



User Manual

---Apply to H23 Series Industrial 4G/3G Router

IOT SOLUTIONS



V3.0

<http://www.homtecsm2m.com>

Jan., 2024



Copyright © Shenzhen Homtecs Technology Company Limited 2012 ~ 2024

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 Homtecs reserves the right of final explanation.

Shenzhen Homtecs Technology Company Limited

Add: 2A, F5 Building, Zhongshanyuan Road, TCL International E-City,
Xili, Nanshan District, China, 518000

Web: <http://www.homtecsm2m.com>

Email: info@homtecsm2m.com

Tel: 86-755-23903495

Contents

1 Hardware Installation	5
1.1 Panel	5
1.2 LED Status	6
1.3 How to Install	7
1.3.1 SIM/UIM card install	7
1.3.2 Ethernet Cable Connection	7
1.3.3 4G and Wi-Fi Antenna Plug	7
1.3.3 Power Supply	7
1.3.4 Review	7
2 Router Configuration	8
2.1 Local Configure	8
2.2 Status	9
2.3 Basic Network Settings	10
2.3.1 WAN Setting	10
2.3.2 Cellular Network Setting	10
2.3.3 LAN Setting	13
2.3.4 Dynamic DNS Setting	13
2.3.5 Routing Setting	14
2.4 WLAN Setting	15
2.4.1 Basic Setting	15
2.4.2 MultiSSID	16
2.4.3 Wireless Filter Setting	16
2.4.4 Advanced Wireless Setting	17
2.4.5 Wireless Survey	18
2.5 Advanced Network Setting	18
2.5.1 Port Forwarding	18
2.5.2 Port Redirecting	19
2.5.3 DMZ Setting	20
2.5.4 IP Passthrough Setting	20
2.5.5 Triggered Setting	21
2.5.6 Serial APP. Setting	22
2.5.7 UPnp/NAT-PMP Setting	23
2.5.8 Bandwidth Control Setting	23
2.5.9 VRRP Setting	24
2.5.10 Static DHCP Setting	24
2.6 Firewall	25
2.6.1 IP/URL Filtering	25
2.6.2 Domain Filtering	26



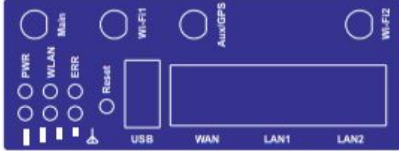
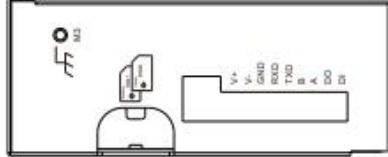
- 2.7 VPN Tunnel 26
 - 2.7.1 GRE Setting 26
 - 2.7.2 OpenVPN Client Setting 27
 - 2.7.3 VPN Client Setting 30
 - 2.7.4 IPSec Setting 32
- 2.8 Administration 34
 - 2.8.1 Identification Setting 35
 - 2.8.2 Time Setting 35
 - 2.8.3 Admin Access Setting 36
 - 2.8.4 Schedule Reboot Setting 36
 - 2.8.5 SNMP Setting 37
 - 2.8.6 M2M Access Setting (Apply to M2M Management Platform 37
 - 2.8.8 System Log Setting 38
 - 2.8.9 Firmware upgrade 39
- 2.9 System Reboot 39
- 2.10 Debugging Setting 40
 - 2.10.1 Logs Setting 40
 - 2.10.2 Ping Setting 40
 - 2.10.3 Trace Setting 41
- 2.11 “Reset” Button for Restore Factory Setting 41
- 2.12 Appendix (For advanced optional features only) 42
 - 2.12.1 GPS Setting 42
 - 2.12.2 Captive Portal Setting 44
 - 2.12.3 VLAN 46
 - 2.12.4 Schedule 49

1 Hardware Installation

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

1.1 Panel

Table 1-1 H23 Structure

Homtecs Tech.	H23 Series
Front panel	
Side panel	

Note:

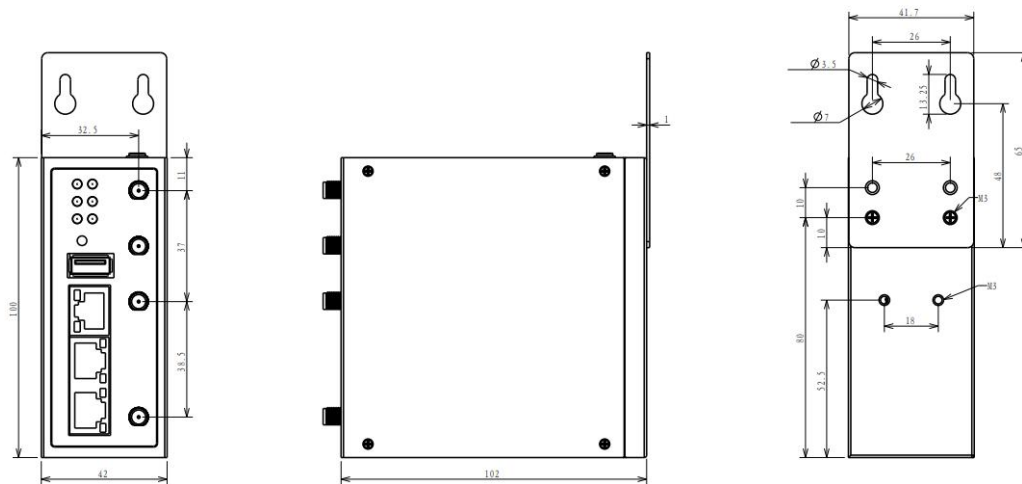
There are some differences on Antenna interface and indicator light for the device with extended Wi-Fi, GPS features.

Table 1-2 H23 Interface

Port	Instruction	Remark
USIM	Plug type SIM Slot, support 1.8/3V/5V automatic detection.	
Main	LTE antenna, SMA connector, 50Ω.	
Aux	LTE MIMO antenna	
GPS	GPS antenna, SMA connector, 50Ω.	
Wi-Fi 1	Wi-Fi dual-band antenna, SMA connector	
Wi-Fi 2	Wi-Fi dual-band antenna, SMA connector	
LAN	10/100/1000Base-TX, MDI/MDIX self-adaption.	2

WAN/LAN	10/100/1000Base-TX, MDI/MDIX self-adaption.	1, Default as LAN
Reset	Reset button, (press on button at least 15 seconds)	
PWR	Power connector	7.5 ~ 32V DC
Serial port	RS-232/RS485.	

H23 Dimension



Note:

The equipment supports a variety of installation methods, such as embedded integration, desktop placement, wall installation and din-rail installation and other ways.

1.2 LED Status

Table 1-4 H23 LED indicator Status

PWR	WLAN	ERR	Signal1	Signal2	Signal3	Indication
			Solid light	Solid light	Solid light	4G online, CSQ: (15-31)
			Solid light	Solid light	Dark	4G online, CSQ: (11-14)
			Solid light	Dark	Dark	4G online, CSQ: ≤ 10
			2S blinking cycle, light 1.5S, off 0.5S	Solid light	Solid light	3G online, CSQ: (15-31)
			2S blinking cycle, light 1.5S, off 0.5S	Solid light	Dark	3G online, CSQ: (11-14)
			2S blinking cycle, light 1.5S, off 0.5S	Dark	Dark	3G online, CSQ: ≤ 10
			0.5S blinking cycle, light 0.25S, off			Sign up for the network

			0.25S			
	Solid light					WLAN enabled, but no data communication
	Blinking quickly					WLAN enabled, and data is in transmitting
	Dark					WLAN disabled
		Dark				Read SIM success
		Solid light				Read SIM failed
Solid light						Power supply is normal

Note:

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

1.3 How to Install

1.3.1 SIM/UIM card install

Please insert the SIM cards before configure the router.

Note:

Before connecting, please disconnect any power resource of router

1.3.2 Ethernet Cable Connection

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

1.3.3 4G and Wi-Fi Antenna Plug

Connect the two magnetic 4G antennas to Main and Aux interfaces, and the one paddle shape Wi-Fi antenna interface.

Note:

Wi-Fi antenna only supports 2.4G.

1.3.3 Power Supply

Plug in power adaptor. Input range of voltage: +7.5~32VDC. (Extended models: 7.5~ 48VDC)

1.3.4 Review

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

CAUTION:

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

Note:

- Step 1 Check the antenna connection.
- Step 2 Check SIM/UIM card, confirm SIM/UIM card is available.
- Step 3 Power on the industrial Router

---END

2 Router Configuration

H Series routers support GUI and CLI configuration. This chapter introduce GUI configuration via Ethernet port, if need CLI configuration guide, please contact our technical support department by email: info@hometecsm2m.com

2.1 Local Configure

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

Step 1 Click “start > control panel”, find “Network Connections” icon and double click it to enter, select “Local Area Connection” corresponding to the network card on this page. Refer to the figure below.



Figure 2-3 Network Connection

Step 2 Obtain a IP address automatically(DHCP) 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(admin/admin) when log in for the first time

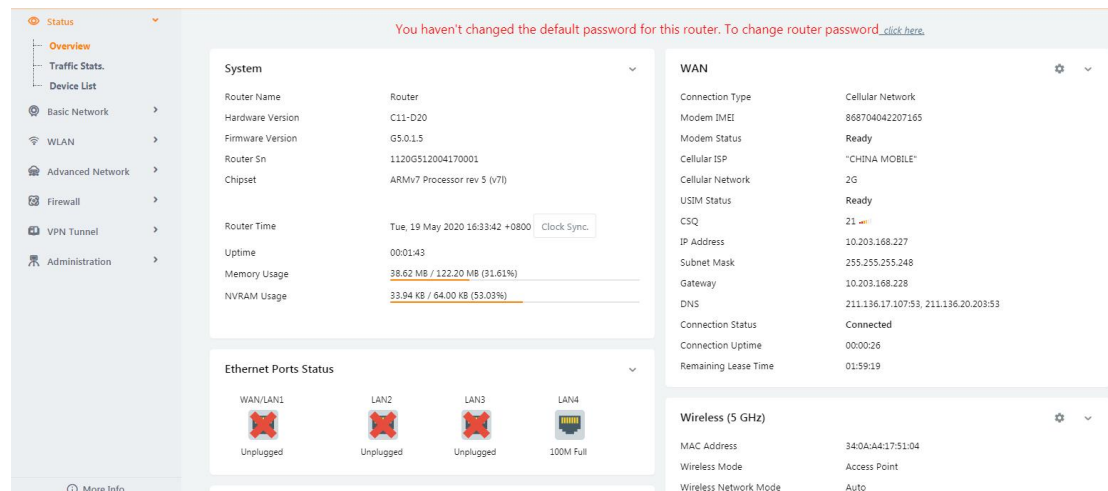


Figure 2-4 User Identify Interface

----END

2.2 Status

Check routers status after login router.



Note:

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

You haven't changed the default password for this router. To change router password [click here.](#)

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

Already changed login password successfully.

2.3 Basic Network Settings

2.3.1 WAN Setting

Step 1 Basic Network>WAN to enter below interface

Table 3-1 WAN Setting Instruction

Parameter	Instruction	Remark
Type	Disable, DHCP, PPPoE, Static IP	
MTU	Default is 1500	

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

----End

2.3.2 Cellular Network Setting

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

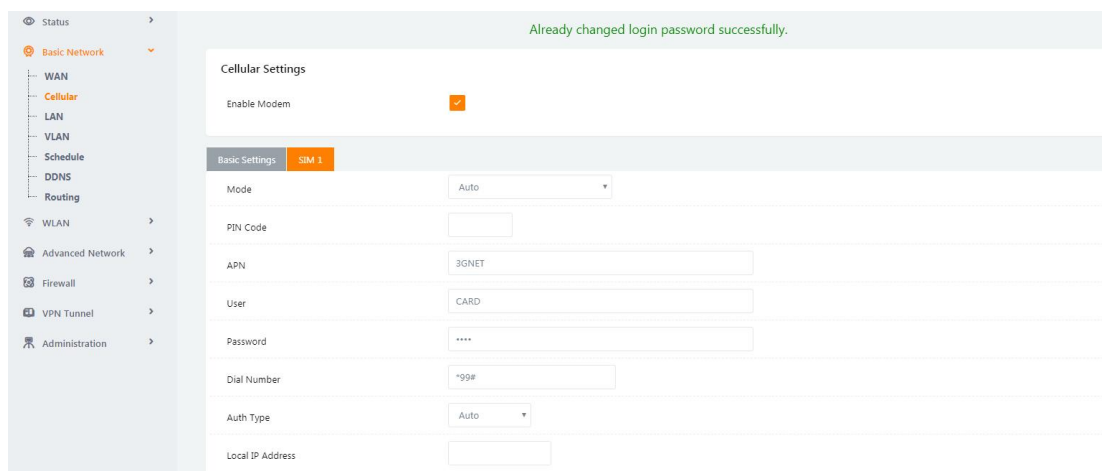


Figure 3-2 Cellular Setting GUI

Parameter	Instruction
Use PPP	ECM dialup as default. PPP optional.
ICMP Check	If enable ICMP check and setup a reachable IP address as destination IP, the router will reconnect/reboot once ICMP check failed.
Cellular Traffic Check	The router will reconnect/reboot once there's no Rx/Tx data.
CIMI Send to	Send CIMI to a defined IP and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock a specified operator for the router by MCC/MNC code.
Dual SIM Mode	<p>【 Fail Over 】 Two SIM cards mutual backup. Once SIM1 failed, it'll switch to SIM2 and work on SIM2, and vice versa.</p> <p>【 SIM1 Only 】 Only SIM1 works.</p> <p>【 SIM2 Only 】 Only SIM2 works.</p> <p>【 Backup 】 SIM1 is the primary SIM. Once SIM1 failed, it'll switch to SIM2 and work on SIM2 for a specified period of time, then it switches back to SIM1</p> <p>NOTE: can be set via Schedule</p>
Connect Mode	<p>【 Auto 】 The router will automatically connect to 3G/4G networks and give priority to 4G.</p> <p>【 LTE 】 Router will connect to 4G only.</p> <p>【 3G 】 Router will connect to 3G only.</p>
Pin Code	Some SIM cards are locked with a Personal Identification Number (PIN) code in case they are lost or stolen.

APN	APN is provided by local ISP, usually in CDMA/EVDO networks APN does not need to be set..
User	SIM card user name is provided by ISP
Password	SIM card password is provided by ISP
Auth. Type	Auto/PAP/Chap/MS-Chap/MS-Chapv2 authentication optional.
SIM Local IP Address	Fix SIM IP. The feature is available if carrier can provide this service.

