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, LTE 450 and NB versions of the modem types. All of the listed settings are similar for the modem versions.

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>WMR</td>
</tr>
<tr>
<td>Document version No.:</td>
<td>REV 1.93</td>
</tr>
<tr>
<td>Number of pages:</td>
<td>53</td>
</tr>
<tr>
<td>Hardware Identifier No.:</td>
<td>BE0077C_CMDA450_2016.04.14</td>
</tr>
<tr>
<td>OpenWRT build version:</td>
<td>2017-08-03</td>
</tr>
<tr>
<td>Firmware version:</td>
<td>2017-03-23</td>
</tr>
<tr>
<td>Document status:</td>
<td>Final</td>
</tr>
<tr>
<td>Compilation date:</td>
<td>26 April 2016</td>
</tr>
<tr>
<td>Last modified:</td>
<td>31 January, 2018</td>
</tr>
<tr>
<td>Approval date:</td>
<td>31 January, 2018</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 ............................................................... 5
   1.4 Web user interface of the router ............................................. 6
   1.5 Accessing the router on ssh connection ............................... 6

2. Web Administration user interface ............................................. 9
   2.1 Login ................................................................................... 10
   2.2 Main page (Dashboard) ......................................................... 11
   2.3 Menu .................................................................................. 11
   2.4 Status menu ....................................................................... 11
   2.5 CDMA menu (only for CDMA devices) ................................. 11
   2.6 System menu ..................................................................... 12
   2.7 Router menu ...................................................................... 13
   2.8 Network menu ................................................................... 13

3. Network configuration of the router ......................................... 14
   3.1 Interface settings ................................................................. 14
   3.2 Mobile internet settings (modem) ....................................... 16
   3.3 Ethernet (LAN) settings ...................................................... 20
   3.4 DHCP settings .................................................................. 23
   3.5 DNS settings ..................................................................... 25
   3.6 Defining the route rules ...................................................... 26
   3.7 Firewall settings ................................................................. 27
   3.8 Port Forward settings .......................................................... 31
   3.9 IP routing, NAT settings ..................................................... 32
   3.10 Dynamic DNS settings ...................................................... 33

4. Special settings ........................................................................ 34
   4.1 M2M Device Manager settings ............................................ 34
   4.2 Monitoring the modem ....................................................... 35
   4.3 Ping an IP address .............................................................. 35
   4.4 Network Time Service (NTP) ................................................. 36
   4.5 TFTP service settings .......................................................... 36
   4.6 Identifying names connecting machines ............................... 37
   4.7 LED configuration .............................................................. 38
   4.8 OpenVPN configuration ....................................................... 39
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, or CDMA 450 **SMA antenna** to the **Antenna** titled SMA-M interface (according to the module/router type).

   In case of 4G version router use two antennas.

2. **Insert an activated data SIM card** 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** chord 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 starting then takes about 1-2 minutes while it will be ready for usage which is signed by the light of the **LED2**. Then you can login to the web user interface.

4. The module and the mobile network registration process is signed by flashing of the **LED3**. When the SIM card network registration was successfully performed, the **LED2** lights continuously and the router has access to the mobile network and can transmit data.

5. **As soon as you can, configure the internet settings of the wireless module (SIM and APN) for connecting to the 2G/3G/4G LTE/LTE 450 network** – in other case the router will be restarted in every 10 minutes.

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)
Now, you can login to the router’s local website (LuCi interface) - through the Ethernet interface – accessing the default URL.

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
The login data are the following:

- **Username**: root
- **Password**: wmrpwd
- then push to the Login button.

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 ssh 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 appear in your command line on your computer.
1.6 Remote access and configuration of the router by the M2M Device Manager software

By optionally, you can use the central remote device management application (M2M Device Manager) for your router devices. Which provides continuous monitoring of the operation, remote configuration and remote firmware updates. The server application assures the opportunity to manage even thousands or routers and listening the network connections. Therefore you can configure, monitorize, refresh a bunch or group of routers, even as singular devices as well. The application is available through different license constructions, please advise our sales.

You can get further information on the M2M Device Manager website: http://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. Check that the *Build Date* (OpenWrt) is 2017-08-03 or newer version, and the *STM32 Firmware* version – which must be at least 2017-03-23 or newer.
At the **Network** part you can identify the **Modem model**, the modem identifier (**IMEI**), the SIM ICC identifier (**SIM ID**), and the **Modem RSSI** (signal strength) and **Modem SQ** (signal quality as 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.

### 2.3 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/restore 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

### 2.4 Status menu

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

The modem’s **MSIN identifier** can be configured here: **CDMA/Set MSIN**.

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.**

2.6 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** 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.

**2.7 Router menu**

• You can define the remote monitoring software connection settings of the az **M2M Device Manager**.
• 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** (saves to a file).

### 2.8 Services menu

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

### 2.9 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.
- At the **Diagnostics** item, you can test the network operation and connection health by the ping an IP address for the interfaces.
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 find 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.

![Interface settings](image)

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

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

APN name: net

**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 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 doing the SIM, APN settings, and saving the settings, the router and the modem will not be automatically restarted futhermore!*

---

### 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 end enabling the **roaming** settings – in **case of international or country border usage** – you may need to setup the **Mobile country code** and **Mobile network code** parameters – even if you are attempted to use only a prefered mobile network.
The international country codes can be found here: [http://mcc-mnc.com](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 (opened)**
APN name: net

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

**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 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 doing the SIM, APN settings, and saving the settings, the router and the modem will not be automatically restarted furthermore!

---

**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 you 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, DHCP and DNS item.

