



Dual SIM Dual band Gigabit Router

CM510Q-W

V1.2

19

Copyright © COMSET 2019

Comset is a registered trademark of Comset. Other brands used in this manual are trademarks of their registered holders.

Specifications are subject to change without notice. No part of this manual may be reproduced without the consent of Comset. All rights reserved.

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

Table of Contents

1 Product Introduction.....	5
1.1 Product overview	5
1.2 Typical Application Diagram	5
1.3 Features.....	6
2 Hardware Installation	7
2.1 Panel.....	7
2.2 LED Status.....	9
2.3 Powering up the CM510 Router	10
3 Router Configuration.....	13
3.1 Configuration from a local network.....	13
3.2 Basic Configuration.....	14
3.3 Tools, Bandwidth, IP Traffic and System	18
3.4 Basic Network.....	22
3.5 WLAN Settings	34
3.6 Advanced Network Settings	37
3.7 Firewall	48
3.8 VPN Tunnel	50
3.9 Administration.....	65
3.9.1 Identification Settings	65
3.9.2 Time Settings.....	66

3.9.3 Admin Access Settings.....	66
3.9.4 Scheduled Reboot Settings.....	67
3.9.5 SNMP Settings	68
3.9.6 Storage Settings	69
3.9.7 M2M Access Settings.....	70
3.9.8 DI/DO Settings.....	71
3.9.9 Configuration Settings	78
3.9.10 System Log Settings	78
3.9.11 Firmware Upgrade.....	79
3.10 Reset Button to Restore Factory Settings	81
4 Configuration Examples.....	82
4.1 Port Forwarding	82
4.2 IP Pass-through.....	84
4.3 Captive Portal	87
4.4 GPS Settings (GPS version only).....	90
4.5 Firewall	91
4.6 VPN Tunnel	93

1 Product Introduction

1.1 Product overview

The Comset CM510Q-W is an industrial grade LTE CAT 6 Modem Router with download speeds of up to 300 Mbps and upload speeds of up to 50 Mbps. With four Gigabit Ethernet ports and concurrent 2.4GHz and 5GHz dual band WiFi, it provides a powerful and rapidly deployable internet solution to commercial customers and small to medium businesses.

The Comset CM510Q-W is an innovative router powered by the latest ARM Cortex A7 900MHz CPU. It features dual SIM card slots for backup redundancy, dual band WiFi 802.11ac to help reduce WiFi traffic congestion and interference and ensure a fast and reliable service, 3 x Gigabit LAN ports for fast wired connections, 1 Gigabit WAN/LAN port, as well as a GPIO with two digital input ports and one digital output port. Other features include VPN IPSEC, PPTP (Server and Client), L2TP and OpenVPN to establish a secure connection over the 3G/4G network.

The innovative design, easy integration and rich built-in features make the CM510Q-W the router of choice for a wide range of business and commercial applications, including SOHO, SMB, industrial automation, building automation, security, surveillance, transportation, health, mining and environmental monitoring.

1.2 Typical Application Diagram

The Comset CM510Q-W 3G/4G/4GX Router is suitable for a wide range of machine-to-machine applications (M2M), as shown in the illustration below:

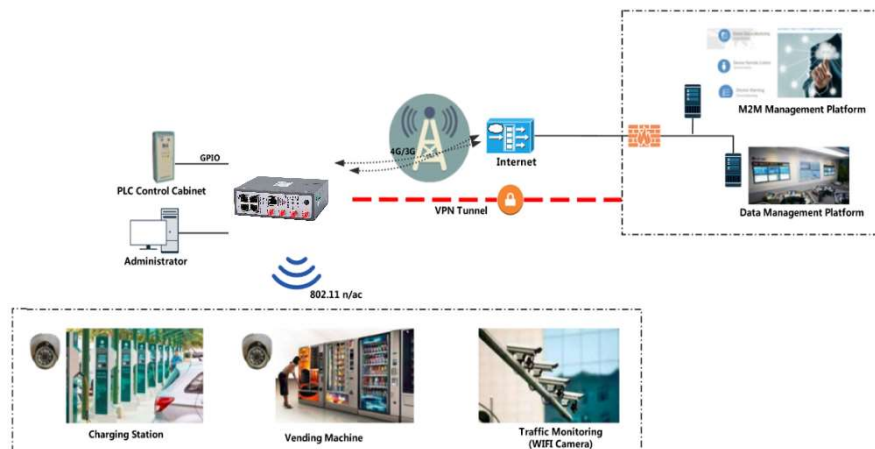


Figure 1-1 Network Topology

1.3 Features

The CM510Q-W supports the following:

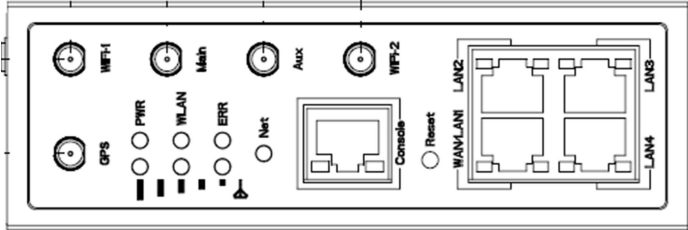
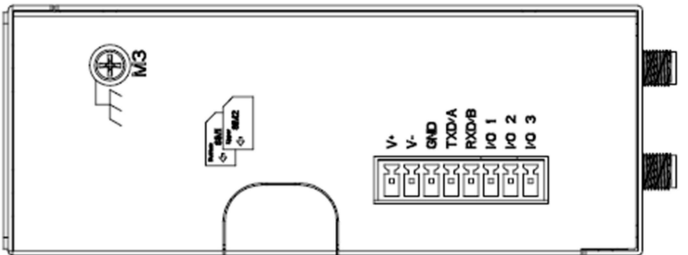
- 4G LTE FDD B1 (2100), B3 (1800), B5 (850), B7 (2600), B8 (900), B20 (800), B28 (700), B32 (1500)
- 4G LTE TDD B38 (2600), B40 (2300), B41 (2500)
- 2 x CA Carrier Aggregation
 - B1+B1/B5/B8/B20/B28;
 - B3+B3/B5/B7/B8/B20/B28;
 - B7+B5/B7/B8/B20/B28;
 - B20+B32;
 - B38+B38;
 - B40+B40;
 - B41+B41
- UMTS/HSPA/HSUPA/HSPA+/DC-HSPA+ 850/900/1900/2100MHz
- Powerful Cortex A7 900MHz CPU
- Concurrent dual band 2.4GHz and 5GHz 802.11 b/g/n/ac
- Four Gigabit Ethernet ports
- Heavy-duty metal enclosure
- DIN Rail mounting
- Shock and vibration resistant
- Schedule reboot via timing/SMS/RMS Software
- Wide temperature range: -30 to +75 degree C
- Built-in watch dog
- Strong electromagnetic interference resistance
- Non-polarity and Anti-reverse power protection
- Firewall and VPN tunnel security (IPsec, OpenVPN, GRE, L2TP and PPTP)

2 Hardware Installation

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

2.1 Panel

Table 2-1 CM510 Interface

COMSET	CM510
Front	
Top	



The Antenna interface and LED lights can be different depending on options such as extended WiFi and GPS.

Table 2-2 Router Interface

Ports	Instructions	Remarks
USIM	Plug type SIM Slot, supports 1.8/3V/5V automatic detection.	
Main	3G/4G antenna, SMA connector, 50Ω.	
Aux	3G/4G antenna, SMA connector, 50Ω.	
GPS	GPS antenna, SMA connector, 50Ω.	GPS optional
Wi-Fi	Two dual-band Wi-Fi antennas, SMA connector.	
LAN	10/100/1000Base-TX, MDI/MDIX self-adaption.	
WAN/LAN	10/100/1000Base-TX, MDI/MDIX self-adaption.	Default as LAN
Reset	Reset button. Press and hold for at least 5 seconds.	
PWR	Power connector.	7.5 ~ 32V DC
I/O	DI-1 and DI-2 are digital input. DO is digital output.	
Console	RJ45-DB9 cable for CLI configuration.	

2.2 LED Status

Table 2-3 Router LED indicator Status

LED	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 quickly		Data is being transmitted.
	Dark		WLAN disabled.
ERR	Dark		System operation and LTE/3G online.
	Solid Light (Red)		System fail indicator. It indicates failure with SIM card/module.
LAN	Green	Solid light	Connected.
	Green	Blinking	Data is being transmitted.
	Green	Dark	Disconnected.



NOTE

The LED indicators can be different depending on additional options such as extended Wi-Fi, GPS function or single/double SIM.

Dimensions

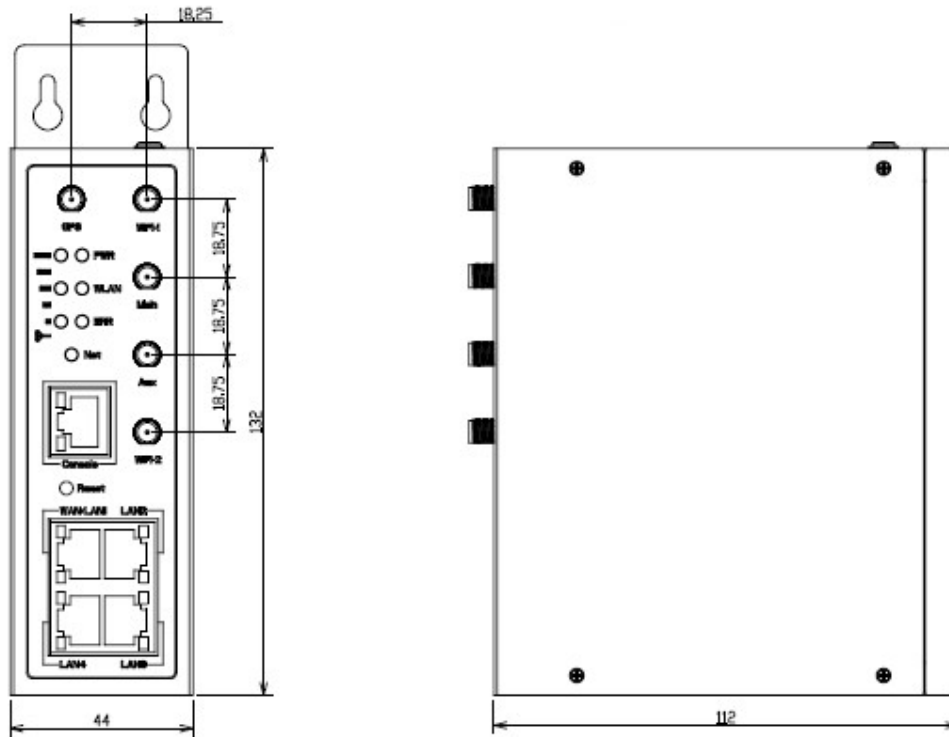


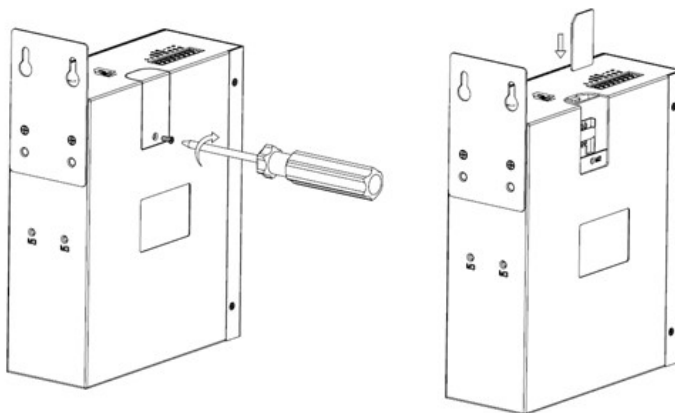
Figure 2-2 CM510 Series Router Dimensions

Note: Mounting brackets can be different

2.3 Powering up the CM510 Router

2.3.1 SIM/UIM card installation

Please insert the SIM card(s) prior to configuring the router.





Before connecting any cables, please disconnect the power source.

2.3.2 Ethernet Cable and Antenna Connection

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

Connect the two magnetic base 4g antennas to the Main and Aux SMA sockets, and the two paddle-shape WiFi antennas to the WiFi1 and WiFi2 SMA sockets. The WiFi antennas support dual-band 2.4GHz and 5GHz.

2.3.3 Serial Port (terminal block) Connection

If you want to connect the router via a serial port to your laptop or any other device, you need to prepare a serial cable or a RJ45 cable. One end connects to the computer serial port, the other end connects to the console port of the router or the terminal block.



Before connecting the serial cable, please disconnect any power source.

Pin	Instruction	Remark
1	V+	Power V+, Anti reverse
2	V-	Power V-
3	GND	GND for RS232 communication
4	RXD/A	RS232 RXD, 57600bps as default
5	TXD/B	RS232 TXD, RS485 optional
6	DI-1	Digital Input, Dry Contact
7	DI-2	Digital Input, Dry Contact
8	DO	Short to GND

2.3.4 Console Port Connection

For CLI configuration and router system debugging, please connect the router console port to a computer using a RJ45-DB9 cable.

Pins	Instructions	Remarks
1	CTS	Input
2	RTS	Output
3	RXD	Input
4	TXD	Output
5	GND	GND
6	DSR	Input
7	DCD	Output
8	DTR	Output

2.3.5 Power Supply

The CM510 router supports a wide range of DC voltage between 7.5VDC and 32VDC.

2.3.6 Review

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



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 industrial Router.

3 Router Configuration

The CM510Q-W can be configured via a web interface using a web browser such as Internet Explorer, Firefox or Google Chrome.

3.1 Configuration from a local network

To configure the CM510Q-W, 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 the “Network Connections” icon and double click it. Select “Local Area Connection” corresponding to the network card on this page. Refer to the figure below:

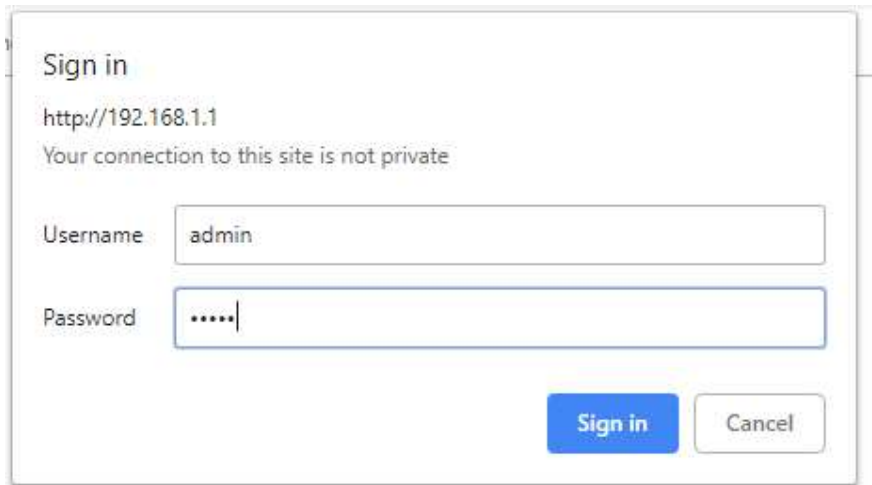


Figure 3-3 Network Connection

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 username is “admin” and the password is “admin”.



Sign in

http://192.168.1.1

Your connection to this site is not private

Username: admin

Password:

Sign in Cancel

Figure 3-4 User Interface

3.2 Basic Configuration

3.2.1 Overview

Below is an overview screenshot of the user interface of the CM510Q-W.

The screenshot displays the Comset router's web management interface. On the left is a blue sidebar with a navigation menu. The main content area on the right shows system information and port status.

Comset
www.comset.com.au

Status (selected)

- Overview
- Traffic Stats.
- Device List
- Basic Network
- WLAN
- Advanced Network
- Firewall
- VPN Tunnel
- Administration

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

System

Router Name	Comset Router
Hardware Version	C11-D13
Firmware Version	G5.0.1.5
Router Sn	1113G511908120002
Chipset	ARMv7 Processor rev 5 (v7l)
Router Time	Fri, 20 Sep 2019 09:41:09 +1000 Clock Sync.
Uptime	00:07:33
Memory Usage	38.73 MB / 122.22 MB (31.69%)
NVRAM Usage	24.47 KB / 64.00 KB (38.24%)

Ethernet Ports Status

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

VPN Status

No Active VPN

Status

Overview

Traffic Stats.

Device List

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

LAN

Router MAC Address

34:0A:98:12:55:05

Router IP Addresses

br0 (LAN) - 192.168.1.1/24

DHCP

br0 (LAN) - 192.168.1.2 - 192.168.1.51

WAN

Connection Type

Cellular Network

Modem IMEI

868186040120352

Modem BAND

B7 + B7

Modem CA

Yes

Modem Status

Ready

Cellular ISP

"Telstra Mobile Telstra"

Cellular Network

LTE Band 7

USIM Selected

USIM Card 1 Running...

