

Industrial Grade 3G 4G 4GX Cellular Router

User Manual

CM820Q-4



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	7
2.1 Overall Dimensions	7
2.2 Ports	8
2.3 Powering up the CM820Q-4	9
2.4 SIM/UIM card	9
2.5 Terminal block	10
2.6 Grounding	10
2.7 Power Supply	10
2.8 LED Description	10
3 Software configuration	12
3.1 Overview	12
3.2 How to log in to the Router	12
3.3 Router status	15
3.3.1 Status overview	15
3.3.2 Network status	16
3.3.3 Firewall status	19
3.3.4 Routes	20
3.3.5 System log	20
3.3.6 Kernel log	21
3.3.7 Realtime graphs	22
3.4 System Configuration	22
3.4.1 Setup wizard	22
3.4.2 System	26
3.4.3 Password	29
3.4.4 Software	30
3.4.5 Backup/Restore	30
3.4.6 Upgrade	31
3.4.7 Reset	32
3.4.8 Reboot	32
3.5 Services configuration	33
3.5.1 ICMP check	33
3.5.2 VRRP	34
3.5.3 Failover (link backup)	35
3.5.4 DTU	37
3.5.5 SNMP	39
3.5.6 GPS (optional)	41

3.5.7 SMS.....	43
3.5.8 VPN.....	48
3.5.8.1 IPSEC.....	48
3.5.8.2 PPTP.....	50
3.5.8.3 L2TP.....	52
3.5.8.4 OpenVPN.....	55
3.5.8.5 GRE tunnel.....	57
3.5.9 DDNS.....	58
3.5.10 Connect Radio Module.....	60
3.6 Network Configuration.....	62
3.6.1 Operation Mode.....	62
3.6.2 Mobile configuration.....	63
3.6.3 Cell mobile data limitation.....	64
3.6.4 LAN settings.....	65
3.6.5 WAN.....	68
3.6.6 WiFi Settings.....	69
3.6.6.1 Wifi General configuration.....	69
3.6.6.2 WiFi Advanced Configuration.....	70
3.6.6.3 WiFi Interface Configuration.....	70
3.6.6.4 WiFi AP client.....	72
3.6.7 Interfaces Overview.....	74
3.6.8 Firewall.....	75
3.6.8.1 General Settings.....	75
3.6.8.2 Port Forwards.....	75
3.6.8.3 Traffic rules.....	76
3.6.8.4 DMZ.....	80
3.6.8.5 Security.....	81
3.6.9 Static Routes.....	83
3.6.10 Switch.....	84
3.6.11 DHCP and DNS.....	85
3.6.12 Diagnostics.....	87
3.6.13 Loopback Interface.....	88
3.6.14 Dynamic Routing.....	88
3.6.15 QoS.....	91

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 can 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: <https://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 CM820Q-4 is an industrial grade 3G/4G/4GX LTE WiFi Modem Router based on the latest OpenWrt platform. With download speeds of up to 150 Mbps and upload speeds of up to 50 Mbps, it is the perfect choice for a wide range of industrial applications.

The Comset CM820Q-4 is designed to suit Australian conditions. It supports the latest LTE technology that performs fast and reliable data communication. It enables users to quickly create a secure and fast wireless network. It features a built-in WiFi N300 with speeds of up to 300 Mbps, one Ethernet WAN port for fixed internet connection and four Ethernet LAN ports. Other features include VPN IPSEC, PPTP, L2TP and Open VPN to establish a secure connection over the 3G/4G network.

The durable and rugged design makes the CM820Q-4 the router of choice for remote harsh environments. The compact design, easy integration and advanced built-in features make it suitable for a wide range of industrial M2M applications, including industrial automation, building automation, smart metering, security, surveillance, transportation, health, mining and environmental monitoring.

1.2 Typical Application Diagram

The Comset CM820Q-4 3G/4G/4GX Router is suitable for a wide range of machine-to-machine applications (M2M). A good example is the connection of ATM machines, POS systems, IP surveillance cameras and PLC controllers back to a server, over a secure 4G connection using a secure VPN IPSEC tunnel, as illustrated in the diagram below.



1.3 Features

The CM820Q-4 supports the following:

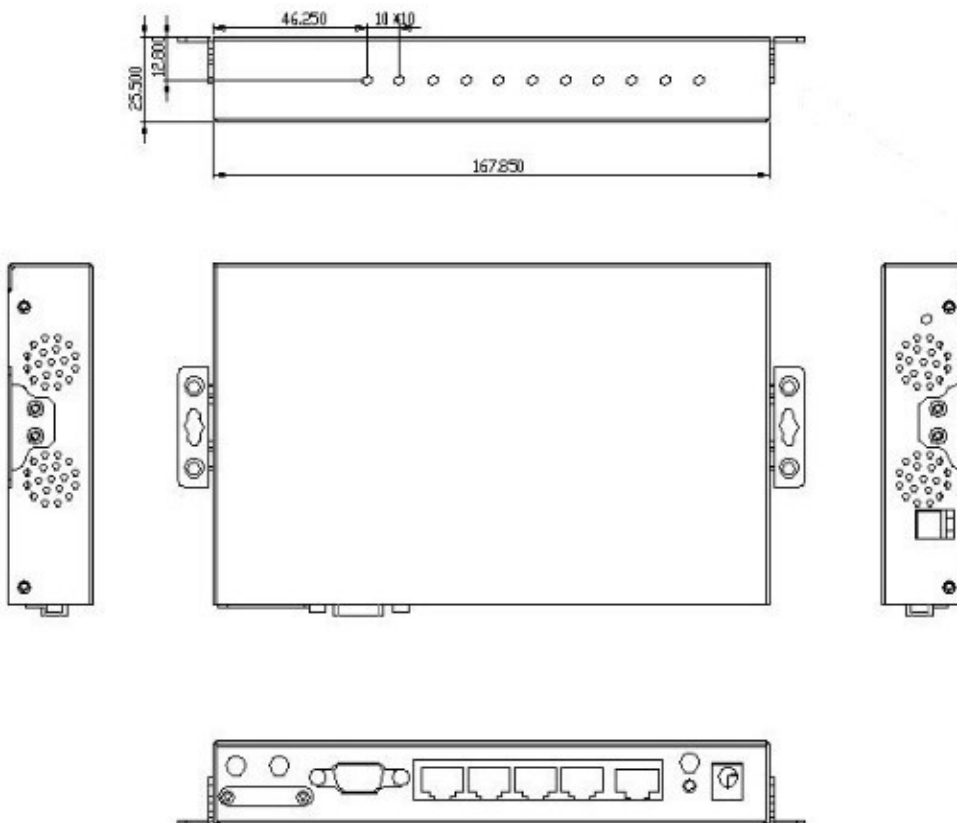
- LTE FDD B1/B2/B3/B4/B5/B7/B8/B28 and LTE TDD B40, with 3G fallback to DC-HSPA+/HSPA+/HSPA/WCDMA B1/B2/B4/B5/B8.
- IEEE802.11b/g/n N300 Wi-Fi AP function, WDS bridging, WEP, WPA/WPA2 Personal/Enterprise, TKIP/AES, Authenticated encryption mode.
- RS232 interface data transparent transmission and protocol conversion.
- On-demand dialing, including time on/off-line, voice or SMS control on/off-line, data trigger online or link idle offline.
- TCP/IP protocol stack, Telnet, HTTP, SNMP, PPP, PPPoE, network protocol.
- VPN IPSEC, PPTP, L2TP and Open VPN.
- Configuration via a user-friendly interface using a web browser.

Chapter 2

2 Hardware Installation

1. Overall Dimensions
2. Accessories
3. Installation

2.1 Overall Dimensions



2.2 Ports



Cell Main: Cellular Main

Cell Aux: Cellular Auxiliary

WiFi1: WiFi 1

SIM: SIM card slot

COM: DB9 serial port

LAN1~LAN4: Four LAN RJ45 Ethernet ports

WAN: WAN RJ45 Ethernet port

RST: System reset button

PWR: DC power socket. 5~40VDC



GND: DC wire ground

VCC: DC wire positive. Voltage range 5~40VDC

WPS: WPS button

WiFi2: WiFi 2



2.3 Powering up the CM820Q-4

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

2.4 SIM/UIM card

If your router has a SIM/UIM card cover, please remove it, and have the SIM card properly 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 “Vin”(DC5~40V).*

PIN	Signal	Description	Note
1	VCC	+5-40V DC Input	Current: 12V/1A
2	GND	Ground	

2.6 Grounding

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

2.7 Power Supply

The CM820Q-4 supports a wide range of DC voltage between 5 VDC and 40 VDC. The router is supplied with a 12 VDC 1.5 A power adapter.

2.8 LED Description

Please refer to the following table for LED description.

LED	Indication Light	Description
SYS	On for 25 seconds	Solid green for 25 seconds after power up
	Blinks	System normal operation
	Off or still on after 25 seconds	System set-up failure
LAN	Blinks	Ethernet data transmission
	Off	No Ethernet connection

	On	Ethernet is connected
VPN	On	VPN tunnel set-up
	Off	VPN tunnel not set-up or VPN failure
CELL	On	Solid orange light. Cell connection is 'UP' and now you have access to the Internet
WIFI	On	WiFi enabled
	Off	WiFi disabled
WAN	Blinks	Ethernet data transmission
	Off	No Ethernet connection
	On	Ethernet is connected
Signal	Off	No signal, or signal checking is not ready
	Blinks once every 4s	Signal bar is 1
	Blinks once every 3s	Signal bar is 2
	Blinks once every 2s	Signal bar is 3
	Blinks once every 1s	Signal bar is 4
	Blinks twice every 1s	Signal bar is 5

Chapter 3

3 Software configuration

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

3.1 Overview

The CM820Q-4 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 in to the Router

3.2.1 Network Configuration

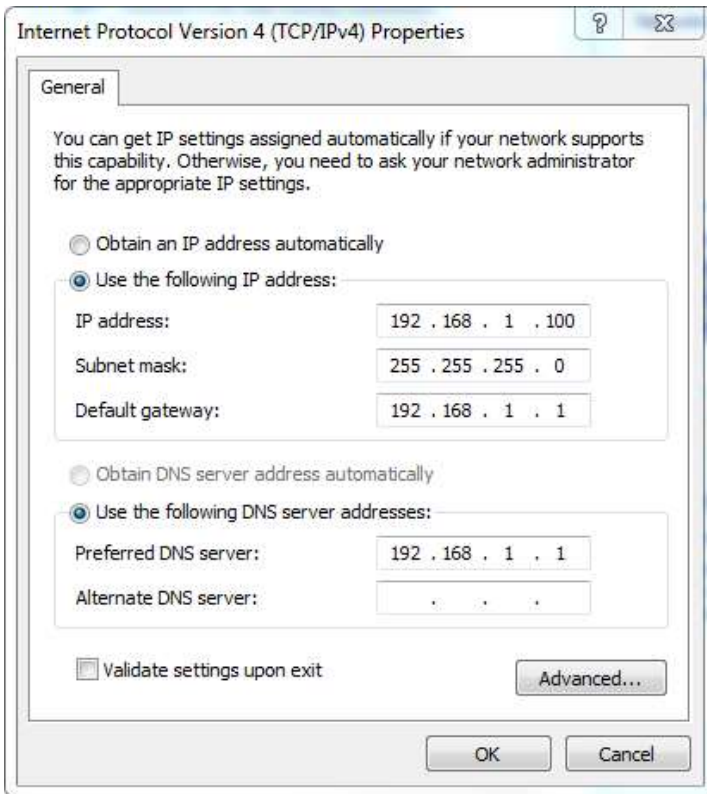
The router's default parameters are:

Default IP	192.168.1.1
Subnet mask	255.255.255.0

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

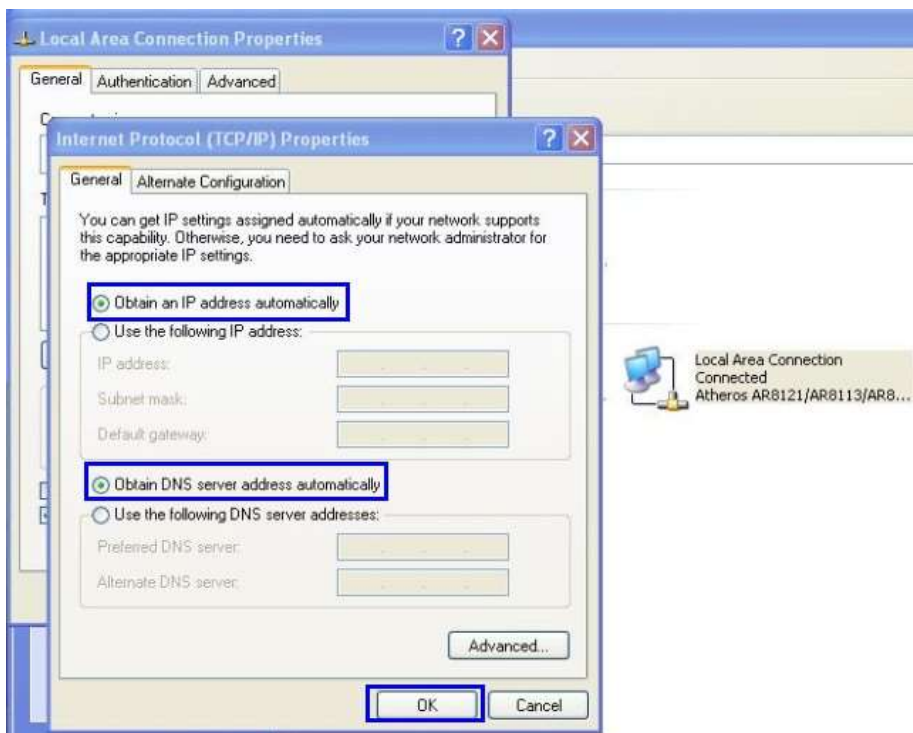
1) Manual settings

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 in to the router

- Open a Web browser and type <http://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.

Authorization Required
Please enter your username and password.

Username

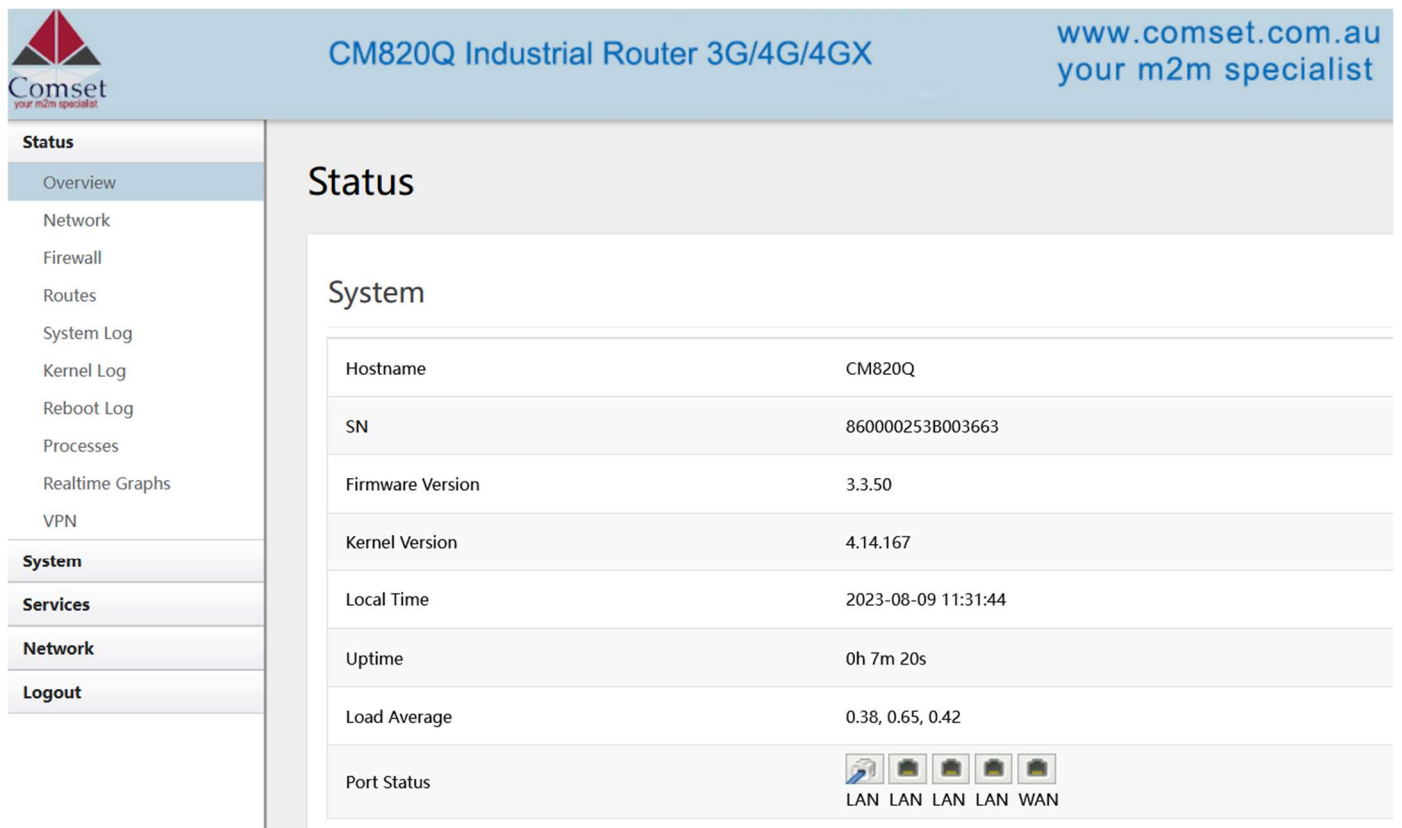
Password

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”.



