MC-MR-L2

User‘s guide

LTE Cat 4 | **WLAN** | **GNU/Linux** | **RS-232 or RS-485** | **USB 2.0** | **Optional GNSS**

Document revision 1.0

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

Table of contents

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

1 Introduction

Thank you for choosing an MC Technologies product.

The MC-MR-L2 are a family of LTE Cat 4 routers optimized for M2M and IoT applications.

They support LTE Cat 4 as well as EDGE and GSM/GPRS and optionally WLAN and GNSS location services (WLAN and GNSS functionality must be ordered explicitly).

These instructions enable the safe and efficient handling of the product. The instructions are an integral part of the product and must be kept accessible at all times to installation, maintenance, commissioning, and operating persons.

1.1 Warranty provisions

Unauthorized use, non-observance of this documentation, the operation or maintenance by insufficiently qualified persons, and unauthorized modifications exclude the manufacturer's liability for resulting damages. Any modification to the device will void the manufacturer warranty. The provisions of our General Terms of Sale (AGB) apply. These can be found on our website:

https://mc-technologies.com/en/agb-aeb/

2 Safety instructions

The safety and maintenance instructions must be strictly followed to ensure safe operation of the product. In addition to the safety and maintenance instructions, the individual sections of this document contain descriptions of procedures and operation instructions with safety-critical information.

General safety regulations and local guidelines for the area of application of the device as well as for the prevention of accidents must be followed strictly.

Only the consideration of all safety guidelines ensures protection of persons and the environment against hazards and the safe and trouble-free operation of the product.

2.1 Technical limits

The product is exclusively intended for use within the technical limitations and maximum ratings specified in this document. The following limitations must be observed in particular:

- The maximum air humidity must not be exceeded, and condensation must be avoided.
- The supply voltage must be within limits.
- The maximum input voltage must not be exceeded.
- The maximum switching voltage and current must not be exceeded.
- The ambient temperature must not be exceeded or dropped below limits.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

2.2 Safety precautions

	**Electrostatic discharges, short circuits and voltage spikes increase the risk of fire, cause damage to the product and may cause bodily harm.** Observe the general precautions for handling electrostatically sensitive components. Turn off the power before performing any work on an electric device. Ensure a suitable surge protection is installed. Do not operate the device with visible or otherwise known damage.
	**Damage due to improper handling, repairs and modifications increase the risk of fire, cause damage to the product and may cause bodily harm.** It is not permitted to open the product for repair work or modifications beyond the removal and insertion of the provided plug-in cards. Ensure power accessory is well-suited for the purpose. Keep the device away from children and animals to prevent hazards like choking of parts and danger due to biting.
	**Dust, debris, moisture and liquids from the surrounding area could get inside the product and increase the risk of fire, cause damage to the product and may cause bodily harm.** The product must not be used in humid environments or in the immediate vicinity of water or other liquids. Install the product in a clean, dry place protected from splashing water, dust and debris that could enter the device.
	**Open flames, harsh chemicals and flammables including aerosols increase the risk of fire, cause damage to the product and may cause bodily harm.** The product must be kept away from direct sunlight, open flames, harsh chemicals, flammables, explosives, aerosols.
	**Extreme temperatures, insufficient heat dissipation or ventilation increase the risk of fire, cause damage to the product and may cause bodily harm.** Operate the device in a well-ventilated area away from direct sunlight. Do not enclose or cover the device or its ventilation holes to allow heat dissipation. The device must be operated well within the operating temperature limits.
	**Strong magnetic or electric fields, vibrations and shocks cause malfunctions and may damage the device.** Keep the device away from electronic appliances that generate strong magnetic or electric fields, such as a microwave oven, radar, electrical motor or generator. Ensure the device is fixed properly and avoid high accelerations.
	**A too small distance between antennas and persons might affect their health.** Be aware that wireless devices may affect the performance of e.g. hearing aids or pacemakers. The antennas must be placed at least 20 cm away from persons during operation. If applicable, respect the rules and regulations for device operations set forth in hospitals and health care facilities.

2.3 Obligations of the operator

The operator must follow regional regulations regarding the operation, functional testing, repair and maintenance of electronic devices at all times.

2.4 Qualification of installers

Installation and maintenance of the product may only be carried out by trained authorised installers which possess the necessary levels of qualification to ensure safe maintenance and operation. The qualified installer must have read and understood this documentation and follow its guidelines and instructions.

The electrical installation and commissioning of the product may only be carried out by persons who, due to their specialist training, knowledge and experience including knowledge of the relevant standards and regulations, are able to carry out work on electrical systems and independently detect and avoid possible hazards.

2.5 Guidelines for transport and storage

The following guidelines must be observed:

- Do not expose the product to moisture or other potentially harmful environmental conditions (radiation, gases, etc.) during transport or storage.
- Protect the product from shocks during transport and storage, e.g. by using air-cushioned packaging.
- Before installing the product, check for possible damages that may have been caused by improper transport or storage. Damage in transit must be noted on the shipping documents. All claims for damages must be made immediately and before being handed to the carrier or company responsible for the storage or logistics respectively.

3 Product label

The label of the product is located on the side of the product. It may contain the following markings, among others:

3.1 Special waste

This symbol indicates that the device must be disposed of separately from residual waste at suitable collection points. Refer to the disposal section at the end of this manual.

3.2 CE marking

By affixing the CE marking, the manufacturer confirms that the product complies with the product-specific regulations of the European Union.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

4 Environmental protection

The disposal of the product and its packaging must be carried out in accordance with all relevant environmental protection regulations. Recycle responsibly by separating the packaging materials like cardboard and paper from plastic and use the dedicated waste collection systems. Refer to the disposal section at the end of this manual for instructions on how to dispose of the product.

5 Technical specifications

5.1 Physical characteristics and limitations

Physical characteristic / limitation	Value
Power supply	8 V … 30 V DC (min. 14 W output power required)*
Dimensions (W x H x D)	44 x 105 x 94 mm
Weight	~ 230 g (~ 4.23 oz)
Operating temperature	-20 °C to +70 °C
Housing material	Aluminium

** See section below for details on power supply requirements.*

5.2 Power supply requirements

The router can be operated using LPS power supplies with a supply voltage of 8 - 30V DC and a minimum rated output power of 14 W. The output power can be calculated as the product of voltage and current. E.g. a 12 V 1.2 A power supply would be suitable as its maximum power output is 12 V times 1.2 A which equals to 14.4 W

An LPS (Limited Power Source) is a fault-protected SELV power supply with an UOC (open circuit voltage) lower than the SELV circuit limits as defined in IEC 60950 and IEC 62368-1 (42.4 V AC, 60 V DC respectively).

5.3 Mobile network features

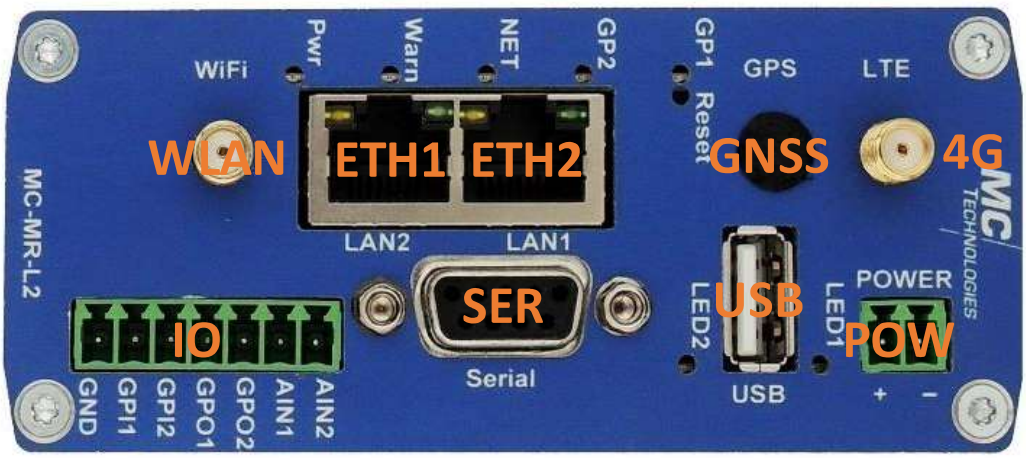
The router comes in different variants with different GSM modem modules. Please refer to the corresponding datasheet for information about technical specifications such as frequency bands, data throughput and other technical capabilities.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

6 Ports, display and operating elements

6.1 Ports



	Connector	Description
POW	Terminal socket	Power supply input
SER	DE-9 female	Either RS-232 or RS-485 interface depending on model variant
LTE	SMA female	GSM antenna connector
GNSS	(optional) SMA female	GNSS antenna connector
WLAN	(optional) SMA female	WLAN antenna connector
USB	USB type A socket	USB 2.0 host interface
IO GND	Terminal socket	Ground reference for IOs
IO ANI1/2	Terminal socket	0 to 10 V analog input (2 mA @ 10 V)
IO GPI1/2	Terminal socket	Digital input
IO GPO1/2	Terminal socket	Digital output

6.1.1 RS-232 port pinout

Port	Signal	Description
2	TXD (OUT)	Transmit line (of the modem)
3	RXD (IN)	Receive line (of the modem)
5	GND	Ground
7	RTR / RTS (IN)	Ready To Receive / Request To Send (Terminal is ready to receive)
8	CTS (OUT)	Clear To Send (Modem is ready to receive)

6.2 LED indicators

LED	Color	Description
Pwr	Green	Indicates if the power supply is working correctly
Warn	Red	Warning state (under voltage situation, system upgrade in progress, custom warning)
NET	Green	Modem status indicator (see table below)
GP1	Green	General purpose (customizable)
GP2	Green	General purpose (customizable)

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

6.2.1 NET LED signal patterns

This LED indicates the status of the integrated GSM module.

Blink pattern	Network Status
Off	Modem is inactive
Short interval (200ms on, 1800ms off)	Network search
Long interval (1800 ms on, 200 ms off)	Idle state
Flickering (125 ms on, 125 ms off)	Data transfer
Always on	Call in progress

6.3 Buttons

Name	Function
Reset	Used for resetting the router to factory defaults
User	Customizable

7 Installation

7.1 Antenna

Mount the supplied antenna to the SMA connector on the MC-MR-L2. Check whether the local network coverage of the mobile phone provider is sufficient.

Warning: Persons must be at least 20 cm away from the antenna during device operation.

7.2 Inserting the SIM card

Most variants come with an externally accessible Mini SIM card slot on the back panel. Otherwise a SIM card holder is located inside the housing. Switch off the power supply and remove all connection cables. Open the housing by loosening the screws and removing the back panel. The SIM card holder is unlocked by sliding and then lifting the holder.

7.3 Vehicle installation

The installation of the MC-MR-L2, its periphery such as cables and antennas as well as the electrical connections in a motor vehicle must be carried out by a qualified specialist workshop.

8 Software

8.1 OpenWrt

The operating system of the router family is based on OpenWrt. OpenWrt is a vastly customisable and expandable GNU/Linux distribution created by networking enthusiasts and professionals for like-minded people. Unleashing the full potential of OpenWrt requires the user to be willing to experiment and research as it is hardly possible to create a full-fledged topical guide.

Therefore, the configuration and application examples presented in this guide, can be considered no more than an introduction created by best effort with no liability for damages or any warranties for accurateness and topicality whatsoever.

8.2 Use of open-source software

This product includes open-source software, which was partially developed by third parties and distributed with a permissive license. The use of this software is royalty-free under the terms of the respective license. In case of a contradiction between our terms and the software license terms, the software license terms take priority as far as the software is affected.

The use of the open-source software is free of charge. We do not charge any usage fees or comparable fees for the open-source software contained in our products.

For retrieving a list of open-source software used in this product, please contact our support department (support@mc-technologies.com). Alternatively, a list of open-source software used can be found in the web interface in *System -> Software -> Installed*.

Customers may request the source code of software contained in our product, which license stipulates that the source code and/or modifications must be made available to the customer Examples of such licenses are the GNU General Public License (GPL), GNU Lesser General Public License (LGPL) and the Clarified Artistic License. We reserve the right to demand a compensation fee for the distribution costs of the source-code (e.g. postal fees and the cost of the medium).

