M2M Router PRO4®

User Manual

OpenWrt® user interface settings

v1.72

2022-11-24

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

Document specifications

This document was made for the **M2M Router PRO4®** device and it contains the detailed description of OpenWrt® configuration possibilities for the proper operation of the device.

Document category:	User Manual
Document subject:	M2M Router PRO4®
Author:	WM Systems LLC
Document version No.:	REV 1.72
Number of pages:	87
Linux Kernel:	4.14.23
OpenWRT software version:	202111251
Document status:	FINAL
Last modified:	24 November, 2022
Approval date:	24 November, 2022

Table of contents

1. Device configuration (OpenWrt user interface)

1.1 Web user interface

Important!

The device's software contains a pre-configured system. Please check the configuration, and if the settings are not match with your expectations, change the configuration settings and save them.

1. The router's **local web user interface (LuCi®) is reachable through the Ethernet** or the **USB** interface – on their default addresses.

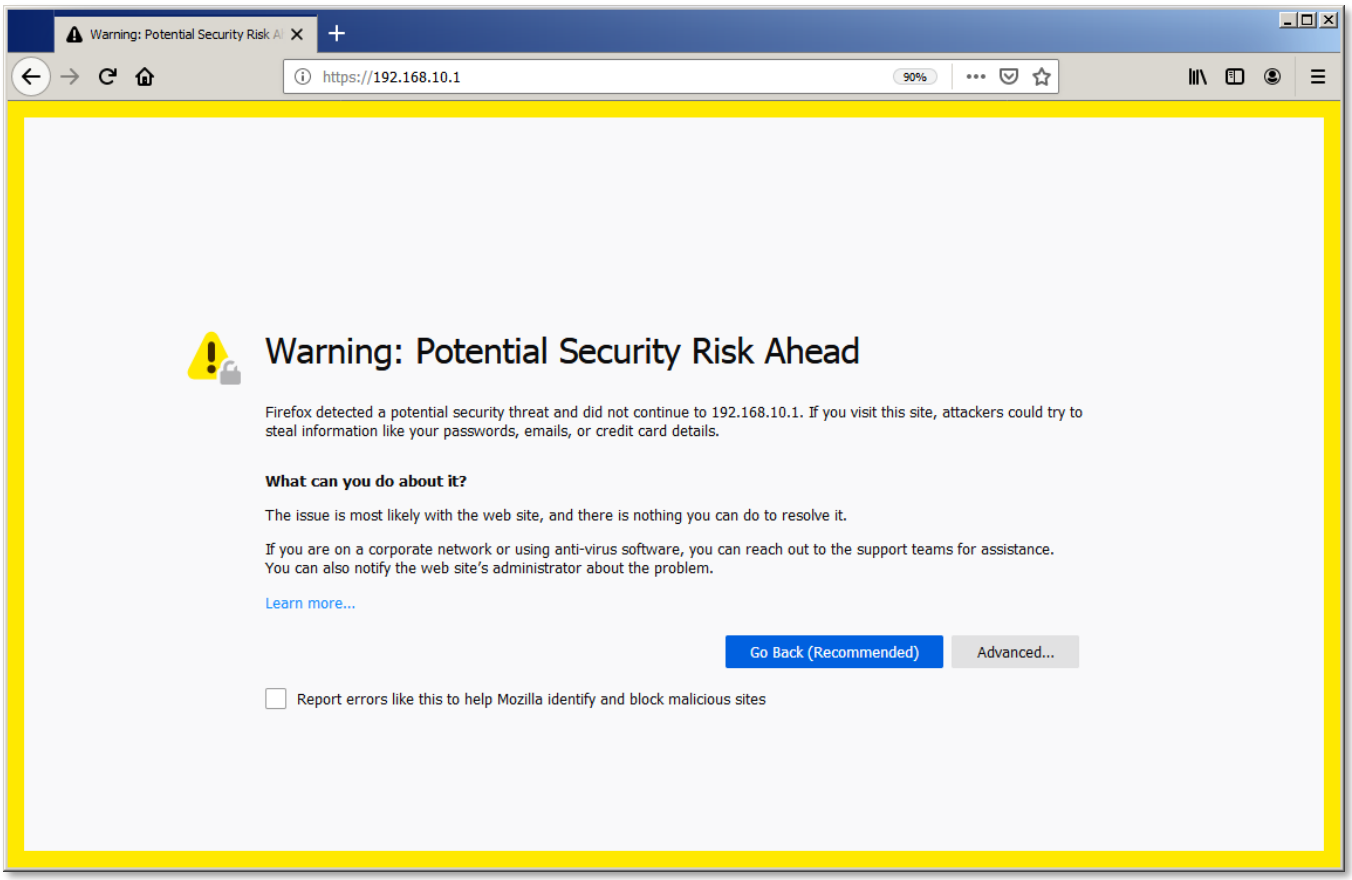
   For the usage you have to **install the „RNDIS Driver" to your computer**, according to the Installation manual Chapter 2.4.

2. Enter the default web user interface URL of the router.

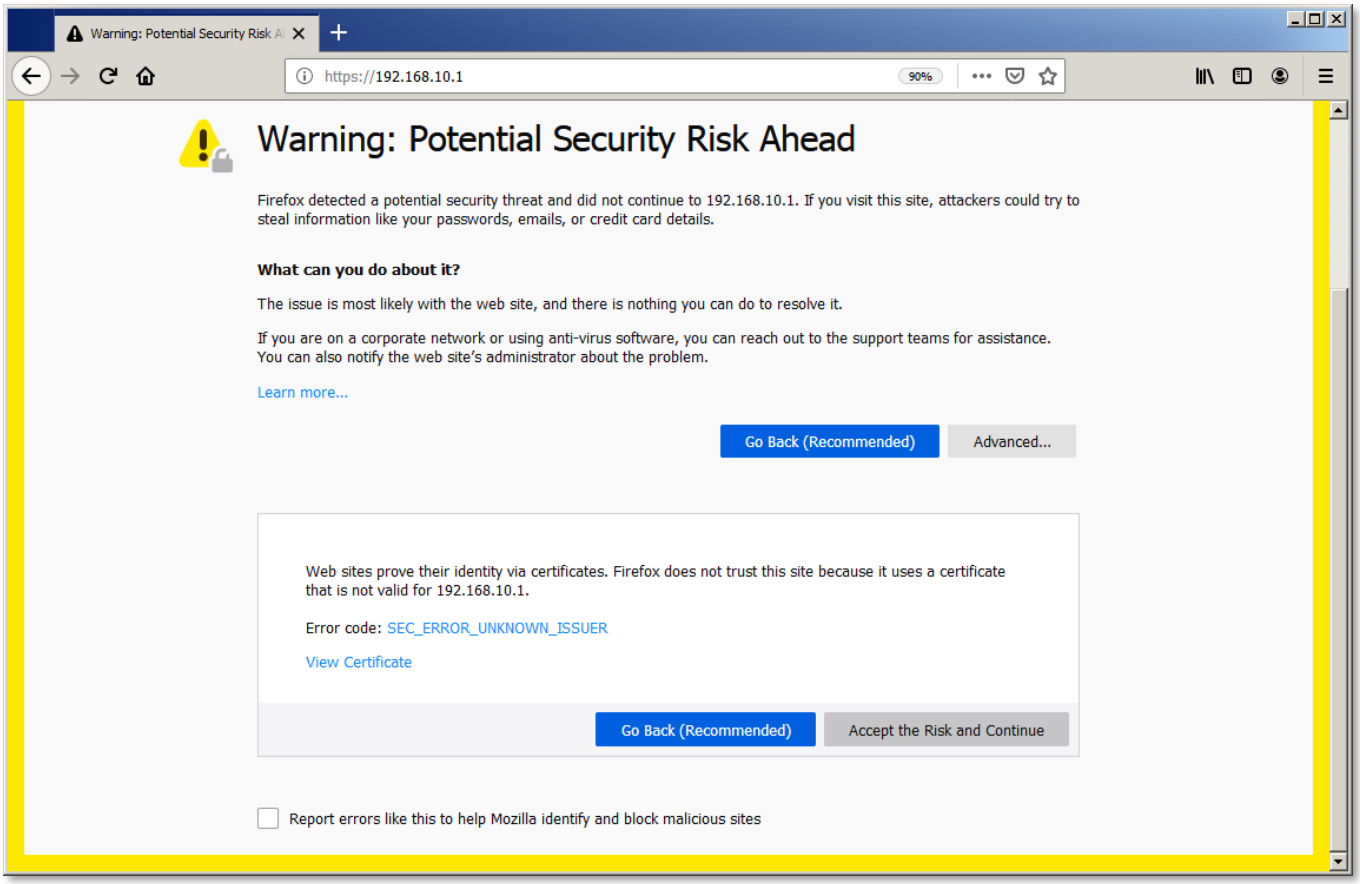
   The **Ethernet** interface default **URL** is: **https://192.168.1.1**

   The micro **USB** interface's default **URL** is: **https://192.168.10.1**

3. In the browser you will get a security risk message, its not important to take care, but choose the **Advanced** option.

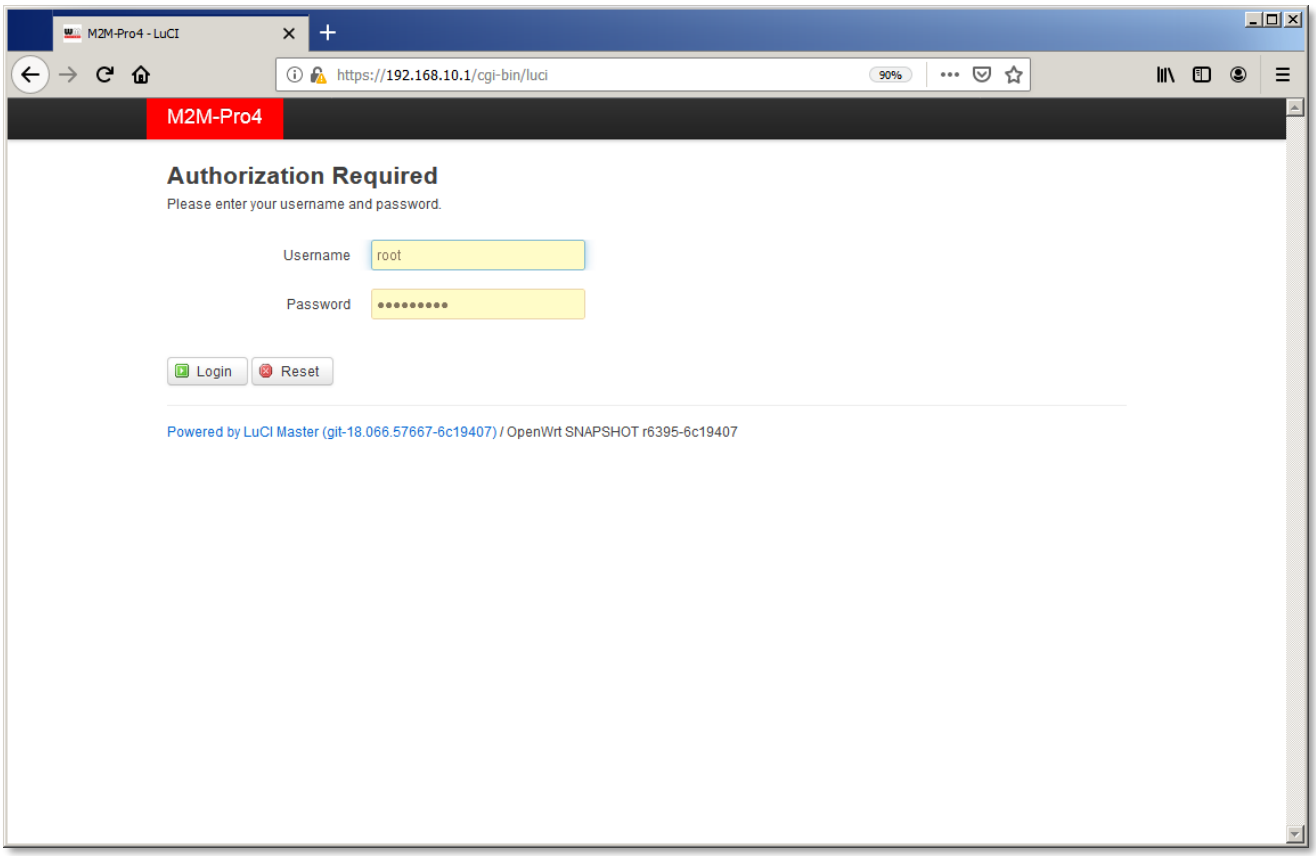


4. Then click on the **Accept the Risk and Continue** button to access the router's webpage.



5. The OpenWRT® system's LuCi® web interface has loaded into your browser. Now fill the **Username** and **Password** fields and click on the **Login** button for the entry.

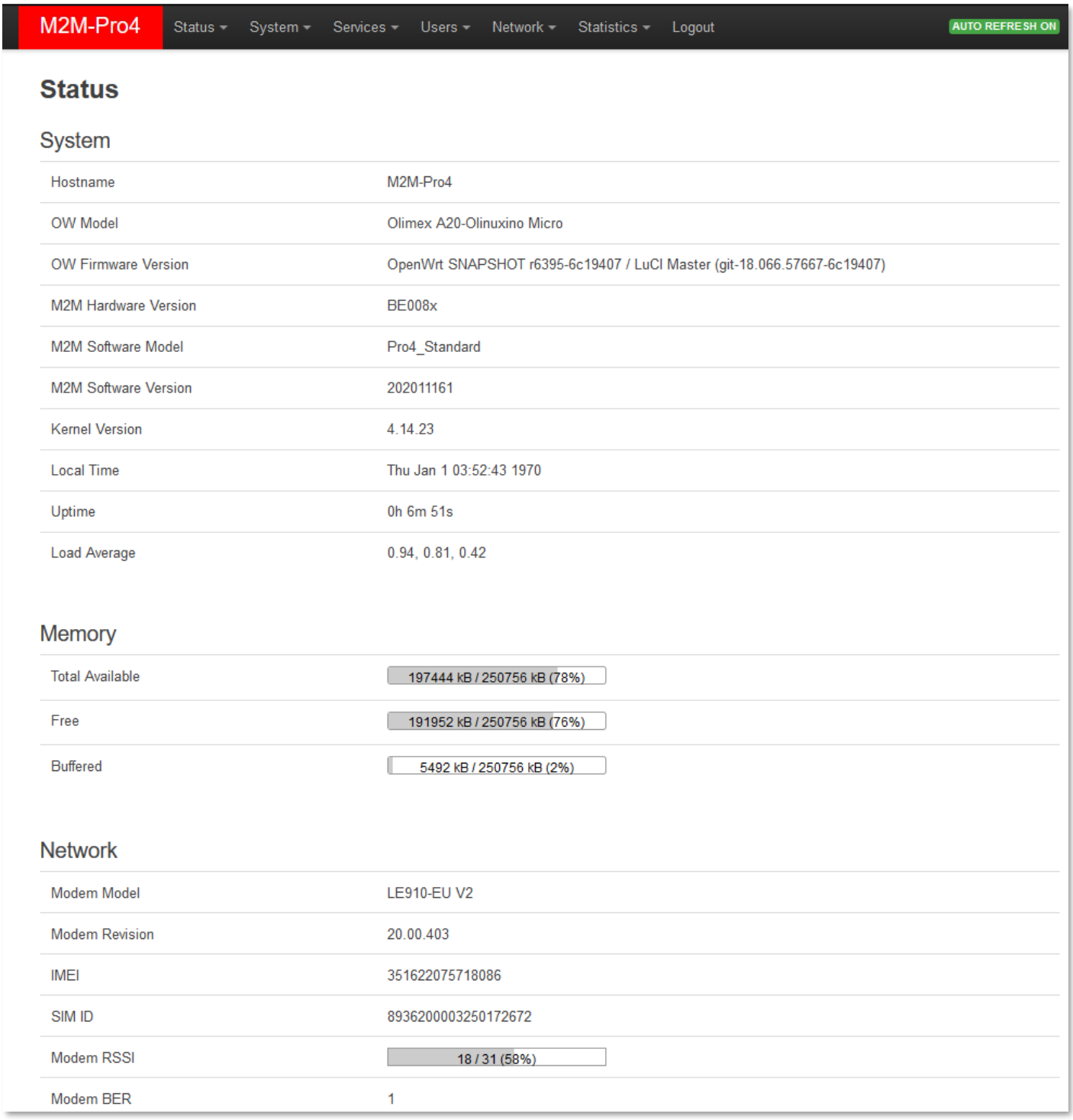
   Username: ***root*** **Password:** ***wmrpwdM2M***



1.2 Dashboard (Main page)

After you have logged in the web interface, a startup screen appears with all relevant information and the current status of the router.

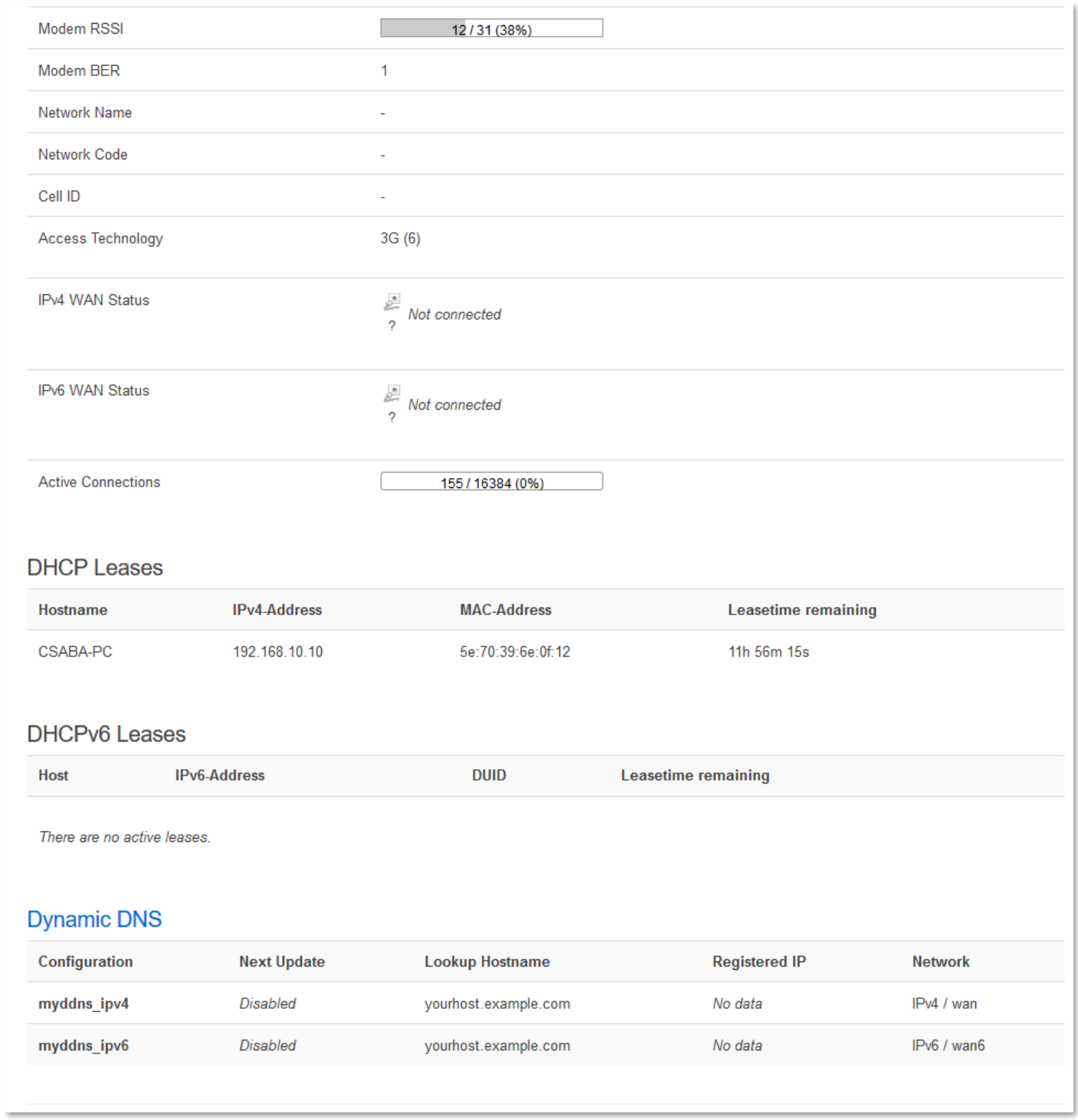
At the **System** part, you can check the installed software build (**M2M Software model** and **M2M Software version**) where it should be ***202111251*** or newer. (If it has an older version, then refresh the firmware, please.)



At the **Local Time** you can check the current time.

The **Uptime** shows the spent time interval since the last bootup (or reboot).

At the **Network** part, first you can check the wireless module availability at **IPv4 WAN Status** or **IPv6 WAN Status** part, as the module's **IMEI** identifier and the **SIM ID** identifier of the used SIM card.



The wireless network access' current status and health, properties can be checked at **Modem RSSI** (cellular network signal strength), **Network Name**, **Network Code** and **Cell ID** is getting from the mobile operator.

The module's wireless network address can be seen at **IPv4 WAN** or IPv6 status. The **Access technology** shows the current wireless network connection type as *2G*, *3G*, *4G LTE* or NB-IoT.

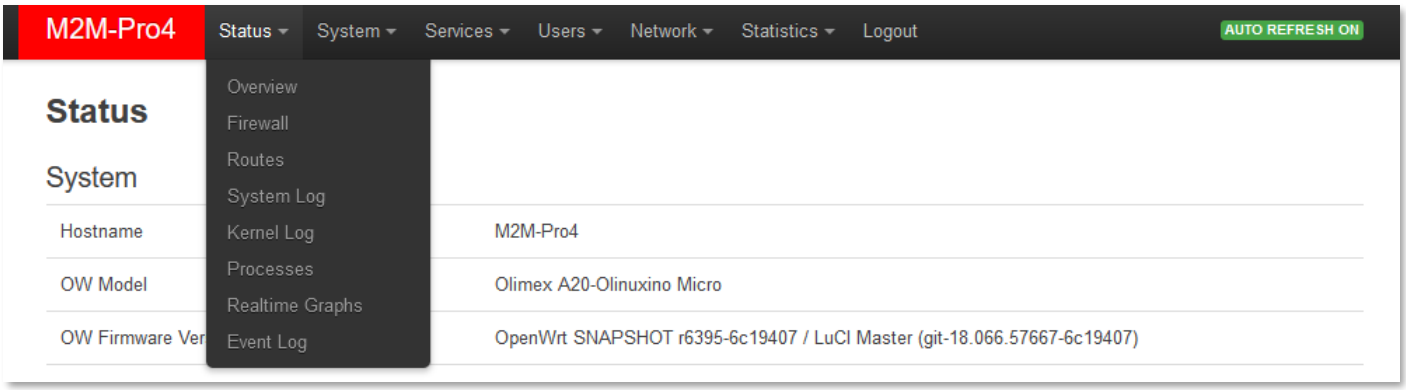
1.3 Menu overview

By the menu you can access the following features:

- **Status** – Status data, operation Logs (system, kernel, event log), monitoring the operation (at Processes and Realtime graphs)
- **System** – System settings and administration, software installation (3rd party tools), Device Manager settings, startup settings, Scheduled tasks, Mount points (uSD card storage and Flash file system content), LED configuration, Firmware flashing, Backup/Restore of the configuration settings, Custom commands, Reboot of the system)
- **Services** – Dynamic DNS, Mbus (available by order only) and OpenVPN settings
- **Users** – Add or delete users, Clone config, Ping an IP address, daily restart
- **Network** – Network interface settings (Ethernet/USB LAN/Wireless module/USB Phone connection), SIM PIN change, DHCP and DNS settings, Hostname, Static routes, Bandwith Diagnostics, Diagnostics, Firewall settings, Serial proxy (RS485) settings, IPSEC, SMS configuration (remote command execute), Voice Call configuration)
- **Statistics** – system graphs and statistics settings
- **Logout** – logout and login with a different user

1.4 Status menu

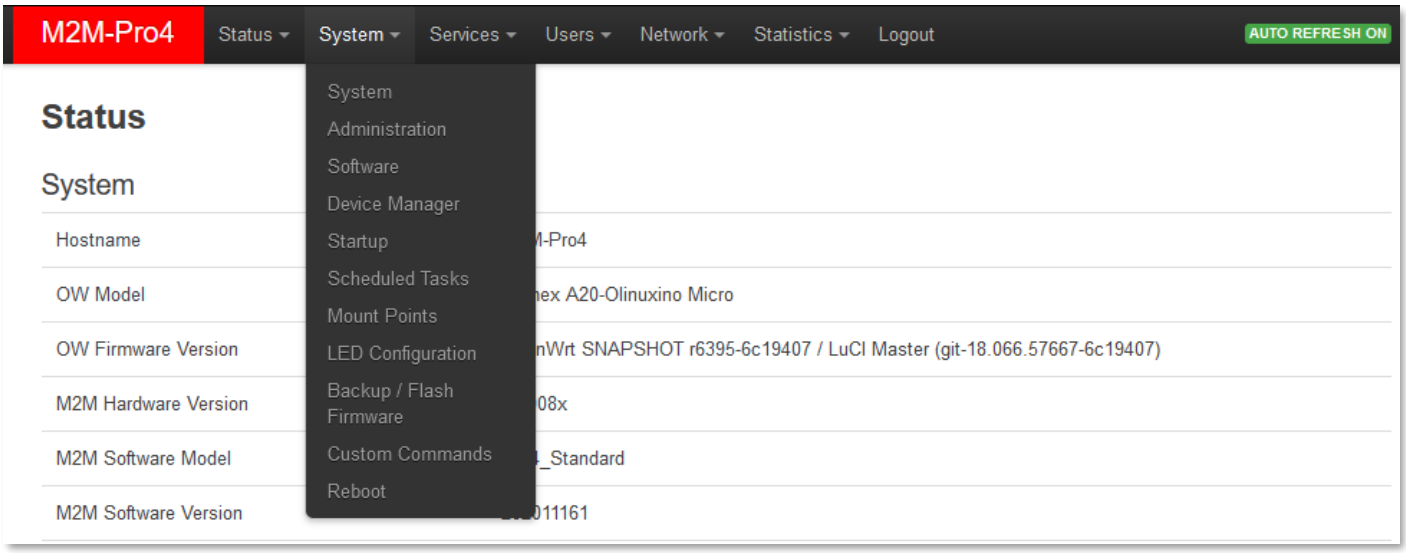
- In the **Status** you can check the current status (**Overview**).
- At the **Firewall** item, you can see the firewall events and information.



- At the **Routes** item the valid/active static route settings.
- Check system messages and event log (**System Log**, **Kernel Log**).
- Check the activities of the router (**Processes**).
- You can find monitoring features of the realtime operation at the **Realtime Graphs.**
- You also can check or download the **Event Log** here.

1.5 System menu

- You will found several system settings in the **System** and **the Administration** menu items.
- Installation of further **Software** (3rd party tools, applications for the Linux distribution).
- **Device Manager** (remote management server settings)
- You can define the **Startup** applicatons
- Initialization of programs can be configured during the operation and the **Scheduled Tasks.**

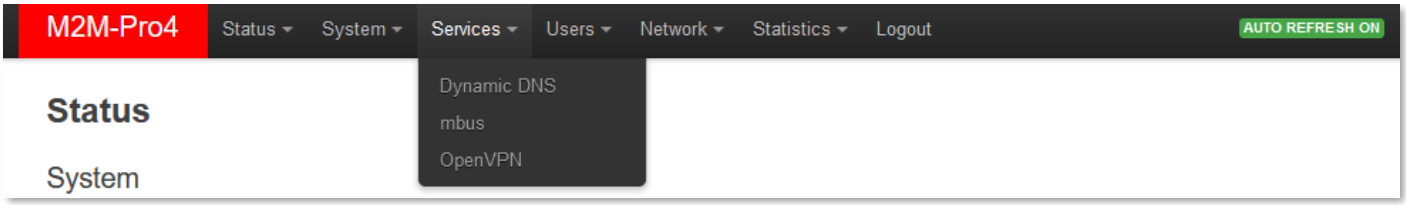


- The **Mount Points** are showing the available (mounted) shares and drives of the uSD card or connected USB driver and the Linux file system (flash).
- The **LED Configuration** is also configurable for custom needs.
- You also can **Backup** and restore your system configuration, applying **Flash firmware** updates
- **Custom Commands** for defining some connads to execute.
- **Reboot** menu: restarting the device.

1.6 Services menu

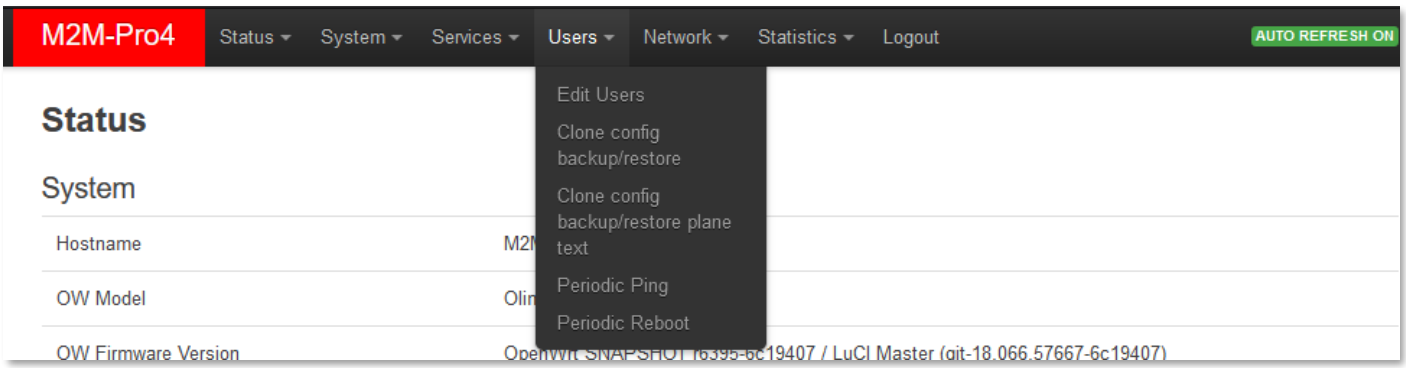
Here you can define settings for

- **Dynamic DNS** service
- **mbus** settings – *MBus is an order option - available on some models only*
- **OpenVPN** tunnel settings for the system



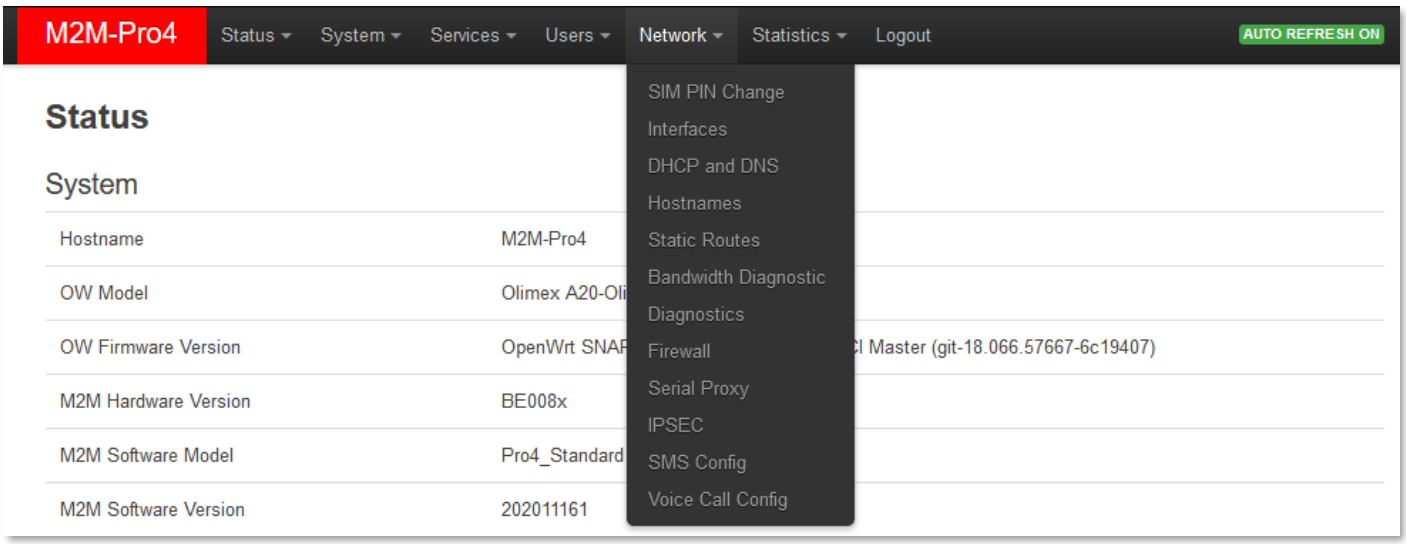
1.7 Users menu

- You can add (define) or modify, delete **Users** for allowing to access the system
- **Clone config backup/restore**)
- **Clone config backup/restore plane text** (the sam in *plain text* format)
- Define **periodic ping** for QoS and network health check
- you can add a **periodic reboot** time (for industrial standard or safety reasons)



1.8 Network menu

- You can change the **SIM PIN Change** settings here.
- Here you can configure the settings of each network **Interfaces.**
- You can modify the **DHCP and DNS** settings.
- Define **Hostnames** for external devices.

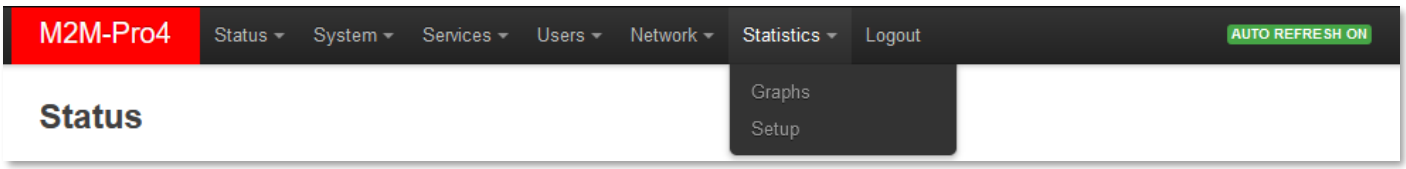


- The **Static routes** can be also defined.

- At the **Bandwith Diagnostics** item, you can configure a diagnostic address for testing the communication health.
- At the **Diagnostics** menu, you can check network access (ping, traceroute, nslookup).
- The **Firewall** rules can be declared here as the following submenu items: Port forward, IP route, NAT settings.
- Also you can configure the RS485 port communication settings at the **Serial Proxy** menu.
- **IPSEC** (tunneling settings for secure connections)
- At the **SMS Config** menu you can define (remotely executable commands) – execution by SMS messages
- The **Voice Call Config** menu is usable for remote control of the router (e.g. remote restart) – execution by voice call

1.9 Statistics menu

- And check the statistics **Graphs -** you can test the network operation and connection health by the ping an IP address for the interfaces.
- Here you can **Setup** the system **Statistics**



1.10 Logout menu

This menu item will allow you to log out from the OpenWrt® environment in your computer browser.

2. Important notes

- By security reasons, we do recommend to **change the web user inteface login** and **password** as soon as you can.
- The **4G LTE** modules can be used by inserting SIM card into the **SIM1** tray
- For the **SIM2** tray you can use an **LTE 450** or an **LTE Cat.M1 / Cat.NB2** module - which is connecting on the internal miniPCI-Express 2.0 slot. These modules can only work with an LTE450, Cat.M, Narrow Band (NB-IoT) compatible SIM cards that can be inserted into the **SIM2** slot. (In this case, only the SIM2 slot can be used.) Please pay attention to the use the **SIM2** tray, the chip is facing up. Ask us about the available compatible modules for **SIM2** tray.
- The **IPv6 protocol** is disabled for the LAN interfaces by default, change it if you want to use it instead of the IPv4 protocol. Use the **Network / Interfaces** menu **LAN1..LAN4** interface and the IPv6 relevant fields.
- The DHCP service is active for all interfaces, therefore the device will giving IP addresses for the **LAN1..LAN4** connected devices, but the protocol which is used, configured for static IP addresses for the ethernet interfaces. If you want to use and distribute IP addresses by DHCP, change its protocol to DHCP client. You can change its settings in the Network / DHCP and DNS settings menu or in the **Network / Interfaces menu**, **LAN** interface and **DHCP** section.
- The **Firewall** service is active by default (by security reasons), therefore all communication is disabled excluding the used ethernet, DHCP, DNS and WAN channels, web port and the necessary services and ports for normal operation for the router.
- We recommend you to disable all ports and protocols in the firewall which you are not using actively or which are not necessary to the connection and data transmitting by respecting the ports which are necessary for the general operation. Use to check Status / Firewall menu to check the data throughput and the **Network / Firewall** to configure new roles.
- The **firewall is not protecting the router against external network or DoS attacks**, if you just enable the firewall feature. For a massive and advanced safety, you have to customize the settings by harmonized with you used current network and connection settings.
- We offer to **check the network traffic** on your router frequently by the **Status / Firewall** menu option to be ensured that all of your connections and active communication channels (port number, incoming IP) are using only the wanted paths and routes and

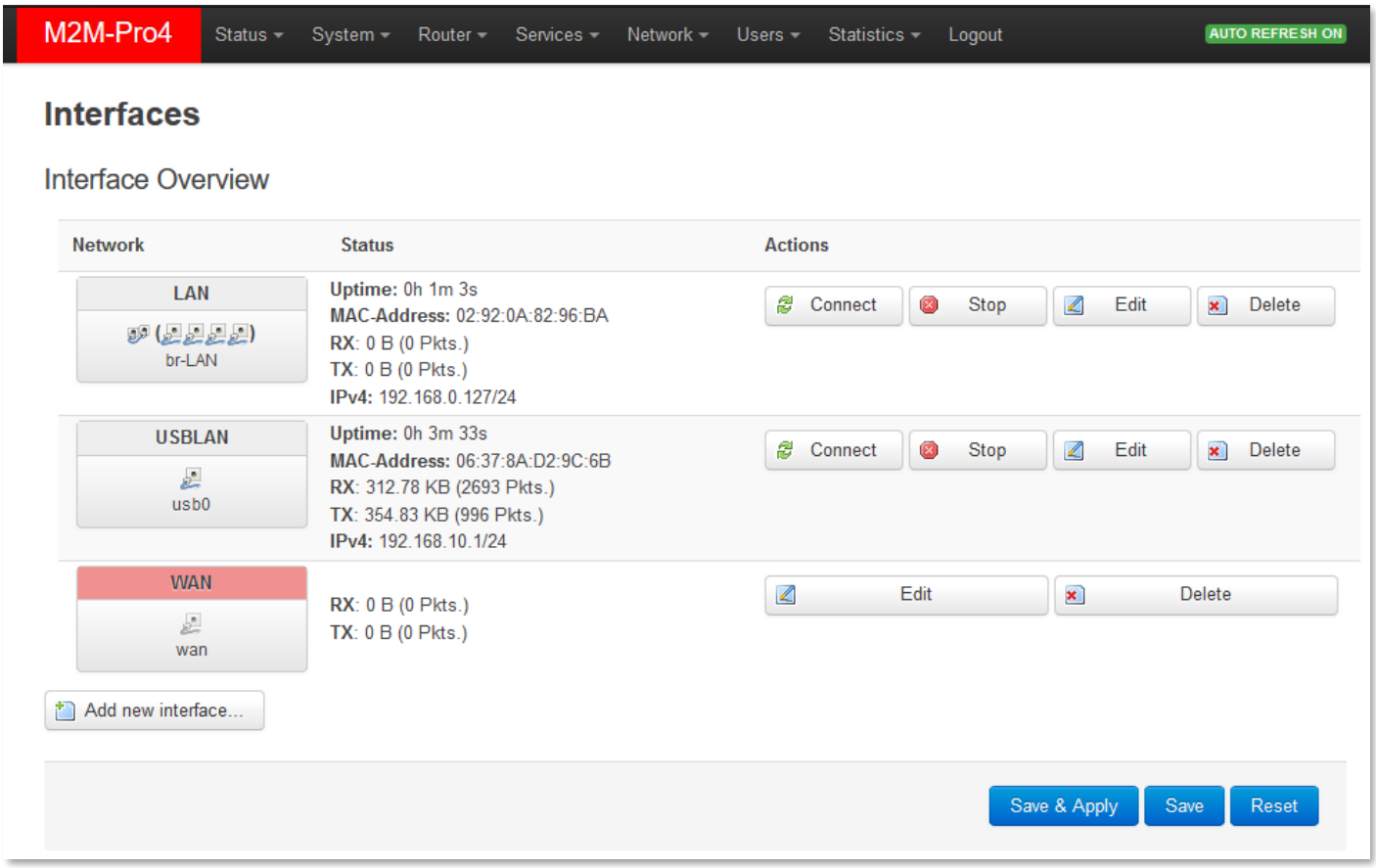
listening the defined incoming activities and consequently occuring the estimated output traffic.

