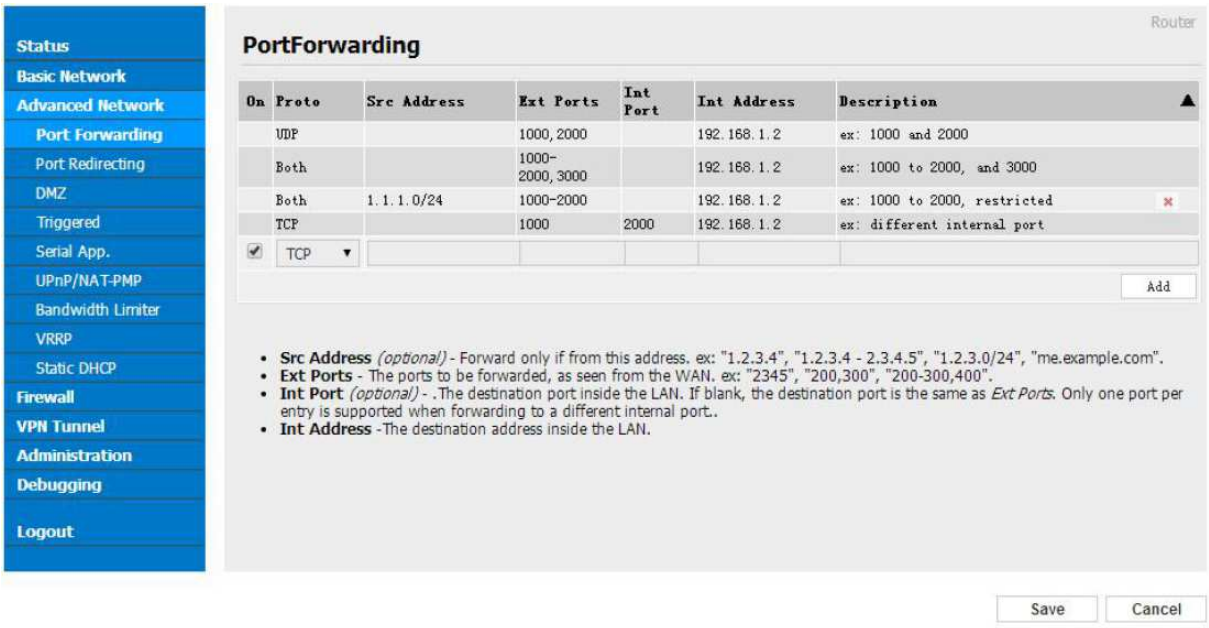


Figure 3-5 Port Forwarding GUI

Table 3-5 "Port Forwarding" Instruction

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

Step 2 Please click ”save” to finish

----End

3.3.2 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 3-6 Port Forwarding GUI