USIM Status

Ready

CSQ

25/31, dBm: -63

IP Address

10.98.185.164

Subnet Mask

255.255.255.248

Gateway

10.98.185.165

DNS

10.4.130.164:53, 10.5.136.242:53

Connection Status

Connected

Connection Uptime

00:07:43

Remaining Lease Time

01:52:01

The screenshot displays the Router Status GUI. On the left is a blue sidebar with navigation links: Status (selected), Overview, Traffic Stats., Device List, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel, and Administration. The main content area shows two sections: 'Wireless (5 GHz)' and 'Wireless (2.4 GHz)'. Each section lists various settings and their current values.

Wireless (5 GHz)	
MAC Address	34:0A:98:12:55:08
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up (LAN)
Radio	Enabled ✓
SSID	Comset Router_125507_5G
Broadcast	Enabled ✓
Security	WPA / WPA2 Personal + TKIP / AES
Channel	149 - 5.745 GHz
Channel Width	80 MHz
Interference Level	Acceptable
Rate	433 Mbps

Wireless (2.4 GHz)	
MAC Address	34:0A:98:12:55:07
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up (LAN)
Radio	Enabled ✓
SSID	Comset Router_125507
Broadcast	Enabled ✓
Security	WPA / WPA2 Personal + TKIP / AES
Channel	7 - 2.442 GHz
Channel Width	40 MHz
Interference Level	Acceptable
Rate	200 Mbps

Figure 3-5 Router Status GUI

**NOTE**

After 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.](#)

System Status

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

Already changed login password successfully.

3.2.2 Traffic Statistics

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



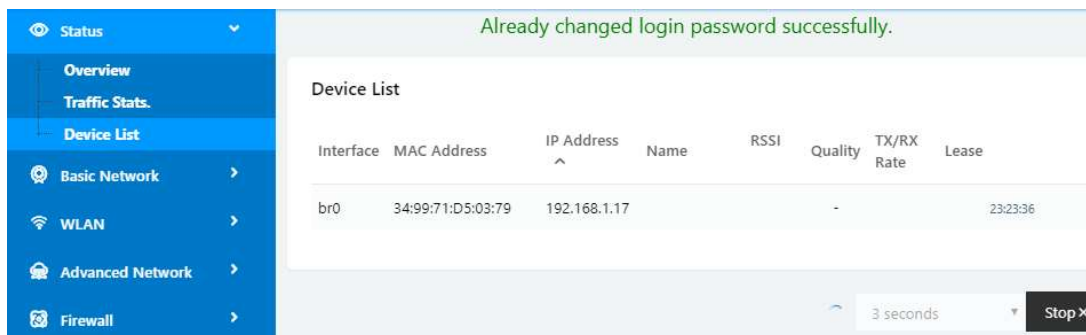
Already changed login password successfully.

Traffic Stats.

Interface	Transmit Data	Receive Data
Cellular(usb0)	12.50 MB	11.29 MB

3.2.3 Device List

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



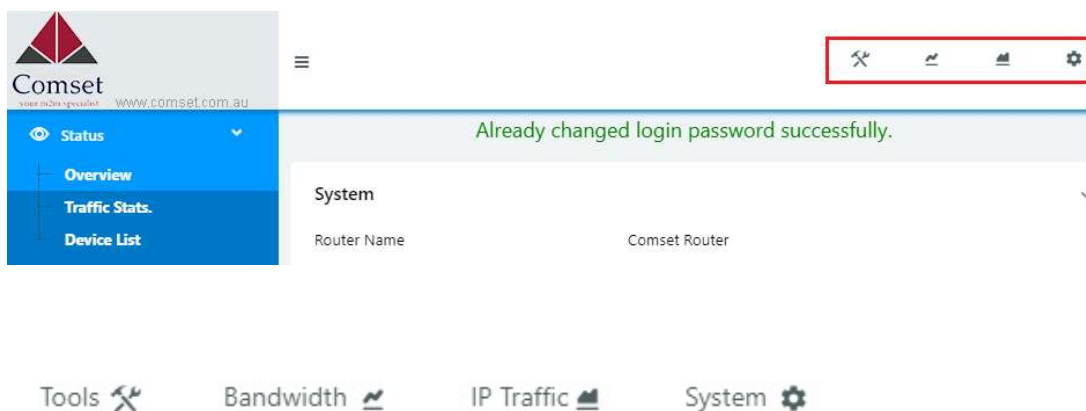
Already changed login password successfully.

Device List

Interface	MAC Address	IP Address	Name	RSSI	Quality	TX/RX Rate	Lease
br0	34:99:71:D5:03:79	192.168.1.17			-		23:23:36

3 seconds Stop X

3.3 Tools, Bandwidth, IP Traffic and System



Comset
www.comset.com.au

Already changed login password successfully.

System

Router Name	Comset Router

Tools Bandwidth IP Traffic System

3.3.1 Tools

3.3.1.1 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.

Already changed login password successfully.

Ping

IP Address: 8.8.8.8 [Ping]

Ping Count: 5

Packet Size: 56 (bytes)

Seq	Address	RX Bytes	TTL	RTT (ms)	+/- (ms)
0	8.8.8.8 (8.8.8.8)	64	54	54.33	
1	8.8.8.8 (8.8.8.8)	64	54	34.07	-20.26
2	8.8.8.8 (8.8.8.8)	64	54	42.99	8.92
3	8.8.8.8 (8.8.8.8)	64	54	31.80	-11.20
4	8.8.8.8 (8.8.8.8)	64	54	40.80	9.00

Round-Trip: 31.795 min, 40.797 avg, 54.331 max
Packets: 5 transmitted, 5 received, 0% lost

3.3.1.2 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.

Already changed login password successfully.

Trace

IP Address: 8.8.8.8 [Trace]

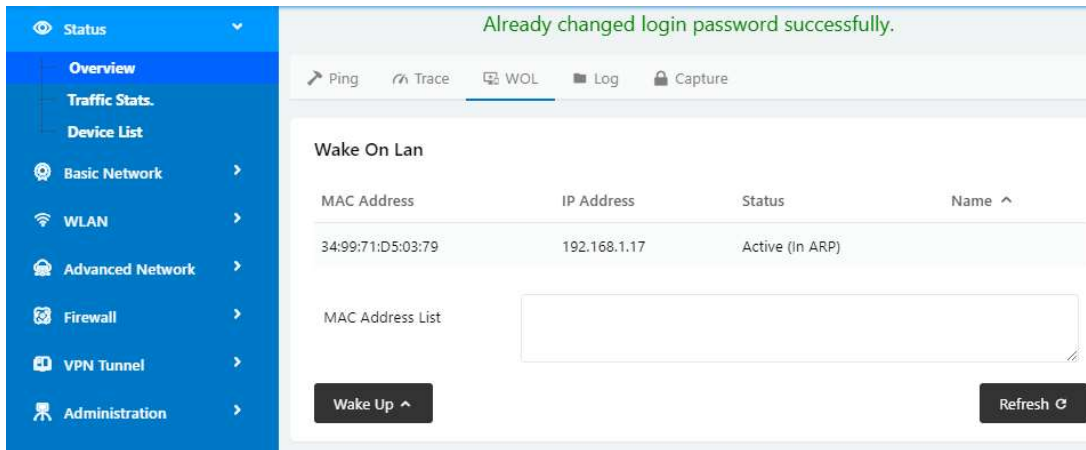
Maximum Hops: 20

Maximum Wait Time: 3 (seconds per hop)

Hop	Address	min (ms)	max (ms)	avg (ms)	+/- (ms)
1	8.8.8.8				

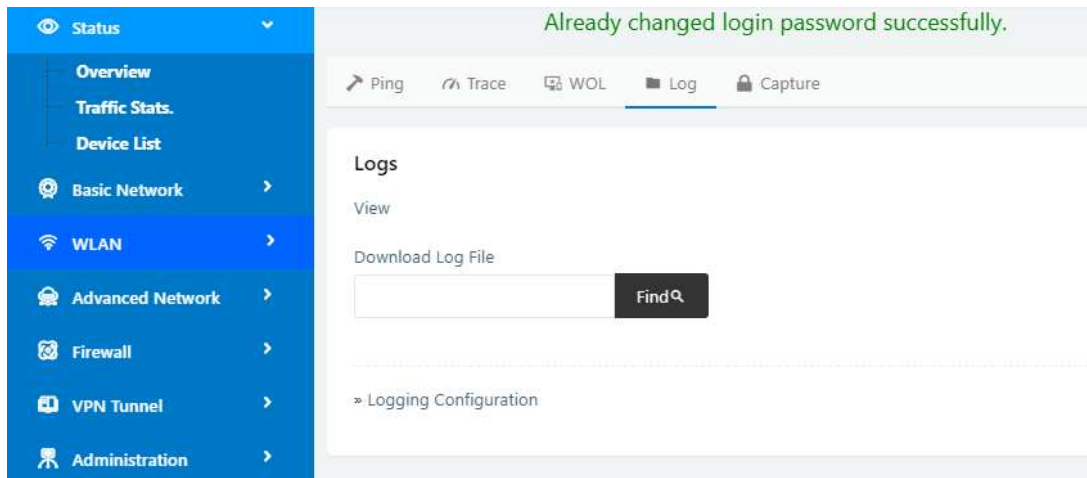
3.3.1.3 WOL

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.



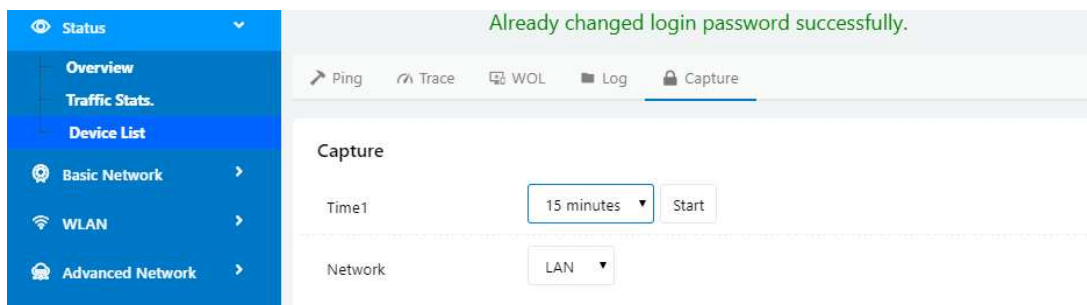
3.3.1.4 Log

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



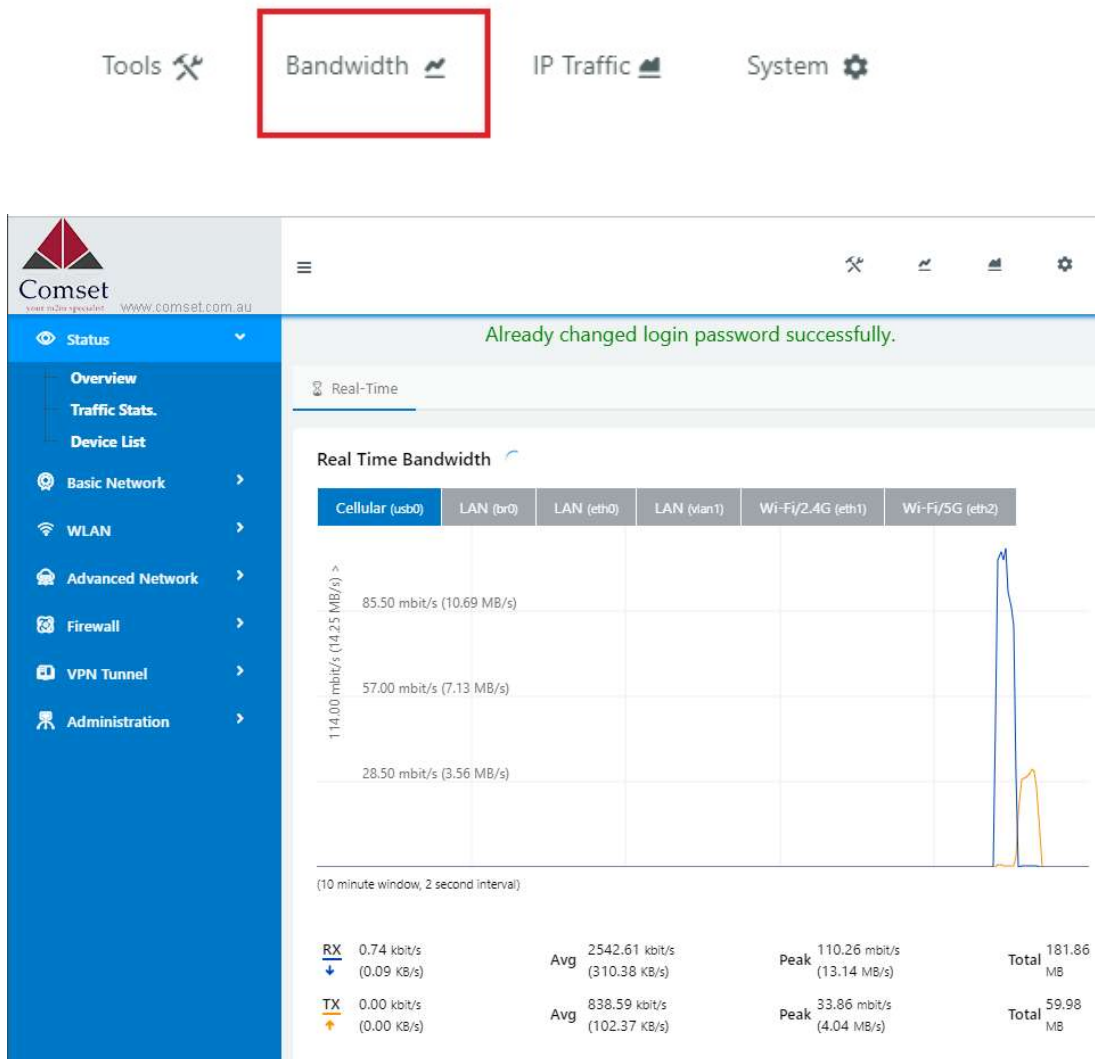
3.3.1.5 Capture

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



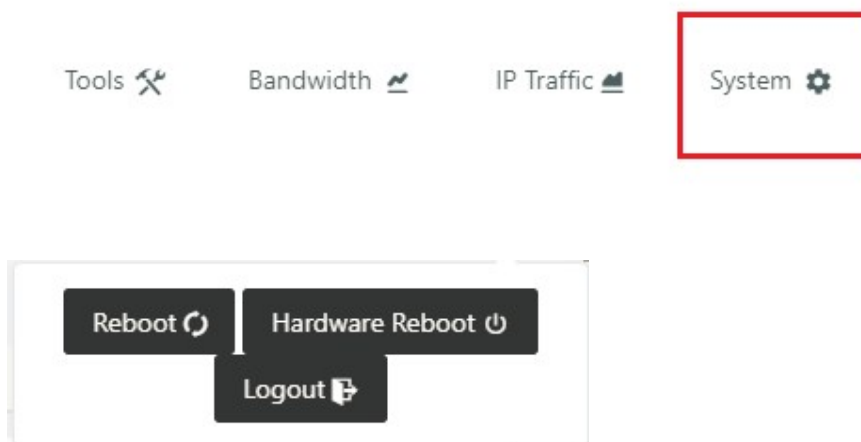
3.3.2 Bandwidth

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



3.3.3 System

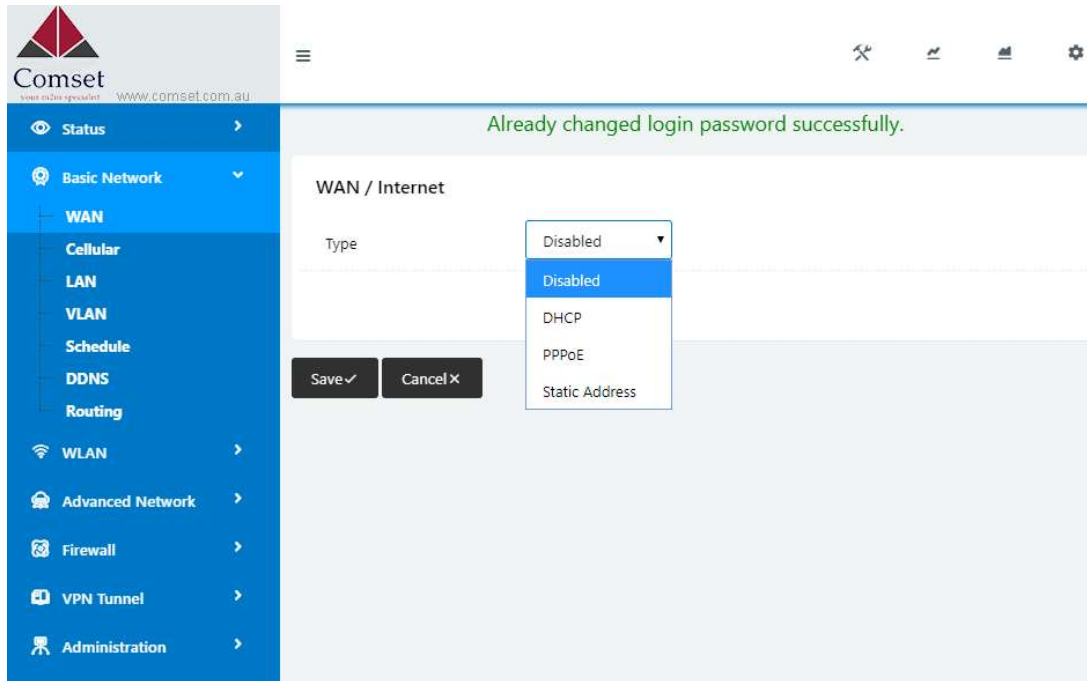
Click on “System” to perform a software reboot, hardware reboot or to logout.



