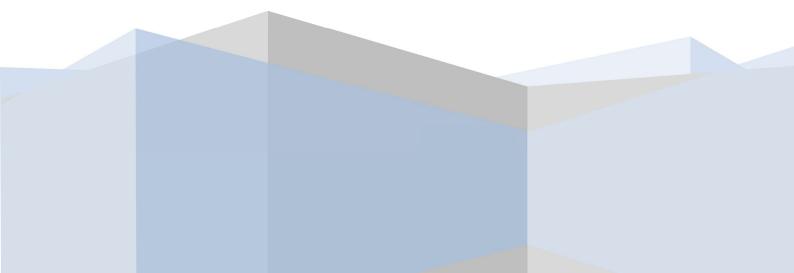




Comset CM550W-POE 5G Router User Guide





Copyright © COMSET 2022

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

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

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



Address:	37/ 125 Highbury Road, Burwood VIC 3125, Australia
Web:	http://www.comset.com.au
Phone:	+61 3 9001 9720
Fax:	+61 3 9888 7100



Contents

1 Hard	ware Installation	
1.1	1 Panel	3
1.2	2 LED Status	4
1.3	3 Dimensions	5
1.4	4 Powering up the CM550W-POE Router	5
2 Route	er Configuration	8
2.1	1 Configuration from a local network	8
2.2	2 Status	9
2.3	3 Tools Column	1
2.4	4 Basic Network1	4
2.5	5 WLAN Settings2	5
2.6	6 Advanced Network Settings2	8
2.7	7 Firewall3	9



	2.8 VPN Tunnel		41
	2.9 Administration		54
	2.10 "Reset" Button to	Restore Factory Settings	70
3 C	onfiguration Examples.		72
	3.1	VLAN	72
	3.2	WAN Backup (WAN as Main, Cellular as Backup)	74
	3.3	Port Forwarding	77
	3.4	IP Passthrough	80
	3.5	Captive Portal	82
	3.6	GPS Settings (GPS version only)	86
	3.7	Firewall	87
	3.8	VPN Tunnel	89



Hardware Installation

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

1.1 Panel

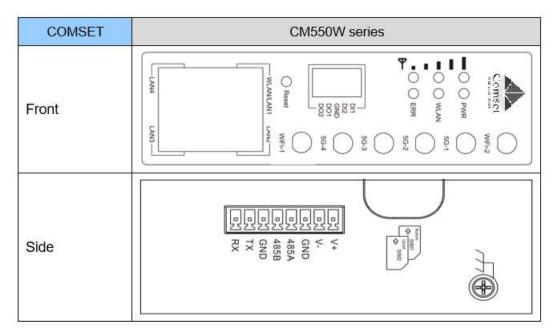


Table 1-1 CM550W-POE Interface

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



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

1.2 LED Status

Table 1-3 Router LED indicator Status

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



silk-screen	:	status	Description
	Green	Light off	Disconnected.

1.3 Dimensions

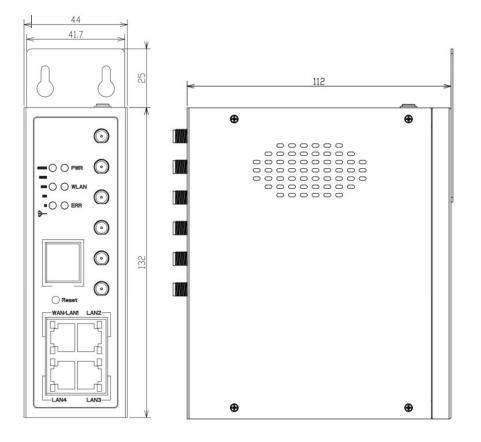


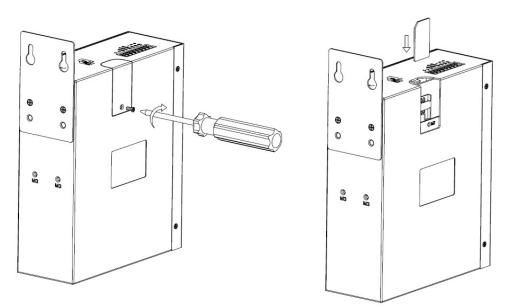
Figure 1-1 CM550W-POE Router Dimensions

1.4 Powering up the CM550W-POE Router

1.4.1 SIM/UIM card installation

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





O CAUTION

Before connecting any cables, please disconnect the power source.

1.4.2 Ethernet Cable Connection

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

1.4.3 5G and Wi-Fi Antenna Plug

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

NOTE NOTE

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

1.4.6 Power Supply

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





1.4.7 Review

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

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

Note:

- Step 1 Check the antennas' connection.
- Step 2 Check the SIM/UIM card is inserted.
- Step 3 Power up the CM550W-POE Router.





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

2.1 Configuration from a local network

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

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



Figure 2-1 Network Connection

- Step 2 Select "Obtain an IP address automatically" or set up a fixed IP address in the range 192.168.1.xxx (xxx can be any number between $2\sim$ 254)
- Step 3 Run Internet Explorer, or any other web browser, and enter 192.168.1.1 in the address bar and press "enter".

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





Figure 2-2 User Identify Interface

2.2 Status

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

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

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

Already changed login password successfully.

2.2.1 Overview

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



omset	omau	=						Tools 🛠	Bandwidth 🛩	IP Traffic 📶	System
Status Overview	~				Already o	hanged login	password successfully.				
Traffic Stats. Device List		System				~	LAN			۵	~
		Router Name	CM55				Router MAC Address	34:0A:19:22:00:41			
Basic Network		Hardware Version	C11-V				Router IP Addresses	br0 (LAN) - 192.168.1.1/24			
	•	Firmware Version	Gx.0.2				DHCP	br0 (LAN) - 192.168.1.2 - 192.16	8.1.51		
Advanced Network		Router Sn Router Time		55102109220017 01 Jan 2020 11:01:04 +1100							
8 Firewall	5	Uptime	00:01:				Wireless (5 GHz)			\$	~
D VPN Tunnel							MAC Address	34:0A:19:22:00:44			
		Ethernet Ports Status				~	Wireless Mode Wireless Network Mode	Access Point Auto			
Administration	•		1756				interface Status	Up			
		WAN/LAN1	LAN2	LAN3	LAN4		Radio	Enabled 🗸			
			1	F	1		SSID	Comset-Router-5G			
		UP	Unplugged	Unplugged	Unplugged		Broadcast	Enabled 🗸			
							Security	WPA(PSK) Personal + AES			
		VPN Status				¢ ~	Channel	36			
		No Active VPN					Channel Width	Auto			
		NO ACTIE VEN					Rate	867 Mbps			
omset	om.au	=						Tools 🛠	Bandwidth 🛩	IP Traffic 📶	Sys
omset vww.comset Status	om.au	≡ Internet				~		Tools 🛠	Bandwigth 🛩	IP Traffic 📶	Syst
Status Overview	om.au		Cellul	ar		~	Wireless (2.4 GHz)	Tools 🛠	Bandwidth 🛫	IP Traffic 🖷	Syste
D Status Overview Traffic Stats.	om.au	Internet		ar 5.95.176		×	Wireless (2.4 GHz)		Bandwidth 🛩		
www.comself Www.comself Status Overview Traffic Stats. Device List	om.au	Internet Connection Type	10.21			v	MAC Address	3404:192200:43	Bandwidth 🛫		
Status Overview Traffic Stats. Device List Basic Network	om.au	Internet Connection Type IP Address Subnet Mask Gateway	10.21 255.2 10.21	5.95.176 55.255.224 5.95.177		×			Bandwidth 🛃		
Status Overview Traffic Stats. Device List Basic Network	om.au	Internet Connection Type IP Address Subnet Mask Gateway DNS	10.21 255.2 10.21 10.1	5.95.176 55.255.224 5.95.177 68.244.100:53, 10.4.58.204:53		~	MAC Address Wireless Mode	3404:19220043 Access Point	Bandwidth 🛫		
D Status Overview Traffic Stats.		Internet Connection Type IP Address Subnet Mask Gateway DNS Connection Status	10.21 255.2 10.21 101.1 101.1	5.95.176 55.255.224 5.95.177 68.244.100:53, 10.4.58.204:53 ected		~	MAC Address Wireless Mode Wireless Network Mode	340x19220043 Access Point Auto	Bandwidth 🛫		
Status Overview Traffic Stats. Device List Basic Network WLAN Advanced Network	> >	Internet Connection Type IP Address Subnet Mask Gateway DNS	10.21 255.2 10.21 10.1	5.95.176 55.255.224 5.95.177 68.244.100:53, 10.4.58.204:53 ected		v	MAC Address Wireless Mode Vireless Network Mode Interface Status Radio SSID	3404/19220043 Access Point Auto Up Enabled ~ Conset-Router-24G	Bandwidth 🛩		
Status Overview Traffic Stats. Device List Basic Network WLAN Advanced Network Ifrewall	> > >	Internet Connecision Type III Address Subort Mask Gatewy DNS Connecision Status Connecision Uptime	10.21 255.2 10.21 101.1 101.1 Conne	5.95.176 55.255.224 5.95.177 68.244.100:53, 10.4.58.204:53 ected			MAC Address Wireless Mode Wireless Network Mode Interface Status Radio SSID Broadcast	340A/19220043 Access Point Auto Up Enabled ✓ Conset Router 2.4G Enabled ✓	Bandwidth 🛫		
Status Overview Traffic State. Device List Basic Network VUAN Advanced Network Firewall Firewall VVN Tunnel	> > >	Internet Connection Type IP Address Subnet Mask Gatewy DNS Connection Status Connection Status Connection Uptime	10.21 255.2 10.21 101.1 Conn 00:01	5.95.176 55.255.224 5.95.177 68.244.100:53, 10.4.58.204:53 ected 35		~ ¢ ~	MAC Address Wireless Mode Wireless Network Mode Interface Status Radio SSID Biroadast Security	340A;19220043 Access Point Aato Ug Enabled → Conset Roster 2.46 Enabled → WRM559 resonal + AES	Bandwidth 🛩		
Status Overview Traffic State. Device List Basic Network VAN Advanced Network Finewall Finewall VNN Tunnel	> > >	Internet Connection Type # Address Safort Mask Gatewy DVS Connection Staffs Connection Uptime Cellular Connection Type	10.21 255.2 10.21 101.1 Comm 00:01	5.95.176 55.255.224 68.244.100/53, 10.4.58.204/53 68.244.100/53, 10.4.58.204/53 35 QMI			MAC Address Wireless Mode Wireless Network Mode Interface Status Radio SSID Broadcast	340x192200x3 Access Point Auto Up Enabled Jr Const4 Router24G Enabled Jr WRA(PSIQ Personal + AES 1	Bandwidth <u>e</u>		
Status Overview Traffic State. Device List Basic Network VAN Advanced Network Finewall Finewall VNN Tunnel	> > >	Internet Connection Type # Address Subert Mask Gateway DVS Connection Status Connection Status Connection Status Connection Type Modern Mel	10.21 255.2 10.21 101.1 Conn 0001 ECM/ 86715	5.95.176 55.255.224 5.85.177 ected 35 CQMI 17050120712			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Bandwidh 🗹		
Status Overview Traffic State. Device List Basic Network VUAN Advanced Network Firewall Firewall VVN Tunnel	> > >	Internet Connection Type # Address Sadar Mask Gateway DNS Connection Status Connection Status Connection Uptime Cellular Connection Type Modem ME	10.21 235.2 10.21 101.1 Comm 00001 ECM// 86716 Ready	5.95.176 55.255.277 5.95.177 6.86.244.100.53, 10.4.58.204.53 ected 35 °CMII 197050120712 Y			MAC Address Wireless Mode Wireless Notwick Mode Interface Status Radio SSID Broadcast Security Channel	340x192200x3 Access Point Auto Up Enabled Jr Const4 Router24G Enabled Jr WRA(PSIQ Personal + AES 1	Eandwidth 🛫		
Status Overview Traffic State. Device List Basic Network VAN Advanced Network Finewall Finewall VNN Tunnel	> > >	Internet Connection Type # Address Sacher Mask Gatewy DNS Connection Uptime Connection Uptime Cellular Connection Type Modem ME Modem Status Cellular SP	10.21 255.2 102.1 101.1 00.01 00.01 00.01 ECM/ 86.7 8.6 Radg "Tebb	5.95.176 55.955.224 59.51.77 62.841.00:53, 10.4.58.20:653 eeted 35 700:51.20712 y extessions Teistra"			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Bandwidh 🛫		
Status Overview Traffic State. Device List Basic Network VAN Advanced Network Finewall Finewall VNN Tunnel	> > >	Internet Connection Type IP Address Subnet Mask Gatewy DNS Connection Status Connection Status Connection Uptime Cellular Cellular Cellular Modem MB Modem Status Cellular SP Cellular SP	1021 255,2 1021 101,1 0001 6001 8675 868 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 867555 867555 8675555 867555 867555 86755555 8	505.176 53.352.24 55.377 68.244.100.53, 10.4.56.204.53 ected 35 CMII 170501.20712 Y rs #n.445Vacx Telstra* TraMLNR0			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Bandwidth <u>e</u>		
Status Overview Traffic State. Device List Basic Network VUAN Advanced Network Firewall Firewall VVN Tunnel	> > >	Internet Connection Type IP Address Sahert Mask Gatewy DVS Connection Status Connection Status Connection Type Modern Mil Modern Status Cellular Network USM Selected	10.21 25.2 101.1 00.0 00001 ECM/10 867/11 863/ 7 Read 50(BL) USM	598.176 592.352.224 692.241.005.3, 104.592.0453 extend 393 COM 70500120712 y ra # tetisous Tetatra" TIRAN_MB) Cut 1 Jaming			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Bandwidth 🛫		
Vournauer WWY20msete Vournauer Vournauer	> > >	Internet Connection Type IP Address Subnet Mask Gatewy DNS Connection Status Connection Status Connection Uptime Cellular Cellular Cellular Modem MB Modem Status Cellular SP Cellular SP	1021 255,2 1021 101,1 0001 6001 8675 868 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 86755 8685 867555 867555 8675555 867555 867555 86755555 8	593.176 93.235.232 93.235.232 93.244.1005.31.104.582.044.93 94.244.1005.31.104.582.044.93 97590120712 77590120712 777904.194 77894.194 7784.1			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Bandwidth 🖉		
Status Overview Traffic State. Device List Basic Network VUAN Advanced Network Firewall Firewall VVN Tunnel	> > >	Internet Connection Type IP Address Subert Mask Gateway DMS Connection Status Connection Uptime Connection Uptime Connection Type Modern Status Cellular Fib Cellular Fib Cellular Fib Cellular Fib Cellular Fib Cellular Siba	10.21 25.2 10.2 10.1 101.1 0001 0001 8071 8045 8071 8045 804 901 001 804 001 804 001 001 804 001 001 804 001 001 804 001 804 001 804 001 804 804 804 804 804 804 804 804 804 804	593.176 93.235.232 93.235.232 93.244.1005.31.104.582.044.93 94.244.1005.31.104.582.044.93 97590120712 77590120712 777904.194 77894.194 7784.1			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Bandwidth 🦟		
Status Overview Traffic State. Device List Basic Network VAN Advanced Network Finewall Finewall VNN Tunnel	> > >	Internet Connection Type IP Address Subnet Mask Gateway DNS Connection Status Connection Status Connection Status Connection Type Modern MD Modern Status Cellular Meteorot USM Status Cellular Meteorot USM Status Cellus Mathematica Cellus Meteorot	10.21 25.2 10.21 101.1 Comm 00:01 867.43 868.43 7 Telsk 5068 87.46 88.43 2.2 2.2 10.21	593.176 593.373.24 692.241.1005.31, 104.542.045.31 692.241.1005.31, 104.542.045.31 693.64 70700.1027172 Y Y Y Y Y Y Y Card I Fouring Y			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Eandwidth 🛫		
Status Overview Traffic State. Device List Basic Network VUAN Advanced Network Firewall Firewall VVN Tunnel	> > >	Internet Condition Type IP Address Subnit Mask Gatewy DVS Connection Status Connection Status Connection Uptime Cellular Cellular Connection Type Modern MB Connection Type Modern MB Caluar ISP Cellular ISP Cellular ISP Cellular ISP Cellular ISP Cellular Status Celluar Status Celluar Status Celluar Status	10.21 25.2 101.1 101.1 Comm 86715 Ready 70685 70685 22	593.176 593.252.24 693.241.005.31, 164.582.0453 extend 004 70500120712 y ra meterixan Telatrar mrank.y46) cut 1 hanning y 5,53.176			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Bandwidth 🗹		
Status Overview Traffic State. Device List Basic Network VAN Advanced Network Finewall Finewall VNN Tunnel	> > >	Internet Connection Type IP Address Subert Mask Gateway Diris Connection Uptime Connection Uptime Connection Type Modern Mati Modern Status Cellular Fib Cellular Fib Cellular Fib Cellular Fib Cellular Fib Cellular Status Cellular Status Cellular Status Cellular Status Cellular Status Cellular Status Cellular Ketorot.	1021 252 202 101.1 00.0 0001 887/1 Read 0587/1 Read 0587/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 1021 1021 1021 1021 1021 1021 1021 10	593.176 93.235.234 93.235.234 93.241.005.31, 10.4.582.0453 93. CMM 97690.102712 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Bandwidth 🛫		
Status Overview Traffic State. Device List Basic Network VUAN Advanced Network Firewall Firewall VVN Tunnel	> > >	Internet Control Type P Address Safar Mask Gatewy DHS Control Type Control Type Mode my Mode my Cellular Control Type Mode my Mode my Safar Cellular EP Cellular Harot Cellular EP Cellular Herot USM Status Cellur Herot	1021 252 202 101.1 00.0 0001 887/1 Read 0587/1 Read 0587/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 887/1 1021 1021 1021 1021 1021 1021 1021 10	593.75 592.352.254 592.352.254 593.257 593.254 593.77 794.244.1005 795.912.0712 77 775.912.0712 77 775.912.0712 775.9170 593.177 593.177 593.177			MAC Address Wireless Mode Wireless Notoe Metrace Status Radio SSID Eroadcast Scorrby Channel Vichth	3404/19/220043 Access Point Auto Up Enabled J Conset Roster 2.46 Enabled J WRM/SIQ Personal + AES 1 Auto	Eandwidth 🛫		

