Industrial 5G Router CM685VX

User Manual

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

Table of Contents

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

Address : 37/ 125 Highbury Road, Burwood VIC 3125, Australia

Web : http://www.comset.com.au

Phone: +61 3 9001 9720

Fax: +61 3 9888 7100

Chapter 1

1 Product Introduction

1.1 Product Overview

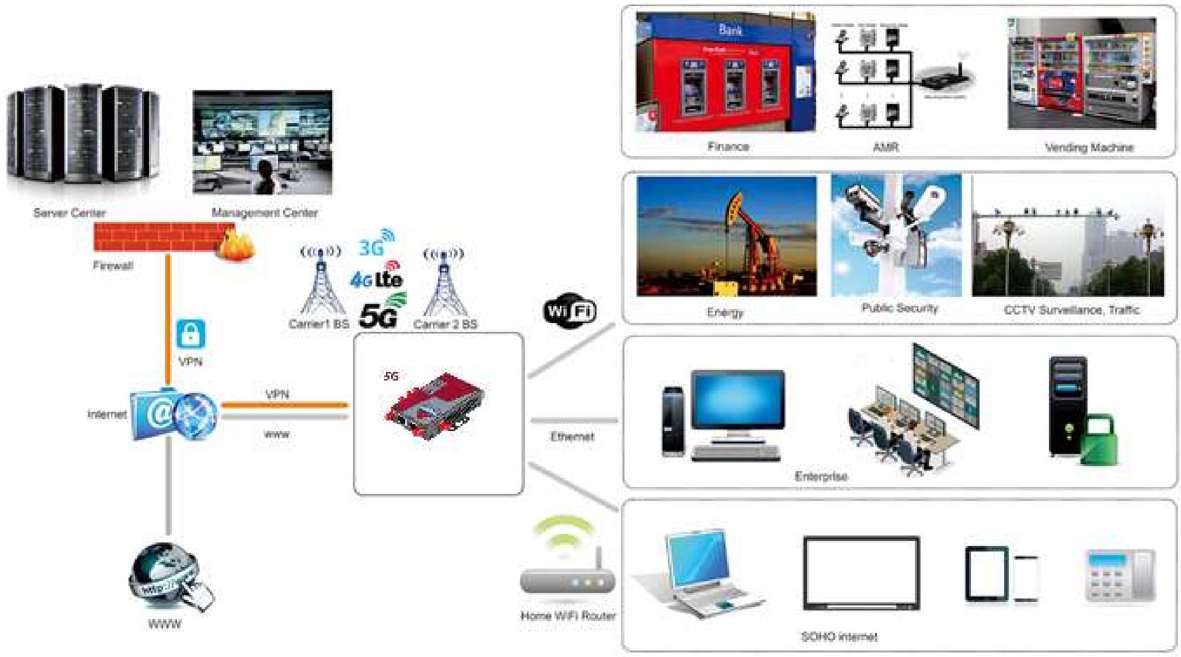
The Comset CM685VX is a New Generation 5G Industrial Router. Supporting both 5G SA and 5G NSA modes, the CM685VX delivers lightning internet speeds of up to 2.5Gbps over the 5G networks with failover to 4G LTE-A Cat 16 with speeds of up to 1.0Gbps. Powered by Qualcomm Snapdragon X55 chipset and built on the fully featured OpenWrt Linux operating system, the CM685VX provides a powerful and rapidly deployable internet solution to commercial customers and small to medium businesses.

The Comset CM685VX is an Innovative Router powered by a powerful 580MHz CPU. It features one Gigabit LAN port for fast wired connections, 1 Gigabit WAN/LAN port for automatic failover between NBN/ADSL and mobile 4G or 5G, as well as a GPIO with four digital input/output ports. Other features include VPN IPSEC, PPTP (Server and Client), L2TP and OpenVPN to establish a secure connection over the 4G/5G network.

The Comset CM685VX is a Global Router, supporting frequencies across all major carriers worldwide. The innovative design, easy integration and rich built-in features make the CM685VX the router of choice for a wide range of business and commercial applications, including SOHO, SMB, industrial automation, building automation, security, surveillance, transportation, health, mining and environmental monitoring.

1.2 Typical Application Diagram

The Comset CM685VX 3G/4G/5G Router is suitable for a wide range of business, commercial and machine-to-machine applications (M2M). A good example is the connection of various IOT and M2M devices back to a server over a secure 5G connection using a secure VPN IPSEC tunnel, as illustrated below.



1.3 Features

The CM685VX supports the following:

- Worldwide 5G and LTE-A coverage
- Both SA and NSA modes
- 1 x Gigabit Ethernet LAN port
- 1 x Gigabit Ethernet WAN/LAN port
- WiFi N300 (802.11 a/b/g/n 2.4Ghz)
- 6 x SMA standard detachable antennas included: 4 x cellular antennas and 2 x WiFi antennas
- Optimised EMC design
- Web management, SMS control, SSH/Telnet/Command, SNMP
- Always on-line: On-line detection and automatic redial
- Built-in transient and reverse polarity voltage protection, over-current and over-voltage protection
- Wide range power input (5-40VDC)
- Smart power management

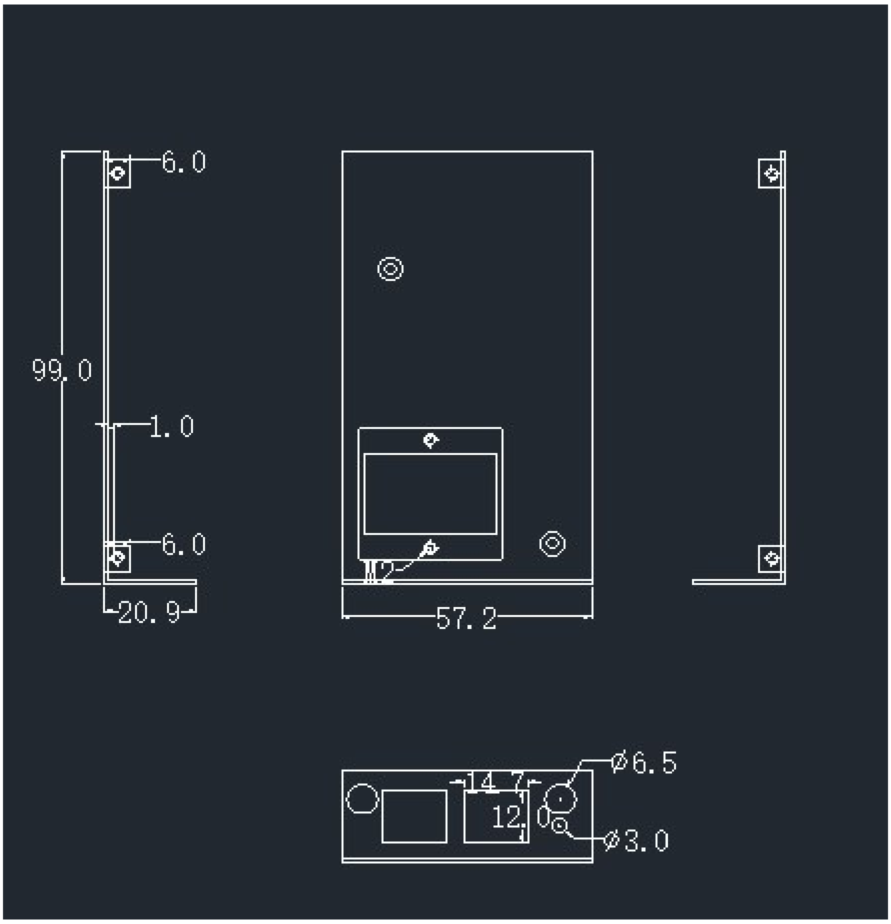
- Serial RS232 port
- 4 x Digital Input ports, that can also be used as Digital Output ports
- User friendly set-up wizard for easy configuration and setup
- Network traffic real-time graphs
- Network Diagnostic Tools (Ping, Traceroute and NSLookup)
- Advanced security, VPN, and stateful firewall to protect sensitive data
- Load balancing
- Robust Metal Case
- Desktop and Wall mount

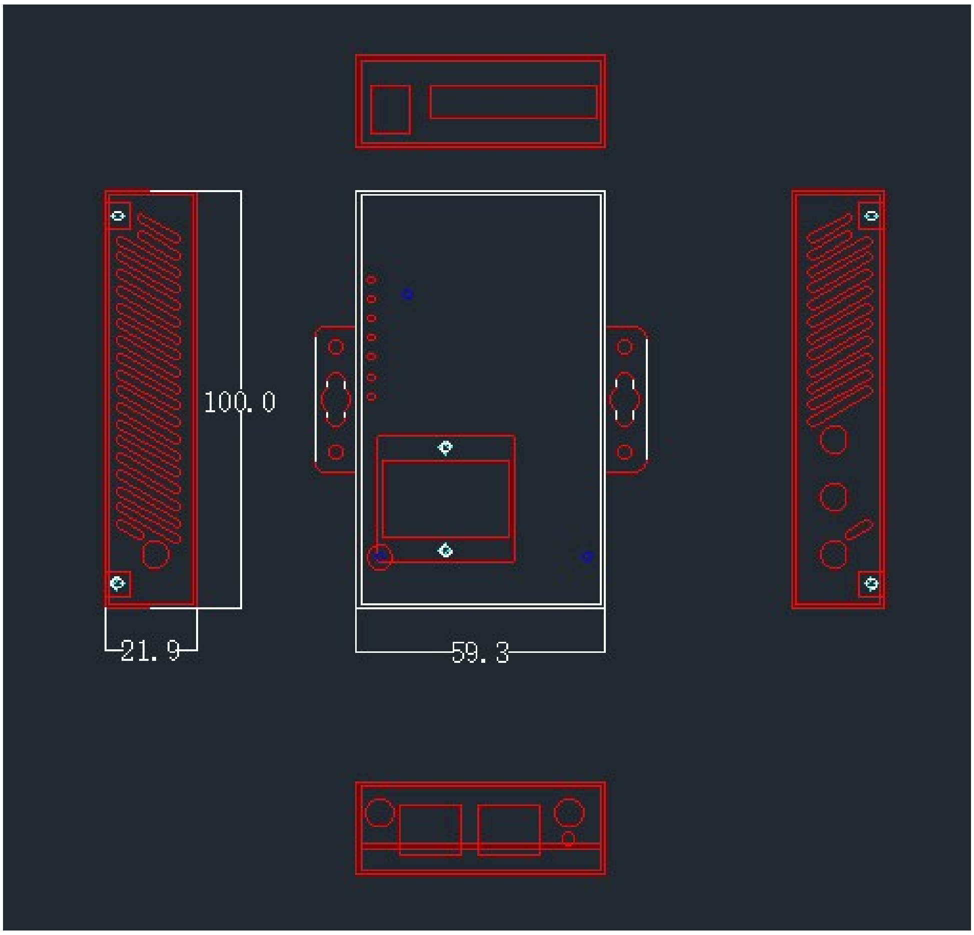
Chapter 2

2 Hardware Installation

1. *Overall Dimensions*
2. *Accessories*
3. *Installation*

2.1 Overall Dimensions





2.2 Ports

LAN: LAN RJ45 Gigabit Ethernet port
WAN: WAN/LAN RJ45 Gigabit Ethernet port
RST: SYS reset button
PWR: DC power socket. DC5~40V standard. (DC5~50V optional)
VCC: DC wire positive pole
GND: DC wire ground
GND: Serial ground
RX: Serial receive
TX: Serial transmit
RST: Reset
DIO0: Digital I/O port 0
DIO1: Digital I/O port 1
DIO2: Digital I/O port 2
DIO3: Digital I/O port 3

Antenna Connection Table

Antenna Connectors	Remarks
Cell1	for cell antenna 1
Cell 2	for cell antenna 2
Cell 3	for cell antenna 3
Cell 4/GPS	for cell antenna 4, or GPS antenna
WiFi1	for WiFi antenna 1
WiFi2	for WiFi antenna 2

2.3 Powering up the CM685VX

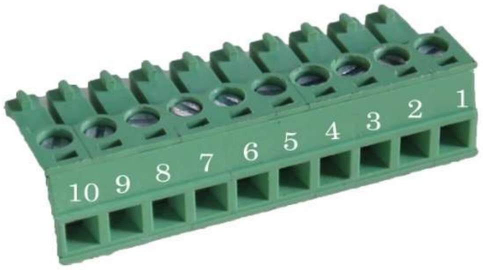
Please ensure the SIM card is inserted, and the antennas are connected before powering up the router.

2.4 SIM/UIM cards

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 "VCC" (DC5~40V).*

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

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

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

2.6 Grounding

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

2.7 Power Supply

The CM685VX supports a wide range of DC voltage between 5 VDC and 40 VDC. The router is supplied with a 12 VDC power adapter.

2.8 LED Description

Please refer to the following table for LED description.

LED	Indication Light	Description
SYS	On for 25 seconds	On for 25 seconds after power up
	Blinks	System normal operation
	Off or still on after 25 seconds	System failure
LAN	Blinks	Ethernet data transmission
	Off	No Ethernet connection
	On	Ethernet is connected
VPN	On	IPSec VPN tunnel set-up
	Off	IPsec VPN tunnel not set-up or Down/Inactive
Cell	Solid orange light	Cell connection is Up and now you have access to the Internet
	Flashing orange light	Attempting to establish an internet connection
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 into the router*
3. *How to configure the router*

3.1 Overview

The CM685VX router has a built-in WEB interface. Below are instructions on how to access the web interface and configure the router.

3.2 How to log into the Router

3.2.1 Network Configuration

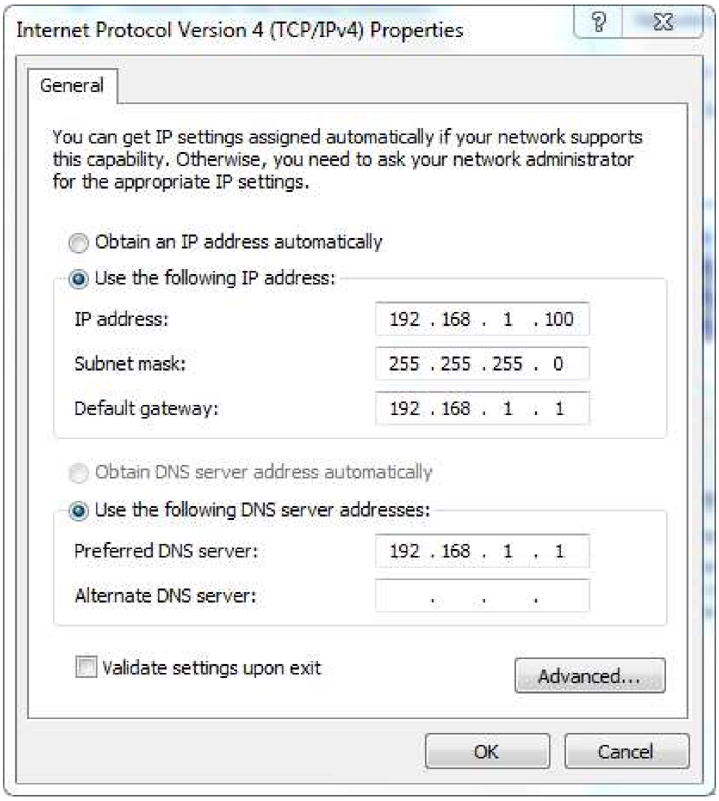
The router's default parameters are:

Default IP:	192.168.1.1
Subnet mask:	255.255.255.0

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

1) Manual settings

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

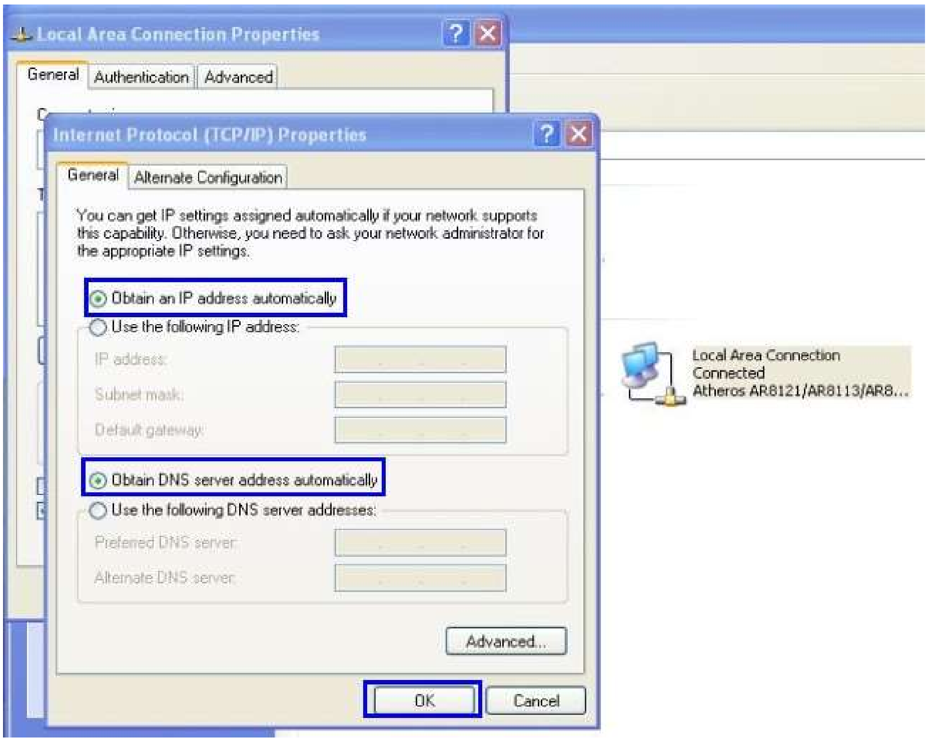
Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

2) DHCP settings

Choose "Obtain an IP address automatically" and "Obtain DNS server address automatically". Then click the 'OK' button.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

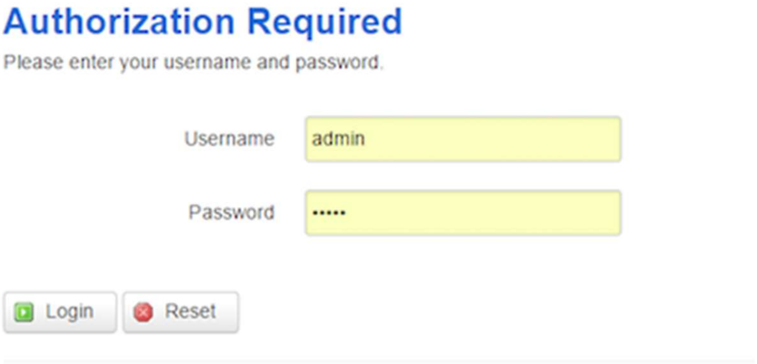
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

3.2.2 Log into the router

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



Authorization Required

Please enter your username and password.

Username: admin

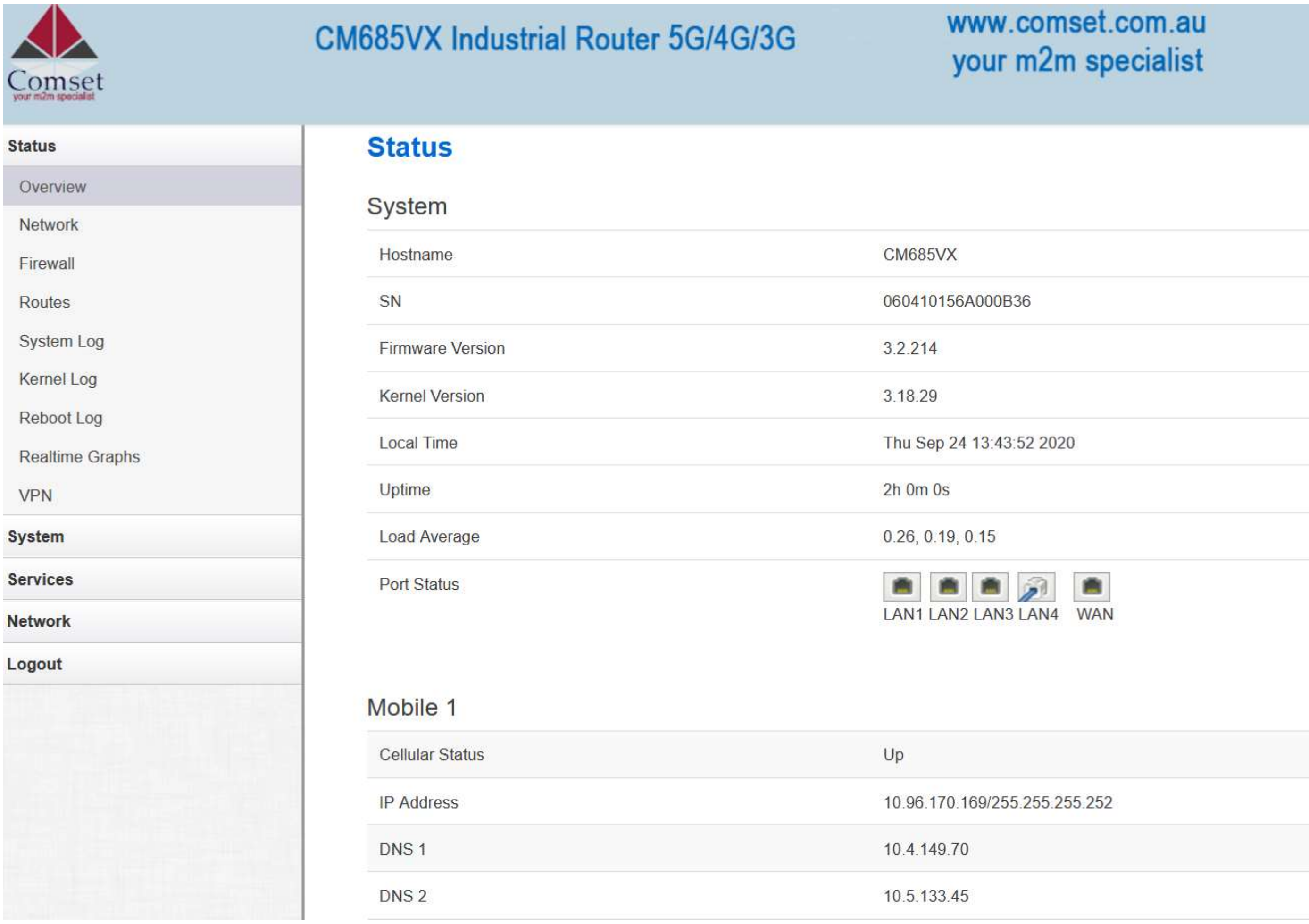
Password: •••••

<u>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</u>

3.3 Router status

3.3.1 Status overview

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



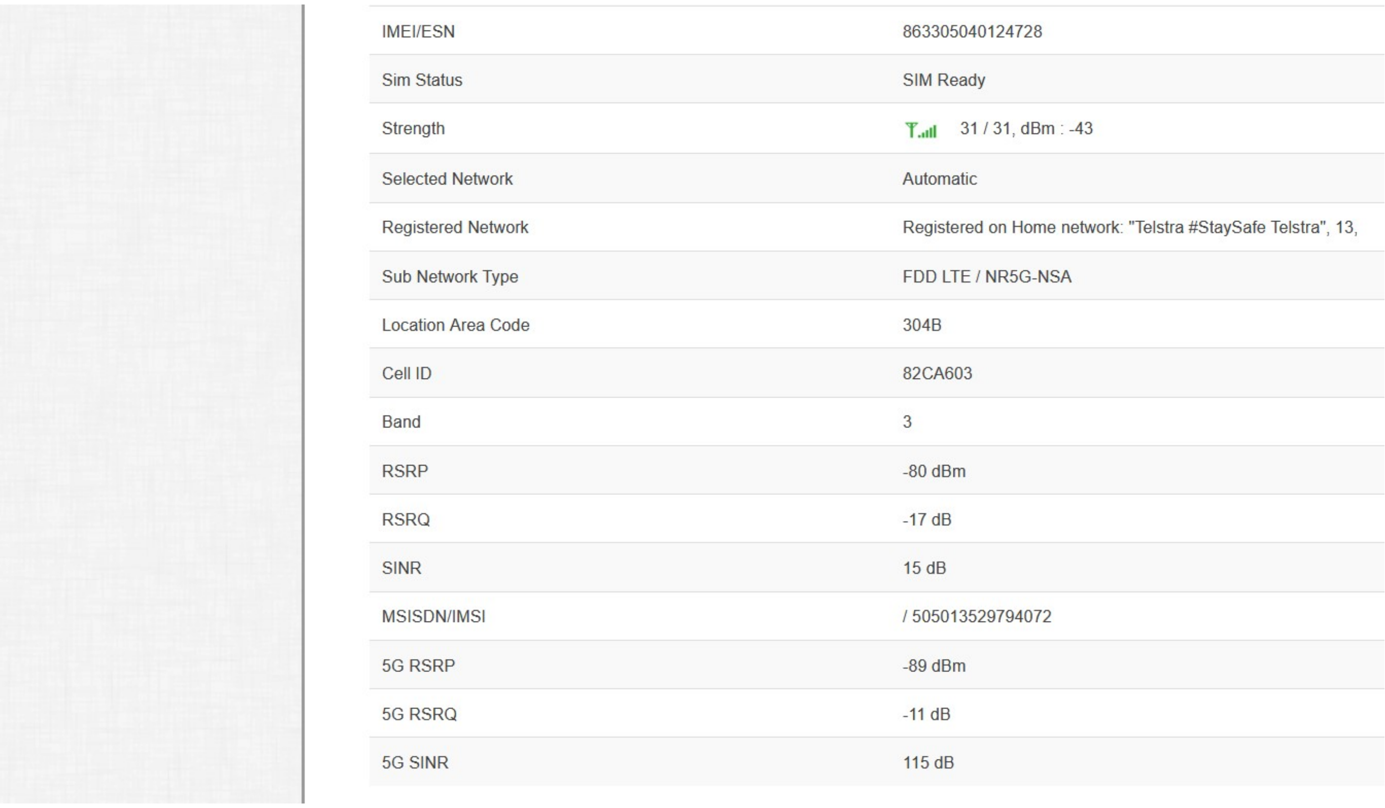
Status

System

Hostname	CM685VX
SN	060410156A000B36
Firmware Version	3.2.214
Kernel Version	3.18.29
Local Time	Thu Sep 24 13:43:52 2020
Uptime	2h 0m 0s
Load Average	0.26, 0.19, 0.15
Port Status	LAN1 LAN2 LAN3 LAN4 WAN

Mobile 1

Cellular Status	Up
IP Address	10.96.170.169/255.255.255.252
DNS 1	10.4.149.70
DNS 2	10.5.133.45

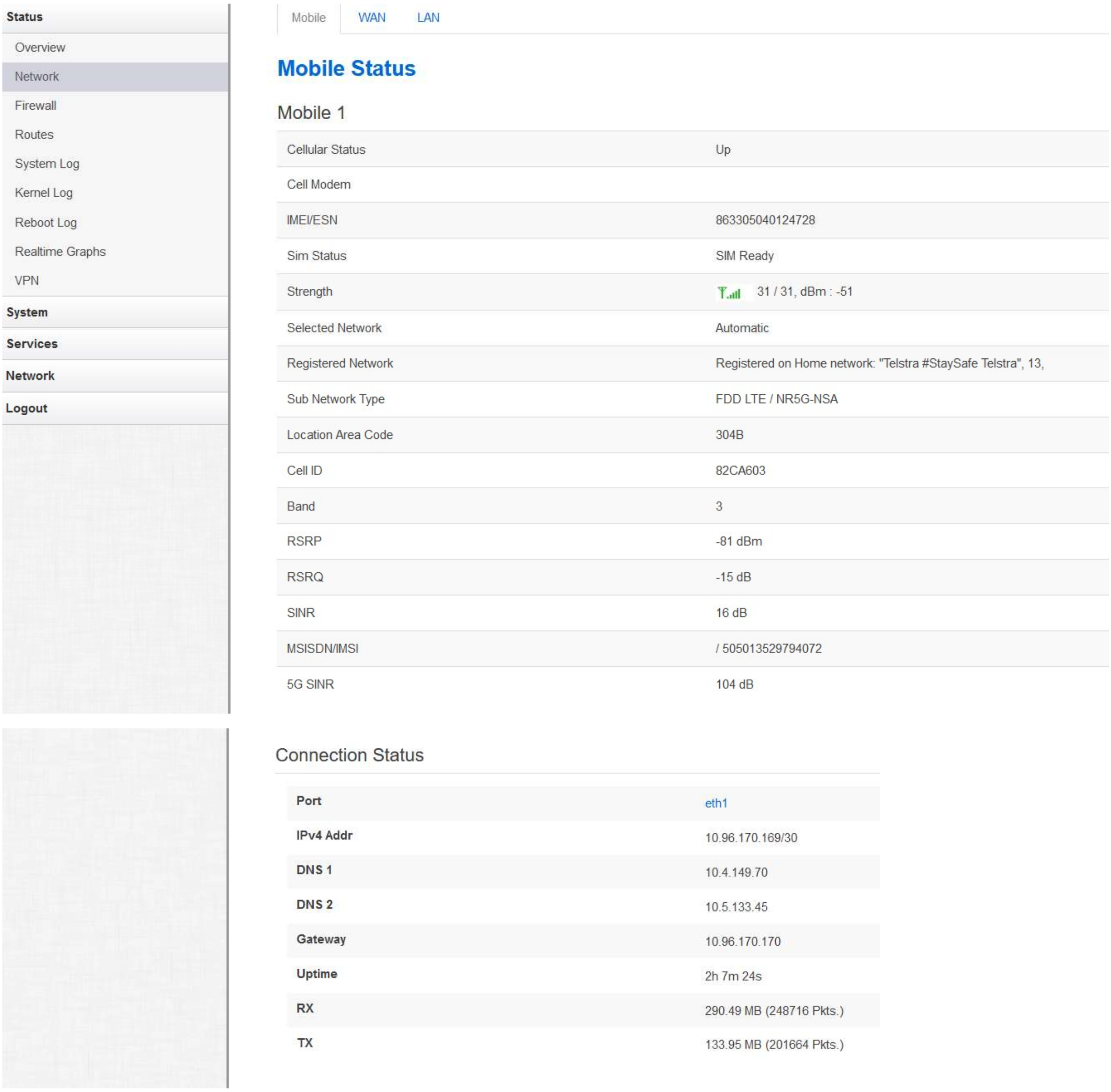


IMEI/ESN	863305040124728
Sim Status	SIM Ready
Strength	📶 31 / 31, dBm : -43
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra #StaySafe Telstra", 13,
Sub Network Type	FDD LTE / NR5G-NSA
Location Area Code	304B
Cell ID	82CA603
Band	3
RSRP	-80 dBm
RSRQ	-17 dB
SINR	15 dB
MSISDN/IMSI	/ 505013529794072
5G RSRP	-89 dBm
5G RSRQ	-11 dB
5G SINR	115 dB

3.3.2 Network status

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

Mobile interface page:



Mobile Status

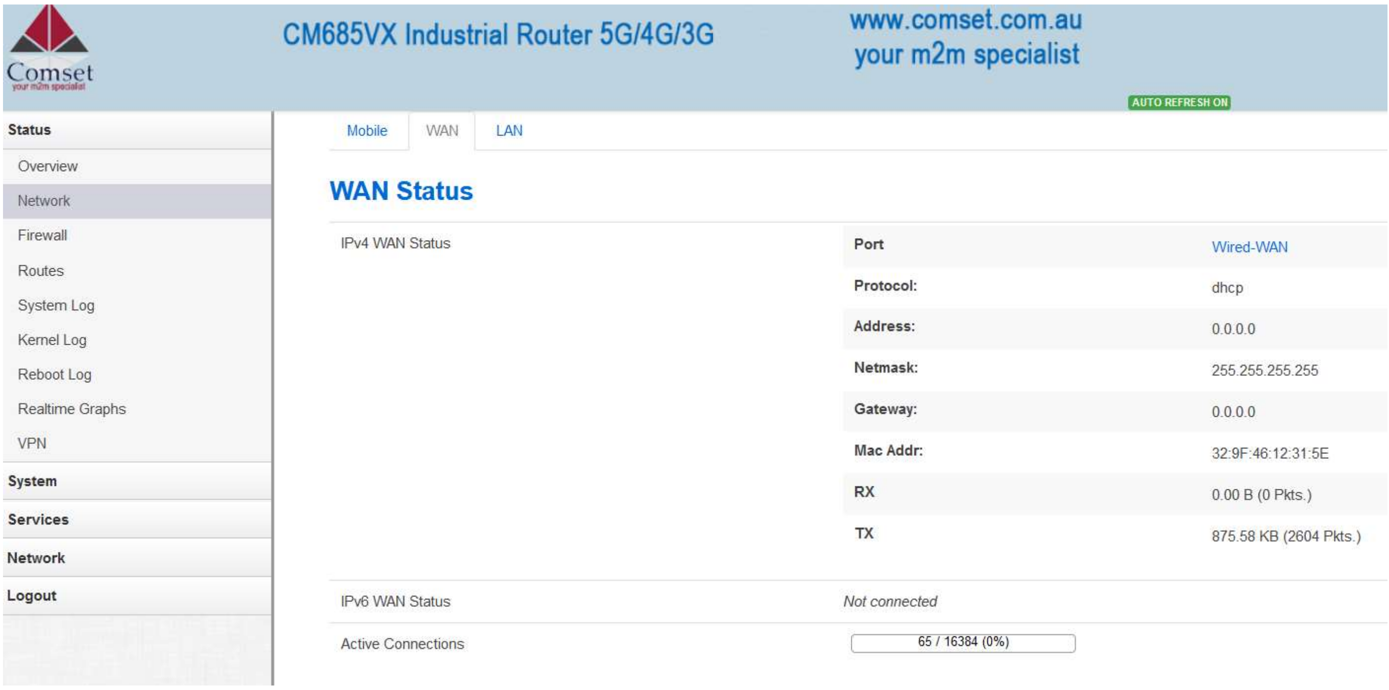
Mobile 1

Cellular Status	Up
Cell Modem	
IMEI/ESN	863305040124728
Sim Status	SIM Ready
Strength	31 / 31, dBm : -51
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra #StaySafe Telstra", 13,
Sub Network Type	FDD LTE / NR5G-NSA
Location Area Code	304B
Cell ID	82CA603
Band	3
RSRP	-81 dBm
RSRQ	-15 dB
SINR	16 dB
MSISDN/IMSI	/ 505013529794072
5G SINR	104 dB

Connection Status

Port	eth1
IPv4 Addr	10.96.170.169/30
DNS 1	10.4.149.70
DNS 2	10.5.133.45
Gateway	10.96.170.170
Uptime	2h 7m 24s
RX	290.49 MB (248716 Pkts.)
TX	133.95 MB (201664 Pkts.)

WAN status page:



WAN Status

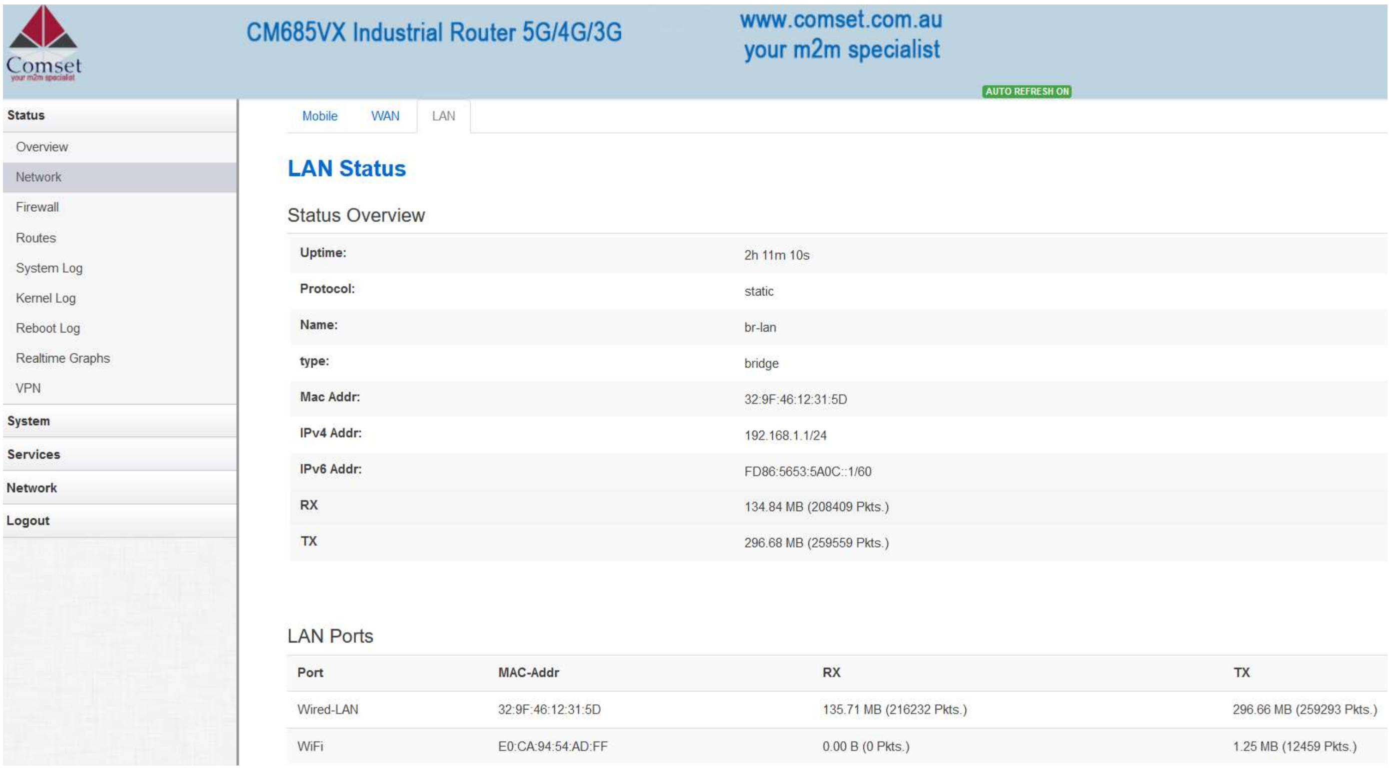
IPv4 WAN Status

Port	Wired-WAN
Protocol:	dhcp
Address:	0.0.0.0
Netmask:	255.255.255.255
Gateway:	0.0.0.0
Mac Addr:	32:9F:46:12:31:5E
RX	0.00 B (0 Pkts.)
TX	875.58 KB (2604 Pkts.)

IPv6 WAN Status *Not connected*

Active Connections 65 / 16384 (0%)

LAN status page:



LAN Status

Status Overview

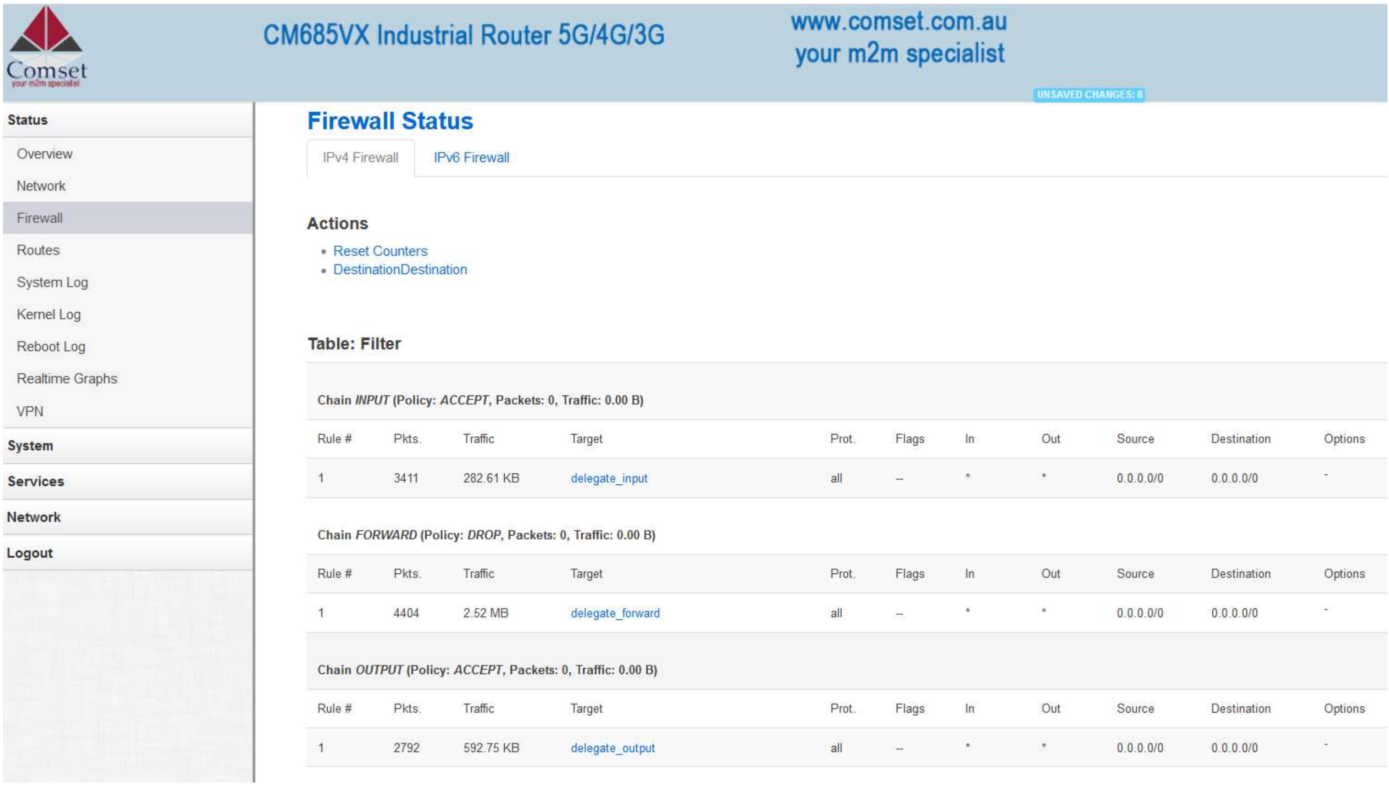
Uptime:	2h 11m 10s
Protocol:	static
Name:	br-lan
type:	bridge
Mac Addr:	32:9F:46:12:31:5D
IPv4 Addr:	192.168.1.1/24
IPv6 Addr:	FD86:5653:5A0C::1/60
RX	134.84 MB (208409 Pkts.)
TX	296.68 MB (259559 Pkts.)

LAN Ports

Port	MAC-Addr	RX	TX
Wired-LAN	32:9F:46:12:31:5D	135.71 MB (216232 Pkts.)	296.66 MB (259293 Pkts.)
WiFi	E0:CA:94:54:AD:FF	0.00 B (0 Pkts.)	1.25 MB (12459 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.



