

Dual SIM Dual band Gigabit Router CM510Q-W

V1.2



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:
 <u>http://www.comset.com.au</u>

 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

Comset CM510Q-W	User Manual
-----------------	-------------

		uai
3.	3.9.3 Admin Access Settings	66
3.	3.9.4 Scheduled Reboot Settings	67
3.	3.9.5 SNMP Settings	68
3.	3.9.6 Storage Settings	69
3.	3.9.7 M2M Access Settings	70
3.	3.9.8 DI/DO Settings	71
3.	3.9.9 Configuration Settings	78
3.	3.9.10 System Log Settings	78
3.	3.9.11 Firmware Upgrade	79
3.	3.10 Reset Button to Restore Factory Settings	81
4 Con	nfiguration Examples	82
4.	4.1 Port Forwarding	82
4.	4.2 IP Pass-through	84
4.	4.3 Captive Portal	87
4.	4.4 GPS Settings (GPS version only)	90
4.	4.5 Firewall	91
4	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-tomachine 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
 - o B1+B1/B5/B8/B20/B28;
 - o B3+B3/B5/B7/B8/B20/B28;
 - o B7+B5/B7/B8/B20/B28;
 - B20+B32;
 - B38+B38;
 - B40+B40;
 - o 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

COMSET	CM510
Front	
Тор	

Table 2-1 CM510 Interface



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

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 \sim 32V DC
I/O	DI-1 and DI-2 are digital input. DO is digital output.	
Console	RJ45-DB9 cable for CLI configuration.	

Table 2-2 Router Interface

2.2 LED Status

LED	st	atus	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.	
	Signal I	Solid Light	Online.	
PWR	Solid Light		System power operation.	
	Solid light		WLAN enabled, but no data communication.	
WLAN	Blinking quickly		Data is being transmitted.	
	Dark		WLAN disabled.	
	Dark		System operation and LTE/3G online.	
EKK	Solid Light (Red)		System fail indicator. It indicates failure with SIM card/module.	
	Green	Solid light	Connected.	
	Green	Blinking	Data is being transmitted.	
LAN	Green	Dark	Disconnected.	
		·	·	

Table 2-3 Router LED indicator Status

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
	V+ V- GND RXD/A TXD/B DI-1 DI-1 DI-2 DO	

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

EVD DCD

0

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".

http://192.16	8.1.1		
our connect	ion to this site is not	private	
lsername	admin		
assword			
	.		

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.

Comset	om.au	Ξ		30 A	*	~	2	٥
 Status Overview 		You haven't change	ed the default passv password	word for this route <u>click here.</u>	er. To cha	ange ro	outer	
Traffic Stats. Device List		System						~
Basic Network		Router Name	Comset F	Router				
S WIAN	>	Hardware Version	C11-D13					
		Firmware Version	G5.0.1.5	1000120002				
Advanced Network	•	Chinset	1113G51 ARM/7 D	rocessor rev 5 (v7l)				
🔯 Firewall	•	cinpset	ALMAY C	10000001101010(171)				
VPN Tunnel	•	Router Time	Fri, 20 Se	p 2019 09:41:09 +1000	Clock Syn	c.		
💂 Administration	•	Uptime	00:07:33					
		Memory Usage	38.73 MB	/ 122.22 MB (31.69%)				
		NVRAM Usage	24.47 кв /	/ 64.00 KB (38.24%)				
		Ethernet Ports Status						~
		WAN/LAN1	LAN2	LAN3		LAN4		
		-	1	1		黨		
		1000M Full	Unplugged	Unplugged	ļ	Unplugge	d	
		VPN Status					4	>~
		No Active VPN						

O Status	*	LAN		á v
Overview				1. 19 7 (1. 19
Traffic Stats.		Router MAC Address	34:0A:98:12:55:05	
Device List		Router IP Addresses	br0 (LAN) - 192.168.1.1/24	
Basic Network	•	DHCP	br0 (LAN) - 192.168.1.2 - 192.168.1.51	
ବି WLAN	•	WAN		\$
Advanced Network	•	Connection Type	Cellular Network	
🔯 Firewall	>	Modem IMEI	868186040120352	
.		Modem BAND	B7 + B7	
		Modem CA	Yes	
R Administration	>	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	





Figure 3-5 Router Status GUI



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:

٥	Status	~	Already changed login password successfully.		
	Overview		T- W- Chite		
	Traffic Stats.		framic Stats.		
	Device List		Interface	Transmit Data	Receive Data
Ø	Basic Network	8	Cellular(usb0)	12.50 <i>MB</i>	11.29 <i>MB</i>
?	WLAN	2			
R	Advanced Network	>			
Ø	Firewall	•			
٠	VPN Tunnel	*			
*	Administration	>			

3.2.3 Device List

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

0	Status	*		Already changed login password successfully.							
	Overview		Device Li	ct							
	Traffic Stats.		Device Li	51							
	Device List		Interface	MAC Address	IP Address	Name	RSSI	Quality	TX/RX Rate	Lease	
٥	Basic Network	>				intume .				Leave	
\$	WLAN	•	br0	34:99:71:D5:03:79	192.168.1.17					23	3:23:36
	Advanced Network	•									
0	Firewall	>						~	3 seconds		▼ Stop×

3.3 Tools, Bandwidth, IP Traffic and System

Comset voermeler specifier	et.com.au	=		[*	<u>~</u>	#	٥
Status			Already changed	login password succe	ssfully.			
Overview Traffic Stats. Device List		System Router Name	c	Comset Router				~
Tools 🛠	Band	dwidth 👱	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.

Status		А	lready char	iged login pass	word successfull	y.		
Overview Traffic Stats.		▶ Ping / Trace 📮	ð WOL 🖿	Log 🔒 Capture				
Device List	•	Ping						
ক wlan	•	IP Address	8.8.8.8		Ping			
Advanced Network	2	Ping Count	5					
🔯 Firewall	>	Packet Size	56	(bytes)				
VPN Tunnel	•							
R Administration	>	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 Packets: 5 transmitted	n, 40.797 avg d. 5received,	, 54.331 max 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.

Status	۲	A	Already changed login password successfully.					
Overview Traffic Stats.		➢ Ping M Trace ☑	WOL	Log 🔒 Capture				
Device List		Trace Route	Trace Route					
Basic Network		IP Address	8.8.8.8		Trace			
ବି WLAN		(Analytication (Berline))	20					
Advanced Network		Maximum Hops	20					
	Ś	Maximum Wait Time	3	(seconds per hop)				
Administration								
A Administration		Hop Address			(ms) max (ms	.) avg (ms) +/- (ms)		

3.3.1.3 WOL

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



۲	Status	٠		Already	changed I	ogin pass	word successful	ly.
	Overview		Ping n Trace	🖫 WOL	E Log	Capture		
	Traffic Stats.			10	9			
	Device List		Wake On Lan					
٢	Basic Network	\$	Wake on Ear					
হ	WLAN		MAC Address		IP Address		Status	Name 🔨
	Advanced Network	•	34:99:71:05:03:79		192,108,1,17		Active (In ARP)	
8	Firewall		MAC Address List					
٩	VPN Tunnel							<i></i>
Ж	Administration	*	Wake Up 🔨					Refresh C

3.3.1.4 Log

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

۲	Status	٠	Already changed login password successfully.		
	Overview Traffic Stats.		➢ Ping 174 Trace State WOL ■ Log A Capture		
٢	Basic Network	*	Logs View		
چ ج	WLAN Advanced Network	> >	Download Log File		
8 0	Firewall VPN Tunnel	>	» Logging Configuration		
黒	Administration	*			

3.3.1.5 Capture

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

٥	Status	~	Already changed login password successfully.
	Overview Traffic Stats.		➢ Ping n Trace ♀ WOL ■ Log
-	Device List		Canture
٥	Basic Network	•	
Ŷ	WLAN	>	Time1 15 minutes Start
۲	Advanced Network	>	Network LAN T

3.3.2 Bandwidth

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

	Tools 🛠	Band	dwidth 🛩	IP Traffic	: <u>at</u>	System 🏚		
Com	set www.comset.ci	≡ om.au				*	2	≝ ≎
۲	Status	* -	ł	Already change	d login passv	vord successfull	у.	
	Overview Traffic Stats. Device List	2	Real-Time					
ø	Basic Network	> Re	eal Time Bandwidth	· · ·				
?	WLAN	•	Cellular (usb0) LAN	(br0) LAN (eth0)	LAN (vlan1)	Wi-Fi/2.4G (eth1)	Wi-Fi/5G (eth	2)
٢	Advanced Network	•		D/-3				A
8	Firewall		4 2 82.20 mbit/s (10.69 M	B/s)				
۰	VPN Tunnel	>	E 57.00 mbit/s (7.13 MB	/s)				
凩	Administration	•	00					
		(10	28.50 mbit/s (3.56 MB	/s) erval)				Λ
		R	X 0.74 kbit/s (0.09 KB/s)	Avg 2542.0 (310.3	51 kbit/s 8 KB/s)	Peak 110.26 mb (13.14 MB)	it/s /s)	Total ^{181.86}
		<u>1</u>	X 0.00 kbit/s (0.00 KB/s)	Avg 838.59 (102.3) kbit/s 7 KB/s)	Peak 33.86 mbit (4.04 MB/s	/s)	Total ^{59,98} MB

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.

