Industrial Grade 3G 4G 4GX Cellular Router

User Manual

CM685V-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

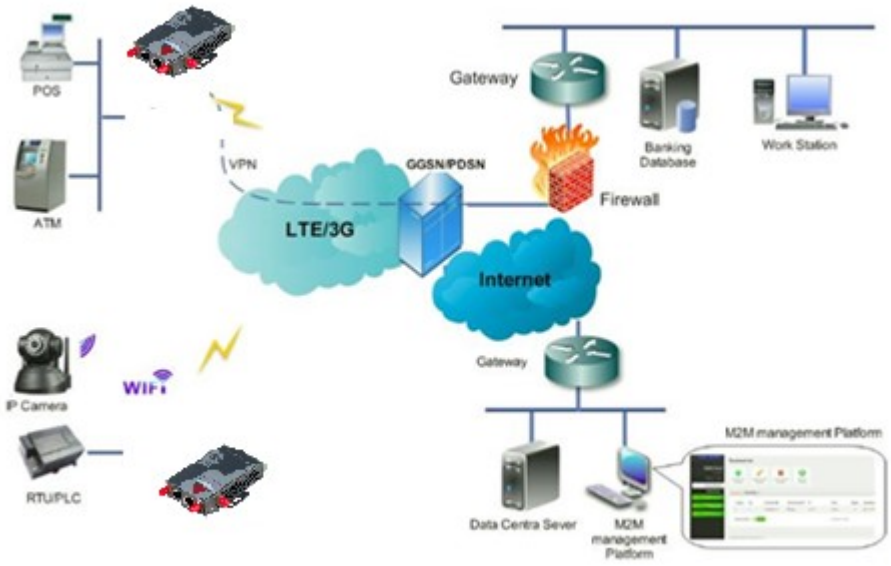
The Comset CM685V-6 is an industrial grade 3G/4G/4GX LTE WiFi Modem Router based on the latest OpenWrt platform. With download speeds of up to 300 Mbps and upload speeds of up to 50 Mbps, it is one of the few routers on the Australian market that supports band B28 (700MHz).

The Comset CM685V-6 is designed to suit Australian conditions. It supports the latest LTE Advanced Technology that performs fast and reliable data communication. It enables users to quickly create a secure and fast wireless network. It features a built-in WiFi N300 with speeds of up to 300 Mbps, one Ethernet WAN port for fixed internet connection and one Ethernet LAN port, as well as a GPIO with two digital output ports. Other features include VPN IPSEC, PPTP, L2TP and Open VPN to establish a secure connection over the 3G/4G network.

The durable and rugged design makes the CM685V-6 the router of choice for remote harsh environments. The compact design, easy integration and advanced built-in features make it suitable for a wide range of industrial M2M applications, including industrial automation, building automation, smart metering, security, surveillance, transportation, health, mining and environmental monitoring.

1.2 Typical Application Diagram

The Comset CM685V-6 3G/4G/4GX Router is suitable for a wide range of machine-to-machine applications (M2M). A good example is the connection of ATM machines and POS systems back to a server over a secure 4G connection using a secure VPN IPSEC tunnel.



1.3 Features

The CM685V-6 supports the following:

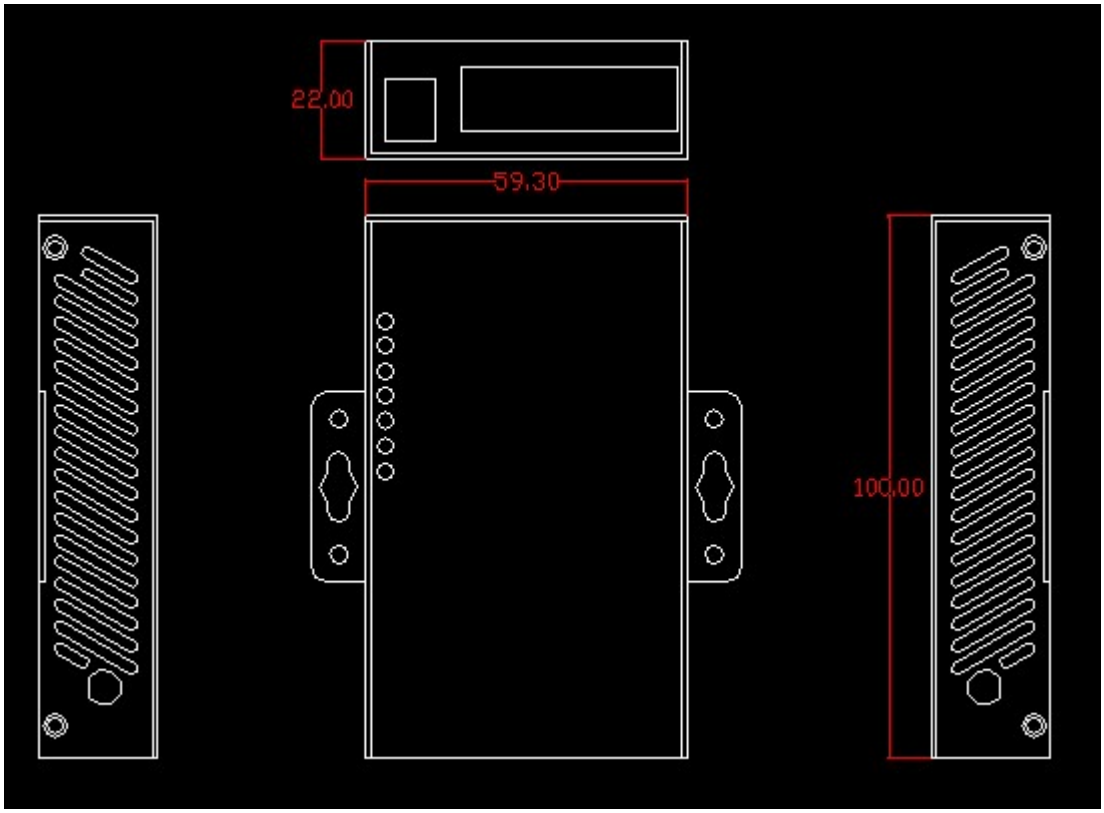
- LTE FDD B1/B3/B5/B7/B8/B20/B28/B32 and LTE TDD B38/B40/B41 with 3G fallback to WCDMA B1/B3/B5/B8
- IEEE802.11b/g/n N300 Wi-Fi AP function, WDS bridging, WEP, WPA/WPA2 Personal/Enterprise, TKIP/AES, Authenticated encryption mode
- RS232 interface data transparent transmission and protocol conversion
- On-demand dialing, including time on/off-line, voice or SMS control on/off-line, data trigger online or link idle offline
- TCP/IP protocol stack, Telnet, HTTP, SNMP, PPP, PPPoE, network protocol
- VPN IPSEC, PPTP, L2TP and Open VPN
- Configuration via a user-friendly interface using a web browser

Chapter 2

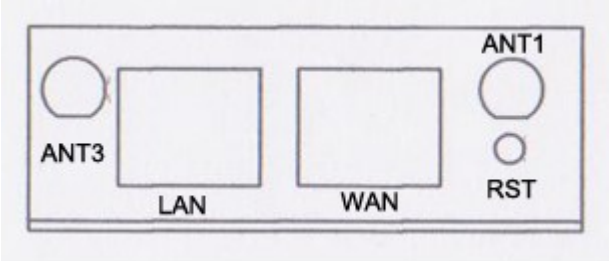
2 Hardware Installation

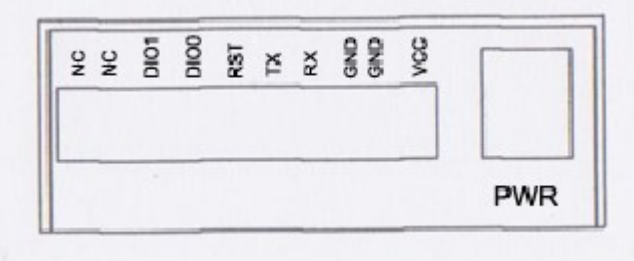
1. *Overall Dimensions*
2. *Accessories*
3. *Installation*

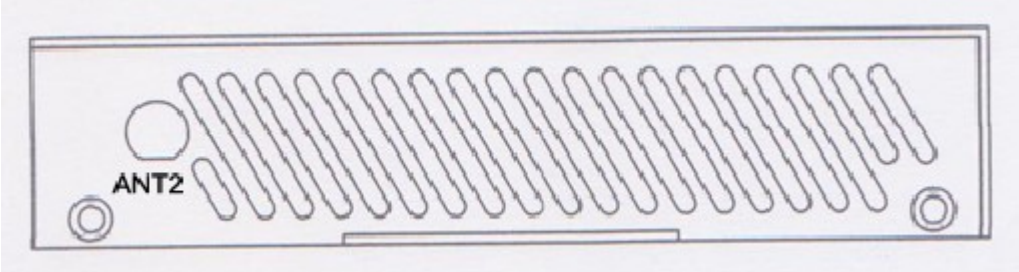
2.1 Overall Dimensions

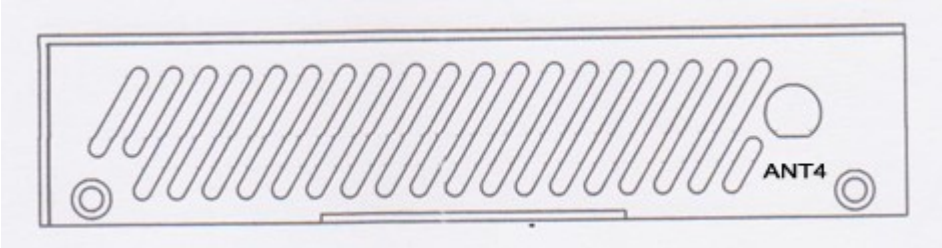


2.2 Ports









LAN: LAN RJ45 Ethernet port
WAN: WAN RJ45 Ethernet port
RST: SYS reset button
PWR: DC power socket. DC5~40V standard. (DC5~50V optional)
VCC: DC wire positive pole
GND: DC wire ground
GND: Serial ground
RX: Serial receive
TX: Serial transmit
RST: Reset
DIO0: Digital I/O port 0
DIO1: Digital I/O port 1
NC: Not connected
WPS: WPS button

Antenna Connections Table

Antenna Connector	Marks
Cell	for main cell antenna
Aux	for auxiliary cell antenna
WiFi 1	for WiFi-1 antenna
WiFi 2	For WiFi-2 antenna
GPS	for GPS antenna (optional)

2.3 Powering up the CM685V-6

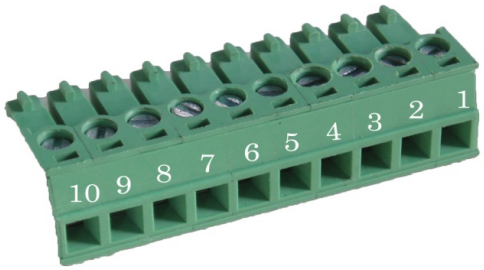
Please ensure the SIM card is inserted, and the antennas are connected before powering up the router.

2.4 SIM/UIM card

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

2.5 Terminal block

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



.

Attention:

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

PIN	Signal	Description	Note
1	VCC	+5-40V DC Input, +5~50V optional	Current: 12V/1A
2	GND	Ground	
3	TX	Transmit Data	
4	RX	Receive Data	
5	PGND	Ground	
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	DIO0	General Purpose I/O	
8	DIO1	General Purpose I/O	
9	NC	Not connected	

I/O Terminal on router	Serial port (RS485 or 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

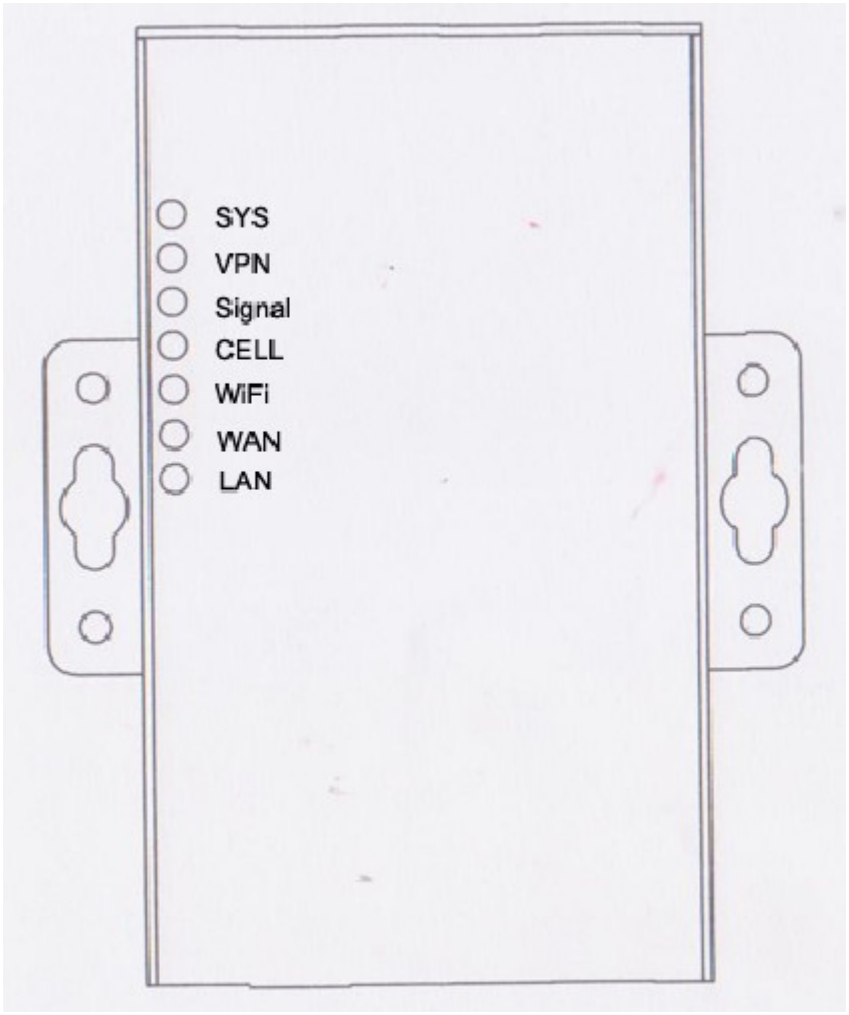
To ensure a safe operation, the cabinet where the router is installed should be grounded properly.

2.7 Power Supply

The CM685V-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
	Blink	System set-up normally
	Off or still on after 25 seconds	System set-up failure
LAN	Blink	Ethernet data transmission
	Off	No Ethernet connection
	On	Ethernet is connected
VPN	On	VPN tunnel set-up
	Off	VPN tunnel not set-up or VPN failure
CELL	On	Cell connection is 'UP' and now you have access to the Internet

WIFI	On	WiFi enabled
	Off	WiFi disabled
WAN	Blink	Ethernet data transmission
	Off	No Ethernet connection
	On	Ethernet is connected
Signal	Off	No signal, or signal checking is not ready
	Blinks once every 4s	Signal bar is 1
	Blinks once every 3s	Signal bar is 2
	Blinks once every 2s	Signal bar is 3
	Blinks once every 1s	Signal bar is 4
	Blinks twice every 1s	Signal bar is 5

Chapter 3

3 Software configuration

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

3.1 Overview

The CM685V-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

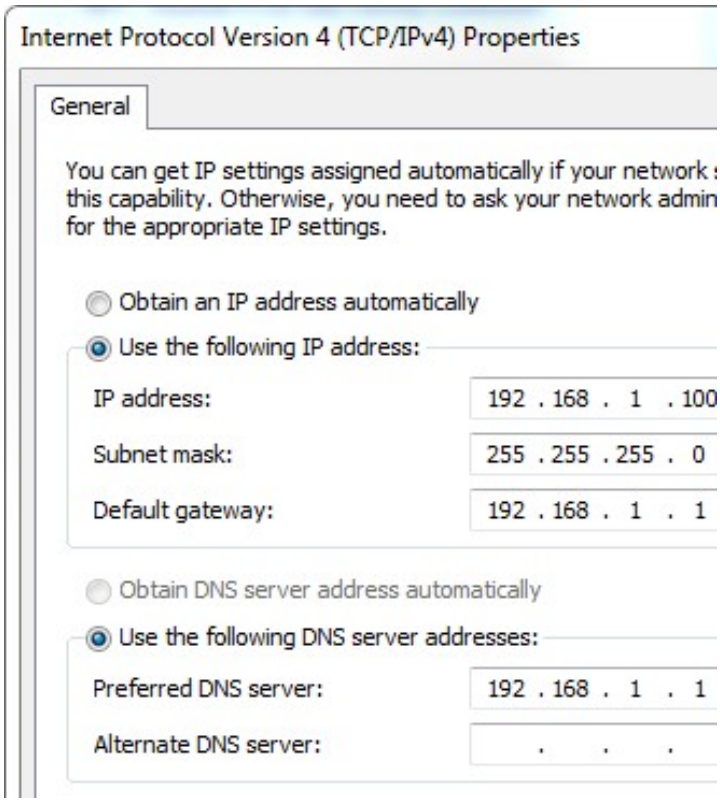
The router's default parameters are:

Default IP: 192.168.1.1
Subnet mask: 255.255.255.0

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

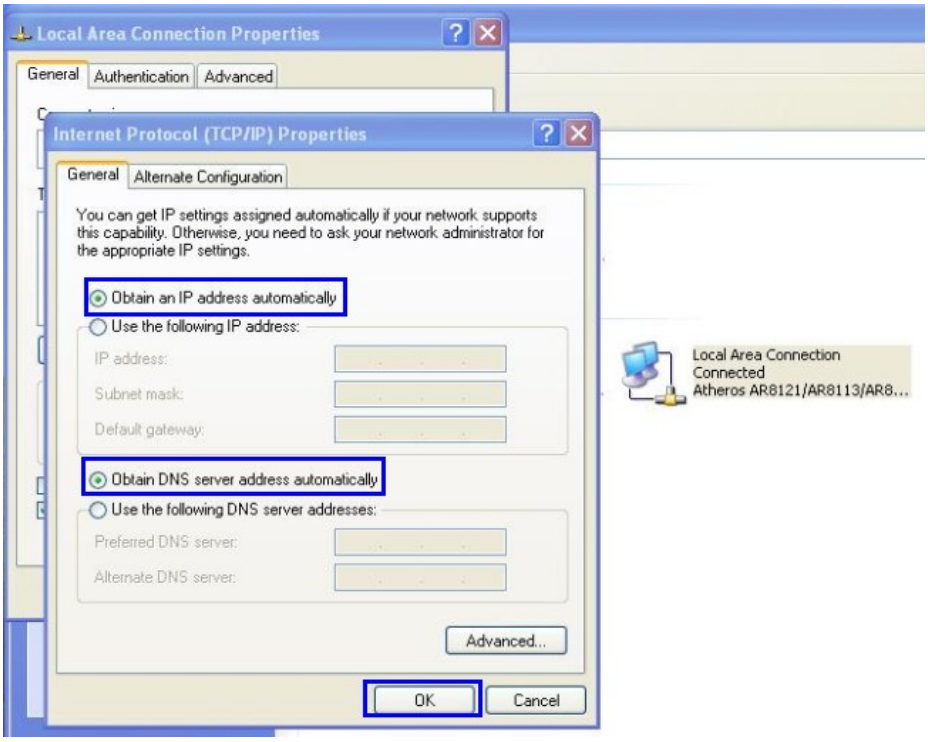
1) Manual settings

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.



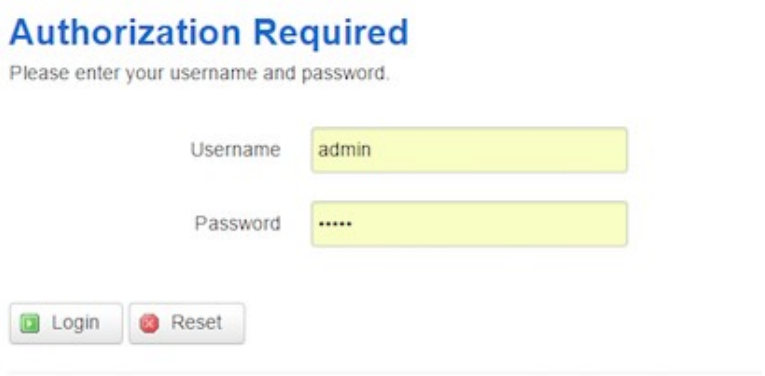
2) DHCP settings

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



3.2.2 Log into the router

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

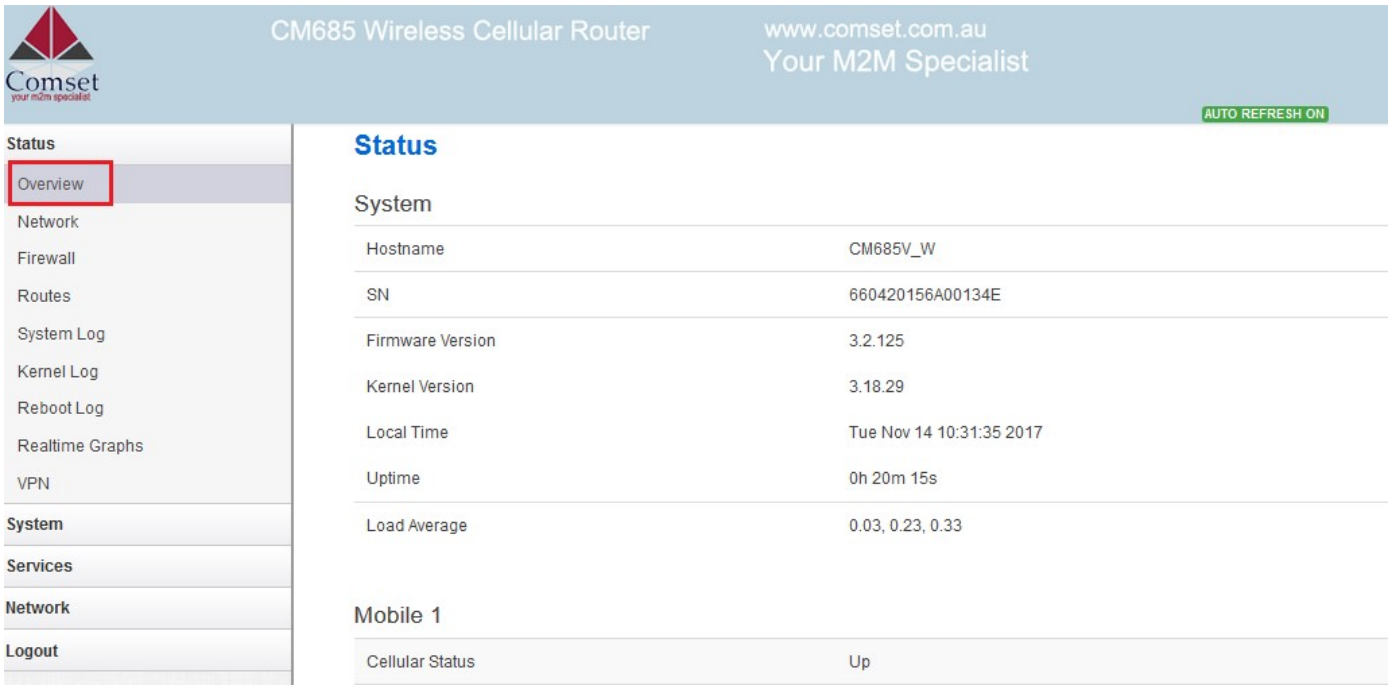


To configure the router, you can skip the following section “Router status” and go straight to System> Setup wizard which is covered in section 3.4.1

3.3 Router status

3.3.1 Status overview

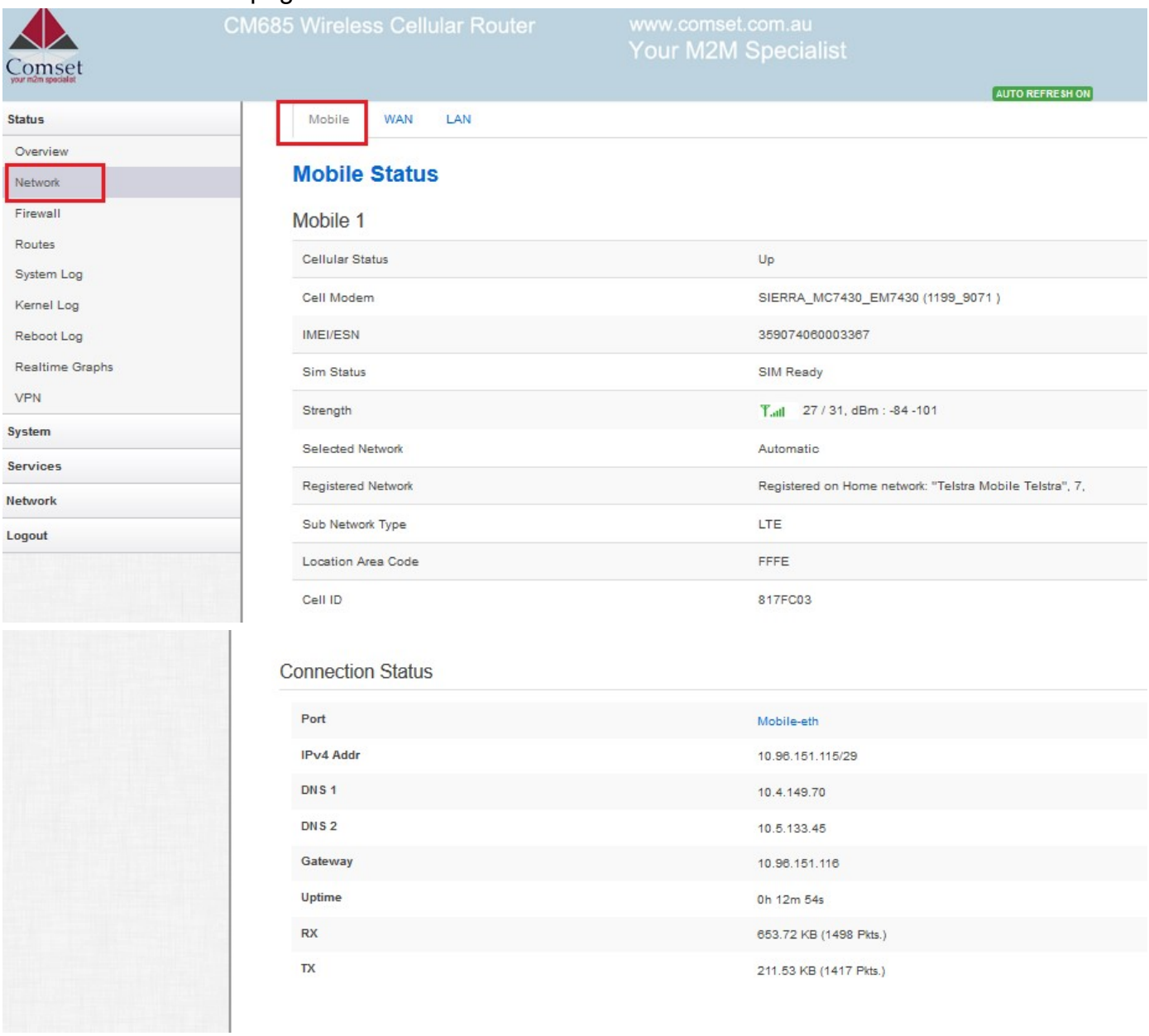
Click “Status” in the navigation bar, and then click “Overview”.



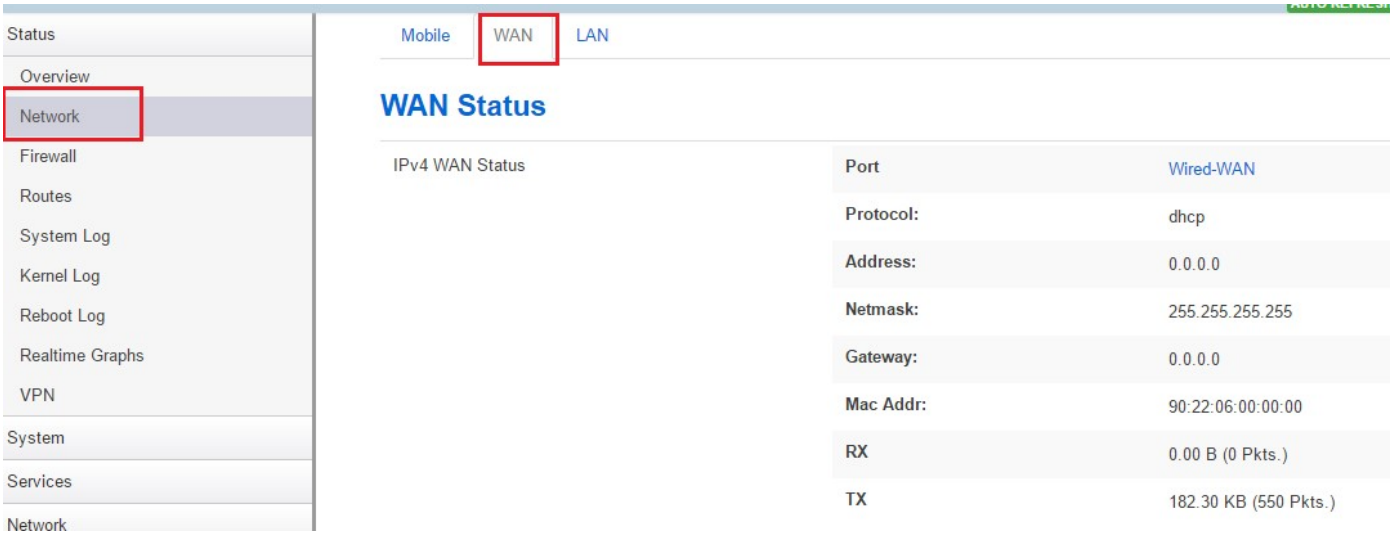
3.3.2 Network status

The Network status page consists of 3 tabs, detailing information about the cell mobile interface, WAN and LAN.

