

WM-E LCB[®]

Load Control Box

User Manual

v1.00



2022-05-02

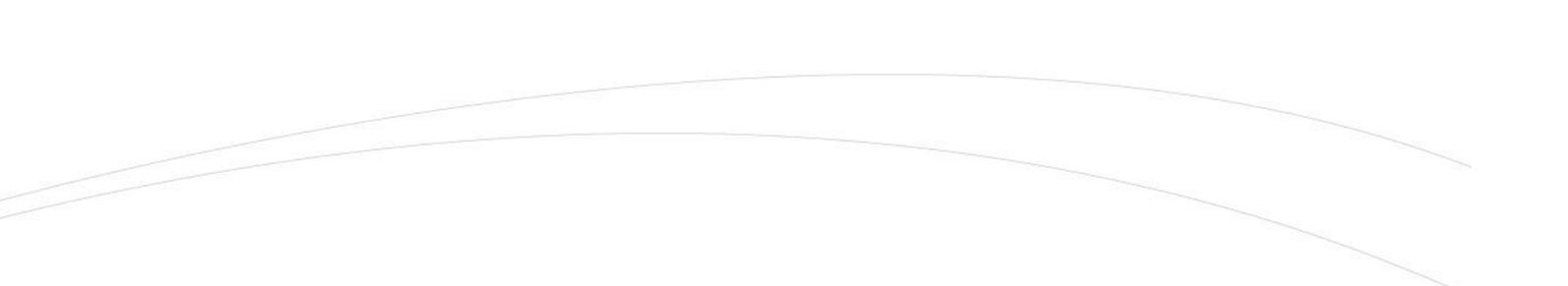
Document specifications

This document was made for the **WM-E LCB[®] Load Control Box** device and it contains the detailed description of the configuration possibilities for the proper operation of the device.

Document category:	User Manual
Document subject:	WM-E LCB [®]
Author:	WM Systems LLC
Document version No.:	REV 1.00
Number of pages:	60
Hardware version:	BE0080B
Linux Kernel:	4.9.184
Bootloader version:	20180522
Microcontroller firmware:	20170914
OpenWRT software version:	202204281_RC
Document status:	FINAL
Last modified:	2 May, 2022
Approval date:	2 May, 2022

Table of contents

CHAPTER 1. DEVICE CONFIGURATION (OPENWRT USER INTERFACE)	5
1.1 Web user interface	5
1.2 Dashboard (Main page)	6
1.3 Menu overview	8
1.4 Status menu	8
1.5 System menu	9
1.6 Router menu	9
1.7 Services menu	10
1.8 Network menu	10
CHAPTER 2. IMPORTANT NOTES	11
CHAPTER 3. NETWORK CONFIGURATION	13
3.1 Interface settings	13
3.2 Cellular internet (WAN) settings	13
3.3 Ethernet (LAN) settings	17
3.4 DHCP and DNS settings	18
3.5 Defining route rules (Static routes).....	21
3.6 Firewall settings	22
3.7 Port Forward settings	26
3.8 NAT settings	26
CHAPTER 4. ADVANCED SERVICES	29
4.1 Ping IP address / checking IP	29
4.2 Network Time Service (NTP)	29
4.3 Identifying and connecting computers	31
4.4 TFTP settings.....	31
4.5 Ser2net (RS485 settings).....	33
4.6 Relay switch settings.....	35
4.7 LED configuration	36
4.8 Using the UCI Command Line Interface	37
4.9 IPSEC settings	37
4.10 Voice call configuration.....	40
4.11 Run commands remotely (SMS config settings).....	41



CHAPTER 5. MAINTENANCE	43
5.1 Firmware refresh	43
5.2 Restarting the device.....	45
5.3 Turn off the device.....	45
5.4 Backup device settings	46
5.5 Restore device settings.....	48
5.6 Clone config backup/restore	48
CHAPTER 6. ADMINISTRATION	50
6.1 Password change	50
6.2 Logging	51
6.3 Language settings	51
6.4 Periodic reboot settings	52
6.5 Periodic ping	52
6.6 Installing 3rd party applications	53
6.7 SSH access	54
6.8 Device Manager settings.....	55
CHAPTER 7. TROUBLESHOOTING	57
CHAPTER 8. SUPPORT	58
CHAPTER 9. LEGAL NOTICE	60

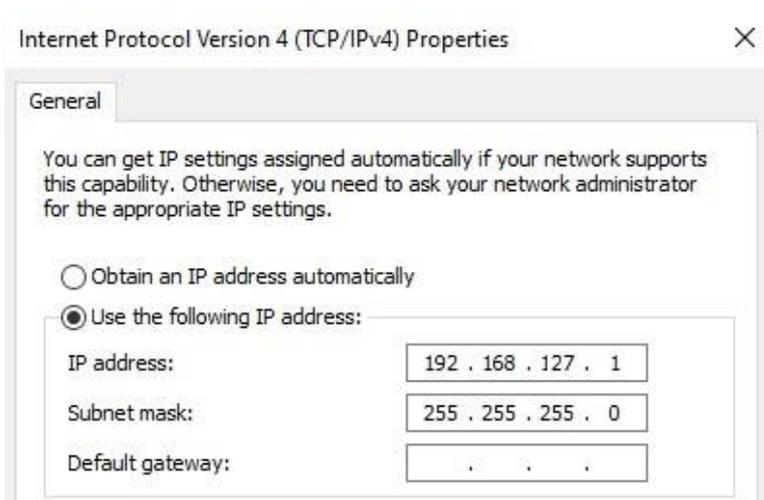
Chapter 1. Device configuration (OpenWrt user interface)

1.1 Web user interface

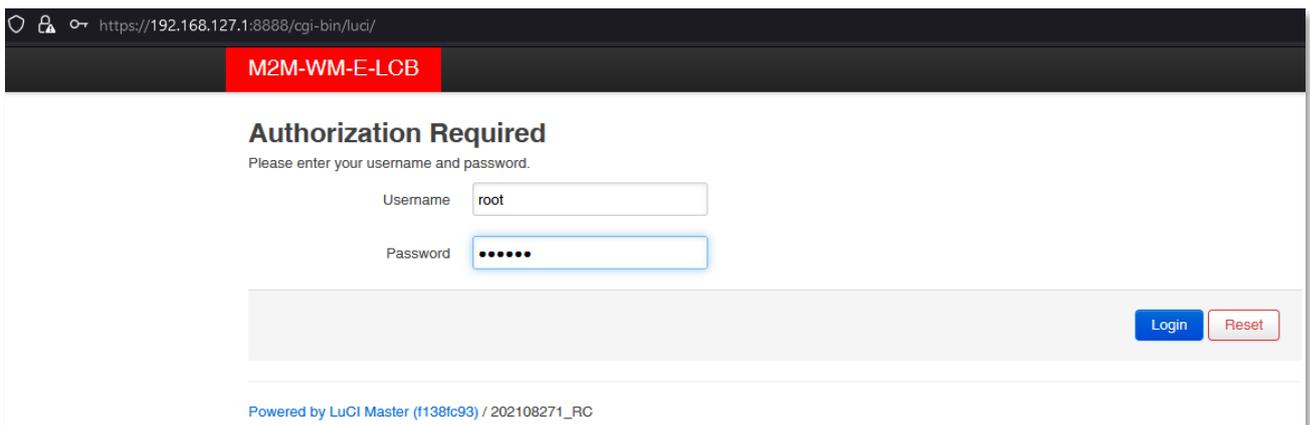
Important!

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

1. Configure the **Ethernet** interface's on your PC for TCP/IPv4 protocol for setup the **IP address: 192.168.127.100** and **subnet mask: 255.255.255.0**



2. Start the device. The local web user interface (LuCi®) will be reachable after 1-2 minutes through the **Ethernet (LAN)** interface – on the device's default IP address in a web browser.
3. Open the device's local website in the **Mozilla Firefox** browser, where the default web user interface address on **Ethernet** port is: <https://192.168.127.1:8888>
Login with the **Username: root**, **Password: wmrpwd** and push to the **Login** button.



1.2 Dashboard (Main page)

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

At the **System** part, you can check the installed software build (**Firmware Version**) where it should be **202108271_RC** or newer. (If it has an older version, then refresh the firmware, please.)

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

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

M2M-WM-E-LCB Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout AUTO REFRESH ON

Status

System

Hostname	M2M-WM-E-LCB
Model	WM-E_LCB
Firmware Version	202108271_RC
Architecture	ARM926EJ-S rev 5 (v5l)
Build Date	2021-08-27 16:09:09.062586533+00:00
Kernel Version	4.9.184
STM32 Firmware	201709141
Local Time	Sat Jan 1 00:06:03 2000
Uptime	0h 5m 59s
Load Average	0.36, 0.38, 0.20

Memory

Total Available	<div style="width: 73%;"><div style="width: 73%;"></div></div> 89.88 MB / 122.18 MB (73%)
Free	<div style="width: 70%;"><div style="width: 70%;"></div></div> 85.71 MB / 122.18 MB (70%)
Buffered	<div style="width: 3%;"><div style="width: 3%;"></div></div> 4.17 MB / 122.18 MB (3%)

Modem

Modem Model	LE910C1-EU
Firmware Version	M0F.220006
MEID	355001096340392
SIM ID	8936200003250172672

At the **Modem** part, first you can the module's **MEID** identifier (IMEI) and the **SIM ID** identifier of the used SIM card.

You can also check the wireless modem availability, current status and health at **Modem RSSI** (cellular network signal strength) and **Modem SQ**. (The lower RSSI means better cellular signal strength / higher SQ value means the better signal quality level).

At the **CREG** field you can get more info about the used cellular network cells. The **COPS** shows the connected network name.

Modem

Modem Model	LE910C1-EU
Firmware Version	M0F.220006
MEID	355001096340392
SIM ID	8936200003250172672
Modem RSSI	12
Modem SQ	2
CREG	2,1,"1204","FB8D7F",2
COPS	1,0,"Telenor HU",2

Network

IPv4 Upstream

Protocol: PPP-4G
Address: 84.224.125.172
Netmask: 255.255.255.255
Gateway: 10.64.64.64
DNS 1: 217.79.129.75
DNS 2: 217.79.128.45
Connected: 0h 9m 40s

Device: Tunnel Interface: "4g-wan"

Active Connections 9 / 16384 (0%)

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
<i>There are no active leases.</i>			

Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
<i>There are no active leases.</i>			

At the **Network** part, you can see the used cellular network IP address at the **Address field**.

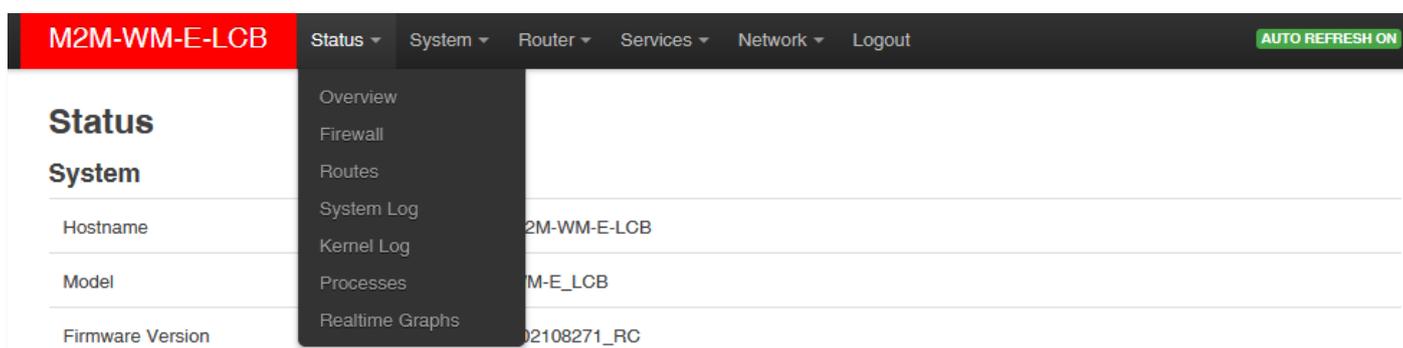
1.3 Menu overview

By the menu you can access the following features:

- **Status** – Status data, operation Logs (system, kernel, event log), Firewall monitoring, monitoring the operation (at *Processes* and *Realtime graphs*)
- **System** – System settings and administration (time sync, device name), software installation (3rd party tools), Startup settings and scheduled tasks, LED configuration, Firmware flashing, Backup/Restore of the configuration settings, Reboot of the system)
- **Router** – Device manager configuration, Modem settings and Logging parameters, Periodic ping and reboot, Factory configuration, Relay switch settings
- **Services** – Ser2net (RS485 configuration)
- **Network** – Network interface settings (for Ethernet and cellular module), DHCP, DynDNS, IP route/NAT, hostname, diagnostics, Firewall, IPSEC settings, voice call settings (remote reboot) and SMS configuration (remote command execution)
- **Statistics** – System graphs and statistics settings
- **Logout** – Logout and login with a different user

1.4 Status menu

- In the **Status** you can check the current status (**Overview**).