3.4 Basic Network

3.4.1 WAN Settings


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








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

3.4.2 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”.


Comset
www.comset.com.au



Status

Basic Network

WAN

Cellular

LAN

VLAN

Schedule

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

Already changed login password successfully.

Cellular Settings

Enable Modem ☒

Basic Settings

SIM 1

SIM 2

Use PPP ☐

ICMP Check ☐

Cellular Traffic Check ☐

CIMI Send to

SMS Code

Operator Lock ex:46001

Band Lock Auto

Currently Available Bands: B7

DualSim Mode

Fail Over

Fail Over

SIM 1 Only

SIM 2 Only

Backup

Save ✓

Cancel ✕

Cellular Settings

Enable Modem



Basic Settings

SIM 1

SIM 2

SIM 1 Mode

Auto ▼

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

Save ✓

Cancel ✕

Cellular Settings

Enable Modem ☒

Basic Settings	SIM 1	SIM 2
SIM 2 Mode		Auto ▼
SIM 2 PIN Code		
SIM 2 APN		telstra.internet
SIM 2 User		
SIM 2 Password		
SIM 2 Dial Number		*99#
SIM 2 Auth Type		Auto ▼
SIM 2 Local IP Address		

Save ✓ Cancel ✕

Table 3-1 Cellular Instructions

Item	Description
Enable Modem	Enable/disable 4G modem.
Use PPP	Default dial-up is ECM. PPP is 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 via TCP protocol.
Operator Lock	Lock the router to a specific carrier by MCC/MNC code.
Band Lock	Lock the router to a specific band. i.e. Band 28.

Dual SIM Mode	<p><u>Fail Over</u>: When SIM 1 fails, the router will switch to SIM 2. When SIM 2 fails, the router will switch back to SIM 1.</p> <p><u>SIM1 Only</u>: Just SIM1 is available.</p> <p><u>SIM2 Only</u>: Just SIM2 is available.</p> <p><u>Backup</u>: 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 at the end of which it will switch back to SIM 1.</p>
Connect Mode	<p><u>Auto</u>: The router will connect automatically to 3G or 4G, with priority given to 4G.</p> <p><u>LTE</u>: Router will only connect to 4G.</p> <p><u>3G</u>: Router will only connect to 3G.</p>
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.
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 different.

【ICMP Check】

If you enable ICMP, the router will automatically check whether the defined IP address is reachable every 60s. If the IP address is unreachable and the ICMP check fails the first time, it will check twice again at a 3s 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.

The screenshot displays the router's web interface. On the left is a blue sidebar menu with options: Basic Network (selected), WAN, Cellular, LAN, VLAN, Schedule, DDNS, Routing, WLAN, Advanced Network, Firewall, VPN Tunnel, and Administration. The main content area is titled 'Cellular Settings'. It includes a toggle for 'Enable Modem' which is checked. Below this are tabs for 'Basic Settings', 'SIM 1', and 'SIM 2'. Under 'Basic Settings', there are several configuration fields: 'Use PPP' (unchecked), 'ICMP Check' (checked), 'Check IP' (8.8.8.8), 'Check IP (Optional)' (8.8.4.4), 'Interval' (60 seconds), 'Retries' (3 times), and '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 traffic received. If no traffic is received within the defined check interval time, the router will implement the “fail action” selected, cellular reconnect or reboot.

This screenshot shows the 'Cellular Traffic Check' configuration page. It features a toggle for 'Cellular Traffic Check' which is checked. Below it are three main settings: 'Check Mode' set to 'Rx', 'Check Interval' set to 10 minutes (with a range of 1 to 1440 minutes), and 'Fail Action' set to 'Cellular Reconnect'.

Step 2 To save your configuration, click on the “save” button.

3.4.3 LAN Settings

Please follow the instructions below:

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 ☐

Add +

DNS

Use Custom DNS ☐

Save ✓ **Cancel ✕**

Table 3-2 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.
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
Add	Add a LAN IP address. Supports four LAN IP addresses.

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

3.4.4 VLAN Settings

Go to Basic Network > VLAN

VLAN

VID	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
1	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	br0
2	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	WAN

0 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ none

Add +

Save ✓ Cancel ✗

Parameter	Instructions
VID	VLAN ID number. The VID ranges from 1 to 15.
LAN1~LAN4, WAN	LAN
Tagged	Enable to allow the router to encapsulate and de-encapsulate the VLAN tag.
Bridge	Router's interfaces br0, br1, br2, br3 and WAN

Click "Save" to finish.

3.4.5 Schedule

Go to Basic Network > Schedule.

Comset
www.comset.com.au

Already changed login password successfully.

Enabled Links

Link Name	Link Type	Description
modem	ECM/QMI	

ICMP Check

On	Link	Destination	Interval	Retries	Description
<input checked="" type="checkbox"/>					

Add +

Schedule

On	Link 1	Link 2	Policy	Description
<input checked="" type="checkbox"/>	modem	modem	FAILOVER	

Add +

Save ✓ Cancel ✕

Parameters	Instruction
modem	The router dials up to the network via the 4G 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
<input checked="" type="checkbox"/>	wan	8.8.8.8	10	5	

☒

Add +

Schedule

On	Link 1	Link 2	Policy	Description
<input checked="" type="checkbox"/>	wan	modem	FAILOVER	wan as primary and modem as secondary

Add +

The VLAN should be configured with WAN and 4G backup together. Please define WAN port as bridge WAN interface in the VLAN GUI as below.

Status

Basic Network

WAN

Cellular

LAN

VLAN

Schedule

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

Already changed login password successfully.

VLAN

0

☐
☐
☐
☐
☐
☐
☐
☐
☐
☐
☐

none

Add +

Save

Cancel

Click “Save” to finish.

3.4.6 Dynamic Settings

Please follow the instructions below:

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

Dynamic DNS	
IP Address	Use WAN IP Address 120.157.126.87 (recommended) ▼
Auto refresh every	28 minutes (0 = Disabled)

Dynamic DNS1	
Service	DynDNS - Dynamic ▼
URL	http://www.dyndns.com/
Username	techsupport
Password
Hostname	comsetdyn.dyndns.org
Wildcard	<input type="checkbox"/>
MX	
Backup MX	<input type="checkbox"/>
Save state when IP changes (nvram commit)	<input checked="" type="checkbox"/>
Force next update	<input type="checkbox"/>
Last IP Address	9/20/2019, 10:29:00 AM: 120.157.126.87
Last Result	9/20/2019, 10:29:00 AM: Update successful.

Table 3-3 DDNS Settings Instructions

Item	Description
IP address	The default is standard DDNS protocol.
Auto refresh time	Set the interval for the DDNS client to obtain a new IP. We suggest 240s or above
Service provider	Select the DDNS service provider from the list.

Step 2 Click “Save” to finish.

3.4.7 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
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="LAN"/>	<input type="text"/>

[Add +](#)

Miscellaneous

Mode:

RIPv1 & v2:

DHCP Routes: ☒

Spanning-Tree Protocol: ☐

[Save ✓](#) [Cancel ✕](#)

Table 3-4 Routing Settings Instructions

Item	Description
Destination	Destination IP address.
Gateway	Next hop IP address which the router will reach.
Subnet Mask	Subnet mask for destination IP address.
Metric	Metrics are used to determine whether one particular route should be chosen over another.
Interface	Interface from router to gateway.
Description	Describes the routing function.

Step 2 Click “Save” to finish.

3.5 WLAN Settings

3.5.1 Basic Settings

Please follow the instructions below:

Step 1 Select “WLAN>Basic Settings”

Already changed login password successfully.

Radio Mode: 2.4G + 5G

Wireless(2.4 GHz) | Wireless(5 GHz)

Enable WLAN: ☒

MAC Address: 34:0A:98:12:55:07

Wireless Mode: Access Point

Wireless Network Mode: Auto

SSID: Comset Router_125507

Broadcast SSID: ☒

Channel: 7 - 2.442 GHz Scan Q

Channel Width: 40 MHz

Control Sideband: Lower

Maximum Clients: 128 (range: 1 - 255)

Security option: WPA / WPA2 Personal

Encryption: TKIP / AES

Shared Key: Random

Group Key Renewal: 3600 (seconds)

Save ✓ Cancel X

More Info

Wireless(2.4 GHz)		Wireless(5 GHz)	
Enable WLAN	<input checked="" type="checkbox"/>		
MAC Address	34:0A:98:12:55:07		
Wireless Mode	Access Point		
Wireless Network Mode	Auto		
SSID	Comset Router_125507		
Broadcast SSID	<input checked="" type="checkbox"/>		
Channel	7 - 2.442 GHz		Scan
Channel Width	40 MHz		
Control Sideband	Lower		
Maximum Clients	128 (range: 1 ~ 255)		
Security option	WPA / WPA2 Personal		
Encryption	TKIP / AES		
Shared Key		Random
Group Key Renewal	3600		(seconds)

Wireless(2.4 GHz)
Wireless(5 GHz)

Enable WLAN ☒

MAC Address 34:0A:98:12:55:08

Wireless Mode Access Point

Wireless Network Mode Auto

SSID Comset Router_125507_5G

Broadcast SSID ☒

Channel Auto Scan

Channel Width 80 MHz

Control Sideband Upper

Maximum Clients 128 (range: 1 ~ 255)

Security option WPA / WPA2 Personal

Encryption TKIP / AES

Shared Key Random

Group Key Renewal 3600 (seconds)

Table 3-5 Basic Settings Instructions

Item	Description
Radio Mode	2.4G+5G default mode.
Enable wireless	Enable or Disable WiFi.
Wireless mode	Supports AP mode.
Wireless Network protocol	Supports Auto/b/g/n for 2.4G. Supports Auto/a/n for 5G.
SSID	The default is 'Comset Router 2.4GHz' or 'Comset Router 5GHz', but this can be changed.
Channel	The channel of wireless network. We suggest keeping the default.
Channel Width	20MHz and 40MHz for 2.4G. 20MHz, 40MHz and 80MHz for 5G.
Security	Supports various encryption methods.

Step 2 Click "Save" to finish.

3.5.2 Wireless Survey

Go to “WLAN> Wireless Survey” to check survey.

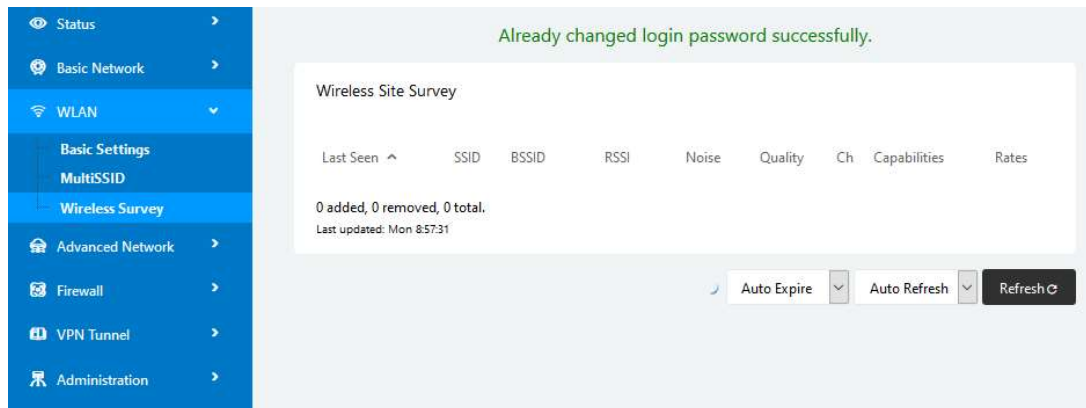


Figure 3-7 Wireless Survey Settings GUI

3.6 Advanced Network Settings

3.6.1 Port Forwarding

Please follow the instructions below:

Step 1 Go to “Advanced Network > Port Forwarding”

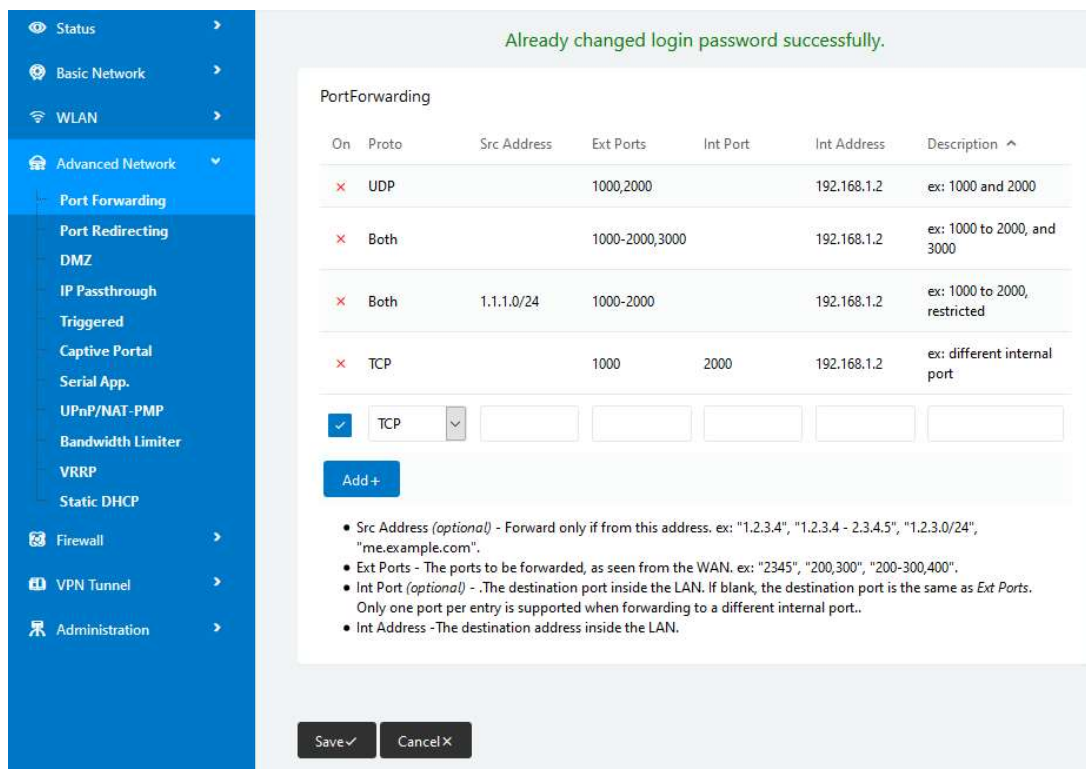


Figure 3-8 Port Forwarding GUI

Table 3-7 Port Forwarding Instructions

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

Step 2 Click “save” to finish.

3.6.2 Port Redirecting

Go to Advanced Network > Port Redirecting.

Already changed login password successfully.

PortRedirecting

On	Proto	Int Port	Dst Address	Ext Port	Description
<input checked="" type="checkbox"/>	TCP				

Add +

Save Cancel

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

Click “Save” to finish.

3.6.3 DMZ Settings

Please follow the instructions below:

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

Figure 3-9 DMZ GUI

Table 3-8 “DMZ” Instructions

Item	Description
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.

3.6.4 IP Pass-through Settings

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

Item	Description
Enable	Enable IP Pass-through
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned SIM IP.
Gateway	If the CM510Q-W is connected to multiple devices, input devices gateway.

Step 2 Click “save” to finish.