Firewall Status

Actions

- Reset Counters
- DestinationDestination

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	3411	282.61 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *FORWARD* (Policy: *DROP*, Packets: 0, Traffic: 0.00 B)

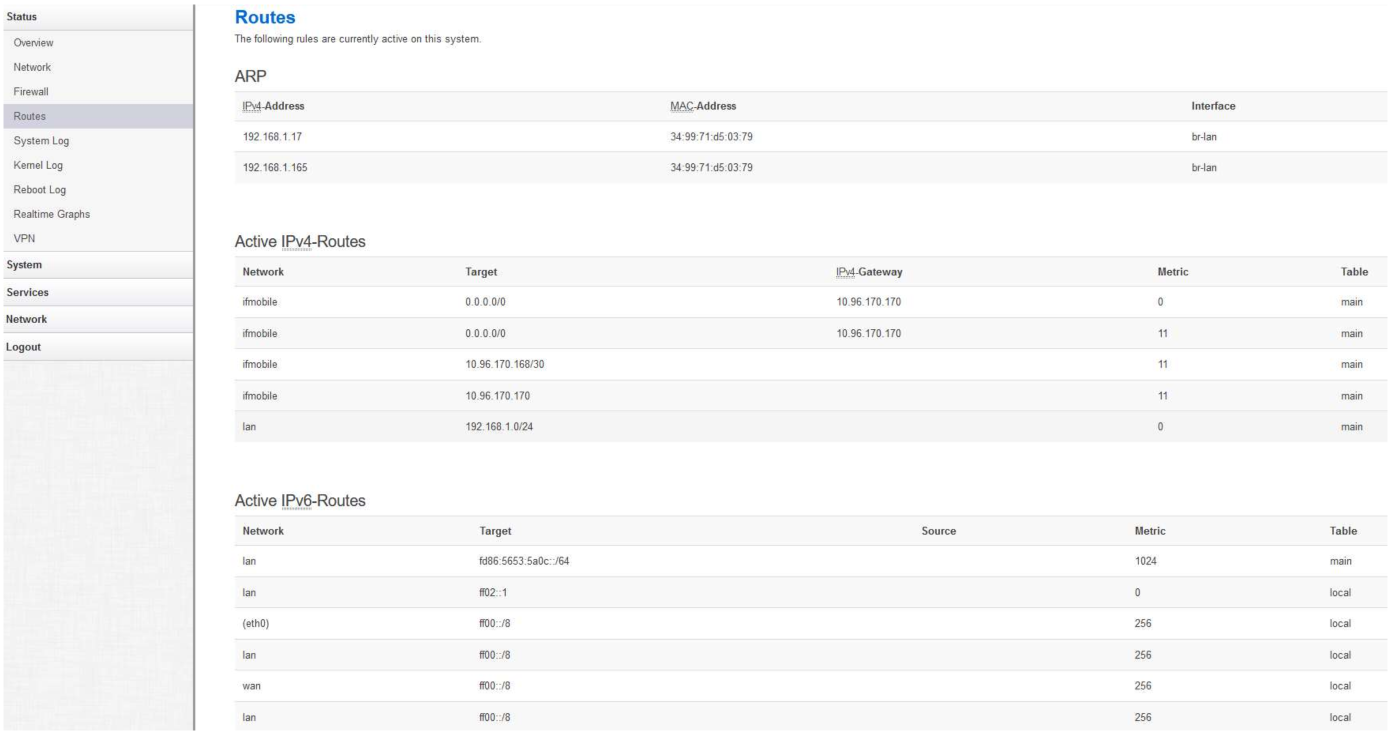
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	4404	2.52 MB	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *OUTPUT* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	2792	592.75 KB	delegate_output	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

3.3.4 Routes

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



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.1.17	34:99:71:d5:03:79	br-lan
192.168.1.165	34:99:71:d5:03:79	br-lan

Active IPv4-Routes

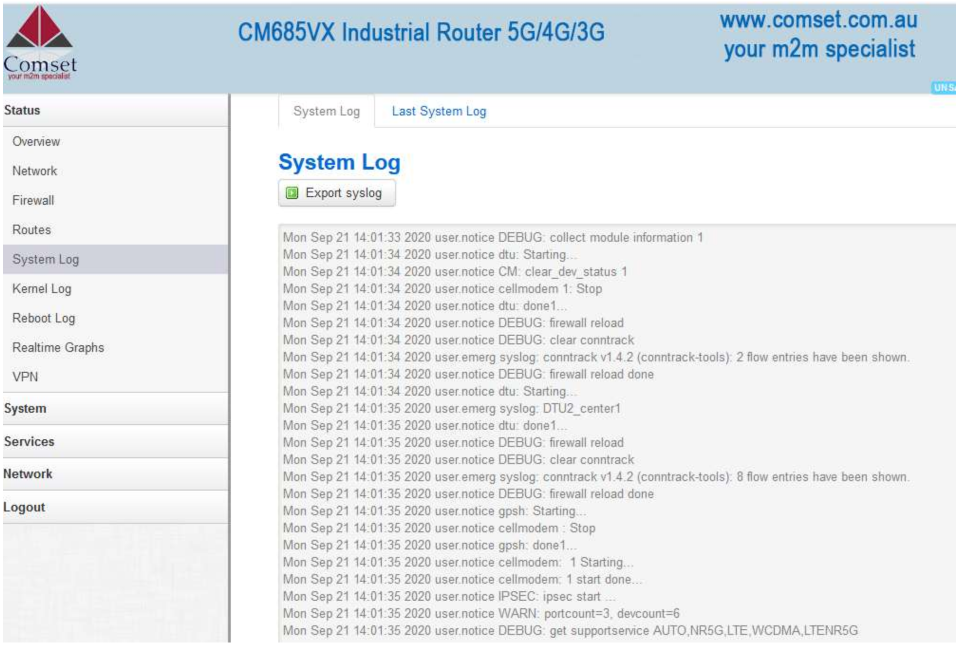
Network	Target	IPv4-Gateway	Metric	Table
ifmobile	0.0.0.0/0	10.96.170.170	0	main
ifmobile	0.0.0.0/0	10.96.170.170	11	main
ifmobile	10.96.170.168/30		11	main
ifmobile	10.96.170.170		11	main
lan	192.168.1.0/24		0	main

Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	fd86:5653:5a0c::/64		1024	main
lan	ff02::1		0	local
(eth0)	ff00::/8		256	local
lan	ff00::/8		256	local
wan	ff00::/8		256	local
lan	ff00::/8		256	local

3.3.5 System log

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

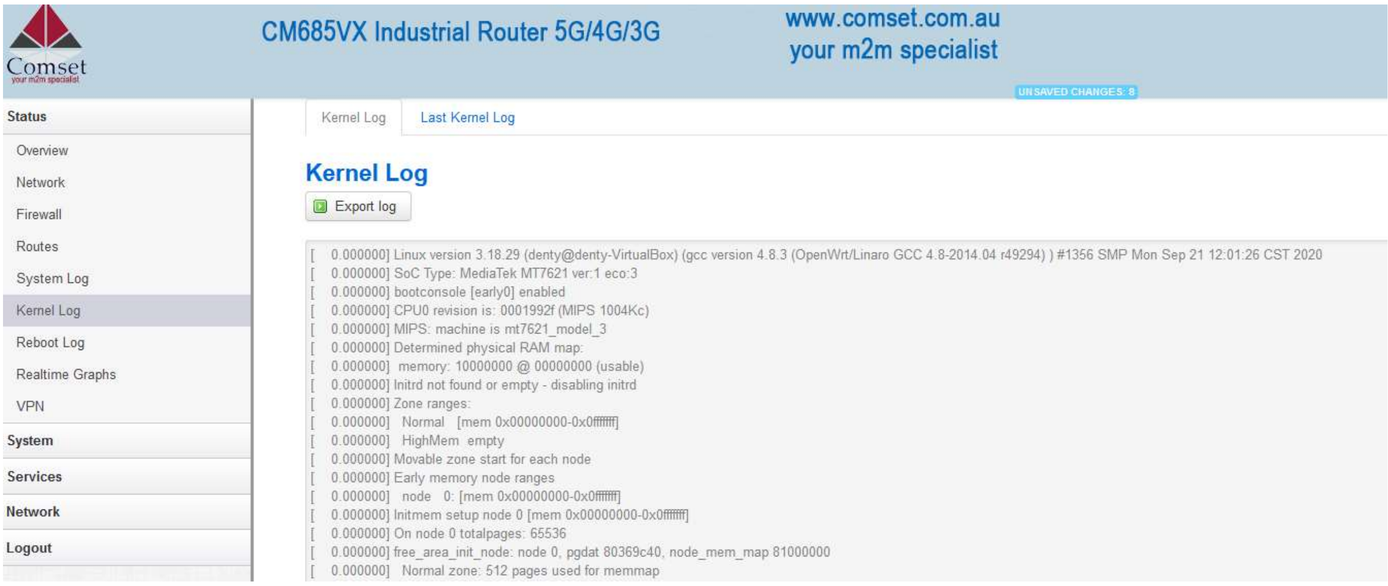


System Log

```
Mon Sep 21 14:01:33 2020 user.notice DEBUG: collect module information 1
Mon Sep 21 14:01:34 2020 user.notice dtu: Starting...
Mon Sep 21 14:01:34 2020 user.notice CM: clear_dev_status 1
Mon Sep 21 14:01:34 2020 user.notice cellmodem 1: Stop
Mon Sep 21 14:01:34 2020 user.notice dtu: done1...
Mon Sep 21 14:01:34 2020 user.notice DEBUG: firewall reload
Mon Sep 21 14:01:34 2020 user.notice DEBUG: clear conntrack
Mon Sep 21 14:01:34 2020 user.emerg syslog: conntrack v1.4.2 (conntrack-tools): 2 flow entries have been shown.
Mon Sep 21 14:01:34 2020 user.notice DEBUG: firewall reload done
Mon Sep 21 14:01:34 2020 user.notice dtu: Starting...
Mon Sep 21 14:01:35 2020 user.emerg syslog: DTU2_center1
Mon Sep 21 14:01:35 2020 user.notice dtu: done1...
Mon Sep 21 14:01:35 2020 user.notice DEBUG: firewall reload
Mon Sep 21 14:01:35 2020 user.notice DEBUG: clear conntrack
Mon Sep 21 14:01:35 2020 user.emerg syslog: conntrack v1.4.2 (conntrack-tools): 8 flow entries have been shown.
Mon Sep 21 14:01:35 2020 user.notice DEBUG: firewall reload done
Mon Sep 21 14:01:35 2020 user.notice gpsh: Starting...
Mon Sep 21 14:01:35 2020 user.notice cellmodem : Stop
Mon Sep 21 14:01:35 2020 user.notice gpsh: done1...
Mon Sep 21 14:01:35 2020 user.notice cellmodem:  1 Starting...
Mon Sep 21 14:01:35 2020 user.notice cellmodem: 1 start done...
Mon Sep 21 14:01:35 2020 user.notice IPSEC: ipsec start ...
Mon Sep 21 14:01:35 2020 user.notice WARN: portcount=3, devcount=6
Mon Sep 21 14:01:35 2020 user.notice DEBUG: get supportservice AUTO,NR5G,LTE,WCDMA,LTENR5G
```

3.3.6 Kernel log

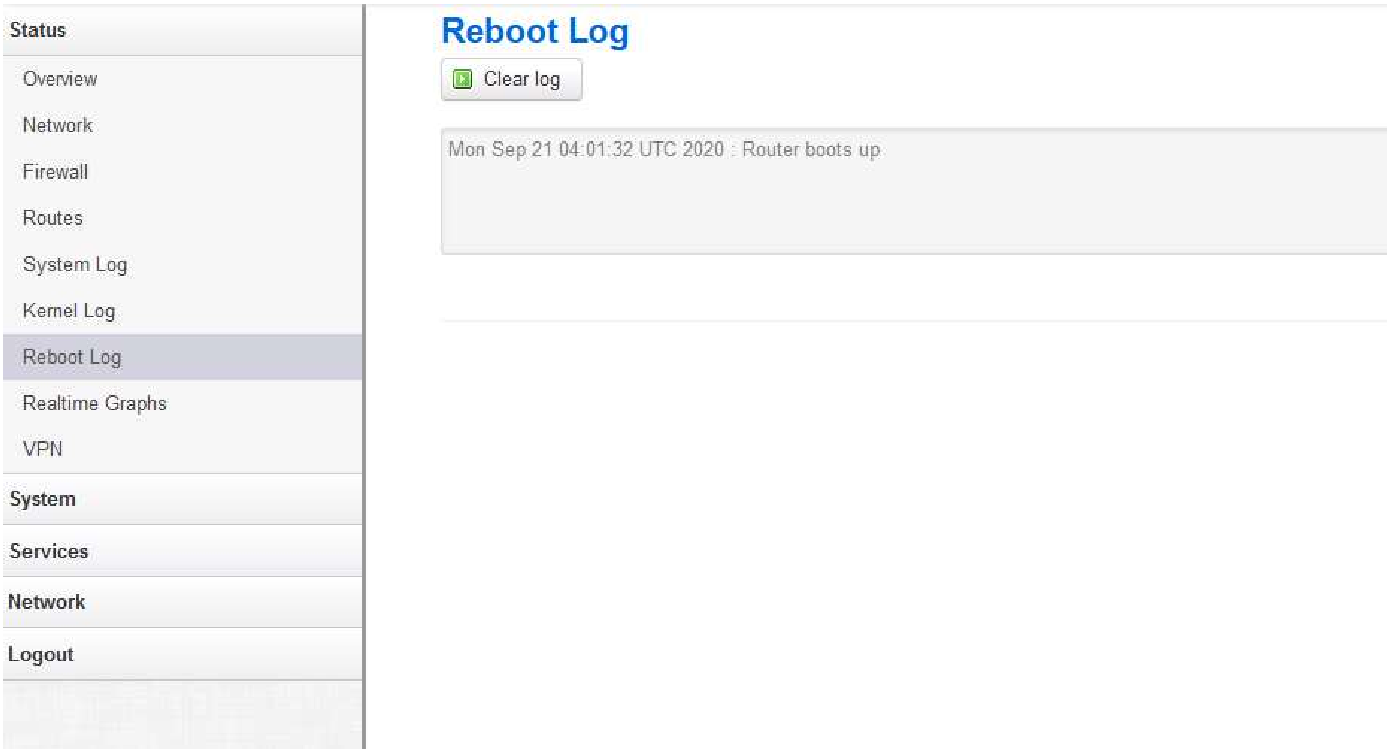
This page shows the kernel log from system boot up. This log is not saved when the router is restarted. It can be exported by clicking the button “Export Log”.



```
[    0.000000] Linux version 3.18.29 (denty@denty-VirtualBox) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r49294) ) #1356 SMP Mon Sep 21 12:01:26 CST 2020
[    0.000000] SoC Type: MediaTek MT7621 ver:1 eco:3
[    0.000000] bootconsole [early0] enabled
[    0.000000] CPU0 revision is: 0001992f (MIPS 1004Kc)
[    0.000000] MIPS: machine is mt7621_model_3
[    0.000000] Determined physical RAM map:
[    0.000000]  memory: 10000000 @ 00000000 (usable)
[    0.000000] Initrd not found or empty - disabling initrd
[    0.000000] Zone ranges:
[    0.000000]   Normal   [mem 0x00000000-0x0fffffff]
[    0.000000]   HighMem  empty
[    0.000000] Movable zone start for each node
[    0.000000] Early memory node ranges
[    0.000000]   node   0: [mem 0x00000000-0x0fffffff]
[    0.000000] Initmem setup node 0 [mem 0x00000000-0x0fffffff]
[    0.000000] On node 0 totalpages: 65536
[    0.000000] free_area_init_node: node 0, pgdat 80369c40, node_mem_map 81000000
[    0.000000]   Normal zone: 512 pages used for memmap
```

3.3.7 Reboot log

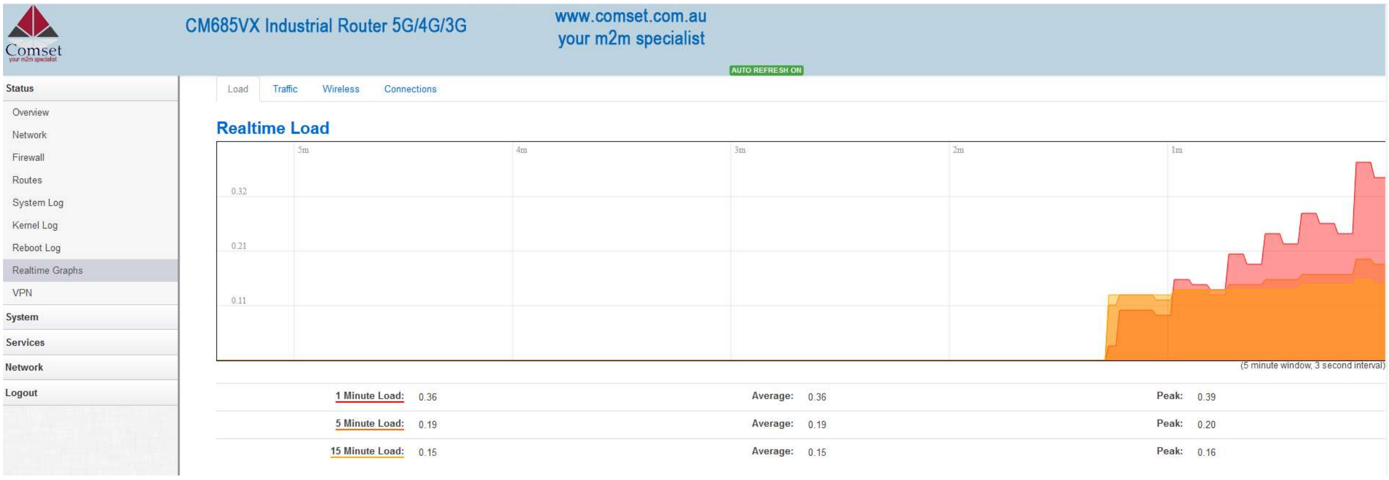
This page shows the reboot log.



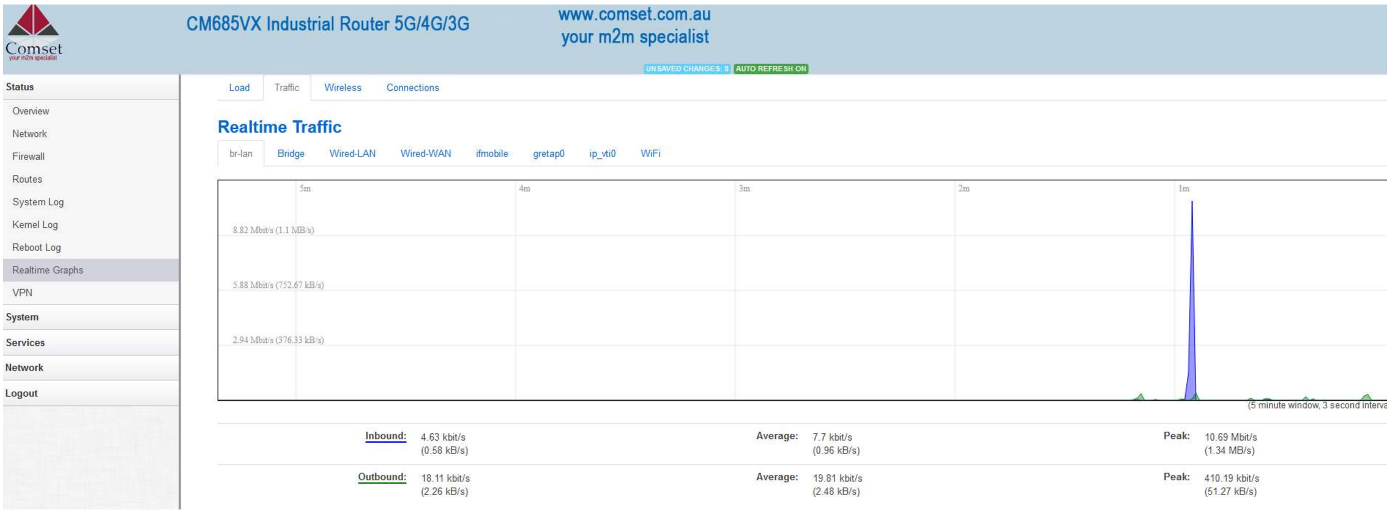
```
Mon Sep 21 04:01:32 UTC 2020 : Router boots up
```

3.3.8 Realtime graphs

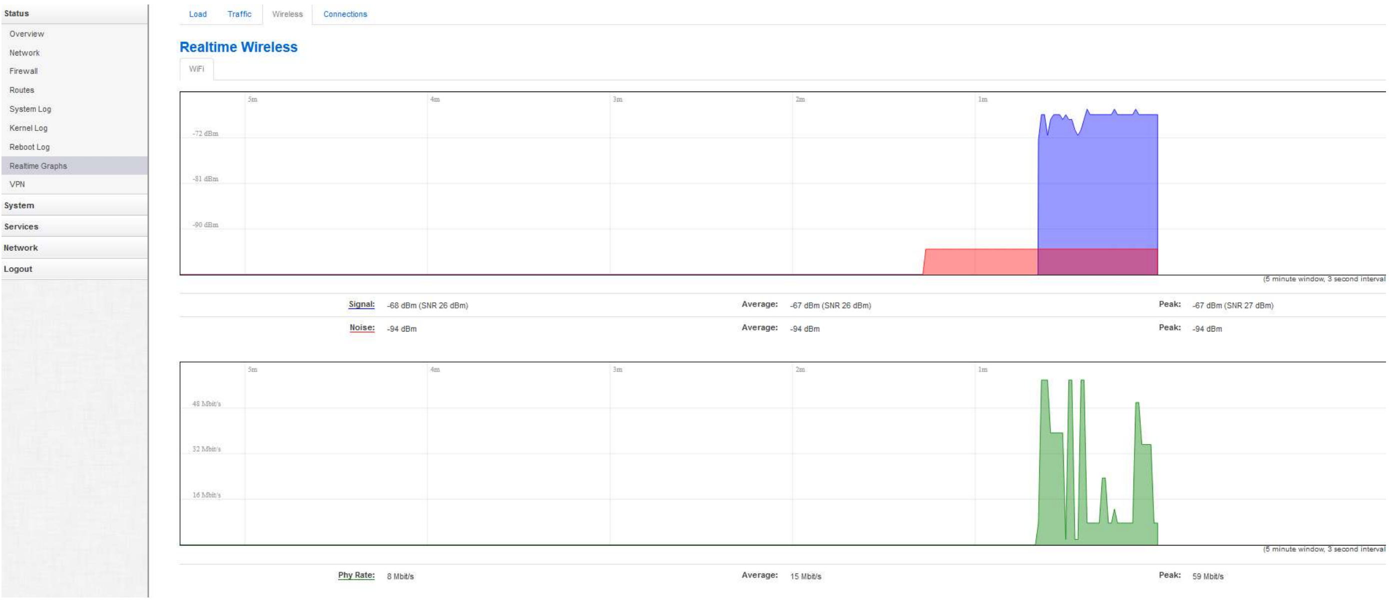
The Realtime Graphs page shows the system load and interfaces traffic in realtime.



1 Minute Load:	0.36	Average:	0.36	Peak:	0.39
5 Minute Load:	0.19	Average:	0.19	Peak:	0.20
15 Minute Load:	0.15	Average:	0.15	Peak:	0.16



Inbound:	4.63 kbit/s (0.58 kB/s)	Average:	7.7 kbit/s (0.96 kB/s)	Peak:	10.69 Mbit/s (1.34 MB/s)
Outbound:	18.11 kbit/s (2.26 kB/s)	Average:	19.81 kbit/s (2.48 kB/s)	Peak:	410.19 kbit/s (51.27 kB/s)



Realtime Wireless

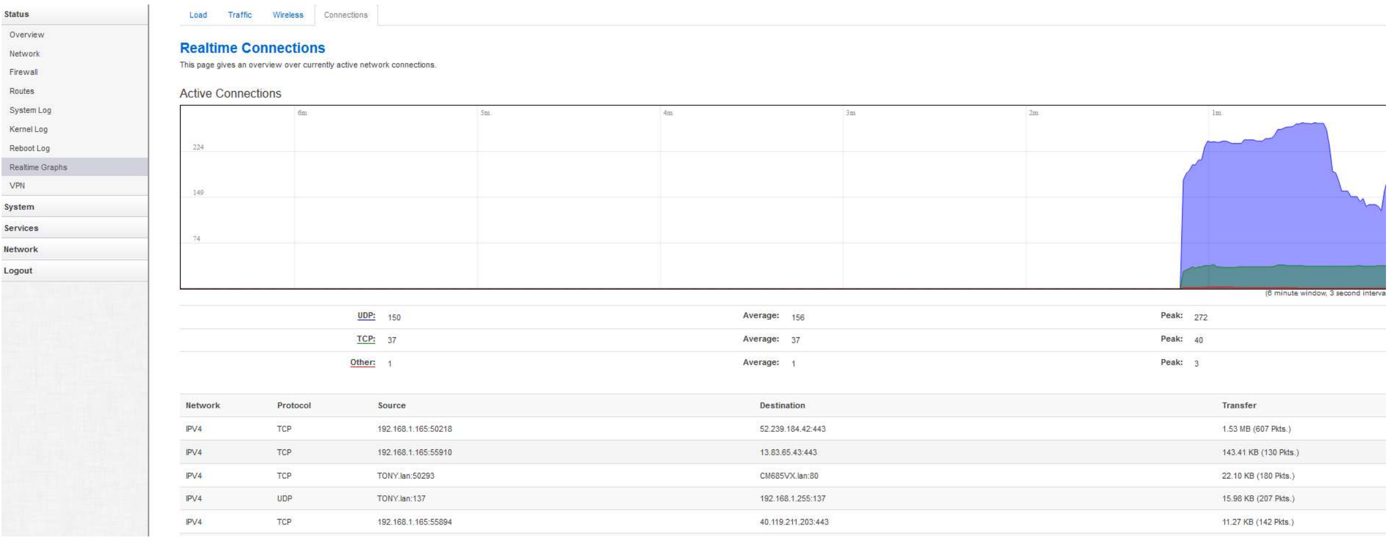
(5 minute window, 3 second interval

Signal: -68 dBm (SNR 26 dBm) Average: -67 dBm (SNR 26 dBm) Peak: -67 dBm (SNR 27 dBm)

Noise: -94 dBm Average: -94 dBm Peak: -94 dBm

(5 minute window, 3 second interval

Phy Rate: 8 Mbit/s Average: 15 Mbit/s Peak: 59 Mbit/s



Realtime Connections

This page gives an overview over currently active network connections.

Active Connections

(6 minute window, 3 second interva

UDP: 150 Average: 156 Peak: 272

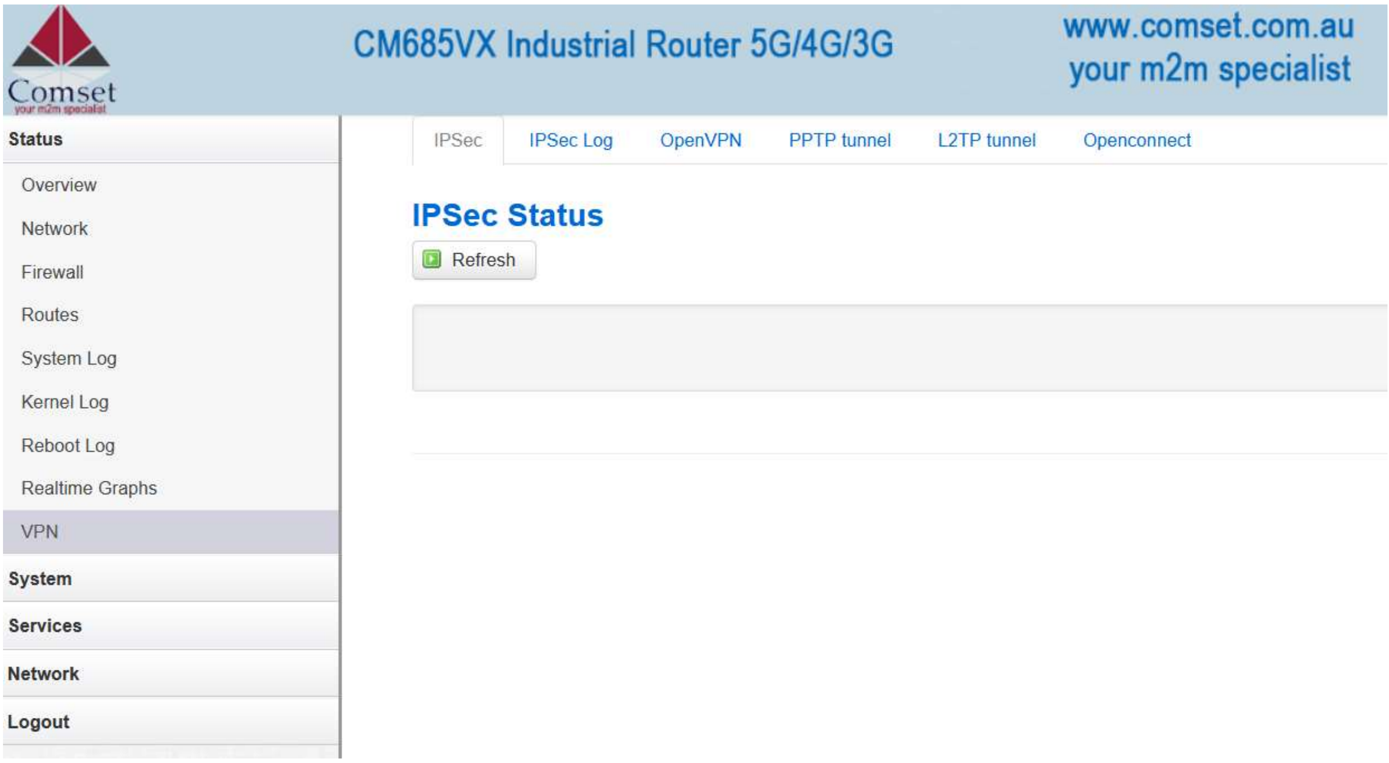
TCP: 37 Average: 37 Peak: 40

Other: 1 Average: 1 Peak: 3

Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.1.165:50218	52.239.184.42:443	1.53 MB (607 Pkts.)
IPV4	TCP	192.168.1.165:55910	13.83.65.43:443	143.41 KB (130 Pkts.)
IPV4	TCP	TONY.lan:50293	CM685VX.lan:80	22.10 KB (180 Pkts.)
IPV4	UDP	TONY.lan:137	192.168.1.255:137	15.98 KB (207 Pkts.)
IPV4	TCP	192.168.1.165:55894	40.119.211.203:443	11.27 KB (142 Pkts.)

3.3.9 VPN

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

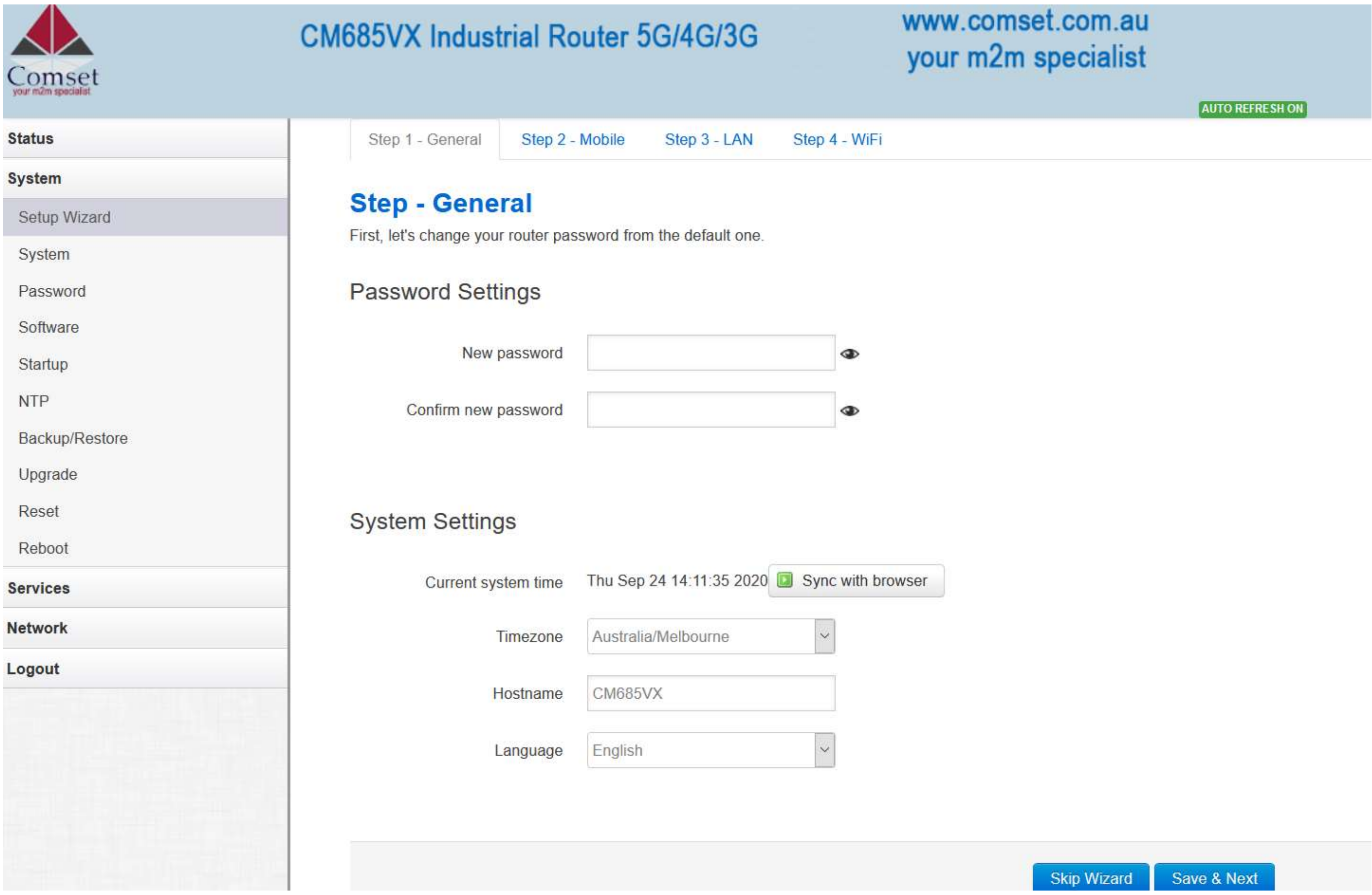


3.4 System Configuration

3.4.1 Setup wizard

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

- General
- Mobile
- LAN
- WiFi



Step - General

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

Password Settings

New password

Confirm new password

System Settings

Current system time: Thu Sep 24 14:11:35 2020

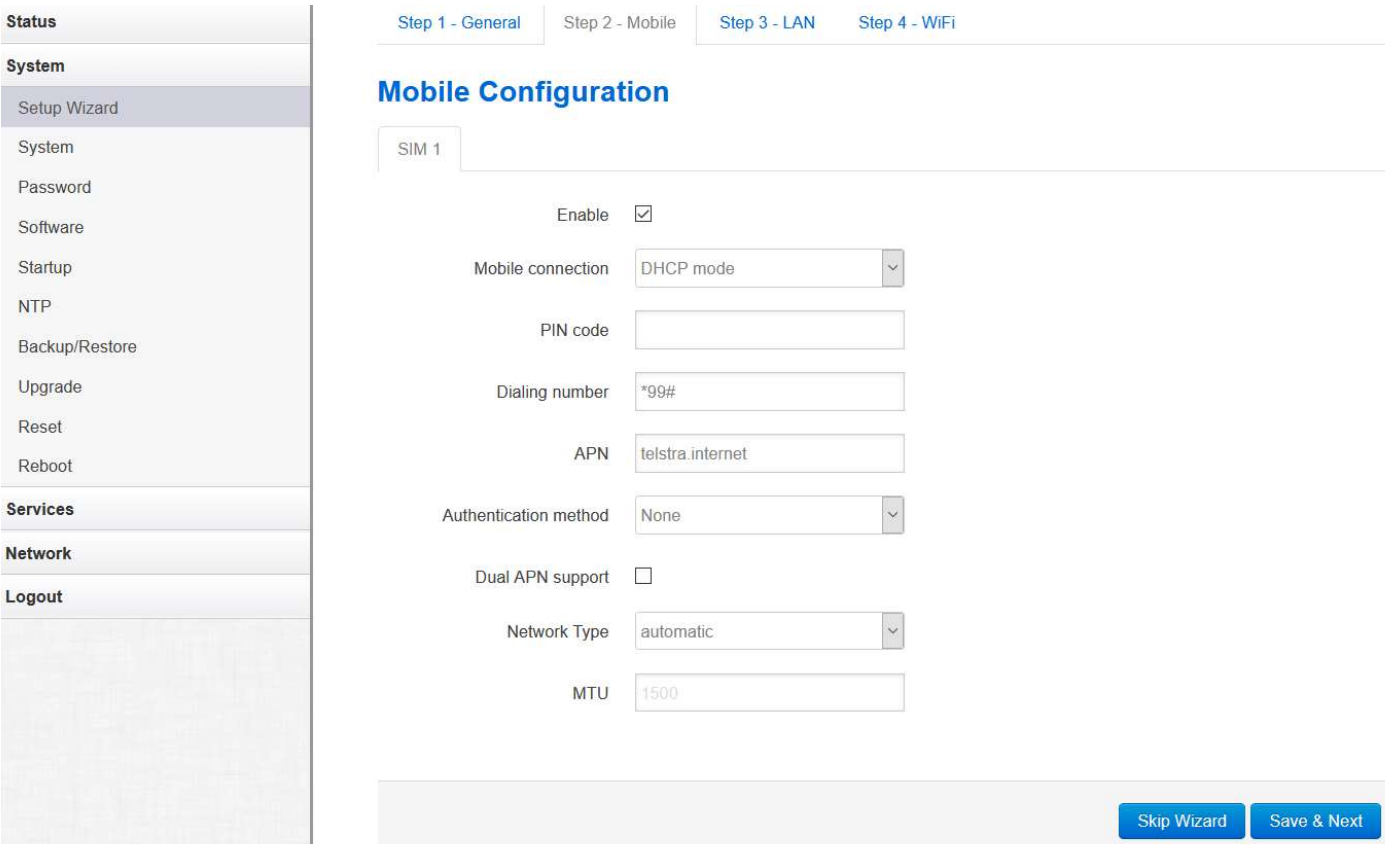
Timezone: Australia/Melbourne

Hostname: CM685VX

Language: English

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

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



Mobile Configuration

Enable ☑

Mobile connection: DHCP mode

PIN code:

Dialing number: *99#

APN: telstra.internet

Authentication method: None

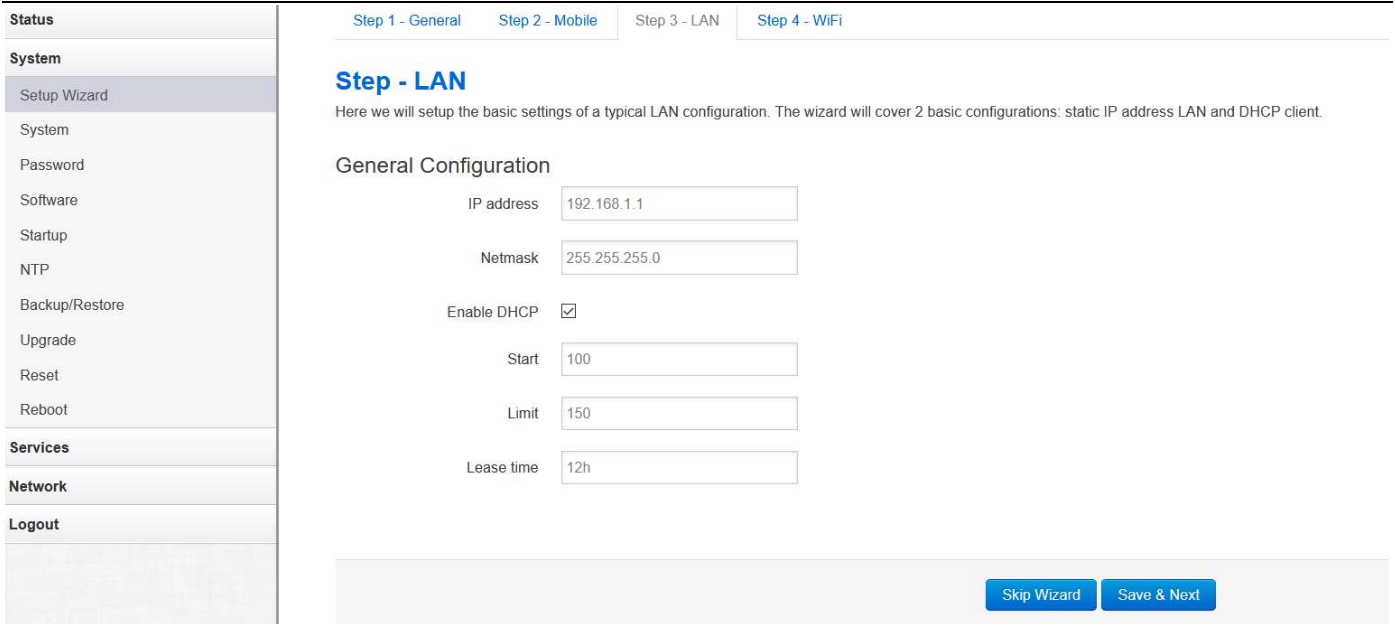
Dual APN support □

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

When finished, click “Save & Next”



Step - LAN

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

General Configuration

IP address: 192.168.1.1

Netmask: 255.255.255.0

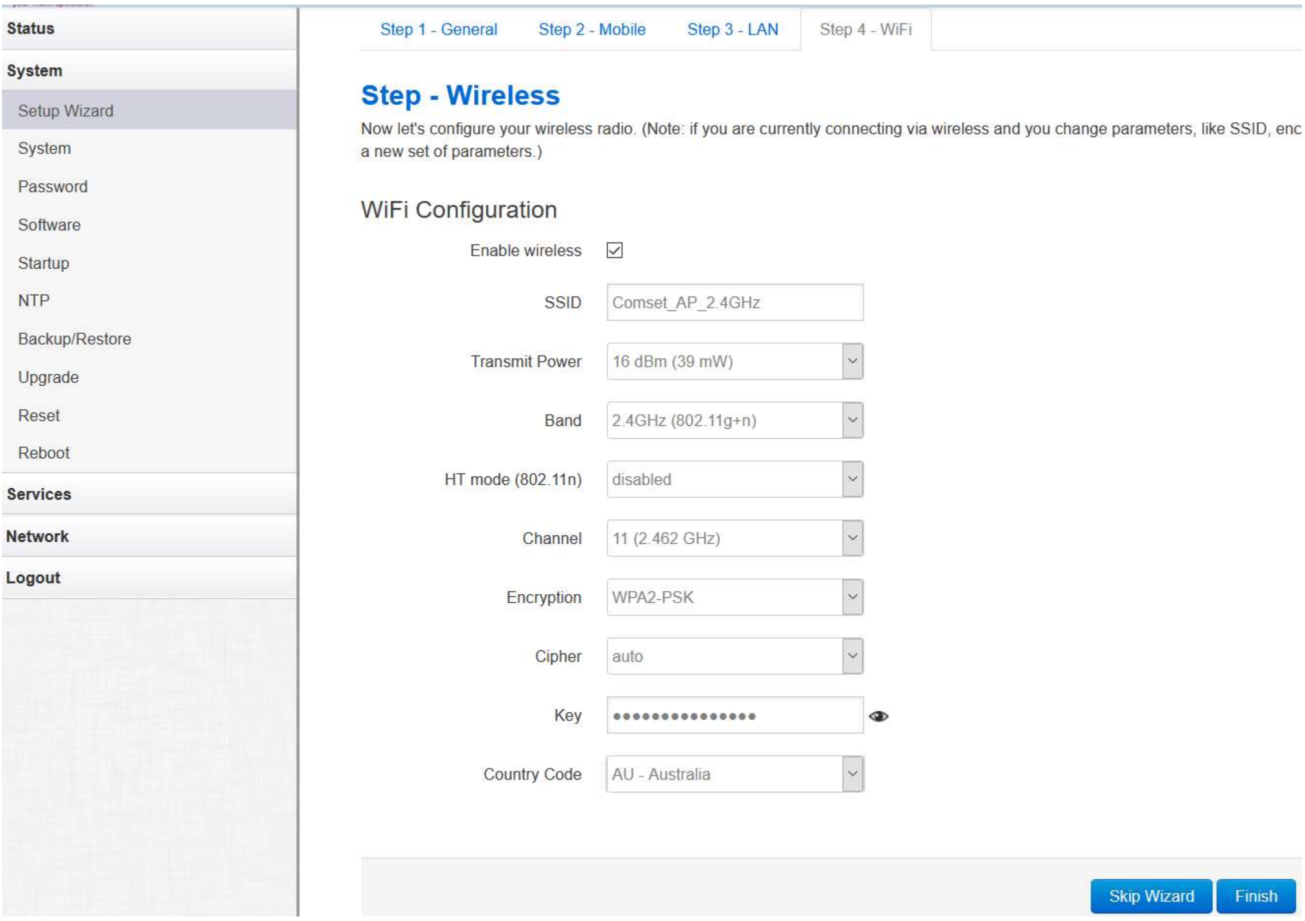
Enable DHCP: ☑

Start: 100

Limit: 150

Lease time: 12h

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



Step - Wireless

Now let's configure your wireless radio. (Note: if you are currently connecting via wireless and you change parameters, like SSID, enc a new set of parameters.)

WiFi Configuration

Enable wireless: ☑

SSID: Comset_AP_2.4GHz

Transmit Power: 16 dBm (39 mW)

Band: 2.4GHz (802.11g+n)

HT mode (802.11n): disabled

Channel: 11 (2.462 GHz)

Encryption: WPA2-PSK

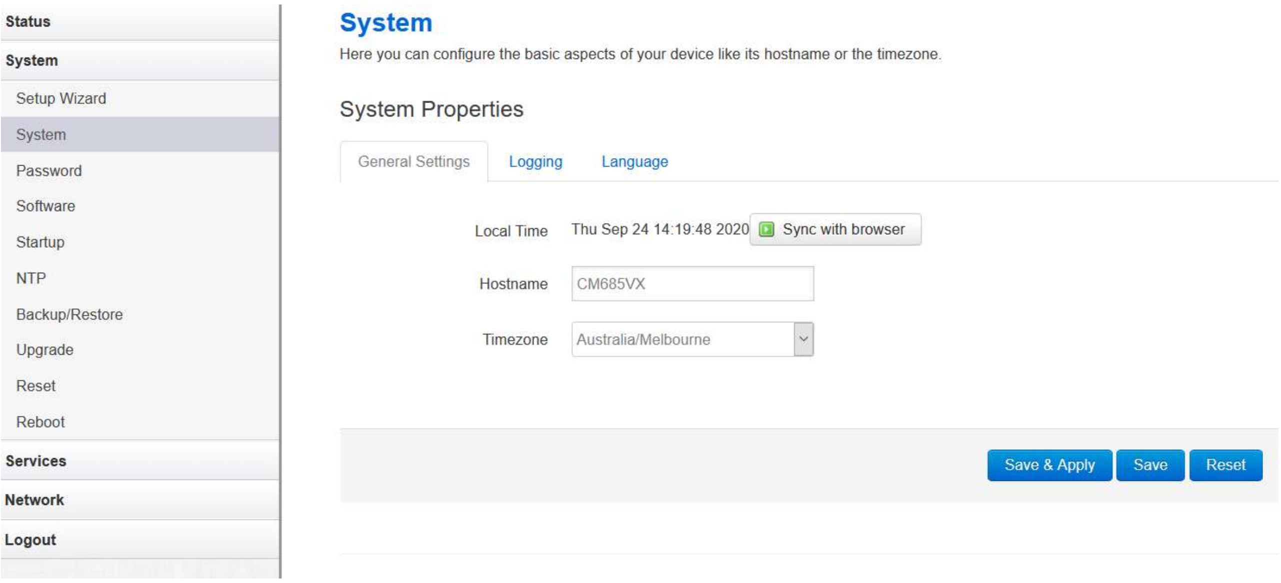
Cipher: auto

Key: ●●●●●●●●●●●●●●●

Country Code: AU - Australia

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

3.4.2 System



System

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

System Properties

Local Time: Thu Sep 24 14:19:48 2020

Hostname: CM685VX

Timezone: Australia/Melbourne

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”.

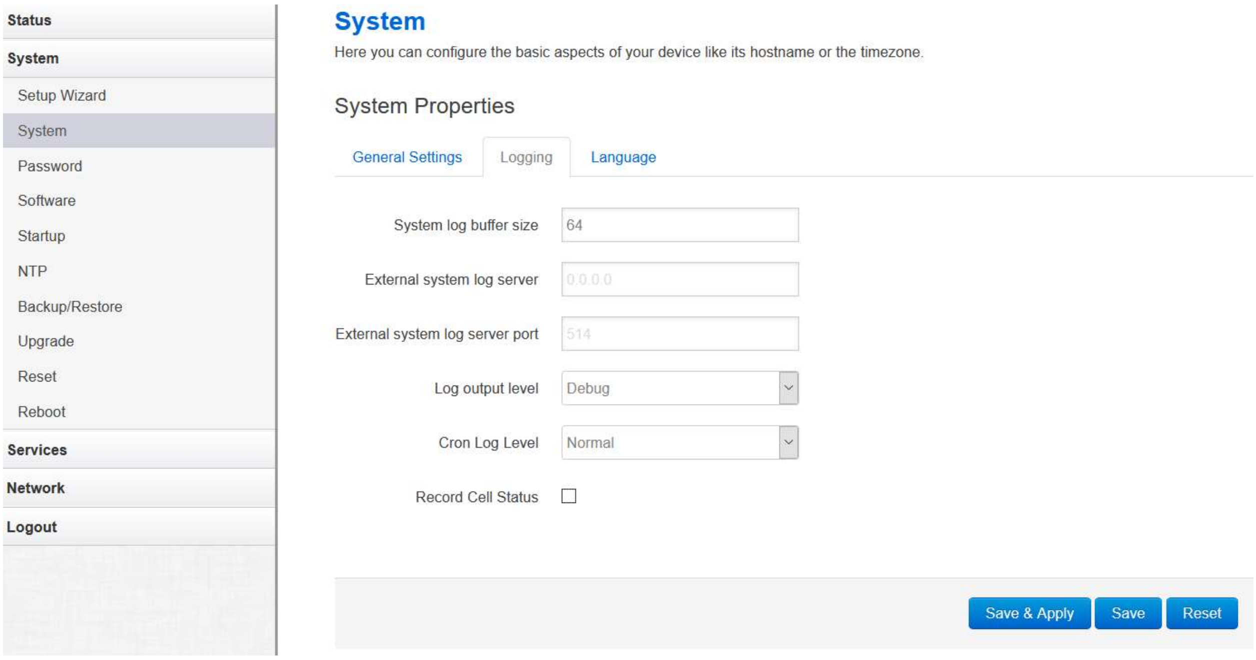
Hostname

It is the router’s name. The default name is “CM685VX”

Time zone

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

Logging



System

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

System Properties

System log buffer size: 64

External system log server: 0.0.0.0

External system log server port: 514

Log output level: Debug

Cron Log Level: Normal

Record Cell Status: □

System log buffer size

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

External system log server

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

External system log server port

This is the UDP port of the external log server.

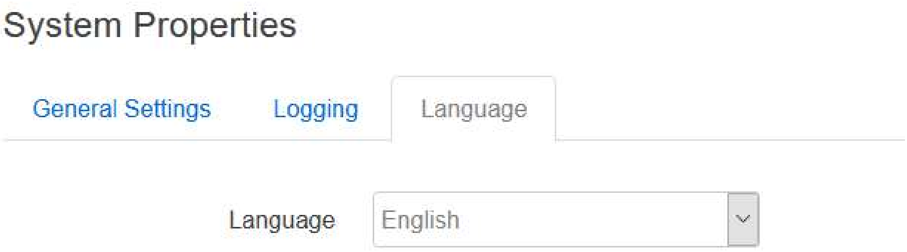
Log output level

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

Cron log level

It is the log level to process Crond.

