

M2M Router®

User Manual

v1.9



2017-06-29

Document specifications

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

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

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

Document category:	User Manual
Document subject:	M2M Router [®]
Author:	WMR
Document version No.:	REV 1.9
Number of pages:	46
Hardware Identifier No.:	BE0077C_CMDA450_2016.04.14
OpenWRT build version:	2017-04-26
Firmware version:	2017-01-24
Kernel version:	4.4.4
Webadmin Build:	2016-07-27 19:31:37
Document status:	Final
Compilation date:	26 April 2016
Last modified:	29 June 2017
Approval date:	29 June 2017

Table of contents

1. Starting up the Router	5
1.1 Interfaces.....	5
1.2 Cable connection	5
1.3 Starting the router	5
1.4 Web user interface of the router	6
1.5 Accessing the router on ssh connection.....	6
2. Web Administration user interface	7
2.1 Login	8
2.2 Main page (Dashboard)	9
2.3 Menu	9
2.4 Status menu	9
2.5 CDMA menu (only for CDMA devices).....	9
2.6 System menu	10
2.7 Router menu	11
2.8 Network menu	11
3. Network configuration of the router	13
3.1 Interface settings.....	13
3.2 Mobile internet settings (modem)	14
3.3 Ethernet (LAN) settings	17
3.4 DHCP settings.....	19
3.5 DNS settings.....	21
3.6 Defining the route rules.....	22
3.7 Firewall settings.....	23
3.8 Port Forward settings	27
3.9 IP routing, NAT settings.....	28
3.10 Dynamic DNS settings	29
4. Special settings	30
4.1 M2M Device Manager settings	30
4.2 Monitoring the modem	31
4.3 Ping an IP address	31
4.4 Network Time Service (NTP)	32
4.5 TFTP service settings.....	32
4.6 Identifying names connecting machines	33
4.7 LED configuration.....	34
5. Software refresh and router maintenance	36
5.1 Firmware refresh.....	36
5.2 Installing applications	37
5.3 Restarting the router	38
5.4 Reset	38
5.5 Password change	39
5.6 Backup and restore of settings	39
5.7 Handling memory cards.....	40



6. Troubleshooting	41
7. Support availability	43
7.1 Contact the support line	43
7.2 Product support	44
8. Legal notice	46

1. Starting up the Router

1.1 Cable connection



1. **Mount** a 2G/3G or 4G or an LTE 450/CDMA 450 **SMA antenna** to the **Antenna** titled SMA-M interface (according to the module/router type).
2. **Insert an activated data SIM card** to the SIM holder, placed the chip-side up and the cutted edge towards to inside and push until it sleeves.
3. **Connect UTP cable** to the **router Ethernet** titled port. The other side of the cable must be **plugged to the PC's Ethernet** port.
4. **The DHCP service is turned off for the router Ethernet interface**, by default. Therefore, **you have to configure an IP address for you PC, manually.**

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

1.2 Starting the router

1. **Plug the 12V DC power adapter** chord **to the POWER** interface, then **plug the adapter to the 230V** electrical network.
2. The router has a pre-installed system (contains uploaded firmware and system software). After plugging the power adapter, the router begins to work, whereas its **LED signals** are showing the current **activity** during the operation.
When power up the router, all the three LEDs will flashes once – as in case of restart.
If the device was under power supply the **LED1** will light continuously (which means that the system booting is in progress).
3. The system starting then takes about 1-2 minutes while it will be ready for usage. Then you can login to the web user interface.

4. The module and the mobile network availability is signed by the **LED2**. When the SIM card network registration was successfully performed, the LED lights continuously.
5. The **LED3** signs the wireless modem and mobile network availability. When the modem successfully registered the SIM card to the network, the LED will light continuously.
6. **As soon as you can, configure the internet settings of the wireless module (SIM and APN) for connecting to the 2G/3G/LTE network – in other case the router will be restarting in every 10 minutes!**
7. If you notice any failure or unusual LED flashing, then go to the **Troubleshooting** chapter.

1.3 Web user interface & Login

For accessing the the router through the web user interface you have to **setup the IP address of** the Ethernet interface on your computer to allow the fixed ipv4 address for the following IP address: 192.168.127.1, Subnet mask: 255.255.255.0)

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

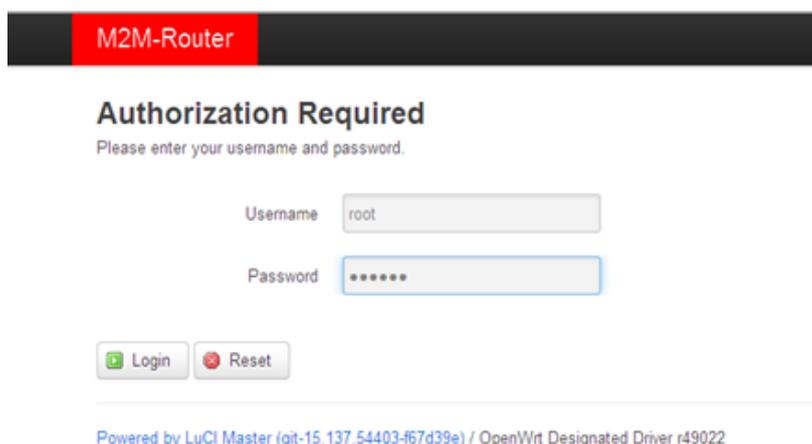
Attention!

For accessing the web user interface we offer the Mozilla Firefox web.

Default web user interface (LuCi) address is: <https://192.168.127.1:8888>

The login data are the following:

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



The screenshot shows the login page of the M2M-Router. At the top, there is a black header with a red bar containing the text "M2M-Router". Below the header, the title "Authorization Required" is displayed in bold. Underneath the title, a subtitle reads "Please enter your username and password." There are two input fields: "Username" with the value "root" and "Password" with a masked password "*****". Below the input fields, there are two buttons: "Login" with a green checkmark icon and "Reset" with a red X icon. At the bottom of the page, there is a footer that reads "Powered by LuCi Master (git-15.137.54403-f67d39e) / OpenWrt Designated Driver r49022".