The screenshot shows the web interface for the CM820Q Industrial Router. The header includes the Comset logo, the product name "CM820Q Industrial Router 3G/4G/4GX", and the website "www.comset.com.au your m2m specialist". A navigation sidebar on the left lists various system functions, with "Status" selected and "Overview" highlighted. The main content area displays the "Status" page, which includes a "System" section with the following details:

Hostname	CM820Q
SN	860000253B003663
Firmware Version	3.3.50
Kernel Version	4.14.167
Local Time	2023-08-09 11:31:44
Uptime	0h 7m 20s
Load Average	0.38, 0.65, 0.42
Port Status	 LAN LAN LAN LAN WAN

Mobile 1

Cellular Status	Connected
IP Address	10.247.151.139/29
DNS	10.3.8.2 10.3.56.162
Cell Modem	QUECTEL_EP06E (2C7C_0306)
Sim Status	SIM Ready
Strength	 25 / 31, dBm : -66
Selected Network	AUTO
Registered Network	Registered on Home network: Telstra Telstra,7
Sub Network Type	FDD LTE
Location Area Code	304B
Cell ID	82CA621
Band	7, 3148
IMEI/ESN	868186040089615
ICCID	89610182000965625752
RSRP	-97 dBm
RSRQ	-11 dB
SINR	15 dB
IMSI	505013539194792
PCI	69
PLMN	50501

3.3.2 Network status


The Network status page consists of 3 tabs, detailing information about the Mobile, WAN and LAN interfaces.

Mobile interface page:

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

Mobile WAN LAN

Mobile 1 Status

Cell Modem	QUECTEL_EP06E (2C7C_0306)
Sim Status	SIM Ready
Strength	 25 / 31, dBm : -63
Selected Network	AUTO
Registered Network	Registered on Home network: Telstra Telstra,7
Sub Network Type	FDD LTE
Location Area Code	304B
Cell ID	82CA621
Band	7, 3148
IMEI/ESN	868186040089615
ICCID	89610182000965625752
RSRP	-97 dBm
RSRQ	-11 dB
SINR	15 dB
IMSI	505013539194792
PCI	69
PLMN	50501

Interface Status

Interface	usb0
Uptime	0h 21m 29s
Protocol	dhcp
IP Addr.	10.247.151.139
Netmask	255.255.255.248
DNS	10.3.8.2 10.3.56.162
Gateway	10.247.151.140
MAC Addr.	02:50:F4:00:00:00
RX	5.02 MB (9853 Pkts.)
TX	1.63 MB (7890 Pkts.)

WAN status page:

Status	Mobile <u>WAN</u> LAN																												
Overview	<h2 style="margin-top: 0;">WAN Status</h2> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Interface</td><td style="text-align: right;">eth0.2</td></tr> <tr><td>Protocol</td><td style="text-align: right;">dhcp</td></tr> <tr><td>MAC Addr.</td><td style="text-align: right;">90:26:08:81:89:1C</td></tr> <tr><td>Connection</td><td style="text-align: right;">Down</td></tr> <tr><td>Uptime</td><td style="text-align: right;">0h 0m 0s</td></tr> <tr><td>RX</td><td style="text-align: right;">0 B (0 Pkts.)</td></tr> <tr><td>TX</td><td style="text-align: right;">12.14 KB (53 Pkts.)</td></tr> </table> <h2 style="margin-top: 10px;">WAN6 Status</h2> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Interface</td><td style="text-align: right;">eth0.2</td></tr> <tr><td>Protocol</td><td style="text-align: right;">dhcpv6</td></tr> <tr><td>MAC Addr.</td><td style="text-align: right;">90:26:08:81:89:1C</td></tr> <tr><td>Connection</td><td style="text-align: right;">Down</td></tr> <tr><td>Uptime</td><td style="text-align: right;">0h 0m 0s</td></tr> <tr><td>RX</td><td style="text-align: right;">0 B (0 Pkts.)</td></tr> <tr><td>TX</td><td style="text-align: right;">12.14 KB (53 Pkts.)</td></tr> </table>	Interface	eth0.2	Protocol	dhcp	MAC Addr.	90:26:08:81:89:1C	Connection	Down	Uptime	0h 0m 0s	RX	0 B (0 Pkts.)	TX	12.14 KB (53 Pkts.)	Interface	eth0.2	Protocol	dhcpv6	MAC Addr.	90:26:08:81:89:1C	Connection	Down	Uptime	0h 0m 0s	RX	0 B (0 Pkts.)	TX	12.14 KB (53 Pkts.)
Interface		eth0.2																											
Protocol		dhcp																											
MAC Addr.		90:26:08:81:89:1C																											
Connection		Down																											
Uptime		0h 0m 0s																											
RX		0 B (0 Pkts.)																											
TX		12.14 KB (53 Pkts.)																											
Interface		eth0.2																											
Protocol		dhcpv6																											
MAC Addr.		90:26:08:81:89:1C																											
Connection		Down																											
Uptime		0h 0m 0s																											
RX		0 B (0 Pkts.)																											
TX		12.14 KB (53 Pkts.)																											
Network																													
Firewall																													
Routes																													
System Log																													
Kernel Log																													
Reboot Log																													
Processes																													
Realtime Graphs																													
VPN																													
System																													
Services																													
Network																													
Logout																													

LAN status page:

Status

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

System

Services

Network

Logout

Mobile WAN **LAN**

LAN Status

Interface	br-lan
Protocol	static
IP Addr.	192.168.1.1
Netmask	255.255.255.0
IPv6 Addr.	fd07:f9d2:6bea::1/60
MAC Addr.	90:26:08:81:89:1B
Uptime	0h 24m 20s
RX	2.53 MB (13422 Pkts.)
TX	9.15 MB (13727 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.

Status

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

System

Services

Network

Logout

Firewall Status

IPv4 Firewall IPv6 Firewall

Hide empty chains Reset Counters Restart Firewall

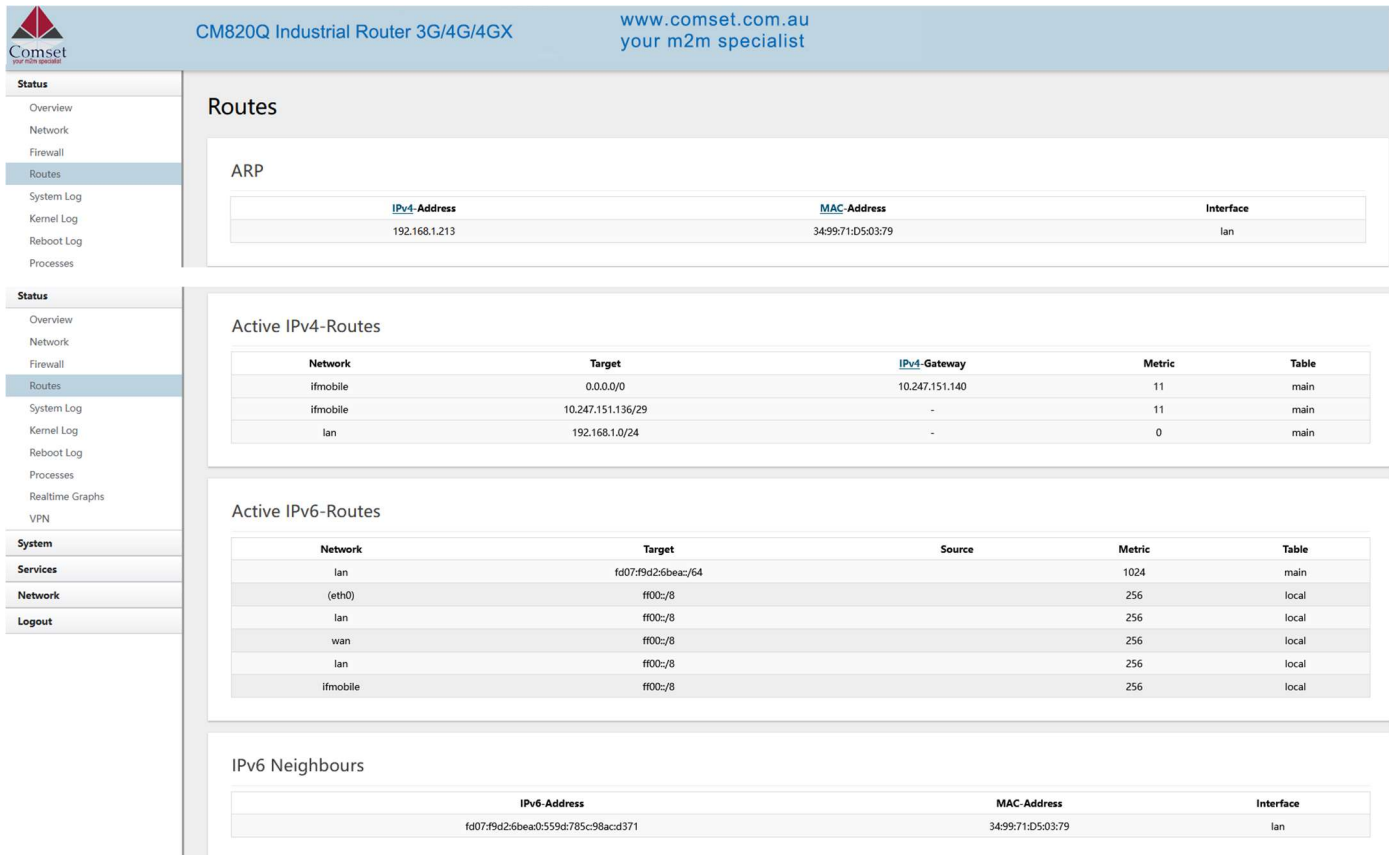
Table: Filter

Chain *INPUT* (Policy: ACCEPT, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1.42 K	140.66 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
4.08 K	521.85 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
3.45 K	480.64 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
299	15.55 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
621	40.88 KB	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	ppp+	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	vti+	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	eth0.2	*	0.0.0.0/0	0.0.0.0/0	-	-
7	335 B	zone_wan_input	all	usb0	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_ppptzone_input	all	ppptp+	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_l2tpzone_input	all	l2tp+	*	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.



The screenshot shows the web interface for the CM820Q Industrial Router. The left sidebar contains navigation options: Status, Overview, Network, Firewall, Routes (selected), System Log, Kernel Log, Reboot Log, Processes, System, Services, Network, and Logout. The main content area is titled 'Routes' and contains the following sections:

- ARP:** A table with columns for IPv4-Address, MAC-Address, and Interface.

IPv4-Address	MAC-Address	Interface
192.168.1.213	34:99:71:D5:03:79	lan
- Active IPv4-Routes:** A table with columns for Network, Target, IPv4-Gateway, Metric, and Table.

Network	Target	IPv4-Gateway	Metric	Table
ifmobile	0.0.0.0/0	10.247.151.140	11	main
ifmobile	10.247.151.136/29	-	11	main
lan	192.168.1.0/24	-	0	main
- Active IPv6-Routes:** A table with columns for Network, Target, Source, Metric, and Table.

Network	Target	Source	Metric	Table
lan	fd07:f9d2:6bea::/64		1024	main
(eth0)	ff00::/8		256	local
lan	ff00::/8		256	local
wan	ff00::/8		256	local
lan	ff00::/8		256	local
ifmobile	ff00::/8		256	local
- IPv6 Neighbours:** A table with columns for IPv6-Address, MAC-Address, and Interface.

IPv6-Address	MAC-Address	Interface
fd07:f9d2:6bea:0:559d:785c:98acd:371	34:99:71:D5:03:79	lan

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	System Log Last System Log
Overview	<h3 style="text-align: center;">System Log</h3> <p style="text-align: center;">Export syslog</p> <pre> Tue Aug 1 08:52:29 2023 kern.notice kernel: Linux version 4.14.167 (denty@denty-VirtualBox) (gcc version 7.5.0 (OpenWrt GCC 7.5.0 r10911-c155900f66)) #0 Wed Jan 29 16:05:35 2020 Tue Aug 1 08:52:29 2023 kern.info kernel: Board has DDR2 Tue Aug 1 08:52:29 2023 kern.info kernel: Analog PMU set to hw control Tue Aug 1 08:52:29 2023 kern.info kernel: Digital PMU set to hw control Tue Aug 1 08:52:29 2023 kern.info kernel: SoC Type: MediaTek MT7628AN ver:1 eco:2 Tue Aug 1 08:52:29 2023 kern.info kernel: CPU0 revision is: 00019655 (MIPS 24KEc) Tue Aug 1 08:52:29 2023 kern.info kernel: MIPS: machine is mt7628_model_3 Tue Aug 1 08:52:29 2023 kern.info kernel: Determined physical RAM map: Tue Aug 1 08:52:29 2023 kern.info kernel: memory: 04000000 @ 00000000 (usable) Tue Aug 1 08:52:29 2023 kern.info kernel: Initrd not found or empty - disabling initrd Tue Aug 1 08:52:29 2023 kern.warn kernel: Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes. Tue Aug 1 08:52:29 2023 kern.warn kernel: Primary data cache 32kB, 4-way, PIPT, no aliases, linesize 32 bytes Tue Aug 1 08:52:29 2023 kern.info kernel: Zone ranges: Tue Aug 1 08:52:29 2023 kern.info kernel: Normal [mem 0x0000000000000000-0x000000003fffffff] Tue Aug 1 08:52:29 2023 kern.info kernel: Movable zone start for each node Tue Aug 1 08:52:29 2023 kern.info kernel: Early memory node ranges Tue Aug 1 08:52:29 2023 kern.info kernel: node 0: [mem 0x0000000000000000-0x000000003fffffff] Tue Aug 1 08:52:29 2023 kern.info kernel: Initmem setup node 0 [mem 0x0000000000000000-0x000000003fffffff] Tue Aug 1 08:52:29 2023 kern.debug kernel: On node 0 totalpages: 16384 Tue Aug 1 08:52:29 2023 kern.debug kernel: free_area_init_node: node 0, pgdat 80464d20, node_mem_map 81000040 Tue Aug 1 08:52:29 2023 kern.debug kernel: Normal zone: 128 pages used for memmap Tue Aug 1 08:52:29 2023 kern.debug kernel: Normal zone: 0 pages reserved Tue Aug 1 08:52:29 2023 kern.debug kernel: Normal zone: 16384 pages, LIFO batch:3 Tue Aug 1 08:52:29 2023 kern.notice kernel: random: get_random_bytes called from 0x80468740 with crng_init=0 Tue Aug 1 08:52:29 2023 kern.info kernel: pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768 Tue Aug 1 08:52:29 2023 kern.debug kernel: pcpu-alloc: [0] 0 Tue Aug 1 08:52:29 2023 kern.info kernel: Built 1 zonelists, mobility grouping on. Total pages: 16256 Tue Aug 1 08:52:29 2023 kern.notice kernel: Kernel command line: console=ttyS0,57600 rootfstype=squashfs,jffs2 Tue Aug 1 08:52:29 2023 kern.info kernel: PID hash table entries: 256 (order: -2, 1024 bytes) Tue Aug 1 08:52:29 2023 kern.info kernel: Dentry cache hash table entries: 8192 (order: 3, 32768 bytes) Tue Aug 1 08:52:29 2023 kern.info kernel: Inode-cache hash table entries: 4096 (order: 2, 16384 bytes) Tue Aug 1 08:52:29 2023 kern.info kernel: Writing ErrCtl register=00000007 Tue Aug 1 08:52:29 2023 kern.info kernel: Readback ErrCtl register=00000007 Tue Aug 1 08:52:29 2023 kern.info kernel: Memory: 58956K/65536K available (3828K kernel code, 183K rwdata, 492K rodata, 1184K init, 198K bss, 6580K reserved, 0K cma-reserved) Tue Aug 1 08:52:29 2023 kern.info kernel: SLUB: Hwalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1 Tue Aug 1 08:52:29 2023 kern.info kernel: NR_IRQS: 256 Tue Aug 1 08:52:29 2023 kern.info kernel: irq: using register map from devicetree Tue Aug 1 08:52:29 2023 kern.info kernel: CPU Clock: 500MHz Tue Aug 1 08:52:29 2023 kern.crit kernel: timer_probe: no matching timers found Tue Aug 1 08:52:29 2023 kern.info kernel: clocksource: MIPS: mask: 0xffffffff max_cycles: 0xffffffff, max_idle_ns: 6590553264 ns Tue Aug 1 08:52:29 2023 kern.info kernel: sched_clock: 32 bits at 290MHz, resolution 3ns, wraps every 7405115902ns Tue Aug 1 08:52:29 2023 kern.info kernel: Calibrating delay loop... 385.04 BogoMIPS (lpj=1929216) Tue Aug 1 08:52:29 2023 kern.info kernel: pid_max: default: 32768 minimum: 301 Tue Aug 1 08:52:29 2023 kern.info kernel: Mount-cache hash table entries: 1024 (order: 0, 4096 bytes) </pre>
Network	
Firewall	
Routes	
System Log	
Kernel Log	
Reboot Log	
Processes	
Realtime Graphs	
VPN	
System	
Services	
Network	
Logout	