Cor	nset www.comset.co	m.au	Ξ			*	2	<u>a</u>	٥
۲	Status	*	Alı	ready changed	login passwo	rd successfully.			
٢	Basic Network		WAN / Internet						
-	Cellular LAN		Туре	Disabled Disabled	•				
	VLAN Schedule DDNS		Save✓ Cancel×	DHCP PPPoE Static Address					
\$	WLAN								
۲	Advanced Network								
8	Firewall	>							
۵	VPN Tunnel	>							
*	Administration	>							

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	=	× ~ # \$
Status	Already changed login passw	vord successfully.
Basic Network WAN	Cellular Settings	
LAN VLAN	Enable Modem	
Schedule DDNS Routing	Use PPP	
🗟 WLAN	ICMP Check	
Advanced Network	Cellular Traffic Check	
Firewall	CIMI Send to :	
Administration	SMS Code	
	Operator Lock ex:46001	
	Band Lock Auto Currently Av	vailable Bands: B7
	DualSim Mode Fail Over	
	Fail Over Save ✓ Cancel × SIM 1 Only SIM 2 Only Backup	

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

🥺 Basic Network 🛛 👻	Cellular Settings		
WAN Cellular	Enable Modem	~	
LAN			
VLAN Schedule	Basic Settings SIM 1	SIM 2	
DDNS Routing	Use PPP		
ŵ wlan ♪	ICMP Check	~	
😭 Advanced Network 🔹	Check IP	8.8.8.8	
🔕 Firewall 🔹 🔹	Check IP (Optional)	8.8.4.4	
VPN Tunnel	Interval	60	(seconds)
T Administration	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 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.

Cellular Traffic Check	~	
Check Mode	Rx	×
Check Interval	10	(minutes)Range: 1 ~ 1440
Fail Action	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

۲	Status	>		Already o	hanged login p	assword succe	essfully.	
٥	Basic Network		LAN					~
	WAN Cellular		Bridge 🔨	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
	LAN VLAN		br0	192.168.1.1	255.255.255.0	*	192.168.1.2 - 51	1440
	DDNS Routing		1 •					
Ŷ	WLAN	•	Add+					
۲	Advanced Network	•	-					
8	Firewall	•	DNS					~
•	VPN Tunnel	?	Use Custom DNS					
栗	Administration	>	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

VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridg
1	~	×	~	×	~	×	~	×	~	×	br0
2	×	×	×	×	×	×	×	×	×	×	WAN
0 •											none

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.

Cor	nset www.comsetc	om.au	=			* •	<u>x w</u>	٥
۲	Status	>		Already changed lo	gin password	successfully.		
Ø	Basic Network		Enabled Links					~
	WAN Cellular		Link Name	Link Type		Description		
-	LAN VLAN		modem	ECM/QMI				
	Schedule		ICMP Check					v
-	Routing		On Link	Destination	Interval	Retries	Description	
↑	WLAN	2						
	Firewall	\$	Add+					
Ð	VPN Tunnel	•						
果	Administration	>	Schedule					~
			On Link 1	Link 2	Policy	Description		
				▼ modem ▼	FAILOVER			
			Add+					
			Save ✓ Cancel ×	Ì				

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.

modem ECM/QMI wan WAN(STATIC) ICMP Check On Link Destination Interval Retries Description v van 8.8.8 10 5	Link Na	me		Link Type			Descripti	on		
wari WAN(STATIC) LCMP Check Interval Retries Description on Link Destination Interval Retries Description wari 8.8.8.8 10 5 Interval Interval </th <th>modem</th> <th></th> <th></th> <th>ECM/QMI</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	modem			ECM/QMI						
ICMP Check Destination Interval Retries Description wan 88.8.3 10 3 a a a a a a a b a a b a b a a a a b a b a a a b a a a b b a b a b a b a b a b a a b a a b a b a a a b b a b b a b b a b a b a b a a b a b a b a a a<	wan			WAN(STATIC	5)					
On Link Destination Interval Retries Description wan 88.8.8 10 5	ICMP C	heck								~
van 8.8.8.8 10 5 Add+	On	Link	Destinati	on		nterval	Retries		Description	
Image: Constraint of the secondary Image: Constraint of the secondary Add+ Image: Constraint of the secondary Schedule Image: Constraint of the secondary On Link 1 Link 2 Policy Description Image: Constraint of the secondary Image: Constraint of the secondary Image: Constraint of the secondary Image: Constraint of the secondary Image: Constraint of the secondary Image: Constraint of the secondary	~	wan	8.8.8		3	10	5			
Add+ Schedule On Link 1 Link 2 Policy Description Image: The second and the second	~									
Schedule On Link 1 Van Van Van Modem Van Modem Van Modem	Add +									
Schedule On Link 1 Link 2. Policy Description Image: Margin and M										
On Link 1 Link 2 Policy Description Image: Second and the s	Schedu	le								~
wan v modem v FAILOVER v wan as primary and modem as secondary	On	Link 1	Link	2		Policy	Description			
	~	wan	v mo	dem	ж	FAILOVER	wan as primary	and modem as	s secondary	
Add+	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	
VLAN	
Schedule	
DDNS	
ক WLAN	
Advanced Network	
🐼 Firewall	
VPN Tunnel	
R Administration	

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:

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.

۲	Status	•	Already changed login password successfully.								
Ø	Basic Network			Current Routing	j Table						~
	WAN Cellular			Destination	Gat	eway / Ne	rt Hop	Subnet Mask	Metric	Interface	
	LAN			120.157.126.88	*			255.255.255.255	0	WAN	
	VLAN Schedule			120.157.126.80				255.255.255.240	0	WAN	
	DDNS			192,168.1.0				255.255.255.0	0	LAN	
	Routing			127.0.0.0				255.0.0.0	0	lo	
1	WLAN			default	120	.157.126.88	l.	0.0.0.0	0	WAN	
\$	Advanced Network	*									
2	Firewall	•		Static Routing T	able						~
•	VPN Tunnel	`		Destination	Gatewa		Subnet Mask	Metric	Interface	Description	
黒	Administration			Destination	Gatewa	y.	Jubliet Mask	metre	interface	Description	
					0.0.0.0			0	LAN V		
				Add+							
			-								
				Miscellaneous							v
				Mode		Gatewa	y 🔻				
				RIPv1 & v2		Disable	d 🔻				
				DHCP Routes		~					
				Spanning-Tree Pro	otocol						
	A1										
	W More Into			Save ✓ Cance	1×						

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"

Status)		Alre	eady changed login password successf
Basic Network	<u>.</u>	Radio Mode	2.4G + 5G 🗸	
S WLAN Basic Settings	•	Wireless(2.4 GHz) Wireless(5 GHz)		
MultiSSID Wireless Survey		Enable WLAN		
Advanced Network	>	MAC Address	34:0A:98:12:55:07	
Firewall	21	Wireless Mode	Access Point 🗸	
VPN Tunnel	•	Wireless Network Mode	Auto ~	
, Administration	2	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
			2600 (carenada)	

Vireless(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)	

/ireless(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 Q	
Channel Width	80 MHz	
Control Sideband	Upper 🗸	
Maximum Clients	128 (range: 1 - 255)	
Security option	WPA / WPA2 Personal	
Encryption	TKIP / AES	
Shared Key	••••••	Randor
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.

Status	*			Already c	hanged lo	gin passv	word succe	ssfully	y.	
Basic Network	•	Wireless Site Su	2 (0) (
🐨 WLAN		Wireless Site Su	vey							
Basic Setting MultiSSID	IS	Last Seen 🧥	SSID	BSSID	RSSI	Noise	Quality	Ch	Capabilities	Rates
Wireless Sur	vey	0 added, 0 remove	d, 0 total.							
Advanced Net	work	Lest updated. Mon o.	1.21							
🔯 Firewall	>					¢	Auto Expire	~	Auto Refresh 🗸	Refresh C
VPN Tunnel	•									
R Administratio	n) 👂									

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"	

0	Status	`			Already	changed log	gin password	successfully.	
۲	Basic Network	>	PortF	onwarding					
7	WLAN	>	Torti	orwarding					
æ	Advanced Network	•	On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description ^
	Port Forwarding		×	UDP		1000,2000		192.168.1.2	ex: 1000 and 2000
	Port Redirecting DMZ		×	Both		1000-2000,30	00	192.168.1.2	ex: 1000 to 2000, and 3000
	IP Passthrough Triggered		×	Both	1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted
	Captive Portal Serial App.		×	ТСР		1000	2000	192.168.1.2	ex: differen <mark>t</mark> internal port
	UPnP/NAT-PMP Bandwidth Limiter		4	ТСР	~				
	VRRP Static DHCP		Ad	id +					
Ø	Firewall	•		Src Address ("me.example	<i>optional</i>) - Forward or .com".	nly if from this ac	ddress. ex: "1.2.3.4	", "1.2.3.4 - 2.3.4.5",	"1.2.3.0/24",
0	VPN Tunnel	•	:	Ext Ports - In Int Port (optic Only one por	ne ports to be forwarde onal)The destination rt per entry is supporte	ed, as seen from n port inside the d when forward	LAN. If blank, the ing to a different i	destination port is t nternal port	the same as <i>Ext Ports</i> .
ѫ	Administration	•	•	Int Address -	The destination addres	ss inside the LAN	1.		
			Save~	Cance	ł×				

Figure 3-8 Port Forwarding GUI

	6
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.