Table 3-6 “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

3.3.3 DMZ Setting

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

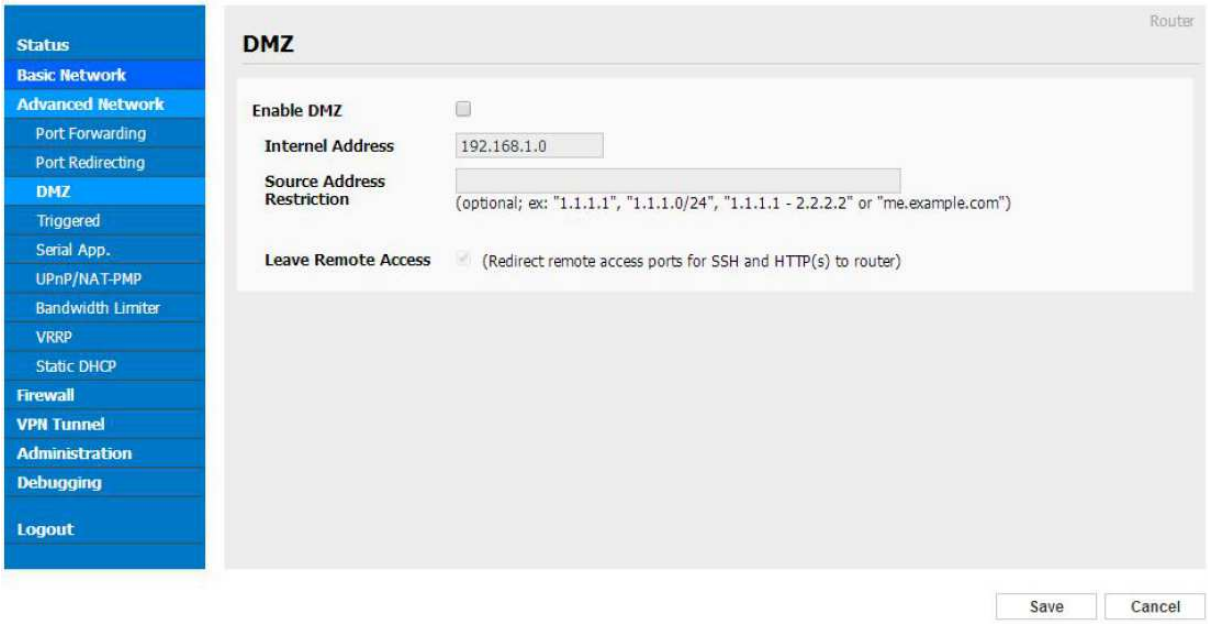


Figure 3-7 Port Redirecting GUI

Table 3-7 “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

3.3.4 IP Passthrough Setting

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

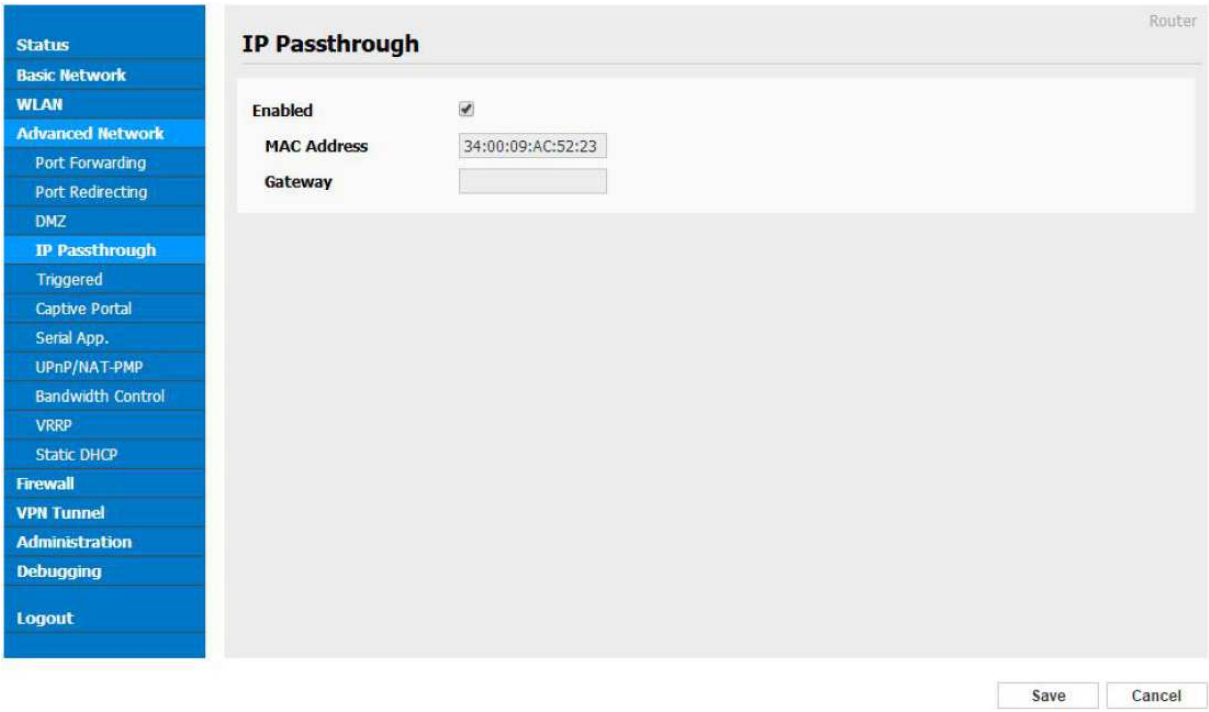


Figure 3-8 IP Passthrough GUI

Table 3-8 “IP Passthrough” Instruction

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

Step 2 Please click ”save” to finish

----End

3.3.5 Triggered Setting

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

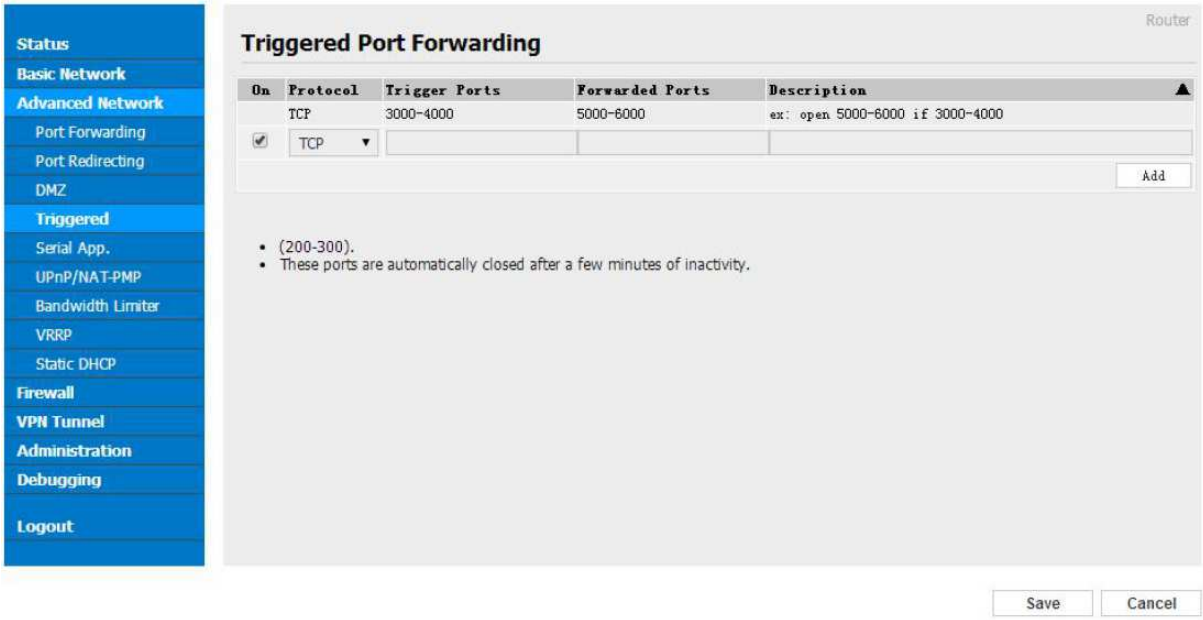


Figure 3-9 Triggered GUI

Table 3-9 “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

3.3.6 Serial App. Setting

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

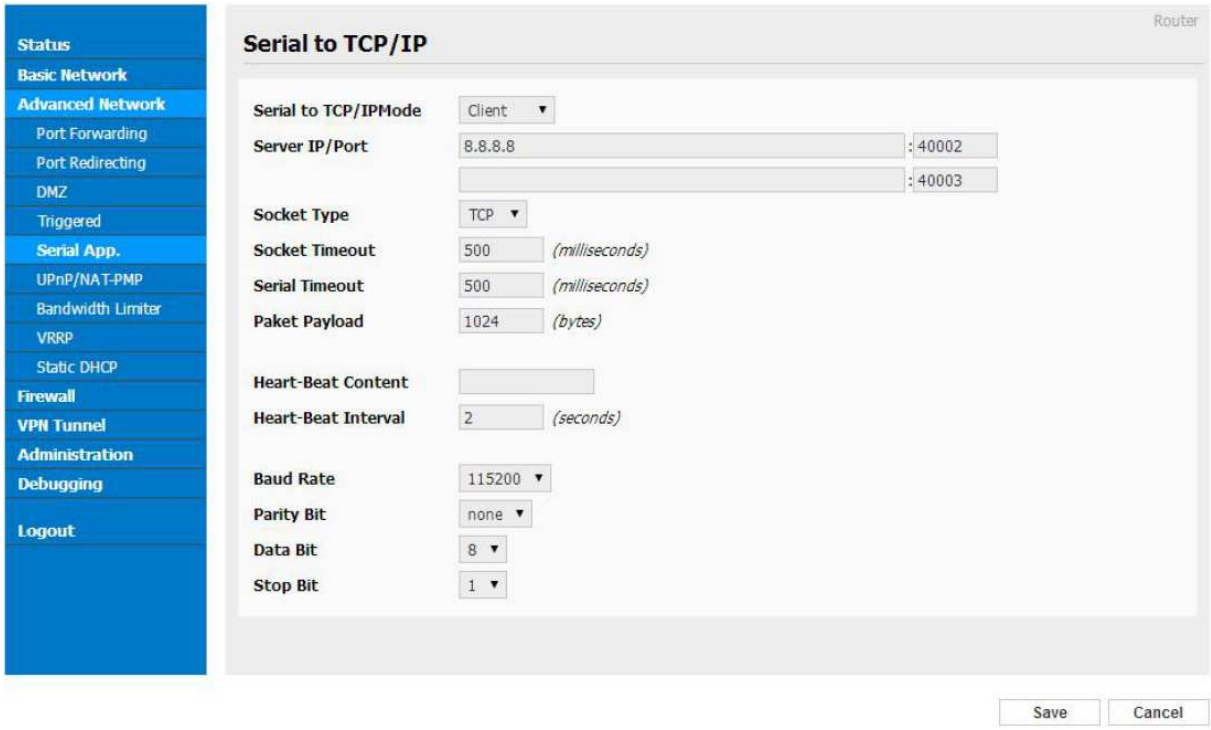


Figure 3-10 Serial App Setting GUI

Table 3-10 “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

Serial port connection

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

Step 2 Please click ”save” to finish.

----End

3.3.7 UPnp/NAT-PMP Setting

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

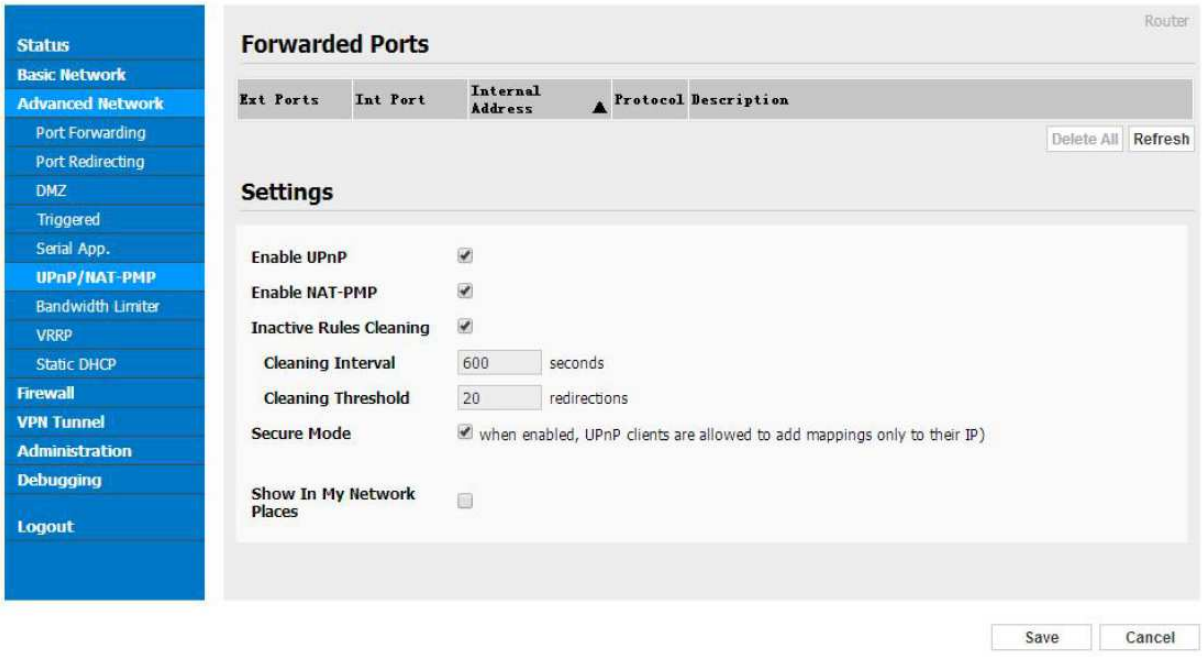


Figure 3-11 UPnp/NAT-PMP Setting GUI

Step 2 Please click ”save” to finish.

---End

3.3.8 Bandwidth Control Setting

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

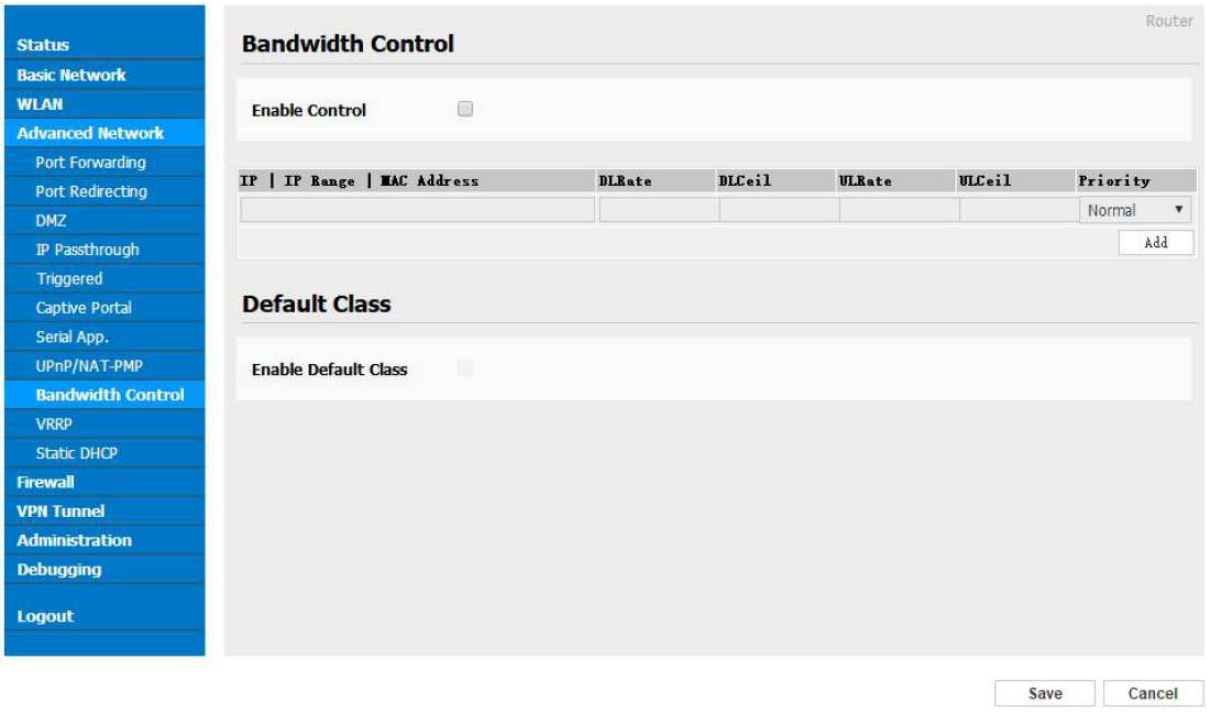
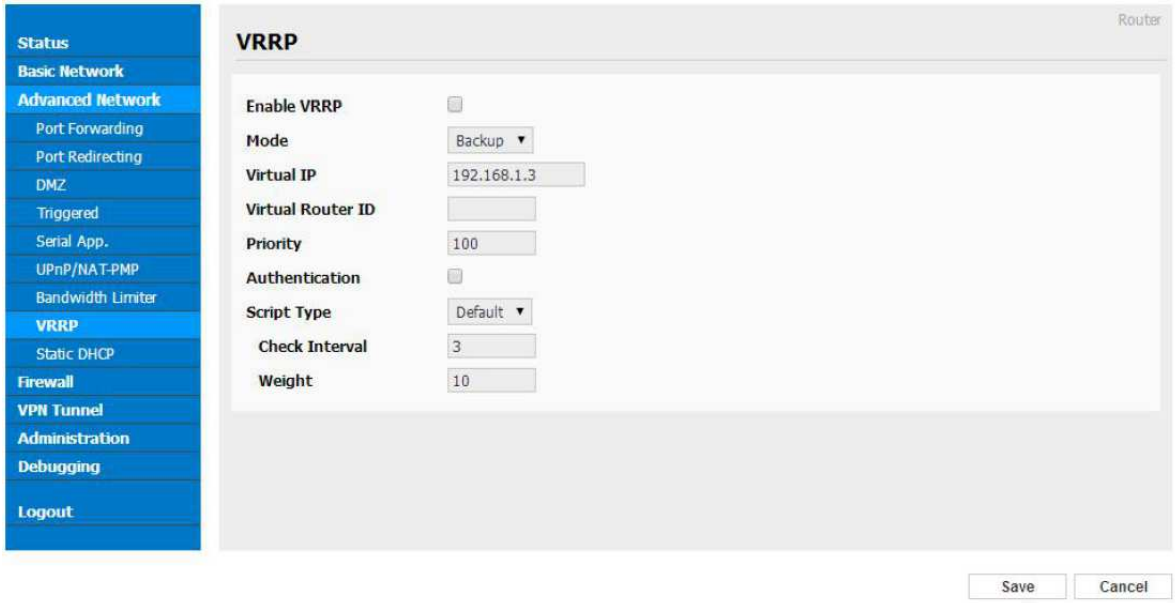


Figure 3-12 Bandwidth Control Setting GUI

Step 2 Please click ”save” to finish.
---End

3.3.9 VRRP Setting

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



Step 2 Please click ”save” to finish.

---End

3.3.10 Static DHCP Setting

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

Figure 3-14 Static DHCP Setting GUI

Step 2 Please click ”save” to finish.