- We offer to **measure your throughput data and network traffic** (by minutes, hours) – use the **Status / Realtime Graphs** or **Statistics / Graphs** and calculate the estimable data transmitting amount according your expectations and the data limits of the used SIM card.
- If you need, you can choose dedicated wireless service type or automatic mode (using which is accessible). Therefore you can limit your data transmitting for 3G instead of 4G – for example. Use the **Network / Interfaces menu**, **WAN** interface, ***Edit*** button and *Service Type* field.
- The available **APN settings** will be assured by the SIM card provider mobile operator or your mobile internet service provider. Ask them about **APN**, password, **SIM PIN** and further necessary information.
- In case of network outage, the wireless and cabled network connections, sessions will be reconnected soon, data will be received and transmitted automatically (by the settings) as the power source was estabilished. The **M-Bus, RS485** data will be received automatically afterall.
- You can configure **RS485 data speed** rate betweeen 300 baud and 115 200 baud, but pls. consider that max. 19 200 baud is guaranteed to receive. We offer to use 9 600 or **19 200 bps** (as they are standards also), because some connected systems can cause loss of characters/data in higher data transmitting speed rate.
- The **MBus** feature is optional – available only by order request.
- The **MBus** is configured for 2400 bps / 300 bps speed rate by default.
- The device is able to receive up to 32 connected **RS485** devices.
- The device is able to receive up to 30 connected **MBus** compatible meters.
- In case of network outage, the wireless and cabled network connections, sessions will be reconnected soon, data will be received and transmitted automatically (by the settings) as the power source was estabilished. The **M-Bus, RS485** data will be received automatically afterall.
- If you want to use the router without the wireless option, as a wired normal Ethernet router with M-Bus/RS485 extension, you can do in the the **Network / Interfaces** menu, by selecting the **WAN** interface settigns and there check in the **Disable modem** option.
- The router has **service modes** by its **Reset** button – for stop, restart and applying the default configuration. You will found further information in the ***Installation Guide - Service features (chapter 2.10)***.

3. Network configuration

3.1 Interface settings

The list of the available network interfaces can be found at the **Network / Interfaces** menu item.



The **USBLAN** interface is assigning the microUSB connection (***usb0*** interface).

The **LAN** interface is assigning the Ethernet port connections (**LAN1**, **LAN2, LAN3, LAN4** physical interfaces, which are bridged to the ***br-lan*** logical interface - at Linux side).

The **WAN** interface means the wireless Internet connection (as ***wwan0***) the physical 4G module.

Modifying the interface settings

At the interfaces, at right you can modify the settings with the 

button.

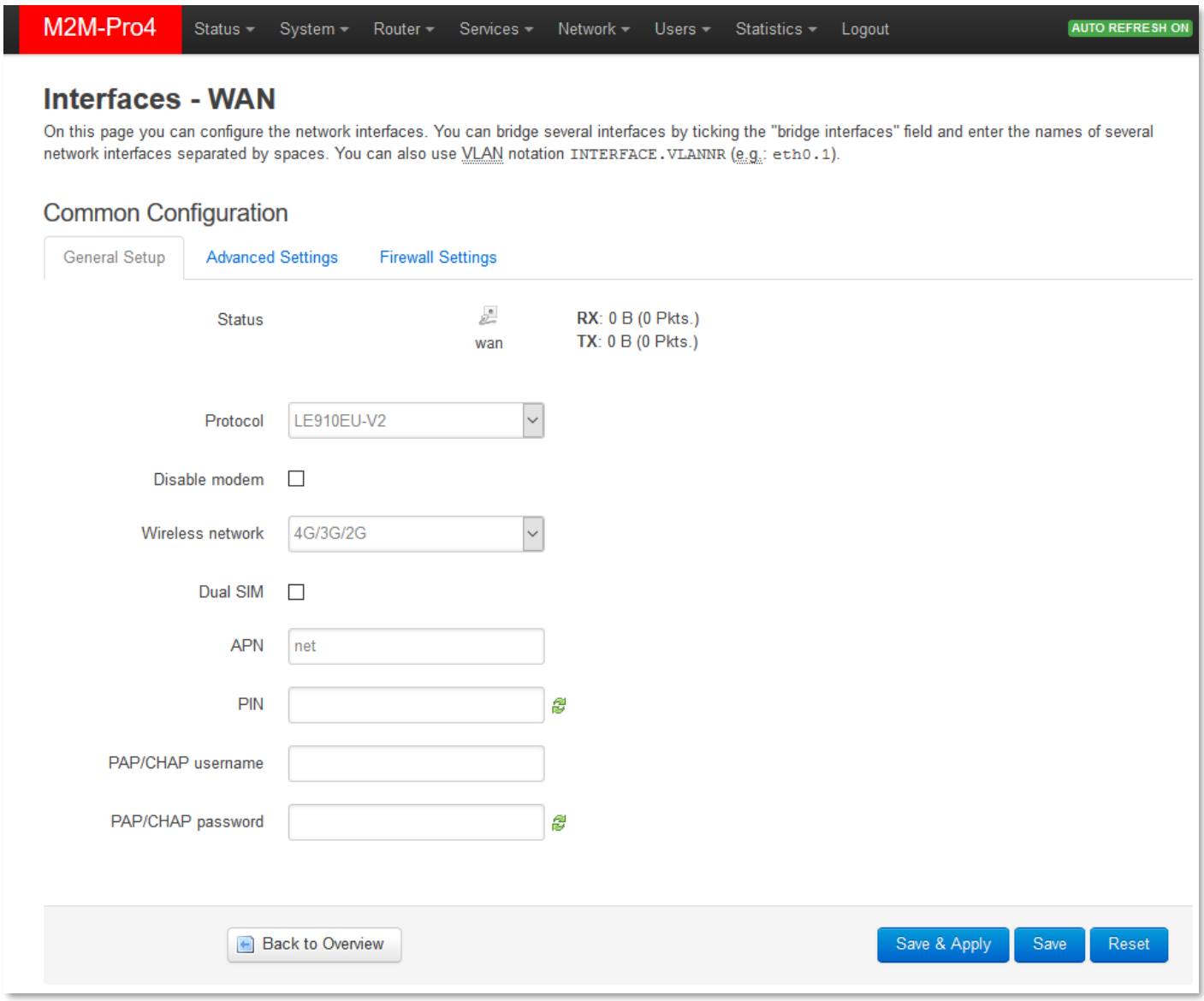
The **Stop** button stops the communication on the current interface, the 

button reconnects the related interface connection.

3.2 Cellular internet settings

The wireless module / cellular network settings of the router can be configured at the **Network** menu, **Interfaces** menu item. Open the **WAN** item from the interface list by the ***Edit*** button.

The wireless connection can be operated through the dynamic and static IP address (IPv4) assignment also - which is provided by your mobile operator.



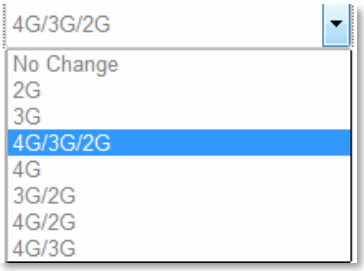
At the **General Setup** tab, you can see the current status of the interface with transmitted data amount.

Configure the module here to the wireless internet and for the 4G LTE network connection (by the network type you want to use) for the **WAN** (***wwan0***) interface.

The **Protocol** means the wireless Internet module – do not reconfigure this field, please.

In case of presence of the LTE450 or LTE Cat.M/Cat.NB module, the device recognizes the module automatically and it configures the **Protocol** field to the neccessary value.

The Service type is the used wireless settings – you can choose a communication band or you can leave it on the default value: *LTE (4G) / UMTS (3G) / GPRS (2G)* – which means *Auto mode*.



This mode grants the best speed and quality option on the network and *fallback* feature (the highest cellular network service is not available - e.g. when the 4G service is not available, the 3G will be used, etc).

If you have to use a dedicated network like 3G, 2G, etc., then choose the required network type. **Take consider, that the fallback mode will be inactive in this mode** – if you choose the *LTE (4G)* and it the network will be not available, there will be no 3G or 2G fallback (if the choosen network is not available, the router won't get mobile network access). For fallback always choose the Auto mode (LTE / UMTS / GPRS).

DUAL SIM – this option is still in development.

Here you can define the **APN** name for the Internet connection, which is necessary to use.
When you will not set any value for the **APN**, then the router will restart the module sequentially in every ca. 10 minutes until it is not configured properly.

Here you can define SIM card's **PIN** code if it is necessary for the connection.
Note, that the **PIN** code which is already configured here, it cannot be seen here due to the security rules – the characters are placed by asterix signs. Just modify the PIN if you would like to change.

> ***Attention!***
> *The available APN settings will be assured by the SIM card provider mobile operator or your mobile internet service provider.*

Important! *If you need to change the PIN code, use the Network / SIM PIN Change menu item.*

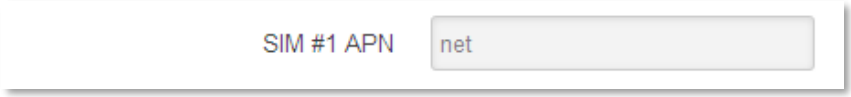
Here you will found some examples for the APN settings.

M2M APN (enclosed)

APN name: wm2m

Public Internet APN

APN name: net



Attention!

ALWAYS use the APN name and password, which was given by your Mobile Operator.

ONLY for NB IoT (Vodafone GDSP SIM)

APN: **nb.inetd.gdsp**

APN password: *(not presented)*

ONLY for GDSP SIM (WM2M GDSP)

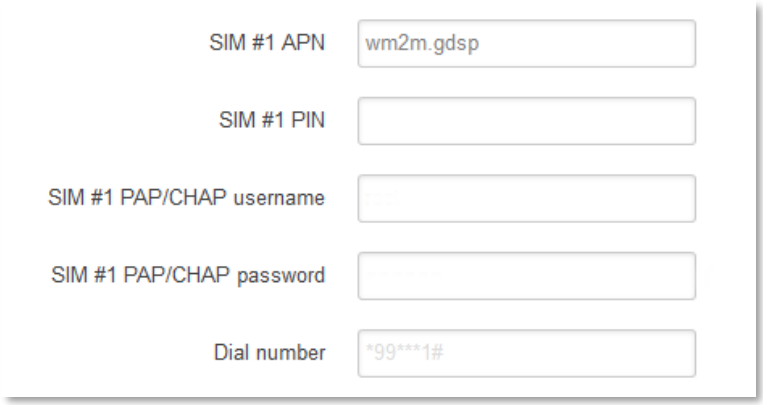
By using the GDSP SIM you have to follow the hints of the mobile operator when filling the SIM #1 APN, APN username and password fields.

In case of APN (WM2M network): **wm2m.gdsp**

APN username: **IMSI** identifier of the **SIM card** (number written on the SIM card, and which is usually starting with „20404" tag)

APN password: **wm2m.gdsp**

(e.g. to use the the Hungarian WM2M)



For further international mobile network providers or in case of using in foreign countries this information is assured by the local GDSP SIM mobile provider.

Automatic mode

When you not set any value for the APN, the router will connect by the SIM-card automatically to the next available network's available APN**.**

Authentication methods:

- The **PAP/CHAP username** and **PAP/CHAP password** settings can be also configured here – if it is required for the connection.
- If you need dialup connection for using the Internet service at your provider, set the **Dial number** value (format: *99***1#).

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

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

The international country codes can be found here: http://mcc-mnc.com
Ask your mobile operator about the available international settings.

If you want to disable the WAN interface (cellular internet module) – e.g. in case of using the router at an Ethernet router – then check in the **Disable modem** option.

Click to the **Save & Apply** button for saving the settings, while the device is restarting the module with the new settings and will connecting to the cellular network.

Then, you can check the data transmitting at the **Network** / **Interfaces** menu, when check the **WAN** interface status at the **Interfaces** part.

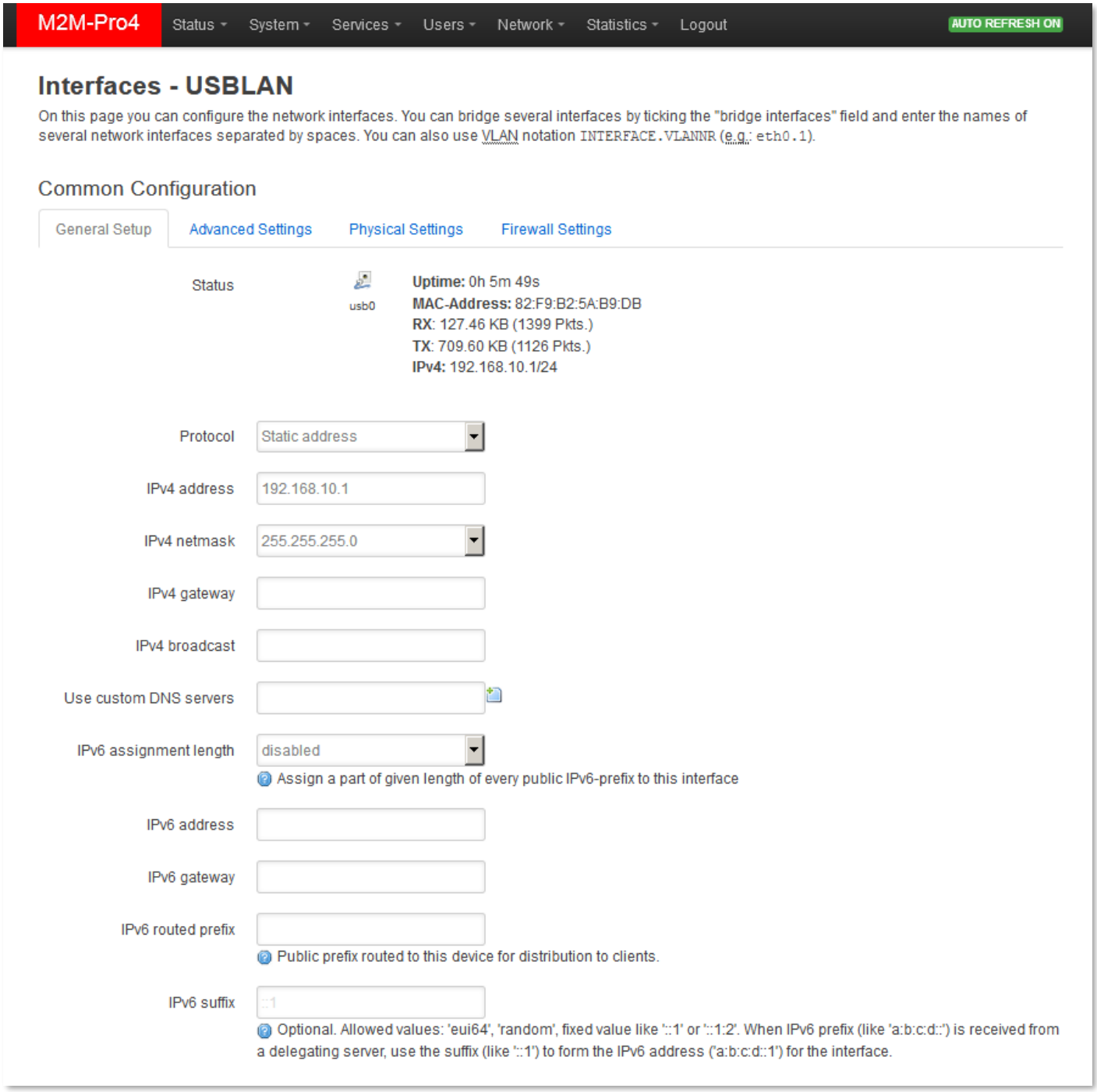
As you can see, the router is already connected to the cellular network, it has active data traffic and the **RX** (received data), **TX** (transmitted data) at **Packets** and **KB** (KBytes) values are growing.
At the **Advanced Settings** tab you will found further settings for the wireless module.

By default we do not offer to change these settings, only if you are special requirements at operating the mobile network communication by the router (these are the **LCP Echo** settings, the **Bring up on boot** and the **use built-in IPv6 management** parameters mainly).

If you have had changed some values here, please click upon the **Save & Apply** button for saving the settings. Then the device will reconnecting the module to the mobile network.

3.3 USB settings (USBLAN interface)

The router has an alternative LAN interface through the USB connection. The usage of this port is ideal for configuration purposes, while you can use active data communication throught your LAN interfaces.



The **USBLAN** interface settings for the USB Ethernet connection, which can be performed by **Network / Interfaces** menu item at the **USBLAN** part, where you need to choose the Edit button. Then choose the **General Setup** tab.

Here you can define **Protocol** *(Static address* or *DHCP client*) for getting IP address from a connected network device (another local router device or similar network host).

You can define the **IPv4 address** of you *static* connection.

The IPv6 addresses can be also used, but by default the setting for the router is disabled by the **IPv6 assignment length** (*disabled*). You can allow this and add the IPv6 settings too.
You can make the **USBLAN** settings according to the Ethernet (**LAN1..LAN4**) configuration parameters which are similar.

If you have had changed some values here, please click upon the **Save & Apply** button for saving the settings.

3.4 Ethernet (LAN) settings

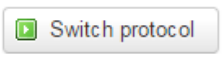
The detailed interface settings for the ***LAN1, LAN2, LAN3, LAN4*** Ethernet ports can be performed by selecting the **Network / Interfaces** menu item.

At the **LAN** interface's 

button, choose the **General Setup** tab**.**

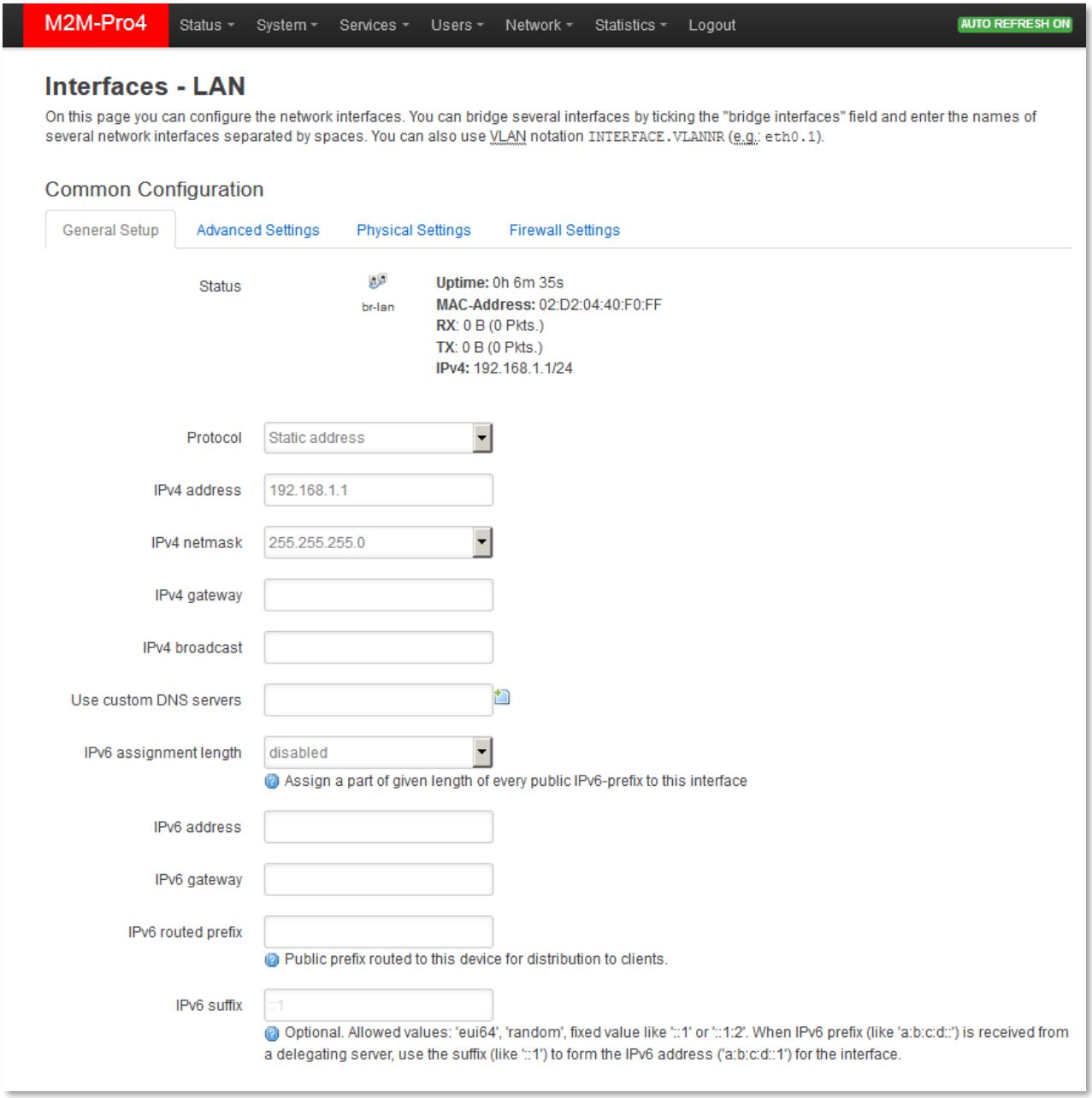
By default the Ethernet IP address is *static*, the default IP address is: 192.168.1.1.). If you wand to switch the **BR-LAN** interface to *dynamic* (at **Protocol** field), then the router will waiting for an IP address on the network.

Define a new **IPv4 address,** check the **IPv4 netmask** (subnet mask), **IPv4 gateway** values for your devices according to your needs – to be able to serve your connecting devices.

When changing the **Protocol** field, youu need to push the 

button.

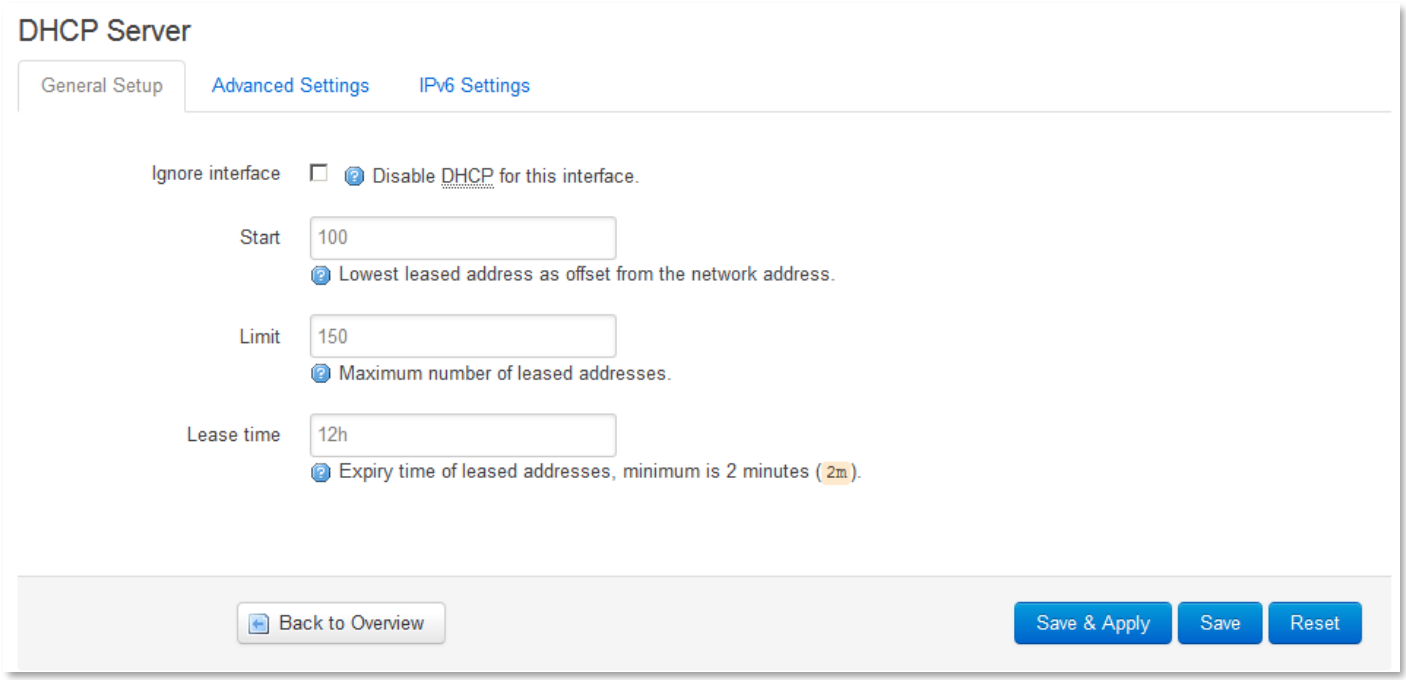
If you want to use the local *DHCP server* – to allow to add IP addresses by the router for the connecting external ethernet devices – then the right setting is the *Static Address*, and the **IP address** should be also changed, and you have to uncheck the *DHCP disabled* option for the **BR-LAN** interface to allow the DHCP server.



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

Then the bridged **BR-LAN** interface IP address will be changed according your request due to the new settings.

The IPv6 addresses can be also used. By default it is *disabled* by the **IPv6 assignment length** (if you want to use, *Enable* it).

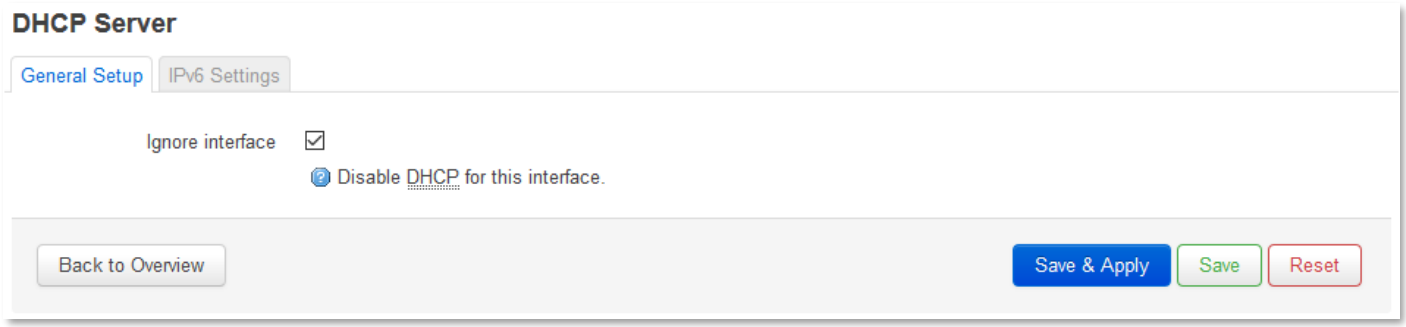


You can find further important *DHCP* settings at the **DHCP and DNS** menu. At the **General Settings tab** tab you can define IP range (**Start**, **Limit**) and **IPv4 netmask** for your network.

3.5 DHCP and 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** menu, **Interfaces** (according to the required interface), *Edit* and **Advanced Setttings** tab item.

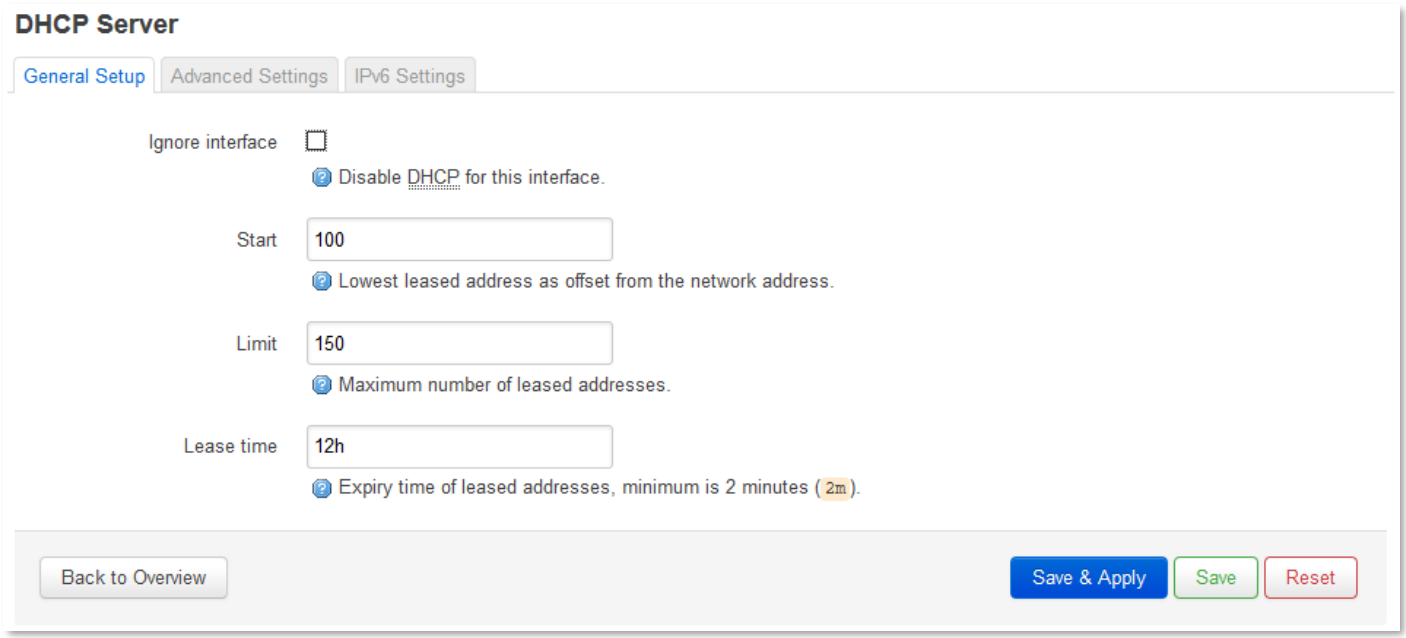


Important!

The DHCP service is disabled by the factory default configuration. First, you have to enable the DHCP service for the usage and performing the further DHCP settings!

If you attempting to enable the DHCP service, uncheck the *Disable DHCP for this interface* option. Then the related parameter settings will be visible with their default settings.

The **Start** field means the starting IP addres in the subnet for the connecting devces (by default 192.168.x…).
You can **Limit** how many IP addresses will be provided. The router will be providing IP addresses for the connecting devices in the 192.168.x subnet within the *Start* and between the *Start+Limit* address range (especially important for WiFi).



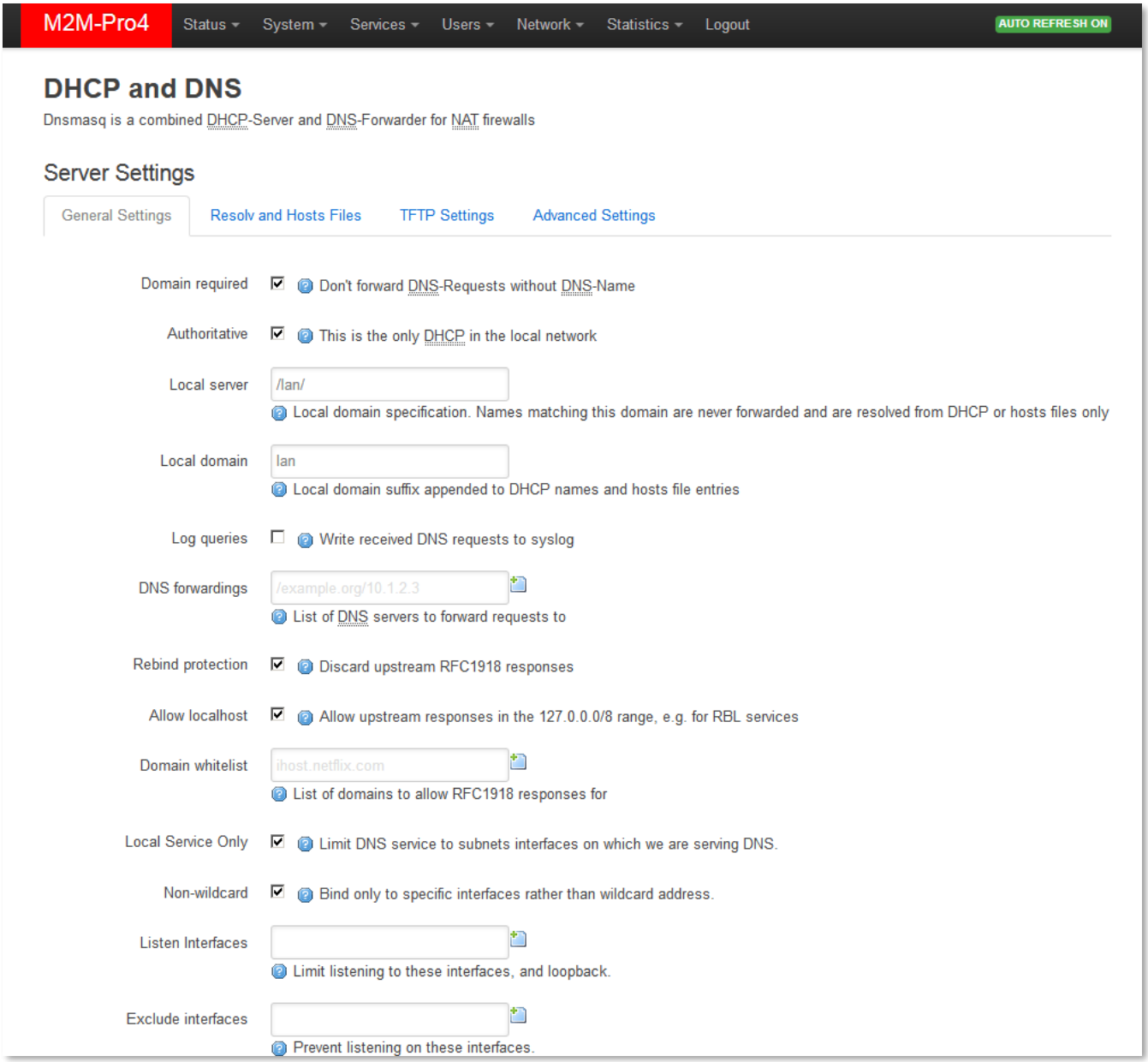
Save the settings with the **Save & Apply** button.

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

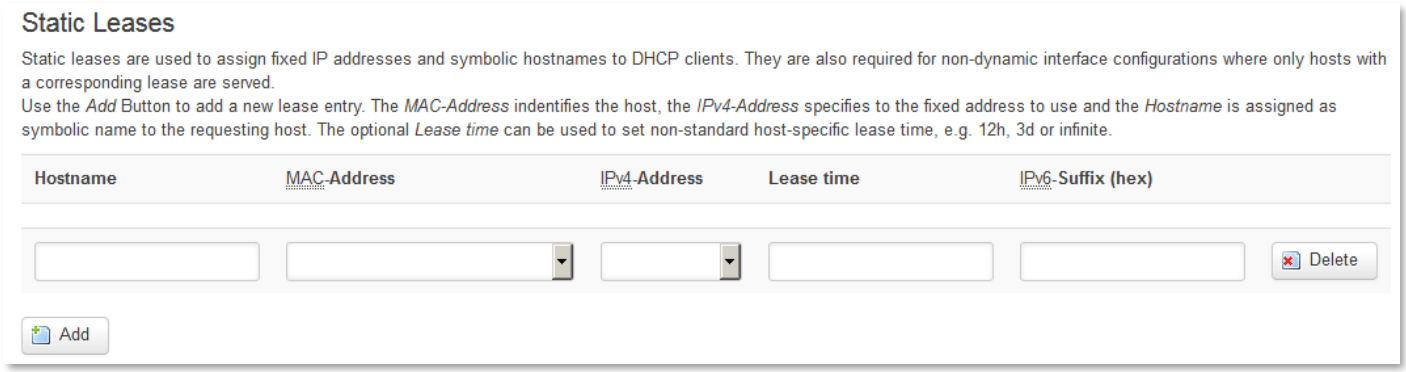
Below, at the **Active DHCP Leases** part you can see the list of the devices, which given their IP addresses from the router's DHCP service (with the renewal *lease time*).

At the **Static Leases** you can add network devices by the 

button to be guaranteed to get the same IP address after every leade time renewal.



