

# M2M Industrial Router® / M2M Industrial MBUS Router®

## User Manual

**v2.40**



2023-08-28

## 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.

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

# Table of contents

<b>CHAPTER 1. Starting the Router .....</b>	<b>5</b>
1.1 Product variants.....	5
1.2 Interface connectors.....	5
1.3 Safety cautions .....	7
1.4 Mounting, fastening .....	9
1.5 Antenna .....	10
1.6 Further accessories.....	10
1.7 Connecting the router .....	12
1.8 First start.....	13
1.9 Web user interface of the router.....	15
1.10 Access via SSH connection.....	17
<b>CHAPTER 2. Web Administration user interface.....</b>	<b>19</b>
2.1 Main page (Dashboard).....	19
2.2 Menu.....	20
2.3 Status menu .....	21
2.4 CDMA menu (only for CDMA450 devices).....	21
2.5 System menu .....	22
2.6 Router menu.....	23
2.7 Services menu.....	23
2.8 Network menu .....	24
<b>CHAPTER 3. Important notes.....</b>	<b>25</b>
<b>CHAPTER 4. Network configuration of the router .....</b>	<b>28</b>
4.1 Interface settings.....	28
4.2 Cellular / Mobile internet settings .....	29
4.3 Ethernet (LAN) settings.....	31
4.4 DHCP settings.....	33
4.5 DNS settings.....	35
4.6 Defining the route rules.....	36
4.7 Firewall settings.....	37
4.8 Port Forward settings.....	42
4.9 IP routing, NAT settings.....	43
4.10 Dynamic DNS settings.....	45
<b>CHAPTER 5. Special settings .....</b>	<b>47</b>
5.1 Device Manager settings .....	47
5.2 Ping an IP address.....	48
5.3 Network Time Service (NTP).....	49
5.4 Identification of connecting devices.....	49
5.5 TFTP settings.....	50
5.6 RS485 settings (Ser2net).....	51
5.7 LED configuration.....	56
5.8 Remote access (SSH).....	57

5.9 UCI usage from the command line.....	58
5.10 IPSEC settings.....	58
5.11 VPN client (OpenVPN) configuration .....	60
5.12 Periodic ping and Periodic reboot settings.....	65
5.13 Voice call settings.....	66
5.14 Run commands remotely (SMS config settings).....	67
<b>CHAPTER 6. Software refresh and router maintenance .....</b>	<b>69</b>
6.1 Firmware refresh.....	69
6.2 Installing applications .....	70
6.3 Restarting the router .....	72
6.4 Shutdown / halt of the router .....	73
6.5 Reset the router .....	73
6.6 Password change.....	73
6.7 Backup and restore of settings .....	74
6.8 Clone configuration.....	77
6.9 Start or stop a system service .....	79
6.10 Log.....	80
<b>CHAPTER 7. Troubleshooting .....</b>	<b>81</b>
<b>CHAPTER 8. Support availability.....</b>	<b>87</b>
8.1 Contact the support line.....	87
8.2 Product support.....	87
<b>CHAPTER 9. Legal notice.....</b>	<b>88</b>

# 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/>

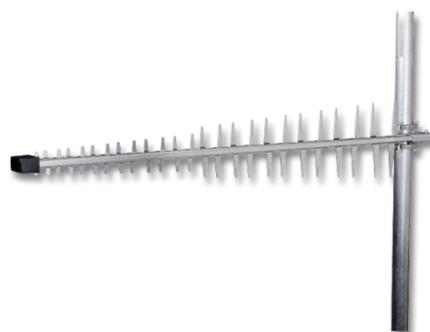
<https://m2mserver.com/en/product/din-rail-mount-unit-one-sided/>

## **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 magnetic mount antenna if 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<sup>2</sup>, 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).

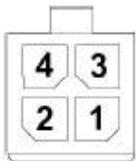
For the wiring and assuring the power supply you should take note to the following figure.



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<sup>2</sup>, 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:

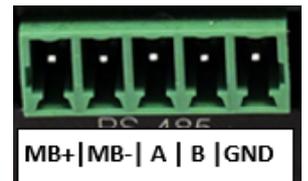
Type: 70 cm, OMYA type, 5 x 0,75 mm<sup>2</sup>, halogen free, double insulated wires, min. 24 V voltage, wires are marked by color and blanked

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).

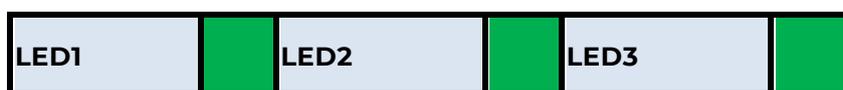
## 1.8 First start

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 available 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 symptoms, 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](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.

**Warning: Potential Security Risk Ahead**

Firefox detected a potential security threat and did not continue to **192.168.10.1**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

**What can you do about it?**

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#) [Advanced...](#)

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 192.168.10.1:8888 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: [SEC\\_ERROR\\_UNKNOWN\\_ISSUER](#)

[View Certificate](#)

[Go Back \(Recommended\)](#) [Accept the Risk and Continue](#)

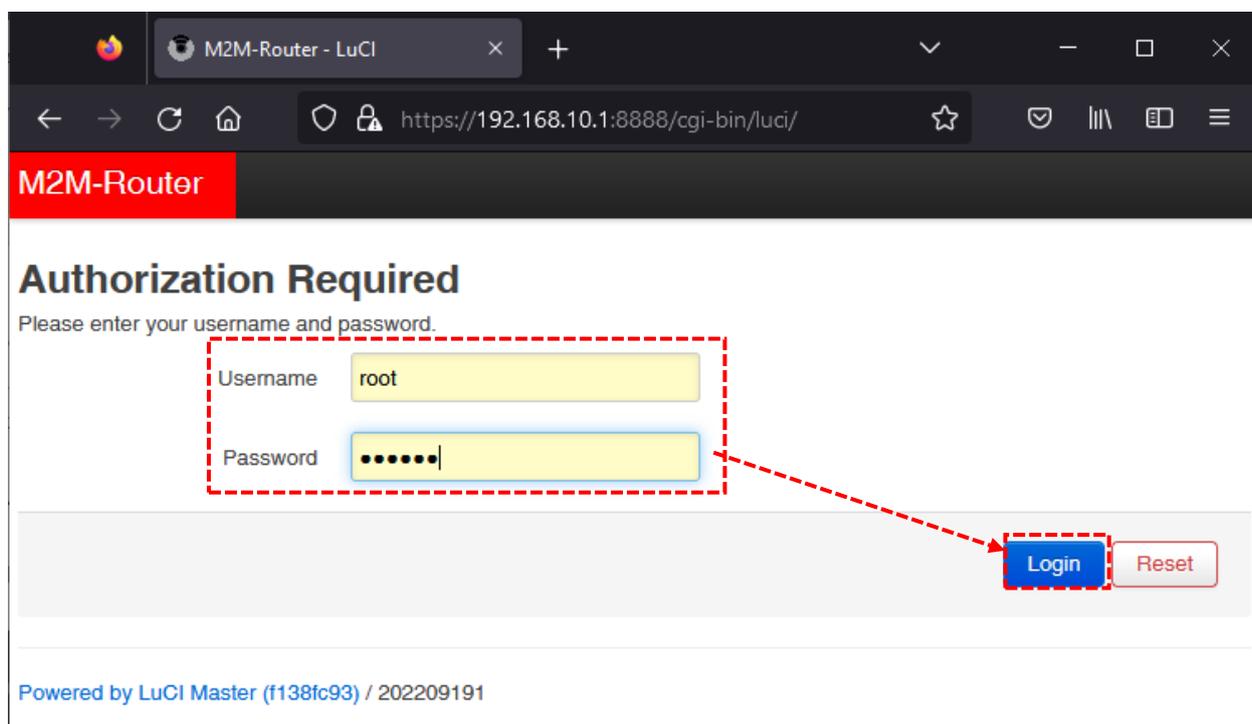
5. Then the router's local web interface will be loaded and you can login.

- **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.



# 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.

**M2M-Router** Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout AUTO REFRESH ON

---

### Status

#### System

Hostname	M2M-Router
Model	Router-Standard
Firmware Version	202209191
Architecture	ARM926EJ-S rev 5 (v5l)
Build Date	2022-10-06 06:17:35.878169453+00:00
Kernel Version	4.9.184
STM32 Firmware	201901181
Local Time	Thu Oct 6 09:17:55 2022
Uptime	0h 20m 29s
Load Average	2.33, 1.22, 0.82

#### Memory

Total Available	<div style="width: 73%;"><div style="width: 73%;"></div></div> 89.23 MB / 122.18 MB (73%)
Free	<div style="width: 69%;"><div style="width: 69%;"></div></div> 84.61 MB / 122.18 MB (69%)
Buffered	<div style="width: 3%;"><div style="width: 3%;"></div></div> 4.62 MB / 122.18 MB (3%)

#### Modem

Modem Model	LE910C1-EU
Firmware Version	25.20.223
MEID	355001090704486
SIM ID	8936200003250172672
Modem RSSI	7
Modem SQ	4
CREG	2,1,"1204","FB8D7F",2
COPS	0,0,"Yettel HU",2

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 **cell 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 significant 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.

**Network**

Active Connections 21 / 16384 (0%)

**Active DHCP Leases**

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
<i>There are no active leases.</i>			

**Active DHCPv6 Leases**

Host	IPv6-Address	DUID	Leasetime remaining
<i>There are no active leases.</i>			

**Dynamic DNS**

DDNS Autostart disabled enable here

Powered by LuCI Master (f138fc93) / 202209191

## 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**.

The screenshot shows the M2M-Router web interface. The top navigation bar includes 'M2M-Router', 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. A green 'AUTO REFRESH ON' button is in the top right. The 'Status' menu is open, showing options: Overview, Firewall, Routes, System Log, Kernel Log, Processes, and Realtime Graphs. The main content area displays system information:

Hostname	M2M-Router
Model	Router-Standard
Firmware Version	202209191

## 2.4 CDMA menu (only for CDMA devices)

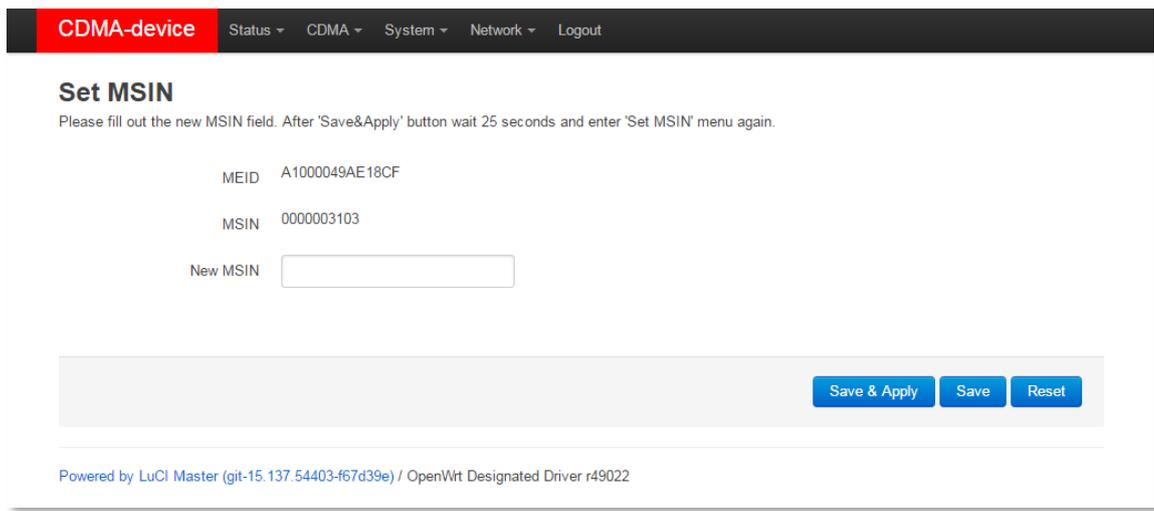
In case of CDMA450 version, the hostname is already configured for *CDMA-450* in the Overview menu (Dashboard).

The screenshot shows the CDMA-device web interface. The top navigation bar includes 'CDMA-device', 'Status', 'CDMA', 'System', 'Network', and 'Logout'. A green 'AUTO REFRESH ON' button is in the top right. The 'Status' menu is open, showing options: Overview, Firewall, Routes, System Log, Kernel Log, Processes, and Realtime Graphs. The main content area displays system information:

Hostname	CDMA-device
Model	Atmel AT91SAM9X25-EK
Firmware Version	OpenWrt Designated Driver (0023-LuCI Master (git-15-137.54.102-67d90e))

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.

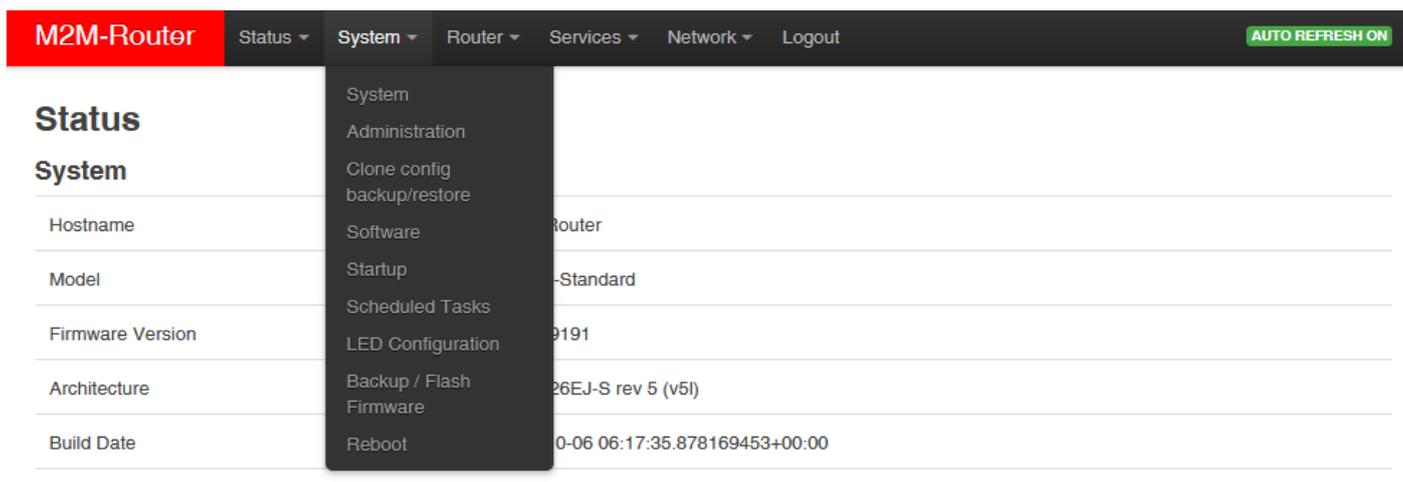


You can store the router settings with the **Save** button. The **Save & Apply** button stores the settings and reconfigures the router related to these settings. **When it was successful, the router will not restart automatically further.**

## 2.5 System menu

You can find 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**

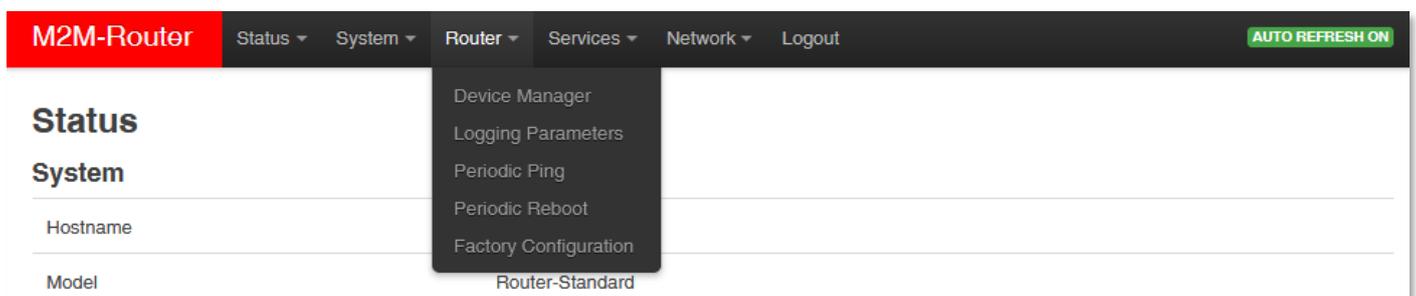


- **Clone config backup / restore** – here you can make a file of the current settings which can be distributable to another router

- Installation of further **Software** (3rd party tools, applications) from the online software repository
- You can setup **Startup** applications 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

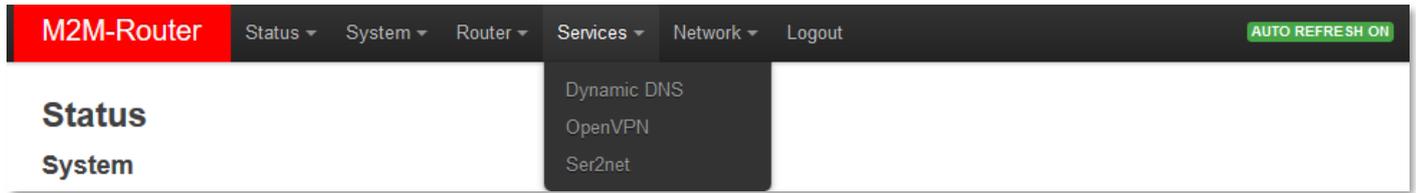


- You can define the remote monitoring software connection settings of the a **Device Manager** (optional remote management software for firmware refresh and reconfiguartion, check QoS).
- You can setup **Logging parameters**
- At the **Periodic Ping** you can configure the cyclic heartbeat ping interval 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

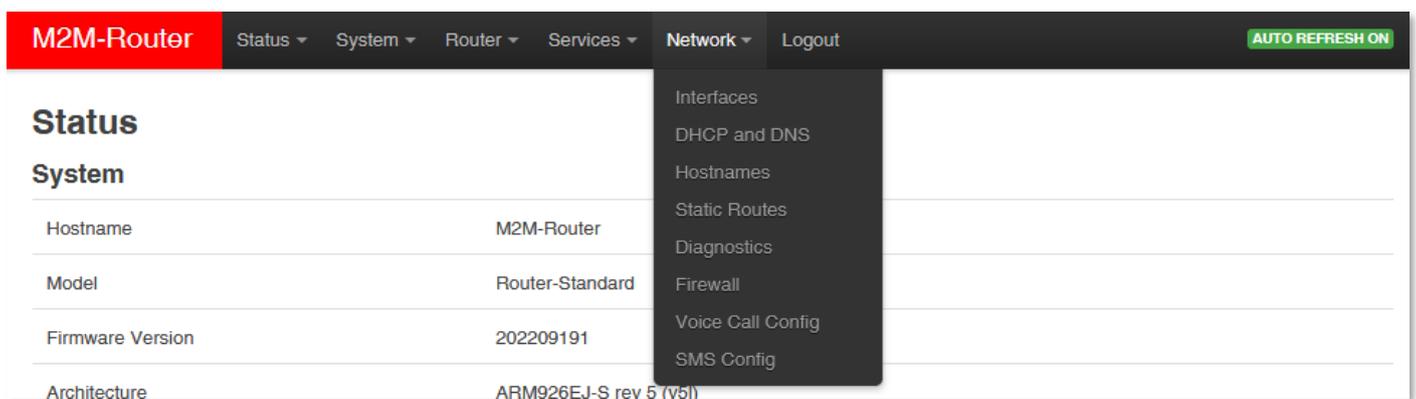
- Here you can setup the **DynDNS** (dynamical DNS) service settings
- And to define the **OpenVPN** client connection settings

- 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 capability, then configure that in the **Network / Interfaces**

menu, remove the **WAN** interface with the  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 interfaces can 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.