---End

3.4 Firewall

3.4.1 IP/URL Filtering

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

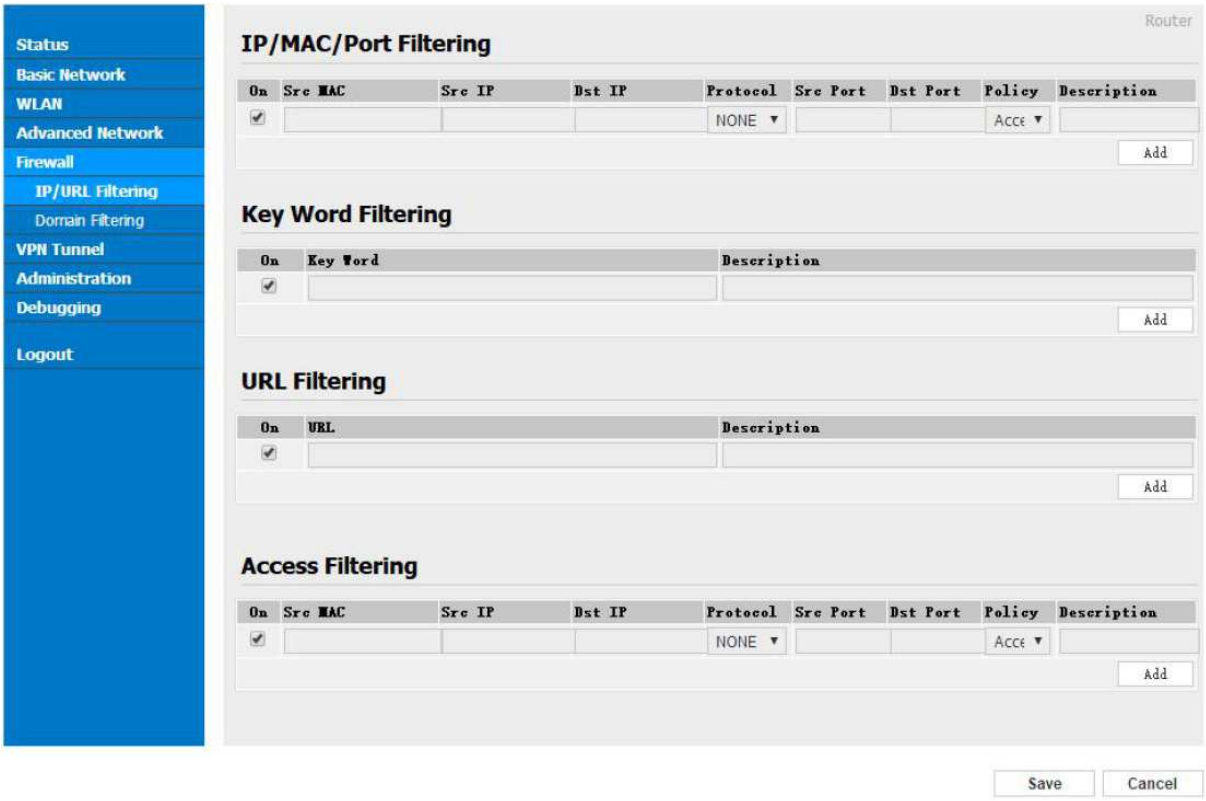


Table 3-11 “IP/URL Filtering” Instruction

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

Step 2 Please click ”save” to finish.

---End

3.4.2 Domain Filtering

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

Figure 3-15 Domain Filtering Setting GUI

Table 3-12 “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

3.5 VPN Tunnel

3.5.1 GRE Setting

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

Table 3-13 “GRE” Instruction

	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 1 Please click ”save” to finish.

----End

3.5.2 OpenVPN Client Setting

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

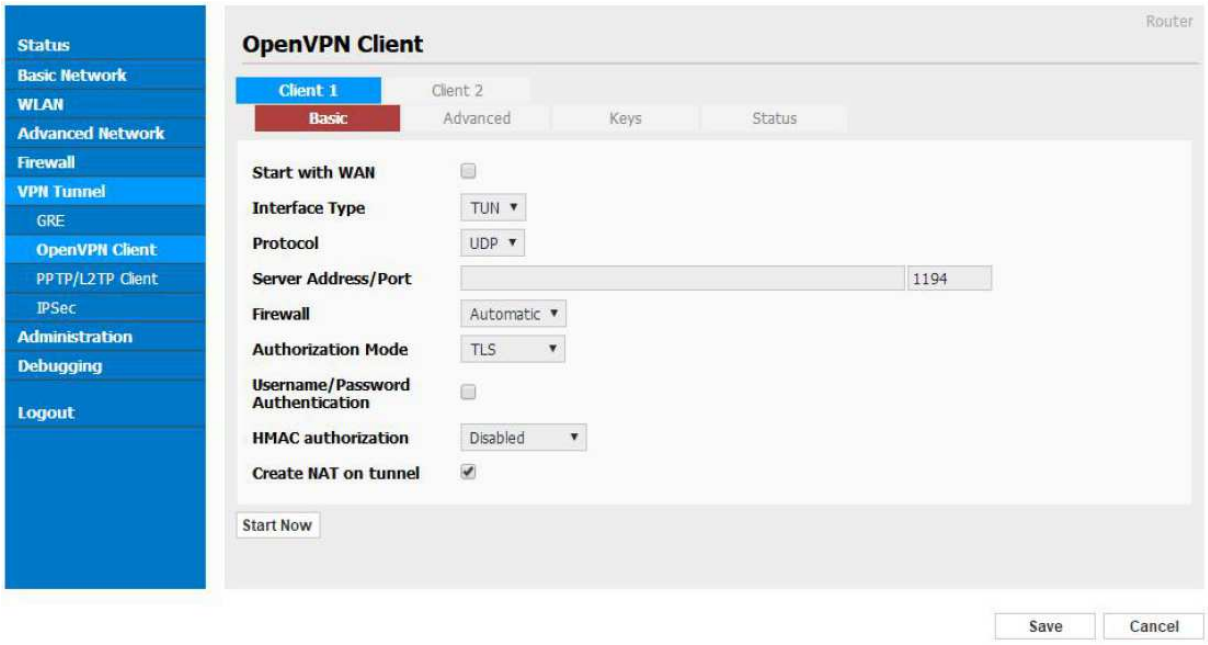
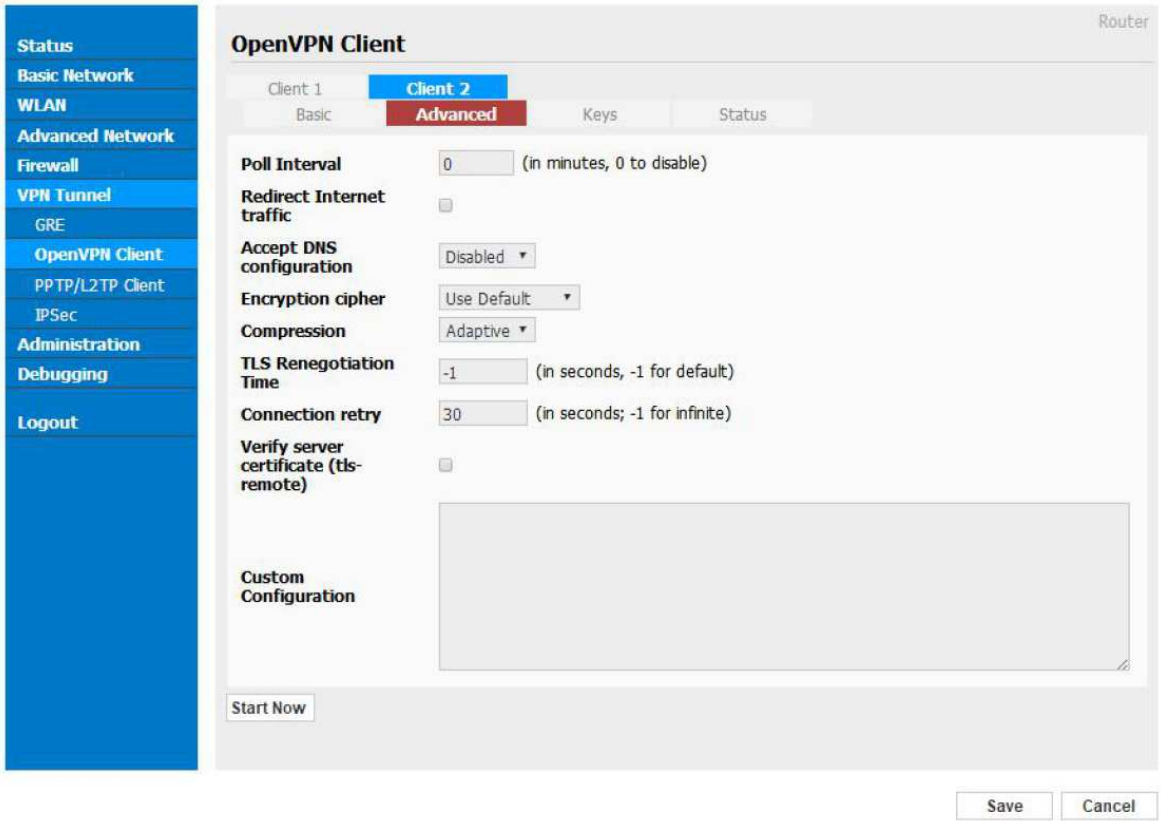


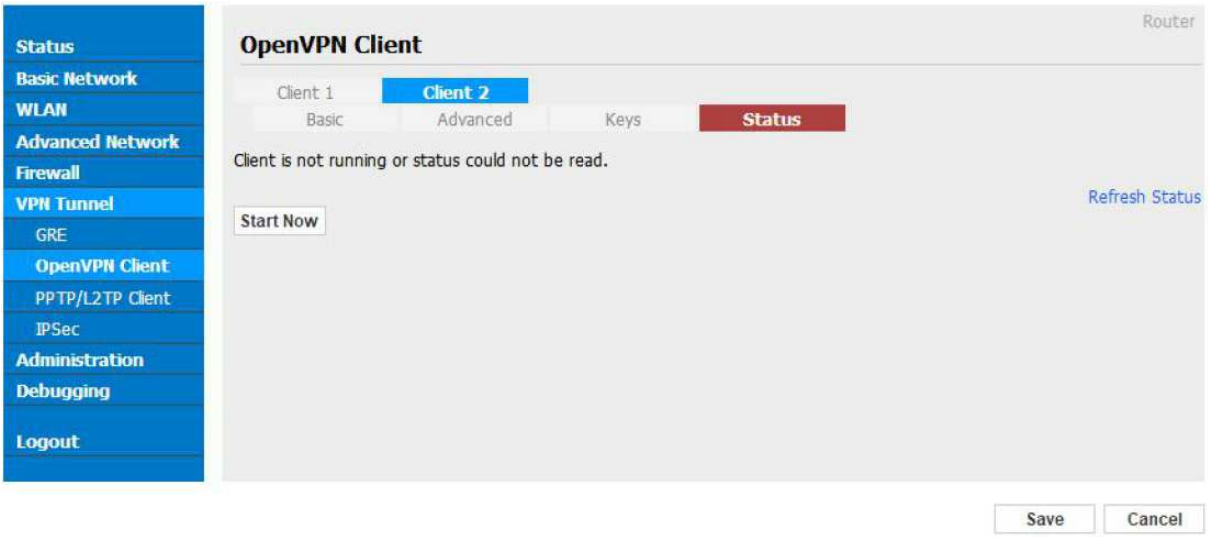
Figure 3-17 OpenVPN Setting GUI

Table 3-14 “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
Certificate Authority	Keep certificate as the same as server
Client Certificate	Keep client certificate as the same as server
Client Key	Keep client key as the same as server



Parameter	Instruction
Status	Check Openvpn status and data statistics.

Step 1 Please click ”save” to finish.