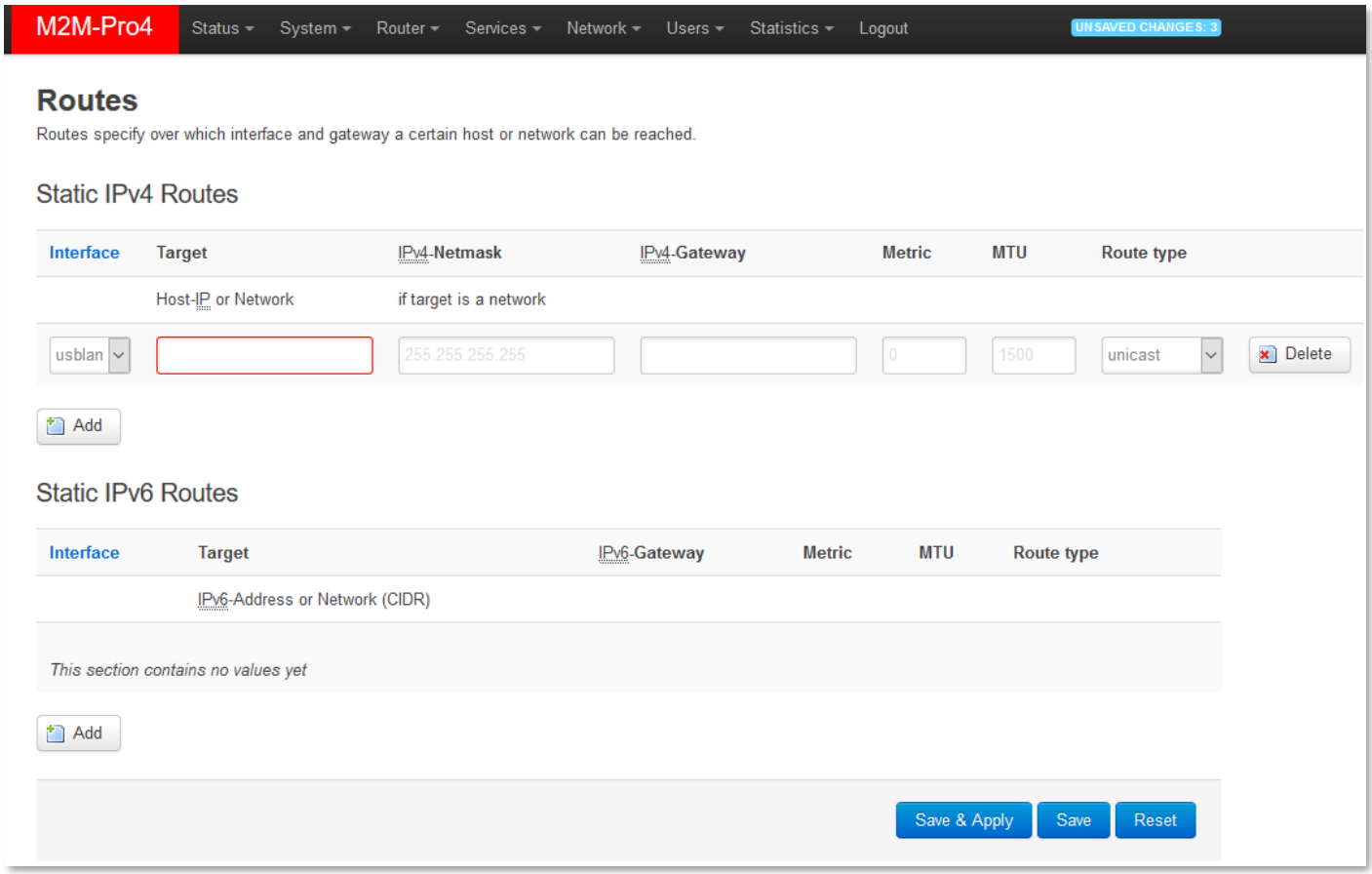
Define a **Hostname** and the valid **MAC-Address** of the device and the required **IPv4-Address**.



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

3.6 Defining the route rules (Static route)

We offer to check the currently used route rules - ARP routes, and the IPv4 and IPv6 route rules which you can find in the **Status** / **Routes** menu.



Here you can define a new IP route rule, 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**.

To apply the new settings, **Save & Apply** your settings you made here.

3.7 Firewall settings

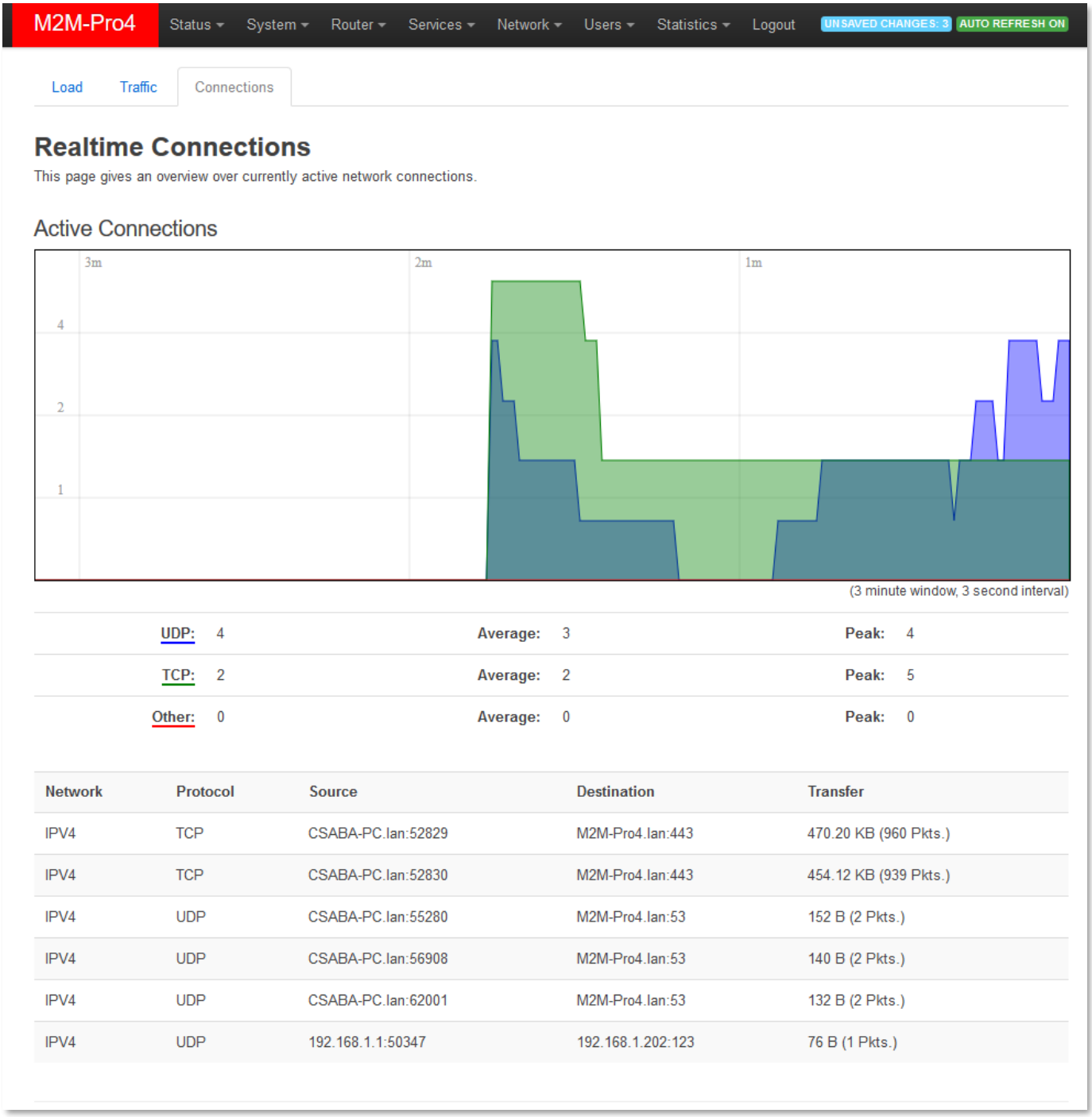
By default, the firewall service is active, but it allows all communication. It can be necessary to limit the traffic.

> ***Important!*** *We offer to check the network traffic on your router. Check connections and active communication channels (port number, incoming IP) and listen the incoming activities and the output traffic!*

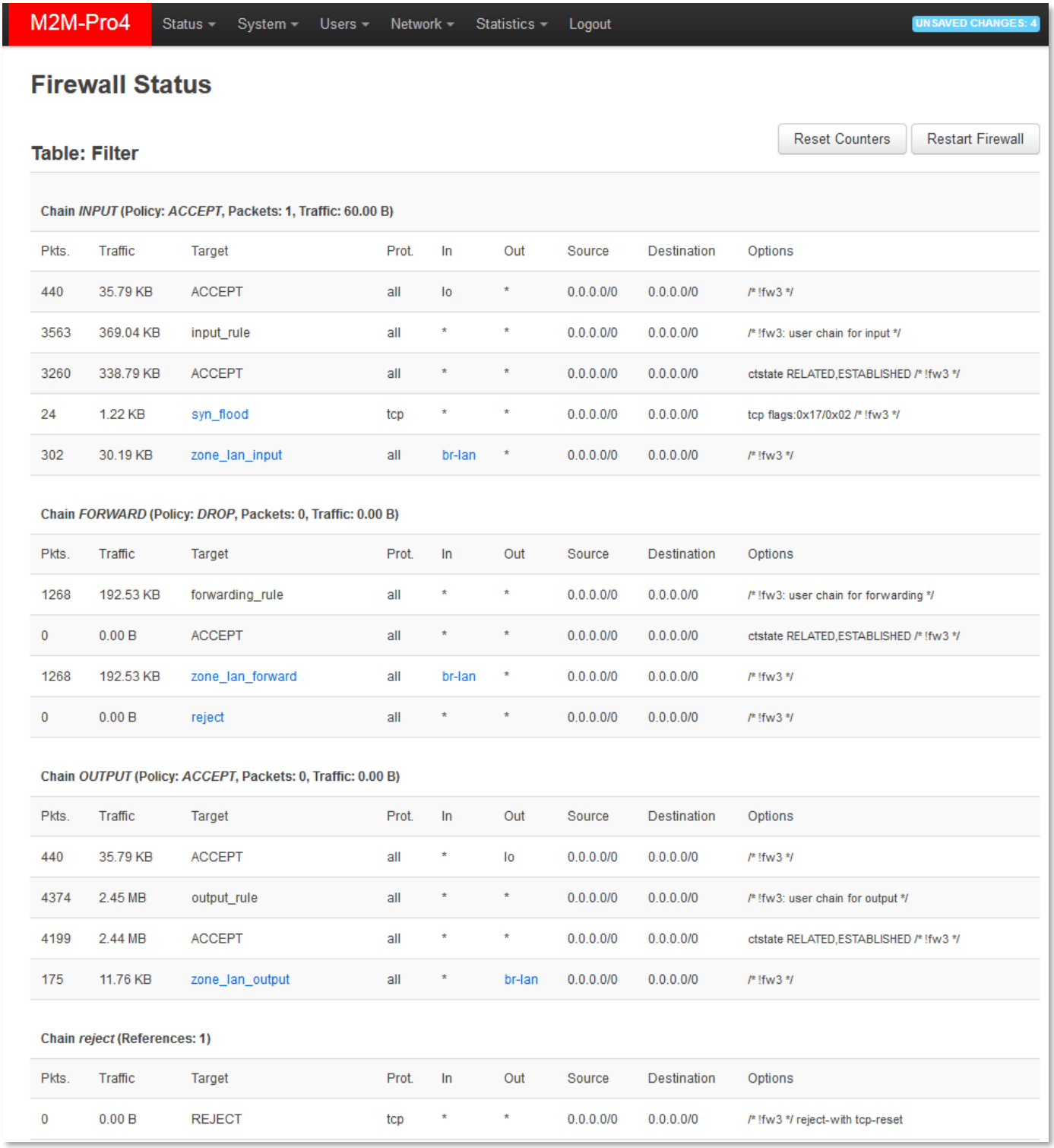
We highly recommend to check the firewall settings and configure the communication to reject the unnecessary boundaries.

On the public Internet, you can have several network attack and getting unwanted communication, internet data collection by applications. These all over the unwanted network activity causes the growing the mobile network traffic and increasing the transmitted amount of data (which is unnecessarily decrease the available data package amount of the SIM card in the router).

You can check all of these at the **Status** menu**, Realtime Graphs** item at the **Connections** tab – where these can be listed.



If you'll find and identify communication from an unwanted IP/port address/range, then you can disable or limit the affected port or IP-segment at the firewall setting rules to deny/prohibit this traffic by disabling the communication on it.



In the **Status** menu, **Firewall** menu item you can check the actual firewall statistic.

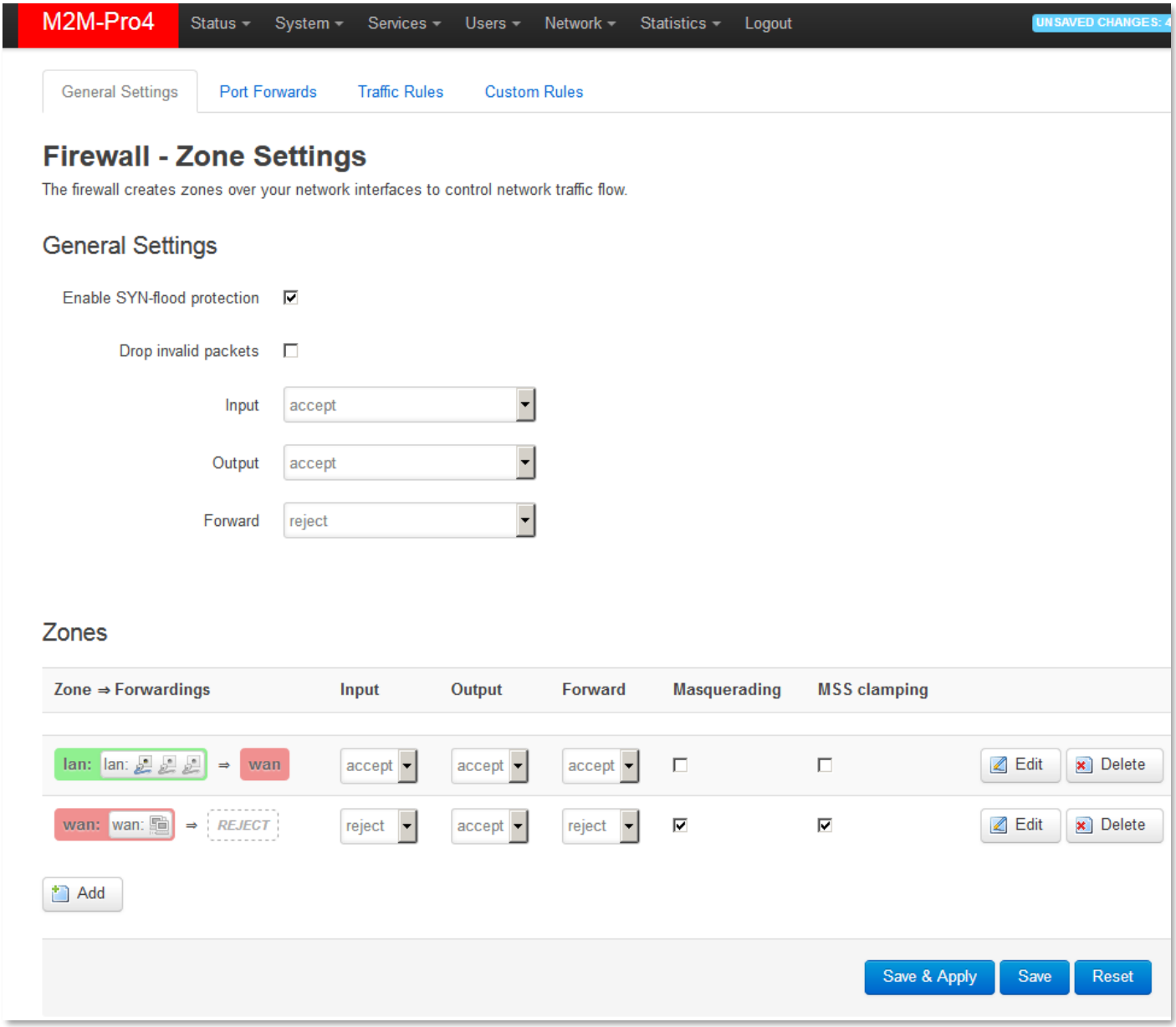
The ***INPUT chain*** means the incoming, the ***OUTPUT chain*** is the outgoing/transmitted and the ***FORWARD chain*** means the forwarded communication/traffic hereby.

You can also see the **Reject**ed chain here below.

As it can be seen, there are several communicating IP addresses on several ports for the router and subnet.

Another method for limitation is to disable all ports, to open and enable only the necessary and used communication ports, define the used IP address range by allowing exact IPs.

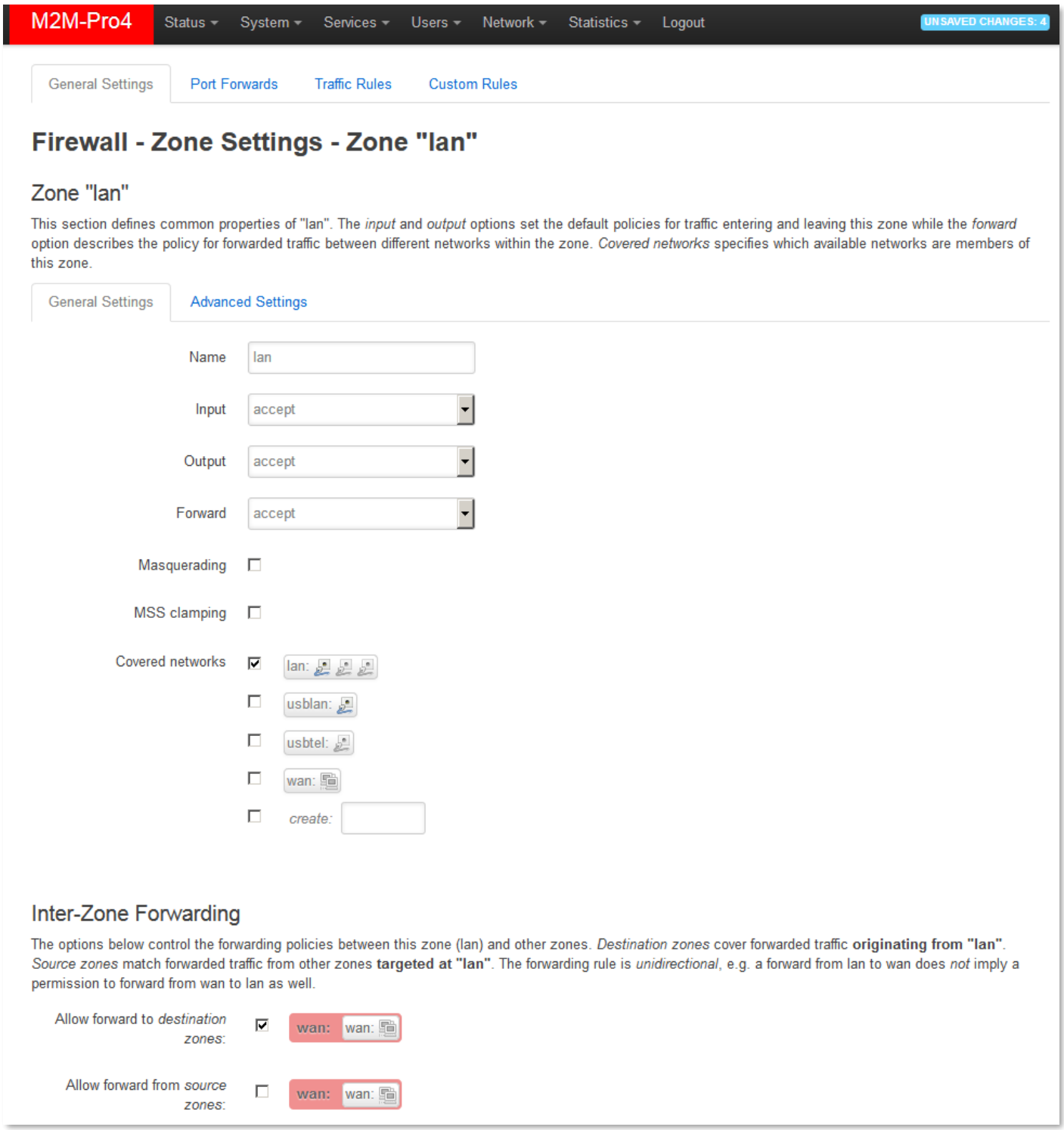
You can modify the firewall settings at the **Network** menu, at the **Firewall** item, **General Settings** tab.



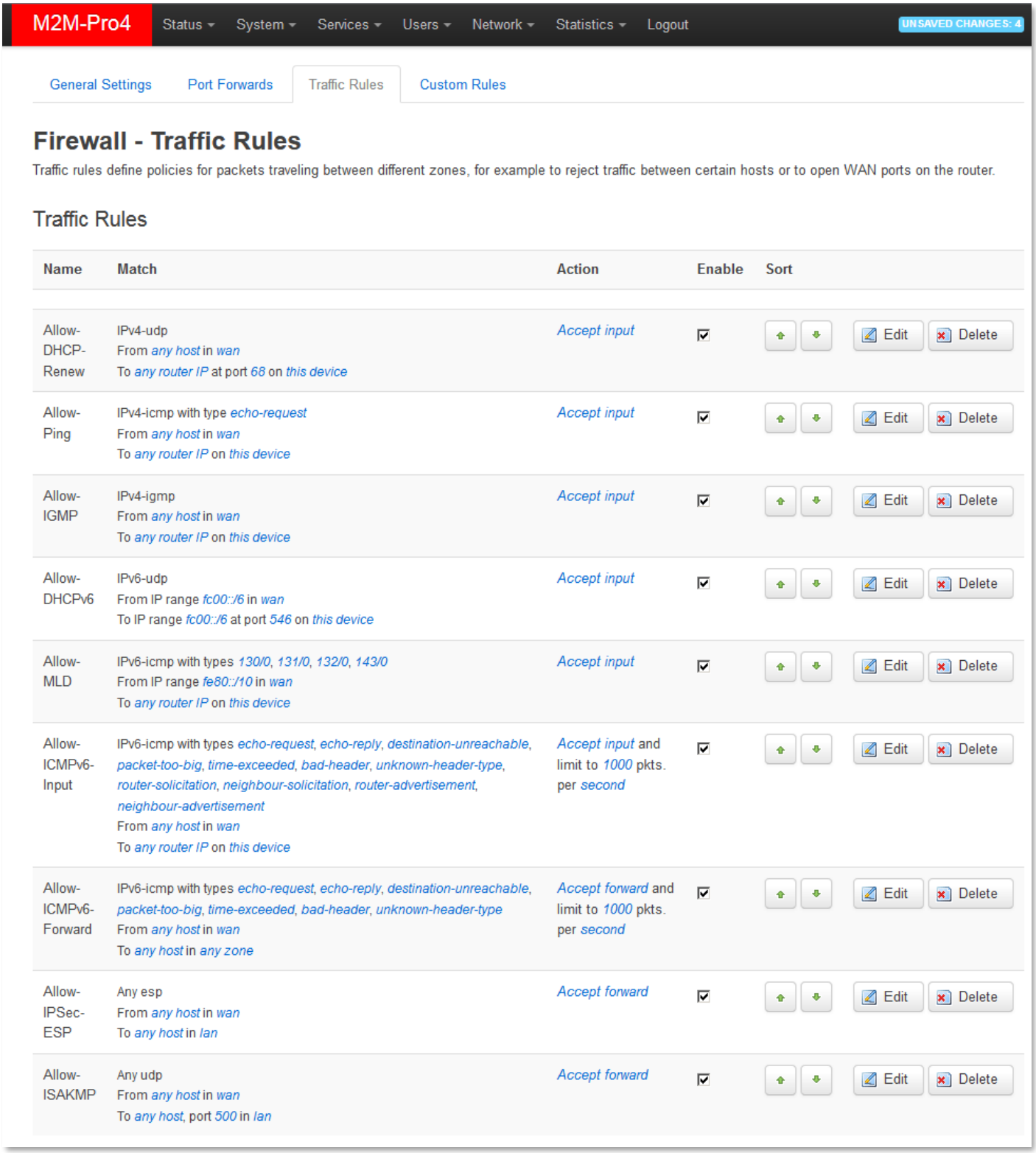
As you can see, the communication rules are listed here by their acceptance (*Accept/Deny/Reject*) with the directions of the communication (*br-lan* to *wan* or other).

Here, you can check or modify these firewall rules for the communication, at the **Input** (incoming), **Output** (outgoing) and **Forward** operations one by one by **accept** it, or **reject**, **drop.**

You can **Delete** the settings or Edit modify. Below, at **Zones** part you can Add a new rule to the current ones. You also can Delete or Edit an existed rule. Save the modified settings by **Save & Apply** button.



Under the **Advanced Settings** tab, you can restrict outbound, inbound, or forward traffic to individual subnets.



If you'd like to **add new rule to the firewall settings,** it must done **carefully**, because you can disable or tilt some ports out of the communication so easy (which ports can be used by the device (by default) or they are necessary to existing for some network services or could required by some other running tasks). E.g. Port nr. 67 is used by DHCP service, as Port nr. 80 for web service, DNS for port nr. 53, OpenVPN at port nr. 1194 and the RS485 also uses a dedicated port).

You can add a new port (which you have configured for the relevant service) to the firewall rules by the Add button. Configure the port and save the settings. Don't forget to Delete the old, not relevant rule for the service. For modifying the Firewall settings, choose Edit button.
If you have changed something, save the settings with the **Save & Apply** button.

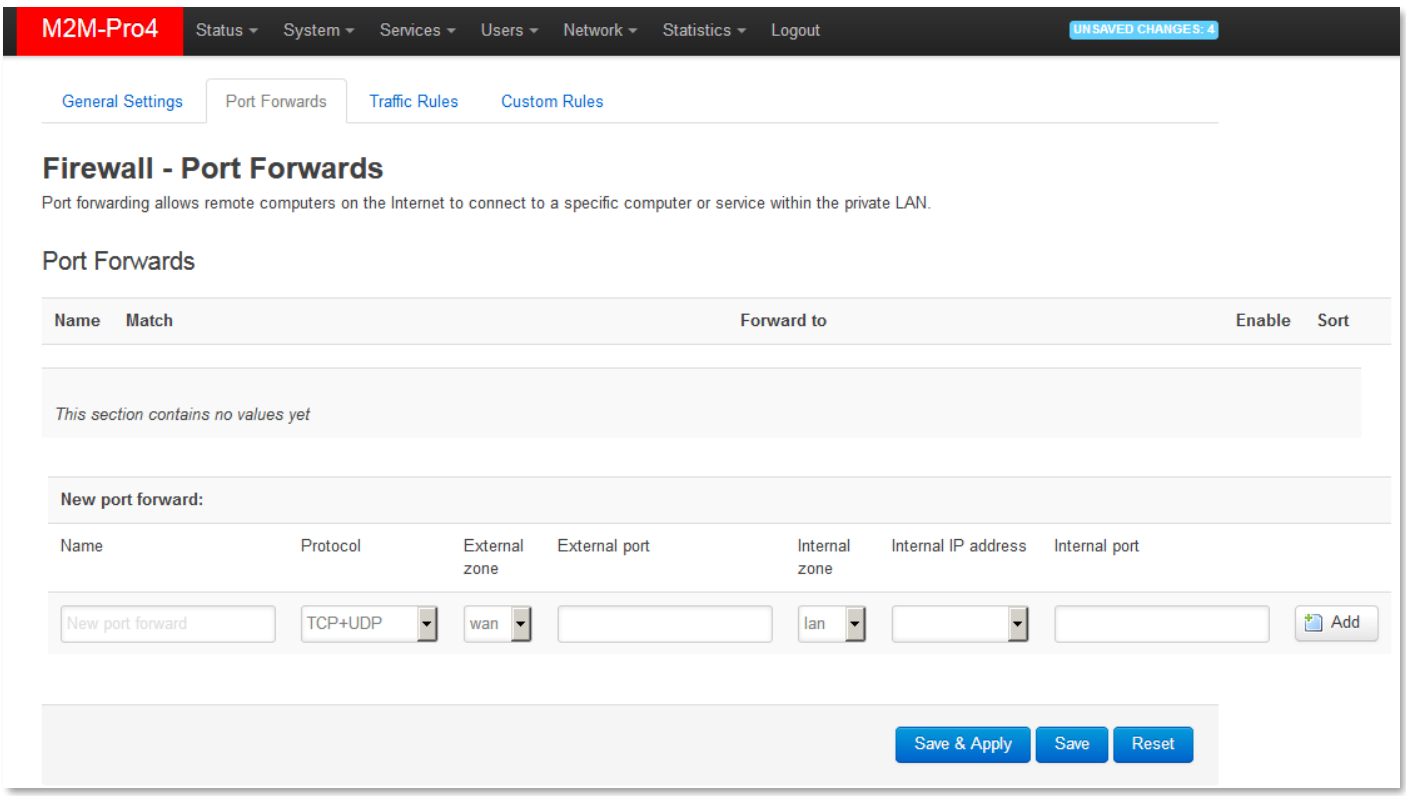
The firewall enables or disables all communications by default, depending on the settings. Therefore, enabling the firewall service does not in itself provide protection, additional ports level filtering or other restrictions on interface traffic!
For a port-level filtering or interface traffic limits or **Traffic Rules** settings are also necessary to define!

Here you can **Enable / Disable** or Edit, Delete a configured rule.
If you have modified the settings, save them by the **Save & Apply** button.

3.8 Port Forward settings

Here in the **Network** menu, at the **Firewall** item, **Port Forwards** tab you can setup the port forwarding rules for the router.

You can add a new rule by the Add button.
Here you can define a rule with the necessary **Protocols**, interface (**External zone** and **Internal zone**), Ports (**External ports**, **Internal ports**) and the **Internal IP address** values.



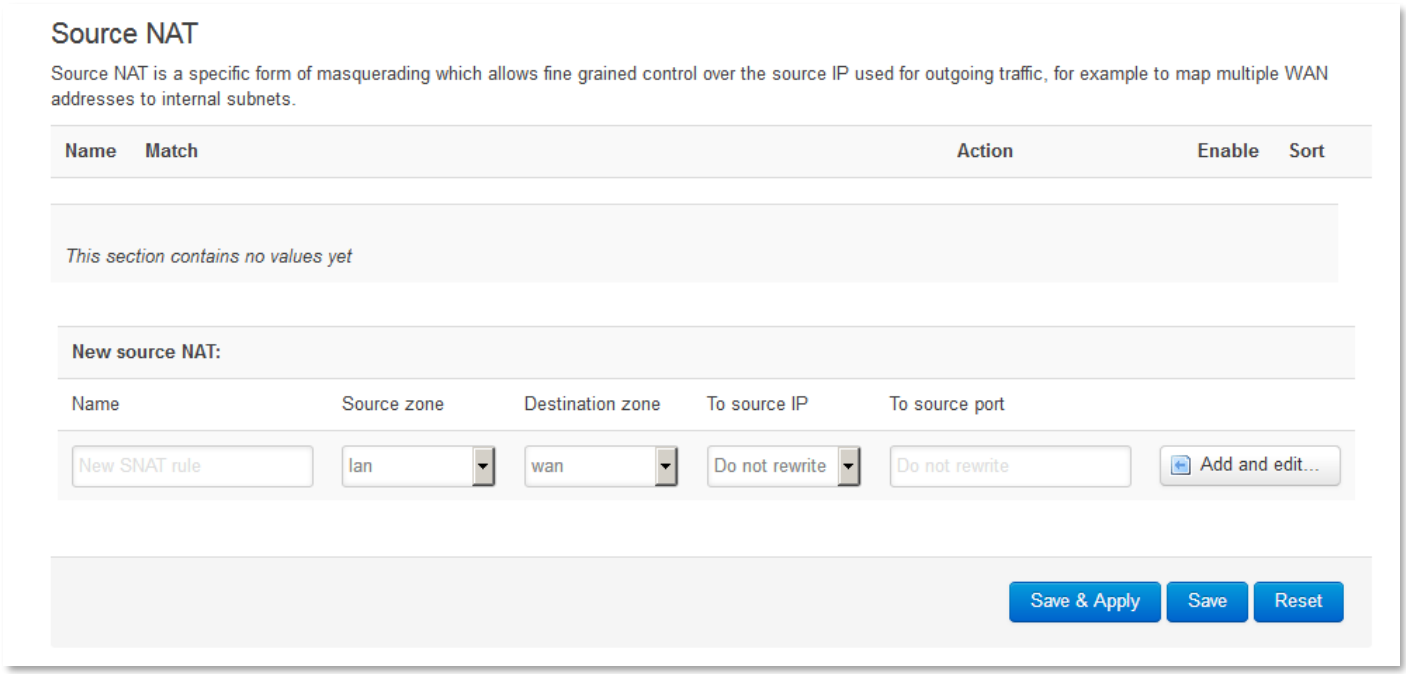
When you modified the settings, save them by the **Save & Apply** button.

If you already have a forwarding rule, you can **Enable**/**Disable**, or **Edit**, **Sort** or **Delete** the rule.

3.9 NAT settings

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

You can add a new rule by the Add button and **Save & Apply** to close the upcoming window.



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

The **Source NAT** settings (below) 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.

These rules must always be defined, not to disallow the general communication.

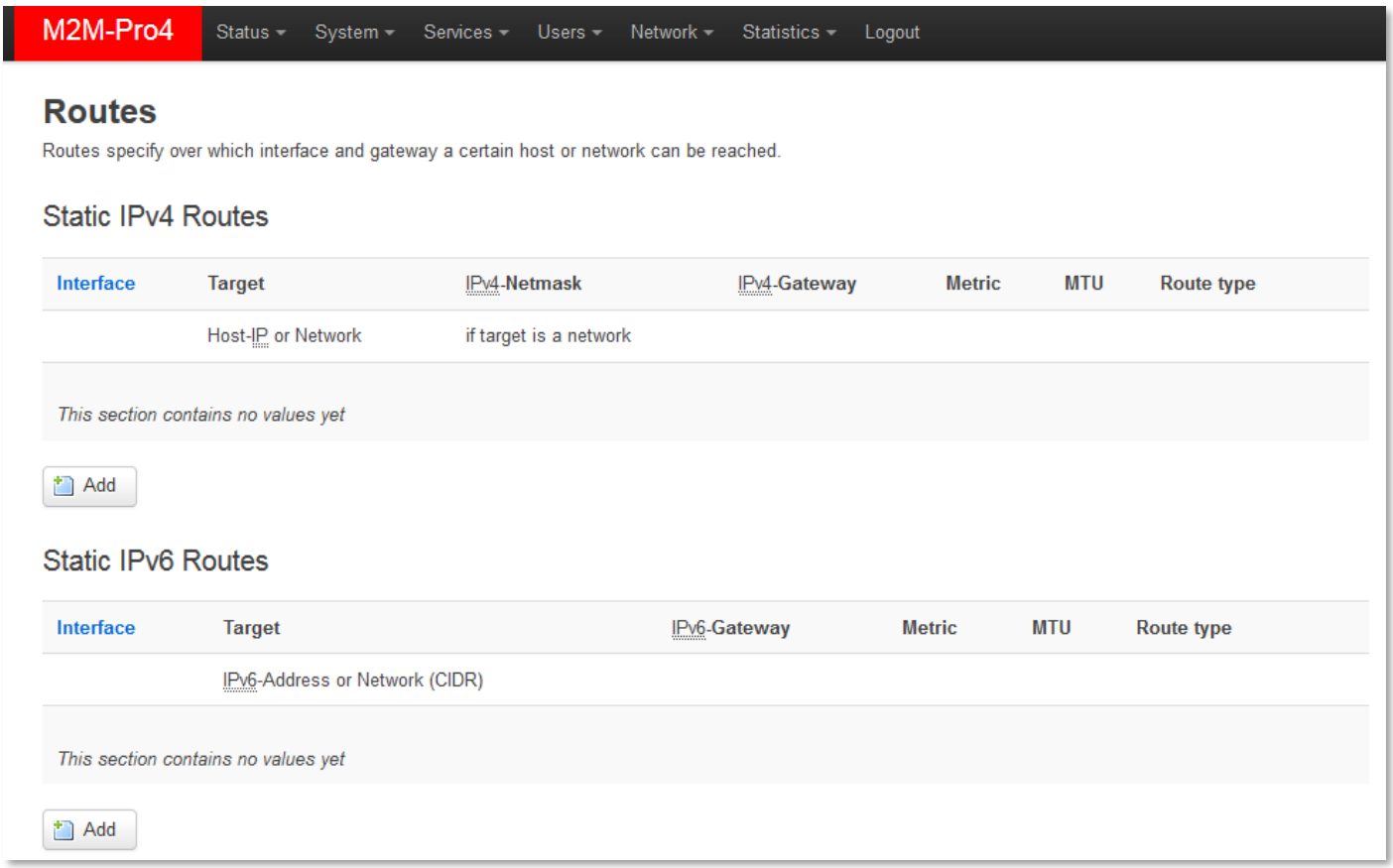
Take care, because it is easy to enclose the router from the network or disabling the remote access. Please, be careful when configure these settings.

> ***Important!*** *Always check the standard ports, which are used by the network services and always allow these to operating (e.g. FTP: port 21, SSH/Telnet: port 22, web: port 80, DHCP: port 53, NTP time server: port 123, general network traffic on Windows: 443, etc).*

The proper port filtering, routes are minimizing the communication, what could be important by safety reasons, and could decrease the open threads and risks of some safety leaks.

Always limit the access of services, and decrease the amount of the throughput communication on the network by these rules to provide the operation only for the necessary services, ports, ip addresses. When you modified the settings, save them by the **Save & Apply** button.

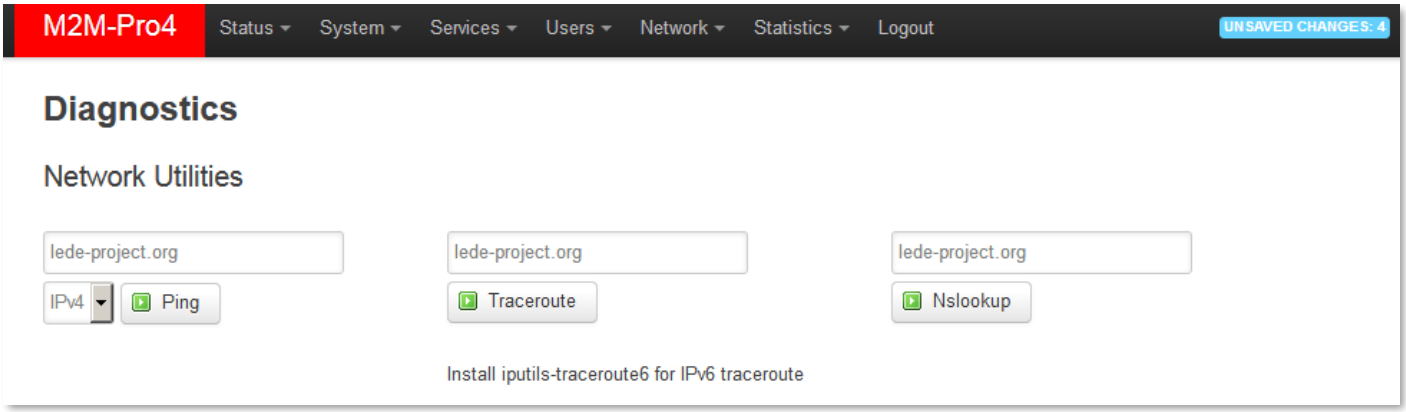
At the **Network** / **Static Routes** menu item you can define a new route.



