

User Manual

M2M Industrial Router 2 DCU MBUS



Rev: 1.21

2024-02-01

Document specifications

This document was completed for the **M2M Industrial Router 2 DCU MBUS®** device and contains the hardware specification, with the most important information and software settings of the device.

Document category:	User Manual
Document subject:	M2M Industrial Router 2 DCU MBUS®
Author:	WM Systems LLc
Document version No.:	REV 1.21
Number of pages:	98
Hardware Identifier No.:	BE0109D_ROUTER_9X60_7070_AXP, BE0114A_ROUTER_9X60_7X7X_P1
Firmware version:	202401221 or later
ST32 Firmware version:	202307121
OpenWRT Linux Kernel version:	5.10.184
Document status:	Final
Last modified:	1 Februar, 2024
Approval date:	1 Februar, 2024

Table of contents

CHAPTER 1. Product information	5
CHAPTER 2. Technical data.....	5
2.1 Power voltage / Current ratings	7
2.2 Cellular modules (order options)	7
CHAPTER 3. Device exterior design and appearance	9
3.1 Safety cautions	10
3.2 Mounting, fastening	12
3.3 Antenna.....	13
3.4 Further accessories.....	13
CHAPTER 4. Software system.....	15
4.1 Operation system.....	15
4.2 LAN block feature	15
4.3 Device Manager platform.....	15
4.4 TLS protocol communication.....	16
4.5 Accessing the device (via SSH connection).....	16
CHAPTER 5. Starting the device	17
5.1 Connecting the DCU	17
5.2 First start.....	18
5.3 Web user interface of the router	19
5.4 Access via SSH connection	21
CHAPTER 6. Web Administration user interface	23
6.1 Main page (Dashboard).....	23
6.2 Menu	25
6.3 Status menu.....	25
6.4 System menu.....	25
6.5 Services menu	26
6.6 Network menu	27
6.7 VPN menu.....	27
CHAPTER 7. Important notes.....	28
CHAPTER 8. Network configuration of the device	30
8.1 Interface settings	30
8.2 Cellular / Mobile internet settings	31
8.3 Ethernet (LAN) settings	33
8.4 DHCP, DNS settings.....	35
8.5 DNS settings.....	37
8.6 Defining the route rules	38
8.7 Firewall settings.....	38

8.8 Port Forward settings	43
8.9 IP routing, NAT settings.....	45
8.10 Dynamic DNS settings	46
CHAPTER 9. Special settings	47
9.1 Ping an IP address.....	47
9.2 Network Time Service (NTP)	48
9.3 TFTP settings.....	48
9.4 LED configuration	49
9.5 Remote access (SSH)	51
9.6 UCI usage from the command line	53
9.7 IPSEC settings	53
9.8 VPN client (OpenVPN) configuration.....	54
9.9 RS485 / Modbus settings (Ser2net).....	58
9.10 Data Collection settings (RS485 / Modbus).....	63
9.11 MBus settings.....	75
9.12 Voice call settings.....	76
9.13 Run commands remotely (SMS config settings)	76
CHAPTER 10. Software refresh and DCU maintenance	78
10.1 Firmware refresh	78
10.2 Installing applications	79
10.3 Restarting the device	82
10.4 Shutdown / halt of the devuce	83
10.5 Reset the device	83
10.6 Password change.....	84
10.7 Backup and restore of settings.....	84
10.8 Clone configuration.....	87
10.9 Start or stop a system service	88
10.10 Log.....	88
CHAPTER 11. Troubleshooting.....	91
CHAPTER 12. Support availability	97
12.1 Contact the support line.....	97
12.2 Product support	97
CHAPTER 13. Legal notice	98

Chapter 1. Product information

The robust DCU device features an Ethernet port, an RS485 port, an MBus port, a cellular module, and compact industrial design.

It is currently available with LTE Cat.1 or LTE Cat.M/Cat.NB modules that provide enhanced coverage.

The Data Concentrator has undergone a complete redesign, providing improved processing speed with an eMMC chip for secure boot and encrypted data storage.

It also features an OTP-enabled memory chip, an option for a Chip SIM (MFF2), and supercapacitor protection along with the latest security protocols and features for maximum security.

Reliable and Rugged Communication Device for Smart Grid and Industrial Applications.

This Data Concentrator is designed for use in various smart grid and industrial M2M / IoT applications, including Automated Metering Infrastructure (AMI) and industrial automation projects.

The DCU is capable of reading Modbus registers from connected PLCs and data from up to 30 MBus meters. It transmits valuable data to the data center through the MQTT protocol, providing a cost-effective solution for industrial automation and smart metering connectivity.

Ports / Interfaces

The device offers the following ports: Ethernet, RS485, Mbus, and micro-USB port (for configuration).

System Software

The DCU utilizes the open-source OpenWRT® operating system, allowing clients to compile their own applications to the firmware. It features a user-friendly web admin interface for easy access and configuration.

The product can also be managed with the state-of-the-art Device Manager® platform (order option), providing clients with the ability to perform OTA firmware updates and mass deployments more efficiently.

Secure storage / Secure Boot

The device has a built-in eMMC chip (4 or 8 GByte storage – by order option) for Secure Boot process / encrypted storage of all customer data. It uses an OTP-enabled memory chip.

The device is secured with Secure Boot system and secure storage mechanism. It uses an SHA-256 encrypted file system (with RSA and SHA-256 assignments).

The device operates with multiple encrypted partitions and file systems, which ensures the security of the device.

Security features

The device uses Secure Boot system with Secure Key Storage features (on encrypted eMMC memory chip).

The DCU continuously monitoring the operation parameters (QoS, module operation, vital signals, etc.).

It has detection of network interface connections / disconnections with an alarm event sending to the Device Manager® management platform.

The software of the device applies unique passwords, firewall and it has support for IPSec tunneling.

Management

Remote management of routers, DCUs using Device Manager® software (order option) via a secure TLS v1.2 connection (by option) during the communication with the router.

The DCU allows clients to do OTA firmware updates and mass deployments significantly faster via Device Manager® platform.

Last GASP – notification of power outage

The device has built-in supercapacitor parts with LastGASP feature (in case of a power outage, the router is operating further, while an immediate notification will be sent from the event to the Device Manager® software).

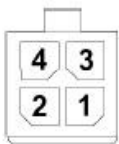
Chapter 2. Technical data

2.1 Power voltage / Current ratings

- **Power Voltage / Ratings:** · 12V DC, 1A power supply (9-32VDC) – powered via Microfit 4-pins power input connection (from external 12V DC power adapter)
- **Current / Consumption:** Average: 200mA - 320mA, 12VDC (according to operation / selected module) / 2.4W – 3.84W, 12VDC

For the connection it is recommended to use the DC microfit connection power adapter or a 12V DC supply according to the pinout which can be seen on the next figure.

4-PIN connector (Power Input)



Pin assignment of 4-pin connector

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

2.2 Cellular modules (order options)

- **LTE Cat.1 / 450 MHz module with 2G „fallback”**

Module:

- SIMCOM A7676E

Bands:

- LTE Cat.1 / 450MHz: B1/B3/B8/B20/B31/B72
- GSM/EGPRS: 900/1800MHz

- **LTE Cat.M / Cat.NB / 450 MHz module with 2G „fallback”**

Module:

- SIMCOM SIM 7070E

Bands:

- LTE Cat.M / 450MHz: B1/B2/B3/B4/B5/B8/B12/B13/B14/B18/B19/B20/B25/
B26/B27/B28/B31/B66/B72/B85
- LTE Cat.NB: B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B26/B28/B31/
B66/B85
- GSM/EGPRS: 850/900/1800/1900MHz

Chapter 3. Device exterior design and appearance



***Industrial DCU, assembled in aluminum casing
with interface connectors / ports***

- 1 – POWER (9-32V DC): Microfit 4-pin power connector (for DC power/adapter)**
- 2 – *SIM card slot (2FF)**
- 3 – micro-USB connector (for configuration)**
- 4 – Reset button (hole)**
- 5 – Ethernet (RJ45, 10/100 Mbit)**
- 6 – Antenna connector (SMA-M, 50 Ohm)**
- 7 – 3 Operation LEDs**
- 8 – RS485 / Modbus connector (3-pin terminal block)**
- 9 – Mbus connector (2-pin terminal block)**

** SIM insertion: push the APN-activated SIM into the SIM tray (2) - the SIM chip surface must be look to top and the cutted edge of the SIM must be look to the DCU – then push the SIM until it will be fixed and closed (you will hear a soft click sound).*



Industrial DCU MBUS with Mbus and RS485 / Modbus connectors



Industrial DCU MBUS, assembled in aluminum casing, attachable to 35mm DIN rail (with an adapter)

3.1 Safety cautions

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

Only a responsible and skilled person with adequate experience and knowledge in wiring and installing a DCU device, as instructed by the service team, should carry out the installation.

It is forbidden for the user to touch or alter the wiring or installation. The device enclosure should not be opened during operation or when connected to power, and the device PCB should not be removed or modified. No modification or repair should be made without the manufacturer's permission, as this will result in the loss of product warranty.

CAUTION! Only certified experts or the manufacturer are authorized to open the device enclosure.

The device uses 9-32V DC power supply within the enclosure, and the enclosure should NOT be opened or the PCB touched.

The IP51 immunity protection will only be effective if the device is used under normal conditions and with undamaged hardware in the provided enclosure / chassis.

Any deliberate damage or malfunction of the device will result in the loss of product warranty.

To ensure safety, the following guidelines should be followed:

- Keep the chassis area clean and free of dust during and after installation.
- Wear appropriate clothing to avoid loose clothing getting caught in the chassis.
- Avoid actions that could cause a hazard to people or equipment.

Safety precautions for Electricity

- Read all safety warnings before working on equipment powered by electricity.

- Locate the emergency power-off switch for quick access in case of an electrical accident.
- Disconnect all power before installing or removing a chassis, working near power supplies, or inserting a SIM card.
- Look for potential hazards in your work area, such as moist floors, ungrounded power cables, frayed cords, and missing safety grounds.
- Never work alone if hazardous conditions exist.
- Always verify that power is disconnected from a circuit before working on it.
- Do not open the internal power supply enclosure of the DCU.
- In case of an electrical accident, follow these steps:
 - Use caution to avoid becoming a victim.
 - Turn off power to the device.
 - If possible, send someone for medical aid. If not, assess the victim's condition and call for help.
 - Determine if rescue breathing or external cardiac compressions are needed, and take appropriate action.

Preventing Electrostatic Discharge Damage

- Electrostatic discharge (ESD) can cause damage to equipment and impair electrical circuitry.
- Always follow ESD prevention procedures when removing and replacing modules:
 - Ensure that the DCU chassis is grounded.
 - Wear an ESD-preventive wrist strap and connect it to an unpainted surface of the chassis frame to safely channel ESD voltages to ground.
 - If a wrist strap is not available, ground yourself by touching a metal part of the chassis.

3.2 Mounting, fastening

The device's bopla aluminum enclosure can be fixed to a DIN-rail using the optional AB800MKL fixation part, or mounted to a wall, placed in a server rack, or fixed in a similar manner.



***The device enclosure
can be mounted using
either the AB-MKL***

one-sided DIN-rail adapter (left) or the AB800MKL adapter (right) on a wall or DIN-rail.

These accessories can be ordered - more information:

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

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

3.3 Antenna

Please be aware that the presence of metal parts in close proximity, the metal material of the cabinet, and industrial conditions such as the use of high power levels or exposure to external radio frequency signals can cause radio interference and result in weak wireless signals during transmission or reception, as well as reduced signal quality.



In these cases, we recommend testing the wireless signal reception and quality. If necessary, you can improve reception by using an external magnetic mount antenna that is mounted outside of the cabinet and placed on its surface.



3.4 Further accessories

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

Microfit power cable:

Type: min. 70 cm, OMYA type, 2 x 1 mm², halogen free, double insulated wires, min. 24 V DC voltage, wires are marked by colors and blanked.

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

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

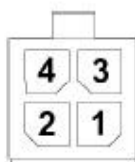
For the wiring and assuring the power supply you should take note to the following figure.



More information:

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

4-PIN connector (Power Input)



Pin assignment of 4-pin connector

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

RS485 cable:

You should use the following cable type: 70 cm OMYA type, 3 x 0,75 mm², halogen-free, double insulated wire pair, up to min. 24V DC breakdown voltage, colour signed cabling, blanked on the cable end – for supporting the 24V DC power voltage.

Type of connection: terminal block, 3-pin

Function: RS485 connection for external devices

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



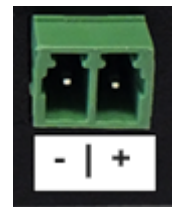
Mbus cable:

You should use the following cable type: 70 cm OMYA type, 2 x 0,75 mm², halogen-free, double insulated wire pair, up to min. 24V DC breakdown voltage, colour signed cabling, blanked on the cable end – for supporting the 24V DC power voltage.

Type of connection: terminal block, 2-pin

Function: Mbus connection for external devices (up to 30 slaves)

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



DC power adapter:

Connector: 4-pins microfit

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

More information:

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



UTP (Ethernet) cable:

Type: Cat5e UTP PVC

Connector: RJ45

Chapter 4. Software system

4.1 Operation system

The device runs on OpenWRT® system with a micro Linux microkernel. The secure boot system is integrated into the hardware-level eMMC secure chip and partitions are encrypted by secure boot.

The DCU comes with a pre-installed system, which is tailored to the customer's requirements and includes the operating system, software, and a factory default configuration. The device uses a web user interface (LuCi®), and standard Linux-based and UCI commands at the command line.

4.2 LAN block feature

If the Ethernet (LAN) cable is disconnected from the DCU or the device it's connected to, the device will notify of the event and the LAN controller will be stopped for security reasons. This can occur at the DCU or the connected device. The LAN controller can be re-enabled from the Device Manager®.

To block the LAN interface, go to the Device Manager software, access the **Device config** tab, and allow it in the DCU's configuration. If the Ethernet removal event occurs, it will be signaled in the Device Manager and the LAN controller will be disabled, stopping LAN traffic immediately. After restarting the device, the DCU will still not be able to communicate on the LAN interface until you allow usage again from the Device Manager® platform.

4.3 Device Manager platform

The Device Manager® software can be used for the remote management of the routers, DCUs. The application allows for remote maintenance and reconfiguration of the devices, as well as continuous monitoring of operating characteristics such as network access, field strength, runtime, and QoS.

You can also replace and install firmware on the device and manage thousands of routers, DCUs from this program, allowing for remote control and execution of tasks on the device. In the Device Manager software, individual or group settings can be made. Legacy or TLS communication can also be allowed in the Device Manager software during the M2M Industrial Router 2's communication.

4.4 TLS protocol communication

TLS v1.2 protocol communication can be activated between the DCU and the Device Manager® from the software side, by choosing TLS mode or legacy communication. The device uses the mbedTLS library and the Device Manager® (DM) uses the OpenSSL library. The encrypted communication is double encrypted using a TLS socket for added security.

The TLS solution uses mutual authentication to identify the two parties involved in communication. Both sides have a private-public key pair, with the private key visible only to the DM and DCU, and the public key in the form of a certificate. The device firmware includes a factory default key and certificate, and until a custom certificate from the DM is received, the DCU will authenticate itself with the embedded certificate. The router only implements factory default, so any TLS connection can be established with any certificate, including self-signed, as long as the encryption inside TLS is known. Access requires knowledge of the encryption and a successful self-authentication with the root password.

4.5 Accessing the device (via SSH connection)

The DCU can be accessed via an ssh connection, either remotely through the cellular network (LTE Cat.1, Cat.M or Cat.NB) within the IP address range of the SIM card on the WAN interface or via the local Ethernet interface (LAN). Access is protected with RSA2 key.

Chapter 5. Starting the device

5.1 Connecting the DCU

1. Ensure that the DCU is not under power voltage, therefore the power adapter cable is removed from the **POWER** titled microfit connector (1) – or the adapter is not connecting to the power network. Ensure, that all the 3 LEDs (7) are blank.
2. **Mount** a proper **LTE antenna** to the **SMA connector** (6).



3. **Insert an activated SIM card** to the SIM slot (2) - the SIM chip surface must be look to top and the cutted edge of the SIM must be look to the DCU – then push the SIM until it will be fixed and closed (you will hear a soft click sound).
(In case of necessary of SIM removal you have to power off the DCU and push the SIM a bit, while it will be released and can be removed).
4. **Connect an UTP cable** to the device's **Ethernet** titled RJ45 port (6). During the configuration the cable's opposite connector must be connected to the PC's Ethernet port. (After the configuration connect it to the network- or industrial device's RJ45 port.)
5. Connect the RS485 device, Modbus meter, etc- to the **RS485** port (8) to receive the data of the external device or meter.

6. Connect Mbus device(s) you want to read out to the **MBus** port (9) to receive the data of the external device(s). Max. 30 Mbus slave devices can be used at the same time.
7. You can also configure the DCU through the **micro-USB slot** (4) by a microUSB-USB cable of the PC connection.

Important! By connecting the micro-USB cable, the device will be powered on, because it can be operated from 5V DC power alternatively (instead of connecting the 12V DC to the Microfit power connector).

5.2 First start

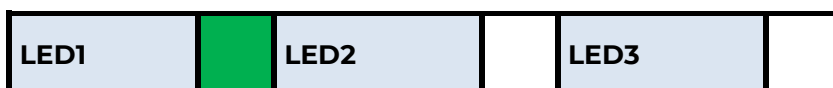
The DCU is provided with pre-installed system (which contains the operating firmware and OpenWrt® system, which are accessible on local website of the device).

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

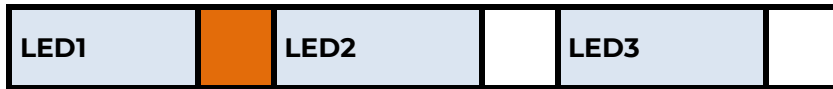
9-32V DC power voltage input (interface nr. 1) should be used by the DC powering with microfit connection 12V DC power adapter, or similar source.

Alternatively you can use the micro-USB cable to provide 5V DC power for the DCU's operation.

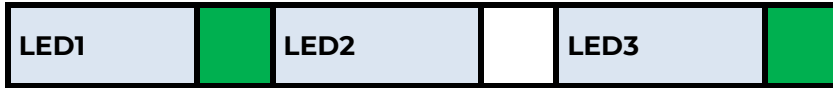
2. **When powering the device on**, the **LED1** will be lighting with **green** color, which means that systems start has began and the charging of the supercapacitors also have started.



3. Later, during the boot, the **LED1** will be lighting with **green** and also flashing with **red** color (which can be perceived as flashing with **orange**).



4. When the system will be ready to use, then **LED1** and **LED3** will be also lighting continuously by **green**.



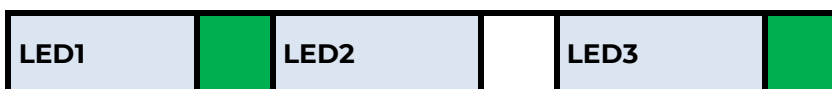
5. The system start requires about 2 minutes, while the device loads the necessary modules and prepares the web configuration user interface, while the system is ready to login.

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

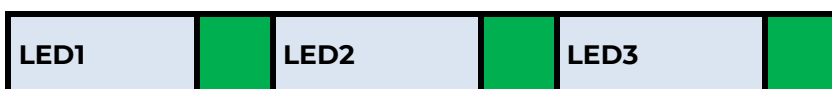
Attention!

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

7. The module registration to the cellular network is signed by the **LED3** flashing with **green** after the settings.



8. If the cellular network SIM card registration was succesful, then the **LED2** will be also active by continous lighting by **green**, which shows that the DCU can access the cellular network already.



9. If you notice an unusual LED activity or other operation misbehaviour symptoms, read the *Troubleshooting* chapter.
10. If you'd like to make the DCU settings via **USB connection** (micro-USB port) then install the **USB Ethernet / RNDIS Gadget** driver to your computer by using your web browser: https://m2mserver.com/m2m-downloads/RNDIS_win10.ZIP

5.3 Web user interface of the DCU

1. To connect to the DCU, allow the device IP address for the Ethernet connector interface in the Windows®'s network settings (IP address for Ethernet connection: 192.168.127.100, Subnet mask: 255.255.255.0)
2. In case of USB connection, you have to setup the **USB Ethernet / RNDIS Gadget** virtual interface to the following IP: 192.168.10.100, subnet mask: 255.255.255.0
3. Open the DCU's local website in internet browser. Default web user interface (LuCi) on **Ethernet** port it's <https://192.168.127.1> on **USB port** it's <https://192.168.10.1>

Warning: Potential Security Risk Ahead

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

What can you do about it?

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

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

[Learn more...](#)

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

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

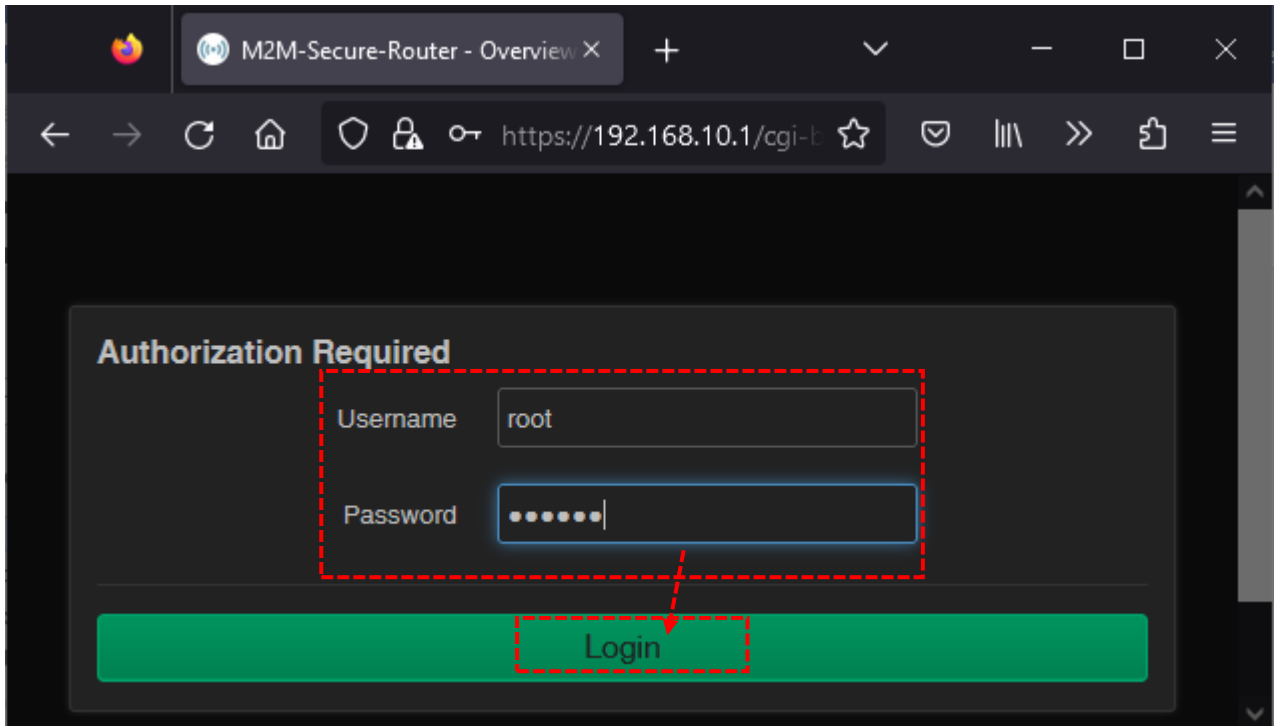
Websites prove their identity via certificates. Firefox does not trust 192.168.10.1:8888 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: `SEC_ERROR_UNKNOWN_ISSUER`

[View Certificate](#)

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

- At the first time, you have to accept the security risk in the browser by choosing the **Advanced** option at the **Potential Security Risk** and Then choose „**Accept the Risk and Continue**” option.
- Then the DCU’s local web interface will be loaded and you can login.
 - **Username: root**
 - **Password: wmrpwd**



- Push to the **Login** button.