3.6.5 Triggered Port Forwarding Settings

Please follow the instructions below:

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

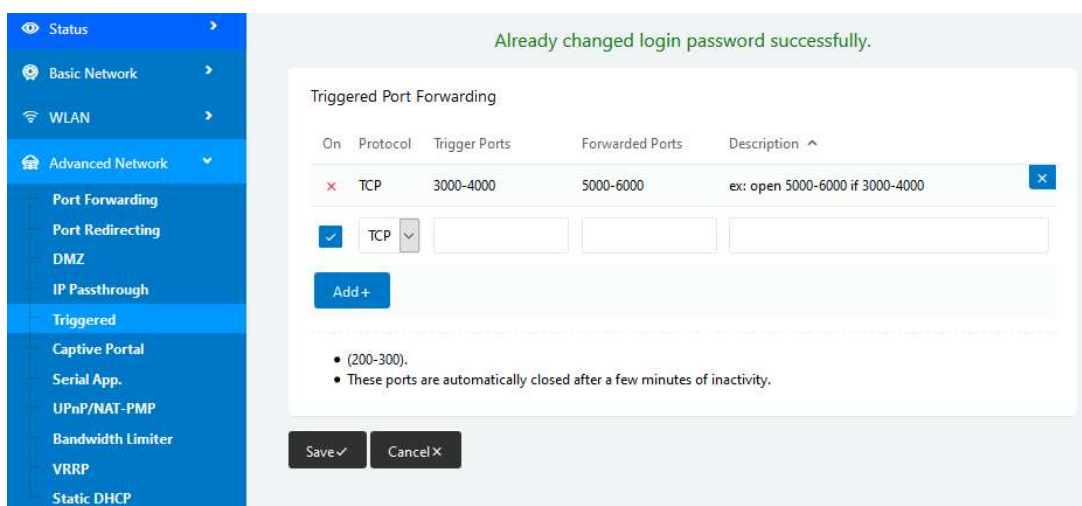


Figure 3-10 Triggered GUI

Table 3-9 “Triggered” Instructions

Item	Description
Protocol	Supports UDP, TCP or both UDP and TCP.
Triggered Ports	Triggered 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.

3.6.6 Captive Portal

Please follow the instructions below:

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 Minutes

Idle Timeout Minutes

Ignore LAN ☒

Redirecting http://

MAC Address Whitelist

Download QOS ☐

Upload QOS ☐

Save ✓ Cancel ✕

Item	Description
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 the router's Flash. Ex-storage: Captive portal file is in extended storage such as SD card.
Web Host	Configure domain name for the captive portal.
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 can be online if there is no network activity via WiFi. At the end of the idle time, the user needs to re-login.

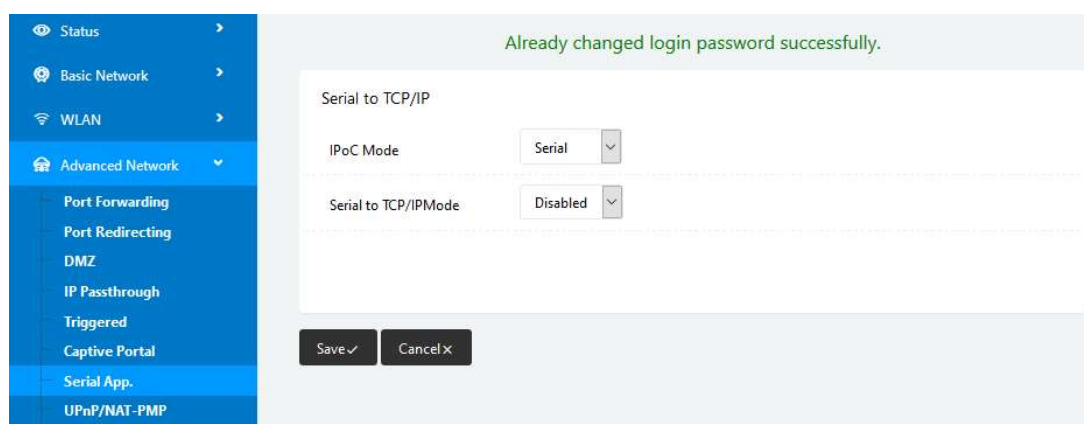
Item	Description
Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.
Redirecting	Router will redirect to the defined link after accepting the terms and conditions on the Captive Portal page.
MAC Whitelist	No captive portal page for Wi-Fi devices.
Download QoS	Enable to apply the Download Bandwidth limit per user.
Upload QoS	Enable to apply the Upload Bandwidth limit per user.

Click “save” to finish.

3.6.7 Serial App Settings

Please follow the instructions below:

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



Serial to TCP/IP

IPoC Mode:

Serial to TCP/IP Mode:

Server IP/Port:

Socket Type:

Socket Timeout: (milliseconds)

Serial Timeout: (milliseconds)

Packet Payload: (bytes)

Heart-Beat Content:

Heart-Beat Interval: (seconds)

Port Type:

Cache Enable: ☒

Debug Enable: ☐

Baud Rate:

Parity Bit:

Data Bit:

Stop Bit:

[More Info](#)

Parameter	Instruction
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.
Socket Timeout	Router will transmit data to the serial port at the end of the defined time.
Serial Timeout	Serial Timeout is the waiting time for transmitting the data package that is less the Packet payload.

Parameter	Instruction
	The default setting is 500ms.
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.
Heart-beat Content	Send heart-beat to the defined server to keep the router online. It 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		

Click “save” to finish.

3.6.8 UPnP/NAT-PMP Settings

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
<input type="button" value="Delete All x"/> <input type="button" value="Refresh"/>				

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 ☐

Click “Save” to finish.

3.6.9 Bandwidth Control Settings

Please follow the instructions below:

Go to “Advanced Network> Bandwidth Limiter” 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
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Norm <input type="button" value="v"/>
<input type="button" value="Add +"/>					

Default Class

Enable Default Class ☐

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.

Click “Save” to finish.

3.6.10 VRRP Settings

Go to “Advanced Network> VRRP” to check or modify the relevant parameters.

Already changed login password successfully.

VRRP

Enable VRRP ☐

Mode backup

Virtual IP

Virtual Router ID

Priority

Authentication ☐

Script Type Default

Check Interval

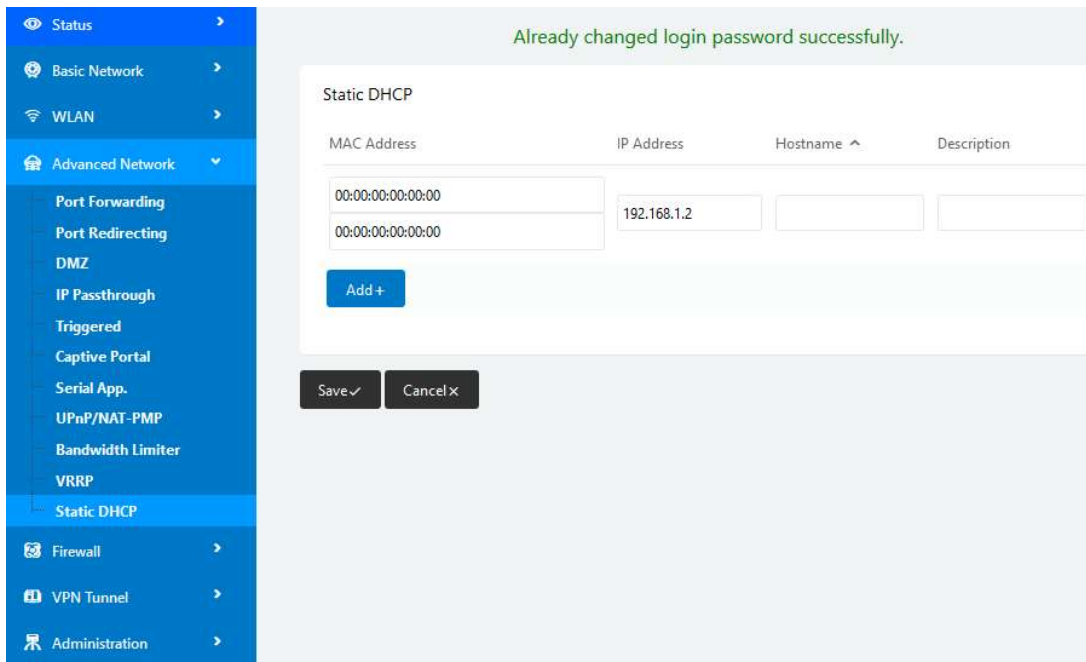
Weight

Save ✓ Cancel ✕

Click “Save” to finish.

3.6.11 Static DHCP Settings

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	192.168.1.2		
00:00:00:00:00:00			

Add +

Save ✓ Cancel x

Click “Save” to finish.

3.7 Firewall

3.7.1 IP/URL Filtering

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
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	NON	<input type="text"/>	<input type="text"/>	Acc	<input type="text"/>
Add +								

Key Word Filtering

On	Key Word	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
Add +		

URL Filtering

On	URL	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>
Add +		

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	NON	<input type="text"/>	<input type="text"/>	Acc	<input type="text"/>
Add +								

Save ✓ Cancel ✕

Item	Description
IP/MAC/Port Filtering	Supports IP address, MAC address and Port filtering. “Accept/Drop” options for filter policy.
Key Word Filtering	Supports key word filtering.
URL Filtering	Supports URL filtering.
Access Filtering	Supports Access filtering.

Click “Save” to finish.

3.7.2 Domain Filtering

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
<input checked="" type="checkbox"/>		

Add +

Save ✓ Cancel ✕

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

Click “Save” to finish.

3.8 VPN Tunnel

3.8.1 GRE Settings

Please follow the instructions below:

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

Already changed login password successfully.

GRE Tunnel

On	Idx	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
<input checked="" type="checkbox"/>					<input type="checkbox"/>			

Add +

GRE Route

On	Tunnel Index	Destination Address	Description
<input checked="" type="checkbox"/>	1		

Add +

Save ✓ Cancel ✕

Figure 3-15 GRE Settings GUI

Table 3-12 “GRE” Instructions

Item	Description
IDx	GRE Tunnel number.
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.
Tunnel Source	Router's 4G/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.

3.8.2 Open VPN Client Settings

Please follow the instructions below:

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

Already changed login password successfully.

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

Save ✓ Cancel ✕

Table 3-13 “OpenVPN Client” Instructions

Parameter	Instruction
Start with WAN	Enable the Openvpn feature for 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.

Parameter	Instruction
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.

Step 2 Click "save" to finish.

Client 1

Client 2

Basic

Advanced

Keys

Status

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

Start Now

Save ✓

Cancel ×

Item	Description
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

Client 1

Client 2

Basic

Advanced

Keys

Status

VPN Client #1 (Stopped)

For help generating keys, refer to the [OpenVPN HOWTO](#).

Certificate Authority

Client Certificate

Client Key

Start Now

Save ✓

Cancel ✕

Parameter	Instruction
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.

OpenVPN Client

Client 1 Client 2

Basic Advanced Keys Status

VPN Client #1 (Stopped)

Client is not running or status could not be read.

Start Now

Save ✓ Cancel ✕

Parameter	Instruction
Status	Check Openvpn status and data statistics.

Click "Save" to finish.

3.8.3 VPN PPTP Server Settings

Please follow the instructions below:

Step 1 Go to "VPN Tunnel> PPTP Server" to check or modify the relevant parameters.

Already changed login password successfully.

PPTP Server

Enable ☐

Local IP Address/Netmask: 192.168.1.1 / 255.255.255.0

Remote IP Address Range: 172.19.0.1 - 172.19.0.6 (6)

Broadcast Relay Mode: Disabled Enabling this may cause HIGH CPU usage

Encryption: MPPE-128

DNS Servers: 0.0.0.0

0.0.0.0

WINS Servers: 0.0.0.0

0.0.0.0

MTU: 1450

MRU: 1450

Poptop Custom configuration

Custom iptables if-up rules

Custom iptables if-down rules

Notes ^

PPTP User List

Username ^ Password

Add +

Save ✓ Cancel ×

» PPTP

Step 2 Click “save” to finish.

3.8.4 VPN PPTP/L2TP Client Settings

Please follow the instructions below:

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

The screenshot displays the configuration interface for PPTP/L2TP Client settings. The left sidebar shows the navigation menu with 'VPN Tunnel' expanded and 'PPTP/L2TP Client' selected. The main area contains four sections: 'L2TP/PPTP Basic', 'L2TP Advanced', 'PPTP Advanced', and 'Schedule'. Each section has a table of configuration parameters with checkboxes, dropdowns, and input fields.

On	Protocol	Name	Server	Username	Password	Firewall	Default Route	Local IP
<input checked="" type="checkbox"/>	L2TP					<input type="checkbox"/>	<input type="checkbox"/>	
Add +								

On	Name	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>		
Add +							

On	Name	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
<input checked="" type="checkbox"/>		NO			<input type="checkbox"/>	<input type="checkbox"/>	
Add +							

On	Name 1	Name 2	Policy	Description
<input checked="" type="checkbox"/>			FAILOVER	
Add +				

Table 2-1 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 2-2 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 2-3 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 2-4 SCHEDULE Instructions

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

Click "Save" to finish.

3.8.5 IPSec Settings

Already changed login password successfully.

IPSec

IPSec 1 IPSec 2 Schedule

Group Setup Basic Setup Advanced Setup

Enable IPSec ☐

IPSec Mode Client

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 ☒

Save ✓ Cancel ✕

3.8.5.1 IPSec Group Setup

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

IPSec

IPSec 1 IPSec 2 Schedule

Group Setup Basic Setup Advanced Setup

Enable IPSec ☐

IPSec Mode Client

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 ☒

Save ✓ Cancel ✕

Table 3-14 “IPSec Group Setup” Instructions

Item	Description
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.
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.

3.8.5.2 IPSec Basic Setup

Step 1 Select “IPSec >Basic Setup” to check or modify the relevant parameters.

IPSec

IPSec 1 IPSec 2 Schedule

Group Setup **Basic Setup** Advanced 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 MD5 HMAC (96-bit)

Phase 2 SA Life Time 3600 seconds

Preshared Key

Save ✓ Cancel ✕

Table 3-15 “IPSec Basic Setup” Instructions

Item	Description
Keying Mode	IKE pre-shared key.
Phase 1 DH Group	Select Group1, Group2, Group5 from the list. It must match the remote IPSec settings.
Phase 1 Encryption	Supports 3DES, AES-128, AES-192, AES-256.
Phase 1 Authentication	Supports HASH MD5 and SHA.
Phase 1 SA Life Time	IPSec Phase 1 SA lifetime.
Phase 2 DH Group	Select Group1, Group2, Group5 from the list. It 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 Life Time	IPSec Phase 2 SA lifetime.
Pre-shared Key	Pre-shared Key.

3.8.5.3 IPSec Advanced Setup

Select “IPSec >Advanced Setup” to check or modify the relevant parameters.

The screenshot shows the 'IPSec Advanced Setup' configuration interface. It includes tabs for 'IPSec 1', 'IPSec 2', and 'Schedule'. Under the 'IPSec 1' tab, there are sub-tabs for 'Group Setup', 'Basic Setup', and 'Advanced Setup'. The 'Advanced Setup' sub-tab is active, displaying a list of configuration options with checkboxes: 'Aggressive Mode', 'Compress(IP Payload Compression)', 'Dead Peer Detection(DPD)', and 'ICMP Check'. Below these are four text input fields for 'IPSec Custom Options 1' through 'IPSec Custom Options 4'. At the bottom of the form are 'Save' and 'Cancel' buttons.

Table 3-16 “IPSec Advanced Setup” Instructions

Item	Description
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.

3.9 Administration

3.9.1 Identification Settings

Please follow the instructions below:

Step 1 Select “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

Save ✓ Cancel ✕

Figure 3-16 Router Identification GUI

Table 3-17 “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.

3.9.2 Time Settings

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

Already changed login password successfully.

Time

Router Time Tue, 24 Sep 2019 08:29:26 +1000 Clock Sync.

Time Zone UTC+10:00 Australia

Auto Daylight Savings Time ☒

Auto Update Time Every 1 Hour

Trigger Connect On Demand ☐

NTP Time Server Default

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

Save ✓ Cancel ✕

Figure 3-17 Time Settings GUI



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

Step 2 Click “Save” to finish.

3.9.3 Admin Access Settings

Please follow the instructions below:

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)

Save ✓ Cancel ✕

Figure 3-18 Admin Access Settings GUI

Step 2 Click “Save” to finish.

3.9.4 Scheduled Reboot Settings

Please follow the instructions below:

Step 1 Select “Administration>Scheduled Reboot” to check and modify relevant parameters.