Figure 2-3 Router Status GUI

2.2.2 Traffic Statistics.

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

Status	*		Already changed login password su	iccess
Overview				
Traffic Stats.		Traffic Stats.		
Device List		Interface	Transmit Data	
Basic Network	*	Cellular(usb0)	1.45 MB	
ବି WLAN	•	Celidial (usbo)	סייו 1.43	
Advanced Network	•			
🕄 Firewall	•			
D VPN Tunnel	•			
R Administration	•			



2.2.3 Device List

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



۲	Status	~			Alroadure	hanged login	password suc	cossfully			
	Overview				Alleddy C	and ged login	password succ	essiuny.			
	Traffic Stats.		Device Lis	t							
	Device List										
0	Basic Network	>	Interface	MAC Address	IP Address	Name	RSSI	Quality	TX/RX Rate	Lease	
\$	WLAN	•	br0	54:E1:AD:C3:99:8B	192.168.1.2			Ā			
۲	Advanced Network	•									14
2	Firewall	•							~	3 seconds	* Stop ×
0	VPN Tunnel	•									
ж	Administration										



2.3 Tools Column

Comset	et com au	≡		*	~	<u>#</u>	۵
Status	*		Already changed logir	n password successfull	y.		i
Overview Traffic Stats. Device List		System Router Name	Comse	t Router			×
Tools 🛠	Bar	ndwidth 👱	IP Traffic 🔳	System 🏚			

Figure 2-6 Tool Column GUI

2.3.2 Tools

2.3.2.1 Ping

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



ing					
P Address	8.8.8.8		Ping		
Ping Count	5				
Packet Size	56	(bytes)			

2.3.2.2 Trace

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

ace Route					
P Address			Trace		
Maximum Hops	20				
Maximum Wait Time	3	(seconds per hop)			

2.3.2.3 WOL

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

	🖿 Log 🛛 🔒 Capture		
Wake On Lan			
MAC Address	IP Address	Status	Name 🔨
54:E1:AD:C3:99:8B	192.168.1.2	Active (In ARP)	
Click to wake up MAC Address List			
Wake Up 🔺			Refresh C



2.3.2.4 Log

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

Logs View Download Log File			
View			
Download Log File			
	FindQ		

2.3.2.5 Capture

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

💣 Ping 🗥 Trace 🖽 W	OL Log Capture	
Capture		
Time1	15 minutes 🔻 Start	
Network	LAN •	

2.3.3 Bandwidth

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





eal Time Bandwi	idth 🤇							
Cellular (usb0)	LAN (br0)	LAN (eth0)	LAN (vlan1)	WAN (vlan2)	Wi-Fi/2.4G (eth1)	Wi-Fi/5G (eth2)		
						Mor	1 05:03 pm / 12942.27 mbit/s (161	7.78 MB/s
n 12885.00 mbit/s	(1610.63 MB/s)							
 12885.00 mbit/s 8590.00 mbit/s (4295.00 mbit/s (1073.75 MB/s)				Π			
4295.00 mbit/s (536.88 MB/s)							
0 minute windov 14.24 kbit (1.74 KB/s	/s	erval)	Avg 114.54 (13.65		Peak	17179.21 mbit/s (2047.92 MB/s)	Total	8,192. MB
x + 10.85 kbit			Avg (13.65	mbit/s	Peak	17179.39 mbit/s (2047.94 MB/s)	Total	8,192. MB

2.3.4 System

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

Tools 🛠	Bandwidth 👱	IP Traffic 💻	System 🌣
Reboot 🇘	Hardware Reboot	Ċ	

2.4 Basic Network

2.4.1 WAN Settings

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

cialist			Comset CM550W-POE 5G Router User
Status	•		Already changed login password successful
Basic Network WAN	*	WAN / Internet	
Cellular		Туре	Disabled •
LAN VLAN			Disabled DHCP
Schedule		Save ✓ Cancel×	PPPoE Static Address
DDNS			
Routing			
ি ₩LAN			
Advanced Network			
Tirewall	•		
VPN Tunnel	2		
R Administration			

Table 2-1 WAN Settings Instructions

Parameter	Instructions
Туре	Supports DHCP, PPPoE, Static IP address

Click "Save" to finish. The router will reboot.

2.4.2 Cellular Settings

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



WAN Cellular LAN VLAN Schedule DDNS Routing				
WAN Cellular LAN VLAN Schedule DDNS Routing VLAN Cellular Traffic Check DNS Routing VLAN Advanced Network SMS Code VPN Tunnel Operator Lock Fail Over Fail Over SIM 1 Only	Basic Network	*	Basic Settings SIM 1 SIM 2	
LAN VLAN Schedule DDNS Routing VLAN	WAN		Dasic Seturgs Silver a Silver 2	
VLAN ICMP Check Schedule Cellular Traffic Check DDNS MTU Routing MTU Advanced Network CIMI Send to Firewall SMS Code VPN Tunnel Operator Lock DualSim Mode Fail Over Fail Over SIM 1 Only	Cellular		Use PPP	
Schedule DDNS Routing VLAN Advanced Network Advanced Network Firewall SMS Code Operator Lock Pail Over Fail Over SIM 1 Only	LAN			
DDNS Routing VLAN Advanced Network Advanced Network CIMI Send to SMS Code VPN Tunnel Operator Lock Eatlover Fail Over SIMS Code	VLAN		ICMP Check	
DDNS Routing WLAN Advanced Network Advanced Network CIMI Send to SMS Code VPN Tunnel Operator Lock DualSim Mode Fail Over Fail Over SIM 1 Only	Schedule			
WLAN Advanced Network Advanced Network Friewall VPN Tunnel Overator Lock Operator Lock Example Fail Over Fail Over SIM 1 Only	DDNS		Cellular Traffic Check	
 WLAN Advanced Network Advanced Network CIMI Send to SMS Code Operator Lock DualSim Mode Fail Over Fail Over SIM 1 Only 	Routing			0
Advanced Network > S Firewall > D VPN Tunnel > Operator Lock ecc46001 DualSim Mode Fail Over Fail Over SIM 1 Only	ବି WLAN	->	міо	(0 for default)
D VPN Tunnel Operator Lock Exc46001 DualSim Mode Fail Over Fail Over SIM 1 Only	Advanced Network		CIMI Send to	:
Administration DualSim Mode Fail Over Fail Over	8 Firewall	>	SMS Code	
Administration DualSim Mode Fail Over Fail Over SIM 1 Only	VPN Tunnel		Operator Lock	ev:46001
DualSim Mode Fail Over Fail Over Fail Over Sill 1 Only Sill 1 Only		15	Operator Lock	
Sill 1 Only	n Administration		DualSim Mode	Fail Over 🗸
Sava de Cancel d				Fail Over
Save Cancel X SIM 2 Only				SIM 1 Only
Silvi 2 Olity			Save Cancel ×	SIM 2 Only
D More Info				Backup

Basic Settings SIM 1 SIM 2	
SIM 1 Mode	Auto 🗸
SIM 1 5G Mode	SA & NSA 🗸
SIM 1 PIN Code	
SIM 1 APN	telstra.internet
SIM 1 User	
SIM 1 Password	
SIM 1 Dial Number	*99#
SIM 1 Auth Type	Auto 🗸
SIM 1 Local IP Address	
Save√ Cancel ×	



Table 2-2 Cellular Settings Instructions

Item	Description
Enable Modem	Enable/Disable 5G modem.
Use PPP	ECM dial-up as default. PPP optional.
ICMP check	To enable or disable "ICMP check" rules. Enable the ICMP check and setup a reachable IP address as a destination IP. When "ICMP check" fails, the router will reconnect/reboot.
Cellular Traffic Check	The router will reconnect/reboot if there is no Rx/Tx traffic.
CIMI Send to	Send CIMI to a defined IP address and port by TCP protocol.
SMS Code	Remote control the router by SMS. Only the configured SMS code will work.
Operator Lock	Lock the router to a specific carrier by MCC/MNC code.
Dual SIM Mode	<u>Fail Over:</u> When SIM 1 fails, the router will switch to SIM 2. When SIM 2 fails, the router will switch back to SIM 1.
	<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 of time, at the end of which it will switch back to SIM 1.
SIM Mode	<u>Auto:</u> The router will connect automatically to 3G, 4G or 5G, with priority given to 5G.
	5G NR: Router will only connect to 5G.
	LTE: Router will only connect to 4G.
	<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.



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

NOTE ICMP Check and Cellular Traffic Check are alternative.

[ICMP Check]

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

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

Check IP	8.8.8.8	
Check IP (Optional)	4.4.4.4	
Interval	60	(seconds)
Retries	3	(Times)
Fail Action	Reboo	t System 🔻

【Cellular Traffic Check】

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

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



Cellular Traffic Check	~	
Check Mode	Rx v	
Check Interval	10	(minutes)Range: 1 ~ 1440
Fail Action	Cellular Reco	nnect 🔻

Step 1 To save the settings, click the "save" button.

2.4.3 LAN Settings

Step 1 Go to Basic Network>LAN

Status	2		Already	changed login passw	ord successfully.		
Basic Network	*	LAN					~
WAN							
Cellular LAN		Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
VLAN		br0	192.168.1.1	255.255.255.0	~	192.168.1.2 - 51	1440
Schedule							
DDNS		1 *					
Routing							
WLAN	•	Add +					
Advanced Network	. . .	Save√ Cancel×					
🔞 Firewall	•						
VPN Tunnel	•						
R Administration	•						
 More Info 							
LAN							~
Bridge 4	^	IP Address	Subnet Mask	DHCP Se	rver	IP Pool	Lease(minutes)
br0		192.168.1.1	255.255.255.0	~		192.168.1.2 - 51	1440
1	v						
Add+							



	-
Item	Description
Bridge	Supports four LAN IP addresses from br0 to br3. If VLAN is required, please go to the VLAN page.
Router IP Address	Router IP address. Default IP is 192.168.1.1
Subnet Mask	Router subnet mask. Default mask is 255.255.255.0
DHCP	Dynamic allocation IP service. When enabled, it will show the IP address range and lease option.
IP Pool	IP address range within the LAN.
Lease	The valid time in minutes.
Add	Add a LAN IP address. Supports four LAN IP addresses.

Table 2-3 LAN Settings Instructions

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

2.4.4 VLAN Settings

Step 1 Go to Basic Network >VLAN.

Basic Network	- 🗢											
WAN		VLAN										
Cellular		VID	^	WAN/LAN1	Tagged	LAN2	Tagged	LAN3	Tagged	LAN4	Tagged	Bridge
LAN		1		1	×	4	×	4	×	~	×	br0
VLAN					24	×	0	Ť	0		0	
Schedule		2		×	×	×	×	×	×	×	×	WAN
DDNS		3			11							none
Routing		2										none
ଟି WLAN	•	Add +										
Advanced Network	•	_										
🐼 Firewall		Save-	Cancel×									

Table	2-4	VLA	N S	Settings
1 0 0 10				Journa of the second se

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

Step 2 Click on "Save" to finish.



2.4.5 Schedule

Step 1 Go to Basic Network >Schedule.