- Check the **Firewall** traffic.
- Check the **Routes**.
- Check system messages and event log (**System Log**, **Kernel Log**).
- Check the activities of the device (**Processes**).
- You can find monitoring features of the realtime operation at the **Realtime Graphs**.

1.5 System menu

- You will find several system settings in the **System** menu (as **Hostname**, **Time synchronisation** (NTP), **Logging** and **Language** settings)
- And in the **Administration** menu also (**Password change** and **SSH Access**).
- **Clone config backup/restore** for easy cloning of the saved settings to another device.
- Installation of further **Software** (3rd party tools, applications for the Linux distribution).
- You can define the **Startup** applications.
- Initialization of programs can be configured during the operation and the **Scheduled Tasks**.

The screenshot shows the web interface for M2M-WM-E-LCB. The top navigation bar includes 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. The 'System' menu is expanded, showing options: System, Administration, Clone config backup/restore, Software, Startup, Scheduled Tasks, LED Configuration, Backup / Flash Firmware, and Reboot. The main content area displays system information:

Status	
Hostname	GB
Model	
Firmware Version	C
Architecture	rev 5 (v51)
Build Date	2018-09-09.062586533+00:00

- The **LED Configuration** is also configurable for custom needs.
- You also can **Backup** and restore your system configuration, applying **Flash firmware** updates.
- **Reboot** menu: for restarting the device.

1.6 Router menu

- **Device Manager** settings can be configured for remote device checking and managing from the Device Manager[®] software.
- **Modem Parameters** – watchdog settings for the cellular module.

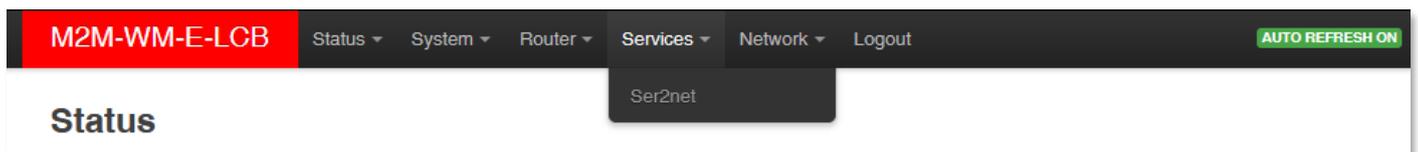
The screenshot shows the web interface for M2M-WM-E-LCB. The top navigation bar includes 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. The 'Router' menu is expanded, showing options: Device Manager, Setting, Modem Parameters, Logging Parameters, Periodic Ping, Periodic Reboot, Factory Configuration, and Relay Switch. The main content area displays system information:

Status	
Hostname	
Model	
Firmware Version	
Architecture	ARM926EJ-S rev 5 (v51)

- **Logging Parameters** – you can setup the log mode.
- Define **periodic ping** (for QoS check) or **periodic reboot** (for industrial standard or safety reasons).
- **Factory Configuration** – save the last good known settings or reload the factory settings
- **Relay Switch** – Relay output settings (configure the control of lighting units / switches)

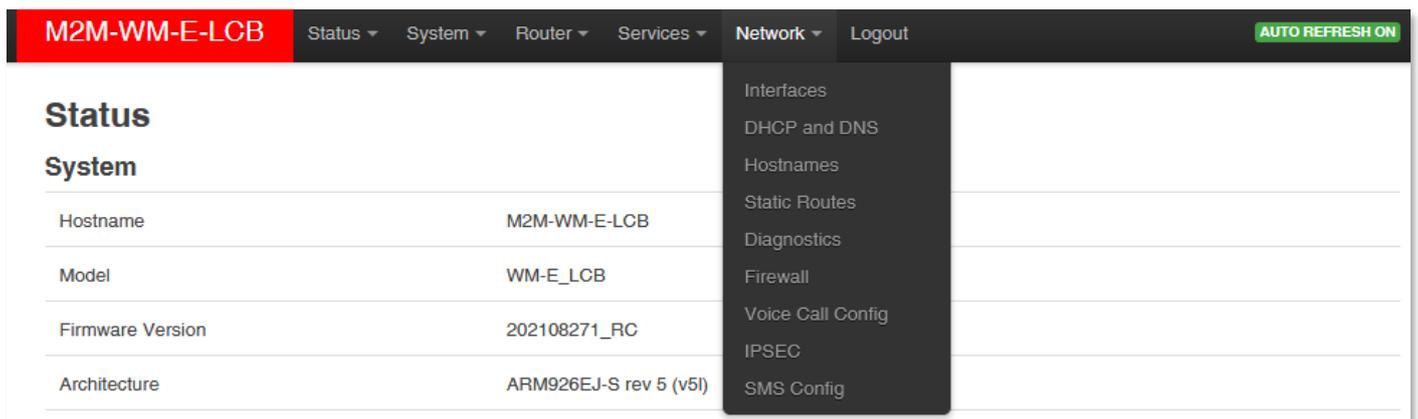
1.7 Services menu

- **Ser2net** – RS485 port settings



1.8 Network menu

- Here are the settings of each network **Interfaces** (for cellular module and Ethernet port)
- You can define the **DHCP and DNS** settings for the wireless LTE module and connection.



- Define **Hostname** for the modem for easier identification of the device on your network.
- At the **Static Routes** are also configurable (IP route settings).
- At the **Diagnostics** menu, you can check network access (ping, traceroute, nslookup).
- **Firewall** settings for control and rule the incoming and outgoing, throughput communication.
- The **Voice Call Config** menu is usable for remote control of the device (e.g. remote restart) – command execution by voice call
- **IPSEC** (tunneling settings for secure connections)
- At the **SMS Config** menu you can define (remotely executable commands) – execution by SMS messages

Chapter 2. Important notes

- By security reasons, we do recommend to **change the web user interface login and password** as soon as you can.
- The **IPv6 protocol** is disabled for the LAN interface by default, change it if you want to use it instead of the IPv4 protocol. Use the **Network / Interfaces** menu **LAN** interface and the IPv6 relevant fields.
- The DHCP service is active, therefore the device will giving IP addresses for the connected devices, but the protocol which is used, configured for static IP addresses for the ethernet interfaces. If you want to use and distribute IP addresses by DHCP, change its protocol to DHCP client. You can change its settings in the Network / DHCP and DNS settings menu or in the **Network / Interfaces** menu, **LAN** interface and **DHCP** section.
- The **Firewall** service is active by default (by security reasons), therefore all communication is disabled excluding the used ethernet, DHCP, DNS and WAN channels, web port and the necessary services and ports for normal operation for the modem.
- We recommend you to disable all ports and protocols in the firewall which you are not using actively or which are not necessary to the connection and data transmitting by respecting the ports which are necessary for the general operation. Use to check **Status / Firewall** menu to check the data throughput and the **Network / Firewall** to configure new roles.
- The **firewall is not protecting the device against external network or DoS attacks**, if you just enable the firewall feature. For a massive and advanced safety, you have to customize the settings by harmonized with you used current network and connection settings.
- We offer to **check the network traffic** on your modem frequently by the **Status / Firewall** menu option to be ensured that all of your connections and active communication channels (port number, incoming IP) are using only the wanted paths and routes and listening the defined incoming activities and consequently occurring the estimated output traffic.
- We offer to **measure your throughput data and network traffic** (by minutes, hours) – use the **Status / Realtime Graphs** or **Statistics / Graphs** and calculate the estimable data transmitting amount according your expectations and the data limits of the used SIM card.
- By default, the modem has an installed OpenWRT® operating system which is ready to use and configure to your SIM card APN and for you usage requirements.

- The device has 4G LTE wireless transmission capabilities and 2G/3G fallback in case of the unavailability of the 4G network. In this case, the device will operating on the 3G or 2G network. When the 4G network will be available again, the device will switch back to the 4G network. This feature is configurable for the **WAN** interface of the device.
- You can check the current cellular signal reception and wireless availability in the *OpenWRT® / LuCI® system's Overview* menu.
- The available APN settings will be assured by the SIM card provider mobile operator or your mobile internet service provider. Ask them about **APN**, password, **SIM PIN** and further necessary information for the configuration.
- If you want to use the device on the wired network (LAN) with RS485 option, then remove the **WAN** interface by the **Delete** button in the **Network / Interfaces** menu. The device will not be restarted further - even if there is no SIM card inserted.
- The **RS485** port should be configured before usage, which can be found in the **Services / Ser2net** menu. There you can configure RS485 data speed rate between 300 baud and 115 200 baud, but please consider that max. 19 200 baud is guaranteed to receive by the device. Note, that we offer to use **9 600 baud** or **2 400 baud** speed rate, which is standard and there can be guaranteed that it will work. With higher data speed rates some connected systems can cause loss of characters/data in case of some connected device(s).
- Note that the device is not detecting the relay connections, it is just signaling the relay switch by the **REL.1..4** LEDs. The compatibility settings should be done at the **Router / Relay Switch** menu.
- Note that all relays are latching relays, which means the device remains the last switching status (even if the power was taken). The **Relay 1** and **Relay 2** having NC, NO, COM pins (and it has two switching mode, where the SET and RESET are also available) while the **Relay 3** and **Relay 4** having only NC and COM pins (does not have RESET, just SET).
- Note, that the device has supercapacitor component inside, which protects the device against possible shorter power outages. In case of a power outage - due to the supercapacitors – the device has enough enegy to provide a safe disconnection and shutdown (before the supercaps will be exhausted). The same if you store the device for months without connecting a power source or using it. Therefore, this component must be charged before usage. When powering the device, the charge of the supercapacitors will be started automatically. The system will be started by the device only after the end of the charge process.

Chapter 3. Network configuration

3.1 Interface settings

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

The screenshot shows a web interface for network configuration. At the top, there is a navigation bar with the device name 'M2M-WM-E-LCB' and menu items: Status, System, Router, Services, Network, and Logout. An 'AUTO REFRESH ON' button is in the top right. Below the navigation bar, there are tabs for 'LAN' and 'WAN'. The main section is titled 'Interfaces' and contains two interface cards. The first card is for the 'LAN' interface (eth0), which is currently selected. It shows a protocol of 'Static address', an uptime of '1h 1m 41s', a MAC address of '6E:F4:13:82:82:38', and traffic statistics: RX: 750.28 KB (6789 Pkts.) and TX: 1.38 MB (6766 Pkts.). The IPv4 address is '192.168.127.1/24'. Action buttons for 'Restart', 'Stop', 'Edit', and 'Delete' are visible. The second card is for the 'WAN' interface (4g-wan), showing a protocol of 'PPP-4G', an uptime of '0h 60m 55s', a MAC address of '00:00:00:00:00:00', and traffic statistics: RX: 16.02 KB (303 Pkts.) and TX: 15.08 KB (251 Pkts.). The IPv4 address is '84.224.125.172/32' and it includes the note 'Information: Not started on boot'. Action buttons for 'Edit' and 'Delete' are visible. At the bottom left, there is a button labeled 'Add new interface...'. At the bottom right, there are buttons for 'Save & Apply', 'Save', and 'Reset'.

The **LAN** interface is listed for configuring and using the device with your PC or an external device through the Ethernet connection (*eth0* interface).

The **WAN** interface means the wireless Internet connection (as *4g-wan*) the physical 4G cellular module.

Modifying the interface settings

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

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

3.2 Cellular internet (WAN) settings

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

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

M2M-WM-E-LCB Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout AUTO REFRESH ON

LAN WAN

Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

General Setup | Advanced Settings | Firewall Settings

Status  **Device:** 4g-wan
Uptime: 1h 3m 15s
MAC: 00:00:00:00:00:00
RX: 16.66 KB (318 Pkts.)
TX: 15.49 KB (261 Pkts.)
IPv4: 84.224.125.172/32

Protocol: PPP-4G ▾

Disable modem:

Wireless network: No Change ▾

NB:

Mobile country code:

Mobile network code:

Dual SIM:

SIM #1 APN: net

PIN: *

SIM #1 PAP/CHAP username:

SIM #1 PAP/CHAP password: *

WAN->LAN port forwarding:
📍 hostip1:port1,hostip2:port2,...