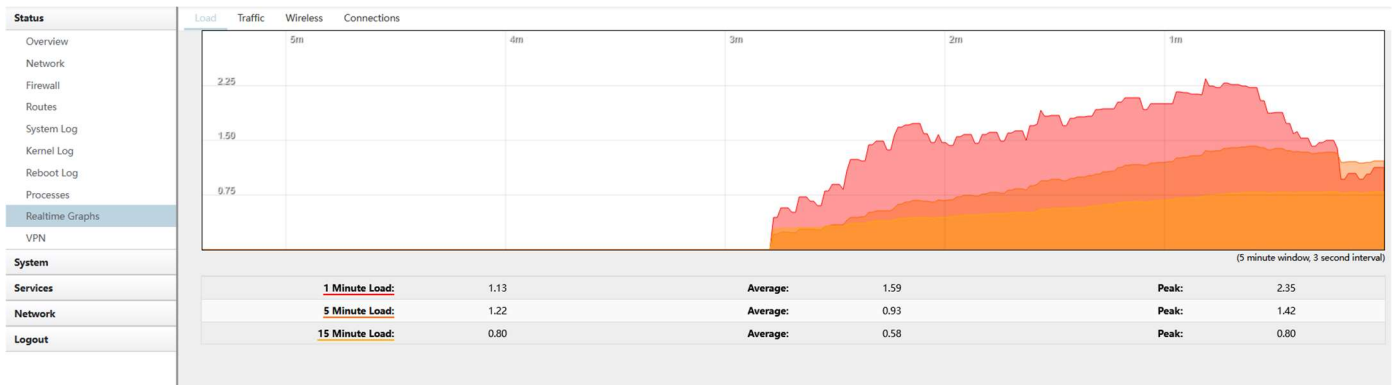
3.3.6 Kernel log

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	Kernel Log Last Kernel Log
Overview	<h3 style="text-align: center;">Kernel Log</h3> <p style="text-align: center;">Export log</p> <pre> Linux version 4.14.167 (denty@denty-VirtualBox) (gcc version 7.5.0 (OpenWrt GCC 7.5.0 r10911-c155900f66)) #0 Wed Jan 29 16:05:35 2020 Board has DDR2 Analog PMU set to hw control Digital PMU set to hw control SoC Type: MediaTek MT7628AN ver:1 eco:2 CPU0 revision is: 00019655 (MIPS 24KEc) MIPS: machine is mt7628_model_3 Determined physical RAM map: memory: 04000000 @ 00000000 (usable) Initrd not found or empty - disabling initrd Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes. Primary data cache 32kB, 4-way, PIPT, no aliases, linesize 32 bytes Zone ranges: Normal [mem 0x0000000000000000-0x000000003fffffff] Movable zone start for each node Early memory node ranges node 0: [mem 0x0000000000000000-0x000000003fffffff] Initmem setup node 0 [mem 0x0000000000000000-0x000000003fffffff] On node 0 totalpages: 16384 free_area_init_node: node 0, pgdat 80464d20, node_mem_map 81000040 Normal zone: 128 pages used for memmap Normal zone: 0 pages reserved Normal zone: 16384 pages, LIFO batch:3 random: get_random_bytes called from 0x80468740 with crng_init=0 pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768 pcpu-alloc: [0] 0 Built 1 zonelists, mobility grouping on. Total pages: 16256 Kernel command line: console=ttyS0,57600 rootfstype=squashfs,jffs2 PID hash table entries: 256 (order: -2, 1024 bytes) Dentry cache hash table entries: 8192 (order: 3, 32768 bytes) </pre>
Network	
Firewall	
Routes	
System Log	
Kernel Log	
Reboot Log	
Processes	
Realtime Graphs	
VPN	
System	
Services	
Network	
Logout	

3.3.7 Realtime graphs

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



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

System

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

Services

Network

Logout

Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi

Step - General

First, let's change your router password from the default one.

Web Password Settings

Current username	<input type="text"/>
Current password	<input type="password"/> *
New password	<input type="password"/> *
Confirm new password	<input type="password"/> *

System Settings

Current system time	Wed Aug 9 12:36:13 2023	Sync with browser
Timezone	Australia/Melbourne ▾	
Hostname	CM820Q	
Language	English ▾	

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

Status

System

System

Setup Wizard

Password

Software

Startup

Backup / Restore

Upgrade

Reset

Reboot

Services

Network

Logout

Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi

Mobile Configuration

SIM 1

Enable

Mobile connection DHCP mode ▾

PIN code

Dialing number *99#

APN telstra.internet

Authentication method None ▾

Dual APN support

Network Type automatic ▾

MTU 1500

- **Enable:** Enable mobile network.
- **Mobile connection:** Select a suitable mode for the mobile connection. The default value is 'DHCP mode'.
- **PIN code:** Most SIM cards don't have a PIN code, in which case you leave this field blank.
- **Dialing number:** Keep as default *99#.
- **APN:** Fill in the related value. This can be obtained from your carrier or SIM Card provider. The default value is telstra.internet.
- **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 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.

When finished, click "Save & Next"

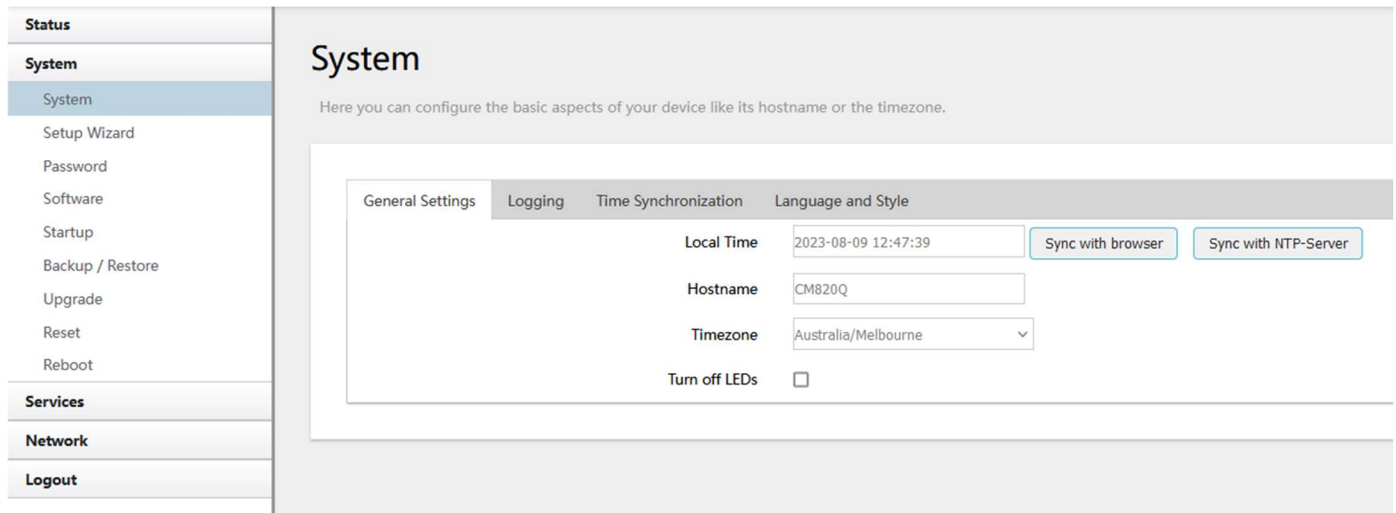
Status	Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi												
System	<h2>Step - LAN</h2> <p>Here we will setup the basic settings of a typical LAN configuration. The wizard will cover 2 basic configurations: static IP address LAN and DHCP client.</p> <h3>General Configuration</h3> <table> <tr> <td>IP address</td> <td><input type="text" value="192.168.1.1"/></td> </tr> <tr> <td>Netmask</td> <td><input type="text" value="255.255.255.0"/></td> </tr> <tr> <td>Enable DHCP</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Start</td> <td><input type="text" value="100"/></td> </tr> <tr> <td>Limit</td> <td><input type="text" value="150"/></td> </tr> <tr> <td>Lease time</td> <td><input type="text" value="12h"/></td> </tr> </table>	IP address	<input type="text" value="192.168.1.1"/>	Netmask	<input type="text" value="255.255.255.0"/>	Enable DHCP	<input checked="" type="checkbox"/>	Start	<input type="text" value="100"/>	Limit	<input type="text" value="150"/>	Lease time	<input type="text" value="12h"/>
IP address		<input type="text" value="192.168.1.1"/>											
Netmask		<input type="text" value="255.255.255.0"/>											
Enable DHCP		<input checked="" type="checkbox"/>											
Start		<input type="text" value="100"/>											
Limit		<input type="text" value="150"/>											
Lease time		<input type="text" value="12h"/>											
System													
Setup Wizard													
Password													
Software													
Startup													
Backup / Restore													
Upgrade													
Reset													
Reboot													
Services													
Network													
Logout													

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

Status	Step 1 - General Step 2 - Mobile Step 3 - LAN Step 4 - WiFi																						
System	<h2>Step - Wireless</h2> <p>Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters,</p> <h3>WiFi Configuration</h3> <table> <tr> <td>Enable wireless</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>SSID</td> <td><input type="text" value="Comset_01891b"/></td> </tr> <tr> <td>Transmit Power</td> <td><input type="text" value="20 dBm (100 mW)"/></td> </tr> <tr> <td>Band</td> <td><input type="text" value="2.4GHz (802.11g+n)"/></td> </tr> <tr> <td>HT mode (802.11n)</td> <td><input type="text" value="40MHz"/></td> </tr> <tr> <td>Force 40MHz mode</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Channel</td> <td><input type="text" value="11 (2.462 GHz)"/></td> </tr> <tr> <td>Encryption</td> <td><input type="text" value="WPA2-PSK"/></td> </tr> <tr> <td>Cipher</td> <td><input type="text" value="auto"/></td> </tr> <tr> <td>Key</td> <td><input type="password" value="....."/></td> </tr> <tr> <td>Country Code</td> <td><input type="text" value="AU - Australia"/></td> </tr> </table>	Enable wireless	<input checked="" type="checkbox"/>	SSID	<input type="text" value="Comset_01891b"/>	Transmit Power	<input type="text" value="20 dBm (100 mW)"/>	Band	<input type="text" value="2.4GHz (802.11g+n)"/>	HT mode (802.11n)	<input type="text" value="40MHz"/>	Force 40MHz mode	<input type="checkbox"/>	Channel	<input type="text" value="11 (2.462 GHz)"/>	Encryption	<input type="text" value="WPA2-PSK"/>	Cipher	<input type="text" value="auto"/>	Key	<input type="password" value="....."/>	Country Code	<input type="text" value="AU - Australia"/>
Enable wireless		<input checked="" type="checkbox"/>																					
SSID		<input type="text" value="Comset_01891b"/>																					
Transmit Power		<input type="text" value="20 dBm (100 mW)"/>																					
Band		<input type="text" value="2.4GHz (802.11g+n)"/>																					
HT mode (802.11n)		<input type="text" value="40MHz"/>																					
Force 40MHz mode		<input type="checkbox"/>																					
Channel		<input type="text" value="11 (2.462 GHz)"/>																					
Encryption		<input type="text" value="WPA2-PSK"/>																					
Cipher		<input type="text" value="auto"/>																					
Key		<input type="password" value="....."/>																					
Country Code		<input type="text" value="AU - Australia"/>																					
System																							
Setup Wizard																							
Password																							
Software																							
Startup																							
Backup / Restore																							
Upgrade																							
Reset																							
Reboot																							
Services																							
Network																							
Logout																							

Fill in parameters as required, then press “Finish”. Note: pressing the button “Save & Next” will save the configuration of the current page and jump to the next page. All configurations will be applied when you click the button “Finish” on this last page (WiFi).

3.4.2 System



The screenshot shows the 'System' configuration page. On the left is a navigation menu with categories: Status, System (selected), Services, Network, and Logout. Under 'System', there are links for System, Setup Wizard, Password, Software, Startup, Backup / Restore, Upgrade, Reset, and Reboot. The main content area is titled 'System' and contains the text: 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Below this is a tabbed interface with four tabs: 'General Settings' (selected), 'Logging', 'Time Synchronization', and 'Language and Style'. The 'General Settings' tab contains the following fields and controls:

Local Time	<input type="text" value="2023-08-09 12:47:39"/>	<input type="button" value="Sync with browser"/>	<input type="button" value="Sync with NTP-Server"/>
Hostname	<input type="text" value="CM820Q"/>		
Timezone	<input type="text" value="Australia/Melbourne"/>		
Turn off LEDs	<input type="checkbox"/>		

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 “CM820Q”.

➤ Time zone

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

➤ Turn off LEDs

Check this box to turn off LED lights if required.

Logging

Status

System

System

Setup Wizard

Password

Software

Startup

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.

General Settings

Logging

Time Synchronization

Language and Style

System log buffer size	<input type="text" value="64"/>
External system log server	<input type="text" value="0.0.0.0"/>
External system log server port	<input type="text" value="514"/>
External system log server protocol	<input type="text" value="UDP"/>
Write system log to file	<input type="text" value="/tmp/system.log"/>
Log output level	<input type="text" value="Debug"/>
Cron Log Level	<input type="text" value="Debug"/>
Record cell status	<input type="checkbox"/>

➤ 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 first lines of data will be lost.

➤ External system log server

Here you enter the IP address of the external log server. You can set up 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.

