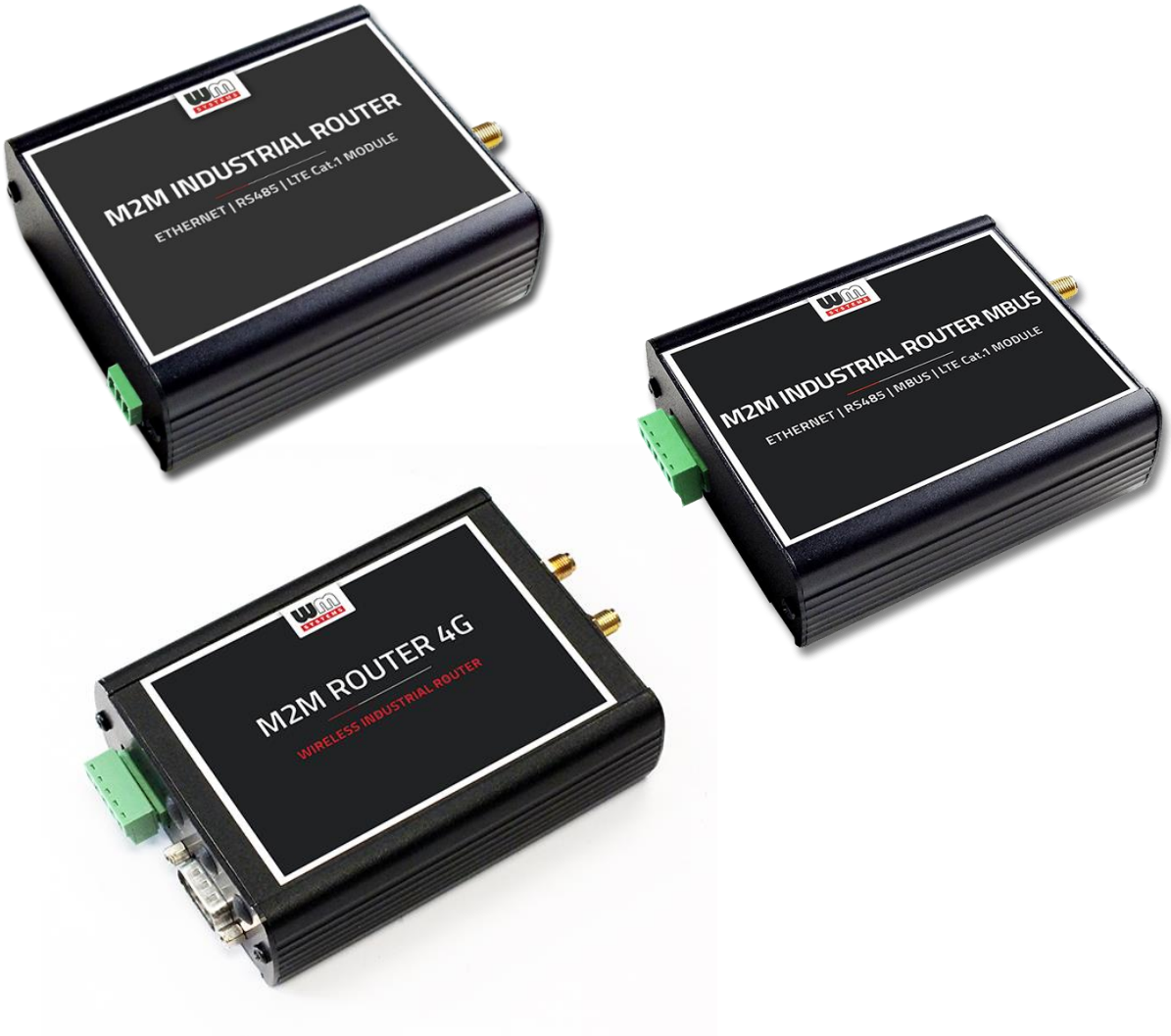
M2M Industrial Router® / M2M Industrial MBUS Router®

User Manual

v2.40



2023-08-28

WM Systems LLC 8 Villa str., Budapest H-1222 HUNGARY
Phone: +36 1 310 7075
Email: sales@wmsystems.hu Web: www.wmsystems.hu

Document specifications

This document was completed for the various versions of the **M2M Industrial Router®**. It contains the detailed description of the router configuration, which is necessary for the proper operation of the device.

You can choose different module types for the router as CDMA 450, 4G LTE Cat.1 and LTE Cat.M / Cat.NB with 2G/3G “fallback”. All of the listed settings are more or less similar for each modem versions.

In case of CDMA450 device, the CDMA-specific MSIN settings are listed in this document.

Document category:	User Manual
Document subject:	M2M Industrial Router®
Author:	WM Systems LLC
Document version No.:	REV 2.40
Number of pages:	88
Hardware Identifier No.:	BE0077F
OpenWRT build version:	202209191
Linux Kernel version:	4.9.184
Firmware version:	2019-01-18
Document status:	Final
Created at:	5 August, 2016
Last modified:	28 August, 2023
Approval date:	28 August, 2023

Table of contents

Chapter 1. Starting the Router

1.1. Product variants

The router can be ordered with LTE Cat.1 or LTE Cat.M / Cat.NB cellular module with 2G/3G fallback feature.

The industrial router contains an RS485 port (transparent or Modbus communication - terminal block connection, 3pins) by default.

As an option, further por texpansions can be ordered for the router as:

- RS232 port (serial port, DSUB-9 connector)
- RS485/Modbus port (terminal block)
- Mbus port (for 0-4 or 51-255 slaves) – terminal block

1.2 Interface connectors

Take notice to the wiring the ground to the device when you connect an external device.

1 – POWER (9-32V DC): Microfit connector power connector (for 12V DC adapter)

2 – SIM card slot (2FF) – *in case of CDMA450 version, not presented*

3 – micro-SD slot

4 – micro-USB connector (for configuration)

5 – Reset button hole

6 – Ethernet (RJ45, 10/100 Mbit)

7 – Primary SMA antenna connector (SMA-M, 50 Ohm - MAIN)

9 – Operation LEDs (LED1..LED3, reconfigurable)

10 – RS485 connector (3-pins terminal block)

11 – RS232 (DSUB-9) connector – *by order*

12 – RS485 / Modbus connector – *by order*

Industrial router with RS485 connector

Industrial router with Modbus / RS485 connector (left side, terminal block, 5-pins) and an RS232 (right side, DSUB-9 connector) expansion

1.3 Safety cautions

The device must be used and operated according to the related user manual.

The installation can be carrying out only by a responsible, instructed and skilled person by the service team, who has enough experience and knowledge about carrying out the wiring and installing a router device.

Its prohibited to touch or modify the wiring or the installation by the user. It is prohibited to open the device enclosure during its operation or under power connection.

It is also prohibited to remove or modify the device PCB. The router and it's parts must not be changed by other items or devices.

Any modification and repairation is not allowed without the permission of the manufacturer. It all causes the loss of product warranty.

CAUTION! Only a certified expert or the manufacturer is allowed to open the device enclosure!

By general the device is using 9-32V DC mains inside the enclosure!

DO NOT OPEN THE ENCLOSURE and DO NOT TOUCH THE PCB.

Router current and consumption

- Power voltage: 9..32 VDC
- Current: 160-260mA, 12V DC (depending on cellular module version)
- Consumption: 1.9W (during 2G/3G communication), 3.1W (during 4G LTE or LTE Cat.M communication)

The IP51 immunity protection will be effective only in case of under normal usage and operation conditions with unharmed hardware conditions by using the device in the provided enclosure/chassis.

Deliberate damage or occing casualty of the device means the loss of product warranty.

To ensure general safety, please follow the following guideline:

▪ Keep the chassis area clear and dust-free during and after installation.

▪ Do not wear loose clothing that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.

▪ Do not perform any action that creates a hazard to people or makes the equipment unsafe.

Safety with Electricity

Follow this guideline when working on equipment powered by electricity.

▪ Read all the warnings in Safety Warnings.

▪ Locate the emergency power-off switch for your installation location. If an electrical accident occurs, you can quickly turn off the power.

▪ Disconnect all power before:

– Installing or removing a chassis

– Working near power supplies

– Insertion a SIM card or change the SIM

▪ Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.

▪ Do not work alone if hazardous conditions exist.

▪ Never assume that power is disconnected from a circuit. Always check.

▪ Never open the enclosure of the router's internal power supply.

▪ If an electrical accident occurs, proceed as follows:

– Use caution; do not become a victim yourself.

– Turn off power to the device.

– If possible, send another person to get medical aid. Otherwise, assess the victim's condition and then call for help.

– Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It may occur if electronic printed circuit cards are improperly handled and may cause complete or intermittent failures. Always follow ESD prevention procedures when removing and replacing modules:

▪ Ensure that the router chassis is electrically connected to earth ground.

▪ Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.

▪ If no wrist strap is available, ground yourself by touching a metal part of the chassis.

Mounting, fastening

The edge of the bopla aluminum enclosure of the device can be fixed by optionally with an AB800MKL fixation part to a DIN-rail. You can also mount the enclosure to wall, place into server rack or similar fixation opportunity.

The device enclosure can be fixed by the AB-MKL (left) one-sided DIN-rail adapter, or by the AB800MKL adapter (right) to a wall or DIN-rail (accessories can be ordered)

More information:
https://m2mserver.com/en/product/din-rail-mount-unit-two-sided/
https://m2mserver.com/en/product/din-rail-mount-unit-one-sided/

1.5 Antenna

Please note that close metal parts, the cabinet metal material and the industrial conditions as the usage of high rate power or other external gained radio frequency signals can cause radio signal disturbance and could cause weak wireless signal at reception or data transmitting or could cause less effective signal reception, weak wireless fidelity. In any of these cases, we recommend you to test the wireless signal reception and quality. If it is necessary use external, magnetic mount antenna which is leaded outside of the cabinet and placed onto the cabinet's surface – to ensure enough reception.

You can use an external magnatic mount antenna is you want.

In case of poor signal quality at problematic installation places you can use directional antenna or directional MIMO antenna.

1.6 Further accessories

The following accessories are not part of the product, these are order options.

Microfit power cable:

Type: min. 70 cm, OMYA type, 2 x 1 mm^2, halogen free, double insulated wires, min. 24 V DC voltage, wires are marked by colors and blanked.

Connector type: 4-pins Microfit (2-pins are wired)

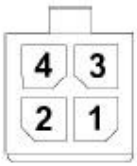
Feature: to provide 9..32V DC power supply connecting for the router (12V DC 1A).

For the wiring and assuring the power supply you should take note to the following figure.

More information:

https://m2mserver.com/en/product/microfit-psu-cable/

4-PIN connector (Power Input)



Pin assignment of 4-pin connector

Pin number	Name	Functions
3	POWER -	DC power negative input
4	POWER+	DC power positive input

DC power adapter:

Connector: 4-pins microfit

Function: 12V DC 1A power voltage for the router

More information:

https://m2mserver.com/en/product/universal-power-supply-12v-1a/

UTP (Ethernet) cable:

Type: Cat5e UTP PVC

Connector: RJ45

RS485 cable:

Type: 70 cm OMYA type, 3 x 0,75 mm^2, halogen-free, double insulated wire pair, up to min. 24V DC breakdown voltage, colour signed cabling, blanked on the cable end – for supporting the 24V DC power voltage.

Type: terminal block, 3 pins

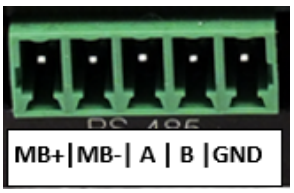
Function: RS485 connection for external devices

Cabling must be done considering the next pinout (from left to right): GND, A, B.

RS485 / Modbus cable:

Type: 70 cm, OMYA type, 5 x 0,75 mm^2, halogen free, double insulated wires, min. 24 V voltage, wires are marked by color and blanked

Connector type: terminal block, 5 pins



Function: RS485- and Modbus connection for external devices / meters

Cabling must be done considering the next pinout (from left to right): MB+, MB-, A, B GND

microUSB-USB configuration cable:

Type: USB-microUSB cable

Connection type: microUSB 2.0 B type connector

Function: for alternative USB-Ethernet connection, according to the RNDIS standard it is simulating an Ethernet adapter for direct computer connection.

1.7 Connecting the router

1. Ensure that the router is not under power voltage, therefore the power adapter cable is removed from the **POWER** titled microfit connector (1) – or the adapter is not connecting to the power network.

2. **Mount a proper LTE antenna to the MAIN (left) SMA connector** (7).

3. **Insert an activated SIM card** to the SIM slot (2) - the SIM chip surface must be look to top and the cutted edge of the SIM must be look to the router – then push the SIM until it will be fixed and closed (you will hear a soft click sound).
   (In case of necessary of SIM removal you have to power off the router and push the SIM a bit, while it will be released and can be removed).

4. **Connect an UTP cable** to the router's **Ethernet** titled RJ45 port (6). During the configuration the cable's opposite connector must be connected to the PC's Ethernet port. (After the configuration connect it to the network- or industrial device's RJ45 port.)

5. You can also configure the router through the **micro-USB slot** (4) by a microUSB-USB cable of the PC connection.

6. Connect the RS485 meter to the **RS485** port (10) to receive the data of the external device or meter. (In case of RS485 / Modbus version connect the external device to the port nr. 12, for RS232 version connect the external device to the port nr. 11).

1.8 First start

The router is provided with pre-installed system (which contains the operating firmware and the OpenWrt® system, which is accessible on the local website of the router).

1. Connect the *microfit* connection **power connector** (1) when the router begins its operation, where the LED lights will be signing and inform you about the current status of the device.

> *9-32V DC power voltage input (interface nr. 1) should be used by the DC powering with the microfit connection 12V DC power adapter, or you can use alternatively 9-32V DC power voltage with own cabling (follow the pinout hints).*

2. **When starting the device** (at power on) – or in case of rebooting – **all the three LEDs of the router** will active for a few seconds.

3. Then the **LED1** light is lighting continously by **green**, which signs that the system is during loading (boot progress).

4. The system start requires about 1-2 minutes, while the device loads the necessary modules or the operation and prepares the web configuration user interface – the **LED2** will sign it. Then the web interface will be availble for login.

5. **Configure the device's wireless internet module settings** (SIM and APN data on the router web interface) **for the cellular internet connection** – otherwise the router will be restarting in ever 10 minutes.

6. The modem registration to the cellular network is signed by the **LED3** flashing after the settings. If it was succesful (to register the SIM card data to the network) then the **LED2** will lighting, which shows that the router can access the cellular network already.

Attention!

- We suggest to change the login password on the web interface.
- If it is necessary, enable the DHCP service.
- Enable the firewall rules and IP route rules for the Ethernet connecting devices.
- Check the RS485 settings (Ser2net).

7. If you notice an unusual LED sign or other operation misbehaviour sympthoms, read the **Troubleshooting** chapter.

8. If you'd like to make the router settings via USB connection (micro-USB port) then install the **USB Ethernet / RNDIS Gadget** driver to your computer by using the following link in your web browser: https://www.m2mserver.com/m2m-downloads/RNDIS_win10.ZIP

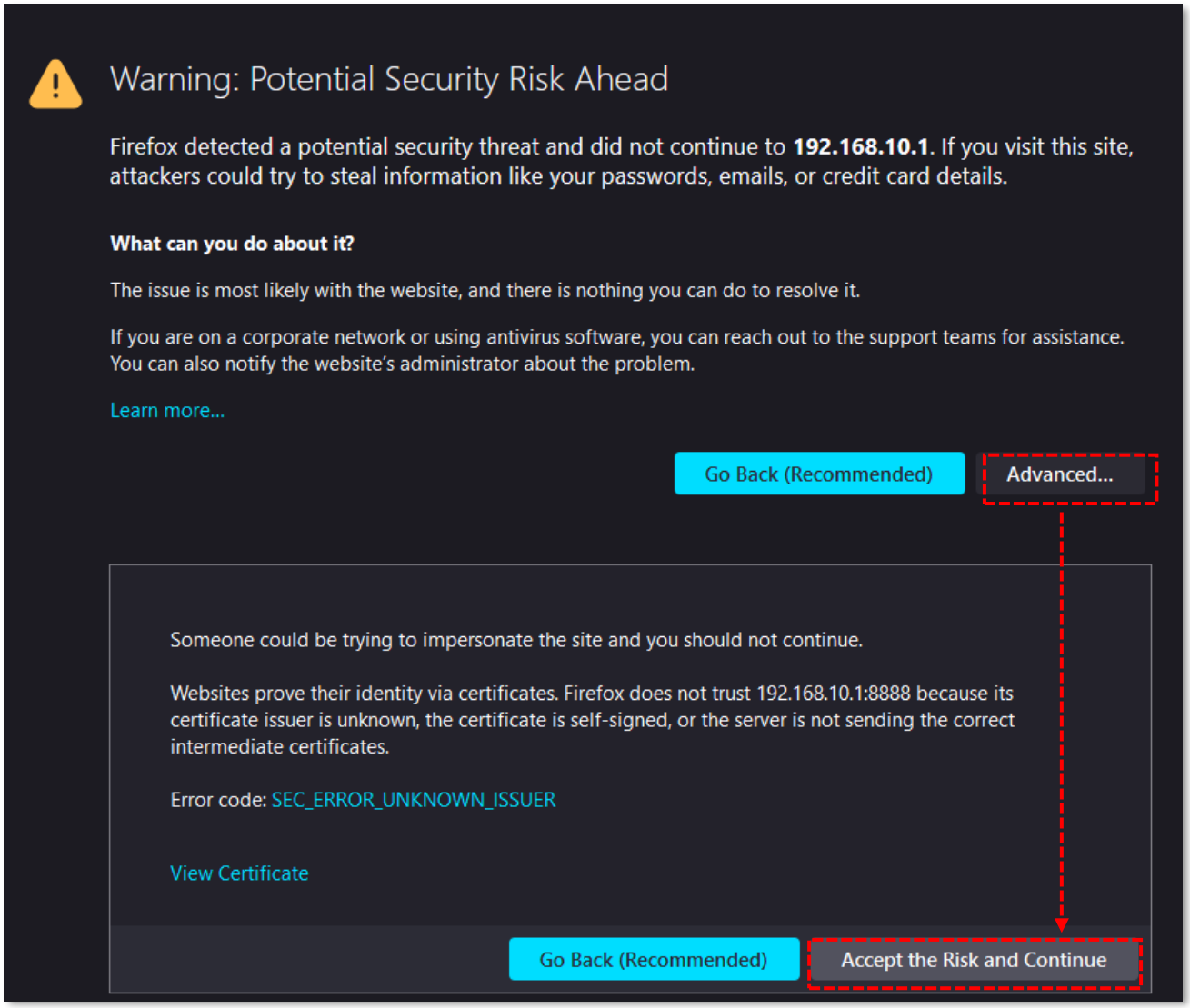
1.9 Web user interface of the router

1. To connect to the router, allow the router IP address for the Ethernet connector interface in the Windows®'s network settings (IP address for Ethernet connection: 192.168.127.100, Subnet mask: 255.255.255.0)

2. In case of USB connection, you have to setup the **USB Ethernet / RNDIS Gadget** virtual interface to the following IP: 192.168.10.100, subnet mask: 255.255.255.0

3. Open the router's local website in the **Mozilla Firefox** browser. By default, the web user interface (LuCi) URL on **Ethernet** port: https://192.168.127.1:8888
   On the **USB** connection the URL is: https://192.168.10.1:8888

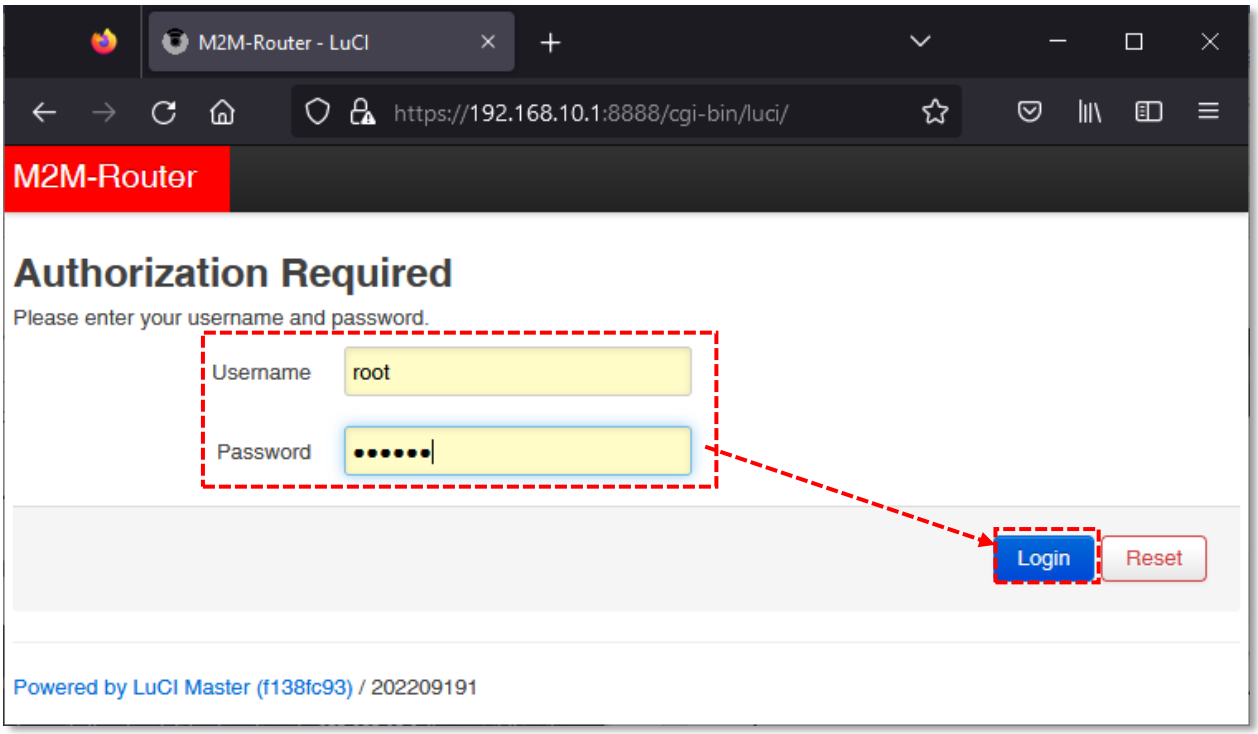
4. At the first time, you have to accept the security risk in the Mozilla® browser by choosing the **Advanced** option at the ***Potential Security Risk*** and Then choose the **Accept the Risk and Continue** option.



5. Then the router's local web interface will be loaded and you can login.
   - **Username**: ***root***
   - **Password: *wmrpwd***

6. Push to the **Login** button.

> ***Attention!***
> *Don't forget to change the login password before connecting the router to the public cellular network!*



1.10 Access via SSH connection

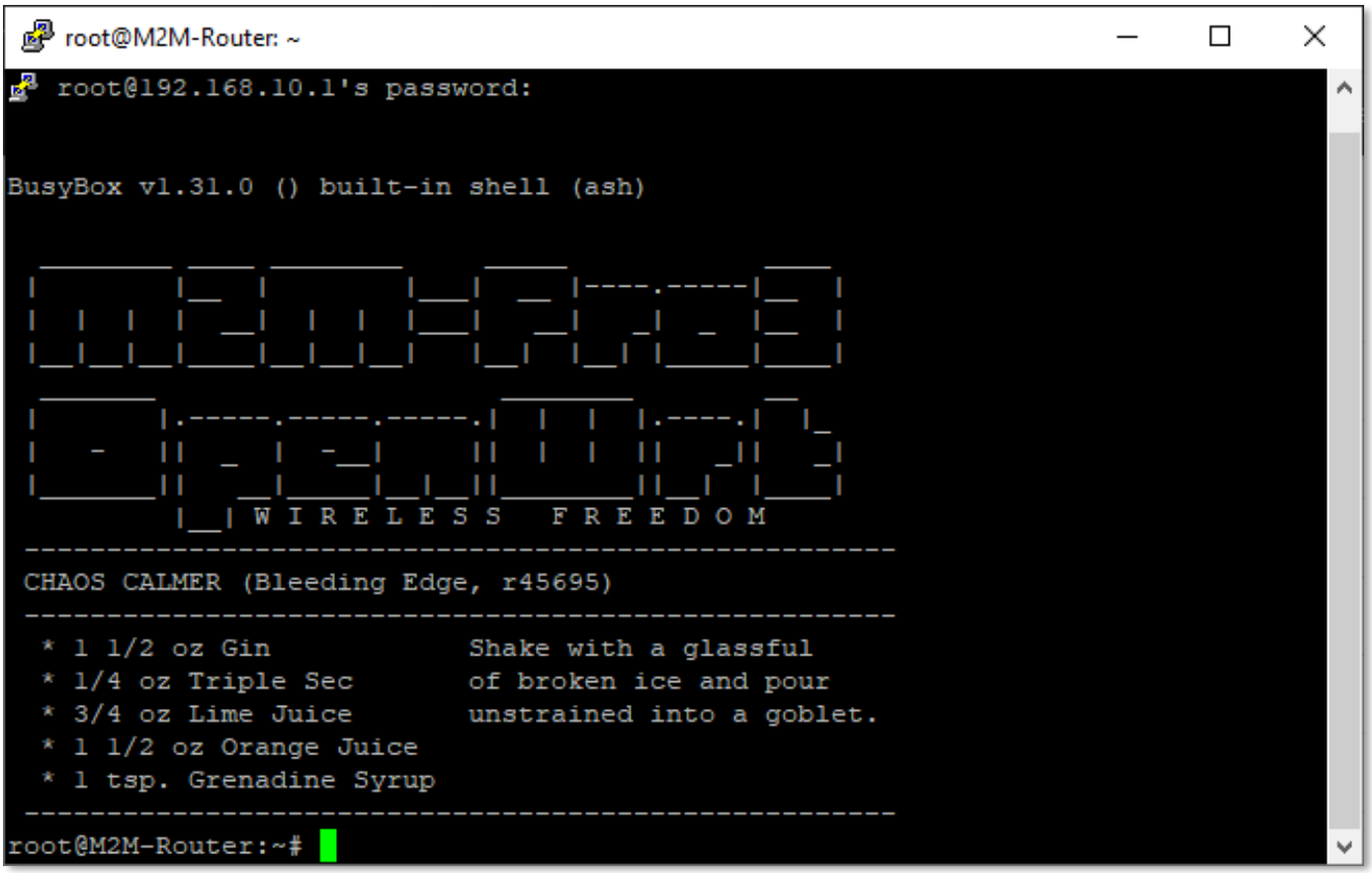
The router can be accessed through ssh connection also, when it is available on its IP address – use the *putty* terminal utility/tool for the connection

1. Connect to the **192.168.10.1:22** IP address.
   (Login: ***root***, Password: ***wmrpwd***)

2. **Accept** the security risk (RSA token) encryption key usage warning notice (visible at first time only).

Then the Linux command line will appear, where you can use standard Uc Linux kernel 4.9 compatible commands and execute scripts on the device.

You can also use ***UCI command line interface*** commands here. The UCI® (Unified Configuration Interface) is an OpenWrt® API utility that allows centralized configuration and management of the OpenWrt® operation system, configuration of the router.



To review the UCI commands and options that can be used, we recommend to read UCI Reference Guide, which can be downloaded from our website.
https://www.m2mserver.com/m2m-downloads/UCI_Command_Line_Reference_v3.pdf

E.g. you can make a query to ask the current setting of a service (openvpn, ser2net, ddns, etc. by using the following command from command line):

```
#uci show service_name
```

You can also having the option to make detailed settings of a service by using the UCI interface.

Chapter 2. Web Administration user interface

2.1 Dashboard (Main page)

After login to the web interface, the startup screen appears with the current status of the router.

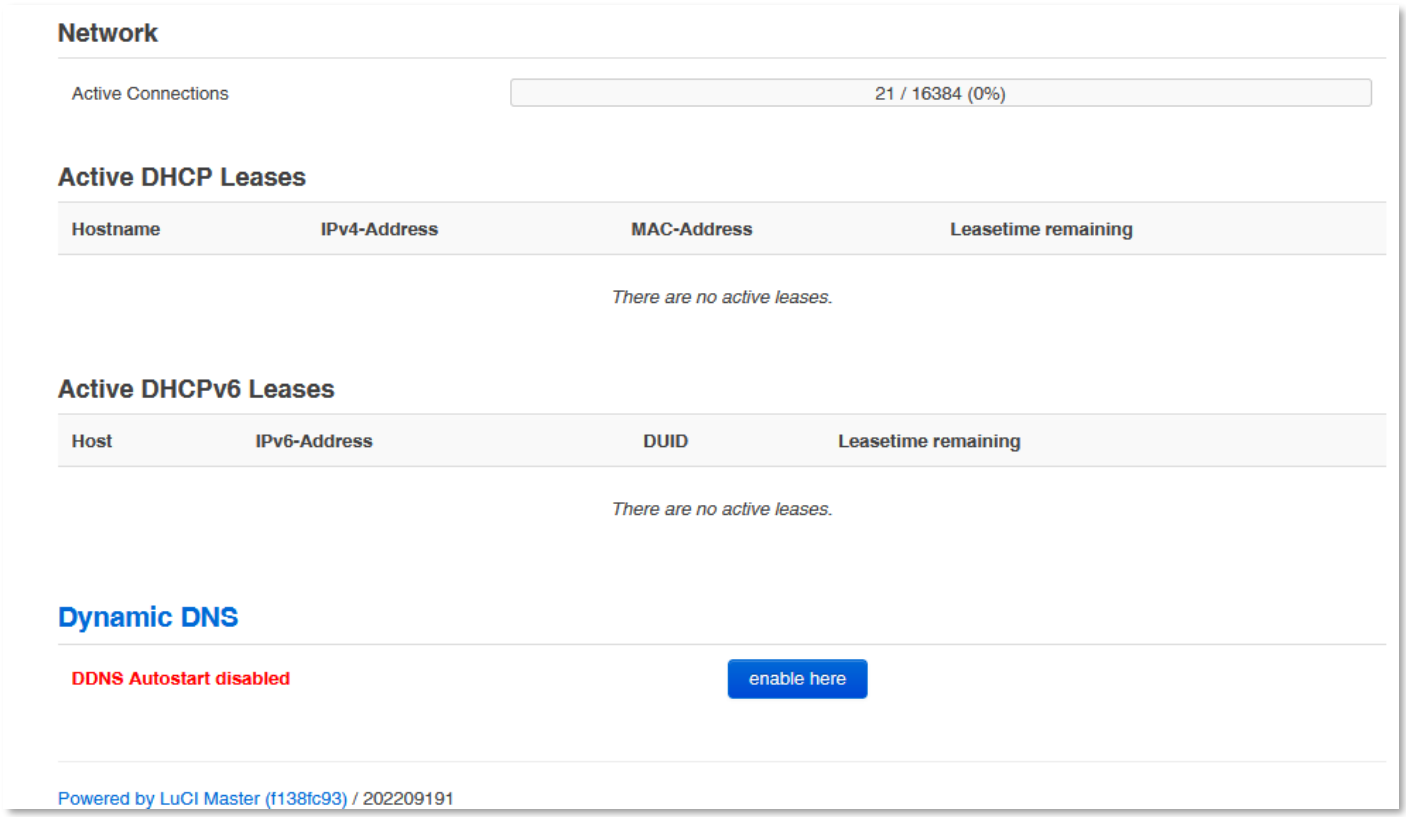
At the **System** part you can check that the **Build Date.** It should be *202209191* or newer version.

The **Local Time** shows the currently received time, the **Uptime** shows the spent time since the last reboot/start.

At the **Modem** part you can identify the **CREG** field you will find the cellular network code and **c**ell identifier. At the **COPS** field the cellular network name**.**

Modem RSSI (dBm value) and **Modem SQ** (CSQ value) show the values of the mobile network reception field strength. (The lower RSSI value siginificant to a better signal level / the higher SQ value means a better signal level).

At the **Network** part you can IP **Address**, which the SIM got from the mobile operator's cellular network.