Dial number: *99***1#

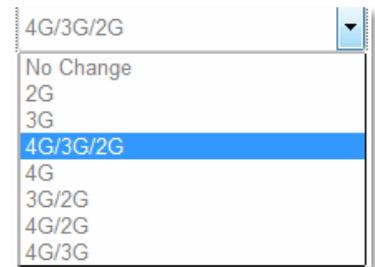
[Back to Overview](#) [Save & Apply](#) [Save](#) [Reset](#)

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

The device detects the 4G module and configuring. You only have to setup the **APN** you want to use for the **WAN** (*ppp-4g*) interface and the **PIN** code of the SIM (if it is presented).

The **Wireless Network** field gives you the opportunity to choose a dedicated cellular technology or you can leave it on default value: *4G/3G/2G* – which means the **Auto** mode.

This mode could grant the best speed and quality option (for *4G* selection), or the guaranteed operation on any network (*fallback* feature for *4G/3G/2G* selection (when the 4G cellular network service is not available the 3G will be used – if 3G is not available, or 2G fallback will be used – when 3G or 4G will be available again, it will switch back to 4G) – **if the internet module of the device's supporting this.**



If you have to use a dedicated network like 3G, 2G, etc., then choose the required network type, please. But **take consider, that the „fallback“ feature will be inactive in this mode** – if you choose the *4G* and it the network will be not available, there will not be provided 3G or 2G fallback (if the chosen network is not available, the device won't get mobile network access). For fallback always choose the **Auto** mode (*4G/3G/2G* setting).

If you choose the **No change** option, the device will be using the last known good configuration here.

There you can also define the **SIM #1 APN** name for the Internet connection, which is necessary to use. **If you will not set any value** for the *APN*, the modem will restart the modem sequentially in every ca. 10 minutes until it is not configured properly.

You can define SIM card's **PIN** code here - if it is necessary for the connection.

Note, that the **PIN** code which is already configured here, it cannot be seen here due to the security rules – the characters are placed by asterix signs. Just modify the PIN if you would like to change.

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

Authentication methods:

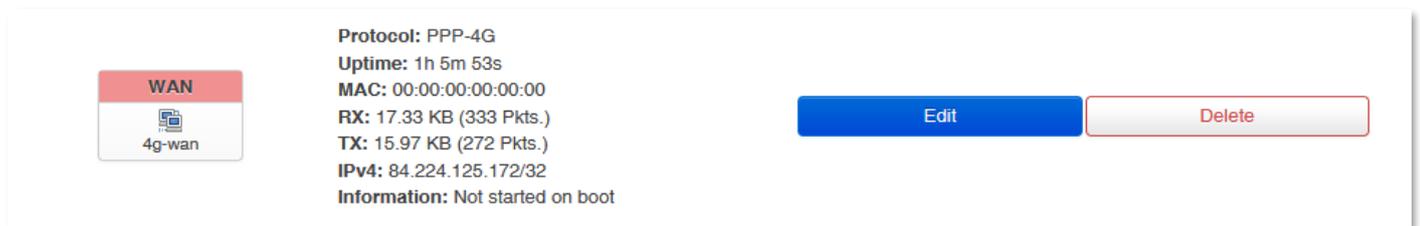
- The **SIM #1 PAP/CHAP username** and **SIM #1 PAP/CHAP password** settings can be also configured here – if it is required for the connection.

- If you need dialup connection for using the Internet service at your provider, set the **Dial number** value (format: *99***1#).

In case of roaming change the **Mobile country code** (MCC) settings to the related country code please. If you are attempting to use a dedicated cellular network, configure the MNC field (**Mobile network code**) please, according the needs. You will found the currently useable MCC / MNC settings here: <https://mcc-mnc-list.com/list>

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

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



The screenshot shows the WAN interface configuration page. On the left, there is a card for the WAN interface with a red header and a '4g-wan' icon. To the right of the card, the following information is displayed: Protocol: PPP-4G, Uptime: 1h 5m 53s, MAC: 00:00:00:00:00:00, RX: 17.33 KB (333 Pkts.), TX: 15.97 KB (272 Pkts.), IPv4: 84.224.125.172/32, and Information: Not started on boot. On the far right, there are two buttons: a blue 'Edit' button and a red 'Delete' button.

The device is already connected to the cellular network, it has active data traffic and the **RX** (received data), **TX** (transmitted data) at **Pkts.** (number of network packets) and **KB** (KBytes) values are growing.

The **WAN** interface data traffic will be signed by the **red** flashing of the **WAN** LED (together with the **green** flashing of the **LAN**) – which all can be indentified as **yellow**.

At the **Advanced Settings** tab you will found further settings for the wireless module.

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

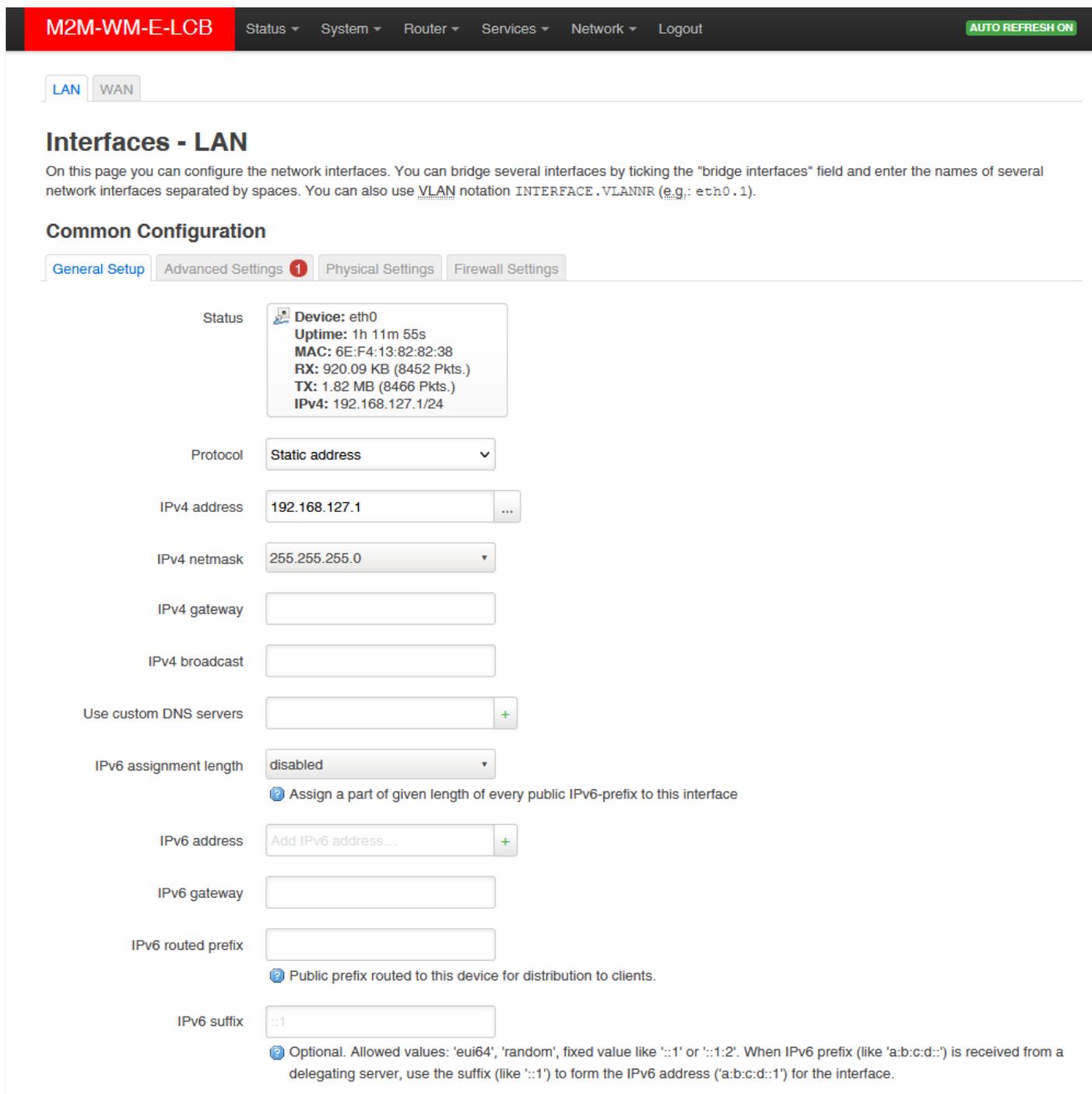
If you changed the configuration here, click upon **Save & Apply** button for saving the settings. Then the device will reconnecting the module to the mobile network.

3.3 Ethernet (LAN) settings

The detailed interface settings for the **LAN** Ethernet port (*eth0*) can be performed by selecting the **Network / Interfaces** menu item.

At the **LAN** interface's  button, choose the **General Setup** tab.

By default the Ethernet IP address is *static*, the default IP address is: 192.168.127.1). If you want to switch the **LAN** (*eth0*) interface to *dynamic* (at **Protocol** field), then the device will waiting for an IP address on the network.



The screenshot shows the Mikrotik WinBox interface for configuring the LAN interface (eth0). The top navigation bar includes 'M2M-WM-E-LCB', 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout', along with an 'AUTO REFRESH ON' button. The main content area is titled 'Interfaces - LAN' and contains a description of the page's purpose. Below this is the 'Common Configuration' section, which is currently on the 'General Setup' tab. The configuration fields are as follows:

- Status:** Device: eth0, Uptime: 1h 11m 55s, MAC: 6E:F4:13:82:82:38, RX: 920.09 KB (8452 Pkts.), TX: 1.82 MB (8466 Pkts.), IPv4: 192.168.127.1/24
- Protocol:** Static address
- IPv4 address:** 192.168.127.1
- IPv4 netmask:** 255.255.255.0
- IPv4 gateway:** (empty)
- IPv4 broadcast:** (empty)
- Use custom DNS servers:** (empty)
- IPv6 assignment length:** disabled
- IPv6 address:** Add IPv6 address...
- IPv6 gateway:** (empty)
- IPv6 routed prefix:** (empty)
- IPv6 suffix:** ::1

Helpful information for IPv6 settings:

- Assign a part of given length of every public IPv6-prefix to this interface
- Public prefix routed to this device for distribution to clients.
- Optional. Allowed values: 'eui64', 'random', fixed value like '::1' or '::1:2'. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like '::1') to form the IPv6 address ('a:b:c:d::1') for the interface.

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

When changing the **Protocol** field, you need to push the  button.

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

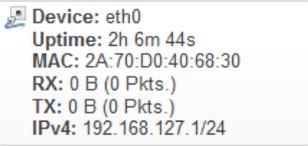
[LAN](#) [USBLAN](#) [WAN](#)

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

[General Setup](#)

Status	 Device: eth0 Uptime: 2h 6m 44s MAC: 2A:70:D0:40:68:30 RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) IPv4: 192.168.127.1/24
Protocol	DHCP client 
Really switch protocol?	

Save your settings by the **Save & Apply** button, and the **LAN** interface IP address will be changed according your request due to the new settings.

3.4 DHCP and DNS

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

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

DHCP Server

[General Setup](#) [IPv6 Settings](#)

Ignore interface
 Disable DHCP for this interface.

[Back to Overview](#)

[Save & Apply](#)

[Save](#)

[Reset](#)

To enable DHCP, uncheck the **Ignore interface** option. The fields required for DHCP configuration and their default values are displayed.

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

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

DHCP Server

[General Setup](#) [Advanced Settings](#) [IPv6 Settings](#)

Ignore interface

Disable DHCP for this interface.

Start

Lowest leased address as offset from the network address.

Limit

Maximum number of leased addresses.

Lease time

Expiry time of leased addresses, minimum is 2 minutes (2m).

[Back to Overview](#) [Save & Apply](#) [Save](#) [Reset](#)

Further settings can be achieved at the [Advanced Settings](#) tab (as dynamic DHCP, *IPv4 Netmask*). Save your settings with the [Save & Apply](#) button.