Language

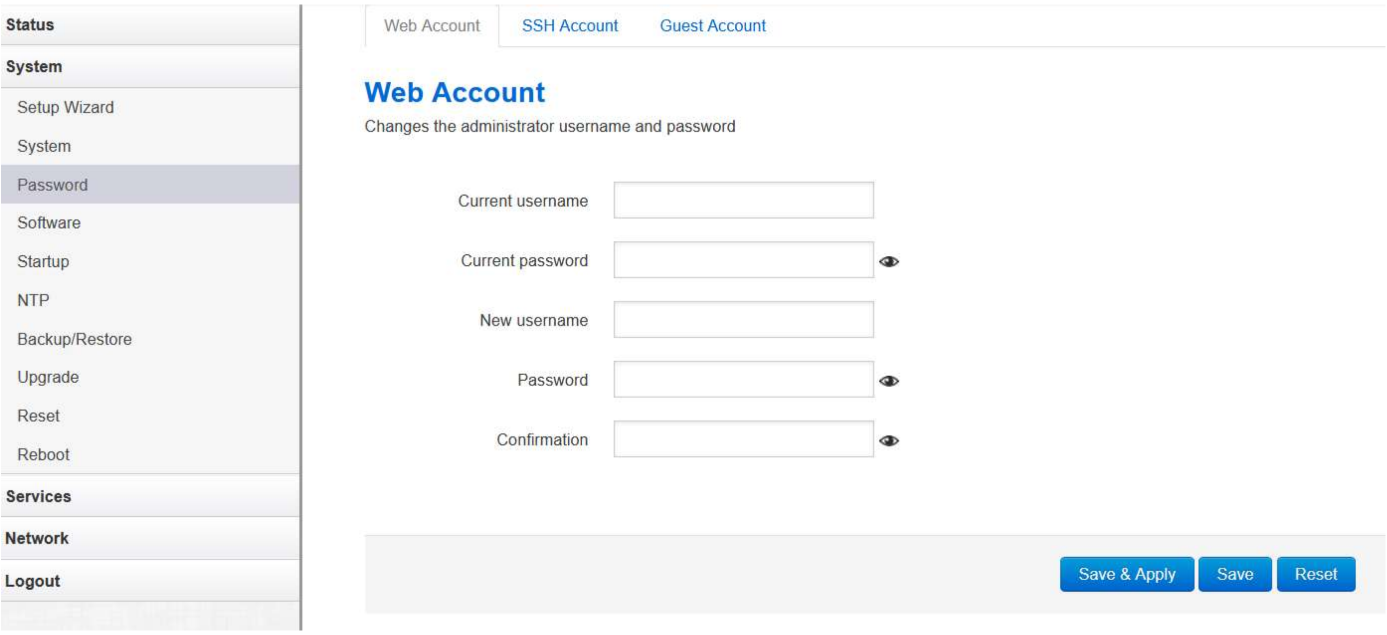


System Properties

Language: English

The default language is “English”.

3.4.3 Password



Web Account

Changes the administrator username and password

Current username

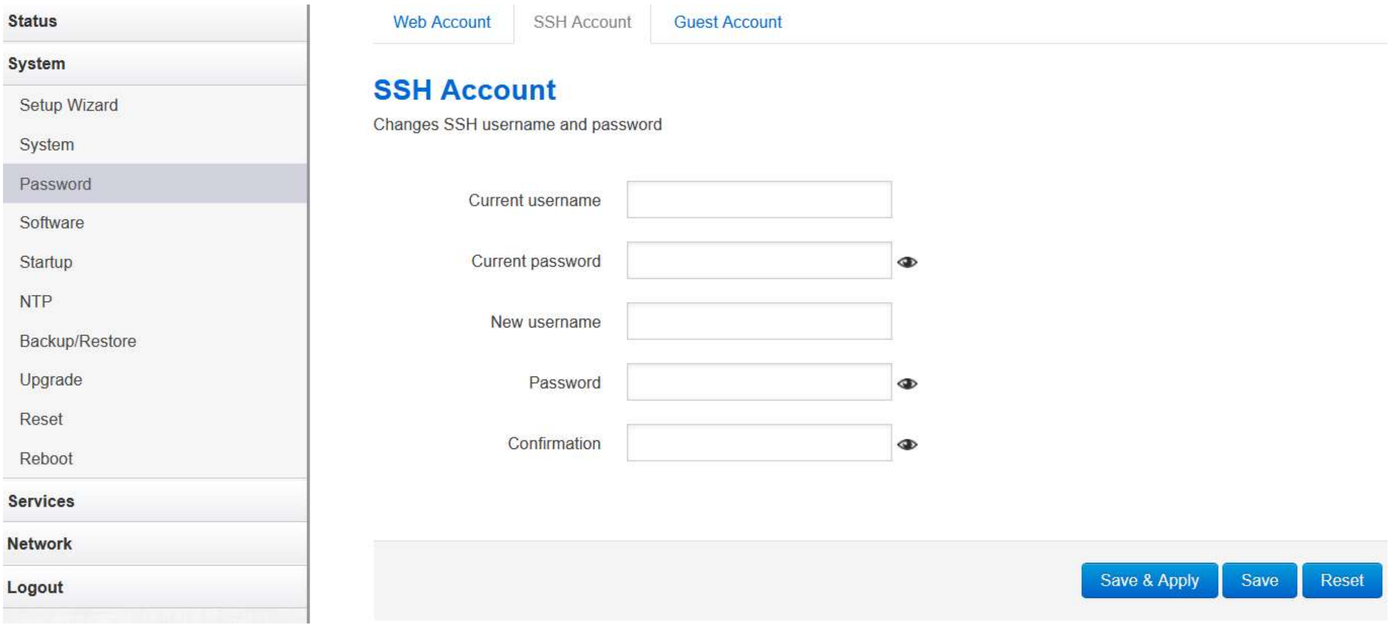
Current password

New username

Password

Confirmation

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



SSH Account

Changes SSH username and password

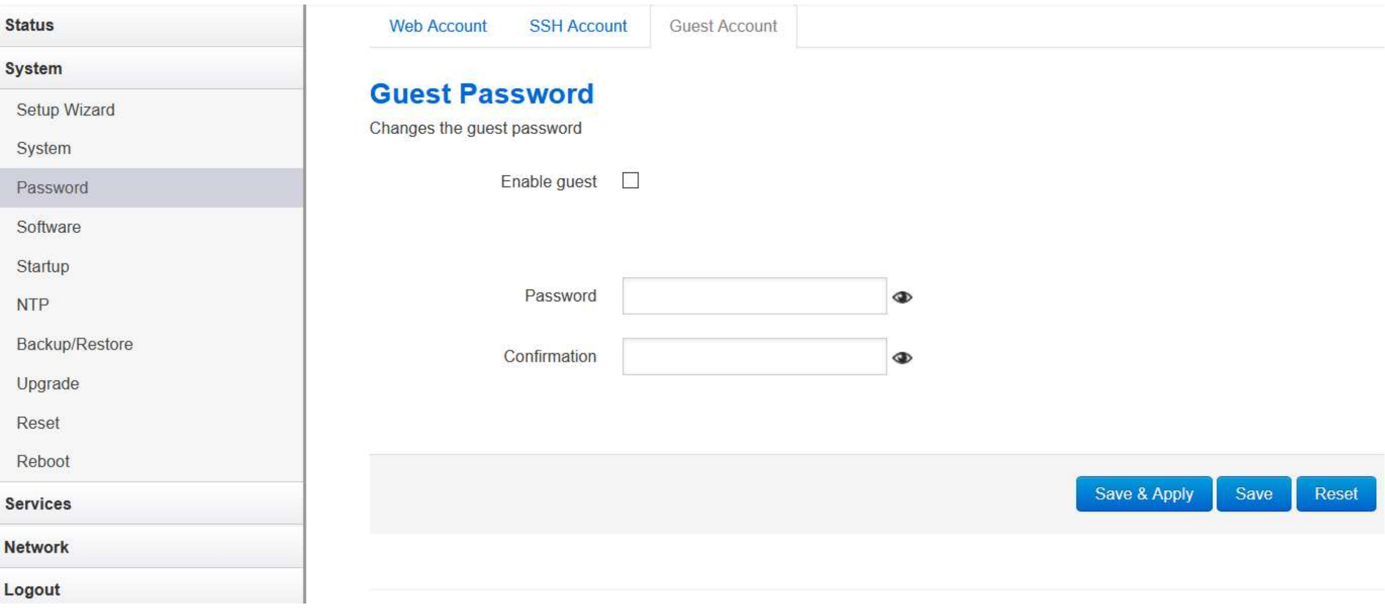
Current username

Current password

New username

Password

Confirmation



Guest Password

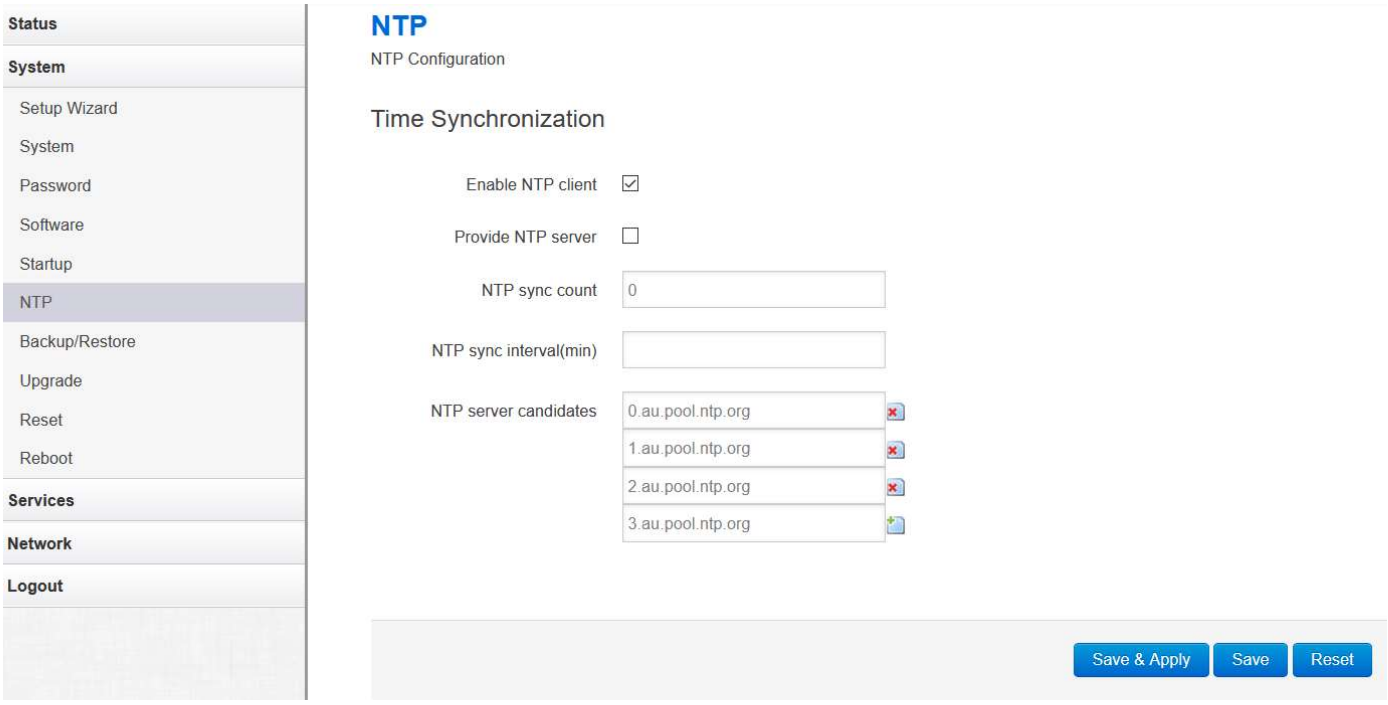
Changes the guest password

Enable guest □

Password

Confirmation

3.4.4 NTP



NTP

NTP Configuration

Time Synchronization

Enable NTP client ☑

Provide NTP server □

NTP sync count 0

NTP sync interval(min)

NTP server candidates 0.au.pool.ntp.org ☒
1.au.pool.ntp.org ☒
2.au.pool.ntp.org ☒
3.au.pool.ntp.org ⊞

NTP is Network Timing Protocol.

- **Enable NTP client**

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

- **Provide NTP server**

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

- **NTP sync count**

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

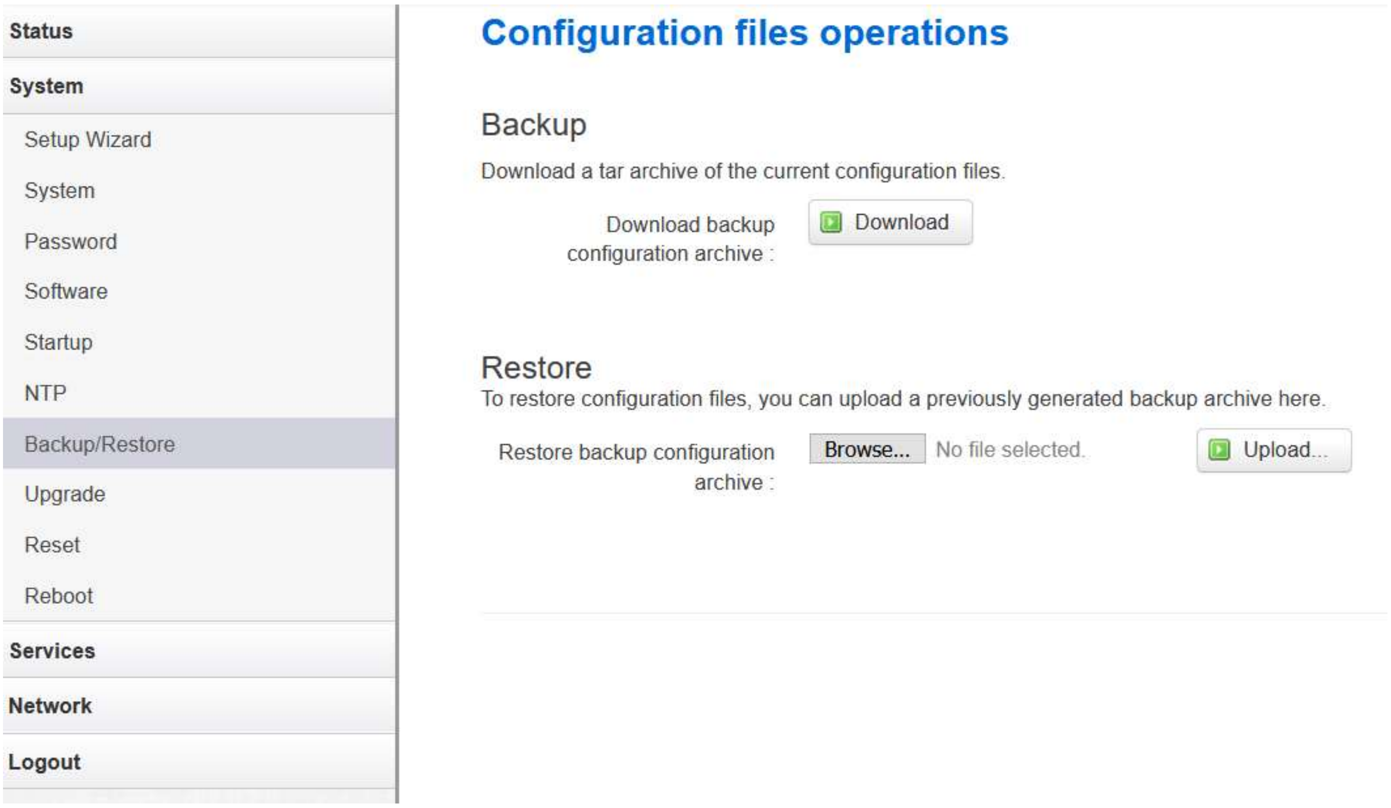
- **NTP sync interval (min)**

This is the interval time between NTP synchronisation.

- **NTP server candidates**

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

3.4.5 Backup/Restore



Configuration files operations

Backup

Download a tar archive of the current configuration files.

Download backup configuration archive : Download

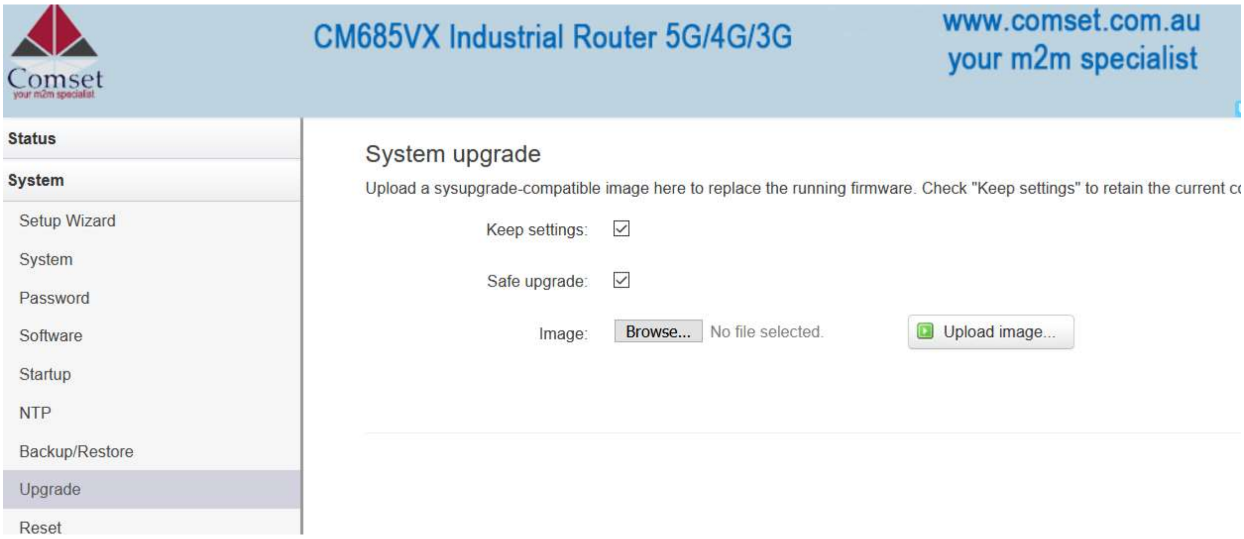
Restore

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup configuration archive : Browse... No file selected. Upload...

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

3.4.6 Upgrade



System upgrade

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current c

Keep settings: ☑

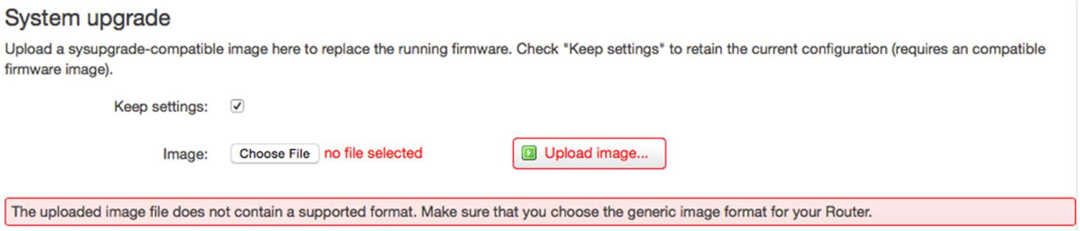
Safe upgrade: ☑

Image: Browse... No file selected.

Upload image...

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

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



System upgrade

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

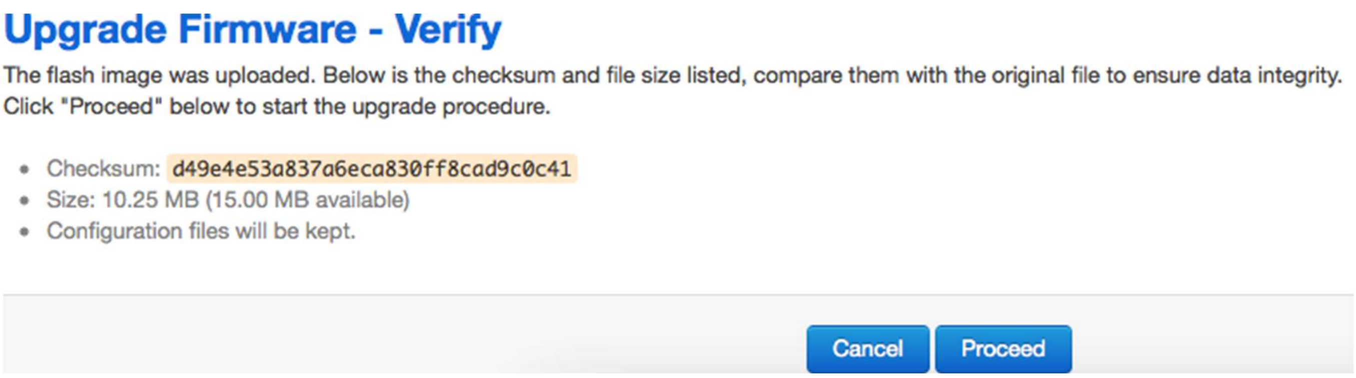
Keep settings: ☑

Image: Choose File no file selected

Upload image...

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

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

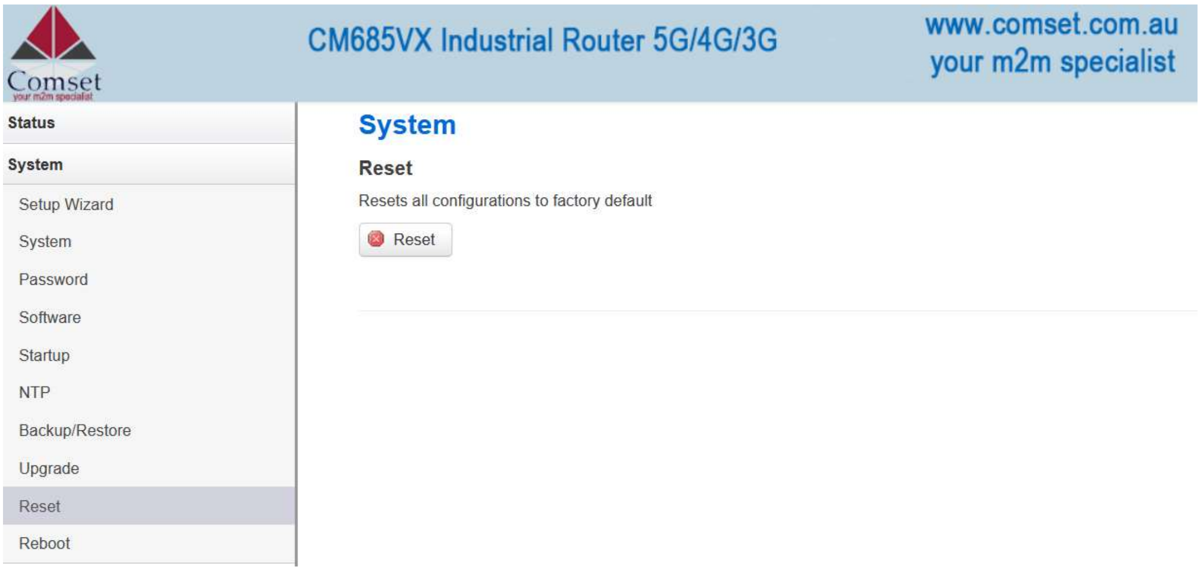


Upgrade Firmware - Verify

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

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

3.4.7 Reset



System

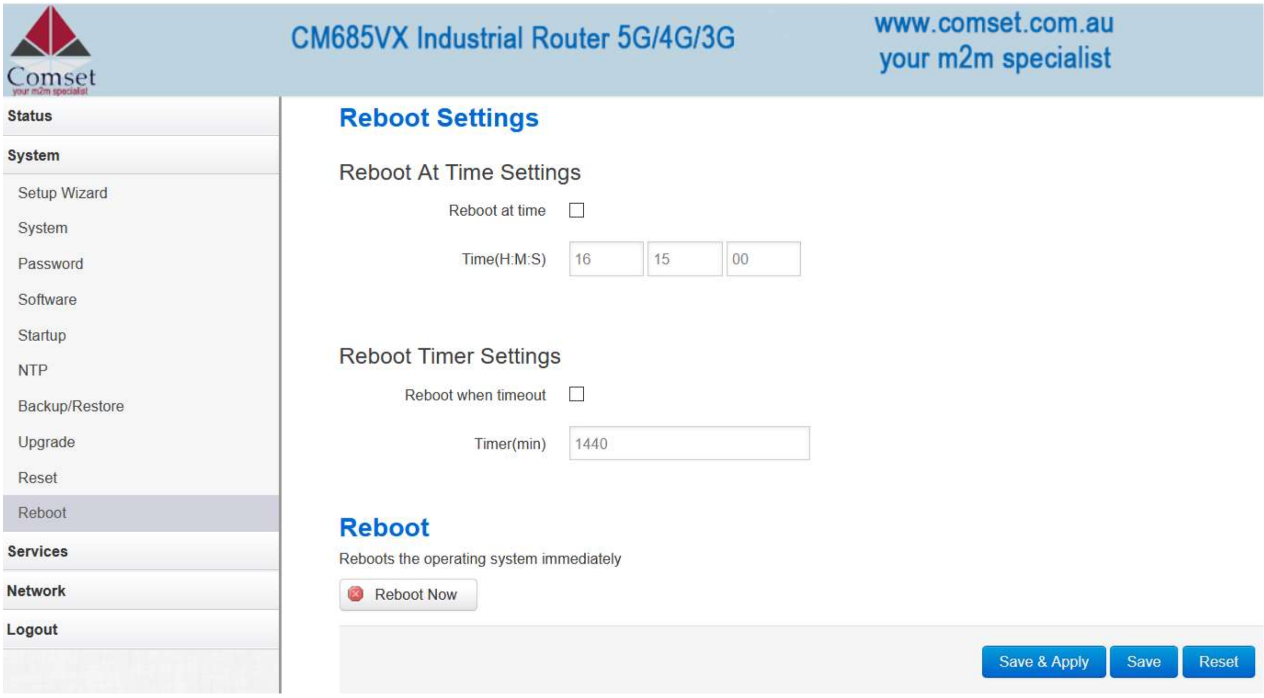
Reset

Resets all configurations to factory default

Reset

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

3.4.8 Reboot



Reboot Settings

Reboot At Time Settings

Reboot at time □

Time(H:M:S) 16 15 00

Reboot Timer Settings

Reboot when timeout □

Timer(min) 1440

Reboot

Reboots the operating system immediately

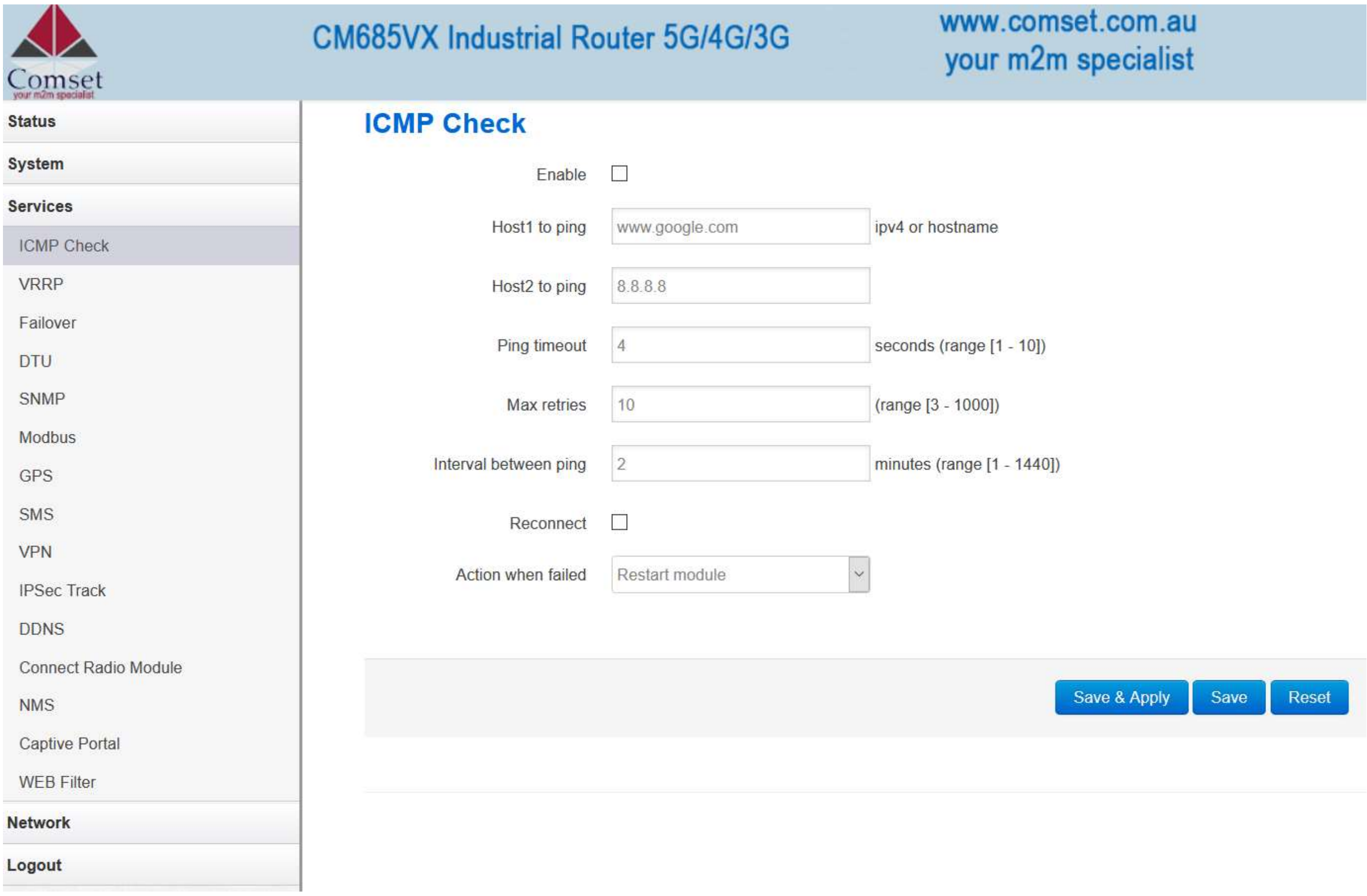
Reboot Now

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

3.5 Services configuration

3.5.1 ICMP check

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



ICMP Check

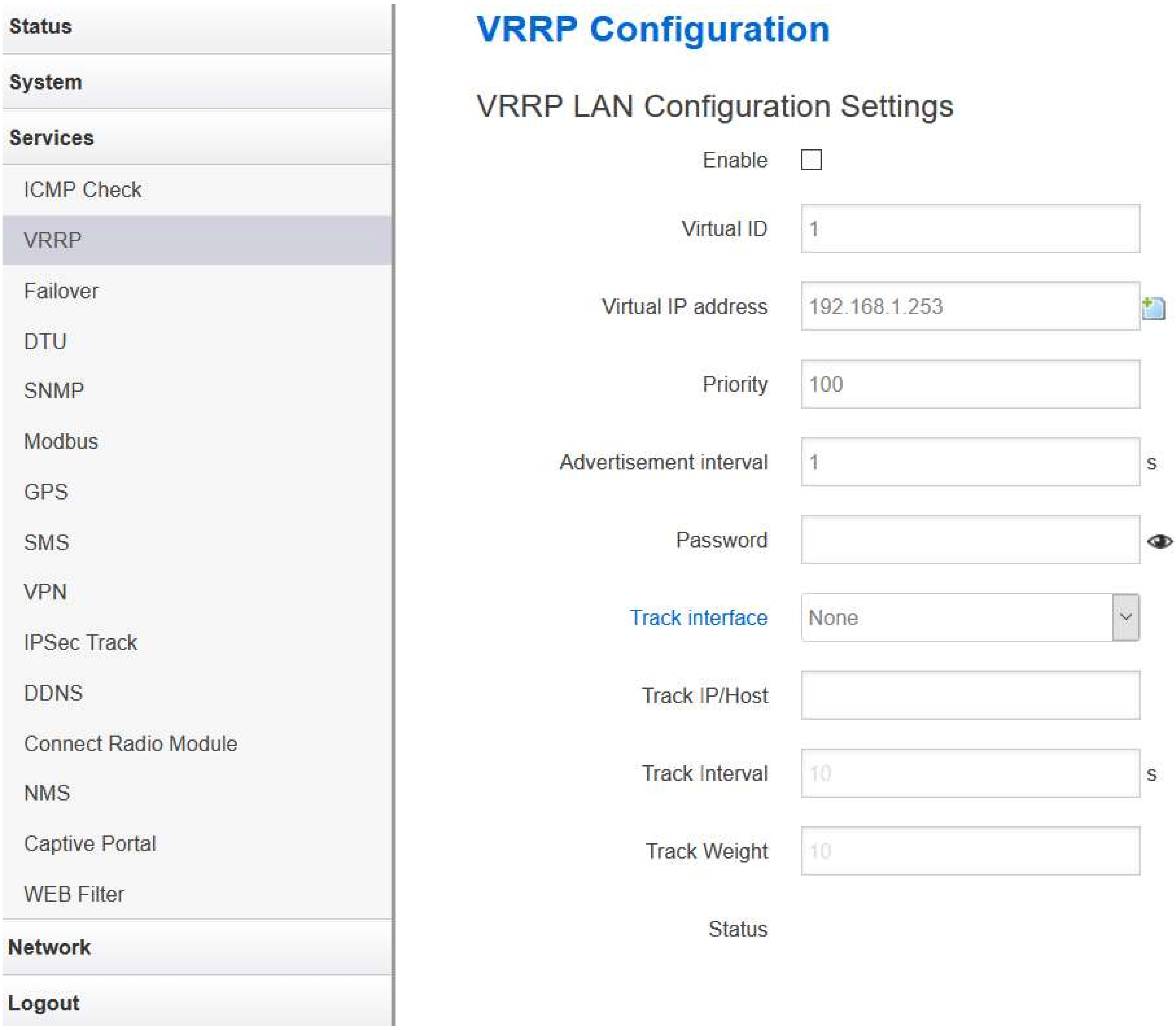
Enable	□	
Host1 to ping	www.google.com	ipv4 or hostname
Host2 to ping	8.8.8.8	
Ping timeout	4	seconds (range [1 - 10])
Max retries	10	(range [3 - 1000])
Interval between ping	2	minutes (range [1 - 1440])
Reconnect	□	
Action when failed	Restart module	

- **Enable**: Enable ICMP check feature.
- **Host1 to ping / Host2 to ping**: The domain name or IP address for checking the network connection.
- **Ping timeout**: After a ping packet is sent, if the response packet is not received before the timeout, then this ping has failed.
- **Max retries**: When the number of failed pings reaches the "Max retries", this will trigger the action

configured in item “Action when failed”.

- **Interval between pings**: The time between two pings in minutes.
- **Reconnect**: Reconnect cell interface if ping failed.
- **Action when failed**: the options are “Restart module” and “Restart router”. “Restart module” will restart the radio module. “Restart router” will restart the whole system including the radio module.

3.5.2 VRRP



VRRP Configuration

VRRP LAN Configuration Settings

Enable ☐

Virtual ID: 1

Virtual IP address: 192.168.1.253

Priority: 100

Advertisement interval: 1 s

Password:

Track interface: None

Track IP/Host:

Track Interval: 10 s

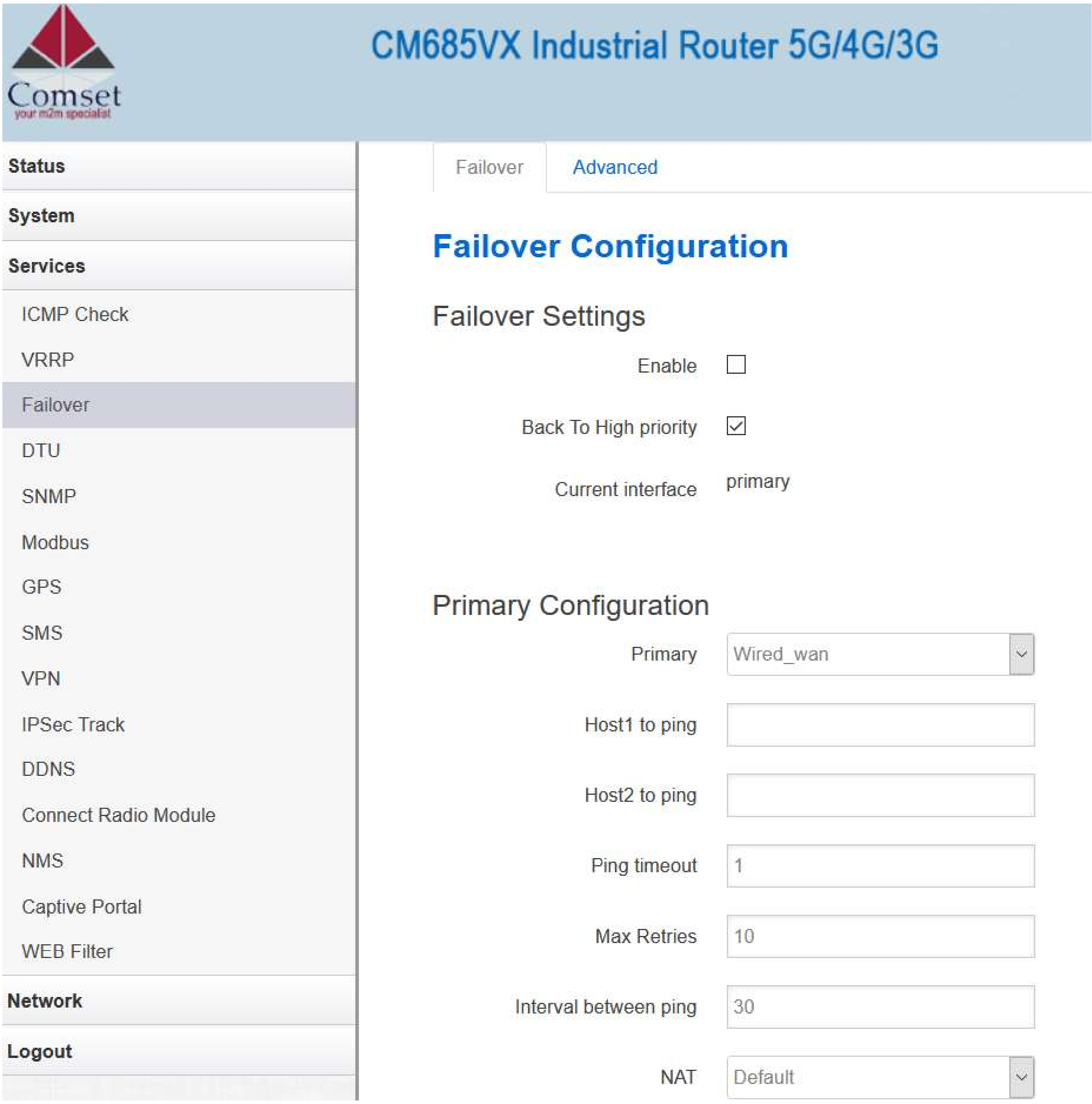
Track Weight: 10

Status

- **Enable**: Enable VRRP (Virtual Router Redundancy Protocol) for LAN.
- **Virtual ID**: Routers with the same IDs will be grouped in the same VRRP cluster, range [1 – 255]
- **Virtual IP address**: Virtual IP address for LAN’s VRRP cluster. IP address entry can be deleted by clicking the button ☒, or added by clicking the button ➕.

- **Priority**: The router with the highest priority in the same VRRP cluster will act as master. Range [1–255]
- **Advertisement interval**: VRRP send packet to a set of VRRP instances to advertise the device in the MASTER state.
- **Password**: The password for VRRP access.
- **Track interface**: Check if the local interface is up or down.
- **Track IP/Host**: The Host or IP address to ping.
- **Track Interval**: The ping interval.
- **Track Weight**: Priority will be subtracted from the initial priority in case of ping failure.
- **Status**: Shows VRRP status (MASTER/BACKUP).

3.5.3 Failover (link backup)



Failover Configuration

Failover Settings

Enable □

Back To High priority ☑

Current interface primary

Primary Configuration

Primary: Wired_wan

Host1 to ping:

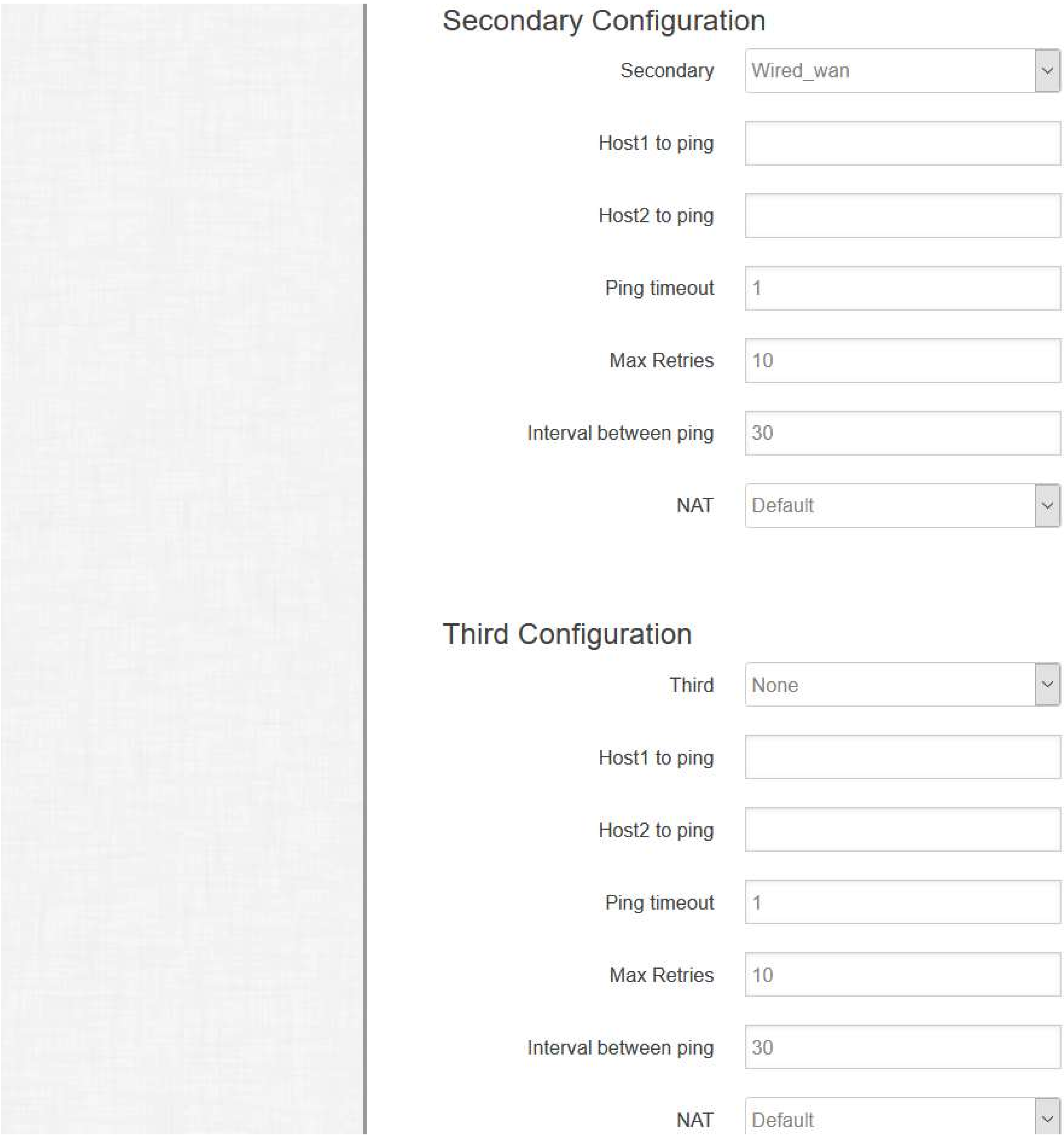
Host2 to ping:

Ping timeout: 1

Max Retries: 10

Interval between ping: 30

NAT: Default



Secondary Configuration

Secondary	Wired_wan
Host1 to ping	
Host2 to ping	
Ping timeout	1
Max Retries	10
Interval between ping	30
NAT	Default

Third Configuration

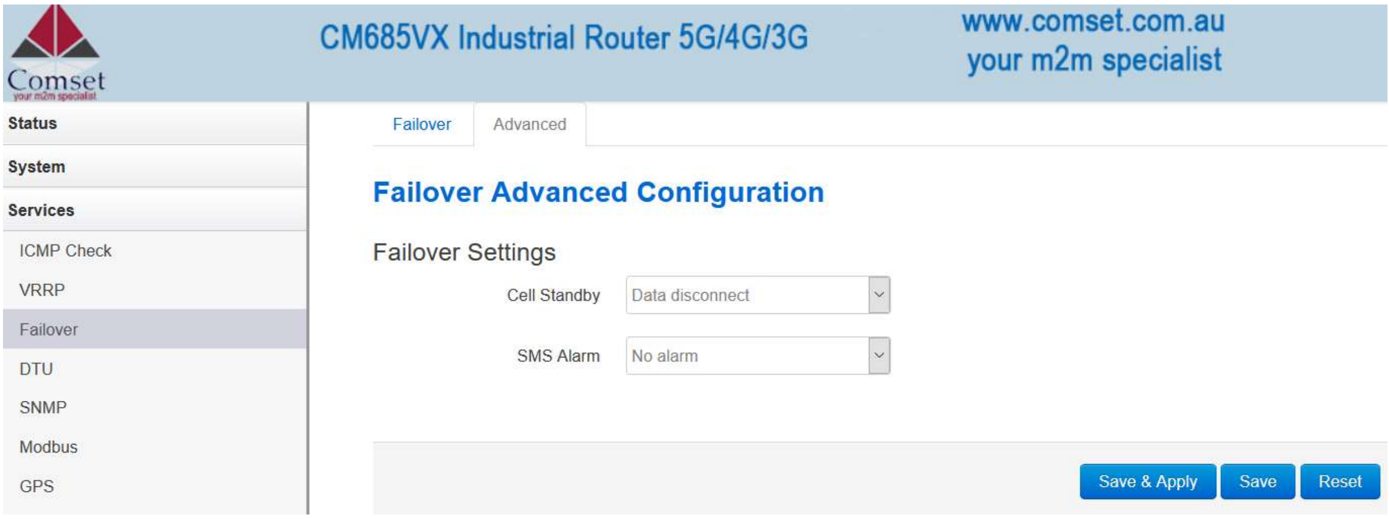
Third	None
Host1 to ping	
Host2 to ping	
Ping timeout	1
Max Retries	10
Interval between ping	30
NAT	Default

- **Enable**: Enable failover feature
  - **Back to high priority**: If “back to high priority” is checked, the router will go back to the selected “high priority” WAN interface when available. The priorities can be set to primary, secondary and third priority. There are four options to choose from: Wired-WAN, Wifi_client, Cell_mobile, and None.
- **Host1 to ping / Host2 to ping**: The domain name or IP address for checking the network

connection.

- **Ping timeout**: After a ping packet is sent, if the response packet is not received before the timeout, then this ping has failed.
- **Max retries**: When the number of failed pings reaches the "Max retries", this will confirm that the WAN interface is unavailable.
- **Interval between pings**: The time between two pings in seconds.