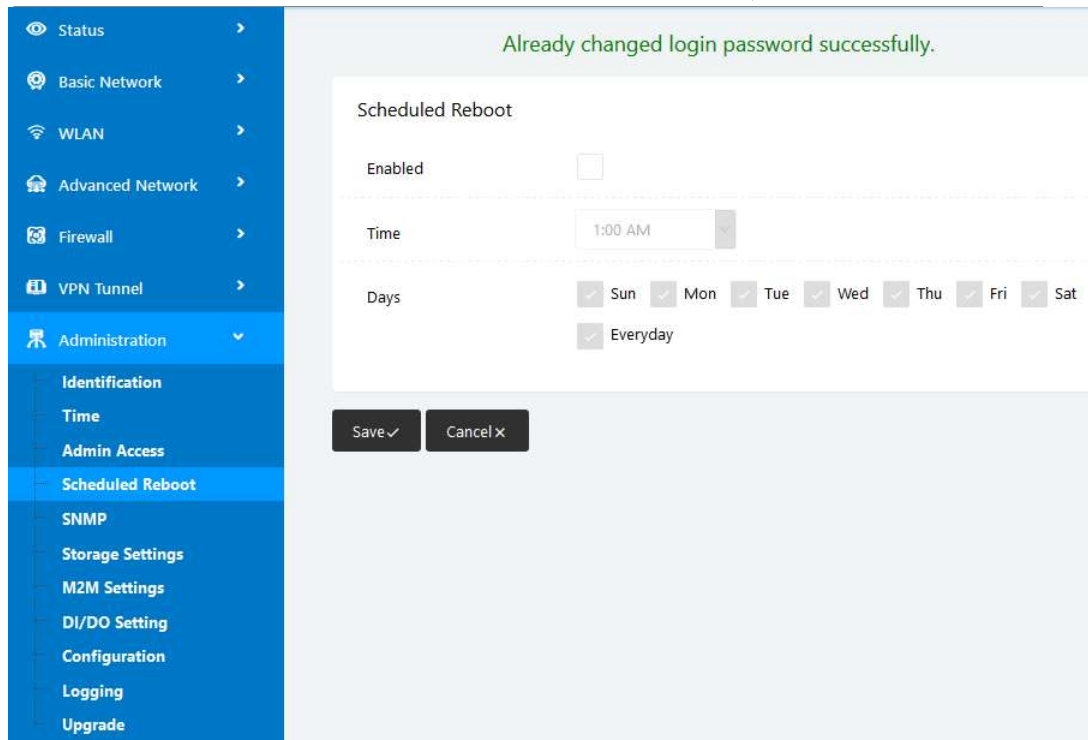


Figure 3-19 Scheduled Reboot Settings GUI

Step 2 Click “Save” to finish.

3.9.5 SNMP Settings

Please follow the instructions below:

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

SNMP Settings

Enable SNMP ☐

Port

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

Contact

RO Community

Custom OID :

1.3.6.1.4.1.2021.505	<input type="text" value="eg:/bin/nvram get snmp_enable"/>
1.3.6.1.4.1.2021.506	<input type="text"/>
1.3.6.1.4.1.2021.507	<input type="text"/>
1.3.6.1.4.1.2021.508	<input type="text"/>
1.3.6.1.4.1.2021.509	<input type="text"/>

Save ✓ Cancel ✕

Figure 3-20 SNMP Settings GUI

Step 2 Click “Save” to finish.

3.9.6 Storage Settings

Step 1 Select “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 Choose File Upload

Current file list

File name	File size	File operation
<div>Save ✓</div> <div>Cancel ✕</div>		

Step 2 Click “Save” to finish.

3.9.7 M2M Access Settings

Step 1 Select “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

Save ✓ Cancel ✕

Figure 3-21 M2M Access Settings
GUI

Step 2 Click “Save” to finish.

3.9.8 DI/DO Settings

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

Already changed login password successfully.

DI Setting

Enabled ☐ Port1 ☐ Port2 ☐

DO Setting

Enabled ☒

Alarm Source ☐ DI Control ☐ SMS Control ☐

Alarm Action

Power On Status

Keep On (*100ms)

Figure 3-22 DI/DO Settings GUI

3.9.8.1 DI Configuration

Already changed login password successfully.

DI Setting

Enabled ☒ Port1 ☒ Port2 ☐

Port1Mode

Filter (*100ms)

SMS Alarm ☐

DO Setting

Enabled ☒

Alarm Source DI Control ☐ SMS Control ☐

Alarm Action

Power On Status

Keep On (*100ms)

Save ✓ Cancel ✕

Table 3-18 "DI" Instructions

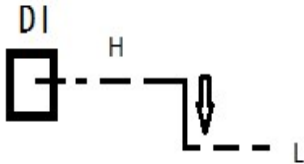
Item	Description
Enable	Enable DI. Port1 is for I/O-1 and Port2 is for I/O-2. Both I/O-1 and I/O-2 are DI ports.
Mode	<p>Selected from OFF, ON and EVENT_COUNTER modes.</p> <p>OFF Mode: When DI changes from High (3.3V) to Low (0V), the alarm is triggered.</p> <p>ON Mode: When DI changes from Low (0V) to High (3.3V), the alarm is triggered.</p> <p>EVENT_COUNTER Mode: Enter EVENT_COUNTER mode.</p>
Filter	<p>Software filtering is used to control switch bounces. Input (1~100)*100ms.</p> <p>Under ON and OFF modes, the CM510 detects the pulse signals and compares with the first pulse shape and the last pulse shape. If both are at the same level, the CM510 will trigger an alarm.</p> <p>Under EVENT_COUNTER mode, if the first pulse shape and the last pulse shape are not at the same level, the CM510 will trigger an alarm according to the Counter Action settings.</p>
Counter Trigger	<p>Available when the DI is under Event Counter mode.</p> <p>Input from 0 to 100. "0" means the alarm is not triggered.</p> <p>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.</p>
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	<p>HI_TO_LO and LO_TO_HI is available when the DI is under Event Counter mode.</p> <p>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, the counter value increases when the switch is pushed and released.</p>
Counter Start	Available when the DI is under EVENT_COUNTER mode. The counting starts when you enable this feature.
SMS Alarm	<p>The alarm SMS will send a text to a specified phone group.</p> <p>Each phone group contains up to 2 phone numbers.</p>
SMS Content	70 ASCII Char Max.
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Click "Save" to finish.



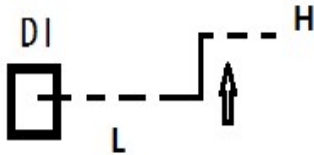
OFF Mode

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



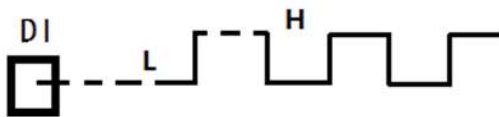
ON Mode

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.



3.9.8.2 DO Configuration

DO Setting

Enabled ☒

Alarm Source ☒ DI Control ☒ SMS Control

Alarm Action

Power On Status

Delay (*100ms)

Low (*100ms)

High (*100ms)

Output

SMS Trigger Content

SMS Reply Content

SMS admin Num1

SMS admin Num2 Backup

[More Info](#)

Table 3-19 “DO” Instructions

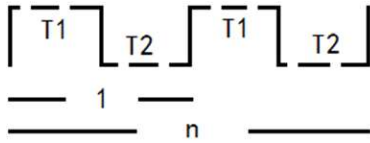
Item	Description
Enable	DO is enabled.
Alarm Source	<p>Digital Output activates according to different alarm sources. You can select between DI Alarm and SMS Control. You can select one or both alarm sources.</p> <p>DI Alarm: The Digital Output gets triggered when there is an alarm from a Digital Input.</p> <p>SMS Control: The Digital Output gets triggered when receiving an SMS from a number in the phone book.</p>

Alarm Action	<p>The Digital Output initiates an alarm action.</p> <p>Select from “OFF”, “ON” and “Pulse”.</p> <p>OFF: Open from GND when triggered.</p> <p>ON: Short contact with GND when triggered.</p> <p>Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.</p>
Power on Status	<p>Specify the Digital Output status when the power is on.</p> <p>Select from “OFF” and “ON”.</p> <p>OFF: Open from GND.</p> <p>ON: Short contact with GND.</p>
Keep On	<p>Available when the DO “Alarm On Action”/ “Alarm Off Action” status is ON. Input the DO “Keep On” status time.</p> <p>Input from 0 to 255 seconds. “0” means ON until the next action.</p>
Delay	<p>Available when you enable “Pulse” in “Alarm On Action”/ “Alarm Off Action”. The first pulse will be generated after a “Delay” .</p> <p>Input from 0 to 30000ms. (0=generate pulse without delay)</p>
Low	<p>Available if Pulse is enabled in “Alarm On Action”/ “Alarm Off Action”.</p> <p>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.</p> <p>Input from 1 to 30000 ms.</p>
High	<p>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.</p> <p>Input from 1 to 30000 ms.</p>
Output	<p>Available if Pulse is enabled in “Alarm On Action”/ “Alarm Off Action”.</p> <p>The number of pulses, input from 0 to 30000. (0 for continuous pulse output)</p>
SMS Trigger Content	<p>Available when you enable SMS Control in Alarm Source.</p> <p>Input the SMS content to enable “Alarm On Action” by SMS (70 ASCII II char max).</p>
SMS Reply Content	<p>Input the SMS content, which will be sent after DO is triggered. (70 ASCII II char max).</p>
Number 1	SMS receiver phone number.
Number 2	SMS receiver phone number.

Step 3 Click “save” to finish.



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



3.9.9 Configuration Settings

Step 1 Select “Administration> Configuration” to configure the backup settings.

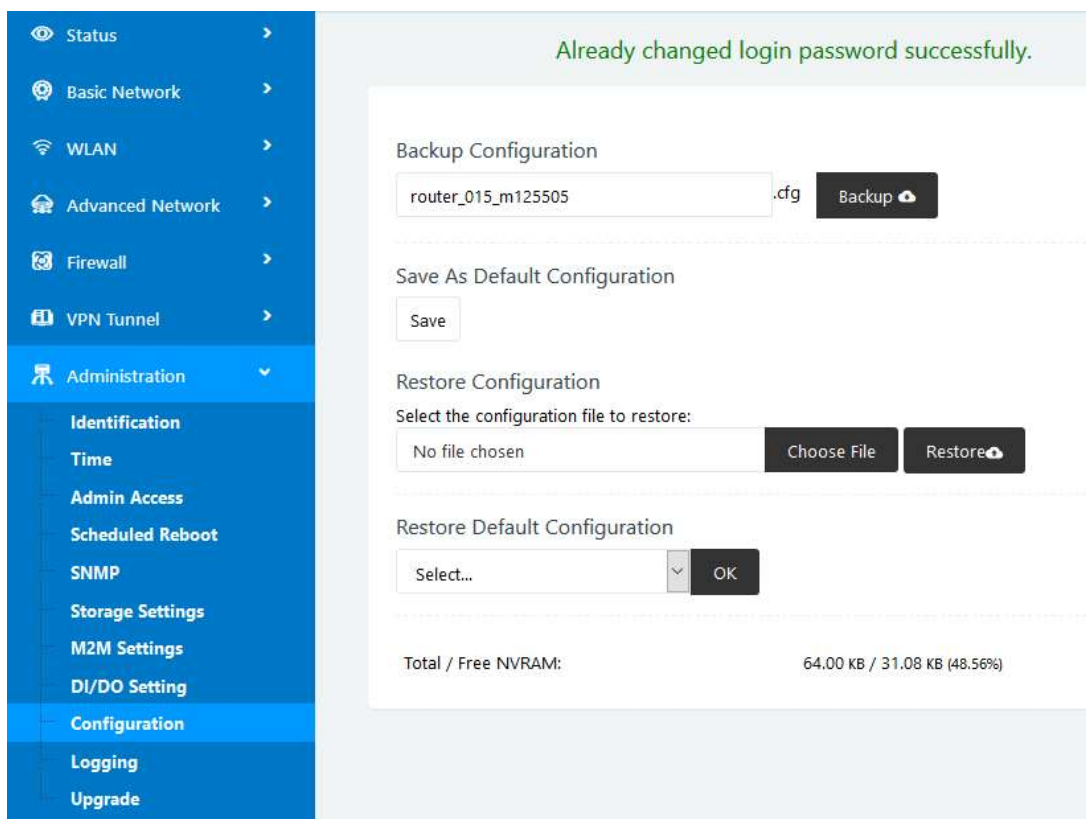


Figure 3-23 Backup and Restore Configuration GUI



“Restore Default” will delete all configuration settings.

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

3.9.10 System Log Settings

Step 1 Select “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 :

Generate Marker

Limit (messages per minute / 0 for unlimited)

Save ✓ Cancel ✕

Figure 3-24 System log Settings GUI

Step 2 Click “Save” to finish.

3.9.11 Firmware Upgrade

Step 1 Select “Administration>Upgrade” to open the upgrade firmware tab.

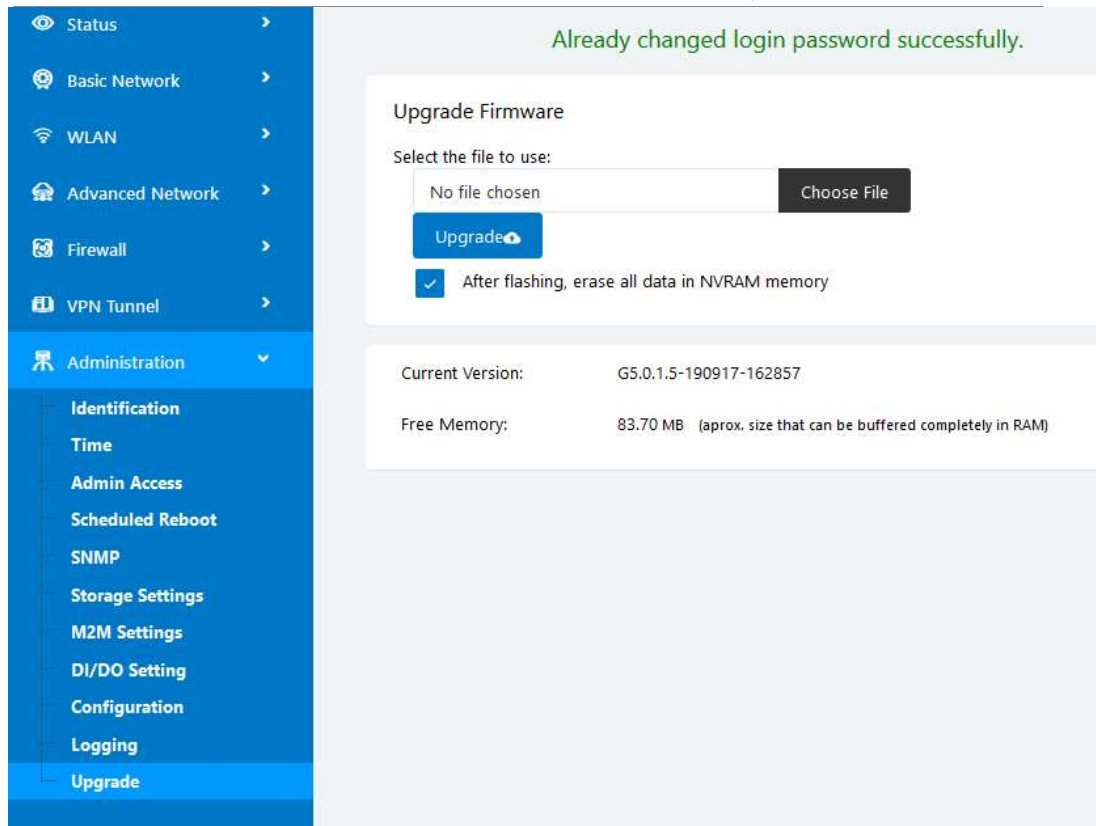


Figure 3-25 Firmware Upgrade GUI

**NOTE**

Please do not disconnect the power when upgrading.

3.10 Reset Button to Restore Factory Settings

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

Table 3-20 System Default Instructions

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

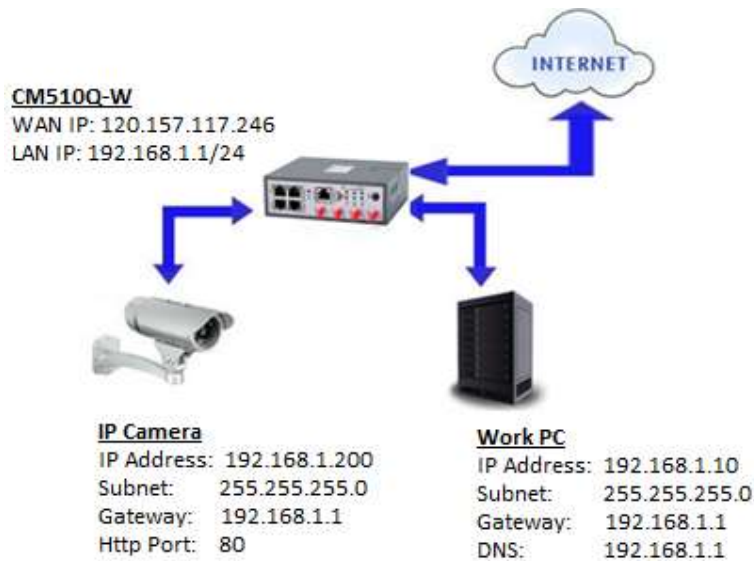
**NOTE**

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

4 Configuration Examples

4.1 Port Forwarding

Network Topology:



A 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 CM510Q-W 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 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

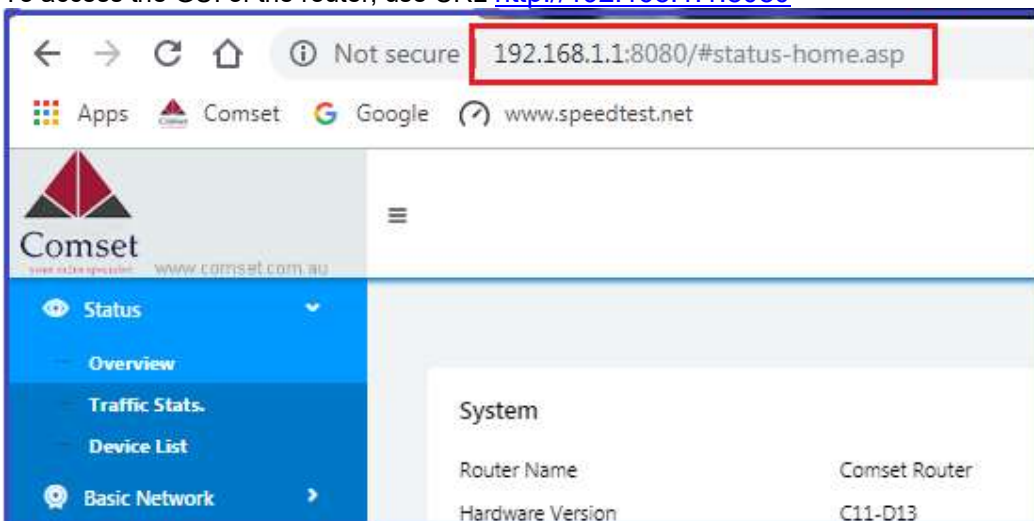
Change router GUI to port 8080 to avoid conflict with IP camera Http port(80).