8.3 Software development kit (SDK)

On request MC Technologies provides an SDK based on the OpenWrt SDK to customers for compiling and running their own software on the device.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

8.4 Liability for software

We however do not assume any warranty or liability for changes made to the software by the customer or third-parties or for the usage of the open-source software contained in our product in a way that does not comply with the intended use as described in the accompanying documentation or, if applicable, the contractually defined application purpose of the product.

This applies likewise to any use of the open-source software outside of our product.

9 Basic routines

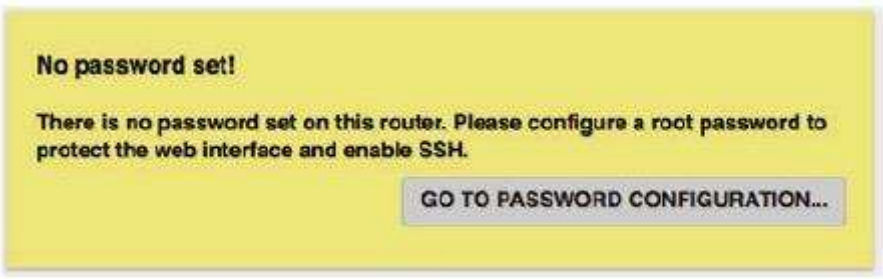
9.1 Accessing the web interface

The router can be configured using its integrated web interface. For accessing the web interface, connect your computer with one of the LAN interfaces of the router.

- If configured accordingly, the computer obtains an IP address automatically using DHCP
- On the computer, open up a web browser and navigate to *https://192.168.2.1*
- A login prompt shows up. The default username is "root". A password is not required.

9.2 Changing the password

As long as no password has been set, a notification will be displayed on the web interface. Click the button in the notification box to change the password.



The password can be changed under *System->Administration* later on.

9.3 Access via SSH

SSH can be used to access the Linux command line interface of the router. For convenient access, a dedicated terminal program like Putty is recommended.

Alternatively, Linux systems and recent Windows systems come with an SSH program built in to their command shell. On Windows, the command shell can be opened up by pressing Windows+r and entering *cmd* in the Run prompt.
To establish an SSH connection execute:

ssh root@192.168.2.1

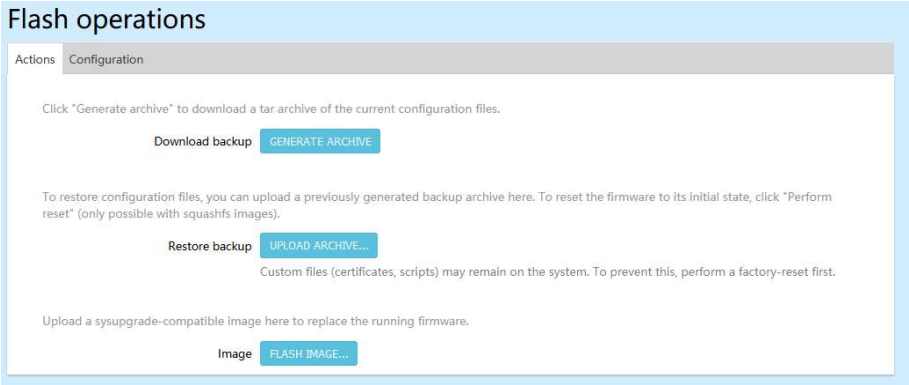
Where *root* is the username and *192.168.2.1* the IP address of the router. Provided a password was set, you will be prompted for the password, when the connection attempt succeeds.

9.4 Flash operations

In *System->Backup / Flash firmware* firmware upgrades can be performed and configuration backups can be created and restored.

9.4.1 Configuration backup

Backup archives containing the configuration files can be downloaded here. These archives can later be uploaded and restored or deployed to another router of the same kind with an equivalent firmware version. Backups must not be restored on different models or routers running different firmware versions, as it cannot be ensured, that the configuration format is identical. This could lead to untraceable errors, system instabilities and even security issues.



9.4.2 Firmware upgrade

The firmware upgrade functionality allows to upgrade the operating system base. This means not only software packages will be updated, but critical system components. Therefore, it is highly recommended, to check, if the upgrade process works in a simulated environment resembling the real-world installation and keeping the devices physically accessible for troubleshooting. This avoids outages and unnecessary service work. Keeping the devices up-to-date is essential for receiving the latest features, security and stability fixes.

To upgrade the firmware, click *FLASH IMAGE...* Next click *BROWSE*, choose the firmware upgrade file and then click *UPLOAD*. Uploading the firmware file may take a while. It is still safe to abort.

After the firmware has been uploaded, a new dialog will display the checksum of the file for confirmation. The upgrade process can be started by clicking the *Continue* button. Do not turn the router off while the upgrade is being performed. After a brief period, the router reboots and then executes additional routines, which can take up to 10 minutes. The upgrade is finished, when the web interface is reachable again.

9.5 Factory reset

WARNING:
All files will be deleted and user settings will be reset to factory defaults. Please ensure the device is accessible for troubleshooting.

- Locate the reset button on your device
- Disconnect the power supply
- Use e.g. a paperclip to press and hold the reset button
- While keeping the button pressed, connect the power supply
- The status LED starts blinking for a few seconds
- Release the button after the status LED stopped blinking

10 Network interface configuration

A listing of the network interfaces can be found in *Network->Interfaces*.

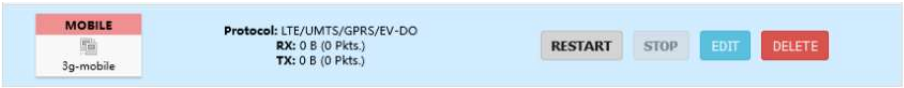
Network interfaces in OpenWrt terminology are virtual in the sense that they represent a set of configuration options like the interfacing protocol, IP address, firewall zone etc. linked to a network device.

Network devices in OpenWrt terminology on the other hand are what is traditionally understood as network interfaces in UNIX terms like hardware ethernet interfaces, virtual bridges etc.

The *lan* interface is in factory default state configured as an interface offering a DHCP server on the *br-lan* network device. *br-lan* is in fact a virtual bridge switching between the hardware interfaces *eth0* and *eth1,* which represent the hardware ethernet interfaces of the MC-MR-L2.

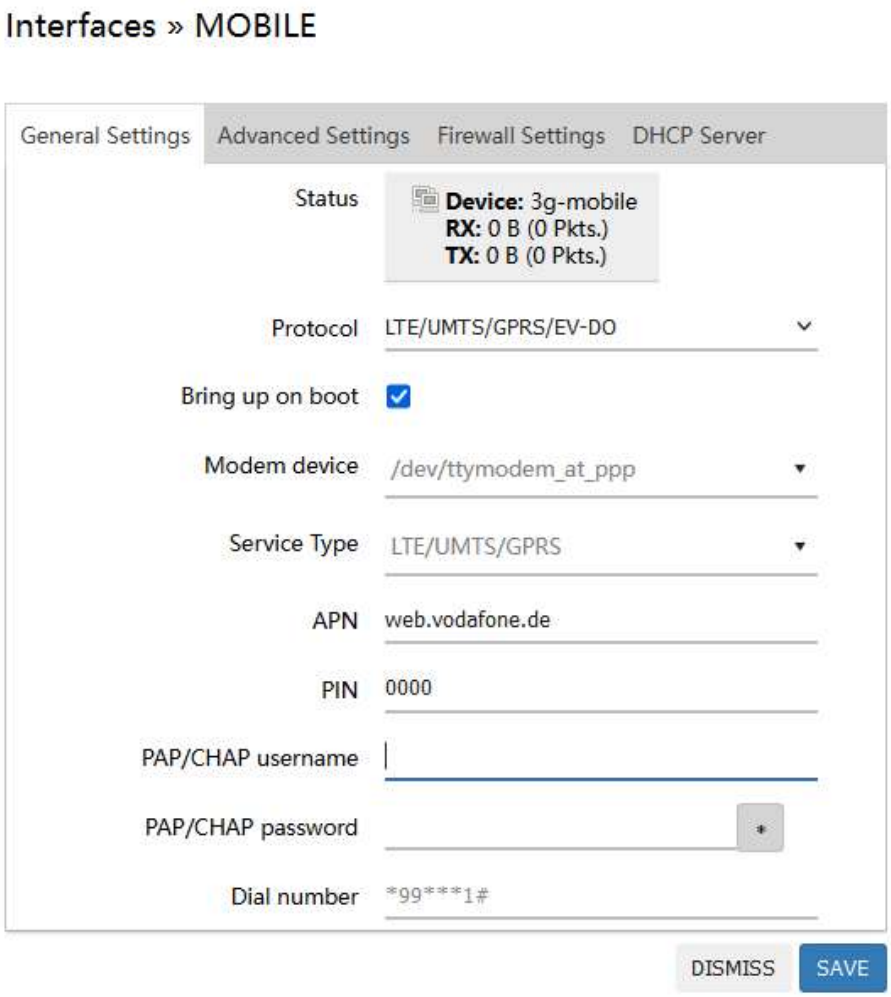
10.1 Cellular connection setup

A mobile WAN interface configuration is present in factory default state, which should only require small provider-dependent adjustments to establish a mobile broadband connection.



Click *EDIT* next to the mobile interface.

Access configuration details like Dial number, APN, username and password need to be obtained from the mobile carrier. Many providers do not require authentication credentials in which case the username and password fields can be left empty. Enter the PIN number of your SIM card. Leave the field empty in case not PIN is set.



Switch to the *Firewall Settings* tab to ensure the mobile interface is added to the *wan* firewall zone.

After clicking *SAVE & APPLY,* it is recommended to reboot or briefly disconnect the router to ensure the modem is properly reinitialized.

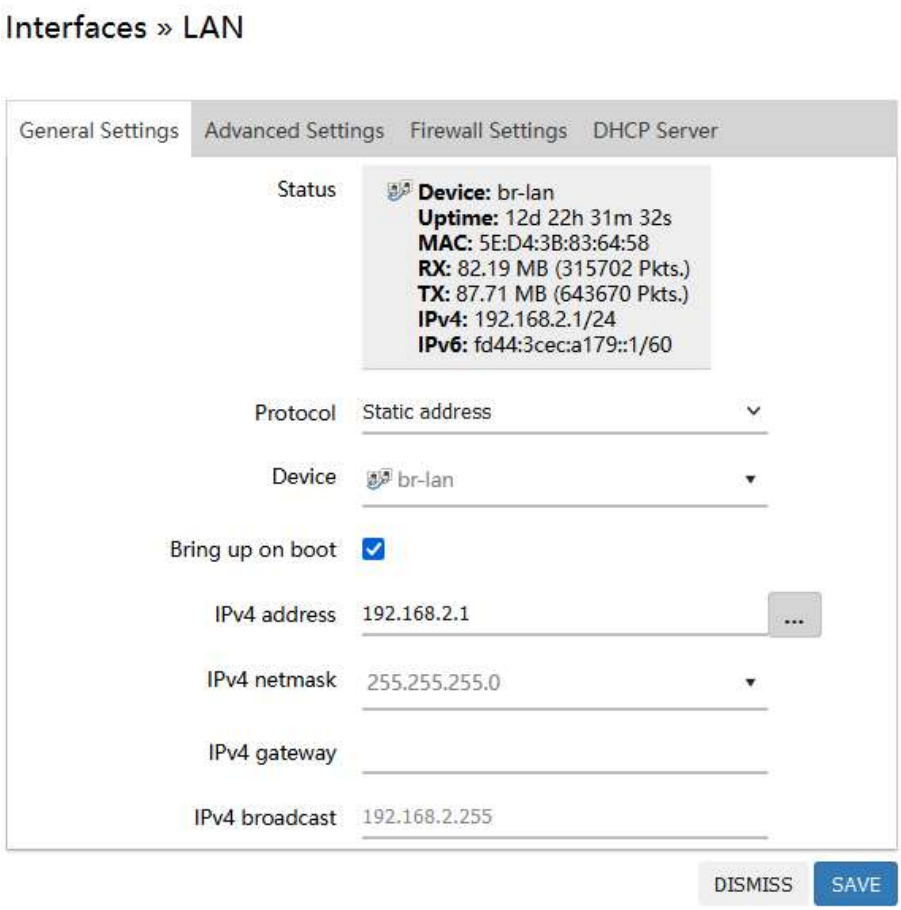
MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

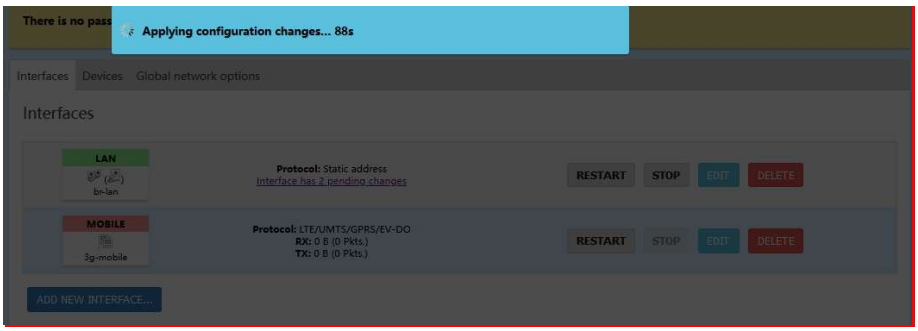
After the start-up, log-in to the web interface again. If the connection was established, the uptime, transmitted and received data statistics should be displayed in Network->Interfaces in the mobile interface entry's box.