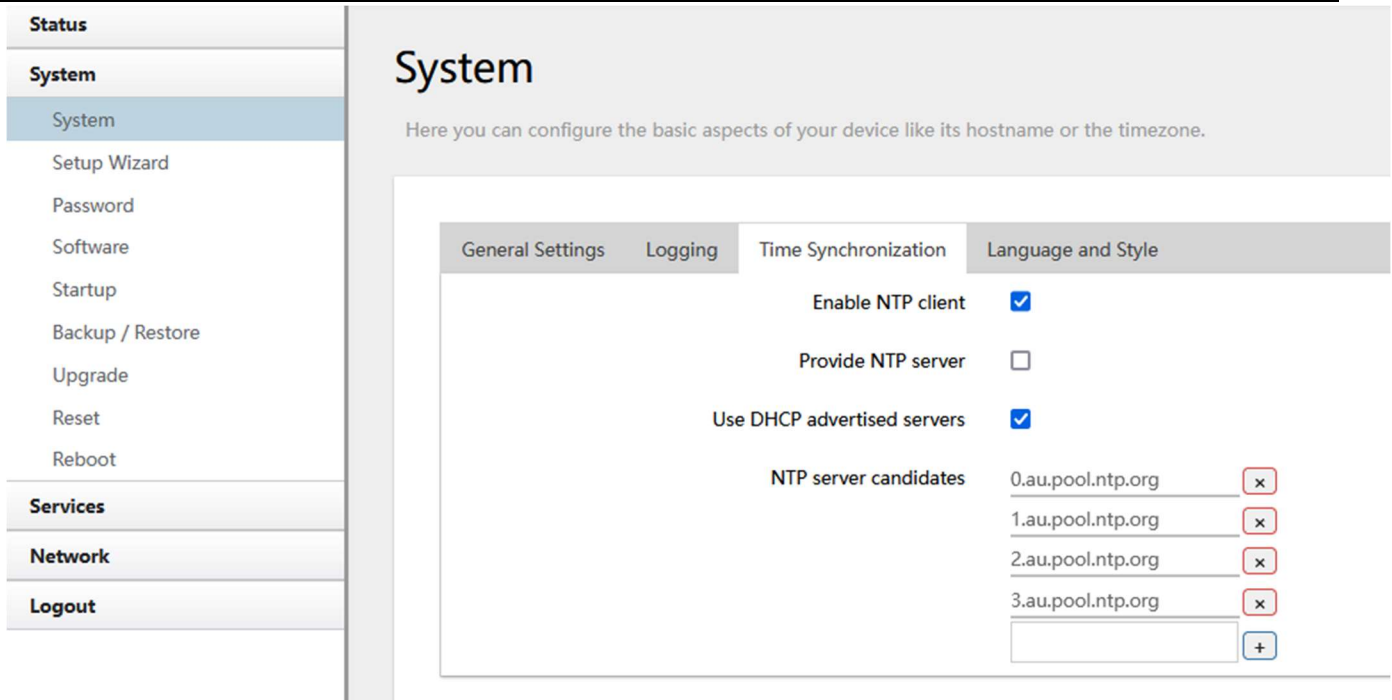
➤ Log output level

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.

Time Synchronisation



Status

System

- System
- Setup Wizard
- Password
- Software
- Startup
- 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.

General Settings Logging **Time Synchronization** Language and Style

Enable NTP client

Provide NTP server

Use DHCP advertised servers

NTP server candidates

0.au.pool.ntp.org	x
1.au.pool.ntp.org	x
2.au.pool.ntp.org	x
3.au.pool.ntp.org	x
<input type="text"/>	+

NTP is Network Timing Protocol. The default is the Australian NTP.



➤ **Enable NTP client**

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

➤ **Provide NTP server**

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

➤ **NTP server candidates**

It 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.

Language and Style

Status

System

- System
- Setup Wizard
- Password
- Software
- Startup
- 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.

- General Settings
- Logging
- Time Synchronization
- Language and Style

Language English

Design Material

The default language is “English”.

3.4.3 Password

Status

System

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

Services

Network

Logout

Web Account SSH Account Guest Account

Web Account

Changes web GUI username and password.
To change password you must enter: Current username, Current password, New password and Repeat new password.
To change Username you must enter: Current username, Current password, New username.

Current username

Current password *

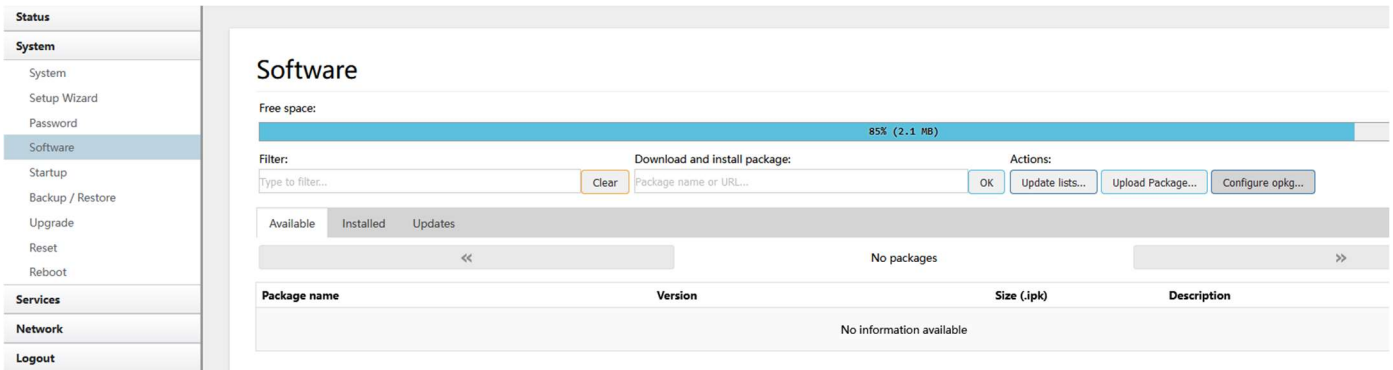
New username

New password *

Repeat new password *

Here you can change the web account username and password for accessing the device, as well as SSH account and Guest account logins.

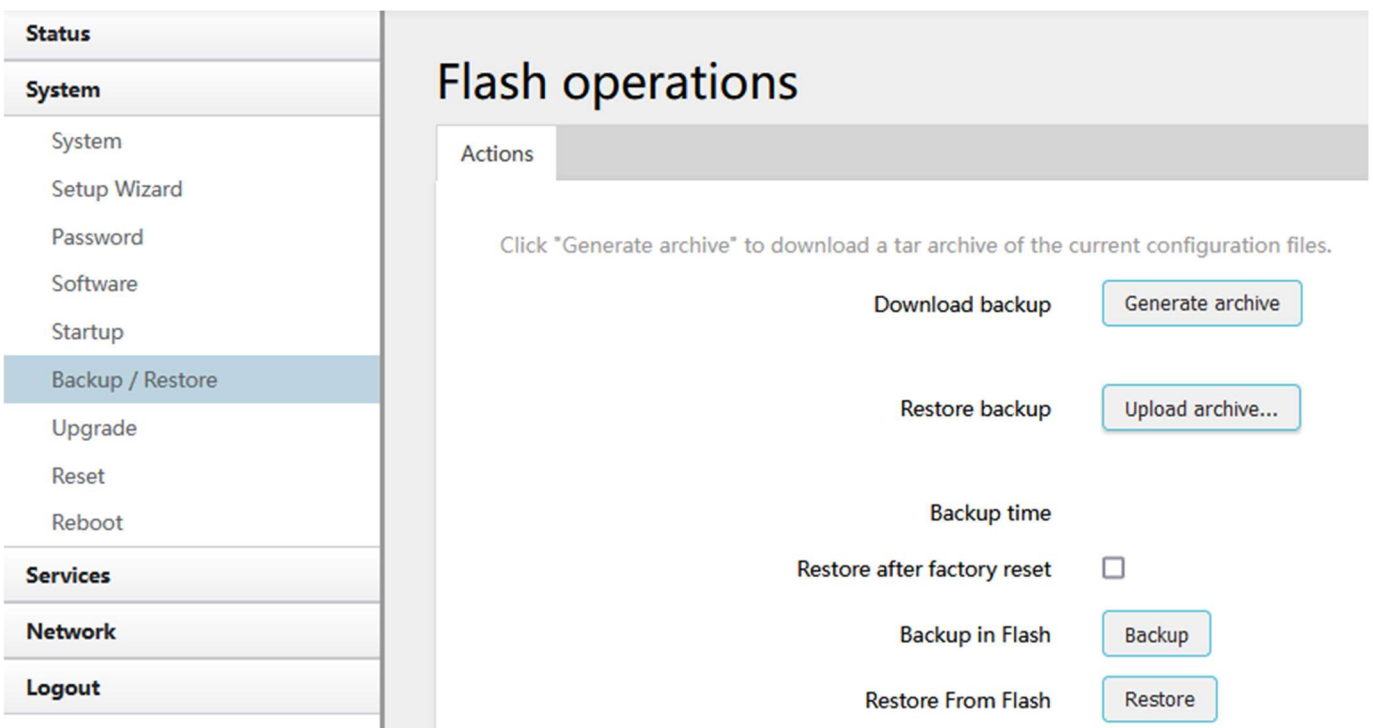
3.4.4 Software



The screenshot shows the 'Software' management page. On the left is a navigation menu with categories: Status, System, Services, Network, and Logout. Under 'System', 'Software' is selected. The main content area shows 'Free space: 85% (2.1 MB)' with a progress bar. Below is a 'Filter:' field and a 'Download and install package:' section with a text input, 'Clear' button, 'OK' button, and 'Update lists...' button. To the right are 'Actions:' buttons: 'Upload Package...', 'Configure opkg...', and 'Update lists...'. A table below shows columns for 'Available', 'Installed', and 'Updates', with 'No packages' displayed. At the bottom, a table header lists 'Package name', 'Version', 'Size (.ipk)', and 'Description', with 'No information available' shown below.

Here you can install custom software packages.

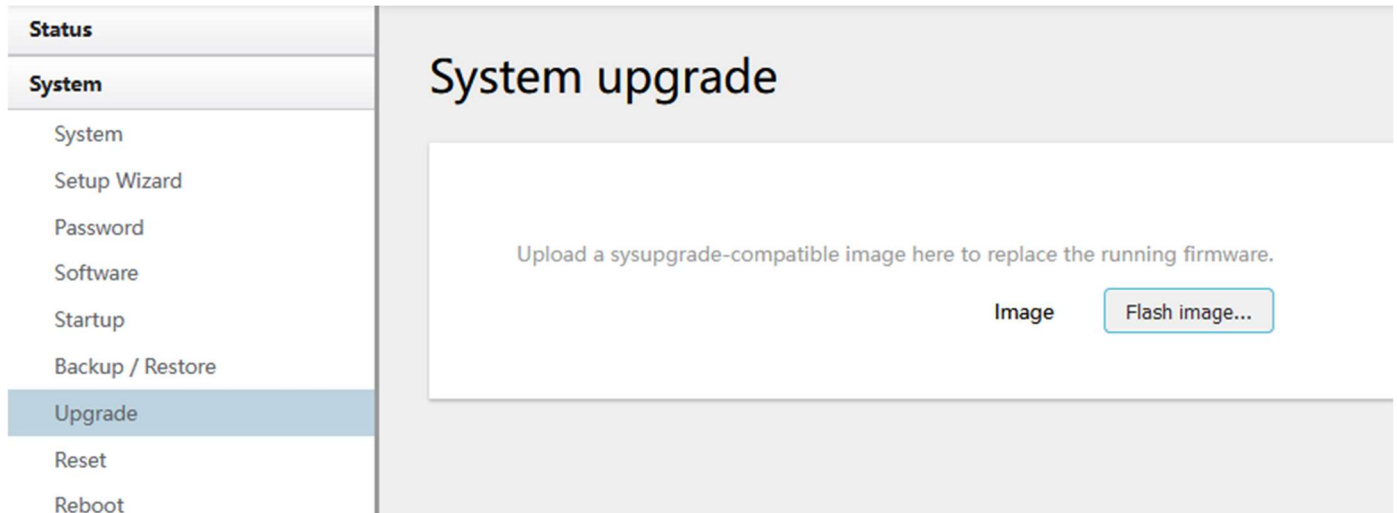
3.4.5 Backup/Restore



The screenshot shows the 'Flash operations' page. The left navigation menu has 'Backup / Restore' selected. The main content area has an 'Actions' tab. A text instruction says: 'Click "Generate archive" to download a tar archive of the current configuration files.' Below are several controls: 'Download backup' with a 'Generate archive' button; 'Restore backup' with an 'Upload archive...' button; 'Backup time' label; 'Restore after factory reset' with an unchecked checkbox; 'Backup in Flash' with a 'Backup' button; and 'Restore From Flash' with a 'Restore' button.

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

3.4.6 Upgrade



The screenshot shows a web interface for system upgrade. On the left is a navigation menu with 'Upgrade' selected. The main content area is titled 'System upgrade' and contains the instruction: 'Upload a sysupgrade-compatible image here to replace the running firmware.' Below this is a text input field labeled 'Image' and a button labeled 'Flash image...'.

Upload a system compatible firmware to replace the current firmware. Click the button “Flash image” and select compatible firmware, then click the button “Upload”. 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 un-checking “Keep settings” to prevent conflicting parameters after the firmware upgrade.

Click the button “Continue”

Flashing...

The system is flashing now.
DO NOT POWER OFF THE DEVICE!
⚙️ Wait a few minutes until you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

The system will restart after a few minutes.

Please Login

Please enter your username and password.

Username
Password

3.4.7 Reset

The screenshot shows a web interface for the 'Factory reset' function. On the left, a sidebar menu lists various system settings, with 'Reset' currently selected and highlighted in blue. The main content area has a header 'Factory reset' and a large white box containing two buttons: 'Reset to defaults' and 'Perform reset'. The 'Perform reset' button is highlighted with a red border.

This button resets all configurations to factory default. After clicking the button “Perform 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

The screenshot shows a web interface for 'Reboot Settings'. The left sidebar menu has 'Reboot' selected and highlighted in blue. The main content area is titled 'Reboot Settings' and contains several configuration options:

- 'Reboot at time' with an unchecked checkbox and three input fields for time (H:M:S) showing '16 :15 :00'.
- 'Reboot when timeout' with an unchecked checkbox and a 'Timer(min)' input field showing '1440'.
- 'Reboot Now' with a 'Perform reboot' button.

Click the button “Reboot Now” and the system will restart.

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	<h2>ICMP Check</h2> <p>Enable <input type="checkbox"/></p> <p>Host1 to ping <input type="text" value="www.google.com"/> ipv4 or hostname</p> <p>Host2 to ping <input type="text" value="8.8.8.8"/></p> <p>Ping packet size <input type="text" value="1"/> bytes.(range [1 - 1000])</p> <p>Ping timeout <input type="text" value="4"/> seconds (range [1 - 10])</p> <p>Max retries <input type="text" value="10"/> (range [3 - 1000])</p> <p>Interval between ping <input type="text" value="2"/> minutes (range [1 - 1440])</p> <p>Reconnect <input type="checkbox"/></p> <p>Start ping after cell up <input checked="" type="checkbox"/></p> <p>Action when failed <input type="text" value="Restart module"/></p>
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
DIO	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
Network	
Logout	

- **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.
- **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	
DIO	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
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. The legal number is from 1 to 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 a master. The legal number is from 1 to 255.