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.



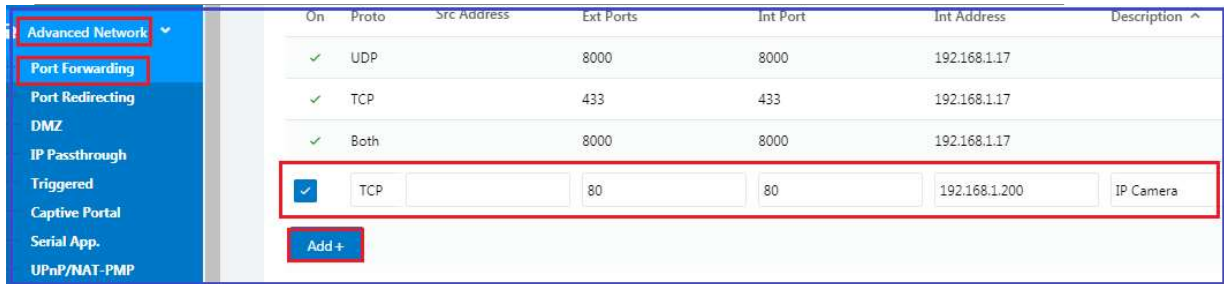
To access the GUI of the router, use URL <http://192.168.1.1:8080>



Configure Port Forwarding for the IP Camera on Port 80.

Go to Advanced Network -> Port Forwarding

Set Proto: TCP, External Ports:80, Internal Ports:80, Internal Address: 192.168.1.200, Description: IP camera, click on the "Add" button.



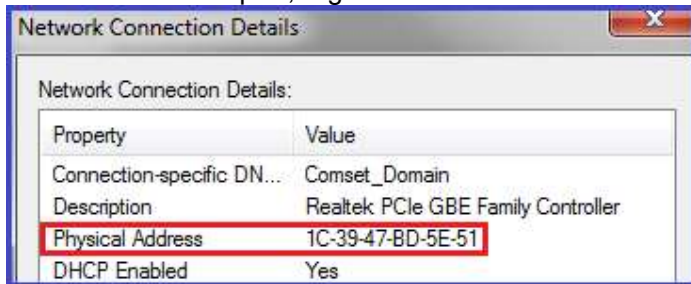
To access the Web GUI of the camera, use URL <http://120.157.117.246> or <http://120.157.117.246:80>

4.2 IP Pass-through

Note: This guide is for IP Pass-through to a PC behind the CM510Q-W. It is also applicable to a Router behind the CM510Q-W. You need to use the MAC Address on the WAN interface of the Router.

1. Check the LAN Mac Address on your PC.

Go to Network Adapter, Right click -> Status -> Details. See screenshot below:

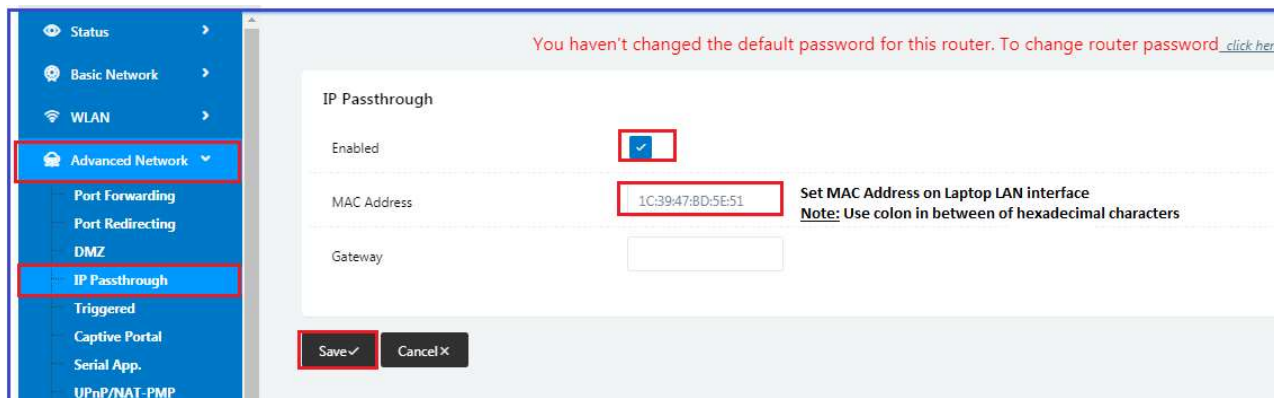


2. Configure IP Pass-through on the Router.

Go to Advanced Network -> IP Pass-through -> check the 'Enabled' box option.

Enter the MAC Address as obtained from your PC LAN interface and click 'Save'.

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

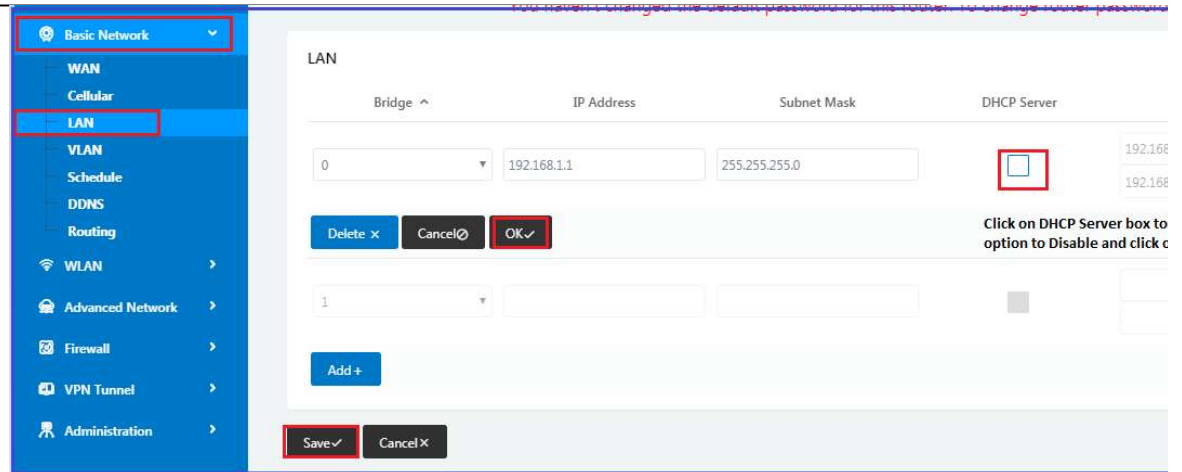


3. Disable DHCP server on the router.

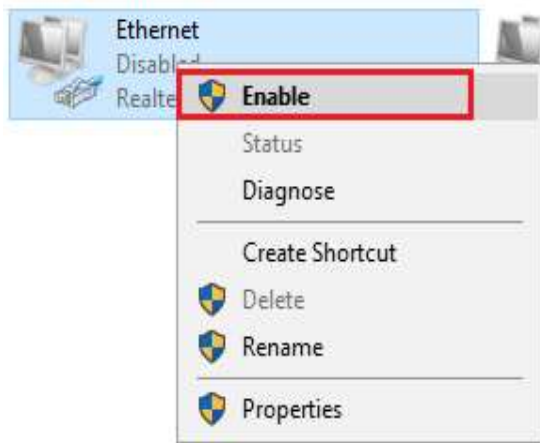
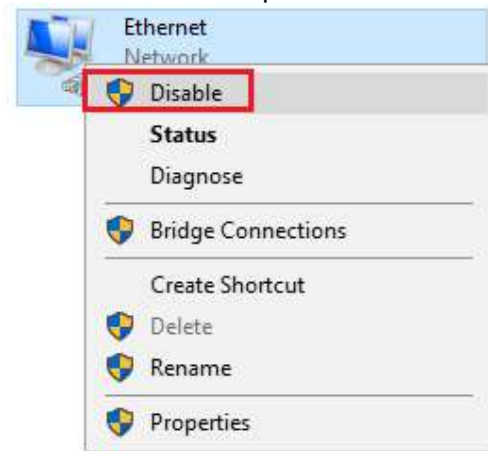
Go to Basic Network -> LAN -> Click on DHCP server to edit and uncheck option to Disable.

Click on the 'OK' and 'Save' buttons.

Note: The router will reboot.



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 and select Enable. See screenshots below:



5. 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 Pass-

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 10:55:1
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

through.

6. 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>
```

4.3 Captive Portal

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

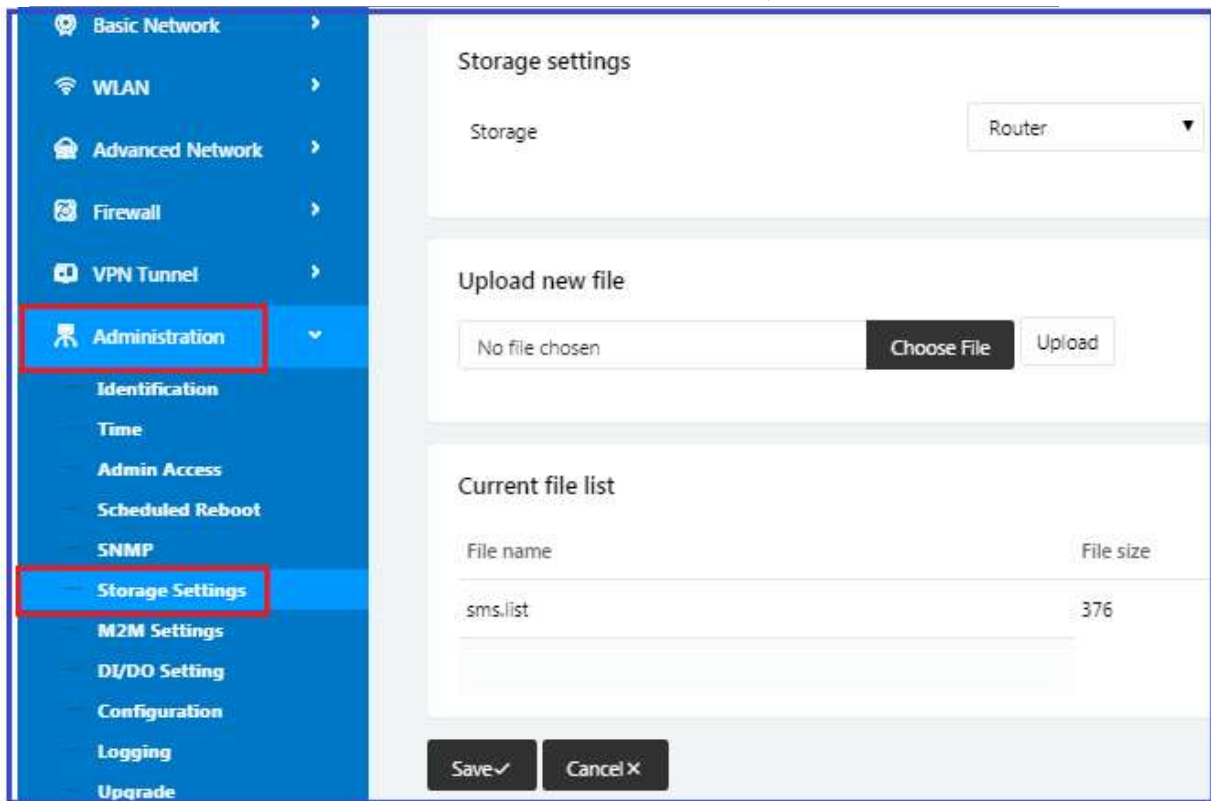
The screenshot shows the 'Captive Portal' configuration page. On the left, a blue sidebar contains a menu with 'Advanced Network' and 'Captive Portal' highlighted with red boxes. The main area is titled 'Captive Portal' and contains the following settings:

Parameter	Value
Enabled	<input checked="" type="checkbox"/>
Auth Type	NONE
WEB Root	Default
WEB Host	
Portal Host	
Login Timeout	0 Minutes
Idle Timeout	0 Minutes
Ignore LAN	<input checked="" type="checkbox"/>
Redirecting http://	www.google.com
MAC Address Whitelist	
Download QOS	<input type="checkbox"/>
Upload QOS	<input type="checkbox"/>

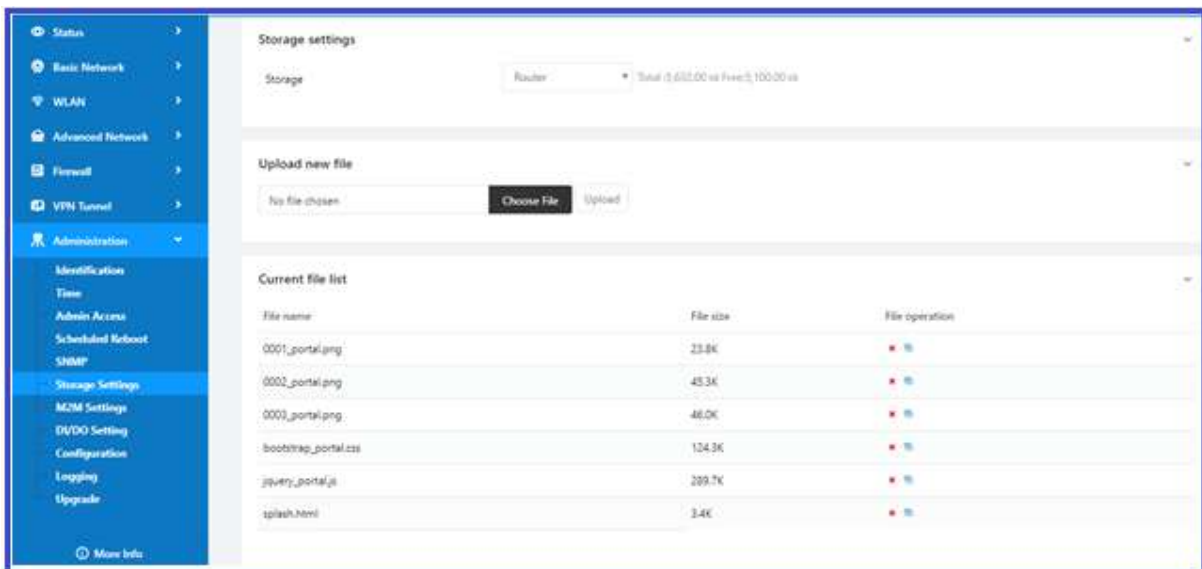
At the bottom of the main area are 'Save ✓' and 'Cancel ✕' buttons.

2. Upload Portal file and Splash.html

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.



Each Ad file supports 3 Ad portal images. Picture format is png or jpg, image size is less than 100Kbytes and resolution is 800*600. 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.




