Dual Modem Dual-Band WiFi Gigabit Router

User Manual

CM770W-6

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

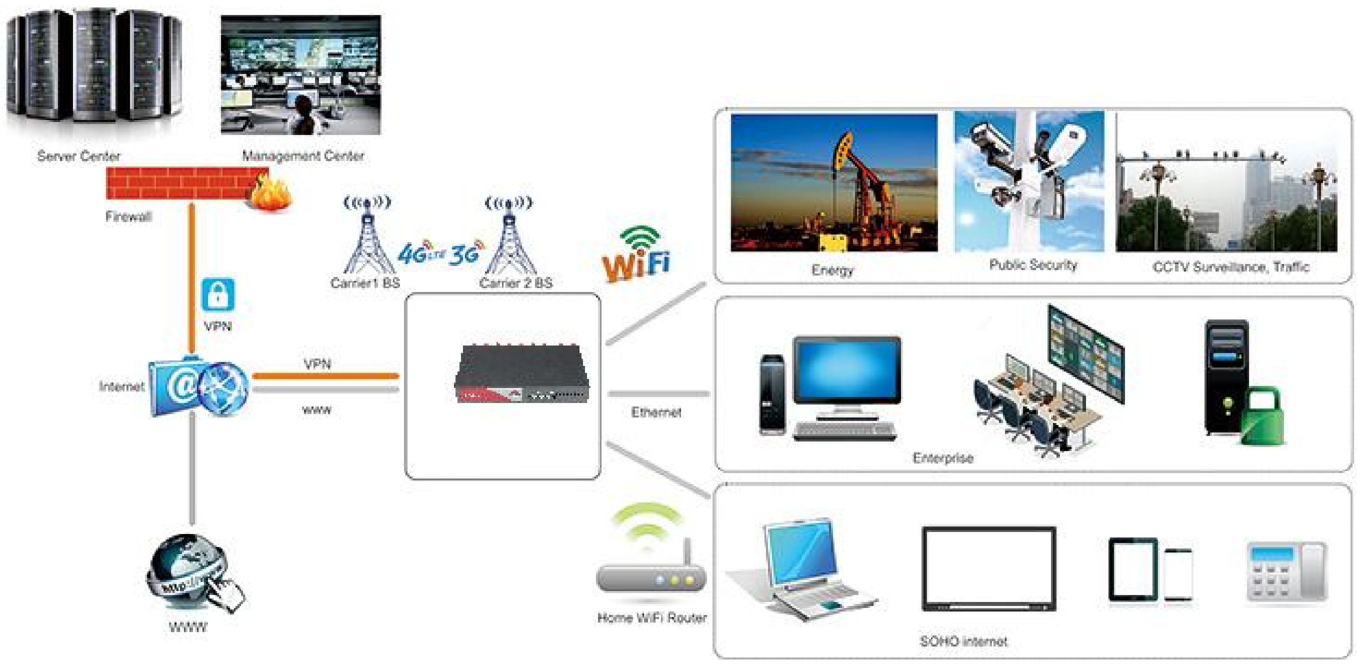
The Comset CM770W-6 is a premium grade modem router with two built-in 4G LTE CAT 6 modems that allow backup redundancy (hot swap) between modem 1 and modem 2 to ensure internet continuity for mission critical applications. With four Gigabit Ethernet ports and concurrent 2.4GHz and 5GHz dual band WiFi, the CM770W-6 provides a powerful and rapidly deployable internet solution to commercial customers and small to medium businesses.

The Comset CM770W-6 is an innovative router powered by a Dual Core CPU. It features dual SIM card slots for backup redundancy, 4 x Gigabit LAN ports for fast wired connections, 1 Gigabit WAN/LAN port for automatic failover between NBN/ADSL and 4G LTE, 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 3G/4G network.

The innovative design, easy integration and rich built-in features make the CM770W-6 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 CM770W-6 3G/4G/4GX Router is suitable for a wide range of machine-to-machine applications (M2M). A good example is the connection of IP Cameras and M2M devices back to a server over a secure 4G connection using a secure VPN IPSEC tunnel.



1.3 Features

The CM770W-6 supports the following:

- Multi-band LTE CAT 6 4G/4GX, DC-HSPA+, HSPA+, HSPA, UMTS
- Load balancing between 4G LTE Modem-1, 4G LTE Modem-2 and fixed WAN ADSL/NBN
- 4 x Gigabit Ethernet LAN RJ45 ports & 1 x Gigabit Ethernet WAN/LAN RJ45 port
- Dual-band, dual concurrent WiFi (802.11 a/b/g/n/ac, 2.4Ghz + 5Ghz)
- USB3.0 port and Micro SD slot
- LTE Advanced with SIM-based auto-carrier selection
- 9 x SMA standard detachable antennas included: 4 x magnetic base cellular antennas, 4 x rubber dual band WiFi antennas and 1 x GPS antenna (CM770W-6G model)
- Optimised EMC design
- TR-069, 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

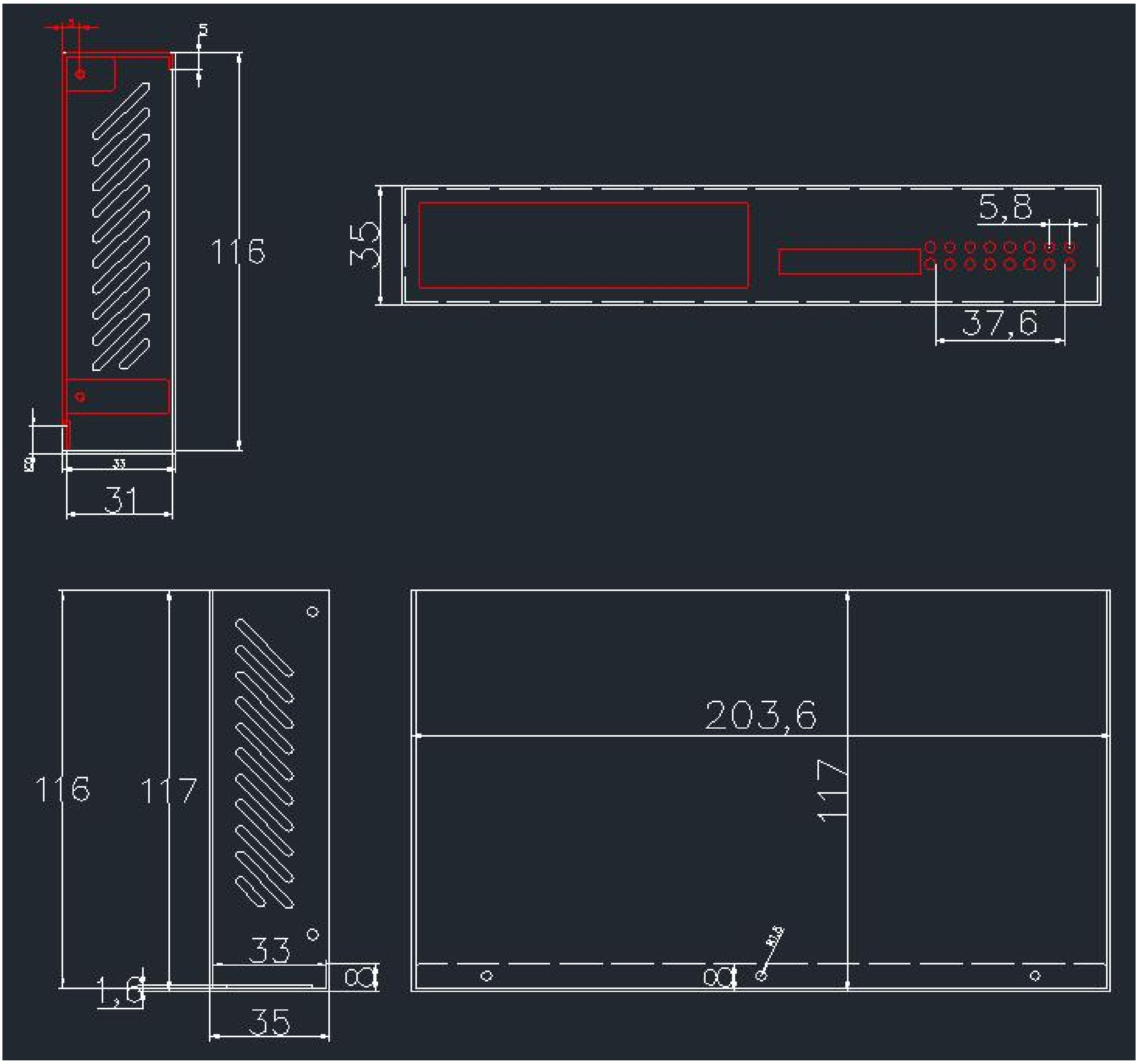
- Wide range power input (5-40VDC)
- Dual power input / power failover
- Smart power management
- Inbuilt GPS/GNSS (CM770W-6G model)
- 2 x Serial ports
- 4 x Digital Input ports, that can also be used as Digital Output ports
- User friendly set-up wizard for easy configuration and setup
- Network traffic real-time graphs
- Network Diagnostic Tools (Ping, Traceroute and NSLookup)
- Secure guest WiFi to passengers
- Advanced security, VPN, and stateful firewall to protect sensitive data
- Robust Metal Case
- Desktop, Wall-mount and Din-rail mount

Chapter 2

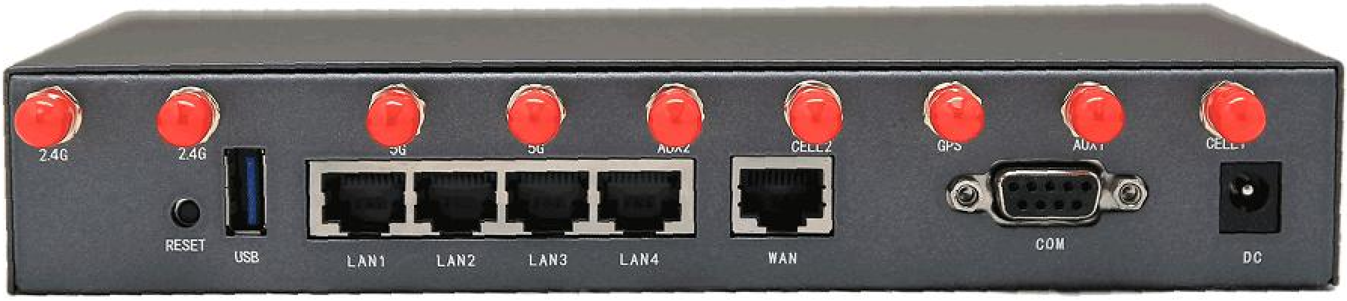
2 Hardware Installation

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

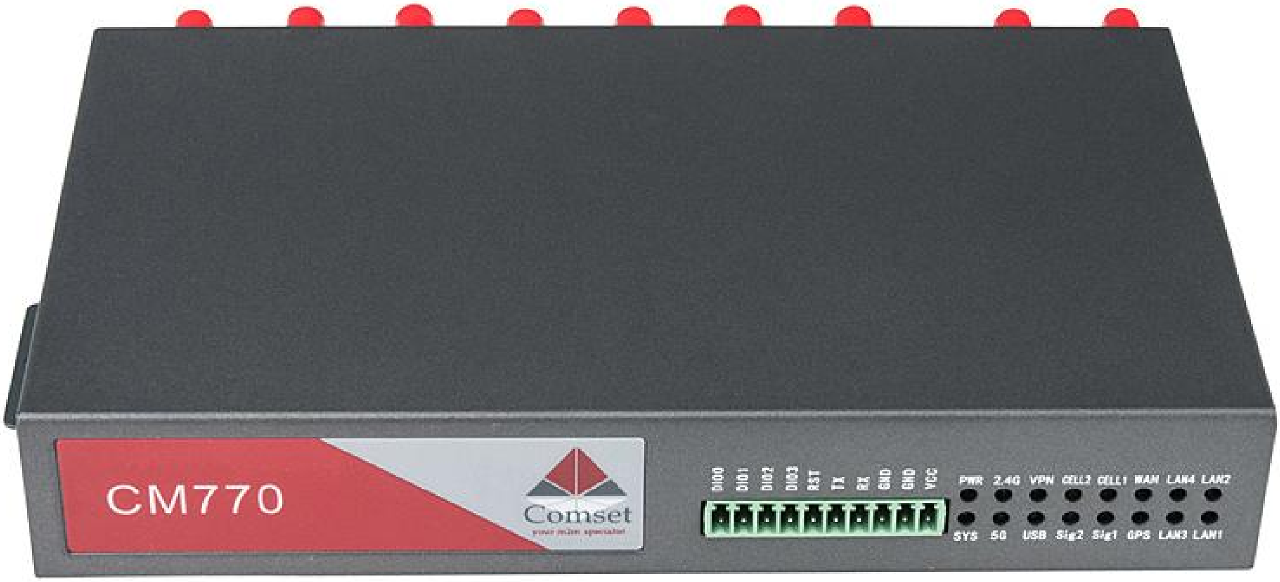
2.1 Overall Dimensions



2.2 Ports



LAN1-LAN4: LAN RJ45 10/100/1000 Ethernet ports
WAN: WAN RJ45 10/100/1000 Ethernet port
RESET: System reset button
DC: DC power socket. DC5~40V
USB: USB3.0 host port
COM: Serial DB9 port



VCC: DC wire positive pole. DC5~40V
GND: DC wire ground
GND: Serial ground
RX: Serial receive
TX: Serial transmit
RST: Reset

DIO0: digital I/O port 0
DIO1: digital I/O port 1
DIO2: digital I/O port 2
DIO3: digital I/O port 3

Antenna Connection Table

Antenna Connectors	Remarks
Cell1	for cell1 main antenna
Aux1	for cell1 auxiliary antenna
Cell2	for cell2 main antenna
Aux2	for cell2 auxiliary antenna
2.4G	for 2.4GHz WiFi antenna x 2
5G	for 5GHz WiFi antenna x 2
GPS	for GPS antenna (CM770W-6G model)

2.3 Powering up the CM770W-6

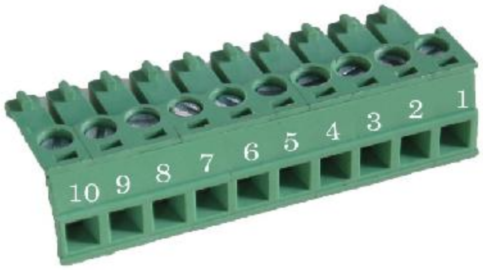
Please ensure the SIM cards are inserted, and the antennas are connected before powering up the router.

2.4 SIM/UIM cards

If your router has a SIM/UIM card cover, please remove it and have the SIM cards properly inserted.

2.5 Terminal block

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



.

Attention:

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

PIN	Signal	Description	Note
1	VCC	+5-40V DC Input (+5~60V optional)	Current: 12V/1A
2	GND	Ground	
3	GND	Serial Ground	
4	RX	Receive Data	
5	TX	Transmit Data	
6	RST	Reset	The Reset Pin has the same function as the reset button. Simply short the RST pin with the GND Pin and hold for 3 sec and the device will restore to factory settings. 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 Port4 and Port5.

2.6 Grounding

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

2.7 Power Supply

The CM770W-6 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 set-up normal
	Off or still on after 25 seconds	System set-up failure
LAN 1-4	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

CELL1 CELL2	On	Cell connection is Up and now you have access to the Internet
2.4G 5G	On	WiFi Enabled
	Off	WiFi Disabled
WAN	Blinks	Ethernet data transmission
	Off	No Ethernet connection
	On	Ethernet is connected
PWR	On	Power is on
USB	On	External USB device is connected
GPS	On	GPS is online
Sig1 Sig2	Off	No signal, or signal checking is not ready
	Blinks once every 2 seconds	Signal bar is 1
	Blinks once every second	Signal bar is 2
	Blinks once every half a second	Signal bar is 3

Chapter 3

3 Software configuration

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

3.1 Overview

The CM770W-6 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

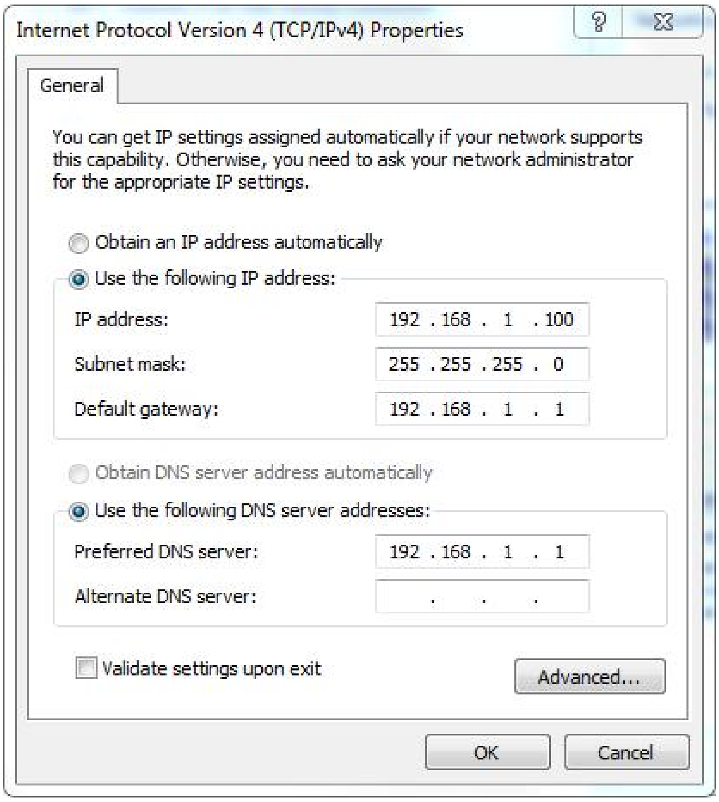
The router's default parameters are:

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

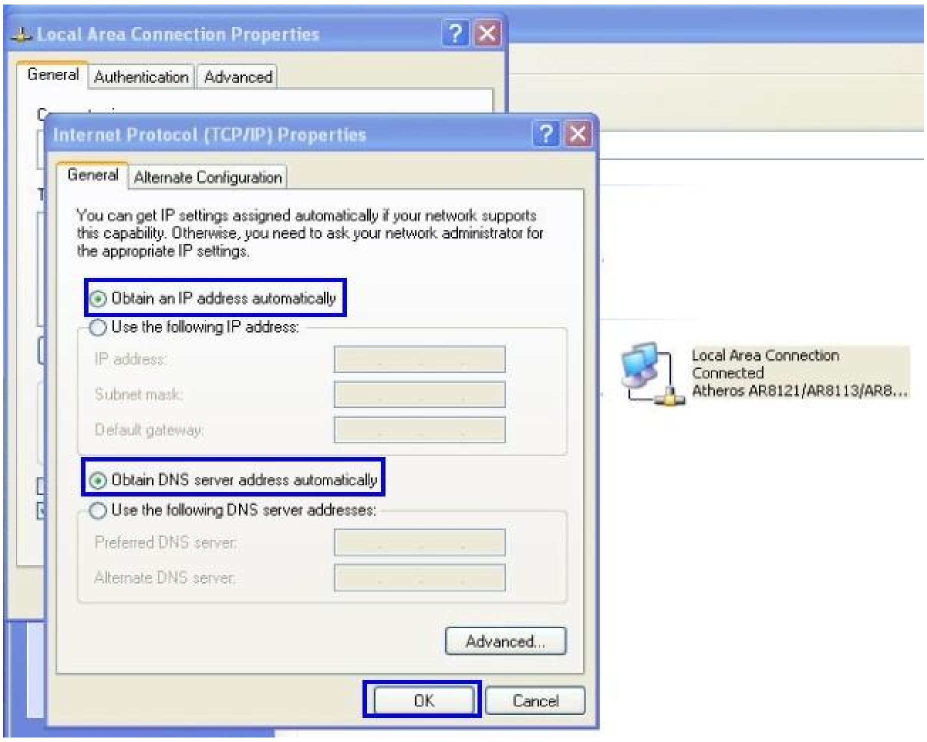
● Use the following DNS server addresses:

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.



Local Area Connection Properties

Internet Protocol (TCP/IP) Properties

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

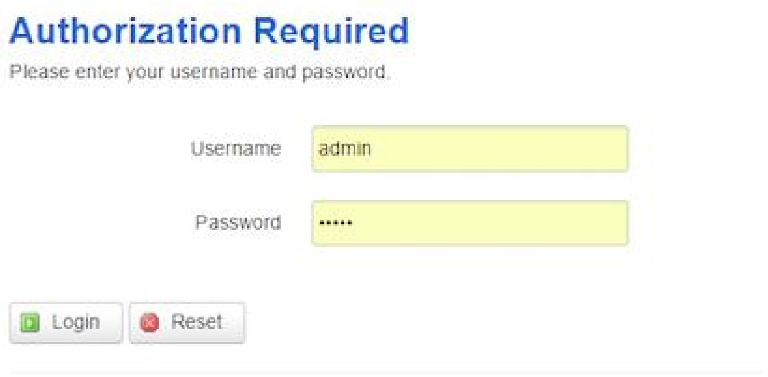
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

3.2.2 Log into the router

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



Authorization Required

Please enter your username and password.

Username admin

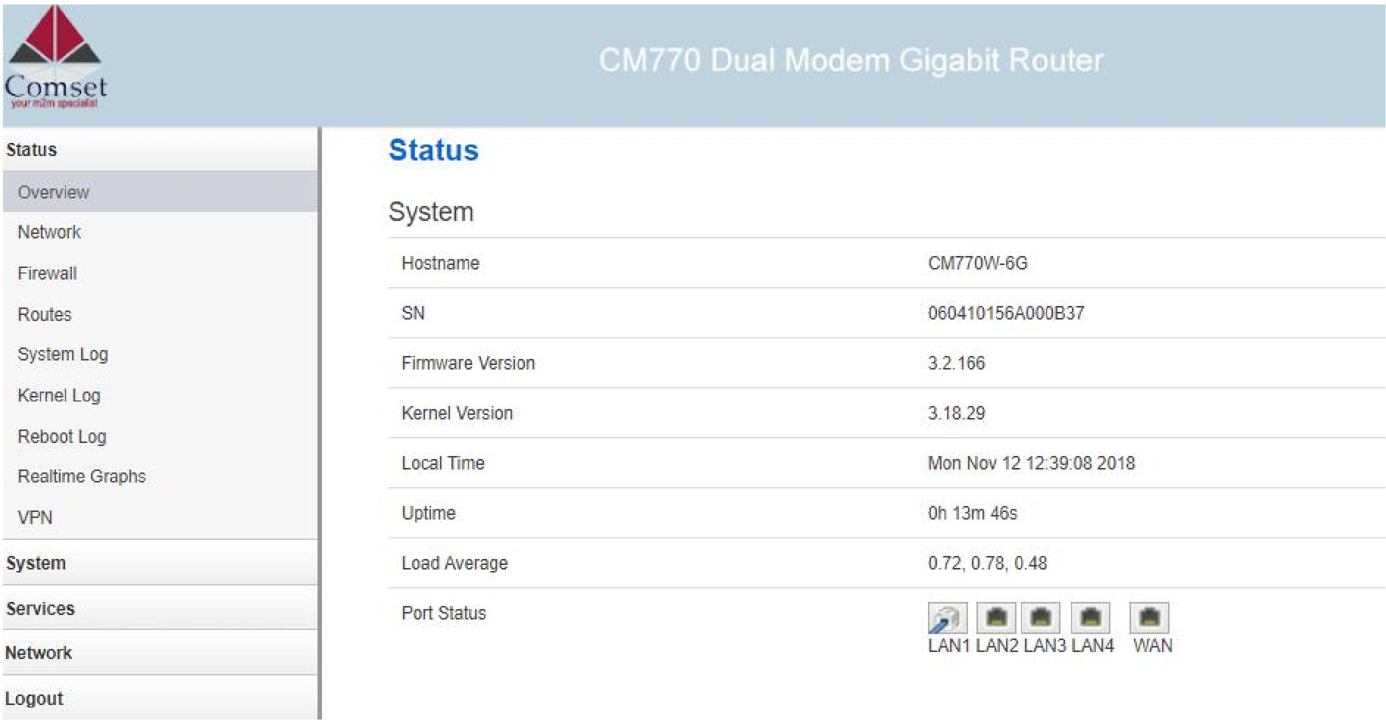
Password •••••

<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

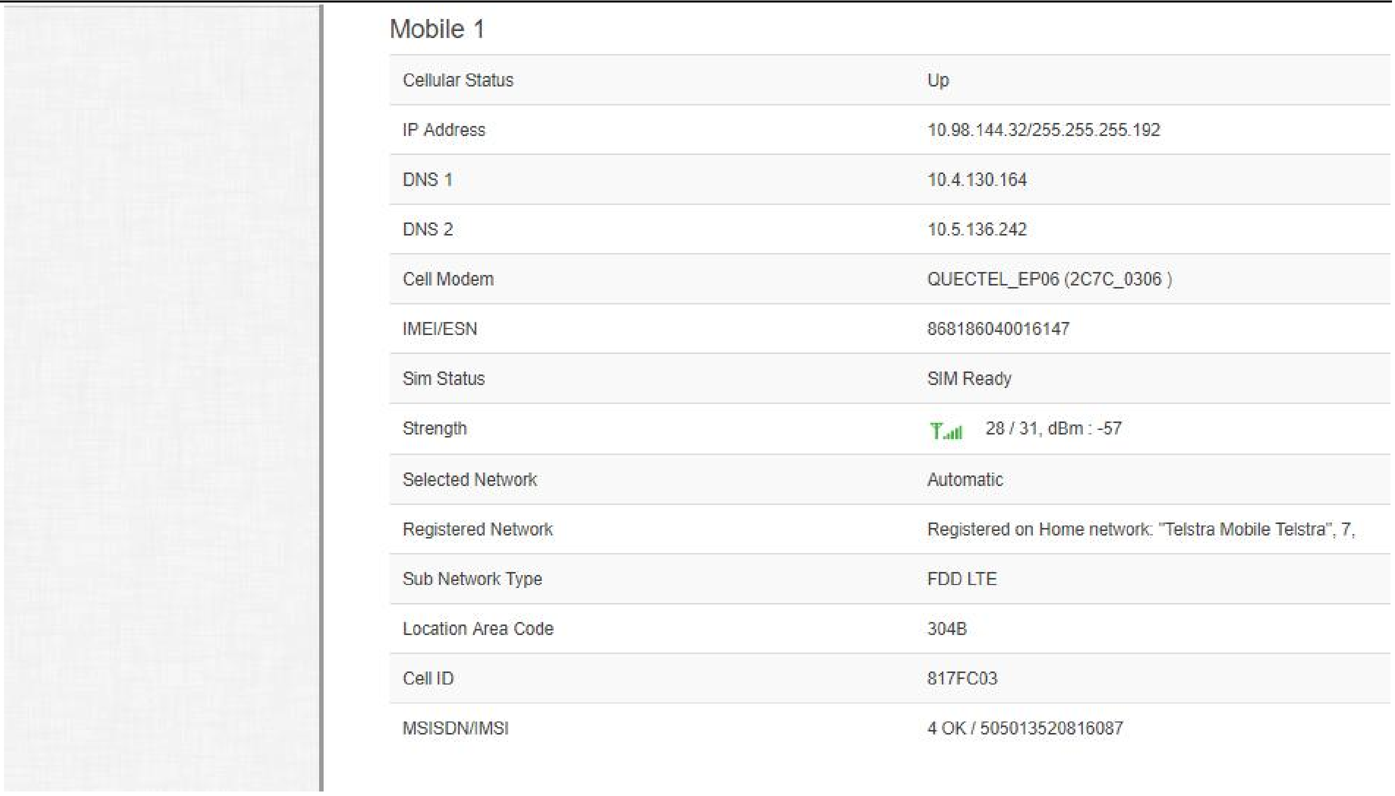
Click “Status” in the navigation bar, and then click “Overview”.



Status

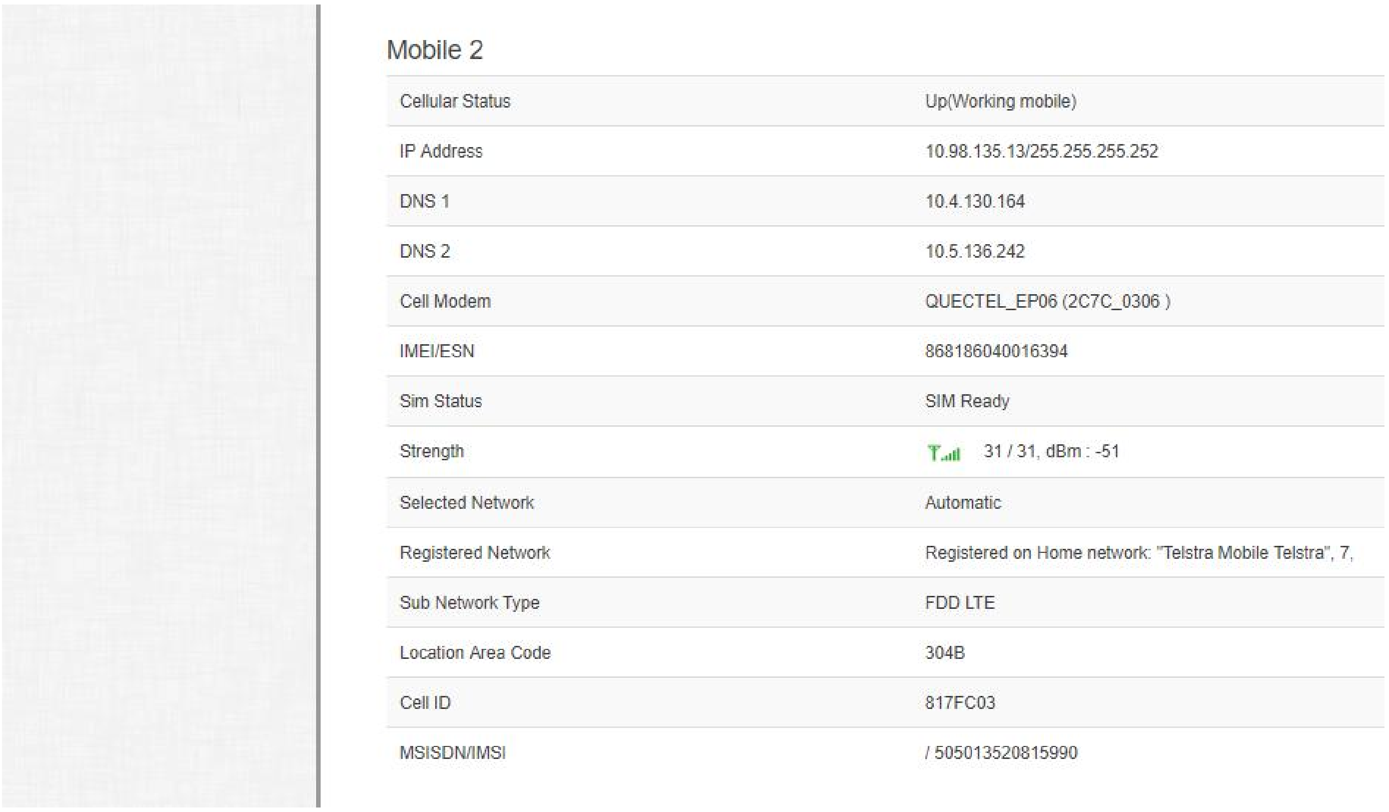
System

Hostname	CM770W-6G
SN	060410156A000B37
Firmware Version	3.2.166
Kernel Version	3.18.29
Local Time	Mon Nov 12 12:39:08 2018
Uptime	0h 13m 46s
Load Average	0.72, 0.78, 0.48
Port Status	LAN1 LAN2 LAN3 LAN4 WAN



Mobile 1

Cellular Status	Up
IP Address	10.98.144.32/255.255.255.192
DNS 1	10.4.130.164
DNS 2	10.5.136.242
Cell Modem	QUECTEL_EP06 (2C7C_0306)
IMEI/ESN	868186040016147
Sim Status	SIM Ready
Strength	📶 28 / 31, dBm : -57
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra Mobile Telstra", 7,
Sub Network Type	FDD LTE
Location Area Code	304B
Cell ID	817FC03
MSISDN/IMSI	4 OK / 505013520816087



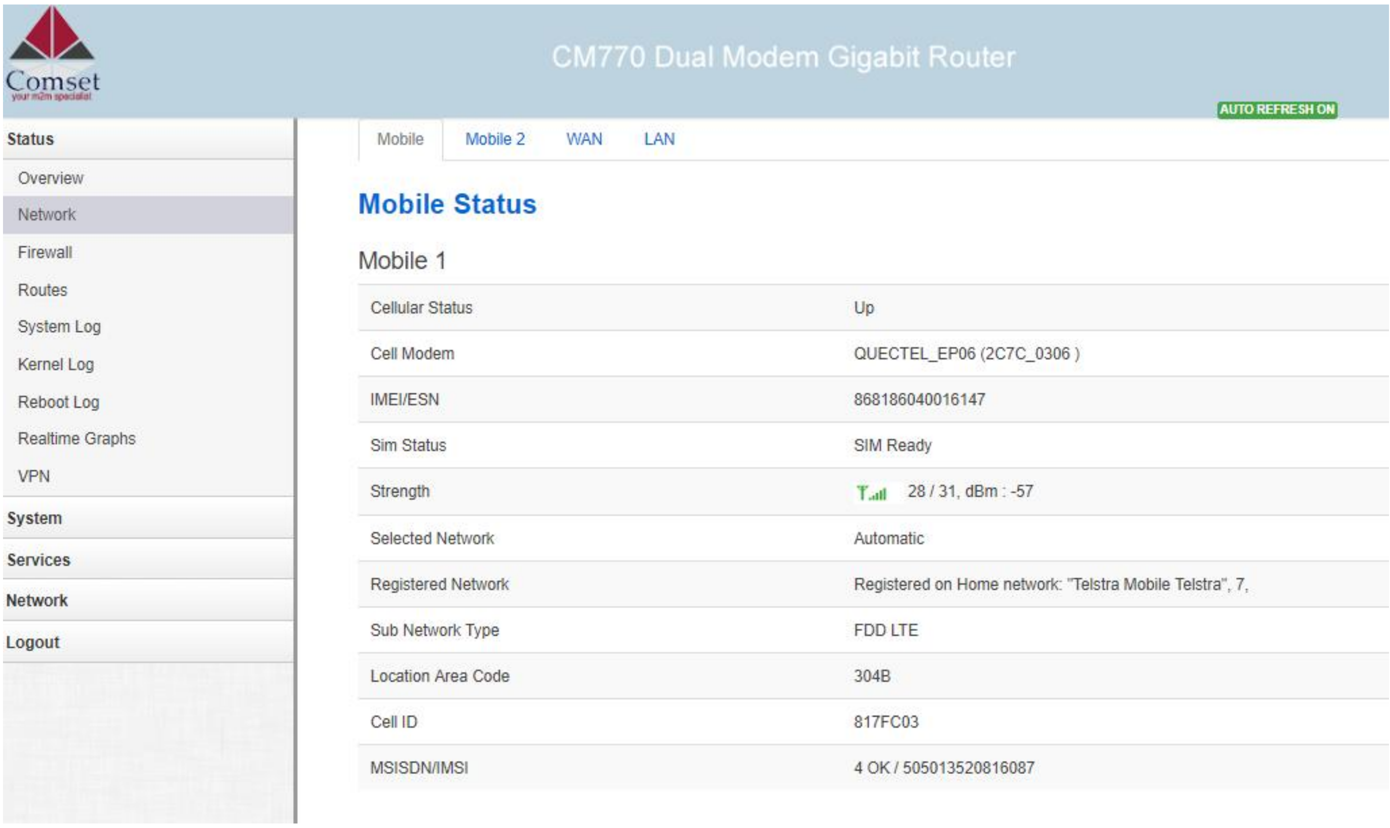
Mobile 2

Cellular Status	Up(Working mobile)
IP Address	10.98.135.13/255.255.255.252
DNS 1	10.4.130.164
DNS 2	10.5.136.242
Cell Modem	QUECTEL_EP06 (2C7C_0306)
IMEI/ESN	868186040016394
Sim Status	SIM Ready
Strength	📶 31 / 31, dBm : -51
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra Mobile Telstra", 7,
Sub Network Type	FDD LTE
Location Area Code	304B
Cell ID	817FC03
MSISDN/IMSI	/ 505013520815990

3.3.2 Network status

The Network status page consists of 4 tabs, detailing information about the cell mobile interface Mobile 1, cell mobile interface Mobile 2, WAN and LAN.

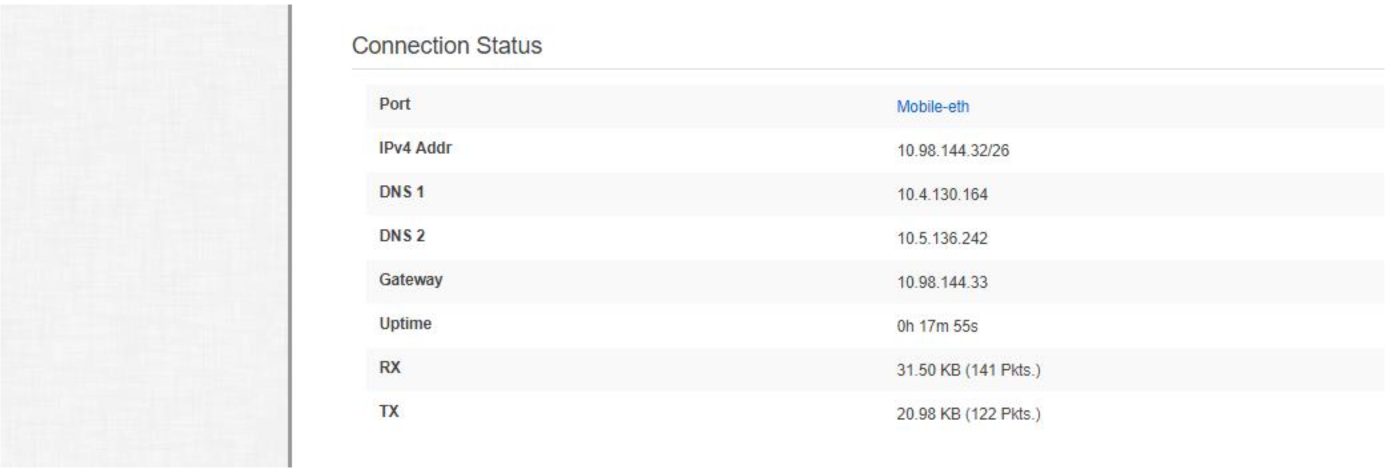
Cell mobile interface Mobile 1 page:



Mobile Status

Mobile 1

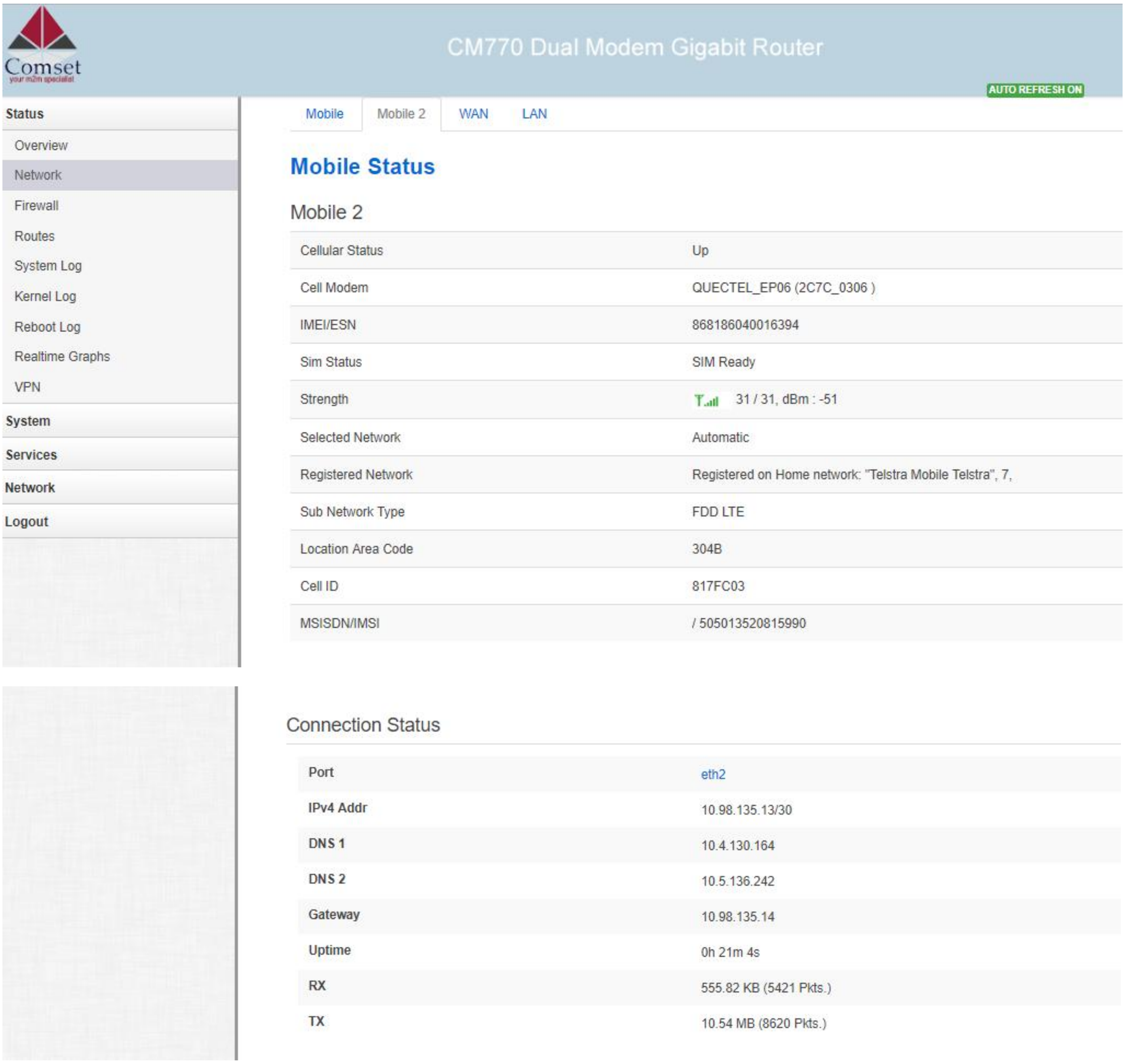
Cellular Status	Up
Cell Modem	QUECTEL_EP06 (2C7C_0306)
IMEI/ESN	868186040016147
Sim Status	SIM Ready
Strength	28 / 31, dBm : -57
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra Mobile Telstra", 7,
Sub Network Type	FDD LTE
Location Area Code	304B
Cell ID	817FC03
MSISDN/IMSI	4 OK / 505013520816087



Connection Status

Port	Mobile-eth
IPv4 Addr	10.98.144.32/26
DNS 1	10.4.130.164
DNS 2	10.5.136.242
Gateway	10.98.144.33
Uptime	0h 17m 55s
RX	31.50 KB (141 Pkts.)
TX	20.98 KB (122 Pkts.)