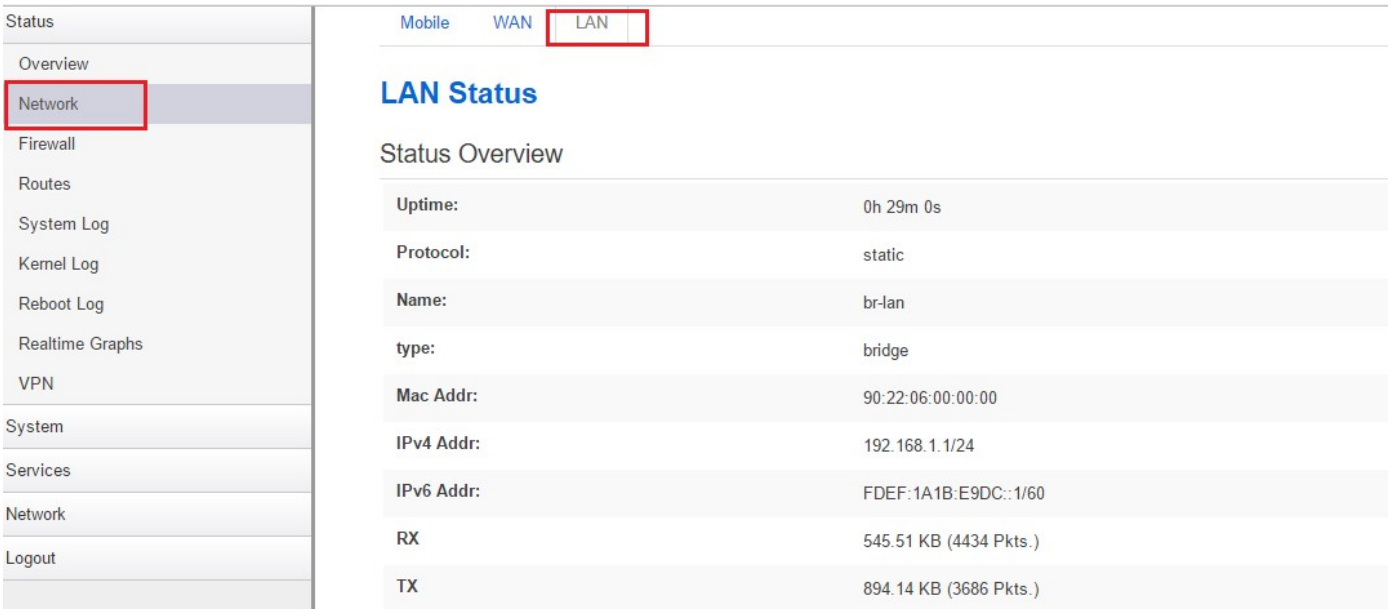
Cell mobile interface page:

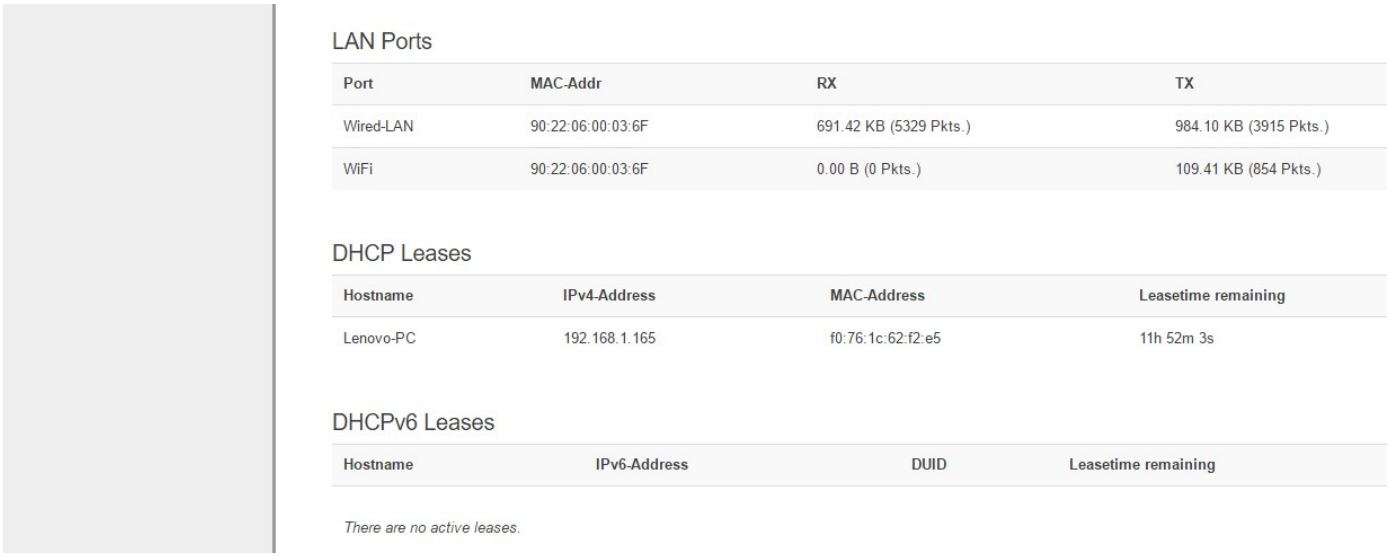


WAN status page:



LAN status page:





LAN Ports

Port	MAC-Addr	RX	TX
Wired-LAN	90:22:06:00:03:6F	691.42 KB (5329 Pkts.)	984.10 KB (3915 Pkts.)
WiFi	90:22:06:00:03:6F	0.00 B (0 Pkts.)	109.41 KB (854 Pkts.)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
Lenovo-PC	192.168.1.165	f0:76:1c:62:f2:e5	11h 52m 3s

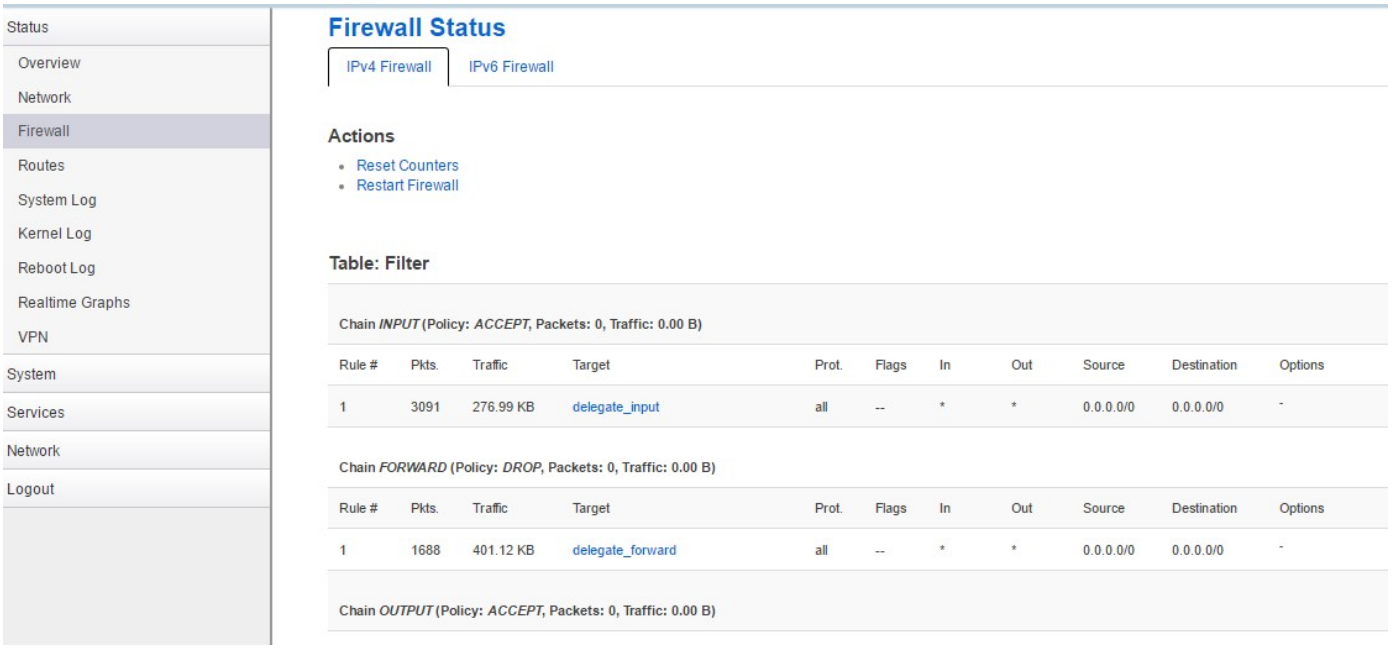
DHCPv6 Leases

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.



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

System
Services
Network
Logout

Firewall Status

IPv4 Firewall | IPv6 Firewall

Actions
- Reset Counters
- Restart Firewall

Table: Filter

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

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	3091	276.99 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

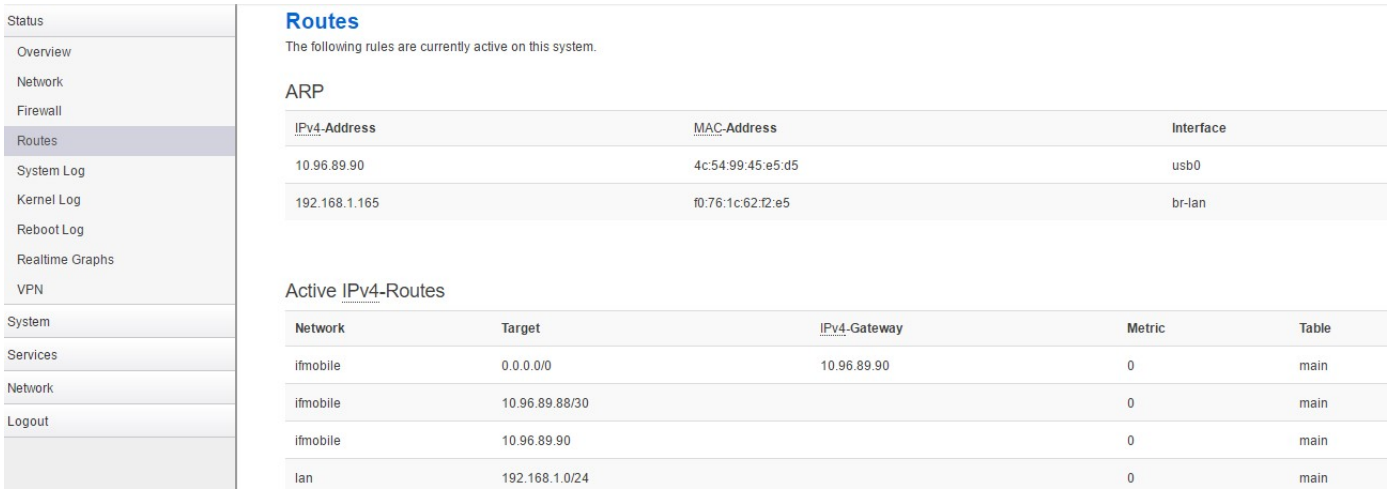
Chain *FORWARD* (Policy: *DROP*, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	1688	401.12 KB	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

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

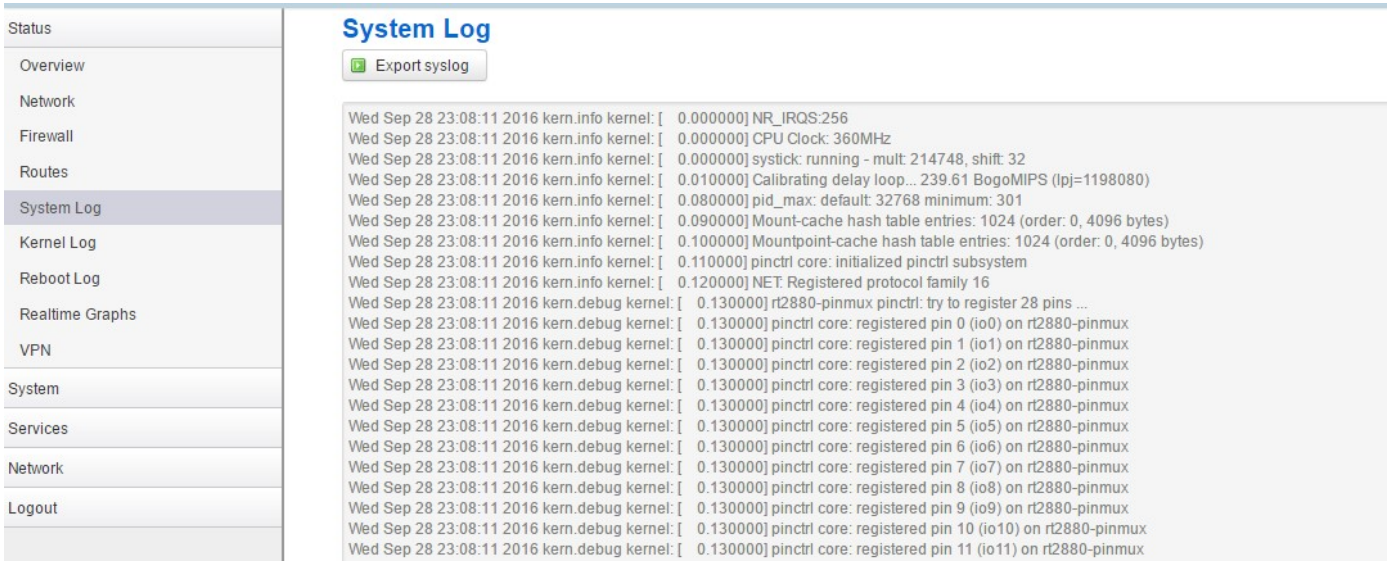
3.3.4 Routes

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



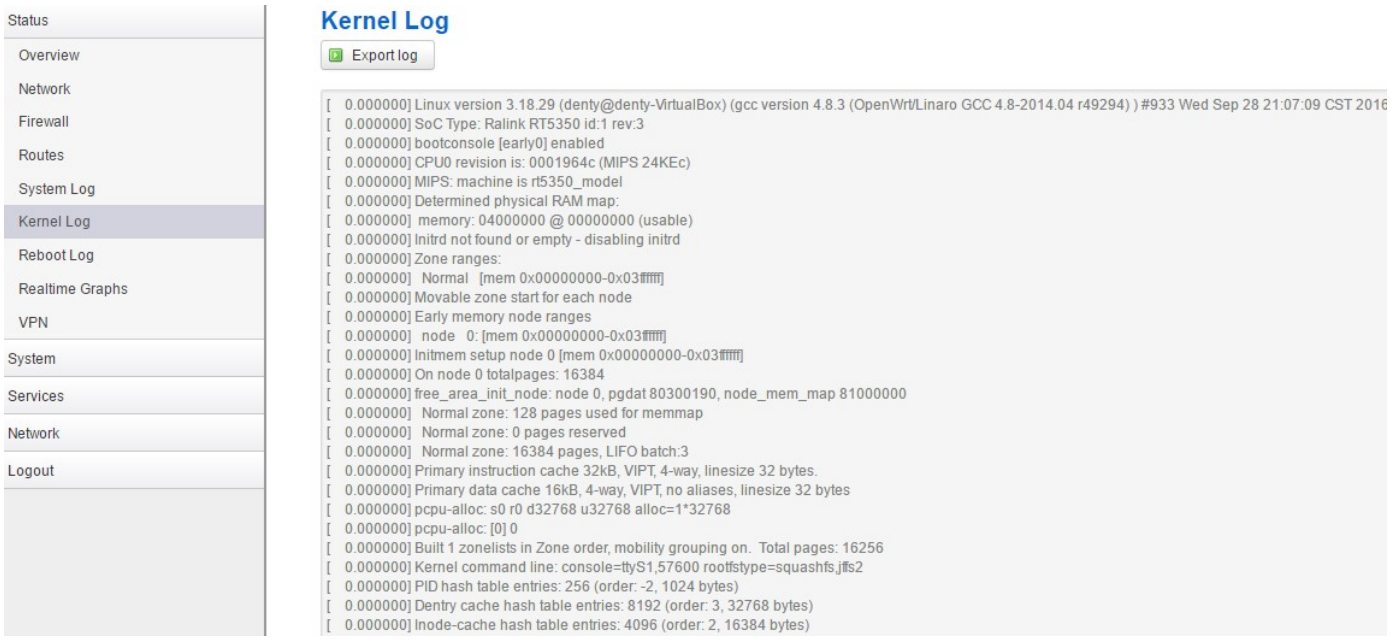
3.3.5 System log

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”.



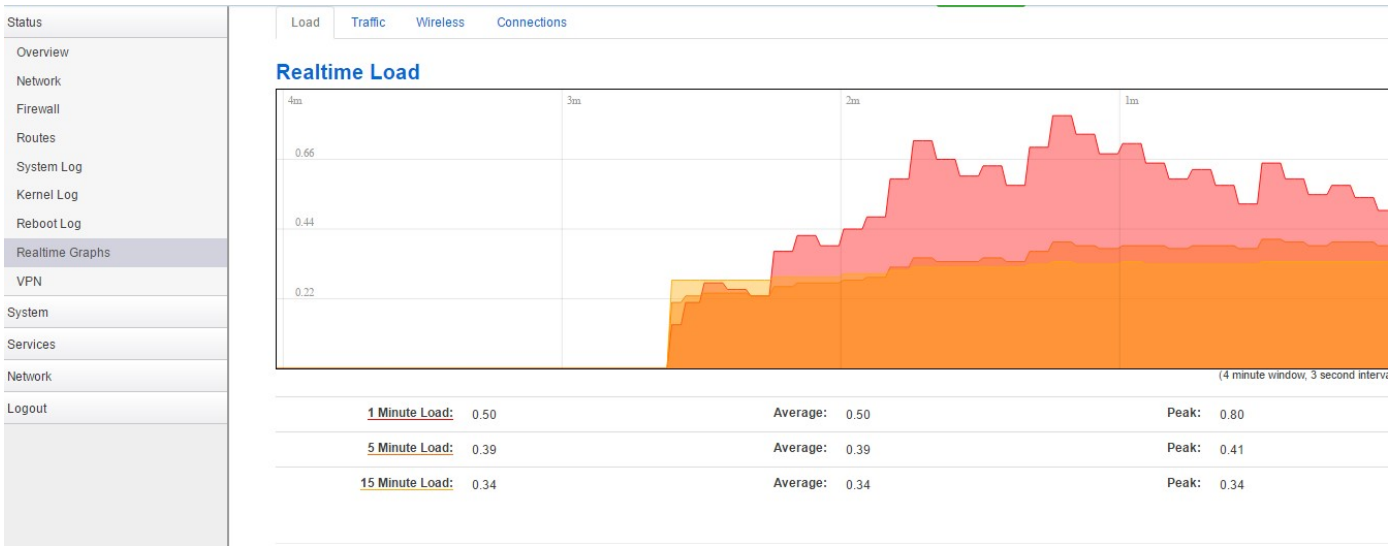
3.3.6 Kernel log

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”.



3.3.7 Realtime graphs

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

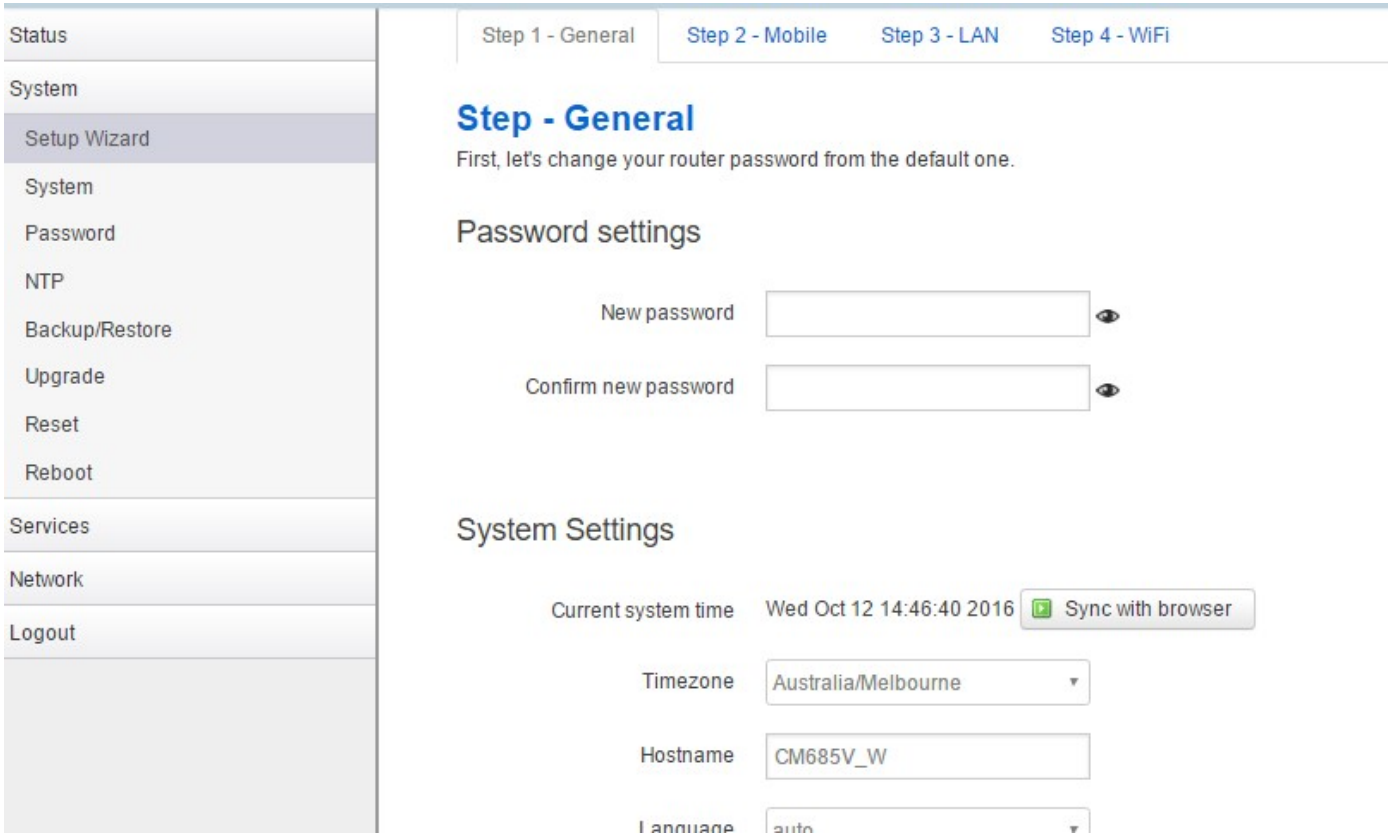


3.4 System Configuration

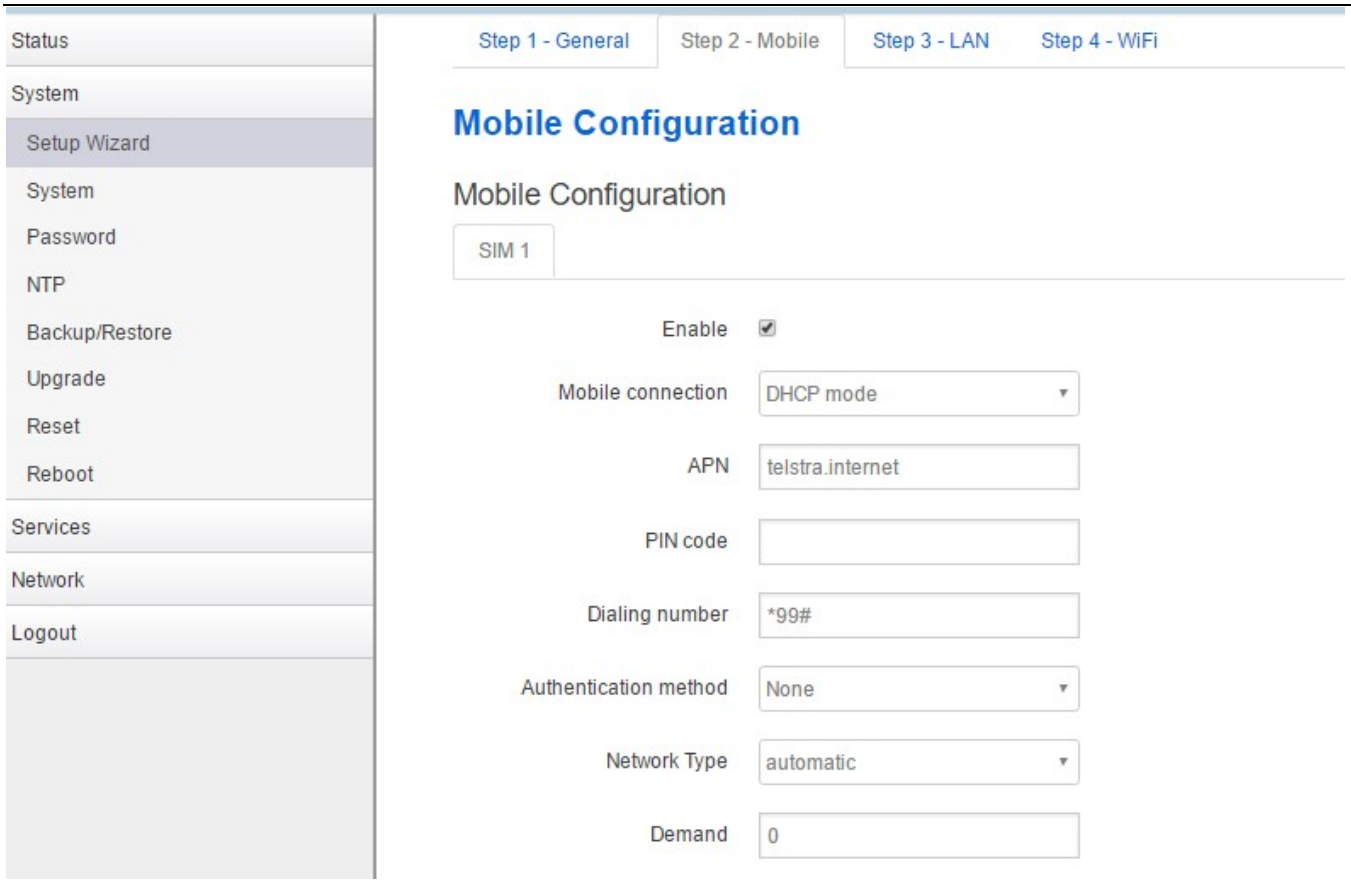
3.4.1 Setup wizard

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

- General
- Mobile
- LAN
- WiFi



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



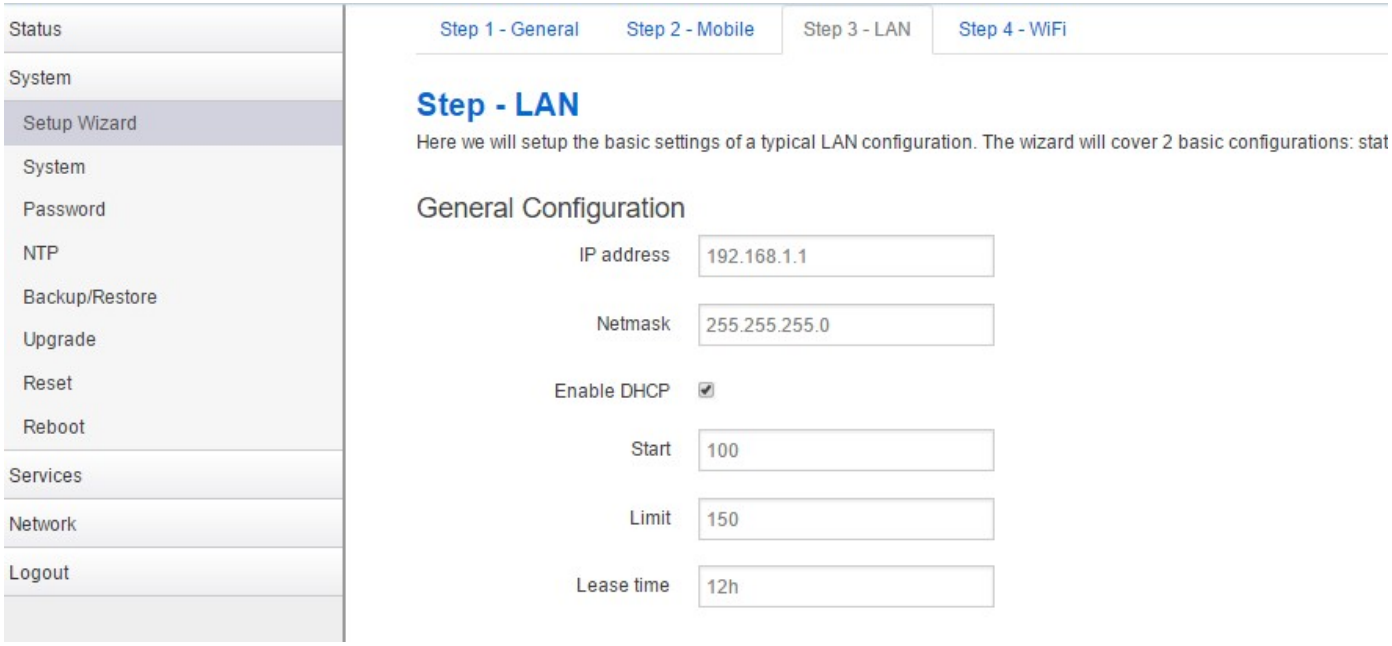
- **Enable:** Enable mobile network;
- **Mobile connection:** Select a suitable mode for the mobile connection. The default value is 'DHCP mode';
- **APN:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider;
- **PIN code:** Most SIM cards don't have a PIN code, in 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.

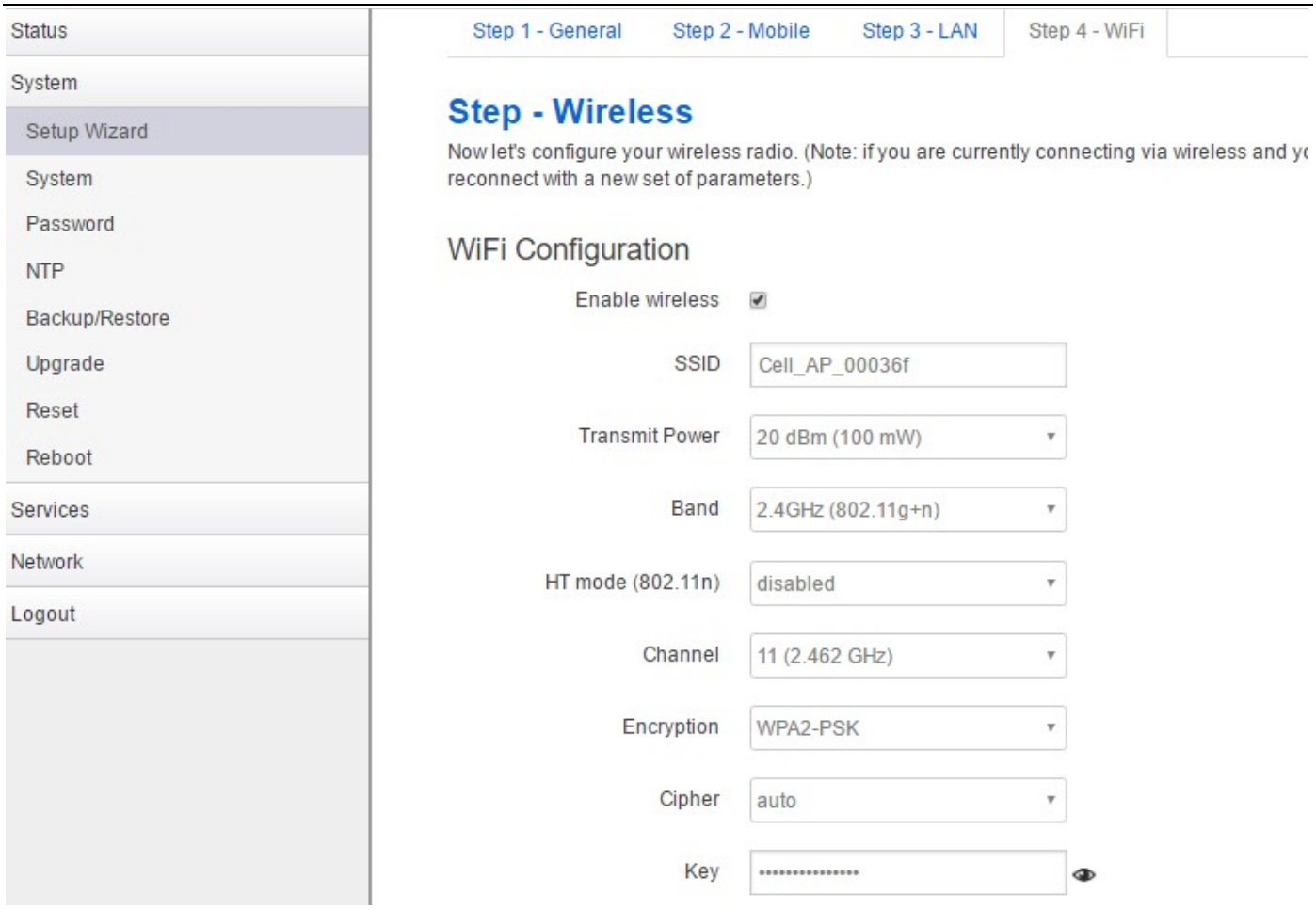
- **Password:** Fill in the related value. This can be obtained from your carrier or SIM Card Provider.
- **Network Type:** Different Cell Modems support different types. The default value is *Automatic*.
- **MTU:** Maximum Transmission Unit. It is the maximum size of packets transmitted on the

network. The default value is 1500. Please configure it to optimise your own network.