----End

3.5.3 VPN Client Setting

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

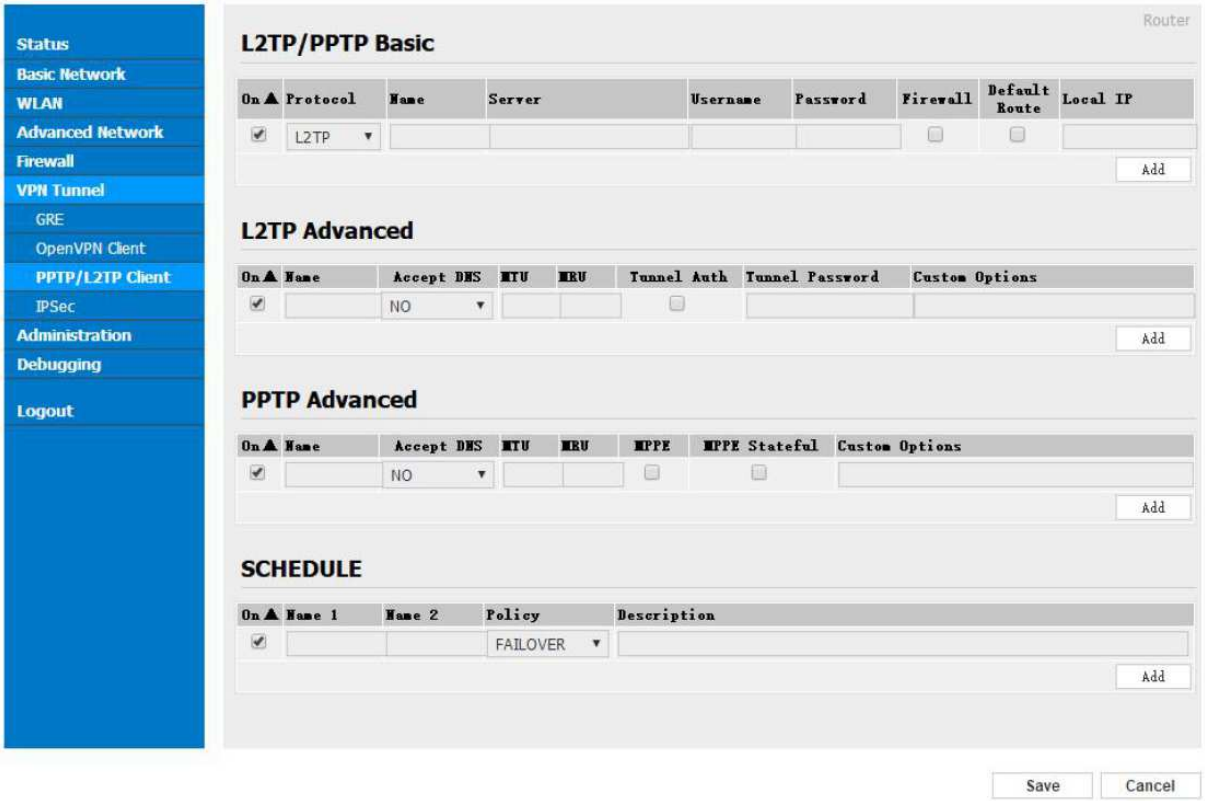


Table 3-15 “PPTP/L2TP Basic” Instruction

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 3-16 “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 3-17 “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

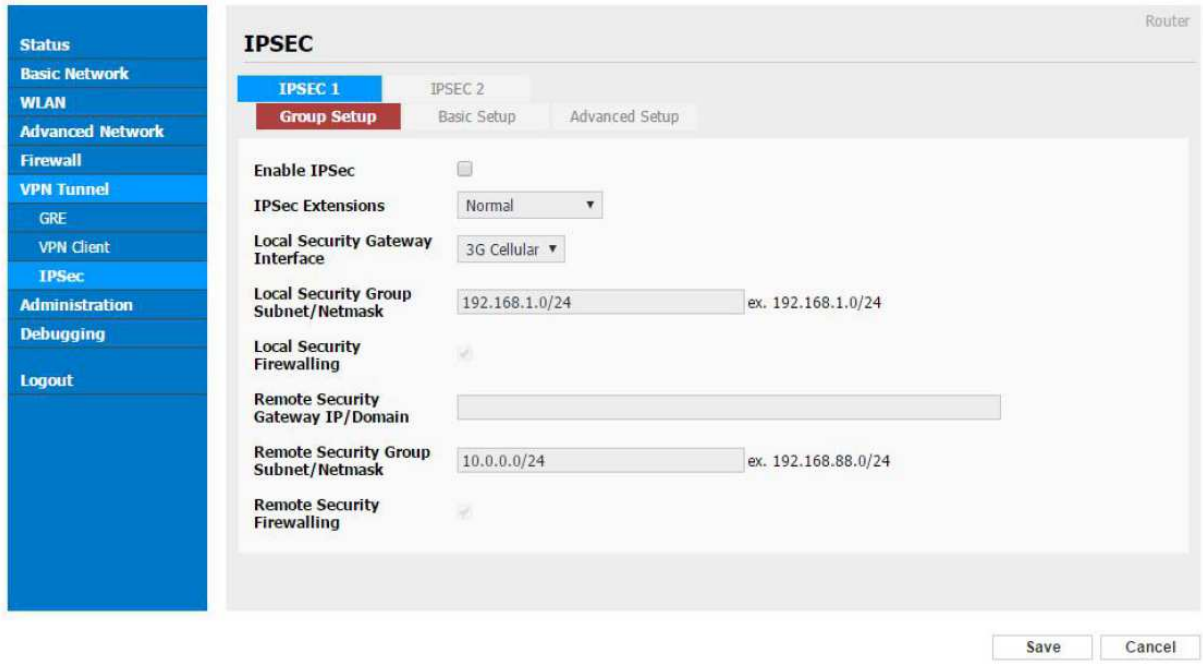
Table 3-18 “SCHEDULE” Instruction

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 1 Please click ”save” to finish.

---End

3.5.4 IPSec Setting



3.5.4.1 IPSec Group Setup

Step 1 Please click “IPSec> Group Setup” to check or modify the relevant parameter.

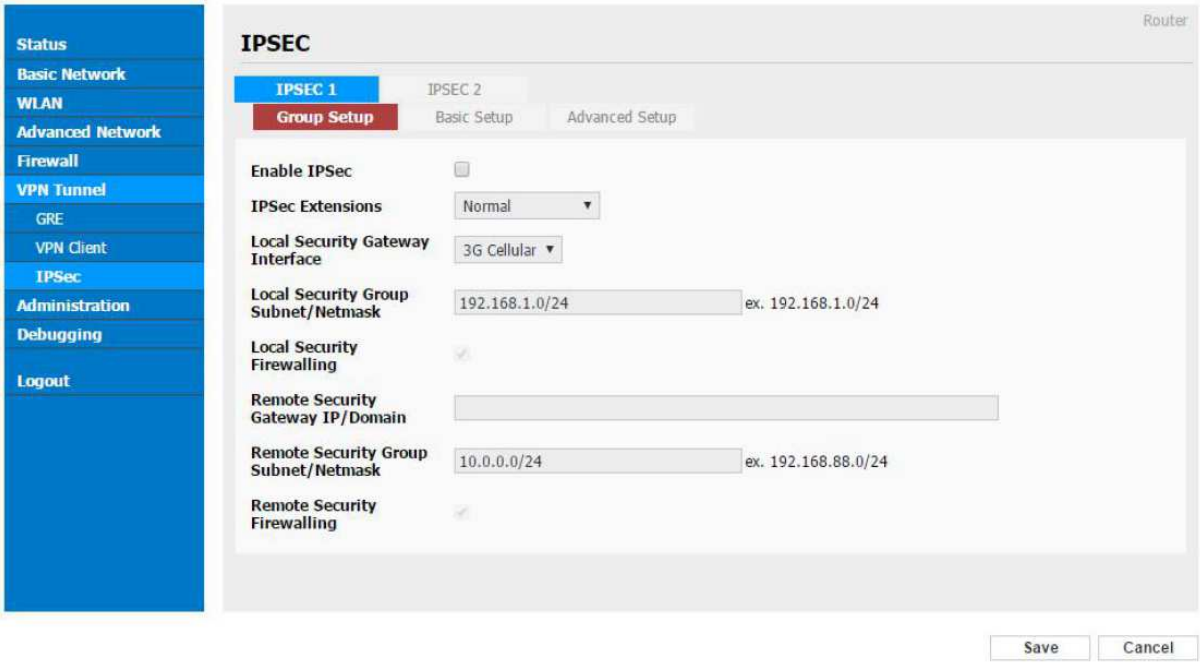


Table 3-1 “ IPSec Group Setup” Instruction

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.

3.5.4.2 IPSec Basic Setup

Step 1 Please click “IPSec >Basic Setup ” to check or modify the relevant parameter.

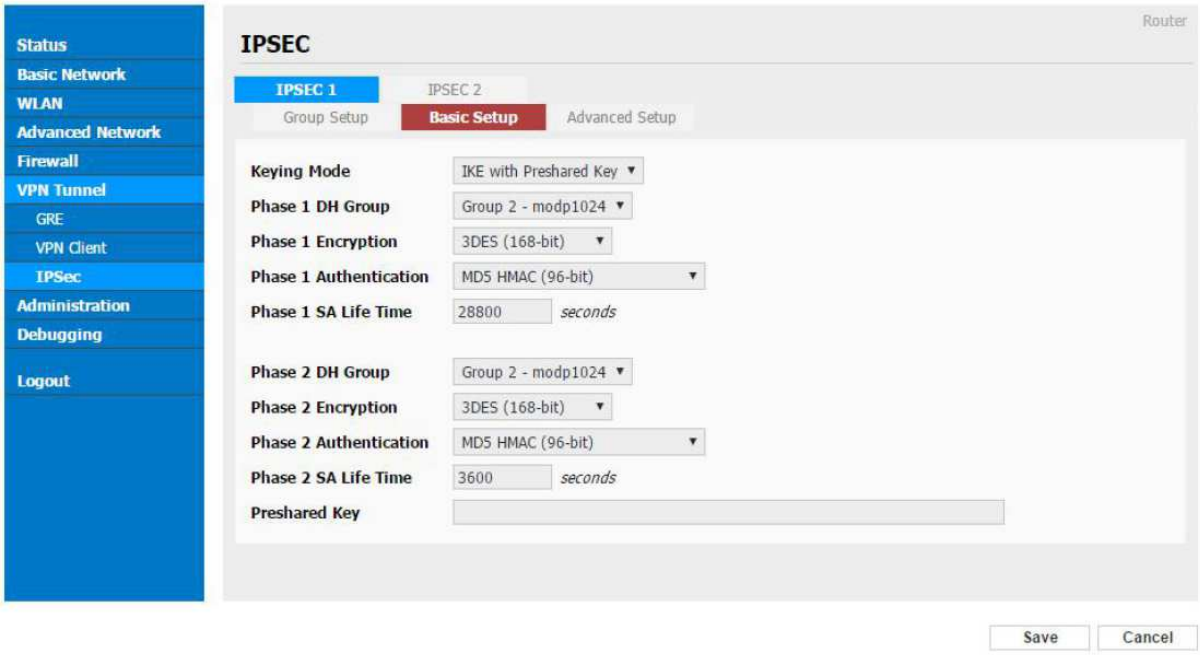


Table 3-2 “ IPSec Basic Setup” Instruction

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.

3.5.4.3 IPSec Advanced Setup

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

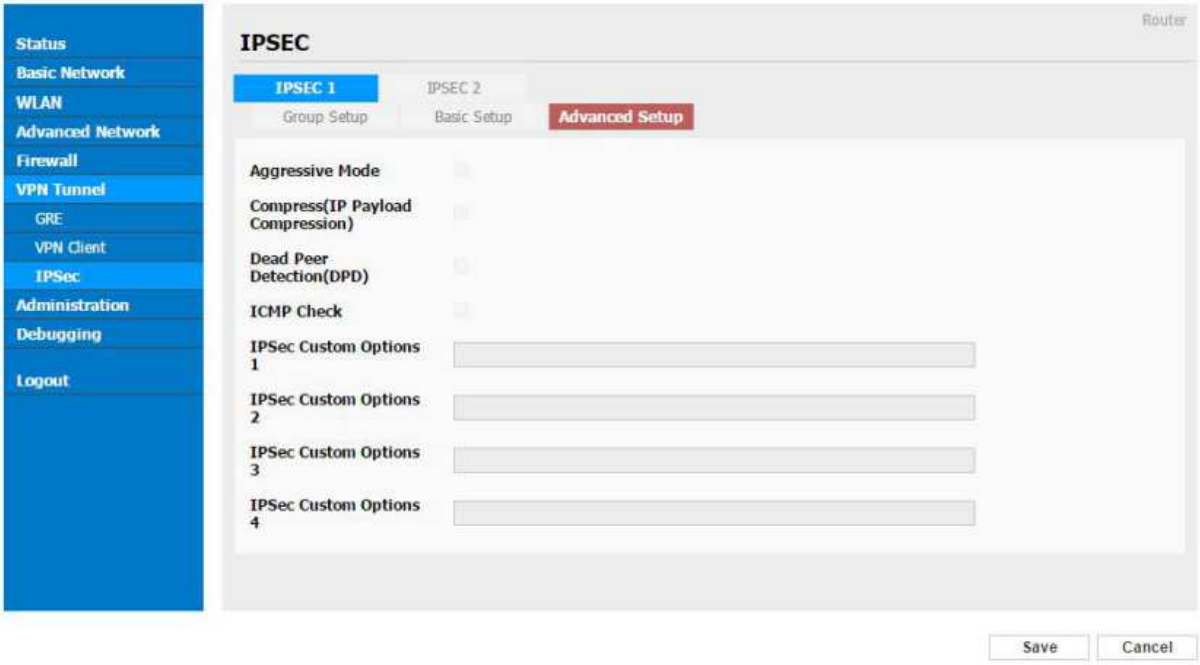


Table 3-3 “ IPSec Advanced Setup” Instruction

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

3.6 Administration

3.6.1 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.