```

<!-- <hr> -->

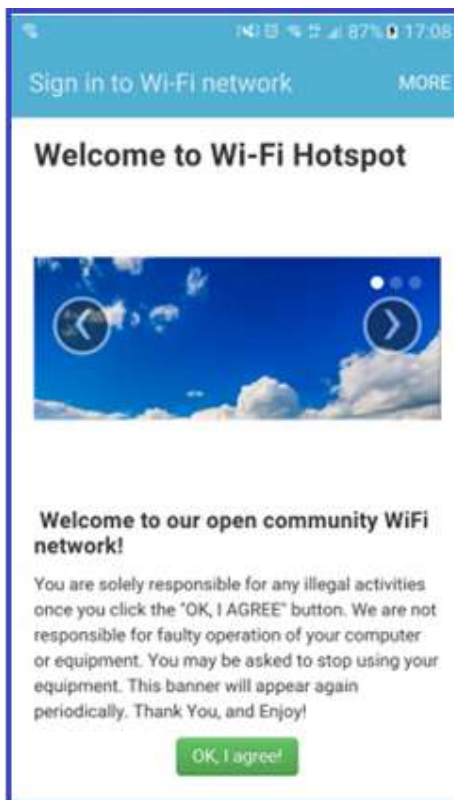
<div id="myCarousel" class="carousel slide marketing">
  <ol class="carousel-indicators">
    <li data-target="#myCarousel" data-slide-to="0" class="active"></li>
    <li data-target="#myCarousel" data-slide-to="1"></li>
    <li data-target="#myCarousel" data-slide-to="2"></li>
  </ol>

