Comset CM550W-POE 5G Router
User Guide

WARNING: Keep at least a 20cm distance between the user’s body and the modem/router device.

Address： *37/ 125 Highbury Road, Burwood VIC 3125, Australia*

Web： *http://www.comset.com.au*

Phone: *+61 3 9001 9720*

Fax: *+61 3 9888 7100*

Contents

1 Hardware Installation

The images below might be slightly different from the actual product, but the specifications are the same.

1.1 Panel

Table 1-1 CM550W-POE Interface

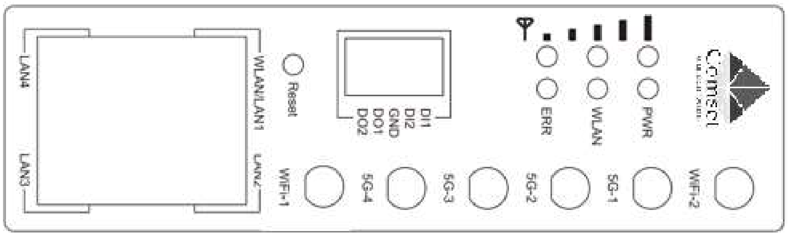
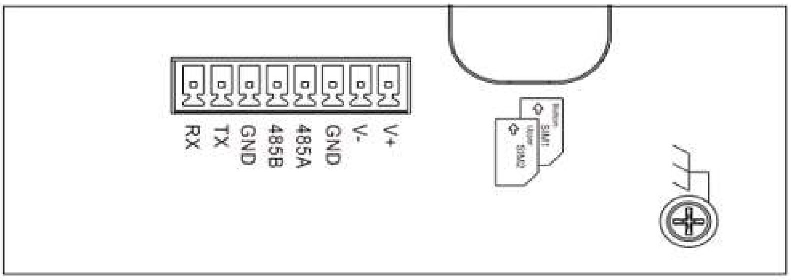
COMSET	CM550W series
Front	
Side	

Table 1-2 Router Interface

Port	Instructions	Remark
USIM	Standard size SIM Slot, supports 1.8/3V/5V automatic detection.	
Main	5G-1~5G-4 antennas, SMA connectors, 50Ω.	
GPS	5G-4 can be used as a GPS antenna, SMA connector, 50Ω.	Optional

Port	Instructions	Remark
Wi-Fi	2.4GHz Wi-Fi, 5GHz Wi-Fi. Dual-band antennas, SMA connectors.	
LAN0~LAN4	10/100/1000Base-TX，MDI/MDIX self-adaption, LAN1 & LAN2 for PoE and PoE+.	
Reset	Reset button. Press and hold for at least 5 seconds.	
PWR	Power connector.	44～57VDC for PoE
IO Interface	5xPins. 2 x DI, 2 x DO and GND.	
Terminal Block	1 x RS232,1 x RS485, 1 x DC Power.	

1.2 LED Status

Table 1-3 Router LED indicator Status

silk-screen	status		Description
Signal	Signal	Solid light	LED1 indicates signal is weak (CSQ0~10) LED2 indicates signal is good (CSQ11~19) LED3 indicates signal is strong (CSQ20~31)
	Signal 1	Blinking	Dialing.
		Solid light	Online.
PWR	Solid light		System power operation.
WLAN	Solid light		WLAN enabled, but no data communication.
	Blinking rapidly		Data is being transmitted.
	Light off		WLAN disabled.
ERR	Light off		System in operation and 5G/4G is online.
	Solid light (Red)		System fail indicator. This indicates failure with the SIM card and/or the module.
LAN	Green	Solid light	Connected.
	Green	Blinking	Data is being transmitted.

silk-screen	status		Description
	Green	Light off	Disconnected.

1.3 Dimensions

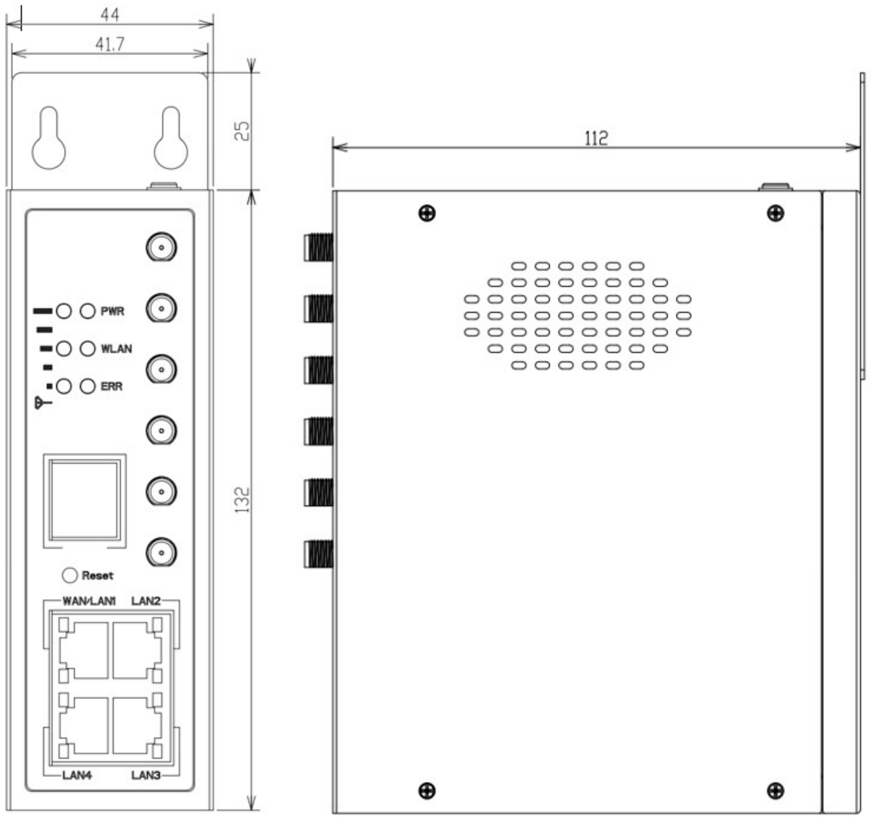
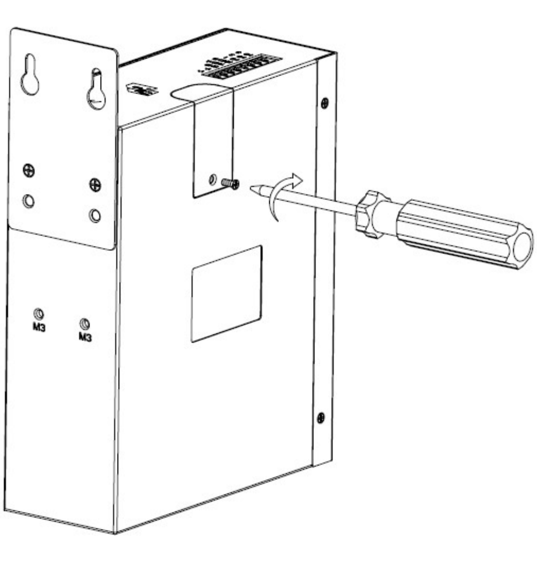
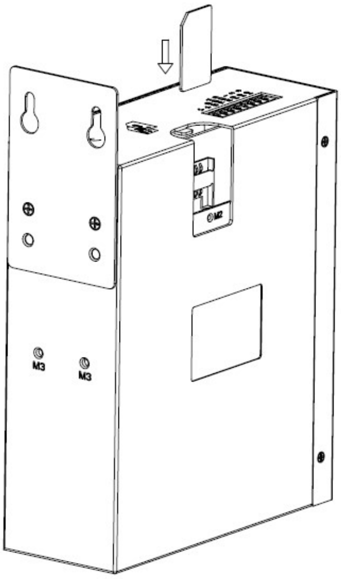


Figure 1-1 CM550W-POE Router Dimensions

1.4 Powering up the CM550W-POE Router

1.4.1 SIM/UIM card installation

Please insert the SIM card(s) prior to configuring the router. Use a standard size SIM card.

CAUTION

Before connecting any cables, please disconnect the power source.

1.4.2 Ethernet Cable Connection

Use an Ethernet cable to connect the LAN port of the 5G Router to the LAN port of your PC or laptop computer.

1.4.3 5G and Wi-Fi Antenna Plug

Connect the four magnetic base 5G antennas to antenna sockets 5G-1 to 5G-4, and the two paddle shape Wi-Fi antennas to the Wi-Fi antenna sockets.

NOTE

The Wi-Fi antennas support dual-band Wi-Fi 2.4GHz and 5GHz bands.

1.4.6 Power Supply

The CM550W-POE router supports a wide range of DC voltage between 44VDC and 57VDC.

1.4.7 Review

After inserting the SIM/UIM card(s) and connecting the Ethernet cable and antennas, please connect the power adaptor or power cable.

CAUTION

Please connect the antennas prior to powering up the router, otherwise you may get a poor signal due to a mismatching impedance.

Note:

Step 1 Check the antennas' connection.

Step 2 Check the SIM/UIM card is inserted.

Step 3 Power up the CM550W-POE Router.

2 Router Configuration

The CM550W-POE Router can be configured via a web interface using a web browser such as Internet Explorer, Firefox, or Google Chrome.

2.1 Configuration from a local network

To configure the CM550W-POE, please connect an Ethernet cable between the router and your PC computer. The IP address on your PC can be a static IP address, or you can select DHCP so that your computer can automatically obtain a Dynamic IP address. The default IP address of the router is 192.168.1.1. The subnet mask is 255.255.255.0. Please follow the instructions below:

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

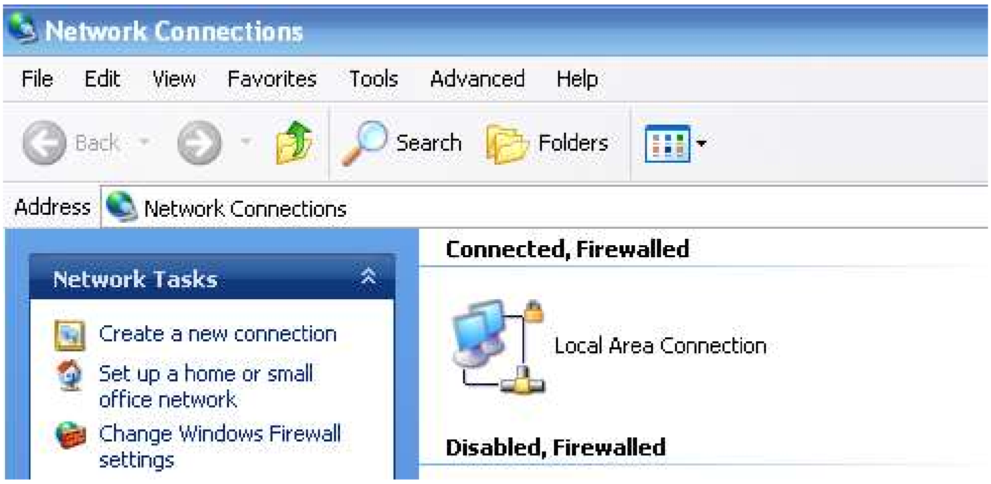
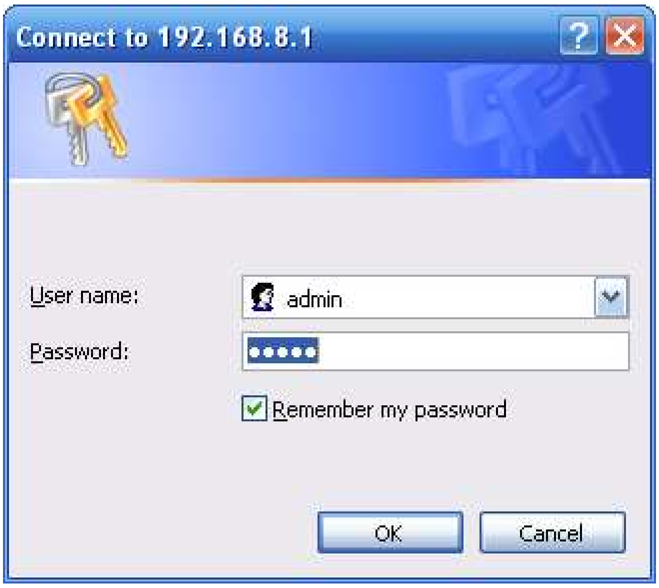


Figure 2-1 Network Connection

Step 2 Select "Obtain an IP address automatically" or set up a fixed IP address in the range 192.168.1.xxx (xxx can be any number between 2～254)

Step 3 Run Internet Explorer, or any other web browser, and enter 192.168.1.1 in the address bar and press "enter".

The default username is admin, and the default password is admin.



Connect to 192.168.8.1

User name: admin

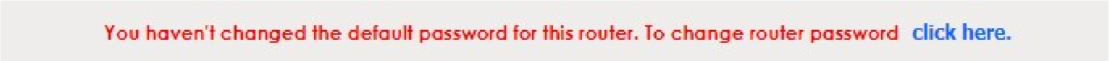
Password: ●●●●●

☑ Remember my password

Figure 2-2 User Identify Interface

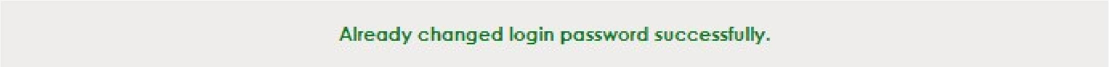
2.2 Status

After you login, a note highlighted in red will prompt you to change the router password. Follow the prompts and change the login password.



You haven't changed the default password for this router. To change router password click here.

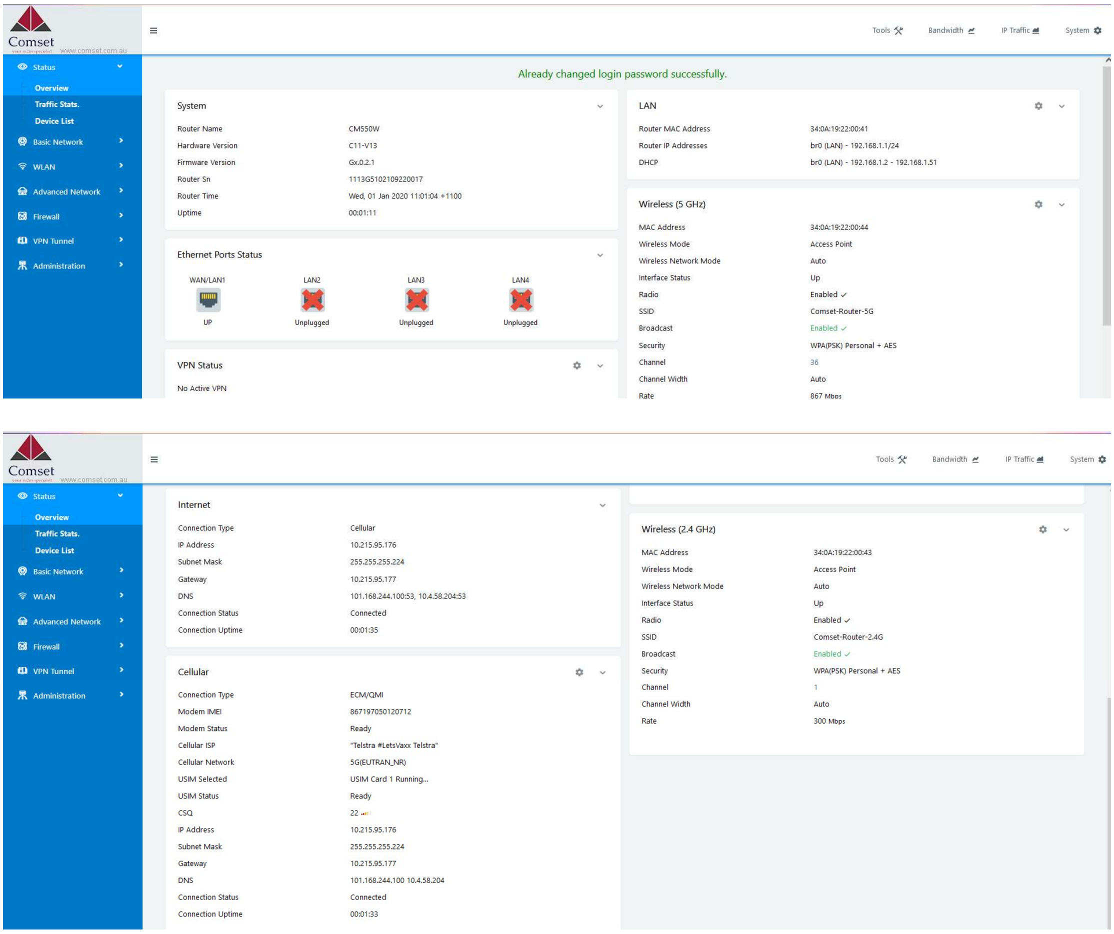
The router will reboot, and the GUI will display “already changed login password successfully”.



Already changed login password successfully.

2.2.1 Overview

The overview page displays router system information, such as Ethernet ports status, VPN connection status, LAN information, 5G connection and WLAN information:



Already changed login password successfully.

System

Router Name	CM550W
Hardware Version	C11-V13
Firmware Version	Gx.0.2.1
Router Sn	1113G5102109220017
Router Time	Wed, 01 Jan 2020 11:01:04 +1100
Uptime	00:01:11

Ethernet Ports Status

WAN/LAN1	LAN2	LAN3	LAN4
UP	Unplugged	Unplugged	Unplugged

VPN Status

No Active VPN

LAN

Router MAC Address	34:0A:19:22:00:41
Router IP Addresses	br0 (LAN) - 192.168.1.1/24
DHCP	br0 (LAN) - 192.168.1.2 - 192.168.1.51

Wireless (5 GHz)

MAC Address	34:0A:19:22:00:44
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up
Radio	Enabled ✓
SSID	Comset-Router-5G
Broadcast	Enabled ✓
Security	WPA(PSK) Personal + AES
Channel	36
Channel Width	Auto
Rate	867 Mbps

Internet

Connection Type	Cellular
IP Address	10.215.95.176
Subnet Mask	255.255.255.224
Gateway	10.215.95.177
DNS	101.168.244.100:53, 10.4.58.204:53
Connection Status	Connected
Connection Uptime	00:01:35

Cellular

Connection Type	ECM/QMI
Modem IMEI	867197050120712
Modem Status	Ready
Cellular ISP	"Telstra #LetsVaxx Telstra"
Cellular Network	5G(EUTRAN_NR)
USIM Selected	USIM Card 1 Running...
USIM Status	Ready
CSQ	22
IP Address	10.215.95.176
Subnet Mask	255.255.255.224
Gateway	10.215.95.177
DNS	101.168.244.100 10.4.58.204
Connection Status	Connected
Connection Uptime	00:01:33

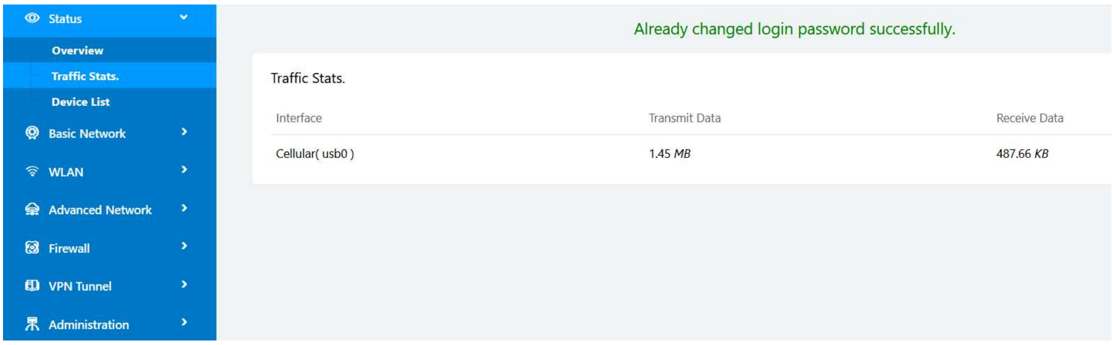
Wireless (2.4 GHz)

MAC Address	34:0A:19:22:00:43
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up
Radio	Enabled ✓
SSID	Comset-Router-2.4G
Broadcast	Enabled ✓
Security	WPA(PSK) Personal + AES
Channel	1
Channel Width	Auto
Rate	300 Mbps

Figure 2-3 Router Status GUI

2.2.2 Traffic Statistics.

Go to Status->Traffic Stats. Here you can check Cellular/WAN traffic in real-time.



Already changed login password successfully.

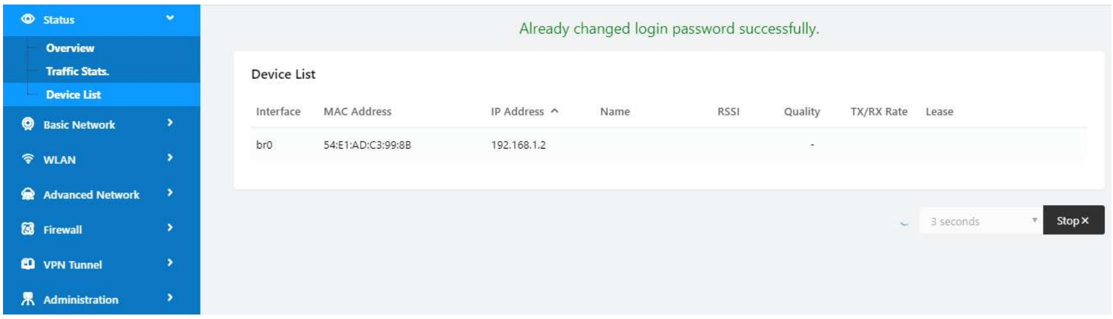
Traffic Stats.

Interface	Transmit Data	Receive Data
Cellular(usb0)	1.45 *MB*	487.66 *KB*

Figure 2-4 Traffic Stats. GUI

2.2.3 Device List

Go to Status > Device List. Here you can check the connected devices:



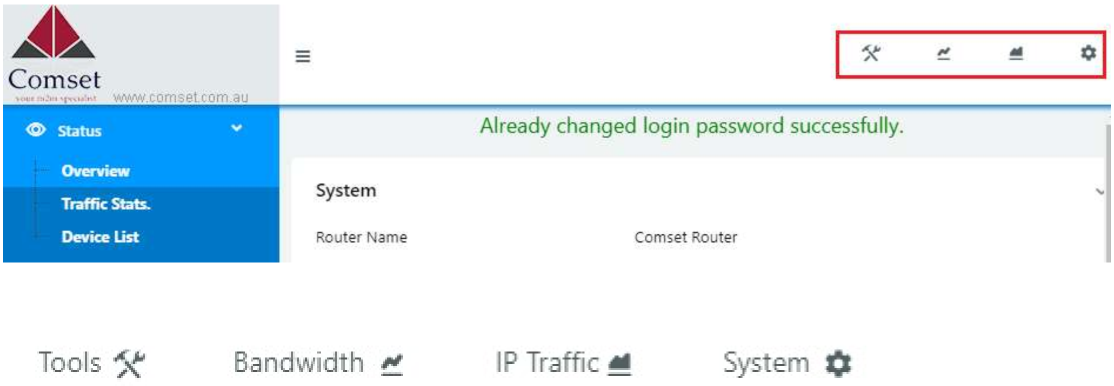
Already changed login password successfully.

Device List

Interface	MAC Address	IP Address	Name	RSSI	Quality	TX/RX Rate	Lease
br0	54:E1:AD:C3:99:8B	192.168.1.2			-		

Figure 2-5 Device List GUI

2.3 Tools Column



Already changed login password successfully.

System

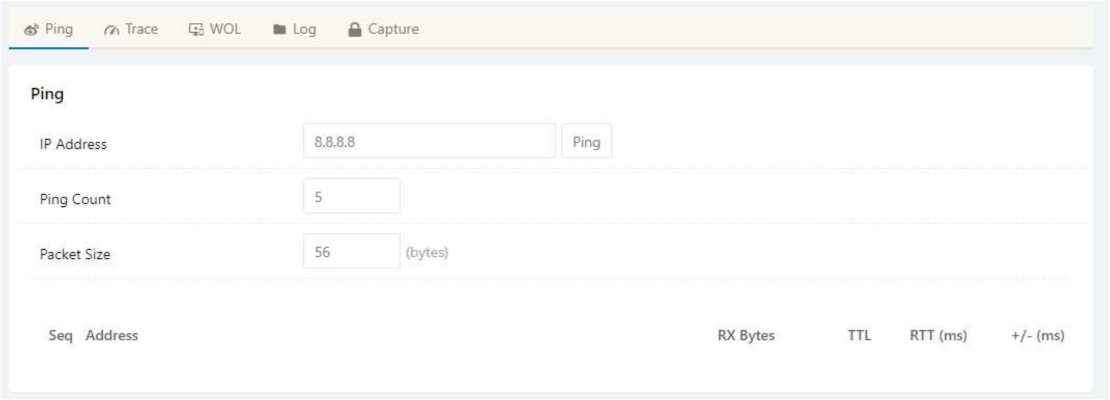
Router Name Comset Router

Figure 2-6 Tool Column GUI

2.3.2 Tools

2.3.2.1 Ping

Click on Tools > Ping. This is used to test the reachability of a host on an Internet IP network and to measure the round-trip time for messages sent from the originating host to a destination server.



Ping

IP Address: 8.8.8.8 Ping

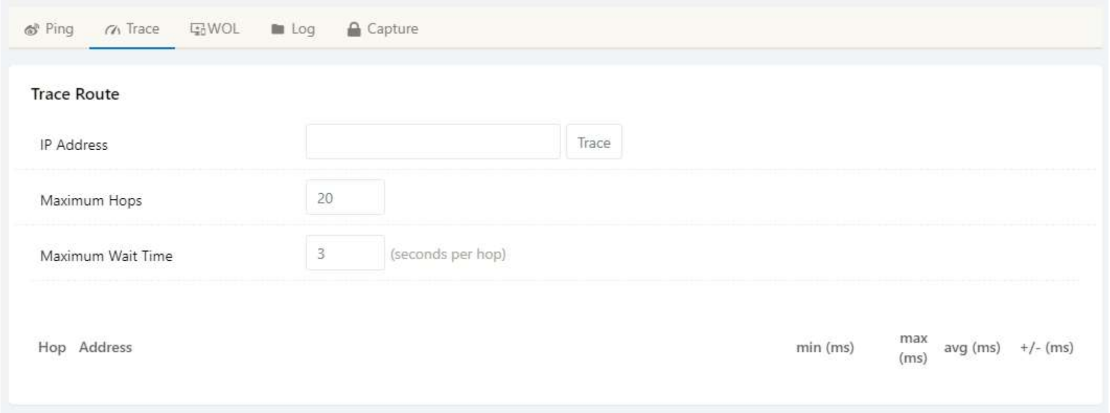
Ping Count: 5

Packet Size: 56 (bytes)

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

2.3.2.2 Trace

Click on Tools > Trace. This is a diagnostics tool for displaying the route and measuring transit delays of packets across an Internet IP network.



Trace Route

IP Address: Trace

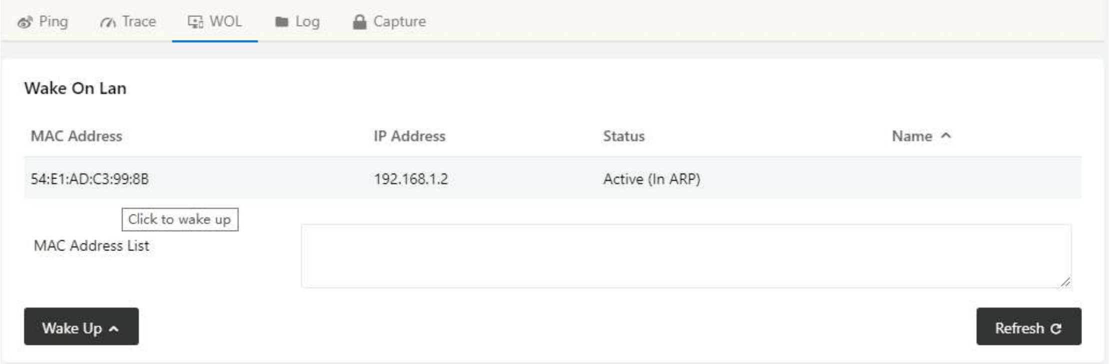
Maximum Hops: 20

Maximum Wait Time: 3 (seconds per hop)

Hop	Address	min (ms)	max (ms)	avg (ms)	+/- (ms)

2.3.2.3 WOL

Click on Tools > WOL. This tool is used to wake up connected devices via WOL protocol. Click the left mouse button to wake up the devices.



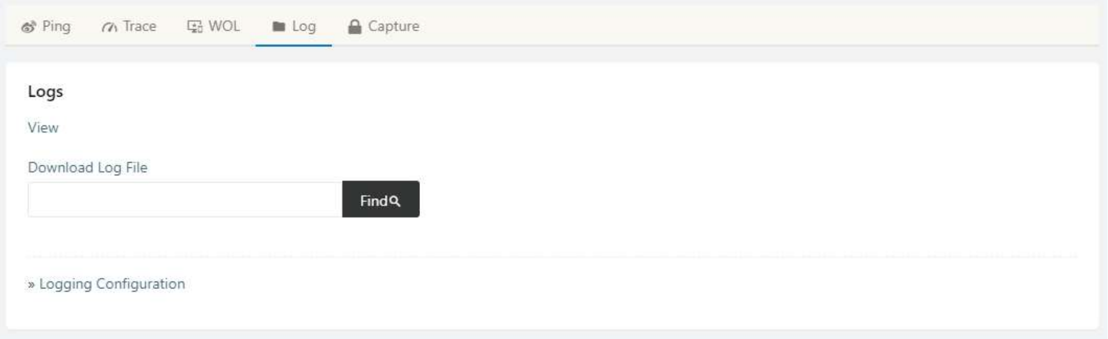
Wake On Lan

MAC Address	IP Address	Status	Name
54:E1:AD:C3:99:8B	192.168.1.2	Active (In ARP)	

MAC Address List

2.3.2.4 Log

Click on Tools > Log. This tool is used to check logs and send logs to the server.



Logs

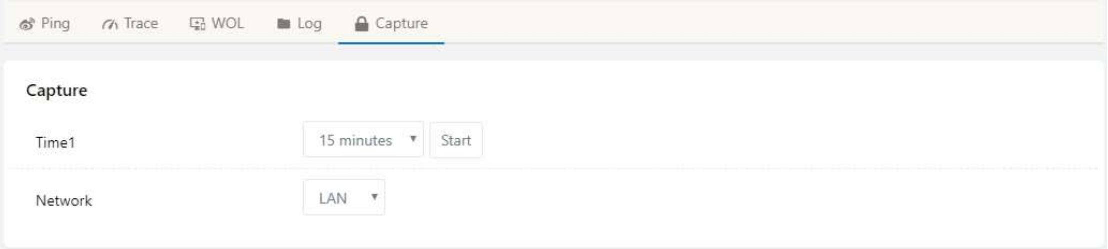
View

Download Log File

» Logging Configuration

2.3.2.5 Capture

Click on Tools > Capture. This tool is used to capture LAN/WAN data packets for analysis.



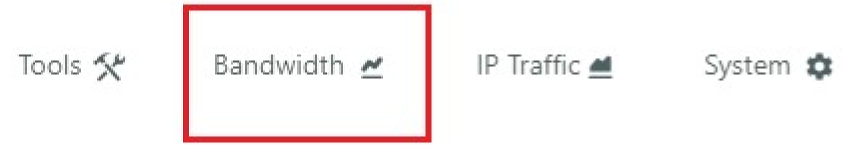
Capture

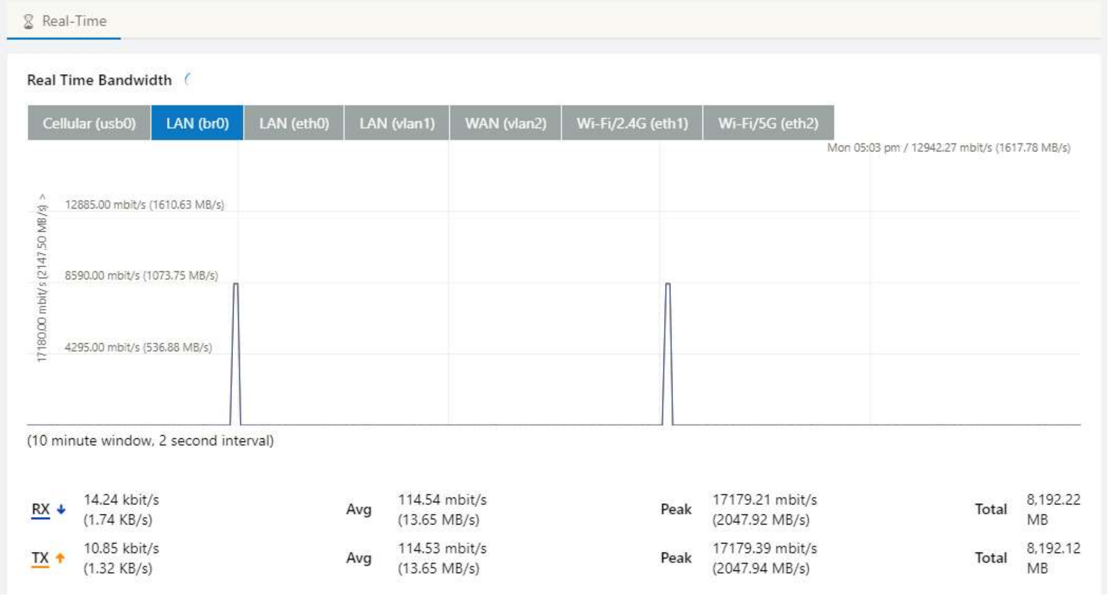
Time1: 15 minutes

Network: LAN

2.3.3 Bandwidth

Click on Bandwidth to check Cellular/LAN/WiFi bandwidth in real-time.





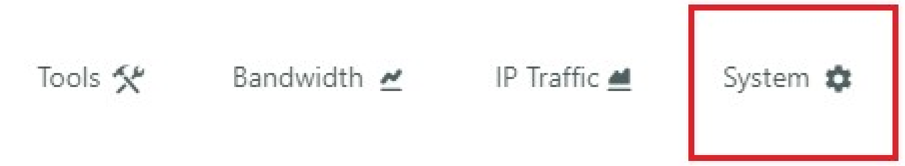
Real-Time
Real Time Bandwidth
Cellular (usb0)
LAN (br0)
LAN (eth0)
LAN (vlan1)
WAN (vlan2)
Wi-Fi/2.4G (eth1)
Wi-Fi/5G (eth2)
Mon 05:03 pm / 12942.27 mbit/s (1617.78 MB/s)
17180.00 mbit/s (2147.50 MB/s) ^
12885.00 mbit/s (1610.63 MB/s)
8590.00 mbit/s (1073.75 MB/s)
4295.00 mbit/s (536.88 MB/s)

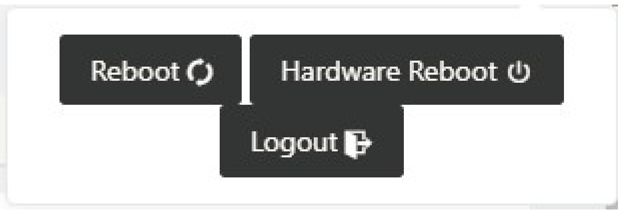
(10 minute window, 2 second interval)

RX ↓	14.24 kbit/s (1.74 KB/s)	Avg	114.54 mbit/s (13.65 MB/s)	Peak	17179.21 mbit/s (2047.92 MB/s)	Total	8,192.22 MB
TX ↑	10.85 kbit/s (1.32 KB/s)	Avg	114.53 mbit/s (13.65 MB/s)	Peak	17179.39 mbit/s (2047.94 MB/s)	Total	8,192.12 MB

2.3.4 System

Click on “System” to perform a software reboot, hardware reboot or to logout.

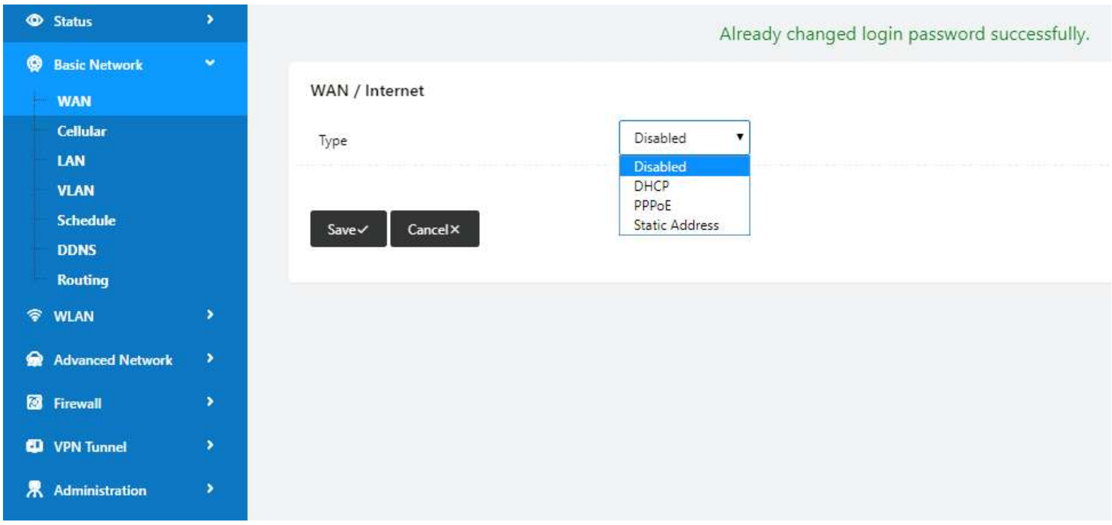




2.4 Basic Network

2.4.1 WAN Settings

Go to Basic Network > WAN. Here you can select DHCP, PPPoE or Static IP address.



Already changed login password successfully.

WAN / Internet

Type: Disabled

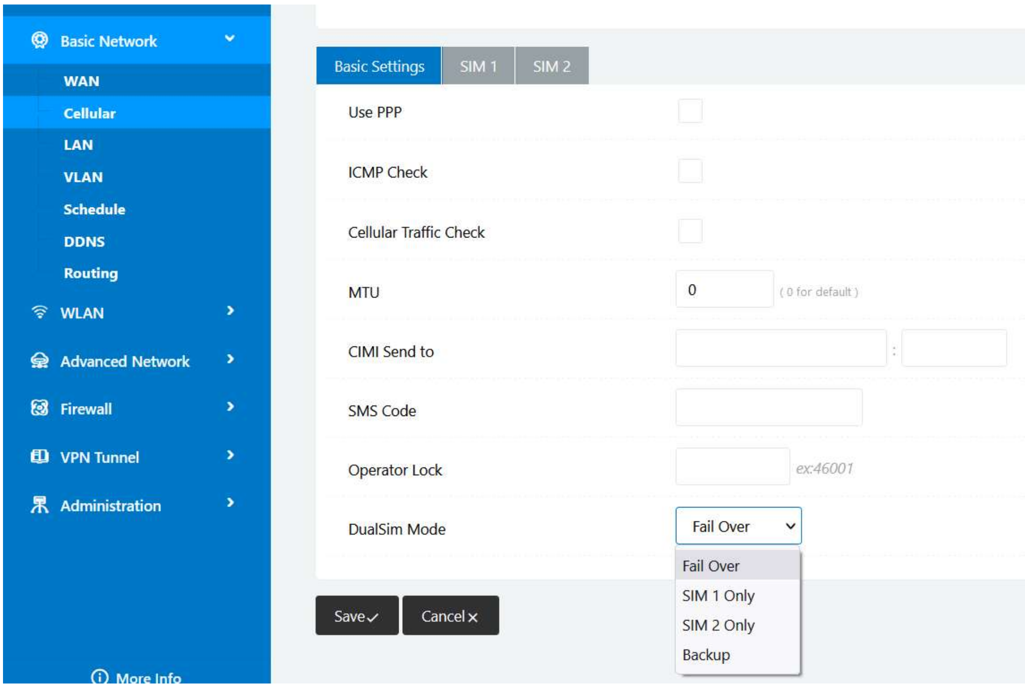
Table 2-1 WAN Settings Instructions

Parameter	Instructions
Type	Supports DHCP, PPPoE, Static IP address

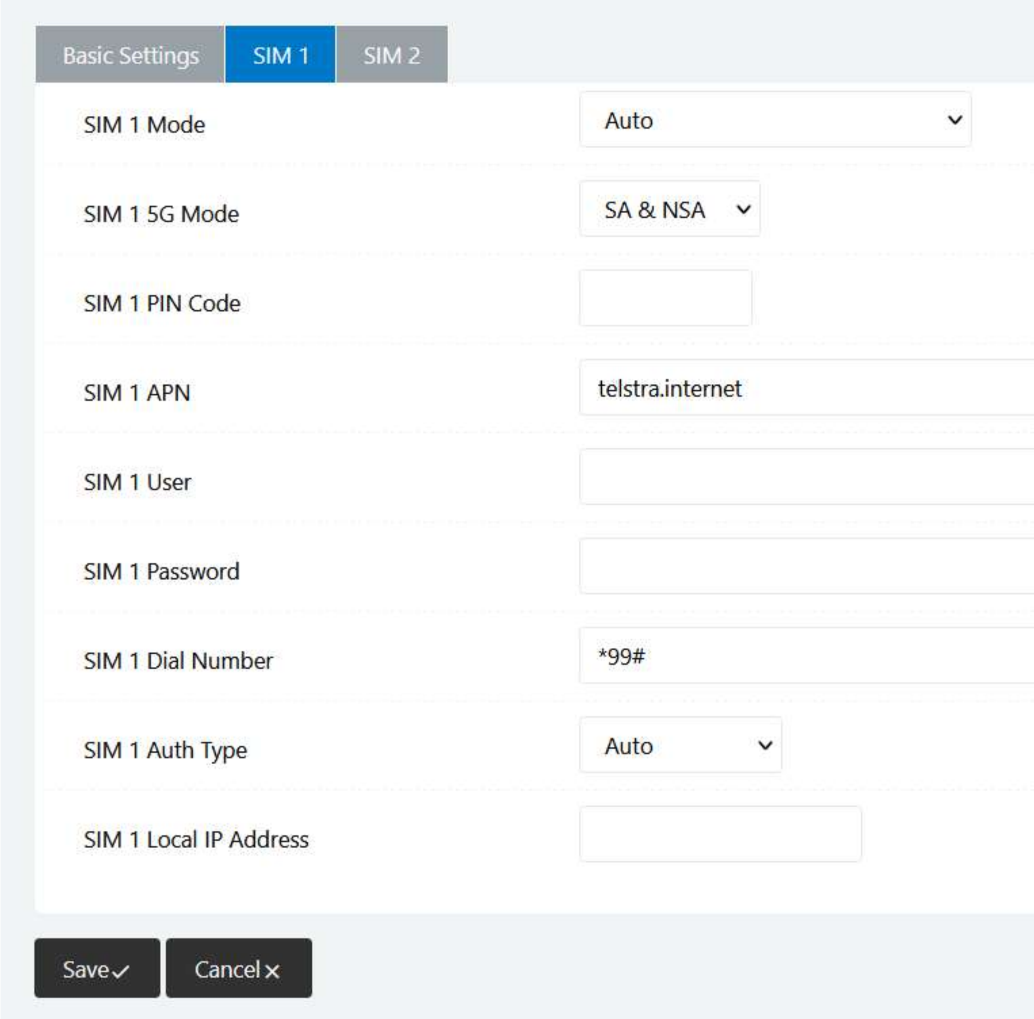
Click “Save” to finish. The router will reboot.

