RACOM
RADIO DATA NETWORKS

User manual

Quick start
>>>

Hardware

Configuration

Parameters

M!DGE2 GPRS/UMTS/HSPA+/LTE router

fw 4.4.x.x
2020-4-23
version 1.5

www.racom.eu

Table of Contents

List of Figures

List of Tables

Important Notice

Copyright

© 2020 RACOM. All rights reserved.
Products offered may contain software proprietary to RACOM s. r. o. (further referred to under the abbreviated name RACOM). The offer of supply of these products and services does not include or imply any transfer of ownership. No part of the documentation or information supplied may be divulged to any third party without the express written consent of RACOM.

Disclaimer

Although every precaution has been taken in preparing this information, RACOM assumes no liability for errors and omissions, or any damages resulting from the use of this information. This document or the equipment may be modified without notice, in the interests of improving the product.

Trademark

All trademarks and product names are the property of their respective owners.

Important Notice

- Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e. have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as the M!DGE are used in an appropriate manner within a well-constructed network. M!DGE should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. RACOM accepts no liability for damages of any kind resulting from delays or errors in data transmitted or received using M!DGE, or for the failure of M!DGE to transmit or receive such data.
- Under no circumstances is RACOM or any other company or person responsible for incidental, accidental or related damage arising as a result of the use of this product. RACOM does not provide the user with any form of guarantee containing assurance of the suitability and fit for purpose.
- RACOM products are not developed, designed or tested for use in applications which may directly affect health and/or life functions of humans or animals, nor to be a component of similarly important systems, and RACOM does not provide any guarantee when company products are used in such applications.

Getting started

M!DGE Wireless Router will only operate reliably over the cellular network if there is a strong signal. For many applications a flexible stub antenna would be suitable but in some circumstances it may be necessary to use a remote antenna with an extension cable to allow the antenna itself to be positioned so as to provide the best possible signal reception.

1. **Install the SIM card**
   Insert a SIM card into the SIM socket. Make sure the SIM is enabled for data transmission.
2. **Connect and fit the cellular antenna**
   If needed, contact RACOM for suitable antennas and other details.
3. **Connect the LAN cable**
   Connect one M!DGE Ethernet port to your computer using an Ethernet cat.5 cable.
4. **Connect the power supply**
   Connect the power supply wires to the M!DGE screw terminals, ensuring correct polarity. Switch on the power supply.
5. **Setting of IP address of the connected computer**
   By default the DHCP server is enabled, thus you can allow the Dynamic Host Configuration Protocol (DHCP) on your computer to lease an IP address from the M!DGE. Wait approximately 20 seconds until your computer has received the parameters (IP address, subnet mask, default gateway, DNS server).
   As an alternative you can configure a static IP address on your PC (e.g. 192.168.1.2/24) so that it is operating in the same subnet as the M!DGE. The M!DGE default IP address for the first Ethernet interface is 192.168.1.1, the subnet mask is 255.255.255.0.
6. **Start setting up using a web browser**
   Open a web browser such as Internet Explorer or Firefox. In the address field of the web browser, enter default IP address of M!DGE (i.e. http://192.168.1.1); initial screen will appear. Follow the instructions and use the M!DGE Web Manager to configure the device.

Fig. 1: Cellular router M!DGE

ⓘ **Note**

M!DGE can be safely turned off by unplugging the power supply.

1. M!DGE router

1.1. Introduction

Although M!DGE wireless routers have been specifically designed for SCADA and telemetry, they are well suited to a variety of wireless applications. M!DGE HW and SW are ready to maintain reliable and secure connections from a virtually unlimited number of remote locations to a central server. Both standard Ethernet/IP and serial interfaces are available. Moreover, a digital input and a digital output can be used for direct monitoring and control of application devices; the second DI and DO are available using an extension module.

M!DGE versatility is further enhanced by four independent Ethernet ports. These can be configured to either support independent LANs (e.g. LAN and WAN settings), or simply connect up to four devices within one LAN (effectively replacing an Eth switch). M!DGE software is based on proven components, including an Embedded Linux operating system and standard TCP/IP communication protocols.