Cell mobile interface Mobile 2 page:



Mobile Status

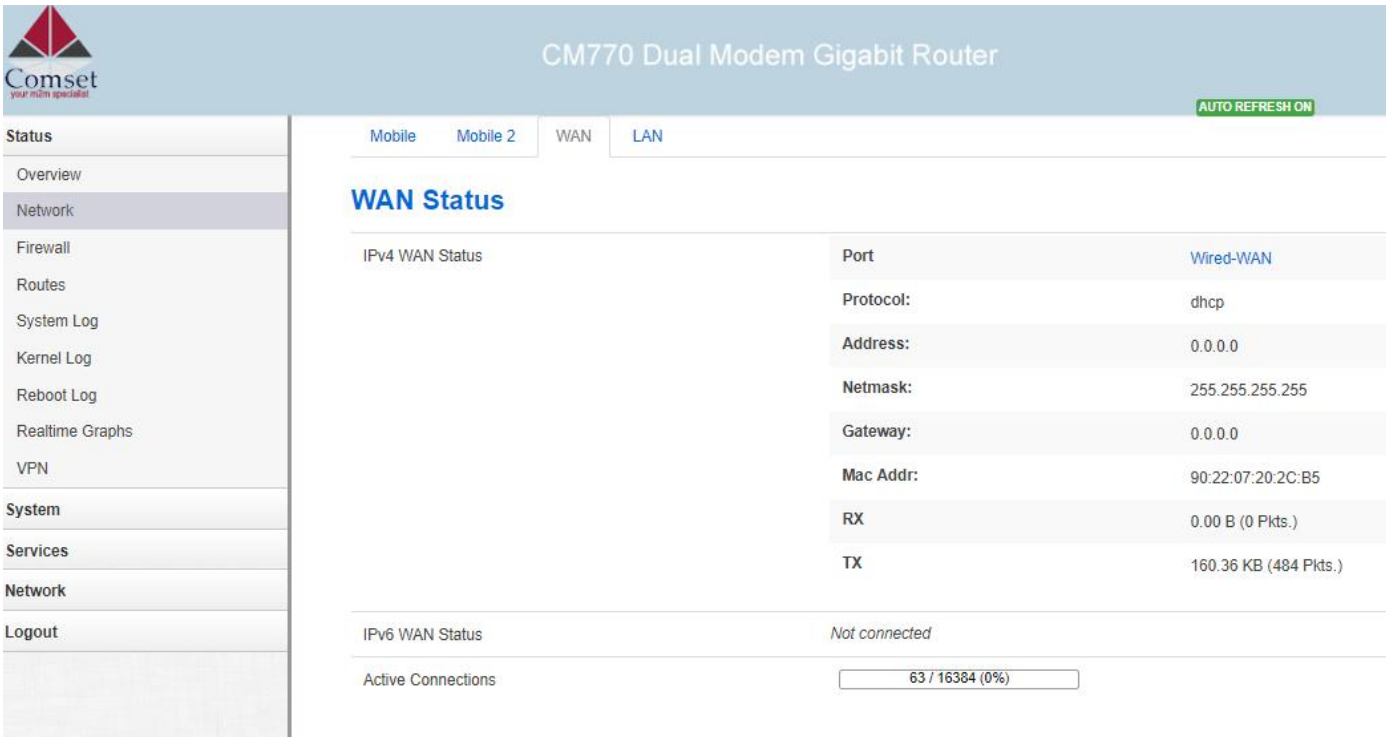
Mobile 2

Cellular Status	Up
Cell Modem	QUECTEL_EP06 (2C7C_0306)
IMEI/ESN	868186040016394
Sim Status	SIM Ready
Strength	31 / 31, dBm : -51
Selected Network	Automatic
Registered Network	Registered on Home network: "Telstra Mobile Telstra", 7,
Sub Network Type	FDD LTE
Location Area Code	304B
Cell ID	817FC03
MSISDN/IMSI	/ 505013520815990

Connection Status

Port	eth2
IPv4 Addr	10.98.135.13/30
DNS 1	10.4.130.164
DNS 2	10.5.136.242
Gateway	10.98.135.14
Uptime	0h 21m 4s
RX	555.82 KB (5421 Pkts.)
TX	10.54 MB (8620 Pkts.)

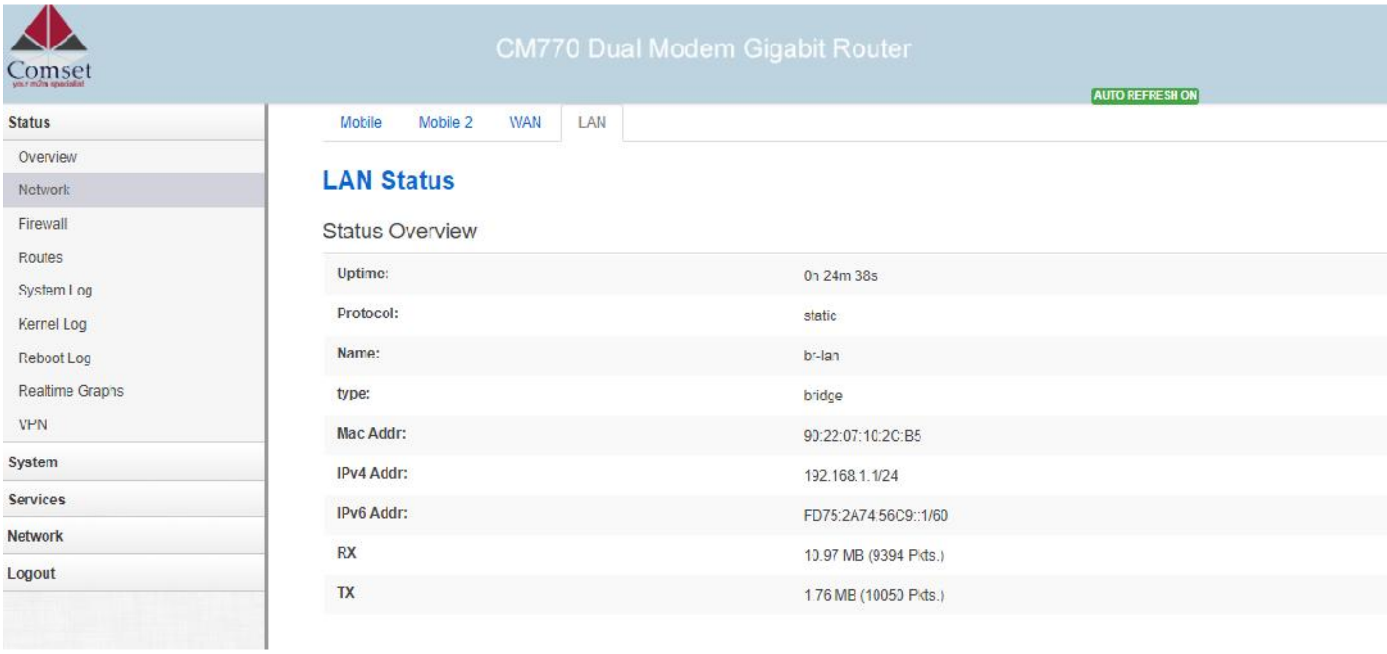
WAN status page:



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:	90:22:07:20:2C:B5
	RX	0.00 B (0 Pkts.)
	TX	160.36 KB (484 Pkts.)
IPv6 WAN Status	*Not connected*	
Active Connections	63 / 16384 (0%)	

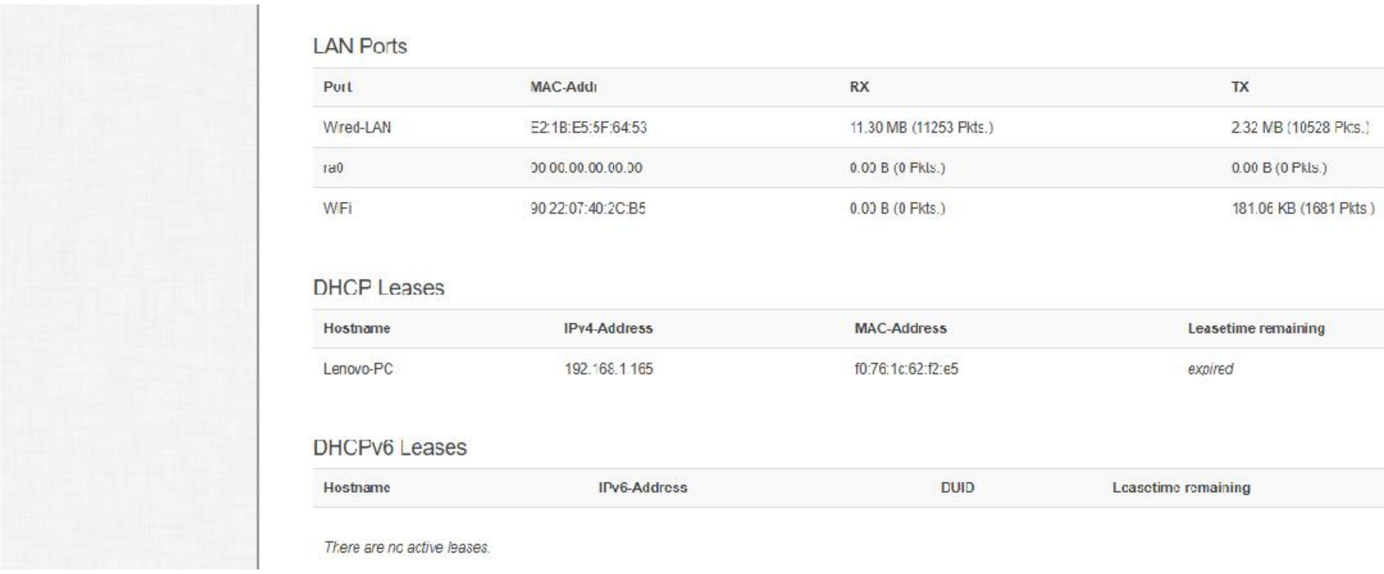
LAN status page:



LAN Status

Status Overview

Uptime:	0h 24m 38s
Protocol:	static
Name:	br-lan
type:	bridge
Mac Addr:	90:22:07:10:2C:B5
IPv4 Addr:	192.168.1.1/24
IPv6 Addr:	FD75:2A74:56C9::1/60
RX	10.97 MB (9394 Pkts.)
TX	1.76 MB (10050 Pkts.)



LAN Ports

Port	MAC-Addr	RX	TX
Wred-LAN	E2:1B:E5:5F:64:53	11.30 MB (11253 Pkts.)	2.32 MB (10528 Pkts.)
ra0	00:00:00:00:00:00	0.00 B (0 Pkts.)	0.00 B (0 Pkts.)
WiFi	90:22:07:40:2C:B5	0.00 B (0 Pkts.)	181.06 KB (1681 Pkts.)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
Lenovo-PC	192.168.1.165	f0:76:1c:62:f2:e5	*expired*

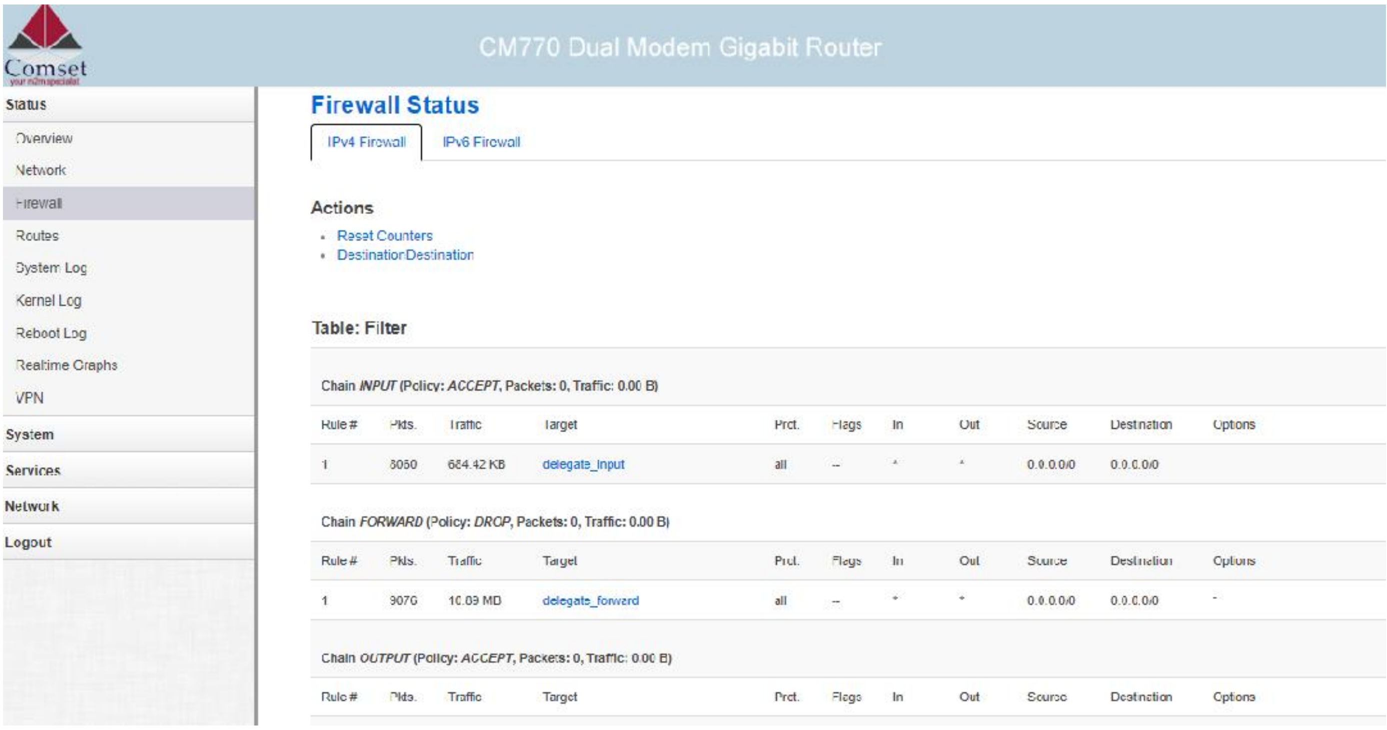
DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining

There are no active leases.

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

IPv4 Firewall | IPv6 Firewall

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	8050	684.42 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

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

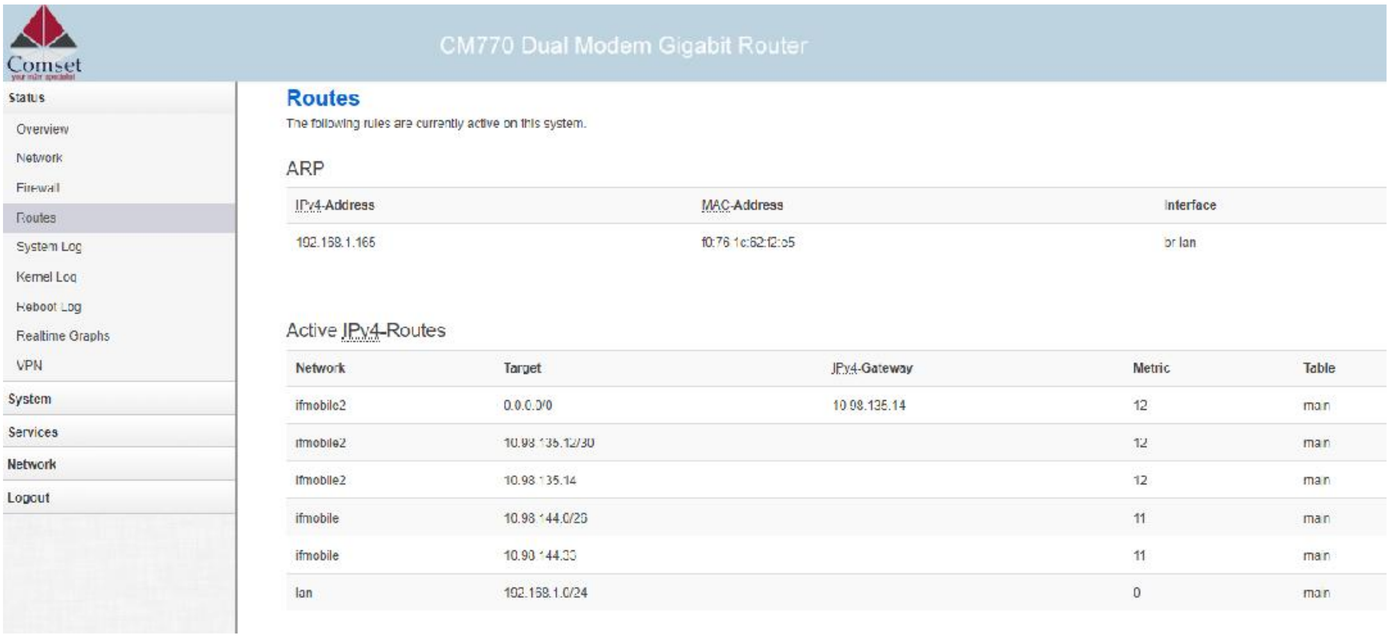
Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	9076	10.09 MB	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

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

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options

3.3.4 Routes

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



Routes

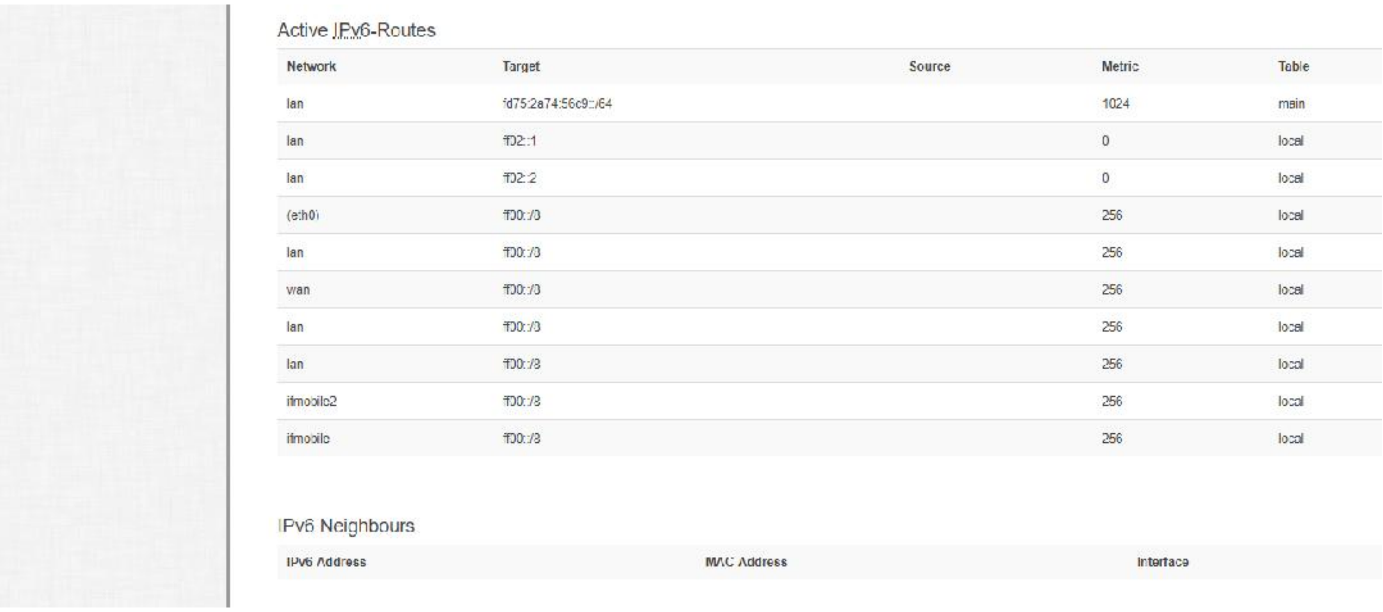
The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.1.165	f0:76:1c:62:f2:c5	br-lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
ifmobile2	0.0.0.0/0	10.98.135.14	12	main
ifmobile2	10.98.135.12/30		12	main
ifmobile2	10.98.135.14		12	main
ifmobile	10.98.144.0/26		11	main
ifmobile	10.98.144.33		11	main
lan	192.168.1.0/24		0	main



Active IPv6-Routes

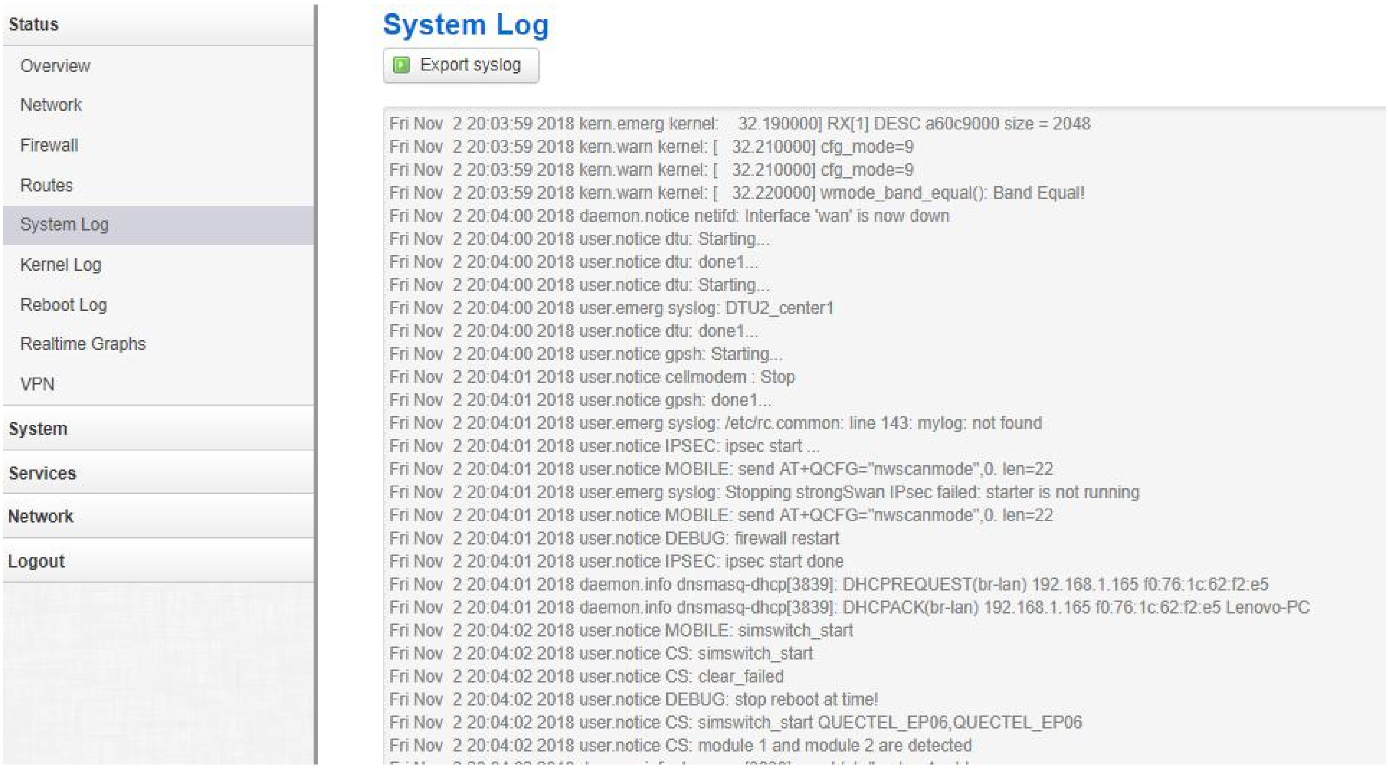
Network	Target	Source	Metric	Table
lan	fd75:2a74:56c9::/64		1024	main
lan	ff02::1		0	local
lan	ff02::2		0	local
(eth0)	ff00::/8		256	local
lan	ff00::/8		256	local
wan	ff00::/8		256	local
lan	ff00::/8		256	local
lan	ff00::/8		256	local
ifmobile2	ff00::/8		256	local
ifmobile	ff00::/8		256	local

IPv6 Neighbours

IPv6 Address	MAC Address	Interface

3.3.5 System log

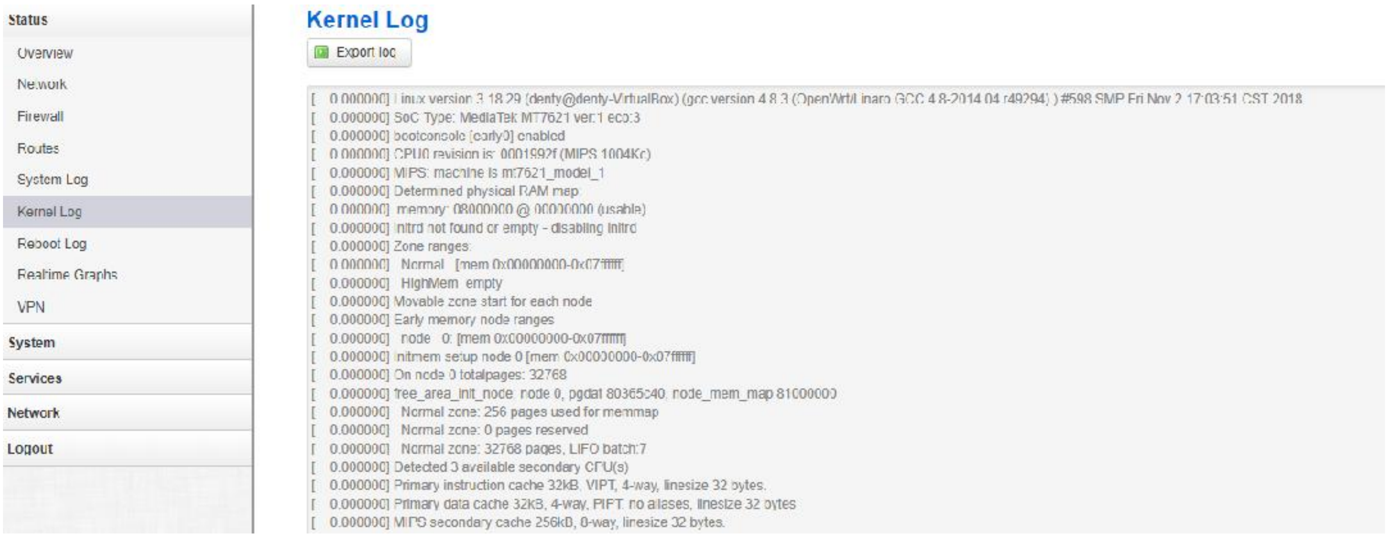
This page shows the system log from system boot up. The system log resets when the router is restarted. You can export the system log by clicking the button “Export Syslog”.



```
Fri Nov  2 20:03:59 2018 kern.emerg kernel:    32.190000] RX[1] DESC a60c9000 size = 2048
Fri Nov  2 20:03:59 2018 kern.warn kernel: [   32.210000] cfg_mode=9
Fri Nov  2 20:03:59 2018 kern.warn kernel: [   32.210000] cfg_mode=9
Fri Nov  2 20:03:59 2018 kern.warn kernel: [   32.220000] wmode_band_equal(): Band Equal!
Fri Nov  2 20:04:00 2018 daemon.notice netifd: Interface 'wan' is now down
Fri Nov  2 20:04:00 2018 user.notice dtu: Starting...
Fri Nov  2 20:04:00 2018 user.notice dtu: done1...
Fri Nov  2 20:04:00 2018 user.notice dtu: Starting...
Fri Nov  2 20:04:00 2018 user.emerg syslog: DTU2_center1
Fri Nov  2 20:04:00 2018 user.notice dtu: done1...
Fri Nov  2 20:04:00 2018 user.notice gpsh: Starting...
Fri Nov  2 20:04:01 2018 user.notice cellmodem : Stop
Fri Nov  2 20:04:01 2018 user.notice gpsh: done1...
Fri Nov  2 20:04:01 2018 user.emerg syslog: /etc/rc.common: line 143: mylog: not found
Fri Nov  2 20:04:01 2018 user.notice IPSEC: ipsec start ...
Fri Nov  2 20:04:01 2018 user.notice MOBILE: send AT+QCFG="nwscanmode",0. len=22
Fri Nov  2 20:04:01 2018 user.emerg syslog: Stopping strongSwan IPsec failed: starter is not running
Fri Nov  2 20:04:01 2018 user.notice MOBILE: send AT+QCFG="nwscanmode",0. len=22
Fri Nov  2 20:04:01 2018 user.notice DEBUG: firewall restart
Fri Nov  2 20:04:01 2018 user.notice IPSEC: ipsec start done
Fri Nov  2 20:04:01 2018 daemon.info dnsmasq-dhcp[3839]: DHCPREQUEST(br-lan) 192.168.1.165 f0:76:1c:62:f2:e5
Fri Nov  2 20:04:01 2018 daemon.info dnsmasq-dhcp[3839]: DHCPACK(br-lan) 192.168.1.165 f0:76:1c:62:f2:e5 Lenovo-PC
Fri Nov  2 20:04:02 2018 user.notice MOBILE: simswitch_start
Fri Nov  2 20:04:02 2018 user.notice CS: simswitch_start
Fri Nov  2 20:04:02 2018 user.notice CS: clear_failed
Fri Nov  2 20:04:02 2018 user.notice DEBUG: stop reboot at time!
Fri Nov  2 20:04:02 2018 user.notice CS: simswitch_start QUECTEL_EP06,QUECTEL_EP06
Fri Nov  2 20:04:02 2018 user.notice CS: module 1 and module 2 are detected
```

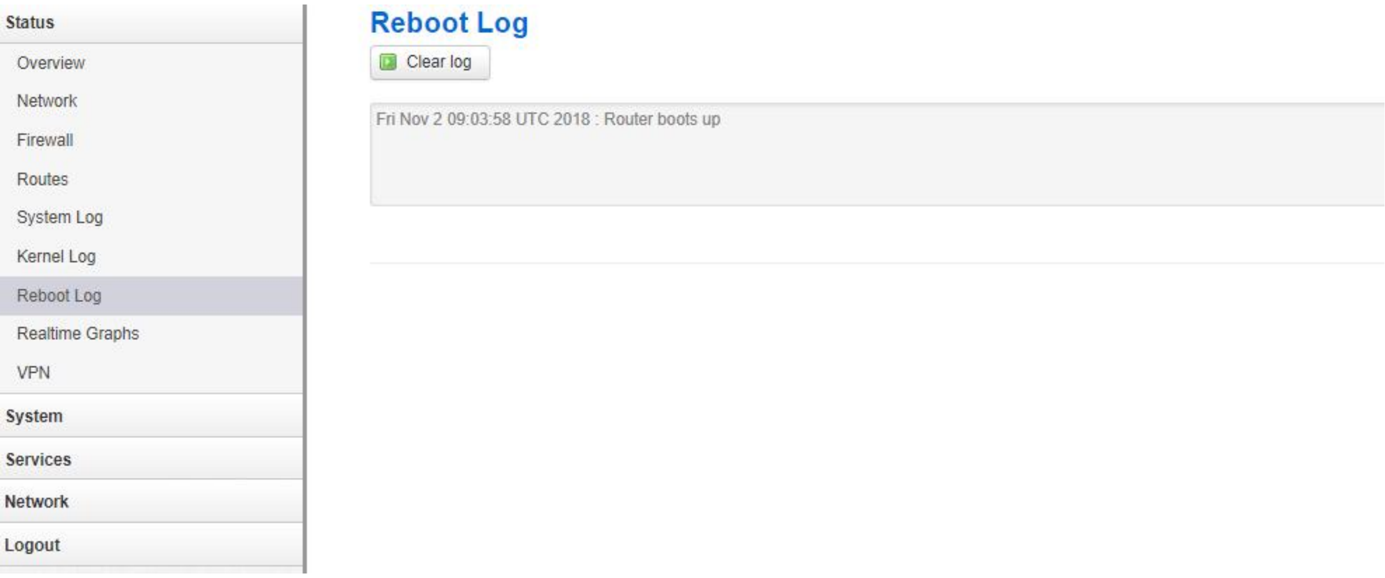
3.3.6 Kernel log

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) ) #598 SMP Fri Nov 2 17:03:51 CST 2018
[    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_1
[    0.000000] Determined physical RAM map:
[    0.000000]  memory: 08000000 @ 00000000 (usable)
[    0.000000] Initrd not found or empty - disabling initrd
[    0.000000] Zone ranges:
[    0.000000]   Normal   [mem 0x00000000-0x07ffffff]
[    0.000000]   HighMem  empty
[    0.000000] Movable zone start for each node
[    0.000000] Early memory node ranges
[    0.000000]   node   0: [mem 0x00000000-0x07ffffff]
[    0.000000] Initmem setup node 0 [mem 0x00000000-0x07ffffff]
[    0.000000] On node 0 totalpages: 32768
[    0.000000] free_area_init_node: node 0, pgdat 80365c40, node_mem_map 81000000
[    0.000000]   Normal zone: 256 pages used for memmap
[    0.000000]   Normal zone: 0 pages reserved
[    0.000000]   Normal zone: 32768 pages, LIFO batch:7
[    0.000000] Detected 3 available secondary CPU(s)
[    0.000000] Primary instruction cache 32kB, VIPT, 4-way, linesize 32 bytes.
[    0.000000] Primary data cache 32kB, 4-way, PIPT, no aliases, linesize 32 bytes
[    0.000000] MIPS secondary cache 256kB, 8-way, linesize 32 bytes.
```

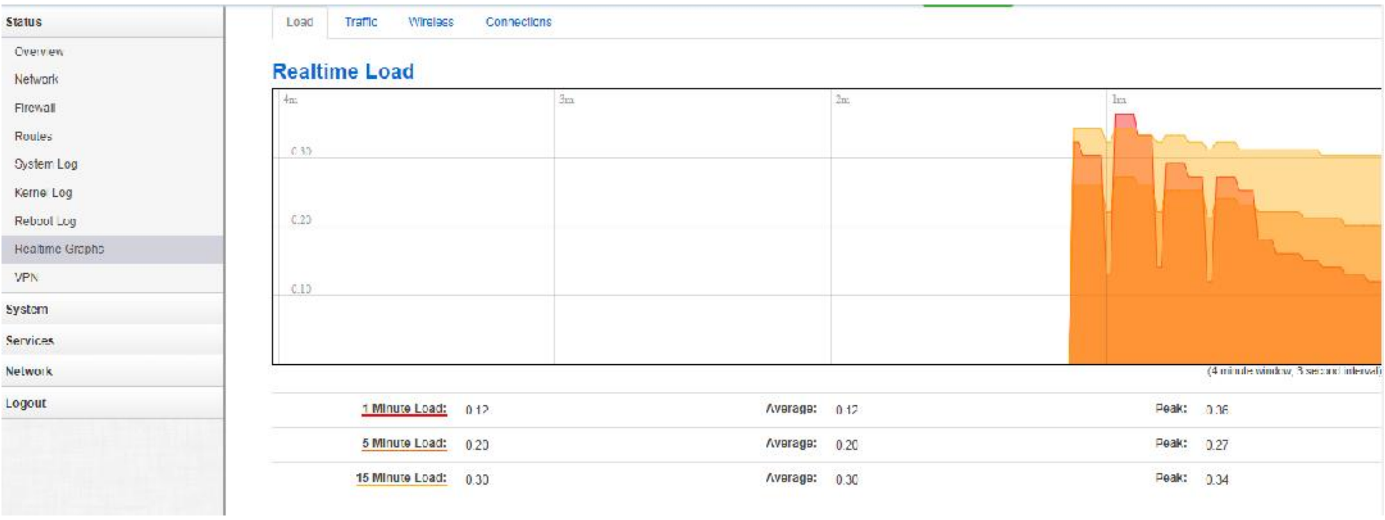
3.3.7 Reboot log