2.4.2 Cellular Settings

Step 1: Select Basic Network> Cellular. Here you can enter the APN of your SIM card. If you have a dual-SIM router, you will need to enter the APN for both SIM1 and SIM2. Dual SIM mode can be “Failover”, “SIM 1 only”, “SIM 2 only” or “Backup”.



Use PPP	□
ICMP Check	□
Cellular Traffic Check	□
MTU	0 (0 for default)
CIMI Send to	:
SMS Code	
Operator Lock	ex:46001
DualSim Mode	Fail Over



SIM 1 Mode	Auto
SIM 1 5G Mode	SA & NSA
SIM 1 PIN Code	
SIM 1 APN	telstra.internet
SIM 1 User	
SIM 1 Password	
SIM 1 Dial Number	*99#
SIM 1 Auth Type	Auto
SIM 1 Local IP Address	

Table 2-2 Cellular Settings Instructions

Item	Description
Enable Modem	Enable/Disable 5G modem.
Use PPP	ECM dial-up as default. PPP optional.
ICMP check	To enable or disable “ICMP check” rules. Enable the ICMP check and setup a reachable IP address as a destination IP. When “ICMP check” fails, the router will reconnect/reboot.
Cellular Traffic Check	The router will reconnect/reboot if there is no Rx/Tx traffic.
CIMI Send to	Send CIMI to a defined IP address and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock the router to a specific carrier by MCC/MNC code.
Dual SIM Mode	Fail Over: When SIM 1 fails, the router will switch to SIM 2. When SIM 2 fails, the router will switch back to SIM 1. SIM1 Only: Just SIM1 is available. SIM2 Only: Just SIM2 is available. Backup: SIM1 is the primary SIM. When SIM 1 fails, the router will switch to SIM 2 and stays on SIM 2 for a set period of time, at the end of which it will switch back to SIM 1.
SIM Mode	Auto: The router will connect automatically to 3G, 4G or 5G, with priority given to 5G. 5G NR: Router will only connect to 5G. LTE: Router will only connect to 4G. 3G: Router will only connect to 3G.
Pin Code	By default, leave this field blank. In some cases, SIM cards are locked with a PIN code.
APN	APN is provided by your ISP. I.e. “telstra.internet” if using a Telstra SIM card.

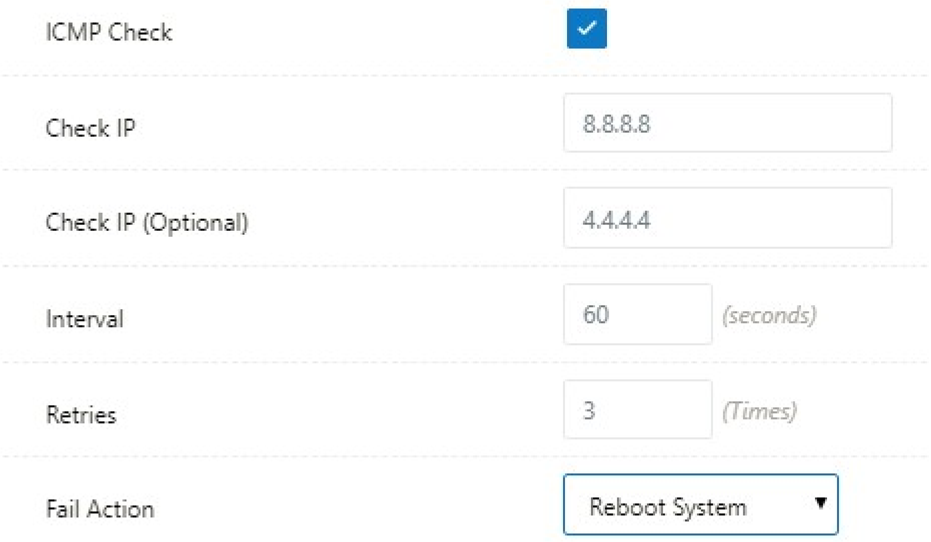
Item	Description
Username	SIM card username is provided by your ISP. Usually leave blank.
Password	SIM card password is provided by your ISP. Usually leave blank.
Auth. Type	Authentication is required in some cases (i.e., when using telstra.corp APN). Options are Auto/PAP/Chap/MS-Chap/MS-Chapv2.
SIM Local IP Address	Fixed SIM IP address. This feature is available if your carrier can provide this service.

NOTE ICMP Check and Cellular Traffic Check are alternative.

【ICMP Check】

If you enable ICMP, the router will automatically check whether the defined IP address is reachable every 60 seconds. If the IP address is unreachable and the ICMP check fails the first time, it will check twice again at a 3-second interval. If the ICMP check fails the third time, the router will implement the “fail action” as configured.

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



ICMP Check ☑

Check IP 8.8.8.8

Check IP (Optional) 4.4.4.4

Interval 60 (seconds)

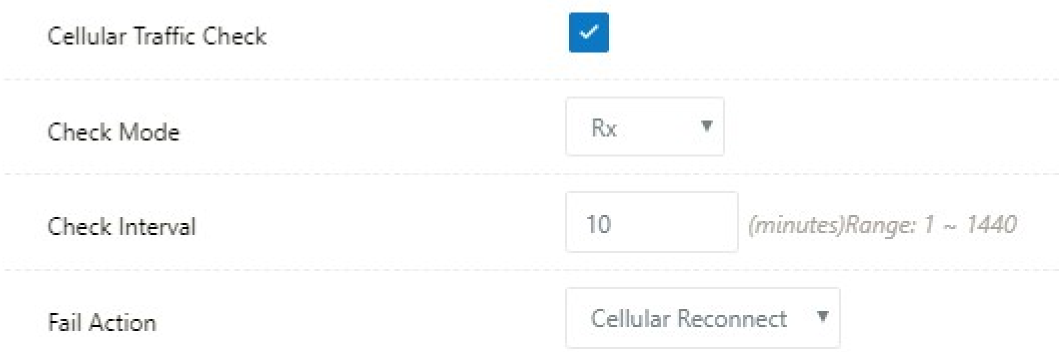
Retries 3 (Times)

Fail Action Reboot System ▾

【Cellular Traffic Check】

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

【Rx】The router will check the 4G/LTE cellular receiver traffic. If no traffic is received within the defined check interval time, the router will implement the specified action reconnect or reboot.



Cellular Traffic Check ☑

Check Mode: Rx

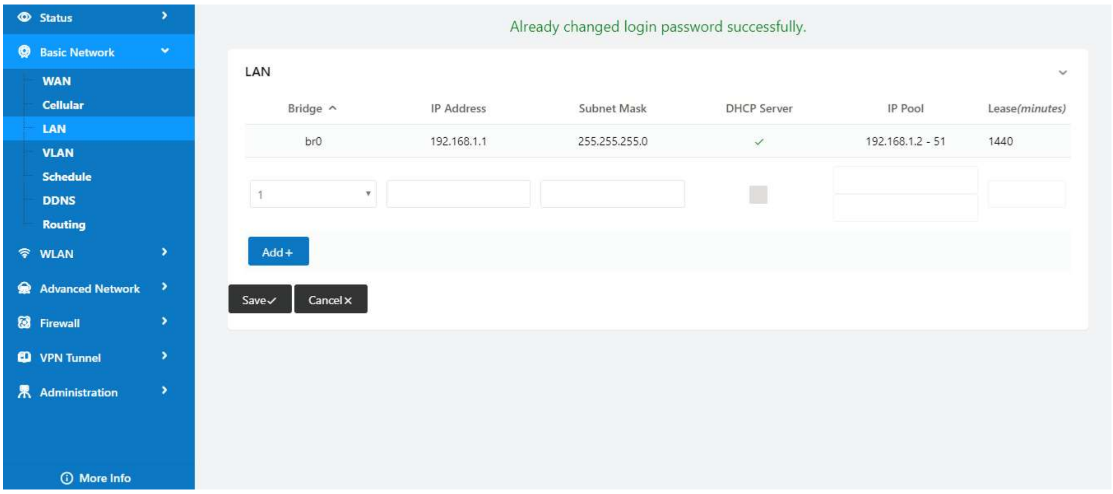
Check Interval: 10 (minutes)Range: 1 ~ 1440

Fail Action: Cellular Reconnect

Step 1 To save the settings, click the “save” button.

2.4.3 LAN Settings

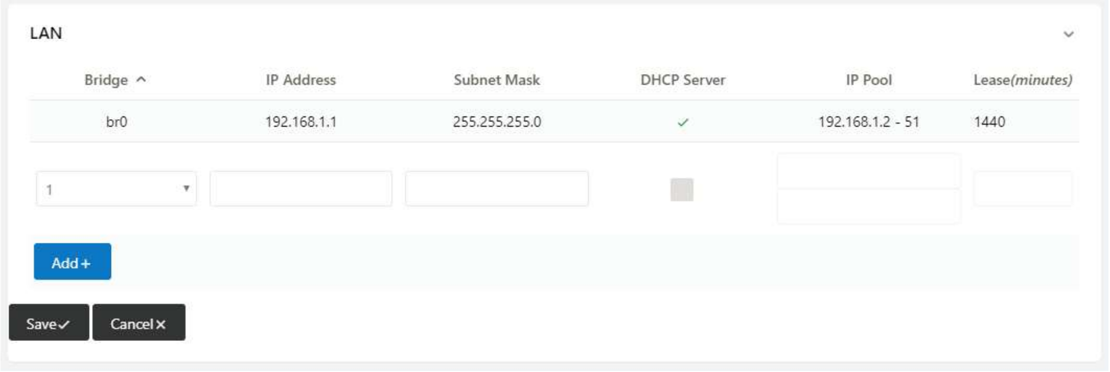
Step 1 Go to Basic Network>LAN



Already changed login password successfully.

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease*(minutes)*
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440
1			□		



LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease*(minutes)*
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440
1			□		

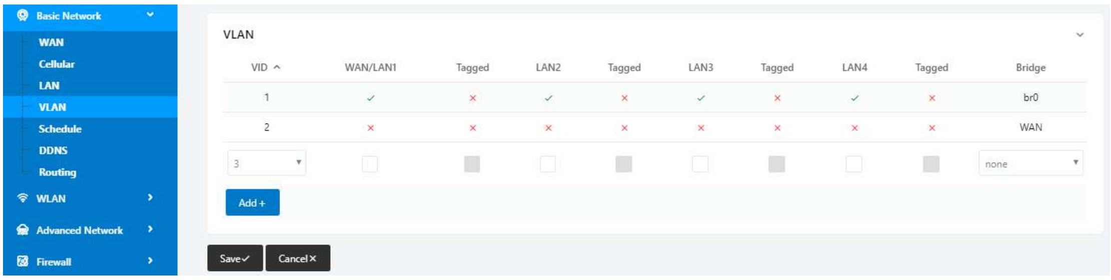
Table 2-3 LAN Settings Instructions

Item	Description
Bridge	Supports four LAN IP addresses from br0 to br3. If VLAN is required, please go to the VLAN page.
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. When enabled, it will show the IP address range and lease option.
IP Pool	IP address range within the LAN.
Lease	The valid time in minutes.
Add	Add a LAN IP address. Supports four LAN IP addresses.

Step 2 Click “save” to save the configuration. The device will reboot.

2.4.4 VLAN Settings

Step 1 Go to Basic Network >VLAN.



VLAN

VID	WAN/LAN1	Tagged	LAN2	Tagged	LAN3	Tagged	LAN4	Tagged	Bridge
1	✓	×	✓	×	✓	×	✓	×	br0
2	×	×	×	×	×	×	×	×	WAN
3 ▾	□	□	□	□	□	□	□	□	none ▾

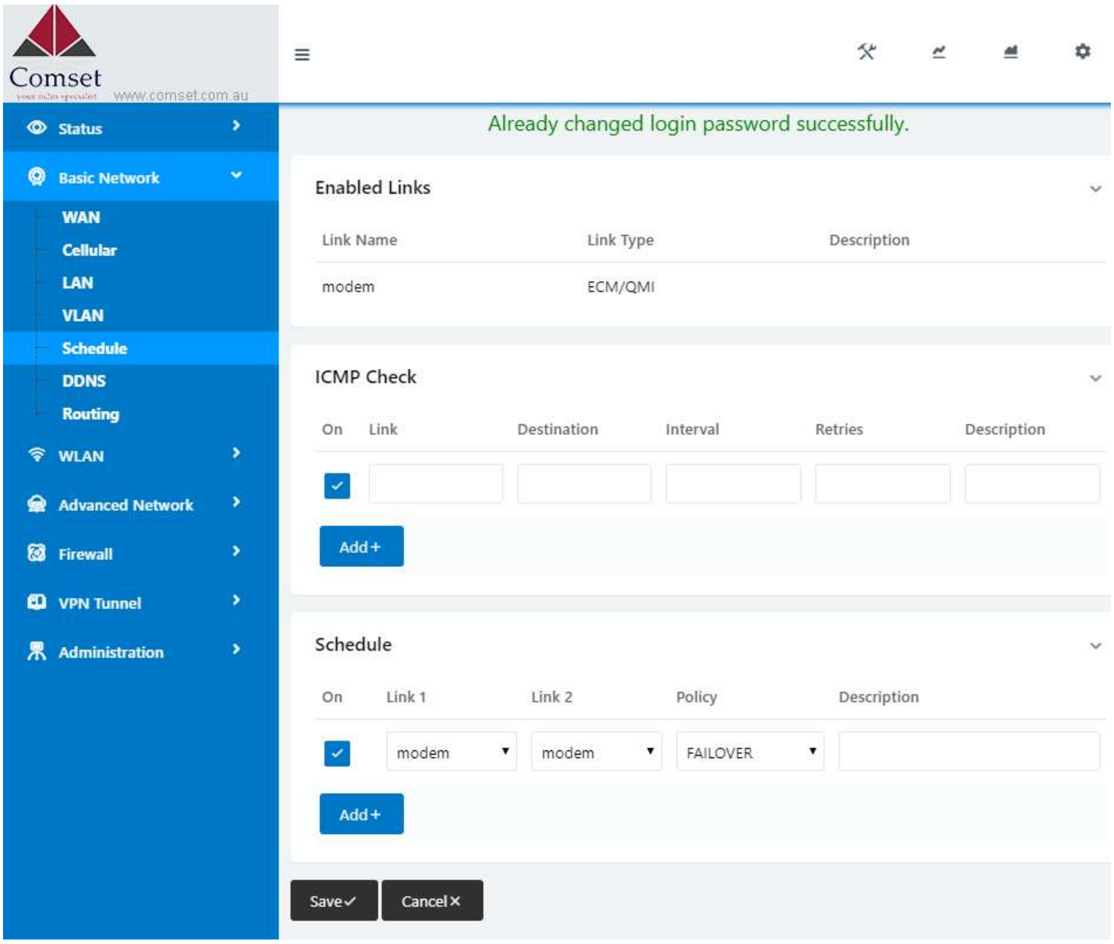
Table 2-4 VLAN Settings

Item	Instructions
VID	VLAN ID number. The VID range is from 1 to 15.
WAN/LAN1~LAN4	Defined LAN ports in different Bridge.
Tagged	Enable to allow the router to encapsulate and de-encapsulate the VLAN tag.
Bridge	Route interface br0, br1, br2, br3 and WAN

Step 2 Click on “Save“ to finish.

2.4.5 Schedule

Step 1 Go to Basic Network >Schedule.



Already changed login password successfully.

Enabled Links

Link Name	Link Type	Description
modem	ECM/QMI	

ICMP Check

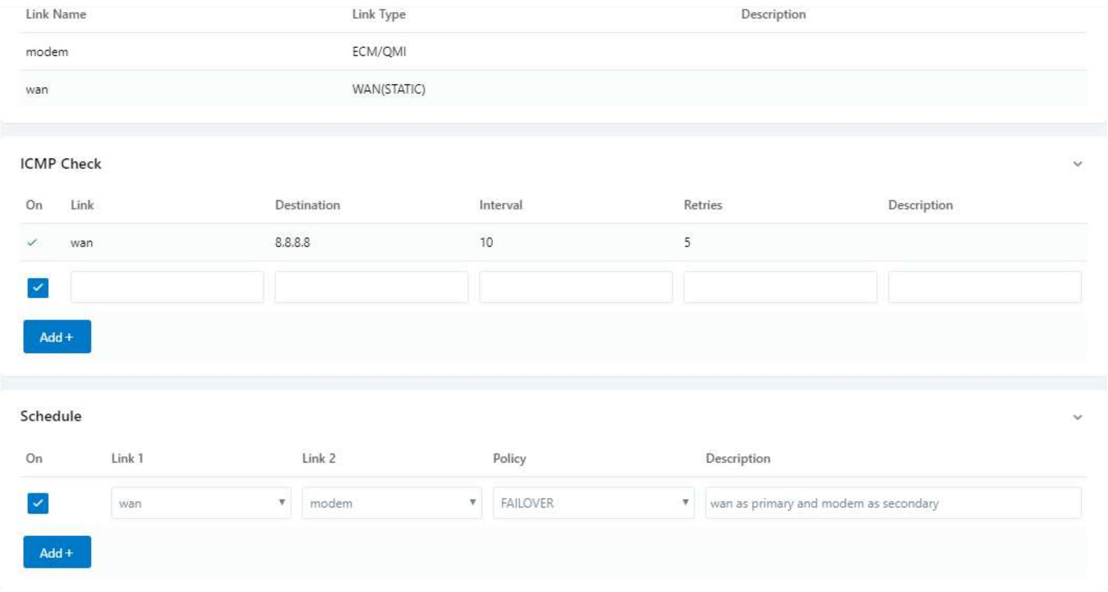
On	Link	Destination	Interval	Retries	Description
☑					

Schedule

On	Link 1	Link 2	Policy	Description
☑	modem	modem	FAILOVER	

Item	Instructions
Modem	The router dials up to the network via the 5G modem.
Wan	The router dials up to the network via the WAN port (DHCP, PPPOE, Static IP)
ICMP Check	When the ICMP Check fails, the switching action between Link1 and Link2 will be triggered.
Link1	The Primary link.
Link2	The Secondary link.
BACKUP	Link1 is the primary link. If Link1 fails, the router will switch to Link2. As

	soon as Link1 recovers, the router will switch back to Link1.
FAILOVER	Link1 is the primary link. If Link1 fails, the router will switch to Link2. If Link2 fails, the router will switch back to Link1.



Link Name	Link Type	Description
modem	ECM/QMI	
wan	WAN(STATIC)	

ICMP Check

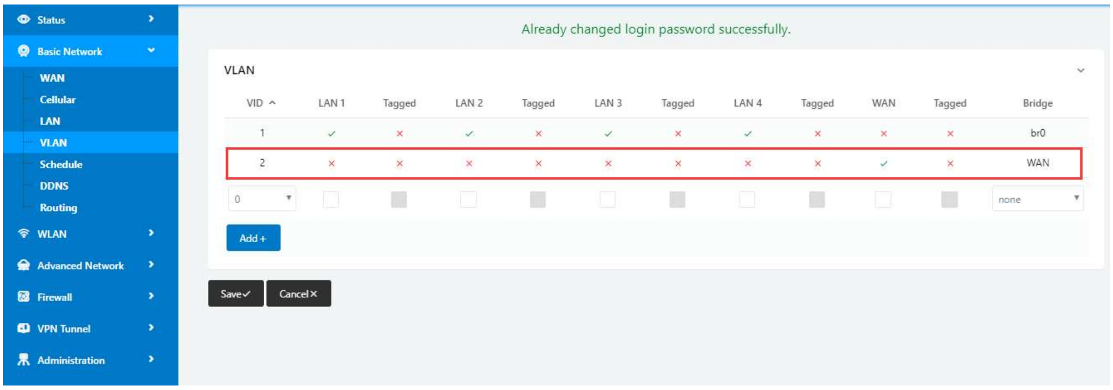
On	Link	Destination	Interval	Retries	Description
✓	wan	8.8.8.8	10	5	
☑					

Schedule

On	Link 1	Link 2	Policy	Description
☑	wan	modem	FAILOVER	wan as primary and modem as secondary

NOTE

The VLAN should be configured with WAN and 5G backup together. Please define WAN port as bridge WAN interface in the VLAN GUI as below.



Already changed login password successfully.

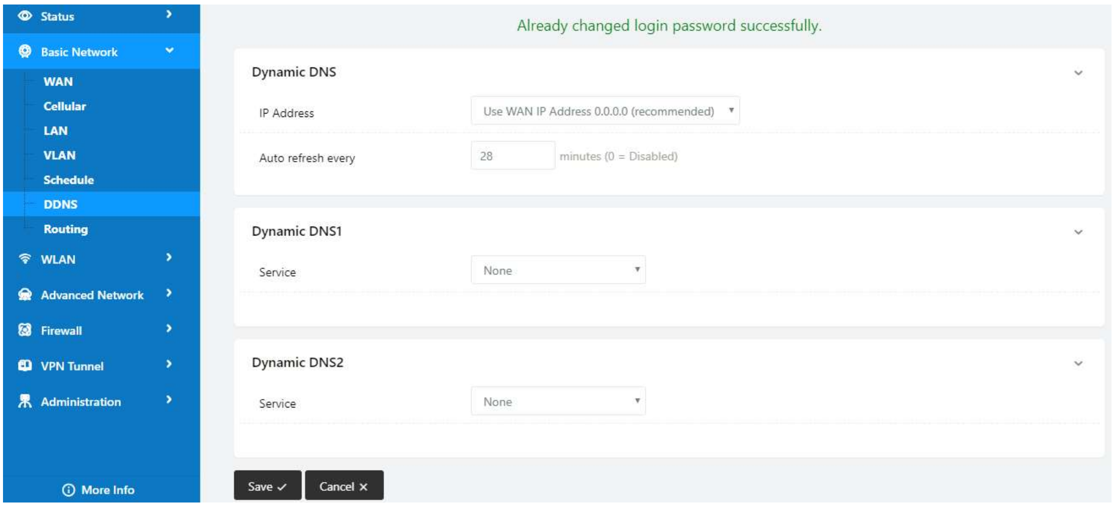
VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	×	✓	×	✓	×	✓	×	×	×	br0
2	×	×	×	×	×	×	×	×	✓	×	WAN
0	□	□	□	□	□	□	□	□	□	□	none

Step 2 Click “Save“ to finish.

2.4.6 Dynamic DNS Settings

Step 1 Go to Basic Network >DDNS and enter the DDNS settings.



Already changed login password successfully.

Dynamic DNS

IP Address: Use WAN IP Address 0.0.0.0 (recommended)

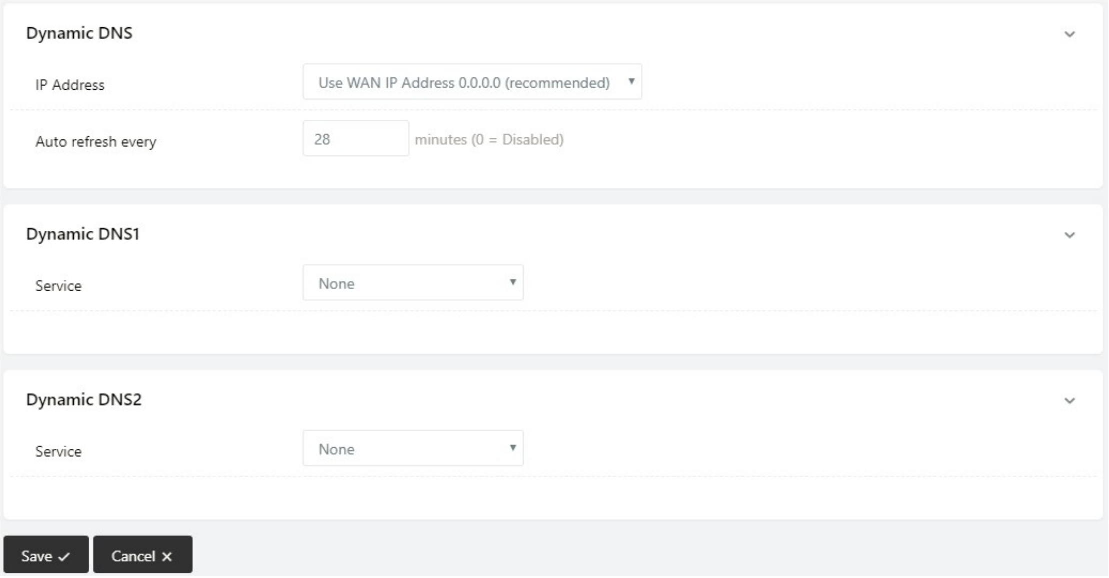
Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None



Dynamic DNS

IP Address: Use WAN IP Address 0.0.0.0 (recommended)

Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: None

Dynamic DNS2

Service: None

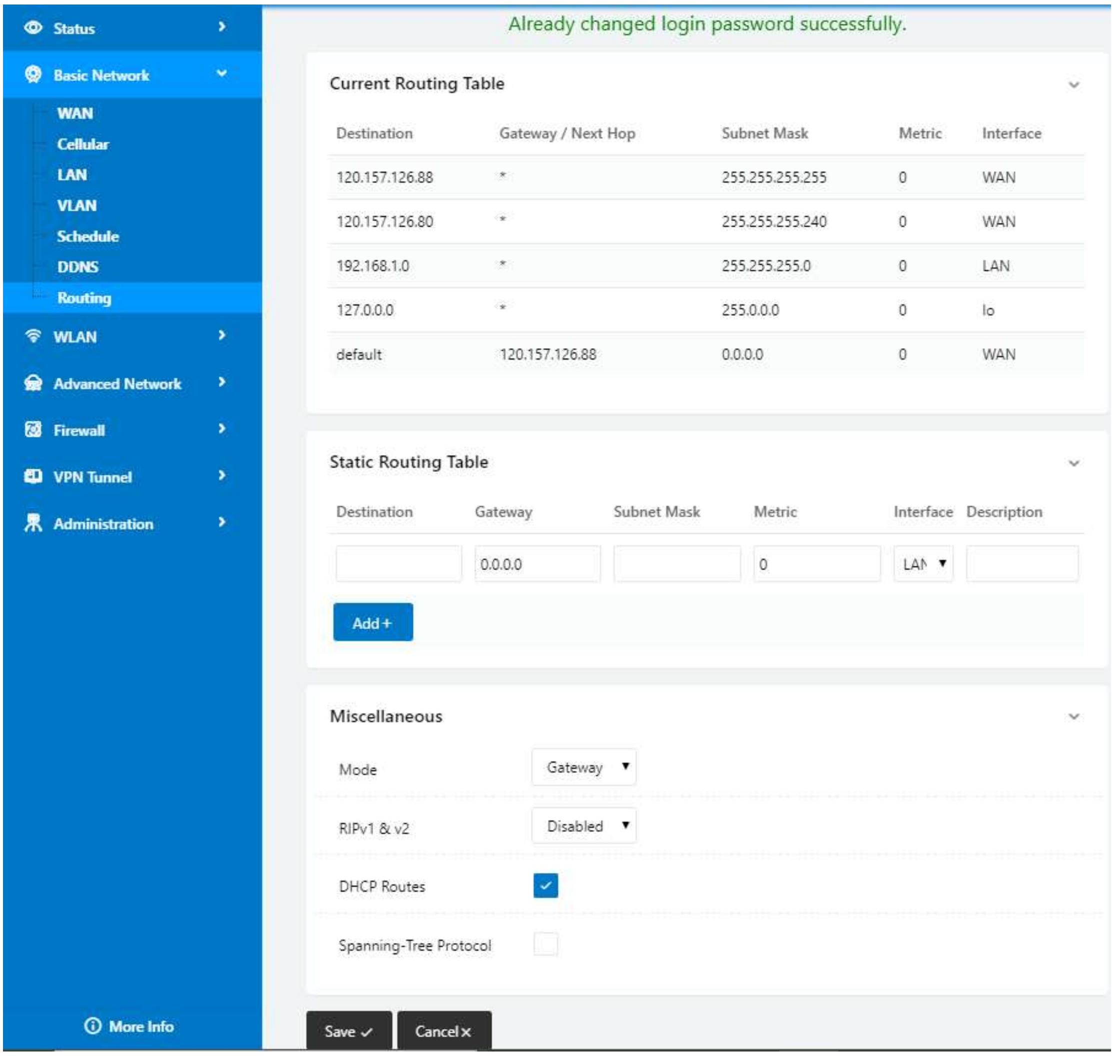
Table 2-5 DDNS Settings

parameter	Instruction
IP address	The default is standard DDNS protocol. In general, use the default IP 0.0.0.0
Auto refresh time	Set the interval for the DDNS client to obtain a new IP. It is recommended 240s or more.
Service provider	Select the DDNS service provider from the list.

Step 2 Click “Save“ to finish.

2.4.7 Routing Settings

Step 1   Go to Basic Network >Routing.



Already changed login password successfully.

Current Routing Table

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
120.157.126.88	*	255.255.255.255	0	WAN
120.157.126.80	*	255.255.255.240	0	WAN
192.168.1.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo
default	120.157.126.88	0.0.0.0	0	WAN

Static Routing Table

Destination	Gateway	Subnet Mask	Metric	Interface	Description
	0.0.0.0		0	LAN	

Miscellaneous

Mode: Gateway

RIPv1 & v2: Disabled

DHCP Routes: ☑

Spanning-Tree Protocol: □

Table 2-6 Routing Settings

Item	Instructions
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 route should be chosen over another.
Interface	Interface from router to gateway.
Description	Describes the routing name.

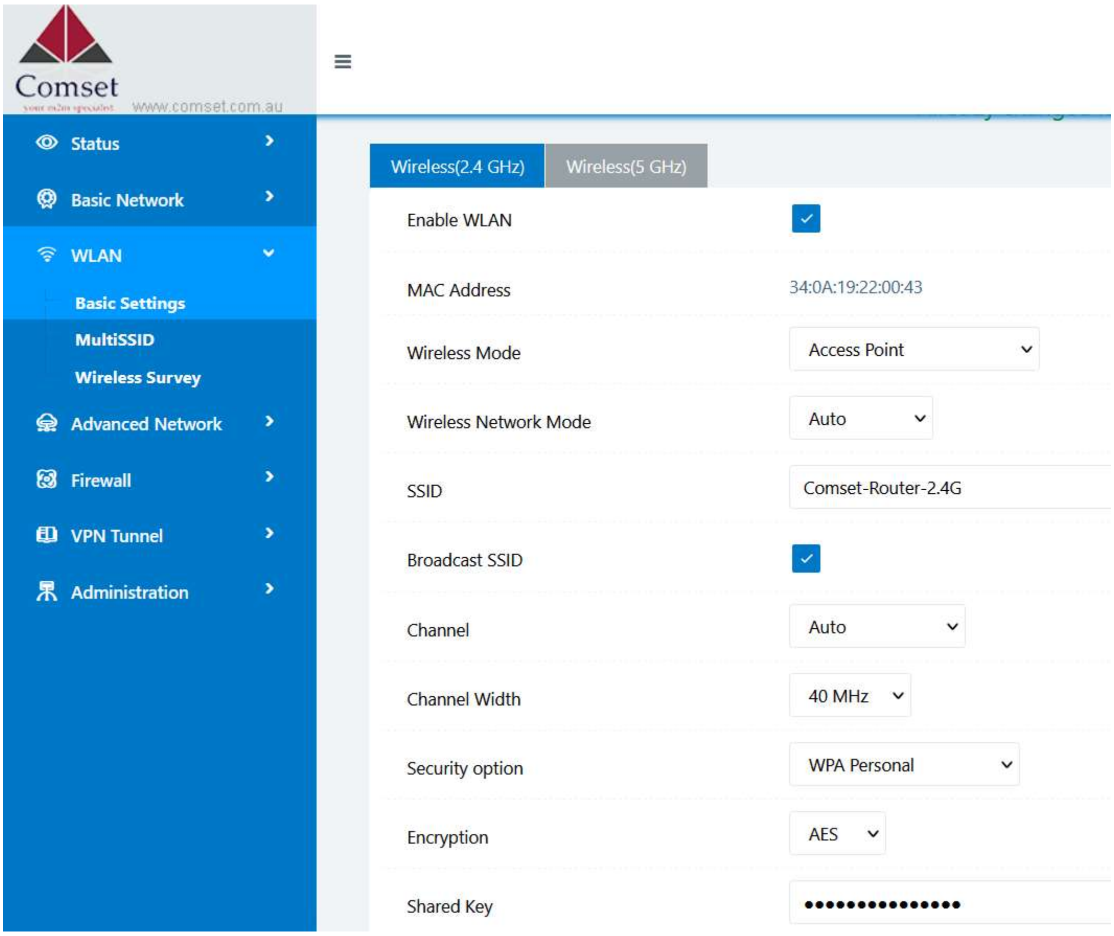
Step 2   Click “Save” to finish.

2.5 WLAN Settings

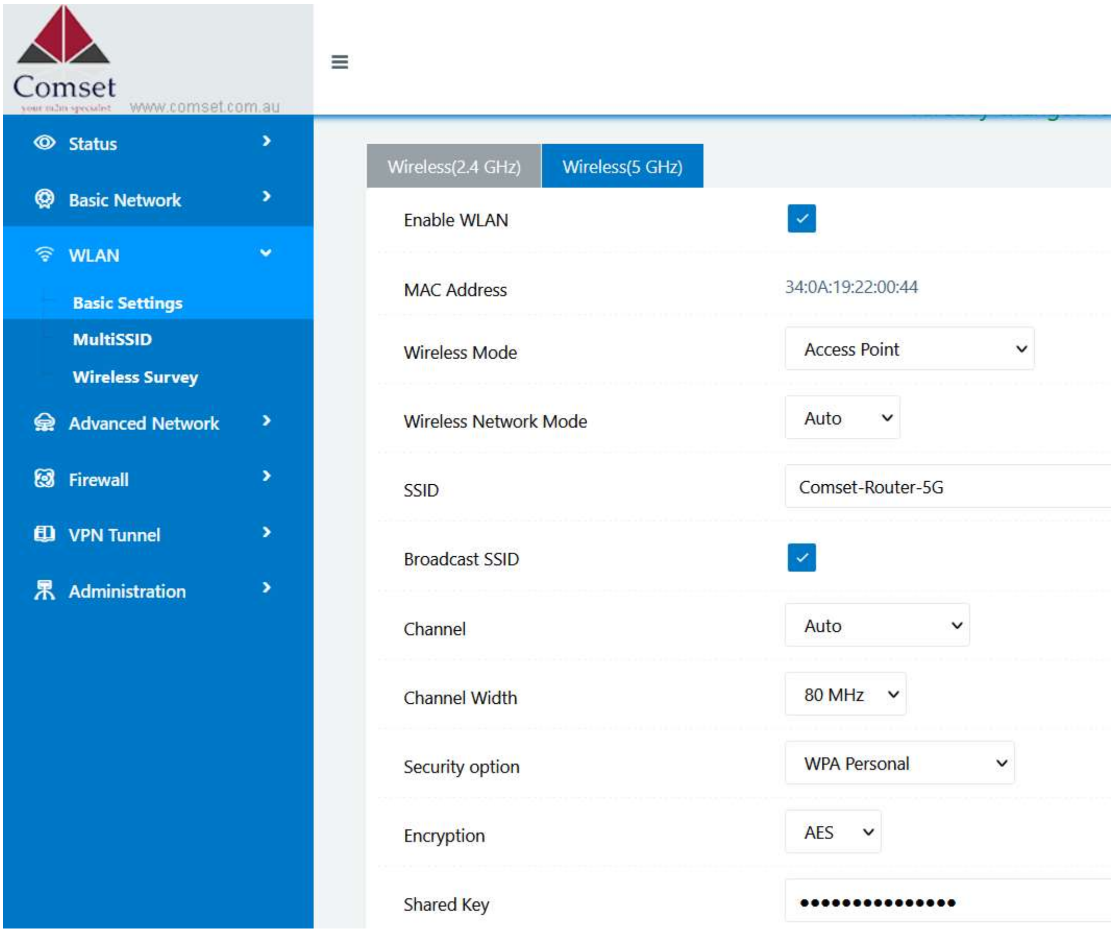
Please follow the instructions below.

2.5.1 Basic Setting

Step 1   Go to WLAN >Basic Settings.



Enable WLAN	☑
MAC Address	34:0A:19:22:00:43
Wireless Mode	Access Point
Wireless Network Mode	Auto
SSID	Comset-Router-2.4G
Broadcast SSID	☑
Channel	Auto
Channel Width	40 MHz
Security option	WPA Personal
Encryption	AES
Shared Key	•••••••••••••••



Enable WLAN ☑

MAC Address 34:0A:19:22:00:44

Wireless Mode Access Point

Wireless Network Mode Auto

SSID Comset-Router-5G

Broadcast SSID ☑

Channel Auto

Channel Width 80 MHz

Security option WPA Personal

Encryption AES

Shared Key •••••••••••••••

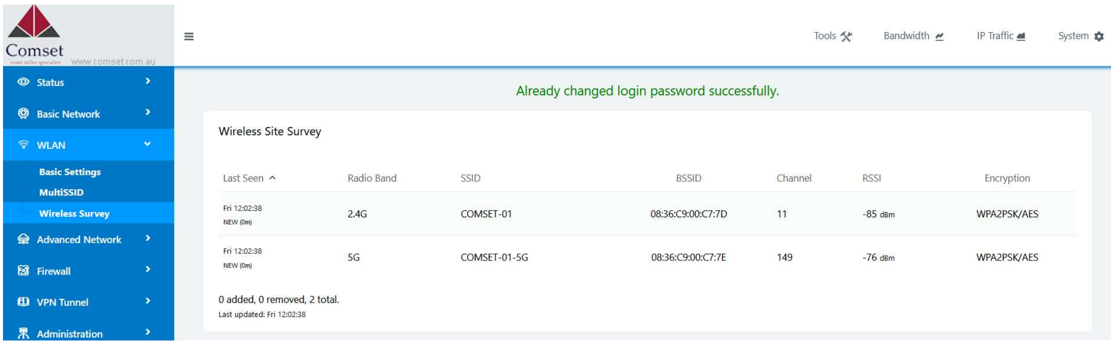
Table 2-7 WLAN Basic Settings Instructions

Item	Instructions
Radio Mode	2.4GHz or 5GHz.
Enable wireless	Enable or Disable WiFi.
Wireless mode	Supports AP mode and Client mode.
Wireless Network protocol	Supports Auto/b/g/n for 2.4GHz. Supports Auto/A/N for 5GHz.
SSID	The default is “Comset-Router-2.4G” for 2.4GHz. The default is “Comset-Router-5G” for 5GHz.
Channel	The channel of wireless network. We suggest keeping the default.
Channel Width	20MHz and 40MHz for 2.4 GHz. 20MHz, 40MHz and 80MHz for 5GHz.
Security	Supports various encryption methods.

Step 2 Click “Save” to finish.

2.5.2 Wireless Survey

Step 1 Go to WLAN> Wireless Survey to check survey.



Already changed login password successfully.

Wireless Site Survey

Last Seen	Radio Band	SSID	BSSID	Channel	RSSI	Encryption
Fri 12:02:38 NEW (0m)	2.4G	COMSET-01	08:36:C9:00:C7:7D	11	-85 dBm	WPA2PSK/AES
Fri 12:02:38 NEW (0m)	5G	COMSET-01-5G	08:36:C9:00:C7:7E	149	-76 dBm	WPA2PSK/AES

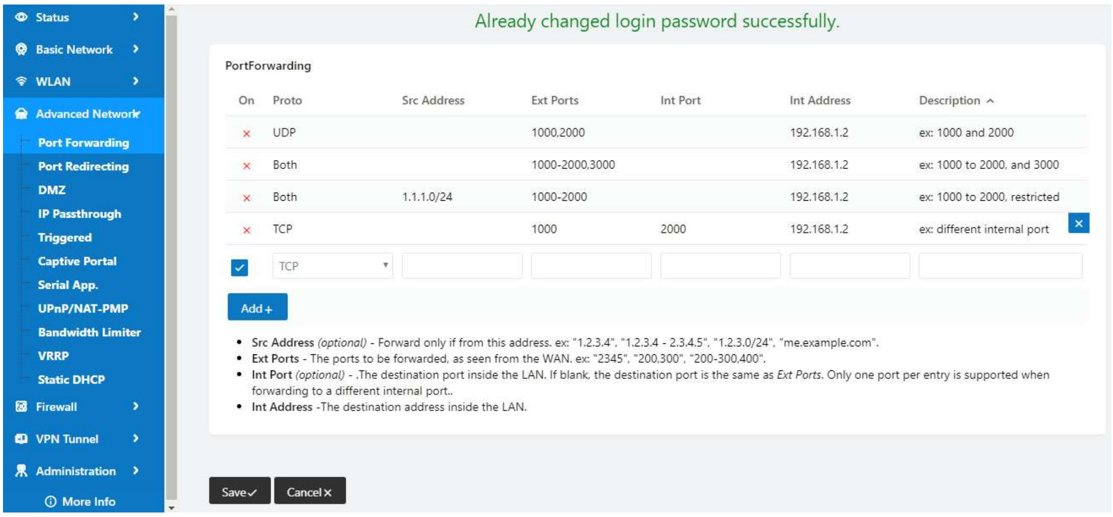
0 added, 0 removed, 2 total.

Last updated: Fri 12:02:38

2.6 Advanced Network Settings

2.6.1 Port Forwarding

Step 1 Go to Advanced Network > Port Forwarding.



Already changed login password successfully.

PortForwarding

On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description
✕	UDP		1000,2000		192.168.1.2	ex: 1000 and 2000
✕	Both		1000-2000,3000		192.168.1.2	ex: 1000 to 2000, and 3000
✕	Both	1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted
✕	TCP		1000	2000	192.168.1.2	ex: different internal port
☑	TCP					

- **Src Address** *(optional)* - Forward only if from this address. ex: "1.2.3.4", "1.2.3.4 - 2.3.4.5", "1.2.3.0/24", "me.example.com".
- **Ext Ports** - The ports to be forwarded, as seen from the WAN. ex: "2345", "200,300", "200-300,400".
- **Int Port** *(optional)* - .The destination port inside the LAN. If blank, the destination port is the same as *Ext Ports*. Only one port per entry is supported when forwarding to a different internal port..
- **Int Address** -The destination address inside the LAN.

Table 2-8 Port Forwarding Instructions

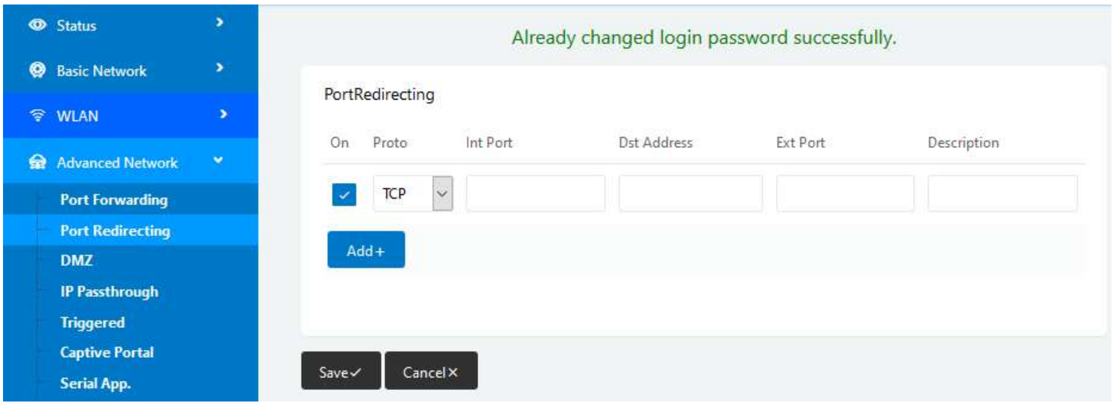
Item	Instructions
Protocol	Supports UDP, TCP, both UDP and TCP.
Src. Address	Source IP address. Forwards only if from this address.
Ext. Ports	External ports. The ports to be forwarded, as seen from the WAN.
Int. Port	Internal port. The destination port inside the LAN. If blank, the destination port is the same as Ext Ports. Only one

Item	Instructions
	port per entry is supported when forwarding to a different internal port.
Int. Address	Internal Address. The destination address inside the LAN.
Description	Brief rule description.

