

User Manual

Industrial DIN Rail Router®



Rev: 1.20

2024-04-15

Document specifications

This document was completed for the **Industrial DIN Rail Router**[®] device and contains the hardware specification, with the most important information and software settings of the device.

Document category:	User Manual
Document subject:	Industrial DIN Rail Router [®]
Author:	WM Systems LLc
Document version No.:	REV 1.20
Number of pages:	84
Hardware Identifier No.:	BE0112B_LM_MODEM, BE0115A_LM_MODEM_EG915
Linux Kernel version:	5.10.154
OpenWRT Firmware version:	202308233 or later
STM32 Firmware version:	202308233
Document status:	Final
Last modified:	15 April, 2024
Approval date:	15 April, 2024

Table of contents

CHAPTER 1. Product information	5
CHAPTER 2. Technical data.....	7
2.1 Power voltage / Current ratings	7
2.2 Cellular modules (order options)	7
CHAPTER 3. Device exterior design and appearance	8
3.1 Safety cautions	9
3.2 Mounting, fastening	11
3.3 Antenna.....	11
3.4 Further accessories.....	12
CHAPTER 4. Software system.....	13
4.1 Operation system.....	13
4.2 Device Manager platform	13
4.4 Accessing the router (via SSH connection).....	13
CHAPTER 5. Starting the device	14
5.1 Connecting the router	14
5.2 First start.....	15
5.3 Web user interface of the router	16
5.4 Access via SSH connection	18
CHAPTER 6. Web Administration user interface	20
6.1 Main page (Dashboard).....	20
6.2 Menu	22
6.3 Status menu.....	22
6.4 System menu.....	22
6.5 Services menu	23
6.6 Network menu	24
6.7 VPN menu.....	24
CHAPTER 7. Important notes.....	25
CHAPTER 8. Network configuration of the router	28
8.1 Interface settings	28
8.2 Cellular / Mobile internet settings	31
8.3 Ethernet (LAN) settings	32
8.4 DHCP, DNS settings.....	33
8.5 DNS settings.....	35
8.6 Defining the route rules	35
8.7 Firewall settings.....	36
8.8 Port Forward settings	41
8.9 IP routing, NAT settings.....	42
8.10 Dynamic DNS settings	43

CHAPTER 9. Special settings	44
9.1 Ping an IP address.....	44
9.2 Network Time Service (NTP)	44
9.3 TFTP settings.....	45
9.4 LED configuration	46
9.5 Remote access (SSH)	47
9.6 UCI usage from the command line	48
9.7 IPSec settings	49
9.8 VPN client (OpenVPN) configuration	50
9.9 RS485 / Modbus settings (Ser2net).....	53
9.10 Data collection settings (RS485 / Modbus).....	57
9.11 Voice call settings.....	63
9.12 Run commands remotely (SMS config settings)	64
CHAPTER 10. Software refresh and router maintenance	66
10.1 Firmware refresh	66
10.2 Installing applications	68
10.3 Restarting the router	71
10.4 Shutdown / halt of the router.....	72
10.5 Start the router.....	72
10.6 Reset the router configuration	72
10.7 Password change.....	73
10.8 Backup and restore of settings	73
10.9 Start or stop a system service	76
10.10 Log.....	77
CHAPTER 11. Troubleshooting.....	79
CHAPTER 12. Support availability	83
12.1 Contact the support line.....	83
12.2 Product support	83
CHAPTER 13. Legal notice	84

Chapter 1. Product information

This industrial LTE router is compact and small in size, making it suitable for various M2M and IoT applications such as smart metering and industrial automation.

The router can be ordered with LTE Cat.4, Cat.1 or Cat.M/Cat.NB module versions.

It can be mounted on a DIN-rail for easy installation.

The router is a cost-effective solution for connecting multiple industrial devices, energy meters, and sensors with a single router.

This device enables remote reading of multiple industrial systems and transmits the data to a central server, including AMI (HES) or Smart Grid infrastructures.

Our cellular router has been specifically designed for industrial and metering environments. It can be mounted on a DIN-rail as an external router and connected to multiple devices simultaneously, such as industrial measurement systems, utility meters, and sensors.

The router features industry-standard interfaces and protocols, making it suitable for use in industrial automation and smart metering.

You can connect your devices to a central server by creating a transparent data link, allowing you to access them remotely.

The router features several interfaces for connecting industrial devices, including Ethernet, RS232 and RS485 ports, and a DI (digital input) interface. It comes in a plastic IP31 housing that can be securely mounted to a 35mm DIN rail.

The device operates on the open-source, Linux-based OpenWRT® operating system and is compatible with our Device Manager® platform.

Ports / Interfaces

The device offers the following ports: Ethernet, RS232, RS485, and a DI port (digital input).

The serial and RS485 ports are suitable for connecting consumption meter devices or industrial measurement devices.

The digital input is suitable for status monitoring of devices, switches or tamper protection.

System Software

The router 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.

Management

Remote management of router using Device Manager® software (order option).

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

Security features

The router's watchdog circuit is 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.

During communication of the router and the Device Manager, you can also choose a secure TLS v1.2 connection (option).

The software of the router applies unique passwords, firewall.

Chapter 2. Technical data

2.1 Power voltage / Current ratings

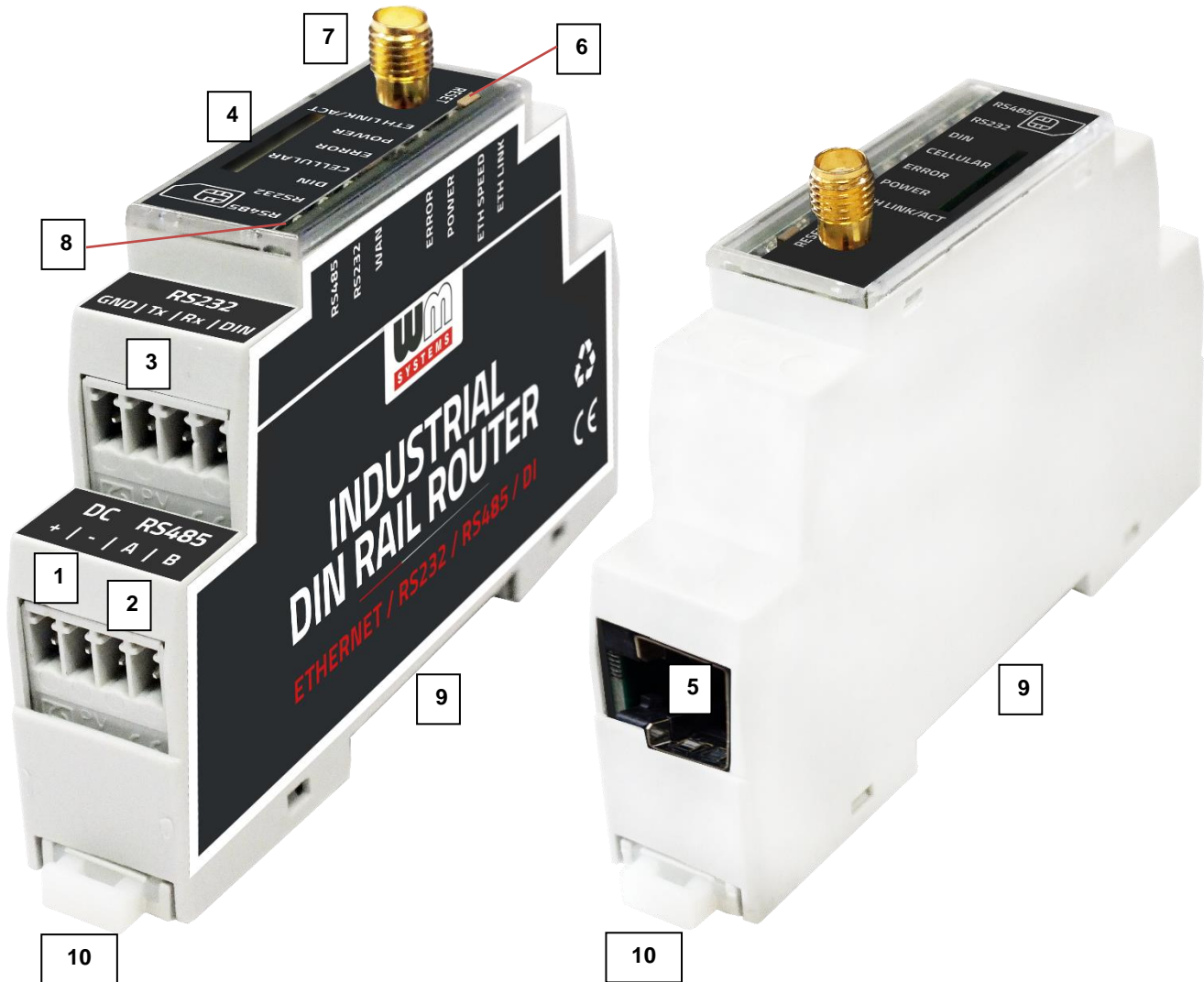
- **Power Voltage / Ratings:** · 12V DC, 1A power supply (9-28VDC) – powered via 2-pin power input connection (from external 12V DC power adapter)
- **Current / Consumption:** Average: 200mA - 320mA, 12VDC (according to module version) / 2.4W – 3.84W, 12VDC

For the **DC power connection** it is recommended to use a 12V / 24V DC power adapter (order option).

2.2 Cellular modules (order options)

- **LTE Cat.4 / 3G / 2G module:** SIMCom A7602A
- **LTE Cat.4 / 3G / 2G module:** SIMCom A7608SA-H
- **LTE Cat.1 with 2G „fallback” module:** Quectel EG915N-EU
- **LTE Cat.1 / 3G / 2G module:** Quectel EG91-EX
- **LTE Cat.M / Cat.NB module:** Quectel BG95-M2
- **LTE Cat.M / Cat.NB with 2G „fallback” module:** Quectel BG95-M3
- **LTE Cat.M / Cat.NB / 450MHz module:** Quectel BG95-M4
- **LTE Cat.M / Cat.NB / 450MHz with 2G „fallback” module:** Quectel BG95-M8

Chapter 3. Device exterior design and appearance



***Industrial DIN-Rail router, assembled in plastic casing
with interface connectors / ports***

- 1 – POWER (9-28V DC): 2-pin terminal block connector (for 12V/24V DC power)
- 2 – RS485 port: 2-pin terminal block connector, pinout from left-to-right: A, B
- 3 – RS232 / DIN: 4-pin terminal block connector, pinout from left-to-right: GND, Tx, Rx (RS232) / GND, DIN (Digital Input)
- 4 – *SIM card slot (2FF)
- 5 – Ethernet (RJ45, 10/100 Mbit)
- 6 – Reset button
- 7 – Antenna connector (SMA-M, 50 Ohm)
- 8 – 7pcs operation LEDs (on top plastic cover)
- 9 –DIN-Rail adapter (35mm standard)
- 10 – Fastening locker of DIN-Rail adapter

**SIM insertion: push the APN-activated SIM into the SIM tray (4) - the SIM chip surface should look to the center of the device. The bottom-side, cutted edge of the SIM should look down, closer to the router. Insert the SIM into the cutted rectangular hole of the product casing's top cover. Then push the SIM until it will be fastened (you will hear a soft click sound).*

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 router 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 9-28V DC power supply within the enclosure, and the enclosure should NOT be opened or the PCB touched.

Router current and consumption

- Power voltage: 9..28 VDC
- Current: 200mA - 320mA, 12V DC
- Consumption: 2.4W - 3.84W (according to module selection)

The IP31 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 router.
- 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 router 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 casing bottom part can be fixed to a 35mm DIN-rail using its built-in DIN-rail fastener. The mount / fastening can be performed by pulling out fastening lockers on two-sides of the product casing's bottom part. Then installing to the DIN rail and release of the lockers. The router will be fastened to the rail.

3.3 Antenna

We offer different small LTE antenna types for the device (order options).

More information:

<https://m2mserver.com/en/product-category/accessories/>

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.

Important! Always turn off the router before mount an antenna or change an antenna to another type.

3.4 Further accessories

DC power adapter:

Connector: 2-pins

Function: 12V DC 1.25A power voltage for the router

More information:

<https://m2mserver.com/en/product/power-supply-hdr-15-12/>

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 router 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 Device Manager platform

The Device Manager® software can be used for the remote management of the routers. 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 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.

4.3 Accessing the router (via SSH connection)

The router can be also accessed via an ssh connection, either remotely through the cellular network 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 router

1. Ensure that the router is **not under power voltage**, therefore the power adapter cable should be removed from the **DC** titled connector (1) – or the adapter is not connecting to the power network. Ensure, that all the LEDs (8) are blank.
2. **Mount** a proper **LTE antenna** to the left **SMA connector** (7).
3. **Insert an activated SIM card** to the SIM slot (4) - the SIM chip surface should look to the center of the device – as it can be seen on the photo. The bottom side, cutted edge of the SIM should look down to the direction of the router.

Insert the SIM into the cutted rectangular hole of the product casing's top cover. 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 should power off the router and push down the SIM card a little bit, while it will be released and can be removed from holder.

4. Based on the needs, **connect** the related **cables** to the interfaces – to **RS232** terminal block (port nr. **3**, left 3-pins), to **RS485** terminal block (nr. **2**, right 2-pins), to **DI** (digital input) terminal block (nr. **3**, left and right side pins) – according to the interface titles. The wiring / connection can be performed by using the opposite side (**green**, terminal block pluggable connectors).



The serial and RS485 ports are suitable for connecting consumption meter devices or industrial measurement devices.

5. In case of wiring **DI** (logical / digital input), you should wire the **GND** pin (common with RS232) and the **DIN** pin. The DI input is suitable for status monitoring of devices, switches or tamper protection.
6. **Connect an UTP cable** to the router's **Ethernet** RJ45 port (5). It should be connected to the PC's Ethernet port. (You should configure the Ethernet port settings on PC side). For permanent usage, later an industrial device can be connected to the Ethernet port if it requires.



5.2 First start

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

1. **Connect 9-28V DC power source** (or use a 12V/24V DC adapter) to the 2-pin **DC** (1). **terminal block connector**. Then the router begins its operation, where the LED lights will be signing and inform you about the current status of the device.
2. After 5 seconds of powering the router, **POWER** LED will be lighting by **green**, to sign presence of DC power.



3. If a device is connected to **Ethernet** (RJ45) cable, the **ETHERNET** LED will be lighting by **green**, or flashing to indicate the network traffic.
4. The system start after power on the devices requires about 1-2 minutes, while it loads the necessary software modules and prepares the web user interface, then the router will be ready to login.
5. If the **RS232**, the **RS485** or the digital input (**DI**) was connected and having traffic, then the related LED(s) of the connection will also indicate it by **green**.
6. **Configure the device's wireless internet module settings** (SIM and APN data on the router web interface) **for the cellular internet connection** – otherwise the router will be restarting in ever 10 minutes.

Attention!

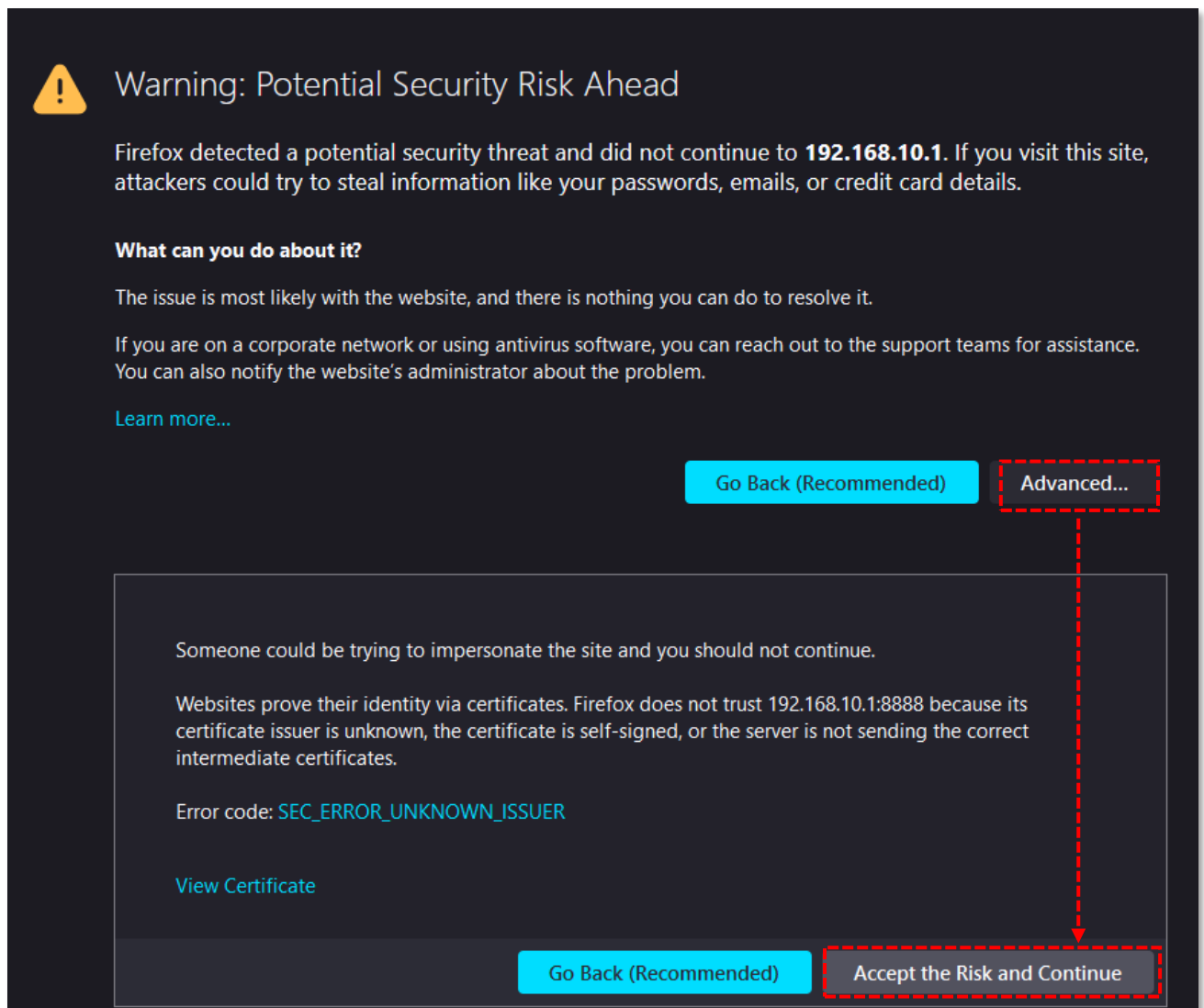
- We suggest to change the login password on the web interface.
- If it is necessary, enable the DHCP service.
- Enable and configure the firewall rules and IP route rules for the connecting devices on Ethernet port, RS485 port, cellular network.
- Check the RS485 connection settings (in **Ser2net** menu)
- Configure the RS485 / Modbus settings (in **Data Collection** menu)

7. If the cellular network registration is in progress on APN, the **CELLULAR** LED will flashing by **green**. The successful network registration of the device is signed by **green** lighting of the LED – after performing the proper settings. It will show that the router can access the cellular network or not.

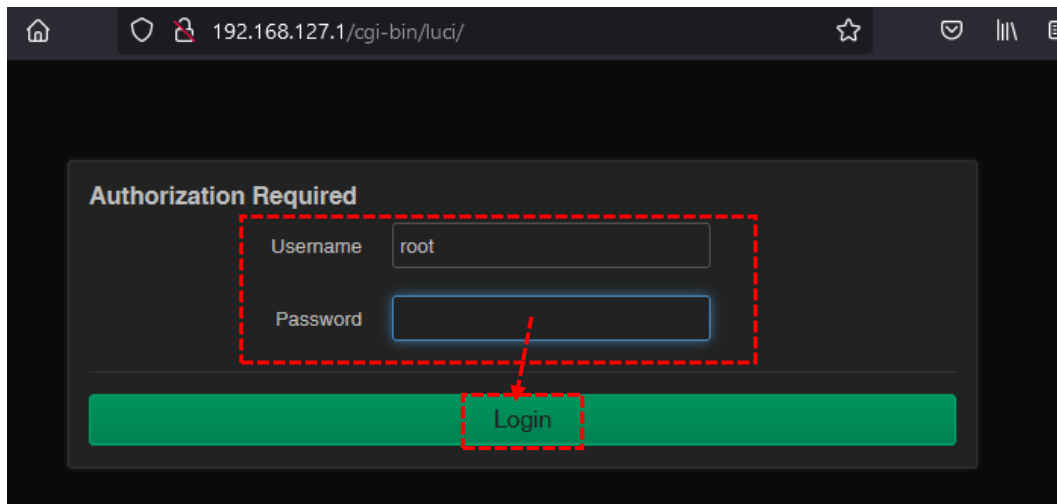
5.3 Web user interface of the router

1. To connect to the router, allow the IP address for Ethernet connector interface in the Windows®'s network settings (IP address for Ethernet connection: **192.168.127.x** (where „**x**” can be between 2 and 255), Subnet mask: 255.255.255.0).