Failover Advanced



Failover Advanced Configuration

Failover Settings

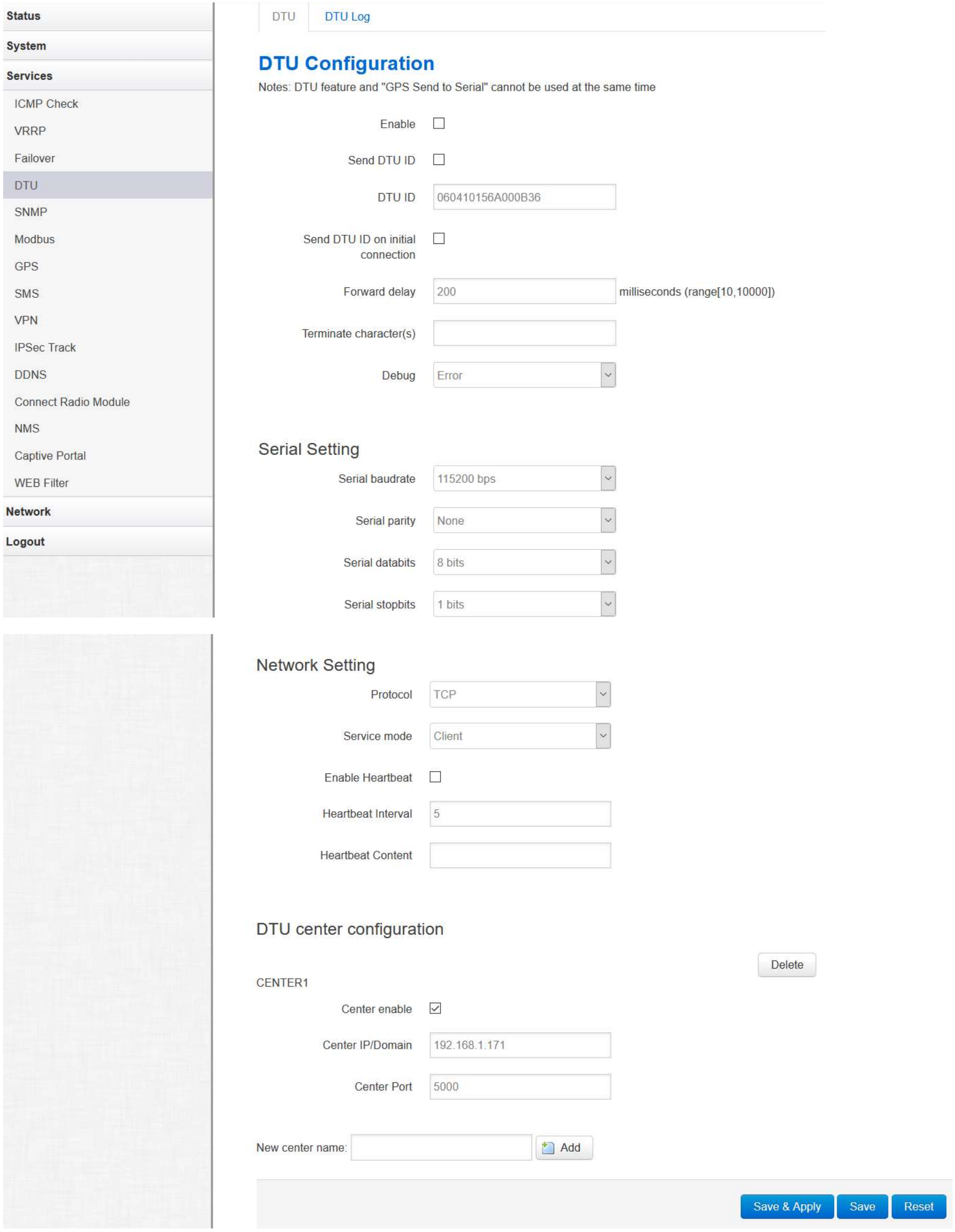
Cell Standby: Data disconnect

SMS Alarm: No alarm

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

3.5.4 DTU

Notes:
1) This feature is for the CM685VX 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.



DTU Configuration

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

Enable □

Send DTU ID □

DTU ID 060410156A000B36

Send DTU ID on initial connection □

Forward delay 200 milliseconds (range[10,10000])

Terminate character(s)

Debug Error

Serial Setting

Serial baudrate 115200 bps

Serial parity None

Serial databits 8 bits

Serial stopbits 1 bits

Network Setting

Protocol TCP

Service mode Client

Enable Heartbeat □

Heartbeat Interval 5

Heartbeat Content

DTU center configuration

CENTER1

Center enable ☑

Center IP/Domain 192.168.1.171

Center Port 5000

New center name:

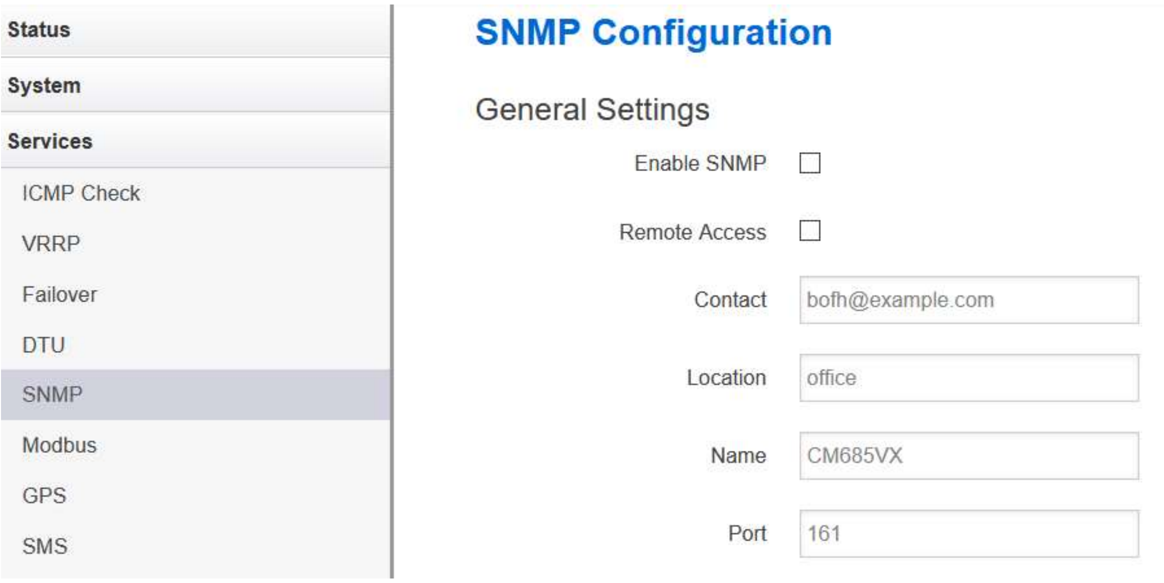
- **Enable**: Enable DTU feature.
- **Send DTU ID**: Send DTU ID at the front of the packet.
- **DTU ID**: The default DTU ID is the SN of the router. You can change it if required.

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

- **Protocol:** Both TCP and UDP are supported.
- **Service mode:** Client and Server are supported.
- **Enable heartbeat:** The heartbeat is used to maintain the “keep alive” connection.
- **Heartbeat interval:** The time between two heartbeat packets.
- **Heartbeat content:** The content of heartbeat packets.
- **DTU center Configuration:** The DTU centre is the DTU server. Simply input the centre name and click the button “Add”.
- **If the centre is not needed, you can delete it by clicking the “Delete” button or set it to ‘Disabled’.**

Notes:
The maximum number of DTU centres is 32.

3.5.5 SNMP



SNMP Configuration

General Settings

Enable SNMP □

Remote Access □

Contact bofh@example.com

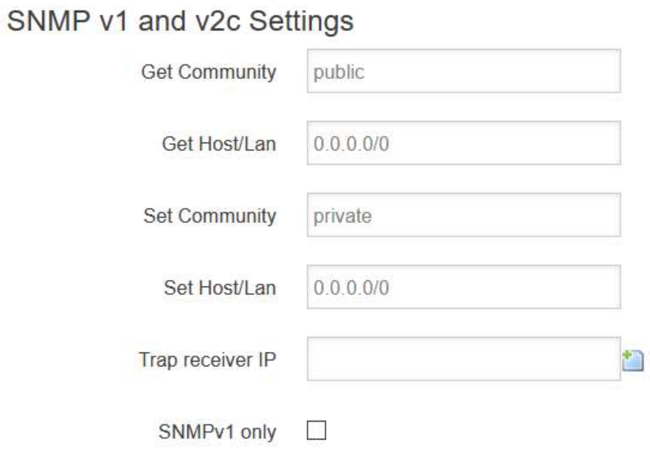
Location office

Name CM685VX

Port 161

- **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: public

Get Host/Lan: 0.0.0.0/0

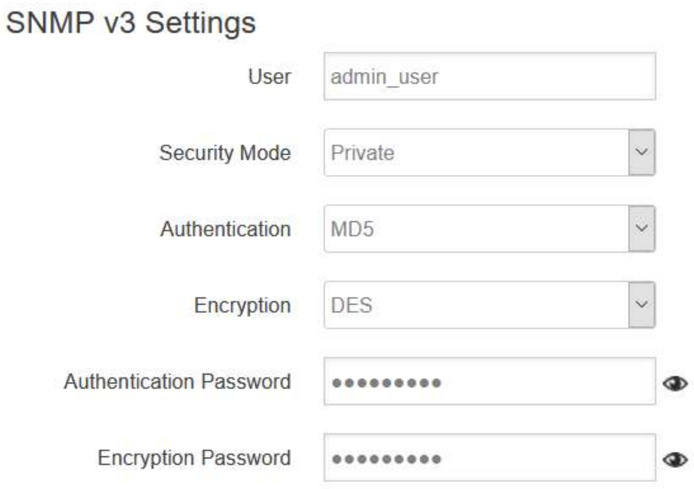
Set Community: private

Set Host/Lan: 0.0.0.0/0

Trap receiver IP:

SNMPv1 only ☐

- **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: admin_user

Security Mode: Private

Authentication: MD5

Encryption: DES

Authentication Password: •••••••••

Encryption Password: •••••••••

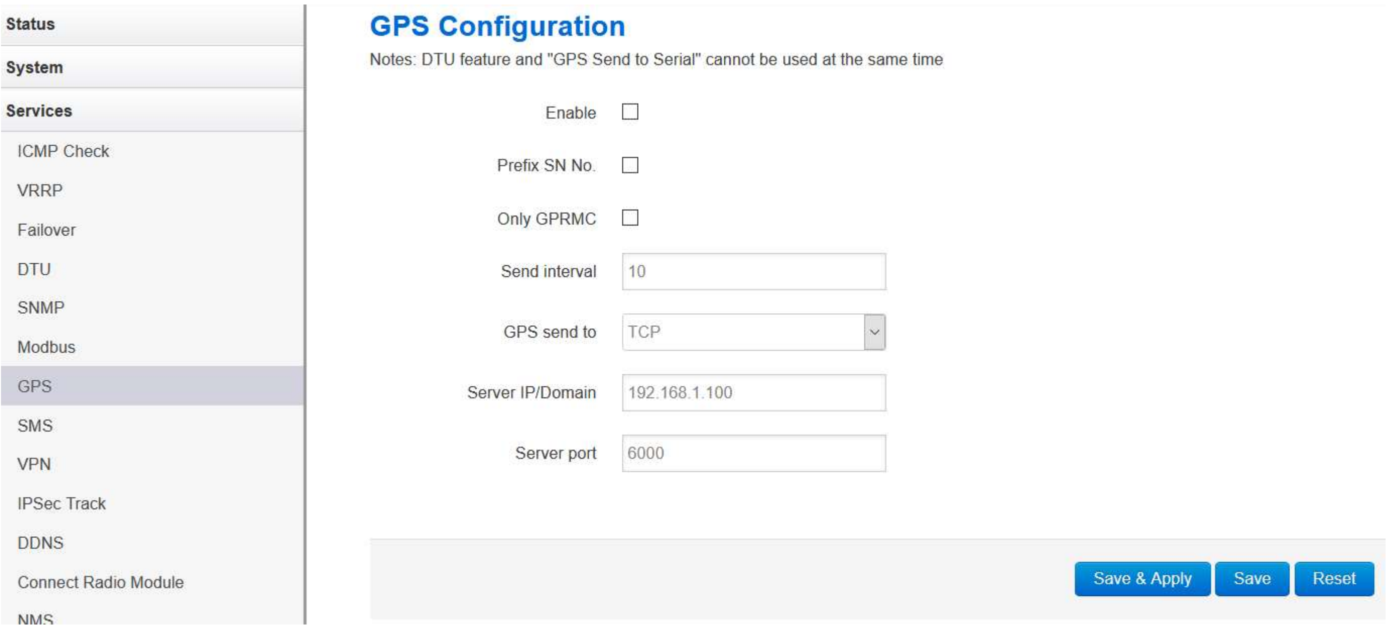
- **User**: SNMPv3 username
- **Security Mode**: Three options: None, Private and Authorised. If it is set to 'None', there is no

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 CM685VX-G model)



GPS Configuration

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

Enable ☐

Prefix SN No. ☐

Only GPRMC ☐

Send interval: 10

GPS send to: TCP

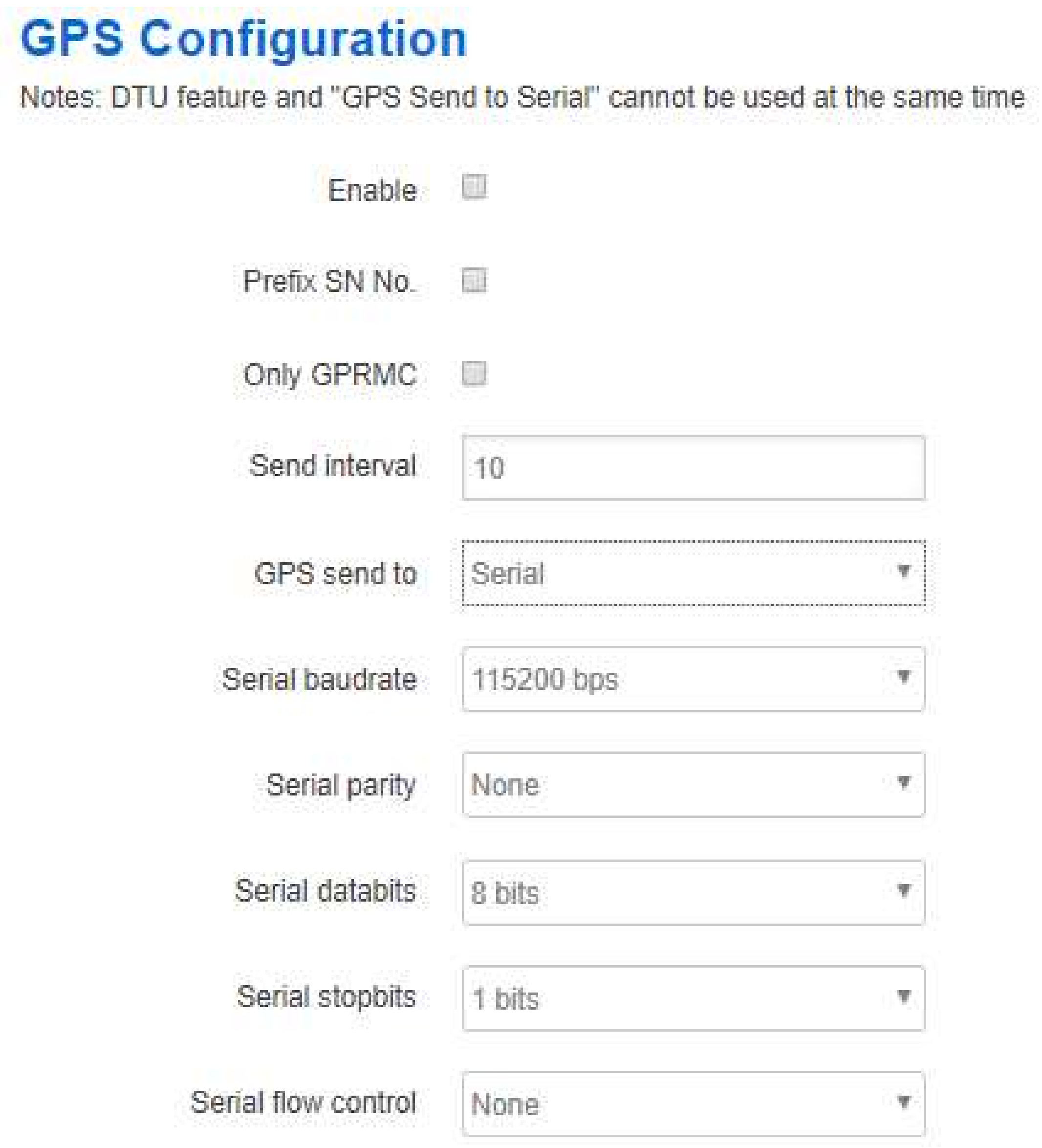
Server IP/Domain: 192.168.1.100

Server port: 6000

- **Enable**: Check this button to enable GPS.
- **Prefix SN No:** If checked, it will add the router's SN to the data packet.
- **Only GPRMC:** If checked, it will only send GPRMC data info (Longitude Latitude altitude)
- **Send interval:** Set the frequency of GPS data packets being sent.
- **GPS Send to**: Choose between "Serial" and "TCP/IP". The router will only receive the GPS signal and will not process it. It will send this GPS signal to your GPS processor devices or servers. If the GPS processor device is connected to the CM685VX Router via a Serial Port, please choose "Serial".
  If the GPS processor device is a remote server, please choose "Serial".

GPS to TCP/UDP Settings

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



GPS Configuration

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

Enable □

Prefix SN No. □

Only GPRMC □

Send interval: 10

GPS send to: Serial

Serial baudrate: 115200 bps

Serial parity: None

Serial databits: 8 bits

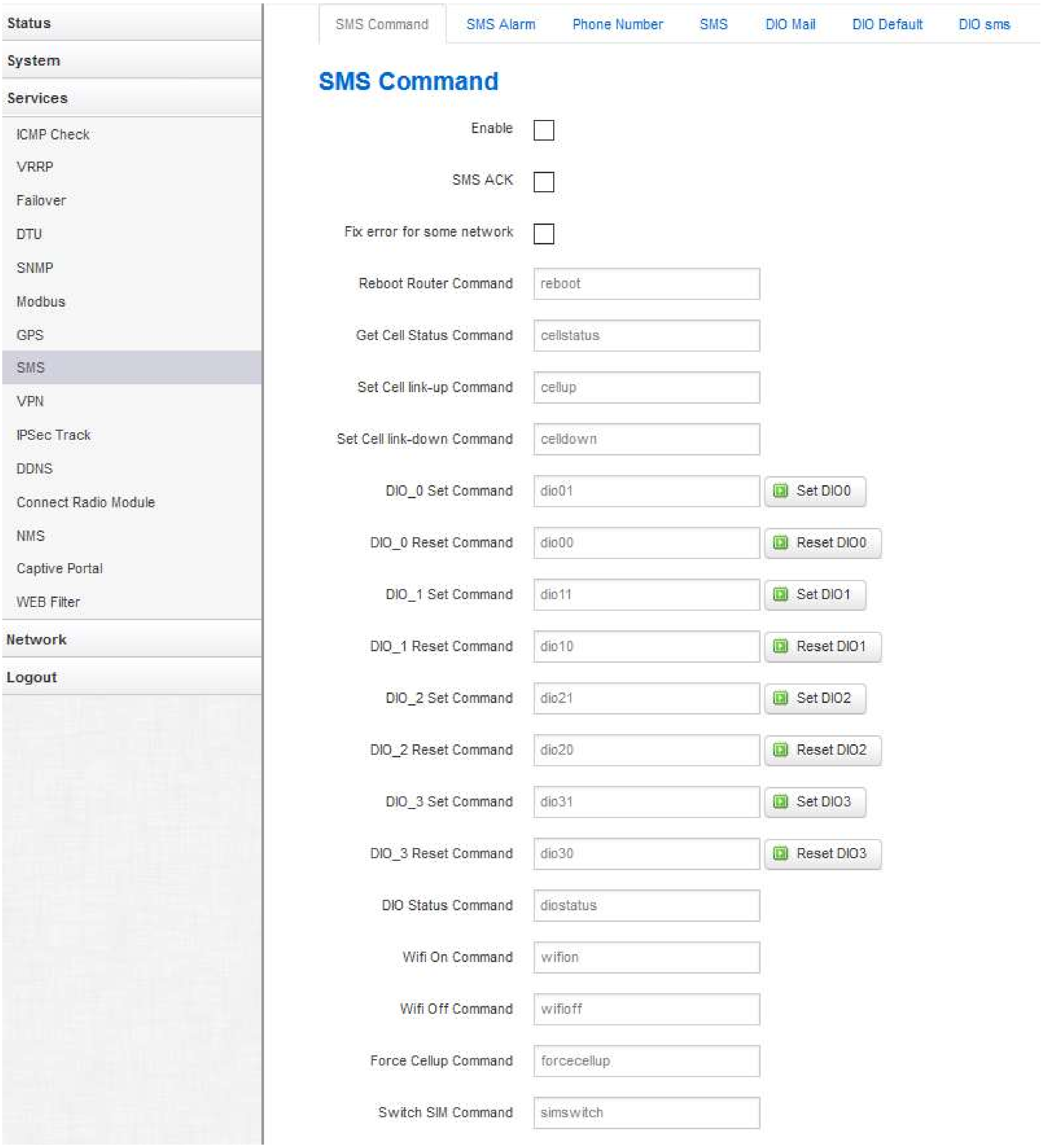
Serial stopbits: 1 bits

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**



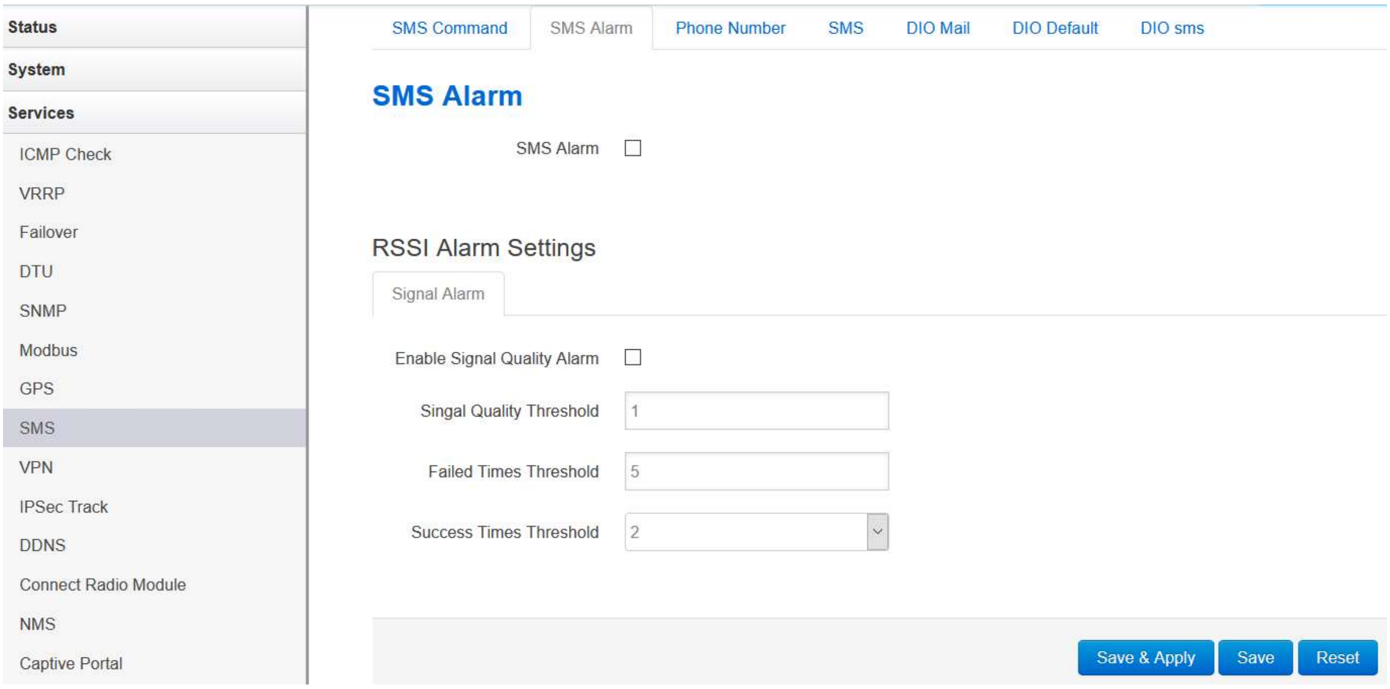
SMS Command

Enable	□	
SMS ACK	□	
Fix error for some network	□	
Reboot Router Command	reboot	
Get Cell Status Command	cellstatus	
Set Cell link-up Command	cellup	
Set Cell link-down Command	celldown	
DIO_0 Set Command	dio01	Set DIO0
DIO_0 Reset Command	dio00	Reset DIO0
DIO_1 Set Command	dio11	Set DIO1
DIO_1 Reset Command	dio10	Reset DIO1
DIO_2 Set Command	dio21	Set DIO2
DIO_2 Reset Command	dio20	Reset DIO2
DIO_3 Set Command	dio31	Set DIO3
DIO_3 Reset Command	dio30	Reset DIO3
DIO Status Command	diostatus	
Wifi On Command	wifion	
Wifi Off Command	wifioff	
Force Cellup Command	forcecellup	
Switch SIM Command	simswitch	

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

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

➢ SMS alarm



SMS Alarm

SMS Alarm □

RSSI Alarm Settings

Signal Alarm

Enable Signal Quality Alarm □

Singal Quality Threshold: 1

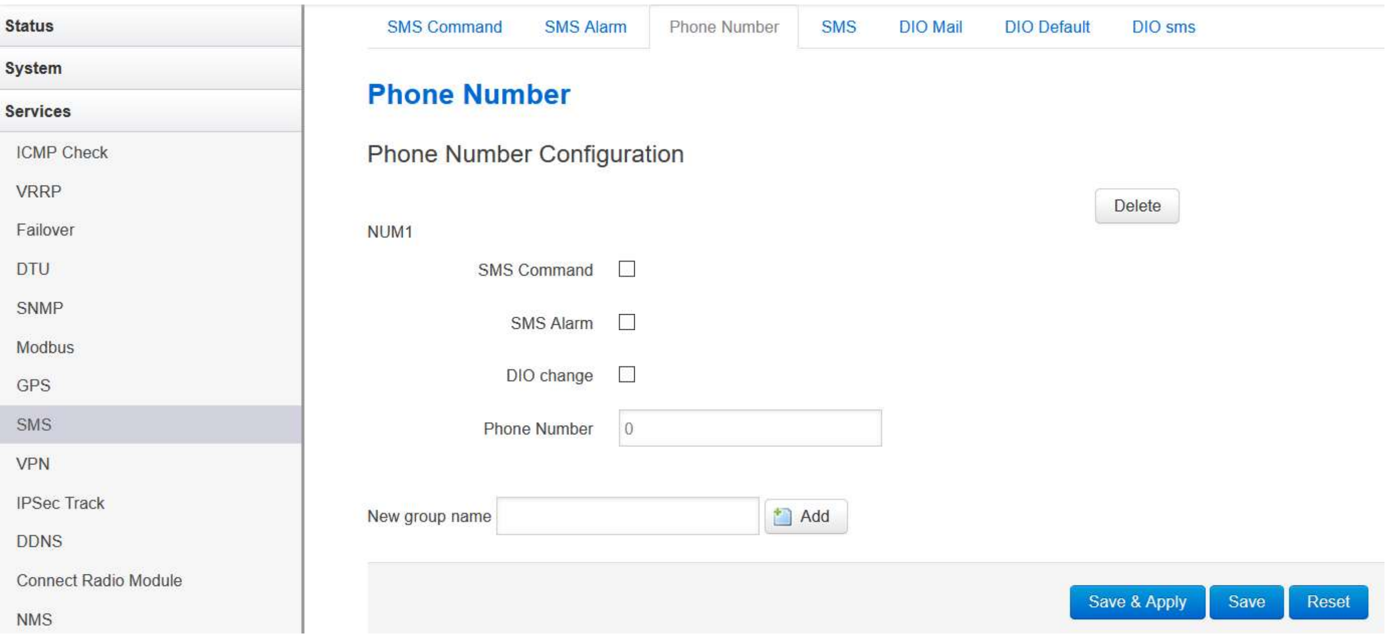
Failed Times Threshold: 5

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



Phone Number

Phone Number Configuration

NUM1

SMS Command □

SMS Alarm □

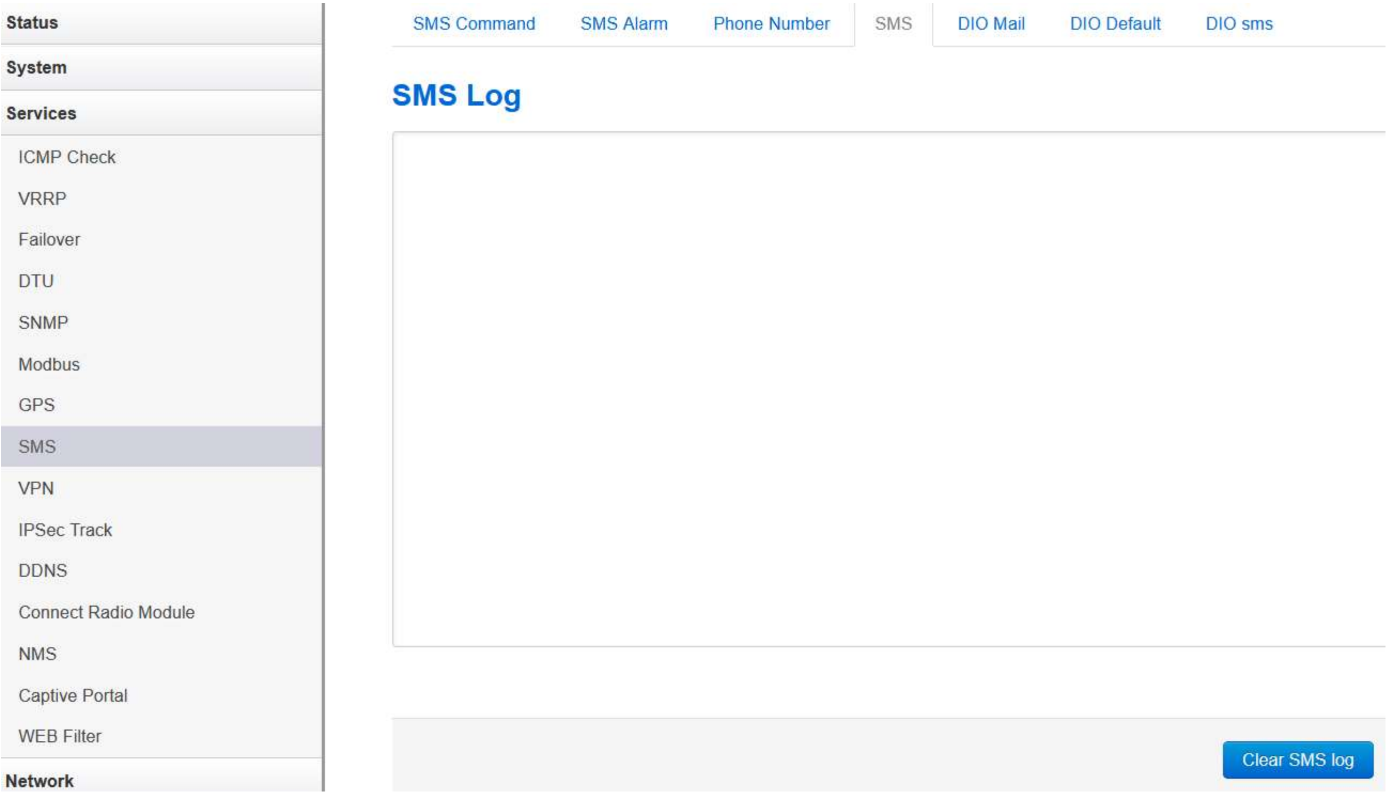
DIO change □

Phone Number 0

New group name

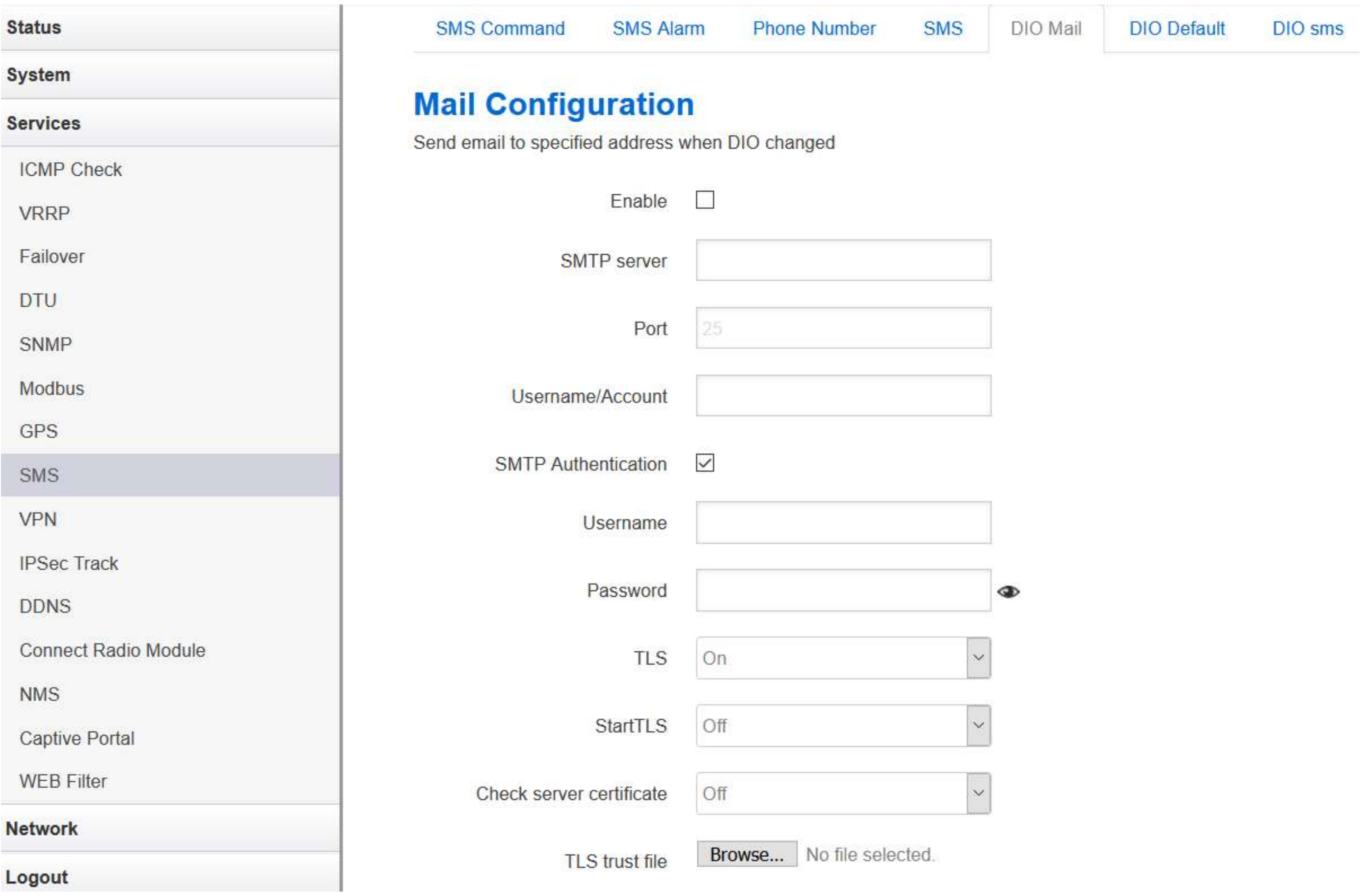
- **Add Phone number**: Input a name and click the button “Add” to add a new Phone number.
- **Delete Phone number**: Click the button “Delete”.
- **SMS command**: Enable the SMS command feature on this phone number.
- **SMS alarm**: This phone number can receive SMS alarms.

- **SMS Log**



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

- **DIO Mail**



Mail Configuration

Send email to specified address when DIO changed

Enable □

SMTP server

Port 25

Username/Account

SMTP Authentication ☑

Username

Password

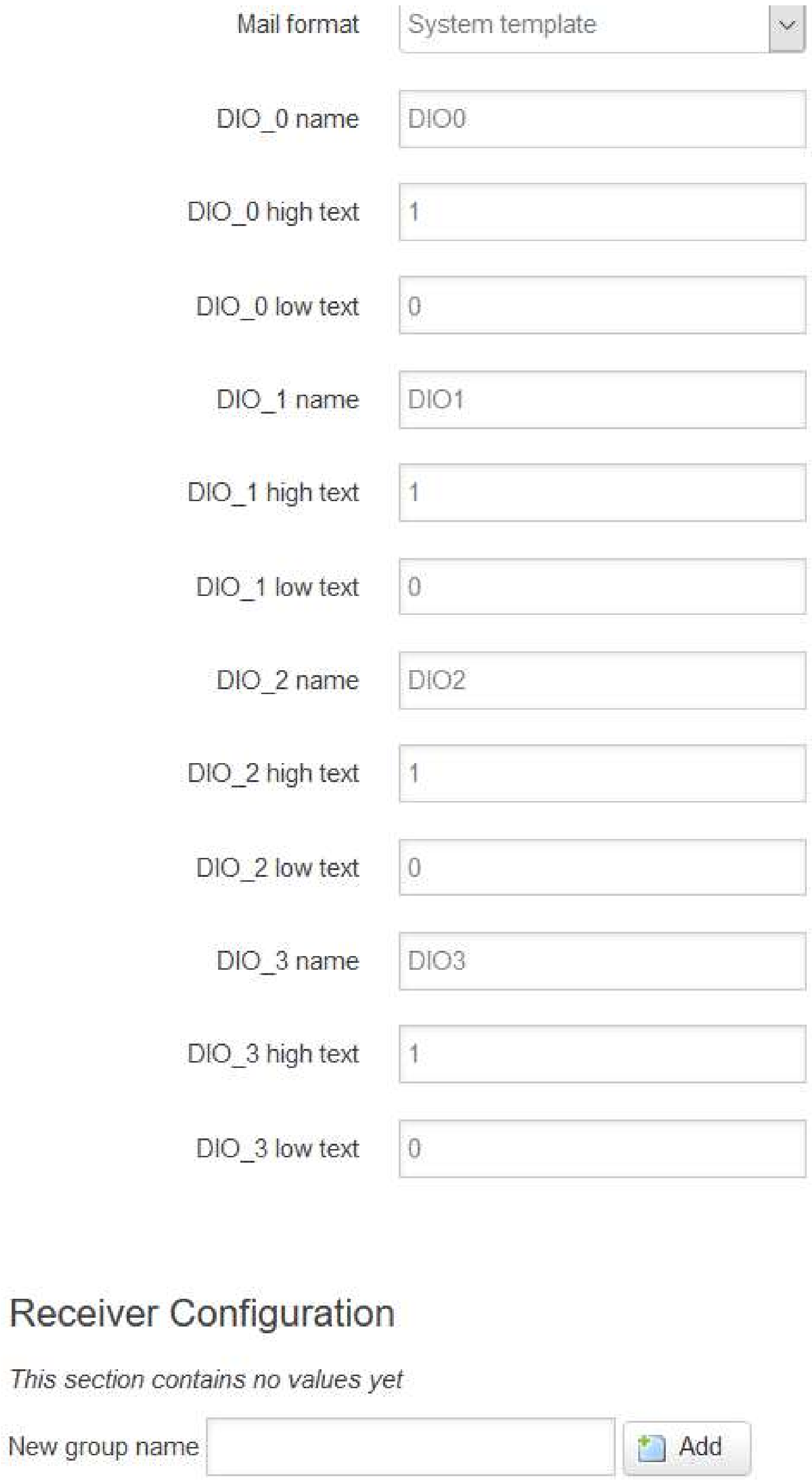
TLS On

StartTLS Off

Check server certificate Off

TLS trust file No file selected.

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



Mail format	System template
DIO_0 name	DIO0
DIO_0 high text	1
DIO_0 low text	0
DIO_1 name	DIO1
DIO_1 high text	1
DIO_1 low text	0
DIO_2 name	DIO2
DIO_2 high text	1
DIO_2 low text	0
DIO_3 name	DIO3
DIO_3 high text	1
DIO_3 low text	0

Receiver Configuration

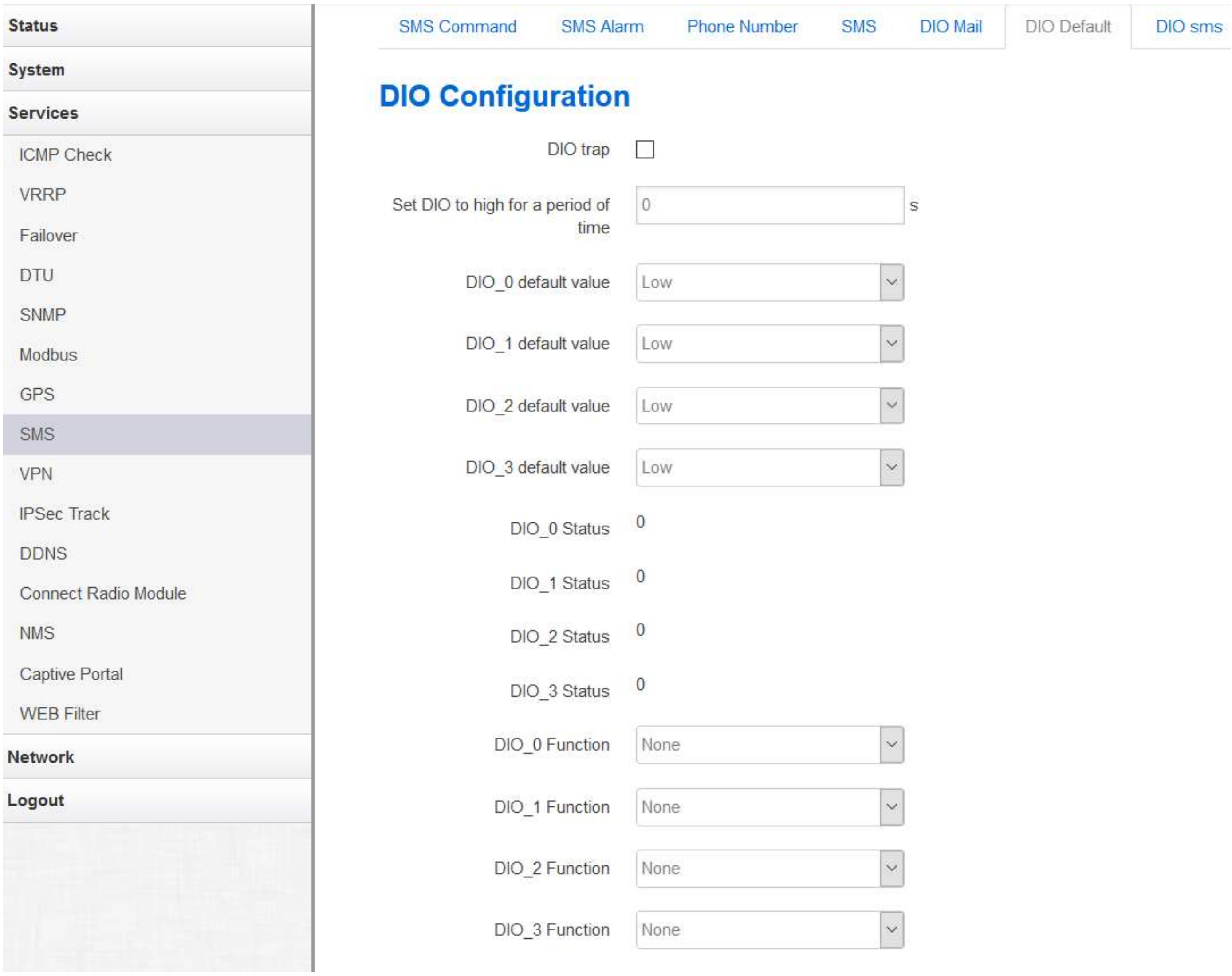
This section contains no values yet

New group name

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

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

➢ DIO Default



DIO Configuration

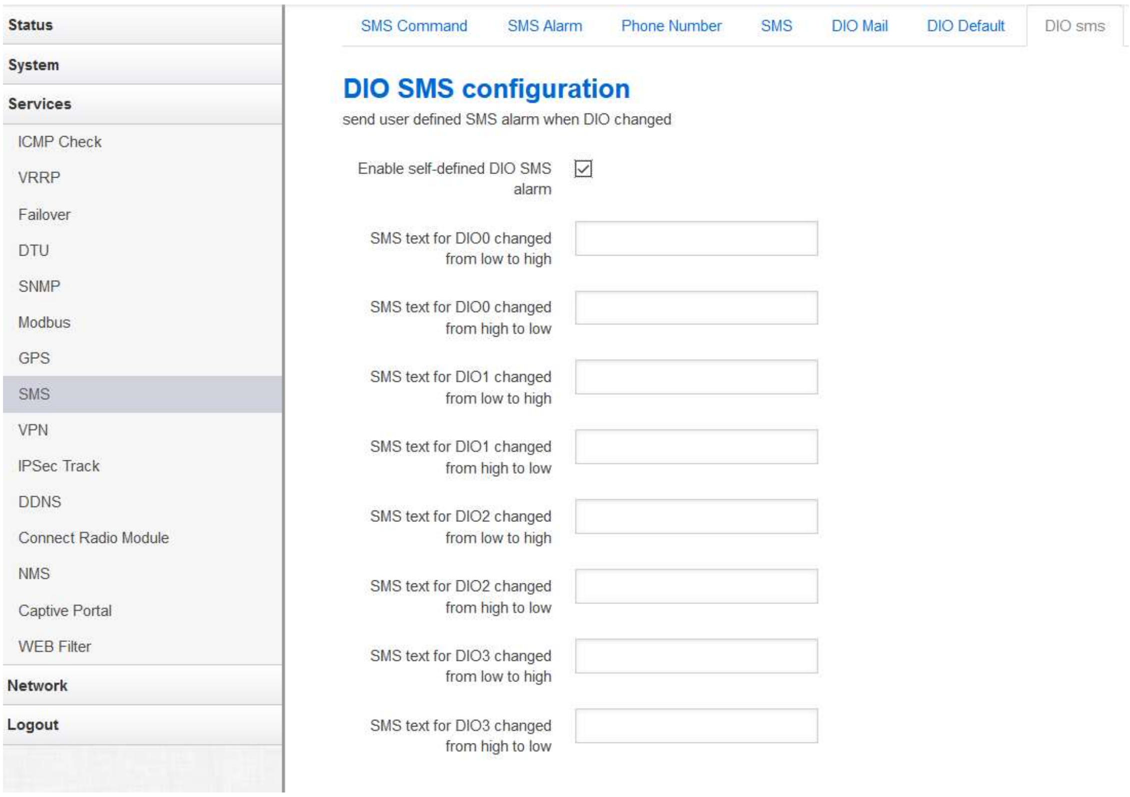
DIO trap	□
Set DIO to high for a period of time	0 s
DIO_0 default value	Low
DIO_1 default value	Low
DIO_2 default value	Low
DIO_3 default value	Low
DIO_0 Status	0
DIO_1 Status	0
DIO_2 Status	0
DIO_3 Status	0
DIO_0 Function	None
DIO_1 Function	None
DIO_2 Function	None
DIO_3 Function	None

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

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

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

➢ DIO SMS



DIO SMS configuration

send user defined SMS alarm when DIO changed

Enable self-defined DIO SMS alarm ☑

SMS text for DIO0 changed from low to high

SMS text for DIO0 changed from high to low

SMS text for DIO1 changed from low to high

SMS text for DIO1 changed from high to low

SMS text for DIO2 changed from low to high

SMS text for DIO2 changed from high to low

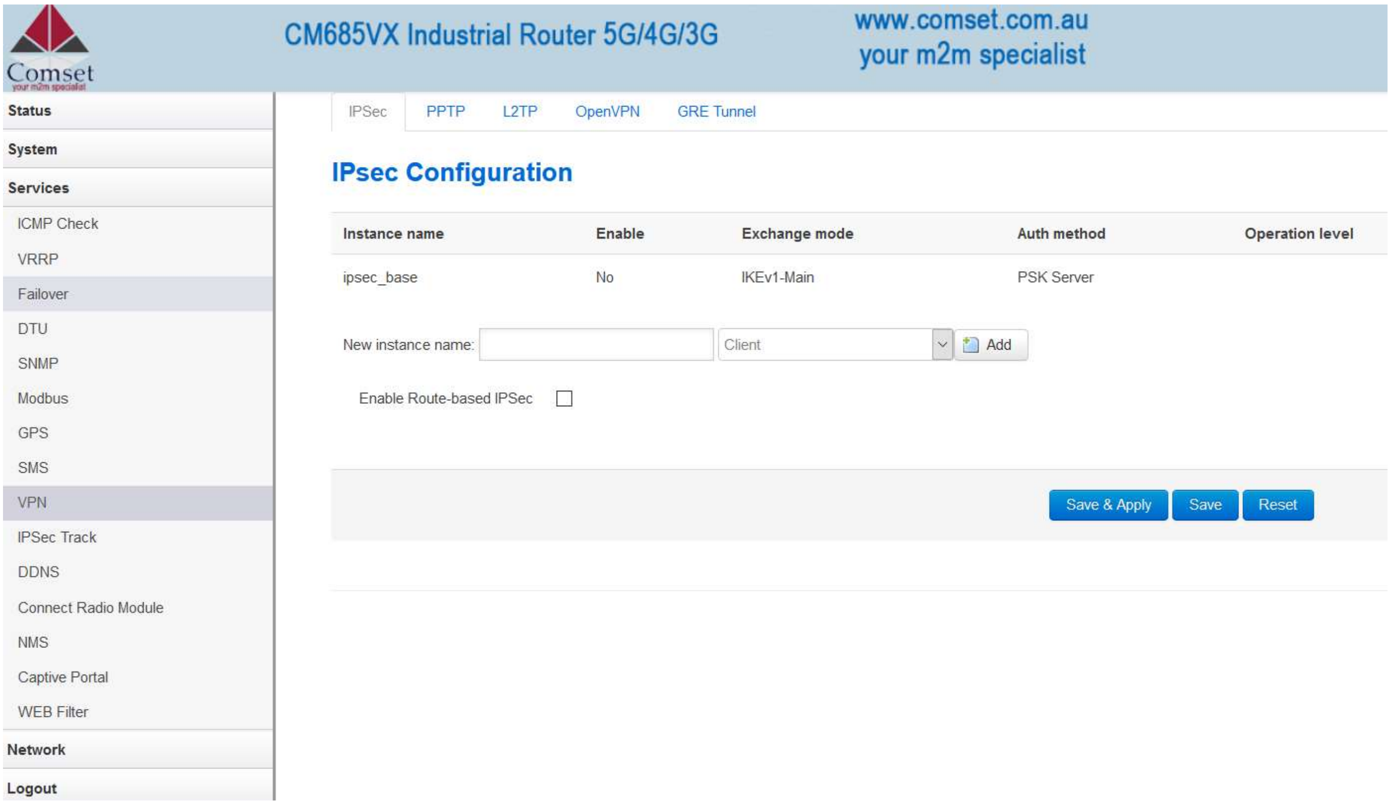
SMS text for DIO3 changed from low to high

SMS text for DIO3 changed from high to low

When the DIO value changes, it will send an SMS text accordingly. You must enable “DIO change”
On the “Phone Number” page. If the user-defined text is empty, it will send the system default SMS text. The default format is SN:[86000000000], [DIOx] is changed from [value1] to [value0].