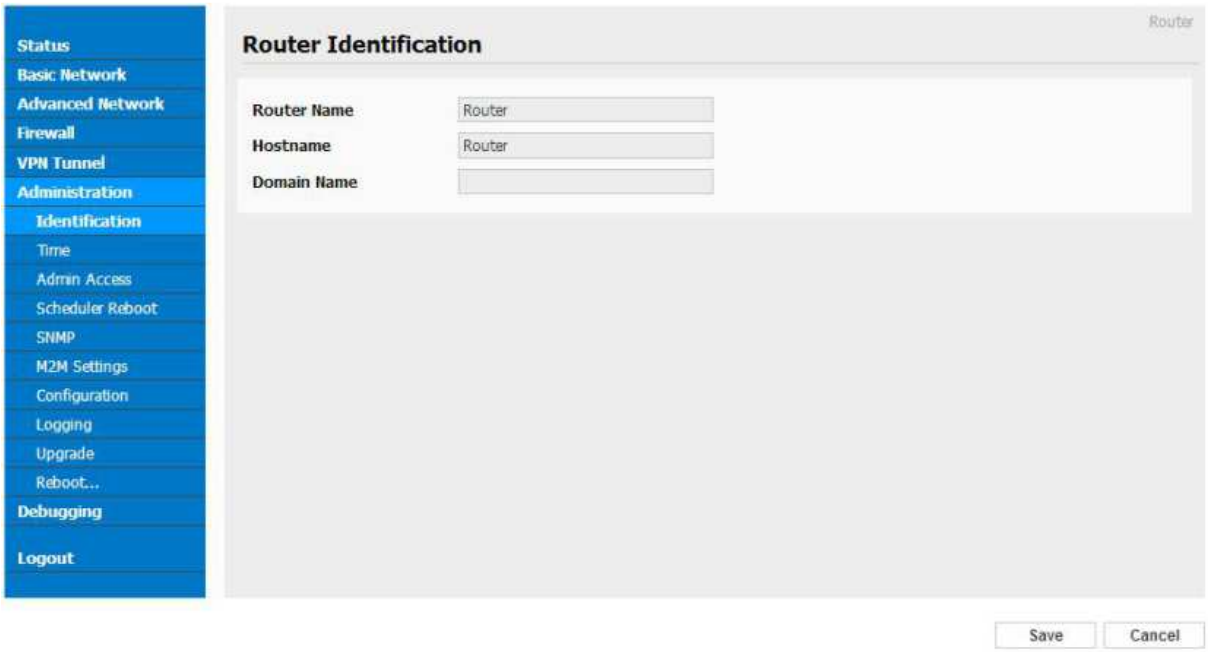


Figure 3-2 Router Identification GUI

Table 3-4 “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

3.6.2 Time Setting

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

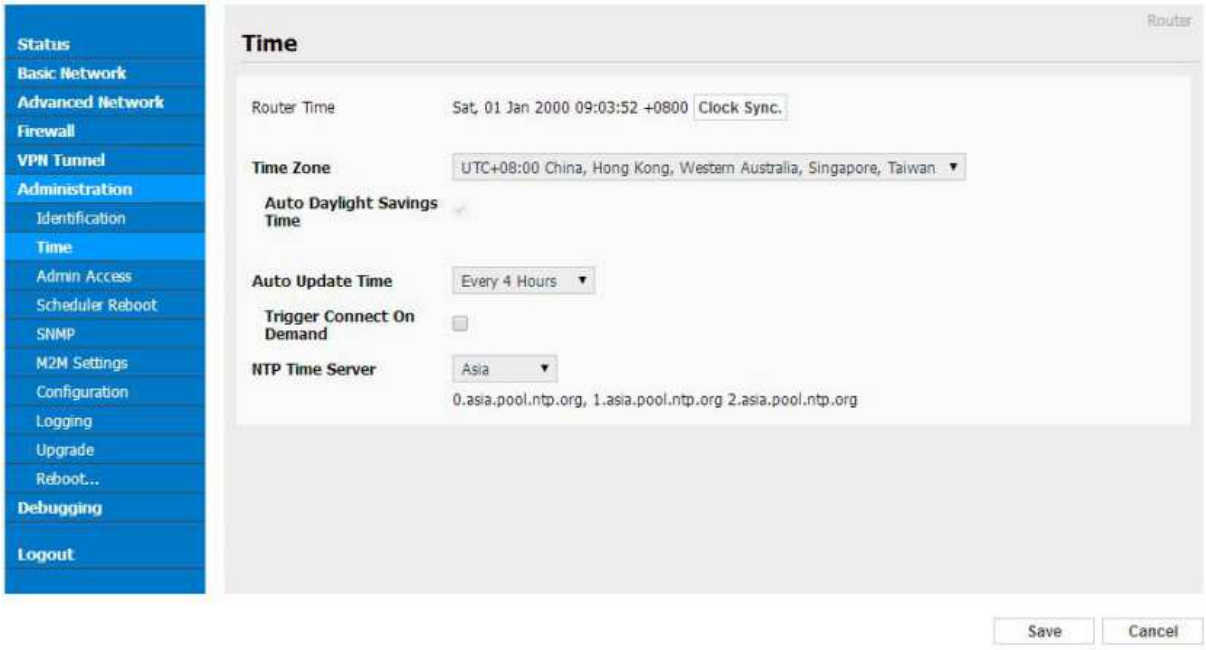


Figure 3-3 System Configuration GUI

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

Step 2 Please click “save to finish.

----End

3.6.3 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.

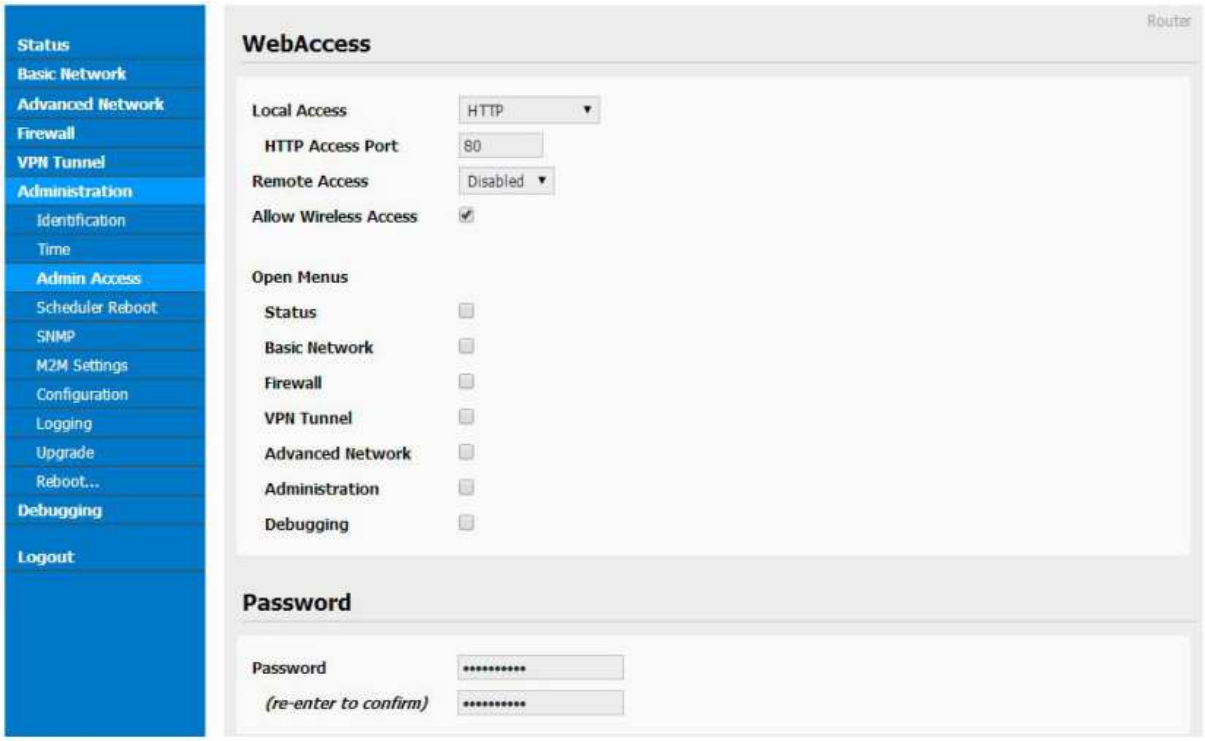


Figure 3-4 Admin Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.6.4 Schedule Reboot Setting

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

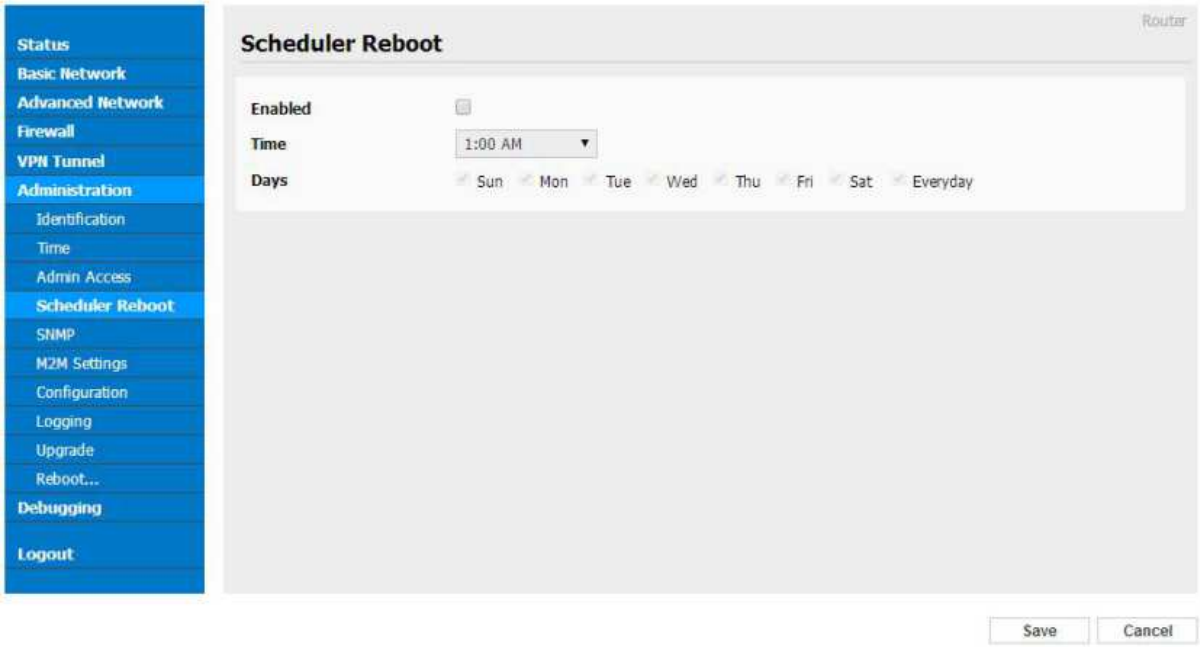


Figure 3-5 Scheduler Reboot Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.6.5 SNMP Setting