3.5.3 Failover (link backup)

Status

System

Services

- ICMP Check
- VRRP
- Failover
- DTU
- SNMP
- Modbus
- GPS
- SMS
- DIO
- VPN
- IPSec Track
- DDNS
- Connect Radio Module
- NMS
- Captive Portal

Network

Logout

Failover Advanced

Failover Configuration

Failover Settings

Enable	<input type="checkbox"/>
Back To High priority	<input checked="" type="checkbox"/>
Current interface	primary

Primary Configuration

Primary	<input type="text" value="Wired_wan"/>
Host1 to ping	<input type="text"/>
Host2 to ping	<input type="text"/>
Ping timeout	<input type="text" value="1"/>
Max Retries	<input type="text" value="10"/>
Interval between ping	<input type="text" value="30"/>
NAT	<input type="text" value="Default"/>

Status	<h2>Secondary Configuration</h2> <p>Secondary: <input type="text" value="Wired_wan"/></p> <p>Host1 to ping: <input type="text"/></p> <p>Host2 to ping: <input type="text"/></p> <p>Ping timeout: <input type="text" value="1"/></p> <p>Max Retries: <input type="text" value="10"/></p> <p>Interval between ping: <input type="text" value="30"/></p> <p>NAT: <input type="text" value="Default"/></p> <hr/> <h2>Third Configuration</h2> <p>Third: <input type="text" value="None"/></p> <p>Host1 to ping: <input type="text"/></p> <p>Host2 to ping: <input type="text"/></p> <p>Ping timeout: <input type="text" value="1"/></p> <p>Max Retries: <input type="text" value="10"/></p> <p>Interval between ping: <input type="text" value="30"/></p> <p>NAT: <input type="text" value="Default"/></p>
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
DIO	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
Network	
Logout	

- **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.

3.5.4 DTU

Notes:

- 1) This feature is for the CM820Q-4 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
- DIO
- VPN
- IPSec Track
- DDNS
- Connect Radio Module
- NMS
- Captive Portal

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

Status	<h3>Network Setting</h3> <p>Protocol: <input type="text" value="TCP"/></p> <p>Service mode: <input type="text" value="Client"/></p> <p>Enable Heartbeat: <input type="checkbox"/></p> <p>Heartbeat Interval: <input type="text" value="5"/></p> <p>Heartbeat Content: <input type="text"/></p>
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
DIO	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
Network	
Logout	

DTU center configuration	
CENTER1	
Center enable	<input checked="" type="checkbox"/>
Center IP/Domain	<input type="text" value="192.168.1.171"/>
Center Port	<input type="text" value="5000"/>
<input type="text"/>	<input type="button" value="Add"/>

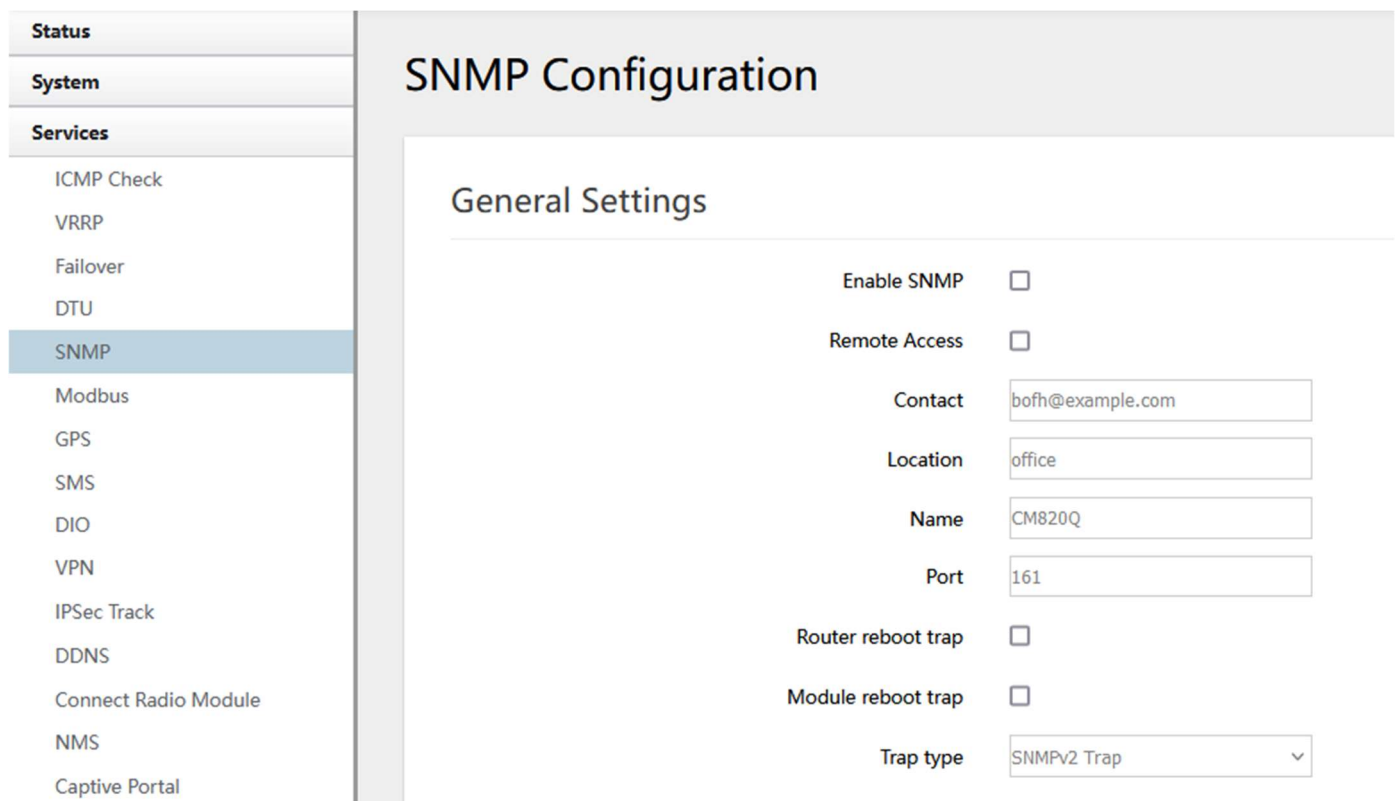
- **Enable:** Enable DTU feature.
- **Send DTU ID:** Send DTU ID at the front of the packet.
- **DTU ID:** The default DTU ID is the SN of the router. You can change it if required.
- **Forward delay:** This unit is in milliseconds. It is the time delay when sending data between the serial port and the network.
- **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 button “Delete” or set it to**

'Disabled'.

Notes:

The maximum number of DTU centers is 32.

3.5.5 SNMP




The screenshot shows the 'SNMP Configuration' page. On the left is a navigation menu with items: Status, System, Services, ICMP Check, VRRP, Failover, DTU, **SNMP**, Modbus, GPS, SMS, DIO, VPN, IPSec Track, DDNS, Connect Radio Module, NMS, and Captive Portal. The main area is titled 'SNMP Configuration' and contains a 'General Settings' section with the following options:

- Enable SNMP:
- Remote Access:
- Contact:
- Location:
- Name:
- Port:
- Router reboot trap:
- Module reboot trap:
- Trap type:



- **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"/> 
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)

Status	<h2>GPS Configuration</h2> <p>Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time</p> <p> <input type="checkbox"/> Enable <input type="checkbox"/> Prefix SN No. <input type="checkbox"/> Only GPRMC <input type="text" value="10"/> Send interval <input type="text" value="TCP"/> GPS send to <input type="text" value="192.168.1.100"/> Server IP/Domain <input type="text" value="6000"/> Server port </p>
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
DIO	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
Network	
Logout	

- **Enable:** Check this button to enable GPS.
- **Only GPRMC:** If checked, it will only send GPRMC data info (Longitude Latitude altitude)
- **Prefix SN No.:** If checked, it will add the router's SN to the data packet.
- **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 CM820Q-4 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 send to	Serial	▼
Serial baudrate	115200 bps	▼
Serial parity	None	▼
Serial databits	8 bits	▼
Serial stopbits	1 bits	▼
Serial flow control	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

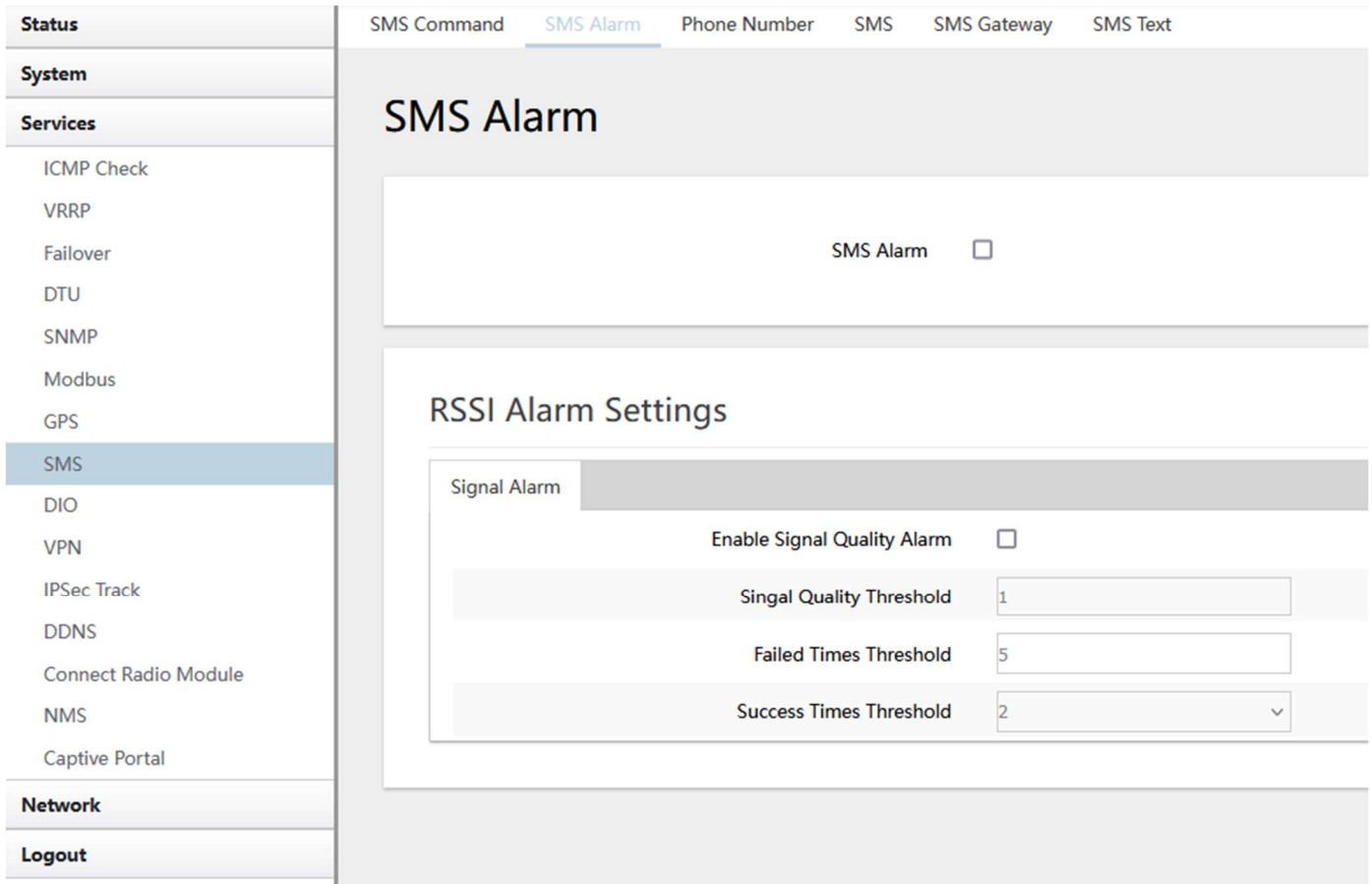
3.5.7 SMS

➤ SMS Command

Status	SMS Command	
System	Enable	<input type="checkbox"/>
Services	SMS ACK	<input type="checkbox"/>
ICMP Check	Fix error for some network	<input type="checkbox"/>
VRRP	Password access	<input type="checkbox"/>
Failover	Reboot Router Command	<input type="text" value="reboot"/>
DTU	Get Cell Status Command	<input type="text" value="cellstatus"/>
SNMP	Set Cell link-up Command	<input type="text" value="cellup"/>
Modbus	Set Cell link-down Command	<input type="text" value="celldown"/>
GPS	DIO_0 Set Command	<input type="text" value="dio01"/> <input type="button" value="Set DIO0"/>
SMS	DIO_0 Reset Command	<input type="text" value="dio00"/> <input type="button" value="Reset DIO0"/>
DIO	DIO_1 Set Command	<input type="text" value="dio11"/> <input type="button" value="Set DIO1"/>
VPN	DIO_1 Reset Command	<input type="text" value="dio10"/> <input type="button" value="Reset DIO1"/>
IPSec Track	DIO_2 Set Command	<input type="text" value="dio21"/> <input type="button" value="Set DIO2"/>
DDNS	DIO_2 Reset Command	<input type="text" value="dio20"/> <input type="button" value="Reset DIO2"/>
Connect Radio Module	DIO_3 Set Command	<input type="text" value="dio31"/> <input type="button" value="Set DIO3"/>
NMS	DIO_3 Reset Command	<input type="text" value="dio30"/> <input type="button" value="Reset DIO3"/>
Captive Portal	DIO Status Command	<input type="text" value="diostatus"/>
Network	Wifi On Command	<input type="text" value="wifion"/>
Logout	Wifi Off Command	<input type="text" value="wifioff"/>
Modbus	Force Cellup Command	<input type="text" value="forcecellup"/>
GPS	Operator List Command	<input type="text" value="operlist"/>
SMS	Operator set Command	<input type="text" value="operset"/>
DIO	Failover Switch Command	<input type="text"/>
VPN	SSH on Command	<input type="text" value="sshon"/>
IPSec Track	SSH off Command	<input type="text" value="sshoff"/>
DDNS	OpenVPN on command	<input type="text" value="openvpnon"/>
Connect Radio Module	OpenVPN off command	<input type="text" value="openvpnoff"/>
NMS		
Captive Portal		

- **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 (For routers with DIO option).
- **DIO_0 Reset Command:** Input the command for I/O port 0. For SMS feature, please keep the default parameters (For routers with DIO option).
- **DIO_1 Set Command:** Input the command for I/O port 1. For SMS feature, please keep the default parameters (For routers with DIO option).
- **DIO_1 Reset Command:** Input the command for I/O port 1. For SMS feature, please keep the default parameters (For routers with DIO option).
- **DIO Status Command:** Input the command for I/O port status. For SMS feature, please keep the default parameters (For routers with DIO option).
- **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**

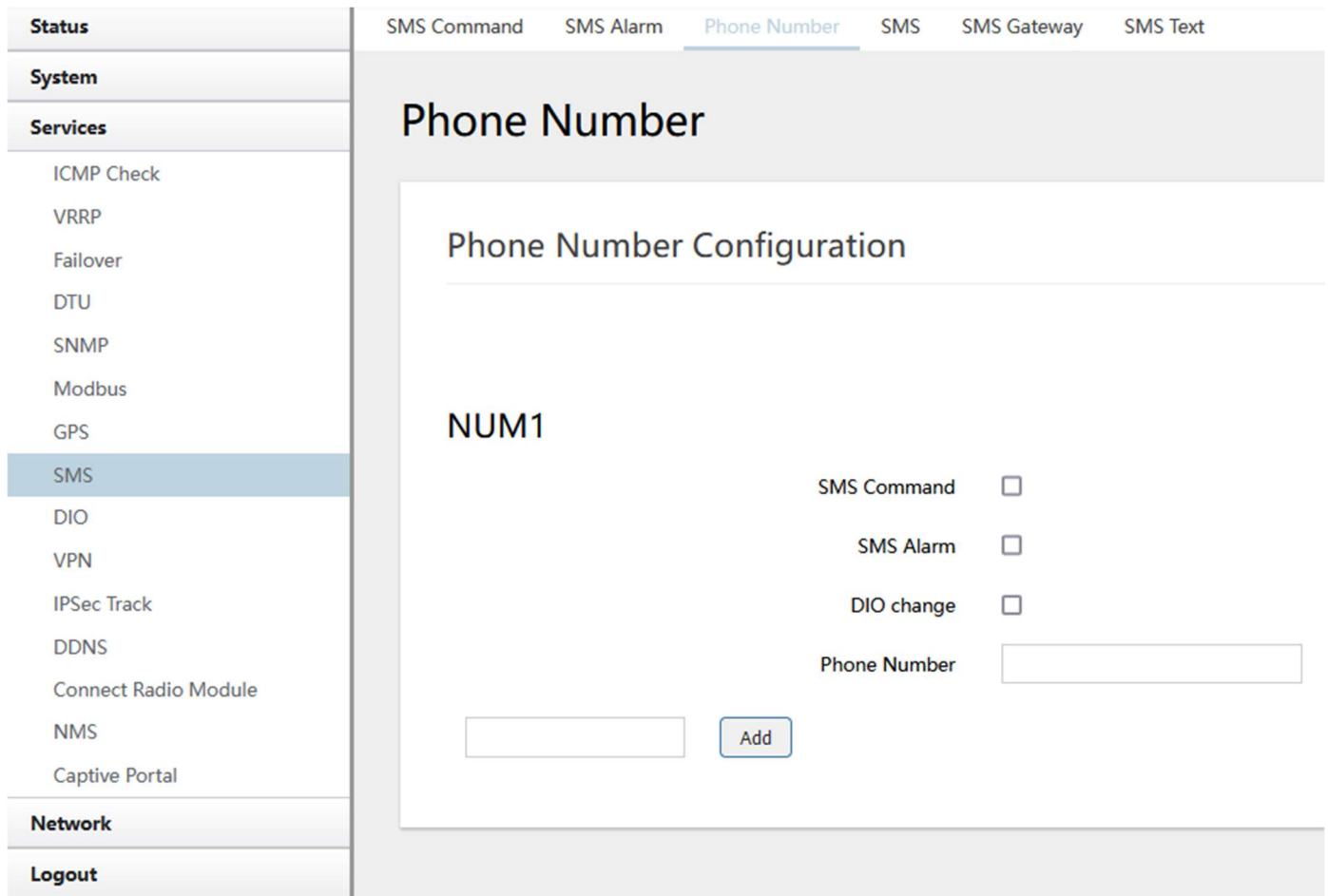


The screenshot displays the 'SMS Alarm' configuration page. The left sidebar includes sections for 'Status', 'System', 'Services', 'Network', and 'Logout'. Under 'Services', 'SMS' is selected. The main content area has tabs for 'SMS Command', 'SMS Alarm', 'Phone Number', 'SMS', 'SMS Gateway', and 'SMS Text'. The 'SMS Alarm' tab is active, showing a title 'SMS Alarm' and a checkbox labeled 'SMS Alarm'. Below this is the 'RSSI Alarm Settings' section, which includes a 'Signal Alarm' sub-section with the following settings:

- Enable Signal Quality Alarm:
- Signal Quality Threshold: 1
- Failed Times Threshold: 5
- Success Times Threshold: 2

- **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**



The screenshot shows a web interface for configuring phone numbers. On the left is a navigation menu with categories: Status, System, Services, SMS, Network, and Logout. The 'SMS' category is selected. The main content area has tabs for 'SMS Command', 'SMS Alarm', 'Phone Number', 'SMS', 'SMS Gateway', and 'SMS Text'. The 'Phone Number' tab is active, displaying a configuration page for a phone number named 'NUM1'. The configuration includes three checkboxes: 'SMS Command', 'SMS Alarm', and 'DIO change', all of which are currently unchecked. Below these is a text input field for the 'Phone Number'. At the bottom of the configuration area, there is another empty text input field and an 'Add' button.

- **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**

Status	SMS Command SMS Alarm Phone Number SMS SMS Gateway SMS Text
System	<h2>SMS Log</h2> <div style="border: 1px solid gray; height: 200px; width: 100%;"></div>
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
DIO	
VPN	
IPSec Track	
DDNS	
Connect Radio Module	
NMS	
Captive Portal	
Network	
Logout	

Here you can view SMS log activity.

3.5.8 VPN

3.5.8.1 IPSEC

Status	IPSec	PPTP	L2TP	OpenVPN	GRE Tunnel	ZeroTier
System	IPSec Instance: Ipsec_base					
Services	<p>Enable <input type="checkbox"/></p> <p>Exchange mode: IKEv1-Main</p> <p>Operation level: Main</p> <p>Authentication method: PSK Server</p> <p>Remote VPN endpoint: -- Please choose --</p> <p>Local endpoint: -- Please choose --</p> <p>Local IKE identifier: <input type="text"/></p> <p>Remote IKE identifier: <input type="text"/></p> <p>Connection type: Tunnel</p> <p>Preshared Keys: <input type="text"/> +</p> <p>Perfect Forward Secrecy: Enable</p> <p>DPD action: None</p> <p>DPD delay: 30 seconds</p> <p>DPD timeout: 150 seconds</p> <p>NAT Traversal: Enable</p> <p>Local source IP: <input type="text"/></p> <p>Remote source IP: <input type="text"/></p> <p>Additional phase1: <input type="text"/> </p> <p>Additional phase2: <input type="text"/> </p>					
Network	<p>Local LAN bypass <input type="checkbox"/></p> <p>Local subnet: 192.168.1.0/24 </p> <p>Remote subnet: 192.168.10.0/24 </p>					
Logout						

- **Enable:** Enable IPSEC feature

- **Exchange mode:** IKEv1-Main, IKEv1-Aggressive and IKEv2-Main modes are supported.
- **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.
- **Preshared Keys:** This is known as PSK. The length is 16 to 32.
- **Local subnet:** The local subnet which connects to the IPSEC VPN.
- **Remote subnet:** The remote subnet which connects to the IPSEC VPN.

Status	Phase 1 Proposal	
System	Enable	<input checked="" type="checkbox"/>
Services	Encryption algorithm	3DES
ICMP Check	Hash algorithm	HMAC_SHA1
VRRP	DH group	MODP1024/2
Failover	Life time	10800 seconds
DTU		
SNMP		
Modbus		
GPS		
SMS		
DIO		
VPN		
IPSec Track		
DDNS		
Connect Radio Module		
NMS		
Captive Portal		
Network		
Logout		
	Phase 2 Proposal	
	Enable	<input checked="" type="checkbox"/>
	Encryption algorithm	AES 128
	PFS group	MODP1024/2
	Authentication	HMAC_SHA1
	Life time	3600 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

Point-to-Point Tunneling Protocol

PPTP Configuration

Name	Type	Enable		
pptpc	Client	No	Edit	Delete
pptpsrv	Server	No	Edit	Delete

New instance name: Client

PPTP NAT enable

This page shows a list of configured PPTP instances and their state. Click the button “Edit” to make changes to an instance or click the button “Delete” to delete it.

➤ **PPTP Client configuration**

Status	PPTP Client Instance: Pptpc
System	
Services	
ICMP Check	
VRRP	
Failover	
DTU	
SNMP	
Modbus	
GPS	
SMS	
DIO	
VPN	Main Settings
IPSec Track	Enable <input type="checkbox"/>
DDNS	Server <input type="text"/>
Connect Radio Module	Username <input type="text"/>
NMS	Password <input type="password"/> *
Captive Portal	Remote LAN subnet <input type="text"/>
Network	Remote LAN netmask <input type="text"/>
Logout	MTU <input type="text" value="1500"/>
	Keep Alive <input type="text"/>
	Use DNS servers advertised by peer <input type="checkbox"/>
	MPPE Encryption <input type="checkbox"/>
	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"/>
	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.
- **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 default gateway:** If unchecked, no default route is configured.
- **Use DNS servers advertised by peer:** If unchecked, the advertised DNS server addresses are ignored.

➤ PPTP Server Configuration

Status

System

Services

ICMP Check

VRRP

Fallover

DTU

SNMP

Modbus

GPS

SMS

DIO

VPN

IPSec Track

DDNS

Connect Radio Module

NMS

Captive Portal

Network

Logout

PPTP Server Instance:

Main Settings

Enable

PPTP Local IP

PPTP remote IP start

PPTP remote IP end

IPCP-accept-remote

ARP Proxy

MPPE Encryption

Debug

Username	Password
youruser	*****
<input type="button" value="Add"/>	<input type="button" value="Delete"/>

- **Local IP:** Indicates the server's IP address.
- **Remote IP:** The remote IP address lease start.
- **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.
- **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 shows a list of configured L2TP instances and their state. Click the button "Edit" to make changes to an instance, or click the button "Delete" to delete it.

IPSec PPTP **L2TP** OpenVPN GRE Tunnel ZeroTier

Layer 2 Tunneling Protocol

L2TP Configuration

Name	Type	Enable	
L2tpc	Client	No	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
L2tpsrv	Server	No	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

New instance name:

L2TP NAT enable

➤ **L2TP Client configuration**

L2TP Client Instance: L2tpc

Main Settings

Enable

Server

Username

Password *

Remote LAN subnet

Remote LAN netmask

MTU

Keep Alive

Refuse PAP

Refuse EAP

Refuse CHAP

Refuse MS-CHAP

Debug

- **Enable:** Enable this L2TP instance.

- **Server:** Domain name or IP address of L2TP server.
- **Username:** Server authentication username.
- **Password:** Server authentication password.
- **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's mainly for the case that netifd sent the connect request yet xl2tpd failed to complete it without the notice of netifd.

➤ **L2TP Server configuration**

L2TP Server Instance: L2tpsrv

Main Settings

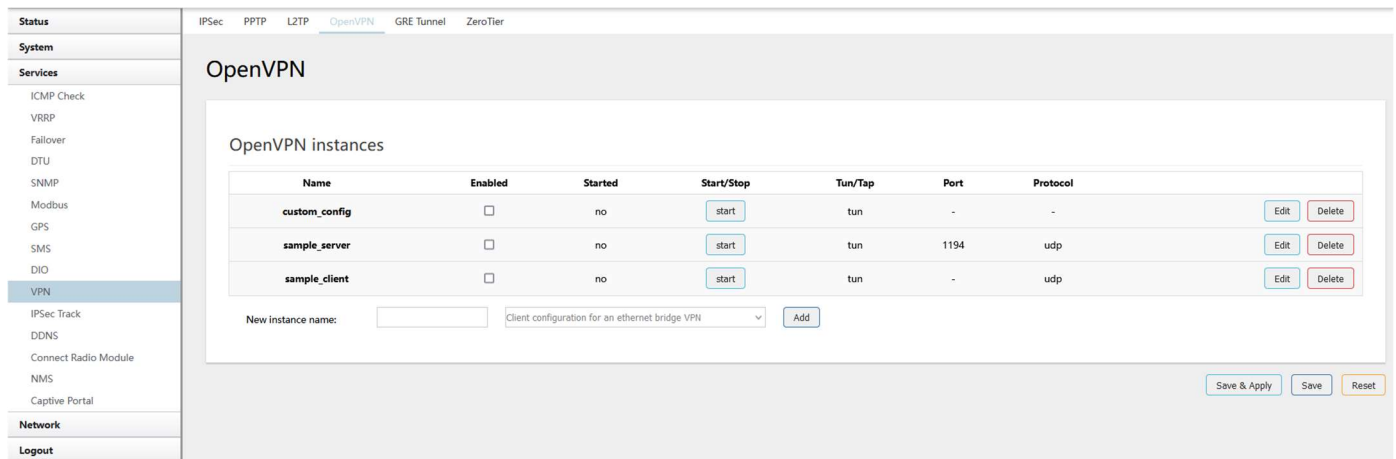
Enable	<input type="checkbox"/>
L2TP Local IP	<input style="width: 150px;" type="text" value="192.168.0.1"/>
Remote IP range begin	<input style="width: 150px;" type="text" value="192.168.0.20"/>
Remote IP range end	<input style="width: 150px;" type="text" value="192.168.0.30"/>
Remote LAN IP	<input style="width: 150px;" type="text"/>
Remote LAN netmask	<input style="width: 150px;" type="text" value="255.255.255.0"/>
DNS	<input style="width: 150px;" type="text"/>
IPCP-accept-remote	<input type="checkbox"/>
Length bit	<input type="checkbox"/>
IPSec saref	<input type="checkbox"/>
ARP Proxy	<input type="checkbox"/>
Debug	<input type="checkbox"/>

- **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:** L2TP client IP.
- **Remote LAN netmask:** The mask of L2TP client IP, the default value is 255.255.255.0
- **Username:** Server authentication username.
- **Password:** Server authentication password.

3.5.8.4 OpenVPN

This page is a list of configured OpenVPN instances and their state. Click the button “Edit” to make changes to an instance, or click the button “Delete” to delete it. Click the button “Start” or “Stop” to start or stop a specific instance.



The screenshot shows the 'OpenVPN' configuration page. On the left is a navigation menu with categories: Status, System, Services, VPN, Network, and Logout. The 'VPN' category is selected. The main content area is titled 'OpenVPN' and contains a table of instances and an 'Add' form.

Name	Enabled	Started	Start/Stop	Tun/Tap	Port	Protocol	
custom_config	<input type="checkbox"/>	no	start	tun	-	-	Edit Delete
sample_server	<input type="checkbox"/>	no	start	tun	1194	udp	Edit Delete
sample_client	<input type="checkbox"/>	no	start	tun	-	udp	Edit Delete

Below the table is a form to add a new instance:

New instance name: Client configuration for an ethernet bridge VPN

At the bottom right of the page are buttons: Save & Apply, Save, and Reset.

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	<input type="checkbox"/>
verb	<input type="text" value="3"/>
port	<input type="text" value="1194"/>
server	<input type="text" value="10.8.0.0 255.255.255.0"/>
keepalive	<input type="text" value="10 120"/>
ca	<input type="button" value="Browse..."/> No file selected.
dh	<input type="button" value="Browse..."/> No file selected.
cert	<input type="button" value="Browse..."/> No file selected.
key	<input type="button" value="Browse..."/> No file selected.
proto	<input type="text" value="udp"/>

3.5.8.5 GRE tunnel

GRE Tunnel

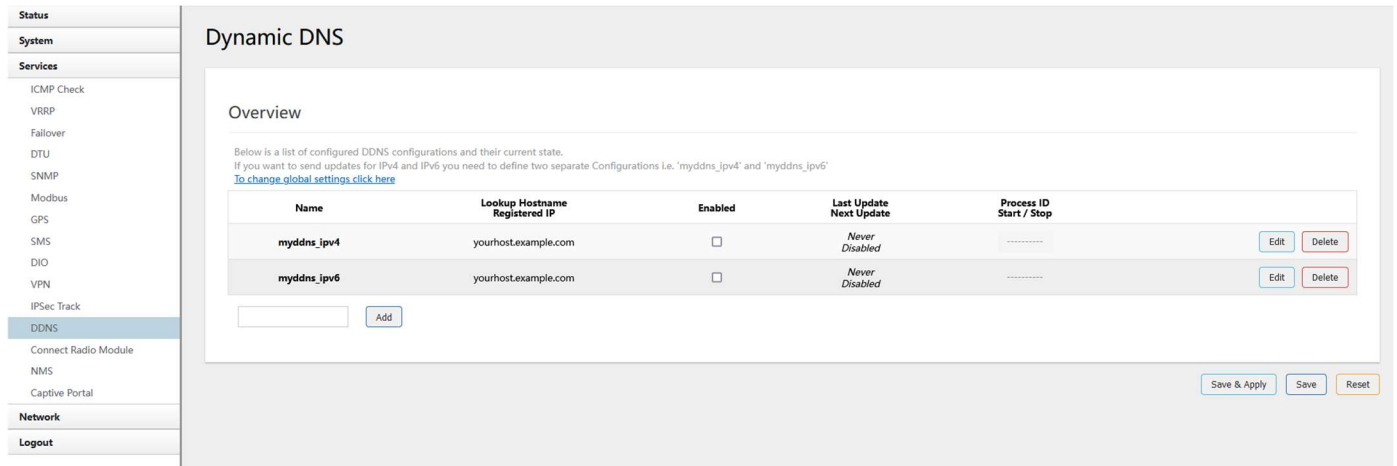
GRE Instance: Gre_tunnel

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 style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="All"/> ▾
Local Tunnel IP		<input type="text"/>
Local Tunnel Mask		<input type="text"/>
IPSec as backup		<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="None"/> ▾
Keepalive		<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="None"/> ▾