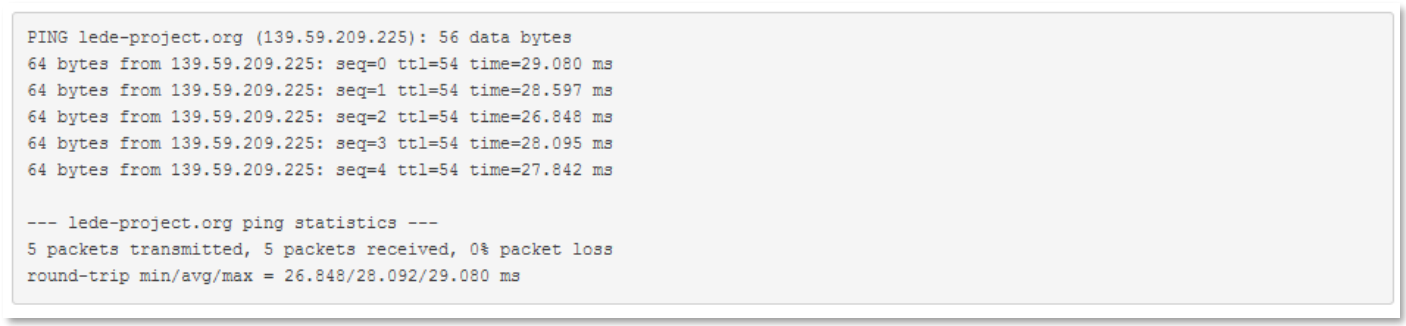
4. Advanced services

4.1 Network diagnostics

Open the **Network** menu, **Diagnostics** item.



Here you can check the availability of an IP address, that is it accessible (push Ping button), is there a naming service provided, and is there response between two IPs (push Nslookup button), furthermore you can query the path of the communication (by Traceroute 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 that IP addresses, which are accessable 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).*

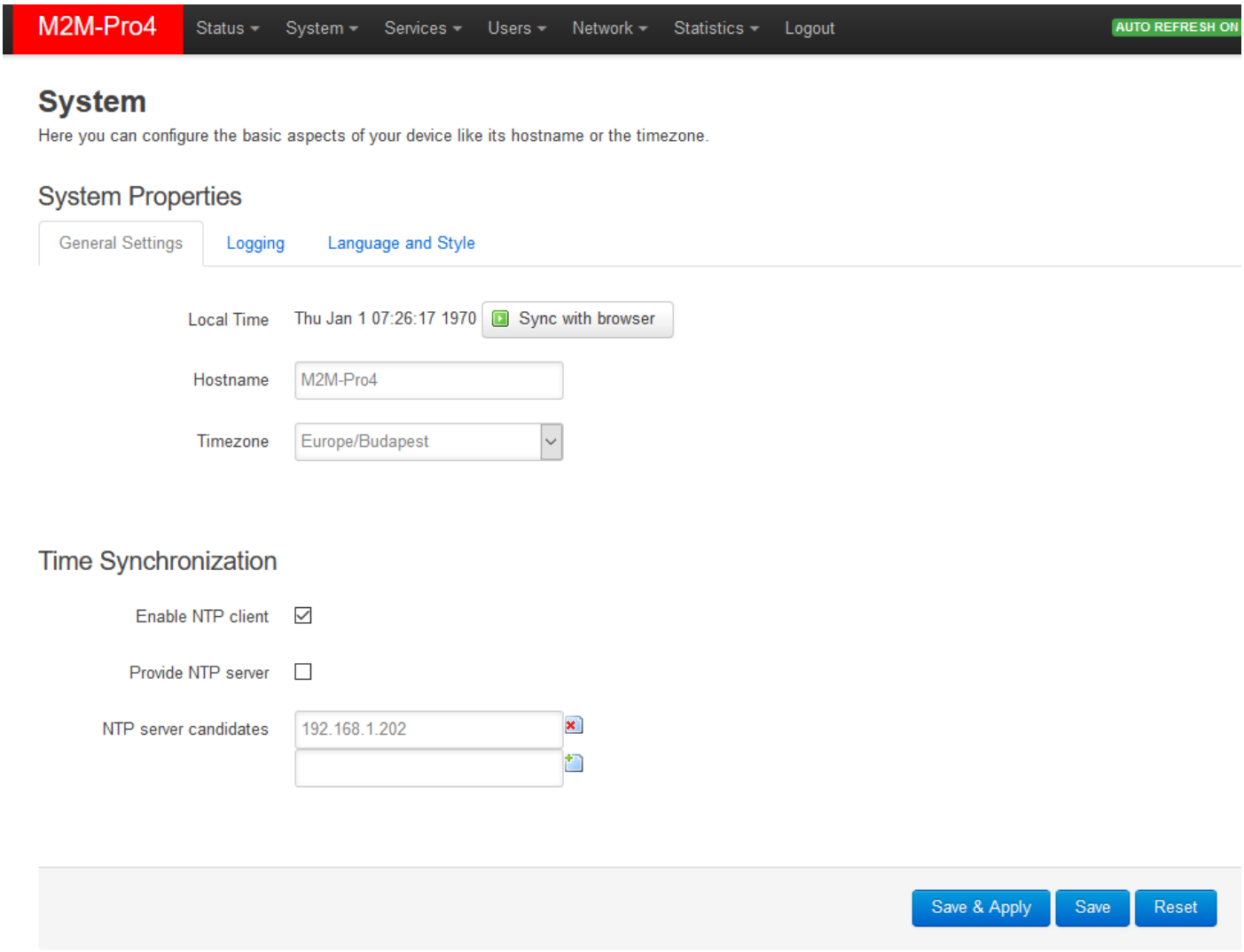
In case of M2M APN the 192.168.1.250 address can be accessed, it is possible to ping the address for checking the 4G network connection.

4.2 Network Time Service (NTP)

Open the **System** / **System** menu item.

Here, at the **Time Synchronisation** part, you can can enable or disable the **NTP client** function (to receive time data from time servers).

You can Add further NTP servers or Delete some.



You can also specify the addresses of the NTP servers (**NTP server candidates**).

The most of the NTP time servers are using the port nr. 123 (UDP) for time synchronisation. Note that the router must have public internet access for reaching the time servers or the time server must be in the same APN zone.

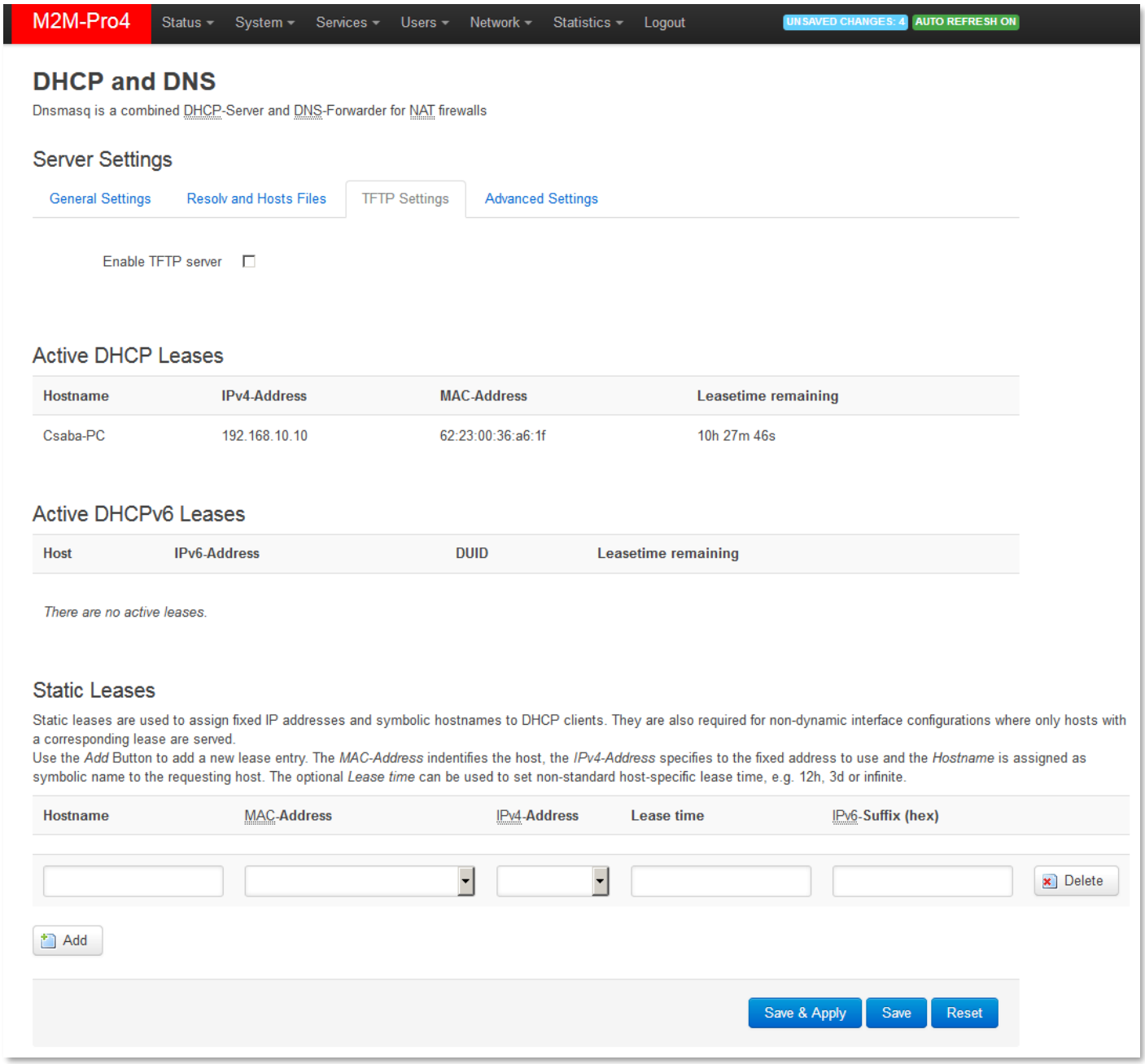
You can also **Provide NTP server** (date and time) for connecting devices.
If you have modified the settings, save by **Save & Apply** button.

4.3 TFTP settings

Open the **Network** menu, **DHCP and DNS** item, **TFTP settings** tab to allow the TFTP service.

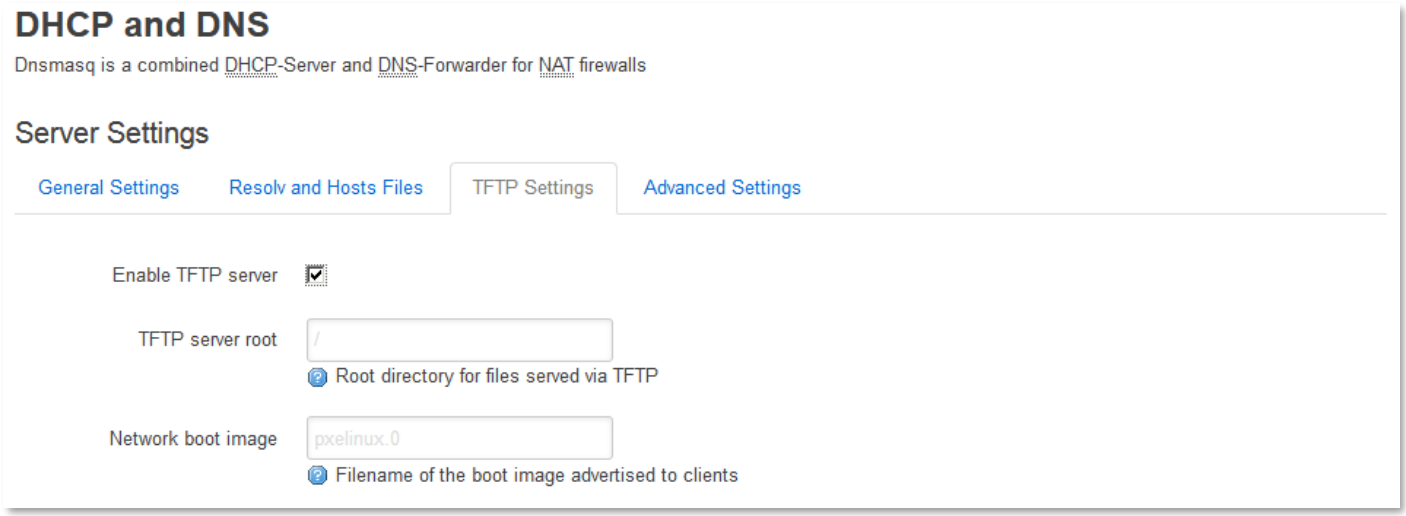
Enable TFTP server, and define the further related parameters to make the FTP service operating for sending files to a remote or distant IP address (e.g. to a server).

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



If you allow to **Enable the TFTP server**, the following fields must be filled: **TFTP server port, Network boot image.**

You can also use SFTP service to connect from the router to an IP address, by the root account and password. If you need more information about the settings, check the OpenSSH settings in Linux command line (see Chapter 9).

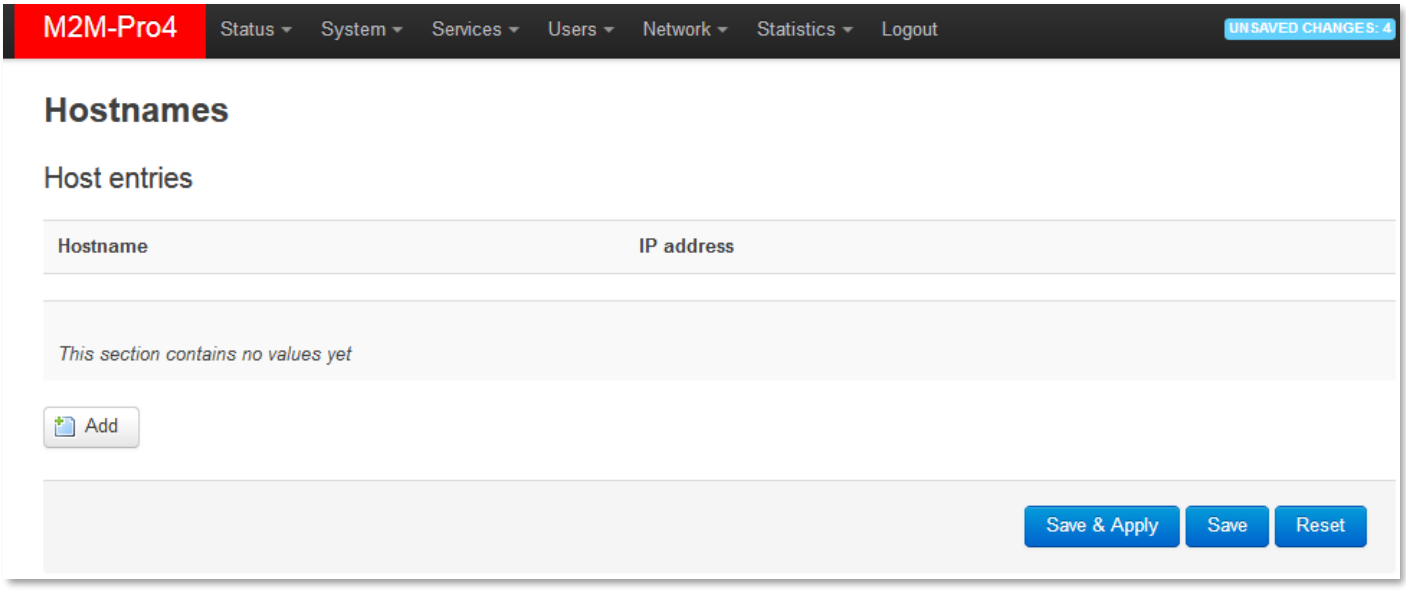


When you have modified the settings, save them by the **Save & Apply** button.

4.4 Identifiying of connecting computers

Open the **Services** menu, **Hostnames** item.

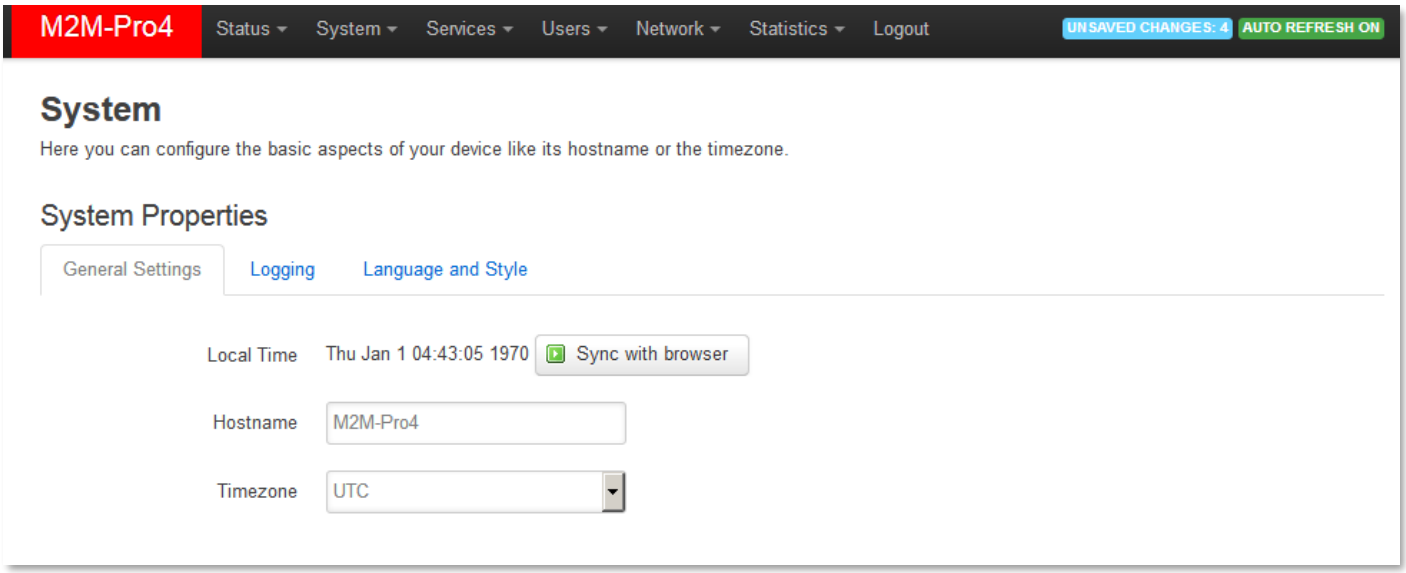
Here you can register those machines, network devices which are using the router's connection - for an easier identification.



You can  logical names to the IP addresses of the connecting machines, which you can see as listed at the **Status / Overview** menu as external connected clients.

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

The local hostname for the router (which name will appear for external devices on the network), it can be changed at the **System** / **System** menu item, where you will find the **General Settings** tab, at the **Hostname** field you can define a unique device name – to make it easy to identify the device on the network.



4.5 Serial Proxy (RS485 settings)

The device is able to receive max. 32 connected RS485 devices.

For the proper RS485 port communication settings, choose the **Network menu, Serial Proxy** menu item. Here you can define the protocol conversion parameter settings, such as receiving the incoming communication in the proper format and the transparent forwarding.

For first, the **Serial Proxy** must be **Enabled** for using RS485 communication and the R485 cabling must be connected to the external measurement device or meter, from which you want to receive or collect the data.

Configure the **Port** number, and choose the required value for the **Protocol**:

- *off*: no dataflow
- *raw*: full duplexity
- *rawlp:* one-direction communication
- *telnet:* for further usage

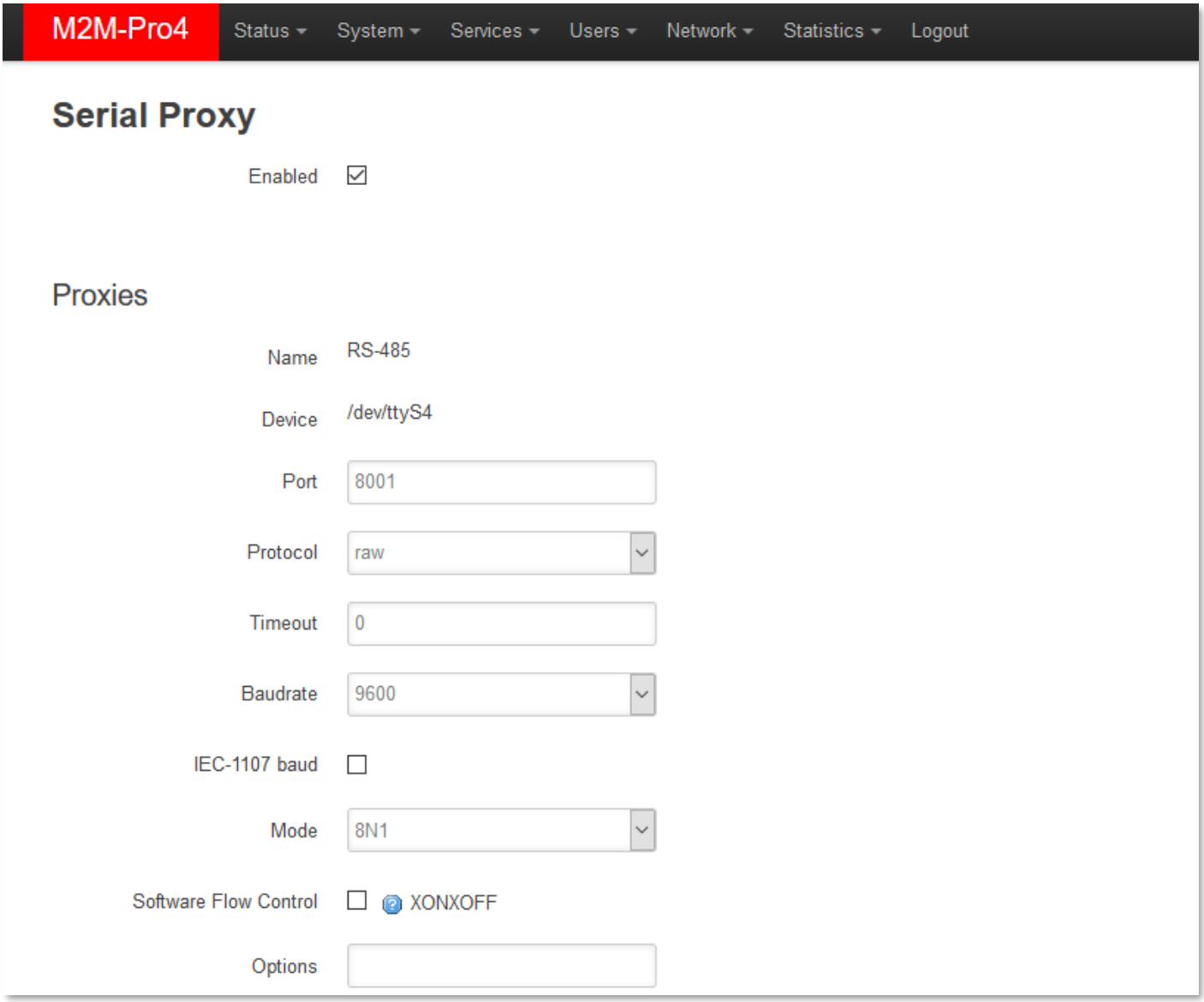
You can configure the **Timeout** value for the communication.

The **Baudrate** (default is *9600* bps, or you can use *19200* bps as standard for RS485).

At the **IEC-1107 baud** field, you can choose the IEC-meter compatible handle (data speed rate will be used according to the meter).

Configure the **Mode** value which can be *7E1* or *8N1* (which means in sequence: *Databits / Parity / Stopbits*).

You can also use **Software Flow Control**.



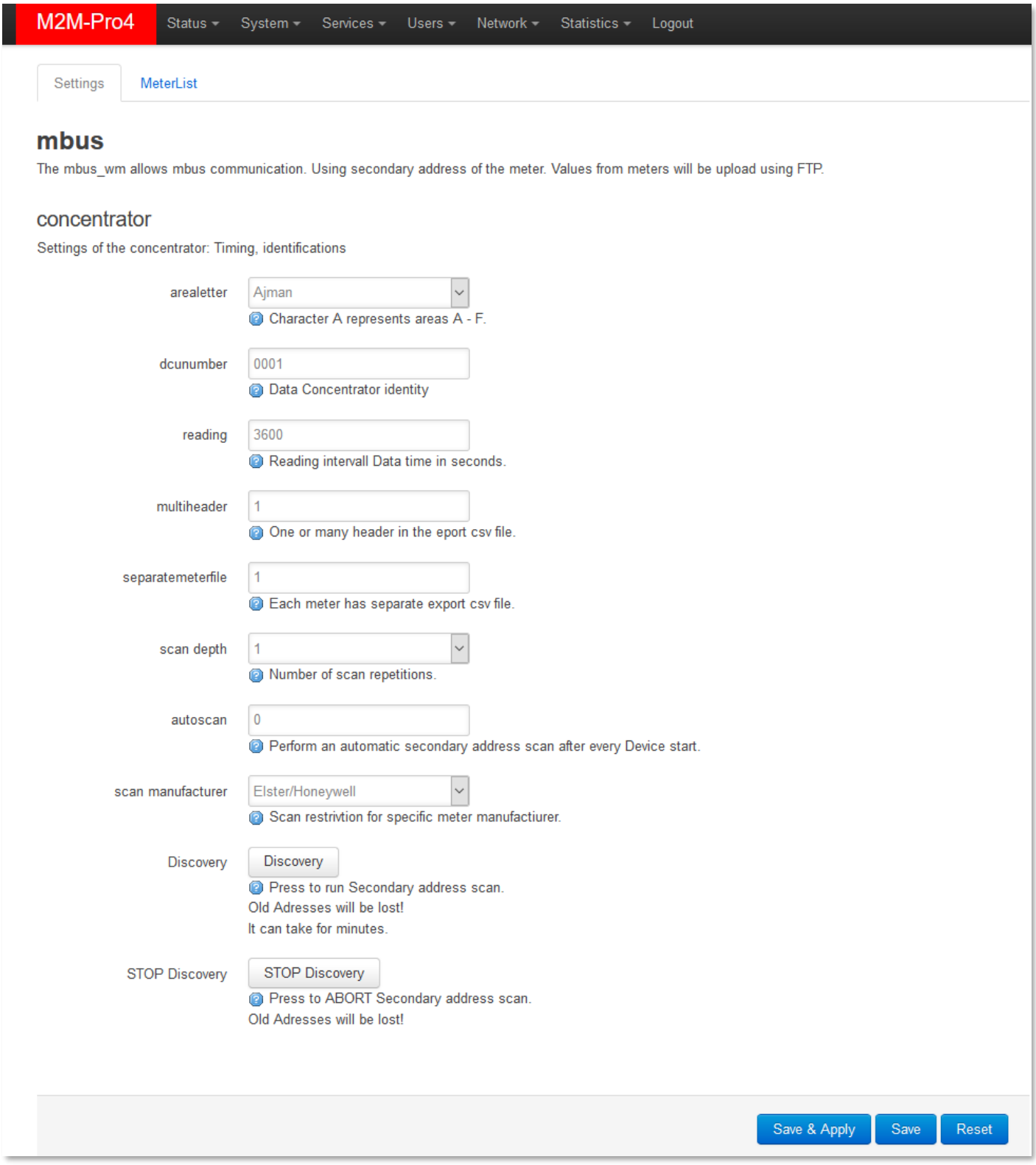
When you modified the settings, save them by the **Save & Apply** button.

Attention! Take consider, when you are attempted to change any of the **Port** numbers, then after saving your settings, you need to allow these ports at the **Firewall settings (see chapter 5.9)**.

4.6 M-Bus meter connection

The device is able to receive up to 30 connected MBus compatible meters. The data speed rate is configured for 2400 bps / 300 bps.

Check the **Services** menu, **Mbus** menu, **Settings** tab, you can define the Mbus data connection parameters.



This shown example is a basic configuration, but we can provide different fields and configuration options at **MBus settings** – according the Customer requirements. (If you have unique request, specify and send us).

At the **arealetter** parameter you can add a logical name for the identification connection.
Define the **dcunumber** for identifing the concentrator device.

The **reading** data periods can be also configured (in seconds).

The **multiheader** option (values: ***0*** (no) or ***1*** (yes)) allows you to make header after each record in the CSV file or not.

The **separatemeterfile** parameter can be ***0*** (no) or ***1*** (yes) where you can define singular or separate file structure during the sending.

The meter **scan depth** means discovery repeat if its value is ***1, 2, 3, ..*** (number of repeats) or disallow this (by ***0***). It can be used well in case of some problemous meters which cannot answer immediately.

Autoscan can be ***1*** (yes) or ***0*** (no) which means that the router will make automatic meter discovery when starting the device.

The **scan manufacturer** can be selected here to search for all meters (any manufacturer type) or by only a selected type of meters - by accordong to their manufacturing code. Select ***all*** or a defined type (e.g. ***Honeywell/Elster****, etc.*) for the discovery process.

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

Important*! In case of starting a new scanning, all current meter device entries will be updated!*

At first time the list is empty - it is normal. Now connect the meter and switch to the **Settings** tab. At the bottom of the page you will find the **Discovery** button - Push it to discover all connected meters. (You can **STOP Discovery** anytime if you need.)
At the end of the discovery process the previous list will be updated by the discovered meters.

The location of the received data

The data will be requested and incoming data of the connected M-Bus devices will be automatically stored in the temporary storage pool (**/tmp**) of the RAM drive.

Then you can ftp the data to a remote IP address (by sftp, tftp, ftp client or server).

Make a connection to upload the stored files to your distant server IP address before data loss – regarding the next setting options.

You can also use *SCP*-compatible connection to the router by your computer with an SCP client (like **WinSCP**). You can also copy the stored files to a locally mounted uSD drive for data collection or further data logging, analysis.

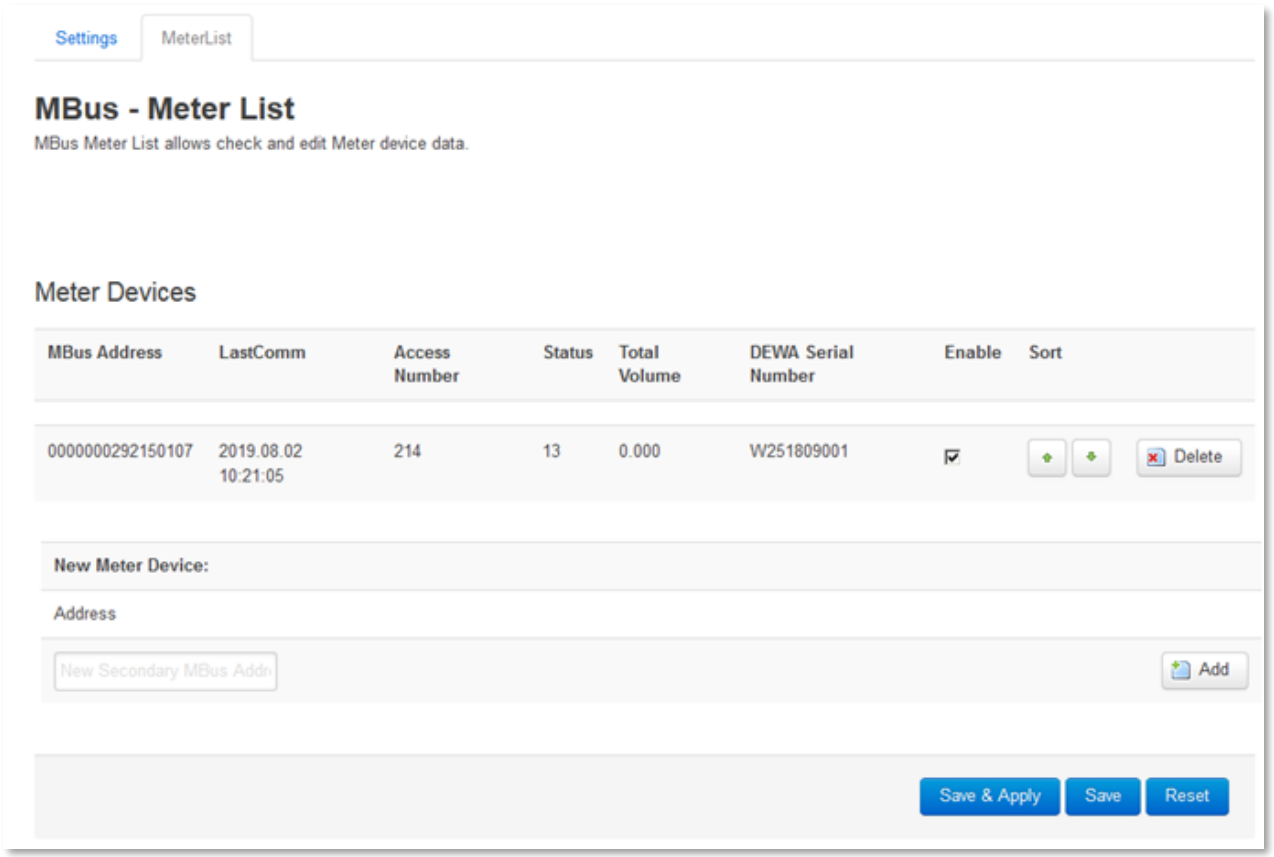
The incoming files of the Modbus devices are stored in CSV format by this syntax in CSV file(s):

- PLC address – meter PLC addres
- STATUS - OK,ERROR, etc.
- timestamp – readout datetime (YYYYMMDDhhmmss)
- *register address N – decimal address
- *register value N – raw data

**The registers are repeating until the end of the data flow*

Example: 200,OK,2019-04-29 13:17:14,7,69

Important! *Note all stored data of the* ***/tmp*** *directory will be deleted after rebooting.*



At the **MeterList** part you can see the registered and discovered MBus compatible utility meters.

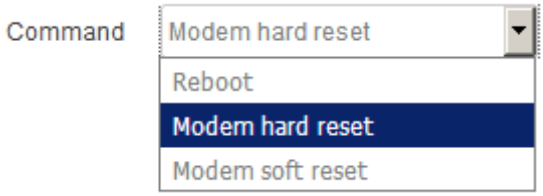
You can **Add** the connected M-Bus meters by configuring the meter parameters.
Save the configured settings by the **Save & Apply** button.

4.7 Voice Call Config

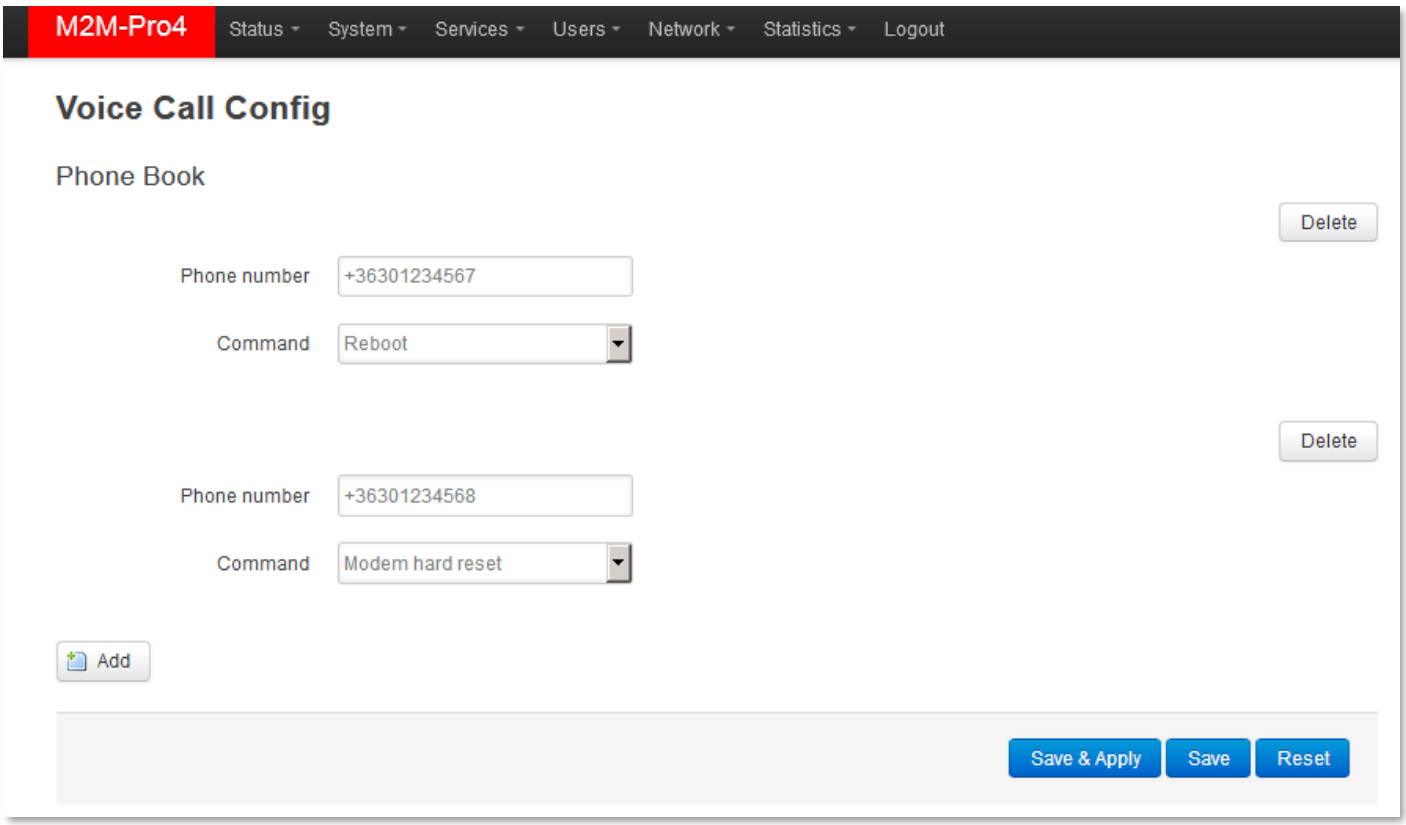
At the **Network / Voice Call Config** menu item it is possible to setup commands you are attempting remote control commands.

These are provided by remote administration and management purposes of the router in case of necessary. For answering an incoming call from the validated phone number(s), the router will be running a pre-defined command, which can be:

- **Reboot** (of the router)
- **Modem hard reset** (restart the module)
- **Modem soft reset** (quickly reinitializing the module)



You can  more phone numbers and select from the pre-defined commands to execute.



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

4.8 LED configuration

The router has 16 LEDs to assign the current operation and connection status of the device.

The **POWER INDICATION** leds and **SIGNAL STRENGTH** leds are fixed, but the further 9 LEDs are reconfigurable (**CONNECTIVITY** leds and **LAN1..LAN4** leds) in the web user interface.

The programmable LEDs has pre-defined default values (see table below), but can be free to change to other meaning/function.

For changing the LED settings, open the **System** menu, **LED Configuration** item. Here you can define the LED rules for the main important events as light/blink each LEDs.