Thanks to the compact size and versatility of M!DGE, wireless routers prove indispensable in many SCADA and telemetry, as well as POS, ATM, lottery and security/surveillance applications.

M!DGE together with RACOM RipEX radio router offers an unrivalled solution for combining cellular and UHF/VHF licensed radios in a single network.

1.2. Key features

Mobile Interface Parameters

- Mobile Connection options: LTE, HSPA+, HSDPA, HSUPA, UMTS, EDGE, GPRS and GSM
- Global connectivity
- Transparent hand-over between 2G, 3G and 4G

Power supply

- Input voltage: 12 – 24 VDC
- Average power consumption: 7 W

Services / Networking

- Fallback Management
- Connection supervision, Automatic connection recovery
- Quality of Service (QoS)
- OpenVPN, IPsec, PPTP, GRE, Dial-In, Mobile IP
- VRRP
- OSPF, BGP
- DHCP server, DNS proxy server, DNS update agent, NTP
- Telnet server, SSH server, Web server
- Device server, Protocol server, SDK, LXC containers
- Port Forwarding (NAPT), Firewall, Access Control Lists
- Modbus TCP - Modbus RTU conversion

Interfaces

- 4 Ethernet ports: LAN, WAN/LAN
- RS232
- 1× DI, 1× DO
- USB host

Diagnostic and Management

- Web interface, CLI available
- File configuration
- OTA SW update
- Advanced troubleshooting
- SMS remote control, SMS and E-mail notification
- SNMPv1/v2c/3

1.3. Standards

Safety / Health	EN 62368-1:2014
	EN 62311:2008
EMC	EN 55032:2015
	EN 55035:2017
	EN 61000-6-2:2016
	EN 61000-6-3:2007+A1:2011+AC:2012
	EN 301 489-1 V2.1.1
	EN 301 489-3 V2.1.1
	EN 301 489-7 V1.3.1
	EN 301 489-17 V3.2.0
	EN 301 489-24 V1.5.1
	EN 301 489-52 V1.1.1
RF Spectrum	EN 300 328 V2.1.1
	EN 301 511 V9.0.2
	EN 301 908-1 V11.1.1
	EN 301 908-2 V11.1.1
	EN 301 908-13 V11.1.1
Vibration & shock	EN 60068-2-6:2008
	ETS 300 019-2-3:1994, Class 3.4
	EN 61850-3:2014
Seismic	EN 60068-2-27:2010
Environmental	EN 61850-3:2014
	IEEE 1613:2009

2. M!DGE in detail

Fig. 2.1: M!DGE front and terminal panel

All M!DGE Wireless Routers run M!DGE Software. Software offers the following key features:

- Interfaces and Connection Management (*Section 7.2, "INTERFACES"*)
  - Dial-out (permanent, on switchover, distributed)
  - Link Supervision
  - Fallback to backup profile
  - SIM and PIN management
  - Automatic or manual network selection
  - Ethernet (LAN, WAN, bridging, IP passthrough, VLAN management)
  - Bridges
  - USB (autorun, device server)
  - Serial port (login console, device server, protocol server, SDK, Modem bridge, Modem emulator)
  - Digital I/O
- Routing (*Section 7.3, "ROUTING"*)
  - Static Routing
  - Extended Routing
  - Multipath Routes
  - Multicast
  - BGP
  - OSPF
  - Mobile IP
  - Quality of Service (QoS)
- Security / Firewall (*Section 7.4, "FIREWALL"*)
  - NAPT / Port Forwarding
  - Stateful Inspection Firewall
  - Firewall
- Virtual Private Networking (VPN) (*Section 7.5, "VPN"*)
  - OpenVPN Server/Client
  - IPsec Peer
  - PPTP Server/Client
  - GRE Peer
- Services (*Section 7.6, "SERVICES"*)