3.5.8 VPN

3.5.8.1 IPSEC



IPsec Configuration

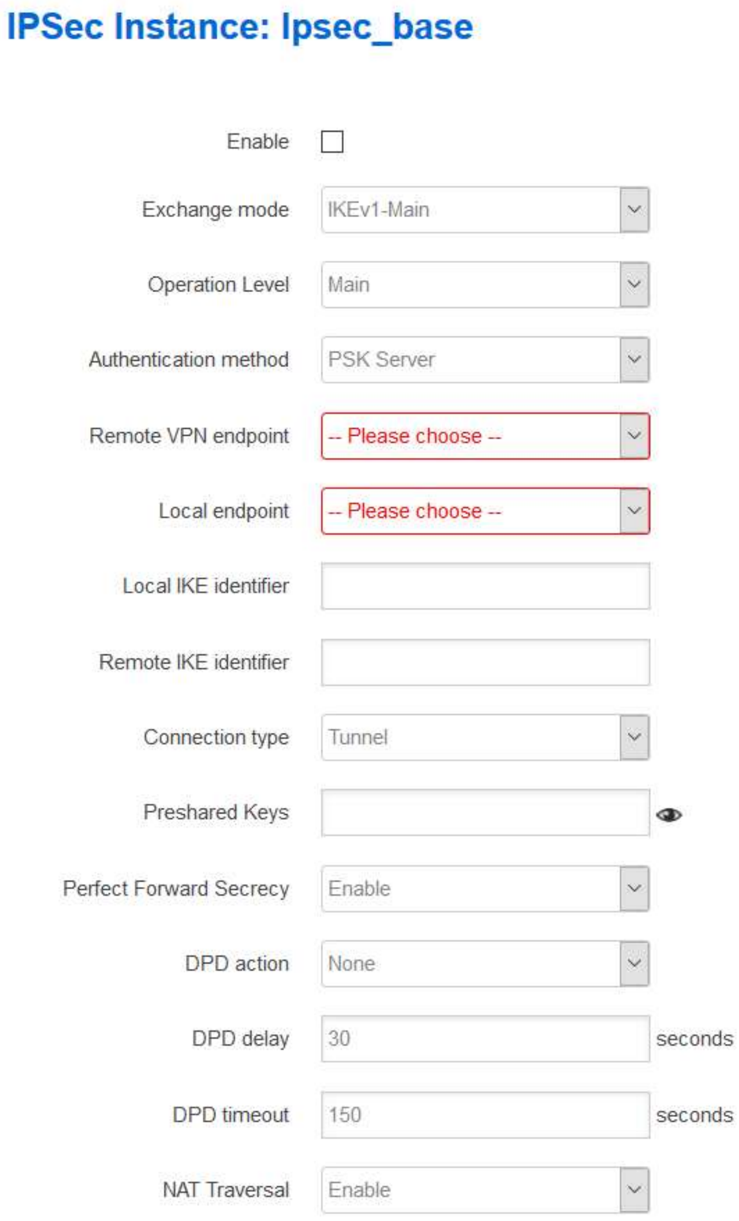
Instance name	Enable	Exchange mode	Auth method	Operation level
ipsec_base	No	IKEv1-Main	PSK Server	

New instance name: Client

Enable Route-based IPSec ☐

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

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

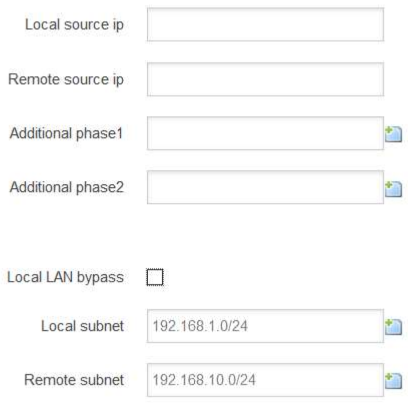


IPSec Instance: Ipsec_base

Enable	□
Exchange mode	IKEv1-Main
Operation Level	Main
Authentication method	PSK Server
Remote VPN endpoint	-- Please choose --
Local endpoint	-- Please choose --
Local IKE identifier	
Remote IKE identifier	
Connection type	Tunnel
Preshared Keys	
Perfect Forward Secrecy	Enable
DPD action	None
DPD delay	30 seconds
DPD timeout	150 seconds
NAT Traversal	Enable

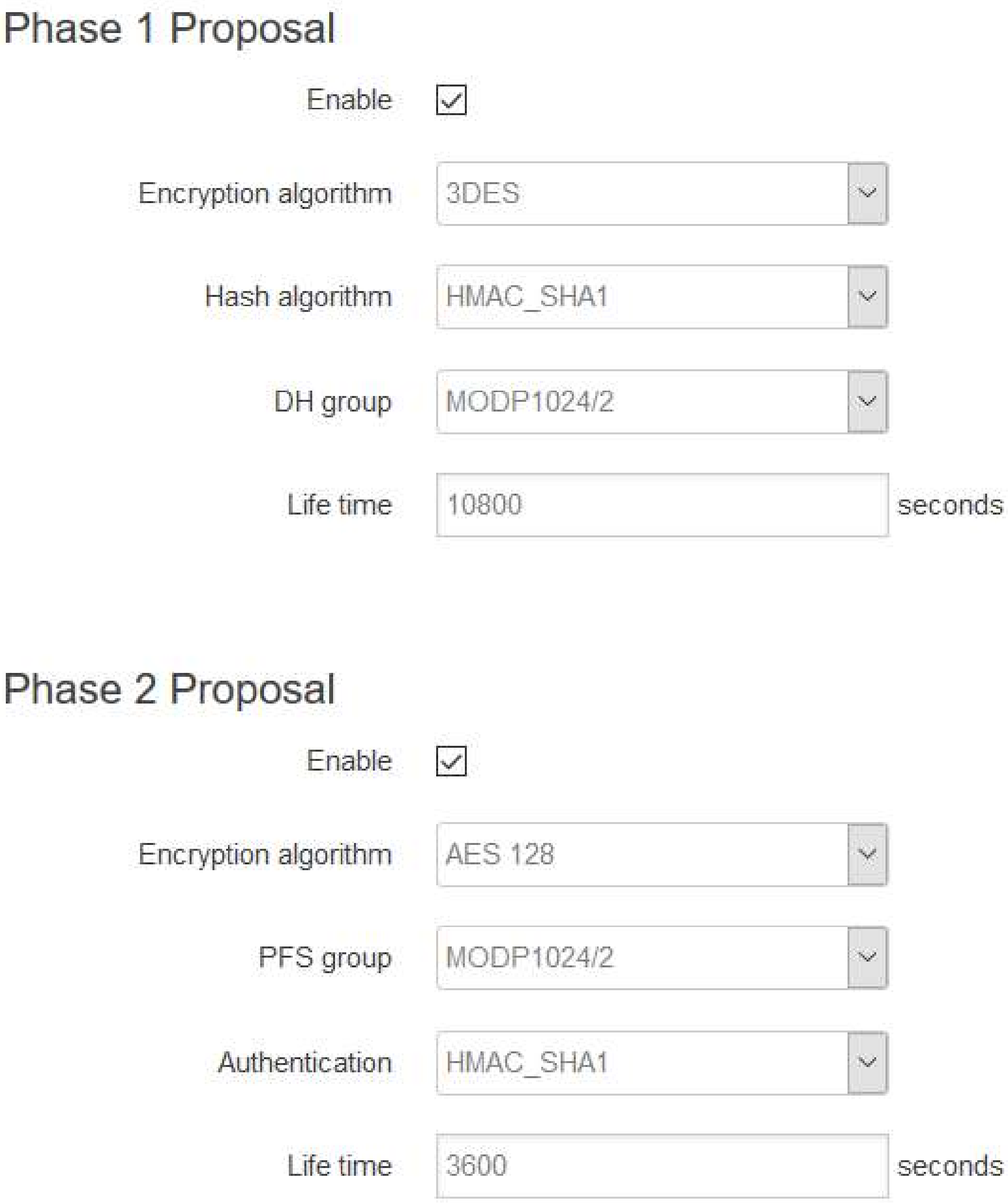
- **Enable**: Enable IPSEC feature
- **Exchange mode**: IKEv1-Main, IKEv1-Aggressive and IKEv2-Main modes are supported.
- **Operation level**: This is for IPSec backup. One instance is “Main”, and another instance is “Backup”. If the “Main” instance is down, it will switch to the “Backup” instance.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

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



Local source ip	
Remote source ip	
Additional phase1	
Additional phase2	
Local LAN bypass	□
Local subnet	192.168.1.0/24
Remote subnet	192.168.10.0/24

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



Phase 1 Proposal

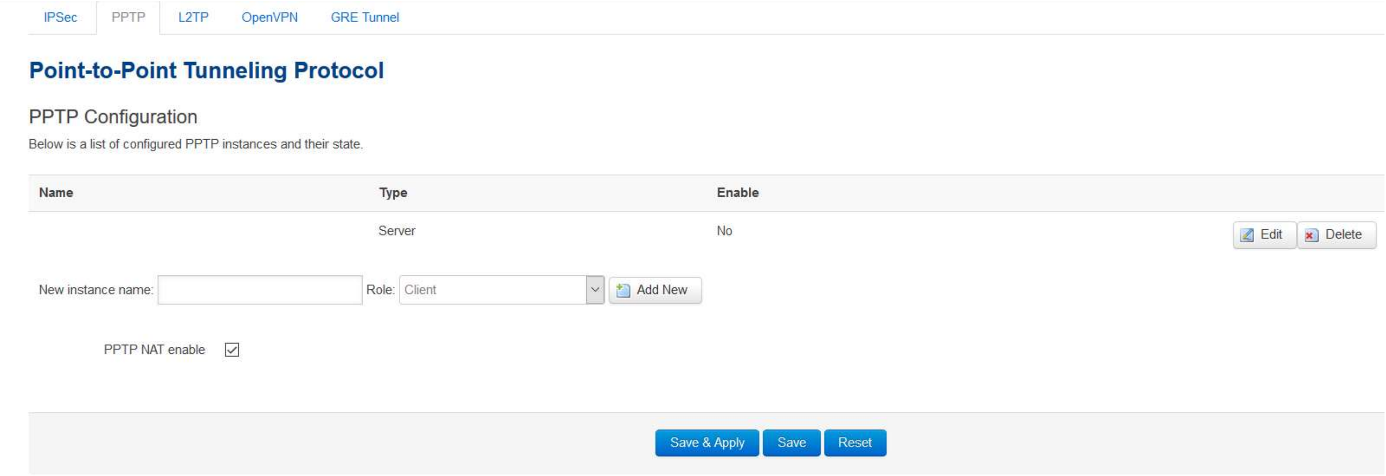
Enable	☑
Encryption algorithm	3DES
Hash algorithm	HMAC_SHA1
DH group	MODP1024/2
Life time	10800 seconds

Phase 2 Proposal

Enable	☑
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

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

Name	Type	Enable	
	Server	No	Edit Delete

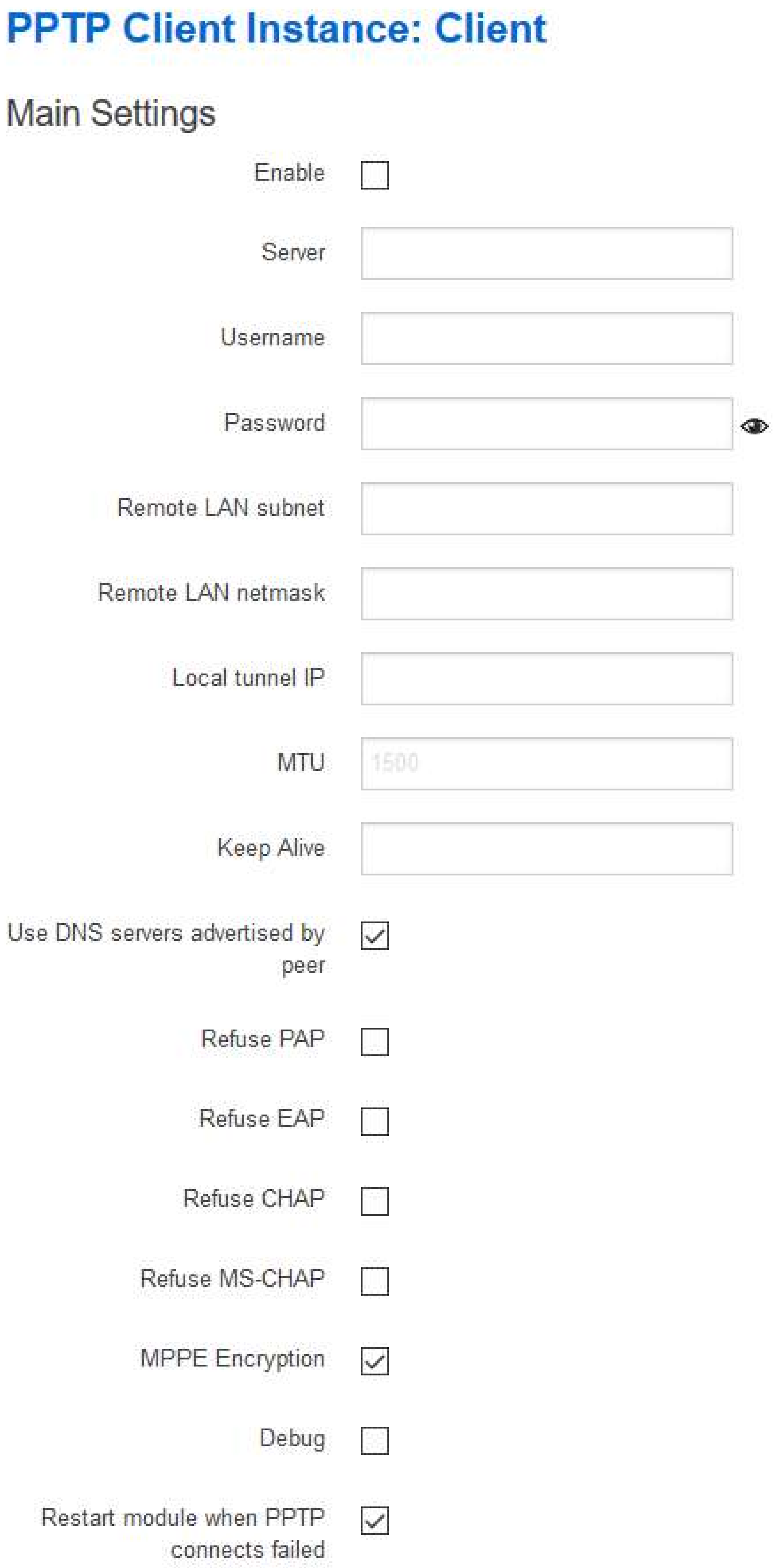
New instance name: Role: Client

PPTP NAT enable ☑

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

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

➢ **PPTP Client configuration**



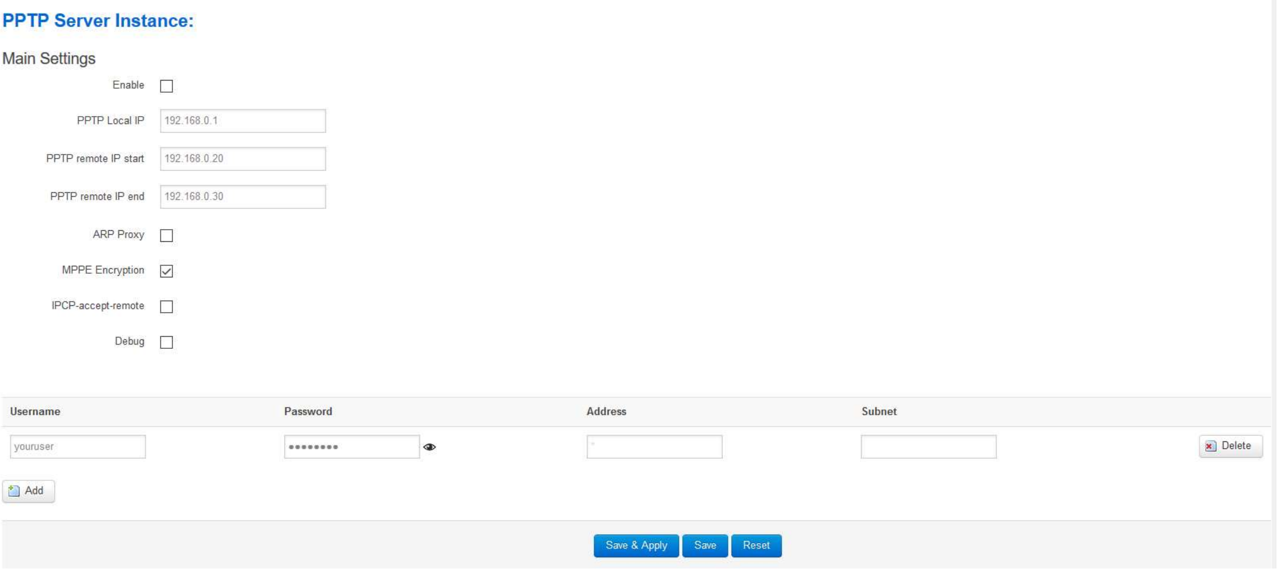
PPTP Client Instance: Client

Main Settings

Enable	☐
Server	
Username	
Password	
Remote LAN subnet	
Remote LAN netmask	
Local tunnel IP	
MTU	1500
Keep Alive	
Use DNS servers advertised by peer	☑
Refuse PAP	☐
Refuse EAP	☐
Refuse CHAP	☐
Refuse MS-CHAP	☐
MPPE Encryption	☑
Debug	☐
Restart module when PPTP connects failed	☑

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

➢ PPTP Server Configuration



PPTP Server Instance:

Main Settings

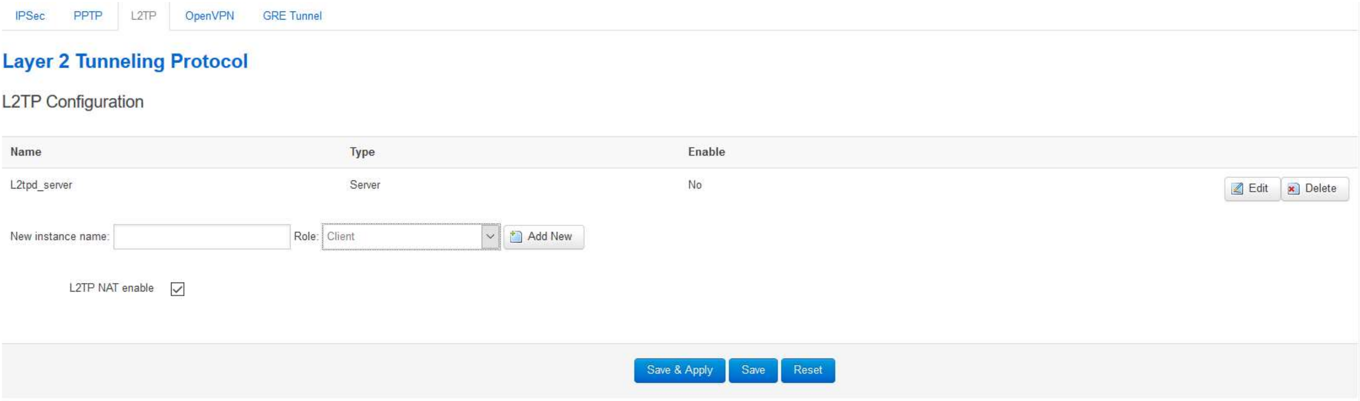
Enable	□
PPTP Local IP	192.168.0.1
PPTP remote IP start	192.168.0.20
PPTP remote IP end	192.168.0.30
ARP Proxy	□
MPPE Encryption	☑
IPCP-accept-remote	□
Debug	□

Username	Password	Address	Subnet	
youruser	••••••••			Delete

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

3.5.8.3 L2TP

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



Layer 2 Tunneling Protocol

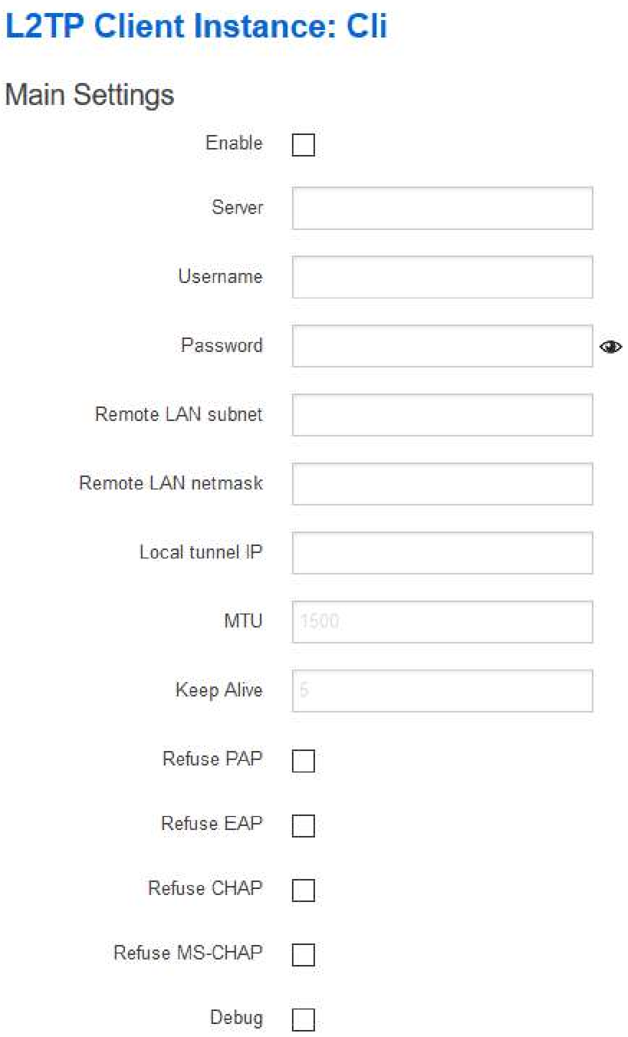
L2TP Configuration

Name	Type	Enable	
L2tpd_server	Server	No	Edit Delete

New instance name: Role: Client

L2TP NAT enable ☑

- **L2TP Client configuration**



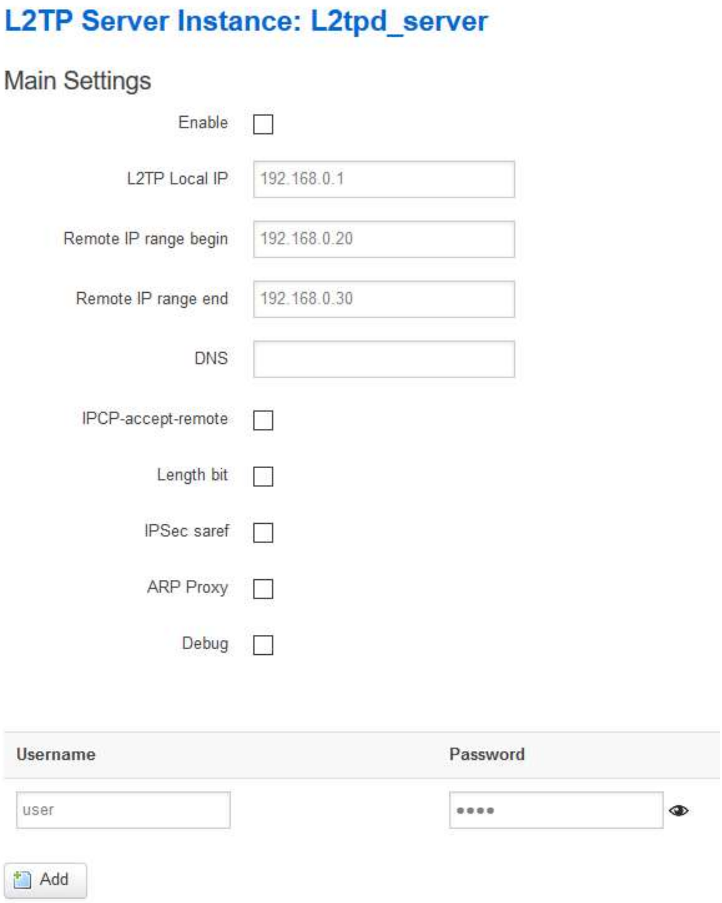
L2TP Client Instance: Cli

Main Settings

Enable	☐
Server	
Username	
Password	
Remote LAN subnet	
Remote LAN netmask	
Local tunnel IP	
MTU	1500
Keep Alive	5
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.
- **Remote LAN subnet**: This is the remote subnet which can be accessed via L2TP tunnel, such as 192.168.10.0.
- **Remote LAN netmask**: This is the netmask for the remote LAN subnet, such as 255.255.255.0.
- **MTU**: Maximum Transmission Unit.
- **Keep Alive**: Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.
- **Checkup Interval**: Number of seconds to pass before checking if the interface is not up since the last setup attempt and retry the connection otherwise. Set it to a value sufficient for a successful L2TP connection for you. It is mainly for the case that netifd sent the connect request yet xl2tpd failed to complete it without the notice of netifd.
- **Debug**: Adds L2TP verbose log into the system log.

➢ L2TP Server configuration



L2TP Server Instance: L2tpd_server

Main Settings

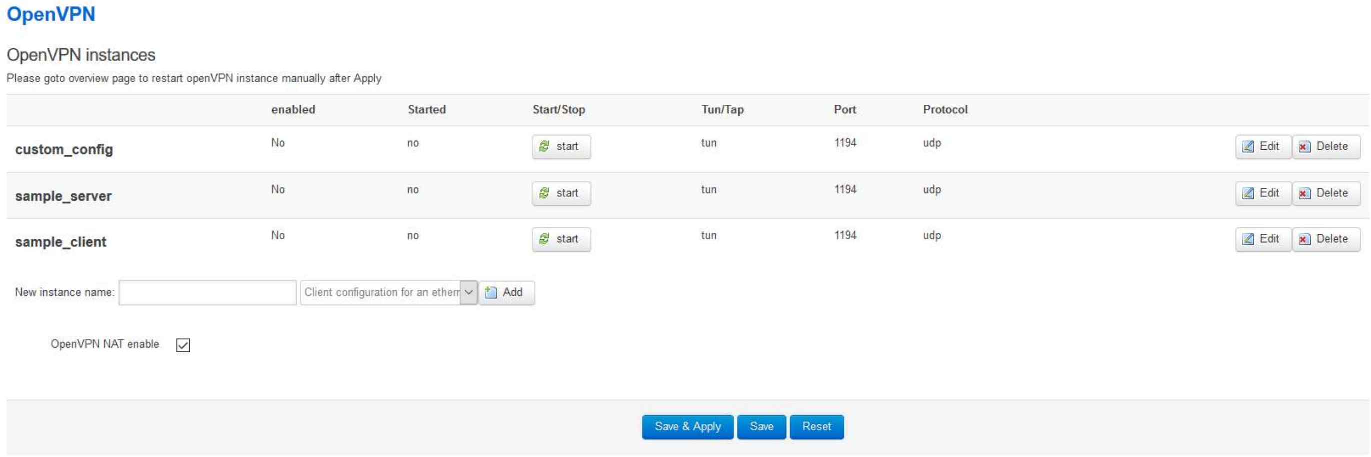
Enable	□
L2TP Local IP	192.168.0.1
Remote IP range begin	192.168.0.20
Remote IP range end	192.168.0.30
DNS	
IPCP-accept-remote	□
Length bit	□
IPSec saref	□
ARP Proxy	□
Debug	□

Username	Password
user	••••

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

3.5.8.4 OpenVPN

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



OpenVPN

OpenVPN instances

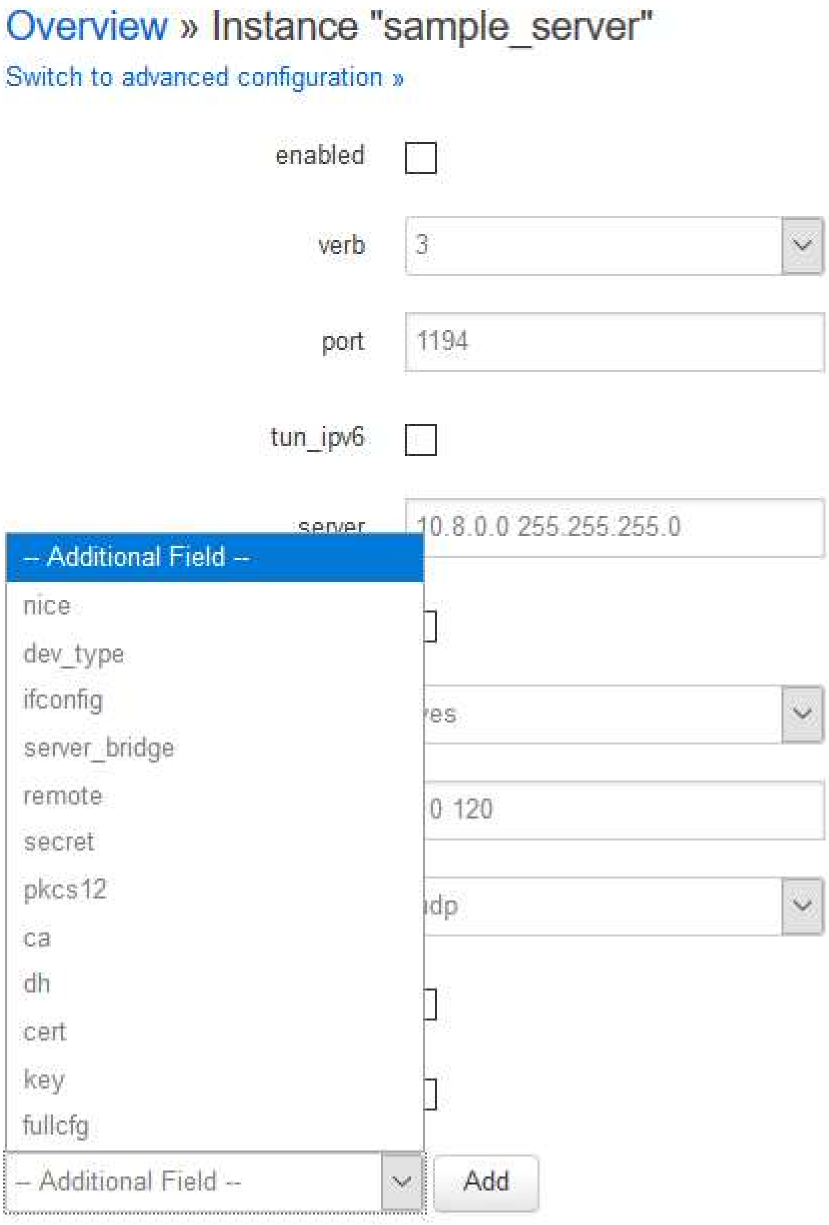
Please goto overview page to restart openVPN instance manually after Apply

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

New instance name: Client configuration for an ethern

OpenVPN NAT enable ☑

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



Overview » Instance "sample_server"

Switch to advanced configuration »

enabled □

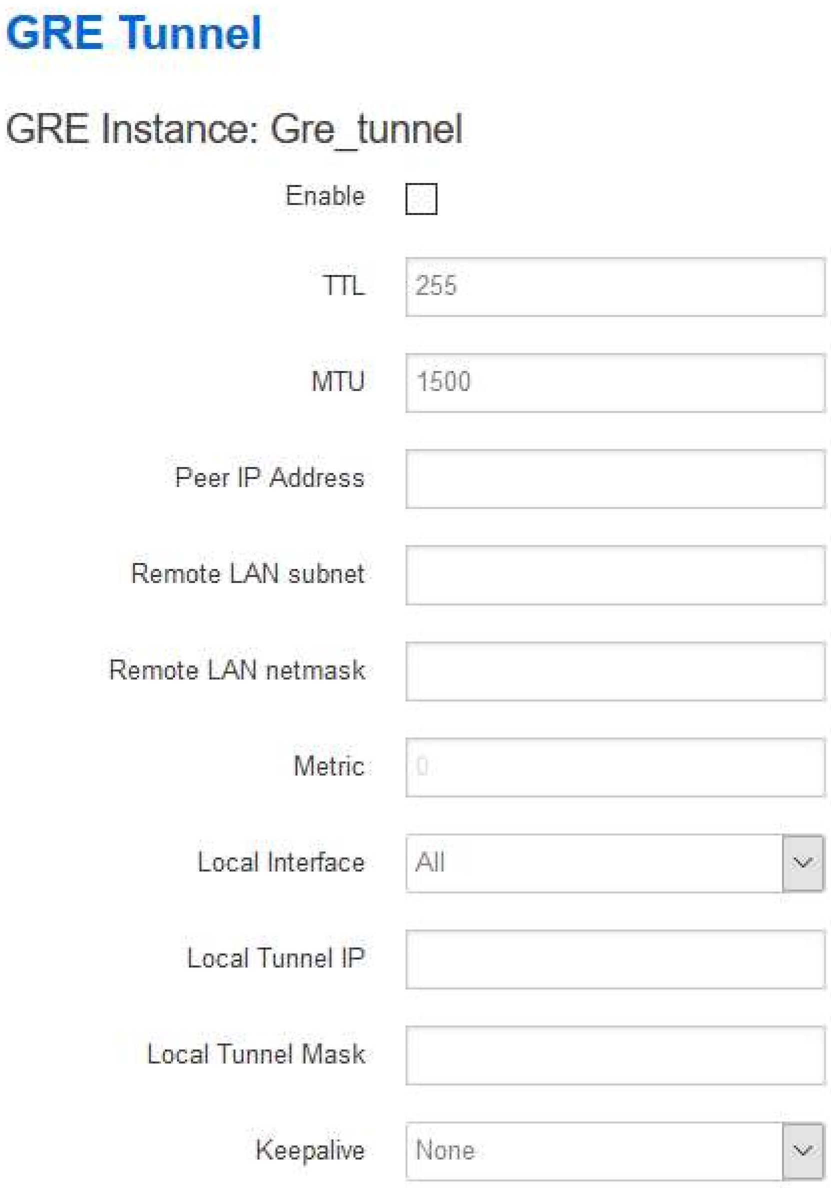
verb 3

port 1194

tun_ipv6 □

server 10.8.0.0 255.255.255.0

3.5.8.5 GRE tunnel



GRE Tunnel

GRE Instance: Gre_tunnel

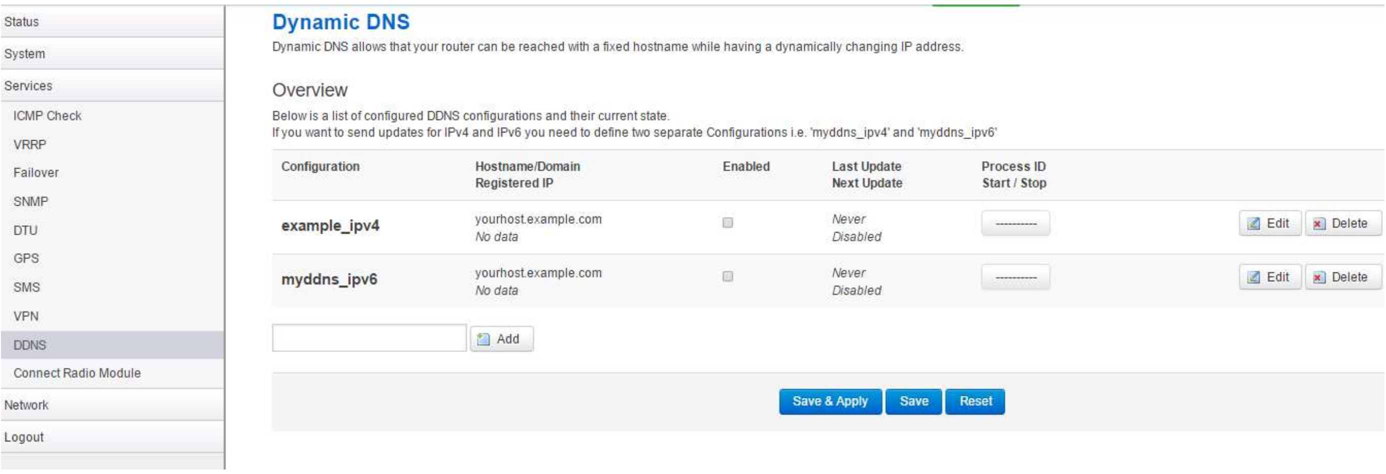
Enable	□
TTL	255
MTU	1500
Peer IP Address	
Remote LAN subnet	
Remote LAN netmask	
Metric	0
Local Interface	All
Local Tunnel IP	
Local Tunnel Mask	
Keepalive	None

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

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

3.5.9 DDNS

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



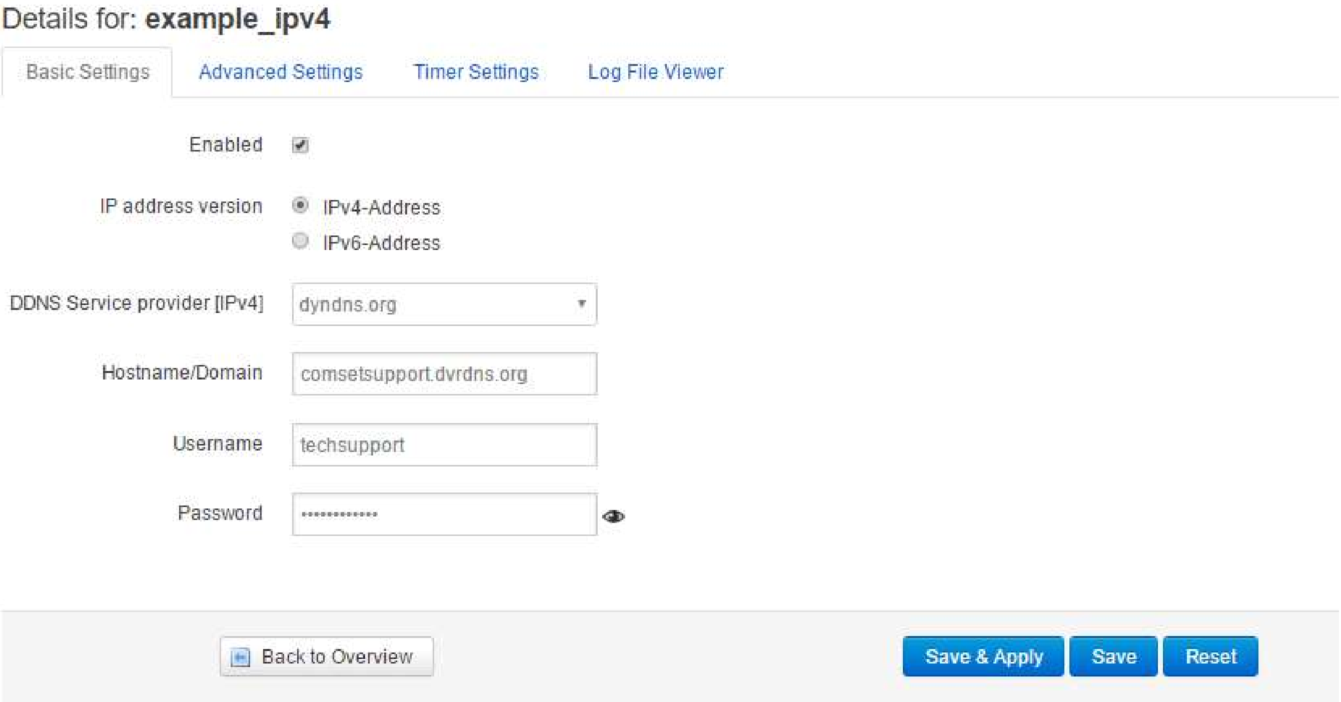
Dynamic DNS

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

Overview

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

Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
example_ipv4	yourhost.example.com *No data*	□	*Never* *Disabled*	----------	Edit Delete
myddns_ipv6	yourhost.example.com *No data*	□	*Never* *Disabled*	----------	Edit Delete



Details for: **example_ipv4**

Enabled ☑

IP address version ● IPv4-Address ○ IPv6-Address

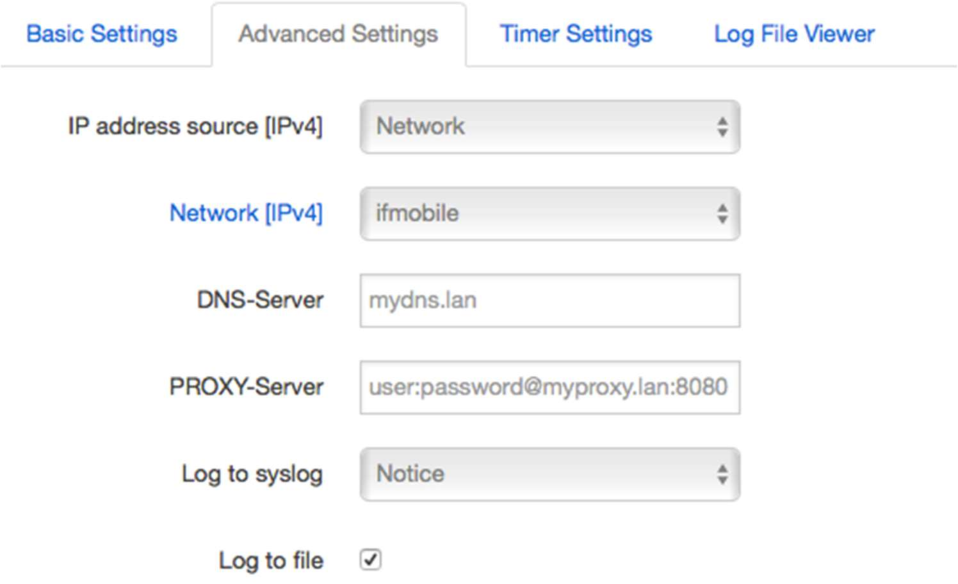
DDNS Service provider [IPv4]: dyndns.org

Hostname/Domain: comsetsupport.dvrdns.org

Username: techsupport

Password: ••••••••••••

- **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.



