

Industrial 5G Router CM950W

User Manual



Comset: 37/ 125 Highbury Rd, Burwood VIC 3125, Australia

Table of Contents

1 Product Introduction	5
1.1 Product Overview	5
1.2 Typical Application Diagram	5
1.3 Features	6
2 Hardware Installation	8
2.1 Overall Dimensions	8
2.2 Ports	10
2.3 Powering up the CM950W	12
2.4 SIM/UIM cards	12
2.5 Terminal block	12
2.6 Grounding	13
2.7 Power Supply	14
2.8 LED Description	14
3 Software configuration	16
3.1 Overview	16
3.2 How to log into the Router	16
3.3 Router status	19
3.3.1 Status overview	19
3.3.2 Network status	20
3.3.3 Firewall Status	23
3.3.4 Routes	23
3.3.5 System log	24
3.3.6 Kernel log	25
3.3.7 Reboot log	25
3.3.8 Realtime graphs	26
3.3.9 VPN	27
3.4 System Configuration	28
3.4.1 Setup wizard	28
3.4.2 System	31
3.4.3 Password	33
3.4.4 NTP	34
3.4.5 Backup/Restore	35
3.4.6 Upgrade	36
3.4.7 Reset	37
3.4.8 Reboot	38
3.5 Services configuration	38
3.5.1 ICMP check	38
3.5.2 VRRP	40
3.5.3 Failover (link backup)	41
3.5.4 DTU	43

3.5.5 SNMP	46
3.5.6 GPS (optional CM950W-G model)	48
3.5.7 SMS	50
3.5.8 VPN	59
3.5.8.1 IPSEC	59
3.5.8.2 PPTP	63
3.5.8.3 L2TP	66
3.5.8.4 OpenVPN	69
3.5.8.5 GRE tunnel	71
3.5.9 DDNS	72
3.5.10 Connect Radio Module	76
3.6 Network Configuration	77
3.6.1 Operation Mode	77
3.6.2 Mobile configuration	78
3.6.3 SIM Switch	79
3.6.4 LAN settings	80
3.6.5 Wired-WAN	85
3.6.6 WiFi Settings	85
3.6.6.1 WiFi General Configuration	86
3.6.6.2 WiFi Advanced Configuration	87
3.6.6.3 WiFi Interface Configuration	88
3.6.6.4 WiFi AP client	90
3.6.7 Interfaces Overview	92
3.6.8 Firewall	93
3.6.8.1 General Settings	93
3.6.8.2 Port Forwards	93
3.6.8.3 Traffic rules	94
3.6.8.4 DMZ	98
3.6.8.5 Security	99
3.6.9 Static Routes	101
3.6.10 Switch	102
3.6.11 DHCP and DNS	103
3.6.12 Diagnostics	105
3.6.13 Loopback Interface	106
3.6.14 Dynamic Routing	106
3.6.15 QoS	109

Copyright © COMSET 2024

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 20 cm 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

Chapter 1

1 Product Introduction

1.1 Product Overview

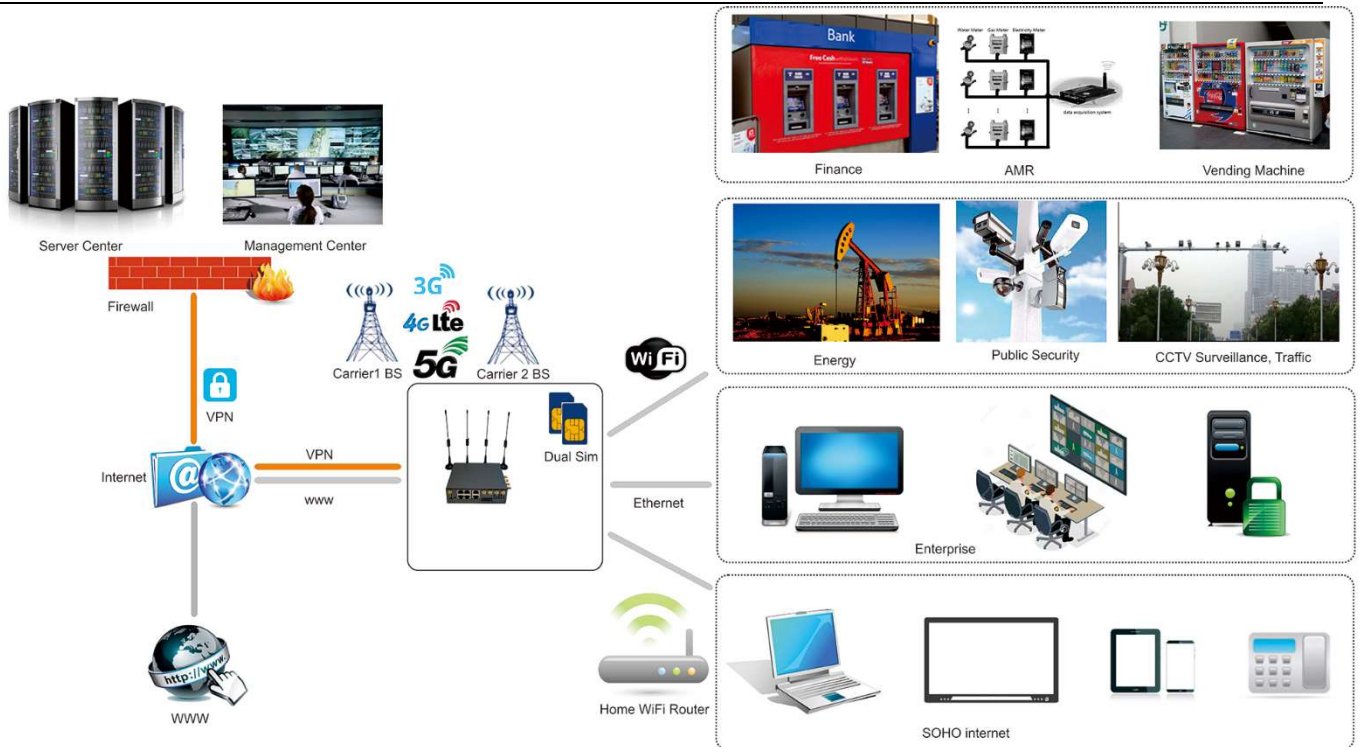
The Comset CM950W is a New Generation 5G Industrial Router. Supporting both 5G SA and 5G NSA modes, the CM950W delivers lightning internet speeds over the 5G networks. With two Gigabit Ethernet ports, two Fast Ethernet ports and dual band 2.4GHz and 5GHz WiFi, the CM950W provides a powerful and rapidly deployable internet solution to commercial customers and small to medium businesses.

The Comset CM950W is an Innovative Router powered by a Dual Core 880MHz CPU. It features dual SIM card slots for backup redundancy, 4 x LAN ports for fast wired connections, 1 Gigabit WAN/LAN port for automatic failover between NBN/ADSL and mobile 4G or 5G, as well as a GPIO with four digital input/output ports. Other features include VPN IPSEC, PPTP (Server and Client), L2TP and OpenVPN to establish a secure connection over the 4G/5G network.

The Comset CM950W is a Global Router, supporting frequencies across all major carriers worldwide. The innovative design, easy integration and rich built-in features make the CM950W the router of choice for a wide range of business and commercial applications, including SOHO, SMB, industrial automation, building automation, security, surveillance, transportation, health, mining and environmental monitoring.

1.2 Typical Application Diagram

The Comset CM950W 3G/4G/5G Router is suitable for a wide range of business, commercial and machine-to-machine applications (M2M). A good example is the connection of various IOT and M2M devices back to a server over a secure 5G connection using a secure VPN IPSEC tunnel, as illustrated below.



1.3 Features

The CM950W supports the following:

- Worldwide 5G and LTE-A coverage
- Both SA and NSA modes
- 2 x Gigabit Ethernet LAN ports & 2 x Fast Ethernet LAN ports
- 1 x Gigabit Ethernet WAN/LAN port
- Dual-band WiFi (802.11 a/b/g/n/ac, 2.4Ghz + 5Ghz)
- Dual SIM card slots
- USB3.0 port
- 6 x SMA standard detachable antennas included: 4 x cellular antennas and 2 x WiFi antennas
- Optimised EMC design
- Web management, SMS control, SSH/Telnet/Command, SNMP
- Always on-line: On-line detection and automatic redial
- Built-in transient and reverse polarity voltage protection, over-current and over-voltage

protection

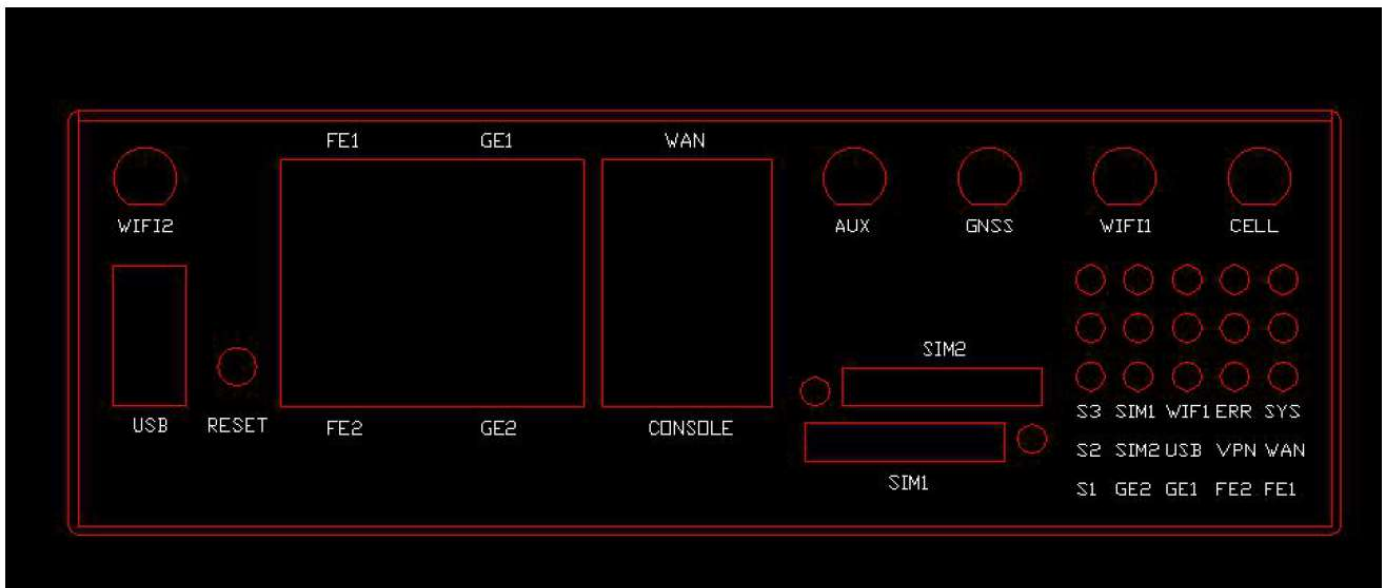
- Wide range power input (5-40VDC)
- Smart power management
- Multi-constellation GNSS receiver for applications requiring fast and accurate positioning
- Serial RS232 port
- 4 x Digital Input ports, that can also be used as Digital Output ports
- User friendly set-up wizard for easy configuration and setup
- Network traffic real-time graphs
- Network Diagnostic Tools (Ping, Traceroute and NSLookup)
- Advanced security, VPN, and stateful firewall to protect sensitive data
- Load balancing
- Robust Metal Case
- Desktop and Wall mount

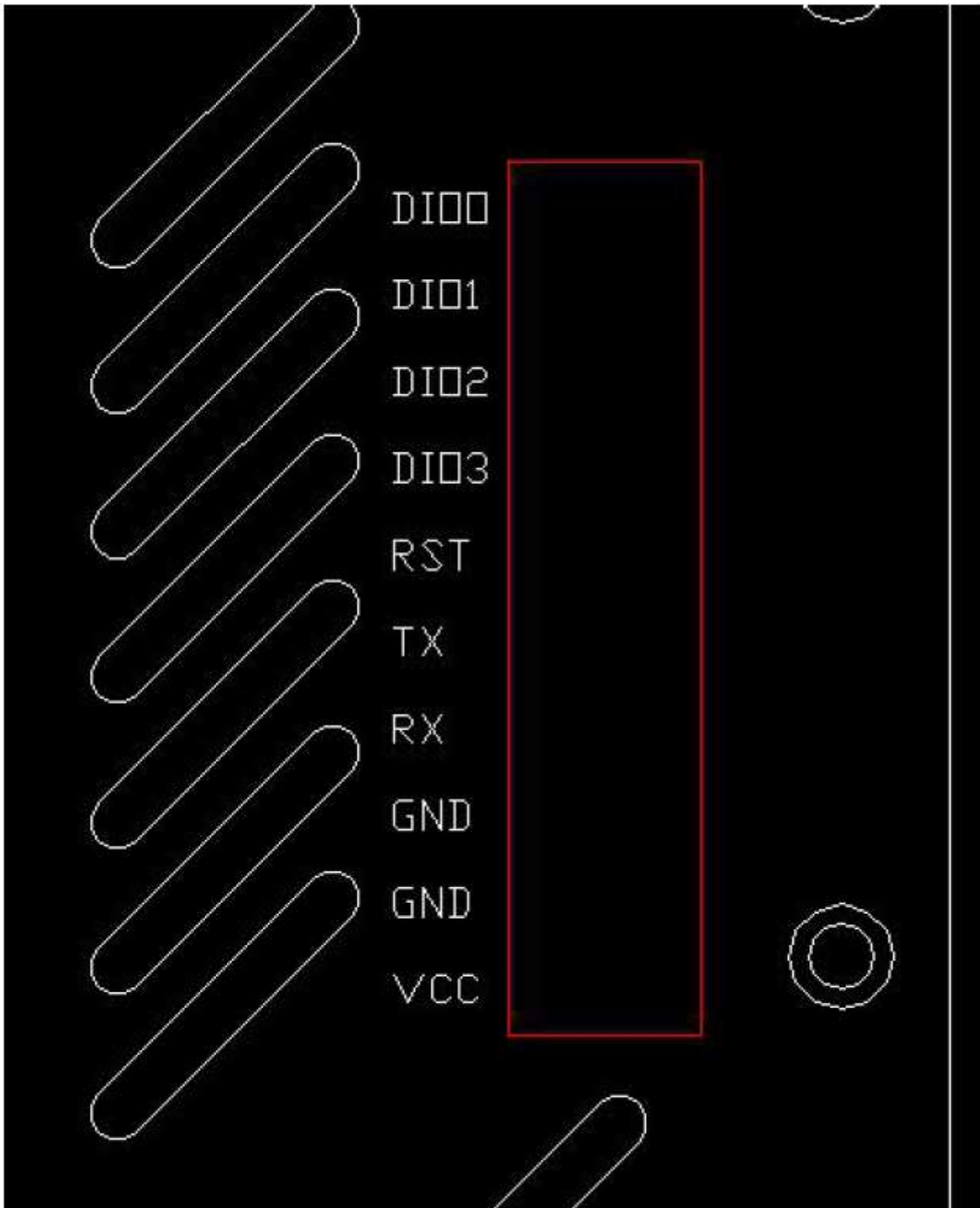
Chapter 2

2 Hardware Installation

1. Overall Dimensions
2. Accessories
3. Installation

2.1 Overall Dimensions







- VCC: DC wire positive pole. DC5~40V
- GND: DC wire ground
- GND: Serial ground
- RX: Serial receive
- TX: Serial transmit
- RST: Reset
- DIO0: digital I/O port 0
- DIO1: digital I/O port 1
- DIO2: digital I/O port 2
- DIO3: digital I/O port 3

Antenna Connection Table



Antenna Connectors	Remarks
Cell1	for cell main antenna 1
Cell2	for cell main antenna 2
Cell3	for cell main antenna 3
Cell4	for cell main antenna 4
WiFi1	for WiFi antenna 1
WiFi2	for WiFi antenna 2

2.3 Powering up the CM950W

Please ensure the SIM cards are inserted, and the antennas are connected before powering up the router.

2.4 SIM/UIM cards

1. Insert a paper clip into the hole next to the SIM tray and gently pull the SIM tray.
2. Place your SIM card into the tray. It will only fit in one position, because of the notch.
3. Insert the tray in the router. Make sure the tray is completely inserted.

2.5 Terminal block

Please refer to the following table on Pin description relating to the terminal block:



Attention:

1. *If you are not using the AC adapter supplied with the router, and if you wish to power up the unit using the terminal block, the power cable should be wired with the correct voltage polarity. Wrong wiring will destroy the equipment. Pin 1 and Pin 2 are reserved for power, where Pin 2 is “GND” and PIN 1 is power input “VCC” (DC5~40V).*

PIN	Signal	Description	Note
1	VCC	+5~40V DC Input	Current: 12V/1A
2	GND	Ground	
3	GND	Serial Ground	
4	RX	Receive Data	
5	TX	Transmit Data	
6	RST	Reset	To reset the router to factory default, simply short the RST pin with the GND Pin and hold for 3 sec. If you hold for 1 sec, the router will reboot.
7	DIO3	General Purpose I/O	
8	DIO2	General Purpose I/O	
9	DIO1	General Purpose I/O	
10	DIO0	General Purpose I/O	

I/O Terminal on router	Serial port RS232
Port 3 (GND)	Pin 5
Port 4 (RX)	Pin 2
Port 5 (TX)	Pin 3

Note: If you do not get a serial connection, try to switch Port 4 and Port 5.

2.6 Grounding

To ensure a safe operation, the cabinet where the router is installed should be grounded properly.

2.7 Power Supply

The CM950W supports a wide range of DC voltage between 5 VDC and 40 VDC. The router is supplied with a 12 VDC power adapter that is wired to VCC and GND on the terminal block.

PS: The CM950W router can also be powered via POE (Power over Ethernet). A passive POE adapter 12VDC or 24VDC is required.

2.8 LED Description

Please refer to the following table for LED description.

LED	Indication Light	Description
SYS	On for 25 seconds	On for 25 seconds after power up
	Blinks	System normal operation
	Off or still on after 25 seconds	System failure
FE 1 FE2 GE1 GE2	Blinks	Ethernet data transmission
	Off	No Ethernet connection
	On	Ethernet is connected
VPN	On	IPSec VPN tunnel set-up
	Off	IPsec VPN tunnel not set-up or Down/Inactive
SIM1 SIM2	Solid orange light	Cell connection is Up and now you have access to the Internet
	Flashing orange light	Attempting to establish an internet connection
2.4G 5G	On	WiFi Enabled
	Off	WiFi Disabled
WAN	Blinks	Ethernet data transmission
	Off	No Ethernet connection

	On	Ethernet is connected
PWR	On	Power is on
USB	On	External USB device is connected
GPS	On	GPS is online
S1	Off	No signal, or signal checking is not ready
S2	Blinks once every 2 seconds	Signal bar is 1
S3		Signal bar is 2
		Signal bar is 3

Chapter 3

3 Software configuration

1. *Overview*
2. *How to log into the router*
3. *How to configure the router*

3.1 Overview

The CM950W router has a built-in WEB interface. Below are instructions on how to access the web interface and configure the router.

3.2 How to log into the Router

3.2.1 Network Configuration

The router's default parameters are:

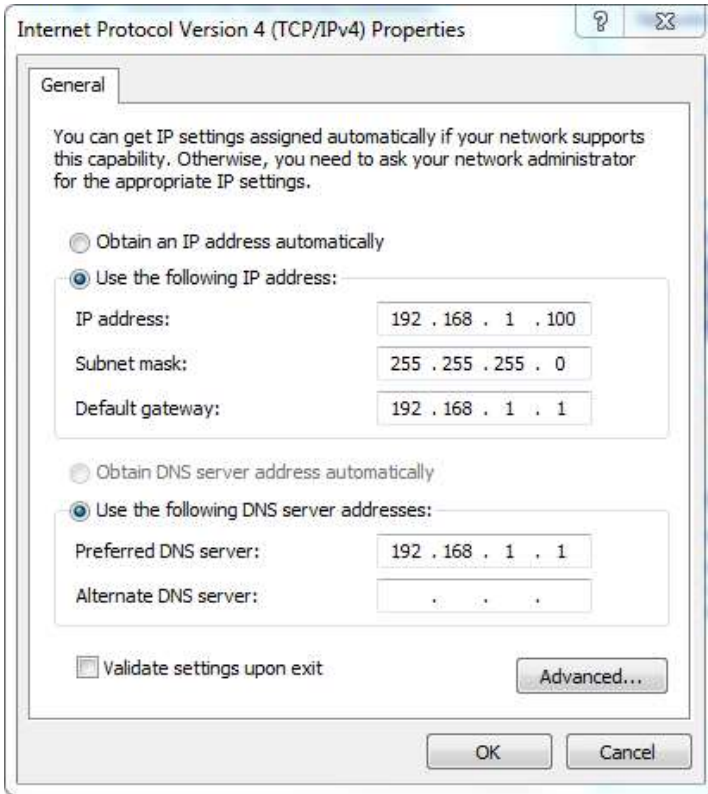
Default IP: 192.168.1.1

Subnet mask: 255.255.255.0

There are two ways to configure the IP address of your PC.

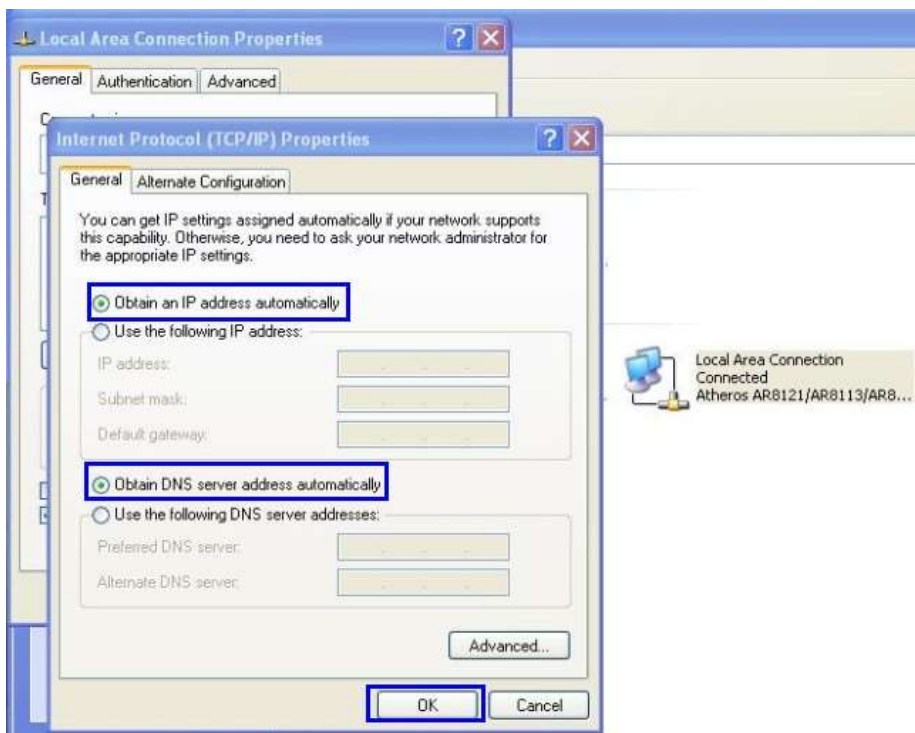
1) Manual settings

Set the PC IP to 192.168.1.xxx (xxx = 2~254), subnet mask: 255.255.255.0, default gateway: 192.168.1.1, primary DNS: 192.168.1.1.