2. Web Administration user interface

2.1 Dashboard (Main page)

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

M2M-Router Status ▾ System ▾ Router ▾ Network ▾ Logout AUTO REFRESH ON

Status

System

Hostname	M2M-Router
Model	Atmel AT91SAM9X25-EK
Firmware Version	OpenWrt Designated Driver r49022 / LuCI Master (git-15.137.54403-f67d39e)
Build Date	2017-04-25 16:58:17.010047729+02:00
Kernel Version	4.4.4
STM32 Firmware	201701173
Local Time	Tue Apr 25 15:38:09 2017
Uptime	0h 38m 25s
Load Average	0.40, 0.29, 0.36

Memory

Total Available	100800 kB / 125560 kB (80%)
Free	99244 kB / 125560 kB (78%)
Buffered	2556 kB / 125560 kB (2%)

Network

Modem Model	HE910-GL
IMEI	351580050521737
SIM ID	8936200003250172672
Modem RSSI	8
Modem SQ	2
CREG	2,1,"1204","1CD3FE4",2
COPS	0,0,"Telenor HU",2

IPv4 WAN Status

	Type: 3g
	Address: 172.31.158.141
	Netmask: 255.255.255.255
	Gateway: 172.31.158.141
	DNS 1: 192.168.1.225
	Connected: 0h 38m 18s

At the **Network** part you can identify the **Modem model**, the modem identifier (**IMEI**), the SIM ICC identifier (**SIM ID**), and the **Modem RSSI** (signal strength) and **Modem SQ** (signal quality as CSQ) with the **IPv4 WAN status** the network connection **Type** and its connection to the public Internet.

2.3 Menu

By the menu you can access the following features:

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

2.4 Status menu

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

The screenshot shows the LuCI interface for an M2M-Router. The top navigation bar includes 'M2M-Router', 'Status', 'System', 'Router', 'Network', and 'Logout', along with an 'AUTO REFRESH ON' button. The 'Status' menu is expanded, showing options: Overview, Firewall, Routes, System Log, Kernel Log, Processes, and Realtime Graphs. The main content area displays system information:

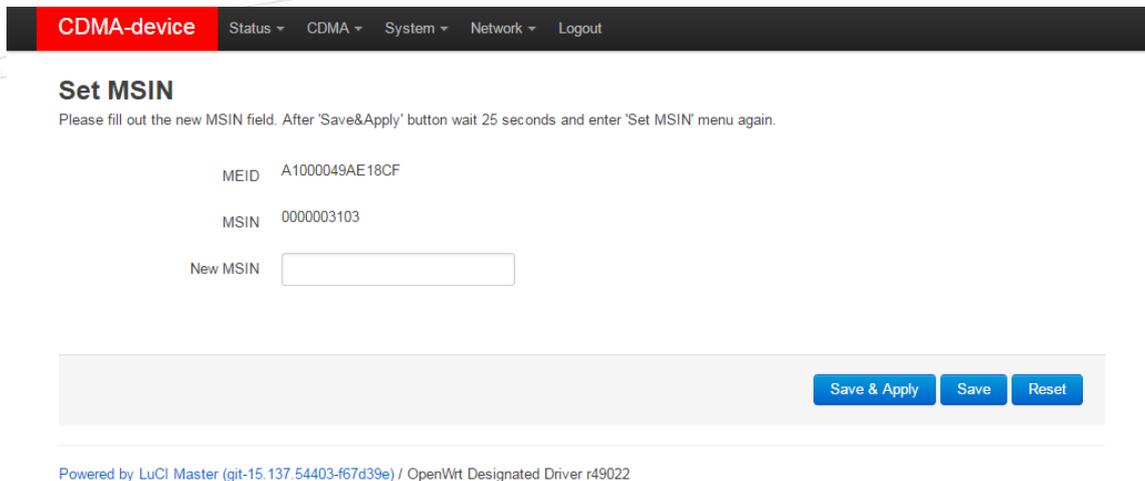
Hostname	M2M-Router
Model	Atmel AT91SAM9X25-EK
Firmware Version	OpenWrt Designated Driver r49022 / LuCI Master (git-15.137.54403-f67d39e)

2.5 CDMA menu (only for CDMA devices)

The modem's **MSIN identifier** can be configured here: [CDMA/Set MSIN.](#)

The screenshot shows the LuCI interface for a CDMA-device. The top navigation bar includes 'CDMA-device', 'Status', 'CDMA', 'System', 'Network', and 'Logout', along with an 'AUTO REFRESH ON' button. The 'Status' menu is expanded, showing options: Overview, Firewall, Routes, System Log, Kernel Log, Processes, and Realtime Graphs. The main content area displays system information:

Hostname	CDMA-device
Model	Atmel AT91SAM9X25-EK
Firmware Version	OpenWrt Designated Driver r49022 / LuCI Master (git-15.137.54403-f67d39e)

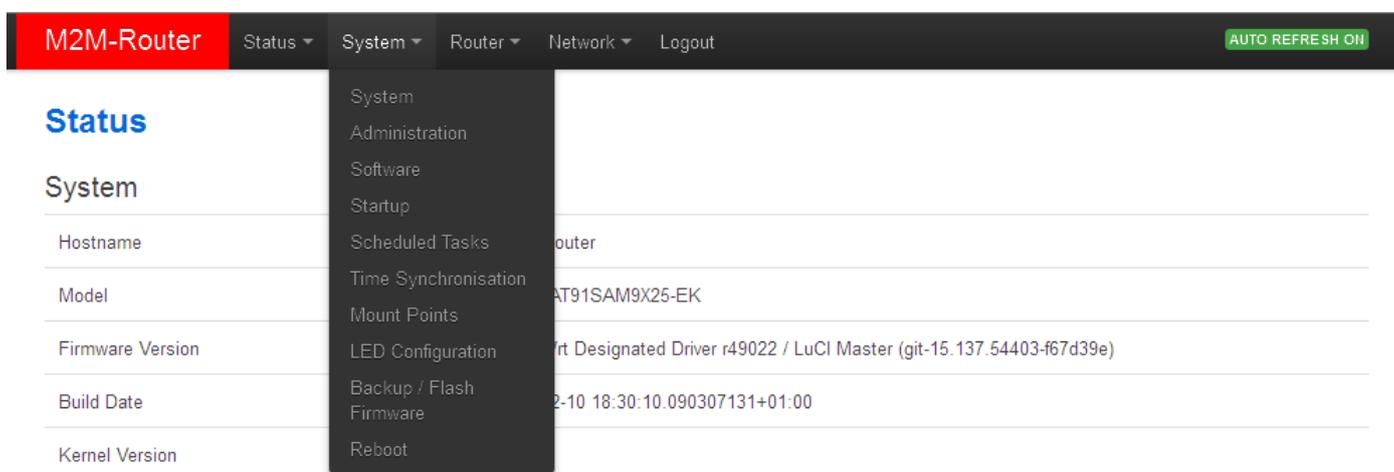


If you give a new **MSIN number**, then the WAN interface will be automatically configured for the router. This setting can be checked at the **Network/Interfaces** menu.

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

2.6 System menu

You can found several system settings in the **System** and **Administration** menu items.