DHCP Server

[General Setup](#) [Advanced Settings](#) [IPv6 Settings](#)

Dynamic DHCP

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

Force

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

IPv4-Netmask

Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options [+](#)

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

[Back to Overview](#) [Save & Apply](#) [Save](#) [Reset](#)

DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

[General Settings](#) [Resolv and Hosts Files](#) [TFTP Settings](#) [Advanced Settings](#)

Domain required	<input checked="" type="checkbox"/>	<input type="radio"/> Don't forward <u>DNS</u> -Requests without <u>DNS</u> -Name
Authoritative	<input checked="" type="checkbox"/>	<input type="radio"/> This is the only <u>DHCP</u> in the local network
Local server	<input type="text" value="/lan/"/>	<input type="radio"/> Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only
Local domain	<input type="text" value="lan"/>	<input type="radio"/> Local domain suffix appended to DHCP names and hosts file entries
Log queries	<input type="checkbox"/>	<input type="radio"/> Write received DNS requests to syslog
DNS forwardings	<input type="text" value="/example.org/10.1.2.3"/> +	<input type="radio"/> List of <u>DNS</u> servers to forward requests to
Rebind protection	<input checked="" type="checkbox"/>	<input type="radio"/> Discard upstream RFC1918 responses
Allow localhost	<input checked="" type="checkbox"/>	<input type="radio"/> Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services
Domain whitelist	<input type="text" value="ihost.netflix.com"/> +	<input type="radio"/> List of domains to allow RFC1918 responses for
Local Service Only	<input checked="" type="checkbox"/>	<input type="radio"/> Limit DNS service to subnets interfaces on which we are serving DNS.
Non-wildcard	<input type="checkbox"/>	<input type="radio"/> Bind dynamically to interfaces rather than wildcard address (recommended as linux default)
Listen Interfaces	<input type="text"/> +	<input type="radio"/> Limit listening to these interfaces, and loopback.
Exclude interfaces	<input type="text"/> +	

Further DHCP server settings can be found in the **Network / DHCP and DNS** menu. Here you can see and configure them under the **General Settings** tab.

At the **Static Leases** you can add network devices by the button to be guaranteed to get the same IP address after every lease time renewal. Define a **Hostname** and the valid **MAC-Address** of the device and the required **IPv4-Address**.

Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	DUID	IPv6-Suffix (hex)	
<input type="text"/>	-- Please choose --	-- Please choose --	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>						

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

3.5 Defining route rules (Static route)

The current IP Route settings can be checked in the **Status / Routes** menu. We offer to check the currently used route rules - ARP routes, and the IPv4 and IPv6 route rules.

To modify the settings or define new rules you should use the **Network / Static Routes** menu.

M2M-WM-E-LCB Status System Router Services Network Logout UNSAVED CHANGES: 4

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.127.100	34:73:5A:B4:CC:B2	lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
4g-wan	0.0.0.0/0	10.64.64.64	0	main
4g-wan	10.64.64.64	-	0	main
lan	192.168.127.0/24	-	0	main

Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	ff00::/8		256	local

IPv6 Neighbours

IPv6-Address	MAC-Address	Interface
--------------	-------------	-----------

Here you can define a new IP route rule, by the button.

These can be performed by choosing the related interface and adding the **Host-IP or Network** name, the **IPv4-Netmask**, and **IPv4-Gateway**.

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

3.6 Firewall settings

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

Important!

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

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

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

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

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

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

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

You can also see the **Rejected** chain here below.

Firewall Status

IPv4 Firewall IPv6 Firewall

Table: Filter

Hide empty chains

Reset Counters

Restart Firewall

Chain INPUT (Policy: ACCEPT, 83 Packets, 3.32 KB Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1.44 K	105.12 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
12.20 K	1.27 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
11.57 K	1.23 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
394	18.53 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
408	21.67 KB	zone_wan_input	all	4g-wan	*	0.0.0.0/0	0.0.0.0/0	-	-
225	16.11 KB	zone_lan_input	all	eth0	*	0.0.0.0/0	0.0.0.0/0	-	-

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

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

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

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1.44 K	105.12 KB	ACCEPT	all	*	lo	0.0.0.0/0	0.0.0.0/0	-	-
12.06 K	2.53 MB	output_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom output rule chain
12.05 K	2.53 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-

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

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

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

M2M-WM-E-LCB Status System Router Services Network Logout UNSAVED CHANGES: 4

General Settings Port Forwards Traffic Rules Custom Rules

Firewall - Zone Settings

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

General Settings

Enable SYN-flood protection

Drop invalid packets

Input: accept

Output: accept

Forward: accept

Zones

Name	Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
wan	wan ⇒ lan	accept	accept	accept	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
lan	lan ⇒ wan	accept	accept	accept	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete

[Add](#)

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

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

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

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

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

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

The screenshot shows the Mikrotik WinBox interface for configuring Firewall Zone Settings for a zone named "newzone". The top navigation bar includes "M2M-WM-E-LCB", "Status", "System", "Router", "Services", "Network", and "Logout", along with an "UNSAVED CHANGES: 10" indicator. The main content area has tabs for "General Settings", "Port Forwards", "Traffic Rules", and "Custom Rules". The "General Settings" tab is active, showing the "Zone 'newzone'" configuration. Below the title, there is a descriptive paragraph: "This section defines common properties of 'newzone'. The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone." Below this, there are two sub-tabs: "General Settings" (active) and "Advanced Settings". The "General Settings" section includes: "Name" (text input: newzone), "Input" (dropdown: accept), "Output" (dropdown: accept), "Forward" (dropdown: accept), "Masquerading" (checkbox: unchecked), "MSS clamping" (checkbox: unchecked), and "Covered networks" (dropdown: -- please select --). Below this is the "Inter-Zone Forwarding" section with a descriptive paragraph: "The options below control the forwarding policies between this zone (newzone) and other zones. *Destination zones* cover forwarded traffic **originating from 'newzone'**. *Source zones* match forwarded traffic from other zones **targeted at 'newzone'**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well." Below this are two dropdown menus: "Allow forward to destination zones:" (dropdown: -- please select --) and "Allow forward from source zones:" (dropdown: -- please select --). At the bottom, there are three buttons: "Back to Overview", "Save & Apply", "Save", and "Reset".

For the port-level filtering or interface traffic limits or **Traffic Rules** settings are also necessary to define!

Here you can **Enable / Disable** or **Edit**, **Delete** a configured rule.

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

3.7 Port Forward settings

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

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

The screenshot shows the web interface for M2M-WM-E-LCB. The top navigation bar includes 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. The 'Network' menu is active, and the 'Port Forwards' tab is selected. The page title is 'Firewall - Port Forwards'. Below the title, there is a description: 'Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.' The main section is titled 'Port Forwards' and contains a table with columns: Name, Match, Forward to, and Enable. The table is empty, with a message: 'This section contains no values yet'. Below the table, there is a 'New port forward' section with a form. The form has the following fields: Name (text input, value: 'New port forwa'), Protocol (dropdown, value: 'TCP+UD'), External zone (dropdown, value: 'newzone'), External port (text input), Internal zone (dropdown, value: 'lan'), Internal IP address (dropdown, value: '-- Please choose --'), and Internal port (text input). There is an 'Add' button to the right of the form. At the bottom right of the page, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red).

When you modified the settings, save them by the [Save & Apply](#) button.

3.8 NAT settings

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

You can add a new rule by the [Add](#) button and [Save & Apply](#) to close the upcoming window.

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

M2M-WM-E-LCB Status System Router Services Network Logout UNSAVED CHANGES: 17

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

Firewall - Traffic Rules

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

Traffic Rules

Name	Match	Action	Enable	
Test	Any tcp, udp From <i>any host</i> in wan To <i>any router IP</i> at port 67 on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>	Up Down Edit Delete

Open ports on router

Name	Protocol	External port	
<input type="text" value="New input rule"/>	TCP+UDP	<input type="text"/>	Add

New forward rule

Name	Source zone	Destination zone	
<input type="text" value="New forward rule"/>	wan	lan	Add and edit...

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable
<i>This section contains no values yet</i>			

New source NAT

Name	Source zone	Destination zone	To source IP	To source port	
<input type="text" value="New SNAT rule"/>	lan	wan	-- Please choose --	Do not rewrite	Add and edit...

Save & Apply Save Reset

The **Source NAT** settings (below) can be performed for each protocol (tcp, udp), that the modem 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.

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

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

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

Important!

Always check the standard ports, which are used by the network services and always allow these to operating (e.g. FTP: port 21, SSH/Telnet: port 22, DHCP: port 53, NTP time server: port 123, etc).

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

Always limit the access of services, and decrease the amount of the throughput communication on the network by these rules to provide the operation only for the necessary services, ports, ip addresses.

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

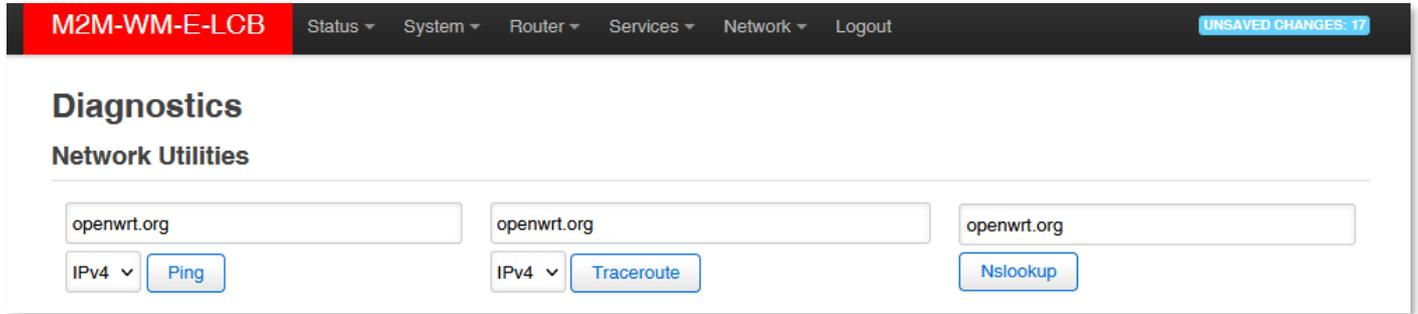
At the **Network / Static Routes** menu item you can define a new route.

The screenshot shows a web interface for configuring network settings. At the top, there is a navigation bar with the title 'M2M-WM-E-LCB' and several menu items: Status, System, Router, Services, Network, and Logout. A notification in the top right corner indicates 'UNSAVED CHANGES: 17'. The main content area is titled 'Routes' and includes a brief description: 'Routes specify over which interface and gateway a certain host or network can be reached.' Below this, there are two sections: 'Static IPv4 Routes' and 'Static IPv6 Routes'. Each section contains a table with columns for 'Interface', 'Target', 'IPv4-Netmask' (or 'IPv6-Address or Network (CIDR)'), 'IPv4-Gateway' (or 'IPv6-Gateway'), 'Metric', 'MTU', and 'Route type'. Both sections currently show 'This section contains no values yet' and have an 'Add' button. At the bottom right of the interface, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red).

Chapter 4. Advanced services

4.1 Ping IP address / checking IP

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



Here you can check the availability of an IP address, that is it accessible (push **Ping** button), is there a naming service provided, and is there response between two IPs (push **Nslookup** button), furthermore you can query the path of the communication (by **Traceroute** button). Then below you will get the results listed.

Important!

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

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

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

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

4.2 Network Time Service (NTP)

Important! This NTP time synchronisation is highly important for data storage of the incoming readout results (metering files) on the modem's memory. Because the device uses file syntax with the current datetime values.

The supercapacitor provides max. a few days of keeping the date-time values, but the NTP sync is also very important to keep updated time for the device and your data. Therefore we highly recommend you to configure NTP time servers and to test the proper functioning of this feature.

Open the **System / System** menu. At the **Time synchronisation** part, allow to **Enable NTP client** option and define an NTP server IP address (**NTP server candidates**).

The screenshot shows the 'System' configuration page for a device named 'M2M-WM-E-LCB'. The page has a navigation bar at the top with 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout' menus. A status bar indicates 'UNSAVED CHANGES: 17' and 'AUTO REFRESH ON'. The main content area is titled 'System' and includes a sub-section 'System Properties' with tabs for 'General Settings', 'Logging', 'Language and Style', and 'Advanced'. Under 'System Properties', the 'Local Time' is '2000-01-04 22:06:29' with buttons for 'Sync with browser' and 'Sync with NTP-Server'. The 'Hostname' is 'M2M-WM-E-LCB' and the 'Timezone' is 'UTC'. The 'Time Synchronization' section has 'Enable NTP client' checked and 'Provide NTP server' unchecked. Below, the 'NTP server candidates' list contains '192.168.1.111', 'de.pool.ntp.org', 'hu.pool.ntp.org', and 'sk.pool.ntp.org', each with a delete button. A plus button is at the bottom of the list. At the bottom right, there are 'Save & Apply', 'Save', and 'Reset' buttons.