Table 3-7 Port Forwarding Instructions

3.6.2 Port Redirecting

Go to Advanced Network > Port Redirecting.

Status	•		Already changed login password successfully.				
Basic Network	2						
🗇 WLAN	•	PortRedirecting					
Advanced Network	•	On Proto	Int Port	Dst Address	Ext Port	Description	
Port Forwarding		🔽 тср 🗸					
Port Redirecting							
DMZ		Add+					
IP Passthrough							
Triggered							
Captive Portal							
Serial App.		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:

0	Status	3		Already changed login password successfully.				
۲	Basic Network	>	DMZ					
	WLAN	•						
龠	Advanced Network	*	Enable DMZ					
	Port Forwarding		Internel Address	192.168.1.0				
	Port Redirecting							
	DMZ		Source Address					
-	IP Passthrough		Restriction	(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1 - 2.2.2.2" or "me.example.com")				
-	Triggered							
=	Captive Portal							
-	Serial App.		Leave CLI Remote Access	(Redirect remote access ports for CLI to router)				
	UPnP/NAT-PMP							
	Bandwidth Limiter		Leave WEB Remote Access	(Redirect remote access ports for HTTP(s) to router)				
	VRRP							
	Static DHCP							
8	Firewall	•	Save√ Cancel×					

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



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.

۲	Status	Already changed login password successfully.
ø	Basic Network	10 Desethereset
1	WLAN	IP Passtnrough
æ	Advanced Network	Enabled
	Port Forwarding	MAC Address
	Port Redirecting	
	DMZ	Gateway
	IP Passthrough	
	Triggered	
	Captive Portal	Save ✓ Cancel ×
	Serial App.	

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.			

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.

0	Status	>	Already changed login password successfully.						
۲	Basic Network	>	Tripering Best Fernandian						
6	WLAN	•	niggi		orwarding				
R	Advanced Network	•	On	Protocol	Irigger Ports	Forwarded Ports	Description *		
	Port Forwarding		×	ICP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000		
	Port Redirecting			тср 🗸					
	DMZ								
	IP Passthrough		Ac	ld +					
	Triggered								
	Captive Portal			(200-300)					
	Serial App.		•	These ports	are automatically c	losed after a few minutes of	f inactivity.		
	UPnP/NAT-PMP								
	Bandwidth Limiter		Saver	Cance	elx				
	VRRP		Jures	Contra					
	Static DHCP								

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> C	aptive Portal to	check or modify	the relevant	parameters.
--------	----------------	------------	------------------	-----------------	--------------	-------------

😧 E ବି \ 🔒 /	Basic Network WLAN	> >	Captive Portal			
হু । ক্লি /	WLAN	>				
@ /			Enabled			
	Advanced Network	*			· · · · · · · · · · · · · · · · · · ·	
Ľ	Port Forwarding Port Redirecting		Auth Type	NONE		
	DMZ		WEB Root	Default	×	
	IP Passthrough Triggered		WEB Host			
-	Captive Portal		Portal Host			
	Serial App. UPnP/NAT-PMP Bandwidth Limiter		Login Timeout	0	Minutes	
	VRRP Static DHCP		Idle Timeout	0	Minutes	
1	Firewall	•	Ignore LAN	~		
@ \	/PN Tunnel	•	Redirecting http://	www.goog	e.com	
泉 /	Administration	•	MAC Address Whitelist			
			Download QOS			
			Upload QOS			

Item	Description
Enable	Enable Captive Portal.
Auth Type	Reserved.
Web Root	Choose captive portal file storage path.
	In storage, Contine portal file is in the reuter's Fleeh
	in-storage: Captive portai 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.

@ Si	tatus	>		Already changed login password successfully.				
😢 В	asic Network		Serial to TCP/IP					
ଙ୍କ M	VLAN		Schur to Yer yn					
😭 A	dvanced Network		IPoC Mode	Serial V				
- P - P - C	Port Forwarding Port Redirecting DMZ P Passthrough		Serial to TCP/IPMode	Disabled V				
T C	friggered Captive Portal		Save√ Cancel×					
s U	JPnP/NAT-PMP							

0	Status	•	Serial to TCP/IP		
Ø	Basic Network	•	IPoC Mode	Serial	~
6	WLAN	•	Serial to TCP/IPMode	Client	- 'I I I I I I I I I I I I I I I I I I I I
A	Advanced Network				
	Port Forwarding Port Redirecting		Server IP/Port	8.8.8.8 40002	
	DMZ IP Passthrough		Socket Type	тср 🗸	
	Triggered Captive Portal		Socket Timeout	500	(millisecands)
	Serial App. UPnP/NAT-PMP		Serial Timeout	500	(milliseconds)
	Bandwidth Limiter VRRP		Packet Payload	1024	(bytes)
8	Static DHCP Firewall	\$	Heart-Beat Content		
a	VPN Tunnel	•	Heart-Beat Interval	2	(seconds)
杘	Administration	•	Port Type	RS485/RS23	2 🗸
			Cache Enable	.	
			Debug Enable		
			Baud Rate	57600 ~]
			Parity Bit	none 🗸	
			Data Bit	8 🛩	
	(i) Marculata		Stop Bit	1 ~	

CM510Q-W Router User Manual

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.



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.

CM510Q-W Router User Manual

۲	Status	*	Already changed login password successfully.					
() ()	Basic Network WLAN		Forwarded Pc	orts				
R	Advanced Network		Ext Ports	Int Port	Internal Address	Protocol	Description	
Ļ	Port Forwarding Port Redirecting					L.	Delete All X C Refresh	
	DMZ IP Passthrough		Settings				×	
	Triggered Captive Portal		Enable UPnP					
	Serial App. UPnP/NAT-PMP		Enable NAT-PI	MP				
	Bandwidth Limiter VRRP		Inactive Rules	Cleaning	1			
-	Static DHCP		Secure Mode		when enabled, UPnP clients are a	llowed to add mappings only t	o their IP)	
8	Firewall	°,	Show In My N	atwork				
風	Administration		Places	Current				
			Save Ca	ncel×				

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.

Status		Already changed login password successfully.						
Ø Basic Network		Bandwidth Control						
🗟 WLAN	•	Table Cashel						
Advanced Network	~							
Port Forwarding Port Redirecting DMZ		IP IP Range MAC Address DLRate DLCeil ULRate ULCeil	Priority					
IP Passthrough Triggered Captive Portal		Add+	Nom					
Serial App. UPnP/NAT-PMP Bandwidth Limiter		Default Class						
VRRP Static DHCP		Enable Default Class						
🐼 Firewall								
VPN Tunnel		Save Cancel X						
R Administration	>							

mum download speed available.

CM510Q-W Router User Manual

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.

letwork	2		
	•	VRRP	
ed Network		Enable VRRP	
orwarding edirecting		Mode	backup 🗸
		Virtual IP	192.168.1.3
red		Virtual Router ID	
e Portal App.		Priority	100
'NAT-PMP vidth Limiter		Authentication	
DHCP		Script Type	Default 🗸
I.	•	Check Interval	3
innel	•	Weight	10
istration	•		
		Save√ Cancel×	l
	ed Network orwarding edirecting sthrough red e Portal App. NAT-PMP vidth Limiter DHCP i unnel istration	ed Network × orwarding edirecting sthrough red e Portal App. NAT-PMP vidth Limiter DHCP 1 > innel > istration >	Red Network porwarding edirecting withough red e Portal App. NAT-PMP with Limiter DHCP > Check Interval weight stration

Click "Save" to finish.

3.6.11 Static DHCP Settings

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

O Status	А	Iready changed login pas	sword successfully	
Basic Network	Static DHCP			
🗟 WLAN	MAC Address	IP Address	Hostname 🛆	Description
Advanced Network				
Port Forwarding Port Redirecting	00:00:00:00:00:00	192.168.1.2		
DMZ				
IP Passthrough Triggered	Add+			
Captive Portal	_			
Serial App. UPnP/NAT-PMP	Save√ Cancel×			
Bandwidth Limiter				
VRRP Static DHCP				
🐼 Firewall				
VPN Tunnel				
R Administration				

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.

Status	*	Already changed login password successfully.
Basic Network	•	IP/MAC/Port Filtering
🗟 WLAN	•	
Advanced Network	>	On SIC MAC SIC IP DELIP Protocol SIC Port DELPOR Policy Description
🐼 Firewall		NON Acc V
IP/URL Filtering		Add +
Domain Filtering		
U VPN Tunnel		Key Word Filtering
R Administration	>	On Key Word Description
		Add+
		URL Filtering
		On UPL Description
		on une Description
		Add+
		Access Filtering
		On Src MAC Src IP Dst IP Protocol Src Port Dst Port Policy Description
		NON ~ Acc ~
		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 log	in password successfully.
2	Domain Filtering		
.	On		
•			
*	Default Policy	White List	
	On Domain		Description
•	×		
•	Add +		
	Save 🗸 🛛 Cancel 🗙		
		 Domain Filtering On Default Policy On Domain Add+ Save (Cancel × 	 Already changed log Domain Filtering On Default Policy White List On Domain 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.