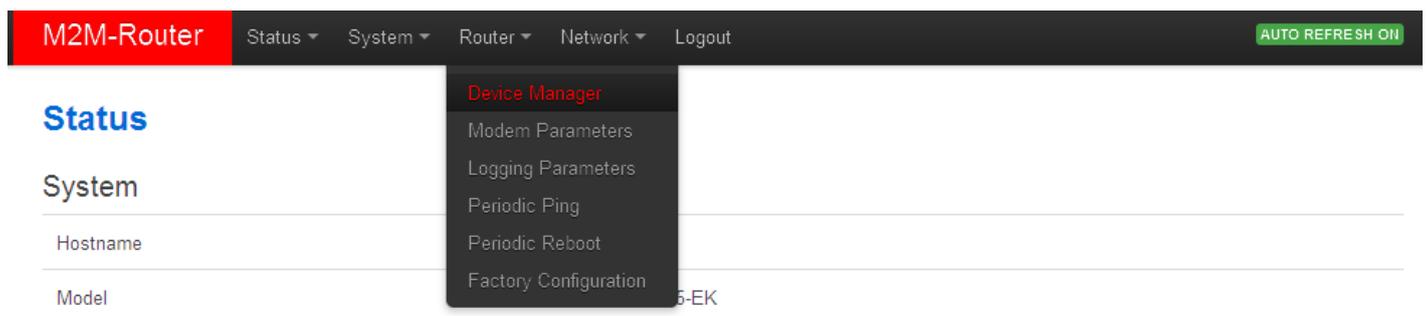
- Installation of further **Software** (3rd party tools, applications for the Linux distribution).
- You can define the **Startup** applicatons – resident programs during the operation and th **Scheduled Tasks**.
- Setup the NTP server for **Time Synchronisation**.
- The **Mount Points** are showing the available (mounted) shares and drives.

- The **LED Configuration** is also configurable.
- You also can **Backup / Flash firmware** updates even **Rebooting** the router device.

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

2.7 Router menu

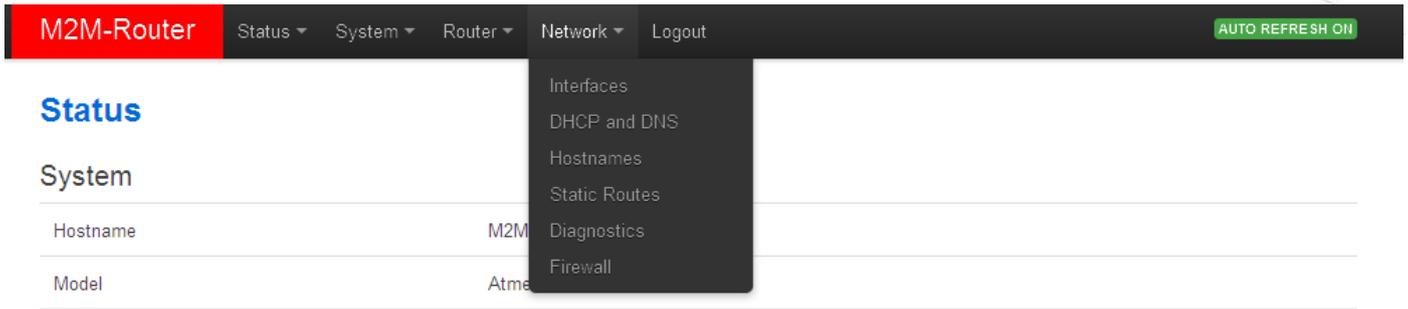
- You can define the remote monitoring software connection settings of the az **M2M Device Manager**.
- Then at the **Modem parameters** (define special parameters for the connection).
- Define the **Logging parameters**.
- At the **Periodic Ping** you can configure the cyclic heartbeat ping interval settings – as a network checking method feature.
- The daily router reboot can be allowed at the **Periodic Reboot** menu item.
- The backup of the factory settings is possible at the **Factory Configuration** (saves to a file).



2.8 Network menu

- Here you can configure the settings of each network **Interfaces**
- You can check the WiFi connected devices at the **WiFi** item.
- You can modify the **DHCP** and **DNS** settings,
- or define the router network device name at the **Hostname**.
- The **Static route** paths can be also defined.
- The **Firewall** rules can be declared here as the following submenu items: Port forward, IP router, NAT settings.

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



M2M-Router Status System Router Network Logout AUTO REFRESH ON

Status

System

Hostname	M2M
Model	Atme

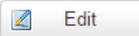
3. Network configuration of the router

3.1 Interface settings

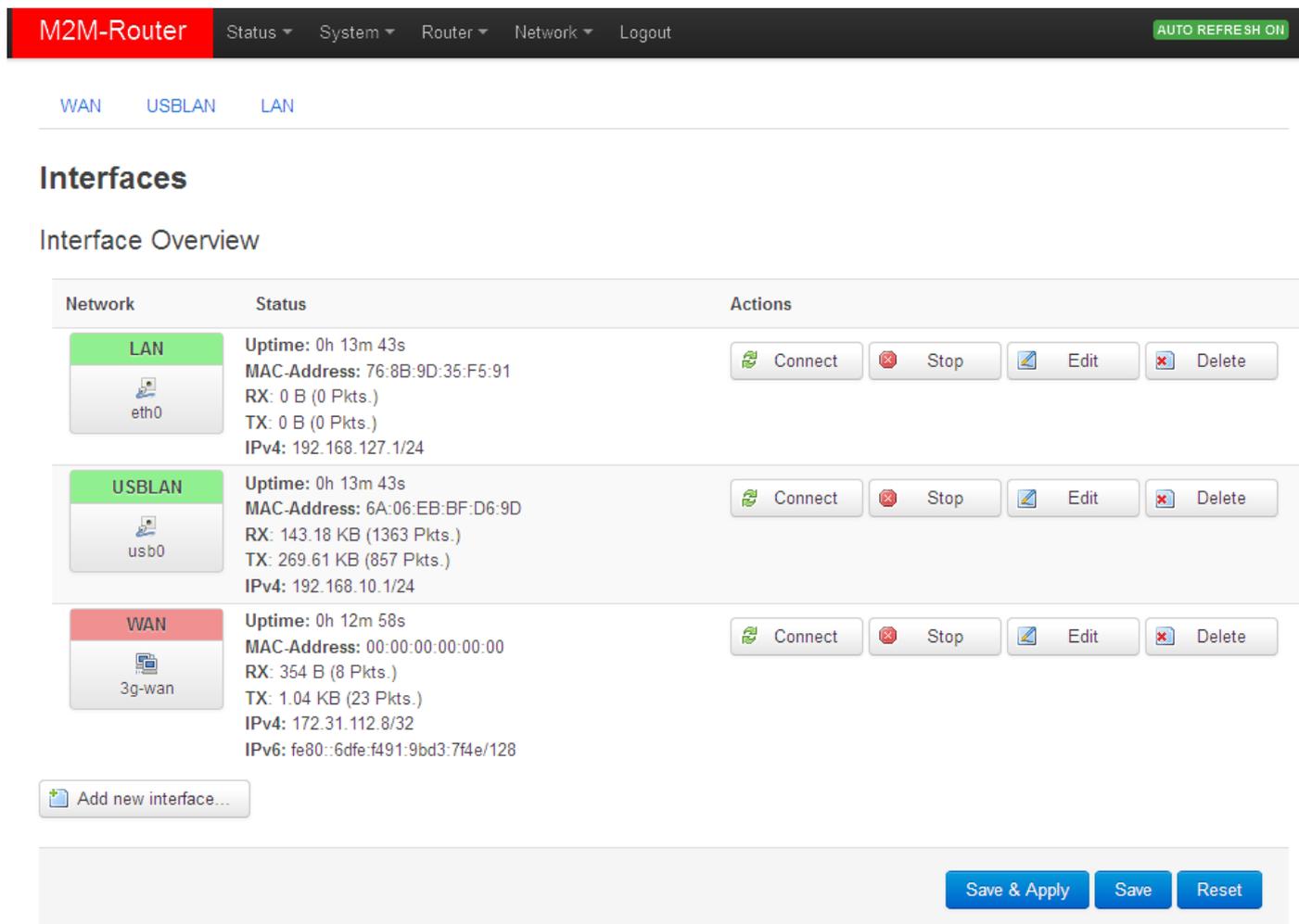
The list of the available network interfaces can be found at the **Interfaces / Interface Overview** menu item.