Step 2 Click ”save” to finish.

2.6.2 Port Redirecting

Step 1 Go to Advanced Network > Port Redirecting.



Already changed login password successfully.

PortRedirecting

On	Proto	Int Port	Dst Address	Ext Port	Description
☑	TCP				

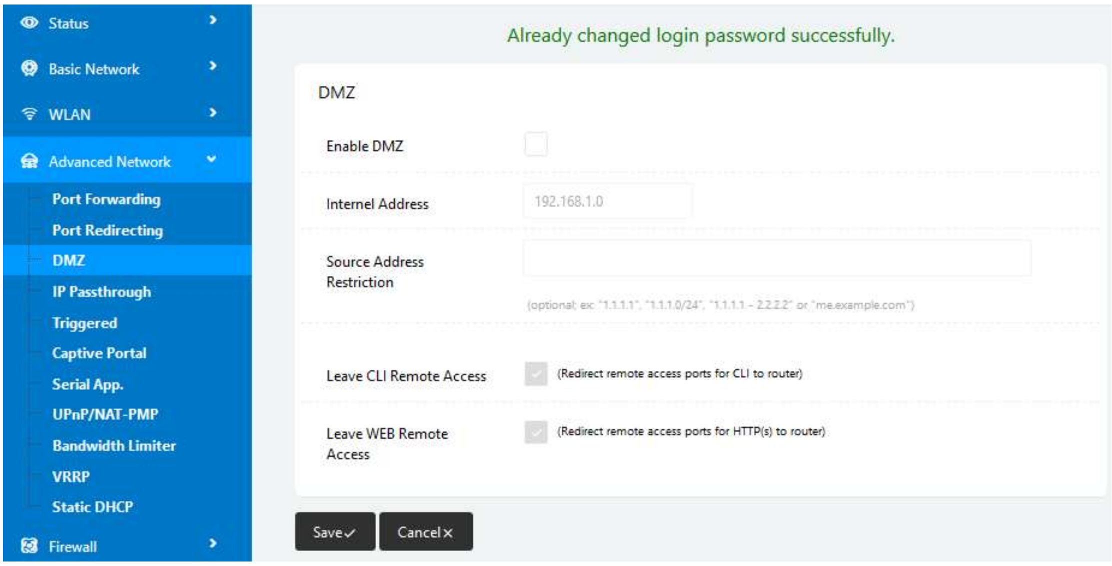
Table 2-9 Port Redirecting Instructions

Item	Instructions
Protocol	Support UDP, TCP, both UDP and TCP.
Int Port	Internal port.
Dst. Address	The destination IP address.
Ext. Ports	External ports.
Description	Brief rule description.

Step 2 Click ”save” to finish

2.6.3 DMZ Settings

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



Already changed login password successfully.

DMZ

Enable DMZ □

Internal Address 192.168.1.0

Source Address Restriction

(optional: ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com")

Leave CLI Remote Access ☑ (Redirect remote access ports for CLI to router)

Leave WEB Remote Access ☑ (Redirect remote access ports for HTTP(s) to router)

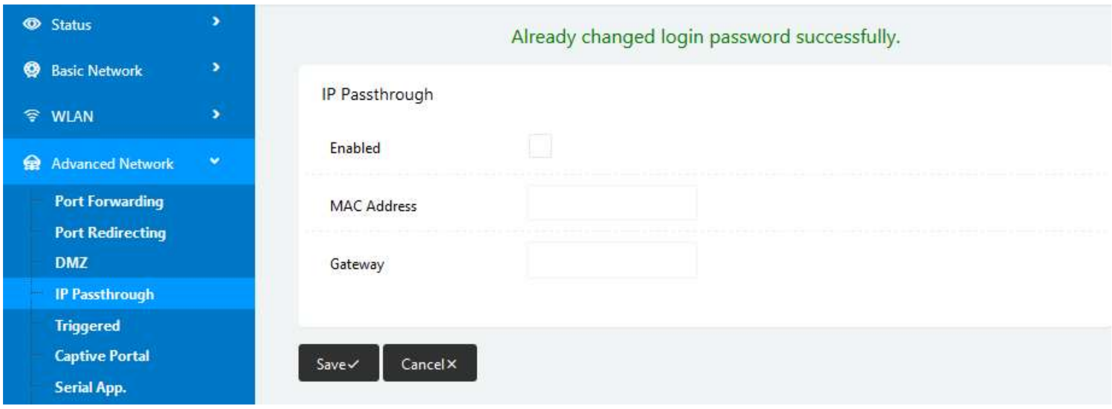
Table 2-10 DMZ Instructions

Item	Instructions
Destination Address	The destination address inside the LAN.
Source Address Restriction	If no IP address is entered, it will allow access to all IP addresses. If a defined IP address is entered, it will just allow access to that IP address.
Leave Remote Access	

Step 2 Click "save" to finish

2.6.4 IP Passthrough Settings

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



Already changed login password successfully.

IP Passthrough

Enabled □

MAC Address

Gateway

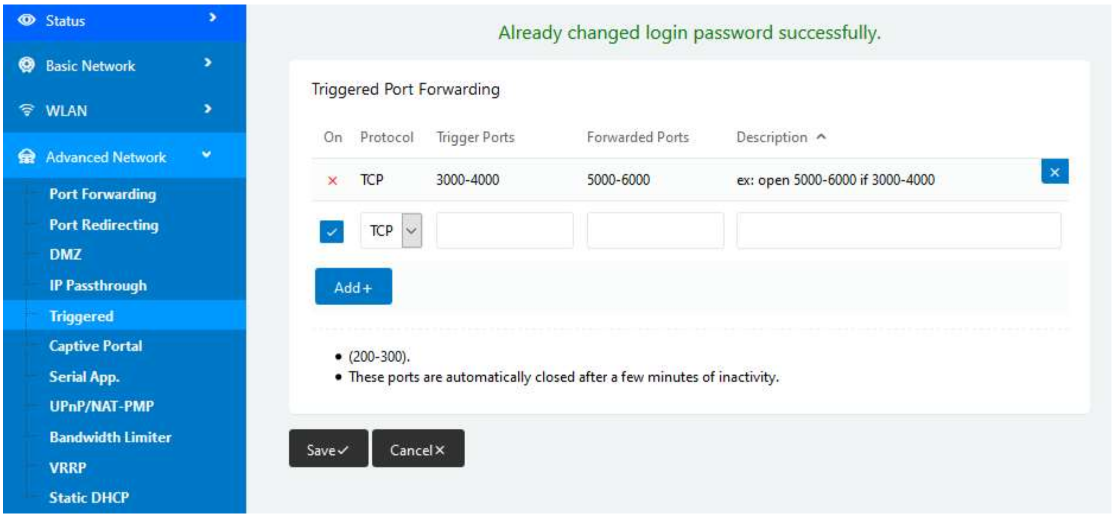
Table 2-11 IP Passthrough Instructions

Item	Instructions
Enable	Enable IP Pass-through
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned a SIM IP.
Gateway	If CM550W-POE is connected to multiple devices, input other devices gateway.

Step 2 Click ”save” to finish

2.6.5 Triggered Port Forwarding Settings

Step 1 Go to Advanced Network> Triggered, to check or modify the relevant parameters.



Already changed login password successfully.

Triggered Port Forwarding

On	Protocol	Trigger Ports	Forwarded Ports	Description
✕	TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000
☑	TCP			

- (200-300).
- These ports are automatically closed after a few minutes of inactivity.

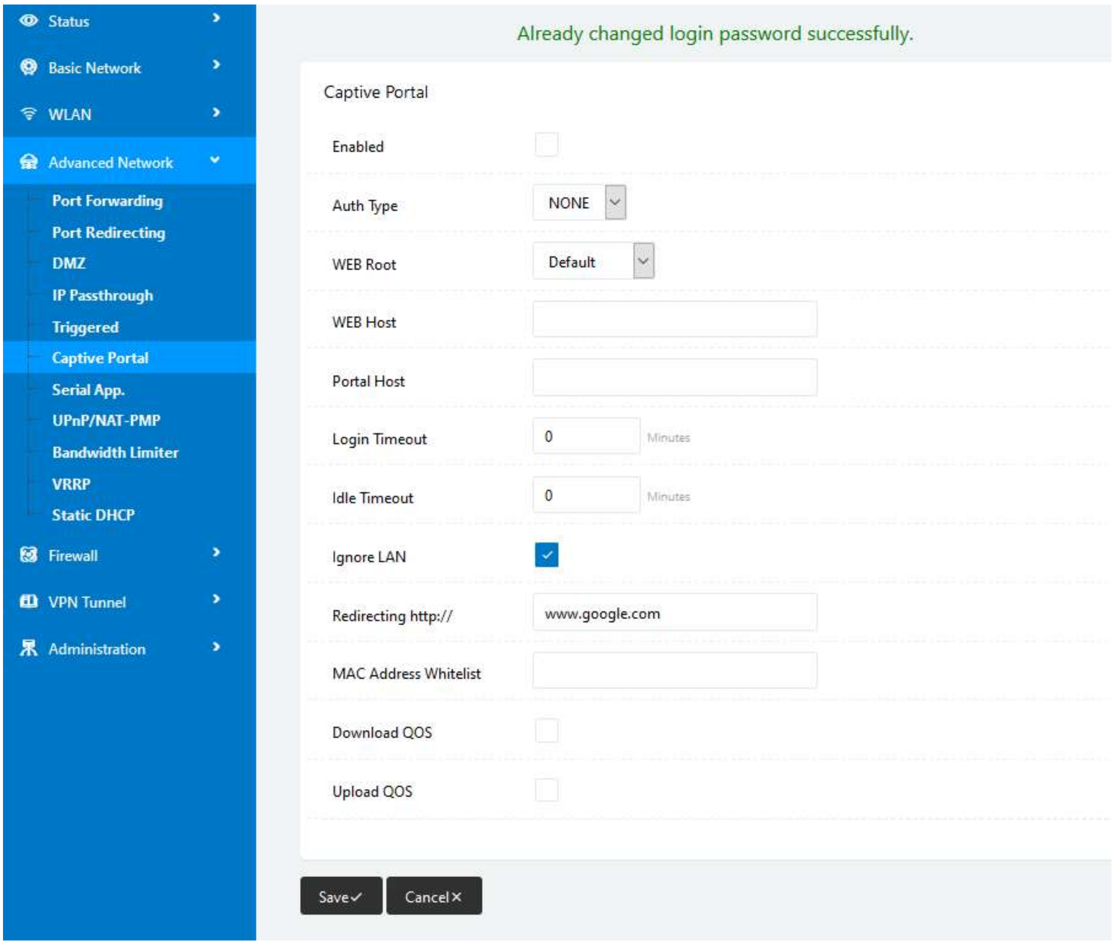
Table 2-12 Triggered Instructions

Item	Instructions
Protocol	Support UDP, TCP, both UDP and TCP.
Trigger 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 Click ”save” to finish.

2.6.6 Captive Portal

Step 1 Go to Advanced Network> Captive Portal, to check or modify the relevant parameters.



Already changed login password successfully.

Captive Portal

Enabled ☐

Auth Type NONE

WEB Root Default

WEB Host

Portal Host

Login Timeout 0 Minutes

Idle Timeout 0 Minutes

Ignore LAN ☑

Redirecting http:// www.google.com

MAC Address Whitelist

Download QOS ☐

Upload QOS ☐

Table 2-13 Captive Portal Instructions

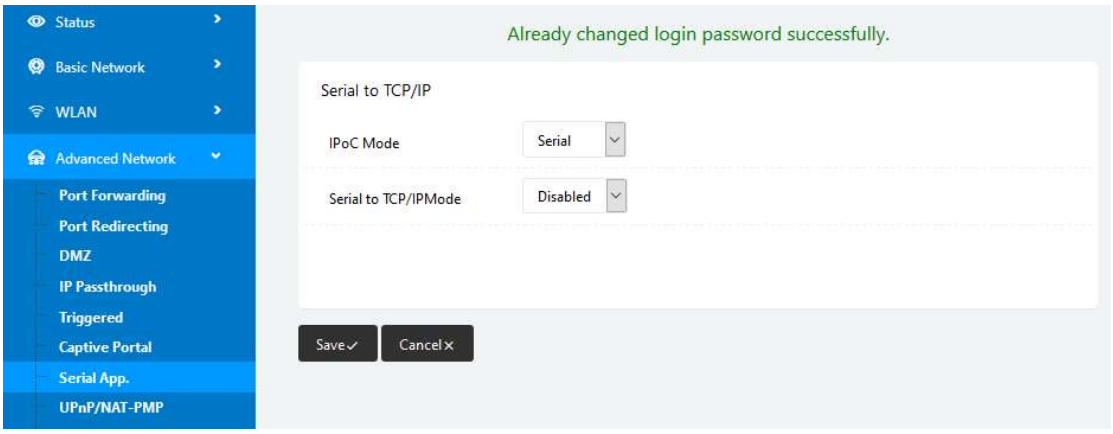
Item	Instructions
Enable	Enable Captive Portal.
Auth Type	Reserved.
Web Root	Choose captive portal file storage path. Default: Captive portal file is in the firmware as default. In-storage: Captive portal file is in router’s Flash. Ex-storage: Captive portal file is in extended storage such as SD

Item	Instructions
	card.
Web Host	Configure domain name for the captive portal access. For example, configure as comset.com.au.
Portal Host	Reserved.
Login Timeout	Maximum time the user can be online. At the end of the defined time, the user needs to re-login.
Idle Timeout	Maximum time the user has connectivity when in idle mode.
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 Bandwidth limit per user.
Upload QoS	Enable to apply the Upload Bandwidth limit per user.

Step 2 Click ”save” to finish.

2.6.7 Serial App. Settings

Step 1 Go to Advanced Network> Serial App, to check or modify the relevant parameters.

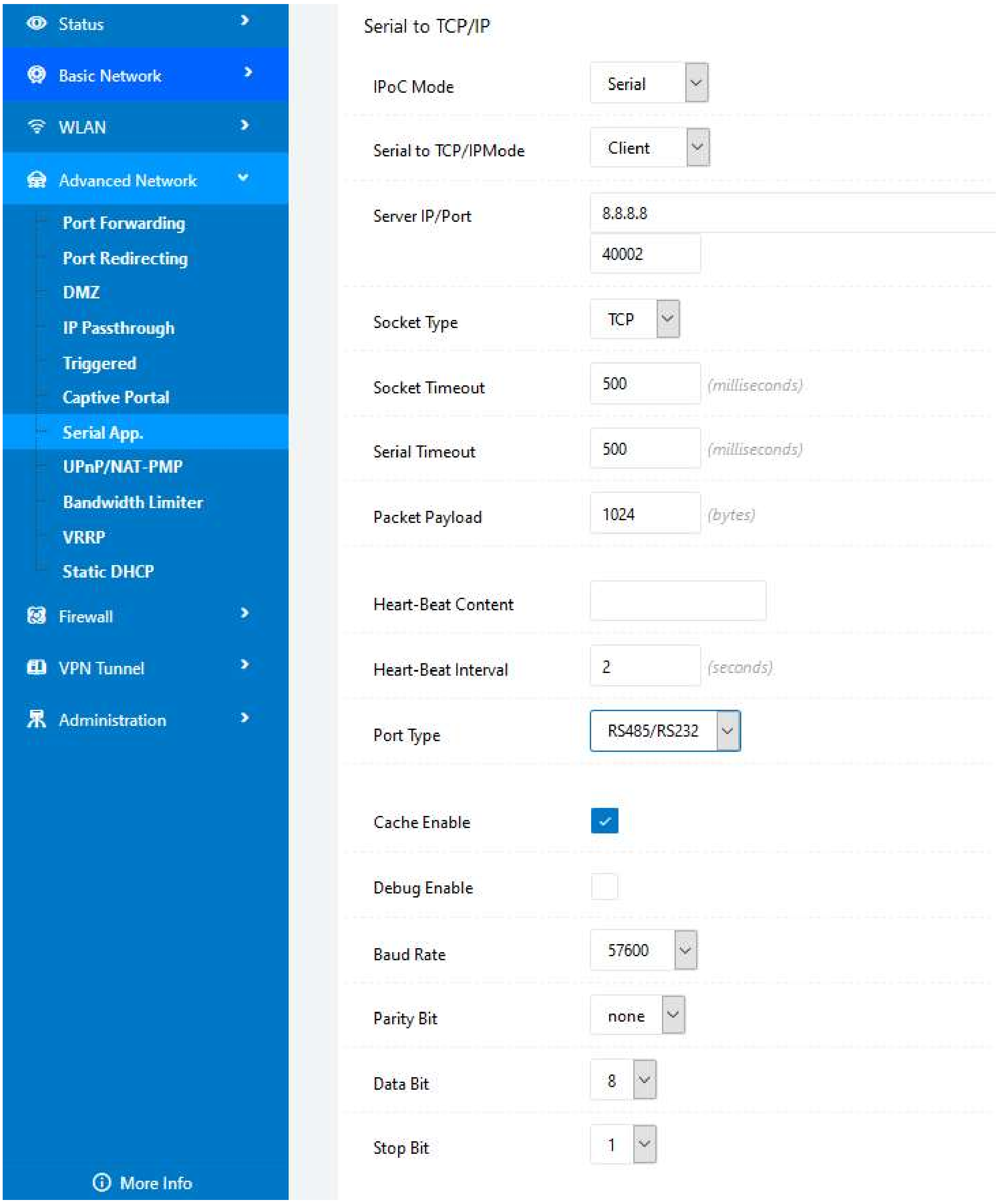


Already changed login password successfully.

Serial to TCP/IP

IPoC Mode: Serial

Serial to TCP/IPMode: Disabled



Serial to TCP/IP

IPoC Mode: Serial

Serial to TCP/IPMode: Client

Server IP/Port: 8.8.8.8 40002

Socket Type: TCP

Socket Timeout: 500 (milliseconds)

Serial Timeout: 500 (milliseconds)

Packet Payload: 1024 (bytes)

Heart-Beat Content:

Heart-Beat Interval: 2 (seconds)

Port Type: RS485/RS232

Cache Enable: ☑

Debug Enable: ☐

Baud Rate: 57600

Parity Bit: none

Data Bit: 8

Stop Bit: 1

Table 2-14 Serial App Instructions

Item	Instructions
Serial to TC/IP mode	Options are: Disable, Server and Client mode.
Server IP/Port	IP address and domain name are acceptable for Server IP.
Socket Type	Supports TCP/UDP protocol.

Item	Instructions
Socket Timeout	Router will transmit data to the serial port at the end of the defined time.
Serial Timeout	Serial Timeout is the wait time for transmitting the data package that is less than the Packet payload. 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 heartbeat to the defined server to keep the router online. This is convenient to monitor the router from the server.
Heart-beat Interval	Heart-beat interval time.
Baud Rate	115200 as default.
Parity Bit	None as default.
Data Bit	8bit as default.
Stop Bit	1bit as default.

NOTE

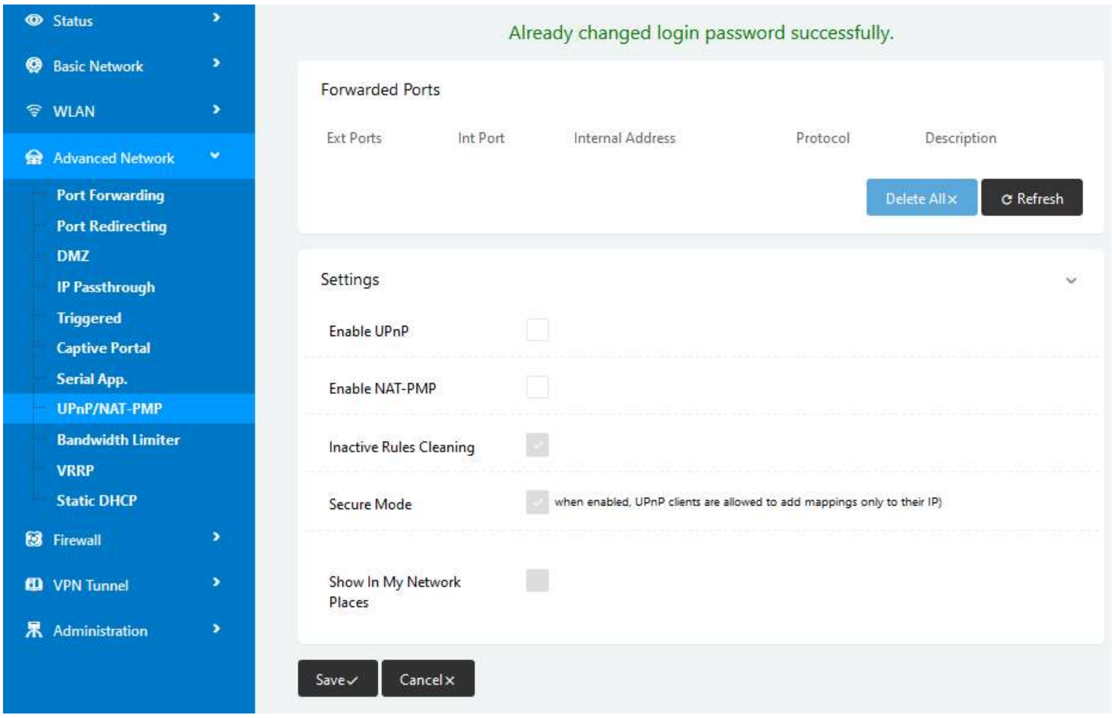
Serial port connection

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

Step 2 Click ”save” to finish.

2.6.8 UPnP/NAT-PMP Settings

Step 1 Go to Advanced Network> UPnP/NAT-PMP, to check or modify the relevant parameters.



Already changed login password successfully.

Forwarded Ports

Ext Ports	Int Port	Internal Address	Protocol	Description

Settings

Enable UPnP □

Enable NAT-PMP □

Inactive Rules Cleaning ☑

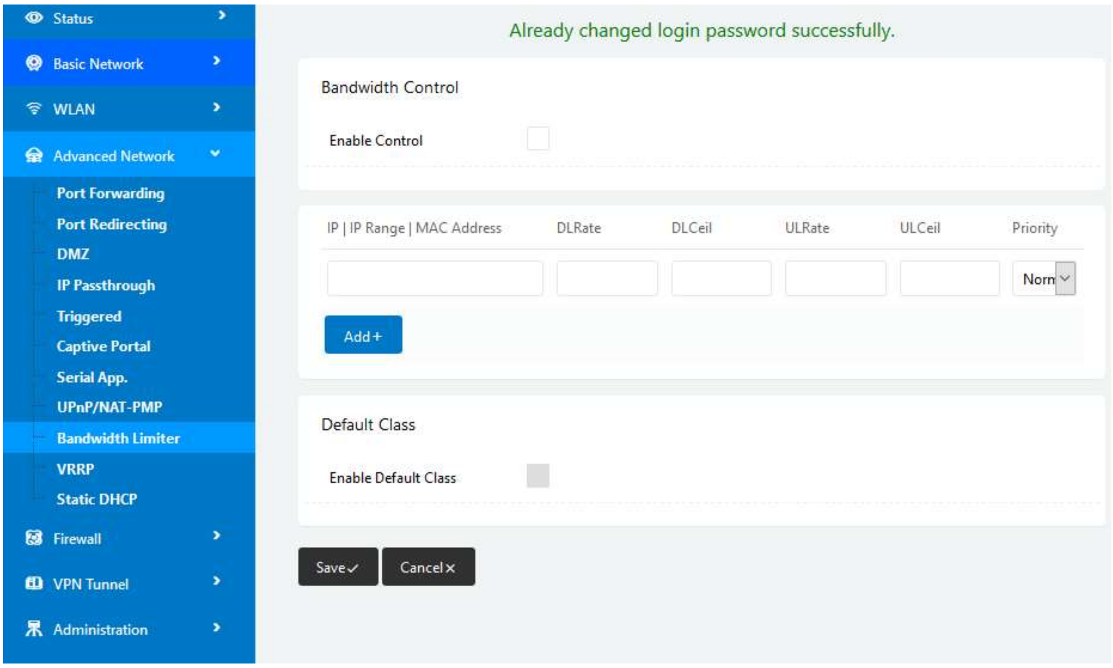
Secure Mode ☑ when enabled, UPnP clients are allowed to add mappings only to their IP)

Show In My Network Places □

Step 2 Click ”save” to finish.

2.6.9 Bandwidth Control Settings

Step 1 Go to Advanced Network> Bandwidth Control, to check or modify the relevant parameters.



Already changed login password successfully.

Bandwidth Control

Enable Control □

IP | IP Range | MAC Address	DLRate	DLCeil	ULRate	ULCeil	Priority
					Norn

Default Class

Enable Default Class □

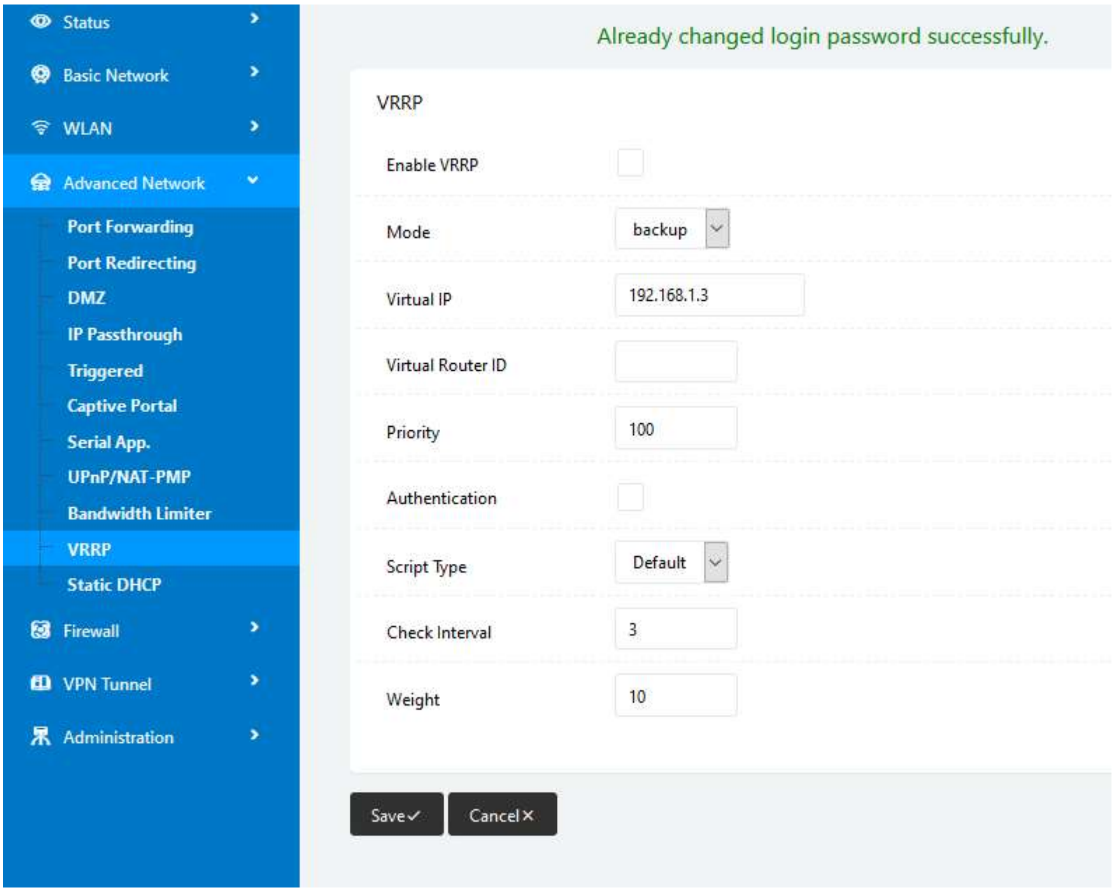
Table 2-15 Bandwidth Control Instructions

Max Available Download	Maximum download speed available.
Max Available Upload	Maximum upload speed available.
IP/ IP Range/ MAC Address	Limits devices speed for specified IP/ IP Range/ MAC Address.
DL Rate	Max download rate.
DL ceil	Max download ceiling.
UL Rate	Max upload rate.
UL ceil	Max upload ceiling.
Priority	The priority for a specific user.
Default Class	If no IP/MAC are specified, the download and upload limits are total available speeds for all devices.

Step 2 Click ”save” to finish.

2.6.10 VRRP Settings

Step 1 Go to Advanced Network> VRRP to check or modify the relevant parameters.



Already changed login password successfully.

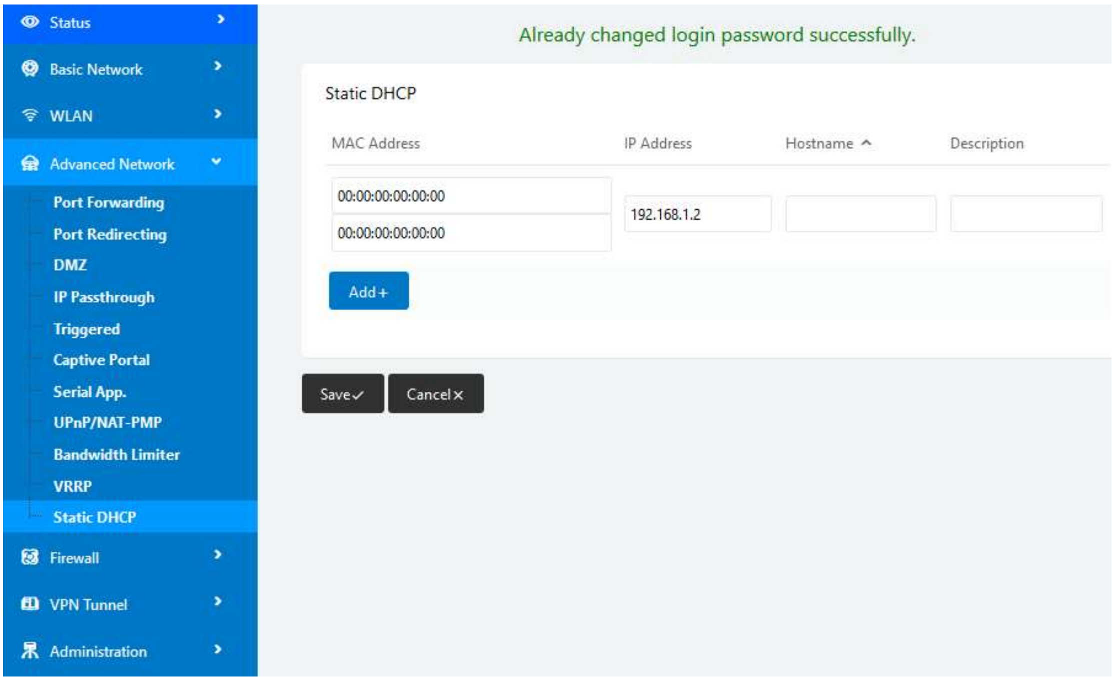
VRRP

Enable VRRP	□
Mode	backup
Virtual IP	192.168.1.3
Virtual Router ID	
Priority	100
Authentication	□
Script Type	Default
Check Interval	3
Weight	10

Step 2 Click ”save” to finish.

2.6.11 Static DHCP Settings

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



Already changed login password successfully.

Static DHCP

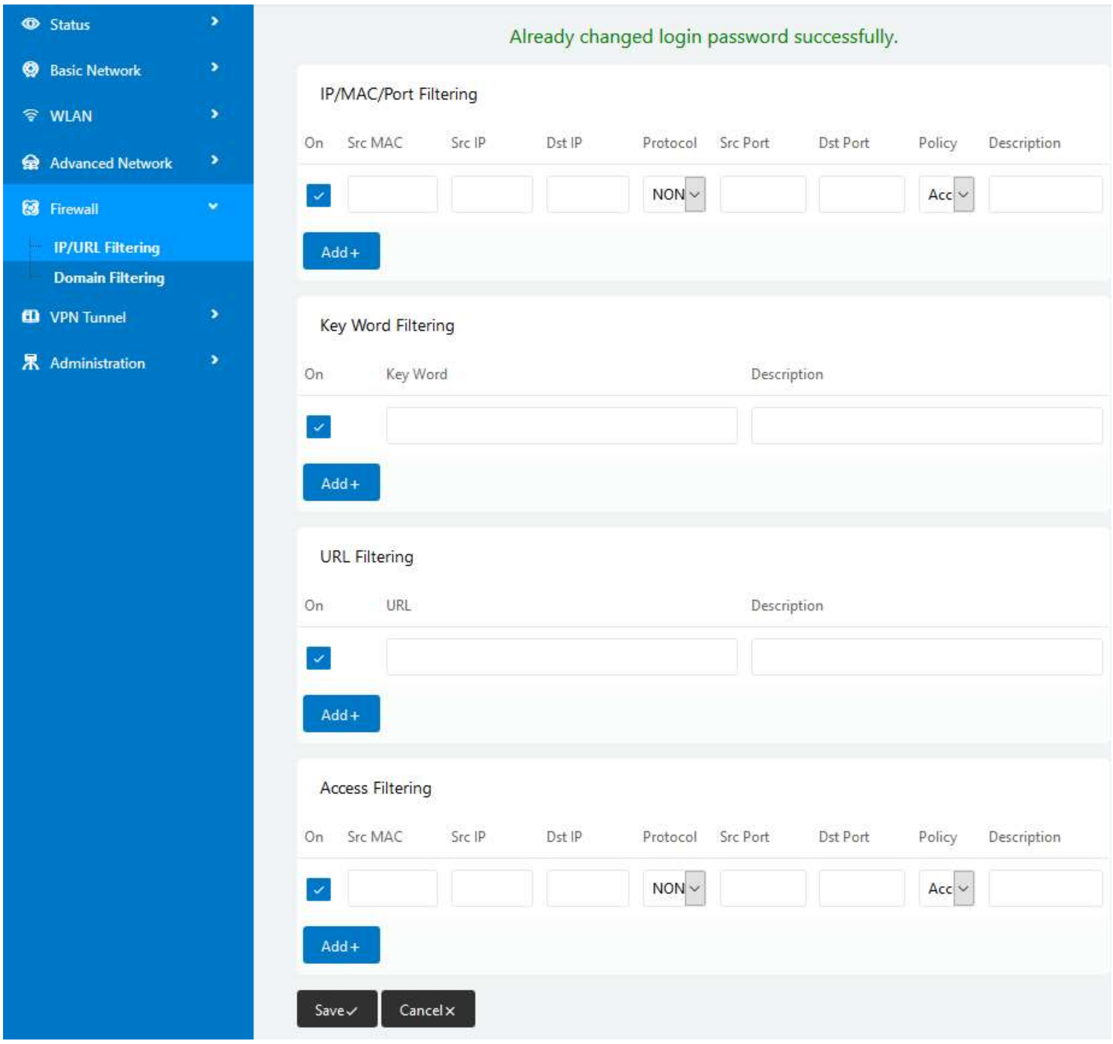
MAC Address	IP Address	Hostname	Description
00:00:00:00:00:00 00:00:00:00:00:00	192.168.1.2		

Step 2 Click ”save” to finish.

2.7 Firewall

2.7.1 IP/URL Filtering

Step 1 Go to Firewall> IP/URL Filtering, to check or modify the relevant parameters.



Already changed login password successfully.

IP/MAC/Port Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NON			Acc	

Key Word Filtering

On	Key Word	Description
☑		

URL Filtering

On	URL	Description
☑		

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NON			Acc	

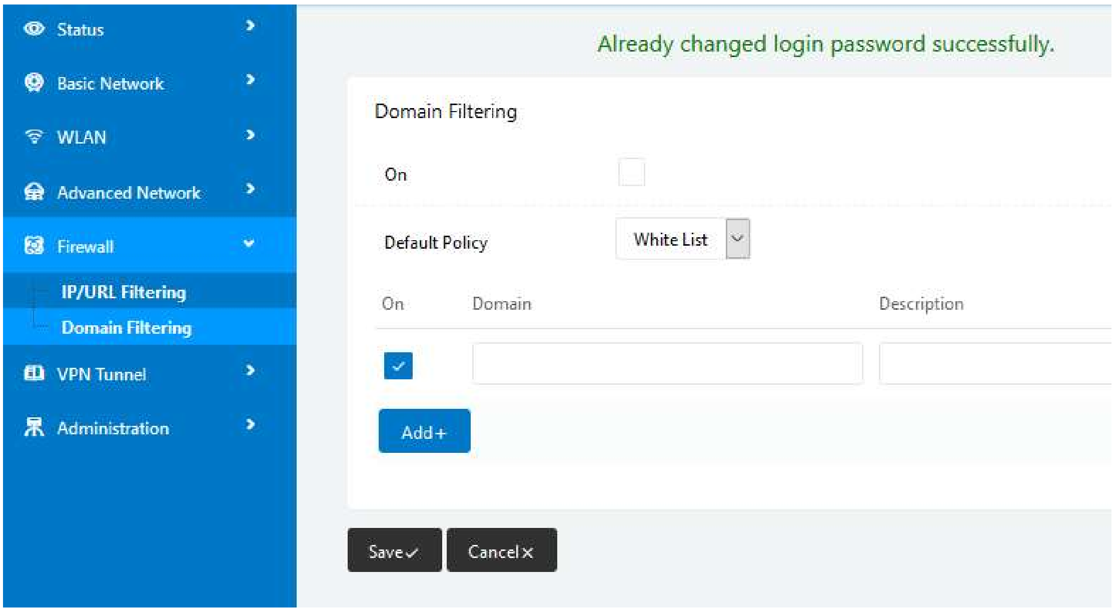
Table 2-16 IP/URL Filtering Instructions

Item	Instructions
IP/MAC/Port Filtering	Supports IP address, MAC address and Port filtering. “Accept/Drop” options for filter policy.
Keyword Filtering	Supports keyword filtering.
URL Filtering	Supports URL filtering.
Access Filtering	Supports Access filtering.

Step 2 Click ”save” to finish.

2.7.2 Domain Filtering

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



Already changed login password successfully.

Domain Filtering

On □

Default Policy: White List

On	Domain	Description
☑		

Table 2-17 Domain Filtering Instructions

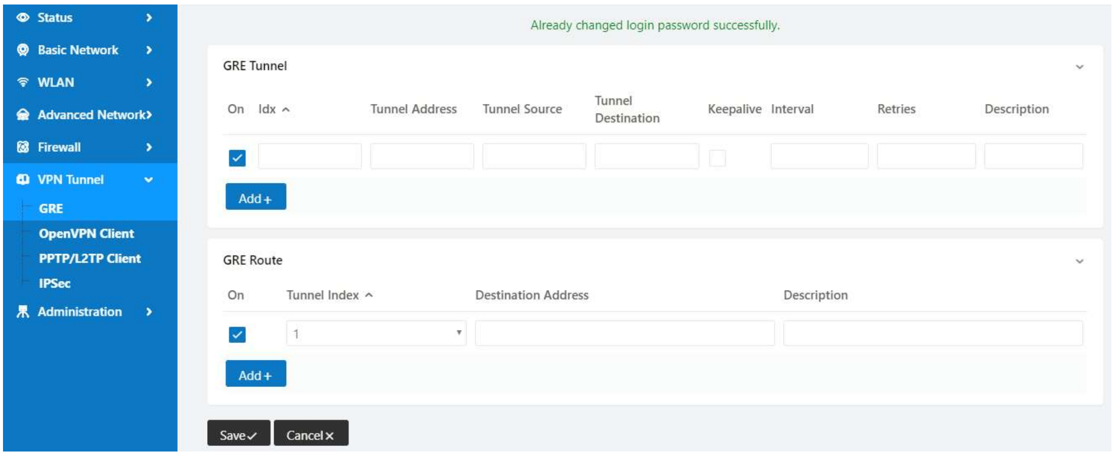
Item	Instructions
Default Policy	Supports blacklist and whitelist.
Local IP Address	Local IP address for LAN.
Domain	Supports Domain filtering.

Step 2 Click ”save” to finish.

2.8 VPN Tunnel

2.8.1 GRE Setting

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



Already changed login password successfully.

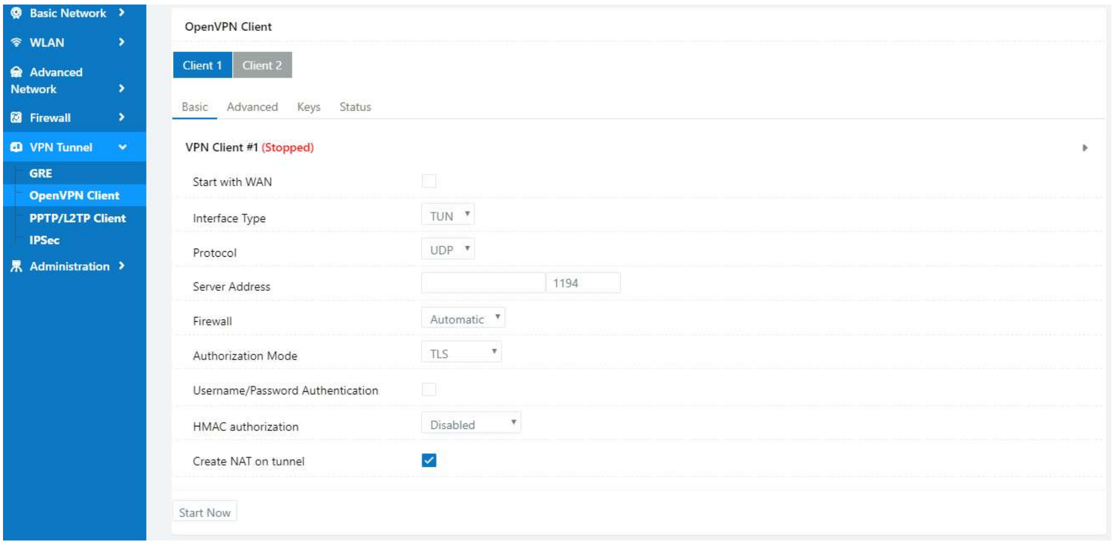
Table 2-18 GRE Instructions

Item	Instructions
IDx	GRE Tunnel number.
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.
Tunnel Source	Router’s 5G/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.
Description	

Step 2 Click ”save” to finish.