2.2 Menu

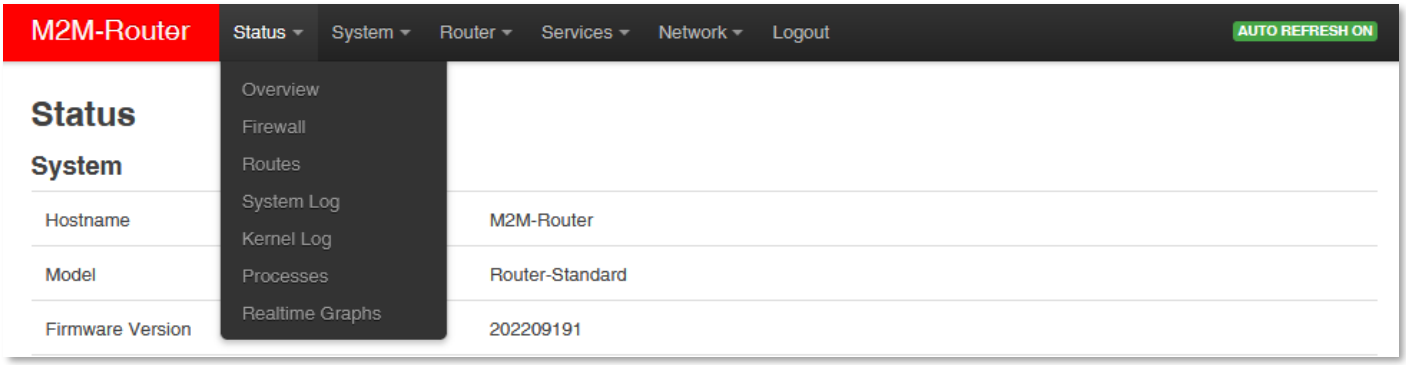
By the menu you can access the following features:

- **Status** – Status data, operation and system log, operation monitoring
- **System** – System settings, administration, software and firmware refresh, backup/restrore of the configuration settings, LED configuration, reboot, etc.
- **Router** – Device Manager settings, Logging parameters, Periodic Ping, daily restart and recovery of Factory configuration

- **Services** – Dynamic DNS settings, OpenVPN settings, Ser2Net (RS485 settings)
- **Network** – network interface settings, DHCP, DNS, hostname, IP route rules (static routes), diagnostics, Firewall, voice call config, SMS config

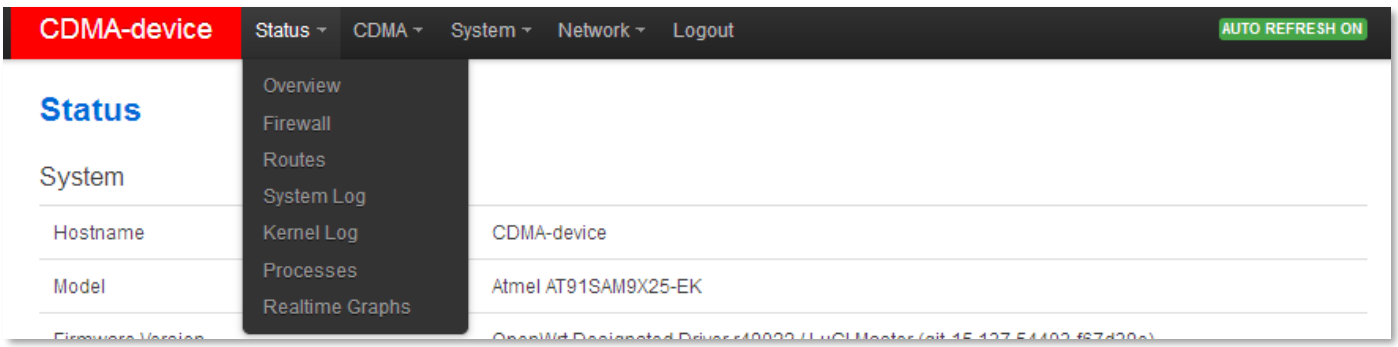
2.3 Status menu

- In the **Status** you can check the current status (**Overview**),
- at the **Firewall** item, you can see the firewall events and information,
- at the **Routes** item the valid/active route settings,
- check the system messages and event log (**System Log** and **Kernel Log**),
- activities of the router (**Processes**),
- monitoring the realtime operation at the **Realtime Graphs.**



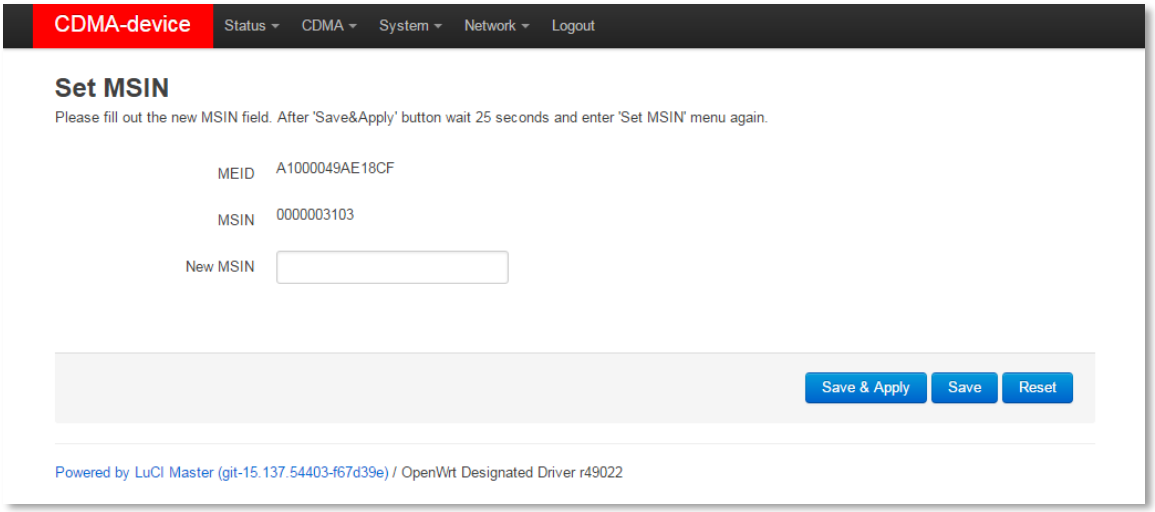
2.4 CDMA menu (only for CDMA devices)

In case of CDMA450 version, the hostname is already configured for *CDMA-450* in the Overview menu (Dashboard).



The modem's **MSIN identifier** can be configured here: **CDMA menu/Set MSIN** which is required to use the router on any CDMA450 network.

If you give a new **MSIN number**, then the WAN interface will be automatically configured for the router. This setting can be checked at the **Network/Interfaces** menu.

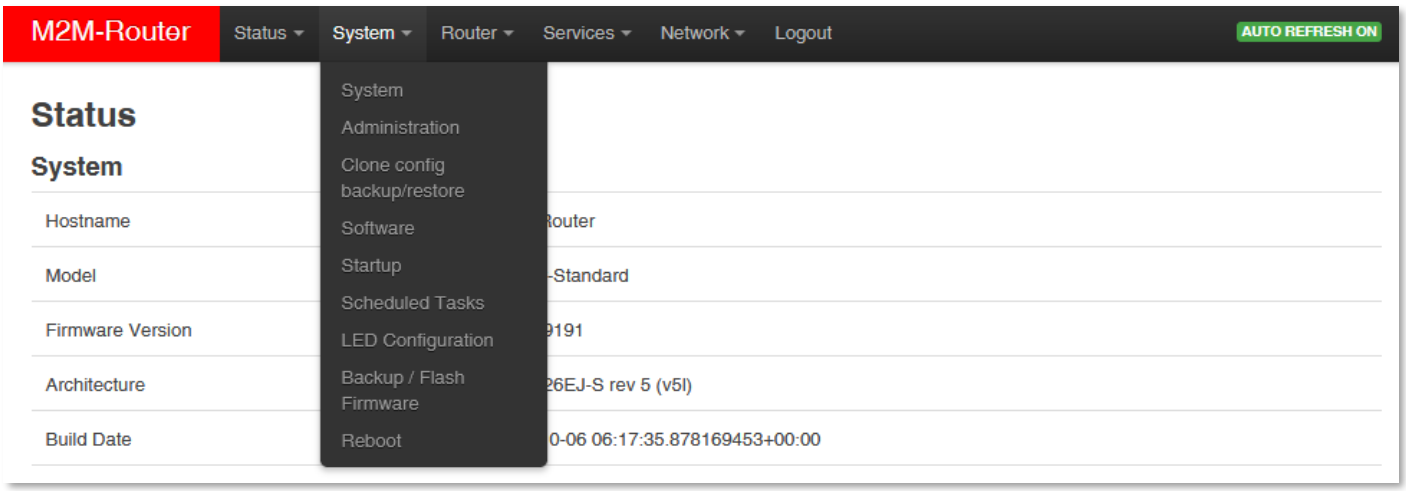


You can store the router settings with the **Save** button. The **Save & Apply** button stores the settings and reconfigure the router related on these settings. **When it was succesful, the router will be not restarting automatically futher.**

2.5 System menu

You can found several system settings in these menu items**:**

- In the **System** menu: **Hostname** (router name), **Time synchronisation** (time and NTP server settings), **Logging**, **Language** (of user interface)
- **Administration**: **Password** (for admin user interface) and the **SSH Access**

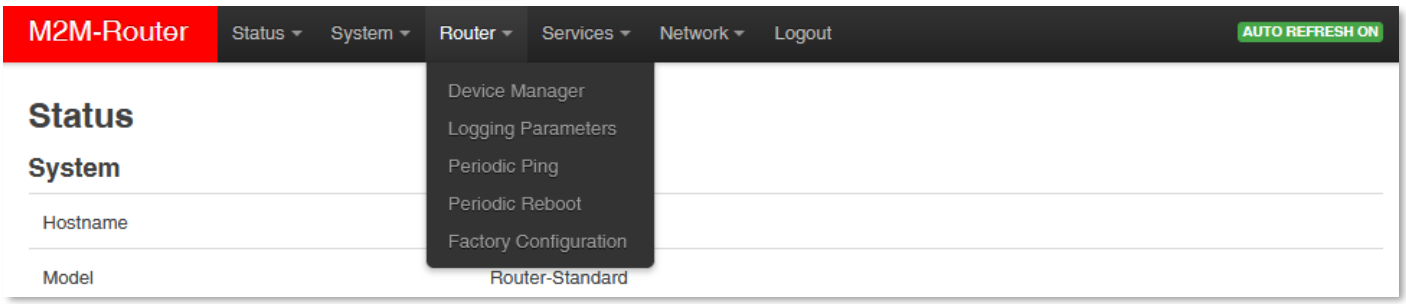


- **Clone config backup / restore** – here you can make a file of the current settings which can be distributable to an another router

- Installation of further **Software** (3rd party tools, applications) from the online software repository
- You can setup **Startup** applicatons and services during the operation (start/stop them)
- You also can define **Scheduled Tasks** for starting them in the right time and sequence
- The **LED Configuration** is also configurable.
- You also can **Backup / Flash firmware** updates
- **Reboot** the router

You can store the router settings with the **Save** button. The **Save & Apply** button stores the settings and reconfigure the router related on these settings.

2.6 Router menu

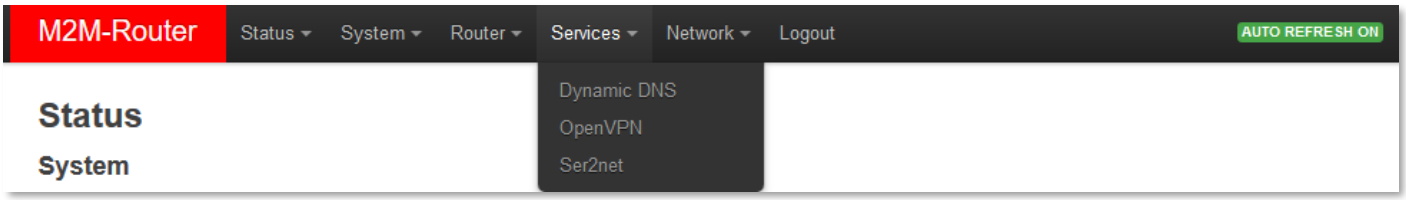


- You can define the remote monitoring software connection settings of the a **Device Manager** (optional remote management software for firmware refresh and reconfiguartion, check QoS).
- You can setup **Logging parameters**
- At the **Periodic Ping** you can configure the cyclic heartbeat ping interval settings – as a network checking method feature.
- The daily router reboot can be allowed at the **Periodic Reboot** menu item.
- The backup of the factory settings is possible at the **Factory Configuration** (save to a file).

2.7 Services menu

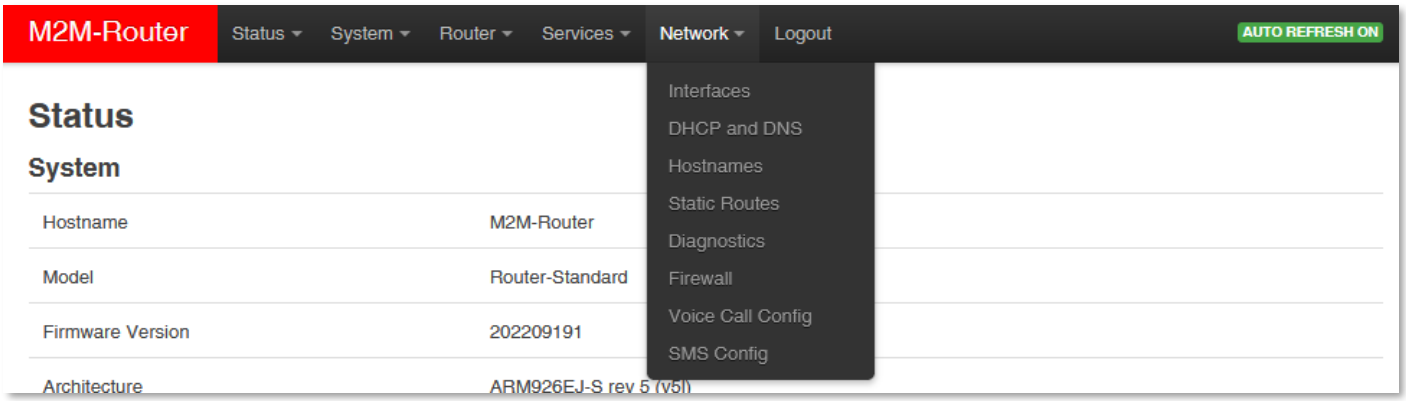
- Here you can setup the **DynDNS** (dynamical DNS) service settings
- And to define the **OpenVPN** client connection settings

- In the **Ser2net** menu you can configure RS485 operation settings



2.8 Network menu

- Here you can configure the settings of each network **Interfaces.**
- You can modify the **DHCP and DNS** settings.
- Define network device name for the router at the **Hostnames.**



- **Static routes** paths can be also defined here.
- **Diagnostics -** you can test network operation and connection health (ping IP address).
- **Firewall** rules can be declared here as the following submenu items: Port forward, IP route, NAT settings.
- A **Voice Call Config** – reboot the router remotely by initiating a voice call – the recorded phone numbers have right for executing the command
- At the **SMS Config** menu you can define the remotely executable commands (can be started by SMS text messages).

Chapter 3. Important notes

- For security reasons, we do recommend to **change the password** immediately for accessing the administration user interface (local webpage). Read Chapter 6.6 for detailed settings.
- Some protocols are disabled by default on the router, but most of them you can enable to use:
    - The **DHCP** service is turned off by default. When enabled, the router assigns IP addresses to connected devices, while the available Ethernet interface addresses use ***static*** addresses. If you want to assign IP addresses by DHCP, change the protocol value to **DHCP client**. You can do this in **the Network / DHCP and DNS settings** menu or under the **Network / Interfaces** menu, in the **LAN** interface, in the **DHCP** section.
    - The **Dynamic DNS** (DDNS) service is disabled by default, but you can enable the service. Read Chapter 4.10 for detailed settings.
    - The **IPSec** service is disabled by default, but you can enable the service. Read Chapter 5.10 for detailed settings.
    - The **OpenVPN** service is disabled by default, but you can enable the service. Read Chapter 5.11 for detailed settings.
    - The **Ser2Net** (RS485) service is disabled by default, but you can enable the service. Read Chapter 5.6 for detailed settings.
- Some protocols are disabled by default on the router and you cannot use them, but you can make a request and indicate your requirement before ordering:
    - The **IPv6** protocol is disabled for **LAN** and **USBLAN** interfaces by default. IPv6 cannot be used on the router!
    - **SFTP** service is currently not usable on the router.
- Notes on Firewall service
    - The **Firewall** feature is enabled by default (for security reasons), which means that all communications are disabled except Ethernet, DHCP, DNS, and WAN channels, the web port, and services and ports that are required for normal, normal, and general operation.
    - **Note, that enabling of the firewall service does not protect the router from external DoS attacks and unauthorized intrusions. For reliable operation, review the settings and allow only the necessary communication.**

- We do recommend to disable all ports and protocols in the **Firewall** that you are not currently using (connection / channel / data transfer) taking into account access to the required ports and channels. To check this, the **Status / Firewall** menu section is an excellent option for scanning through traffic and the **Network / Firewall** menu, where you can add new rules or modify existing ones.
- Please check the network traffic of the router frequently in the **Status / Firewall** menu (port number, incoming IP, especially outgoing data traffic and downloaded data).
- Measure throughput and network traffic (per minute, per hour) - with the help of the **Status / Realtime Graphs** menu or **Statistics / Graphs** where you can view the calculated and expected traffic volumes, which is important if you want to avoid congestion. or the data traffic limit of the SIM card used is limited.

- If necessary, you can select a dedicated mobile network type (such as 3G only or 4G only), or you can use automatic mode (which connects to the fastest network type currently available). This allows you to limit the baud rate (and volume) with the manual settings. You can set this in the **Network / Interfaces** menu on the **WAN** interface by clicking the 

button and setting of the **Wireless network** and **Select IoT Technology** fields.
- The parameters that can be used for the **APN settings** are always provided by the SIM card issuer (mobile service provider). Contact them for **APN**, **password**, **SIM PIN** and other information. You can set them in the **Network / Modem settings** menu.
- The router constantly checks the interfaces and the viability of the connections. In the event of a power failure or power failure, the network and data connections are automatically reconnected after the conditions are restored.
- The **RS485** data speed can be set between 300 and 115,200 baud on the web interface, but the device is able to serve the channel up to 19 200 baud. We recommend that you use the standard 9 600 baud (for general industrial devices) or 2 400 baud (for utility meters) for the better compatibility.
- If you do not want to use the router on a mobile network, but as a wired Ethernet router with RS485 capabilitiy, then configure that in the **Network / Interfaces**

menu, remove the **WAN** interface with the Delete button. From then on, the router will not be restarted even if no SIM card is inserted.

- **HTTP**, **HTTPS** redirect and HTTPS certifications and **SSL** certifications are used.
- Paths on the file system of the router:
    - If you are using the RS485 port, the Device path is */dev/ttyS3*
    - If you are using the RS232 port, the Device path is */dev/ttyS4*

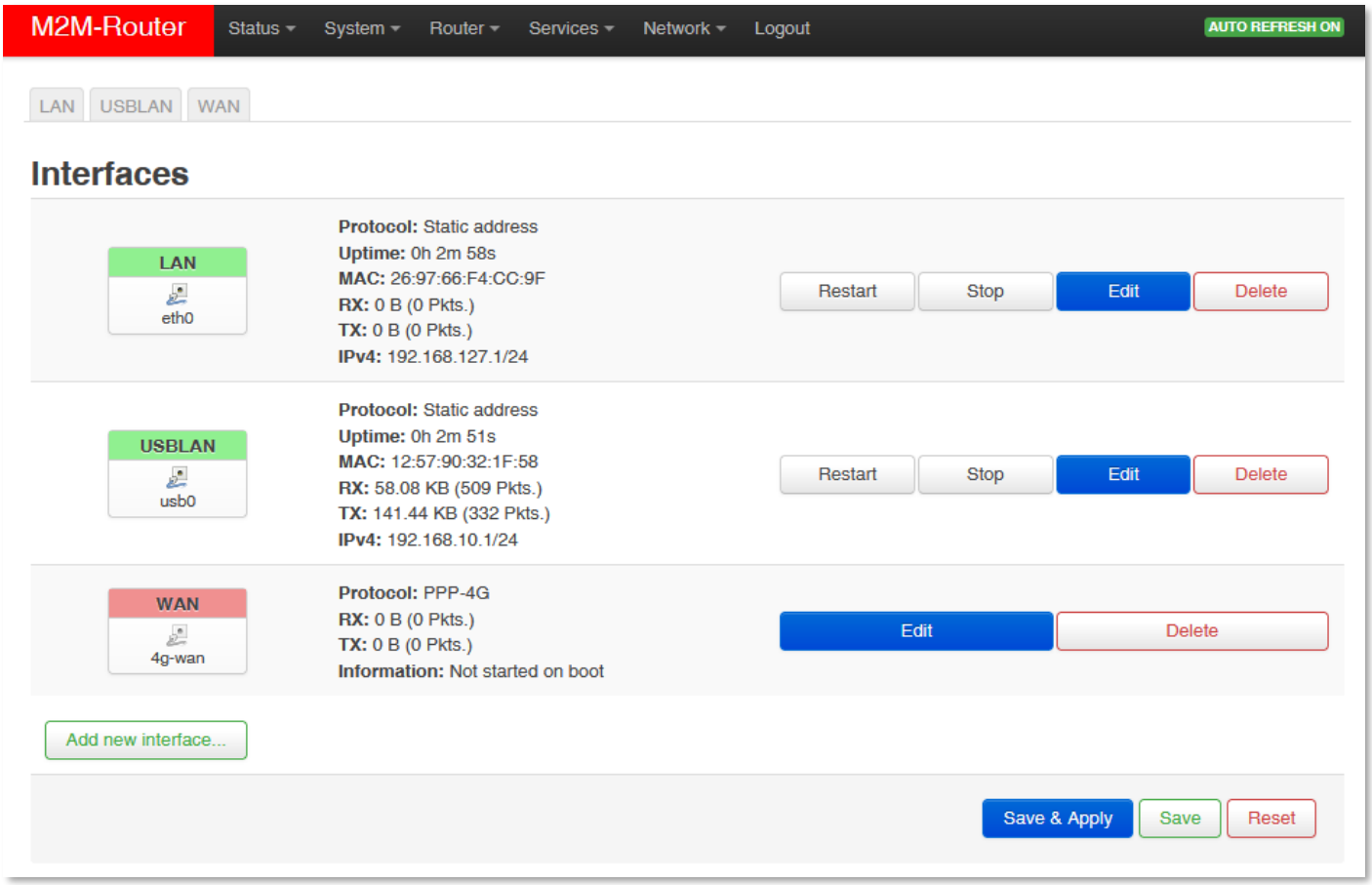
Chapter 4. Network configuration of the router

4.1 Interface settings

The list of the available network interfacescan be found at the **Interfaces / Interface Overview** menu item.

The network interfaces are listed at the **Interface Overview**.

The **LAN** interface means (***eth0***) the Ethernet port connection, the **USBLAN** is the USB-Ethernet (***usb0***) and the **WAN** interface is the public wireless Internet connection (***4g-wan***) for the cellular modem.



Modifying the LAN interface settings

At the interfaces, at right you can modify the settings with the Edit button.

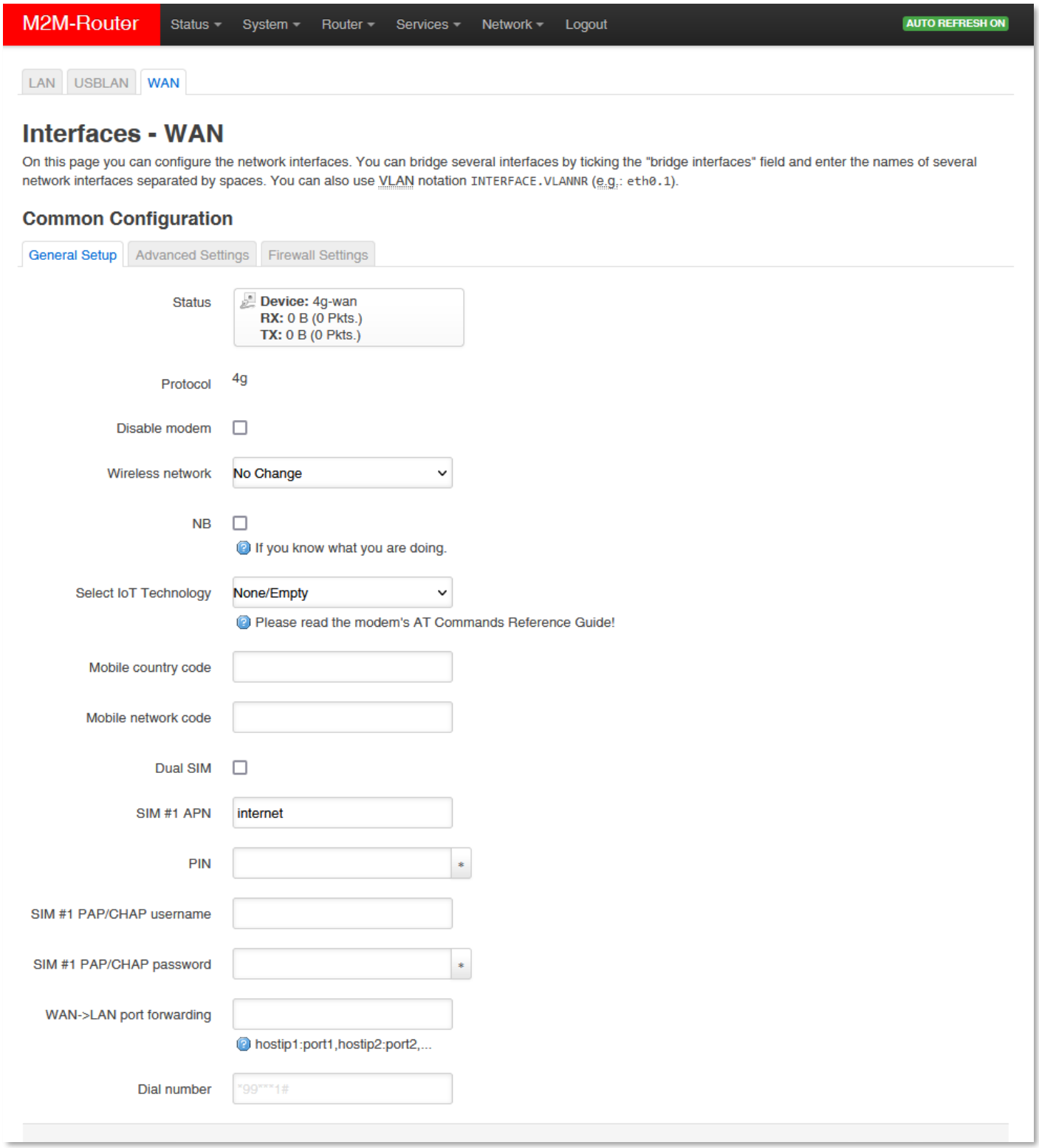
The Stop button stops the communication on the current interface, the Restart button reconnects the related interface connection.

At the upper **WAN**, **USBLAN**, **LAN** title you will found further settings for the chosen Interface.

4.2 Cellular / mobile internet settings

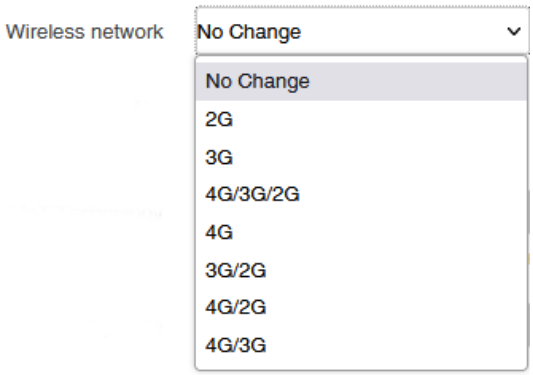
Open the **WAN** item from the upper selection. Then at the **General Setup** tab you can see the current status of the interface and the transmitted data amount.

Setup the module for connecting to the CDMA 450 / 2G / 3G / LTE or Cat.M / Cat.NB cellular network (according to the assembled module type) – at the **WAN** interface tab.



Attention!
In case of CDMA450 router version you don't need to configure these settings.

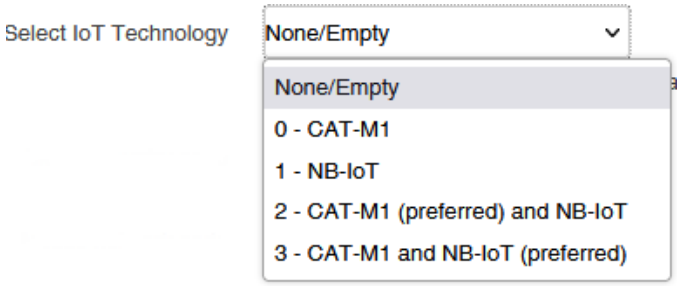
Wireless network field – we offer to use the ***No Change*** option or use the ***4G/3G/2G*** option (automatic detection mode with 3G/2G „fallback" option).



For further „fallback" modes, choose ***4G/2G*** or ***4G/3G*** modes.

If you want to use a dedicated network type, just choose it (e.g. ***4G***).

Select IoT Technology field – in case if LTE Cat.M / Cat.NB (Narrow Band) version modules, you can choose between LPWA networks – available only for LTE Cat.M or Cat.NB (Narrow Band) modules. Choose a cellular access technology!



Fill the **SIM #1 APN** name.

If you won't set any value for **SIM #1 APN**, the router will try to connect by the SIM-card automatically to the next available network's APN**.**

Fill the SIM **PIN** code if it is necessary for the connection.

The **SIM #1 PAP/CHAP username** and **SIM #1 PAP/CHAP password** settings can be also configured here – if it is required for the connection.

To configure and enable the **roaming** settings – in **case of international or country border usage** – you may need to setup the **Mobile country code** and **Mobile network code** parameters – even if you are attempted to use only a prefered mobile network.

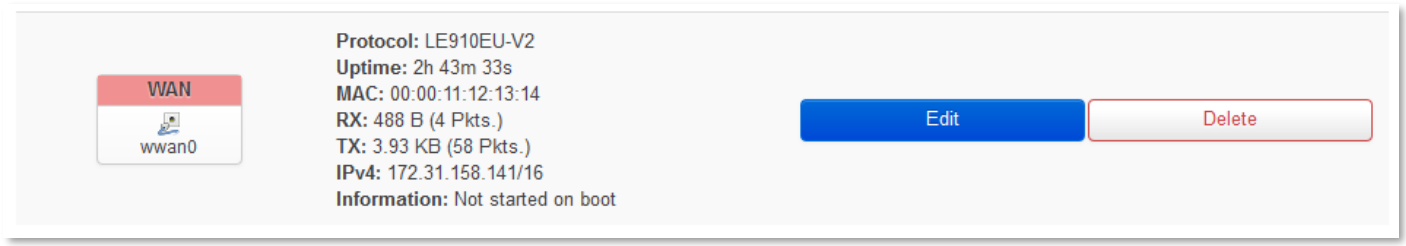
The international country codes can be found here: https://mcc-mnc-list.com/list

Attention!
The available APN settings will be provided by the SIM card provider mobile operator or your mobile internet service provider. The available international settings and roaming services are provided also by the M.O.s.

Attention!
LTE450, LTE Cat.M and Cat.NB (Narrow Band) networks require a compatible SIM card! Ask your network operator / service provider for a useful 2FF type SIM card.

Click to the **Save & Apply** button for saving the settings, while the devices attempts then connecting to the mobile network.

Once this is done, the router will no longer be constantly restarted!
After that, you should check data traffic at **Network / Interfaces** menu for **WAN** interface.



As you can see, the device is already connected to the mobile internet network and is currently active - **RX** (received data), **TX** (sent data) and **KB** (KBytes) are constantly increasing.

During the settings, **LED2** indicates the network registration process - if the APN and SIM settings are correct, the LED will be **flashing** by **green**.

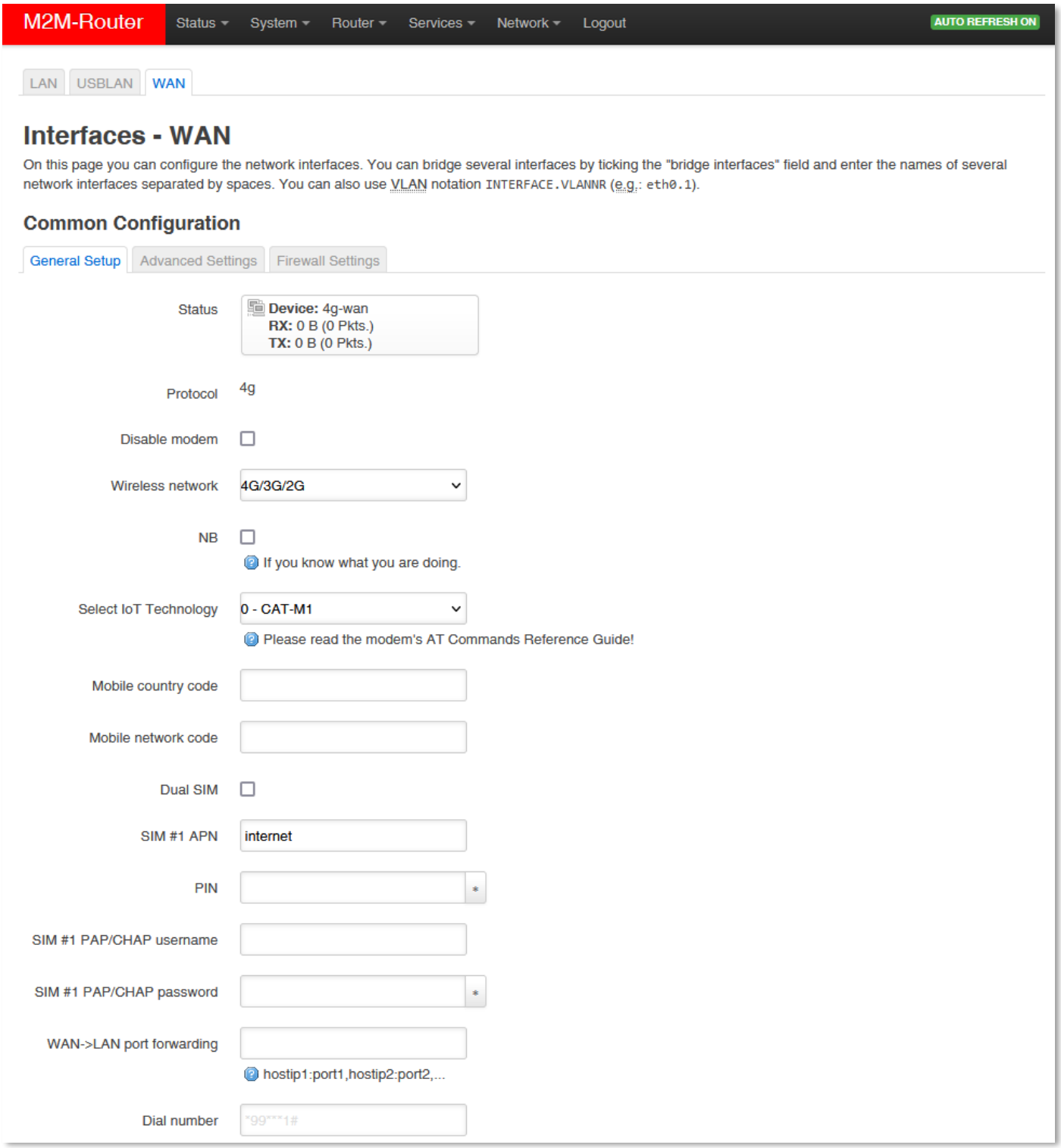
When the network registration was successful, the **LED2** will be **lighting continuously** by **green**.

Data traffic from the **WAN** interface (mobile network) is indicated by a fast **green** flashing of **LED2**.

You can find more network settings on the **Advanced Settings** tab if you want to set more.

4.3 Ethernet (LAN) settings

For the **LAN** interface, at the **LAN** menu item at the **General Setup** tab you can define an own IP range (**IPv4 address**), with the related **IPv4 netmask** (subnet mask).