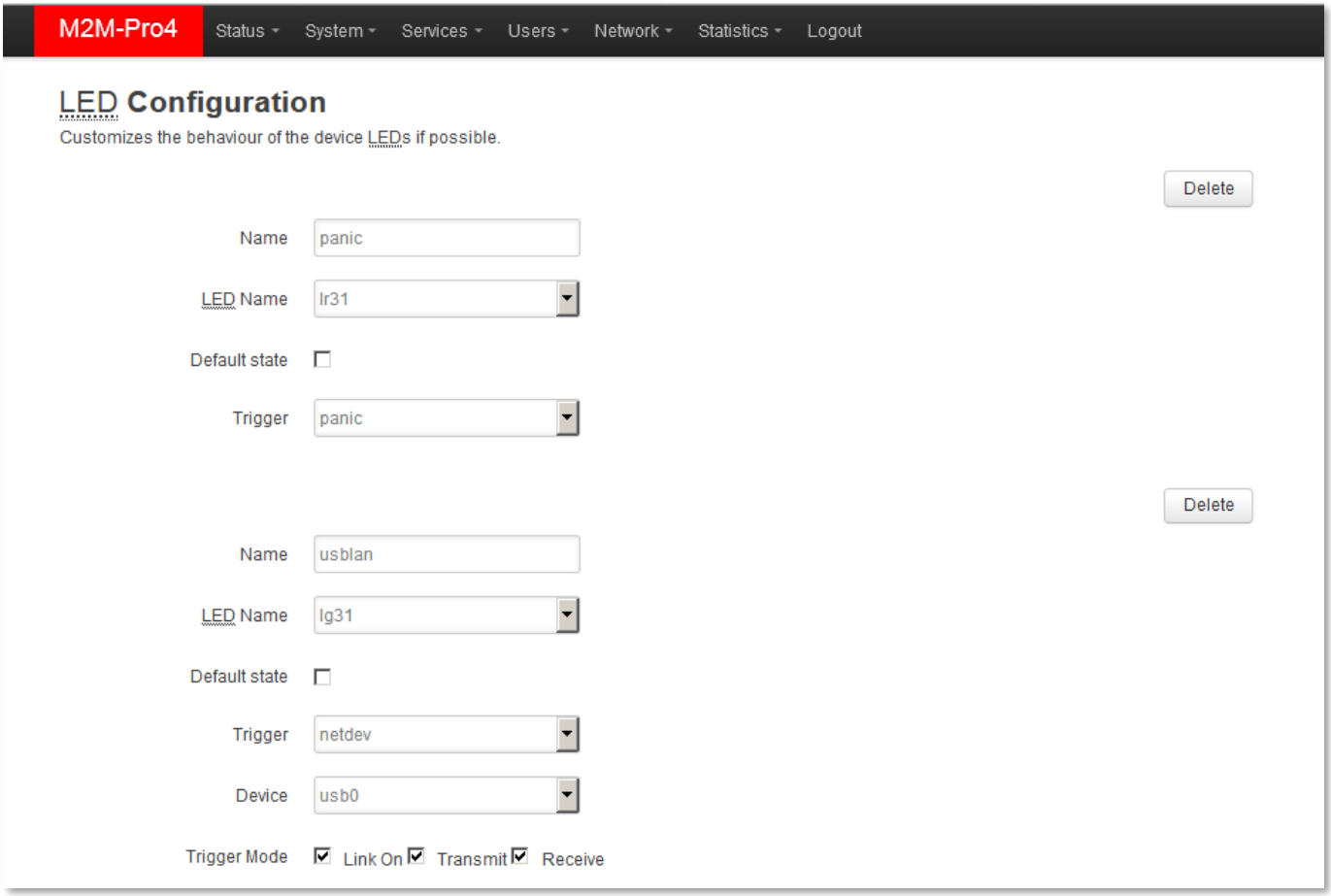
By the **Name** field add a logical name (for identifying the led) and choose a physical led for the setting by the **LED Name** field, then declare the event of operation by the **Trigger** field and the interface at the **Device** (which will be valid for). All useable possibilities are listed on the web UI.

LED operations / signals which can be changed:

CONNECTIVITY LEDs				
- ***MBus - reserved***	- ***RS485 - reserved***	**LED: lg32 (modem)** (by default: **WAN** connection)	**LED: lg31 (usblan)** (by default: **USBLAN** connection)	**LED: Lr31 (panic)** (by default: **KERNEL** (failure/panic))
		Green LED	***Green LED***	***Red LED***

LAN1..LAN4 LEDs	
LED: lg24 (**LAN1** ethernet data receive/transmit)	***Green LED***
LED: lg23 (**LAN2** ethernet data receive/transmit)	***Green LED***
LED: lg22 (**LAN3** ethernet data receive/transmit)	***Green LED***
LED: lg21 (**LAN4** ethernet data receive/transmit)	***Green LED***

Here you find the webadmin settings of the LED settings of the router.



You can Add a LED to define or Delete a LED setting from the list.

The **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. Select a **Trigger** type from list, if additional option required then additional menu will appear.

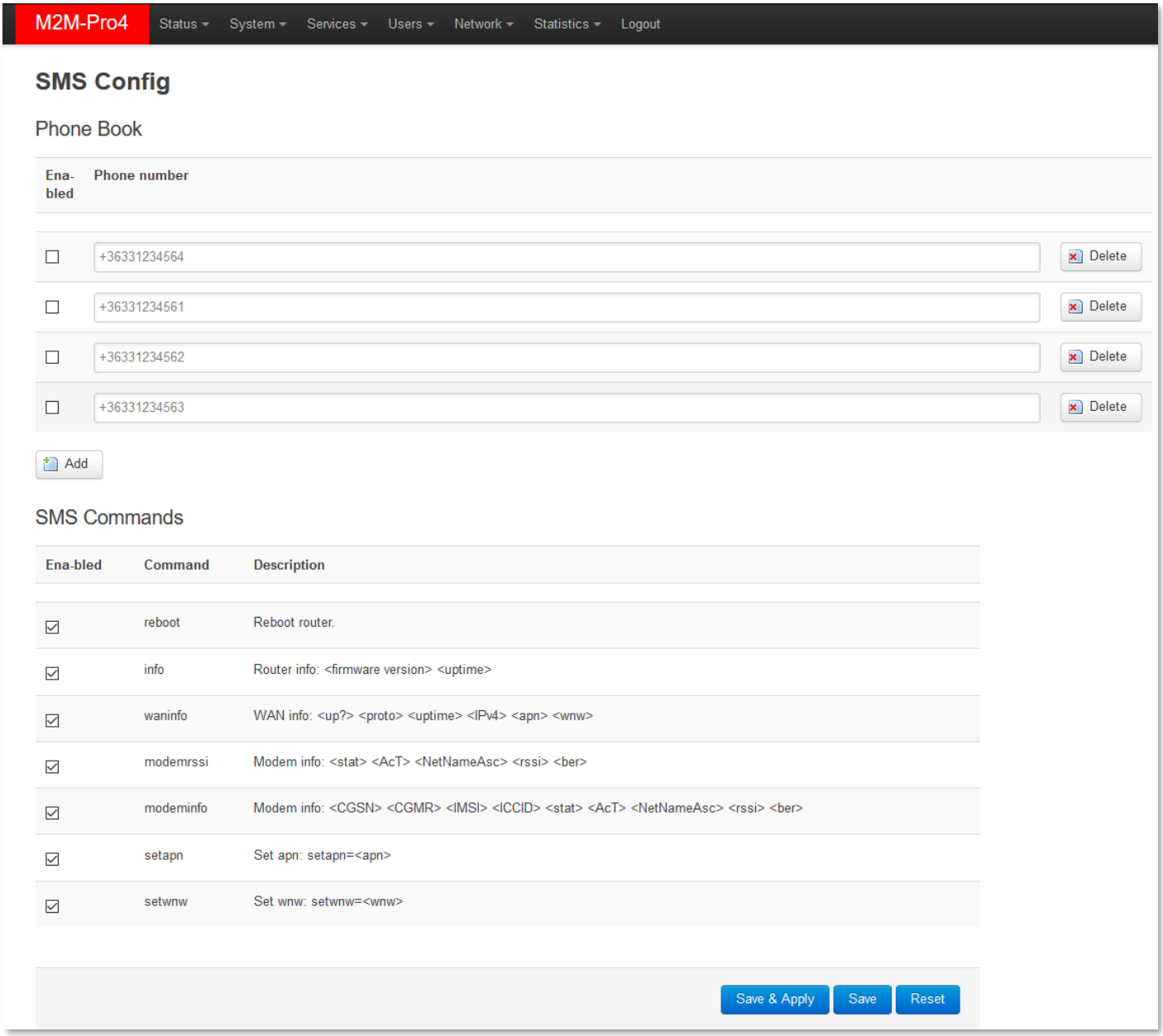
The **Trigger mode** and the **Link On** can be also defined as the Transmit (Tx) or Receive (Rx) for data flow.

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

4.9 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**

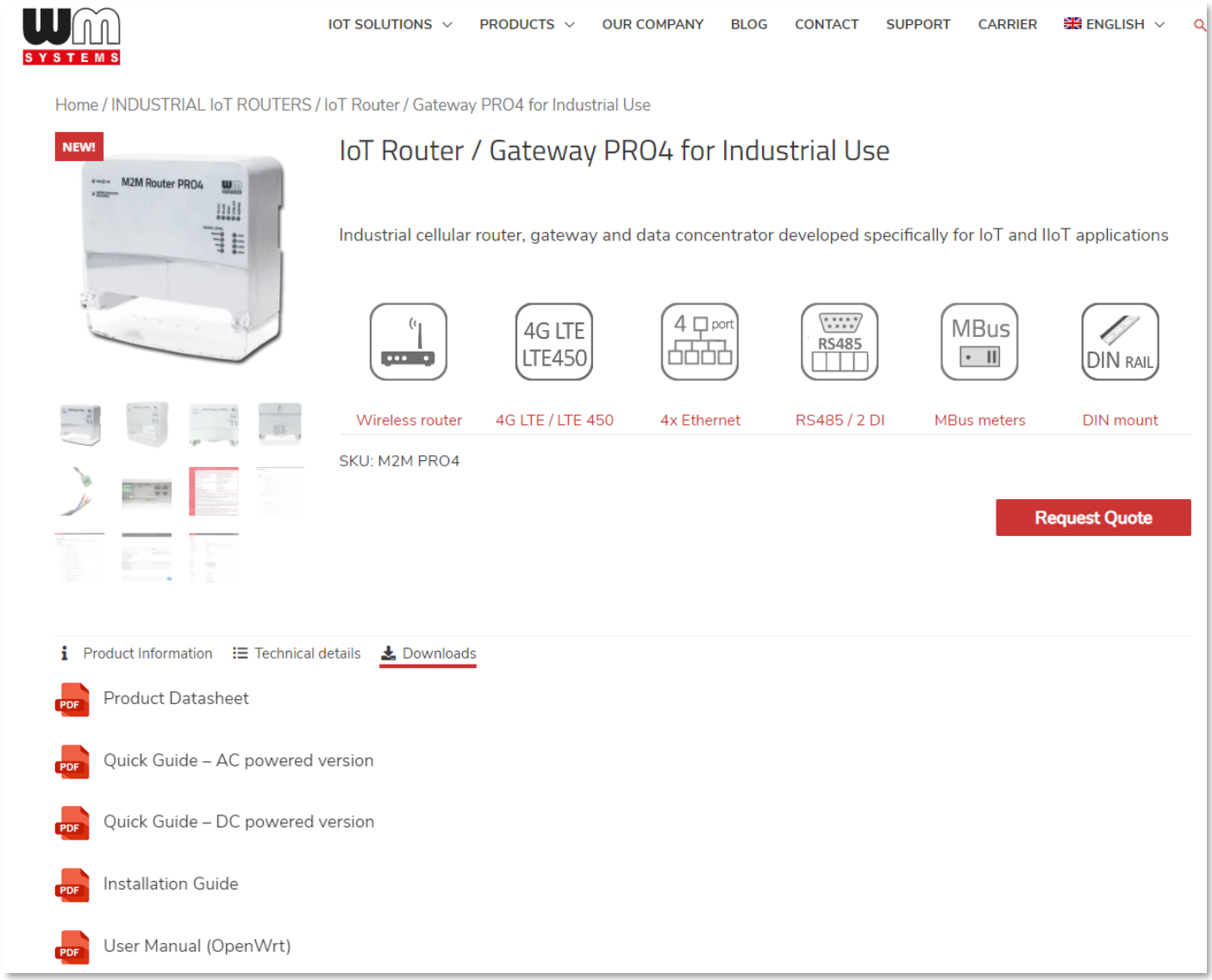
For other commands, the router returns the information in a reply SMS message (e.g. when sending the "**info**" command in SMS, the router sends the firmware version number and the elapsed time since the last boot info to the phone where the SMS has been sent).
When you have changed something, press the **Save & Apply** button to save the settings.

5. Maintenance

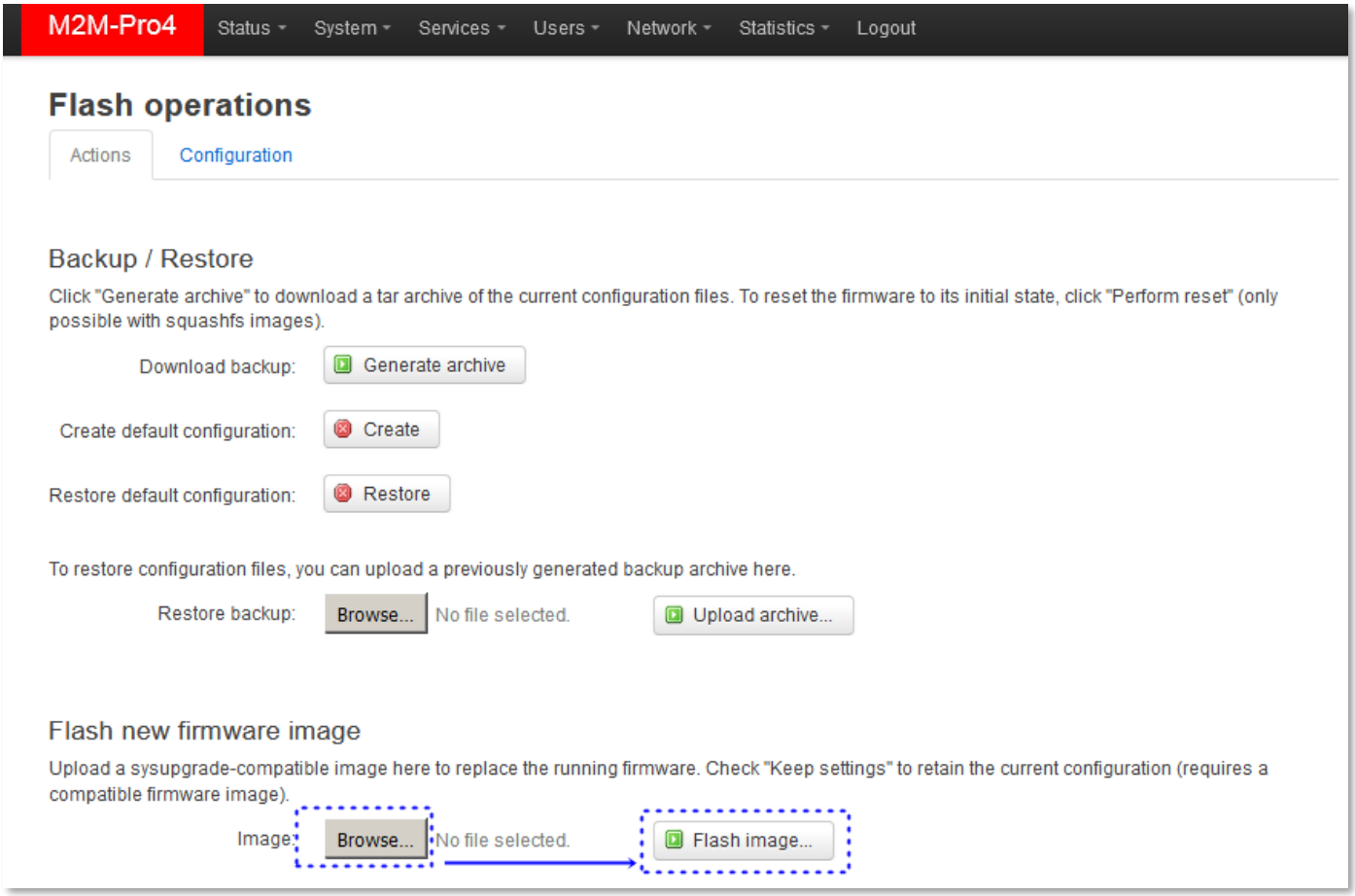
5.1 Firmware Flashing

1. Download the latest firmware from our website for the router - by using the following URL in your web browser: **https://www.m2mserver.com/en/product/m2m-router-pro4/**

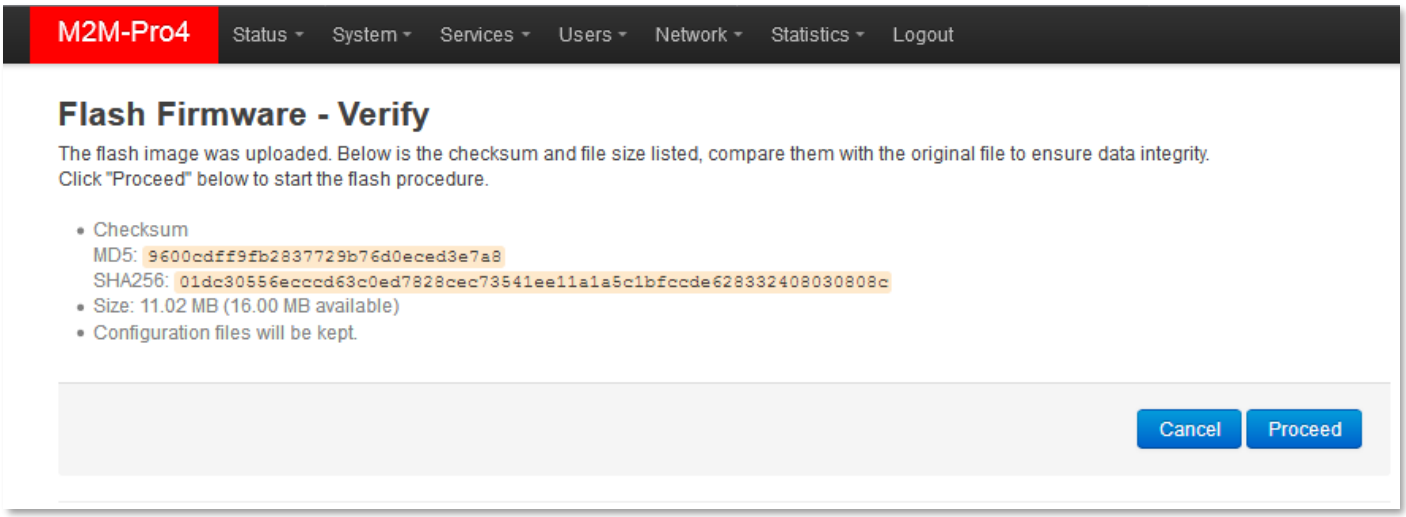
   Choose the **Downloads** tab at the middle on the router's website, then look at the **Firmware** part. **Download the file** to your computer from there.



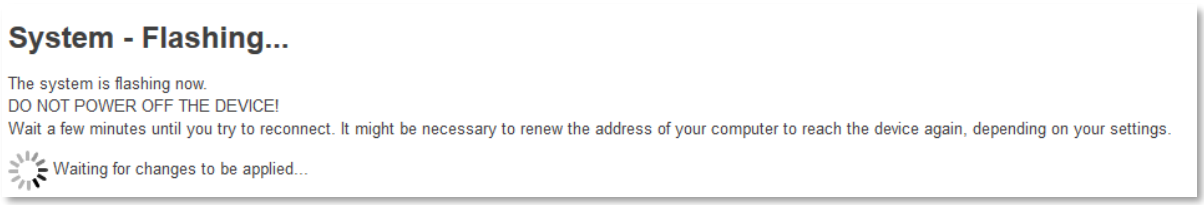
2. Open the **System** menu, **Backup / Flash Firmware** menu item.
3. At first just by safety, **backup your system** before changing the firmware version (see instructions later)
4. Push **Browse** for selecting the compressed and downloaded firmware file (***fwos-....*** file with **.zip** extension) from your computer, then push to the **Flash image** button.



5. After the compressed firmware file upload to the router, a new window will appear where the uploaded file is checked. Then you can start the system software refresh by the **Proceed** button.



6. Then another message appears on the screen in the browser, that he refresh method has been started.



7. When beginning the firmware installation, the router's LED lights will check the installation progress. During the whole installation **KERNEL** LED is continously ligthing until the finish. When the installation begins, the **USBLAN** LED is flashing then later ligthing by **green**.

8. Later the **WAN** LED is also flashing by **green** – with the **USBLAN** led.

9. Soon, the **RS485** LED will be also flashing together with the previously listed LEDs (**green**).

10. Then as sigining the progress of installation, the **MBUS** LED will also flashing by **green**.

11. When the installation has been completed, the **KERNEL** LED will be blank, but all further progress leds in the line will be **green**, which signs that the installation has been over and the router was rebooted.

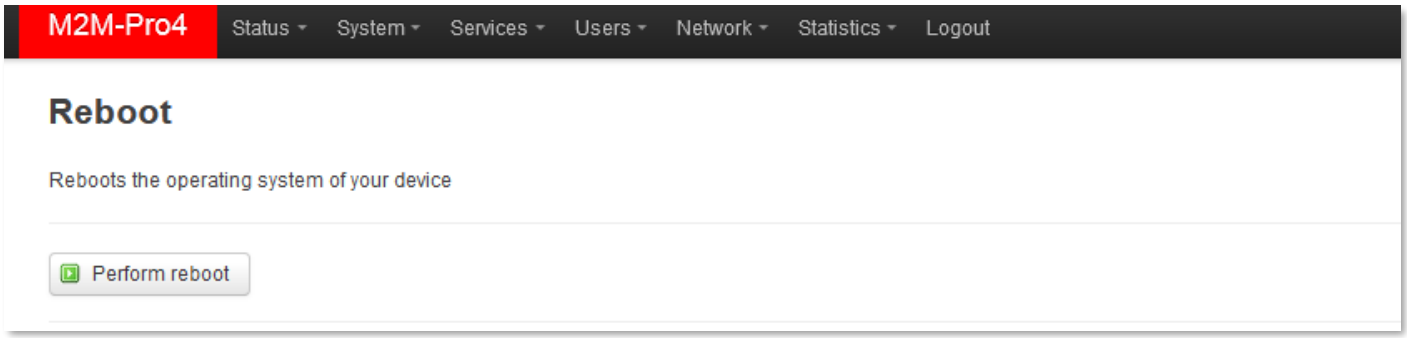
12. The router will be started as usually. After 40-50 seconds the interface signals (**CONNECTION** leds) will be active (if the **WAN** interface was already configured, then the **WAN** led will be also lighting after successful registration to the wireless network).

13. When the **CONNECTION** LEDs are active, then your **can login to the router.**

5.2 Restarting the device

Choose the **System** / **Reboot** menu item. There push the **Perform reboot** button for rebooting the router.

Then the router will be restarted, where its LED lights will assign. After 40-50 seconds it will be available again and accessible on its default address. You can login again to the web user interface.

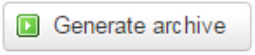


5.3 Backup device settings

The router settings are automatically stored by the OpenWrt® system, but there can be other situations when you need to restore the settings to a previously saved settings.

You can save these settings to your computer or restore to the device anytime, by following the next hints.

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

To backup your system settings into an archive file, choose a the **Backup / Restore** part, the **Download backup** and push the 

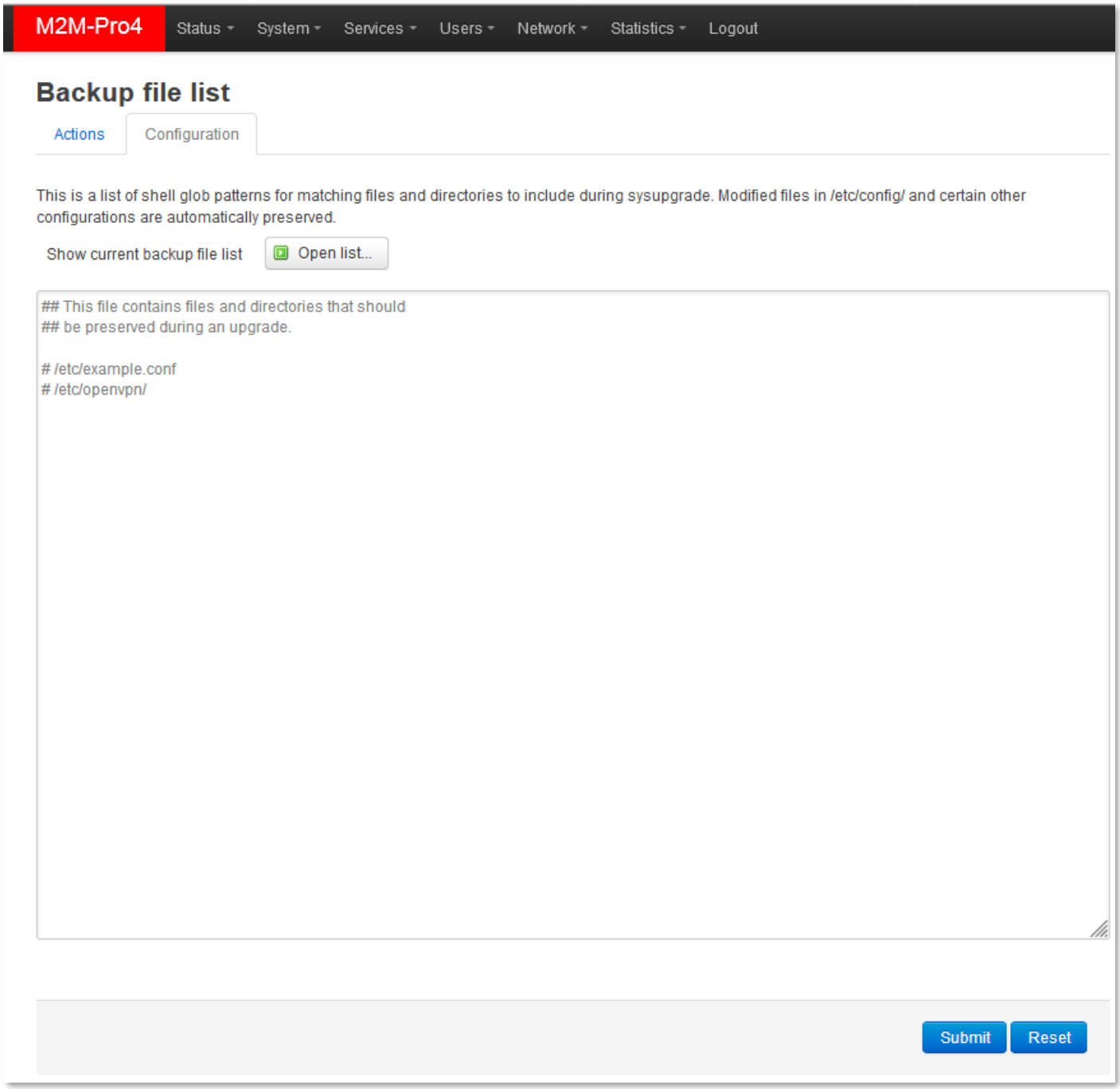
button. It is saving current settings to a compressed file to your computer (with .tar.gz extension). This is very useful during the first configurations.

A pop-up message will appear to save the archive file to your computer. **Save** the file, please.

IMPORTANT! After the next reboots, the system will always starting with these stored settings – as a new default configuration.

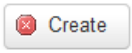
Note that the device stores only its own settings and components! If you have instakked 3rd party applications or using your own scripts, the system WILL NOT BACKUP these and these are not part of the compressed backup file! You must save all the additional files, scripts and directories manually by your own.

You can include or exclude your files and directories in your backup process by using the **Configuration** tab here. You can edit the list with all necessary directories you need.

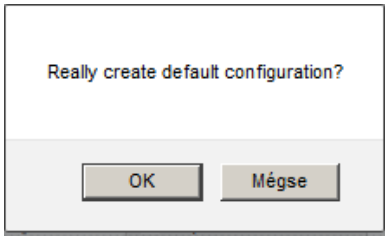


Of course, you need to know the router's file system to make it right. Therefore, we offer to check the OpenWrt® system structure, directories by standard Linux-side commands from the CLI.

When you are ready with the modifications, push the **Submit** button for the changes.

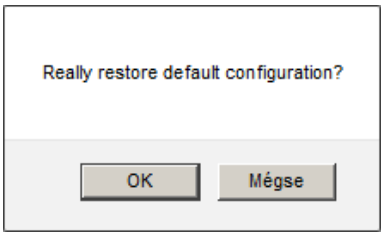
At the **Actions** tab, you can **Create default configuration** feature allows you to save the current configuration as a last known good configuration for saving by the  button.

Then the device will backup the configuration to the router. A popup window will appear, where you have to push **OK**.



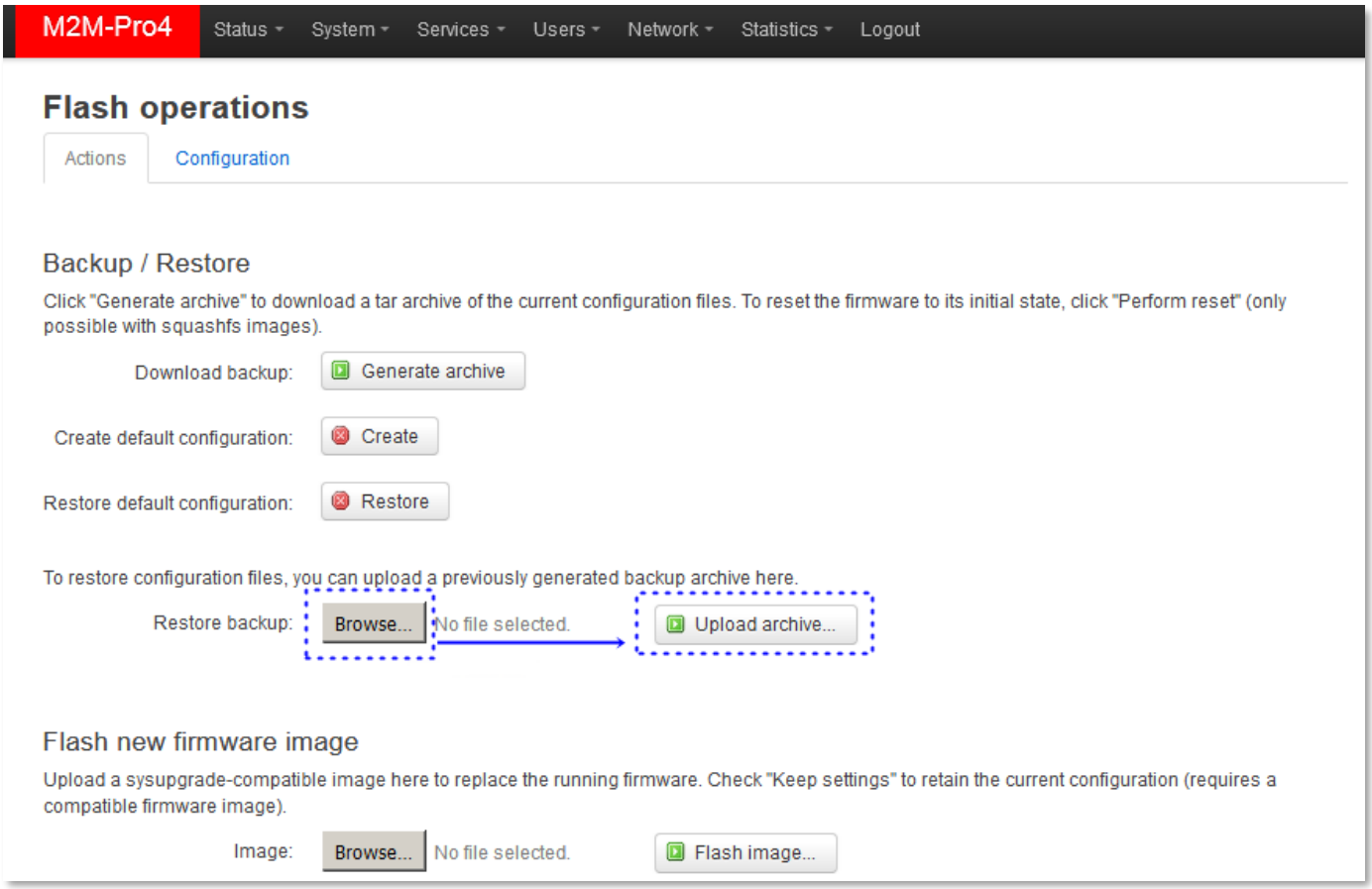
5.4 Restore the settings

You can **Restore default configuration –** your previously saved system configuration archive – as a saved last good know configuration - from your router.



For this, just push the  button if you want to restore a previously saved (factory default) configuration. A popup window will appear, where push **OK** if you want the restore the default configuration. The device uses your previous backup as valid configuration and will continue its operation regarding the stored settings.

For making a **complete restore** from your computer (.tar.gz. format) to the router, open the **System** menu, **Backup / Flash Firmware** item.



By the **Restore backup** option you can restore a previously saved system configuration archive – which was saved to your computer –to the router and apply.

Push the **Browse** button at **Restore backup** part and choose the previously saved archive file (tar.gz extension compressed file) from your computer and then push the Upload archive... button.

Then the system will reload the saved backup the saved archive file content **from your computer to the router** apply by restoring the system, then afterall the router will restart the system and applying the previously used system.

Important!

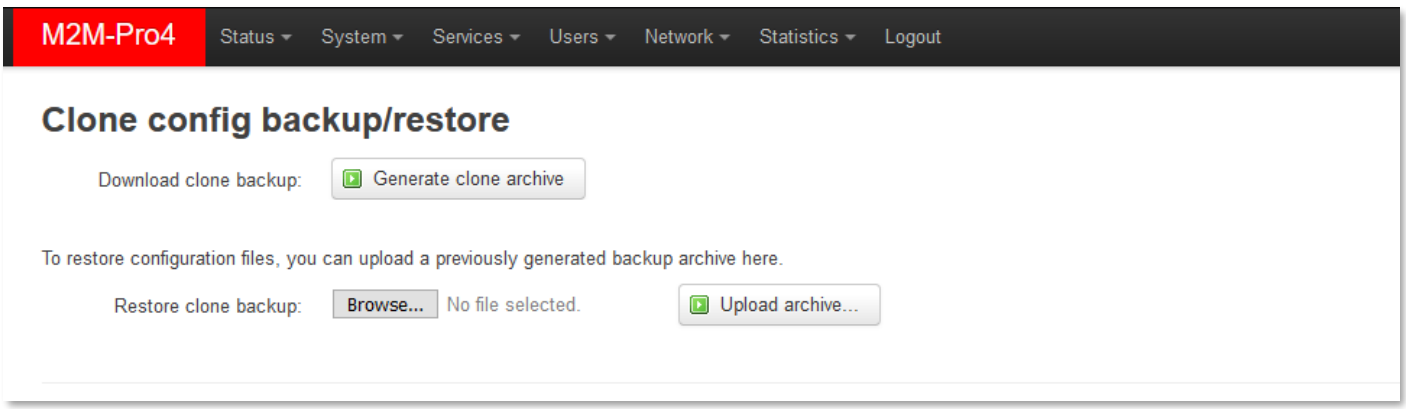
Note that your custom saved settings must be loaded seperately – it won't be restored automatically.

You can also restore the *default configuration* or the *factory configuration* of the router manually by the **Reset** button - without using the OpenWrt® web interface. For more information, please Check the *Installation Guide*, **Service Features** part.

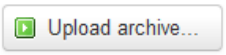
5.5 Clone configuration

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

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



In the pop-up window, **Browse** to the location where you want to save, and then save the file to your computer.

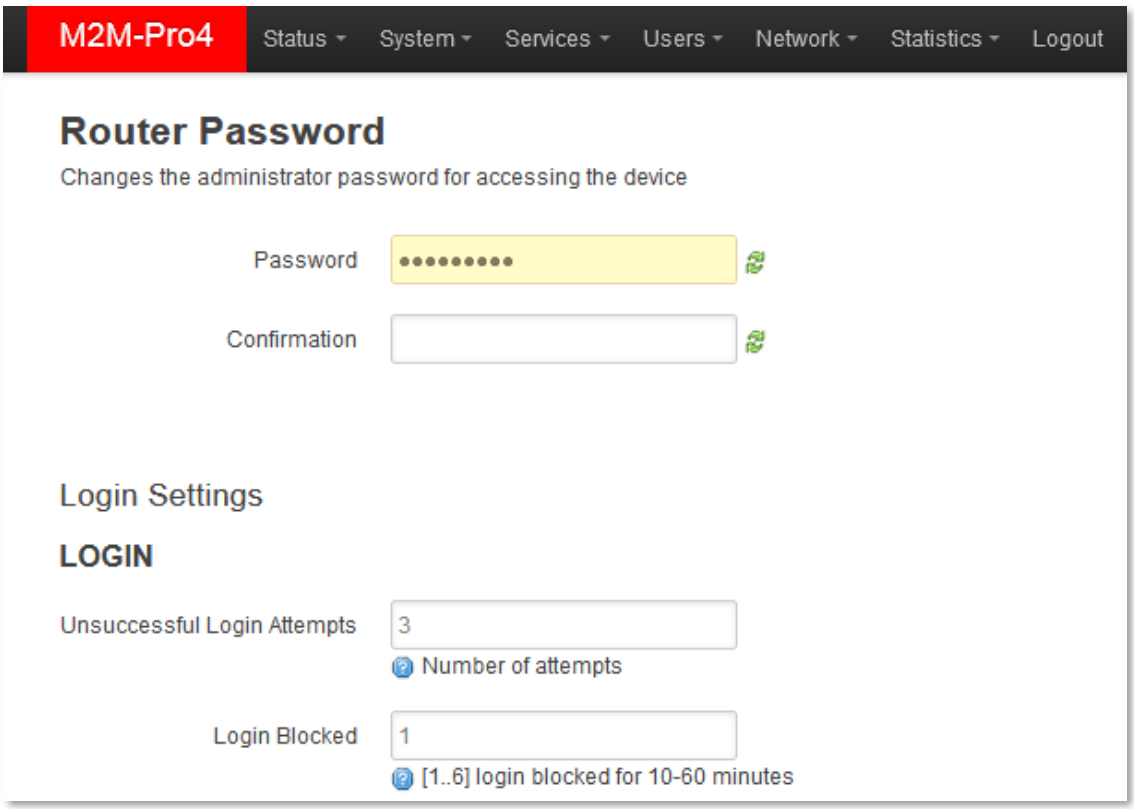
This is especially useful if you save the configured configuration to your computer and want to load it to multiple routers (as a basic configuration) - making the settings easier. What can be uploaded to other devices with the 

button after browsing.