2.8.2 OpenVPN Client Setting

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



OpenVPN Client

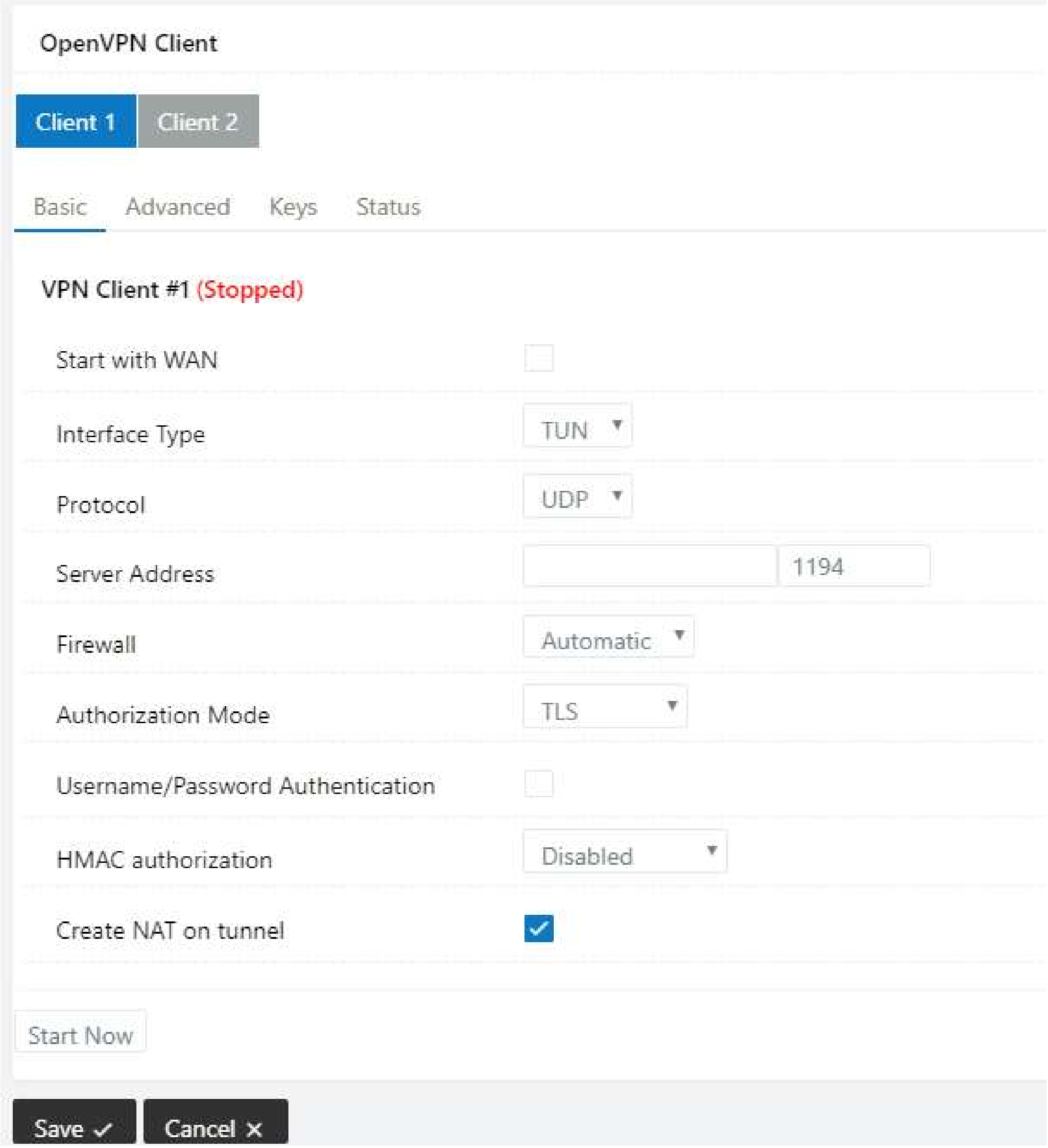
Client 1 | Client 2

Basic | Advanced | Keys | Status

VPN Client #1 (Stopped)

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

Start Now


OpenVPN Client

Client 1 | Client 2

Basic | Advanced | Keys | Status

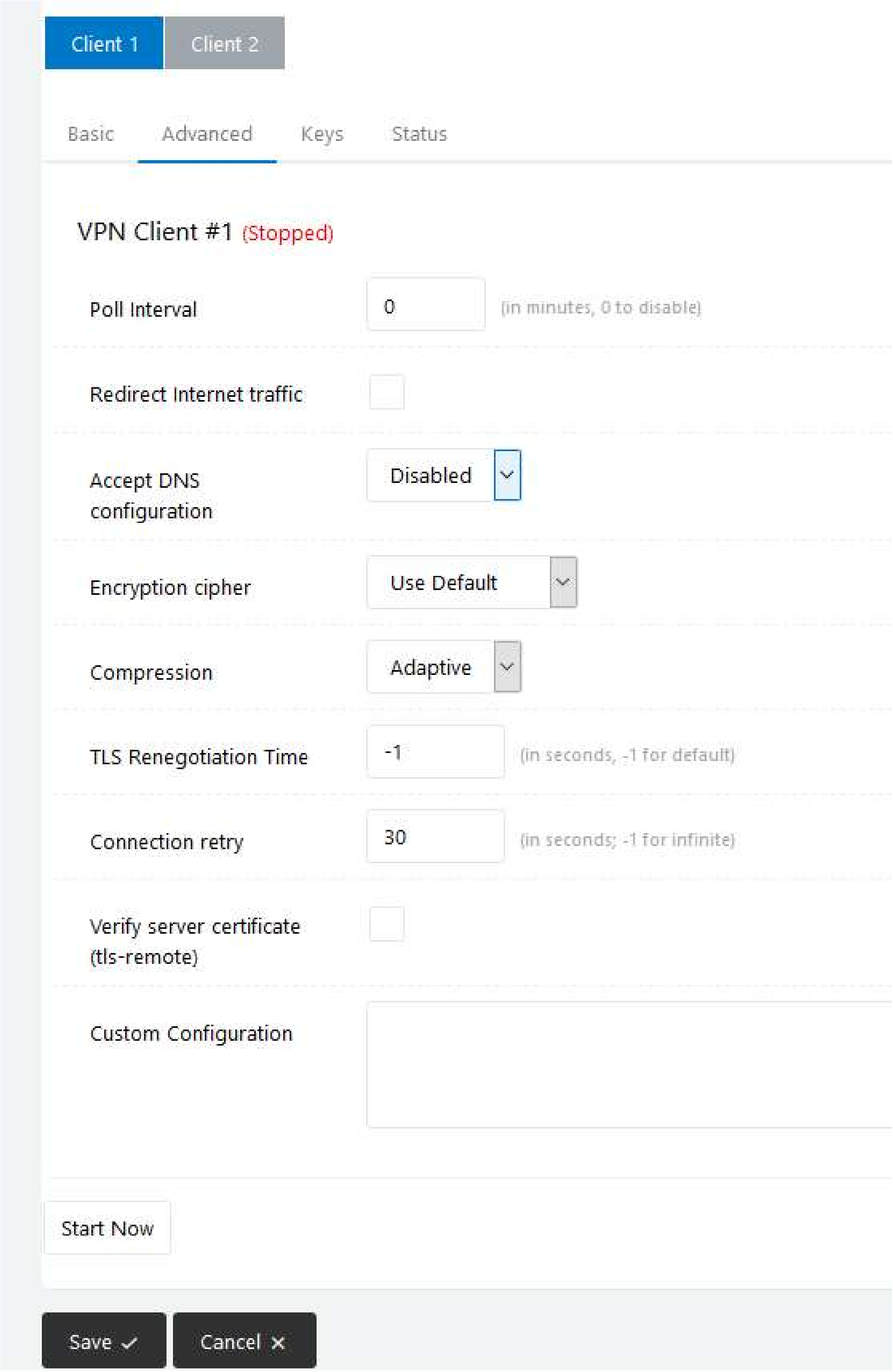
VPN Client #1 (Stopped)

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

Start Now

Table 2-19 Basic OpenVPN Instructions

Item	Instructions
Start with WAN	Enable the Openvpn feature for 5G/4G/3G/WAN port.
Interface Type	Tap and Tun type options available. Tap is for bridge mode and Tunnel is for routing mode.
Protocol	UDP and TCP options available.
Server Address	The Openvpn server public IP address and port.
Firewall	Automatic and Custom options available.
Authorization Mode	TLS, Static key and Custom options available.
Username/Password Authentication	As per user’s configuration.
HMAC authorization	As per user’s configuration.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.

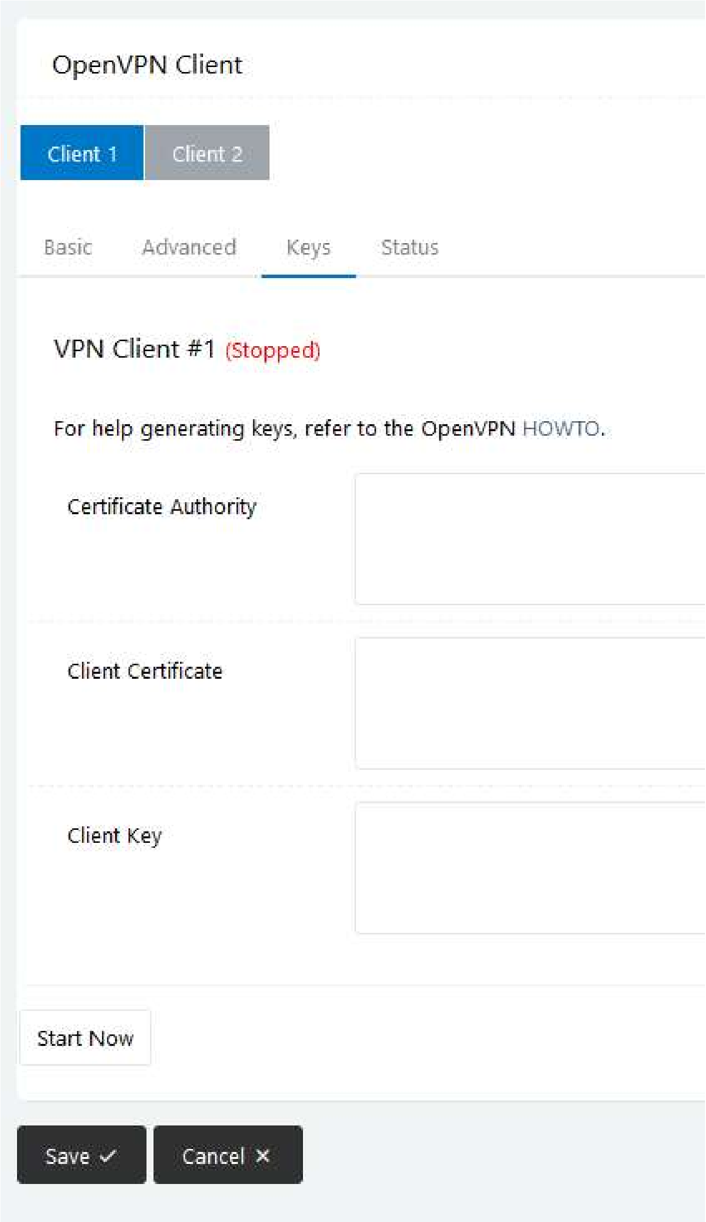


VPN Client #1 (Stopped)

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		

Table 2-20 Advanced OpenVPN Instructions

Item	Instructions
Poll Interval	Openvpn client checks router’s status at interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As per user’s configuration.
Encryption	As per user’s configuration.
Compression	As per user’s configuration.
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.
Connection Retry Time	Openvpn retry to connection interval.
Verify server certificate	As per user’s configuration.
Custom Configuration	As per user’s configuration.



OpenVPN Client

VPN Client #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

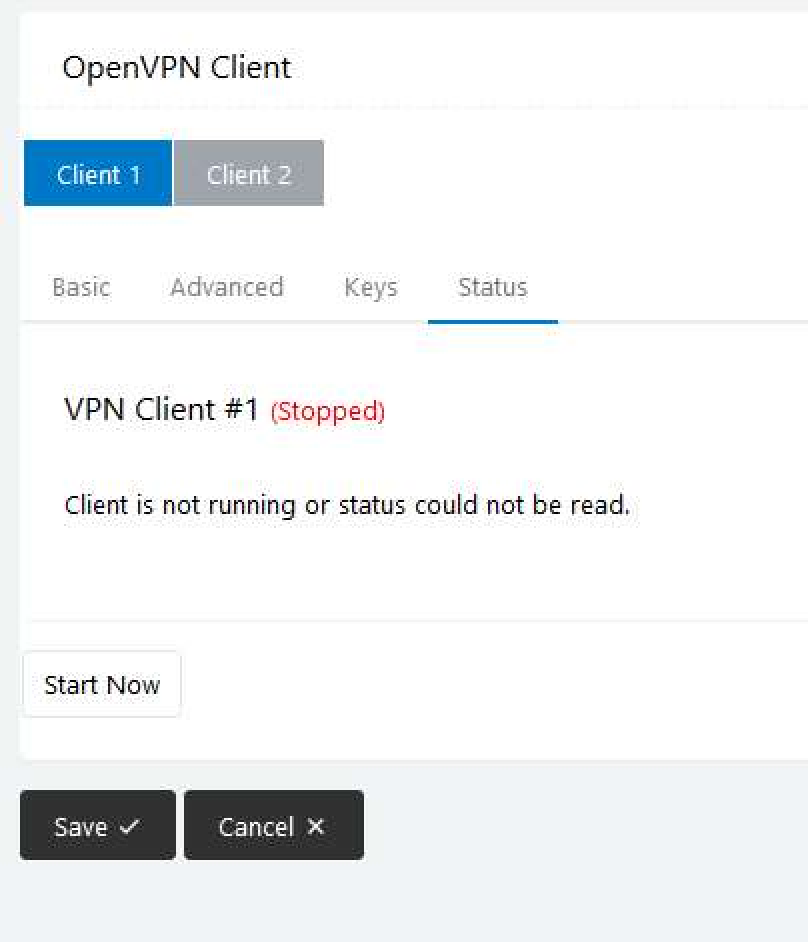
Certificate Authority

Client Certificate

Client Key

Table 2-21 Keys of OpenVPN Instructions

Item	Instructions
Certificate Authority	Keep certificate the same as the server.
Client Certificate	Keep client certificate the same as the server.
Client Key	Keep client key the same as the server.



VPN Client #1 (Stopped)

Client is not running or status could not be read.

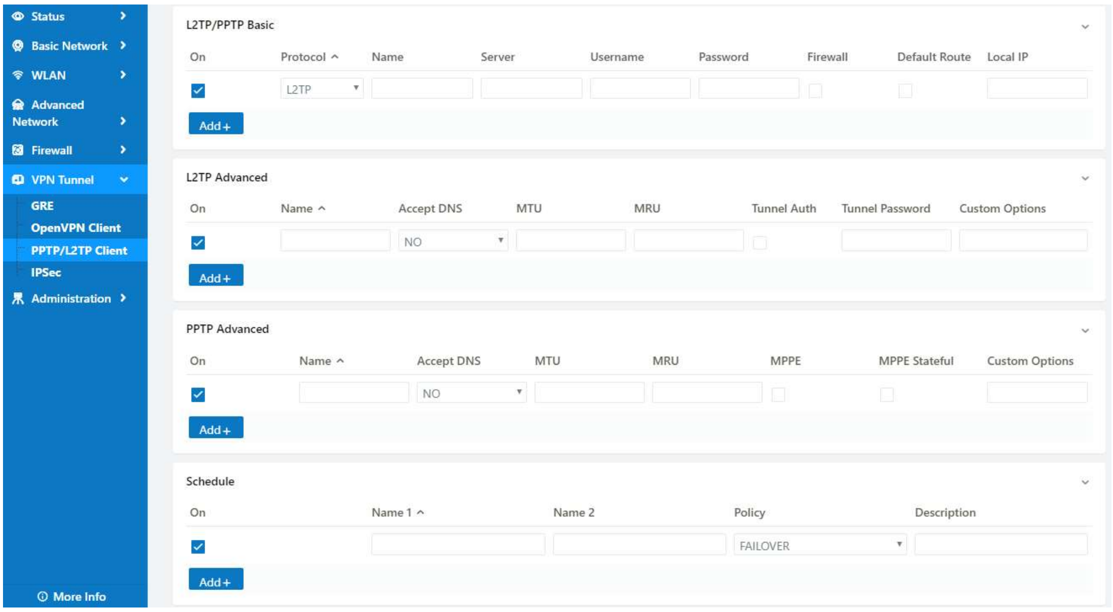
Table 2-22 Status of OpenVPN Instructions

Item	Instructions
Status	Check Openvpn status and data statistics.

Step 2 Click ”save” to finish.

2.8.3 VPN PPTP/L2TP Client Settings

Step 1 Go to VPN Tunnel> PPTP/L2TP Client to check or modify the relevant parameters.



L2TP/PPTP Basic

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
☑	L2TP					□	□	

Add+

L2TP Advanced

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

Add+

PPTP Advanced

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

Add+

Schedule

On	Name 1	Name 2	Policy	Description
☑			FAILOVER	

Add+

Table 2-23 PPTP/L2TP Basic Instructions

Item	Instructions
On	VPN enable.
Protocol	VPN Mode for PPTP and L2TP.
Name	VPN Tunnel name.
Server Address	VPN Server IP address.
Username	As per user’s configuration.
Password	As per user’s configuration.
Firewall	Firewall for VPN Tunnel.
Local IP	Defined Local IP address for tunnel.

Table 2-24 L2TP Advanced Instructions

On	L2TP Advanced enable.
Name	L2TP Tunnel name.
Accept DNS	As per user’s configuration.

MTU	MTU is 1450bytes as default.
MRU	MRU is 1450bytes as default.
Tunnel Auth.	L2TP authentication Optional as per user’s configuration.
Tunnel Password	As per user’s configuration.
Custom Options	As per user’s configuration.

Table 2-25 PPTP Advanced Instructions

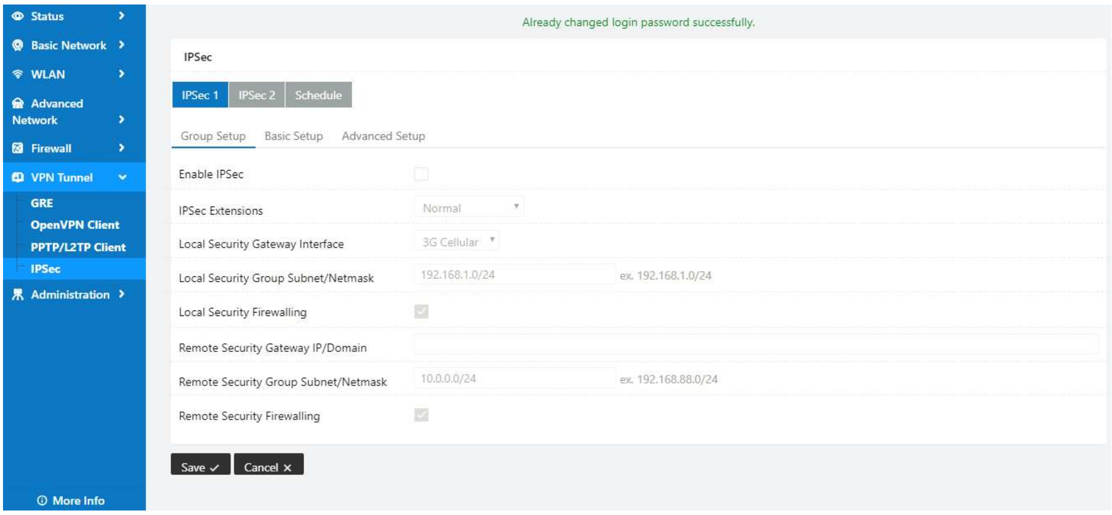
On	PPTP Advanced enable.
Name	PPTP Tunnel name.
Accept DNS	As per user’s configuration.
MTU	MTU is 1450bytes as default.
MRU	MRU is 1450bytes as default.
MPPE	As per user’s configuration.
MPPE Stateful	As per user’s configuration.
Customs	As per user’s configuration.

Table 2-26 SCHEDULE Instructions

On	VPN SCHEDULE feature enabled.
Name1	VPN tunnel name.
Name2	VPN tunnel name.
Policy	Supports VPN tunnel backup and failover modes.
Description	As per user’s configuration.

Step 2 Click ”save” to finish.

2.8.4 IPSec Settings



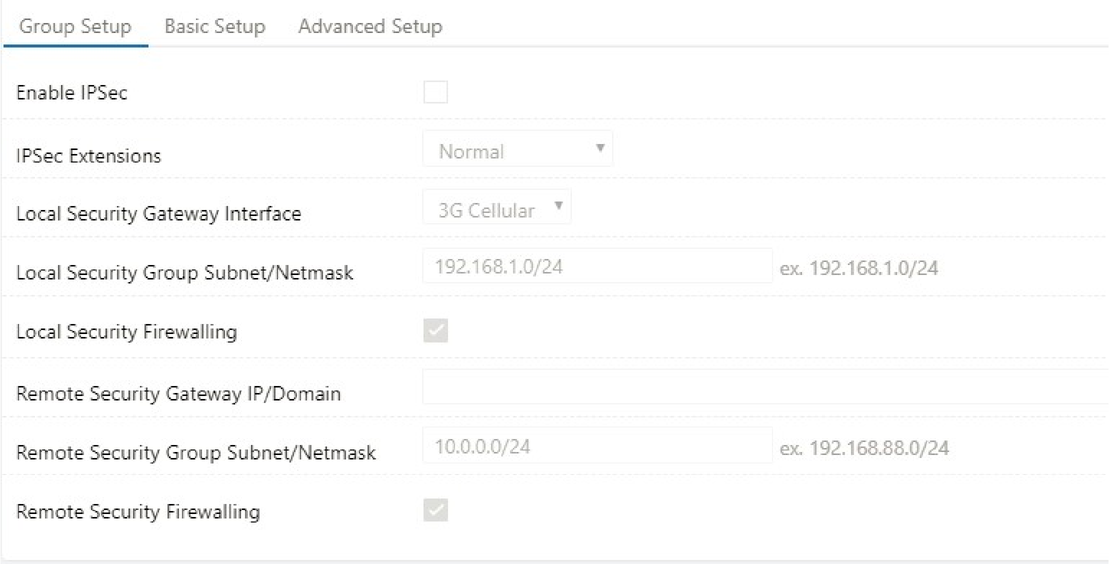
Already changed login password successfully.

IPSec

Enable IPSec	□	
IPSec Extensions	Normal	
Local Security Gateway Interface	3G Cellular	
Local Security Group Subnet/Netmask	192.168.1.0/24	ex. 192.168.1.0/24
Local Security Firewalling	☑	
Remote Security Gateway IP/Domain		
Remote Security Group Subnet/Netmask	10.0.0.0/24	ex. 192.168.88.0/24
Remote Security Firewalling	☑	

2.8.4.1 IPSec Group Setup

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



Enable IPSec	□	
IPSec Extensions	Normal	
Local Security Gateway Interface	3G Cellular	
Local Security Group Subnet/Netmask	192.168.1.0/24	ex. 192.168.1.0/24
Local Security Firewalling	☑	
Remote Security Gateway IP/Domain		
Remote Security Group Subnet/Netmask	10.0.0.0/24	ex. 192.168.88.0/24
Remote Security Firewalling	☑	

Table 2-27 IPSec Group Setup Instructions

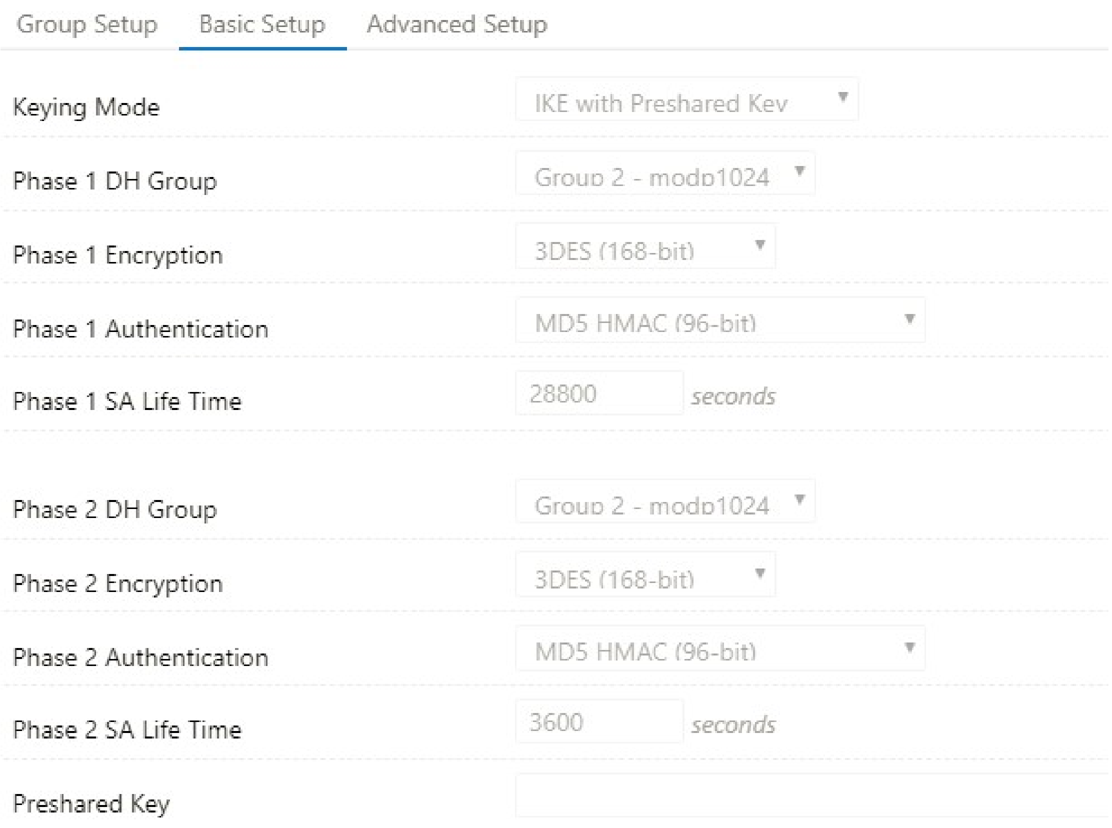
Item	Instructions
IPSec Extensions	Supports Standard IPSec, GRE over IPSec, L2TP over IPSec.
Local Security Interface	Defines the IPSec security interface.
Local Subnet/Mask	IPSec local subnet and mask.

Item	Instructions
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 Click ”save” to finish.

2.8.4.2 IPSec Basic Setup

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



Keying Mode: IKE with Preshared Kev

Phase 1 DH Group: Group 2 - modp1024

Phase 1 Encryption: 3DES (168-bit)

Phase 1 Authentication: MD5 HMAC (96-bit)

Phase 1 SA Life Time: 28800 seconds

Phase 2 DH Group: Group 2 - modp1024

Phase 2 Encryption: 3DES (168-bit)

Phase 2 Authentication: MD5 HMAC (96-bit)

Phase 2 SA Life Time: 3600 seconds

Preshared Key:

Table 2-28 IPSec Basic Setup Instructions

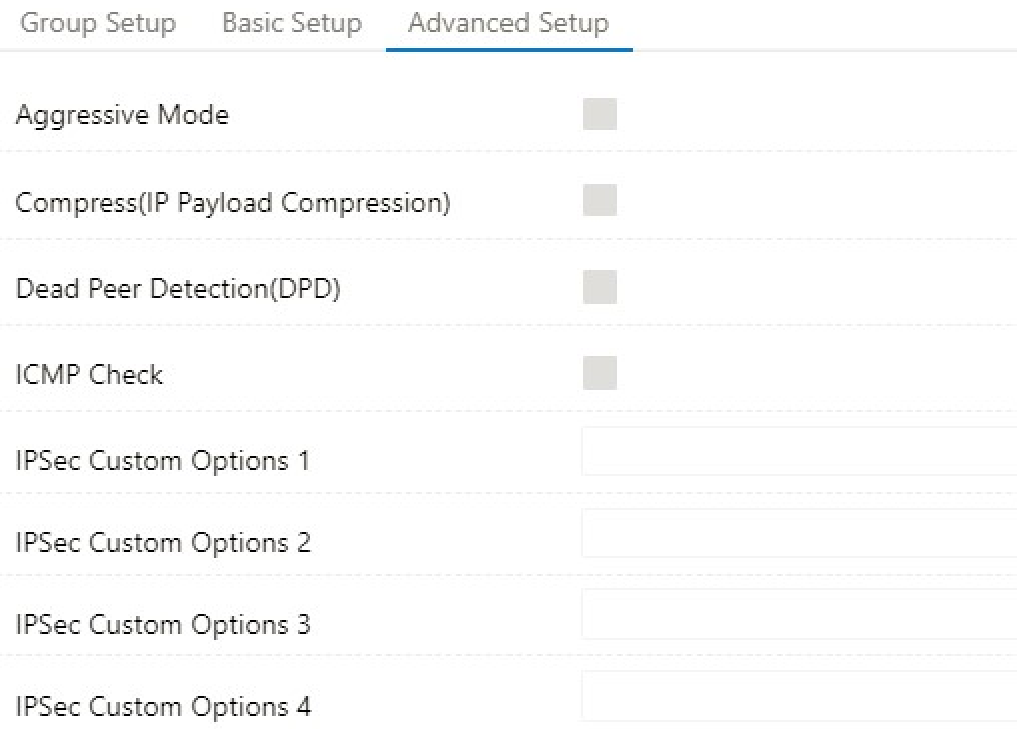
Item	Instructions
Keying Mode	IKE pre-shared key.
Phase 1 DH Group	Select Group1, Group2, Group5 from the list. This must match the remote IPSec settings.

Item	Instructions
Phase 1 Encryption	Supports 3DES, AES-128, AES-192, AES-256.
Phase 1 Authentication	Supports HASH MD5 and SHA.
Phase 1 SA Lifetime	IPSec Phase 1 SA lifetime.
Phase 2 DH Group	Select Group1, Group2, Group5 from the list. This must match the remote IPSec settings.
Phase 2 Encryption	Supports 3DES, AES-128, AES-192, AES-256.
Phase 2 Authentication	Supports HASH MD5 and SHA.
Phase 2 SA Lifetime	IPSec Phase 2 SA lifetime.
Pre-shared Key	Pre-shared Key.

Step 2 Click ”save” to finish.

2.8.4.3 IPSec Advanced Setup

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



Aggressive Mode	□
Compress(IP Payload Compression)	□
Dead Peer Detection(DPD)	□
ICMP Check	□
IPSec Custom Options 1	
IPSec Custom Options 2	
IPSec Custom Options 3	
IPSec Custom Options 4	

Table 2-29 IPSec Advanced Setup Instructions

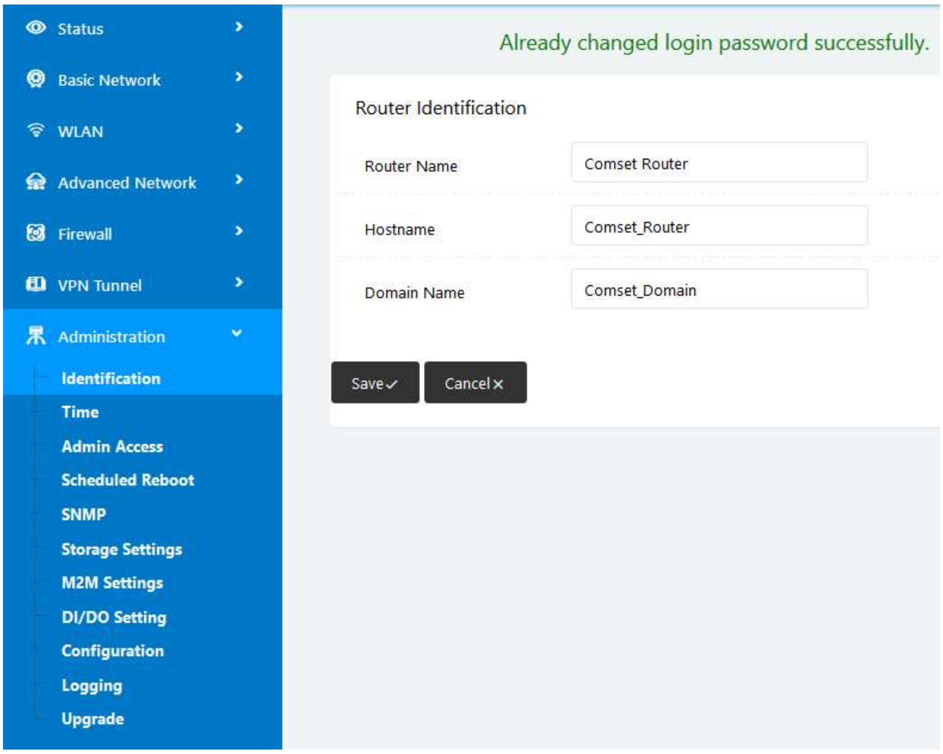
Item	Instructions
Aggressive Mode	Default for main mode.
ID Payload Compress	Enable ID Payload compress.
DPD	To enable DPD service.
ICMP	ICMP Check for IPSec tunnel.
IPSec Custom Options	IPSec advanced settings such as left/right ID.

Step 2 Click ”save” to finish.

2.9 Administration

2.9.1 Identification Settings

Step 1 Go to Administration> Identification to enter the GUI, you may modify the router name, Host name and Domain name as required.



Already changed login password successfully.

Router Identification

Router Name: Comset Router

Hostname: Comset_Router

Domain Name: Comset_Domain

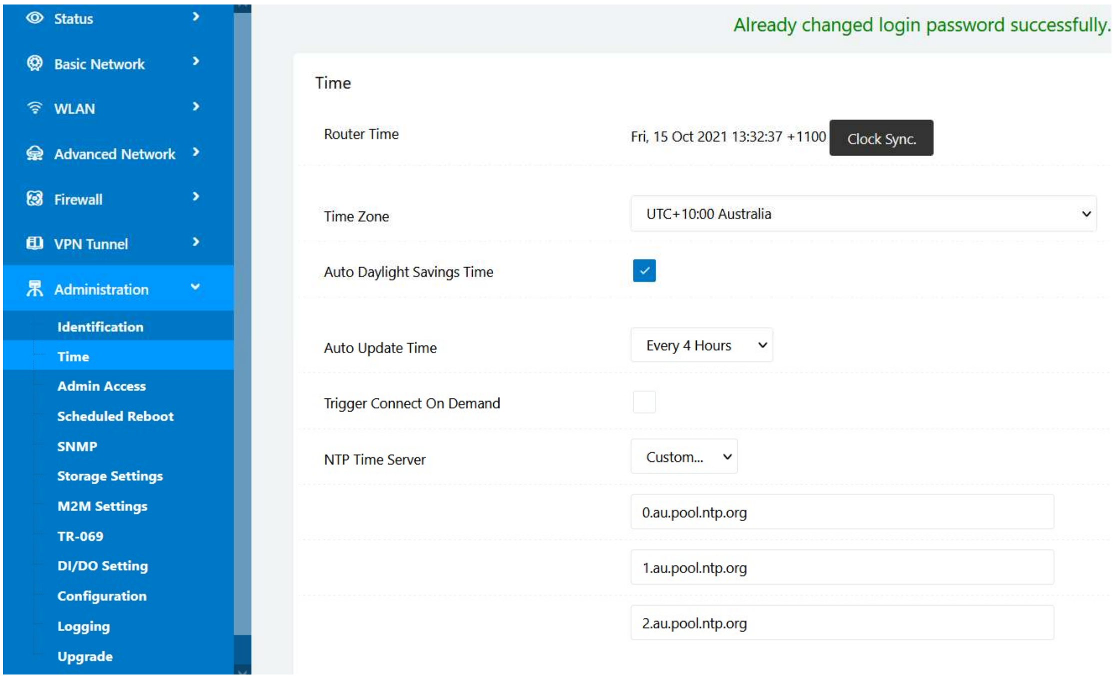
Table 2-30 Router Identification Instructions

Item	Description
Router name	Default is Comset Router. Maximum is 32 characters.
Host name	Default is Comset_Router. Maximum is 32 characters.
Domain name	Default is Comset_Domain. Maximum is 32 characters. This is the WAN domain. There is no need to configure it in most applications.

Step 2 Click ”save” to finish

2.9.2 Time Settings

Step 1 Go to “Administration> Time” to check or modify the relevant parameters.



Already changed login password successfully.

Time

Router Time	Fri, 15 Oct 2021 13:32:37 +1100
Time Zone	UTC+10:00 Australia
Auto Daylight Savings Time	☑
Auto Update Time	Every 4 Hours
Trigger Connect On Demand	□
NTP Time Server	Custom...
	0.au.pool.ntp.org
	1.au.pool.ntp.org
	2.au.pool.ntp.org

CAUTION

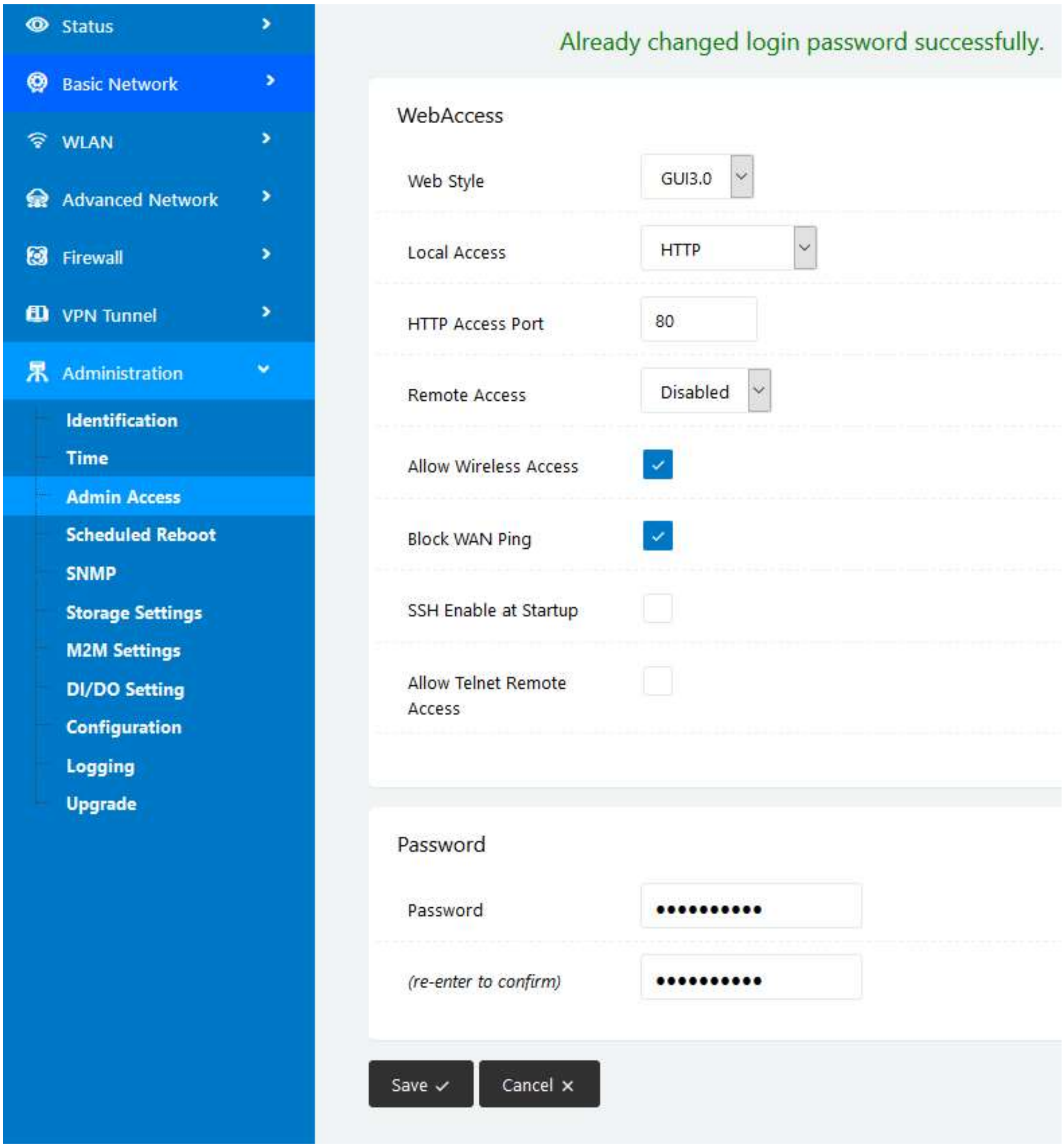
If the time fails to update, try a different NTP Time Server.

Step 2 Click “save” to finish.

2.9.3 Admin Access Settings

Step 1 Go to “Administration>Admin Access” to check and modify relevant parameters.

In this page, you can configure the basic web parameters.



Already changed login password successfully.

WebAccess

Web Style: GUI3.0

Local Access: HTTP

HTTP Access Port: 80

Remote Access: Disabled

Allow Wireless Access: ☑

Block WAN Ping: ☑

SSH Enable at Startup: □

Allow Telnet Remote Access: □

Password

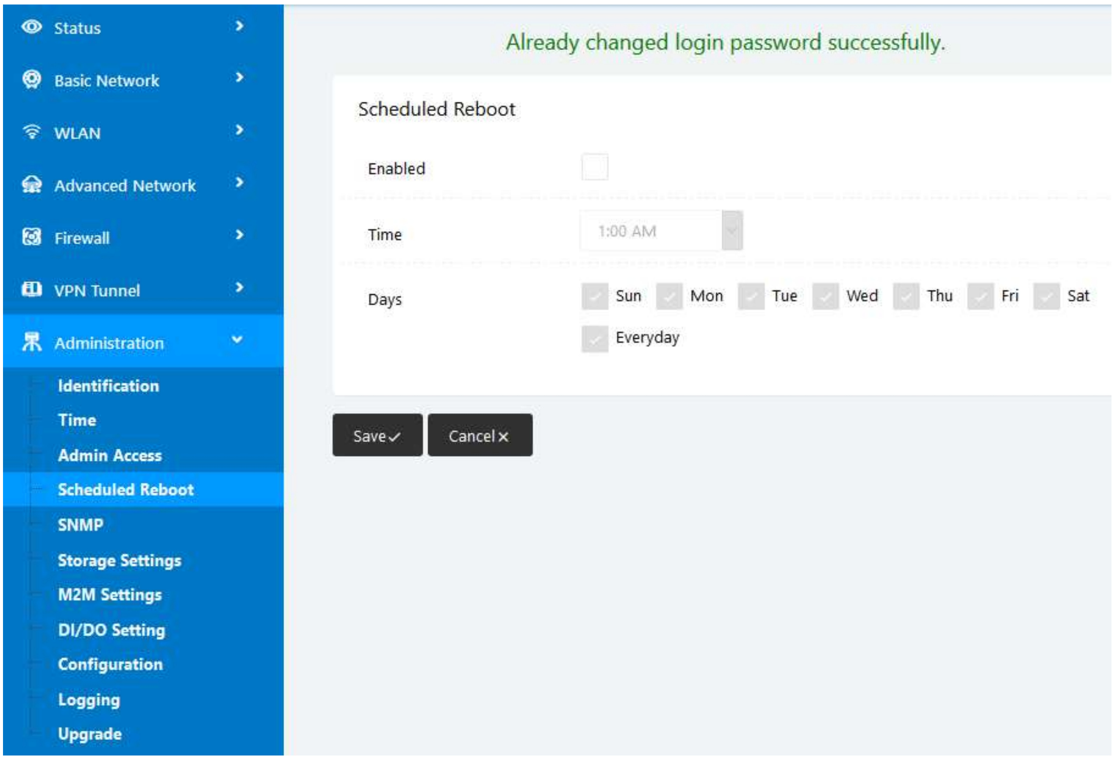
Password: ●●●●●●●●●●

(re-enter to confirm): ●●●●●●●●●●

Step 2 Click “Save” to finish.

2.9.4 Schedule Reboot Settings

Step 1 Go to “Administration>Schedule Reboot” to check and modify relevant parameters.



Already changed login password successfully.