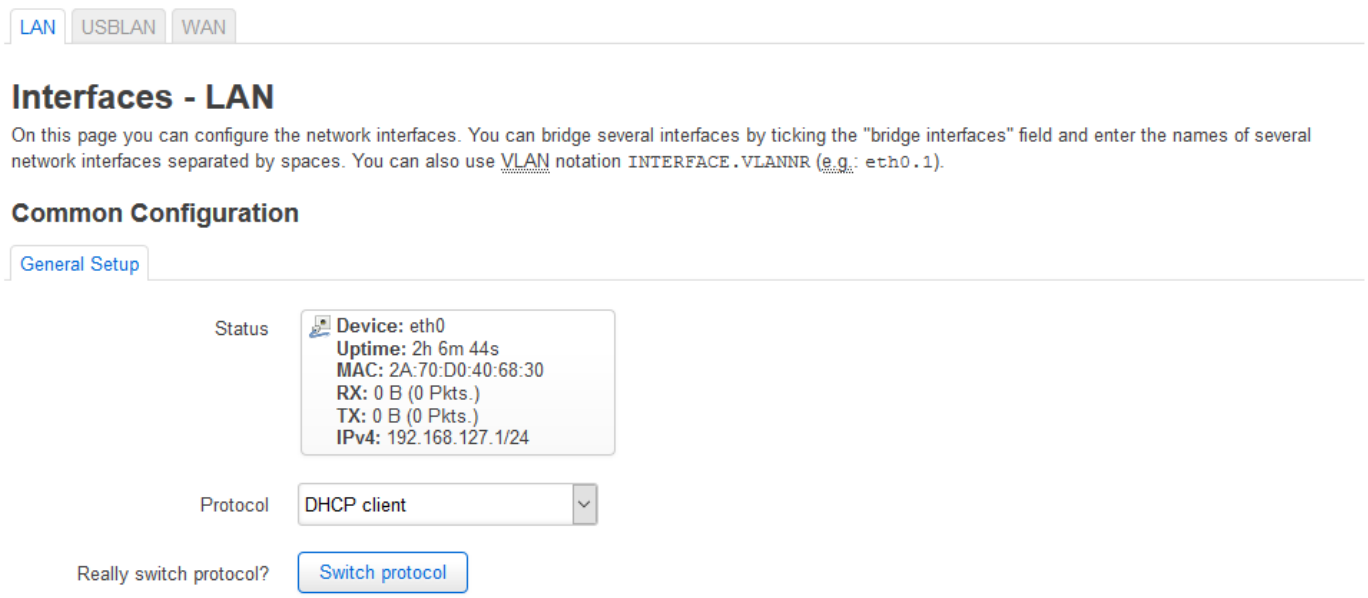


The detailed **LAN** interface settings can be performed by the **Network Interfaces** menu item at the **LAN** interface Edit button.
We recommend that you change the router's **default** *192.168.127.1* **address** (IPv4 address) to a custom IP address, depending on your subnet - or the way you want it to be served by the router device.

Also check **IPv4 netmask** field to make sure it is appropriate for the class you want to use.
(Note that IPv6 service cannot be used, so do not enable or configure the fields that apply to it.)

To make the setting, press the **Save & Apply** button at the bottom of the page.

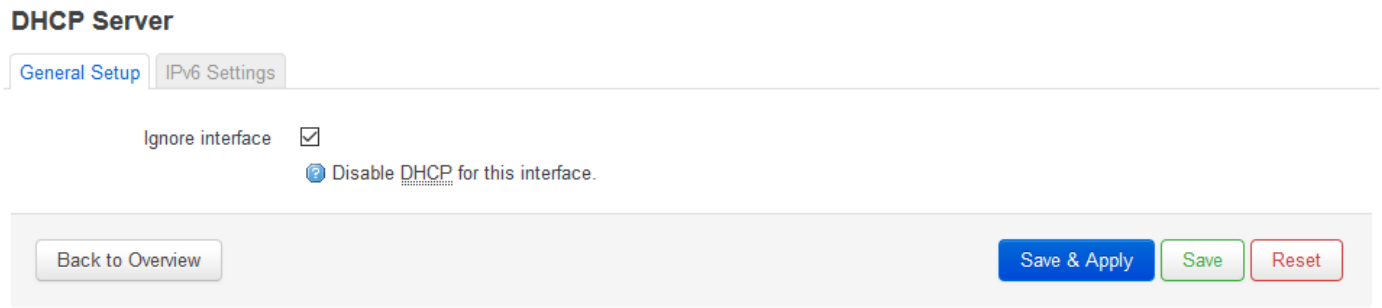
If you do not want to assign a fixed IP address to the router, but want the device to obtain its IP address from another network device (via DHCP), rewrite the IPv4 address as described above for the IP of the associated gateway or other network device. address, then in the **Protocol** field, select *DHCP client* instead of Static address and press Switch protocol button. The DHCP client setting for the ethernet interface will then be active.



When you have modified the settings, save them by the **Save & Apply** button.

4.4 DHCP, DNS settings

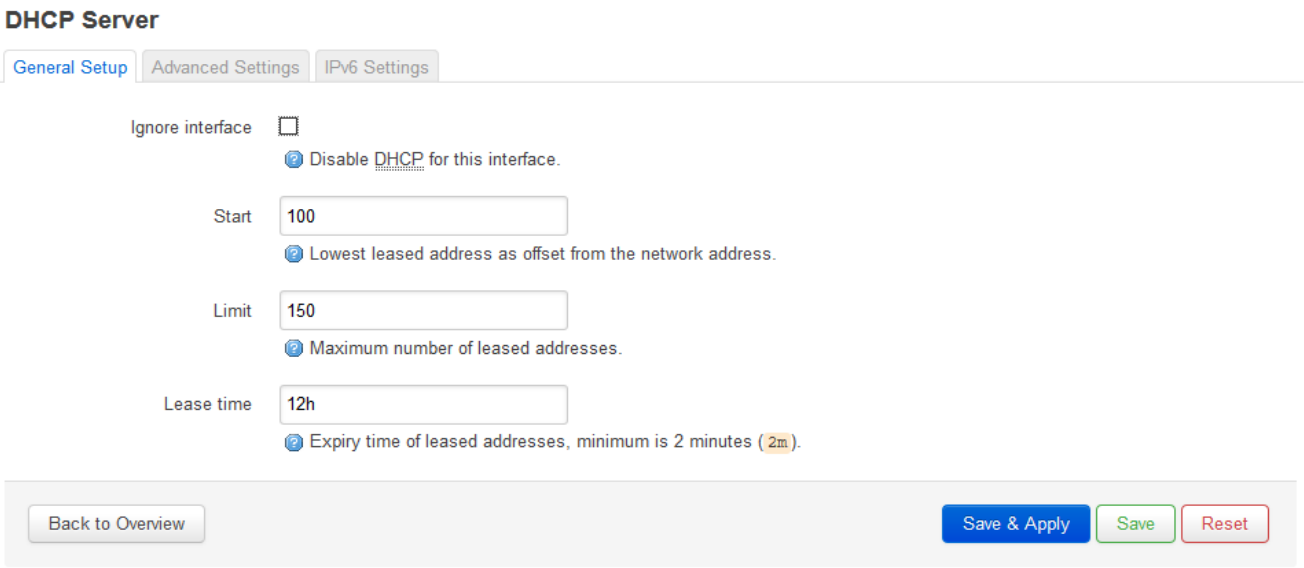
The DHCP service allows the automatic IP address providing for the connecting devices in the current IP segment by the router. The DHCP settings can be found at the **Network / Interfaces** menu (according to the required interface).



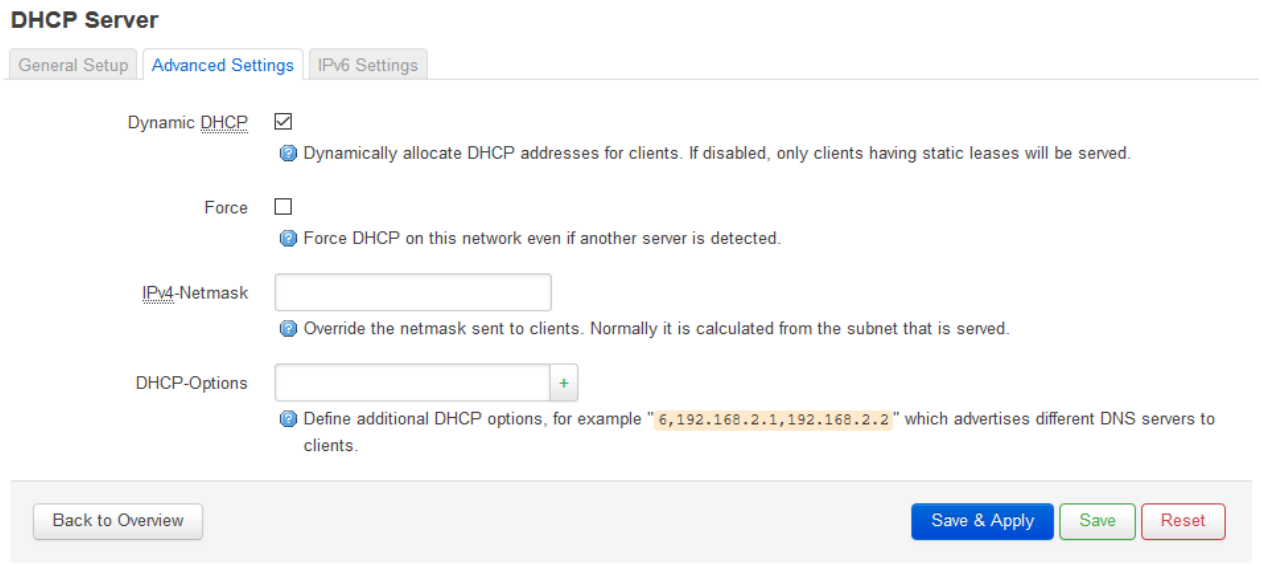
To enable DHCP service, uncheck "**Ignore interface**". For this, the fields required for DHCP configuration are displayed, with default values.

The **Start** field means what the starting address should be within the subnet used by the router (in our case 192.168.x...).

Use the **Limit** field to limit how many IP addresses are assigned. That is, the router on subnet 192.168.x will assign IP addresses in the address range between **Start** and **Start + Limit** to the devices that want to connect.

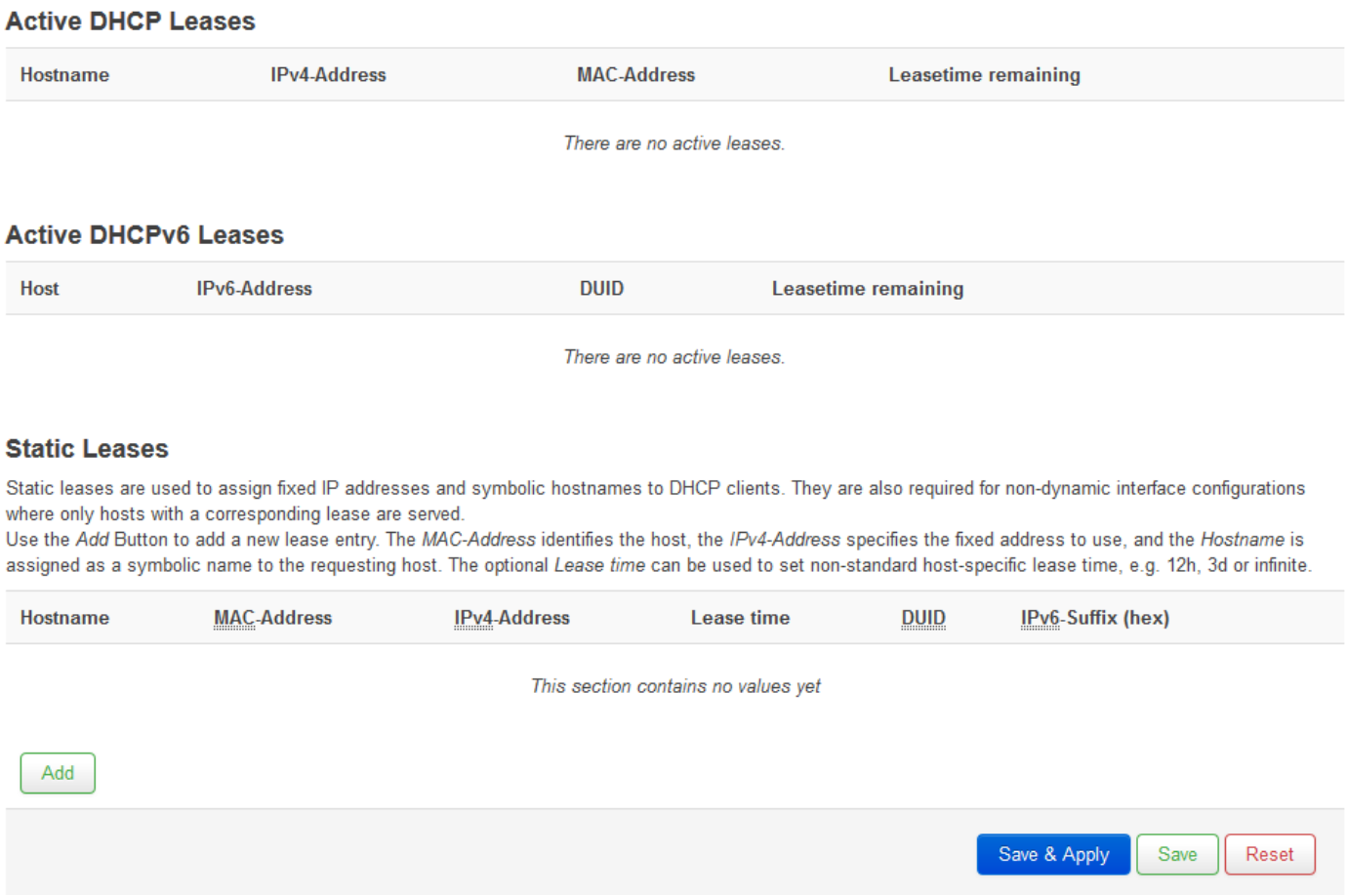


Additional settings on the **Advanced Settings** tab, if required (Dynamic DHCP, Subnet Mask (IPv4-Netmask)). Save the settings with the **Save & Apply** button.



The further DHCP settings can be achieved at the **Network** menu, at the **DHCP and DNS** item, **General Settings** tab.

At the **Active DHCP Leases** part you can see the list of the devices, which given their IP addresses from the router's DHCP service (with the renewal *lease time*).

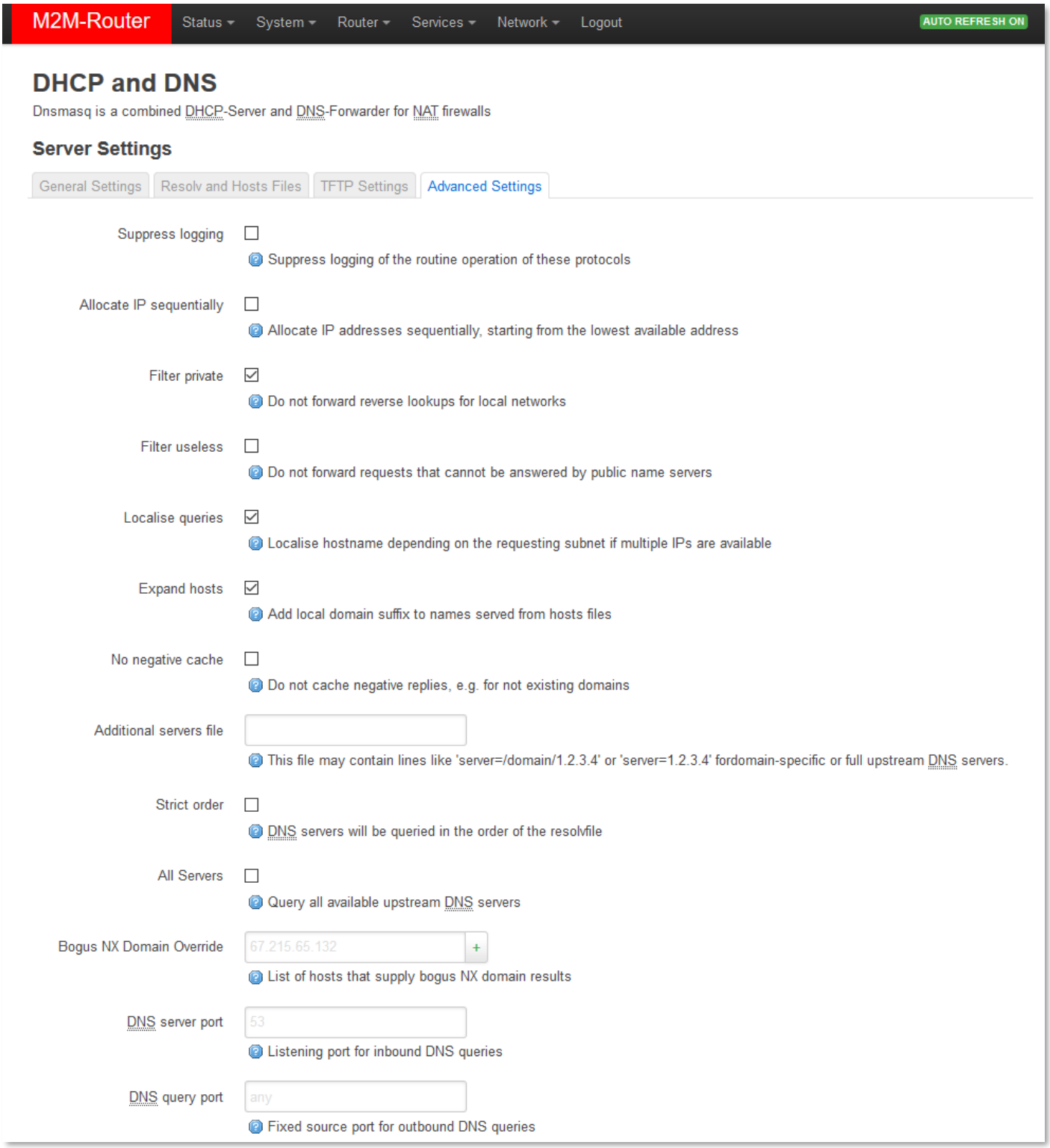


In the **Static Leases** part you can  devices to always provide the same dedicated IP address by the router.

This can be required by adding values to the **Hostname**, the **MAC-Address** and the **IPv4-Address**. When you have modified the settings, save them by the **Save & Apply** button.

4.5 DNS settings

You can configure the DNS service from the **Network** / **DHCP and DNS** menu, with chossing the **Advanced Settings** tab.



At the **DNS server port** field you can define the port for the DNS service (by default its port number is 53).

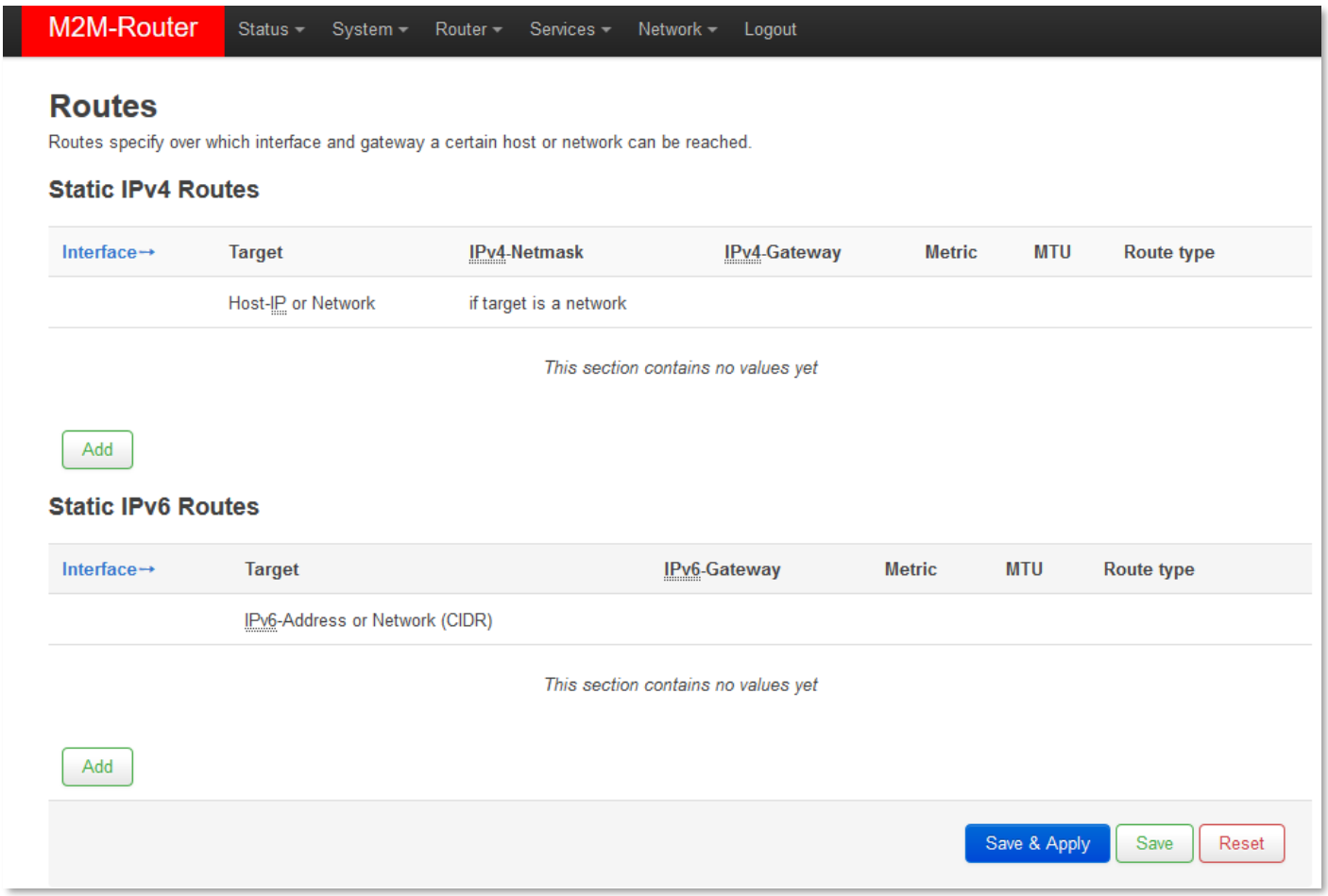
When you have modified the settings, save them by the **Save & Apply** button.

4.6 Defining the route rules

In the **Network** / **Static routes** menu you can define the rules for the current routing.

You can define a new one by the Add button.

These can be perormed by choosing the related interface and adding the **Host-IP or Network** name, the **IPv4-Netmask**, and **IPv4-Gateway**.



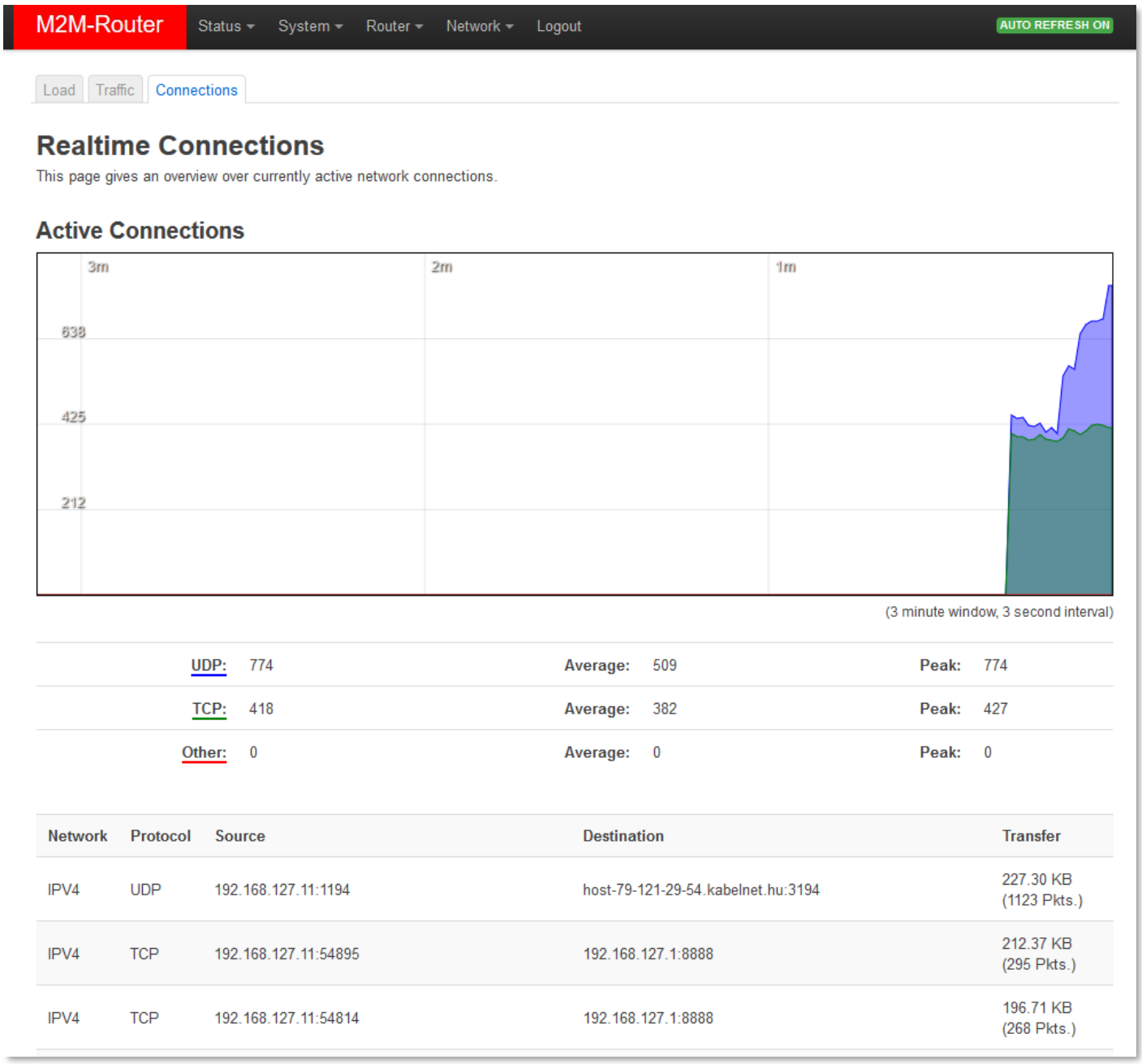
Save the settings by the **Save & Apply** button.

4.7 Firewall settings

By default, the firewall is active, but it allows all communication by default. It is necessary to limit the traffic. On public internet a device can suffer from several network attacks and getting unwanted traffic, data collection. These unwanted network activities causing the grow of the mobile network traffic and increasing the transmitted data amount (which is unnecessarily decrease the available data capacity of the SIM card).

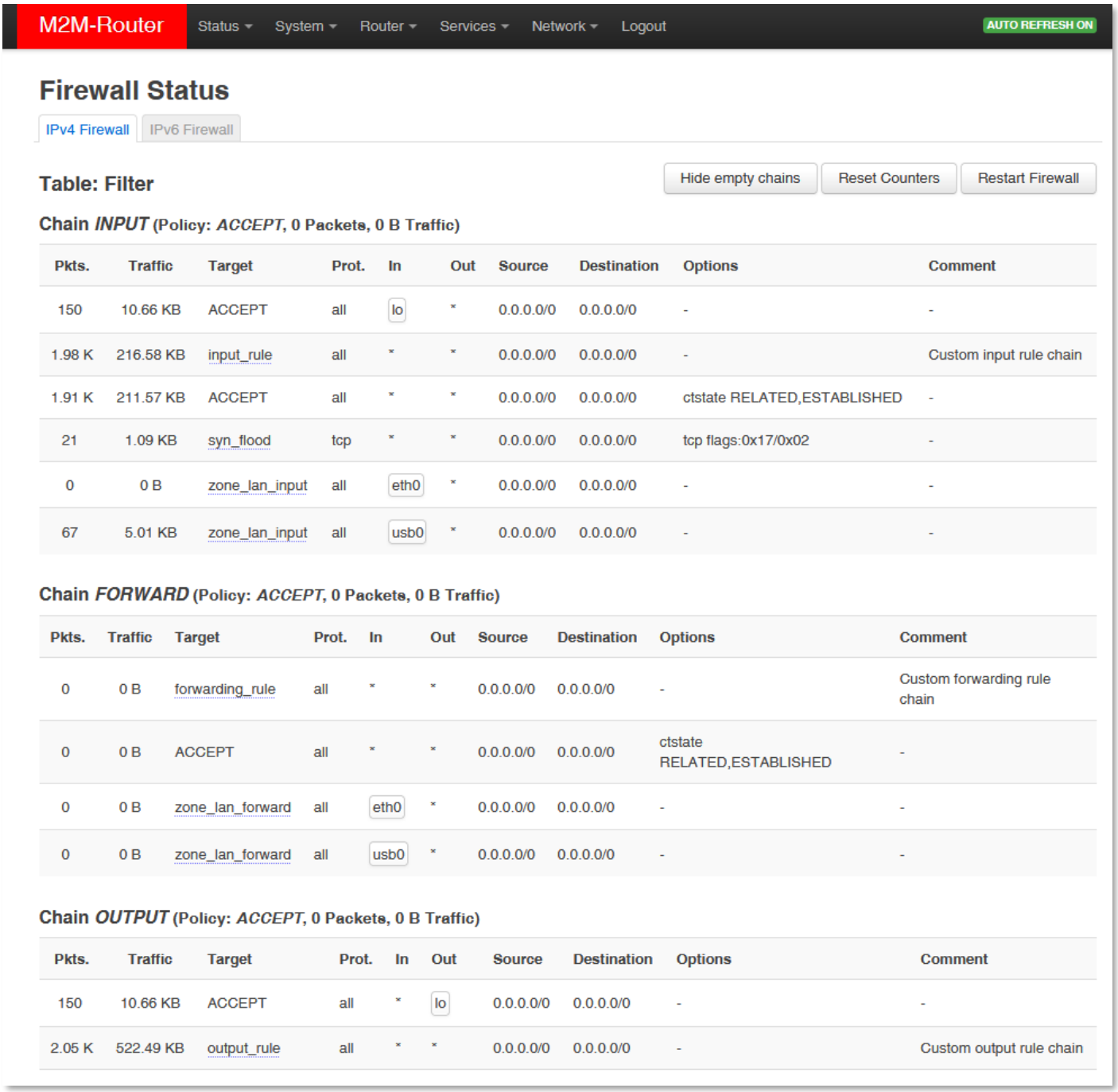
Therefore, we offer to check network traffic on the router: connections, communication channels (port number, incoming IP) and to listen incoming and outgoing network activities!

You can check these in **Status** / **Realtime Graphs** menu at **Connections** tab – where these can be listed.



If will you identify communication from an unwanted IP/port, then you have to disable or limit the occured port or IP-segment at the firewall setting rules to deny this traffic.

In the **Status / Firewall** menu you can check the firewall statistic.
The **INPUT** means the incoming, the **OUTPUT** the outgoing/transmitted and the **FORWARD** means the forwarded communication/traffic hereby. As you can see, there are several communicating IP addresses on several ports to the router and the subnet. Another method for limitation can bve the whole disabling with opening and enabling only necessary communication ports, IP-segments or allowing exact IPs.

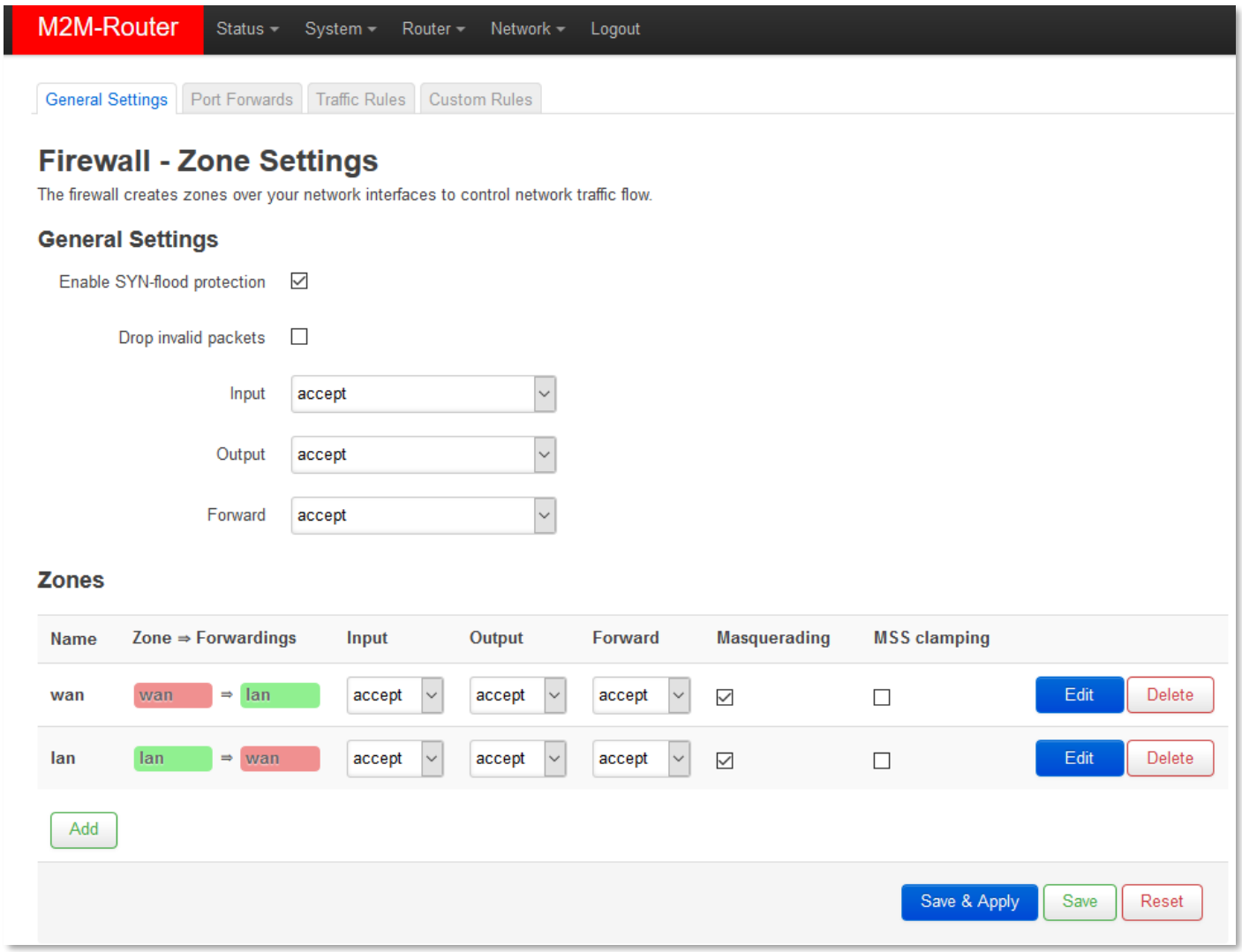


You can modify firewall settings at **Network / Firewall** menu, **General Settings** tab.

For first, the communication rules are listed here with the directions and operation of the communication rules.
Here, you can see and modify the general rules of the communication, at the **Input** (incoming), **Output** (outgoing) and **Forward** operations one by one by **accept** it, or **reject**, **drop.** You can **Delete** the settings or Edit modify.