10.2 Changing the LAN IP address

Navigate to *Network->Interfaces* and click *EDIT* next to the LAN interface. Change the IPv4 address and netmask as required. In case a DHCP server is being provided by another device in the LAN network, the DHCP server must be turned off in the *DHCP Server* tab to avoid conflicts.
Click *SAVE*, but do not apply the changes, yet.



After applying the changes, a countdown will start. If this countdown elapses, before you were able to access the web interface using the new IP address, the router will revert the changes. This is a countermeasure against accidentally locking yourself out from the system. Once you are prepared for accessing the web interface using the new IP address, proceed by clicking *SAVE & APPLY*.



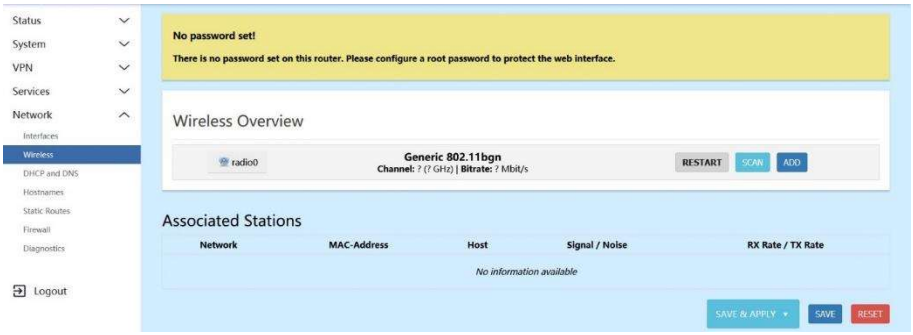
10.1 WLAN setup

WLAN is an optional feature integrated only in some models of the MC-MR-L2 family. Please ensure the router in question has a corresponding SMA connector.

10.1.1 Access point mode (AP)

The router can be used as an access point for other devices to wirelessly connect to it.

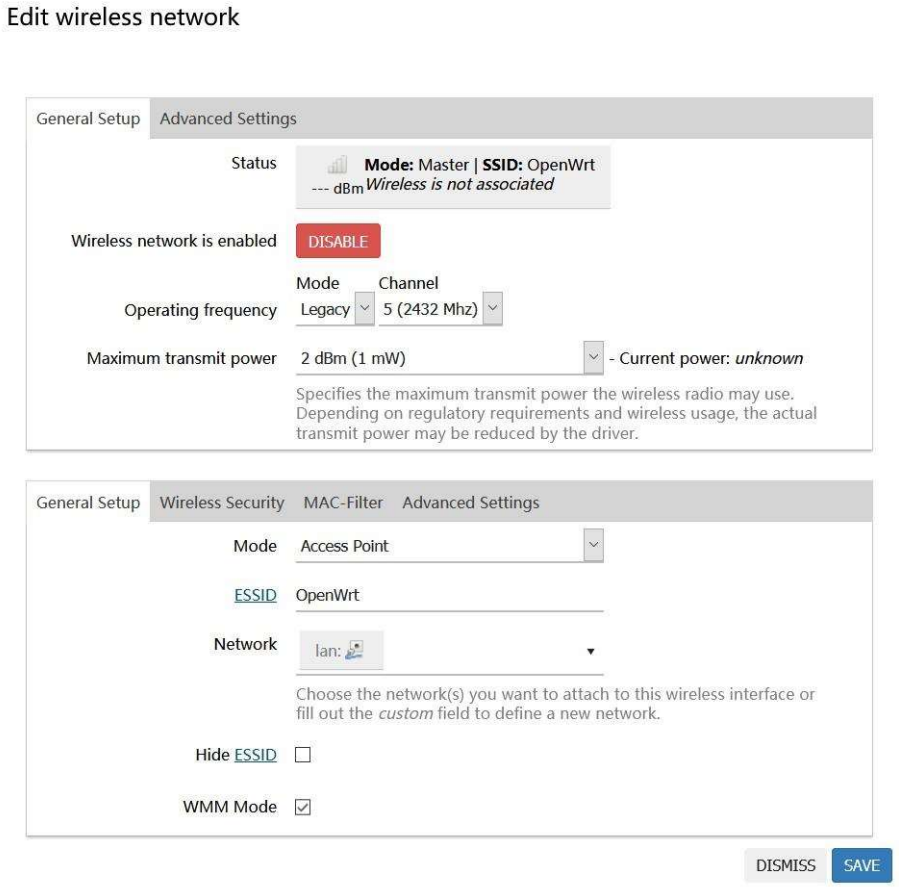
Navigate to *Network->Wireless* and click *ADD* to add a virtual WLAN device to *radio0.*



Set *Network* to *LAN*, and set a name for the WLAN network in the *ESSID* field.
Click *Wireless Security* to set the type encryption (WPA2 or better recommended).

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

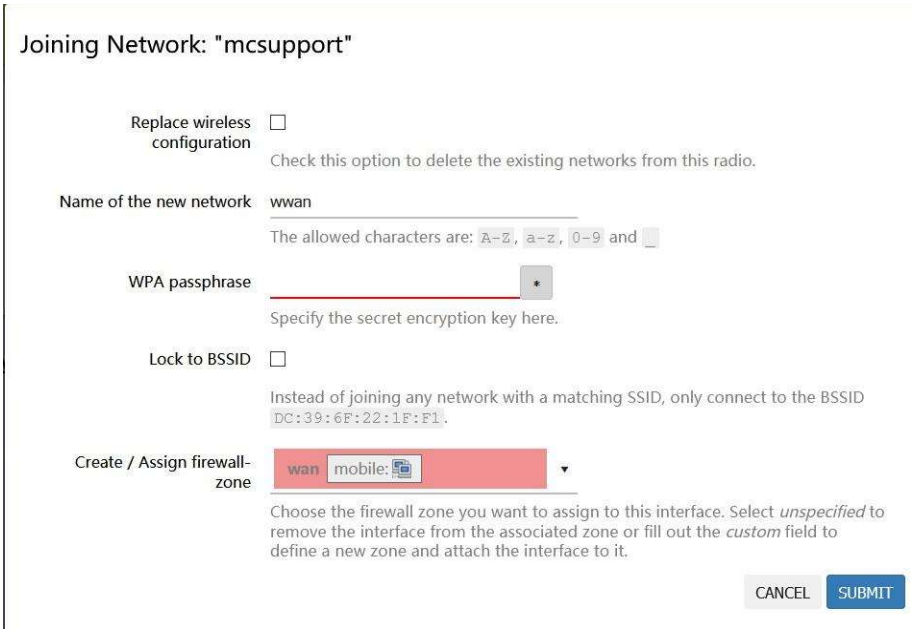
mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150



Click *SAVE*, then *SAVE&APPLY*.
After a brief moment, you should be able to connect to the WLAN network and access the web interface.

10.1.2 Client mode (STA)

The router can be used as a WLAN client to connect to an access point. Navigate to *Network->Wireless* and click *SCAN* in the *Wireless Overview*. Choose the network to connect to and click *JOIN*.



Enter the WLAN password in the *WPA passphrase* field.
Click *SUBMIT*, then *SAVE&APPLY*.
The WLAN connection now serves as a WAN connection.

11 Firewall

11.1 Introduction

OpenWrt's firewall configuration is as powerful as it is complex. Understanding the concepts might be overwhelming for beginners, but rewards with an ability to maintain a more sophisticated network setup than less professional firewalls.

From an abstract view, the firewall is a set of mechanisms to regulate the exchange of network traffic between the host (the router), different networks like a DMZ (Demilitarized zone), proxy, VPN, WAN or LAN and their corresponding network interfaces. It does usually not influence routing decisions directly nor directly restricts any programs or services running on the router. More precisely, the firewall can be thought of as a mechanism filtering, marking and manipulating headers of packets travelling back and forth between applications or network interfaces and the operating system's routing mechanism until the traffic has been rejected, silently dropped or delivered to its destination network interface or application socket.

The firewall is able to inspect, filter and manipulate the packets to an extent which allows to define rule-based policies for handling the forwarding of packets between different network interfaces or the host. This not only allows to implement security measures for e.g. defining access policies to restrict access from one network to the other or to specific services (ports), but also to e.g. share a limited IP address space by utilizing NAT (Network address translation) and using address mapping or port forwarding to enable access to services running on devices in the LAN from the WAN network.

OpenWrt's firewall implementation is basically a sophisticated stack of iptables rules that are being generated from an abstraction layer called fw3 that groups network interfaces into so-called *Zones.* This approach allows to keep an overview in complex setups, as the user does not need to create redundant iptables rules, which would otherwise be hardly manageable. The generated iptables rulesets are intuitively understood. The interested user may want to inspect them by executing *iptables-save or fw3 show* in an SSH session.

Understanding the path, a data packet travels in an operating system's network stack, is very complicated. It is e.g. important, to keep in mind, how different kinds of data packets are handled - e.g. depending on whether they originate from the host itself, meaning they originate from an application or service running on the router like a wget command or a web server, or whether they originate from a network interface. Such packets do not necessarily follow the same rules a packet received on a network interface does. Only understanding the whole network stack, allows to be confident in a firewall. The comparison falls short, but think of the firewall as a postal worker checking the addresses, the stamp, relabelling the address for rerouting and so forth and of the routing mechanism as a mail carrier who just delivers to the address on the label. You are the logistics engineer. To be up to the job, you need to know the process. It is unavoidable to read and understand the iptables documentation at some point:

https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html

11.2 Overview

The firewall configuration has five subsections: General Settings, Port Forwards, Traffic Rules, NAT rules and Custom Rules.

In the *General Settings* or *Zone settings* tab, basic configuration options and default packet handling rules can be set for the so-called Zone concept, which is outlined in the subsequent chapters.

Port Forwards, as the name suggests, allows to set traditional port forwarding rules between different Zones.

Traffic rules allow to add exceptions to the Zone rules and fine-granular filtering capabilities for matching traffic.

With *NAT rules*, address rewriting and connection tracking mechanisms can be implemented.

11.3 General Settings (Zone Settings)

The Zone concept groups network interfaces into so-called Zones. Every zone has a basic set of rule chains (Input, Output and Forward) shared among its network interface. These rule chains represent the policy of handling packets for that zone. The policy is enforced upon all traffic originating from or destined to network interfaces in that zone. On top of that the forwarding of traffic between zones can be policed and restricted on a zone to zone basis and fine-tuned using port forwards, traffic rules and NAT rules.

Explaining the policing of traffic flows between the host and the network interfaces of a zone deserves special emphasis as will be shown. *Host* denotes the router and the sockets of the applications and services running on the router themselves. Rules police the flow and especially the forwarding of traffic between interfaces of a zone among each other and, on a higher level, between zones and other zones.

The default policy is applied when no exceptive rule matches and can either be to accept (Accept), silently drop (Drop) or drop and reply to the packet with an ICMP unreachable message (Reject).

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 network interfaces within the zone. These must not be confused with the Input and output chain of iptables.

11.3.1 Input rules

The Input rules handle the traffic originating from one of the zone's network interfaces destined to a socket of the host i.e. an application like its web interface or a simple ping. As an example, if the input policy for the LAN network is set to drop with no exceptions, devices in the LAN network are no longer able to reach the web interface of the router.