Scheduled Reboot

Enabled □

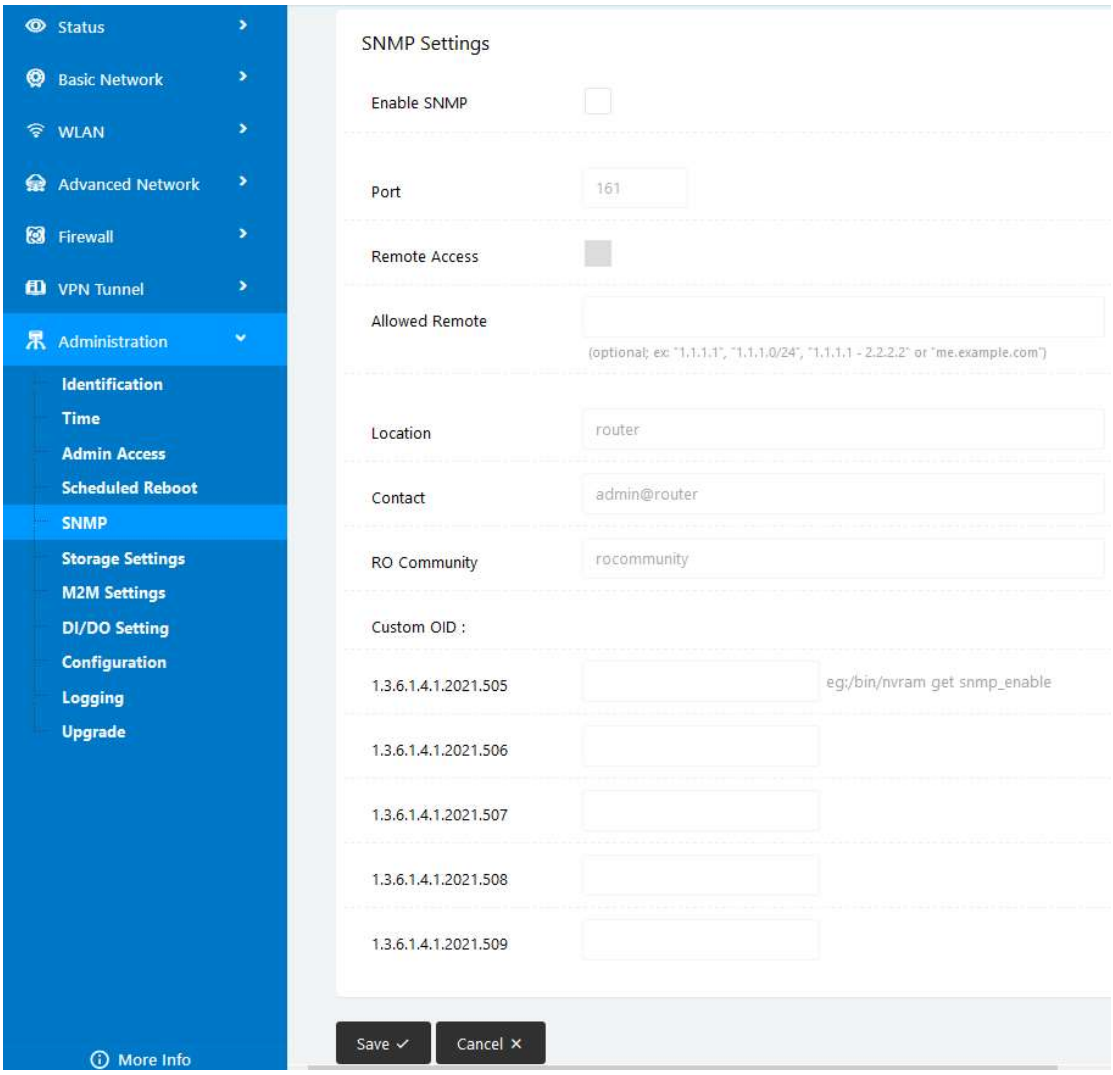
Time 1:00 AM

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

Step 2 Click “Save” to finish.

2.9.5 SNMP Settings

Step 1 Go to “Administration>SNMP” to check and modify relevant parameters.



SNMP Settings

Enable SNMP □

Port 161

Remote Access □

Allowed Remote

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

Location router

Contact admin@router

RO Community rocommunity

Custom OID :

1.3.6.1.4.1.2021.505 eg:/bin/nvram get snmp_enable

1.3.6.1.4.1.2021.506

1.3.6.1.4.1.2021.507

1.3.6.1.4.1.2021.508

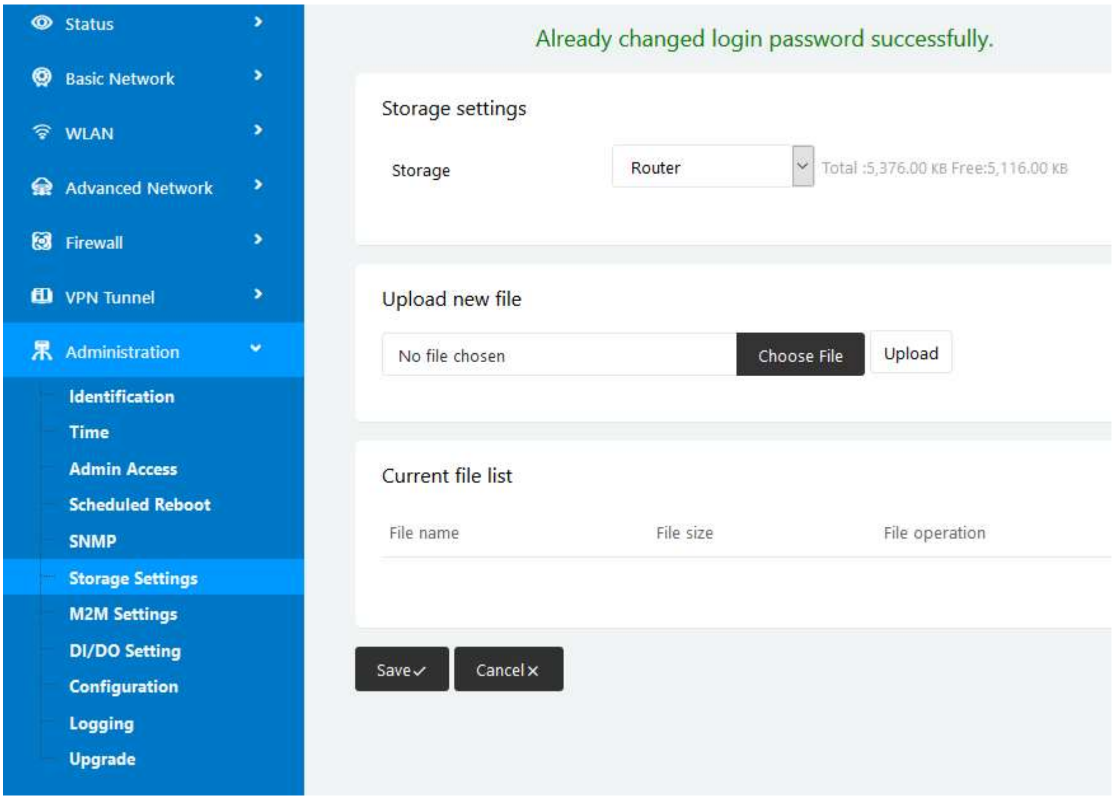
1.3.6.1.4.1.2021.509

Save ✓ Cancel ✕

Step 2 Click “Save” to finish.

2.9.6 Storage Settings

Step 1 Go to “Administration>Storage Settings” to check and modify relevant parameters.



Already changed login password successfully.

Storage settings

Storage: Router — Total :5,376.00 KB Free:5,116.00 KB

Upload new file

No file chosen

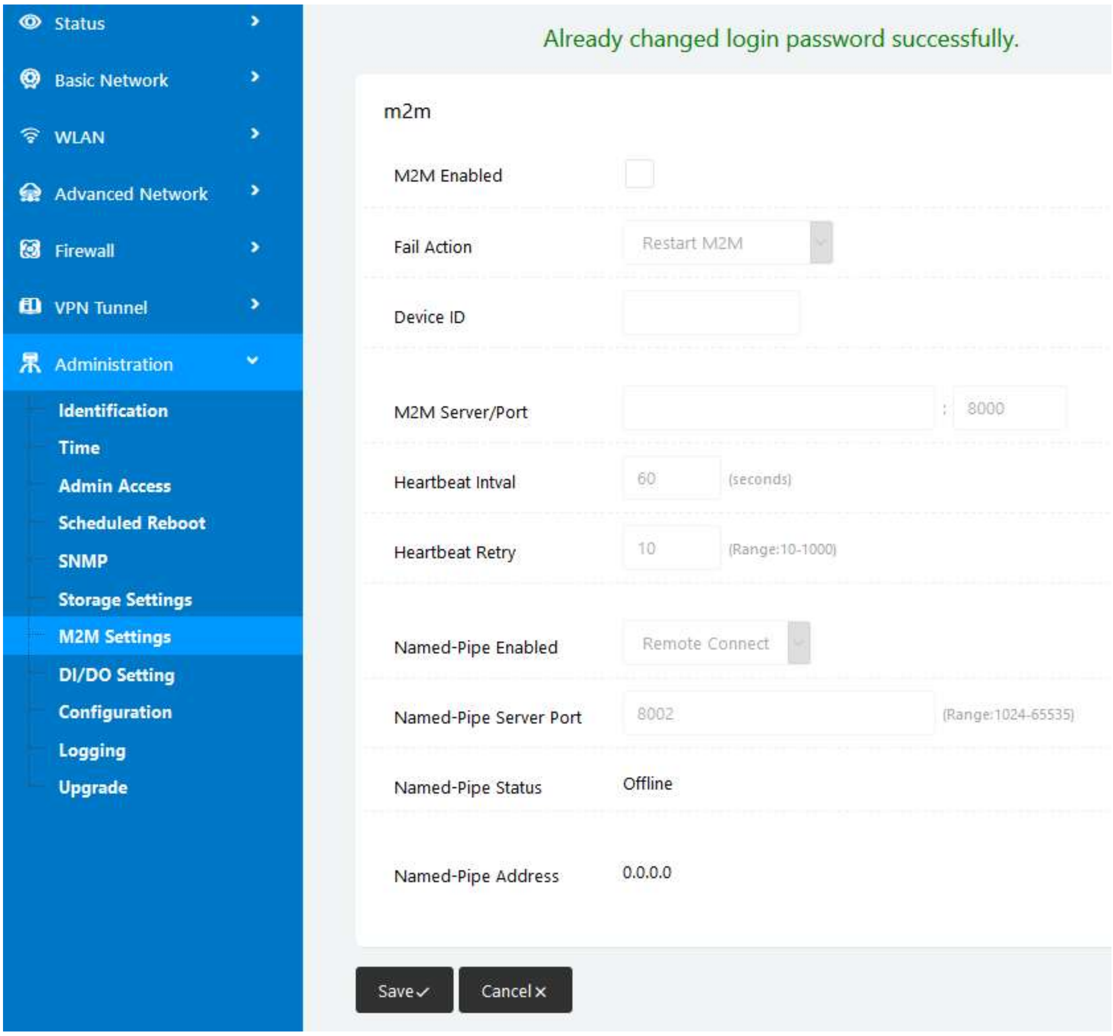
Current file list

File name	File size	File operation

Step 2 Click “Save” to finish.

2.9.7 M2M Settings

Step 1 Go to “Administration>M2M Settings” to check and modify relevant parameters.



Already changed login password successfully.

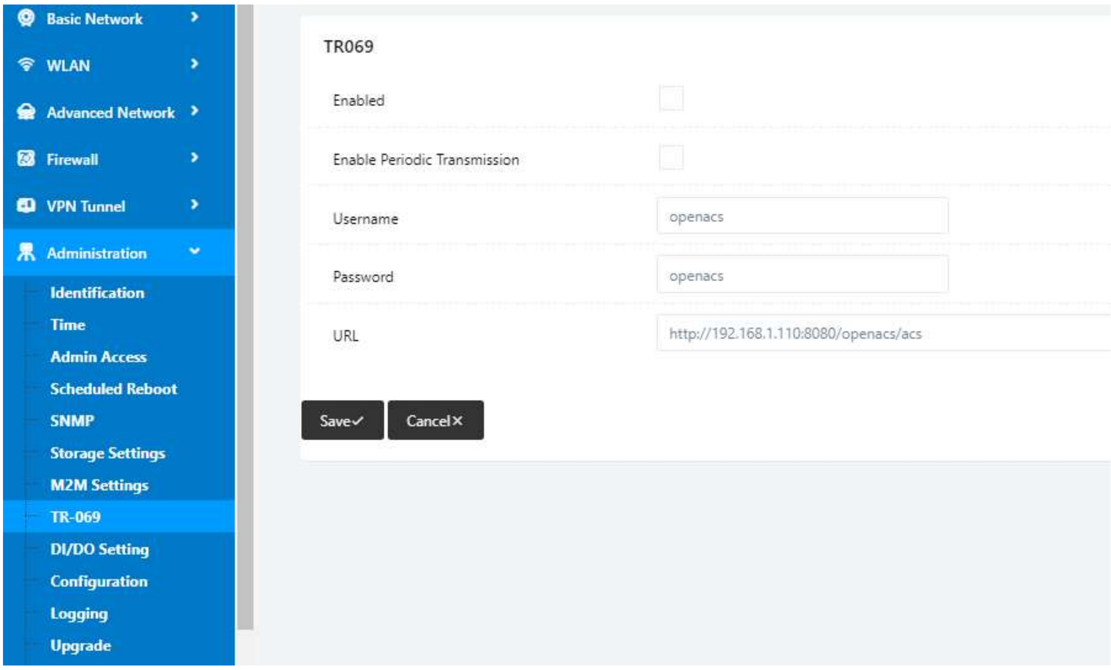
m2m

M2M Enabled	□
Fail Action	Restart M2M
Device ID	
M2M Server/Port	: 8000
Heartbeat Intval	60 (seconds)
Heartbeat Retry	10 (Range:10-1000)
Named-Pipe Enabled	Remote Connect
Named-Pipe Server Port	8002 (Range:1024-65535)
Named-Pipe Status	Offline
Named-Pipe Address	0.0.0.0

Step 2 Click “save” to finish.

2.9.8 TR-069 Settings

Step 3 Please click “Administration>TR-069 Settings” to check and modify relevant parameters.



TR069

Enabled □

Enable Periodic Transmission □

Username: openacs

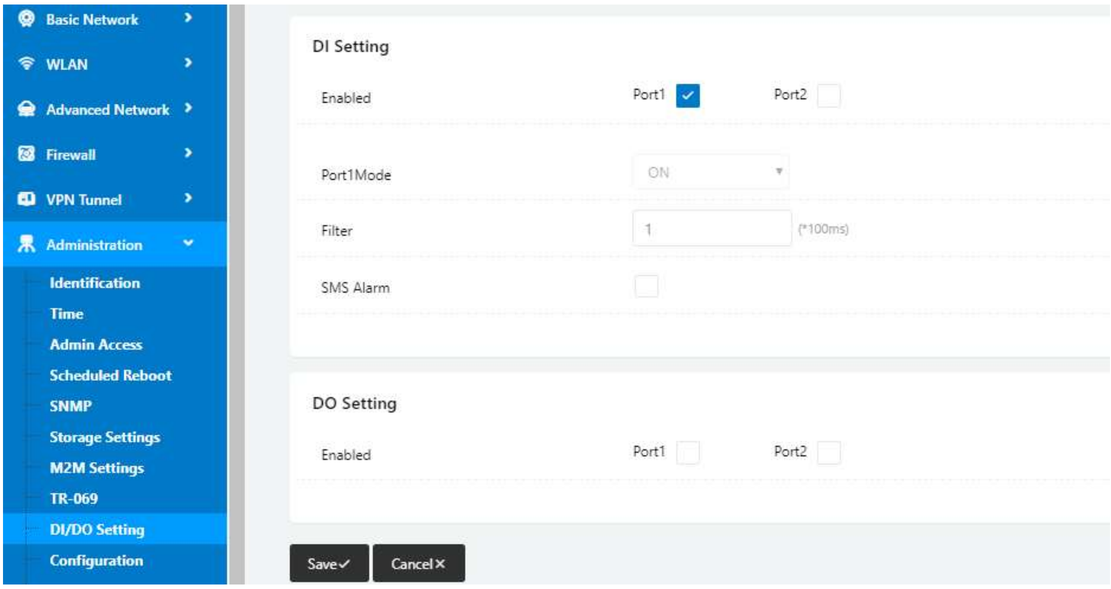
Password: openacs

URL: http://192.168.1.110:8080/openacs/acs

Step 4 Click “Save” to finish.

2.9.9 DI/DO Setting

Step 1 Go to “Administration>DI/DO Settings” to check and modify relevant parameters.



DI Setting

Enabled Port1 ☑ Port2 □

Port1Mode: ON

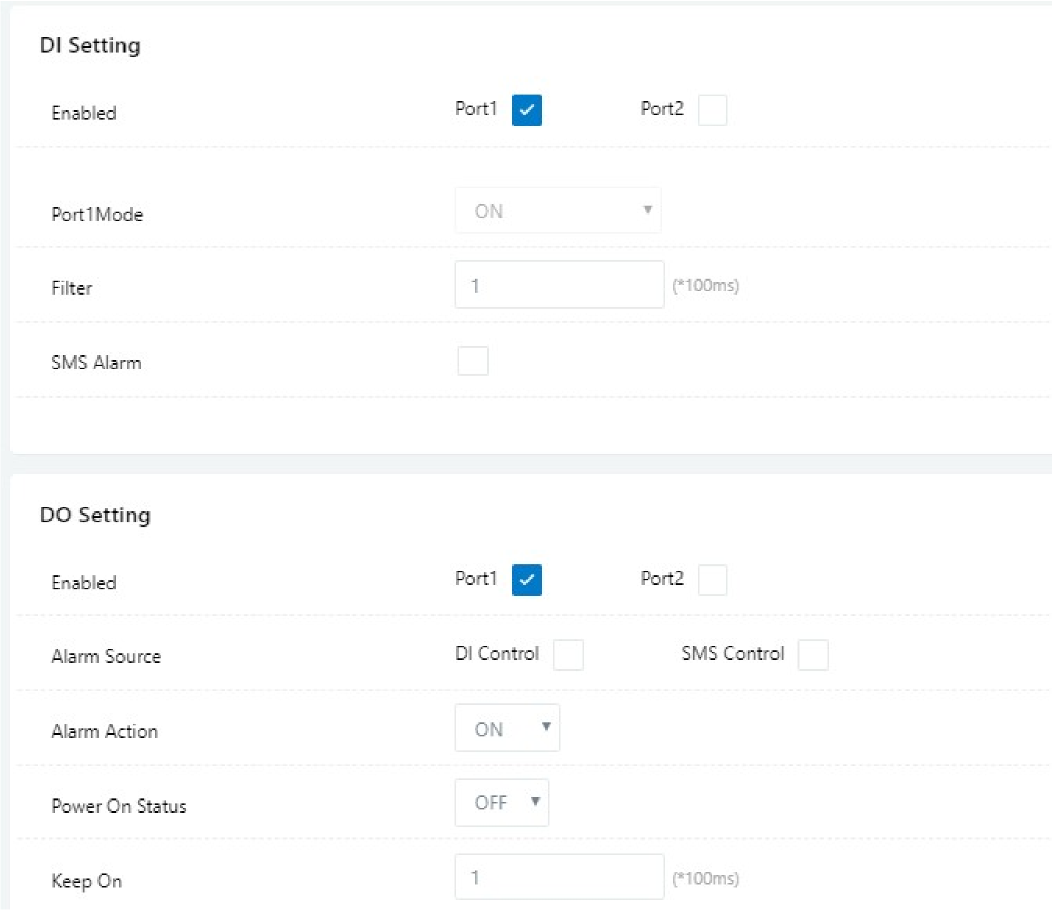
Filter: 1 (*100ms)

SMS Alarm □

DO Setting

Enabled Port1 □ Port2 □

2.9.7.1 DI Configuration



DI Setting

Enabled Port1 ☑ Port2 □

Port1Mode ON

Filter 1 (*100ms)

SMS Alarm □

DO Setting

Enabled Port1 ☑ Port2 □

Alarm Source DI Control □ SMS Control □

Alarm Action ON

Power On Status OFF

Keep On 1 (*100ms)

Table 2-31 DI Instructions

Item	Description
Enable	Enable DI. Port1 is for I/O-1 and Port2 is for I/O-2. Both I/O-1 and I/O-2 are DI ports.
Mode	Selected from OFF, ON and EVENT_COUNTER modes. OFF Mode: When DI changes from High (3.3V) to Low (0V), the alarm is triggered. ON Mode: When DI changes from Low (0V) to High (3.3V), the alarm is triggered. EVENT_COUNTER Mode: Enter EVENT_COUNTER mode.
Filter	Software filtering is used to control switch bounces. Input (1~100)*100ms. Under ON and OFF modes, the CM550W-POE detects the pulse signals and compares them with the first pulse shape and the last pulse shape. If both are at the same level, the CM550W-POE will trigger an alarm. Under EVENT_COUNTER mode, if the first pulse shape and the last

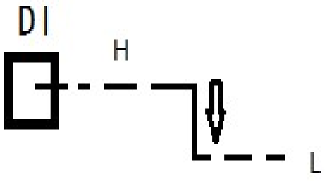
Item	Description
	pulse shape are not at the same level, the CM550W-POE will trigger an alarm according to the Counter Action settings.
Counter Trigger	Available when the DI is under Event Counter mode. Input from 0 to 100. "0" means the alarm is not triggered. The alarm will be triggered when the counter reaches the set value. After the alarm is triggered, the DI will keep counting but will not trigger the alarm again.
Counter Period	This is a reachable IP address. Once the ICMP check fails, GRE will be re-established.
Counter Recover	It will re-count after a counter trigger alarm. The value is 0~30000(*100ms). "0" means no counter.
Counter Action	HI_TO_LO and LO_TO_HI is available when the DI is under Event Counter mode. In Event Counter mode, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When LO_TO_HI is selected, the counter value increases when the attached switch is pushed. When HI_TO_LO is selected, thecounter value increases when the switch is pushed and released.
Counter Start	Available when the DI is under EVENT_COUNTER mode. The counting starts when you enable this feature.
SMS Alarm	The alarm SMS will send a text to a specified phone group. Each phone group contains up to 2 phone numbers.
SMS Content	70 ASCII Char Max.
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 2 Click "Save" to finish.

NOTE

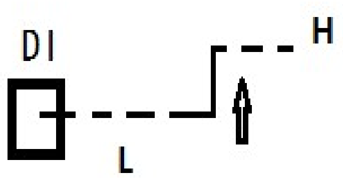
OFF Mode

DI from high level 3.3~5V to low level 0V will be triggered.



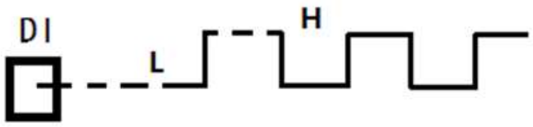
ON Mode

DI from low level 0V to high level 3.3~5V will be triggered.

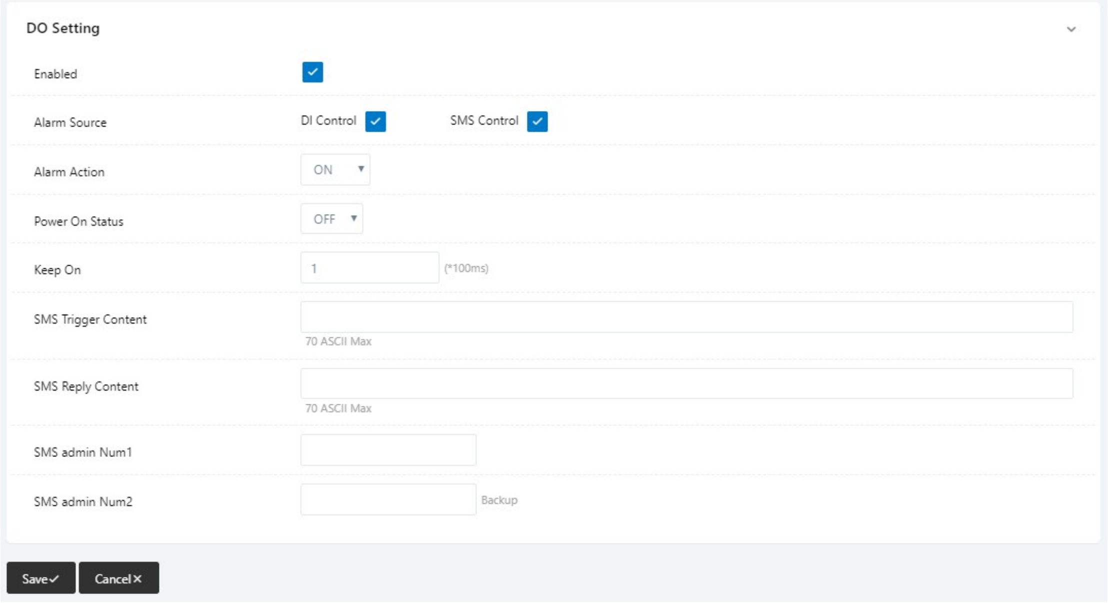


EVENT_COUNTER Mode

The counted number of pulses will be triggered.



2.9.7.2 DO Configuration



DO Setting

Enabled	☑	
Alarm Source	DI Control ☑	SMS Control ☑
Alarm Action	ON ▾	
Power On Status	OFF ▾	
Keep On	1 (*100ms)	
SMS Trigger Content	70 ASCII Max	
SMS Reply Content	70 ASCII Max	
SMS admin Num1		
SMS admin Num2	Backup	

Table 2-32 DO Instructions

Item	Instructions
Enable	DO is enabled.
Alarm Source	Digital Output activates according to different alarm sources.

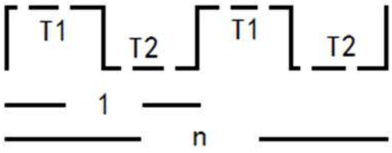
Item	Instructions
	You can select between DI Alarm and SMS Control. You can select one or both alarm sources. DI Alarm: The Digital Output gets triggered when there is an alarm from a Digital Input. SMS Control: The Digital Output gets triggered when receiving an SMS from a number in the phone book.
Alarm Action	The Digital Output initiates an alarm action. Select from “OFF”, “ON” and “Pulse”. OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.
Power on Status	Specify the Digital Output status when the power is on. Select from “OFF” and “ON”. OFF: Open from GND. ON: Short contact with GND.
Keep On	Available when the DO “Alarm On Action”/ “Alarm Off Action” status is ON. Input the DO “Keep On” status time. Input from 0 to 255 seconds. “0” means ON until the next action.
Delay	Available when you enable “Pulse” in “Alarm On Action”/ “Alarm Off Action”. The first pulse will be generated after a “Delay”. Input from 0 to 30000ms. (0=generate pulse without delay)
Low	Available if Pulse is enabled in “Alarm On Action”/ “Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low-level widths are specified here. Input from 1 to 30000 ms.
High	Available if Pulse is enabled in “Alarm On Action”/ “Alarm Off Action”. In “Pulse Output” mode, the selected Digital Output channel will generate a square wave as specified in the pulse mode parameters. The high-level widths are specified here. Input from 1 to 30000 ms.

Item	Instructions
Output	Available if Pulse is enabled in “Alarm On Action”/ “Alarm Off Action”. The number of pulses, input from 0 to 30000. (0 for continuous pulse output)
SMS Trigger Content	Available when you enable SMS Control in Alarm Source. Input the SMS content to enable “Alarm On Action” by SMS (70 ASIC II char max).
SMS Reply Content	Input the SMS content, which will be sent after DO is triggered. (70 ASIC II char max).
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 3 Click ”Save” to finish.

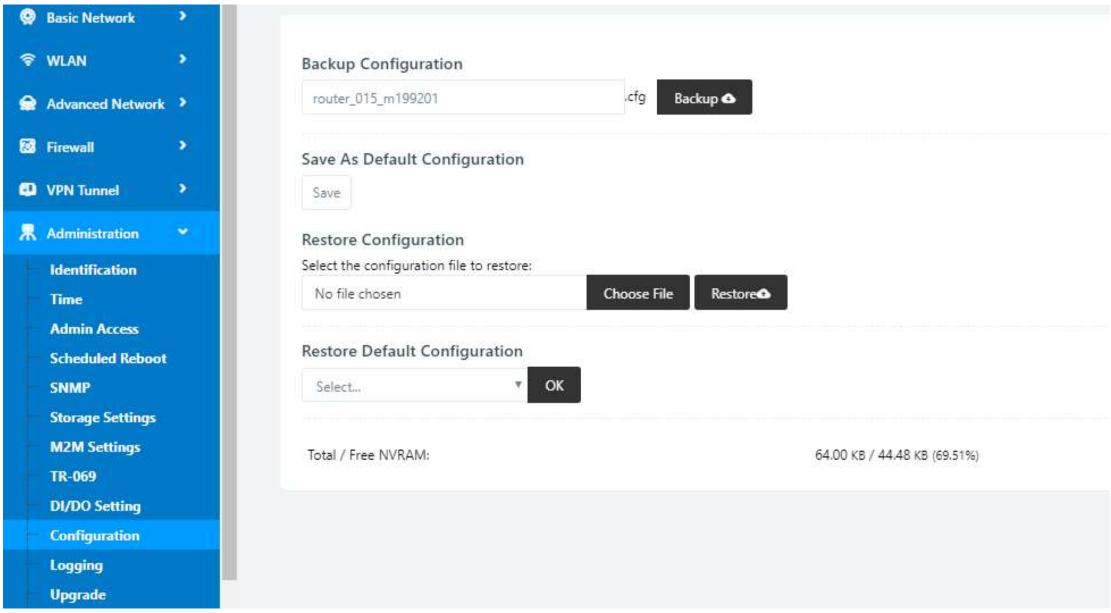
NOTE

DO can be customised in pulse width ratio: T1, T2 duration and n value.



2.9.10 Configuration Settings

Step 1 Go to “ Administration> Configuration ” to configure backup.



Backup Configuration

router_015_m199201 .cfg Backup

Save As Default Configuration

Save

Restore Configuration

Select the configuration file to restore:

No file chosen Choose File Restore

Restore Default Configuration

Select... OK

Total / Free NVRAM: 64.00 KB / 44.48 KB (69.51%)

Figure 3-1 Backup and Restore Configuration GUI

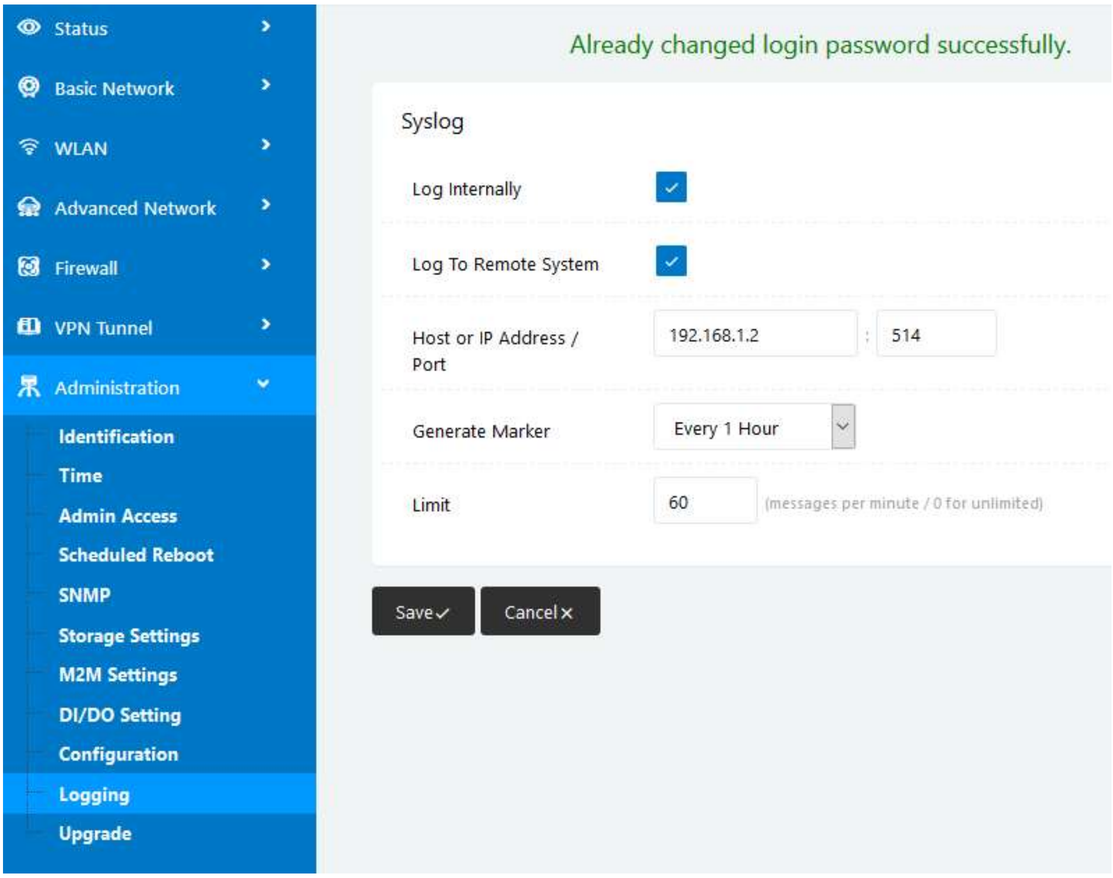
CAUTION

“Restore Default” will delete all configuration settings.

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

2.9.11 System Log Settings

Step 1 Go to “Administration> Logging” to start the configuration. You can set the file path to save the log (Local or remote sever).



Already changed login password successfully.

Syslog

Log Internally ☑

Log To Remote System ☑

Host or IP Address / Port: 192.168.1.2 : 514

Generate Marker: Every 1 Hour

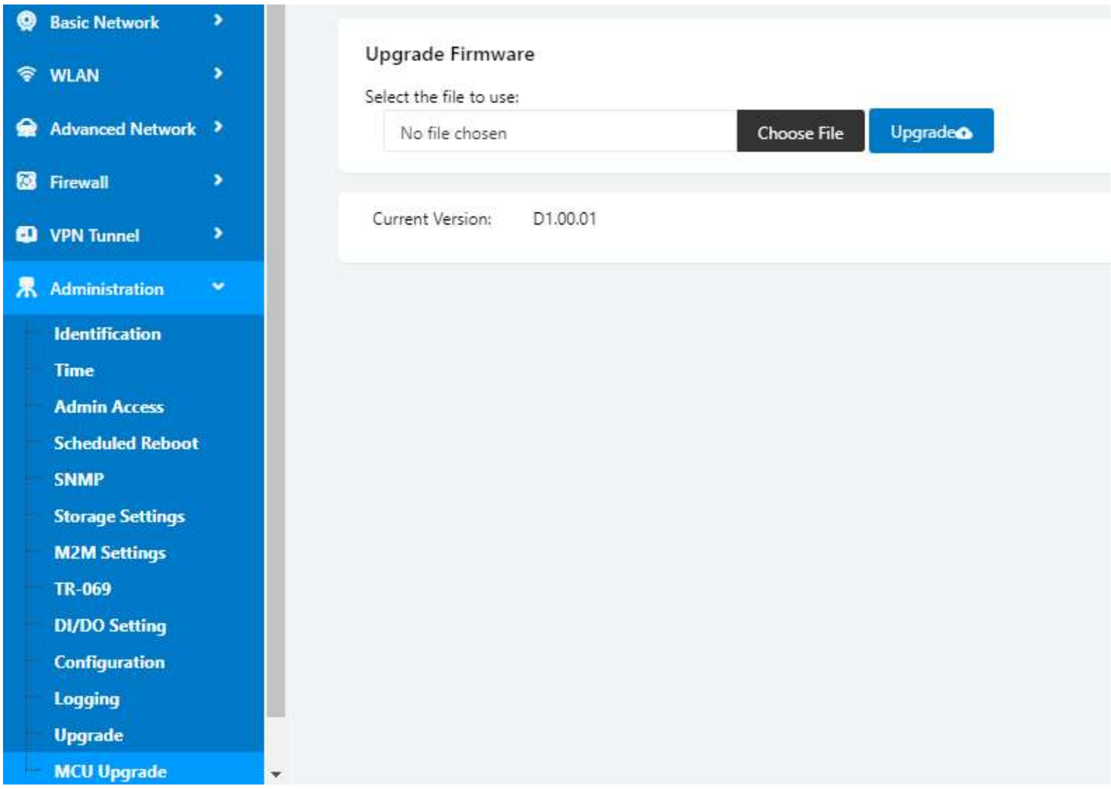
Limit: 60 (messages per minute / 0 for unlimited)

Figure 3-1 System log Settings GUI

Step 2 Click “Save” to finish.

2.9.12 Firmware upgrade

Step 1 Go to "Administration>Upgrade" to open upgrade firmware tab.



Upgrade Firmware

Select the file to use: No file chosen

Current Version: D1.00.01

Figure 3-1 Firmware Upgrade GUI

NOTE

Do not disconnect the power during upgrade. The upgrade takes about 4 minutes to complete.

2.10 "Reset" Button to Restore Factory Settings

If you can't access the GUI interface, you can perform a hardware reset. Press and hold the "Reset" button for 12 seconds then release. The system will be restored to factory default settings.

Table 2-33 System Default Instructions

Item	Default settings
LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP server	Enabled

Item	Default settings
Username	admin
Password	admin

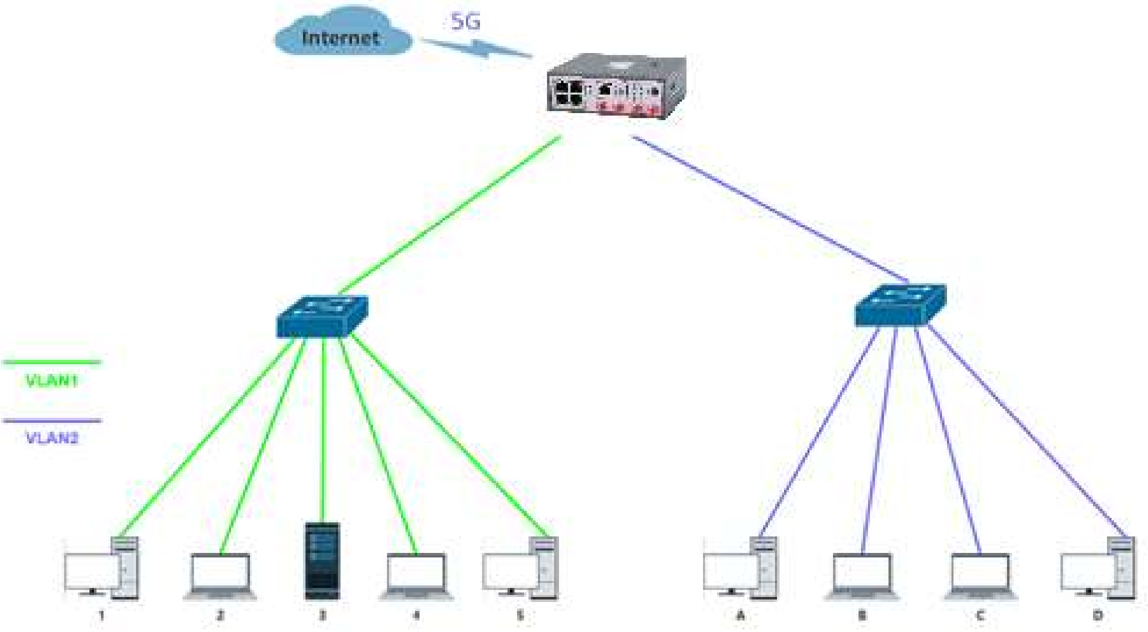
NOTE

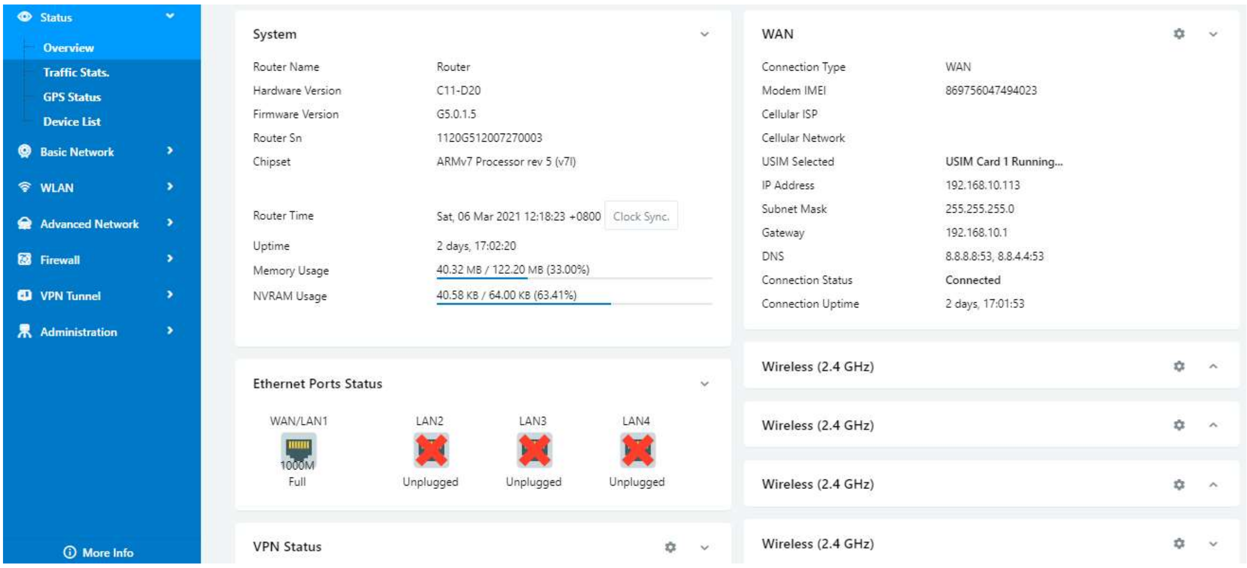
After reboot, the configuration will be deleted and restored to factory settings.

3 Configuration Examples

3.1 VLAN

The CM550W-POE supports VLAN partition based on Ethernet port (LAN1~LAN4)





System

Router Name Router
Hardware Version C11-D20
Firmware Version G5.0.1.5
Router Sn 1120G512007270003
Chipset ARMv7 Processor rev 5 (v7l)

Router Time Sat, 06 Mar 2021 12:18:23 +0800 Clock Sync.
Uptime 2 days, 17:02:20
Memory Usage 40.32 MB / 122.20 MB (33.00%)
NVRAM Usage 40.58 KB / 64.00 KB (63.41%)

Ethernet Ports Status

WAN/LAN1	LAN2	LAN3	LAN4
1000M Full	Unplugged	Unplugged	Unplugged

VPN Status

WAN

Connection Type WAN
Modem IMEI 869756047494023
Cellular ISP
Cellular Network
USIM Selected USIM Card 1 Running...
IP Address 192.168.10.113
Subnet Mask 255.255.255.0
Gateway 192.168.10.1
DNS 8.8.8.8:53, 8.8.4.4:53
Connection Status Connected
Connection Uptime 2 days, 17:01:53

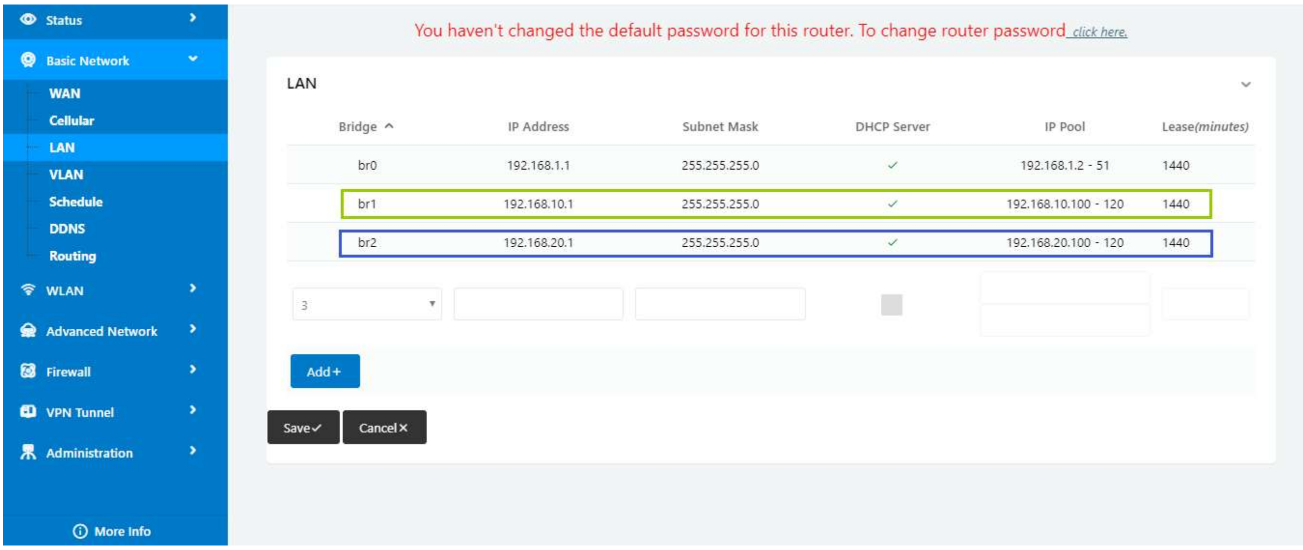
Wireless (2.4 GHz)

Wireless (2.4 GHz)

Wireless (2.4 GHz)

Wireless (2.4 GHz)

1) Configure LAN with Basic Network.