Note:

ICMC Check and Cellular Traffic Check are alternative.

【ICMP Check】

Enable ICMP, Router will automatically check whether the defined IP address is reachable per 60s.

If the IP address is unreachable and ICMP check is timeout at the first time, it will check 2 times every 3 seconds. If the third time is still failed, the router will redial.

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

ICMP Check

Check IP

Check IP (Optional)

Interval (seconds)

Retries (Times)

Fail Action

【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

Check Interval (minutes)Range: 1 ~ 1440

Fail Action

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

----End

2.3.3 LAN Setting

Step 1 Basic Network>LAN to enter below interface

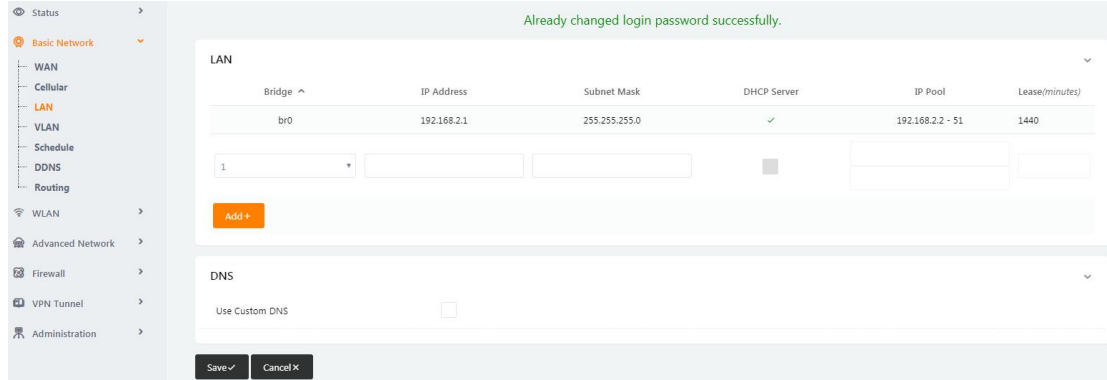


Figure 3-3 LAN Setting GUI

Table 3-2 LAN Setting Instruction

Parameter	Instruction
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 Server	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

2.3.4 Dynamic DNS Setting

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

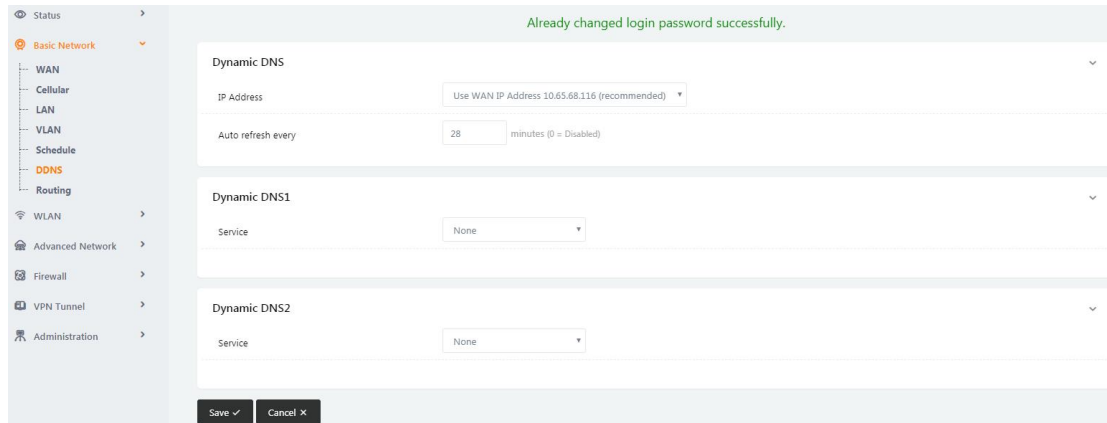


Figure 3-4 DDNS Setting GUI

Table 3-3 DDNS Setting Instruction

Parameter	Instruction
IP address	Default is standard DDNS protocol, for customized protocol, please contact Homtecs engineer. Usually, use default IP 0.0.0.0
Auto refresh every	Set the interval of the DDNS client obtains new IP, suggest 240s or above
Dynamic DNS1 Dynamic DNS2	Select the DDNS service provider that listed.

Step 2 Please Click “Save” to finish.

----End

2.3.5 Routing Setting

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

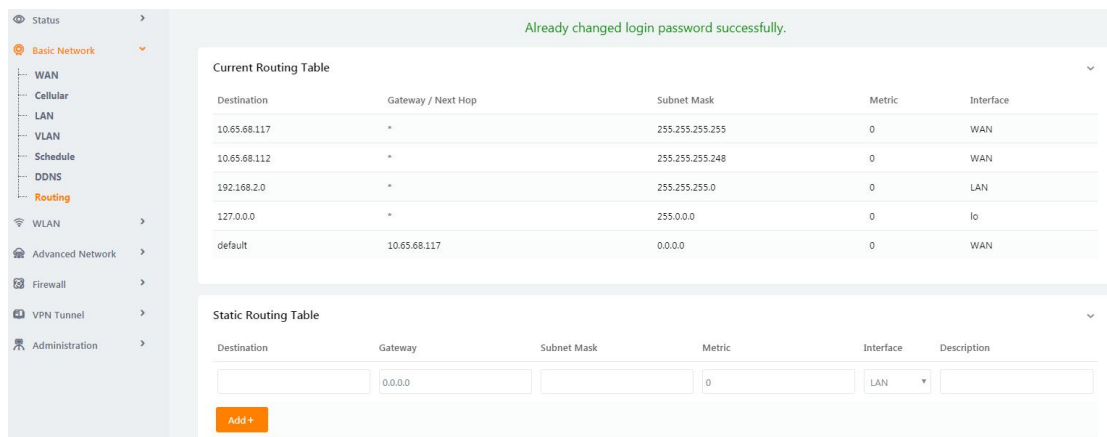


Figure 3-5 Routing Setting

Table 3-4 Routing Setting Instruction

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

----End

2.4 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

2.4.1 Basic Setting

Step 1 WLAN->Basic Setting to configure relative parameter

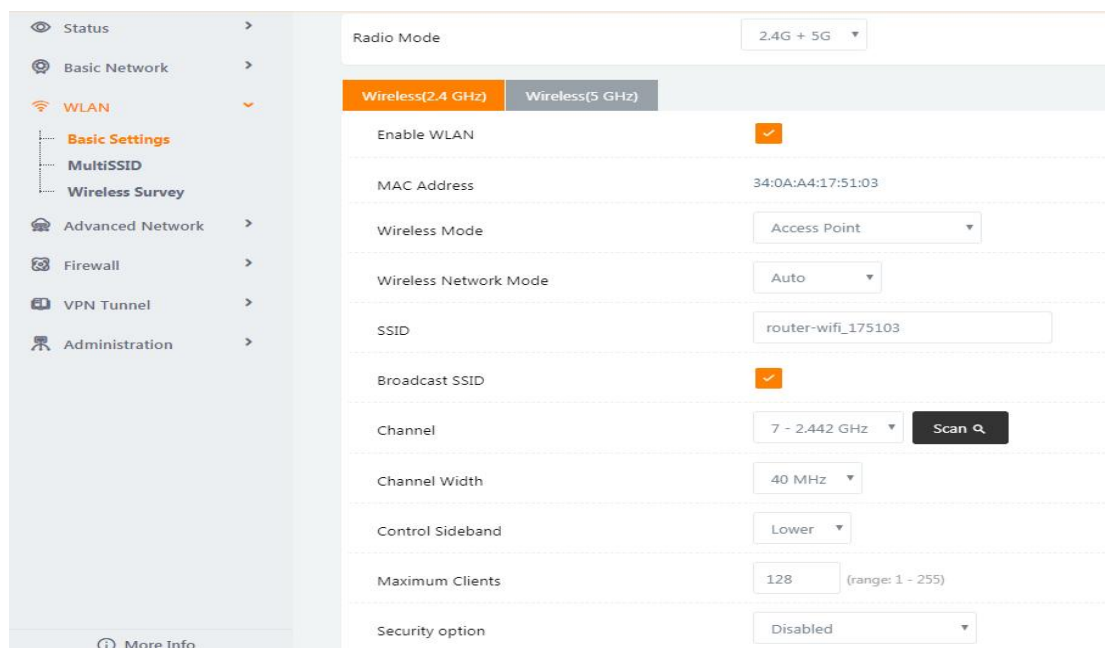


Figure 3-6 WLAN Basic Settings GUI

Table 3-5 Basic Setting Instruction

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

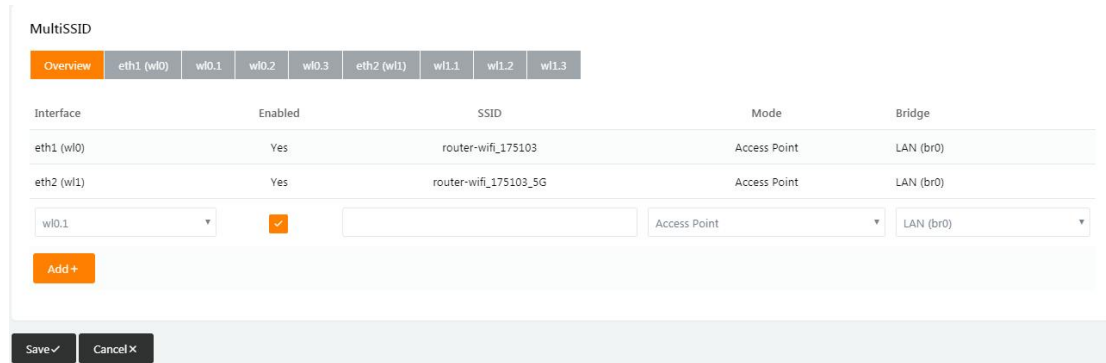
Step 2 Please click “Save” to finish.

-

---End

2.4.2 MultiSSID

Step 1 WLAN > MultiSSID



MultiSSID

Overview eth1 (w0) w0.1 w0.2 w0.3 eth2 (w1) w1.1 w1.2 w1.3

Interface	Enabled	SSID	Mode	Bridge
eth1 (w0)	Yes	router-wifi_175103	Access Point	LAN (br0)
eth2 (w1)	Yes	router-wifi_175103_5G	Access Point	LAN (br0)

w0.1 Access Point LAN (br0)

Add +

Save ✓ Cancel ✕

2.4.3 Wireless Filter Setting

Step 1 WLAN > Wireless Filter

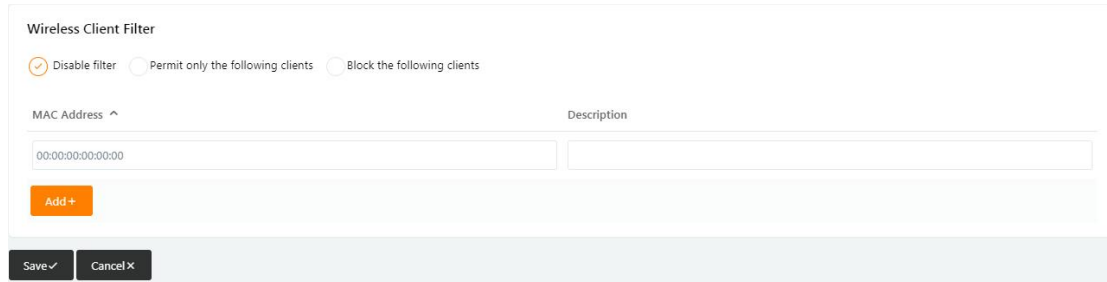


Figure 3-7 Wireless Client Filter Setting GUI

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

Table 3-6 “Wireless Client Filter” Setting Instruction

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

Step 2 Please click “Save” to finish

----End

2.4.4 Advanced Wireless Setting

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

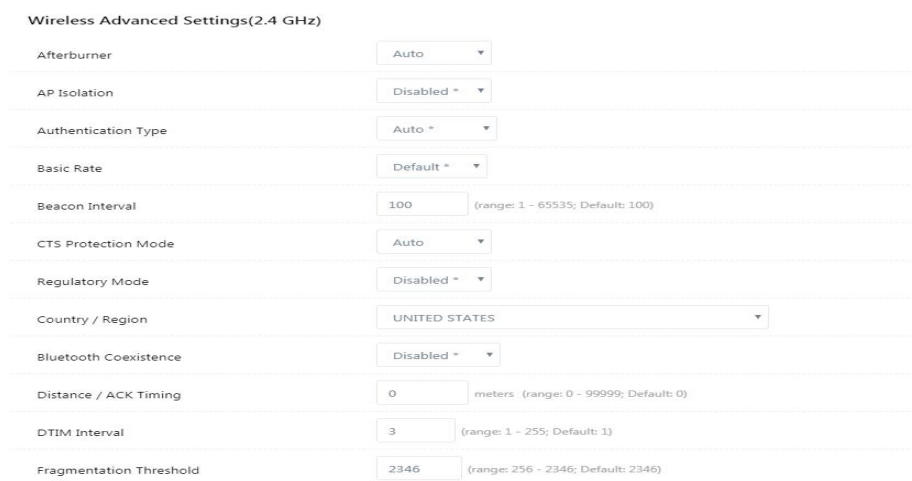


Figure 3-8 Advanced Wireless Setting GUI

Table 3-7 “Port Forwarding” Instruction

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

Step 2 Please click “Save” to finish.

----End

2.5.2 Port Redirecting

Step 1 Advanced Network > Port Redirecting to enter the GUI, you may modify the router name, Host name and Domain name according to the application requirement.