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

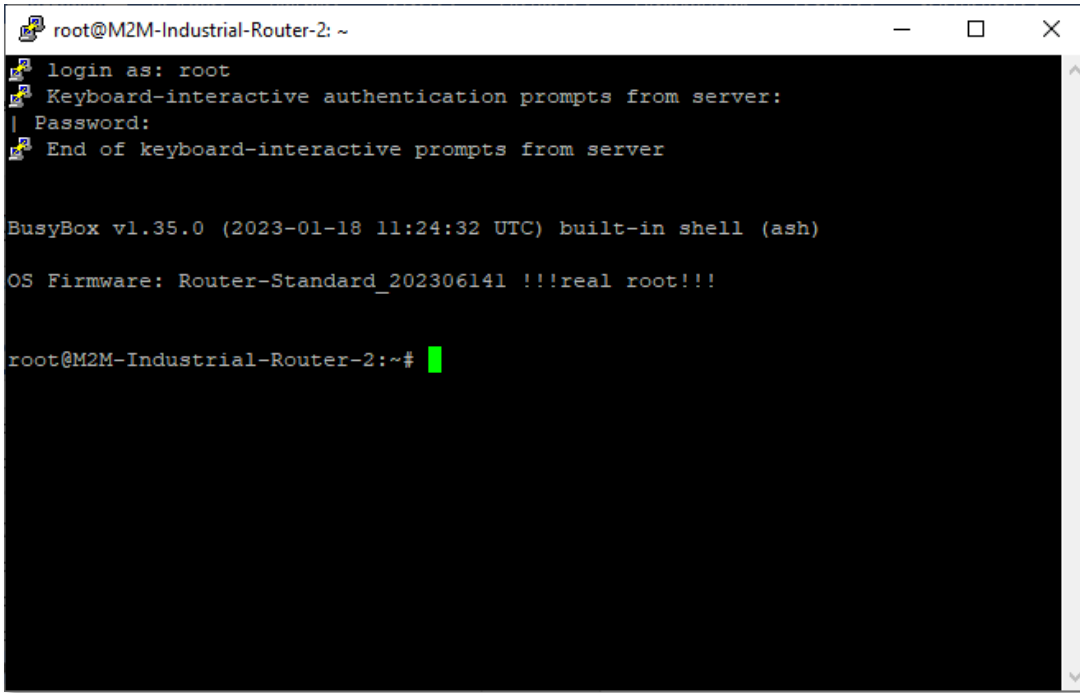
5.4 Access via SSH connection

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

- Connect to the **192.168.10.1:222** IP address.
(Login: **root**, Password: **wmrpwd**)

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

Then the Linux command line will appear, where you can use standard Uc Linux kernel 5.10 compatible commands and execute scripts on the device.



```
root@M2M-Industrial-Router-2: ~  
login as: root  
Keyboard-interactive authentication prompts from server:  
| Password:  
End of keyboard-interactive prompts from server  
  
BusyBox v1.35.0 (2023-01-18 11:24:32 UTC) built-in shell (ash)  
OS Firmware: Router-Standard_202306141 !!!real root!!!  
  
root@M2M-Industrial-Router-2:~#
```

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

To review the UCI commands and options that can be used, we recommend to read UCI Reference Guide, which can be downloaded from our website.

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

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

```
#uci show service_name
```

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

Chapter 6. Web Administration user interface

6.1 Dashboard (Main page)

After login to the web interface, the startup screen appears with the current status of the DCU. At the **System** part you can check that the **Firmware version**. It should be 202401221 or newer version.

The screenshot displays the web administration interface for 'M2M-Industrial-Router-2'. The top navigation bar includes 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout', with a 'REFRESHING' button on the right. The main content is divided into three sections: 'System', 'Memory', and 'Modem'. The 'System' section lists various parameters such as Hostname, Model, Firmware Version (202401221), Architecture, Target Platform, Kernel Version, STM32 Firmware, Local Time, Uptime, and Load Average. The 'Memory' section features four horizontal progress bars representing Total Available, Used, Buffered, and Cached memory usage. The 'Modem' section lists details like Modem Model, Firmware Version, Serial, IMSI, SIM ID, Operation Mode, and Operator.

System	
Hostname	M2M-Industrial-Router-2
Model	Router-Standard
Firmware Version	202401221
Architecture	ARM926EJ-S rev 5 (v5I)
Target Platform	at91/sam9x
Kernel Version	5.10.184
STM32 Firmware	202307121
Local Time	2024-02-01 15:28:09
Uptime	0h 11m 52s
Load Average	2.86, 1.05, 0.46

Memory	
Total Available	57.37 MiB / 118.86 MiB (48%)
Used	78.77 MiB / 118.86 MiB (66%)
Buffered	13.49 MiB / 118.86 MiB (11%)
Cached	45.86 MiB / 118.86 MiB (38%)

Modem	
Modem Model	SIMCOM_SIM7070
Firmware Version	Revision:1951B12SIM7070
Serial	868110060091392
IMSI	216012315089768
SIM ID	8936200003150897683f
Operation Mode	Online
Operator	Yettel HU

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

At the **Modem** part you will find the SIM info (**SIM ID**). There the **Operation mode** and **Access Technology** values will inform you about the current status of the cellular connection.

There you can identify the **Operator** information, cellular **Network registration**, **Network code** and **Network Cellid** (cell identifier).

The screenshot displays a network status interface with the following sections:

- Access Technology:** 7 (LTE CAT-M1)
- CSQ/RSSI:** 19 (-76dBm)
- CSQ/BER:** 99
- MCC-MNC:** 216-01
- Network Registration:** 1
- Network Code:** -
- Network Cellid:** -

Storage

- Disk space:** 46.20 MiB / 487.21 MiB (9%)
- Temp space:** 528.00 KiB / 59.43 MiB (0%)

Network

IPv4 Upstream

- Protocol: PPP-4G
- Address: 10.255.228.248/32
- Gateway: 10.84.84.84
- DNS 1: 192.168.1.225
- Connected: 0h 11m 12s
- Device: Tunnel Interface: "4g-wan"

Active Connections: 128 / 15360 (0%)

Powered by LuCI branch (git-22.292.53764-34d4bb8) / OpenWrt SNAPSHOT r0-aeff2f03

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

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

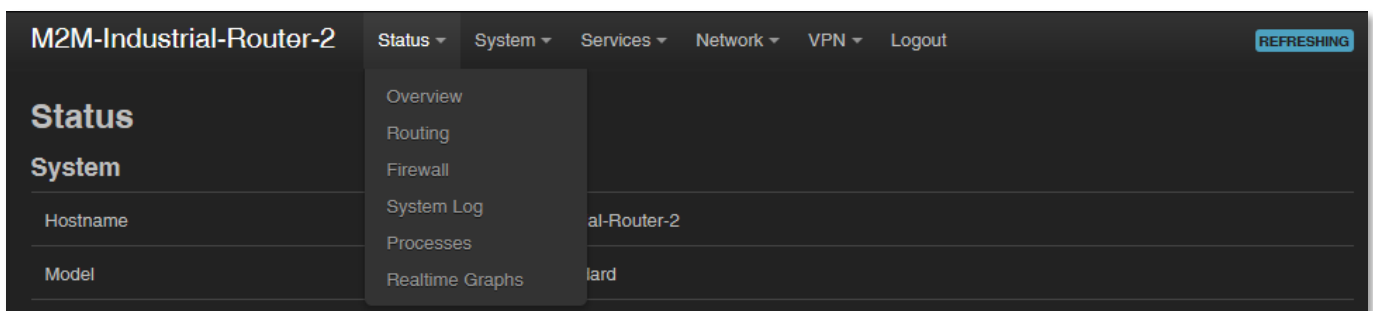
6.2 Menu

By the menu you can access the following features:

- **Status** – Status data, operation and system log, operation monitoring
- **System** – System settings, administration, software and firmware refresh, backup/restore of the configuration settings, LED configuration, reboot, etc.
- **Services** – Dynamic DNS settings, ser2net settings (RS485), Data Collection (RS485 Modbus and Mbus settings, PLC registers)
- **Network** – Network interface settings, DHCP, DNS, IP route rules (static routes), diagnostics, Firewall, voice call config, SMS config
- **VPN** – OpenVPN settings

6.3 Status menu

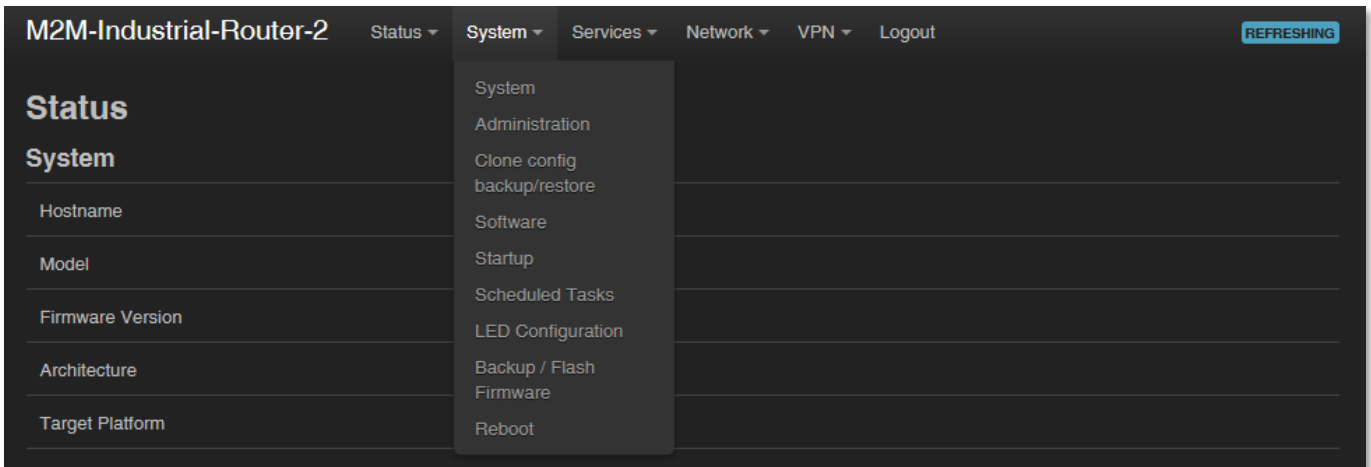
- In the **Status** you can check the current status (**Overview**),
- at the **Routing** item the valid/active route settings,
- at the **Firewall** item, you can see the firewall events and information,
- check the system messages and event log (**System Log**)
- activities of the device (**Processes**)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



6.4 System menu

You can find several system settings in these menu items:

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

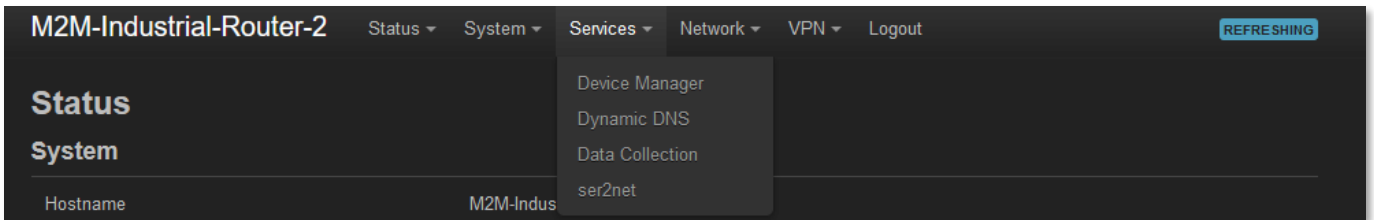


- **Clone config backup / restore** – here you can make a file of the current settings which can be distributable to an another DCU device
- Installation of further **Software** (3rd party tools, applications) from the online software repository
- You can setup **Startup** applications and services during the operation (start/stop them)
- You also can define **Scheduled Tasks** for starting them in the right time and sequence
- The **LED Configuration** is also configurable.
- You also can **Backup / Flash firmware** updates (save system configuration and refresh system FW)
- **Reboot** the device

The **Save** button stores the settings and reconfigure the DCU related on these settings.

6.5 Services menu

- **Device Manager** menu to configure the management server settings
- Here you can setup the **DynDNS** (dynamical DNS) service settings
- **Data collection** menu, where you can setup the Modbus, PLC and Mbus data collection properties
- In the **Ser2net** menu you can configure RS485 operation settings



6.6 Network menu

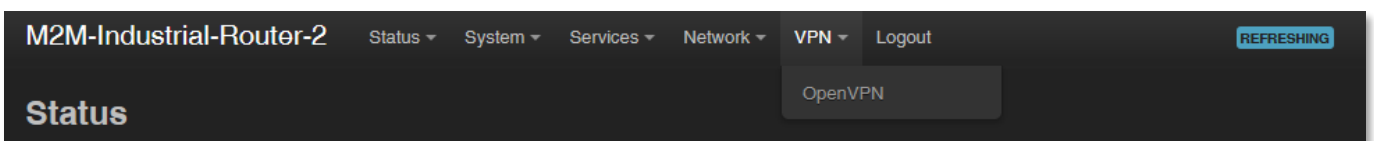
- Here you can configure the settings of each network **Interfaces**.
- **Routing** – static route paths can be also defined here.
- You can modify the **DHCP and DNS** settings.



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

6.7 VPN menu

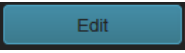
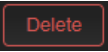
- Define the **OpenVPN** client VPN tunneling connection settings.



Chapter 7. Important notes

- For security reasons, we do recommend to **change the password** immediately for accessing the administration user interface (local webpage). Read Chapter 9.6 for detailed settings.
- Some protocols are disabled by default on the DCU, but most of them you can enable to use:
 - The **DHCP** service is turned off by default. When enabled, the DCU assigns IP addresses to connected devices, while the available Ethernet interface addresses use **static** addresses. If you want to assign IP addresses by DHCP, change the protocol value to **DHCP client**. You can do this in the **Network / DHCP and DNS settings** menu or under the **Network / Interfaces** menu, in the **LAN** interface, in the **DHCP** section.
 - The **IPSec** service is disabled by default, but you can enable the service. Read Chapter 9.7 for detailed settings.
 - The **OpenVPN** service is disabled by default, but you can enable the service. Read Chapter 9.8 for detailed settings.
 - The **Ser2Net** (RS485/Modbus) service is disabled by default, but you can enable the service. Read Chapter 9.9 for detailed settings.
 - The Modbus / Mbus data acquisition feature can be activated and configured in the **Services / Data Collection** menu.
- Some protocols are disabled by default on the DCU and you cannot use them, but you can make a request and indicate your requirement before ordering:
 - The **IPv6** protocol is disabled for **LAN** and **USBLAN** interfaces by default.
- Notes on Firewall service:
 - The **Firewall** feature is enabled by default (for security reasons), which means that all communications are disabled except Ethernet, DHCP, DNS, and WAN channels, the web port, and services and ports that are required for normal, normal, and general operation.
 - **Note, that enabling of the firewall service does not protect the device from external DoS attacks and unauthorized intrusions. For reliable operation, review settings and enable only the necessary channels.**
 - We do recommend to disable all ports and protocols in the **Firewall** that you are not currently using (connection / channel / data transfer) taking

into account access to the required ports and channels. To check this, the **Status / Firewall** menu section is an excellent option for scanning through traffic and the **Network / Firewall** menu, where you can add new rules or modify existing ones.

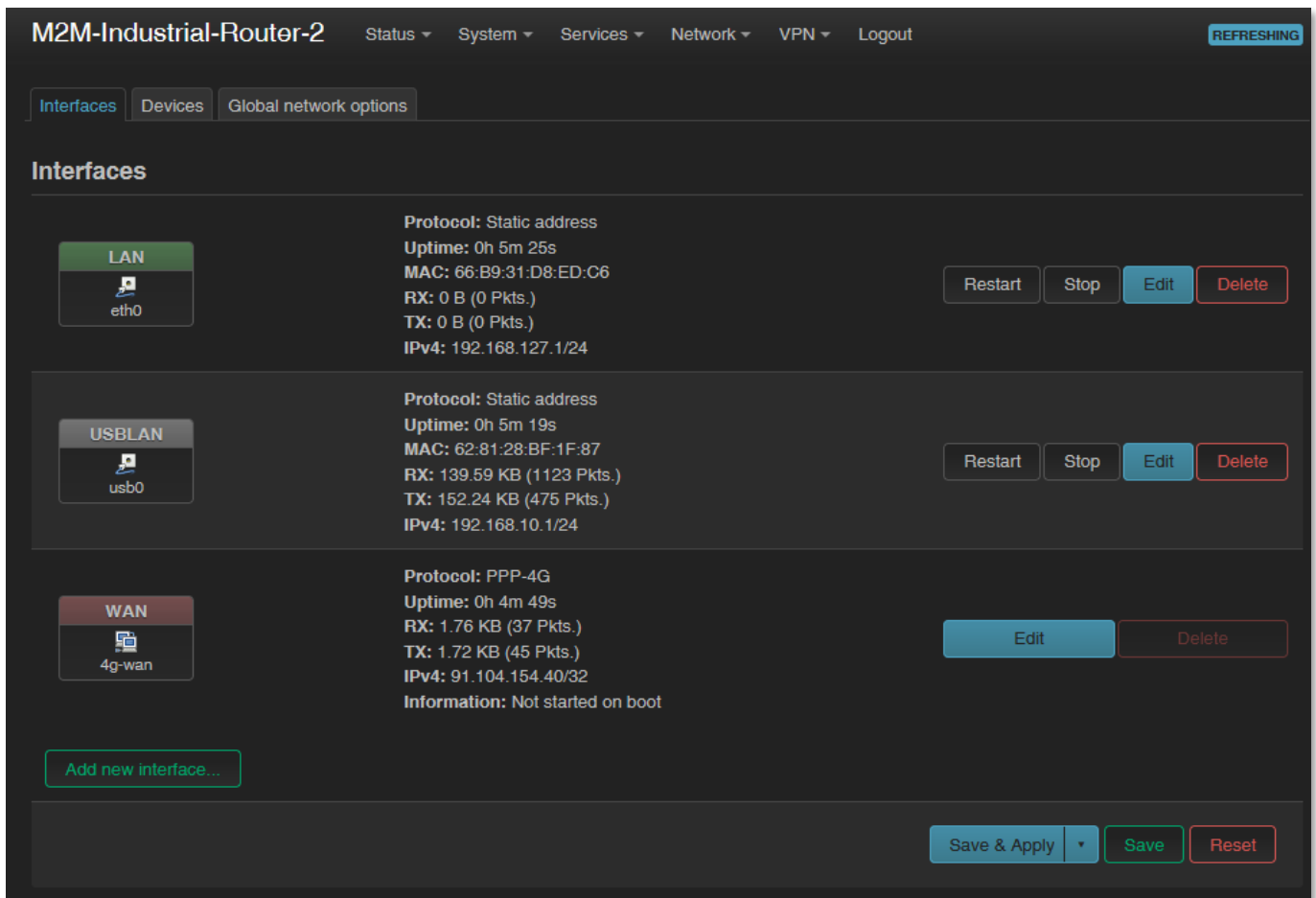
- Please check the network traffic of the DCU frequently in the **Status / Firewall** menu (port number, incoming IP, especially outgoing data traffic and downloaded data).
- Measure throughput and network traffic (per minute, per hour) - with the help of the **Status / Realtime Graphs** menu or **Statistics / Graphs** where you can view the calculated and expected traffic volumes, which is important if you want to avoid congestion. or the data traffic limit of the SIM card used is limited.
- If necessary, you can select a dedicated mobile network type (such as LTE only, GSM only (2G)), or you can use automatic mode (which connects to the fastest network type currently available). This allows you to limit the baud rate (and volume) with the manual settings. You can set this in the **Network / Interfaces** menu on the **WAN** interface by clicking the  button.
- The parameters that can be used for the APN settings are always provided by the SIM card issuer (mobile service provider). Contact them for **APN**, **SIM PIN**, **PAP/CHAP username**, **PAP/CHAP password** and other information.
- The device constantly checks the interfaces and the viability of the connections. In case of the power failure or power failure event, the network and data connections are automatically reconnected after conditions are restored.
- The **RS485** data speed can be set between 300 and 19 200 baud on the web interface. We recommend to you use 9 600 baud (for general industrial devices), 1 200 or 2 400 baud (for utility meters) for better compatibility.
- If you do not want to use the DCU on a mobile network, but as a wired Ethernet and RS485 data concentrator, then configure that in the **Network / Interfaces** menu, remove the **WAN** interface with the  button. From then on, the device will not be restarted even if no SIM card is inserted.
- **HTTP**, **HTTPS** redirect and HTTPS certifications and **SSL** certifications are used.

Chapter 8. Network configuration of the DCU

8.1 Interface settings

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

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



Modifying the LAN interface settings

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

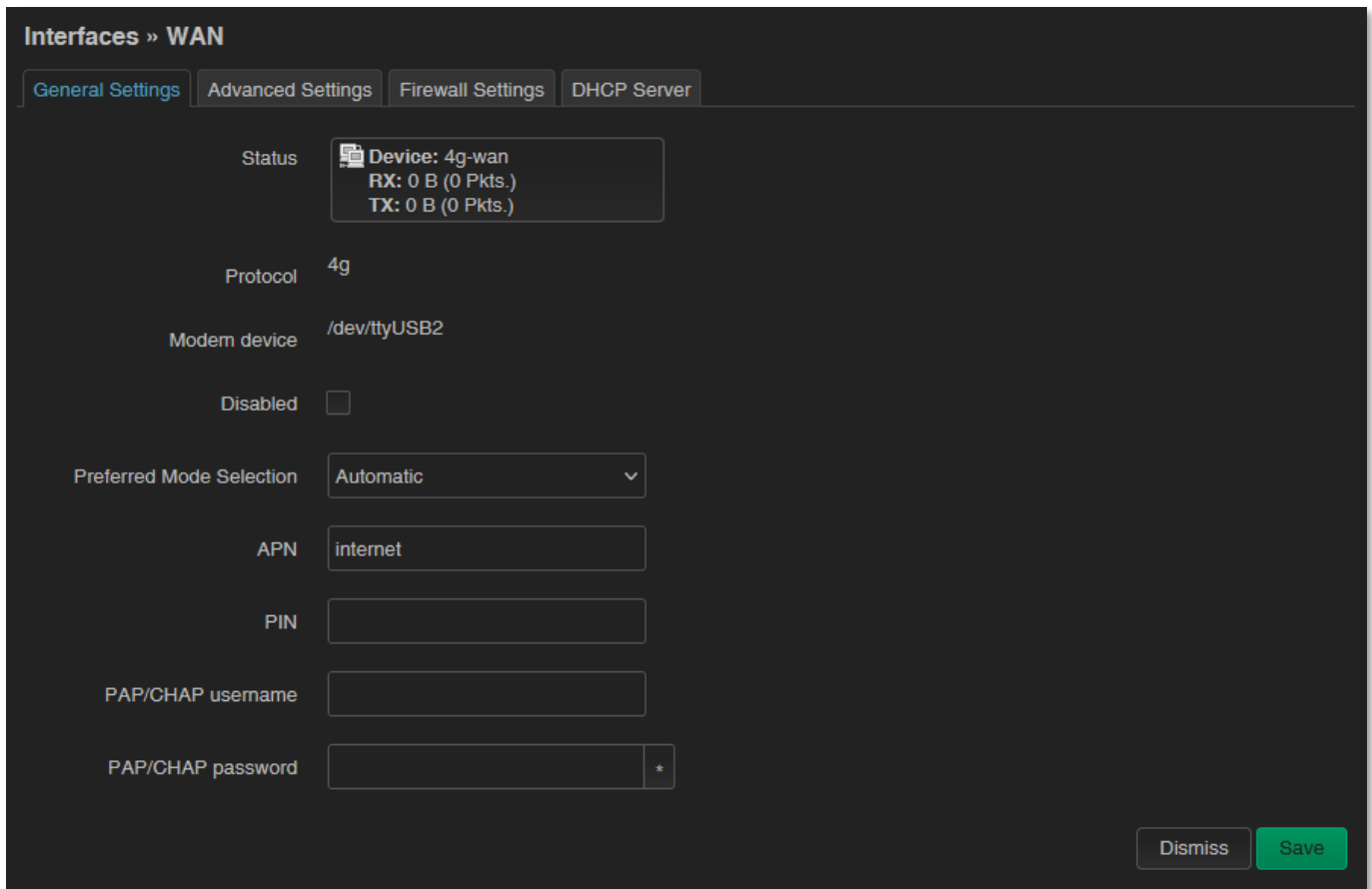
The **Stop** button stops the communication on the current interface, the **Restart** button reconnects the related interface connection.

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

8.2 Cellular / mobile internet settings

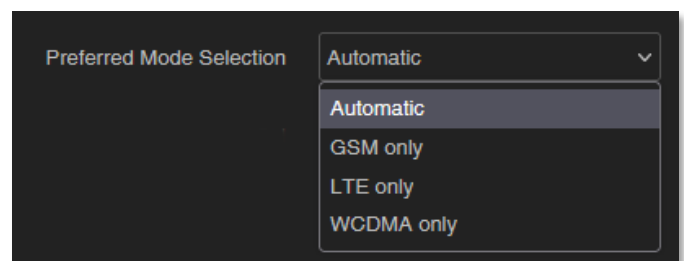
Open the **WAN** item from the upper selection. Then at the **General Settings** tab you can see the current status of the interface and the transmitted data amount.

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



The screenshot shows the 'Interfaces » WAN' configuration page. It has four tabs: 'General Settings' (selected), 'Advanced Settings', 'Firewall Settings', and 'DHCP Server'. The 'Status' section shows 'Device: 4g-wan', 'RX: 0 B (0 Pkts.)', and 'TX: 0 B (0 Pkts.)'. The 'Protocol' is set to '4g'. The 'Modem device' is '/dev/ttyUSB2'. There is a 'Disabled' checkbox which is unchecked. The 'Preferred Mode Selection' is a dropdown menu currently set to 'Automatic'. Below it are input fields for 'APN' (containing 'internet'), 'PIN', 'PAP/CHAP username', and 'PAP/CHAP password' (with a password mask). At the bottom right are 'Dismiss' and 'Save' buttons.

Preferred Mode Selection field – we suggest to use the **Automatic** option, which will force the module to connect to the last time used network connection type. But, you can also choose **LTE only** (LTE or Cat.M/Cat.NB) or **GSM only** (2G), etc. modes. Choose a cellular access technology!



This is a close-up of the 'Preferred Mode Selection' dropdown menu. The menu is open, showing the following options: 'Automatic' (highlighted), 'GSM only', 'LTE only', and 'WCDMA only'.

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

Attention!