The screenshot shows the 'M2M-Router' web interface. At the top, there is a navigation bar with 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout' menus, and an 'AUTO REFRESH ON' button. Below the navigation bar, there are tabs for 'LAN', 'USBLAN', and 'WAN'. The main content area is titled 'Interfaces' and lists three interfaces:

- LAN** (eth0): Protocol: Static address, Uptime: 0h 2m 58s, MAC: 26:97:66:F4:CC:9F, RX: 0 B (0 Pkts.), TX: 0 B (0 Pkts.), IPv4: 192.168.127.1/24. Buttons: Restart, Stop, Edit, Delete.
- USBLAN** (usb0): Protocol: Static address, Uptime: 0h 2m 51s, MAC: 12:57:90:32:1F:58, RX: 58.08 KB (509 Pkts.), TX: 141.44 KB (332 Pkts.), IPv4: 192.168.10.1/24. Buttons: Restart, Stop, Edit, Delete.
- WAN** (4g-wan): Protocol: PPP-4G, RX: 0 B (0 Pkts.), TX: 0 B (0 Pkts.), Information: Not started on boot. Buttons: Edit, Delete.

At the bottom left, there is a button 'Add new interface...'. At the bottom right, there are buttons 'Save & Apply', 'Save', and 'Reset'.

### 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 find 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.

The screenshot shows the M2M-Router configuration interface. At the top, there is a navigation bar with 'M2M-Router' on the left and 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout' on the right. A green 'AUTO REFRESH ON' button is also present. Below the navigation bar, there are tabs for 'LAN', 'USBLAN', and 'WAN', with 'WAN' being the active tab. The main heading is 'Interfaces - WAN'. Below this, there is a descriptive paragraph about configuring network interfaces. The 'Common Configuration' section is active, with sub-tabs for 'General Setup', 'Advanced Settings', and 'Firewall Settings'. The 'General Setup' sub-tab contains the following configuration options:

- Status:** Device: 4g-wan, RX: 0 B (0 Pkts.), TX: 0 B (0 Pkts.)
- Protocol:** 4g
- Disable modem:**
- Wireless network:** No Change (dropdown)
- NB:**  If you know what you are doing.
- Select IoT Technology:** None/Empty (dropdown). Below it is a link: Please read the modem's AT Commands Reference Guide!
- Mobile country code:** (text input)
- Mobile network code:** (text input)
- Dual SIM:**
- SIM #1 APN:** internet (text input)
- PIN:** (text input with asterisk icon)
- SIM #1 PAP/CHAP username:** (text input)
- SIM #1 PAP/CHAP password:** (text input with asterisk icon)
- WAN->LAN port forwarding:** (text input). Below it is a link: hostip1:port1,hostip2:port2,...
- Dial number:** \*99\*\*\*1# (text input)

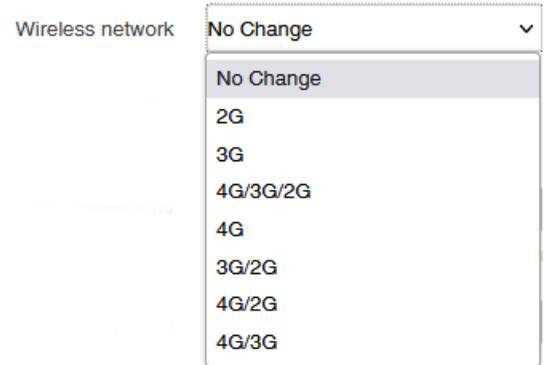
**Attention!**

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

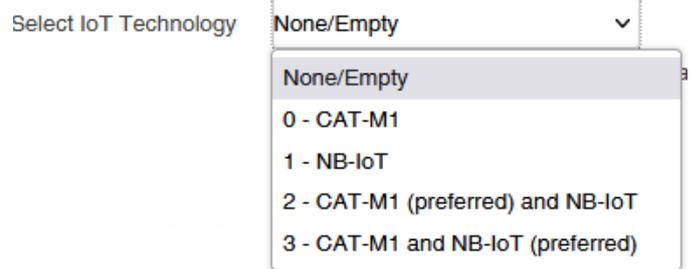
**Wireless network** field – we offer to use the **No Change** option or use the **4G/3G/2G** option (automatic detection mode with 3G/2G „fallback” option).

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 preferred 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.

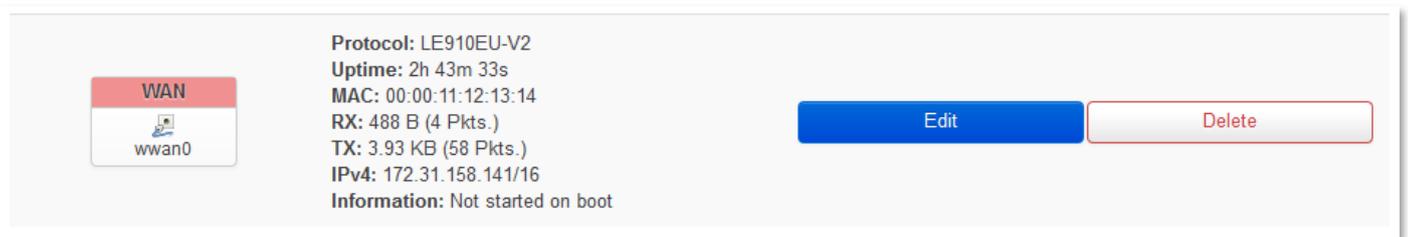
**Attention!**

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 device attempts then connecting to the mobile network.

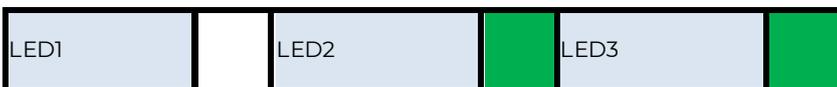
**Once this is done, the router will no longer be constantly restarted!**

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 screenshot shows the M2M-Router configuration interface. At the top, there is a navigation bar with 'M2M-Router' on the left and 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout' on the right. A green 'AUTO REFRESH ON' button is also present. Below the navigation bar, there are tabs for 'LAN', 'USBLAN', and 'WAN', with 'WAN' selected. The main heading is 'Interfaces - WAN'. Below this, there is a descriptive paragraph: 'On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).' Underneath is the 'Common Configuration' section with sub-tabs for 'General Setup', 'Advanced Settings', and 'Firewall Settings', with 'General Setup' selected. The configuration fields include: 'Status' (Device: 4g-wan, RX: 0 B (0 Pkts.), TX: 0 B (0 Pkts.)), 'Protocol' (4g), 'Disable modem' (checkbox), 'Wireless network' (4G/3G/2G dropdown), 'NB' (checkbox with help icon and text 'If you know what you are doing.'), 'Select IoT Technology' (0 - CAT-M1 dropdown with help icon and text 'Please read the modem's AT Commands Reference Guide!'), 'Mobile country code' (text input), 'Mobile network code' (text input), 'Dual SIM' (checkbox), 'SIM #1 APN' (internet text input), 'PIN' (text input with asterisk), 'SIM #1 PAP/CHAP username' (text input), 'SIM #1 PAP/CHAP password' (text input with asterisk), 'WAN->LAN port forwarding' (text input with help icon and text 'hostip1:port1,hostip2:port2,...'), and 'Dial number' (\*99\*\*\*1# text input).

The detailed **LAN** interface settings can be performed by the **Network Interfaces** menu item at the **LAN** interface  button.

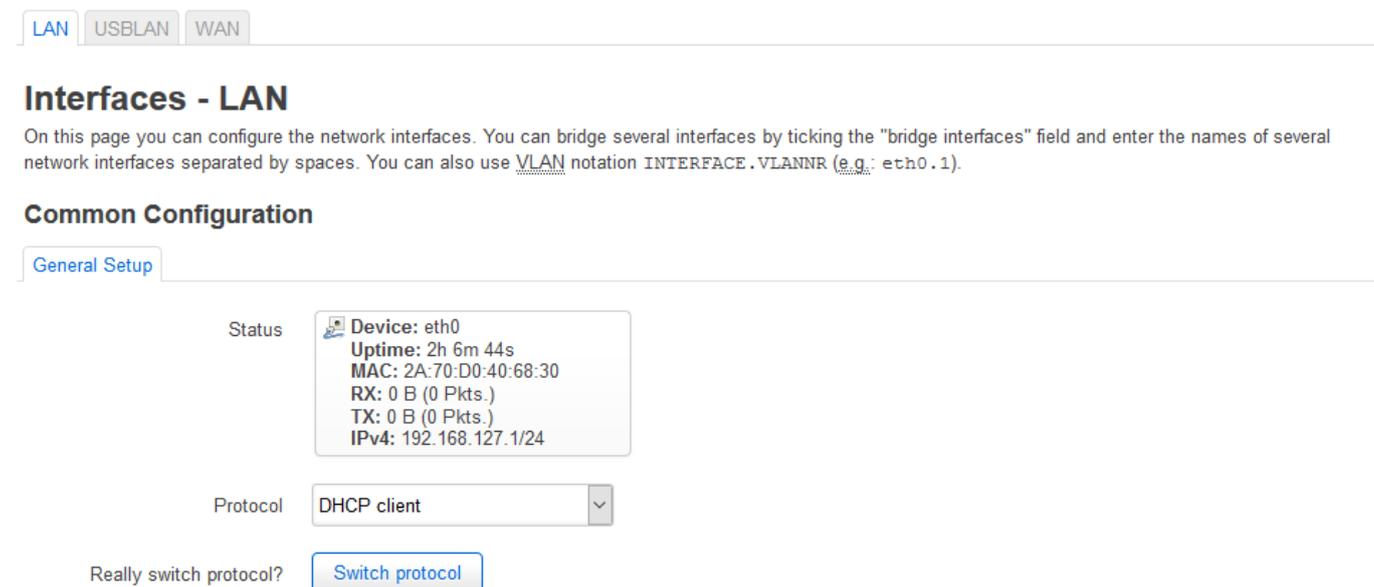
We recommend that you change the router's **default** *192.168.127.1* **address** (IPv4 address) to a custom IP address, depending on your subnet - or the way you want it to be served by the router device.

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  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  button. The DHCP client setting for the ethernet interface will then be active.



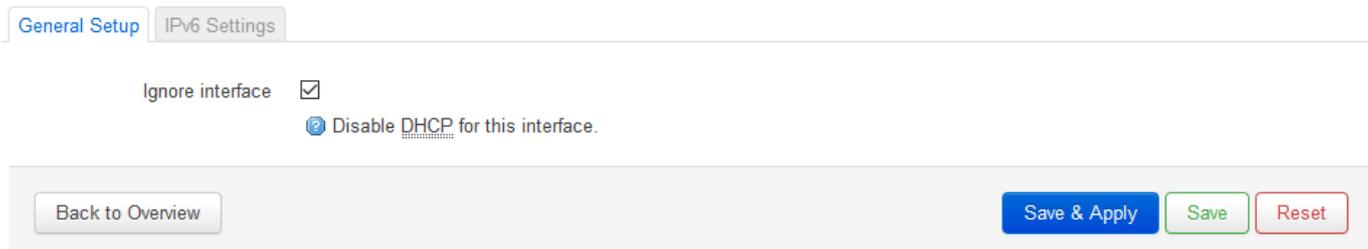
The screenshot shows the configuration page for the LAN interface. At the top, there are tabs for 'LAN', 'USBLAN', and 'WAN'. The main heading is 'Interfaces - LAN'. Below this, there is a descriptive paragraph about configuring network interfaces. Under the 'Common Configuration' section, there is a 'General Setup' tab. The configuration area includes a 'Status' field with a box containing details for the 'eth0' device: 'Uptime: 2h 6m 44s', 'MAC: 2A:70:D0:40:68:30', 'RX: 0 B (0 Pkts.)', 'TX: 0 B (0 Pkts.)', and 'IPv4: 192.168.127.1/24'. Below this is a 'Protocol' dropdown menu currently set to 'DHCP client'. At the bottom, there is a 'Really switch protocol?' label and a 'Switch protocol' button.

When you have modified the settings, save them by the  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).

### DHCP Server



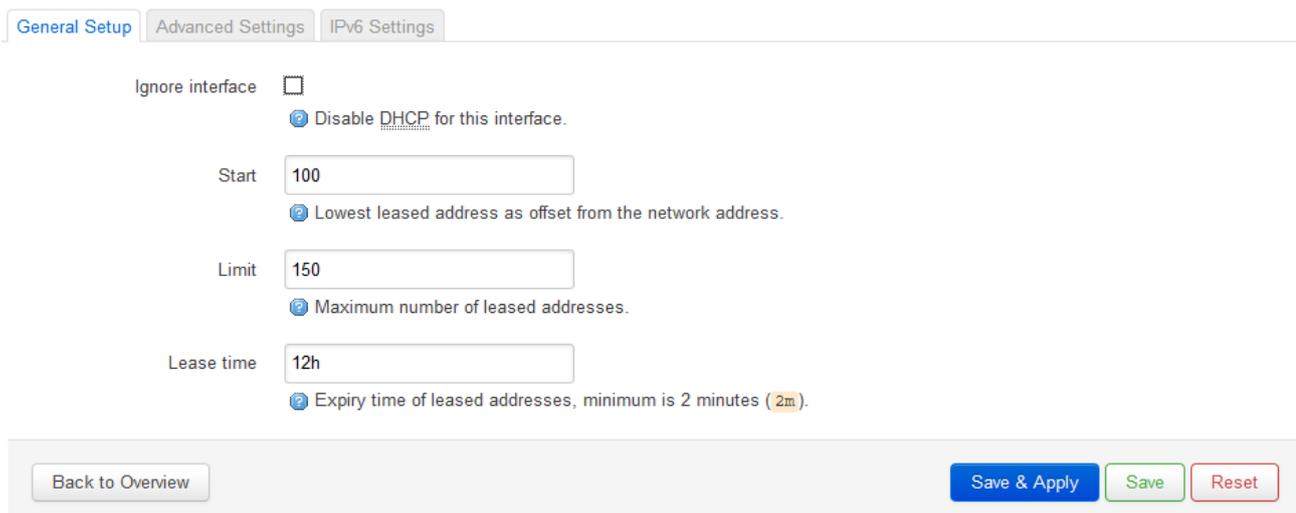
The screenshot shows the 'DHCP Server' configuration page with the 'General Setup' tab selected. The 'Ignore interface' checkbox is checked, and a tooltip indicates 'Disable DHCP for this interface.' At the bottom, there are three buttons: 'Back to Overview', 'Save & Apply', 'Save', and 'Reset'.

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.

### DHCP Server



The screenshot shows the 'DHCP Server' configuration page with the 'Advanced Settings' tab selected. The 'Ignore interface' checkbox is unchecked. The 'Start' field is set to 100, the 'Limit' field is set to 150, and the 'Lease time' field is set to 12h. A tooltip for the 'Lease time' field indicates 'Expiry time of leased addresses, minimum is 2 minutes (2m)'. At the bottom, there are three buttons: 'Back to Overview', 'Save & Apply', 'Save', and 'Reset'.

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

## DHCP Server

General Setup **Advanced Settings** IPv6 Settings

Dynamic DHCP

[?](#) Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force

[?](#) Force DHCP on this network even if another server is detected.

IPv4-Netmask

[?](#) Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options

+  
[?](#) Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

[Back to Overview](#)

[Save & Apply](#)

[Save](#)

[Reset](#)

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*).

### Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
----------	--------------	-------------	---------------------

*There are no active leases.*

### Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
------	--------------	------	---------------------

*There are no active leases.*

### Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	DUID	IPv6-Suffix (hex)
----------	-------------	--------------	------------	------	-------------------

*This section contains no values yet*

[Add](#)

[Save & Apply](#)

[Save](#)

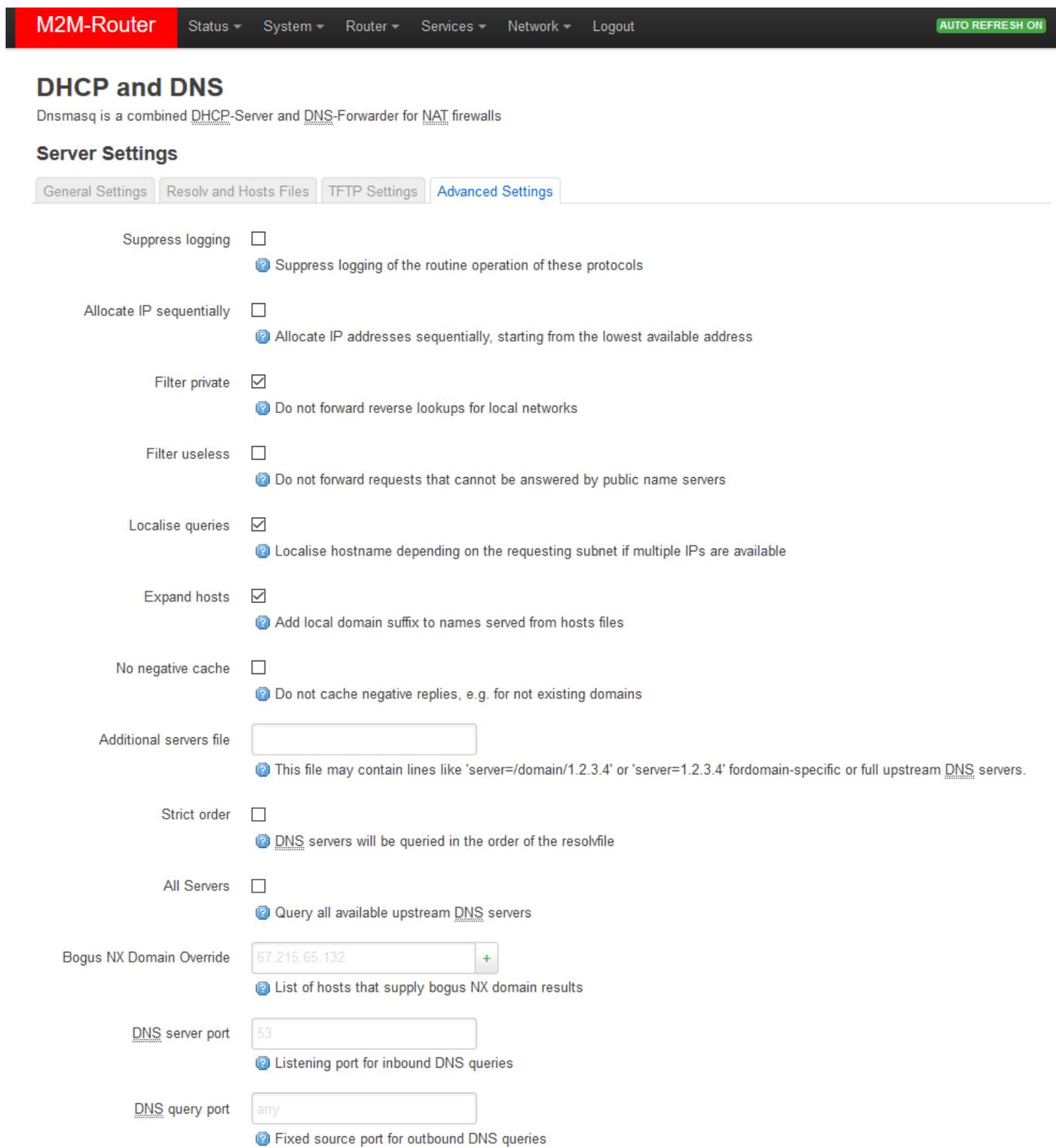
[Reset](#)

In the **Static Leases** part you can [Add](#) 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 choosing the **Advanced Settings** tab.



The screenshot shows the M2M-Router web interface. At the top, there is a navigation bar with 'M2M-Router' on the left and 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout' on the right. A green 'AUTO REFRESH ON' button is also visible. Below the navigation bar, the page title is 'DHCP and DNS'. A subtitle reads: 'Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls'. The main section is titled 'Server Settings' and contains several tabs: 'General Settings', 'Resolve and Hosts Files', 'TFTP Settings', and 'Advanced Settings'. The 'Advanced Settings' tab is active. The settings are as follows:

- Suppress logging:  (Help icon) Suppress logging of the routine operation of these protocols
- Allocate IP sequentially:  (Help icon) Allocate IP addresses sequentially, starting from the lowest available address
- Filter private:  (Help icon) Do not forward reverse lookups for local networks
- Filter useless:  (Help icon) Do not forward requests that cannot be answered by public name servers
- Localise queries:  (Help icon) Localise hostname depending on the requesting subnet if multiple IPs are available
- Expand hosts:  (Help icon) Add local domain suffix to names served from hosts files
- No negative cache:  (Help icon) Do not cache negative replies, e.g. for not existing domains
- Additional servers file:  (Help icon) This file may contain lines like 'server=/domain/1.2.3.4' or 'server=1.2.3.4' for domain-specific or full upstream DNS servers.
- Strict order:  (Help icon) DNS servers will be queried in the order of the resolvfile
- All Servers:  (Help icon) Query all available upstream DNS servers
- Bogus NX Domain Override:  + (Help icon) List of hosts that supply bogus NX domain results
- DNS server port:  (Help icon) Listening port for inbound DNS queries
- DNS query port:  (Help icon) Fixed source port for outbound DNS queries

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

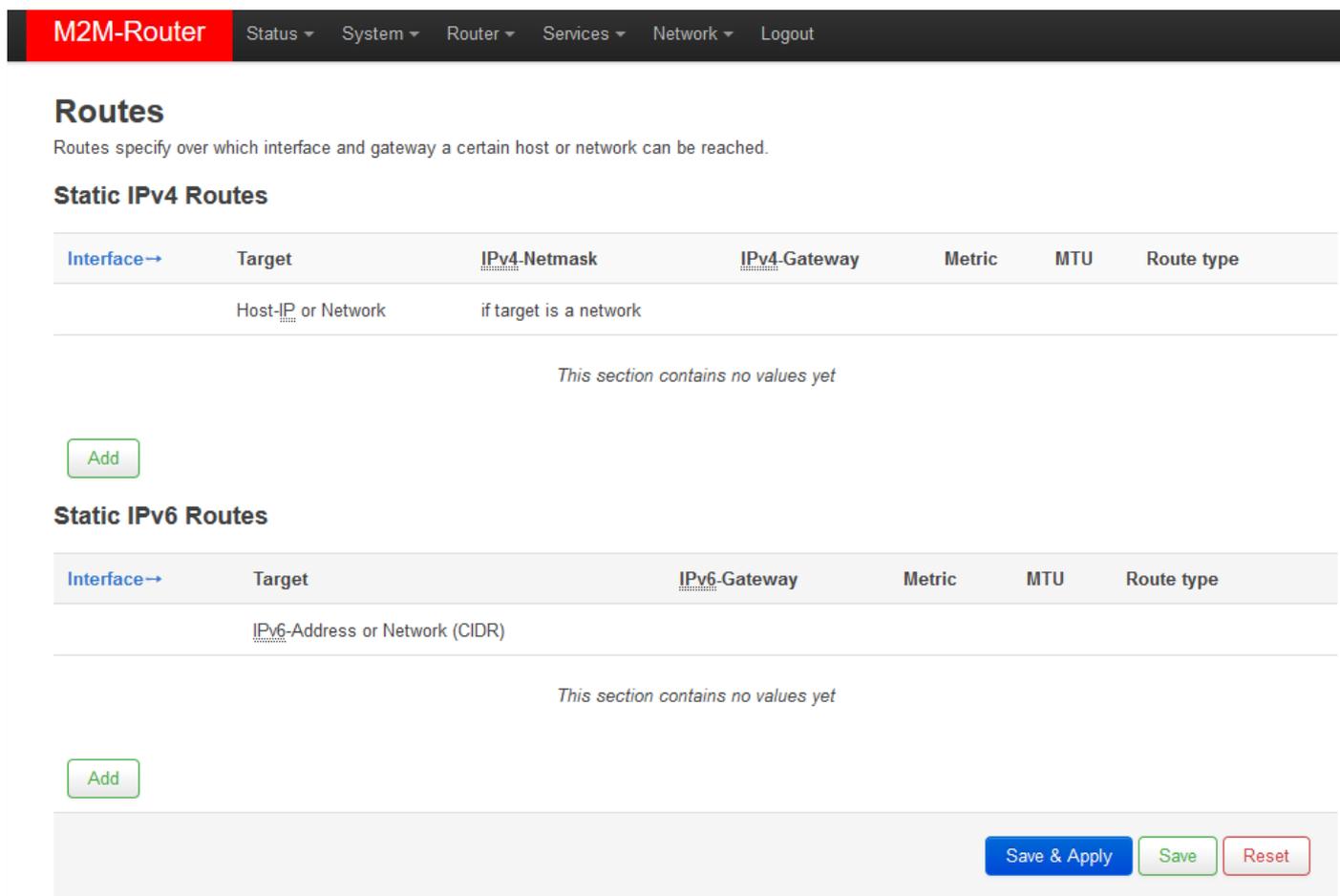
When you have modified the settings, save them by the **Save & Apply** button.

## 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  button.

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



The screenshot shows the M2M-Router configuration interface. At the top, there is a navigation bar with the following items: M2M-Router, Status, System, Router, Services, Network, and Logout. Below the navigation bar, the page title is "Routes" with a subtitle: "Routes specify over which interface and gateway a certain host or network can be reached."

The main content area is divided into two sections:

- Static IPv4 Routes**: This section contains a table with the following columns: Interface, Target, IPv4-Netmask, IPv4-Gateway, Metric, MTU, and Route type. Below the table, there is a placeholder text: "This section contains no values yet".
- Static IPv6 Routes**: This section contains a table with the following columns: Interface, Target, IPv6-Gateway, Metric, MTU, and Route type. Below the table, there is a placeholder text: "This section contains no values yet".

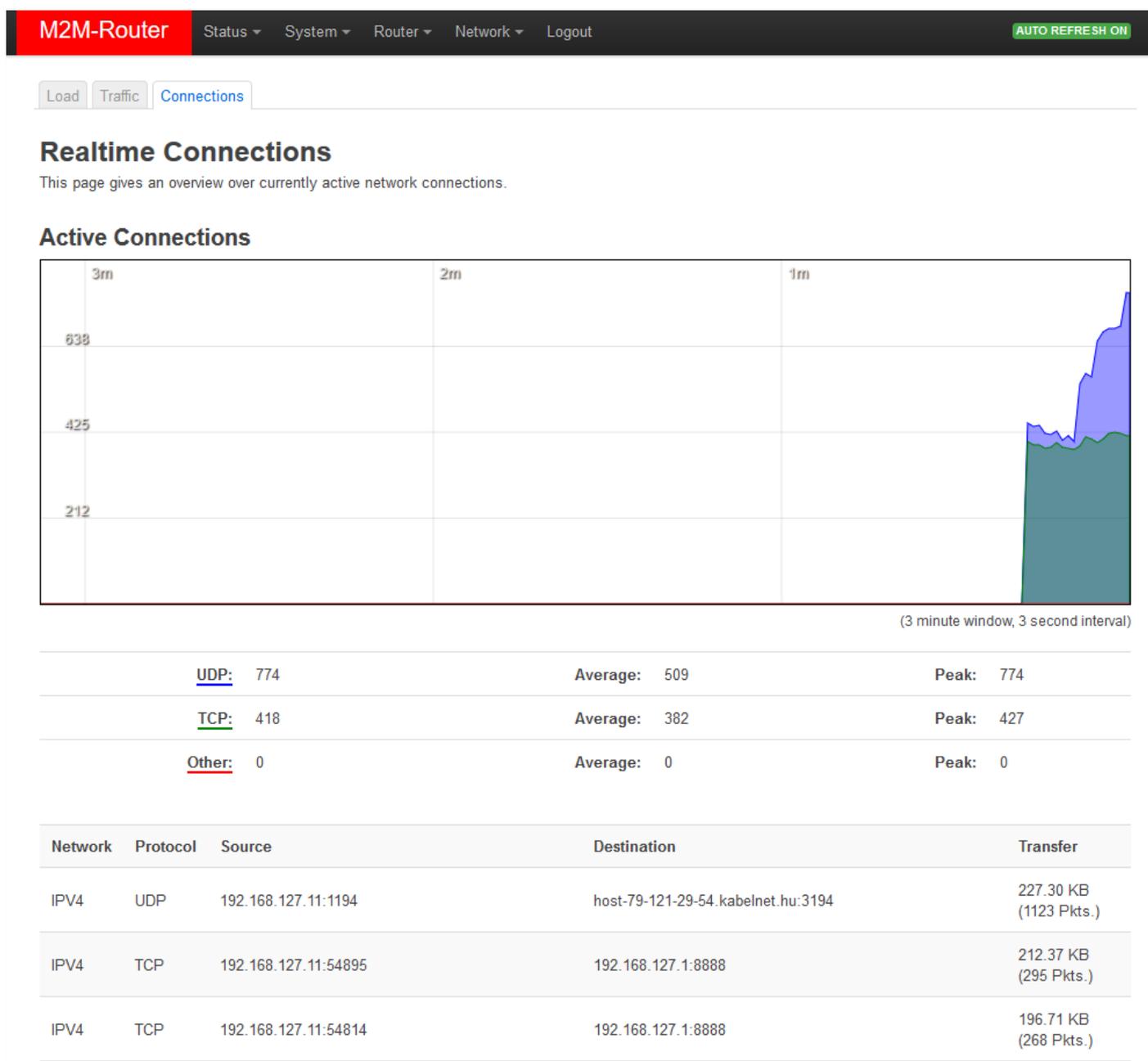
Each section has an "Add" button below it. At the bottom right of the page, there are three buttons: "Save & Apply", "Save", and "Reset".

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 occurred 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 be the whole disabling with opening and enabling only necessary communication ports, IP-segments or allowing exact IPs.

M2M-Router

[Status](#) [System](#) [Router](#) [Services](#) [Network](#) [Logout](#)
AUTO REFRESH ON

---

## Firewall Status

IPv4 Firewall
IPv6 Firewall

Hide empty chains
Reset Counters
Restart Firewall

**Table: Filter**

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
150	10.66 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
1.98 K	216.58 KB	<a href="#">input_rule</a>	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
1.91 K	211.57 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
21	1.09 KB	<a href="#">syn_flood</a>	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
0	0 B	<a href="#">zone_lan_input</a>	all	eth0	*	0.0.0.0/0	0.0.0.0/0	-	-
67	5.01 KB	<a href="#">zone_lan_input</a>	all	usb0	*	0.0.0.0/0	0.0.0.0/0	-	-

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	<a href="#">forwarding_rule</a>	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
0	0 B	<a href="#">zone_lan_forward</a>	all	eth0	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	<a href="#">zone_lan_forward</a>	all	usb0	*	0.0.0.0/0	0.0.0.0/0	-	-

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
150	10.66 KB	ACCEPT	all	*	lo	0.0.0.0/0	0.0.0.0/0	-	-
2.05 K	522.49 KB	<a href="#">output_rule</a>	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom output rule chain

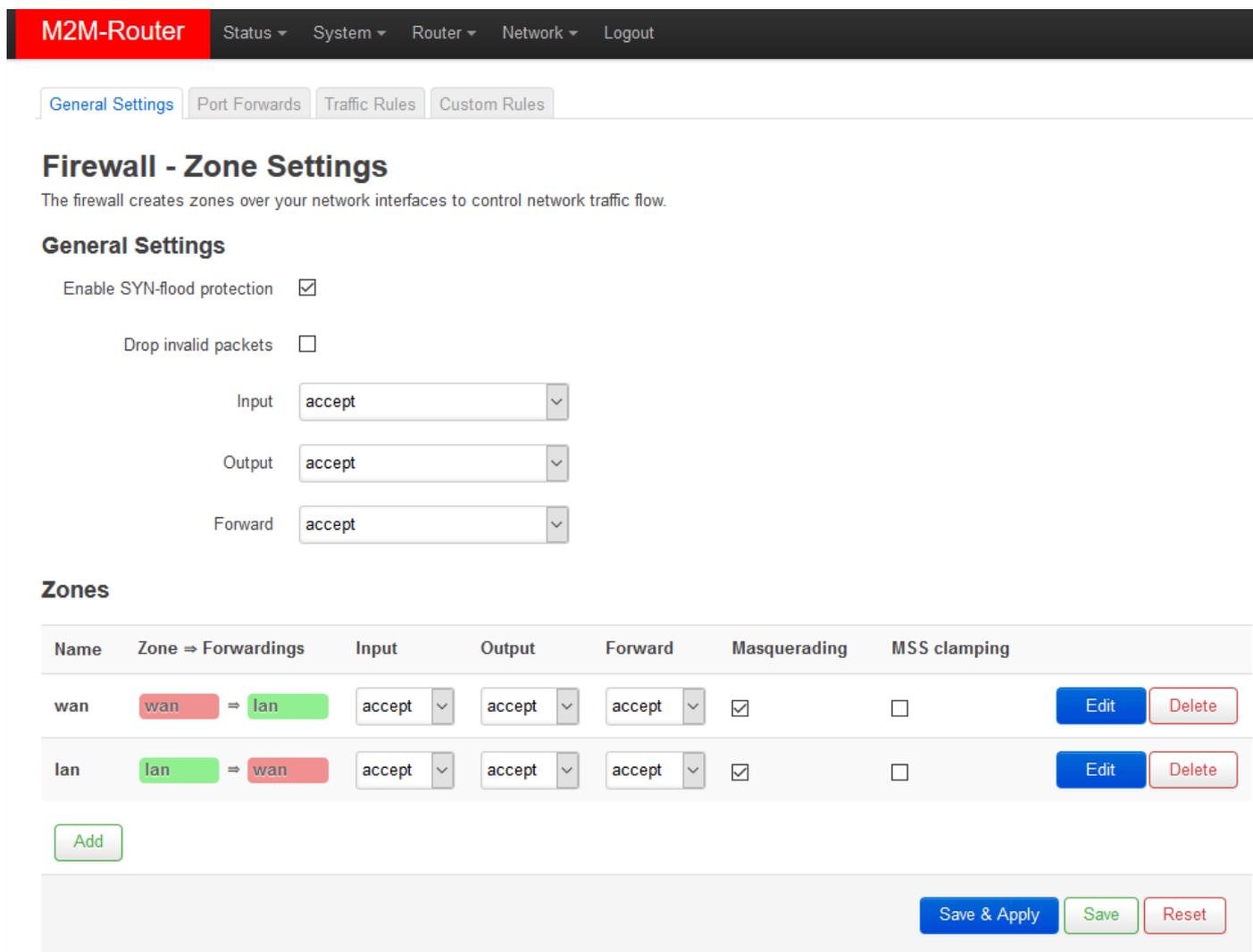
You can modify firewall settings at **Network / Firewall** menu, **General Settings** tab.