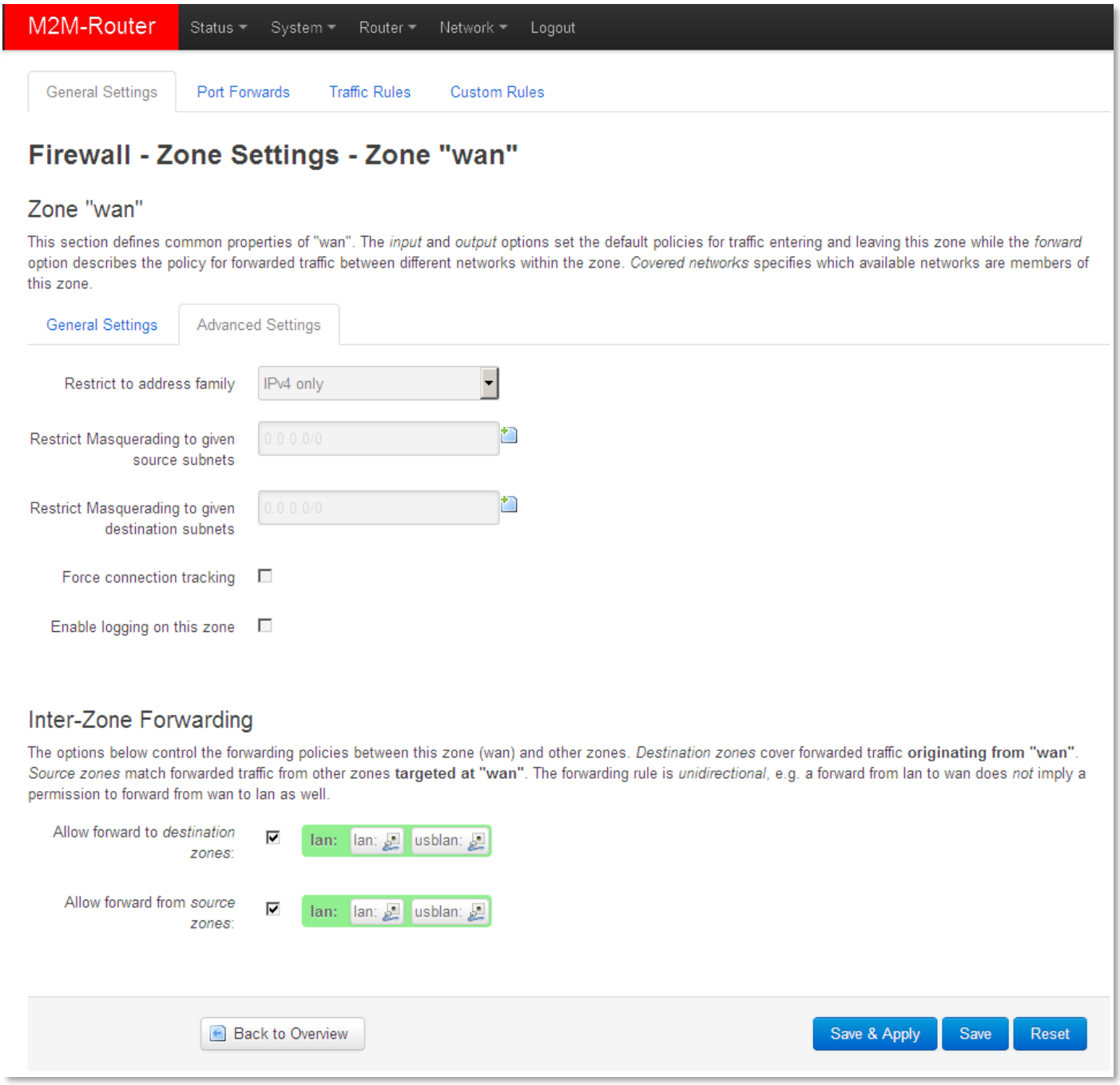
At the **Zones** part you can Add a new rule to the current ones. You also can Delete or Edit an existed rule.

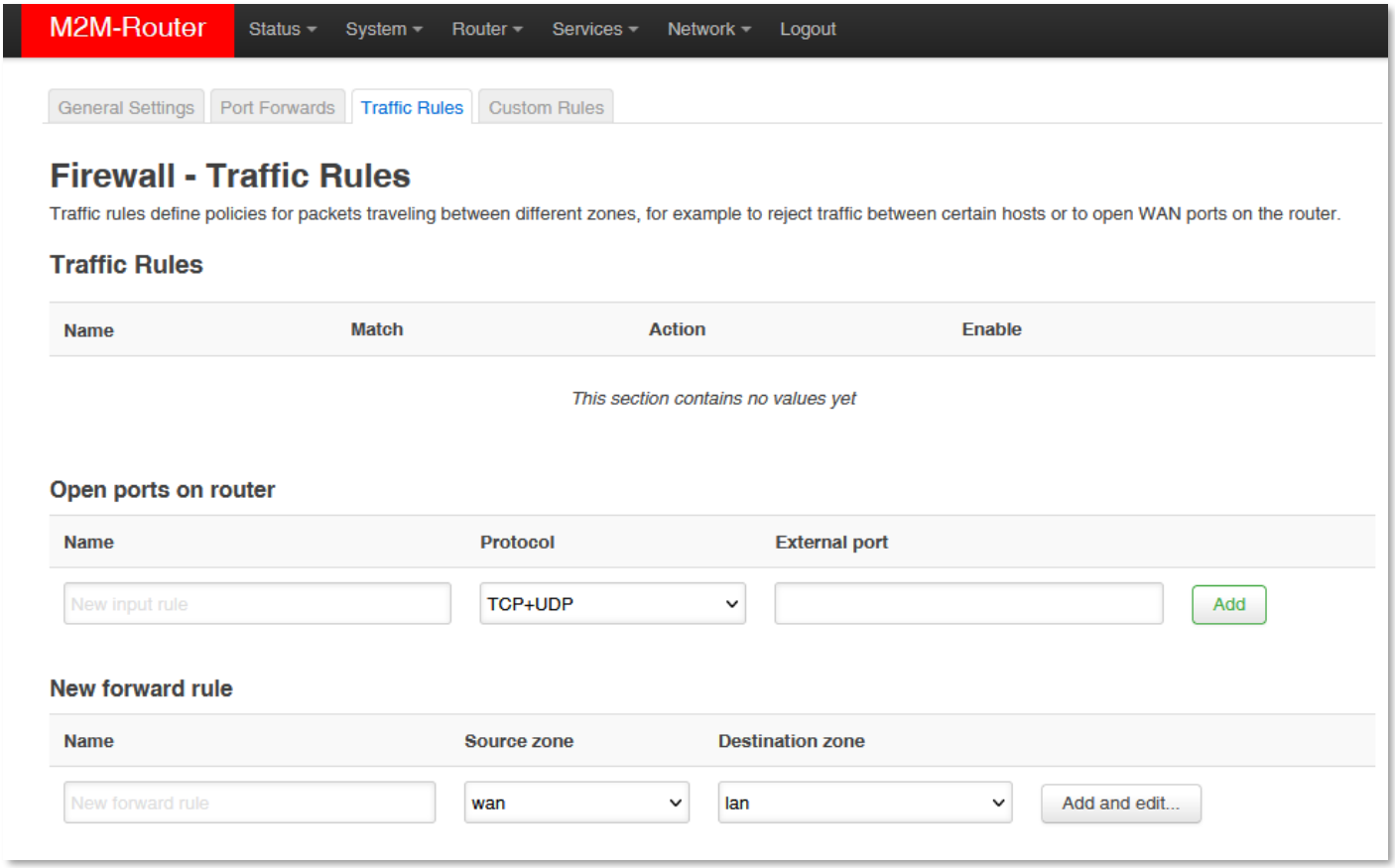
When you want to add a new firewall rule, it must be performed very carefully, because you can disable or tilt ports communication which are used by the router or some network services by general (e.g. Port nr. 67 is necessary for the DHCP service and 80 port for the, port nr. 52 for DNS, port nr. 1194 for OpenVPN, etc).



At the **Advanced Settings** tab you can limit the incoming, outgoing, and forwarded traffic for each subnets. When you have modified the settings, save them by the **Save & Apply** button.

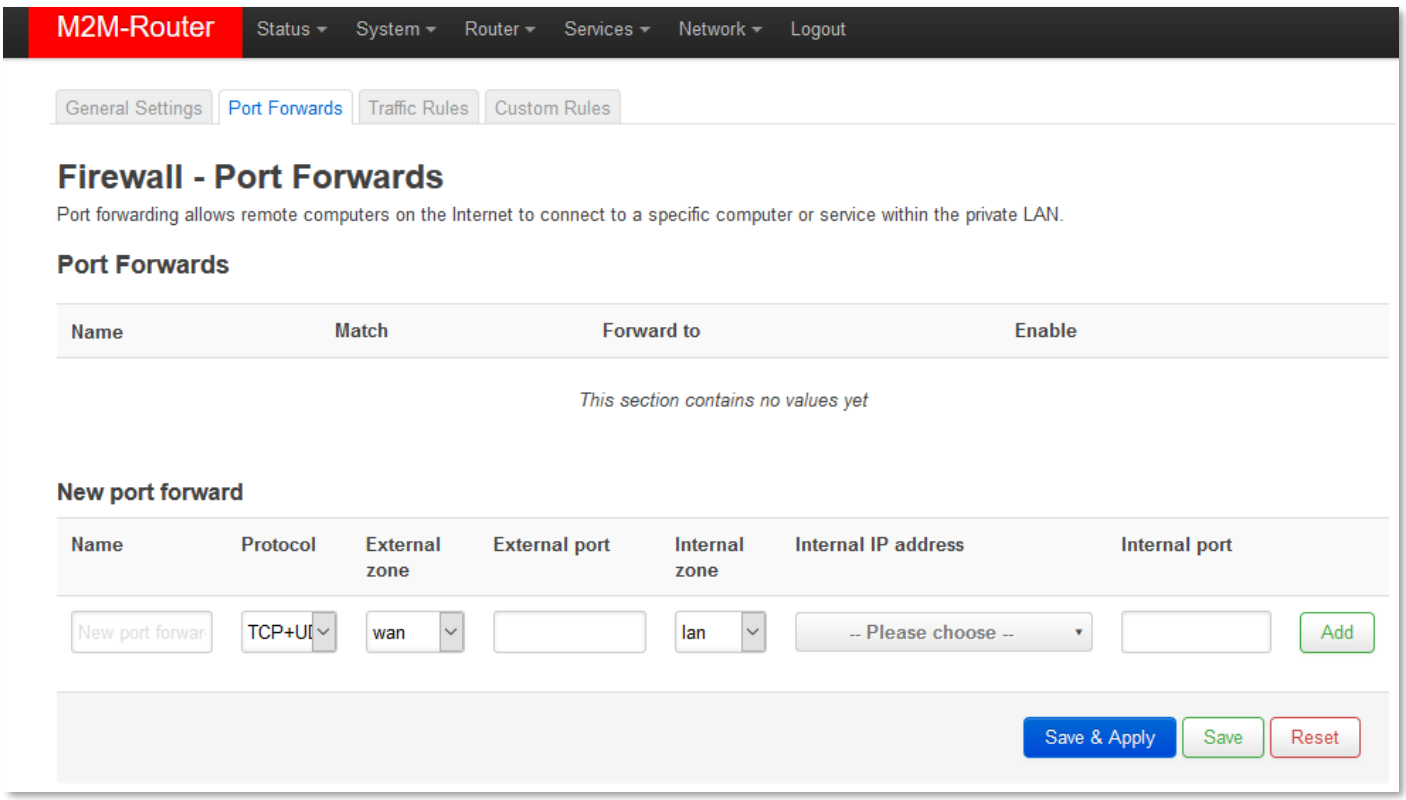
The firewall can be configured by default to allow or tilt the communication – according to the chosen settings. It won't protect the router against external network attacks or intrusions when just enabling the firewall feature.
Further port-level filtering or interface traffic limits, or **Traffic Rules** settings are necessary to define! When you have modified the settings, save them by the **Save & Apply** button.





4.8 Port Forward settings

Here in the **Network**/**Firewall** menu, **Port Forwards** tab you can setup, that which port forwarding rules should be valid. Here you can add the necessary ports and IP adresses.

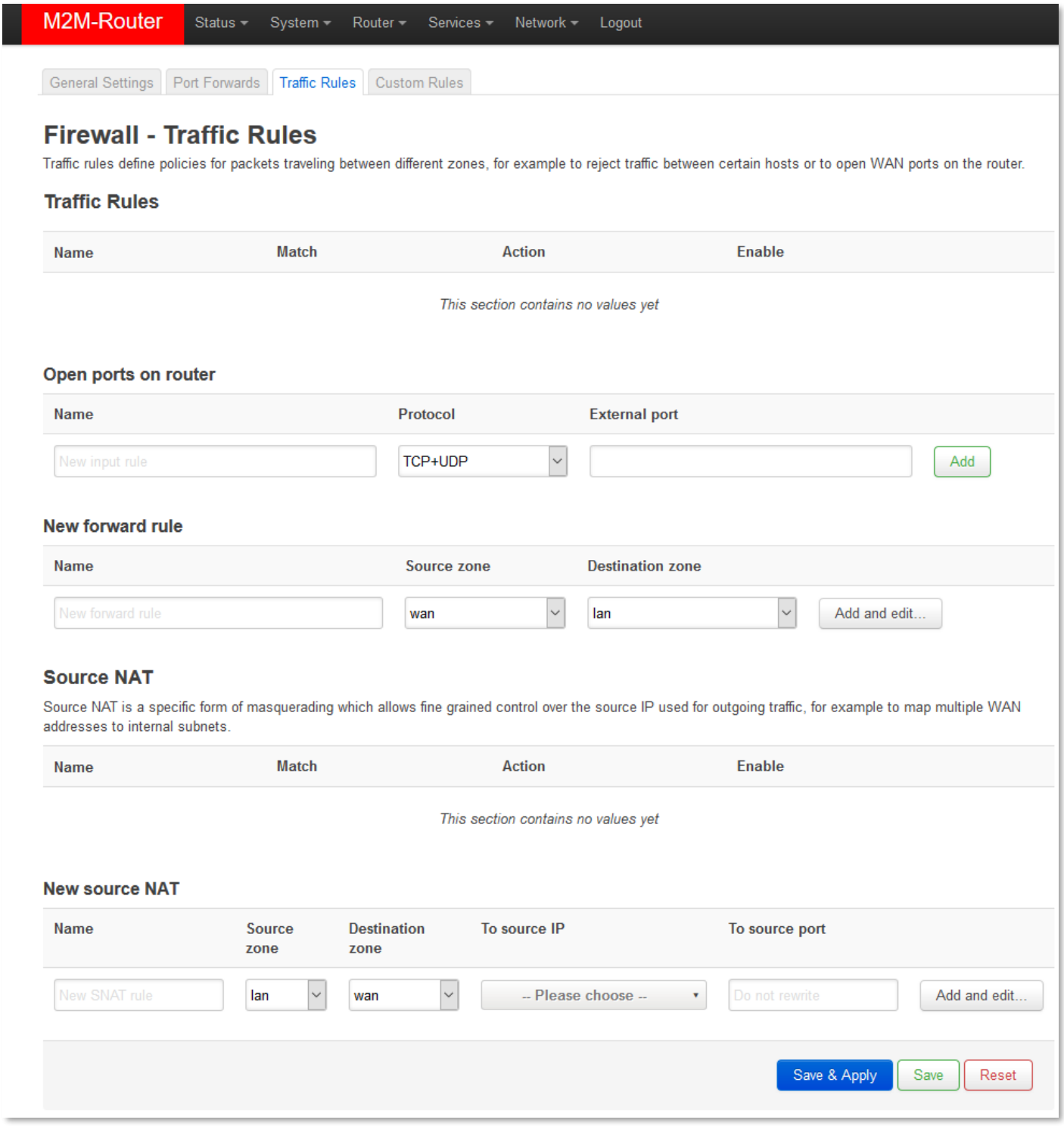


You can define the necessary port and IP address. Or you can add a new rule by the Add button.

When you have modified the settings, save them by the **Save & Apply** button.

4.9 IP routing, NAT settings

In the **Network** menu, **Firewall** item, **Traffic Rules** tab you can setup the **Traffic Rules**, and the **Source NAT** settings.



You can add a new rule by the Add button. When you have modified the settings, save them by the **Save & Apply** button.

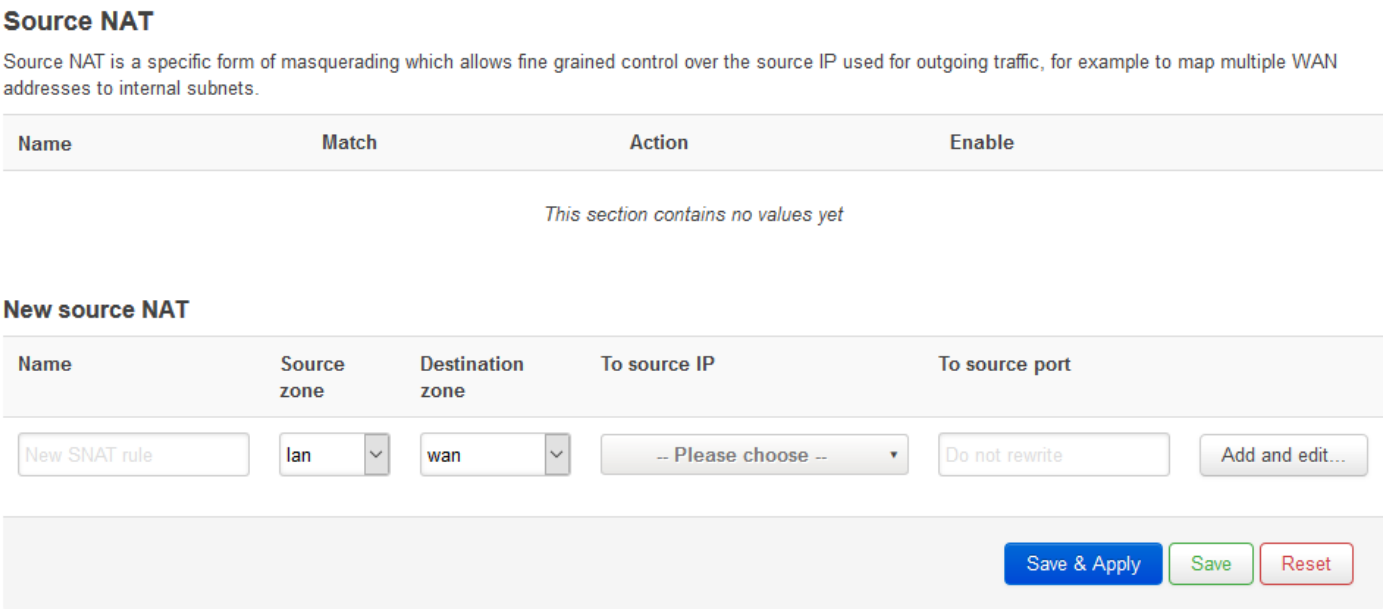
Here you can open ports (e.g. for TCP) for the packages, or you can define new forwarding rule settings for the interfaces (**New forward rule**).

Always set the rules carefully so as not to exclude the possibility of basic communication, and you should also make sure that the router remains available on the network, because it is easy to exclude ourselves or just the possibility of remote login.

You should find out about the standard port numbers used by each service (E.g. FTP: port 21, SSH/Telnet: port 22, web: port 80, etc).

Properly designed port filters and rules minimize communication, which is very important from a data traffic point of view, and can minimize the risk of an open vulnerability. It's a good idea to set the rules so that only the most necessary services and ports can distribute data on the network.

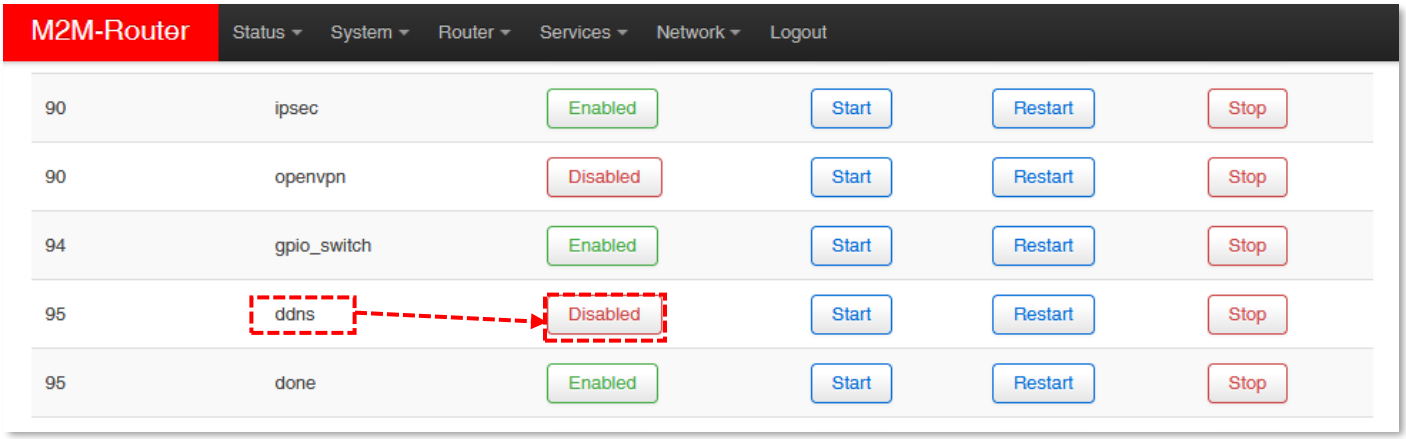
The **Source NAT** settings can be performed for each protocol (tcp, udp), that the router allows the redirection of data – which incoming IP address and port must be redirected to which outgoing IP address and port and must be forwarded the data traffic. You also can define a port range, hereby.



If you have modified the settings, save them by the **Save & Apply** button.

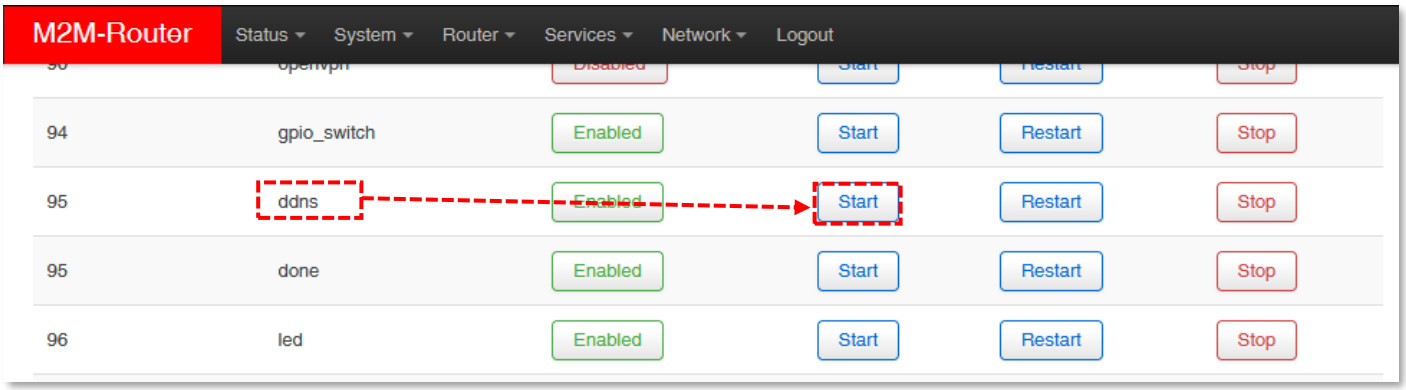
4.10 Dynamic DNS settings

First you have to start the *Dynamic DNS* service. Open the **Systems / Startup** menu to enable the feature.

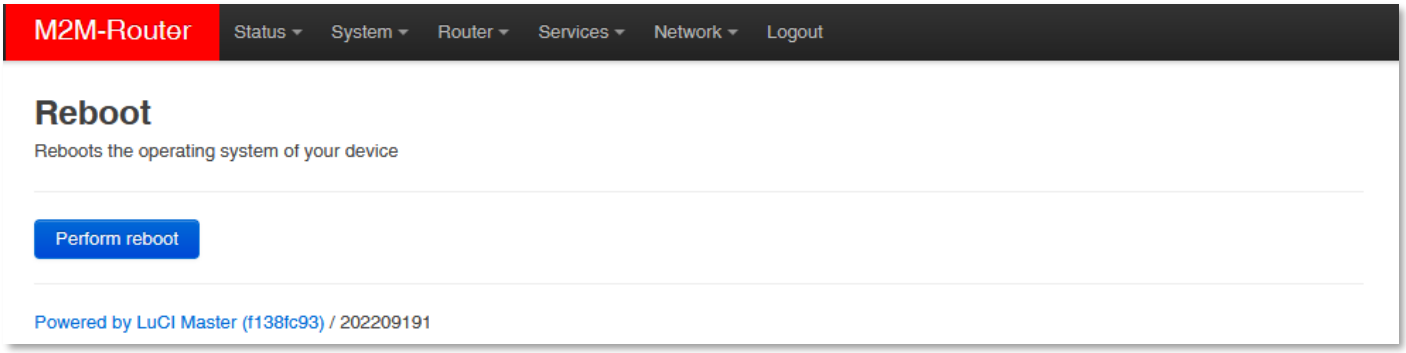


Roll down to the „**ddns**" feature and push to the Disabled button to initialize the service. Then wait until the service list will be refreshed and the „**ddns**" will be listed as an Enabled service.

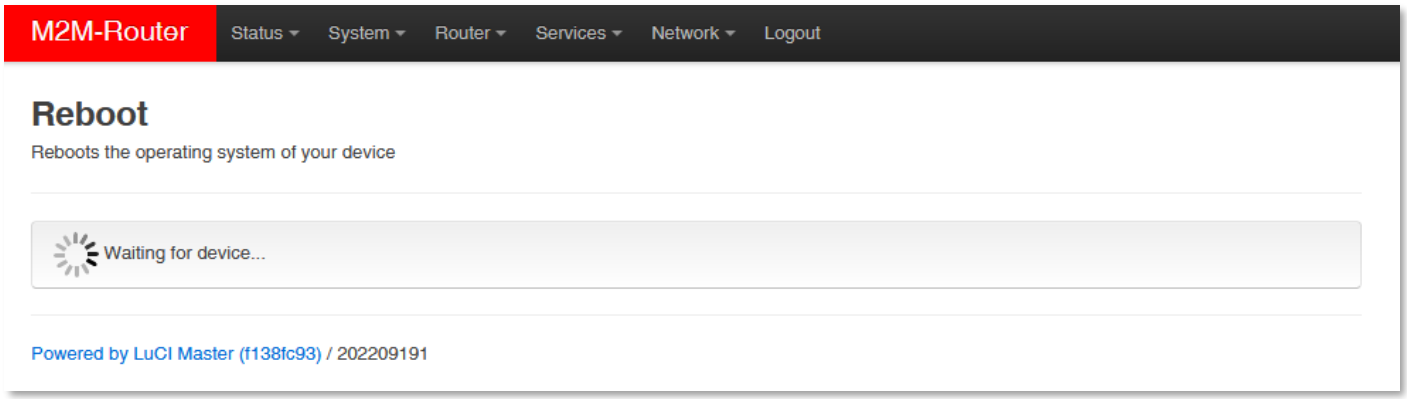
Then push to the start button of the line of the „**ddns**" service to start the feature.



Then restart the device from the **System / Reboot** menu.

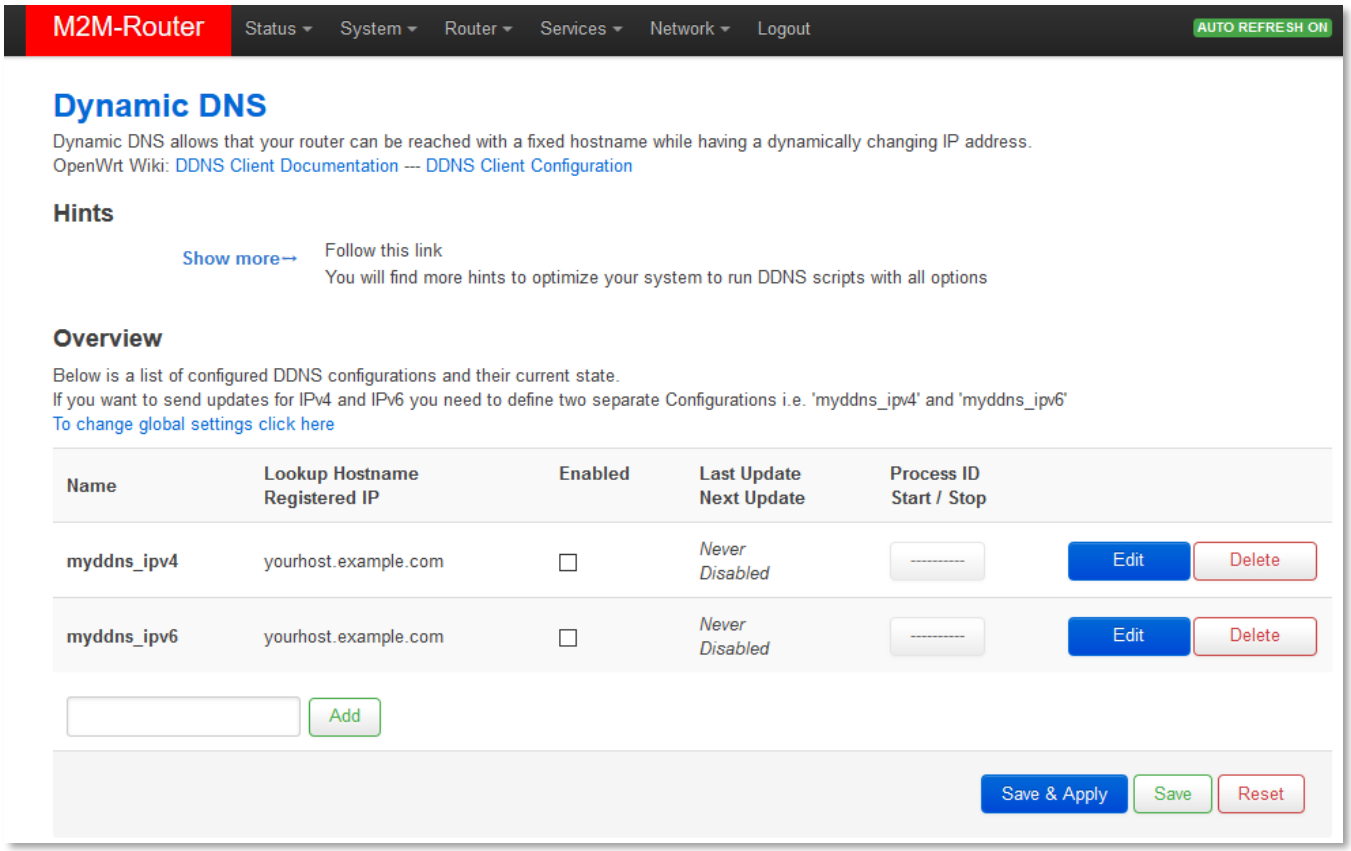


There push to the Perform reboot button.



After the restart, you have to log in again and configure the „**ddns**" service.
For that, in the **Services / Dynamic DNS** menu you can allow the DDNS service providing and the IP address of the DDNS.

New settings can be Add by the button or the current can be changed by the Edit button – even for IPv4 or IPv6.



When you have modified the settings, save them by the **Save & Apply** button.

Chapter 5. Special settings

5.1 Device Manager® settings

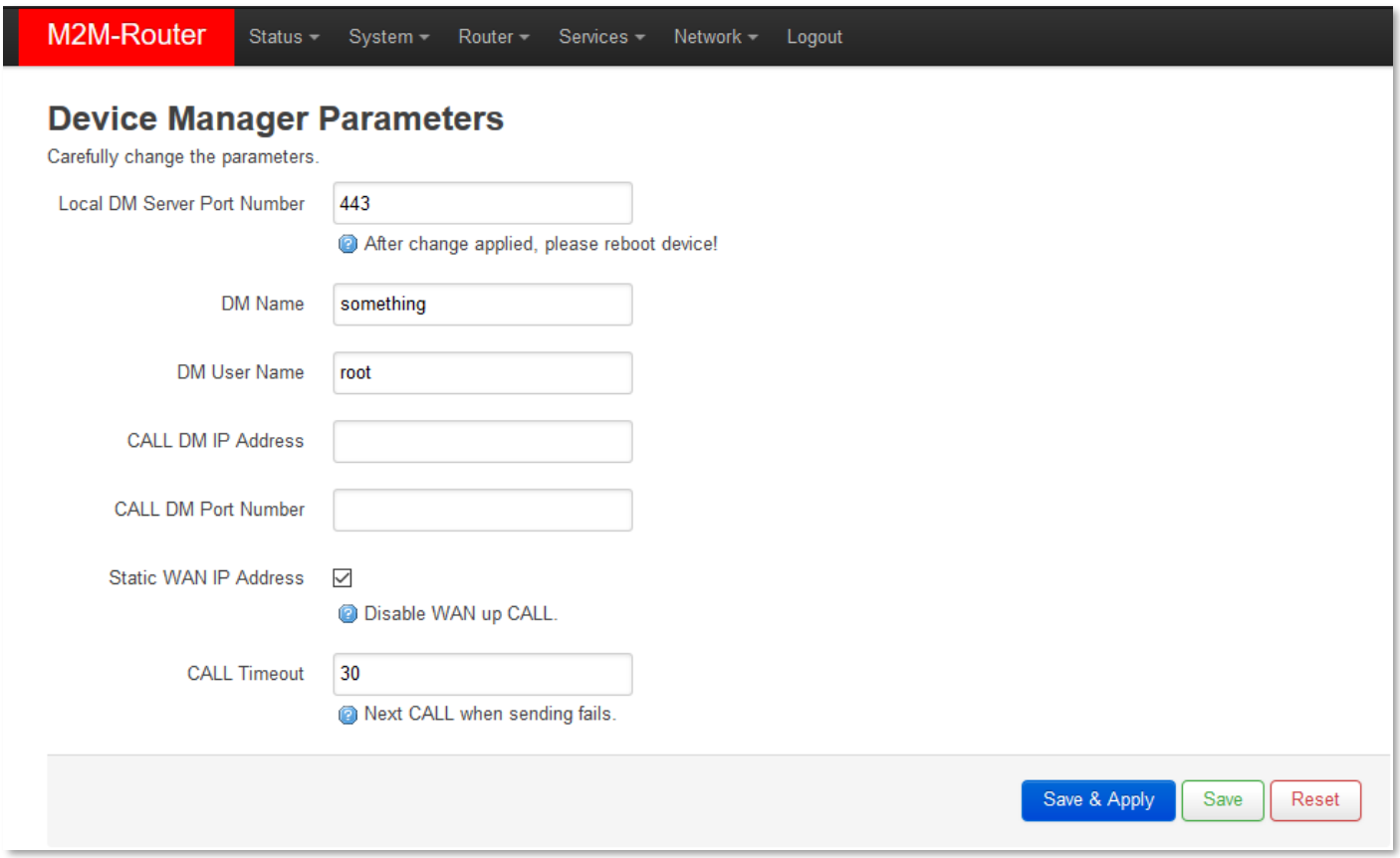
Our Device Manager® application can be used for the remote management of the router, which is used for the remote maintenance and reconfiguration of the router in addition to the continuous monitoring of the operating characteristics (network access, field strength, runtime, QoS). In addition, it is possible to replace and install the firmware running on the device. You can manage thousands of routers from this program in this way.