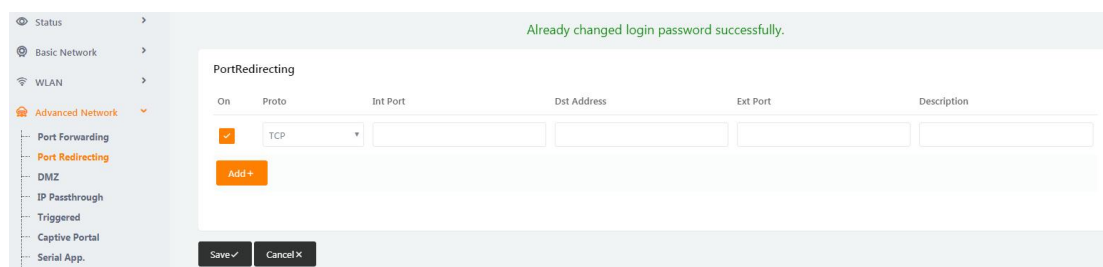


Figure 3-11 Port Forwarding GUI

Table 3-8 “Port Redirecting” Instruction

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

2.5.3 DMZ Setting

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

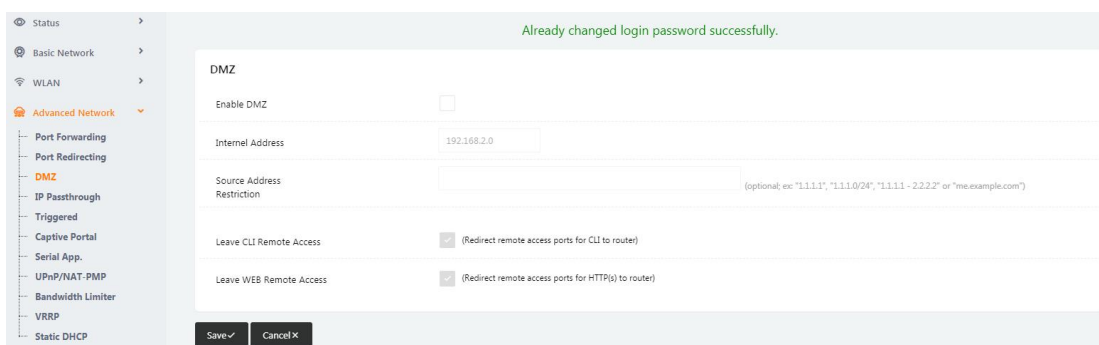


Figure 3-12 DMZ GUI

Table 3-9 “DMZ” Instruction

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

Step 2 Please click “Save” to finish.

----End

2.5.4 IP Passthrough Setting

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

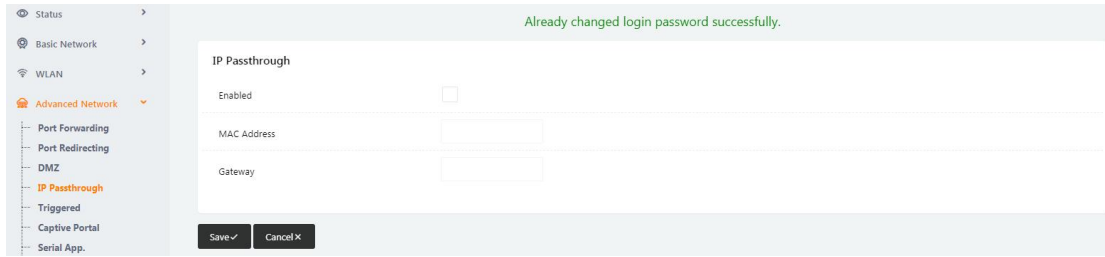


Figure 3-13 IP Passthrough GUI

Table 3-10 “IP Passthrough” Instruction

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

Step 2 Please click “Save” to finish.

----End

2.5.5 Triggered Setting

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

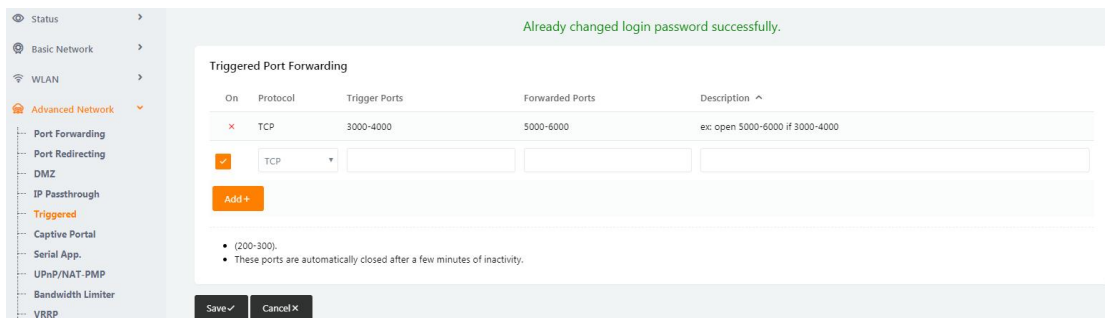


Figure 3-14 Triggered GUI

Table 3-11 “Triggered” Instruction

Parameter	Instruction
Protocol	Support UDP, TCP, both UDP and TCP
Triggered Ports	Trigger Ports are the initial LAN to WAN "trigger".

Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.
Note	Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic.

Step 2 Please click "Save" to finish.

----End

2.5.6 Serial APP. Setting

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

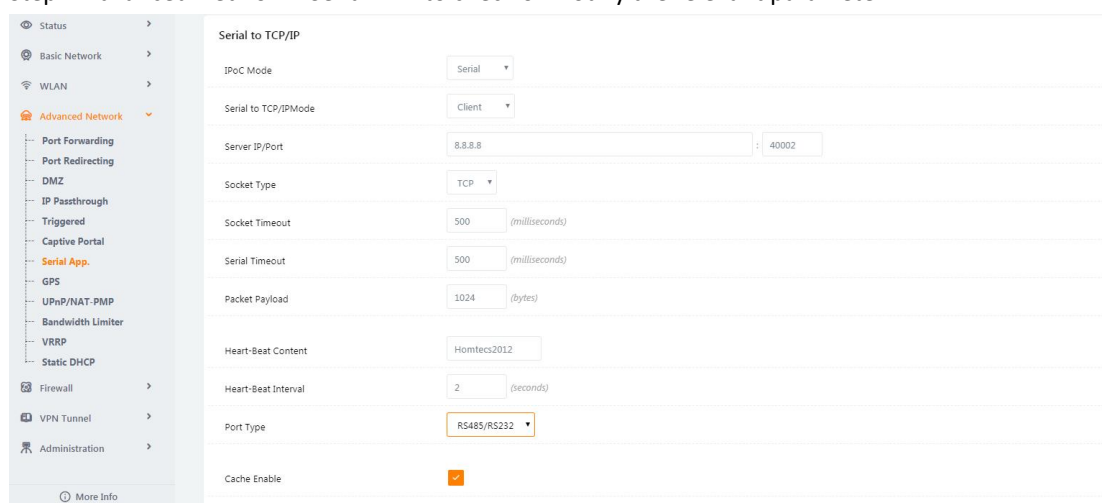


Figure 3-15 Serial App Setting GUI

Table 3-12 "Serial App" Instruction

Parameter	Instruction
Serial to TC/IP mode	Support Disable, Server and Client mode. Such as Client.
Server IP/Port	IP address and domain name are acceptable for Server IP
Socket Type	Support TCP/UDP protocol
Socket Timeout	Router will wait the setting time to transmit data to serial port.
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that is less the Packet payload. If the last package equals to the Packet payload, Serial port will transmit it immediately. The default setting is 500ms.
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.

Heart-beat Content	Send heart beat to the defined server to keep router online. Meantime, it's convenient to monitor router from server.
Heart beat Interval	Heart beat interval time
Baud Rate	115200 as default
Parity Bit	None as default
Data Bit	8bit as default
Stop Bit	1bit as default

Step 2 Please click “Save” to finish.

----End

2.5.7 UPnp/NAT-PMP Setting

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

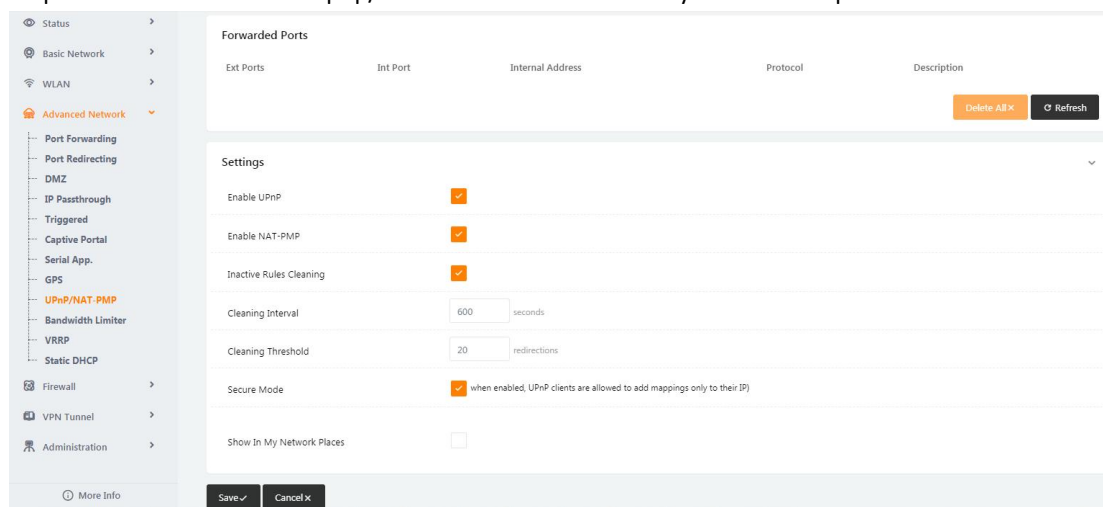


Figure 3-16 UPnp/NAT-PMP Setting GUI

Step 2 Please click “Save” to finish.

2.5.8 Bandwidth Control Setting

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

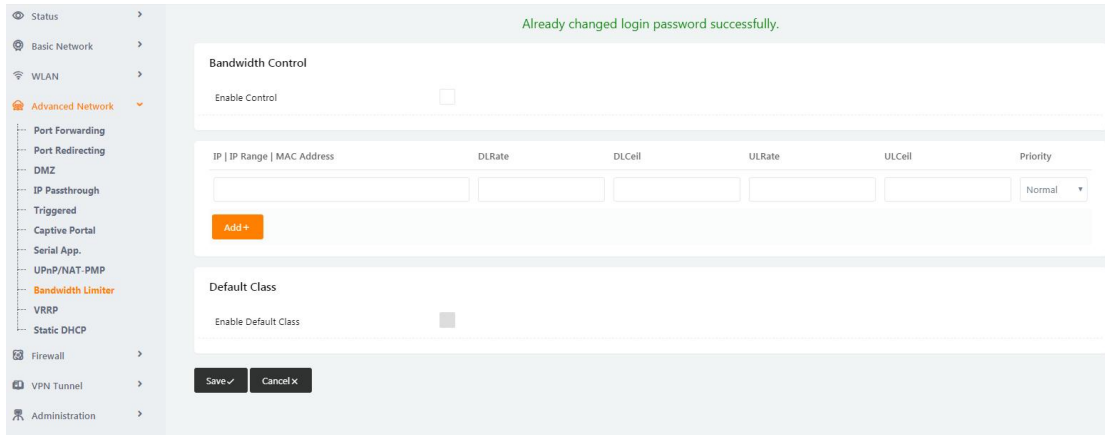


Figure 3-17 Bandwidth Control Setting GUI

Step 2 Please click “Save” to finish.

----End

2.5.9 VRRP Setting

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

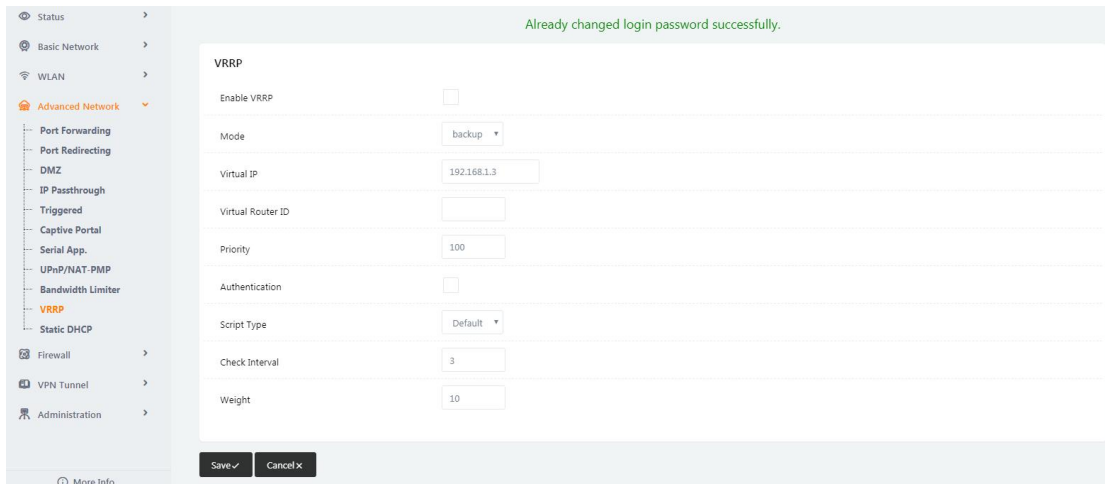


Figure 3-18 VRRP Setting GUI

Step 2 Please click “Save” to finish.

----End

2.5.10 Static DHCP Setting

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

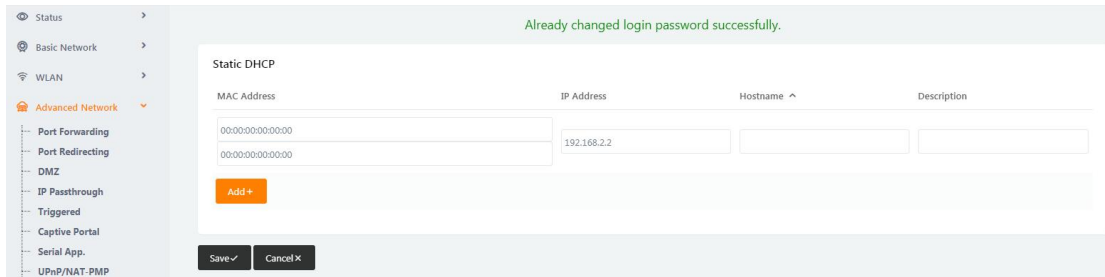


Figure 3-19 Static DHCP Setting GUI

Step 2 Please click “Save” to finish.

----End

2.6 Firewall

2.6.1 IP/URL Filtering

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

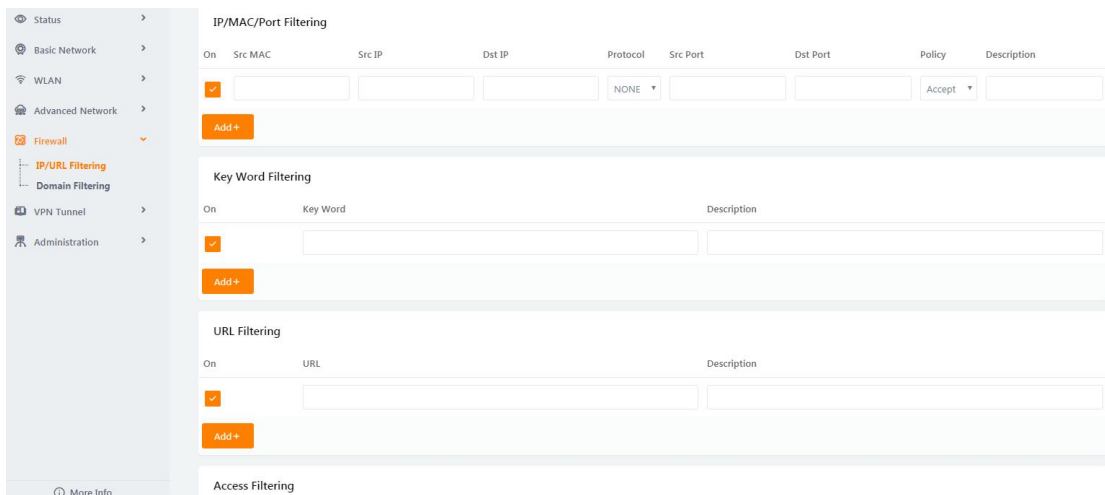


Table 3-13 “IP/URL Filtering” Instruction

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

Step 2 Please click “Save” to finish.