- ○ SDK
- ○ NTP Server
- ○ DHCP Server
- ○ DNS Server
- ○ Dynamic DNS Client
- ○ E-mail Client
- ○ Notification via E-mail and SMS
- ○ SMS Client
- ○ SSH/Telnet Server
- ○ SNMP Agent
- ○ Web Server
- ○ Redundancy
- ○ Modbus TCP
- ○ Discovery
- ○ Terminal server
- ○ LXC containers
- System Administration (*Section 7.7, "SYSTEM"*)
  - ○ Configuration via Web Manager
  - ○ Configuration via Command Line Interface (CLI) accessible via Secure Shell (SSH) and telnet
  - ○ Batch configuration with text files
  - ○ User administration
  - ○ Troubleshooting tools
  - ○ Over the air software update
  - ○ Licensing (extra features)
  - ○ Keys and certificates (HTTPS, SSH, OpenVPN, ...)
  - ○ Legal Notice

3. Implementation notes

3.1. Ethernet SCADA protocols

SCADA equipment with an Ethernet protocol behaves as standard Ethernet equipment from a communications perspective. Thus the communication goes transparently through the cellular network. The implementation requires heightened caution to IP addressing and routing. NAPT functionality should be used frequently.

3.2. Serial SCADA protocols

A SCADA serial protocol typically uses simple 8 or 16 bit addressing. The mobile network address scheme is an IP network, where range is defined by the service provider (sometimes including individual addresses, even in the case of a private APN). Consequently, a mechanism of translation between SCADA and the IP addresses is required. To make matters worse, IP addresses may be assigned to GPRS (EDGE, UMTS, etc.) devices dynamically upon each connection.

Please read application note *"M!DGE/MG102i - Serial SCADA Protocols"*[1] which describes how to efficiently solve this problem using RACOM routers.

3.3. Network center

In every network, the center plays a key role and has to be designed according to customer's requirements. Several possible solutions are described in the application note *"M!DGE/MG102i - Typical usage"*[2].

3.4. VPN tunnels

Customer data security arriving through the mobile network is often very important. Private APN is the basic security requirement, but not safe enough for such applications.

VPN tunnels solution is closely connected with the center and is also described in application note *"M!DGE/MG102i - VPN Configuration"*[3].

---

[1] https://www.racom.eu/eng/products/m!midge/app/scada.html
[2] https://www.racom.eu/eng/products/m!midge/app/midge-mg102i_centre.html
[3] https://www.racom.eu/eng/products/m!midge/app/VPN_config.html

---

4. Product

4.1. Dimensions
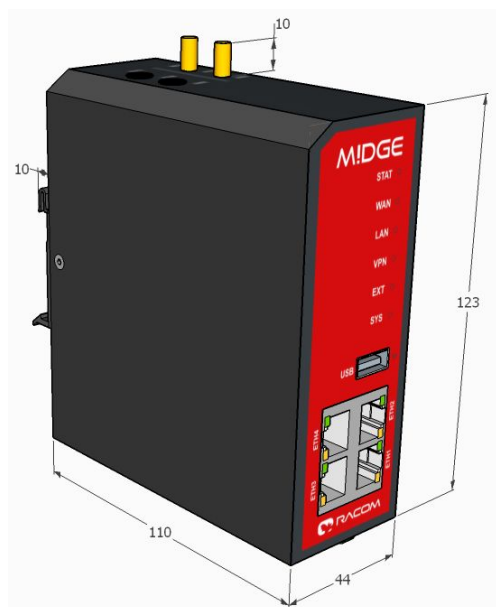
Fig. 4.1: Dimensions in millimeters

4.2. Connectors

4.2.1. Antenna SMA

Fig. 4.2: Antenna connectors SMA

The M!DGE router is equipped with two antenna connectors. The ANT connector serves as a main antenna connection, the AUX connector is auxiliary and serves for better communication with BTS (diversity).