O Status	\$	Already changed login password successfully.	
Basic Network	•	GRE Tunnel	~
🗟 WLAN	•	Total Total Total	
Advanced Network	•	On Idx Address Source Destination Keepalive Interval Retries	Description
🔯 Firewall	•		
VPN Tunnel GRE	۲	Add+	
OpenVPN Client PPTP Server PPTP Online PPTP/L2TP Client IPSec	•	GRE Route On Tunnel Index A Destination Address Description I I I I I I I I I I I I I I I I I I I	~

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.

Status	>	Already changed login password successfully.
Basic Network	>	Open V/IN Client
ଙ୍କ WLAN	•	
Advanced Network	٠	Client 1 Client 2
🐼 Firewall		Basic Advanced Keys Status
VPN Tunnel	*	
GRE		VPN Client #1 (Stopped)
OpenVPN Client		Start with WAN
PPTP Online		TIN
PPTP/L2TP Client		Interface lype
IPSec		Protocol UDP 🗸
R Administration	•	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.

CM510Q-W Router User Manual

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.

CM510Q-W Router User Manual

Poll Interval	0 (in minutes, 0 to disa	ble)
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 <mark>(</mark> tls-remote)		
Custom Configuration		

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 time1 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.

Client 1	Client 2		
Basic	Advanced	Keys	Status
VPN (Client #1 <mark>(Sto</mark>	pped)	
For hel	p generating k	eys, refer	to the OpenVPN HOWTO.
Certif	icate Authority		
Client	Certificate		
Client	Key		

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.

OpenV	/PN Client				
Client 1	Client 2				
Basic	Advanced	Keys	Status		
VPN C	lient #1 (St not running	opped) or status c	ould not be	≥ read.	
Start Nov	i				
Save ✓	Cancel	×			
arameter		Instructio	'n		

Click "Save" to finish.

Status

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.

Check Openvpn status and data statistics.

CM510Q-W Router User Manual

Status	>	Already changed login password successfully.			
😨 Basic Network 중 WLAN	> >	PPTP Server			
Advanced Network	>	Enable			
🔞 Firewall	>	Local IP Address/Netmask	192.168.1.1 / 255.25	5.255.0	
VPN Tunnel GRE	~	Remote IP Address Range	172.19.0.1	- 172.19.0.6	(6)
OpenVPN Client PPTP Server		Broadcast Relay Mode	Disabled	Enabling this may cause HIG	H CPU usage
PPTP Online PPTP/L2TP Client		Encryption	MPPE-128		
IPSec		DNS Servers	0.0.0.0		
Administration			0.0.0		
		WINS Servers	0.0.00		
			0.0.0.0		
		MTU	1450		
		MRU	1450		
		Poptop Custom configuration			
OpenVPN Client					
PPTP Server PPTP Online PPTP/L2TP Client		Custom iptables if-up rules			
IPSec R Administration	•	Custom iptables if-down rules			
		Notes A			
		PPTP User List			
		Username 🔨		Password	
		Add +			
		Save ✓ Cancel ×			» РРТР