When finished, click “Save & Next”

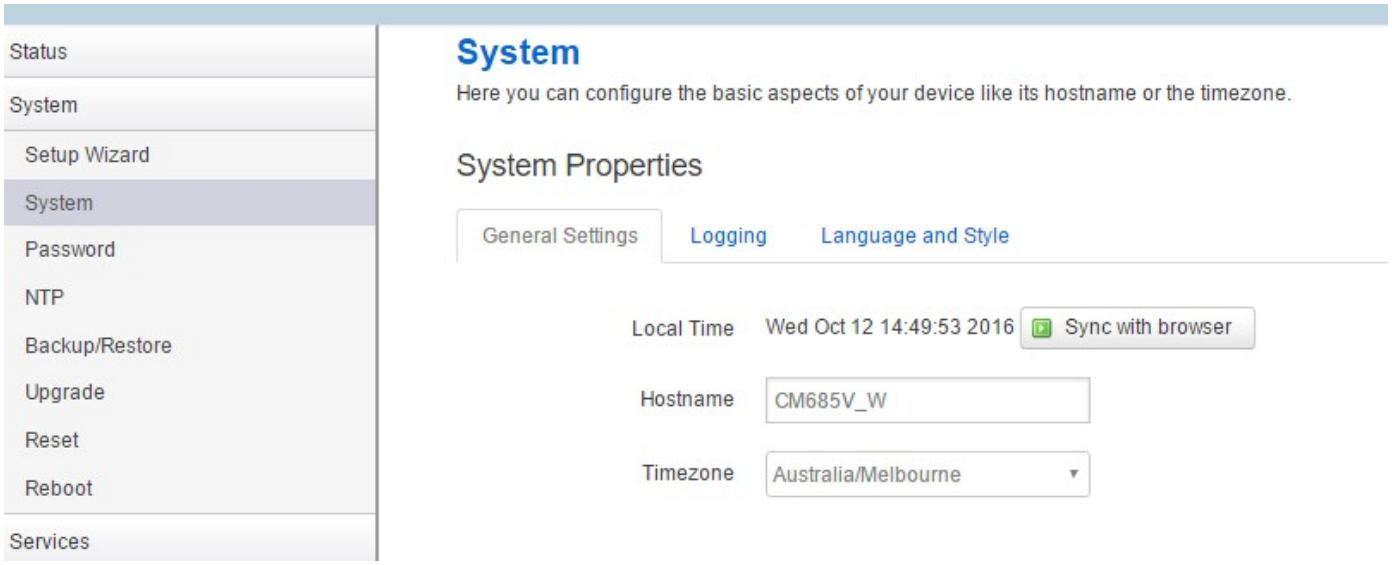


Fill in parameters as required. When finished, click “Save & Next”



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



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”.

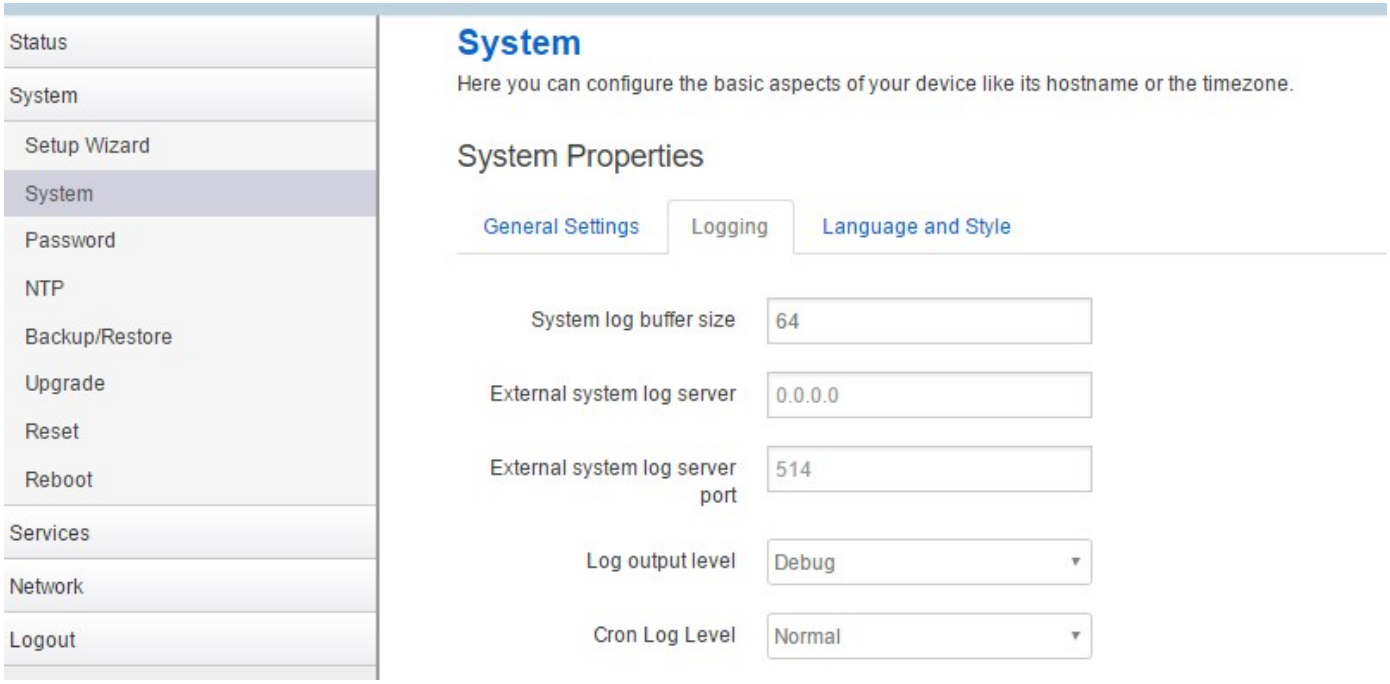
- **Hostname**

It is the router’s name. The default name is “CM685V_W”

- **Time zone**

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

Logging



- **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.

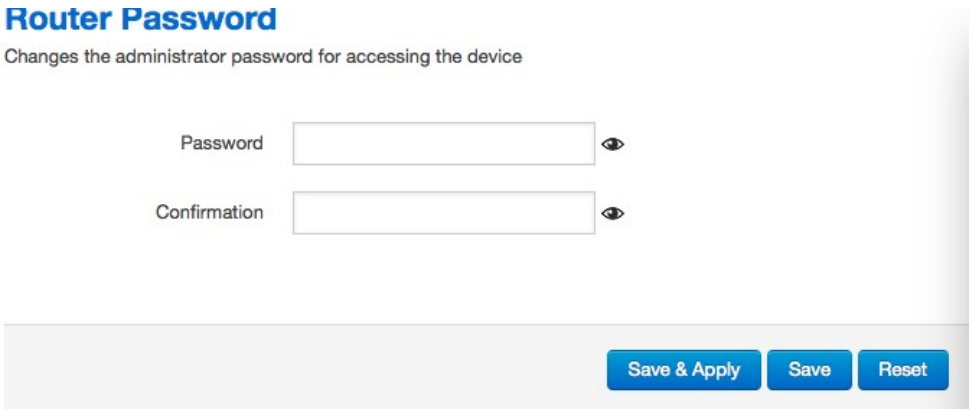
- **Cron log level**

It is the log level to process Crond.

Language and Style

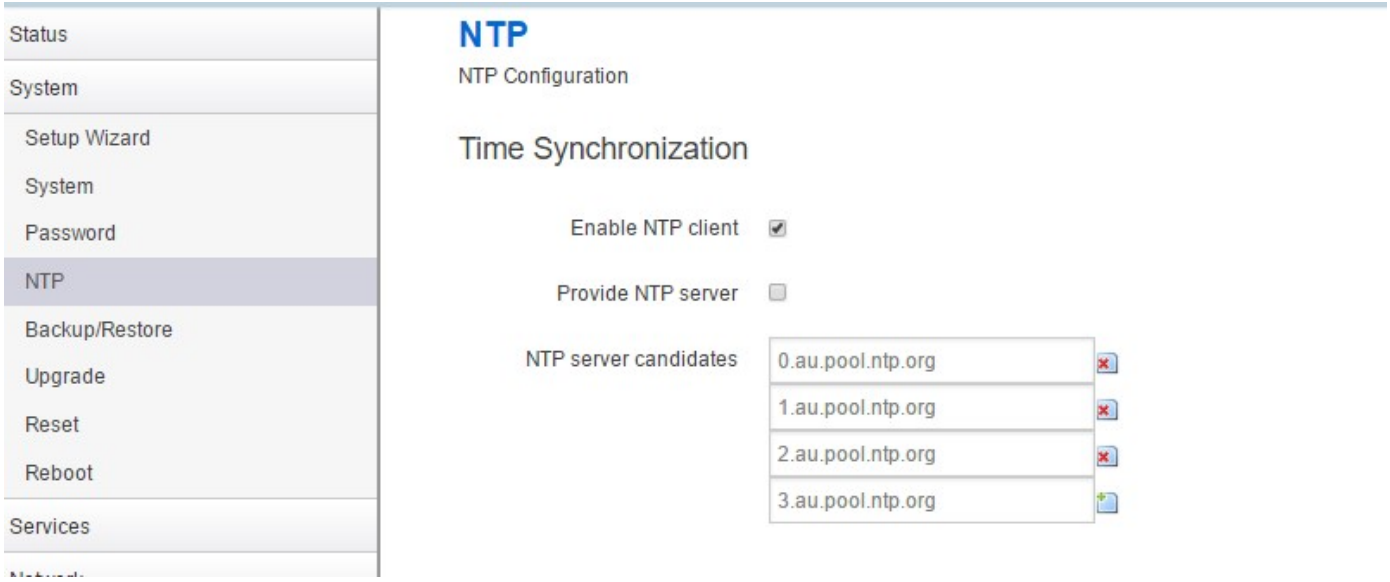
The default language is "English".

3.4.3 Password



Here you can change the administrator's password for accessing the device. Click the "eye button" to show the new password you entered.

3.4.4 NTP



NTP is Network Timing Protocol.

- **Enable NTP client**

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

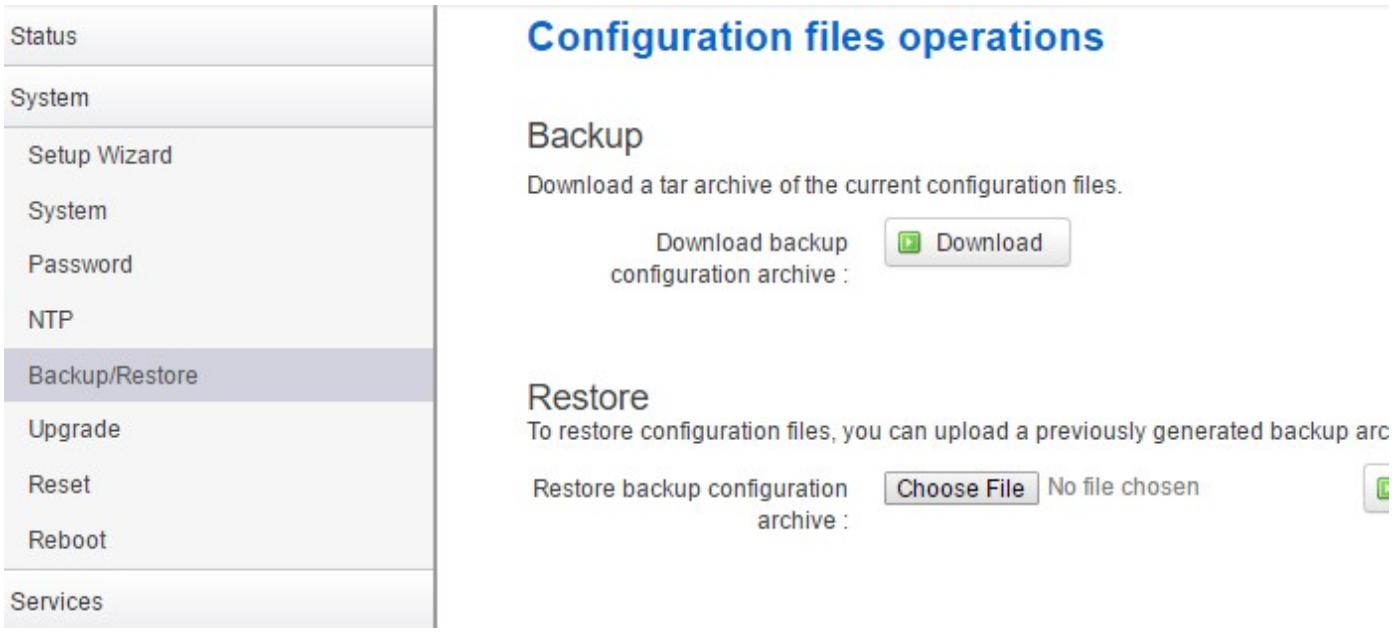
- **Provide NTP server**

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

- **NTP server candidates**

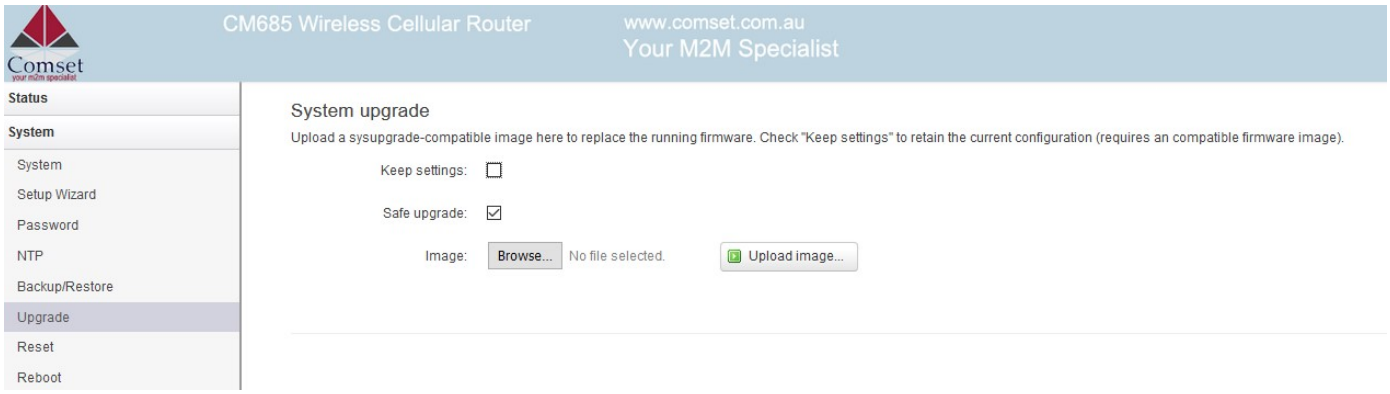
  It is the NTP server list. Multiple NTP servers are accepted. You can click the button to delete an entry, or click the button to add a new entry.

3.4.5 Backup/Restore



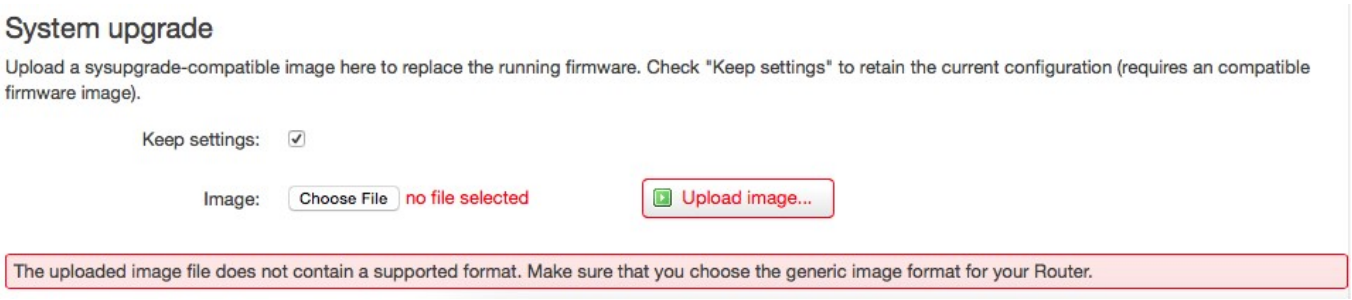
- To backup the configuration files, click the button “Download”. Then an archive file will be generated and downloaded to your PC automatically.
- To restore the configuration files, click the button “Choose File” and select an archived configuration file. Click the button “Upload”. The system will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

3.4.6 Upgrade

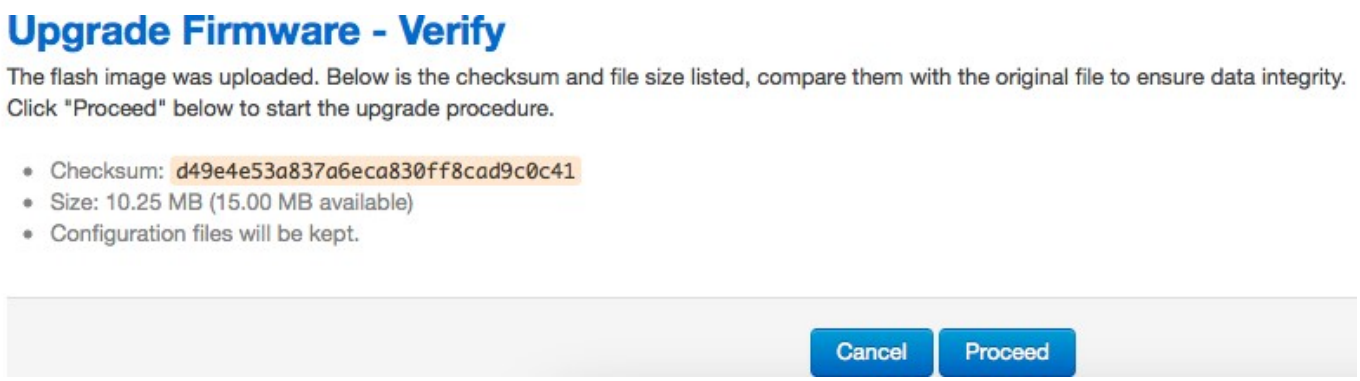


Upload a system compatible firmware to replace the current firmware. The default value for “Keep settings” is checked, which means the existing configuration will be kept after the system upgrade, otherwise the router will be reset to factory settings. We recommend to un-check “Keep settings” to prevent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

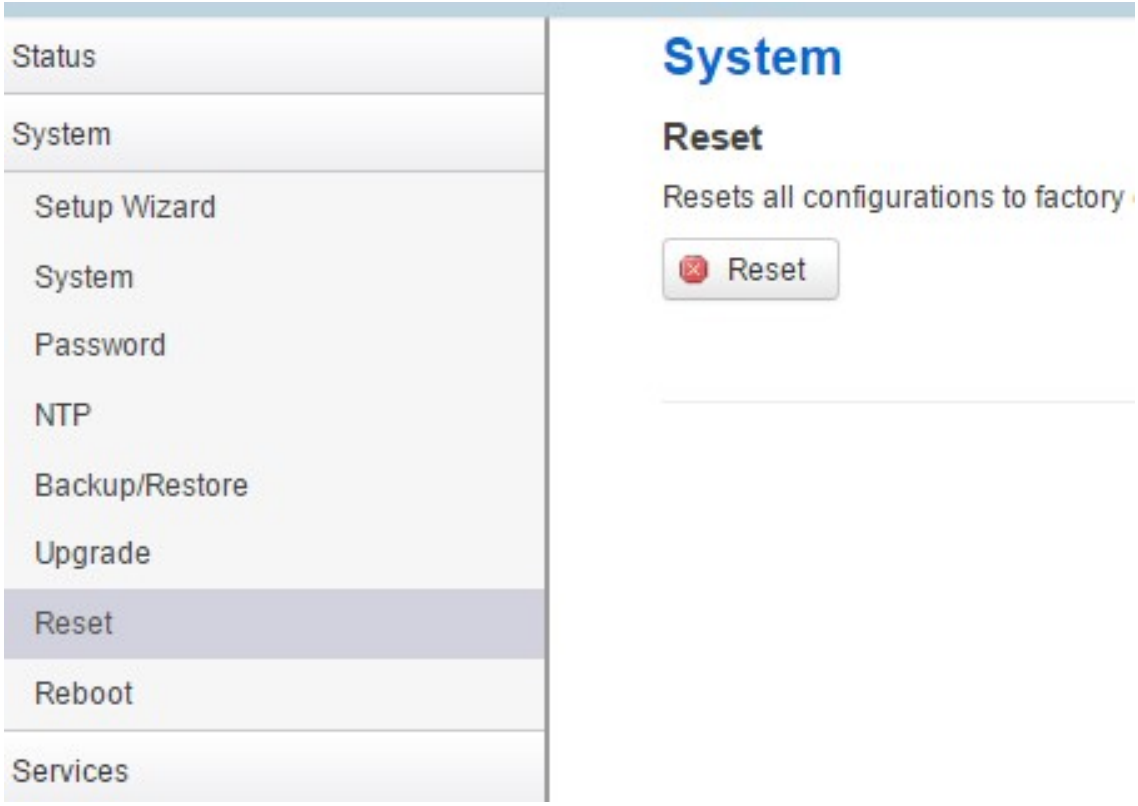
Click the button “Choose File” and select a compatible firmware, then click the button “Upload image”. The router will run a basic check of the file. If it is an incompatible file, an error message will appear like this one below:



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

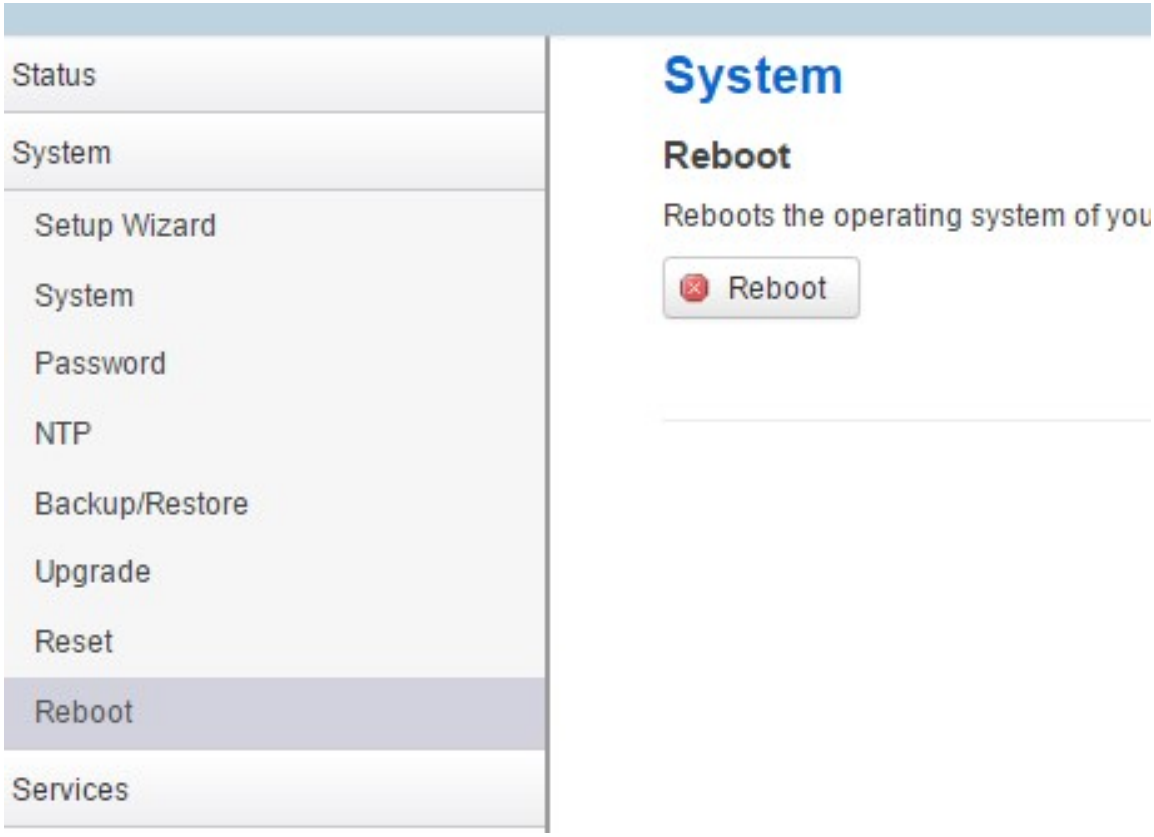


3.4.7 Reset



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

3.4.8 Reboot

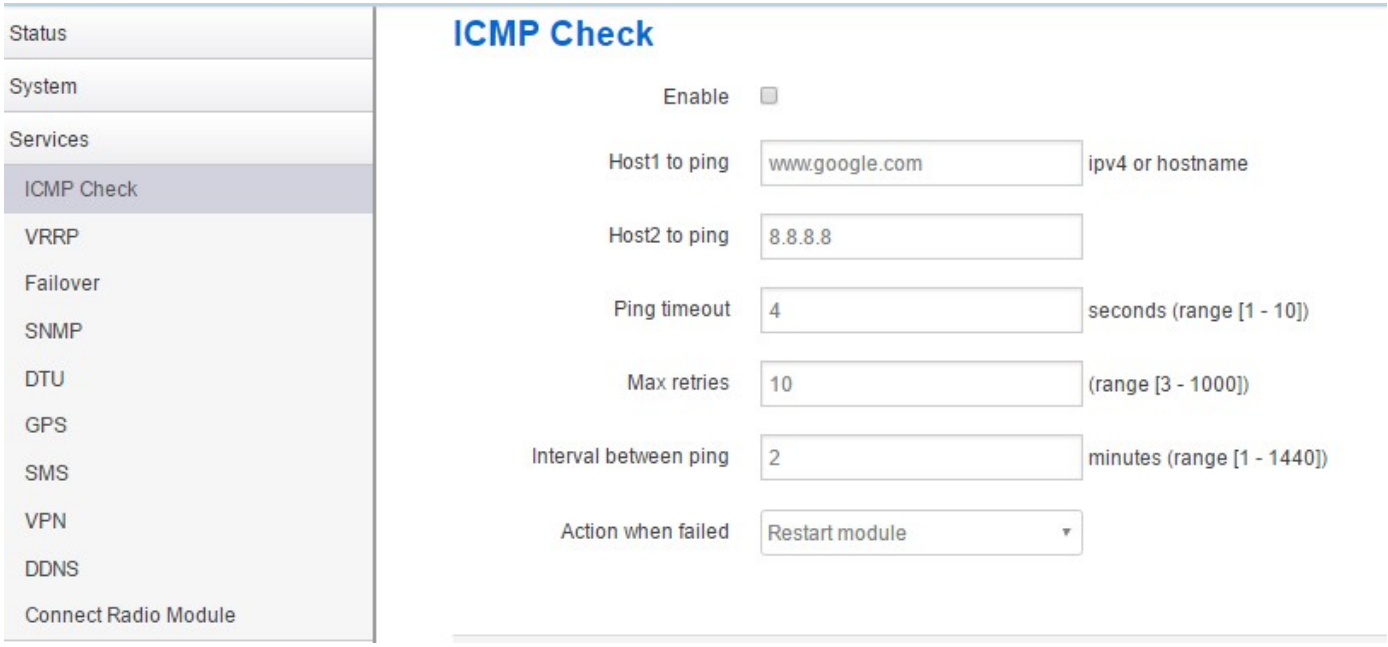


Click the button “Reboot” and the system will restart.

3.5 Services configuration

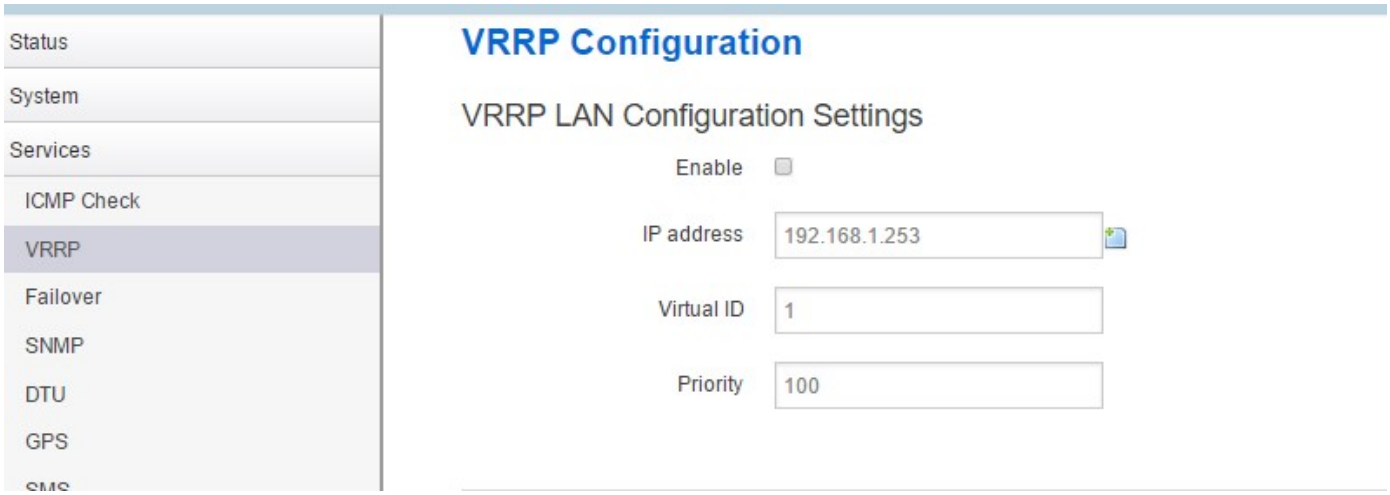
3.5.1 ICMP check

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.