Comset	om.au	≡ 5% ~ ≝ 3	¢
Status	>	Already changed login password successfully.	
Basic Network WAN		Enabled Links Link Name Link Type Description	~
Cellular LAN VLAN		modem ECM/QMI	
Schedule DDNS Routing		ICMP Check On Link Destination Interval Retries Description	~
중 WLAN ✿ Advanced Network	> >	Link Destination interval Retries Description	
Ser Advanced Network	>	Add+	
VPN Tunnel	*		
R Administration	•	Schedule On Link 1 Link 2 Policy Description Image: modem modem FAILOVER Image: modem Add+ Save Cancel ×	

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



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

Link Name			Link Type				Description		
modem			ECM/QMI						
wan			WAN(STATIC)					
CMP Cheo	ck								
On Link	k	Destina	tion	h	iterval	Re	etries	Description	
✓ wan		8.8.8.8		1	D	5			
~									
Add +									,
On	Link 1	Lin	k 2		Policy		Description		
~	wan	v m	odem	ж	FAILOVER		wan as primary and	modem as secondary	
Add +									



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

Status	•						Already	Already changed log	Already changed login password	Already changed login password successful	Already changed login password successfully.	Already changed login password successfully.	Already changed login password successfully.	Already changed login password successfully.
Basic Network														
WAN		VLA	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN
Cellular		Į.	VID ^	VID ^ LAN 1	VID ~ LAN 1 Tagged	VID ^ LAN 1 Tagged LAN 2	VID ^ LAN 1 Tagged LAN 2 Tagged	VID ^ LAN 1 Tagged LAN 2 Tagged LAN 3	VID ^ LAN 1 Tagged LAN 2 Tagged LAN 3 Tagged	VID ^ LAN 1 Tagged LAN 2 Tagged LAN 3 Tagged LAN 4	VID ^ LAN 1 Tagged LAN 2 Tagged LAN 3 Tagged LAN 4 Tagged	VID A LAN 1 Tagged LAN 2 Tagged LAN 3 Tagged LAN 4 Tagged WAN	VID ^ LAN 1 Tagged LAN 2 Tagged LAN 3 Tagged LAN 4 Tagged WAN Tagged	VID ^ LAN 1 Tagged LAN 2 Tagged LAN 3 Tagged LAN 4 Tagged WAN Tagged Bridge
LAN VLAN			1	1 🗸	1 ~ ×	1 × × ×	1 × × × ×	1 × × × × ×	1 × × × × ×	1 × × × × × ×	1 × × × × × × ×	1 ~ x ~ x ~ x ~ x ×	1	
Schedule			2	2 ×	2 × ×	2 × × ×	2 × × × ×	2 × × × × ×	2 × × × × × ×	2 x x x x x x x	2 × × × × × × × ×	2 x x x x x x x x x	2 × × × × × × × × × ×	2 x x x x x x x x x x WAN
DDNS		0	0 *	0 *	0 *	0 *	0 *	0 •	0 7	0 *	0 •			0 T
Routing														
		A	Add +	Add +	Add +	Add +	Add +	Add +	Add +	Add +	Add+	Add +	Add+	Add+
Advanced Network														
Firewall		Save	Save Cance	Save ✓ Cancel ×	Save-/ Cancel×	Save ✓ Cancel ×	Save ✓ Cancel ×	Save ✓ Cancel×	Save ✓ Cancel ×	Save√ Cancel×	Save-✓ Cancel×	Save-/ Cancel×	Save-/ Cancel×	Save ✓ Cancel ×
VPN Tunnel														
Administration														

Step 2 Click "Save" to finish.



2.4.6 Dynamic DNS Settings

Step 1	Go to Basic Network >DDNS and enter the DDNS settings.	
•	5	

Status	•	Already changed login password successfully.	
Basic Network WAN	*	Dynamic DNS	~
Cellular LAN		IP Address Use WAN IP Address 0.0.0.0 (recommended)	
VLAN Schedule		Auto refresh every 28 minutes (0 = Disabled)	
DDNS Routing		Dynamic DNS1	v
হু WLAN	•	Service None *	
Advanced Network	2		
 Firewall VPN Tunnel 	> >	Dynamic DNS2	~
R Administration	2	Service None *	
 More Info 		Save ✓ Cancel ×	
Dynamic DNS			~
IP Address		Use WAN IP Address 0.0.0.0 (recommended)	
Auto refresh ever	ſy	28 minutes (0 = Disabled)	
Dynamic DNS1			~
Service		None •	
Dynamic DNS2			~
Service		None v	
Save 🗸 Cance	el X		

Table 2-5 DDNS Settings

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

Step 2 Click "Save" to finish.



2.4.7 Routing Settings

Step 1 Go to Basic Network >Routing.

ntus	•		Already	changed login	password succes	sfully.		
sic Network	*	Current Routing	Table					8
VAN 'ellular		Destination	Gateway /	Next Hop	Subnet Mask	Metric	Interface	
AN		120.157.126.88	(*)		255.255.255.255	0	WAN	
VLAN		120.157.126.80	<u>ن</u> و		255.255.255.240	0	WAN	
Schedule D DNS		192.168.1.0	(*)		255.255.255.0	0	LAN	
Routing		127.0.0.0	æ		255.0.0.0	0	lo	
WLAN	•	default	120.157.12	5.88	0.0.0.0	0	WAN	
Advanced Network	•							
Firewall	S []							
VPN Tunnel	>	Static Routing T	able					
Administration		Destination	Gateway	Subnet Mask	Metric	Interface	Description	
			0.0.0.0		0	LAN V		
		Add+						
		Miscellaneous						
		Mode	Gati	eway 🔻				
		RIPv1 & v2	Disa	bled 🔻				
		DHCP Routes	~					
		Spanning-Tree Pro	otocol					



	Table 2-6 Routing Settings					
ltem	Instructions					
Destination	Router can reach the destination IP address.					
Gateway	Next hop IP address which the router will reach.					
Subnet Mask	Subnet mask for destination IP address.					
Metric	Metrics are used to determine whether one route should be chosen over another.					
Interface	Interface from router to gateway.					
Description	Describes the routing name.					

Step 2 Click "Save" to finish.

2.5 WLAN Settings

Please follow the instructions below.

2.5.1 Basic Setting

Step 1 Go to WLAN >Basic Settings.



Comset	≡		
Status	>	Wireless(2.4 GHz) Wireless(5 GHz)	
Ø Basic Network		Enable WLAN	
WLAN Basic Settings	× 1	MAC Address	34:0A:19:22:00:43
MultiSSID Wireless Survey		Wireless Mode	Access Point 🗸
Advanced Network	•	Wireless Network Mode	Auto 🗸
🔞 Firewall	•	SSID	Comset-Router-2.4G
VPN Tunnel	()	Broadcast SSID	~
ℜ Administration	•	Channel	Auto 🗸
		Channel Width	40 MHz 🗸 🗸
		Security option	WPA Personal ~
		Encryption	AES 🗸
		Shared Key	•••••



Comset	≡ om.au				
Status	•	Wireless(2.4 GHz) Wireless(5 GHz)			
Basic Network	•	Enable WLAN			
🗟 WLAN	~		34:0A:19:22:00:44		
Basic Settings		MAC Address	54:0A:19:22:00:44		
MultiSSID		Wireless Mode	Access Point V		
Wireless Survey					
Advanced Network	>	Wireless Network Mode	Auto 🗸		
🕲 Firewall	>	SSID	Comset-Router-5G		
VPN Tunnel	5	Broadcast SSID	~		
R Administration	>				
		Channel	Auto 🗸		
		Channel Width	80 MHz 🗸 🗸		
		Security option	WPA Personal V		
		Encryption	AES 🗸		
		Shared Key	•••••		

Table 2-7 WLAN Basic Settings Instructions

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

Step 2 Click "Save" to finish.



2.5.2 Wireless Survey

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

Comset www.comsetc		=				Tools	🛠 Bandwidth 🛩	IP Traffic 🔳 Sy
Status	>			Already ch	anged login password successfi	ally.		
Basic Network	•							
ଙ୍କ WLAN	~	Wireless Site Survey						
Basic Settings		Last Seen 🔨	Radio Band	SSID	BSSID	Channel	RSSI	Encryption
MultiSSID Wireless Survey		Fri 12:02:38	2.4G	COMSET-01	08:36:C9:00:C7:7D	11	-85 dBm	WPA2PSK/AES
Advanced Network		NEW (0m)	240	COMSET-01	00.50.05.00.07.715		-05 060	WEALESWALS
Firewall	•	Fri 12:02:38 NEW (0m)	5G	COMSET-01-5G	08:36:C9:00:C7:7E	149	-76 dBm	WPA2PSK/AES
VPN Tunnel	•	0 added, 0 removed, 2 1 Last updated: Fri 12:02:38	total.					
R Administration		Lask upwalter: PT 12:02:38						

2.6 Advanced Network Settings

2.6.1 Port Forwarding

Step 1 Go to Advanced Network > Port Forwarding.

Status >			Alı	eady changed lo	ogin password	successfully.	
Basic Network	PortFor	warding					
WLAN >							
Advanced Network	On	Proto	Src Address	Ext Ports	Int Port	Int Address	Description A
Port Forwarding	×	UDP		1000,2000		192.168.1.2	ex: 1000 and 2000
Port Redirecting	×	Both		1000-2000,3000		192.168.1.2	ex: 1000 to 2000, and 3000
DMZ	×	Both	1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted
IP Passthrough Triggered	×	TCP		1000	2000	192.168.1.2	ex: different internal port
Captive Portal		TCP					
Serial App. UPnP/NAT-PMP Bandwidth Limiter VRRP Static DHCP Firewall	Ext Int for	: Address (option t Ports - The po Port (optional) warding to a d	and) - Forward only if from th vrts to be forwarded, as seen The destination port inside fferent internal port destination address inside th	from the WAN. ex: "2345" the LAN. If blank, the de	, "200,300", "200-300,4	400".	ort per entry is supported when
VPN Tunnel >							

Table 2-8 Port Forwarding Instructions

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



Comset CM550W-POE 5G Router User

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

Step 2 Click "save" to finish.

2.6.2 Port Redirecting

Step 1 Go to Advanced Network > Port Redirecting.

Status	>		Alread	ly changed login pa	ssword successfu	lly.	
Basic Network	>	PortRedirectin					
ଙ୍କ WLAN	•			121 0101	2.2		
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 Ca	ncel×				

Table 2-9 Port Redirecting Instructions

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

Step 2 Click "save" to finish

2.6.3 DMZ Settings

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



٩	Status	>	Already changed login password successfully.
() ()	Dasie Network	DMZ	
ŵ	Advanced Network	✓ Enable DMZ	
	Port Forwarding Port Redirecting	Internel Address	192.168.1.0
	DMZ IP Passthrough	Source Address Restriction	
	Triggered		(optional: es: "11.11", "1.11.0/24", "1.11.1 - 22.2.2" os: "me.example.com")
	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		
Ø	Firewall	> Save√ Cancel×	

Table 2-10 DMZ Instructions

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

Step 2 Click "save" to finish

2.6.4 IP Passthrough Settings

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

۲	Status	Already changed login password successfully.
ø	Basic Network	ID Barathanush
1	WLAN	IP Passthrough
@	Advanced Network	Enabled
H	Port Forwarding	MAC Address
	Port Redirecting DMZ	
	IP Passthrough	Gateway
	Triggered	
	Captive Portal	Save
	Serial App.	



1	Table 2-11 IF F assunough instructions		
Item	Instructions		
Enable	Enable IP Pass-through		
MAC Address	Enable DHCP of device. Configure device Mac. Device will be assigned a SIM IP.		
Gateway	If CM550W-POE is connected to multiple devices, input other devices gateway.		

Table 2-11 IP Passthrough Instructions

Step 2 Click "save" to finish

2.6.5 Triggered Port Forwarding Settings

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

Status	3			Alread	dy changed login pa	assword successfully.
Basic Network	>	Trigge	ared Port I	orwarding		
🗟 WLAN	•					
Advanced Network	*		Protocol	Trigger Ports	Forwarded Ports	Description A
Port Forwarding		×	TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000
Port Redirecting			TCP 🗸			
DMZ			_			
IP Passthrough		Ad	ld +			
Triggered						
Captive Portal			(200-300).			
Serial App.		•	These ports	are <mark>automatically</mark> cl	osed after a few minutes o	f inactivity.
UPnP/NAT-PMP						
Bandwidth Limiter		Save 🗸	Canc	el×		
VRRP						
Static DHCP						

Table 2-12	Triggered	Instructions
------------	-----------	--------------

Item	Instructions	
Protocol	Support UDP, TCP, both UDP and TCP.	
Trigger Ports	Trigger Ports are the initial LAN to WAN "trigger".	
Transferred Ports	Forwarded Ports are the WAN to LAN ports that are opened if the "trigger" is activated.	
Note	Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic.	

Step 2 Click "save" to finish.



2.6.6 Captive Portal

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

۲	Status	•		Already char	nged login password successfully.
0	Basic Network	>	Contine Dented		
\$	WLAN	•	Captive Portal		
ŵ	Advanced Network		Enabled		
	Port Forwarding		Auth Type	NONE 🛩	
	Port Redirecting DMZ		WEB Root	Default	v
Ī	IP Passthrough Triggered		WEB Host		
	Captive Portal Serial App.		Portal Host		
	UPnP/NAT-PMP Bandwidth Limiter		Login Timeout	0	Minutes
	VRRP Static DHCP		Idle Timeout	0	Minutes
8	Firewall		Ignore LAN	~	
•	VPN Tunnel	•	Redirecting http://	www.google	com
杲	Administration	•	MAC Address Whitelist		
			Download QOS		
			Upload QOS		
			Save≁ Cancel×		

Table 2-13 Captive Portal Instructions

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



Item	Instructions
	card.
Web Host	Configure domain name for the captive portal access. For example, configure as comset.com.au.
Portal Host	Reserved.
Login Timeout	Maximum time the user can be online. At the end of the defined time, the user needs to re-login.
Idle Timeout	Maximum time the user has connectivity when in idle mode.
Ignore LAN	If enabled, LAN devices will bypass the Captive Portal page.
Redirecting	Router will redirect to the defined link after accepting the terms and conditions on the Captive Portal page.
MAC Whitelist	No captive portal page for Wi-Fi device.
Download QoS	Enable to apply the Download Bandwidth limit per user.
Upload QoS	Enable to apply the Upload Bandwidth limit per user.

Step 2 Click "save" to finish.

2.6.7 Serial App. Settings

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

۲	Status	>	Already changed login password successfully.	
٢	Basic Network	>		
7	WLAN	•	Serial to TCP/IP	
R	Advanced Network	•	IPoC Mode	Serial 🗡
	Port Forwarding Port Redirecting DMZ IP Passthrough		Serial to TCP/IPMode	Disabled V
	Triggered Captive Portal Serial App.		Save ✓ Cancel X	
	UPnP/NAT-PMP			



Comset CM550W-POE 5G Router User

Status	Serial to TCP/IP	
Basic Network	IPoC Mode	Serial 🗸
🗟 WLAN 🔹 🔸	Serial to TCP/IPMode	Client
😭 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 (milliseconds)
Serial App. UPnP/NAT-PMP	Serial Timeout	500 (milliseconds)
Bandwidth Limiter VRRP	Packet Payload	1024 (bytes)
Static DHCP	Heart-Beat Content	
🛍 VPN Tunnel 🔹	Heart-Beat Interval	2 (seconds)
R Administration	Port Type	RS485/RS232 ~
	Cache Enable	×
	Debug Enable	
	Baud Rate	57600 ~
	Parity Bit	none 🗸
	Data Bit	8 ~
① More Info	Stop Bit	1 ~

Table 2-14 Serial App Instructions

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



Item	Instructions
Socket Timeout	Router will transmit data to the serial port at the end of the defined time.
Serial Timeout	Serial Timeout is the wait time for transmitting the data package that is less than the Packet payload. The default setting is 500ms.
Packet payload	Packet payload is the maximum transmission length for serial port data packet. The default setting is 1024bytes.
Heart-beat Content	Send heartbeat to the defined server to keep the router online. This is convenient to monitor the router from the server.
Heart-beat Interval	Heart-beat interval time.
Baud Rate	115200 as default.
Parity Bit	None as default.
Data Bit	8bit as default.
Stop Bit	1bit as default.