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.
```

Status	.	LITE/DEE Paris	
Basic Network	•	LZIP/PPIP Dasic	~
🗟 WLAN		On Protocol Name Server Username Password Firewall Default Loca	il IP
Advanced Network	•	L2TP V	
🔯 Firewall		Add+	
D VPN Tunnel	•		
GRE OpenVPN Client		L2TP Advanced	~
PPTP Server PPTP Online		On Name Accept DNS MTU MRU Tunnel Tunnel Custom Auth Password	Options
PPTP/L2TP Client			
- IPSec			
		PPTP Advanced On Name Accept DNS MTU MRU MPPE Cust Stateful Opti	∼ tom ions
		Add+	
		Schedule On Name 1 ^ Name 2 Policy Description	v
		FAILOVER V	
		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

Status		Already changed login pass	word successfully.
Basic Network	IPSec		
WLAN Advanced Network	IPSec 1 IPSec 2 Scher	dule	
3 Firewall	Group Setup Basic Setup	Advanced Setup	
VPN Tunnel	Enable IPSec		
GKE OpenVPN Client PPTP Server	IPSec Mode	Client	
PPTP Online PPTP/L2TP Client	IPSec Extensions	Normal	
IPSec	Local Security Gateway Interface	3G Cellular	
T Administration	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 X		

3.8.5.1 IPSec Group Setup

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

Group Setup Basic Setup	Advanced Setup	
Enable IPSec		
PSec Mode	Client	
IPSec Extensions	Normal	
Local Security Gateway Interface	3G Cellular	
Local Security Gro <mark>u</mark> p Subnet/Netmask	192:168.1.0/24	ex, 192.168.1.0/24
.ocal Security Firewalling		
Remote Security Gateway P/Domain		
Remote Security Group Subnet/Netmask	10.0.0/24	ex. 192.168.88.0/24
Remote Security Firewalling		

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.

3.8.5.2 IPSec Basic Setup

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

Group Setup Basic Setup	Advanced Se	tup		
Ceying Mode	IKE with F	Preshared Key		
hase 1 DH Group	Group 2 -	modp1024		
Phase 1 Encryption	3DES (168	-bit)		
Phase 1 Authentication	MD5 HM	AC (96-bit)		
Phase 1 SA Life Time	28800	seconds		
hase 2 DH Group	Group 2 -	modp1024		
hase 2 Encryption	3DES (168	3DES (168-bit)		
hase 2 Authentication	MD5 HM	AC (96-bit)		
hase 2 SA Life Time	3600	seconds		
reshared Key				

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.

Table 3-15 "IPSec Basic Setup" Instructions

3.8.5.3 IPSec Advanced Setup

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

IPSec 1 IPSec 2 Sched	ule
Group Setup Basic Setup	Advanced Setup
Aggressive Mode	
Compress(IP Payload Compression)	
Dead Peer Detection(DPD)	
CMP Check	-
PSec Custom Options 1	
PSec Custom Options 2	
PSec Custom Options 3	
PSec Custom Options 4	

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	IPSec advanced settings such as left/right ID.
Options	

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.

0	Status	•
0	Basic Network	*
ি	WLAN	*
	Advanced Network	,
8	Firewall	Ŷ
٠	VPN Tunnel	•
凩	Administration	*
	Time	
	Admin Access	
	Scheduled Reboot	
	Storage Settings	
	M2M Settings	
	DI/DO Setting Configuration	
	Logging	
	Upgrade	

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. O Status Already changed login password successfully. Basic Network • Time 🛜 WLAN > Router Time Tue, 24 Sep 2019 08:29:26 +1000 Clock Sync. Advanced Network > S Firewall UTC+10:00 Australia Time Zone VPN Tunnel Auto Daylight Savings R Administration Time Identification Time Every 1 Hour Auto Update Time Admin Access **Scheduled Reboot** Trigger Connect On SNMP Demand **Storage Settings** Default NTP Time Server M2M Settings **DI/DO Setting** 0.pool.ntp.org, 1.pool.ntp.org 2.pool.ntp.org Configuration Logging Upgrade Save✓ Cancel ×

Figure 3-17 Time Settings GUI

CAUTION

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.

		CM	I510Q-W Router User Manual
Status	>	Alrea	dy changed login password successfully.
Basic Network		WebAccess	
	\$ \$	Web Style	GUI3.0 V
Se Firewall	27 >	Local Access	нттр 🗸
VPN Tunnel	•	HTTP Access Port	80
R Administration	·•	Remote Access	Disabled Y
Identification Time	Pro 1		
Admin Access		Allow Wireless Access	
Scheduled Reboot SNMP		Block WAN Ping	
Storage Settings		SSH Enable at Startup	
M2M Settings DI/DO Setting Configuration		Allow Telnet Remote Access	
Logging Upgrade			
	1	Password	
		Password	
		(re-enter to confirm)	•••••
		Save ✓ Cancel ×	

Figure 3-18 Admin Access Settings GUI

3.9.4 Scheduled Reboot Settings

Please follow the instructions below:

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

				CM510Q-W Router User Manual	
0	Status	8	Already changed login password successfully.		
0	Basic Network	>	Scheduled Rehoot		
(¢	WLAN	>	Scheduled Report		
£	Advanced Network	*	Enabled		
Ø	Firewall	>	Time	1:00 AM	
۵	VPN Tunnel	>	Days	Sun Sun Tue Wed Fri Sat	
凩	Administration			Everyday Everyday	
	Identification				
	Time		Save & Cancely	1	
	Admin Access		Savev		
	Scheduled Reboot				
	SNMP				
	Storage Settings				
	M2M Settings				
	DI/DO Setting				
	Configuration				
	Logging				
	Upgrade				
			Figure 3-1	9 Scheduled Reboot Settings GUI	

3.9.5 SNMP Settings

Please follow the instructions below:

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

♥ Status	SNMP Settings	
Basic Network	Enable SNMP	
후 WLAN > 🔗 🙀 Advanced Network	Port	161
🐼 Firewall 🔹	Remote Access	
VPN Tunnel	Allowed Remote	
Identification		(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" of "me.example.com")
Time Admin Access	Location	router
Scheduled Reboot	Contact	admin@router
Storage Settings M2M Settings	RO Community	rocommunity
DI/DO Setting Configuration	Custom OID :	erv/hin/nyram.net.snmn.enable
Logging Upgrade	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	
More Info	Save ✓ Cancel ×	

Figure 3-20 SNMP Settings GUI

3.9.6 Storage Settings

Step 1 Select "Administration>Storage Settings" to check and modify relevant parameters.

CM510Q-W Router User Manual

			CM510Q-W	Router User Manual
OStatus	>	Alread	dy changed login pa	ssword successfully.
Basic Network	>	Storage settings		
ବି WLAN	>	Storage	Router	✓ Total :5 376.00 KB Free:5 116.00 KB
Advanced Network	>	ototuge		
🕄 Firewall	\$			
💷 VPN Tunnel	>	Upload new file		
R Administration		No file chosen	Cho	ose File Upload
Identification				
Time				
Admin Access		Current file list		
Scheduled Reboot		300 YO X X X X X X X X X X X X X X X X X X		
SNMP		File name	File size	File operation
Storage Settings				
M2M Settings				
DI/DO Setting		Save Cancel X		
Configuration		المستقا التفسي		
Logging				
Upgrade				

Step 2 Click "Save" to finish.

3.9.7 M2M Access Settings

Step 1 Select "Administration>M2M Settings" to check and modify relevant parameters.

			CN	1510Q-W Router Us	ser Manual
Status	•	Alread	ly change	ed login password	successfully.
Basic Network	, m	2m			
중 WLAN	, N	12M Enabled			
🐼 Firewall	> F	ail Action	Restart	M2M	
VPN Tunnel	>	Device ID			
R Administration	✓				
Identification	N	/I2M Server/Port			; 8000
Admin Access	H	leartbeat intval	60	(seconds)	
Scheduled Reboot	E Contraction de la contractio	leartbeat Retry	10	(Range:10-1000)	
Storage Settings					
M2M Settings DI/DO Setting	Ň	Jamed-Pipe Enabled	Remote	e Connect 🤟	
Configuration	М	lamed-Pipe Server Port	8002 (Ra		(Range:1024-65535)
Upgrade	N	lamed-Pipe Status	Offline		
	٨	lamed-Pipe Address	0.0,0,0		
	Sav	re✓ Cancel×			
		Figure 3-21 N	12M Acc GUI	ess Settings	

3.9.8 DI/DO Settings

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

http://www.comset.com.au

			CM510Q-W Ro	outer User Manual	
𝑁 Status	>	Alr	Already changed login password successfull		
Basic Network	•				
ବି WLAN	•	DI Setting			
Advanced Network	> 1	Enabled	Port1	Port2	
🛿 Firewall	•				
🗓 VPN Tunnel	<u>.</u>				
R Administration	•	DO Setting			
Identification		Enabled	×		
Time Admin Access		Alarm Source	DI Control	SMS Control	
Scheduled Reboot		Alarm Action	on ~		
Storage Settings M2M Settings		Power On Status	OFF 🛩		
DI/DO Setting		Keep On	1	(*100ms)	
Configuration					
Logging					
Upgrade		Save Cancel 🗙			

Figure 3-22 DI/DO Settings GUI
3.9.8.1 DI Configuration

● Status >	Alro	eady changed logi	n password successfully.
Basic Network S WLAN	DI Setting		
Advanced Network	Enabled	Port1 🗸	Port2
🔞 Firewall >	Port1Mode	ON	~
VPN Tunnel	Filter	1	(*100ms)
Identification Time Admin Access	SMS Alarm		
Scheduled Reboot SNMP Storage Settings	DO Setting Enabled	×.	
DI/DO Setting Configuration	Alarm Source	DI Control	SMS Control
Logging Upgrade	Alarm Action	ON ~	
	Power On Status	OFF 🗸	
	Keep On	1	(*100ms)
	Save 🗸 🛛 Cancel 🗙		

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 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.
	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.
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.
	HI_TO_LO and LO_TO_HI is available when the DI is under Event Counter mode.
Counter Action	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.
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.

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
•	-			

ବି WLAN	•	DO Setting		
Advanced Network	•	Enabled		
🕄 Firewall	2	Alarm Source	DI Control 🔽	SMS Control 🔽