The browser takes some time, then displays a timeout error. The reason is, that the packet gets dropped before it reaches the web server. If it had been set to reject, an ICMP unreachable response would have been sent, which would have let the browser displayed a "website unreachable" error instead almost instantly.

In case a packet is being accepted by the Input policy, a connection tracking entry will be created for this so-called “flow” allowing a bi-directional communication even if the Zone of the instantiator of the connection has a Drop or Reject output policy.

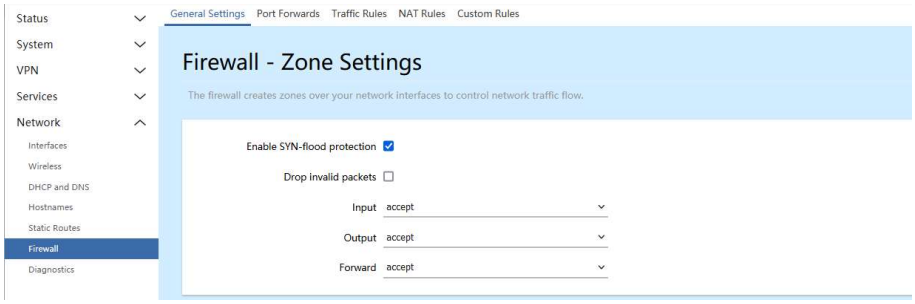
Accordingly, accepting the packet will not only pass the packet from the LAN interface to the web server, but allows the web server to reply regardless of the output policy of that zone.

11.3.2 Output rules

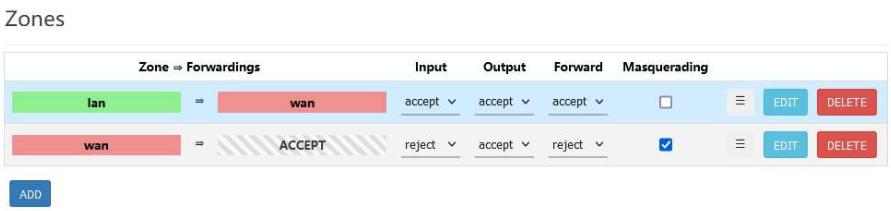
The output rules describe what happens with traffic that originates from the host that is destined to a network interface in the corresponding zone. As the instantiator of the connection is the host itself, this decision is done right before transmitting the packet on that network interface. The filter could still manipulate or even just drop the packet aborting the transmission procedure.

11.3.3 Forwarding rules

If set to *Accept*, traffic originating from a network interface in the zone is permitted to be forwarded to another network interface in that zone. This means it could be routed if a suitable route is present. Otherwise it will be silently dropped (Drop) or dropped and replied to with an ICMP unreachable message (Reject).

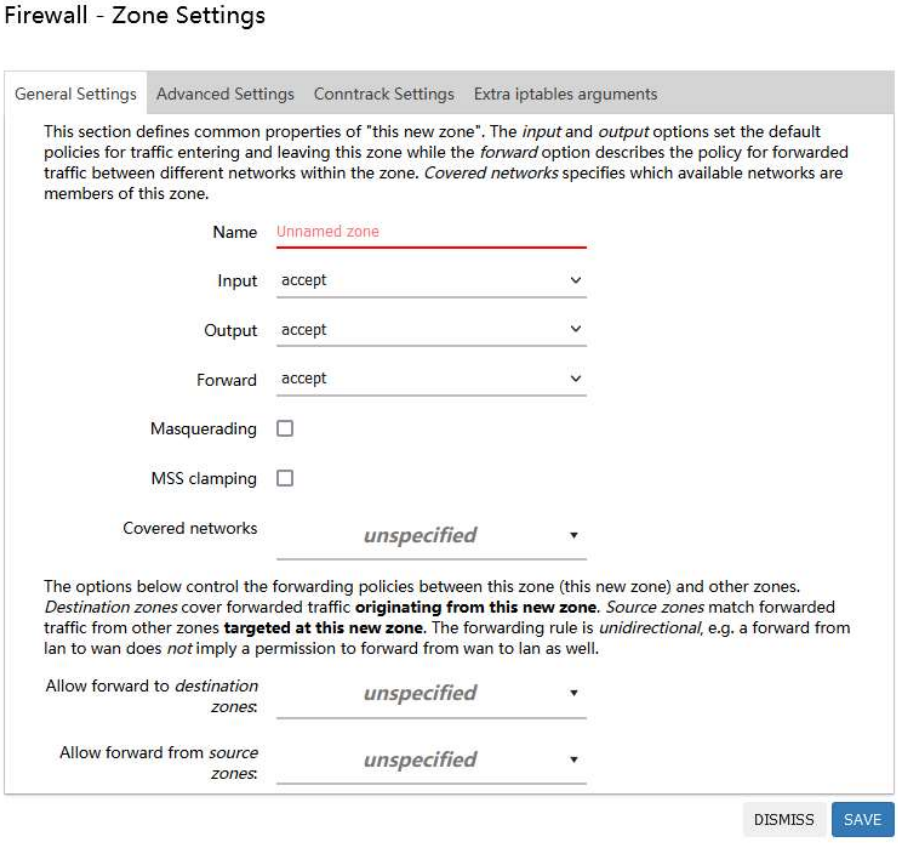


The zone default rules for Input, Output and Forward traffic are being overridden by a set of zone-specific rules defined below the basic configuration options.



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.

11.3.4 General zone settings

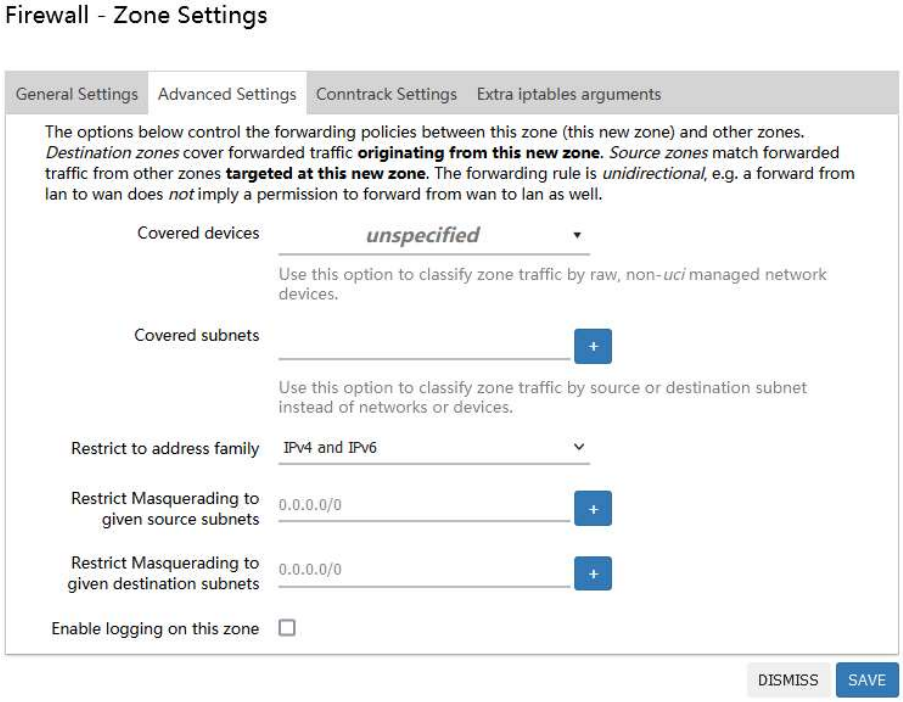


MSS clamping: MSS clamping automatically fragments and defragments TCP packets forwarded between network interfaces with different MTU characteristics. Ordinarily PMTU discovery would lead the TCP connections to use a packet size fit for the lowest MTU along the path. This could limit the throughput if there is a big difference in MTU sizes. MSS clamping may improve this situation. It however requires a higher computational effort for fragmentation and defragmentation, which may lead to performing worse or causing latency issues. Sometimes it may be necessary to use MSS clamping if the MTU of a path is too small. E.g. IPv6 packets require a packet size of at least 1280 bytes and could otherwise not fit through an interface with a smaller MTU. Usually it is safe to turn MSS clamping off.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

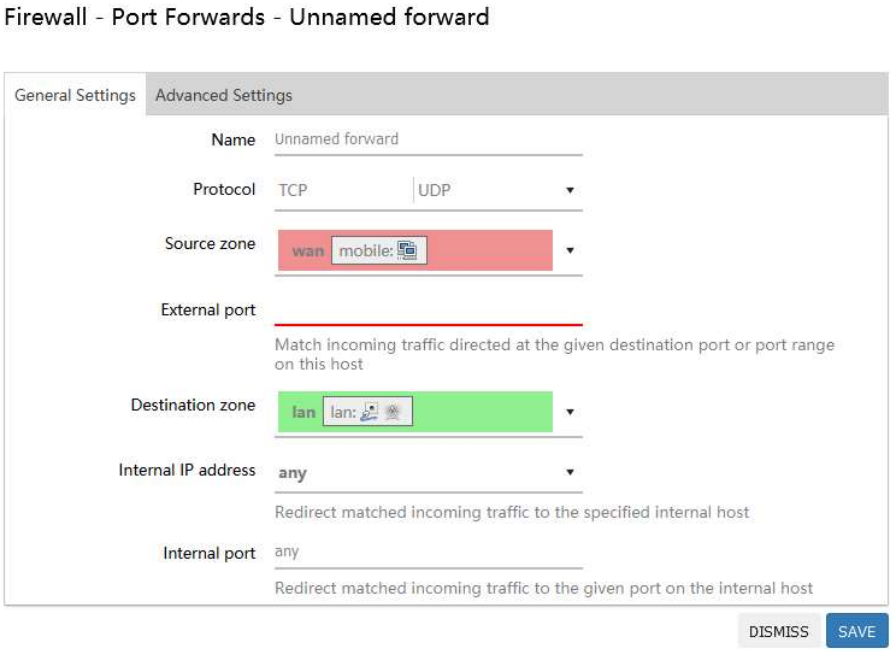
11.3.5 Advanced zone settings



- Restrict to address family: defines to what IP families the zone belongs to IPv4, IPv6 or both.
- Restrict masquerading to given source/destination subnets defines one or more subnets for which the masquerading option is applied to.
- Connection tracking and logging options enable additional information gathering on the zone.
- Controls of the forwarding policies between new/edited zone and other zones.
- Destination zones cover forwarded traffic originating from the new/edited zone.
- Source zones match forwarded traffic from other zones targeted at the new/edited zone.

11.4 Port forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN. It is done in a way of routing network packets within a private network created by the device. Settings for the port forwarding of the device are defined as follows:

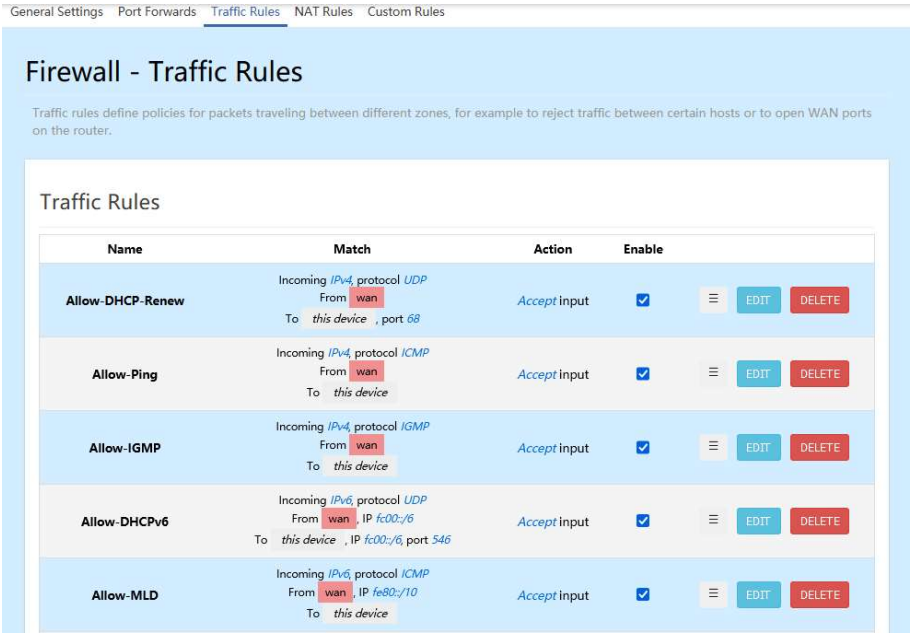


- Name: The name of the port forwarding rule.
- Protocol: Used protocol (Any/TCP/UDP/ICMP)
- Source Zone: Informs which interface forward is matched to.
- External port: Informs what port forward is matched to.
- Destination Zone: Informs which interface is forwarded to.
- Forward to: Informs where the port is forwarded to.
- Internal IP address: Redirect matched incoming traffic to the specified internal host.
- Internal port: Redirect matched incoming traffic to the given port on the internal host.