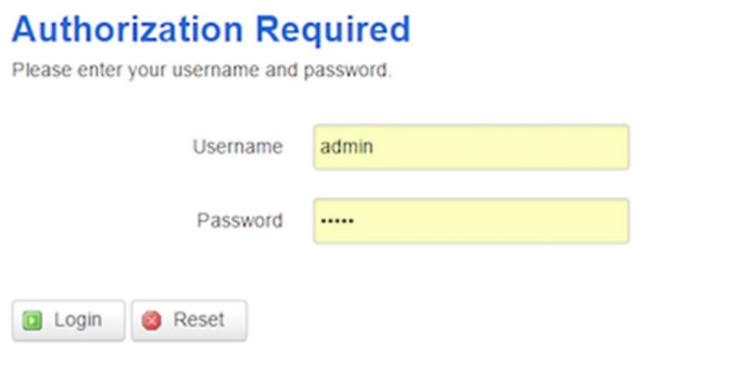
2) DHCP settings

Choose “Obtain an IP address automatically” and “Obtain DNS server address automatically”. Then click the ‘OK’ button.



3.2.2 Log into the router

- Open a Web browser and type in 192.168.1.1 into the address field, then press “Enter”.
- Type in the username and password. Both username and password are “admin”. Then click on the “Login” button.




The screenshot shows a web browser window displaying the router's login page. The page has a white background with a blue heading "Authorization Required" and a sub-heading "Please enter your username and password." Below this, there are two input fields: "Username" with the text "admin" and "Password" with five dots. At the bottom, there are two buttons: "Login" with a green arrow icon and "Reset" with a red circular arrow icon.
















To configure the router, you can skip the following section “Router status” and go straight to System> Setup wizard which is covered in section 3.4.1

3.3 Router status


3.3.1 Status overview

Click “Status” in the navigation bar, and then click “Overview”.


CM950W Industrial Router 5G/4G/3G
www.comset.com.au
your m2m specialist

<p>Status</p> <ul style="list-style-type: none"> Overview Network Firewall Routes System Log Kernel Log Reboot Log Realtime Graphs VPN <p>System</p> <p>Services</p> <p>Network</p> <p>Logout</p>	<h3>Status</h3> <h4>System</h4> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Hostname</td><td>CM950W</td></tr> <tr><td>SN</td><td>060410156A000B97</td></tr> <tr><td>Firmware Version</td><td>3.2.210</td></tr> <tr><td>Kernel Version</td><td>3.18.29</td></tr> <tr><td>Local Time</td><td>Thu Aug 20 12:12:31 2020</td></tr> <tr><td>Uptime</td><td>0h 3m 16s</td></tr> <tr><td>Load Average</td><td>1.29, 0.52, 0.20</td></tr> <tr><td>Port Status</td><td>      LAN1 LAN2 LAN3 LAN4 WAN </td></tr> </table> <h4>Mobile 1</h4> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Cellular Status</td><td>Up(SIM 1)</td></tr> <tr><td>IP Address</td><td>10.99.20.155/255.255.255.248</td></tr> <tr><td>DNS 1</td><td>10.4.130.164</td></tr> <tr><td>DNS 2</td><td>10.5.136.242</td></tr> </table>	Hostname	CM950W	SN	060410156A000B97	Firmware Version	3.2.210	Kernel Version	3.18.29	Local Time	Thu Aug 20 12:12:31 2020	Uptime	0h 3m 16s	Load Average	1.29, 0.52, 0.20	Port Status	     LAN1 LAN2 LAN3 LAN4 WAN	Cellular Status	Up(SIM 1)	IP Address	10.99.20.155/255.255.255.248	DNS 1	10.4.130.164	DNS 2	10.5.136.242
Hostname	CM950W																								
SN	060410156A000B97																								
Firmware Version	3.2.210																								
Kernel Version	3.18.29																								
Local Time	Thu Aug 20 12:12:31 2020																								
Uptime	0h 3m 16s																								
Load Average	1.29, 0.52, 0.20																								
Port Status	     LAN1 LAN2 LAN3 LAN4 WAN																								
Cellular Status	Up(SIM 1)																								
IP Address	10.99.20.155/255.255.255.248																								
DNS 1	10.4.130.164																								
DNS 2	10.5.136.242																								



IMEI/ESN	863305040124728
Sim Status	SIM Ready
Strength	 29 / 31, dBm : -55
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra #StaySafe Telstra", 13,
Sub Network Type	FDD LTE / NR5G-NSA
Location Area Code	304B
Cell ID	82CA621
MSISDN/IMSI	/ 505013529794072
Band	7
RSRP	-84 dBm
RSRQ	-9 dB
SINR	19 dB
5G RSRP	-92 dBm
5G RSRQ	-11 dB
5G SINR	102 dB

3.3.2 Network status

The Network status page consists of three tabs, detailing information about Mobile, WAN and LAN interfaces status.

Mobile interface page:

Status
Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout



Mobile WAN LAN

Mobile Status

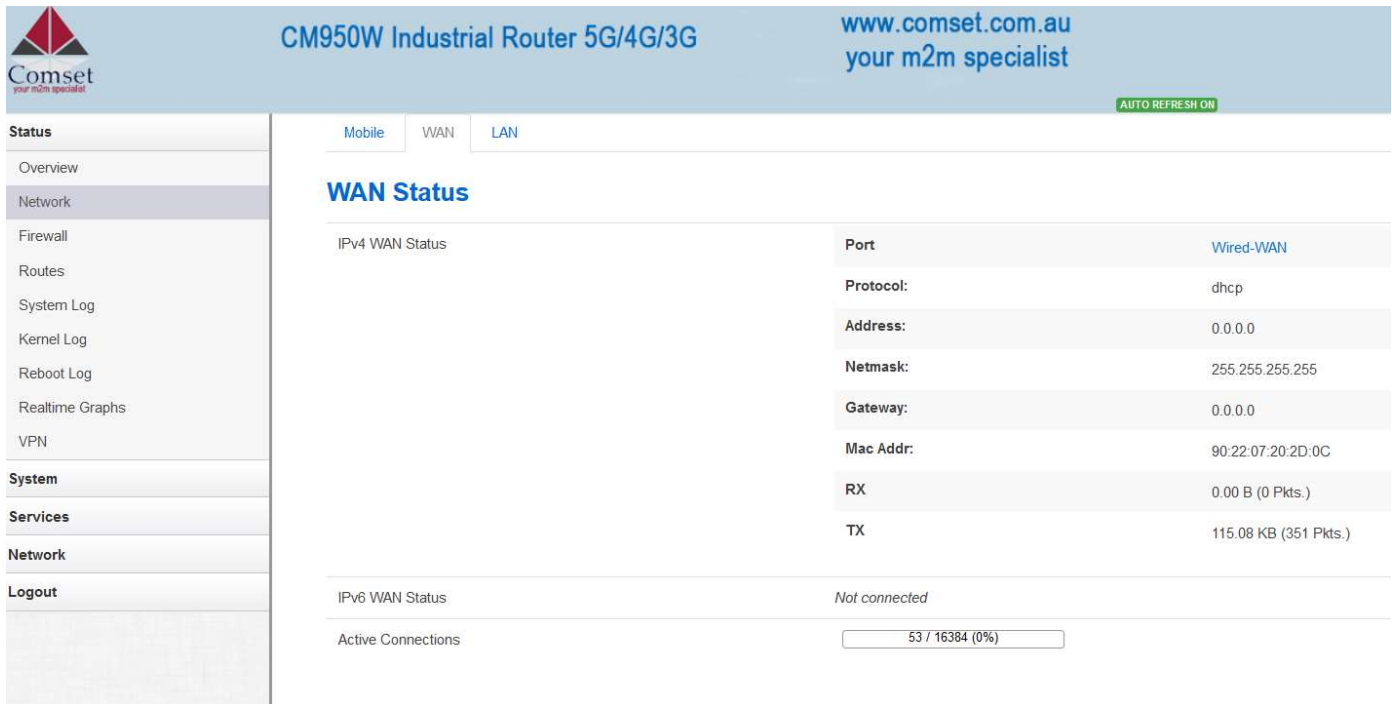
Mobile 1

Cellular Status	Up
Cell Modem	
IMEI/ESN	863305040124728
Sim Status	SIM Ready
Strength	27 / 31, dBm : -61
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra #StaySafe Telstra", 13,
Sub Network Type	FDD LTE / NR5G-NSA
Location Area Code	304B
Cell ID	82CA621
Band	7
RSRP	-88 dBm
RSRQ	-9 dB
SINR	19 dB
MSISDN/IMSI	/ 505013529794072
5G RSRP	-94 dBm
5G RSRQ	-12 dB
5G SINR	107 dB

Connection Status

Port	eth1
IPv4 Addr	10.99.20.155/29
DNS 1	10.4.130.164
DNS 2	10.5.136.242
Gateway	10.99.20.156
Uptime	0h 23m 23s
RX	1.57 MB (3852 Pkts.)
TX	1.33 MB (3736 Pkts.)

WAN status page:



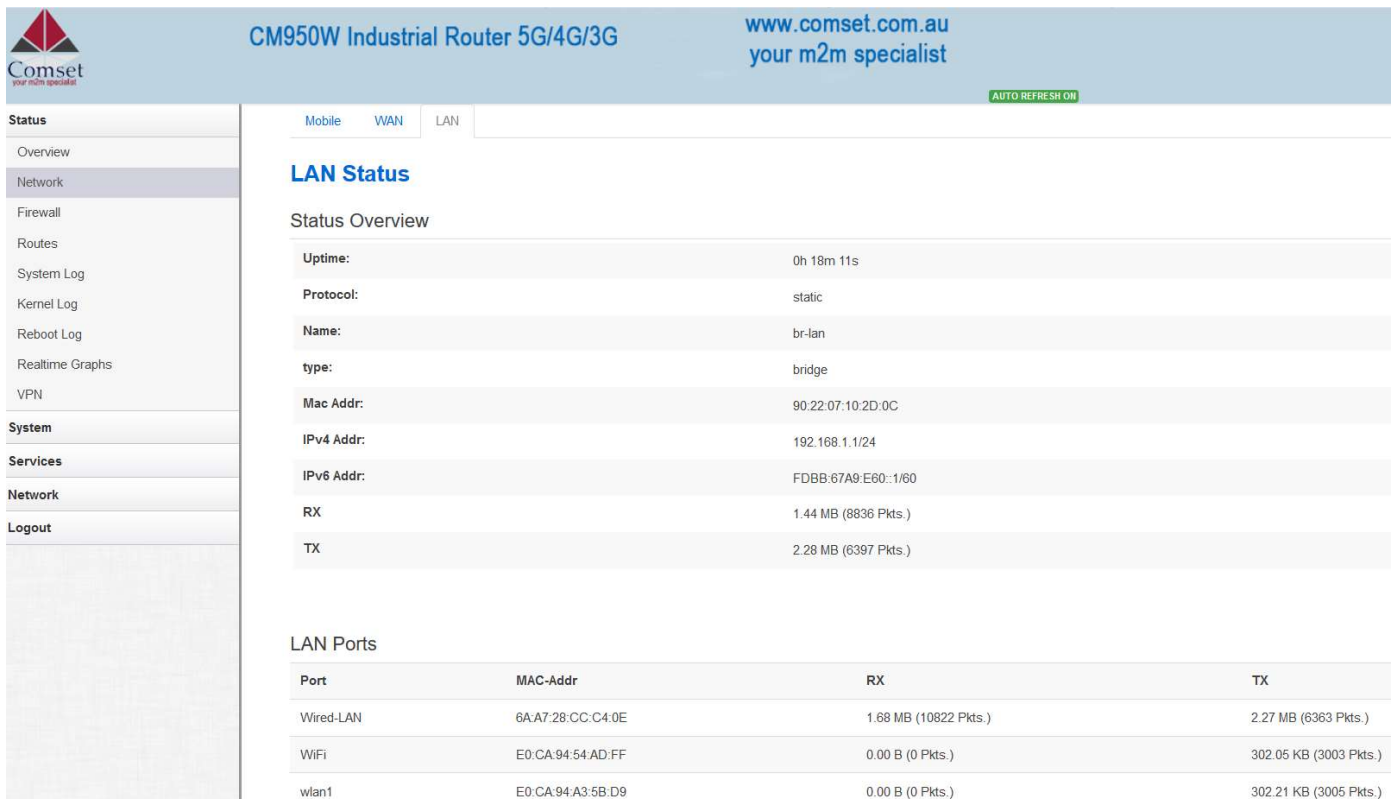
The screenshot shows the WAN Status page for the CM950W Industrial Router. The page header includes the Comset logo, the router model 'CM950W Industrial Router 5G/4G/3G', and the website 'www.comset.com.au your m2m specialist'. A navigation menu on the left lists various system and network functions. The main content area has tabs for 'Mobile', 'WAN', and 'LAN', with 'WAN' selected. The 'WAN Status' section is titled and contains two sub-sections: 'IPv4 WAN Status' and 'IPv6 WAN Status'. The IPv4 status is detailed in a table, and the IPv6 status is noted as 'Not connected'. A summary bar at the bottom shows 'Active Connections' as 53 / 16384 (0%).

Port	Wired-WAN
Protocol:	dhcp
Address:	0.0.0.0
Netmask:	255.255.255.255
Gateway:	0.0.0.0
Mac Addr:	90:22:07:20:2D:0C
RX	0.00 B (0 Pkts.)
TX	115.08 KB (351 Pkts.)

IPv6 WAN Status: Not connected

Active Connections: 53 / 16384 (0%)

LAN status page:



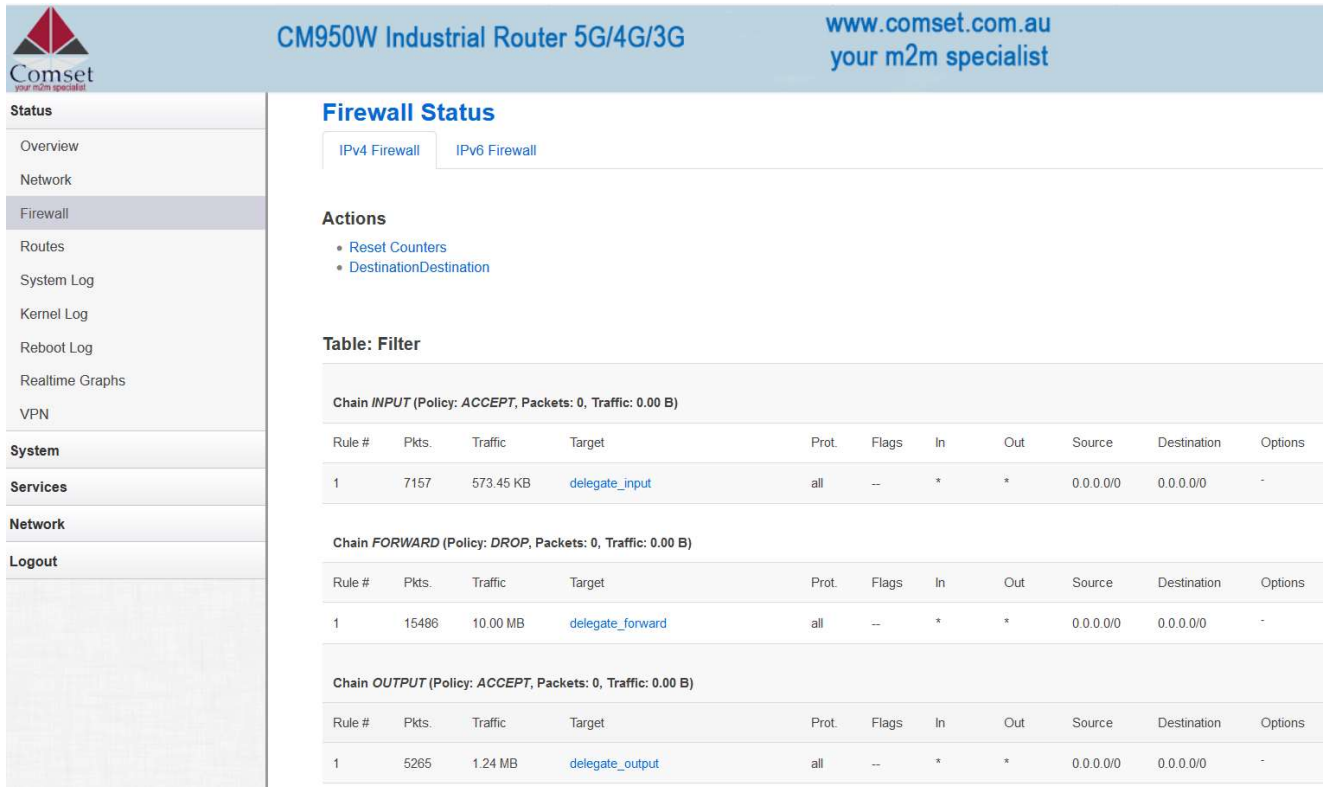
The screenshot shows the LAN Status page for the CM950W Industrial Router. The page header is identical to the WAN status page. The navigation menu on the left is the same. The main content area has tabs for 'Mobile', 'WAN', and 'LAN', with 'LAN' selected. The 'LAN Status' section is titled and contains a 'Status Overview' table and a 'LAN Ports' table. The Status Overview table lists various parameters like Uptime, Protocol, Name, type, Mac Addr, IPv4 Addr, IPv6 Addr, RX, and TX. The LAN Ports table lists details for Wired-LAN, WiFi, and wlan1 ports, including MAC-Addr, RX, and TX statistics.

Uptime:	0h 18m 11s
Protocol:	static
Name:	br-lan
type:	bridge
Mac Addr:	90:22:07:10:2D:0C
IPv4 Addr:	192.168.1.1/24
IPv6 Addr:	FDBB:67A9:E60::1/60
RX	1.44 MB (8836 Pkts.)
TX	2.28 MB (6397 Pkts.)

Port	MAC-Addr	RX	TX
Wired-LAN	6A:A7:28:C4:0E	1.68 MB (10822 Pkts.)	2.27 MB (6363 Pkts.)
WiFi	E0:CA:94:54:AD:FF	0.00 B (0 Pkts.)	302.05 KB (3003 Pkts.)
wlan1	E0:CA:94:A3:5B:D9	0.00 B (0 Pkts.)	302.21 KB (3005 Pkts.)

3.3.3 Firewall Status

The Firewall status page shows the IPv4 and IPv6 rules and counters. Here, you can reset the counters and restart the firewall functionality.



The screenshot shows the Firewall Status page. The page title is "Firewall Status" and it includes tabs for "IPv4 Firewall" and "IPv6 Firewall". The "IPv4 Firewall" tab is active. Under "Actions", there are links for "Reset Counters" and "DestinationDestination". The "Table: Filter" section displays three chains: INPUT, FORWARD, and OUTPUT. Each chain has a table of rules with columns for Rule #, Pkts, Traffic, Target, Prot., Flags, In, Out, Source, Destination, and Options.

Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)											
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options	
1	7157	573.45 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-	

Chain FORWARD (Policy: DROP, Packets: 0, Traffic: 0.00 B)											
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options	
1	15486	10.00 MB	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-	

Chain OUTPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)											
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options	
1	5265	1.24 MB	delegate_output	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-	

3.3.4 Routes

The Routes page shows rules which are currently active on the router. An ARP table is displayed as well.

Status
Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.1.165	34:99:71:d5:03:79	br-lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
ifmobile	0.0.0.0/0	10.99.20.156	11	main
ifmobile	10.99.20.152/29		11	main
ifmobile	10.99.20.156		11	main
lan	192.168.1.0/24		0	main

Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	fdbb:67a9:e60::/64		1024	main
lan	:::1		0	local
(eth0)	:::8		256	local

3.3.5 System log

This page shows the system log from system boot up. The system log resets when the router is restarted. You can export the system log by clicking the button “Export Syslog”.

Status
Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout

System Log [Last System Log](#)

System Log

[Export syslog](#)

```
Thu Aug 20 12:09:57 2020 user.notice DEBUG: collect module information 1
Thu Aug 20 12:09:57 2020 user.notice dtu: Starting...
Thu Aug 20 12:09:57 2020 user.notice CM: clear_dev_status 1
Thu Aug 20 12:09:58 2020 user.notice dtu: done1...
Thu Aug 20 12:09:58 2020 user.notice cellmodem 1: Stop
Thu Aug 20 12:09:58 2020 user.notice DEBUG: firewall reload
Thu Aug 20 12:09:58 2020 user.notice DEBUG: clear conntrack
Thu Aug 20 12:09:58 2020 user.emerg syslog: conntrack v1.4.2 (conntrack-tools): 1 flow entries have been shown.
Thu Aug 20 12:09:58 2020 user.notice DEBUG: firewall reload done
Thu Aug 20 12:09:58 2020 user.notice dtu: Starting...
Thu Aug 20 12:09:58 2020 user.emerg syslog: DTU2_center1
Thu Aug 20 12:09:58 2020 user.notice dtu: done1...
Thu Aug 20 12:09:58 2020 user.notice DEBUG: firewall reload
Thu Aug 20 12:09:58 2020 user.notice DEBUG: clear conntrack
Thu Aug 20 12:09:58 2020 user.emerg syslog: conntrack v1.4.2 (conntrack-tools): 1 flow entries have been shown.
Thu Aug 20 12:09:58 2020 user.notice DEBUG: firewall reload done
Thu Aug 20 12:09:58 2020 user.notice gpsh: Starting...
Thu Aug 20 12:09:58 2020 user.notice cellmodem : Stop
Thu Aug 20 12:09:58 2020 user.notice gpsh: done1...
Thu Aug 20 12:09:59 2020 user.notice cellmodem: 1 Starting...
Thu Aug 20 12:09:59 2020 user.notice cellmodem: 1 start done...
Thu Aug 20 12:09:59 2020 user.notice IPSFC: insec start
```


3.3.6 Kernel log

This page shows the kernel log from system boot up. This log is not saved when the router is restarted. It can be exported by clicking the button “Export Log”.