Serial port connection

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

Step 2 Click "save" to finish.



2.6.8 UPnP/NAT-PMP Settings

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

۲	Status	×.			A	lready c	hanged login	password	successfu	ully.		
0	Basic Network	>	Forwar	ded Ports								
()	WLAN	>	Ext Por	ts	Int Port	In	ternal Address		Protocol	Descri	otion	
₽	Advanced Network Port Forwarding	*										
	Port Redirecting									Delete All ×	C Refres	h
	DMZ IP Passthrough		Setting	s								~
	Triggered Captive Portal		Enable	UPnP								
-	Serial App.		Enable	NAT-PMP								
	UPnP/NAT-PMP Bandwidth Limiter		Inactiv	e Rules Cleani	ing							
	VRRP Static DHCP		Secure	Mode		when	enabled, UPnP clients	are allowed to a	dd mappings c	only to their IP)		
8	Firewall	\$										
۵	VPN Tunnel	>	Show I Places	n My Networl	c							
杲	Administration	>			_							
			Save√	Cancel×								

Step 2 Click "save" to finish.

2.6.9 Bandwidth Control Settings

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



۲	Status	>	A	ready change	ed login passv	word successf	ully.	
۲	Basic Network	•	Bandwidth Control					
\$	WLAN	•						
A	Advanced Network	-	Enable Control					
	Port Forwarding Port Redirecting DMZ IP Passthrough Triggered Captive Portal Serial App.		IP IP Range MAC Address	DLRate	DLCeil	ULRate	ULCeil	Priority Nom ~
	UPnP/NAT-PMP Bandwidth Limiter		Default Class					
	VRRP Static DHCP		Enable Default Class					
8	Firewall	•						
60	VPN Tunnel	>	Save Cancel X					
杲	Administration	•						

Table 2-15 Bandwidth Control Instructions

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

Step 2 Click "save" to finish.

2.6.10 VRRP Settings

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



Status		Already changed login password successfully.
Basic Network S WLAN	VRRP	
😭 Advanced Network 🛛 👻	Enable VRRP	
Port Forwarding Port Redirecting	Mode	backup 🛩
DMZ	Virtual IP	192.168.1.3
IP Passthrough Triggered	Virtual Router ID	
Captive Portal Serial App.	Priority	100
UPnP/NAT-PMP Bandwidth Limiter	Authentication	
VRRP Static DHCP	Script Type	Default 🗸
🐼 Firewall >	Check Interval	3
VPN Tunnel	Weight	10
R Administration		
	Save ✓ Cancel ×	

Step 2 Click "save" to finish.

2.6.11 Static DHCP Settings

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



tatus	•	Al	ready changed login pas	sword successfully	
sic Network	•				
LAN	•	Static DHCP			
vanced Network		MAC Address	IP Address	Hostname 🔨	Descrip
rt Forwarding		00:00:00:00:00:00			
Redirecting		00:00:00:00:00:00	192.168.1.2		
2					
ssthrough		Add+			
ered		18			
ve Portal		and the second sec			
Арр.		Save ✓ Cancel ×			
/NAT-PMP					
width Limiter					
tic DHCP					
tic DHCP wall	>				
	> >				

Step 2 Click "save" to finish.

2.7 Firewall

2.7.1 IP/URL Filtering

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



Status	•	Already changed login password successfully.
🔮 Basic Network 중 WLAN	> >	IP/MAC/Port Filtering
Advanced Network	•	On Src MAC Src IP Dst IP Protocol Src Port Dst Port Policy Description
🕄 Firewall	*	
IP/URL Filtering Domain Filtering		Add+
VPN Tunnel	>	Key Word Filtering
R Administration		On Key Word Description
		Add+
		URL Filtering
		On URL Description
		Add+
		Access Filtering
		On Src MAC Src IP Dst IP Protocol Src Port Dst Port Policy Description
		NON~ Acc~
		Add+
		Save ✓ Cancel ×

Table 2-16 IP/URL Filtering Instructions

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

Step 2 Click "save" to finish.



2.7.2 Domain Filtering

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

St	tatus	>			Already chang	ed login pass	word successfully.
	asic Network	•	Domain F	iltering			
ଙ୍କ M		3	On				
	dvanced Network		Default Po	alicy	White List		
	P/URL Filtering		On	Domain			Description
0	Domain Filtering			Domain			
@ v	PN Tunnel	>	~				
" A	dministration	•	Add +				
			Save 🗸 📗	Cancel×			

Table 2-17 Domain Filtering Instructions

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

Step 2 Click "save" to finish.

2.8 VPN Tunnel

2.8.1 GRE Setting

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



•				Already o	hanged login pass	word successfu	lly.		
•									
>	GRE Tunr	nel							
ork>	On Ida	x ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
•									
×									
	Add +								
t									
nt	GRE Rout	te							
	On	Tunnel Index	^	Destination Addres	is.		Description		
>							besenption		
	~	1	.*						
	_	-							
	Add +								
	> ork> > t	→ GRE Tuni → On Idd → Add+ t GRE Rou → On	GRE Tunnel On: Idx ~ Add+ GRE Route On: Tunnel Index	GRE Tunnel On Idx ∧ Tunnel Address Add + GRE Route On Tunnel Index ∧	GRE Tunnel On Idx Tunnel Address Tunnel Source Add+ GRE Route On Tunnel Index Destination Address	GRE Tunnel On Idx Tunnel Address Tunnel Source Tunnel Destination GRE Route On Tunnel Index Destination Address	GRE Tunnel On Idx Tunnel Address GRE Tunnel GRE Route On Tunnel Index Destination Address	Arready changed login password successfully.	GRE Tunnel On ldx Tunnel Address Tunnel Source Tunnel Destination Keepalive Interval Retries Add+ GRE Route On Tunnel Index Destination Address Description

Table 2-18 GRE Instructions

Item	Instructions
IDx	GRE Tunnel number.
Tunnel Address	GRE Tunnel local IP address which is a virtual IP address.
Tunnel Source	Router's 5G/WAN IP address.
Tunnel Destination	GRE Remote IP address. Usually a public IP address.
Keep alive	GRE tunnel keep alive to keep GRE tunnel connection.
Interval	Keep alive interval time.
Retries	Keep alive retry times.
Description	

Step 2 Click "save" to finish.

2.8.2 OpenVPN Client Setting

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



Comset CM550W-POE 5G Router User

nced	Client 1 Client 2						
	Client 1 Client 2						
all 🔶	Basic Advanced Keys Status						
unnel 👻	VPN Client #1 (Stopped)						
/PN Client							
L2TP Client	Interface Type	TUN *					
istration >	Protocol	UDP *					
	Server Address	1000 (1100) (1100) (10	1194				
	Firewall	Automatic *					
	Authorization Mode	TLS V					
	HMAC authorization	Disabled					
	Create NAT on tunnel	*					
	Start Now						
	Client 2 dvanced Keys Stat	us					
sic Ad	dvanced Keys Stat	us					
sic Ad PN Clien Start with	dvanced Keys Stat It #1 (Stopped) In WAN	us	TUN				
sic Ad PN Clien Start with	dvanced Keys Stat I t #1 (Stopped) In WAN	us	TUN T UDP T				
sic Ad PN Clien Start with Interface Protocol	dvanced Keys Stat at #1 (Stopped) h WAN	us					
sic Ad PN Clien Start with nterface Protocol Server A	dvanced Keys Stat at #1 (Stopped) h WAN	us	UDP *				
sic Ad PN Clien Start with Interface Protocol Server A Firewall	dvanced Keys Stat at #1 (Stopped) h WAN	us	UDP • 1194				
sic Ad PN Clien Start with Interface Protocol Server A Firewall Authoriz	dvanced Keys Stat at #1 (Stopped) h WAN		UDP T 1194 Automatic T				
sic Ad PN Clien Start with Interface Protocol Server A Firewall Authoriz Usernam	dvanced Keys Stat at #1 (Stopped) h WAN Type ddress		UDP I1194 Automatic TLS				
PN Clien Start with Interface Protocol Server A	dvanced Keys Stat at #1 (Stopped) h WAN	us	UDP • 1194				



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

Table 2-19 Basic OpenVPN Instructions



Comset CM550W-POE 5G Router User

PN Client #1 (Stopped)		
Poll Interval	0	(in minutes, 0 to disable)
Redirect Internet traffic		
Accept DNS configuration	Disabled	~
Encryption cipher	Use Defaul	t 🗸
Compression	Adaptive	~
TLS Renegotiation Time	-1	(in seconds, -1 for default)
Connection retry	30	(in seconds; -1 for infinite)
Verify server certificate (tls-remote)		
Custom Configuration		



Item	Instructions
Poll Interval	Openvpn client 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.

Table 2-20 Advanced OpenVPN Instructions



Comset CM550W-POE 5G Router User

Open\	/PN Client		
Client 1	Client 2	l.	
Basic	Advanced	Keys	Status
VPN C	lient #1 <mark>(Sto</mark>	pped)	
For help	o generating k	eys, refer	to the OpenVPN HOWTO.
Certifi	cate Authority		
Client	Certificate		
Client	Key		
Start Nov	v		
Save 🗸	Cancel >	¢	



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

Table 2-21 Keys of OpenVPN Instructions

Open	VPN Client			
Client 1	Client 2			
Basic	Advanced	Keys	Status	
	Client #1 (Sto		ould not be r	ead.
Start No	w			

Item	Instructions
Status	Check Openvpn status and data statistics.

Step 2 Click "save" to finish.





2.8.3 VPN PPTP/L2TP Client Settings

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

© Status	•	L2TP/PPTP Basic							~
Basic Network	•	On	Protocol ^	Name	Server	Username	Password Fir	ewall Default Ro	oute Local IP
😤 WLAN	>		L2TP *		Server	osemane			
Advanced Network	•	Add +	L2TP						
🔀 Firewall	>								
VPN Tunnel	*	L2TP Advanced							~
GRE		On	Name ^	Accept DNS	MTU	MRU	Tunnel Auth	Tunnel Password	Custom Options
OpenVPN Clier		~		NO	Ŧ				
PPTP/L2TP Clic IPSec	εnτ	Add+							
R Administration	5	Add+							
		PPTP Advanced							~
		On	Name ^	Accept DN	s MTU	MRU	MPPE	MPPE Statefu	Custom Options
				NO	v				
		_		1.119					
		Add+							
		Schedule							×
		On		Name 1 ^	Name	2	Policy	Descrip	otion
		~					FAILOVER	•	
		Add+							
③ More Info									

Table 2-23 PPTP/L2TP Basic Instructions

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

Table 2-24 L2TP Advanced Instructions

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



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

Table 2-25 PPTP Advanced Instructions

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

Table 2-26 SCHEDULE Instructions

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

Step 2 Click "save" to finish.



2.8.4 IPSec Settings

Status		Already changed login password successfully.	
Basic Network		IPSec	
🕸 WLAN		Louis and	
Advanced		IPSec 1 IPSec 2 Schedule	
🔯 Firewall 🔷		Group Setup Basic Setup Advanced S	Setup
VPN Tunnel		Enable IPSec	
GRE OpenVPN Client		IPSec Extensions	Normal
PPTP/L2TP Client		Local Security Gateway Interface	3G Cellular
IPSec		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	10.0.0/24 ex. 192.168.88.0/24
		Remote Security Firewalling	2
		Save ✓ Cancel ×	
③ More Info			

2.8.4.1 IPSec Group Setup

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

Group Setup Basic Setup Advanced S	etup	
Enable IPSec		
IPSec Extensions	Normal	
Local Security Gateway Interface	3G Cellular ▼	
Local Security Group Subnet/Netmask	192.168.1.0/24	ex. 192.168.1.0/24
Local Security Firewalling		
Remote Security Gateway IP/Domain		
Remote Security Group Subnet/Netmask	10.0.0/24	ex. 192.168.88.0/24
Remote Security Firewalling		

Table 2-27 IPSec Group Setup Instructions

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



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

Step 2 Click "save" to finish.

2.8.4.2 IPSec Basic Setup

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

Group Setup Basic Setup Advan	iced Setup	
Keying Mode	IKE with Preshared Kev 🔻	
Phase 1 DH Group	Group 2 - modp1024 🔻	
Phase 1 Encryption	3DES (168-bit) *	
Phase 1 Authentication	MD5 HMAC (96-bit)	
Phase 1 SA Life Time	28800 seconds	
Phase 2 DH Group	Group 2 - modp1024 🔻	
Phase 2 Encryption	3DES (168-bit) *	
Phase 2 Authentication	MD5 HMAC (96-bit)	
Phase 2 SA Life Time	3600 seconds	
Preshared Key		

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



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

Step 2 Click "save" to finish.

2.8.4.3 IPSec Advanced Setup

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

Group Setup	Basic Setup	Advanced Setup	
Aggressive Mo	de		
Compress(IP Pa	ayload Compres	ssion)	
Dead Peer Dete	ection(DPD)		
ICMP Check			
IPSec Custom (Options 1		
IPSec Custom (Options 2		
IPSec Custom (Options 3		
IPSec Custom (Options 4		



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

Table 2-29 IPSec Advanced Setup Instructions

Step 2 Click "save" to finish.

2.9 Administration

2.9.1 Identification Settings

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

Status	Al	lready changed login password successfully.
Basic Network	Router Identificatio	n
ବି WLAN	Router Name	Comset Router
Advanced Network	Router Name	
🔞 Firewall	Hostname	Comset_Router
💷 VPN Tunnel	Domain Name	Comset_Domain
R Administration		
Identification	Save ✓ Cancel ×	
Time		•
Admin Access		
Scheduled Reboot		
SNMP		
Storage Settings		
M2M Settings		
DI/DO Setting		
Configuration		
Logging		
Upgrade		



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.		

Table 2-30 Router Identification Instructions

Step 2 Click "save" to finish



2.9.2 Time Settings

Status	· ·		Already changed login password	successfull
Basic Network	•	Time		
🕅 WLAN	•			
Advanced Network		Router Time	Fri, 15 Oct 2021 13:32:37 +1100 Clock Sync.	
Firewall	•	T	UTC+10:00 Australia	~
VPN Tunnel	S	Time Zone	UTC+ 10.00 Australia	
Administration	~	Auto Daylight Savings Time	✓	
Identification		Auto Update Time	Every 4 Hours 🗸	
Time Admin Access				
Scheduled Reboot		Trigger Connect On Demand		
SNMP		NTP Time Server	Custom 🗸	
Storage Settings		NTF TIME Server		
M2M Settings			0.au.pool.ntp.org	
TR-069				
DI/DO Setting			1.au.pool.ntp.org	
Configuration Logging			2.au.pool.ntp.org	
Upgrade				

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

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

Step 2 Click "save" to finish.