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

Modifying the interface settings

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

The **Stop** button stops the communication on the current interface, the  button reconnects the related interface connection. At the upper **WAN, USBLAN, LAN** title you will found further settings for the chosen Interface.



The screenshot shows the M2M-Router web interface. At the top, there is a navigation bar with 'M2M-Router' and menu items: Status, System, Router, Network, and Logout. An 'AUTO REFRESH ON' button is on the right. Below the navigation bar, there are tabs for 'WAN', 'USBLAN', and 'LAN'. The main content area is titled 'Interfaces' and 'Interface Overview'. It contains a table with three rows representing network interfaces: LAN, USBLAN, and WAN. Each row has columns for 'Network', 'Status', and 'Actions'. The 'Actions' column contains buttons for 'Connect', 'Stop', 'Edit', and 'Delete'. Below the table is an 'Add new interface...' button. At the bottom right, there are 'Save & Apply', 'Save', and 'Reset' buttons.

Network	Status	Actions
LAN eth0	Uptime: 0h 13m 43s MAC-Address: 76:8B:9D:35:F5:91 RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) IPv4: 192.168.127.1/24	Connect Stop Edit Delete
USBLAN usb0	Uptime: 0h 13m 43s MAC-Address: 6A:06:EB:BF:D6:9D RX: 143.18 KB (1363 Pkts.) TX: 269.61 KB (857 Pkts.) IPv4: 192.168.10.1/24	Connect Stop Edit Delete
WAN 3g-wan	Uptime: 0h 12m 58s MAC-Address: 00:00:00:00:00:00 RX: 354 B (8 Pkts.) TX: 1.04 KB (23 Pkts.) IPv4: 172.31.112.8/32 IPv6: fe80::6dfe:f491:9bd3:7f4e/128	Connect Stop Edit Delete

Add new interface...

Save & Apply Save Reset

3.2 Mobile internet settings (modem)

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

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

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

M2M-Router Status ▾ System ▾ Router ▾ Network ▾ Logout AUTO REFRESH ON

WAN USBLAN LAN

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	 3g-wan	Uptime: 0h 15m 29s MAC-Address: 00:00:00:00:00:00 RX: 354 B (8 Pkts.) TX: 1.04 KB (23 Pkts.) IPv4: 172.31.112.8/32 IPv6: fe80::6dfe:f491:9bd3:7f4e/128
--------	--	---

Protocol	UMTS/GPRS/EV-DO ▾
Modem device	/dev/ttyACM3 ▾
Service Type	UMTS/GPRS ▾
Mobile country code	<input type="text"/>
Mobile network code	<input type="text"/>
Dual SIM	<input type="checkbox"/>
SIM #1 APN	<input type="text" value="wm2m"/>
SIM #1 PIN	<input type="text"/>
SIM #1 PAP/CHAP username	<input type="text" value="root"/>
SIM #1 PAP/CHAP password	<input type="password" value="•••••"/>
Dial number	<input type="text" value="*99***1#"/>

Configure the module to the wireless internet and for the 2G/3G/LTE network connection (by the modem type and network behaviour) here for the **WAN** interface.

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

The international country codes can be found here: <http://mcc-mnc.com>

Ask your mobile operator about the available international settings.

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

Attention!

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

Here you will find some examples for the APN settings.

M2M APN (enclosed)

APN name: wm2m

SIM #1 APN

wm2m

Public Internet APN (opened)

APN name: net

SIM #1 APN

net

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

Automatic mode

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

Authentication

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

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

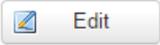
Attention!

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

3.3 Ethernet (LAN) settings

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

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

the **LAN** interface  button.

Change the default 192.168.127.1 router **IPv4 address** to an own IP address, regarding the current subnet. Check the **IPv4 netmask** to be proper for the selected and required network class which you are attempted to use.

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

Advanced Settings

Physical Settings

Firewall Settings

Status



eth0

Uptime: 0h 43m 41s

MAC-Address: 0E:64:1B:3E:B0:87

RX: 666.23 KB (6330 Pkts.)

TX: 1.59 MB (5863 Pkts.)

IPv4: 192.168.127.1/24

Protocol

Static address

IPv4 address

192.168.127.1

IPv4 netmask

255.255.255.0

IPv4 gateway

IPv4 broadcast

Use custom DNS servers

IPv6 assignment length

disabled

Assign a part of given length of every public IPv6-prefix to this interface

IPv6 address

IPv6 gateway

IPv6 routed prefix

Public prefix routed to this device for distribution to clients.

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

Important!

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

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

Protocol, the *DHCP client* setting, and push the  button.

Then the DHCP client will be activated for ethernet interface.

WAN USBLAN LAN

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



eth0

Uptime: 0h 4m 49s
MAC-Address: 76:8B:9D:35:F5:91
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 192.168.127.1/24

Protocol DHCP client

Really switch protocol?

DHCP Server

General Setup

IPv6 Settings

Ignore interface Disable DHCP for this interface.

Push the **Save & Apply** button for performing the changes.