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

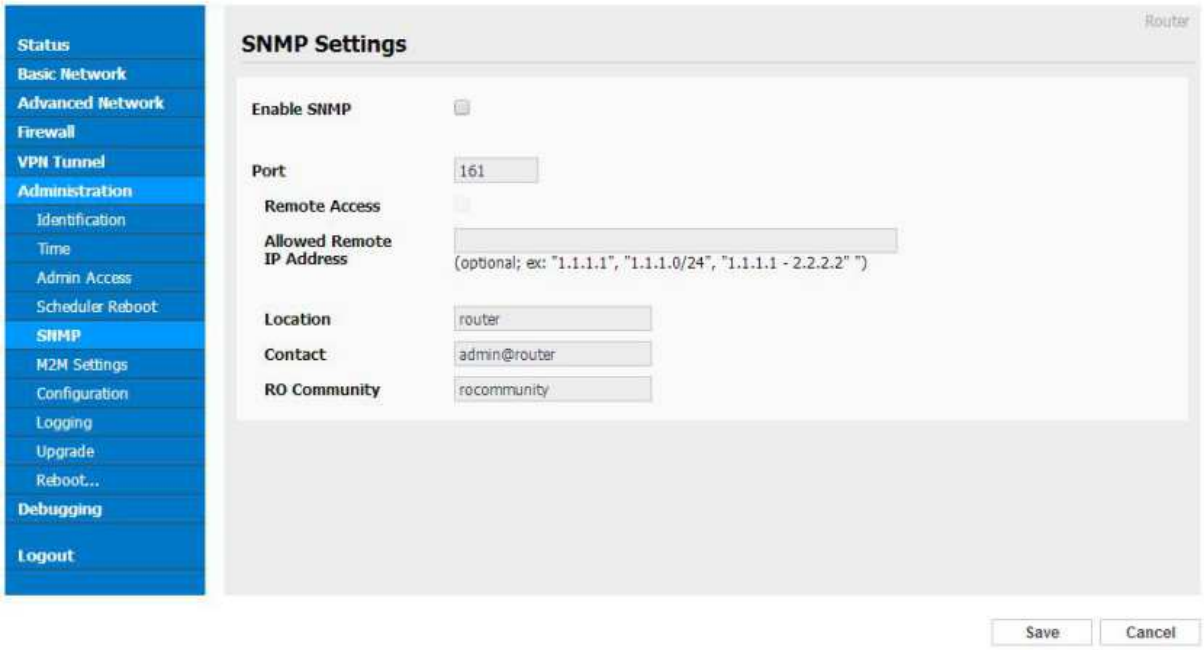


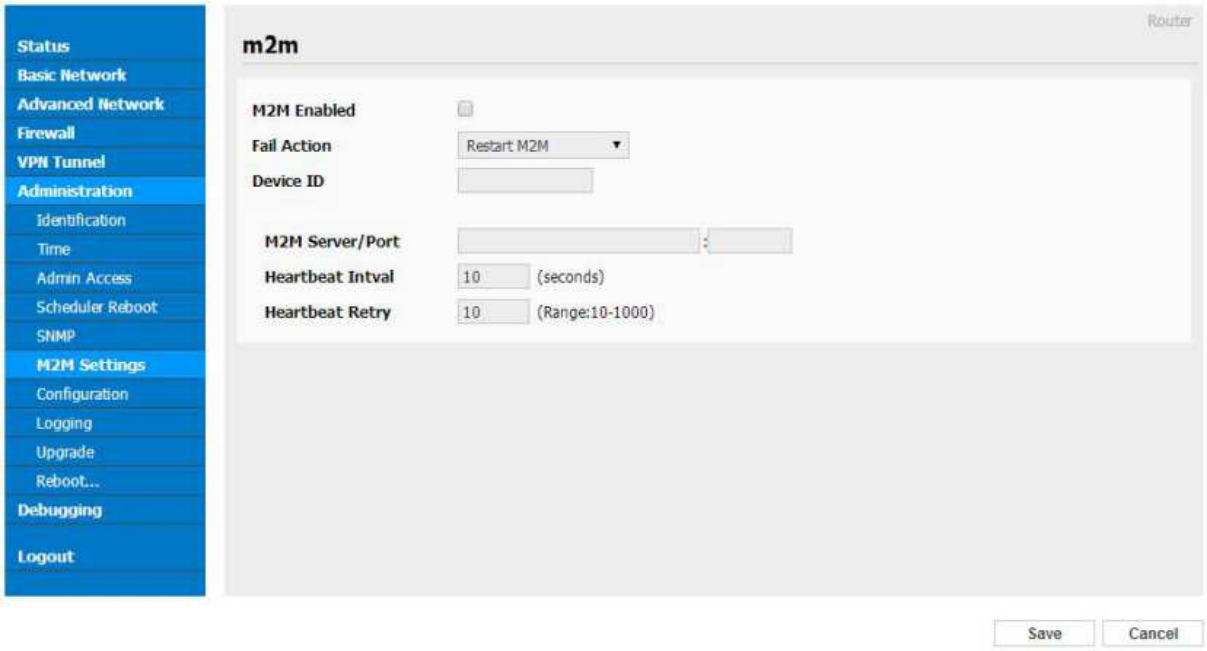
Figure 3-6 SNMP Setting GUI

Step 2 Please click save iron to finish the setting

----End

3.6.6 M2M Access Setting (Apply to M2M management platform installation application only)

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



Step 2 Please click save iron to finish the setting

----End

3.6.7 Configuration Setting

Step 1 Please click " Administration> Configuration " to do the backup setting

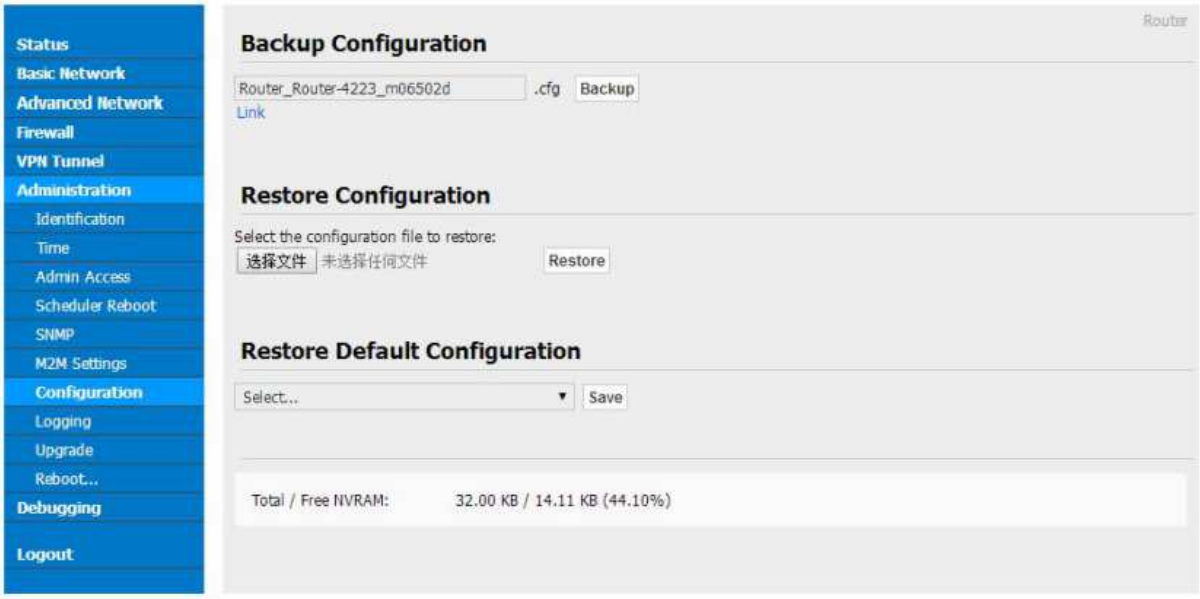


Figure 3-8 Backup and Restore Configuration GUI

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

3.6.8 Logging 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).

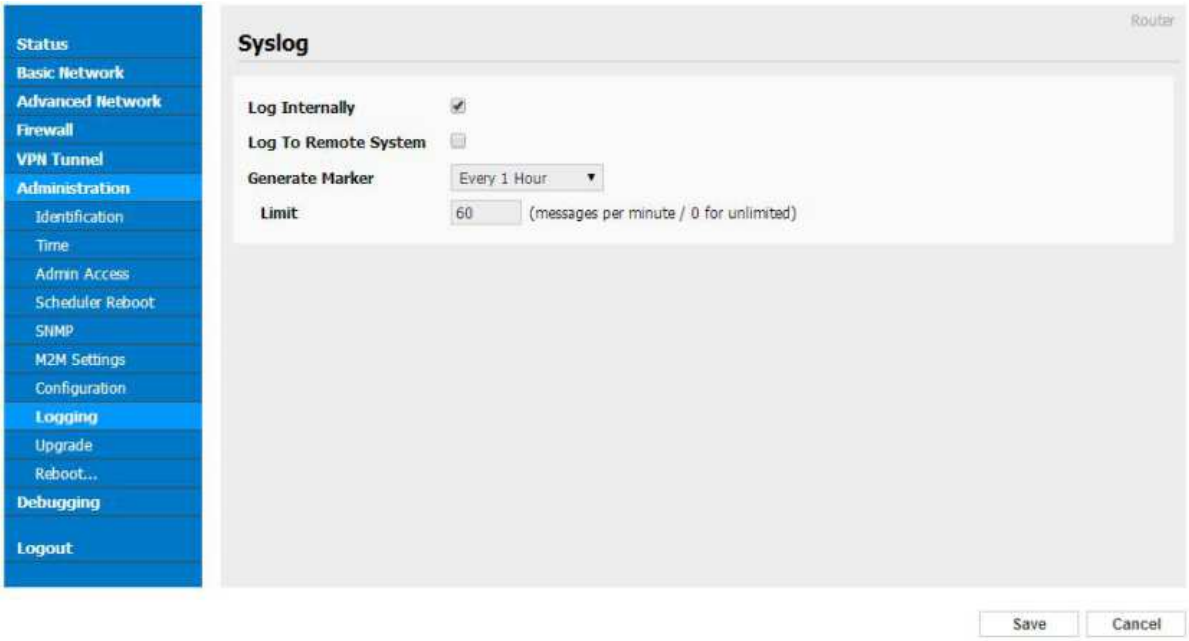


Figure 3-9 System log Setting GUI

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

----End

3.6.9 Firmware upgrade

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

Figure 3-10 Firmware Upgrade GUI

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

3.6.10 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

3.7 Debugging Setting

3.7.1 Logs Setting

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

Figure 3-11 Logs GUI

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

----End

3.7.2 Ping Setting

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

Figure 3-12 Ping GUI

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

----End

3.7.3 Trace Setting

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

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

----End

3.8 “RST” Button for Restore Factory Setting

If you couldn’t enter web interface for other reasons, you can also use this way. For R100 Series, “RST” button is on the left or Ethernet port, for R100 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 3-5 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