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  modify.

At the **Zones** part you can  a new rule to the current ones. You also can  or  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).



**M2M-Router** Status ▾ System ▾ Router ▾ Network ▾ Logout

[General Settings](#) [Port Forwards](#) [Traffic Rules](#) [Custom Rules](#)

## Firewall - Zone Settings

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

### General Settings

Enable SYN-flood protection

Drop invalid packets

Input

Output

Forward

### Zones

Name	Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
wan	wan ⇒ lan	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>
lan	lan ⇒ wan	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Edit</a> <a href="#">Delete</a>

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

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.

The screenshot shows the M2M-Router web interface. At the top, there is a navigation bar with 'M2M-Router' in a red box and menu items: Status, System, Router, Network, and Logout. Below this is a breadcrumb trail: General Settings > Port Forwards > Traffic Rules > Custom Rules. The main heading is 'Firewall - Zone Settings - Zone "wan"'. Underneath, there is a sub-heading 'Zone "wan"' and a descriptive paragraph: 'This section defines common properties of "wan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.' There are two tabs: 'General Settings' (active) and 'Advanced Settings'. The 'General Settings' tab contains several configuration options: 'Restrict to address family' is set to 'IPv4 only' in a dropdown; 'Restrict Masquerading to given source subnets' and 'Restrict Masquerading to given destination subnets' are both set to '0.0.0.0/0' with copy icons; 'Force connection tracking' and 'Enable logging on this zone' are both unchecked checkboxes. Below this is the 'Inter-Zone Forwarding' section with a descriptive paragraph: 'The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic originating from "wan". *Source zones* match forwarded traffic from other zones targeted at "wan". The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.' There are two checked checkboxes: 'Allow forward to destination zones:' and 'Allow forward from source zones:'. Each has a green button with 'lan:', 'lan:', and 'usblan:' and copy icons. At the bottom, there is a 'Back to Overview' button with a left arrow, and three buttons: 'Save & Apply', 'Save', and 'Reset'.

**M2M-Router** Status System Router Services Network Logout

General Settings Port Forwards **Traffic Rules** Custom Rules

## Firewall - Traffic Rules

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

### Traffic Rules

Name	Match	Action	Enable
<i>This section contains no values yet</i>			

### Open ports on router

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

### New forward rule

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

## 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 addresses.

**M2M-Router** Status System Router Services Network Logout

General Settings **Port Forwards** Traffic Rules Custom Rules

## Firewall - Port Forwards

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

### Port Forwards

Name	Match	Forward to	Enable
<i>This section contains no values yet</i>			

### New port forward

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
<input type="text" value="New port forward"/>	TCP+U	wan	<input type="text"/>	lan	-- Please choose --	<input type="text"/>

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.

The screenshot shows the M2M-Router web interface. At the top, there is a navigation bar with 'M2M-Router' and several menu items: Status, System, Router, Services, Network, and Logout. Below this, there are tabs for 'General Settings', 'Port Forwards', 'Traffic Rules' (which is selected), and 'Custom Rules'. The main heading is 'Firewall - Traffic Rules'. A descriptive text states: 'Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.' Below this, there is a section titled 'Traffic Rules' with a table header: 'Name', 'Match', 'Action', and 'Enable'. The table is currently empty, with a message below it: 'This section contains no values yet'. Underneath, there is a section 'Open ports on router' with a table header: 'Name', 'Protocol', and 'External port'. The form shows 'New input rule' in the Name field, 'TCP+UDP' in the Protocol dropdown, and an empty External port field. An 'Add' button is to the right. Below that is 'New forward rule' with a table header: 'Name', 'Source zone', and 'Destination zone'. The form shows 'New forward rule' in the Name field, 'wan' in the Source zone dropdown, and 'lan' in the Destination zone dropdown. An 'Add and edit...' button is to the right. The next section is 'Source NAT' with a descriptive text: 'Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.' Below this is another empty table with header: 'Name', 'Match', 'Action', and 'Enable', and the message 'This section contains no values yet'. At the bottom, there is a section 'New source NAT' with a table header: 'Name', 'Source zone', 'Destination zone', 'To source IP', and 'To source port'. The form shows 'New SNAT rule' in the Name field, 'lan' in the Source zone dropdown, 'wan' in the Destination zone dropdown, '-- Please choose --' in the To source IP dropdown, and 'Do not rewrite' in the To source port field. An 'Add and edit...' button is to the right. At the very bottom right, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red).

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.

### Source NAT

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

Name	Match	Action	Enable
------	-------	--------	--------

*This section contains no values yet*

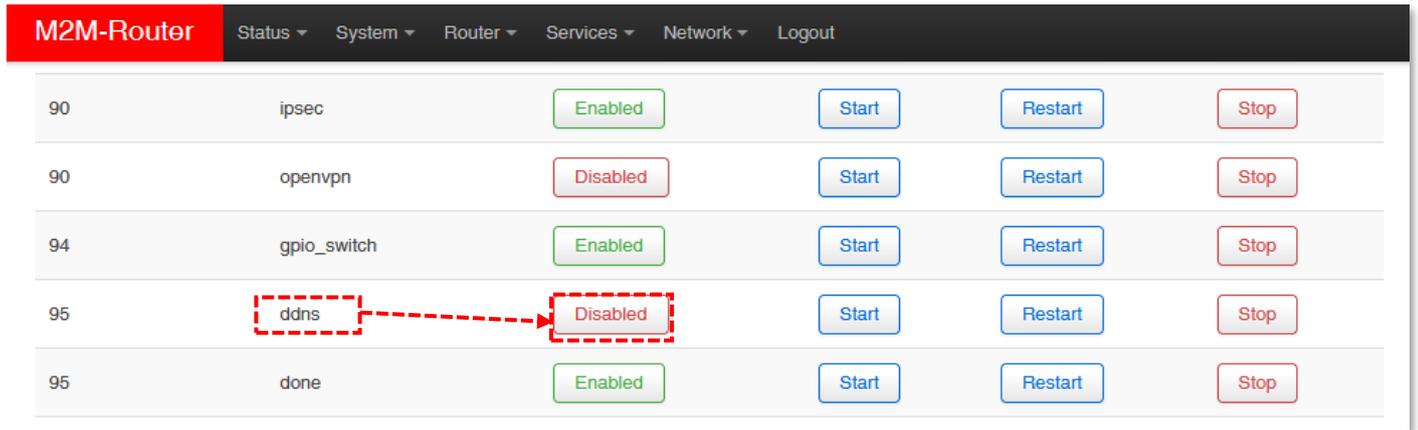
### New source NAT

Name	Source zone	Destination zone	To source IP	To source port
<input type="text" value="New SNAT rule"/>	<input type="text" value="lan"/> ▼	<input type="text" value="wan"/> ▼	<input type="text" value="-- Please choose --"/> ▼	<input type="text" value="Do not rewrite"/>

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.

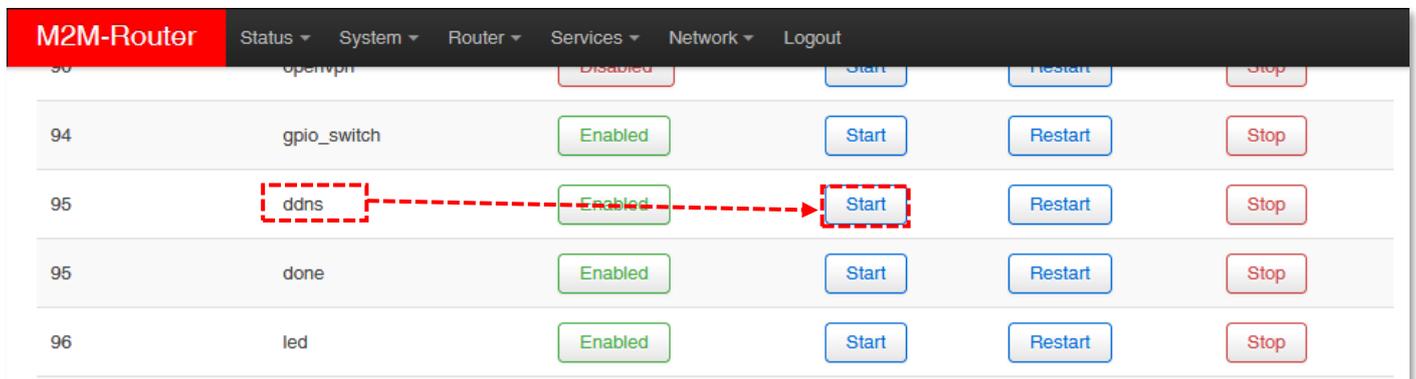


The screenshot shows the 'Services' menu in the M2M-Router interface. The 'ddns' service is currently disabled. A red dashed box highlights the 'ddns' service name and its 'Disabled' status, with a red arrow pointing from the name to the status.

ID	Service Name	Status	Start	Restart	Stop
90	ipsec	Enabled	Start	Restart	Stop
90	openvpn	Disabled	Start	Restart	Stop
94	gpio_switch	Enabled	Start	Restart	Stop
95	ddns	Disabled	Start	Restart	Stop
95	done	Enabled	Start	Restart	Stop

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.

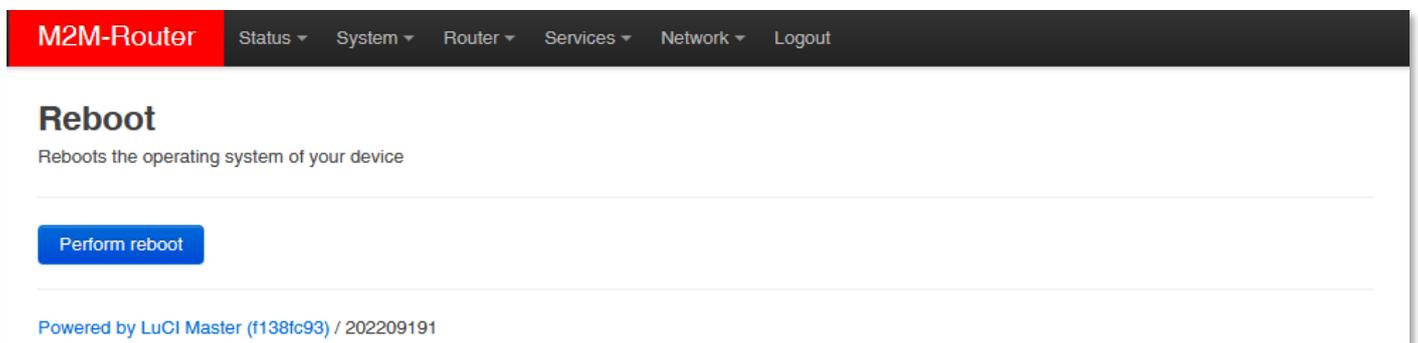
Then push to the **start** button of the line of the „**ddns**” service to start the feature.



The screenshot shows the 'Services' menu after the 'ddns' service has been enabled. A red dashed box highlights the 'ddns' service name and its 'Enabled' status, with a red arrow pointing from the name to the status.

ID	Service Name	Status	Start	Restart	Stop
90	openvpn	Disabled	Start	Restart	Stop
94	gpio_switch	Enabled	Start	Restart	Stop
95	ddns	Enabled	Start	Restart	Stop
95	done	Enabled	Start	Restart	Stop
96	led	Enabled	Start	Restart	Stop

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



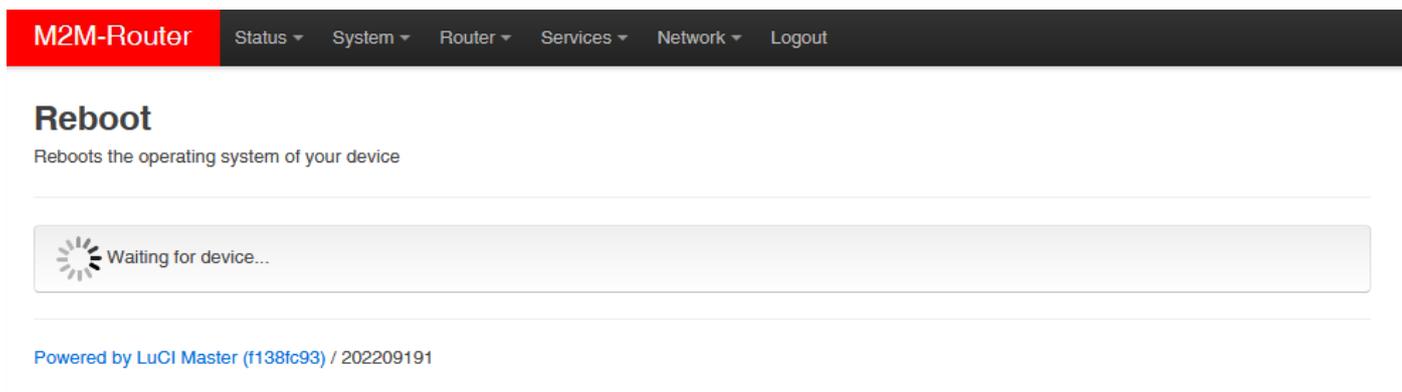
The screenshot shows the 'Reboot' menu in the M2M-Router interface. It includes a 'Perform reboot' button and a footer indicating the device is powered by LuCI Master (f138fc93) / 202209191.

**Reboot**  
Reboots the operating system of your device

[Perform reboot](#)

Powered by LuCI Master (f138fc93) / 202209191

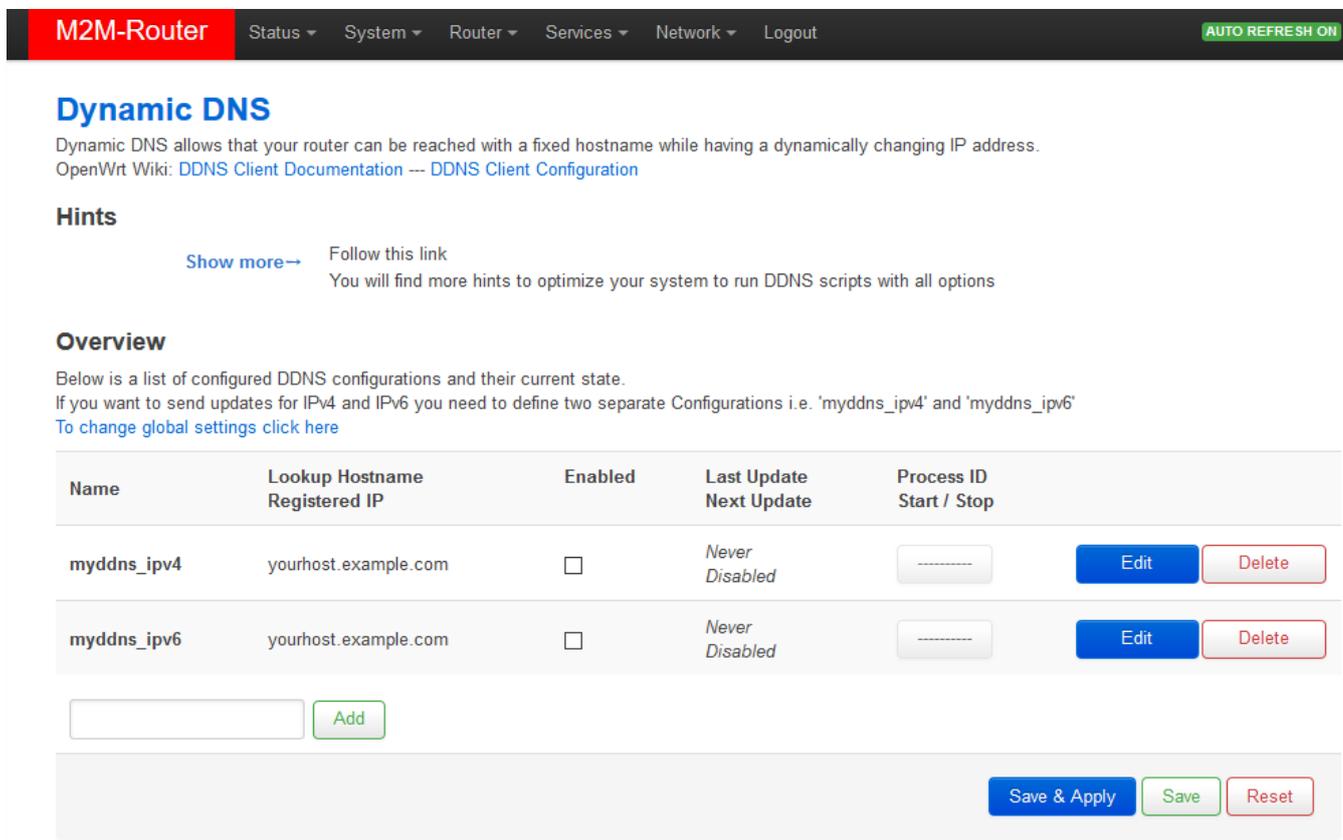
There push to the **Perform reboot** button.



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 screenshot shows the 'Device Manager Parameters' configuration page in the M2M-Router interface. The page has a dark navigation bar at the top with 'M2M-Router' in red and several menu items: Status, System, Router, Services, Network, and Logout. Below the navigation bar, the title 'Device Manager Parameters' is displayed, followed by the instruction 'Carefully change the parameters.' The configuration fields are as follows:

- Local DM Server Port Number: 443 (with a note: 'After change applied, please reboot device!')
- DM Name: something
- DM User Name: root
- CALL DM IP Address: (empty field)
- CALL DM Port Number: (empty field)
- Static WAN IP Address:  (with a note: 'Disable WAN up CALL.')
- CALL Timeout: 30 (with a note: 'Next CALL when sending fails.')

At the bottom right of the form, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red).