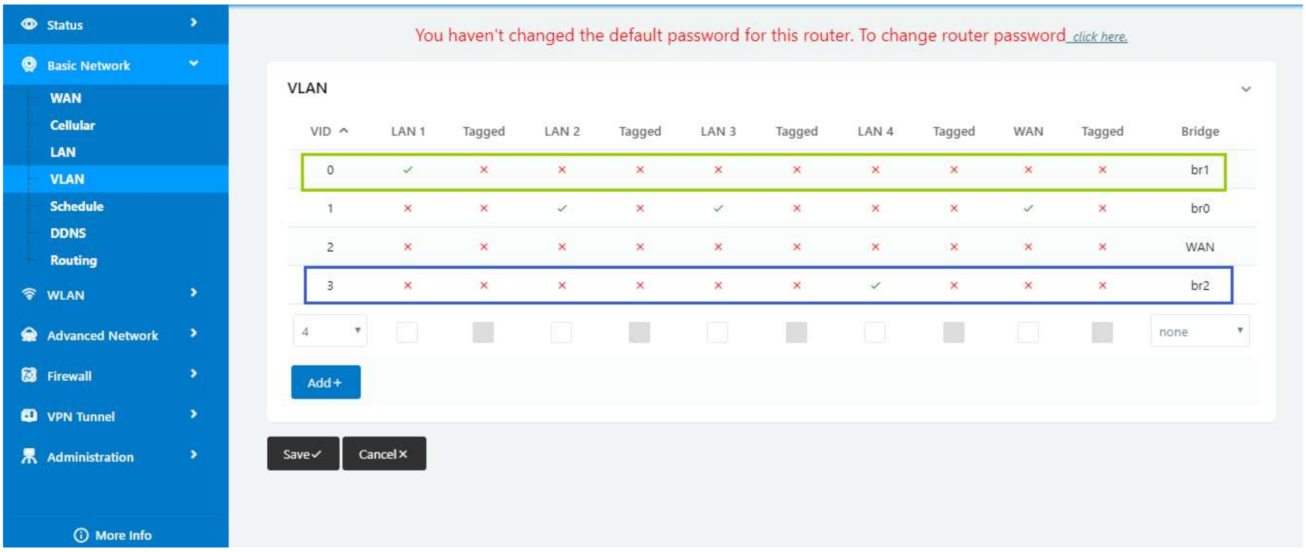


You haven't changed the default password for this router. To change router password click here.

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440
br1	192.168.10.1	255.255.255.0	✓	192.168.10.100 - 120	1440
br2	192.168.20.1	255.255.255.0	✓	192.168.20.100 - 120	1440
3			□		

2) If br1 and br2 are untagged, there won't be access between SW1 and SW2.

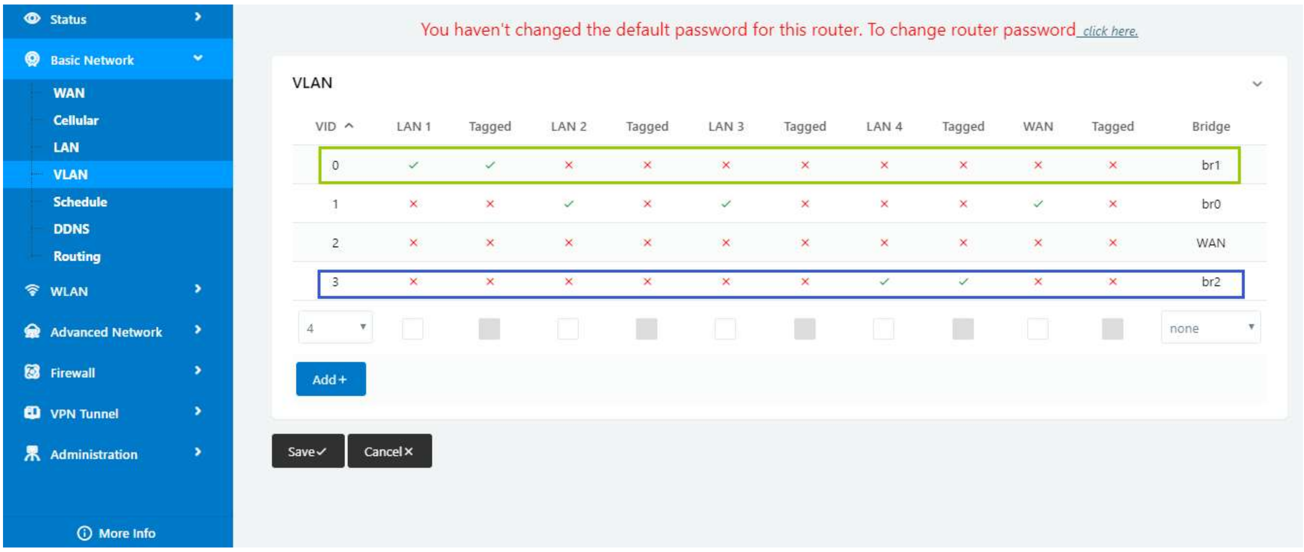


You haven't changed the default password for this router. To change router password click here.

VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
0	✓	×	×	×	×	×	×	×	×	×	br1
1	×	×	✓	×	✓	×	×	×	✓	×	br0
2	×	×	×	×	×	×	×	×	×	×	WAN
3	×	×	×	×	×	×	✓	×	×	×	br2
4 ▾	□	□	□	□	□	□	□	□	□	□	none ▾

3) If br1 and br2 are tagged, there will be access between sw1 and sw2.



You haven't changed the default password for this router. To change router password click here.

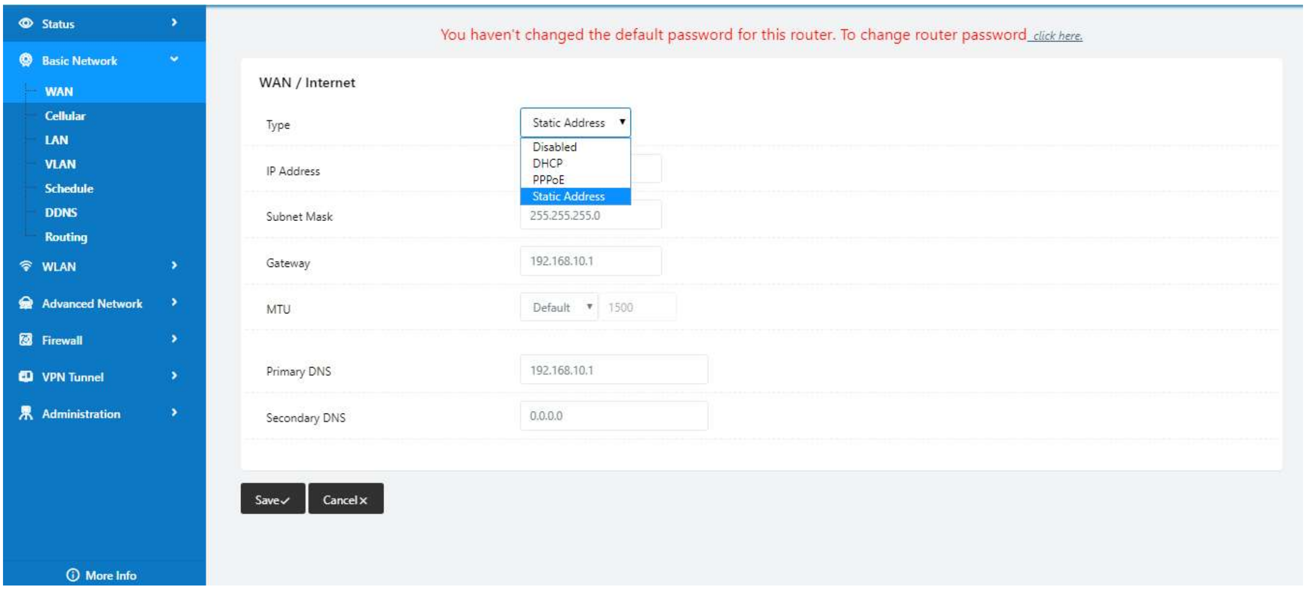
VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
0	✓	✓	×	×	×	×	×	×	×	×	br1
1	×	×	✓	×	✓	×	×	×	✓	×	br0
2	×	×	×	×	×	×	×	×	×	×	WAN
3	×	×	×	×	×	×	✓	✓	×	×	br2
4 ▾	□	□	□	□	□	□	□	□	□	□	none ▾

3.2 WAN Backup (WAN as Main, Cellular as Backup)

The WAN and Cellular backup allows you to automatically switch traffic to Cellular (link2) when WAN (link1) fails.

1) Navigate to Basic **Network > WAN**. Configure the WAN parameters as required.

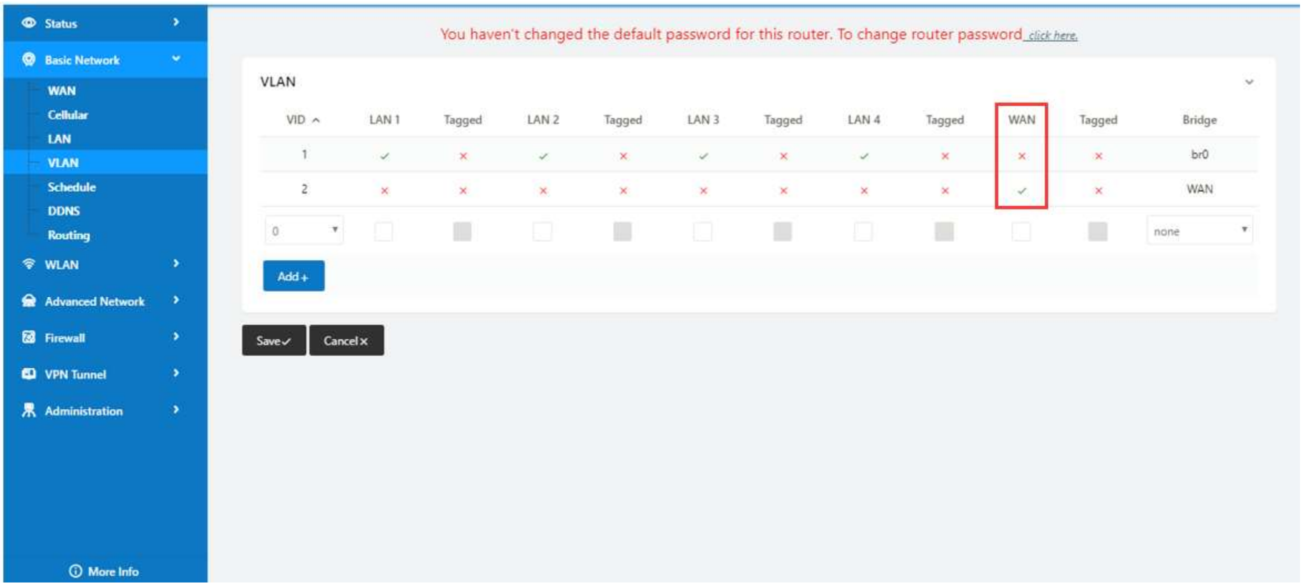


You haven't changed the default password for this router. To change router password click here.

WAN / Internet

Type	Static Address
IP Address	
Subnet Mask	255.255.255.0
Gateway	192.168.10.1
MTU	Default 1500
Primary DNS	192.168.10.1
Secondary DNS	0.0.0.0

2) Navigate to **Basic Network > VLAN**, and enable the LAN1 as WAN Ethernet

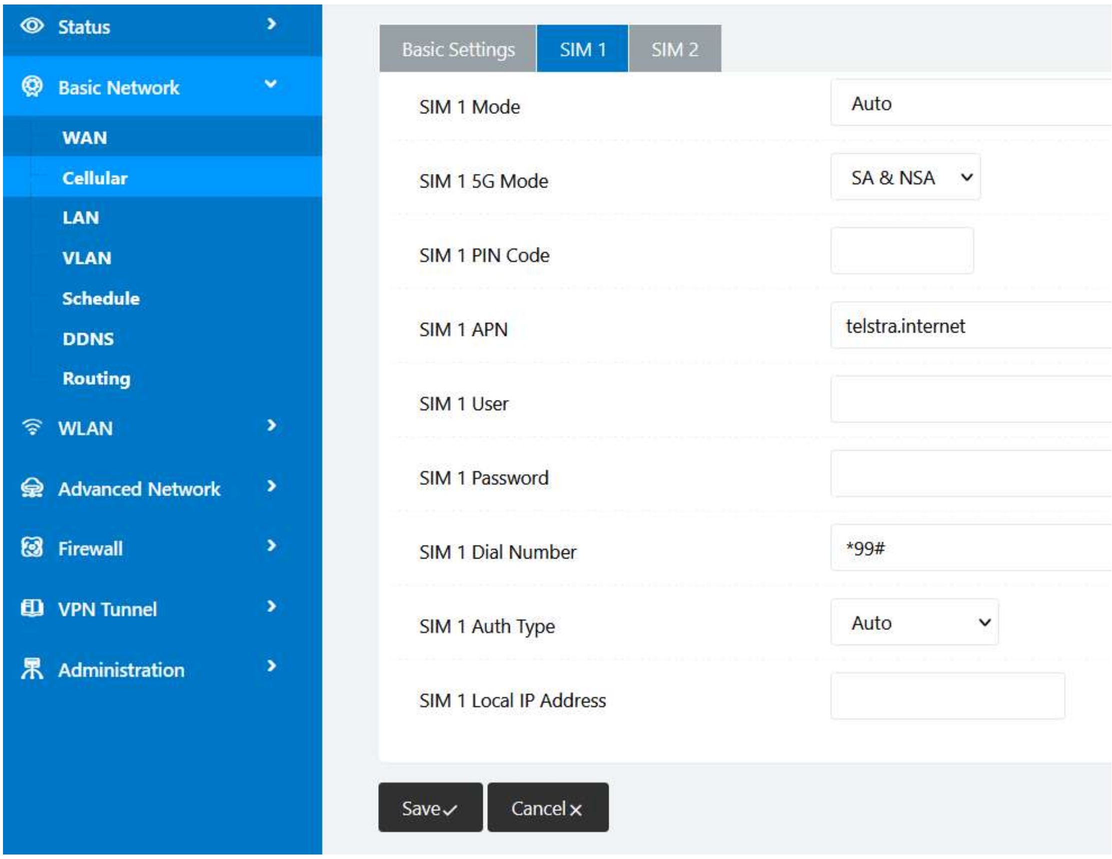


You haven't changed the default password for this router. To change router password click here.

VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	×	✓	×	✓	×	✓	×	×	×	br0
2	×	×	×	×	×	×	×	×	✓	×	WAN
0	□	□	□	□	□	□	□	□	□	□	none

3) Navigate to **Basic network > Cellular**, then configure the APN.

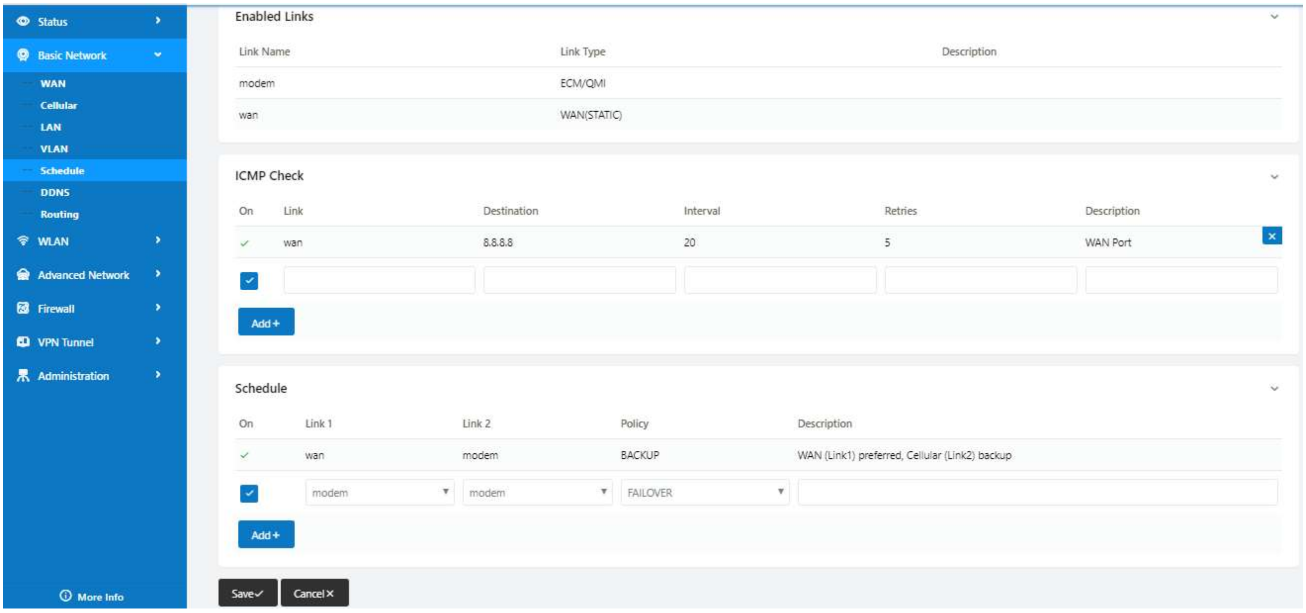


SIM 1 Mode	Auto
SIM 1 5G Mode	SA & NSA
SIM 1 PIN Code	
SIM 1 APN	telstra.internet
SIM 1 User	
SIM 1 Password	
SIM 1 Dial Number	*99#
SIM 1 Auth Type	Auto
SIM 1 Local IP Address	

4) Navigate to **Basic Network > Schedule.** Configure WAN (Link1) as preferred and Cellular (Link2) as backup.

Add ICMP Check to WAN

Set the working mode (Schedule)



Enabled Links

Link Name	Link Type	Description
modem	ECM/QMI	
wan	WAN(STATIC)	

ICMP Check

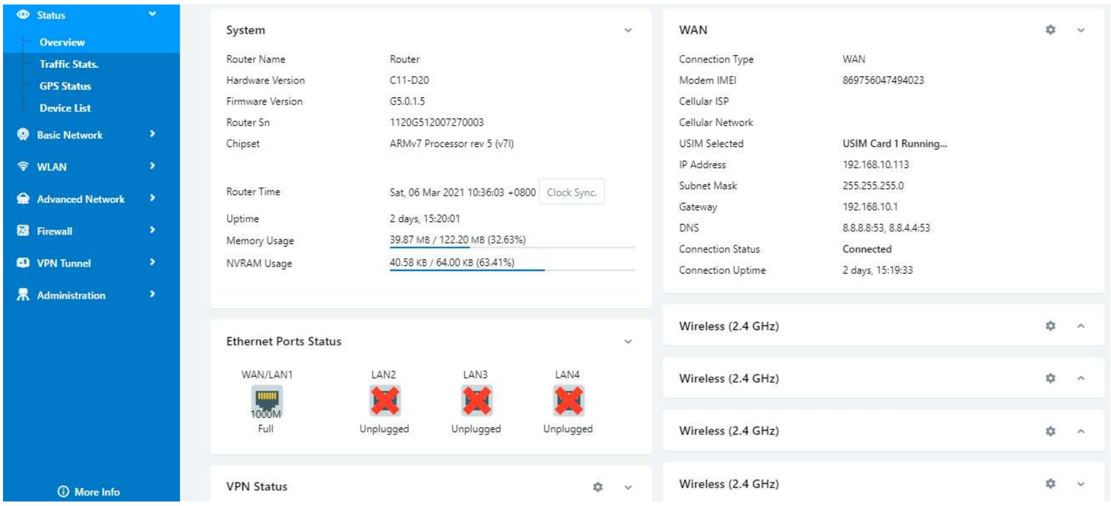
On	Link	Destination	Interval	Retries	Description
✓	wan	8.8.8.8	20	5	WAN Port
☑					

Schedule

On	Link 1	Link 2	Policy	Description
✓	wan	modem	BACKUP	WAN (Link1) preferred, Cellular (Link2) backup
☑	modem	modem	FAILOVER	

Item	Instructions
modem	The router dials up to the network via the modem.
wan	The router dials up to the network via WAN Ethernet (DHCP, PPPOE, Static IP)
ICMP Check	When ICMP Check fails, the switch between Link1 and Link2 will be triggered.
Link1	The preferred link.
Link2	The backup link.
BACKUP	In backup mode, Link1 and Link2 will remain online at the same time.
FAILOVER	In failover mode, Link2 will dial up as soon as Link1 fails.

5) Status: WAN working



System

Router Name	Router
Hardware Version	C11-D20
Firmware Version	G5.0.1.5
Router Sn	1120G512007270003
Chipset	ARMv7 Processor rev 5 (v7l)
Router Time	Sat, 06 Mar 2021 10:36:03 +0800
Uptime	2 days, 15:20:01
Memory Usage	39.87 MB / 122.20 MB (32.63%)
NVRAM Usage	40.58 KB / 64.00 KB (63.41%)

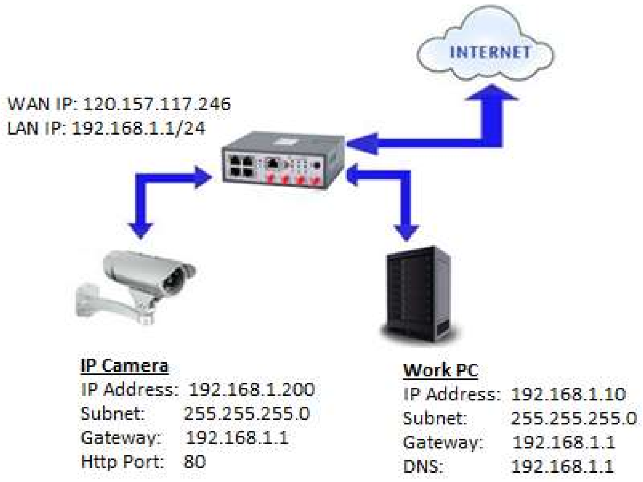
WAN

Connection Type	WAN
Modem IMEI	869756047494023
Cellular ISP	
Cellular Network	
USIM Selected	USIM Card 1 Running...
IP Address	192.168.10.113
Subnet Mask	255.255.255.0
Gateway	192.168.10.1
DNS	8.8.8.8:53, 8.8.4.4:53
Connection Status	Connected
Connection Uptime	2 days, 15:19:33

6) The system switches traffic to Cellular as soon as WAN fails.

3.3 Port Forwarding

1) Network topology:



WAN IP: 120.157.117.246
LAN IP: 192.168.1.1/24

IP Camera
IP Address: 192.168.1.200
Subnet: 255.255.255.0
Gateway: 192.168.1.1
Http Port: 80

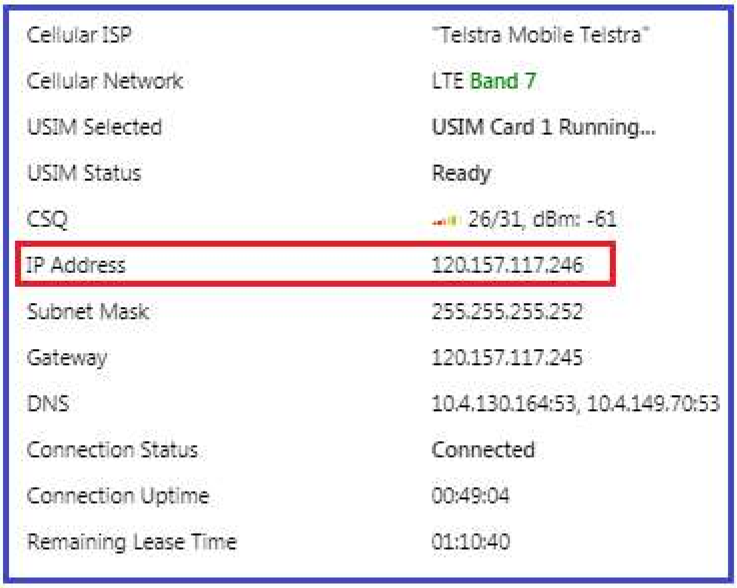
Work PC
IP Address: 192.168.1.10
Subnet: 255.255.255.0
Gateway: 192.168.1.1
DNS: 192.168.1.1

Port forwarding or port mapping is a way of making a computer on your home or business network accessible to computers on the internet, even though they are behind a router.

NOTE:

To configure Port Forwarding on the CM550W-POE router, please configure the router with the correct APN that will provide you with a Public WAN IP address, such as **telstra.extranet** for a Telstra Data SIM. You need to ask your carrier to activate your SIM card with a Public WAN IP.

Check the WAN IP address on the Status Page of the router.

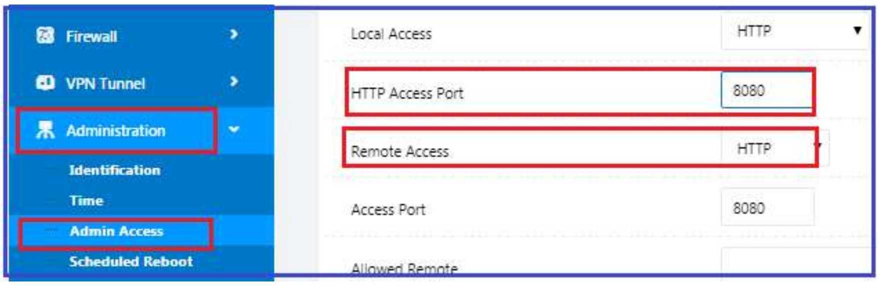


Cellular ISP	"Telstra Mobile Telstra"
Cellular Network	LTE Band 7
USIM Selected	USIM Card 1 Running...
USIM Status	Ready
CSQ	26/31, dBm: -61
IP Address	120.157.117.246
Subnet Mask	255.255.255.252
Gateway	120.157.117.245
DNS	10.4.130.164:53, 10.4.149.70:53
Connection Status	Connected
Connection Uptime	00:49:04
Remaining Lease Time	01:10:40

2) Change the router GUI to port 8080 to avoid conflict with the IP camera Http port (80).

Go to Administration -> Admin Access -> HTTP Access port set to 8080.

Note: Set Remote Access to "HTTP" to allow remote access over the internet via a public WAN IP.



Local Access: HTTP

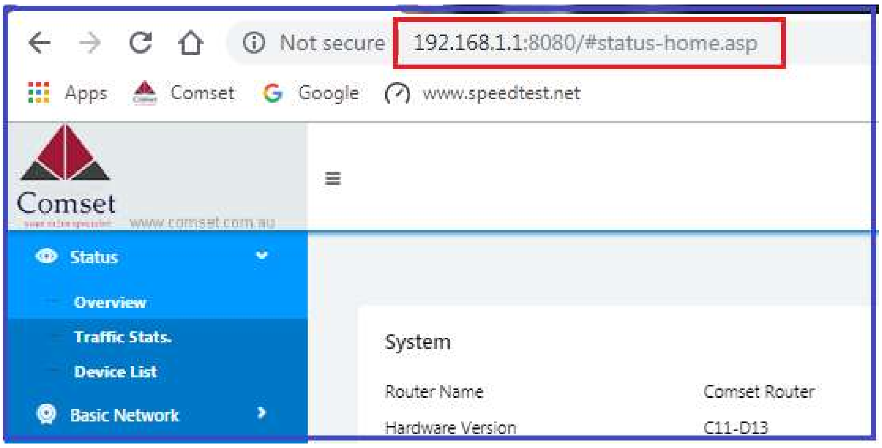
HTTP Access Port: 8080

Remote Access: HTTP

Access Port: 8080

Allowed Remote

To access the GUI of the router, use URL http://192.168.1.1:8080



192.168.1.1:8080/#status-home.asp

System

Router Name: Comset Router

Hardware Version: C11-D13

3) Configure Port Forwarding for the IP Camera on Port 80.

Go to Advanced Network -> Port Forwarding, and set the following:

Proto: TCP

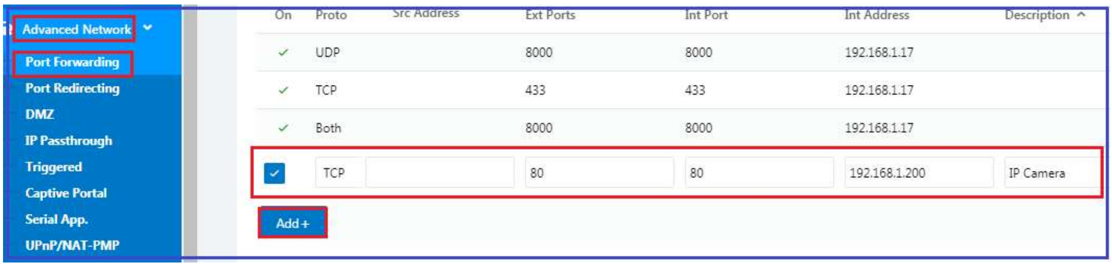
External Ports: 80

Internal Ports: 80

Internal Address: 192.168.1.200

Description: IP camera

Then click on the "Add" button.

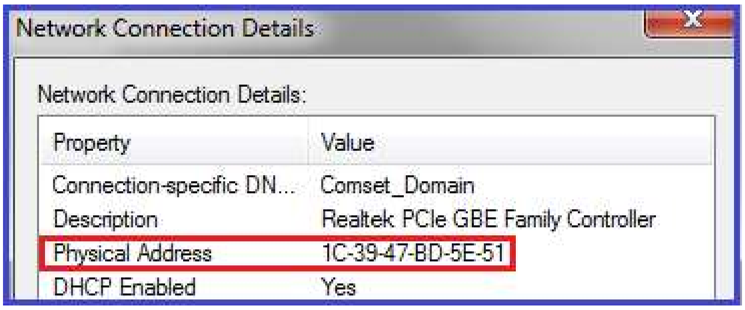


On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description
✓	UDP		8000	8000	192.168.1.17	
✓	TCP		433	433	192.168.1.17	
✓	Both		8000	8000	192.168.1.17	
☑	TCP		80	80	192.168.1.200	IP Camera

4) To access the Web GUI of the camera, use URL http://120.157.117.246 or http://120.157.117.246:80

3.4 IP Passthrough

1) The IP Passthrough feature allows a single PC, or a single router on the LAN, to have the Router's public IP address assigned to it. IP passthrough works essentially the same as a bridged mode. Check the LAN MAC address on your PC. Go to Network Adapter. Right click> Status> Details. See below:



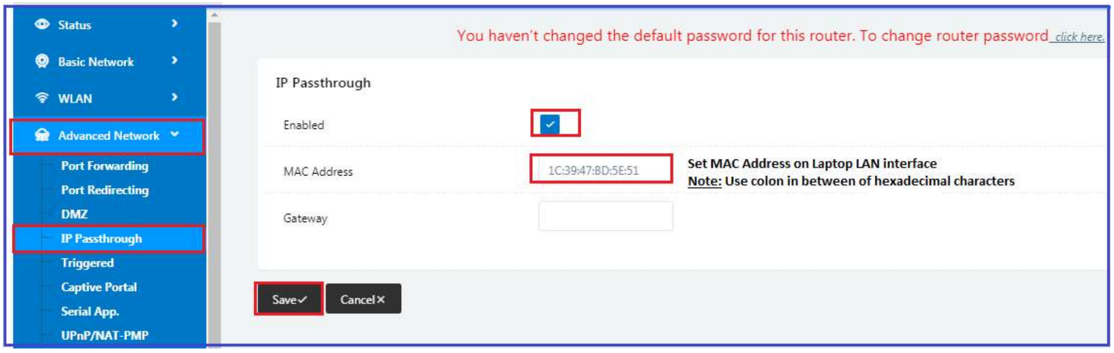
Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	Comset_Domain
Description	Realtek PCIe GBE Family Controller
Physical Address	1C-39-47-BD-5E-51
DHCP Enabled	Yes

2) Configure IP passthrough on the router. Go to Advanced Network> IP Passthrough> Tick the "Enabled" box. Input the MAC Address as obtained from your PC LAN interface and click "Save".

Note: Use a colon between the hexadecimal characters. See below:



You haven't changed the default password for this router. To change router password click here.

IP Passthrough

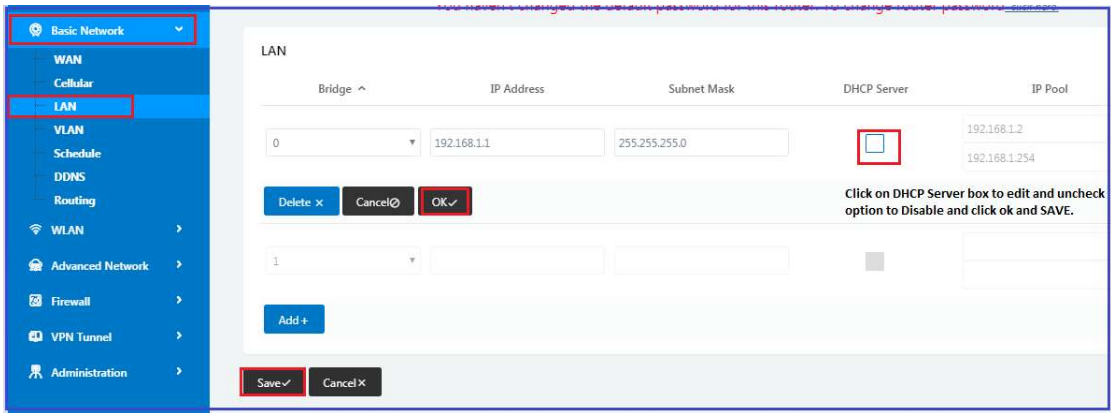
Enabled ☑

MAC Address 1C:39:47:BD:5E:51

Set MAC Address on Laptop LAN interface
Note: Use colon in between of hexadecimal characters

Gateway

3) Disable DHCP server on the router. Go to Basic Network> LAN. Click on DHCP Server to edit and untick the box to disable. Click on "OK" then click on "Save".

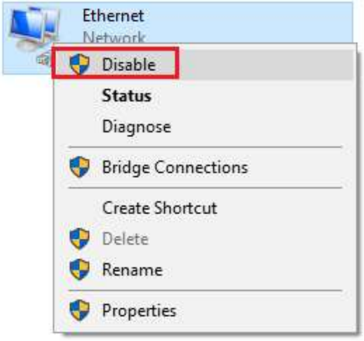


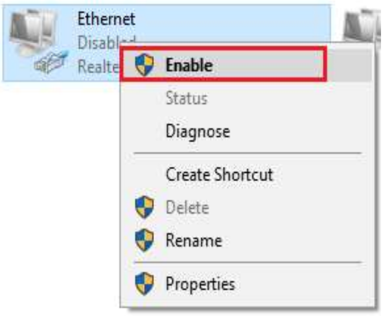
LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool
0	192.168.1.1	255.255.255.0	□	192.168.1.2 192.168.1.254
1				

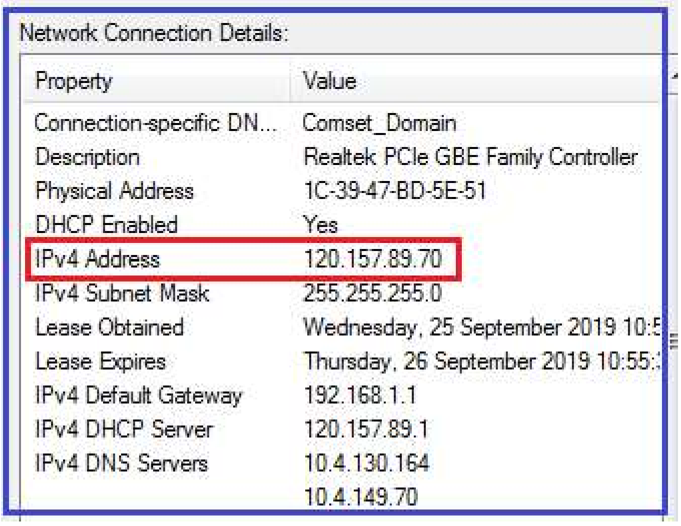
Click on DHCP Server box to edit and uncheck option to Disable and click ok and SAVE.

4) Refresh the network adapter by clicking on the Disable/Enable button. Right click on the network adapter and select Disable. Right click on the network adapter again and select Enable. See below:





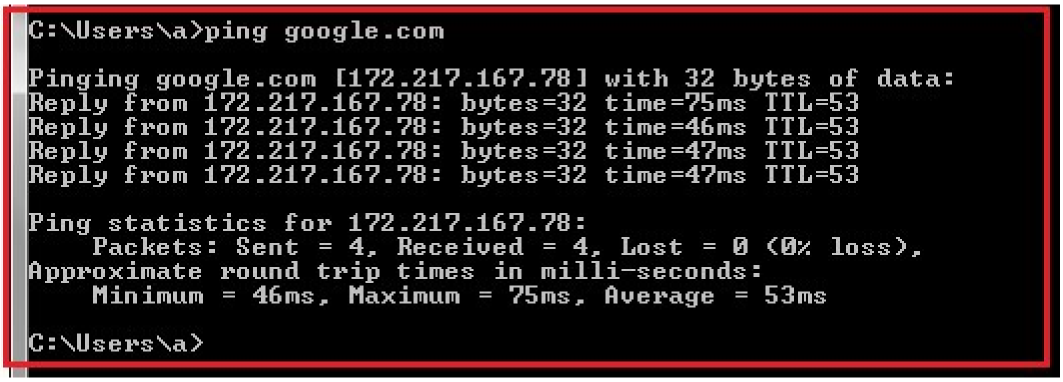
4) Check Status of the LAN interface. Go to Network Adapter> Right click> Status> Details. The LAN adapter is now using Public WAN IP address 120.157.89.70 via IP Passthrough.



Network Connection Details:

Property	Value
Connection-specific DN...	Comset_Domain
Description	Realtek PCIe GBE Family Controller
Physical Address	1C-39-47-BD-5E-51
DHCP Enabled	Yes
IPv4 Address	120.157.89.70
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, 25 September 2019 10:5
Lease Expires	Thursday, 26 September 2019 10:55:
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	120.157.89.1
IPv4 DNS Servers	10.4.130.164
	10.4.149.70

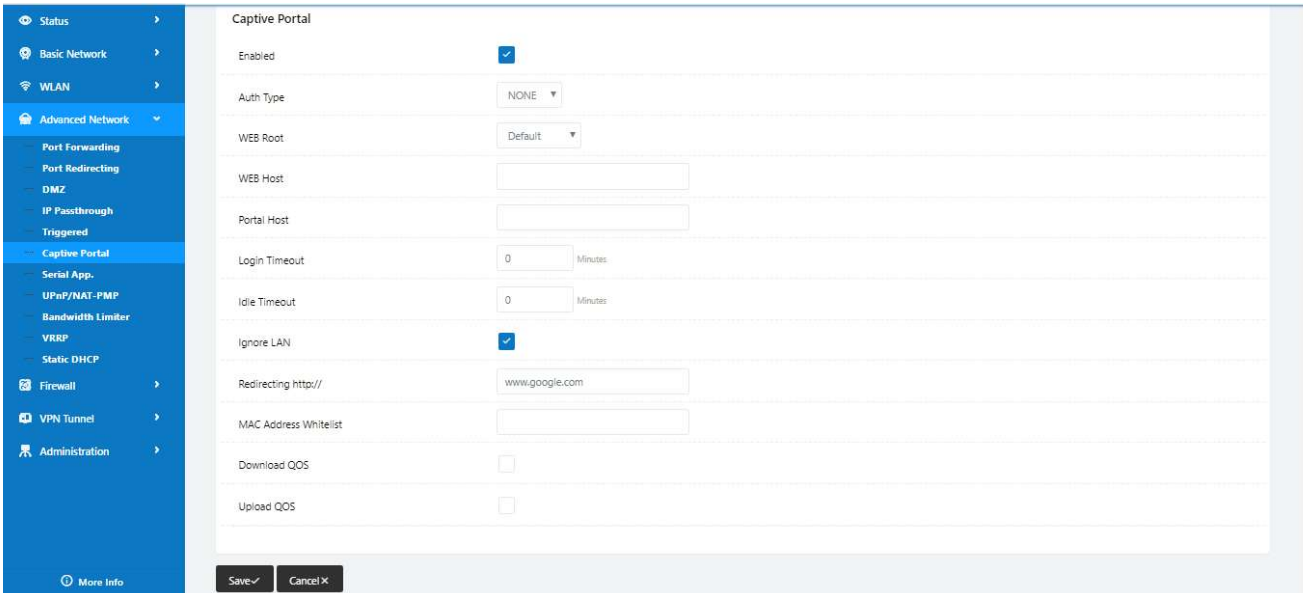
5) Check internet connection via command line:



```
C:\Users\a>ping google.com

Pinging google.com [172.217.167.78] with 32 bytes of data:
Reply from 172.217.167.78: bytes=32 time=75ms TTL=53
Reply from 172.217.167.78: bytes=32 time=46ms TTL=53
Reply from 172.217.167.78: bytes=32 time=47ms TTL=53
Reply from 172.217.167.78: bytes=32 time=47ms TTL=53

Ping statistics for 172.217.167.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 75ms, Average = 53ms

C:\Users\a>
```

3.5 Captive Portal

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

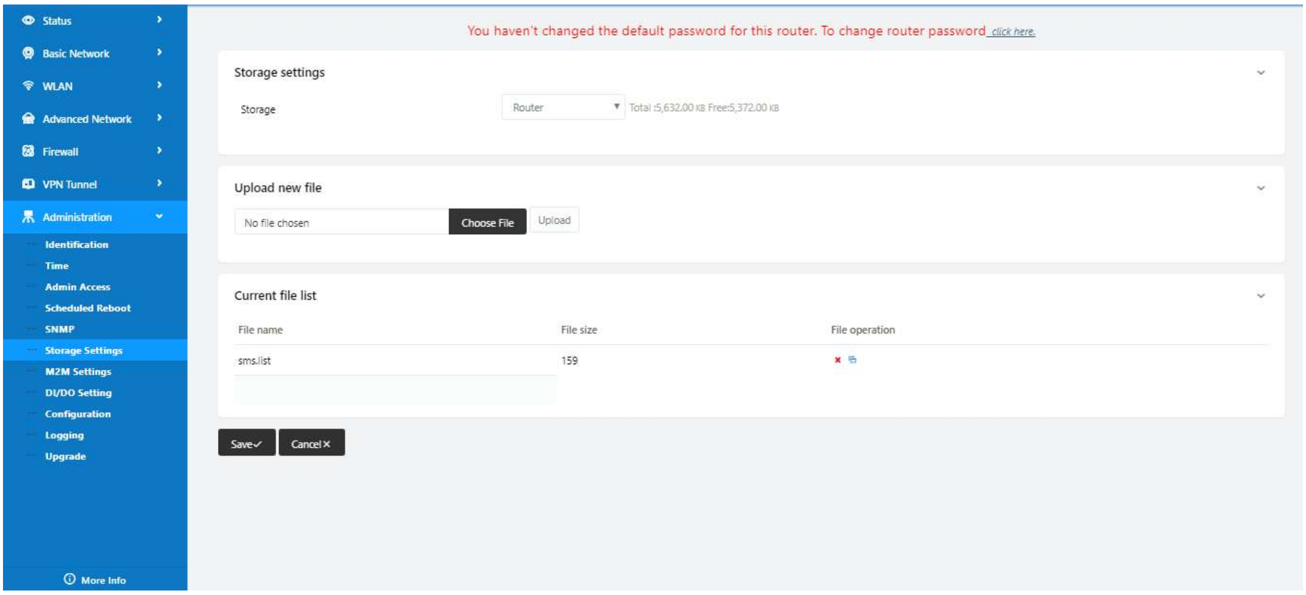


Captive Portal

Enabled	☑
Auth Type	NONE
WEB Root	Default
WEB Host	
Portal Host	
Login Timeout	0 Minutes
Idle Timeout	0 Minutes
Ignore LAN	☑
Redirecting http://	www.google.com
MAC Address Whitelist	
Download QOS	□
Upload QOS	□

1) Upload Portal file and Splash.html by local

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



You haven't changed the default password for this router. To change router password click here.