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

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

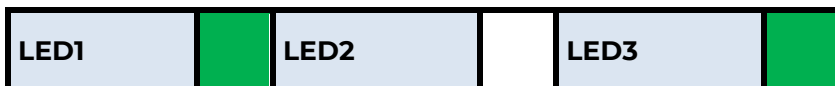
The **PAP/CHAP username** and **PAP/CHAP password** settings can be also configured here – if it is required for the connection.

Attention!

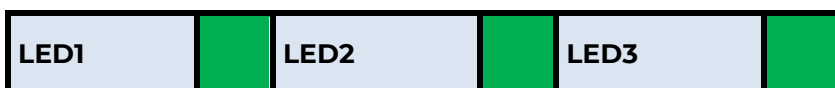
The available APN settings will be provided by the SIM card provider mobile operator or your mobile internet service provider.

Click to the **Save** button for saving the settings, then on the interfaces page click to the **Save & Apply** button. The DCU will attempt to connect to the mobile network.

The module registration to the cellular network is signed by the **LED3** flashing with **green** after the settings.

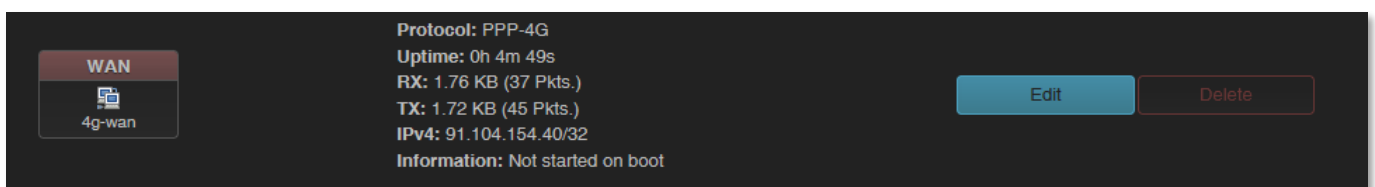


If the cellular network SIM card registration was succesful, then the **LED2** will be also active by continous lighting by **green**, which shows that the DCU can access the cellular network already.




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

After that, check data traffic at **Network / Interfaces** menu for **WAN** interface.

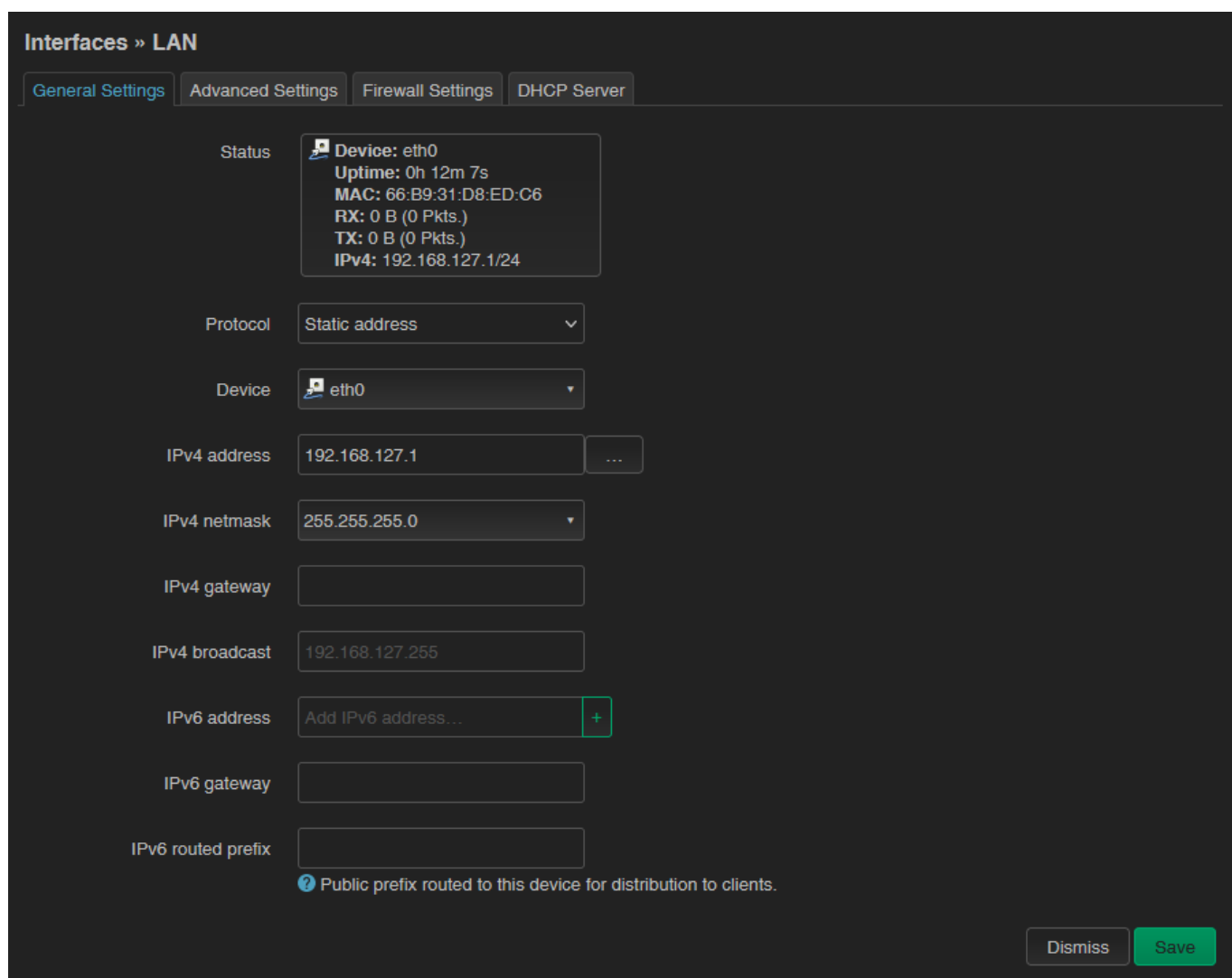


As you can see, the device is connected to the mobile internet network and currently active - **RX** (received data), **TX** (sent data) and **KB** (KBytes) are constantly increasing. You can find further network settings at [Advanced Settings](#) tab.

8.3 Ethernet (LAN) settings

For the **LAN** interface, at the **LAN** menu item at the **Network Interfaces** menu item at the **LAN** interface  button.

On the new screen click to the **General Settings** tab, where you can define an own IP range (**IPv4 address**), with the related **IPv4 netmask** (subnet mask).



The screenshot shows the 'Interfaces » LAN' configuration page. It features four tabs: 'General Settings' (selected), 'Advanced Settings', 'Firewall Settings', and 'DHCP Server'. The 'Status' section displays: Device: eth0, Uptime: 0h 12m 7s, MAC: 66:B9:31:D8:ED:C6, RX: 0 B (0 Pkts.), TX: 0 B (0 Pkts.), and IPv4: 192.168.127.1/24. The 'Protocol' is set to 'Static address'. The 'Device' is 'eth0'. The 'IPv4 address' is '192.168.127.1'. The 'IPv4 netmask' is '255.255.255.0'. The 'IPv4 gateway' is empty. The 'IPv4 broadcast' is '192.168.127.255'. The 'IPv6 address' is 'Add IPv6 address...' with a '+' button. The 'IPv6 gateway' and 'IPv6 routed prefix' are empty. A note at the bottom states: '? Public prefix routed to this device for distribution to clients.' At the bottom right, there are 'Dismiss' and 'Save' buttons.

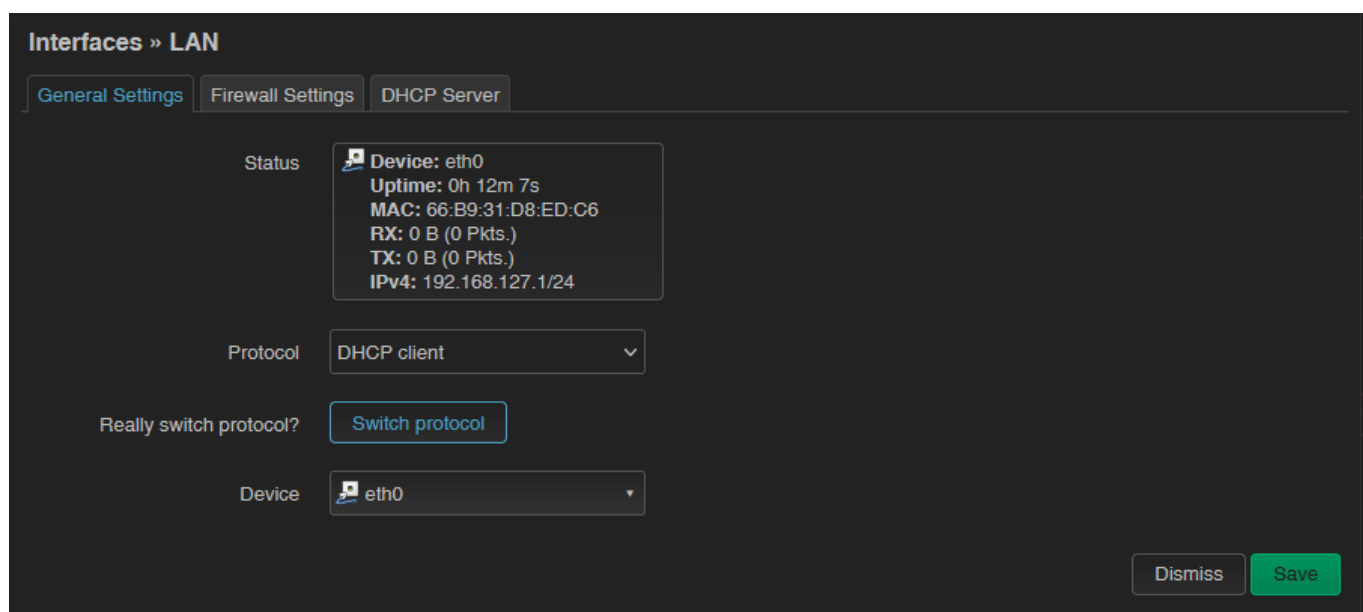
We recommend that you change the device's default `192.168.127.1` address (**IPv4 address**) to a custom IP address, depending on your subnet - or the way you want it to be served by the DCU device.

Also check **IPv4 netmask** field to make sure it is appropriate for the class you want to use.

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

Important! IPv6 service cannot be used, so do not enable or configure the fields that apply to it.

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

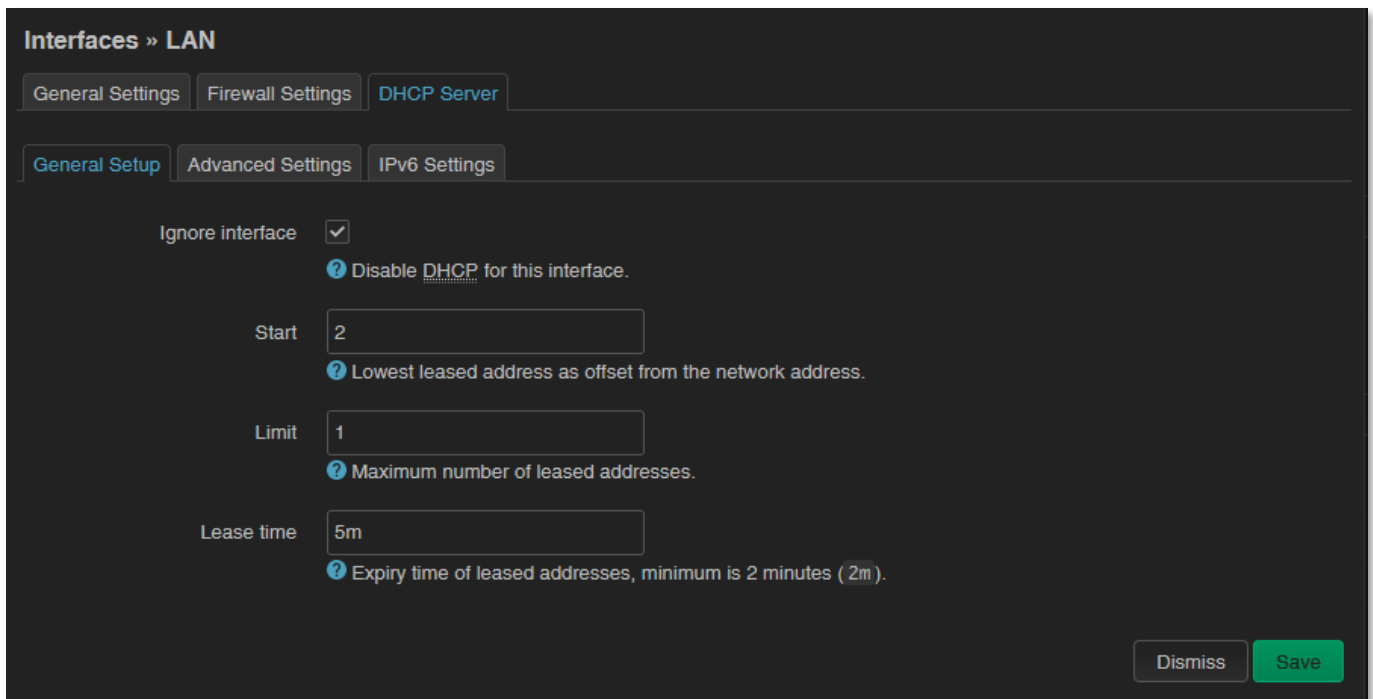


When you have modified the settings, saving them by the **Save** button.

8.4 DHCP, DNS settings

The DHCP service allows the automatic IP address providing for the connecting devices in the current IP segment by the DCU.

The DHCP settings can be found at the **Network / Interfaces** menu (according to the required interface). Choose **DHCP Server** tab for the settings.



The screenshot shows the configuration page for the DHCP Server on a LAN interface. The page has a dark theme. At the top, there are tabs for 'General Settings', 'Firewall Settings', and 'DHCP Server', with 'DHCP Server' being the active tab. Below this, there are sub-tabs for 'General Setup', 'Advanced Settings', and 'IPv6 Settings', with 'General Setup' being active. The main configuration area includes:

- 'Ignore interface' checkbox: checked.
- Help icon and text: 'Disable DHCP for this interface.'
- 'Start' field: contains the value '2'. Help icon and text: 'Lowest leased address as offset from the network address.'
- 'Limit' field: contains the value '1'. Help icon and text: 'Maximum number of leased addresses.'
- 'Lease time' field: contains the value '5m'. Help icon and text: 'Expiry time of leased addresses, minimum is 2 minutes (2m).'

At the bottom right, there are two buttons: 'Dismiss' and 'Save'.

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

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

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

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

Interfaces » LAN

General Settings | Firewall Settings | **DHCP Server**

General Setup | **Advanced Settings** | IPv6 Settings

Dynamic DHCP
 ? Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force
 ? Force DHCP on this network even if another server is detected.

IPv4-Netmask
 ? Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options +
 ? Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

Dismiss Save

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

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

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

General Settings | Resolv and Hosts Files | PXE/TFTP Settings | Advanced Settings | **Static Leases** | Hostnames | IP Sets

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
 Use the *Add* Button to add a new lease entry. The *MAC address* identifies the host, the *IPv4 address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.



Hostname	MAC address	IPv4 address	Lease time	DUID	IPv6 suffix (hex)
<i>This section contains no values yet</i>					

Add

Active DHCP Leases

Hostname	IPv4 address	MAC address	Lease time remaining
<i>There are no active leases</i>			

Save & Apply Save Reset

Here you can  devices to always provide the same dedicated IP address by the device. This can be required by adding values to the **Hostname**, the **MAC-Address** and the **IPv4-Address**. Save your settings by the  button.

8.5 DNS settings

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



DHCP and DNS
Dnsmasq is a lightweight [DHCP](#) server and [DNS](#) forwarder.

General Settings | **Resolv and Hosts Files** | PXE/TFTP Settings | **Advanced Settings** | Static Leases | Hostnames | IP Sets

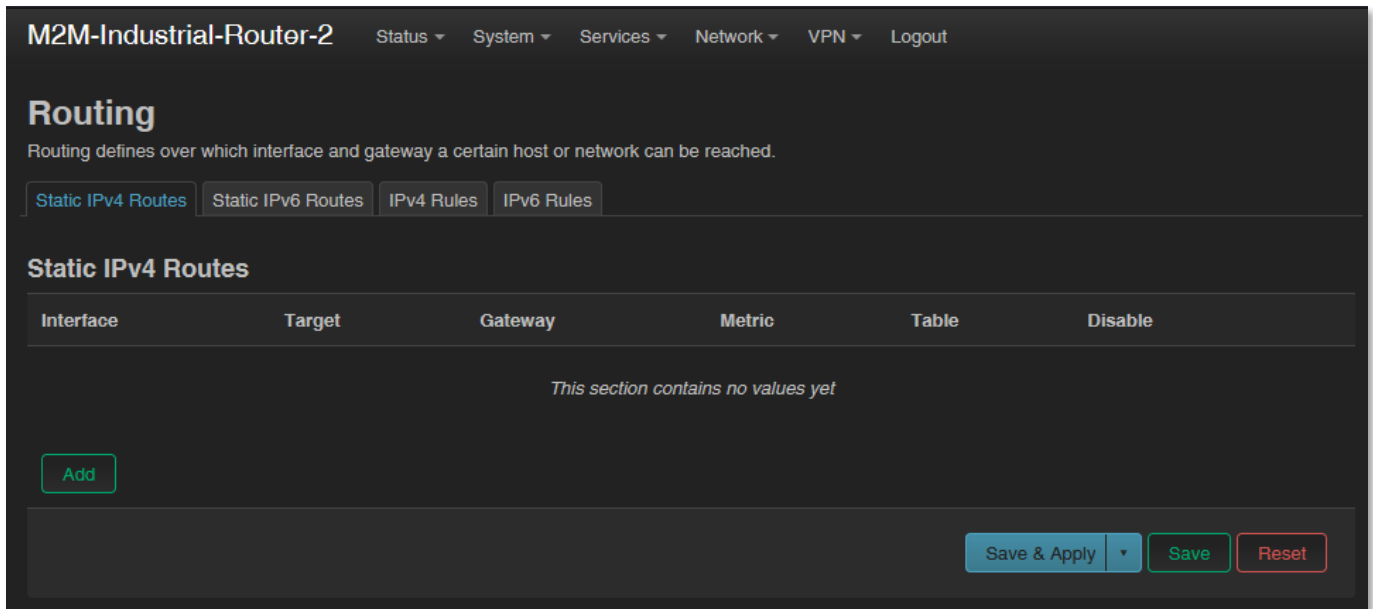
- Suppress logging
 Suppress logging of the routine operation for the DHCP protocol.
- Allocate IPs sequentially
 Allocate IP addresses sequentially, starting from the lowest available address.
- Filter private
 Do not forward reverse lookups for local networks.
- Filter useless
 Avoid uselessly triggering dial-on-demand links (filters SRV/SOA records and names with underscores). May prevent VoIP or other services from working.
- Localise queries
 Return answers to DNS queries matching the subnet from which the query was received if multiple IPs are available.
- Expand hosts
 Add local domain suffix to names served from hosts files.
- No negative cache
 Do not cache negative replies, e.g. for non-existent domains.
- Additional servers file
 File listing upstream resolvers, optionally domain-specific, e.g. `server=1.2.3.4`, `server=/domain/1.2.3.4`.
- Strict order
 Upstream resolvers will be queried in the order of the resolv file.
- All servers
 Query all available upstream resolvers.
- IPs to override with NXDOMAIN 
 List of IP addresses to convert into NXDOMAIN responses.
- DNS server port
 Listening port for inbound DNS queries.
- DNS query port
 Fixed source port for outbound DNS queries.

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

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

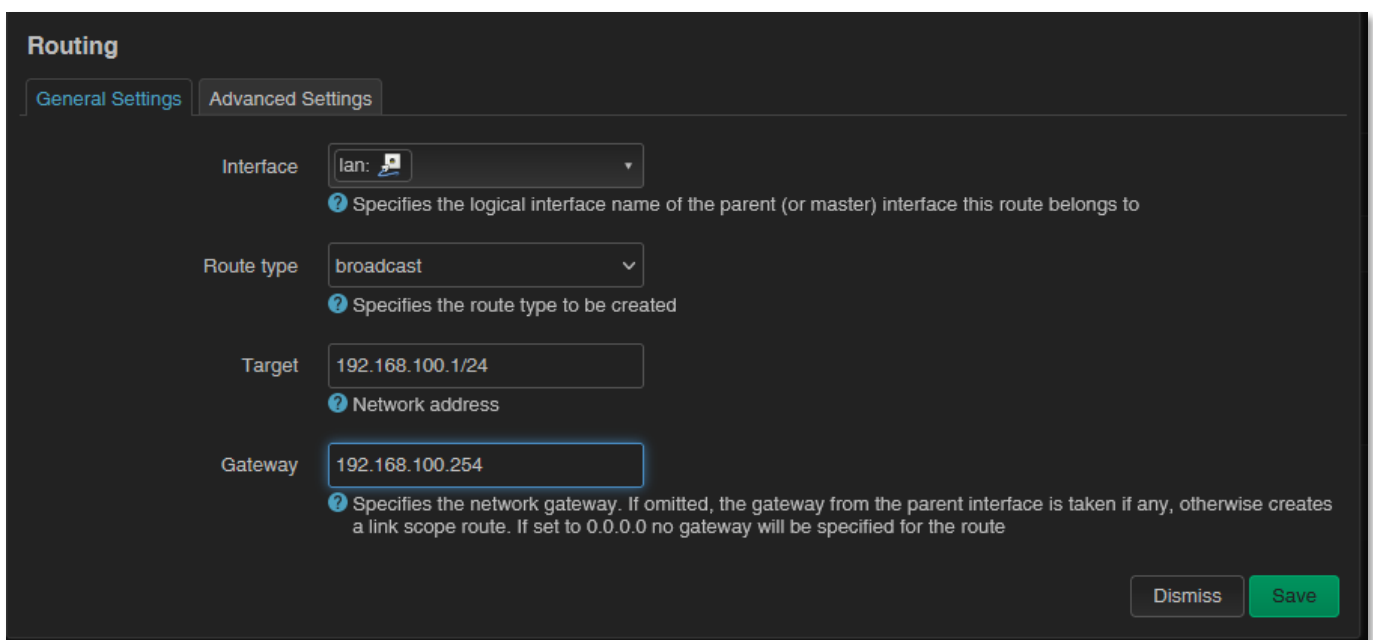
8.6 Defining the route rules

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



You can define a new one by the **Add** button.

These can be performed by choosing the related interface and adding the **Route Type**, the **Target** IP address with Netmask, and **Gateway** IP address.



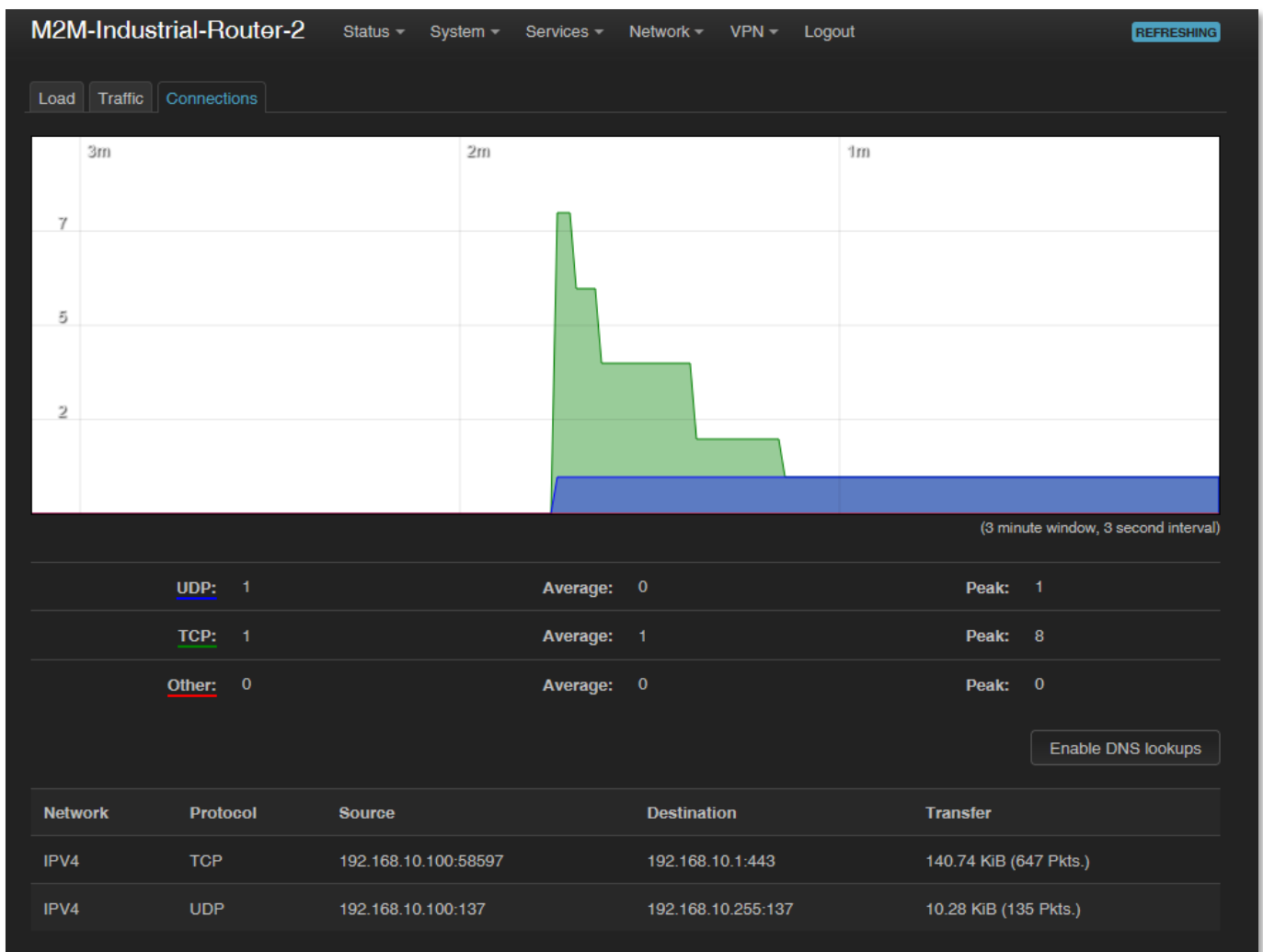
Save the settings by the **Save** button.