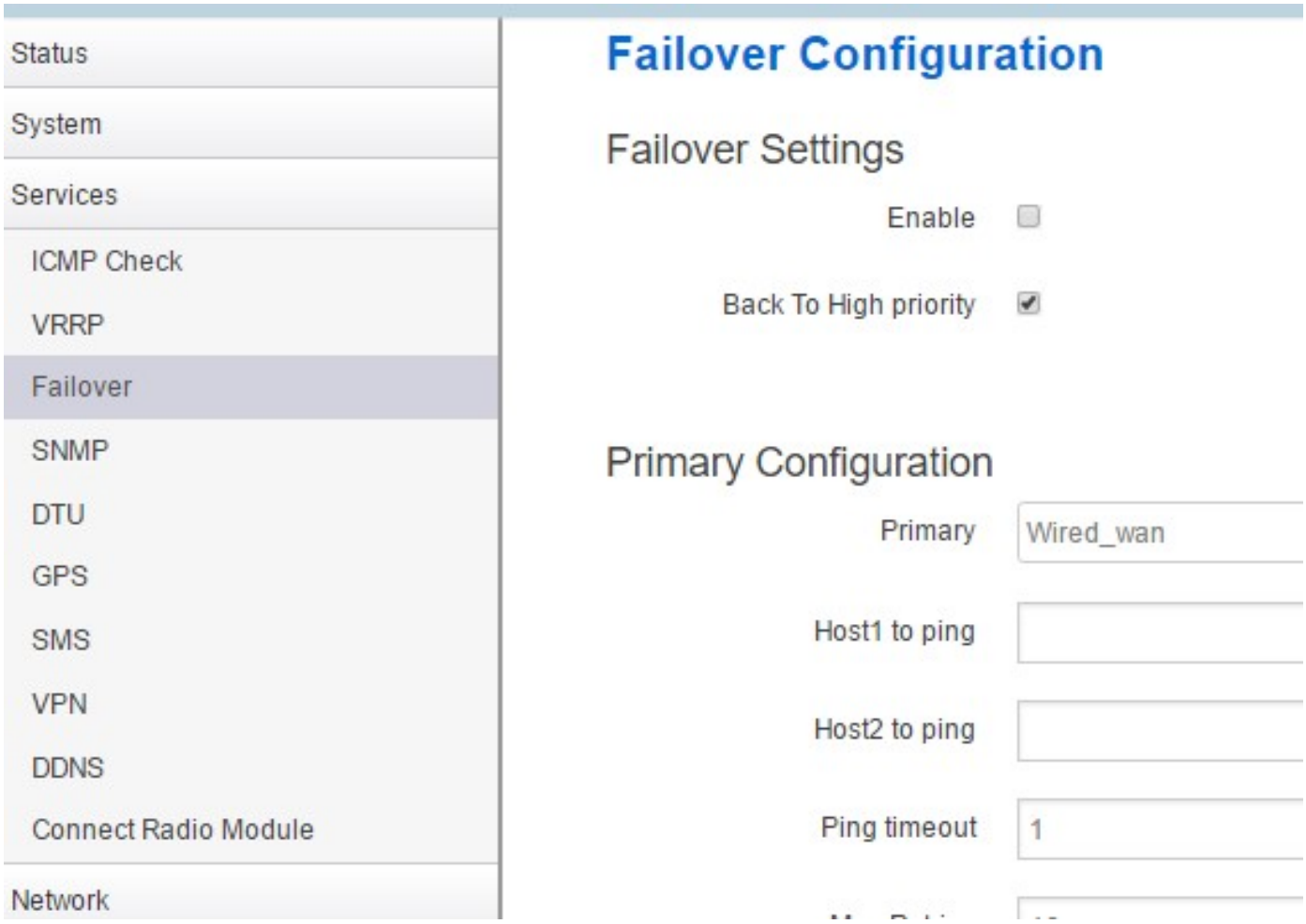
- **Enable**: Enable ICMP check feature
- **Host1 to ping / Host2 to ping**: The domain name or IP address for checking the network connection.
- **Ping timeout**: After a ping packet is sent, if the response packet is not received before the timeout, then this ping has failed.
- **Max retries**: When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

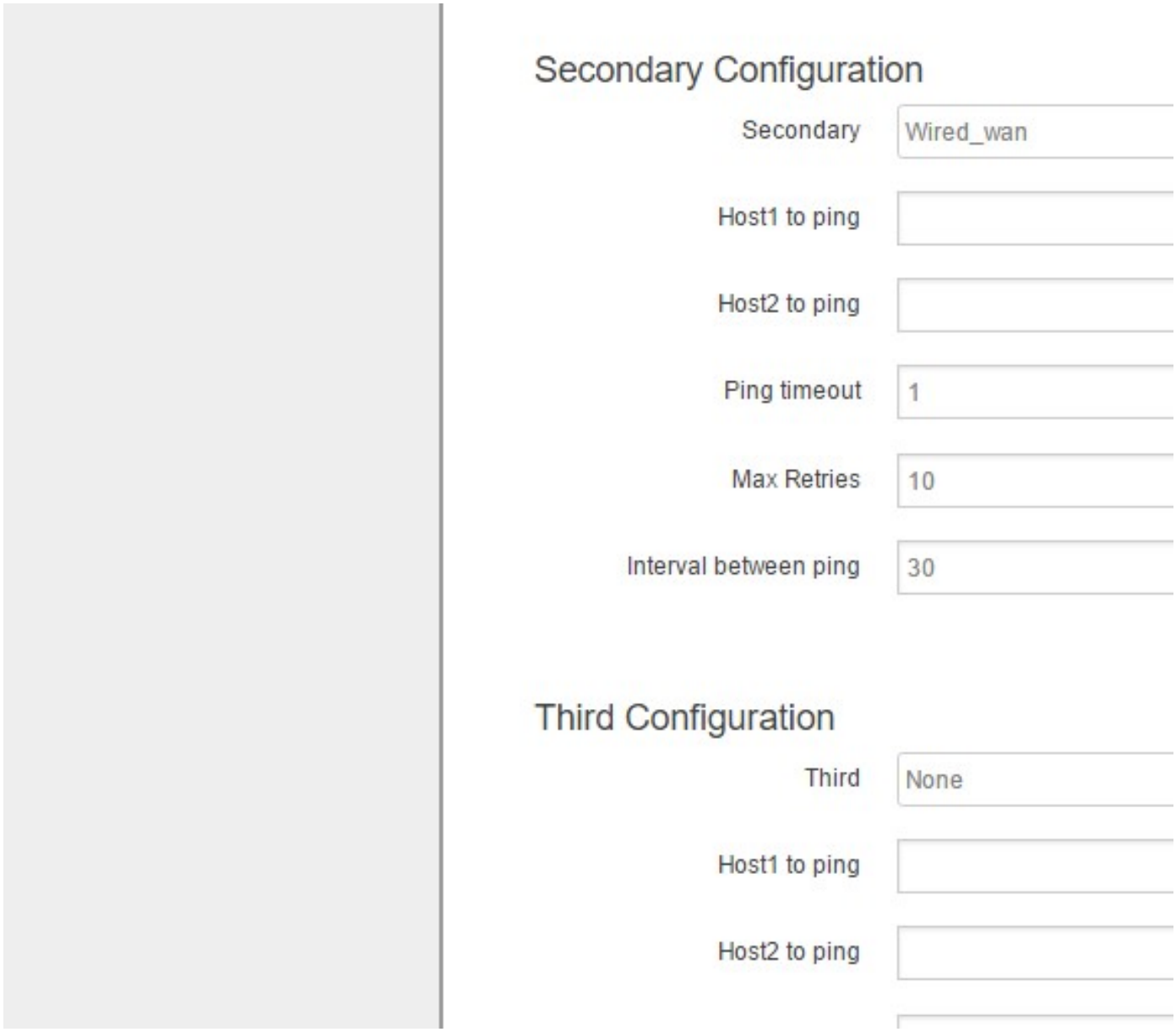
3.5.2 VRRP



- **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)

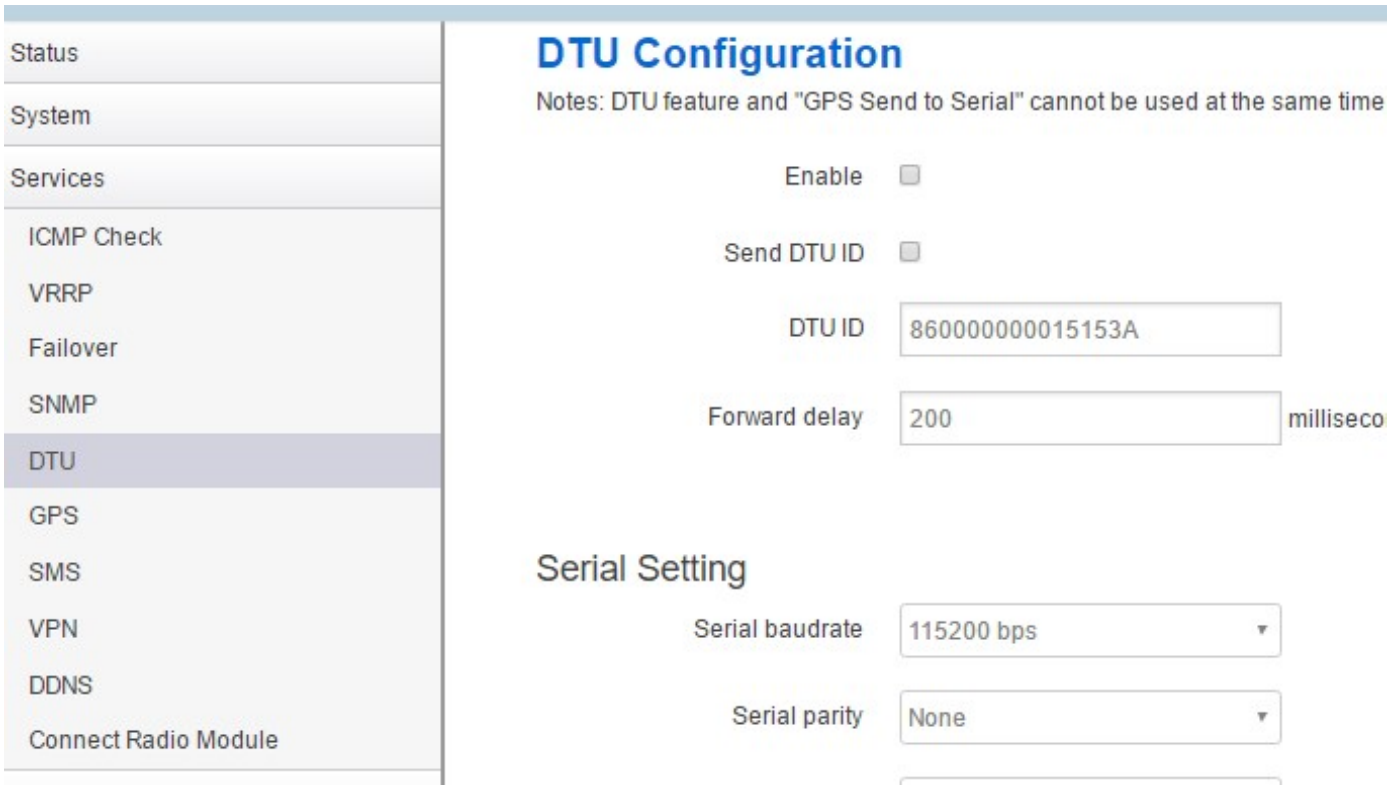


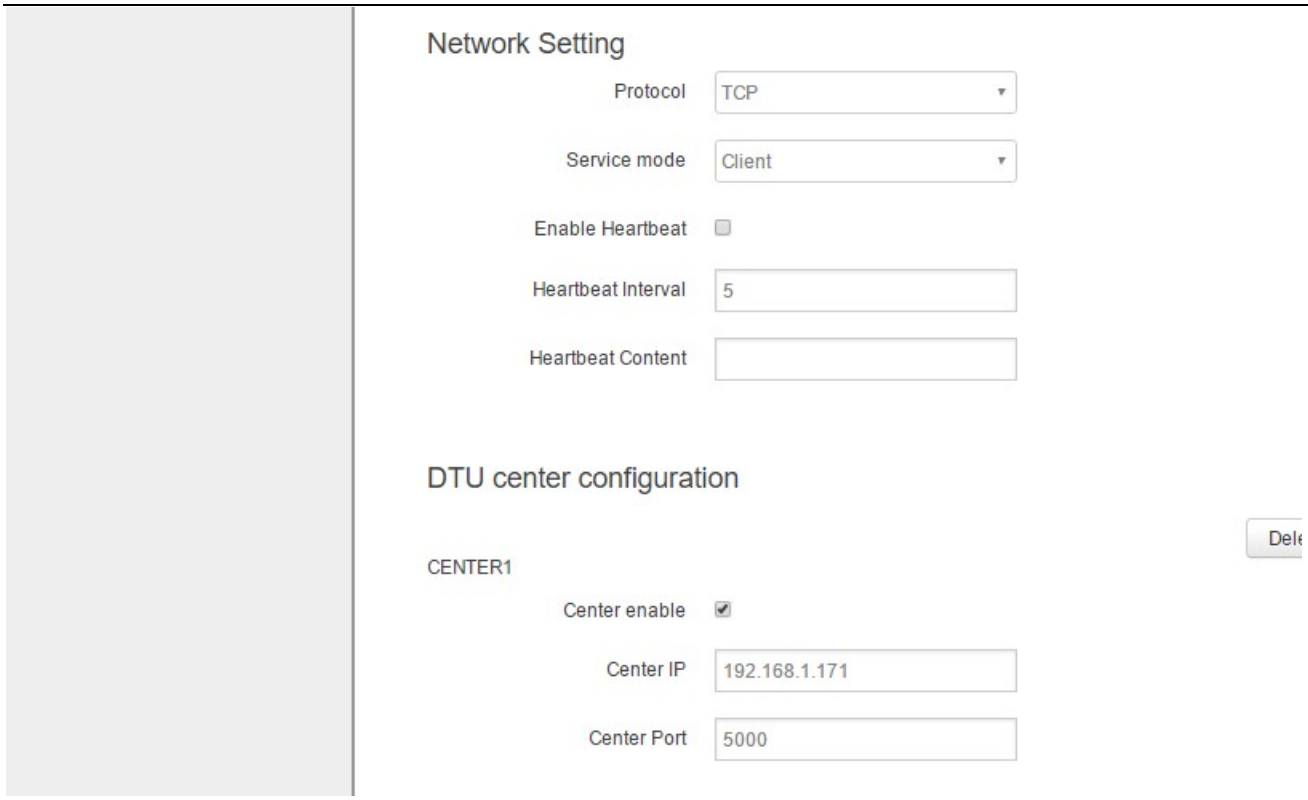


- **Enable**: Enable failover feature
  - **Back to high priority**: If “back to high priority” is checked, the router will go back to the selected “high priority” WAN interface when available. The priorities can be set to primary, secondary and third priority. There are four options to choose from: 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 CM685V-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.





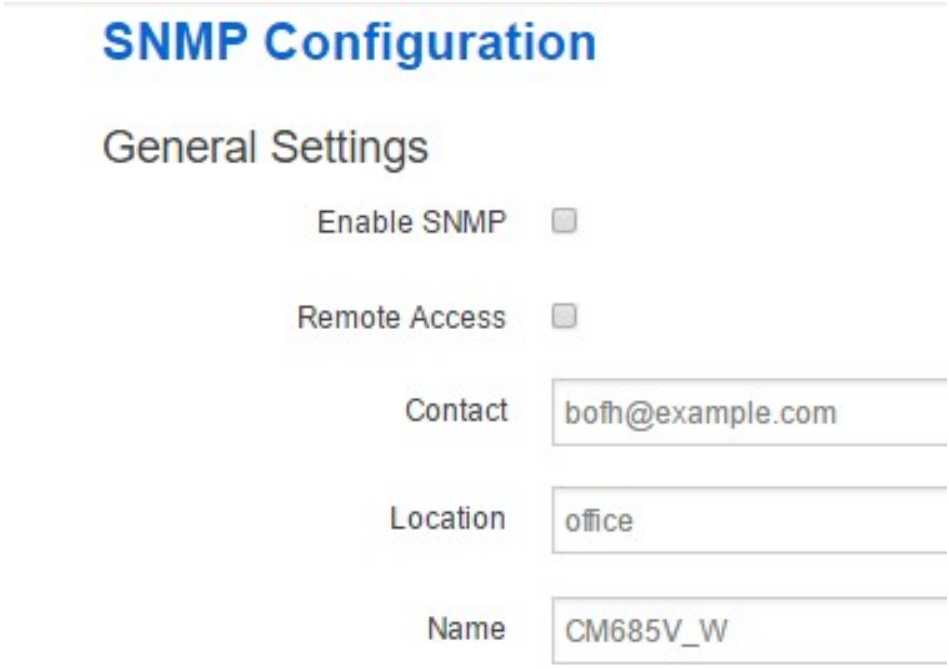
- **Enable**: Enable DTU feature.
- **Send DTU ID**: Send DTU ID at the front of the packet.
- **DTU ID**: The default DTU ID is the SN of the router. You can change it if required.
- **Forward delay**: This unit is in milliseconds. It is the time delay when sending data between the serial port and the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

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

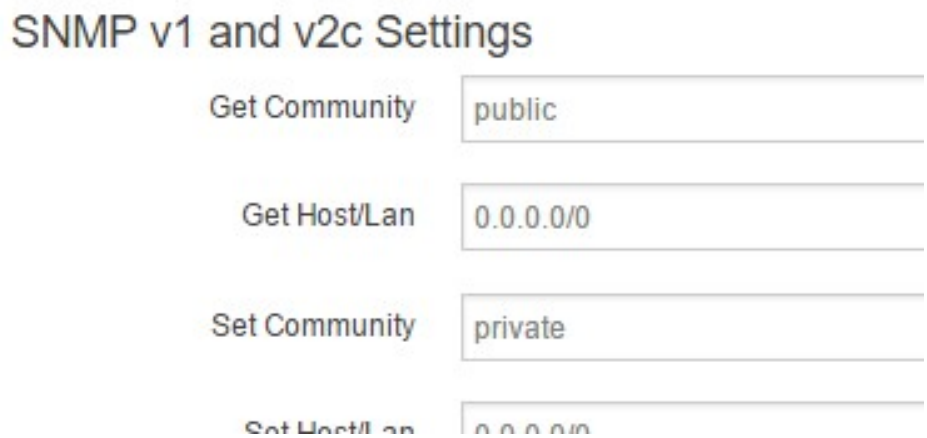
- **Protocol:** Both TCP and UDP are supported
- **Service mode:** Client and Server are supported.
- **Enable heartbeat:** The heartbeat is used to maintain the “keep alive” connection.
- **Heartbeat interval:** The time between two heartbeat packets.
- **Heartbeat content:** The content of heartbeat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

Notes:
The maximum number of DTU centers is 32.

3.5.5 SNMP

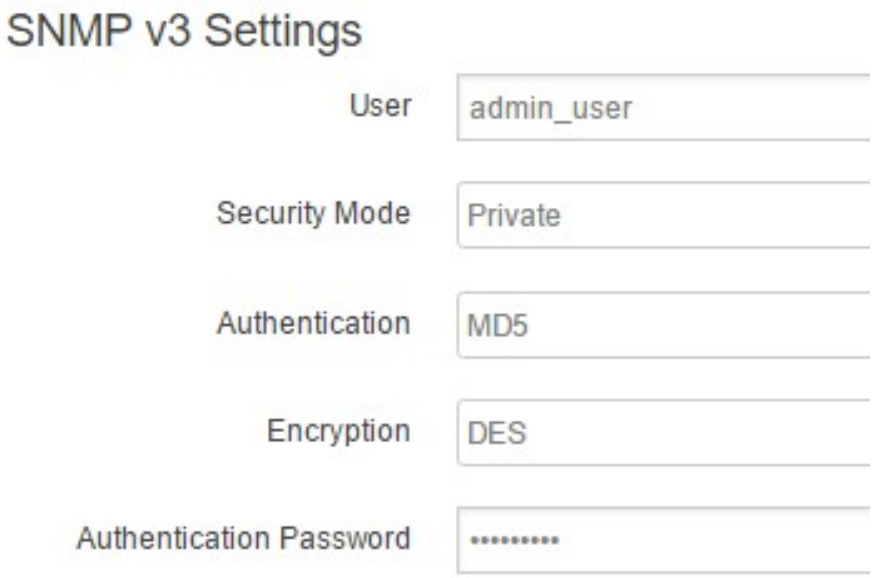


- **Enable SNMP**: Enable the SNMP feature
- **Remote Access**: Allow SNMP remote access. If it is unchecked, only the LAN subnet can access SNMP.
- **Contact**: Set the contact information here.
- **Location**: Set the router's physical address.
- **Name**: Set the router's name in SNMP.
- **Port**: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



- **Get Community**: The username for SNMP get. The default value is 'public'. SNMP get is read-only.

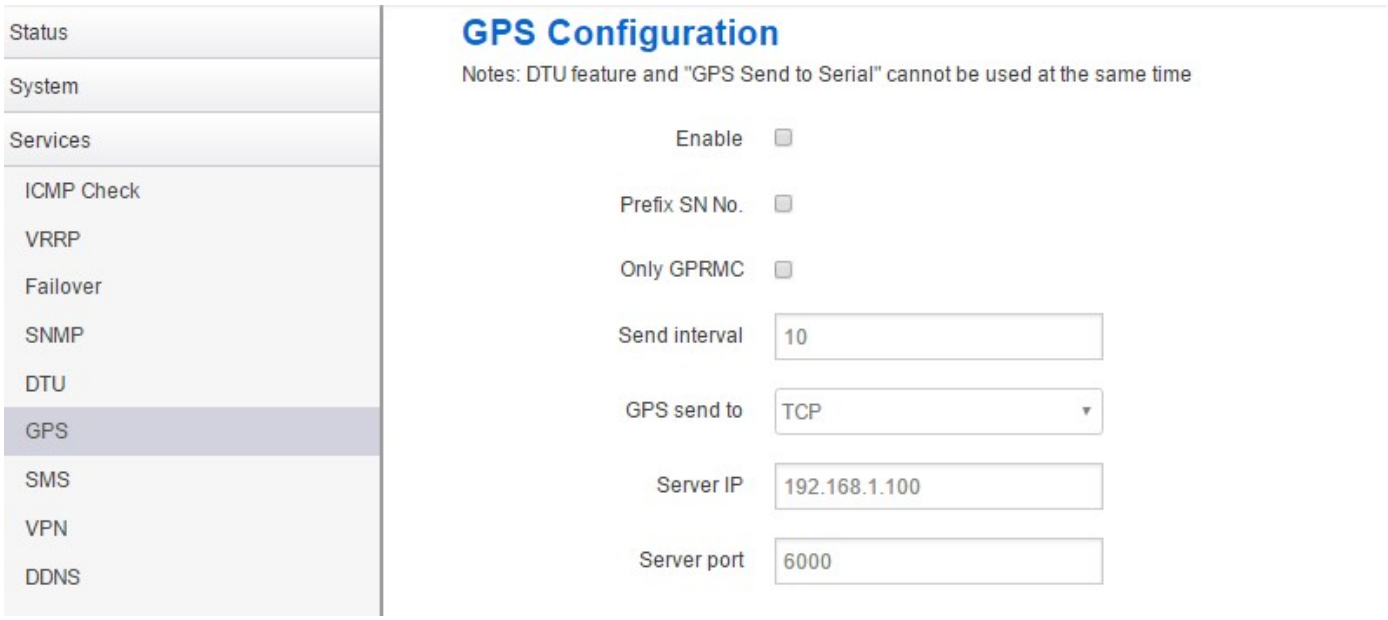
- **Get Host/Lan**: The network range to get the router via SNMP, default is ‘0.0.0.0./0’
- **Set Community**: The username for SNMP set. The default value is ‘private’. SNMP set is read-write.
- **Set Host/Lan**: The network range to set the router via SNMP, default is ‘0.0.0.0./0’



- **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.

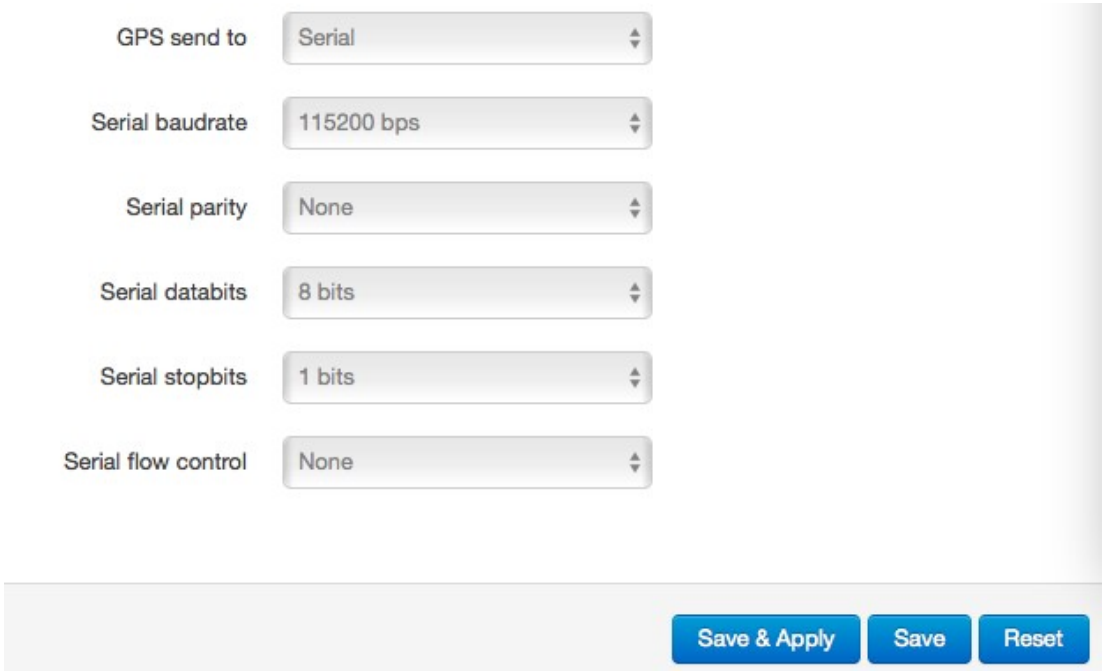
3.5.6 GPS (optional)



- **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 CM685V-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

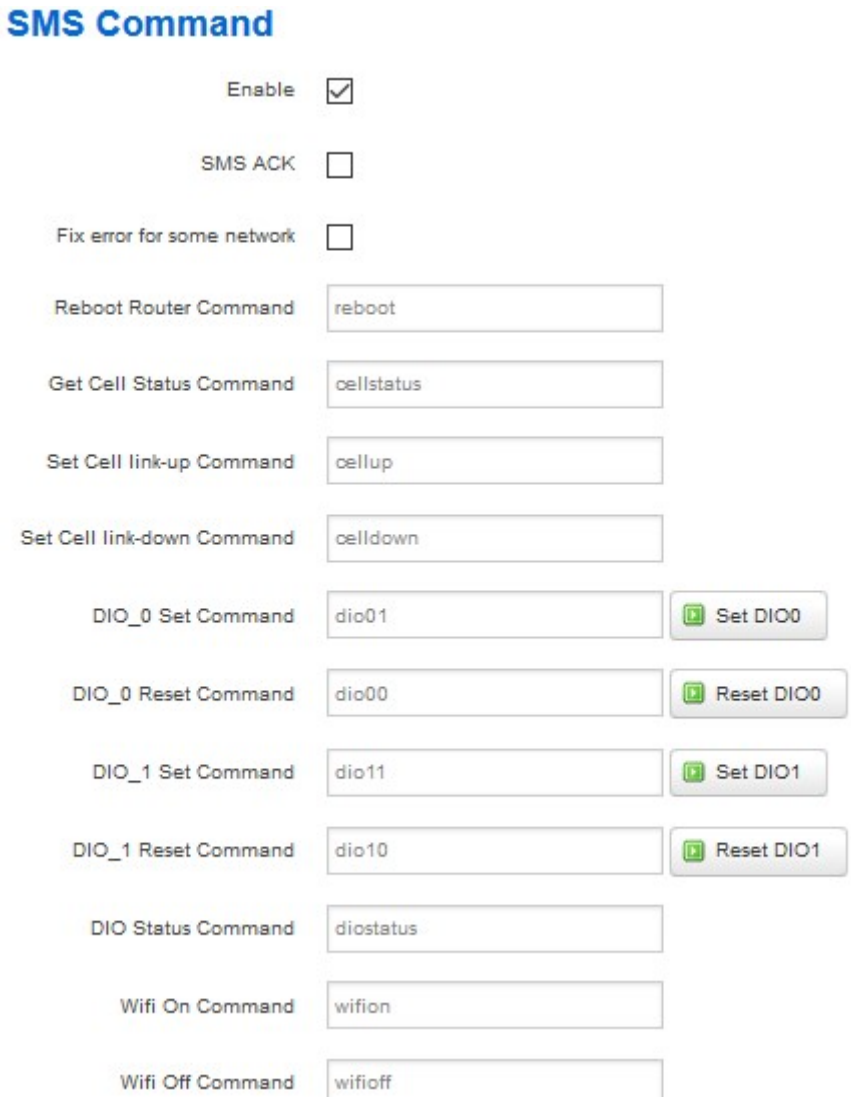
- **Server IP**: Fill in the correct destination server IP or domain name.
- **Server port**: Fill in the correct destination server port.



- **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

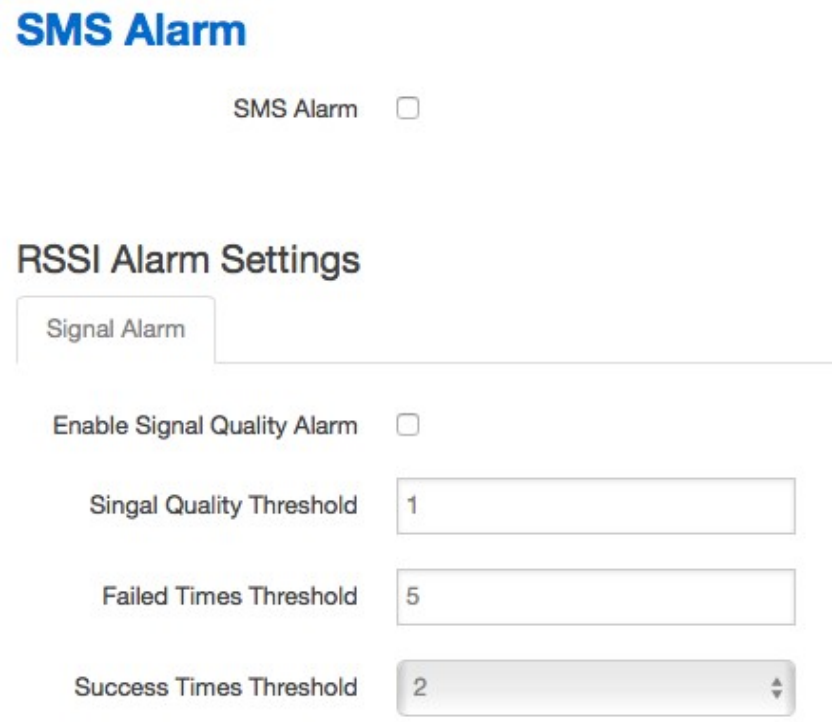
- **SMS Command**



- **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.