DHCP Server

<table>
<thead>
<tr>
<th>General Setup</th>
<th>IPv6 Settings</th>
</tr>
</thead>
</table>

- Ignore interface
- Disable DHCP for this interface

---

**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).

DHCP Server

<table>
<thead>
<tr>
<th>General Setup</th>
<th>Advanced Settings</th>
<th>IPv6 Settings</th>
</tr>
</thead>
</table>

- Ignore interface
- Disable DHCP for this interface
- **Start**
- **Limit**
- **Leasetime**

---

Save & Apply  Save  Reset
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 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 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.

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 in the router).

**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.*

If will you identify communication from an unwanted IP/port, then you have to disable or limit the occured 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.

![Firewall Status](image)

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 edit or delete 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.
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.

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 **Add** by the button or the current can be **Edit**-ed.

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

4.1 M2M Device Manager settings

The further router parameters can be easily and remotely configured by the az M2M Device Manager® server application. It is also capable of performing remote monitoring and 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 M2M Device Manager. You can check it by performing a ping.

When 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.

![Modem Parameters](image)

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**).

![Diagnostics](image)
**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.

### 4.4 Network Time Service (NTP)

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**.

- **General**
  - Current system time: Tue Dec 5 15:34:24 2017
  - Update interval (in seconds): 500
  - Count of time measurements: 0

- **Clock Adjustment**
  - Offset frequency: 0

- **Time Servers**
  - Hostname: 0.openwrt.pool.ntp.org, Port: 123
  - Hostname: 1.openwrt.pool.ntp.org, Port: 123
  - Hostname: 2.openwrt.pool.ntp.org, Port: 123
  - Hostname: 3.openwrt.pool.ntp.org, Port: 123

![M2M-Router interface](image_url)

**Save & Apply**
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.

You can [Delete] the LED setting.

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](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 the 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.

By sake of the proper advanced 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
### Service

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>verb</td>
<td>Set output verbosity</td>
</tr>
<tr>
<td>mlock</td>
<td>Disable Paging</td>
</tr>
<tr>
<td>disable_ecn</td>
<td>Disable options consistency check</td>
</tr>
<tr>
<td>passtos</td>
<td>TOS passthrough (applies to IPv4 only)</td>
</tr>
<tr>
<td>suppress_timestamps</td>
<td>Don't log timestamps</td>
</tr>
<tr>
<td>fast_io</td>
<td>Optimize TUN/TAP/UDP writes</td>
</tr>
<tr>
<td>down_pre</td>
<td>Call down cmd/script before TUN/TAP close</td>
</tr>
<tr>
<td>up_restart</td>
<td>Run up/down scripts for all restarts</td>
</tr>
<tr>
<td>client_disconnect</td>
<td>Run script cmd on client disconnection</td>
</tr>
</tbody>
</table>

---

[Add Additional Field]
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.

5. Later the **LED2** will blank and 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!

### 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 exchange
Open the **System / Administration** menu.
At the **Router password** you can fill the new **Password** and again to the **Confirm password** fields. You will be able to login further by this new password.

The default account is **root**, the default pass is **wmrpwd**

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 ** Generate archive ** 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 a memory card

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.
6. Troubleshooting

**LED activities**

Can you see a LED signal activity? It is not sure that after 1-2 minutes of LED inactivity it must mean a failure. It is possible that the router is currently under restart progress or it has just booting. Wait 2-3 minutes, then check the LEDs. If the **LED1..LED2..LED3** are not blinking or light then the device hasn’t got its power supply or the device has damaged, or it has a malfunction.

**In case of LED blinking after restart**

After cca. 2 minutes of the the router starting the **LED1** must not light and the **LED3** starts to blinking in green. The router tries to connect to the mobile network (autenticates and logging to the APN zone and will be initiating the network connection). The **LED3** blinking will be finished within 1-2 minutes and the **LED2** will light continuously, which signs the successful modem network connection and the available ppp (WAN) connection. *(Attention! in case of the 4G version, the **LED2** will not light after the connection).*

The device is communicating on the network and will send a couple of minutes later proper **RSSI** values and life signals. During the operation, the **LED1** will blinks once in every 10 seconds. This means the normal operation of the router.

**Power supply**

Check that the router that it has its power source through its microfit connector (**POWER**). If it does not, then reconnect the power cable. When it has its power source the LED signals will sign it. In this case please wait for 2-3 minutes, while the router will register to the network then check the life signals in the **Element Manager**. *When the power source will be added, 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.*

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 on the microfit connector of the power adapter that it provides 12V power supply or not. If it is not providing, remote the 12V DC adapter and get an other one with the proper pinout.
Ethernet connection
Check or connect the RJ45 UTP cable to the Ethernet port. When the router is operating, the Ethernet port LEDs must sign the network activities.

When can not access the 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 your PC, manually. Add for e.g. 192.168.127.10 IP address to your computer’s Ethernet interface for connecting to the router.
(If you have the WiFi onboard version of the router, then you can configure your router on WiFi (DHCP activated).
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
- 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 the driver for the mini USB cable connection from the M2M website before using the connection:
http://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!

**Cyclical restarting 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.

**Restarting of the router**
If the router is not responding somehow, let’s restart it with disconnecting the power cable then connect it again (**POWER** port).

**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!**

**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 for the **Element Manager**. Always use a antenna type regarding to the used module and mobile network, bandwith. In case of using 4G connection and module, you need a 4G antenna, in case of CDMA 450 or LTE 450 a
450MHz antenna. In other hand the router cannot access the network or can operating only on the accessible frequency bands.

**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-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 your 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 useable 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@m2mserver.com

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:

http://www.m2mserver.com/en/products/m2m-router

The documentation and software released for this product can be accessed via the following link:

http://www.m2mserver.com/en/support/

Online product support can be required here:

http://www.m2mserver.com/en/support/
8. Legal notice

©2018. 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.