If you allow the **Provide NTP server** option, the connected device(s) will get NTP time from the WM-E LCB device.

The most NTP time servers are using the UDP Port nr. 123 for time synchronisation. You can find a NTP time servers on the Internet. Note, that the modem must access the public Internet for the NTP time server sync. Also take care of using the IPv4 and IPv6 dependent time servers.

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

The time zone and synchronization of the system can be achieved also here, above. You can define the **Timezone**.

4.3 Identifying of connecting computers

Open the **Network / Hostnames** menu.

Here you can register external connecting network devices / machines, for easier identification.



The screenshot shows a web interface for configuring hostnames. At the top, there is a navigation bar with the title 'M2M-WM-E-LCB' and several menu items: 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. A notification in the top right corner indicates 'UNSAVED CHANGES: 18'. The main content area is titled 'Hostnames' and contains a section for 'Host entries'. This section has a table with two columns: 'Hostname' and 'IP address'. The first row shows 'External_PC' in the 'Hostname' column and '192.168.127.1 (6E:F4:13:82:82:38)' in the 'IP address' column. To the right of the IP address is a 'Delete' button. Below the table is an 'Add' button. At the bottom right of the form, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

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

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

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

4.4 TFTP settings

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

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

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

DHCP and DNS

Dnsmasq is a combined [DHCP-Server](#) and [DNS-Forwarder](#) for [NAT](#) firewalls

Server Settings

General Settings Resolv and Hosts Files **TFTP Settings** Advanced Settings

Enable TFTP server

TFTP server root

[?](#) Root directory for files served via TFTP

Network boot image

[?](#) Filename of the boot image advertised to clients

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
----------	--------------	-------------	---------------------

There are no active leases.

Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
------	--------------	------	---------------------

There are no active leases.

Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	DUID	IPv6-Suffix (hex)	
----------	-------------	--------------	------------	------	-------------------	--

-- Please choose -- ▾

-- Please choose -- ▾

Delete

Add

Save & Apply

Save

Reset

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

Of course, you can also use SFTP on your device by sending the data to IP addresses by entering your account and password information. if you need more help, see Chapter 9 in the OpenSSH Linux command line settings.

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

4.5 Ser2net (RS485 settings)

For the proper settings of the RS485 port connection, choose the **Services / Ser2net** menu item.

Here you can define the protocol conversion parameter settings, such as receiving the incoming communication in the proper format and data exchange.

For first, the **RS485** feature must be enabled and RS485 cabling of RJ45 port must be connected to the external device, which you want to get data from or collect data.

The screenshot shows a web interface for configuring Ser2net. At the top, there is a navigation bar with the following items: M2M-WM-E-LCB, Status, System, Router, Services, Network, and Logout. The main heading is "Ser2net". Below the heading, there is a brief description: "The ser2net allows telnet and tcp sessions to be established with a unit's serial ports." A "Proxies" section follows, explaining that the program opens TCP ports and waits for connections, and that it refuses connections if another user is already using the port. On the right side of the page, there is a "Delete" button. The configuration fields are as follows: "RS485" is checked; "TCP Port" is set to 8000; "State" is set to "Raw"; "Timeout" is set to 30; "Device" is set to "/dev/ttyS5"; and "Options" is set to "9600 1STOPBIT 7DATABITS EVE". Each field has a help icon and a detailed explanation of its function.

M2M-WM-E-LCB Status System Router Services Network Logout

Ser2net

The ser2net allows telnet and tcp sessions to be established with a unit's serial ports.

Proxies

The program comes up normally as a service, opens the TCP ports specified in the configuration file, and waits for connections. Once a connection occurs, the program attempts to set up the connection and open the serial port. If another user is already using the connection or serial port, the connection is refused with an error message.

Delete

RS485

TCP Port

Name or number of the TCP/IP port to accept connections from for this device.
A port number may be of the form [host,]port, such as 127.0.0.1,2000 or localhost,2000.
If this is specified, it will only bind to the IP address specified for the port.
Otherwise, it will bind to all the ports on the machine.

State

Either raw or rawlp or telnet or off. off disables the port from accepting connections.
It can be turned on later from the control port.
raw enables the port and transfers all data as-is between the port and the long.
rawlp enables the port and transfers all input data to device, device is open without any termios setting.
It allow to use /dev/lpX devices and printers connected to them.
telnet enables the port and runs the telnet protocol on the port to set up telnet parameters. This is most useful for using telnet.

Timeout

The time (in seconds) before the port will be disconnected if there is no activity on it.
A zero value disables this functon.

Device

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

Options

Sets operational parameters for the serial port.
Values may be separated by spaces or commas.
Options 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 set the various baud rates. EVEN, ODD, NONE set the parity.
1STOPBIT, 2STOPBITS set the number of stop bits.
7DATABITS, 8DATABITS set the number of data bits. [-]XONXOFF turns on (- off) XON/XOFF support.
[-]RTSCTS turns on (- off) hardware flow control.
[-]LOCAL ignores (- checks) the modem control lines (DCD, DTR, etc.) [-]HANGUP_WHEN_DONE lowers (- does not lower) the modem control lines (DCD, DTR, etc.) when the connection closes.
NOBREAK Disables automatic clearing of the break setting of the port.
remctl allows remote control of the serial port parameters via RFC 2217.

TCP Port - nr. 8000 by default, which you have to configure to your needs.

State field - choose the right protocol type here:

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

We offer to use the **raw** option here, because the meters are sending raw text format files to the modem.

Timeout – default value is 30 (0 means without delay).

Options: A complex parameter with **Baudrate** selection + **Stopbit** definition + **Databits** definition + **Parity** type

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

Examples:

For standard speed 7E1 mode use this command: ***9600 1STOPBIT 7DATABIT EVEN***

For lower speed 8N1 mode use this one: ***2400 1STOPBIT 8DATABIT NONE***

Important! Note that maximum 115 200 baud speed rate can be used wheather of the configuration options. ***But, we offer to use the standard 9600 baud or 2400 baud speed rate for receiving or transmitting data without character / data loss.***

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

Note, that you should add the specified RS485 port number to the **Firewall** rules (**Network / Firewall** menu), otherwise the router will not receive any data.

You can also specify additional members, such as *hardware flow control* with the **RTSCTS**, which can be turned off with the "-" prefix. A **space** character must be placed between members.

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

4.6 Relay switch settings

The relay output settings can be achieved in the **Router / Relay Switch** menu.

At the **Network** part, configure the **Listen port** – here you can define a port for detecting the relay switch success, load control box events.

At the **Control box** part you will find the **enable the iec1107 mode** field, which is for protocol compatibility. It has the following protocol conversions to be selected:

- *ON 1107* – IEC 1107 protocol compatible mode
- *OSLP* – Open Street Light Protocol compatible mode
- *ON 1107 + OSLP* – IEC 1107 and Open Street Light Protocol compatible method

The screenshot shows the 'Control Box' configuration page in the M2M-WM-E-LCB interface. The page has a dark header with the title 'M2M-WM-E-LCB' and navigation links for Status, System, Router, Services, Network, and Logout. The main content area is titled 'Control Box' with the subtitle 'Set Relays using IEC1107 W1 set.' It is divided into two sections: 'Network' and 'Control Box'. In the 'Network' section, the 'Listen port' is set to 7799, with a help icon and the text 'Port number connect to'. In the 'Control Box' section, there are four fields: 'enable iec1107 mode' is a dropdown menu set to 'ON 1107' with a help icon and 'Enable IEC 1107 switching'; 'manufacturer code' is a text input field containing 'ABB' with a help icon and 'Three capital letters.'; 'version string' is a text input field containing '5.40' with a help icon and 'Numbers dot numbers spaces. !Without letter "V"'; and 'Baudrate code' is a dropdown menu set to '5' with a help icon and 'Just for compatibility.'. At the bottom right, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red).

Manufacturer code – Usable for further identification

Version string – see the load control box documentation for more

Baudrate code – can be selected from the following standard speed rates:

- 0: which means 300 baud
- 1: which means 600 baud

- 2: which means 1200 baud
- 3: which means 2400 baud
- 4: which means 4800 baud
- 5: which means 9600 baud
- 6: which means 19200 baud

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

4.7 LED configuration

The device has 5 LEDs to assign the current relay switch status and network connection. The first 4 relay LEDs are fixed (**REL.1..4**), but the 5th LED - the **WAN** LED (network connection) - is reprogrammable.

M2M-WM-E-LCB

[Status](#) [System](#) [Router](#) [Services](#) [Network](#) [Logout](#)
UNSAVED CHANGES: 8

LED Configuration

Customizes the behaviour of the device LEDs if possible.

Delete

Name

LED Name

Default state

Trigger

Device

Trigger Mode Link On Transmit Receive

Delete

Name

LED Name

Default state

Trigger

Device

Trigger Mode Link On Transmit Receive

Add

Save & Apply
Save
Reset

The **WAN** LED has a pre-defined default value, but you change its operation in the **System / LED Configuration** menu. There you can define a LED rule for events - as lighting/blinking.

By the **Name** field add a logical name (for identifying the led) and choose a physical led for the setting by the **LED Name** field.

Then declare the event of operation by the **Trigger** field and the interface at the **Device** (which will be valid for). All useable possibilities are listed on the web UI.

The **Trigger** allows to choose an event type of operation. E.g. *netdev* means the network interface connection type, and **Device** identifies the related network interface. Select a **Trigger** type from list, if additional option required then additional menu will appear.

At the **Trigger mode**, the **Link On** (network activity), **Transmit** (data transmitting) or **Receive** (data receive) can be choosed for signing the data flow or activity by he LED flashing.

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

4.8 Using the UCI Command Line Interface

The operating system uses the embedded Micro uClinux, kernel 4.9 version, **UCI Command line interface** – check command line compatibility before using the commands here.

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

You can find the UCI command line interface options, setting parameters in the UCI® CLI document. Check the „*UCI® Command Line Interface Reference*“ documentation for more information of using the *UCI*.

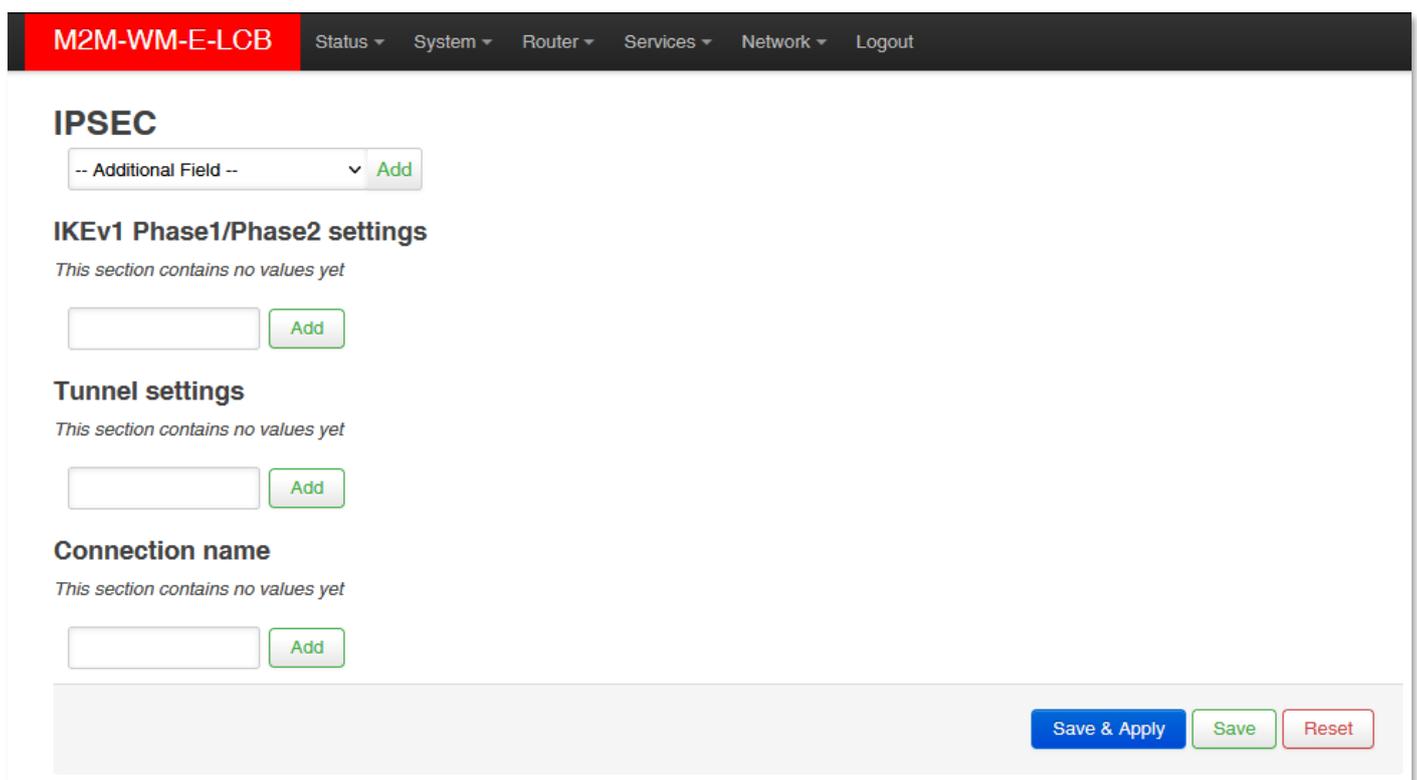
https://www.m2mserver.com/m2m-downloads/UCI_Command_Line_Reference_v3.pdf

4.9 IPSEC settings

Open **Network / IPSEC** to configure *Strongswan IPsec* settings. In the **IPSEC** section, you can set the Listen on interface option and then press the button - the available interfaces will be displayed.