```
Fri Nov 2 09:03:58 UTC 2018 : Router boots up
```

3.3.8 Realtime graphs

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



Realtime Load

(4 minute window, 3 second interval)

1 Minute Load: 0.12 Average: 0.12 Peak: 0.36

5 Minute Load: 0.20 Average: 0.20 Peak: 0.27

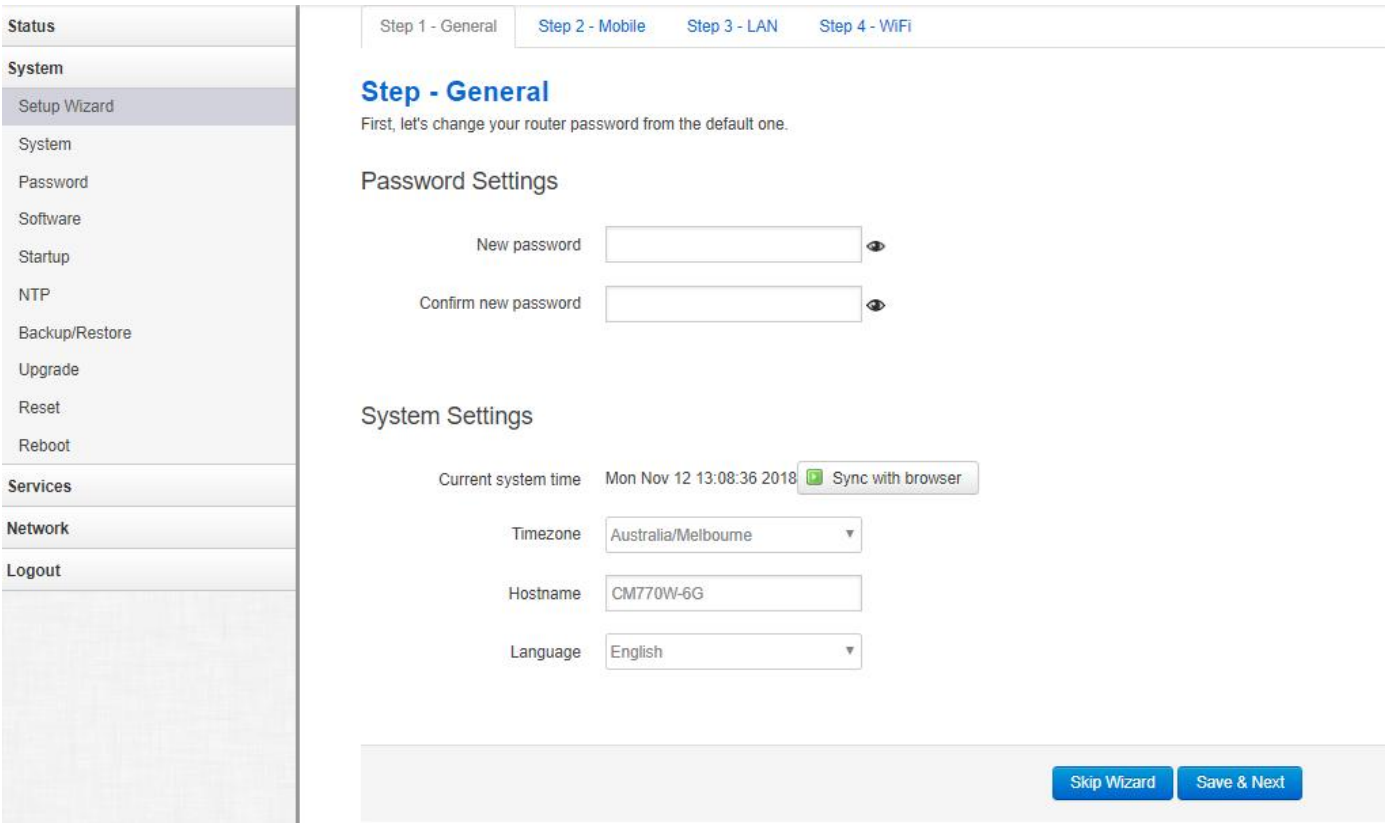
15 Minute Load: 0.30 Average: 0.30 Peak: 0.34

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

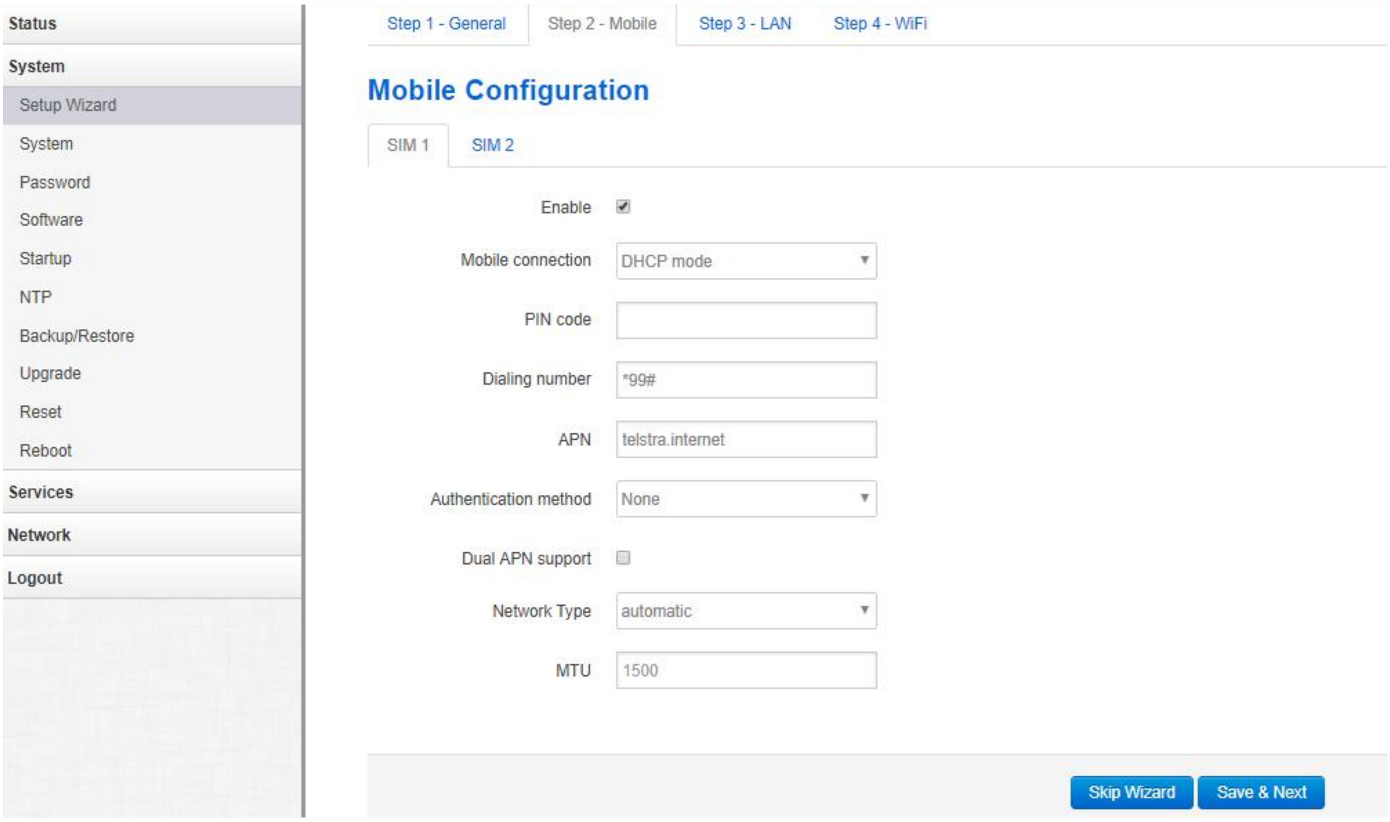
Current system time: Mon Nov 12 13:08:36 2018 Sync with browser

Timezone: Australia/Melbourne

Hostname: CM770W-6G

Language: English

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



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

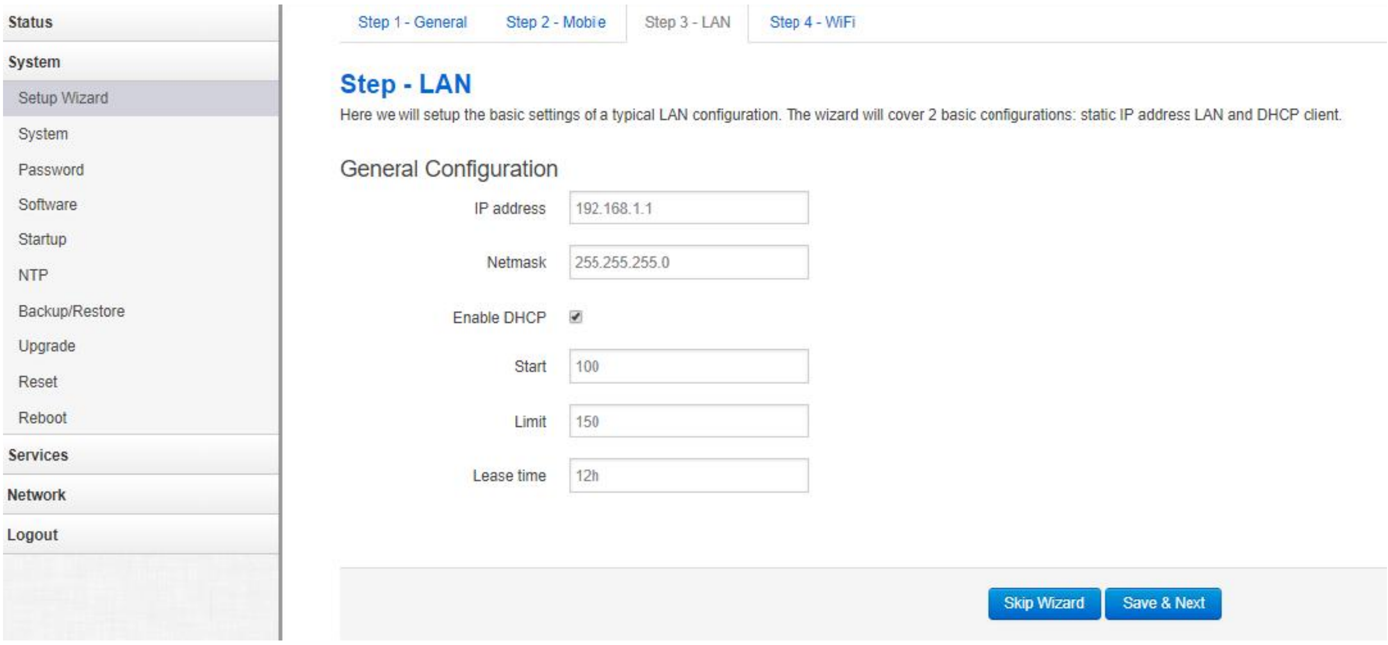
- **Enable:** Enable mobile network;
- **Mobile connection:** Select a suitable mode for the mobile connection. The default value is ‘DHCP mode’;
- **APN:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider;
- **PIN code:** Most SIM cards don’t have a PIN code, in 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 user name, please input the default value, otherwise the router may not dialup. If the Authentication method is ‘None’, this option will not appear.

- **Password:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider.
- **Network Type:** Different Cell Modems support different types. The default value is *Automatic*.
- **MTU:** Maximum Transmission Unit. It is the maximum size of packets transmitted on the network. The default value is 1500. Please configure it to optimise your own network.

Note: Do the same for SIM 2.

When finished, click “Save & Next”



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

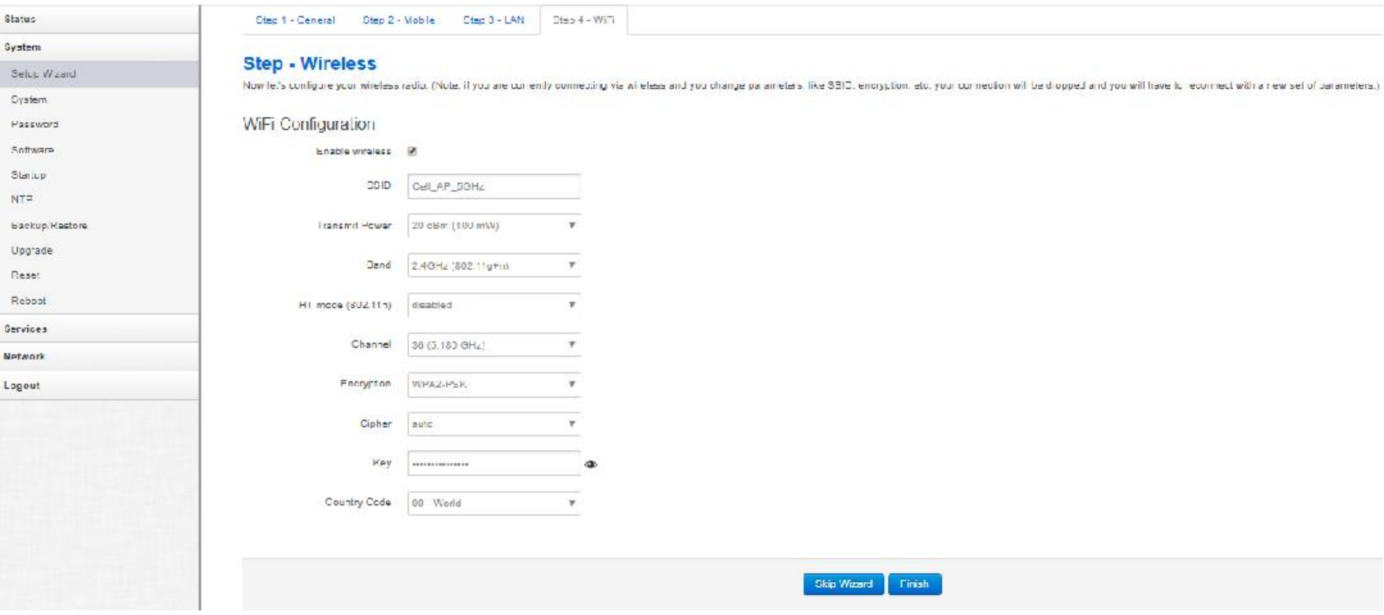
Enable DHCP: ☑

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, encryption, etc. your connection will be dropped and you will have to reconnect with a new set of parameters.)

WiFi Configuration

Enable wireless ☑

SSID: Cell_AP_5GHz

Transmit Power: 20 dBm (100 mW)

Band: 2.4GHz (802.11g+n)

HT mode (802.11n): disabled

Channel: 36 (5.180 GHz)

Encryption: WPA2-PSK

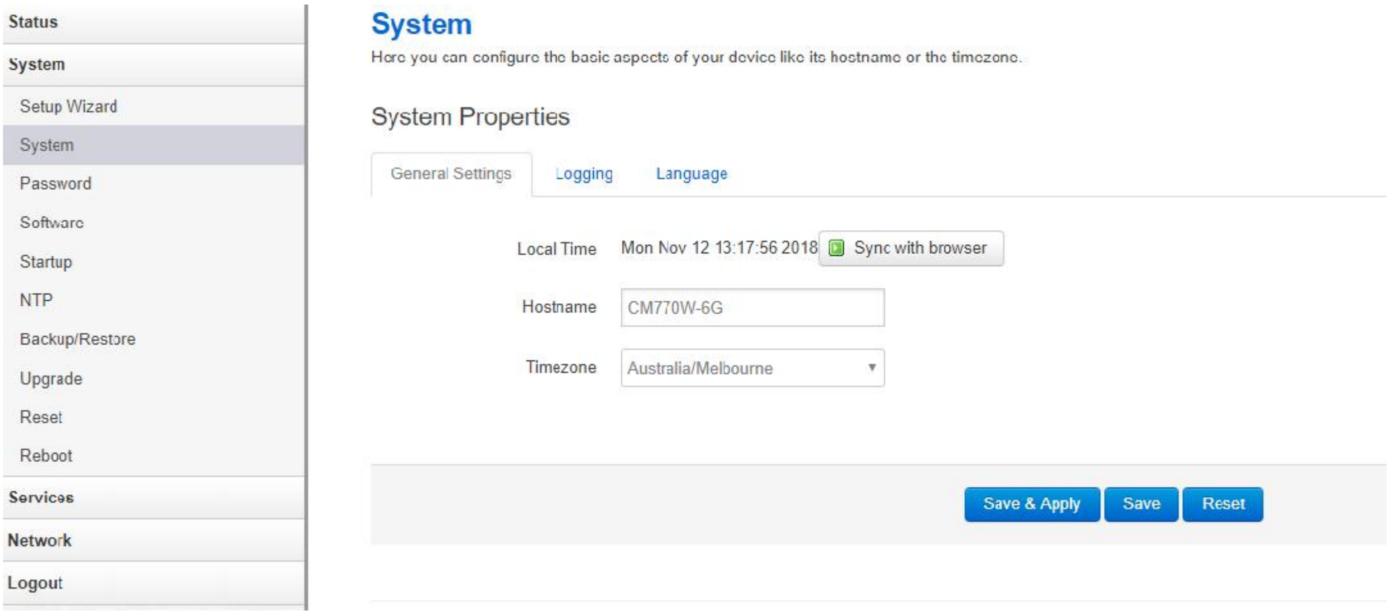
Cipher: auto

Key: ••••••••••••••

Country Code: 00 - World

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

3.4.2 System



System

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

System Properties

Local Time: Mon Nov 12 13:17:56 2018

Hostname: CM770W-6G

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".

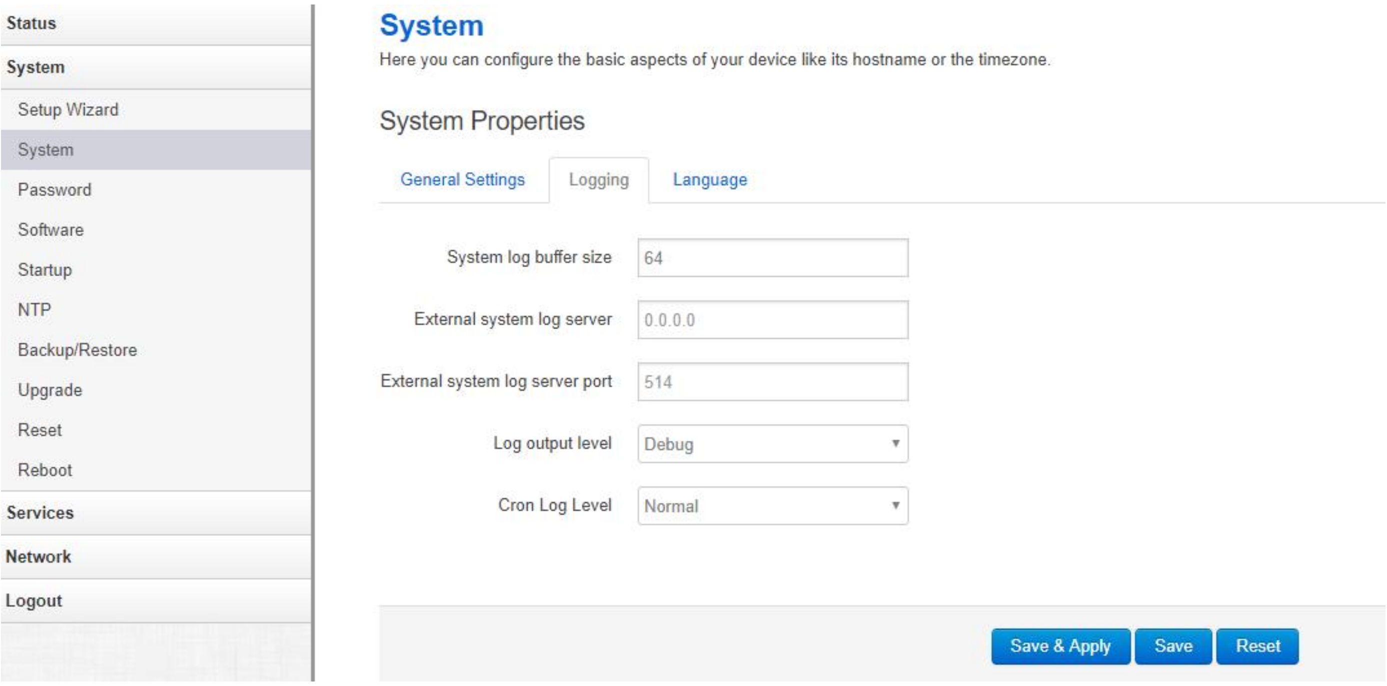
- **Hostname**

It is the router's name. The default name is "CM770W_6G"

- **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

- **System log buffer size**

The unit is KB. The default value is 64 KB. If the actual log size exceeds the set value, then the first lines of data will be lost.

- **External system log server**

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

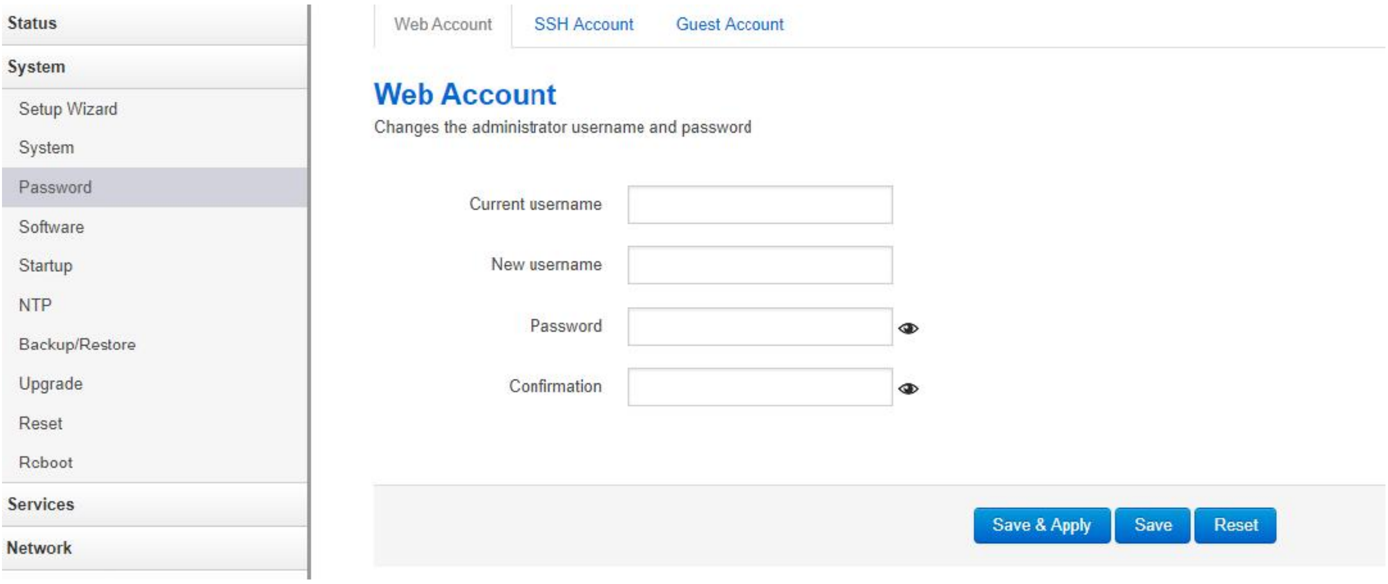
It is the log level to process Crond.

Language and Style

Language: English

The default language is “English”.

3.4.3 Password

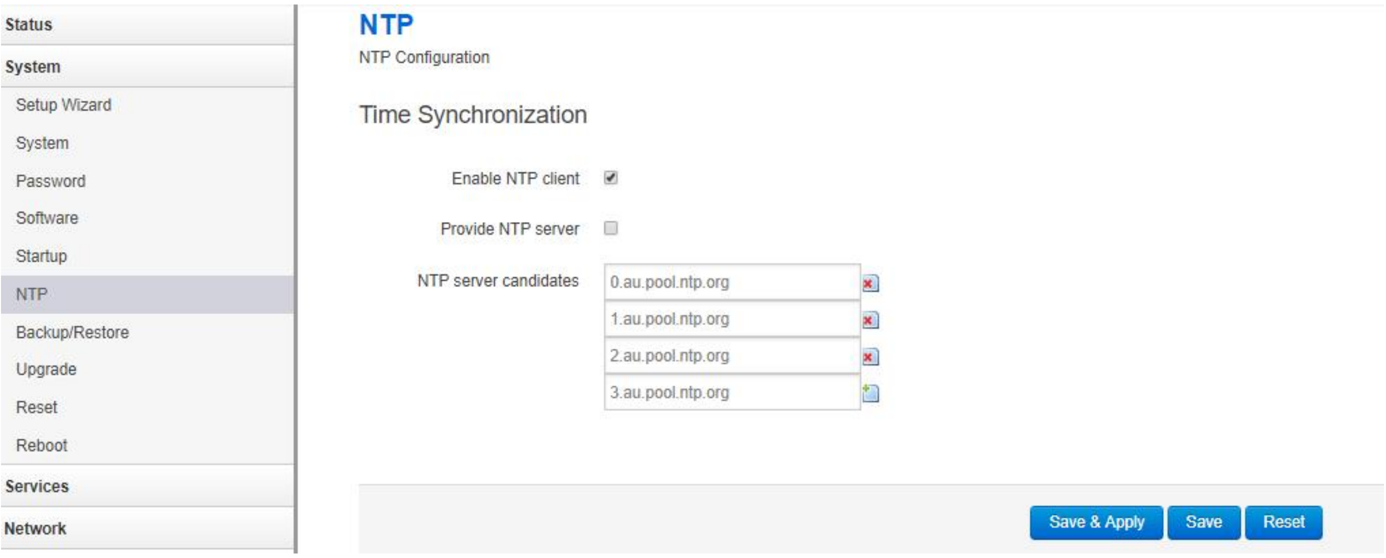


Web Account

Changes the administrator username and password

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.

3.4.4 NTP



NTP

NTP Configuration

Time Synchronization

Enable NTP client ☑

Provide NTP server □

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 a NTP client.

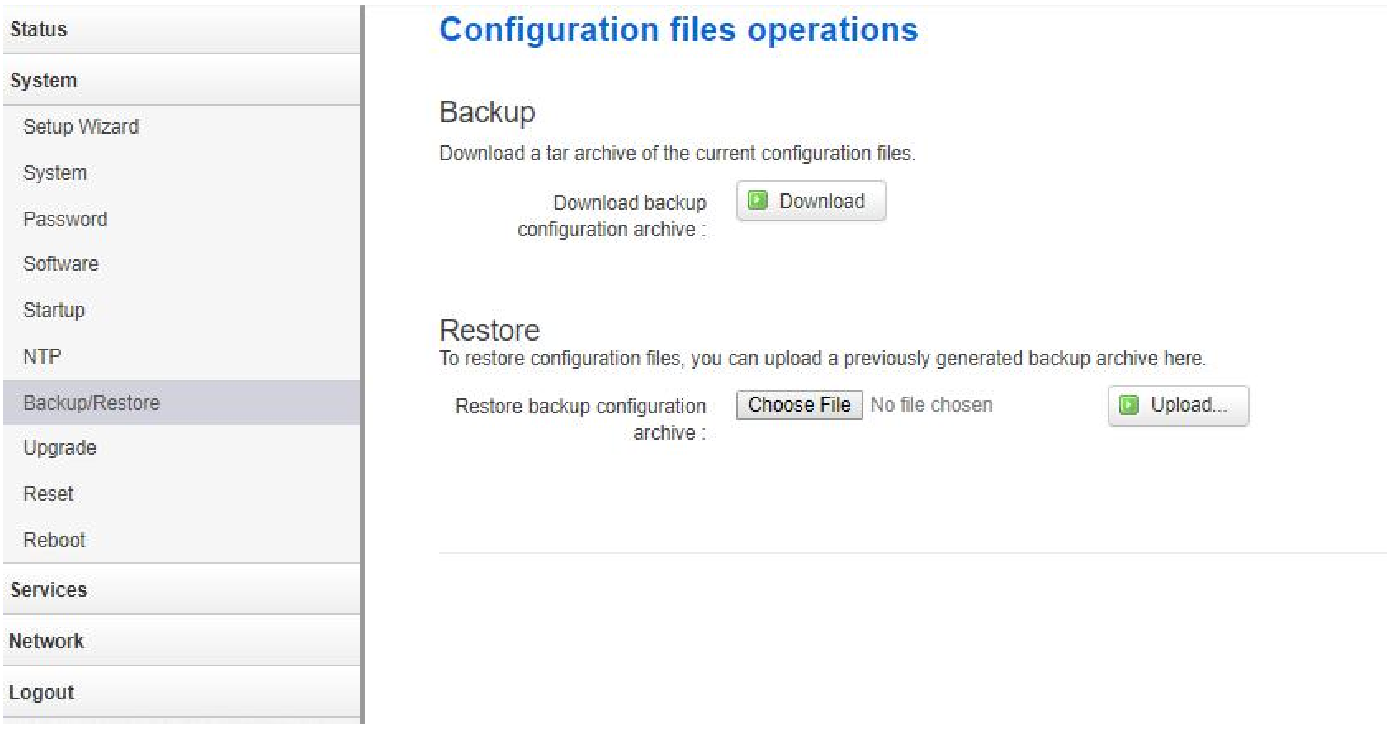
- **Provide NTP server**

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

- **NTP server candidates**

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

3.4.5 Backup/Restore



Configuration files operations

Backup

Download a tar archive of the current configuration files.

Download backup configuration archive : Download

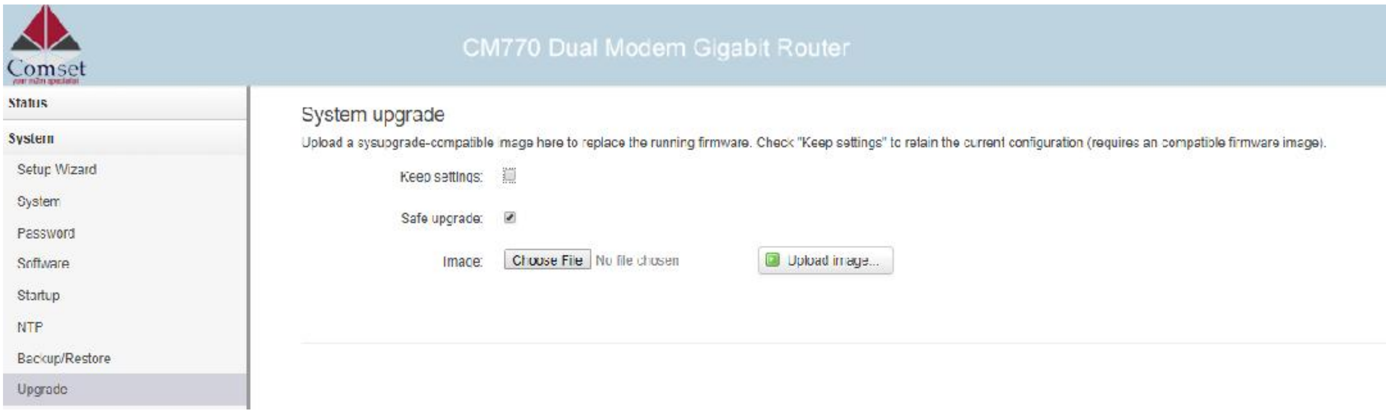
Restore

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

Restore backup configuration archive : Choose File No file chosen Upload...

- ➢ To backup 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 configuration (requires an compatible firmware image).

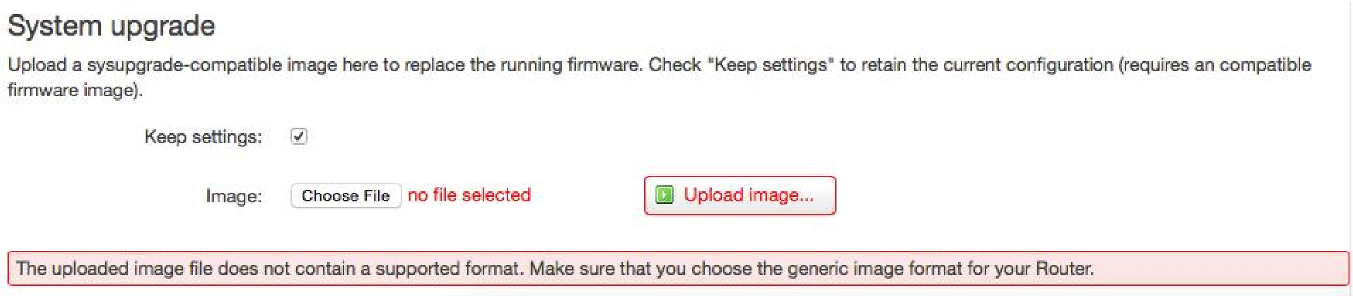
Keep settings: □

Safe upgrade: ☑

Image: Choose File No file chosen 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 “Choose File” 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

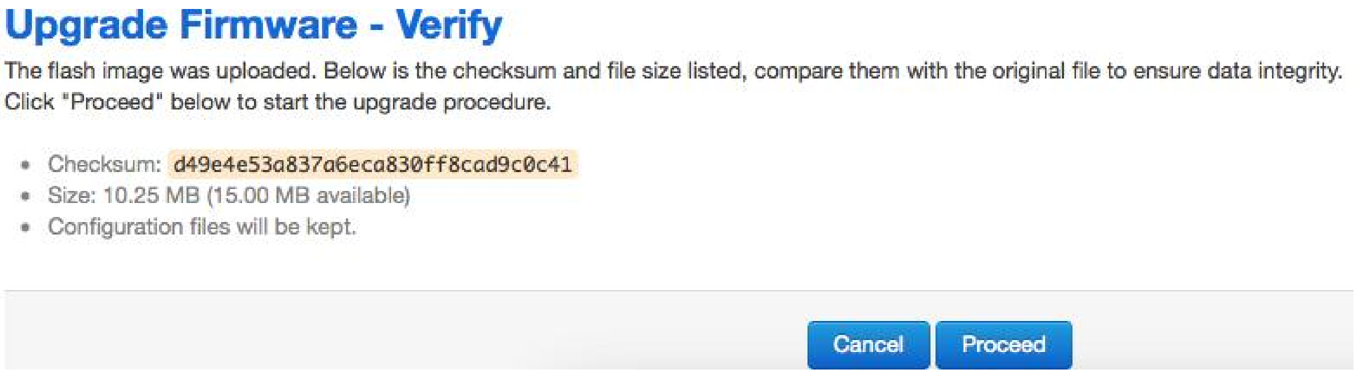
Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an compatible firmware image).

Keep settings: ☑

Image: Choose File no file selected

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.

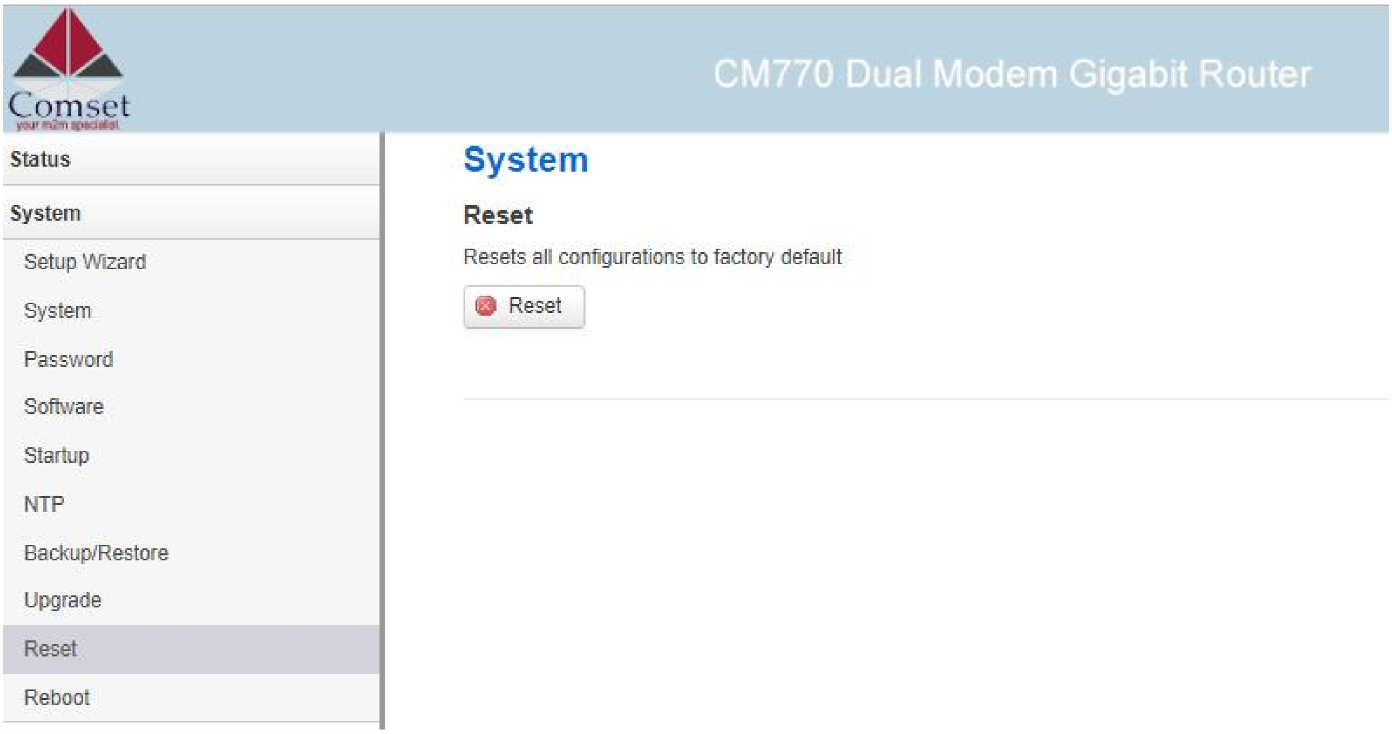


Upgrade Firmware - Verify

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.

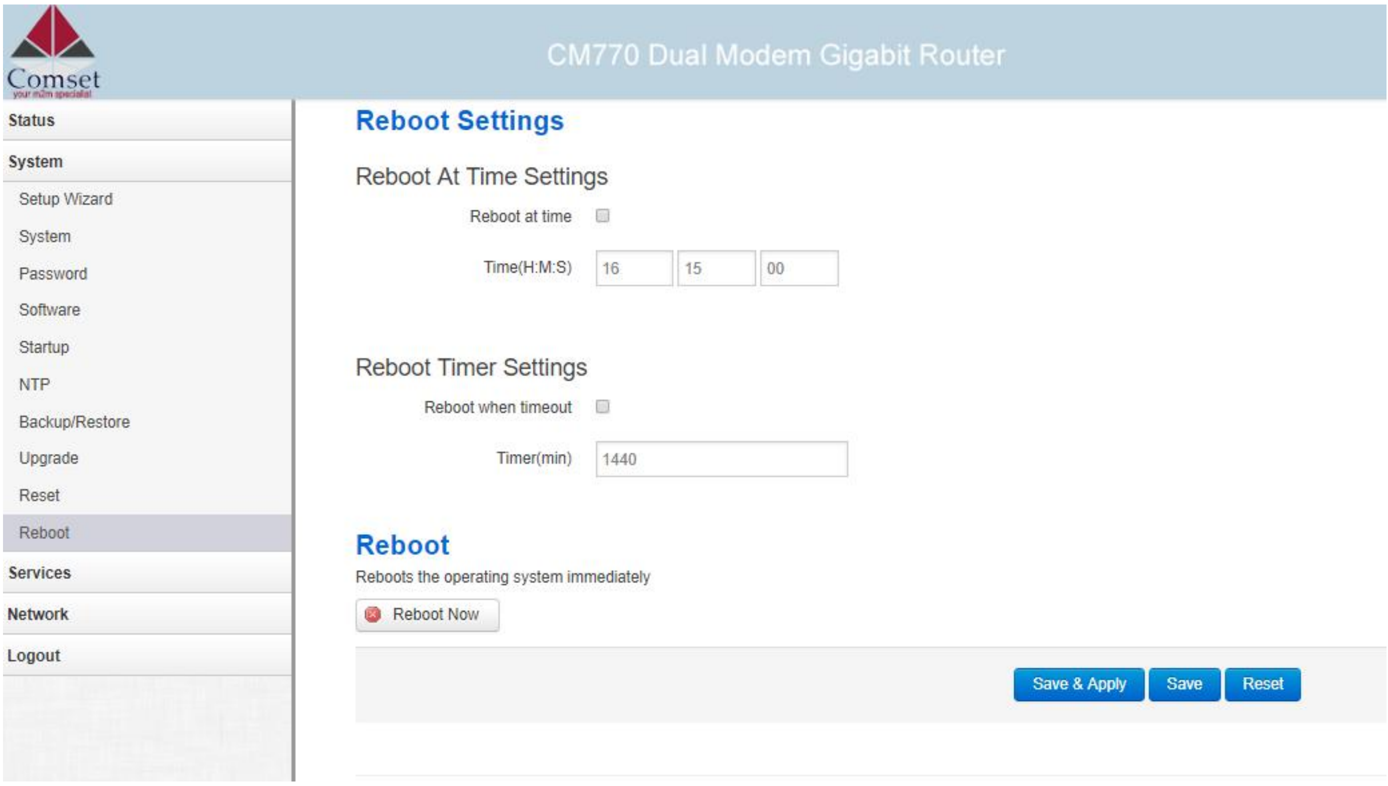
3.4.7 Reset



Resets all configurations to factory default

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

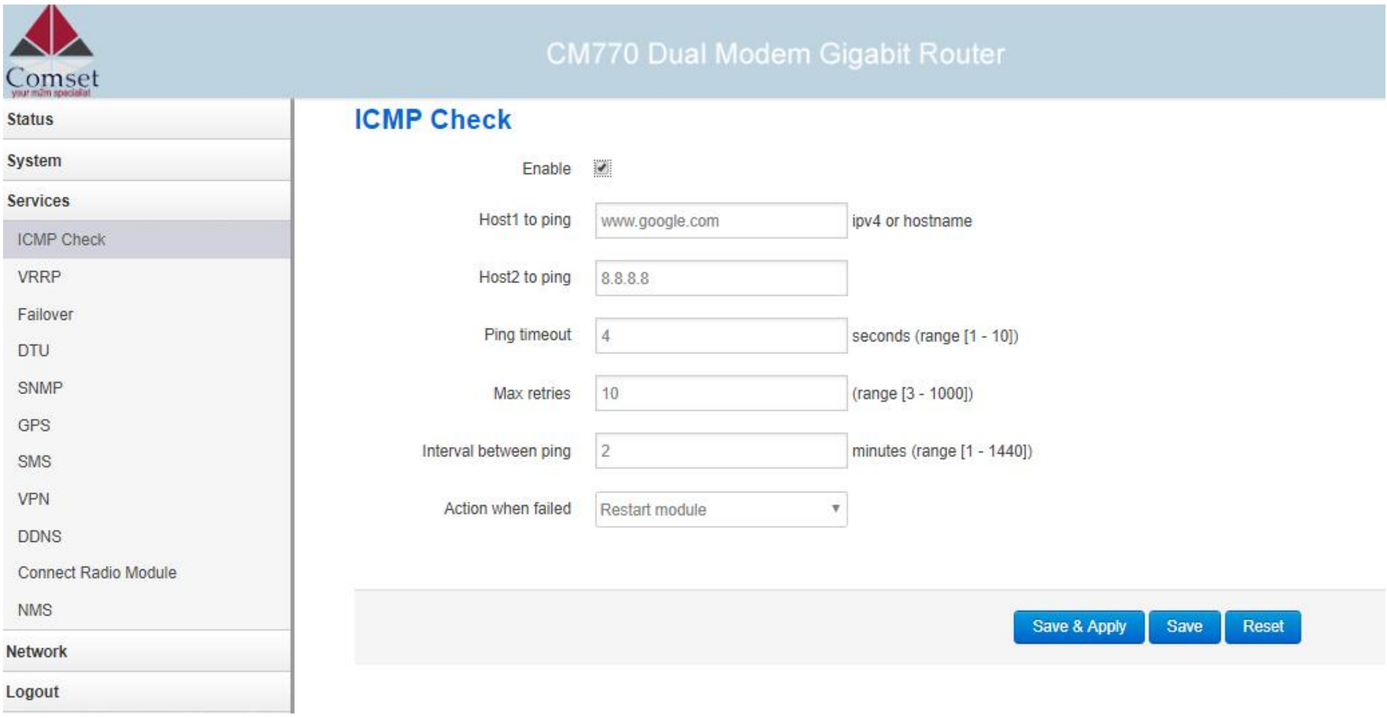
Reboot Now

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

3.5 Services configuration

3.5.1 ICMP check

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



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])

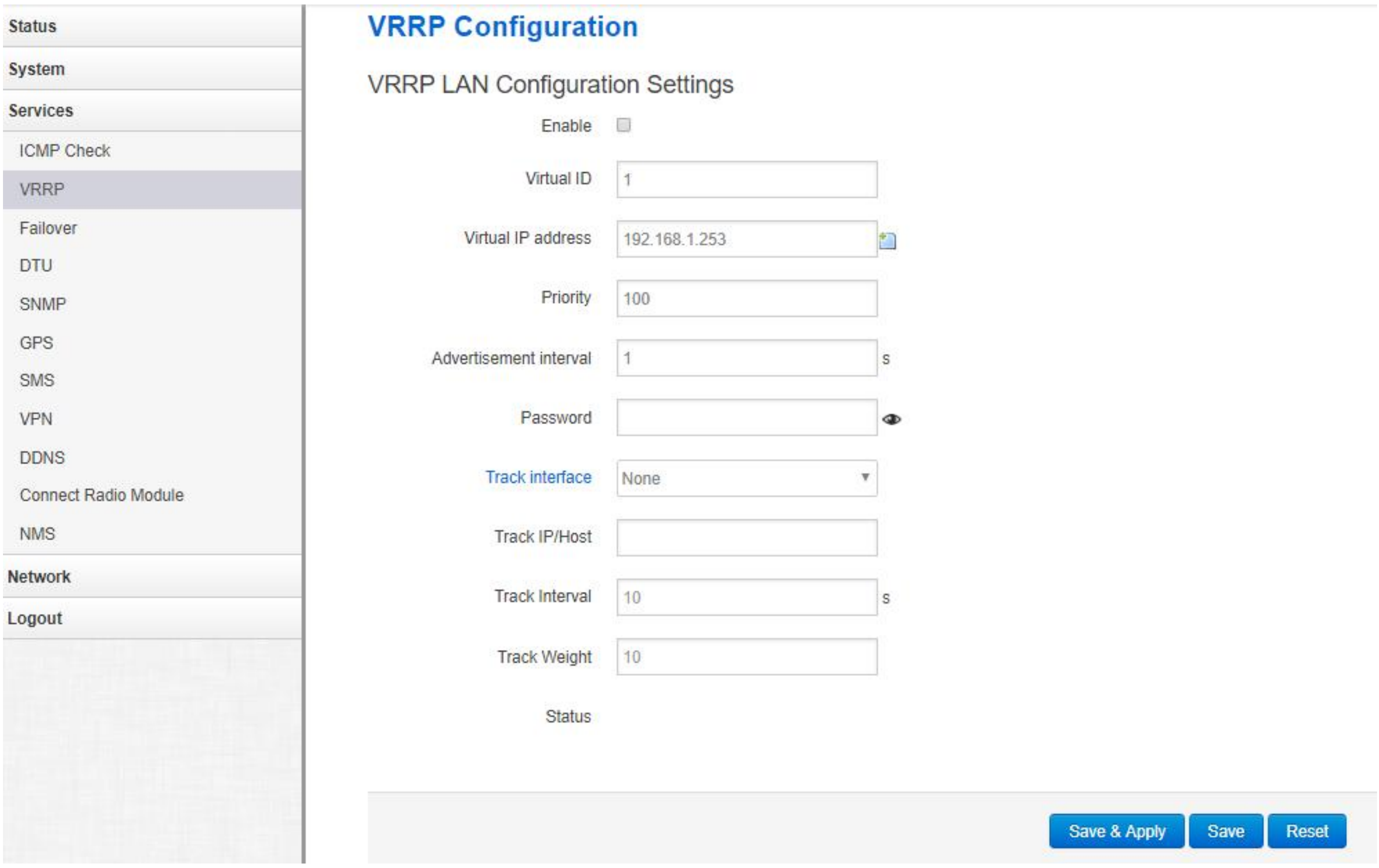
Max retries: 10 (range [3 - 1000])

Interval between ping: 2 minutes (range [1 - 1440])

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.
- **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



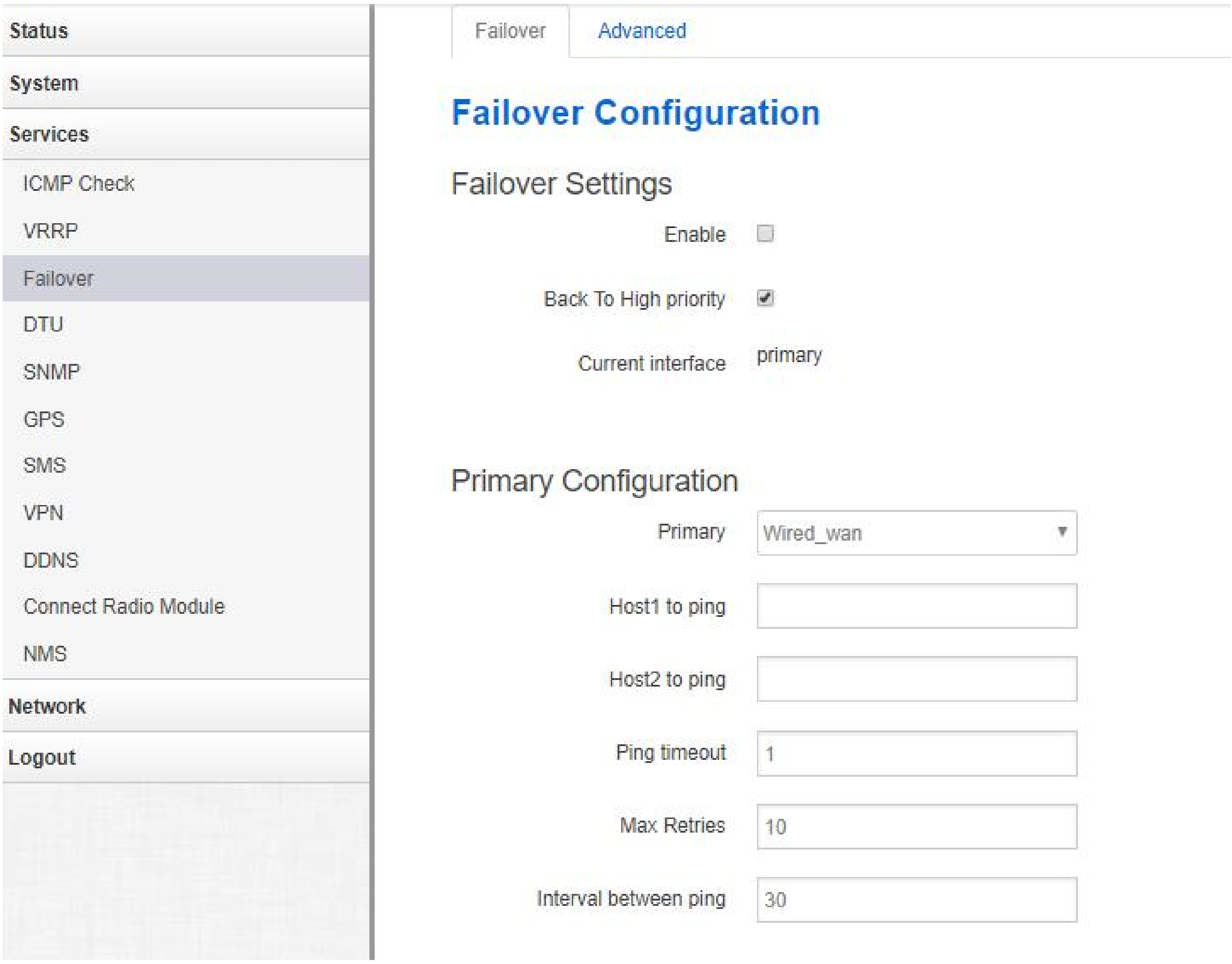
VRRP Configuration

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.
- **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 ➕.
- **Virtual ID**: Routers with the same IDs will be grouped in the same VRRP cluster. The legal number is from 1 to 255.
- **Priority**: The router with the highest priority in the same VRRP cluster will act as a master. The legal number is from 1 to 255.

3.5.3 Failover (link backup)



Failover Configuration

Failover Settings

Enable □

Back To High priority ☑

Current interface primary

Primary Configuration

Primary: Wired_wan

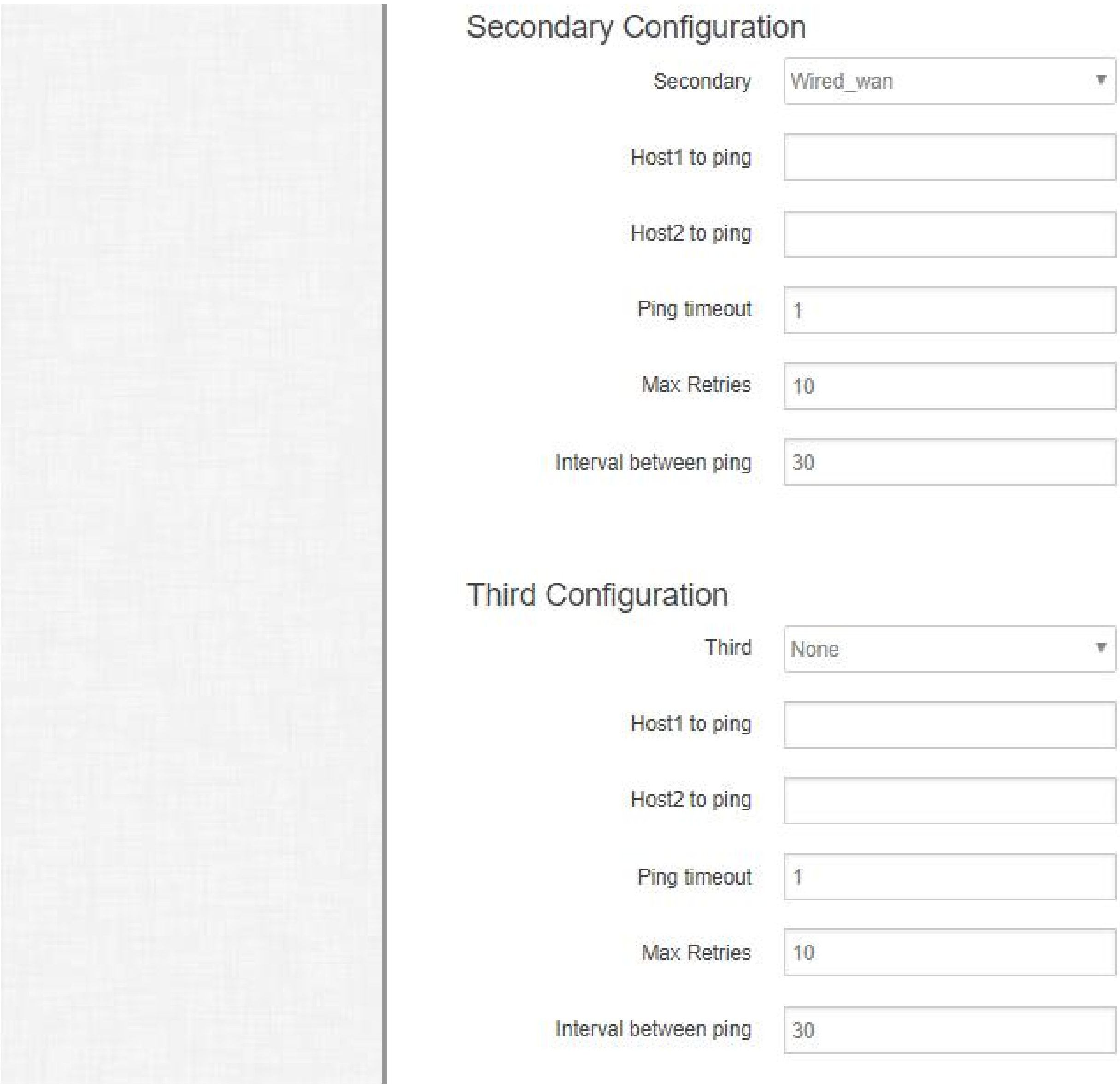
Host1 to ping:

Host2 to ping:

Ping timeout: 1

Max Retries: 10

Interval between ping: 30



Secondary Configuration

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