8.7 Firewall settings

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

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

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



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

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

Check the valid Firewall rules at **Status / Firewall** menu. Here you can see the rule and direction of each communication channel.

M2M-Industrial-Router-2
Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout
REFRESHING

Firewall Status

IPv4 Firewall
IPv6 Firewall
Hide empty chains
Show raw counters
Reset Counters
Restart Firewall

Table: Filter

Chain INPUT (Policy: *ACCEPT*, 339 Packets, 25.57 KB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
88	7.10 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
2.67 K	372.24 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
2.30 K	345.06 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
76	3.71 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
0	0 B	zone_lan_input	all	eth0	*	0.0.0.0/0	0.0.0.0/0	-	-
37	1.61 KB	zone_wan_input	all	4g-wan	*	0.0.0.0/0	0.0.0.0/0	-	-

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
0	0 B	zone_lan_forward	all	eth0	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_forward	all	4g-wan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	reject	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
-------	---------	--------	-------	----	-----	--------	-------------	---------	---------

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

M2M-Industrial-Router-2 Status System Services Network VPN Logout

General Settings Port Forwards Traffic Rules NAT Rules Custom Rules

Firewall - Zone Settings

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

General Settings

Enable SYN-flood protection

Drop invalid packets

Input: accept

Output: accept

Forward: reject

Routing/NAT Offloading

Experimental feature. Not fully compatible with QoS/SQM.

Software flow offloading

Software based offloading for routing/NAT

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	
lan ⇒ wan	accept	accept	accept	<input type="checkbox"/>	≡ Edit Delete
wan ⇒ REJECT	reject	accept	reject	<input checked="" type="checkbox"/>	≡ Edit Delete

Add

Save & Apply Save Reset

For first, the communication rules are listed here with the directions and operation of the communication rules.

Here, you can see and modify the general rules of the communication, at the **Input** (incoming), **Output** (outgoing) and **Forward** operations one by one by **accept** it, or **reject, drop**.

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

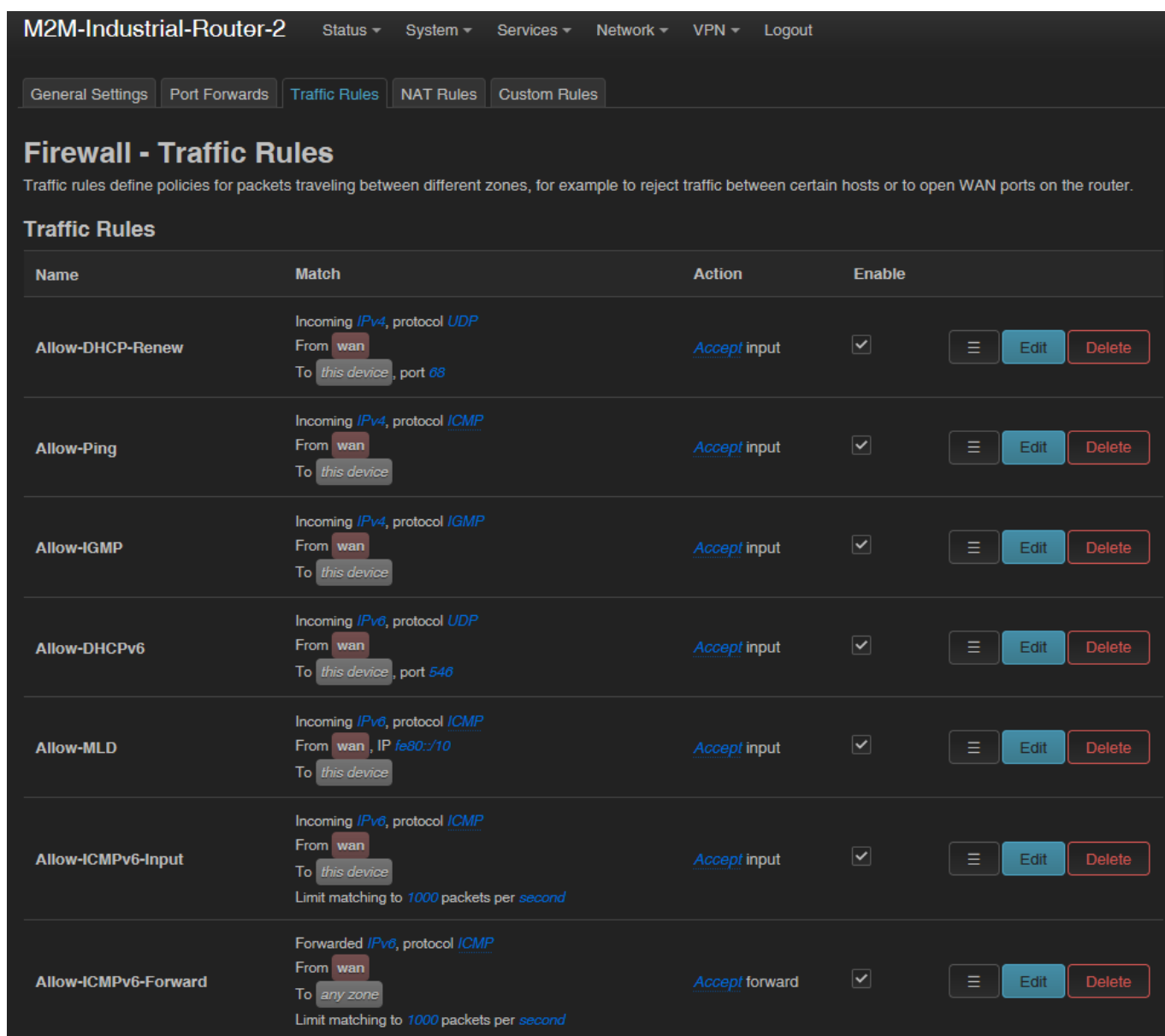
When you want to add a new firewall rule, it must be performed very carefully, because you can disable or tilt ports communication which are used by the DCU or

some network services by general (e.g. Port nr. 67 is necessary for the DHCP service and 80 port for the, port nr. 52 for DNS, port nr. 1194 for OpenVPN, etc).

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

The firewall can be configured by default to allow or disallow the communication – according to the chosen settings. It won't protect the DCU against external network attacks or intrusions when just enabling the firewall feature.

Further port-level filtering or interface traffic limits, or **Traffic Rules** settings are necessary to define! When you have modified the settings, save them by the **Save** button.



M2M-Industrial-Router-2 Status System Services Network VPN Logout

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

Firewall - Traffic Rules

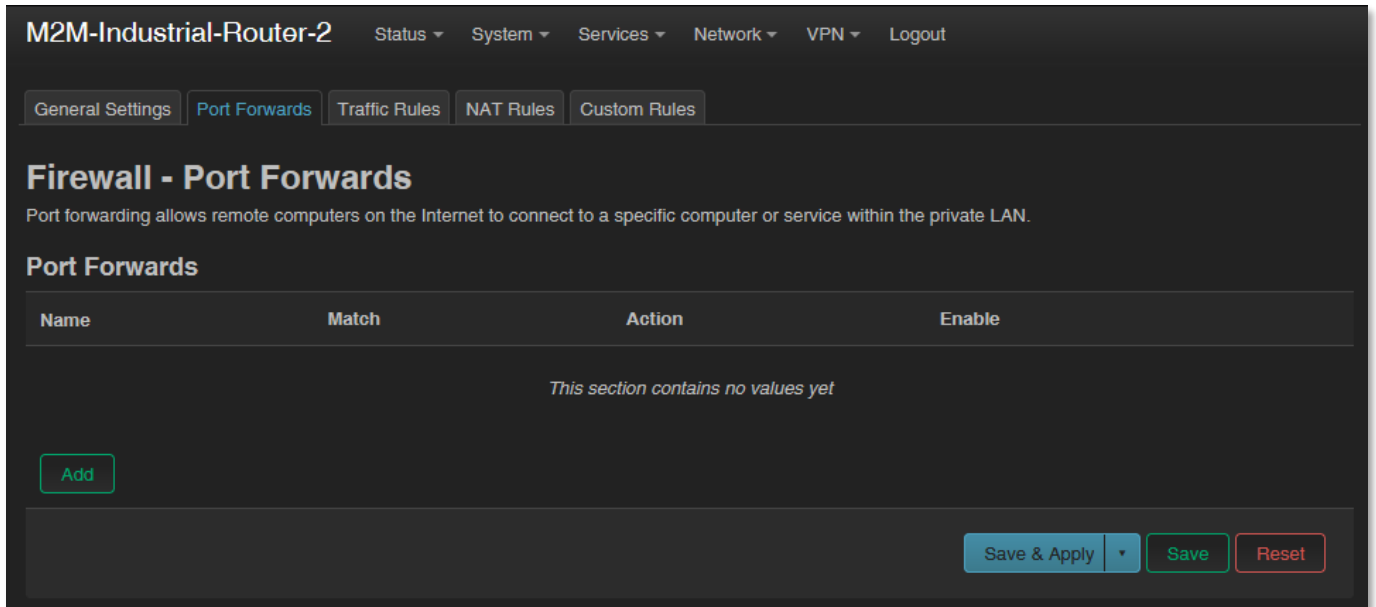
Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

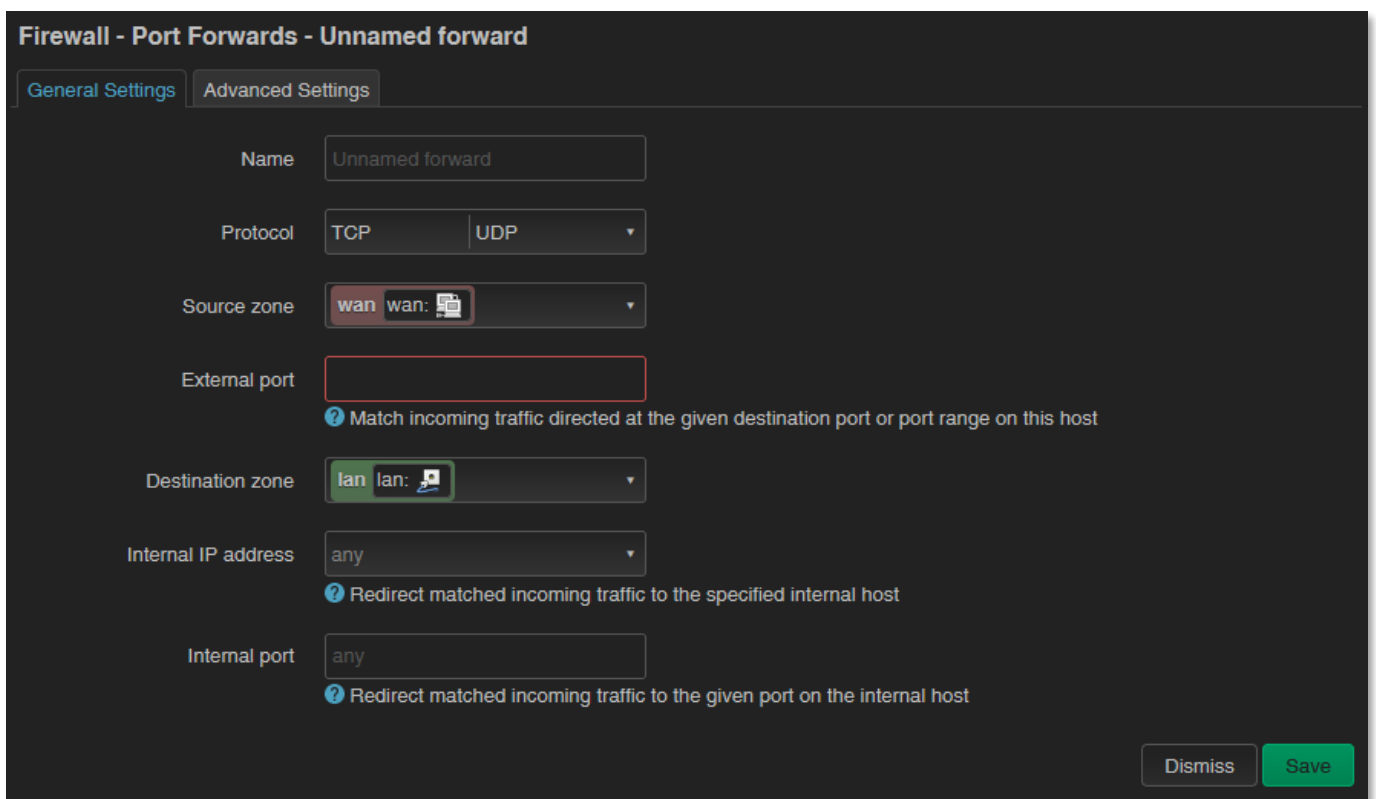
Name	Match	Action	Enable	
Allow-DHCP-Renew	Incoming IPv4, protocol UDP From wan To this device, port 68	Accept input	<input checked="" type="checkbox"/>	☰ Edit Delete
Allow-Ping	Incoming IPv4, protocol ICMP From wan To this device	Accept input	<input checked="" type="checkbox"/>	☰ Edit Delete
Allow-IGMP	Incoming IPv4, protocol IGMP From wan To this device	Accept input	<input checked="" type="checkbox"/>	☰ Edit Delete
Allow-DHCPv6	Incoming IPv6, protocol UDP From wan To this device, port 546	Accept input	<input checked="" type="checkbox"/>	☰ Edit Delete
Allow-MLD	Incoming IPv6, protocol ICMP From wan, IP fe80::/10 To this device	Accept input	<input checked="" type="checkbox"/>	☰ Edit Delete
Allow-ICMPv6-Input	Incoming IPv6, protocol ICMP From wan To this device Limit matching to 1000 packets per second	Accept input	<input checked="" type="checkbox"/>	☰ Edit Delete
Allow-ICMPv6-Forward	Forwarded IPv6, protocol ICMP From wan To any zone Limit matching to 1000 packets per second	Accept forward	<input checked="" type="checkbox"/>	☰ Edit Delete

8.8 Port Forward settings

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



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

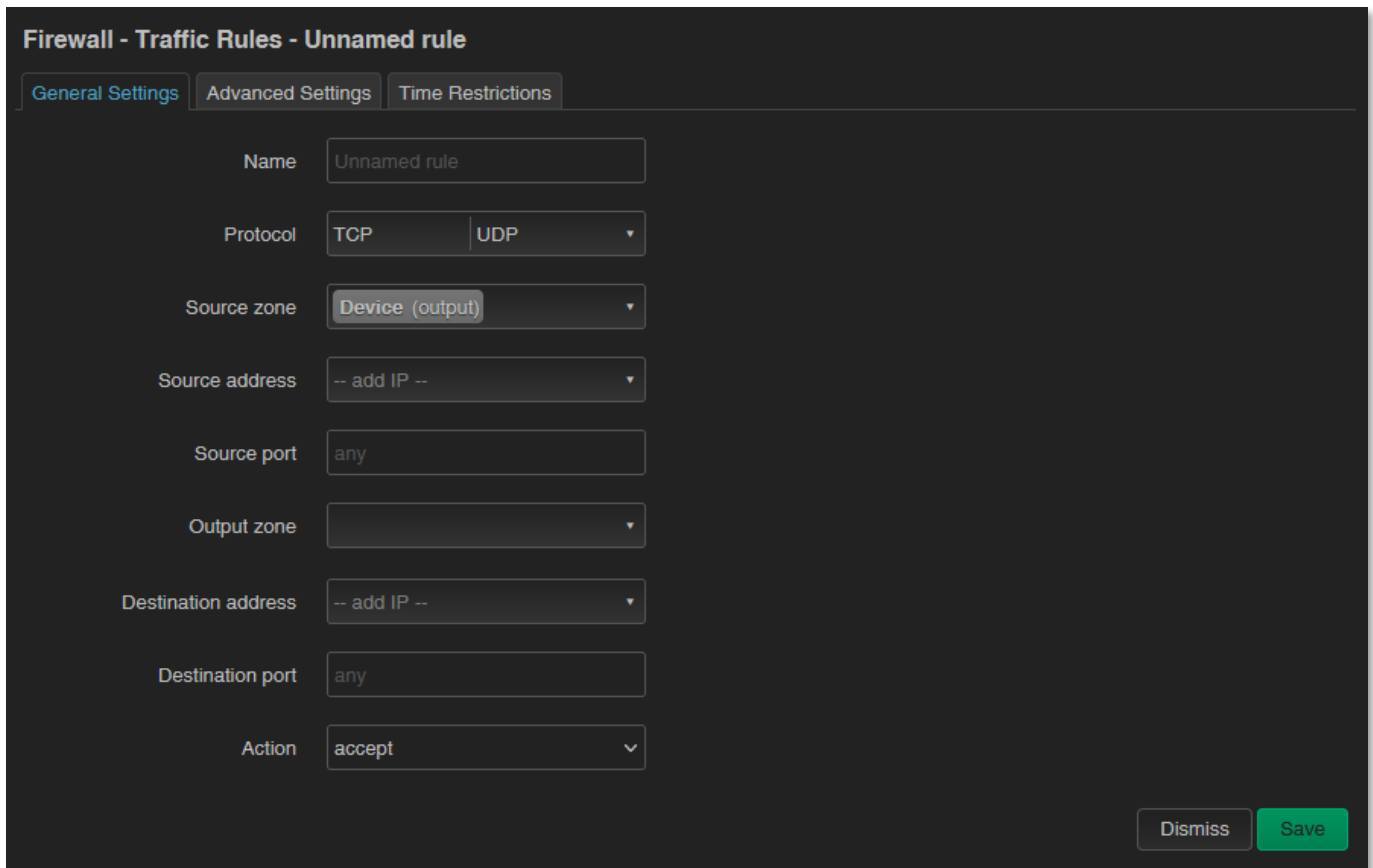


When you have modified the settings, save them by the **Save** button.

8.9 IP routing, NAT settings

In the **Network / Firewall** menu, at **Traffic Rules** tab you can setup the **Traffic Rules**.

You can add a new rule by the  button.



The screenshot shows the configuration page for a new firewall rule. The title is "Firewall - Traffic Rules - Unnamed rule". There are three tabs: "General Settings" (selected), "Advanced Settings", and "Time Restrictions". The form contains the following fields:

- Name: Unnamed rule
- Protocol: TCP | UDP (dropdown)
- Source zone: Device (output) (dropdown)
- Source address: -- add IP -- (dropdown)
- Source port: any
- Output zone: (empty dropdown)
- Destination address: -- add IP -- (dropdown)
- Destination port: any
- Action: accept (dropdown)

At the bottom right, there are two buttons: "Dismiss" and "Save".

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

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

Always set the rules carefully so as not to exclude the possibility of basic communication, and you should also make sure that the DCU remains available on the network, because it is easy to exclude ourselves or just the possibility of remote login. E.g. you should find out about the standard port numbers used by each service (E.g. FTP: port 21, SSH/Telnet: port 222, web: port 80, etc).

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

8.10 Dynamic DNS settings

In the **Services / Dynamic DNS** menu you can allow the DDNS service providing and the IP address of the DDNS.

For first, the Dynamic DNS service should be started by the **Start DDNS** button.

The screenshot shows the 'Dynamic DNS' configuration page. At the top, there is a navigation bar with 'M2M-Industrial-Router-2', 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout'. A 'REFRESHING' indicator is in the top right. The page title is 'Dynamic DNS' with tabs for 'Information' and 'Global Settings'. The 'Information' tab is active, showing the following details:

- Dynamic DNS Version:** 2.8.2-29
- State:** DDNS Autostart disabled. A note explains: 'Currently DDNS updates are not started at boot or on interface events. This is the default if you run DDNS scripts by yourself (i.e. via cron with force_interval set to '0')'. Below this are buttons for 'Start DDNS' and 'Restart DDns'.
- Services list last update:** NO_LIST. Below this is a button for 'Update DDns Services List'.
- Binding to a specific network not supported:** A note states: 'Neither GNU Wget with SSL nor cURL installed to select a network to use for communication. - You should install 'wget' or 'curl' package. - GNU Wget will use the IP of given network, cURL will use the physical interface. - In some versions cURL/libcurl in OpenWrt is compiled without proxy support.'
- DNS requests via TCP not supported:** A note states: 'BusyBox's nslookup and hostip do not support to specify to use TCP instead of default UDP when requesting DNS server! - You should install 'bind-host' or 'knot-host' or 'drill' package for DNS requests.'

Below the information is a 'Services' section with a table:

Status	Name	Lookup Hostname Registered IP	Enabled	Last Update Next Update	
Not Running	myddns_ipv4	yourhost.example.com No Data	<input type="checkbox"/>	Never Stopped	Stop Reload Edit Delete
Not Running	myddns_ipv6	yourhost.example.com No Data	<input type="checkbox"/>	Never Stopped	Stop Reload Edit Delete

At the bottom of the services table is a button 'Add new services...'. At the very bottom of the page are buttons for 'Save & Apply', 'Save', and 'Reset'.

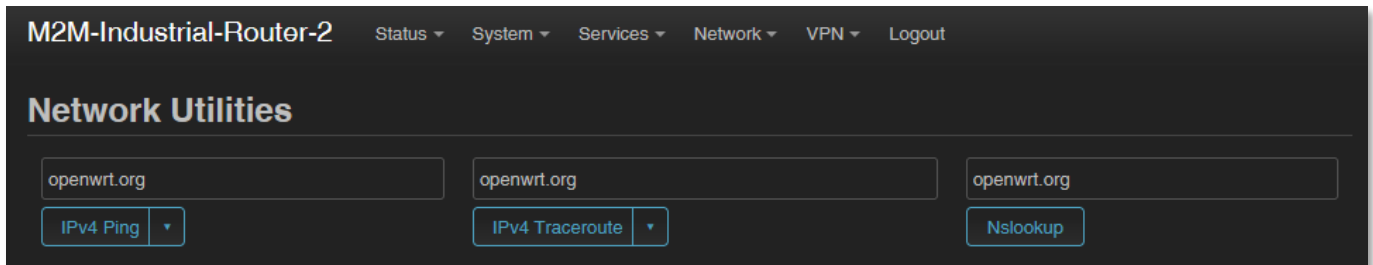
New DDNS entry can be **Add** by the button or the current can be changed by the **Edit** button – even for IPv4 or IPv6.

Save the settings by the **Save** button.

Chapter 9. Special settings

9.1 Ping an IP address

Open the **Network / Diagnostics** menu.