---End

2.6.2 Domain Filtering

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

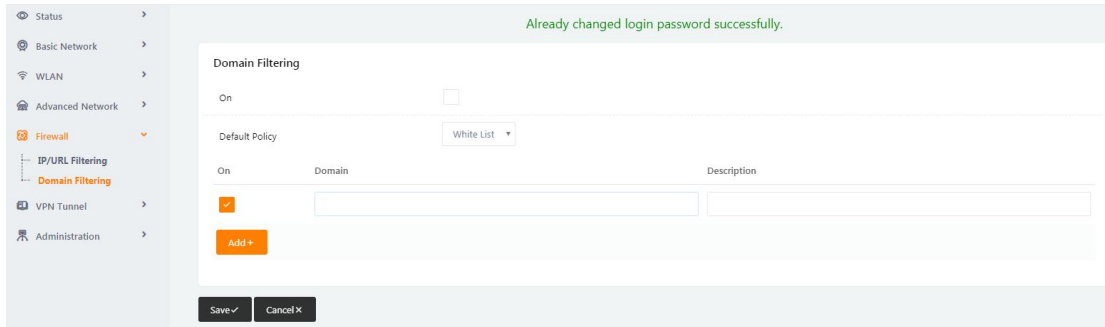


Figure 3-20 Domain Filtering Setting GUI

Table 3-14 “Domain Filtering” Instruction

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

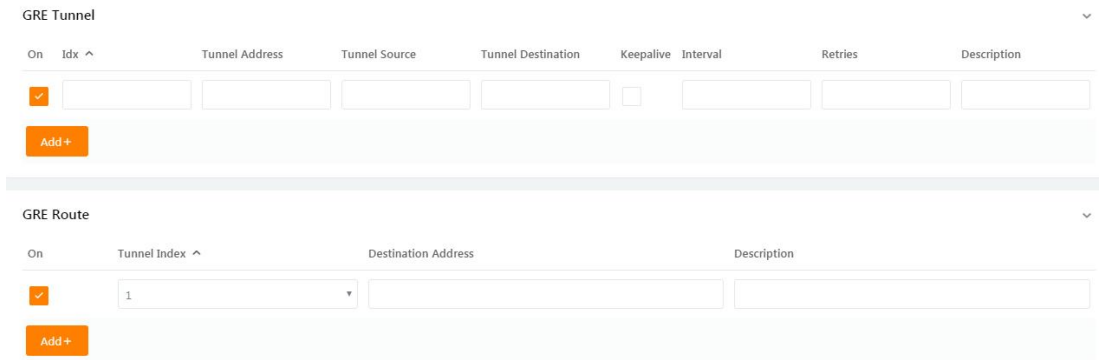
Step 2 Please click “Save” to finish.

----End

2.7 VPN Tunnel

2.7.1 GRE Setting

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



The image shows two configuration sections in a web interface. The top section is titled 'GRE Tunnel' and contains a table with columns: On, Idx, Tunnel Address, Tunnel Source, Tunnel Destination, Keepalive, Interval, Retries, and Description. Below the table is an 'Add +' button. The bottom section is titled 'GRE Route' and contains a table with columns: On, Tunnel Index, Destination Address, and Description. Below this table is also an 'Add +' button.

Figure 3-21 GRE Setting GUI

Table 3-15 “GRE” Instruction

Parameter	Instruction
IDE	GRE tunnel number
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.
Tunnel Source	Router’s 3G/WAN IP address.
Tunnel Destination	GRE Remote IP address. Usually, it’s a public IP address
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.
Parameter	Instruction
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

2.7.2 OpenVPN Client Setting

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

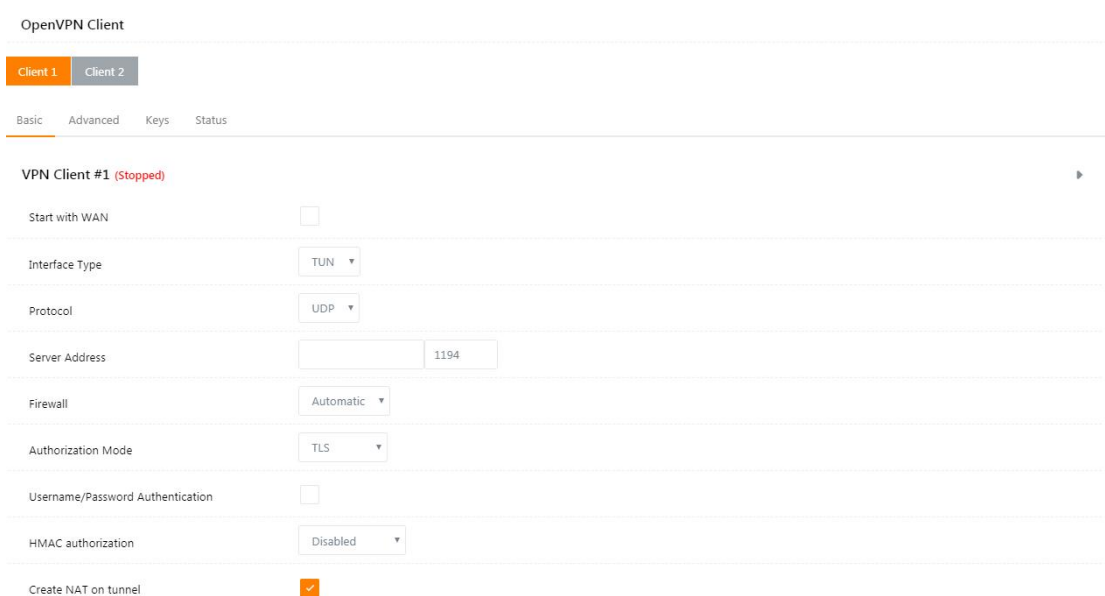


Figure 3-22 OpenVPN Setting GUI

Table 3-16 “OpenVPN” Instruction

Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 4G/3G/WAN port.
Interface Type	Tap and Tun type are optional. Tap is for bridge mode and Tunnel is for routing mode
Protocol	UDP and TCP optional.
Server Address	The Openvpn server public IP address and port.
Parameter	Instruction
Firewall	Auto, External only and Custom are optional
Authorization Mode	TLS, Static key and Custom are optional.
User name/Password Authentication	As the configuration requested.
HMAC authorization	As the configuration requested.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.



OpenVPN Client

Client 1 Client 2

Basic Advanced Keys Status

VPN Client #1 (Stopped) ▶

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)

Parameter	Instruction
Poll Interval	Openvpn client check router's status as interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As the configuration requested.
Encryption	As the configuration requested.
Compression	As the configuration requested.
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.
Connection Retry Time	OpenVPN retry to connection interval.
Parameter	Instruction
Verify server certificate	As the configuration requested.
Custom Configuration	As the configuration requested.

OpenVPN Client

Client 1 Client 2

Basic Advanced **Keys** Status

VPN Client #1 (Stopped) ▶

For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

Client Certificate

Client Key

Start Now

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

OpenVPN Client

Client 1 Client 2

Basic Advanced **Keys** Status

VPN Client #1 (Stopped) ▶

Client is not running or status could not be read. Refresh Status

Start Now

Save ✓ Cancel ✕

Step 2 Please click “Save” to check OpenVPN status and data statistics.

----End

2.7.3 VPN Client Setting

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

L2TP/PPTP Basic

On Protocol Name Server Username Password Firewall Default Route Local IP

Add +

L2TP Advanced

On Name Accept DNS MTU MRU Tunnel Auth Tunnel Password Custom Options

Add +

PPTP Advanced

On Name Accept DNS MTU MRU MPPE MPPE Stateful Custom Options

Add +

Table 3-17 “PPTP/L2TP Basic” Instruction

Parameter	Instruction
On	VPN enable
Protocol	VPN Mode for PPTP and L2TP
Name	VPN Tunnel name
Server Address	VPN Server IP address
User name	As the configuration requested
Password	As the configuration requested
Firewall	Firewall For VPN Tunnel
Local IP	Defined Local IP address for tunnel

Table 3-18 “L2TP Advanced” Instruction

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

Table 3-19 “PPTP Advanced” Instruction

Parameter	Instruction
On	PPTP Advanced enable
Name	PPTP Tunnel name

Accept DNS	As the configuration requested
MTU	MTU is 1450bytes as default
MRU	MRU is 1450bytes as default
MPPE	As the configuration requested
MPPE Stateful	As the configuration requested
Customs	As the configuration requested

Table 3-20 "SCHEDULE" Instruction

Parameter	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

2.7.4 IPSec Setting

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

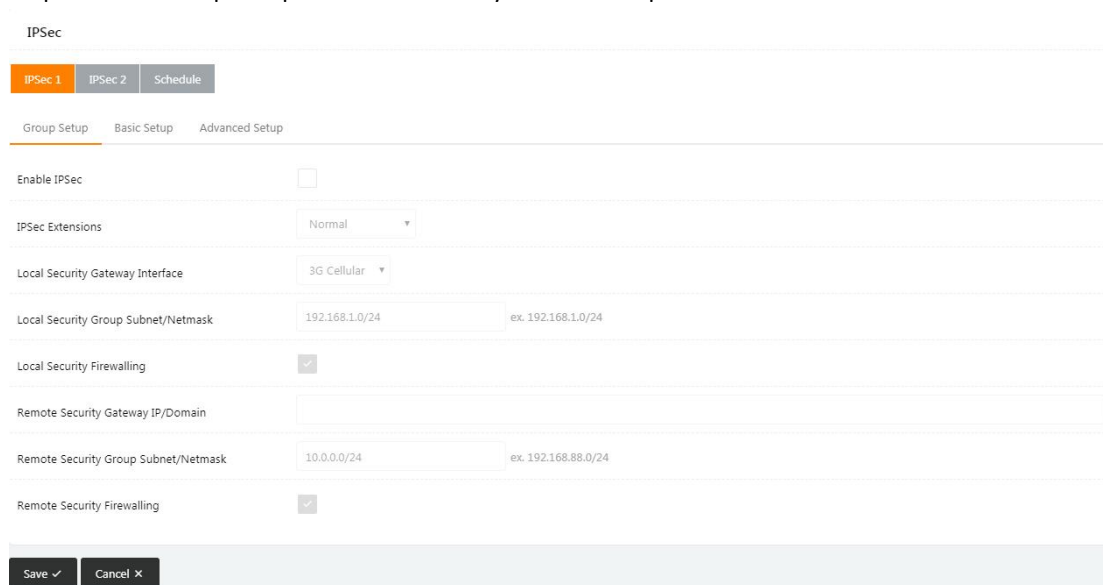


Table 3-21 "IPSec Group Setup" Instruction

Parameter	Instruction
IPSec Extensions	Support Standard IPSec, GRE over IPSec, L2TP over IPSec
Local Security Interface	Defined the IPSec security interface

Local Subnet/Mask	IPSec local subnet and mask
Local Firewall	Forwarding-firewalling for Local subnet
Remote IP/Domain	IPsec peer IP address/domain name
Remote Subnet/Mask	IPSec remote subnet and mask
Remote Firewall	Forwarding-firewalling for Remote subnet

Step 2 IPSec >Basic Setup to check or modify the relevant parameter

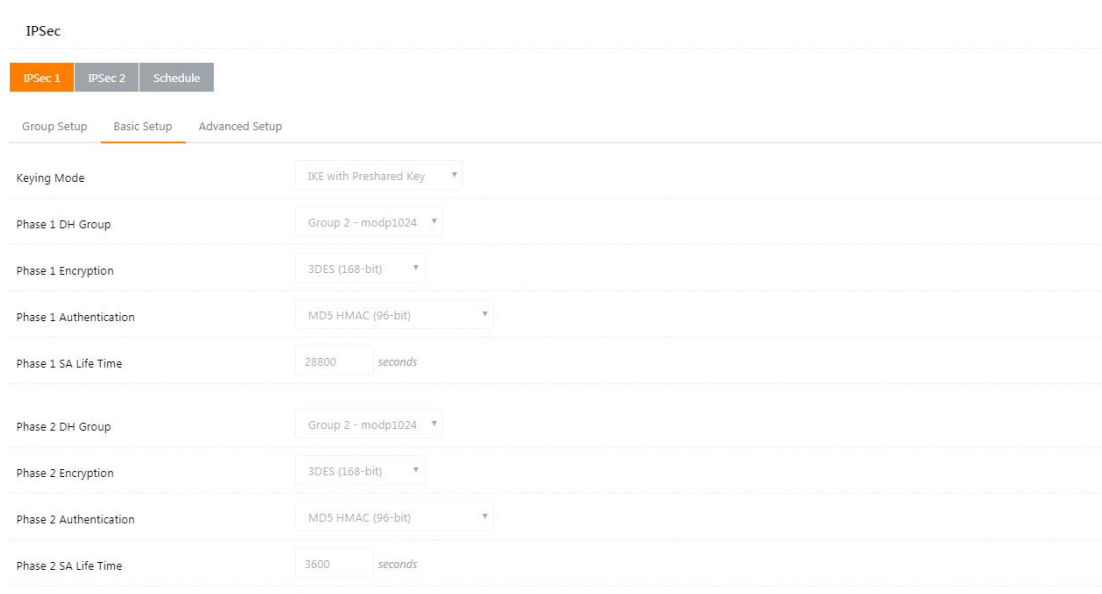


Table 3-22 “IPSec Basic Setup” Instruction

Parameter	Instruction
Keying Mode	IKE preshared key
Phase 1 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.
Phase 1 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase 1 Authentication	Support HASH MD5 and SHA
Phase 1 SA Life Time	IPSec Phase 1 SA lifetime
Phase 2 DH Group	Select Group1, Group2, Group5 from list. It must be matched to remote IPSec setting.