The user can add, edit, or delete port forwarding rules.

11.5 Traffic rules

Traffic rules define policies for packets traveling between different zones. The matching filter allows a fine granular definition for what kind of traffic the action is being performed.



Traffic can i.e. be matched based on:

- IP protocol
- Source and destination zones
- Source IP address and port
- Destination IP address and port
- Source MAC address
- Packet mark
- DSCP (QoS)

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

The name of the traffic rule is just for internal reference and can be arbitrarily chosen.

11.6 NAT Rules

SNAT (Source NAT) allows to rewrite the source IP address of packets used for an outgoing traffic flow. In conjunction with connection tracking and a DNAT (Destination NAT) for the incoming replies of the traffic flow, this becomes the so-called Masquerading which is quite popular to share a limited set of WAN IP addresses between different devices in the LAN network.

The user can add, edit, or delete source NAT rules. For every rule these options can be defined:

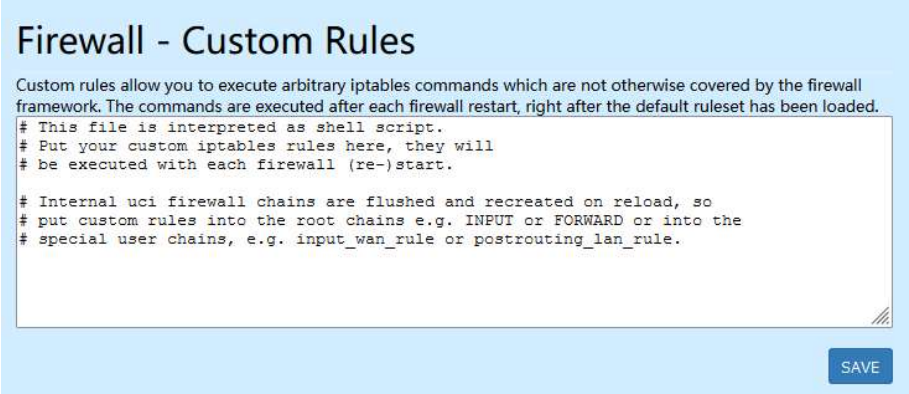
- Name
- Protocol
- source and destination zones
- source
- destination
- SNAT IP addresses
- Ports
- extra arguments
- month
- weekdays
- start/stop dates and times, time in UTC.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

11.7 Custom rules

Custom rules allow to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.



12 Configuration and application examples

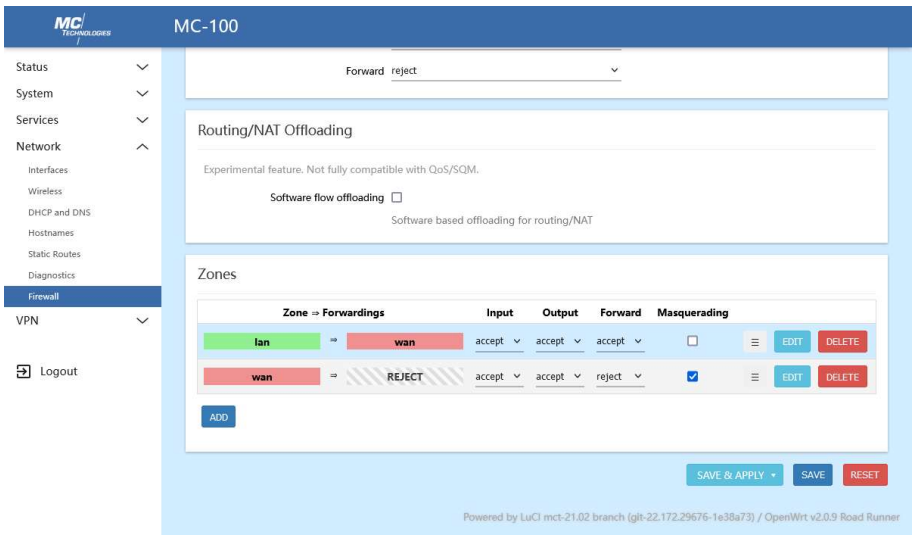
12.1 Reconfiguring an ethernet port as a WAN interface

If your router does not have a WAN interface configured already, it is necessary to reconfigure the existing LAN interface as a WAN interface. In case a WAN interface has been configured already, please ensure the settings match the suggestions outlined below.

12.1.1 Granting access to the web interface from the WAN network

Before removing the LAN interface, it is required to grant firewall access from the WAN network zone to the router. Otherwise it will not be possible to access the router anymore and a factory reset might be the only resort to restore access. **Please be aware that this poses a security risk as the web interface and services will be exposed to all networks in that firewall zone including the mobile WAN network.** It is possible to e.g. create a separate zone for restricting access from the mobile WAN network, but that is out of scope for this particular example.

For granting access to the router from the WAN zone, select *accept* in the *Input* column of the *wan=>REJECT* forwarding rule and then click *SAVE & APPLY*.

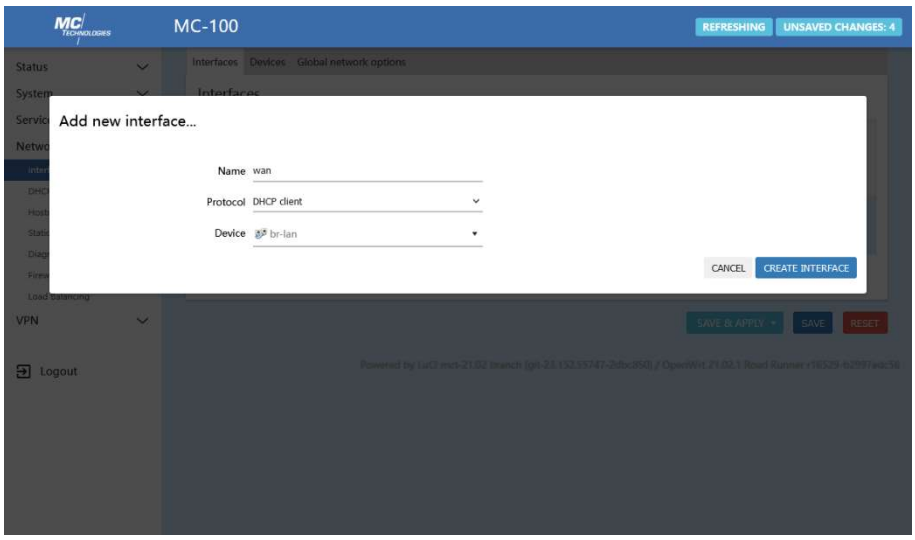


12.1.2 Removing the existing LAN interface

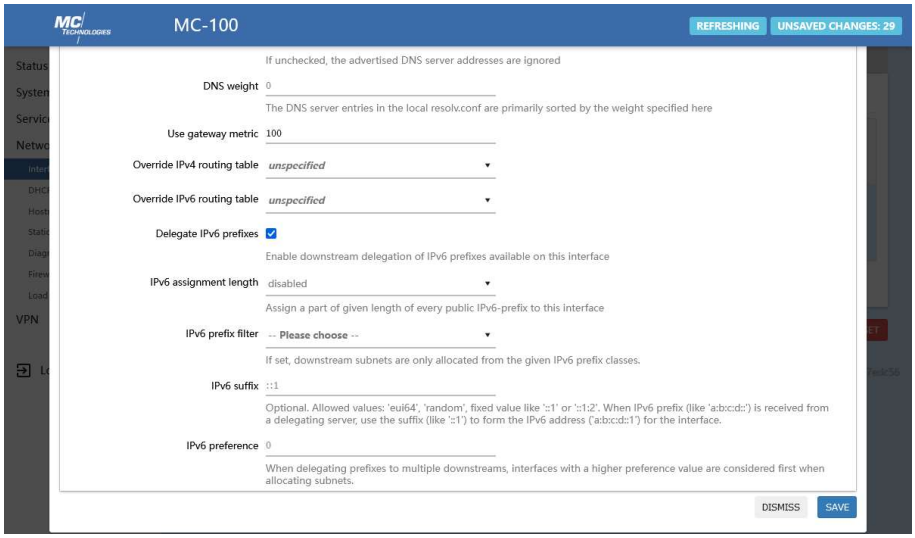
Navigate to *Network->Interfaces* and click the *Delete* button next to the LAN interface. **Do not apply the changes, yet.**

12.1.3 Creating a WAN interface

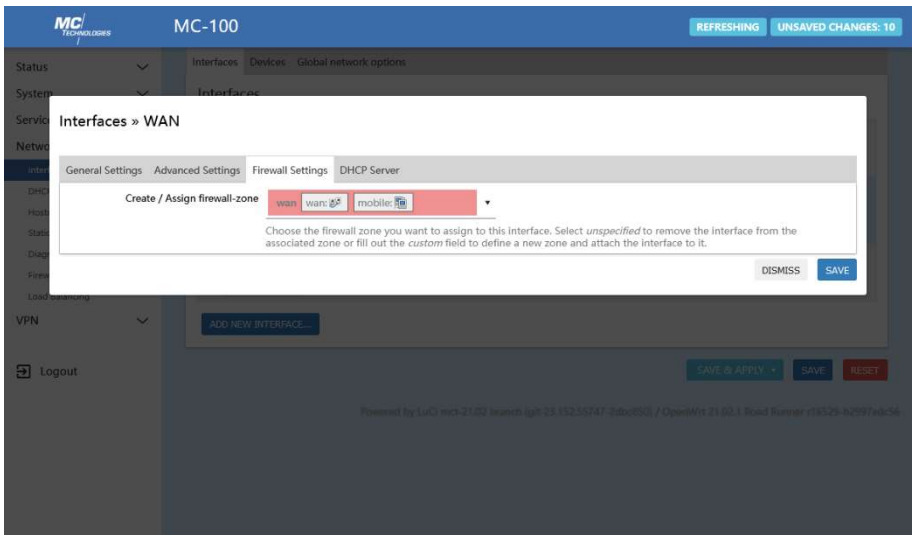
Click the *ADD NEW INTERFACE...* button. In the dialog, enter *wan* as the *Name*, select *DHCP client* as the *Protocol* and *br-lan* as the *Device*. Then click *CREATE INTERFACE*.



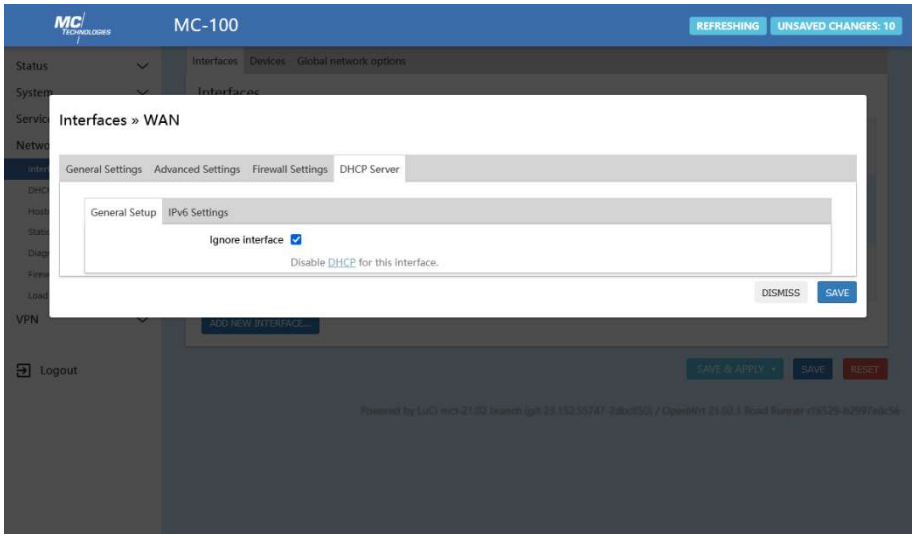
In the *Advanced Settings* tab, set *Use gateway metric* to 100.