2.9.3 Admin Access Settings

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

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

O Status	>	Already changed login password successfully.		
Basic Network	•	WebAccess		
ବି WLAN	21			
Advanced Network	>	Web Style	GUI3.0	
🔞 Firewall	•	Local Access	нттр	
VPN Tunnel	20	HTTP Access Port	80	
R Administration	*	Remote Access	Disabled 👻	
Identification Time		Allow Wireless Access		
Admin Access Scheduled Reboot		Block WAN Ping	~	
SNMP Storage Settings		SSH Enable at Startup		
M2M Settings DI/DO Setting Configuration Logging		Allow Telnet Remote Access		
Upgrade		Password		
		Password	•••••	
		(re-enter to confirm)	•••••	
		Save ✓ Cancel ×		

Step 2 Click "Save" to finish.

2.9.4 Schedule Reboot Settings

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



Status	>	Alı	ready changed login password successfully.
Basic Network			
WLAN	>	Scheduled Reboot	
Advanced Network	•	Enabled	
🕽 Firewall		Time	1:00 AM
VPN Tunnel	•	Days	🗸 Sun 🗸 Mon 🗸 Tue 🗸 Wed 🗸 Thu 🗸 Fri 🗸 Sa
R Administration	•		Everyday
Identification			
Time		Save ✓ Cancel ×	
Admin Access			
Scheduled Reboot			
SNMP			
Storage Settings			
M2M Settings			
DI/DO Setting			
Configuration			
Logging			
Upgrade			

Step 2 Click "Save" to finish.

2.9.5 SNMP Settings

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



 Status Basic Network 	SNMP Settings Enable SNMP	
Image: Symplectic symplect symplectic symplectic symplectic symplectic symplectic sy	Port	161
Image: Second	Remote Access	
■ Administration ✓ Identification ✓	Allowed Remote	(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com")
Time Admin Access	Location	router
Scheduled Reboot	Contact	admin@router
Storage Settings M2M Settings DI/DO Setting	RO Community Custom OID :	rocommunity
Configuration Logging Upgrade	1.3.6.1.4.1.2021.505	eg:/bin/nvram get snmp_enable
opgrate	1.3.6.1.4.1.2021.506	
	1.3.6.1.4.1.2021.507	
	1.3.6.1.4.1.2021.509	
① More Info	Save ✓ Cancel ×	

Step 2 Click "Save" to finish.

2.9.6 Storage Settings

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



Status	>	Alre	eady changed login pa	ssword successfully.
Basic Network	•			
ବି WLAN	•	Storage settings		
Advanced Network	>	Storage	Router	Y Total :5,376.00 кв Free:5,116.00 кв
I Firewall	•			
D VPN Tunnel	•	Upload new file		
R Administration	•	No file chosen	Choo	ose File Upload
Identification				
Time				
Admin Access		Current file list		
Scheduled Reboot				
SNMP		File name	File size	File operation
Storage Settings				
M2M Settings				
DI/DO Setting		Save ✓ Cancel ×		
Configuration		Save Cancel X		
Logging				
Upgrade				

Step 2 Click "Save" to finish.

2.9.7 M2M Settings

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



O Status	>	Already changed login password successfully				
Basic Network WLAN	> >	m2m				
Advanced Network	>	M2M Enabled				
🔯 Firewall	•	Fail Action	Restar	t M2M		
🛍 VPN Tunnel	•	Device ID				
R Administration	~	M2M Server/Port			: 8000	
Time Admin Access		Heartbeat Intval	60	(seconds)		
Scheduled Reboot		Heartbeat Retry	10	(Range:10-1000)		
Storage Settings M2M Settings DI/DO Setting		Named-Pipe Enabled	Remot	e Connect		
Configuration Logging		Named-Pipe Server Port	8002		(Range:1024-65535)	
Upgrade		Named-Pipe Status	Offline			
		Named-Pipe Address	0.0.0.0			
		Save ✓ Cancel ×				

Step 2 Click "save" to finish.

2.9.8 TR-069 Settings

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

Comset your m2m specialist Guide		Comset CM550W-POE 5G Router User
Basic Network >	TR069	
🗟 WLAN 🔷	TRUG9	
Advanced Network	Enabled	
🐼 Firewall 🔹	Enable Periodic Transmission	
VPN Tunnel	Username	openacs
💂 Administration 🛛 👻		
Identification	Password	openacs
Time	URL	http://192.168.1.110:8080/openacs/acs
Admin Access		
Scheduled Reboot		
SNMP Storage Settings	Save- Cancel×	
M2M Settings		
TR-069		
DI/DO Setting		
Configuration		
Logging		
Upgrade		

Step 4 Click "Save" to finish.

2.9.9 DI/DO Setting

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

Basic Network S WLAN Advanced Network	DI Setting Enabled	Port1 🗸	Port2
Image: Stress Image: Stress Image: Stress Image: Stress Image: Stress Image: Stress	Port1Mode	ON	*
🕱 Administration 👻	Filter	1	(*100ms)
Identification Time Admin Access	SMS Alarm		
Scheduled Reboot	DO Setting		
Storage Settings M2M Settings	Enabled	Port1	Port2
TR-069 DI/DO Setting			
Configuration	Save ✓ Cancel ×		

2.9.7.1 DI Configuration



inabled	Port1 🗸	Port2
Port1Mode	ON	v
lilter	1	(*100ms)
SMS Alarm		
O Setting		
	Port1 🗸	Port2
nabled	Port1 🔽 DI Control	Port2 SMS Control
O Setting Enabled Alarm Source Alarm Action		
Enabled Alarm Source	DI Control	

Table 2-31 DI Instructions

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

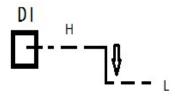


Item	Description		
	pulse shape are not at the same level, the CM550W-POE will trigger an alarm according to the Counter Action settings.		
Counter Trigger	Available when the DI is under Event Counter mode.		
	Input from 0 to 100. "0" means the alarm is not triggered.		
	The alarm will be triggered when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

Step 2 Click "Save" to finish.

NOTE

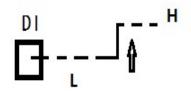
OFF Mode DI from high level 3.3~5V to low level 0V will be triggered.





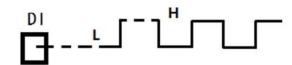
ON Mode

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



EVENT_COUNTER Mode

The counted number of pulses will be triggered.



2.9.7.2 DO Configuration

DO Setting	~
Enabled	
Alarm Source	DI Control 🗸 SMS Control 🗸
Alarm Action	ON ·
Power On Status	OFF •
Keep On	1 (*100ms)
SMS Trigger Content	70 ASCII Max
SMS Reply Content	70 ASCII Max
SMS admin Num1	
SMS admin Num2	Backup
Save√ Cancel×	

Table 2-32 DO Instructions

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



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

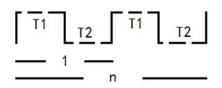


Item	Instructions		
Output	Available if Pulse is enabled in "Alarm On Action"/ "Alarm Off Action".		
	The number of pulses, input from 0 to 30000. (0 for continuous pulse output)		
SMS Trigger	Available when you enable SMS Control in Alarm Source.		
Content	Input the SMS content to enable "Alarm On Action" 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

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



2.9.10 Configuration Settings

Step 1 Go to "Administration> Configuration " to configure backup.

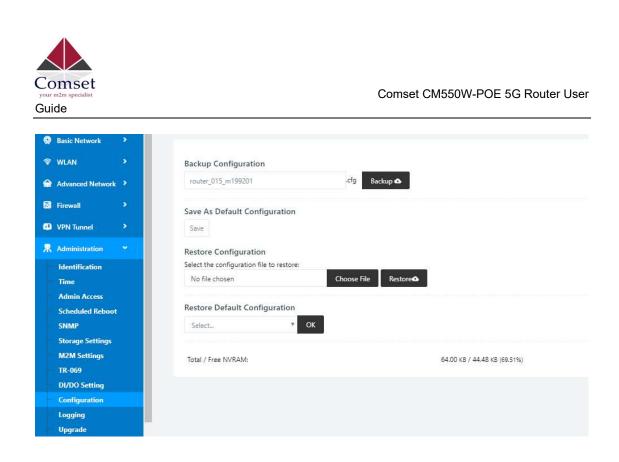


Figure 3-1 Backup and Restore Configuration GUI

© CAUTION "Restore Default" will delete all configuration settings.

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



2.9.11 System Log Settings

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

	Status	•	Already changed login password successfully.				
Ø	Basic Network	*	Syslog				
((*	WLAN	2		-			
ଜ	Advanced Network	>	Log Internally				
8	Firewall	÷	Log To Remote System				
0	VPN Tunnel	2	Host or IP Address /	192 <mark>.1</mark> 68.1.2	2	514	
杲	Administration	*	Port				
-	Identification Generate Marker		Every 1 Hour				
-	Time			60			
	Admin Access		Limit 60 (messages per minute / 0 for un		r unlimited)		
	Scheduled Reboot						
	SNMP		Save 🗸 🛛 Cancel 🗙				
	Storage Settings						
-	M2M Settings						
	DI/DO Setting						
-	Configuration						
	Logging						
	Upgrade						

Figure 3-1 System log Settings GUI

Step 2 Click "Save" to finish.



2.9.12 Firmware upgrade

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

Basic Network	>
☞ WLAN	Upgrade Firmware Select the file to use:
😭 Advanced Network	No file chosen Choose File Upgrade
🔀 Firewall	• • • • • • • • • • • • • • • • • • •
VPN Tunnel	Current Version: D1.00.01
R Administration	• ·
Identification	
Time	
Admin Access	
Scheduled Reboot	
SNMP	
Storage Settings	
M2M Settings	
TR-069	
DI/DO Setting	
Configuration	
Logging	
Upgrade	
MCU Upgrade	*

Figure 3-1 Firmware Upgrade GUI



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

2.10 "Reset" Button to Restore Factory Settings

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

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

Table 2-33 System Default Instructions



Item	Default settings
Username	admin
Password	admin

NOTE

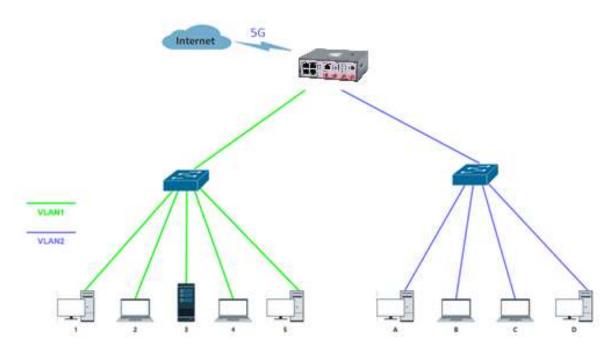
After reboot, the configuration will be deleted and restored to factory settings.



3 Configuration Examples

3.1 VLAN

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





Status	~	Curtaria			~	WAN		â	
Overview		System			~	WAN		4	~
Traffic Stats.		Router Name	Router			Connection Type	WAN		
GPS Status		Hardware Version	C11-D20			Modem IMEI	869756047494023		
Device List		Firmware Version	G5.0.1.5			Cellular ISP			
Basic Network	3	Router Sn	1120G512007270003			Cellular Network			
Basic Network		Chipset	ARMv7 Processor rev 5 (v7I)			USIM Selected	USIM Card 1 Running		
WLAN	>					IP Address	192.168.10.113		
Advanced Network		Router Time	Sat, 06 Mar 2021 12:18:23 +0800	Clock Sync.		Subnet Mask	255.255.255.0		
Advanced Network		Uptime	2 days, 17:02:20			Gateway	192.168.10.1		
Firewall	•	Memory Usage	40.32 MB / 122.20 MB (33.00%)			DNS	8.8.8.8:53, 8.8.4.4:53		
VPN Tunnel			40.58 KB / 64.00 KB (63.41%)			Connection Status	Connected		
VPN Junnel	- C	NVRAM Usage	40.38 KB / 04.00 KB (03.41%)			Connection Uptime	2 days, 17:01:53		
Administration	•								
		Ethernet Ports Status			~	Wireless (2.4 GHz)		۵	
		WAN/LAN1	LAN2 LAN3	LAN4		Wireless (2.4 GHz)		\$	
		10001	M M	1					
		Full	Unplugged Unplugged	Unplugged		Wireless (2.4 GHz)		٥	
		VPN Status		0	~	Wireless (2.4 GHz)		0	

1) Configure LAN with Basic Network.

•	Status	<u> </u>		You haven't chang	jed the default password fo	r this router. To chang	ge router password <u>click here.</u>	
Ø	Basic Network	*						
	WAN		LAN					`
	Cellular		Bridge	A IP Addre	ess Subnet Mask	DHCP Serve	er IP Pool	Lease(minutes,
	LAN		br0	192.168.	.1.1 255.255.255.0) <i>v</i>	192.168.1.2 - 51	1440
	VLAN					s 245		
	Schedule		br1	192,168.1	10.1 255.255.255.0) <i>v</i>	192.168.10.100 - 120	1440
	DDNS Routing		br2	192.168.2	20.1 255.255.255.0) <i>~</i>	192.168.20.100 - 120	1440
?	WLAN	*	3	•				
2	Advanced Network	>						
3	Firewall	•	Add+					
D	VPN Tunnel	•	Save - Can	cel×				
R	Administration	•						
	More Info							

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



Basic Network	** *												
WAN		VLAN											
Cellular		VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
LAN		0	~	×	×	×	×	×	×	×	×	×	br1
VLAN		0	Ŷ		^	^	^	^	^		^	^	DET
Schedule		1	×	×	~	×	~	×	×	×	~	×	br0
DDNS		2	×	×	×	×	×	×	×	×	×	×	WAN
Routing													Prost.
🗟 WLAN	>	3	×	×	×	×	×	×	~	×	×	×	br2
Advanced Network	•	4 *											none
Firewall	>	Add+											
D VPN Tunnel	•												
Administration		Save√ C	ancel×										

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

Status	•		You	haven't ch	hanged the	e default p	assword fo	or this rout	er. To char	ige router	password	click here.	
Basic Network	~												
WAN		VLAN											
Cellular		VID ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge
LAN		0	~	~	×	×	×	×	×	×	×	×	br1
VLAN		U	~	~	^	<u>^</u>	^	<u>(</u>	<u>^</u>	^	<u>^</u>	^	DIT
Schedule		3	×	×	~	×	~	×	×	×	~	×	br0
DDNS		2	×	×	×	×	×	×	×	×	×	×	WAN
Routing			×	×	×	×	×	×	~	~	×	×	br2
🗟 WLAN	2	3	^	^	^	^	^	<u>^</u>	~	~	^	^	DIZ
Advanced Network	•	4 ▼											none
Firewall	•	Add+											
VPN Tunnel	•												
Administration		Save√ Ca	ncel×										
 More Info 													