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

3.9 Appendix (GPS&OpenVPN only)

3.9.1 GPS Setting

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

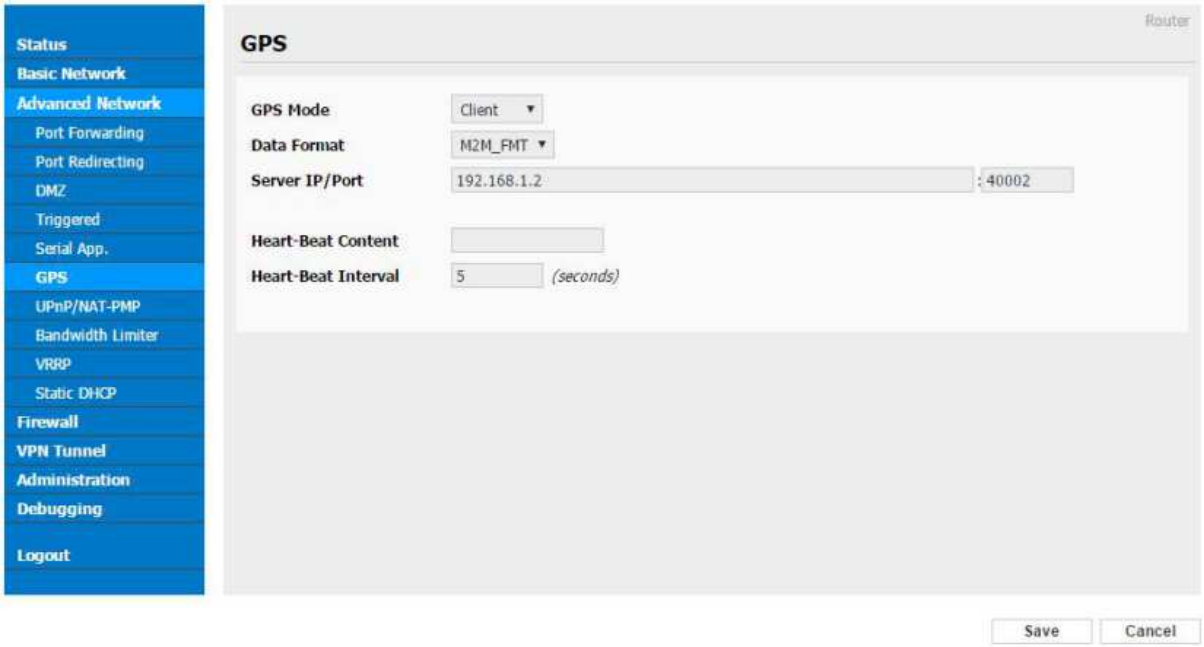


Figure 3-14 GPS Setting GUI

Table 3-6 “GPS” Instruction

parameter	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 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

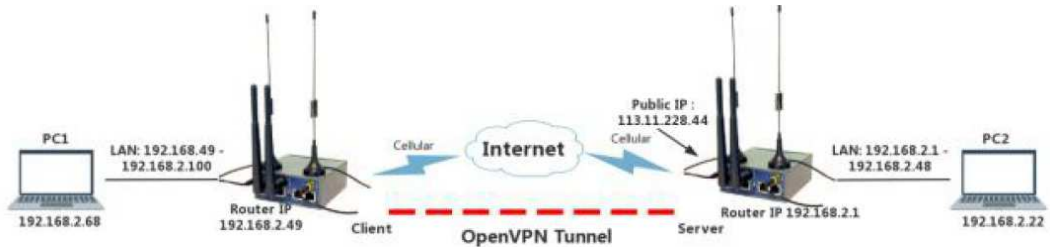
2. Example
0001_R081850ac,150904,043215.0,06,2234.248130,N,11356.626179,E,0.0,91.5,1,1.2,97.5

3. GPS data description

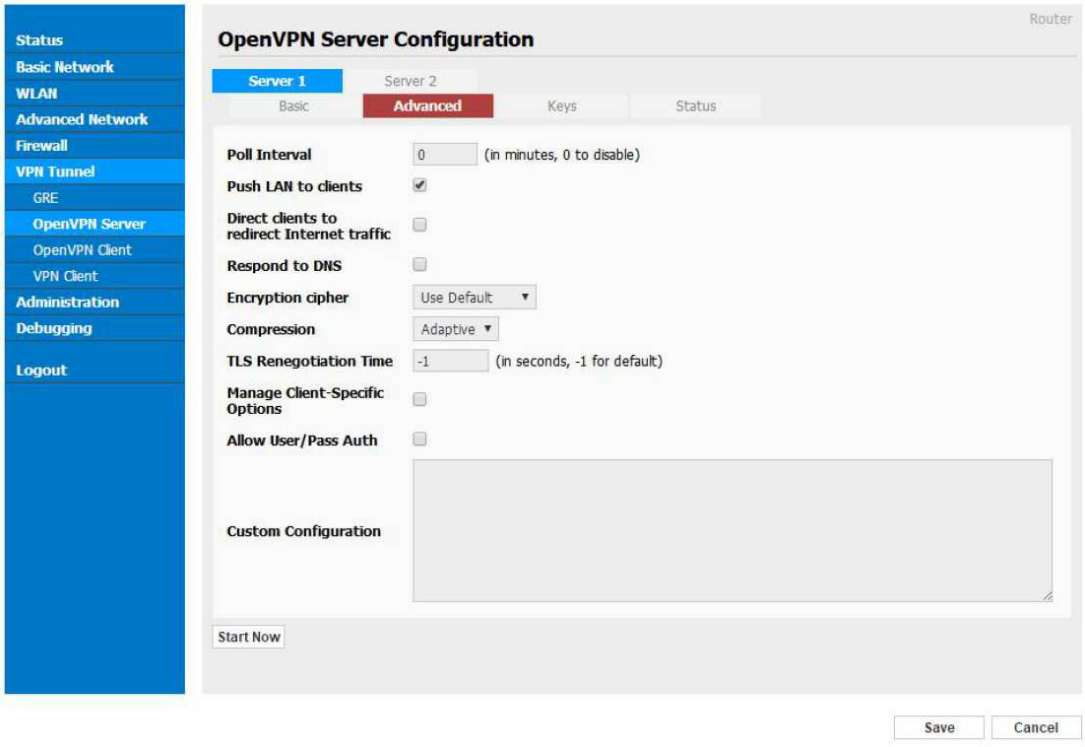
Field No.	Name	Format	Example	Description
1	Router ID	String	0001_R081850ac	0001 customizable product ID. _R router indicator. 081850ac Last 8digits of routers MAC address.
2	gps_date	yymmdd	150904	Date in year,month,day
3	gps_time	hhmmss.sss	043215.0	UTC Time, Time of position fix.
4	gps_use	numeric	06	Satellites Used, Range 0 to 12.
5	gps_latitude	ddmm.mmmm	2234.248130	Latitude, Degrees + minutes.
6	gps_NS	character	N	N/S Indicator,N=north or S=south.
7	gps_longitude	ddmm.mmmm	11356.626179	Longitude, Degrees + minutes.
8	gps_EW	character	E	E/W indicator, E=east or W=west.
9	gps_speed	numeric	0.0	Speed over ground, units is km/h.
10	gps_degrees	numeric	91.5	Course over ground, unit is degree.
11	gps_FS	digit	1	Position Fix Status Indicator,
12	gps_HDOP	numeric	1.2	HDOP, Horizontal Dilution of Precision
13	gps_MSL	numeric	97.5	MSL Altitude, units is meter.

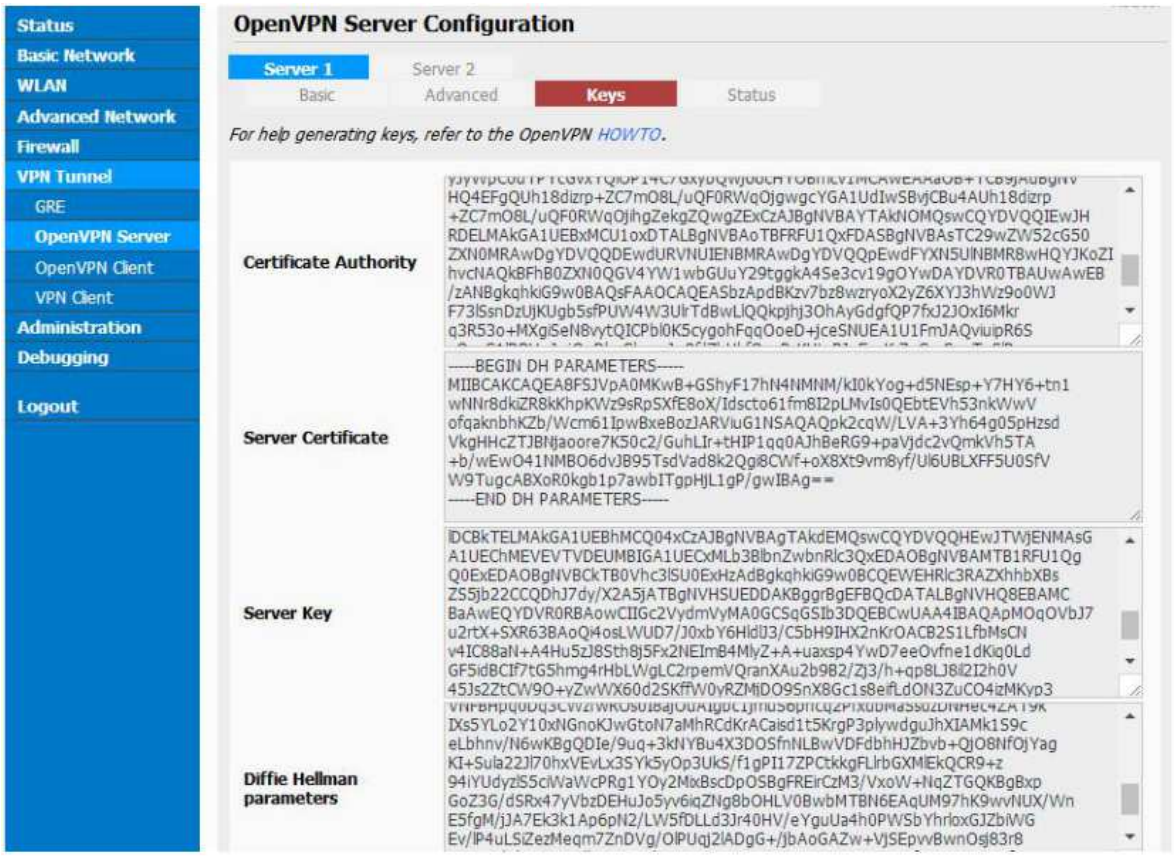
3.9.2 OpenVPN Demo (TAP Mode)