Status

- Overview
- Network
- Firewall
- Routes
- System Log
- Kernel Log**
- Reboot Log
- Realtime Graphs
- VPN

System

Services

Network

Logout

Kernel Log [Last Kernel Log](#)

Kernel Log

[Export log](#)

```
[ 0.000000] Linux version 3.18.29 (denty@denty-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r49294) ) #1259 SMP Thu Aug 20 10:09:57 CST 2020
[ 0.000000] SoC Type: MediaTek MT7621 ver:1 eco:3
[ 0.000000] bootconsole [early0] enabled
[ 0.000000] CPU0 revision is: 0001992f (MIPS 1004Kc)
[ 0.000000] MIPS: machine is mt7621_model_2
[ 0.000000] Determined physical RAM map:
[ 0.000000] memory: 08000000 @ 00000000 (usable)
[ 0.000000] Initrd not found or empty - disabling initrd
[ 0.000000] Zone ranges:
[ 0.000000] Normal [mem 0x00000000-0x07ffffff]
[ 0.000000] HighMem empty
[ 0.000000] Movable zone start for each node
[ 0.000000] Early memory node ranges
[ 0.000000] node 0: [mem 0x00000000-0x07ffffff]
[ 0.000000] Initmem setup node 0 [mem 0x00000000-0x07ffffff]
[ 0.000000] On node 0 totalpages: 32768
[ 0.000000] free_area_init_node: node 0, pgdat 80369c40, node_mem_map 81000000
[ 0.000000] Normal zone: 256 pages used for memmap
```

3.3.7 Reboot log

This page shows the reboot log.

Status

- Overview
- Network
- Firewall
- Routes
- System Log
- Kernel Log
- Reboot Log**
- Realtime Graphs
- VPN

System

Services

Network

Logout

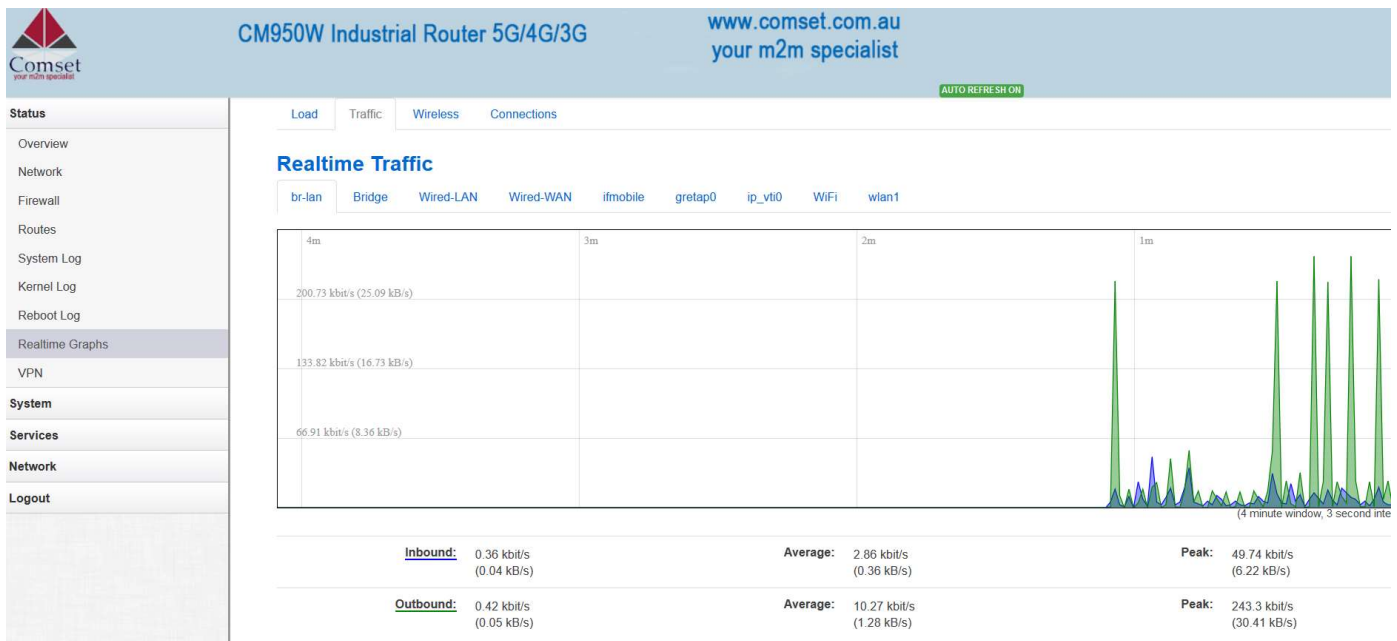
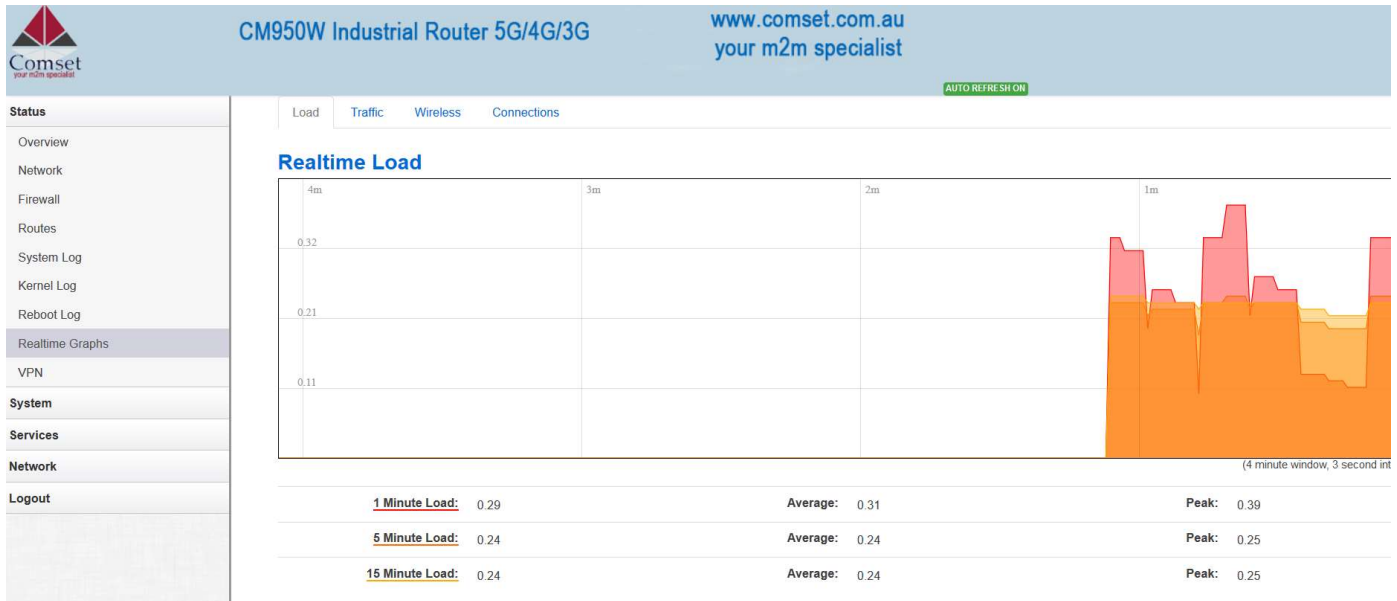
Reboot Log

[Clear log](#)

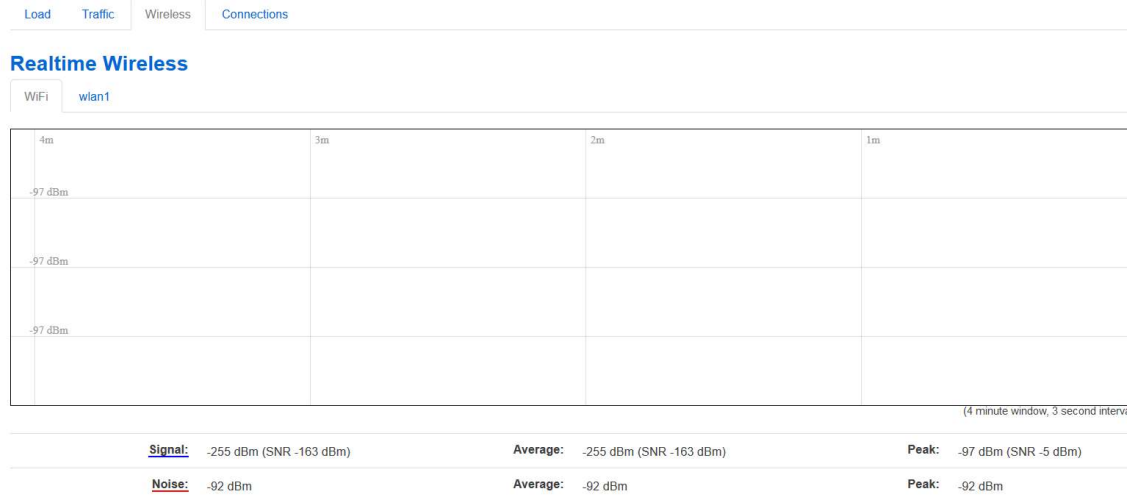
Thu Aug 20 02:09:56 UTC 2020 : Router boots up

3.3.8 Realtime graphs

The Realtime Graphs page shows the system load and interfaces traffic in realtime.



Status
Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout



Status
Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout



3.3.9 VPN

This page shows the status of VPN IPsec, IPsec log, OpenVPN, PPTP tunnel, L2TP tunnel and Openconnect.



The screenshot shows the web interface of the CM950W Industrial Router. The header includes the Comset logo and the text "CM950W Industrial Router 5G/4G/3G" and "www.comset.com.au your m2m specialist". The left sidebar contains a navigation menu with sections: Status, System, Services, Network, and Logout. The "Status" section is expanded, showing options like Overview, Network, Firewall, Routes, System Log, Kernel Log, Reboot Log, Realtime Graphs, and VPN. The "VPN" section is selected. The main content area shows the "IPSec Status" page with a "Refresh" button and a large empty box below it. The top navigation bar includes tabs for IPSec, IPSec Log, OpenVPN, PPTP tunnel, L2TP tunnel, and Openconnect.

3.4 System Configuration

3.4.1 Setup wizard

When you login to the router for the first time, you will need to configure the Setup Wizard page. This page consists of 4 sections:

- General
- Mobile
- LAN
- WiFi

Status	Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi
System	Step - General
Setup Wizard	First, let's change your router password from the default one.
System	Password Settings
Password	New password <input type="password"/>
Software	Confirm new password <input type="password"/>
Startup	System Settings
NTP	Current system time Sat Aug 22 12:14:58 2020 <input type="button" value="Sync with browser"/>
Backup/Restore	Timezone Australia/Melbourne <input type="text"/>
Upgrade	Hostname CM950W <input type="text"/>
Reset	Language English <input type="text"/>
Reboot	
Services	
Network	
Logout	

Fill in parameters as required, then click “Save & Next”.

Note: Pressing “Save & Next” will save the configuration and jump to the next page. All configurations will be applied after you click the button “Finish” at the final step “Step4-WiFi”.

Status	Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi
System	Mobile Configuration
Setup Wizard	SIM 1 SIM 2
System	Enable <input checked="" type="checkbox"/>
Password	Mobile connection DHCP mode <input type="text"/>
Software	PIN code <input type="text"/>
Startup	Dialing number *99# <input type="text"/>
NTP	APN telstra.internet <input type="text"/>
Backup/Restore	Authentication method None <input type="text"/>
Upgrade	Dual APN support <input type="checkbox"/>
Reset	Network Type automatic <input type="text"/>
Reboot	MTU 1500 <input type="text"/>
Services	
Network	
Logout	

- **Enable:** Enable mobile network.
- **Mobile connection:** Select a suitable mode for the mobile connection. The default value is 'DHCP mode'.
- **APN:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider.
- **PIN code:** Most SIM cards do not have a PIN code; in which case you leave this field blank.
- **Dialing number:** Fill in the related value. The default value is *99#. This can be obtained from your carrier or SIM Card Provider.
- **Authentication method:** There are three options to choose from (None, PAP, CHAP). Please confirm with your carrier the type of authentication. Default is *None*.
- **Username:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider.
- **Note:** If your SIM card has no username, please input the default value, otherwise the router may not dialup. If the Authentication method is 'None', this option will not appear.
- **Password:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider.
- **Network Type:** Different Cell Modems support different types. The default value is *Automatic*.
- **MTU:** Maximum Transmission Unit. It is the maximum size of packets transmitted on the network. The default value is 1500. Please configure it to optimise your own network.
- **Note: Do the same for SIM 2.**
- When finished, click "Save & Next"

Status	Step 1 - General	Step 2 - Mobile	Step 3 - LAN	Step 4 - WiFi
System				
Setup Wizard				
System				
Password				
Software				
Startup				
NTP				
Backup/Restore				
Upgrade				
Reset				
Reboot				
Services				
Network				
Logout				

Step - LAN

Here we will setup the basic settings of a typical LAN configuration. The wizard will cover 2 basic configurations: static IP address LAN and DHCP client.

General Configuration

IP address

Netmask

Enable DHCP

Start

Limit

Lease time

Fill in parameters as required. When finished, click "Save & Next"

System

Setup Wizard

System

Password

Software

Startup

NTP

Backup/Restore

Upgrade

Reset

Reboot

Services

Network

Logout

Step - Wireless

Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters, like SSID, encryption, etc. your connection will be dropped and you will have to reconnect with a new set of parameters.)

WiFi Configuration

Enable wireless

SSID

Transmit Power

Band

HT mode (802.11n)

Channel

Encryption

Cipher

Key

Country Code

Fill in parameters as required, then press “Finish”.

3.4.2 System

Status

System

Setup Wizard

System

Password

Software

Startup

NTP

Backup/Restore

Upgrade

Reset

Reboot

Services

Network

Logout

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings **Logging** Language

Local Time Sat Aug 22 12:30:03 2020

Hostname

Timezone

General Settings

Local Time

This page shows the system time. You can sync the time with the browser by clicking the button “Sync with browser”.

Hostname

It is the router’s name. The default name is “CM950W”

Time zone

Select a suitable time zone. The default value is “Australia/Melbourne”

Logging

Status	<h3>System</h3> <p>Here you can configure the basic aspects of your device like its hostname or the timezone.</p> <h4>System Properties</h4> <p>General Settings Logging Language</p> <p>System log buffer size <input type="text" value="64"/></p> <p>External system log server <input type="text" value="0.0.0.0"/></p> <p>External system log server port <input type="text" value="514"/></p> <p>Log output level <input style="border: none; border-bottom: 1px solid #ccc; padding: 2px 5px;" type="text" value="Debug"/> ▾</p> <p>Cron Log Level <input style="border: none; border-bottom: 1px solid #ccc; padding: 2px 5px;" type="text" value="Normal"/> ▾</p> <p>Record Cell Status <input type="checkbox"/></p> <p style="text-align: right;"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </p>
System	
Setup Wizard	
System	
Password	
Software	
Startup	
NTP	
Backup/Restore	
Upgrade	
Reset	
Reboot	
Services	
Network	
Logout	

System log buffer size

The unit is KB. The default value is 64 KB. If the actual log size exceeds the set value, then the oldest log lines will be dropped.

External system log server

Here you enter the IP address of the external log server. You can setup a Linux machine with syslogd run as a log server.

External system log server port

This is the UDP port of the external log server.

Log output level

This is the Log level. The default is ‘Debug’ with highest level. Emergency is the lowest level.

Cron log level




It is the log level to process Crond.

Language




Language

The default language is “English”.

3.4.3 Password

Status System Setup Wizard System Password Software Startup NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	Web Account SSH Account Guest Account
	<h4>Web Account</h4> <p>Changes the administrator username and password</p>
	Current username <input type="text"/>
	Current password <input type="password"/> 
	New username <input type="text"/>
	Password <input type="password"/> 
	Confirmation <input type="password"/> 
	<div style="text-align: right;"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div>

Here you can change the administrator’s password for accessing the device, as well as changing SSH username and password and Guest’s username and password. Click the “eye button” to show the new password you entered.

Status System Setup Wizard System Password Software Startup NTP Backup/Restore Upgrade Reset Reboot Services Network Logout	Web Account SSH Account Guest Account
	<h4>SSH Account</h4> <p>Changes SSH username and password</p>
	Current username <input type="text"/>
	Current password <input type="password"/> 
	New username <input type="text"/>
	Password <input type="password"/> 
	Confirmation <input type="password"/> 
	<div style="text-align: right;"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div>

Status	Web Account SSH Account Guest Account
System	<h3 style="color: #0070c0;">Guest Password</h3> <p>Changes the guest password</p> <p>Enable guest <input type="checkbox"/></p> <p>Password <input style="width: 150px;" type="password"/></p> <p>Confirmation <input style="width: 150px;" type="password"/></p> <div style="text-align: right; margin-top: 20px;"> Save & Apply Save Reset </div>
Setup Wizard	
System	
Password	
Software	
Startup	
NTP	
Backup/Restore	
Upgrade	
Reset	
Reboot	
Services	
Network	
Logout	

3.4.4 NTP

Status	<h3 style="color: #0070c0;">NTP</h3> <p>NTP Configuration</p> <h4 style="color: #0070c0;">Time Synchronization</h4> <p>Enable NTP client <input checked="" type="checkbox"/></p> <p>Provide NTP server <input type="checkbox"/></p> <p>NTP sync count <input type="text" value="0"/></p> <p>NTP sync interval(min) <input type="text"/></p> <p>NTP server candidates</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">0.au.pool.ntp.org</td> <td style="text-align: right; padding: 2px;">✖</td> </tr> <tr> <td style="padding: 2px;">1.au.pool.ntp.org</td> <td style="text-align: right; padding: 2px;">✖</td> </tr> <tr> <td style="padding: 2px;">2.au.pool.ntp.org</td> <td style="text-align: right; padding: 2px;">✖</td> </tr> <tr> <td style="padding: 2px;">3.au.pool.ntp.org</td> <td style="text-align: right; padding: 2px;">+</td> </tr> </table>	0.au.pool.ntp.org	✖	1.au.pool.ntp.org	✖	2.au.pool.ntp.org	✖	3.au.pool.ntp.org	+
0.au.pool.ntp.org	✖								
1.au.pool.ntp.org	✖								
2.au.pool.ntp.org	✖								
3.au.pool.ntp.org	+								
System									
Setup Wizard									
System									
Password									
Software									
Startup									
NTP									
Backup/Restore									
Upgrade									
Reset									
Reboot									
Services									
Network									
Logout									

NTP is Network Timing Protocol.

- **Enable NTP client**

The default value is checked. The router acts as an NTP client.

- **Provide NTP server**

The default value is unchecked. The router acts as an NTP server.



- **NTP sync count**

This is the NTP running counts, after the router is connected to the internet. 0 means infinite.

- **NTP sync interval (min)**

This is the interval time between NTP synchronisation.

- **NTP server candidates**

This is the NTP server list. Multiple NTP servers are accepted. You can click the button  to delete an entry or click the button  to add a new entry.

3.4.5 Backup/Restore

Status	<h2>Configuration files operations</h2> <h3>Backup</h3> <p>Download a tar archive of the current configuration files.</p> <p>Download backup configuration archive : <input type="button" value="Download"/></p> <h3>Restore</h3> <p>To restore configuration files, you can upload a previously generated backup archive here.</p> <p>Restore backup configuration archive : <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload..."/></p>
System	
Setup Wizard	
System	
Password	
Software	
Startup	
NTP	
Backup/Restore	
Upgrade	
Reset	
Reboot	
Services	
Network	
Logout	

- To back up the configuration files, click the button “Download”. Then an archive file will be generated and downloaded to your PC automatically.
- To restore the configuration files, click the button “Choose File” and select an archived configuration file. Click the button “Upload”. The system will upload the file and then restart the router.

3.4.6 Upgrade



The screenshot shows the web interface for the CM950W Industrial Router. The header includes the Comset logo, the product name "CM950W Industrial Router 5G/4G/3G", and the website "www.comset.com.au your m2m specialist". A notification "UNSAVED CHANGES: 7" is visible in the top right. On the left is a navigation menu with categories: Status, System (Setup Wizard, System, Password, Software, Startup, NTP, Backup/Restore, Upgrade, Reset, Reboot), Services, Network, and Logout. The main content area is titled "System upgrade" and contains the following text: "Upload a sysupgrade-compatible image here to replace the running firmware. Check 'Keep settings' to retain the current configuration (requires an compatible firmware image)". Below this are two checkboxes: "Keep settings:" (unchecked) and "Safe upgrade:" (checked). The "Image:" field shows "Browse..." (highlighted), "No file selected.", and an "Upload image..." button.

Upload a system compatible firmware to replace the current firmware. The default value for “Keep settings” is checked, which means the existing configuration will be kept after the system upgrade, otherwise the router will be reset to factory settings. We recommend to un-check “Keep settings” to prevent conflicting parameters after the firmware upgrade.

Click the button “Browse” and select a compatible firmware, then click the button “Upload image”. The router will run a basic check of the file. If it is an incompatible file, an error message will appear like this one below:

System upgrade

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an compatible firmware image).

Keep settings:

Image: no file selected

The uploaded image file does not contain a supported format. Make sure that you choose the generic image format for your Router.

If the firmware file is ok, a verification message will appear. Click the button “Proceed”, and the system will restart after a few minutes.