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

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

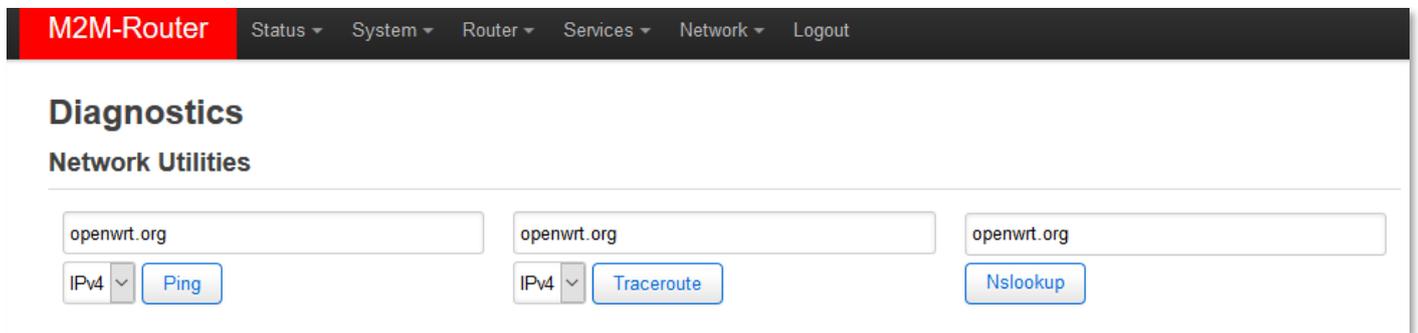
If you modified the settings, save them by the **Save & Apply** button.

## 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.



The screenshot shows the 'M2M-Router' web interface. At the top, there is a navigation bar with 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout' menus. Below this, the 'Diagnostics' section is active, showing 'Network Utilities'. There are three input fields, each containing the text 'openwrt.org'. Underneath each field are buttons for 'IPv4', 'Ping', 'Traceroute', and 'Nslookup'.

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

```
PING lede-project.org (139.59.209.225): 56 data bytes
64 bytes from 139.59.209.225: seq=0 ttl=54 time=29.080 ms
64 bytes from 139.59.209.225: seq=1 ttl=54 time=28.597 ms
64 bytes from 139.59.209.225: seq=2 ttl=54 time=26.848 ms
64 bytes from 139.59.209.225: seq=3 ttl=54 time=28.095 ms
64 bytes from 139.59.209.225: seq=4 ttl=54 time=27.842 ms

--- lede-project.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 26.848/28.092/29.080 ms
```

### **Important!**

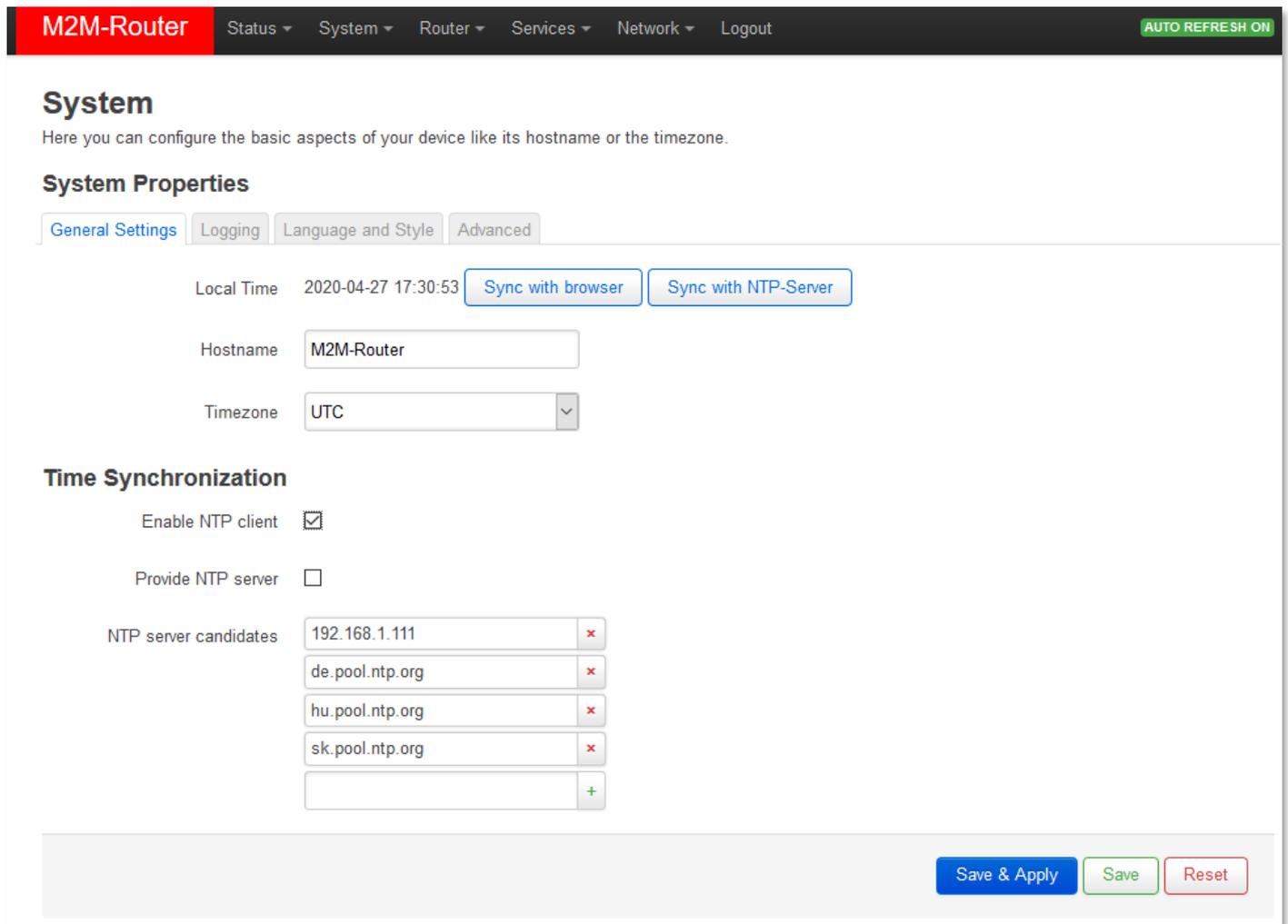
Check only IP addresses, which are available to access from the current IP segment and APN zone for sure (e.g. from an enclosed APN zone the router will not access the public internet, and from the public internet it will not access the enclosed M2M APN zone).

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)**.



The screenshot shows the 'System' configuration page for an 'M2M-Router'. The page has a navigation bar at the top with 'M2M-Router' in red, and dropdown menus for 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. A green 'AUTO REFRESH ON' button is in the top right. The main content area is titled 'System' and includes a subtitle: 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Below this is the 'System Properties' section with tabs for 'General Settings', 'Logging', 'Language and Style', and 'Advanced'. The 'General Settings' tab is active, showing 'Local Time' as '2020-04-27 17:30:53' with buttons for 'Sync with browser' and 'Sync with NTP-Server'. The 'Hostname' is 'M2M-Router' and the 'Timezone' is 'UTC'. The 'Time Synchronization' section has 'Enable NTP client' checked and 'Provide NTP server' unchecked. Under 'NTP server candidates', there are four entries: '192.168.1.111', 'de.pool.ntp.org', 'hu.pool.ntp.org', and 'sk.pool.ntp.org', each with a red 'x' delete button. A green '+' button is at the bottom of the list. At the bottom right of the page are 'Save & Apply', 'Save', and 'Reset' buttons.

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.

M2M-Router Status System Router Services Network Logout UNSAVED CHANGES: 1

## Hostnames

Host entries

Hostname	IP address	
<input type="text" value="MyRouter_1"/>	192.168.10.1 (12:57:90:32:1F:58) ▾	<input type="button" value="Delete"/>

You can assign the selected hostnames to the IP address with the  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  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  button.

## DHCP and DNS

Dnsmasq is a combined [DHCP-Server](#) and [DNS-Forwarder](#) for [NAT](#) firewalls

### Server Settings

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

Enable TFTP server

TFTP server root

Root directory for files served via TFTP

Network boot image

Filename of the boot image advertised to clients

### Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
----------	--------------	-------------	---------------------

*There are no active leases.*

### Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
------	--------------	------	---------------------

*There are no active leases.*

### Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the **Add** Button to add a new lease entry. The **MAC-Address** identifies the host, the **IPv4-Address** specifies the fixed address to use, and the **Hostname** is assigned as a symbolic name to the requesting host. The optional **Lease time** can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	DUID	IPv6-Suffix (hex)
----------	-------------	--------------	------------	------	-------------------

*This section contains no values yet*

Add

Save & Apply

Save

Reset

## 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.

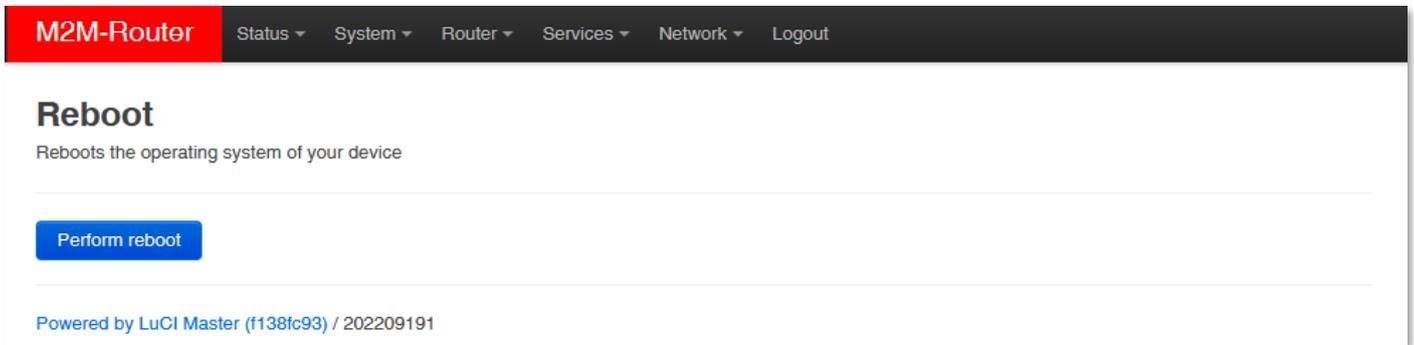
M2M-Router		Status ▾	System ▾	Router ▾	Services ▾	Network ▾	Logout
18	gpio	Enabled			Start	Restart	Stop
19	dnsmasq	Enabled			Start	Restart	Stop
19	dropbear	Enabled			Start	Restart	Stop
19	firewall	Enabled			Start	Restart	Stop
20	network	Enabled			Start	Restart	Stop
35	odhcpd	Enabled			Start	Restart	Stop
45	modemd	Enabled			Start	Restart	Stop
50	cron	Enabled			Start	Restart	Stop
50	uhttpd	Enabled			Start	Restart	Stop
75	ser2net	Disabled			Start	Restart	Stop
80	ucitrack	Enabled			Start	Restart	Stop
90	ipsec	Disabled			Start	Restart	Stop
90	openvpn	Disabled			Start	Restart	Stop
94	gpio_switch	Enabled			Start	Restart	Stop

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

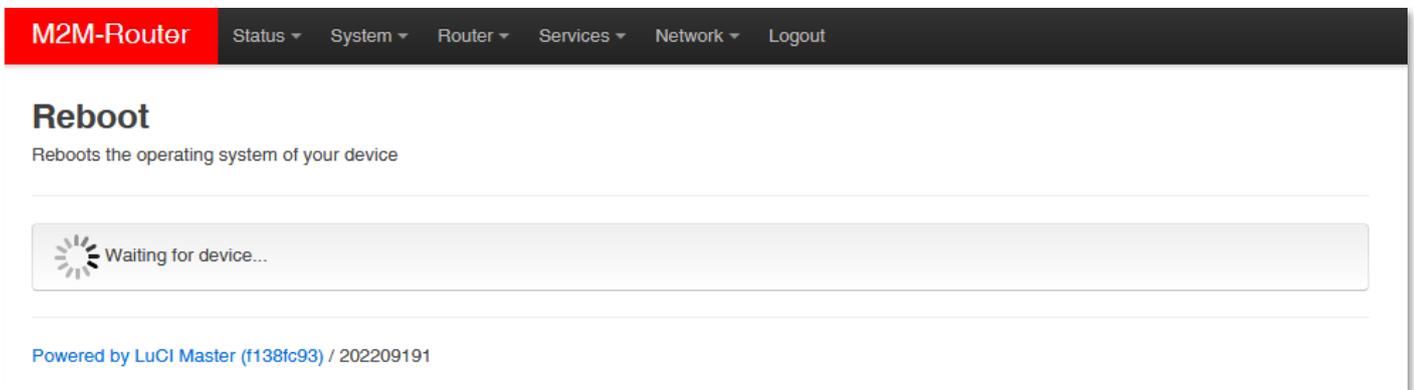
M2M-Router		Status ▾	System ▾	Router ▾	Services ▾	Network ▾	Logout
45	modemd	Enabled			Start	Restart	Stop
50	cron	Enabled			Start	Restart	Stop
50	uhttpd	Enabled			Start	Restart	Stop
75	ser2net	Enabled			Start	Restart	Stop
80	ucitrack	Enabled			Start	Restart	Stop

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  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

## Ser2net

The ser2net allows telnet and tcp sessions to be established with a unit's serial ports.

### Proxies

The program comes up normally as a service, opens the TCP ports specified in the configuration file, and waits for connections.

Once a connection occurs, the program attempts to set up the connection and open the serial port.

If another user is already using the connection or serial port, the connection is refused with an error message.

[Delete](#)

RS485

TCP Port

- Name or number of the TCP/IP port to accept connections from for this device.  
A port number may be of the form [host,]port, such as 127.0.0.1,2000 or localhost,2000.  
If this is specified, it will only bind to the IP address specified for the port.  
Otherwise, it will bind to all the ports on the machine.

State

- Either raw or rawlp or telnet or off. off disables the port from accepting connections.  
It can be turned on later from the control port.  
raw enables the port and transfers all data as-is between the port and the long.  
rawlp enables the port and transfers all input data to device, device is open without any termios setting.  
It allow to use /dev/lpX devices and printers connected to them.  
telnet enables the port and runs the telnet protocol on the port to set up telnet parameters. This is most useful for using telnet.

Timeout

- The time (in seconds) before the port will be disconnected if there is no activity on it.  
A zero value disables this functon.

Device

- The name of the device to connect to.  
This must be in the form of /dev/.

Options

- Sets operational parameters for the serial port.  
Values may be separated by spaces or commas.  
Options 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 set the various baud rates. EVEN, ODD, NONE set the parity.  
1STOPBIT, 2STOPBITS set the number of stop bits.  
7DATABITS, 8DATABITS set the number of data bits. [-]XONXOFF turns on (- off) XON/XOFF support.  
[-]RTSCTS turns on (- off) hardware flow control.  
[-]LOCAL ignores (- checks) the modem control lines (DCD, DTR, etc.) [-]HANGUP\_WHEN\_DONE lowers (- does not lower) the modem control lines (DCD, DTR, etc.) when the connection closes.  
NOBREAK Disables automatic clearing of the break setting of the port.  
remctl allows remote control of the serial port parameters via RFC 2217.

the README for more info. displays the given banner when a user connects to the port.

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.*

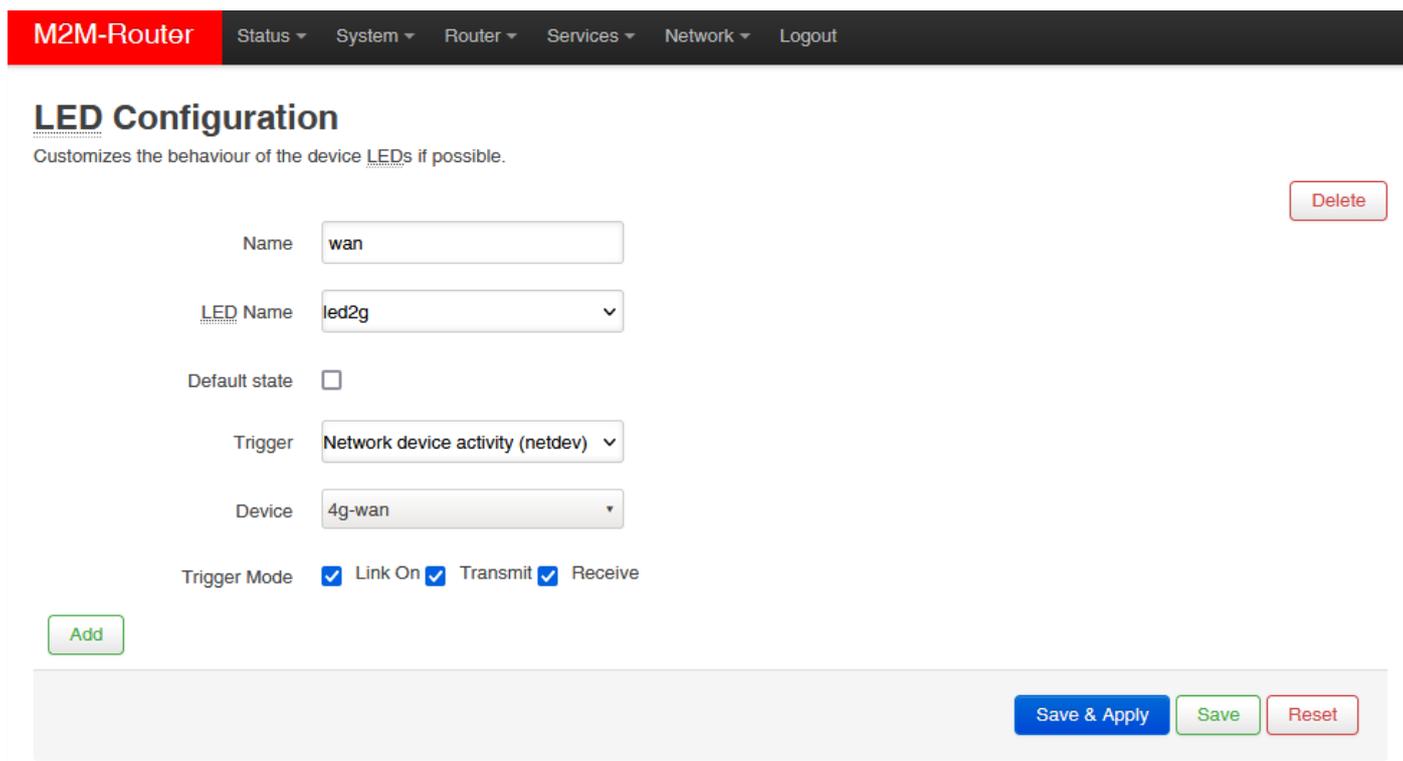
## 5.7 LED configuration

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:

- *led2g* – **LED2 green** light
- *led1r* – **LED1 red** light
- *led2r* – **LED2 red** light
- *led3r* – **LED3 red** light

Only free LEDs that are not reserved are displayed.