Ensure that the interface is added to the firewall zone *wan* in the tab *Firewall Settings*.



Also ensure that the *Ignore interface* checkbox is checked in the *DHCP Server* tab.

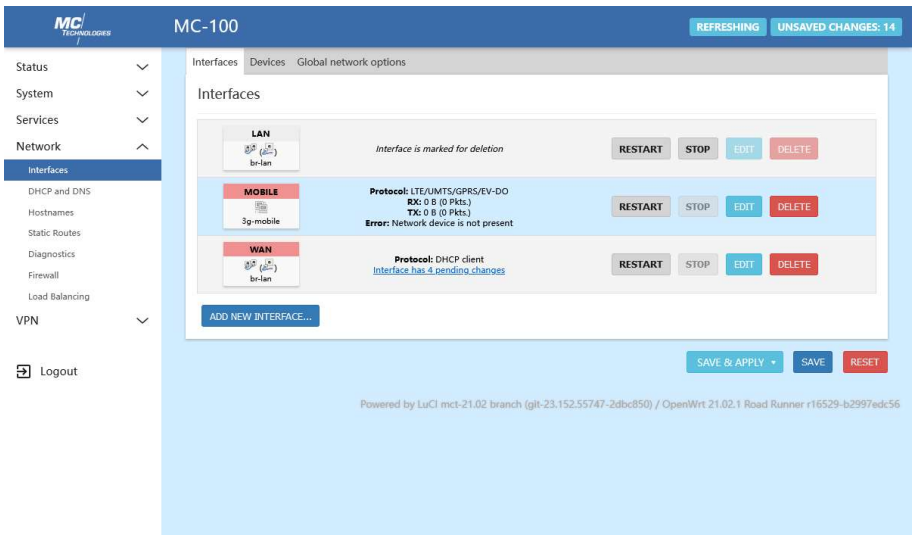


Click *SAVE*.

Before moving on to applying the changes, prepare for accessing the router from the WAN network in a timely fashion. After applying the changes, a countdown will start. If this countdown elapses before you were able to access the web interface from the WAN network, the router will revert the changes. This is a countermeasure against accidentally locking yourself out from the system. Once you are prepared for accessing the web interface from the WAN network, proceed by clicking *SAVE & APPLY*.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150



MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

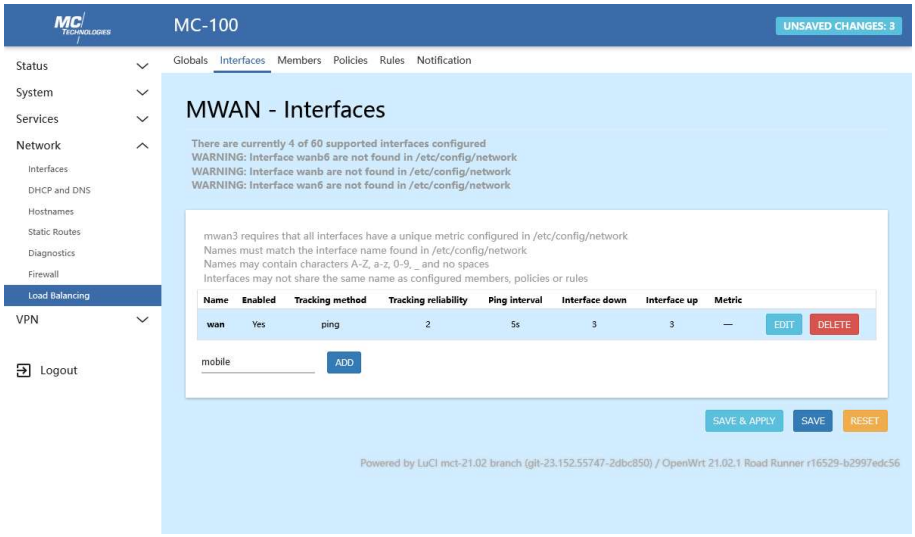
12.2 Connection fail-over and load balancing

It is highly recommended to set a metric value for all default routes of interfaces used with mwan3. This ensures that the routes with the lowest metric value will be preferred even in case of a failure.

Click the *Edit* button next to the *mobile* interface. To configure the mobile interface as the preferred interface, set *Use gateway metric* to 50 in the *Advanced Settings* tab. Otherwise set it to 200.

12.2.1 Adding the interfaces for connectivity tracking

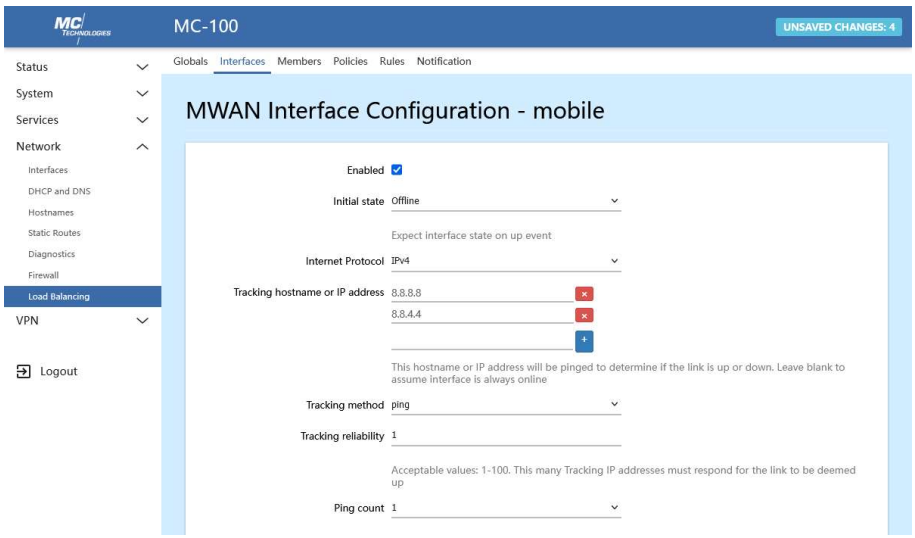
Go to *Network->Load Balancing->Interfaces* and delete all pre-configured interface definitions by clicking *DELETE* next to the entries. Then enter the name of the interface to add (wan or mobile in this example) in the lower-left text field and click the *ADD* button next to it.



You will be presented with many options for determining the connection status of the interface. The default is an ordinary ping command which will be executed according to the options specified herein. It is possible to define multiple *Tracking hostnames or IP addresses.* The *Tracking reliability* option defines how many of these addresses need to be pinged successfully for considering the connection working. Advanced settings allow connection quality checks by also evaluating the packet loss.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150



Google and OpenDNS servers (8.8.8.8, 8.8.4.4 and 208.67.222.222, 208.67.220.220 respectively) have been proven to be reliable indicators for a working internet connectivity. Yet these services are not guaranteed to be available forever, nor that being able to ping them means that the internet connection is working properly. There are other test methods, which can be selected from the *Tracking method* dropdown field, each offering their own set of options. E.g. *httping* for checking the reachability of HTTP(S) servers.

12.2.2 Grouping interfaces using Member profiles

Delete all pre-configured *Member* profiles by clicking the *DELETE* buttons next to the entries.

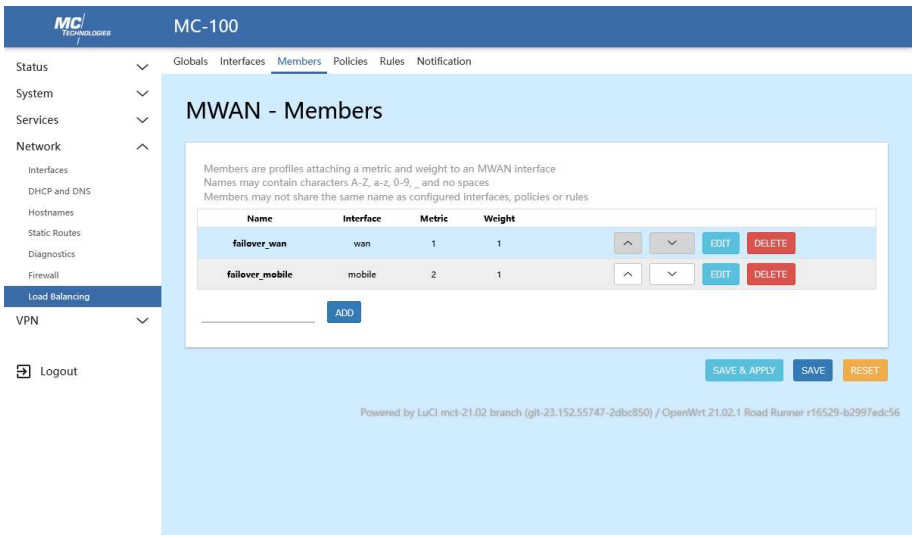
For grouping interfaces in (multiple) *Policies* later, they need to be added to *Member* profiles first. *Member* profiles basically have two options:

The *Metric* prioritizes the interfaces for a failover case (just as with a routing metric, a lower metric value means the interface is preferred compared to another one with a higher value). Please do not confuse this with the default route metric configured earlier.

The *Weight* value is used for allowing load balancing of two or more interfaces sharing the same metric value. E.g. considering a policy consisting of two interfaces A and B, sharing the same metric value, with a weight value of 3 for interface A and 2 for interface B generally means that 60% (3 * 100% / (3 + 2)) of the newly instantiated connections will be using interface A.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

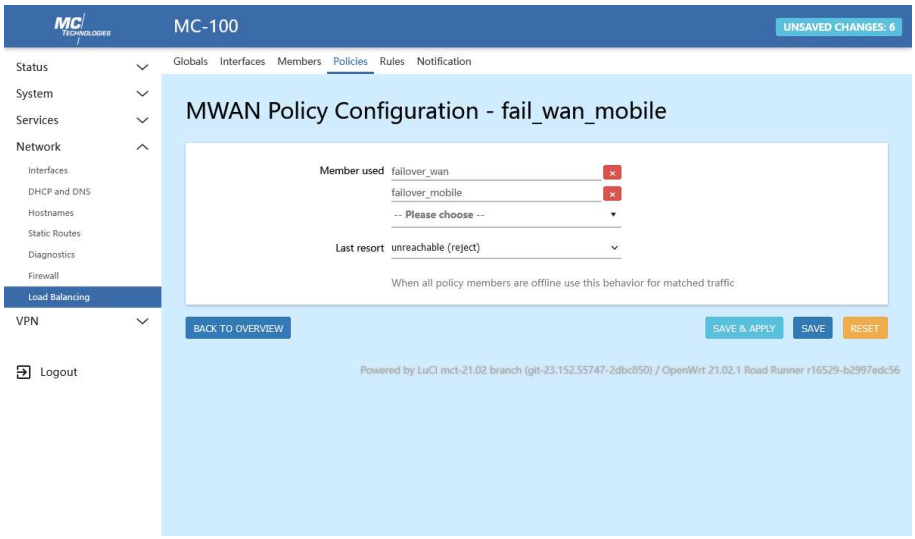
mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150



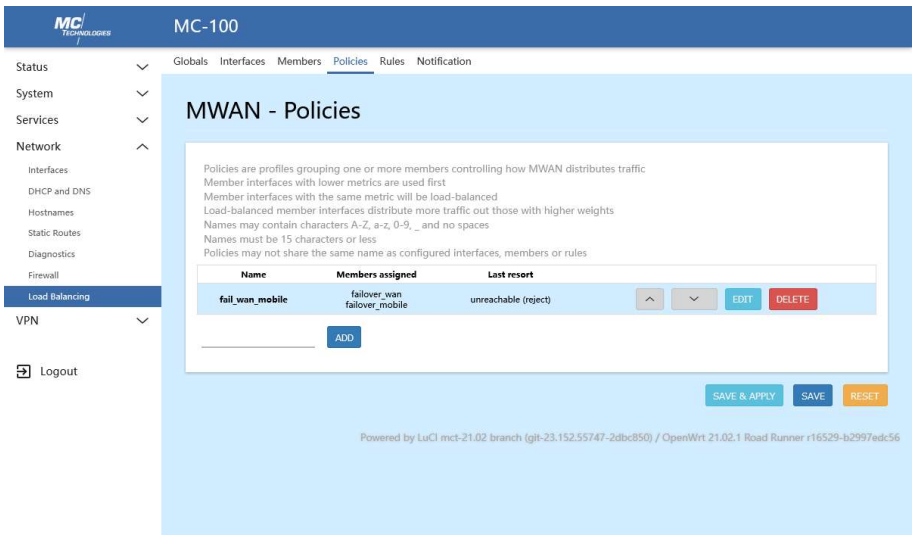
12.2.3 Policies

Delete all pre-configured *Policies* by clicking the *DELETE* buttons next to the entries.