Upgrade Firmware - Verify

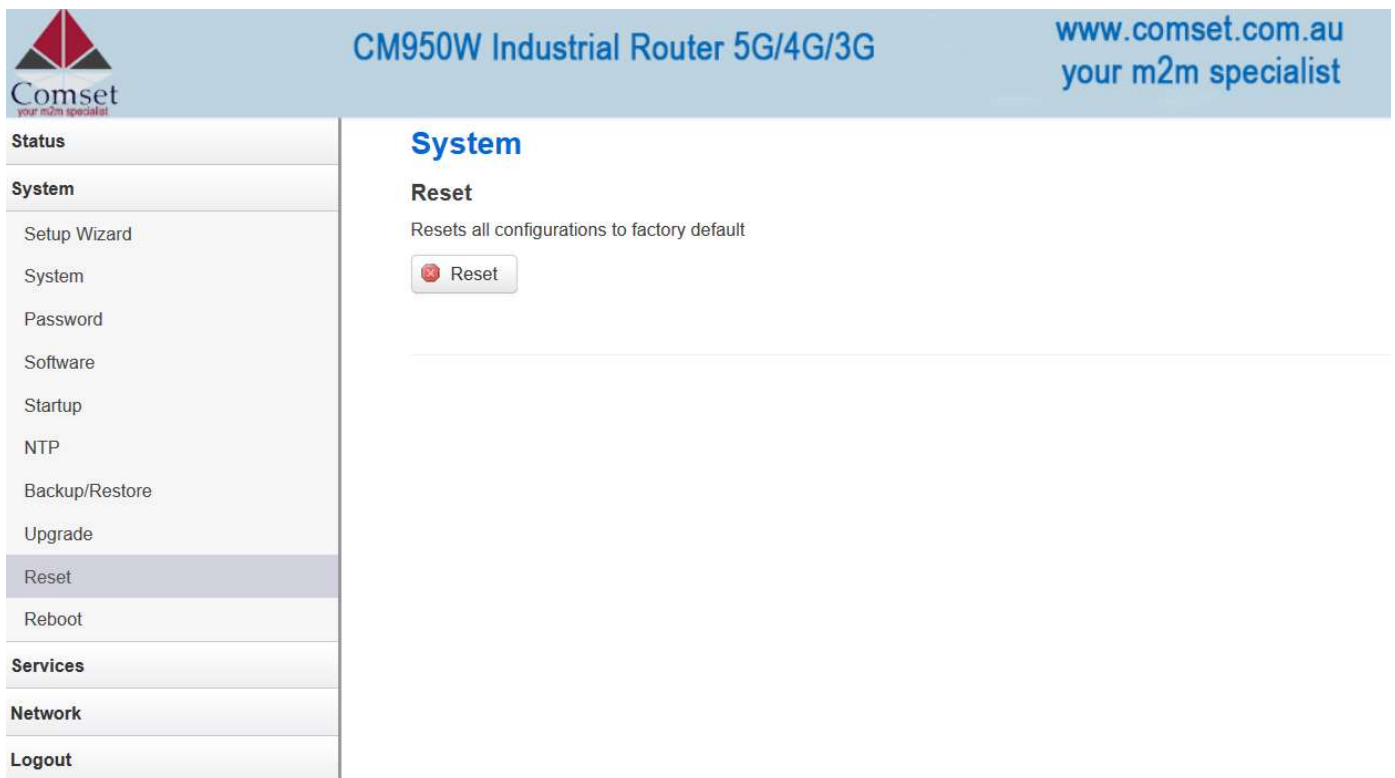
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the upgrade procedure.

- Checksum: **d49e4e53a837a6eca830ff8cad9c0c41**
- Size: 10.25 MB (15.00 MB available)
- Configuration files will be kept.

Cancel

Proceed

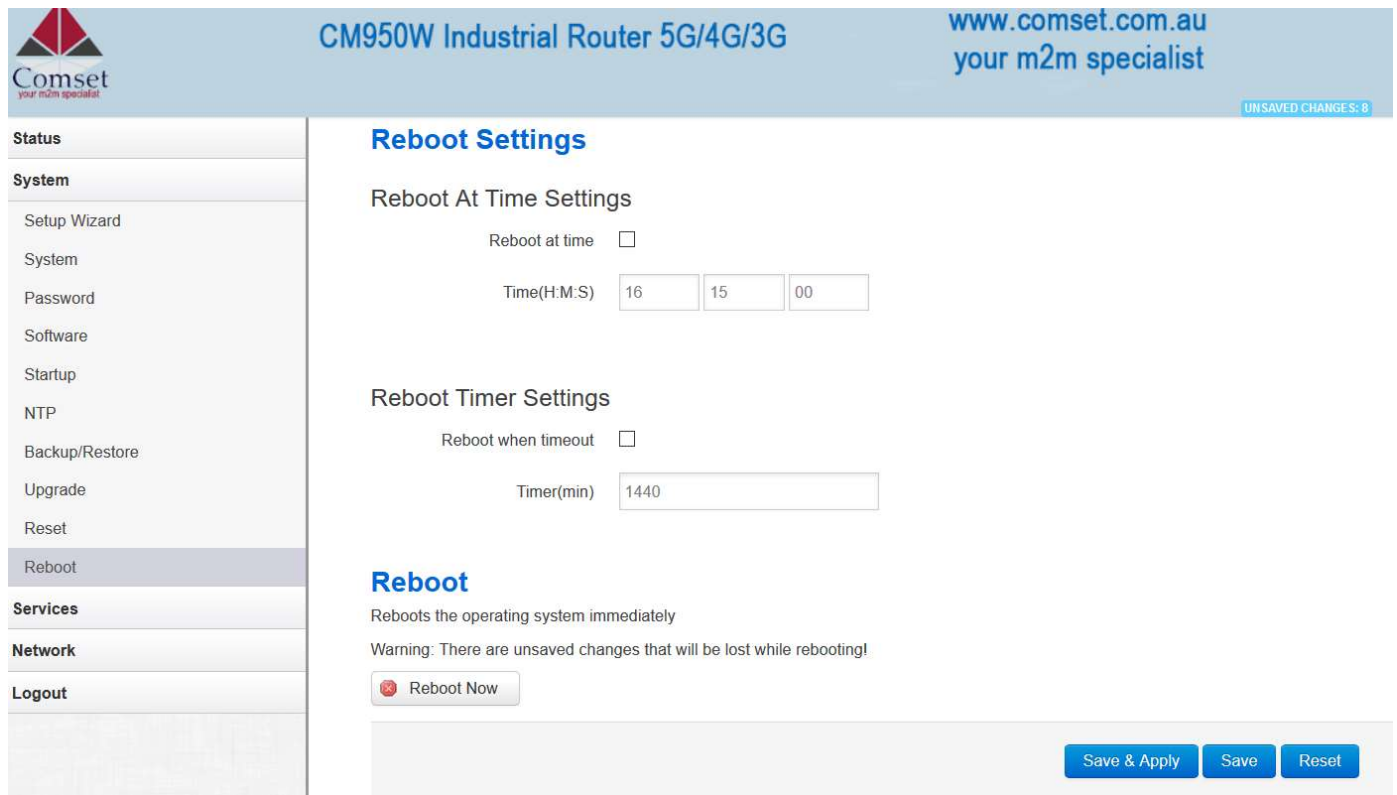
3.4.7 Reset



The screenshot shows the web interface for the CM950W Industrial Router. The header includes the Comset logo, the product name "CM950W Industrial Router 5G/4G/3G", and the website "www.comset.com.au your m2m specialist". A left-hand navigation menu lists various system settings, with "Reset" highlighted. The main content area is titled "System" and contains a "Reset" section with the description "Resets all configurations to factory default" and a "Reset" button.

This button resets all configurations to factory default. After clicking the button "Reset", a message will appear prompting you to confirm. By clicking "OK", the router will reset to factory default and the system will restart.

3.4.8 Reboot



Comset your m2m specialist

CM950W Industrial Router 5G/4G/3G

www.comset.com.au
your m2m specialist

UNSAVED CHANGES: 8

Status

System

- Setup Wizard
- System
- Password
- Software
- Startup
- NTP
- Backup/Restore
- Upgrade
- Reset
- Reboot**

Services

Network

Logout

Reboot Settings

Reboot At Time Settings

Reboot at time

Time(H:M:S)

Reboot Timer Settings

Reboot when timeout

Timer(min)

Reboot

Reboots the operating system immediately

Warning: There are unsaved changes that will be lost while rebooting!

- **Reboot at time reboots:** the router at a specific time.
- **Reboot when timeout:** reboots the router after timer timeout.
- **Click the button “Reboot Now”:** the system will restart after a few seconds.

3.5 Services configuration

3.5.1 ICMP check

For a stable operation, we suggest you enable ICMP check. With this feature, the router will periodically ping a hostname and automatically restart when a problem is detected.

Status
System
Services
ICMP Check
VRRP
Failover
DTU
SNMP
Modbus
GPS
SMS
VPN
IPSec Track
DDNS
Connect Radio Module
NMS
Captive Portal
WEB Filter
Network
Logout

ICMP Check

Enable

Host1 to ping ipv4 or hostname

Host2 to ping

Ping timeout seconds (range [1 - 10])

Max retries (range [3 - 1000])

Interval between ping minutes (range [1 - 1440])




Reconnect



Action when failed

Save & Apply Save Reset


- **Enable:** Enable ICMP check feature.
- **Host1 to ping / Host2 to ping:** The domain name or IP address for checking the network connection.
- **Ping timeout:** After a ping packet is sent, if the response packet is not received before the timeout, then this ping has failed.
- **Max retries:** When the number of failed pings reaches the “Max retries”, this will trigger the action configured in item “Action when failed”.
- **Interval between pings:** The time between two pings in minutes.
- **Reconnect:** Reconnect cell interface if ping failed.
- **Action when failed:** the options are “Restart module” and “Restart router”. “Restart module” will restart the radio module. “Restart router” will restart the whole system including the radio module.

3.5.2 VRRP

Status	<h3>VRRP Configuration</h3> <h4>VRRP LAN Configuration Settings</h4> <p>Enable <input type="checkbox"/></p> <p>Virtual ID <input type="text" value="1"/></p> <p>Virtual IP address <input type="text" value="192.168.1.253"/> </p> <p>Priority <input type="text" value="100"/></p> <p>Advertisement interval <input type="text" value="1"/> s</p> <p>Password <input type="password"/> </p> <p>Track interface <input type="text" value="None"/> </p> <p>Track IP/Host <input type="text"/></p> <p>Track Interval <input type="text" value="10"/> s</p> <p>Track Weight <input type="text" value="10"/></p> <p>Status</p>
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
WEB Filter	
Network	
Logout	

- **Enable:** Enable VRRP (Virtual Router Redundancy Protocol) for LAN.
- **Virtual ID:** Routers with the same IDs will be grouped in the same VRRP cluster, range [1 – 255]
- **Virtual IP address:** Virtual IP address for LAN's VRRP cluster. IP address entry can be deleted by clicking the button , or added by clicking the button .
- **Priority:** The router with the highest priority in the same VRRP cluster will act as master. Range [1–255]
- **Advertisement interval:** VRRP send packet to a set of VRRP instances to advertise the device in the MASTER state.
- **Password:** The password for VRRP access.
- **Track interface:** Check if the local interface is up or down.
- **Track IP/Host:** The Host or IP address to ping.
- **Track Interval:** The ping interval.
- **Track Weight:** Priority will be subtracted from the initial priority in case of ping failure.
- **Status:** Shows VRRP status (MASTER/BACKUP).

3.5.3 Failover (link backup)


CM950W Industrial Router 5G/4G/3G

Status

System

Services

ICMP Check

VRRP

Failover

DTU

SNMP

Modbus

GPS

SMS

VPN

IPSec Track

DDNS

Connect Radio Module

NMS

Captive Portal

WEB Filter

Network

Logout

Failover
Advanced

Failover Configuration

Failover Settings

Enable

Back To High priority

Current interface primary

Primary Configuration

Primary Wired_wan v

Host1 to ping

Host2 to ping

Ping timeout

Max Retries

Interval between ping

NAT Default v



Secondary Configuration

Secondary

Host1 to ping

Host2 to ping

Ping timeout

Max Retries

Interval between ping

NAT

Third Configuration

Third

Host1 to ping

Host2 to ping

Ping timeout

Max Retries

Interval between ping

NAT

- **Enable:** Enable failover feature
 - **Back to high priority:** If “back to high priority” is checked, the router will go back to the selected “high priority” WAN interface when available. The priorities can be set to primary, secondary and third priority. There are four options to choose from: Wired-WAN, Wifi_client, Cell_mobile, and None.
- **Host1 to ping / Host2 to ping:** The domain name or IP address for checking the network connection.
- **Ping timeout:** After a ping packet is sent, if the response packet is not received before the timeout, then this ping has failed.
- **Max retries:** When the number of failed pings reaches the “Max retries”, this will confirm that the WAN interface is unavailable.
- **Interval between pings:** The time between two pings in seconds.

Failover Advanced

- **Cell Standby:** When the cell is in backup mode, you can choose between data connect, data disconnect or radio off.
- **SMS Alarm:** This is if you need to send an SMS alarm every time the working interface switches over.

3.5.4 DTU

Notes:

- 1) This feature is for the CM950W with DTU option only.
- 2) This feature conflicts with the “Connect Radio module” and “GPS send to serial” features. Please disable “DTU” when using either of the above two functions.

Status
System
Services
ICMP Check
VRRP
Failover
DTU
SNMP
Modbus
GPS
SMS
VPN
IPSec Track
DDNS
Connect Radio Module
NMS
Captive Portal
WEB Filter
Network
Logout

DTU DTU Log

DTU Configuration

Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time

Enable

Send DTU ID

DTU ID

Send DTU ID on initial connection

Forward delay milliseconds (range[10,10000])

Terminate character(s)

Debug

Serial Setting

Serial baudrate

Serial parity

Serial databits

Serial stopbits

Network Setting

Protocol

Service mode

Enable Heartbeat

Heartbeat Interval

Heartbeat Content

DTU center configuration

CENTER1

Center enable

Center IP/Domain

Center Port

New center name:

- **Enable:** Enable DTU feature.
- **Send DTU ID:** Send DTU ID at the front of the packet.
- **DTU ID:** The default DTU ID is the SN of the router. You can change it if required.
- **Forward delay:** This unit is in milliseconds. It is the time delay when sending data between the serial port and the network.
- **Terminate Character:** This is to split serial port data into different packages with terminate character. This can be a string or hexadecimal which starts with 0x, such as 0x0a0d.
- **Debug:** Debug level for log output.
- **Serial baudrate:** Supports 300/1200/2400/4800/9600/19200/38400/57600/115200bps.
- **Serial parity:** Can be none, odd or even.
- **Serial databits:** Can be 7 bits or 8 bits.
- **Serial stopbit:** Can be 1 bit or 2 bits.

- **Protocol:** Both TCP and UDP are supported.
- **Service mode:** Client and Server are supported.
- **Enable heartbeat:** The heartbeat is used to maintain the “keep alive” connection.
- **Heartbeat interval:** The time between two heartbeat packets.

- **Heartbeat content:** The content of heartbeat packets.
- **DTU center Configuration:** The DTU centre is the DTU server. Simply input the centre name and click the button “Add”.
- **If the centre is not needed, you can delete it by clicking the “Delete” button or set it to ‘Disabled’.**

Notes:

The maximum number of DTU centres is 32.

3.5.5 SNMP

Status	<h2 style="color: #0070c0;">SNMP Configuration</h2> <h3>General Settings</h3> <p>Enable SNMP <input type="checkbox"/></p> <p>Remote Access <input type="checkbox"/></p> <p>Contact <input type="text" value="bofh@example.com"/></p> <p>Location <input type="text" value="office"/></p> <p>Name <input type="text" value="CM950W"/></p> <p>Port <input type="text" value="161"/></p>
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	



- **Enable SNMP:** Enable the SNMP feature
- **Remote Access:** Allow SNMP remote access. If it is unchecked, only the LAN subnet can access SNMP.
- **Contact:** Set the contact information here.
- **Location:** Set the router’s physical address.
- **Name:** Set the router’s name in SNMP.
- **Port:** SNMP service port, the default value is 161.

SNMP v1 and v2c Settings

Get Community	<input type="text" value="public"/>
Get Host/Lan	<input type="text" value="0.0.0.0/0"/>
Set Community	<input type="text" value="private"/>
Set Host/Lan	<input type="text" value="0.0.0.0/0"/>
Trap receiver IP	<input type="text" value=""/> 
SNMPv1 only	<input type="checkbox"/>

- **Get Community:** The username for SNMP get. The default value is 'public'. SNMP get is read-only.
- **Get Host/Lan:** The network range to get the router via SNMP, default is '0.0.0.0./0'
- **Set Community:** The username for SNMP set. The default value is 'private'. SNMP set is read-write.
- **Set Host/Lan:** The network range to set the router via SNMP, default is '0.0.0.0./0'

SNMP v3 Settings

User	<input type="text" value="admin_user"/>
Security Mode	<input type="text" value="Private"/> ▼
Authentication	<input type="text" value="MD5"/> ▼
Encryption	<input type="text" value="DES"/> ▼
Authentication Password	<input type="password" value="••••••••"/> 
Encryption Password	<input type="password" value="••••••••"/> 

- **User:** SNMPv3 username
- **Security Mode:** Three options: None, Private and Authorised. If it is set to 'None', there is no password required. If it is set to 'Authorised', only Authentication method and password are required.
- **Authentication:** Authentication method with two options: MD5 and SHA.
- **Encryption:** Encryption method DES and AES supported.
- **Authentication password:** SNMPv3 authentication password is at least 8 characters long.
- **Encryption password:** SNMPv3 encryption password is at least 8 characters long.

After all items are setup, click the button "Save & Apply" to enable SNMP functionality.

3.5.6 GPS (optional CM950W-G model)

Status	<h4 style="color: #0070c0;">GPS Configuration</h4> <p>Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time</p> <p>Enable <input type="checkbox"/></p> <p>Prefix SN No. <input type="checkbox"/></p> <p>Only GPRMC <input type="checkbox"/></p> <p>Send interval <input type="text" value="10"/></p> <p>GPS send to <input type="text" value="TCP"/></p> <p>Server IP/Domain <input type="text" value="192.168.1.100"/></p> <p>Server port <input type="text" value="6000"/></p> <div style="text-align: right;"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </div>
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	

- **Enable:** Check this button to enable GPS.
- **Prefix SN No:** If checked, it will add the router's SN to the data packet.
- **Only GPRMC:** If checked, it will only send GPRMC data info (Longitude Latitude altitude)
- **Send interval:** Set the frequency of GPS data packets being sent.
- **GPS Send to:** Choose between "Serial" and "TCP/IP". The router will only receive the GPS signal and will not process it. It will send this GPS signal to your GPS processor devices or servers. If the GPS processor device is connected to the CM950W Router via a Serial Port, please choose "Serial".
If the GPS processor device is a remote server, please choose "Serial".

GPS to TCP/UDP Settings

- **Server IP:** Fill in the correct destination server IP or domain name.
- **Server port:** Fill in the correct destination server port.

GPS Configuration

Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time

Enable	<input type="checkbox"/>
Prefix SN No.	<input type="checkbox"/>
Only GPRMC	<input type="checkbox"/>
Send interval	<input type="text" value="10"/>
GPS send to	<input type="text" value="Serial"/>
Serial baudrate	<input type="text" value="115200 bps"/>
Serial parity	<input type="text" value="None"/>
Serial databits	<input type="text" value="8 bits"/>
Serial stopbits	<input type="text" value="1 bits"/>
Serial flow control	<input type="text" value="None"/>

- **Serial baudrate:** 9600/19200/38400/57600/115200bps
- **Serial parity:** none/odd/even
- **Serial databits:** 7/8
- **Serial stopbits:** 1/2
- **Serial flow control:** none/hardware/software

3.5.7 SMS

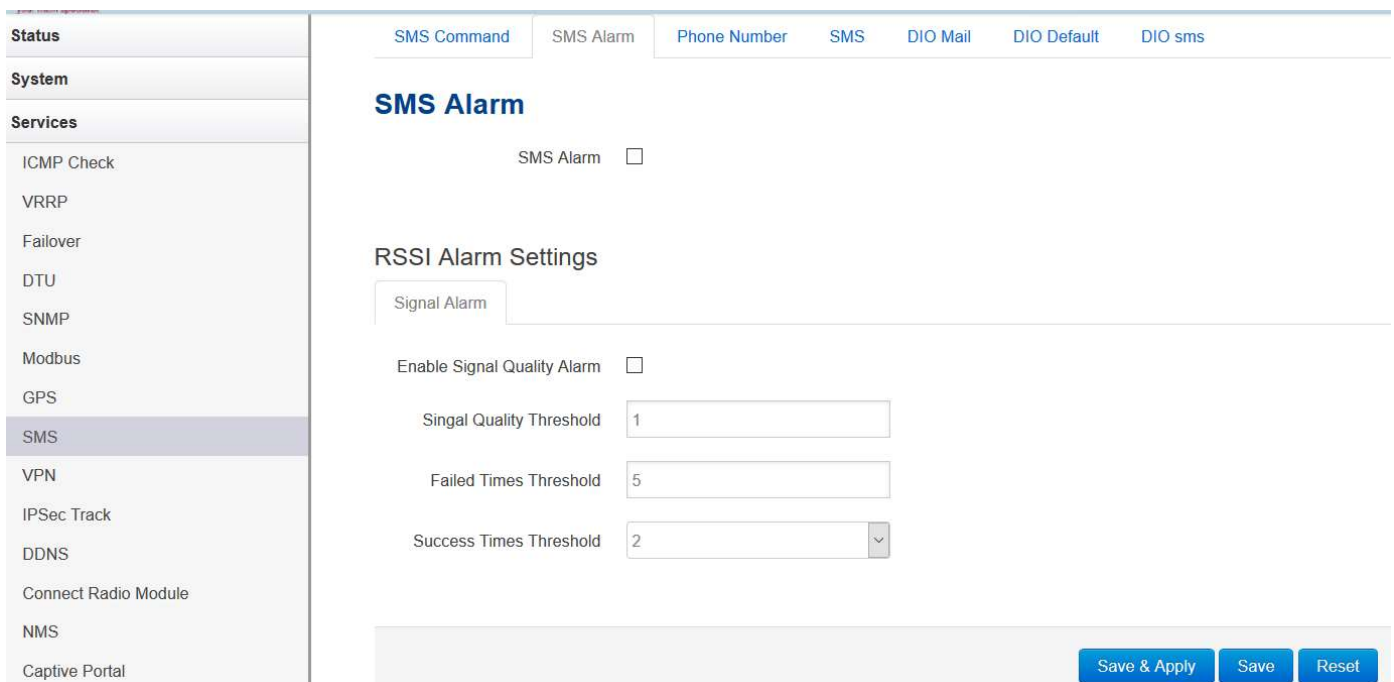
- **SMS Command**

<p>Status</p> <hr/> <p>System</p> <hr/> <p>Services</p> <p>ICMP Check</p> <p>VRRP</p> <p>Failover</p> <p>DTU</p> <p>SNMP</p> <p>Modbus</p> <p>GPS</p> <p>SMS</p> <p>VPN</p> <p>IPSec Track</p> <p>DDNS</p> <p>Connect Radio Module</p> <p>NMS</p> <p>Captive Portal</p> <p>WEB Filter</p> <hr/> <p>Network</p> <hr/> <p>Logout</p>	<p>SMS Command SMS Alarm Phone Number SMS DIO Mail DIO Default DIO sms</p> <h3>SMS Command</h3> <p>Enable <input type="checkbox"/></p> <p>SMS ACK <input type="checkbox"/></p> <p>Fix error for some network <input type="checkbox"/></p> <p>Reboot Router Command <input type="text" value="reboot"/></p> <p>Get Cell Status Command <input type="text" value="cellstatus"/></p> <p>Set Cell link-up Command <input type="text" value="cellup"/></p> <p>Set Cell link-down Command <input type="text" value="celldown"/></p> <p>DIO_0 Set Command <input type="text" value="dio01"/> <input type="button" value="Set DIO0"/></p> <p>DIO_0 Reset Command <input type="text" value="dio00"/> <input type="button" value="Reset DIO0"/></p> <p>DIO_1 Set Command <input type="text" value="dio11"/> <input type="button" value="Set DIO1"/></p> <p>DIO_1 Reset Command <input type="text" value="dio10"/> <input type="button" value="Reset DIO1"/></p> <p>DIO_2 Set Command <input type="text" value="dio21"/> <input type="button" value="Set DIO2"/></p> <p>DIO_2 Reset Command <input type="text" value="dio20"/> <input type="button" value="Reset DIO2"/></p> <p>DIO_3 Set Command <input type="text" value="dio31"/> <input type="button" value="Set DIO3"/></p> <p>DIO_3 Reset Command <input type="text" value="dio30"/> <input type="button" value="Reset DIO3"/></p> <p>DIO Status Command <input type="text" value="diostatus"/></p> <p>Wifi On Command <input type="text" value="wifion"/></p> <p>Wifi Off Command <input type="text" value="wifioff"/></p> <p>Force Cellup Command <input type="text" value="forcecellup"/></p> <p>Switch SIM Command <input type="text" value="simswitch"/></p>
--	--

- **Enable:** Check it to enable the SMS command feature.
- **SMS ACK:** If checked, the router will send the command feedback to the sender's mobile phone number.
- **Reboot Router Command:** Input the command for "reboot" operation, default is "reboot".