The screenshot shows the 'LED Configuration' page in the M2M-Router web interface. The page title is 'LED Configuration' and the subtitle is 'Customizes the behaviour of the device LEDs if possible.' The interface includes a navigation bar with 'M2M-Router' and menu items: Status, System, Router, Services, Network, and Logout. The main form contains the following fields and controls:

- Name:** Input field with the value 'wan'.
- LED Name:** Dropdown menu with the value 'led2g'.
- Default state:** A checkbox that is currently unchecked.
- Trigger:** Dropdown menu with the value 'Network device activity (netdev)'.
- Device:** Dropdown menu with the value '4g-wan'.
- Trigger Mode:** Three checkboxes: 'Link On' (checked), 'Transmit' (checked), and 'Receive' (checked).

At the bottom right of the form, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red). A 'Delete' button (red) is located at the top right of the form area. An 'Add' button (green) is located at the bottom left of the form area.

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* means the network interface connection type, and **Device** identifies the related network interface.

You can  a new one, or  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).

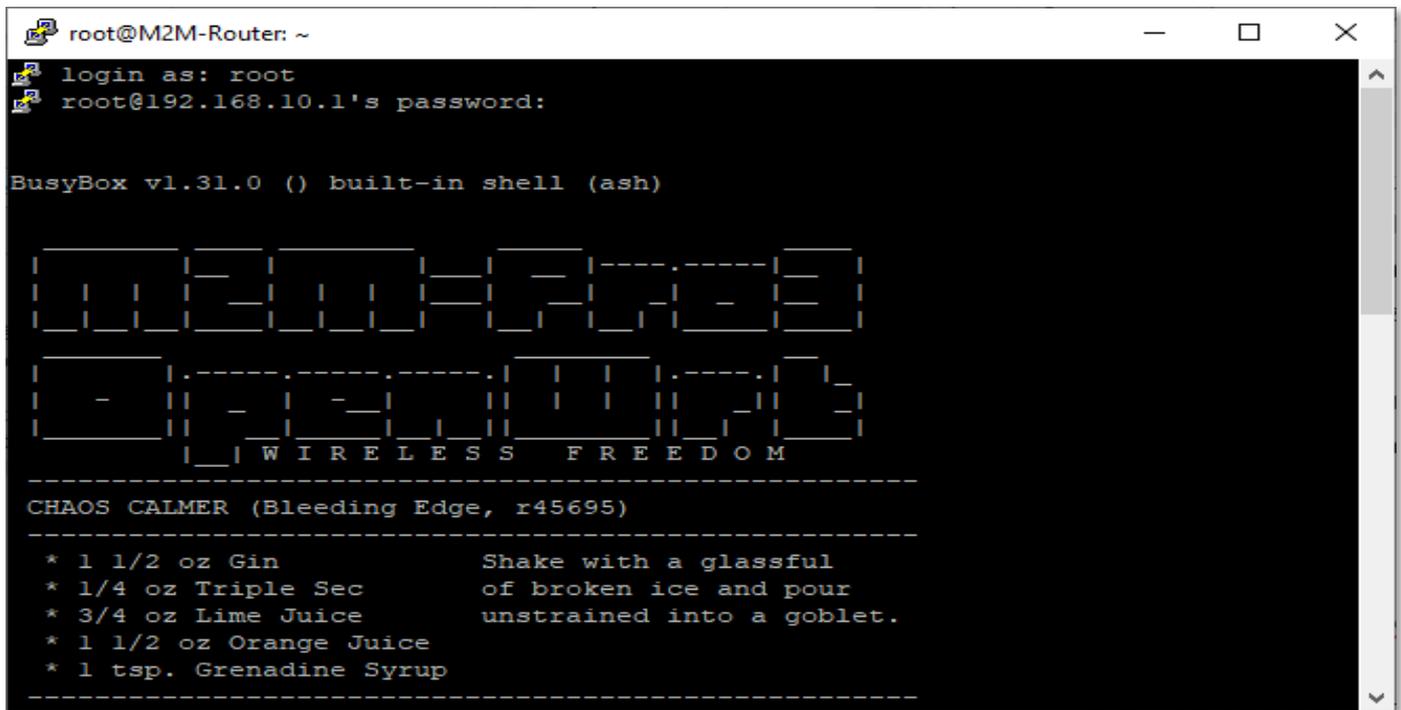
The same is possible at **192.168.10.1:22** - for the **USBLAN** port.

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**



```
root@M2M-Router: ~
login as: root
root@192.168.10.1's password:

BusyBox v1.31.0 () built-in shell (ash)

-----
|_| W I R E L E S S   F R E E D O M
-----

CHAOS CALMER (Bleeding Edge, r45695)
-----
* 1 1/2 oz Gin           Shake with a glassful
* 1/4 oz Triple Sec     of broken ice and pour
* 3/4 oz Lime Juice     unstrained into a goblet.
* 1 1/2 oz Orange Juice
* 1 tsp. Grenadine Syrup
-----
```

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](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.

M2M-Router						Status ▾	System ▾	Router ▾	Services ▾	Network ▾	Logout
18	gpio	Enabled	Start	Restart	Stop						
19	dnsmasq	Enabled	Start	Restart	Stop						
19	dropbear	Enabled	Start	Restart	Stop						
19	firewall	Enabled	Start	Restart	Stop						
20	network	Enabled	Start	Restart	Stop						
35	odhcpd	Enabled	Start	Restart	Stop						
45	modemd	Enabled	Start	Restart	Stop						
50	cron	Enabled	Start	Restart	Stop						
50	uhttpd	Enabled	Start	Restart	Stop						
75	ser2net	Disabled	Start	Restart	Stop						
80	ucitrack	Enabled	Start	Restart	Stop						
90	ipsec	Disabled	Start	Restart	Stop						
90	openvpn	Disabled	Start	Restart	Stop						
94	gpio_switch	Enabled	Start	Restart	Stop						

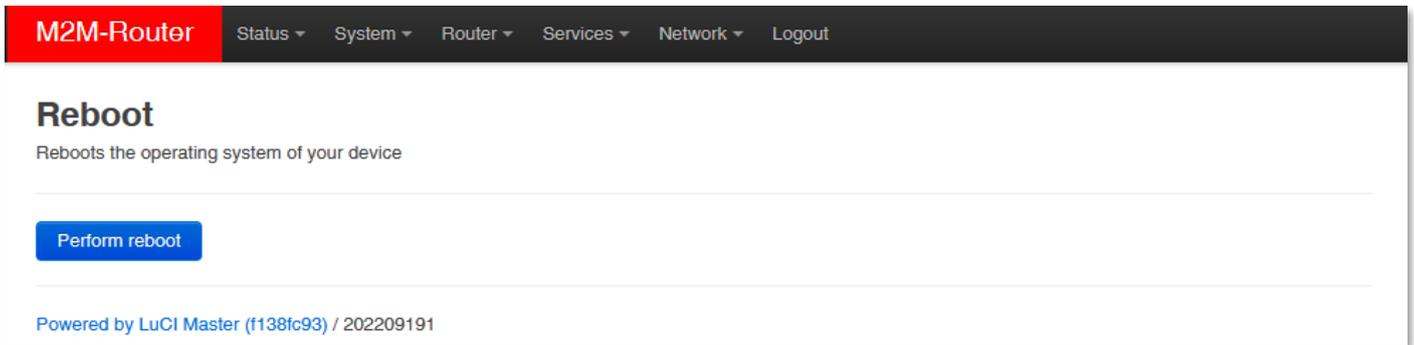
Roll down to the „**ipsec**” feature and push to the  button to initialize the service.

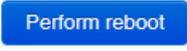
Then wait until the service list will be refreshed and the IPsec will be listed as an  service.

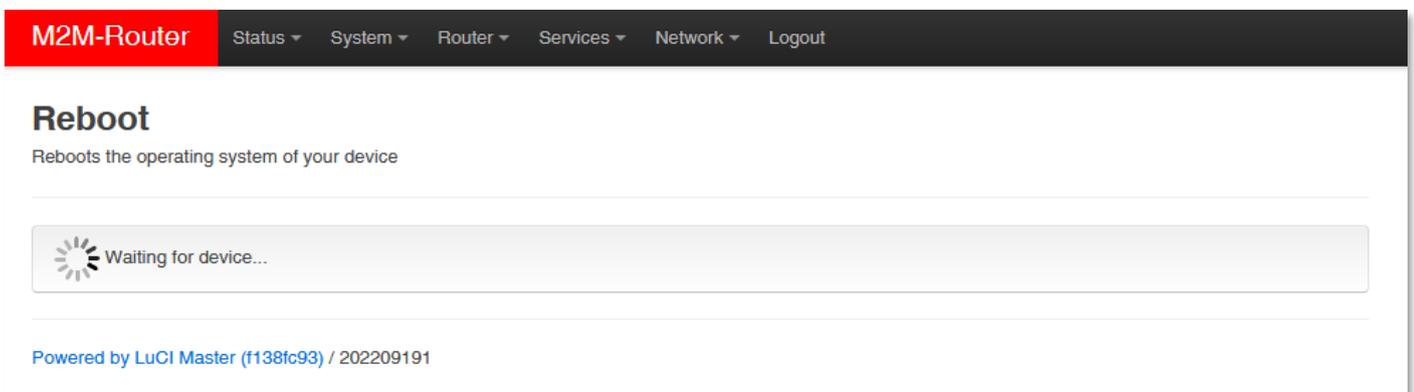
Then push to the  button of the line of the IPsec service to start the feature.

M2M-Router						Status ▾	System ▾	Router ▾	Services ▾	Network ▾	Logout
50	uhttpd	Enabled	Start	Restart	Stop						
75	ser2net	Disabled	Start	Restart	Stop						
80	ucitrack	Enabled	Start	Restart	Stop						
90	ipsec	Enabled	Start	Restart	Stop						
90	openvpn	Disabled	Start	Restart	Stop						

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



There push to the  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.

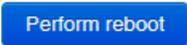
Roll down to the „**openvpn**” feature and push to the  button to initialize the service.

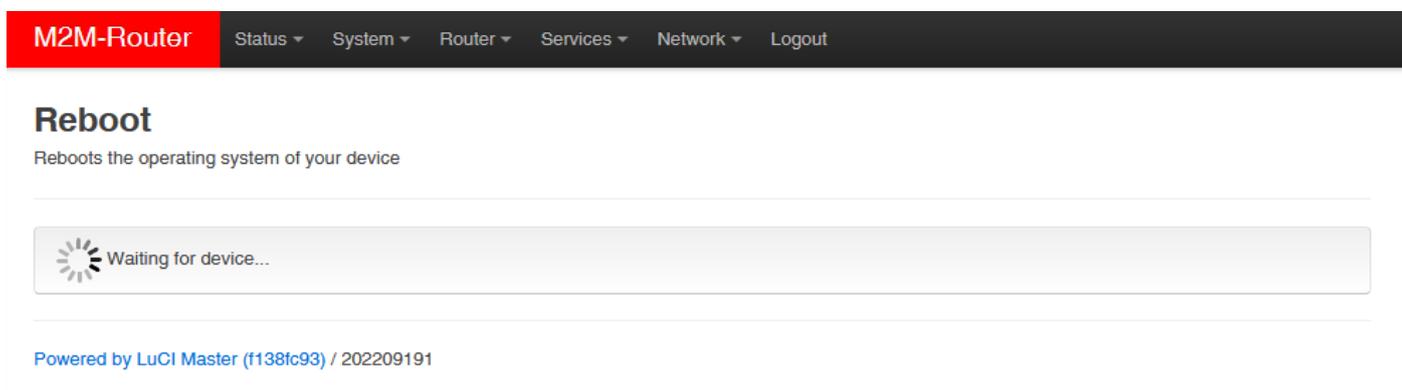
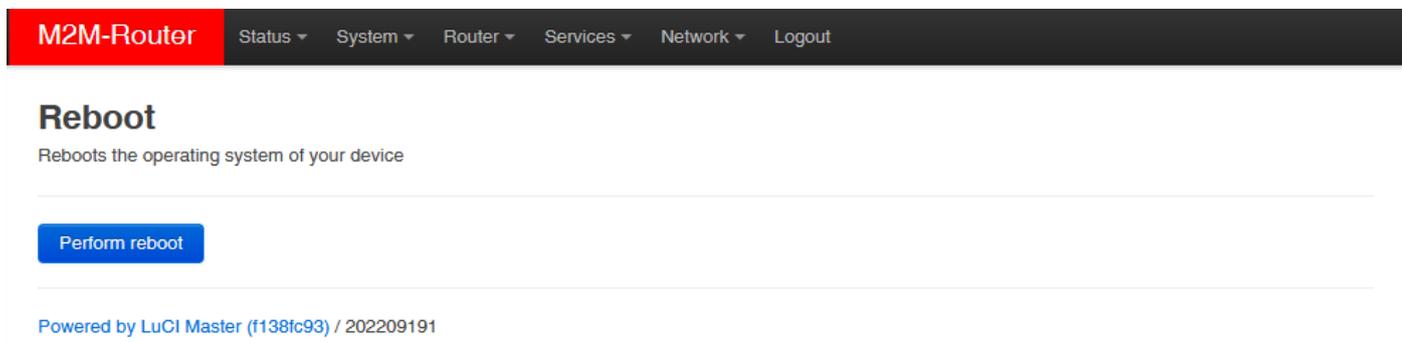
Then wait until the service list will be refreshed and the „**openvpn**” will be listed as an  service.

M2M-Router						Status ▾	System ▾	Router ▾	Services ▾	Network ▾	Logout
18	gpio	Enabled	Start	Restart	Stop						
19	dnsmasq	Enabled	Start	Restart	Stop						
19	dropbear	Enabled	Start	Restart	Stop						
19	firewall	Enabled	Start	Restart	Stop						
20	network	Enabled	Start	Restart	Stop						
35	odhcpd	Enabled	Start	Restart	Stop						
45	modemd	Enabled	Start	Restart	Stop						
50	cron	Enabled	Start	Restart	Stop						
50	uhttpd	Enabled	Start	Restart	Stop						
75	ser2net	Disabled	Start	Restart	Stop						
80	ucitrack	Enabled	Start	Restart	Stop						
90	ipsec	Disabled	Start	Restart	Stop						
90	openvpn	Disabled	Start	Restart	Stop						
94	gpio_switch	Enabled	Start	Restart	Stop						

Then push to the  button of the line of the „**openvpn**” service to start the feature. Then restart the device from the **System / Reboot** menu.

M2M-Router						Status ▾	System ▾	Router ▾	Services ▾	Network ▾	Logout
80	ucitrack	Enabled	Start	Restart	Stop						
90	ipsec	Enabled	Start	Restart	Stop						
90	openvpn	Enabled	Start	Restart	Stop						
94	gpio_switch	Enabled	Start	Restart	Stop						
95	ddns	Enabled	Start	Restart	Stop						

There push to the  button.

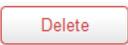


After the restart, you have to log in again and configure the „**openvpn**” service.

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  button to start that VPN rule.

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

**M2M-Router** Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout UNSAVED CHANGES: 1

## OpenVPN

### OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

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

### Template based configuration

Instance name  Select template ... ▾

### OVPN configuration file upload

Instance name   No file selected.

So, choose any profile from the ones listed - e.g. the **sample\_client** profile - that is, the VPN client, then press the  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  button.