Here you can check the availability of an IP address, that is it accessible or can be pinged (by **IPv4 Ping** button), is there a naming service provided, is there a response between two points (by **Nslookup** button), furthermore the path of the communication (by **IPv4 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

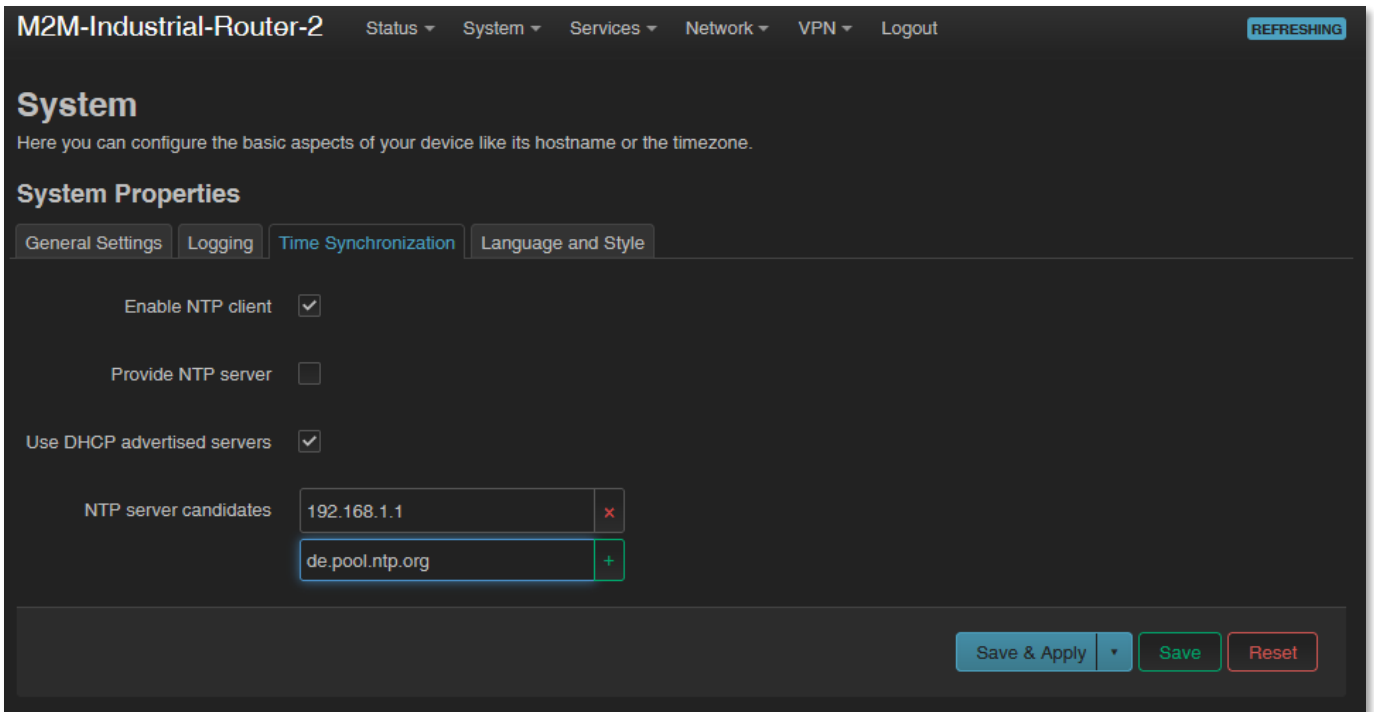
--- lede-project.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 26.848/28.092/29.080 ms
```

Important!

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

9.2 Network Time Service (NTP)

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



Enable or disable the NTP service at the **Enable NTP client** function (when receiving time data) and provide NTP time to connected devices (**Provide NTP server**).

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

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

9.3 TFTP settings

Open the **Network / DHCP and DNS** menu.

Here on the **PXE / TFTP settings** tab you can enable the TFTP server (**Enable TFTP server**) and enter additional information about it.

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

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

M2M-Industrial-Router-2 Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout REFRESHING

DHCP and DNS

Dnsmasq is a lightweight [DHCP](#) server and [DNS](#) forwarder.

General Settings | **Resolv and Hosts Files** | **PXE/TFTP Settings** | Advanced Settings | Static Leases | Hostnames | IP Sets

Enable TFTP server
 ⓘ Enable the built-in single-instance TFTP server.

TFTP server root
 ⓘ Root directory for files served via TFTP. Enable TFTP server and TFTP server root turn on the TFTP server and serve files from TFTP server root.

Network boot image
 ⓘ Filename of the boot image advertised to clients.

Special [PXE](#) boot options for Dnsmasq.

Filename	Server name	Server address	DHCP Options	Network-ID	Force	Instance
<i>This section contains no values yet</i>						

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

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

9.4 LED configuration

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

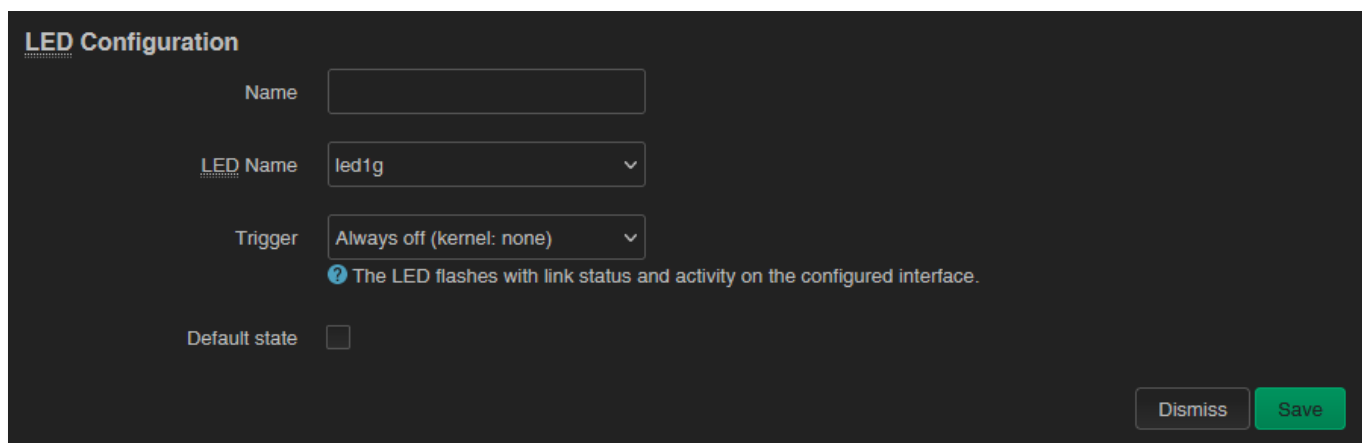
M2M-Industrial-Router-2 Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

LED Configuration

Customizes the behaviour of the device [LEDs](#) if possible.

Name	LED Name	Trigger	
wan	led2g	netdev	<input type="button" value="⋮"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Click to the **Add LED action** button for adding a new LED operation / action rule.



The image shows a dark-themed 'LED Configuration' form. It includes a 'Name' text input field, an 'LED Name' dropdown menu with 'led1g' selected, and a 'Trigger' dropdown menu with 'Always off (kernel: none)' selected. Below the trigger dropdown is a blue help icon and the text 'The LED flashes with link status and activity on the configured interface.' There is also a 'Default state' checkbox which is currently unchecked. At the bottom right, there are 'Dismiss' and 'Save' buttons.

Add a **Name** and choose a **LED Name*** you can select which a **Trigger** you want to set.

*At LED Name you can choose from the selected items, by understanding the following naming convention: **LED_LedNumber_LightingColor**, where:

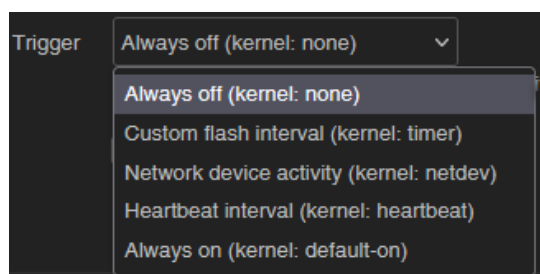
- Number can be: **1** (LED1), **2** (LED2) or **3** (LED3)
- Lighting color can be: **r** (red) or **g** (green)

You can also **Delete** a LED action rule or **Edit** an existing LED setting.

From the **Trigger** list, you can select which event to affect.

You can choose an event type of LED activity from the following list.

Save the settings by the **Save** button.



The image shows a dropdown menu for the 'Trigger' field. The current selection is 'Always off (kernel: none)'. The menu is open, showing the following options: 'Always off (kernel: none)', 'Custom flash interval (kernel: timer)', 'Network device activity (kernel: netdev)', 'Heartbeat interval (kernel: heartbeat)', and 'Always on (kernel: default-on)'.

9.5 Remote access (SSH)

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

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

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

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

SSH connection

The DCU can also be accessed over an SSH connection, with a terminal program (e.g. the software called *putty*), at the IP address of the device - e.g. **192.168.127.1:222** (port nr. 222 on the **Ethernet** port).

The same is possible at **192.168.10.1:222** - for the **USBLAN** port.

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

SSH login:

Login as: root **Password: wmrpwdM2M**

Here you can use micro uCLinux kernel 5.10 compatible commands or execute scripts.

The DCU's operating system uses the embedded Micro uCLinux kernel version 5.10 and interprets **UCI Command line interface** commands - see. For downloadable commands, see the downloadable guide for more information.

9.6 UCI usage from the command line

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

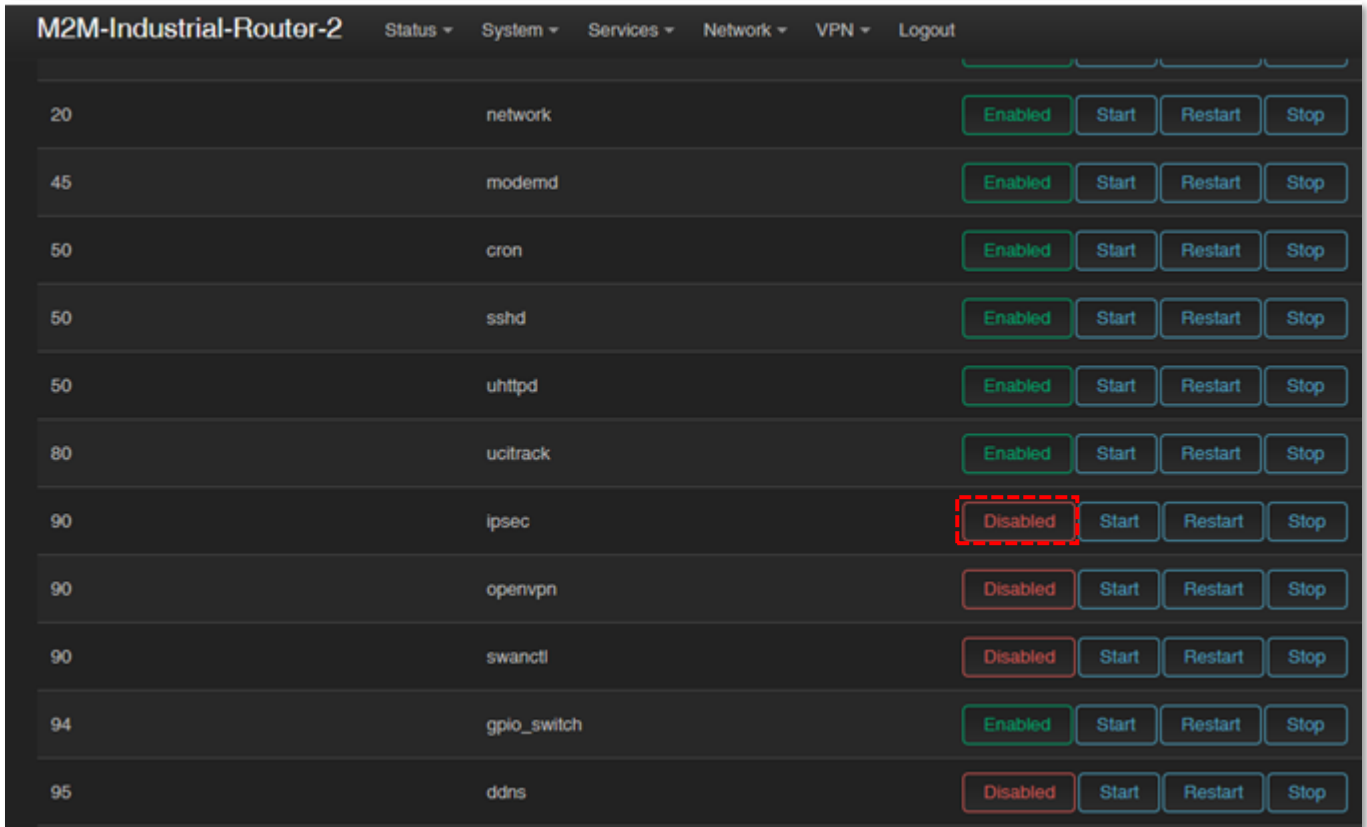
To review the useable UCI commands and options that can be used, we recommend to read the UCI guide, which can be downloaded from our website:

[https:// m2mserver.com/m2m-downloads/UCI_Command_Line_Reference_v3.pdf](https://m2mserver.com/m2m-downloads/UCI_Command_Line_Reference_v3.pdf)

9.7 IPSEC settings

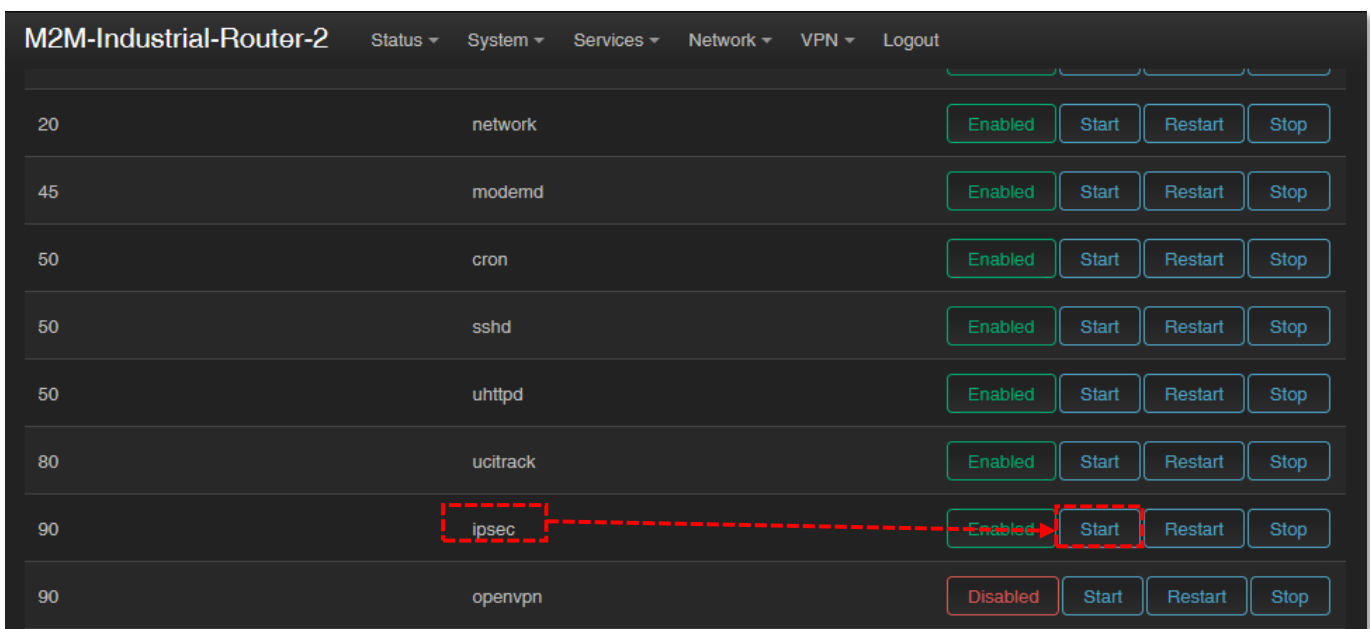
Open the **Systems / Startup** menu to enable *strongSwan* IPsec feature.

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



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

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



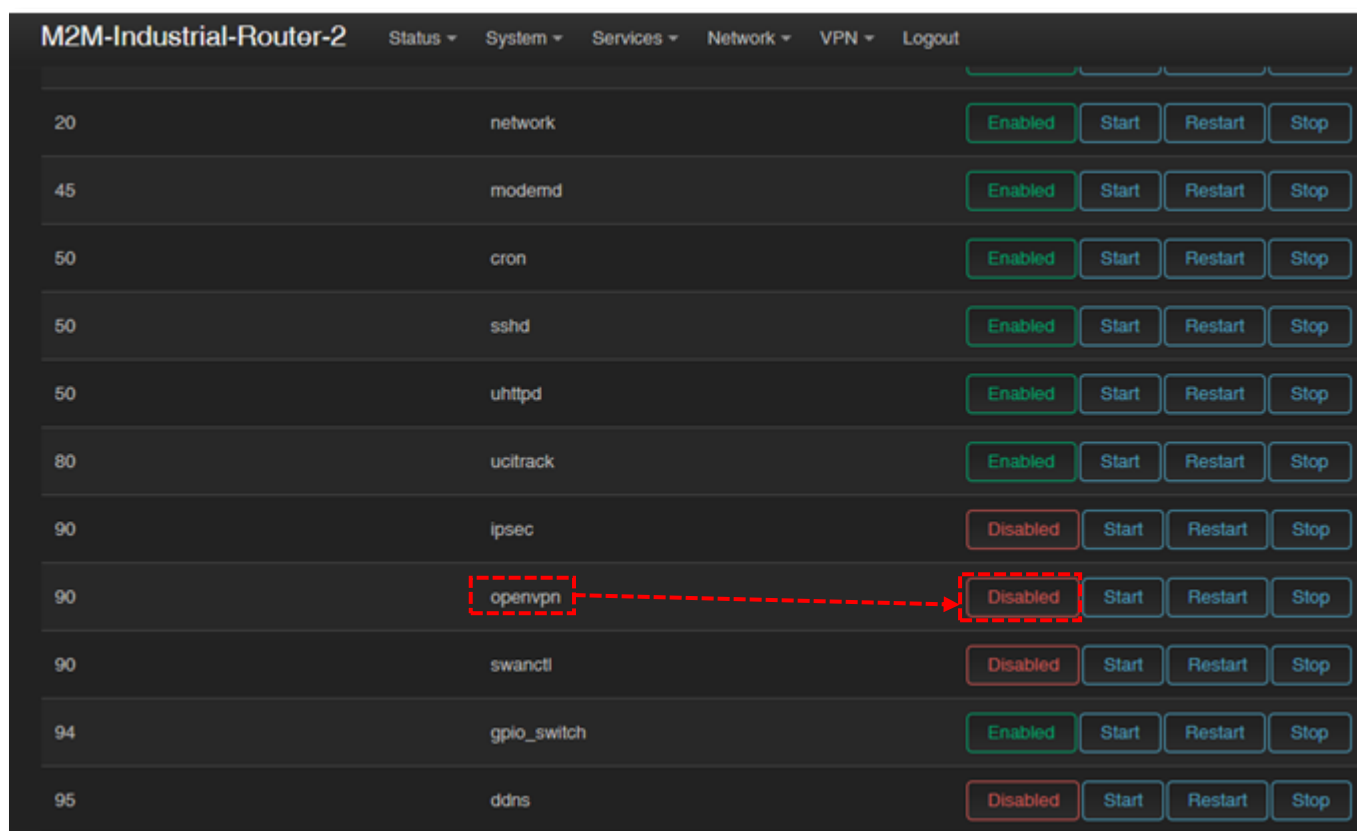
Configure the *strongSwan* IPsec service through ssh connection, from command line. Read the OpenWrt website for more information on possible IPsec settings: <https://openwrt.org/docs/guide-user/services/vpn/ipsec/strongswan/start>

9.8 VPN client (OpenVPN) configuration

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

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

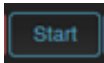
Then wait until the service list will be refreshed and the „**openvpn**” will be listed as **Enabled** service.

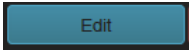
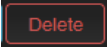


Then push to the **Start** button of the line of the „**openvpn**” service to start the feature.

Open the **VPN / OpenVPN** menu, where you can set up an OpenVPN connection. The default port of the OpenVPN service is nr. 1194.

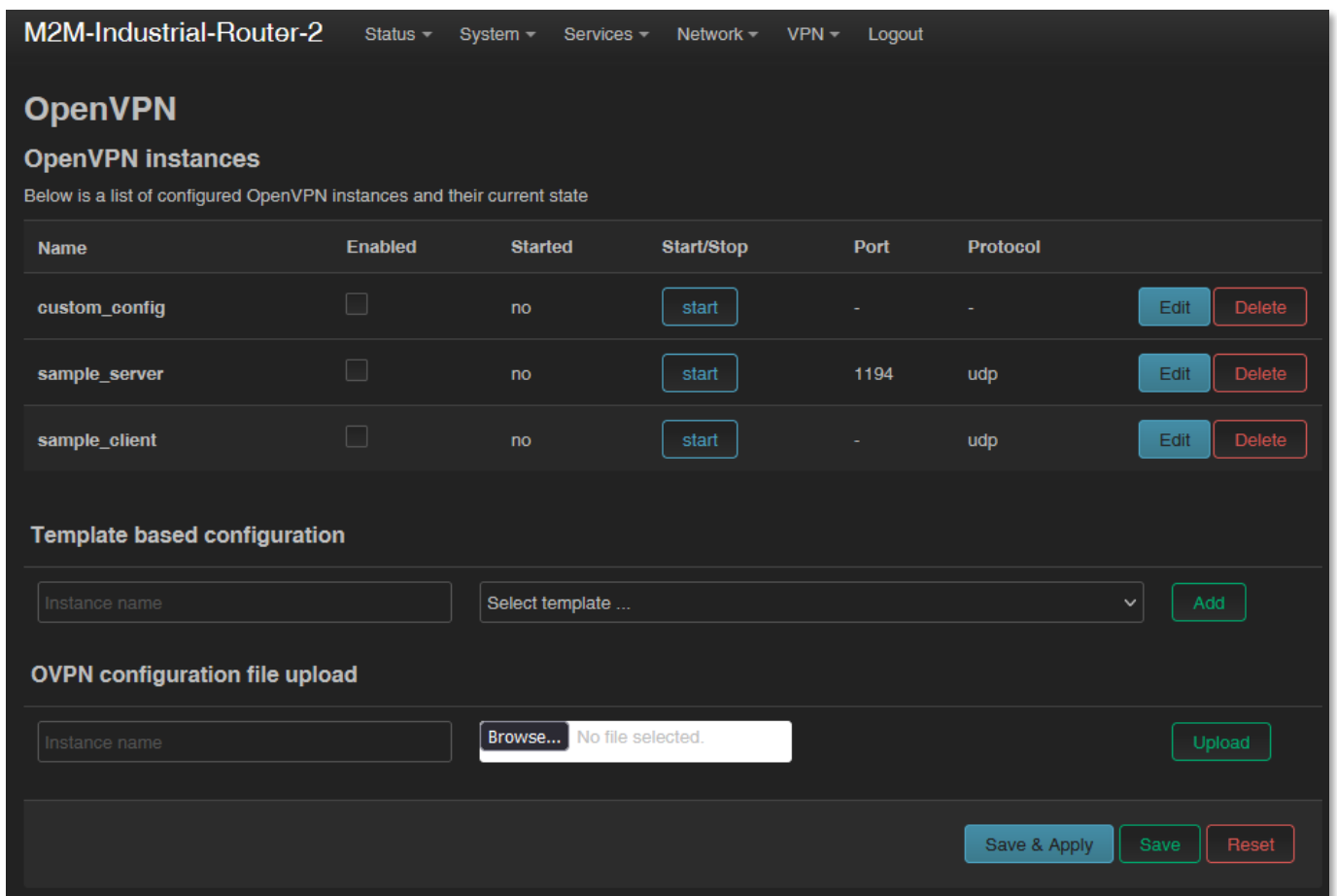
You will find three pre-configured VPN connections that you can enable or change your settings.

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


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

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

You can also **Browse** and **Upload** an OVPN configuration file here.



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

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

The following window will appear, where you can set the following. Configure at least the next fields on this page:

- **proto** (Protocol): here define the connection type – e.g. *udp*
- **client**: check in (to connect to the VPN server)
- **remote**: define the remote and existing VPN connection IP address or host name.
- **ca**: here you can add a manufacturer's CA certification file (grants the validity of the **cert** file).

The screenshot shows the configuration page for an OpenVPN instance named "sample_client". The interface is dark-themed and includes the following elements:


- Header:** "Overview » Instance 'sample_client'" and a link to "Switch to advanced configuration »".
- verb:** A dropdown menu set to "3". Below it is a help icon and the text "Set output verbosity".
- nobind:** A checked checkbox. Below it is a help icon and the text "Do not bind to local address and port".
- client:** A checked checkbox. Below it is a help icon and the text "Configure client mode".
- remote:** A text input field containing "my_server_1 1194" with a red "x" clear button and a green "+" add button. Below it is a help icon and the text "Remote host name or IP address".
- ca:** A file selection button showing "/etc/openvpn/ca.crt (File not accessible)". Below it is a help icon and the text "Certificate authority".
- cert:** A file selection button showing "/etc/openvpn/client.crt (File not accessible)". Below it is a help icon and the text "Local certificate".
- key:** A file selection button showing "/etc/openvpn/client.key (File not accessible)". Below it is a help icon and the text "Local private key".
- proto:** A dropdown menu set to "udp". Below it is a help icon and the text "Use protocol".
- Footer:** A dropdown menu with "-- Additional Field --" and an "Add" button. On the right, there are three buttons: "Back to Overview", "Save & Apply", "Save", and "Reset".

- **cert**: you can add the device certification for the DCU's connection
- **key**: you can add a public key

The TLS v1.2 communication settings here can be made. The TLS settings should be made at the Device Manager side.

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

Then return to the **OpenVPN** menu, where you can enable the given setting with the **Enable** option.

Press the  button to start the configured VPN connection, then press the **Save** button again to save the status of the service.

For the proper settings, we offer to read the related tunnelling service description of the *OpenWrt*[®] administration interface which you are currently using:

https://wiki.openwrt.org/doc/howto/vpn.openvpn#tab__traditional_tun_server1

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

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