2. Open the router's local website in an internet browser. The default web user interface (LuCi) URL on **Ethernet** port: <https://192.168.127.1>
3. At the first time, you have to accept the security risk in the browser by choosing the **Advanced** option at the **Potential Security Risk**.
4. Then choose „**Accept the Risk and Continue**” option and the login screen of the web administration user interface will appear.



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



Attention! Change the login password before connecting the router to the public cellular network!

5.4 Access via SSH connection

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

1. Connect to the **192.168.127.1:22** IP address.
(Login: **root**, Password: **wmrpwd**)
2. **Accept** the security risk (RSA token) encryption key usage warning notice (visible at first time only).

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

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

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

https://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 (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 services by using UCI.

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 router. At the **System** part you can check that the **Firmware version**. It should be 202308233 or newer version.

The screenshot displays the web administration interface for a DIN_Rail_Router. The top navigation bar includes 'DIN_Rail_Router', 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout', along with a 'REFRESHING' button. The main content is divided into three sections: 'Status', 'Memory', and 'Modem'.

Status

System

Hostname	DIN_Rail_Router
Model	DINModem-Standard
Firmware Version	202306141
Architecture	ARMv7 Processor rev 5 (v7l)
Target Platform	sunxi/cortexa7
Kernel Version	5.10.154
STM32 Firmware	
Local Time	2023-05-17 12:46:14
Uptime	0h 1m 28s
Load Average	1.24, 0.43, 0.15

Memory

Total Available	17.62 MiB / 54.18 MiB (32%)
Used	32.00 MiB / 54.18 MiB (59%)
Cached	10.85 MiB / 54.18 MiB (20%)

Modem

Modem Model	EG915N
Firmware Version	EG915NEUAGR03A09M16
Serial	866760050925181
IMSI	216012325017267
SIM ID	8936200003250172672F
Operation Mode	-
Operator	Yettel HU
Access Technology	3 (-)

The **Local Time** shows the current time (received from NTP or mobile operator), the **Uptime** shows the spent time since the last reboot/start.

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

You can also identify the **Network code** and **Network Cellid** (cell identifier).

CSQ/RSSI (in dBm) shows the quality of the cellular network (signal strength). (Lower RSSI value significant to a better signal level / higher CSQ value means better signal).

The screenshot displays the Mikrotik WinBox interface for a router named 'DIN_Rail_Router'. The top navigation bar includes 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout'. A 'REFRESHING' button is visible in the top right corner.

Modem Status:

Operator	Yettel HU
Access Technology	3 (-)
CSQ/RSSI	23 (-68dBm)
CSQ/BER	0
MCC-MNC	-
Network Registration	1
Network Code	0E1C
Network Cellid	3FDF

Storage:

Disk space	320.00 KiB / 2.19 MiB (14%)
Temp space	308.00 KiB / 27.09 MiB (1%)

Network:

IPv4 Upstream

Protocol: PPP-4G
Address: 37.234.31.72/32
Gateway: 10.64.64.64
DNS 1: 217.79.129.76
DNS 2: 217.79.128.40
Connected: 0h 44m 19s

Device: Tunnel Interface: "4g-wan"

Active Connections: 42 / 7168 (0%)

Active DHCP Leases

Hostname	IPv4 address	MAC address	Lease time remaining	Static Lease
There are no active leases				

Active DHCPv6 Leases

Host	IPv6 address	DUID	Lease time remaining	Static Lease
There are no active leases				

At the **Network** part you can ensure that the router is on **WAN** (cellular) network or not. Here you will find the IP **Address**, which got from mobile operator network.

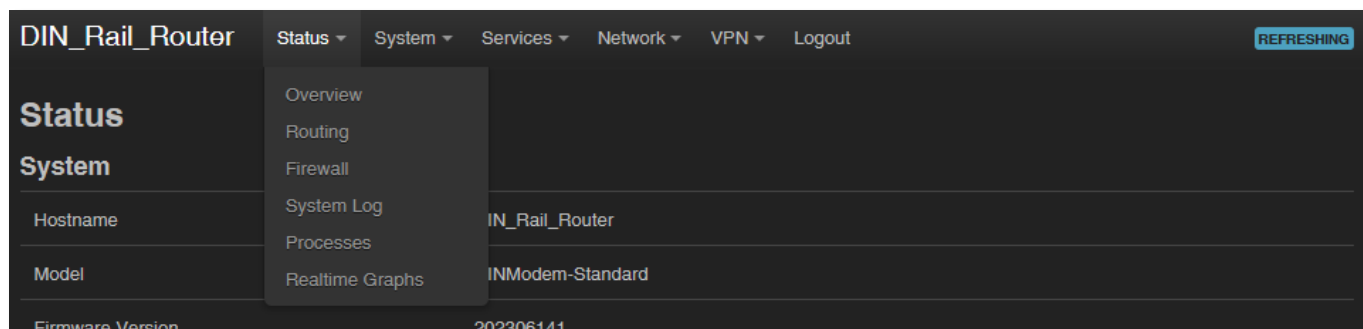
6.2 Menu

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/restoration of the configuration settings, LED configuration, reboot, etc.
- **Services** – Dynamic DNS settings, ser2net settings (RS232/RS485), Data Collection (settings of RS485 Modbus, PLC register readout) – optional
- **Network** – network interface settings, DHCP, DNS, hostname, IP route rules (static routes), diagnostics, Firewall, voice call config, SMS config
- **VPN** – OpenVPN settings

6.3 Status menu

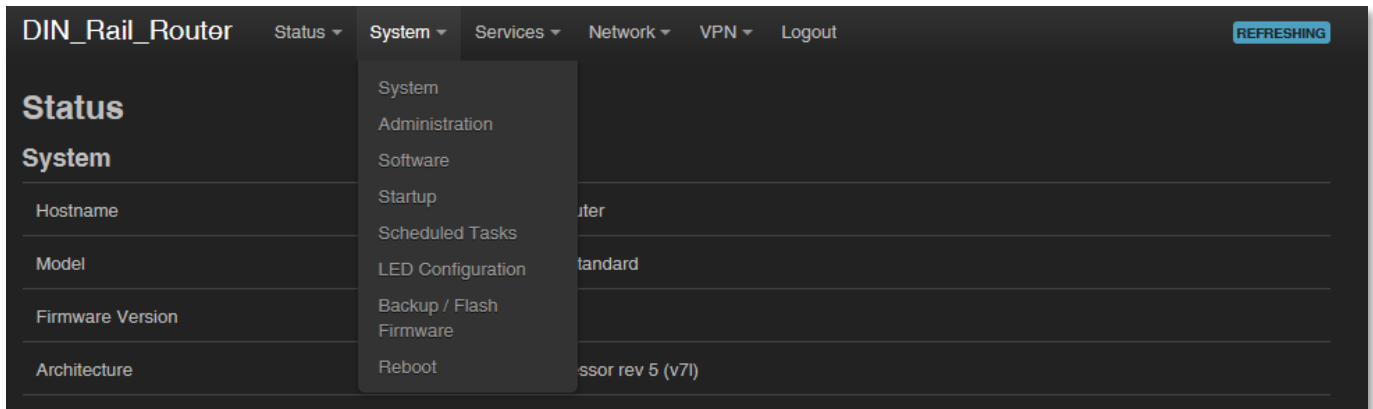
- In the **Status** menu you can check the current status (in **Overview**).
- at the **Routing** item the valid/active route settings.
- at the **Firewall** item, you can see the firewall events and information.
- check the system messages and event log (**System Log, Kernel Log**).
- activities of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



6.4 System menu

You can find several system settings in these menu items:

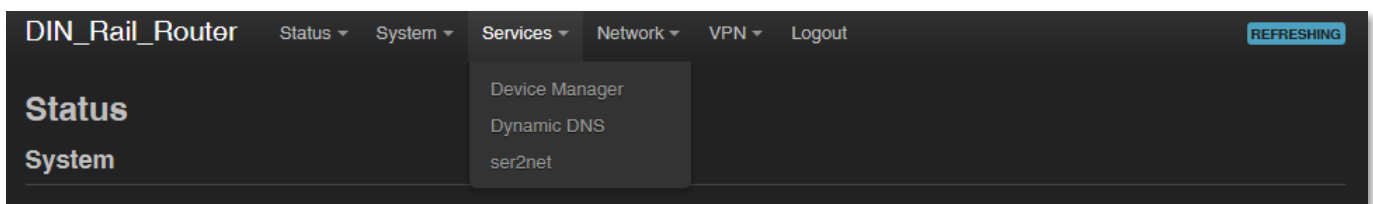
- In the **System** menu: **Hostname** (router name), **Time synchronisation** (time and NTP server settings), **Logging, Language** (of user interface)
- **Administration: Router Password** (for user interface) and the **SSH Access**
- Installation of further **Software** (3rd party tools, applications) 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** update, backup or restore settings
- **Reboot** the router

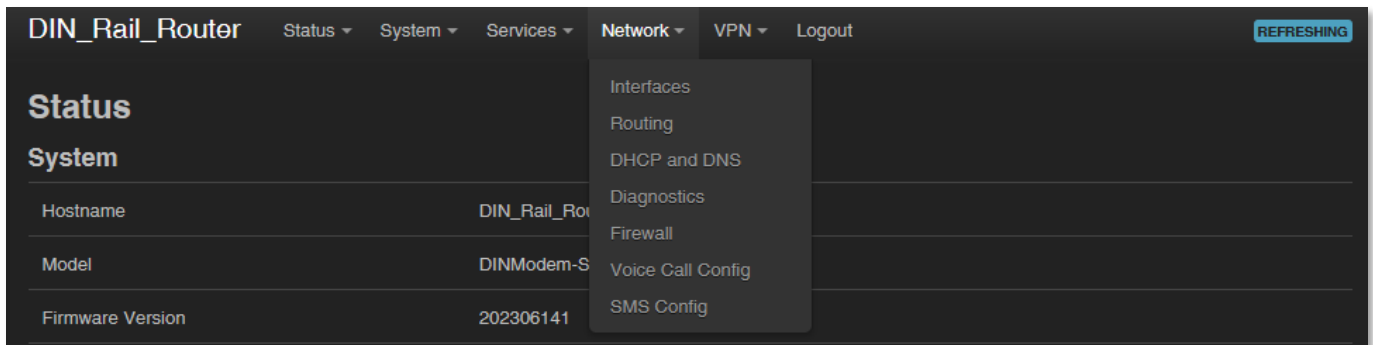
6.5 Services menu

- Here you can setup the **Device Manager** server settings
- **DynDNS** (dynamical DNS) service settings can be also performed
- In **Ser2net*** menu you can configure RS485 / Modbus operation settings
- In the **Data collection** menu you can configure the parameters of Modbus / PLC data collection – order option



6.6 Network menu

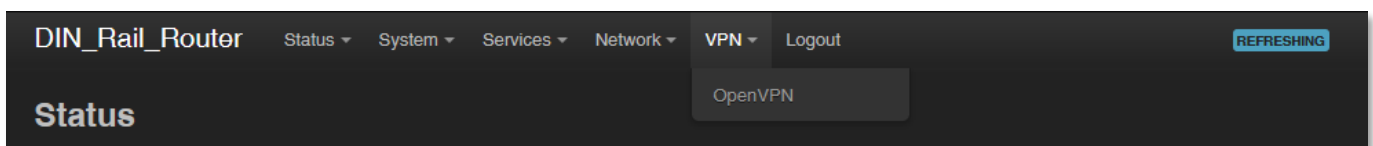
- Here you can configure the settings of each network **Interfaces**.
- **Routing** – static route paths can be also defined here.
- You can modify the **DHCP and DNS** settings.



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

6.7 VPN menu

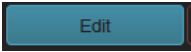
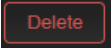
- You can configure the **OpenVPN** settings here



Anywhere in the menus, a setting can be stored with the **Save** button. The **Save & Apply** button stores the settings and reconfigure the router related on these settings.

Chapter 7. Important notes

- For security reasons, we do recommend to **change the password** as soon as you can for accessing the administration web user interface. Read Chapter 10.6 for detailed settings.
- Some protocols are disabled by default on the router, but most of them you can enable to use:
 - The **DHCP** service is turned off by default. When enabled, the router assigns IP addresses to connected devices, while the available Ethernet interface addresses use **static** addresses. If you want to assign IP addresses by DHCP, change the protocol value to **DHCP client**. You can do this in the **Network / DHCP and DNS settings** menu or under the **Network / Interfaces** menu, in the **LAN** interface, in the **DHCP** section.
 - The **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 data collection can be switched on and configured in **Services / Data Collection** menu. Read Chapter 9.10 for detailed settings.
- Some protocols are disabled by default on the router and you cannot use them, but you can make a request and indicate your requirement before ordering:
 - The **IPv6** protocol is disabled for **LAN** interface 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 router from external DoS attacks and unauthorized intrusions. For reliable operation, review the settings and allow only the necessary communication.**

- We do recommend to disable all ports and protocols in the **Firewall** that you are not currently using (connection / channel / data transfer) taking into account access to the required ports and channels. To check this, the **Status / Firewall** menu section is an excellent option for scanning through traffic and the **Network / Firewall** menu, where you can add new rules or modify existing ones.
- Please check the network traffic of the router frequently in the **Status / Firewall** menu (port number, incoming IP, especially outgoing data traffic and downloaded data).
- Measure throughput and network traffic (per minute, per hour) - with the help of the **Status / Realtime Graphs** menu or **Statistics / Graphs** where you can view the calculated and expected traffic volumes, which is important if you want to avoid congestion. or the data traffic limit of the SIM card used is limited.
- If necessary, you can select a dedicated mobile network type (such as LTE only, Cat.M / NB-IoT only, etc), 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 router constantly checks the interfaces and the viability of the connections. In case of a power failure or power failure event, the network and data connections are automatically reconnected after the conditions are restored.
- If you do not want to use the router on a mobile network, but as a wired Ethernet router, then configure that in the **Network / Interfaces** menu, remove the **WAN** interface with the  button. From then on, the router will not be restarted even if no SIM card is inserted.
- **HTTP**, **HTTPS** redirect and HTTPS certifications and **SSL** certifications are used.

- The industrial **RS485** data speed rate can be configured between 300 and 19 200 baud. We suggest to use the standard 9 600 baud (for industrial measurement systems and devices) or the 1 200 baud / 2 400 baud (for utility meters) rate setting for the better compatibility.

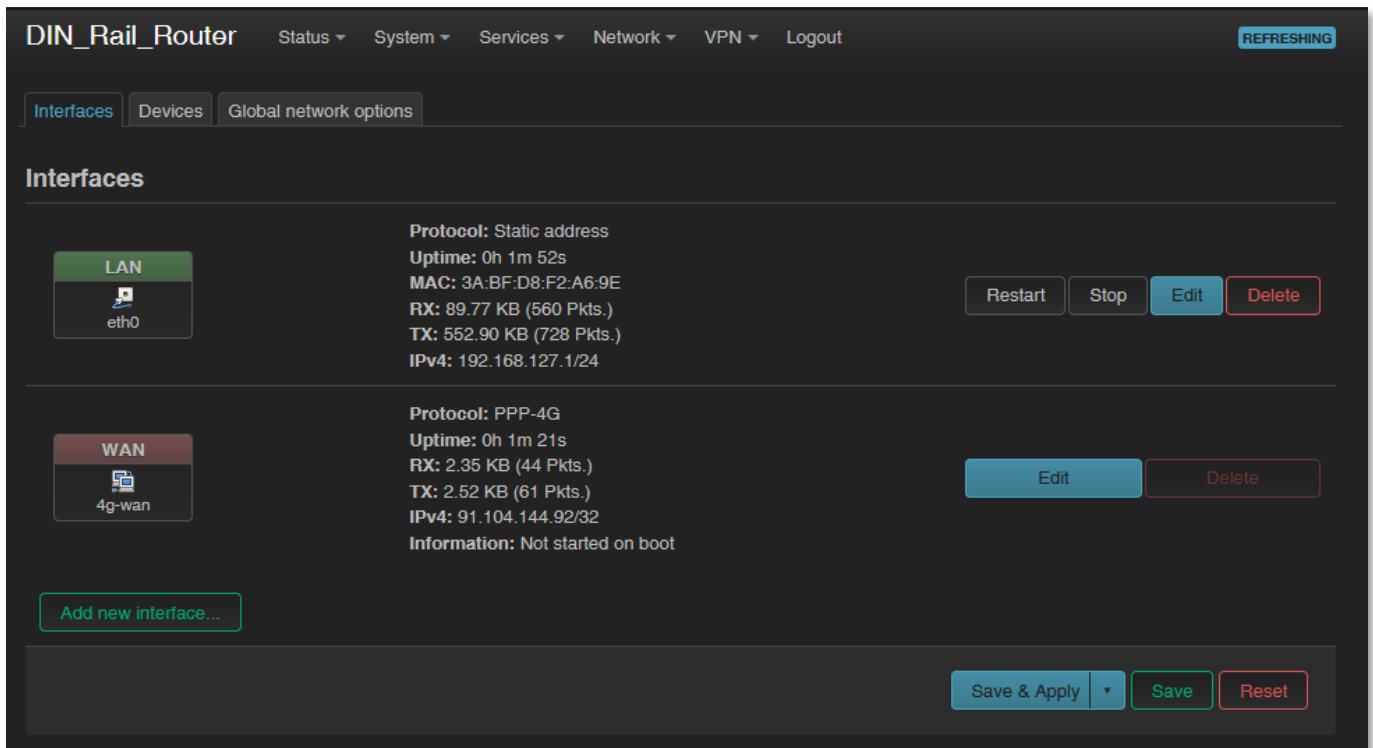
Chapter 8. Network configuration of the router

8.1 Interface settings

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

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

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



Modifying the LAN interface settings

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

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

At the upper **WAN**, **LAN** title you will found 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 or Cat.NB or 2G 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 a device icon and text: '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 showing 'Automatic'. Below it are input fields for 'APN' (containing 'internet'), 'PIN', 'PAP/CHAP username', and 'PAP/CHAP password' (with a masked asterisk). 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 four options: 'Automatic' (highlighted), 'GSM only', 'LTE only', and 'WCDMA only'. The dropdown is set against a dark background.

Fill the **APN** name. If you won't set any value for **APN**, the router 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.

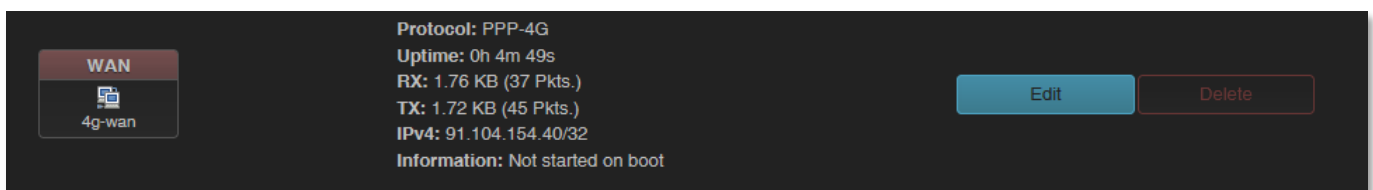
Important! Note, if your SIM is not using PAP/CHAP authentication, please delete the content of the **PAP/CHAP username** and **PAP/CHAP password** fields.

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

The module tries to register to the cellular network. When the cellular network registration is in progress on APN, the **CELLULAR** LED will flashing by **green**. The successful network registration of the device will be indicated by **green** lighting, which shows that the router 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.



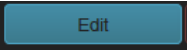
WAN 4g-wan	Protocol: PPP-4G Uptime: 0h 4m 49s RX: 1.76 KB (37 Pkts.) TX: 1.72 KB (45 Pkts.) IPv4: 91.104.154.40/32 Information: Not started on boot	Edit	Delete
----------------------	---	-------------	---------------

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.