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

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

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



Basic Network			
WAN		WAN / Internet	
Cellular		Туре	Static Address 🔻
LAN			Disabled
VLAN		IP Address	DHCP PPPoE
Schedule DDNS		Subnet Mask	Static Address 255.255.255.0
Routing		Subnet Mask	233233233.0
ି WLAN	•	Gateway	192.168.10.1
Advanced Network	•	MTU	Default 🔻 1500
Firewall			
VPN Tunnel	•	Primary DNS	192.168.10.1
Administration	*	Secondary DNS	0.0.0

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

0	Basic Network														
	WAN	VLAN													2
	Cellular	VI	D ^	LAN 1	Tagged	LAN 2	Tagged	LAN 3	Tagged	LAN 4	Tagged	WAN	Tagged	Bridge	
	LAN		1	~	×	~	×	~	×	4	×	×	×	br0	
	Schedule		2	×	×	×	×	×	×	×	×	1	×	WAN	
	DDNS Routing	0	۷											none	,
7	WLAN	Add	4												
•	Advanced Network														
72	Firewall	Save 🗸	Саги	cel X											
•	VPN Tunnel														
-	Administration														

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



tatus	>	Basic Settings SIM 1 SIM 2	
ic Network	2 % ()	SIM 1 Mode	Auto
N			
llular		SIM 1 5G Mode	SA & NSA 🗸
N			
AN		SIM 1 PIN Code	
chedule			telstra.internet
DNS		SIM 1 APN	teistra.internet
outing		SIM 1 User	
AN	2		
anced Network	>	SIM 1 Password	
wall	>	SIM 1 Dial Number	*99#
l Tunnel		SIM 1 Auth Type	Auto 🗸
ninistration	>	SIM 1 Local IP Address	

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

Add ICMP Check to WAN

Enabled Links Status Link Name Link Type Description Basic Network ECM/QMI WAN modem Cellular wan WAN(STATIC) ICMP Check Interval On Link Destination Retries Description 🕆 WLAN 8.8.8.8 20 5 WAN Port Advanced Netw -Firewall VPN Tunnel • R Administration Schedule On Link 1 Link 2 Policy Description BACKUP WAN (Link1) preferred, Cellular (Link2) backup wan * FAILOVER moder 1 Save-/ Cancel×

Set the working mode (Schedule)

×



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

5) Status: WAN working

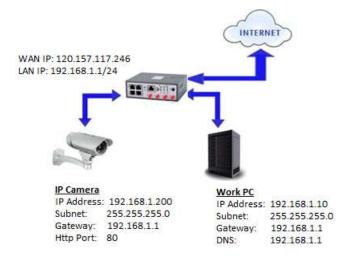
Status	. 👻	5			~	WAN		۵	
Overview		System			~	WAN		4	~
Traffic Stats.		Router Name	Router			Connection Type	WAN		
GPS Status		Hardware Version	C11-D20			Modem IMEI	869756047494023		
Device List		Firmware Version	G5.0.1.5			Cellular ISP			
	1.1.1	Router Sn	1120G512007270003			Cellular Network			
Basic Network	•	Chipset	ARMv7 Processor rev 5 (v7l)			USIM Selected	USIM Card 1 Running		
🗇 WLAN	>					IP Address	192.168.10.113		
						Subnet Mask	255.255.255.0		
Advanced Network	•	Router Time	Sat, 06 Mar 2021 10:36:03 +0800	Clock Sync.		Gateway	192.168.10.1		
S Firewall		Uptime	2 days, 15:20:01			DNS	8.8.8.53. 8.8.4.4:53		
Cost Firewall	>	Memory Usage	39.87 MB / 122.20 MB (32.63%)			Connection Status	Connected		
VPN Tunnel	>	NVRAM Usage	40.58 KB / 64.00 KB (63.41%)				2 days, 15:19:33		
		1				Connection Uptime	2 days, 15:19:55		
R Administration	2								
		Ethernet Ports Status			÷	Wireless (2.4 GHz)		¢	^
		WAN/LAN1	LAN2 LAN3	LAN4		Wireless (2.4 GHz)		¢	^
		1000M Full	Unplugged Unplugged	Unplugged		Wireless (2.4 GHz)		٥	^
③ More Info		VPN Status		٥	~	Wireless (2.4 GHz)		٥	~

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

3.3 Port Forwarding

1) Network topology:





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

NOTE:

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

Cellular ISP	"Telstra Mobile Telstra"
Cellular Network	LTE Band 7
USIM Selected	USIM Card 1 Running
USIM Status	Ready
CSQ	
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

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

2) Change the router GUI to port 8080 to avoid conflict with the IP camera Http port (80).Go to Administration -> Admin Access -> HTTP Access port set to 8080.



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

🕄 Firewall	2	Local Access	HTTP
VPN Tunnel	•	HTTP Access Port	8080
Administration	~	Remote Access	нттр
Identification		Remote Access	
Time		Access Port	8080
Admin Access			
Scheduled Reboot		Allowed Remote	

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

← → C ☆ H Apps ▲ Comse		ecure 192.168.1.1:8080/#s gle 🕜 www.speedtest.net	tatus-home.asp
Comset	E norm au		
Status Overview	•		
Traffic Stats. Device List		System	
Basic Network	•	Router Name Hardware Version	Comset Router C11-D13

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

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

Proto: TCP

External Ports: 80

Internal Ports: 80

Internal Address: 192.168.1.200

Description: IP camera

Then click on the "Add" button.

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 IP Passthrough	~	Both		8000	8000	192.168.1.17	
Triggered Captive Portal		TCP		80	80	192.168.1.200	IP Camera
Serial App. UPnP/NAT-PMP	Add	+					



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

3.4 IP Passthrough

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

twork Connection Detail	s
Network Connection Details:	
Property	Value
Connection-specific DN Description	Comset_Domain Realtek PCIe GBE Family Controller
Physical Address	1C-39-47-BD-5E-51
DHCP Enabled	Yes

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

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

Status	*	You haven't changed the defau	It password for this router. To change router password <u>click here</u>
Basic Network	IP Passthrough	and a set of the set o	
🗟 WLAN	in rassurough		
Advanced Network	Enabled		
Port Forwarding	MAC Address	1C:39:47:8D:5E:51	Set MAC Address on Laptop LAN interface Note: Use colon in between of hexadecimal characters
Port Redirecting DMZ	Gateway	ar ar 111 - 1 ²⁸ 11] - 1111 - 1111 - 1111 - 1111	
IP Passthrough	Guttiny		
Triggered			
Captive Portal	Court Court		
Serial App.	Save ✓ Cancel ×		
UPnP/NAT-PMP			

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



0	Basic Network	~		5-1 <u>0</u>	u navan Lunanya		www.ivuidige.ivuidi	CHOK MORE
	WAN		LAN					
	Cellular		Bridg	ge ^	IP Address	Subnet Mask	DHCP Server	IP Pool
	VLAN							192.168.1.2
	Schedule		0	v 192	.168.1.1	255.255.255.0		
	DDNS							192.168.1.254
	Routing		Delete x	CancelØ OK	/			rver box to edit and uncheck
Ŷ	WLAN				-		option to Disable	and click ok and SAVE.
e	Advanced Network		1	*				
8	Firewall		Add +					
۵	VPN Tunnel		Add +					
泉	Administration		Save√ Can	cel×				

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

-	twork Disable	
	Status	
	Diagnose	
•	Bridge Connections	
1	Create Shortcut	
9	Delete	
•	Rename	
	Properties	
		1
Ether	net	
Ether	net	
Ether	net • Enable	
Ether	net Enable Status	
Ether	net Enable Status Diagnose	
Ether	net Enable Status Diagnose Create Shortcut	

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





Property	Value
Connection-specific DN	Comset_Domain
Description	Realtek PCIe GBE Family Controller
Physical Address	1C-39-47-BD-5E-51
DHCP Enabled	Yes
IPv4 Address	120.157.89.70
Pv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, 25 September 2019 10:
Lease Expires	Thursday, 26 September 2019 10:55
Pv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	120.157.89.1
IPv4 DNS Servers	10.4.130.164
	10.4.149.70

5) Check internet connection via command line:

<pre>Pinging google.com [172.217.167.78] with 32 bytes of data: Reply from 172.217.167.78: bytes=32 time=75ms TIL=53 Reply from 172.217.167.78: bytes=32 time=46ms TIL=53 Reply from 172.217.167.78: bytes=32 time=47ms TIL=53 Reply from 172.217.167.78: bytes=32 time=47ms TIL=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</pre>	C:\Users\a>ping google.com
Ping statistics for 172.217.167.78: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:	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
C:\Users\a>	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

3.5 Captive Portal

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



Status	•	Captive Portal	
Basic Network	•	Enabled	
🗟 WLAN	2	Auth Type	NONE *
Advanced Network	*	WEB Root	Default V
Port Forwarding Port Redirecting DMZ		WEB Host	
 IP Passthrough Triggered 		Portal Host	
Captive Portal Serial App.		Login Timeout	0 Minutes
UPnP/NAT-PMP Bandwidth Limiter		idie Timeout	0 Minutes
VRRP Static DHCP		Ignore LAN	
🔀 Firewall	•	Redirecting http://	www.google.com
VPN Tunnel		MAC Address Whitelist	
R Administration	•	Download QOS	
		Upload QOS	
More Info		Save-/ Cancel×	

1) Upload Portal file and Splash.html by local

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

Status		You haven't changed the default password	d for this router. To change router password <u>click here</u> ,	
Basic Network				
🗣 WLAN	Storage settings			~
Advanced Network	Storage	Router Total :5,632.00 KB Fre	e:5,372.00 K8	
🔯 Firewall				
VPN Tunnel	Upload new file			
R Administration	No file chosen	Choose File Upload		
- Identification				
Time Admin Access				
Scheduled Reboot	Current file list			ř
SNMP	File name	File size	File operation	
Storage Settings	sms.list	159	× e	
M2M Settings DI/DO Setting				
Configuration				
- Logging	Save ✓ Cancel ×			
Upgrade	Surce Concerv			
More Info				

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



Status	•	Storage settings				23
Basic Network	•	Storage	Router 🔻	Total :5,632.00 кв Free;5,100.00 кв		
ବି WLAN						
Advanced Network	•					
🔯 Firewall	•	Upload new file				
VPN Tunnel	•	No file chosen	Choose File Upload			
R Administration						
ldentification Time		Current file list				2.
Admin Access		File name		File size	File operation	
Scheduled Reboot		0001_portal.png		23.8K	× 8	
Storage Settings		0002_portal.png		45.3K	× =	
M2M Settings DI/DO Setting		0003_portal.png		46.0K	× B	
Configuration		bootstrap_portal.css		124.3K	a a	
Logging		jquery_portal.js		289.7K	* 8	
Upgrade		splash.html		3.4K	* 3	
① More Info						



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





2) Modify portal file storage path.

Modify portal file storage for In-storage as below:

Status	Captive Portal	
Basic Network	Enabled	
🗟 WLAN		
Advanced Network	Auth Type	NONE *
Port Forwarding Port Redirecting	WEB Root	In-storage 💌
DMZ IP Passthrough	WEB Host	
Triggered	Portal Host	
Captive Portal Serial App.	Login Timeout	0 Minutes
UPnP/NAT-PMP		
Bandwidth Limiter	Idle Timeout	0 Minutes
VRRP Static DHCP	Ignore LAN	
🔀 Firewall	Redirecting http://	www.google.com
VPN Tunnel	MAC Address Whitelist	
R Administration	Download QOS	
(i) More Info	Upload QOS	



3.6 GPS Settings (GPS version only)

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

O Status	Yo	ou haven't changed the default password for	this router. To change router password <u>click here.</u>	
Basic Network				
🗣 WLAN	GPS			
Advanced Network	GPS Mode	Client 🔻		
Port Forwarding	Data Format	M2M_FMT		
Port Redirecting DMZ	Server IP/Port	192.168.1.2	: 40002	
IP Passthrough				
Triggered Captive Portal	Heart-Beat Content			
Serial App.	Heart-Beat Interval	5 (seconds)		
GPS UPnP/NAT-PMP				
Bandwidth Limiter	Save ✓ Cancel ×			
VRRP Static DHCP	Jave V Concer A			
🐼 Firewall				
VPN Tunnel				
R Administration				
 More Info 				

Table 4-6 "GPS" Instructions

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

Step 1 Click on "Save" to finish.

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

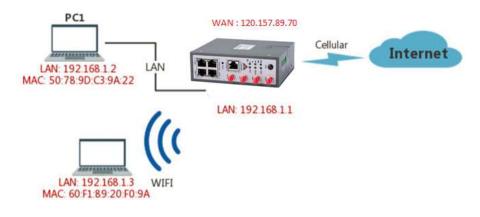
Step 3 Check GPS Status.



Status	Ť	You haven't cha	anged the default password for this router. To change router password_ <u>click here.</u>
Overview			
Traffic Stats.		GPS Status	
GPS Status			27
Device List		Current	OK
Basic Network	>	System Type	GPS
Basic Network	2	Satellites Numbers	05
WLAN	>	Satellites Clock	190404 - 022121.00
		Positioning	2234.22520N - 11356.63170E
Advanced Network	1	Google Map	View
Firewall	5		
VPN Tunnel	2		
Administration	>		
 More Info 			

3.7 Firewall

Network Topology



1) IP/MAC/Port Filtering

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

Test case:

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

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



Status	•	IP/MAC	/Port Filtering						
Basic Network	•	On Src M		Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy Description
🗟 WLAN	•	v -	inc.	any/0	any/0	-	-		Drop
Advanced Network	•			any/0 any/0	192.168.1.0/24	-		-	Accept
Firewall		× -							
IP/URL Filtering			:9D:C3:9A:22	any/0	any/0	÷	4		Accept
Domain Filtering		✓ 60:F1	:89:20:F0:9A	any/0	any/0	×		÷.	Accept
VPN Tunnel	•	✓ 00:1E	:64:DF:E8:46	any/0	any/0	2	3	127	Accept
Administration	*					NON *			Accer 🔻
		Add+ Key Wo On	rd Filtering Key Word				Description		
		Add+							

2) Keyword Filtering

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

Status	>						
Basic Network	>	URL Filterin	ng				
常 WLAN		On	URL		Descriptio	on	
😭 Advanced Network	•	~	youtube				
S Firewall	~	~	facebook				
IP/URL Filtering							
Domain Filtering							
VPN Tunnel	>	Add+					
R Administration	•	Access Filte	ering				
		On Src MAC	Src IP	Dst IP	Protocol Src Port	Dst Port	Policy Description
					NOT *		Acce *
		Add +					
		Save✓	Cancel×				

3) URL Filtering

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

4) Access Filtering



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

Test case:

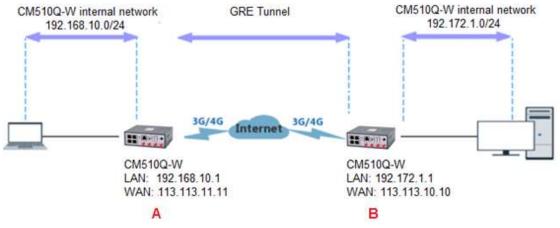
- 4.1) Intercept all TCP packets accessing the router's WAN/Cellular(120.157.89.70).
- 4.2) Only two devices (MAC/LAN/WLAN) can be accessed from Internet packets.