VPN Tunnel	>	Alarm Action	Pulse 🗸	
R Administration	*			
Identification		Power On Status	ON Y	
Time Admin Access		Delay	0	(*100ms)
Scheduled Reboot SNMP		Low	10	(*100ms)
Storage Settings M2M Settings		High	10	(*100ms)
DI/DO Setting		Output	1	
Configuration Logging		SMS Trigger Content		
Upgrade			70 ASCII Max	
		SMS Reply Content	70 ASCII Max	
		SMS admin Num1		
		SMS admin Num2		Backup
① More Info		Save ✓ Cancel ×		

Table 3-19 "DO" Instructions

Item	Description
Enable	DO is enabled.
Alarm Source	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.
	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	Specify the Digital Output status when the power is on.
Status	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.
	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.
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	Available when you enable SMS Control in Alarm Source.
Content	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 NOTE

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.

0	Status	>	Alrea	Already changed login	Already changed login password
Ø	Basic Network	>			
(7	WLAN	•	Backup Configuration	Backup Configuration	Backup Configuration
@	Advanced Network	\$	router_015_m125505	router_015_m125505 .cf	router_015_m125505 .cfg Backup
Ø	Firewall	•	Save As Default Configu	Save As Default Configuration	Save As Default Configuration
8	VPN Tunnel	•	Save	Save	Save
杲	Administration	*	Restore Configuration	Restore Configuration	Restore Configuration
	Identification		Select the configuration file	Select the configuration file to restore:	Select the configuration file to restore:
	Time		No file chosen	No file chosen	No file chosen Choose File
	Admin Access Scheduled Reboot		Restore Default Configu	Restore Default Configuration	Restore Default Configuration
	SNMP		Select	Select 🗸 OK	Select 🗸 OK
	Storage Settings M2M Settings DI/DO Setting		Total / Free NVRAM:	Total / Free NVRAM:	Total / Free NVRAM: 64.00 KB / 31
	Configuration				
	Logging				
	Upgrade				





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).





Step 2 Click "Save" to finish.

3.9.11 Firmware Upgrade

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



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.

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

Table 3-20 System Default Instructions



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

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.

co rirewali	2	Local Access		HTTP
VPN Tunnel		HTTP Access Port		8080
R Administration	.	Remote Access		нттр
Identification Time		Access Port	ſ	8080
Admin Access Scheduled Reboot	1	Allowed Remote		
access the GUI of the	e router, us	se URL <u>http://192.168.1.1:8</u>	<u>3080</u>	
< 7 U U	U NOT SE	T37.100.1.1:0000/#St	atus-nome.asp	
👖 Apps Comset	G Goog	gle (?) www.speedtest.net		
Apps 📤 Comset	G Goog	gle (?) www.speedtest.net		
Apps 📤 Comset	G Goog E Minau	gle (?) www.speedtest.net		
Apps Apps Comset	G Goog = 	gle (?) www.speedtest.net		
Apps Comset	G Goog	gle (?) www.speedtest.net		
Apps Comset	G Goog	gle (?) www.speedtest.net	Connect Parities	

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.



				CM510Q-W Router User Manual			
Advanced Network	On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description ^
Port Forwarding	~	UDP		8000	8000	192.168.1.17	
Port Redirecting	~	TCP		433	433	192.168.1.17	
DMZ		Poth		8000	8000	102159117	
IP Passthrough	_	boun		8000	8000	192.100.1.17	
Triggered		TCP		80	80	192.168.1.200	IP Camera
Captive Portal	-	, I.,		1.11	1.1		
Serial App.	Add	+					
UPnP/NAT-PMP	_						

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

4.2 IP Pass-through

<u>Note</u>: 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:

Network Connection Detail	s 📃 🔨
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 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'.

er the MAC Address as obtained from your PC LAN Internace and click Save.

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

Delow:		
Status	You haven't cha	nged the default password for this router. To change router password <u>click h</u>
Basic Network		
🗟 WLAN 🔹 🕨	IP Passthrough	
🚔 Advanced Network 👻	Enabled]
Port Forwarding	MAC Address 10:	9:47:BD:5E:51 Set MAC Address on Laptop LAN interface
Port Redirecting		Note: Use colon in between of hexadecimal characters
DMZ	Gateway	
IP Passthrough		
Triggered		
Captive Portal	Save / Cancel X	
Serial App.	Cancerto	
UPnP/NAT-PMP		

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.

				CM510Q-W	Router User Manual		
۲	Basic Network	LAN				<u> </u>	
	WAN	LAN					
	Cellular	Bric	lge 🔨	IP Address	Subnet Mask	DHCP Server	
	VLAN Schedule	0	*	192.168.1.1	255.255.255.0		192.168 192.168
	Routing	Delete ×	CancelØ	OK		Click on DHCP Se	erver box to
?	WLAN			لكنت		option to Disabl	e and click o
•	Advanced Network	1	*				
20	Firewall						
ø	VPN Tunnel	Add +					
界	Administration	Save√ Ca	ncel×				

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:

	Ethe Netv	rnet vork	
-	💡 D	isable	
	S	tatus	
	D	iagnose	
	🌍 В	ridge Connections	
	С	reate Shortcut	
	💡 D	elete	
	🦁 R	ename	
	🤣 Pi	roperties	
1	-		
C.	Ether	net	A
and the second sec	L/ISdC		_
de la	Realt	e 💡 Enable	
	Realt	e 😯 Enable Status	
all a	r Realt	e 😯 Enable Status Diagnose	
	Realt	e 😵 Enable Status Diagnose Create Shortcu	t
	r Realt	E Status Diagnose Create Shortcu	t
all a	f Realt	E Status Diagnose Create Shortcu Delete Rename	t

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-

Property	Value
Connection-specific DN Description Physical Address	Comset_Domain Realtek PCIe GBE Family Controller 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

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.

	8005		Captive Portal	10.00	1
🤵 Ba	isic Network	•	Enabled	.	
ବ WI	LAN	•	Auth Type	NONE •	
😭 Ad	Ivanced Network	*			
Po	ort Forwarding		WEB Root	Default	X
Po	ort Redirecting MZ		WEB Host		
IP Tr	Passthrough riggered		Portal Host		
G	aptive Portal		Login Timeout	0	Minutes
Se	erial App.				
U	PnP/NAT-PMP		Idle Timeout	0	Minutes
vi St	RRP tatic DHCP		Ignore LAN	4	
🐼 Fin	rewall		Redirecting http://	www.google	.com
💷 VP	'N Tunnel	•	MAC Address Whitelist		
롰 Ad	Iministration		Download QOS		
			Upload OOS		
			Save ✓ Cancel x		

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.

		CM510C	Q-W Router User Manual
Basic Network	2	Storage settings	
 WLAN Advanced Network 	,	Storage	Router 🔻
8 Firewall	*		
VPN Tunnel	>	Upload new file	
R Administration	*	No file chosen	Choose File Upload
Identification			
Time			
Admin Access Scheduled Reboot		Current file list	
SNMP		File name	File size
Storage Settings		100.00	
M2M Settings		sms.list	3/6
DI/DO Setting			
Configuration			
Logging		Save Cancel X	
Upgrade		Community Community and	

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.

• Status	3	Storage settings				
😡 Basic Network		Storage	Rauter	 Takat (1,612.00 va Freed) 100.00 va 		
· WLAN	2	222-22				
· Advanced Network	- 5					
E forest	10	Upload new file				
VIN Tunnel		No file chosen	Choose File Uple	ed		
R Administration						
Mentilication Time		Current file list				
Admin Access		Ele name		File size	File operation	
Scheduled Reboot		gristerog,1000		23.6K	**	
Storage Settings		0002_portwiping		4536		
M2M Settlege		0000_portal.prg		46.04		
Configuration		boots/map_portal.com		124.36	1.2	
Logging		jąvery portal ja		289.7%		
Upgrade		splash.html		346	1.0	
O More Info						



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.

			CM510Q-W Router User Manual
 Status Rasir Network 	*	Captive Portal Enabled	
🗣 WLAN		Auth Type	NONE 🔻
Advanced Network	*	WEB Root	In-storage 🔻
Port Forwarding Port Redirecting		WEB Host	
DMZ IP Passthrough		Portal Host	
Triggered Captive Portal	ē	Login Timeout	0 Minutes
Serial App. UPnP/NAT-PMP		Idle Timeout	0 Minutes
Bandwidth Limiter VRRP	È.	Ignore LAN	
Static DHCP		Redirecting http://	www.google.com
VPN Tunnel	•	MAC Address Whitelist	
Administration	•	Download QOS	
		Save Cancel x	—

4.4 GPS Settings (GPS version only)

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

© Satar 3	8	You haven't changed the default password for this ro	uter. To change router password, <u>clasters</u> ,
W MAN	GPS		
G. Advanced National	GPS Mode	Clare *	
Port Forwarding Port Referencies	Data Format	M2M_FMT •	
DMZ IP Paratheough	Server R/Port	792.586.1.2	4000
Triggered Caption Partial	Hean-Beat Content		
Section Appo	Heart-Seat Interval	3 (second)	
Dirar/NAU /Mar Bandwidth Limiter VIIII Static DHC?	Save - Cancel X		
53 Forward > © VPN Surved > Administration > © More Info			
tem	Instructions		
GPS Mode	Enable/Disable.		
GPS Format	NMEA and M2M_F	MT.	

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.

• Little		You haven't changed the default password for this router. To change router password size he
Overview		
Traffic Stats.	GPS Status	
GPS Status	Convert	OK .
Device List	Sottem Type	025
Basic Network	Satellites Nur	nbers 05 -