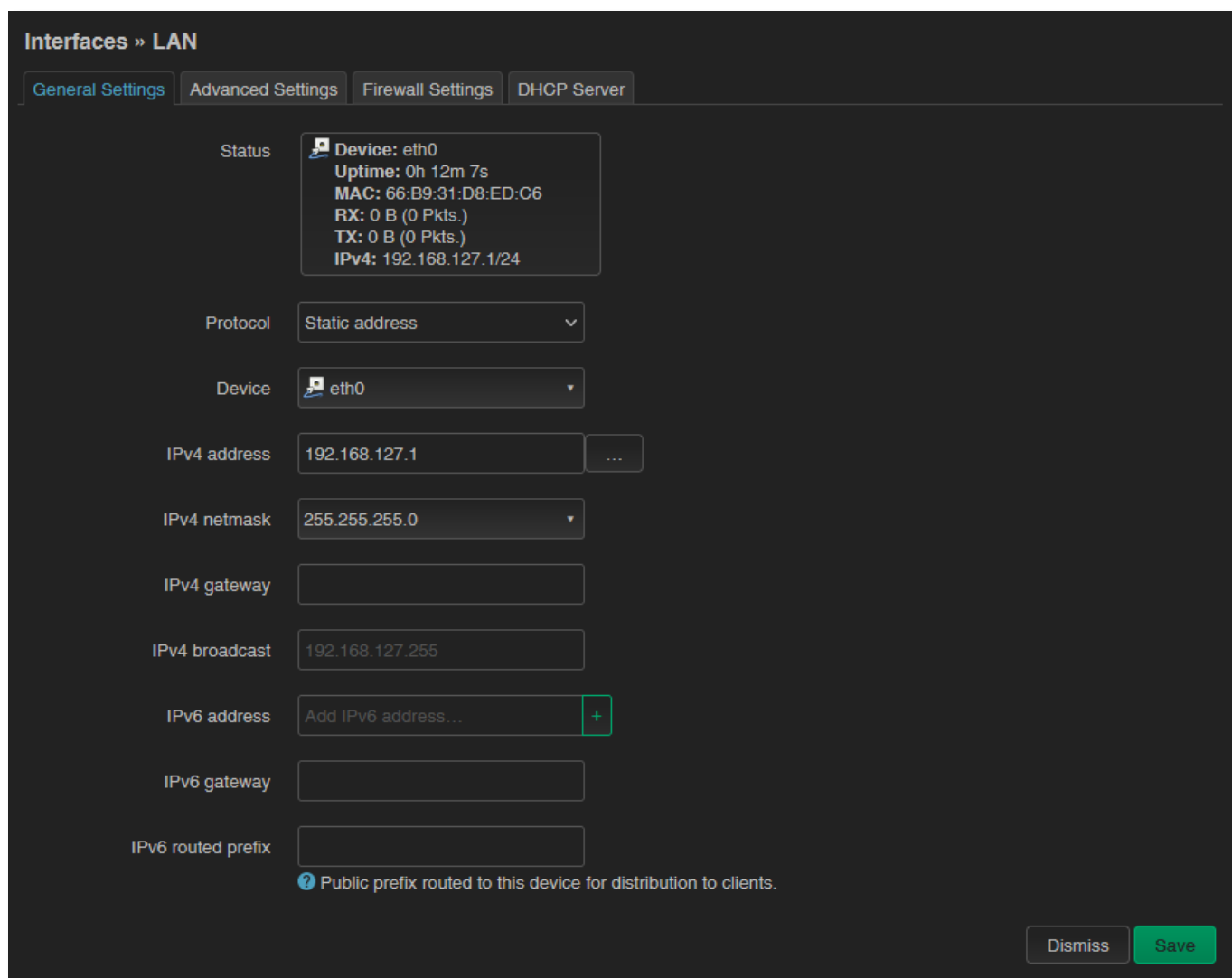
You can find further network settings at [Advanced Settings](#) tab.

You can also check the **Status Overview** menu, where at **Network** part you can ensure that the router is on WAN (cellular) network or not. Here you will find the **IP Address**, which got from mobile operator network.

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).




Interfaces » LAN

[General Settings](#) [Advanced Settings](#) [Firewall Settings](#) [DHCP Server](#)

Status  Device: eth0
Uptime: 0h 12m 7s
MAC: 66:B9:31:D8:ED:C6
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 192.168.127.1/24

Protocol Static address


Device  eth0

IPv4 address 192.168.127.1

IPv4 netmask 255.255.255.0


IPv4 gateway

IPv4 broadcast 192.168.127.255

IPv6 address Add IPv6 address... 

IPv6 gateway

IPv6 routed prefix

 Public prefix routed to this device for distribution to clients.

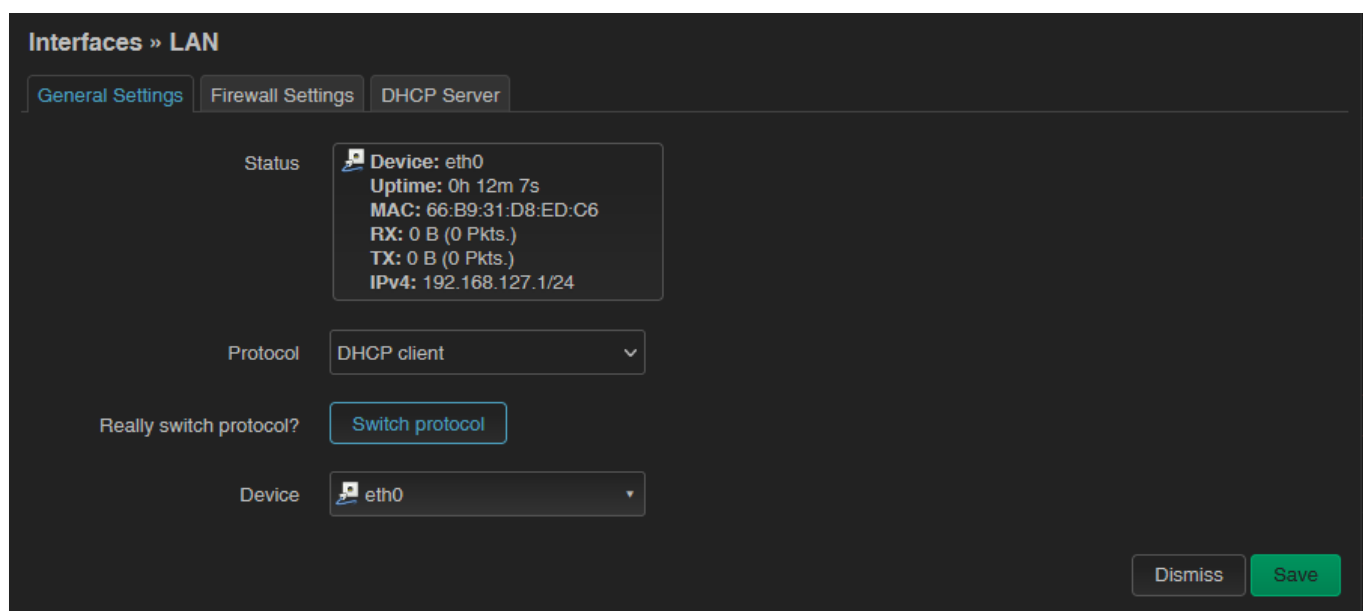
[Dismiss](#) [Save](#)

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

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

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

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



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

8.4 DHCP, DNS settings

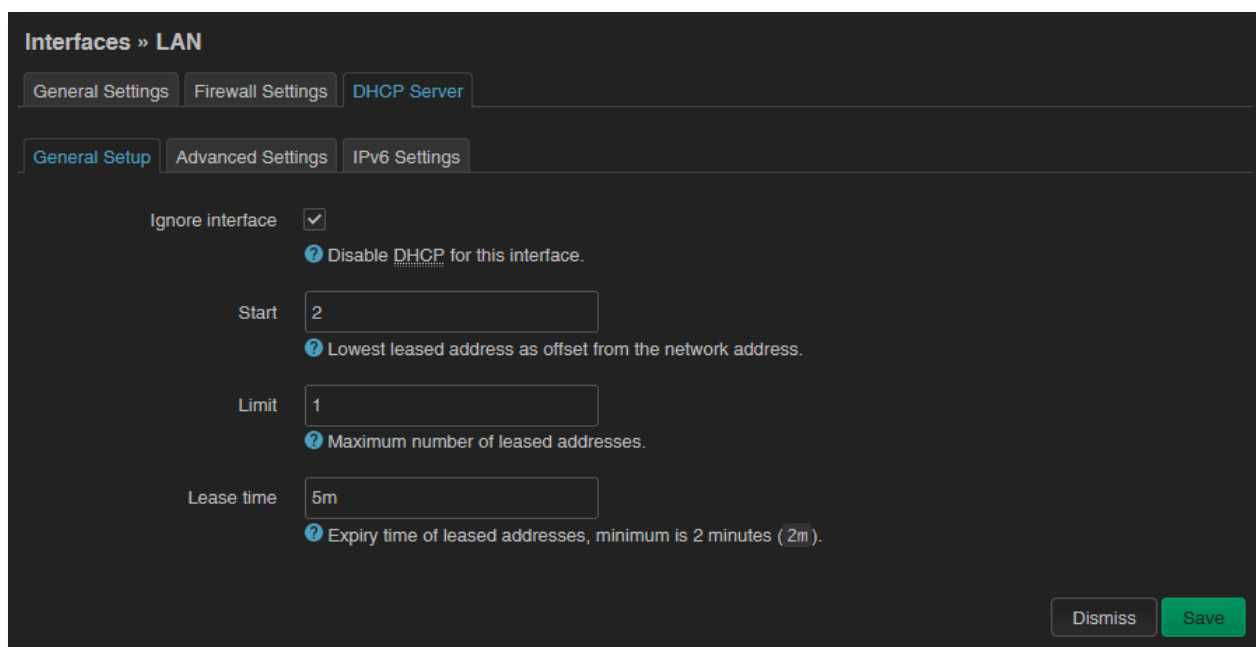
The DHCP service allows the automatic IP address providing for the connecting devices in the current IP segment by the router.

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

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

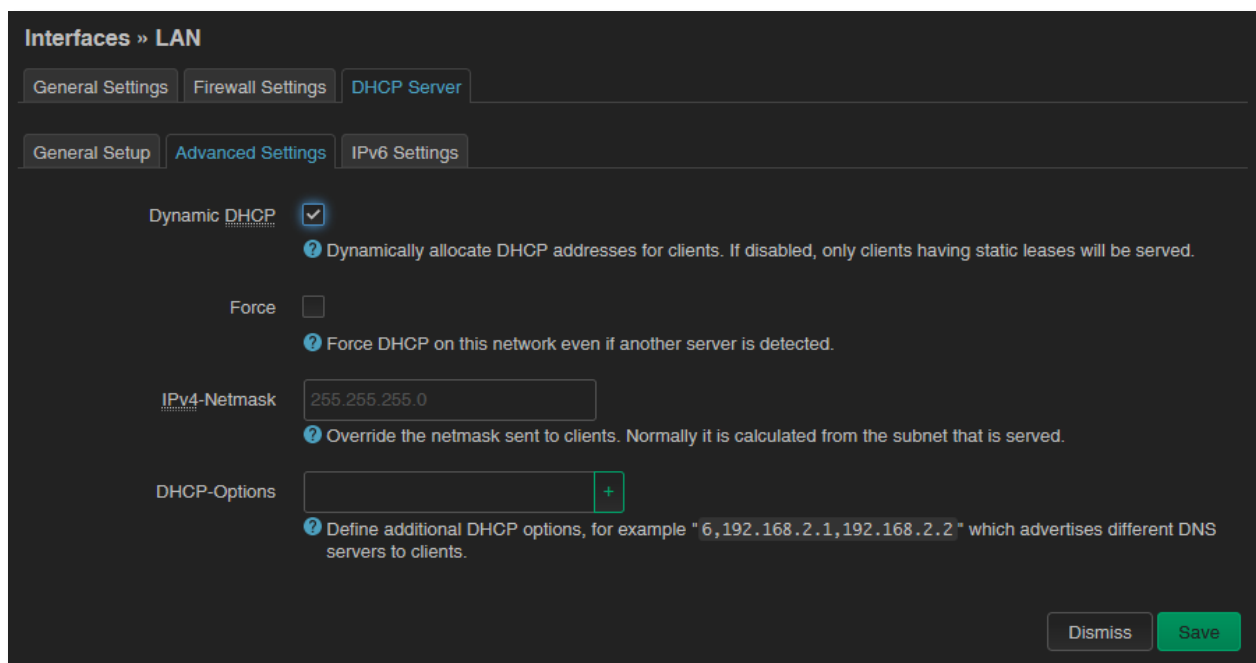
The **Start** field means what the starting address should be within the subnet used by the router (in our case 192.168.x...).

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



The screenshot shows the 'Interfaces » LAN' configuration page with the 'DHCP Server' tab selected. Under the 'General Setup' sub-tab, the 'Ignore interface' checkbox is checked. Below it are three input fields: 'Start' with the value '2', 'Limit' with the value '1', and 'Lease time' with the value '5m'. Each input field has a help icon and a descriptive tooltip. At the bottom right, there are 'Dismiss' and 'Save' buttons.

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



The screenshot shows the 'Interfaces » LAN' configuration page with the 'DHCP Server' tab selected and the 'Advanced Settings' sub-tab active. The 'Dynamic DHCP' checkbox is checked. Below it are three input fields: 'Force' (unchecked), 'IPv4-Netmask' with the value '255.255.255.0', and 'DHCP-Options' with a '+' button. Each input field has a help icon and a descriptive tooltip. At the bottom right, there are 'Dismiss' and 'Save' buttons.

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 router's DHCP service (with the renewal *lease time*).

The screenshot shows the 'DHCP and DNS' configuration page with the 'Static Leases' tab selected. The page includes a description of Dnsmasq, a navigation bar with tabs for 'General Settings', 'Resolv and Hosts Files', 'PXE/TFTP Settings', 'Advanced Settings', 'Static Leases', 'Hostnames', and 'IP Sets'. Below the navigation bar, there is explanatory text about static leases and an 'Add' button. A table with columns for 'Hostname', 'MAC address', 'IPv4 address', 'Lease time', 'DUID', and 'IPv6 suffix (hex)' is shown, containing the message 'This section contains no values yet'. Below the table is another 'Add' button. At the bottom, there is a section for 'Active DHCP Leases' with a table showing columns for 'Hostname', 'IPv4 address', 'MAC address', and 'Lease time remaining', containing the message 'There are no active leases'. At the bottom right, there are buttons for 'Save & Apply', 'Save', and 'Reset'.

Here you can **Add** 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 **Save** 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.

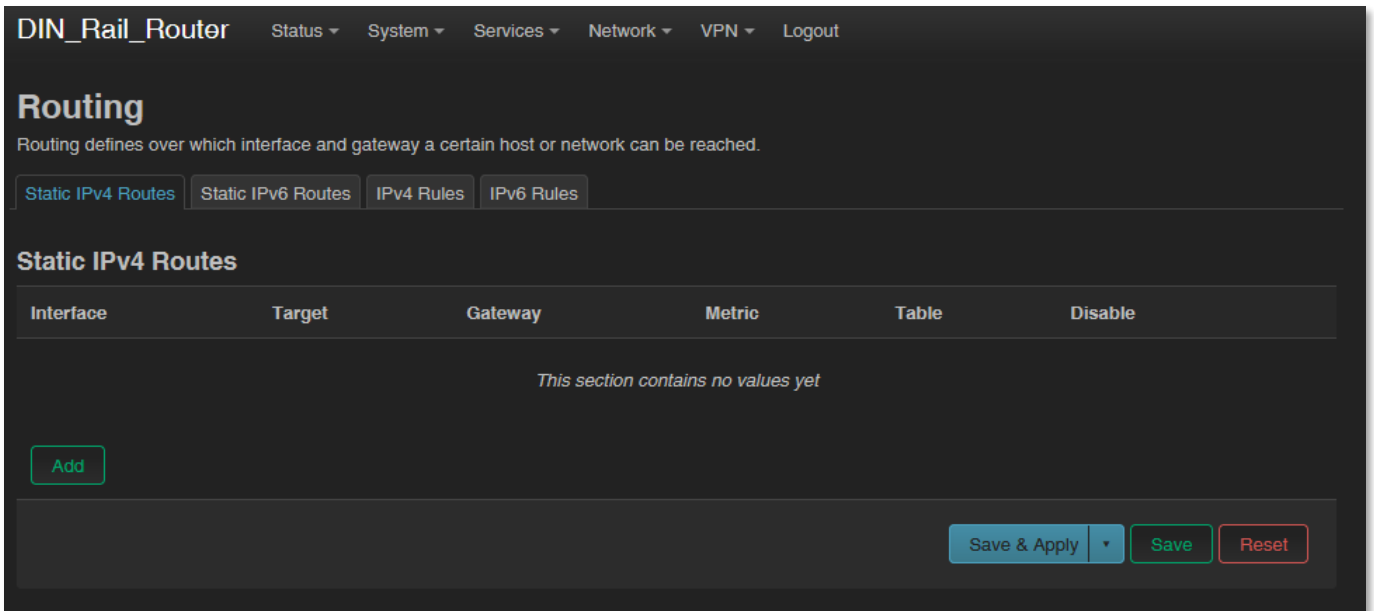
DNS query port
[?](#) Fixed source port for outbound DNS queries.

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.

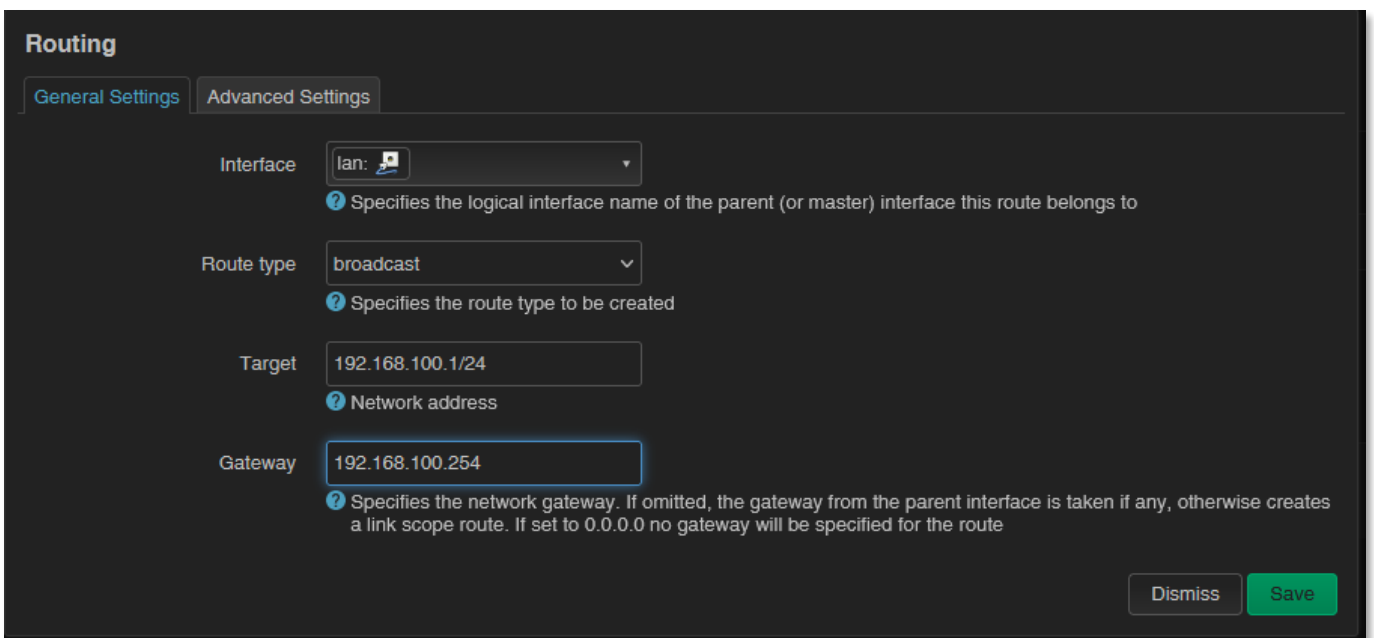
8.6 Defining the route rules

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.

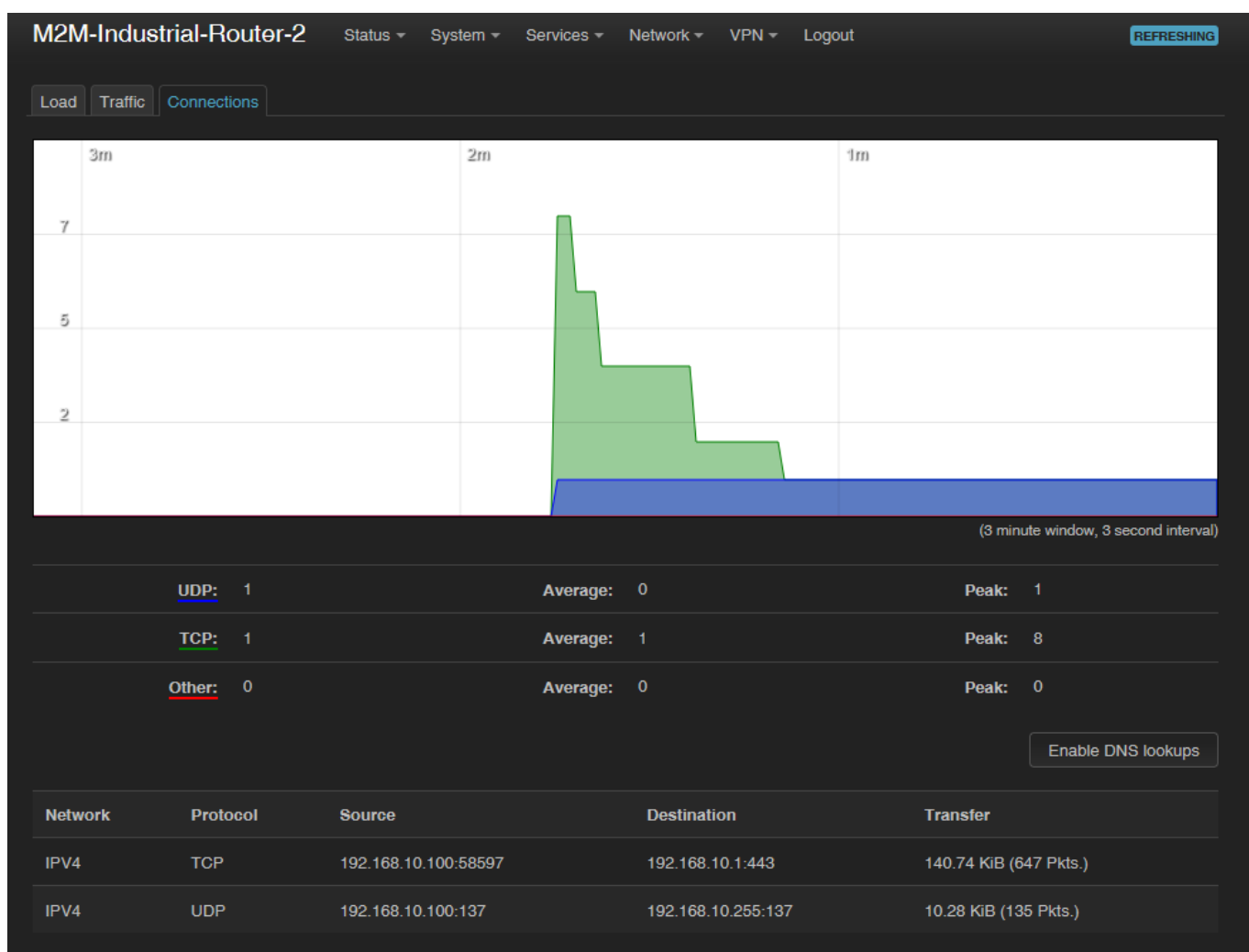
8.7 Firewall settings

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 router: connections, communication channels (port number, incoming IP) and to listen incoming and outgoing network activities!

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



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

In the **Status / Firewall** menu you can check the firewall statistic. The **INPUT** means the incoming, the **OUTPUT** the outgoing/transmitted and the **FORWARD** means the forwarded communication/traffic hereby. As you can see, there are several

communicating IP addresses on several ports to the router and the subnet. Another method for limitation can be the whole disabling with opening and enabling only necessary communication ports, IP-segments or allowing exact IP addresses.

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

DIN_Rail_Router

[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*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
No rules in this chain.									

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
No rules in this chain.									

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
No rules in this chain.									

Table: NAT

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
No rules in this chain.									

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
No rules in this chain.									

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
No rules in this chain.									

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

DIN_Rail_Router 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 router or

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

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 router against external network attacks or intrusions when just enabling the firewall feature.

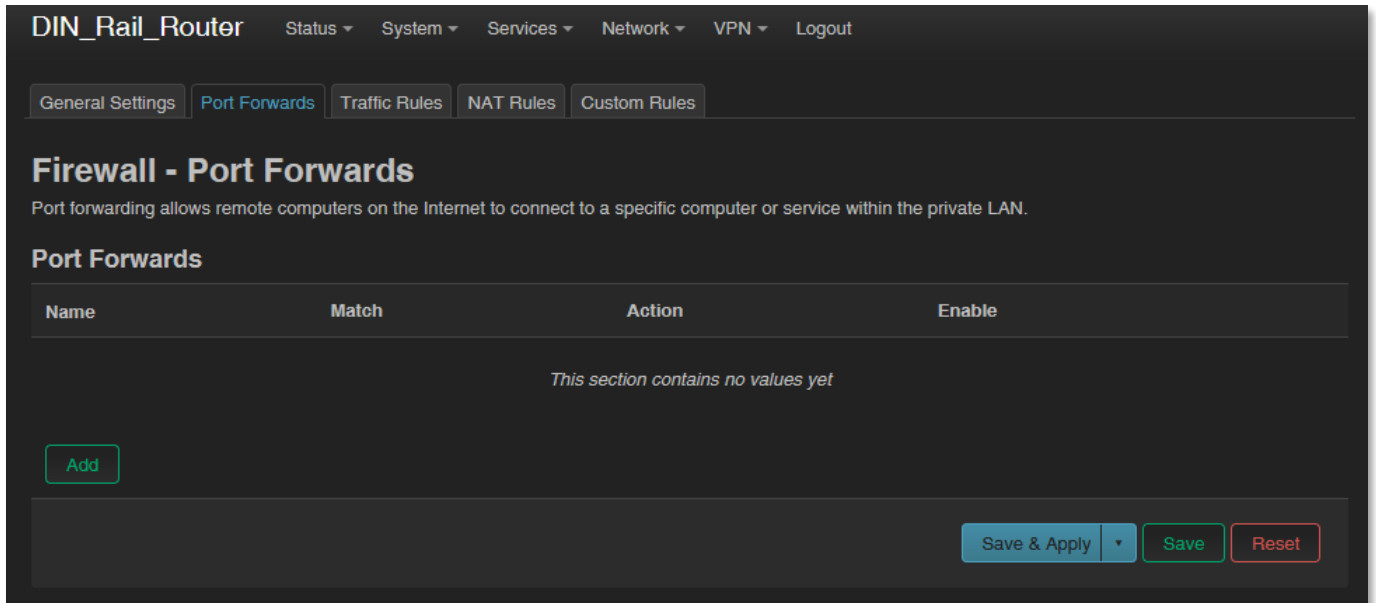
Further port-level filtering or interface traffic limits, or **Traffic Rules** settings are necessary to define! When you have modified the settings, save them by the **Save** button.

The screenshot shows the Mikrotik Router configuration interface for "DIN_Rail_Router". The navigation menu includes Status, System, Services, Network, VPN, and Logout. The "Traffic Rules" tab is selected, showing a list of firewall rules. Each rule has a Name, Match criteria, Action, and Enable status, along with Edit and Delete buttons.

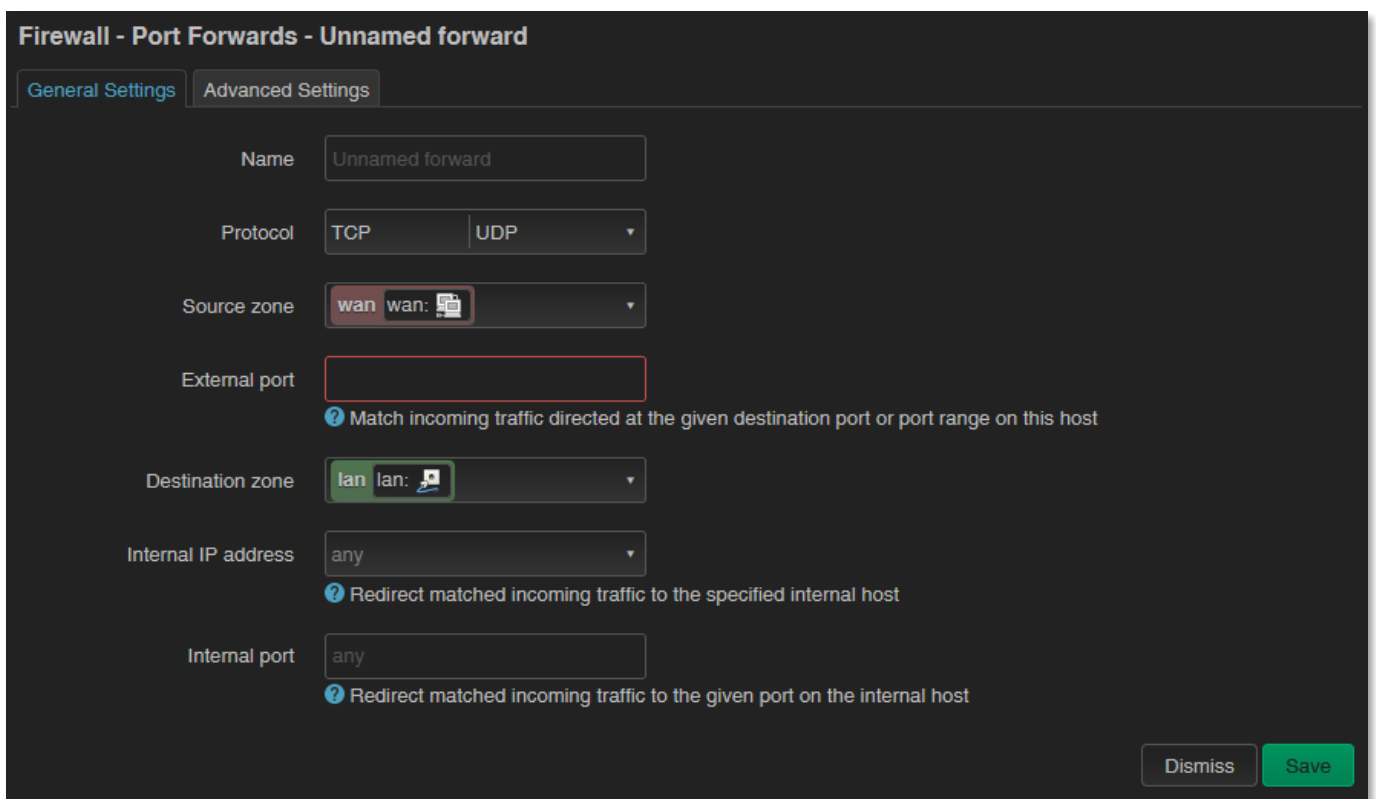
Name	Match	Action	Enable	
Allow-DHCP-Renew	Incoming IPv4, protocol UDP From wan To this device, port 68	Accept input	<input checked="" type="checkbox"/>	≡ Edit Delete
Allow-Ping	Incoming IPv4, protocol ICMP From wan To this device	Accept input	<input checked="" type="checkbox"/>	≡ Edit Delete
Allow-IGMP	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.

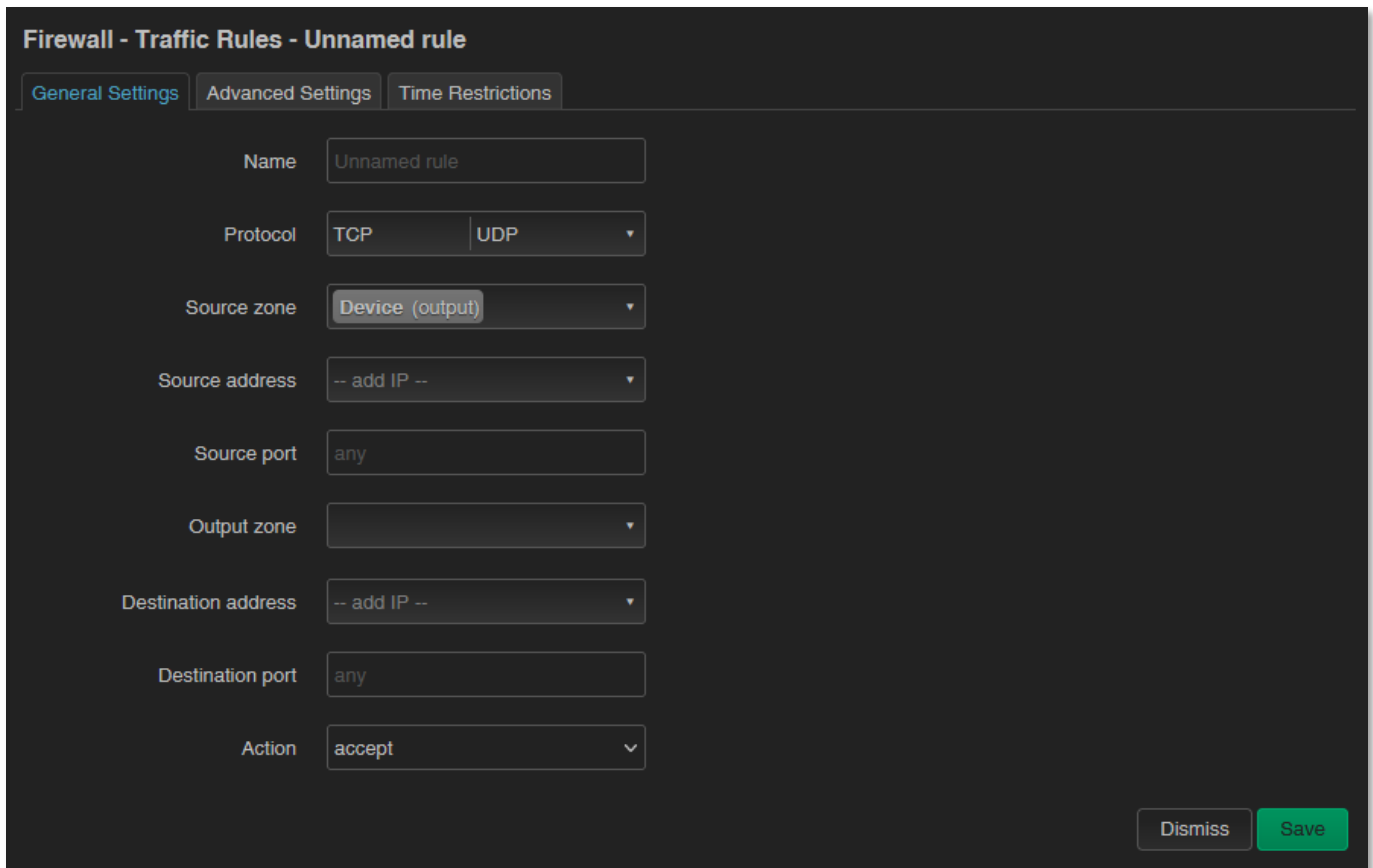


When you have modified the settings, save them by the **Save** button.

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.



Firewall - Traffic Rules - Unnamed rule

General Settings | Advanced Settings | Time Restrictions

Name: Unnamed rule

Protocol: TCP | UDP

Source zone: Device (output)

Source address: -- add IP --

Source port: any

Output zone:

Destination address: -- add IP --

Destination port: any

Action: accept

Dismiss 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 router 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 22, web: port 80, etc).

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

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 in the OpenWrt web interface. The page is titled 'DIN_Rail_Router' and has a 'REFRESHING' indicator in the top right. The main heading is 'Dynamic DNS', with sub-sections for 'Information' and 'Global Settings'. The 'Information' section displays the following details:

- Dynamic DNS Version:** 2.8.2-29
- State:** DDNS Autostart disabled. A note indicates: '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'.

There are two informational notes with arrows pointing to the right:

- Binding to a specific network not supported**: 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**: 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.

The 'Services' section contains a table with the following data:

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

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

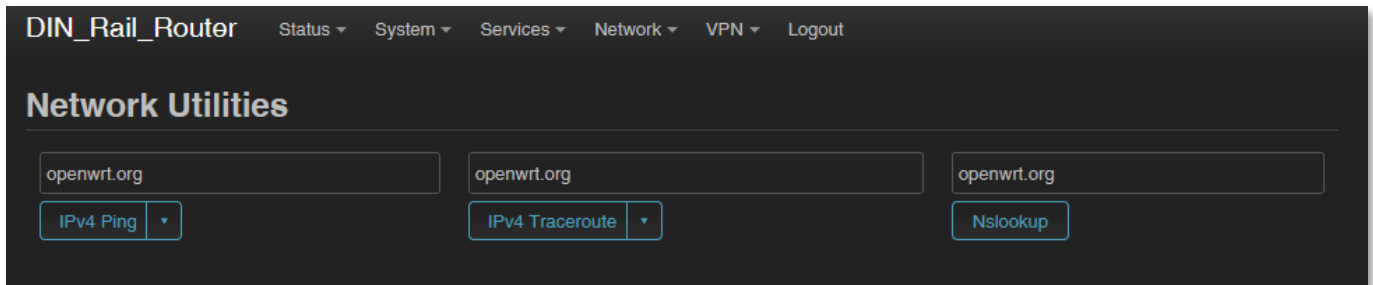
New DDNS entry can be **Add** by the button or the current can be changed by the **Edit** button – even for IPv4 or IPv6.

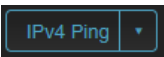

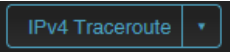
Save the settings by the **Save** button.

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  button), is there a naming service provided, is there a response between two points (by  button), furthermore the path of the communication (by  button).

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

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

Important!

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

9.2 Network Time Service (NTP)

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

The screenshot shows the 'System Properties' configuration page for a 'DIN_Rail_Router'. The 'Time Synchronization' tab is active. The page includes several settings: 'Enable NTP client' (checked), 'Provide NTP server' (checked), 'Bind NTP server' (set to 'wan'), 'Use DHCP advertised servers' (checked), and 'NTP server candidates' (a list containing '192.168.1.1' and 'de.pool.ntp.org'). At the bottom right, there are buttons for 'Save & Apply', 'Save', and 'Reset'. A 'REFRESHING' indicator is visible in the top right corner.

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 TFTP 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**. If you've modified, save it by the **Save** button.

DIN_Rail_Router 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 router by sending the data to IP addresses by entering your account and password information. if you need more help, see the OpenSSH Linux command line settings.

9.4 LED configuration

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

DIN_Rail_Router Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

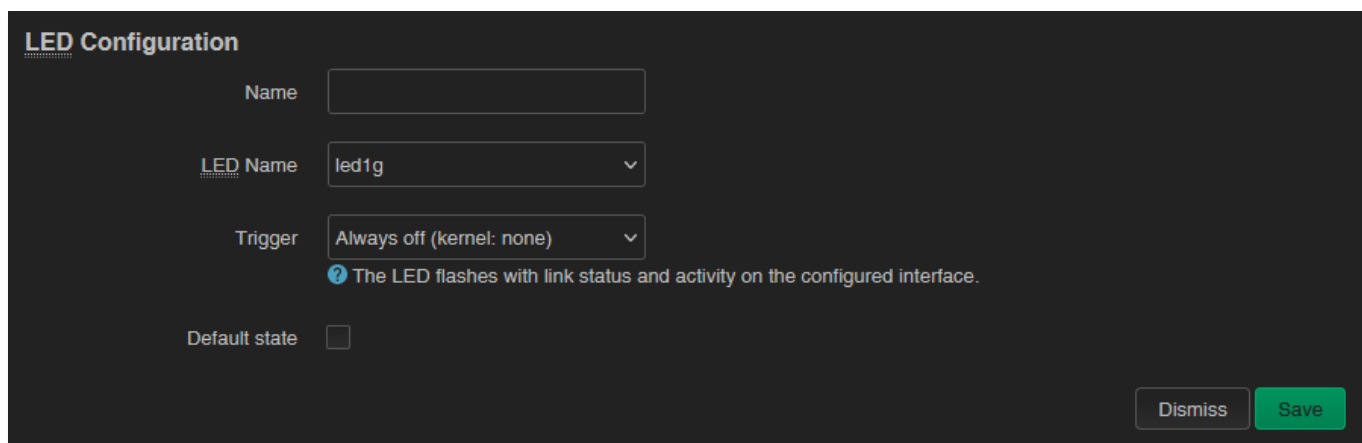
LED Configuration

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

Name	LED Name	Trigger	
wan	led_g3	netdev	<input type="button" value="≡"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
lan	led_g5	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:

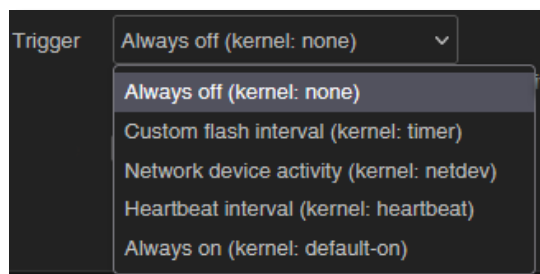
- Number can be: **1** (LED1), **2** (LED2) or **3** (LED3)
- Lighting color can be: **r** (red) or **g** (green)

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 menu is open, showing several 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)'. The top option is currently selected.

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 router can also be accessed over an SSH connection, with a terminal program (e.g. the software called *putty*), at the IP address of the device - e.g. **192.168.127.1:22** (port nr. 22 on the **Ethernet** port).

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

SSH login:

Login as: root **Password: wmrpwd**

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

The router'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

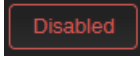
The UCI® (Unified Configuration Interface) is an OpenWrt® API / utility that allows centralized configuration and further management of the OpenWrt® system.

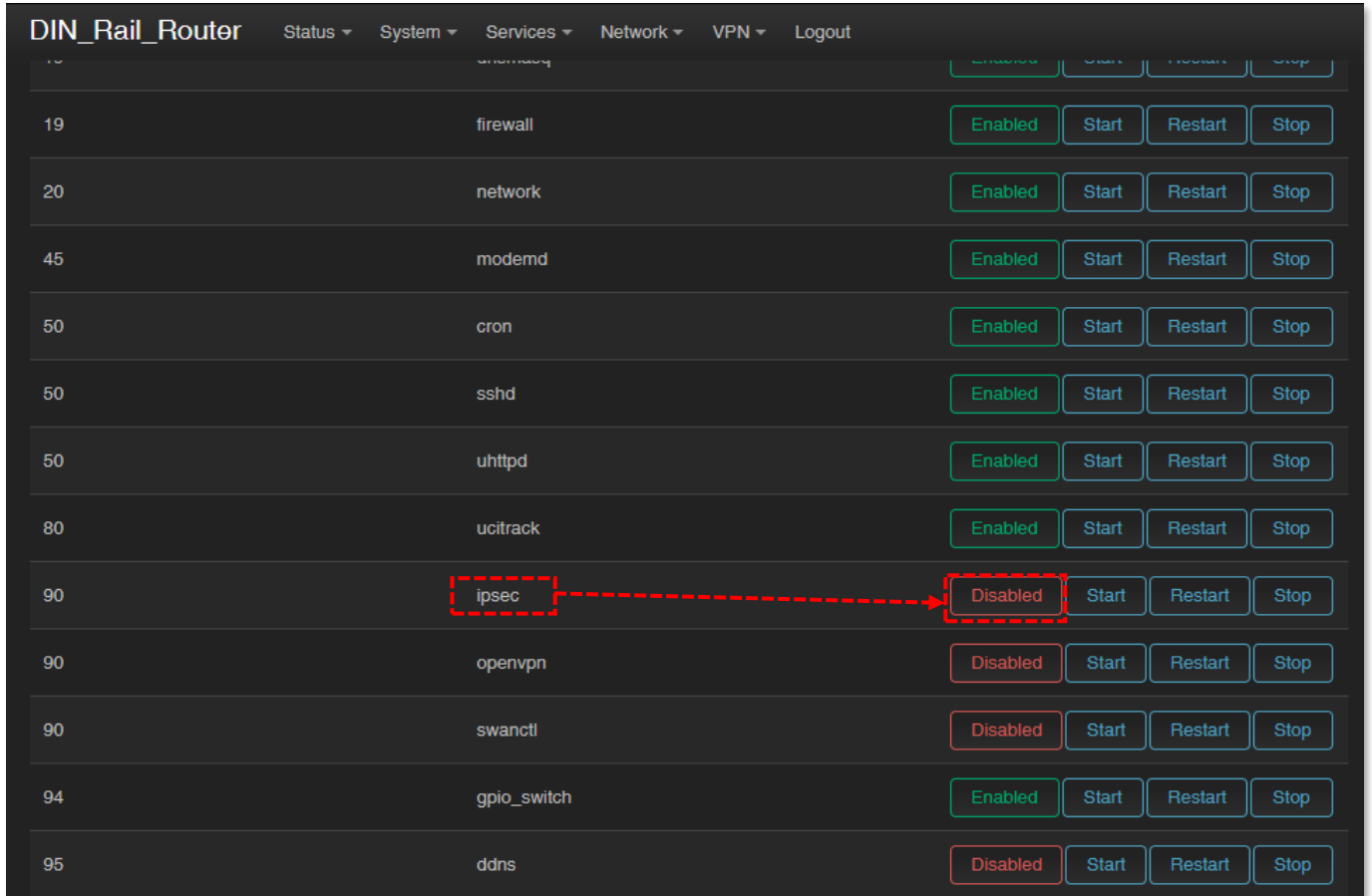
To review the useable UCI commands and options that can be used, we recommend to read the UCI guide, which can be downloaded from our website:

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

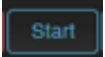
9.7 IPSEC settings

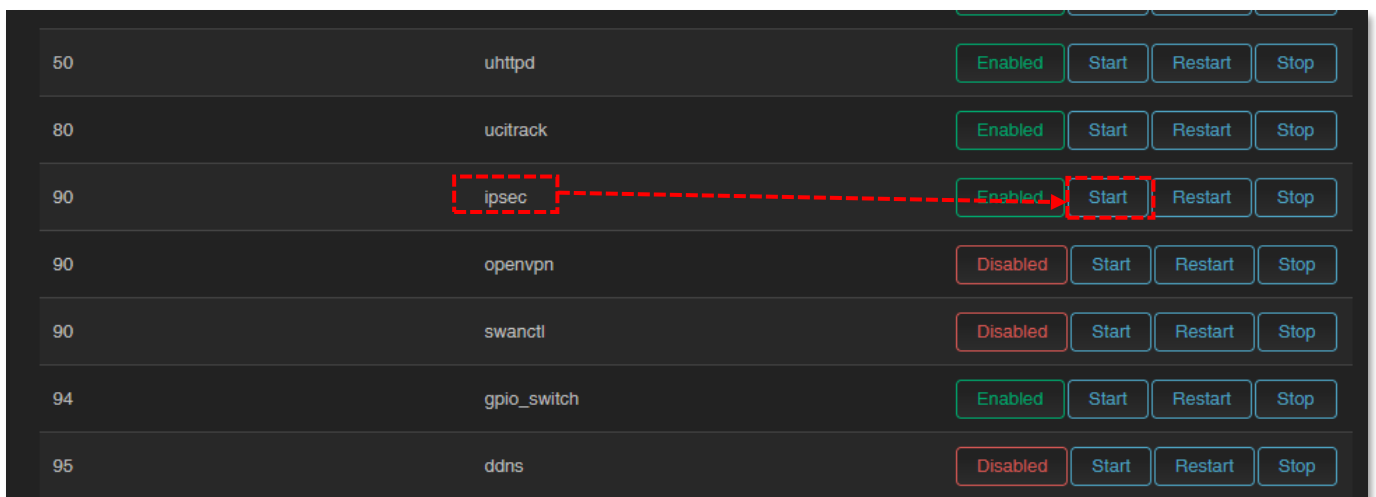
Open the **Systems / Startup** menu to enable *strongSwan* IPsec feature.

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



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

Then push to the  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>

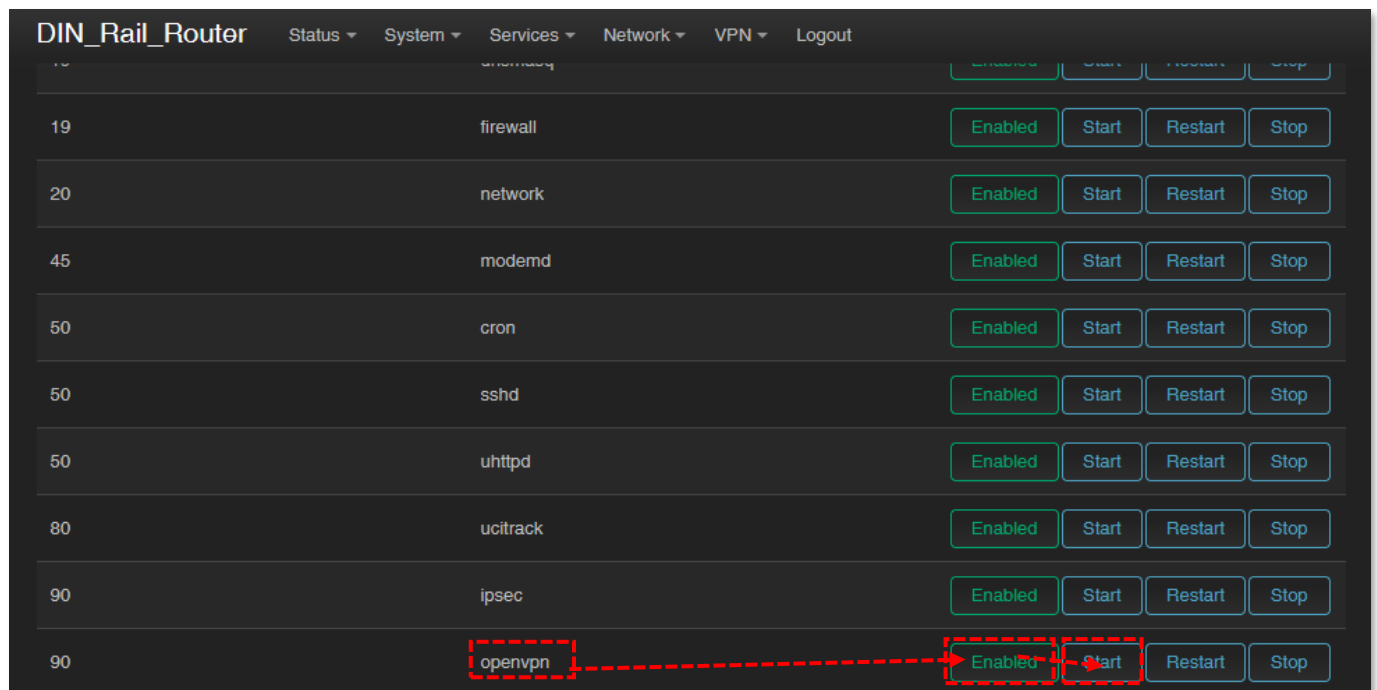
9.8 VPN client (OpenVPN) configuration

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.

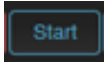
Then wait until the service list will be refreshed and the „**openvpn**” will be listed as **Enabled** service.


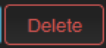
Then push to the **Start** button of the line of the „**openvpn**” service to start the feature.



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

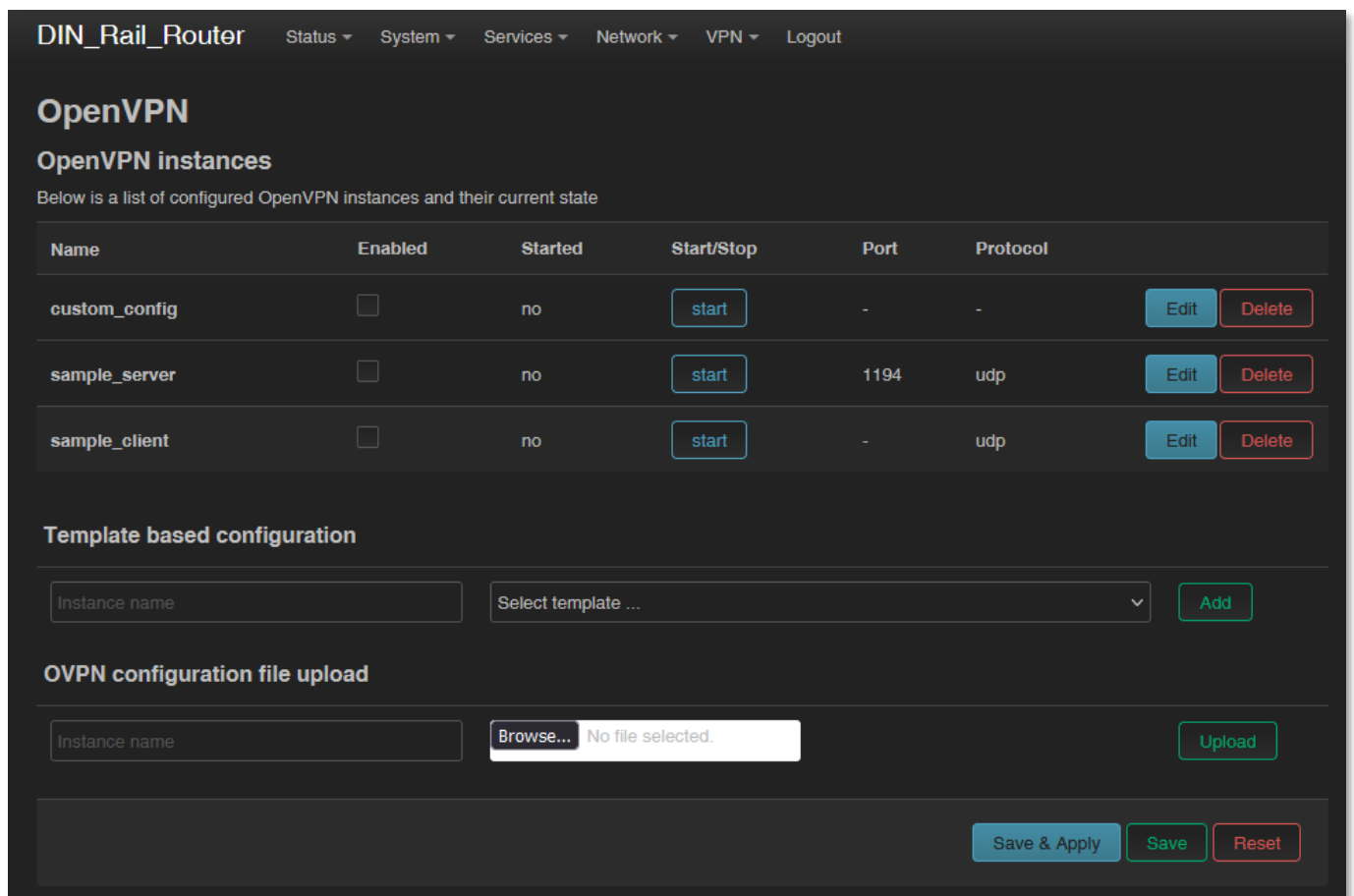
You will find three pre-configured VPN connections that you can enable or change your settings.

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 router 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.



The screenshot shows the OpenVPN configuration page on a router. At the top, there is a navigation bar with 'DIN_Rail_Router' and several menu items: Status, System, Services, Network, VPN, and Logout. The main heading is 'OpenVPN', followed by 'OpenVPN instances'. Below this, a text line states: 'Below is a list of configured OpenVPN instances and their current state'. A table lists three instances: 'custom_config', 'sample_server', and 'sample_client'. Each row has columns for Name, Enabled (checkbox), Started (text), Start/Stop (button), Port, Protocol, and Edit/Delete buttons. Below the table is a 'Template based configuration' section with an 'Instance name' input, a 'Select template ...' dropdown, and an 'Add' button. The 'OVPN configuration file upload' section has an 'Instance name' input, a 'Browse...' button, a file selection area showing 'No file selected.', and an 'Upload' button. At the bottom right, there are 'Save & Apply', 'Save', and 'Reset' buttons.

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'" with a link to "Switch to advanced configuration »".
- Configuration Fields:**
 - 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". To its right is a red "x" icon. Below the field is a green "+" icon and a help icon with 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 side, there are three buttons: "Back to Overview", "Save & Apply", "Save", and "Reset".

- **cert**: you can add the device certification for the router'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'
```

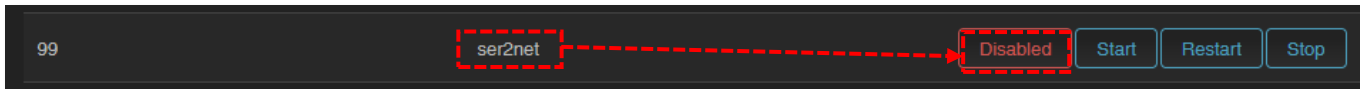
```
#uci commit
```

9.9 RS485 / Modbus settings (Ser2net)

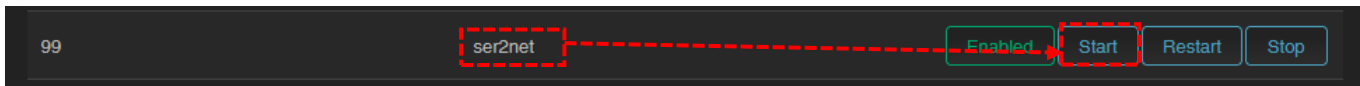
RS485 / Modbus feature can be used for connecting industrial devices, utility meters to the data concentrator.

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

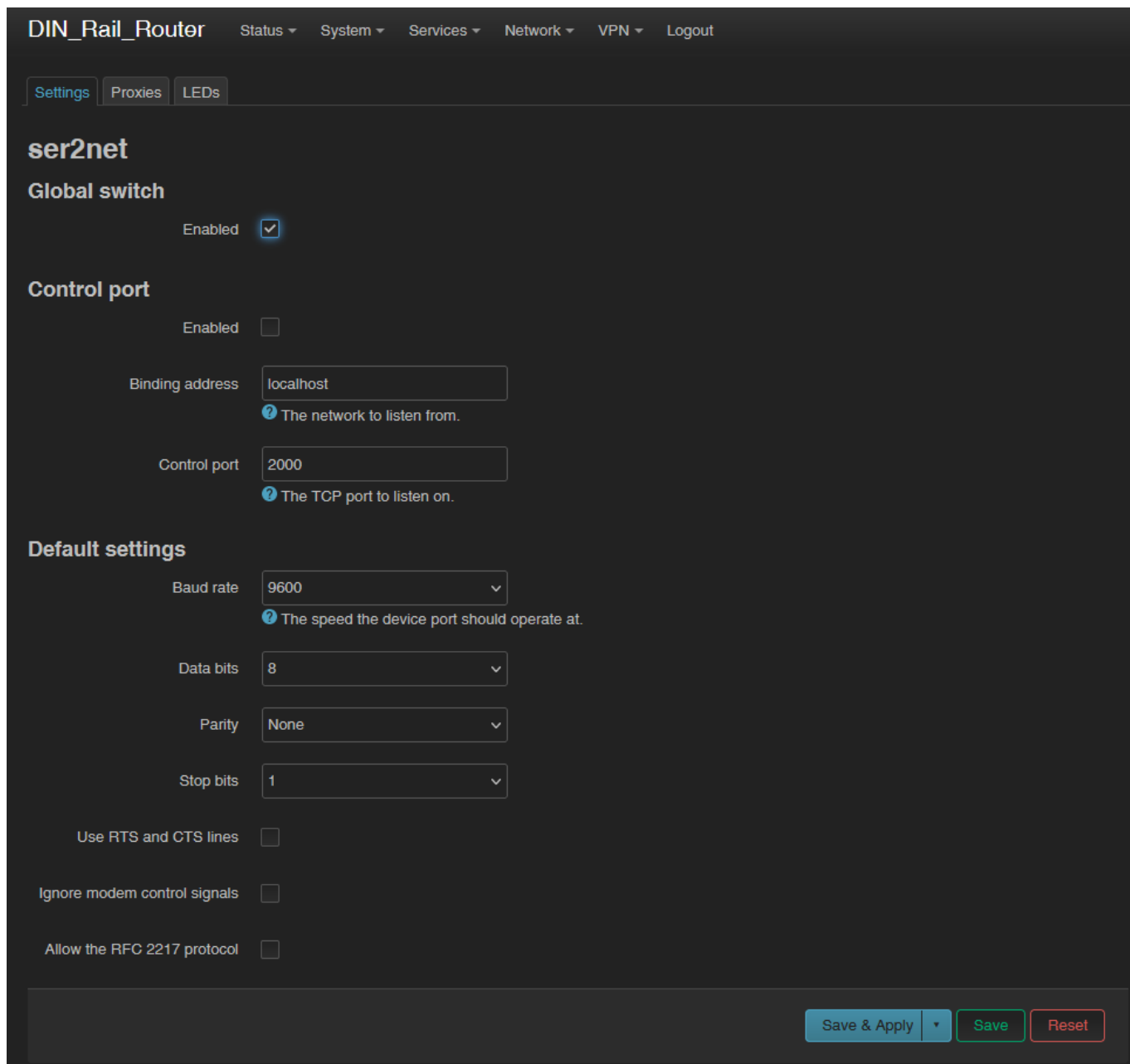


Enabled service.



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. We offer to use the **raw** option by default:

- **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**

DIN_Rail_Router 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

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 router 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*.

***Important!** This feature is currently inactive.

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

Important!

To take effect of the changes in the service settings, you should stop (with **STOP** button) and then start (with **START** button) the **ser2net** service from the **Systems / Startup** menu, as listed at the beginning of this chapter.

Warning!

If you do not use Modbus data transmission, we recommend stopping the **gedacc** and **modbusGW** services in the **Systems / Startup** menu.

9.10 Data collection settings (RS485 / Modbus)

Attention! This menu and feature can be ordered optionally. Ask our Sales!

First of all, you should **enable** and **START** the **gedacc** and **modbusGW** services in the **Systems / Startup** menu.

In the **Settings** tab, you can configure the data acquisition settings for collecting data of utility meters, PLCs. **Enable** the 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**.

DIN_Rail_Router 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).

remote

Settings of the target server: Host, protocol, timing

Enable

[?](#) Enable this service

Name

Description

Protocol

[?](#) Protocol for upload data

Server Address

[?](#) Name or IP address of server.

Server port

[?](#) Port number of server.

Username

[?](#) Username for server connection

Password *

[?](#) Password for server connection

Uploading periodicity [min]

[?](#) Uploading periodicity to gead end server in minutes.

MQTT topic

[?](#) MQTT topic name

MQTT context account name

[?](#) MQTT context account name

The **Username**, **ClientID**, **QoS** fields are necessary to fill only in case of using the MQTT data transmitting settings.

Important! Note, that all data will be collected and stored locally on the router.

Fill the **Upload periodicity** interval (in minutes) for defining the data transmission cycle to the HES.

The screenshot shows the configuration page for the MQTT context on a DIN_Rail_Router. The page has a dark theme and a navigation bar at the top with links for Status, System, Services, Network, VPN, and Logout. The main content area contains several configuration fields, each with a label, a text input or dropdown, and a help icon (a question mark in a circle). The fields are: MQTT context account name (text input: 'devices'), MQTT clientid (text input: 'clientid'), MQTT QoS (dropdown: '0 at most once'), CA certificate (text input: '/tmp/missing.crt'), TLS certificate (text input: '/tmp/missing.crt'), TSL key (text input: '/tmp/missing.crt'), Collector Template (text input: '"CollectorName": "%COL_NAME%'), Device Template (text input: '"Address": "%PLC_ADDR%", "N'), Register Template (text input: '"%REG_NAME%" "%REG_V,'), and Data format (develop) (dropdown: 'Template'). At the bottom right, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red).

DIN_Rail_Router Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

MQTT context account name devices

MQTT context account name

MQTT clientid clientid

MQTT clientid name

MQTT QoS 0 at most once ▾

MQTT QoS 0/1/2

CA certificate /tmp/missing.crt

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

TLS certificate /tmp/missing.crt

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

TSL key /tmp/missing.crt

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

Collector Template "CollectorName": "%COL_NAME%

Collector (DCU) related information

Device Template "Address": "%PLC_ADDR%", "N

Measuring device related part

Register Template "%REG_NAME%" "%REG_V,

Measured date related part

Data format (develop) Template ▾

Output formats 0/1/2

Save & Apply Save Reset

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

Use complete paths (directory names) for file path.

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

On the **Meter List** tab the meter properties of the incoming transparent data transmission can be also added at **RS485 – Meter Devices** part. Here you can **Add** devices for each part (**RS485 – Meter devices** and **TCP - Meter devices: Modbus PLC device** or **Data registers: register data**).

DIN_Rail_Router 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	
<input type="text" value="New Modbus PLC address"/>	<input type="text" value="New Name of PLC"/>	<input type="text" value="New Read periodicity seconds"/>	<input type="text" value="9600"/>	<input type="text" value="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	
<input type="text" value="New Modbus PLC address"/>	<input type="text" value="New Name of PLC"/>	<input type="text" value="New Read periodicity [sec]"/>	<input type="text" value="IP Address of PLC"/>	<input type="text" value="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	
<input type="text" value="New Register Address"/>	<input type="text" value="Name of PLC"/>	<input type="text" value="1"/>	<input type="text" value="UNSIGNED"/>	<input type="text" value="New Name of register"/>	Add

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

At the **RS485 - Meter Devices** part you can add **Meter devices** with their following parameter values:

- **Name** – Name of the meter device
- **Modbus Address** – address of the meter
- **Description**
- **Speed** – selection: **2400 / 4800 / 9600 / 19200 / 38400 / 115200** baud
- **Data bits** – value can be **7** or **8**
- **Stop bits** – value can be **1** or **2**
- **Parity** – value can be **NONE**, **ODD** or **EVEN**
- **Data read periodicity (sec)** – by default it is 60 seconds

Fill the required fields consequently regarding the meter data collection requirements.

The screenshot shows a web interface for configuring a meter device. The page title is "Data Collection - Meter Device for RS485 - TemperatureSensor". Below the title, there is a subtitle: "This page allows you to change properties of the meter device entry." The form contains the following fields:

- Name:** TemperatureSensor (with a help icon and text "Name of PLC")
- Modbus Address:** 10 (with a help icon and text "PLC Modbus Address")
- Description:** Temperature Sensor modbus (with a help icon and text "Description of PLC device (optional)")
- Speed:** 9600 (dropdown menu)
- Data bits:** 8 (dropdown menu)
- Stop bits:** 1 (dropdown menu)
- Parity:** NONE (dropdown menu)
- Data read periodicity [sec]:** 60 (with a help icon and text "Data read out periodicity from PLC in seconds")

At the bottom of the form, there are three buttons: "Back to Overview", "Save & Apply", and "Save" (highlighted in green), and a "Reset" button.

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

At the **TCP Meter Devices** part you can add **Modbus or PLC devices** with their following parameter values:

- **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 web interface of a DIN_Rail_Router. The top navigation bar includes 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout'. Below the navigation, there are tabs for 'Settings', 'DirectAccess', and 'MeterList'. The main heading is 'Data Collection - Meter Device for ModbusTCP - diagslave'. A sub-heading states: '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 three buttons: 'Back to Overview', 'Save & Apply', and 'Reset'.

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

At the **Data Registers** part you can add new **Register data** for the list.

Fill the required fields consequently regarding the data collection requirements.

Save & Apply settings fo data register entry.

Note, that you can also choose MQTT protocol to send the collected meter data to the data center.

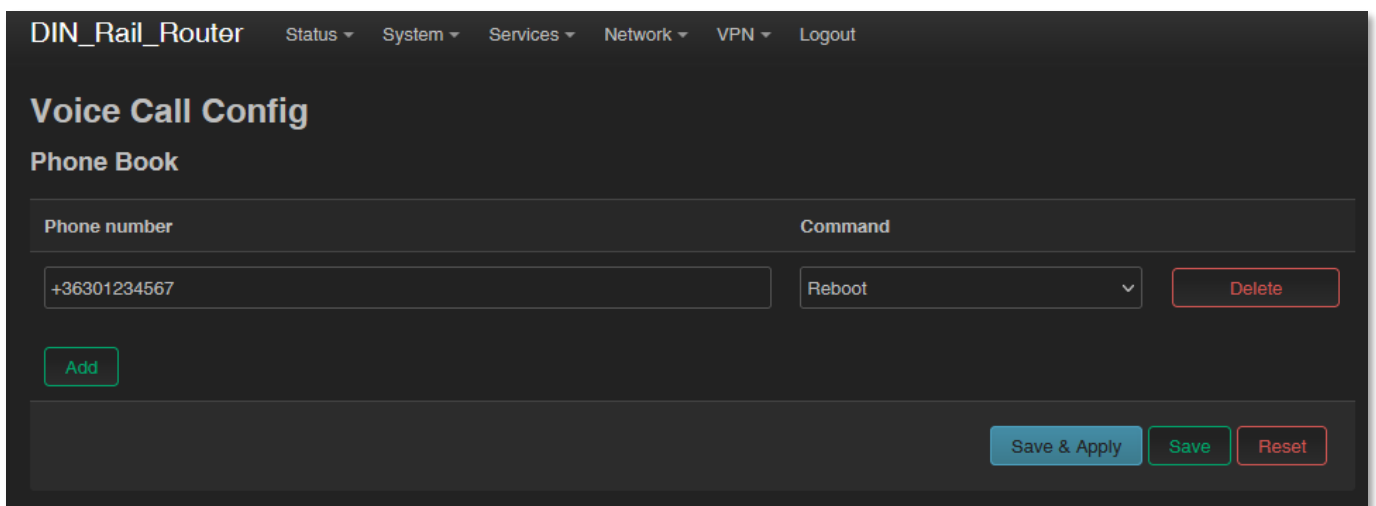
Important!

To take effect of the changes in the service settings, you shoud stop (with **STOP** button) and then start (with **START** button) the **gedacc** and **modbusGW** services from the **Systems / Startup** menu, as listed at the beginning of this chapter.

9.11 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. At the top, there is a navigation bar with 'DIN_Rail_Router' and several menu items: 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout'. Below the navigation bar, the title 'Voice Call Config' is displayed, followed by the sub-section 'Phone Book'. A table is shown with two columns: 'Phone number' and 'Command'. The first row contains the phone number '+36301234567' and the command 'Reboot'. To the right of the 'Reboot' command is a 'Delete' button. Below the table, there is an 'Add' button. At the bottom right of the interface, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.


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.

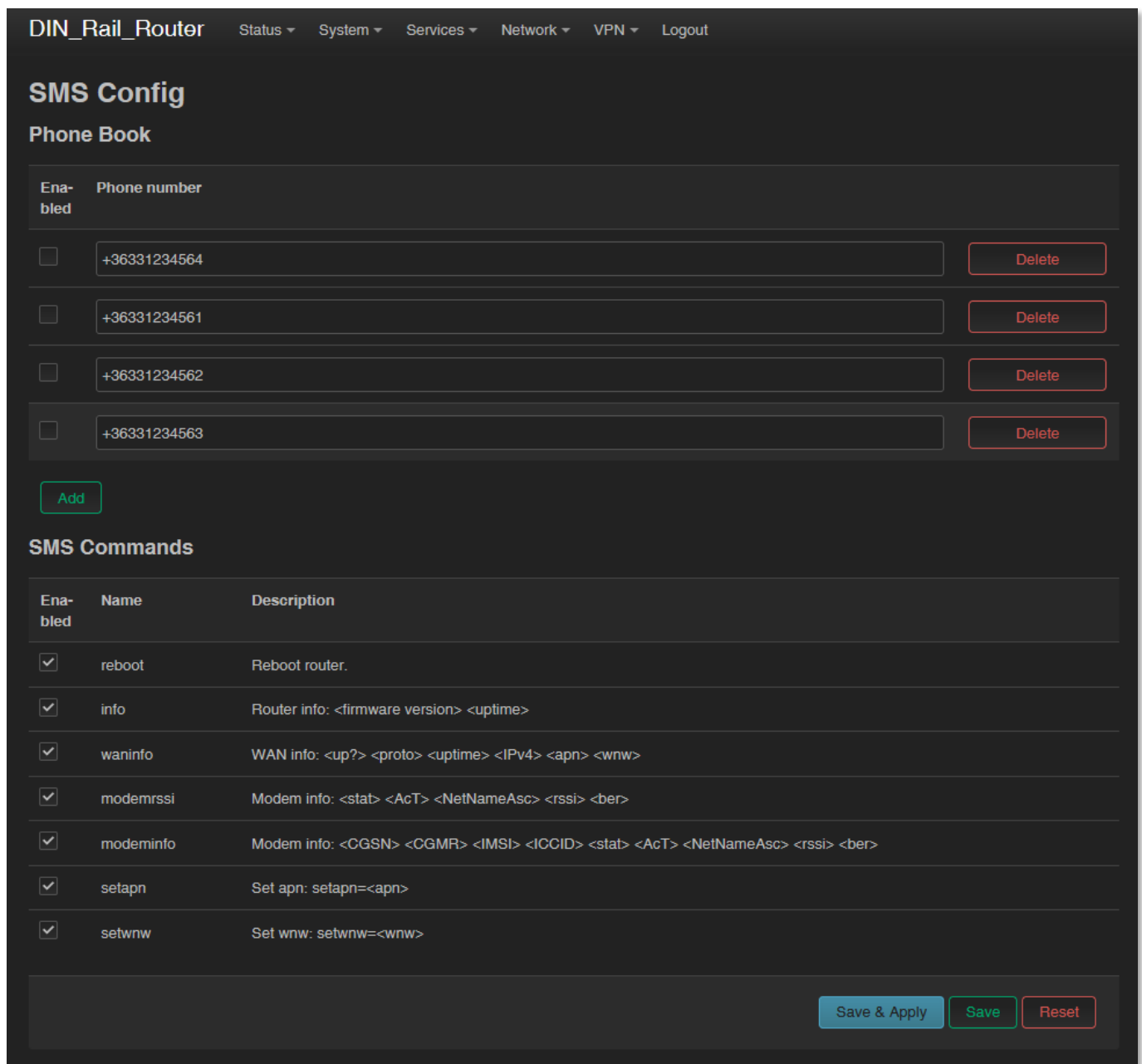
9.12 Run commands remotely (SMS config settings)

You can execute commands on the router 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  phone number(s).

Then you have to check the **Enabled** option for the selected phone number(s).



DIN_Rail_Router Status ▾ System ▾ Services ▾ Network ▾ VPN ▾ Logout

SMS Config

Phone Book

Enabled	Phone number	
<input type="checkbox"/>	+36331234564	Delete
<input type="checkbox"/>	+36331234561	Delete
<input type="checkbox"/>	+36331234562	Delete
<input type="checkbox"/>	+36331234563	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 router runs the preset command (s) assigned to the phone number: e.g. **Reboot**

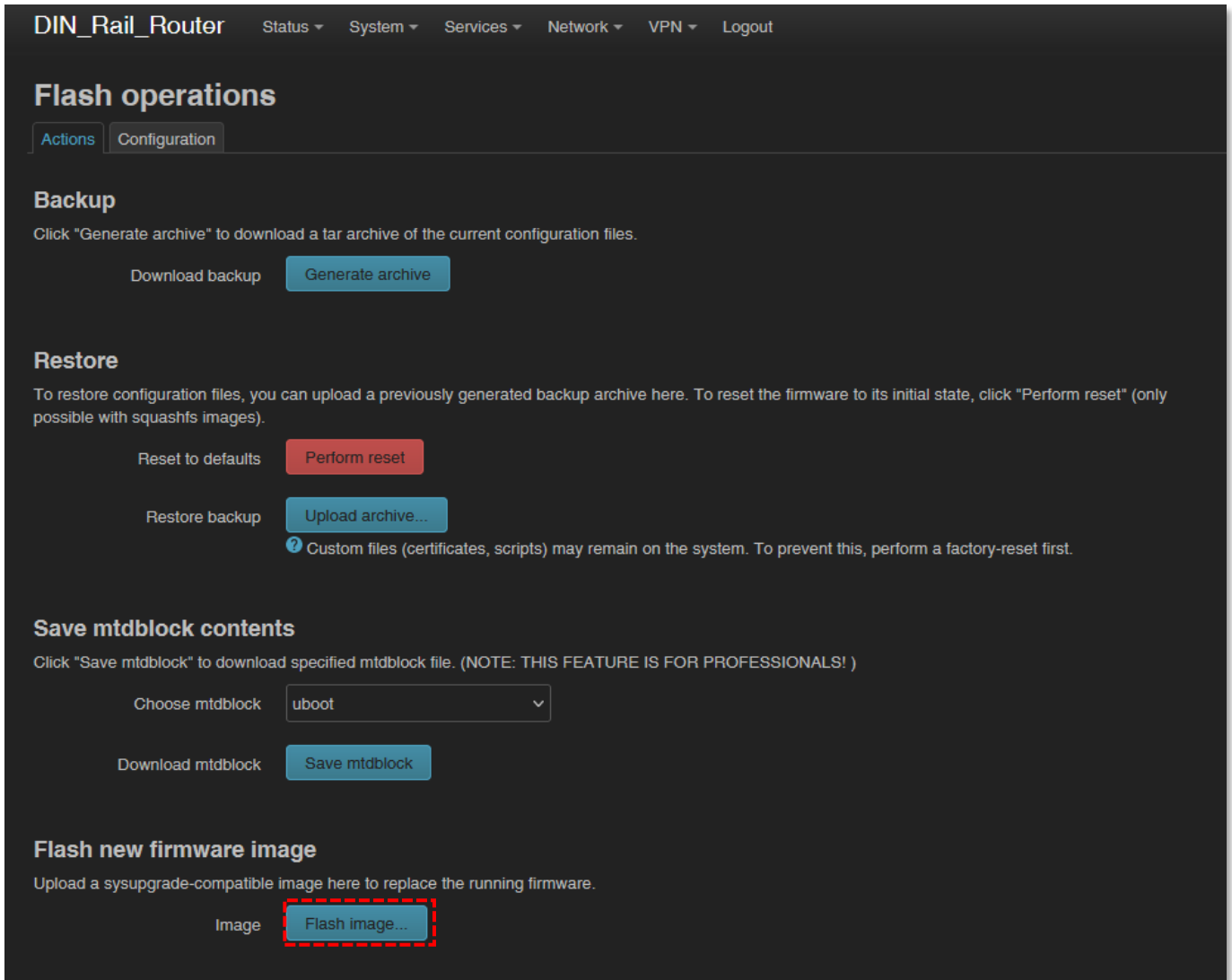
For other commands, the router returns the information in a reply SMS message (e.g. when sending the **"info"** command in SMS, the device sends the firmware version number and the elapsed time since the last boot info to the phone where the SMS has been sent).

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

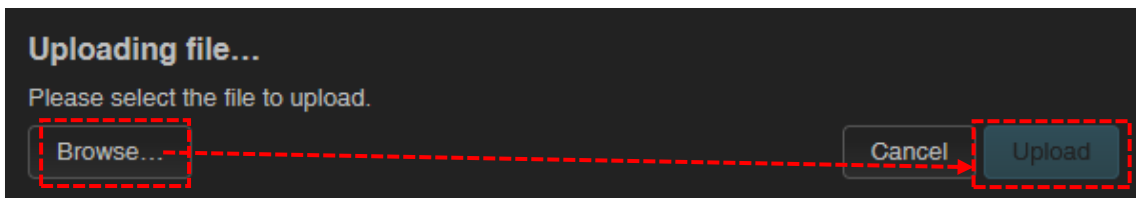
Chapter 10. Software refresh, maintenance

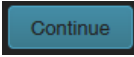
10.1 Firmware refresh

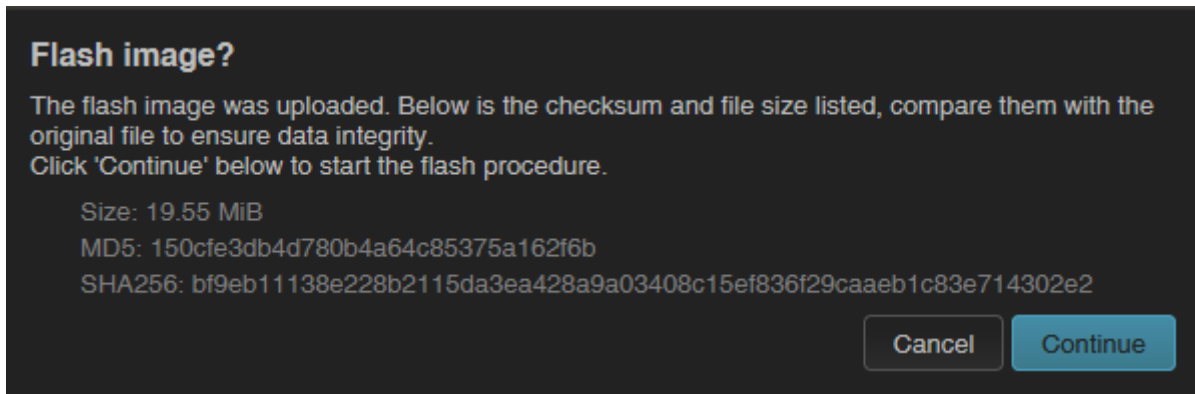
1. Open the **System** menu, **Backup / Flash firmware** item.
2. At **Flash new firmware image** part, push to the  button.



3.  the **fwos-....** compressed firmware file and push to the  button.



- Then another window is loaded, where the checked file will be uploaded and verified for approx. in half a minute.
- A new window will appear where the file will be checked. When it is okay, the system refreshment is possible by the  button.



- Then **Flashing...** message will appear on the screen. The firmware update will be started. Ca. 5-10 seconds later the **ERROR** LED will be lighting by **red** (during the firmware update process). At this time the **CELLULAR** LED will be also flashing by **green**. This flashing is signing the progress of the current firmware installation.



- Later, the **CELLULAR** LED will be changed to continuous **green** lighting, while the **DIN** LED will be flashing by **green**.



- Later, the **DIN** LED will be changed to continuous **green** lighting, while the **RS232** LED will be flashing by **green**.



- When the installation has been finished, the **ERROR** LED will be changed blank, while any other LEDs will be lighting by **green** for 1 seconds.



10. When all LEDs will be blank, the system will rebooting with the newly installed system firmware.



11. Soon the *OpenWrt*[®] system will be loaded and started as it was described before. When **POWER** LED will lighting again by **green** and **ETHERNET** LED or **CELLULAR** LED may sign some activity, you can login to the OpenWrt interface of the router.

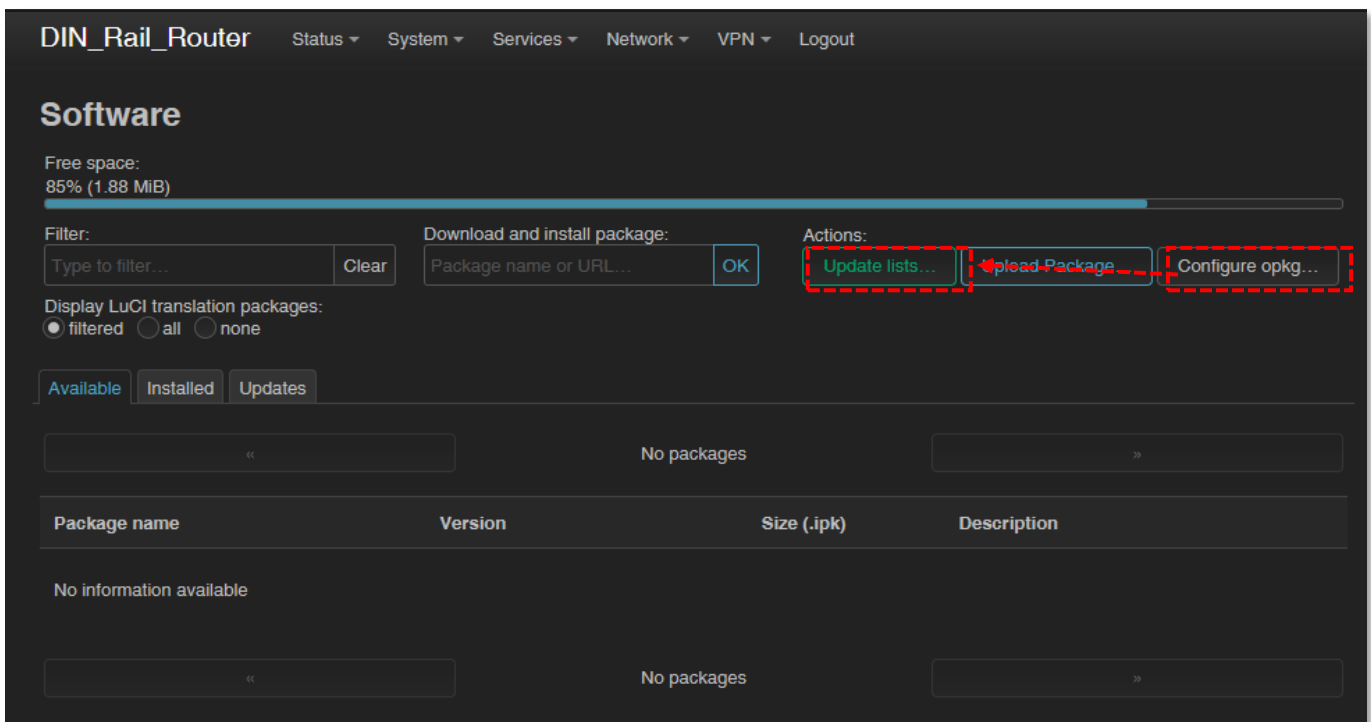


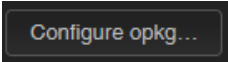
Important! The firmware update window in the browser will not close and automatically and it does not detect the availability of the OpenWrt page. Refresh the browser window and Login to the web user interface with credentials.

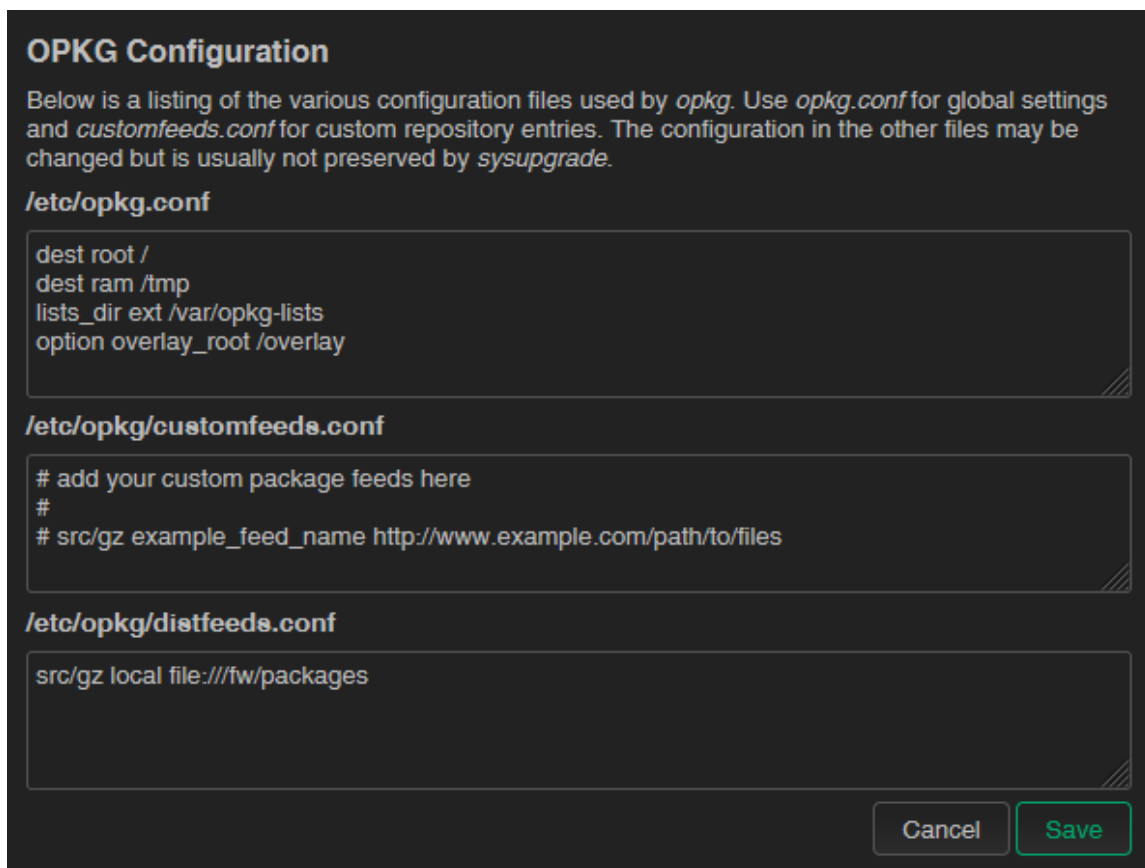
12. Check the updated software version at **Status / Overview** menu.


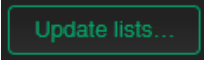
10.2 Installing applications

Open the **System / Software** menu.

A screenshot of the OpenWrt LuCI 'Software' page. The page title is 'DIN_Rail_Router' and the breadcrumb is 'System / Software'. It shows a progress bar for free space at 85% (1.88 MiB). There are input fields for filtering and installing packages, and a set of action buttons: 'Update lists...', 'Upload Package...', and 'Configure opkg...'. The 'Upload Package...' button is highlighted with a red dashed box. Below the buttons, there are two empty table containers, both showing 'No packages'.

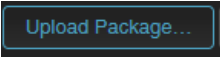
First you have to push the  button and setup the software distribution configuration in the popup windows, where you have to define the path of the installation packages are stored.



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

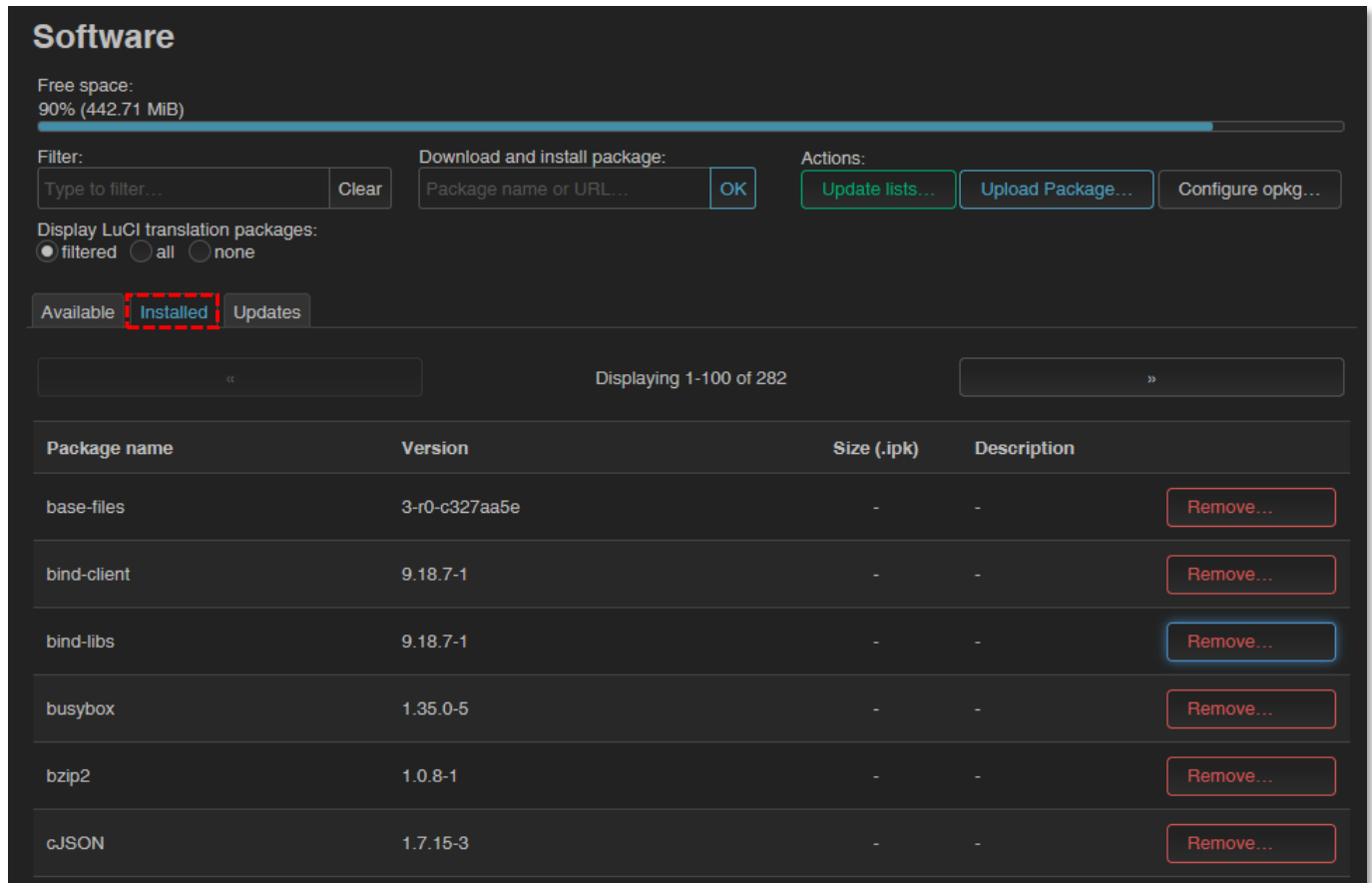
Important!

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 router then push to the  button.

You can  unnecessary packages, if you want.

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)'. Below this, there are sections for 'Filter:', 'Download and install package:', and 'Actions:'. The 'Filter:' section has a text input field and a 'Clear' button. The 'Download and install package:' section has a text input field and an 'OK' button. The 'Actions:' section has three buttons: 'Update lists...', 'Upload Package...', and 'Configure opkg...'. Below these sections, there are radio buttons for 'Display LuCI translation packages:' with options 'filtered', 'all', and 'none'. At the bottom, there are three tabs: 'Available', 'Installed', and 'Updates'. The 'Installed' tab is selected and highlighted with a red dashed box. Below the tabs, there is a pagination bar showing 'Displaying 1-100 of 282'. Below the pagination bar, there is a table with the following columns: 'Package name', 'Version', 'Size (.ipk)', and 'Description'. The table lists several installed packages, each with a 'Remove...' button in the rightmost column.

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	-	-

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 **OK** button for the installation – regarding the upcoming hints on the screen.

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

You can also install distributed packages to the router from of the official OpenWRT repository website of the current CPU architecture (Cortex A7 v5):

1. https://downloads.openwrt.org/releases/22.03.4/packages/arm_cortex-a7/
2. Download the IPK package to your computer – file(s) with *.ipk extension, which you want to install to the router.

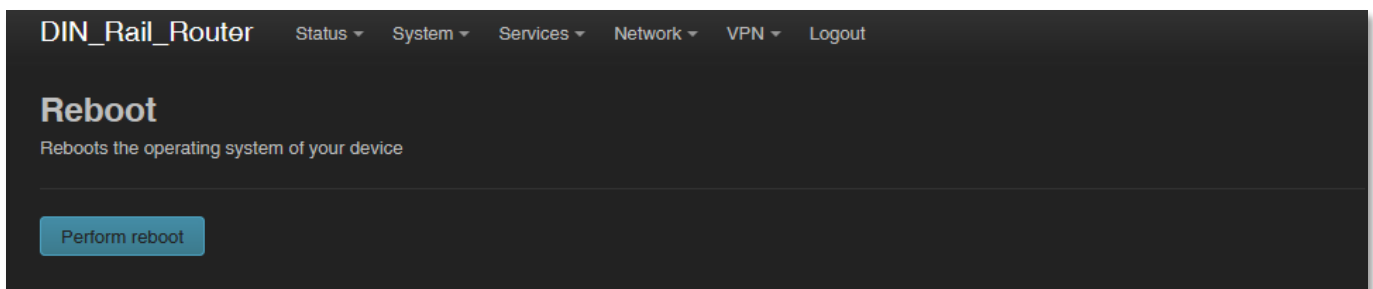
3. Open an SFTP connection to the router (e.g with *WinSCP* on **port** nr. **22** with the known credentials (username: **root**, password: **wmrpwd**).
4. Copy the required *.ipk files into the **/tmp** directory
5. Open an SSH command line (e.g. with *putty*) and use the following commands to install:

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

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

10.3 Restarting the router

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



Alternatively, you can also use the **Reset** button (6) on the device to push it shortly for less than 10 seconds.

Then the router will be restarted as it was described before (all the LEDs will be blank for a few seconds, then later the **POWER** LED will be lighting by **green** - assigns the booting process. Later other LEDs could be also indicating activity).

Then the router will be operating ordinary and will be connected to the internet according the configuration settings.

10.4 Shutdown / halt of the router

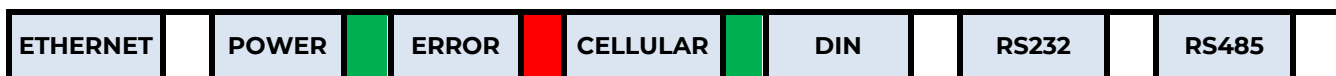
Turn off the router by pulling out / disconnecting the DC power connector from the **DC** input of device.

10.5 Start the router

You can start the device anytime by adding the 9-28V DC power to the 2-pins of the **DC** power connector (or by connecting an 12V / 24V DC adapter). Soon the **POWER** LED will be lighting, and the router will begins its start sequence.

10.6 Reset the router configuration

1. Push down the **Reset** button (6) on the device for at least 10 seconds, then release.
2. When the **Reset** button has been released, the **ERROR** LED will lighting by **red** and the **CELLULAR** LED will lighting by **green** for ca. 1-2 seconds to sign that the system configuration has been restored to the factory settings.

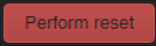


3. The router will be restarted immediately, all the LEDs will be blank for 15-20 seconds.



4. Soon the *OpenWrt*[®] system will be loaded and started with the factory configuration settings. When the **POWER** LED will lighting again by **green** and **ETHERNET** LED or **CELLULAR** LED may sign some activity, you can login to the OpenWrt interface of the router.

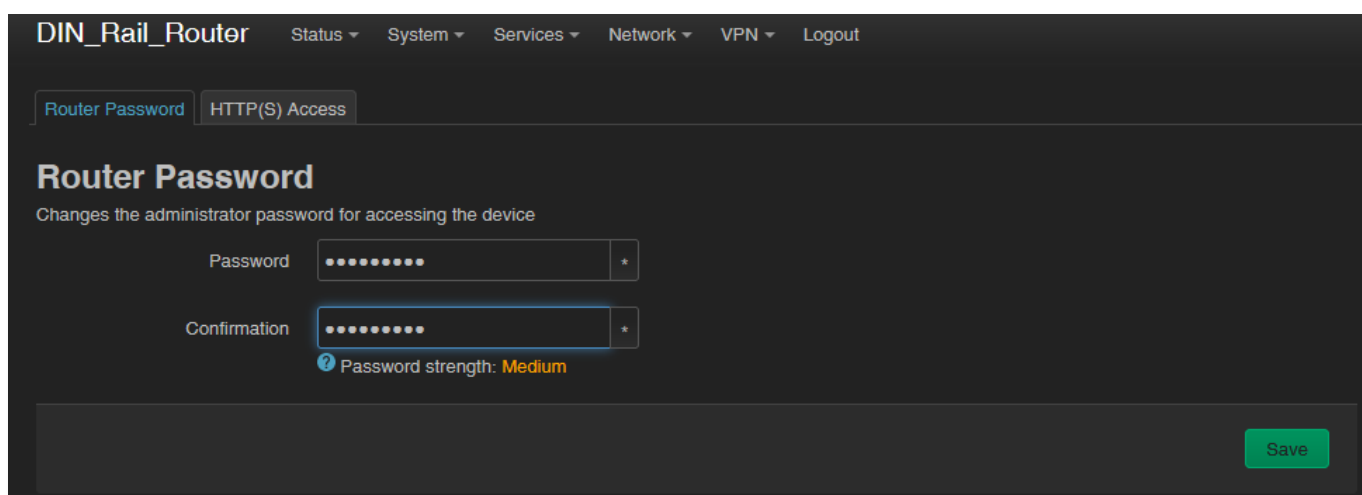


Alternatively, the reset can be initiated by choosing the **System / Backup and Flash Firmware** menu, by pushing the  button.

10.7 Password change

Open the **System / Administration** menu.

At **Router password** part, you should fill the new **Password** and once more to the **Confirmation** field. You will be able to login further by this new password.



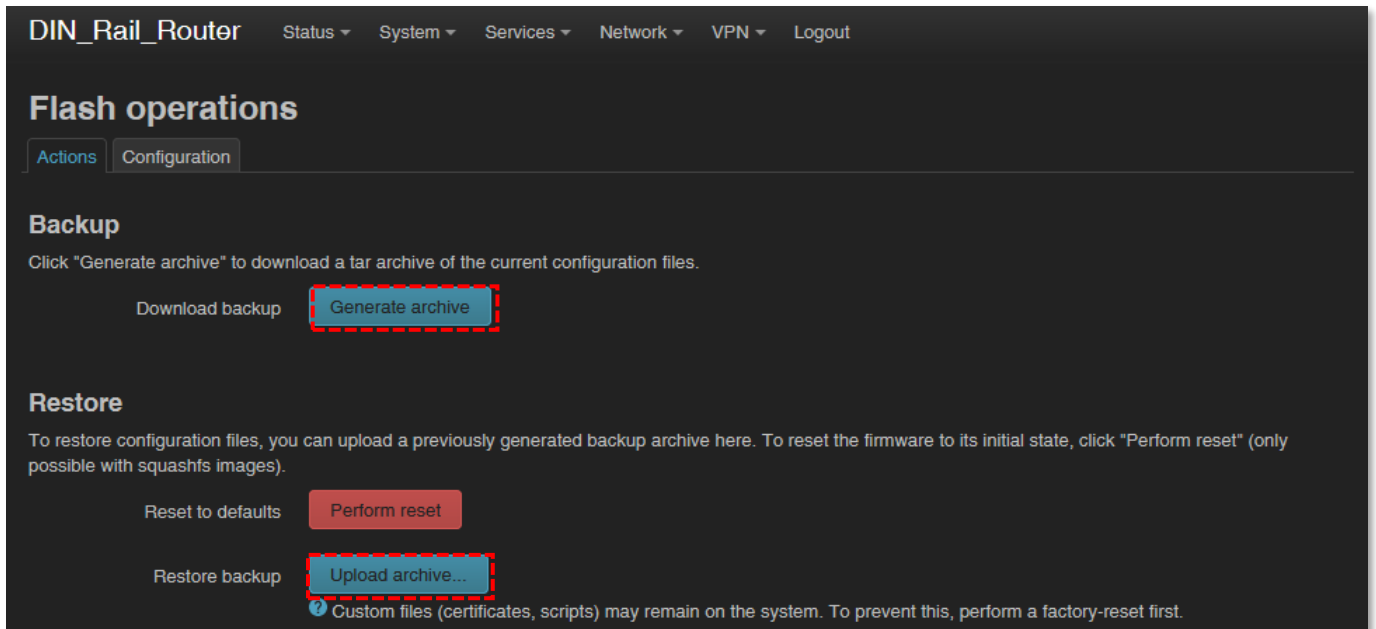
The screenshot shows the 'Router Password' configuration page in the OpenWrt web interface. The page title is 'DIN_Rail_Router' and the navigation menu includes 'Status', 'System', 'Services', 'Network', 'VPN', and 'Logout'. The 'Router Password' tab is selected, and the sub-tab is 'HTTP(S) Access'. The main heading is 'Router Password' with the subtitle 'Changes the administrator password for accessing the device'. There are two password input fields: 'Password' and 'Confirmation', both containing asterisks. A 'Password strength: Medium' indicator is visible below the confirmation field. A green 'Save' button is located at the bottom right of the form.

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

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

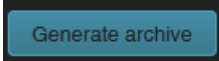
10.8 Backup and restore of settings

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



Therefore, you can save the settings to your computer as follows and restore them to the 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!

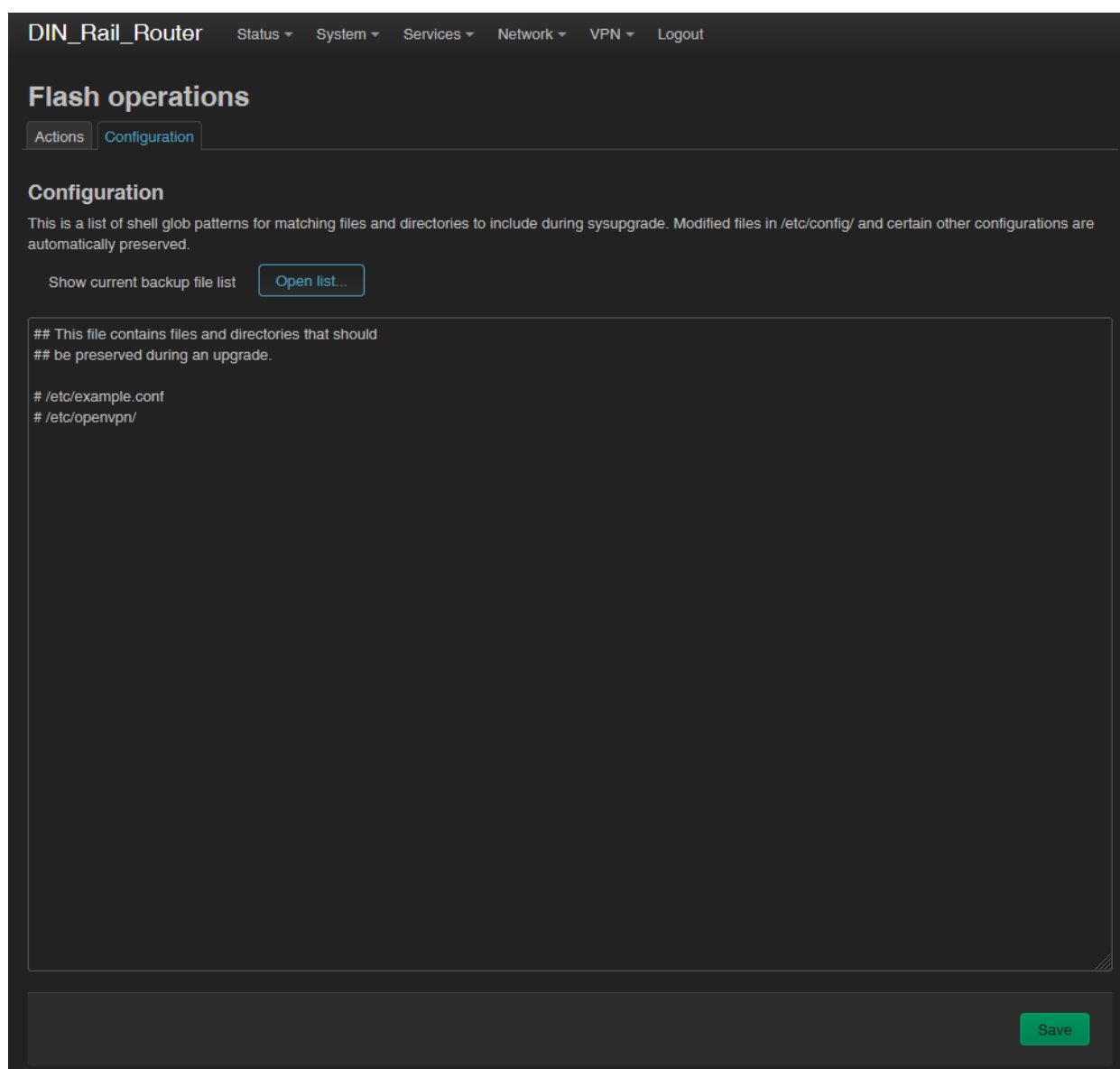
During subsequent restarts, the router will always start with these saved settings - as the default configuration.

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

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

To use it properly, you need some directory- and file-level knowledge of the 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 backup file previously saved to your computer – in .tar.gz. format – and here you can upload back to the router. You can validate your request at **Restore backup** part.

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

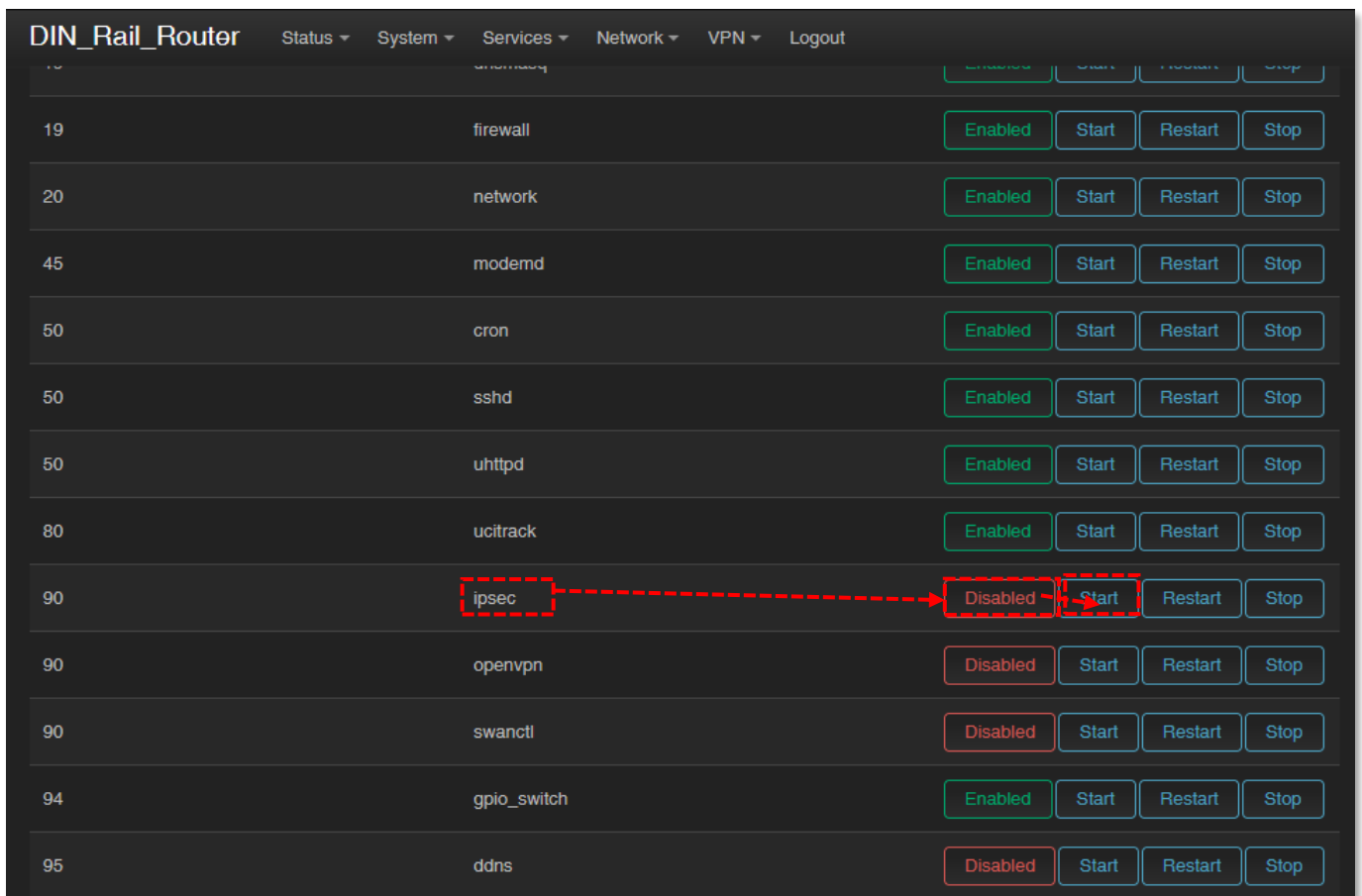


Click the **Browse...** button to select the previously saved file from your computer and push the **Upload** button to perform the restore of settings.

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.

10.9 Start or stop a system service

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



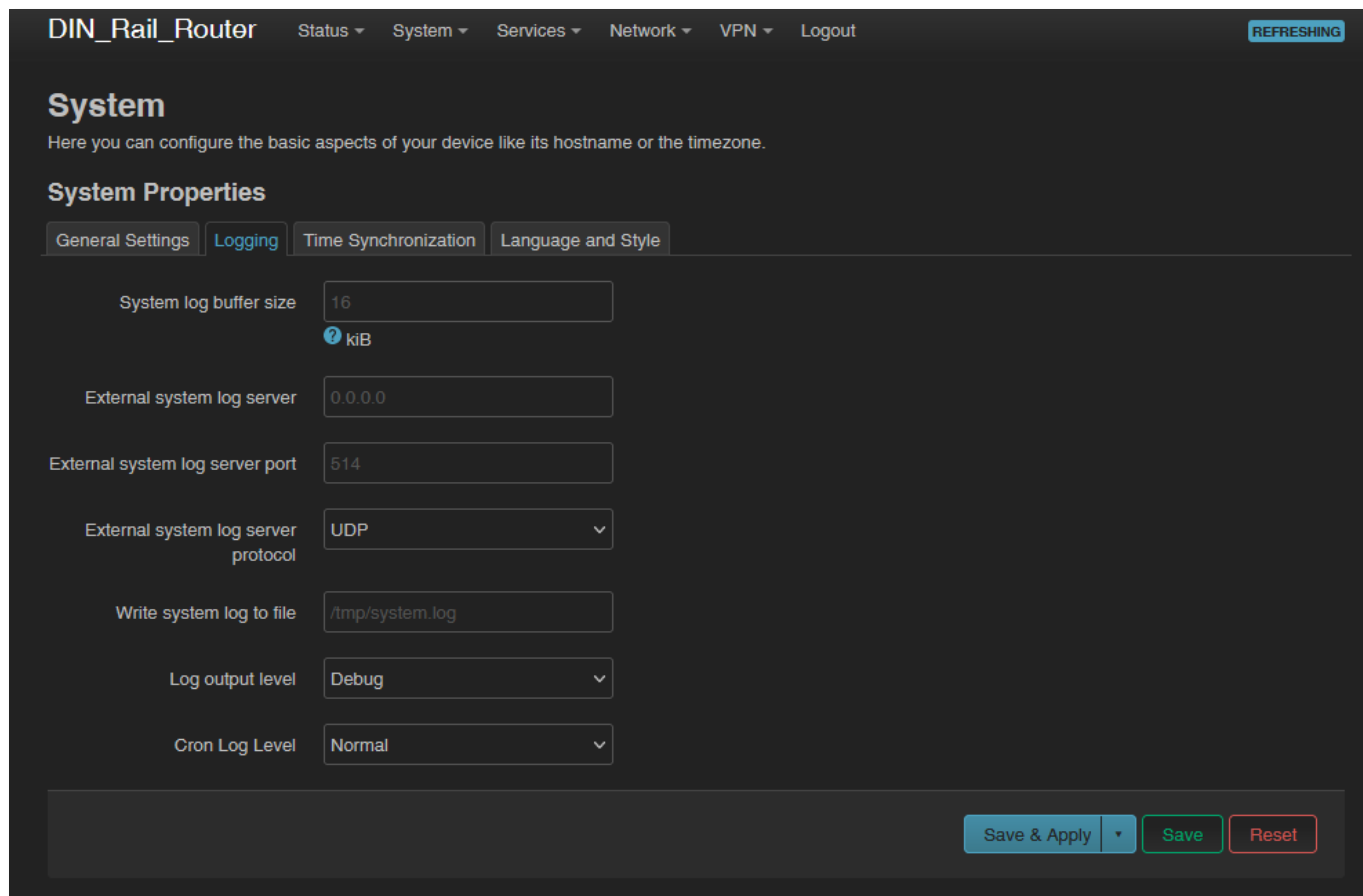
Click the **Disabled** button of the service. Wait while the system will refresh the list, then now it should already have **Enabled** status. You can start the service by pushing to the **Start** button to initialize the required service.

You can stop the service anytime by pushing the  button.

10.10 Log

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

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**.



The screenshot shows the 'System Properties' configuration page for a 'DIN_Rail_Router'. The 'Logging' tab is selected, showing various settings for system logging. The settings include:

- 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
- Cron Log Level: Normal

At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

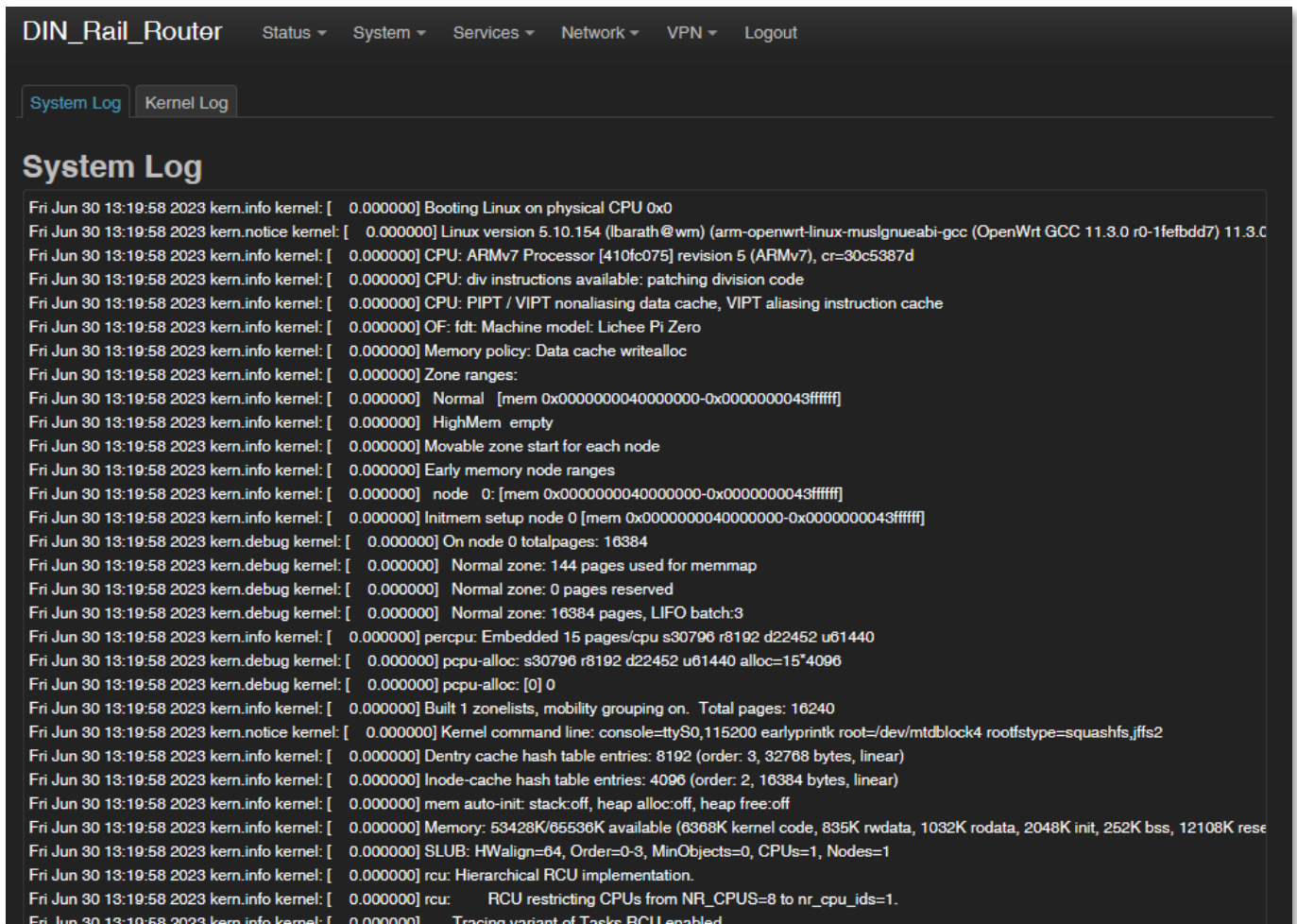
You can limit the size of the log file (**System log buffer size**) and set the IP address of the **External log server** (IP address), **port**, **protocol** - to send the log files to a remote server.

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 router was last rebooted. This can be especially useful when found an operation issue, when a features is not available yet, or even if the cellular module indicates some connection trouble.



The screenshot shows the 'System Log' tab selected in the 'DIN_Rail_Router' interface. The log content is as follows:

```
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Booting Linux on physical CPU 0x0
Fri Jun 30 13:19:58 2023 kern.notice kernel: [ 0.000000] Linux version 5.10.154 (lbarath@wm) (arm-openwrt-linux-muslgnueabi-gcc (OpenWrt GCC 11.3.0 r0-1fefbdd7) 11.3.0)
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] CPU: ARMv7 Processor [410fc075] revision 5 (ARMv7), cr=30c5387d
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] CPU: div instructions available: patching division code
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] CPU: PIPT / VIPT nonaliasing data cache, VIPT aliasing instruction cache
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] OF: fdt: Machine model: Lichee Pi Zero
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Memory policy: Data cache writealloc
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Zone ranges:
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Normal [mem 0x0000000040000000-0x0000000043ffffff]
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] HighMem empty
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Movable zone start for each node
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Early memory node ranges
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] node 0: [mem 0x0000000040000000-0x0000000043ffffff]
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Initmem setup node 0 [mem 0x0000000040000000-0x0000000043ffffff]
Fri Jun 30 13:19:58 2023 kern.debug kernel: [ 0.000000] On node 0 totalpages: 16384
Fri Jun 30 13:19:58 2023 kern.debug kernel: [ 0.000000] Normal zone: 144 pages used for memmap
Fri Jun 30 13:19:58 2023 kern.debug kernel: [ 0.000000] Normal zone: 0 pages reserved
Fri Jun 30 13:19:58 2023 kern.debug kernel: [ 0.000000] Normal zone: 16384 pages, LIFO batch:3
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] percpu: Embedded 15 pages/cpu s30796 r8192 d22452 u61440
Fri Jun 30 13:19:58 2023 kern.debug kernel: [ 0.000000] pcpu-alloc: s30796 r8192 d22452 u61440 alloc=15*4096
Fri Jun 30 13:19:58 2023 kern.debug kernel: [ 0.000000] pcpu-alloc: [0] 0
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Built 1 zonelists, mobility grouping on. Total pages: 16240
Fri Jun 30 13:19:58 2023 kern.notice kernel: [ 0.000000] Kernel command line: console=ttyS0,115200 earlyprintk root=/dev/mtdblock4 rootfstype=squashfs,jffs2
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Dentry cache hash table entries: 8192 (order: 3, 32768 bytes, linear)
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Inode-cache hash table entries: 4096 (order: 2, 16384 bytes, linear)
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] mem auto-init: stack:off, heap alloc:off, heap free:off
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Memory: 53428K/65536K available (6368K kernel code, 835K rwddata, 1032K rodata, 2048K init, 252K bss, 12108K reserved)
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] rcu: Hierarchical RCU implementation.
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] rcu: RCU restricting CPUs from NR_CPUS=8 to nr_cpu_ids=1.
Fri Jun 30 13:19:58 2023 kern.info kernel: [ 0.000000] Tracing variant of Tasks RCU enabled
```

Chapter 11. Troubleshooting

LED activity

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

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

First you should ensure about the router is still under starting / booting phase or not. Please wait 2-3 minutes, then check the LED signals again. If the LEDs on the top cover are constantly 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.

Power source

Check that the router can get any power through its power connector (**DC**) – the power adapter is connected to the router's **DC** connector and the 12V / 24V DC adapter to the 230V AC plug.

When it receives 9-28V DC power, the **POWER** LED indicates it by **green** light.

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 **RJ45** port. When the router is operating, the **ETHERNET** LED should sign the network activities.

If the router is not starting

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

Periodic restart of the router (by 10 minutes periods)

When router was not be configured properly for the 4g-wan connection or the modem was not started then the router will be restarted within in 10 minutes.

Restart of the router

Restart the router from the web user interface, in **System / Reboot** menu. The device will be rebooting, while the **POWER** LED will be blank for ca. 5 seconds (all of the LEDs will be blank during the start of the rebooting). After 1-2 minutes, the router will be available again on its interfaces.

Shutdown / halt the router

Push the **Reset** button (6) on the device for less than 10 seconds. Then the router will be powered off immediately when you release the button. Then all LEDs will be blank.

***Important!** Note, that in this case the router can be started later only by removing / disconnecting the DC power cable and then reconnecting the cable tot he **DC** input. Alternatively, you can turn off the router by pulling out / disconnecting the DC power connector from the **DC** input of device.*

Turn on the router

You can start the device anytime by adding the 9-28V DC power to the 2-pins of the **DC** power connector (or by connecting an 12V / 24V DC adapter). Soon the **POWER** LED will be lighting, and the router will begins its start sequence.

***Important!** Note, that in this case the router can be started later only by removing / disconnecting the DC power cable and then reconnecting the cable tot he **DC** input. Alternatively, you can turn off the router by pulling out / disconnecting the DC power connector from the **DC** input of device.*

Antenna

Use the proper antenna type regarding the used cellular module and mobile network. Connect the SMA antenna properly to the antenna connector (7) by mounting it.

Check RSSI signal value and vital signals on the OpenWrt web interface (**Status / Overview** menu, at RSSI / CSQ values).

Important! Always turn off the router before mount an antenna or change an antenna to another type.

Successful cellular network registration

The cellular module operation is signed by the **CELLULAR** LED.

If the cellular network registration is in progress on APN, the LED will flashing by **green**.

When network registration, APN access is succesful then the LED will lighting by **green**. This means that the router can access the cellular network.

SIM/APN failure

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

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

The SIM / APN error can also be caused by incorrect 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 router, insert a working SIM properly, start the router, configure the APN and SIM settings on the local website of the router.

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

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

- **No NW registration** - The APN name or SIM is not configured or these settings are incorrect.
- **Check NW registration** - The APN connection is in progress.
- **Check RSSI** - No antenna connected and / or SIM is incorrectly configured or incorrect. Check the antenna and SIM again.
- **RSSI timeout** – The cellular network registration was attempted to try several times, but it was not successful. Restart the router for the further cellular network connection attempts.

SIM card cannot be detected

Turn off the router - unplug the power plug from the **DC** connector (2) of the device. Then, make sure that there is a SIM card in the **SIM** slot (4) 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 **DC** power connector (2).

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.

Faults, errors

In case of any error or fault, the **ERROR** LED will be lighting or blinking by **red**.

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/industrial-din-rail-router/>

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.