Status	12	×	youtube							
Basic Network	5	5	facebook	i.						
V WLAN										
Advanced Network		Add+								
2 rineat	189									
IP/URL Filtering		Acces	ss Filtering							
Domain Filtering		On Sr	IT MAC	Sire 10	Out 1P	Protocol	Src Port	Dat Port	Policy	Description
D VPN Tunnel	.			any/0	any/0	TCP	+))	4	Drop	
R Administration	1		010/64/07 58:46	any/0	any/0	TCP		14	Accept	
		× 60	DF1/8920F09A	any/0	any/0	TCP	ŧ	19 19	Accept	
						500F *			Acce +	
		Add+								
		Saver	Cancel X							
More into		and the second s								

3.8 VPN Tunnel

3.8.1 GRE

GRE Tunnel between two COMSET Routers





1) CM550W-POE(A) Configuration

Navigate to **Basic Network > LAN**

۲	Status	You h	aven't changed the de	and the second for this r	outer. To change rout	er password <u>click here.</u>	
Ø	Basic Network						
-	WAN	LAN					~
-	Cellular	Bridge 🔿	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
	LAN	br0	192.168.10.1	255.255.255.0	~	192.168.10.2 - 51	1440
	VLAN Schedule	-					
	DDNS	1					
	Routing						
Ŷ	WLAN	Add+					
۲	Advanced Network						
8	Firewall	Save ✓ Cancel ×					
٩	VPN Tunnel						
黒	Administration						
	(i) More Info						

Navigate to VPN Tunnel > GRE

٩	Status	GRE	Tunnel								~
Ø	Basic Network	On	Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description	
\$	WLAN	~	1	192.168.10.10	113.113.11.11	113.111.10.10	~	10	5	А	
۲	Advanced Network										
8	Firewall		ld+								
•	VPN Tunnel										
	GRE										
	OpenVPN Client	GRE	Route								~
	PPTP/L2TP Client	On	Tunnel I	ndex 🔨	Destination Add	ress		Descriptio	on		
累	Administration	~	1		192.172.1.0/24			А			×
m	Administration		1		•						
		Ad	ld +								
		Save✓	Cancel×								
		Savev	Cancer×								

2) CM550W-POE(B) Config

Navigate to **Basic Network > LAN**



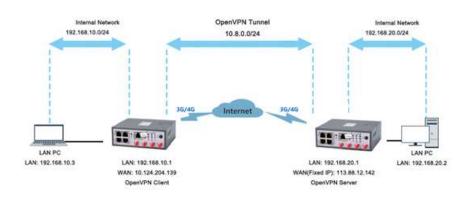
0	Status	*		You h	aven't changed the de	efault password for this	router. To change rout	er password <u>click here.</u>	
Ø	Basic Network	*							
	WAN		LAN						~
	Cellular		Bridg	ge 🔨	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)
	LAN		b	r0	192.172.1.1	255.255.255.0	~	192.172.1.2 - 51	1440
	VLAN				02002000	200,200,200,00			1110
	Schedule DDNS		T	Ŧ					
	Routing								
?	WLAN	*	Add+						
۲	Advanced Network	>							
2	Firewall	>	Save≁ C	ancel ×					
•	VPN Tunnel	•							
黒	Administration	•							
	 More Info 								

Navigate to VPN Tunnel > GRE

O Status	•	GRE	Tunnel								~
Basic Network		On	Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description	
WLAN		~	1	192.172.1.10	113.111.10.101	113.113.11.11	~	10	5	В	
Advanced Network		~									
🔕 Firewall			id+								
VPN Tunnel											
GRE OpenVPN Client		GRE	Route								~
PPTP/L2TP Client		On		Index ^	Destination Add	ess		Descriptio	n		
R Administration		~	1		192.168.10.0/24			В			×
		_	1		•						
		Ac	id +								
		Save✓	Cancel×								
(i) More Info		-									

3.8.2 OpenVPN





OpenVPN between CM550W-POE client and Server

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

Comset	=	
Status		Aneady changed
Basic Network	OpenVPN Client	
ବି WLAN	Client 1 Client 2	
Advanced Network	Basic Advanced Keys Status	
🔞 Firewall 🔹		
🖨 VPN Tunnel 👻	VPN Client #1 (Stopped)	
GRE	Start with WAN	
OpenVPN Client		
PPTP/L2TP Client	Interface Type	TUN 🗸
IPSec 不 Administration >	Protocol	UDP V
	Server Address	1194
	Firewall	Automatic 🗸
	Authorization Mode	TLS V
	Username/Password Authentication	
	HMAC authorization	Disabled 💙
	Create NAT on tunnel	
	Start Now	

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



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

Status	
Basic Network OpenVPN Client	
WLAN Client 1 Client 2	
Advanced Network Basic Advanced Keys Status	
Firewall	
C VPN Tunnel VPN Client #1 (Stopped)	
GRE Poll Interval 0 .(in minutes, 0 to	disable)
OpenVPN Client Redirect Internet traffic	
IPSec Accept DNS configuration Disabled ✓	
Encryption cipher Use Default 🗸	
Compression Adaptive 🗸	
TLS Renegotiation Time -1 (in seconds, -1	for default)
Connection retry 30 (in seconds; -1	for infinite)
Verify server certificate (tls-remote)	
Custom Configuration	

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



Access DNS	As per user's configuration.
Encryption	As per user's configuration.
Compression	As per user's configuration.
TLS Renegotiation Time	TLS negotiation 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.

Status	You ha	ven't changed the default password for this router. To change router password <u>click here</u> .
Basic Network	OpenVPN Client	
🗟 WLAN	Client 1 Client 2	
Advanced Network		
🔯 Firewall	Basic Advanced Keys Status	
VPN Tunnel	VPN Client #1 (Stopped)	<u>×</u>
GRE OpenVPN Client	For help generating keys, refer to the OpenVPN HOWTO.	
PPTP/L2TP Client IPSec	Certificate Authority	
R Administration		۲ ۲
	Client Certificate	
		4 F //
	Client Key	
		4 D
	Start Now	
O More Info	Save ✓ Cancel ×	

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



Status	You haven't changed the default password for this router. To change router password <u>click here.</u>
Basic Network	
🕈 WLAN	OpenVPN Client
Advanced Network	Client 1 Client 2
🔕 Firewall	Basic Advanced Keys Status
VPN Tunnel	
GRE	VPN Client #1 (Stopped)
OpenVPN Client	Client is not running or status could not be read.
PPTP/L2TP Client	Crient is not full mining of status coold not be read. Refresh Status
IPSec	remer i destruite
R Administration	Start Now
	Save ✓ Cancel ×
O More Info	

Item	Instructions
Status	Check OpenVPN status and data statistics.

Click "save" and "start now" to start OpenVPN.

OpenVPN Keys Guide

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

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

← → C Secure | https://openvpn.net/release/

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
1zo-1.08-4.0.rh9.rf.i386.rpm	21-Feb-2012 00:50	59K
1zo-1.08-4.1.el3.rf.i386.rpm	21-Feb-2012 00:50	58K
1zo-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 <u>http://openvpn.net</u> for more information)



	Choose Components	
PENVPN	Choose which features of OpenVPN 2.3.0-I001 you was install.	nt to
Select the components to i service if it is running. All [install/upgrade. Stop any OpenVPN processes or the Open DLLs are installed locally.	VPN
Select components to insta	OpenSSL Utilities	_ ^
	OpenVPN RSA Certificate Management Scrip Add OpenVPN to PATH Add Shortcuts to Start Menu Dependencies (Advanced)	E
	Description	-
Space required: 4.4MB	Description Position your mouse over a component to see its description.	

PC > Newdisk (D:) > OpenVPN >

ame	Date modified	Туре	Size
1.	2010 01 10 11 12		
bin	2019-01-10 11:42	File folder	
config	2019-01-10 14:10	File folder	
doc	2019-01-10 11:42	File folder	
easy-rsa	2019-01-10 11:54	File folder	
log	2019-01-10 14:10	File folder	
sample-config	2019-01-10 11:41	File folder	
) icon.ico	2015-02-18 17:56	lcon	22 KB
Uninstall.exe	2019-01-10 11:42	Application	117 KB

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



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

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

Client certificate (Generated on the server)

Name	Date modified	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
n client.ovpn	2019-01-10 14:08	OpenVPN Config	4 KB
📄 ta.key	2019-01-10 12:04	KEY File	1 KB

OpenVPN>easy-rsa>keys



01.pem	2019-01-10 12:01	PEM File	Status	OpenVPN Client
02.pem	2019-01-10 12:04	PEM File	Binic Network	
eacet	2019-01-10 11:57	Security Certificate	2 3 5 M ()	Oet1 Det2
cakey	2019-01-10 11:57	KEY File	🕈 WAN 🔹	
client.ort	12:04	Security Certificate	Advanced Network	Basic Advanced Keys Status
client.csr	2019-01-10 12/04	CSR File	A PARALLO PECHANA	
client.key.	2019-01-10 12:04	KEY FIRE	E firmel >	Little Close at a
dh1024.pem	2019-01-10 12:02	PEM File	100 March 1	VPN Client #1 (Stopped)
index.bt	2019-01-10 12:04	Test Document	d) Vincent 🔷	For help generating keys, refer to the OpenVPN HOW70.
index.bit.attr	2010-01-10 12:04	ATTREAM	GAL	
setial	2019-01-10 19-04	File	OpenVIN Class	Centrale Authority Fishch-AMUMUreCHEXCOSOL-BasilablePYWoPysi-JanaDe
server.ort	2019-01-10 12:01	Seturity Certificate	Printed Clean	auDounter.9ngDOMICV.cxG3bjChra.55NWecPm3b/sm+bi
server.csr	2019-01-10 12:01	CSR File	15k	
server.key	2019-03-10 12:01	KEY File		
ta.key	2019-01-10 12:04	KEY File	Administration	Cient Cetificate x7
				Qb7zH4z2pR66-Q3VEV7pw++
				END CERTIFICATE
				+SDNdesborhOOMmadshilluGulaaddfadbirgAmul
				Ciert Key WH
				11GrayNaCht/RALBULDireWCpU62X/GxB/9a8/ay0+
				Start Now
		,		Save - Cancel X

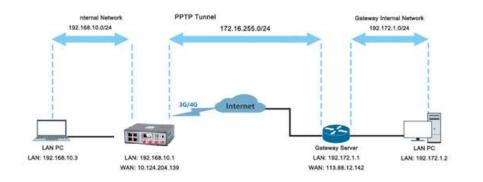
Ping test your server when the tunnel is established:

Basic Network	>				
		Basic Advanced Keys	Status		
₽ WLAN	>				
Advanced Network	>	VPN Client #1 (Running)			
B Firewall	•	Data current as of Thu Apr 4 11:3	4:22 2019.		
		General Statistics			
VPN Tunnel	~	Name		Value	
GRE		TUN/TAP read bytes		0	
OpenVPN Client			Command Prompt - C X		
PPTP/L2TP Client		TUN/TAP write bytes	(c) 2017 Microsoft Corporation. All rights reserved.	0	
IPSec		TCP/UDP read bytes	C:\Users\Root>ping 10.8.0.1	7168	
Administration	*	TCP/UDP write bytes	Pinging 10.8.0.1 with 32 bytes of data:	5531	
	Auth read bytes	RepIy from 10.8.0.1: bytes=32 time=13ms TTL=63 RepIy from 10.8.0.1: bytes=32 time=21ms TTL=63	48		
		pre-compress bytes	Reply from 10.8.0.1: bytes=32 time=10ms TTL=63 Reply from 10.8.0.1: bytes=32 time=16ms TTL=63	0	
		post-compress bytes	Ping statistics for 10.8.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),	0	
		pre-decompress bytes	Approximate round trip times in milli-seconds:	0	
		post-decompress bytes	Minimum = 10ms, Maximum = 21ms, Average = 15ms	0	
			C:\Users\Root>		Refresh Statu

3.8.3 L2TP/PPTP

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





Test case: PPTP

On	Protocol ^	Name	Server	Username	Password	Firewall	Default R	oute Local IP
~	РРТР	3	comset.dyndns.org	test123	test123	~	×	
~	L2TP							
Add +								
PTP Advan	iced							
On	Name 🔿	Accept DN	S MTU	MRU	MPPE	MP	PE Stateful	Custom Options
-								debug;noipdefault;require-

Note: The Custom Options are based on your server.

Test case: L2TP

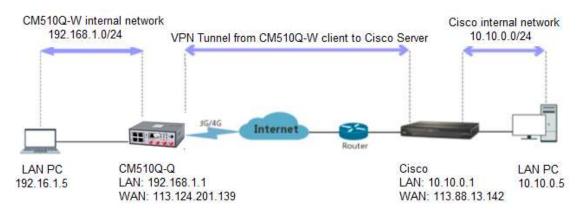
On	Protocol 个	Name	Server	Username	Password	Firewall	Default	Route Local IP
<i>v.</i>	PPTP	3	comset.dyndns.org	test123	test123	~	×	
	LZTP							
Add+								
PTP Advanced								
On	Name 🔿	Accept DNS	MTU	MRU	MPPE	Ν	1PPE Stateful	Custom Options
<i>x</i>	3	NO	1440	1440		*	£	debug:noipdefault mppe-128

Note: The Custom options are based on your server.