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

<!-- <hr> -->

```

Now you can see the results by connecting to the router's WIFI.



3. 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 Minutes

Idle Timeout Minutes

Ignore LAN ☒

Redirecting http://

MAC Address Whitelist

Download QOS ☐

Save ✓ **Cancel ✕**

4.4 GPS Settings (GPS version only)

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

GPS

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

GPS Mode Client ▾

Data Format M2M_FMT ▾

Server IP/Port

Heart-Beat Content

Heart-Beat Interval seconds

Save ✓ **Cancel ✕**

Item	Instructions
GPS Mode	Enable/Disable.
GPS Format	NMEA and M2M_FMT.

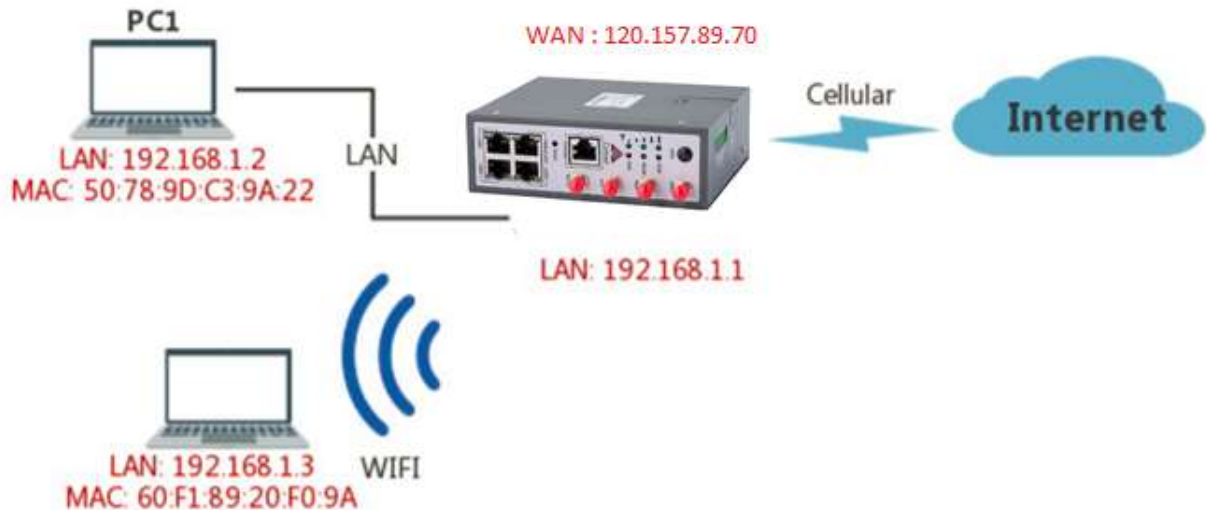
Item	Instructions
Server IP/Port	GPS server IP and port.
Heart-Beat	If you choose M2M_FMT format, the heart-beat ID will be packed into the GPS data.
Interval	GPS data transmits at the interval time.

2. Click on “Save” to Finish.
3. Connect the GPS antenna to the router GPS interface.
4. Check GPS Status.



4.5 Firewall

Network Topology



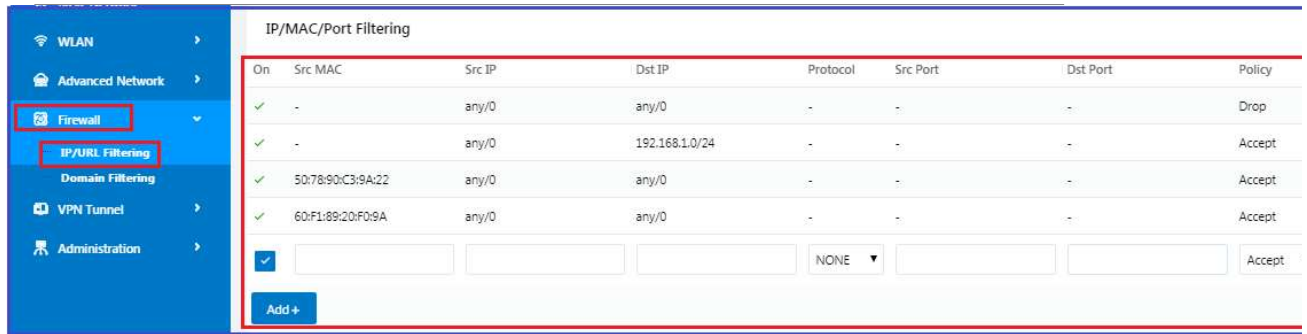
4.5.1 IP/MAC/Port Filtering

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

Test case:

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

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

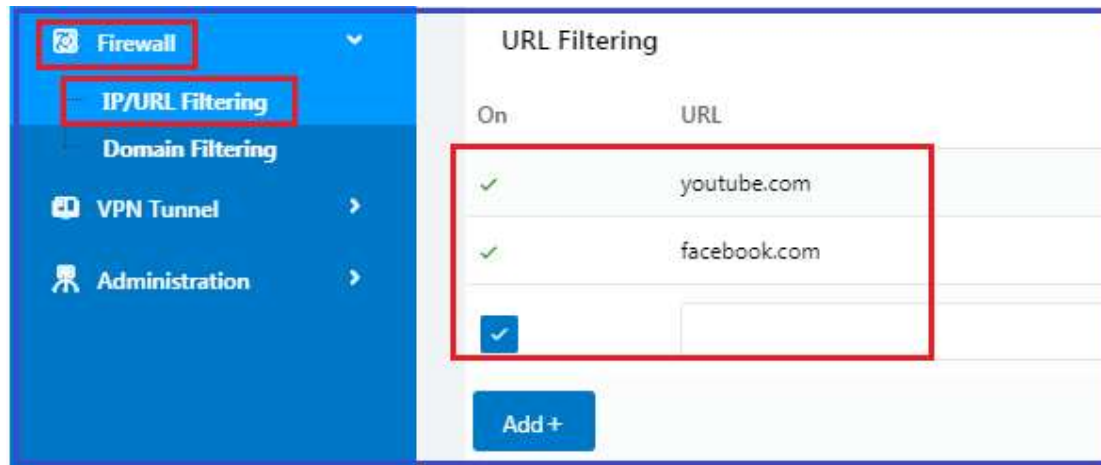


4.5.2 Keyword Filtering

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

4.5.3 URL Filtering

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



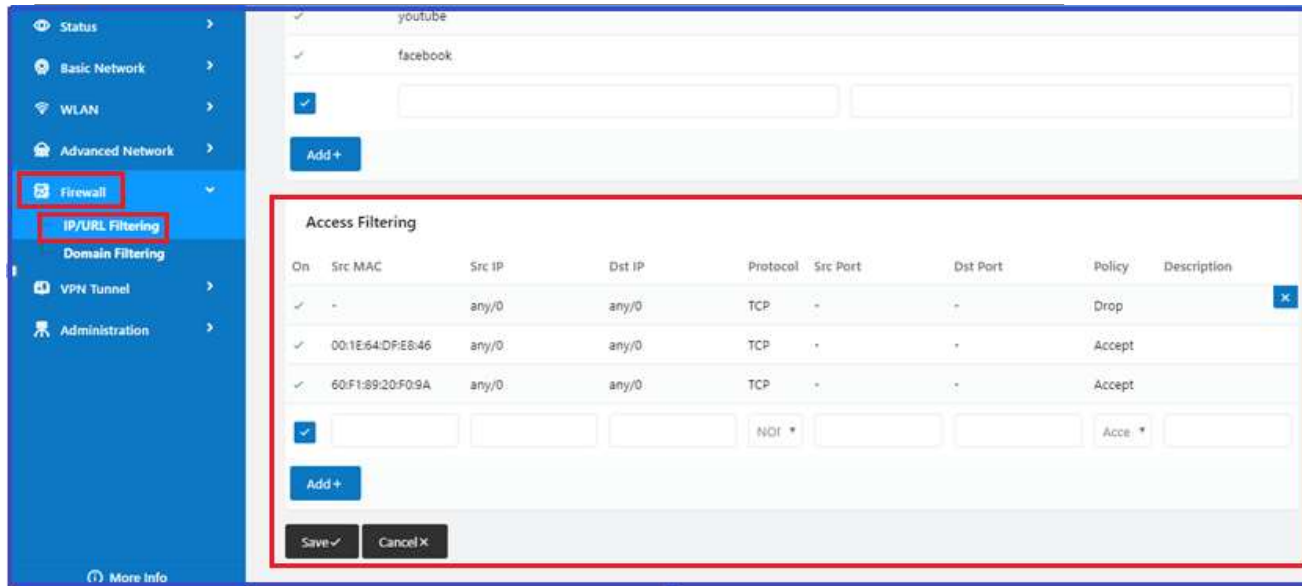
4.5.4 Access Filtering

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

Test case:

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

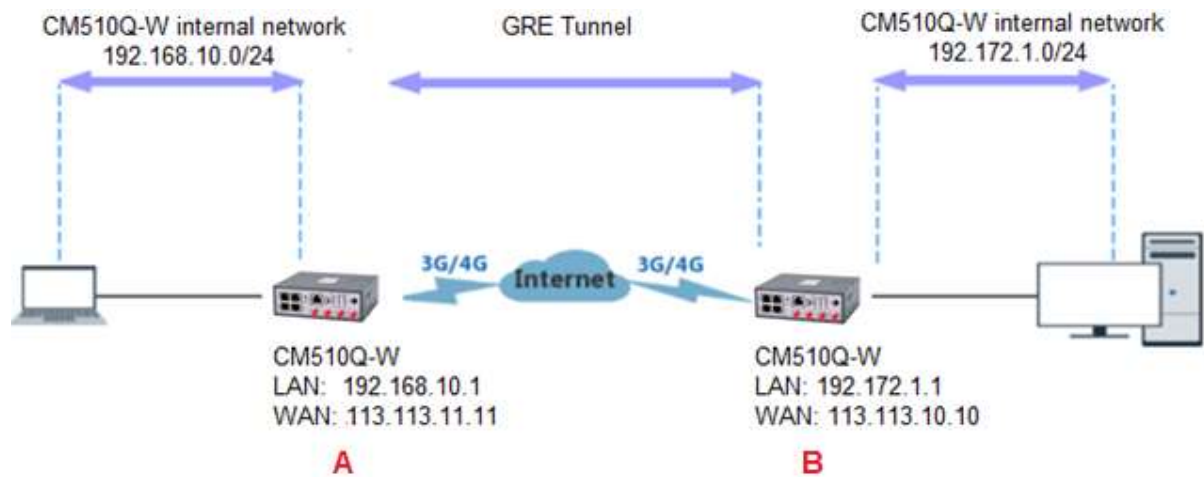
Only two devices (MAC/LAN/WLAN) can be accessed from Internet packets.



4.6 VPN Tunnel

4.6.1 GRE Tunnel between two CM510Q-W

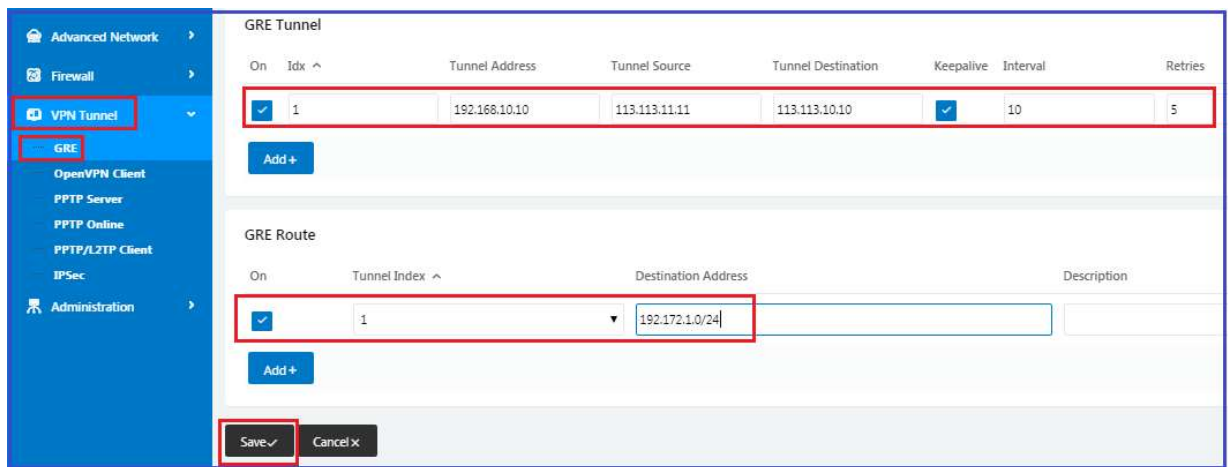
Network Topology



- 1) CM510Q-W (A) Configuration
 - 1.1) Navigate to Basic Network > LAN



1.2) Navigate to VPN Tunnel > GRE



2) CM510Q-W(B) Configuration

2.1) Navigate to Basic Network > LAN



2.2) Navigate to VPN Tunnel > GRE

VPN Tunnel

GRE Tunnel

On	Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries
<input checked="" type="checkbox"/>	1	192.172.1.10	113.113.10.10	113.113.11.11	<input checked="" type="checkbox"/>	10	5

Add+

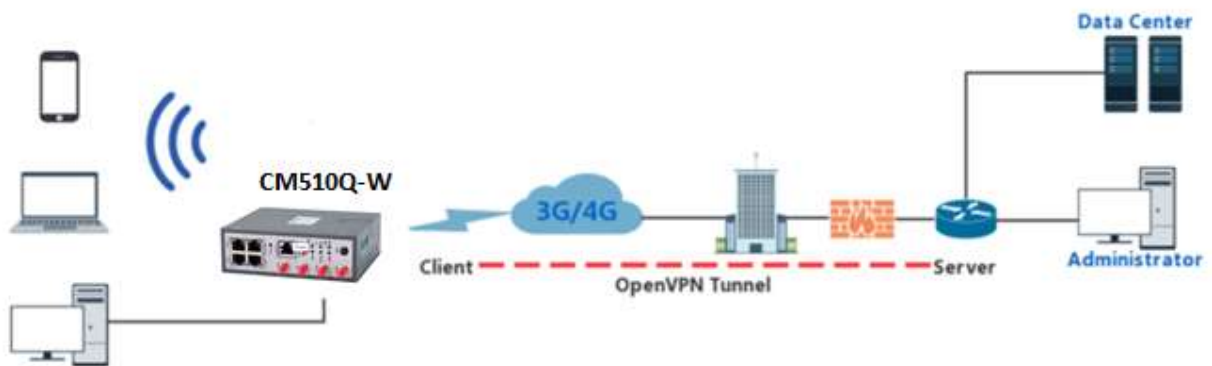
GRE Route

On	Tunnel Index ^	Destination Address	Description
<input checked="" type="checkbox"/>	1	192.168.10.0/24	

Add+

4.6.2 Open VPN

Network Topology



OpenVPN between CM510Q-W Client and Server

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

Basic Settings:

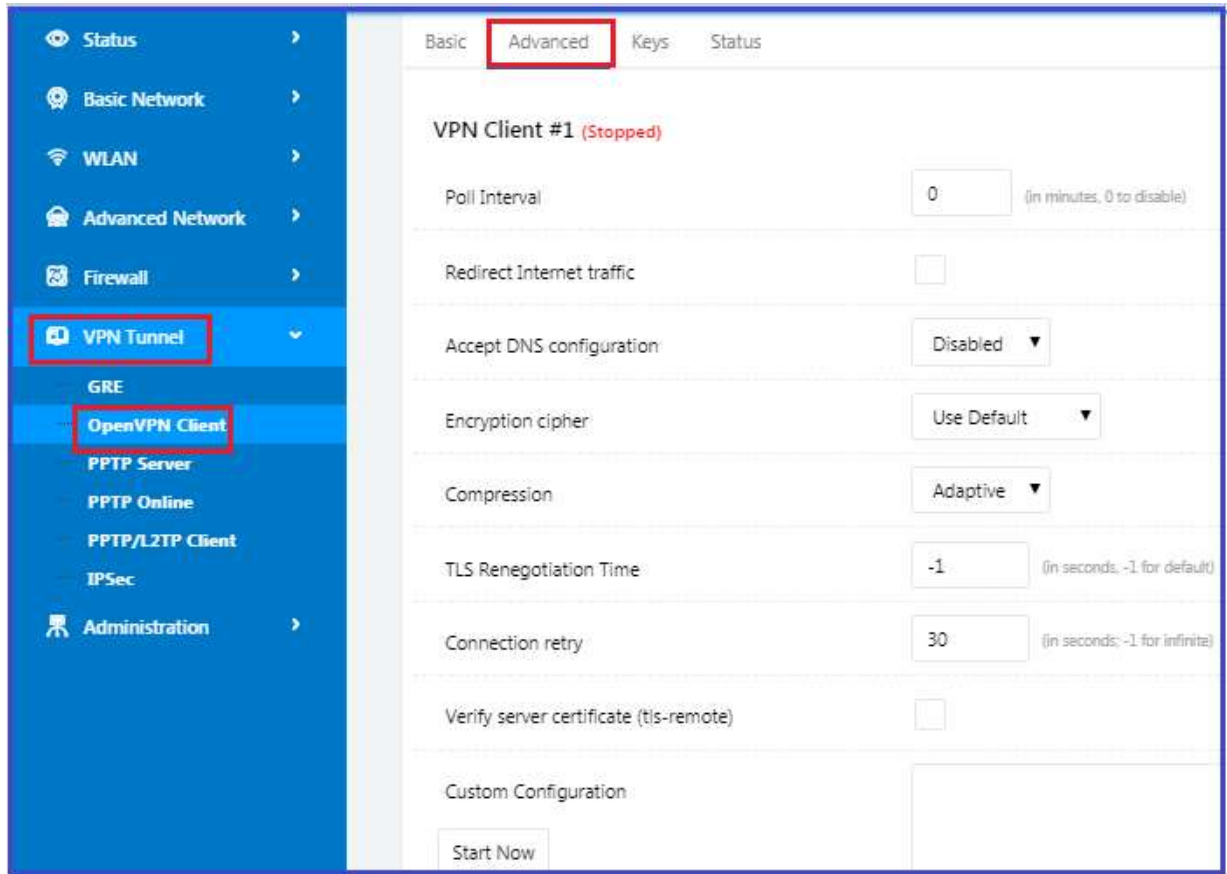
The screenshot displays the 'VPN Client #1 (Stopped)' configuration page. The left sidebar contains a menu with 'VPN Tunnel' and 'OpenVPN Client' highlighted. The main panel has tabs for 'Basic', 'Advanced', 'Keys', and 'Status'. The 'Basic' tab is active, showing the following settings:

- Start with WAN:** ☒
- Interface Type:** TUN
- Protocol:** UDP
- Server Address:** comset.dyndns.org 1194
- Firewall:** Automatic
- Authorization Mode:** TLS
- Username/Password Authentication:** ☐
- HMAC authorization:** Disabled
- Create NAT on tunnel:** ☒

A 'Start Now' button is located at the bottom left of the configuration area.

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

Advanced Configuration:



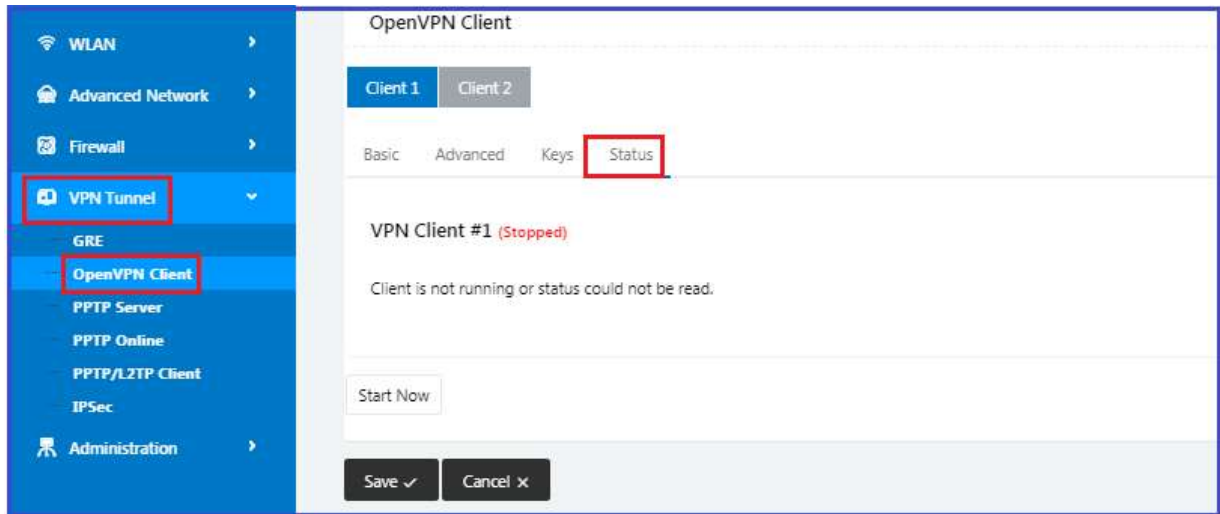
Parameter	Instruction
Poll Interval	Openvpn client checks router's status at interval time.
Redirect Internet Traffic	Configure Openvpn as default routing.
Access DNS	As per user's configuration.
Encryption	As per user's configuration.
Compression	As per user's configuration.
TLS Renegotiation Time	TLS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

Keys Configuration

The screenshot displays the 'OpenVPN Client' configuration page. The left sidebar contains a navigation menu with the following items: Status, Basic Network, WLAN, Advanced Network, Firewall, VPN Tunnel (highlighted), GRE, OpenVPN Client (highlighted), PPTP Server, PPTP Online, PPTP/L2TP Client, IPSec, and Administration. The main content area is titled 'OpenVPN Client' and has tabs for 'Client 1', 'Client 2', 'Basic', 'Advanced', 'Keys' (selected), and 'Status'. Below the tabs, it shows 'VPN Client #1 (Stopped)' and a note: 'For help generating keys, refer to the OpenVPN HOWTO.' There are three input fields: 'Certificate Authority', 'Client Certificate', and 'Client Key'. A 'Start Now' button is located at the bottom left of the main area.

Parameter	Instruction
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.

Status



Parameter	Instruction
Status	Check OpenVPN status and data statistics.

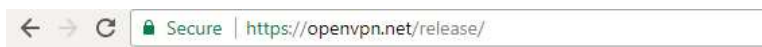
Click “save” and “start now” to start OpenVPN.



OpenVPN Keys Guide

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

You may access to (<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)



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

1. Configure "vas.bat.sample" to complete the initialization step and keys.

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

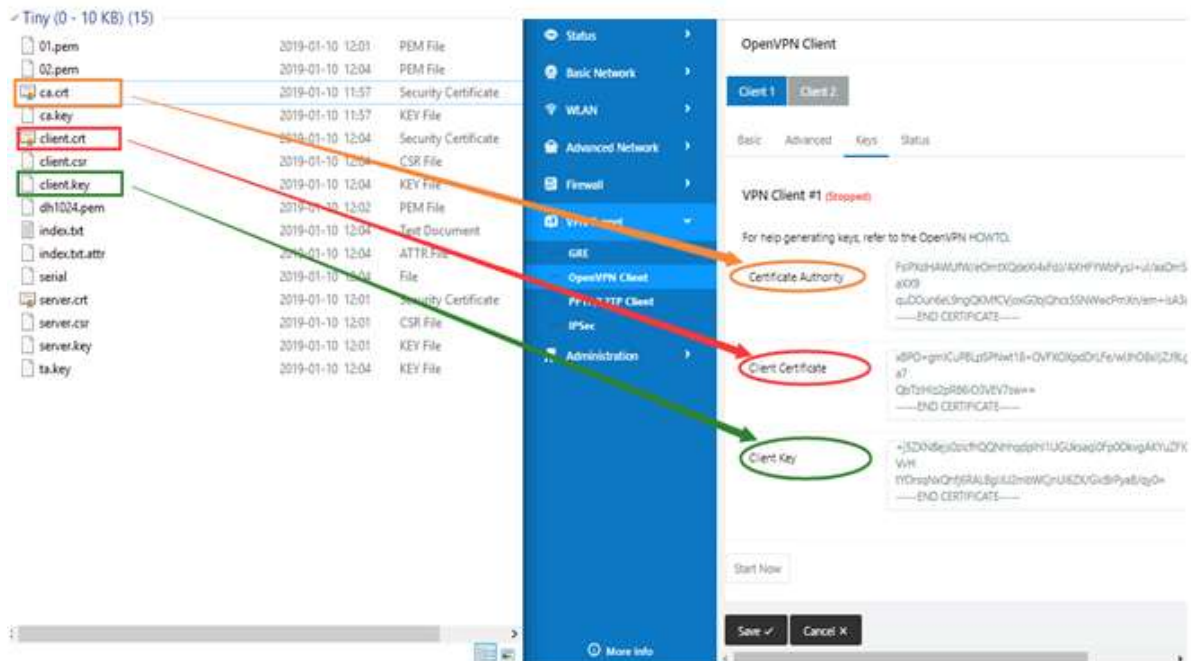
Name	Date modified	Type	Size
keys	2019-01-10 12:04	File folder	
.rnd	2019-01-10 12:04	RND File	1 KB
build-ca.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-dh.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key.bat	2016-01-04 20:41	Windows Batch File	1 KB
build-key-pass.bat	2016-01-04 20:41	Windows 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

2. You can configure the client keys for the CM510Q-W OpenVPN client GUI when you create the server and client certificate in the path OpenVPN/easy-rsa/keys.

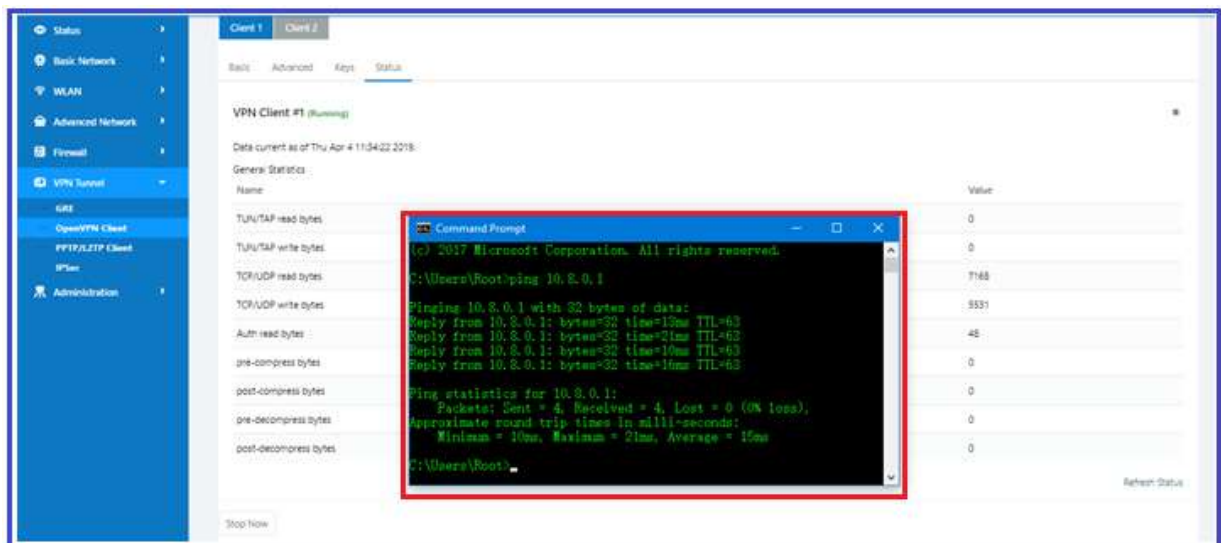
3. Client certificate (Generated on the server)

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

4. OpenVPN>easy-rsa>keys



5. You can now ping test your server when the tunnel is established:



4.6.3 L2TP/PPTP

Go to "VPN Tunnel > PPTP/L2TP Client" to view or modify the relevant parameters.

Test case: PPTP

VPN Tunnel ▼

- GRE
- OpenVPN Client
- PPTP Server
- PPTP Online
- PPTP/L2TP Client**

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

Add +

PPTP Advanced

On	Name ^	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
✓	3	NO	1440	1440	✓	✗	debug;noipdefault;requ 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							

Add +

PPTP Advanced

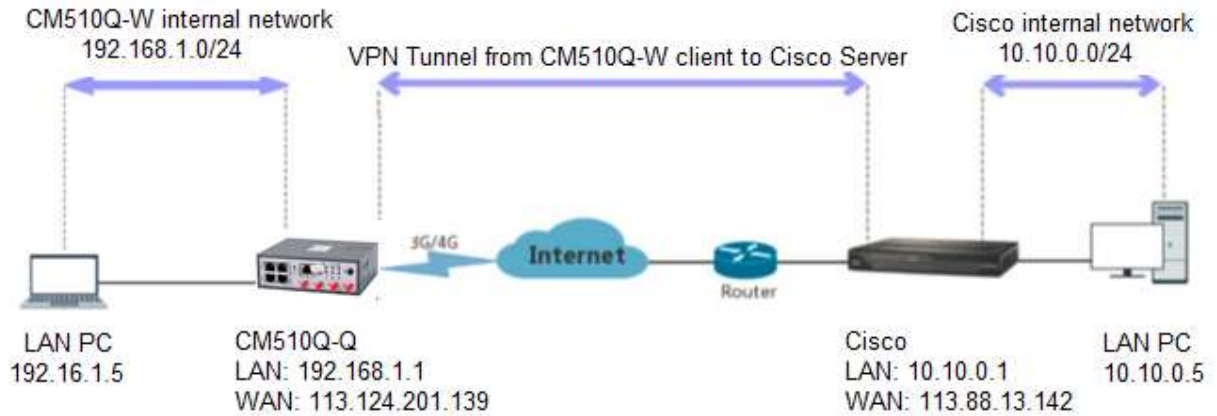
On	Name ^	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
✓	3	NO	1440	1440	✓	✗	debug;noipdefault;requ mppe-128

Note: The Custom options are based on your server.

4.6.4 IPSEC

IPSec between a Comset CM510Q-W and a Cisco Router

Network Topology



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) CM510Q-W Configuration

2.1) Navigate to VPN Tunnel > IPSec > Group Setup

The screenshot displays the IPsec configuration interface of the CM510Q-W Router. The left sidebar shows the navigation menu with 'VPN Tunnel' and 'IPSec' highlighted. The main area shows the 'IPSec' configuration page with tabs for 'IPSec 1', 'IPSec 2', and 'Schedule'. The 'Group Setup' tab is active. A red box highlights the 'Group Setup' tab and the configuration fields. The fields include:

- Enable IPsec: ☒
- IPsec Mode: Client
- IPsec Extensions: Normal
- Local Security Gateway Interface: 3G Cellular
- Local Security Group Subnet/Netmask: 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
- Remote Security Firewalling: ☒

There are 'Save' and 'Cancel' buttons at the bottom.

2.2) Navigate to VPN Tunnel > IPsec > Basic Setup

The screenshot shows the 'Basic Setup' tab for IPsec 1. The left sidebar has 'VPN Tunnel' and 'IPSec' highlighted. The main configuration area is divided into two columns. The right column contains the following settings, which are highlighted by a red box:

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

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

2.3) Navigate to VPN Tunnel > IPsec > Advanced Setup

The screenshot shows the 'Advanced Setup' tab for IPsec 1. The left sidebar has 'VPN Tunnel' and 'IPSec' highlighted. The main configuration area is divided into two columns. The right column contains the following settings, which are highlighted by a red box:

- Aggressive Mode: ☐
- Compress(IP Payload Compression): ☐
- Dead Peer Detection(DPD): ☐
- ICMP Check: ☒
- Check Period Time Interval: 3 seconds
- Check Timeout Count: 3 Times
- Check IP: 10.10.0.1
- IPsec Custom Options 1: rightid=%any

2.4) Check **Status** of the VPN IPsec connection.

The screenshot displays the router's web interface. On the left, a blue sidebar contains a 'Status' menu with a dropdown arrow. The 'Overview' option is selected and highlighted with a red rectangle. Below it are 'Traffic Stats.', 'GPS Status', and 'Device List'. Further down are 'Basic Network', 'WLAN', 'Advanced Network', 'Firewall', 'VPN Tunnel', and 'Administration', each with a right-pointing arrow. The main content area is white. At the top, a table shows IPsec status: 'IPSec 1' is 'Connected', 'Phase 1 Status' is '21 seconds', 'Phase 1 IKE' is '3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024', 'Phase 2 Status' is 'TUNNEL', 'Phase 2 ESP' is '3DES_CBC/HMAC_SHA1_96', 'IPSec Recv.' is '84 Bytes', and 'IPSec Send.' is '84 Bytes'. This table is enclosed in a red border. Below this is a 'LAN' section with a gear icon and a dropdown arrow. It lists 'Router MAC Address' as '34:0A:94:01:51:01', 'Router IP Addresses' as 'br0 (LAN) - 192.168.1.1/24', and 'DHCP' as 'br0 (LAN) - 192.168.1.2 - 192.168.1.51'.

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

--End