Select one or more interfaces through which you want to use IPSEC.

Below, in the **IKEv1 Phase1 / Phase2** settings, you can use the button to give a logical name to the **IPSEC connection**, then select the **Encryption algorithm** and **Hash algorithm**, and set the Diffie-Hellmann group to the tunnel.



The screenshot shows a web interface for configuring IPSEC settings. At the top, there is a navigation bar with the following items: "M2M-WM-E-LCB" (highlighted in red), "Status", "System", "Router", "Services", "Network", and "Logout". Below the navigation bar, the main content area is titled "IPSEC". Under this title, there is a dropdown menu with "-- Additional Field --" and an "Add" button. The next section is "IKEv1 Phase1/Phase2 settings", which contains the text "This section contains no values yet" and a single "Add" button. Below that is the "Tunnel settings" section, also with the text "This section contains no values yet" and an "Add" button. The final section is "Connection name", with the text "This section contains no values yet" and an "Add" button. At the bottom right of the page, there are three buttons: "Save & Apply" (blue), "Save" (green), and "Reset" (red).

Below, in the **Tunnel settings** section, the button can be used to enter the settings for the tunnel by entering a logic name again. **Local Subnet** and **Remote Subnet** indicate the IP address range of the local and remote subnets.

IPSEC

Listen on interface 4g-wan

IKEv1 Phase1/Phase2 settings

[Delete](#)

11

Encryption algorithm

Hash algorithm

Diffie-Hellman group

[Add](#)

Tunnel settings

This section contains no values yet

[Add](#)

Connection name

This section contains no values yet

[Add](#)

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

The name of the **IKEv1 Phase 2** option is an optional name where you must specify the **Key exchange** method.

Tunnel settings

[Delete](#)

TUNNEL

Local subnet

Remote subnet

IKEv1 Phase2 setting's name

Key exchange

[Add](#)

Below, in the **Connection** name section, you can enable or disable the connection (**Enable / Disable** connection).

OFFICETUNNEL

Local subnet

Remote subnet

IKEv1 Phase2 setting's name

Key exchange

Attention! The IPSEC used by the program uses Strongswan-based IPsec. To learn more about it, visit the OpenWrt page for more information on possible settings:

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

Enter **the IP setting** for VPN connection's **remote gateway address**, select **Authentication mode**, and enter the PSK (**Secret or PSK of connection**) key.

IKEv1 connection mode can be main or aggressive.

Enter the keys for the **Local gateway identifier** and the **Remote gateway identifier**.

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

You can read more about IPSEC settings that can also be set from the UCI (Command Line UCI Command) here: <https://oldwiki.archive.openwrt.org/doc/uci/ipsec>

IPSEC can also be configured using the Linux-side Strongswan daemon using the UCI - from the command line - using SSH. Some examples of its use:

To query OpenVPN settings:

```
#uci show ipsec
```

For this, the current IPSEC settings are displayed on the command line.

Configuration by the following syntax. Then you have to commit.

```
#uci set ipsec1.encryption algorithm='aes128'  
  
#uci commit
```

4.10 Voice call settings

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

The screenshot shows the web interface for M2M-WM-E-LCB. The top navigation bar includes 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. The 'Voice Call Config' section is active, showing a 'Phone Book' table. The table has two columns: 'Phone number' and 'Command'. A single entry is shown with the phone number '+36301234567' and the command 'Reboot'. There is a 'Delete' button next to the entry. Below the table is an 'Add' button. At the bottom right, there are 'Save & Apply', 'Save', and 'Reset' buttons. The top right corner of the interface indicates 'UNSAVED CHANGES: 7'.

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

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

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

4.11 Run commands remotely (SMS config settings)

You can execute commands on the device remotely when an SMS message is sent to the device SIM card's phone number. To set these remote control commands, open **Network / SMS Config** menu.

M2M-WM-E-LCB Status System Router Services Network Logout UNSAVED CHANGES: 8

SMS Config

Phone Book

Enabled	Phone number	
<input type="checkbox"/>	+36331234564	Delete
<input type="checkbox"/>	+36331234561	Delete
<input type="checkbox"/>	+36331234562	Delete
<input type="checkbox"/>	+36331234563	Delete

Add

SMS Commands

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

Save & Apply Save Reset

First you can see the **Phone Book** where you can define or phone numbers.

Then you have to **Enable** the selected phone number.

At the **SMS commands** part you can choose preset commands by selecting them for the number. In the case of an SMS from a preset phone number, the device runs the preset command (s) assigned to the phone number: e.g. **Reboot**

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

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

Chapter 5. Maintenance

5.1 Firmware refresh

1. Download the latest device firmware from our website by the following URL:
https://www.m2mserver.com/m2m-downloads/fwos-BE0080x_WM-E_LCB.202204281_RC.tar.gz
2. Open the **System** menu, **Backup / Flash Firmware** menu item.
3. At first just by safety, **backup your system** before changing the firmware version (see the instructions later).
4. Push the button for selecting the compressed and downloaded firmware file (***fwos-....*** file with **.zip** extension) from your computer, then push to the button.

M2M-WM-E-LCB Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout UNSAVED CHANGES: 0

Flash operations

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashts images).

Reset to defaults

Restore backup No file selected.

🔗 Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Save mtblock contents

Click "Save mtblock" to download specified mtblock file. (NOTE: THIS FEATURE IS FOR PROFESSIONALS!)

Choose mtblock

Download mtblock

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).

Image No file selected.

Powered by LuCI Master (f138fc93) / 202108271_RC

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

M2M-WM-E-LCB Status System Router Services Network Logout UNSAVED CHANGES: 0

Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.

- Checksum
 - MD5: 2b80e724c498d9ada87b29a0719c944b
 - SHA256: ad6bc83b4d7edcc859c4cac8e8325a8c6cac448ca0eb34ce786148e43337f991
- Size: 6.33 MB (16.00 MB available)

Cancel Proceed

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

M2M-WM-E-LCB

System - Flashing...

The system is flashing now.

DO NOT POWER OFF THE DEVICE!

Wait a few minutes before you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

Waiting for changes to be applied...

7. All network connections will be disconnected during the installation.

When the firmware installation begins, the **WAN** LED will assign the installation, which will be continuously blank until the finish of the installation. The firmware refresh requires about 2-4 minutes.

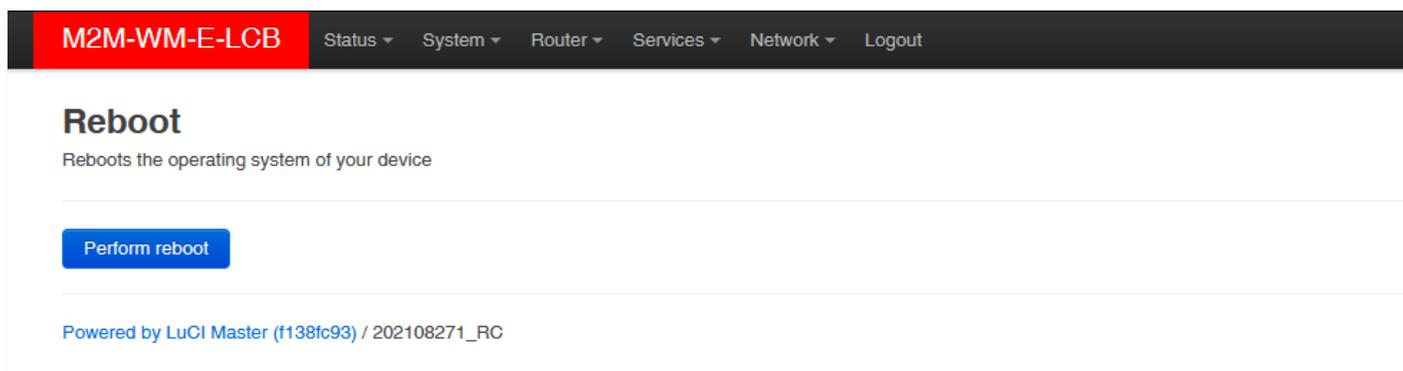


Note, that the signals of relay LEDs will be not changing during the firmware update.

8. At the end of the installation, device will be restarted automatically, which will be signed by the short **WAN** LED activity. All further operation / LED signals will be the same as it is written in the Installation Manual, Chapter 2.2.

5.2 Restarting the device

The device can be restart from the LuCi web user interface, from the **System / Reboot** menu, by pushing the  button.



Then the device will disconnect the **LAN** and **WAN** network interfaces, which will be signed after 5-10 seconds by the blank **WAN** LED.



Then the device will be restarted, and after ~1-2 minutes the network interfaces will be available again, which will be signed by the active **WAN** LED.

5.3 Turn off the device

The device can be turned off by removing the power wire (No. 5) from the AC plug. The device will be turned off safely. It will disconnect the **LAN** and **WAN** network interfaces, which will be signed after 5-10 seconds by the blank **WAN** LED.



After ~10 seconds all the four LEDs will be blank, which is signing that the device is not powered by the AC voltage further.



IMPORTANT!

THE AC POWER INPUT WIRES ARE STILL CONNECTED TO THE DEVICE. THEREFORE DO NOT OPEN THE DEVICE ENCLOSURE UNTIL NOT REMOVED THE AC POWER FROM THE PLUG OR THE POWER SOURCE!

The device can be started anytime again by adding the power source for the device (connect the AC power plug to the electricity network). The device will be operating as it is written in the Installation Manual, Chapter 2.2.

5.4 Backup device settings

The modem settings are automatically stored by the OpenWrt® system, but there can be other situations when you need to restore the settings to a previously saved settings. You can save these settings to your computer or restore back to the modem anytime by following the next hints.

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

A screenshot of the OpenWrt web interface. At the top is a navigation bar with a red header 'M2M-WM-E-LCB' and a dark grey menu containing 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. Below the navigation bar is the 'Flash operations' section. It has two tabs: 'Actions' (selected) and 'Configuration'. Under 'Flash operations', there are two sub-sections: 'Backup' and 'Restore'. The 'Backup' section has the text 'Click "Generate archive" to download a tar archive of the current configuration files.' and a 'Download backup' label next to a blue button labeled 'Generate archive' which is highlighted with a red dashed border. The 'Restore' section has the text 'To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).' and contains three elements: a 'Reset to defaults' label next to a red button labeled 'Perform reset'; a 'Restore backup' label next to a 'Browse...' button, the text 'No file selected.', and a blue button labeled 'Upload archive...'; and a small blue icon followed by the text 'Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.'

To backup your system settings into an archive file, choose a the **Backup / Restore** part, the **Download backup** and push to the  button. It is saving current settings to a compressed file to your computer. This is very useful during the first configurations.

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

Important!

After the next reboot, the system will starting the system by these stored settings – as the new default configuration.

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

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

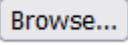
Of course, you need to know the modem device's file system to make it right. Therefore, we offer to check the OpenWrt® system structure, directories by standard Linux-side commands from the CLI.

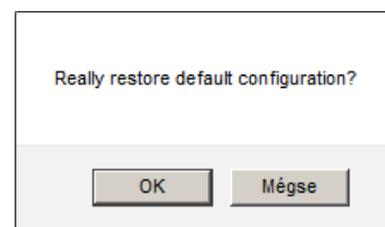
When you are ready with the modifications, push the  button for the changes.

5.5 Restore device settings

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

Here you can restore your previously saved system configuration archive – as a saved last good know configuration.