3.8.4 IPSec

IPSec between a COMSET Router and a Cisco Router



1) Cisco Configuration (main mode)

```
i
```

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

ļ

ļ

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

crypto ipsec nat-transparency spi-matching

ļ

2) COMSET Configuration

Navigate to VPN Tunnel > IPSec > Group Setup



Status	•		You haven't changed the default password for this router. To change router password <u>click here</u> .
Basic Network	•		
🗟 WLAN	•	IPSec	
Advanced Network	2	IPSec 1 IPSec 2 Schedule	
8 Firewall	•	Group Setup Basic Setup Advanced Setup	
VPN Tunnel	* /	Enable IPSec	
GRE		Enable iPSec	
OpenVPN Client PPTP/L2TP Client		IPSec Extensions	Normal T
		Local Security Gateway Interface	3G Cellular 🔻
Administration	3	Local Security Group Subnet/Netmask	192.168.1.0/24 ex. 192.168.1.0/24
		Local Security Firewalling	
		Remote Security Gateway IP/Domain	113.88.13.142
		Remote Security Group Subnet/Netmask	10.10.0/24 ex. 192.168.88.0/24
		Remote Security Firewalling	
		Save 🗸 Cancel 🗙	

Navigate to VPN Tunnel > IPSec > Basic Setup

Status	•		
Basic Network	•	IPSec 1 IPSec 2 Schedule	
🗢 WLAN	•	Group Setup Basic Setup Advanced Setup	
Advanced Network	•	Keying Mode	IKE with Preshared Key 🔹
🔯 Firewall	•	Phase 1 DH Group	Group 2 - modp1024 Y
VPN Tunnel	~		
GRE		Phase 1 Encryption	3DES (168-bit) *
OpenVPN Client PPTP/L2TP Client		Phase 1 Authentication	MD5 HMAC (96-bit) Y
		Phase 1 SA Life Time	28800 seconds
R Administration			
		Phase 2 DH Group	Group 2 - modp1024 🛛 🔻
		Phase 2 Encryption	3DES (168-bit) •
		Phase 2 Authentication	SHA1 HMAC (95-bi) *
		Phase 2 SA Life Time	3600 seconds
		Preshared Key	
(i) More Info		Save ✓ Cancel ×	

Navigate to VPN Tunnel > IPSec > Advanced Setup



Status	•	IPSec											
Basic Network	•	IPSec 1 IPSec 2 Schedule											
WLAN	•												
Advanced Network	•	Group Setup Basic Setup Advance	ed Setup										
🔯 Firewall		Aggressive Mode											
VPN Tunnel	•	Compress(IP Payload Compression)											
GRE OpenVPN Client PPTP/L2TP Client		Dead Peer Detection(DPD)											
- IPSec		ICMP Check		1									
R Administration	(*)	Check Period Time Interval		10	seconds								
		Check Timeout Count		3	Times								
		Check IP		10.10.0.1									
		IPSec Custom Options 1		rightid=%any									
		IPSec Custom Options 2											
		IPSec Custom Options 3											
		IPSec Custom Options 4											
		IPSec Lustom Options 4											
① More Info		Save Cancel x											
() More Info													
Status	•	Save 🗸 Cancel x						Wireless Mor		Access F	Point		
 Status Overview 	•						¢ ~	Wireless Moo Wireless Net Interface Stat	work Mode	Access F Auto Up (LAN			
 Status Overview Traffic Stats. 	•	Save 🗸 Cancel x	2			8	¢ ~	Wireless Net	work Mode	Auto	4)		
 Status Overview Traffic Stats. GPS Status 	•	Save J Cancel x VPN Status Name Protocol	L2TP				¢ ~	Wireless Net Interface Stat	work Mode	Auto Up (LAN Enabled	4)		
 Status Overview Traffic Stats. GPS Status Device List 		Save J Cancel x VPN Status Name Protocol Connection Status	L2TP Disconnec	ted		3	¢ ~	Wireless Net Interface Stat Radio	work Mode	Auto Up (LAN Enabled	4) - ~ vifi_015103_5G		
 Status Overview Traffic Stats. GPS Status 	•	Save J Cancel x VPN Status Name Protocol	L2TP Disconnec 0.0.0.0	ted		8	¢ ~	Wireless Net Interface Stat Radio SSID Broadcast	work Mode	Auto Up (LAN Enabled router-w	l) ↓ ✓ ↓ ↓ ↓ ✓		
 Status Overview Traffic Status GPS Status Device List 		Save J Cancel x VPN Status Name Protocol Connection Status IP Address Gateway	L2TP Disconnec 0.0.0.0 0.0.0.0				¢ ~	Wireless Net Interface Stat Radio SSID	work Mode	Auto Up (LAN Enabled router-w Enabled	l) ✓ ✓ ✓ 1		
 Status Overview Traffic Stats. GPS Status: Device List Basic Network WLAN 	*	Save , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1	L2TP Disconnec 0.0.0.0 0.0.00 Connected	1			¢ ~	Wireless Net Interface Stat Radio SSID Broadcast Security	work Mode us	Auto Up (LAN Enabled router-w Enabled disabled	l) ∽ ∽ ∽ 1		
 Status Overview Traffic Stats. GPS Status Device List Basic Network WLAN Advanced Network 	> > < >	Save J Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status	L2TP Disconnec 0.0.0.0 0.0.0.0 Connected 21 second	j s				Wireless Net Interface Stat Radio SSID Broadcast Security Channel	work Mode us	Auto Up (LAN Enabled router-w Enabled disabled 149 - 5.7	4) ✓ vifi_015103_5G ✓ f 745 GHz		
 Status Overview Traffic Stats. GPS Status: Device List Basic Network WLAN 	*	Save J Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec1 Phase 1 Status Phase 1 IKE	L2TP Disconnec 0.0,0,0 0.0,0,0 Connected 21 second: 3DES_CBC,	1	IPRF_HMAC_1			Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid	work Mode us	Auto Up (LAN Enabled router-w Enabled disabled 149 - 5.7. 80 MHz	4) ↓ ∽ ↓ ∽ 1 745 GHz bble		
 Status Overview Traffic Stats. GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall 	> > < >	Save J Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 IKE Phase 2 Status	L2TP Disconnect 0.0.0.0 0.0.0.0 Connectec 21 second 3DES_CBC, TUNNEL	s /HMAC_MD5_96/				Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference	work Mode us	Auto Up (LAN Enabled router-w Enabled disabled 149 - 5.7 80 MHz Accepta	4) ↓ ∽ ↓ ∽ 1 745 GHz bble		
 Status Overview Traffic Stats. GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Save J Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 IKE Phase 2 Status Phase 2 Status Phase 2 Status	L2TP Disconnec 0.0.0,0 Connected 21 second 3DES_CBC TUNNEL 3DES_CBC	j s				Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference Rate	work Mode us th Level	Auto Up (LAN Enabled router-w Enabled disabled 149 - 5.7 80 MHz Accepta	4) ↓ ∽ ↓ ∽ 1 745 GHz bble		
 Status Overview Traffic Stats. GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall 	2 2 2 2 2 2	Save , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 2 Status Phase 2 ESP IPSec Recv,	L2TP Disconnec 0.0.0,0 Connected 21 second 3DES_CBC, TUNNEL 3DES_CBC, 84 Bytes	s /HMAC_MD5_96/				Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference	work Mode us th Level	Auto Up (LAN Enabled router-w Enabled disabled 149 - 5.7 80 MHz Accepta	4) ↓ ∽ ↓ ∽ 1 745 GHz bble	0	£ ¥
 Status Overview Traffic Status GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Save J Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 IKE Phase 2 Status Phase 2 Status Phase 2 Status	L2TP Disconnec 0.0.0,0 Connected 21 second 3DES_CBC TUNNEL 3DES_CBC	s /HMAC_MD5_96/				Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference Rate	work Mode us th Level	Auto Up (LAN Enabled disabled 149 - 5.7 80 MHz Accepta 433 Mbp	4) ↓ ∽ ↓ ∽ 1 745 GHz bble	Đ	: V
 Status Overview Traffic Status GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Save , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 2 Status Phase 2 ESP IPSec Recv,	L2TP Disconnec 0.0.0,0 Connected 21 second 3DES_CBC, TUNNEL 3DES_CBC, 84 Bytes	s /HMAC_MD5_96/				Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference Rate Wireless (2)	work Mode us th Level 4 GHz)	Auto Up (LAN Enabled disabled 149 - 5.7 80 MHz Accepta 433 Mbp	4) V (f)_015103_5G V i 745 GHz ble a k01:51:03	0	
 Status Overview Traffic Status GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Save , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 2 Status Phase 2 ESP IPSec Recv,	L2TP Disconnec 0.0.0,0 Connected 21 second 3DES_CBC, TUNNEL 3DES_CBC, 84 Bytes	s /HMAC_MD5_96/		MD5/MODP_1(Wireless Net Interface Stal Radio SSID Broadcast Security Channel Wid Interference Rate Wireless (2 MAC Address Wireless Net	work Mode us th Level 2.4 GHz) s s te work Mode	Auto Up (LAN Enabled disabled disabled 149 - 52 80 MHz Accepta 433 Mep 340Ad9 Accept Auto	0) v vft_015103_5G v ft 1745 GHz bile 4 401:51:03 Point	٥	. v
 Status Overview Traffic Status GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Save J Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 Status Phase 2 Status	L2TP Disconnect 0.0.0 0.0.0 Connected 21 second 3DES_CBC TUNNEL 3DES_CBC 84 Bytes 84 Bytes	1 s /HMAC_MD5_96/ /HMAC_SHA1_96		MD5/MODP_1(224	Wireless Net Interface Stat Radio SID Broadcast Security Channel Channel Wirel Rate Wireless Kot Wireless Mot Wireless Mot	work Mode us th Level 2.4 GHz) s s te work Mode	Auto Up (LAN Enabled router-w Enabled 149 - 51 80 Mm; Accepta 433 Mep 34-0A-94 Access F Auto Up (LAN	0) v vf.015103_5G 1 745 cm 4 ble 4 4 401:51:03 Point 0)	0	8 V
 Status Overview Traffic Status GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Swe , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 2 Status Phase 2 Status Phase 2 ESP IPSec Recv, IPSec Send, IPSec Send,	L2TP Disconnect 0.0.00 Connected 21 second 30E5_CBC TUNNEL 30E5_CBC 64 Bytes 84 Bytes 340As940	8 s /HMAC_MD5_96/ /HMAC_SHA1_96 1:51:01		MD5/MODP_1(224	Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference Rate Wireless Mo Wireless Mo Wireless Ma Wireless Rat Radio	work Mode us th Level 2.4 GHz) s s te work Mode	Auto Up (LAN Enabled router-w Enabled 149 - 51 80 MHz Accepta 433 Mbp 34:0A:94 Access F Auto Up (LAN Enabled	i) ✓ vift_015103_5G i 745 cmc ble s 401:51:03 Joint 0 ✓	٥	E V
 Status Overview Traffic Status GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Swe , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 Status Phase 2 Status P	L2TP Disconnec 0.0.0 0.0.0 Connected 21 second 3055_CBC 3405_CBC 84 8yres 84 8yres 34:0A;94:0 br0 (LAN)	8 s /HMAC_MD5_96/ /HMAC_SHA1_96 1:51:01 - 192.168.1.1/24		MD5/MODP_1(224	Wireless Net Interface Stat Radio SID Broadcast Security Channel Channel Wirel Rate Wireless Kot Wireless Mot Wireless Mot	work Mode us th Level 2.4 GHz) s s te work Mode	Auto Up (LAN Enabled router-w Enabled 149 - 5:7 80 MHz Accepta 433 Mtp 34:0A:54 Accept Accept Accept Accept Accept Auto Up (LAN Enabled router-w	4) vift_015103_5G vift_015103_5G vift_015103 401:51:03	0	£ ¥
 Status Overview Traffic Status GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Swe , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 2 Status Phase 2 Status Phase 2 ESP IPSec Recv, IPSec Send, IPSec Send,	L2TP Disconnec 0.0.0 0.0.0 Connected 21 second 3055_CBC 3405_CBC 84 8yres 84 8yres 34:0A;94:0 br0 (LAN)	8 s /HMAC_MD5_96/ /HMAC_SHA1_96 1:51:01		MD5/MODP_1(224	Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference Rate Wireless Mo Wireless Mo Wireless Ma Wireless Rat Radio	work Mode us th Level 2.4 GHz) s s te work Mode	Auto Up (LAN Enabled router-w Enabled 149 - 51 80 MHz Accepta 433 Mbp 34:0A:94 Access F Auto Up (LAN Enabled	4) vift_015103_5G vift_015103_5G vift_015103 401:51:03	0	E 4
 Status Overview Traffic Stats. GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Swe , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 Status Phase 2 Status P	L2TP Disconnec 0.0.0 0.0.0 Connected 21 second 3055_CBC 3405_CBC 84 8yres 84 8yres 34:0A;94:0 br0 (LAN)	8 s /HMAC_MD5_96/ /HMAC_SHA1_96 1:51:01 - 192.168.1.1/24		MD5/MODP_1(224	Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference Rate Wireless (2 MAC Address Wireless Mot Wireless Net Interface Stat Radio SSID	work Mode us th Level 2.4 GHz) s s te work Mode	Auto Up (LAN Enabled router-w Enabled 149 - 5:7 80 MHz Accepta 433 Mtp 34:0A:54 Accept Accept Accept Accept Accept Auto Up (LAN Enabled router-w	0) ✓ vhf_015103_5G V f 1745 GHE ble st 401:51:03 Voint 0) ✓ vhf_015103 V 1005103 V	۵	E ×
 Status Overview Traffic Stats. GPS Status: Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Swe , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 Status Phase 2 Status P	L2TP Disconnec 0.0.0 0.0.0 Connected 21 second 3055_CBC 3405_CBC 84 8yres 84 8yres 34:0A:94:0 br0 (LAN)	8 s /HMAC_MD5_96/ /HMAC_SHA1_96 1:51:01 - 192.168.1.1/24		MD5/MODP_1(224	Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference Rate Wireless (2 MAC Address Wireless Mo Wireless Net Interface Stat SSID Broadcast	work Mode us th Level 2.4 GHz) s s te work Mode	Auto Up (LAN Enabled router-w Enabled disbited 149 - 51 80 MHz Accepta 433 Mbp 340A34 Access F Auto Up (LAN Enabled router-w Enabled	i) √ vrft_015103_5G √ i 745 GHE ble ko1:51:03 Point i √ i v v i v v i v v v v v v v v v v	0	E V
 Status Overview Traffic Stats. GPS Status GPS Status Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Swe , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 Status Phase 2 Status P	L2TP Disconnec 0.0.0 0.0.0 Connected 21 second 3055_CBC 3405_CBC 84 8yres 84 8yres 34:0A:94:0 br0 (LAN)	8 s /HMAC_MD5_96/ /HMAC_SHA1_96 1:51:01 - 192.168.1.1/24		MD5/MODP_1(224	Wireless Net Interface Stat Radio SSID Broadcast Security Channel Channel Wid Interference Rate Wireless (2 MAC Address Wireless Net Interface Stat Radio SSID Broadcast Security	work Mode us th Level L4 GHz) s fe Vork Mode us	Auto Up (LAN Enabled router-w- Enabled disabled 149 - 53 80 MHz Accepta 433 Mkp 34:0A:94 Accepta 433 Mkp Up (LAN Enabled disabled disabled	i) √ vrft_015103_5G √ i 745 GHE ble ko1:51:03 Point i √ i v v i v v i v v v v v v v v v v	0	E ¥
 Status Overview Traffic Stats. GPS Status: Device List Basic Network WLAN Advanced Network Firewall VPN Tunnel 	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Swe , Cancel x VPN Status Name Protocol Connection Status IP Address Gateway IPSec 1 Phase 1 Status Phase 1 Status Phase 2 Status P	L2TP Disconnec 0.0.0 0.0.0 Connected 21 second 3055_CBC 3405_CBC 84 8yres 84 8yres 34:0A:94:0 br0 (LAN)	8 s /HMAC_MD5_96/ /HMAC_SHA1_96 1:51:01 - 192.168.1.1/24		MD5/MODP_1(224	Wireless Net Interface Stat Radio SID Broadcast Security Channel Wireless (2 MAC Address Wireless Mo Wireless Mo Wireless Mo Wireless Mo SID Broadcast Security Channel	work Mode us th Level L4 GHz) s s se vork Mode us th	Auto Up (LAN Enabled router-w Enabled 149 - 51 80 Mm; Accepta 433 Mop 340A494 Access R Auto Up (LAN Enabled router-w Enabled router-w	() ✓ wrft_015103_5G 1 745 Gez ble 8 4:01:51:03 Point 0 ✓ 4: 0 ✓ 1 2: GHz	0	ε ν