- **Get Cell Status Command:** Input the command for “router cell status” operation, default is “cellstatus”.
- **Set cell link-up Command:** Input the command for “router cell link up” operation, default is “cellup”. If the router gets this command, the Router Cell will go online.
- **Set cell link-down Command:** Input the command for “router cell link down” operation, default is “celldown”. If the router gets this command, the Router Cell will go offline.
- **DIO_0 Set Command:** Input the command for I/O port 0. For SMS feature, please keep the default parameters.
- **DIO_0 Reset Command:** Input the command for I/O port 0. For SMS feature, please keep the default parameters.
- **DIO_1 Set Command:** Input the command for I/O port 1. For SMS feature, please keep the default parameters.
- **DIO_1 Reset Command:** Input the command for I/O port 1. For SMS feature, please keep the default parameters.
- **DIO Status Command:** Input the command for I/O port status. For SMS feature, please keep the default parameters.
- **Wifi on Command:** input the command for turning on WiFi. For SMS feature, please keep the default parameters.
- **Wifi off Command:** input the command for turning off WiFi. For SMS feature, please keep the default parameters.

➤ SMS alarm



The screenshot shows the 'SMS Alarm' configuration page. On the left is a navigation menu with 'SMS' selected. The main content area has tabs for 'SMS Command', 'SMS Alarm', 'Phone Number', 'SMS', 'DIO Mail', 'DIO Default', and 'DIO sms'. The 'SMS Alarm' tab is active, showing a title 'SMS Alarm' and a checkbox for 'SMS Alarm' which is currently unchecked. Below this is the 'RSSI Alarm Settings' section, which includes a 'Signal Alarm' dropdown menu, an 'Enable Signal Quality Alarm' checkbox (unchecked), and three input fields: 'Singal Quality Threshold' (value 1), 'Failed Times Threshold' (value 5), and 'Success Times Threshold' (value 2). At the bottom right of the configuration area are three buttons: 'Save & Apply', 'Save', and 'Reset'.

- **SMS Alarm:** Enable the SMS alarm feature.
- **Enable Signal Quality Alarm:** Enable Signal Quality Alarm feature.
- **Signal Quality Threshold:** Set the signal quality threshold.

- **Failed Times Threshold:** If the failed counter exceeds this threshold, a signal alarm will be generated.
- **Success Times Threshold:** If a signal alarm is generated, and the success counter is greater or equal to the Success Times Threshold, this will clear the signal alarm.

➤ Phone Number

Status

System

Services

ICMP Check

VRRP

Failover

DTU

SNMP

Modbus

GPS

SMS

VPN

IPSec Track

DDNS

Connect Radio Module

NMS

SMS Command SMS Alarm Phone Number SMS DIO Mail DIO Default DIO sms

Phone Number

Phone Number Configuration

NUM1	<input type="button" value="Delete"/>
SMS Command	<input type="checkbox"/>
SMS Alarm	<input type="checkbox"/>
DIO change	<input type="checkbox"/>
Phone Number	<input type="text" value="0"/>

New group name

- **Add Phone number:** Input a name and click the button “Add” to add a new Phone number.
- **Delete Phone number:** Click the button “Delete”.
- **SMS command:** Enable the SMS command feature on this phone number.
- **SMS alarm:** This phone number can receive SMS alarms.

➤ **SMS Log**

Status System Services ICMP Check VRRP Failover DTU SNMP Modbus GPS SMS VPN IPSec Track DDNS Connect Radio Module NMS Captive Portal WEB Filter Network	SMS Command SMS Alarm Phone Number SMS DIO Mail DIO Default DIO sms
	<h3>SMS Log</h3> <div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>
	<input type="button" value="Clear SMS log"/>

- **SMS Log:** SMS send and receive log.

➤ **DIO Mail**

Status System Services ICMP Check VRRP Failover DTU SNMP Modbus GPS SMS VPN IPSec Track DDNS Connect Radio Module NMS Captive Portal WEB Filter Network Logout	SMS Command SMS Alarm Phone Number SMS DIO Mail DIO Default DIO sms
	<h3>Mail Configuration</h3> <p>Send email to specified address when DIO changed</p>
	Enable <input type="checkbox"/>
	SMTP server <input type="text"/>
	Port <input type="text" value="25"/>
	Username/Account <input type="text"/>
	SMTP Authentication <input checked="" type="checkbox"/>
	Username <input type="text"/>
	Password <input type="password"/>
	TLS <input type="text" value="On"/>
	StartTLS <input type="text" value="Off"/>
	Check server certificate <input type="text" value="Off"/>
	TLS trust file <input type="button" value="Browse..."/> No file selected.

- **Enable:** Activate DIO Mail functionality.
- **SMTP server:** SMTP server IP address or URL.
- **Port:** SMTP server port.
- **SMTP Authentication:** Enable it if SMTP server requires SMTP authentication.
- **Username:** Username for SMTP authentication.
- **Password:** Password for SMTP authentication.
- **TLS:** Enable or disable TLS (also known as SSL) for secured connections.
- **StartTLS:** Choose the TLS variant. Start TLS from within the session (default is 'on') or tunnel the session through TLS ('off').
- **Check server certificate:** Activate server certificate verification using a list of trusted Certification Authorities (CAs).
- **TLS trust file:** Activate server certificate verification using trusted Certification Authorities (CAs).

Mail format	<input type="text" value="System template"/>
DIO_0 name	<input type="text" value="DIO0"/>
DIO_0 high text	<input type="text" value="1"/>
DIO_0 low text	<input type="text" value="0"/>
DIO_1 name	<input type="text" value="DIO1"/>
DIO_1 high text	<input type="text" value="1"/>
DIO_1 low text	<input type="text" value="0"/>
DIO_2 name	<input type="text" value="DIO2"/>
DIO_2 high text	<input type="text" value="1"/>
DIO_2 low text	<input type="text" value="0"/>
DIO_3 name	<input type="text" value="DIO3"/>
DIO_3 high text	<input type="text" value="1"/>
DIO_3 low text	<input type="text" value="0"/>

Receiver Configuration

This section contains no values yet

New group name 

The default email title is “[DIOx] changed”, and content is SN:8600000000, [DIOx] has changed from [value0] to [value1}.

Configure email title and content, replace string in [].

➤ **DIO Default**

Status	SMS Command SMS Alarm Phone Number SMS DIO Mail DIO Default DIO sms
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
WEB Filter	
Network	
Logout	

DIO Configuration

DIO trap

Set DIO to high for a period of time s

DIO_0 default value

DIO_1 default value

DIO_2 default value

DIO_3 default value

DIO_0 Status

DIO_1 Status

DIO_2 Status

DIO_3 Status

DIO_0 Function

DIO_1 Function

DIO_2 Function

DIO_3 Function

- **DIO trap:** Sends SNMP trap when DIO changes from 1 to 0, or 0 to 1.
- **Set DIO to high for a period of time:** DIO will stay on high for the set period of time, at the end of which DIO will revert back to low. Value 0 means disable this function.
- **DIO_0 default value:** DIO default value is low (0). If this value is set to high (1), and as soon as the device is 'up', this value will be set to high automatically.
- **DIO_1 default value:** DIO default value is low (0). If this value is set to high (1), and as soon as the device is 'up', this value will be set to high automatically.
- **DIO_2 default value:** DIO default value is low (0). If this value is set to high (1), and as soon as the device is 'up', this value will be set to high automatically.
- **DIO_3 default value:** DIO default value is low (0). If this value is set to high (1), and as soon as the device is 'up', this value will be set to high automatically.

- **DIO_0 value:** DIO current value. 0 means low and 1 means high.
- **DIO_1 value:** DIO current value. 0 means low and 1 means high.
- **DIO_2 value:** DIO current value. 0 means low and 1 means high.
- **DIO_3 value:** DIO current value. 0 means low and 1 means high.
- **DIO_0 Function:** The DIO function can be set to None, GPS, WiFi1, WiFi2 or Cell. The DIO value can be set to high to turn on functionality or set to low to turn it off. If the value is None, then no action is taken.
- **DIO_1 Function:** The DIO function can be set to None, GPS, WiFi1, WiFi2 or Cell. The DIO value can be set to high to turn on functionality or set to low to turn it off. If the value is None, then no action is taken.
- **DIO_2 Function:** The DIO function can be set to None, GPS, WiFi1, WiFi2 or Cell. The DIO value can be set to high to turn on functionality or set to low to turn it off. If the value is None, then no action is taken.
- **DIO_3 Function:** The DIO function can be set to None, GPS, WiFi1, WiFi2 or Cell. The DIO value can be set to high to turn on functionality or set to low to turn it off. If the value is None, then no action is taken.

➤ DIO SMS

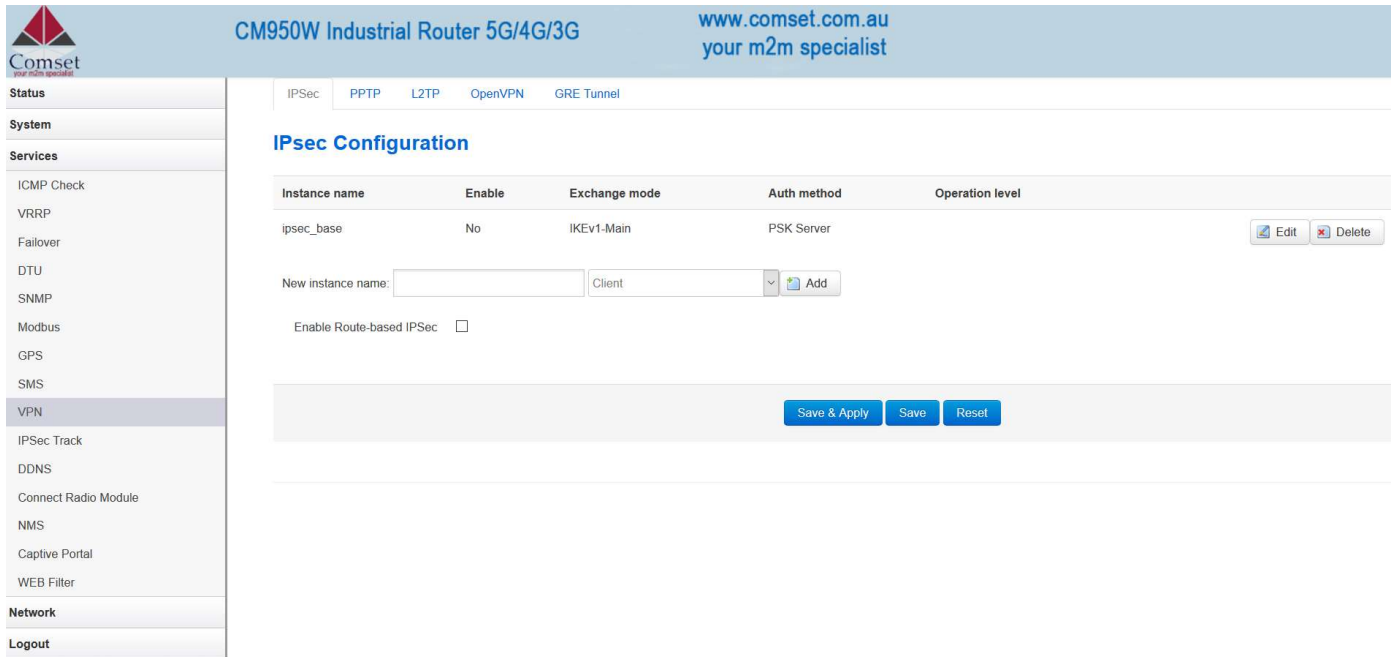
Status	SMS Command	SMS Alarm	Phone Number	SMS	DIO Mail	DIO Default	DIO sms
System	DIO SMS configuration						
Services	send user defined SMS alarm when DIO changed						
ICMP Check	Enable self-defined DIO SMS alarm <input checked="" type="checkbox"/>						
VRRP	SMS text for DIO0 changed from low to high <input type="text"/>						
Failover	SMS text for DIO0 changed from high to low <input type="text"/>						
DTU	SMS text for DIO1 changed from low to high <input type="text"/>						
SNMP	SMS text for DIO1 changed from high to low <input type="text"/>						
Modbus	SMS text for DIO2 changed from low to high <input type="text"/>						
GPS	SMS text for DIO2 changed from high to low <input type="text"/>						
SMS	SMS text for DIO3 changed from low to high <input type="text"/>						
VPN	SMS text for DIO3 changed from high to low <input type="text"/>						
IPSec Track							
DDNS							
Connect Radio Module							
NMS							
Captive Portal							
WEB Filter							
Network							
Logout							

When the DIO value changes, it will send an SMS text accordingly. You must enable “DIO change”

On the “Phone Number” page. If the user-defined text is empty, it will send the system default SMS text. The default format is SN:[86000000000], [DIOx] is changed from [value1] to [value0].

3.5.8 VPN

3.5.8.1 IPSEC



The screenshot shows the web interface for the CM950W Industrial Router. The top navigation bar includes the Comset logo, the router model 'CM950W Industrial Router 5G/4G/3G', and the website 'www.comset.com.au your m2m specialist'. A left-hand menu lists various system services, with 'VPN' selected. The main content area is titled 'IPsec Configuration' and features tabs for 'IPSec', 'PPTP', 'L2TP', 'OpenVPN', and 'GRE Tunnel'. Below the tabs is a table of configured instances:

Instance name	Enable	Exchange mode	Auth method	Operation level
ipsec_base	No	IKEv1-Main	PSK Server	Edit Delete

Below the table, there is a form for adding a new instance: 'New instance name:' followed by an input field, a dropdown menu set to 'Client', and an 'Add' button. There is also a checkbox for 'Enable Route-based IPsec' which is currently unchecked. At the bottom of the configuration area are three buttons: 'Save & Apply', 'Save', and 'Reset'.

This page displays a list of already configured IPsec instances and their state. Click the “Edit” button to modify the instance or click the “Delete” button to delete it.

The default settings are policy based IPsec. If you tick the “Enable Route-based IPsec” button, and click on “Save & Apply”, the settings will switch to router based IPsec.

IPSec Instance: Ipsec_base

Enable

Exchange mode

Operation Level

Authentication method


Remote VPN endpoint

Local endpoint

Local IKE identifier

Remote IKE identifier

Connection type

Preshared Keys 

Perfect Forward Secrecy

DPD action

DPD delay seconds

DPD timeout seconds


NAT Traversal


- **Enable:** Enable IPSEC feature
- **Exchange mode:** IKEv1-Main, IKEv1-Aggressive and IKEv2-Main modes are supported.
- **Operation level:** This is for IPsec backup. One instance is “Main”, and another instance is “Backup”. If the “Main” instance is down, it will switch to the “Backup” instance.
- **Authentication method:** Client and Server. Client is the machine which starts the IPSEC connection.
- **Remote VPN endpoint:** Domain name or IP address of the remote endpoint. This needs to be accessed over the internet.

- **Local endpoint:** Domain name, IP address or interface name of this device.
- **Local IKE identifier:** Identity to use for the local device authentication.
- **Remote IKE identifier:** Identity to use for the remote device authentication.
- **Preshared Keys:** This is known as PSK. The length is 16 to 32.
- **Perfect Forward Secrecy:** Enable or Disable.
- **DPD action:** This controls the use of DPD RFC 3706 (Dead Peer Detection protocol), where R_U_THERE notification messages (IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically sent in order to check the liveness of the IPsec peer. The values clear, hold, and restart all activate DPD and determine the action to perform on a timeout. With clear the connection is closed with no further actions taken. hold installs a trap policy, which will catch matching traffic and tries to re-negotiate the connection on demand. restart will immediately trigger an attempt to re-negotiate the connection. The default is none which disables the active sending of DPD messages.
- **DPD delay:** This defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer.
- **DPD timeout:** This defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.
- **NAT traversal:** This indicates whether the device is behind a NAT device or not.


Local source ip:


Remote source ip:

Additional phase1: 

Additional phase2: 

Local LAN bypass:

Local subnet: 

Remote subnet: 

- **Local source ip:** The internal source IP of the local device to use in a tunnel, also known as virtual IP.
- **Remote source ip:** The internal source IP of the remote device to use in a tunnel, also known as virtual IP.
- **Local subnet:** The local subnet which connects to the IPSEC VPN.
- **Remote subnet:** The remote subnet which connects to the IPSEC VPN.

Phase 1 Proposal

Enable

Encryption algorithm

Hash algorithm

DH group

Life time seconds

Phase 2 Proposal

Enable

Encryption algorithm

PFS group

Authentication

Life time seconds

Note:

All configurations in Phase 1 Proposal and Phase 2 Proposal must match with the remote endpoint to establish an IPSEC connection.



3.5.8.2 PPTP

IPSec | **PPTP** | L2TP | OpenVPN | GRE Tunnel

Point-to-Point Tunneling Protocol

PPTP Configuration

Below is a list of configured PPTP instances and their state.

Name	Type	Enable	
	Server	No	 Edit  Delete

New instance name: Role: Client

PPTP NAT enable


This page displays a list of already configured PPTP instances and their state. Click the “Edit” button to modify the instance or click the “Delete” button to delete it.

- **PPTP NAT enable:** This is to enable PPTP interface NAT.

➤ PPTP Client configuration

PPTP Client Instance: Client

Main Settings

Enable	<input type="checkbox"/>
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/> 
Remote LAN subnet	<input type="text"/>
Remote LAN netmask	<input type="text"/>
Local tunnel IP	<input type="text"/>
MTU	<input type="text" value="1500"/>
Keep Alive	<input type="text"/>
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>
Refuse PAP	<input type="checkbox"/>
Refuse EAP	<input type="checkbox"/>
Refuse CHAP	<input type="checkbox"/>
Refuse MS-CHAP	<input type="checkbox"/>
MPPE Encryption	<input checked="" type="checkbox"/>
Debug	<input type="checkbox"/>
Restart module when PPTP connects failed	<input checked="" type="checkbox"/>

- **Enable:** Enable this instance.
- **Server:** Domain name or IP address of PPTP server.
- **Username:** Server authentication username.
- **Password:** Server authentication password.
- **Remote LAN subnet:** This is the remote subnet which can be accessed via PPTP tunnel, such as 192.168.10.0.
- **Remote LAN netmask:** This is the netmask for the remote LAN subnet, such as 255.255.255.0.
- **MTU:** Maximum Transmission Unit.
- **Keep Alive:** Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.
- **Use DNS servers advertised by peer:** If unchecked, the advertised DNS server addresses are ignored.
- **MPPE Encryption:** Microsoft Point-to-Point Encryption.
- **Debug:** Adds verbose PPTP log in system log.
- **Restart module when PPTP connect fails:** In some networks, PPTP cannot connect until the module is restarted.

➤ PPTP Server Configuration

PPTP Server Instance:

Main Settings

Enable

PPTP Local IP

PPTP remote IP start

PPTP remote IP end

ARP Proxy

MPPE Encryption

IPCP-accept-remote

Debug

Username	Password	Address	Subnet
<input type="text" value="youruser"/>	<input type="password" value="*****"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Delete"/>			
<input type="button" value="Add"/>			
<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>			

- **PPTP Local IP:** Indicates the server's IP address.
- **PPTP Remote IP start:** The remote IP address lease start.
- **PPTP Remote IP end:** The remote IP address lease end.
- **ARP Proxy:** If the remote IP has the same subnet as the LAN, check it for connecting with each other.
- **MPPE Encryption:** Microsoft Point-to-Point Encryption.
- **Debug:** For PPTP server debug, the log can be monitored in the system log.
- **Username:** Server authentication username
- **Password:** Server authentication password.

3.5.8.3 L2TP

This page displays a list of already configured L2TP instances and their state. Click the “Edit” button to modify the instance or click the “Delete” button to delete it.