**M2M-Pro4** Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Users ▾ Statistics ▾ Logout UNSAVED CHANGES: 17

**Overview » Instance "sample\_client"**  
[Switch to advanced configuration »](#)

verb  ▾  
[? Set output verbosity](#)

tun\_ipv6  [? Make tun device IPv6 capable](#)

nobind  [? Do not bind to local address and port](#)

proto  ▾  
[? Use protocol](#)

client  [? Configure client mode](#)

client\_to\_client  [? Allow client-to-client traffic](#)

remote  [+](#)  
[? Remote host name or ip address](#)

▾

Then return to the **OpenVPN** menu, where you can enable the given setting with the **Enable** option, then press the  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 tunnelling service description of the *OpenWrt*<sup>®</sup> administration interface which you are currently using:

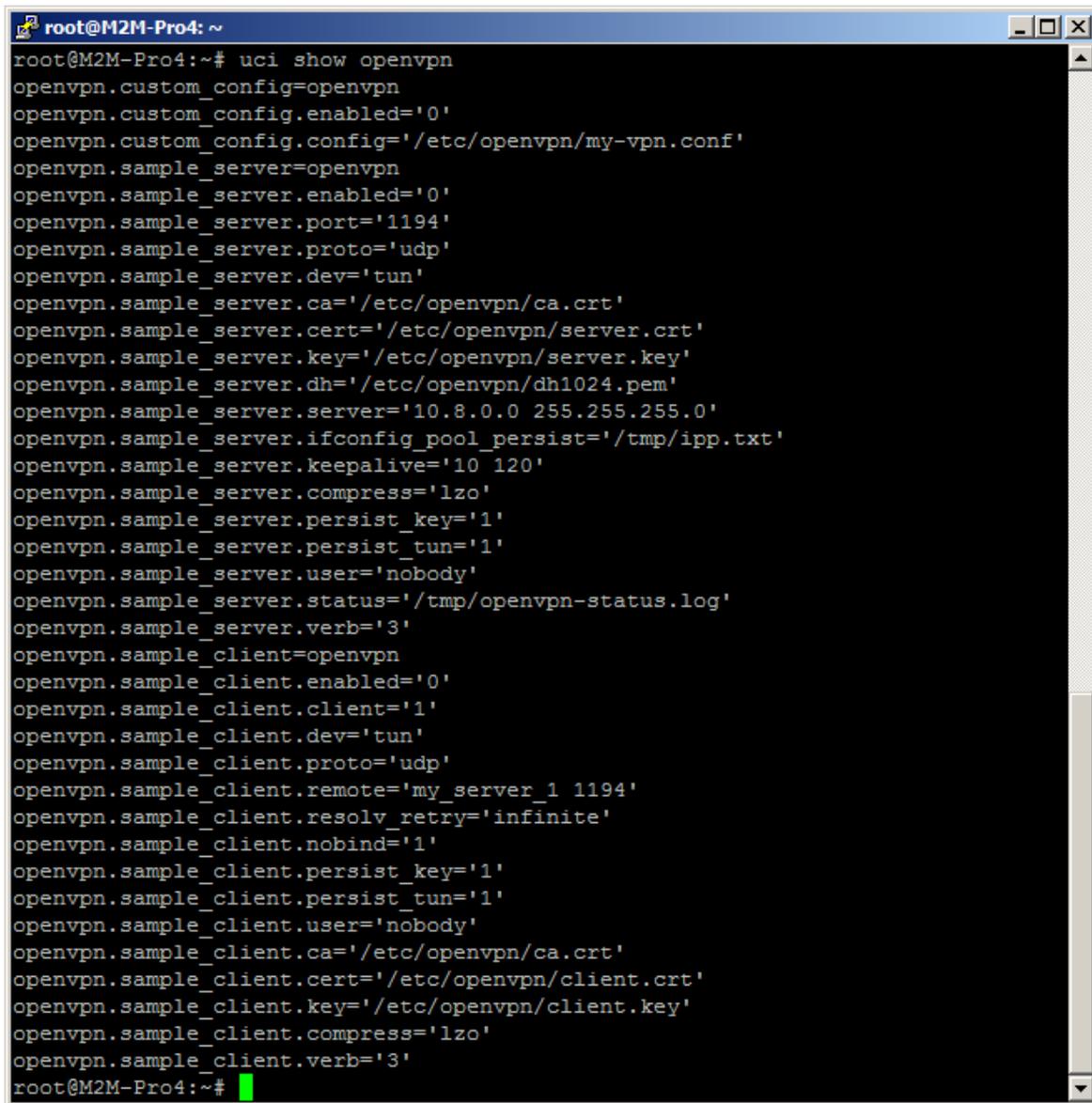
[https://wiki.openwrt.org/doc/howto/vpn.openvpn#tab\\_traditional\\_tun\\_server1](https://wiki.openwrt.org/doc/howto/vpn.openvpn#tab_traditional_tun_server1)

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:

A terminal window titled 'root@M2M-Pro4: ~' showing the output of the command 'uci show openvpn'. The output lists various configuration parameters for the OpenVPN service, including custom config, sample server and client settings, certificates, and network options.

```
root@M2M-Pro4:~# uci show openvpn
openvpn.custom_config=openvpn
openvpn.custom_config.enabled='0'
openvpn.custom_config.config='/etc/openvpn/my-vpn.conf'
openvpn.sample_server=openvpn
openvpn.sample_server.enabled='0'
openvpn.sample_server.port='1194'
openvpn.sample_server.proto='udp'
openvpn.sample_server.dev='tun'
openvpn.sample_server.ca='/etc/openvpn/ca.crt'
openvpn.sample_server.cert='/etc/openvpn/server.crt'
openvpn.sample_server.key='/etc/openvpn/server.key'
openvpn.sample_server.dh='/etc/openvpn/dh1024.pem'
openvpn.sample_server.server='10.8.0.0 255.255.255.0'
openvpn.sample_server.ifconfig_pool_persist='/tmp/ipp.txt'
openvpn.sample_server.keepalive='10 120'
openvpn.sample_server.compress='lzo'
openvpn.sample_server.persist_key='1'
openvpn.sample_server.persist_tun='1'
openvpn.sample_server.user='nobody'
openvpn.sample_server.status='/tmp/openvpn-status.log'
openvpn.sample_server.verb='3'
openvpn.sample_client=openvpn
openvpn.sample_client.enabled='0'
openvpn.sample_client.client='1'
openvpn.sample_client.dev='tun'
openvpn.sample_client.proto='udp'
openvpn.sample_client.remote='my_server_1 1194'
openvpn.sample_client.resolv_retry='infinite'
openvpn.sample_client.nobind='1'
openvpn.sample_client.persist_key='1'
openvpn.sample_client.persist_tun='1'
openvpn.sample_client.user='nobody'
openvpn.sample_client.ca='/etc/openvpn/ca.crt'
openvpn.sample_client.cert='/etc/openvpn/client.crt'
openvpn.sample_client.key='/etc/openvpn/client.key'
openvpn.sample_client.compress='lzo'
openvpn.sample_client.verb='3'
root@M2M-Pro4:~#
```

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.

**M2M-Router** Status System Router Services Network Logout **UNSAVED CHANGES: 3**

## Periodic Reboot

Setting restart time.

Hour

Minute

Powered by LuCI Master (git-15.137.54403-f67d39e) / OpenWrt Designated Driver r49022

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.

**M2M-Router** Status System Router Services Network Logout **UNSAVED CHANGES: 3**

## Periodic Ping

Test connection and restart modem if needed.

Ping IP Address

Ping failure threshold   
 When the device exceeds the restricted number of ping failures, it will be restarted.

Ping interval   
 Send ping requests at the given interval in seconds, only effective in conjunction with failure threshold

Powered by LuCI Master (git-15.137.54403-f67d39e) / OpenWrt Designated Driver r49022

## 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.

M2M-Router Status System Router Services Network Logout UNSAVED CHANGES: 1

### Voice Call Config

#### Phone Book

Phone number +36301234567

Command Reboot

Add

Delete

Save & Apply Save Reset

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

Press the  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  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).

**M2M-Router** Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout

## SMS Config

### Phone Book

Enabled	Phone number	
<input type="checkbox"/>	<input type="text" value="+36331234564"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	<input type="text" value="+36331234561"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	<input type="text" value="+36331234562"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	<input type="text" value="+36331234563"/>	<input type="button" value="Delete"/>

### SMS Commands

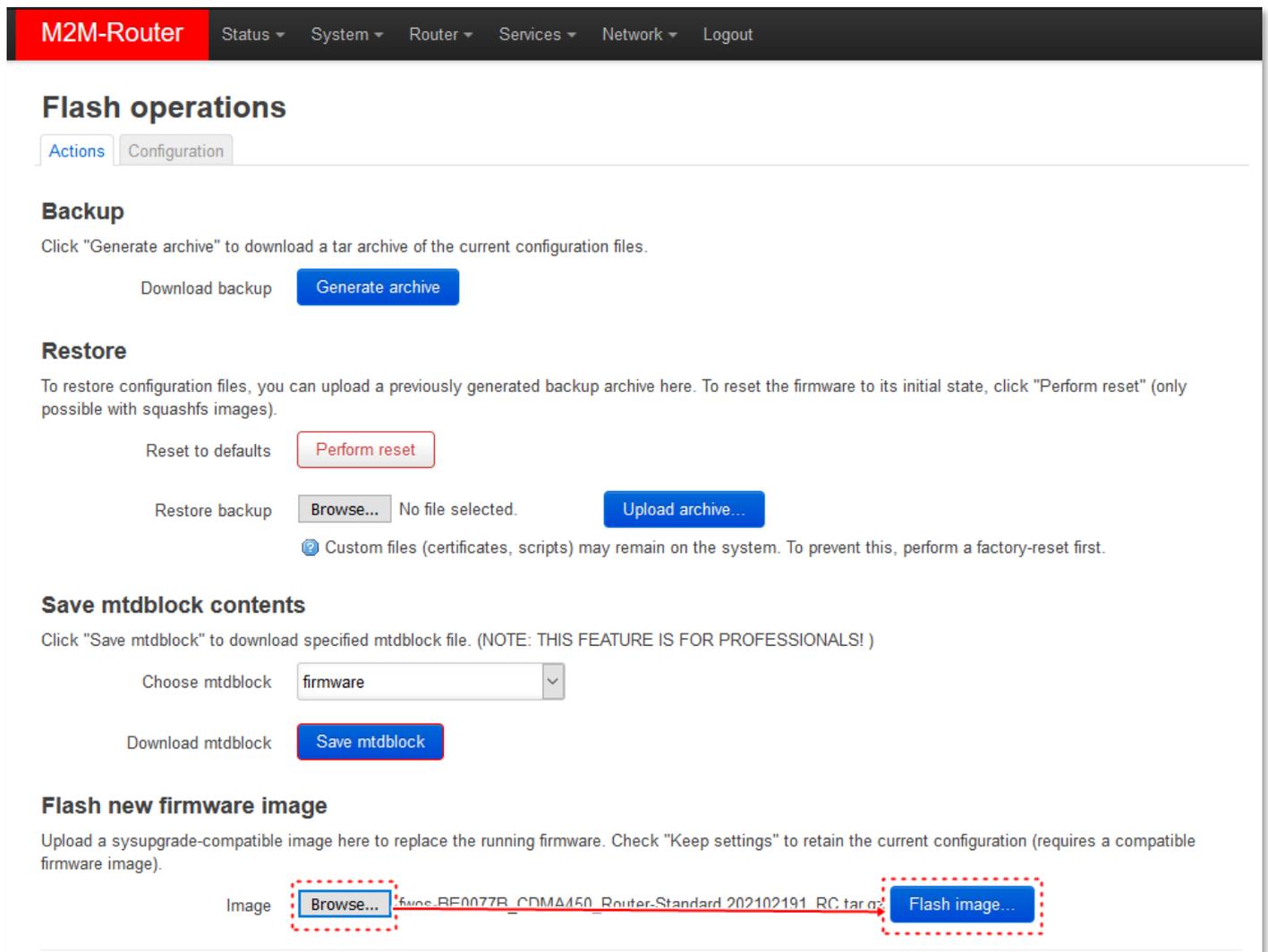
Enabled	Name	Description
<input checked="" type="checkbox"/>	reboot	Reboot router.
<input checked="" type="checkbox"/>	info	Router info: <firmware version> <uptime>
<input checked="" type="checkbox"/>	waninfo	WAN info: <up?> <proto> <uptime> <IPv4> <apn> <wnw>
<input checked="" type="checkbox"/>	modemrssi	Modem info: <stat> <AcT> <NetNameAsc> <rssi> <ber>
<input checked="" type="checkbox"/>	modeminfo	Modem info: <CGSN> <CGMR> <IMSI> <ICCID> <stat> <AcT> <NetNameAsc> <rssi> <ber>
<input checked="" type="checkbox"/>	setapn	Set apn: setapn=<apn>
<input checked="" type="checkbox"/>	setwnw	Set wnw: setwnw=<wnw>

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

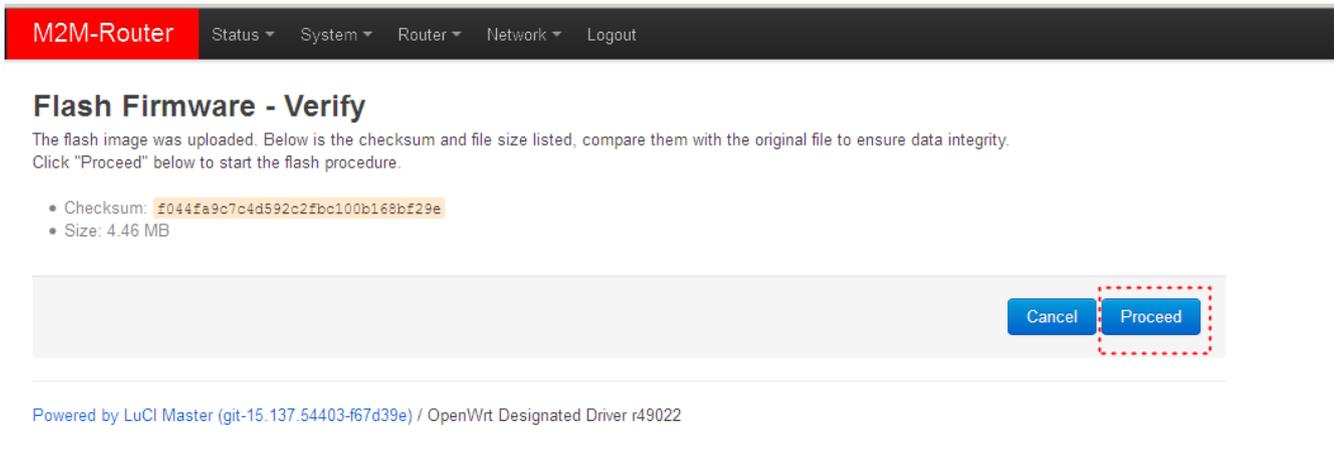
# Chapter 6. Software refresh and router maintenance

## 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 another 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.

### System - Flashing...

The system is flashing now.

DO NOT POWER OFF THE DEVICE!

Wait a few minutes before you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.



Waiting for changes to be applied...

6. At the end of the installation - the LEDs will no longer flash - the system will reboot 2x, then the *OpenWrt*<sup>®</sup> 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  button and setup the software distribution configuration in the popup windows, where you have to define the path of the installation packages are stored.

### OPKG Configuration

Below is a listing of the various configuration files used by *opkg*. Use *opkg.conf* for global settings and *customfeeds.conf* for custom repository entries. The configuration in the other files may be changed but is usually not preserved by *sysupgrade*.

**opkg.conf**

```
dest root /
dest ram /tmp
lists_dir ext /var/opkg-lists
option overlay_root /overlay
# option check_signature 1
```

**opkg/customfeeds.conf**

```
# add your custom package feeds here
#
# src/gz example_feed_name http://www.example.com/path/to/files
# Old feeds from previous image
# Uncomment to reenale
#
# src/gz local file:///install/packages
```

**opkg/distfeeds.conf**

```
src/gz local file:///install/packages
```

Then  the settings by the button. Afterall, push to the  button to refeed the available software catalog - from the software repository.

**M2M-Router** Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout

## Software

Free space:  90% (655.4 KB)

Filter:   Download and install package:   Actions:

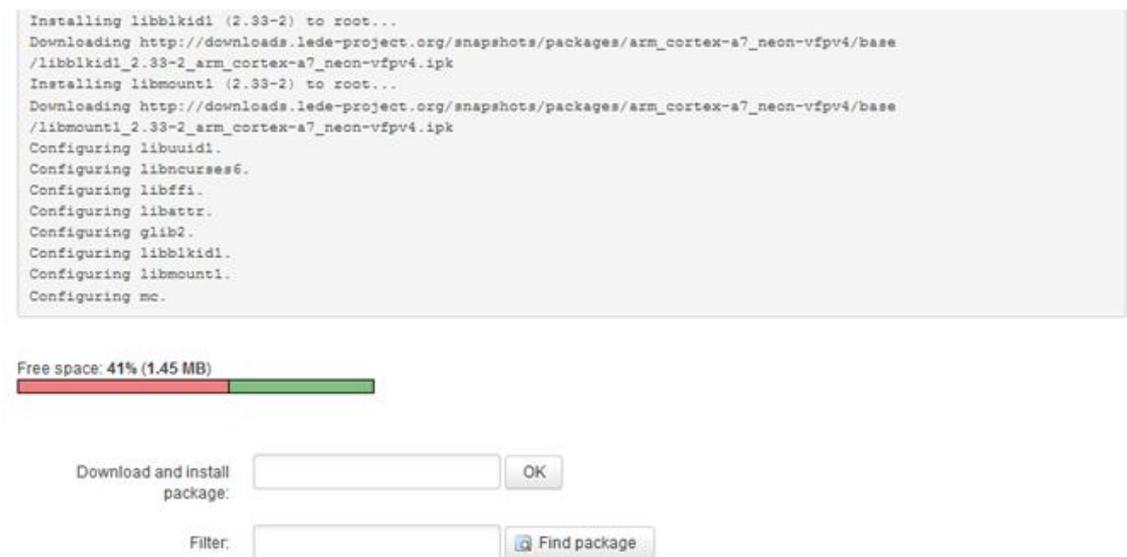
No packages

Package name	Version	Size (.ipk)	Description
No information available			

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

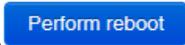
**When it has been successful**, then add the name of the application you are attempted to install at the **Download and install package** field (e.g. „MC” in case of *Midnight Commander*), and push to the **OK** button for the installation – regarding the upcoming hints on the screen.

The installed software packages are listed under **Status** with their **Version** information.

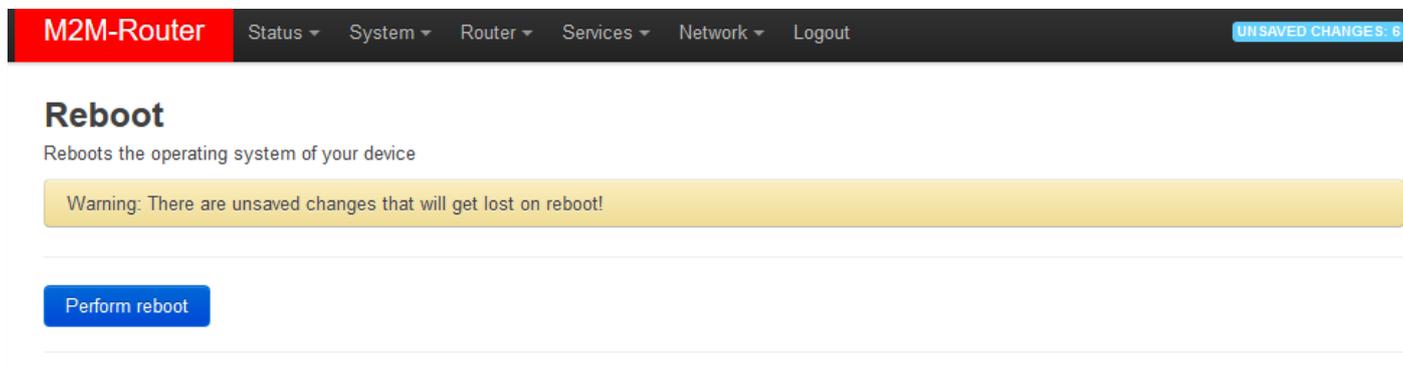


You can now configure and use the installed Linux program. You can configure or run it from the command line using the SSH terminal window. (Staying with our example: type "mc" at the Linux command prompt to run the program.)