6. Administration

6.1 Password change

Open the **System / Administration** menu.



At the **Router Password** part you can fill the **Password** and and confirm it the at the **Confirmation** field.

IMPORTANT NOTES

- The password must contain min. 8 characters, lowercase and uppercase letters and numbers or special characters are allowed.
- It is obligatory to use passwords by using minimum 3 special characters (upper case, numbers or special characters (e.g. underline)
- The currently used Password cannot be seen here due to some security rules – the characters shown as are empty here.
- When you are changing the password, the written characters will be placed by asterix signs.

You are able to limit the numbers the **Unsuccesful Login Attempts** and you can make the **Login Blocked** for a while (in 6 piece of 10 minutes-steps between 1 to 6).

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

Now, you will be able to login with the new password.

6.2 Logging

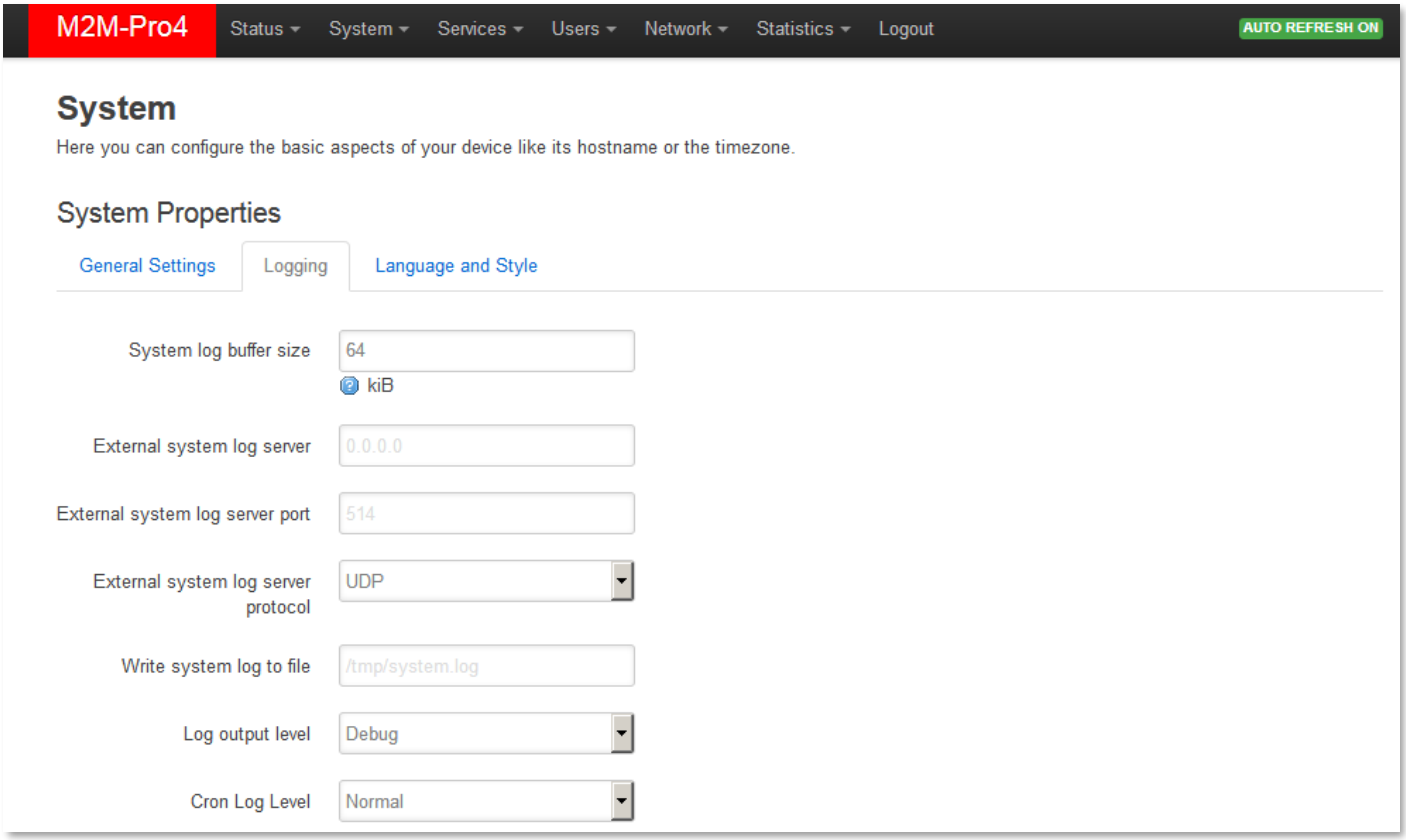
Open the **System / System** menu find the **Logging** tab.

There you can define a log file (**Write system log file**) and the level of logging (**Log output level**).

You also are able to limit the log file size (**System log buffer size**), and you can define an **External system log server** (IP address) and its **port, protocol** for sending the log files for a distant IP address.

The **Log output level** can be also defined for the added log file (**Write system log to a file**) – filename should be added with directory path.

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

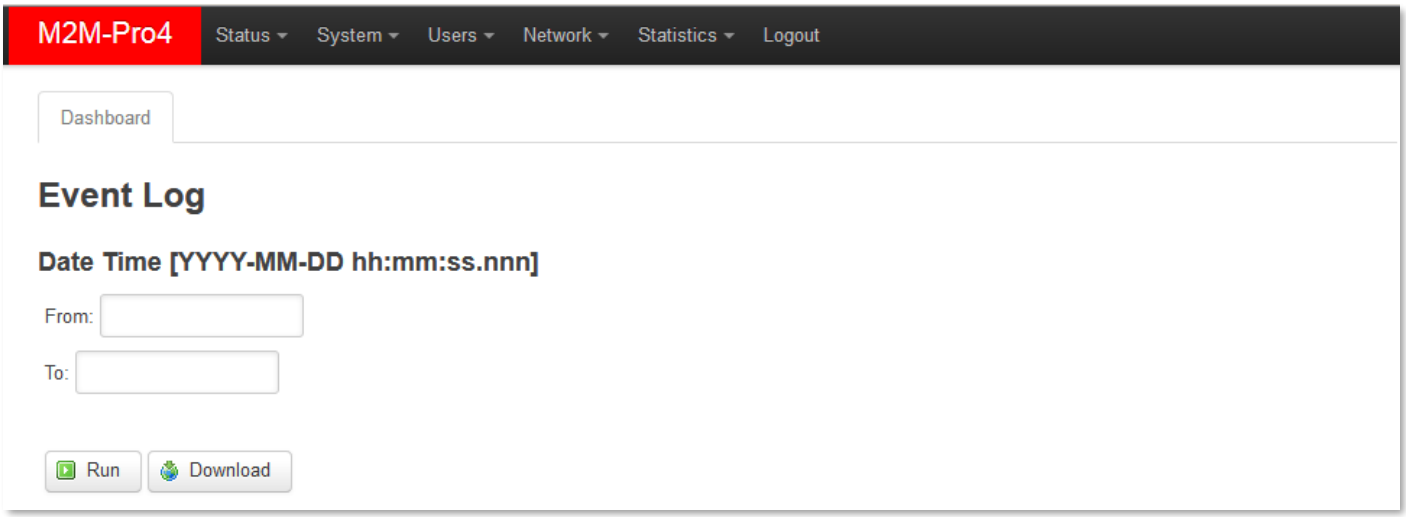


Remember that you can use further log features from the **Status** menu, where the **System log**, the **Kernel Log** helps you to understand what is happening on the router currently since its last reboot, you also can check the proper operation at these menus.

The **System / Event Log** menu item will also help you to list (**Run**) or **Download** the recorded events to your computer.

When you are checking the event log, you can define an interval for identifying the events within a period by the **From:** and **To:** parameters. (Use the date (*YYYY-MM-DD*) and time

(*hh:mm:ss*) values if you would like to filter the listing.) Sure, it's not obligatory to define the whole datetime format, you can use just years and month or else.

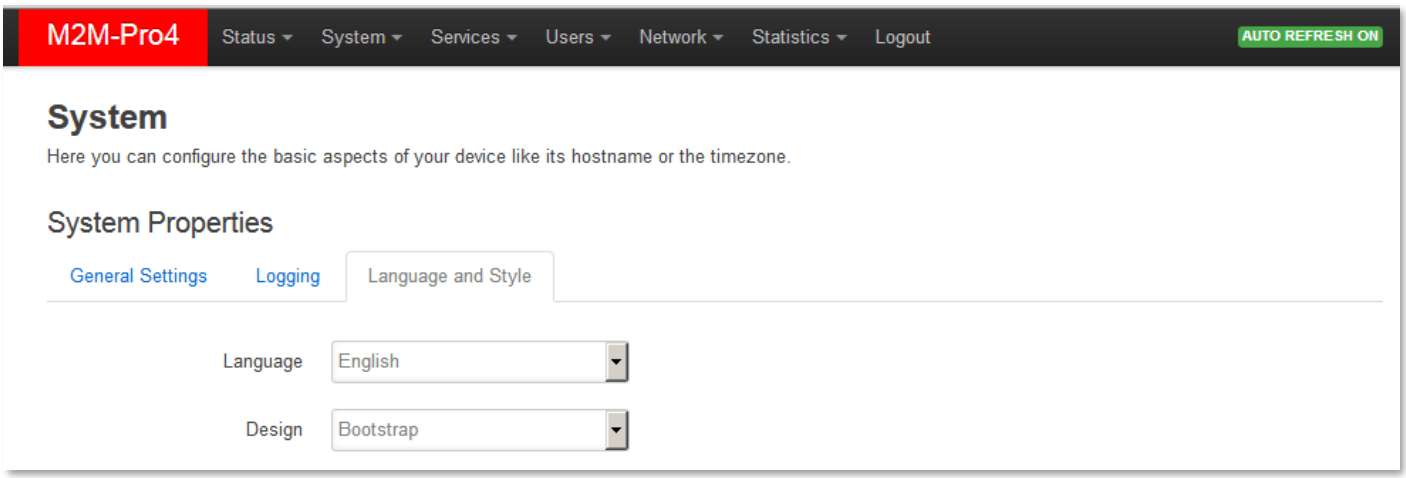


6.3 Language settings

Open the **System / System** menu find the **Language and Style** tab.

Here you can choose a pre-defined **Language** for the web user interface by selecting an item from the list.

The *Auto* preference means that the OpenWrt® UI language will be configured according to your browser language settings (e.g for English will be configured to English).



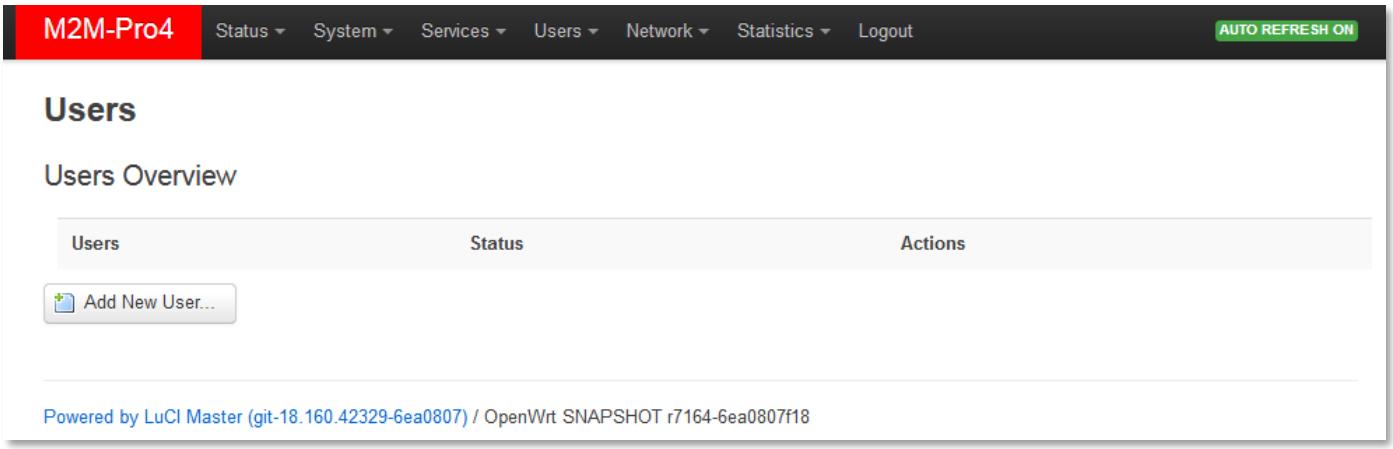
Push to the **Save & Apply** button when you have changed the language, then the new language translated texts will appear.

6.4 User management

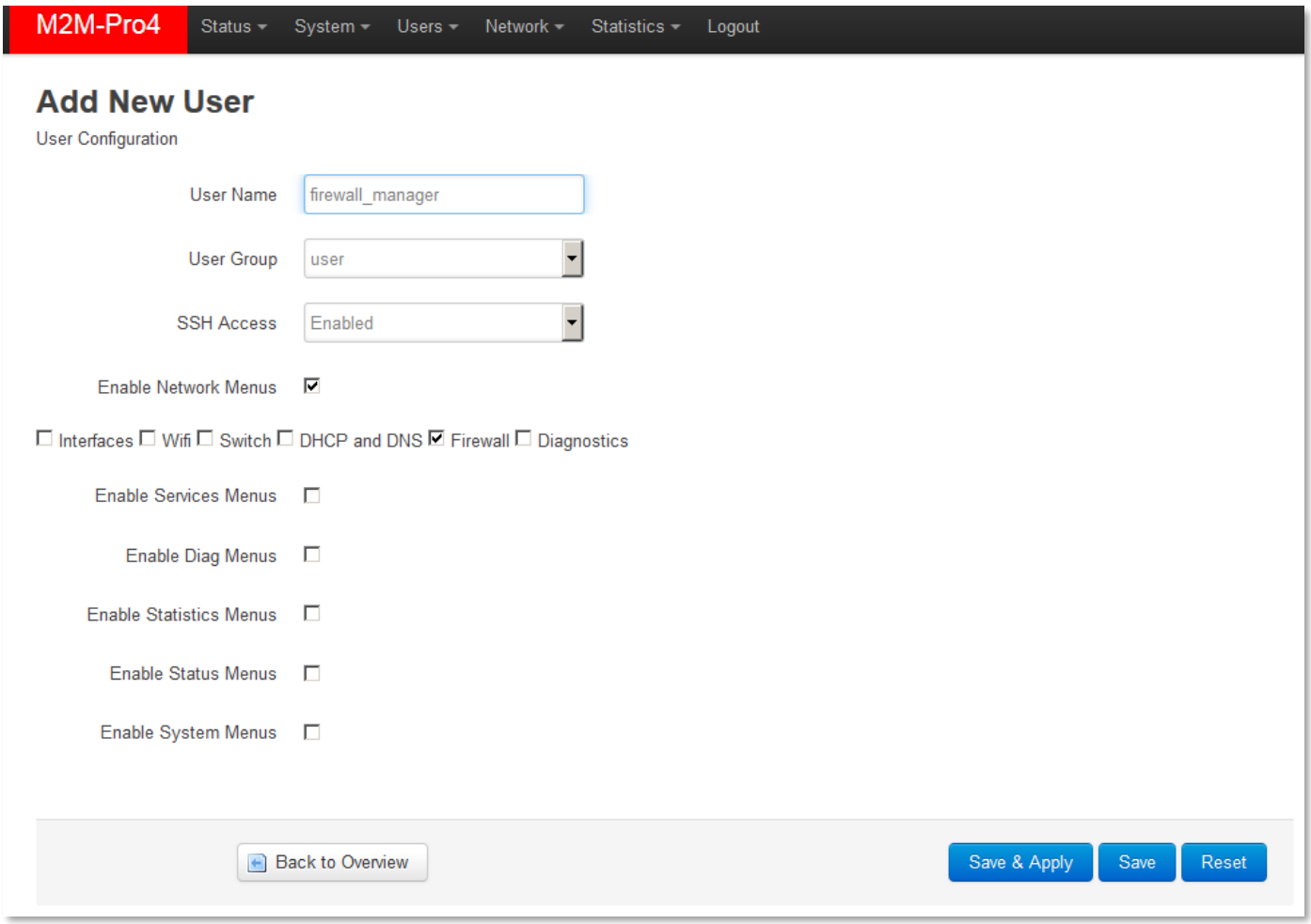
The device can handle multiply user accounts for accessing the system or the web and limit the permissions, defining roles.

This makes the router able to providing a multi-user capable environment, which is supporting the workgroups, to execute tasks for the users (e.g. administrator role, installer, maintanence group, riport maker roles, etc.).

Choose the **Users** menu / **Edit Users** menu item for the user settings.



Here you can **Add New User** by its button. Then a new window will appear.



Define **User Name** and select a **User Group** for the permission / entry-level.

Then choose the required ***Menu*** items by *enabling* the related checkboxes to provide the required menus for the role of the user account.

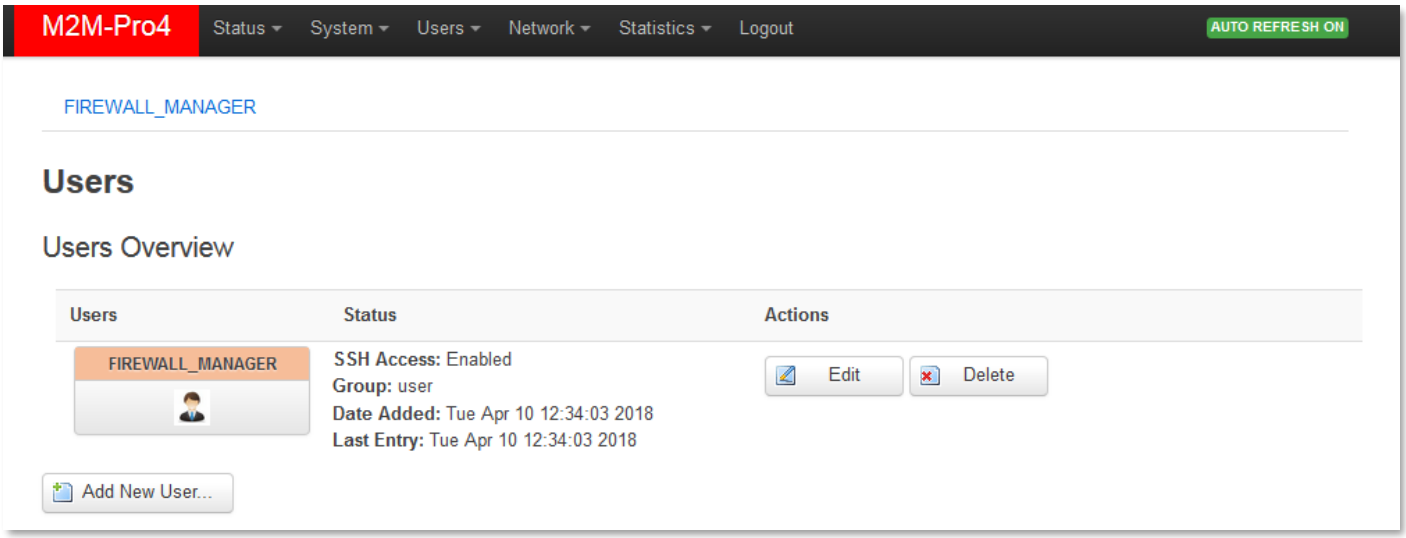
Then, the selectable sub-menus will be appearing, where you can grant a more detailed permission for the menu items by selecting the sub-items.

Certainly, only the configured menu items and permissions will be valid for the configured user account.

You can also grant ***SSH*** access permission to the account.

When you have finished, push to the **Save & Apply** button for saving the new account settings.

Now, as you can see, the new user account is listed. Here you can Edit the settings of the user account or Delete this account from the system.

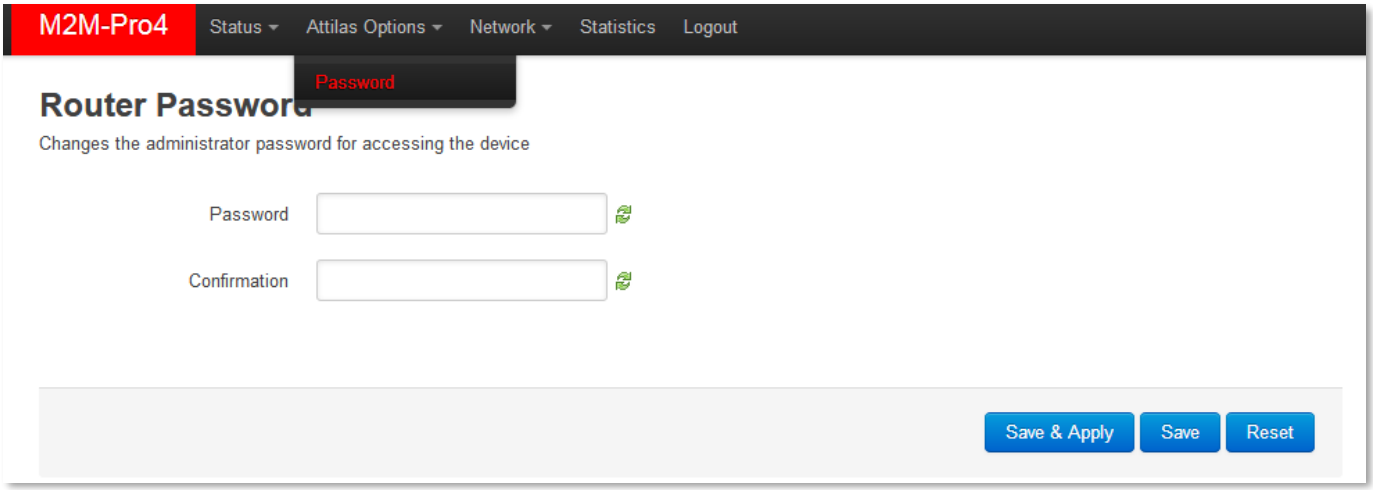


Then, after **Logout** from the system, a new user can **Login** with his account and able to access the allowed menus, features by the pre-defined roles.

Note that the **default password** for all manually added users is the following: ***wmrpwdM2M***

After, you have will login by the new user login there will be a new menu item, the ***User Options***, with a **Password** menu item.

There you can change the user **Password** for unique one. Do the **Confirmation** and **Save & Apply** your settings.



Important!

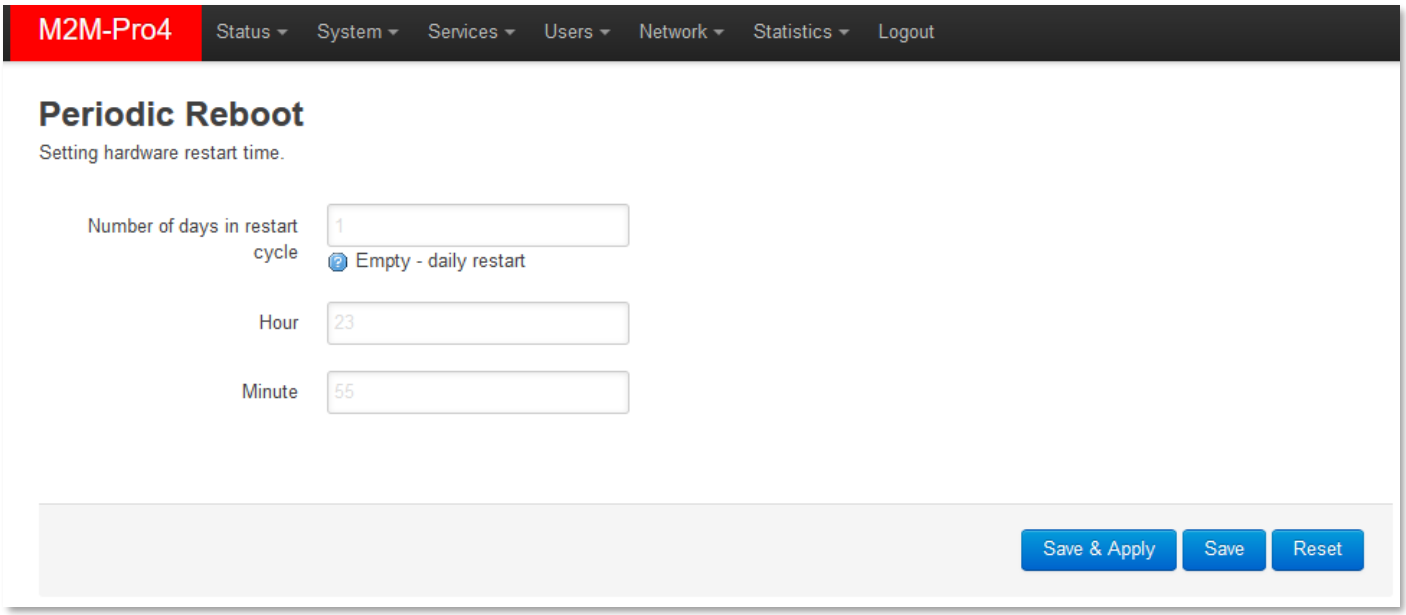
The password must contain min. 8 characters, lowercase and uppercase letters and numbers or special characters are allowed.

It is obligatory to use passwords by using minimum 3 special characters (upper case, numbers or special characters (e.g. numbers)).

Note, that the current **Password** cannot be seen here due to some security rules – the characters shown as are empty here. When you are changing the password, the written characters will be placed by asterix signs.

6.5 Periodic ping and reboot

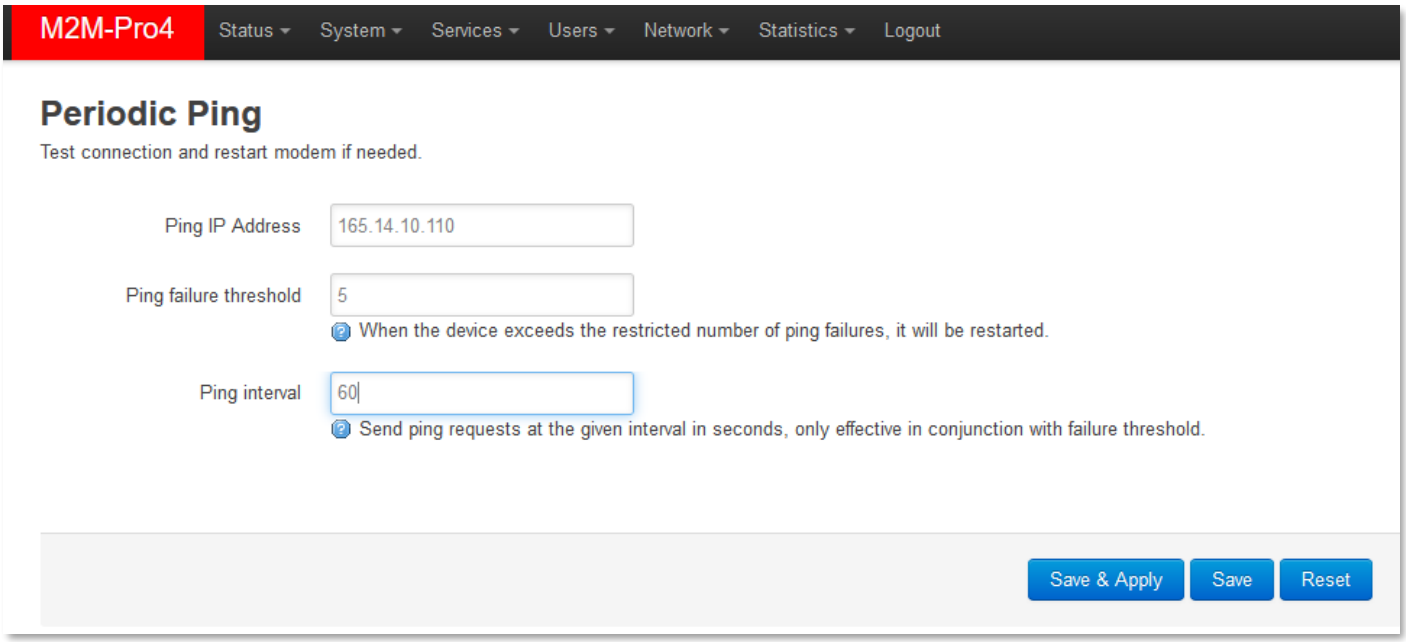
For matching the industrial standard requirements, you can define an time interval for periodic daily restart of the device if you want in the **Services** menu / **Periodic Reboot** item.



At the **Day** value, you can define how many days of period will be applied to the modem reboot. E.g. Day=2 means reboot on every second day at the **Hour**/**Minute** defined time.

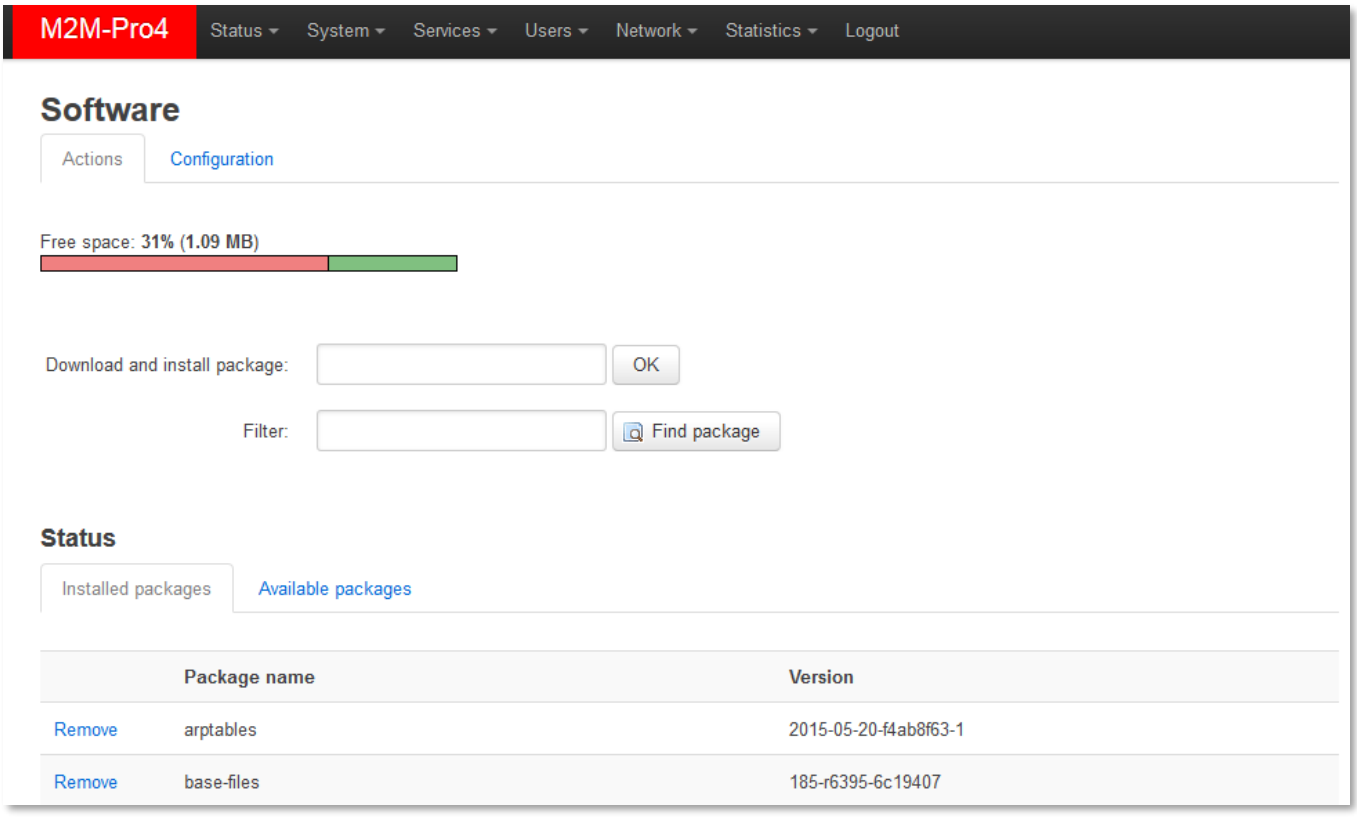
If you want to use periodic ping as checking an IP address or remote server, device as checking its availability by the device if you want to use this service by accessing from the **Services** menu / **Periodic Ping** item.

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



6.6 Installing 3rd party applications

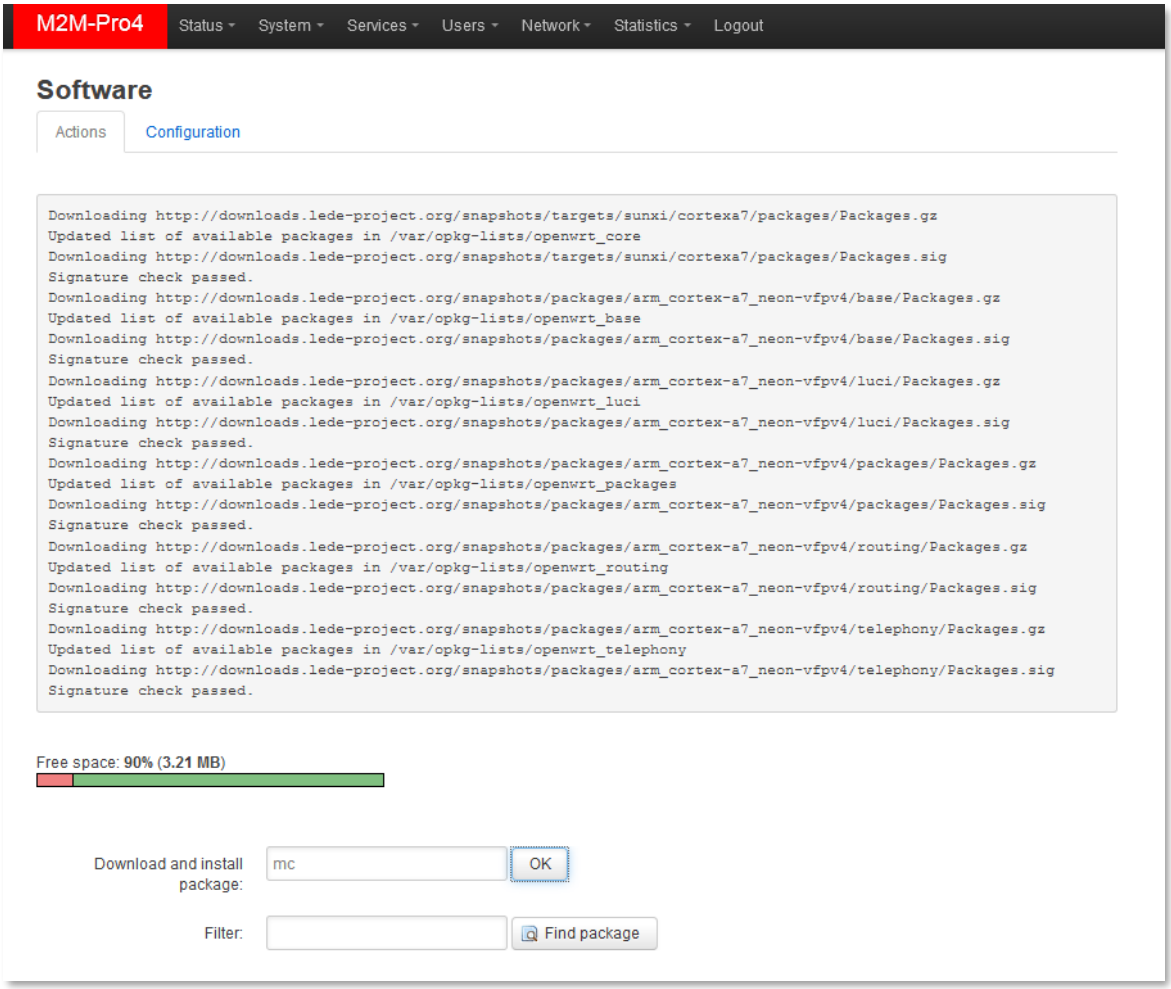
Open the **System** menu / **Software** menu item, find the **Actions** tab.



The installed packages are listed at the **Installed** tab by its **Version**.

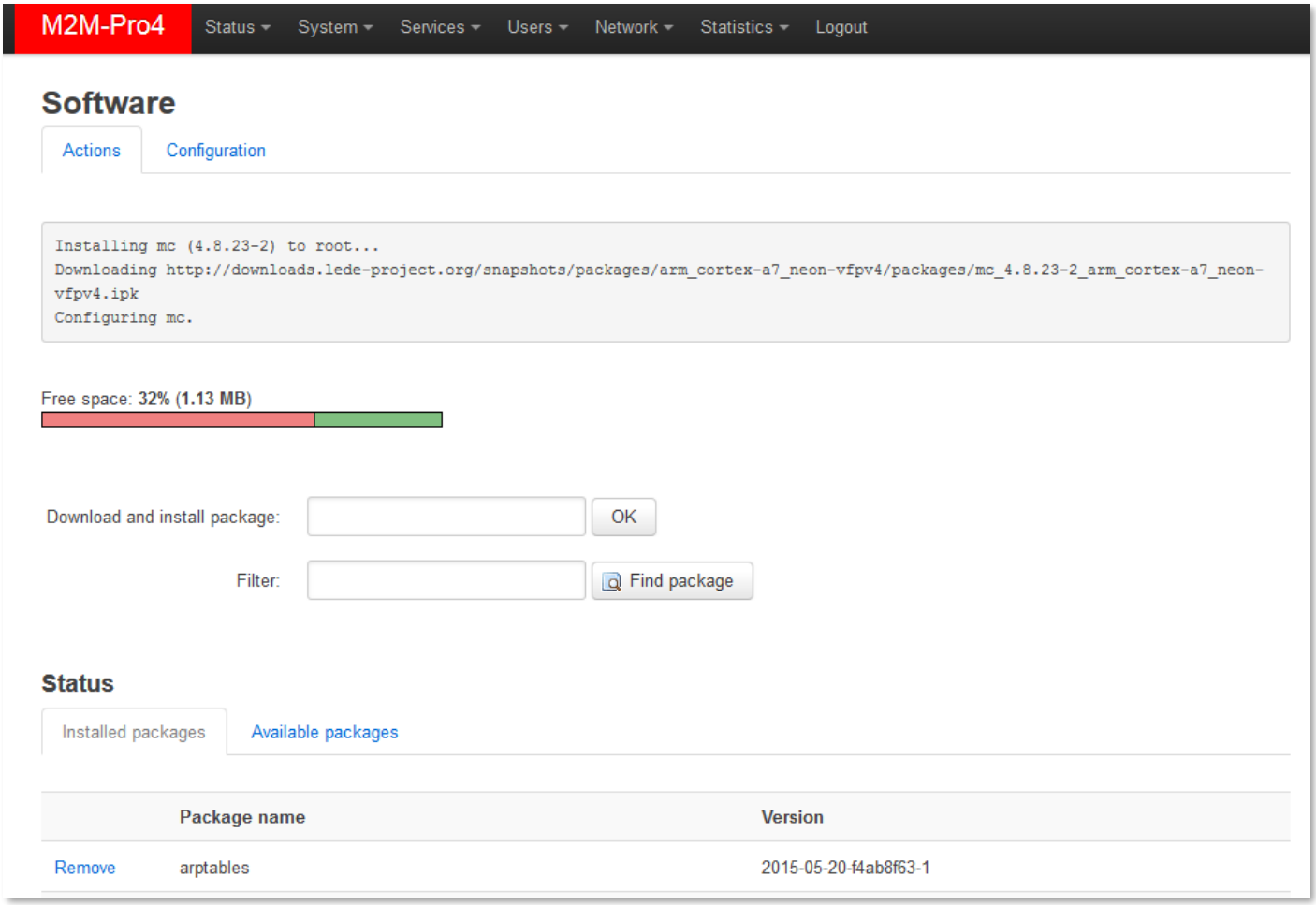
To download the software catalog, first you have to push to the Update lists button, when the **configured opkg** list will be downloaded from the repository with the list of the available applications.