Third Configuration

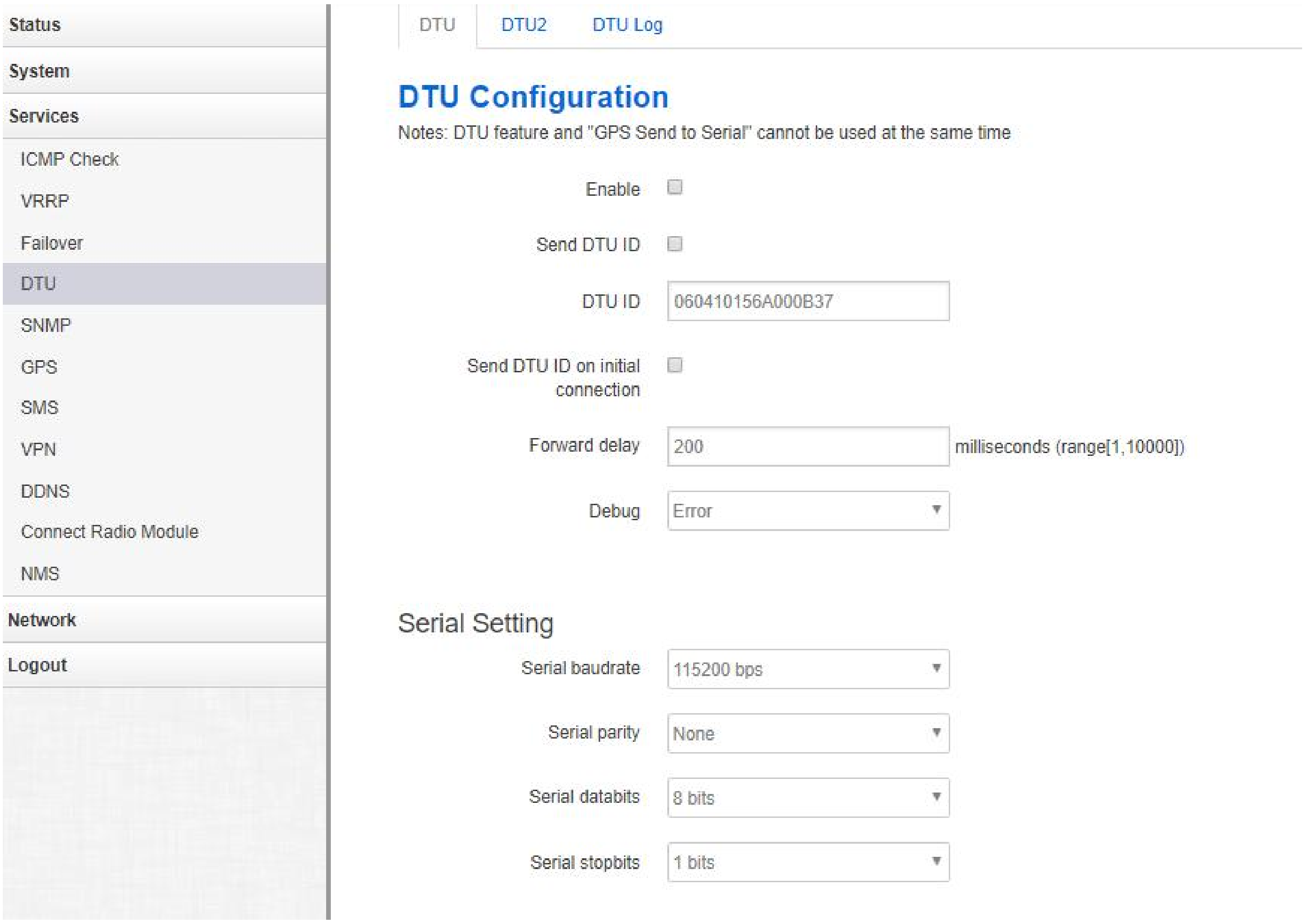
Third	None ▾
Host1 to ping	
Host2 to ping	
Ping timeout	1
Max Retries	10
Interval between ping	30

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

- **Interval between pings**: The time between two pings in seconds.

3.5.4 DTU

Notes:
1) This feature is for the CM770W-6 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 060410156A000B37

Send DTU ID on initial connection □

Forward delay 200 milliseconds (range[1,10000])

Debug Error

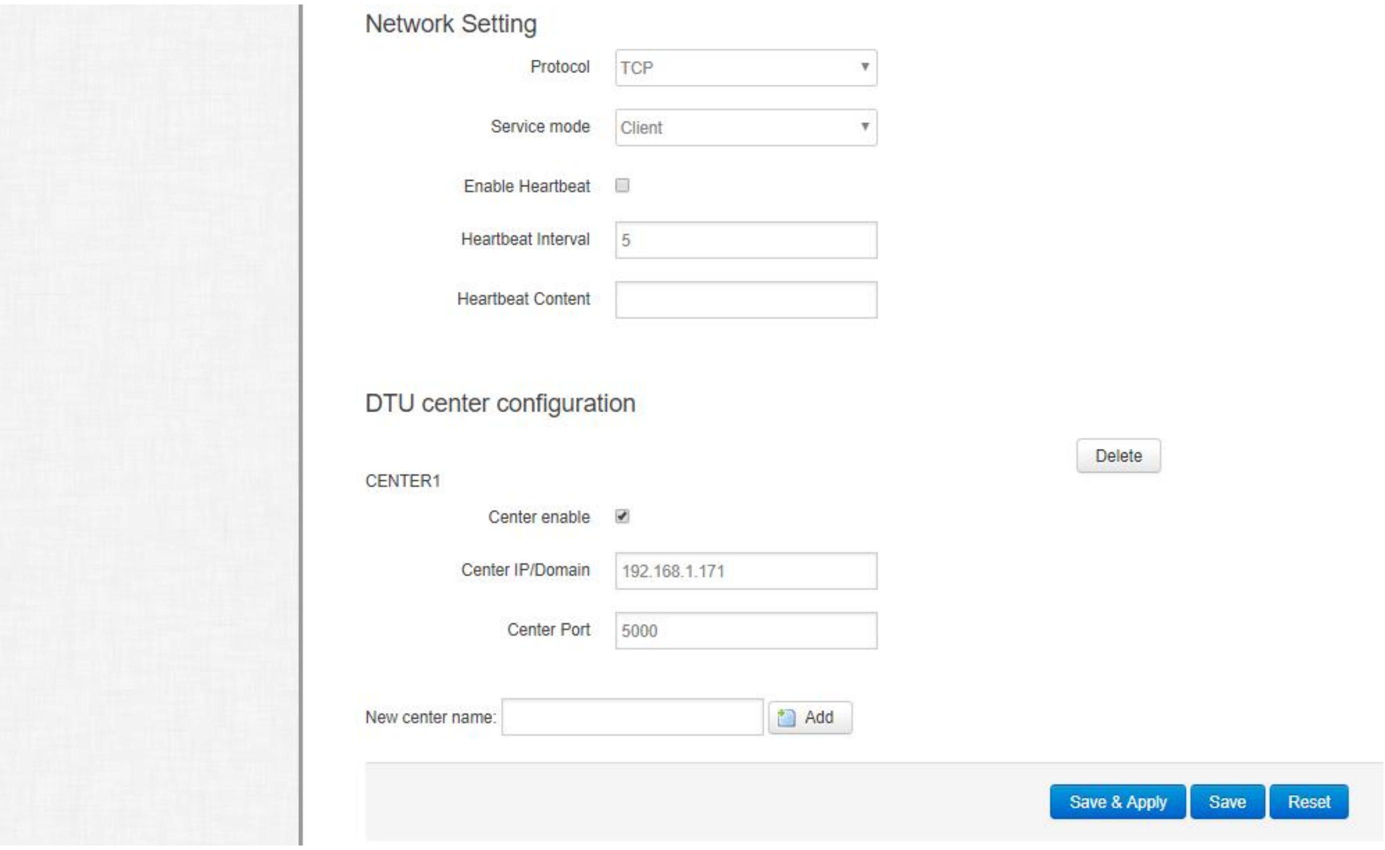
Serial Setting

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.

- **Serial baudrate**: Supports 300/1200/2400/4800/9600/19200/38400/57600/115200bps
- **Serial parity:** Can be none, odd or even
- **Serial databits:** Can be 7 bits or 8 bits
- **Serial stopbit:** Can be 1 bit or 2 bits

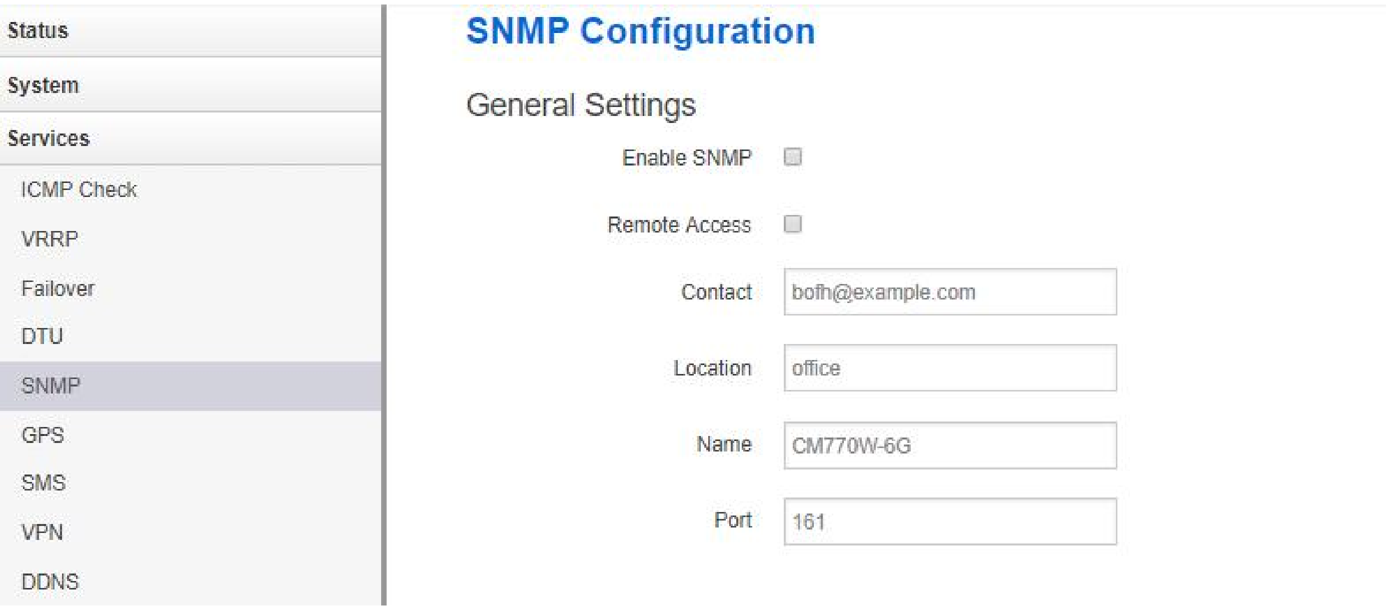
- **Protocol:** Both TCP and UDP are supported
- **Service mode:** Client and Server are supported.
- **Enable heartbeat:** The heartbeat is used to maintain the “keep alive” connection.
- **Heartbeat interval:** The time between two heartbeat packets.
- **Heartbeat content:** The content of heartbeat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

'Disabled'.

Notes:
The maximum number of DTU centers is 32.

Repeat the same process for DTU 2.

3.5.5 SNMP



SNMP Configuration

General Settings

Enable SNMP □

Remote Access □

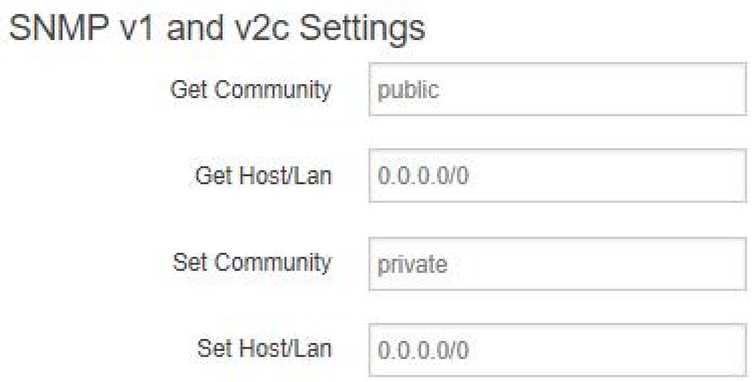
Contact: bofh@example.com

Location: office

Name: CM770W-6G

Port: 161

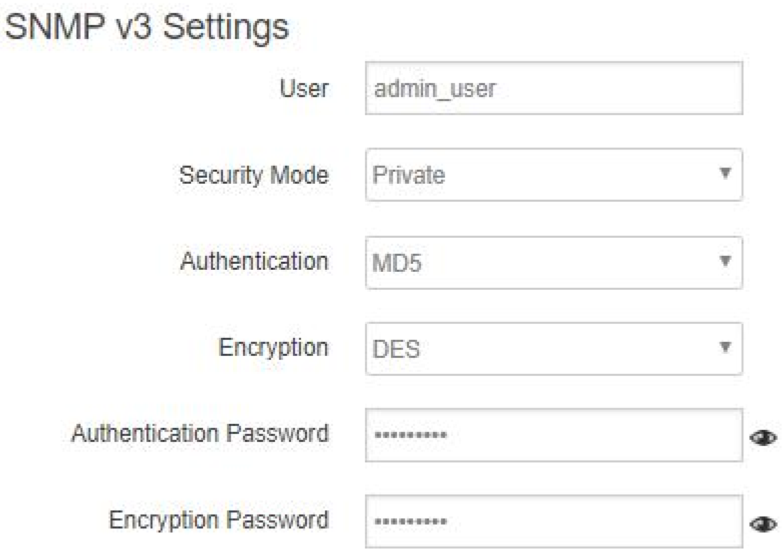
- **Enable SNMP**: Enable the SNMP feature
- **Remote Access**: Allow SNMP remote access. If it is unchecked, only the LAN subnet can access SNMP.
- **Contact**: Set the contact information here.
- **Location**: Set the router's physical address.
- **Name**: Set the router's name in SNMP.
- **Port**: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

- **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

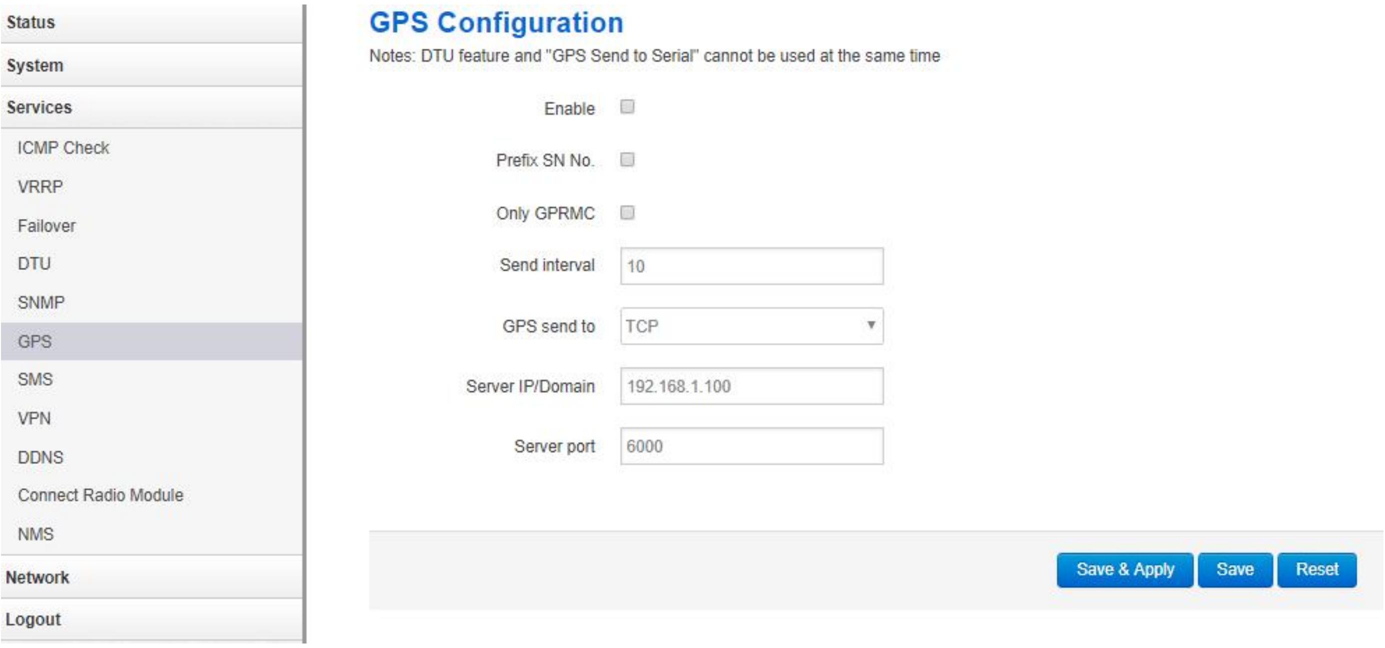
User	admin_user
Security Mode	Private
Authentication	MD5
Encryption	DES
Authentication Password	••••••••••
Encryption Password	••••••••••

- **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 CM770W-6G model)



GPS Configuration

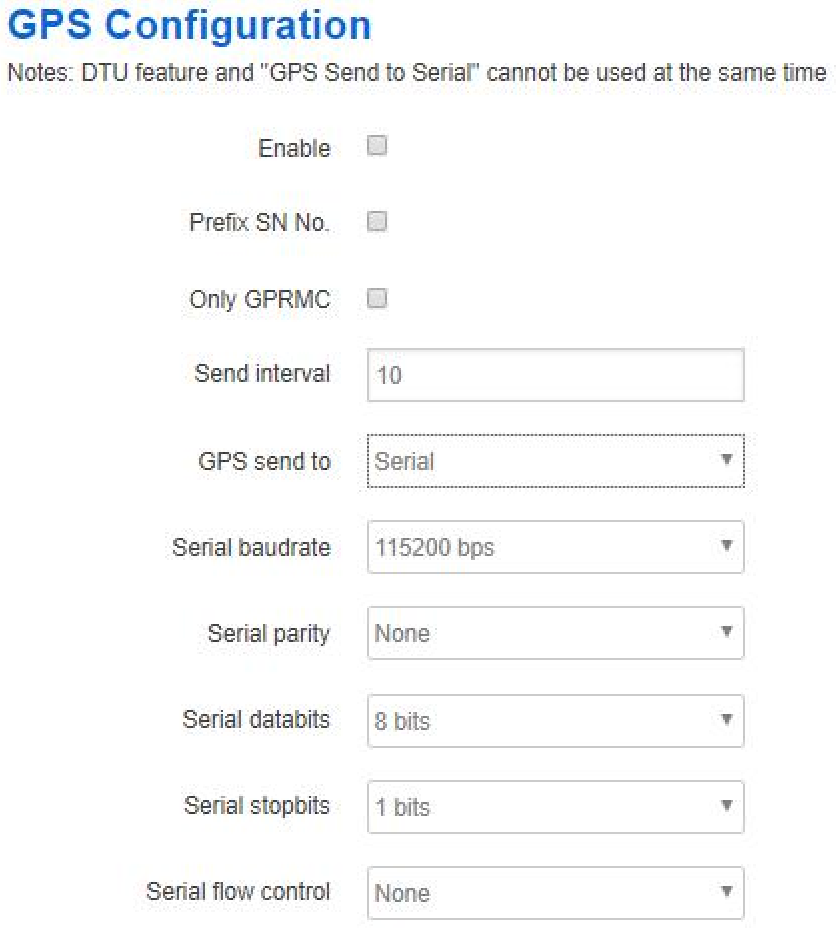
Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time

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.
- **Only GPRMC:** If checked, it will only send GPRMC data info (Longitude Latitude altitude)
- **Prefix SN No.:** If checked, it will add the router’s SN to the data packet.
- **Send interval:** Set the frequency of GPS data packets being sent.
- **GPS Send to**: Choose between “Serial” and “TCP/IP”. The router will only receive the GPS signal and will not process it. It will send this GPS signal to your GPS processor devices or servers. If the GPS processor device is connected to the CM770W-6 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

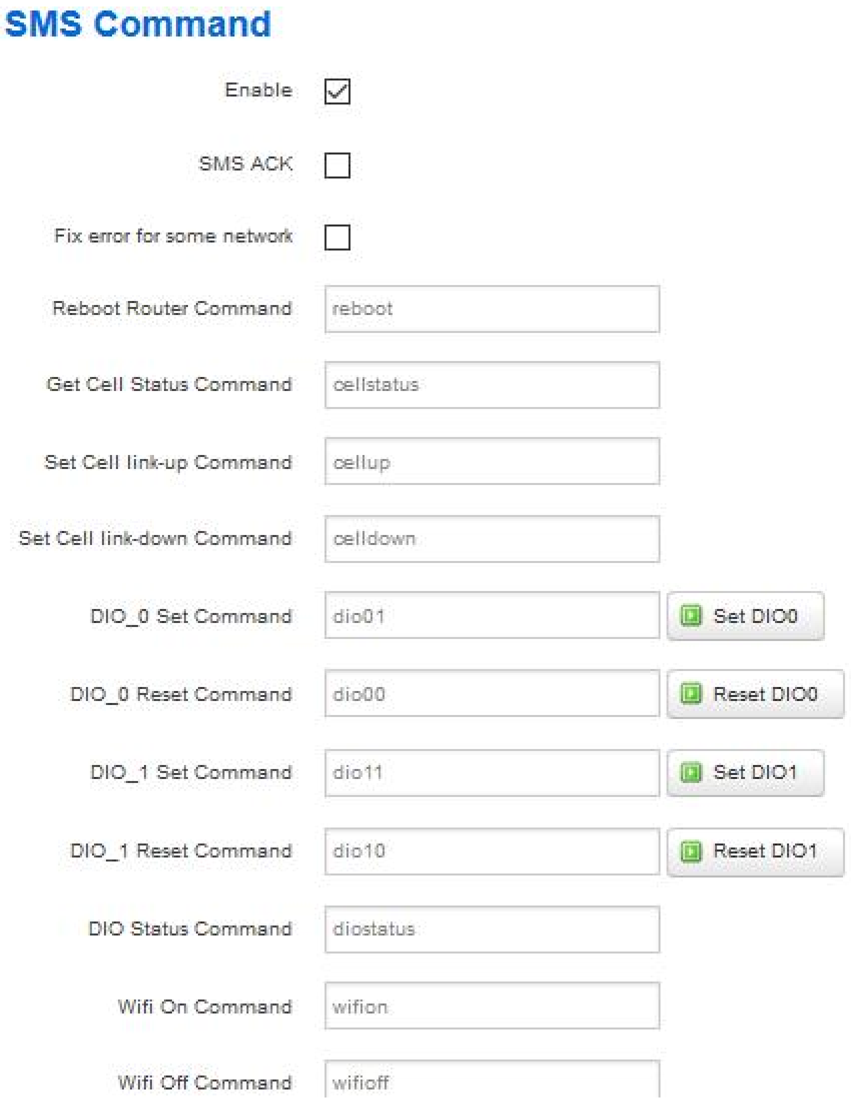
Notes: DTU feature and "GPS Send to Serial" cannot be used at the same time

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

DIO_0 Reset Command: dio00

DIO_1 Set Command: dio11

DIO_1 Reset Command: dio10

DIO Status Command: diostatus

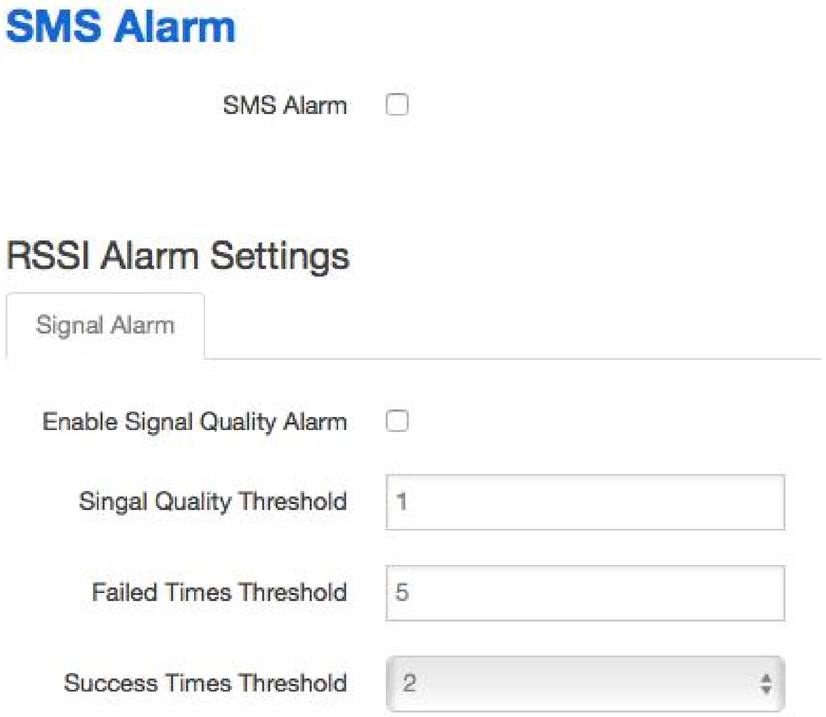
Wifi On Command: wifion

Wifi Off Command: wifioff

- **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

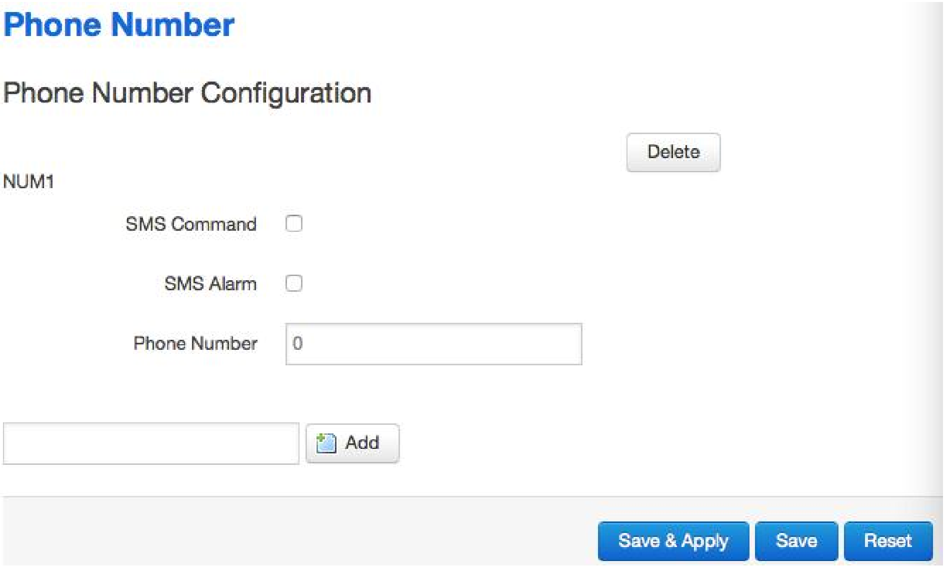
Success Times Threshold 2

- **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

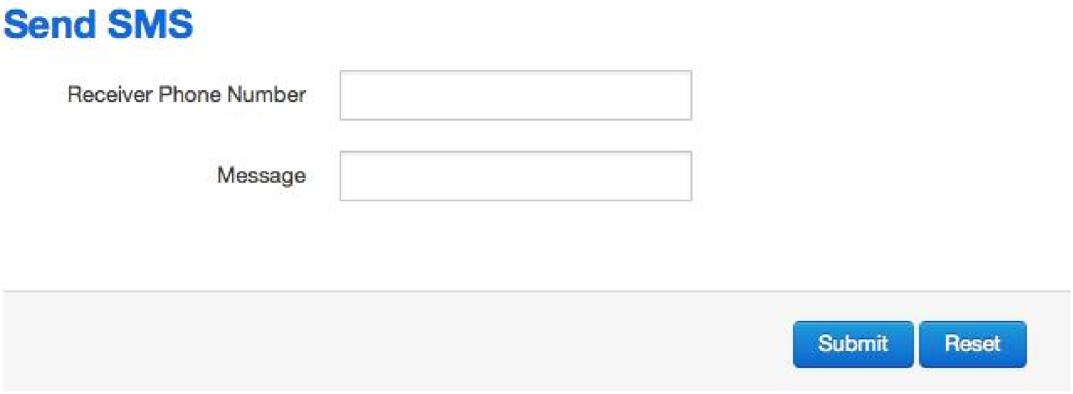
SMS Command □

SMS Alarm □

Phone Number: 0

- **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



Send SMS

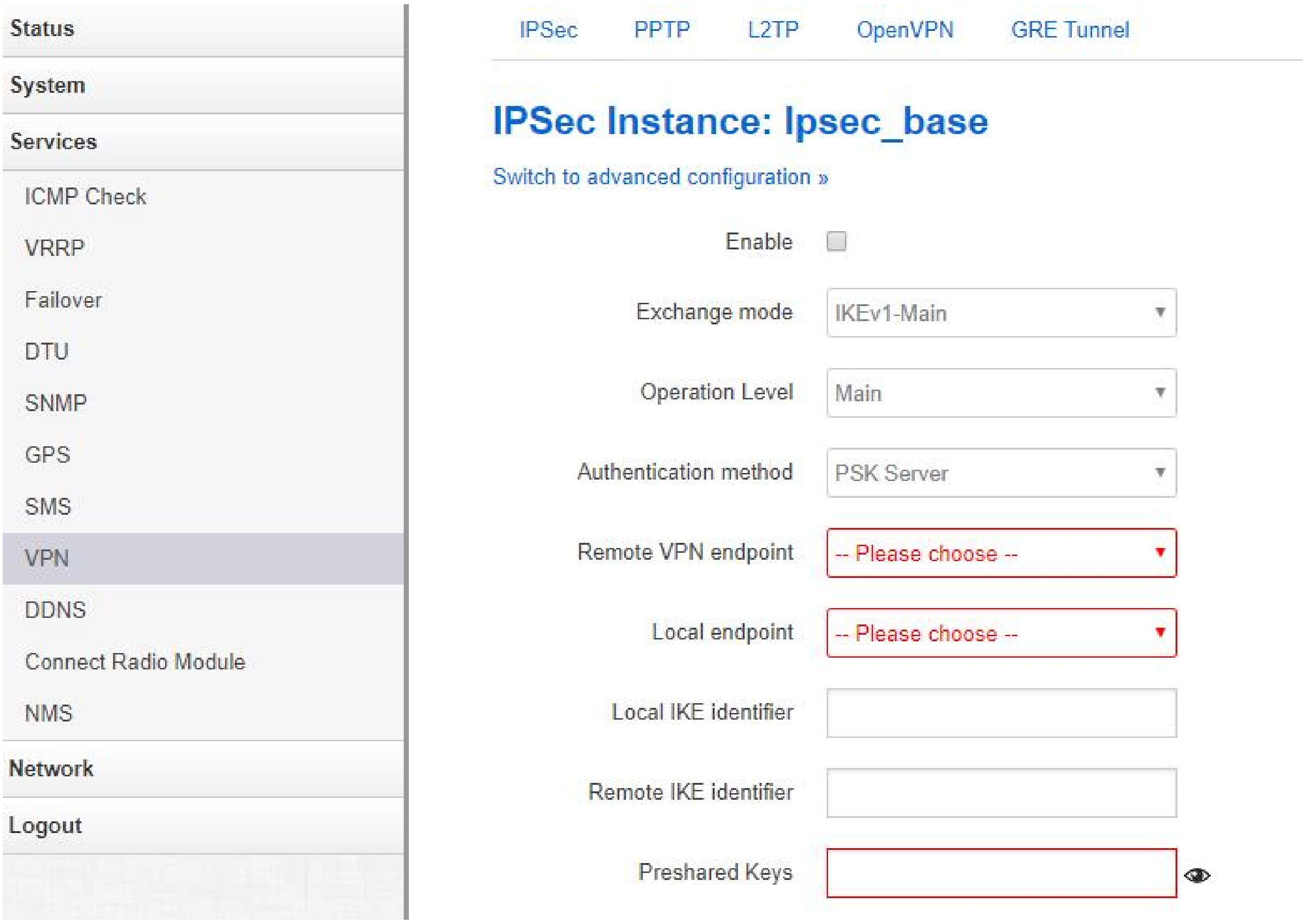
Receiver Phone Number

Message

- **Receiver Phone Number**: The phone number that receives SMS messages.
- **Message**: Message content.
- **Submit**: Click the button “Submit” to send the message immediately.

3.5.8 VPN

3.5.8.1 IPSEC



IPSec Instance: Ipsec_base

Enable □

Exchange mode: IKEv1-Main

Operation Level: Main

Authentication method: PSK Server

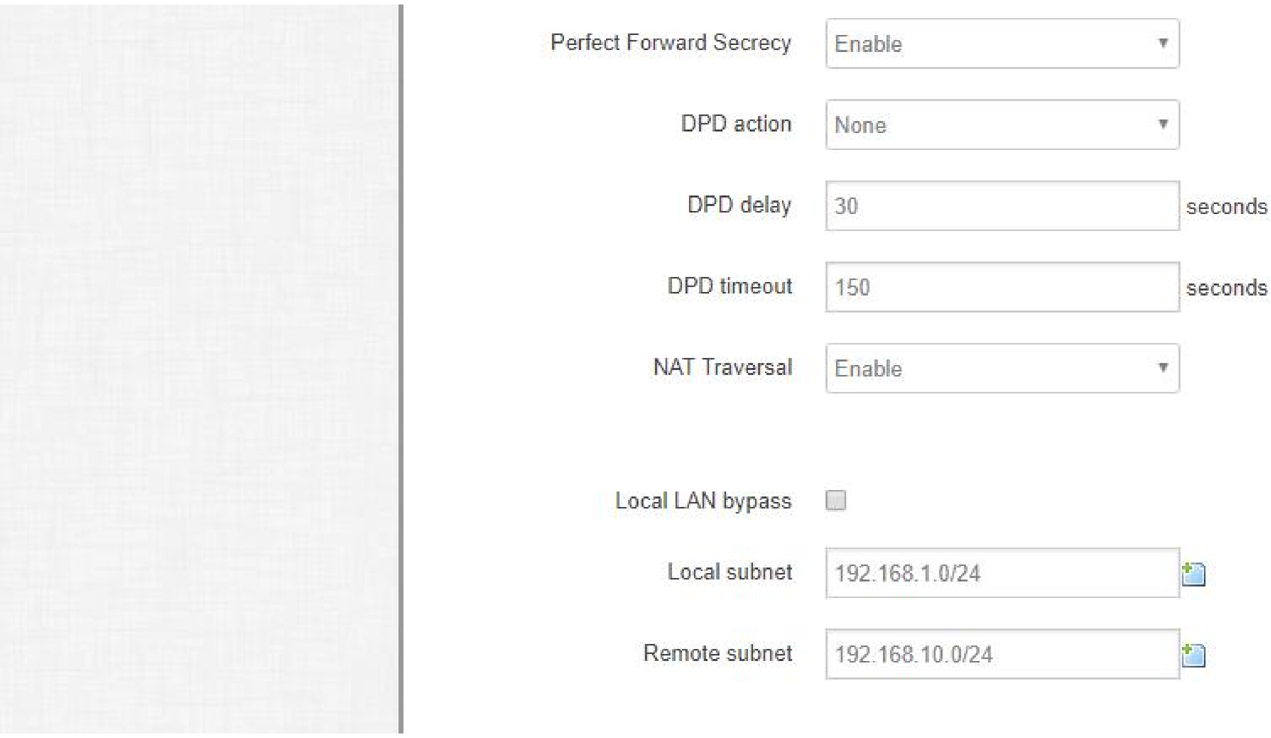
Remote VPN endpoint: -- Please choose --

Local endpoint: -- Please choose --

Local IKE identifier:

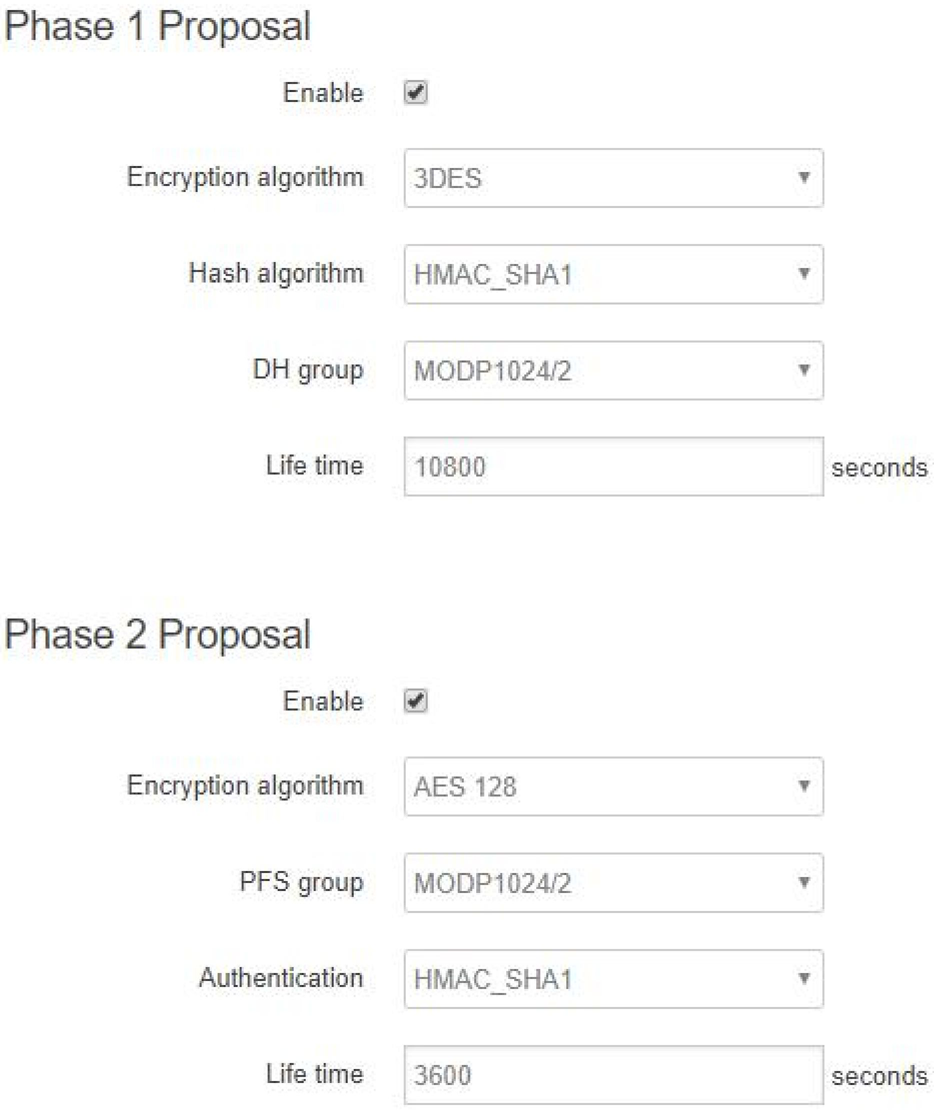
Remote IKE identifier:

Preshared Keys:



Perfect Forward Secrecy	Enable
DPD action	None
DPD delay	30 seconds
DPD timeout	150 seconds
NAT Traversal	Enable
Local LAN bypass	□
Local subnet	192.168.1.0/24
Remote subnet	192.168.10.0/24

- **Enable**: Enable IPSEC feature
- **Exchange mode**: IKEv1-Main, IKEv1-Aggressive and IKEv2-Main modes are supported.
- **Authentication method**: Client and Server. Client is the machine which starts the IPSEC connection.
- **Remote VPN endpoint**: Domain name or IP address of the remote endpoint. This needs to be accessed over the internet.
- **Preshared Keys**: This is known as PSK. The length is 16 to 32.
- **Local subnet**: The local subnet which connects to the IPSEC VPN.
- **Remote subnet**: The remote subnet which connects to the IPSEC VPN.



Phase 1 Proposal

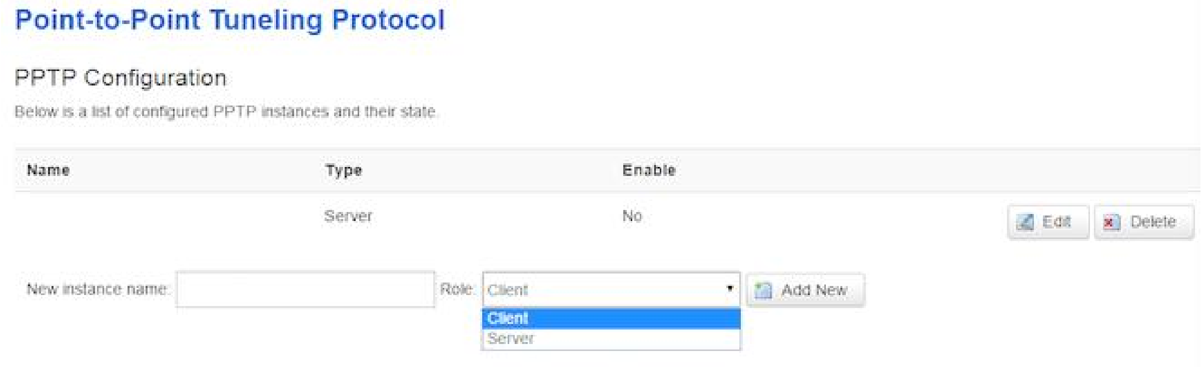
Enable	☑
Encryption algorithm	3DES ▾
Hash algorithm	HMAC_SHA1 ▾
DH group	MODP1024/2 ▾
Life time	10800 seconds

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 Tuneling Protocol

PPTP Configuration

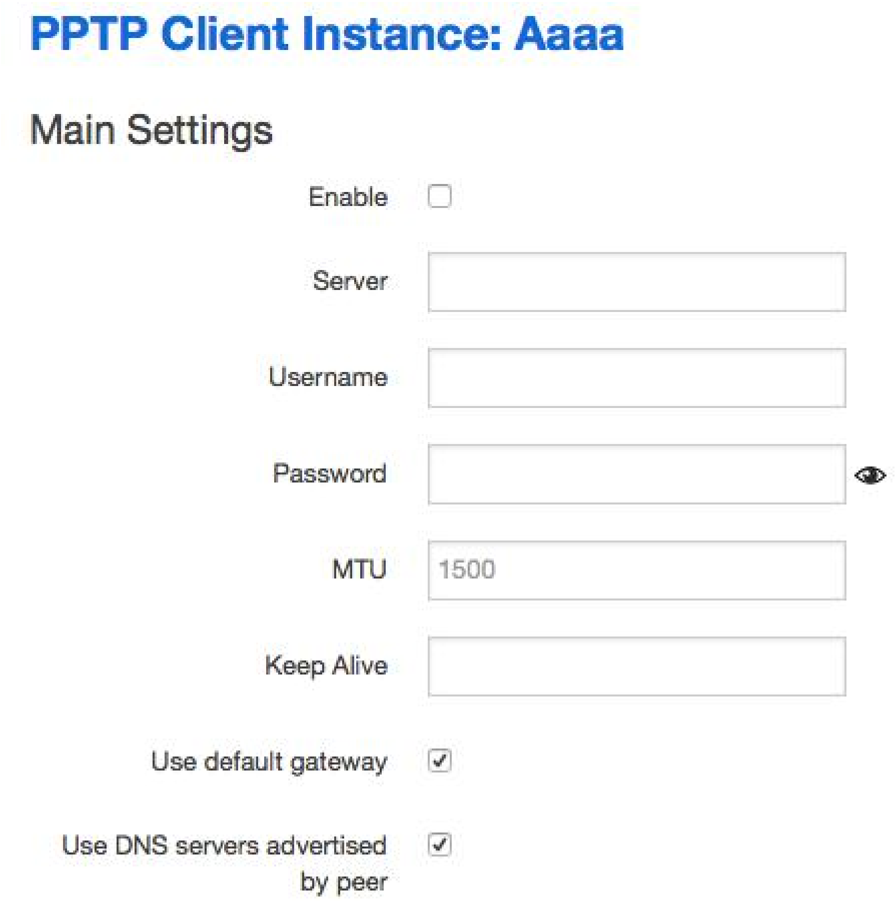
Below is a list of configured PPTP instances and their state.

Name	Type	Enable	
	Server	No	Edit Delete

New instance name: Role: Client ▾ Add New

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

- **PPTP Client configuration**



PPTP Client Instance: Aaaa

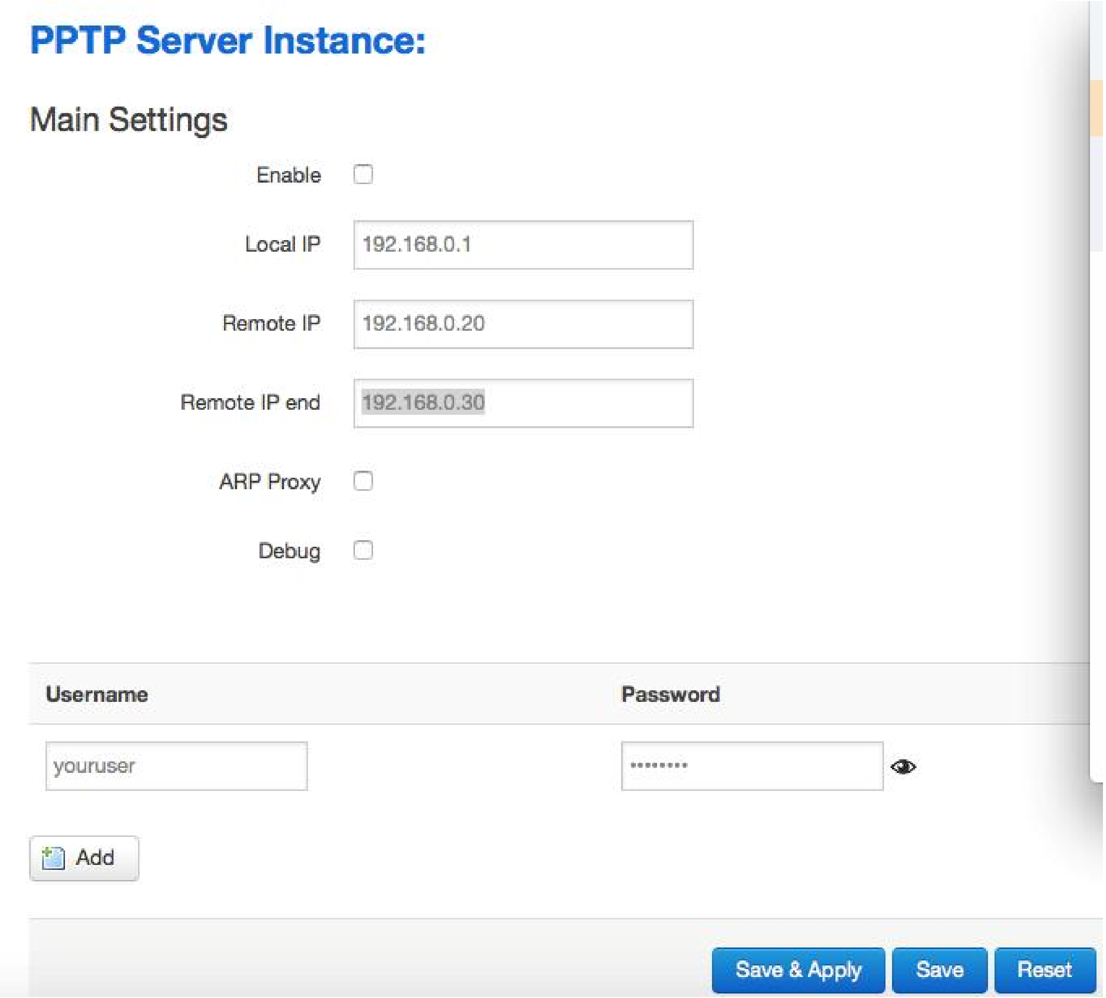
Main Settings

Enable	☐
Server	
Username	
Password	
MTU	1500
Keep Alive	
Use default gateway	☑
Use DNS servers advertised by peer	☑

- **Enable**: Enable this instance.
- **Server**: Domain name or IP address of PPTP server.
- **Username**: Server authentication username.
- **Password**: Server authentication password.
- **MTU**: Maximum Transmission Unit.

- **Keep Alive**: Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.
- **Use default gateway**: If unchecked, no default route is configured.