IPSec PPTP L2TP OpenVPN GRE Tunnel

Layer 2 Tunneling Protocol

L2TP Configuration

Name	Type	Enable	
L2tpd_server	Server	No	Edit Delete

New instance name: Role: [Add New](#)


L2TP NAT enable

[Save & Apply](#) [Save](#) [Reset](#)

➤ L2TP Client configuration

L2TP Client Instance: Cli

Main Settings

Enable	<input type="checkbox"/>
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/> 
Remote LAN subnet	<input type="text"/>
Remote LAN netmask	<input type="text"/>
Local tunnel IP	<input type="text"/>
MTU	<input type="text" value="1500"/>
Keep Alive	<input type="text" value="5"/>
Refuse PAP	<input type="checkbox"/>
Refuse EAP	<input type="checkbox"/>
Refuse CHAP	<input type="checkbox"/>
Refuse MS-CHAP	<input type="checkbox"/>
Debug	<input type="checkbox"/>

- **Enable:** Enable this L2TP instance.
- **Server:** Domain name or IP address of L2TP server.
- **Username:** Server authentication username.
- **Password:** Server authentication password.
- **Remote LAN subnet:** This is the remote subnet which can be accessed via L2TP tunnel, such as 192.168.10.0.
- **Remote LAN netmask:** This is the netmask for the remote LAN subnet, such as 255.255.255.0.
- **MTU:** Maximum Transmission Unit.
- **Keep Alive:** Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.
- **Checkup Interval:** Number of seconds to pass before checking if the interface is not up since the last setup attempt and retry the connection otherwise. Set it to a value sufficient for a successful L2TP connection for you. It is mainly for the case that netifd sent the connect request yet xl2tpd failed to complete it without the notice of netifd.
- **Debug:** Adds L2TP verbose log into the system log.

➤ L2TP Server configuration

L2TP Server Instance: L2tpd_server

Main Settings

Enable

L2TP Local IP

Remote IP range begin

Remote IP range end

DNS


IPCP-accept-remote


Length bit

IPSec saref

ARP Proxy

Debug

Username	Password
<input type="text" value="user"/>	<input type="password" value="....."/> 

 Add

- **Local IP:** Indicates the server's IP address.
- **Remote IP range begin:** The remote IP address lease start.
- **Remote IP range end:** The remote IP address lease end.
- **Remote LAN IP:** The remote LAN subnet that can be accessed via L2TP tunnel, such as 192.168.10.0.
- **Remote LAN netmask:** The mask of L2TP client IP. The default value is 255.255.255.0
- **ARP Proxy:** This allows the remote L2TP client to access the local LAN subnet. The remote IP range should be included in the LAN subnet, such as local LAN subnet 192.168.1.0/24. Then configure Remote IP range to begin with 192.168.1.20 and Remote IP range to end with 192.168.1.30 and enable ARP Proxy.
- **Debug:** This adds L2TP verbose log into the system log.
- **Username:** Server authentication username.
- **Password:** Server authentication password.

3.5.8.4 OpenVPN

This page displays a list of already configured OpenVPN instances and their state. Click the “Edit” button to modify the instance or click the “Delete” button to delete it. Click the “Start” or “Stop” buttons to start or stop a specific instance.

OpenVPN

OpenVPN instances

Please goto overview page to restart openVPN instance manually after Apply

	enabled	Started	Start/Stop	Tun/Tap	Port	Protocol	
custom_config	No	no	start	tun	1194	udp	Edit Delete
sample_server	No	no	start	tun	1194	udp	Edit Delete
sample_client	No	no	start	tun	1194	udp	Edit Delete

New instance name: Client configuration for an ethernet Add

OpenVPN NAT enable

Note: For OpenVPN configuration help, hover the cursor over the item to get more information. If the item you need is not shown on the main page, please check the “Additional Field” dropdown list at the bottom of the page.

Overview » Instance "sample_server"

[Switch to advanced configuration »](#)

enabled

verb

port

tun_ipv6

server

- Additional Field –
- nice
- dev_type
- ifconfig
- server_bridge
- remote
- secret
- pkcs12
- ca
- dh
- cert
- key
- fullcfg
- Additional Field –

3.5.8.5 GRE tunnel

GRE Tunnel

GRE Instance: Gre_tunnel

Enable	<input type="checkbox"/>
TTL	<input type="text" value="255"/>
MTU	<input type="text" value="1500"/>
Peer IP Address	<input type="text"/>
Remote LAN subnet	<input type="text"/>
Remote LAN netmask	<input type="text"/>
Metric	<input type="text" value="0"/>
Local Interface	<input type="text" value="All"/> <input type="button" value="v"/>
Local Tunnel IP	<input type="text"/>
Local Tunnel Mask	<input type="text"/>
Keepalive	<input type="text" value="None"/> <input type="button" value="v"/>

- **Enable:** Enable GRE tunnel feature.
- **TTL:** Time-to-live.
- **MTU:** Maximum Transmission Unit.
- **Peer IP address:** Remote WAN IP address.
- **Remote Network IP:** Remote LAN subnet address that can be accessed via GRE tunnel, such as 192.168.10.0.
- **Remote Netmask:** Remote LAN subnet mask, such as 255.255.255.0.
- **Local Tunnel IP:** Virtual IP address. This cannot be in the same subnet as the LAN network.
- **Local Tunnel Mask:** Virtual IP mask.

- **Local Interface:** Bond a specific interface for GRE tunnel.
- **keepalive:** Values are “none”, “receive only” and “send and receive”. If the value is “none”, The GRE tunnel will remain up. If the value is “receive only” and if no GRE keepalive message has been received for peer device, this will set the tunnel up. If the value is “send and receive”, this will send a keepalive message to the remote peer, as well as receive a keepalive message from the peer.

3.5.9 DDNS

DDNS allows a router to be reached via a fixed domain name while having a dynamically changing IP address.

Status

System

Services

ICMP Check

VRRP

Failover

SNMP

DTU

GPS

SMS

VPN

DDNS

Connect Radio Module

Network

Logout

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Overview

Below is a list of configured DDNS configurations and their current state.
If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'

Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
example_ipv4	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	<i>Never Disabled</i>	-----	Edit Delete
myddns_ipv6	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	<i>Never Disabled</i>	-----	Edit Delete

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

Details for: **example_ipv4**

Basic Settings | **Advanced Settings** | Timer Settings | Log File Viewer


Enabled

IP address version IPv4-Address
 IPv6-Address

DDNS Service provider [IPv4]

Hostname/Domain

Username

Password 

[Back to Overview](#) [Save & Apply](#) [Save](#) [Reset](#)

- **Enabled:** Enable this instance.
- **IP address version:** IPv4 and IPv6 supported.
- **DDNS Service provider:** Select a suitable provider.
- **Hostname/Domain:** The Domain name to remotely access the router.

Basic Settings | **Advanced Settings** | Timer Settings | Log File Viewer

IP address source [IPv4]

Network [IPv4]

DNS-Server

PROXY-Server

Log to syslog

Log to file

- **IP address source:** Defines the source of the systems IPv4-Address which will be sent to the DDNS provider. We recommend the option 'Network'.
- **Network:** Defines the network of the systems IPv4-Address.
- **DNS-server:** OPTIONAL: Use non-default DNS-Server to detect 'Registered IP'. IP

address and domain name are required.

- **Log to syslog:** Writes log messages to the syslog. Critical errors will always be written to the syslog.
- **Log to file:** Writes detailed messages to the log file. File will be truncated automatically.

Basic Settings **Advanced Settings** Timer Settings Log File Viewer

Check Interval

Force Interval

Error Retry Counter

Error Retry Interval

- **Check Interval:** The minimum check interval is 1 minute=60seconds.
- **Force interval:** The minimum check interval is 1 minute=60seconds.
- **Error Retry Counter:** On Error, the script will stop execution after a given number of retries. The default settings of '0' will retry indefinitely.

Basic Settings Advanced Settings **Timer Settings** Log File Viewer

Read / Reread log file

```

/var/log/ddns/example_ipv4.log
Please press [Read] button

```

Read the log file of DDNS.

Note:

If you use the DDNS server no-ip.com, please tick the box " [Use HTTP Secure](#)" and input "8.8.8.8" for the DNS-Server.

Details for: **example_ipv4**

Basic Settings **Advanced Settings** Timer Settings Log File Viewer

Enabled

IP address version IPv4-Address
 IPv6-Address

DDNS Service provider [IPv4]

Hostname/Domain

Username

Password

Use HTTP Secure

Path to CA-Certificate

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Details for: **example_ipv4**

Basic Settings **Advanced Settings** Timer Settings Log File Viewer

IP address source [IPv4]

Network [IPv4]

DNS-Server

PROXY-Server

Log to syslog

Log to file

3.5.10 Connect Radio Module

The Connect Radio Module feature is used for exchanging data between Radio module and serial.

Note:

This feature conflicts with the “DTU” and “GPS sent to serial” functions. Please make sure the other two features are disabled before enabling the Connect Radio Module. Otherwise, the following error will appear:

Status	<h3>Connect Radio Module Configuration</h3> <p>Exchange data between radio module and serial</p> <p>Enable <input type="checkbox"/></p> <p>Connect mode: Serial</p> <p>Serial baudrate: 115200 bps</p> <p>Serial parity: None</p> <p>Serial databits: 8 bits</p> <p>Serial stopbits: 1 bits</p> <p style="text-align: right;"> <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/> </p>
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
WEB Filter	
Network	
Logout	

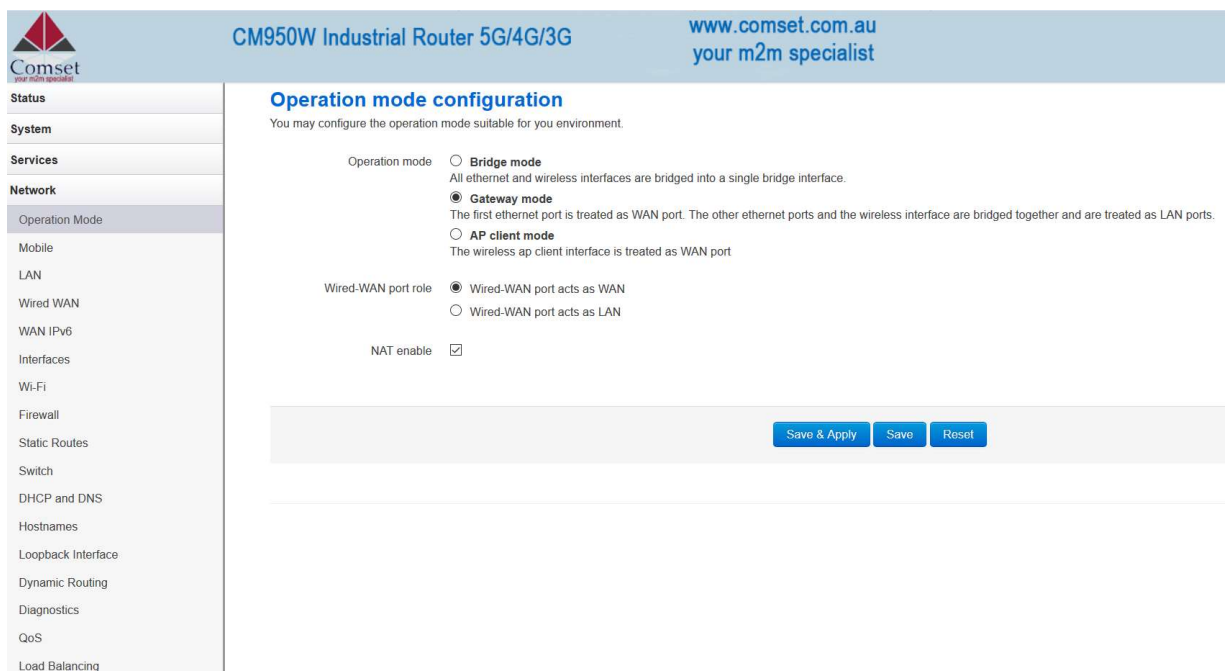
- **Connect Mode:** Serial only

Modem to Serial Settings

- **Serial baudrate:** 9600/19200/38400/57600/115200bps
- **Serial parity:** none/odd/even
- **Serial databits:** 7 bits/ 8 bits
- **Serial stopbit:** 1 bit/ 2 bits
- **Serial Flow Control:** none/hardware/software

3.6 Network Configuration

3.6.1 Operation Mode



The screenshot shows the web interface for the CM950W Industrial Router. The page title is "Operation mode configuration". The left sidebar contains a navigation menu with the following items: Status, System, Services, Network (highlighted), Operation Mode (highlighted), Mobile, LAN, Wired WAN, WAN IPv6, Interfaces, Wi-Fi, Firewall, Static Routes, Switch, DHCP and DNS, Hostnames, Loopback Interface, Dynamic Routing, Diagnostics, QoS, and Load Balancing. The main content area contains the following configuration options:

- Operation mode:**
 - Bridge mode: All ethernet and wireless interfaces are bridged into a single bridge interface.
 - Gateway mode: The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.
 - AP client mode: The wireless ap client interface is treated as WAN port.
- Wired-WAN port role:**
 - Wired-WAN port acts as WAN
 - Wired-WAN port acts as LAN
- NAT enable:**

At the bottom right of the configuration area, there are three buttons: "Save & Apply", "Save", and "Reset".

- **Operation mode**
 - **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface.
 - **Gateway:** The first Ethernet port is treated as a WAN port. The second Ethernet port and the wireless interface are bridged together and are treated as LAN ports.
 - **AP Client:** The wireless apcli interface is treated as a WAN port and the wireless AP interface and the Ethernet ports are treated as LAN ports.
- **NAT Enabled**
Network Address Translation. Default is *Enabled*.
- **Ethernet WAN port:**
 - Wired-WAN port acts as WAN**
Default is checked.
 - Wired-WAN port acts as LAN**
Default is un-checked. If you check this box, the WAN port will act as a LAN port.

The default operation is in "Gateway mode".

3.6.2 Mobile configuration

The router supports dual SIM. Here you can configure the parameters for both SIM cards.

The screenshot shows the 'Mobile Configuration' page for SIM 1. The 'SIM Switch' tab is active. The settings are as follows:

- Enable:
- Mobile connection: DHCP mode
- PIN code: (empty)
- Dialing number: *99#
- APN: telstra.internet
- Authentication method: None
- Dual APN support:
- Network Type: automatic
- MTU: 1500
- Default route:

Buttons at the bottom: Save & Apply, Save, Reset.

The screenshot shows the 'Mobile Configuration' page for SIM 2. The 'SIM Switch' tab is active. The settings are as follows:

- Enable:
- Mobile connection: DHCP mode
- PIN code: (empty)
- Dialing number: *99#
- APN: telstra.internet
- Authentication method: None
- Dual APN support:
- Network Type: automatic
- MTU: 1500
- Default route:

Buttons at the bottom: Save & Apply, Save, Reset.

- **Enable:** Enable mobile network.
- **Mobile connection:** Keep the default value DHCP.
- **Pin Code:** Most SIM cards do not have a PIN number; in which case you leave blank.
- **Dialing number:** Keep the default value *99#
- **APN:** Fill in the related value. The default value is telstra.internet.
- **Authentication method:** There are three options to choose from (None, PAP, CHAP). The common value is *None*. PAP and CHAP modes require a username and a password.
- **Dual APN support:** Here you can enter a second APN.
- **Network Type:** Options are *Automatic*, *NR5G*, *4G (LTE) only*, *WCDMA only*, *LTENR5G*. It is recommended to keep the default value *Automatic*.
- **MTU:** Maximum Transmission Unit. It is the maximum size of packets transmitted on the network. The default value is 1500.

3.6.3 SIM Switch

Status

System

Services

Network

Operation Mode

Mobile

LAN

Wired WAN

WAN IPv6

Interfaces

Wi-Fi

Firewall

Static Routes

Switch

DHCP and DNS

Hostnames

Loopback Interface

Dynamic Routing

Diagnostics

QoS

Load Balancing

Logout

General

SIM Switch

Cell Switch Configuration

Master SIM SIM 1 ▼

Enable SIM switch

Switch Rules

On Time

On ICMP check

On signal strength

On dial fail

On data limit

Switch to master

Save & Apply
Save
Reset

Item	Description	
Master SIM	Choose SIM1 or SIM2 as a master SIM. The other SIM will act as a backup SIM.	
Enable SIM switch	Check this box to enable the SIM switch feature. Otherwise, the router will work with a single SIM.	
Switch Rules	On Time	The switch will occur based on the set schedule.
	On ICMP check	The switch will occur based on ICMP check.
	On Signal strength	The switch will occur if the signal strength drops below a set CSQ value. Values can be between 1 and 30.
	On dial fail	The switch will occur if the number of re-dials exceeds the set value.
	On data limit	The switch will occur if the working SIM reaches a pre-set data limit.
	Switch to master	The router will switch back to the master SIM after a set time.
Notes: some trigger rules can be selected and used at the same time to meet different applications.		

3.6.4 LAN settings

Status

System

Services

Network

Logout

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

General Setup

Advanced Settings

Physical Settings

Firewall Settings

Status

Uptime: 1h 14m 41s

MAC-Address: F6:7C:AE:36:26:3A

RX: 5.53 MB (24840 Pkts.)

TX: 7.94 MB (16109 Pkts.)

IPv4: 192.168.1.1/24

IPv6: fd56:67a9:e60::1/60

Protocol Static address ▼

Really switch protocol? Switch protocol

IPv4 address 192.168.1.1

IPv4 netmask 255.255.255.0 ▼

IPv4 gateway

IPv4 broadcast

Use custom DNS servers +

IPv6 assignment length 60 ▼

IPv6 assignment hint

- **Protocol:** Only static address is supported for LAN.
- **Use custom DNS servers:** Multiple DNS servers are supported.
- **IPv6 assignment length:** Assign a part of given length of every public IPv6-prefix to LAN interface.
- **IPv6 assignment hint:** Assign prefix parts using this hexadecimal sub prefix ID for LAN interface.

www.comset.com.au

80

Status
System
Services
Network
Logout

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

[General Setup](#)
[Advanced Settings](#)
[Physical Settings](#)

[Firewall Settings](#)

Bring up on boot

Use builtin IPv6-management

Secondary IP address

Secondary Mask

Override MAC address

Override MTU

Use gateway metric

- **Bring up on boot:** If checked, the LAN interface will be set to 'up' upon system boot-up. If unchecked, the LAN interface will be 'down'. Don't uncheck it if not required.
- **Use built-in IPv6-management:** The default is checked. If IPv6 is not needed, it can be unchecked.
- **Override MAC address:** Overrides LAN MAC address.
- **Override MTU:** Maximum Transmission Unit.
- **Use gateway metric:** The LAN subnet's metric to gateway.

Status
System
Services
Network
Operation Mode
Mobile
LAN
Wired WAN
WAN IPv6
Interfaces
Wi-Fi
Firewall
Static Routes
Switch
DHCP and DNS
Hostnames
Loopback Interface
Dynamic Routing

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR (e.g.: eth0.1)`.

Common Configuration

General Setup **Advanced Settings** Physical Settings

Firewall Settings

Bridge interfaces

Enable STP

Interface eth0

Wired-LAN (lan)

Wired-WAN (wan, wan6)

eth1 (ifmobile)

gretap0

ip_vti0

WiFi (lan)

WiFi1 (lan)

- **Bridge interfaces:** LAN bridges wired-LAN and WiFi in the same LAN subnet.
- **Enable STP:** Enable Spanning Tree Protocol on LAN. The default value is unchecked.

Status
System
Services
Network
Operation Mode
Mobile
LAN
Wired WAN
WAN IPv6
Interfaces
Wi-Fi
Firewall
Static Routes
Switch
DHCP and DNS
Hostnames
Loopback Interface
Dynamic Routing
Diagnostics
QoS
Load Balancing

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR (e.g.: eth0.1)`.

Common Configuration

General Setup **Advanced Settings** Physical Settings

Firewall Settings

Create / Assign firewall-zone l2tpzone: (empty)

lan: lan:

openvpn: (empty)

pptpzone: (empty)

vpnzone: (empty)

wan: wan: wan6: ifmobile:

unspecified -or- create:

DHCP Server

General Setup **Advanced Settings** IPv6 Settings

Ignore interface

Start

Limit

Leasetime

- **Ignore interface:** If it is checked, this will disable DHCP on LAN.
- **Start:** Lowest leased address as offset from the network address.
- **Limit:** Maximum number of leased addresses.
- **Leasetime:** Expiry time of leased addresses, minimum is 2 minutes (2m). 12h means 12 hours.


DHCP Server

General Setup **Advanced Settings** IPv6 Settings

Dynamic DHCP

Force

IPv4-Netmask

DHCP-Options 

- **Dynamic DHCP:** Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
- **Force:** Force DHCP on this network even if another server is detected.
- **IPv4-Netmask:** Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
- **DHCP-Options:** Define additional DHCP options. (For example, '6,192.168.2.1,192.168.2.2' which advertises different DNS servers to clients.)