IP address source [IPv4]: Network

Network [IPv4]: ifmobile

DNS-Server: mydns.lan

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

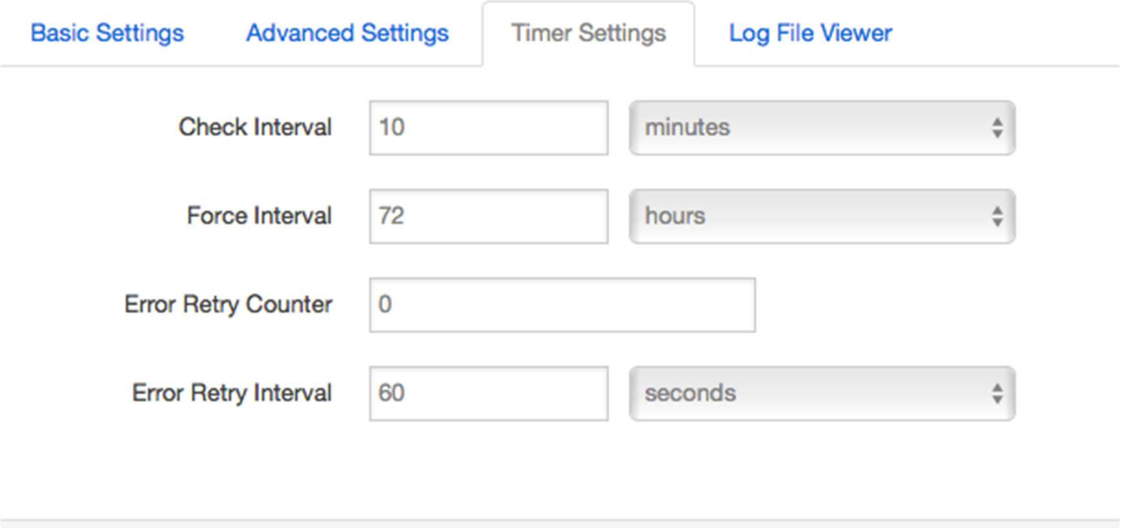
Log to syslog: Notice

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

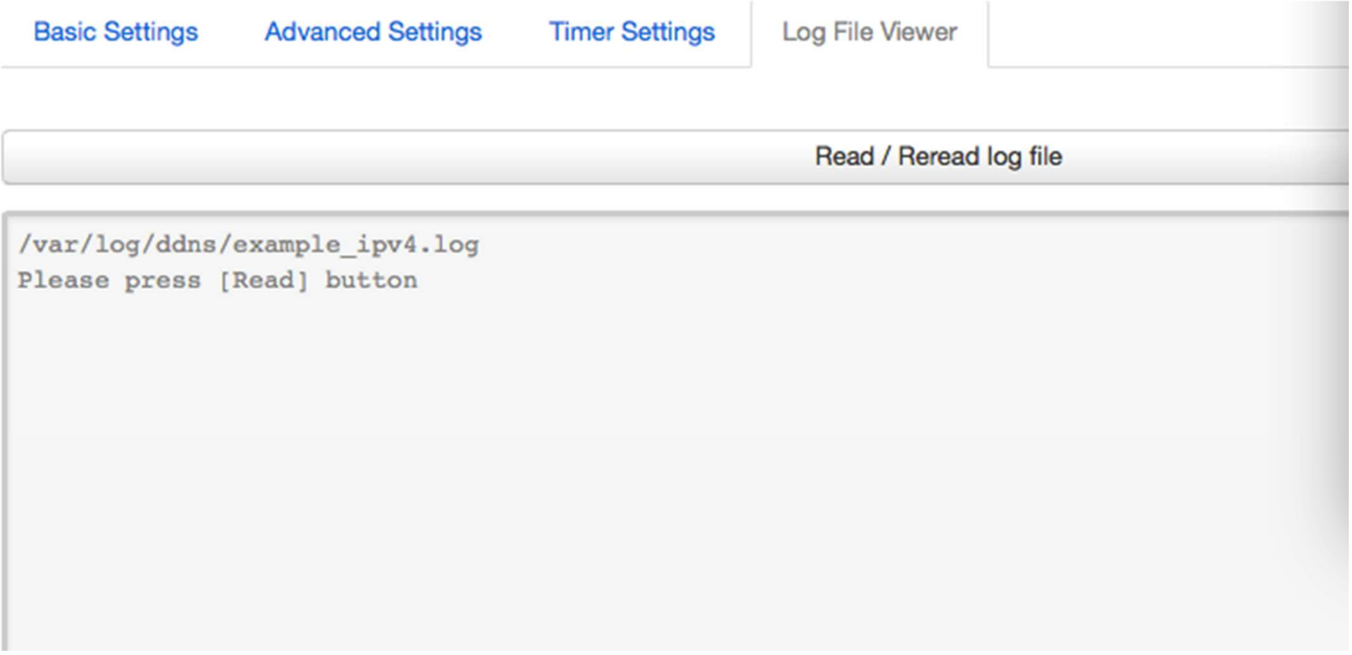
address and domain name are required.

- **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.



Check Interval: 10 minutes
Force Interval: 72 hours
Error Retry Counter: 0
Error Retry Interval: 60 seconds

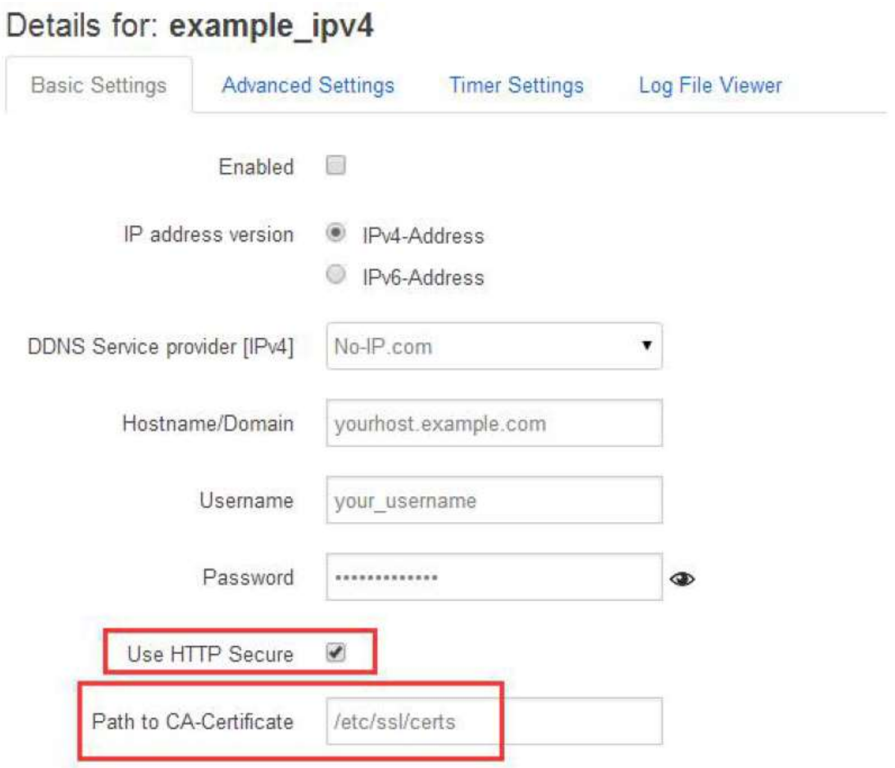
- **Check Interval:** The minimum check interval is 1 minute=60seconds.
- **Force interval:** The minimum check interval is 1 minute=60seconds.
- **Error Retry Counter:** On Error, the script will stop execution after a given number of retries. The default settings of ‘0’ will retry indefinitely.



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

Read the log file of DDNS.

Note:
If you use the DDNS server no-ip.com, please tick the box " Use HTTP Secure" and input "8.8.8.8" for the DNS-Server.



Details for: **example_ipv4**

Enabled □

IP address version ● IPv4-Address ○ IPv6-Address

DDNS Service provider [IPv4] No-IP.com

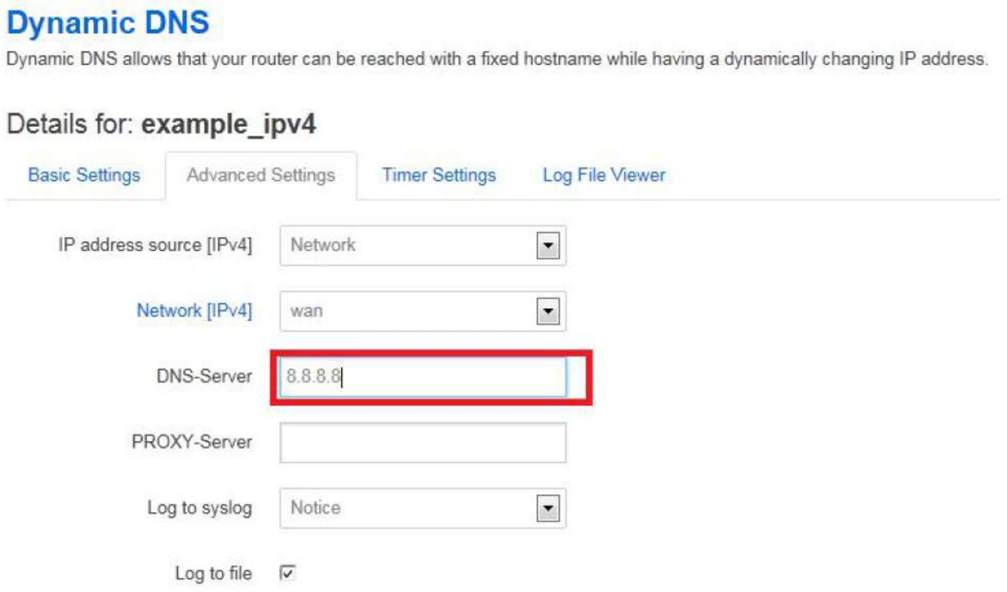
Hostname/Domain yourhost.example.com

Username your_username

Password ••••••••••••••

Use HTTP Secure ☑

Path to CA-Certificate /etc/ssl/certs



Dynamic DNS

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

Details for: **example_ipv4**

IP address source [IPv4] Network

Network [IPv4] wan

DNS-Server 8.8.8.8

PROXY-Server

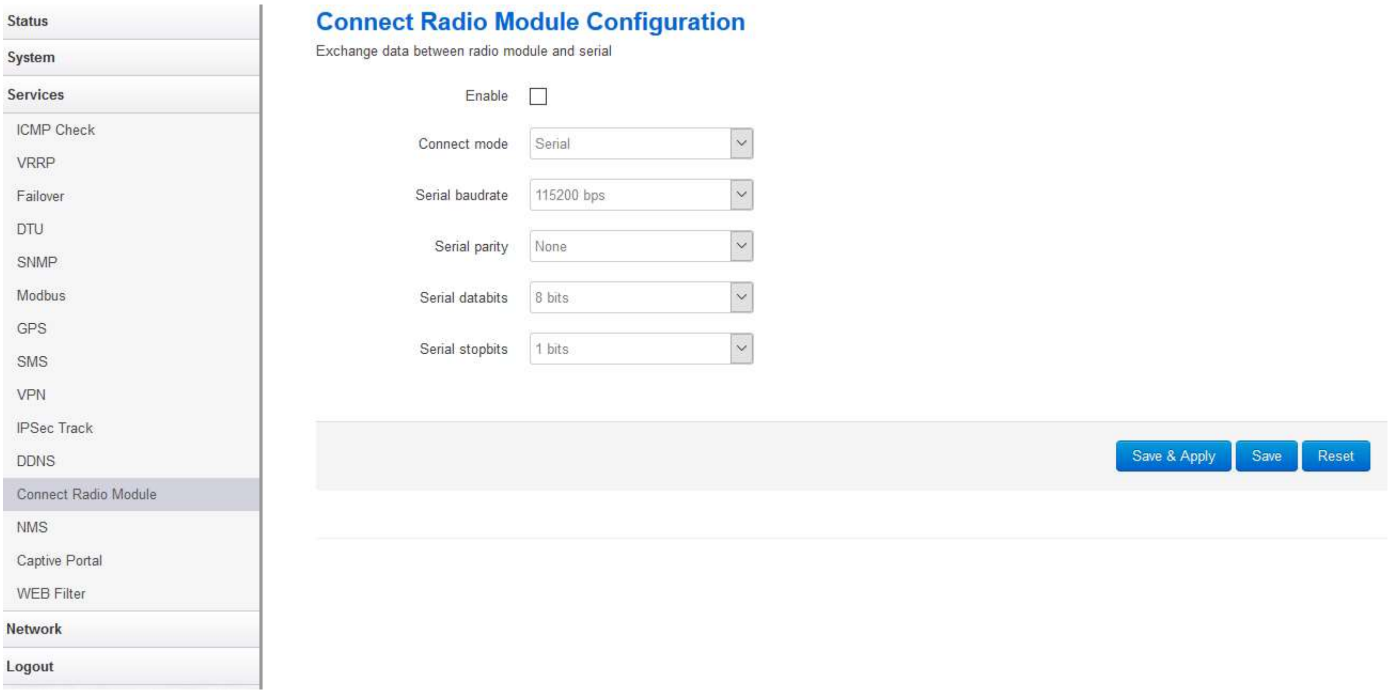
Log to syslog Notice

Log to file ☑

3.5.10 Connect Radio Module

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

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



Connect Radio Module Configuration

Exchange data between radio module and serial

Enable □

Connect mode: Serial

Serial baudrate: 115200 bps

Serial parity: None

Serial databits: 8 bits

Serial stopbits: 1 bits

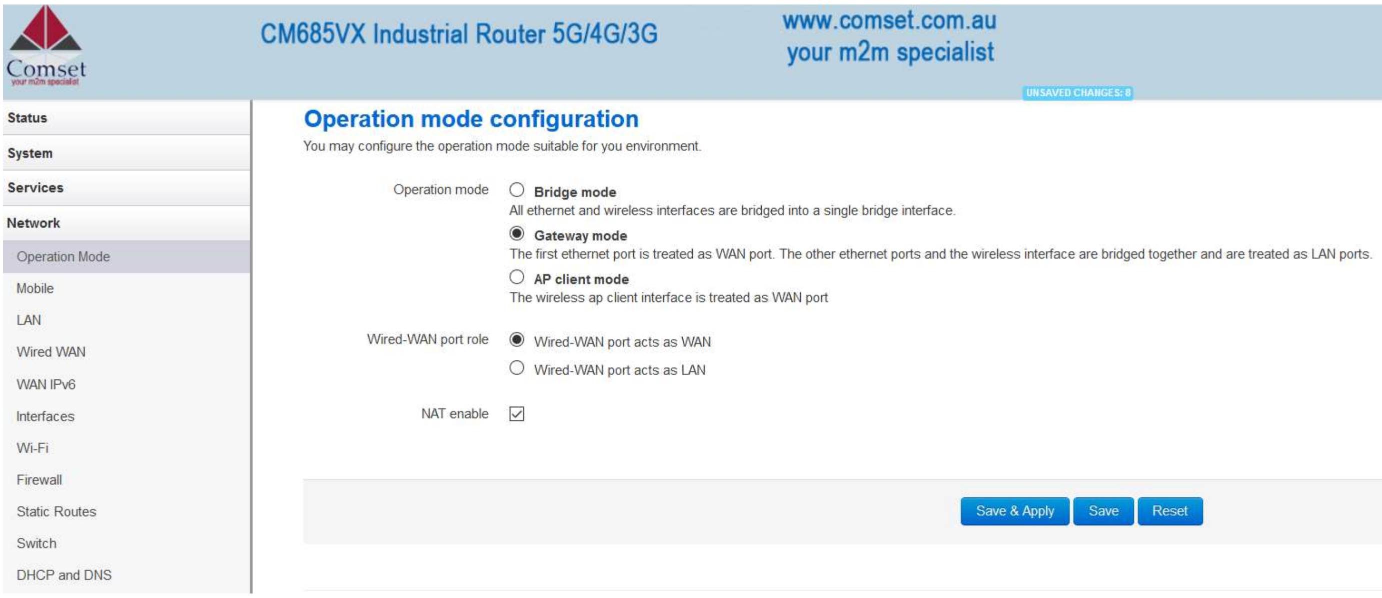
- **Connect Mode:** Serial only

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



Operation mode configuration

You may configure the operation mode suitable for you environment.

Operation mode
○ Bridge mode
All ethernet and wireless interfaces are bridged into a single bridge interface.
● Gateway mode
The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.
○ AP client mode
The wireless ap client interface is treated as WAN port

Wired-WAN port role
● Wired-WAN port acts as WAN
○ Wired-WAN port acts as LAN

NAT enable ☑

- **Operation mode**
  - **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface.
  - **Gateway:** The first Ethernet port is treated as a WAN port. The second Ethernet port and the wireless interface are bridged together and are treated as LAN ports.
  - **AP Client:** The wireless apcli interface is treated as a WAN port and the wireless AP interface and the Ethernet ports are treated as LAN ports.
- **NAT Enabled**

  Network Address Translation. Default is *Enabled.*
- **Ethernet WAN port:**

  Wired-WAN port acts as WAN

  Default is checked.

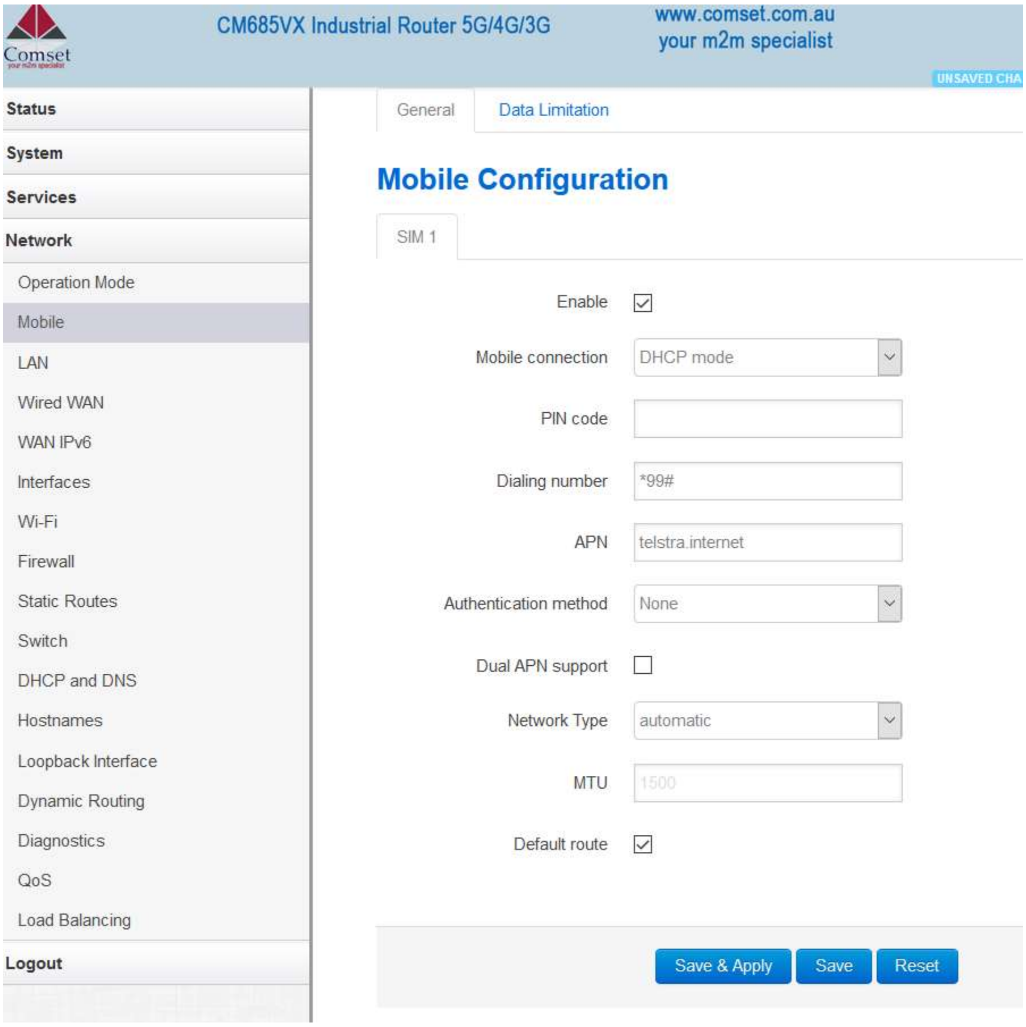
  Wired-WAN port acts as LAN

  Default is un-checked. If you check this box, the WAN port will act as a LAN port.

The default operation is in “Gateway mode”.

3.6.2 Mobile configuration

Here you can configure the parameters for the SIM card.



Mobile Configuration

Enable ☑

Mobile connection: DHCP mode

PIN code:

Dialing number: *99#

APN: telstra.internet

Authentication method: None

Dual APN support ☐

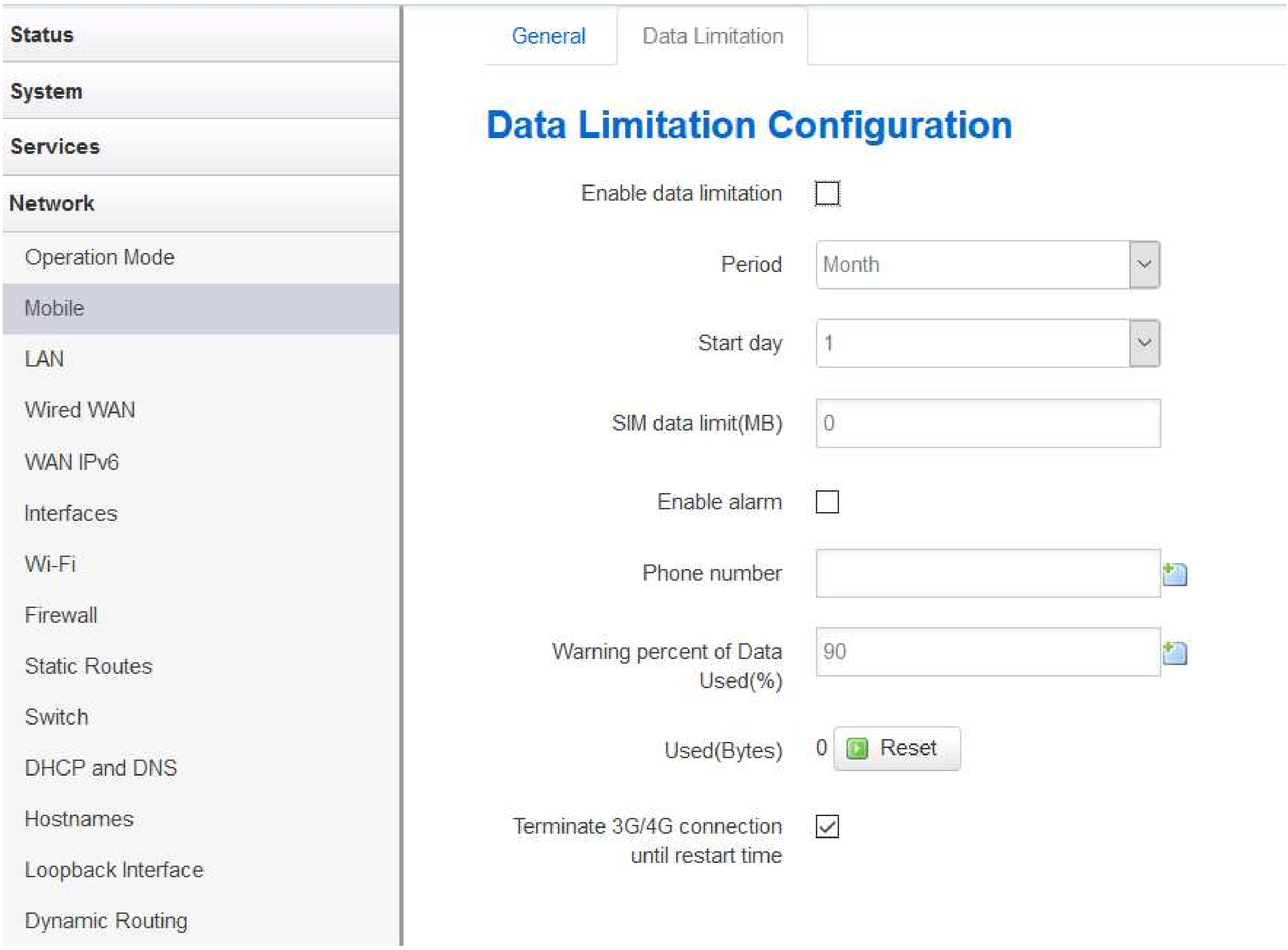
Network Type: automatic

MTU: 1500

Default route ☑

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

3.6.3 Data Limitation

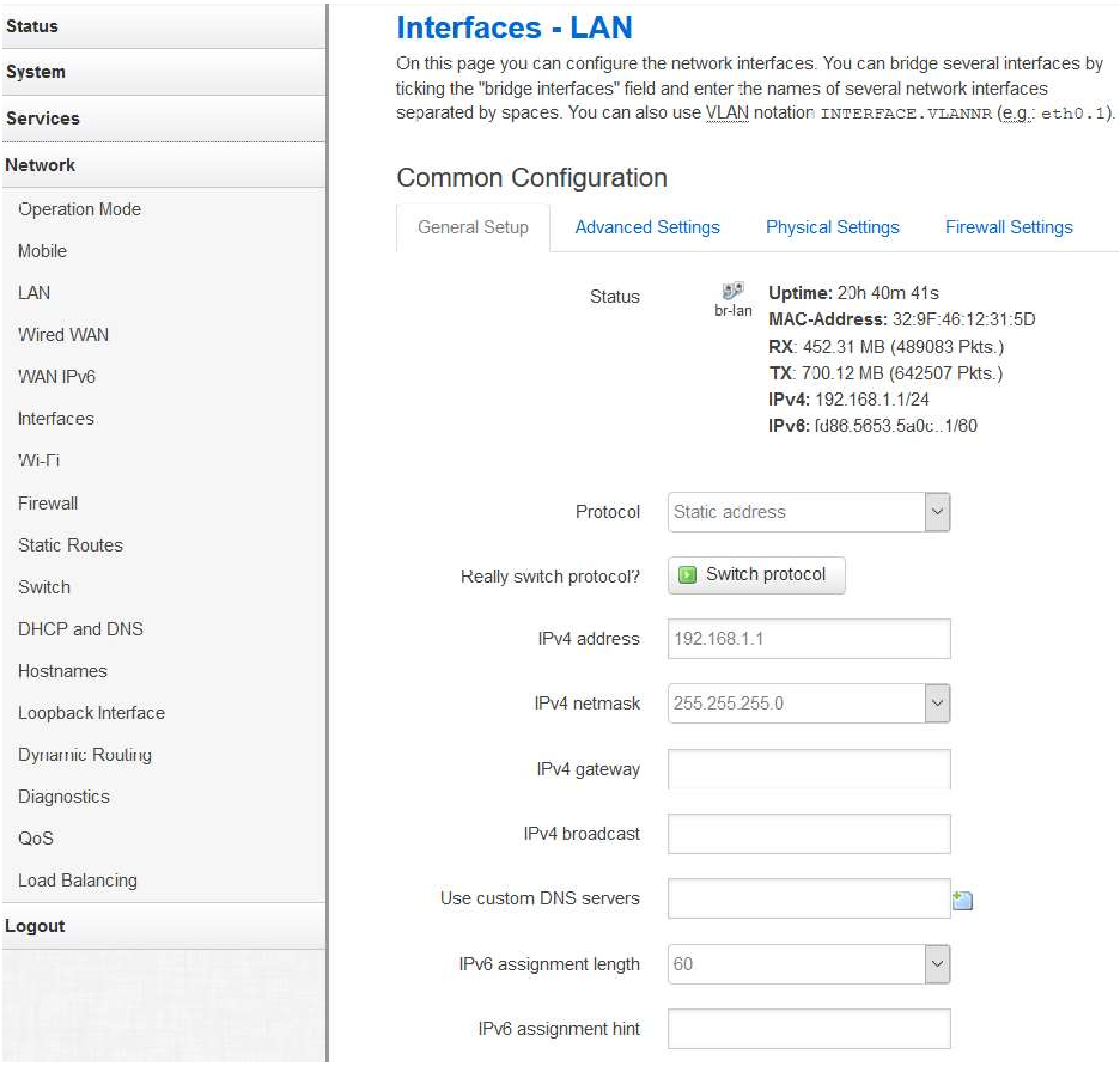


Data Limitation Configuration

Enable data limitation	□
Period	Month
Start day	1
SIM data limit(MB)	0
Enable alarm	□
Phone number	
Warning percent of Data Used(%)	90
Used(Bytes)	0
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



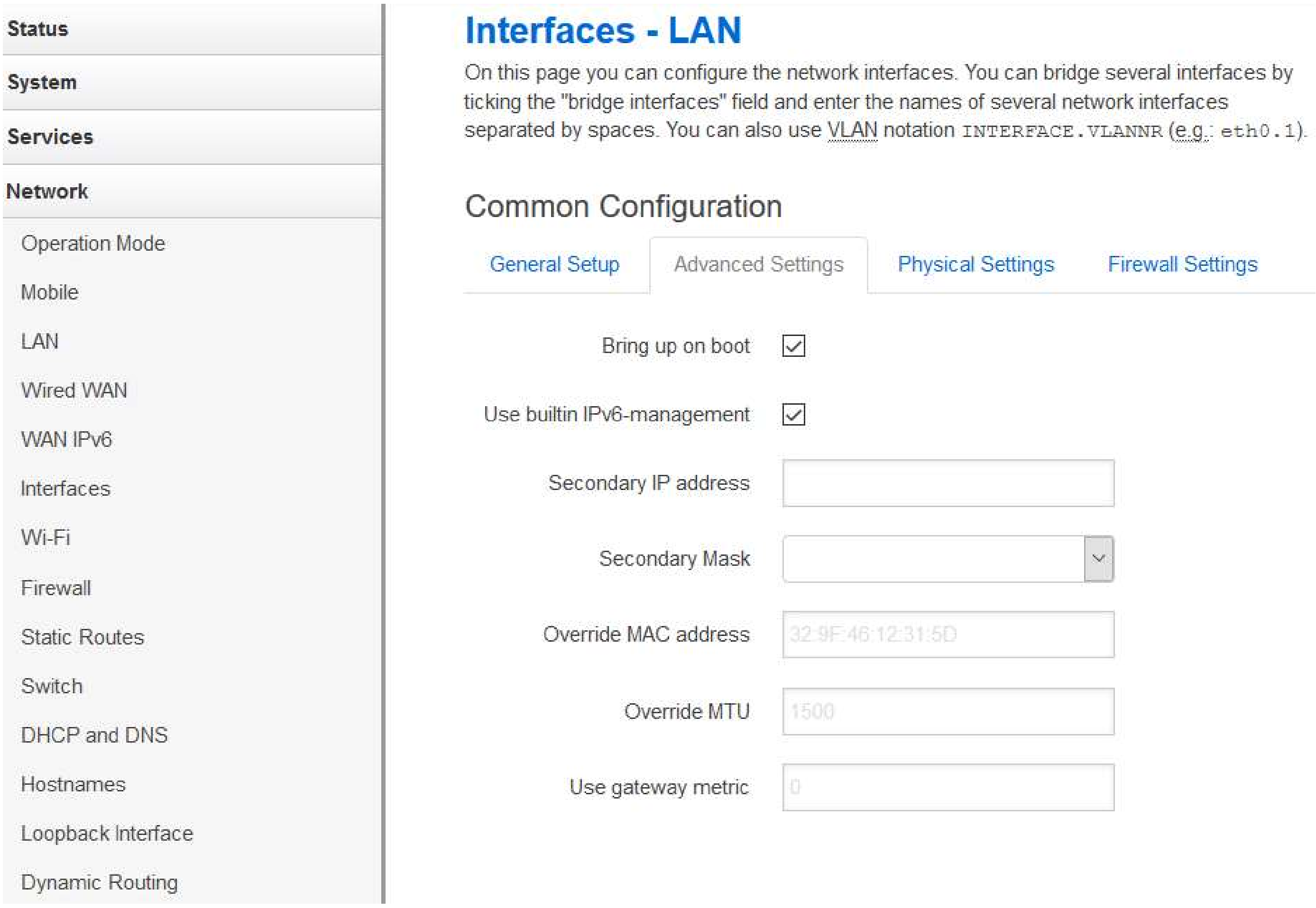
Interfaces - LAN

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

Common Configuration

Status	br-lan **Uptime:** 20h 40m 41s **MAC-Address:** 32:9F:46:12:31:5D **RX**: 452.31 MB (489083 Pkts.) **TX**: 700.12 MB (642507 Pkts.) **IPv4:** 192.168.1.1/24 **IPv6:** fd86:5653:5a0c::1/60
Protocol	Static address
Really switch protocol?	Switch protocol
IPv4 address	192.168.1.1
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	
IPv6 assignment length	60
IPv6 assignment hint	

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



Interfaces - LAN

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

Common Configuration

Bring up on boot ☑

Use builtin IPv6-management ☑

Secondary IP address

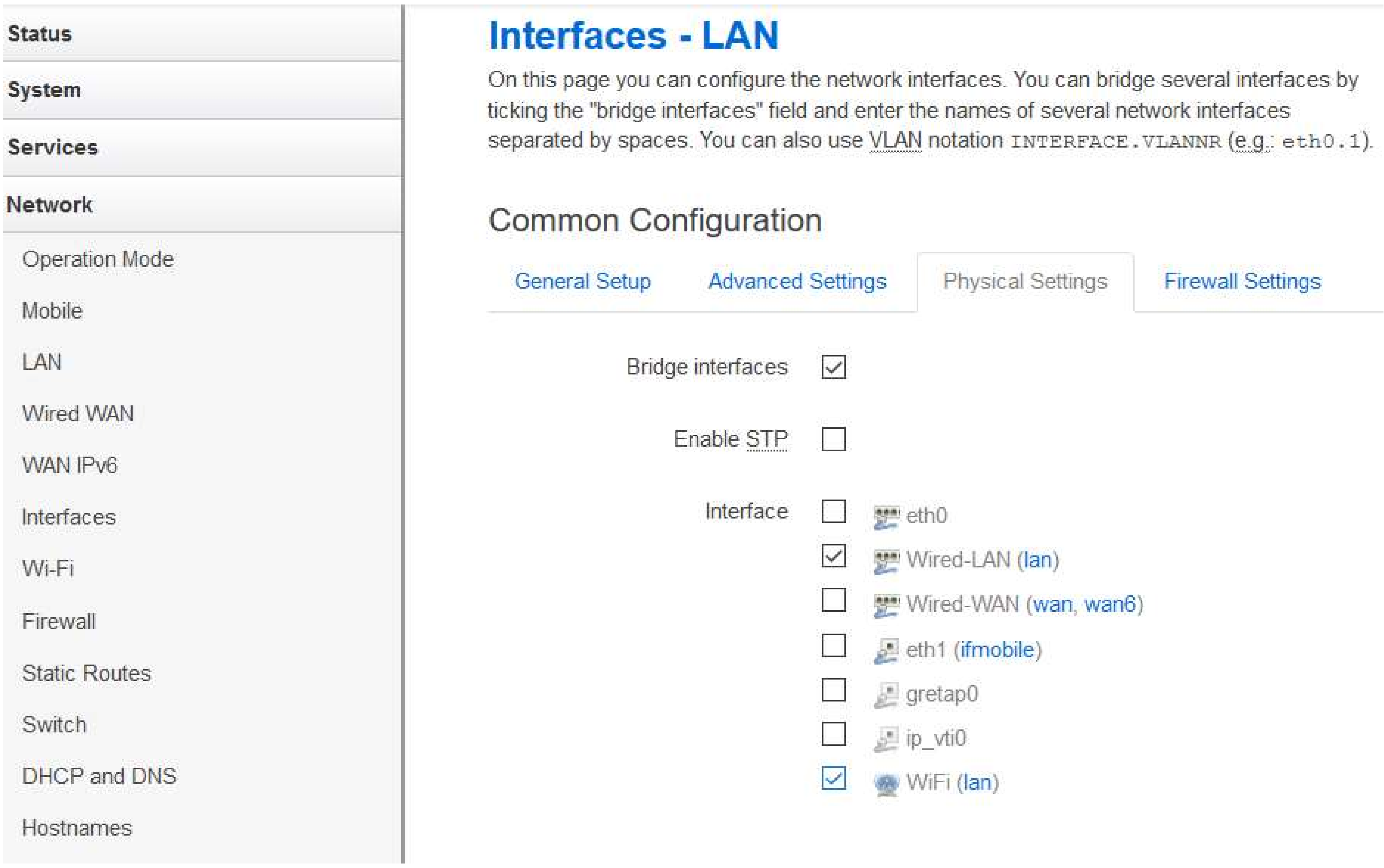
Secondary Mask

Override MAC address 32:9F:46:12:31:5D

Override MTU 1500

Use gateway metric 0

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



Interfaces - LAN

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

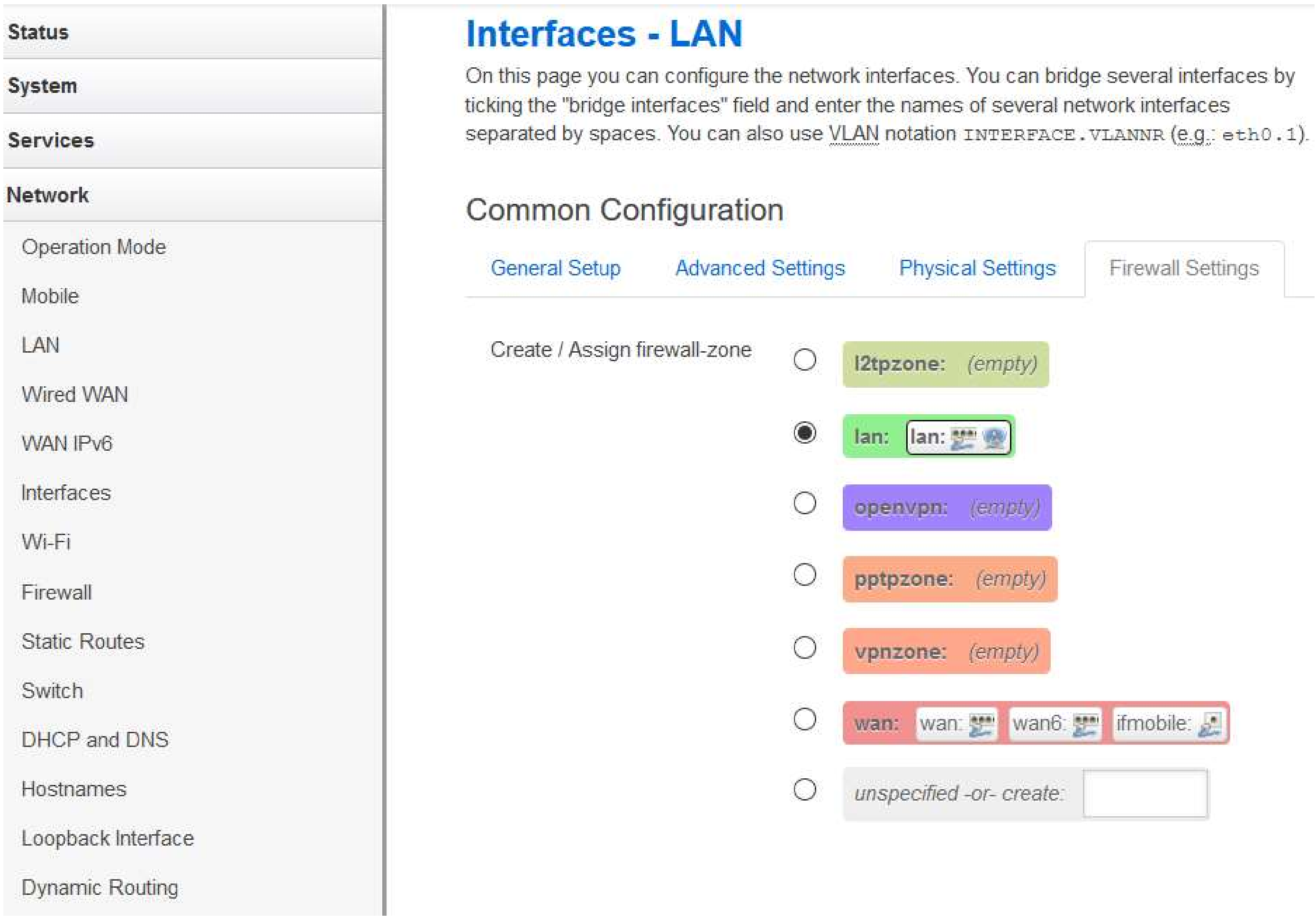
Common Configuration

Bridge interfaces ☑

Enable STP □

Interface
□ eth0
☑ Wired-LAN (lan)
□ Wired-WAN (wan, wan6)
□ eth1 (ifmobile)
□ gretap0
□ ip_vti0
☑ WiFi (lan)

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



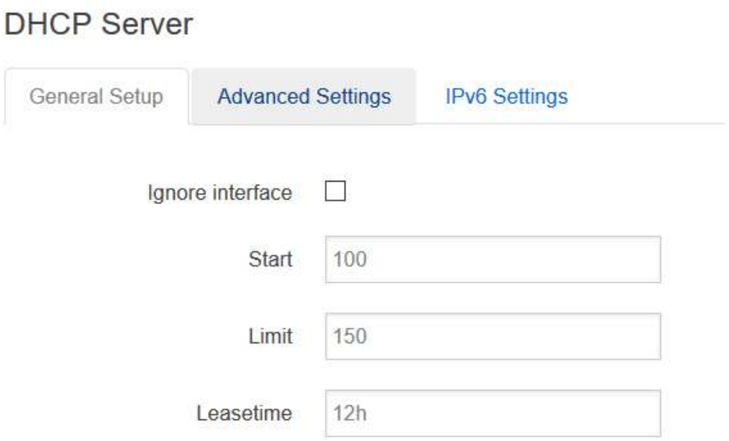
Interfaces - LAN

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

Common Configuration

Create / Assign firewall-zone

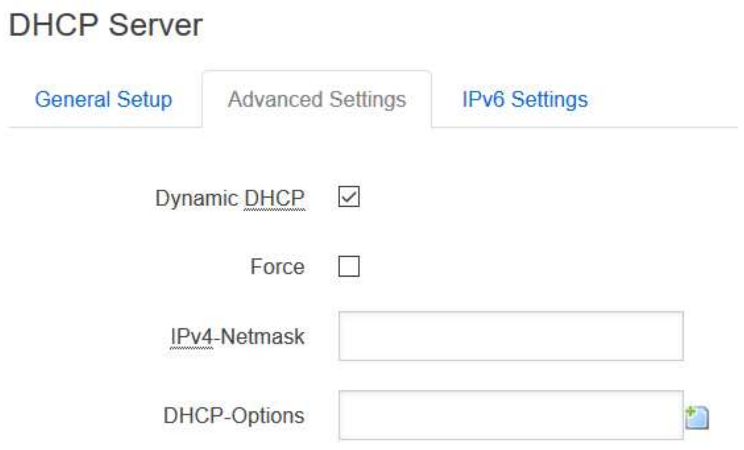
○ l2tpzone: *(empty)*
● lan: lan:
○ openvpn: *(empty)*
○ pptpzone: *(empty)*
○ vpnzone: *(empty)*
○ wan: wan: wan6: ifmobile:
○ *unspecified -or- create:*



DHCP Server

Ignore interface	□
Start	100
Limit	150
Leasetime	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). 12h means 12 hours.



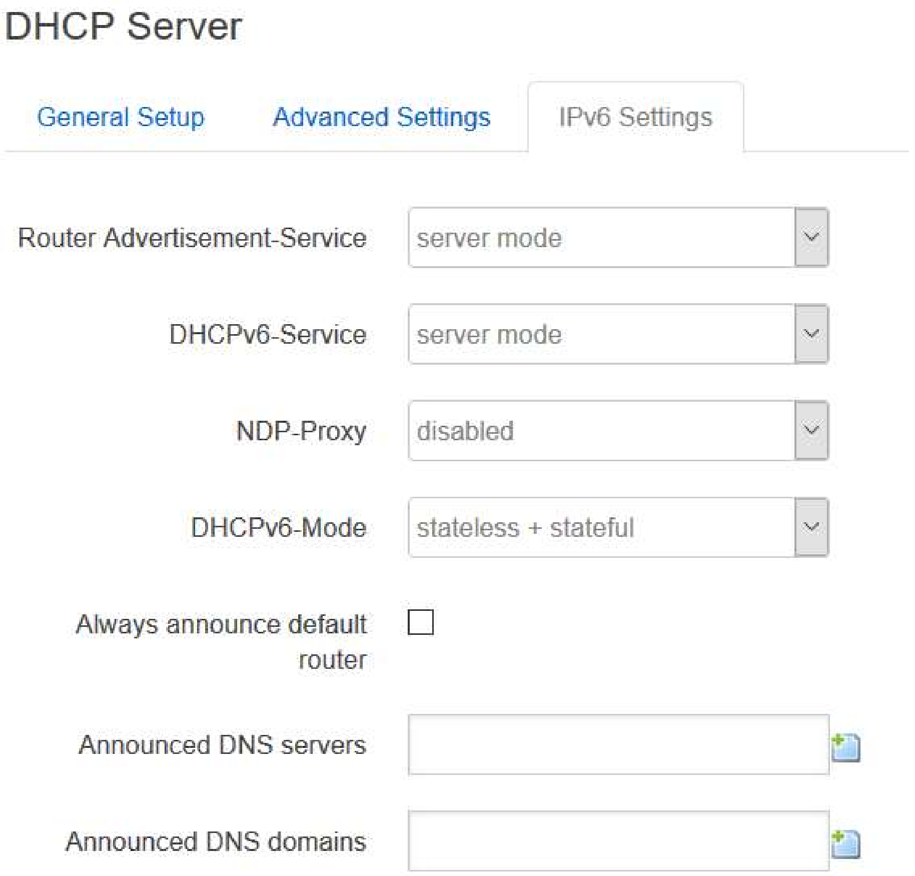
Dynamic DHCP ☑

Force □

IPv4-Netmask

DHCP-Options

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



DHCP Server

Router Advertisement-Service: server mode

DHCPv6-Service: server mode

NDP-Proxy: disabled

DHCPv6-Mode: stateless + stateful

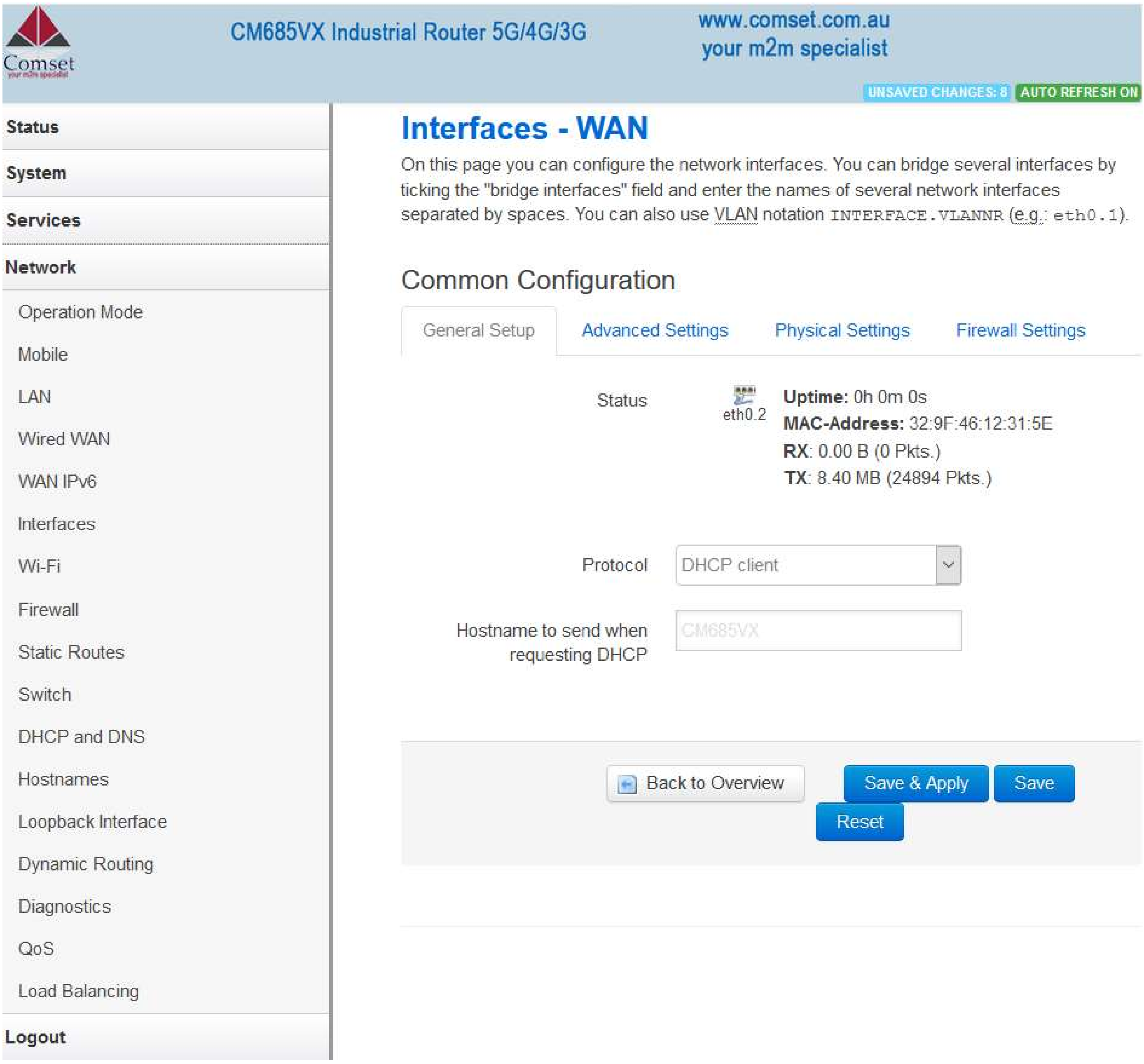
Always announce default router: □

Announced DNS servers:

Announced DNS domains:

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

3.6.5 Wired-WAN



Interfaces - WAN

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

Common Configuration

Status: eth0.2 **Uptime:** 0h 0m 0s **MAC-Address:** 32:9F:46:12:31:5E **RX**: 0.00 B (0 Pkts.) **TX**: 8.40 MB (24894 Pkts.)