The requested settings can be made individually or for a group of devices in one step.

To use the application, you need to purchase a license, please contact our Dealer.

More info: https://m2mserver.com/en/product/device-manager/

The *Device Manager* settings can be defined in the **Router / Device Manager** menu.



The main importants are the **DM IP Address**, the **DM Port Number** and **DM User Name**.

The default DM Port number is **443**.

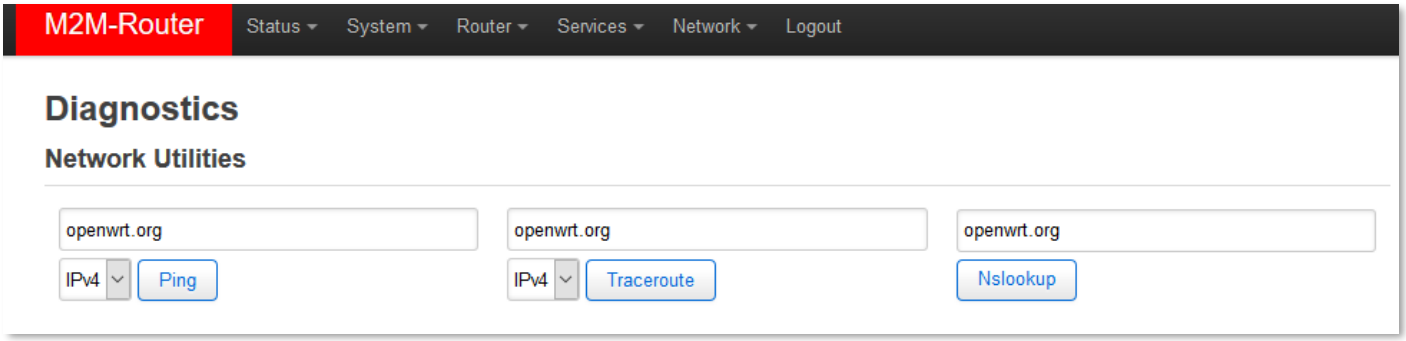
If you modified the settings, save them by the **Save & Apply** button.

IMPORTANT!

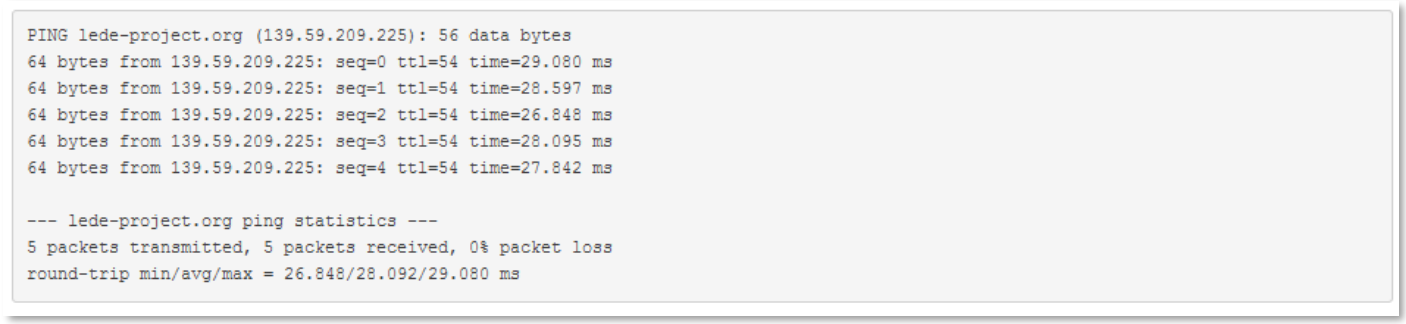
These must be also configured in the Device Manager and the router must access the IP address of the Device Manager server (where the application is executing remotely). You can check that it is accessed by performing a ping.

5.2 Ping an IP address

Open the **Network** / **Diagnostics** menu.



Here you can check the availability of an IP address, that is it accessible or can be pinged (by Ping button), is there a naming service provided, is there a response between two points (by Nslookup button), furthermore the path of the communication (by Traceroute button).



Important!

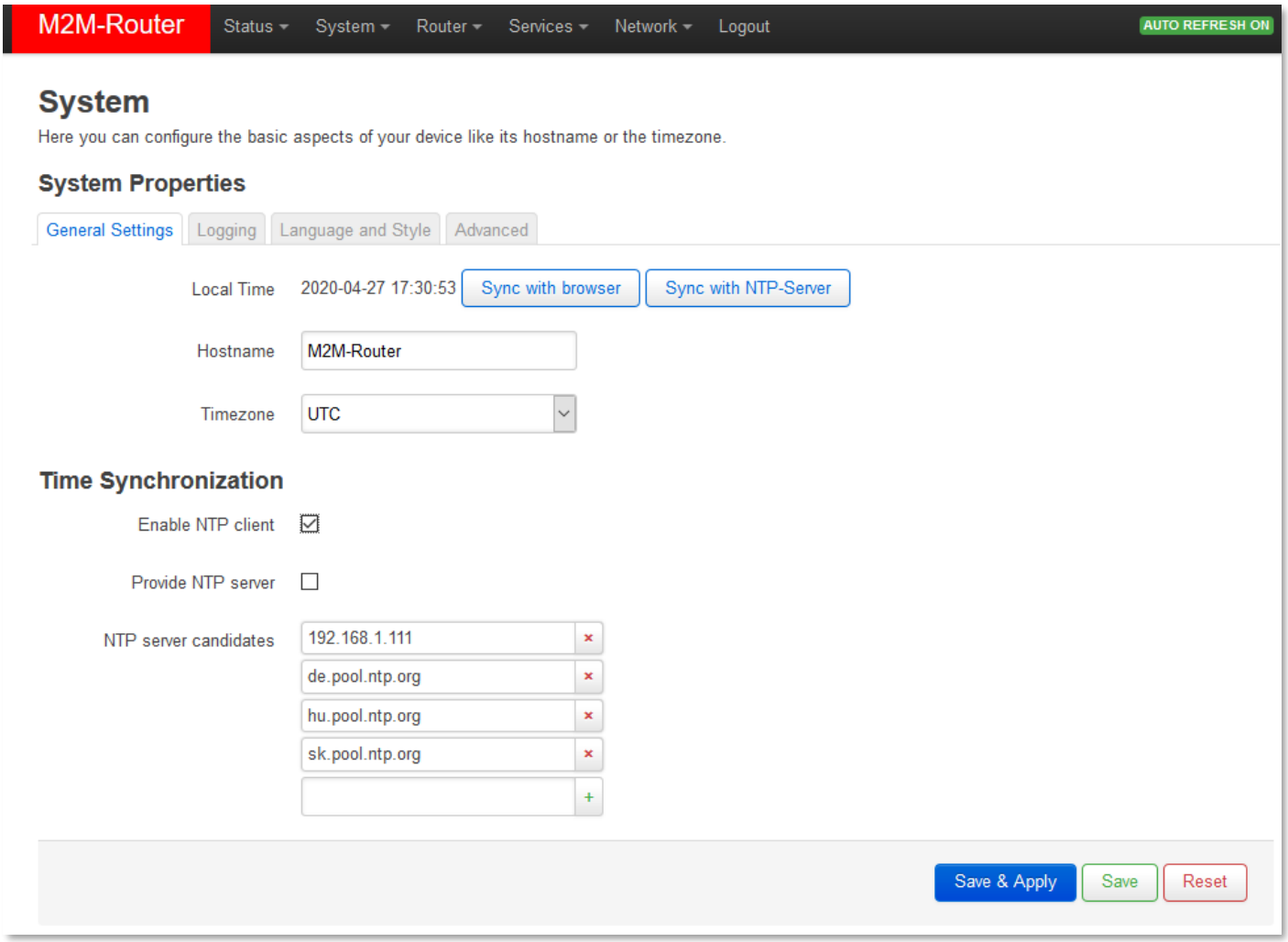
Check only IP addresses, which are available to access from the current IP segment and APN zone for sure (e.g. from an enclosed APN zone the router will not access the public internet, and from the public internet it will not access the enclosed M2M APN zone).

In case of M2M APN the 192.168.1.250 address can be accessed, it is possible to ping the address for checking the 3G network connection.

5.3 Network Time Service (NTP)

Open the **System / System** menu, **Time Synchronisation** part.

You can add hereby the refresh interval at the **Update interval (in seconds)**.



Here, you can setup the **timezone** can enable or disable the **NTP client** function (when receiving time data) and provide NTP time to connected devices (**Provide NTP server**). You can also specify the addresses of the NTP servers (**NTP server candidates**).

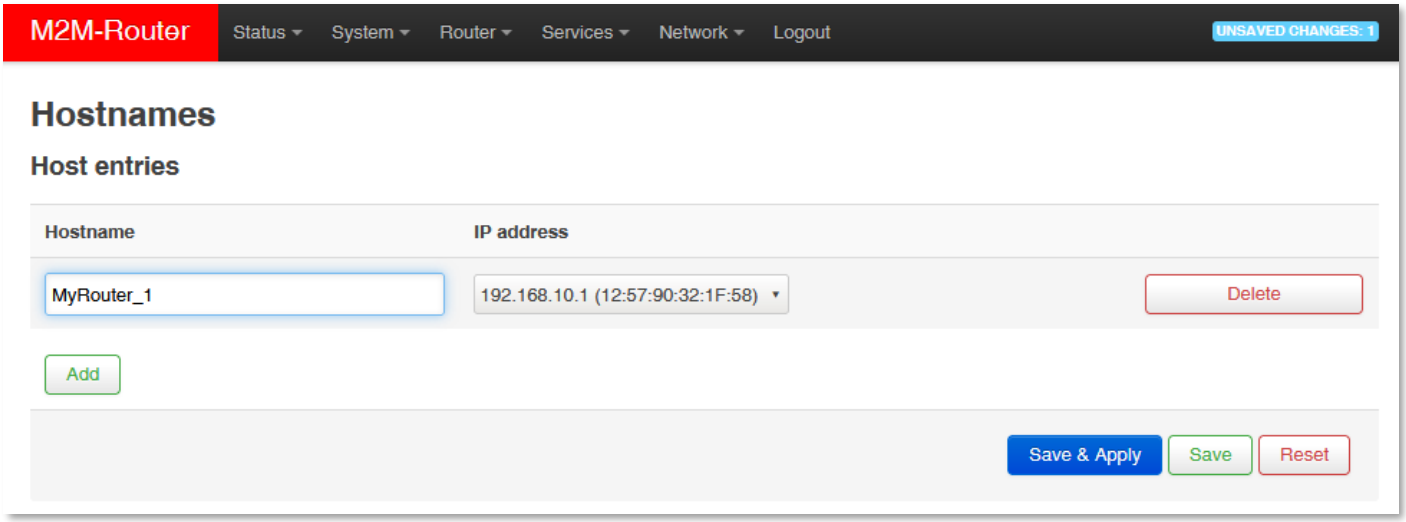
If you have modified the settings, save by **Save & Apply** button.

5.4 Identification of connecting devices

Open the **Network** / **Hostnames** menu.

Here you can register network devices that use a router connection to more easily identify them.

You will also see the logical names entered here for IP addresses on the status page as they connect to the router.



You can assign the selected hostnames to the IP address with the Add button, then if connected, the clients will appear in the **Status / Overview** menu item on the main page with this name.

If you have modified the settings, save by **Save & Apply** button.

5.5 TFTP settings

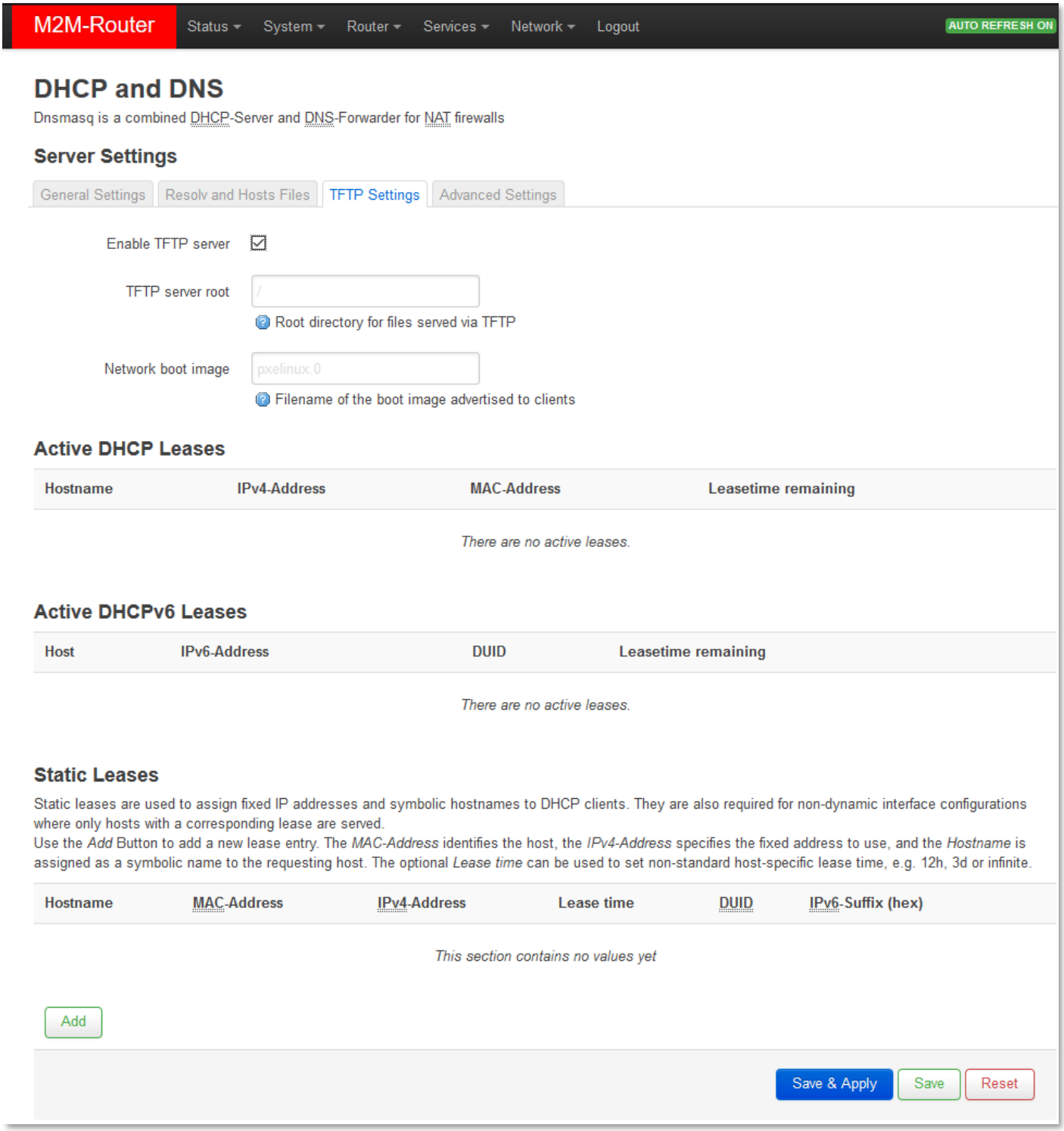
Open the **Network / DHCP and DNS** menu.
Here on the **TFTP settings** tab you can enable the TFTP server (**Enable TFTP server**) and enter additional information about it.

The FTP service can be useful for forwarding the data of connected devices and meters via ftp - to a server, remote IP address.

To enable the TFTP server, you must enter the following server information: **TFTP server root, Network boot image.**

Of course, you can also use SFTP on your router by sending the data to IP addresses by entering your account and password information. if you need more help, see the OpenSSH Linux command line settings.

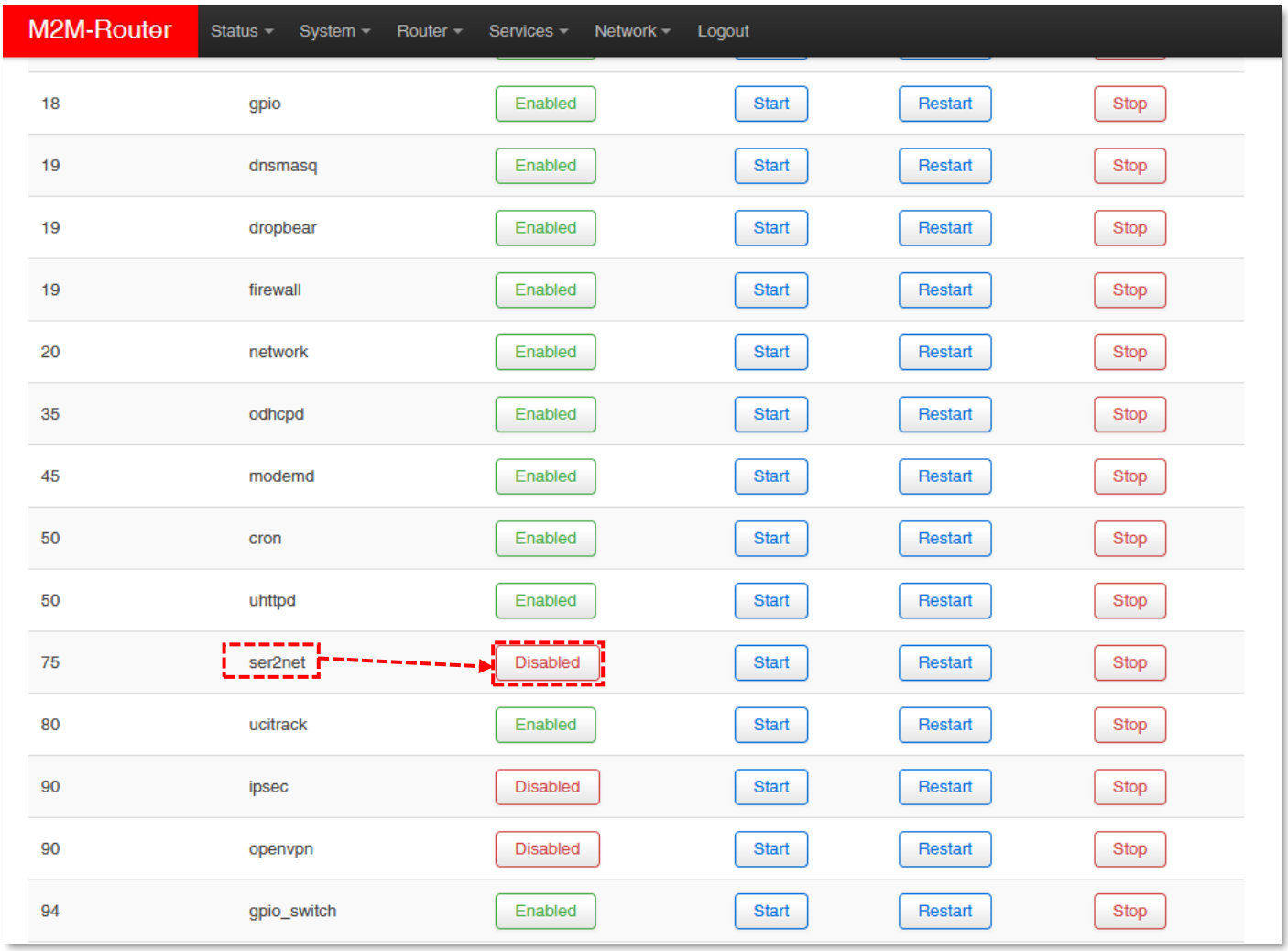
If you have modified the settings, save by **Save & Apply** button.



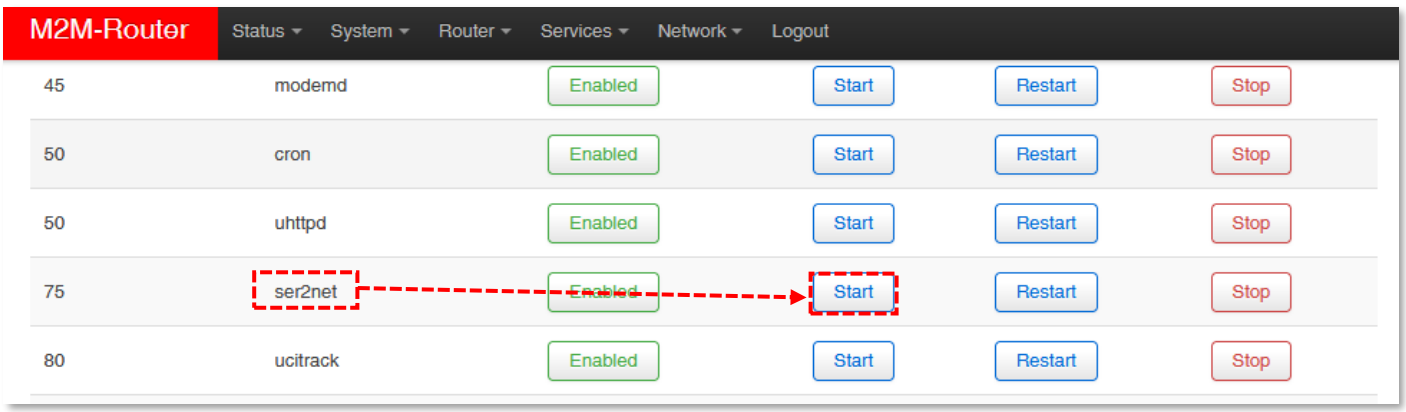
5.6 RS485 settings (Ser2net)

First you have to start the „**ser2net**" service. Open the **Systems / Startup** menu to enable the feature.

Roll down to the „**ser2net**" feature and push to the Disabled button to initialize the service.

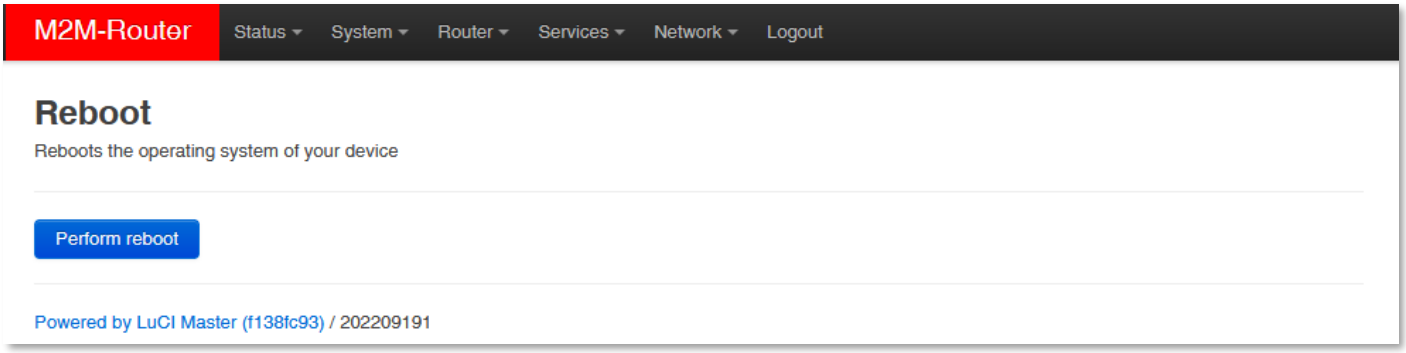


Then wait until the service list will be refreshed and the „**ser2net**" will be listed as an Enabled service.

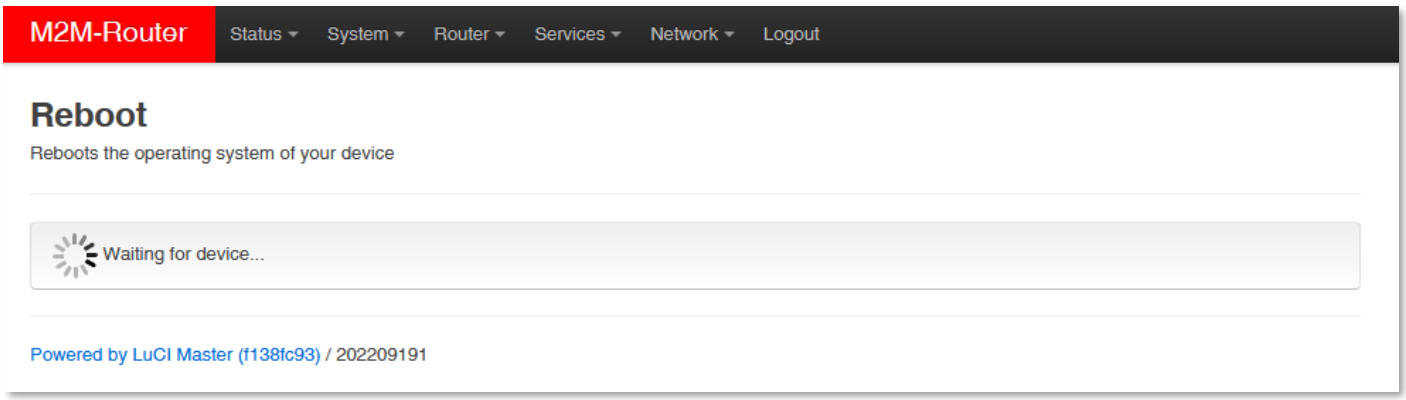


Then push to the start button of the line of the „**ser2net**" service to start the feature.

Then restart the device from the **System / Reboot** menu.



There push to the Perform reboot button.



After the restart, you have to log in again and configure the „**ser2net**" service.

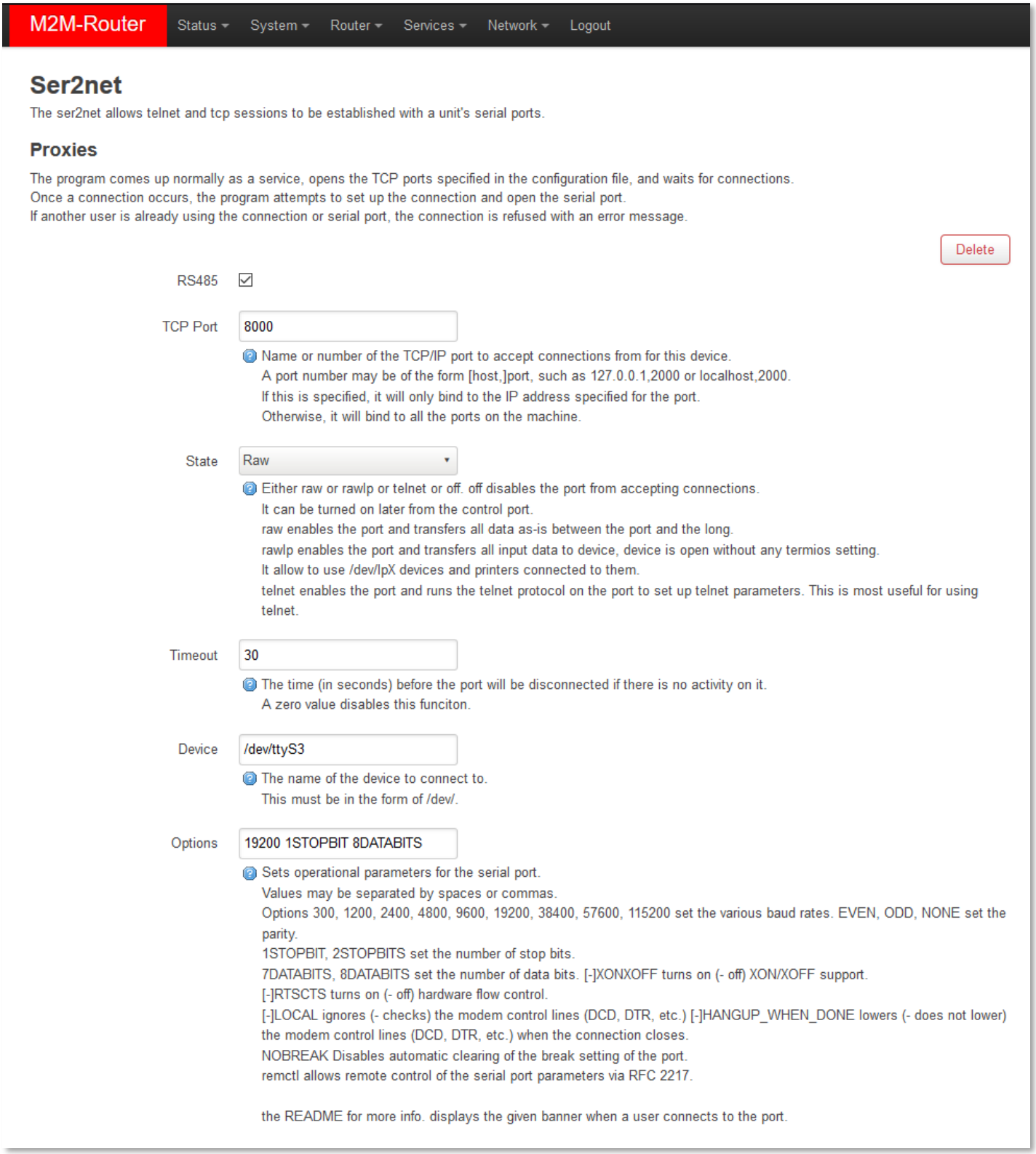
To configure the RS485 port, open the **Services / Ser2net** menu. Here you can define the properties of the incoming transparent data transmission.

At the **Proxies** section, enable the **RS485** option to activate the communication.

Then define the **TCP Port** number (which is port no. 8000 by default).

In the **State** field, the data format can be set:

- *off*: no data stream
- *raw*: full duplex
- *rawlp*: one-way communication
- *telnet*: for further use



For the **Timeout** value, you can specify the amount of timeout (in seconds) – default value is 30 seconds, 0 value means transparent transmitting without delay.

Do not change the value of the **Device** field!

Options: A complex parameter with **Baudrate** selection + **Stopbit** definition + **Databits** definition + **Parity** type

- **Baudrate** (default is *9600* bps for the RS485) can be defined between 300 bps and 115 200 bps.
- **Stopbit** value can be 1 or 2
- **Databits** value can be 7 or 8
- **Parity** value can be EVEN, ODD or NONE

Examples:

For standard speed 7E1 mode use this command: ***9600 1STOPBIT 7DATABIT EVEN***

For lower speed 8N1 mode use this one: ***2400 1STOPBIT 8DATABIT NONE***

Important! *Note that maximum 115 200 baud speed rate can be used wheather of the configuration options.* ***But, we offer to use the standard 9600 baud or 2400 baud speed rate for receiving or transmitting data without character / data loss.***
The incoming RS485 data are not stored locally, they will be transparently transmitted from the device through the cellular network.

Note, that you should add the specified RS485 port number to the **Firewall** rules (**Network / Firewall** menu), otherwise the router will not receive any data.
You can also specify additional members, such as *hardware flow control* with the **RTSCTS**, which can be turned off with the "**-**" prefix. A ***space*** character must be placed between members.

If you have modified the settings, save by **Save & Apply** button.

You can connect an **IIoT IO/RS485 concentrator** to collect input signals, readout status of digital inputs: https://m2mserver.com/en/product/iiot-io-data-concentrator-16di/

Important!
In case of Modbus / RS485 interface connector you can use the router with the RS485 settings as a transparent Modbus gateway without any change.
If you have special request on Modbus, indicate or declare your interest with details by ordering. We can provide a customized command line interface operated special modbus program for the needs.

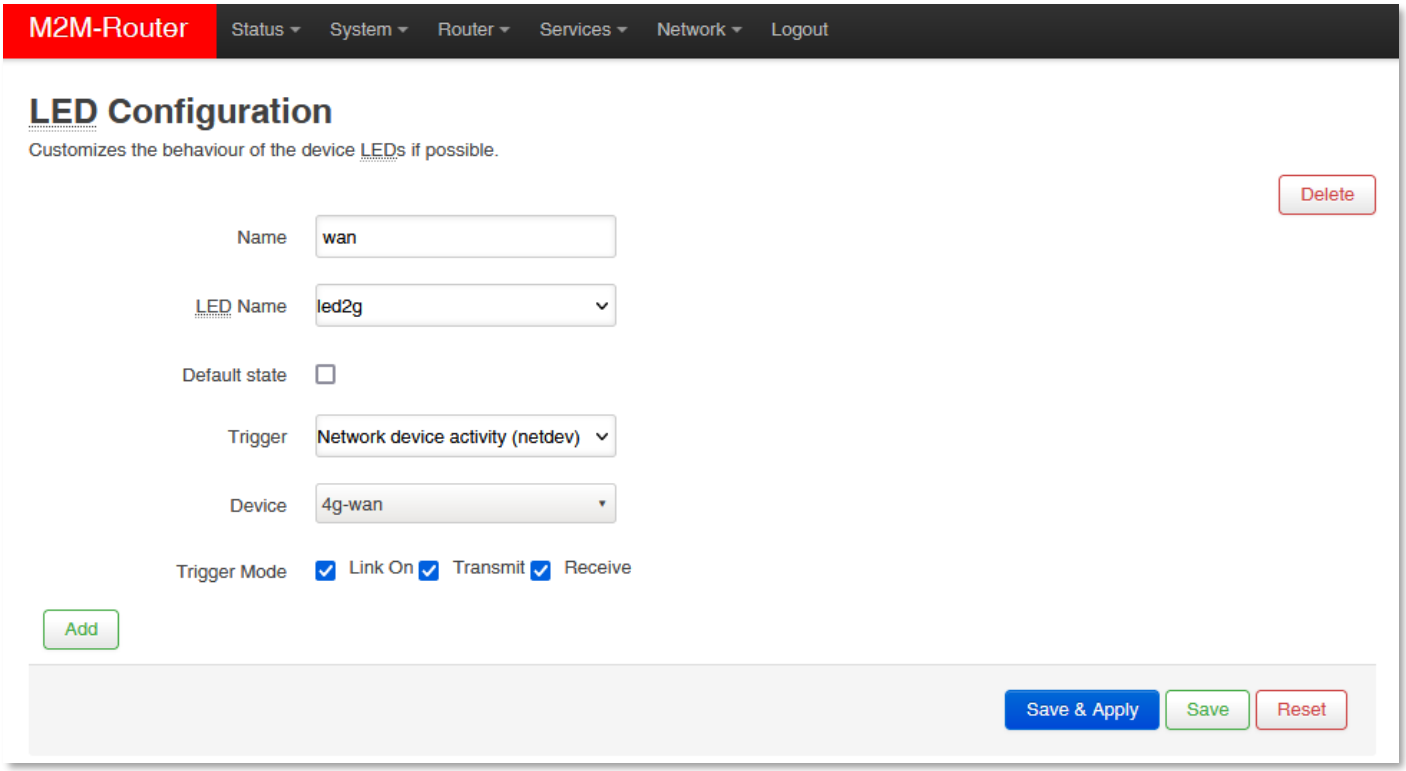
5.7 LED configuration

Open the **System / LED Configuration** menu. Here you can specify the rules for the LEDs for each LED status.