For this, just push the  button at **Restore backup** option and choose the previously saved archive file (tar.gz extension compressed file) from your computer. Then push to the  button.



Then a popup window will appear, where push **OK** if you want the restore the default configuration.

M2M-WM-E-LCB Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout

Flash operations

Actions Configuration

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults

Restore backup No file selected.

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Then the system will reload the saved backup and restore the settings to the device. After all the device will be restarted by the system and applying the previously used configuration.

Important!

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

5.6 Clone config backup/restore

The device current configuration settings can be saved (backup) and stored by the **System** menu, **Clone config backup / restore** menu item.

M2M-WM-E-LCB Status ▾ System ▾ Router ▾ Services ▾ Network ▾ Logout

Clone config backup/restore

Download clone backup:

To restore configuration files, you can upload a previously generated backup archive here.

Restore clone backup: No file selected.

To backup your system settings, push the button to define the path/directory to save the file and push to the button.

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

This is very helpful to move the saved configuration file to your computer and then later restore these settings to a different modem device by the **Browsing...** and then the  button. There you can save time by this quick configuration method.

Chapter 6. Administration

6.1 Password change

Open the **System / Administration** menu.

At the **Password** part you can fill the new **Password** and repeat it the at the **Confirmation** field.

The screenshot shows a web interface for configuring the Router Password. At the top, there is a navigation bar with the title 'M2M-WM-E-LCB' and several menu items: Status, System, Router, Services, Network, and Logout. Below the navigation bar, there are three tabs: 'Router Password' (which is active), 'SSH Access', and 'SSH-Keys'. The main content area is titled 'Router Password' and includes a subtitle 'Changes the administrator password for accessing the device'. There are two input fields: 'Password' and 'Confirmation', both of which are currently empty and have an asterisk (*) on the right side, indicating that the characters are hidden. At the bottom right of the form, there is a blue 'Save' button.

IMPORTANT NOTES

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

When you have modified the settings, save them by the **Save & Apply** button. Now you can login with the new password.

Note, that the **SSH Access** can be reconfigured here as the **SSH Keys** can be defined also.

6.2 Logging

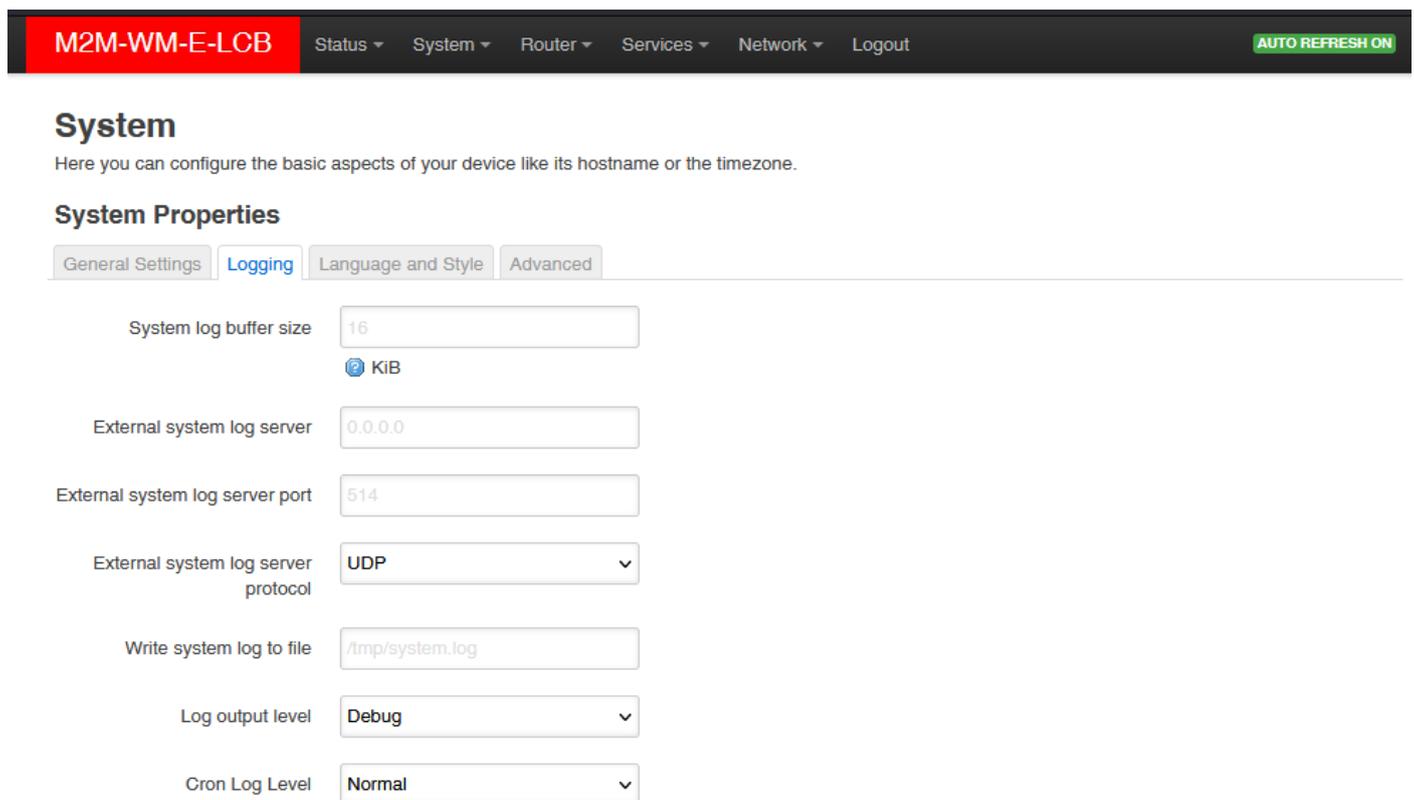
Open the **System / System** menu find the **Logging** tab.

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

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

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

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



The screenshot shows the web interface for M2M-WM-E-LCB. The top navigation bar includes 'M2M-WM-E-LCB', 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. An 'AUTO REFRESH ON' button is visible in the top right. The main content area is titled 'System' and contains the text: 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Below this is the 'System Properties' section with tabs for 'General Settings', 'Logging', 'Language and Style', and 'Advanced'. The 'Logging' tab is active, showing the following configuration options:

- System log buffer size: 16 KiB
- External system log server: 0.0.0.0
- External system log server port: 514
- External system log server protocol: UDP
- Write system log to file: /tmp/system.log
- Log output level: Debug
- Cron Log Level: Normal

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

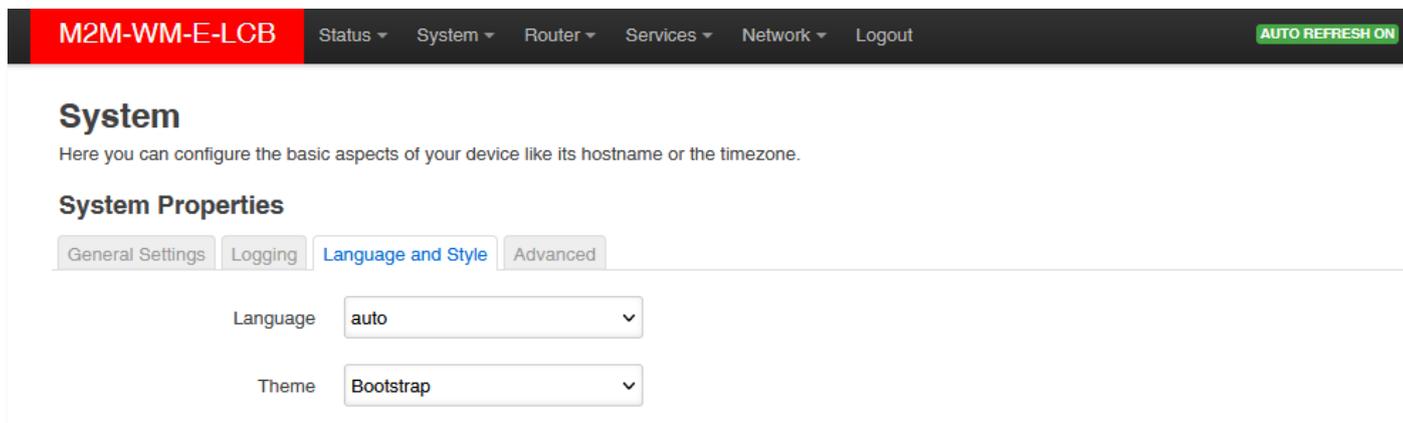
There are other log files generated by default that we have already mentioned in part. These include the **System log** and the **Kernel Log** file in the **Status** menu, which help you understand what has happened during operation since the router was last rebooted. This can be especially useful when detecting an error.

6.3 Language settings

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

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

The *Auto* preference means that the OpenWrt® UI language will be configured according to your browser language settings.

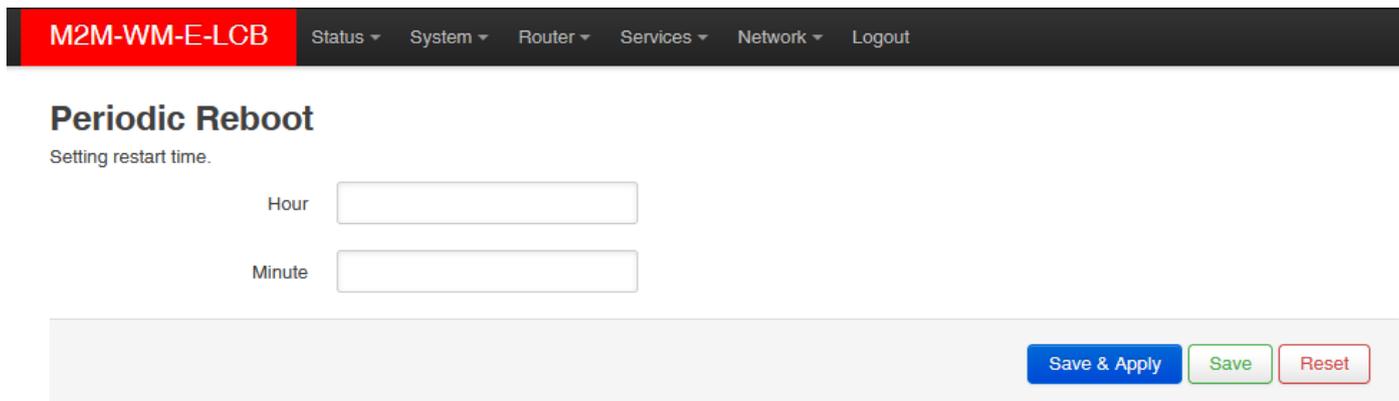


The screenshot shows the OpenWrt web interface. At the top, there is a navigation bar with the device name 'M2M-WM-E-LCB' on the left and a menu with 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. On the right of the navigation bar is a green button labeled 'AUTO REFRESH ON'. Below the navigation bar, the main content area is titled 'System' and contains the text 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Underneath, there is a section titled 'System Properties' with four tabs: 'General Settings', 'Logging', 'Language and Style' (which is selected and highlighted in blue), and 'Advanced'. In the 'Language and Style' tab, there are two dropdown menus: 'Language' with 'auto' selected and 'Theme' with 'Bootstrap' selected.