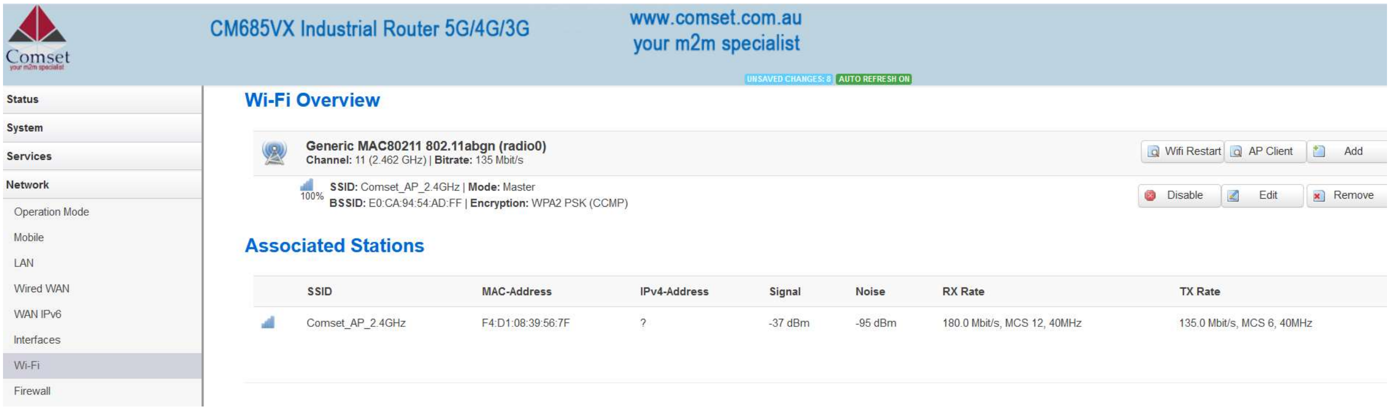
Protocol: DHCP client

Hostname to send when requesting DHCP: CM685VX

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

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

3.6.6 WiFi Settings



Wi-Fi Overview

Generic MAC80211 802.11abgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 135 Mbit/s

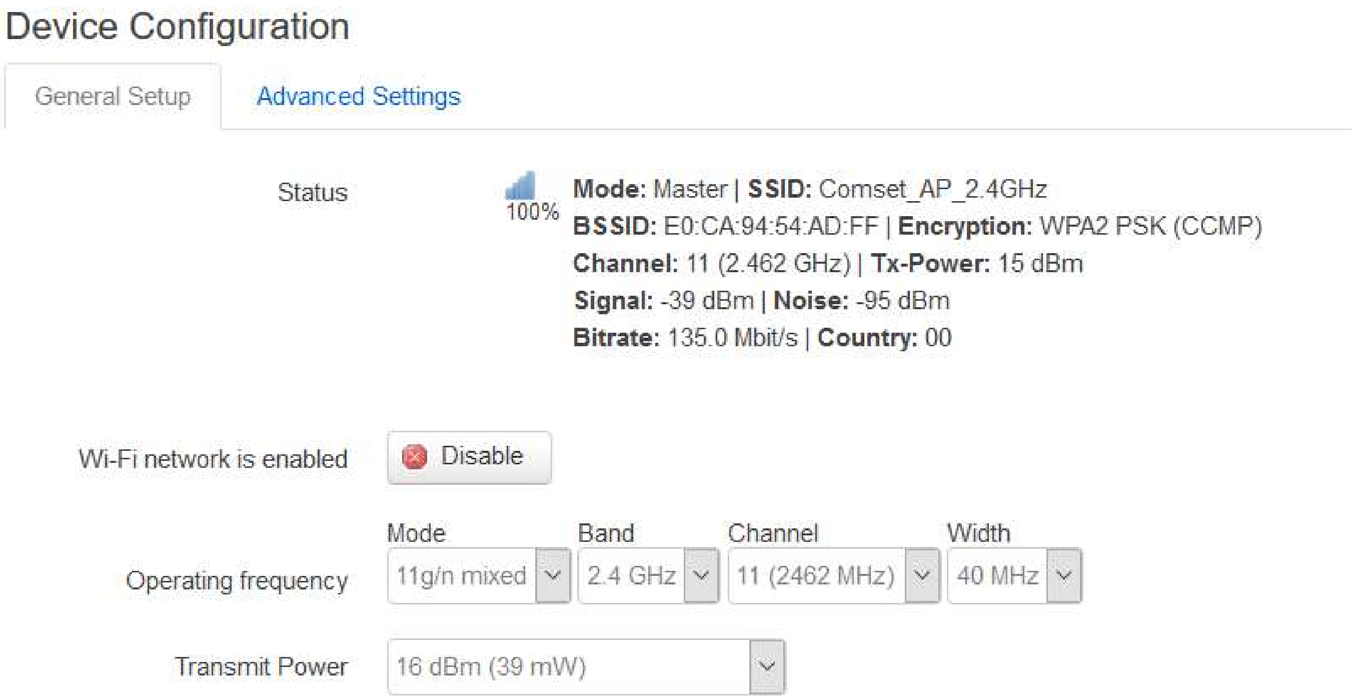
100% **SSID:** Comset_AP_2.4GHz | **Mode:** Master
BSSID: E0:CA:94:54:AD:FF | **Encryption:** WPA2 PSK (CCMP)

Associated Stations

	SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
	Comset_AP_2.4GHz	F4:D1:08:39:56:7F	?	-37 dBm	-95 dBm	180.0 Mbit/s, MCS 12, 40MHz	135.0 Mbit/s, MCS 6, 40MHz

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

3.6.6.1 WiFi General Configuration



Device Configuration

Status: 100%
Mode: Master | **SSID:** Comset_AP_2.4GHz
BSSID: E0:CA:94:54:AD:FF | **Encryption:** WPA2 PSK (CCMP)
Channel: 11 (2.462 GHz) | **Tx-Power:** 15 dBm
Signal: -39 dBm | **Noise:** -95 dBm
Bitrate: 135.0 Mbit/s | **Country:** 00

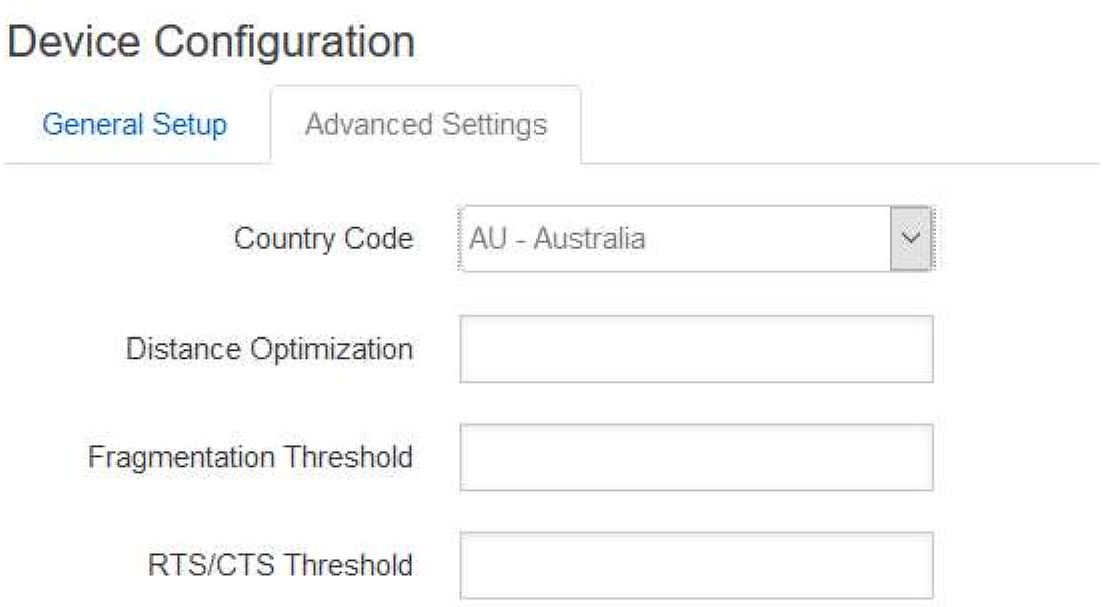
Wi-Fi network is enabled: Disable

Operating frequency: Mode: 11g/n mixed; Band: 2.4 GHz; Channel: 11 (2462 MHz); Width: 40 MHz

Transmit Power: 16 dBm (39 mW)

- **Status**: Shows the WiFi signal strength, mode, SSID.
- **Operating frequency Mode**: Supports 802.11b/g/n.
- **Band**: 2.4GHz.
- **Channel**: Channel 1-11.
- **Width**: 20MHz and 40MHz.
- **Transmit Power**: From 0dBm to 16dBm.

3.6.6.2 WiFi Advanced Configuration



Device Configuration

Country Code: AU - Australia

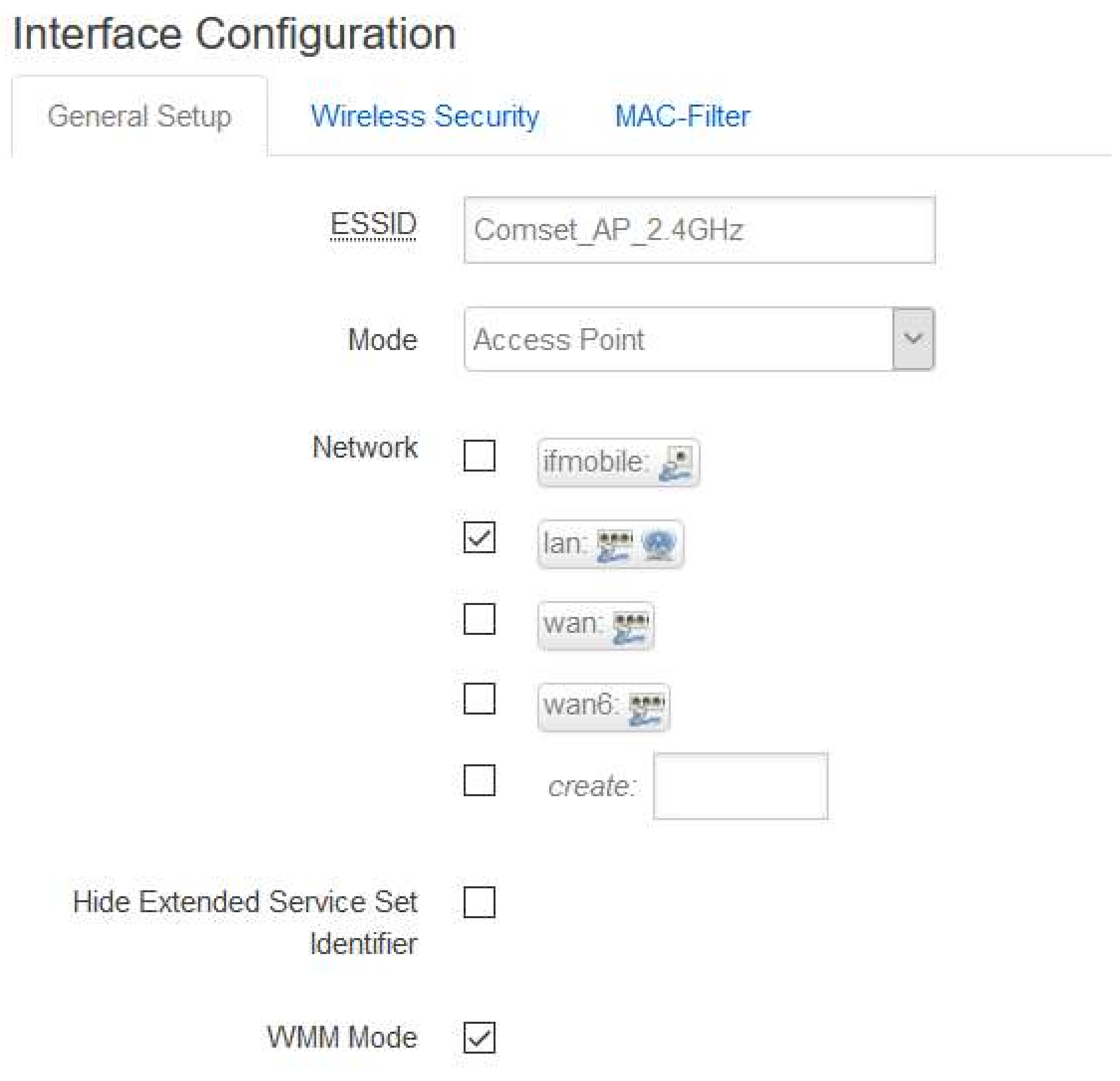
Distance Optimization

Fragmentation Threshold

RTS/CTS Threshold

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

3.6.6.3 WiFi Interface Configuration



Interface Configuration

ESSID: Comset_AP_2.4GHz

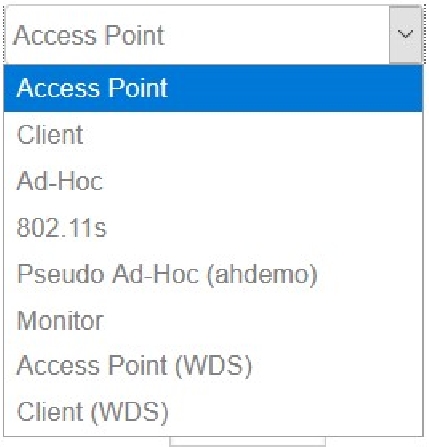
Mode: Access Point

Network:
□ ifmobile:
☑ lan:
□ wan:
□ wan6:
□ create:

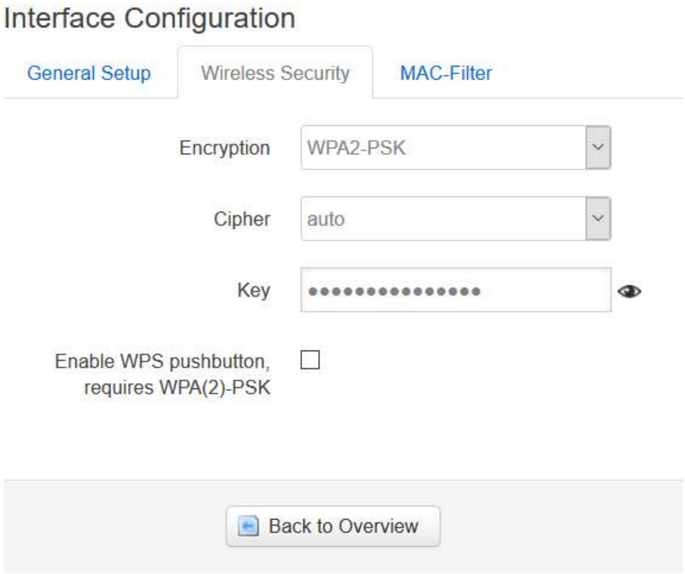
Hide Extended Service Set Identifier □

WMM Mode ☑

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



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


Interface Configuration

General Setup | Wireless Security | MAC-Filter

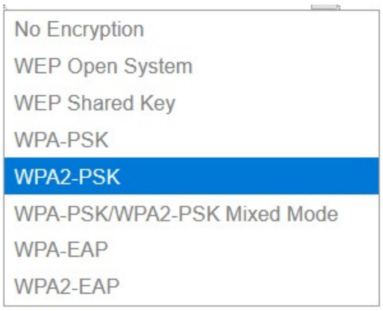
Encryption: WPA2-PSK

Cipher: auto

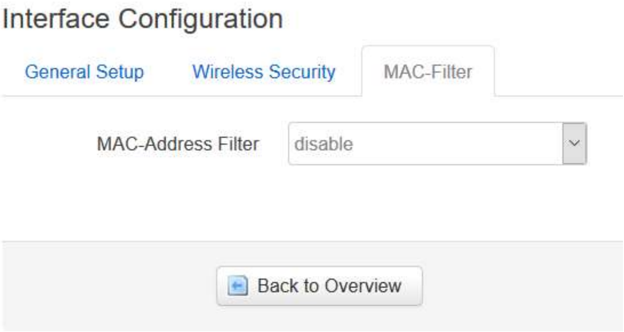
Key: ●●●●●●●●●●●●●●●

Enable WPS pushbutton, requires WPA(2)-PSK ☐

- **Encryption:**



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



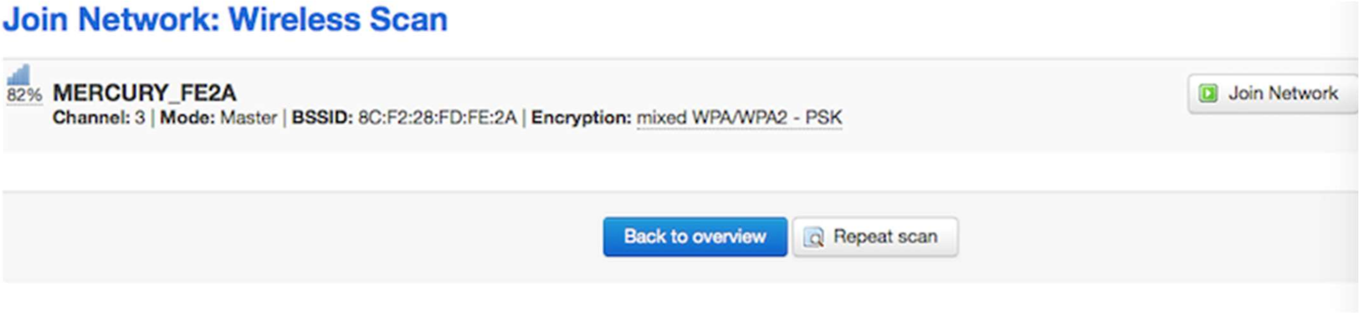
Interface Configuration

MAC-Address Filter: disable

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

3.6.6.4 WiFi AP client

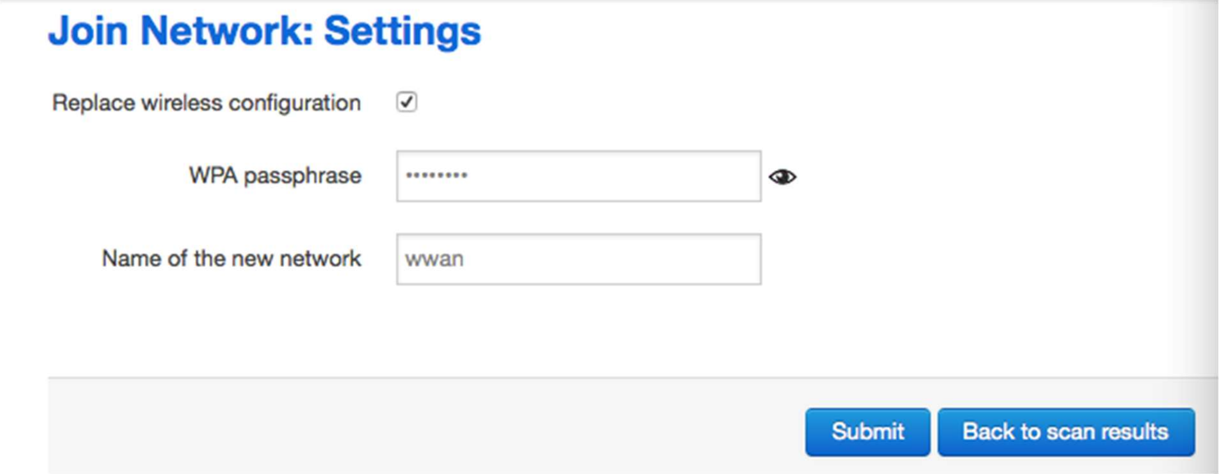
- **Steps 1)** Click the button “AP Client” on the wireless overview page, then the system will start to scan all WiFi signals.



Join Network: Wireless Scan

82% **MERCURY_FE2A**
Channel: 3 | **Mode:** Master | **BSSID:** 8C:F2:28:FD:FE:2A | **Encryption:** mixed WPA/WPA2 - PSK

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



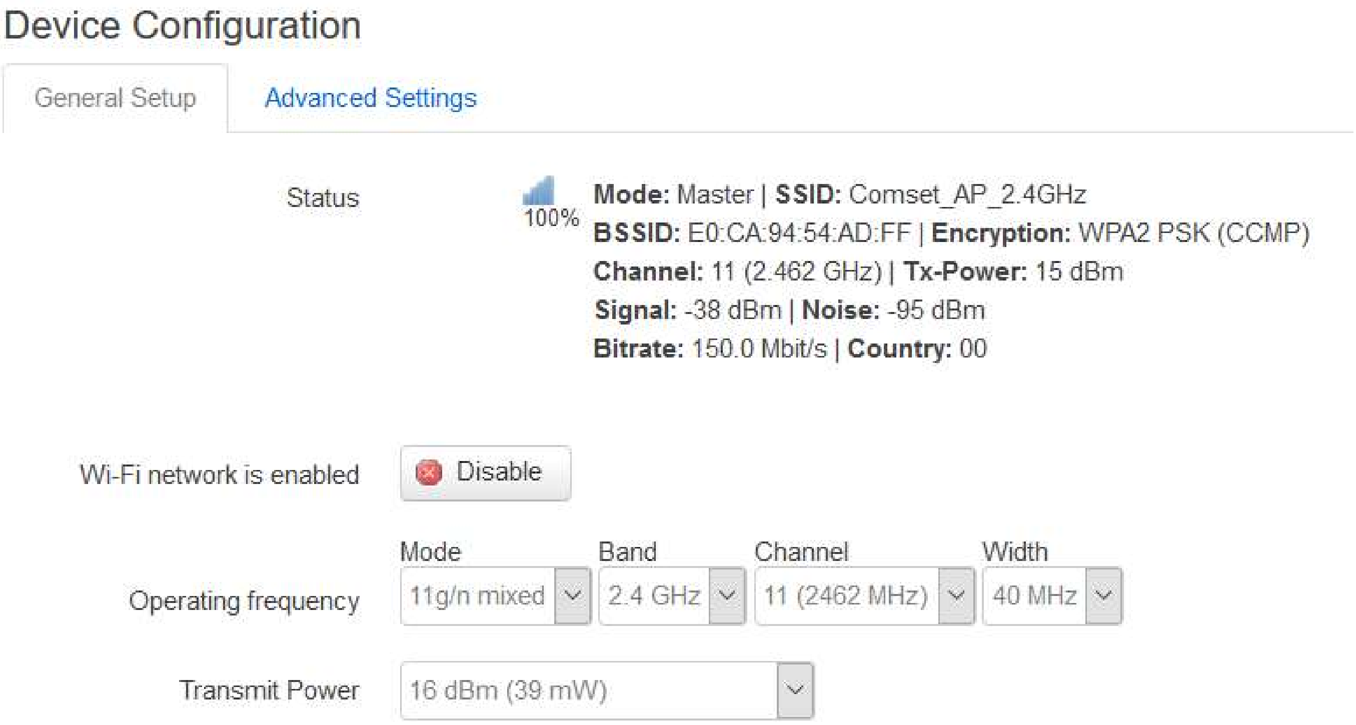
Join Network: Settings

Replace wireless configuration ☑

WPA passphrase: ••••••••

Name of the new network: wwan

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



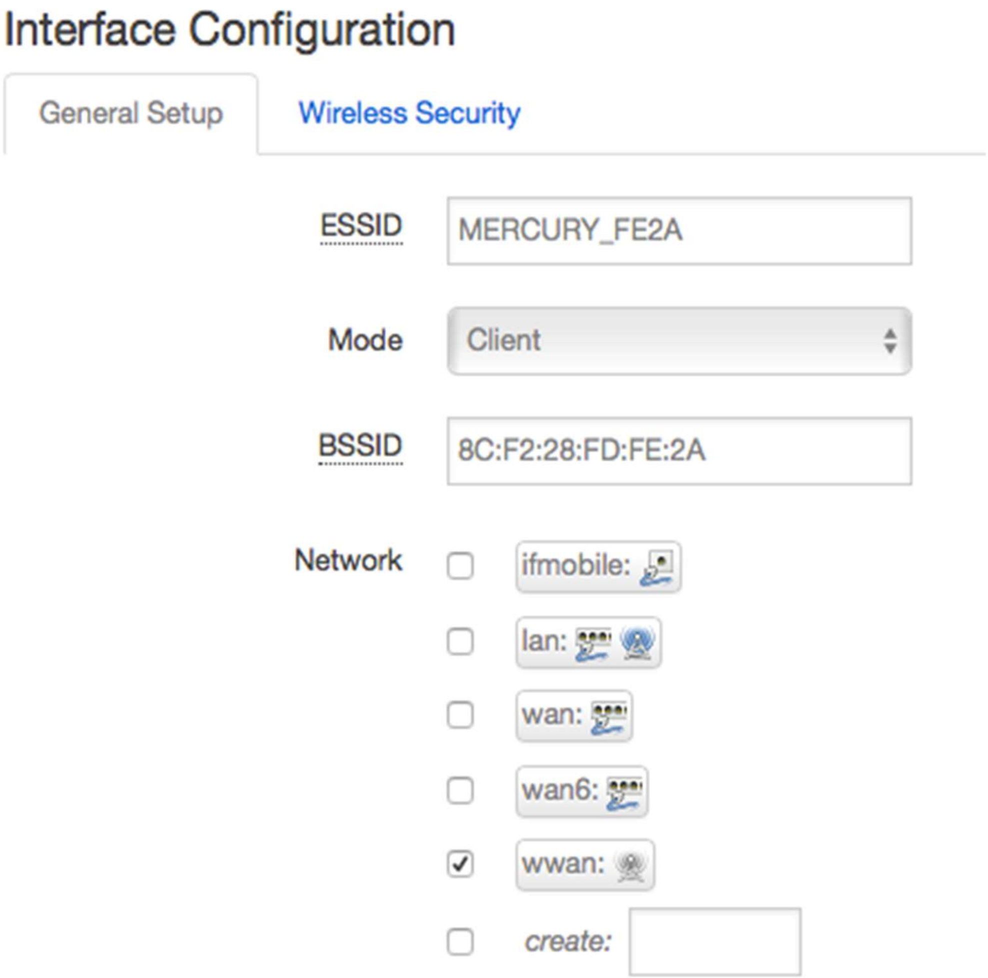
Device Configuration

Status: 100% **Mode:** Master | **SSID:** Comset_AP_2.4GHz
BSSID: E0:CA:94:54:AD:FF | **Encryption:** WPA2 PSK (CCMP)
Channel: 11 (2.462 GHz) | **Tx-Power:** 15 dBm
Signal: -38 dBm | **Noise:** -95 dBm
Bitrate: 150.0 Mbit/s | **Country:** 00

Wi-Fi network is enabled: Disable

Operating frequency: Mode 11g/n mixed; Band 2.4 GHz; Channel 11 (2462 MHz); Width 40 MHz

Transmit Power: 16 dBm (39 mW)



Interface Configuration

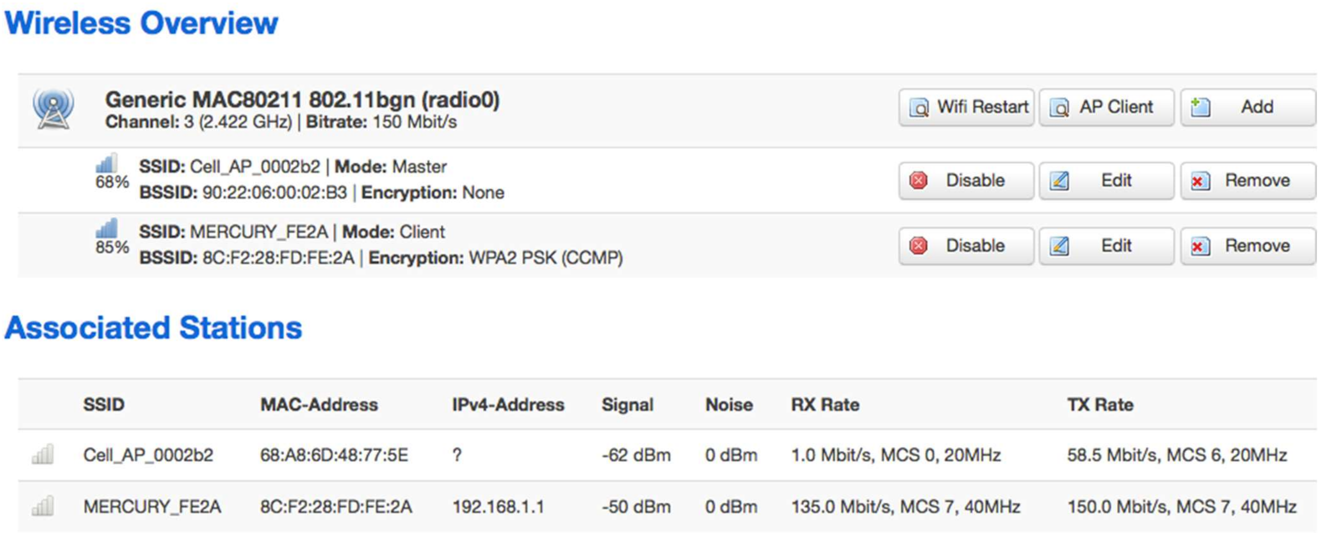
ESSID: MERCURY_FE2A

Mode: Client

BSSID: 8C:F2:28:FD:FE:2A

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

68% **SSID:** Cell_AP_0002b2 | **Mode:** Master
BSSID: 90:22:06:00:02:B3 | **Encryption:** None

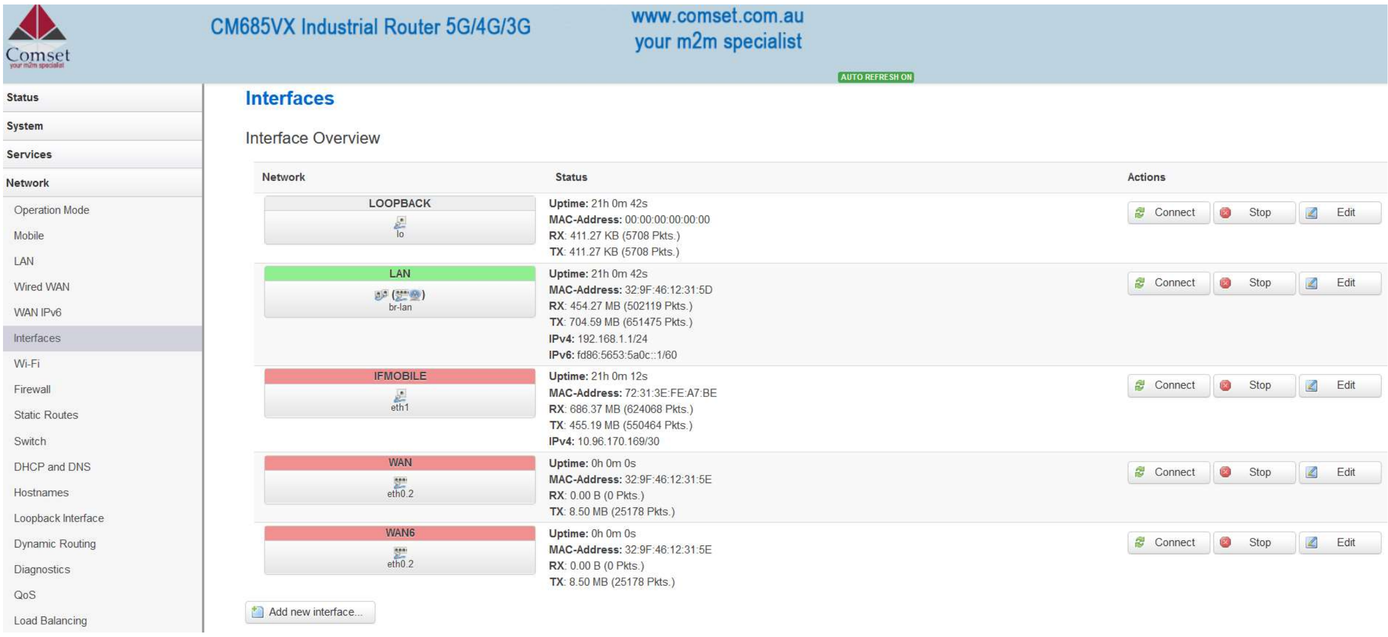
85% **SSID:** MERCURY_FE2A | **Mode:** Client
BSSID: 8C:F2:28:FD:FE:2A | **Encryption:** WPA2 PSK (CCMP)

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

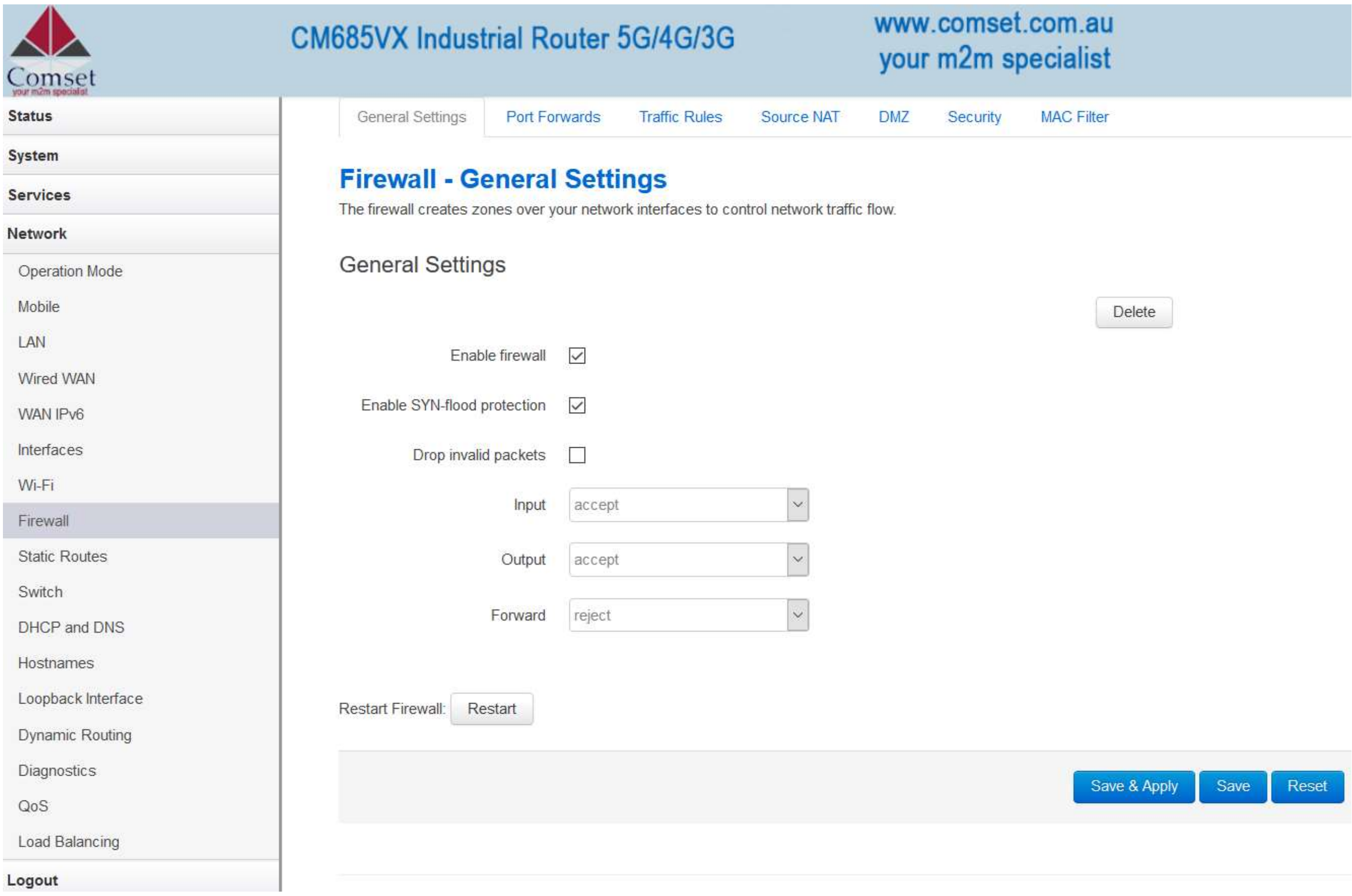
Interface Overview

Network	Status	Actions
LOOPBACK lo	**Uptime:** 21h 0m 42s **MAC-Address:** 00:00:00:00:00:00 **RX**: 411.27 KB (5708 Pkts.) **TX**: 411.27 KB (5708 Pkts.)	Connect Stop Edit
LAN br-lan	**Uptime:** 21h 0m 42s **MAC-Address:** 32:9F:46:12:31:5D **RX**: 454.27 MB (502119 Pkts.) **TX**: 704.59 MB (651475 Pkts.) **IPv4:** 192.168.1.1/24 **IPv6:** fd86:5653:5a0c::1/60	Connect Stop Edit
IFMOBILE eth1	**Uptime:** 21h 0m 12s **MAC-Address:** 72:31:3E:FE:A7:BE **RX**: 686.37 MB (624068 Pkts.) **TX**: 455.19 MB (550464 Pkts.) **IPv4:** 10.96.170.169/30	Connect Stop Edit
WAN eth0.2	**Uptime:** 0h 0m 0s **MAC-Address:** 32:9F:46:12:31:5E **RX**: 0.00 B (0 Pkts.) **TX**: 8.50 MB (25178 Pkts.)	Connect Stop Edit
WAN6 eth0.2	**Uptime:** 0h 0m 0s **MAC-Address:** 32:9F:46:12:31:5E **RX**: 0.00 B (0 Pkts.) **TX**: 8.50 MB (25178 Pkts.)	Connect Stop Edit

Add new interface...

3.6.8 Firewall

3.6.8.1 General Settings



Firewall - General Settings

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

General Settings

Enable firewall ☑

Enable SYN-flood protection ☑

Drop invalid packets ☐

Input: accept

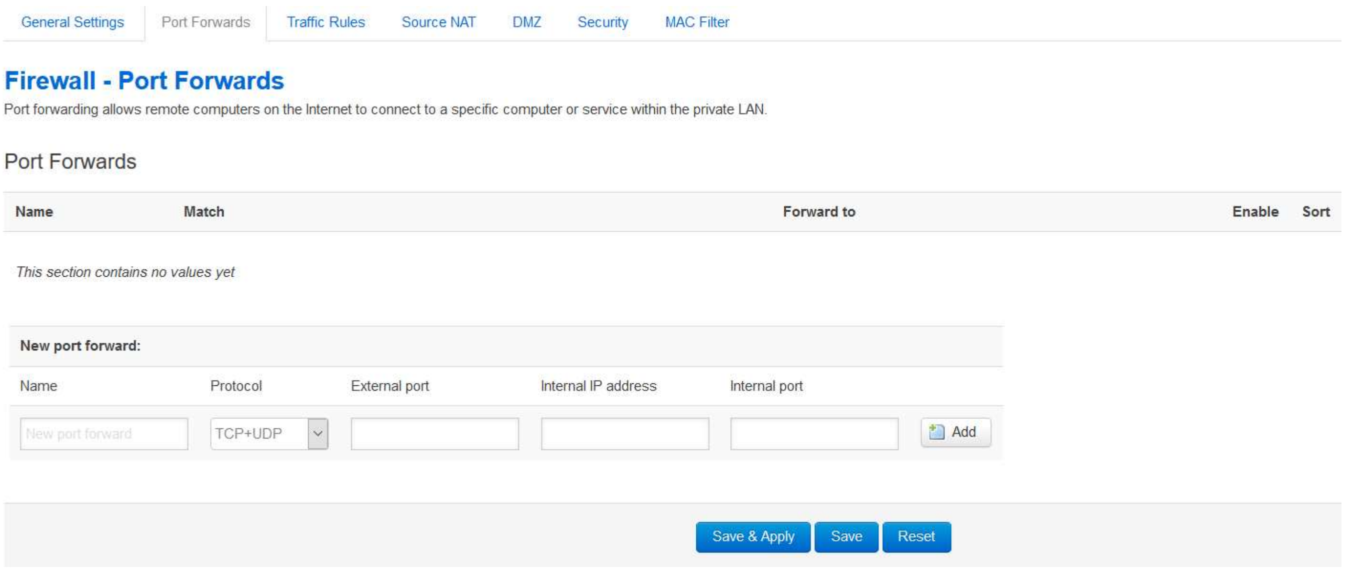
Output: accept

Forward: reject

Restart Firewall: Restart

3.6.8.2 Port Forwards

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



Firewall - Port Forwards

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

Port Forwards

Name	Match	Forward to	Enable	Sort

This section contains no values yet

New port forward:

Name	Protocol	External port	Internal IP address	Internal port	
New port forward	TCP+UDP				Add

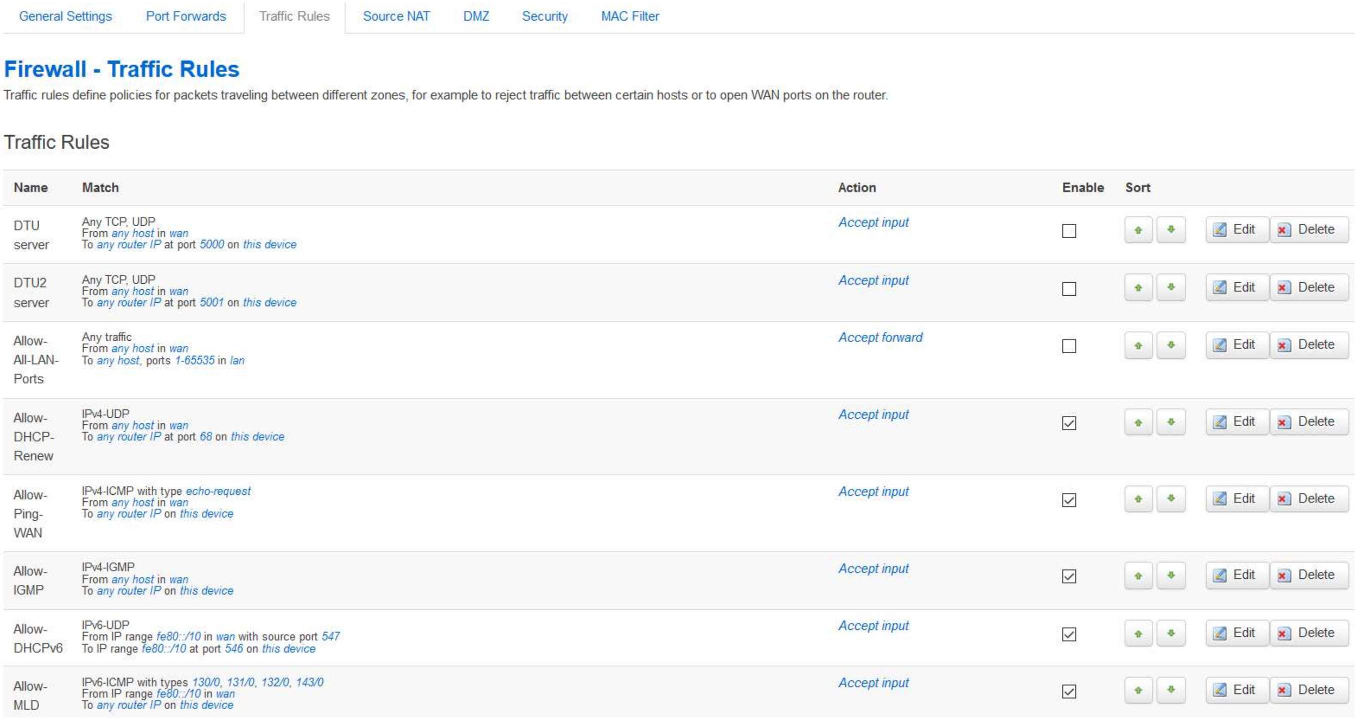
- **Name**: Port Forward instance name.
- **Protocol**: Options are TCP+UDP, UDP or TCP.
- **External zone**: The recommended option is ‘wan’.
- **External port**: Match incoming traffic directed at the given destination port on this host.
- **Internal zone**: The recommended zone is ‘lan’.
- **Internal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

3.6.8.3 Traffic rules

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

The traffic rules overview page contains the following functionalities:

Traffic rules list:



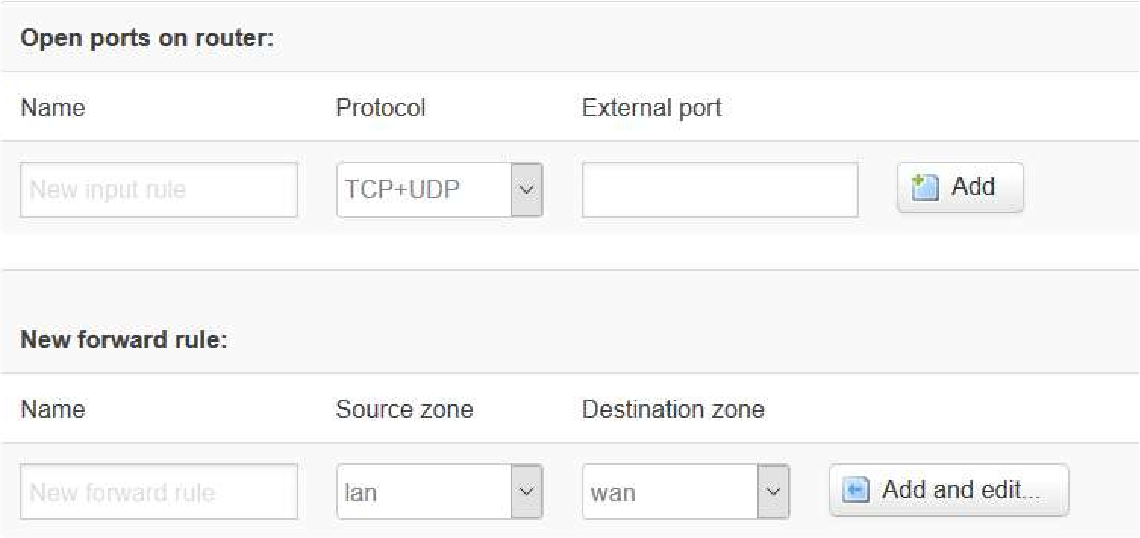
Firewall - Traffic Rules

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

Traffic Rules

Name	Match	Action	Enable	Sort	
DTU server	Any TCP, UDP From *any host* in *wan* To *any router IP* at port *5000* on *this device*	*Accept input*	□	↑ ↓	Edit Delete
DTU2 server	Any TCP, UDP From *any host* in *wan* To *any router IP* at port *5001* on *this device*	*Accept input*	□	↑ ↓	Edit Delete
Allow-All-LAN-Ports	Any traffic From *any host* in *wan* To *any host*, ports *1-65535* in *lan*	*Accept forward*	□	↑ ↓	Edit Delete
Allow-DHCP-Renew	IPv4-UDP From *any host* in *wan* To *any router IP* at port *68* on *this device*	*Accept input*	☑	↑ ↓	Edit Delete
Allow-Ping-WAN	IPv4-ICMP with type *echo-request* From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓	Edit Delete
Allow-IGMP	IPv4-IGMP From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓	Edit Delete
Allow-DHCPv6	IPv6-UDP From IP range *fe80::/10* in *wan* with source port *547* To IP range *fe80::/10* at port *546* on *this device*	*Accept input*	☑	↑ ↓	Edit Delete
Allow-MLD	IPv6-ICMP with types *130/0, 131/0, 132/0, 143/0* From IP range *fe80::/10* in *wan* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓	Edit Delete

Open ports on router and create ‘new forward rules’:



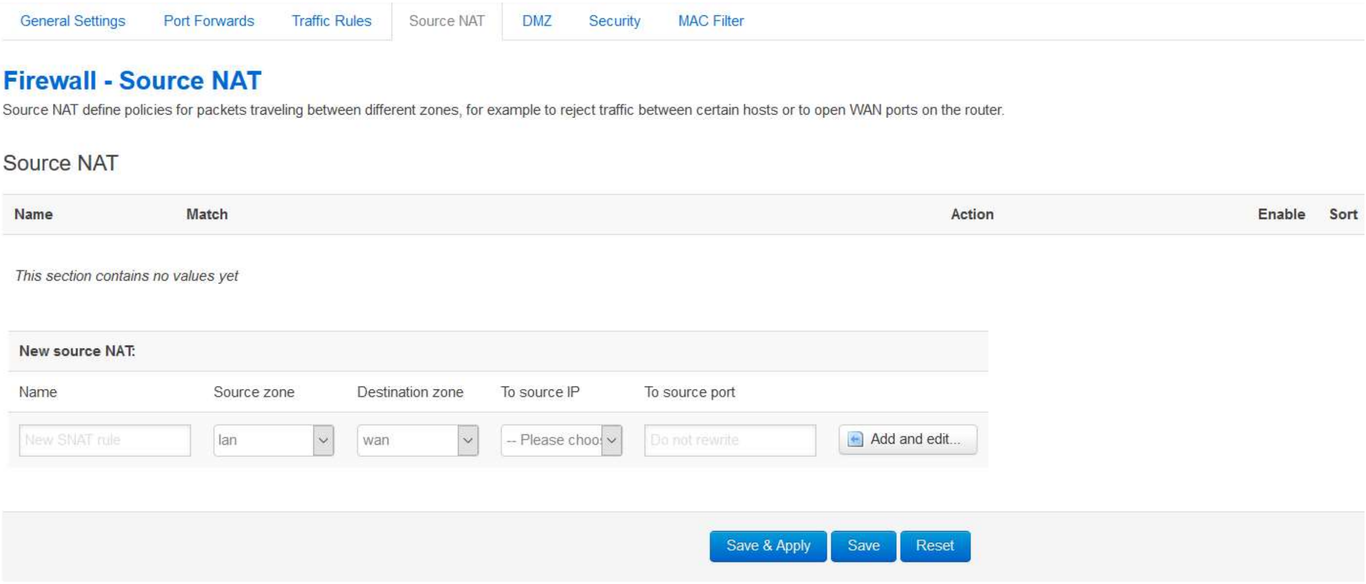
Open ports on router:

Name	Protocol	External port	
New input rule	TCP+UDP		Add

New forward rule:

Name	Source zone	Destination zone	
New forward rule	lan	wan	Add and edit...