- **Use DNS servers advertised by peer**: If unchecked, the advertised DNS server addresses are ignored.

➢ PPTP Server Configuration



PPTP Server Instance:

Main Settings

Enable □

Local IP 192.168.0.1

Remote IP 192.168.0.20

Remote IP end 192.168.0.30

ARP Proxy □

Debug □

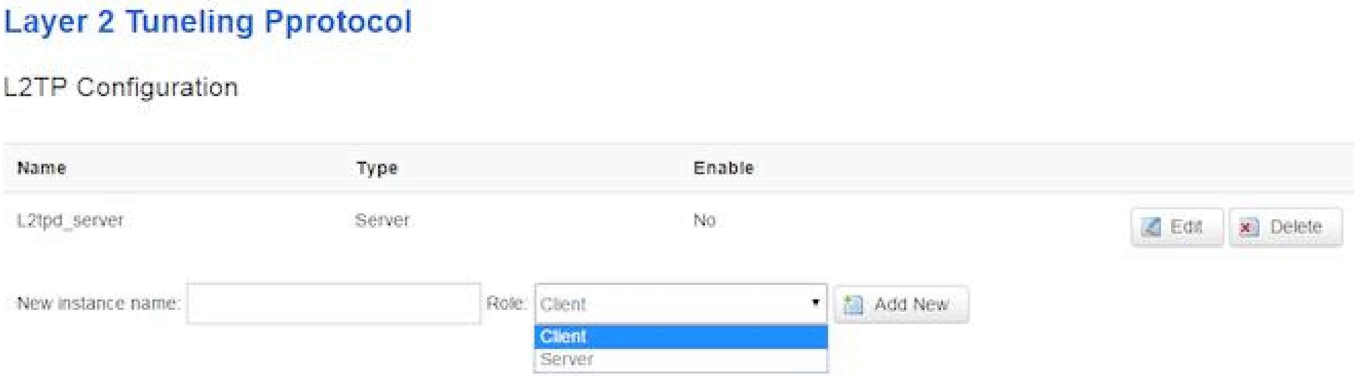
Username	Password
youruser	••••••••

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

- **Password**: Server authentication password.

3.5.8.3 L2TP

This page shows a list of configured L2TP instances and their state. Click the button “Edit” to make changes to an instance, or click the button “Delete” to delete it.



Layer 2 Tuneling Pprotocol

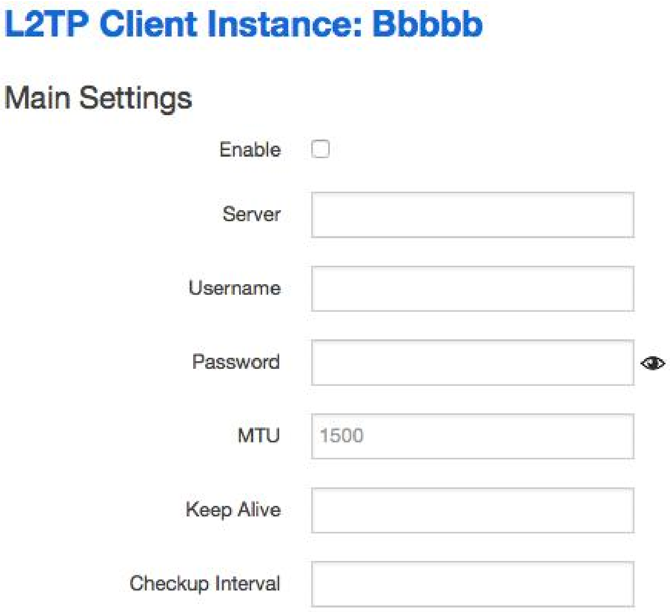
L2TP Configuration

Name	Type	Enable	
L2tpd_server	Server	No	Edit Delete

New instance name: ______ Role: Client ▾ Add New

Client
Server

- **L2TP Client configuration**



L2TP Client Instance: Bbbbb

Main Settings

Enable □

Server

Username

Password

MTU 1500

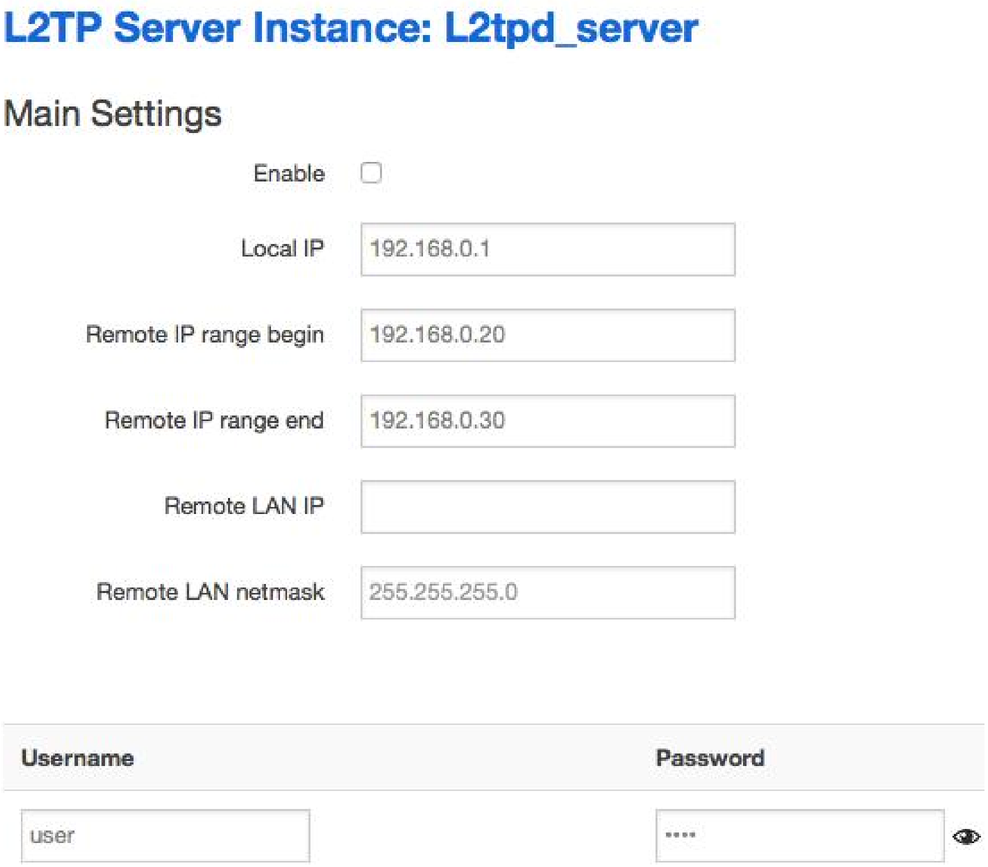
Keep Alive

Checkup Interval

- **Enable**: Enable this L2TP instance.
- **Server**: Domain name or IP address of L2TP server.

- **Username**: Server authentication username.
- **Password**: Server authentication password.
- **MTU**: Maximum Transmission Unit.
- **Keep Alive**: Number of unanswered echo requests before considering the peer dead. The interval between echo requests is 5 seconds.
- **Checkup Interval**: Number of seconds to pass before checking if the interface is not up since the last setup attempt and retry the connection otherwise. Set it to a value sufficient for a successful L2TP connection for you. It's mainly for the case that netifd sent the connect request yet xl2tpd failed to complete it without the notice of netifd.

➢ **L2TP Server configuration**



L2TP Server Instance: L2tpd_server

Main Settings

Enable ☐

Local IP: 192.168.0.1

Remote IP range begin: 192.168.0.20

Remote IP range end: 192.168.0.30

Remote LAN IP:

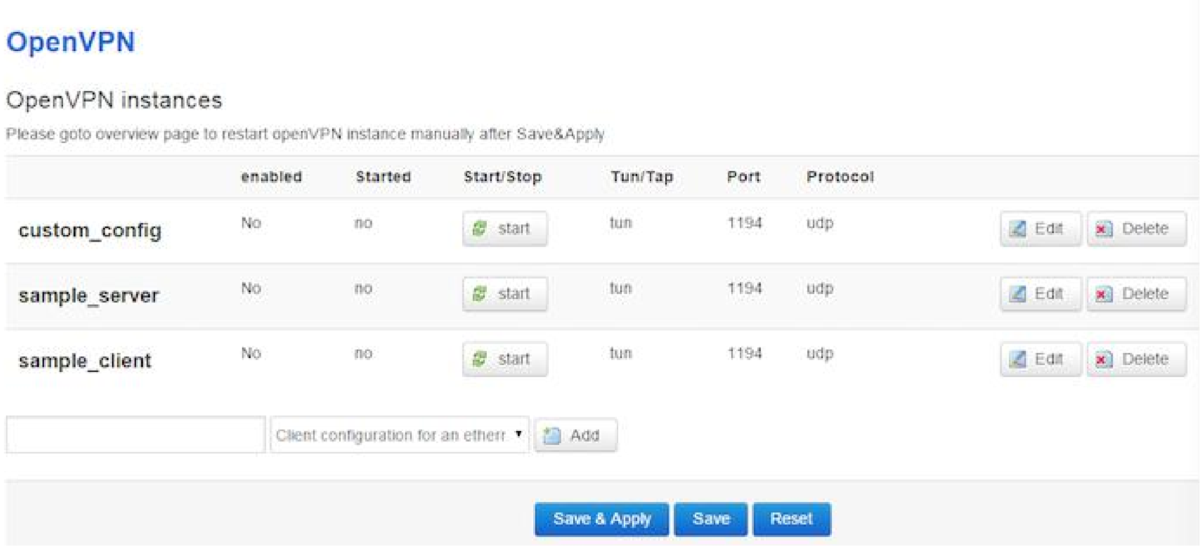
Remote LAN netmask: 255.255.255.0

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

3.5.8.4 OpenVPN

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



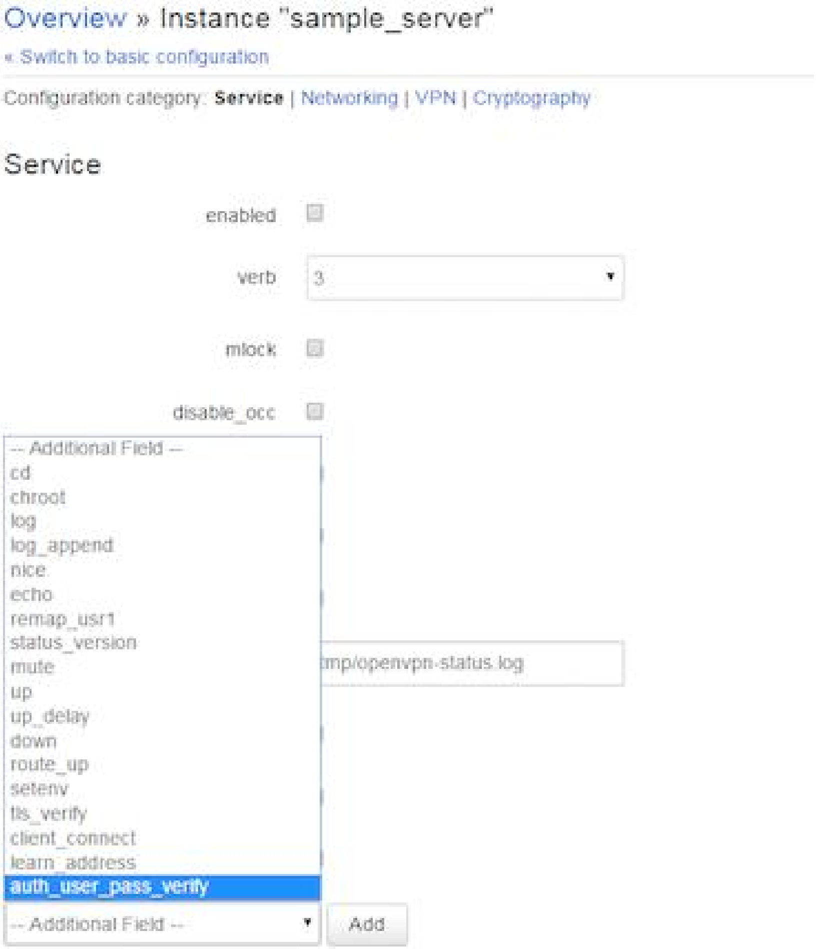
OpenVPN

OpenVPN instances

Please goto overview page to restart openVPN instance manually after Save&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

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 basic configuration

Configuration category: **Service** | Networking | VPN | Cryptography

Service

enabled □

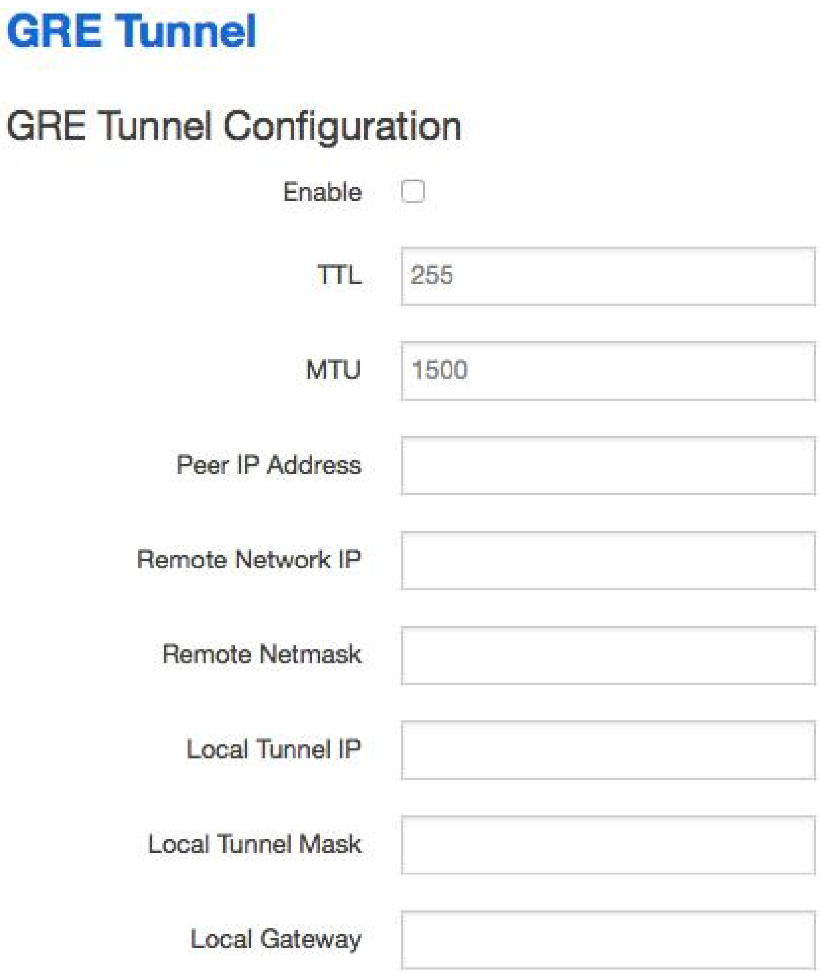
verb 3

mlock □

disable_occ □

mp/openvpn-status.log

3.5.8.5 GRE tunnel



GRE Tunnel

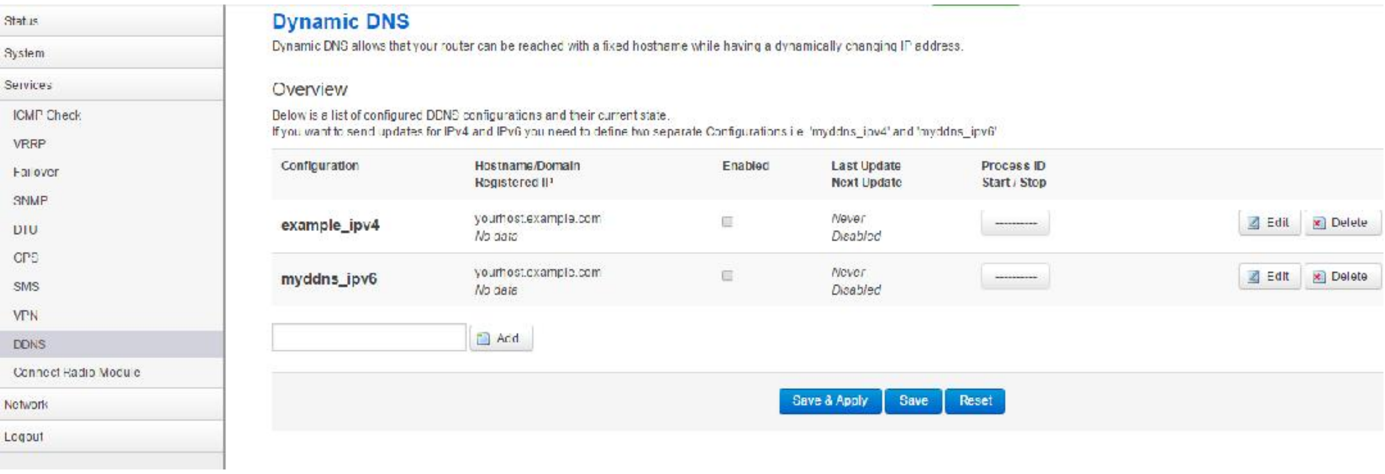
GRE Tunnel Configuration

Enable	☐
TTL	255
MTU	1500
Peer IP Address	
Remote Network IP	
Remote Netmask	
Local Tunnel IP	
Local Tunnel Mask	
Local Gateway	

- **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.
- **Remote Netmask**: Remote LAN subnet mask.
- **Local Tunnel IP**: Virtual IP address. This cannot be in the same subnet as the LAN network.
- **Local Tunnel Mask**: Virtual IP mask.
- **Local Gateway**: Local gateway

3.5.9 DDNS

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



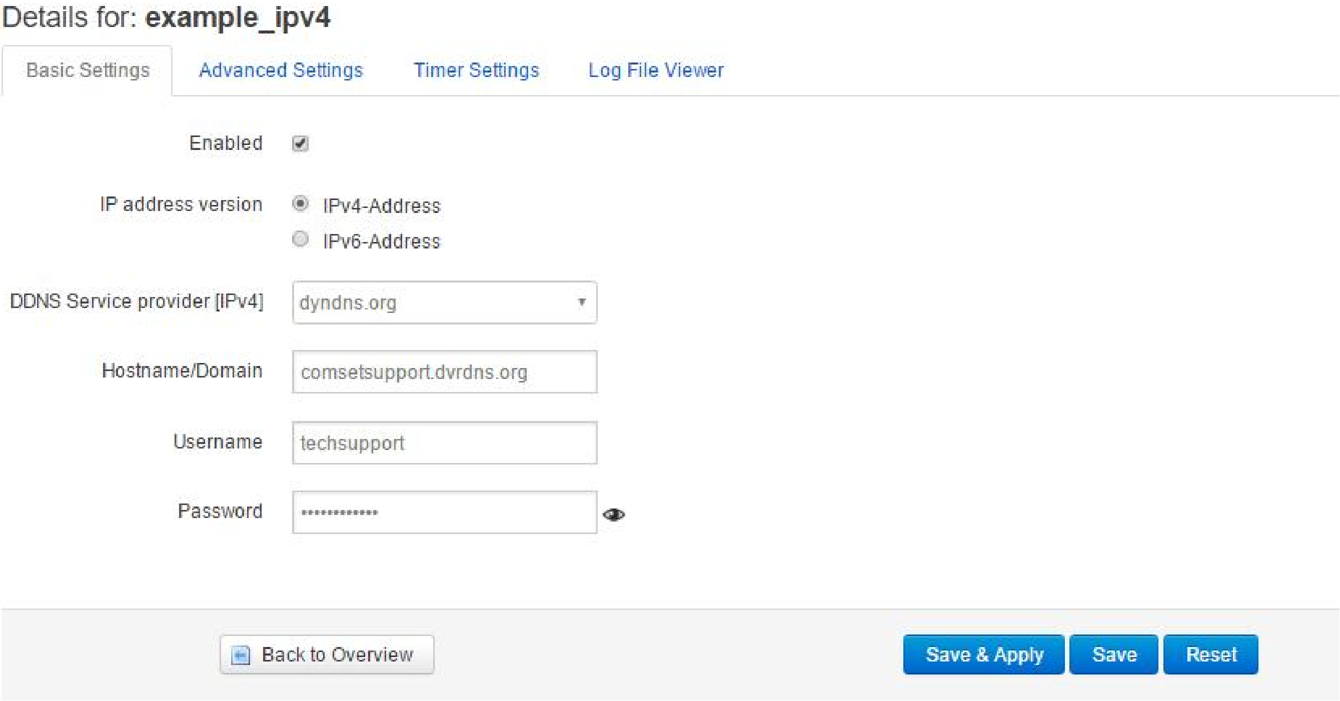
Dynamic DNS

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

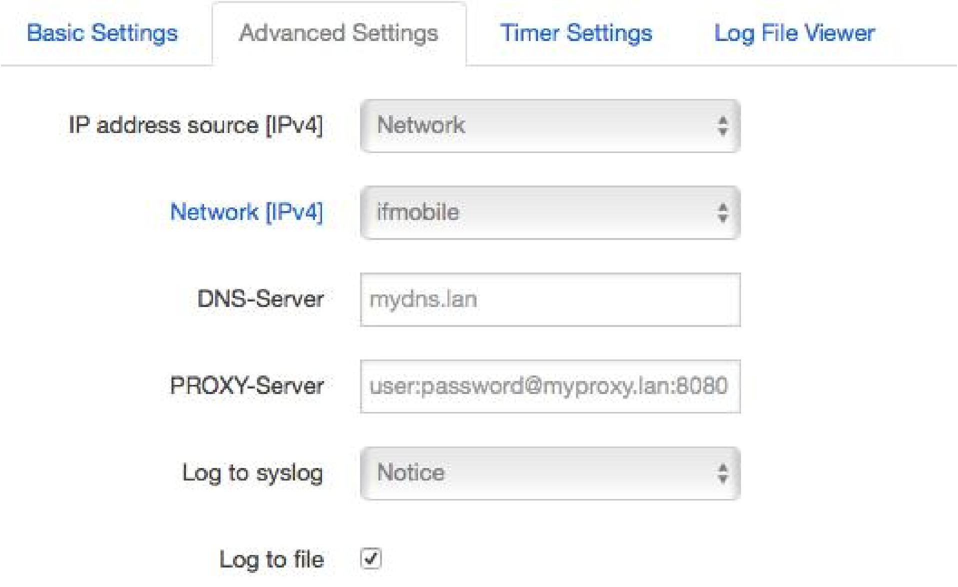
DDNS Service provider [IPv4] dyndns.org

Hostname/Domain comsetsupport.dvrdns.org

Username techsupport

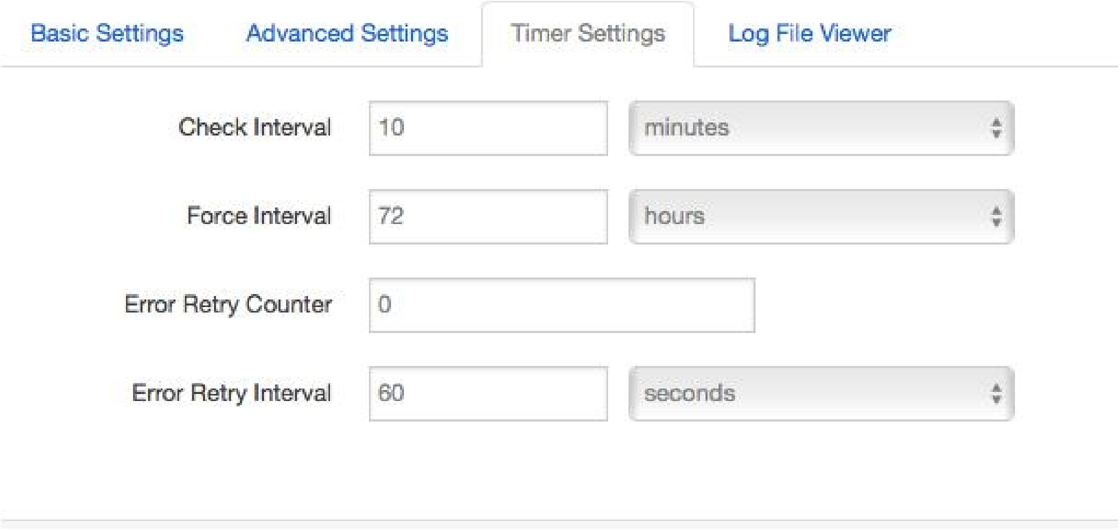
Password ••••••••••••

- **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.



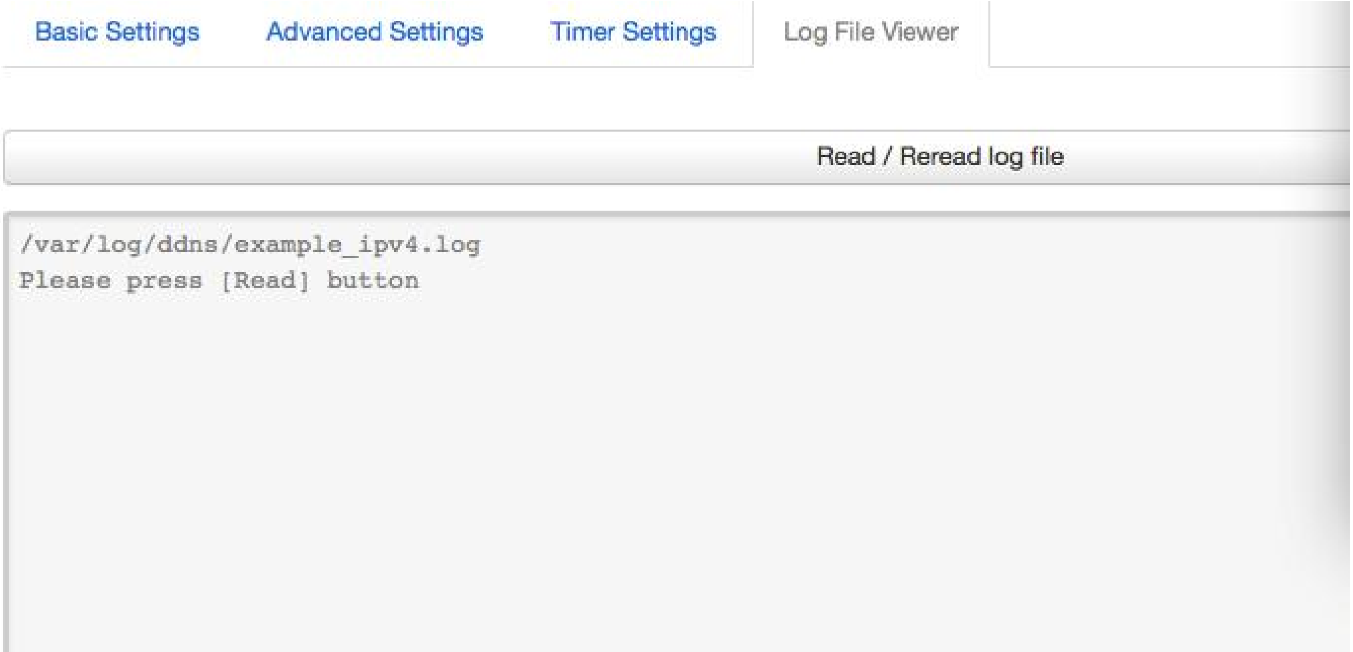
IP address source [IPv4]: Network
Network [IPv4]: ifmobile
DNS-Server: mydns.lan
PROXY-Server: user:password@myproxy.lan:8080
Log to syslog: Notice
Log to file: ☑

- **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.



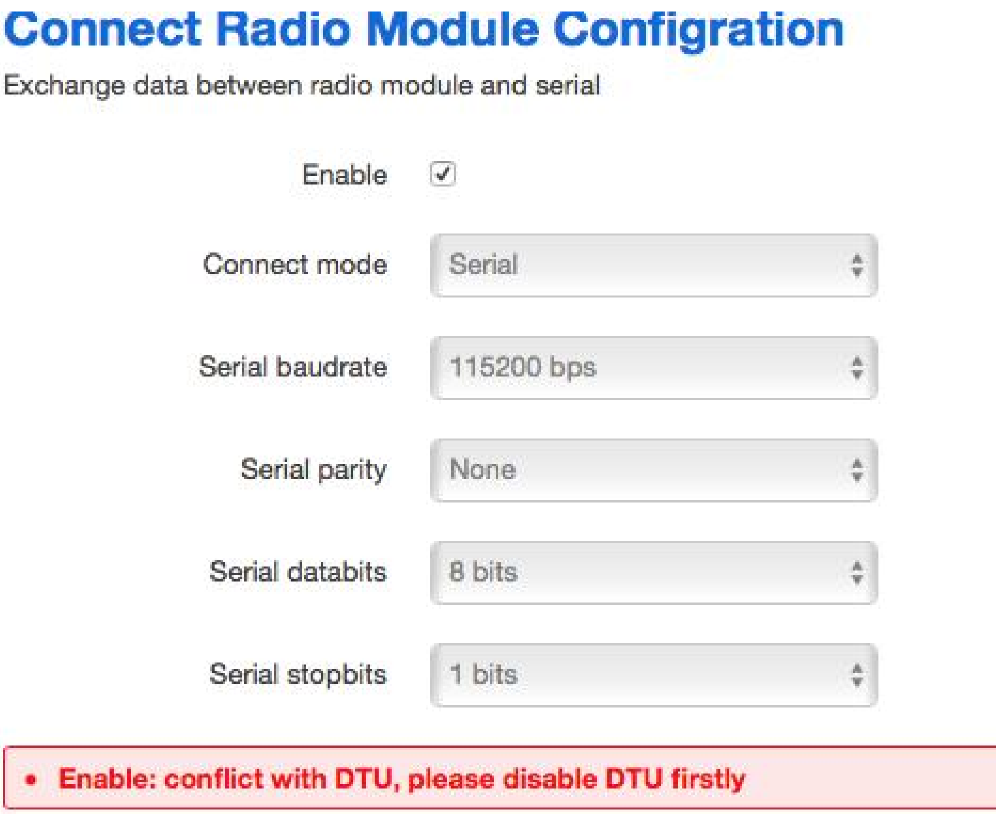
```
/var/log/ddns/example_ipv4.log
Please press [Read] button
```

Read the log file of DDNS.

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 Configration

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

- Enable: conflict with DTU, please disable DTU firstly

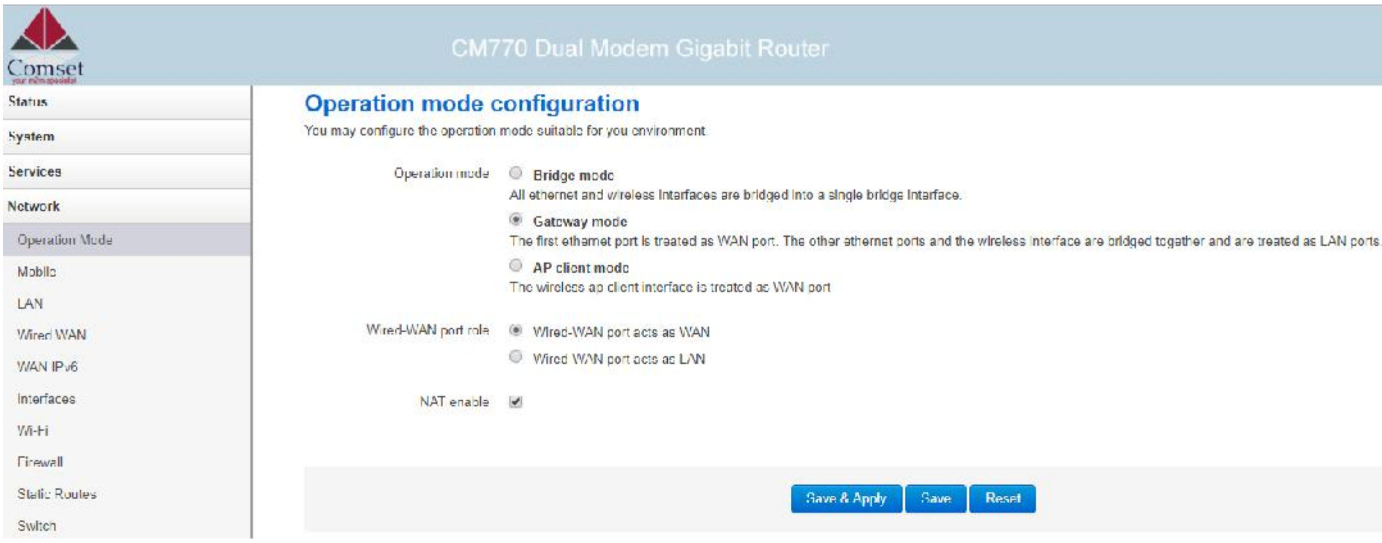
- **Connect Mode:** Serial only

Modem to Serial Settings

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

3.6 Network Configuration

3.6.1 Operation Mode



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

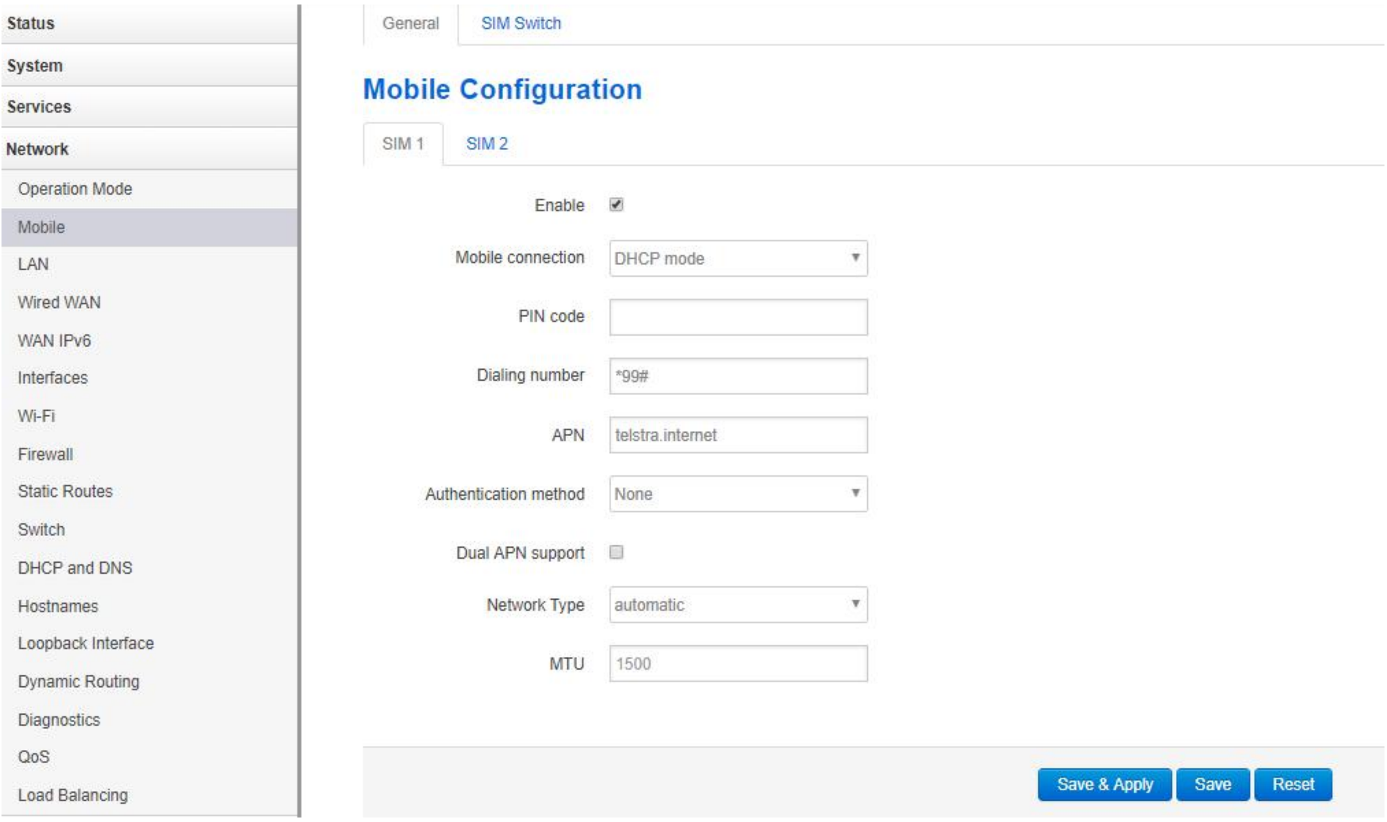
NAT enable ☑

- **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
  Wired-WAN port acts as LAN

The default operation is in “Gateway mode”.

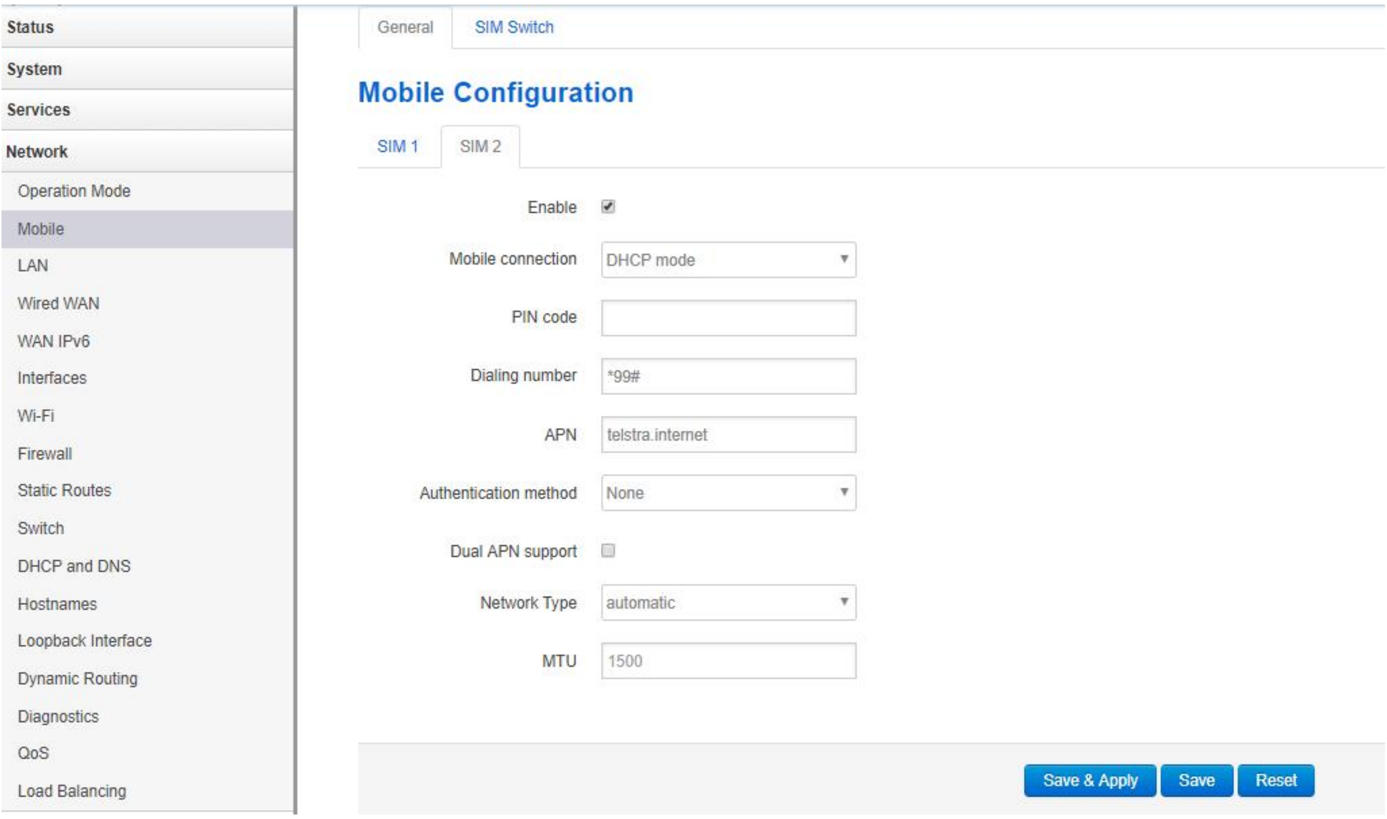
3.6.2 Mobile configuration

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



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



Mobile Configuration

Enable ☑

Mobile connection: DHCP mode

PIN code:

Dialing number: *99#

APN: telstra.internet

Authentication method: None

Dual APN support □

Network Type: automatic

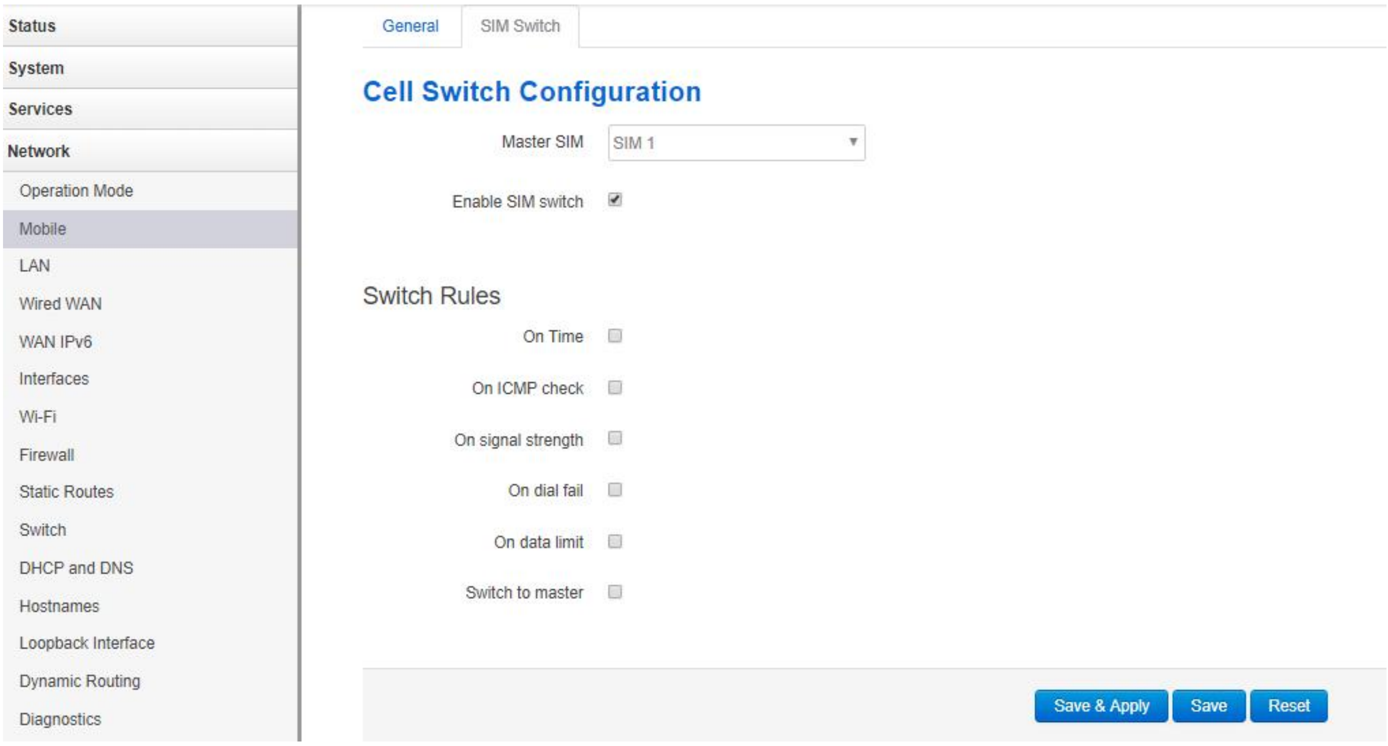
MTU: 1500

- **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 number:** Most SIM cards don’t have a PIN number, in which case you leave this field blank;
- **Dialing number:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider;
- **Authentication method:** There are three options to choose from (None, PAP, CHAP). Please confirm with your carrier the type of authentication. Normally select *None*;
- **Username:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider;

Note: If your SIM card has no username, please input the default value, otherwise the router may not dialup. If the authentication method is ‘None’, this option will not appear.

- **Password:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider.
- **Network Type:** Different Cell Modems support different types. The default value is *Automatic*.
- **MTU:** Maximum Transmission Unit. It is the maximum size of packets transmitted on the network. The default value is 1500. Please configure it to optimise your own network.

3.6.3 SIM Switch



Cell Switch Configuration

Master SIM: SIM 1

Enable SIM switch ☑

Switch Rules

On Time □