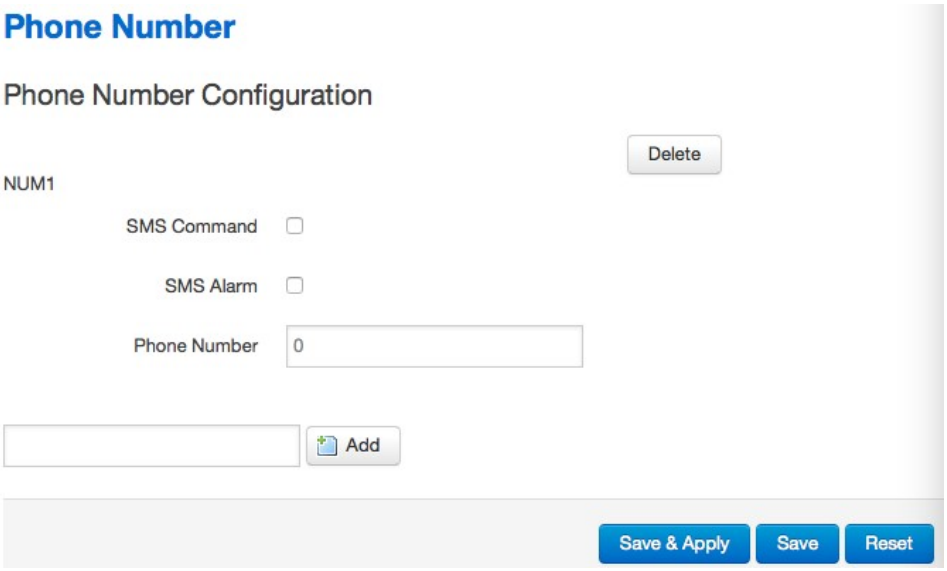
- **DIO_0 Reset Command**: Input the command for I/O port 0. For SMS feature, please keep the default parameters.
- **DIO_1 Set Command**: Input the command for I/O port 1. For SMS feature, please keep the default parameters.
- **DIO_1 Reset Command**: Input the command for I/O port 1. For SMS feature, 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**: 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**



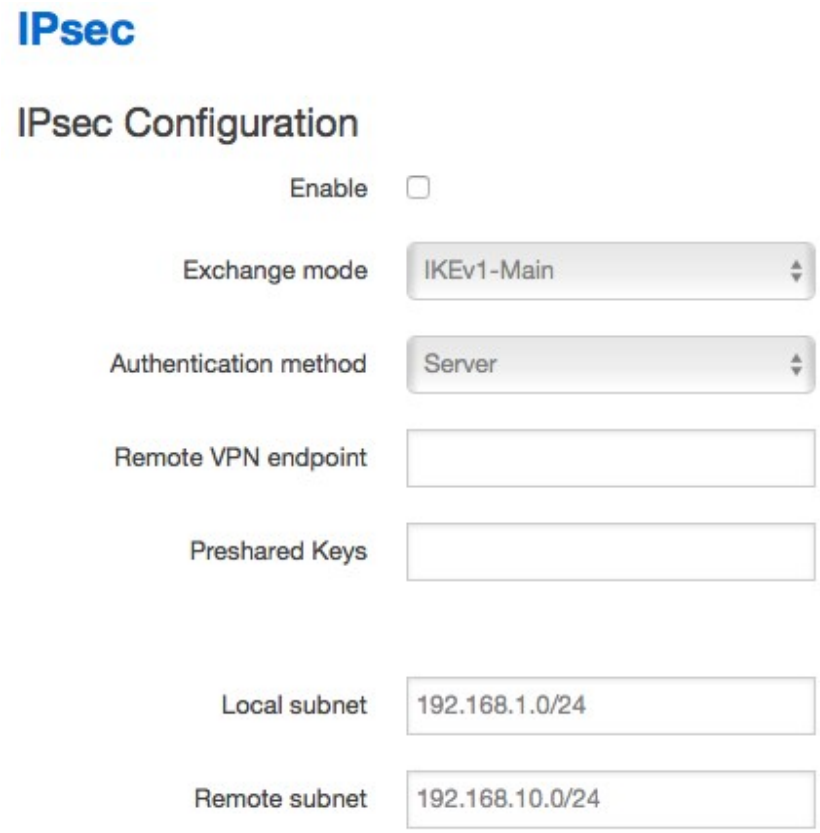
- **Add Phone number**: Input a name and click the button “Add” to add a new Phone number.
- **Delete Phone number**: Click the button “Delete”.
- **SMS command**: Enable the SMS command feature on this phone number.
- **SMS alarm**: This phone number can receive SMS alarms.

➢ **SMS**

- **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

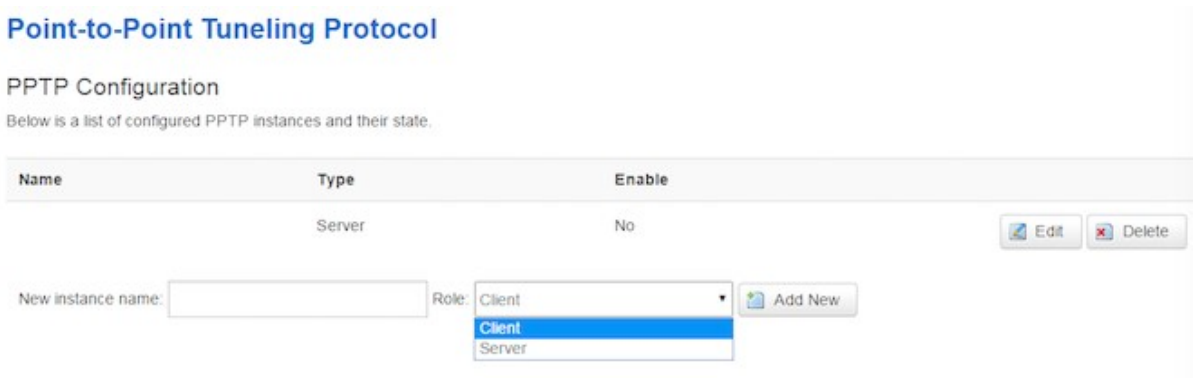
3.5.8.1 IPSEC



- **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.

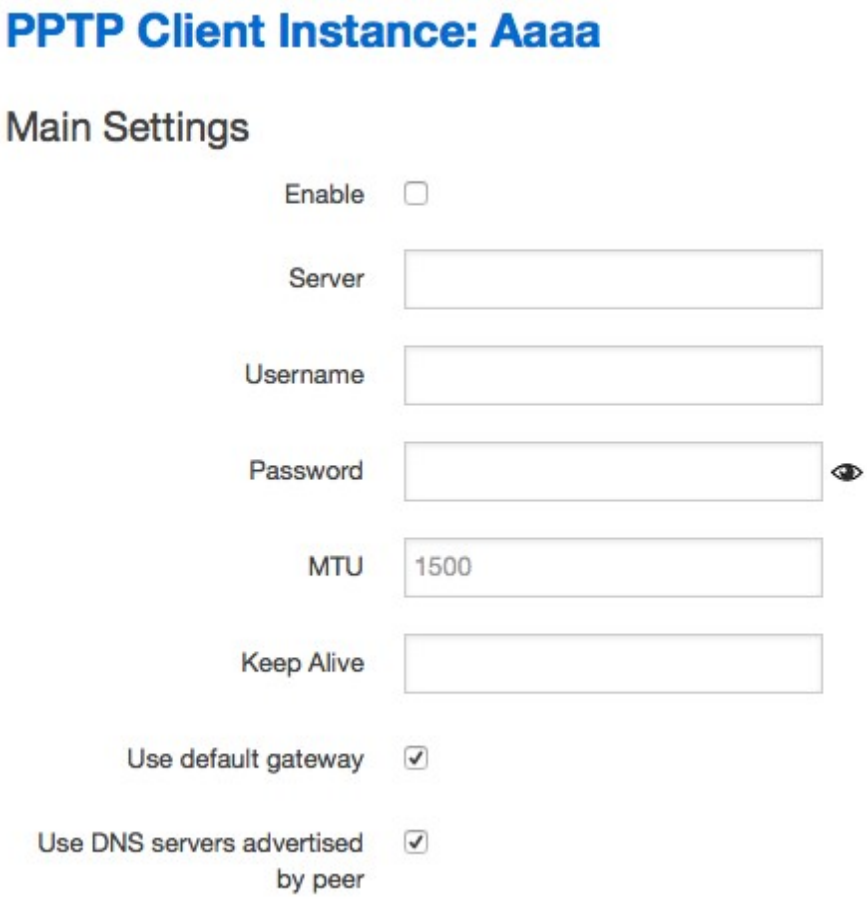
Note:
All configurations in Phase 1 Proposal and Phase 2 Proposal must match with the remote endpoint to establish an IPSEC connection.

3.5.8.2 PPTP



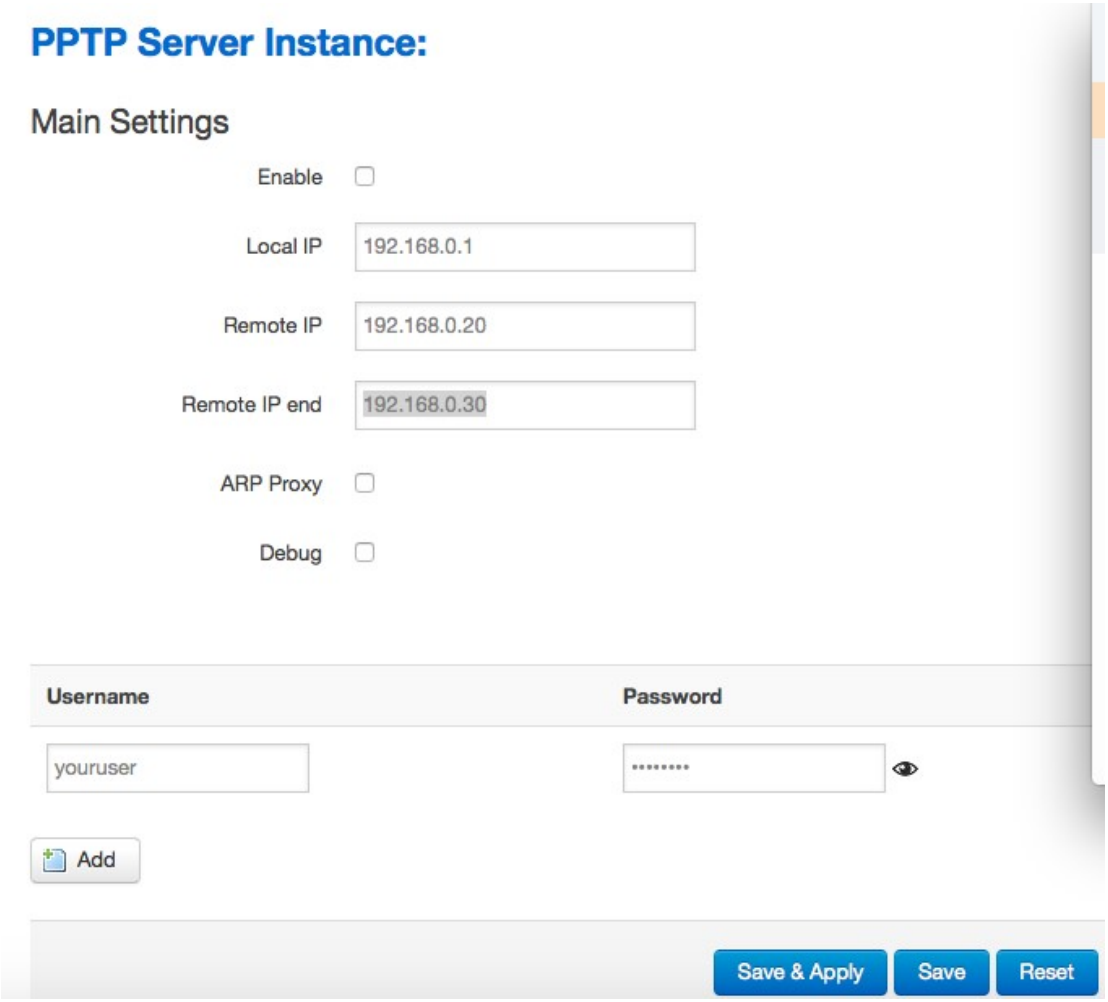
This page shows a list of configured PPTP instances and their state. Click the button “Edit” to make changes to an instance, or click the button “Delete” to delete it.

- **PPTP Client configuration**



- **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.

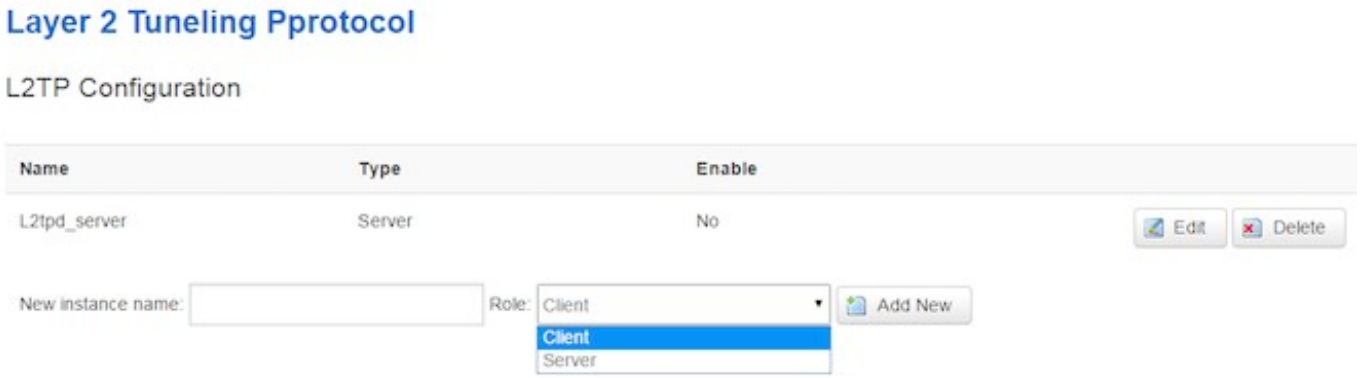
➢ **PPTP Server Configuration**



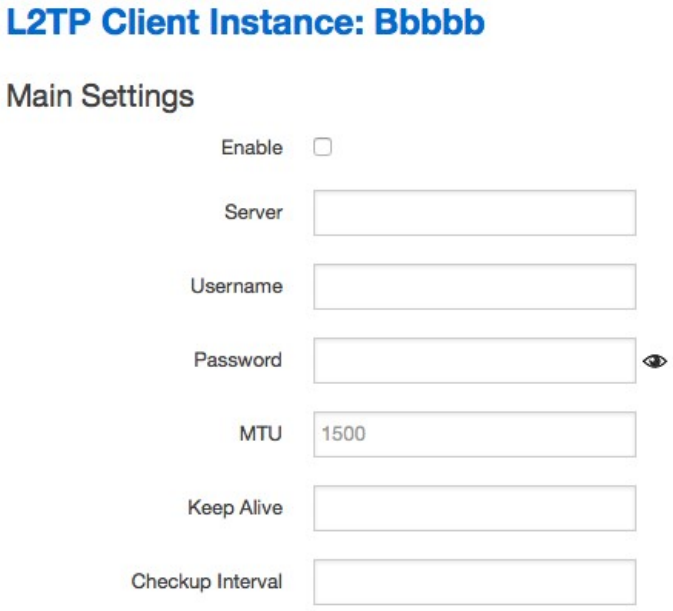
- **Local IP**: Indicates the server's IP address.
- **Remote IP**: The remote IP address lease start.
- **Remote IP end**: The remote IP address lease end.
- **ARP Proxy**: If the remote IP has the same subnet as the LAN, check it for connecting with each other.
- **Debug**: For PPTP server debug, the 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.

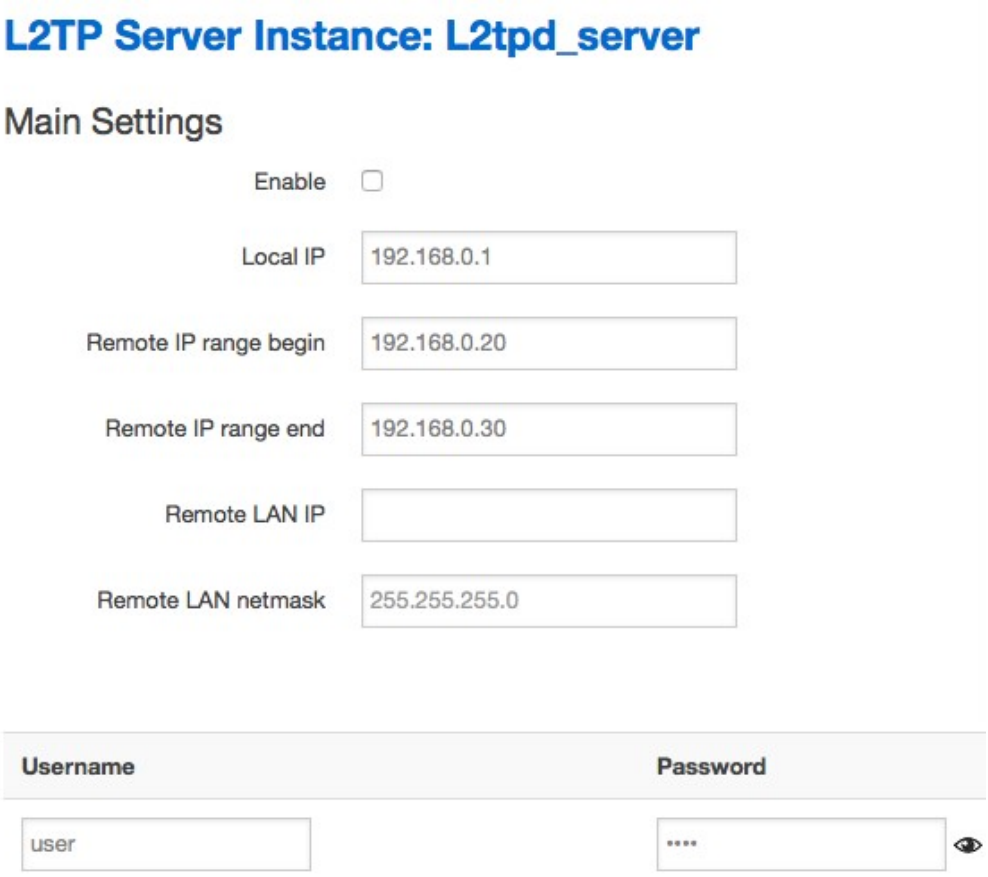


- **L2TP Client configuration**



- **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.

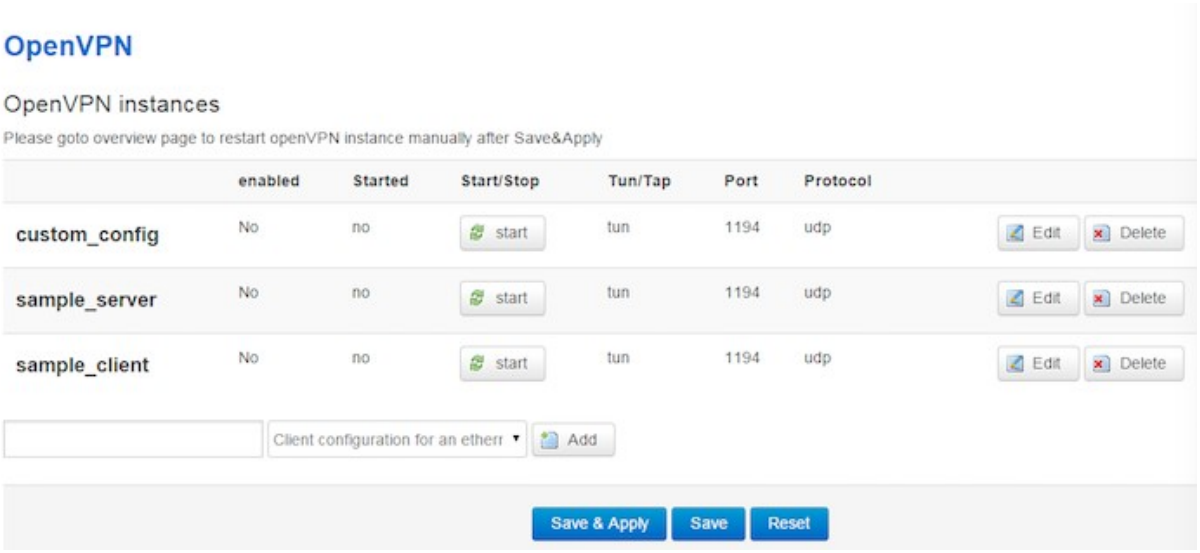
➢ **L2TP Server configuration**



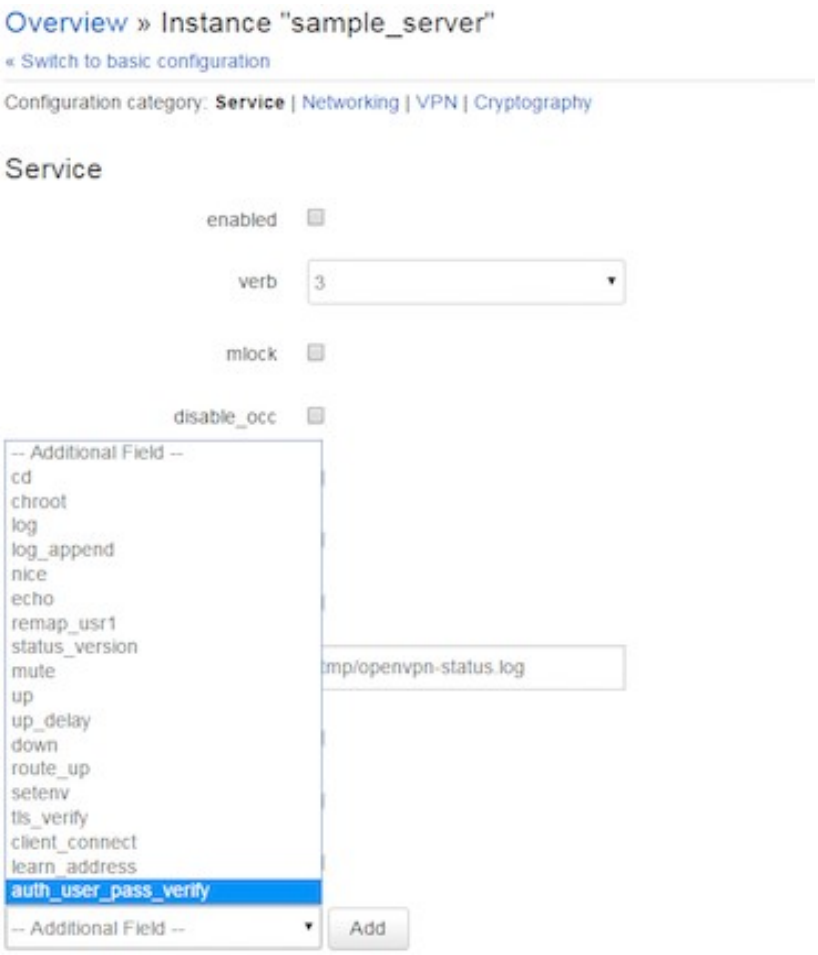
- **Local IP**: Indicates the server's IP address.
- **Remote IP range begin**: The remote IP address lease start.
- **Remote IP range end**: The remote IP address lease end.
- **Remote LAN IP**: L2TP client IP.
- **Remote LAN netmask**: The mask of L2TP client IP, the default value is 255.255.255.0
- **Username**: Server authentication username.
- **Password**: Server authentication password.

3.5.8.4 OpenVPN

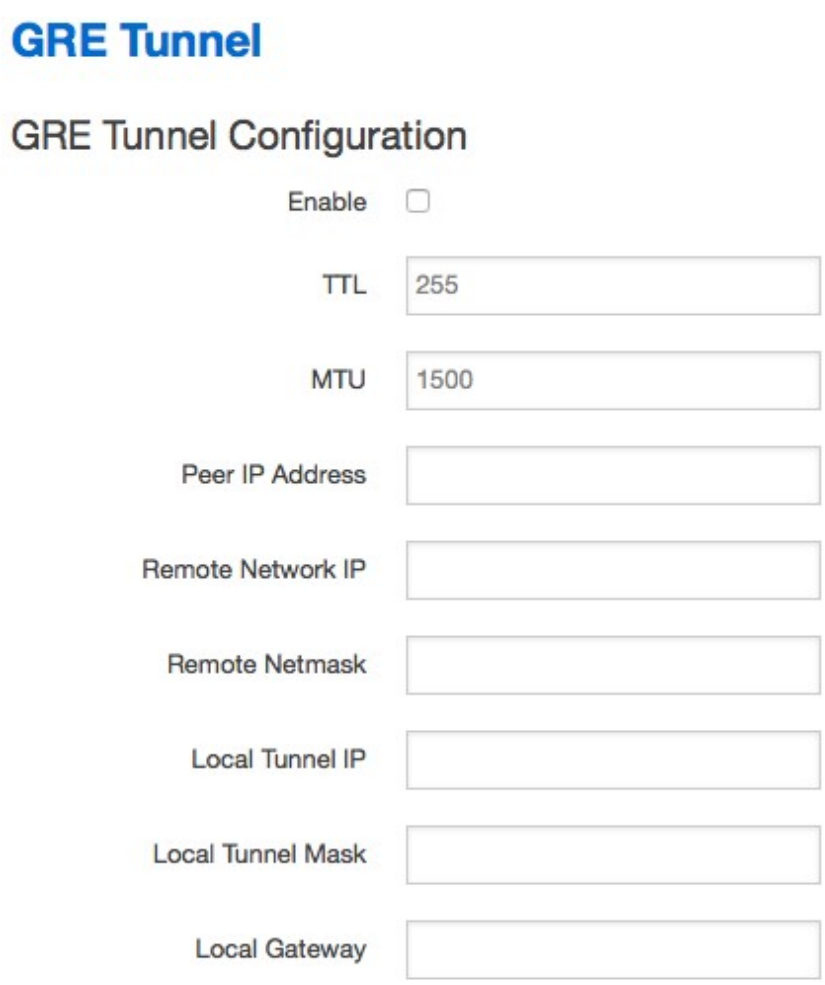
This page is a list of configured OpenVPN instances and their state. Click the button "Edit" to make changes to an instance, or click the button "Delete" to delete it. Click the button "Start" or "Stop" to start or stop a specific instance.



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.



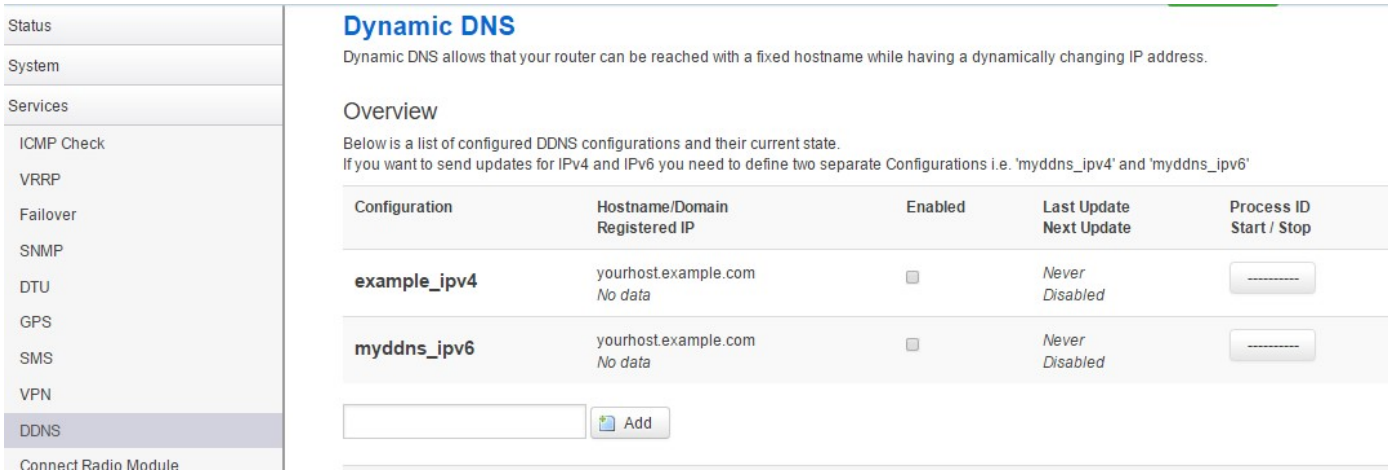
3.5.8.5 GRE tunnel

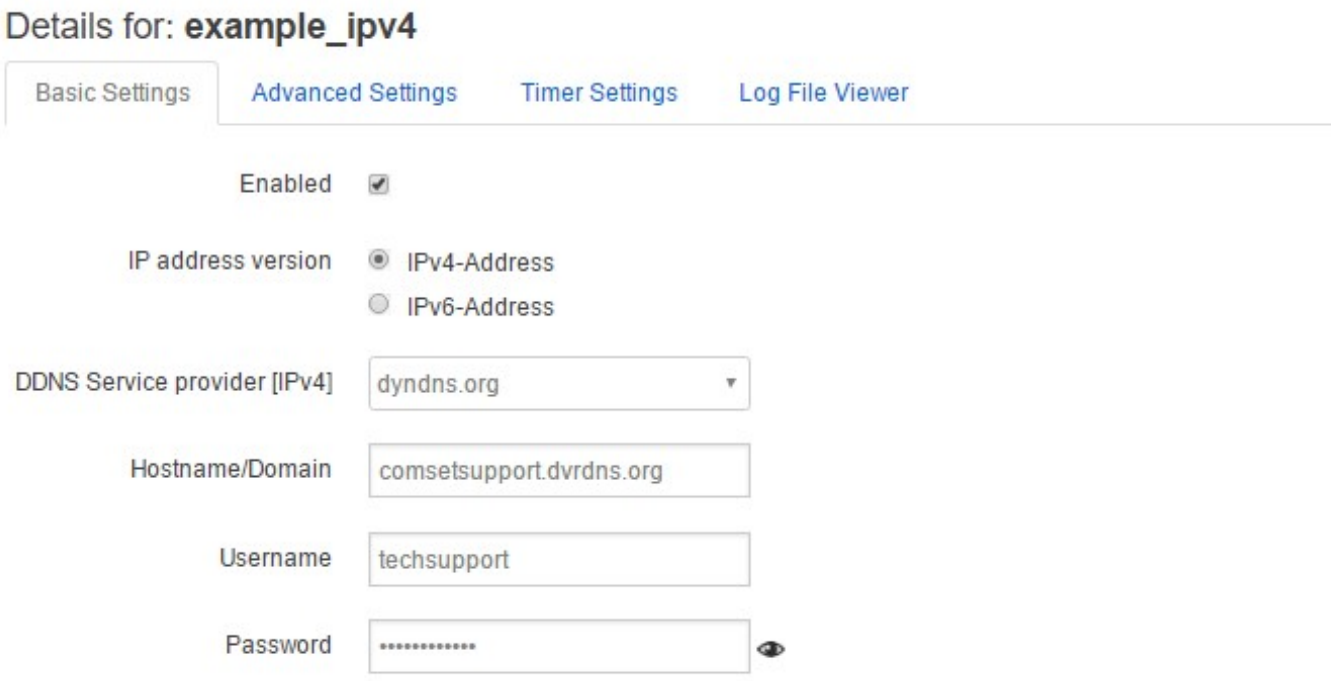


- **Enable**: Enable GRE tunnel feature.
- **TTL**: Time-to-live.
- **MTU**: Maximum Transmission Unit.
- **Peer IP address**: Remote WAN IP address.
- **Remote Network IP**: Remote LAN subnet address.
- **Remote Netmask**: Remote LAN subnet mask.
- **Local Tunnel IP**: Virtual IP address. This cannot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