3.4 DHCP, DNS settings

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

The DHCP settings can be found at the **Network** menu, **DHCP and DNS** item.

DHCP Server

General Setup

IPv6 Settings

Ignore interface Disable DHCP for this interface.

[Back to Overview](#)

Save & Apply

Save

Reset

Important!

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

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

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

DHCP Server

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.

Leasetime

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

[Back to Overview](#)

Save & Apply

Save

Reset

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

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

M2M-Router Status System Router Network Logout **AUTO REFRESH ON!**

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 Don't forward DNS-Requests without DNS-Name

Authoritative This is the only DHCP in the local network

Local server
Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only

Local domain
Local domain suffix appended to DHCP names and hosts file entries

Log queries Write received DNS requests to syslog

DNS forwardings
List of DNS servers to forward requests to

Rebind protection Discard upstream RFC1918 responses

Allow localhost Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist
List of domains to allow RFC1918 responses for

Active DHCP Leases

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

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

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

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

3.5 DNS settings

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

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](#)

- [Filter private](#) [Do not forward reverse lookups for local networks](#)
- [Filter useless](#) [Do not forward requests that cannot be answered by public name servers](#)
- [Localise queries](#) [Localise hostname depending on the requesting subnet if multiple IPs are available](#)
- [Expand hosts](#) [Add local domain suffix to names served from hosts files](#)
- [No negative cache](#) [Do not cache negative replies, e.g. for not existing domains](#)
- [Additional servers file](#)
[This file may contain lines like 'server=/domain/1.2.3.4' or 'server=1.2.3.4' for domain-specific or full upstream \[DNS\]\(#\) servers.](#)
- [Strict order](#) [DNS servers will be queried in the order of the resolvfile](#)
- [Bogus NX Domain Override](#) [List of hosts that supply bogus NX domain results](#)
- [DNS server port](#)
[Listening port for inbound DNS queries](#)
- [DNS query port](#)
[Fixed source port for outbound DNS queries](#)
- [Max. DHCP leases](#)
[Maximum allowed number of active DHCP leases](#)
- [Max. EDNS0 packet size](#)
[Maximum allowed size of EDNS.0 UDP packets](#)
- [Max. concurrent queries](#)
[Maximum allowed number of concurrent DNS queries](#)

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

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

3.6 Defining the route rules

In the **Network** menu, **Static routes** item you can define the rules for the current routing.

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

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

Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
	Host-IP or Network	if target is a network			
This section contains no values yet					

 Add

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
	IPv6-Address or Network (CIDR)			
This section contains no values yet				

 Add

Save & Apply

Save

Reset

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

3.7 Firewall settings

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

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

Important!

*It is offered to check the network traffic on the router. Check the connections, the active communication channels (port number, incoming IP) and listen the incoming activities and for sure the output traffic! These all you can check in the **Status** menu, **Realtime Graphs** item at the **Connections** tab – where these can be listed.*

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

M2M-Router

[Status](#) ▾
 [System](#) ▾
 [Router](#) ▾
 [Network](#) ▾
 [Logout](#)
AUTO REFRESH ON

[Load](#)
[Traffic](#)
[Wireless](#)
Connections

Realtime Connections

This page gives an overview over currently active network connections.

Active Connections

(3 minute window, 3 second interval)

<u>UDP</u> : 3	Average: 2	Peak: 3
<u>TCP</u> : 2	Average: 1	Peak: 2
<u>Other</u> : 0	Average: 0	Peak: 0

Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.10.2:59104	192.168.10.1:8888	74.03 KB (218 Pkts.)
IPV4	TCP	192.168.10.2:59105	192.168.10.1:8888	5.91 KB (93 Pkts.)
IPV4	UDP	192.168.10.2:137	192.168.10.255:137	1.83 KB (24 Pkts.)
IPV4	UDP	172.31.158.141:39342	192.168.1.225:53	201 B (2 Pkts.)
IPV4	UDP	172.31.158.141:123	84.2.44.19:123	76 B (1 Pkts.)

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

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

Firewall Status

IPv4 Firewall

IPv6 Firewall

Reset Counters

Restart Firewall

Table: Filter

Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
18	1.32 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
2096	244.20 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 /* user chain for input */
1915	231.03 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate RELATED,ESTABLISHED
0	0.00 B	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 ctstate INVALID
36	1.83 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	ID:66773300 tcp flags:0x17/0x02
0	0.00 B	zone_wan_input	all	3g-wan	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
0	0.00 B	zone_lan_input	all	eth0	*	0.0.0.0/0	0.0.0.0/0	ID:66773300
181	13.17 KB	zone_lan_input	all	usb0	*	0.0.0.0/0	0.0.0.0/0	ID:66773300

Another method for limitation can be the whole disabling with opening and enabling only the necessary communication ports, IP-segments or allowing exact IPs.

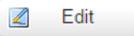
You can modify the firewall settings at the **Network** menu, at the **Firewall** item, **General Settings** tab.

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

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

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

At the **Zones** part you can  a new rule to the current ones. You also can  or

 an existed rule.

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

Output

Forward

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
wan: wan:  = lan	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 Edit  Delete
lan: lan:  usblan:  = wan	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input type="checkbox"/>	<input type="checkbox"/>	 Edit  Delete
 Add						

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

When you are attempted to add a new firewall rule, it must be performed very carefully, because you can disable or tilt ports communication which are used by the router or some network services by general (e.g. Port nr. 67 is necessary for the DHCP service and 80 port for the, etc).

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

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

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

Firewall - Zone Settings - Zone "wan"

Zone "wan"

This section defines common properties of "wan". 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.

Restrict to address family

Restrict Masquerading to given source subnets

Restrict Masquerading to given destination subnets

Force connection tracking

Enable logging on this zone

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from "wan"**. *Source zones* match forwarded traffic from other zones **targeted at "wan"**. 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.

Allow forward to *destination* zones: lan:

Allow forward from *source* zones: lan:

[Back to Overview](#)

Save & Apply

Save

Reset

The firewall can be configured by default to allow or tilt the communication – according to the chosen settings.