Storage settings

Storage: Router Total :5,632.00 KB Free:5,372.00 KB

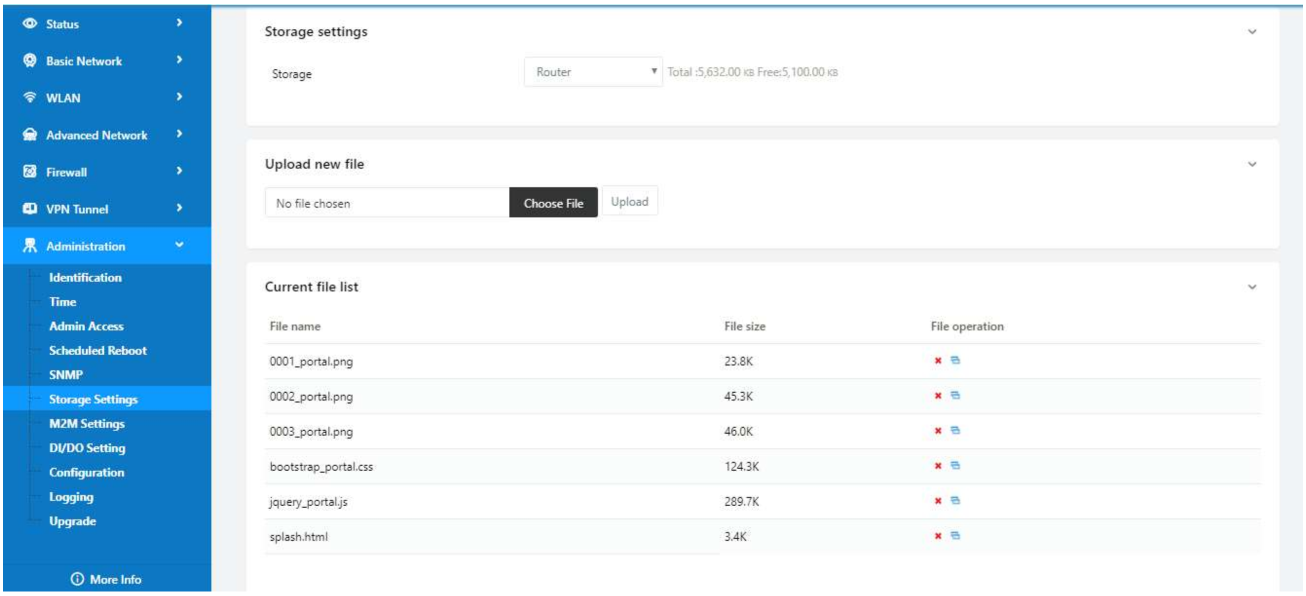
Upload new file

No file chosen

Current file list

File name	File size	File operation
sms.list	159	✕

Each Ad file supports 3 Ad portal images. Picture format is png or jpg. Image size is less than 100Kbytes. Resolution is 800x600. Picture name is 0001_portal.png, 0002_portal.png and 0003_portal.png. Please keep image names the same between portal file and splash.html.



Storage settings

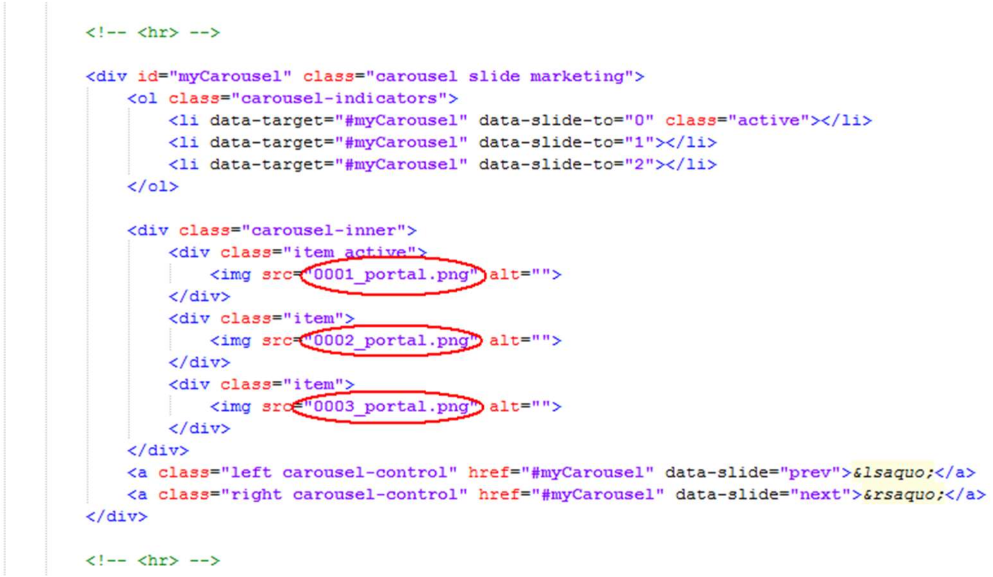
Storage: Router — Total :5,632.00 KB Free:5,100.00 KB

Upload new file

No file chosen

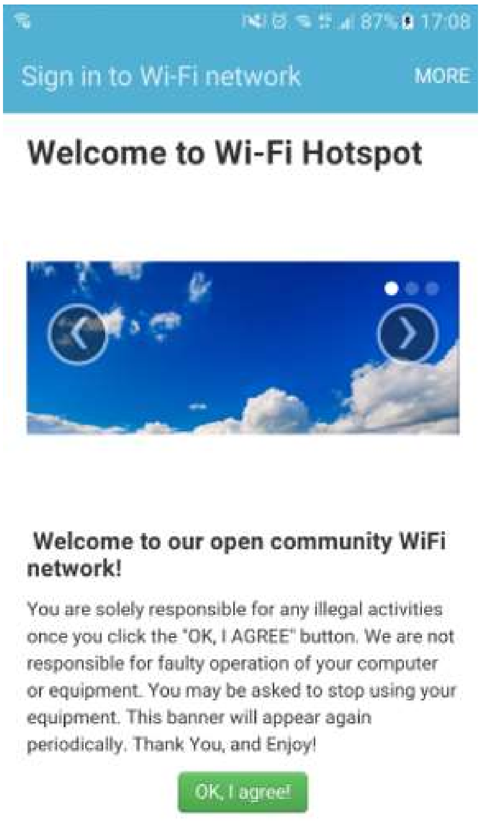
Current file list

File name	File size	File operation
0001_portal.png	23.8K	✖ ▤
0002_portal.png	45.3K	✖ ▤
0003_portal.png	46.0K	✖ ▤
bootstrap_portal.css	124.3K	✖ ▤
jquery_portal.js	289.7K	✖ ▤
splash.html	3.4K	✖ ▤



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

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

    <div class="carousel-inner">
        <div class="item active">
            <img src="0001_portal.png" alt="">
        </div>
        <div class="item">
            <img src="0002_portal.png" alt="">
        </div>
        <div class="item">
            <img src="0003_portal.png" alt="">
        </div>
    </div>
    <a class="left carousel-control" href="#myCarousel" data-slide="prev">&lsaquo;</a>
    <a class="right carousel-control" href="#myCarousel" data-slide="next">&rsaquo;</a>
</div>

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

Now you can see the results by connecting to the router’s WiFi.



Sign in to Wi-Fi network MORE

Welcome to Wi-Fi Hotspot

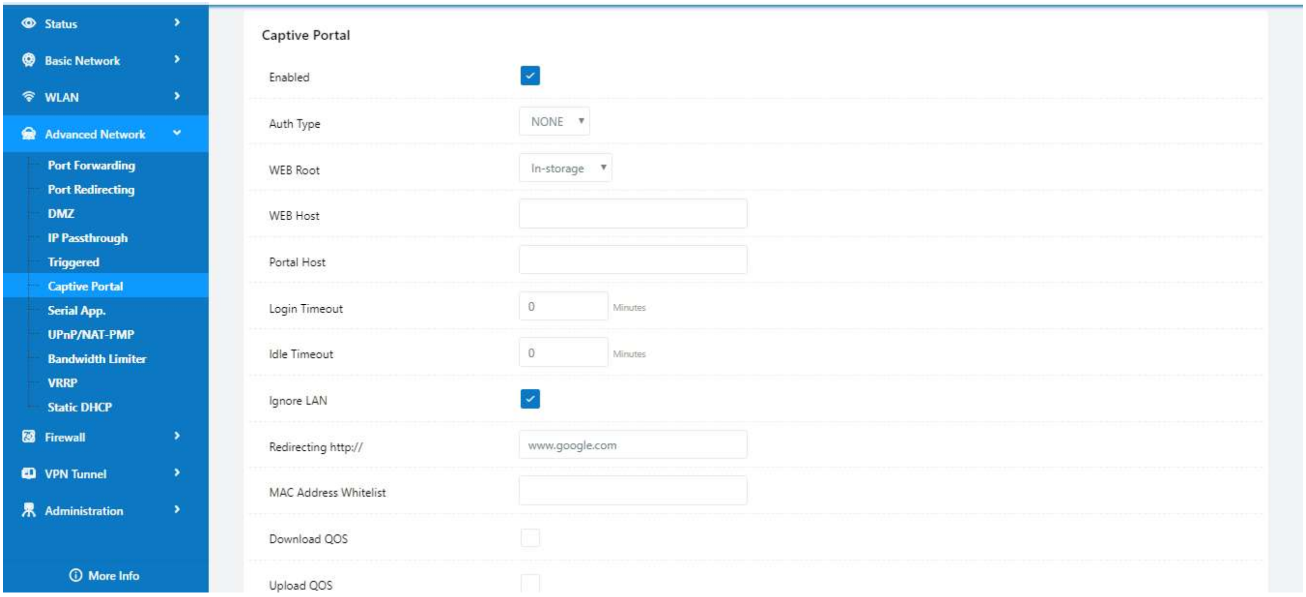
Welcome to our open community WiFi network!

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

OK, I agree!

2) Modify portal file storage path.

Modify portal file storage for In-storage as below:

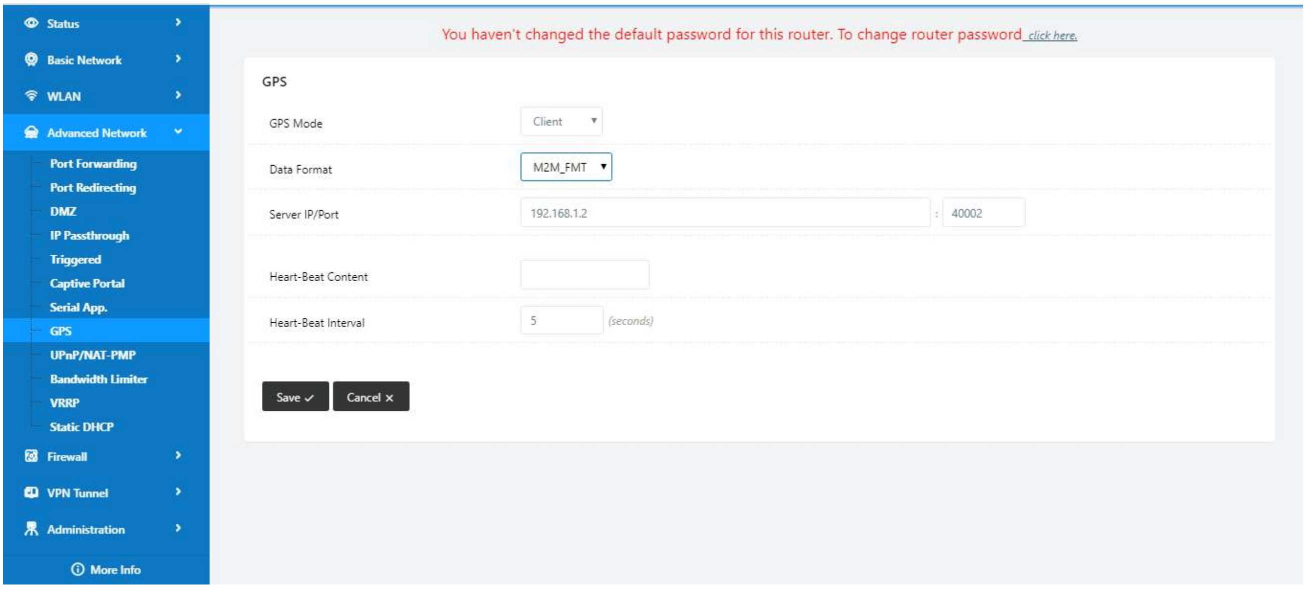


Captive Portal

Enabled	☑
Auth Type	NONE
WEB Root	In-storage
WEB Host	
Portal Host	
Login Timeout	0 Minutes
Idle Timeout	0 Minutes
Ignore LAN	☑
Redirecting http://	www.google.com
MAC Address Whitelist	
Download QOS	□
Upload QOS	□

3.6 GPS Settings (GPS version only)

Go to “Advanced Network> GPS” to view or modify the relevant parameters.



You haven't changed the default password for this router. To change router password click here.

GPS

GPS Mode: Client

Data Format: M2M_FMT

Server IP/Port: 192.168.1.2 : 40002

Heart-Beat Content:

Heart-Beat Interval: 5 (seconds)

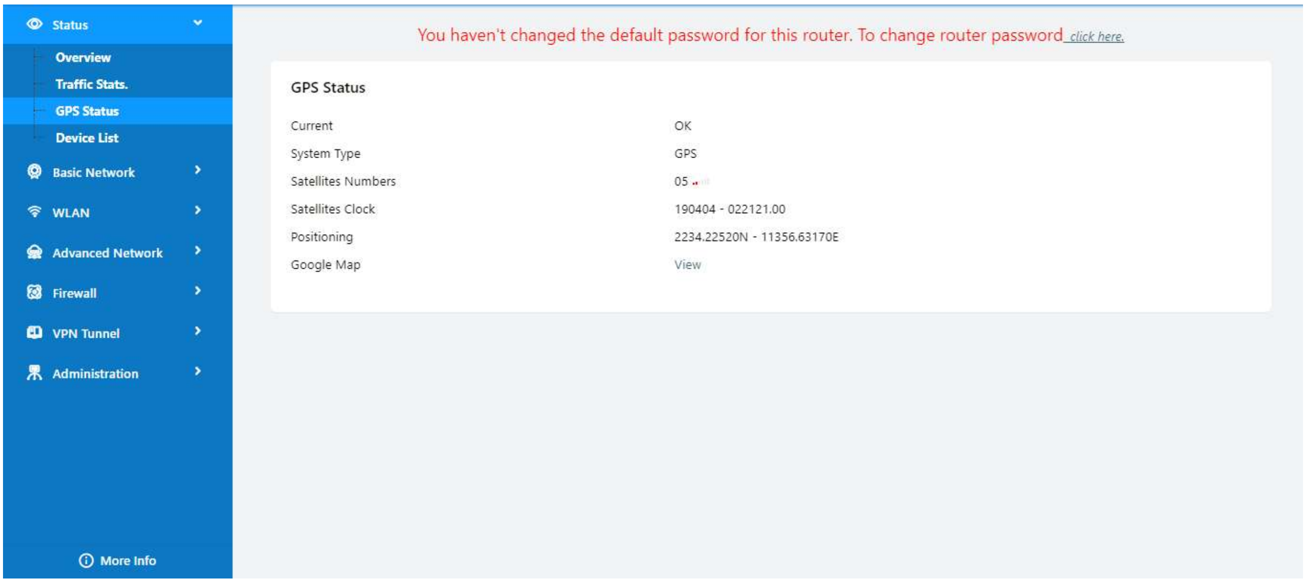
Table 4-6 “GPS” Instructions

Item	Instructions
GPS Mode	Enable/Disable.
GPS Format	NMEA and M2M_FMT.
Server IP/Port	GPS server IP and port.
Heartbeat	If you choose M2M_FMT format, heartbeat ID will be packed into the GPS data.
Interval	GPS data transmits at the interval time.

Step 1 Click on “Save” to finish.

Step 2 Connect the GPS antenna to the router GPS interface.

Step 3 Check GPS Status.



You haven't changed the default password for this router. To change router password click here.

GPS Status

Current OK

System Type GPS

Satellites Numbers 05

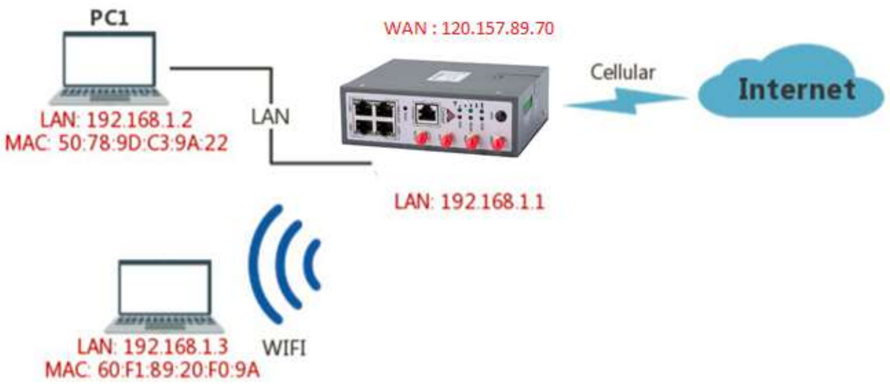
Satellites Clock 190404 - 022121.00

Positioning 2234.22520N - 11356.63170E

Google Map View

3.7 Firewall

Network Topology



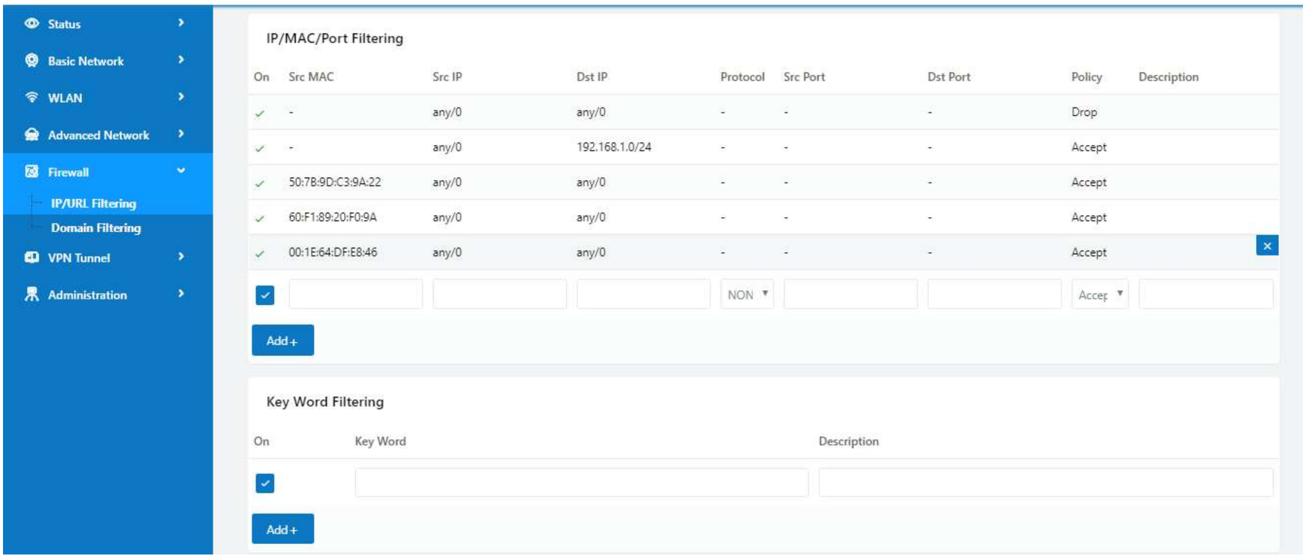
1) IP/MAC/Port Filtering

This allows you to intercept packages from the router’s WAN/ Cellular interface to the internet.

Test case:

Only allows three devices (MAC/LAN/WLAN) access the Internet via WAN: (120.157.89.70)

Only allows three devices (MAC/LAN/WLAN) access the router page: (192.168.1.1)



IP/MAC/Port Filtering

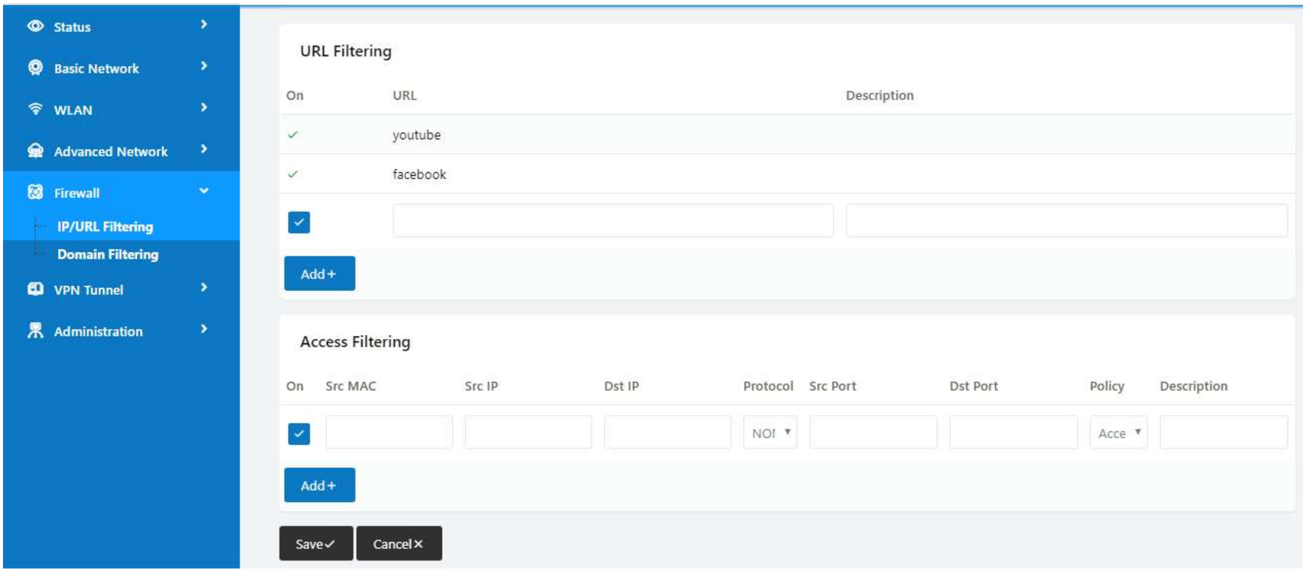
On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
✓	-	any/0	any/0	-	-	-	Drop	
✓	-	any/0	192.168.1.0/24	-	-	-	Accept	
✓	50:7B:9D:C3:9A:22	any/0	any/0	-	-	-	Accept	
✓	60:F1:89:20:F0:9A	any/0	any/0	-	-	-	Accept	
✓	00:1E:64:DF:E8:46	any/0	any/0	-	-	-	Accept	
☑				NON ▾			Accep ▾	

Key Word Filtering

On	Key Word	Description
☑		

2) Keyword Filtering

This allows you to filter specific keywords from the router's WAN/Cellular interface to the internet.



URL Filtering

On	URL	Description
✓	youtube	
✓	facebook	
☑		

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
☑				NOI ▾			Acce ▾	

3) URL Filtering

This allows you to filter specific URLs from the router's WAN/Cellular interface to the internet.

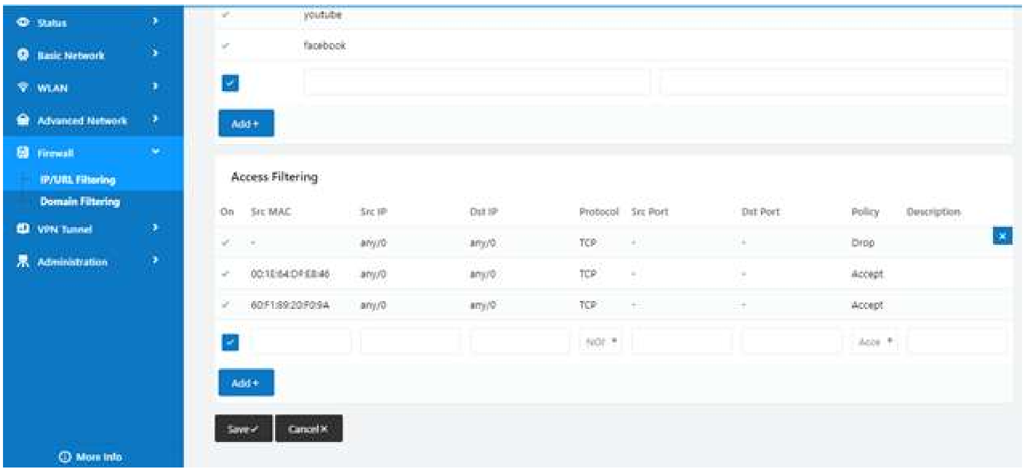
4) Access Filtering

This allows you to filter packages from the internet to the router’s WAN/Cellular interface.

Test case:

4.1) Intercept all TCP packets accessing the router's WAN/Cellular(120.157.89.70).

4.2) Only two devices (MAC/LAN/WLAN) can be accessed from Internet packets.



✓	youtube
✓	facebook
☑	

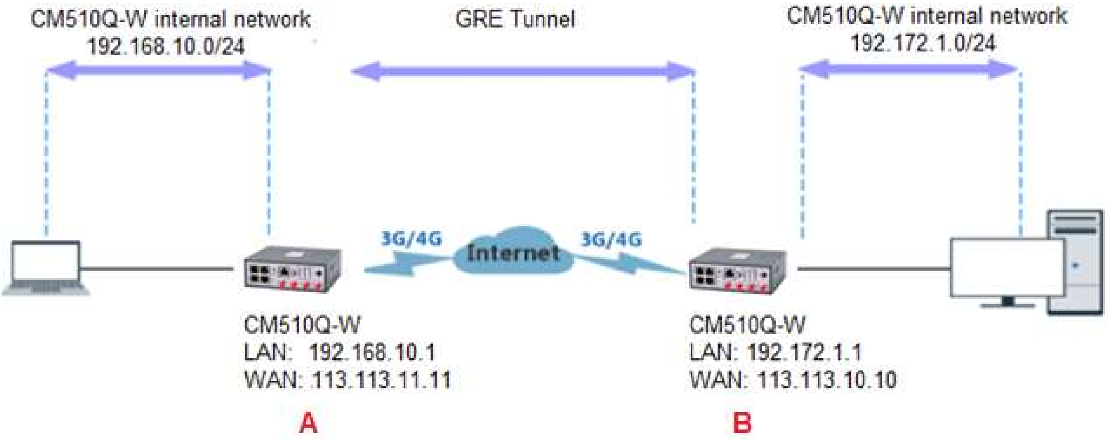
Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
✓	-	any/0	any/0	TCP	-	-	Drop	
✓	00:1E:64:DF:E8:46	any/0	any/0	TCP	-	-	Accept	
✓	60:F1:89:20:F0:9A	any/0	any/0	TCP	-	-	Accept	
☑				NOT			Acce	

3.8 VPN Tunnel

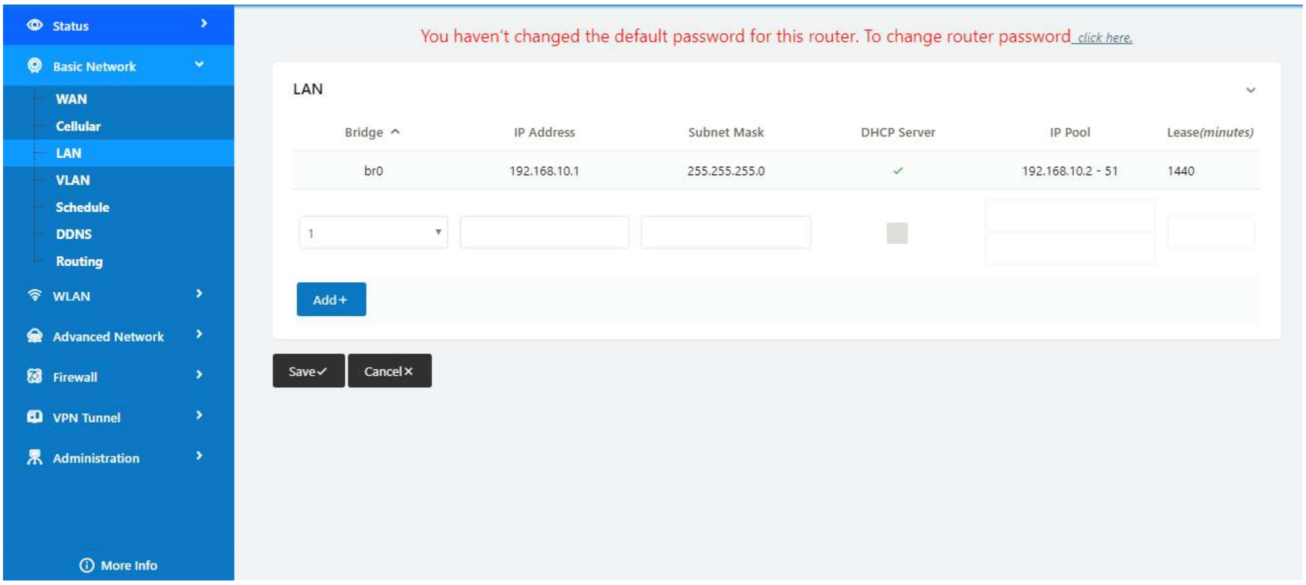
3.8.1 GRE

GRE Tunnel between two COMSET Routers



1) CM550W-POE(A) Configuration

Navigate to **Basic Network > LAN**

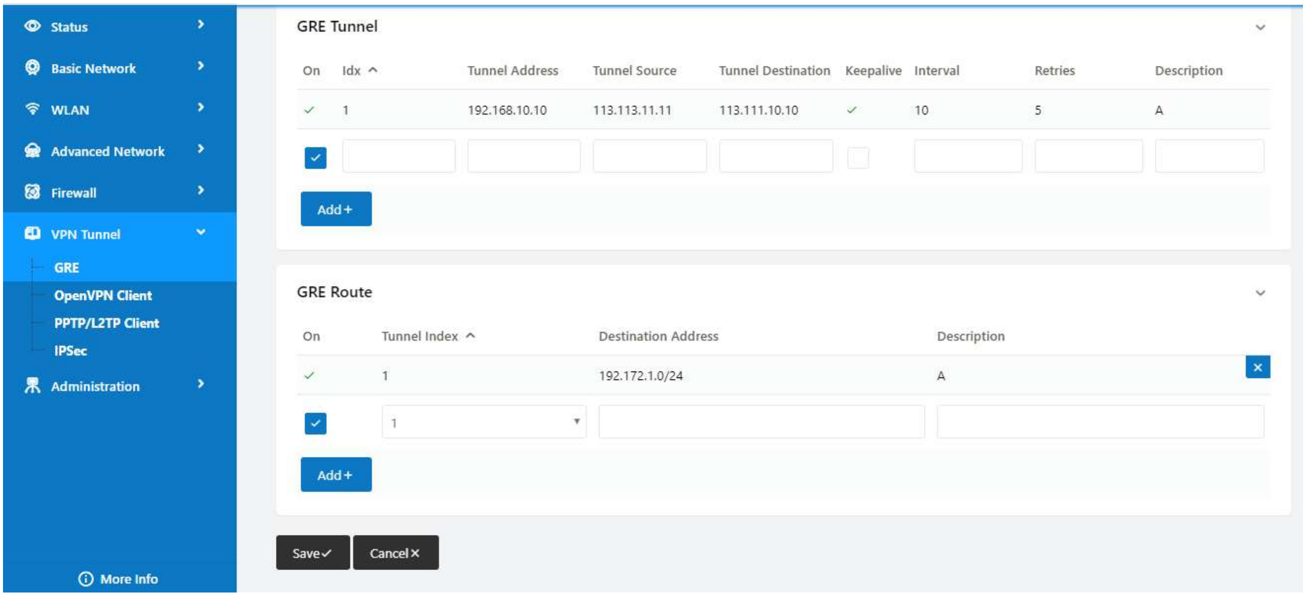


You haven't changed the default password for this router. To change router password click here.

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease*(minutes)*
br0	192.168.10.1	255.255.255.0	✓	192.168.10.2 - 51	1440
1			□		

Navigate to **VPN Tunnel > GRE**



GRE Tunnel

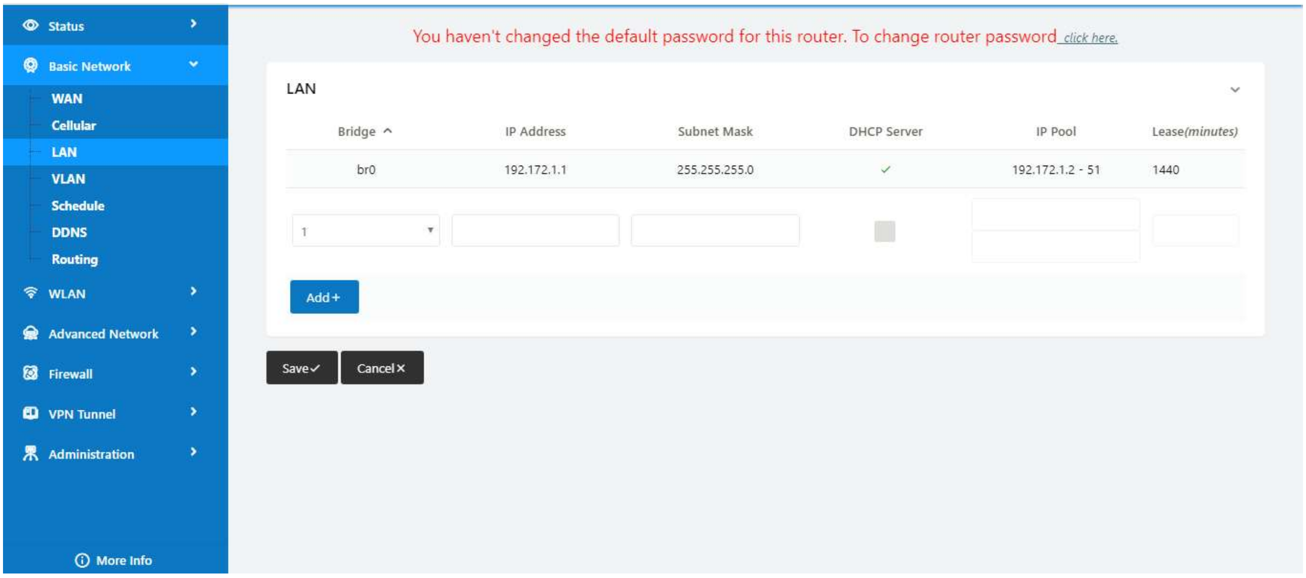
On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	1	192.168.10.10	113.113.11.11	113.111.10.10	✓	10	5	A
☑					□			

GRE Route

On	Tunnel Index	Destination Address	Description
✓	1	192.172.1.0/24	A
☑	1		

2) CM550W-POE(B) Config

Navigate to **Basic Network > LAN**

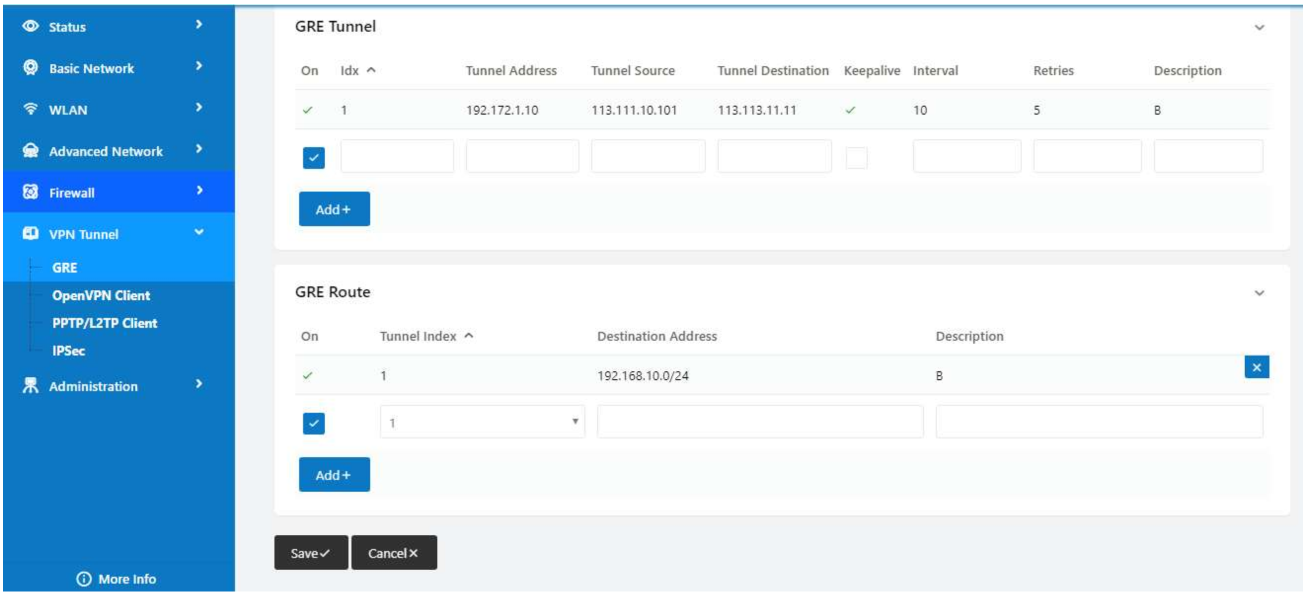


You haven't changed the default password for this router. To change router password click here.

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease*(minutes)*
br0	192.172.1.1	255.255.255.0	✓	192.172.1.2 - 51	1440
1			□		

Navigate to **VPN Tunnel > GRE**



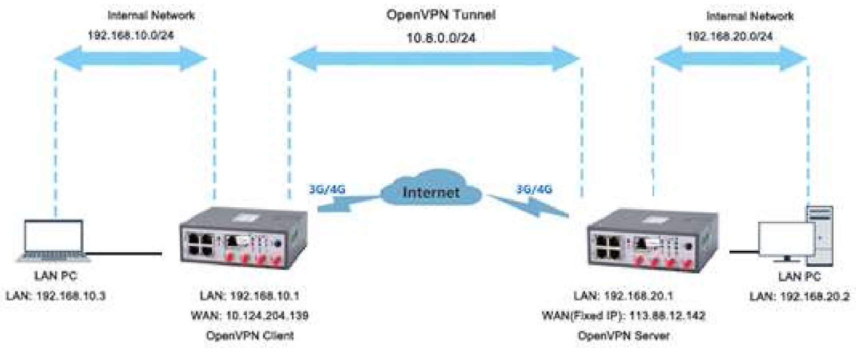
GRE Tunnel

On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	1	192.172.1.10	113.111.10.101	113.113.11.11	✓	10	5	B
☑					□			

GRE Route

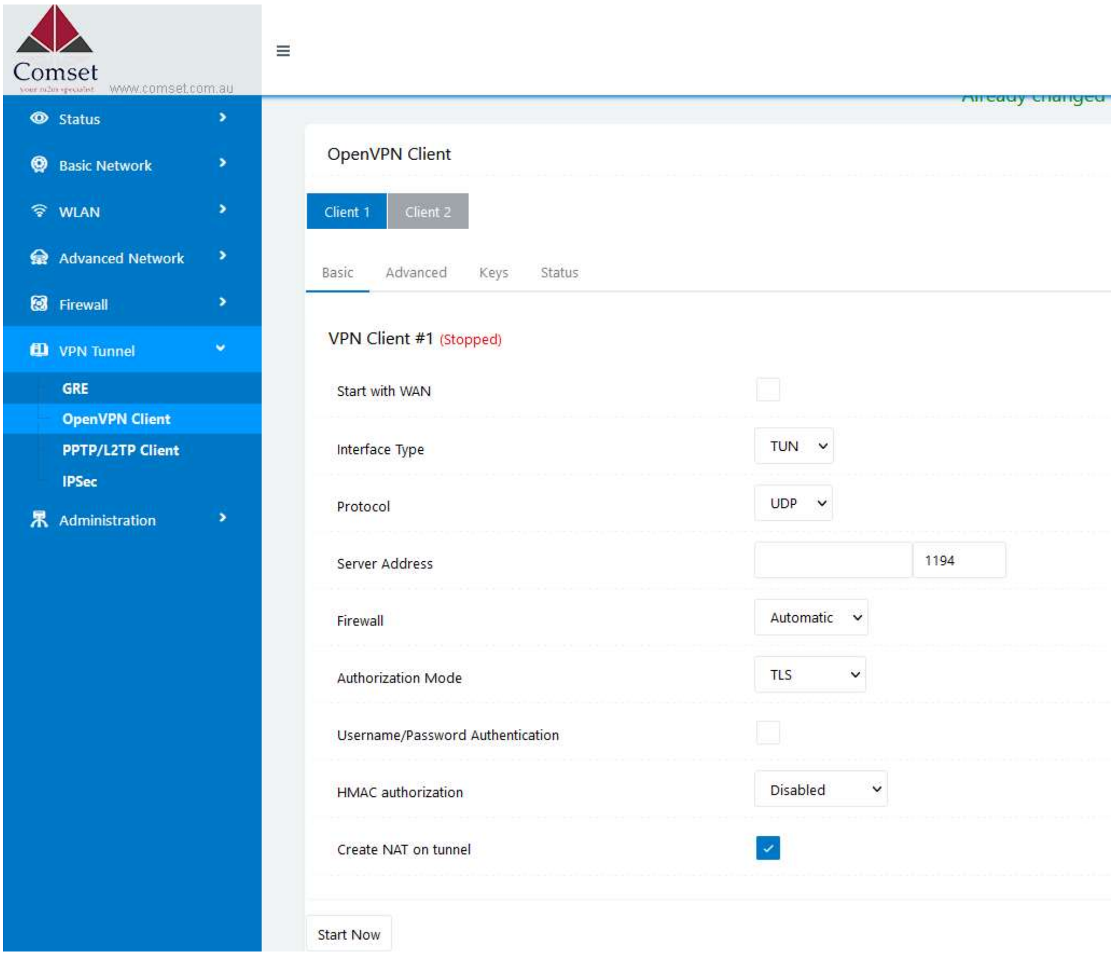
On	Tunnel Index	Destination Address	Description
✓	1	192.168.10.0/24	B
☑	1		

3.8.2 OpenVPN



OpenVPN between CM550W-POE client and Server

Go to “VPN Tunnel> OpenVPN Client” to check or modify the relevant parameters.