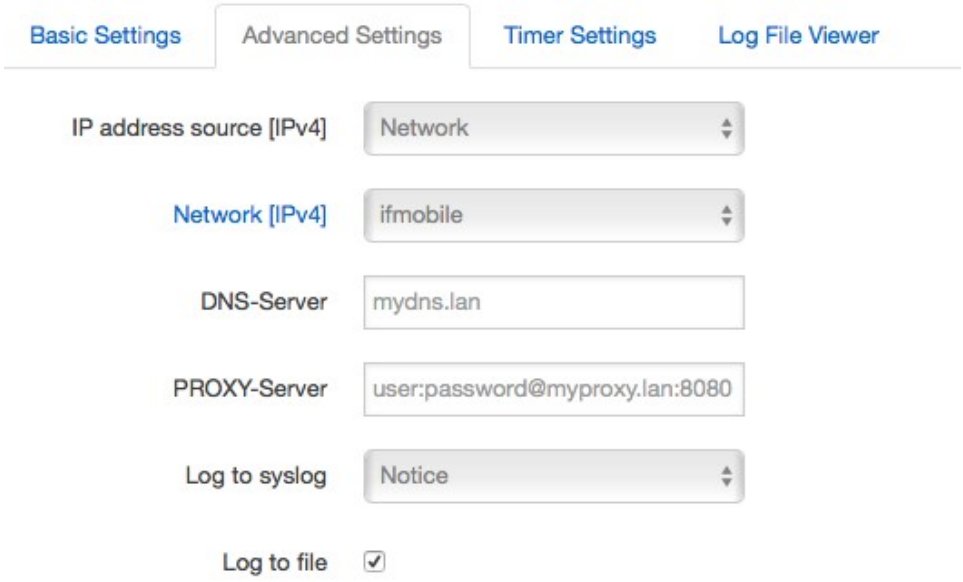
3.5.9 DDNS

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

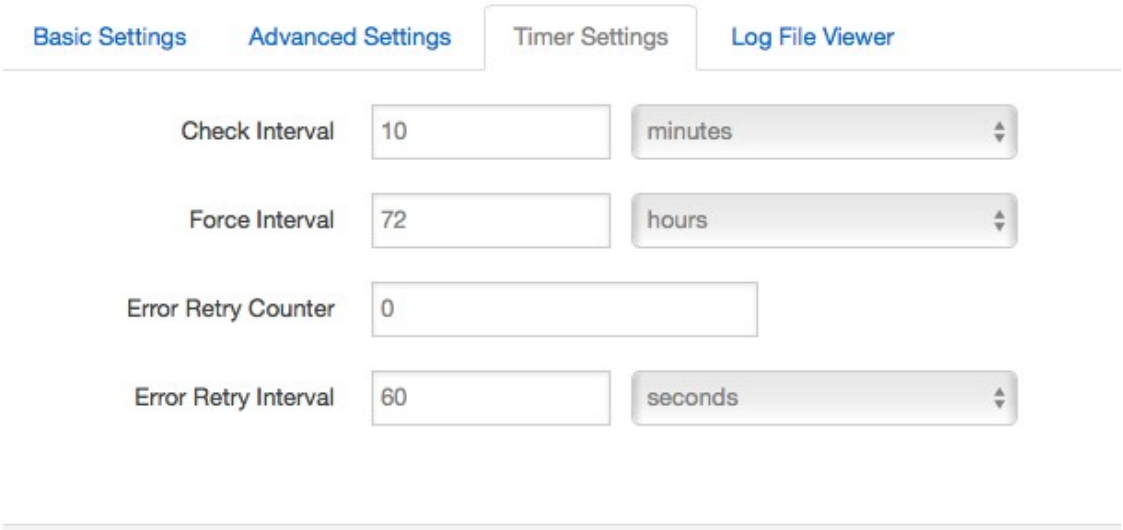




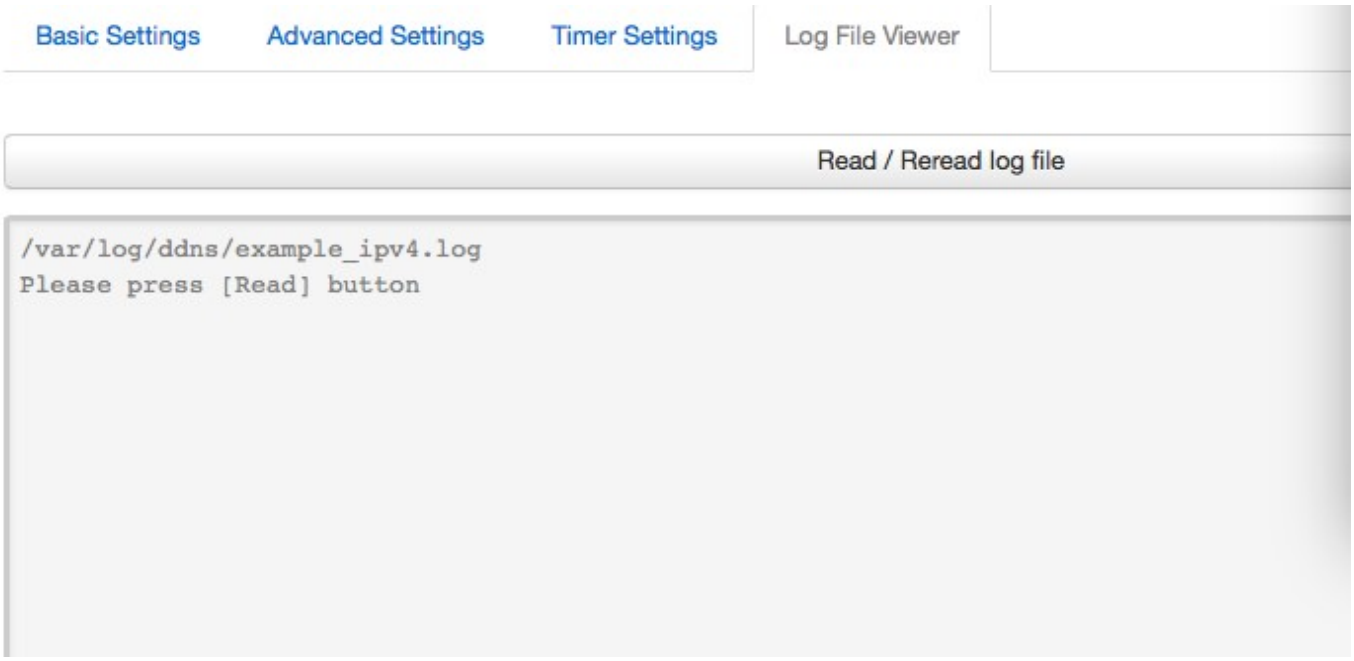
- **Enabled**: Enable this instance.
- **IP address version**: IPv4 and IPv6 supported.
- **DDNS Service provider**: Select a suitable provider.
- **Hostname/Domain**: The Domain name to remotely access the router.



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

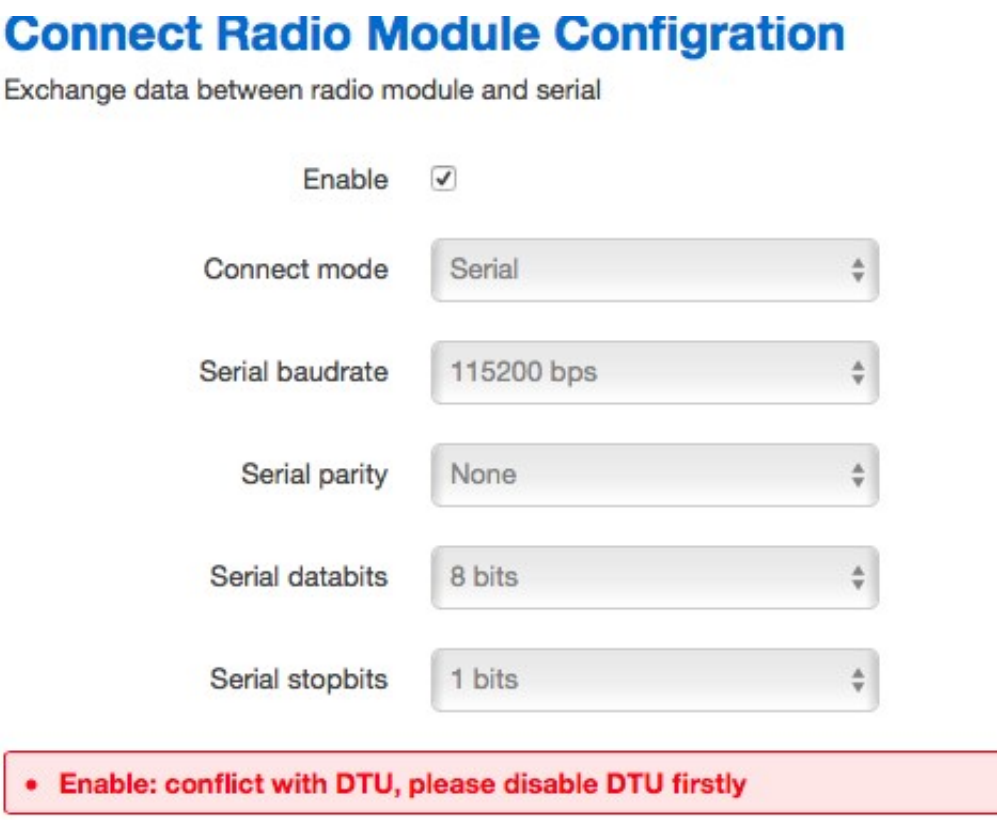


Read the log file of DDNS.

3.5.10 Connect Radio Module

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

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



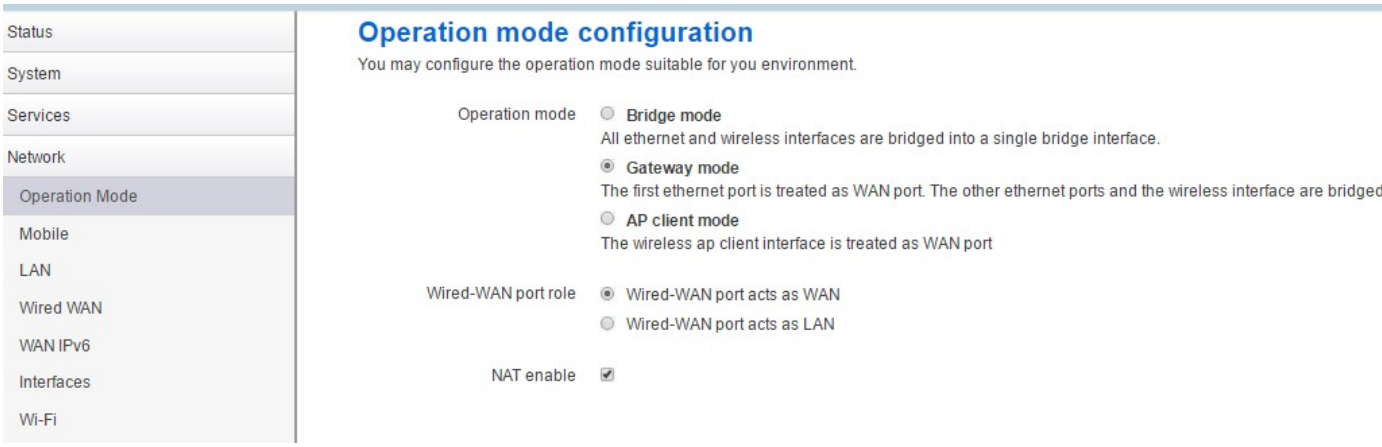
- **Connect Mode:** Serial only

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

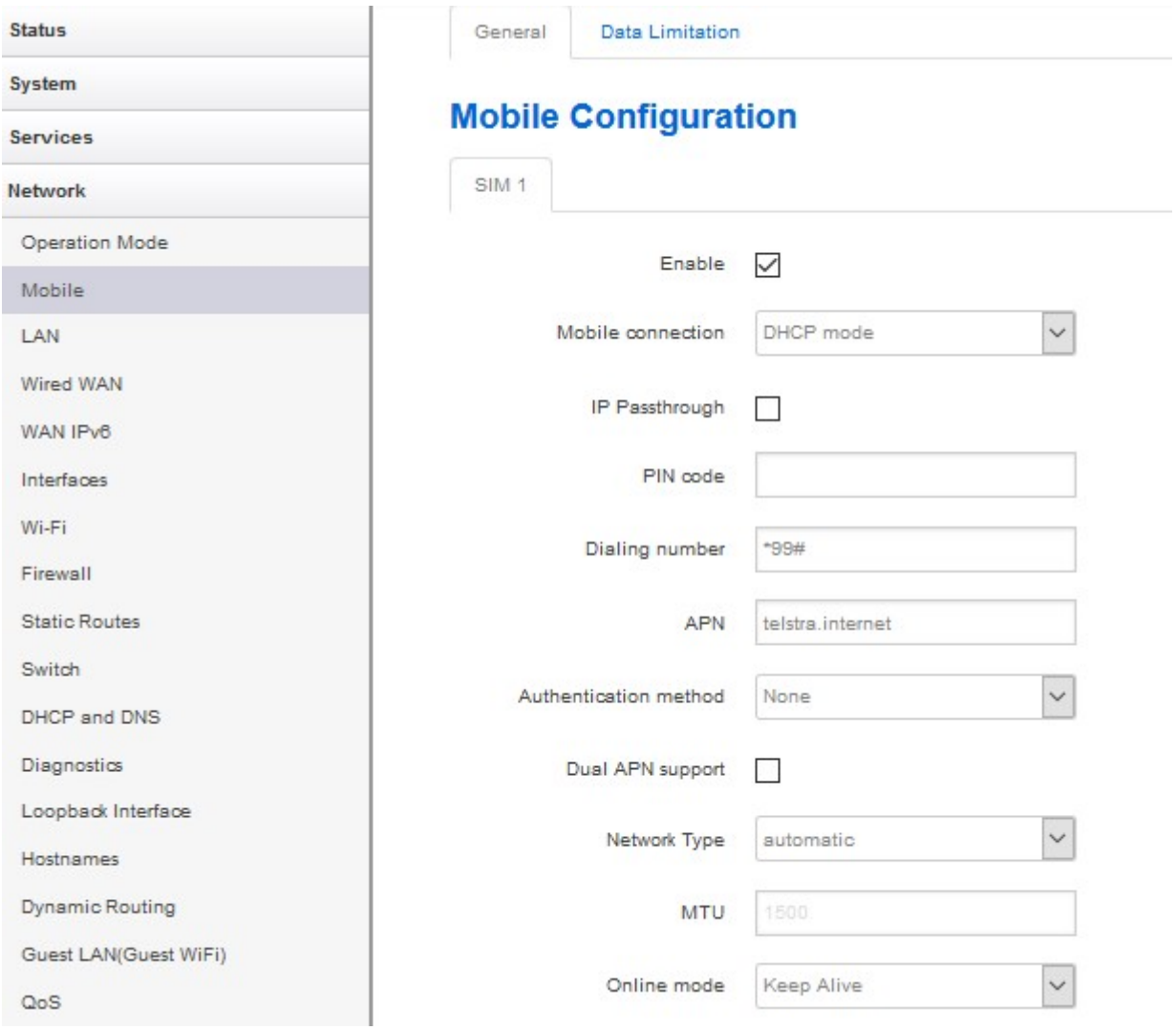


- **Operation mode**
  - **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface.
  - **Gateway:** The first Ethernet port is treated as a WAN port. The second Ethernet port and the wireless interface are bridged together and are treated as LAN ports.
  - **AP Client:**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

The default operation is in “Gateway mode”.

3.6.2 Mobile configuration

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



- **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.
- **Online Mode**

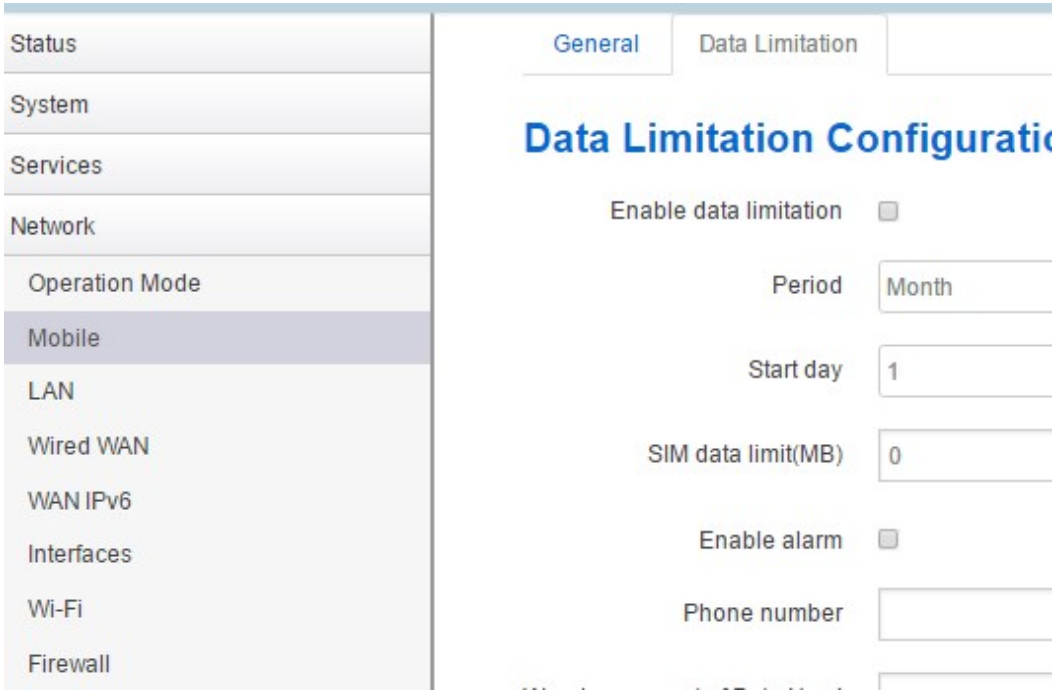
  Keep Alive: Means always online. The router will keep online whether there is data for transmission or not.

  On Demand: The router will dialup only when there is data for transmission.

  Idle time (minutes): Fill in the time. For example, if you fill in 5, the router will go offline after 5 minutes if there is no data for transmission.

  Scheduled: The router will dialup or go offline depending on the schedule.

3.6.3 Cell mobile data limitation

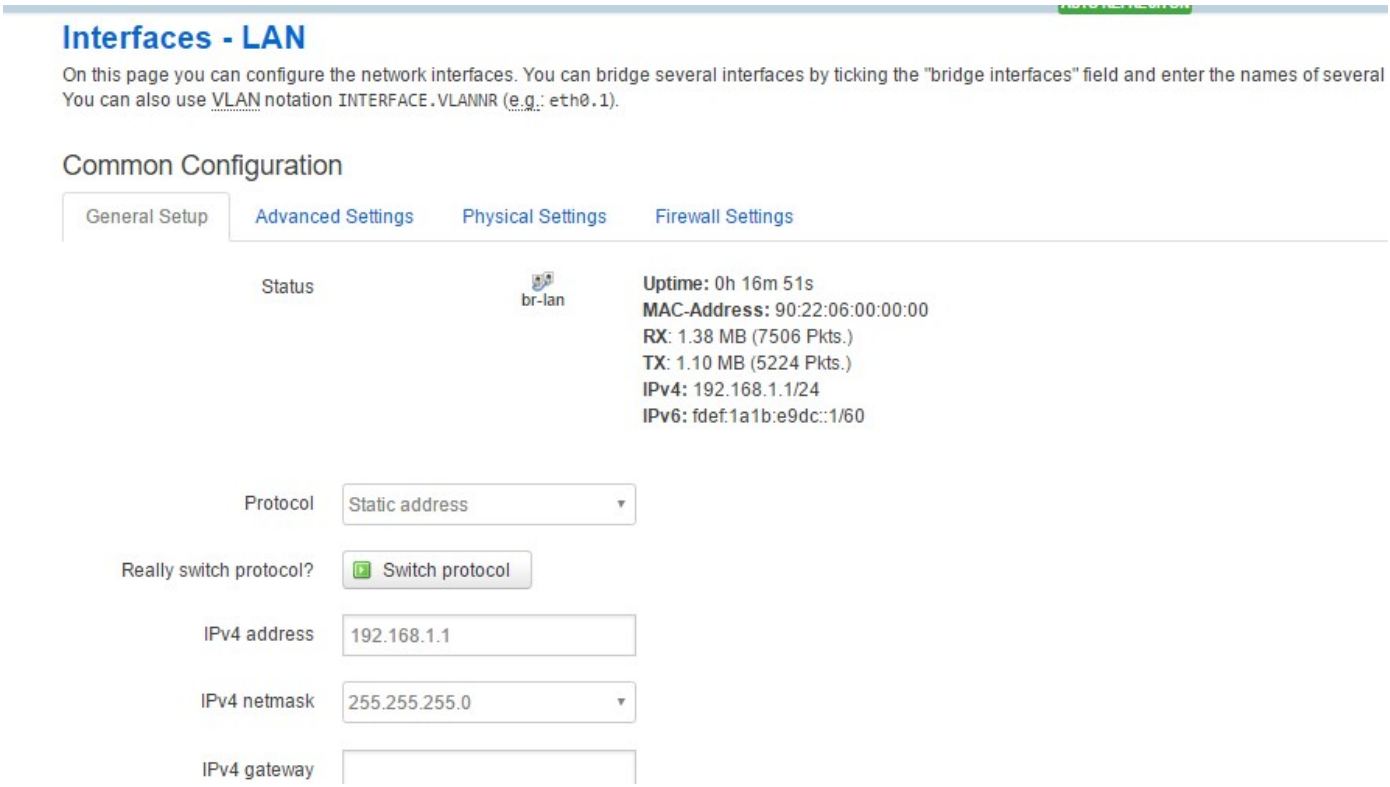


- **Enable data limitation**:
- **Period**: Month, Week or Day.
- **Start day**: The first day of the period.
- **SIM data limit (MB)**: The maximum data that can be used during this period. If it is exceeded,

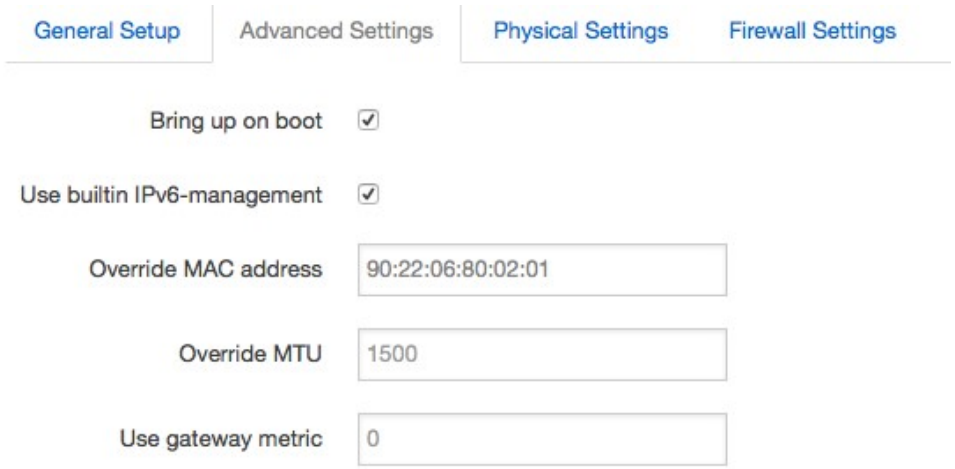
the router will terminate the cell mobile connection.

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

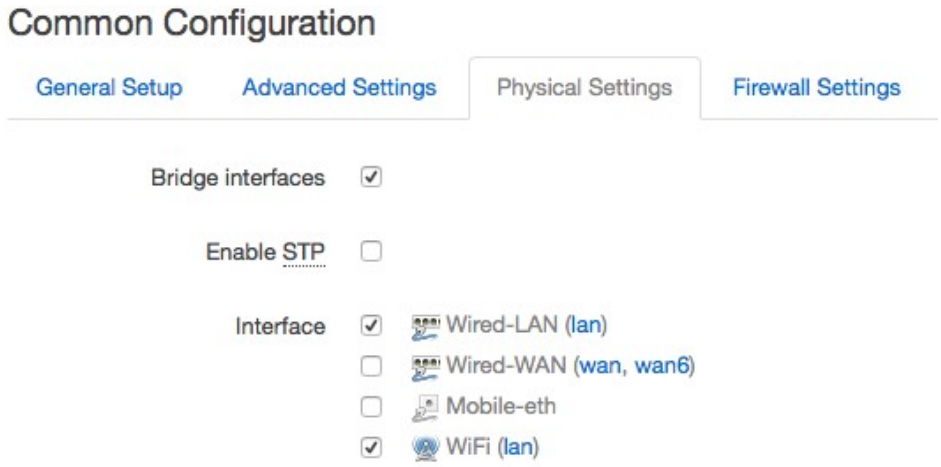
3.6.4 LAN settings



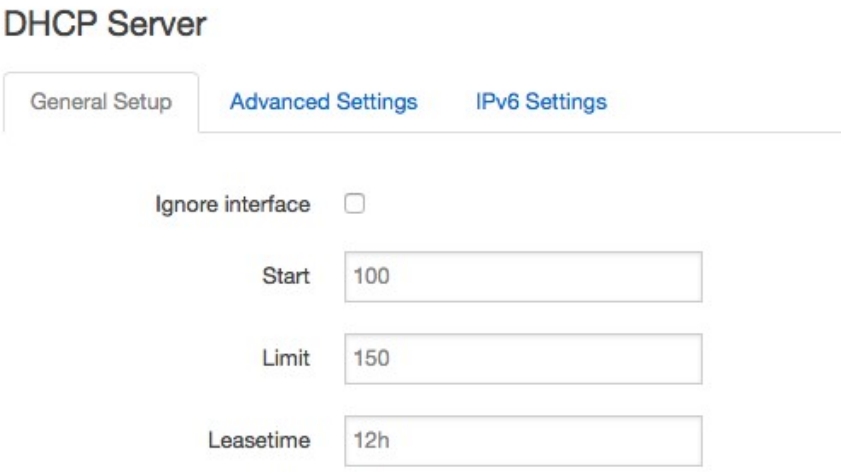
- **Protocol**: Only static address is supported for LAN.
- **Use custom DNS servers**: Multiple DNS servers are supported.
- **IPv6 assignment length**: Assign a part of given length of every public IPv6-prefix to LAN interface.
- **IPv6 assignment hint**: Assign prefix parts using this hexadecimal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



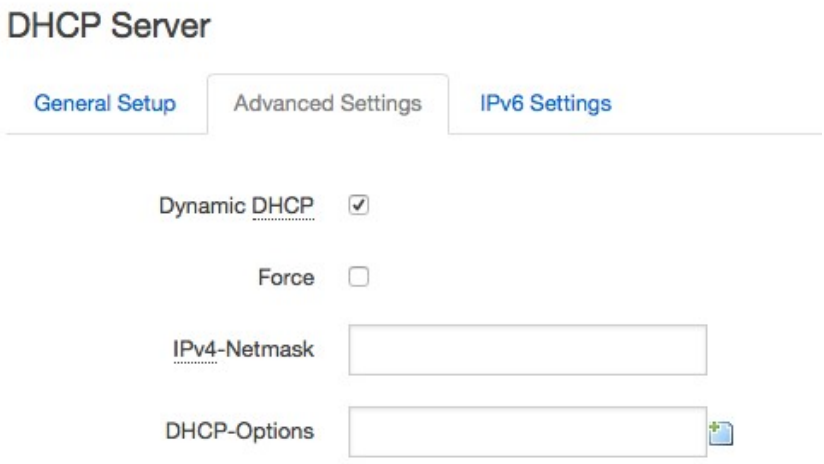
- **Bring up on boot**: If checked, the LAN interface will be set to ‘up’ upon system boot-up. If unchecked, the LAN interface will be ‘down’. Don’t uncheck it if not required.
- **Use built-in IPv6-management**: The default is checked. If IPv6 is not needed, it can be unchecked.
- **Override MAC address**: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



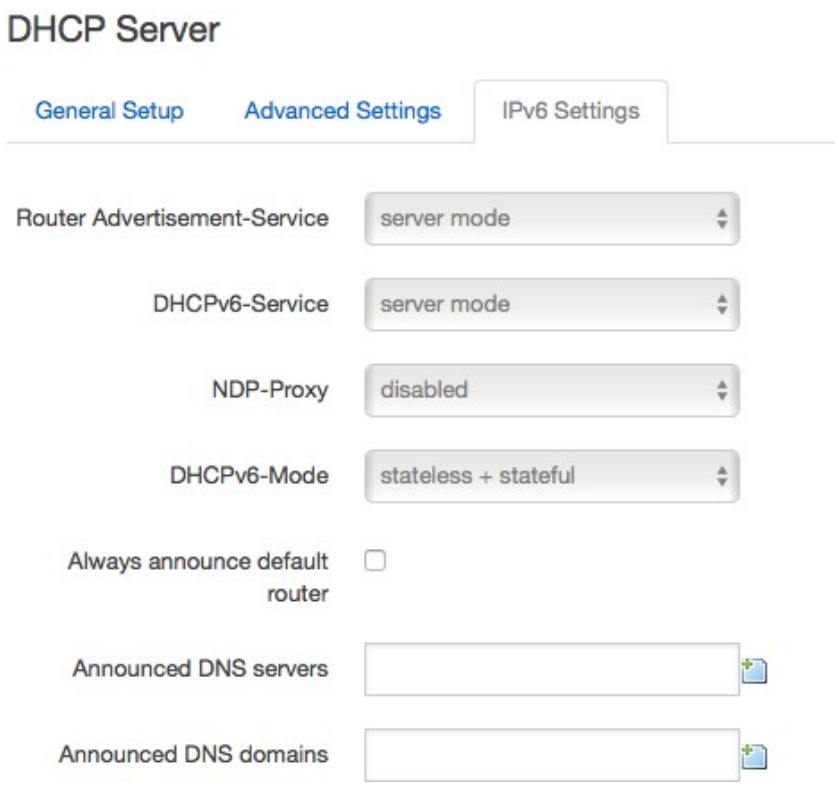
- **Bridge interfaces**: LAN bridges wired-LAN and WiFi in the same LAN subnet.
- **Enable STP**: Enable Spanning Tree Protocol on LAN. The default value is unchecked.



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

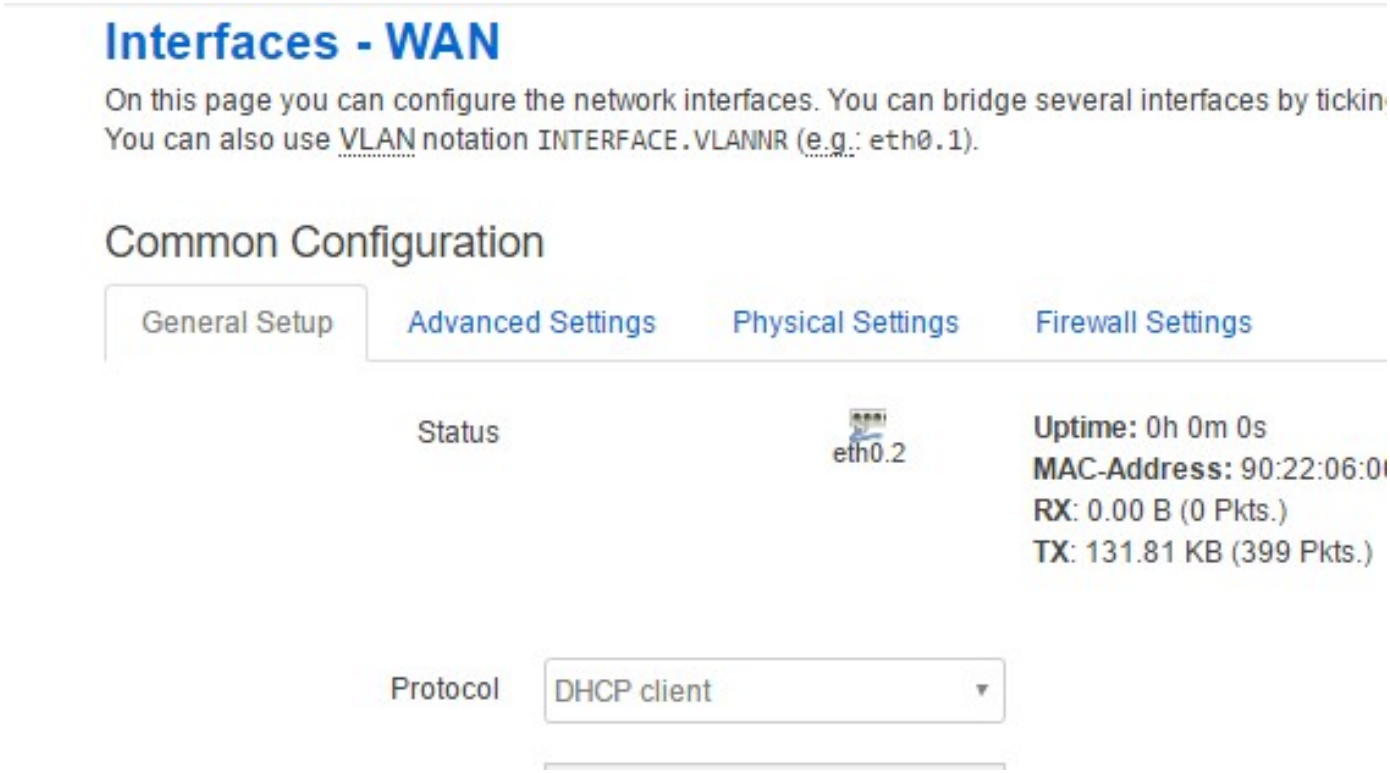


- **Dynamic DHCP**: Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
- **Force**: Force DHCP on this network even if another server is detected.
- **IPv4-Netmask**: Override the netmask sent to clients. Normally it is calculated from the 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.)