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

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

[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	Sort
------	-------	--------	--------	------

This section contains no values yet

Open ports on router:

Name	Protocol	External port
------	----------	---------------

<input type="text" value="New input rule"/>	TCP+UDP ▾	<input type="text"/>	<input type="button" value="Add"/>
---	-----------	----------------------	------------------------------------

New forward rule:

Name	Source zone	Destination zone
------	-------------	------------------

<input type="text" value="New forward rule"/>	lan ▾	wan ▾	<input type="button" value="Add and edit..."/>
---	-------	-------	--

3.8 Port Forward settings

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

[General Settings](#)[Port Forwards](#)[Traffic Rules](#)[Custom Rules](#)

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

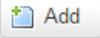
Name	Match	Forward to	Enable	Sort
------	-------	------------	--------	------

This section contains no values yet

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
------	----------	---------------	---------------	---------------	---------------------	---------------

<input type="text" value="New port forward"/>	TCP+UDP ▾	wan ▾	<input type="text"/>	lan ▾	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
---	-----------	-------	----------------------	-------	----------------------	----------------------	------------------------------------

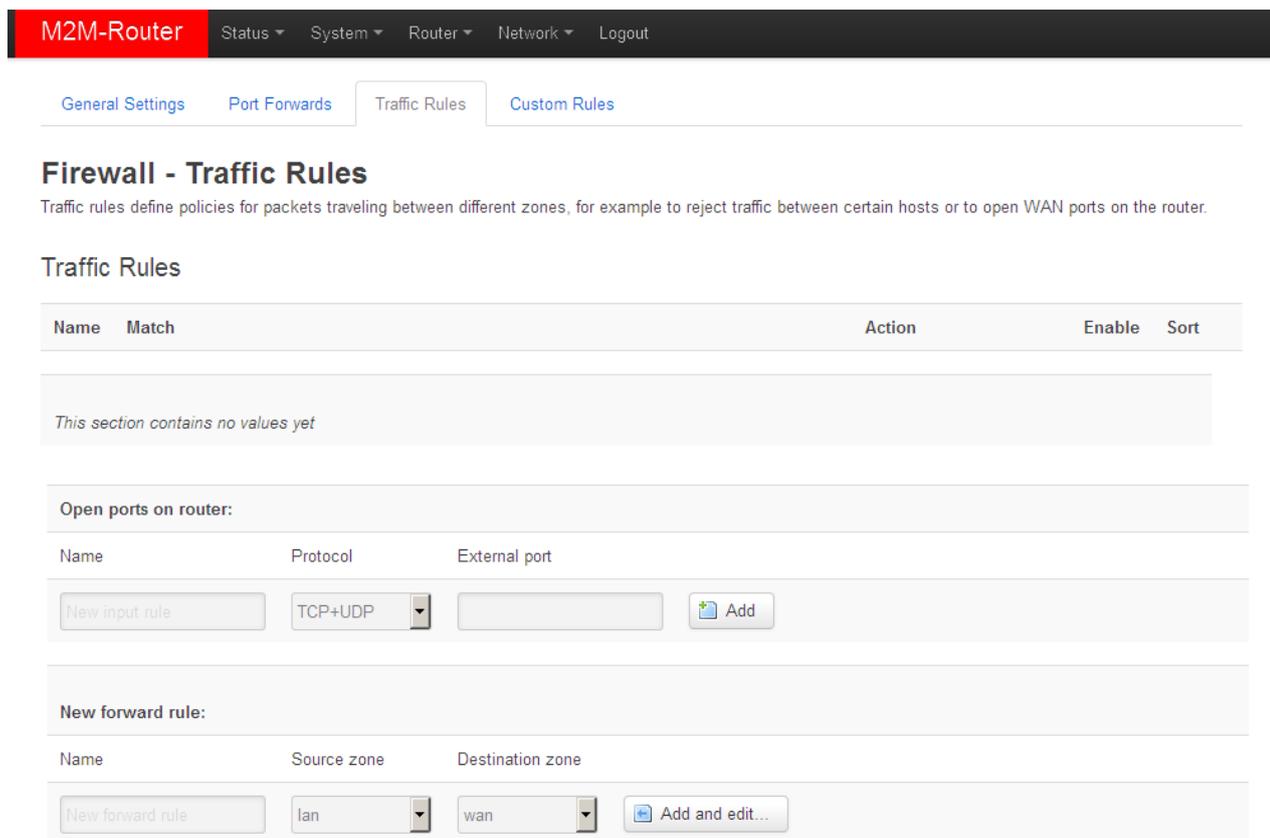
You can add a new rule by the  button.

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

3.9 IP routing, NAT settings

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

You can add a new rule by the  button.



The screenshot shows the M2M-Router web interface. The top navigation bar includes 'M2M-Router', 'Status', 'System', 'Router', 'Network', and 'Logout'. Below this, there are tabs for 'General Settings', 'Port Forwards', 'Traffic Rules', and 'Custom Rules'. The main heading is 'Firewall - Traffic Rules', with a sub-heading 'Traffic Rules' and a description: '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.' Below this, there is a table with columns 'Name', 'Match', 'Action', 'Enable', and 'Sort'. The table is currently empty, with a message 'This section contains no values yet'. Below the table, there are two sections: 'Open ports on router:' and 'New forward rule:'. The 'Open ports on router:' section has a table with columns 'Name', 'Protocol', and 'External port'. The 'Name' column has a text input field with 'New input rule', the 'Protocol' column has a dropdown menu with 'TCP+UDP' selected, and the 'External port' column has a text input field. There is an 'Add' button to the right. The 'New forward rule:' section has a table with columns 'Name', 'Source zone', and 'Destination zone'. The 'Name' column has a text input field with 'New forward rule', the 'Source zone' column has a dropdown menu with 'lan' selected, and the 'Destination zone' column has a dropdown menu with 'wan' selected. There is an 'Add and edit...' button to the right.

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

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

The **Source NAT** settings can be performed for each protocol (tcp, udp), that the router allows the redirection of data –which incoming IP address and port must be redirected to which outgoing IP address and port and must be forwarded the data traffic. You also can define a port range, hereby.

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	Sort
This section contains no values yet				
New source NAT:				
Name	Source zone	Destination zone	To source IP	To source port
<input type="text" value="New SNAT rule"/>	<input type="text" value="lan"/>	<input type="text" value="wan"/>	<input type="text" value="Do not rewrite"/>	<input type="text" value="Do not rewrite"/>
<input type="button" value="Add and edit..."/>				

These rules must always be defined, not disallowing the general communication and must consider that the router must be further available on the network. It is easy to enclose the router from the network or disabling the remote access. Please, be careful when configure these settings.

Important!

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

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

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

3.10 Dynamic DNS settings

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

New settings can be by the button or the current can be -ed.

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

4. Special settings

4.1 M2M Device Manager settings

The further router parameters can be easily and remotely configured by the az *M2M Device Manager*[®] server application. It is also capable of performing remote monitoring and firmware updates.

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

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

The default DM Port number is 443.

These must be also configured in the Device Manager and the router must access the IP address of the M2M Device Manager. You can check it by performing a ping.