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

3.5.9 DDNS

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

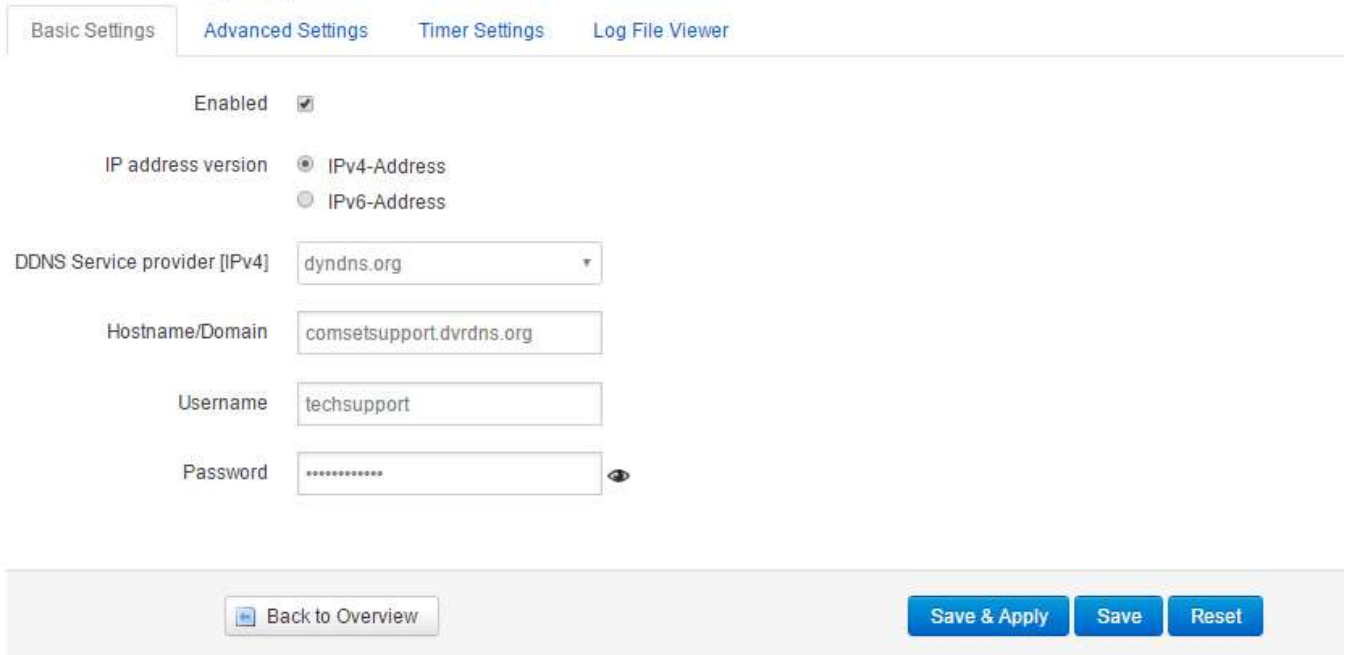


The screenshot shows the 'Dynamic DNS' configuration page. On the left is a navigation menu with categories: Status, System, Services, Network, and Logout. The 'Services' section is expanded, showing options like ICMP Check, VRRP, Failover, DTU, SNMP, Modbus, GPS, SMS, DIO, VPN, IPsec Track, and DDNS (which is selected). The main content area is titled 'Dynamic DNS' and contains an 'Overview' section. Below the overview, there is a table listing configured DDNS instances:

Name	Lookup Hostname Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
myddns_ipv4	yourhostexample.com	<input type="checkbox"/>	Never Disabled	-----	Edit Delete
myddns_ipv6	yourhostexample.com	<input type="checkbox"/>	Never Disabled	-----	Edit Delete

Below the table is an 'Add' button. At the bottom right of the page are 'Save & Apply', 'Save', and 'Reset' buttons.

Details for: example_ipv4



The screenshot shows the 'Details for: example_ipv4' configuration page. At the top, there are four tabs: 'Basic Settings' (selected), 'Advanced Settings', 'Timer Settings', and 'Log File Viewer'. The configuration options are as follows:

- Enabled:**
- IP address version:** IPv4-Address, IPv6-Address
- DDNS Service provider [IPv4]:** dyndns.org
- Hostname/Domain:** comsetsupport.dvrDNS.org
- Username:** techsupport
- Password:** [masked]

At the bottom of the page, there is a 'Back to Overview' button and 'Save & Apply', 'Save', and 'Reset' buttons.

- **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

Network [IPv4] ifmobile

DNS-Server mydns.lan

PROXY-Server user:password@myproxy.lan:8080

Log to syslog Notice

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

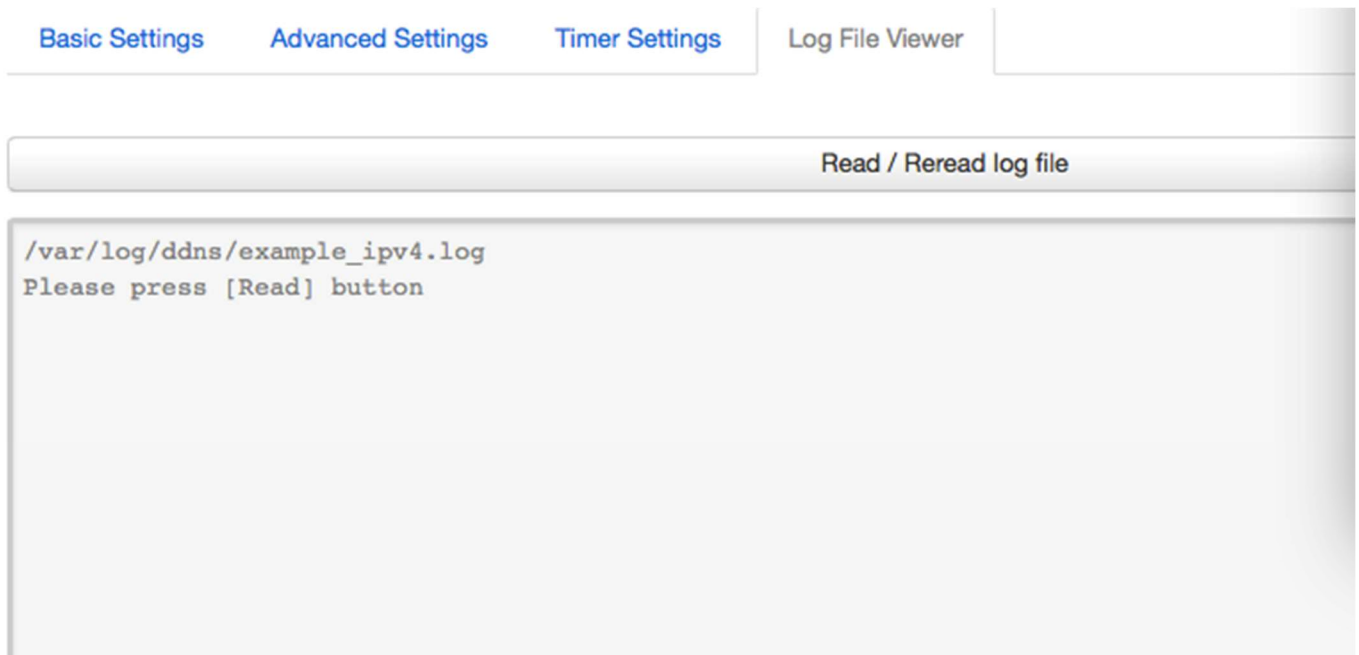
Check Interval 10 minutes

Force Interval 72 hours

Error Retry Counter 0

Error Retry Interval 60 seconds

- **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.



Read the log file of DDNS.

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:

Connect Radio Module Configuration

Exchange data between radio module and serial

Enable

Connect mode

Serial baudrate

Serial parity

Serial databits

Serial stopbits

• **Enable: conflict with DTU, please disable DTU firstly**

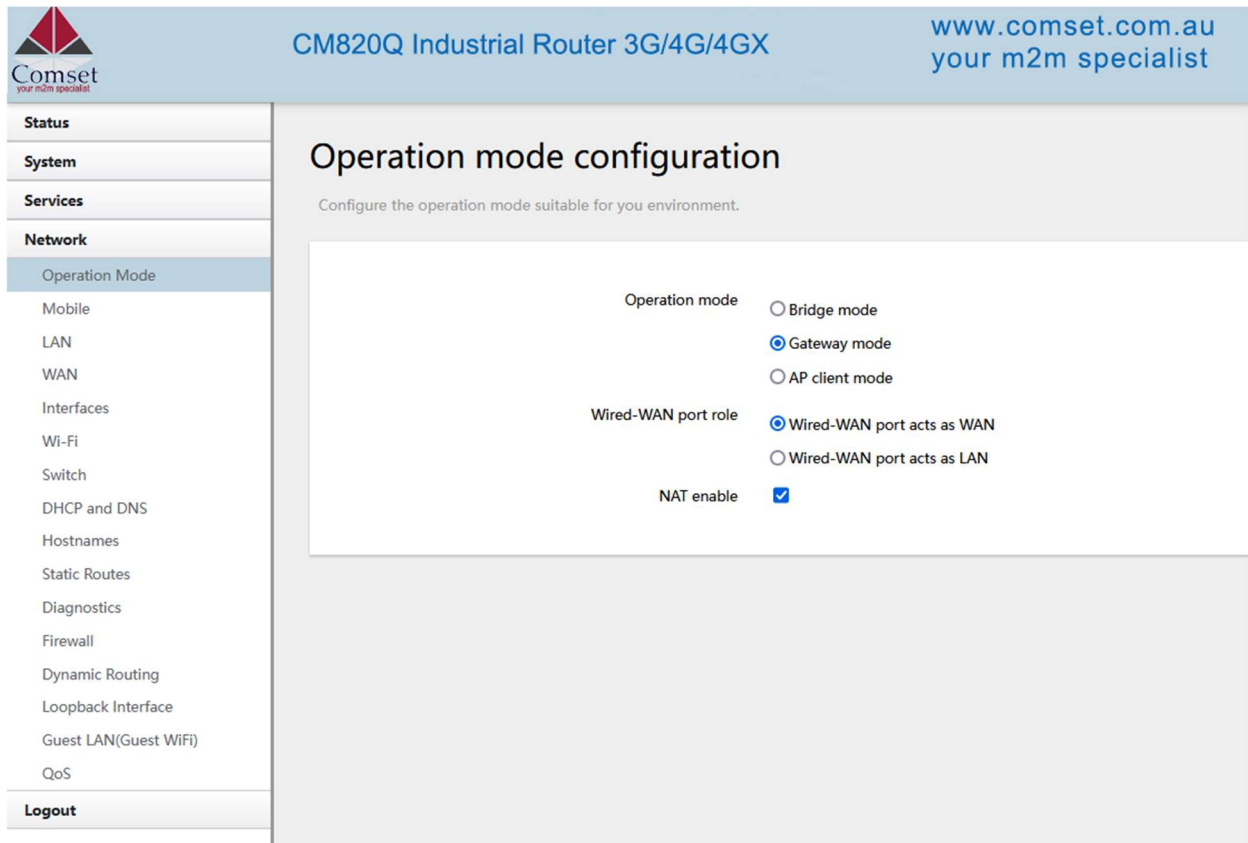
- **Connect Mode:** Serial only

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 CM820Q Industrial Router 3G/4G/4GX. The page title is "Operation mode configuration" and the subtitle is "Configure the operation mode suitable for you environment." The left sidebar contains a navigation menu with the following items: Status, System, Services, Network (highlighted), Mobile, LAN, WAN, Interfaces, Wi-Fi, Switch, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, Dynamic Routing, Loopback Interface, Guest LAN(Guest WiFi), QoS, and Logout. The main content area shows the following configuration options:

- Operation mode:
 - Bridge mode
 - Gateway mode
 - AP client mode
- Wired-WAN port role:
 - Wired-WAN port acts as WAN
 - Wired-WAN port acts as LAN
- NAT enable:

- **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**
 - Wired-WAN port acts as LAN**

The default operation is in "Gateway mode".

3.6.2 Mobile configuration

The router supports several cell modems. If you replace the original cell modem with a different one, the router will automatically detect the new modem.

Status	General	Data Limitation	Operator Selection 1
System	<h3>Mobile Configuration</h3> <p>SIM 1</p> <p>Enable <input checked="" type="checkbox"/></p> <p>Mobile connection <input type="text" value="DHCP mode"/></p> <p>IP Passthrough <input type="checkbox"/></p> <p>PIN code <input type="text"/></p> <p>Dialing number <input type="text" value="*99#"/></p> <p>APN <input type="text" value="telstra.internet"/></p> <p>Authentication method <input type="text" value="None"/></p> <p>Dual APN support <input type="checkbox"/></p> <p>Network type <input type="text" value="automatic"/></p> <p>MTU <input type="text" value="1500"/></p> <p>IPv4 netmask <input type="text"/></p> <p>Default route <input checked="" type="checkbox"/></p>		
Services			
Network			
Operation Mode			
Mobile			
LAN			
WAN			
Interfaces			
Wi-Fi			
Switch			
DHCP and DNS			
Hostnames			
Static Routes			
Diagnostics			
Firewall			
Dynamic Routing			
Loopback Interface			
Guest LAN(Guest WiFi)			
QoS			
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 number:** Most SIM cards don't have a PIN number; in which case you leave this field blank.

- **Dialing number:** Fill in the related value. 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. Normally select *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.

3.6.3 Cell mobile data limitation

Data Limitation Configuration


Enable data limitation


Period

Start day

SIM data limit(MB)

Enable alarm

Phone number 

Warning percent of Data Used(%) 

Used(Bytes)

Terminate 3G/4G connection until restart time

- **Enable data limitation:**
- **Period:** Month, Week or Day.
- **Start day:** The first day of the period.
- **SIM data limit (MB):** The maximum data that can be used during this period. If it is exceeded, the router will terminate the cell mobile connection.

- **Enable alarm:** Enable 'data limitation' alarm.
- **Phone number:** The phone number that receives the data limitation alarm SMS.
- **Warning percent of data used:** If the used data reaches this level, a data limitation alarm SMS will be sent.
- **Used (MB):** The data that has been consumed so far during this period.

3.6.4 LAN settings

- **Protocol:** Only static address is supported for LAN.
- **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 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.

General Settings	Advanced Settings	Physical Settings	Firewall Settings	DHCP Server
		Override MAC address	<input type="text" value="90:26:08:81:89:1B"/>	
		Override MTU	<input type="text" value="1500"/>	
		Use gateway metric	<input type="text" value="0"/>	

- **Override MAC address:** Overrides LAN MAC address.
- **Override MTU:** Maximum Transmission Unit.
- **Use gateway metric:** The LAN subnet's metric to gateway.

General Settings	Advanced Settings	Physical Settings	Firewall Settings	DHCP Server
		Bridge interfaces	<input checked="" type="checkbox"/>	
		Enable STP	<input type="checkbox"/>	
		Enable IGMP snooping	<input type="checkbox"/>	
		Interface	<input type="text" value="eth0.1"/> <input type="text" value="wlan0"/>	

- **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.

General Settings	Advanced Settings	Physical Settings	Firewall Settings	DHCP Server
		Ignore interface	<input type="checkbox"/>	
		Start	<input type="text" value="100"/>	
		Limit	<input type="text" value="150"/>	
		Lease time	<input type="text" value="12h"/>	

- **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).

General Setup	Advanced Settings	IPv6 Settings
		Dynamic DHCP <input checked="" type="checkbox"/>
		Force <input type="checkbox"/>
		IPv4-Netmask <input type="text" value="255.255.255.0"/>
		DHCP-Options <input type="text"/> <input style="float: right;" type="button" value="+"/>

- **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, '192.168.2.1 and 192.168.2.2' which advertises different DNS servers to clients.)

General Setup	Advanced Settings	IPv6 Settings
		Router Advertisement-Service <input type="text" value="server mode"/> <input type="button" value="v"/>
		DHCPv6-Service <input type="text" value="server mode"/> <input type="button" value="v"/>
		NDP-Proxy <input type="text" value="disabled"/> <input type="button" value="v"/>
		DHCPv6-Mode <input type="text" value="stateless + stateful"/> <input type="button" value="v"/>
		Always announce default router <input type="checkbox"/>
		Announced DNS servers <input type="text"/> <input style="float: right;" type="button" value="+"/>
		Announced DNS domains <input type="text"/> <input style="float: right;" type="button" value="+"/>

- **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 WAN

- **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.