```
#uci show openvpn
```

Set according to the following syntax and then comment:

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

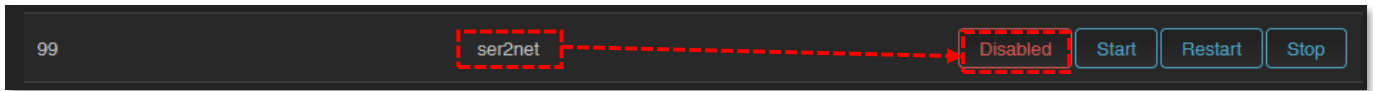
```
#uci commit
```

9.9 RS485 / Modbus settings (Ser2net)

RS485 / Modbus feature can be used for connecting industrial devices, utility meters to the data concentrator.

The RS485 feature is disabled by default. At first you have to start the „**ser2net**” service for the proper operation. Open the **Systems / Startup** menu to *enable* the feature.

Roll down to „**ser2net**” feature and push to the **Disabled** button to initialize the service. Then wait until the service list will be refreshed and the „**ser2net**” will be listed as an

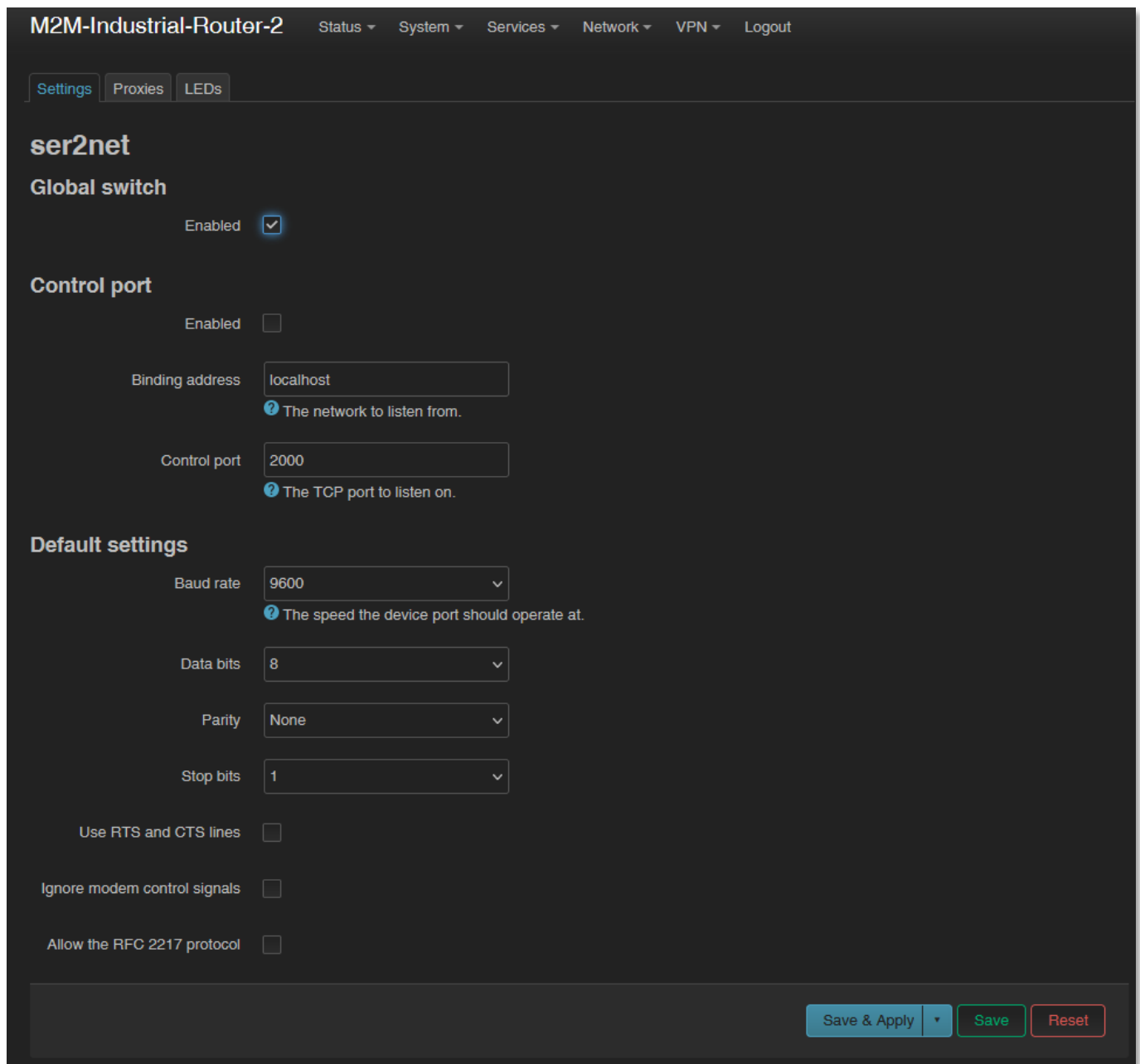


Enabled service.



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

To configure the RS485 / Modbus port, open the **Services / Ser2net** menu.



At **Settings** tab define the parameters of the incoming transparent data transmission.

Make sure that **Global Switch** option is **Enabled**.

At the **Default settings** part, you should configure the following parameters:

- **Baudrate** (default is **9600** bps for the RS485) can be defined between **300** bps and **19 200 bps**.
- **Databits** value can be **7** or **8**
- **Stopbit** value can be **1** or **2**
- **Parity** value can be **Even, Odd** or **None**

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

Make sure that the service option is **Enabled**.

Then define the **Service Port** number (which is port no. 5000 by default).

At the **Protocol** field, the data format can be chosen:

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

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

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

The following communication settings can be also refined here:

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

M2M-Industrial-Router-2 Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

Settings Proxies LEDs

ser2net

Proxies

[Delete](#)

Enabled

Service port
🔗 The TCP port to listen on.

Protocol
🔗 The protocol to listen to.

Timeout
🔗 The amount of seconds of inactivity before a disconnect occurs.
 A value of zero means wait indefinitely.

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

Baud rate
🔗 The speed the device port should operate at.

Data bits

Parity

Stop bits

Use RTS and CTS lines

Ignore modem control signals

Allow the RFC 2217 protocol

Extra options

TX LED configuration

RX LED configuration

Important!

Note, that the incoming RS485 data are not stored locally, they will be transparently transmitted from the device through the cellular network.

The RS485 / Modbus interface can be used as a transparent Modbus gateway without any change. If you have special request on Modbus, indicate or declare your

interest with details by ordering. We can provide a customized command line interface operated special Modbus program for the needs.

Important!

You should add the specified RS485 port number to the **Firewall** rules (**Network / Firewall** menu), otherwise the DCU may not receive any data.

You can also specify additional members, such as *hardware flow control* by enabling the **Use RTS and CTS lines** option.

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

9.10 Data collection settings (RS485 / Modbus / Mbus)

Here you can configure the data acquisition settings for collecting data of utility meters, PLCs.

9.10.1 Prerequisites

For the proper operation you should connect the Modbus device via RS-485 to the M2M Industrial Router 2.

Set up MQTT Server, and configure the connection data.

9.10.2 MQTT Data collection settings

To configure Modbus and RS485 data collection settings open the **Services / Data Collection** menu.

In the **Settings** tab, **Enable** data collection feature by check in.

Add a **Name** for the Target device.

Choose the **Protocol** for data transmission.

Add the **Server address** (IP) and **Server port**.

Setup **Username**, **Password**, **MQTT topic** and **Data format** fields to activate the MQTT data transmission.

The screenshot shows the web interface for 'M2M-Industrial-Router-2'. The 'Settings' tab is selected and highlighted with a red dashed box. Below the navigation bar, the 'Data Collection' section is visible, with a sub-section for 'remote' settings. The settings are as follows:

- Enable:** Checked.
- Name:** Target1
- Description:** Test Target1
- Protocol:** MQTT
- Server Address:** test.mosquitto.org
- Server port:** 1883
- Username:** root
- Password:** (masked with dots)
- Uploading periodicity [min]:** 5
- MQTT topic:** topic1wm777
- MQTT context account name:** devices

You can also add **CA certificate** file, a **TLS certificate** file and **TLS key** for securing the communication.

Use complete paths (directory names) for file path.

MQTT clientid name

MQTT QoS

MQTT QoS 0/1/2

CA certificate

CA certificate file for secured server connection
PEM format, pem extension

TLS certificate

TLS certificate file for secured server connection
PEM format, pem extension

TSL key

TLS key file of this device for secured server connection
PEM format, pem extension

Collector Template

Collector (DCU) related information

Devices Array Name

Contains All devices/readouts Array Name

Device Template

Measuring device related part

Register Array Name

Register Array Name

Register Template

Measured date related part

Data format

Output formats 0/1/2

Push to **Save & Apply** button to save the modified settings.

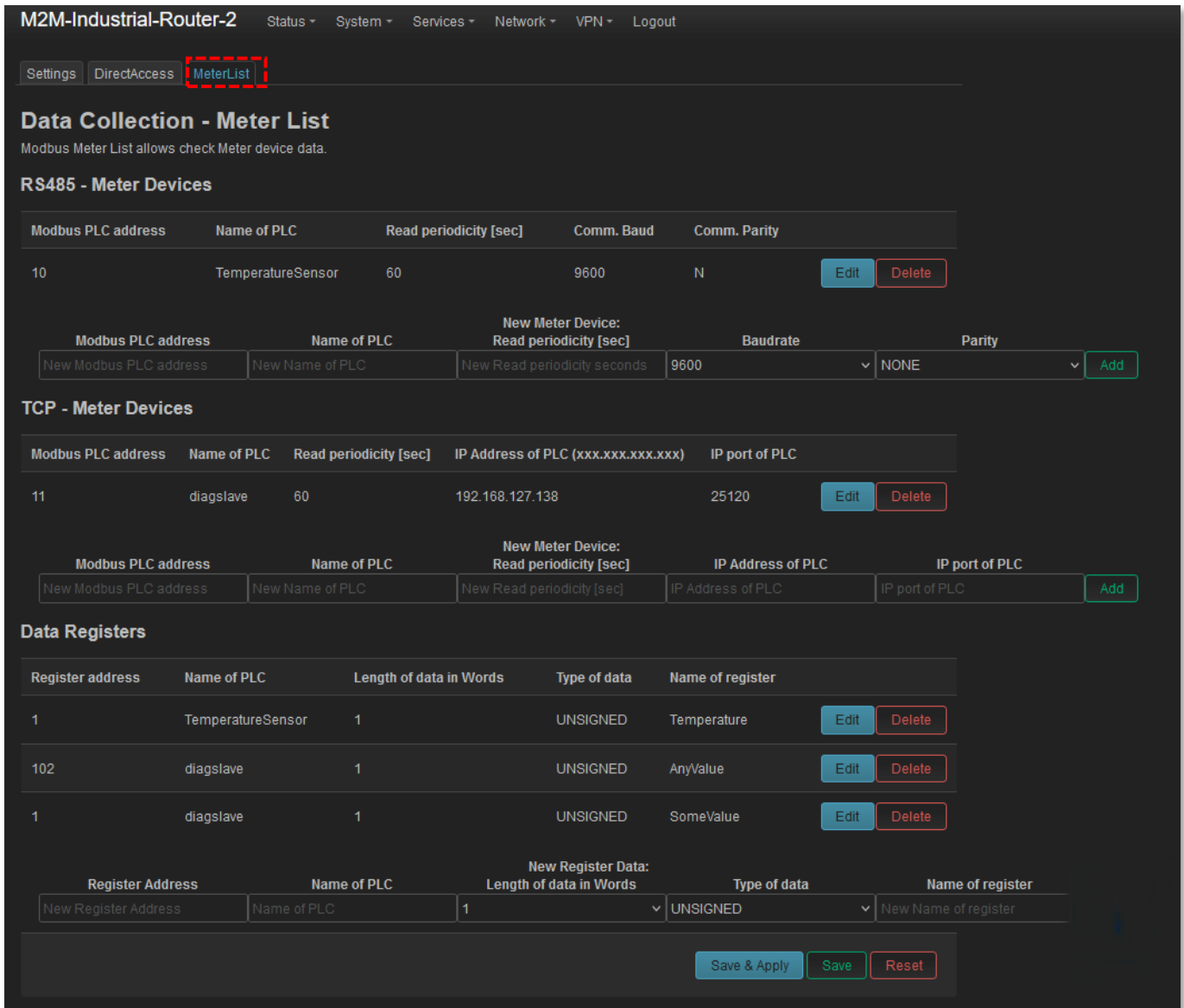
9.10.3 Configure the Modbus data items

On the **MeterList** tab add a PLC device or more devices.

At **RS485 – Meter Devices** part, fill the **Modbus PLC Address**, the **Name of PLC** and **New Meter Device: Read periodicity [sec]** fields.

You can change the RS485 communication speed (**Baudrate**), and **Parity** value.

Then press to the  button to add the new device to the device list.



M2M-Industrial-Router-2 Status System Services Network VPN Logout

Settings DirectAccess **MeterList**

Data Collection - Meter List

Modbus Meter List allows check Meter device data.

RS485 - Meter Devices

Modbus PLC address	Name of PLC	Read periodicity [sec]	Comm. Baud	Comm. Parity	
10	TemperatureSensor	60	9600	N	Edit Delete

New Meter Device:

Modbus PLC address	Name of PLC	Read periodicity [sec]	Baudrate	Parity	
New Modbus PLC address	New Name of PLC	New Read periodicity seconds	9600	NONE	Add

TCP - Meter Devices

Modbus PLC address	Name of PLC	Read periodicity [sec]	IP Address of PLC (xxx.xxx.xxx.xxx)	IP port of PLC	
11	diagslave	60	192.168.127.138	25120	Edit Delete

New Meter Device:

Modbus PLC address	Name of PLC	Read periodicity [sec]	IP Address of PLC	IP port of PLC	
New Modbus PLC address	New Name of PLC	New Read periodicity [sec]	IP Address of PLC	IP port of PLC	Add



Data Registers


Register address	Name of PLC	Length of data in Words	Type of data	Name of register	
1	TemperatureSensor	1	UNSIGNED	Temperature	Edit Delete
102	diagslave	1	UNSIGNED	AnyValue	Edit Delete
1	diagslave	1	UNSIGNED	SomeValue	Edit Delete

New Register Data:

Register Address	Name of PLC	Length of data in Words	Type of data	Name of register	
New Register Address	Name of PLC	1	UNSIGNED	New Name of register	

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

 If the **Data bits** setting in the communication should not be value „8” or the **Stop bit** should not be value „1”, then push to the  button at **Comm. Parity** field after you've added the device and then configure the following bit settings.

Push to  button to save the modified settings on this window and let's back to the **MeterList** tab.


M2M-Industrial-Router-2 Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

Settings DirectAccess **MeterList**


Data Collection - Meter Device for RS485 - TemperatureSensor

This page allows you to change properties of the meter device entry.


Name

 Name of PLC

Modbus Address

 PLC Modbus Address

Description

 Description of PLC device (optional)


Speed

Data bits

Stop bits

Parity

Data read periodicity [sec]

 Data read out periodicity from PLC in seconds

9.10.4 Add registers to the list

At **Data registers** tab add registers to the list (assigned to an existing PLC device) by following these hints.

Fill the **Register Address** in decimal value.

Important! Note, that the value at **Register address** field should be the same as it is used in protocol message.

To the **Name of PLC** field please refer to the existing **Name of PLC** field value, **New Register Data: Length in Words** should be calculated as „n* 16 bit”.

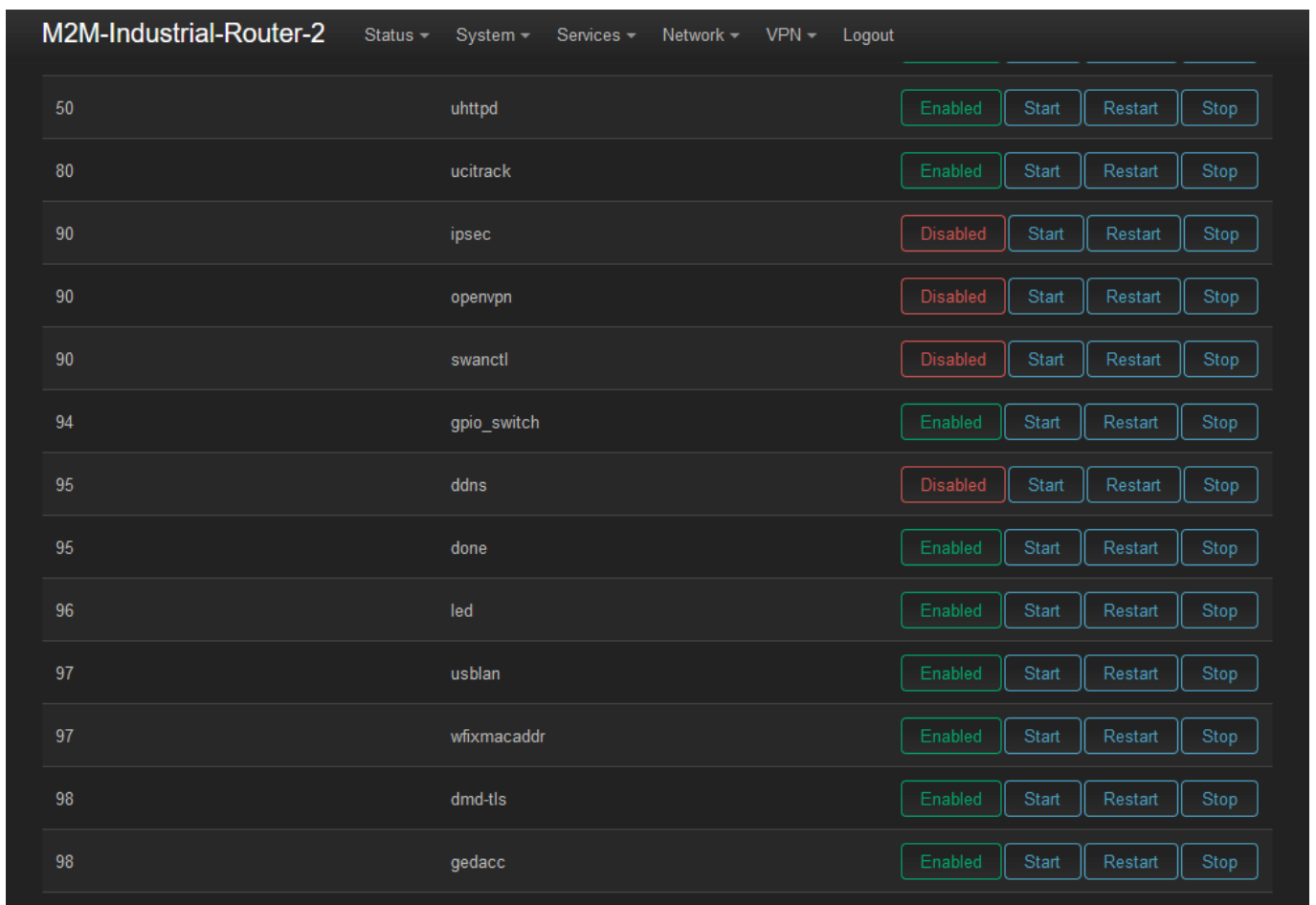
Then choose the **Type of data** and fill the **Name of register**.

Then press to the  button to add the new register to the list.

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

9.10.5 Configure service state

In the **System / Startup** menu make sure you can see the green **Enabled** button at the **gedacc** service in the list. This means that the service will be automatically started at device start. If it is **Disabled**, then you should switch it by pushing the **Start** button to be enabled.



9.10.6 Custom program communication

When the data collector program (gedacc service) is running, it is using the „serial” device file. If you want to communicate on RS-485, you should **disable** the **gedacc** service in **System / Startup** menu.

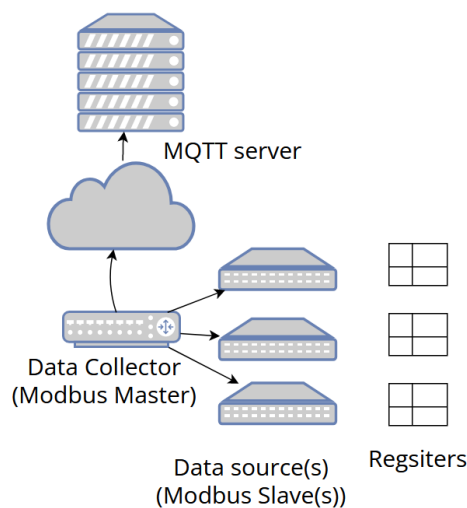
Use the **/dev/ttyS3** device file to access the serial device file.

9.10.7 Communication format

The device connected to one or more data source of devices. The communication can be Modbus RTU or Modbus TCP. Each data source of devices have unique **PLC Address** on the bus and data date stored in registers. **Registers** has **Addresses**, length and types.

The collector reads the „holding registers” (Function Code: 03) of the devices. It stores and publishes them to an MQTT server.

⚠ In MQTTS mode the server authentication can not be omitted. You must provide a valid CA certificate file to communicate.



Data collecting layout

9.10.8 MQTT + JSON

The JSON payload can be used in two formats, depending on the **Settings** tab **Data format** value: **FIX JSON** or **Template JSON**.

Data format: Fix JSON (structure and content)

The concept is the following.

In **JSON** content everything is fixed. Only data values can be changed. See the example (fix elements are marked with **red**, changeable values are marked with **blue**).

In an MQTT publish message, there contained ALL registers when a PLC device is reading at once. Therefore, separate publish messages are necessary for each device, and each periodic reading.

If there are more registers assigned for a "PLC", data named array should have more objects.

Example:

```
Publish 1: { "PLCAddress": 10 , "Status": "OK", "Timestamp": "2024-01-10 18:16:00", "Timestamp_epoch": "1704910560", "data" : [ { "RegisterAddress": 1, "RegisterValue": 120 } ] }
```

```
Publish 2: { "PLCAddress": 10 , "Status": "OK", "Timestamp": "2024-01-10 18:17:00", "Timestamp_epoch": "1704910620", "data" : [ { "RegisterAddress": 1, "RegisterValue": 125 } ] }
```

Data format: Custom JSON Template

In order to make flexible JSON content inside a MQTT publish message, you should choose the **Template JSON**.

Then fill the template fields as:

- **Collector Template**
- **Devices Array Name**

- **Device Template**
- **Register Array name**
- **Register Template**

Here are listed some of the default template values:

Collector template:

"CollectorName": "%COL_NAME%", "CollectorDescription": "%COL_DESCR%",

Device Template:

"Address": %PLC_ADDR% , "Name": "%PLC_NAME%", "Timestamp": %epoch%,
 "Date": "%DATETIME%",

Register Template:

"%REG_NAME%": "%REG_VALUE%"

Variables

Variables are used to change the current values to the message text. The following list contains the useable variables.

Name	Legend	Source
%COL_NAME%	Data collector device name	Settings tab, "Name" field
%COL_DESCR%	Data collector device	Settings tab, "Description" field
%PLC_ADDR%	PLC address value	MeterList tab, "Modbus PLC address" field
%PLC_NAME%	Name of the PLC	MeterList tab, "Name of PLC" field
%epoch%	Time of the data in seconds since 1970-01-01	OS date/time value
%DATETIME%	Time of the data in ISO 8601 like format*: "YYYY-MM-DD hh:mm:ss"	OS date/time value *
%REG_NAME%	Name of the next register	MeterList tab, "Register Address" field
%REG_VALUE%	Value of the next register	Data source of device eg. PLC

*Time is local time, not UTC time; Date/Time delimiter is space character and it is not capital T ; no Z Zulu timezone after seconds. "2024-01-10 19:17:00" not "2024-01-10T18:17:00Z"

The message begins with the **Collector Template** (if there is), then an object array follows.

Its name is the value of the **Devices Array Name** setting field. Default value is **TelemetryData**. Each object, which has two parts: the first is the **Device Template** and the second is an object array.

The name of this array is the value of the **Register Array Name** setting field. Initial value is **RegisterData**. The array elements are the data derived from the **Register Template**.

See the next Example:

```
{
  "CollectorName": "Target1",
  "CollectorDescriptor": "Test Target1",
  "TelemetryData": [
    {
      "Address": 10,
      "Name": "TemperatureSensor",
      "timestamp": 1705415760,
      "date": "2024-01-16 14:36:00",
      "RegisterData": [ { "Temperature": "0" } ]
    },
    {
      "Address": 10,
      "Name": "TemperatureSensor",
      "timestamp": 1705415820,
      "date": "2024-01-16 14:37:00",
      "RegisterData": [ { "Temperature": "0" } ]
    },
    {
      "Address": 10,
      "Name": "TemperatureSensor",
      "timestamp": 1705415880,
      "date": "2024-01-16 14:38:00",
      "RegisterData": [ { "Temperature": "0" } ]
    }
  ],
  ...
}
```

Afterall, push to the **Save & Apply** settings.

9.10.9 Direct Access

Modbus RTU capable data source devices (PLCs) can read out remotely using modbusTCP.

To configure this feature, click to the **DirectAccess** tab and the Modbus communication parameters can be set there.

M2M-Industrial-Router-2 Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

Settings DirectAccess MeterList

Data Collection

The Data Collection allows modbus communication. Values from meters will be upload using MQTT(S).

Modbus Access

Settings of Direct Access of RS485 line

Enable

[? Enable this service](#)

Server port

[? Port number of server.](#)

Speed

Data bits

Stop bits

Parity

M-Bus Access

Settings of Direct Access of M-Bus line

Enable

[? Enable this service](#)

Server port

[? Port number of server.](#)

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

⚠ Only one communication setting is valid at once. If more PLCs having different communication settings, you should have to alter manually the **DirectAccess** settings before performing the connection.

Afterall, push to the **Save & Apply** settings.

9.10.10 TCP Meter Devices (Modbus or PLC devices)

At the **TCP Meter Devices** part you can add **Modbus or PLC devices** connected on RS485 or Ethernet. Here you can configure the following parameters:

- **Name** – Name of the Modbus device
- **PLC IP Address** – address of the PLC device
- **Port** – Port number of the device

- **Modbus Address** – Address of the Modbus device
- **Description**
- **Data read periodicity (sec)** – by default it is 60 seconds

Fill the required fields consequently regarding the Modbus meter / PLC data collection requirements.

The screenshot shows the configuration page for a ModbusTCP meter device. The page title is "Data Collection - Meter Device for ModbusTCP - diagslave". Below the title, there is a sub-header "Data Collection - Meter Device for ModbusTCP - diagslave" and a note: "This page allows you to change properties of the meter device entry." The form contains the following fields:

- Name:** diagslave
- PLC IP address:** 192.168.127.138
- Port:** 25120
- Modbus Address:** 11
- Description:** PC emulated modbusTCP
- Data read periodicity [sec]:** 60

At the bottom of the form, there are four buttons: "Back to Overview", "Save & Apply", "Save", and "Reset".

Afterall, push to the **Save & Apply** settings for record the new device.

9.11 Mbus settings

The Mbus feature can be used for connecting up to 30 slave Mbus devices, utility meters to the data concentrator.

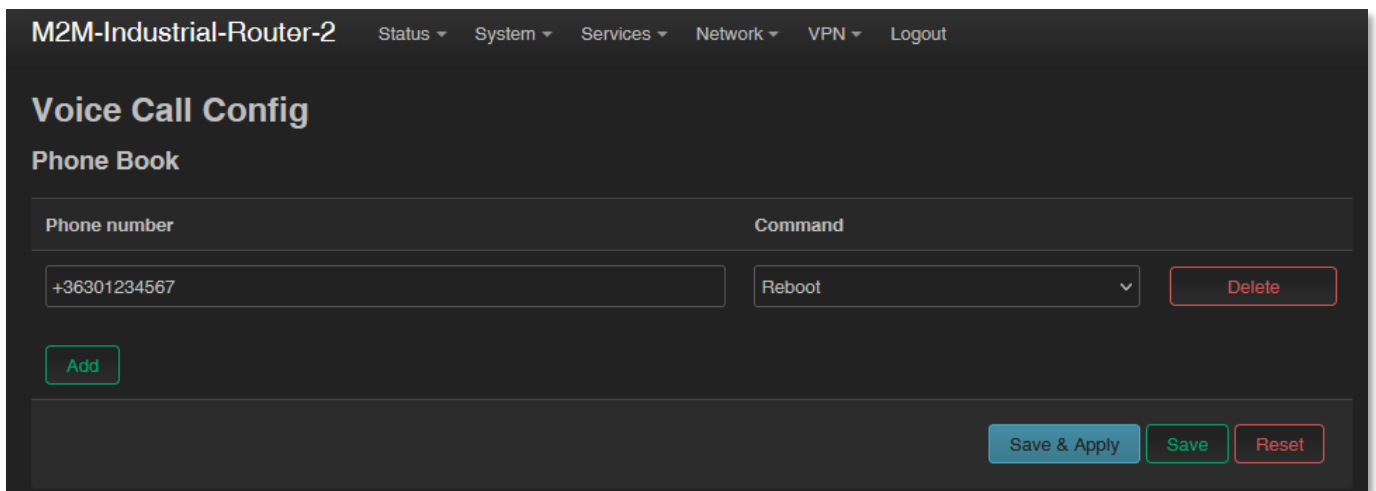
The Mbus port speed rate can be configured between 1 200, 2 400, 4 800 or 9 600 baud.

The DCU MBUS provides 24-36V DC power to the connecting external devices for the proper operation.

9.12 Voice call settings

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

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



The screenshot shows the 'Voice Call Config' interface for 'M2M-Industrial-Router-2'. The 'Phone Book' section contains a table with two columns: 'Phone number' and 'Command'. A single entry is visible with the phone number '+36301234567' and the command 'Reboot'. There is a 'Delete' button next to the entry. Below the table is an 'Add' button. At the bottom right, there are 'Save & Apply', 'Save', and 'Reset' buttons.

Phone number	Command
+36301234567	Reboot

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

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

9.13 Run commands remotely (SMS config settings)

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

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

First you can see the **Phone Book** where you can define or **Add** phone number(s). Then you have to check the **Enabled** option for the selected phone number(s).

M2M-Industrial-Router-2 Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

SMS Config

Phone Book

Enabled	Phone number	
<input type="checkbox"/>	+36331234561	Delete

Add

SMS Commands

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

Save & Apply Save Reset

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 DCU runs the preset command (s) assigned to the phone number: e.g. **Reboot**

For other commands, the DCU returns the information in a reply SMS message (e.g. when sending the **“info”** command in SMS, the device 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** button to save the settings.

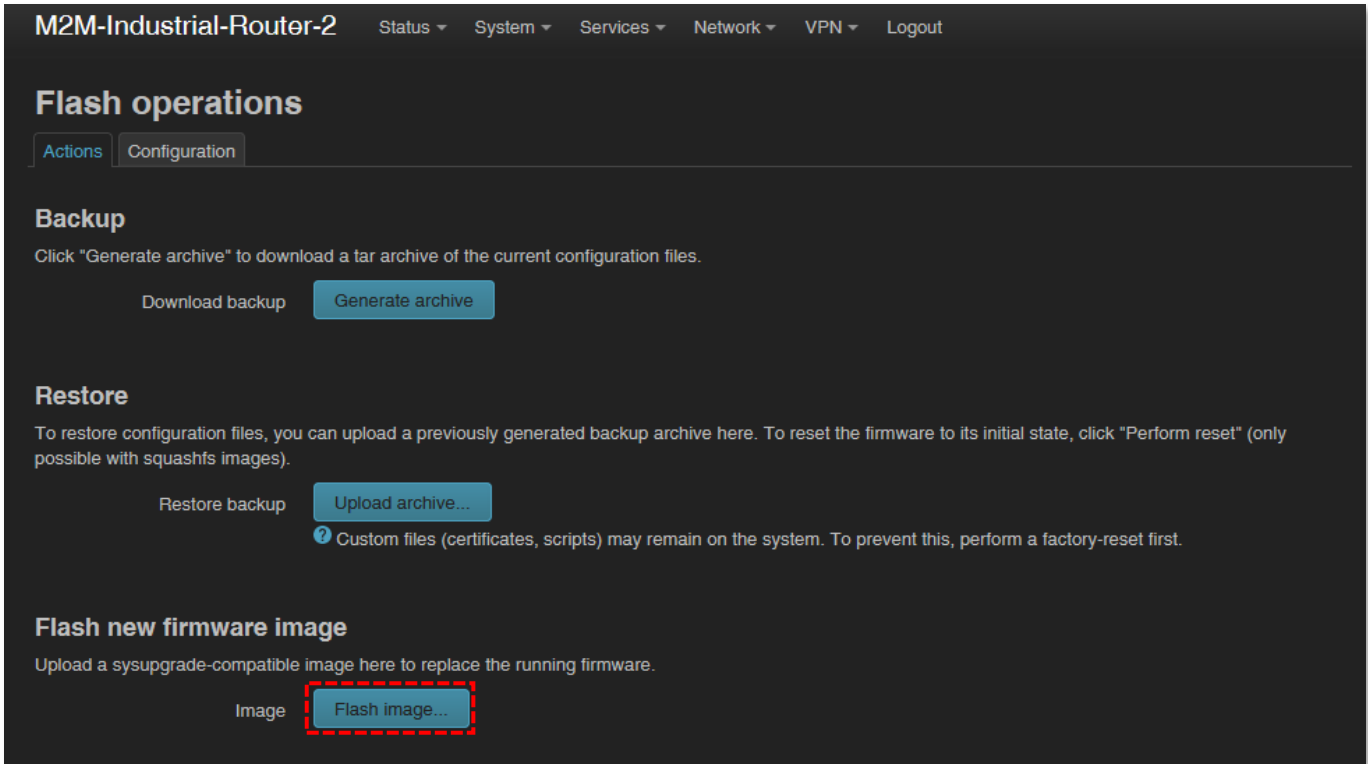
Chapter 10. Software refresh, maintenance

10.1 Firmware refresh

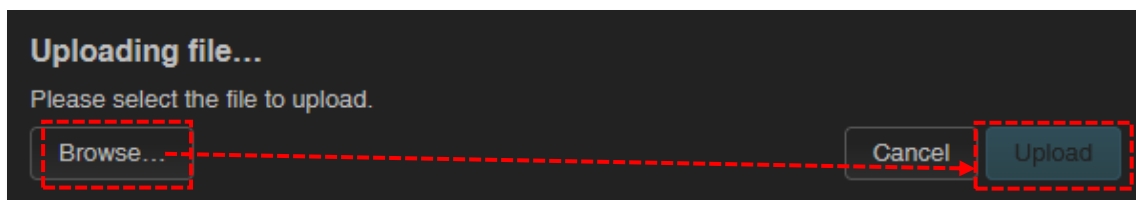
1. Open the **System** menu, **Backup / Flash firmware** item.

2. At the bottom part, at **Flash new firmware image** part, push to the

Flash image...

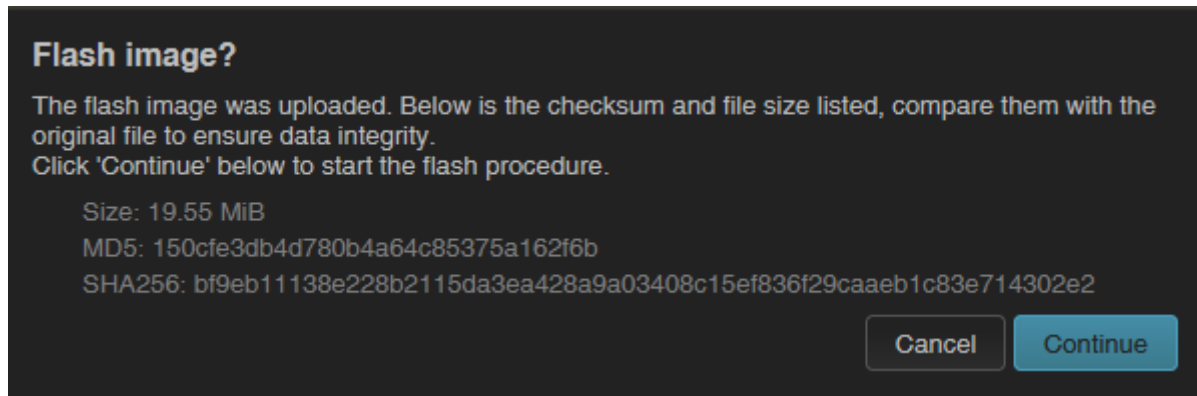


3. **Browse...** the **fw-....** compressed firmware file and push to the **Upload** button.



4. Then another window is loaded, where the checked file will be uploaded and verified for approx. in half a minute.

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



6. Then the a **Flashing...** message will appear on the screen. The refresh method will be started, while the **LED3** will be continuously lighting by **red** and sometimes the **LED2** will be also flashing.
7. At the end of the installation - the LEDs will no longer flash - the system will reboot two times, then the *OpenWrt*[®] system will start and load as described.

Important! *The update window will not close and automatically and it does not detect the availability of the OpenWrt website. Therefore, close the upgrade browser window after the end of the refresh / installation process.*

8. When **LED3** or **LED2** is available again and stays **green**, , you can login to the OpenWrt interface of the router.
9. Open a new web page and enter URL, login credentials.
10. Check the updated software version at **Status / Overview** menu.

10.2 Installing applications

Open the **System / Software** menu.

M2M-Industrial-Router-2 Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

Software

Free space:
90% (442.71 MiB)

Filter: Download and install package: Actions:

Display LuCI translation packages:
 filtered all none

« No packages »

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

« No packages »

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

OPKG Configuration

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

/etc/opkg.conf

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

/etc/opkg/customfeeds.conf

```
# add your custom package feeds here
#
# src/gz example_feed_name http://www.example.com/path/to/files
```

/etc/opkg/distfeeds.conf

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

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

Important!

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

If you want to install a locally stored package from the DCU then push to the **Upload Package...** button.


You can check the **Installed** packages also. If there is a possible for the installed package, it will be listed at **Update** tab.

The screenshot shows the 'Software' management interface. At the top, it displays 'Free space: 90% (442.71 MiB)' with a progress bar. Below this are input fields for 'Filter:' and 'Download and install package:', along with 'Clear', 'OK', and 'Update lists...' buttons. There are also radio buttons for 'Display LuCI translation packages: filtered (selected), all, none'. A tab bar at the bottom shows 'Available', 'Installed' (highlighted with a red dashed box), and 'Updates'. The main area displays a table of installed packages with columns for 'Package name', 'Version', 'Size (.ipk)', and 'Description'. Each row has a 'Remove...' button. The table shows the following data:

Package name	Version	Size (.ipk)	Description
base-files	3-r0-c327aa5e	-	-
bind-client	9.18.7-1	-	-
bind-libs	9.18.7-1	-	-
busybox	1.35.0-5	-	-
bzip2	1.0.8-1	-	-
cJSON	1.7.15-3	-	-

You can **Remove...** unnecessary packages, if you want.

To install a new software component or package, select one package from the list or **Add** the name of the application you are attempted to install at the **Download**

and **install package** field and push to the  button for the installation – regarding the upcoming hints on the screen.

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

You can also install distributed packages to the DCU / Router from of the official OpenWRT repository website of the current CPU architecture (ARM 926EJ-S):

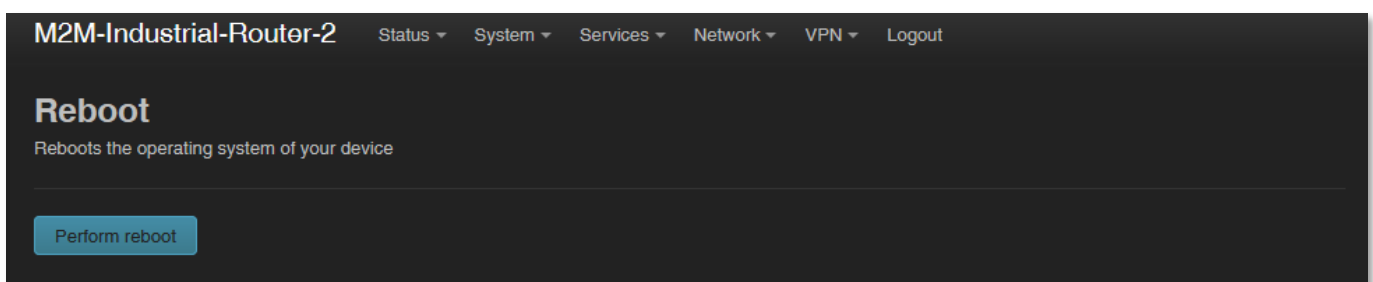
1. https://downloads.openwrt.org/releases/22.03.4/packages/arm_arm926ej-s/packages/
2. Download the IPK package to your computer – file(s) with *.ipk extension, which you want to install to the router.
3. Open an SFTP connection to the DCU/Router (e.g with *WinSCP* on **port** nr. **222** with the known credentials (username: **root**, password: **wmrpwd**).
4. Copy the required *.ipk files into the **/tmp** directory
5. Open an SSH command line (e.g. with *putty*) and use the following commands to install:

```
cd tmp
opkg install package_name.ipk
```

Then the package(s) will be installed to the router's system.

10.3 Restarting the device

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



Then the DCU will be restarted as it was described before (**3 LEDs lighting shortly** by **red** colour for a second, and the **LED1** will be flashing assigns the booting process).



Then the DCU will be operating as normal, and will be connected to the internet according the configuration settings.

Instead all of these, you can restart the DCU by pushing its **Reset** button on its interface / port side. Push this button for 10 seconds, by a sharp and thin object. Then the device will be restarted.

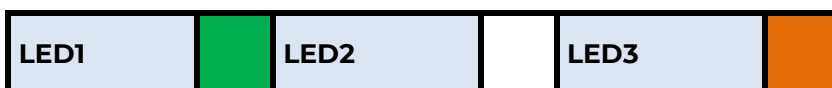
10.4 Shutdown / halt of the DCU

Pull out the power connector from the AC electricity plug.

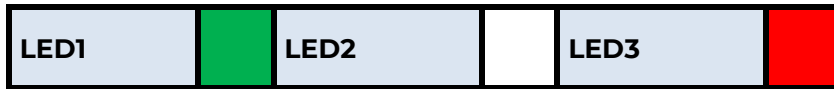
Note, that the router will be still powered if the USB connector was plugged, because the device receives 5VDC power on USB connection. Therefore, you have to disconnect the USB cable to power down the router.

Note, that the router will not powered off immediately, due to it have supercapacitor components inside. Therefore, the router will getting enough spare power (ca. for up to 10 seconds) to close every connection, interfaces and ports and shutdown the device safely. The shutdown sequence is the following:

1. The **LED1** will be still active (green) which means that after removing the power from the device, the supercapacitors still having enough power for powering the device. But the **LED3** will be lighting by **orange** color. This shows, that the router interfaces are during disconnection and the system will be halted soon.



2. Soon, the **LED3** lighting will be changed to color **red**, which means that the system is under power down.



3. Soon, when the supercapacitors will be exhausting and the system is down, the **LED1** and **LED3** will be also blank, which means that the router is halted.



10.5 Start the device

You can start the device anytime by adding the 12V DC (9-32V DC) power to the 4-pin Microfit power connector (by its 12V DC adapter). The **Power** LED will be lighting, and the DCU will begins its start sequence.

10.6 Password change

Open the **System / Administration** menu.

A screenshot of a web interface for 'M2M-Industrial-Router-2'. The top navigation bar includes 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout'. Below the navigation, there are two tabs: 'Router Password' (selected) and 'HTTP(S) Access'. The main heading is 'Router Password' with a sub-heading 'Changes the administrator password for accessing the device'. There are two input fields: 'Password' and 'Confirmation', both with asterisks (*) indicating they are required. A green 'Save' button is located at the bottom right of the form area.

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

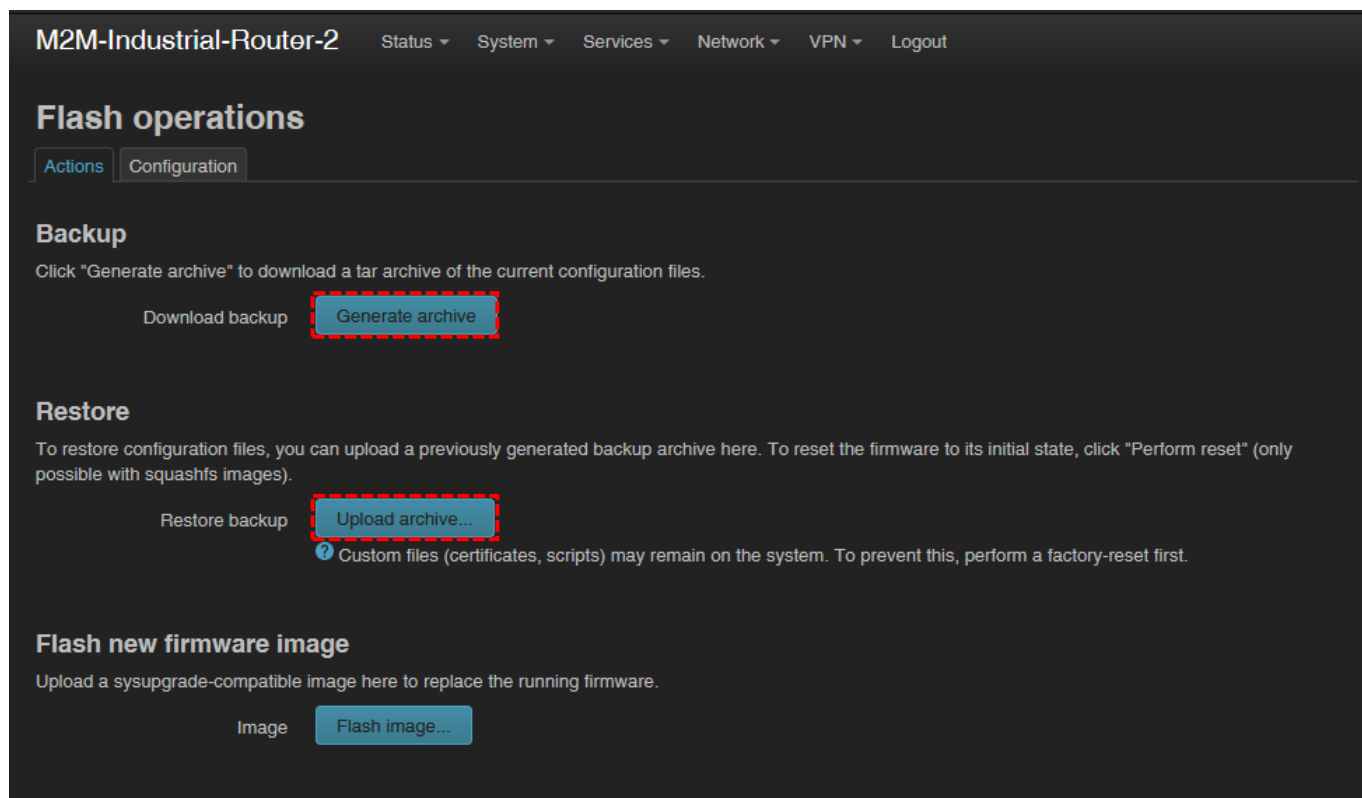
When you enter the password, the web interface replaces the entered characters with asterix (*). At least 6 characters must be entered for the password.

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

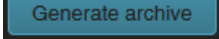
10.7 Backup and restore of settings

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

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



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

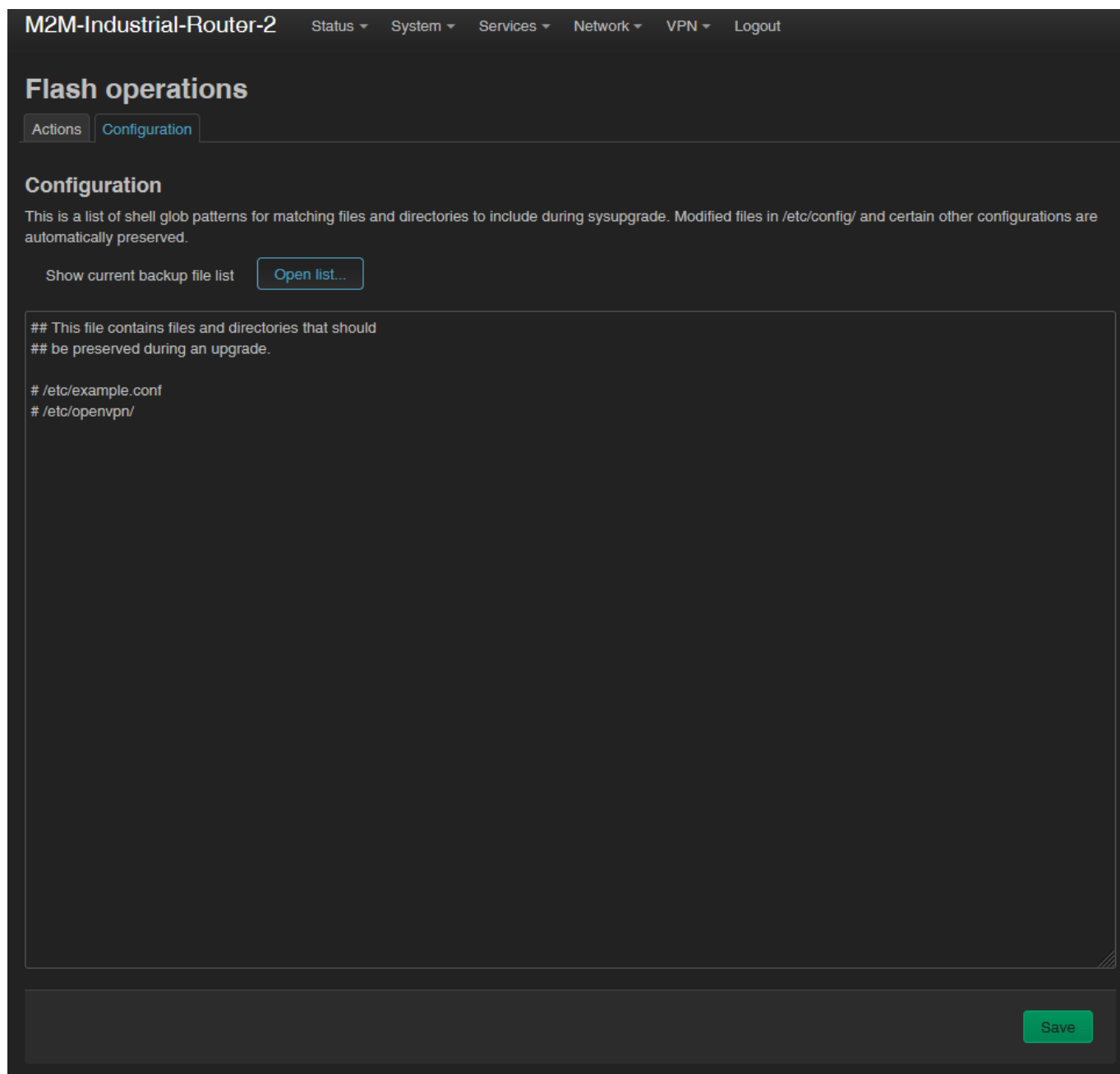
At the **Backup / Restore** part, **Download backup** feature push the  button for saving the settings (backup) into a file (to .tar.gz extension) to your computer.

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

The DCU only saves its own settings and services! If you have manually installed additional programs or are using your own scripts, it is IMPORTANT to know that they

will NOT be saved! You need to ensure that non-standard applications, scripts, directories are backed up manually.

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



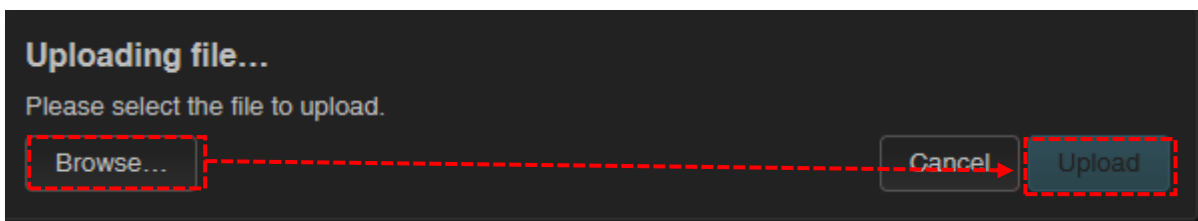
The screenshot shows the web interface for 'M2M-Industrial-Router-2'. At the top, there is a navigation bar with 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout' menus. Below this is the 'Flash operations' section, which has two tabs: 'Actions' and 'Configuration'. The 'Configuration' tab is active. Underneath, there is a heading 'Configuration' followed by a descriptive paragraph: 'This is a list of shell glob patterns for matching files and directories to include during sysupgrade. Modified files in /etc/config/ and certain other configurations are automatically preserved.' Below the text, there is a link 'Show current backup file list' and a button 'Open list...'. A large text area contains the following content: '## This file contains files and directories that should ## be preserved during an upgrade.' followed by two lines: '# /etc/example.conf' and '# /etc/openvpn/'. At the bottom right of the interface, there is a green 'Save' button.

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

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

If you want to request a configuration restore, at the **Restore** part, save the archive (full) backup file previously saved to your computer – in .tar.gz. format - you can download it back to your device. To do it, you can validate your request at the **Restore backup** part.

Press the **Upload archive...** button to upload a previously saved (backup) compressed configuration file to the DCU.



Browse... the previously saved file from your computer and push to the **Upload** button to perform.

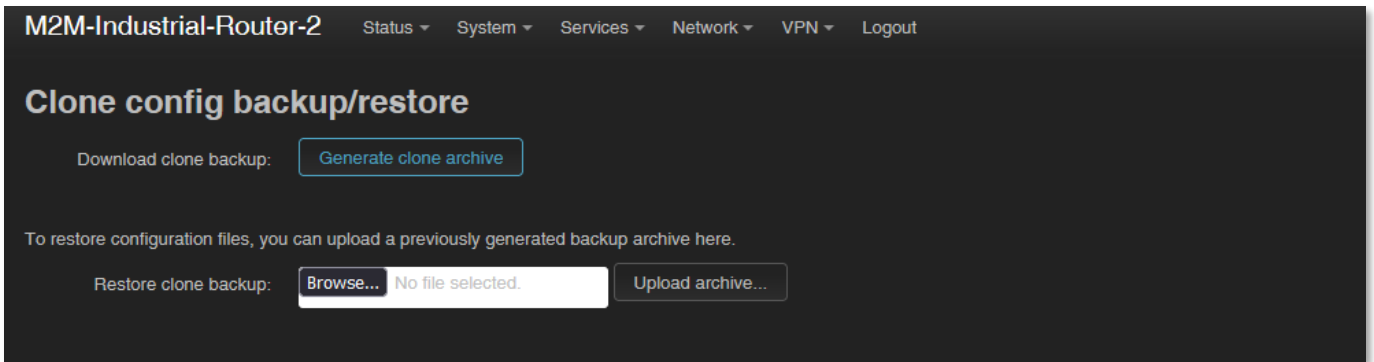
Important! You will then have to manually back up and play back the backups of custom configurations and programs - as they are not part of the system restore.

10.8 Clone configuration

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

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

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

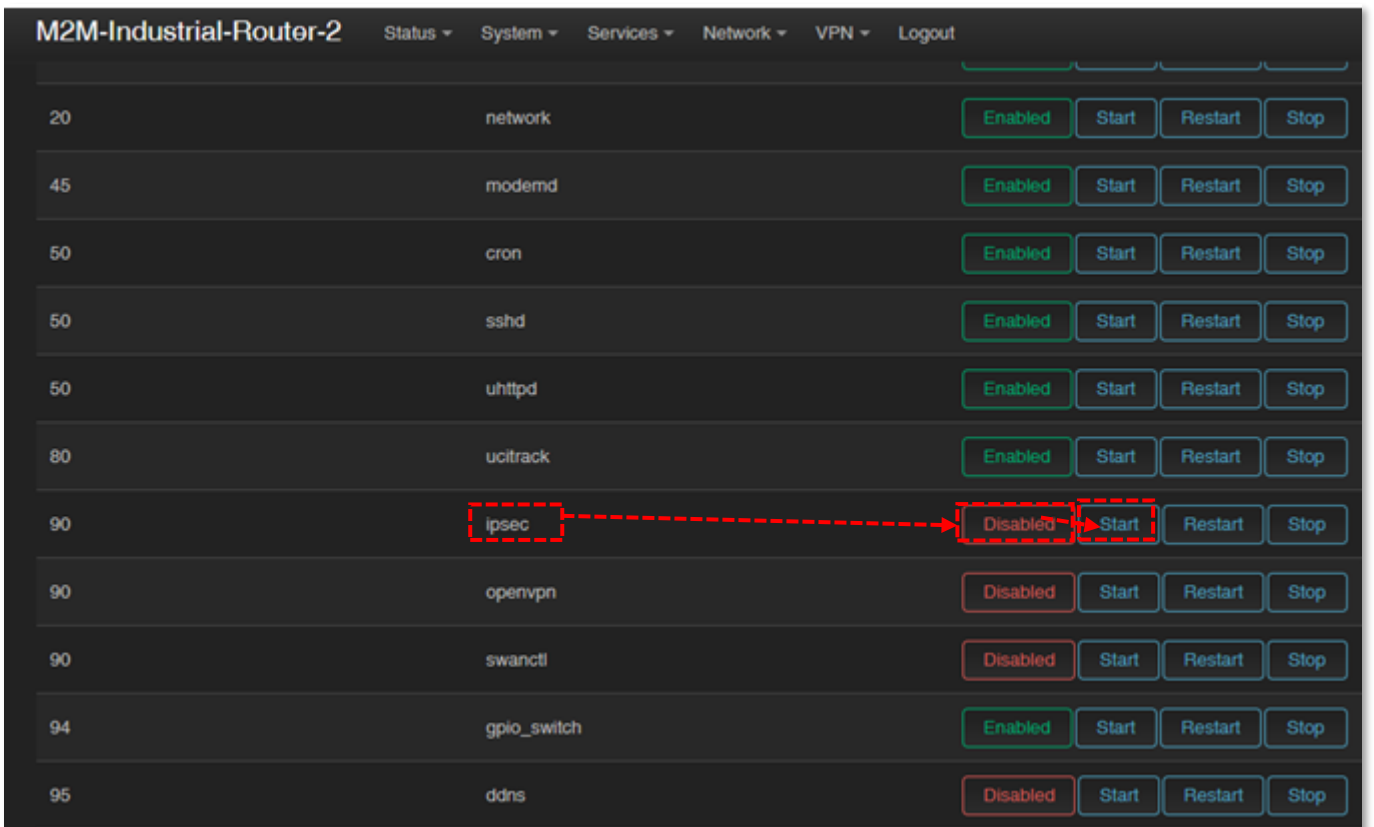


This is especially useful if you save the configured configuration to your computer and want to load it to multiple DCUs (as a basic configuration) - making the settings easier.

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

10.9 Start or stop a system service

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

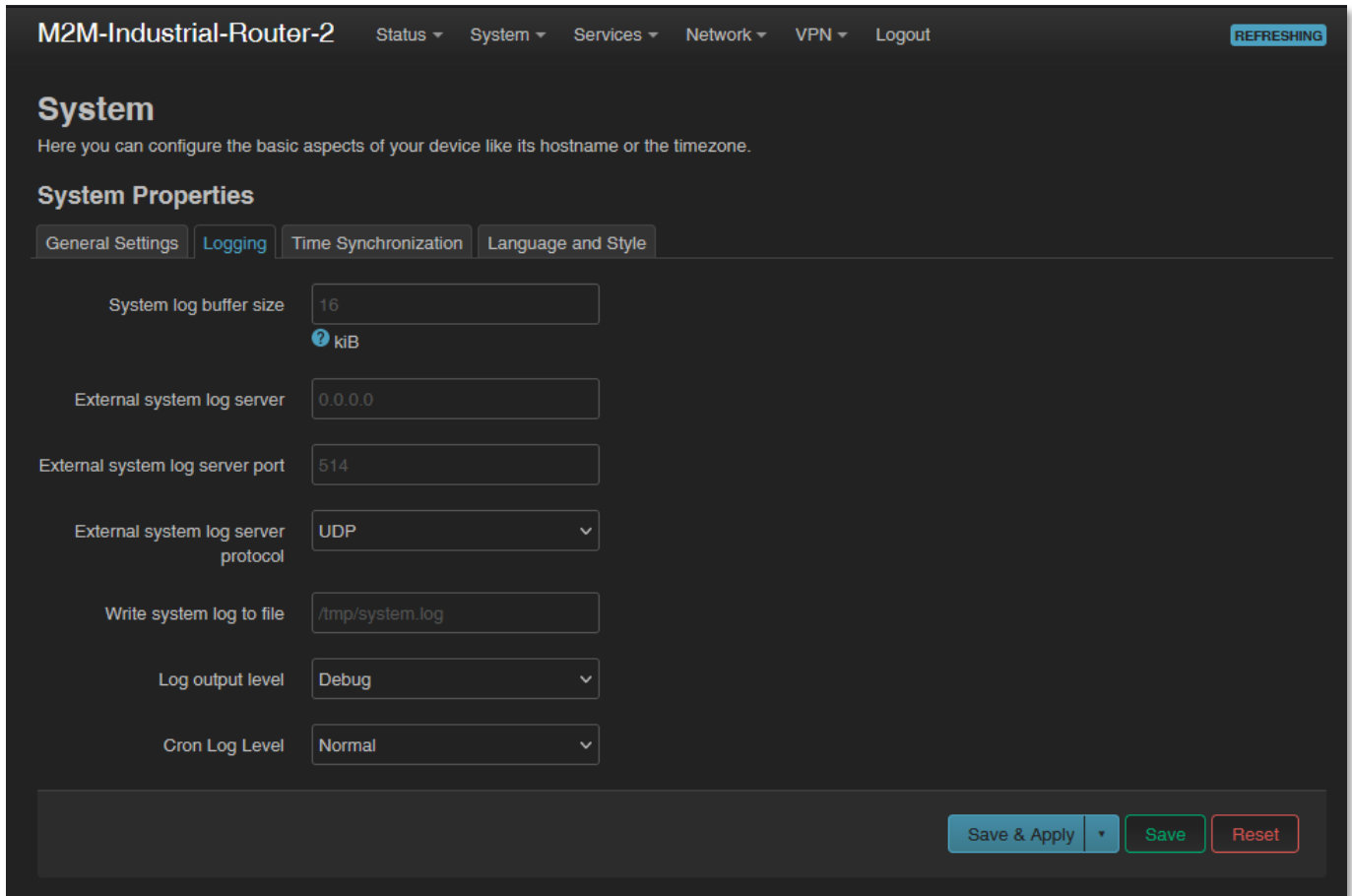


Push to the **Disabled** button of the service. Wait while the system will refresh the list, then now it should already have **Enabled** status. You can start the service by pushing to the **Start** button to initialize the required service.

You can stop the service anytime by pushing the  button.

10.10 Log

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



The screenshot displays the configuration interface for the 'Logging' tab within the 'System Properties' section of the M2M-Industrial-Router-2. The interface includes a navigation bar at the top with 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout' menus, and a 'REFRESHING' button. The 'System' title is followed by a subtitle: 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Below this, the 'System Properties' section is active, with sub-tabs for 'General Settings', 'Logging', 'Time Synchronization', and 'Language and Style'. The 'Logging' sub-tab contains several configuration fields: 'System log buffer size' (16 kiB), 'External system log server' (0.0.0.0), 'External system log server port' (514), 'External system log server protocol' (UDP), 'Write system log to file' (/tmp/system.log), 'Log output level' (Debug), and 'Cron Log Level' (Normal). At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

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

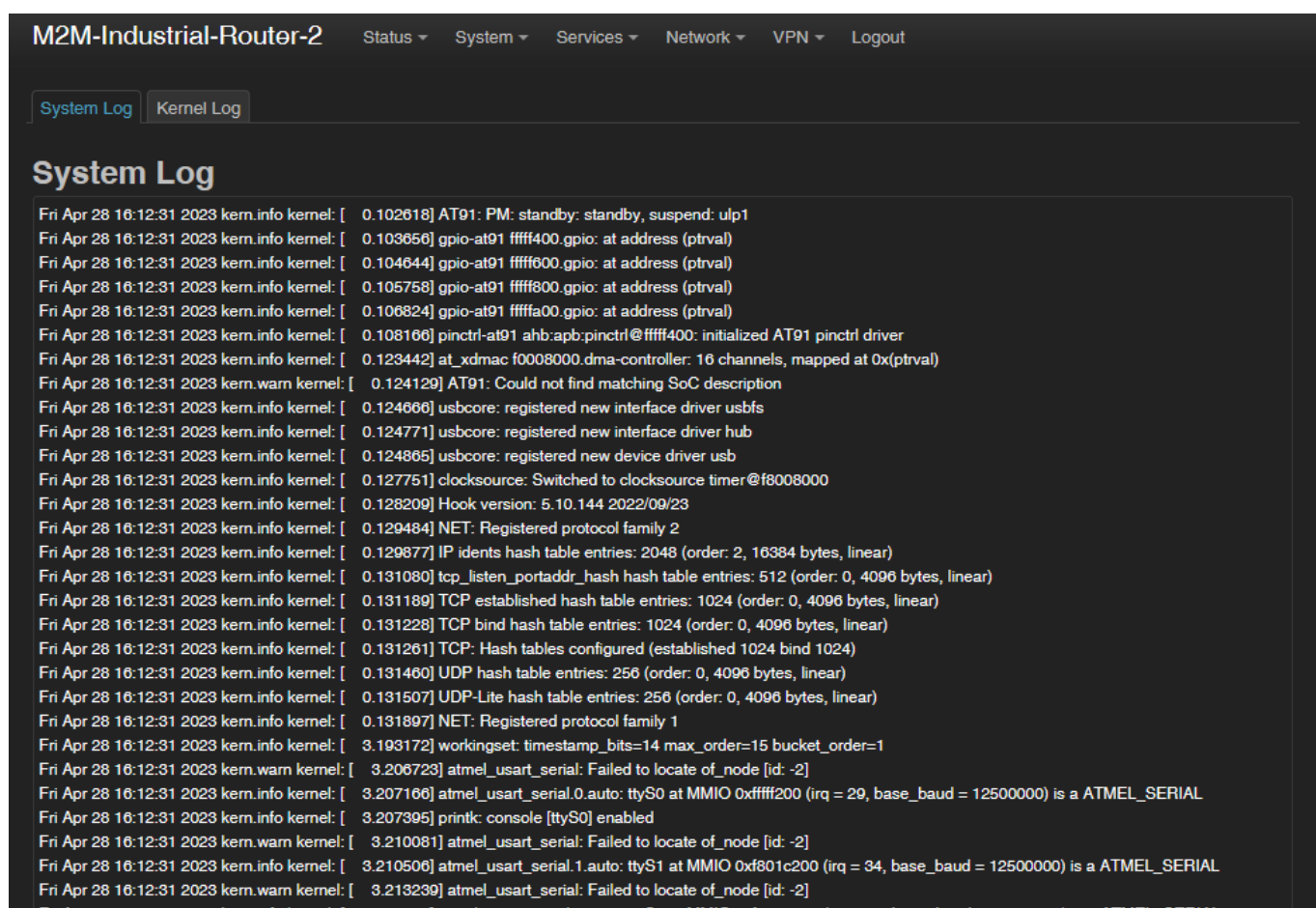
You can limit the size of the log file (**System log buffer size**) and set the IP address of the **External log server** (IP address), **port, protocol** - to send the log files to a remote server.

Press the **Save** button to complete the settings.

There are other log files generated by default, which we have already mentioned in part.

These include in the **Status** / at **System log** menu, which will help you to check the current operation – at the **System Log** tab and the **Kernel log** tab.

This help you to understand some events that have occurred during operation since the DCU was last rebooted. This can be especially useful when found an operation issue, when a features is not available yet, or even if the cellular module indicates some connection trouble.



The screenshot shows the 'System Log' interface for 'M2M-Industrial-Router-2'. The top navigation bar includes 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout'. Below the navigation, there are two tabs: 'System Log' (selected) and 'Kernel Log'. The main content area is titled 'System Log' and displays a list of log entries. Each entry starts with a timestamp 'Fri Apr 28 16:12:31 2023' followed by the log level (e.g., 'kern.info', 'kern.warn') and the kernel name 'kernel:'. The log entries describe various system events, including AT91 PM standby, GPIO address mappings, pinctrl driver initialization, dma-controller mapping, SoC description lookup, usbcore driver registration, clocksource switching, Hook version, NET protocol family registration, TCP/UDP hash table configurations, and atmel_usart_serial driver initialization and failures.

```
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.102618] AT91: PM: standby: standby, suspend: ulp1
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.103656] gpio-at91 ffff400.gpio: at address (ptrval)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.104644] gpio-at91 ffff600.gpio: at address (ptrval)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.105758] gpio-at91 ffff800.gpio: at address (ptrval)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.106824] gpio-at91 ffffa00.gpio: at address (ptrval)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.108166] pinctrl-at91 ahb:apb:pinctrl@ffff400: initialized AT91 pinctrl driver
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.123442] at_xdmac f0008000.dma-controller: 16 channels, mapped at 0x(ptrval)
Fri Apr 28 16:12:31 2023 kern.warn kernel: [ 0.124129] AT91: Could not find matching SoC description
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.124666] usbcore: registered new interface driver usbfs
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.124771] usbcore: registered new interface driver hub
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.124865] usbcore: registered new device driver usb
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.127751] clocksource: Switched to clocksource timer@f8008000
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.128209] Hook version: 5.10.144 2022/09/23
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.129484] NET: Registered protocol family 2
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.129877] IP idents hash table entries: 2048 (order: 2, 16384 bytes, linear)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.131080] tcp_listen_portaddr_hash hash table entries: 512 (order: 0, 4096 bytes, linear)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.131189] TCP established hash table entries: 1024 (order: 0, 4096 bytes, linear)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.131228] TCP bind hash table entries: 1024 (order: 0, 4096 bytes, linear)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.131261] TCP: Hash tables configured (established 1024 bind 1024)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.131460] UDP hash table entries: 256 (order: 0, 4096 bytes, linear)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.131507] UDP-Lite hash table entries: 256 (order: 0, 4096 bytes, linear)
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 0.131897] NET: Registered protocol family 1
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 3.193172] workingset: timestamp_bits=14 max_order=15 bucket_order=1
Fri Apr 28 16:12:31 2023 kern.warn kernel: [ 3.206723] atmel_usart_serial: Failed to locate of_node [id: -2]
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 3.207166] atmel_usart_serial.0.auto: ttyS0 at MMIO 0xfffff200 (irq = 29, base_baud = 12500000) is a ATMEL_SERIAL
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 3.207395] printk: console [ttyS0] enabled
Fri Apr 28 16:12:31 2023 kern.warn kernel: [ 3.210081] atmel_usart_serial: Failed to locate of_node [id: -2]
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 3.210506] atmel_usart_serial.1.auto: ttyS1 at MMIO 0xf801c200 (irq = 34, base_baud = 12500000) is a ATMEL_SERIAL
Fri Apr 28 16:12:31 2023 kern.warn kernel: [ 3.213239] atmel_usart_serial: Failed to locate of_node [id: -2]
Fri Apr 28 16:12:31 2023 kern.info kernel: [ 3.213688] atmel_usart_serial.2.auto: ttyS2 at MMIO 0xf8020200 (irq = 35, base_baud = 12500000) is a ATMEL_SERIAL
```

Chapter 11. Troubleshooting

LED activity

Can you see any LED activity (flashing, lighting)?

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

First you should ensure about the DCU is still under starting / booting phase or not.

Please wait 2-3 minutes, then check the LED signals again. If the **LED1..LED2..LED3** are blank, then the device hasn't got its power supply or it has some trouble.

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

In case of LED blinking after restart

After ca. 2 minutes of the DCU start the **LED2** will be blank and the **LED3** starts to flashing by **green**. This signs that the device begins try to connect to the cellular network (logins to the APN and builds the connection).

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

The device is communicating on the network and will send a couple of minutes later proper *RSSI / CSQ* values and life signals.

Power source

Check that the DCU can get any power through its microfit connector (**POWER**) – power adapter is connected to the router microfit connector and the adapter to the AC plug. Alternatively you can power the device through the USB connection with 5V DC power.

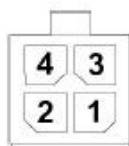
When the device receiving power, the LED signals will sign it. Then the router will be booting and starting its operation.

Wait for ca. 2 minutes, while the interfaces of the device will be availble and it is registering to the wireless network.

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

Check the next figure for the pinout and check the 9-32V DC voltage on the microfit connector (by a multimeter) of the power adapter that it provides DC power or not. If not, than remove the 12V DC adapter and get another one with the proper pinout and voltage.

4-PIN connector (Power Input)



Pin assignment of 4-pin connector

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

Connecting to the router, checking connection

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

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

Ethernet connection

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

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

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

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

Unzip the downloaded zip file into a directory and install.

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

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

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

If the router is not starting

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

Periodic restart of the device (by 10 minutes periods)

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

Restart of the DCU

Restart the router by pushing its **Reset** button on its interface / port side. Push this button for 10 seconds, by a sharp and thin object. The device will be restarted.

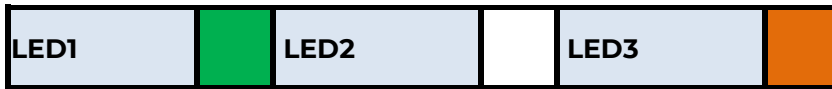
Shutdown / halt the DCU

Pull out the power connector from the AC electricity plug.

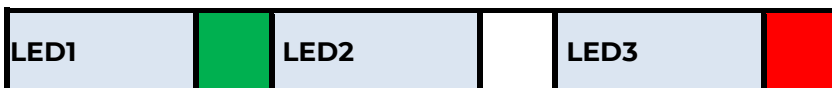
Note, that the router will be still powered if the USB connector was plugged, because the device should receive 5V DC power on USB connection. So, you have to disconnect the USB cable to power down the router.

Note, that the router will not powered off immediately, due to it have supercapacitor components inside. Therefore, the router will getting enough spare power (ca. for up to 10 seconds) to close every connection, interfaces and ports and shutdown the device safely. The shutdown sequence is the following:

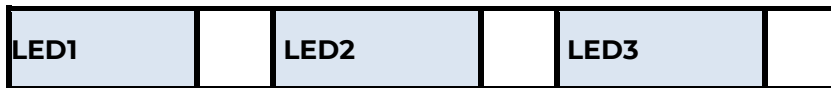
4. The **LED1** will be still active (green) which means that after removing the power from the device, the supercapacitors still having enough power for powering the device. But the **LED3** will be lighting by **orange** color. This shows, that the router interfaces are during disconnection and the system will be halted soon.



5. Soon, the **LED3** lighting will be changed to color **red**, which means that the system is under power down.



6. Soon, when the supercapacitors will be exhausting and the system is down, the **LED1** and **LED3** will be also blank, which means that the router is halted.



Antenna

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

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

Check RSSI signal value and vital signals on the OpenWrt web interface.

In case of using LTE 4G or Cat.M, Cat.NB (Narrow Band) networks – always use the proper antenna which is harmonizing to the frequency/band. In other way the router will not able to access the cellular network.



SIM/APN failure

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

If the device is not registering to the network, then the modem was not initiated properly, and the router will restart itself after 10 minutes. This could be caused by a not proper APN setting.

Check with your mobile service provider that issues your SIM card for the APN names and passwords you are using.

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

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

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

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

SIM card cannot be detected

Turn off the router - unplug the power plug from the **POWER** connector of the device. Then, make sure that there is a SIM card in the **SIM** slot with the chip facing up and the bevelled corner facing inward, and then push the card in until it stops. Check with your mobile service provider that the SIM card is active and ready to use data packet (IP communication).

Restart the router by reconnecting the power connector.

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

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

Always use the proper antenna type regarding to the module and mobile network, which is harmonized to the frequency/band. In other way the router will not able to access the network.

Note that for Narrow Band (NB-IoT) networks it could be needed to wait 5-15 minutes for the first successfully network registration.

Chapter 12. Support availability

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

E-mail: support@wmsystems.hu

Phone: +36 20 333 1111

12.1 Contact the support line

For the proper identification of the router you should use the sticker on the device, which contains important information for the call center.

Attach the OpenWrt related important information – marked - of modem identifiers to the problem ticket, which will help resolving the problem! Thank you!

12.2 Product support

Documentation and released firmware for the product can be accessed via the following link.

<https://m2mserver.com/en/product/m2m-industrial-router-2-dcu-mbus/>

Online product support can be required here:

<https://www.m2mserver.com/en/support/>

Chapter 13. Legal notice

©2024. WM Systems LLC.

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

The pictures in the user guide are only for illustration purposes.

WM Systems LLC. does not acknowledge or accept responsibility for any mistakes in the information contained in the user guide.

The published information in this document is subject to *change without notice*.

All data contained in the user guide is for information purposes only. For further information, please, contact our colleagues.

Warning

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