On ICMP check □

On signal strength □

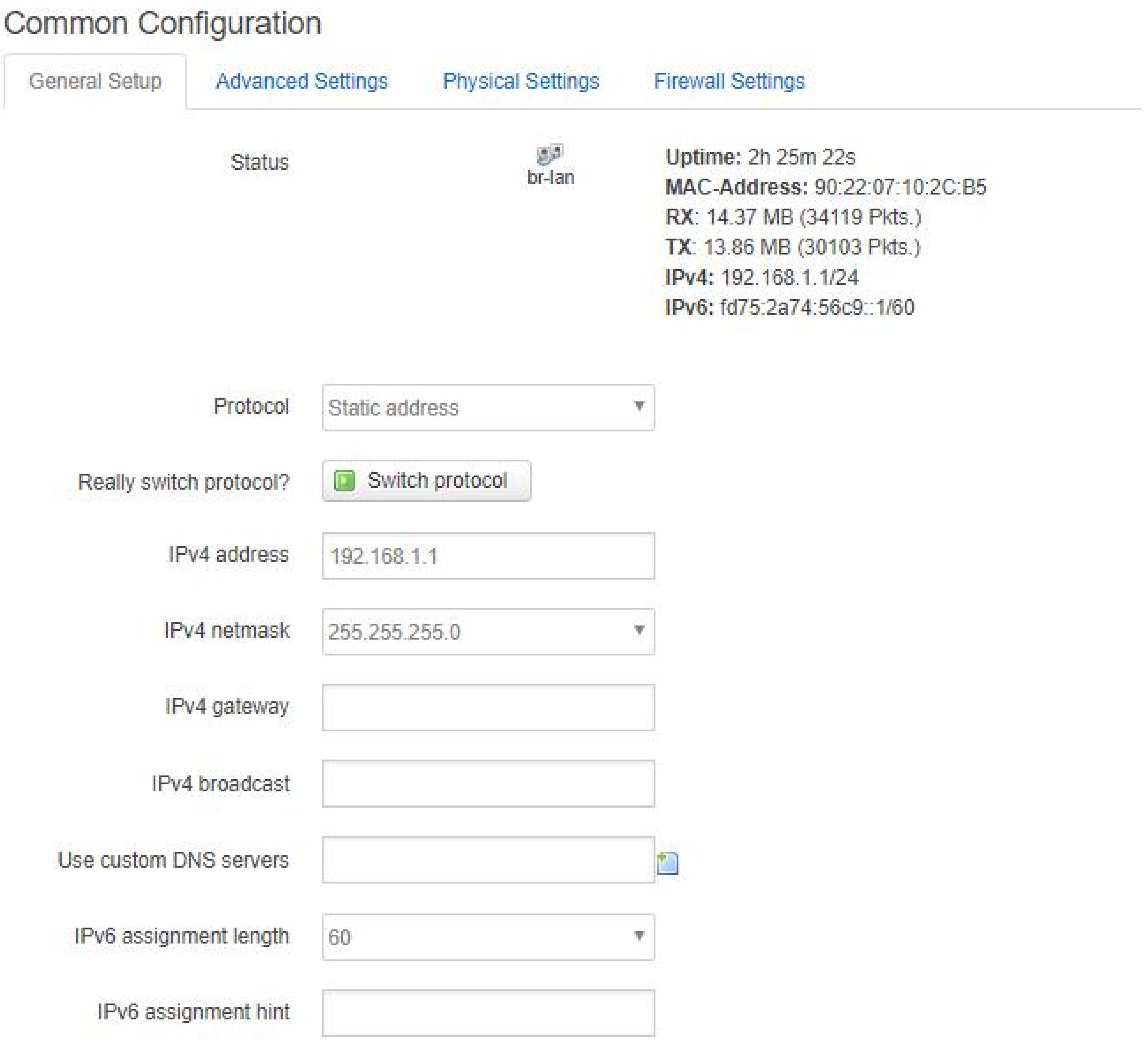
On dial fail □

On data limit □

Switch to master □

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

3.6.4 LAN settings



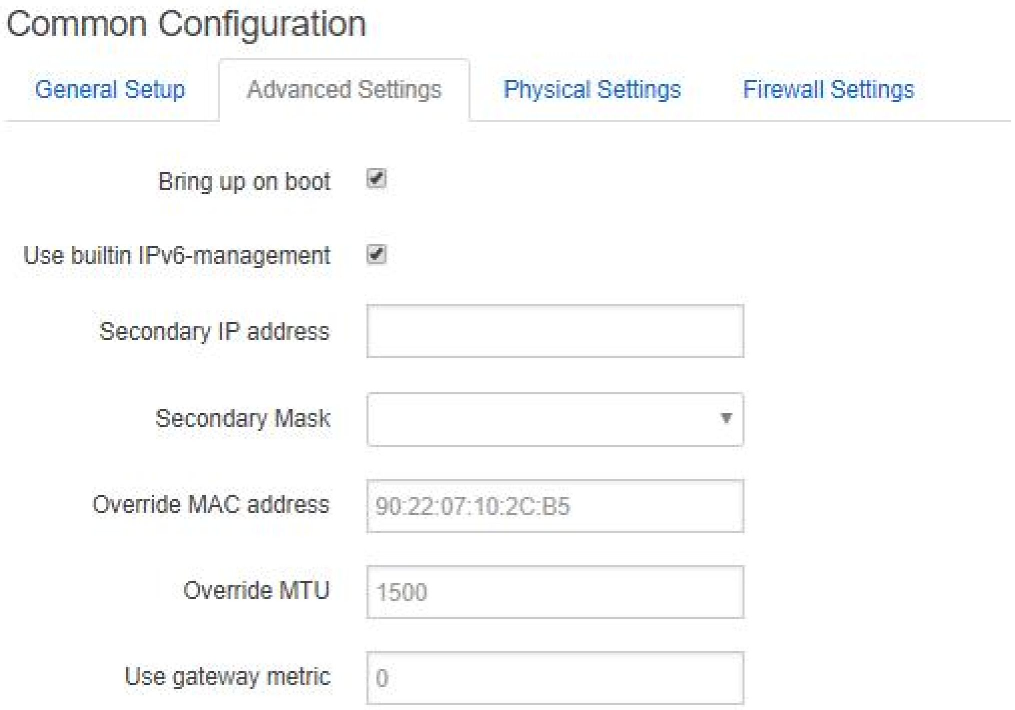
Common Configuration

Status br-lan

Uptime: 2h 25m 22s
MAC-Address: 90:22:07:10:2C:B5
RX: 14.37 MB (34119 Pkts.)
TX: 13.86 MB (30103 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fd75:2a74:56c9::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.



Common Configuration

Bring up on boot ☑

Use builtin IPv6-management ☑

Secondary IP address

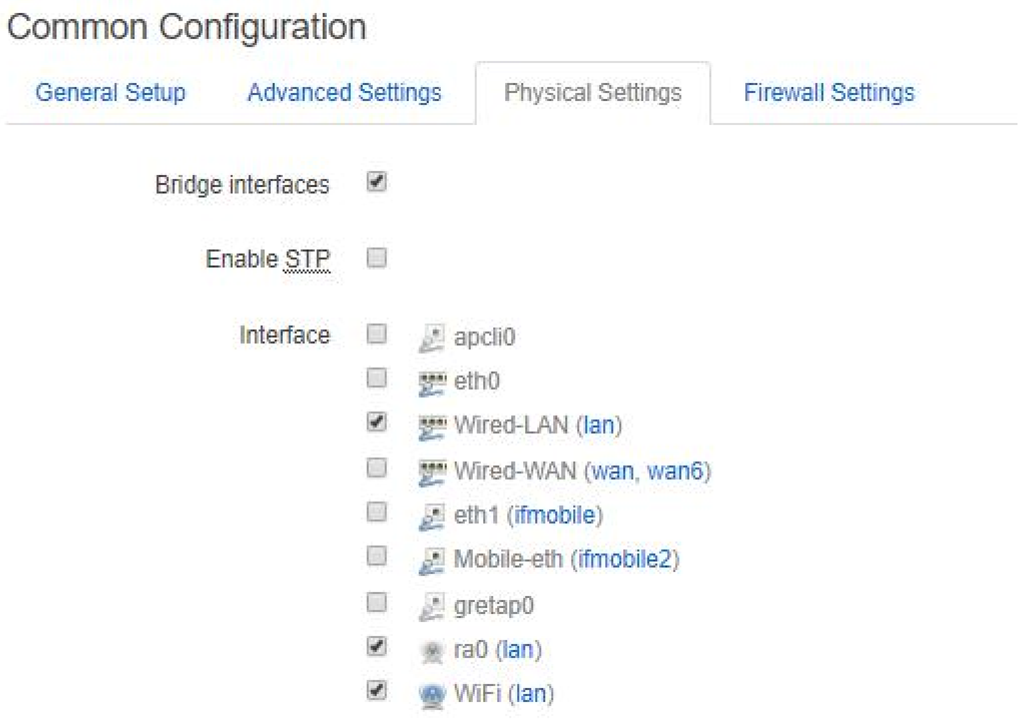
Secondary Mask

Override MAC address 90:22:07:10:2C:B5

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.



Common Configuration

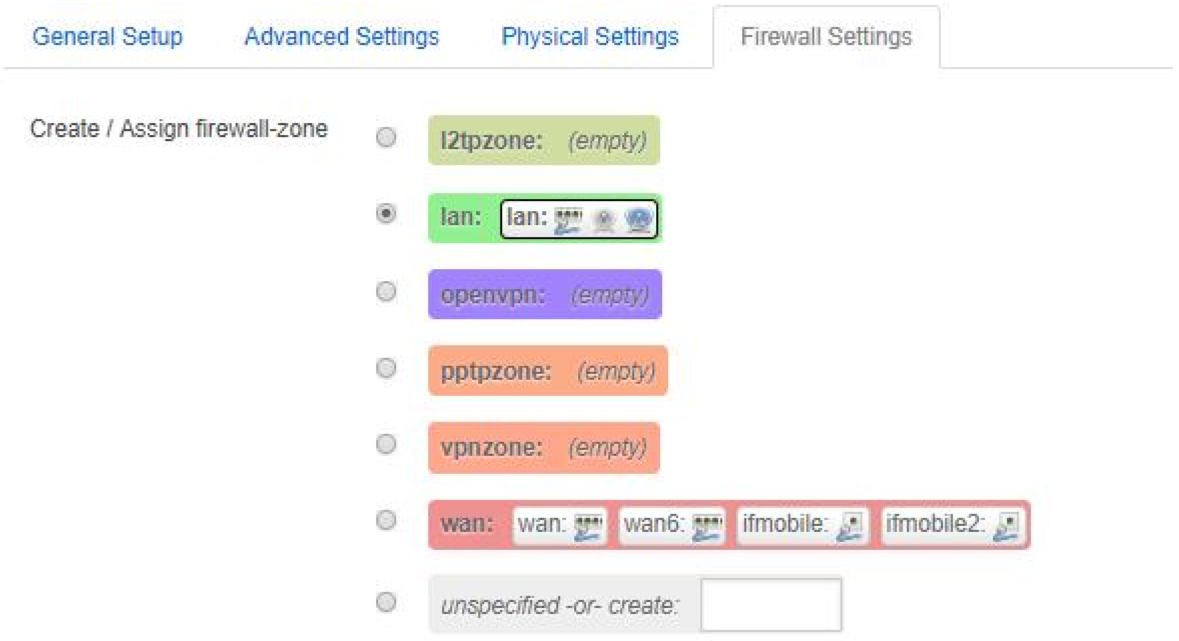
General Setup | Advanced Settings | Physical Settings | Firewall Settings

Bridge interfaces ☑

Enable STP ☐

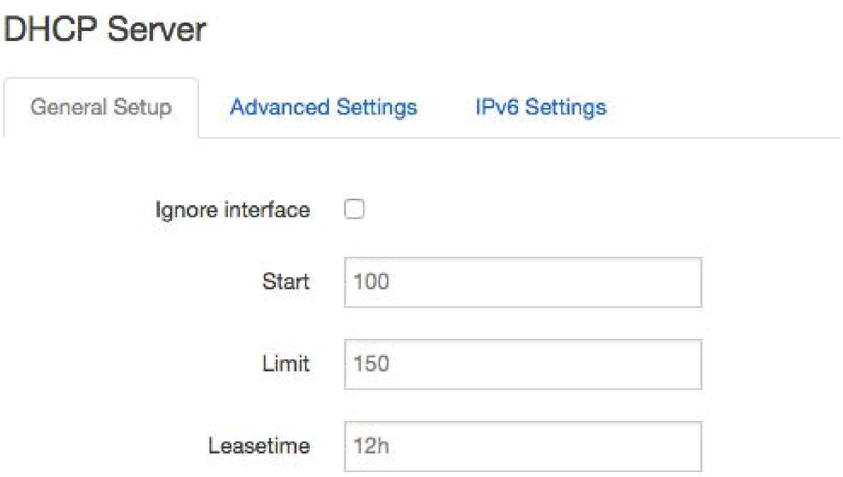
Interface
☐ apcli0
☐ eth0
☑ Wired-LAN (lan)
☐ Wired-WAN (wan, wan6)
☐ eth1 (ifmobile)
☐ Mobile-eth (ifmobile2)
☐ gretap0
☑ ra0 (lan)
☑ WiFi (lan)

- **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.



General Setup | Advanced Settings | Physical Settings | Firewall Settings

Create / Assign firewall-zone
○ l2tpzone: (empty)
● lan: lan:
○ openvpn: (empty)
○ pptpzone: (empty)
○ vpnzone: (empty)
○ wan: wan: wan6: ifmobile: ifmobile2:
○ unspecified -or- create:



DHCP Server

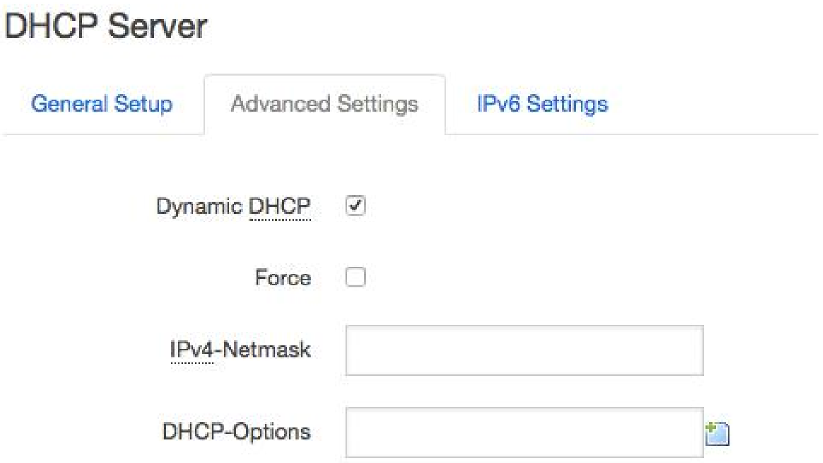
Ignore interface □

Start 100

Limit 150

Leasetime 12h

- **Ignore interface**: If it is unchecked, 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).



DHCP Server

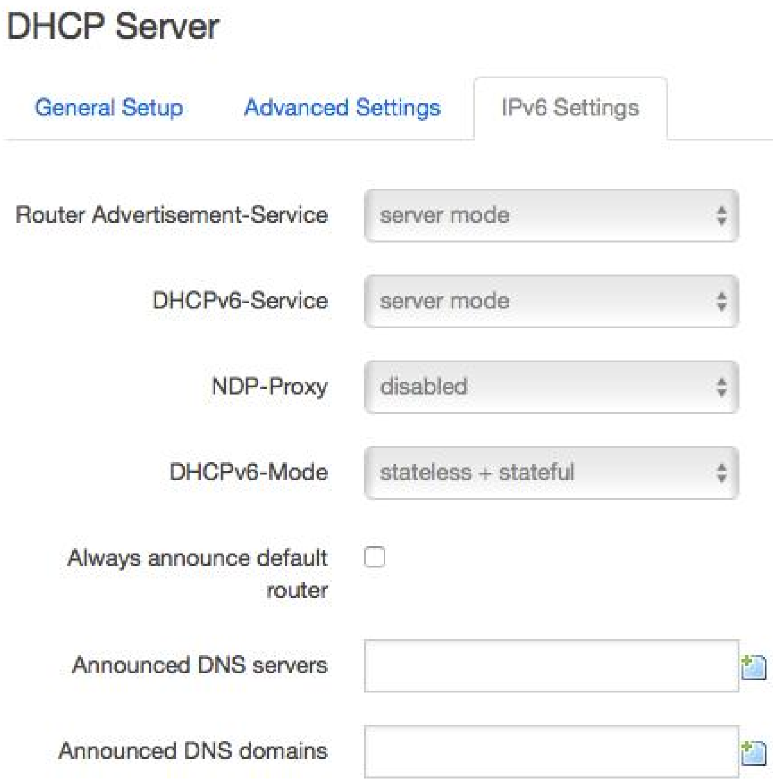
Dynamic DHCP ☑

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 ‘192.168.2.1 and 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

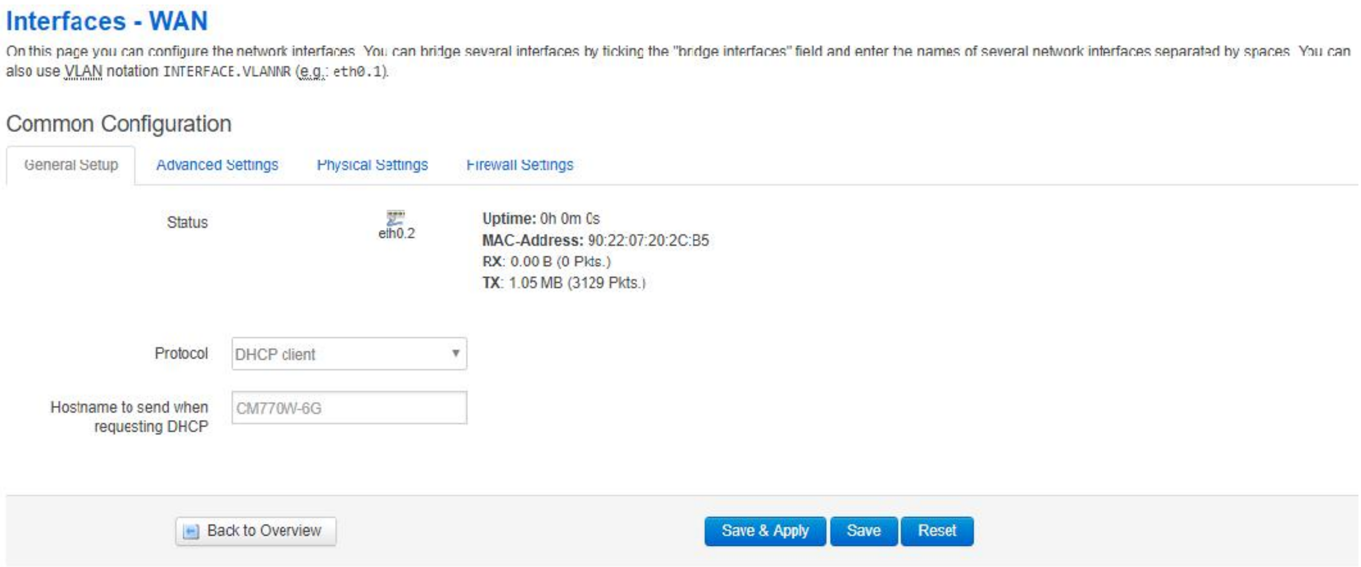
Always announce default router: □

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: 90:22:07:20:2C:B5
RX: 0.00 B (0 Pkts.)
TX: 1.05 MB (3129 Pkts.)

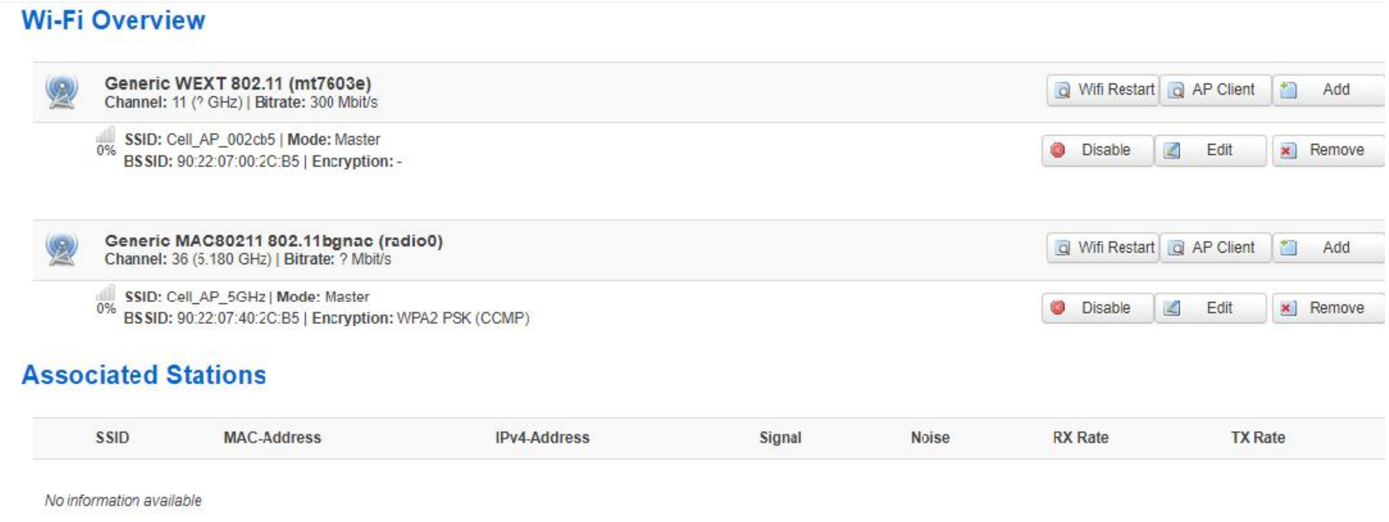
Protocol: DHCP client

Hostname to send when requesting DHCP: CM770W-6G

- **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 WEXT 802.11 (mt7603e)
Channel: 11 (? GHz) | **Bitrate:** 300 Mbit/s

0% **SSID:** Cell_AP_002cb5 | **Mode:** Master
BSSID: 90:22:07:00:2C:B5 | **Encryption:** -

Generic MAC80211 802.11bgnac (radio0)
Channel: 36 (5.180 GHz) | **Bitrate:** ? Mbit/s

0% **SSID:** Cell_AP_5GHz | **Mode:** Master
BSSID: 90:22:07:40:2C:B5 | **Encryption:** WPA2 PSK (CCMP)

Associated Stations

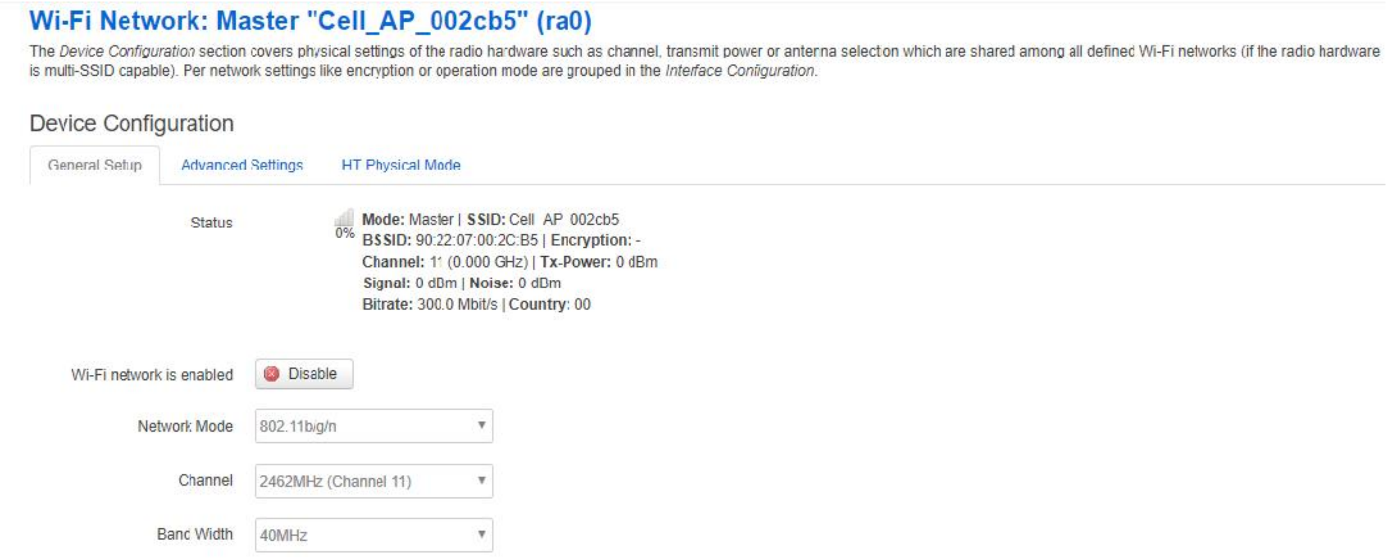
SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate

No information available

- **Wifi Restart**: turn WiFi off then on.

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

3.6.6.1 Wifi General configuration



Wi-Fi Network: Master "Cell_AP_002cb5" (ra0)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined Wi-Fi networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

Status: 0%
Mode: Master | **SSID:** Cell AP 002cb5
BSSID: 90:22:07:00:2C:B5 | **Encryption:** -
Channel: 11 (0.000 GHz) | **Tx-Power:** 0 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 300.0 Mbit/s | **Country:** 00

Wi-Fi network is enabled: Disable

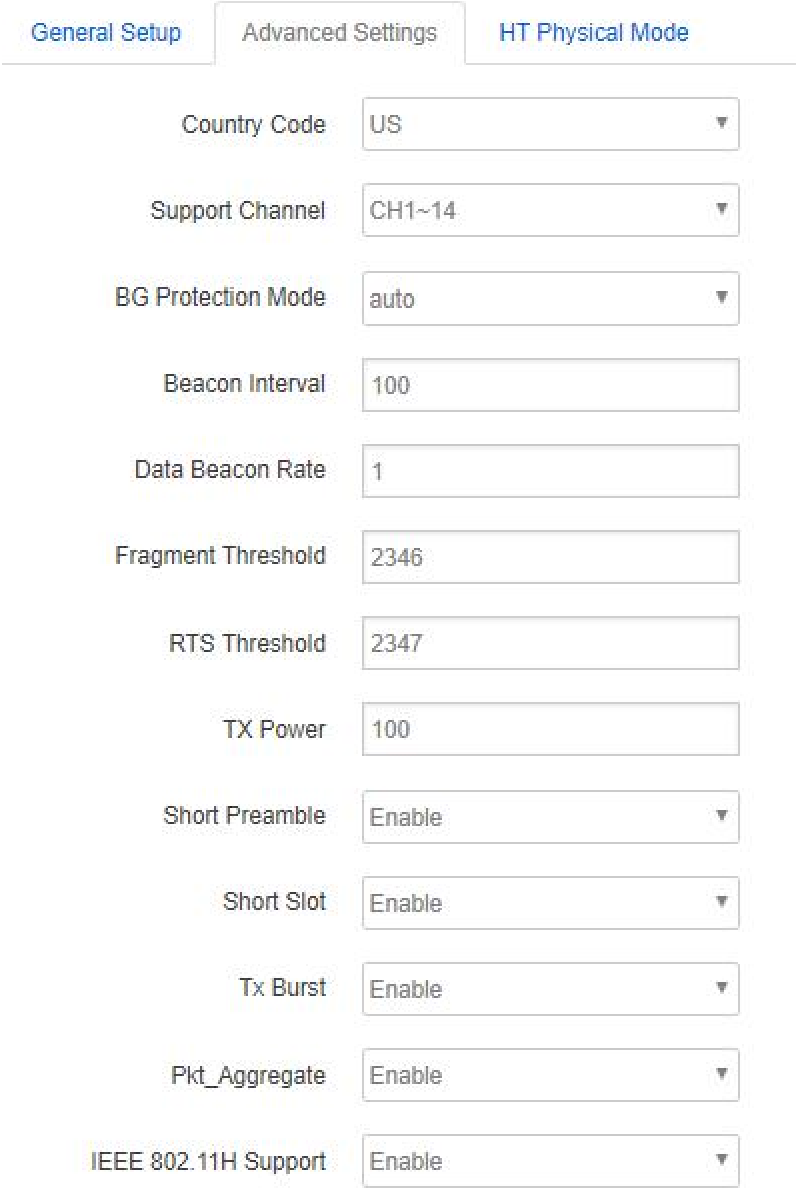
Network Mode: 802.11b/g/n

Channel: 2462MHz (Channel 11)

Band Width: 40MHz

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

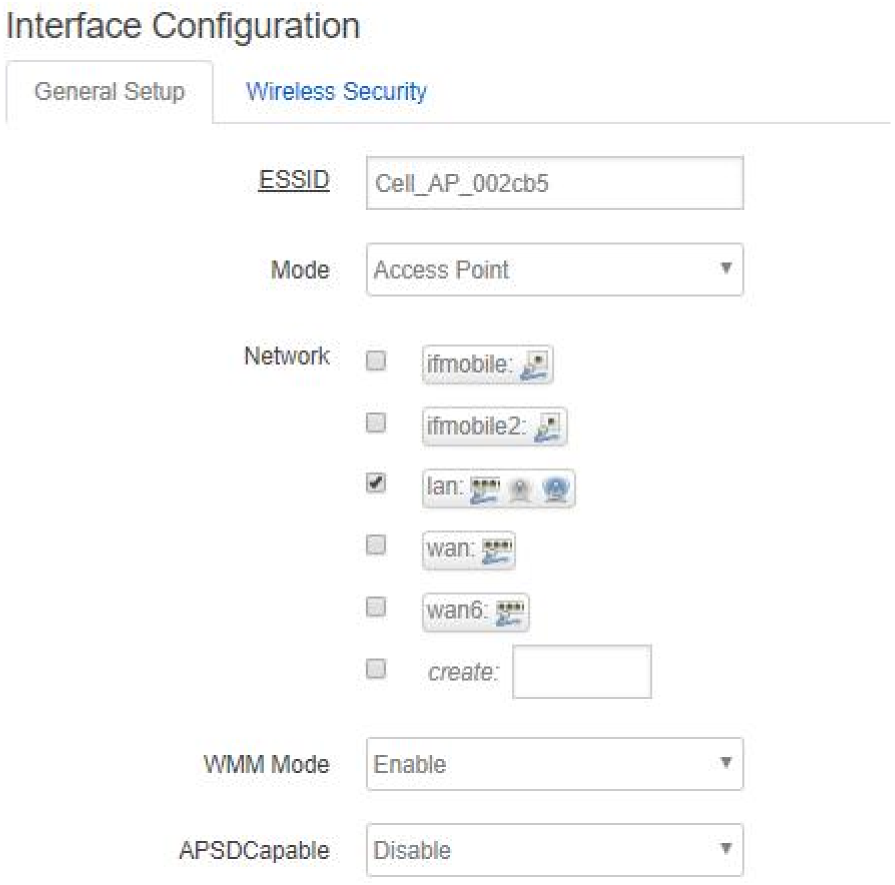
3.6.6.2 WiFi Advanced Configuration



Country Code	US
Support Channel	CH1~14
BG Protection Mode	auto
Beacon Interval	100
Data Beacon Rate	1
Fragment Threshold	2346
RTS Threshold	2347
TX Power	100
Short Preamble	Enable
Short Slot	Enable
Tx Burst	Enable
Pkt_Aggregate	Enable
IEEE 802.11H Support	Enable

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

3.6.6.3 WiFi Interface Configuration



Interface Configuration

General Setup | Wireless Security

ESSID: Cell_AP_002cb5

Mode: Access Point

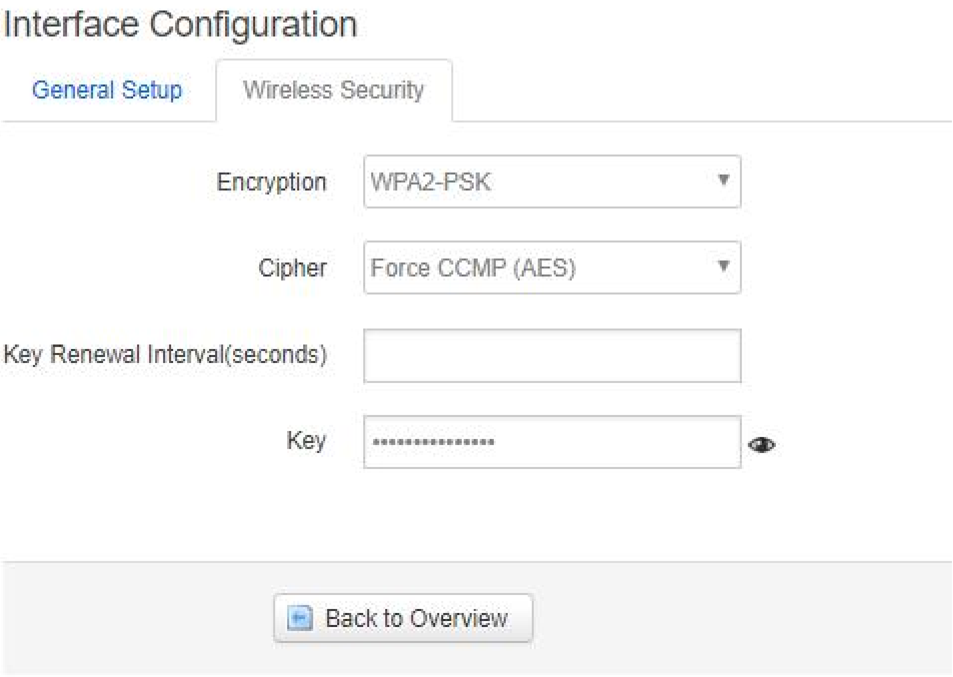
Network:
- □ ifmobile:
- □ ifmobile2:
- ☑ lan:
- □ wan:
- □ wan6:
- □ *create:*

WMM Mode: Enable

APSDCapable: Disable

- **ESSID**: Extended Service Set Identifier. It is the broadcast name.
- **Mode**: Supported options are *Access Point* and *Client*

- **Network**: Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
- **WMM Mode**



Interface Configuration

General Setup | Wireless Security

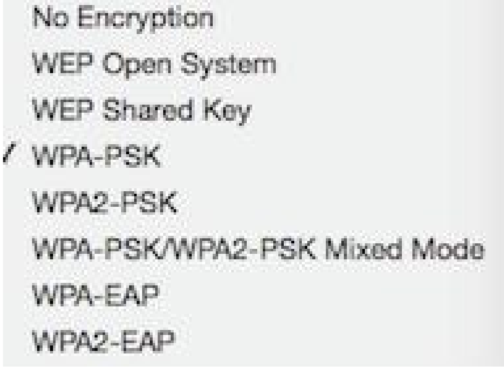
Encryption: WPA2-PSK

Cipher: Force CCMP (AES)

Key Renewal Interval(seconds):

Key: ••••••••••••••••

- **Encryption:**

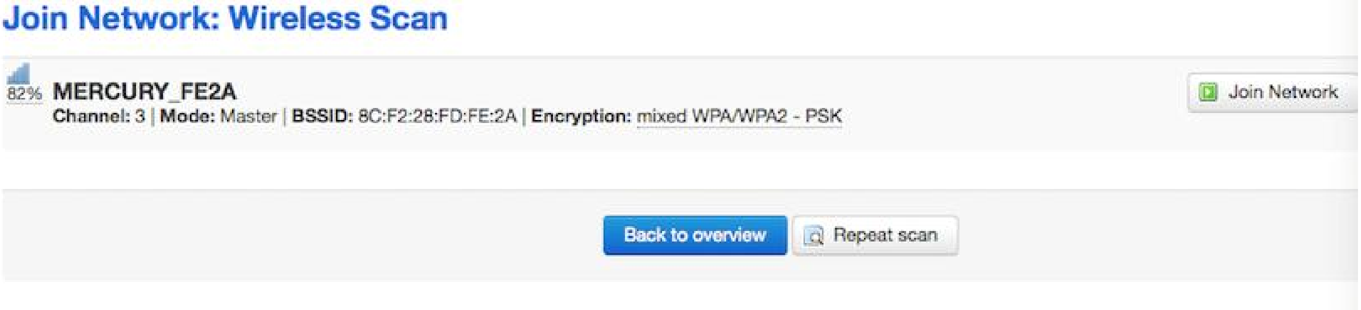


No Encryption
WEP Open System
WEP Shared Key
✓ WPA-PSK
WPA2-PSK
WPA-PSK/WPA2-PSK Mixed Mode
WPA-EAP
WPA2-EAP

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

3.6.6.4 WiFi AP client

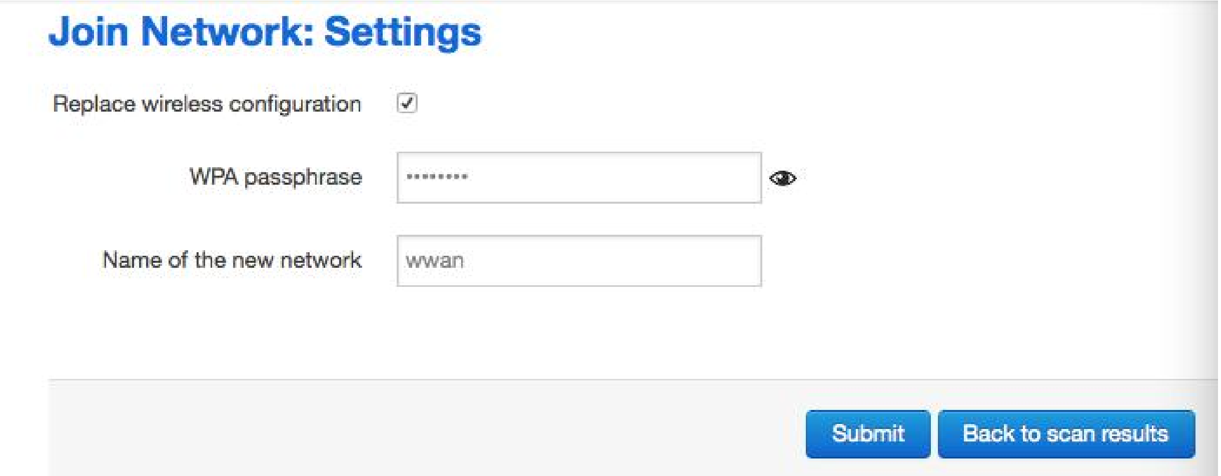
- **Steps 1)** Click the button “AP Client” on the wireless overview page, then the system will start to scan all WiFi signals.



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” accordingly. If it is not, click “Repeat Scan” until you find the WiFi that you want to join.



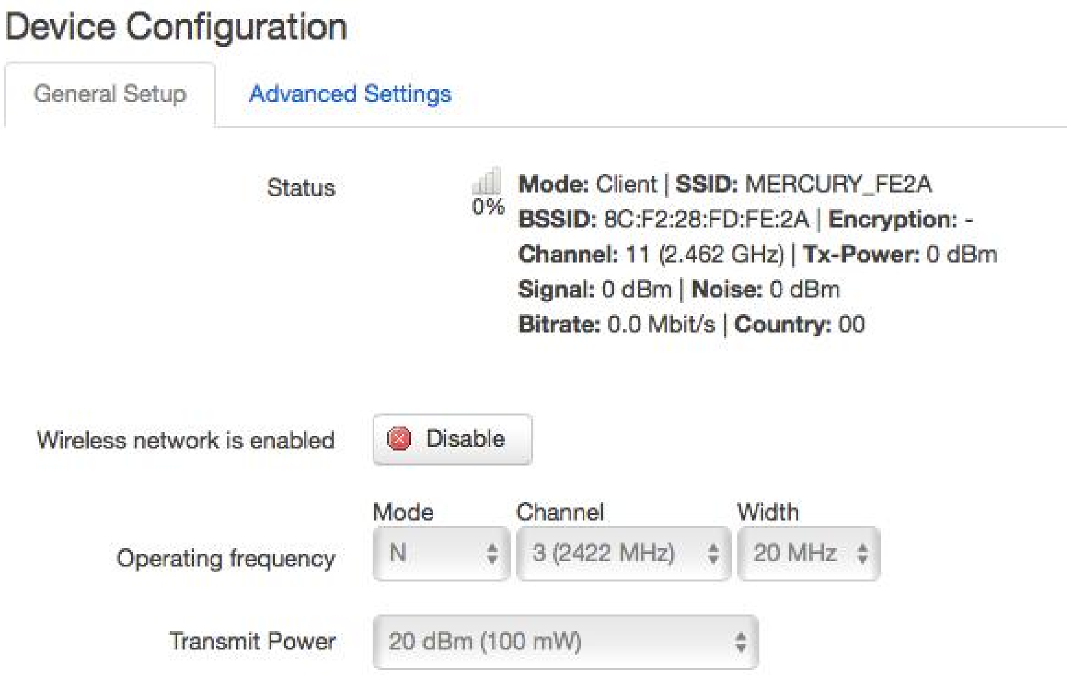
Join Network: Settings

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. Don’t change the operating frequency. Make sure the ESSID and BSSID are for the Wi-Fi you want to join.



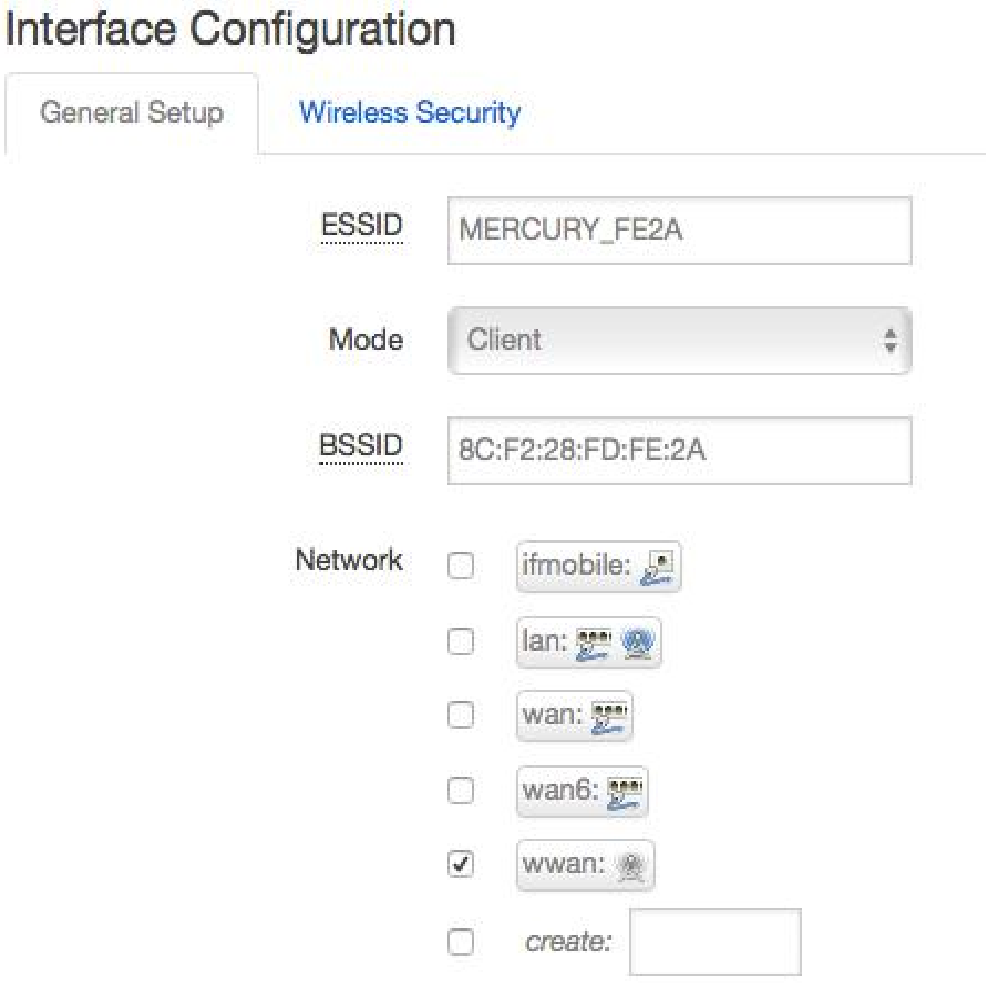
Device Configuration

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

Wireless network is enabled — Disable

Operating frequency — Mode: N; Channel: 3 (2422 MHz); Width: 20 MHz

Transmit Power — 20 dBm (100 mW)



Interface Configuration

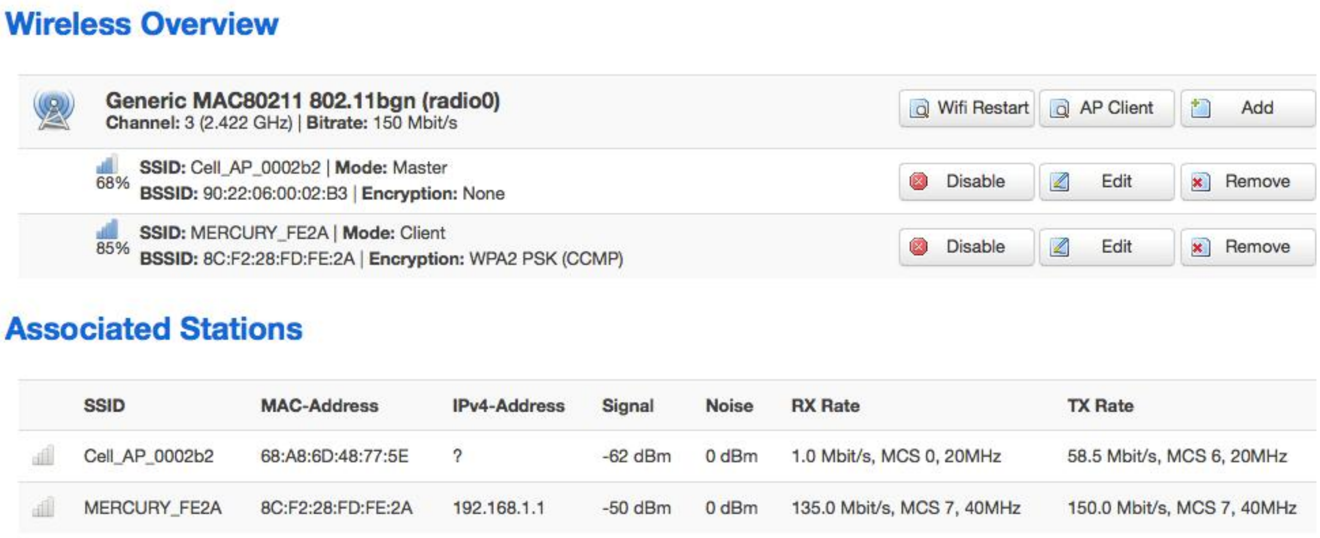
ESSID: MERCURY_FE2A

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

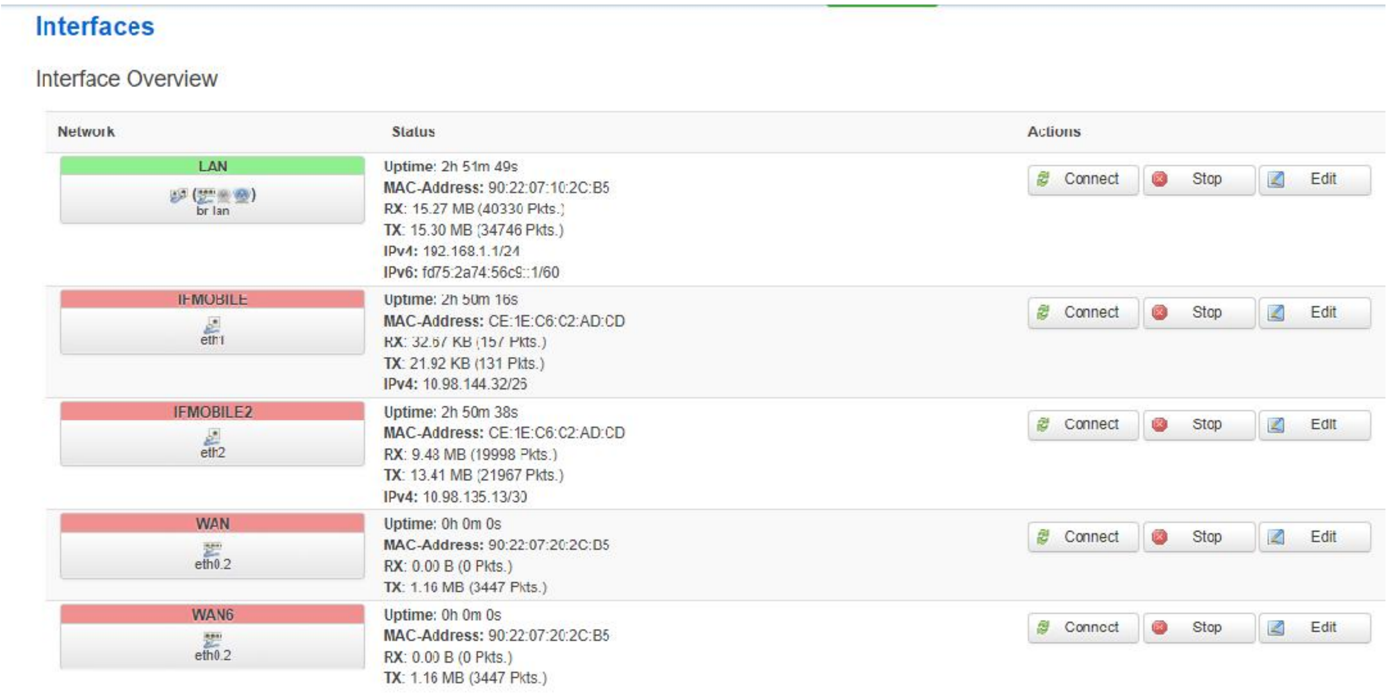
85% **SSID:** MERCURY_FE2A | **Mode:** Client
BSSID: 8C:F2:28:FD:FE:2A | **Encryption:** WPA2 PSK (CCMP)

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.



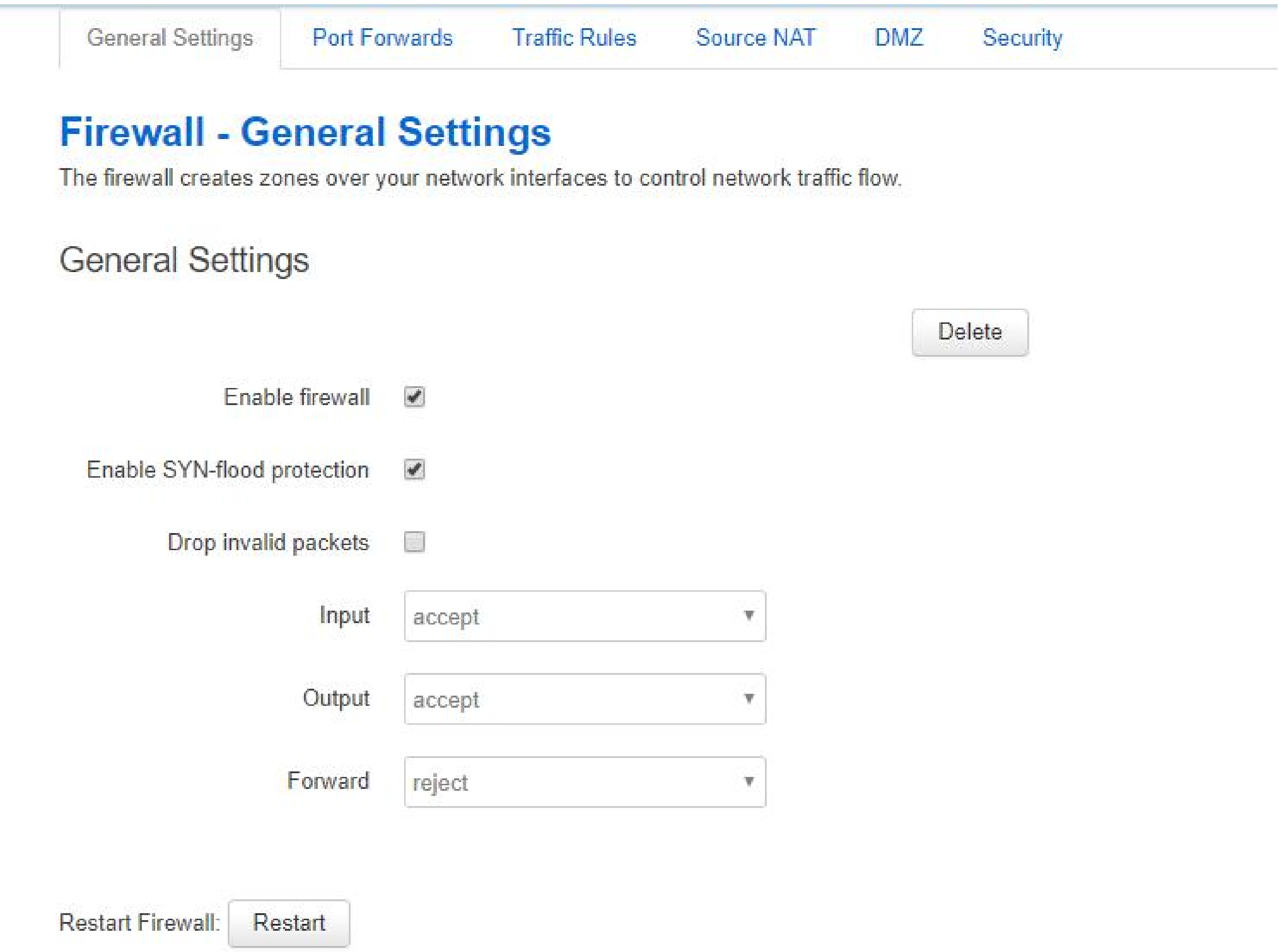
Interfaces

Interface Overview

Network	Status	Actions