DHCP Server

General Setup Advanced Settings IPv6 Settings

Router Advertisement-Service: server mode

DHCPv6-Service: server mode

NDP-Proxy: disabled

DHCPv6-Mode: stateless + stateful

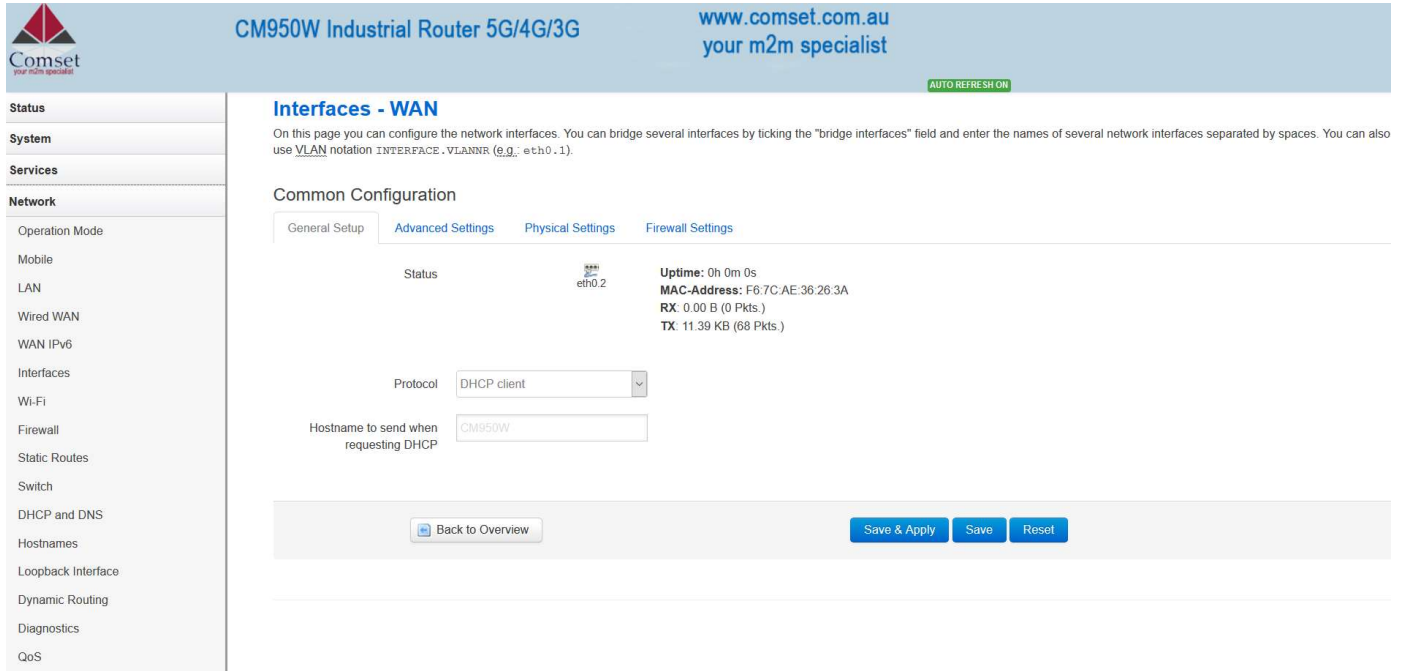
Always announce default router:

Announced DNS servers:

Announced DNS domains:

- **Router Advertisement-Service:** Four options: *disabled*, *server mode*, *relay mode* and *hybrid mode*.
- **DHCPv6-Service:** Same options as above.
- **NDP-Proxy:** Three options: *disabled*, *relay mode* and *hybrid mode*.
- **Always announce default router:** Announce as default router even if no public prefix is available.

3.6.5 Wired-WAN



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANID (e.g., eth0.1).

Common Configuration

General Setup | **Advanced Settings** | Physical Settings | Firewall Settings

Status eth0.2 Uptime: 0h 0m 0s
 MAC-Address: F8:7C:AE:36:26:3A
 RX: 0 00 B (0 Pkts.)
 TX: 11.39 KB (68 Pkts.)

Protocol: DHCP client

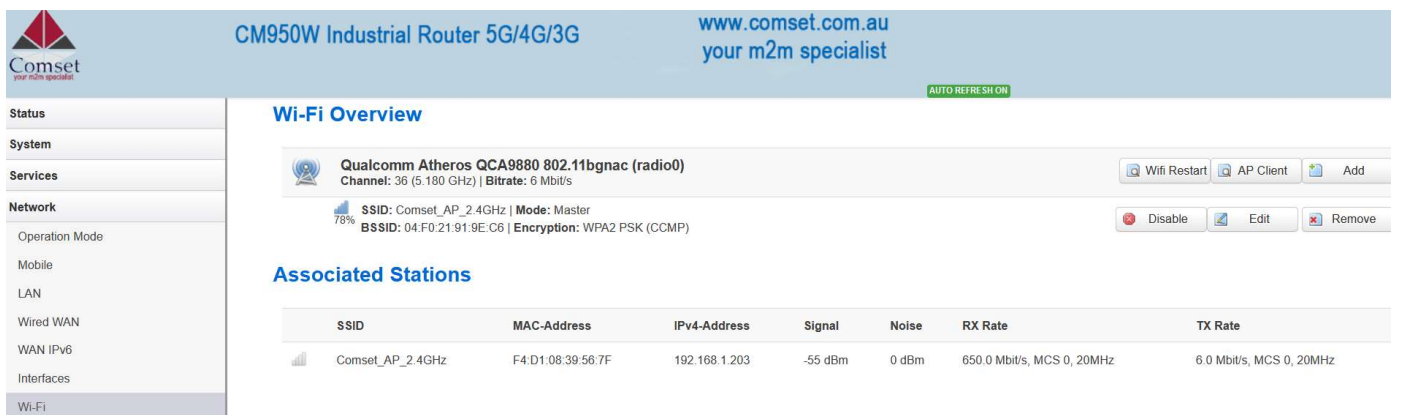
Hostname to send when requesting DHCP: CM950W

Buttons: Back to Overview, Save & Apply, Save, Reset

- **Protocol:** The default protocol is DHCP client. If you need to change it to a different protocol (i.e. PPPoE), select the protocol from the drop-down menu, then click the button “Switch protocol”.

Note: the ‘Advanced Settings’ is different for different protocols. Move the mouse over the title to get help information. We recommend you use Google Chrome.

3.6.6 WiFi Settings



Wi-Fi Overview

Qualcomm Atheros QCA9880 802.11bgnac (radio0)
 Channel: 36 (5.180 GHz) | Bitrate: 6 Mbit/s

SSID: Comset_AP_2.4GHz | Mode: Master
 BSSID: 04:F0:21:91:9E:C6 | Encryption: WPA2 PSK (CCMP)

Buttons: Wifi Restart, AP Client, Add, Disable, Edit, Remove

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Comset_AP_2.4GHz	F4:D1:08:39:56:7F	192.168.1.203	-55 dBm	0 dBm	650.0 Mbit/s, MCS 0, 20MHz	6.0 Mbit/s, MCS 0, 20MHz

- **Wifi Restart:** turn WiFi off then on.
- **AP Client:** Scan all frequencies to get the WiFi network information.
- **Add:** Add a new wireless network.
- **Disable:** Disable a wireless network.
- **Edit:** Modify settings on the wireless network.
- **Remove:** Delete a wireless network.
- **Associated Stations:** This is a list of connected wireless stations.

3.6.6.1 WiFi General Configuration

Device Configuration

General Setup

Advanced Settings

Status



Mode: Master | **SSID:** Comset_AP_2.4GHz

BSSID: 04:F0:21:91:9E:C6 | **Encryption:** WPA2 PSK (CCMP)

Channel: 36 (5.180 GHz) | **Tx-Power:** 23 dBm

Signal: -59 dBm | **Noise:** 0 dBm

Bitrate: 6.0 Mbit/s | **Country:** US

Wi-Fi network is enabled

 Disable

	Mode	Channel	Width
Operating frequency	AC	36 (5180 MHz)	80 MHz
Transmit Power	23 dBm (199 mW)		

- **Status:** Shows the WiFi signal strength, mode, SSID.
- **Operating frequency Mode:** Supports 802.11b/g/n/ac.
- **Band:** 2.4GHz and 5GHz.
- **Channel:** Channel 1-11.
- **Width:** 20MHz, 40MHz and 80MHz.
- **Transmit Power:** From 0dBm to 23dBm.

3.6.6.2 WiFi Advanced Configuration

Device Configuration

General Setup

Advanced Settings

Country Code

AU - Australia

Distance Optimization

Fragmentation Threshold

RTS/CTS Threshold

- **Country Code:** Uses ISO/IEC 3166 alpha2 country codes; Select "AU - Australia".
- **Distance Optimization:** Distance to furthest network device in meters.
- **Fragmentation Threshold**
- **RTS/CTS Threshold**

3.6.6.3 WiFi Interface Configuration

Interface Configuration

General Setup

Wireless Security

MAC-Filter

ESSID

Mode

Network ifmobile:

lan:

wan:

wan6:

create:

Hide Extended Service Set Identifier

WMM Mode

- **ESSID:** Extended Service Set Identifier. It is the broadcast name.
- **Mode:** Supported options are *Access Point, Client, Ad-Hoc, 802.11s, Pseudo Ad-Hoc, Monitor, Access Point (WDS) and Client (WDS)*

Access Point

Access Point

Client

Ad-Hoc

802.11s

Pseudo Ad-Hoc (ahdemo)

Monitor

Access Point (WDS)

Client (WDS)

- **Network:** Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
- **Hide Extended Service Set Identifier:** This allows you to hide the SSID so that WiFi cannot be scanned by others.
- **WMM Mode:** Enabled.

Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

Encryption: WPA2-PSK

Cipher: auto

Key: ●●●●●●●●●●

Enable WPS pushbutton, requires WPA(2)-PSK

[Back to Overview](#)

● Encryption:

- No Encryption
- WEP Open System
- WEP Shared Key
- WPA-PSK
- WPA2-PSK
- WPA-PSK/WPA2-PSK Mixed Mode
- WPA-EAP
- WPA2-EAP

- **Key:** It is the password to join the wireless network. If the Encryption is set to “No Encryption”, no password is needed.

Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

MAC-Address Filter: disable

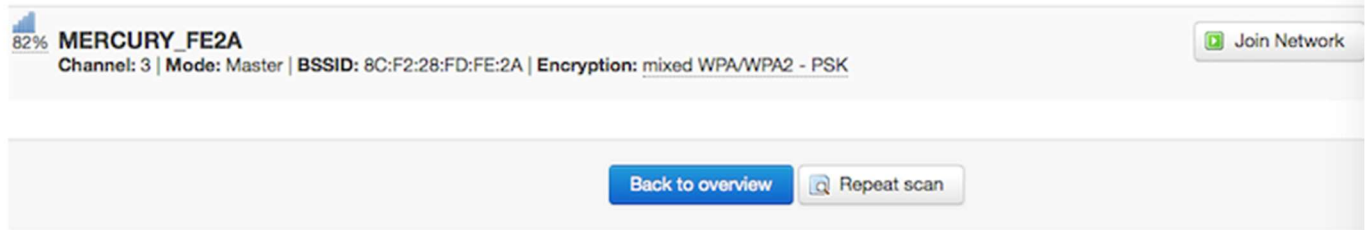
[Back to Overview](#)

- **MAC-Address Filter:** This is the MAC address access policy.
 - **Disable:** Disables MAC address access functionality.
 - **Allow list:** Only the MAC address in the list can forward.
 - **Deny list:** All packets can forward, except the MAC address in the list.
- **MAC-List:** Here you can add or delete MAC addresses.

3.6.6.4 WiFi AP client

- **Steps 1)** Click the button “AP Client” on the wireless overview page, then the system will start to scan all WiFi signals.

Join Network: Wireless Scan



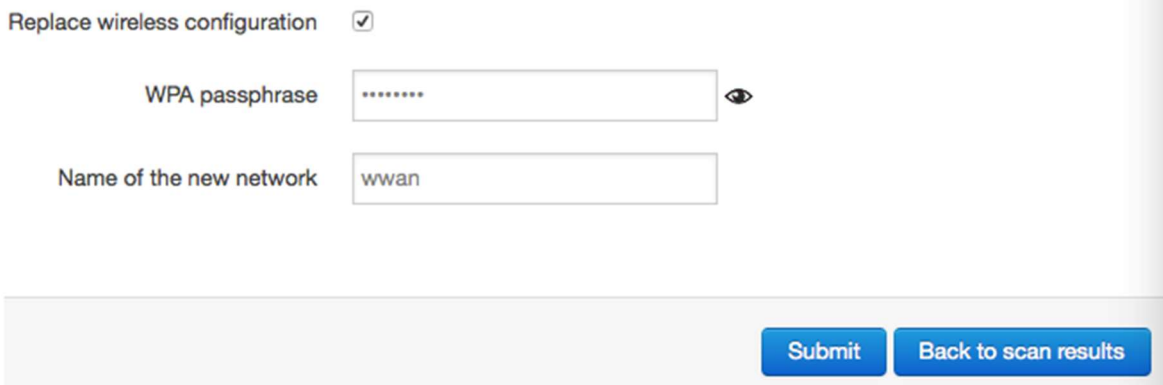
82% **MERCURY_FE2A** Join Network

Channel: 3 | Mode: Master | BSSID: 8C:F2:28:FD:FE:2A | Encryption: mixed WPA/WPA2 - PSK

Back to overview Repeat scan

- **Step 2)** If the WiFi you want to join is on the list, click the button “Join Network”. If it is not, click “Repeat Scan” until you find the WiFi that you want to join.

Join Network: Settings



Replace wireless configuration

WPA passphrase 👁

Name of the new network

Submit Back to scan results

- **Step 3)** Join Network Settings
 Replace wireless configuration: An additional wireless network will be created if it is unchecked. Otherwise it will replace the old configuration.
 WPA passphrase: Specify the secret encryption key here.
 Name of the new network: The default value is ‘wwan’. Please change it if it conflicts with other interfaces.
- **Step 4)** Click ‘Submit’ if everything is configured. The below is the Wi-Fi configuration page. Do not change the operating frequency. Make sure the ESSID and BSSID are for the Wi-Fi you want to join.

Device Configuration

General Setup

Advanced Settings

Status



Mode: Client | **SSID:** MERCURY_FE2A
BSSID: 8C:F2:28:FD:FE:2A | **Encryption:** -
Channel: 11 (2.462 GHz) | **Tx-Power:** 0 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** 00

Wireless network is enabled

Disable

	Mode	Channel	Width
Operating frequency	N	3 (2422 MHz)	20 MHz
Transmit Power	20 dBm (100 mW)		

Interface Configuration






General Setup

Wireless Security

ESSID

Mode

BSSID



- Network
- ifmobile: 
 - lan: 
 - wan: 
 - wan6: 
 - wwan: 
 - create:

- **Step 5)** Click the button “Save & Apply” to start the AP client.

Wireless Overview


	Generic MAC80211 802.11bgn (radio0) Channel: 3 (2.422 GHz) Bitrate: 150 Mbit/s	 Wifi Restart	 AP Client	 Add
68%	SSID: Cell_AP_0002b2 Mode: Master BSSID: 90:22:06:00:02:B3 Encryption: None	 Disable	 Edit	 Remove
85%	SSID: MERCURY_FE2A Mode: Client BSSID: 8C:F2:28:FD:FE:2A Encryption: WPA2 PSK (CCMP)	 Disable	 Edit	 Remove

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
 Cell_AP_0002b2	68:A8:6D:48:77:5E	?	-62 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	58.5 Mbit/s, MCS 6, 20MHz
 MERCURY_FE2A	8C:F2:28:FD:FE:2A	192.168.1.1	-50 dBm	0 dBm	135.0 Mbit/s, MCS 7, 40MHz	150.0 Mbit/s, MCS 7, 40MHz

3.6.7 Interfaces Overview

The “Interfaces Overview” page shows all Interfaces status, including uptime, MAC-address, RX, TX and IP address.


CM950W Industrial Router 5G/4G/3G
www.comset.com.au
your m2m specialist
AUTO REFRESH ON

Status

System

Services

Network

Operation Mode

Mobile

LAN

Wired WAN

WAN IPv6

Interfaces

Wi-Fi

Firewall

Static Routes

Switch

DHCP and DNS

Hostnames

Loopback Interface




















Dynamic Routing

Diagnostics

QoS

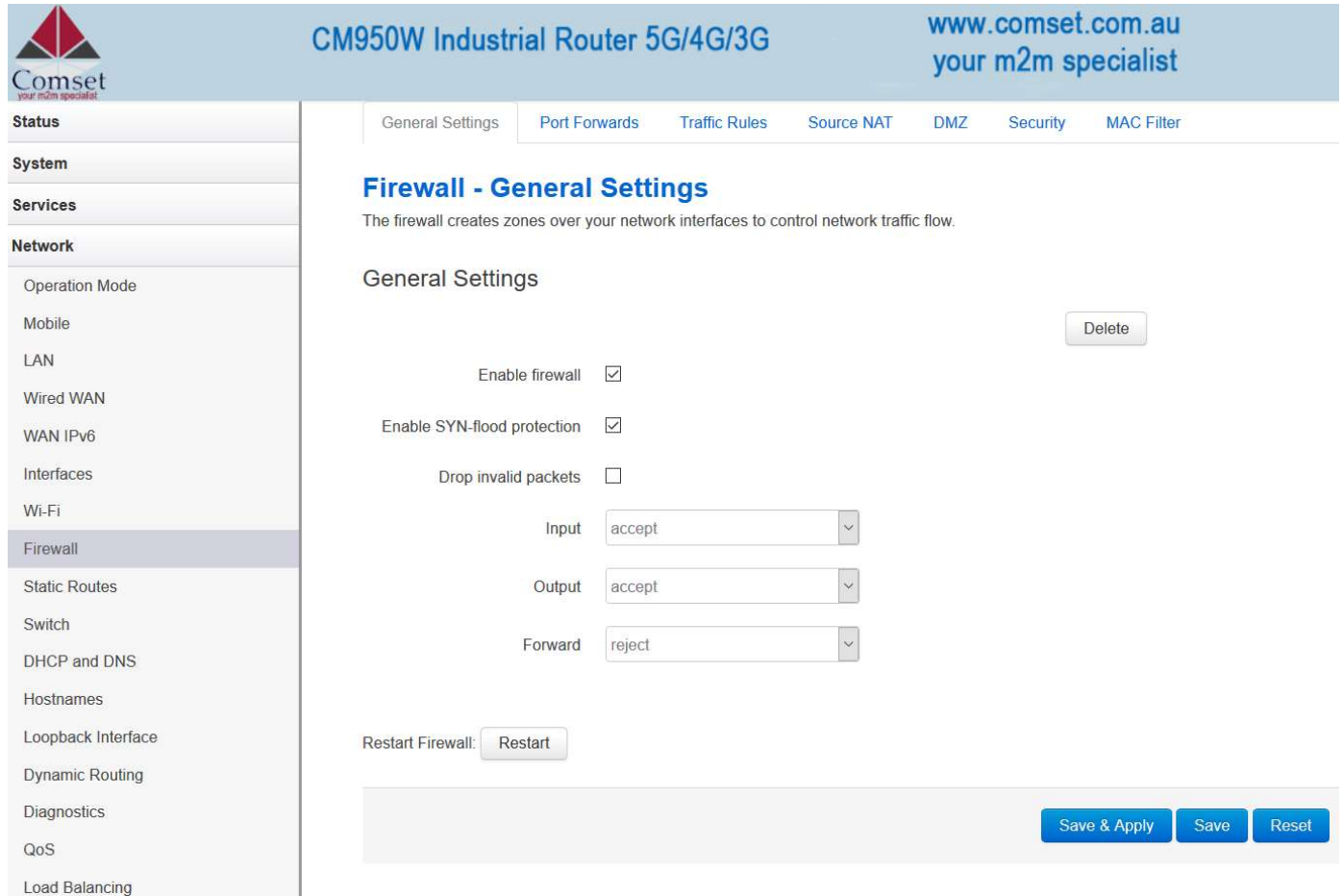
Interfaces

Interface Overview

Network	Status	Actions
LOOPBACK  lo	Uptime: 4h 38m 22s MAC-Address: 00:00:00:00:00:00 RX: 16.10 KB (224 Pkts.) TX: 16.10 KB (224 Pkts.)	 Connect  Stop  Edit
LAN  br-lan	Uptime: 4h 38m 22s MAC-Address: F6:7C:AE:36:26:3A RX: 27.68 MB (129599 Pkts.) TX: 89.75 MB (115380 Pkts.) IPv4: 192.168.1.1/24 IPv6: fd8b:67a9:e60::1/60	 Connect  Stop  Edit
IFMOBILE  eth1	Uptime: 4h 37m 44s MAC-Address: 2E:F5:CC:1C:3E:88 RX: 81.98 MB (88281 Pkts.) TX: 22.77 MB (65546 Pkts.) IPv4: 10.115.124.156/29	 Connect  Stop  Edit
WAN  eth0.2	Uptime: 0h 0m 0s MAC-Address: F6:7C:AE:36:26:3A RX: 0.00 B (0 Pkts.) TX: 26.57 KB (160 Pkts.)	 Connect  Stop  Edit
WAN6  eth0.2	Uptime: 0h 0m 0s MAC-Address: F6:7C:AE:36:26:3A RX: 0.00 B (0 Pkts.) TX: 26.57 KB (160 Pkts.)	 Connect  Stop  Edit

3.6.8 Firewall

3.6.8.1 General Settings



The screenshot shows the web interface for the CM950W Industrial Router. The top navigation bar includes the Comset logo, the router model name, and the website URL. A sidebar on the left lists various system settings, with 'Firewall' selected. The main content area displays the 'Firewall - General Settings' page, which includes a 'Delete' button, checkboxes for 'Enable firewall', 'Enable SYN-flood protection', and 'Drop invalid packets', and dropdown menus for 'Input', 'Output', and 'Forward' actions. A 'Restart Firewall' button is also present. At the bottom right, there are 'Save & Apply', 'Save', and 'Reset' buttons.

3.6.8.2 Port Forwards

This page includes the “Port Forwards” list and how to add new “Port Forwards” rules.

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
------	-------	------------	--------	------

This section contains no values yet

New port forward:

Name	Protocol	External port	Internal IP address	Internal port	
<input type="text" value="New port forward"/>	TCP+UDP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

- **Name:** Port Forward instance name.
- **Protocol:** Options are TCP+UDP, UDP or TCP.
- **External zone:** The recommended option is 'wan'.
- **External port:** Match incoming traffic directed at the given destination port on this host.
- **Internal zone:** The recommended zone is 'lan'.
- **Internal IP address:** Redirect matched incoming traffic to the specific host.
- **Internal port:** Redirect matched incoming traffic to the given port on the internal host.