Policies allow the grouping of *Members* for defining failover, load-balanced or even mixed *Rules*.



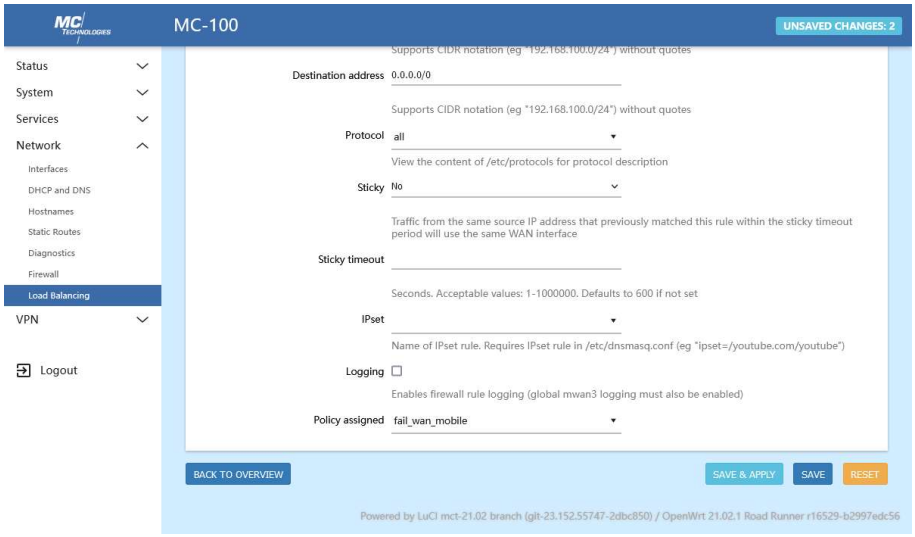
As stated previously, mwan3 checks the connectivity status of the *Members* in the first run ordered by their metric values. If multiple of the functional members with the lowest metric of that policy share the same metric value, only then the weight value is considered for load-balancing the connections.



12.2.4 Rules

Finally, *Rules* need to be set up for defining the application cases of the policies. Delete all pre-configured *Rule* definitions by clicking the *DELETE* buttons next to the entries.

Rules define for what type of connections a policy shall be applied. It is possible to define the IP protocols, the *Source* and *Destination address*, port range and advanced load balancing settings. It is even possible to define a custom *IPSet* for dynamic setups.



12.3 OpenVPN

The configuration of OpenVPN is highly customizable. It is required to match the client and server configuration. In the following an example of the process of interpreting and configuring an OpenVPN configuration will be given. For setups that require a more sophisticated configuration, reading the official OpenVPN documentation, is unavoidable.

An OpenVPN server requires security certificates. If you are using OpenVPN as a client, the required certificates are usually provided with the configuration details. OpenVPN can be configured either by using the web interface or by uploading the configuration files e.g. using. OpenVPN will automatically attempt to load all *.conf files placed in the /etc/openvpn folder. OpenVPN example configurations are available online. These can usually be adapted with minor changes.

Before starting, create your own Certificate Authority (CA), certificates and keys for an OpenVPN server and clients.

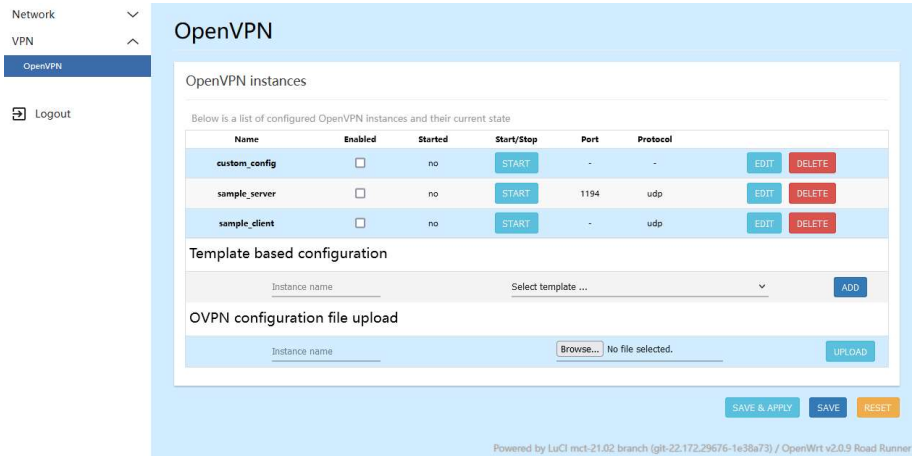
You will need:

- Certificate authority (ca.crt)
- Server certificate (server.crt) and server key (server.key)
- Client certificate (client.crt) and client key (client.key)
- Client configuration

12.3.1 Client configuration

You will need the Certificate authority "ca" (.CRT), local certificate "cert" (.CRT), and the local private key "key" (.key) files.

Navigate to *OpenVPN->VPN*.

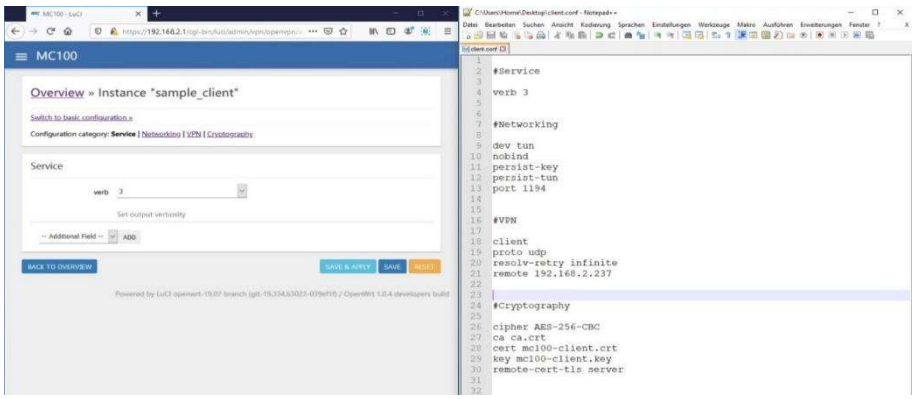


Click *EDIT* next to *sample_client*.

Click *Switch to advanced configuration*.

Edit the settings according to the ones in the client.conf file.

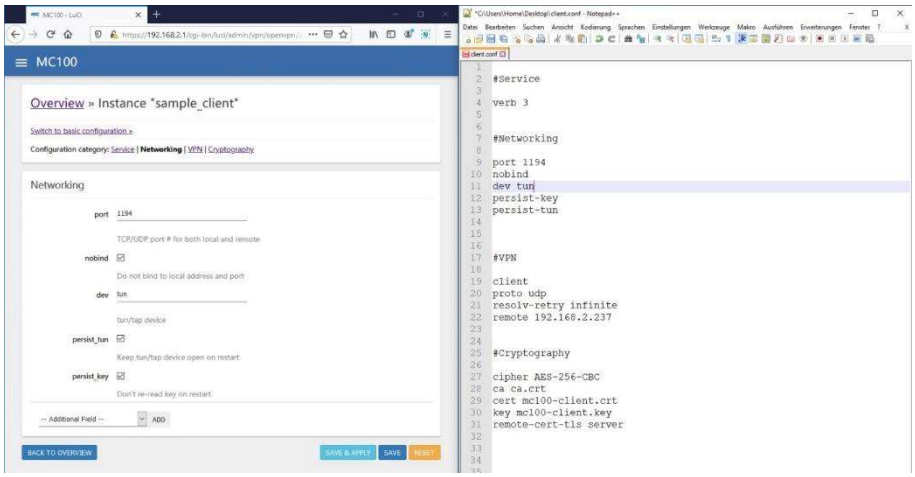
Example:



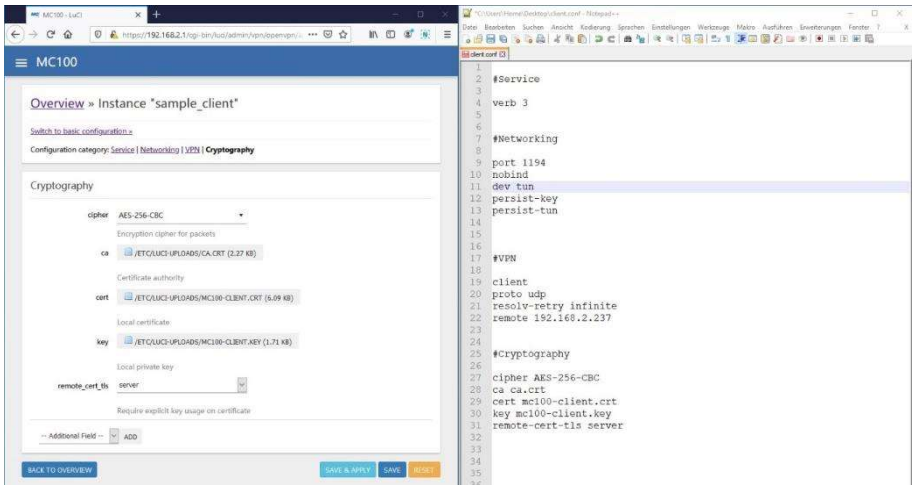
Under Service, change "verb" (verbosity) same as given in the .conf file (here it is 3).

Under Networking, change every setting as same as given in the .conf file.

Apply the same settings for the VPN section.



Under *Cryptography* change the cipher type to the one given in the .conf file.



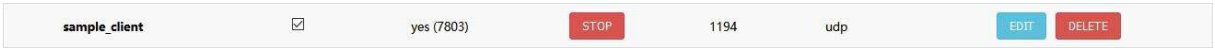
Upload the files to the /etc/luci-uploads/ folder.

MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150

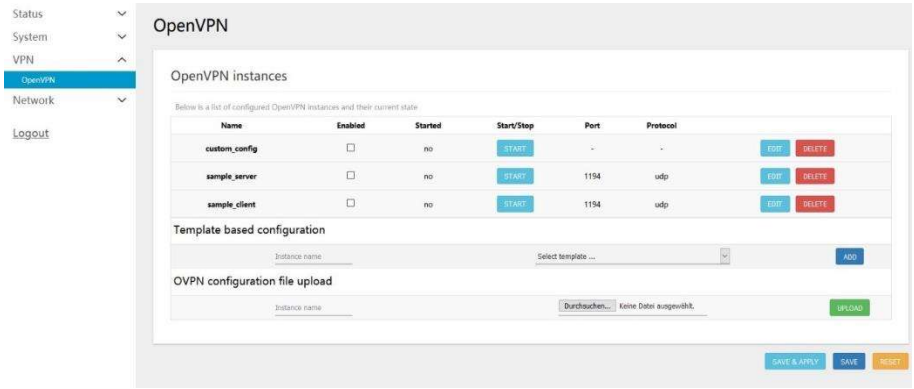
Click *SAVE & APPLY* and then *BACK TO OVERVIEW*.

Enable the configured instance, then click "SAVE AND APPLY", then "START".



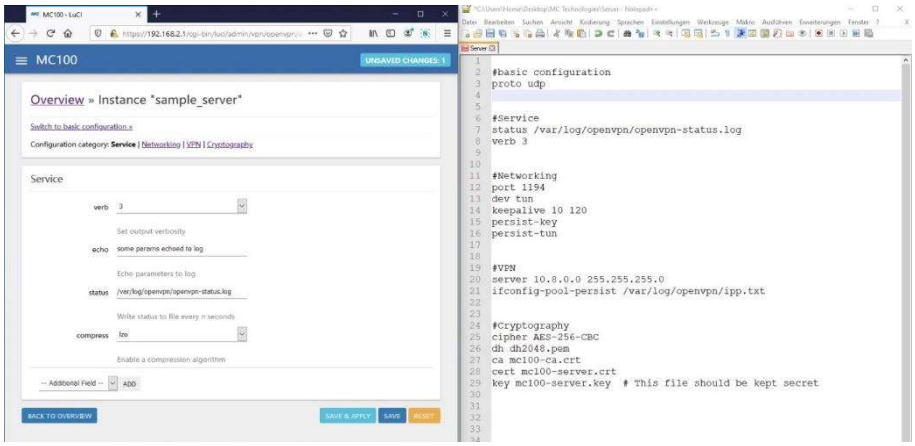
12.3.2 Server configuration

Navigate to VPN->OpenVPN.