The screenshot shows the web interface for M2M-Router-PRO. At the top, there is a navigation bar with the following items: M2M-Router-PRO (highlighted in red), Status, System, Router, Services, Network, and Logout. Below the navigation bar, the page title is "Device Manager Parameters" with a subtitle "Carefully change the parameters." The configuration area contains several input fields and checkboxes:

- DM Name: Input field containing "something".
- DM User Name: Input field containing "root".
- DM IP Address: Empty input field.
- DM Port Number: Empty input field.
- Static WAN IP Address: Checked checkbox with a tooltip "Disable WAN up CALL".
- CALL Timeout: Input field containing "30" with a tooltip "Next CALL when sending fails".

At the bottom right of the configuration area, there are three buttons: "Save & Apply", "Save", and "Reset".

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

4.2 Monitoring the modem

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

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

M2M-Router Status System Router Network Logout

Modem Parameters

Watchdog timeout (>300) [s]

Maximum RSSI error count in 10s increments

Debug level

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

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

4.3 Ping an IP address

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

M2M-Router Status System Router Network Logout

Diagnostics

Network Utilities

IPv4 IPv4

Important!

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

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

4.4 Network Time Service (NTP)

Open the **System** menu, **Time Synchronisation** item.

You can add hereby the refresh interval at the **Update interval (in seconds)**.

You can define the time synch at the **Clock Adjustment**.

M2M-Router Status System Router Network Logout

Time Synchronisation

Synchronizes the system time

General

Current system time Fri Feb 10 17:38:06 2017

Update interval (in seconds)

Count of time measurements

empty = infinite

Clock Adjustment

Offset frequency

Time Servers

Hostname	Port	
<input type="text" value="0.openwrt.pool.ntp.org"/>	<input type="text" value="123"/>	<input type="button" value="Delete"/>
<input type="text" value="1.openwrt.pool.ntp.org"/>	<input type="text" value="123"/>	<input type="button" value="Delete"/>
<input type="text" value="2.openwrt.pool.ntp.org"/>	<input type="text" value="123"/>	<input type="button" value="Delete"/>
<input type="text" value="3.openwrt.pool.ntp.org"/>	<input type="text" value="123"/>	<input type="button" value="Delete"/>

At the **Time Servers** part you can  NTP time servers by its **Hostname**, IP-address or server name, and **Port**. When you have modified the settings, save by **Save & Apply** button.

4.5 TFTP service settings

Open the **Network** menu, **DHCP and DNS** item, **TFTP settings** tab to allow the TFTP service (**Enable TFTP server**), and the related further parameters.

M2M-Router Status ▾ System ▾ Router ▾ Network ▾ Logout AUTO REFRESH ON

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

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>			

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 to the fixed address to use and the *Hostname* is assigned as 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	IPv6-Suffix (hex)
<i>This section contains no values yet</i>				



Save & Apply **Save** **Reset**

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

4.6 Identifying names connecting machines

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

4.7 LED configuration

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

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

- *led2g* – LED2 green light
- *led1r* – LED1 red light
- *led2r* – LED2 red light
- *led3r* – LED3 red light

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

M2M-Router Status System Router Network Logout

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

Add

Save & Apply Save Reset

The **Trigger** allows to choose an event type of operation. E.g. *netdev* menads the network interface connection type, and **Device** identifies the related network interface.

You can  the LED setting.

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

5. Software refresh and router maintenance

5.1 Firmware refresh

1. Open the **System** menu, **Backup / Flash firmware** item.
2. Browse the *fwos-....* compressed file then push to the **Flash image** button.



Flash operations



Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).



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



Flash new firmware image

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



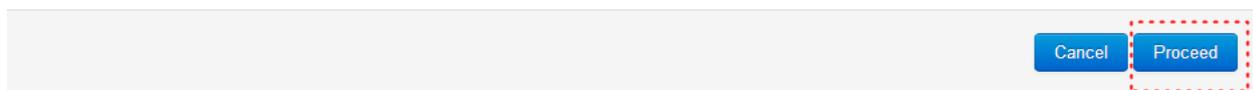
3. A new window will appear where the file will be checked. When it is okay, the system refreshment is possible by the **Proceed** button.



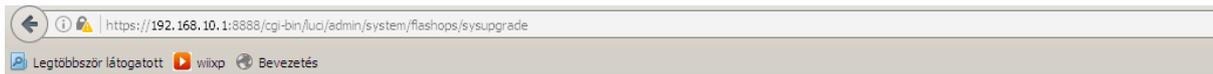
Flash Firmware - Verify

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: `E044fa9c7c4d592c2fbc100b168bf29e`
- Size: 4.46 MB



- Then the next message appears on the screen in the browser. Then the refresh method has started, while the **LED2** and **LED3** is continuously lighting by **red**.



System - Flashing...

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...

- Later the **LED2** will be blank and only the **LED3** lighting with **red**.
- At the end of the installation – the LEDs are not lighting further – the system restarting twice while **all the three LEDs** are continuously lighting with **green**, then the OpenWrt system will be loaded as it was described before.

Important!

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

- When the middle **Cell LED** is lighting continuously in **green**. Login to main page and check the software version!

5.2 Installing applications

Open the **System / Software** menu.

Important!

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

You can refresh the catalog of the available applications by the **Update lists** button.

When it was successful, fill the name of the application you are attempted to install at the **Download and install package** field (e.g. MC – Midnight Commander esetében), and push to the **OK** button for the installation – regarding the upcoming hints on the screen. The installed packages of the router are listed lower at the **Status** part.

M2M-Router Status System Router Network Logout

Software

Actions Configuration

No package lists available

Free space: 93% (652.00 KB)

Download and install package:

Filter:

Status

Installed packages Available packages

	Package name	Version
Remove	base-files	168-r49022
Remove	block-mount	2016-01-10-96415afece..d21
Remove	busybox	1.24.1-2

5.3 Restarting the router

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

M2M-Router Status System Router Network Logout

Reboot

Reboots the operating system of your device

5.4 Reset

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

Important!

Configure the router on its web user interface!

5.5 Password change

Open the **System / Administration** menu.