LAN br lan	**Uptime:** 2h 51m 49s **MAC-Address:** 90:22:07:10:2C:B5 **RX:** 15.27 MB (40330 Pkts.) **TX:** 15.30 MB (34746 Pkts.) **IPv4:** 192.168.1.1/24 **IPv6:** fd75:2a74:56c9::1/60	Connect Stop Edit
IFMOBILE eth1	**Uptime:** 2h 50m 16s **MAC-Address:** CE:1E:C6:C2:AD:CD **RX:** 32.67 KB (157 Pkts.) **TX:** 21.92 KB (131 Pkts.) **IPv4:** 10.98.144.32/26	Connect Stop Edit
IFMOBILE2 eth2	**Uptime:** 2h 50m 38s **MAC-Address:** CE:1E:C6:C2:AD:CD **RX:** 9.48 MB (19998 Pkts.) **TX:** 13.41 MB (21967 Pkts.) **IPv4:** 10.98.135.13/30	Connect Stop Edit
WAN eth0.2	**Uptime:** 0h 0m 0s **MAC-Address:** 90:22:07:20:2C:B5 **RX:** 0.00 B (0 Pkts.) **TX:** 1.16 MB (3447 Pkts.)	Connect Stop Edit
WAN6 eth0.2	**Uptime:** 0h 0m 0s **MAC-Address:** 90:22:07:20:2C:B5 **RX:** 0.00 B (0 Pkts.) **TX:** 1.16 MB (3447 Pkts.)	Connect Stop Edit

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

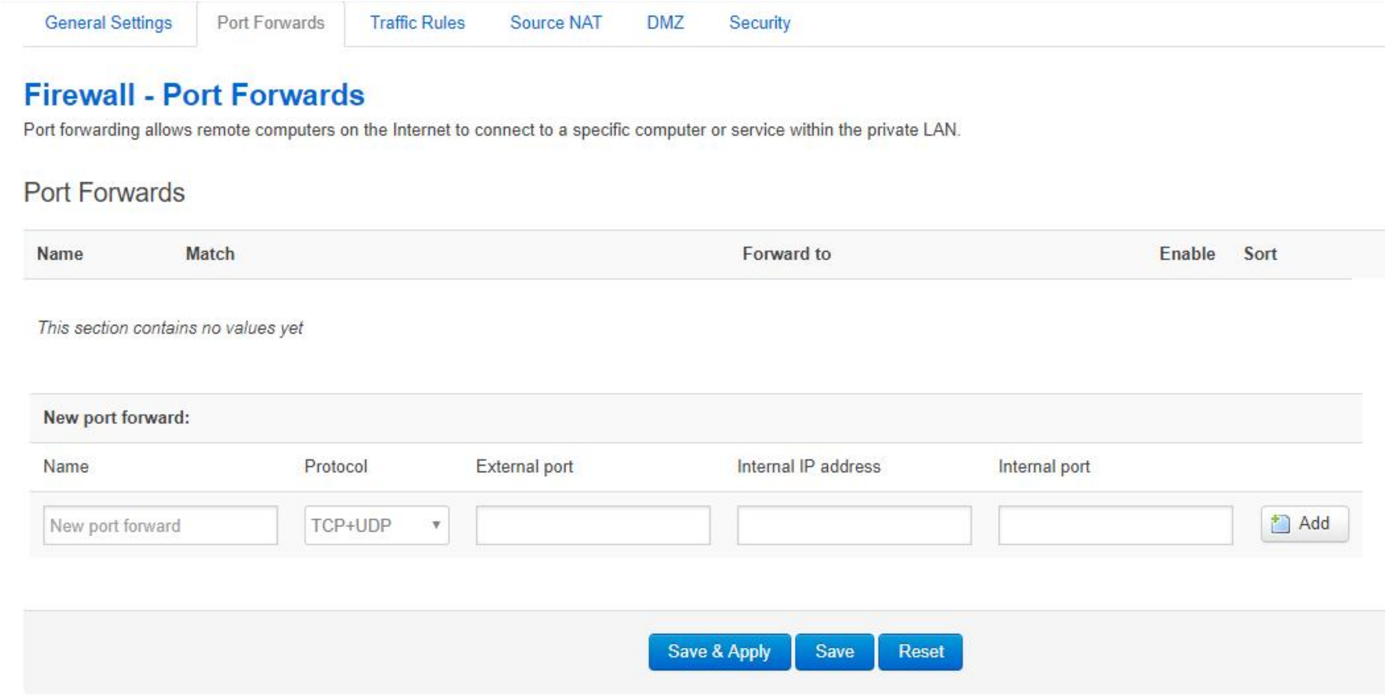
Output: accept

Forward: reject

Restart Firewall:

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

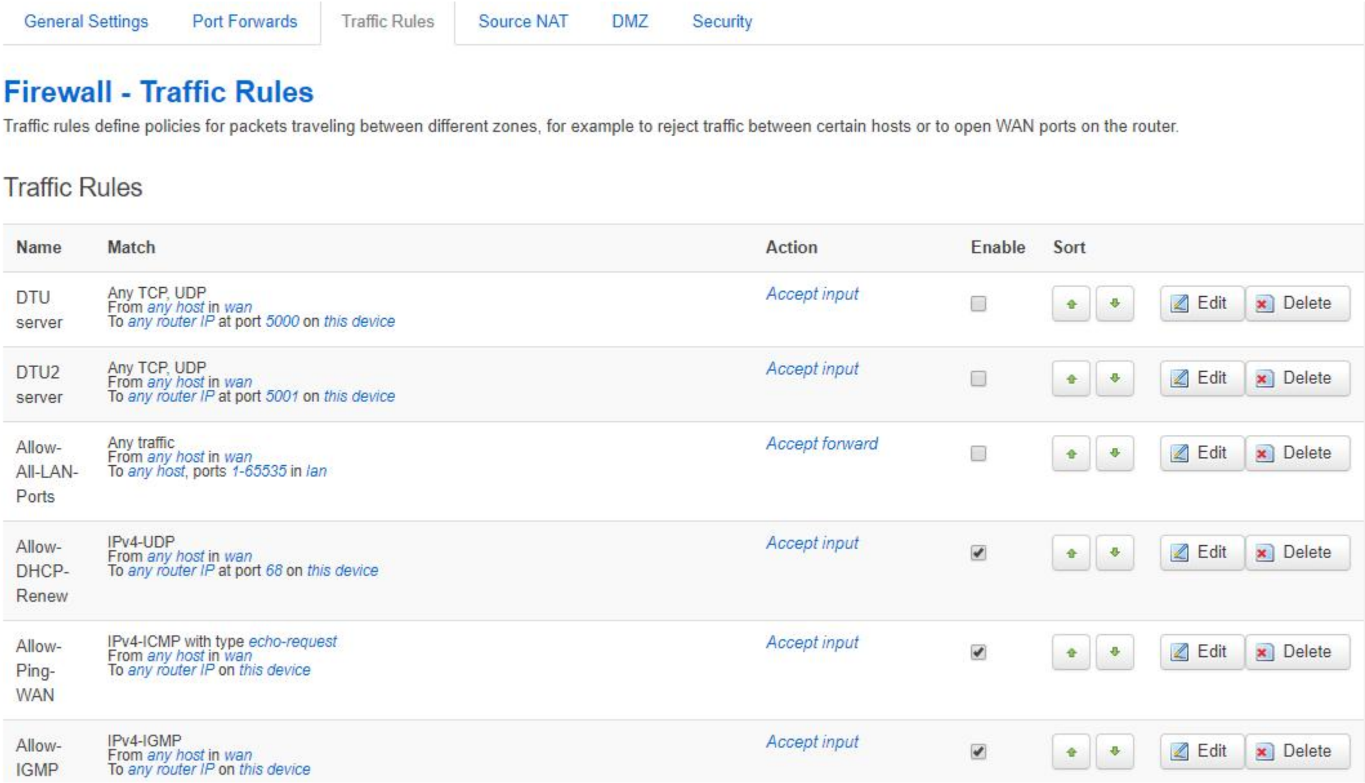
- **Name**: Port Forward instance name.
- **Protocol**: TCP+UDP, UDP and TCP can be chosen.
- **External zone**: The recommended option is ‘wan’.
- **External port**: Match incoming traffic directed at the given destination port on this host.
- **Internal zone**: The recommended zone is ‘lan’.
- **Internal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

3.6.8.3 Traffic rules

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

The traffic rules overview page contains the following functionalities:

Traffic rules list:



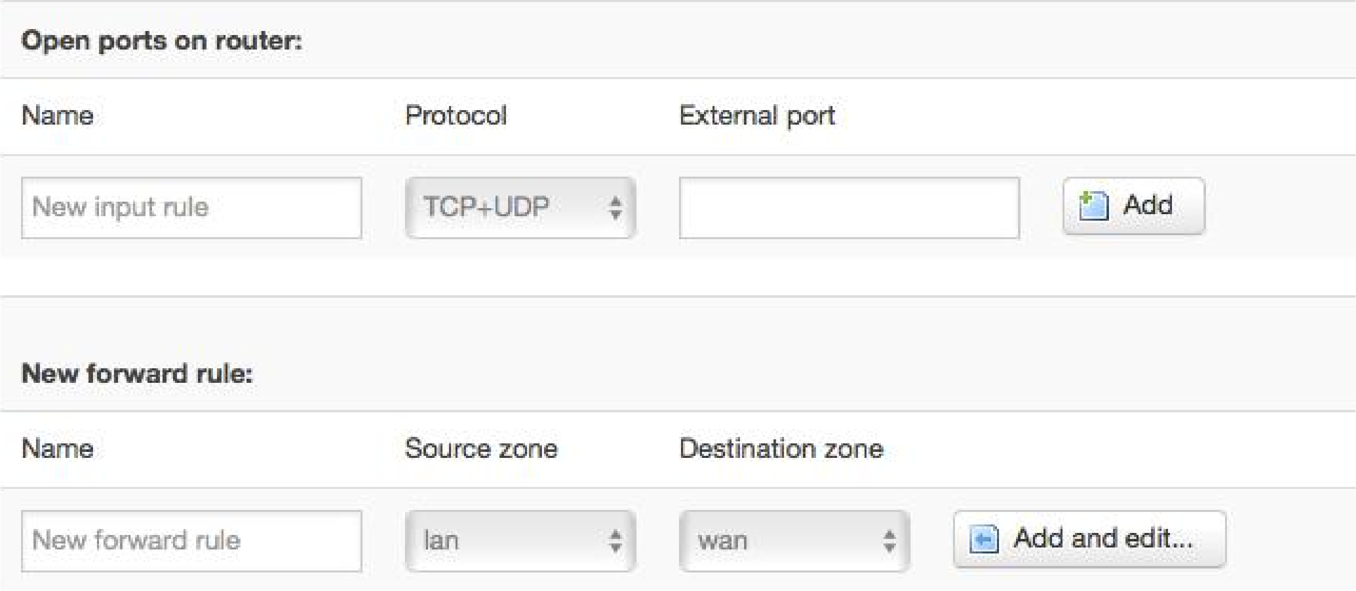
Firewall - Traffic Rules

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

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



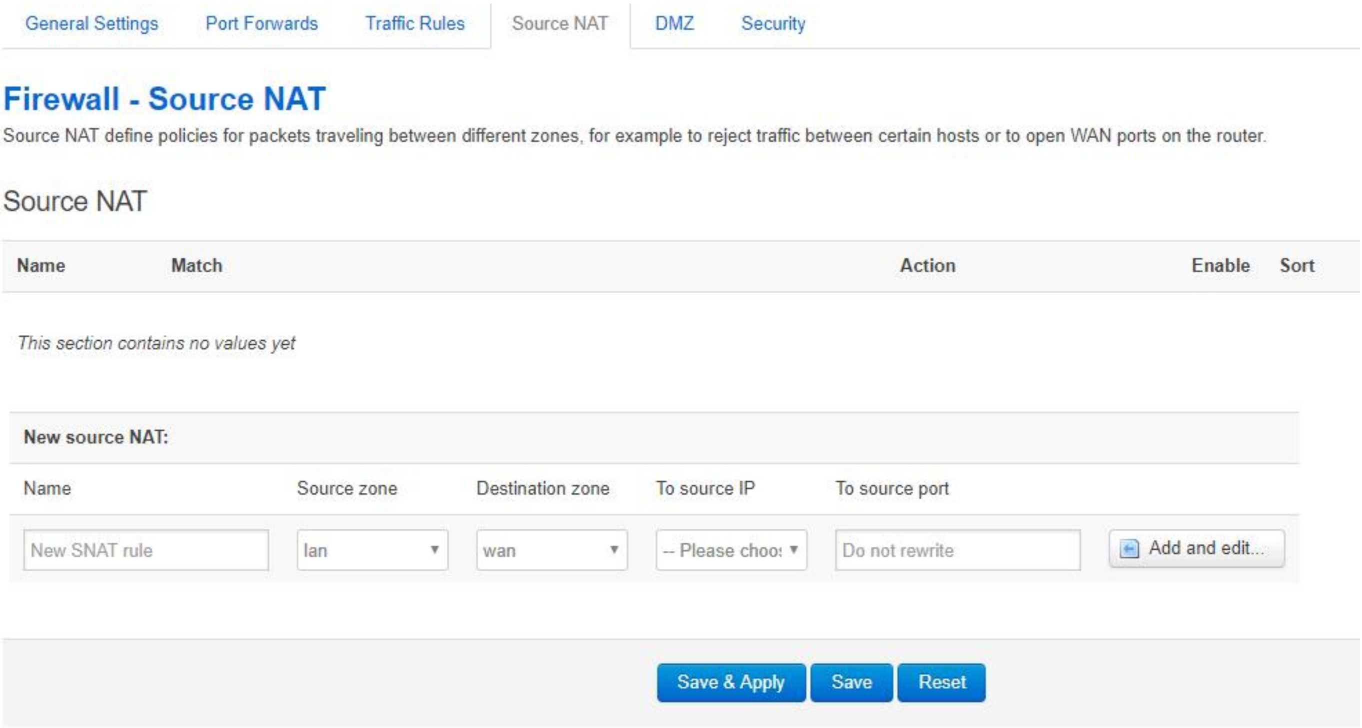
Open ports on router:

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:



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

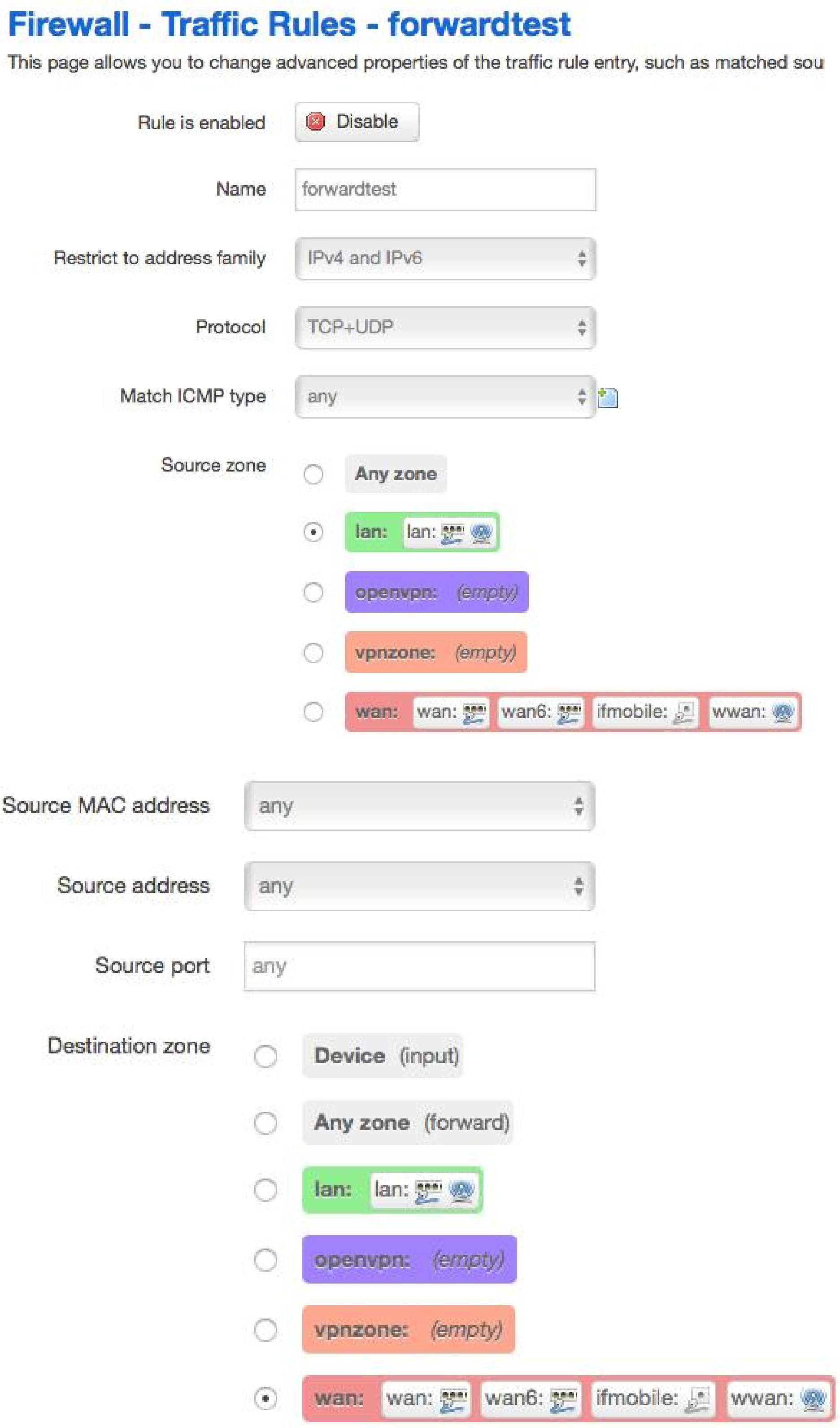
Name	Match	Action	Enable	Sort

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 choo:	Do not rewrite	Add and edit...

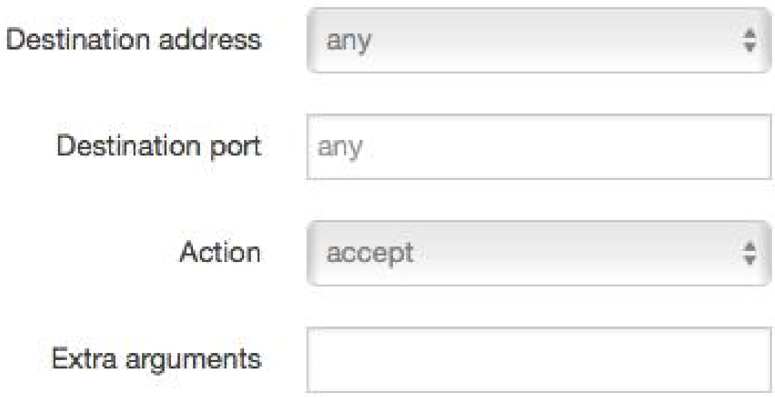
Traffic rule configuration page: This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.



Firewall - Traffic Rules - forwardtest

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

Rule is enabled	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

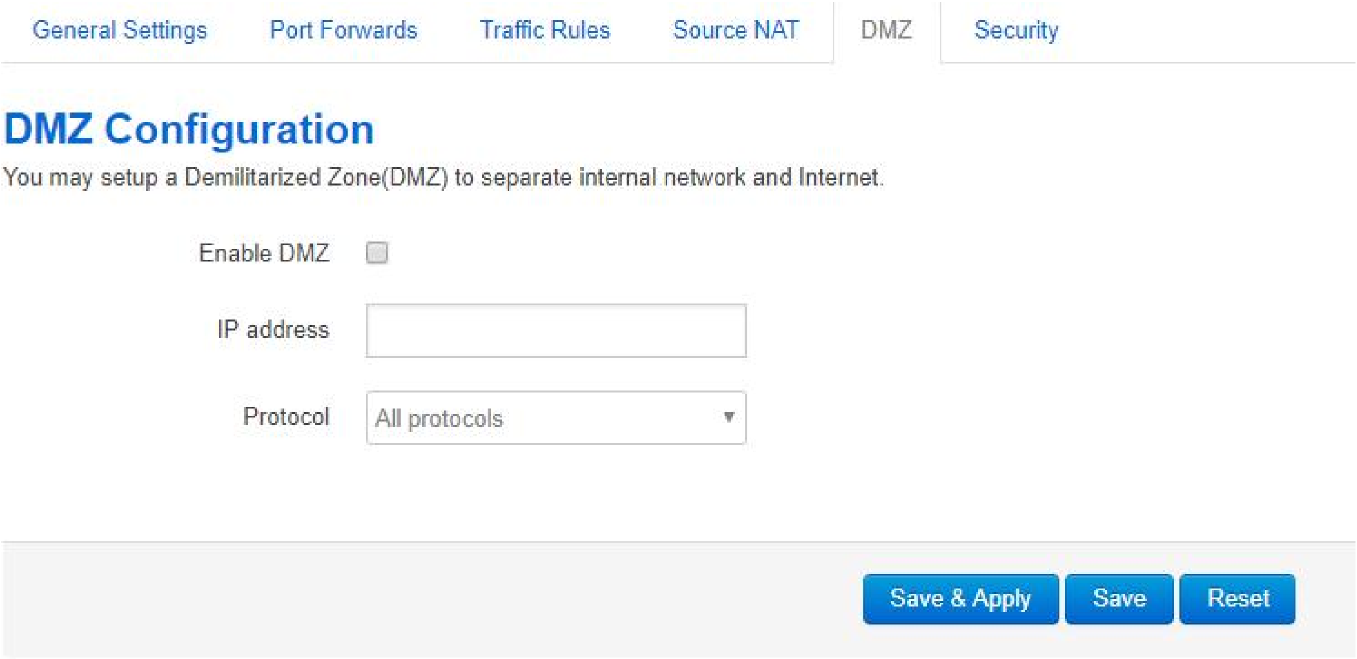
Destination port: any

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

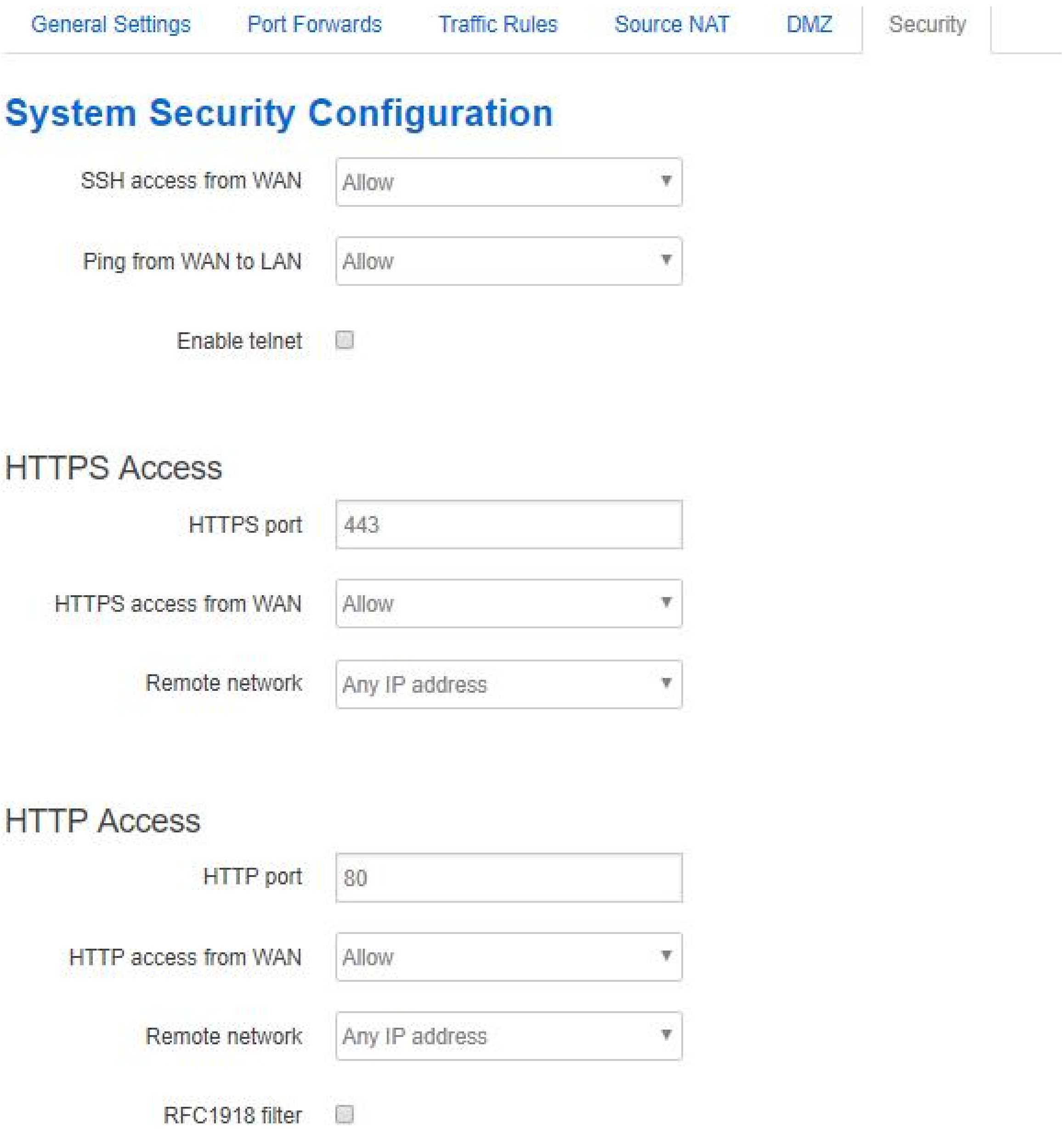
Protocol: All protocols

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 access from WAN: Allow

Ping from WAN to LAN: Allow

Enable telnet □

HTTPS Access

HTTPS port: 443

HTTPS access from WAN: Allow

Remote network: Any IP address

HTTP Access

HTTP port: 80

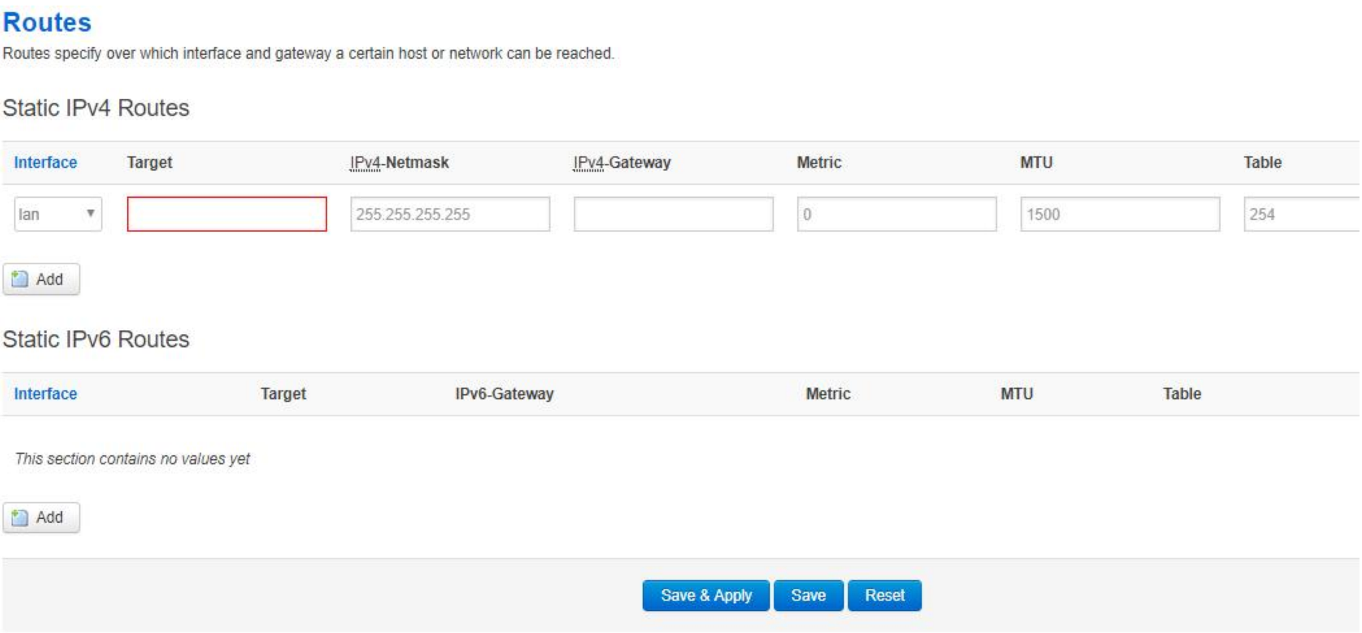
HTTP access from WAN: Allow

Remote network: Any IP address

RFC1918 filter □

- **SSH access from WAN**: Allow or deny users to access the router from remote side.
- **Ping from WAN to LAN**: Allow or deny ping from remote side to the internal LAN subnet.
- **HTTPS access from WAN**: Allow or deny access to the router web management page from the remote side.
- **Remote network**: Any IP Address, Single IP address, Subnet.
- **IP address**: Fill a remote IP address that can access the router's web management page.
- **Netmask**: 24 means net mask 255.255.255.0, 32 means 255.255.255.255, the value is from 1 to 32.

3.6.9 Static Routes



Routes

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

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	Table
lan ▾		255.255.255.255		0	1500	254

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU	Table

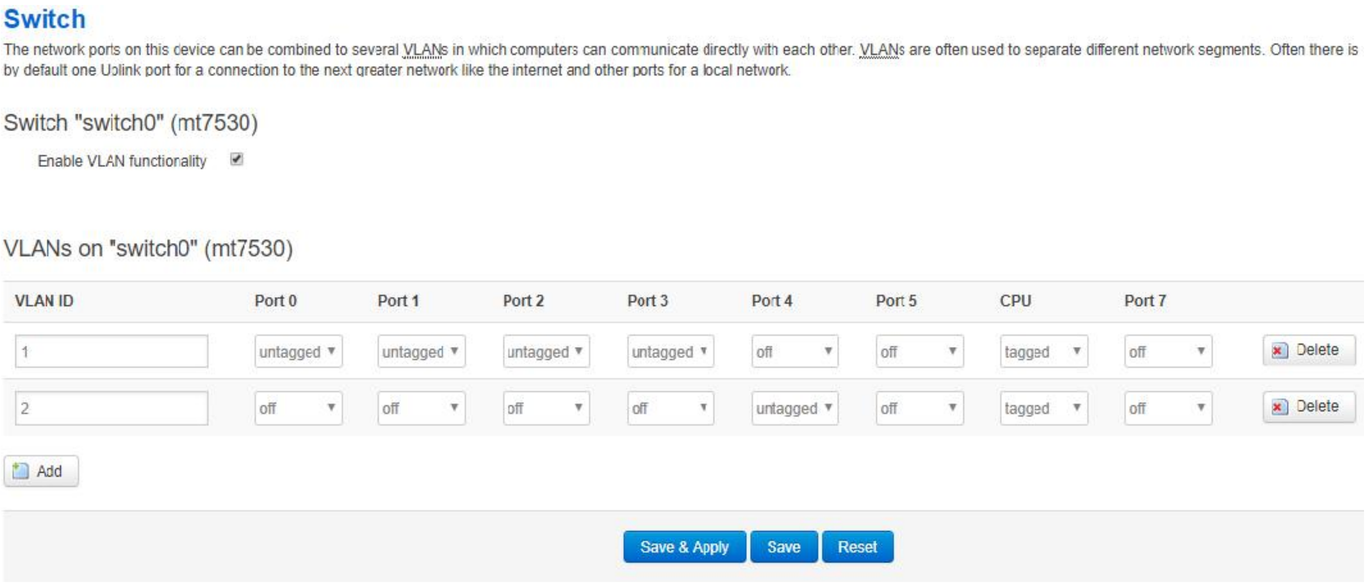
This section contains no values yet

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

  Notice:

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

3.6.10 Switch



Switch

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

Switch "switch0" (mt7530)

Enable VLAN functionality ☑

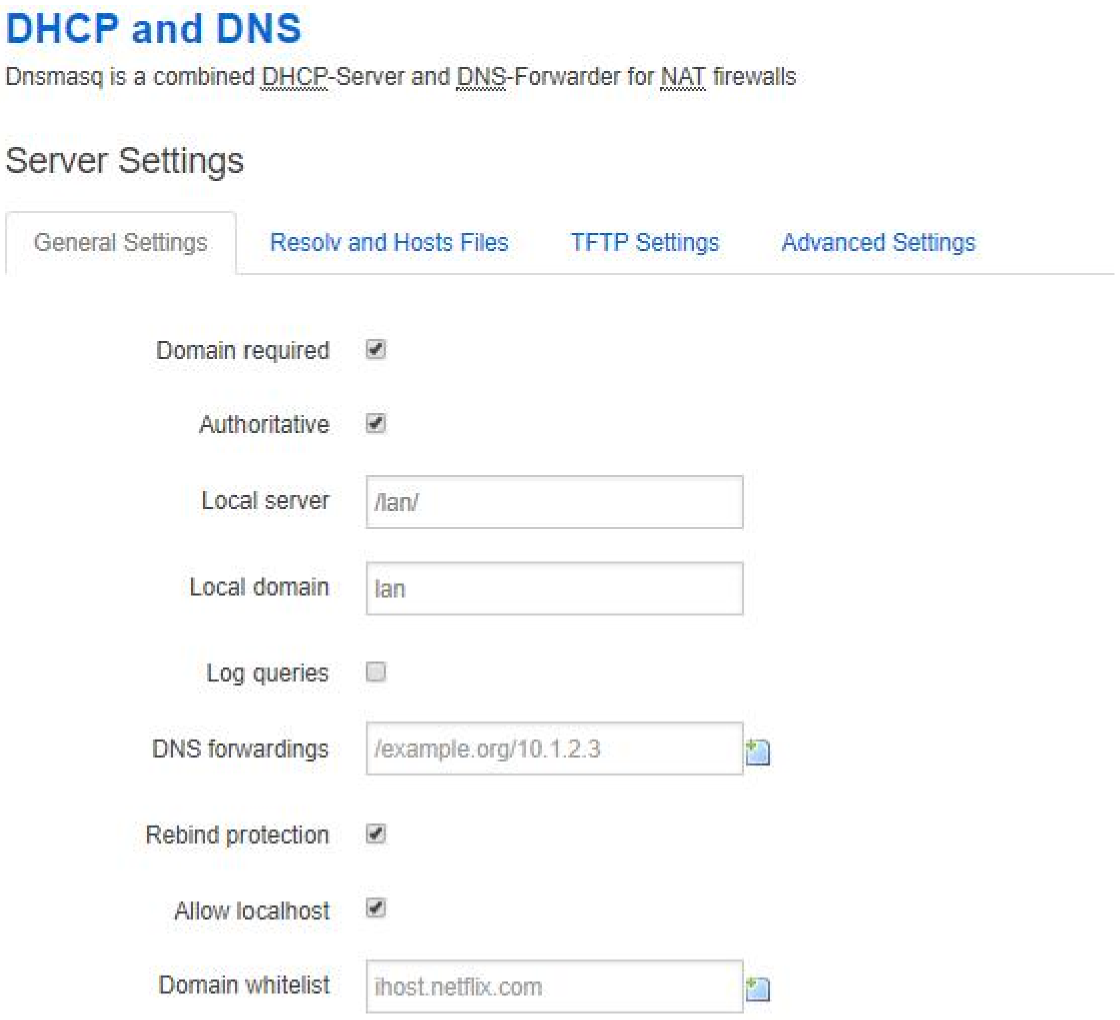
VLANs on "switch0" (mt7530)

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 □

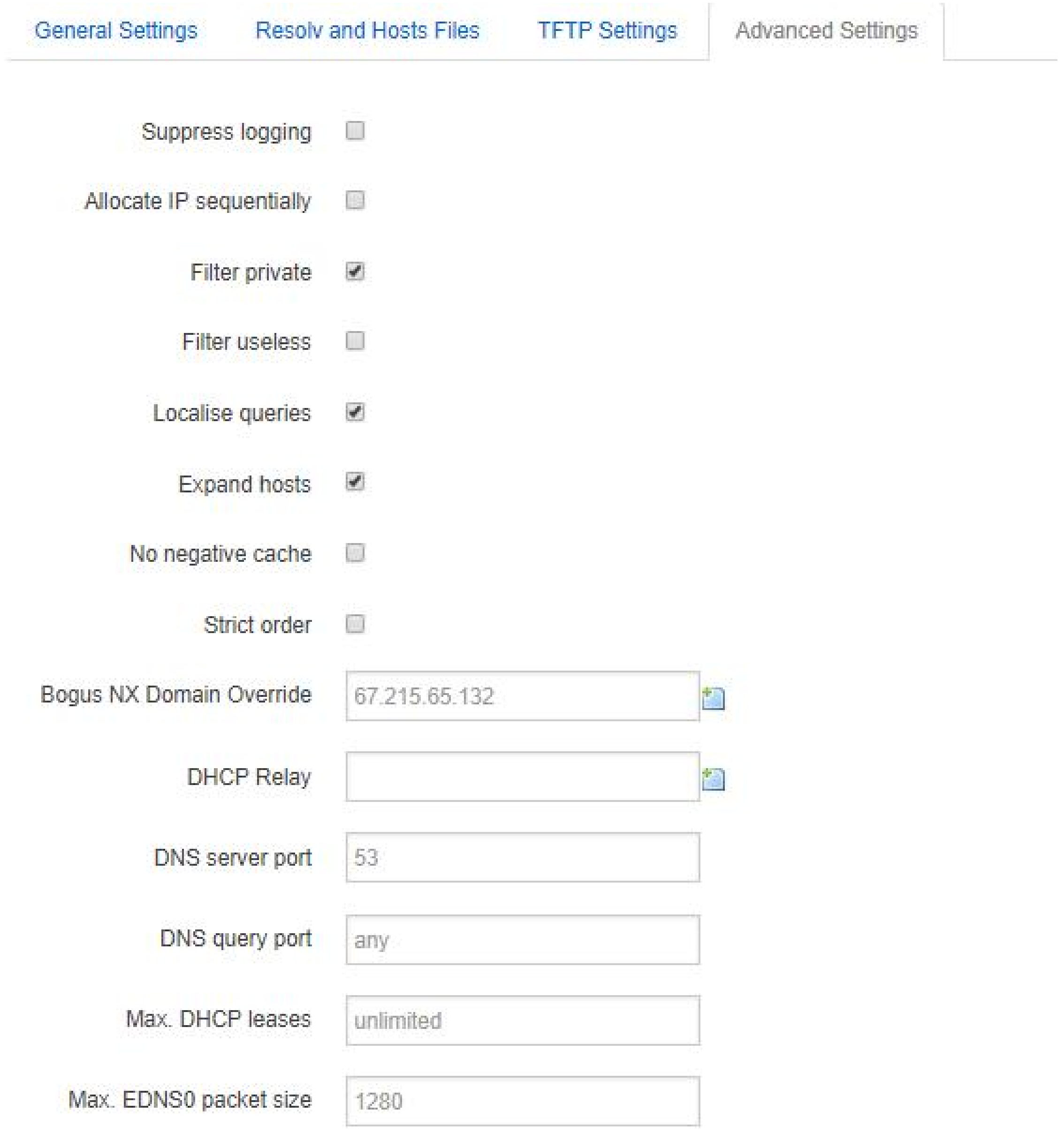
DNS forwardings /example.org/10.1.2.3

Rebind protection ☑

Allow localhost ☑

Domain whitelist ihost.netflix.com

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



General Settings | Resolv and Hosts Files | TFTP Settings | Advanced 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

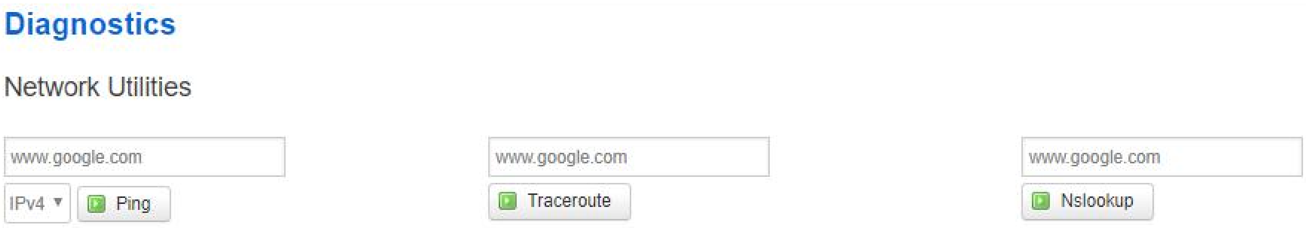
Max. DHCP leases unlimited

Max. EDNS0 packet size 1280

- **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.

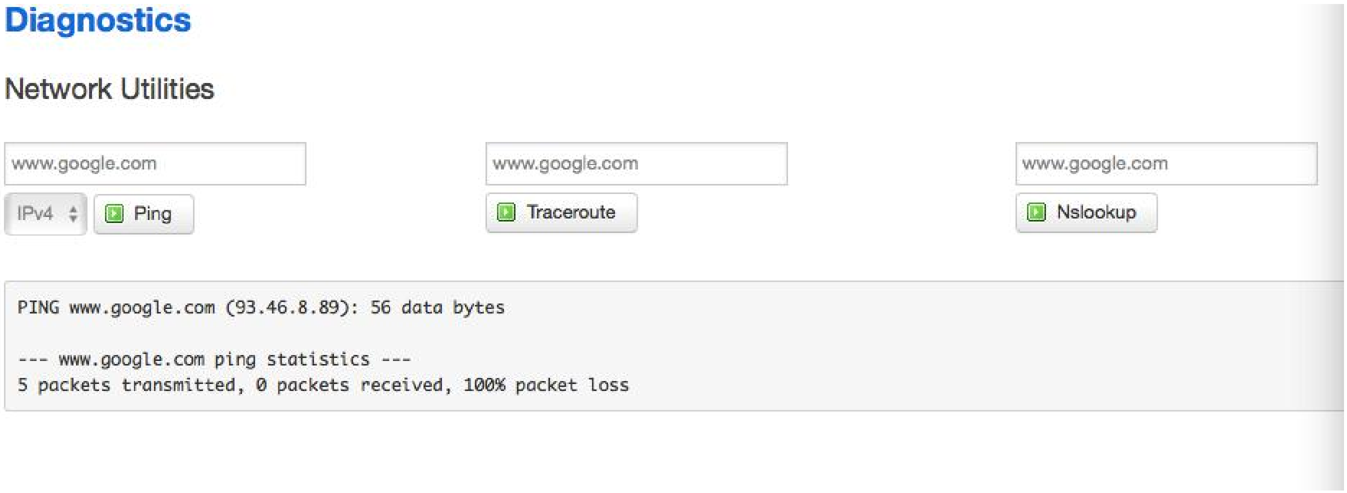
- **DNS query port**: Fixed source port for outbound DNS queries.
- **Max DHCP leases**: Maximum allowed number of active DHCP leases.
- **Max edns0 packet size**: Maximum allowed size of EDNS.0 UDP packets.
- **Max concurrent queries**: Maximum allowed number of concurrent DNS queries.

3.6.12 Diagnostics



- **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.

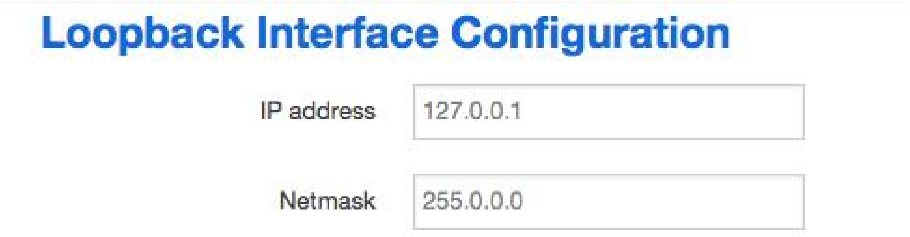
For example if you want to ping www.google.com, type the target domain name or IP address, then click the button “Ping”. Wait a couple of seconds, the result will be shown as below.



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

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

3.6.13 Loopback Interface



Loopback Interface Configuration

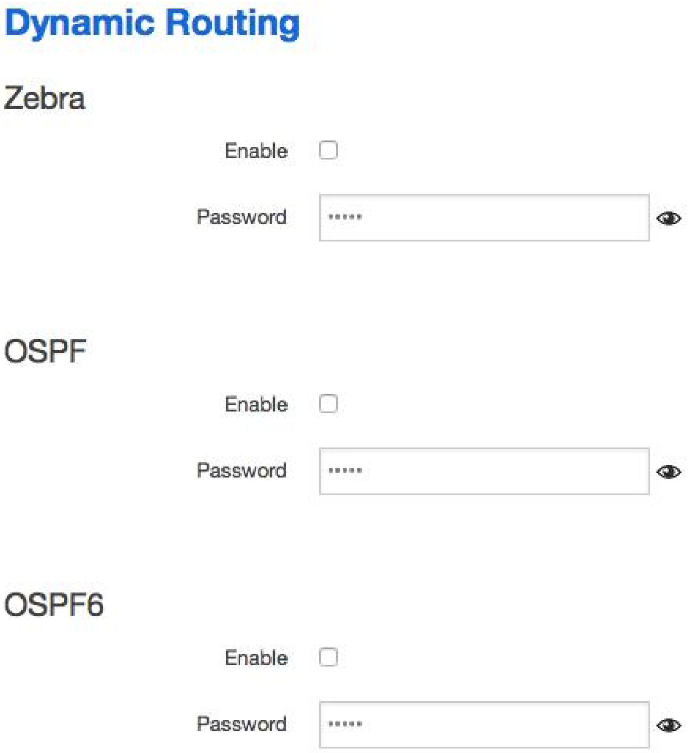
IP address: 127.0.0.1

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

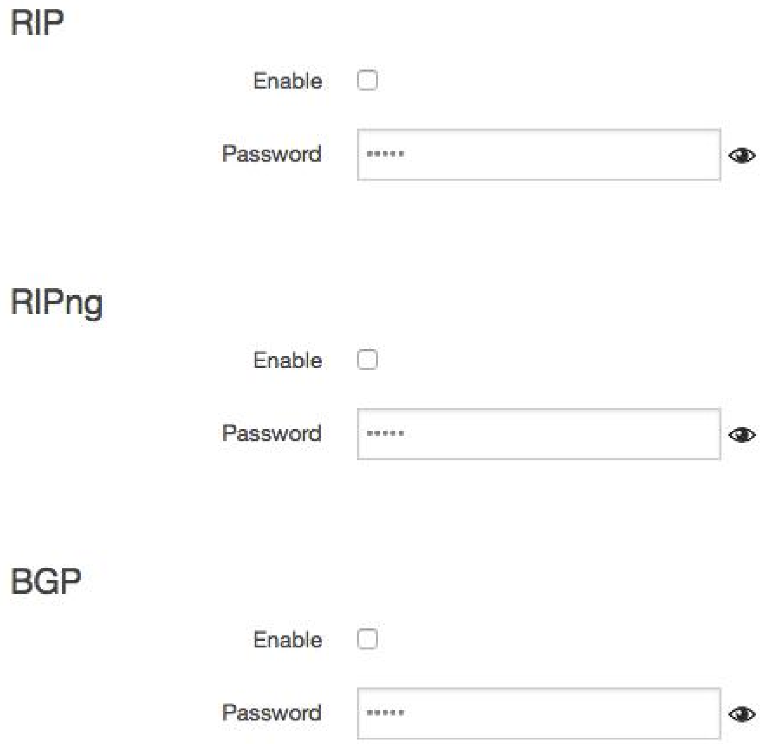
Enable ☐

Password •••••

OSPF6

Enable ☐

Password •••••



RIP

Enable □

Password •••••

RIPng

Enable □

Password •••••

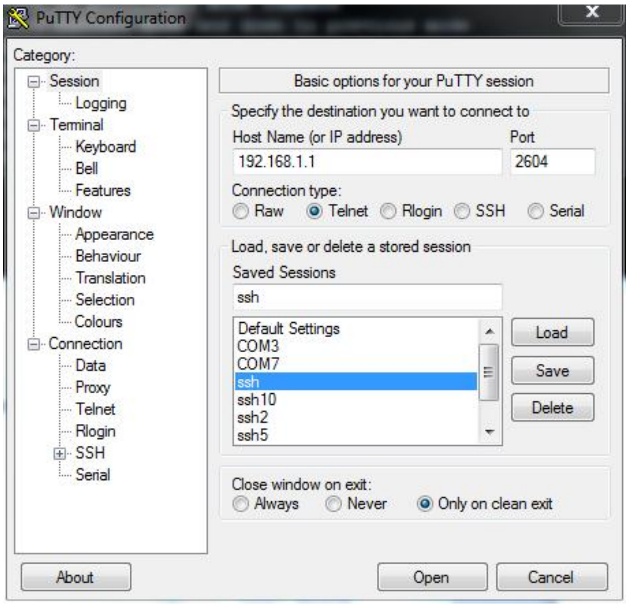
BGP

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:



PuTTY Configuration

Basic options for your PuTTY session

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

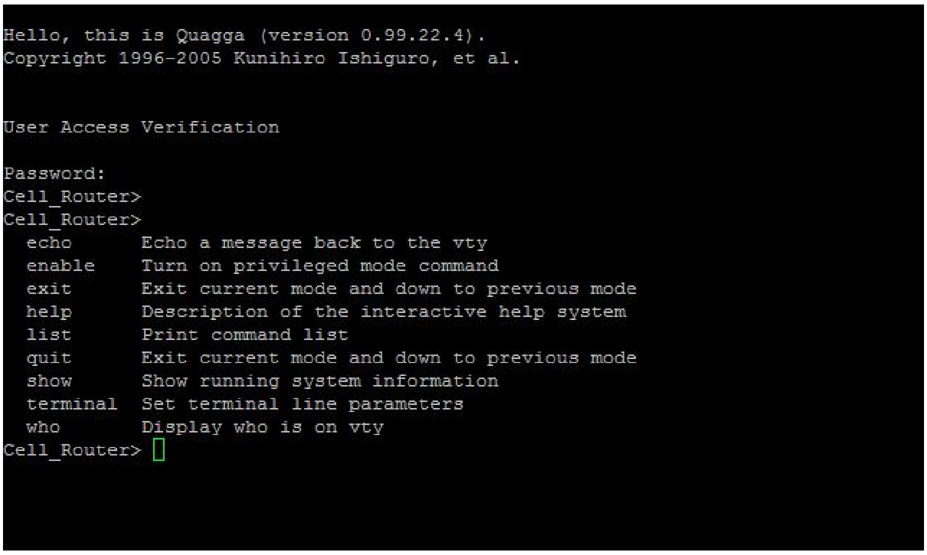
Load, save or delete a stored session

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.



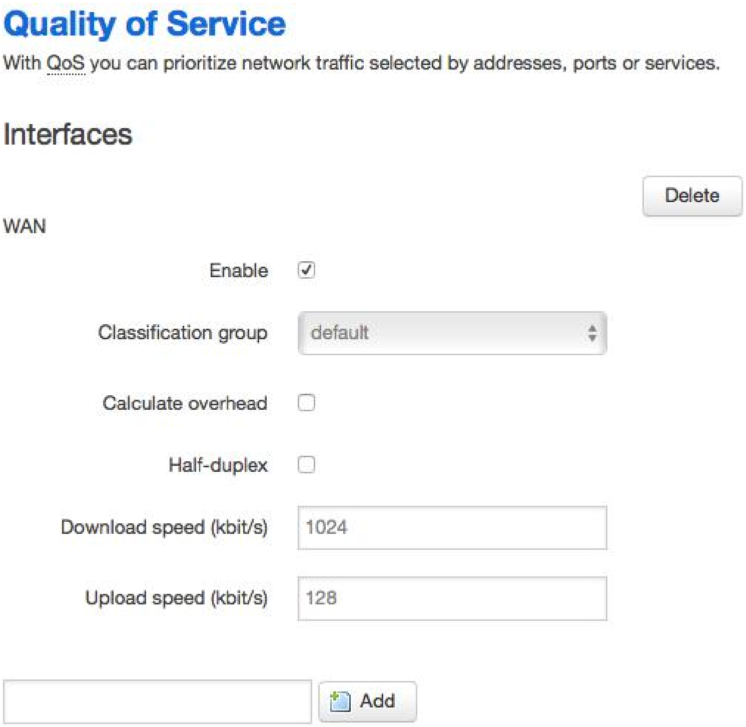
```
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