VILAN	Satellites Clov	180404 - 022121.00
	Positioning	2254.22520N - 11356.68170E
Advanced metwork	Google Map	View
E trevel		
VPN Tunnel		
	5	

4.5 Firewall



4.5.1 IP/MAC/Port Filtering

This allows to intercept packages from router's WAN/Cellular interface to the internet. <u>Test case</u>:

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

A	On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy
Advanced Network	~	2	any/0	any/0		B		Drop
IP/URL Filtering	~	17	any/0	192.168.1.0/24	ø	5	a .	Accept
Domain Filtering	~	50:78:90:C3:9A:22	any/0	any/0	s	3 0		Accept
VPN Tunnel	4	60:F1:89:20:F0:9A	any/0	any/0	<i>.</i> :	5	1	Accept
R Administration					NONE •			Accept

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.

D Firewall	~	URL Fil	tering	
IP/URL Filtering		On	URL	
Domain Filtering		~	voutube.com	
VPN Tunnel	*		freebook.com	
R Administration	•	~	lacebook.com	
		Image: A state of the state		
		Addt	1	
		Addit		

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.

				С	M510Q-W R	outer User Manua	
Status	•	1	youtube				
Basic Network	•	-	facebook				
🕸 WLAN	*	2					
Advanced Network		Add+					
S Firewall IP/URL Filtering Domain Filtering		Access Filt	ering				
VPN Tunnel	•	On Src MAC	Src IP	Dst IP	Protocol Sro	Port Dst Port	Policy Description
		1.1	any/0	any/0	TCP -	7	Drop
Administration		 ✓ 00:1E:64 	DF:E8:46 any/0	any/0	TCP .	22	Accept
		 ✓ 60:F1:89 	20:F0:9A any/0	any/0	TCP -	67	Accept
					NOT *		Acce *
		Add+					
		Save-	Cancel ×				
More Info		-		1225			

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

O Prote Mathematic			Already changed login passwo	nd successfully.
	LAN			
Cellular	Bridge A	IP Address	Subnet Mask	DHCP Server
LAN	hr0	192168101	255 255 255 0	4
VLAN			2572572575	~
DDNS	1	•		
Routing				
🗟 WLAN 🔸	Add+			

1.2) Navigate to VPN Tunnel > GRE

	Advanced Network	•	GRE T	unnel								
8	Firewall		On	Idx 🔿		Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval		Retries
•	VPN Tunnel	•	~	1]	192.168.10.10	113.113.11.11	113,113,10,10	×	10		5
	GRE		Add	i+								
	OpenVPN Client PPTP Server											
	PPTP Online PPTP/L2TP Client		GRE R	oute								
	IPSec		On		Tunnel Index 🦒		Destination Address				Description	
₹	Administration	•			1		▼ 192.172.1.0/24					
			Add	i+								
		[Save√	Canci	el×							

2) CM510Q-W(B) Configuration

2.1) Navigate to Basic Network > LAN

Basic Network *	LAN				
WAN		Bridge 🔨	IP Address	Subnet Mask	DHCP Server
Cellular		br0	192.172.1.1	255,255,255.0	~
VIAN					
Schedule	1		•		
DDNS					
Routing	Add+				
🕆 WLAN					

2.2) Navigate to VPN Tunnel > GRE

6	Advanced Network	GRE Tunnel						
8	Firewall	On Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries
	VPN Tunnel	1	192.172.1.10	113.113.10.10	113.113.11.11	~	10	5
1	GRE OpenVPN Client	Add+						
	PPTP Server							
	PPTP Online PPTP/L2TP Client	GRE Route						
	IPSec	On	Tunnel Index 🔨	Destination Addr	ess		Description	
7	Administration		1	▼ 192.168.10.0/24				
		Add+						

4.6.2 Open VPN



OpenVPN between CM510Q-W Client and Server

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

Status >	Basic Advanced Keys Status	
Basic Network >	VPN Client #1 (Stopped)	
🗣 WLAN 🔷 👌	vera cheric et (stoppes)	
Advanced Network	Start with WAN	×
🕄 Firewall 🔹 🔸	Interface Type	TUN 🔻
🕄 VPN Tunnel 🛛 👻	Prótocol	UDP V
GRE		
OpenVPN Client	Server Address	comset.dyndns.org 1194
PPTP Server PPTP Online	Firewall	Automatic 🔻
PPTP/L2TP Client IPSec	Authorization Mode	TLS 🔻
R Administration	Username/Password Authentication	
	HMAC authorization	Disabled •
	Create NAT on tunnel	~
	Start Now	

Basic Settings:

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:

Status	•	Basic Advanced Keys Status			
Basic Network	•	VDN Client #1			
🕈 WLAN	•	VPIN Client #1 (Stopped)			
Advanced Network	•	Poli Interval	0 (in minutes, 0 to disable)		
🖾 Firewall	•	Redirect Internet traffic			
VPN Tunnel	۲	Accept DNS configuration	Disabled V		
GRE			Una Dažajula		
OpenVPN Client		Encryption cipher	Use Default		
PPTP Server PPTP Online		Compression	Adaptive 🔻		
PPTP/L2TP Client IPSec		TLS Renegotiation Time	-1 (in seconds, -1 for default)		
R Administration	•	Connection retry	30 (in seconds; -1 for infinite)		
		Verify server certificate (tis-remote)			
		Custom Configuration			
		Start Now			

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 time1 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

ø	Status	*	OpenVPN Client
۲	Basic Network		
Ŷ	WLAN	•	Client 1 Client 2
۲	Advanced Network	•	Basic Advanced Keys Status
8	Firewall	۲	VPN Client #1 (Stopped)
80	VPN Tunnel		
	GRE		For help generating keys, refer to the OpenVPN HOWTO.
	OpenVPN Client		Certificate Authority
	PPTP Server		
	PPTP Online		
	PPTP/L2TP Client		
	IPSec		Client Certificate
ѫ	Administration	*	
			Client Key
			Start Now

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

\$	WLAN	•	OpenVPN Client
	Advanced Network	٠	Client 1 Client 2
2	Firewall	•	Basic Advanced Keys Status
۵	VPN Tunnel		
	GRE		VPN Client #1 (Stopped)
	OpenVPN Client		"Flight is not supplier as status could not be could
	PPTP Server		chert is not running or status could not be read.
	PPTP Online		
	PPTP/L2TP Client		
	IPSec		Start Now
杘	Administration	•	
			Save ✓ Cancel ×

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		-
1zo-1.08-3.0.el2.dag.i386.rpm	21-Feb-2012 00:50	55K
1zo-1.08-3.0.rh7.dag.i386.rpm	21-Feb-2012 00:50	54K
1zo-1.08-3.0.rh8.dag.i386.rpm	21-Feb-2012 00:50	58K
2 lzo-1.08-4.0.rh9.rf.i386.rpm	21-Feb-2012 00:50	59K
2 lzo-1.08-4.1.el3.rf.i386.rpm	21-Feb-2012 00:50	58K
2 lzo-1.08-4.1.el3.rf.x86_64.rpm	21-Feb-2012 00:50	55K
1zo-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)

PENVPN	hoose Components Choose which features of OpenVPN 2.3.0-I001 you want to nstall.
Select the components to insta service if it is running. All DLLs	all/upgrade. Stop any OpenVPN processes or the OpenVPN 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 Opendencies (Advanced)
Space required: 4.4MB	Description Position your mouse over a component to see its description.
lsoft Install System v2.46-101	

PC > Newdisk (D:) > OpenVPN >							
Name	Date modified	Туре	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					
	2019-01-10 14:10	File folder					
sample-config	2019-01-10 11:41	File folder					
n icon.ico	2015-02-18 17:56	lcon	22 KB				
🚱 Uninstall.exe	2019-01-10 11:42	Application	117 KB				

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

U

^		-	U_
lame	Date modified	lype	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.

5. Client certificate (5. Chefit Certificate (Generated on the server)							
Name	Date modified	Туре	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					

3. Client certificate (Generated on the server)

4. OpenVPN>easy-rsa>keys



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

NAN Participation WAN Participation Advanced Memory Participation Prevail Control for thicker and the system Prevail Control for thicker and the system Main Prevail Control for thicker and the system Control for thicker and the system Main Prevail Control for thicker and the system Control for thicker and the system Control for thicker and the system Main Prevail Control for thicker and the system Control for thicker and the system Control for thicker and the system Main Prevail Control for thicker and the system Main Control for thicker and the system Main Control for thicker and the system Control for thicker and the system Control for thicker and the system Control for thicker and t		152				
WAM > Advanced behaved. > Advanced behaved. > Deficience fait of Thy April 114422 2018. > Convert at of Thy April 114422 2018. > Marco of the optic at the of Thy April 114422 2018. > Marco of the optic at the of Thy April 114422 2018. > Marco of the optic at the of Thy April 114422 2018. > Marco of the optic at the of Thy April 114422 2018. > Marco of the optic at the of Thy April 114422 2018. > Marco of the optic at the of the optic at the of the optic at the optic a	Burge Party of the	10	Balt Advised Keys	Satu		
• Advenced betweek VPA Client #1 (Numma) • Reveal • Inse Deta current as of Thu Apr 4 11/34/22 2018 • Reveal • Inse Servers Statistics • Reveal	T. WLAN	12 - C				
Parend	Advanced Network	0	VPN Client #1 (Running)			
General Statistics Composition Series Statistics Value Annowalization Name 0 0 TUV/TAP werk Sprint(c) TUV/TAP werk Sprint(c) 0 0 Print, Statistics TUV/TAP werk Sprint(c) 0 0 Print, Statistics TUV/TAP werk Sprint(c) 0 0 Print, Statistics TUV/TAP werk Sprint C: VUberro/Roothping 10, 8, 0, 1 Print, Tights resourced. 0 TUV/TAP werk Sprint C: VUberro/Roothping 10, 8, 0, 1 Print, Tights resourced. 0 0 TUV/TAP werk Sprint Print, Trans, 10, 8, 0, 1: Vytess 23; tiges=10mg TTL=63 95331 46 Non-Network Print, Trans, 10, 8, 0, 1: Vytess 23; tiges=10mg TTL=63 0 0 Print, Trans, 10, 8, 0, 1: Vytess 23; tiges=10mg TTL=63 0 0 0 Print, Trans, 10, 8, 0, 1: Vytess 23; tiges=10mg TTL=63 0 0 0 Print, Tur, 10, 8, 0, 1: Vytess 23; tiges=10mg TTL=63 0 0 0 Print, Tur, 10, 8, 0, 1: Vytess 23; tiges=10mg TTL=63 0 0 0 0 Print, Tura, 10, 8, 0, 1: Vytess 23; tiges=10mg TTL=63 </td <td>C Frend</td> <td>22</td> <td>Deta current as of Thu Apr 4 113</td> <td>422.2018</td> <td></td> <td></td>	C Frend	22	Deta current as of Thu Apr 4 113	422.2018		