Phase 2 Encryption	Support 3DES, AES-128, AES-192, AES-256
Phase 2 Authentication	Support HASH MD5 and SHA
Phase 2 SA Life Time	IPSec Phase 2 SA lifetime
Preshared Key	Preshared Key

Step 3 IPSec >Advanced Setup to check or modify the relevant parameter

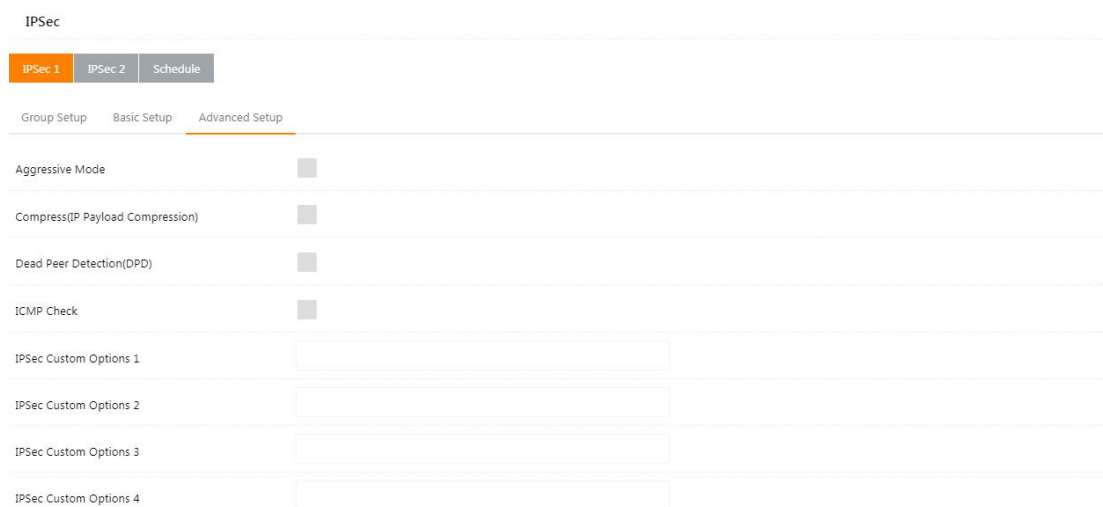


Table 3-23 “IPSec Advanced Setup” Instruction

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

Step 4 Please click “Save” to finish.

---End

2.8 Administration

2.8.1 Identification Setting

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

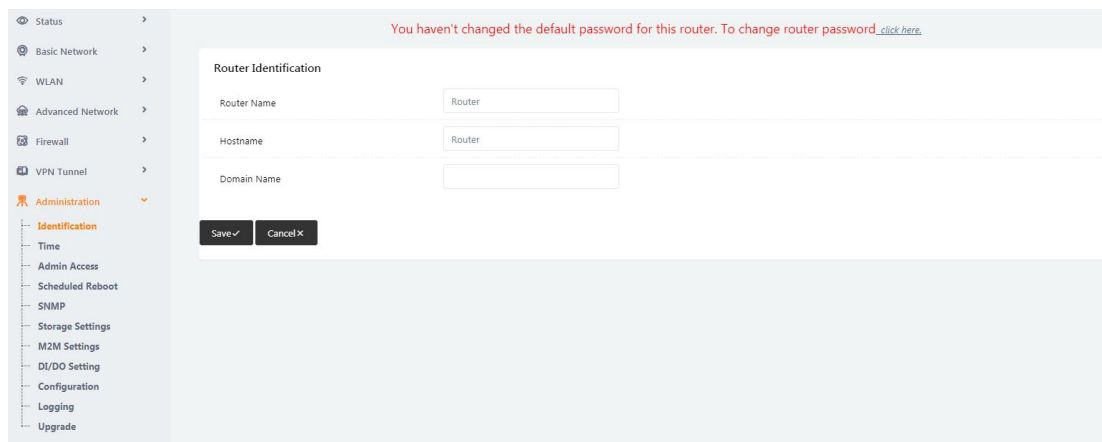


Figure 3-23 Router Identification GUI

Table 3-24 “Router Identification” Instruction

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

Step 2 Please click “Save” to finish

---End

2.8.2 Time Setting

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

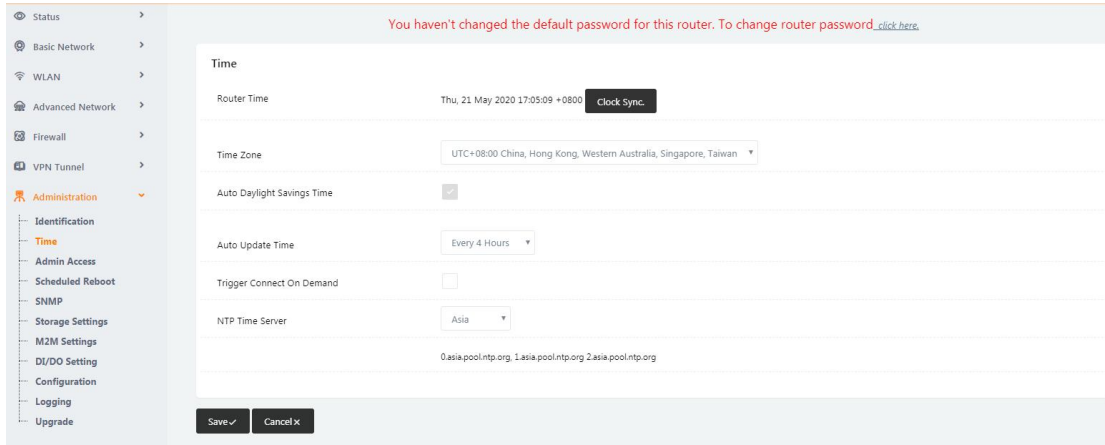


Figure 3-24 System Configuration GUI

CAUTION:

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

Step 2 Please click “Save” to finish.

----End

2.8.3 Admin Access Setting

Step 1 Please click “Administrator>Admin Access” 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.

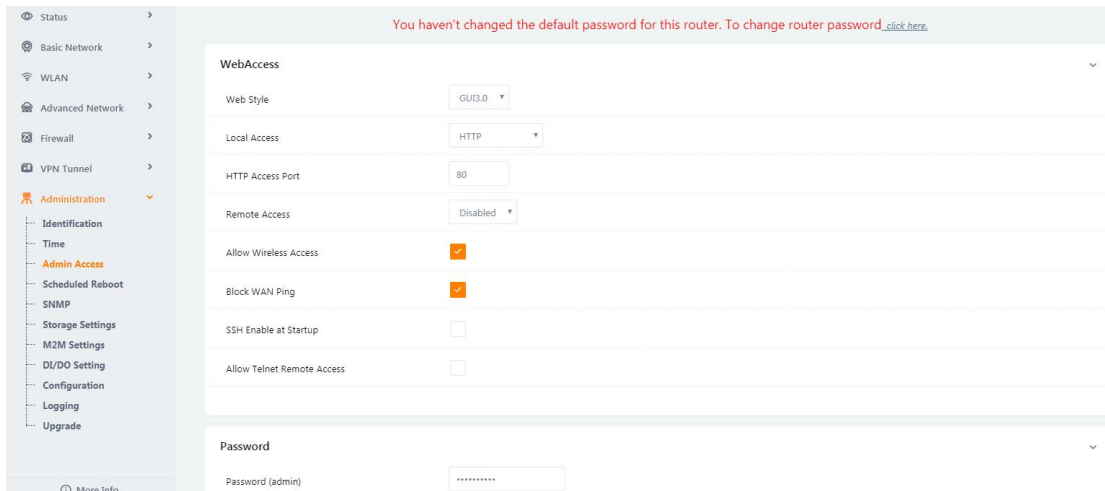


Figure 3-25 Admin Setting GUI

Step 2 Please click “Save” finish the setting

----End

2.8.4 Schedule Reboot Setting

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

parameter.

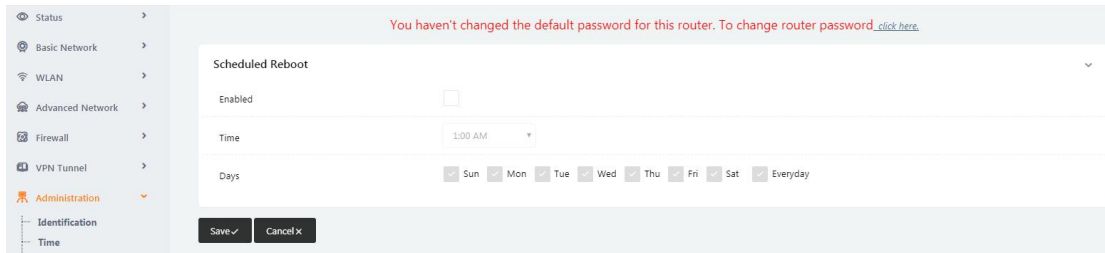


Figure 3-26 Scheduler Reboot Setting GUI

Step 2 Please click “Save” to finish the setting

----End

2.8.5 SNMP Setting

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

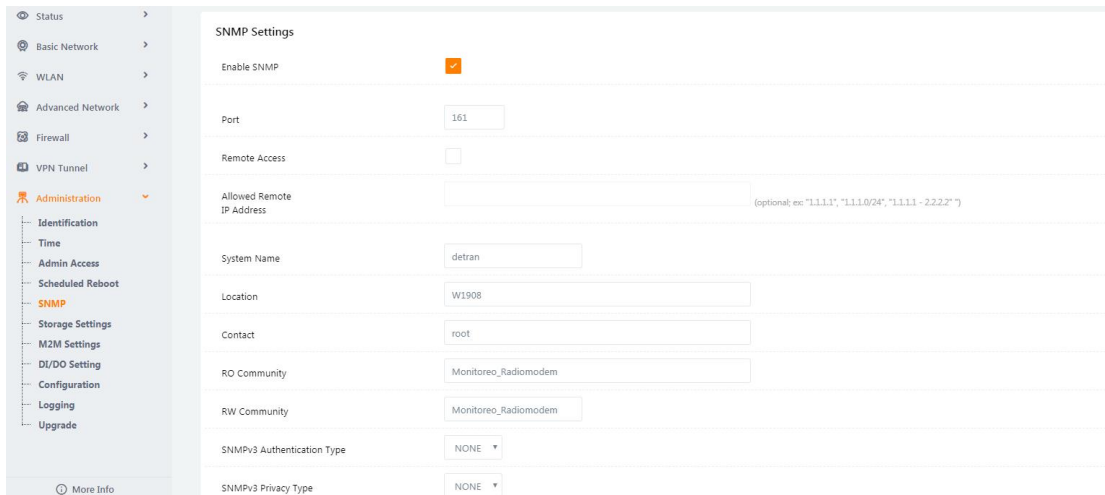


Figure 3-27 SNMP Setting GUI

Step 2 Please click “Save” to finish the setting

----End

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

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

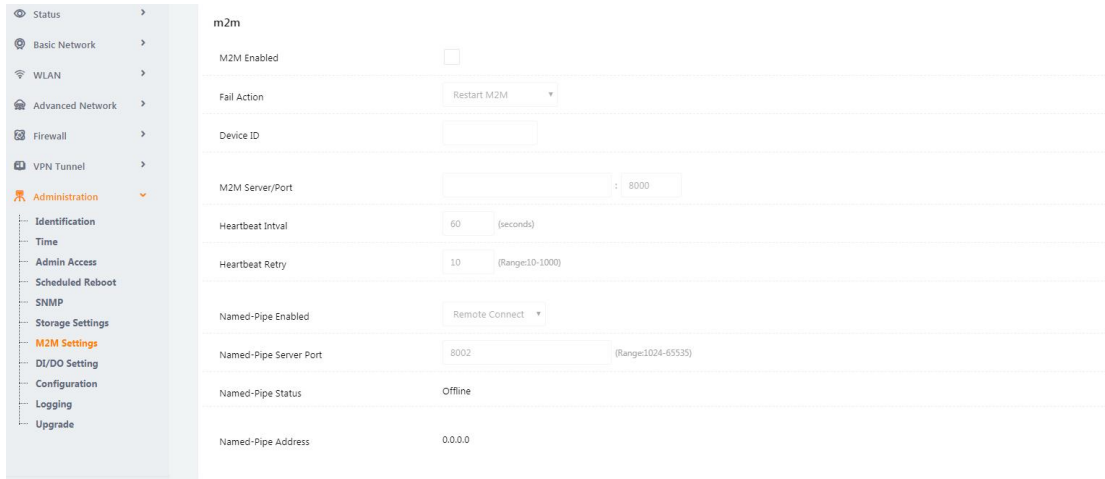


Figure 3-28 M2M Access Setting GUI

Step 2 Please click “Save” to finish the setting

----End

2.8.7 Configuration Setting

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

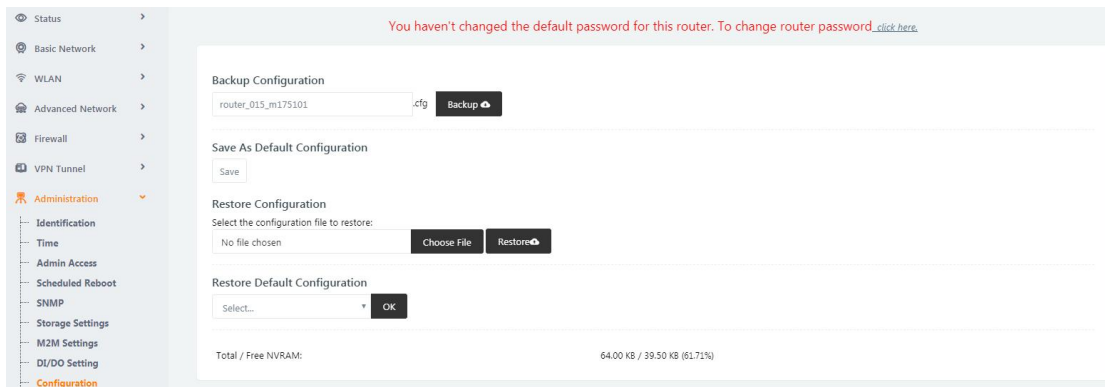


Figure 3-29 Backup and Restore Configuration GUI

CAUTION:

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

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

----End

2.8.8 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).