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

6.4 Periodic reboot settings

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



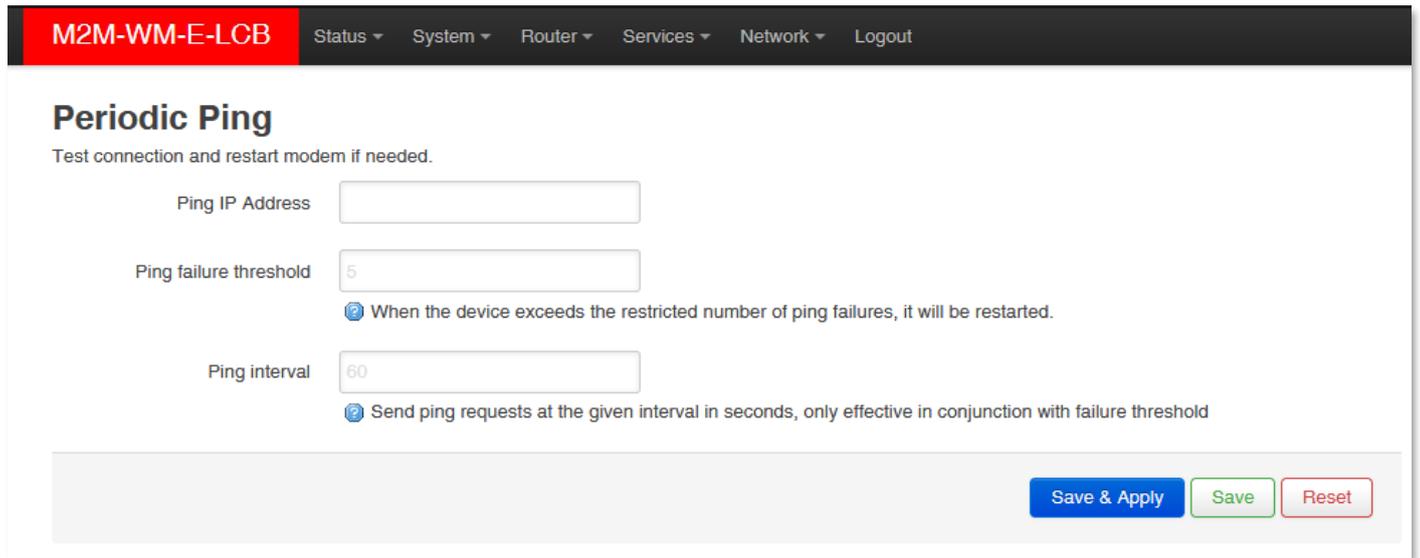
The screenshot shows the 'Periodic Reboot' settings page in the OpenWrt web interface. The navigation bar is the same as in the previous screenshot. The main content area is titled 'Periodic Reboot' and contains the text 'Setting restart time.' Below this, there are two input fields: 'Hour' and 'Minute'. At the bottom right of the page, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red).

At the **Hour** and **Minute** values, you can define the daily HH:MM period to be applied for the device reboot.

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

6.5 Periodic ping

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



Ping IP Address – define the IP address to be progress the ping command.

Ping failure threshold – ping failure numbers to be ignored (e.g. in case of 5, which means 5 errors for a ping interval is normal, not signed as a fail/error).

Ping interval – length of ping running in seconds (e.g. 60 means ping for 1 minute).

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

6.6 Installing 3rd party applications

Open the **System / Software** menu.

The installation software repositories can be defined at the **Configure opkg...** button). Save the repository settings by the **Save** button.

Push to the **Update lists...** button to refresh the available software catalog from the configured software repositories.

Then choose one or the name of the application, which you are attempted to install to the **Download and install package** field.

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

The screenshot shows the 'Software' management interface for the M2M-WM-E-LCB device. At the top, there is a navigation bar with 'M2M-WM-E-LCB' in a red box and menu items for 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout'. Below the navigation bar, the 'Software' section displays 'Free space: 92% (970.8 KB)' with a blue progress bar. There are three main input areas: a 'Filter' field with a 'Clear' button, a 'Download and install package:' field with an 'OK' button, and an 'Actions:' section with 'Update lists...' and 'Configure opkg...' buttons. Below these are tabs for 'Available', 'Installed', and 'Updates'. A pagination area shows 'No packages' between left and right arrow buttons. A table header is visible with columns for 'Package name', 'Version', 'Size (.ipk)', and 'Description'. The table content is currently empty, showing 'No information available'.

E.g. fill the „mc” - which means the *Midnight Commander* application – to the **Download and install package** and push to the **OK** button.

Then the package will be installed and after all the installed package will be listed with its Version. Now you can use the installed Linux application / component.

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

Important!

Note, that this feature is available only, when the public Internet is accessible by the SIM card and the used APN.

6.7 SSH access

You can access the device remotely according to the current settings. Consider, the device can access external devices or data due to the SIM card IP-segment possibilities.

The same issue when you are attempted to access the device remotely: your computer must be located in the same IP segment or APN zone as the modem has. (In case of public internet access, there is no limit for that.)

The remote access is possible by SSH and FTP service.

SSH Connection

The device can be accessed through SSH connection, when it is available on its IP address – by a terminal utility (e.g. *putty*) – at the **192.168.127.1:22** (port nr. 22 – **LAN** interface).

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



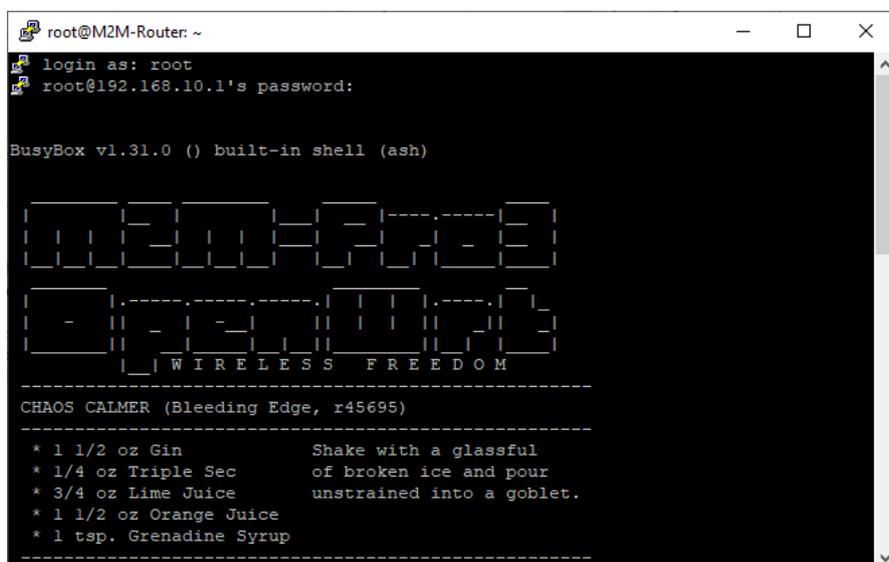
SSH login data:

Login: *root*

Password: *wmrpwdM2M*

Now you are logged in, at the OpenWrt®'s command line.

Here you can use Linux commands or using scripts or the *uci* commands on the device. (Check chapter 4.8 for more information about the *UCI*®.)



6.8 Device Manager® settings

Our Device Manager® application can be used for the remote management of the load control box (WM-E LCB device), which is used for the remote maintenance and reconfiguration of the device in addition to the continuous monitoring of the operating characteristics (network access, field strength, runtime, QoS).

In addition, it is possible to replace and install the firmware running on the device. You can manage hundreds of load control box devices from this software in this way.

The requested settings can be made individually or for a group of devices in one step.

To use the application, you need to purchase a license, please contact our Dealer.

More info: <https://m2mserver.com/en/product/device-manager/>

The *Device Manager* settings can be defined in the **Router / Device Manager** menu.

The main important ones are the **DM IP Address**, the **DM Port Number** and **DM User Name**.

The default DM Port number is **443**.

The screenshot shows the 'Device Manager Parameters' configuration page. At the top, there is a navigation bar with 'M2M-WM-E-LCB' on the left and 'Status', 'System', 'Router', 'Services', 'Network', and 'Logout' on the right. A 'UNSAVED CHANGES: 8' indicator is in the top right corner. The main heading is 'Device Manager Parameters' with a sub-note: 'Carefully change the parameters.' The form contains the following fields and options:

- Local DM Server Port Number:** Input field with value '443'. Below it is a radio button labeled 'After change applied, please reboot device!' which is selected.
- DM Name:** Input field with value 'something'.
- DM User Name:** Input field with value 'root'.
- CALL DM IP Address:** Empty input field.
- CALL DM Port Number:** Empty input field.
- Static WAN IP Address:** A checked checkbox. Below it is a radio button labeled 'Disable WAN up CALL.' which is selected.
- CALL Timeout:** Input field with value '30'. Below it is a radio button labeled 'Next CALL when sending fails.' which is selected.

At the bottom right of the form, there are three buttons: 'Save & Apply' (blue), 'Save' (green), and 'Reset' (red).

These must be also configured in the Device Manager[®] software for the proper operation.

The WM-E LCB device must access the IP address of the 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.

Chapter 7. Troubleshooting

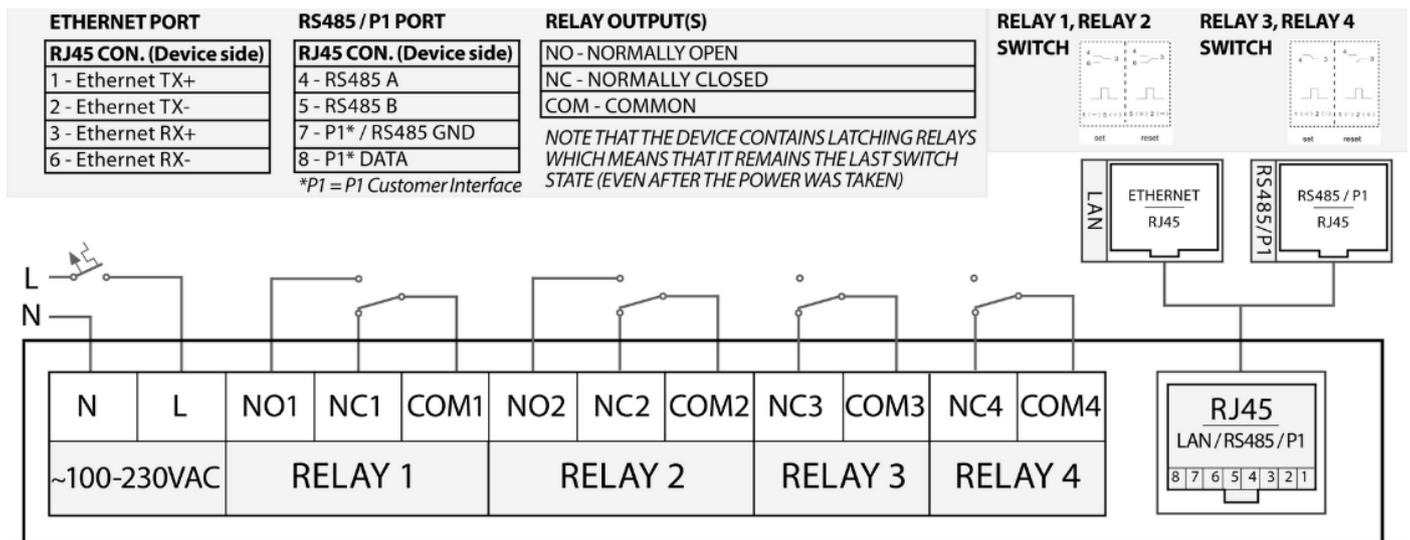
LED signals / LED activity

For understanding the LED activities, please check the *Installation Manual*, Chapter 1.10.

Connecting relays, power input, RJ45 connection

Read the *Installation Manual*, Chapter 1 for more information.

CAUTION! Take care, the device uses ~100-240V AC power source! Only a certified expert persons are allowed to open the device's enclosure or modify the wiring.



SIM-card is not detected

Ask you Mobile Operator about the SIM card is healthness and activation, APN.

SIM/APN failure

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

- **No SIM or SIM error** – means: there is no SIM card presented, insert an active SIM card, not inserted properly or the SIM card is wrong. **Ask the Installation expert person!**
- **Not enough RSSI value** – means: Antenna problem. **Ask the Installation expert person!**

- **No NW registration** – means: APN name for the SIM card is not configured well or the setting is wrong. Consult with your mobile operator and reconfigure the SIM **APN**, username and password on the LuCi® web user interface.
- **Check RSSI** – Antenna or SIM trouble. ***Ask the Installation expert person!***

WAN LED is inactive

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

If the problem is still occurring, ask your Mobile Operator about the SIM card's condition and activation status, correct APN name and configure the modem with the new information.

If it does not help, ***ask the Installation expert person!***

Cannot access the device on SSH / LuCi web interface

You tried a wrong IP address or you cannot connect to the device properly.

Check the IP address, ping the device. If it is still not working, reconfigure the IP address on your PC (IP: 192.168.127.100 / Subnet mask: 255.255.255.0).

For accessing the device's web user interface we offer to use the *Mozilla Firefox* web browser.

Try to access the modem on its USB interface by your browser: <https://192.168.127.1:8888>

Ensure that the **APN** was already configured and the **WAN** led is active or not.

- Username: **root** / Password: **wmrpwdM2M**
- Push to the **Login** button to access the web UI.

8. Support

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

E-mail: iotsupport@wmsystems.hu

Phone: +36 20 3331111

Online product support can be required here at our website:

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

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

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

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

<https://m2mserver.com/en/product/wme-lcb/>

GNU/Linux license and open source code

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

9. Legal notice

©2021. WM Systems LLC.

The content of this documentation (all information, pictures, tests, descriptions, guides, logos) is under copyright protection. Copying, using, distributing and publishing 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 confirm 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.