3.6.8.3 Traffic rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

The traffic rules overview page contains the following functionalities:

Traffic rules list:

General Settings Port Forwards Traffic Rules Source NAT DMZ Security MAC Filter

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort	
DTU server	Any TCP, UDP From any host in wan To any router IP at port 5000 on this device	Accept input	<input type="checkbox"/>	+	
DTU2 server	Any TCP, UDP From any host in wan To any router IP at port 5001 on this device	Accept input	<input type="checkbox"/>	+	
Allow-All-LAN-Ports	Any traffic From any host in wan To any host, ports 1-65535 in lan	Accept forward	<input type="checkbox"/>	+	
Allow-DHCP-Renew	IPv4-UDP From any host in wan To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	+	
Allow-Ping-WAN	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	+	
Allow-IGMP	IPv4-IGMP From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	+	
Allow-DHCPv6	IPv6-UDP From IP range fe80::/10 in wan with source port 547 To IP range fe80::/10 at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	+	
Allow-MLD	IPv6-ICMP with types 130/0, 131/0, 132/0, 143/0 From IP range fe80::/10 in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	+	
Allow-ICMPv6-Input	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement From any host in wan To any router IP on this device	Accept input and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	+	
Allow-ICMPv6-Forward	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone	Accept forward and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	+	

Open ports on router and create 'new forward rules':

Open ports on router:

Name

Protocol

External port

New input rule

TCP+UDP

Add

New forward rule:

Name

Source zone

Destination zone

New forward rule

lan

wan

Source NAT list and create source NAT rule:

General Settings | Port Forwards | Traffic Rules | **Source NAT** | DMZ | Security | MAC Filter

Firewall - Source NAT

Source NAT define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Source NAT

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
<input type="text" value="New SNAT rule"/>	<input type="text" value="lan"/>	<input type="text" value="wan"/>	<input type="text" value="-- Please choose --"/>	<input type="text" value="Do not rewrite"/>	<input type="button" value="Add and edit..."/>

Traffic rule configuration page: This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Firewall - Traffic Rules - forwardtest

This page allows you to change advanced properties of the traffic rule entry, such as matched sou

Rule is enabled






Name

Restrict to address family

Protocol

Match ICMP type

Source zone

- Any zone
- lan: lan: 
- openvpn: (empty)
- vpnzone: (empty)
- wan: wan:  wan6:  ifmobile:  wwan: 

Source MAC address


Source address

Source port

Destination zone





Device (input)

Any zone (forward)

lan: lan: 

openvpn: (empty)

vpnzone: (empty)

wan: wan:  wan6:  ifmobile:  wwan: 

Destination address

Destination port

Action

Extra arguments

- **Name:** Traffic rule entry name.
- **Restrict to address family:** IPv4+IPv6, IPv4 and IPv6 can be selected. Specify the matched IP address family.
- **Protocol:** Specify the protocol matched in this rule. “Any” means any protocol is matched.
- **Source zone:** It is the zone that the traffic comes from.
- **Source MAC address:** Traffic rule check if the incoming packet’s source MAC address is matched.
- **Source address:** Traffic rule check if the incoming packet’s source IP address is matched.
- **Source port:** Traffic rule check if the incoming packet’s TCP/UDP port is matched.
- **Destination zone:** The zone that the traffic will go to.
- **Destination address:** Traffic rule check if the incoming packet’s destination IP address is matched.

- **Destination port:** Traffic rule check if the incoming packet's TCP/UDP port is matched.
- **Action:** If traffic is matched, the system will handle traffic according to the Action (accept, drop, reject, don't track).
- **Extra argument:** Passes additional argument to the iptable.

3.6.8.4 DMZ

General Settings Port Forwards Traffic Rules Source NAT DMZ Security MAC Filter

DMZ Configuration

You may setup a Demilitarized Zone(DMZ) to separate internal network and Internet.

Enable DMZ

IP address

Protocol

Save & Apply Save Reset

In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).

- **IP Address:** Please Enter the IP address of the computer which you want to set as DMZ host
- **Protocol:** All protocols, TCP+UDP,TCP,UDP.

Note: When DMZ host is settled, the computer is completely exposed to the external network; the firewall will not influence this host.

3.6.8.5 Security

<p>Status</p> <p>System</p> <p>Services</p> <p>Network</p> <p>Operation Mode</p> <p>Mobile</p> <p>LAN</p> <p>Wired WAN</p> <p>WAN IPv6</p> <p>Interfaces</p> <p>Wi-Fi</p> <p>Firewall</p> <p>Static Routes</p> <p>Switch</p> <p>DHCP and DNS</p> <p>Hostnames</p> <p>Loopback Interface</p> <p>Dynamic Routing</p> <p>Diagnostics</p> <p>QoS</p> <p>Load Balancing</p> <p>Logout</p>	<p>General Settings Port Forwards Traffic Rules Source NAT DMZ Security MAC Filter</p> <h3>System Security Configuration</h3> <p>SSH port <input type="text" value="22"/></p> <p>SSH access from WAN <input type="text" value="Allow"/></p> <p>Ping from WAN to LAN <input type="text" value="Allow"/></p> <p>Enable telnet <input type="checkbox"/></p> <h3>HTTPS Access</h3> <p>HTTPS port <input type="text" value="443"/></p> <p>HTTPS access from WAN <input type="text" value="Allow"/></p> <p>Remote network <input type="text" value="Any IP address"/></p> <h3>HTTP Access</h3> <p>HTTP port <input type="text" value="80"/></p> <p>HTTP access from WAN <input type="text" value="Allow"/></p> <p>Remote network <input type="text" value="Any IP address"/></p> <p>RFC1918 filter <input type="checkbox"/></p> <p>Enable lock account <input type="checkbox"/></p> <h3>Access Whitelist</h3> <p>Allow the whitelist to access device, others will be blocked</p> <p>Enable <input type="checkbox"/></p>
---	---

- **SSH access from WAN:** Allow or deny users to access the router from remote side.
- **Ping from WAN to LAN:** Allow or deny ping from remote side to the internal LAN subnet.
- **Enable telnet:** Default is “disable” for security.
- **HTTPS port:** Set HTTPS port. The default is 443.
- **HTTPS access from WAN:** Allow or deny access to the router web management page from the remote side.
- **Remote network:** Any IP Address, Single IP address, Subnet.
- **IP address:** Fill a remote IP address that can access the router’s web management page.

- **Netmask:** 24 means netmask 255.255.255.0, 32 means 255.255.255.255, the value is from 1 to 32.
- **HTTP port:** Set HTTP port. The default is 80.
- **HTTP access from WAN:** Allow or deny access to the router web management page from the remote side.
- **Remote network:** Any IP Address, Single IP address, Subnet.
- **IP address:** Fill a remote IP address that can access the router's web management page.
- **Netmask:** 24 means netmask 255.255.255.0, 32 means 255.255.255.255, the value is from 1 to 32.
- **RFC1918 filter:** Reject requests from RFC1918 IPs to public server IPs.
- **Enable lock account:** The web account will be locked after a number of unsuccessful login attempts.

Enable lock account

Max retries

Lock time minute(s)

- **Access Whitelist:** Allows IP addresses in the whitelist to access the device, and blocks everything else.

Access Whitelist

Allow the whitelist to access device, others will be blocked

Enable

IP address

3.6.9 Static Routes

Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	Table	
lan	192.168.8.0	255.255.255.0	192.168.1.107	0	1500	128	Delete

Add

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU	Table
-----------	--------	--------------	--------	-----	-------

This section contains no values yet

Add


Save & Apply Save Reset

- **Interface:** You can choose the corresponding interface type.
- **Target:** The destination host IP or network.
- **IPv4-Netmask:** The destination IP netmask.
- **IPv4-Gateway:** IP address of the next hop.
- **Metric:** Used by the router to make routing decisions.
- **MTU:** Maximum transmission unit.
- **Table:** The route table ID. The default value is 254. Valid table ID 1-254.

Note:

- The Gateway and LAN IP of this router must belong to the same network segment.
- If the destination IP address is that of a host, then the Netmask must be 255.255.255.255.
- If the destination IP address is an IP network segment, it must match with the Netmask. For example, if the destination IP is 10.0.0.0, and the Netmask is 255.0.0.0.

3.6.10 Switch


CM950W Industrial Router 5G/4G/3G
www.comset.com.au
your m2m specialist
AUTO REFRESH ON

Status

System

Services

Network

Operation Mode

Mobile

LAN

Wired WAN

WAN IPv6

Interfaces

Wi-Fi

Firewall

Static Routes

Switch

DHCP and DNS

Switch

The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Switch "switch0" (mt7530)

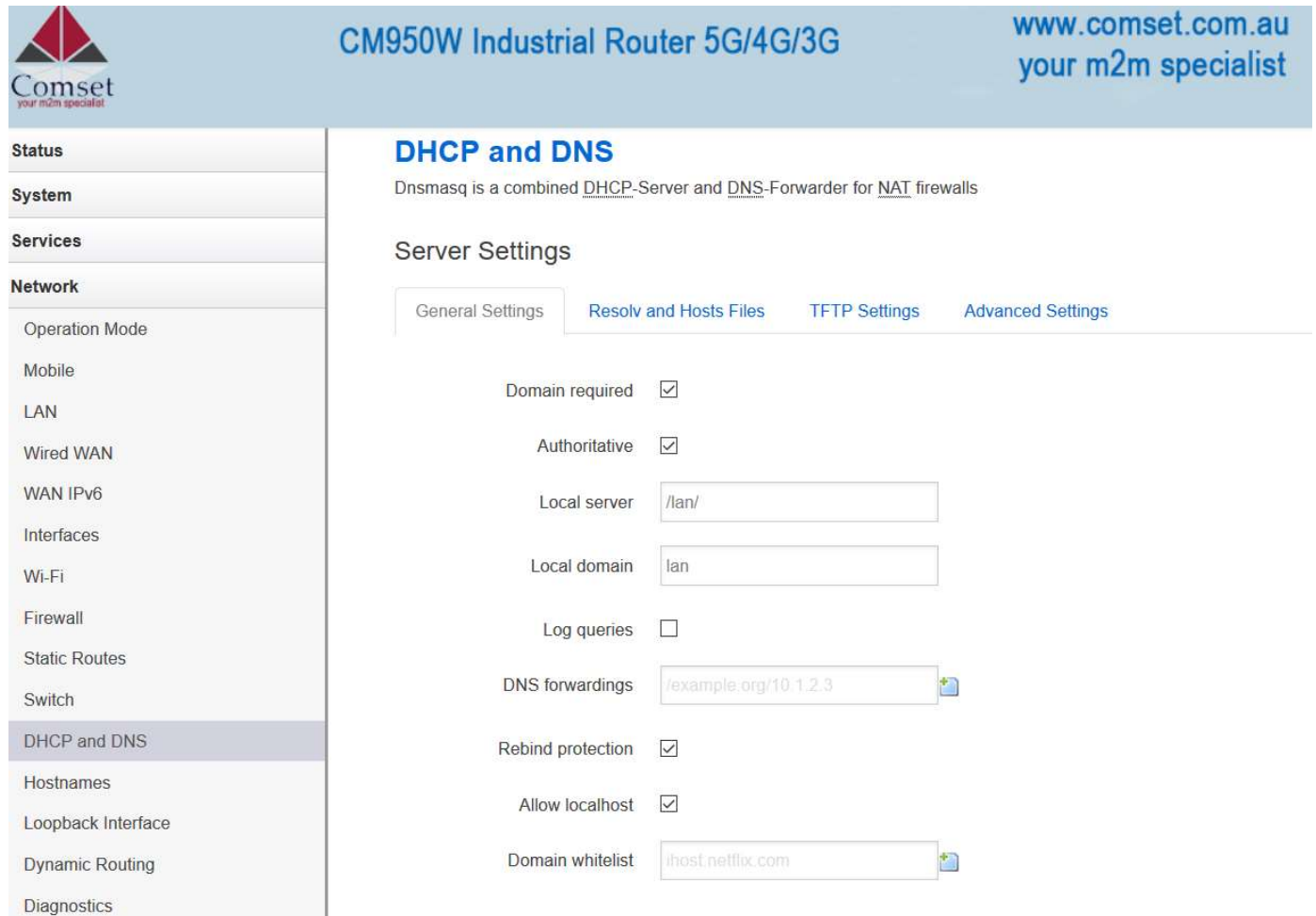
VLANs on "switch0" (mt7530)

VLAN ID	Port 0	Port 1	Port 2	Port 3	Port 4	Port 5	CPU	Port 7	
1	untagged	untagged	untagged	untagged	off	off	tagged	off	Delete
2	off	off	off	off	untagged	off	tagged	off	Delete



Note:

1. Port 4 is Wired-WAN port, port 0, port 1, port 2, port 3 are LAN ports.
2. "Untagged" means the Ethernet frame transmits from this port without VLAN tag.
3. "Tagged" means the Ethernet frame transmits from this port with VLAN tag.
4. "Off" means this port does not belong to VLAN. For default settings, port 0 belongs to VLAN1, but does not belong to VLAN 2.

3.6.11 DHCP and DNS



The screenshot shows the web interface for the CM950W Industrial Router. The top navigation bar includes the Comset logo, the product name 'CM950W Industrial Router 5G/4G/3G', and the website 'www.comset.com.au your m2m specialist'. On the left is a sidebar menu with categories: Status, System, Services, and Network. Under Network, options include Operation Mode, Mobile, LAN, Wired WAN, WAN IPv6, Interfaces, Wi-Fi, Firewall, Static Routes, Switch, DHCP and DNS (highlighted), Hostnames, Loopback Interface, Dynamic Routing, and Diagnostics. The main content area is titled 'DHCP and DNS' and contains a description: 'Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls'. Below this is a 'Server Settings' section with four tabs: 'General Settings' (selected), 'Resolv and Hosts Files', 'TFTP Settings', and 'Advanced Settings'. The 'General Settings' tab contains the following configuration items:

- Domain required:
- Authoritative:
- Local server:
- Local domain:
- Log queries:
- DNS forwardings: 
- Rebind protection:
- Allow localhost:
- Domain whitelist: 



- **Domain required:** Do not forward DNS-requests without DNS-Name.
- **Authoritative:** This is the only DHCP on the local network.
- **Local server:** Local domain specifications. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only.
- **Local domain:** Local domain suffix appended to DHCP names and hosts file entries.
- **Log queries:** Write received DNS requests to syslog.
- **DNS forwardings:** List of DNS servers to forward requests to.
- **Rebind protection:** Discard upstream RFC1918 responses.
- **Allow localhost:** Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services.
- **Domain whitelist:** List of domains to allow RFC1918 responses for.

General Settings

Resolv and Hosts Files

TFTP Settings

Advanced Settings

Suppress logging	<input type="checkbox"/>
Allocate IP sequentially	<input type="checkbox"/>
Filter private	<input checked="" type="checkbox"/>
Filter useless	<input type="checkbox"/>
Localise queries	<input checked="" type="checkbox"/>
Expand hosts	<input checked="" type="checkbox"/>
No negative cache	<input type="checkbox"/>
Strict order	<input type="checkbox"/>
Bogus NX Domain Override	<input type="text" value="67.215.65.132"/> 
DHCP Relay	<input type="text"/> 
DNS server port	<input type="text" value="53"/>
DNS query port	<input type="text" value="any"/>
Max. DHCP leases	<input type="text" value="unlimited"/>
Max. EDNS0 packet size	<input type="text" value="1280"/>
Max. concurrent queries	<input type="text" value="150"/>

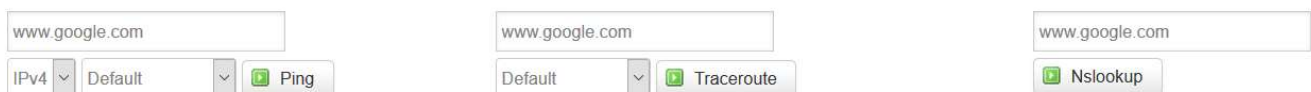
- **Suppress logging:** Suppress logging of the routine operation of these protocols.
- **Allocate IP sequentially:** Allocate IP addresses sequentially, starting from the lowest available address.
- **Filter private:** Do not forward reverse lookups for local networks.
- **Filter useless:** Do not forward requests that cannot be answered by public name servers.
- **Localise queries:** Localise hostname depending on the requesting subnet if multiple IPs are available.

- **Expand hosts:** Add local domain suffix to names served from hosts files.
- **No negative cache:** Do not cache negative replies, e.g. for non-existing domains.
- **Strict order:** DNS servers will be queried in the order of the resolvfile.
- **Bogus NX Domain Override:** List of hosts that supply bogus NX domain results.
- **DNS server port:** Listening port for inbound DNS queries.
- **DNS query port:** Fixed source port for outbound DNS queries.
- **Max DHCP leases:** Maximum allowed number of active DHCP leases.
- **Max edns0 packet size:** Maximum allowed size of EDNS.0 UDP packets.
- **Max concurrent queries:** Maximum allowed number of concurrent DNS queries.

3.6.12 Diagnostics

Diagnostics

Network Utilities

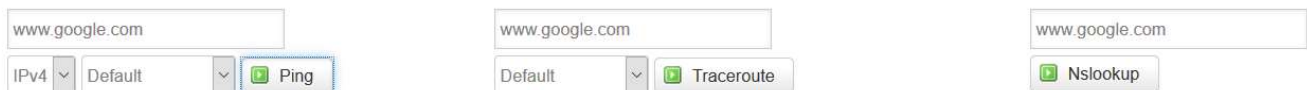


The image shows three separate input forms for network utilities. Each form has a text input field containing 'www.google.com'. The first form has dropdown menus for 'IPv4' and 'Default', and a 'Ping' button. The second form has a dropdown menu for 'Default' and a 'Traceroute' button. The third form has an 'Nslookup' button.

- **Ping:** It is a tool used to test the reachability of a host on an Internet Protocol (IP) network.
- **Traceroute:** It is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.
- **Nslookup:** It is a network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

For example if you want to ping www.google.com, type the target domain name or IP address, then click the button “Ping”. Wait a couple of seconds, the result will be shown as below.

Network Utilities



The image shows three separate input forms for network utilities, identical to the previous image. The 'Ping' button in the first form is highlighted with a blue border.

```
PING www.google.com (142.250.66.196): 56 data bytes
64 bytes from 142.250.66.196: seq=0 ttl=114 time=33.537 ms
64 bytes from 142.250.66.196: seq=1 ttl=114 time=33.106 ms
64 bytes from 142.250.66.196: seq=2 ttl=114 time=52.814 ms
64 bytes from 142.250.66.196: seq=3 ttl=114 time=52.517 ms
64 bytes from 142.250.66.196: seq=4 ttl=114 time=52.231 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 33.106/44.841/52.814 ms
```

3.6.13 Loopback Interface

Loopback Interface Configuration

IP address	<input type="text" value="127.0.0.1"/>
Netmask	<input type="text" value="255.0.0.0"/>

The default Loopback interface has IP address 127.0.0.1. You can change it if required.

3.6.14 Dynamic Routing

Dynamic Routing is implemented by quagga-0.99.22.4. Dynamic Routing services can be enabled:



CM950W Industrial Router 5G/4G/3G

Status

System

Services

Network

Operation Mode

Mobile

LAN

Wired WAN

WAN IPv6

Interfaces

Wi-Fi

Firewall

Static Routes

Switch

DHCP and DNS

Hostnames

Loopback Interface

Dynamic Routing

Diagnostics

QoS

Load Balancing

Logout

Dynamic Routing

Zebra

Enable

Password 

OSPF

Enable

Password 

OSPF6

Enable

Password 

RIP

Enable

Password 

RIPng

Enable

Password 

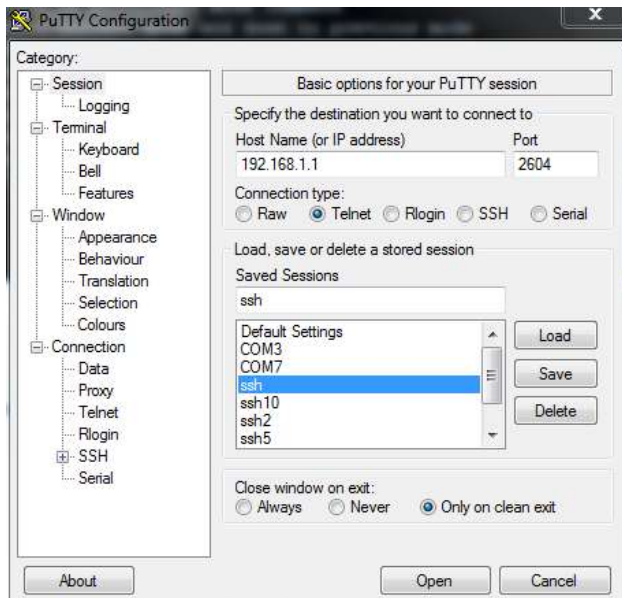
BGP

Enable

Password 

- **Zebra:** Zebra is an IP routing manager. Telnet port number is 2601.
- **OSPF:** Open Shortest Path First. Telnet port number is 2604.
- **OSPF6:** Open Shortest Path First for IPv6. Telnet port number is 2606.
- **RIP:** Routing Information Protocol. Telnet port number is 2602.
- **RIPng:** It is an IPv6 reincarnation of the RIP protocol. Telnet port number is 2603.
- **BGP:** Border Gateway Protocol. Telnet port number is 2605.

Example: The router's LAN IP is 192.168.10.1. If we want to configure OSPF, we need to set OSPF to "Enable" first, then open putty in windows:



Input the password of OSPF. Then press key"?" for help.

```

Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
Cell_Router>
Cell_Router>
  echo      Echo a message back to the vty
  enable    Turn on privileged mode command
  exit      Exit current mode and down to previous mode
  help      Description of the interactive help system
  list      Print command list
  quit      Exit current mode and down to previous mode
  show      Show running system information
  terminal   Set terminal line parameters
  who       Display who is on vty
Cell_Router> [

```

3.6.15 QoS

QoS (Quality of Service) can prioritise network traffic selected by addresses, ports, or services.

Quality of Service

With QoS you can prioritize network traffic selected by addresses, ports or services.

Interfaces

WAN

Enable

Classification group

Calculate overhead

Half-duplex

Download speed (kbit/s)

Upload speed (kbit/s)

- **Enable:** Enable QoS on this interface.
- **Classification group:** Specify class group used for this interface.
- **Calculate overhead:** Decrease upload and download ratio to prevent link saturation.
- **Download speed:** Download limit in kilobits/second.
- **Upload speed:** Upload limit in kilobits/second.

Classification Rules

Target	Source host	Destination host	Service	Protocol	Ports	Number of bytes	Comment
priority	all	all	all	all	22,53		ssh, dns
normal	all	all	all	TCP	20,21,25,80,110,443,993,995		ftp, smtp, http(s), imap
express	all	all	all	all	5190		AOL, iChat, ICQ

Each section defines one group of packets and which target (i.e. bucket) this group belongs to. All the packets share the bucket specified.

- **Target:** The four defaults are: priority, express, normal, low.
- **Source host:** Packets matching this source host(s) (single IP or in CIDR notation) belong to the bucket defined in target.

- **Destination host:** Packets matching this destination host(s) (single IP or in CIDR notation) belong to the bucket defined in target.
- **Protocol:** Matching packets belong to the bucket defined in target.
- **Ports:** Matching packets belong to the bucket defined in target. If more than 1 port is required, they must be separated by a comma.
- **Number of bytes:** Matching packets belong to the bucket defined in target.