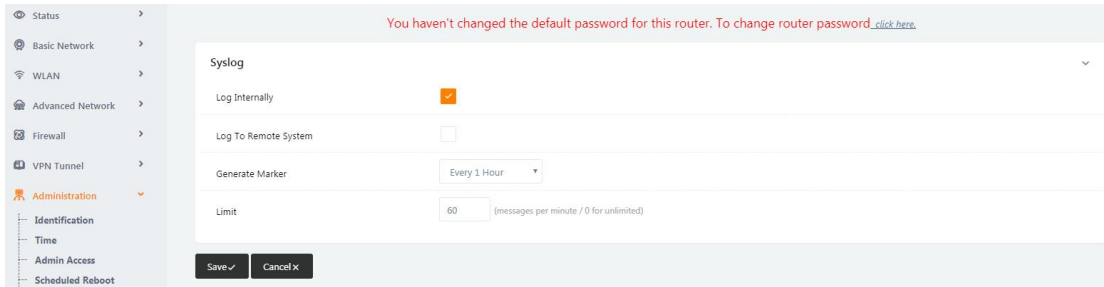


Figure 3-30 System log Setting GUI

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

----End

2.8.9 Firmware upgrade

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

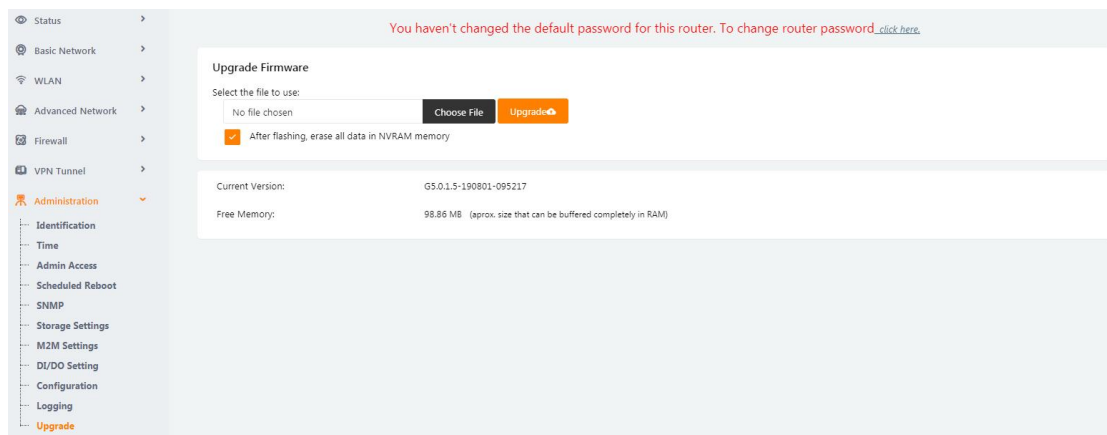


Figure 3-31 Firmware Upgrade GUI

CAUTION:

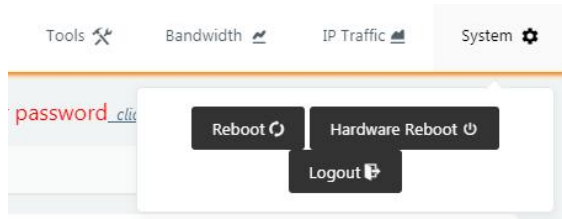
When upgrading, please don't cut off the power.

Step 2 After complete, you will see a button “Continue”, click it to continue.

----End

2.9 System Reboot

Step 1 Please click “System >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

2.10 Debugging Setting

2.10.1 Logs Setting

Step 1 Please click “Tools>Log” to check and modify relevant parameter.

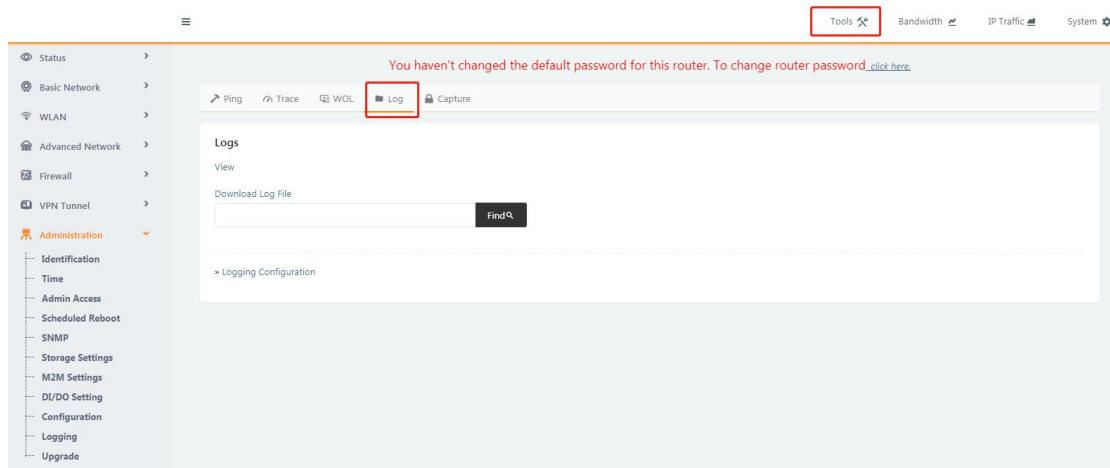


Figure 3-32 Logs GUI

----End

2.10.2 Ping Setting

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

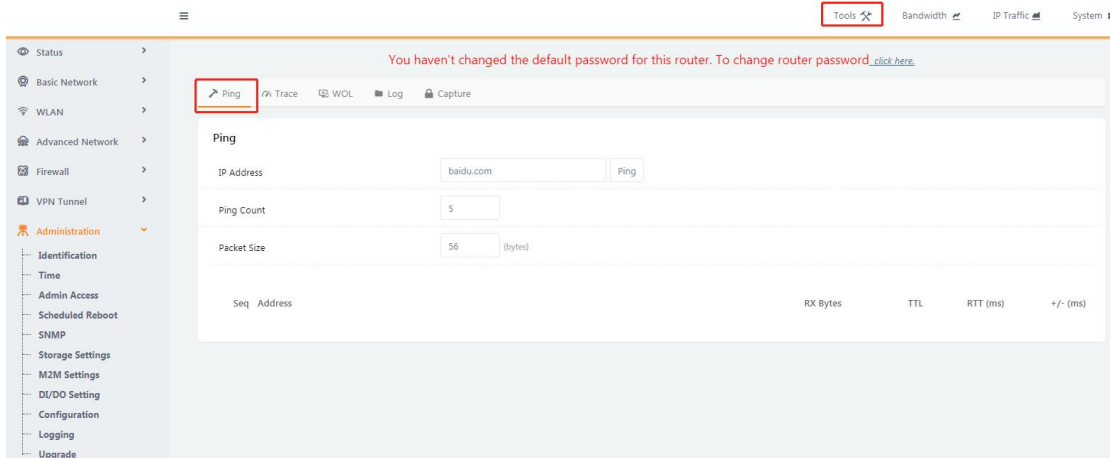


Figure 3-33 Ping GUI

----End

2.10.3 Trace Setting

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

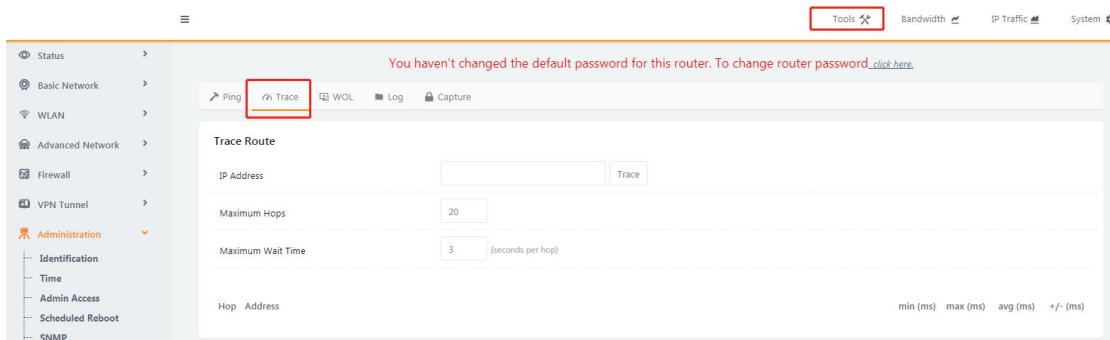


Figure 3-34 Trace GUI

----End

2.11 “Reset” Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way.

“Reset” button is near to Console port in G51 panel, This button can be used when the router is in use or when the router is turned on.

Press the “RST” button and keep more than 8 seconds till the NET light stopping blink.

The system will be reverted to factory.

Table 3-27 System Default Instruction

Parameter	Default setting

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

NOTE:

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

2.12 Appendix (For advanced optional features only)

2.12.1 GPS Setting

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

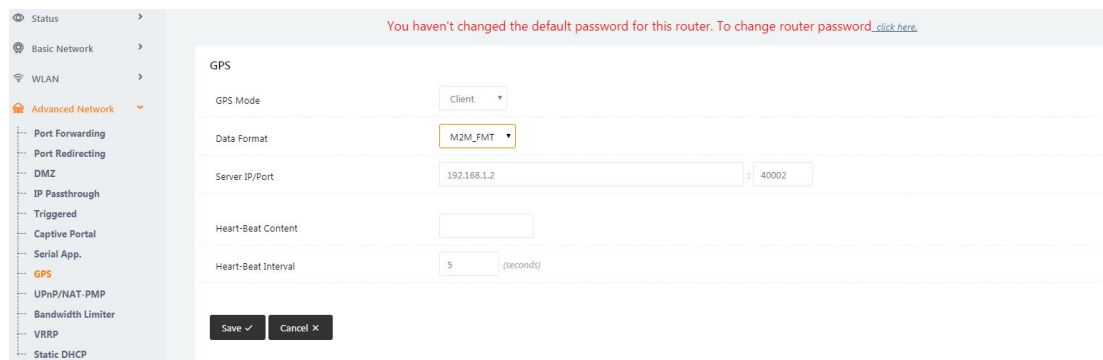


Figure 3-35 GPS Setting GUI

Table 3-28 “GPS” Instruction

Parameter	Instruction
GPS Mode	Enable/Diable
GPS Format	NMEA and M2M_FMT(HOMTECS)
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

NOTE:

M2M_FMT Format as below.

1. GPS data structure:

Router ID, gps_date, gps_time, gps_use, gps_latitude, gps_NS, gps_longitude, gps_EW, gps_speed, gps_degrees, gps_FS, gps_HDOP, gps_MSL

2. Example:

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

3. GPS data description

Field No.	Name	Format	Example	Description
1	Router ID	String	0001_R081850ac	0001 -customizable product ID. _R -router indicator. 081850ac -last 8digits of routers MAC address.
2	gps_date	yymmdd	150904	Date in year,month,day
3	gps_time	hhmmss.ss	043215.0	UTC Time, Time of position fix.
4	gps_use	numeric	06	Satellites Used, Range 0 to 12.
5	gps_latitude	ddmm.mm	2234.248130	Latitude, Degrees + minutes.
6	gps_NS	character	N	N/S Indicator,N=north or S=south.
7	gps_longitude	ddmm.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, unit is meter.
----	---------	---------	------	------------------------------

----End

2.12.2 Captive Portal Setting

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

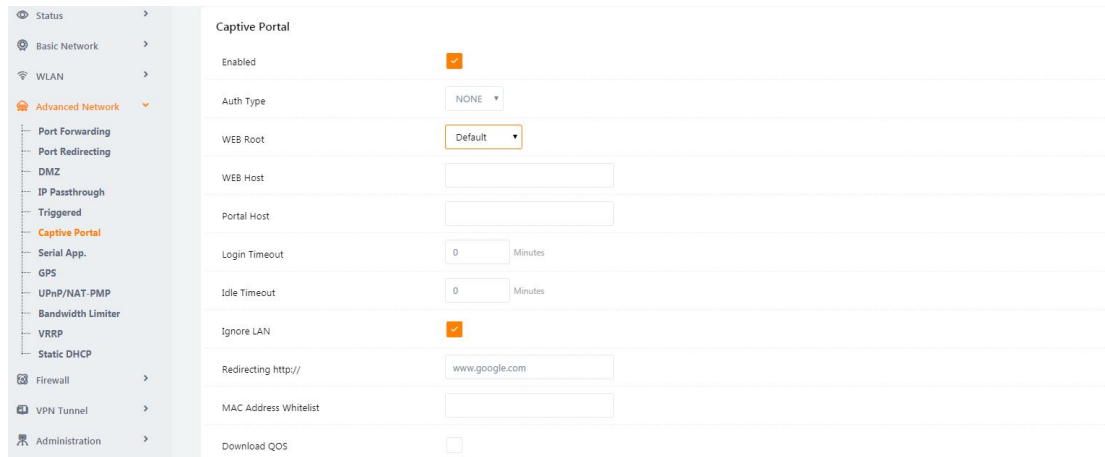


Figure 3-36 Captive Portal Setting GUI

Table 3-29 “Serial App” Instruction

Parameter	Instruction
Enable	Enable Captive portal feature.
Auth Type	Reserved.
Web Root	Choose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router’s Flash. Ex-storage: Captive portal file is in extended storage such as SD card.
Web Host	Configure domain name for the captive portal access. For example, Configure as www.homtecsm2m.com, we might directly access to captive portal page in the website as www.homtecsm2m.com
Portal Host	Reserved.
Logged Timeout	Maximum time user has connectivity. User need to re-login Captive Portal page after defined time.
Idle Timeout	Maximum time user has connectivity if no network activity from Wi-Fi User. If User need to re-login Captive page to surf internet.
Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.