Source NAT list and create source NAT rule:



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

Firewall - Source NAT

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

Source NAT

Name	Match	Action	Enable	Sort

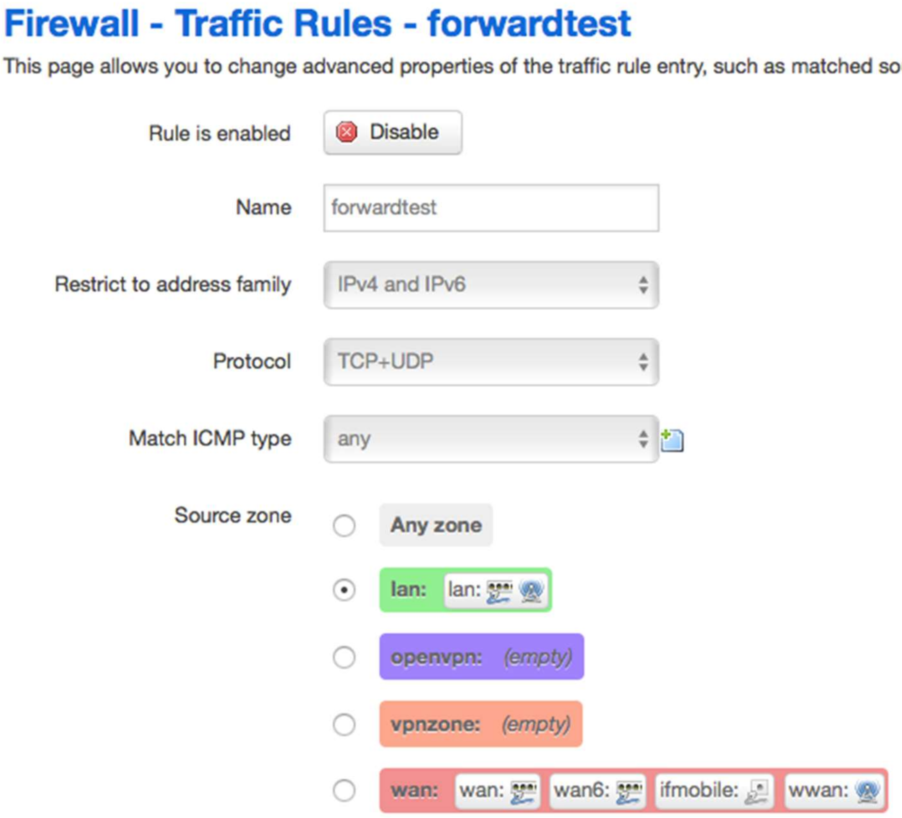
This section contains no values yet

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
New SNAT rule	lan	wan	-- Please choos	Do not rewrite	Add and edit...

Save & Apply | Save | Reset

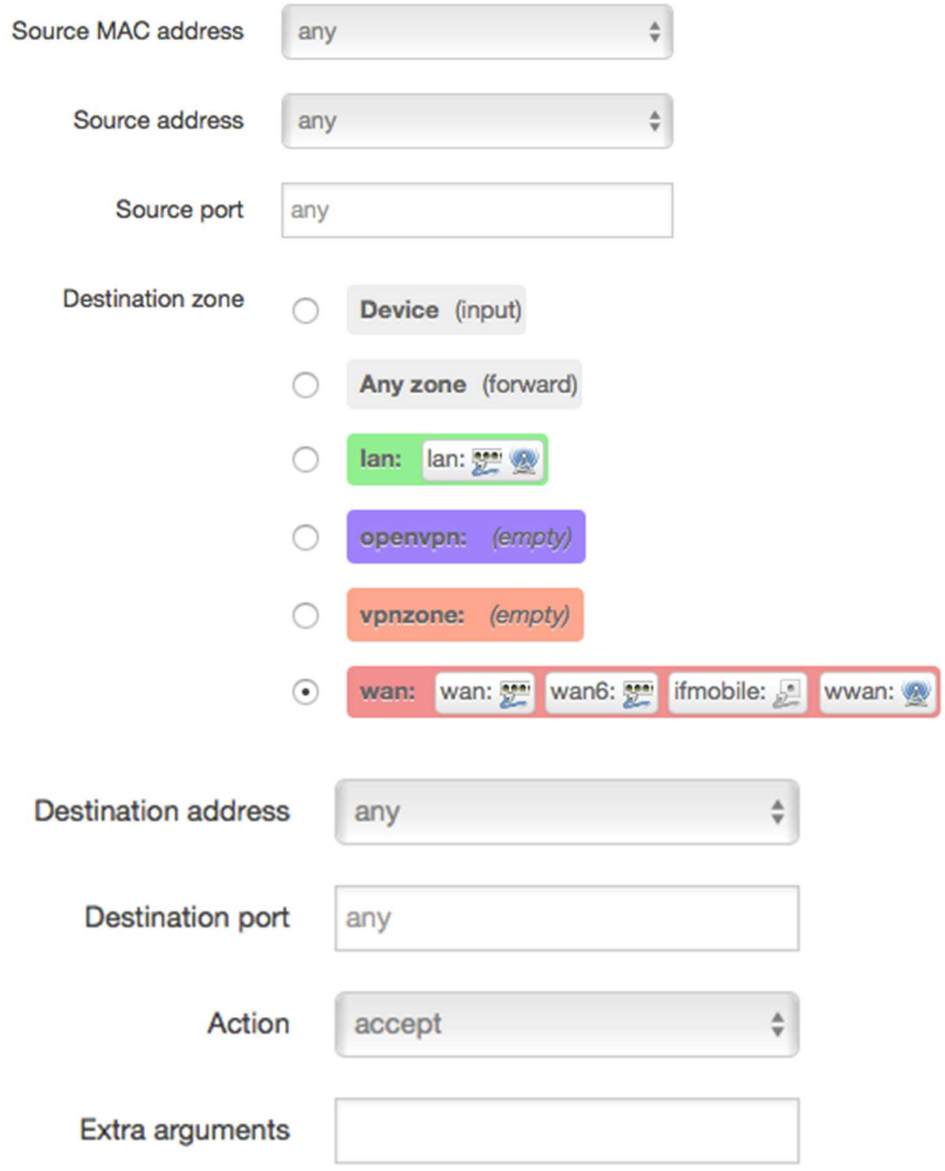
Traffic rule configuration page: This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.



Firewall - Traffic Rules - forwardtest

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

Rule is enabled	Disable
Name	forwardtest
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	○ Any zone ● lan: lan: ○ openvpn: (empty) ○ vpnzone: (empty) ○ wan: wan: wan6: ifmobile: wwan:



Source MAC address: any

Source address: any

Source port: any

Destination zone:
○ Device (input)
○ Any zone (forward)
○ lan: lan:
○ openvpn: (empty)
○ vpnzone: (empty)
● wan: wan: wan6: ifmobile: wwan:

Destination address: any

Destination port: any

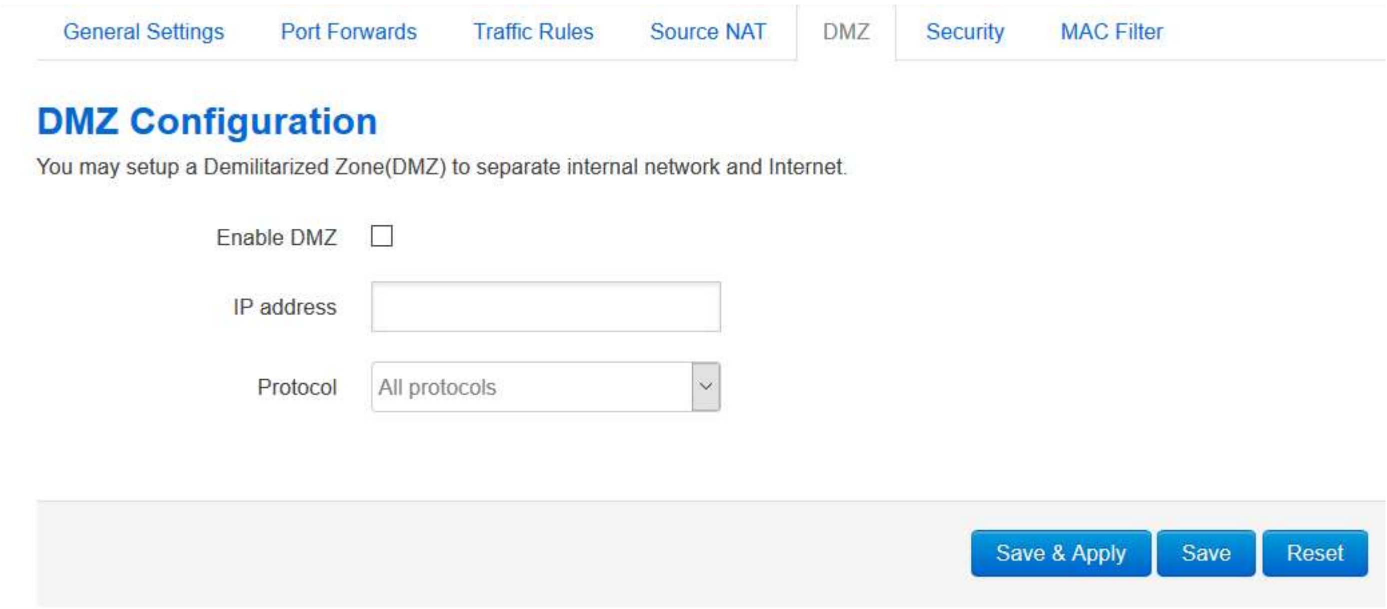
Action: accept

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



DMZ Configuration

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

Enable DMZ □

IP address

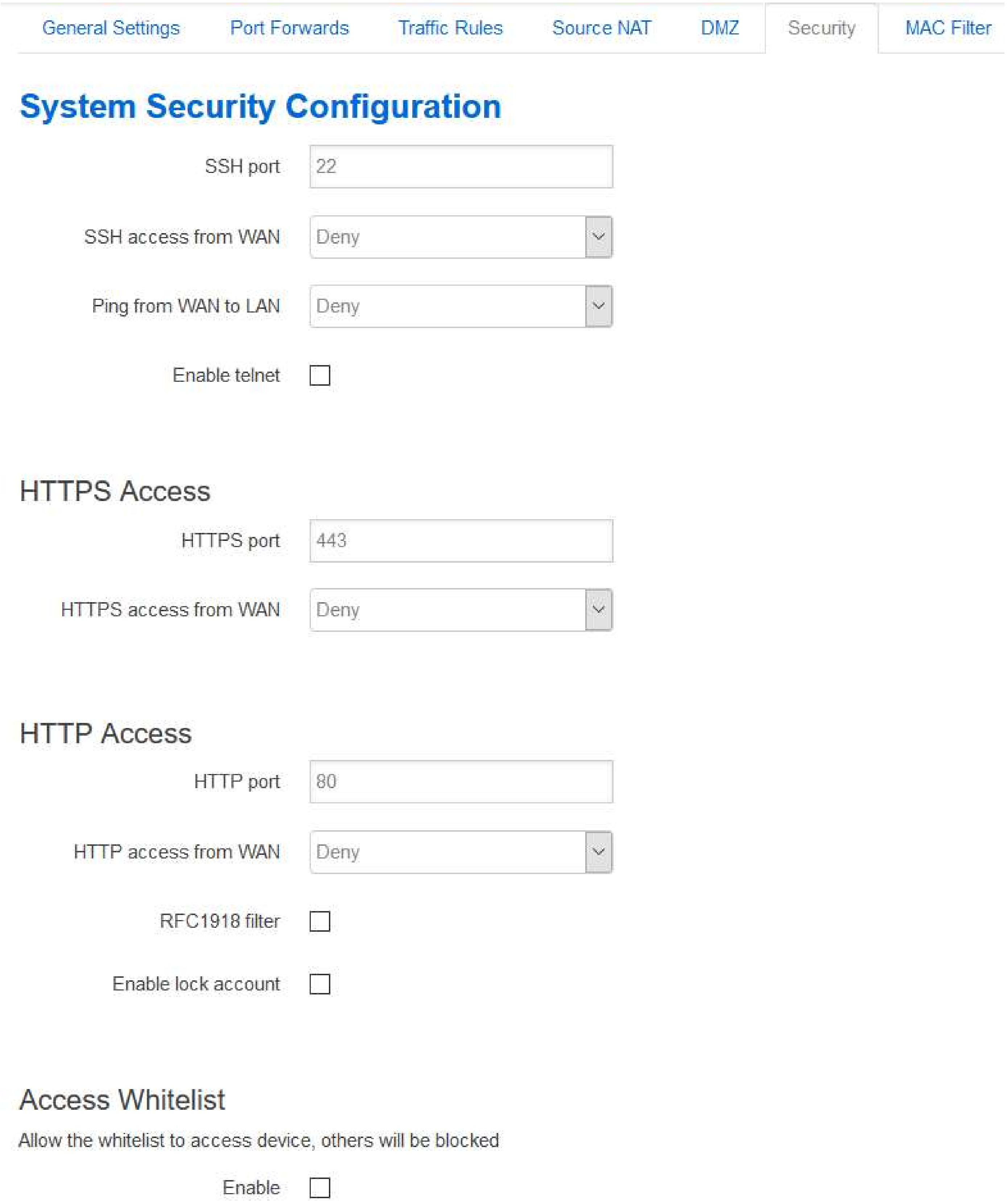
Protocol: All protocols

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



System Security Configuration

SSH port: 22

SSH access from WAN: Deny

Ping from WAN to LAN: Deny

Enable telnet □

HTTPS Access

HTTPS port: 443

HTTPS access from WAN: Deny

HTTP Access

HTTP port: 80

HTTP access from WAN: Deny

RFC1918 filter □

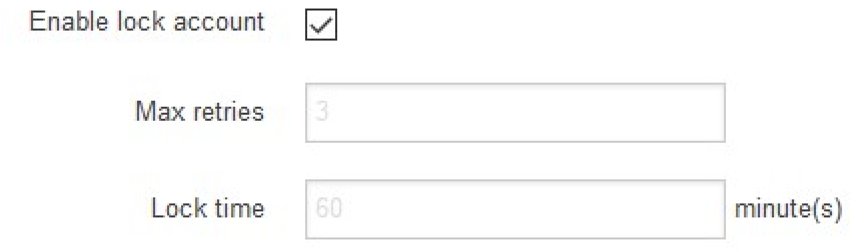
Enable lock account □

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.
- **Enable telnet**: Default is “disable” for security.
- **HTTPS port**: Set HTTPS port. The default is 443.
- **HTTPS access from WAN**: Allow or deny access to the router web management page from the remote side.
- **Remote network**: Any IP Address, Single IP address, Subnet.
- **IP address**: Fill a remote IP address that can access the router’s web management page.
- **Netmask**: 24 means netmask 255.255.255.0, 32 means 255.255.255.255, the value is from 1 to 32.
- **HTTP port**: Set HTTP port. The default is 80.
- **HTTP access from WAN**: Allow or deny access to the router web management page from the remote side.
- **Remote network**: Any IP Address, Single IP address, Subnet.
- **IP address**: Fill a remote IP address that can access the router’s web management page.
- **Netmask**: 24 means netmask 255.255.255.0, 32 means 255.255.255.255, the value is from 1 to 32.
- **RFC1918 filter**: Reject requests from RFC1918 IPs to public server IPs.
- **Enable lock account**: The web account will be locked after a number of unsuccessful login attempts.

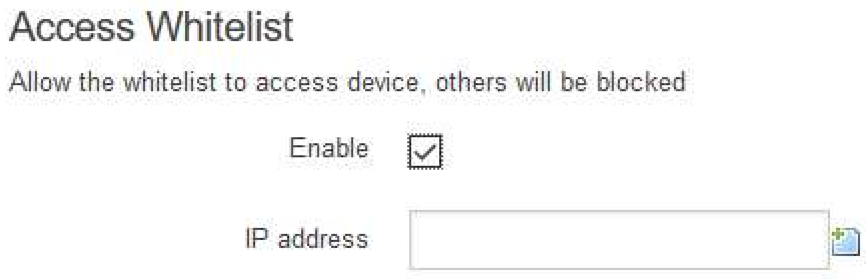


Enable lock account ☑

Max retries 3

Lock time 60 minute(s)

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



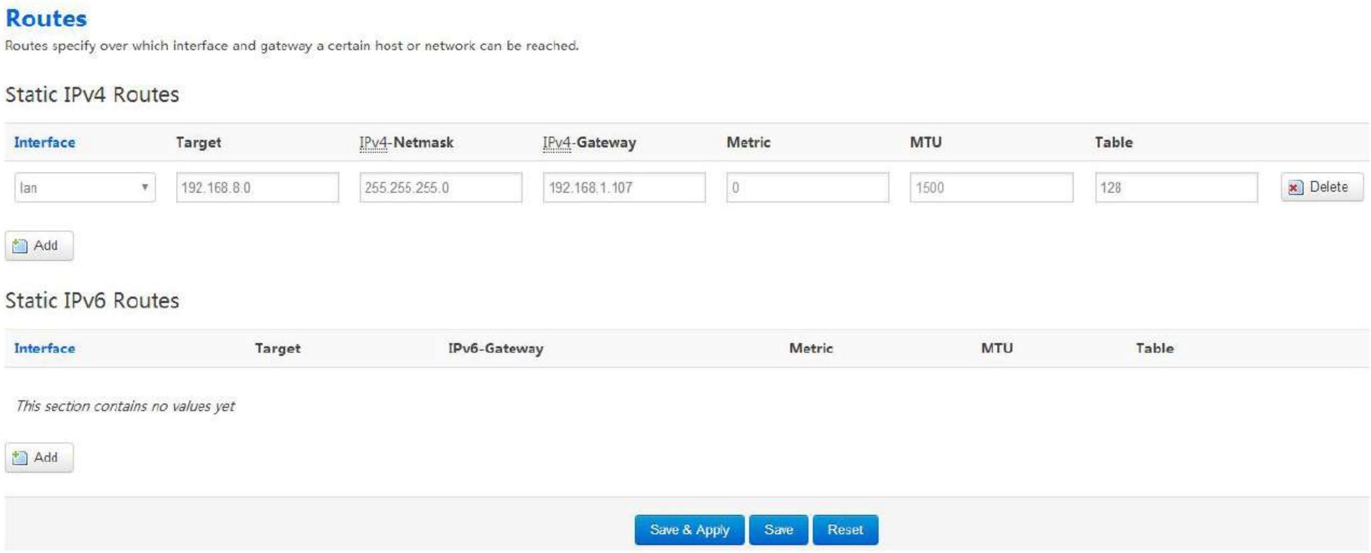
Access Whitelist

Allow the whitelist to access device, others will be blocked

Enable ☑

IP address

3.6.9 Static Routes



Routes

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

Static IPv4 Routes

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

Static IPv6 Routes

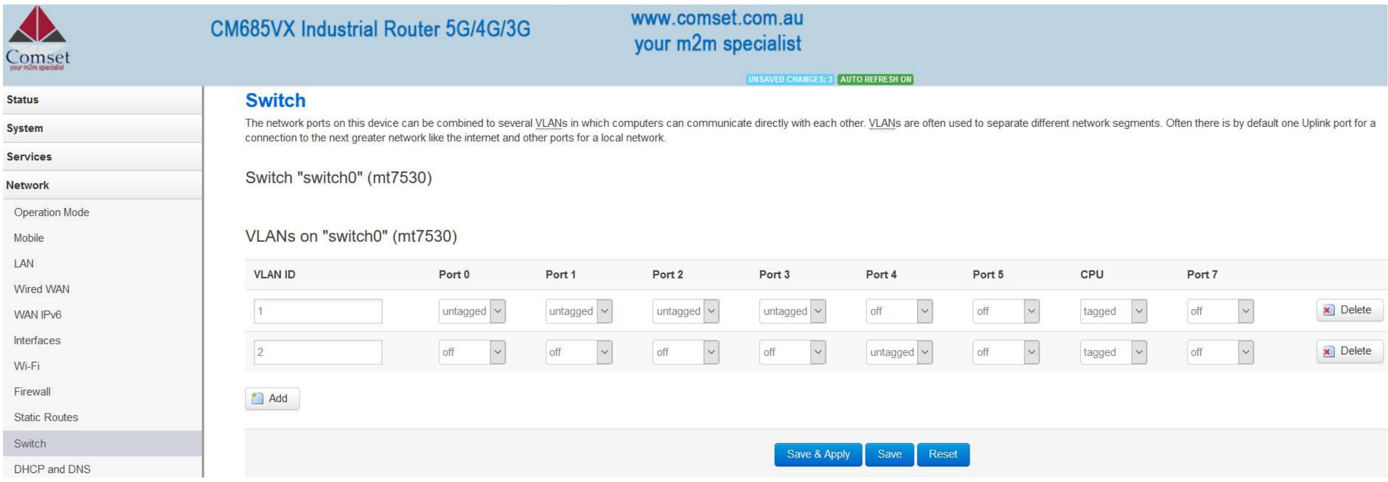
Interface	Target	IPv6-Gateway	Metric	MTU	Table

This section contains no values yet

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

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

3.6.10 Switch



Switch

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

Switch "switch0" (mt7530)

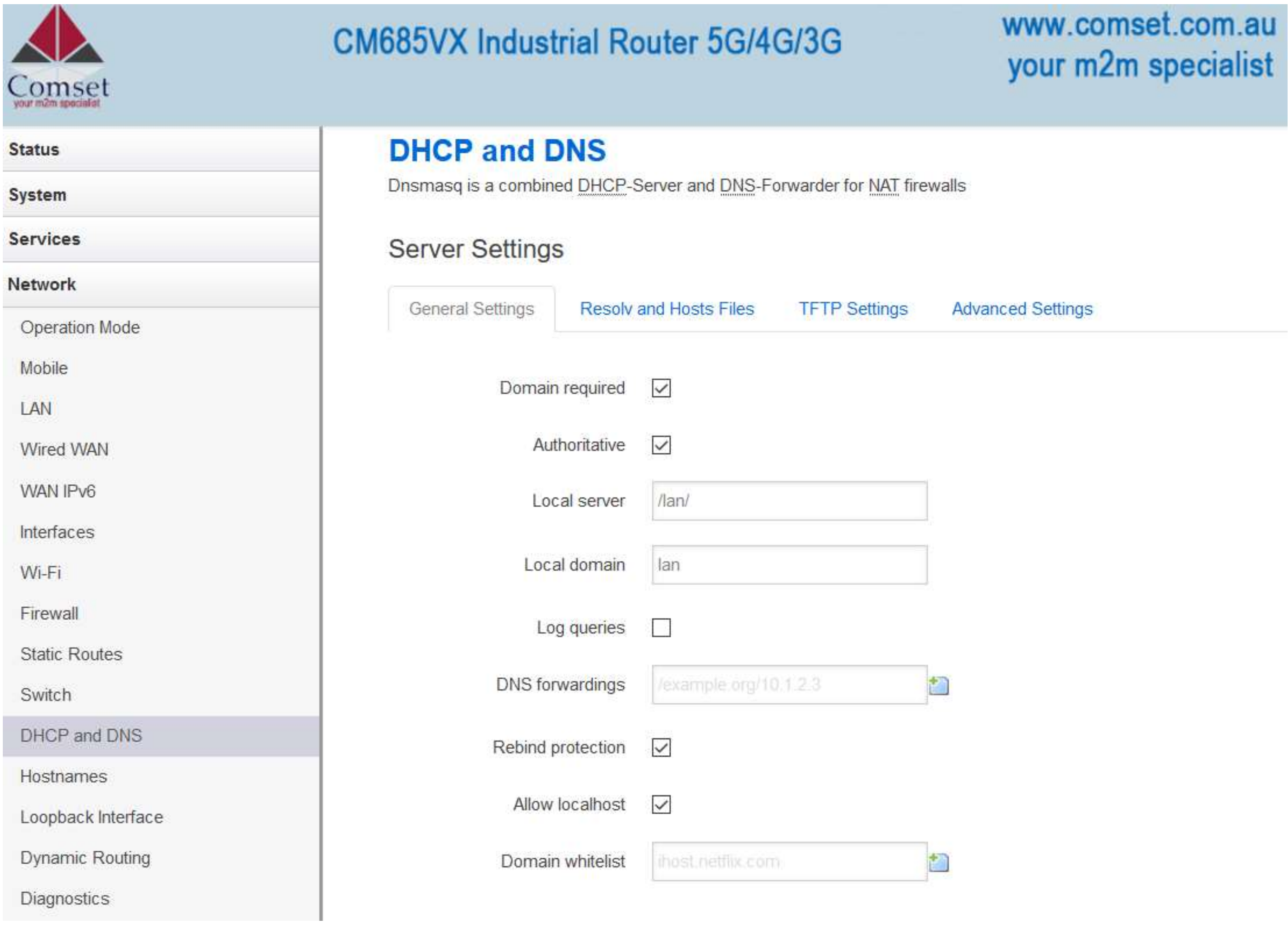
VLANs on "switch0" (mt7530)

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

Note:

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

3.6.11 DHCP and DNS



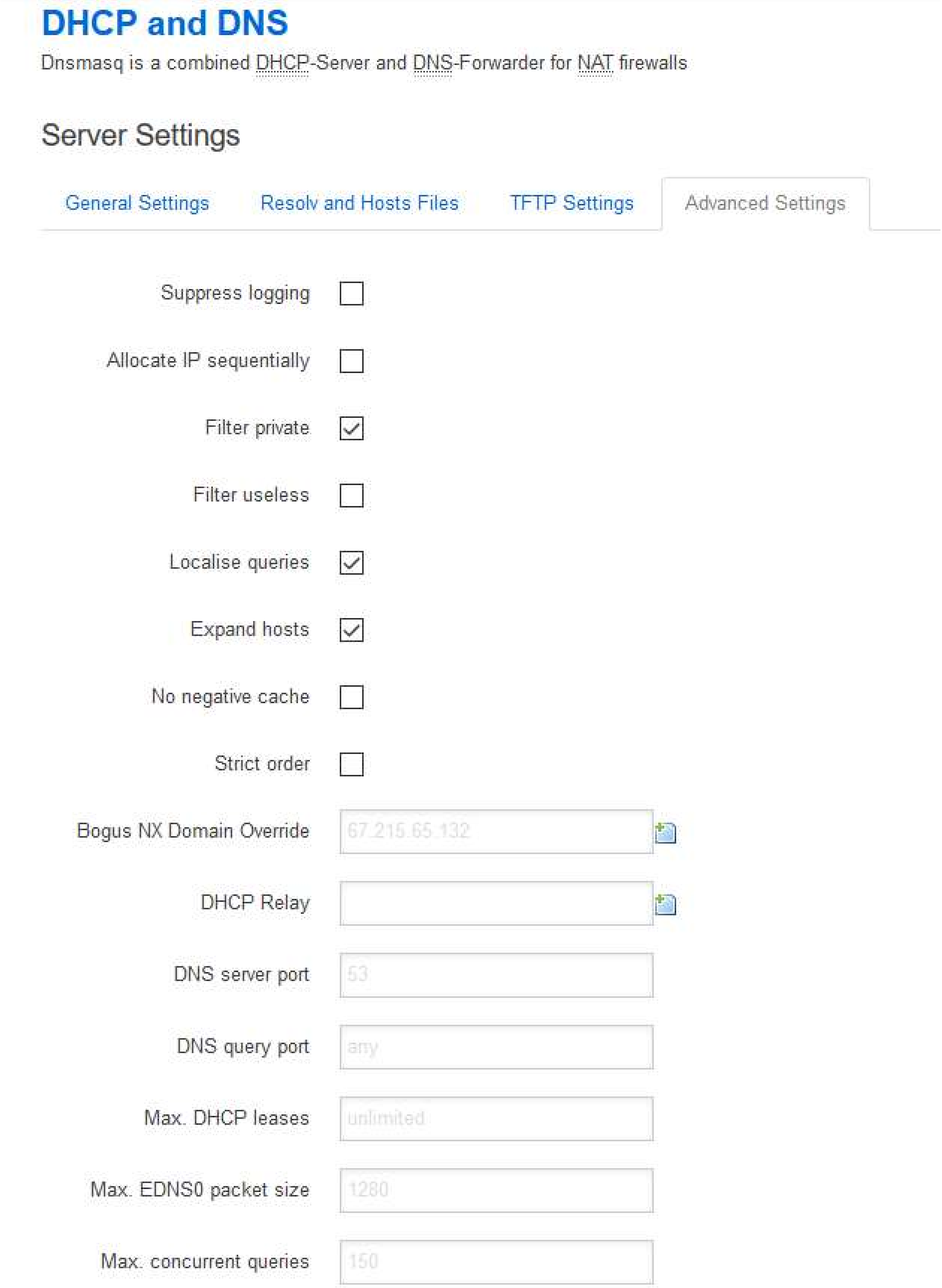
DHCP and DNS

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

Server Settings

Domain required	☑
Authoritative	☑
Local server	/lan/
Local domain	lan
Log queries	□
DNS forwardings	/example.org/10.1.2.3
Rebind protection	☑
Allow localhost	☑
Domain whitelist	ihost.netflix.com

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



DHCP and DNS

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

Server Settings

Suppress logging □

Allocate IP sequentially □

Filter private ☑

Filter useless □

Localise queries ☑

Expand hosts ☑

No negative cache □

Strict order □

Bogus NX Domain Override 67.215.65.132

DHCP Relay

DNS server port 53

DNS query port any

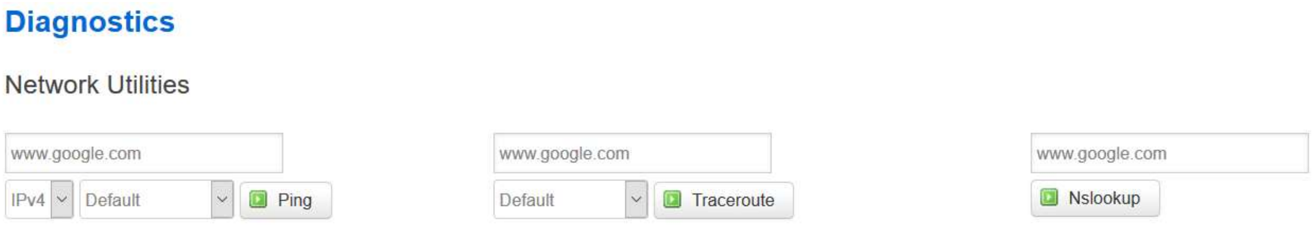
Max. DHCP leases unlimited

Max. EDNS0 packet size 1280

Max. concurrent queries 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

www.google.com

IPv4 Default

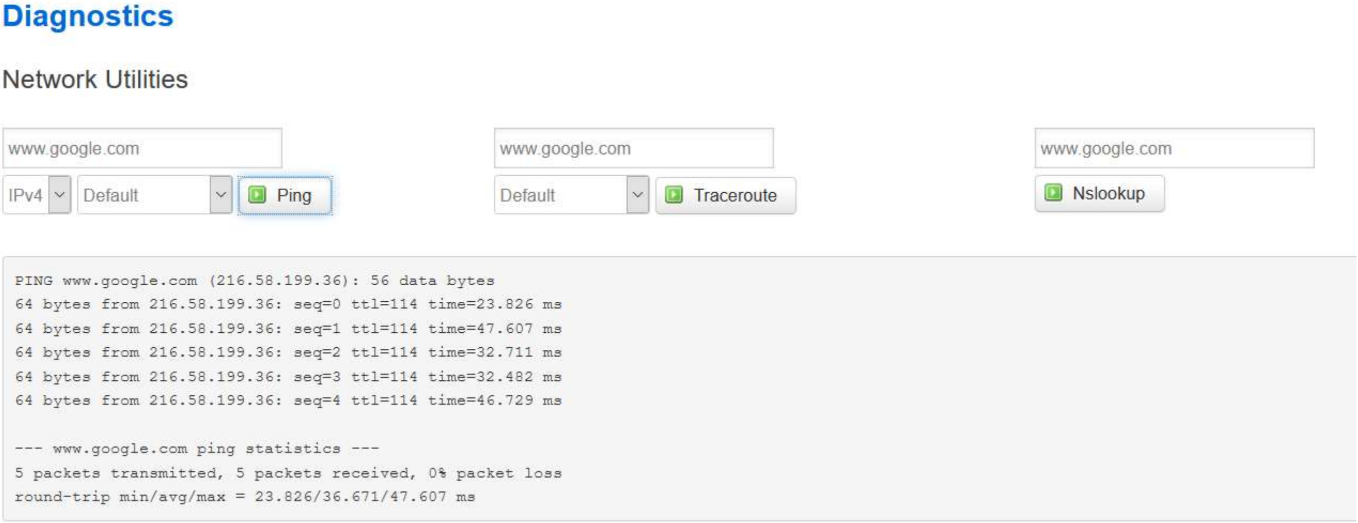
www.google.com

Default

www.google.com

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

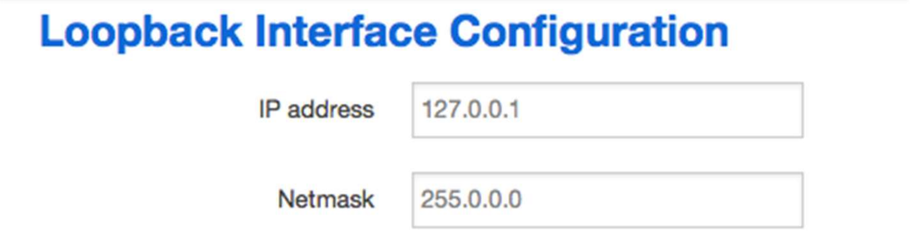
For example if you want to ping www.google.com, type the target domain name or IP address, then click the button “Ping”. Wait a couple of seconds, the result will be shown as below.



```
PING www.google.com (216.58.199.36): 56 data bytes
64 bytes from 216.58.199.36: seq=0 ttl=114 time=23.826 ms
64 bytes from 216.58.199.36: seq=1 ttl=114 time=47.607 ms
64 bytes from 216.58.199.36: seq=2 ttl=114 time=32.711 ms
64 bytes from 216.58.199.36: seq=3 ttl=114 time=32.482 ms
64 bytes from 216.58.199.36: seq=4 ttl=114 time=46.729 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 23.826/36.671/47.607 ms
```

3.6.13 Loopback Interface



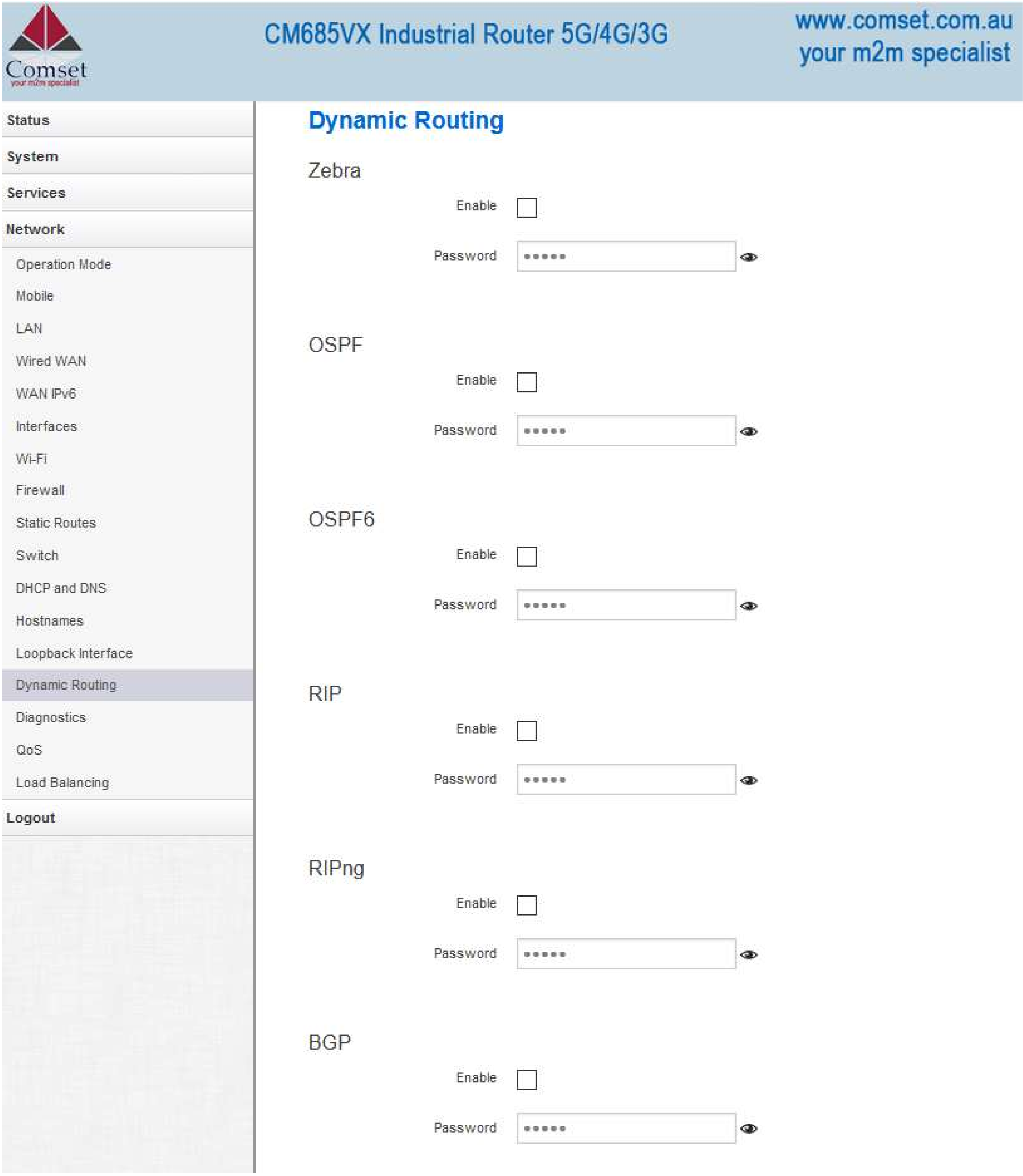
IP address: 127.0.0.1

Netmask: 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

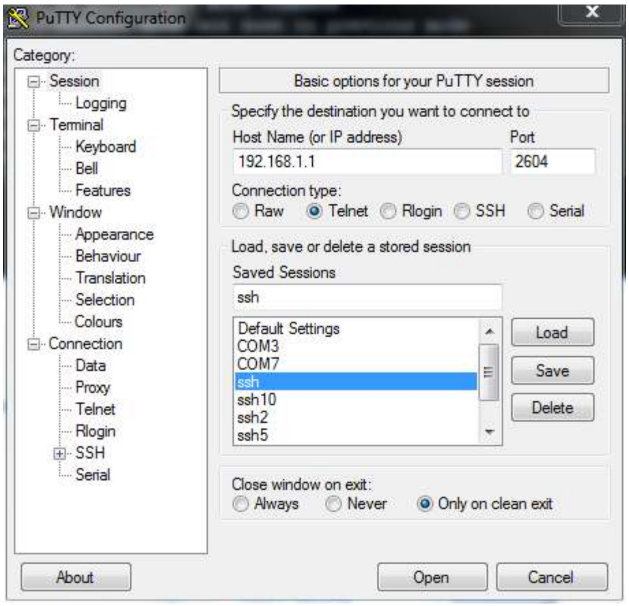
Enable □

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:



Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.1

Port: 2604

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

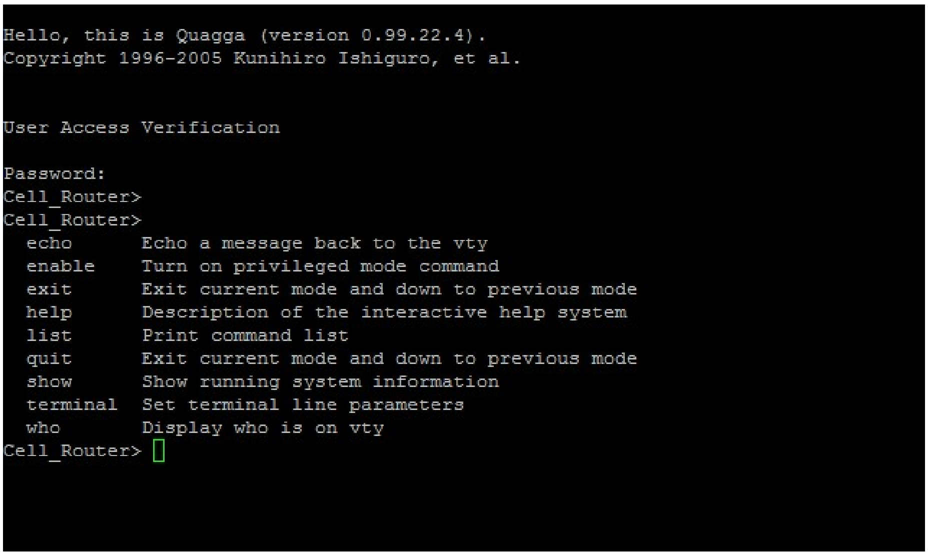
Load, save or delete a stored session

Saved Sessions: ssh

Default Settings
COM3
COM7
ssh
ssh10
ssh2
ssh5

Close window on exit: ○ Always ○ Never ● Only on clean exit

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



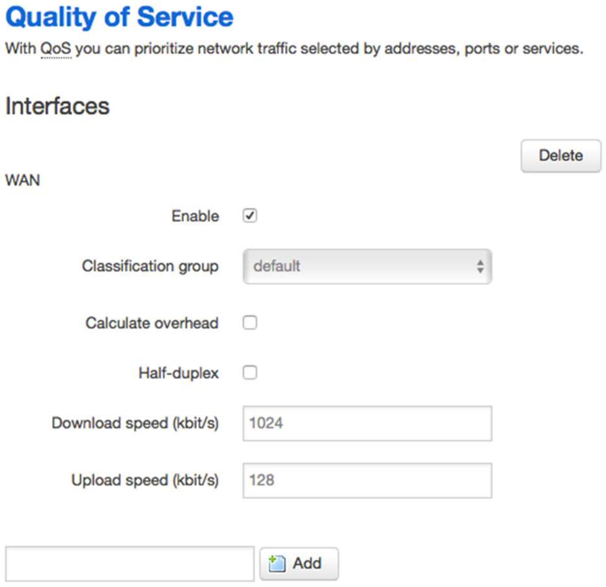
```
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

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

3.6.15 QoS

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



Quality of Service

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

Interfaces

WAN

Enable ☑

Classification group: default

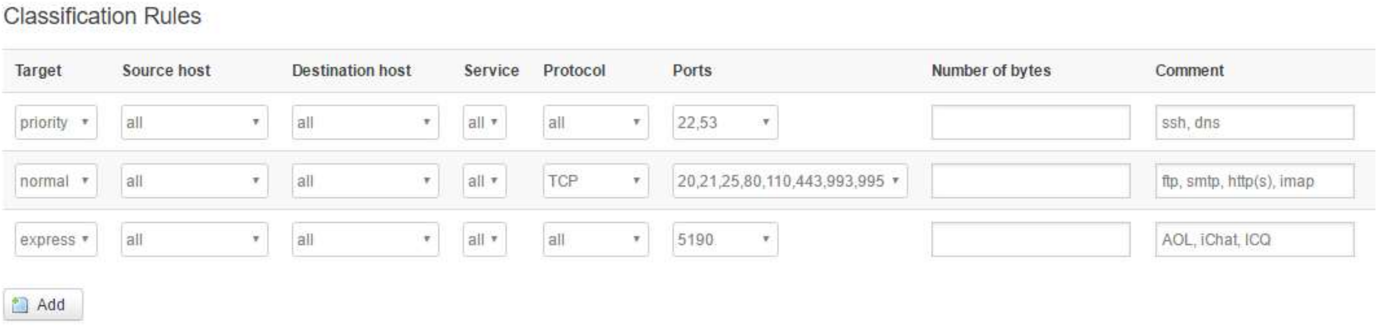
Calculate overhead □

Half-duplex □

Download speed (kbit/s): 1024

Upload speed (kbit/s): 128

- **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.