### 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.

The screenshot shows the M2M-Router web interface. At the top, there is a navigation bar with the title 'M2M-Router' and several menu items: Status, System, Router, Services, Network, and Logout. A notification in the top right corner indicates 'UNSAVED CHANGES: 6'. Below the navigation bar, there are three tabs: 'Router Password' (which is active), 'SSH Access', and 'SSH-Keys'. The main content area is titled 'Router Password' and includes the subtitle 'Changes the administrator password for accessing the device'. There are two input fields: 'Password' and 'Confirmation', both of which have asterisks (\*) next to them, indicating that the entered characters are masked. A blue 'Save' button is located at the bottom right of the form area.

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.

**M2M-Router** Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout

## Flash operations

Actions Configuration

### Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup

### Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults

Restore backup  No file selected.

 Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

### **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.

**M2M-Router** Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout

## Backup file list

Actions Configuration

This is a list of shell glob patterns for matching files and directories to include during sysupgrade. Modified files in `/etc/config/` and certain other configurations are automatically preserved.

Show current backup file list [Open list...](#)

```
## This file contains files and directories that should
## be preserved during an upgrade.

# /etc/example.conf
# /etc/openvpn/
```

[Submit](#) [Reset](#)

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 [Browse...](#) button to **browse** the previously saved file from your computer, then press the [Upload archive...](#) 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.*

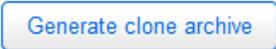
## To reset the router configuration:

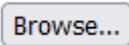
You can do it here in the OpenWrt interface, by also pressing the  button in the web interface menu item.

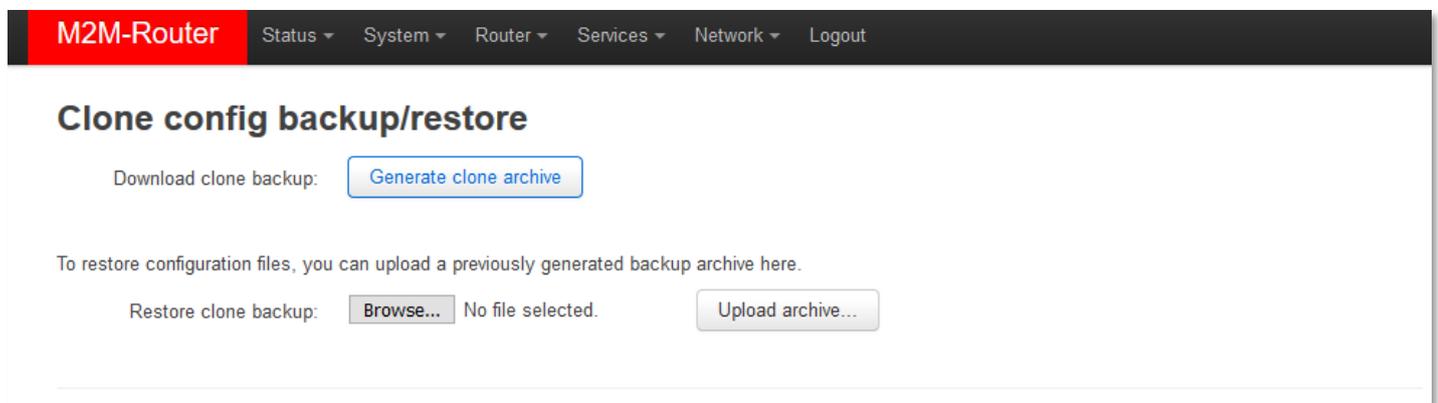
Or you can use the **Reset** button on the router to reset the router to factory defaults - see. router reset chapter.

## 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  button.

In the popup window, click to  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  button after browsing.

## 6.9 Start or stop a system service

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

M2M-Router					
<a href="#">Status</a> ▾ <a href="#">System</a> ▾ <a href="#">Router</a> ▾ <a href="#">Services</a> ▾ <a href="#">Network</a> ▾ <a href="#">Logout</a>					
18	gpio	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
19	dnsmasq	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
19	dropbear	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
19	firewall	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
20	network	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
35	odhcpd	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
45	modemd	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
50	cron	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
50	uhttpd	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
75	ser2net	<span>Disabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
80	ucitrack	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
90	ipsec	<span>Disabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
90	openvpn	<span>Disabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>
94	gpio_switch	<span>Enabled</span>	<a href="#">Start</a>	<a href="#">Restart</a>	<a href="#">Stop</a>

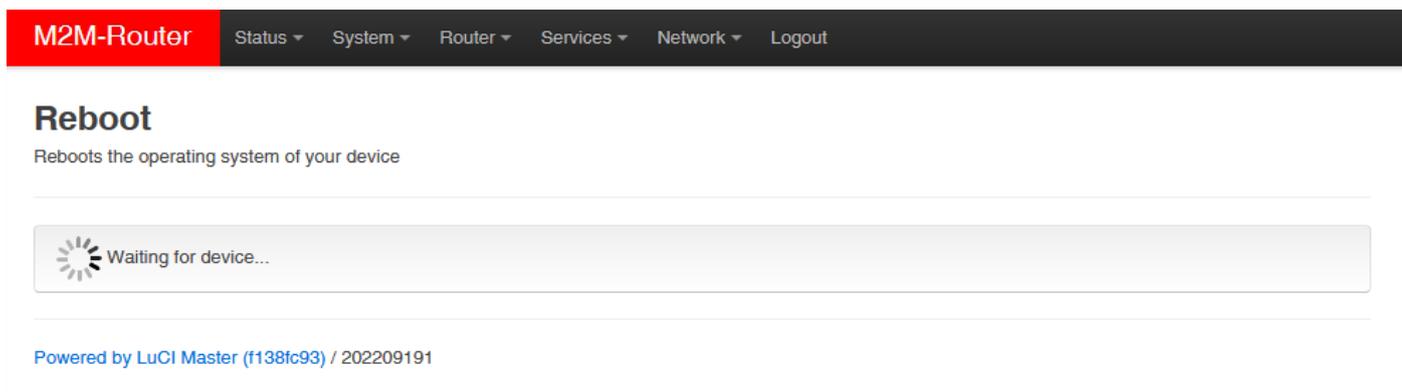
If the service has Enabled status, then you can start the service by pushing the [start](#) button to initialize the service. To stop the service, push to the [Stop](#) button.

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.

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

M2M-Router					
<a href="#">Status</a> ▾ <a href="#">System</a> ▾ <a href="#">Router</a> ▾ <a href="#">Services</a> ▾ <a href="#">Network</a> ▾ <a href="#">Logout</a>					
<h2>Reboot</h2> <p>Reboots the operating system of your device</p> <hr/> <p><a href="#">Perform reboot</a></p> <hr/> <p>Powered by LuCI Master (f138fc93) / 202209191</p>					

There push to the  button.

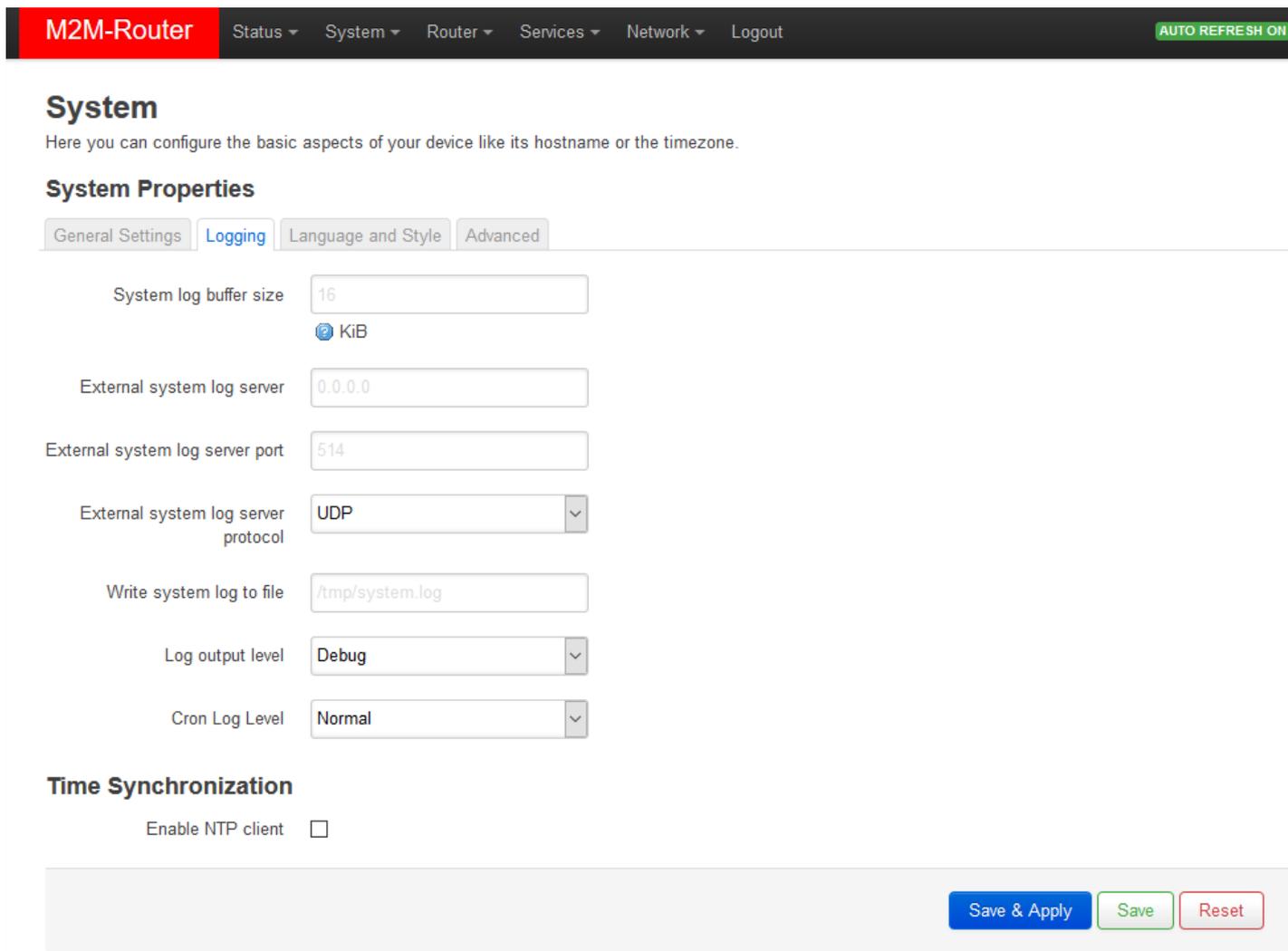


The screenshot shows the M2M-Router interface with a navigation bar at the top containing 'M2M-Router', 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. The main content area is titled 'Reboot' and includes the text 'Reboots the operating system of your device'. Below this is a large grey box with a loading spinner and the text 'Waiting for device...'. At the bottom, it says 'Powered by LuCI Master (f138fc93) / 202209191'.

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.



The screenshot shows the M2M-Router 'System' configuration page. The navigation bar includes 'M2M-Router', 'Status', 'System', 'Router', 'Services', 'Network', 'Logout', and an 'AUTO REFRESH ON' button. The main heading is 'System' with the subtitle 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Below this is the 'System Properties' section with tabs for 'General Settings', 'Logging', 'Language and Style', and 'Advanced'. The 'Logging' tab is active, showing several configuration fields: 'System log buffer size' (16 KiB), 'External system log server' (0.0.0.0), 'External system log server port' (514), 'External system log server protocol' (UDP), 'Write system log to file' (/tmp/system.log), 'Log output level' (Debug), and 'Cron Log Level' (Normal). At the bottom, there is a 'Time Synchronization' section with an 'Enable NTP client' checkbox. The footer contains three buttons: 'Save & Apply', 'Save', and 'Reset'.

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.

**M2M-Router** Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout

## System Log

```
Thu Oct 6 07:42:30 2022 daemon.debug pppd[6452]: sent [LCP ConfReq id=0x59 <auth chap MD5> <pcomp> <accomp>]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): rcvd [LCP ConfReq id=0x59 <asyncmap 0x0> <auth chap MD5> <magic 0x28074209> <pcomp> <accomp>]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0x2ad541d4>]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): No auth is possible
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): sent [LCP ConfReq id=0x59 <auth chap MD5> <pcomp> <accomp>]
Thu Oct 6 07:42:30 2022 daemon.debug pppd[6452]: rcvd [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0x2ad541d4>]
Thu Oct 6 07:42:30 2022 daemon.debug pppd[6452]: rcvd [LCP ConfReq id=0x5a <asyncmap 0x0> <magic 0x28074209>]
Thu Oct 6 07:42:30 2022 daemon.debug pppd[6452]: sent [LCP ConfAck id=0x5a <asyncmap 0x0> <magic 0x28074209>]
Thu Oct 6 07:42:30 2022 daemon.debug pppd[6452]: sent [LCP EchoReq id=0x0 magic=0x2ad541d4]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): rcvd [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0x2ad541d4>]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): rcvd [LCP ConfReq id=0x5a <asyncmap 0x0> <magic 0x28074209>]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): sent [LCP ConfAck id=0x5a <asyncmap 0x0> <magic 0x28074209>]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): sent [LCP EchoReq id=0x0 magic=0x2ad541d4]
Thu Oct 6 07:42:30 2022 daemon.debug pppd[6452]: sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns2 0.0.0.0>]
Thu Oct 6 07:42:30 2022 daemon.debug pppd[6452]: rcvd [LCP DiscReq id=0x5b magic=0x28074209]
Thu Oct 6 07:42:30 2022 daemon.debug pppd[6452]: rcvd [LCP EchoRep id=0x0 magic=0x28074209 2a d5 41 d4]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns2 0.0.0.0>]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): rcvd [LCP DiscReq id=0x5b magic=0x28074209]
Thu Oct 6 07:42:30 2022 daemon.notice netifd: wan (6452): rcvd [LCP EchoRep id=0x0 magic=0x28074209 2a d5 41 d4]
Thu Oct 6 07:42:31 2022 daemon.debug pppd[6452]: sent [LCP EchoReq id=0x1 magic=0x2ad541d4]
Thu Oct 6 07:42:31 2022 daemon.notice netifd: wan (6452): sent [LCP EchoReq id=0x1 magic=0x2ad541d4]
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: started, version 2.80 cachesize 150
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: DNS service limited to local subnets
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: compile time options: IPv6 GNU-getopt no-DBus no-i18n no-IDN DHCP no-DHCPv6 no-Lua TFTP no-contrack no-ipse
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: using local addresses only for domain test
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: using local addresses only for domain onion
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: using local addresses only for domain localhost
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: using local addresses only for domain local
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: using local addresses only for domain invalid
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: using local addresses only for domain bind
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: using local addresses only for domain lan
Thu Oct 6 07:42:31 2022 daemon.warn dnsmasq[6554]: no servers found in /tmp/resolv.conf.auto, will retry
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: read /etc/hosts - 6 addresses
Thu Oct 6 07:42:31 2022 daemon.info dnsmasq[6554]: read /tmp/hosts/dhcp.cfg01411c - 0 addresses
Thu Oct 6 07:42:31 2022 daemon.debug pppd[6452]: rcvd [IPCP ConfNak id=0x1 <ms-dns1 10.11.12.13> <ms-dns2 10.11.12.14> <ms-wins 10.11.12.13> <ms-wins 10.11.12.14>]
Thu Oct 6 07:42:31 2022 daemon.debug pppd[6452]: sent [IPCP ConfReq id=0x2 <addr 0.0.0.0> <ms-dns1 10.11.12.13> <ms-dns2 10.11.12.14> <ms-wins 10.11.12.13> <ms-wins 10.11.12.14>]
Thu Oct 6 07:42:31 2022 daemon.notice netifd: wan (6452): rcvd [IPCP ConfNak id=0x1 <ms-dns1 10.11.12.13> <ms-dns2 10.11.12.14> <ms-wins 10.11.12.13> <ms-wins 10.11.12.14>]
Thu Oct 6 07:42:31 2022 daemon.notice netifd: wan (6452): sent [IPCP ConfReq id=0x2 <addr 0.0.0.0> <ms-dns1 10.11.12.13> <ms-dns2 10.11.12.14> <ms-wins 10.11.12.13> <ms-wins 10.11.12.14>]
Thu Oct 6 07:42:31 2022 daemon.notice pppd[6452]: Modem hangup
Thu Oct 6 07:42:31 2022 daemon.notice pppd[6452]: Connection terminated.
Thu Oct 6 07:42:31 2022 daemon.notice netifd: wan (6452): Modem hangup
Thu Oct 6 07:42:31 2022 daemon.notice netifd: wan (6452): Connection terminated.
Thu Oct 6 07:42:32 2022 daemon.info pppd[6452]: Exit.
Thu Oct 6 07:42:33 2022 daemon.notice netifd: Interface 'wan' is now down
```

# 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.

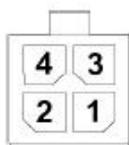
When it receives 12V DC power, the LED signals will sign it: *all the three LEDs will light for a short period*, then the **LED1 (green)** will lighting for 2 or 3 minutes, then after that only blinks once in every 10 seconds. The router is booting and just started.

(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](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 on the 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 be able to access the cellular network.

### If there is no SIM slot

In case of using CDMA 450 network in many countries there is no need of usage of SIM cards. The identification of the routers (their cellular modules) and the registration to the cellular network is executed 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 be 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, while you will get appropriate signal values at reception.

#### **Network**

Modem Model	ME910C1-E1
IMEI	356345080013401
SIM ID	89882390000052445353
Modem RSSI	99
Modem SQ	99
CREG	2,2
COPS	0
IPv4 WAN Status	 Not connected ?
IPv6 WAN Status	 Not connected ?

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 be able to access the network.

Note that for Narrow Band (NB-IoT) networks it could be needed to wait 5-15 minutes for the first successful 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](mailto: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

©2022. WM Systems LLC.

The content of this documentation (all information, pictures, tests, descriptions, guides, logos) is under copyright protection. Copying, using, distributing and publishing it is only permitted with the consent of WM Systems LLC., with clear indication of the source.

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.