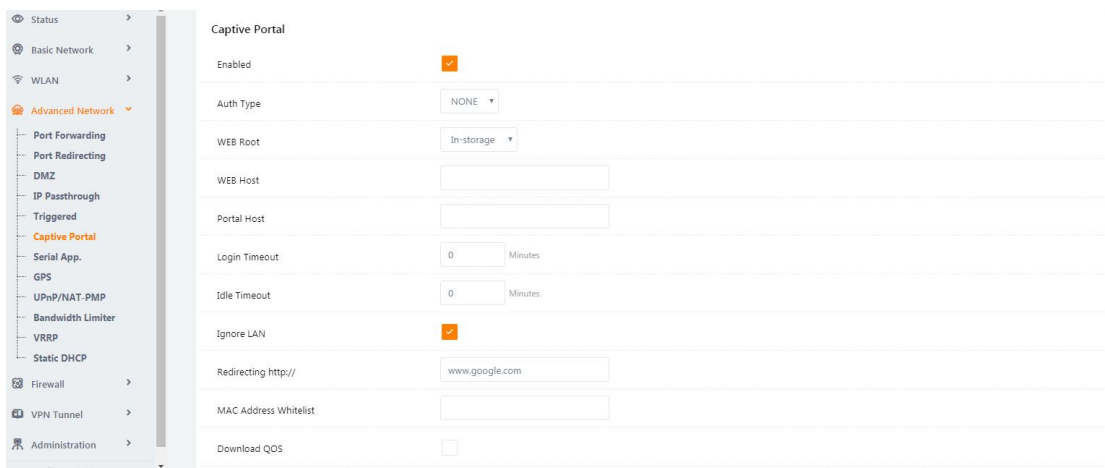
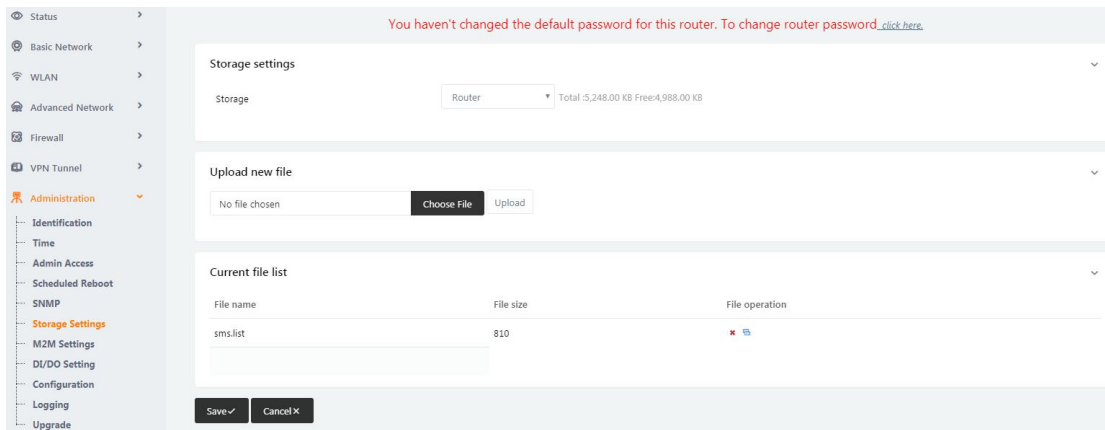
Redirecting	Router will redirect to the defined link after accepting the terms and conditions on the Captive Portal page
MAC Whitelist	No captive portal page for Wi-Fi device.
Download QoS	Enable to apply the Download and Upload per user limits.
Upload QoS	Maximum download speed available to each user.

NOTE:

1) Upload Portal file and Splash.html by local

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

Furthermore, also might upload splash with images together.



```

<!-- <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

2.12.3 VLAN

Virtual local area network (VLAN) is a set of logical devices and users that are not limited by physical location, and can be organized according to factors such as functionality, and application, as if they were in the same network segment, Thereby getting the name of the department, virtual local area network. A VLAN is a new technology that works on Layer 2 and Layer 3 of the OSI reference model, a VLAN is a broadcast domain, and the communication between VLANs is done through a Layer 3 router. Compared with the traditional LAN technology, the VLAN technology is more flexible, it has the following advantages: the movement of network devices, the management cost of adding and modifying is reduced; the broadcast activity can be controlled, and the security of the network can be improved.

Select “Base Network > VLAN” in the navigation bar. In the open page, you can modify the relevant parameters to configure the dynamic domain name. As shown:

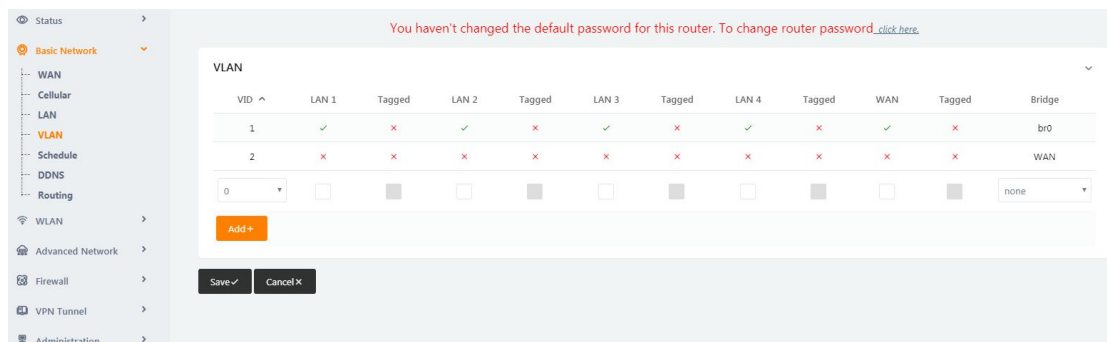


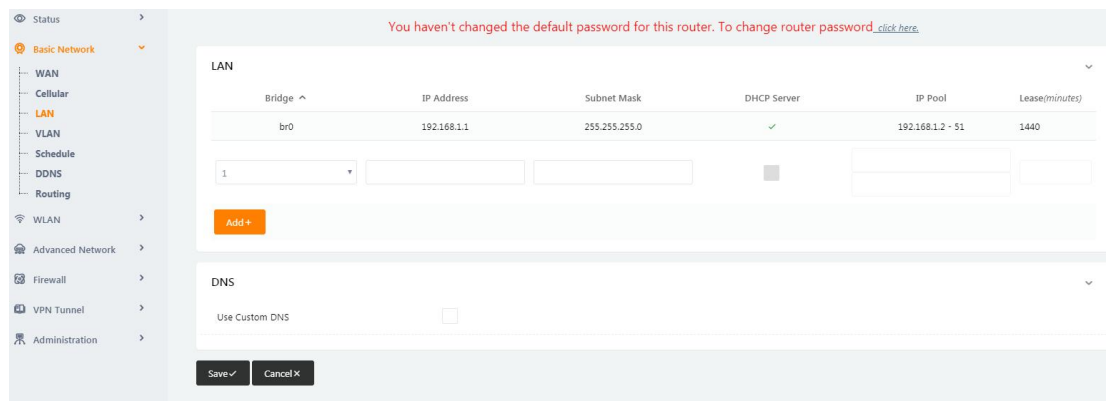
Table 3-30 “VLAN” Instruction

Parameter	Instruction
-----------	-------------

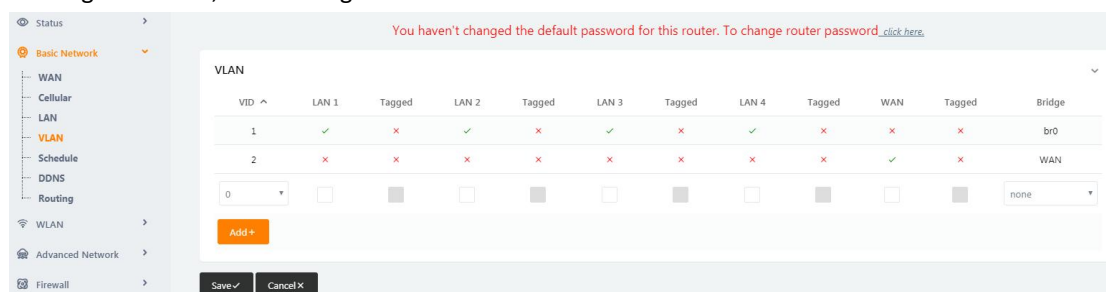
VID	Each VLAN switch port needs to be bound to a VID; (VID range: 0 - 15).
LAN1/WAN, LAN2, LAN3	Interface, 3*LAN, or 2*LAN + 1*WAN
Tag	Trunk port (equivalent to checking the tagged-tag check) the data frame received from this port is typed by the tag, and the data frame sent by the tag, from this type of port requires tag (regardless of the default VLAN).

Example:

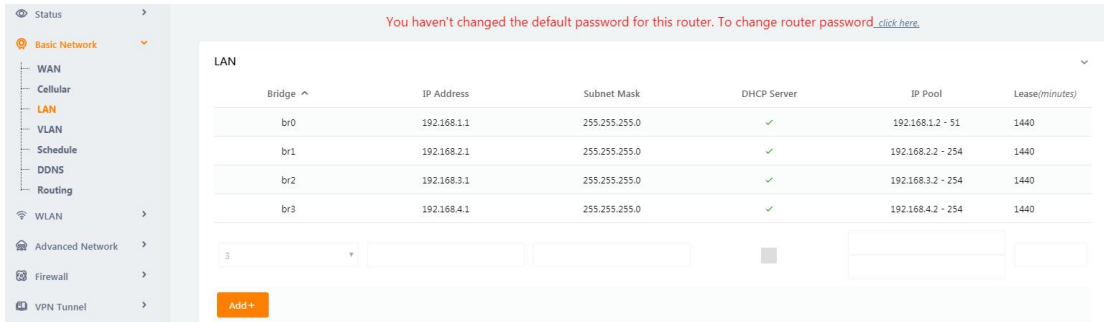
1. Each VLAN switch port needs to be bound to a VID; (VID range: 0 - 15).
2. Each VLAN switch port is in one of the following three categories: access, trunk.
 - 2.1. Access port (equal to or not checked): The data frame received from such port is not tag, and the data frame sent from such port is not tag;
 - 2.2. Trunk port (equal to the check-tagged-tag): The data frame received from such a port is tag, and the data frame sent from such a port needs to be tag (the default VLAN is not considered);
3. LAN port default is br0192.168.1.1 segment, can add 4 address segments on different interfaces.



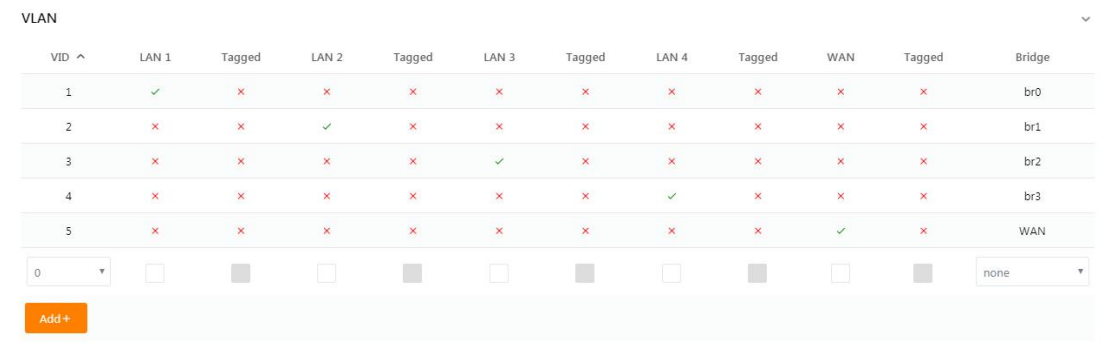
4. Set up 4 LANs, one WAN with the following diagram, assign the WAN to the VID 2, that is to bridge the WAN, and to assign the other interfaces to the br0 interface.



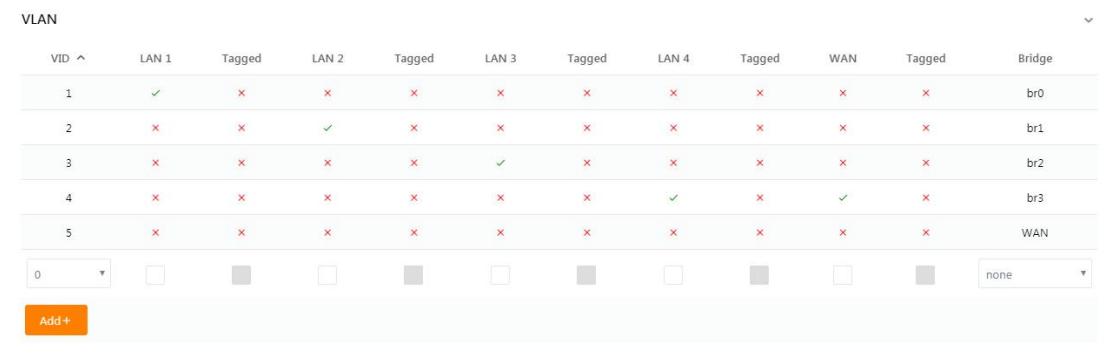
5. With the increase of br1, br2, br3 in LAN, VLAN can be divided into four LAN ports with different IP segments independently for WAN ports, as shown in the following figure.



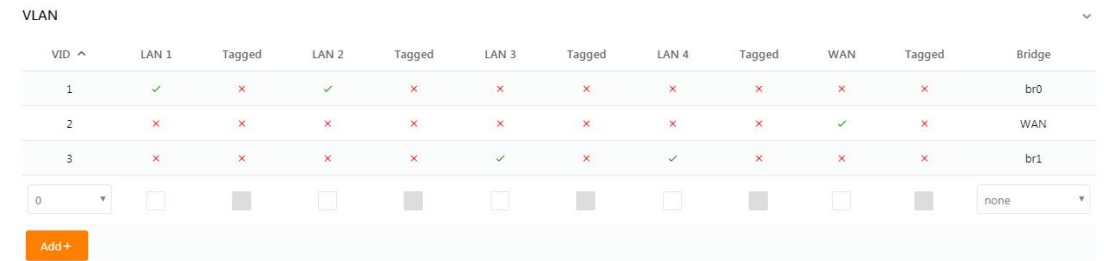
6. Four LAN ports and WAN ports are configured independently.



7. WAN uses the configuration as one of the LAN ports on the same network segment.



8. The VLAN divides a group of LAN1 and LAN2, a group of LAN3 and LAN4, and the independent WAN port is shown in the following figure. One IP segment of LAN1 and LAN2, one IP segment of LAN3 and LAN4, and the WAN port is configured independently.



9. The WAN port and one of the LAN ports are configured with the IP section.

VLAN

VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	br0
2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	WAN
3	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	br2
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none

Add +

10.VLAN tagging trunk requires setting the accessed device to the same VID of 1.

VLAN

VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	br0
2	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	WAN
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none

Add +

---End

2.12.4 Schedule

Select “Basic Network > Schedule” in the navigation bar. On the open page, you can configure link scheduling WAN and 3G/4G backup or mutual standby mode.

NOTE:

The version of the 3G/ 4G and the wired network backup is only available for this feature, depending on the actual product version.

Features:

- 1, The ICMP link detection determines whether the link is normal through the IP address, and if the PING checks the IP block abnormal trigger switching mechanism.
- 2, The link scheduling strategy can be selected in BACKUP mode: link 1 fills in "WAN", WAN network is dominant, link 2 is filled with "modem", link 1 is filled in "modem", 4G network is dominant, link 2 is filled in "WAN", link 1 is standby, in BACKUP mode, link 1 is dominant when link 1 is online, link 1 is switched to link 2 when link 1 fails after ICMP detection. Link 1 is switched back to link 1 after ICMP detection recovery takes effect.
- 3, The link scheduling policy is an optional FAILOVER mode, which refers to the backup mode of the link 1 and the link 2; when the link 1 is on-line, the link 1 is the main link; after the link 1 fails, the link 1 is switched to the link 2 through the ICMP detection, and the link 2 is the main link; and when the link 1 is in effect, the link 2 is still the primary link and does not switch back link 3.to the link 1; after the link 2 fails, the ICMP detection is switched to the link 1, where the link 1 is the primary link.

4, WAN port supports DHCP automatic acquisition and static address, PPPoE fixed network access, WAN default shutdown needs to be enabled.

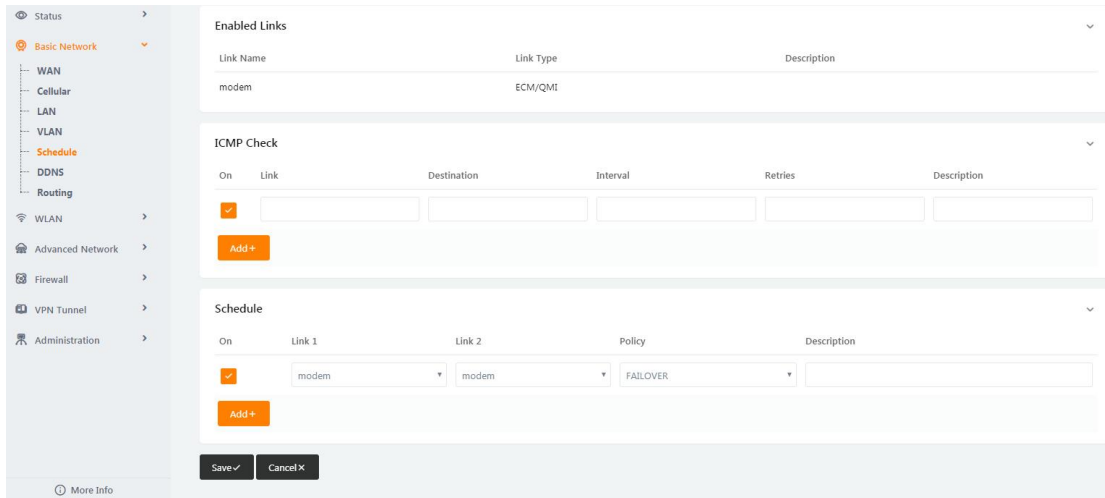


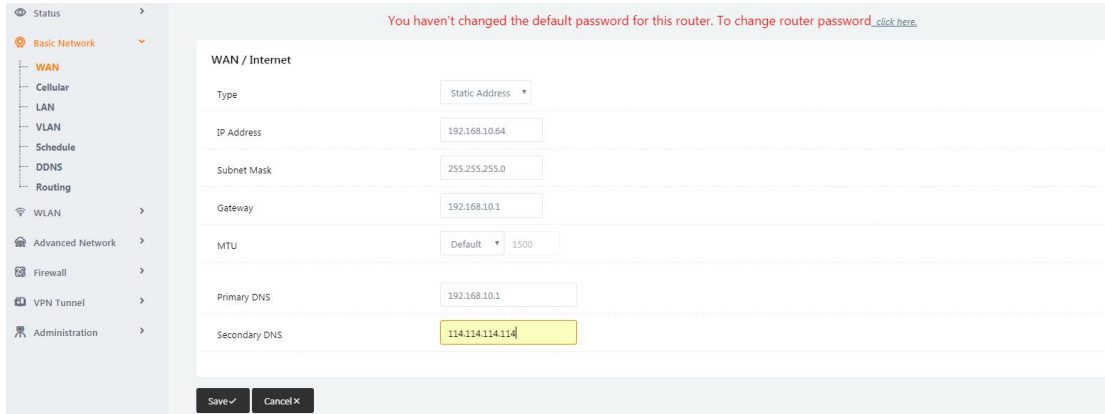
Table 3-30 "Schedule" Instruction

Parameter	Instruction
ICMP Link Detection-Link	Link,"modem, wan"
ICMP Link Detection-Destination Address	The IP address or domain name that the link needs to detect, whether the host is reachable and whether the route is available
ICMP Link Detection-Interval	The time interval for detecting the IP address
ICMP Link Detection-retry	Retry the secondary consecutive failure after the failure has failed to set the number of setting times.
Link scheduling-Link 1	Link,"modem, wan"
Link scheduling-Link 2	Link,"modem, wan"
Link scheduling-Policy	Link scheduling policy can be selected in BACKUP mode, "Link 1 is WAN, Link 2 is 4G" or "Link 1 is 4G, Link 2 is WAN" these two modes. Or in FAILOVER mode, refers to do backup between the link 1 and the link 2

Example:

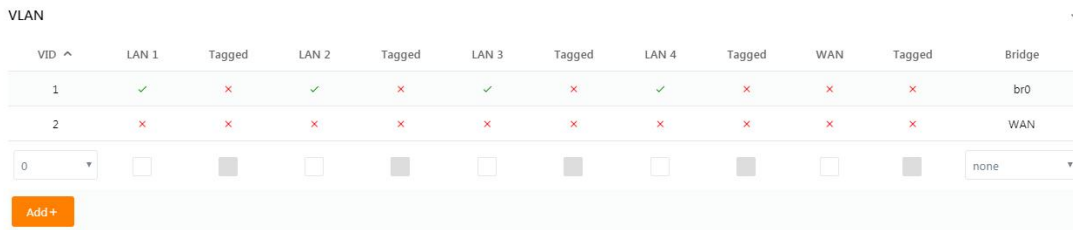
Step 1:

Select "Basic Network > WAN" in the navigation bar. In the open page, the drop-down box selects the static address, configure the parameters of the static address, and click on the save settings; as shown in the following figure (note: the parameter configuration is an example that actually needs to be configured according to the field situation)

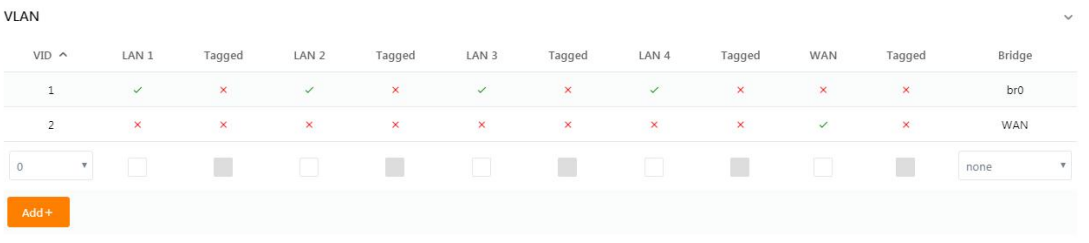


Step 2:

Select "Basic Network > VLAN" in the navigation bar. On the open page, remove the WAN, click OK that checks VID1, as shown in the following figure:

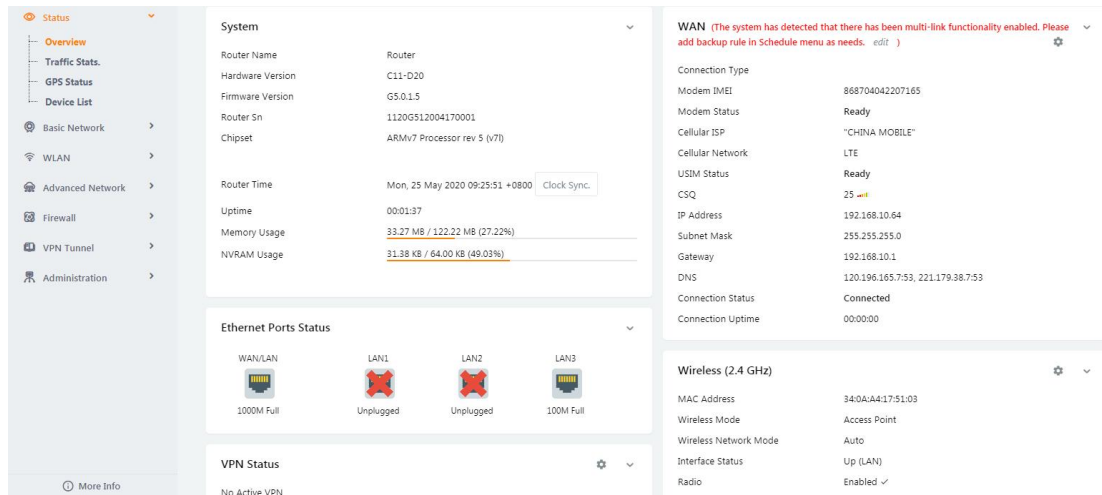


In the page of the VLAN, add the VID2, check the WAN, click OK, and click Save Settings after the setting is complete, as shown in the following figure:



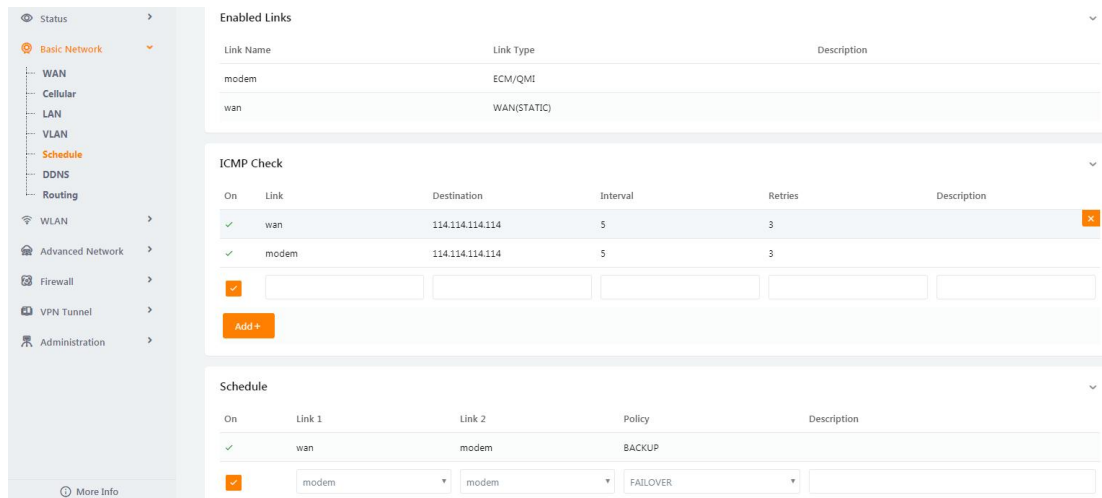
Step 3:

Select the "Status> Overview" in the navigation bar. In the open page, view the WAN network status and access the external network, as shown in the figure:



Step 4:

Select “Basic Network> Schedule”, configure the ICMP link detection item and the link scheduling item (note: link 1 is WAN, link 2 is modem), and the policy is backup; configure to complete the click save and wait for the device to restart.

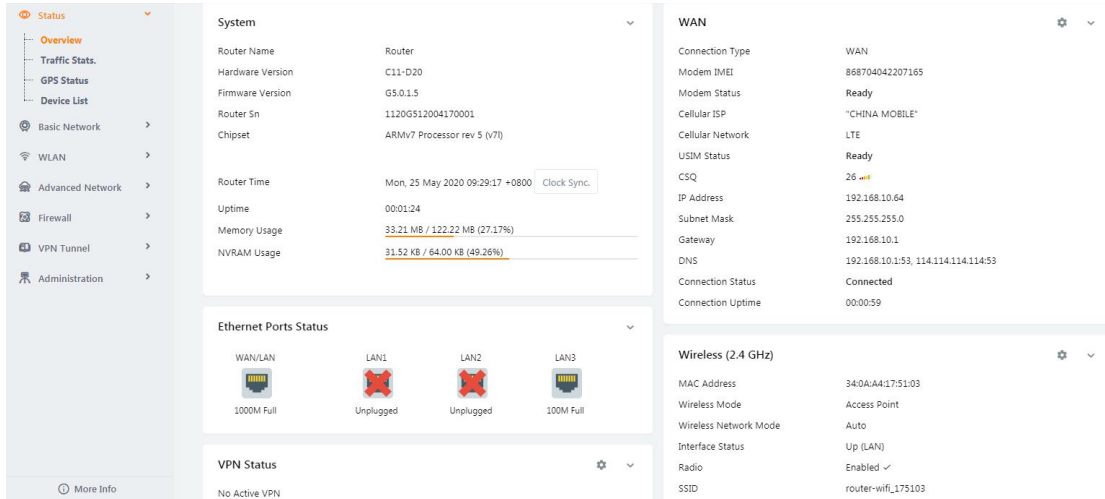


NOTE:

WAN prefer, Modem backup

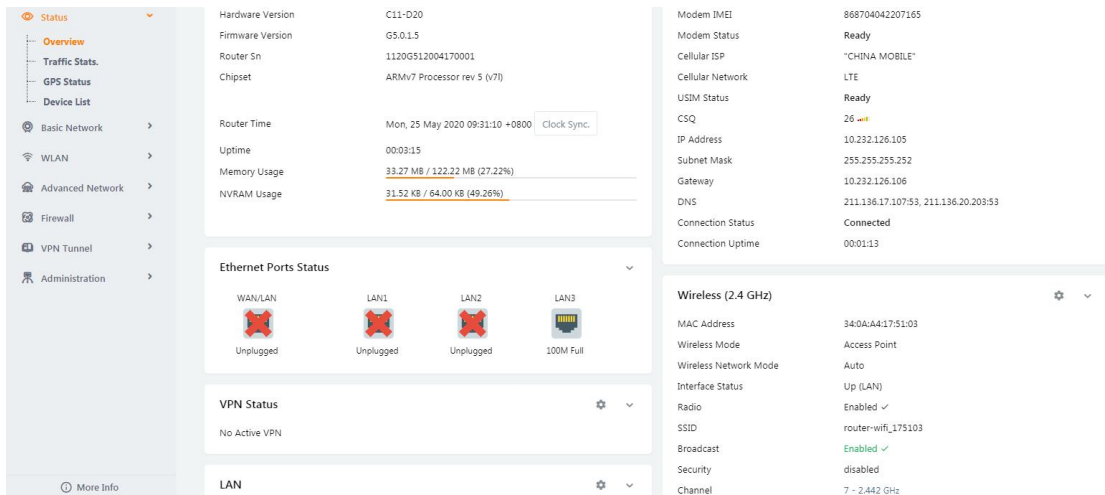
Step 5:

Click “Status> Overview” to view the WAN connection status (the WAN is the main), as shown in the following figure:



Step 6:

Disconnect the network cable from the WAN port and look again at the connection status of the WAN (this is the line on the card), as shown in the following figure:



Step 7:

When you insert the network cable into the router's WAN port again, check the connection status of the WAN (at this time static Internet access), as shown in the following figure:

