M2M Router®
User Manual
v2.10

WM Systems LLC  8 Villa str., Budapest  H-1222  HUNGARY
Phone: +36 1 310 7075  Fax: +36 1 319 8249
Email: sales@m2mserver.com  Web: www.m2mserver.com
Document specifications

This document was completed for the **M2M Router®** device and contains the detailed description of the device configuration which is necessary for the proper operation of the device.

You can choose CDMA 450, 2G, 3G, 4G, LTE 450 and Narrow Band versions of the modem types. All of the listed settings are more or less similar for the modem versions.

If you are using the router with RS232/RS485 additional interface, pls. check the RS232/RS485 chapter at Serial Proxy part in this document.

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

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Document subject:</td>
<td>M2M Router®</td>
</tr>
<tr>
<td>Author:</td>
<td>WM Systems LLC</td>
</tr>
<tr>
<td>Document version No.:</td>
<td>REV 2.10</td>
</tr>
<tr>
<td>Number of pages:</td>
<td>36</td>
</tr>
<tr>
<td>Hardware Identifier No.:</td>
<td>BE0077D_CMADA450, BE0077C_CMADA450, BE0077B_CMADA450</td>
</tr>
<tr>
<td>OpenWRT build version:</td>
<td>2020-03-05</td>
</tr>
<tr>
<td>Linux Kernel version:</td>
<td>4.4.4</td>
</tr>
<tr>
<td>Firmware version:</td>
<td>2019-01-18</td>
</tr>
<tr>
<td>Document status:</td>
<td>Final</td>
</tr>
<tr>
<td>Last modified:</td>
<td>16 November, 2019</td>
</tr>
<tr>
<td>Approval date:</td>
<td>16 November, 2019</td>
</tr>
</tbody>
</table>
# Table of contents

1. **Starting up the Router** .................................................................................. 5
   1.1 Interfaces ........................................................................................................ 5
   1.2 Cable connection .............................................................................................. 5
   1.3 Starting the router .......................................................................................... 6
   1.4 Web user interface of the router ...................................................................... 7
   1.5 Accessing the router on ssh connection ......................................................... 8
   1.6 Remote configuration of the router by Remote Device Manager software ........ 9

2. **Web Administration user interface** ................................................................. 10
   2.1 Main page (Dashboard) .................................................................................. 10
   2.2 Menu .............................................................................................................. 11
   2.3 Status menu .................................................................................................... 13
   2.4 CDMA menu (only for CDMA devices) ......................................................... 13
   2.5 System menu .................................................................................................. 13
   2.6 Router menu .................................................................................................. 14
   2.8 Services menu ............................................................................................... 14
   2.8 Network menu ............................................................................................... 14

3. **Network configuration of the router** .............................................................. 15
   3.1 Interface settings ........................................................................................... 15
   3.2 Mobile internet settings (modem) ................................................................. 16
   3.3 Ethernet (LAN) settings ................................................................................. 23
   3.4 DHCP settings .............................................................................................. 25
   3.5 DNS settings ................................................................................................ 27
   3.6 Defining the route rules ................................................................................. 28
   3.7 Firewall settings ........................................................................................... 28
   3.8 Port Forward settings .................................................................................... 33
   3.9 IP routing, NAT settings .............................................................................. 34
   3.10 Dynamic DNS settings .............................................................................. 35

4. **Special settings** .............................................................................................. 37
   4.1 Remote Device Manager settings ................................................................. 37
   4.2 Monitoring the modem .................................................................................. 38
   4.3 Ping an IP address ......................................................................................... 38
   4.4 Network Time Service (NTP) ....................................................................... 39
   4.5 TFTP service settings ................................................................................... 40
   4.6 Identifying names connecting machines ..................................................... 41
   4.7 LED configuration ......................................................................................... 41
   4.8 OpenVPN configuration .............................................................................. 42
   4.9 Ser2Net (RS232, RS485) configuration ....................................................... 44
   4.10 Periodic ping and periodic reboot configuration ....................................... 45
5. Software refresh and router maintenance .......................................................... 47
  5.1 Firmware refresh ............................................................................................ 47
  5.2 Installing applications ..................................................................................... 48
  5.3 Restarting the router ...................................................................................... 49
  5.4 Shutdown / halt of the router .......................................................................... 50
  5.5 Reset the router .............................................................................................. 50
  5.6 Password change ............................................................................................ 50
  5.7 Backup and restore of settings ....................................................................... 50
  5.8 Handling external storage (uSD card, USB drives) ......................................... 51
  5.9 RS485 MBus meter connection ....................................................................... 53
  5.10 SSH configuration .......................................................................................... 56

6. Troubleshooting .................................................................................................. 58

7. Support availability .............................................................................................. 64
  7.1 Contact the support line .................................................................................. 64
  7.2 Product support ............................................................................................... 65

8. Legal notice .......................................................................................................... 66
1. **Starting up the Router**

1.1 **Accessories**

Unpack the router and the antennas from the product paper box. Prepare for the installation and the configuration, follow the next hints.

1.2 **Cable connection**

1. **Mount** a 2G, 3G or LTE 450, CDMA 450 or Narrow Band **SMA**-type communication **antenna** to the **Antenna** (Main) titled SMA-M interface (according to the module/router type).

**Attention!**

*In case of 4G version router, please use two antennas for the good signal reception!*
2. **Insert a SIM card** (APN and data activated) to the SIM holder, placed the chip-side up and the cutted edge towards to inside and push until it sleeves.

3. **Connect UTP cable** to the router Ethernet titled port. The other side of the cable must be **plugged to the PC’s Ethernet port**.

4. **The DHCP service is turned off for the router Ethernet interface**, by default. Therefore, **you have to configure an IP address for you PC, manually.**

   As an example, add the 192.168.127.10 IP address to your computer’s Ethernet interface for connecting to the router.

### 1.3 Starting the router

1. **Plug** the **12V DC power adapter cable to the POWER interface**, then **plug the adapter to the 230V electrical network**.

2. The router has a pre-installed system (contains uploaded firmware and system software). After plugging the power adapter, the router begins to work, whereas its **LED signals** are showing the current **activity** during the operation.

   When power up the router, all the three LEDs will flashes once – as in case of restart.

   If the device was under power supply the **LED1** will light continuously (which means that the system booting is in progress).

3. The system is starting, which takes about 1-2 minutes. During the boot the **LED1** will lighting by **green**. After cca. 2 minutes, **LED1** will flashing once in every 10 seconds which means it is available on its local interfaces. Now you can login to the web user interface.

4. **As soon as you can, configure the internet settings of the wireless module (SIM and APN) for connecting to the NB-IoT network** – in other case the router will be **restarted in every 10 minutes**.

5. Then the router tries to connect to the mobile network (autenticates and logging to the APN zone and will be initiating the network connection) – if that was configured and the SIM card network registration has performed, then the **LED2** will lighting continuously, which signs that the the router has access to the mobile network and can transmit data.

6. **Change the web login password as soon as you can.**

7. If you need, turn on the DHCP service.

If you notice any failure or unusual LED flashing, then go to the **Troubleshooting** chapter.
1.4 Web user interface & Login
For accessing the router through the web user interface you have to setup the IP address of the Ethernet interface on your computer to allow the fixed ipv4 address for the following IP address: 192.168.127.1, Subnet mask: 255.255.255.0)

**Attention!**
For accessing the web user interface we offer the Mozilla Firefox web.

Default web user interface (LuCi) address is: [https://192.168.127.1:8888](https://192.168.127.1:8888)
(USB web address: [https://192.168.10.1:8888](https://192.168.10.1:8888))

At first time, you have to allow the security risk in the Mozilla® browser by choosing the Advanced option at the Potential Security Risk.

![Warning: Potential Security Risk Ahead](image)

Then choose the Accept the Risk and Continue option here.
Now, you can login to the router's local website (LuCi interface) - through the Ethernet interface – accessing the default URL.

The login data are the following:

- **Username:** root
- **Password:** wmrpwd

Then push to the **Login** button to load the configuration management user interface of the router.

**Attention!**
When connecting to the public network, it is recommended to change the login password!
The ethernet IP address can be modified after login from the OpenWrt.
1.5 Accessing the router on ssh connection

The router can be accessed through an OpenSSH connection, when it is available on its IP address – by a terminal utility (e.g. putty) – at 192.168.10.1:22 (Login: root, Password: wmrpwd). When connecting, you have to allow the usage and store of the encryption key on your client, then the following login screen appeas in your command line on your computer.

1.6 Remote configuration of the router by Device Manager® software

You can use the remote device management application (Remote Device Manager®) for maintaining your m2m routers. The application provides you continuous QoS monitoring of operation, remote re-configuration and installation of firmware updates.

There you can manage hundreds of routers by checking their network availability.

You can also storage the current configuration or reconfigure mass of the routers in one step or refresh the firmware for a group of routers - or singular devices as well.
The application is available through license pack constructions, please advise our sales about the license pack options.

You can get further information on the Remote Device Manager® website:

https://www.m2mserver.com/en/product/m2m-device-manager/
# 2. Web Administration user interface

## 2.1 Dashboard (Main page)

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

<table>
<thead>
<tr>
<th><strong>System</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>M2M-Router</td>
</tr>
<tr>
<td>Model</td>
<td>Atnal AT91SAM3X25-EK</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>OpenWrt Designated Driver r49022 / LuCI Master (git-15.137.54403-67d39e)</td>
</tr>
<tr>
<td>Build Date</td>
<td>2019-07-10 14:00:58.491974475+02:00</td>
</tr>
<tr>
<td>Kernel Version</td>
<td>4.4.4</td>
</tr>
<tr>
<td>STM32 Firmware</td>
<td>201901181</td>
</tr>
<tr>
<td>Local Time</td>
<td>2019-07-10 12:51:14</td>
</tr>
<tr>
<td>Uptime</td>
<td>0h 15m 46s</td>
</tr>
<tr>
<td>Load Average</td>
<td>0.38, 0.32, 0.26</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Memory</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Available</td>
<td>95744 kB / 125450 kB (75%)</td>
</tr>
<tr>
<td>Free</td>
<td>91980 kB / 125450 kB (73%)</td>
</tr>
<tr>
<td>Buffered</td>
<td>3784 kB / 125450 kB (3%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Network</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Modern Model</td>
<td>ME910C1-E1</td>
</tr>
<tr>
<td>IMEI</td>
<td>356345080013401</td>
</tr>
<tr>
<td>SIM ID</td>
<td>89882350000652445353</td>
</tr>
<tr>
<td>Modern RSSI</td>
<td>11</td>
</tr>
<tr>
<td>Modern SQ</td>
<td>99</td>
</tr>
<tr>
<td>CREG</td>
<td>2,5,”1072”,”E785C”.9</td>
</tr>
<tr>
<td>COPS</td>
<td>0.0, ”vodafone HU”.9</td>
</tr>
<tr>
<td>IPv4 WAN Status</td>
<td>3g</td>
</tr>
<tr>
<td>Type:</td>
<td>3g</td>
</tr>
<tr>
<td>Address:</td>
<td>10.21.40.7</td>
</tr>
<tr>
<td>wan Netmask:</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

Check that the **Build Date** (OpenWrt) is 2019-07-10 or newer version, and the **STM32 Firmware version** – which must be at least 2019-01-18 or newer.
At the **Network** part you can identify the **Modem Model**, the modem identifier (**IMEI**), the SIM identifier (**SIM ID**), and the **Modem RSSI** (signal strength) and **Modem SQ** (signal quality in CSQ) and the **mobile network registration, login and access information** as well (**CREG, COPS**).

You also can check the **IPv4** and **IPv6 WAN status** and the connection **Type** to the public Internet. There you can check the **DHCP** and **DNS** information as well.

### 2.2 Menu

By the menu you can access the following features:

- **Status** – Status data, operation logs, operation monitoring
- **System** – System settings, administration, software and fw-refresh, backup/restrore of the configuration settings
- **Router** – Device Manager settings, Modem and Logging parameters, Ping an IP address, Daily restart, Factory settings
- **Services** – DynDNS (dynamical DNS) settings, OpenVPN settings
- **Network** – network interface settings, DHCP, DNS, Route rules, diagnostics, firewall

### 2.3 Status menu

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

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

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

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

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

2.5 System menu

You can found several system settings in these menu items:

- In the System menu: Hostname (router name), Time synchronisation (time and NTP server settings), Logging, Language (of user interface)
- Administration: Password (for admin user interface) and the SSH Access
- Installation of further **Software** (3rd party tools, applications for the Linux distribution).
- You can define the **Startup** applications - resident - programs during the operation.
- You also can define **Scheduled Tasks** for starting them in the right time and sequence.
- Setup the NTP server for **Time Synchronisation**.
- The **Mount Points** are showing the available (mounted) shares and drives.
- The **LED Configuration** is also configurable.
- You also can **Backup / Flash firmware** updates.
- Even the **Reboot**ing the router.

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

### 2.6 Router menu

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

### 2.7 Services menu

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

### 2.8 Network menu

- Here you can configure the settings of each network **Interfaces**
- You can modify the **DHCP** and **DNS** settings,
- or define the router network device name at the **Hostname**.
- The **Static route** paths can be also defined.
- The **Firewall** rules can be declared here as the following submenu items: Port forward, IP router, NAT settings.
- **Diagnostics** - you can test network operation and connection health (ping IP address).
3. Network configuration of the router

3.1 Interface settings

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

The network interfaces are listed at the Interface Overview. The LAN interface means the Ethernet port connection (eth0), the USBLAN is the USB-Ethernet (usb0) and the WAN interface is the public wireless Internet connection (3g-wan) for the CDMA450, 2G, 3G, 4G LTE or LTE 450 modem. You can modify the settings with the Edit button.

Modifying the 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 button reconnects the related interface connection. At the upper WAN, USBLAN, LAN title you will found further settings for the chosen Interface.
3.2 Mobile internet settings (modem)

3.2.1 Configuring the 4G module

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

Setup the module for connecting to the CDMA 450 / 2G / 3G / 4G / LTE 450 or Narrow Band mobile network (according to the assembled module type) – at the **WAN** interface tab.

Configure the module to the wireless internet and for the 2G/3G/LTE network connection (by the modem type and network behaviour) here for the **WAN** interface.
For configuring and enabling the roaming settings — in case of international or country border usage — you may need to setup the Mobile country code and Mobile network code parameters — even if you are attempted to use only a preferred mobile network.

The international country codes can be found here: [http://mcc-mnc.com](http://mcc-mnc.com)

Ask your mobile operator about the available international settings.

You can define the SIM #1 APN account name, and the SIM #1 PIN code if it is necessary for the connection.

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

Here you will found some examples for the APN settings.

**M2M APN (enclosed)**

APN name: wm2m

**Public Internet APN**

APN name: net

**Attention!**
* ALWAYS use the given APN name and password of your Mobile Operator.

**ONLY for NB IoT (Vodafone GDSP SIM)**

APN: nb.inetd.gdsp

APN password: *(not presented)*

**ONLY for GDSP SIM (WM2M GDSP)**

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

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

APN username: **IMSI** identifier of the SIM card (number written on the SIM card, and which is usually starting with “20404” tag)
APN password: **wm2m.gdsp**  // for using the Hungarian WM2M

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

**Automatic mode**

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

**Authentication**

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

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

**Attention!**

After configuring the APN and saving & applying the settings of the WAN interface, you must restart the router as soon as you can! Choose the System menu / Reboot item and reboot the router - then the modem will be restarting by the new settings!
3.2.2 Configuring the 2G, 3G, LTE 450 or NB module

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

**In case of CDMA450 router version you must not configure this settings, step to the Chapter 1.10, please.**

Setup the module for connecting to the CDMA 450 / 2G / 3G / 4G / LTE 450 mobile network (according to the assembled module type) – at the **WAN** interface tab.
Configure the module to the wireless internet and for the 2G/3G/LTE network connection (by the modem type and network behaviour) here for the **WAN** interface.

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

The international country codes can be found here: [http://mcc-mnc.com](http://mcc-mnc.com)

Ask your mobile operator about the available international settings.

You can define the **SIM #1 APN** account name, and the **SIM #1 PIN** code if it is necessary for the connection.

**Attention!**

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

Here you will found some examples for the APN settings.

**M2M APN (enclosed)**

APN name: wm2m

**Public Internet APN**

APN name: net

**Attention!**

*ALWAYS use the given APN name and password of your Mobile Operator.*

*The LTE450 communication needs special network and an LTE450 capable SIM-card for the successful connection!*  

**ONLY for using the GDSP SIM (WM2M GDSP)**

By using the GDSP SIM you have to follow the hints of the mobile operator when filling the SIM #1 APN, APN username and password fields.
In case of APN (WM2M network): **wm2m.gdsp**

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

APN password: **wm2m.gdsp** // for using the Hungarian WM2M

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

**Automatic mode**

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

**Authentication**

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

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

**Attention!**

*After configuring the APN and saving & applying the settings of the WAN interface, you must restart the router as soon as you can! Choose the System menu / Reboot item and reboot the router - then the modem will be restarting by the new settings!***
3.3 Ethernet (LAN) settings

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

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

Change the default 192.168.127.1 router IPv4 address to an own IP address, regarding the current subnet. Check the IPv4 netmask to be proper for the selected and required network class which you are attempted to use.
When you have modified the settings, save them by the **Save & Apply** button.

**Important!**

*The DHCP service is turned off for the router Ethernet interface, by default. Therefore, you have to configure an IP address for your PC, manually.*

If you are not attempted to use a fixed IP address for the router, and if you are attempted to use given IP by a different network device (by DHCP service), then modify the IPv4 address to the connecting gateway – or other network device - IP address, and choose the *Static address* at the **Protocol**, the **DHCP client** setting, and push the **Switch protocol** button.

Then the DHCP client will be activated for ethernet interface.

Push the **Save & Apply** button for performing the changes.
**3.4 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** menu, **Interfaces** (according to the required interface), **Edit** and **Advanced Settings** tab item.

---

**Important!**

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

---

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

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

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

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

In the **Static Leases** part you can add devices to always provide the same dedicated IP address by the router. This can be required by adding values to the **Hostname**, the **MAC-Address** and the **IPv4-Address**.

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

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

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

When you have modified the settings, save them by the **Save & Apply** button.
3.6 Defining the route rules
In the **Network** menu, **Static routes** item 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 **Host-IP** or **Network** name, the **IPv4-Netmask**, and **IPv4-Gateway**. Save the settings by the **Save & Apply** button.

![M2M-Router Network menu](image)

3.7 Firewall settings
By default, the firewall is active, but it allows all communication. It can be necessary to limit the traffic.
On the public internet the you can have several network attack and getting unwanted communication, internet data collection by applications. These all over the unwanted network activity causes the growing the mobile network traffic and increasing the transmitted amount of data (which is unnecessarily decrease the available data package amount of the SIM card).
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** menu, **Firewall** item 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 it can be seen, there are several communicating IP addresses on several ports to the router and subnet.

---

**Important!**

It is offered to check the network traffic on the router. Check the connections, the active communication channels (port number, incoming IP) and listen the incoming activities and for sure the output traffic! These all you can check in the **Status** menu, **Realtime Graphs** item at the **Connections** tab – where these can be listed.
Another method for limitation can be the whole disabling with opening and enabling only the necessary communication ports, IP-segments or allowing exact IPs.

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

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

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

You can **Delete** the settings or **modify**.

At the **Zones** part you can **Add** a new rule to the current ones. You also can **Delete** or **modify** an existed rule.
When you are attempted 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, etc).

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

At the **Advanced Settings** tab you can limit the incoming, outgoing, and forwarded traffic for each subnets.

When you have modified the settings, save them by the **Save & Apply** button.
The firewall can be configured by default to allow or tilt the communication – according to the chosen settings.

Therefore it does not protect the router against external network attacks or intrusions when just enabling the firewall feature. Further port-level filtering or interface traffic limits, or Traffic Rules settings are necessary to define!

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

Here in the **Network** menu, at the **Firewall** item, **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 add a new rule by the Add button.

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

### 3.9 IP routing, NAT settings

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

You can add a new rule by the Add button.

![Firewall - Traffic Rules](image)

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

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

The Source NAT settings can be performed for each protocol (tcp, udp), that the router allows the redirection of data – which incoming IP address and port must be redirected to which outgoing IP address and port and must be forwarded the data traffic. You also can define a port range, hereby.
These rules must always be defined, not disallowing the general communication and must consider that the router must be further available on the network. It is easy to enclose the router from the network or disabling the remote access. Please, be careful when configure these settings.

**Important!**

Always check the used standard ports by the network services and allow these (e.g. FTP: port 21, SSH/Telnet: port 22, web: port 80, general network traffic on windows: 443, etc.).

The proper port filtering, routes are minimizing the communication, what could be important by safety reasons, and could decrease the open threads and risks of safety leaks. Always limit the access of services, and decrease the amount of the throughput communication on the network by rules to provide the operation of the necessary services, ports.

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

### 3.10 Dynamic DNS settings

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

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

You can **Enabled** or disabled the DNS rules to a registered hostname or IP.
When you have modified the settings, save them by the **Save & Apply** button.
4. Special settings

4.1 Remote Device Manager® settings

The router parameters can be remotely reconfigured by the az M2M Device Manager® application. It is also capable of performing remote monitoring of QoS and for installing firmware updates. The necessary Device Manager settings can be defined in the Router / Device Manager menu.

The main importants are the DM IP Address, the DM Port Number and DM User Name. The default DM Port number is 443.

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

If you modified the settings, save them by the Save & Apply button.
4.2 Monitoring the modem

At the **Router / Modem Parameters** menu you can define some special operation monitoring and listener parameters for the modem. The **Watchdog timeout** can be declared as a modem restarting time interval trigger in case of mobile network unaccessibility.

The **Max. RSSI error count** means the possible max. error in case of continuous signal strength troubles. If it is permanently low or not available, the modem will be restarted as it is defined according the **Watchdog timeout** parameter.

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

4.3 Ping an IP address

Open the **Network** menu, **Diagnostics** item. Here you can check the availability of an IP address, that is it accessible or can be pinged (**Ping**), is there a naming service provided, is there a response between two points (**Nslookup**), furthermore the path of the communication (**Traceroute**).
4.4 Network Time Service (NTP)

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

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

Open the System menu, Time Synchronisation item.
You can add hereby the refresh interval at the Update interval (in seconds).
You can define the time synch at the Clock Adjustment.

![Screenshot of Time Synchronisation page](image-url)
At the **Time Servers** part you can NTP time servers by its **Hostname**, IP-address or server name, and **Port**. When you have modified the settings, save by **Save & Apply** button.

### 4.5 TFTP service settings

Open the **Network** menu, **DHCP and DNS** item.

At the **TFTP settings** tab you can allow the TFTP service (**Enable TFTP server**), and the related further parameters.

When you have modified the settings, save them by the **Save & Apply** button.
4.6 Identifying names connecting machines

Open the **Services** menu, **Hostnames item**. Here you can register those machines, network devices which are using the router connection - for an easier identification. You can add logical names to the IP addresses which you can see as listed at the status overview.

4.7 LED configuration

Open the **System** menu, **LED Configuration** item. Here you can define the LED operation rules for the main important events.

By the **Name** field you can identify a rule, at the **LED Name** filed, where you can choose the LED light according to the following:

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

Only the free – not used - LED statuses will be visible and listed here.

The **Trigger** allows to choose an event type of operation. E.g. **netdev** menads the network interface connection type, and **Device** identifies the related network interface.
When you have modified the settings, save them by the **Save & Apply** button.

### 4.8 VPN client (OpenVPN) configuration

Open the **Services** menu, **OpenVPN** item. Here you can define and setup OpenVPN client connection and the related settings. The OpenVPN service uses the port nr. 1194.

![OpenVPN configuration page](image)

**Attention!**

For using the VPN client connection service by the router, you an already existed and properly configured VPN server setting and accessibility to the VPN network.

Choose a pre-defined instance (connection profile) – e.g. **sample_client** – then push to the **Edit** button. Then the next window appears.

Configure at least the next fields on this page:

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

Save the configured settings by the **Save & Apply** button.
The in the OpenVPN menu (previous page), push the Start button beside the configured instance name – e.g. at the sample_client record – to start the VPN service.
When you have modified the OpenVPN connection settings push the **Save** button here too.

The further advanced settings of the VPN connection can be edited by the **Edit** button, at the profile settings left side and can be initiated by the "**Switch to advanced configuration**" link at top of the screen.

For sake of the exact settings, we offer to read the related tunelling service description of the OpenWrt® administration interface which you are currently using:

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

### 4.9 Ser2Net (RS232, RS485) configuration

In case of ordering the RS232/RS485 expansion to the router, you can use the serial connection which you have to configure first.

Open the **Services** menu, **Ser2Net** item. Here you can configure the RS485 settings.
There is a **TCP Port** as the connection port.

Note that the port which is defined here, will be automatically added to the firewall settings to allow the communication. (Check Firewall settings later to ensure that it is enabled).  

The **State, Timeout** values are on factory default – so you don’t need to modify them it is not necessary. The **Device** is also pre-defined, no need to change it!

But the **Options** field is where you can declare connection parameters, separated with commas or space.

Please check these settings and if it’s necessary reconfigure the **Options** by the following hints.

- first parameter is the **baud rate** (you can use one of the following: 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200)
- second here the **parity** as EVEN, ODD, NONE
- then the **stop bits** as 1STOPBIT, 2STOPBITS
- next is the **data bits** as 7DATABITS, 8DATABITS

**Syntax** for **OPTIONS** is: baudrate parity stopbit databit  
(or baudrate,parity,stopbit,databit)

**Examples:**
- 9600 NONE 1STOPBIT 8DATABITS
- 19200,EVEN,1STOPBIT,7DATABITS

**Important!**

We offer to test the settings with 9600 baud speed rate first, then if it is communicating fluently with your connected device, then you can try further data speed rates.

At bottom of the settings, there is an **Add** button, where you can add more ports for the RS485 configuration. Save the configured settings by the **Save & Apply** button.

**4.10 Periodic ping and Periodic reboot settings**

For matching the industrial standard requirements, you can define an time interval for periodic daily restart of the router if you want in the **Services** menu / **Periodic Reboot** item.
If you want to use periodic ping as checking an IP address or remote server, device as checking its availability by the router if you want to use this service by accessing from the Services menu / Periodic Ping item.

Save the configured settings by the Save & Apply button.
5. Software refresh and router maintenance

5.1 Firmware refresh

1. Open the System menu, Backup / Flash firmware item.
2. Browse the fwos-.... compressed file then push to the Flash image button.
3. A new window will appear where the file will be checked. When it is okay, the system refreshment is possible by the Proceed button.
4. Then the next message appears on the screen in the browser. Then the refresh method has started, while the LED2 and LED3 is continuously lighting by red.

![System - Flashing...]

5. Later the LED2 will be blank, only the LED3 lighting with red.

6. At the end of the installation – the LEDs are not lighting further – the system restarting twice while all the three LEDs are continuously lighting with green, then the OpenWrt system will be loaded as it was described before.

**Important!**
This flashing... window will not closed automatically, and the browser cannot sense the availability of the OpenWrt site. Then, close the windows after the refresh and open a new with the default URL in your browser.

7. When the middle Cell LED is lighting continuously in green. Login to main page and check the software version. The installation has been finished.

8. **Important!** Restart the router from the System / Reboot menu item, then the router will now booting with the new installed system.

### 5.2 Installing applications

Open the System / Software menu.

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

You can refresh the catalog of the available applications by the **Update lists** button.
When it was successful, fill the name of the application you are attempted to install at the Download and install package field (e.g. MC – Midnight Commander esetében), and push to the OK button for the installation – regarding the upcoming hints on the screen.

The installed packages of the router are listed lower at the Status part.

5.3 Restarting the router

Choose the System / Reboot item and push upon the Perform reboot button. Then the router will be restarted as it was described before (the 3 LEDs lighting shortly by red colour for a second, and the St. LED flashing assigns the booting process, then the router will be operating as normal, and will be connected to the internet according the configuration settings.
5.4 Shutdown / halt of the router

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

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

5.5 Reset the router

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

**Important!**
Reconfigure the router on its web user interface!

5.6 Password change

Open the System / Administration menu.

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

5.7 Backup and restore of settings

Open the System menu, Backup / Flash Firmware item.

At the Backup / Restore part and Download backup feature push the button for saving the settings into a file.
The **Restore backup** is possible to reload – a previously saved configuration – when you will be able to browse and load from your computer to the router memory by pushing the button.

### 5.8 Handling of external storages (uSD card, USB drive)

The router is able to handle the connected and mounted uSD cards, USB memory sticks. But these are only possible to access from the Linux command line (ssh connection).

The partitions and memory areas are listed when you will attempted to choose the **System / Mount Points** menu. At the **Mount Points** part will be listed the automatically connected and mounted devices. These will be attached under the /mnt.

You can also using the **ftp** service and by Linux CLI (through SSH) copy the collected data to a remote location/IP address.

At the **System** menu, **Mount Points** you can check the connected drives and mounted file systems. You can **Unmount** a drive or (deteach) a file system if you don’t need it anymore.
5.9 RS485 Mbus meter connection

In case of using RS485 M-Bus connection note, that the device is able to receiv 1-250 connected MBus compatible meters.

All incoming data of the connected meters will be automatically stored under the /tmp directory on the RAM drive.

**Important! Note that, this is a temporary storage pool, where all stored data of the directory will be deleted after rebooting.**

Therefore, we suggest to use ftp or tftp, sftp client or server and make connection to upload the stored files to your distant server IP address before data loss – regarding the next setting options.
You can also use *SCP*-compatible connection to the router by your computer with an SCP client (like *WinSCP*). You can also copy the stored files to a locally mounted uSD drive for data collection or further data logging, analysis.

The incoming files of the Modbus device are stored here in CSV format by the following syntax in the CSV file:

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

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

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

**The M-Bus configuration in OpenWrt:**
You have to use *2019-09-20* or later firmware versions for MBus meter configuration where it is available.

After the firmware refresh, check the Services menu, MBus menu item at the MeterList part, where you can see the registered and discovered MBus compatible utility meters.
At first time the list is empty - it is normal. Now connect the meter and switch to the **Settings** tab. At the bottom of the page you will find the **Discovery** button - Push it to discover all connected meters. (You can **STOP Discovery** anytime if you need.)

At the end of the discovery process the previous list will be updated by the discovered meters.

Now here in the **Settings** tab, you can define the Mbus data connection parameters. This shown example is a basic configuration, but we can provide different fields and configuration options at MBus settings – according the Customer requirements. (If you have unique request, specify and send us).
At the Protocol you can select the FTP or SFTP protocol.

Configure the **IP address** of the remote (s)ftp server with **FTP port number** (port 21 is the default). The given IP address will be used in the file names.

It is necessary to use ftp **username** and **password** at the ftp server by the **targetDir** (e.g. /ftp/). Note, that these must be already existing and used at the distant server side!

You can declare an **Id** (identifier) for the concentrator connection with **reading** data periods (in seconds) and **sending** intervals (in seconds) – by (s)ftp.
The **reportid** means that you can use a logical identifier to when sending CSV file to the distant server. The filenames will contain this tag and the files will be identified such easy by this ID at the server side during reception of the files and evaluation of the data.

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

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

**Meter scan parameters:**

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

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

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

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

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

**5.10 SSH configuration**

In **System** menu, **Administration** submenu item, you will get the **SSH Access**, you can define the **Port** (standard port nr. 22) and **Interface** for the OpenSSH connection with required the authorization level – by **Password authentication** or not.

You can add rules for every **Interfaces**.

At the bottom of the screen, you can give the **SSH-keys** for each connection.
SSH Access
Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance

- Interface:
  - lan
  - usblan
  - wan
  - unspecified
- Port: 22
  - Listen only on the given interface or, if unspecified, on all
- Password authentication
  - Allow SSH password authentication
- Allow root logins with password
  - Allow the root user to login with password
- Gateway ports
  - Allow remote hosts to connect to local SSH forwarded ports

SSH-Keys
Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.
6. Troubleshooting

**LED activity**

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

Over 1-2 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 1-2 minutes, then check the LED signals again. If the **LED1..LED2..LED3** are not blinking or does not light then the device hasn’t got its power supply or it has some trouble. Connect the power source and if it does not helps, ask our support, please.

**In case of LED blinking after restart**

During the boot the **LED1** will lighting by green. After cca. 2 minutes, **LED1** will flashing once in every 10 seconds which means it is available on its local interfaces.

Then the router tries to connect to the mobile network (autenticates and logging to the APN zone and will be initiating the network connection) – if that was configured. Then the **LED2** will lighting continuously, which signs the successful modem network connection and the available ppp (**WAN**) connection.

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

**Which Power Adapter?**

Always use proper power adapter for the router (min. 10V DC is required, 12V DC 1A is recommended to use) with industrial standard 4-pins microfit connector.

**4-PIN connector (Power Input)**

![4-PIN connector diagram]

**Pin assignment of 4-pin connector**

<table>
<thead>
<tr>
<th>Pin number</th>
<th>Name</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>POWER -</td>
<td>DC power negative input</td>
</tr>
<tr>
<td>4</td>
<td>POWER +</td>
<td>DC power positive input</td>
</tr>
</tbody>
</table>
You can order a power supply from us, or buy one. Please consider the wiring and polarity, according to the previous figure of connector pinout. (Top 2-pins of the microfit plugin are wired only, the left pin is the negative.)

**No power?**
Check router that it can get any power through its microfit connector (POWER) – power adapter is connected to the router microfit connector and the adapter to the 230V AC plug.
When it receives 12V DC power, the LED signals will sign it: *all the three LEDs will light for a short period*, then the **LED1** (green) will light for 2 minutes, then after that only blinks once in every 10 seconds. The router is booting and just started.
(Wait for 1-2 minutes, while the router is registering to the wireless network then check the life signals).
In case of failure, check the power supply connection at the socket plug side and on the microfit connector at the router side. The top 2-pins of the microfit plugin are wired only, the left pin is the negative. Check the 12V DC voltage on the microfit connector (by a multimeter) of the power adapter that it provides 12V or not. If not, than remove the 12V DC adapter and get another one with the proper pinout and voltage.

**Ethernet connectivity**
Check or connect the RJ45 UTP6a type cable to the **ETHERNET** port. When the router is operating, the **Ethernet** port LEDs must sign the network activities.

**When you cannot access router through SSH or on its web interface**
The DHCP service is turned off for the router Ethernet interface, by default. Therefore, you have to configure an IP address for you PC, manually. Add fog e.g. 192.168.127.10 IP address to your computer’s Ethernet interface for connecting to the router. (For microUSB connection use the 192.168.10.1 address)
For accessing the web user interface we offer the Mozilla Firefox web.