1) Network topology

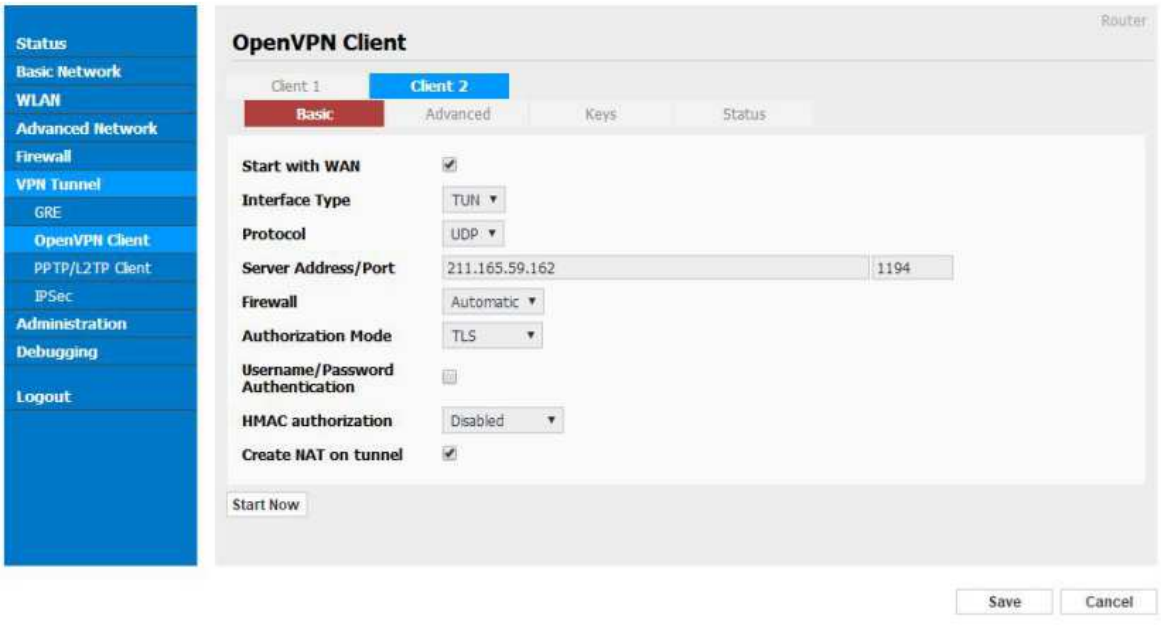


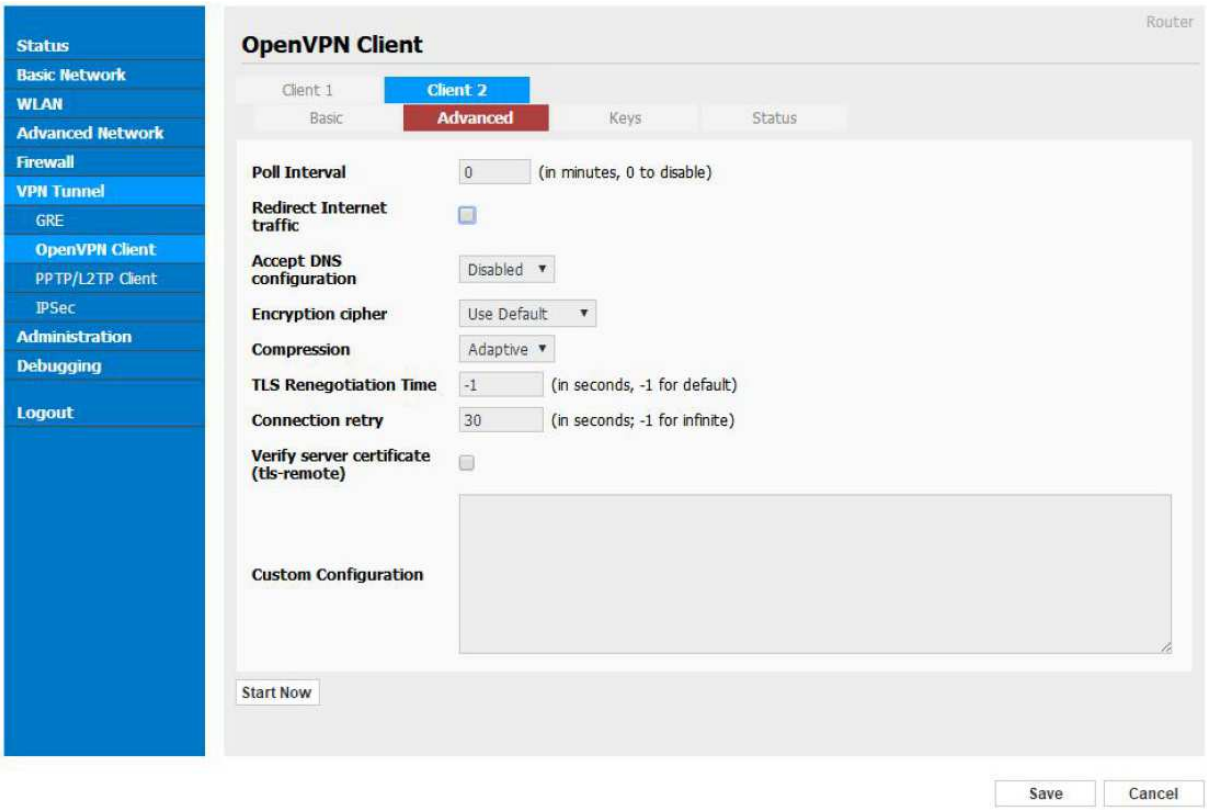
2) OpenVPN Server Config Demo

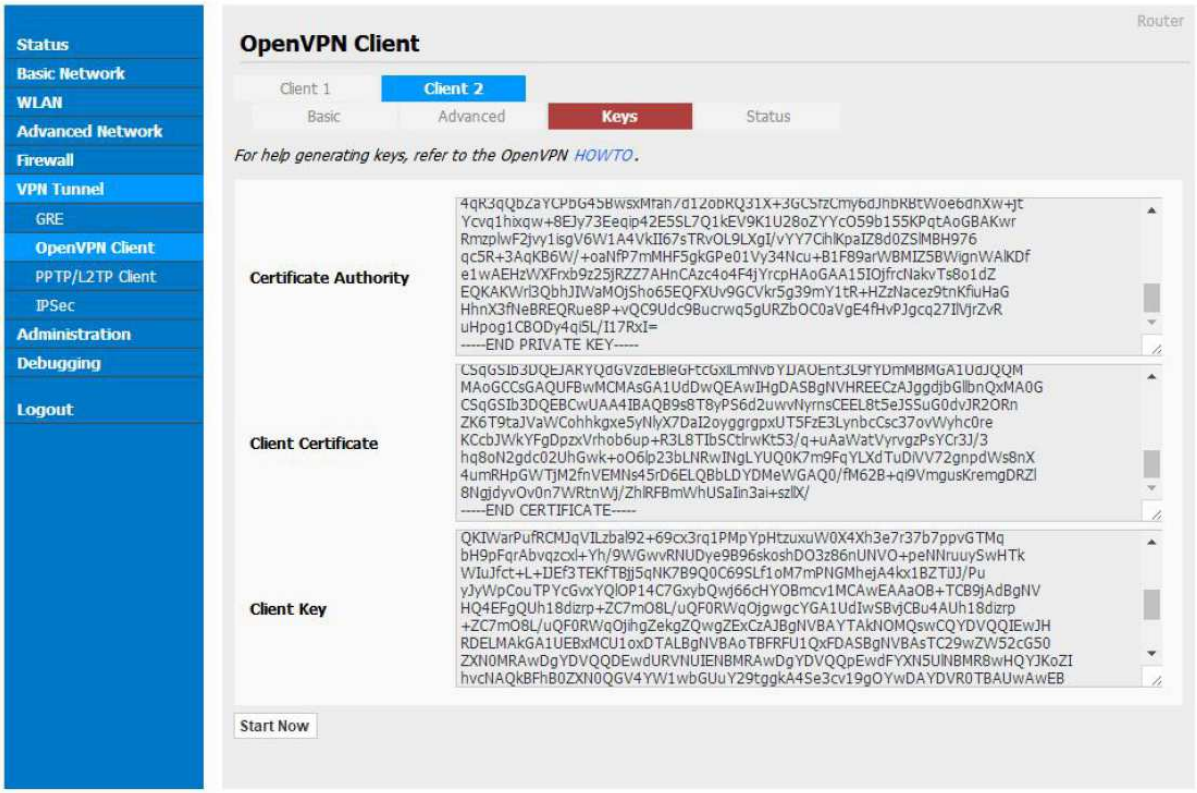




3) OpenVPN Client Config Demo




Router
Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
Debugging
Logout
OpenVPN Client
Client 1
Client 2
Basic
Advanced
Keys
Status
Poll Interval
0
(in minutes, 0 to disable)
Redirect Internet traffic
Accept DNS configuration
Disabled
Encryption cipher
Use Default
Compression
Adaptive
TLS Renegotiation Time
-1
(in seconds, -1 for default)
Connection retry
30
(in seconds; -1 for infinite)
Verify server certificate (tls-remote)
Custom Configuration
Start Now
Save
Cancel


Router
Status
Basic Network
WLAN
Advanced Network
Firewall
VPN Tunnel
GRE
OpenVPN Client
PPTP/L2TP Client
IPSec
Administration
Debugging
Logout
OpenVPN Client
Client 1
Client 2
Basic
Advanced
Keys
Status
For help generating keys, refer to the OpenVPN HOWTO.
Certificate Authority
Ycvq1hixqw+8EJy73Eeqip42E5SL7Q1kEV9K1U28oZYYcO59b155KPqtAoGBAKwr
RmzplwF2jvy1isgV6W1A4VkII67sTRvOL9LXgI/vYY7ClhlKpaIZ8d0ZSlMBH976
qc5R+3AqKB6W//+oaNfP7mMHF5gkGPe01Vy34Ncu+B1F89arWBMIZ5BWignWAlKDf
e1wAEHzWXFrxb9z25jRZZ7AHnCAzc4o4F4jYrcpHAoGAA15IOjfrcNakvTs8o1dZ
EQKAKWrl3QbhJIWaMOjSho65EQFXUv9GCVkr5g39mY1tR+HZzNacez9tnKfiuHaG
HhnX3fNeBREQRue8P+vQC9Udc9Bucrwq5gURZbOC0aVgE4fHvPJgcq27IlVjrZvR
uHpog1CBODy4qi5L/I17RxI=
-----END PRIVATE KEY-----
Client Certificate
MAoGCCsGAQUFBwMCMAsGA1UdDwQEAwIHgDASBgNVHREECzAJggdjbGlbnQxMA0G
CSqGSIb3DQEBCwUAA4IBAQB9s8T8yPS6d2uwvNyrnsCEEL8t5eJSSuG0dvJR2ORn
ZK6T9taJVaWCohhkgxe5yNlyX7DaI2oyggrgpxUT5FzE3LynbcCsc37ovWyhc0re
KCcbJWkYFgDpzxVrhob6up+R3L8TIbSCtlrwKt53/q+uAaWatVyrvgzPsYCr3J/3
hq8oN2gdc02UhGwk+oO6lp23bLNRwINgLYUQ0K7m9FqYLXdTuDiVV72gnpdWs8nX
4umRHpGWTjM2fnVEMNs45rD6ELQBbLDYDMeWGAQ0/fM62B+qi9VmgusKremgDRZl
8NgjdyvOv0n7WRtnWj/ZhlRFBmWhUSaIin3ai+szllX/
-----END CERTIFICATE-----
Client Key
QKIWarPufRCMJqVILzbal92+69cx3rq1PMpYpHtzuxuW0X4Xh3e7r37b7ppvGTMq
bH9pFqrAbvqzcxl+Yh/9WGwvRNUDye9B96skoshDO3z86nUNVO+peNNruuySwHTk
WIuJfct+L+IJEf3TEKfTBjj5qNK7B9Q0C69SLf1oM7mPNGMhejA4kx1BZTiJ/Pu
yJyWpCouTPYcGvxYQlOP14C7GxybQwj66cHYOBmcv1MCAwEAAaOB+TCB9jAdBgNV
HQ4EFgQUh18dizrp+ZC7mO8L/uQF0RWqOjgwgcYGA1UdIwSBvjCBu4AUh18dizrp
+ZC7mO8L/uQF0RWqOjihgZekgZQwgZExCzAJBgNVBAYTAkNOMQswCQYDVQQIEwJH
RDELMAkGA1UEBxMCU1oxDTALBgNVBAoTBFRFU1QxFDASBgNVBAsTC29wZW52cG50
ZXN0MRAwDgYDVQQDEwdURVNUIENBMRAwDgYDVQQpEwdFYXN5UlNBMR8wHQYJKoZI
hvcNAQkBFhB0ZXN0QGV4YW1wbGUuY29tggkA4Se3cv19gOYwDAYDVR0TBAUwAwEB
Start Now