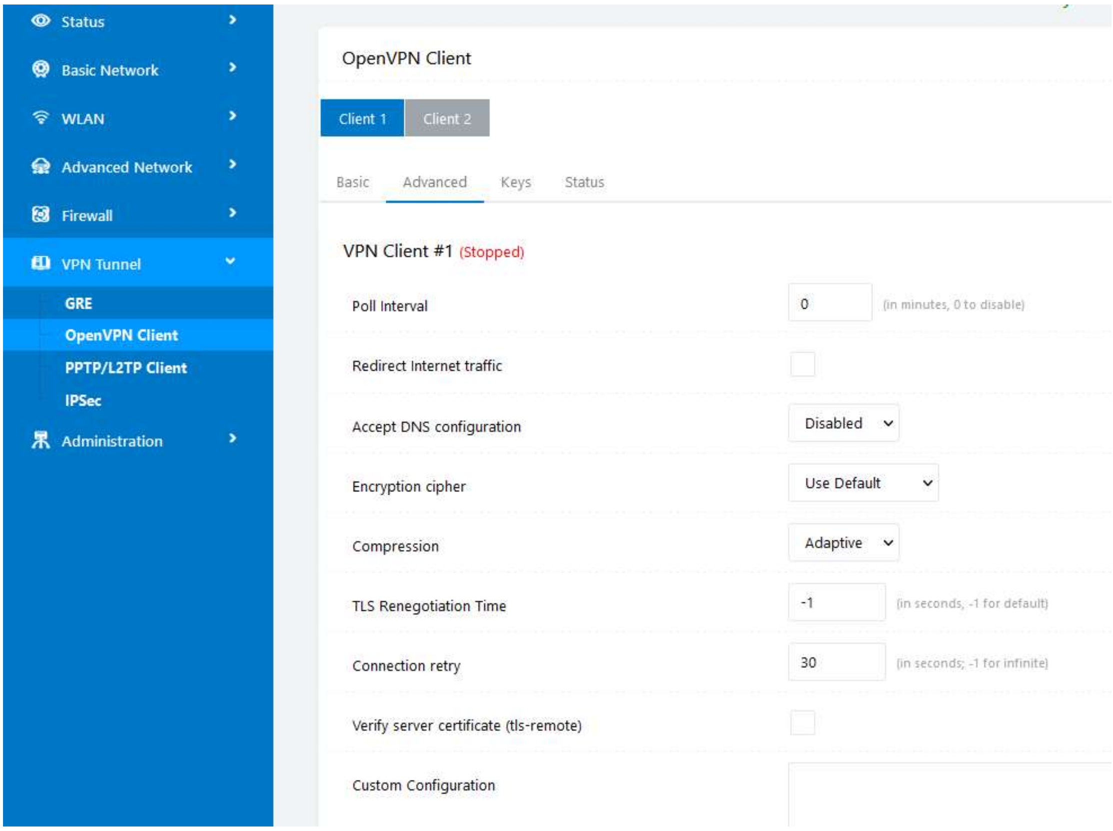
OpenVPN Client

VPN Client #1 (Stopped)

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

Item	Instructions
Start with WAN	Enable Openvpn for 5G/4G/3G/WAN port.

Interface Type	Tap and Tun types are optional. Tap is for bridge mode and Tunnel is for routing mode.
Protocol	UDP and TCP options.
Server Address	The Openvpn server public IP address and port.
Firewall	Auto Custom options.
Authorization Mode	TLS, Static key and Custom options.
Username/Password Authentication	As per user’s configuration.
HMAC authorization	As per user’s configuration.
Create NAT on tunnel	Configure NAT in Openvpn tunnel.



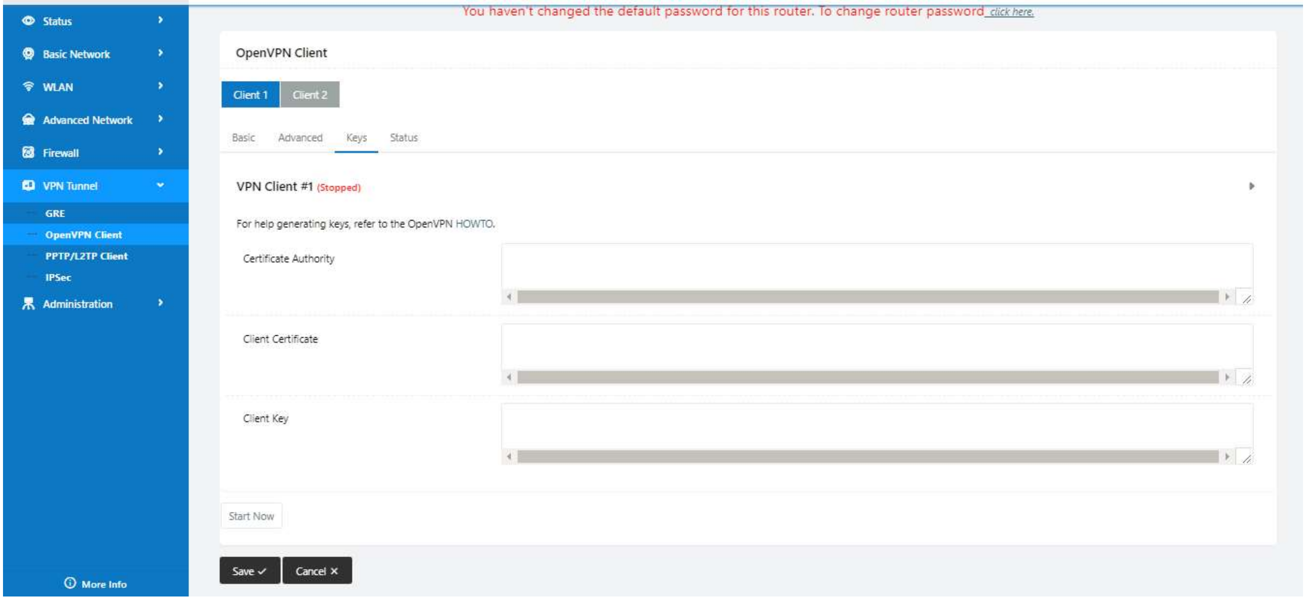
OpenVPN Client

VPN Client #1 (Stopped)

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		

Item	Instructions
Poll Interval	Openvpn client check router’s status at interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.

Access DNS	As per user's configuration.
Encryption	As per user's configuration.
Compression	As per user's configuration.
TLS Renegotiation Time	TLS negotiation time. -1 as default for 60s.
Connection Retry Time	Openvpn retry to connect time interval.
Verify server certificate	As per user's configuration.
Custom Configuration	As per user's configuration.



You haven't changed the default password for this router. To change router password click here.

OpenVPN Client

VPN Client #1 (Stopped)

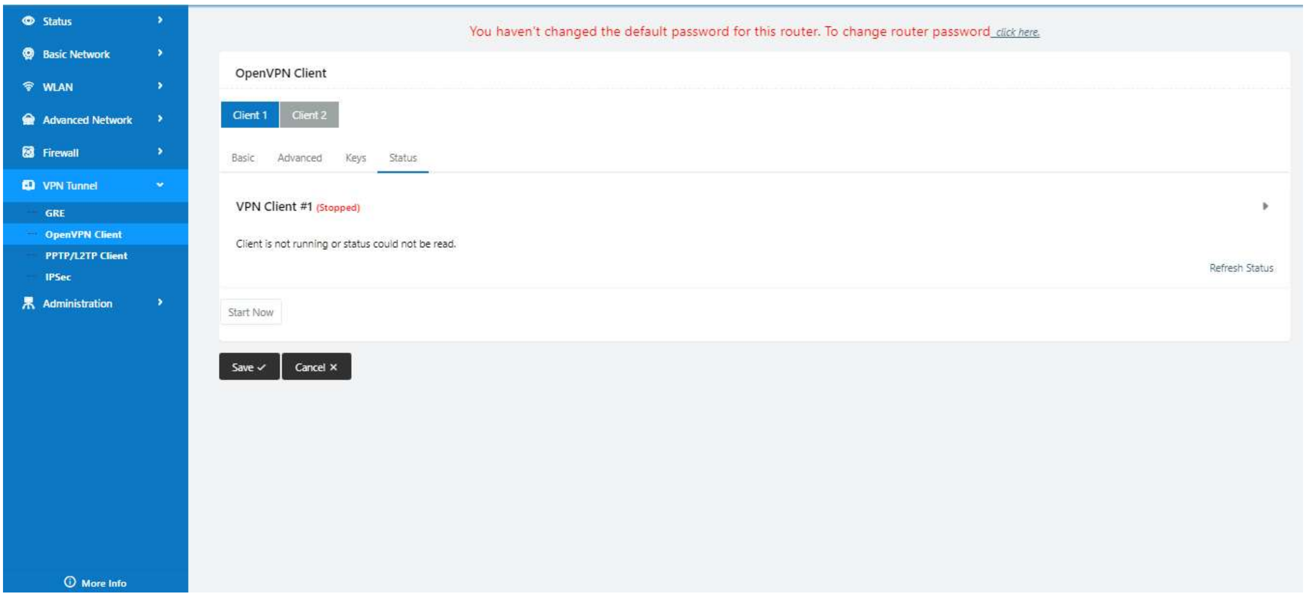
For help generating keys, refer to the OpenVPN HOWTO.

Certificate Authority

Client Certificate

Client Key

Item	Instructions
Certificate Authority	Keep the certificate the same as the server.
Client Certificate	Keep the client certificate the same as the server.
Client Key	Keep the client key the same as the server.



You haven't changed the default password for this router. To change router password click here.

VPN Client #1 (Stopped)

Client is not running or status could not be read.

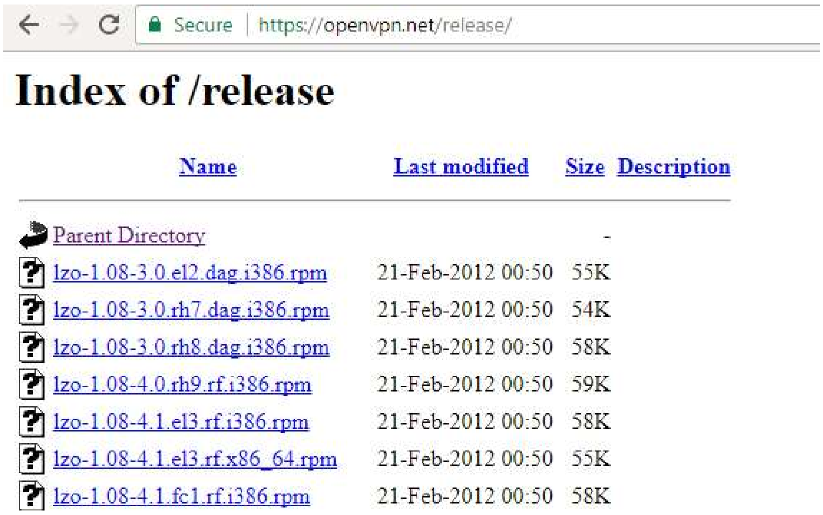
Item	Instructions
Status	Check OpenVPN status and data statistics.

Click “save” and “start now” to start OpenVPN.

OpenVPN Keys Guide

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

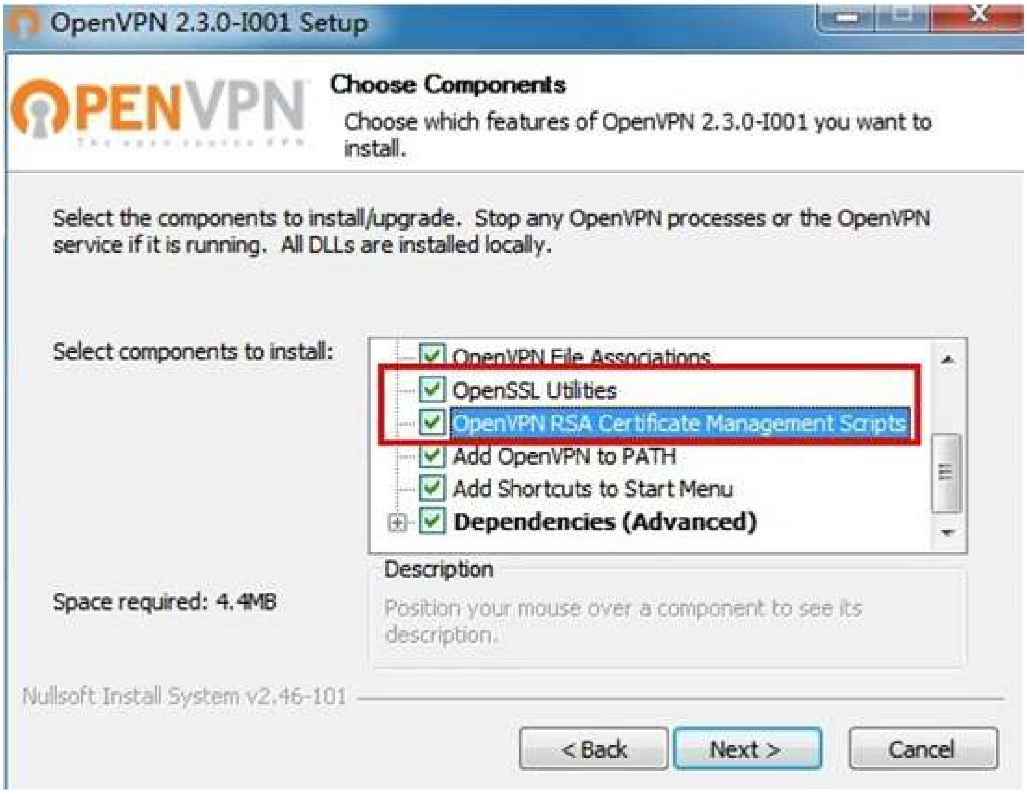
Access (http://openvpn.net/release/) and download the file “openvpn-2.3.0-install.exe” (or higher)



Index of /release

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

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



OpenVPN 2.3.0-I001 Setup

Choose Components

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

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

Select components to install:

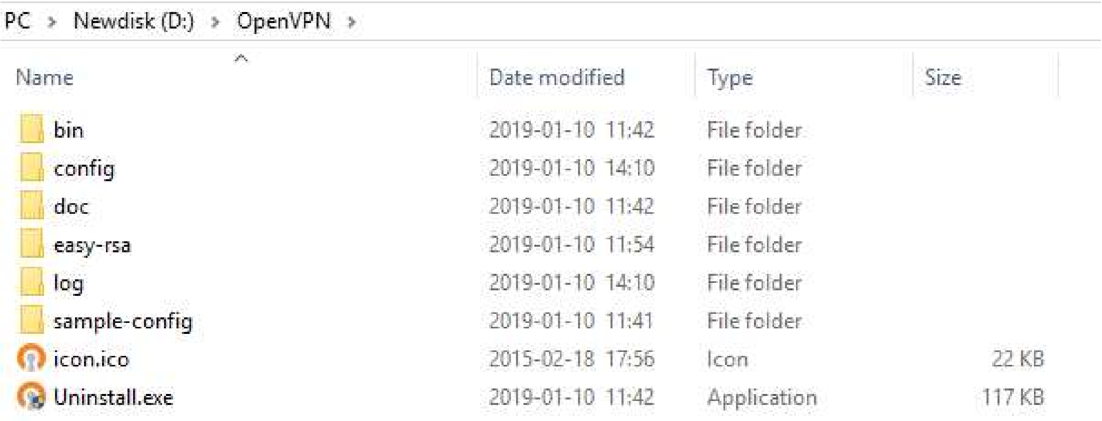
- ☑ OpenVPN File Associations
- ☑ OpenSSL Utilities
- ☑ OpenVPN RSA Certificate Management Scripts
- ☑ Add OpenVPN to PATH
- ☑ Add Shortcuts to Start Menu
- ☑ **Dependencies (Advanced)**

Space required: 4.4MB

Description

Position your mouse over a component to see its description.

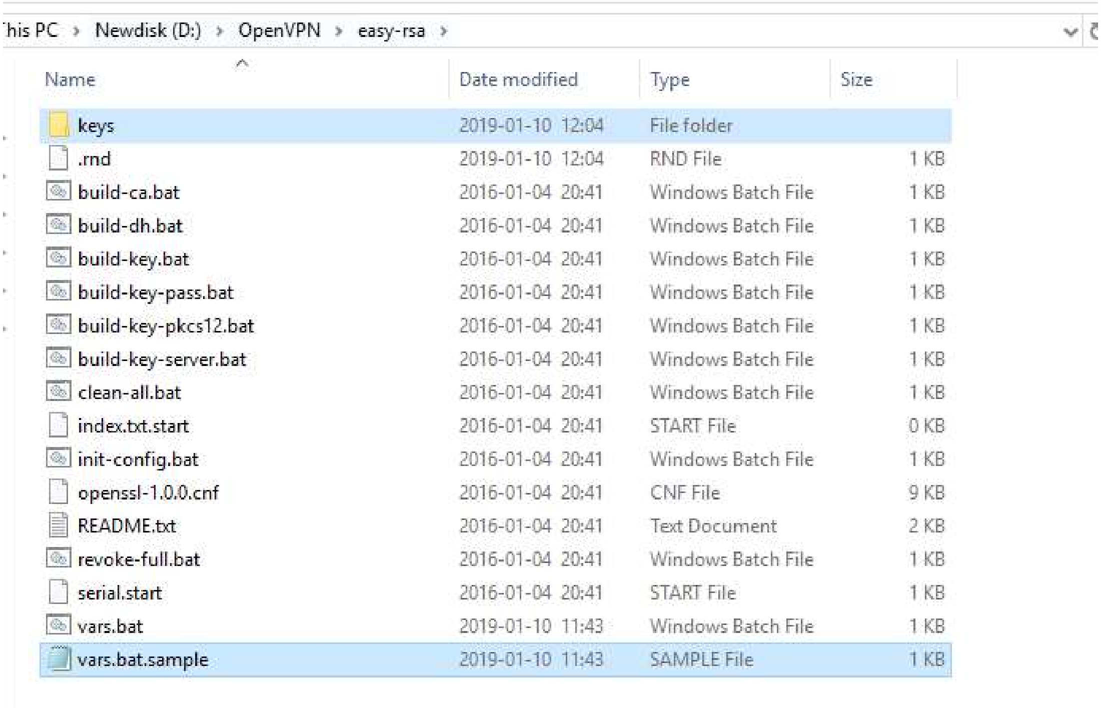
Nullsoft Install System v2.46-101



PC › Newdisk (D:) › OpenVPN ›

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

Configure “vas.bat.sample” to complete the initialisation steps and keys.

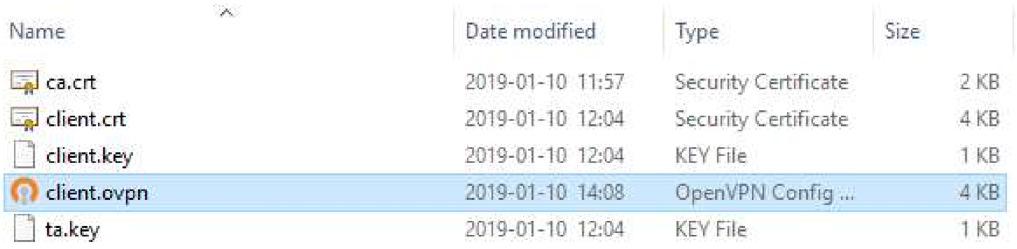


'his PC › Newdisk (D:) › OpenVPN › easy-rsa ›

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

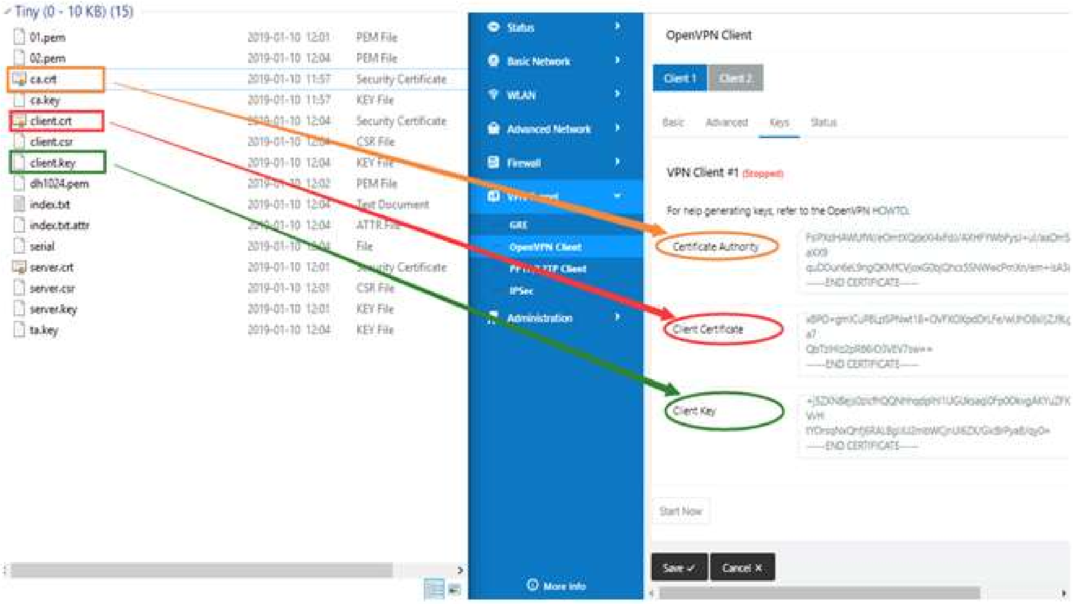
Configure the client keys to COMSET OpenVPN client GUI, when you create the server and client certificate in the path OpenVPN/easy-rsa/keys.

Client certificate (Generated on the server)



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

OpenVPN>easy-rsa>keys



Tiny (0 - 10 KB) (15)

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

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
[illegible]
-----END CERTIFICATE-----

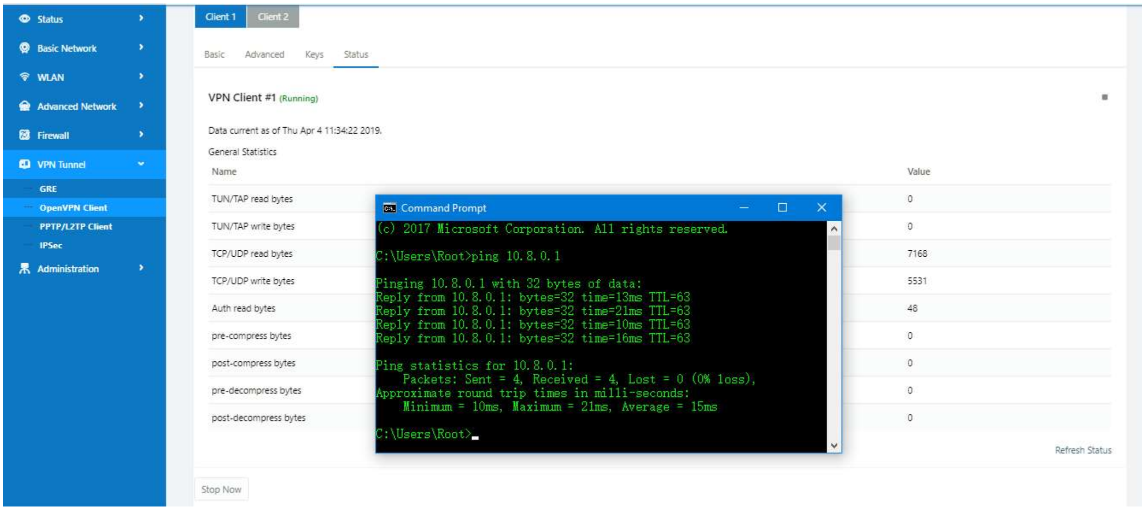
Client Certificate
[illegible]
-----END CERTIFICATE-----

Client Key
[illegible]
-----END CERTIFICATE-----

Start Now

Save ✓ | Cancel ✕

Ping test your server when the tunnel is established:



Client 1 | Client 2

Basic | Advanced | Keys | Status

VPN Client #1 (Running)

Data current as of Thu Apr 4 11:34:22 2019.

General Statistics

Name	Value
TUN/TAP read bytes	0
TUN/TAP write bytes	0
TCP/UDP read bytes	7168
TCP/UDP write bytes	5531
Auth read bytes	48
pre-compress bytes	0
post-compress bytes	0
pre-decompress bytes	0
post-decompress bytes	0

Refresh Status

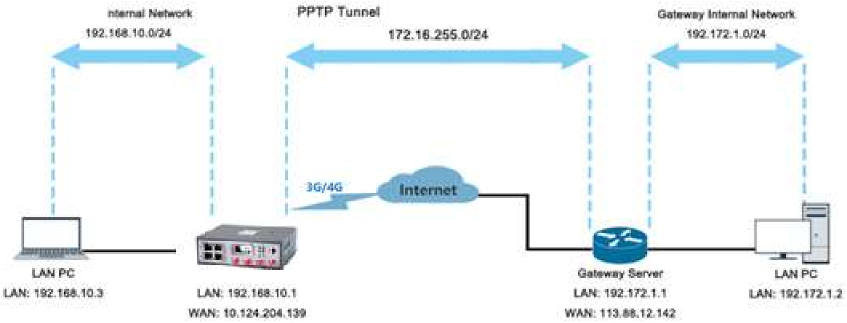
Stop Now

Command Prompt

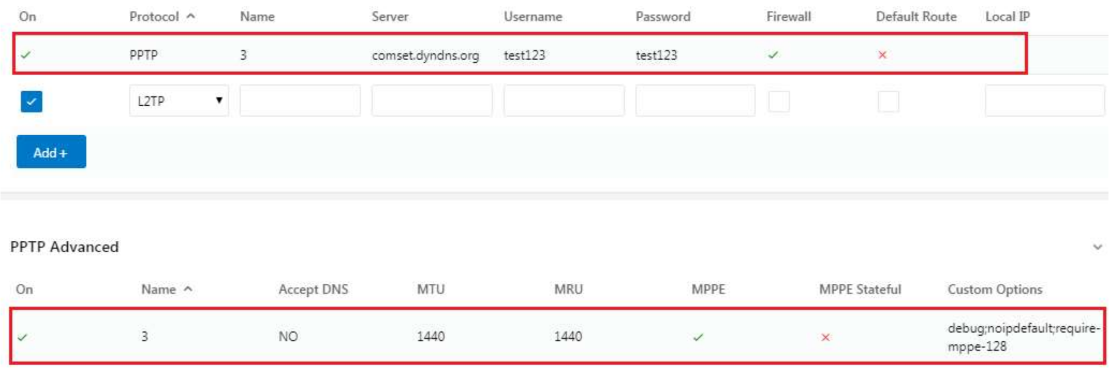
```
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Root>ping 10.8.0.1

Pinging 10.8.0.1 with 32 bytes of data:
Reply from 10.8.0.1: bytes=32 time=13ms TTL=63
Reply from 10.8.0.1: bytes=32 time=21ms TTL=63
Reply from 10.8.0.1: bytes=32 time=10ms TTL=63
Reply from 10.8.0.1: bytes=32 time=16ms TTL=63

Ping statistics for 10.8.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 21ms, Average = 15ms

C:\Users\Root>
```

3.8.3 L2TP/PPTP

Click “VPN Tunnel>PPTP/L2TP Client” to view or modify the relevant parameters.



Test case: PPTP



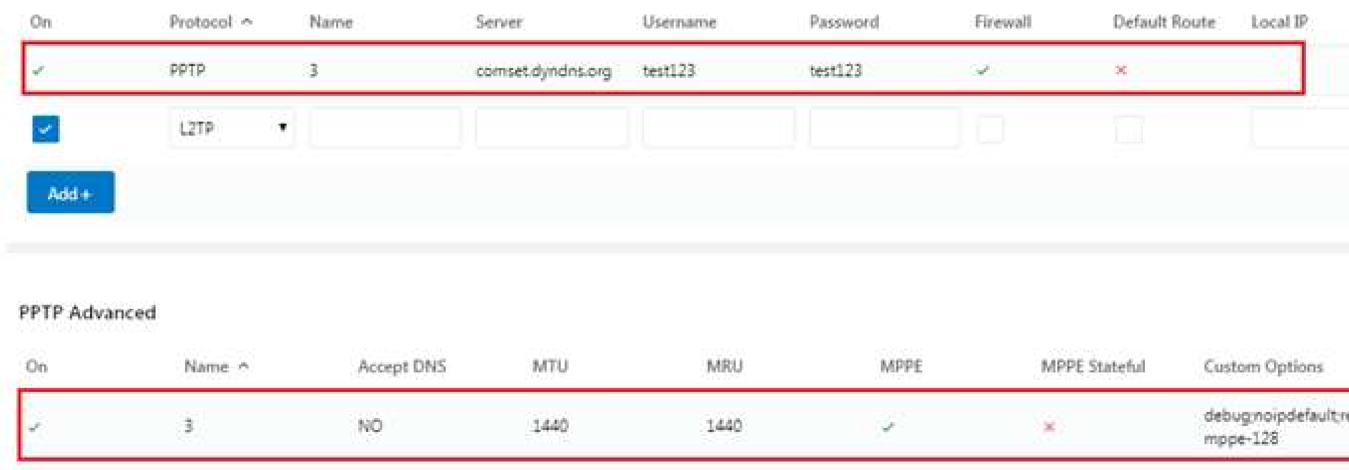
On	Protocol ^	Name	Server	Username	Password	Firewall	Default Route	Local IP
✓	PPTP	3	comset.dyndns.org	test123	test123	✓	✕	
☑	L2TP ▾					□	□	

PPTP Advanced

On	Name ^	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
✓	3	NO	1440	1440	✓	✕	debug;noipdefault;require-mppe-128

Note: The Custom Options are based on your server.

Test case: L2TP



On	Protocol ^	Name	Server	Username	Password	Firewall	Default Route	Local IP
✓	PPTP	3	comset.dyndns.org	test123	test123	✓	✕	
☑	L2TP ▾					□	□	

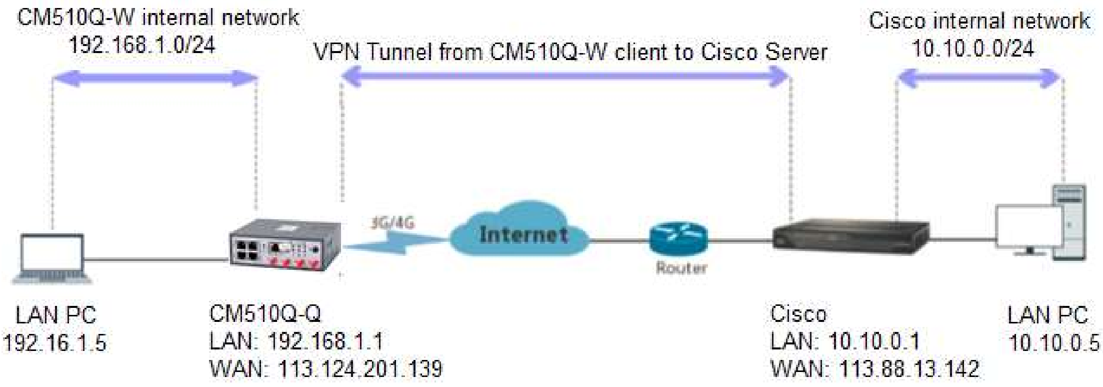
PPTP Advanced

On	Name ^	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
✓	3	NO	1440	1440	✓	✕	debug;noipdefault;re mppe-128

Note: The Custom options are based on your server.

3.8.4 IPSec

IPSec between a COMSET Router and a Cisco Router

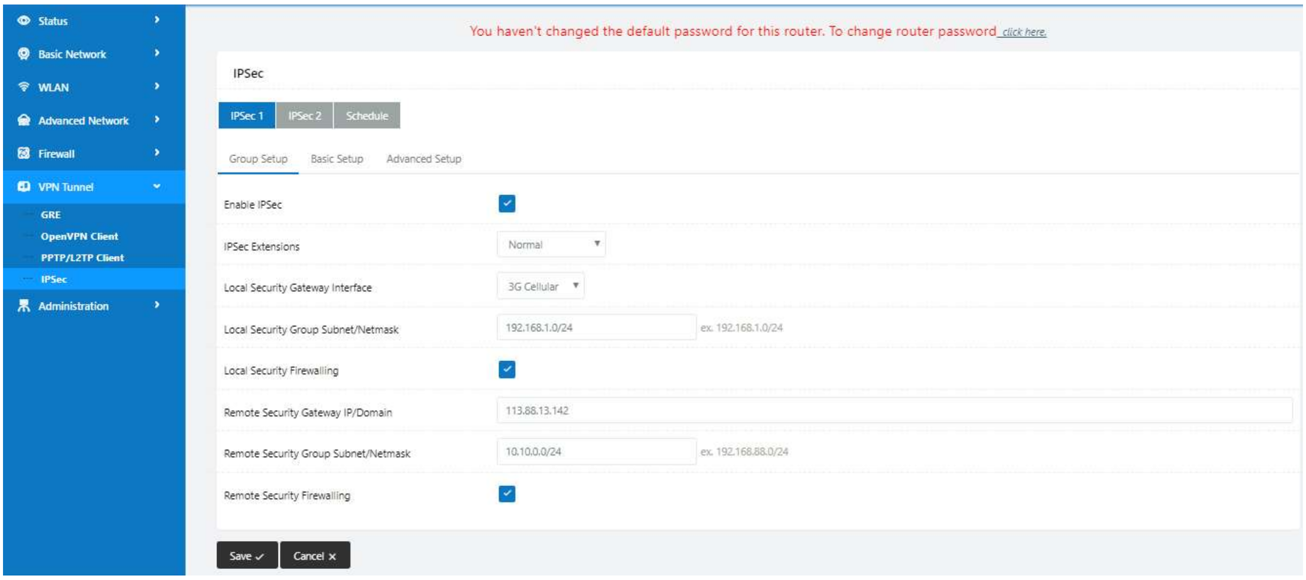


1) Cisco Configuration (main mode)

```
!

crypto isakmp policy 10

  encr 3des

  hash md5

  authentication pre-share

  group 2

crypto isakmp key test1234 address 0.0.0.0    0.0.0.0

!

!

crypto ipsec transform-set Tran-set esp-3des esp-sha-hmac

crypto ipsec nat-transparency spi-matching

!
```

2) COMSET Configuration

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

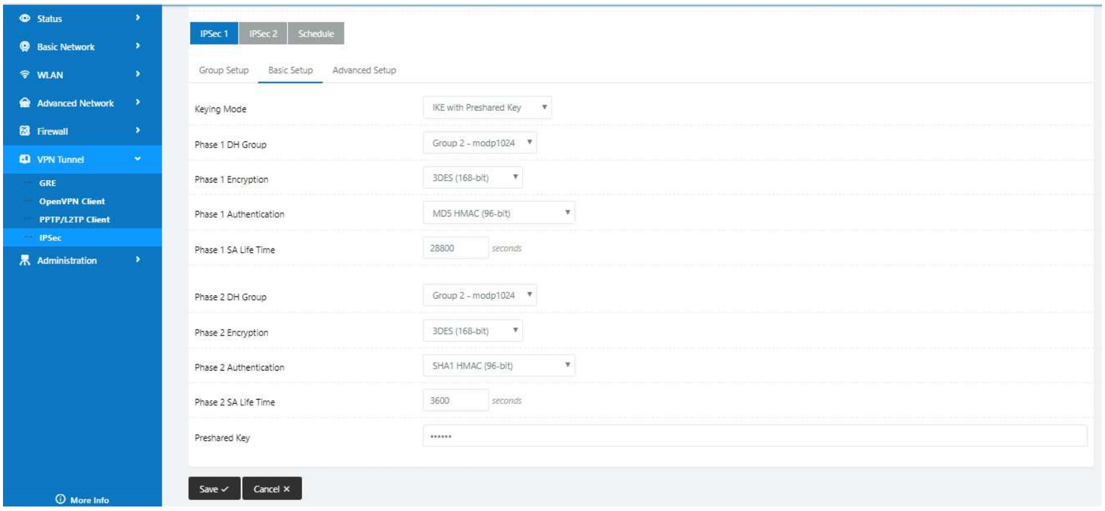


You haven't changed the default password for this router. To change router password click here.

IPSec

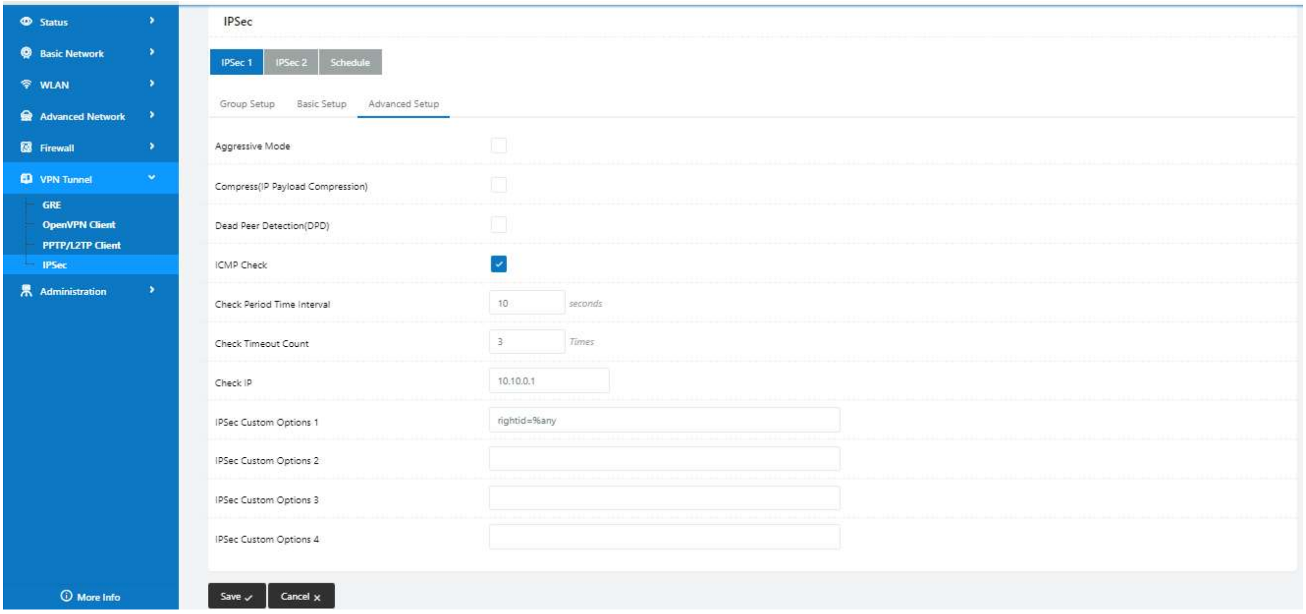
Enable IPSec	☑	
IPSec Extensions	Normal	
Local Security Gateway Interface	3G Cellular	
Local Security Group Subnet/Netmask	192.168.1.0/24	ex. 192.168.1.0/24
Local Security Firewalling	☑	
Remote Security Gateway IP/Domain	113.88.13.142	
Remote Security Group Subnet/Netmask	10.10.0.0/24	ex. 192.168.88.0/24
Remote Security Firewalling	☑	

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



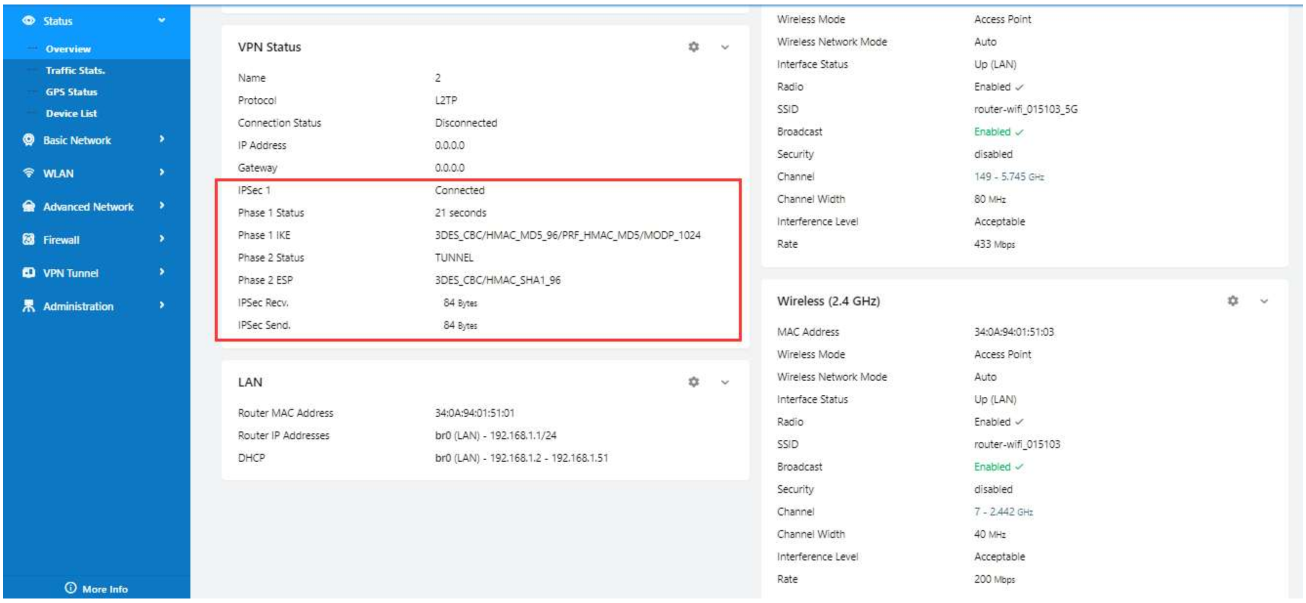
Keying Mode	IKE with Preshared Key	
Phase 1 DH Group	Group 2 - modp1024	
Phase 1 Encryption	3DES (168-bit)	
Phase 1 Authentication	MD5 HMAC (96-bit)	
Phase 1 SA Life Time	28800	seconds
Phase 2 DH Group	Group 2 - modp1024	
Phase 2 Encryption	3DES (168-bit)	
Phase 2 Authentication	SHA1 HMAC (96-bit)	
Phase 2 SA Life Time	3600	seconds
Preshared Key	••••••	

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



IPSec

Aggressive Mode	□
Compress(IP Payload Compression)	□
Dead Peer Detection(DPD)	□
ICMP Check	☑
Check Period Time Interval	10 seconds
Check Timeout Count	3 Times
Check IP	10.10.0.1
IPSec Custom Options 1	rightid=%any
IPSec Custom Options 2	
IPSec Custom Options 3	
IPSec Custom Options 4	



VPN Status

Name	2
Protocol	L2TP
Connection Status	Disconnected
IP Address	0.0.0.0
Gateway	0.0.0.0
IPSec 1	Connected
Phase 1 Status	21 seconds
Phase 1 IKE	3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
Phase 2 Status	TUNNEL
Phase 2 ESP	3DES_CBC/HMAC_SHA1_96
IPSec Recv.	84 Bytes
IPSec Send.	84 Bytes

LAN

Router MAC Address	34:0A:94:01:51:01
Router IP Addresses	br0 (LAN) - 192.168.1.1/24
DHCP	br0 (LAN) - 192.168.1.2 - 192.168.1.51

Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up (LAN)
Radio	Enabled ✓
SSID	router-wifi_015103_5G
Broadcast	Enabled ✓
Security	disabled
Channel	149 - 5.745 GHz
Channel Width	80 MHz
Interference Level	Acceptable
Rate	433 Mbps

Wireless (2.4 GHz)

MAC Address	34:0A:94:01:51:03
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up (LAN)
Radio	Enabled ✓
SSID	router-wifi_015103
Broadcast	Enabled ✓
Security	disabled
Channel	7 - 2.442 GHz
Channel Width	40 MHz
Interference Level	Acceptable
Rate	200 Mbps