Use **Name** to add a name for a rule. Under the **LED Name** you can select which **LED status** you want to set:

- *leg2g* – **LED2 green** light
- *led1r* – **LED1 red** light
- *led2r* – **LED2 red** light
- *led3r* – **LED3 red** light

Only free LEDs that are not reserved are displayed.



From the **Trigger** list, you can select which event to affect. E.G. for netdev, indicates the status of the network connection, and under Device, you can specify which interface it applies to.

This **Trigger** allows to choose an event type of operation. E.g. *netdev* menads the network interface connection type, and **Device** identifies the related network interface.

You can Add a new one, or Delete a LED setting.

When you have modified the settings, save them by the **Save & Apply** button.

5.8 Remote access (SSH)

The device can be accessed remotely, including its settings - which you can change remotely.

Remote access is via the mobile network, the IP address range of the SIM card. Therefore, the device must be on the public Internet or in the same zone from which you want to access the device. Remote access is also possible via SSH and FTP.

You can specify remote access from the external zone between the **Network / Static routes** and **Network / Firewall** settings by enabling the port and IP range and subnet masks for specific interfaces as *transmit / receive data*.

Provide remote access via SSH, web interface, and voice dialing by enabling certain commands to a specific phone number.

SSH connection

The router can also be accessed over an SSH connection, with a terminal program (e.g. the software called *putty*), at the IP address of the router - e.g. **192.168.127.1:22** (port # 22 on the **Ethernet** port).
The same is possible at **192.168.10.1:22** - for the **USBLAN** port.

Allow the Putty program to access SSH by pressing the OK button under the security message “Security Alert of the RSA2 key of the router to allow and trust the connection”. You can now access the OpenWrt® Linux command line.

SSH login:
Login as: ***root***
Password: ***wmrpwdM2M***

Here you can use micro uCLinux kernel 4.9 compatible commands or execute scripts.

The router's operating system uses the embedded Micro uClinux kernel version 4.9 and interprets ***UCI Command line interface*** commands - see. For downloadable commands, see the downloadable guide for more information.

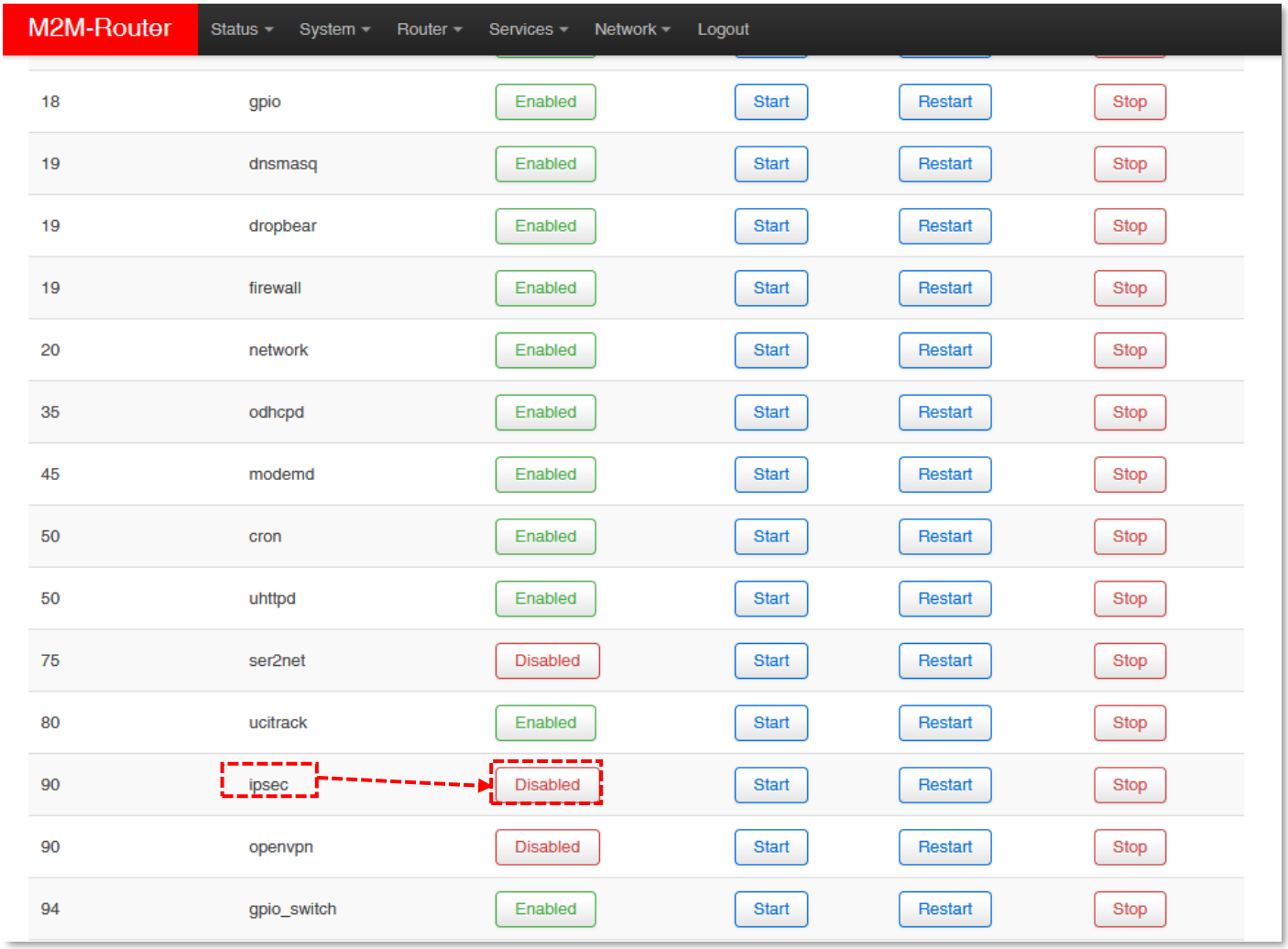
5.9 UCI usage from the command line

The UCI® (Unified Configuration Interface) is an OpenWrt® API / utility that allows centralized configuration and further management of the OpenWrt® system.

To review the useable UCI commands and options that can be used, we recommend to read the UCI guide, which can be downloaded from our website:
https://www.m2mserver.com/m2m-downloads/UCI_Command_Line_Reference_v3.pdf

5.10 IPSEC settings

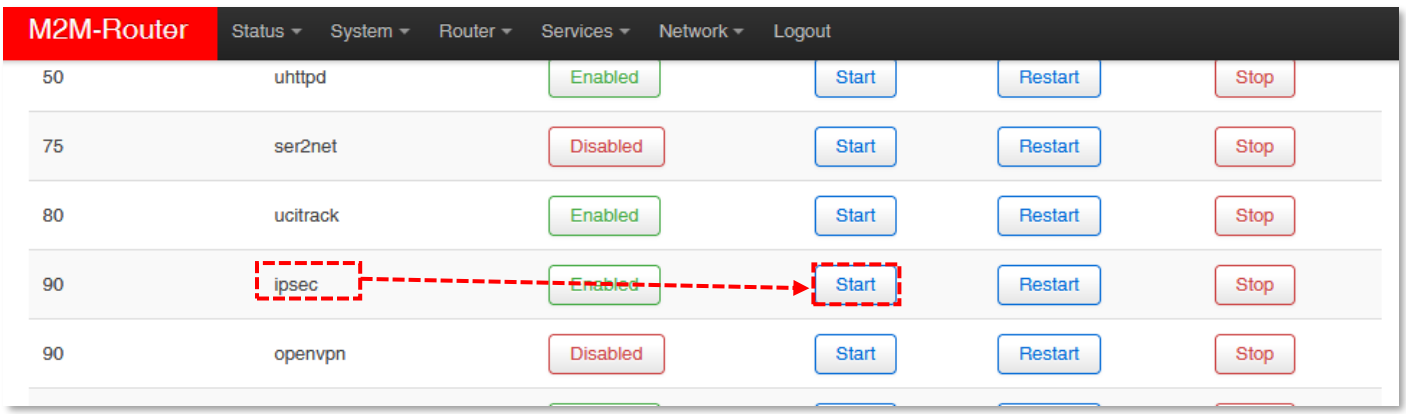
Open the **Systems / Startup** menu to enable *strongSwan* IPSec feature.



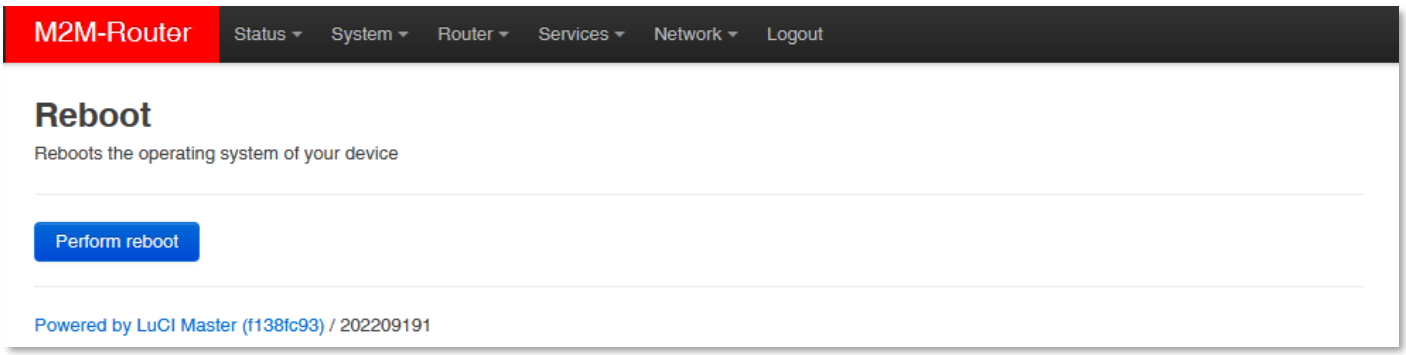
Roll down to the „**ipsec**" feature and push to the Disabled button to initialize the service.

Then wait until the service list will be refreshed and the IPsec will be listed as an Enabled service.

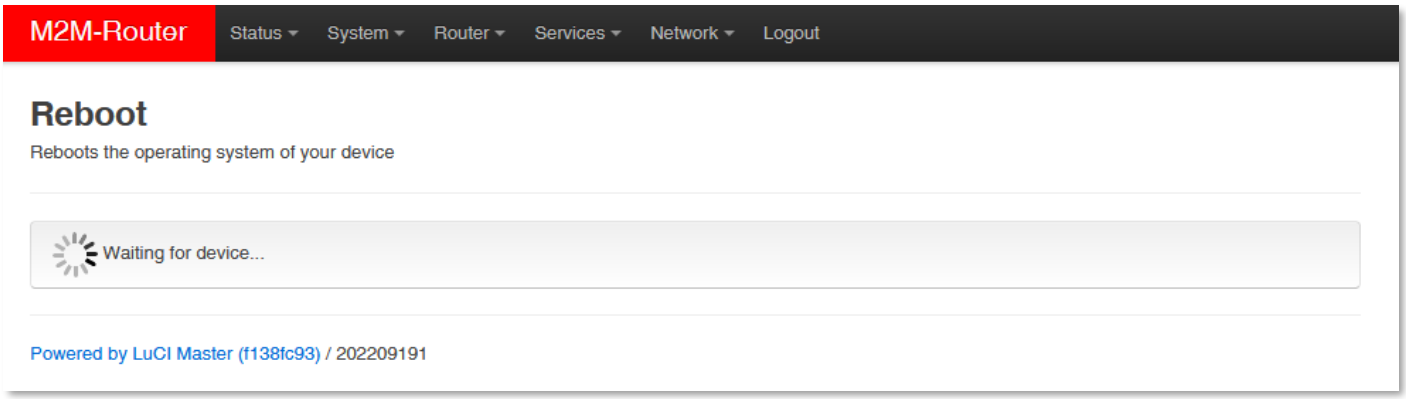
Then push to the start button of the line of the IPSec service to start the feature.



Then restart the device from the **System / Reboot** menu.



There push to the Perform reboot button.



After the restart, you have to log in again and configure the *strongSwan* IPsec.

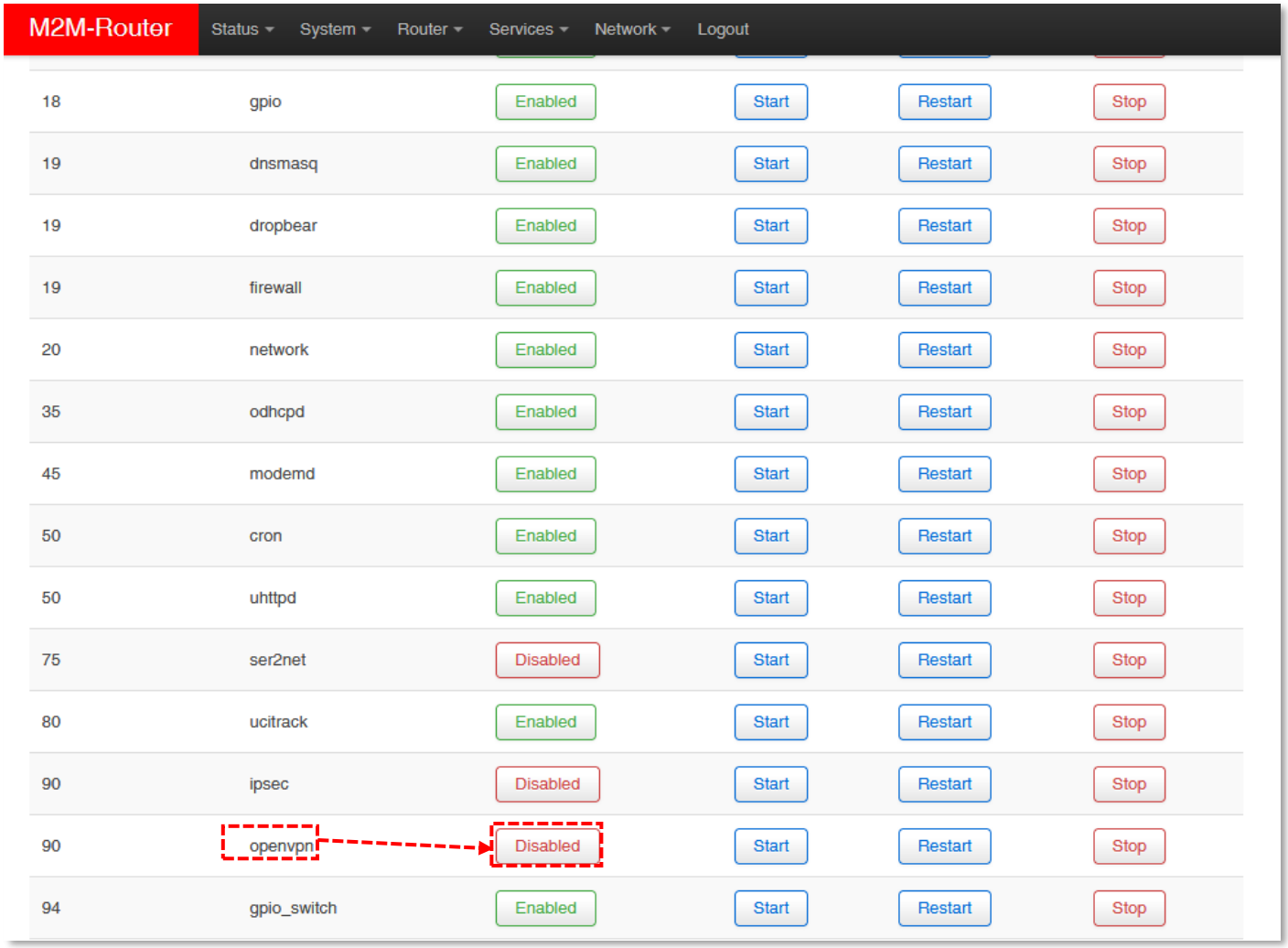
You can configure the service through ssh connection, from command line.
Read the OpenWrt website for more information on possible IPSec settings:
https://openwrt.org/docs/guide-user/services/vpn/ipsec/strongswan/start

5.11 VPN client (OpenVPN) configuration

First you have to start the OpenVPN service. Open the **Systems / Startup** menu to enable *the OpenVPN* feature.

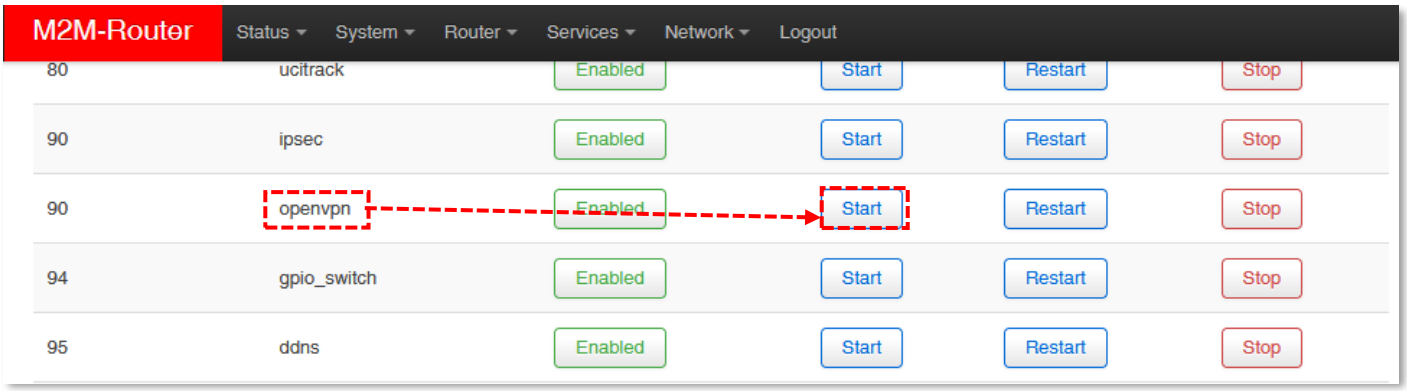
Roll down to the „**openvpn**" feature and push to the Disabled button to initialize the service.

Then wait until the service list will be refreshed and the „**openvpn**" will be listed as an Enabled service.

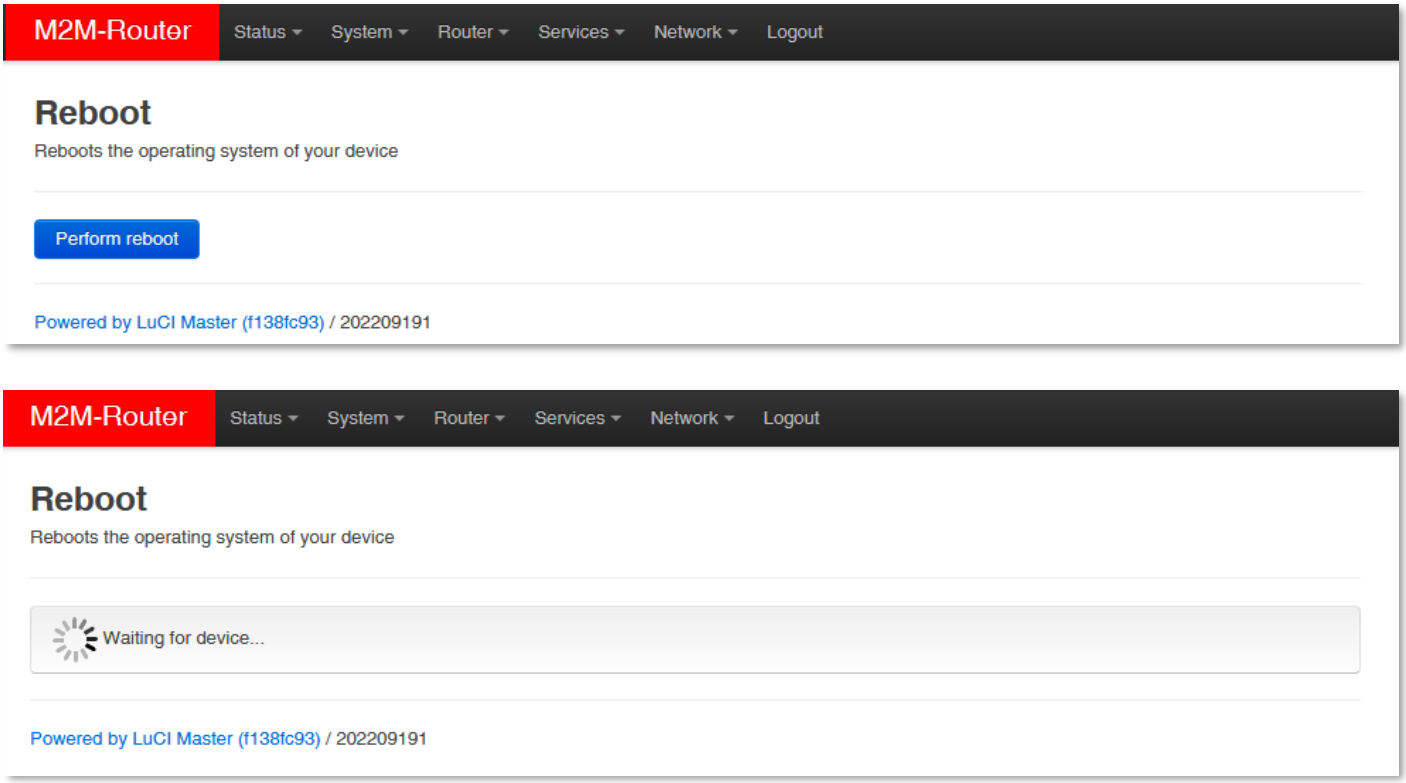


Then push to the start button of the line of the „**opevpn**" service to start the feature.

Then restart the device from the **System / Reboot** menu.



There push to the Perform reboot button.



After the restart, you have to log in again and configure the „**openvpn**" service.

For that, open the **Services** / **OpenVPN** menu, where you can set up an **OpenVPN** connection. The OpenVPN service default port nr. is 1194.

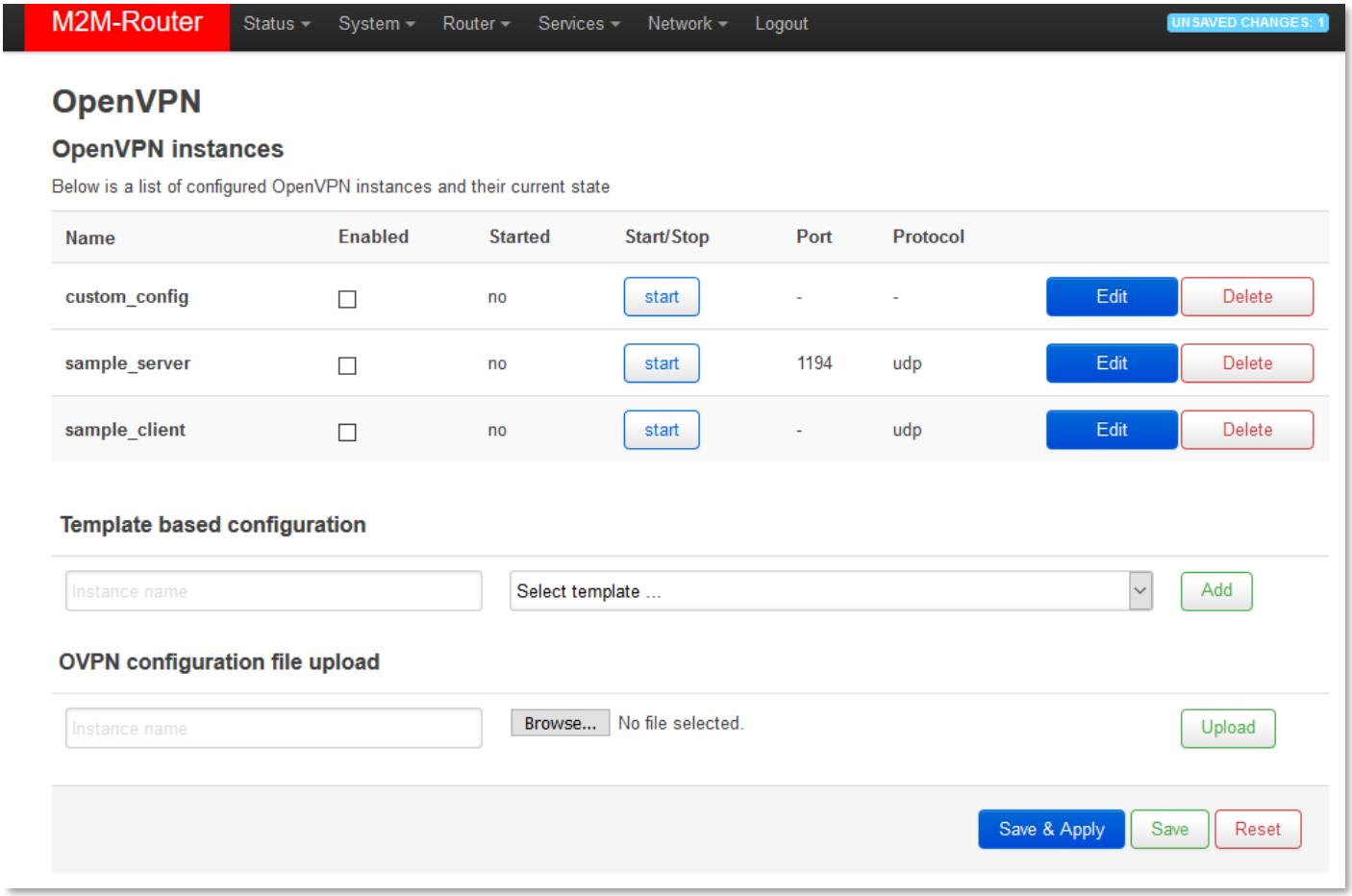
You will find three pre-configured VPN connections that you can enable or change your settings.

Use the **Enable** option to enable that setting, and then press to start button to start that VPN rule.

Of course, the rules can be edited by the Edit button and deleted with the Delete button.

Attention!

You can also set up a VPN server or client connection here. However, when using a VPN client, the router assumes the existence of an existing VPN server-side connection, the connection details of which you must enter here, in the interface.



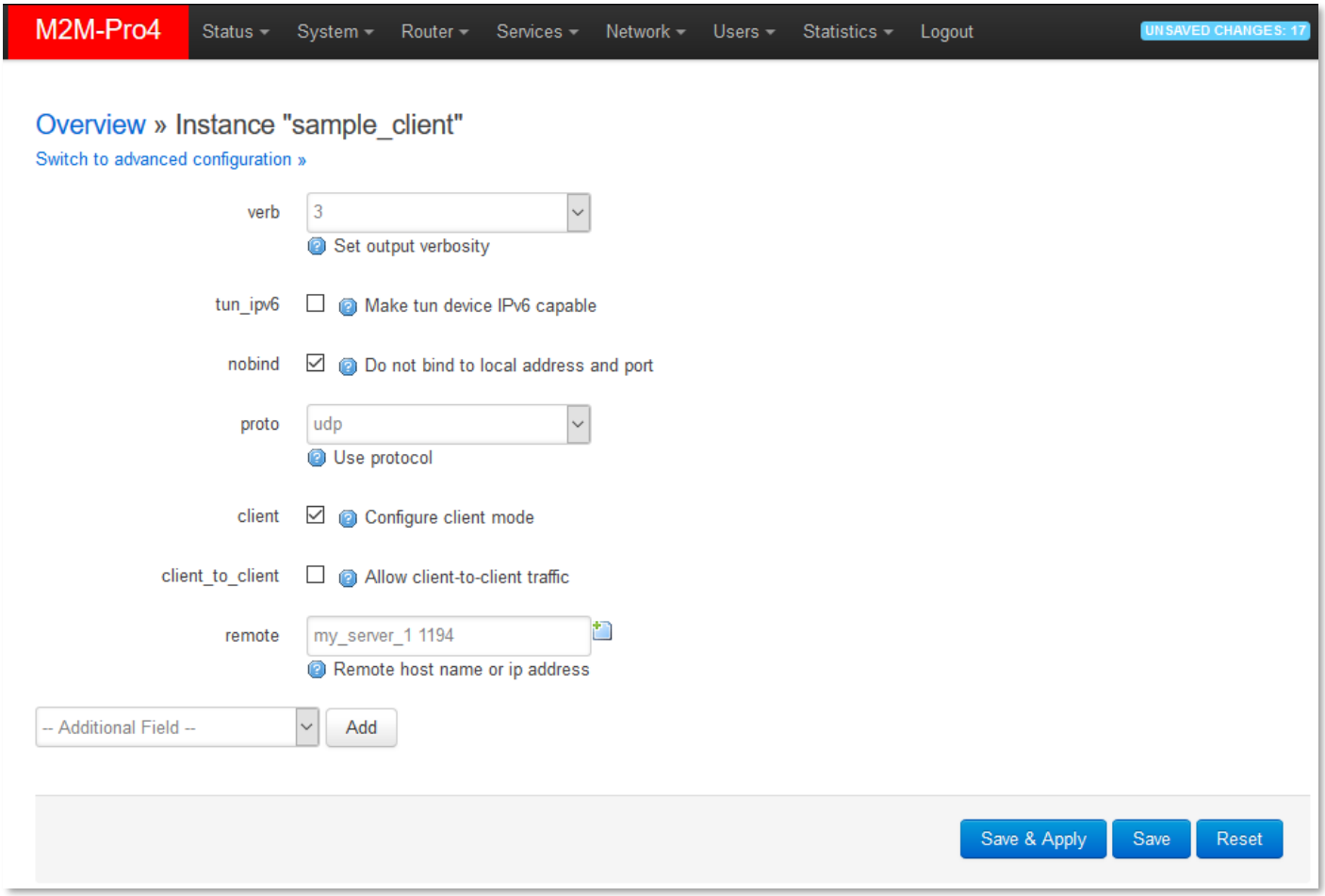
So, choose any profile from the ones listed - e.g. the **sample_client** profile - that is, the VPN client, then press the Edit button to edit.

The following window will appear, where you can set the following:

Configure at least the next fields on this page:

- **proto** (Protocol): here define the connection type –e.g. *udp*
- **client**: check in (to connect to the VPN server)
- **remote**: define the remote and existing VPN connection IP address or host name.

Save the configured settings by the **Save & Apply** button.



Then return to the **OpenVPN** menu, where you can enable the given setting with the **Enable** option, then press the start button to start the configured VPN connection, then press the **Save & Apply** button again to save the status of the services.