> ***Important!***
> *This feature is available only, when the public Internet is accessable by the SIM card and the used APN.*



Then enter the name of the application, which you are attempted to install to the **Download and install package** field (e.g. *MC* – which means the Midnight Commander application) if you are exactly sure about the filename.

If you want to select the file, then use the **Filter** field and enter the program name you are searching for.



Then the list of the application with the name will be listed. Choose the package you want and choose the installation option.

After the installation of the selected package, now you can use the installed Linux application / component which you were chosen.

Now you can use the installed Linux application / component which you were installed. Open SSH terminal window to configure your new application or use it. E.g. about our example, enter the „mc" to start the *Midnight Commander* tool which you were installed from the repository.

6.7 Mount points

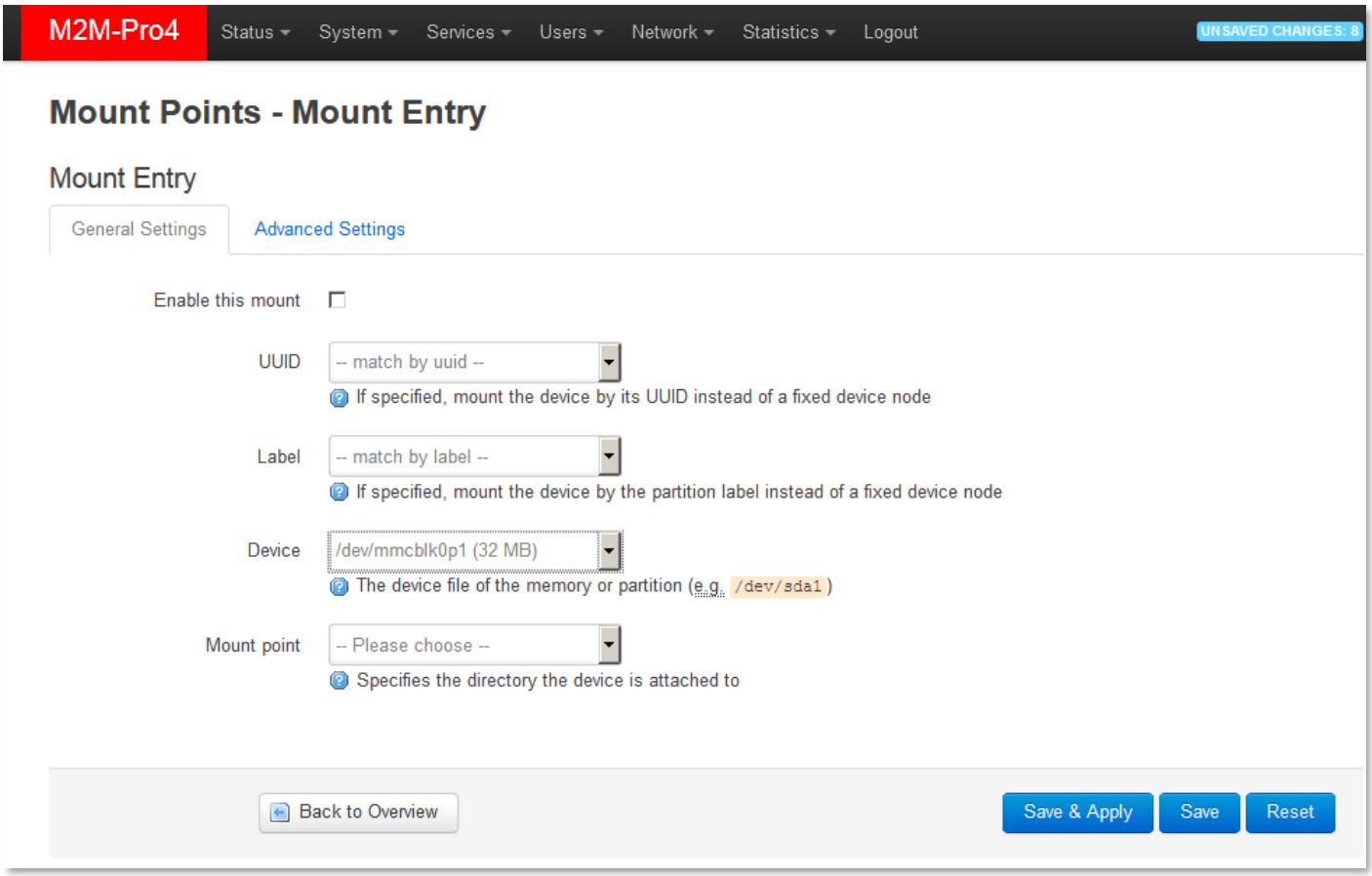
The device is handling the connected and mounted file systems of the uSD card, connected USB devices and the internal Flash. Choose the **System** menu / **Mount Poins** menu item.

There at the **Global Settings** part, you can configure the *Mount* and *Swap* areas.

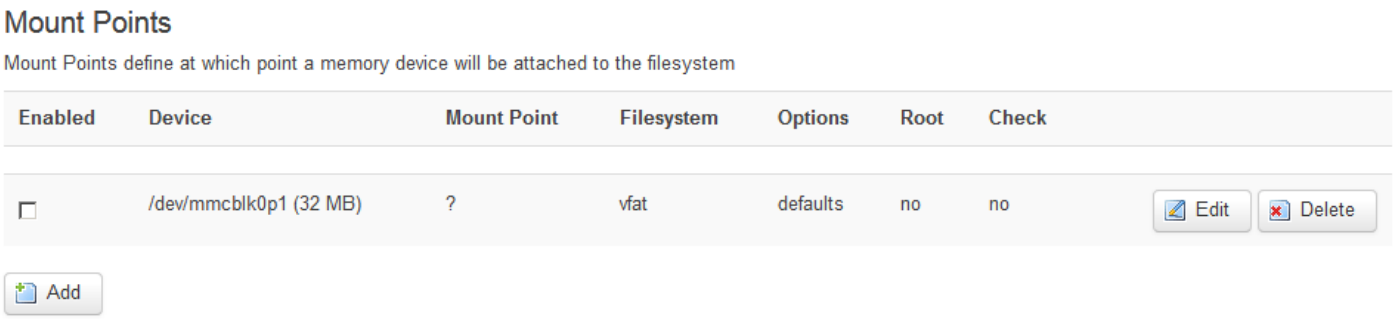
The **Mounted file systems** are listed the connected and mounted devices (such as uSD card, connected USB pendrives, hard disks, USB and internal Flash). These file systems will be attached under the */mnt* directory in SSH.
Certainly, only the formatted and partitioned filesystems can be seen here.

Here you can Edit the settings of a device (media) or Delete a device from the list. You can also Add new mount points here.

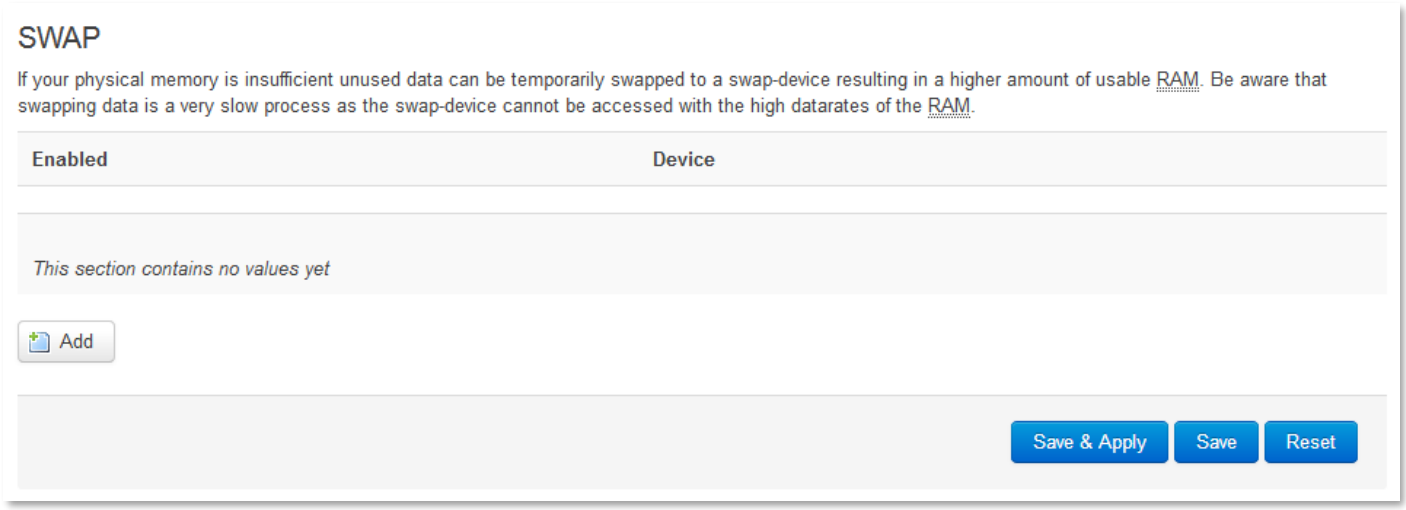
To add an inserted uSD card choose the Add button and choose the **Device** (*/dev/sda1* as */dev/mmcblk0p1* for uSD card) and push to the **Save & Apply** button.



Then push the Back to Overview button for the device listing. Now the mounted uSD card is listed here.



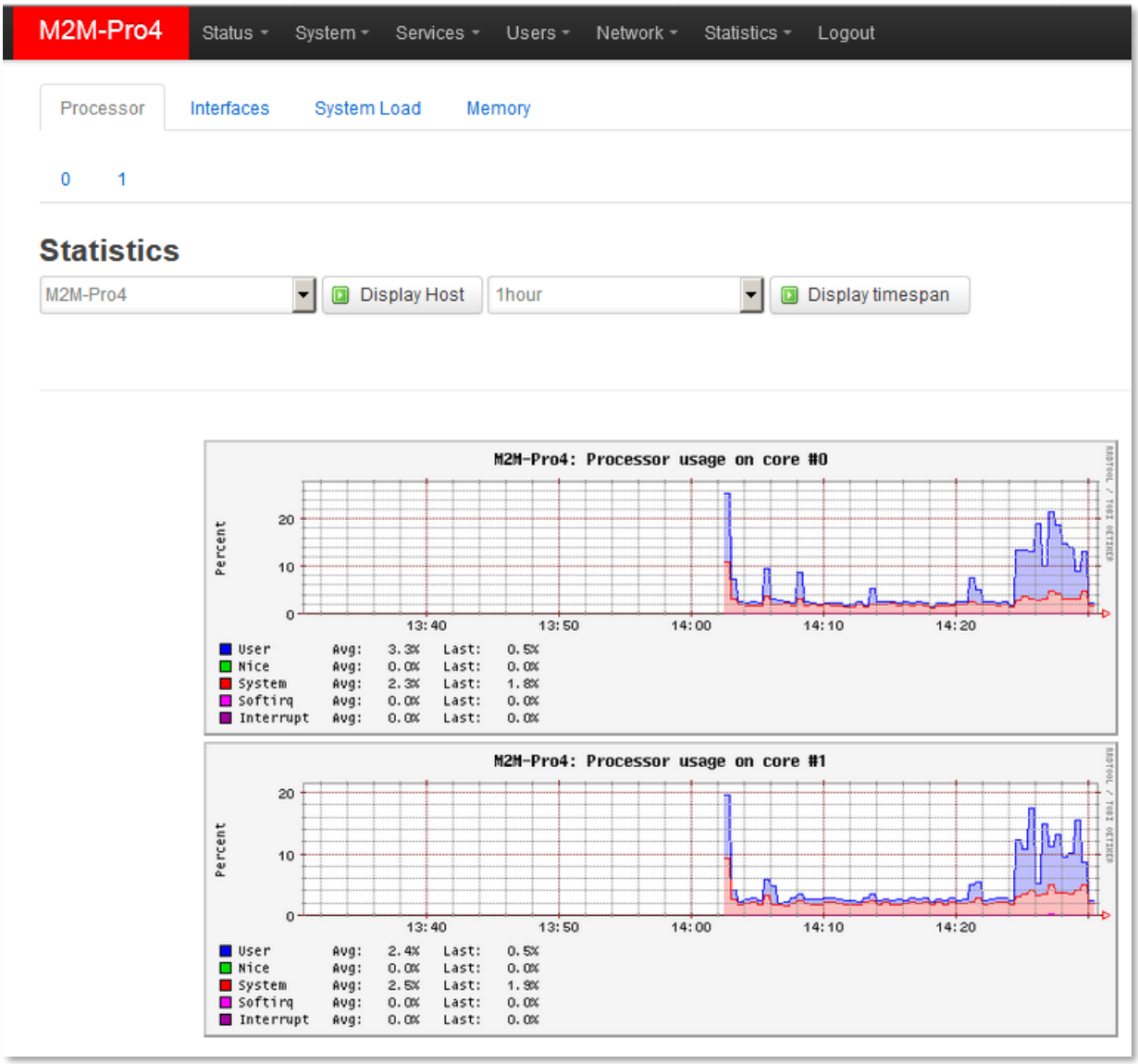
At the bottom of the screen you can define **SWAP** area for the system. It is suitable for temporary files and speed-up the file-system handling. This can be necessary when you are using a massive amount of memory and for some 3rd party applications.



6.8 Statistics

6.8.1 View the statistics reports

In the **Statistics** menu / **Graphs** menu item, you can see the current and archive statistic graphs of the router's perfomance.



Choose a tab (**Processor**, **Interface**, **System Load**, **Memory**) to check the stored QoS /resource statistics.

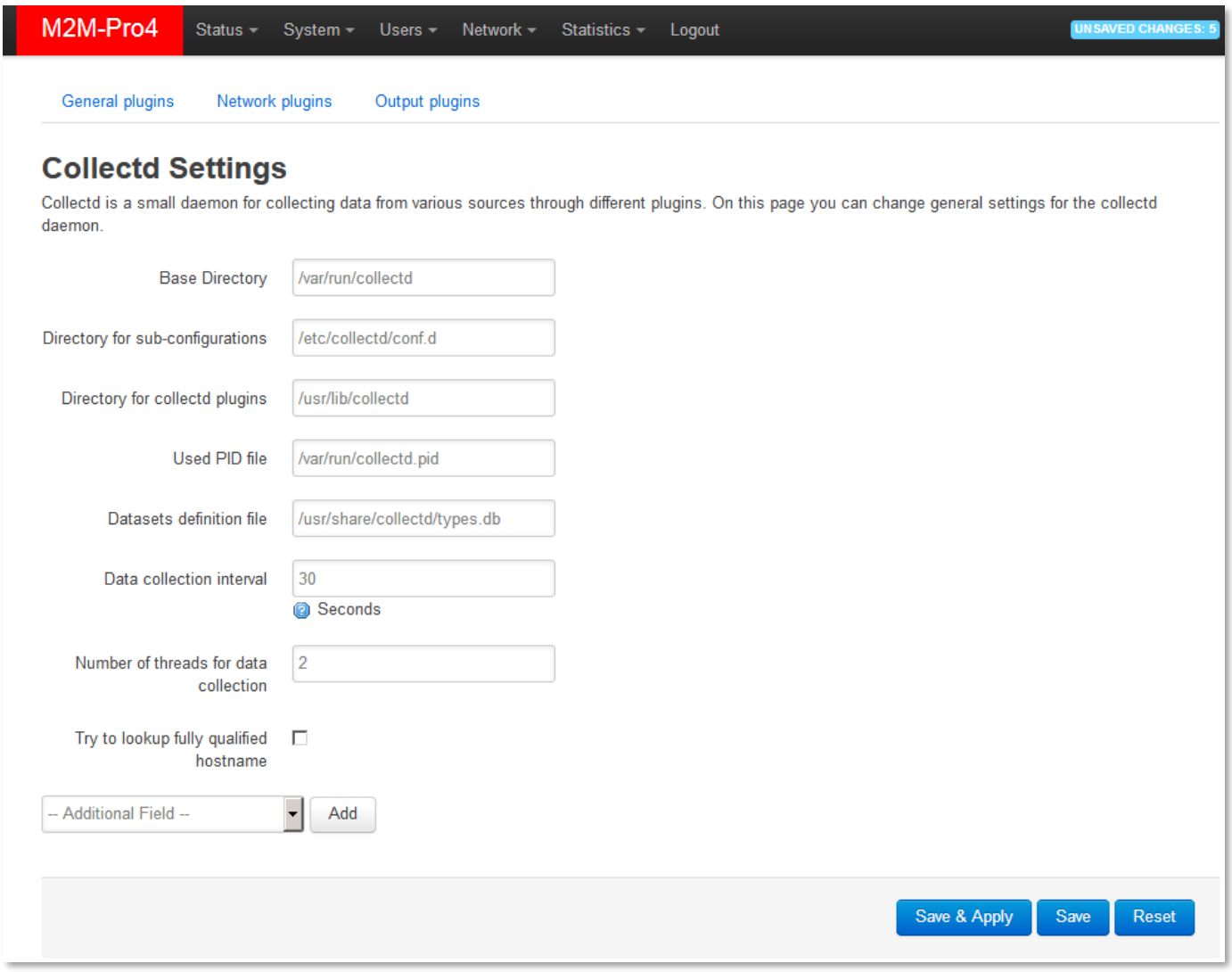
6.8.2 Configuring statistics reports

In the **Statistics** menu / **Setup** menu item, you can configure the current statistic settings for collecting and evaluating router's performance data and the performance graph settings.

The main screen is the **Collectd Settings**, where you can define the **Data collection interval** and the Linux-side settings.

When you have changed the configuration, push to the **Save & Apply** button.

The changes will be active in the next statistic cycle interval.



There are further tabs in the upper sub menu as **General Plugins**, **Network Plugins**, **Output plugins** where you can enable the collected performance items, interfaces, etc.

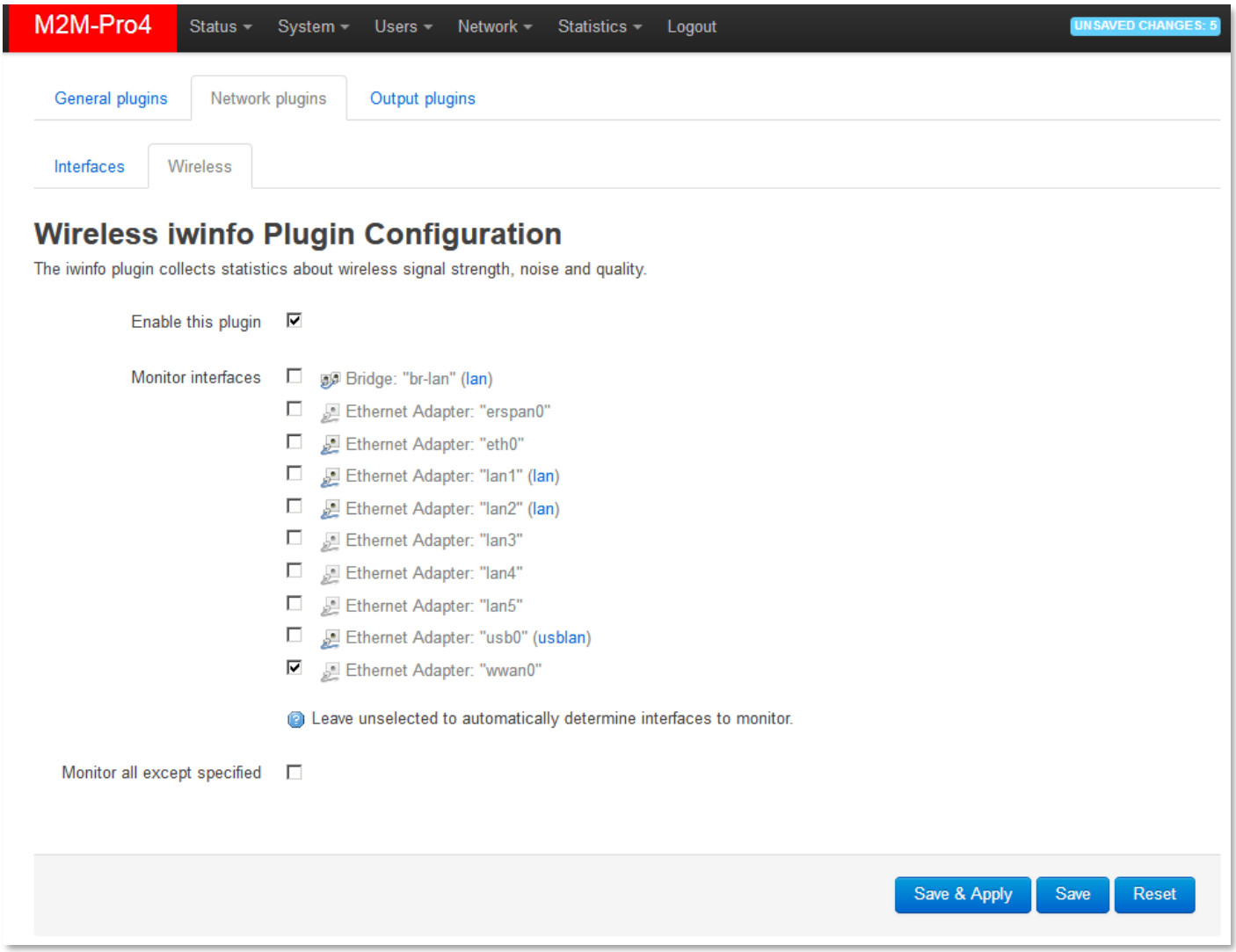
For example, to the wireless network statistics settings, let's choose the **Network** tab, and there the **Wireless** tab below.

Then allow the **Enable this plugin** and enable the ***wwan0*** inteface too.

To performing the change of the new settings, you have push to the **Save & Apply** button.

The changes will be active in the next statistic cycle interval.

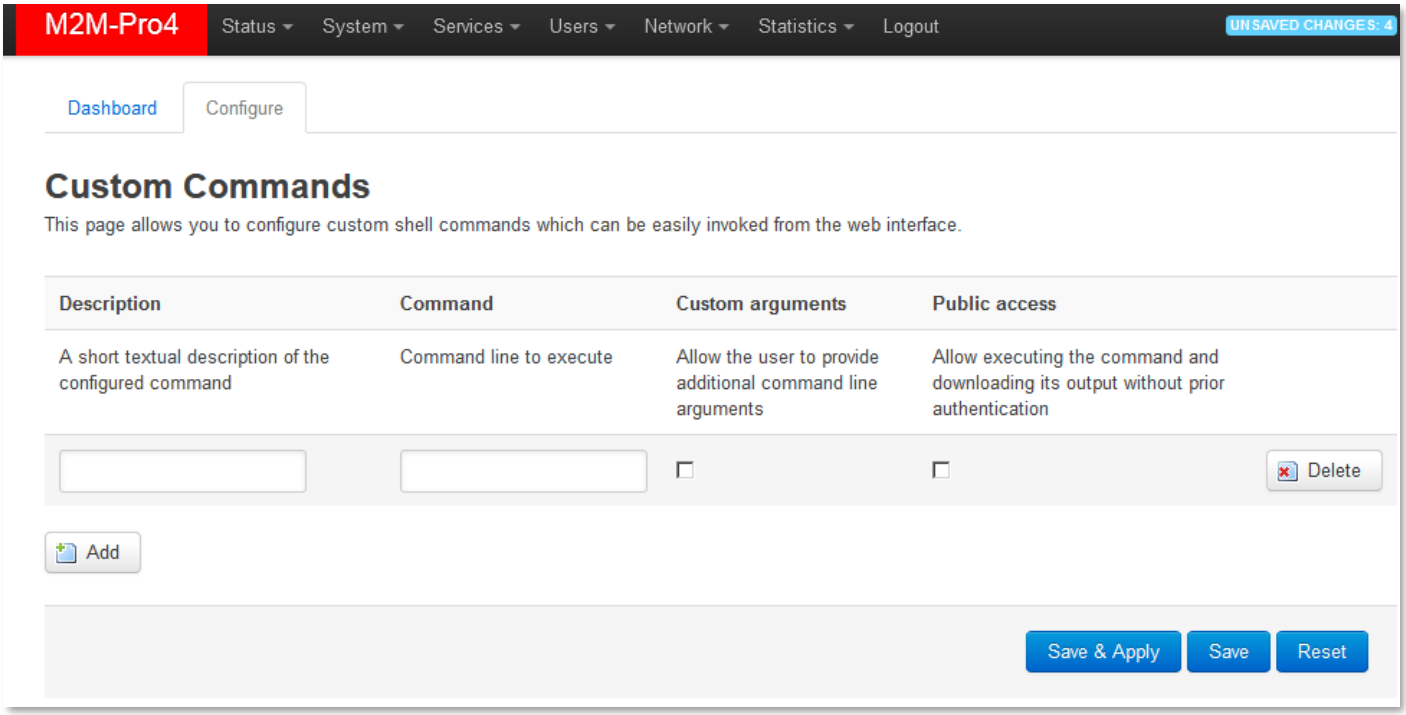
Then wait a couple of minutes and go to the **Statistics** menu / **Graphs** item and check the **Interfaces** tab, where the ***wwan0*** interface will be now listed.



6.9 Custom commands

You can configure and initiate custom Linux commands on the rotuer at the **System** menu, **Custom Commands** menu item.

With the Add button you can define a **Description** for the **Command** and the **Custom arguments** (user can define the further parameters and arguments) and the **Public access** to any user.



Here you can configure a list of custom commands as a startup script to your device (running a script or load a resident program).

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

6.10 Remote access (SSH)

You can access the device remotely according the current network and firewall settings.

Consider, the router can access devices or data due to the SIM card IP-segment possibilities. The same issue when you are attempted to access the router remotely: your computer must be located in the same IP segment or APN zone. (In case of public internet access, there is no limit for that.)

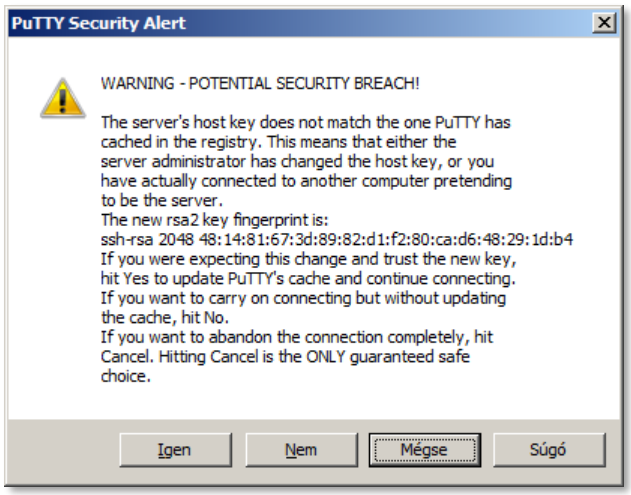
For the remote access you need to configure the **Network** / **Static route** and **Network** / **Firewall** settings to allow the ports, IP segment and the interfaces, subnet masksto *transmit/receive* data from the external zone.

The remote access is possible with SSH, web, by phone call or any other rule and port which you were configured.

SSH Connection

The router can be accessed through SSH connection, when it is available on its IP address – by a terminal utility (e.g. *putty*) – at the **192.168.1.1:22** (port nr. 22 for the bridged **Ethernet** port of ***LAN1***, ***LAN2, LAN3, LAN4*** interfaces) or **192.168.10.1:22** (port nr. 22 for the **USB** interface).

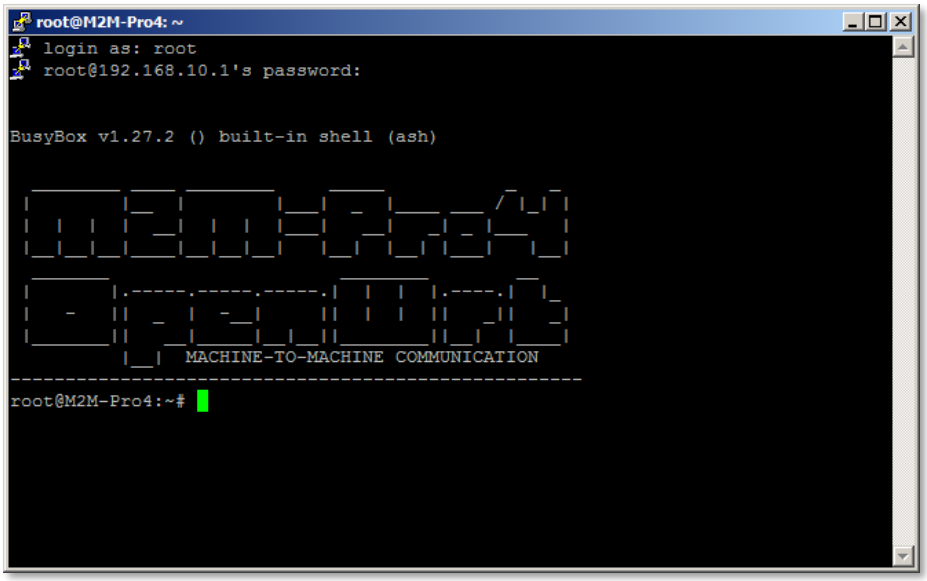
Accept (Yes) the Putty or other SSH terminal's Security Alert of the RSA2 key of the router to allow and trust the connection – by security reasons.



SSH login data:

Login: ***root*** **Password**: ***wmrpwdM2M***

Now you are logged in, at the OpenWrt®'s command line. Here you can executing Linux commands or using scripts on the device.



6.11 UCI usage by command line

The operating system uses the embedded Micro uClinux, kernel 4.4 version, ***UCI Command line interface*** – check command line compatibility before using the commands here.

The **UCI®** (***Unified Configuration Interface***) is an OpenWrt® API. This tool makes able the central configuration of the device and the command line configuration from the OpenWrt® system.

The following daemons and services can be accessed from SSH, at the Linux command line interface.

Connect the router with a terminal program at port nr. 22 by its current IP address and configure the following daemon.

The **Unified Configuration Interface** (**UCI®**) is an API of OpenWrt® which is also the utility to intend and to centralize the whole configuration of a device running on OpenWrt®.

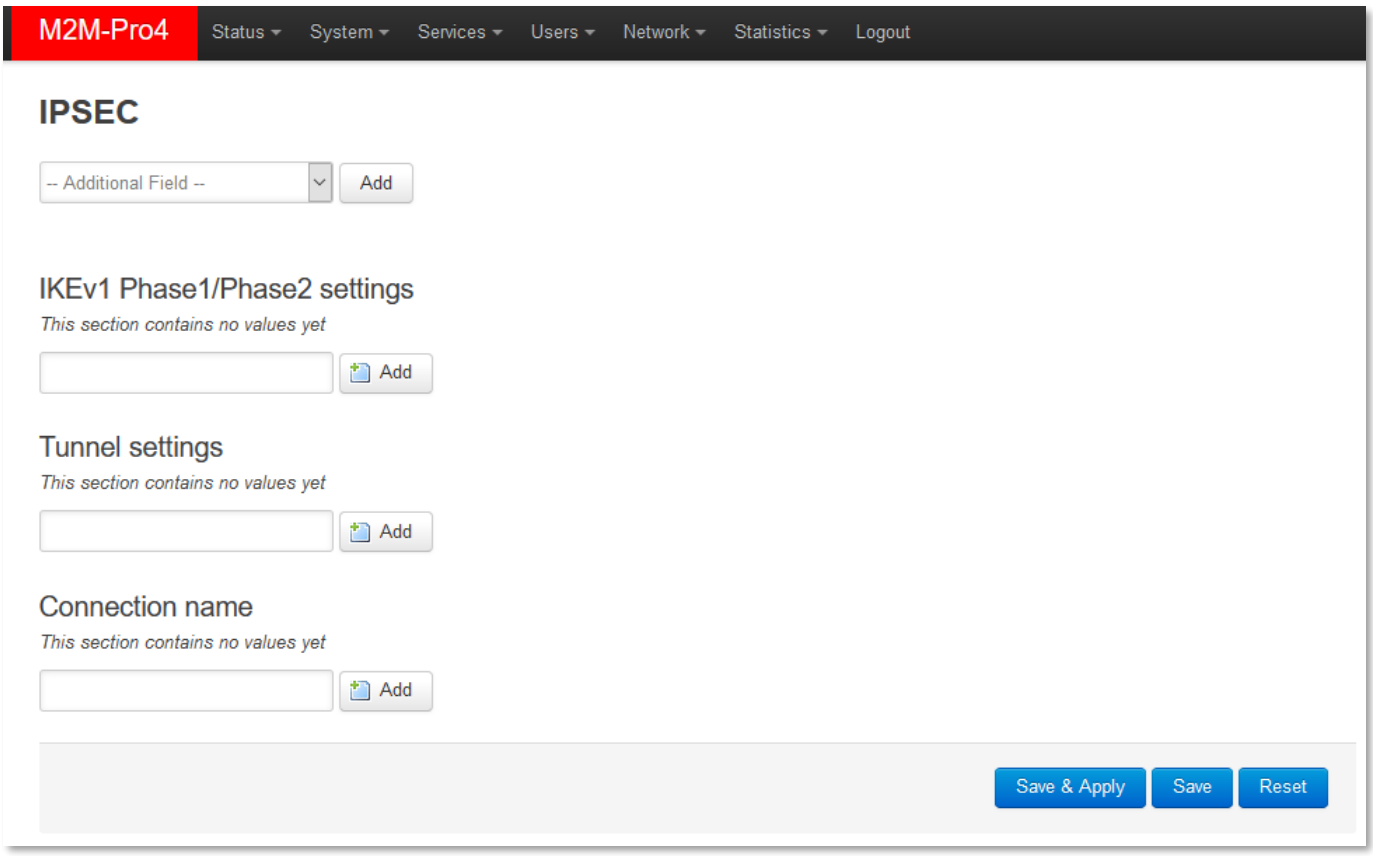
You can find the UCI command line interface options, setting parameters in the UCI CLI document. For further useable commands, please check the downloadable documentation from our website:

https://www.m2mserver.com/m2m-downloads/UCI_Command_Line_Reference_v3.pdf

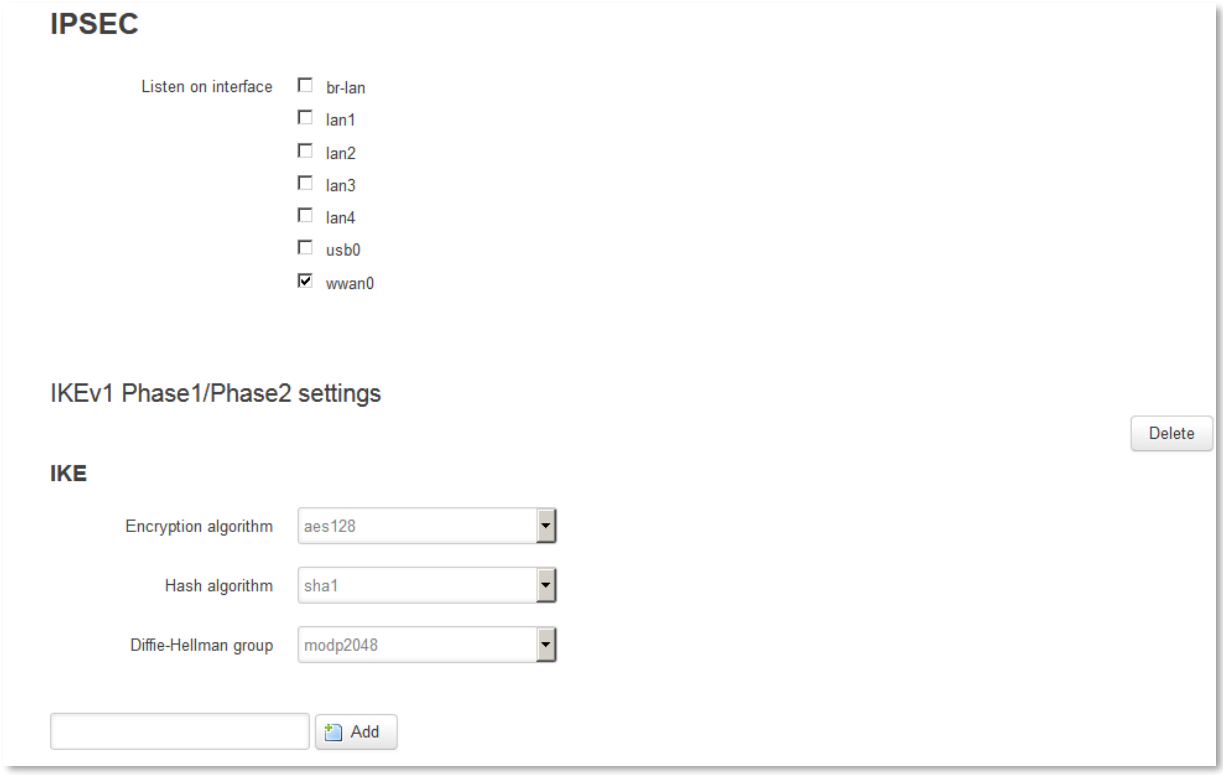
6.12 IPSec

You can configure IPSec for tunneling at the **Network / IPSEC** menu item.

Here at the **IPSEC** part, you can setup the *Listen on interface* option by the Add button. Choose one or more interface, which you want to configure the IPSEC service.