- **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



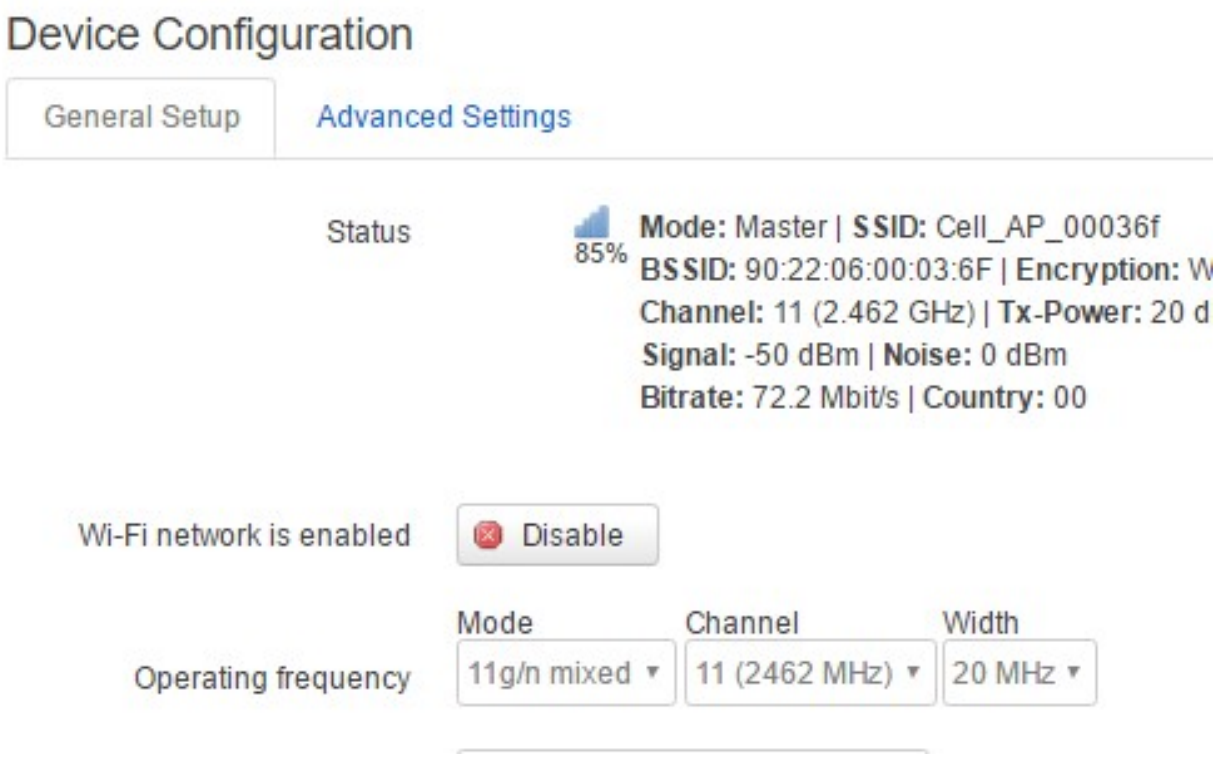
- **Protocol**: The default protocol is DHCP client. If you need to change it to a different protocol (i.e. PPPoE), select the protocol from the drop-down menu, then click the button “Switch protocol”.

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

3.6.6 WiFi Settings

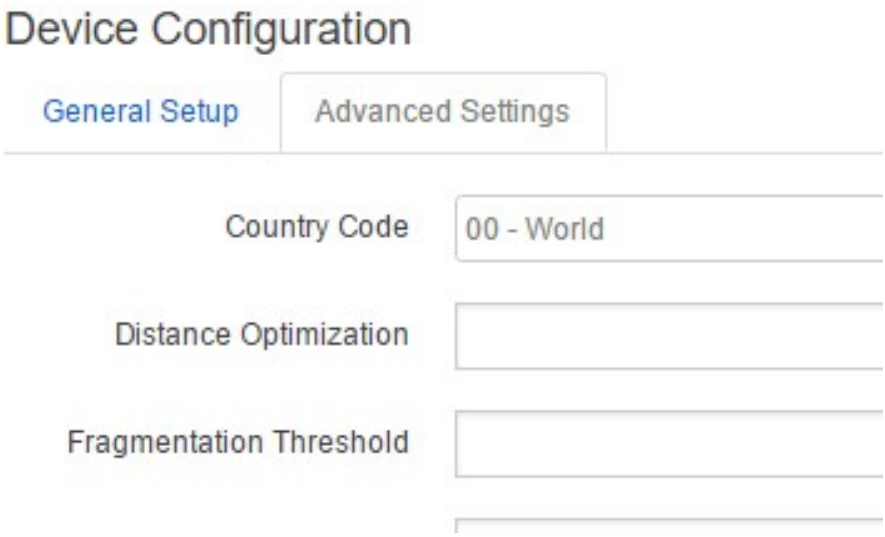
- **Wifi Restart**: turn WiFi off then on.
- **AP Client**: Scan all frequencies to get the WiFi network information.
- **Add**: Add a new wireless network.
- **Disable**: Disable a wireless network.
- **Edit**: Modify settings of the wireless network.
- **Remove**: Delete a wireless network.
- **Associated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

3.6.6.1 Wifi General configuration



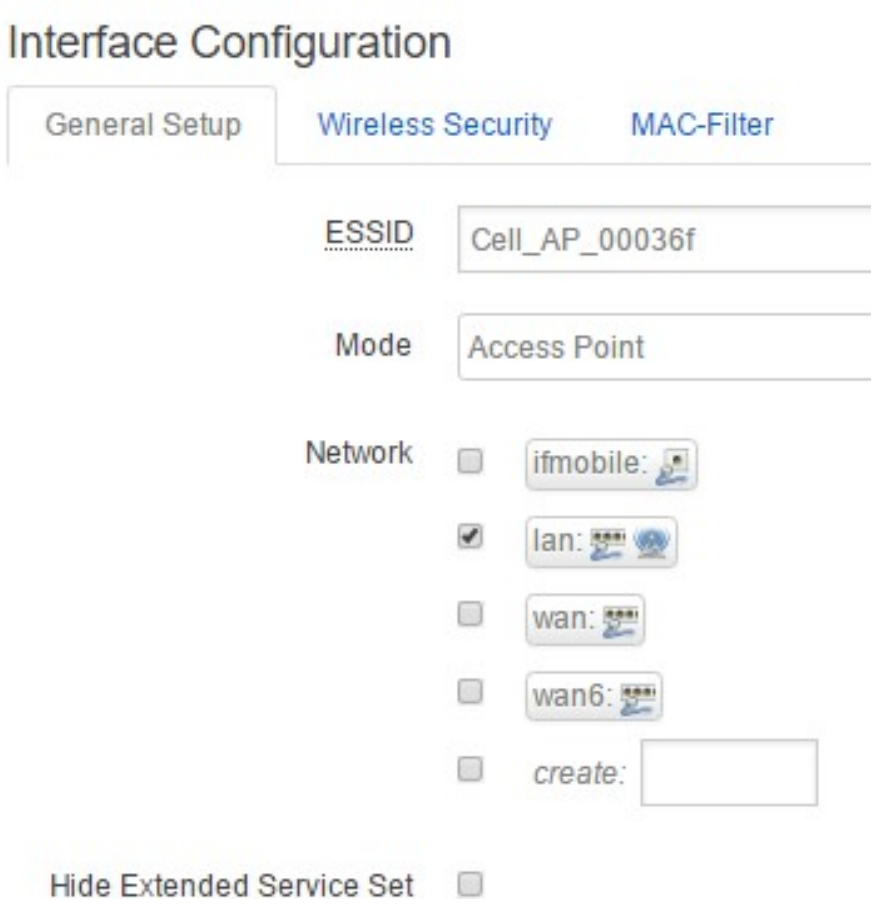
- **Status**: Shows the WiFi signal strength, mode, SSID.
- **Operating frequency Mode**: Supports 802.11b/g/n. the Legacy means 802.11b/g. “N” means 802.11n.
- **Channel**: Channel 1-11.
- **Width**: 20MHz and 40MHz.
- **Transmit Power**: From 0dBm to 20dBm.

3.6.6.2 WiFi Advanced Configuration

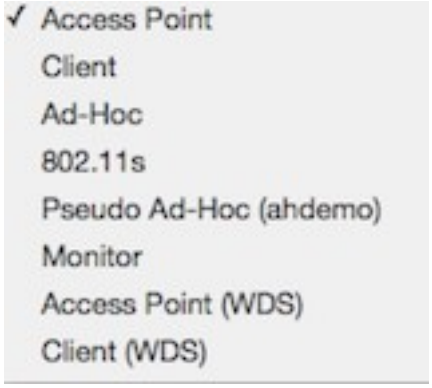


- **Country Code:** Use ISO/IEC 3166 alpha2 country codes.
- **Distance Optimization:** Distance to furthest network member in meters**.**
- **Fragmentation Threshold**
- **RTS/CTS Threshold**

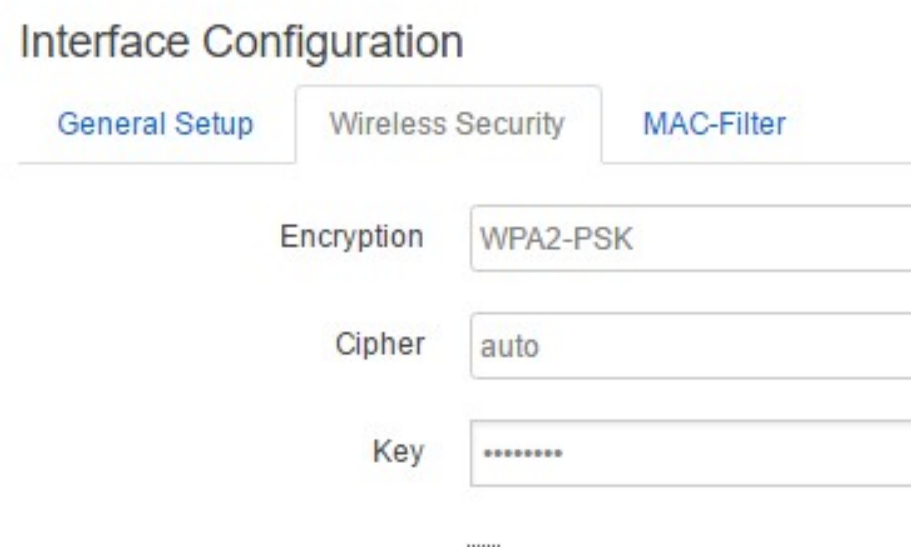
3.6.6.3 WiFi Interface Configuration



- **ESSID**: Extended Service Set Identifier. It is the broadcast name.
- **Mode**: Supported options.



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



- **Encryption:**

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

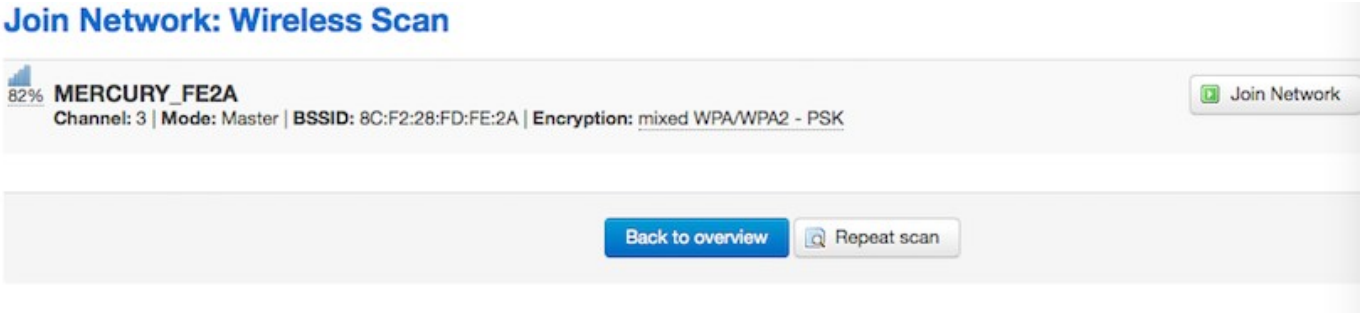
- **MAC-Address Filter**: MAC Address Access Policy. Disabled: disable MAC-address filter

functionality. Allow list: only the MAC address in the list is allowed to forward. Deny list: all packet is allowed to forward except MAC address in the list.

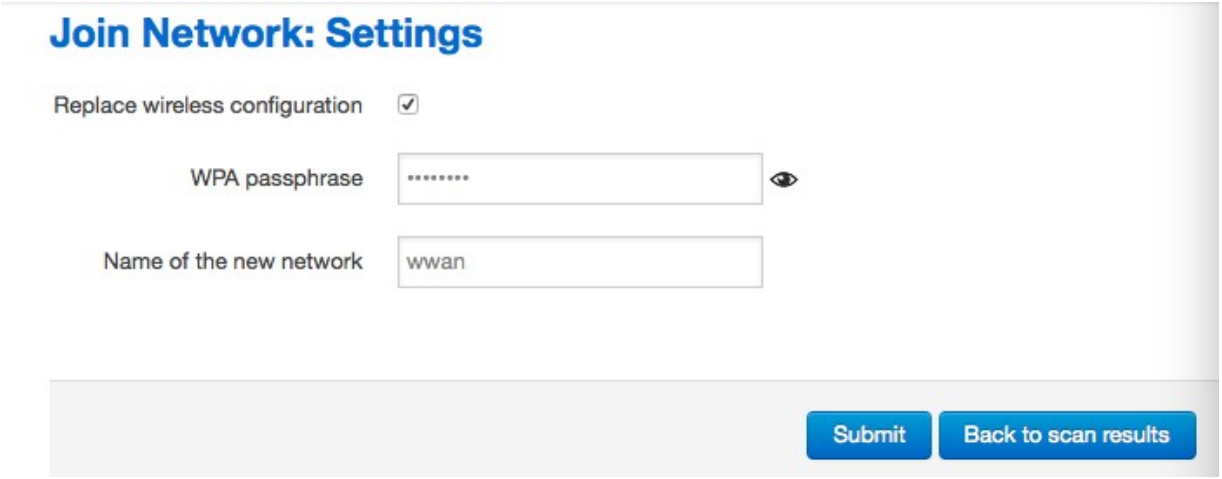
- **MAC-List**: Click button to delete a MAC address from list, click button to add a new MAC address to the list.

3.6.6.4 WiFi AP client

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



- **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.



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

Device Configuration

General Setup | Advanced Settings

Status: 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

General Setup | Wireless Security

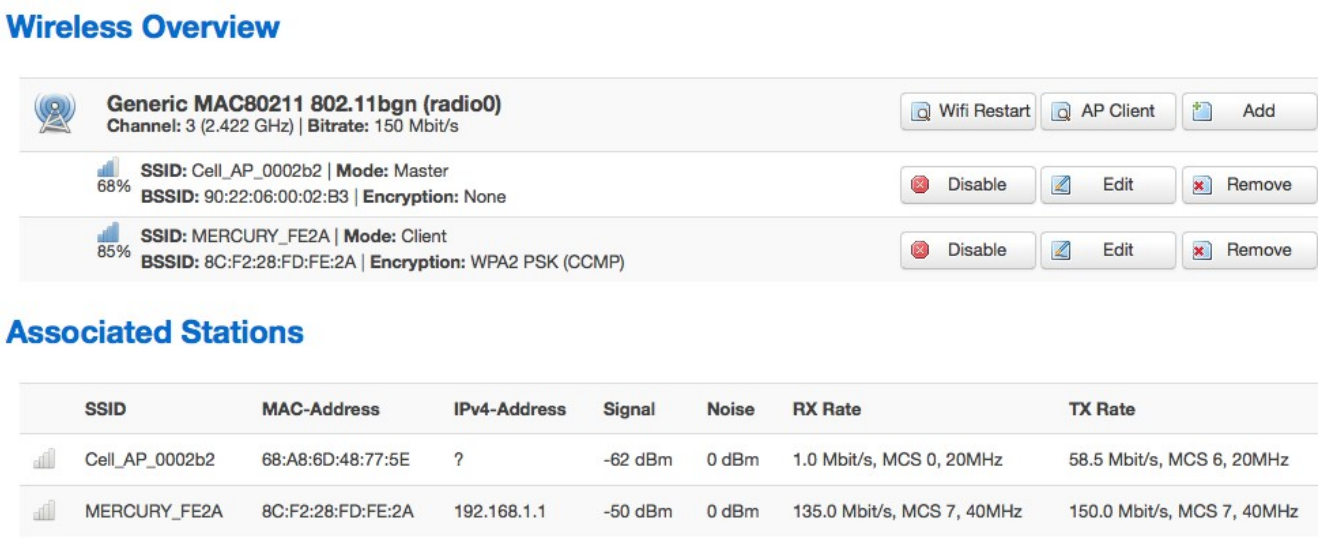
ESSID: MERCURY_FE2A

Mode: Client

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

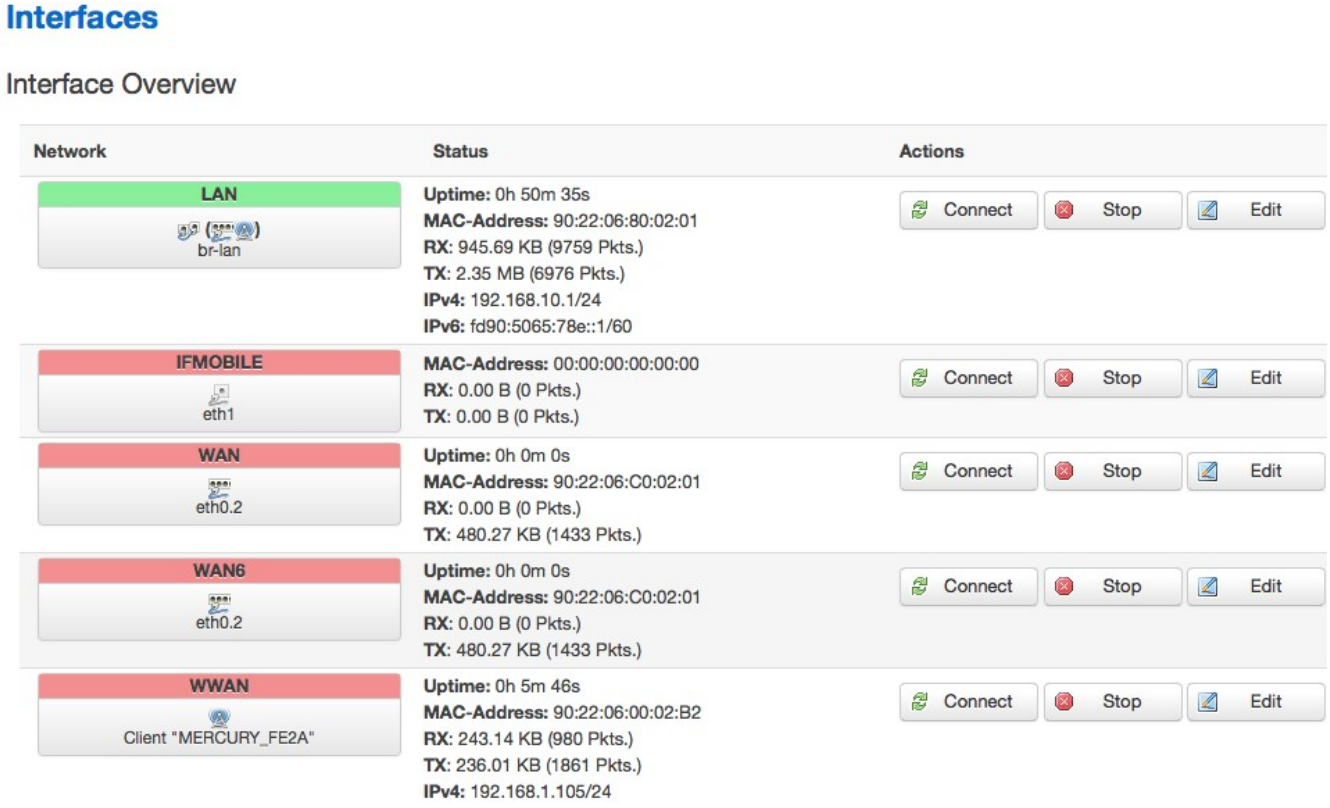
Network:
- [ ] ifmobile:
- [ ] lan:
- [ ] wan:
- [ ] wan6:
- [x] wwan:
- [ ] create:

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



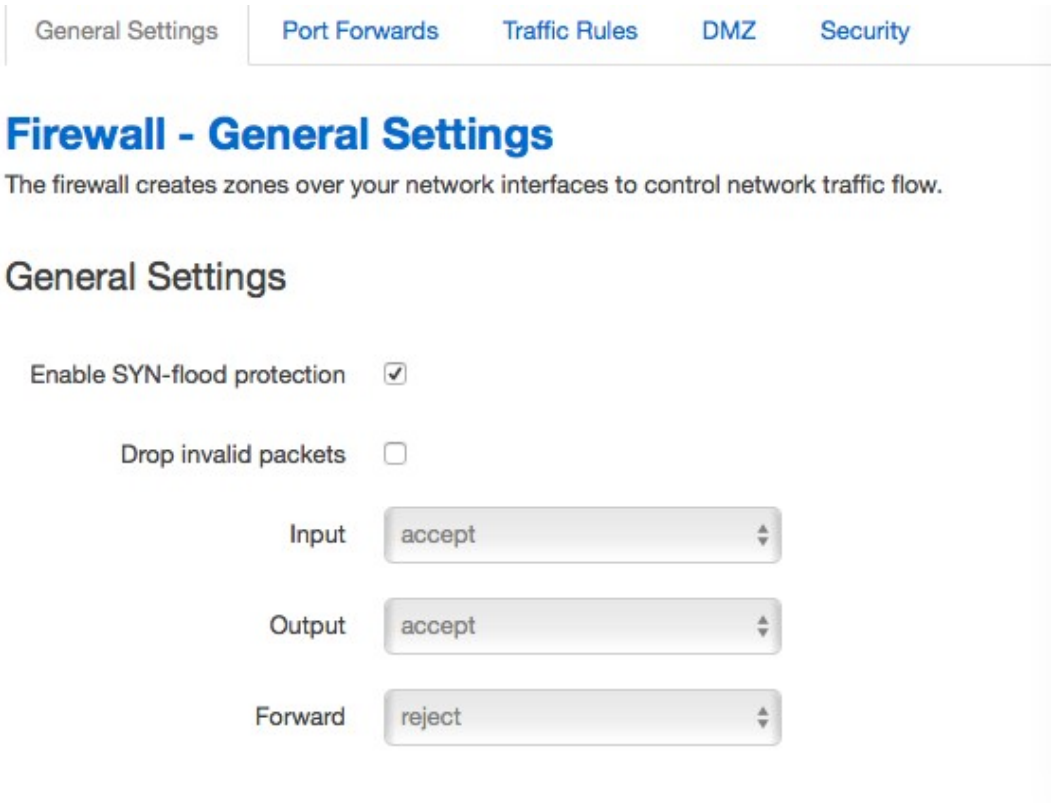
3.6.7 Interfaces Overview

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



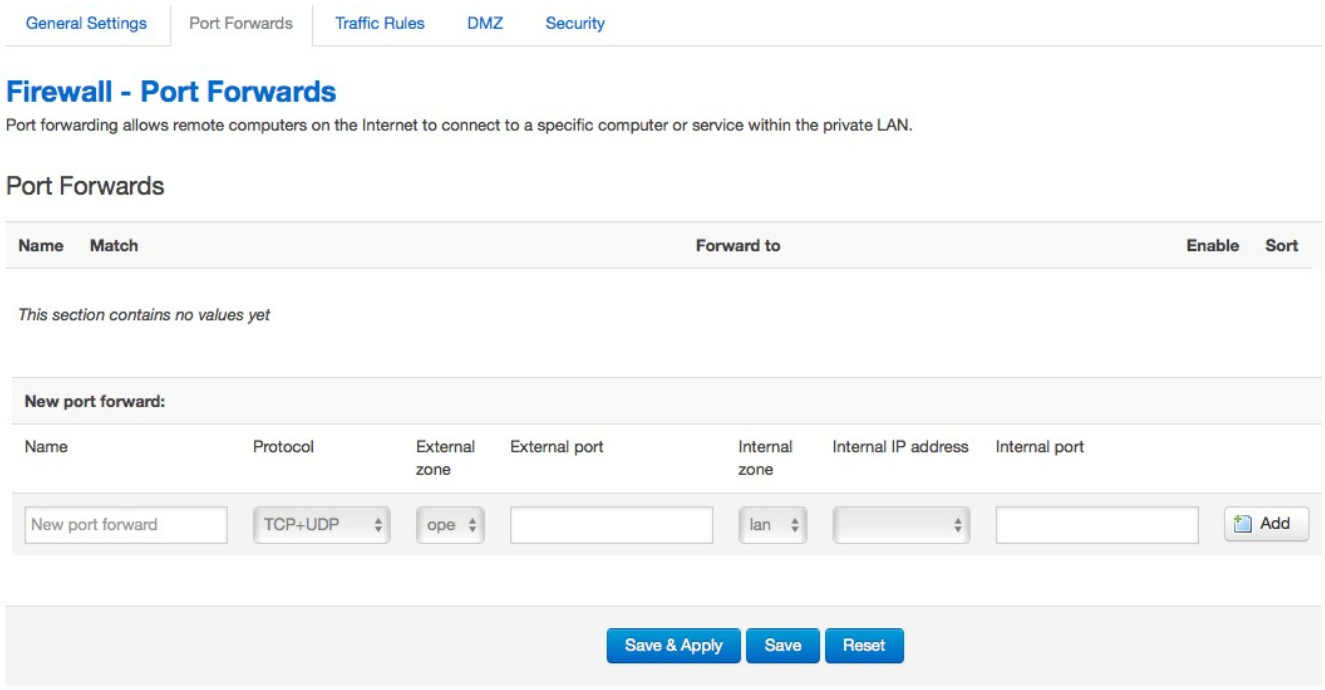
3.6.8 Firewall

3.6.8.1 General Settings



3.6.8.2 Port Forwards

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



- **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:

Traffic Rules

Name	Match	Action	Enable	Sort		
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	IPv4-ICMP with type *echo-request* From *any host* in *wan* To *any host* in *any zone*	*Accept forward*	☑	↑ ↓	Edit	Delete
Allow-IGMP	IPv4-IGMP From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
Allow-DHCPv6	IPv6-UDP From IP range *fe80::/10* in *wan* with source port *547* To IP range *fe80::/10* at port *546* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
Allow-MLD	IPv6-ICMP with types *130/0*, *131/0*, *132/0*, *143/0* From IP range *fe80::/10* in *wan* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
Allow-ICMPv6-Input	IPv6-ICMP with types *echo-request*, *echo-reply*, *destination-unreachable*, *packet-too-big*, *time-exceeded*, *bad-header*, *unknown-header-type*, *router-solicitation*, *neighbour-solicitation*, *router-advertisement*, *neighbour-advertisement* From *any host* in *wan* To *any router IP* on *this device*	*Accept input* and limit to *1000* pkts. per *second*	☑	↑ ↓	Edit	Delete
Allow-ICMPv6-Forward	IPv6-ICMP with types *echo-request*, *echo-reply*, *destination-unreachable*, *packet-too-big*, *time-exceeded*, *bad-header*, *unknown-header-type* From *any host* in *wan* To *any host* in *any zone*	*Accept forward* and limit to *1000* pkts. per *second*	☑	↑ ↓	Edit	Delete

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

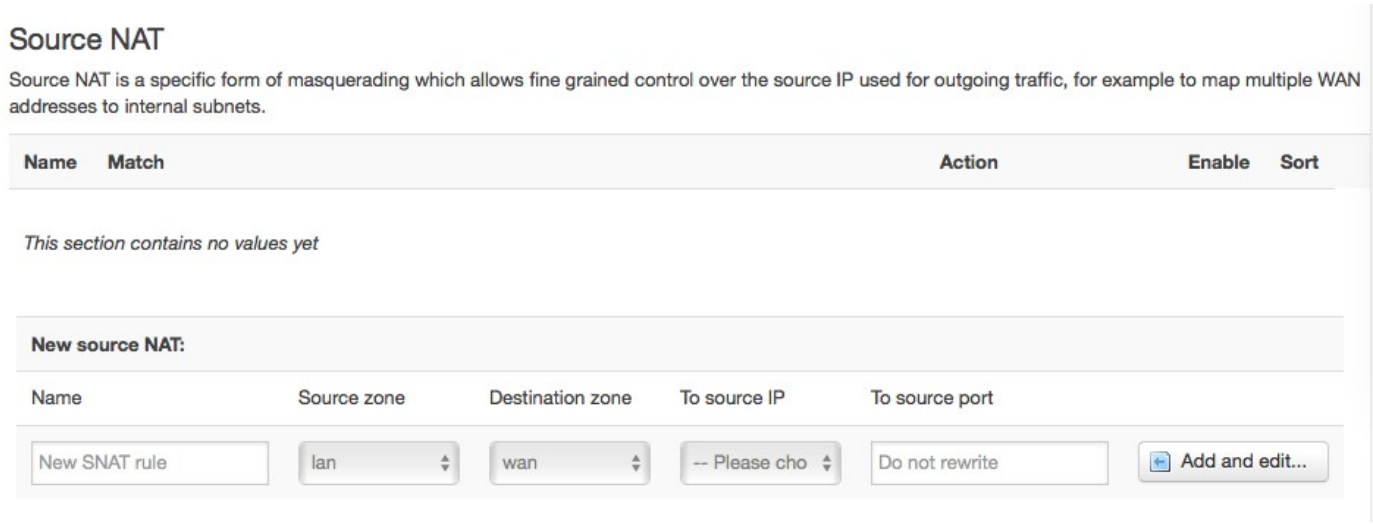
Open ports on router:

Name	Protocol	External port	
New input rule	TCP+UDP		Add

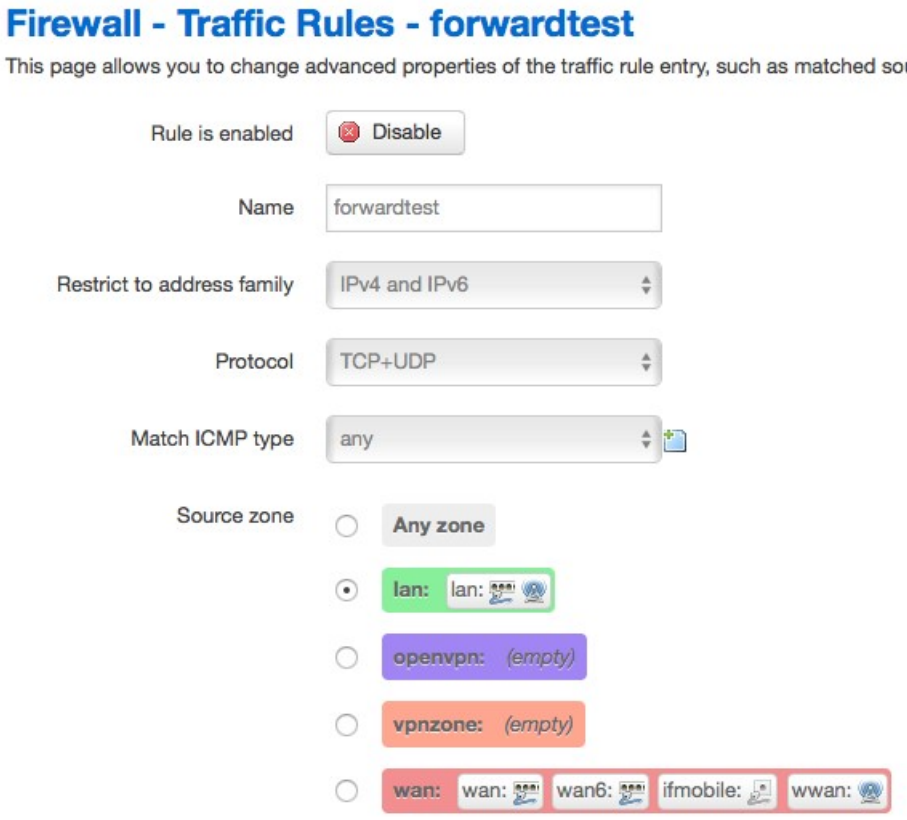
New forward rule:

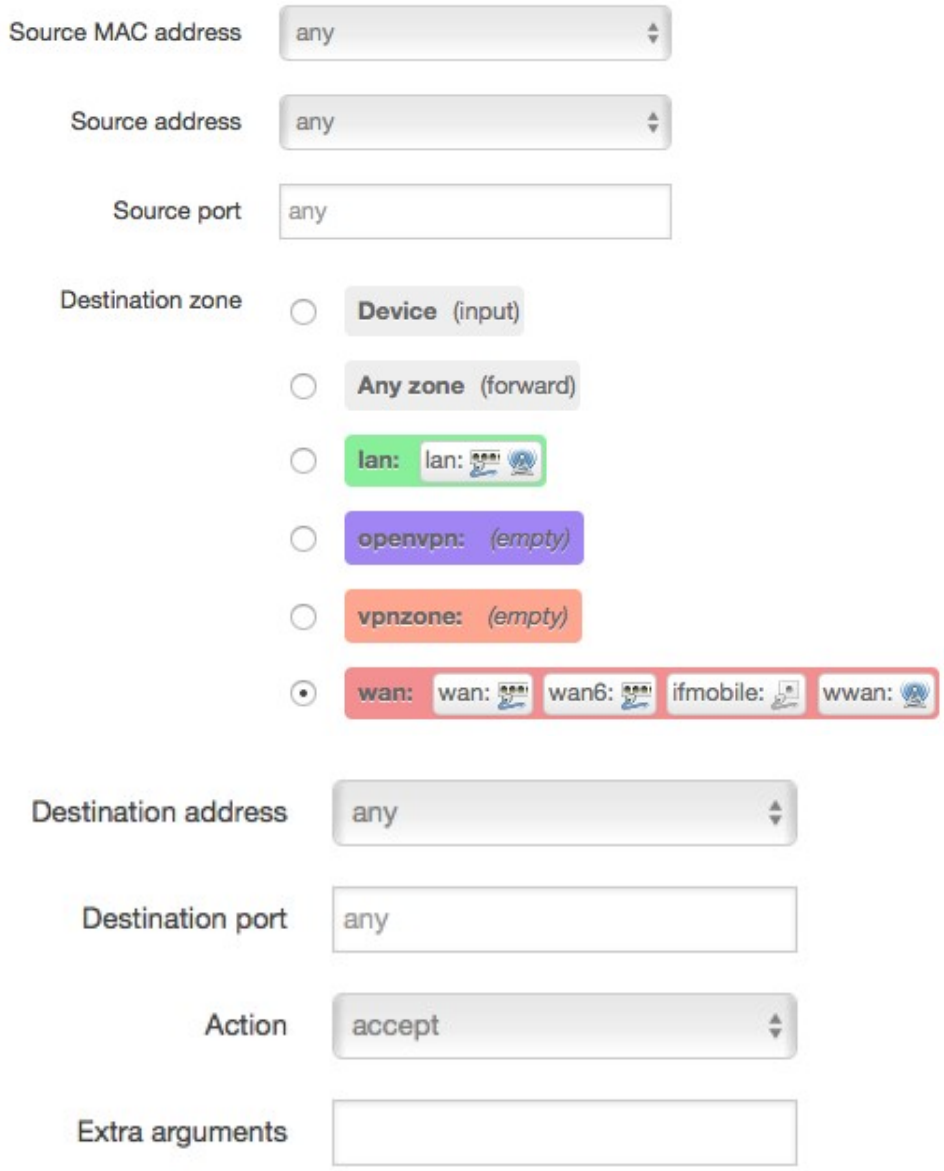
Name	Source zone	Destination zone	
New forward rule	lan	wan	Add and edit...

Source NAT list and create source NAT rule:



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

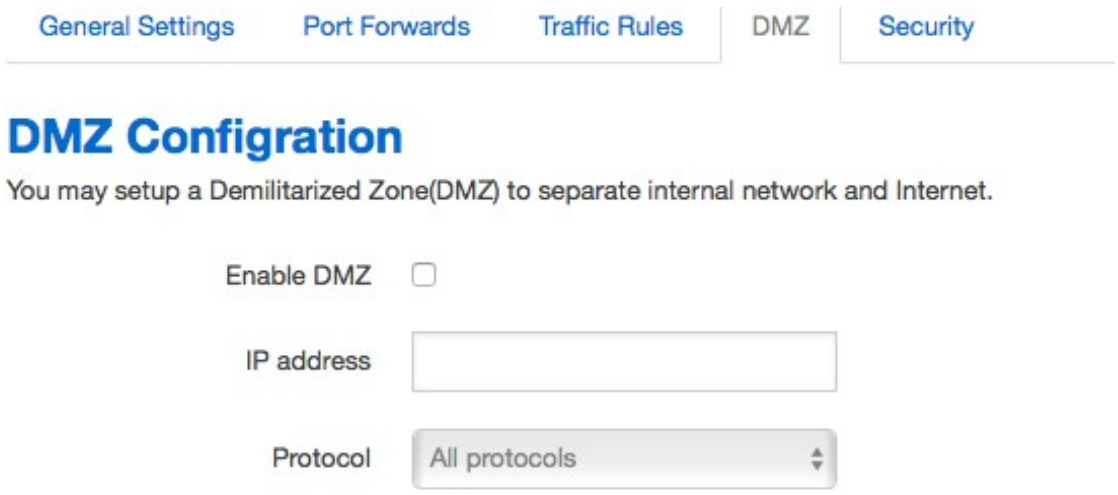




- **Name**: Traffic rule entry name.
- **Restrict to address family**: IPv4+IPv6, IPv4 and IPv6 can be selected. Specify the matched IP address family.
- **Protocol**: Specify the protocol matched in this rule. “Any” means any protocol is matched.
- **Source zone**: It is the zone that the traffic comes 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

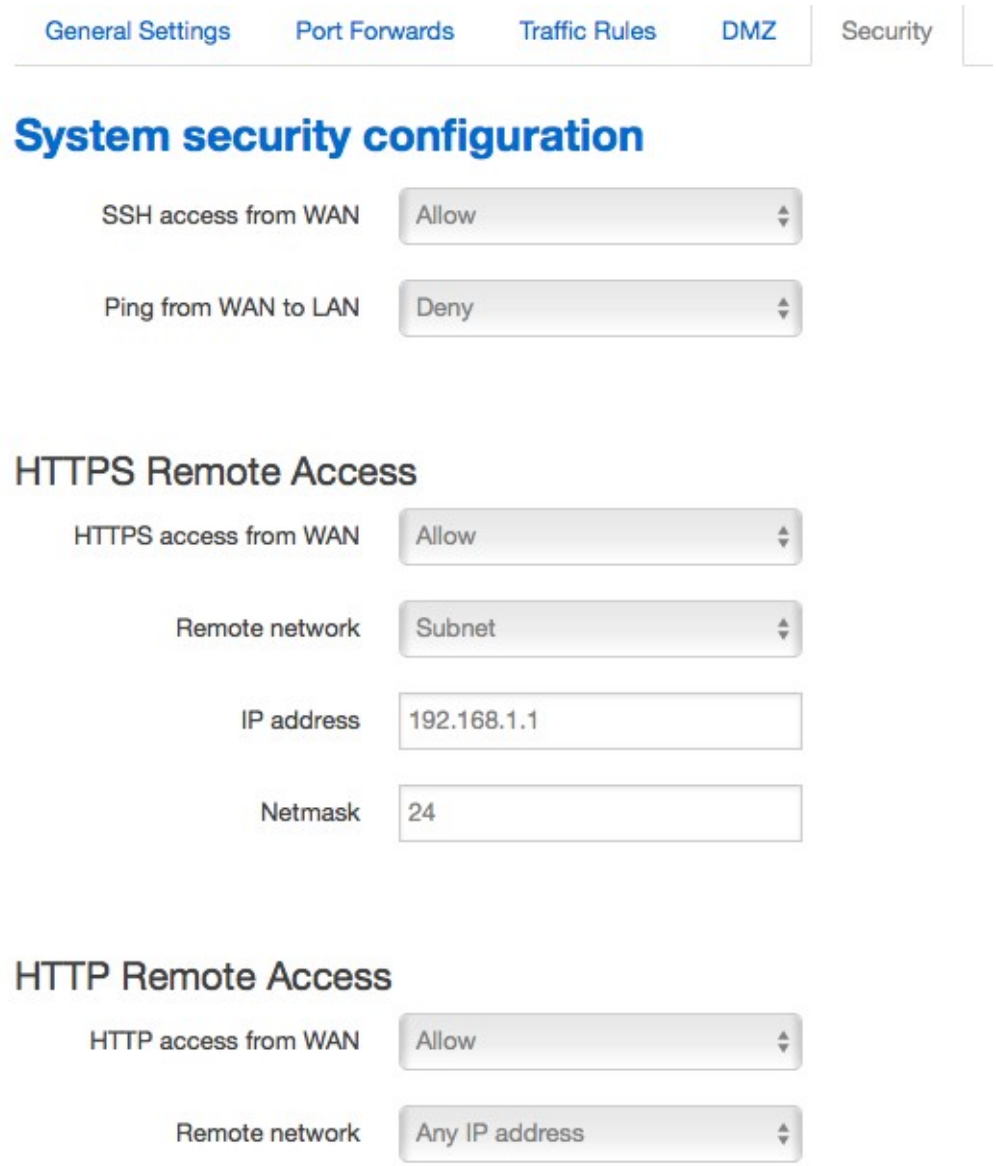


In computer networking, DMZ is a firewall configuration for securing local area networks (LANs).

- **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.

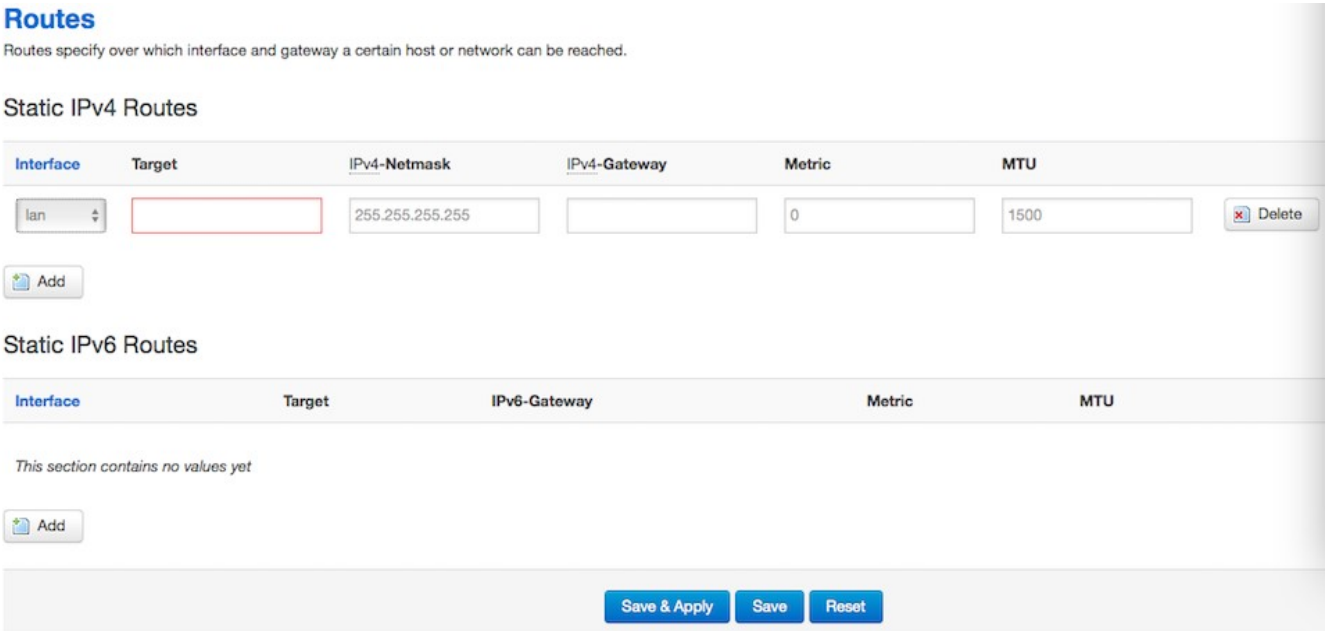
Note: When DMZ host is settled, the computer is completely exposed to the external network; the firewall will not influence this host.

3.6.8.5 Security



- **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



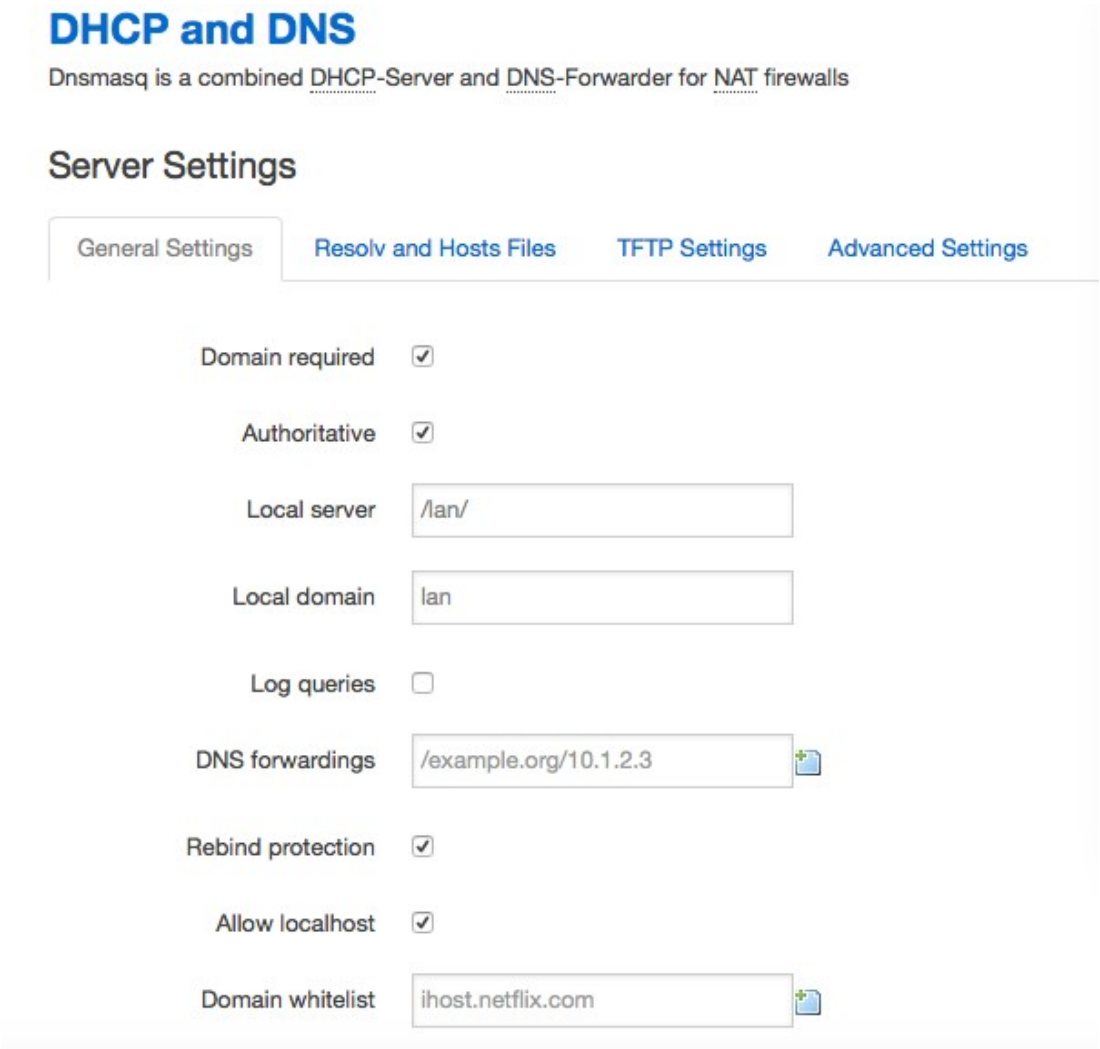
- **Interface:** You can choose the corresponding interface type.
- **Target:** The destination host IP or network.
- **Gateway:** IP address of the next router.

  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

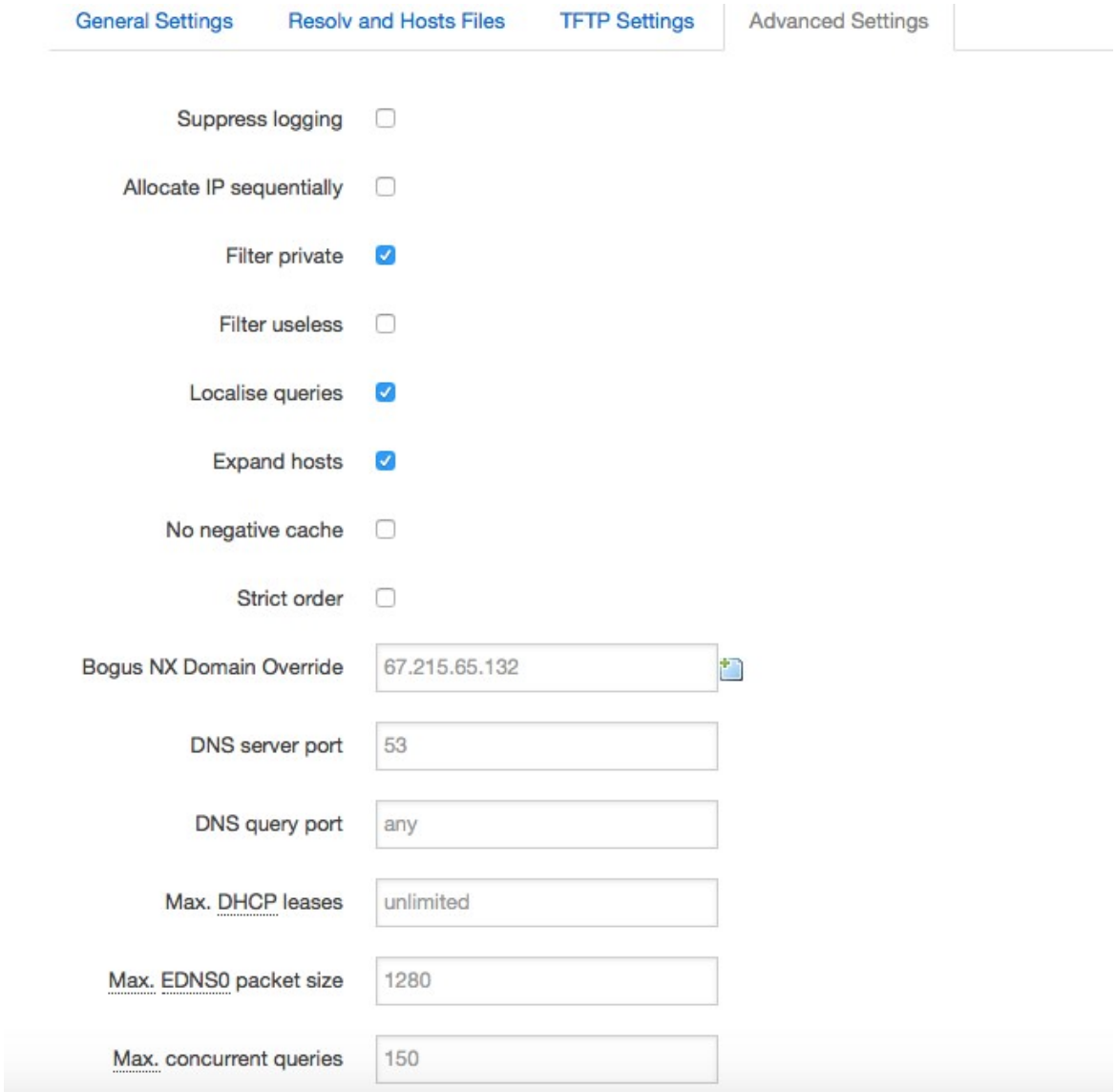
Note:
1. Port 4 is Wired-WAN port, port 0, port 1, port 2, port 3 are LAN ports.
2. “Untagged” means the Ethernet frame transmits from this port without VLAN tag.
3. “Tagged” means the Ethernet frame transmits from this port with VLAN tag.
4. “Off” means this port does not belong to VLAN. For default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

3.6.11 DHCP and DNS



- **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.



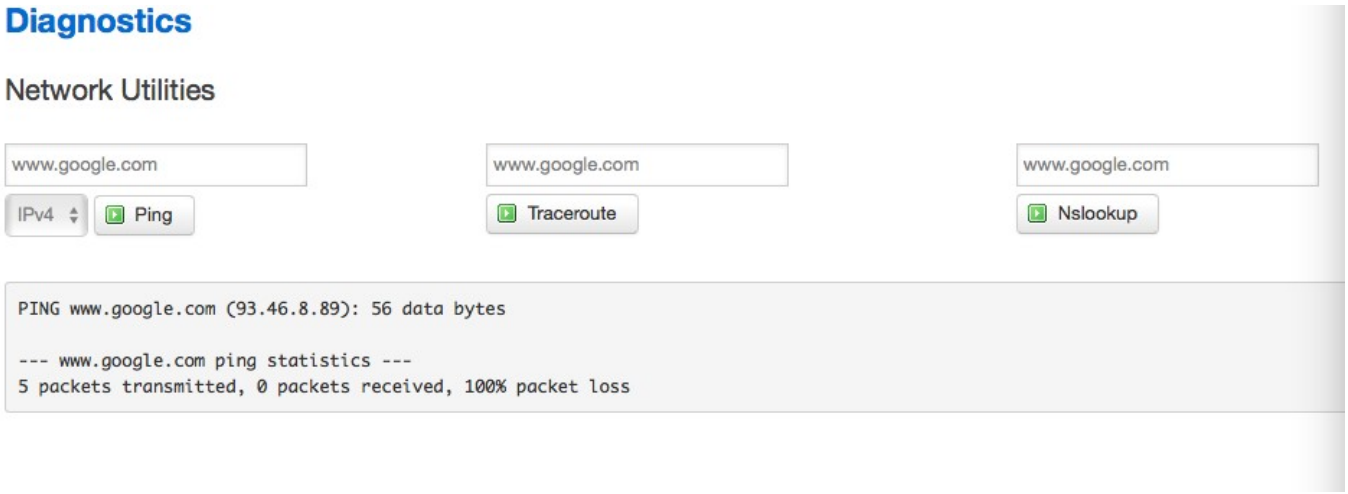
- **Suppress logging**: Suppress logging of the routine operation of these protocols.
- **Allocate IP sequentially**: Allocate IP addresses sequentially, starting from the lowest available address.
- **Filter private**: Do not forward reverse lookups for local networks.
- **Filter useless**: Do not forward 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.

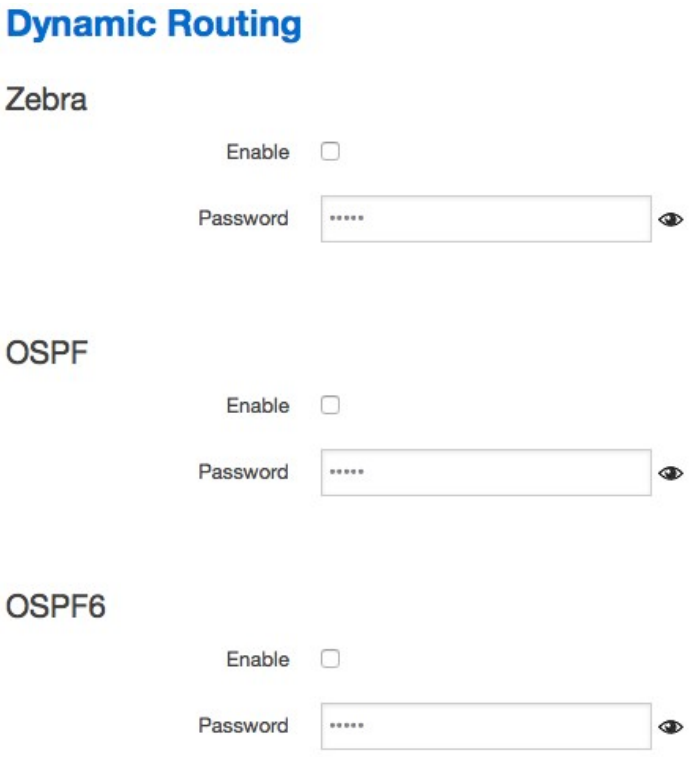


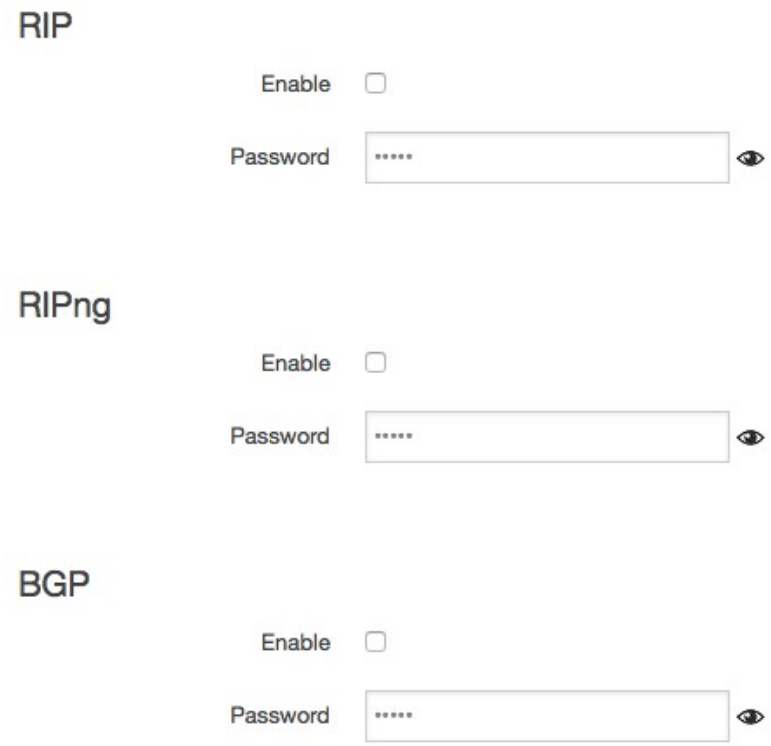
3.6.13 Loopback Interface

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

3.6.14 Dynamic Routing

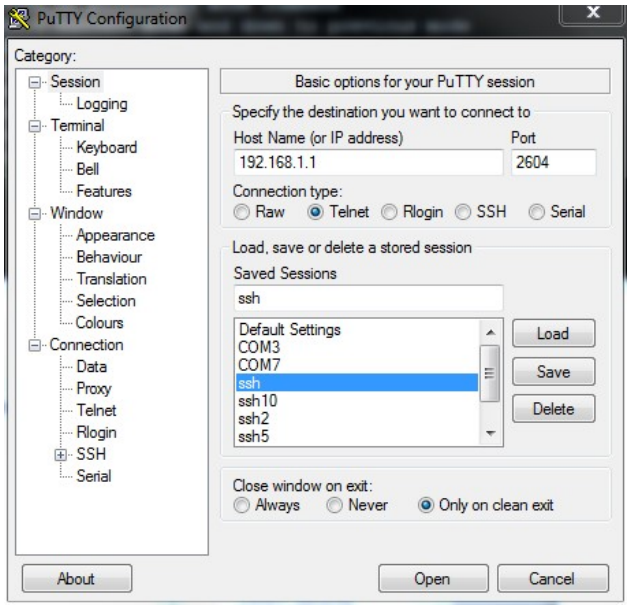
Dynamic Routing is implemented by quagga-0.99.22.4. Dynamic Routing services can be enabled:





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

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



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

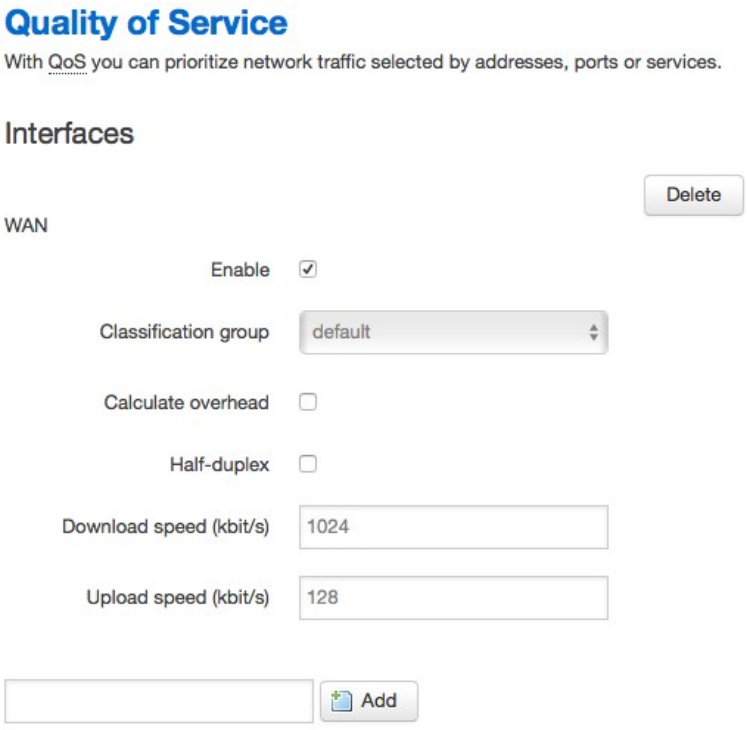
```
Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

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

3.6.15 QoS

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



- **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
priority	all	all	all	all	22,53	
normal	all	all	all	TCP	20,21,25,80,110,443,993,995	
express	all	all	all	all	5190	

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.