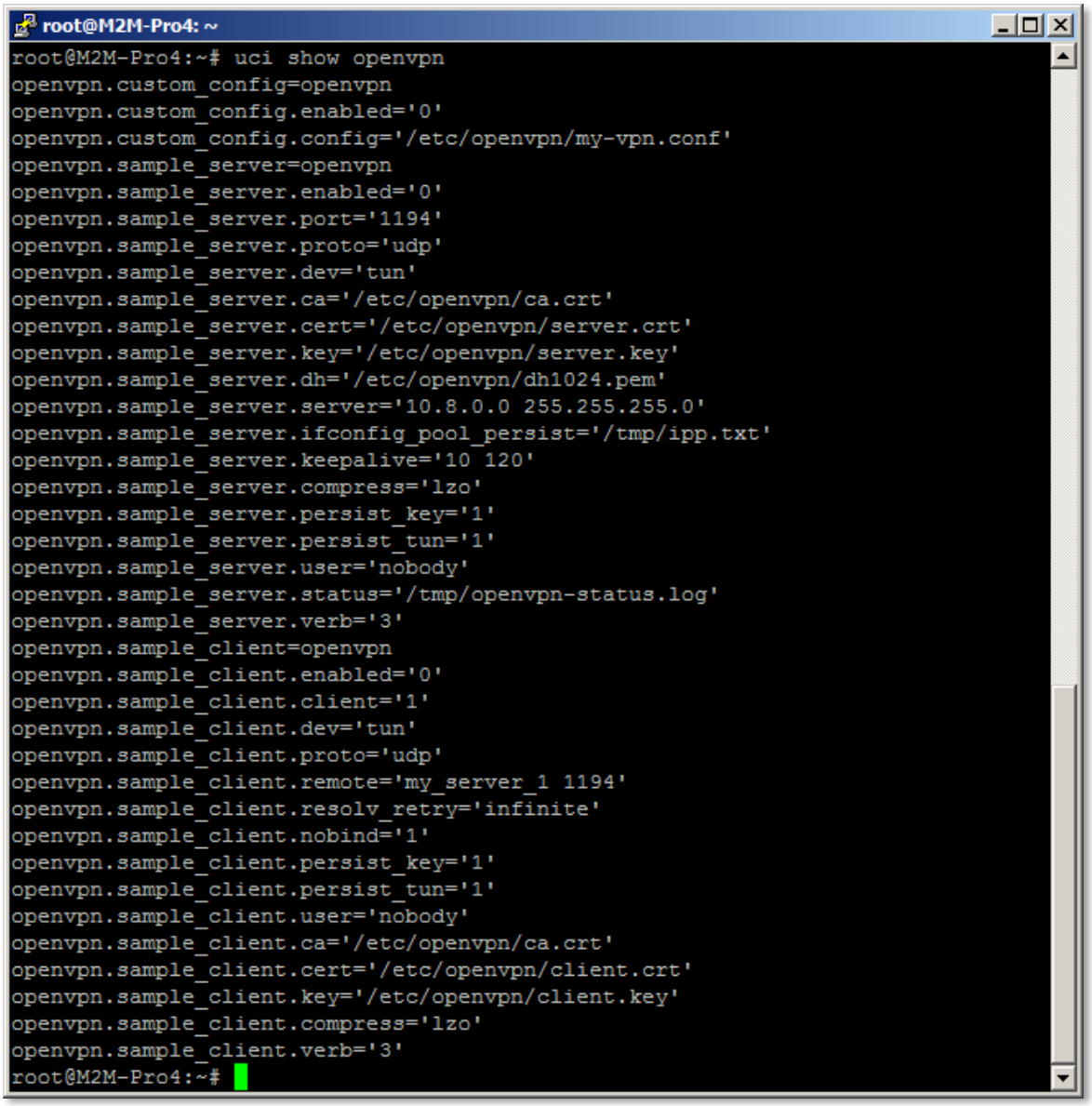
For the proper settings, we offer to read the related tunelling service description of the *OpenWrt*® administration interface which you are currently using: https://wiki.openwrt.org/doc/howto/vpn.openvpn#tab__traditional_tun_server1

OpenVPN settings can also be configured using the openVPN daemon on the Linux side using the UCI - from the command line - using SSH. Some examples of its use:

You can make a query to ask the current OpenVPN settings:

```
#uci show openvpn
```

For this, the current OpenVPN settings are displayed on the command line:



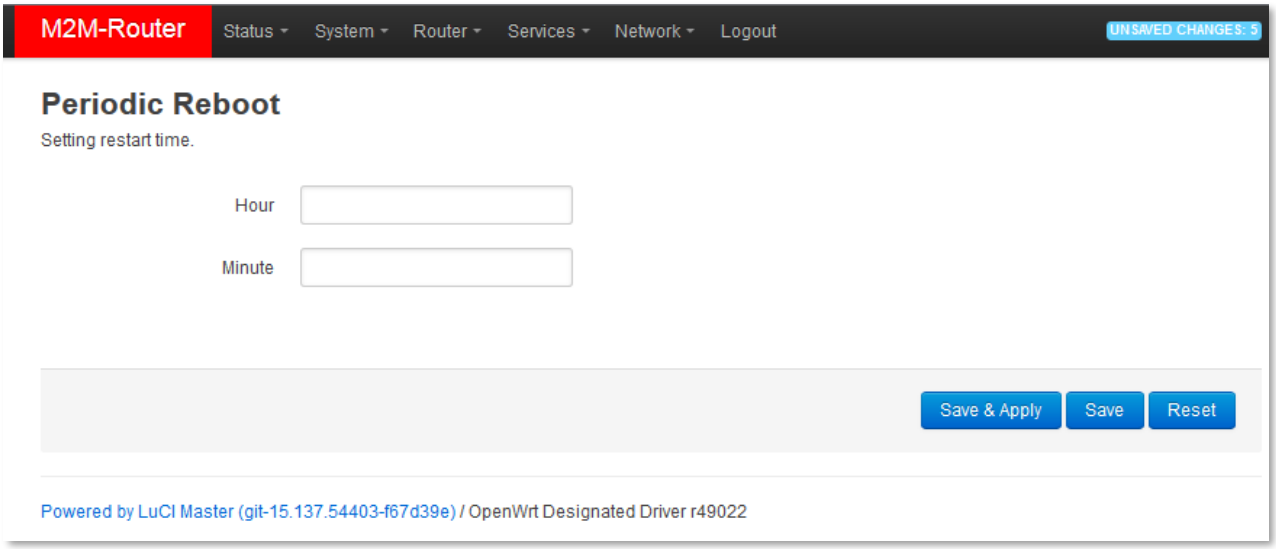
Set according to the following syntax and then comment:

```
#uci set openvpn.sample_server.dev='tun'

#uci commit
```

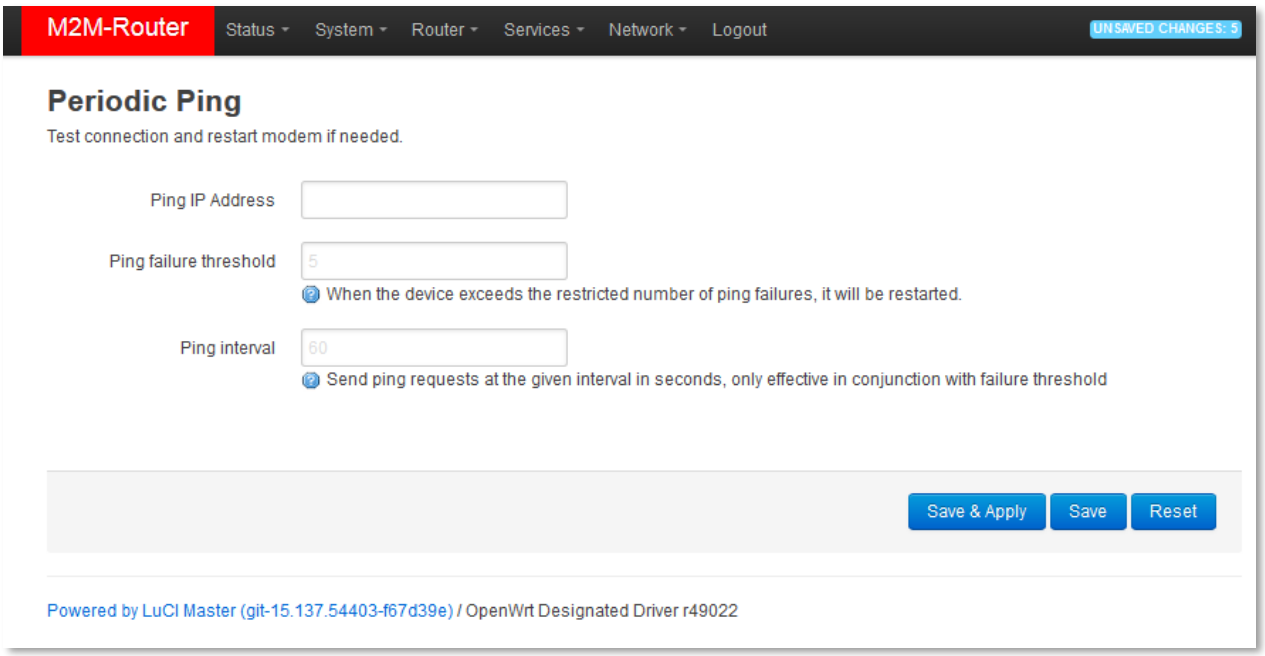
5.12 Periodic ping and Periodic reboot settings

For matching the industrial standard requirements, you can define an time interval for periodic daily restart of the router if you want in the **Router** / **Periodic Reboot** menu.



If you want to use periodic ping as checking an IP address or remote server, device as checking its availability by the router if you want to use this service by accessing from the **Router** / **Periodic Ping** menu.

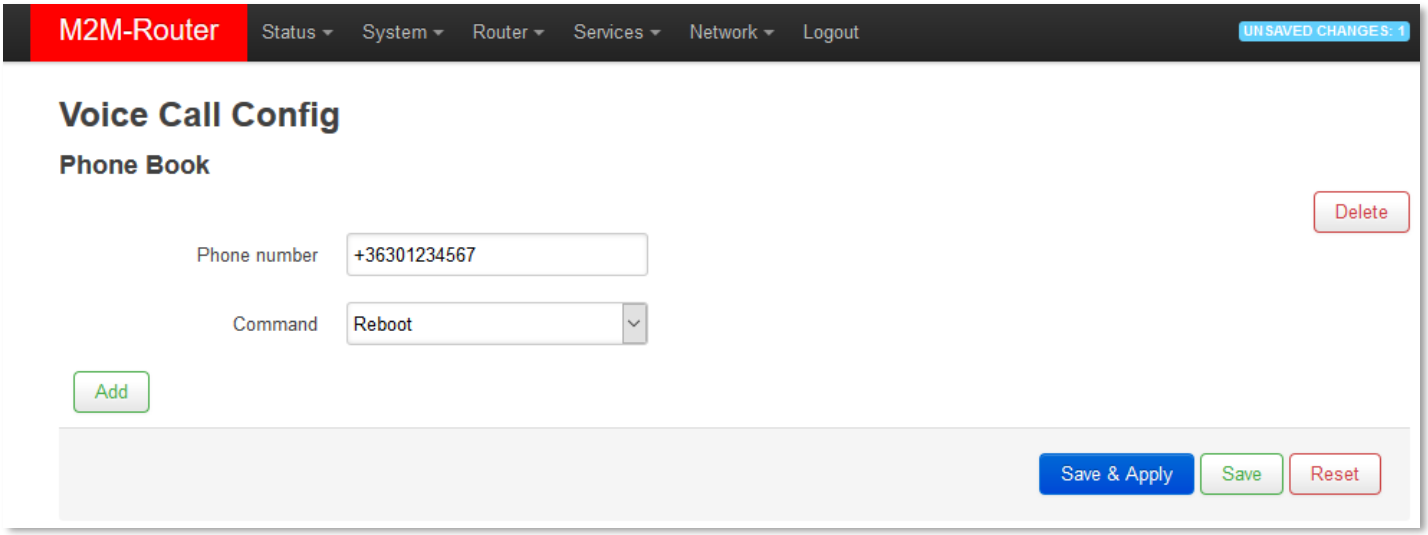
Save the configured settings by the **Save & Apply** button.



5.13 Voice call settings

You can set remote reboot commands in the **Network / Voice Call Config** menu.

For an incoming call from an allowed / assigned phone number, the device runs a *reboot* command.



You can also use the Add button to add additional phone numbers and select the *reboot* command for the phone numbers.

Press the **Save & Apply** button to save the settings.

5.14 Run commands remotely (SMS config settings)

You can execute commands on the router remotely when an SMS message was sent to the router's SIM phone number.

To set these remote control commands, open the **Network / SMS Config** menu.

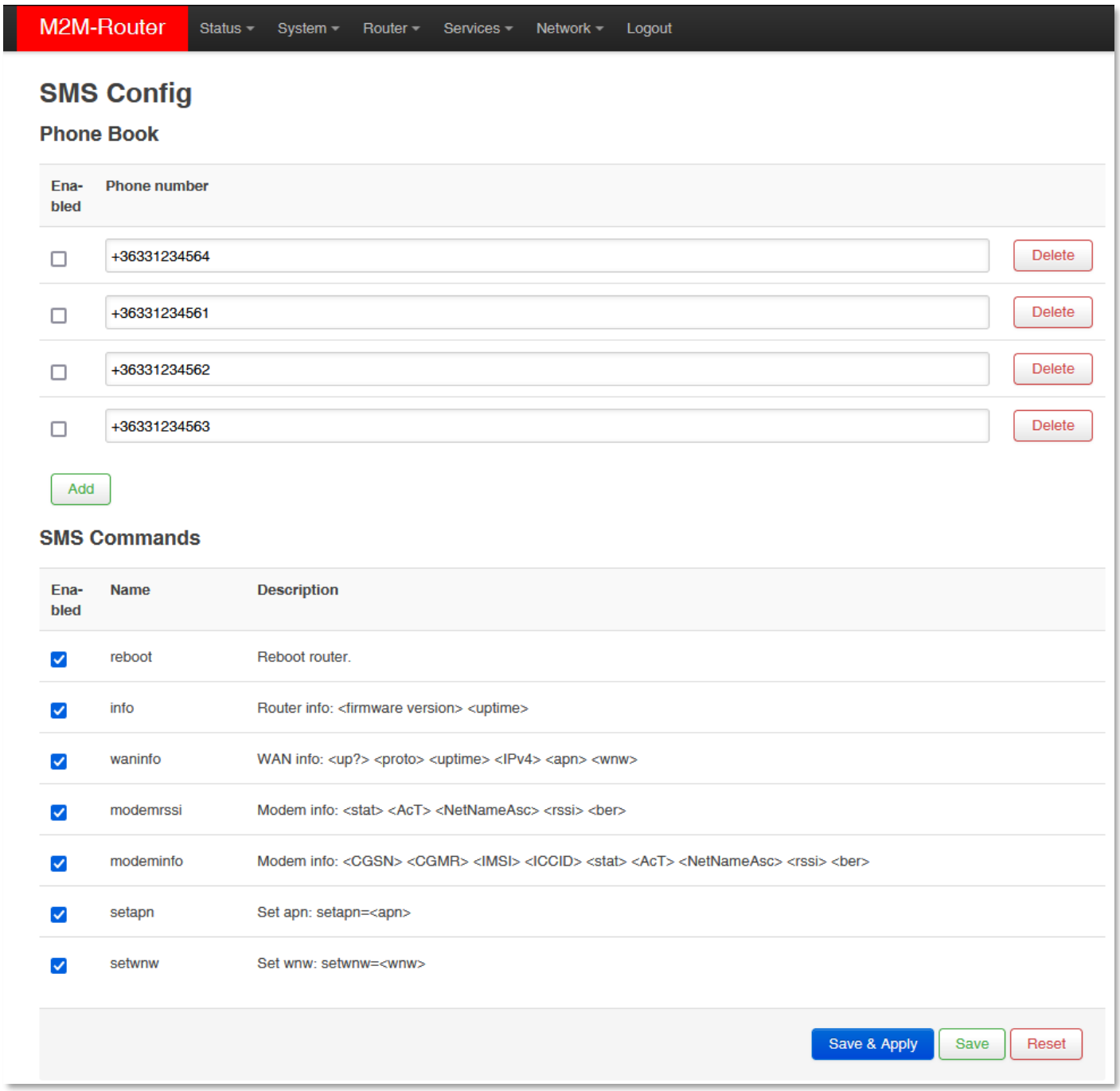
First you can see the **Phone Book** where you can define or Add phone numbers.
Then you have to **Enable** the selected phone number.

At the **SMS commands** part you can choose preset commands by selecting them for the number.

In the case of an SMS from a preset phone number, the router runs the preset command (s) assigned to the phone number: e.g. **Reboot**

For other commands, the router returns the information in a reply SMS message (e.g. when sending the "**info**" command in SMS, the router sends the firmware version

number and the elapsed time since the last boot info to the phone where the SMS has been sent).

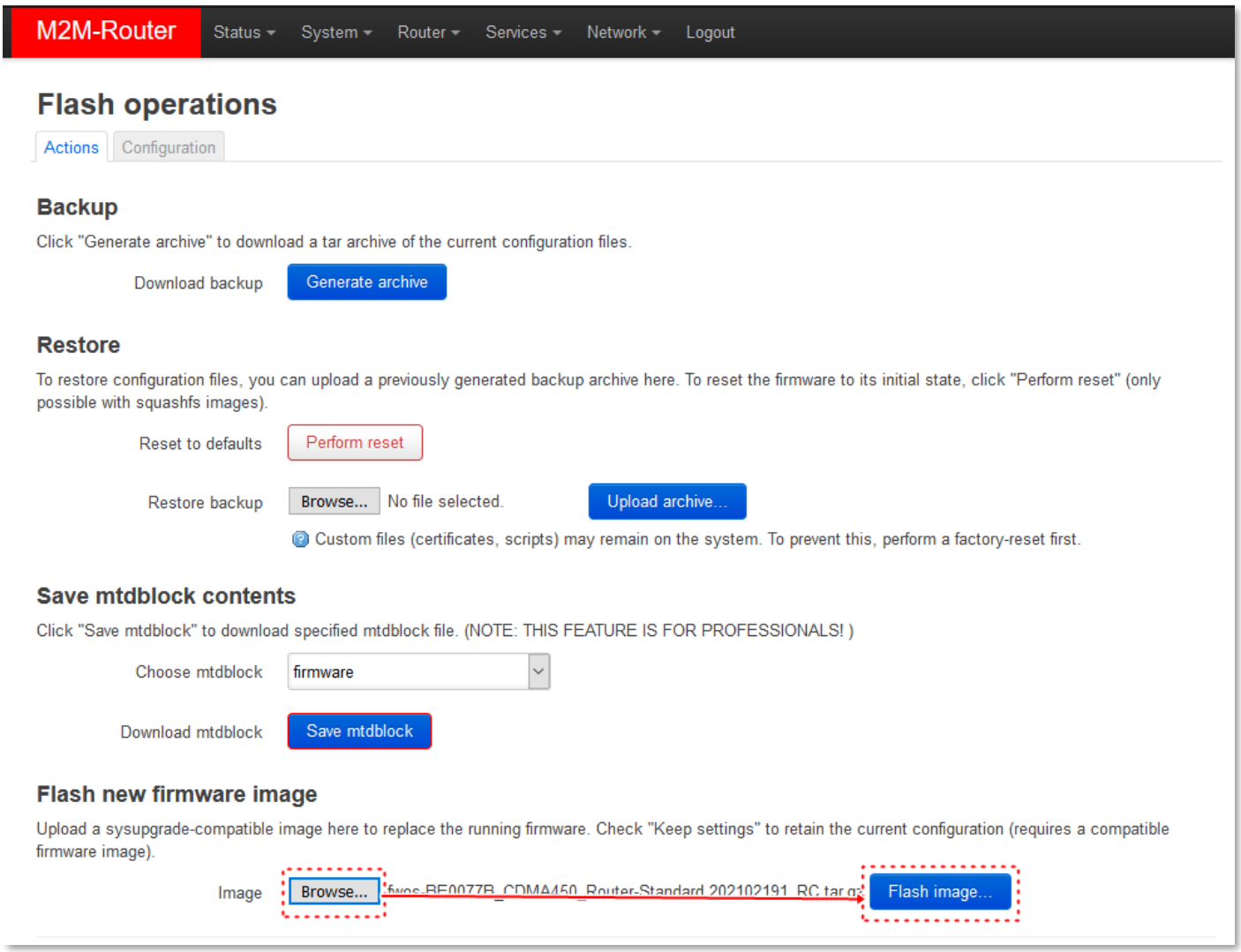


When you have changed something, press the **Save & Apply** button to save the settings.

Chapter 6. Software refresh and router maintenance

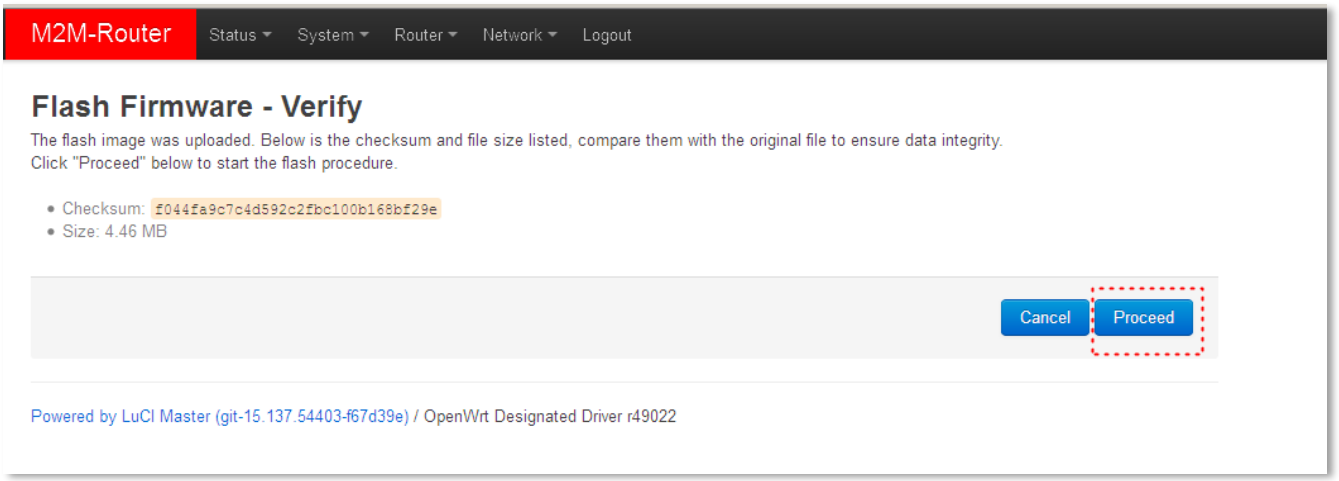
6.1 Firmware refresh

1. Open the **System** menu, **Backup / Flash firmware** item.
2. At the bottom part, browse the ***fwos***-…. compressed file at the **Image Browse** button, then push to the Flash image... button.

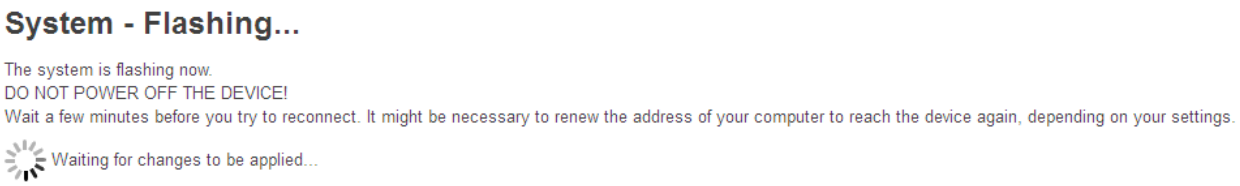


3. Then an nother window is loaded, where the checked file is checked for approx. in half a minute.

4. A new window will appear where the file will be checked. When it is okay, the system refreshment is possible by the **Proceed** button.



5. Then the next message appears on the screen in the browser. Then the refresh method has started, while the **LED3** is continuously lighting by **red** and sometimes the **LED2** is flashing.



6. At the end of the installation - the LEDs will no longer flash - the system will reboot 2x, then the *OpenWrt®* system will start and load as described.

***Important**! The update window does not close and does not detect the availability of the OpenWrt website. Therefore, close the upgrade browser window at the end of the installation.*

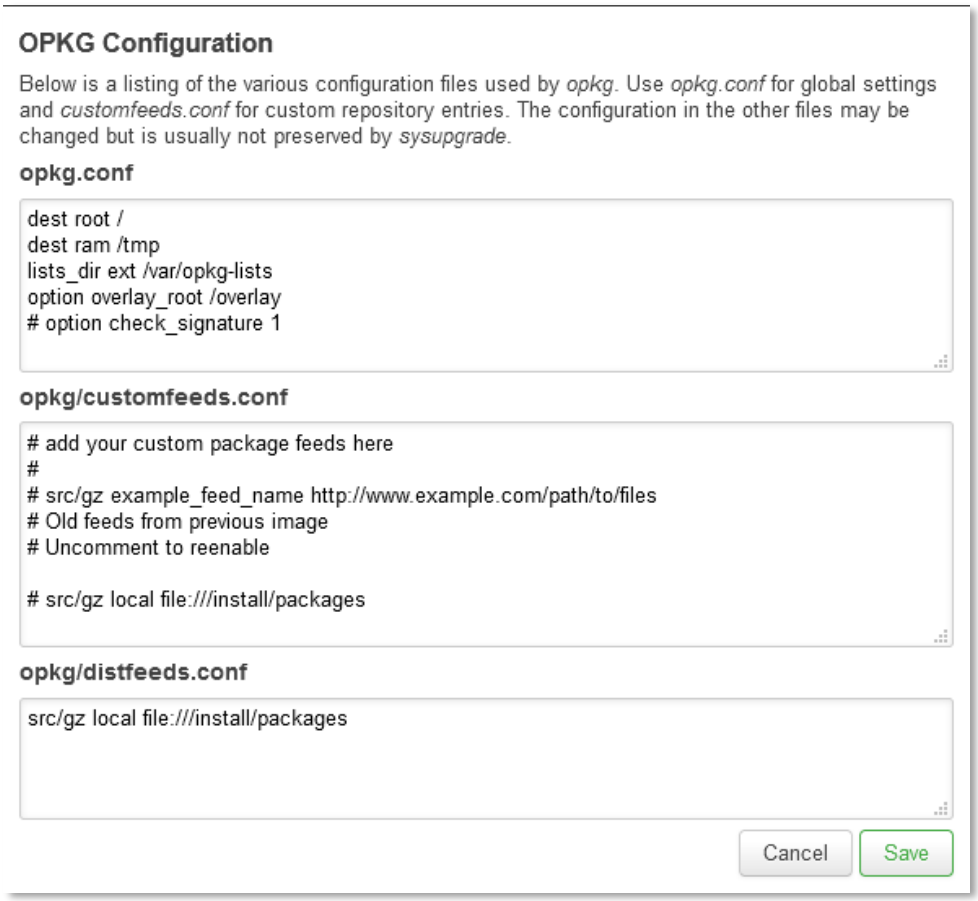
7. When **LED3** or **LED2** is available again and stays green, re-enter the home page address in Mozilla Firefox to access the local OpenWrt interface.

8. Check the updated software versions on the home page for statuses.

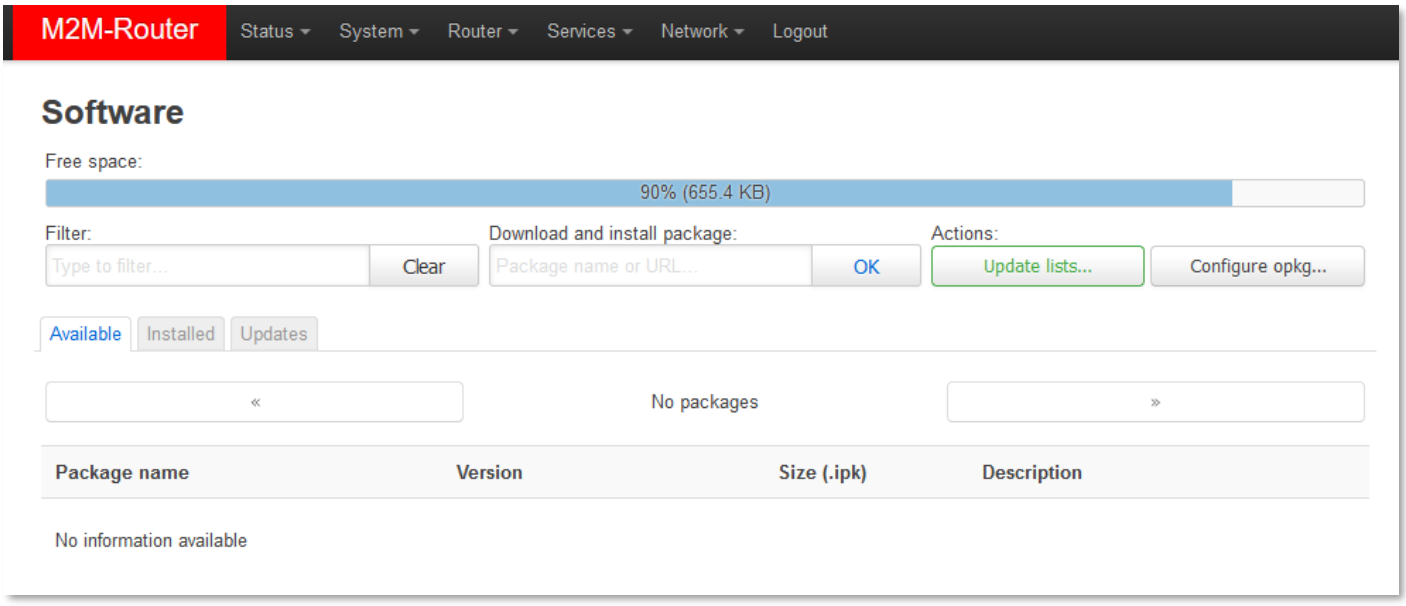
6.2 Installing applications

Open the **System** / **Software** menu.

First you have to push the Configure opkg... button and setup the software distribution configuration in the popup windows, where you have to define the path of the installation packages are stored.

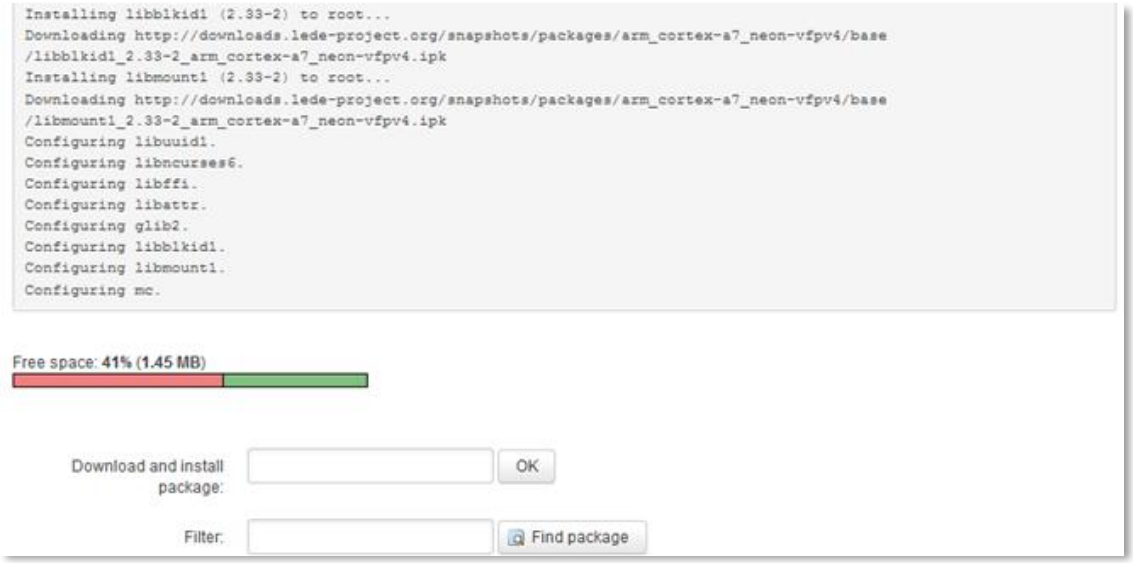


Then Save the settings by the button. Afterall, push to the Update lists... button to refrest the available software catalog - from the software repository.



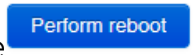
Important! *This feature is available when the public internet can be accessed by the SIM card, APN zone.*

When it has been successful, then add the name of the application you are attempted to install at the **Download and install package** field (e.g. *„MC" in case of Midnight Commander*), and push to the **OK** button for the installation – regarding the upcoming hints on the screen.
The installed software packages are listed under **Status** with their **Version** information.



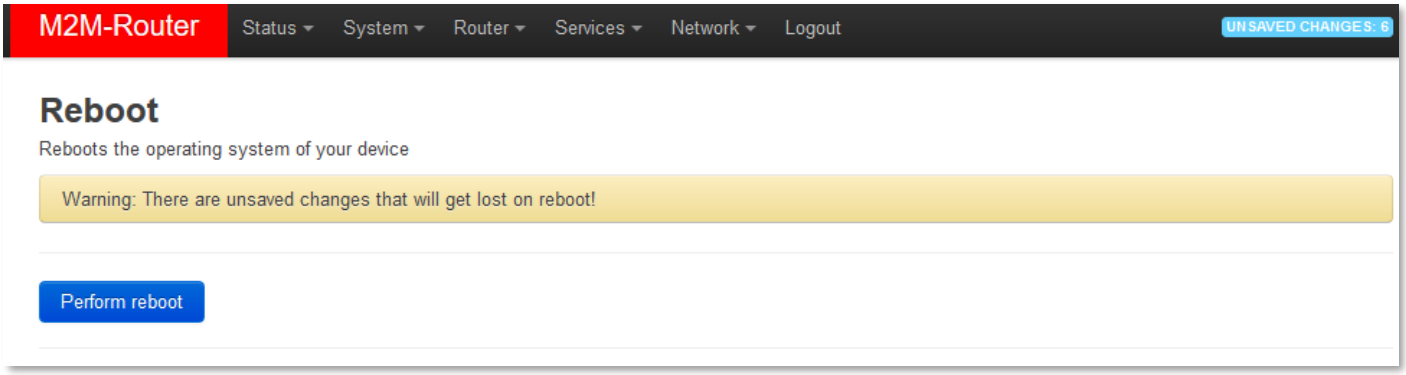
You can now configure and use the installed Linux program. You can configure or run it from the command line using the SSH terminal window. (Staying with our example: type "mc" at the Linux command prompt to run the program.)

6.3 Restarting the router

Choose the **System** / **Reboot** item and push upon the 

button.

Then the router will be restarted as it was described before (**the 3 LEDs lighting shortly** by **red** colour for a second, and the **St. LED** flashing assigns the booting process, then the router will be operating as normal, and will be connected to the internet according the configuration settings.



6.4 Shutdown / halt of the router

To shutdown the router device, first you have to reboot by the **System / Reboot** menu. When all the three LEDs blinks at once, the router is restarted and can be switched off safely as soon as you can – pull out the power connector from the 230V AC electricity plug.

Attention!

Never stops the router without requesting the reboot process, and do not remove the power socket without restarting the router before this action!

6.5 Reset the router

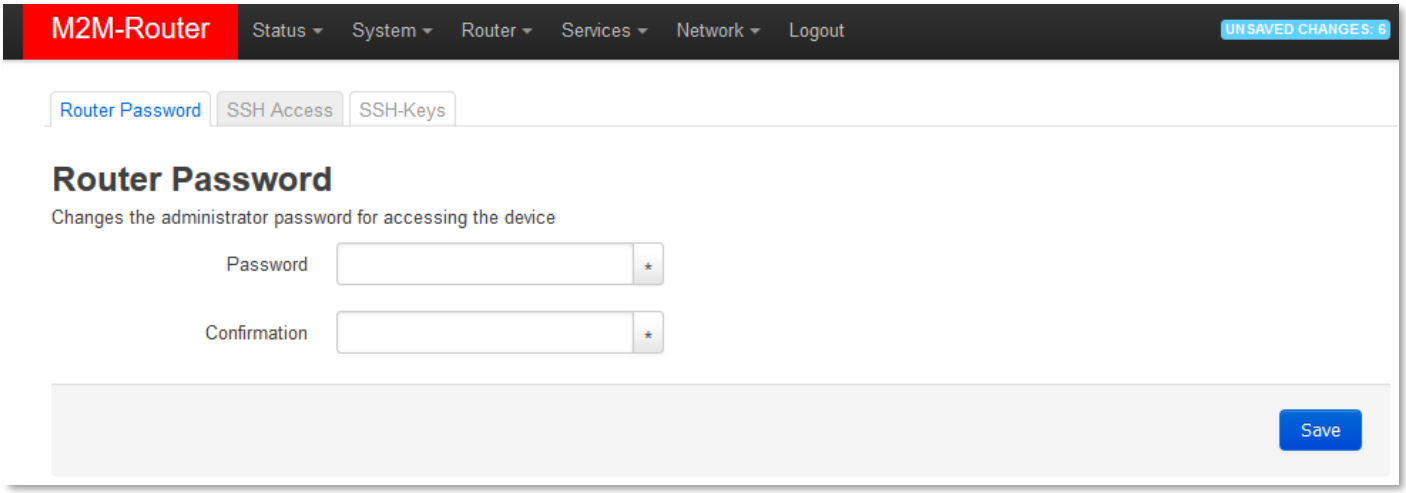
When the router is not reacting or it was not possible to configure properly, push in the **Reset** titled low-case button for 10 seconds – by a sharp and thin object. Then the router will be restarted by the factory configuration, whereas the LED lights will assign it. After a few minutes, the router will be available and accessible on its default address.

Configure the router in its web interface!

6.6 Password change

Open the **System / Administration** menu.

At the **Router password** you can fill the new **Password** and again to the **Confirm password** fields. You will be able to login further by this new password.



When you enter the password, the web interface replaces the entered characters with asterix (*).
At least 6 characters must be entered for the password.

Press the **Save** button to save the new password.

6.7 Backup and restore of settings

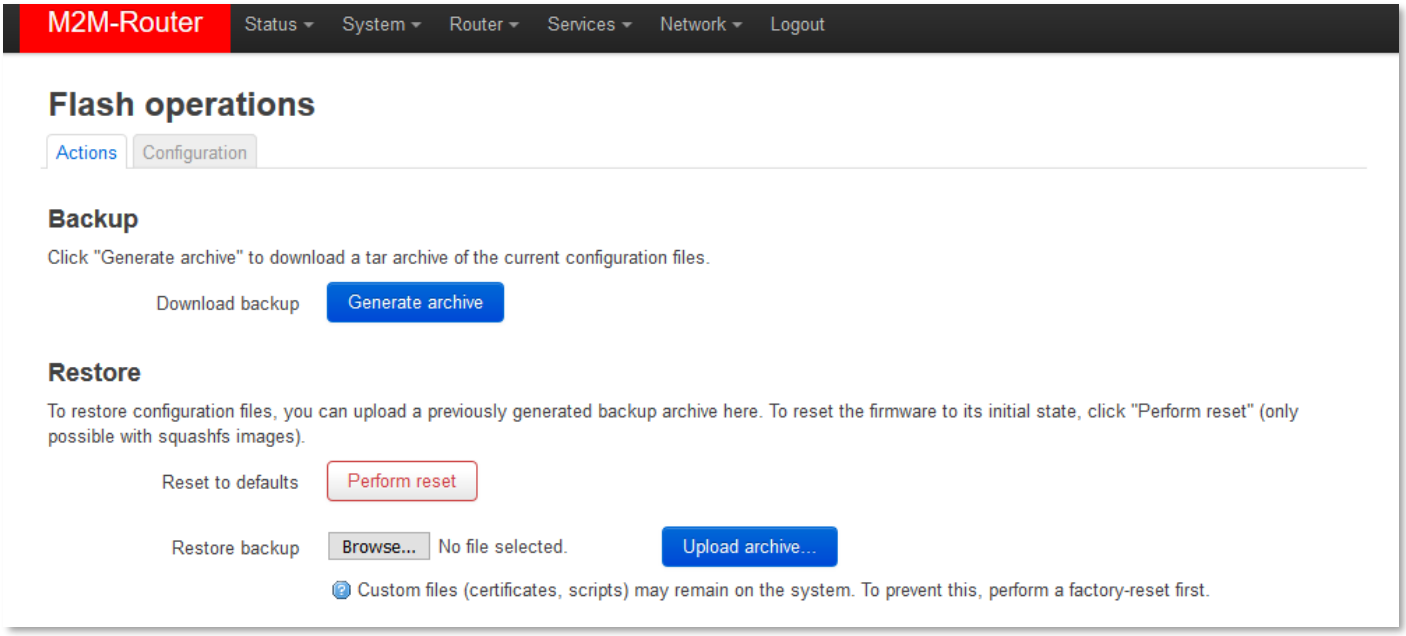
The router settings are automatically saved by the OpenWrt® system. However, there may be situations where it may be necessary to restore a previously saved configuration state.

Therefore, you can save the settings to your computer as follows and restore them to the router if necessary. This is very useful during initial configurations, for example.

Open the **System** menu, **Backup / Flash Firmware** item.

At the **Backup / Restore** part and **Download backup** feature push the Generate archive button for saving the settings into a file (to .tar.gz extension).

In the pop-up window, you can select where to save the file (configuration) to your computer.



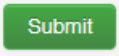
***Important**!*

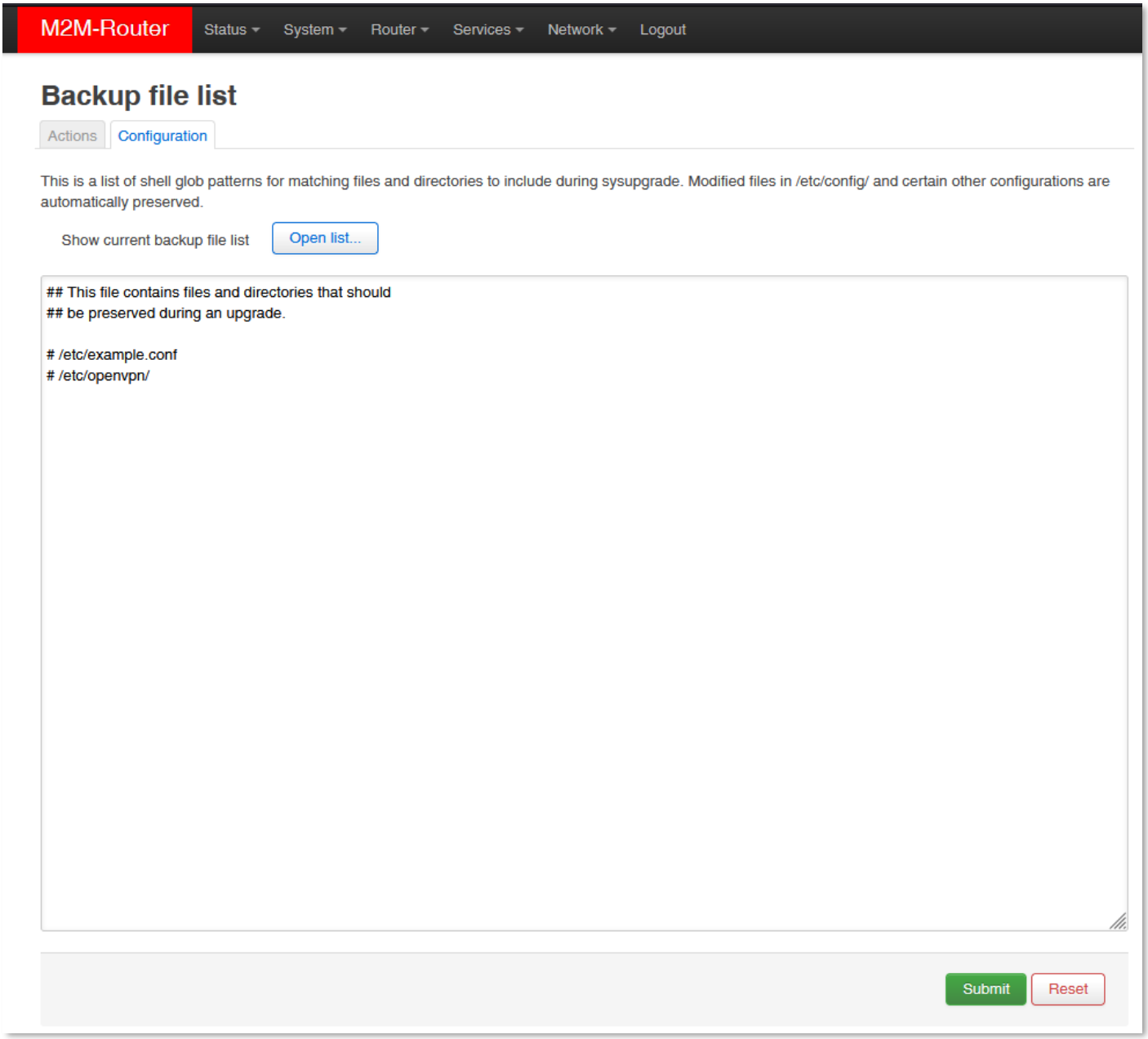
During subsequent restarts, the router will always start with these saved settings - as the default configuration.

The router only saves its own settings and services! If you have manually installed additional programs or are using your own scripts, it is IMPORTANT to know that they will NOT be saved! You need to ensure that non-standard applications, scripts, directories are backed up manually.

You can include or exclude files and directories during the installation. You can control exactly what is saved by clicking the **Configuration** tab, where you can edit the list by specifying each directory.

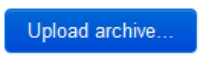
To use it properly, you need some directory- and file-level knowledge of the router's file system, so we recommend that you first connect to an SSH connection and review the directory structure and options from the Linux command line using standard Linux commands.

When you have created the save file, click to  button.



If you want to request a **full system restore**, save the archive (full) backup file previously saved to your computer - .tar.gz. format - you can download it back to your device.
To do this, you can validate your request here in the **System** - in **the Backup / Flash Firmware** menu, in the **Restore backup** field.

Press the 

button to **browse** the previously saved file from your computer, then press the 

button to download it back to the router.

Important!
You will then have to manually back up and play back the backups of custom configurations and programs - as they are not part of the system restore.

To reset the router configuration:

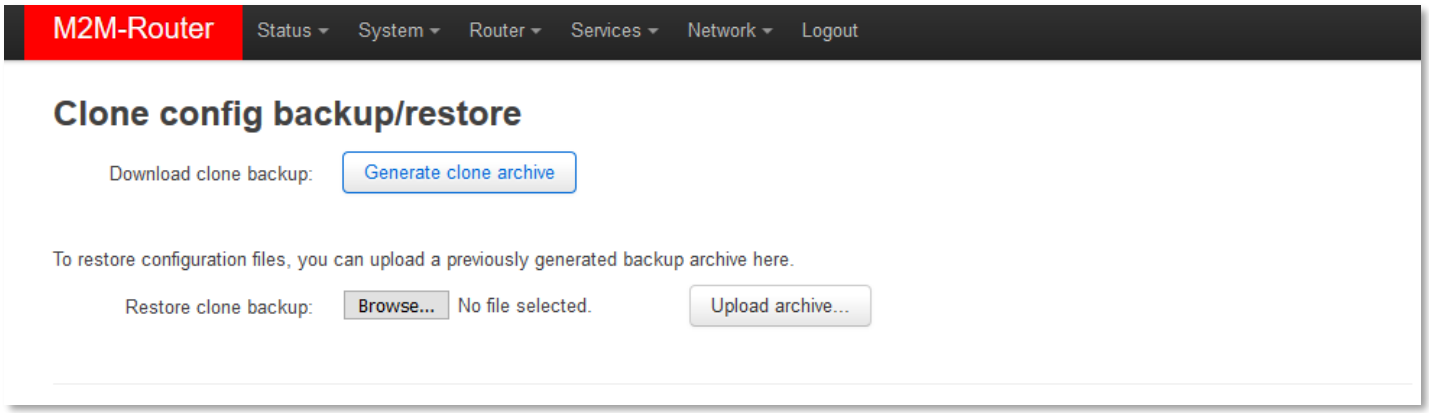
You can do it here in the OpenWrt interface, by also pressing the Perform reset button in the web interface menu item.
Or you can use the **Reset** button on the router to reset the router to factory defaults - see. router reset chapter.

6.8 Clone configuration

The current configuration settings of the device can be saved in plain text format. You can request this with the **System** menu**, Clone config backup / restore** menu item.

Here you can save the current settings to your computer using the Generate clone archive button.

In the popup window, click to Browse... for browsing the location where you want to save it, and then save the file to your computer.

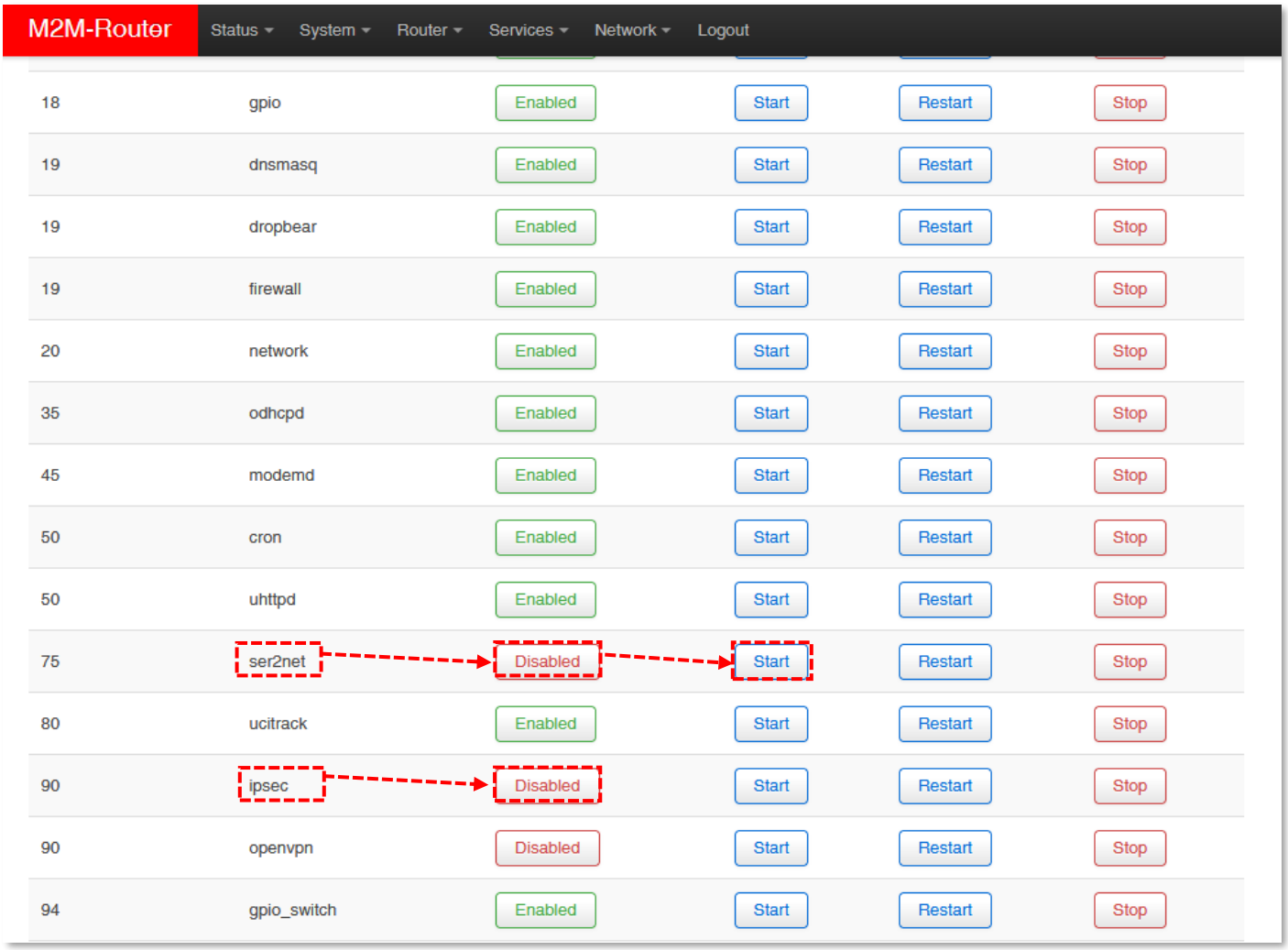


This is especially useful if you save the configured configuration to your computer and want to load it to multiple routers (as a basic configuration) - making the settings easier.

Which can be uploaded to other devices with the Upload archive... button after browsing.

6.9 Start or stop a system service

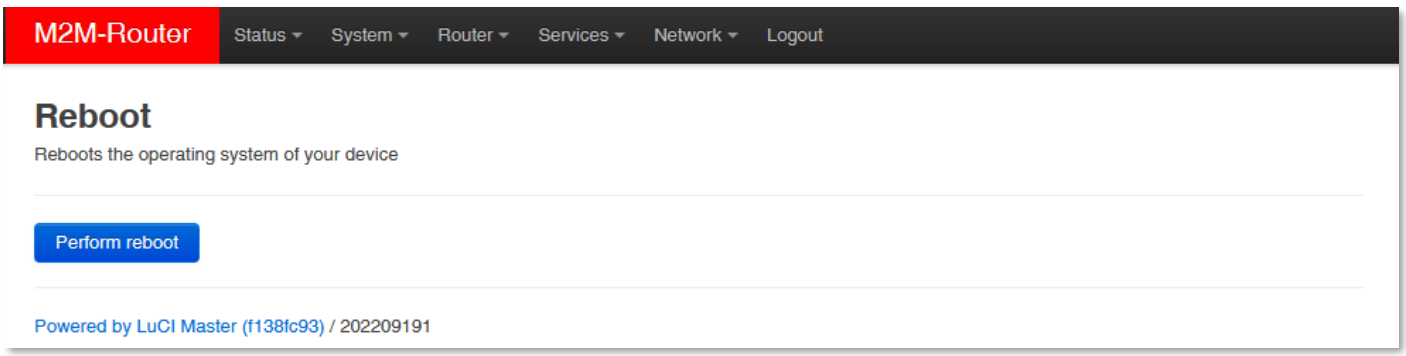
Open the **Systems / Startup** menu to enable or disable a system service.



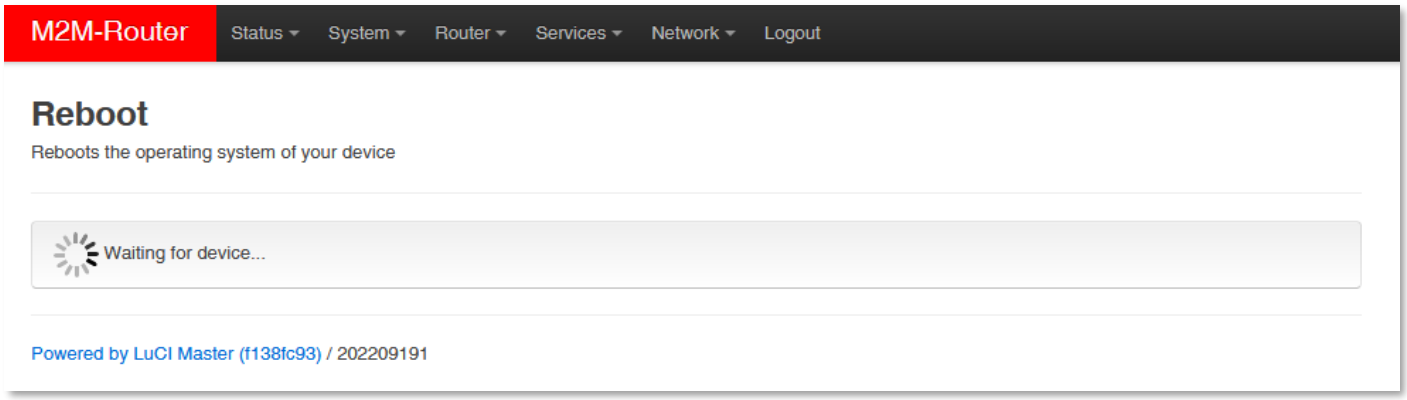
If the service has Enabled status, then you can start the service by pushing the start button to initialize the service. To stop the service, push to the Stop button.

If the service has been listed as Disabled, then push to this button and wait for the refresh of the list. When the status of the service will be Enabled then you can start the service as it was described above.

Afterall, you have to restart the device from the **System / Reboot** menu.



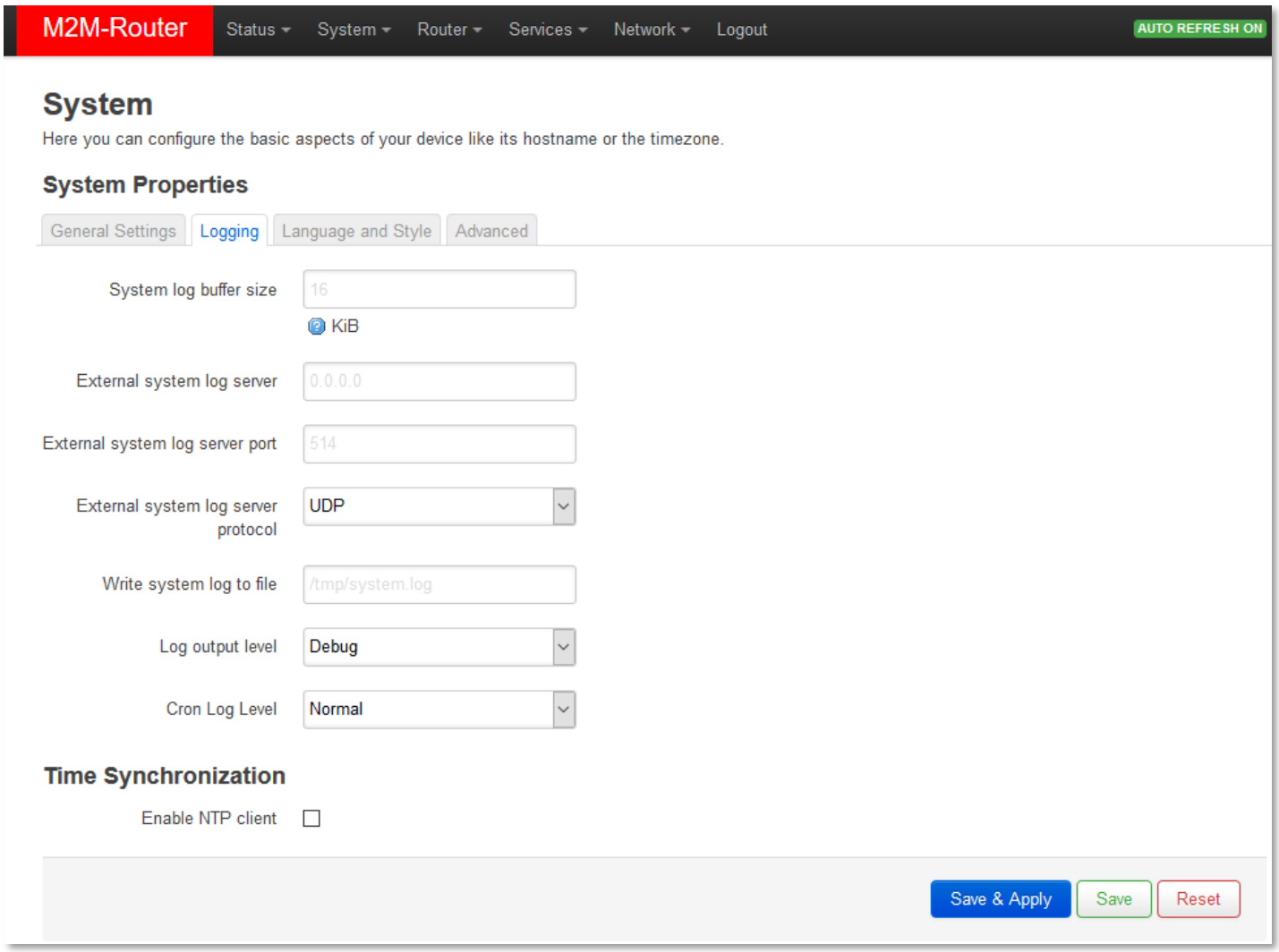
There push to the Perform reboot button.



After the restart, you have to log in to the system and you can use the configured service.

6.10 Log

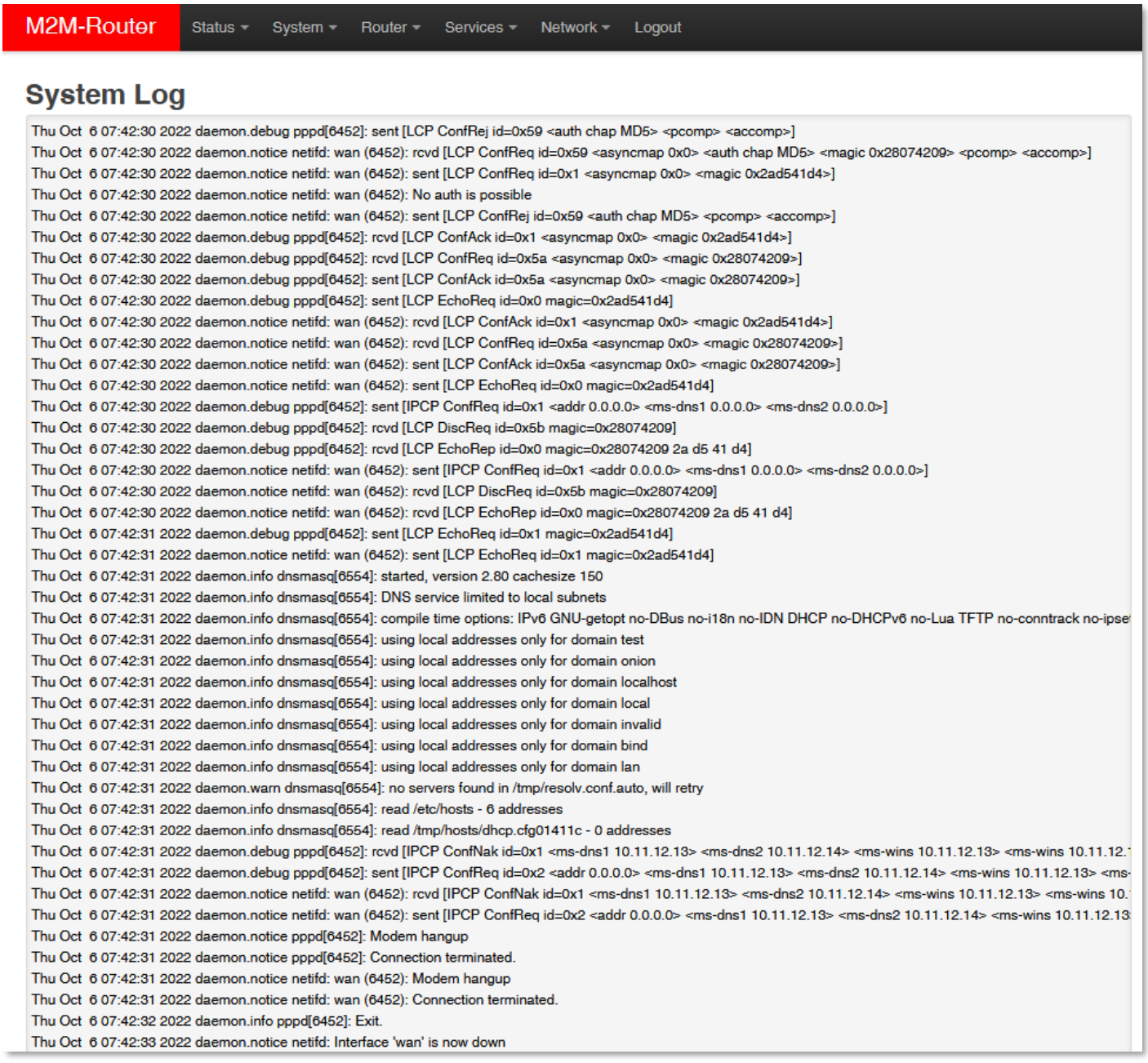
Open the **System / System** menu, check the **Logging** tab.



Here you can define a system log file (**Write system log file**) - where a directory structure, path and file name must be specified - and also set the log output level.

You can limit the size of the log file (**System log buffer size)** and set the IP address of the **External log server** (IP address), **port, protocol** - to send the log files to a remote server.
Press the **Save & Apply** button to complete the settings.

There are other log files generated by default, which we have already mentioned in part. These include in the **Status** menu, at **System log** and **Kernel Log**, which all will help you to check the current operation, understand some events that have occurred during operation since the router was last rebooted. This can be especially useful when found an operation issue, when a features is not available yet, or even if the cellular module indicates some connection trouble.



Chapter 7. Troubleshooting

LED activity

Can you see any LED activity (flashin, light)?

After ca. 2 minutes inactivity of the LEDs could mean the router has a failure (configuration or firmware trouble).

First you should ensure about the router is still under starting / booting phase or not. Please wait 2-3 minutes, then check the LED signals again. If the **LED1..LED2..LED3** are not blinking or does not lighting then the device hasn't got its power supply or it has some trouble.

Connect the power source and if it does not helps, ask our support, please.

In case of LED blinking after restart

After ca. 2 minutes of the router start the **LED1** will be blank and the **LED3** starts to flashing by **green**. This signs that the router begins try to connect to the cellular network (logins to the APN and builds the connection).

After 1 or 2 minutes, the **LED2** must be lighting continuously, which signs the successful modem network connection and the available ppp (**WAN**) connection.

(in case of 4G version the **LED2** does not lighting here.)

The device is communicating on the network and will send a couple of minutes later proper *RSSI* values and life signals. Meanwhile the **LED1** will flashing once in every 10 seconds - which means it is operating properly.

Power source

Check router that it can get any power through its microfit connector (**POWER**) – power adapter is connected to the router microfit connector and the adapter to the 230V AC plug.

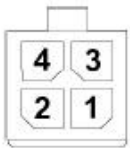
When it receives 12V DC power, the LED signals will sign it: *all the three LEDs will light for a short* period, then the **LED1** (**green**) will lighting for 2 or 3 minutes, then after that only blinks once in every 10 seconds. The router is booting and just started.

(Wait for 1-2 minutes, while the router is registering to the wireless network then check the life signals).

In case of failure, check the power supply connection at the socket plug side and on the microfit connector at the router side. The top 2-pins of the microfit plugin are wired only, the left pin is the negative.

Check the next figure for the pinout and check the 12V DC voltage on the microfit connector (by a multimeter) of the power adapter that it provides 12V or not. If not, than remove the 12V DC adapter and get another one with the proper pinout and voltage.

4-PIN connector (Power Input)



Pin assignment of 4-pin connector

Pin number	Name	Functions
3	POWER -	DC power negative input
4	POWER+	DC power positive input

Connecting to the router, checking connection

Set the IP address of the **Ethernet interface** on the PC where it can be reached (in the Microsoft Windows®: **Control panel / Network / Network Adapter / Adapter settings)**.

Ping the router IP address.

If you can connect, you can ping an IP address out of the OpenWrt interface to check network access on the mobile Internet.

Ethernet connection

Check or connect the RJ45 UTP6a type cable to the **ETHERNET** port. When the router is operating, the **Ethernet** port LEDs must sign the network activities. If you do not have an Ethernet cable connection, you can use a micro USB connection for the bridge connection to access the router's web interface.

When you cannot access router through SSH or on its web interface

Download the micro-USB cable **driver** from here:

http://www.wmsystems.hu/m2m-downloads/USB_Ethernet_RNDIS_DRIVER.zip

Unzip the downloaded zip file into a directory and install.

Establish a USB connection between the PC and the router with a micro-USB cable connected to the socket marked **USB**. (The driver must be installed on the PC according to the ***Installation Guide***).

Set the IP address of the **USB-Ethernet interface** on the PC for the "**USB Ethernet / RNDIS Gadget**" network connection (***Control Panel / Network / Network Adapter / Adapter Settings***). You can also voltage the device on the **USB** connection at the IP address.

To connect to the website, enable access to the router's IP address in the browser (from the computer on the USB network interface it should always appear as **192.168.10.10** IP address, Subnet mask: 255.255.255.0 - this is set in ***Control Panel / Network and Sharing Center / Adapter Settings / Under Network Connections***, to the **USB Ethernet / RNDIS Gadget Interface**.)

If the router is not starting

It is possible that there is no uploaded software available on the router. Upload the router software or ask our support line!

Periodic restart of the router (by 10 minutes periods)

When router was not be configured properly for the ppp/wan connection or the modem was not started then the router will be restarted within in 10 minutes.

You can also configure the periodic ping interval from the LuCi / OpenWrt.

Restart of the router

If the router is not responding permanently, you can restart it by disconnecting power cable (**POWER** titled microfit connector) then after a few second plug it again. The LEDs must assign the presence of the power source.

Shutdown / halt the router

To shutdown the router, first you have to reboot by the **System / Reboot** menu. When all the three LEDs blinks at once, the router is restarted and can be switched off safely as soon as you can – pull out the power connector from electricity plug.

Attention! Never stop the router without requesting the reboot process, and do not remove the power socket without restarting the router before this action!

Antenna

Use the proper antenna type regarding the used cellular module and mobile network.

Connect the SMA antenna properly to the antenna connector by mounting to the antenna interface.

In case of presence of two antenna connectors, the left antenna is the **MAIN**, the secondary is the **DIVERSITY**.

Check RSSI signal value and vital signals ont he OpenWrt web interface.

In case of using CDMA 450, LTE 450, LTE Cat.M or Cat.NB (Narrow Band) networks – always use the proper antenna which is harmonizing to the frequency/band. In other way the router will not abble to access the cellular network.

If there is no SIM slot

In case of using CDMA 450 network in many countries there are no need of usage of SIM cards. The identification of the routers (their cellular modules) and the registration to the cellular network is executing by a completely different way and method. Therefore, on M2M Router CDMA450 version we do not provide SIM card slot. If your mobile network provider requires a SIM card upon this network, contact us before ordering.

SIM/APN failure

It means a SIM or APN failure, if the **LED2** will not light for minutes.

If the device is not registering to the network, then the modem was not initiated properly, and the router will restart itself after 10 minutes. This could caused by a not proper APN setting – or in case of CDMA version the wrong MSIN setting (you can configure it on the local web user interface).

The SIM / APN error can also be caused by incorrect APN setting – in case of CDMA it is the MSIN - which can be set by the router from the local web interface. Check with your mobile service provider that issues your SIM card for the APN names and passwords you are using.

After turning off the router, insert a working SIM properly, start the router, configure the APN and SIM settings on the local website of the router.

If the problem persists, contact your mobile service provider for the SIM card and the APN settings that you can use.

Always check the **SIM ID** field in the **Status / Overview** menu for the current SIM status. Normally, there is the SIM ID number. In the event of an error, one of the following SIM errors is displayed:

- **No SIM or SIM error** - No SIM or SIM is not active, incorrect SIM, or not inserted correctly, SIM may not be in contact.
- **Not enough RSSI value** - connect a suitable antenna to the primary antenna connector - for both antennas for version 4G - for the correct RSSI signal strength value.
- **No NW registration** - The APN name or SIM is not configured or these settings are incorrect
- **Check RSSI** - No antenna connected and / or SIM is incorrectly configured or incorrect. Check the antenna and SIM again.

SIM card cannot be detected

Turn off the router - unplug the power plug from the **POWER** connector of the device. Then, make sure that there is a SIM card in the **SIM** slot with the chip facing up and the bevelled corner facing inward, and then push the card in until it stops. Check with your

mobile service provider that the SIM card is active and ready to use data packet (IP communication).
Restart the router by reconnecting the power connector.

RSSI and CSQ values (signal strength of the cellular network)

If you will receive 99 RSSI and CSQ signal value continuously, that means you have to use another antenna or move the antenna to another position, whil you will get appropriate signal values at reception.

Always use the proper antenna type regarding to the module and mobile network, which is harmonized to the frequency/band. In other way the router will not abble to access the network.
Note that for Narrow Band (NB-IoT) networks it could be needed to wait 5-15 minutes for the first successfully network registration.

RS485 connection

You can connect Modbus devices, industrial measurement devices or meters to the router with an RS485 cable using the RS485 terminal connector, with the appropriate cable. Data communication can be defined in the **Services / Ser2net** menu, by enabling and configuring the **RS485** option, and according the TFTP settings (of FTP data transmission).

Chapter 8. Support availability

If you have any questions concerning the use of the device, contact us at the following address:

E-mail: support@wmsystems.hu

Telephone: +36 20 333 1111

8.1 Contact the support line

For the proper identification of the router you should use the sticker on the device, which contains important information for the call center.
Attach the OpenWrt related important information – marked - of modem identifiers to the problem ticket, which will help resolving the problem! Thank you!

8.2 Product support

Documentation and released firmware for the product can be accessed via the following links:

M2M Industrial Router
https://m2mserver.com/en/product/m2m-industrial-router/

M2M Industrial Router MBUS
https://m2mserver.com/en/product/m2m-industrial-mbus-router/

Online product support can be required here:
https://www.m2mserver.com/en/support/

Chapter 9. Legal notice

The pictures in the user guide are only for illustration purposes.
WM Systems LLC. does not acknowledge or accept responsibility for any mistakes in the information contained in the user guide.
The published information in this document is subject to *change without notice*.
All data contained in the user guide is for information purposes only. For further information, please, contact our colleagues.

Warning

Any errors occurring during the program update process may result in failure of the device.