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

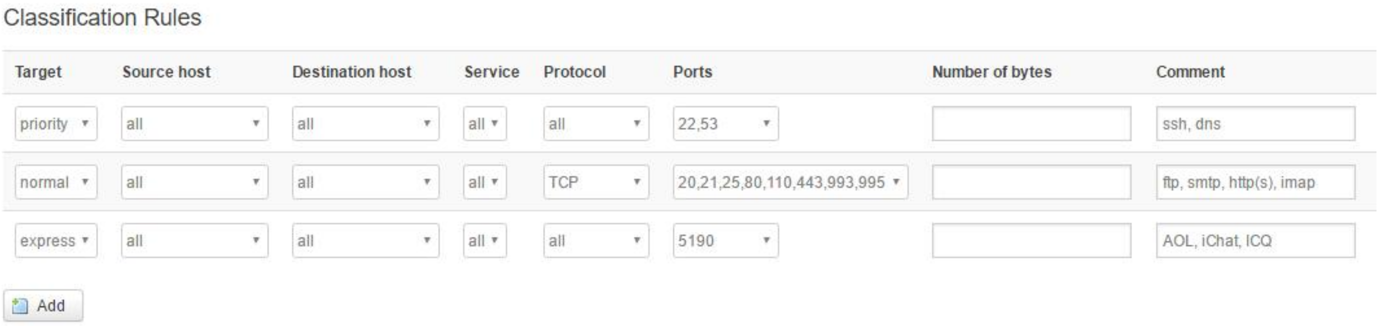
Calculate overhead □

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.