Kall Name Value Generative Command Prompt	A Stational		General Statistics			
TUVCTAP each bytel TUVCTAP each bytel 0 Operative State TUVCTAP each bytel 0 PTID_III (Same) Print (Same) 0 PTID_III (Same) Print (Same) 0 PTID_III (Same) Print (Same) 0 Print (Same) <			Name		Whe	
TWUTAP white hyte: (c) 2017 Microsoft Corporation. All rights reserved. 0 Wine: TCRUDP and hytes. C:\Users\Root\ping 10, 8, 0, 1 748 R Advectations TCRUDP and hytes. C:\Users\Root\ping 10, 8, 0, 1 748 R Advectations Pinging 10, 8, 0, 1 with S2 bytes of data: 5533 COUCH wite opts: Pinging 10, 8, 0, 1: bytes 32; time=10ms TTL=63 46 Autread hyte: Pinging 10, 8, 0, 1: bytes 32; time=10ms TTL=63 46 pat-conversi byte: Ping statistics for 10, 8, 0, 1: bytes 32; time=10ms TTL=63 0 perf-conversi byte: Ping statistics for 10, 8, 0, 1: bytes 32; time=10ms TTL=63 0 perf-conversi byte: Ping statistics for 10, 8, 0, 1: bytes 32; time=10ms TTL=63 0 perf-conversi byte: Ping statistics for 10, 8, 0, 1: bytes 32; time=10ms TTL=63 0 perf-conversi byte: Ping statistics for 10, 8, 0, 1: bytes 32; time=10ms TTL=63 0 perf-conversi byte: Ping statistics for 10, 8, 0, 1: bytes 32; time=10ms TTL=63 0 perf-conversi byte: Ping statistics for 10, 8, 0, 1: bytes 32; time=10ms TTL=63 0 perf-conversi byte: Ping statistics for 10, 8, 0, 1: bytes 32; time=10ms TTL=63 0 perf-conversi byte: Pi	OpenVTN Clevel		TUN/TAP read bytes	🗰 Command Prompt - D X	0	
Prime TCR/UDP read hypes C:\UDerrs\Root.ping 10, 8, 0, 1 T148 R Advectations Yinging 10, 8, 0, 1 with 92 bytes of data: 5333 YOMOP wite optes Pinging 10, 8, 0, 1 with 92 bytes of data: 5333 Autread hytes Pinging 10, 8, 0, 1 with 92 bytes of data: 5333 Autread hytes Pinging 10, 8, 0, 1: bytes 93; time=70 mg TTL=63 46 Autread hytes Rophy from 10, 8, 0, 1: bytes 93; time=70 mg TTL=63 0 pet-congress bytes Rophy from 10, 8, 0, 1: bytes 93; time=70 mg TTL=63 0 pet-congress bytes Ping statistics for 10, 8, 0, 1: 0 pet-congress bytes Ping statistics for 10, 8, 0, 1: 0 pet-congress bytes Ping statistics for 10, 8, 0, 1: 0 pet-congress bytes Ping statistics for 10, 8, 0, 1: 0 interame Ping statistics for 10, 8, 0, 1: 0 interame Ping statistics for 10, 8, 0, 0; 0 interame Ping statistics for 10, 8, 0, 0; 0 interame Ping statistics for 10, 8, 0; 0 interame Ping statistics for 10, 8, 0; 0 <	PPIPALITY Client		TURUTAR write bytes	(c) 2017 Microsoft Corporation. All rights reserved.	0	
Administration 10/A/OP write optes Pinging 10, 8, 0, 1 with S2 bytes of data: \$333 Autremed bytes Supty from 10, 8, 0, 1; bytes S2 time=15ms TTL=6.5 #46 Autremed bytes Supty from 10, 8, 0, 1; bytes S2 time=15ms TTL=6.5 #46 pst-concernent bytes Supty from 10, 8, 0, 1; bytes S2 time=16ms TTL=6.5 #6 pst-concernent bytes Supty from 10, 8, 0, 1; bytes S2 time=16ms TTL=6.5 #6 pst-concernent bytes Ping statistics for 10, 8, 0, 1; bytes S2 time=16ms TTL=6.5 0 pst-concernent bytes Ping statistics for 10, 8, 0, 1; bytes S2 time=16ms TTL=6.5 0 pst-concernent bytes Ping statistics for 10, 8, 0, 1; bytes S2 time=16ms TTL=6.5 0 pst-concernent bytes Ping statistics for 10, 8, 0, 1; bytes S2 time=16ms 0 pst-concernent bytes Ping statistics for 10, 8, 0, 1; bytes S2 time=16ms 0 pst-concernent bytes Ping statistics for 10, 8, 0, 1; bytes S2 time=15ms 0	and the second s		TCF/UDP read bytes	C:\Uperr\Root)ping 10.8.0,1	7168	
Reply from 10.8.0.1: bytes 32 flass 15ms TTL=63 46 Autread bytes Reply from 10.8.0.1: bytes 32 flass 15ms TTL=63 46 pub-conversibytes Reply from 10.8.0.1: bytes 32 flass 15ms TTL=63 0 pub-conversibytes Reply from 10.8.0.1: bytes 32 flass 15ms TTL=63 0 pub-conversibytes Reply from 10.8.0.1: bytes 32 flass 15ms TTL=63 0 performent bytes Ping statistics for 10.8.0.1: bytes 32 flass 15ms 0 performent bytes Ping statistics for 10.8.0.1: bytes 32 flass 15ms 0 performent bytes Ping statistics for 10.8.0.1: bytes 32 flass 15ms 0 performent bytes Ping statistics for 10.8.0.1: bytes 32 flass 15ms 0 performent bytes Ping statistics for 10.8.0.1: bytes 32 flass 15ms 0 performent bytes Ping statistics for 10.8.0.1: bytes 32 flass 15ms 0	Administration		TCP/UDP write cyces	Pinging 10, 8, 0, 1 with 32 bytes of data: Reply from 10, 8, 0, 1; bytes=52 time=12m TL=63 Neelly from 10, 8, 0, 1; bytes=52 time=21m TL=63	9531	
Burght from 10, 2, 0, 1: bytes 32 time TDms TTL=63 0 performers bytes Reply from 10, 2, 0, 1: bytes 32 time thms TTL=63 0 performers bytes Ping statistics for 10, 2, 0, 1: Packets; Cent = 4, Needtwis = 4, Lost = 0 (ON loss), Approximate round trip times in milli-seconds: 0 performers bytes Approximate round trip times in milli-seconds: 0			Auth read bytes		45	
perf-compressibilities for 10.8.0.1: Packets; Cent = 4, Nacelved = 4, Lost = 0 (0N loss), pre-secongressibilities of Universe in milli-seconds: Approximate round trip times in milli-seconds: Discussion of the second of the			pré-compress bytes	Reply from 10.8.0.1: bytes=32 time=10mm TTL=63 Reply from 10.8.0.1: bytes=32 time=10mm TTL=63	a	
per-secondersingtes per-secondersingtes Approximate round trip times in milli-seconds: 0			post-compress bytes	Pirg statistics for 10.8.0.1: Packate: Sent = 4, Received = 4, Lost = 0 (ON 1000);	0	
Winterna = 100m, Hasiana = 20m, Average = 15m			pre-decompress bytes			
			cost decisioners in the	Minimum = 10mm, Maximum = 21mm, Average = 15mm		
C:\Usern\Booti_			Provident - 0,000 (0,00)	C:\Usere\Root>_	1 N	
And						Refeat Statu

4.6.3 L2TP/PPTP

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

Test case: PPTP

				CM	510Q-W Router	User Manual		
8	VPN Tunnel	~						
	GRE							
	OpenVPN Client	t						
	PPTP Server							
	PPTP Online							
	PPTP/L2TP Clier	ıt						
On	Protocol ^	Name	Server	Username	Password	Firewall	Default Route	Local IP
~	PPTP	3	comset.dyndns.org	test123	test123	~	×	
1	L2TP	•						
Adda								
AGG								

PPTP Advanced

On	Name ^	Accept DNS	MTU	MRU	MPPE	MPPE Stateful	Custom Options
~	3	NO	1440	1440	~	X	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	e Local IP
<i>v.</i>	PPTP	3	comset.dyndns.org	test123	test123	~	×	
✓ Add+	L2TP •							
PPTP Advanced	Name o	Accept DNS	мти	MRU	MPPE	мр	PE Stateful (ustom Options
<i></i>	3	NO	1440	1440	×.	×	6	lebug:noipdefault.requ nppe-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)

ļ

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

R

		CM510Q-W R	outer User Manual
Basic Network	•	IPSec	
🕈 WLAN	•	Group Setup Basic Setup Advanced Setup	
Advanced Network	•		
🔕 Firewall	•	Enable IPSec	
VPN Tunnel	*	IPSec Mode	Client 🔻
GRE OpenVPN Client		IPSec Extensions	Normal
PPTP Server		Local Security Gateway Interface	3G Cellular 🔻
PPTP/L2TP Client		Local Security Group Subnet/Netmask	192.168.1.0/24
IPSec			
R Administration	•	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	
		Save ✓ Cancel ×	

2.2) Navigate to VPN Tunnel > IPSec > Basic Setup

		CM510Q-W Router User Manual			
Status	•	IPSec1 IPSec2 Schedule			
Basic Network	•	Group Setup Basic Setup Advanced Setup			
🕏 WLAN		Keying Mode	IKE with Preshared Key 🔻		
Advanced Network	•	Record DH Cours	Group 2 - modp1024		
Firewall	1.	Phase I DH Group	Group 2 - moup1024		
VPN Tunnel	-	Phase 1 Encryption	3DES (168-bit)		
GRE		Phase 1 Authentication	MD5 HMAC (96-bit)		
OpenVPN Client PPTP Server		Dhase 1 CA Life Time	28800 seconds		
PPTP Online		Pridse I SA Life finite			
PPTP/L2TP Client		Phase 2 DH Group	Group 2 - modp1024 🔻		
Administration	э.	Phase 2 Encryption	3DES (168-bit)		
		Phase 2 Authentication	MD5 HMAC (96-bit)		
		Phase 2 SA Life Time	3600 seconds		
		Preshared Key			
		Save ✓ Cancel ×			

2.3) Navigate to VPN Tunnel > IPSec > Advanced Setup

 Status 	`	Group Setup 8asic Setup Advanced Setup		
Basic Network		Aggressive Mode		
Advanced Network		Compress(IP Payload Compression)		
🗃 Firewall		Dead Peer Detection(DPD)		
VPN Tunnel	*	ICMP Check		
GRE OpenVPN Client		Check Period Time Interval	3	seconds
PPTP Server PPTP Online		Check Timeout Count	3	Times
PPTP/L2TP Client IPSec		Check IP	10.10.0.1	
R Administration	•	IPSec Custom Options 1	rightid=%any	

2.4) Check Status of the VPN IPSec connection.



Status	*			
Overview		IPSec 1	Connected	
Traffic Stats		Phase 1 Status	21 seconds	
GPS Status		Phase 1 IKE	3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024	
Device List		Phase 2 Status	TUNNEL	
A	1	Phase 2 ESP	3DES_CBC/HMAC_SHA1_96	
Basic Network		IPSec Recv.	84 Bytes	
WLAN	•	IPSec Send.	84 Bytes	
Advanced Network	•	- Br		
🔀 Firewall	•	LAN	¢ ~	
VPN Tunnel	1	Router MAC Address	34:0A:94:01:51:01	
		Router IP Addresses	br0 (LAN) - 192.168.1.1/24	
R Administration	•	DHCP	br0 (LAN) - 192.168.1.2 - 192.168.1.51	

--End

IJ