Click *EDIT* next to the *sample_server* entry, then click *Switch to advanced configuration*.

Edit the settings to match the ones in the *server.conf* file.

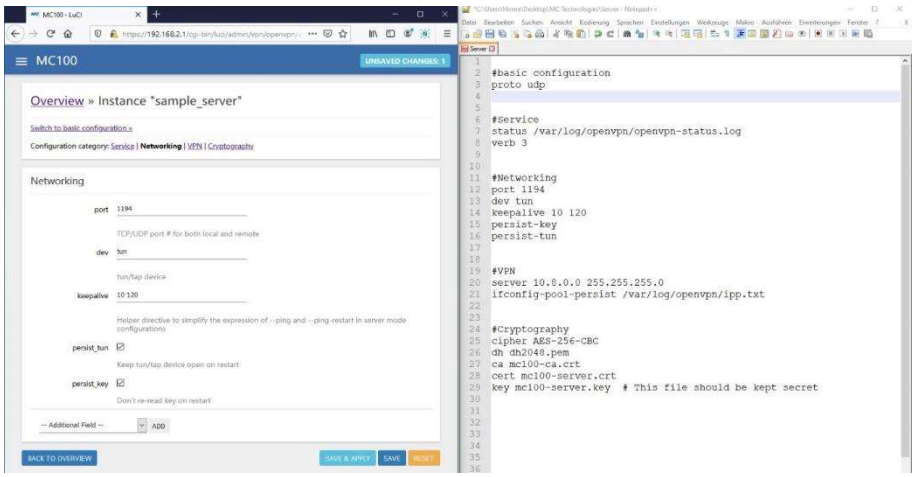


Under *Service*, change "verb" (verbosity) to the same value as in the .conf file (here it is 3).

Under *Networking*, change every setting as same as given in the .conf file.

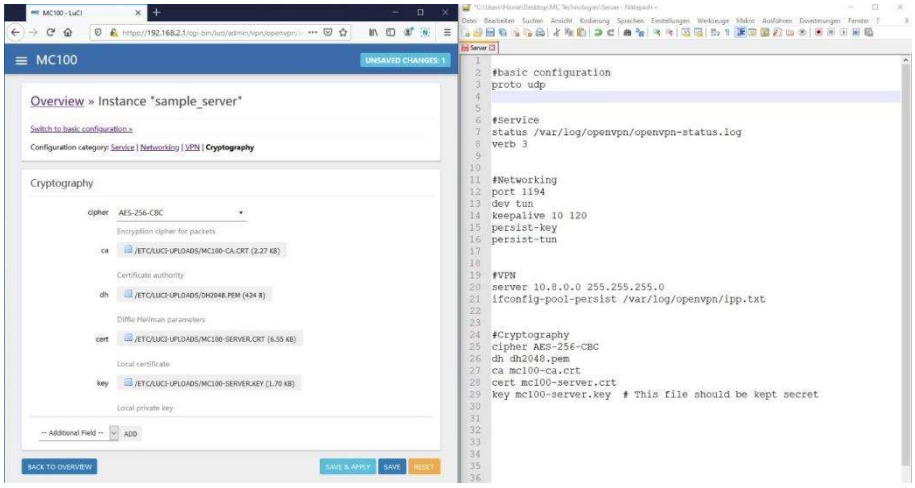
MC Technologies GmbH
Kabelkamp 2
30179 Hannover
Germany

mc-technologies.com
info@mc-technologies.com
Tel: +49-511-676 999-0
Fax: +49-511-676 999-150



Apply the same settings as in the VPN section.

Under *Cryptography* change the cipher type to the one given in the .conf file.



Upload the files to the /etc/luci-uploads/ folder.

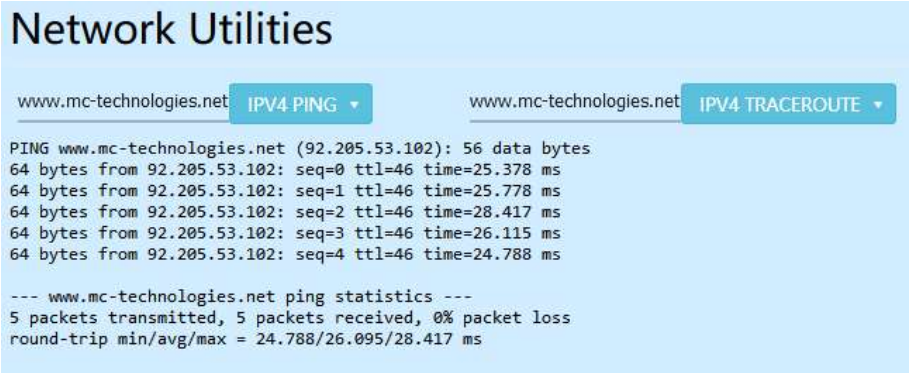
Click *SAVE & APPLY* and then *BACK TO OVERVIEW*.

Enable the configured instance, and then click *SAVE AND APPLY*, then *START*.

13 Diagnostics

13.1 Connectivity check

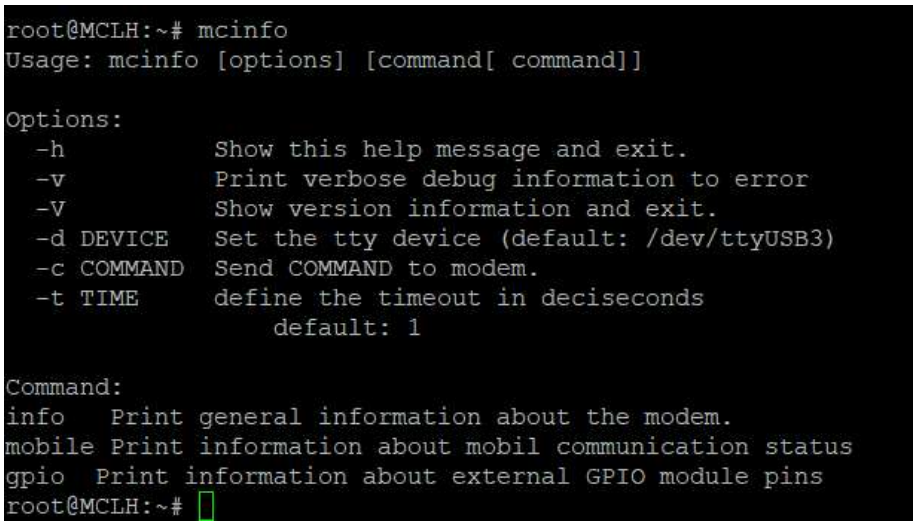
A tool for performing ping and traceroute tests can be found in Network->Diagnostics. Click the corresponding buttons under "Network Utilities" to perform a test.



13.2 mcinfo

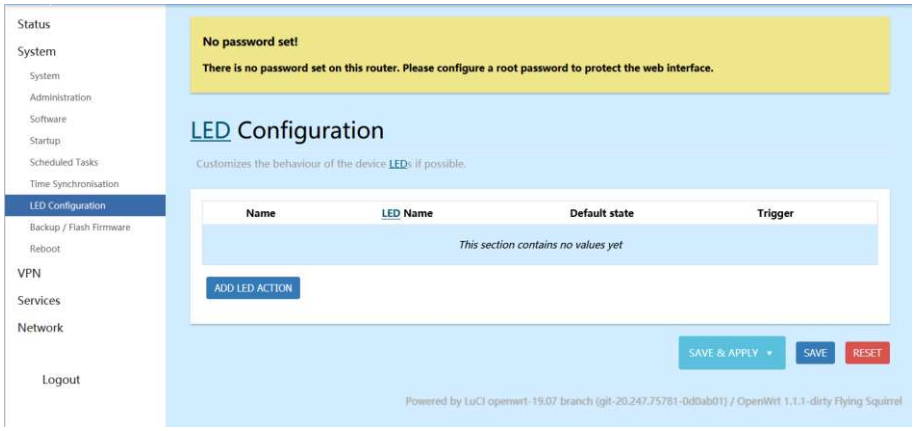
mcinfo is a command line utility installed on the router which can be used via SSH. It offers in-depth debugging information like the modem status and device information.

Command	Use to
mcinfo info	Print general information about the modem.
mcinfo mobile	Print information about mobile communication status.

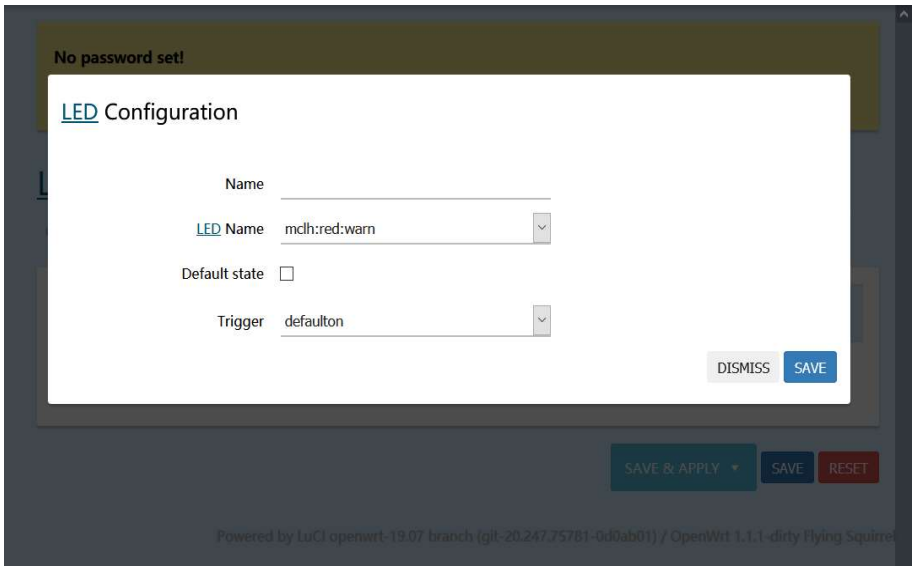


13.3 LED configuration

The signal triggers and blinking patterns of the LEDs can be customized. The settings can be found in *System->LED Configuration*.



Click *ADD LED ACTION* to create a new customized LED definition.



The *Name* of the LED definition can be chosen arbitrarily, but choosing the *LED Name* in the dropdown field is mandatory. The *Default state* defines whether the LED should be on or off initially before any trigger signal changes its state.
What signal source the LED blinking pattern is controlled by can be chosen using the *Trigger* dropdown field. OpenWrt offers a wide variety of system signals for controlling the signalling patterns.

LED	LED Name
INFO	mclx:orange:info
STATUS	mclx:orange:status
WARN	mclx:red:warn
1	mclx-cb:green:led1
2	mclx-cb:red:led2

Click SAVE, then SAVE & APPLY to make the LED configuration come into effect.

14 Product care and handling

14.1 Maintenance

The product is maintenance-free and requires no special regular maintenance.

14.2 Troubleshooting

If a fault occurs during operation of the product and you need assistance, please contact MC Technologies support. You can reach our support department by email:

support@mc-technologies.com

14.3 Repair

Only qualified personnel at MC Technologies GmbH is authorised to perform repairs.

Send defective products with a detailed error description to:

MC Technologies

-Repair-

Kabelkamp 2

30179 Hannover

Before shipping the device make sure to:

- Call our support team and ask for an RMA number (Return to Manufacturer Authorisation)
- Remove any personal belongings like inserted SIM cards
- Back up any relevant data like configurations on the device

14.4 Disposal

In accordance with WEEE regulations, the return and recycling of old MC Technologies equipment for our customers is regulated as follows:

Please send your old devices carriage paid to the following address:

MC Technologies

-Disposal-

Kabelkamp 2

30179 Hannover