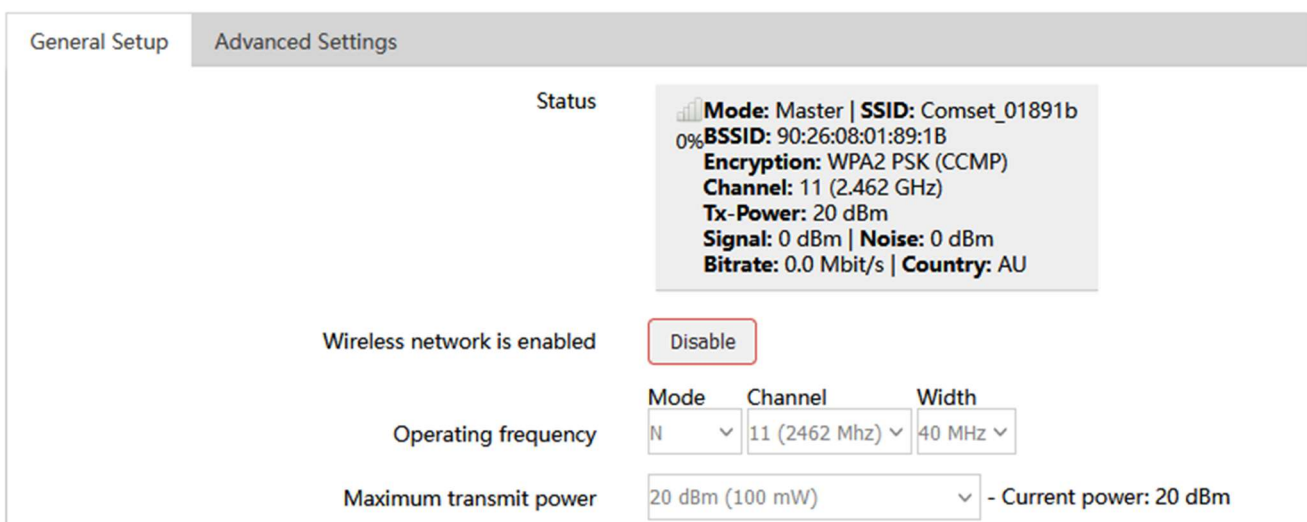
3.6.6 WiFi Settings



- **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 of 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

Wireless Network: Master "Comset_01891b" (wlan0)



- **Status:** Shows the WiFi signal strength, mode, SSID.
- **Operating frequency Mode:** Supports 802.11b/g/n. the Legacy means 802.11b/g. "N" means 802.11n.

- **Channel:** Channel 1-11.
- **Width:** 20MHz and 40MHz.
- **Transmit Power:** From 0dBm to 20dBm.

3.6.6.2 WiFi Advanced Configuration

General Setup	Advanced Settings
Country Code	AU - Australia
Allow legacy 802.11b rates	<input checked="" type="checkbox"/>
Distance Optimization	auto
Fragmentation Threshold	off
RTS/CTS Threshold	off
Force 40MHz mode	<input checked="" type="checkbox"/>
Beacon Interval	100

- **Country Code:** Use ISO/IEC 3166 alpha2 country codes.
- **Distance Optimization:** Distance to furthest network member in meters.
- **Fragmentation Threshold**
- **RTS/CTS Threshold**

3.6.6.3 WiFi Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Mode	Access Point		
ESSID	Comset_01891b		
Network	lan		
Hide ESSID	<input type="checkbox"/>		
WMM Mode	<input checked="" type="checkbox"/>		

- **Mode:** Supported options.
- **ESSID:** Extended Service Set Identifier. It is the broadcast name.
- **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:** 'Hide SSID' means this WiFi cannot be scanned by others.
- **WMM Mode**

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

Encryption: WPA2-PSK (strong security) [v]

Cipher: auto [v]

Key: [.....] *

802.11r Fast Transition:

802.11w Management Frame Protection: Disabled [v]

Enable key reinstallation (KRACK) countermeasures:

● **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: Allow list [v]

MAC-List:

- 00:1E:10:1F:00:00 (10.223.164) [v] [x]
- 68:A8:6D:48:77:5E (dentydeME) [v] [x]
- 90:22:06:80:02:01 (Cell_Router) [v] [+

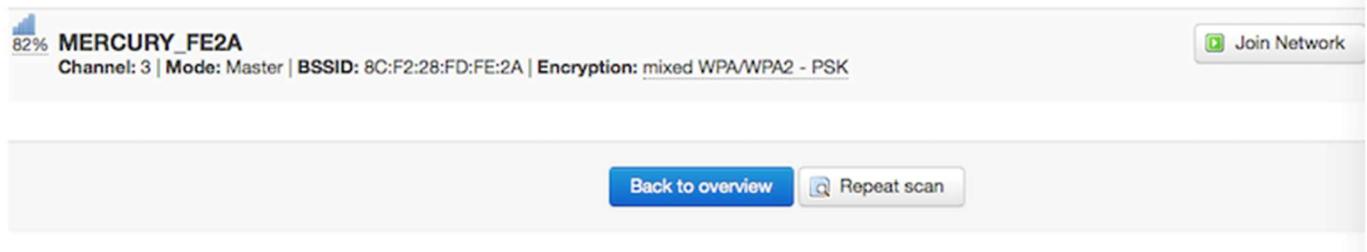
- **MAC-Address Filter:** MAC Address Access Policy. Disabled: disable MAC-address filter functionality. Allow list: only the MAC address in the list is allowed to forward. Deny list: all packet is allowed to forward except MAC address in the list.
- **MAC-List:** Click button [x] to delete a MAC address from list, click button [+] to add a new

MAC address to the list.

3.6.6.4 WiFi AP client

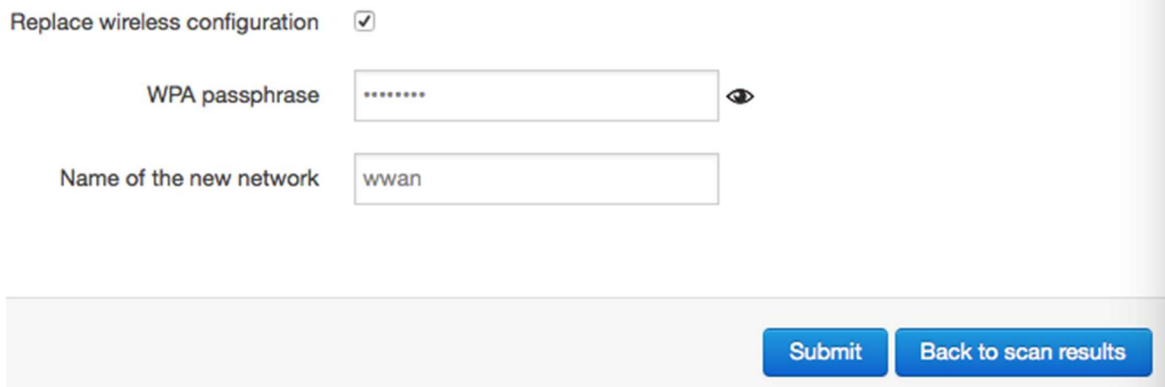
- **Steps 1)** Click the button “AP Client” on the wireless overview page, then the system will start to scan all WiFi signals.

Join Network: Wireless Scan



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

Join Network: Settings



- **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. Don’t 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

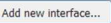
3.6.7 Interfaces Overview



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

Interfaces Global network options

Interfaces

IFMOBILE  usb0	Protocol: DHCP client Uptime: 3h 20m 59s MAC: 02:50:F4:00:00:00 RX: 77.40 MB (125505 Pkts.) TX: 29.25 MB (98716 Pkts.) IPv4: 10.143.28.170/30 Information: Not started on boot	 Restart  Stop  Edit  Delete
LAN  br-lan	Protocol: Static address Uptime: 3h 21m 48s MAC: 90:26:08:81:89:1B RX: 31.71 MB (118641 Pkts.) TX: 86.64 MB (135839 Pkts.) IPv4: 192.168.1.1/24 IPv6: fd07:f9d2:6beac:1/60	 Restart  Stop  Edit  Delete
LOOPBACK  lo	Protocol: Static address Uptime: 3h 21m 48s RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) IPv4: 127.0.0.1/8	 Restart  Stop  Edit  Delete
WAN  eth0.2	Protocol: DHCP client MAC: 90:26:08:81:89:1C RX: 0 B (0 Pkts.) TX: 26.65 KB (142 Pkts.)	 Restart  Stop  Edit  Delete
WAN6  eth0.2	Protocol: DHCPv6 client MAC: 90:26:08:81:89:1C RX: 0 B (0 Pkts.) TX: 26.65 KB (142 Pkts.)	 Restart  Stop  Edit  Delete

 Add new interface...

 Save & Apply
  Save
  Reset

3.6.8 Firewall

3.6.8.1 General Settings

General Settings | Port Forwards | Traffic Rules | NAT Rules | DMZ | Security | Custom Rules

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

Enable firewall	<input checked="" type="checkbox"/>
Enable SYN-flood protection	<input checked="" type="checkbox"/>
Drop invalid packets	<input type="checkbox"/>
Input	<input type="text" value="accept"/>
Output	<input type="text" value="accept"/>
Forward	<input type="text" value="reject"/>

3.6.8.2 Port Forwards

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

Firewall - Port Forwards - Unnamed forward

General Settings	Advanced Settings
Name	Unnamed forward
Protocol	TCP UDP
Source zone	wan wan: wan6: ifmobile:
External port	
Destination zone	lan lan: lan6:
Internal IP address	any
Internal port	any

- **Name:** Port Forward instance name.
- **Protocol:** TCP+UDP, UDP and TCP can be chosen.
- **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** NAT Rules DMZ Security Custom Rules

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	
L2TP SERVER	Incoming IPv4 and IPv6, protocol UDP From wan To this device , port 1701	Accept input	<input type="checkbox"/>	⋮ Edit Delete
DTU2 server	Incoming IPv4 and IPv6, protocol TCP, UDP From wan To this device , port 5001	Accept input	<input type="checkbox"/>	⋮ Edit Delete
DTU2 center1	Incoming IPv4 and IPv6, protocol TCP From wan , IP 192.168.1.171, port 5001 To this device	Accept input	<input type="checkbox"/>	⋮ Edit Delete
Allow-All-LAN-Ports	Forwarded IPv4 and IPv6 From wan To lan , port 1-65535	Accept forward	<input type="checkbox"/>	⋮ Edit Delete
Allow-DHCP-Renew	Incoming IPv4, protocol UDP From wan To this device , port 68	Accept input	<input checked="" type="checkbox"/>	⋮ Edit Delete
Allow-Ping-WAN	Incoming IPv4, protocol ICMP From wan To this device	Accept input	<input checked="" type="checkbox"/>	⋮ Edit Delete

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

Open ports on router:

Name	Protocol	External port	
<input type="text" value="New input rule"/>	TCP+UDP	<input type="text"/>	 Add

New forward rule:

Name	Source zone	Destination zone	
<input type="text" value="New forward rule"/>	lan	wan	 Add and edit...

Source NAT list and create source NAT rule:

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
<i>This section contains no values yet</i>				
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 cho"/>	<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 NAT Rules **DMZ** Security Custom Rules

DMZ Configuration

Setup a Demilitarized Zone(DMZ) to separate internal network and Internet.

Enable

IP address

Protocol

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

General Settings Port Forwards Traffic Rules NAT Rules DMZ **Security** Custom Rules

System Security Configuration

SSH port

SSH access from WAN

Ping from WAN to LAN

Enable telnet

HTTPS Access

HTTPS port

HTTPS access from WAN

HTTP Access

HTTP port

HTTP access from WAN

RFC1918 filter

Enable lock account

Access Whitelist

Allow the whitelist to access device, others will be blocked

Enable

- **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.
- **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 in a remote IP address that can access the router's web management page.
- **Netmask:** 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the value is from 1 to 32.

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	
lan	<input type="text"/>	<input type="text" value="255.255.255.255"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="1500"/>	<input type="button" value="Delete"/>

Static IPv6 Routes

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

This section contains no values yet

- **Interface:** You can choose the corresponding interface type.
- **Target:** The destination host IP or network.
- **Gateway:** IP address of the next router.

Notice:

- 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

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.

Enable VLAN functionality

VLANs on "switch0" (rt305x-esw)

VLAN ID	CPU (eth0)	LAN 1	LAN 2	LAN 3	LAN 4	WAN
Port status:	 1000baseT full-duplex	 1000baseT full-duplex	 no link	 no link	 no link	 no link
1	tagged	untagged	untagged	untagged	untagged	off
2	tagged	off	off	off	off	untagged

Add VLAN

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

Status

System

Services

Network

- Operation Mode
- Mobile
- LAN
- WAN
- Interfaces
- Wi-Fi
- Switch
- DHCP and DNS
- Hostnames
- Static Routes
- Diagnostics
- Firewall
- Dynamic Routing
- Loopback Interface
- Guest LAN(Guest WiFi)
- QoS

Logout

DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

General Settings

Resolv and Hosts Files

TFTP Settings

Advanced Settings

Static Leases

Domain required	<input checked="" type="checkbox"/>
Authoritative	<input checked="" type="checkbox"/>
Local server	<input type="text" value="/lan/"/>
Local domain	<input type="text" value="lan"/>
Log queries	<input type="checkbox"/>
DNS forwardings	<input type="text" value="/example.org/10.1.2.3"/> +
Rebind protection	<input checked="" type="checkbox"/>
Allow localhost	<input checked="" type="checkbox"/>
Domain whitelist	<input type="text" value="host.netflix.com"/> +
Local Service Only	<input checked="" type="checkbox"/>
Non-wildcard	<input checked="" type="checkbox"/>
Listen Interfaces	<input type="text"/> +
Exclude interfaces	<input type="text"/> +

- **Domain required:** Don't 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.

www.comset.com.au

85

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings	Static Leases
			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"/>
			Additional servers file	<input type="text"/>
			Strict order	<input type="checkbox"/>
			All Servers	<input type="checkbox"/>
			Bogus NX Domain Override	<input type="text" value="67.215.65.132"/> <input style="border: 1px solid #ccc; padding: 2px 5px;" type="button" value="+"/>
			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"/>
			Size of DNS query cache	<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





<input type="text" value="www.google.com"/>	<input type="text" value="www.google.com"/>	<input type="text" value="www.google.com"/>
IPv4  		

- **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 below.

Diagnostics

Network Utilities

<input type="text" value="www.google.com"/>	<input type="text" value="www.google.com"/>	<input type="text" value="www.google.com"/>
IPv4  		

```

PING www.google.com (93.46.8.89): 56 data bytes

--- www.google.com ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
  
```

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:

Dynamic Routing

Zebra

Enable

Password *

OSPF

Enable

Password *

OSPF6

Enable

Password *

RIP

Enable

Password

RIPng

Enable

Password

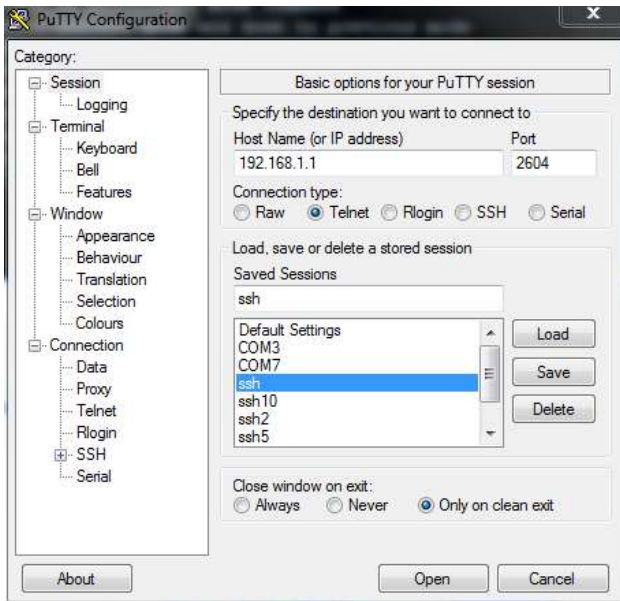
BGP

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 the 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.