Default web user interface (LuCi) address is: [https://192.168.127.1:8888](https://192.168.127.1:8888)
( USB web address: [https://192.168.10.1:8888](https://192.168.10.1:8888) )

- **Username**: root
- **Password**: wmrpwd
- then push to the **Login** button.
Allow the accessing of the router default IP address in your browser by pushing to the Special button, then allow the safety exclusion into the pop-up window.

**Checking the connection - connecting to the router through USB**

Download and install driver for USB connection from our website:

https://www.m2mserver.com/m2m-downloads/USB_Ethernet_RNDIS_DRIVER.zip

Unpack the downloaded zipped file and install the driver. After you’ve connected the USB cable you can add the driver at the Windows / Start / Control Panel / System / Device Manager. Find the **Network Cards**, extend it and you will found the „**USB Ethernet / RNDIS Gadget**”. Double click on the entry and choose the **Driver** tab, and the **Refresh** button, then browse the uncompressed file’s directory then **Install** the driver.)

Build a connection between the PC and the router with a micro-USB cable. (The driver must be installed on the PC – related the **Installation Manual**).

Configure the **USB-Ethernet interface** IP address on your PC for the „**USB Ethernet/RNDIS Gadget**” and setup the next fixed ipv4 address: 192.168.10.10, subnet mask is: 255.255.255.0 – connect these settings.

(You can ping the device through the USB connection on its IP address.)

**If the router is not starting**

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

**Periodic restart of the router (by 10 minutes periods)**

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

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

**Restart of the router**

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

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

Attention!

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

Antenna

Check or connect proper SMA fit antenna to the Antenna connector and mount it to the interface. The router must send and assure proper RSSI signal value and life signals.
Always use the antenna type regarding to the used module and mobile network, bandwidth. In case of using 4G connection and module, you need two 4G antennas (Main and Diversity). In case of using CDMA 450 or LTE 450 or Narrow Band – always use the special antenna which is harmonized to the frequency/band. In other way the router will not able to access the network. If you will receive 99 RSSI and CSQ signals during minutes, that means you have to use another antenna or move the antenna or the router for another position where you will get enough signal reception.

<table>
<thead>
<tr>
<th>Network</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem Model</td>
<td>ME910C1-E1</td>
</tr>
<tr>
<td>IMEI</td>
<td>35634508013401</td>
</tr>
<tr>
<td>SIM ID</td>
<td>89882390000052445353</td>
</tr>
<tr>
<td>Modem RSSI</td>
<td>99</td>
</tr>
<tr>
<td>Modem SQ</td>
<td>99</td>
</tr>
<tr>
<td>CREG</td>
<td>2,2</td>
</tr>
<tr>
<td>COPS</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 WAN Status</td>
<td>Not connected</td>
</tr>
<tr>
<td>IPv6 WAN Status</td>
<td>Not connected</td>
</tr>
</tbody>
</table>

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

Configure the **Ethernet interface** IP address on your PC where you can access it ([Control panel / Network / Network Adapter / Adapter settings](#)). Ping the router IP address.

**When the router will not started...**

Follow the hints of the Installation manual.

**No SIM card slot presented**

In case of the modern CDMA 450 network in many countries there is no need of usage of the SIM cards. The identification of the modules and the registration to the mobile network service is executing on a different way and method, therefore on the CDMA450 version or M2M Routers we are not providing SIM card slot by general. If your mobile network provider requires a SIM card upon this network, contact us before ordering.

**SIM ERROR**

If you get the SIM ERROR message in the Status/Overview menu (dashboard) at the **SIM ID value**, then your SIM card is inactive or has malfunction. Restart the router and try again.

Add valid **APN** settings in the **Interfaces / WAN** connection, **Save and apply** the settings and restart the router as soon as you can from the **System / Reboot** menu.

If it does not help, consult with your Mobile Operator and ask about the SIM availability and ask them about the network registration in their system (the mobile operator can check the module registration in their system).

**SIM-card (in case of 4G router only)**

Turn off the router. Check that a SIM card was inserted to the **SIM** holder in the proper position and orientation. Push the SIM card back and ask you Mobile Operator that the SIM card is active or not. Let’s start the router again and check it, please.

The SIM/APN troubles can be caused by the not proper settings of the **APN** – or **MSIN** (in case of CDMA450 version) – settings. You can setup and configure these from the router local website. The usable APN, password information are provided by your SIM card’s mobile operator.

**SIM/APN failure**

It means a SIM or APN failure, if the **LED2** will not light for minutes. If the device is not registering to the network, then the modem was not initiated properly, and the router will restart itself after 10 minutes.
This could caused by a not proper APN setting – or in case of CDMA version the wrong MSIN setting (you can configure it on the local web user interface).
7. Support availability

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

E-mail: support@wmsystems.hu

Telephone: +36 20 333 1111

7.1 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!
7.2 Product support

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

The documentation and software released for this product can be accessed via the following link:
https://www.m2mserver.com /en/support/

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

©2019. 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.