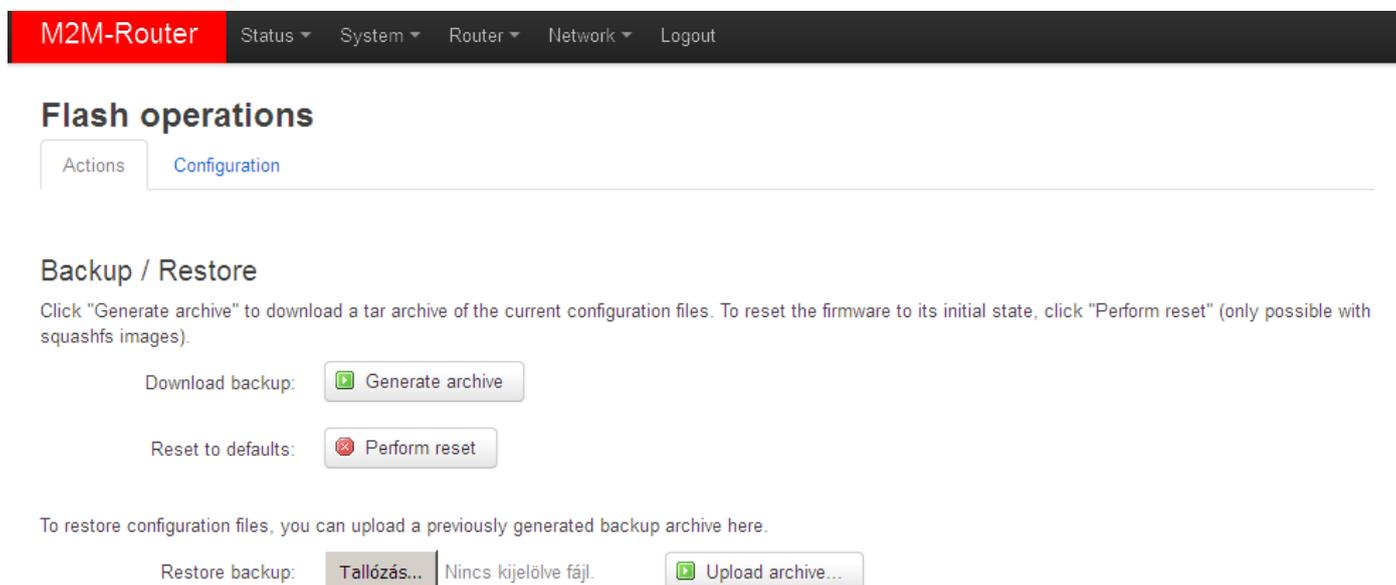
At the **Router password** you can fill the new **Password** and again to the **Confirm password** fields. You will be able to login further by this new password.

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

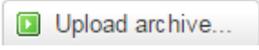
5.6 Backup and restore of settings

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

At the **Backup / Restore** part and **Download backup** feature push the  button for saving the settings into a file.



The screenshot shows the M2M-Router web interface. At the top, there is a navigation bar with the title "M2M-Router" and several menu items: "Status", "System", "Router", "Network", and "Logout". Below the navigation bar, the main content area is titled "Flash operations". Under this title, there are two tabs: "Actions" and "Configuration". The "Configuration" tab is active. Below the tabs, the section is titled "Backup / Restore". A paragraph of text explains the "Generate archive" and "Perform reset" buttons. There are two rows of buttons: "Download backup:" with a "Generate archive" button, and "Reset to defaults:" with a "Perform reset" button. Below this, another paragraph explains the "Restore backup" feature. There is a "Restore backup:" label, a file selection button labeled "Tallózás...", and an "Upload archive..." button. The text "Nincs kijelölve fájl." is visible between the file selection button and the upload button.

The **Restore backup** is possible to reload – a previously saved configuration – when you will be able to browse and load from your computer to the router memory by pushing the  button.

5.7 Handle of memory cards

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

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

6. Troubleshooting

LED activities

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

In case of LED blinking after restart

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

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

Power supply

Check that the router that it has its power source through its microfit connector (**POWER**). If it does not, then reconnect the power cable. When it has its power source the LED signals will sign it. In this case please wait for 2-3 minutes, while the router will register to the network then check the life signals in the *Element Manager*. *When the power source will be added, all the three LEDs will light for a short period, then the **LED1** (green) will light for 2 minutes, then after that only blinks once in every 10 seconds. The router is booting and just started.*

Cable connection

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

Continuous restarting...

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

Starting up the router

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

Antenna

Check or connect proper SMA fit antenna to the **Antenna** connector and mount it to the interface. The router must send and assure proper RSSI signal value and life signals for the *Element Manager*.

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

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

SIM/APN failure

It means a SIM or APN failure, if the **LED2** will not light for minutes. If the device is not registering to the network, then the modem was not initiated properly, and the router will restart itself after 10 minutes.

This could caused by a not proper APN setting – or in case of CDMA version the wrong MSIN setting (you can configure it on the local web user interface).

Connection to the router, checking the connection

Download and install the driver for the mini USB cable connection from the M2M website before using the connection:

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

Unpack the downloaded zipped file and install the driver. After you've connected the USB cable you can add the driver at the Windows / **Start / Control Panel / System / Device Manager**.

Find the **Network Cards**, extend it and you will find the „**USB Ethernet / RNDIS Gadget**“. Double click on the entry and choose the **Driver** tab, and the **Refresh** button, then browse the uncompressed file's directory then **Install** the driver.)

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

Configure the **USB-Ethernet interface** IP address on your PC for the „**USB Ethernet/RNDIS Gadget**“ and setup the next fixed ipv4 address: 192.168.10.1, subnet mask is: 255.255.255.0 – connect these settings.

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

When the router will not started ...

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

Cannot access the router on ssh or on the LuCi web interface

The DHCP service is turned off for the router Ethernet interface, by default. Therefore, you have to configure an IP address for your PC, manually. Add for e.g. 192.168.127.10 IP address to your computer's Ethernet interface for connecting to the router.

(If you have the WiFi onboard version of the router, then you can configure your router on WiFi (DHCP activated).

For accessing the web user interface we offer the Mozilla Firefox web.

Default web user interface (LuCi) address is: <https://192.168.127.1:8888>

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

Allow the accessing of the router default IP address in your browser by pushing to the Special button, then allow the safety exclusion into the pop-up window.

7. Support availability

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

E-mail: support@m2mserver.com

Telephone: +36203331111

7.1 Contact the support line

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

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

M2M-Router Status ▾ System ▾ Router ▾ Network ▾ Logout AUTO REFRESH ON

Status

System

Hostname	M2M-Router
Model	Atmel AT91SAM9X25-EK
Firmware Version	OpenWrt Designated Driver r49022 / LuCI Master (git-15.137.54403-f67d39e)
Build Date	2017-02-10 18:30:10.090307131+01:00
Kernel Version	4.4.4
STM32 Firmware	201604191
Local Time	Fri Feb 10 18:10:24 2017
Uptime	0h 38m 7s
Load Average	0.27, 0.23, 0.27

Memory

Total Available	101404 kB / 125560 kB (80%)
Free	98936 kB / 125560 kB (78%)
Buffered	2468 kB / 125560 kB (1%)

Network

Modem Model	HE910-GL
Modem RSSI	8

7.2 Product support

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

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

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

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

Online product support can be required here:

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

8. Legal notice

©2017. WM Systems LLC.

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

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

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

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

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

Warning

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