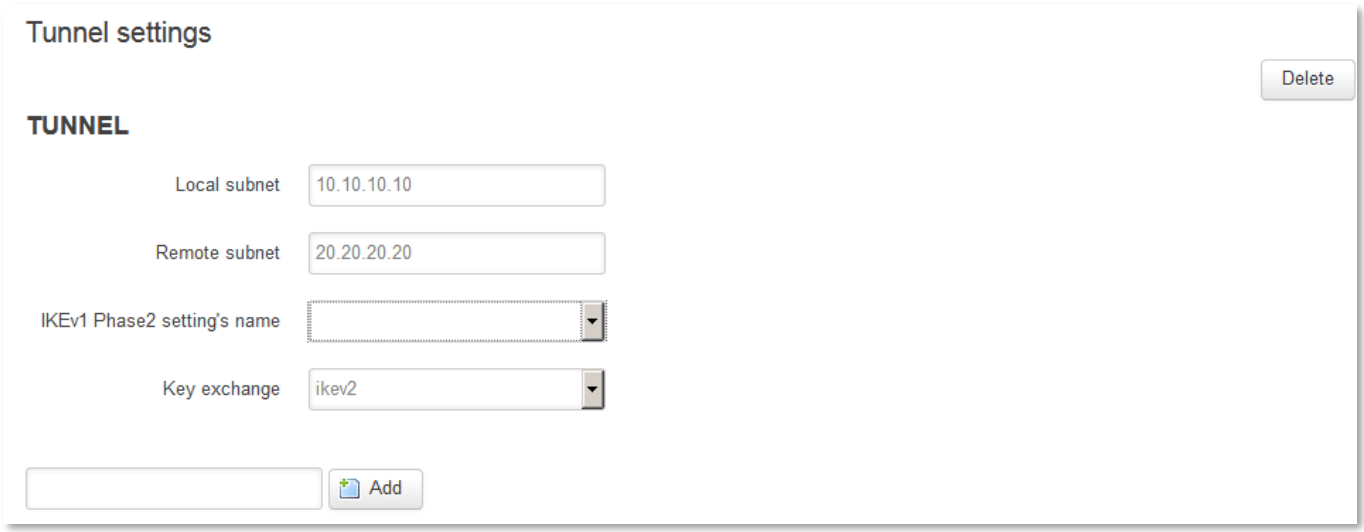
At **IKEv1 Phase1/Phase2 settings** you can define and Add a logical name for **Encryption algorithm** and **Hash algorithm**, **Diffie-Hellmann group** settings for the tunnel.



Then at **Tunnel settings** part you can define and 

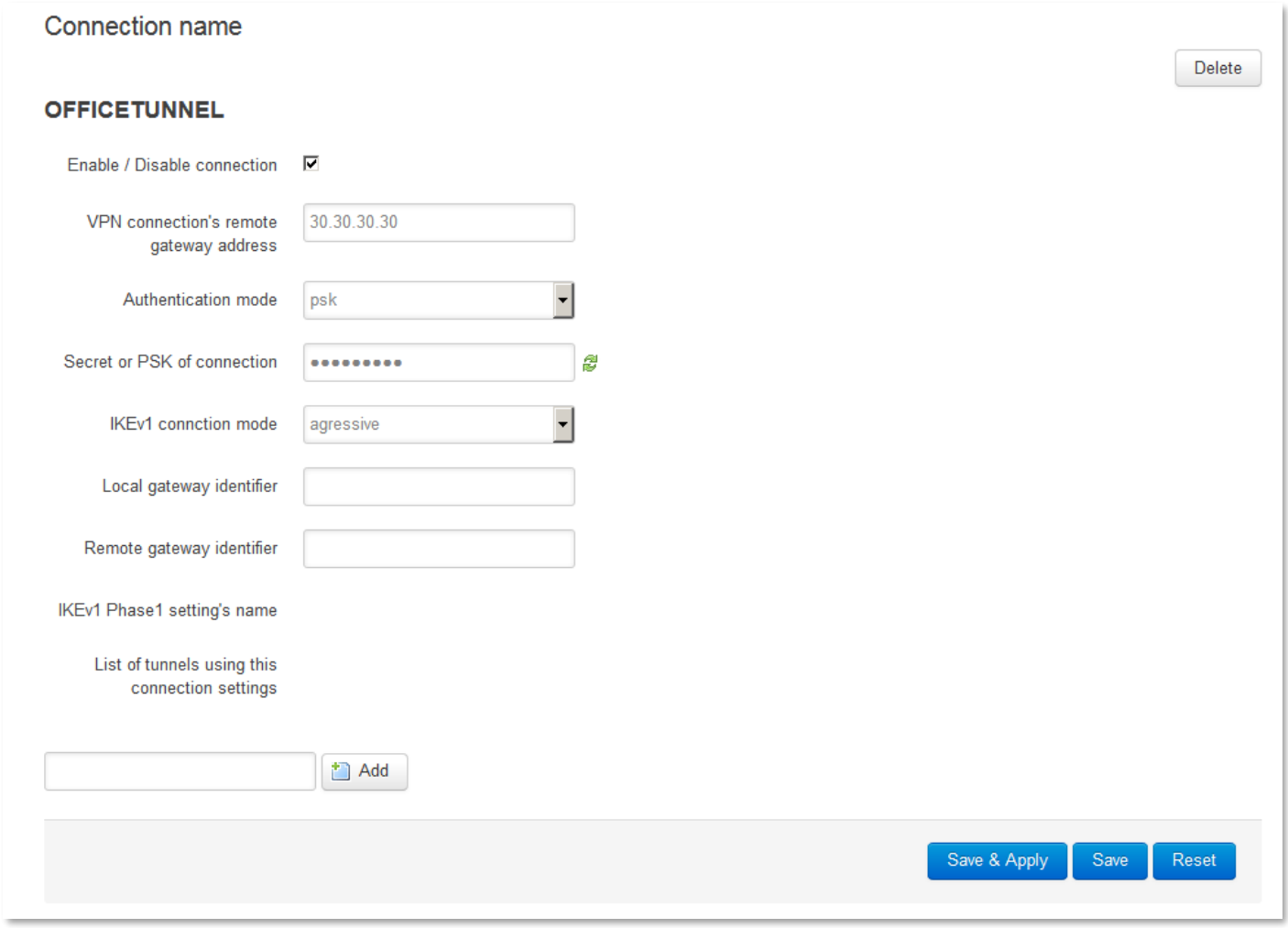
a logical name for **Local Subnet** and **Remote Subnet** of the subnets – add the IP segment addressess please to the fields.

The **IKEv1 Phase 2** name is a free to choose logical name for the tunnel connection, where the **Key exchange** method can be selected for the tunnel.



For the **Connection name** part you can **Enable/disable connection**.

Add the **VPN connection's remote gateway address** and choose **Authentication mode**, and add the *„psk key"* is to the **Secret or PSK of connection** field.



The **IKEv1 connection** mode can be *main* or *agressive*.

Add keys to the **Local gateway identifier** and **Remote gateway identifier** fields.

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

Important!

The used IPSEC method in the IPSEC menu has a Strongswan based operation. You can read more about the Strongswan and the useful parameters in the OpenWrt website here:

https://openwrt.org/docs/guide-user/services/vpn/ipsec/strongswan/start

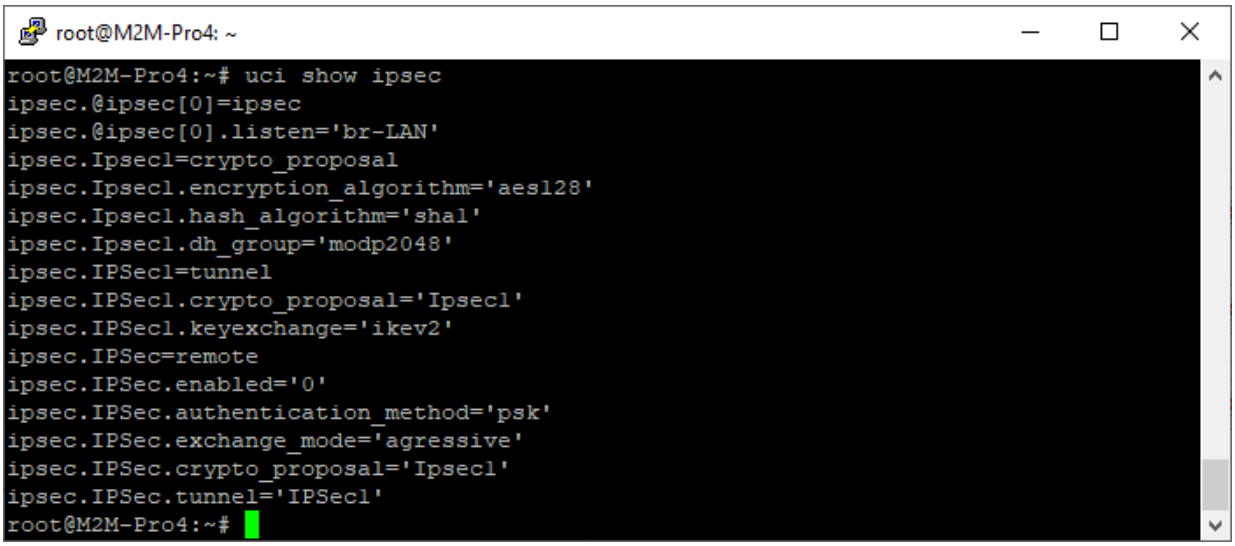
The IPSEC can be also configured from UCI (command line). ou can get more information about it here: https://oldwiki.archive.openwrt.org/doc/uci/ipsec

The IPSEC (Linux-side) *Strongswan* daemon can be configured by UCI here – from SSH. Some exampler for the settings can be found below.

The OpenVPN settings of IPSEC:

```
#uci show ipsec
```

Then the current IPSEC settings will be visible in the command line (SSH):



Configuration by the next syntax and sending to commit:

```
#uci set ipsec1.encryption_algorhitm=’aes128’

#uci commit
```

6.13 OpenVPN settings

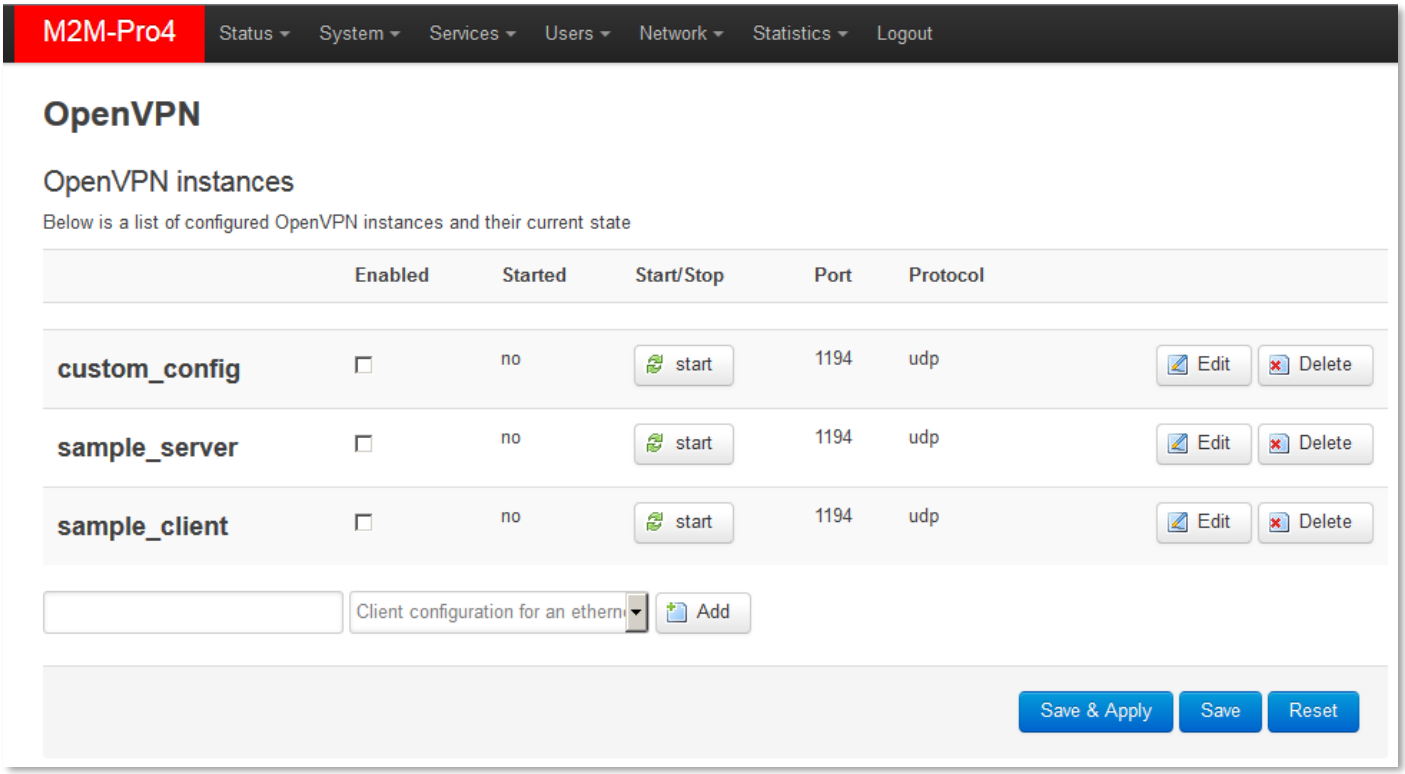
You can configure VPN tunnel at the **Services** menu, **OpenVPN** menu item. The service uses the default nr. 1194 port during its operation.

Here you will found three pre-configured instances for operating VPN connections. For activating a rule (setting), you have to **Enable** the instance, and then 

it. You can also 

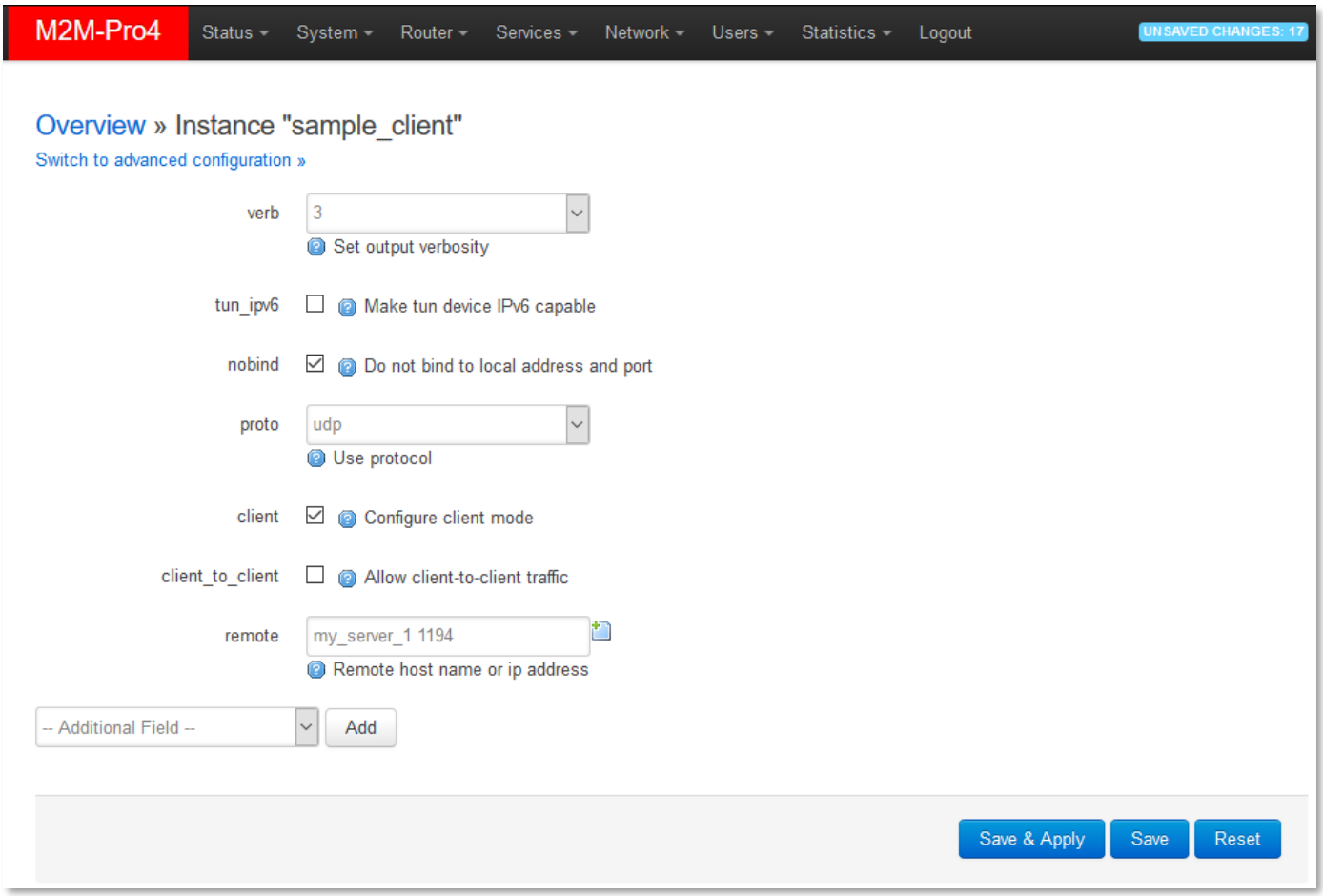
the existing settings here.
Save & Apply if you changed anything here.

Important! *You can configure VPN server or client connection here. In case of choosing the VPN client, the router wants to use an existing VPN server connection – which you have to be used and you have to define the current settings here also.*



Choose a profile from the pre-configured example settings - e.g. the a **sample_client** profile – which means a VPN client and configure its settings by the Edit button.

Then the next window appears where you can configure the VPN connection settings:



At **proto** field choose a protocol – as *udp* or *tcp.*
The **client** option needs to be checked if you want to use the VPN as VPN client. The **remote** field is here for configuring the remote server IP address (for client).

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

Then you will step back into the **OpenVPN** menu, where you have to **Enable** the configured entry and start the service by its button. Push to the **Save & Apply** again, please.

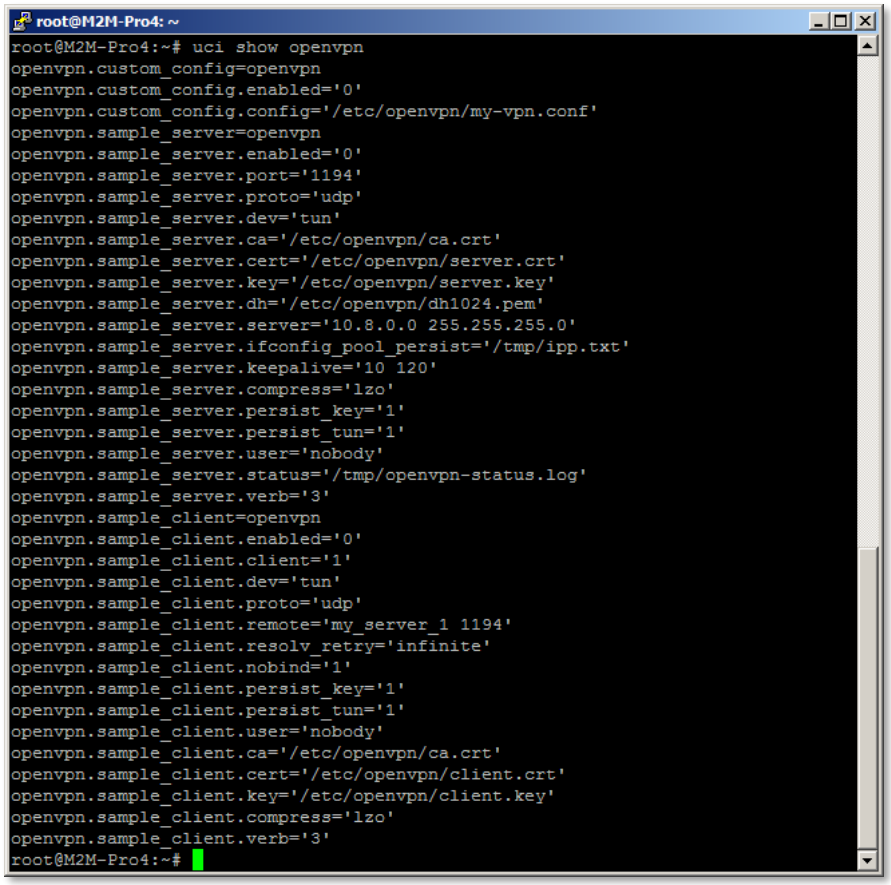
You can find more information at the OpenWrt® website about the tunneling settings here: https://wiki.openwrt.org/doc/howto/vpn.openvpn#tab__traditional_tun_server1

Further OpenVPN settings can be performed at Linux-side by the openVPN daemon and by using the supported UCI command line interface (see UCI interface for more information).

To check the OpenVPN settings from the UCI command line interface, open an SSH terminal and enter and execute the next UCI command at the command line:

```
#uci show openvpn
```

Then the current arguments of the OpenVPN settings will be listed to the CLI:



To setup a listed parameter you have use the following syntax and to commit the changes to apply.

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

#uci commit
```

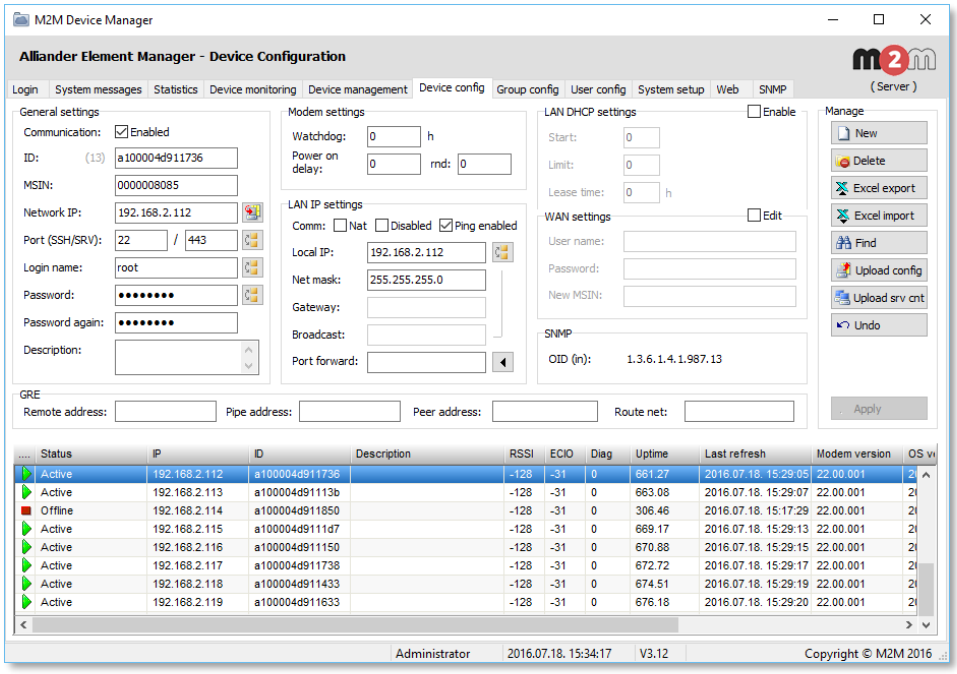
6.14 Device Manager settings

The application is available through license pack constructions, please advise our sales about the license pack options.

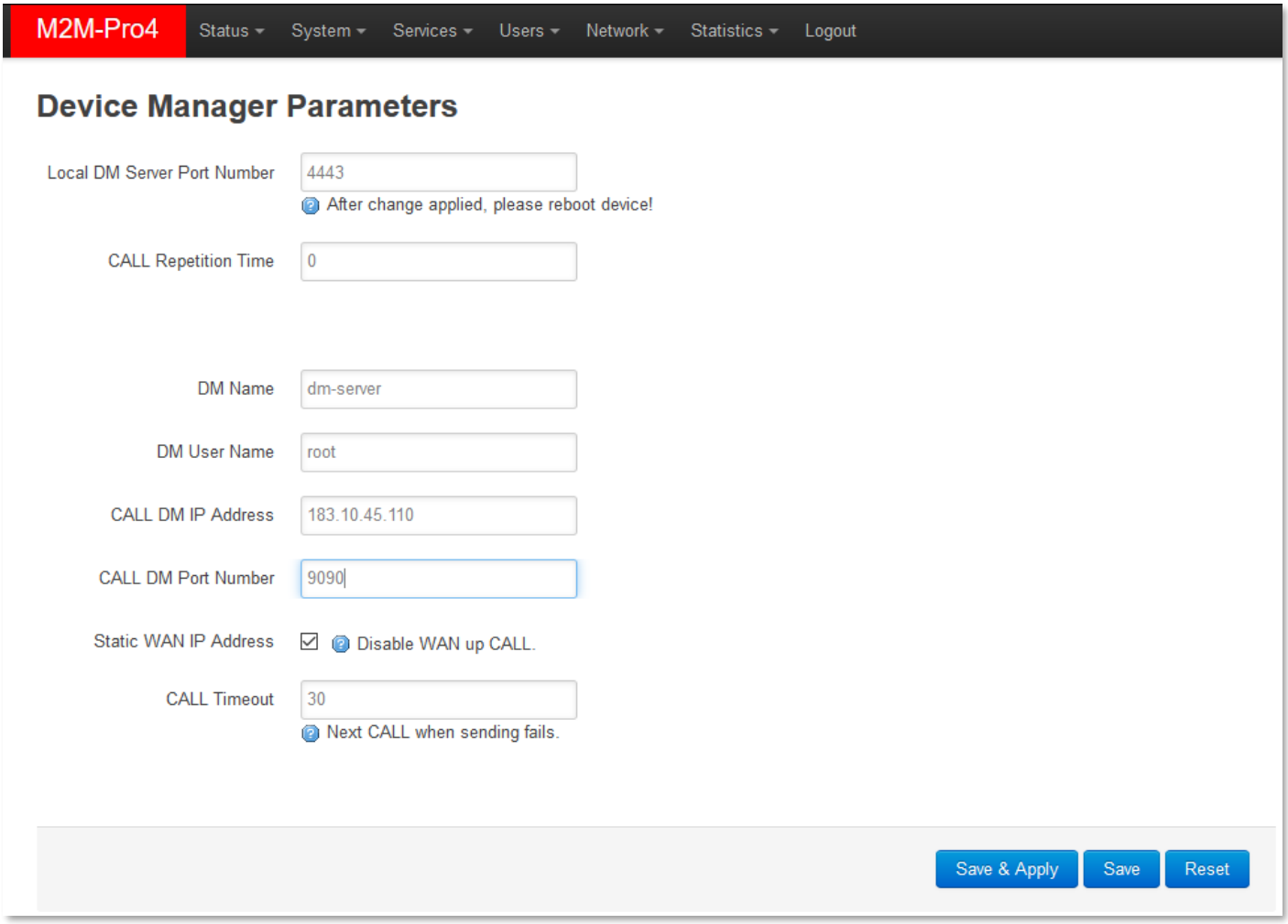
You can get further information on our website, the **Device Manager®** web page.

You can use remote monitoring and management features on the router by our optional Device Manager® application.
This is continuously provides operation parameters and status (as health of network access, signal strength, QoS, etc.).

Beyond the monitoring features, it can be used as well as for maintenance and reconfiguration of devices. You can also change the firmware of the device. You can manage one or even thousands of router devices by the application.



The software needs license to use, therefore we'd like to ask you contact our sales. You will find info about the software here: https://www.m2mserver.com/en/product/device-manager



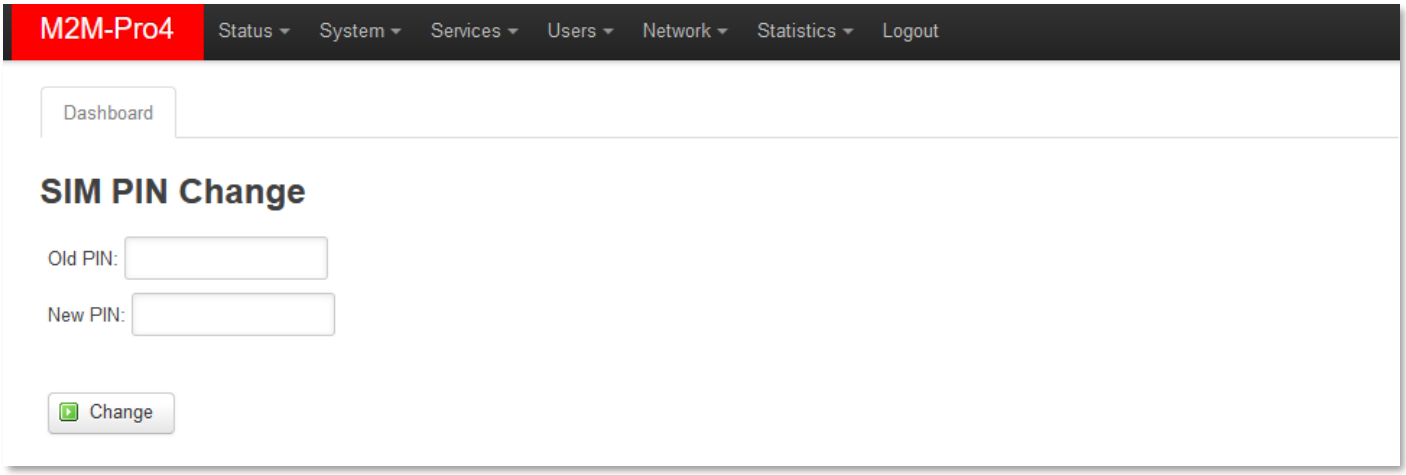
For the configuration of the Device Manager® open the **Router / Device Manager** menu item. Configure the **DM Port Number** – by default it is the nr. 4443.

The **DM Name** is the name of the serverad a unique identifier, where **DM User Name** is the server account and the **DM IP Address** (server IP) is also necessary for the connection.
Push the **Save & Apply** button for saving the settings.

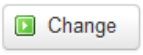
When you are configuring the DM, the server-side settings and the DM server must be alive. You can check the server availability by a simple ping from the router menu.

6.15 PIN code change

Choose the **Network / SIM PIN Change** menu item for changing the PIN code of the SIM.



Add the **Old PIN** and add the **New PIN** also.

When you modified the settings, save them by the 

button.

7. Troubleshooting

LED signals / LED activity

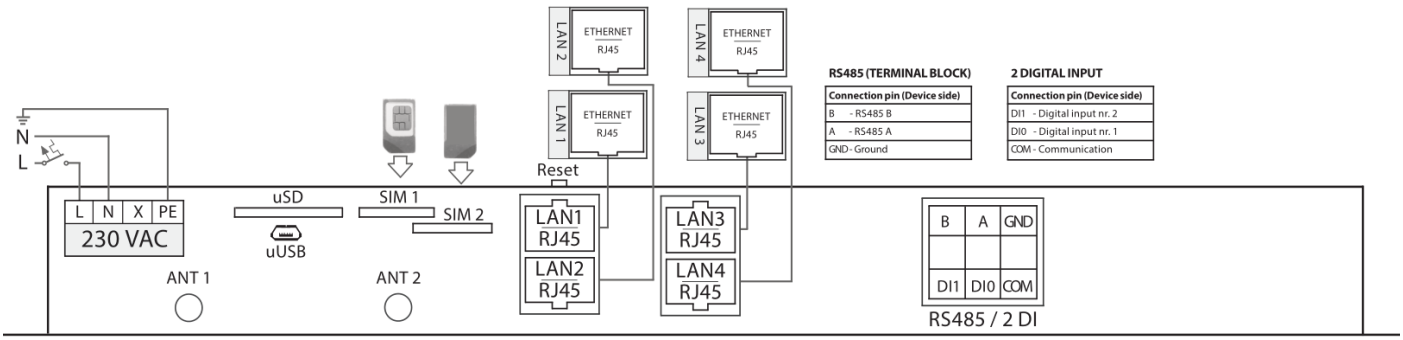
For understanding the LED activities, please check the Chapter 1.5 and Chapter 6.6.

Power supply

Connect the AC power supply according the hints of the following figure.

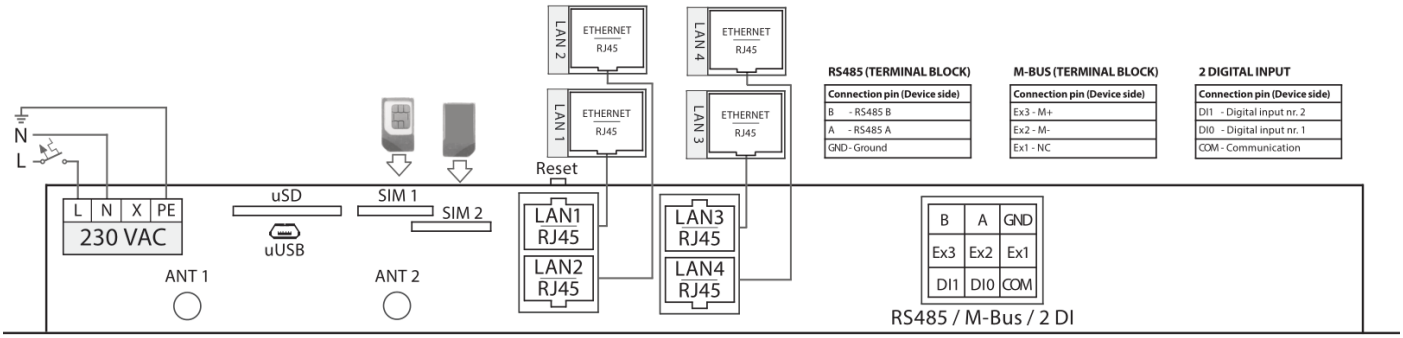
Then the router must be powered on, and the **PWR** (Power) and **ON** LEDs must be lighting and the device has been started, the boot process begins.

M2M PRO4 Router without MBus port - schematic draw / pinout:



M2M ROUTER PRO4

M2M PRO4 Router with MBus port - schematic draw / pinout:



M2M PRO4 DCU

Removing the power supply

When you are removing the AC power supply, the **PWR** (Power) LED will be blank and the super-capacitor will activated inside the device, for granting temporary (internal) power supply for the router. This is possible for 5 seconds now by default settings – technically this can be setup for 30-60 seconds also.

After 5 seconds, all connections will be closed and the file systems will be unmounted until you will adding the power supply again to the modem. Then all connections will be reconnecting and the mounting points will be accessable again.

USB connection

You can access the device on microUSB-to-USB cable, there you need to connect this cable to the ***USBLAN*** interface of the router.

The other side of the USB cable must be connected to a computer.

Then the **USB** LED must be lighting when the cable was connected.

RS485 connection

You can make utility meter connection to the modem by connecting **RS485** cables to upper 3-pins of the industrial terminal block connector.

You also need to configure and enable the operation by the **Network / Serial Proxy** menu.

When data traffic is performed through the cable, the **RS485** LED will be blinking during the communication (Rx and Tx) – by signing the data exchange between the device and the meter(s).

M-Bus connection – order option

The M-Bus feature is only available by order request.

There you can make M-Bus device connection to the modem by connecting the MBus cable to middle 3-pins of the industrial terminal block connector.

You also need to configure and enable the operation by the **Services / mbus** menu.

When data traffic is performed through the cable, the **Mbus** LED will be blinking during the communication – by signing the data exchange between the device and the M-Bus devices.

Digital input connection

You can make connection from the modem to external device(s) for monitoring status changes of digital inputs (logical). Connecti the cables to lower 3-pins of the industrial terminal block connector at the **2DI** title.

SIM-card is not detected

Turn off the device by removing the AC connection.

Check that a SIM card was inserted to the **SIM** holder and the proper orientation of the card. Insert and push the SIM card to the holder. Start the device by reconnecting the AC power to the device.

If the problem is still occuring, ask you Mobile Operator about the SIM card is healthness and activation, APN.

SIM/APN failure

Always check the **Status / Overview** menu first at the **SIM ID** field for the current status of the SIM card. In normal case you have to see the SIM identifier there. But, in case of a problem, the SIM error message will be shown, as:

- **No SIM or SIM error –** means: there is no SIM card presented, insert an active SIM card, not inserted properly or the SIM card is wrong. Check the SIM and the insertion again.
- **Not enough RSSI value** – means: connect a proper 4G antenna to the **ANTENA** mount or use a better gained antenna to the device for the better RSSI value (signal strength).
- **Check NW registration** – means: APN and SIM registration is in progress
- **Wrong NW registration** – means: APN name for the SIM card is not configured well or the setting is wrong
- **Check RSSI** – antenna is not presented and/or the SIM card is not configured or wrong, Check antenna and SIM again.

During the operation, when the **WAN** LED is not lighting for long, then the device cannot be registered to the wireless network or the modem was not initiated properly. This could also caused by a wrong APN setting.

When the APN setting is not right or the network registration was not made successfully, the **SIGNAL LEVEL** bottom led blinking.

Please check SIM card insertion and orientation (after power off the device). Power on the router. Re-configure the APN and SIM settings on its local web user interface.

If the problem is still occuring, ask you Mobile Operator about the SIM card is condition and activation status, correct APN name and configure the modem with the new SIM and SIM info.

Power outage – disconnecting the ports and data connection

In case of power/electricity network outage or maintain, the wireless and RS485 meter data connection and session will be established if it was interrupted throug a way and it was later estabilished, reconnected.

Power outage

In case of an unwanted power outage, after 5 seconds the device will disconnect all sessions and connections - by safety reasons.

After estabilishing the power source, the device will automatically revert to enable data transmission, builds up the network connections and mounts the data mounting points.
Switching on is possible according to the described operation of the reset button, or the device is started by applying the power supply again.

Cannot access the device on SSH / LuCi web interface

You tried a wrong IP address or you cannot connected to the device properly.
Check the IP address, ping the device.
Reconfigure the IP address on you PC.
For accessing the router's web user interface we offer the Mozilla Firefox web browser only.
Try to access the router on its USB interface by your browser: **https://192.168.10.1**
Ensure that the router uses a SIM card and it's **APN** is already confifured and the **WAN, SIGNAL LEVEL** leds are active or not.

Default login data:

- **Username**: ***root***
- **Password**: ***wmrpwdM2M***
- Push to the **Login** button to access the web UI.
- Allow the accessing of the device's default IP address in your browser by pushing to the ***Special*** button, then allow the safety exclusion into the pop-up window.

8. Hardware additions & settings

8.1 Supporting mini-PCIe modules

The router contains an embedded 4G LTE cellular module (soldered to the mainboard by factory default).

There are some order options for using an LTE450 or an LTE Cat.M/Cat.NB module on the internal miniPCIe interface (module is attachable). The following wireless modules are supported:

- Cellient® MPL200 (for LTE 450 network)
- Quecktel® EC25 (for Narrow band network)
- Quecktel® EC21 (for Narrow band network)
- Quecktel® BC95 (for LTE Cat.M1/NB2 network)

Ask us about the available cellular module options.

8.2 Supporting the „One-wire" interface

The router is supporting the "One-wire" standard industrial interface for temperature measurement. If you need more information regarding on this topic, please ask us for getting the related documentation, order options.

9. Support

9.1 Technical Support

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

E-mail: iotsupport@wmsystems.hu **Phone**: +36 20 3331111

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

For the proper identification of your device, use the device's glued sticker and its information, which contains important information for the call center.

Due to the support questions, the product identifier is important for resolve your problem. Please, when you are attempting to tell us an incident, please send us the IMEI and SN (serial number) information from the product warranty sticker (located on the front face of the product housing).

The documentation and software release for this product can be accessed via the following link:
https://www.m2mserver.com/en/product/m2m-router-pro4/

9.2 GNU/Linux license and open source code

The router's operating system and OpenWrt®/Luci open source code is available on our website at the product site. The router's software is under GNU/Linux licensing.

There at the **Downloads** tab at the middle on the router's local website, at the **Source Code** part you will found the **source code** of the device's software and **GNU/Linux license notice**.

10. Legal notice

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

Warning

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