4.2.2. 4× Eth RJ45
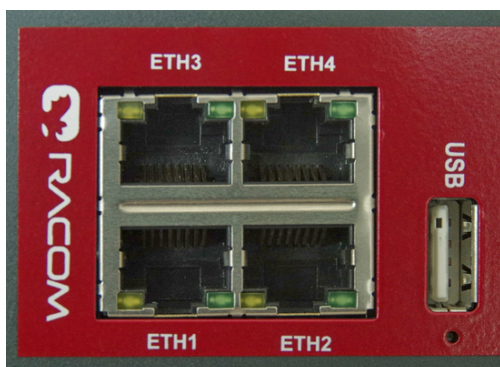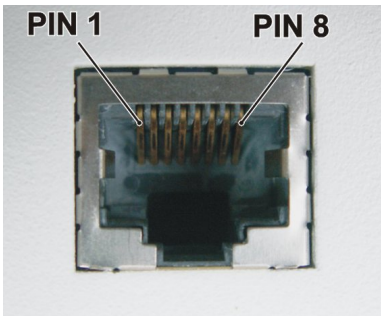
Fig. 4.3: 4× Eth RJ45 Plug

Tab. 4.1: Pin assignment Ethernet interface

RJ-45 Socket	ETH (Ethernet 10BaseT and 100BaseT)	
pin	signal	
1	TX+	
2	TX−	
3	RX+	
6	RX−	

> **Note**
>
> Pairs 4-5 and 7-8 have an internal 75 Ohm termination.
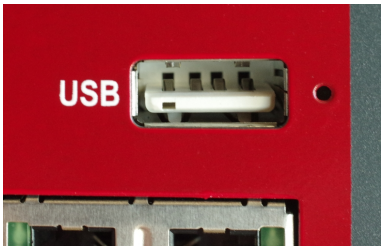
Tab. 4.2: Ethernet Port Specification

Feature	Specification
Speed	10/100 Mbps
Mode	TX−
Crossover	Automatic MDI/MDI-X

4.2.3. USB

M!DGE uses USB 2.0, Host A interface. USB interface is wired as standard:

Tab. 4.3: USB 2.0 Host Port Specification

Feature	Specification	
Speed	Low, Full & Hi-Speed	
Current	max. 500 mA	
Max. cable length	3 m	
Cable shield	mandatory	
Connector type	Type A	

Tab. 4.4: USB pin description

USB pin	signal	wire
1	+5 V	red
2	Data (−)	white
3	Data (+)	green
4	GND	black

4.2.4. MicroSIM cards
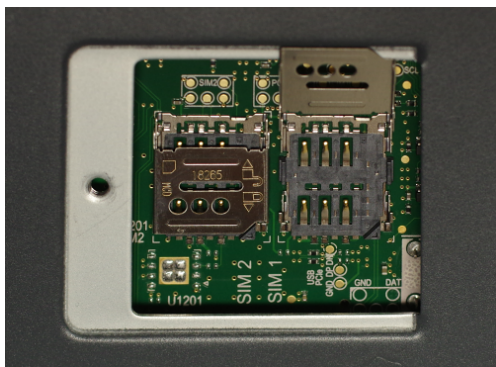
Fig. 4.4: MicroSIM cards slots

The M!DGE router is equipped with two MicroSIM (3FF) cards slots which are placed under a SIM card cover. Use PH0 screw driver for its opening. If using only one SIM card, use holder one.

The SIM card holder has a locking mechanism - for opening pull the front part of the holder down and then you can open it. After inserting of SIM card (cropped edge left, connectors down), close the holder and lock it.

⚠️ **Important**

Power off the router before inserting the SIM card.

4.2.5. Screw terminal

Fig. 4.5: Screw terminal

Screw terminal plug types:
Phoenix Contact 1847204 (MC 1.5/10-STF-3.5) for 10 pins plug and
Phoenix Contact 1847181 (MC 1.5/ 8-STF-3.5) for 8 pins plug (or equivalent).
This EXT plug is delivered only for units equipped with internal extension module.
Nominal cross section: 1.5 mm²

Tab. 4.5: Screw terminal pin assignment

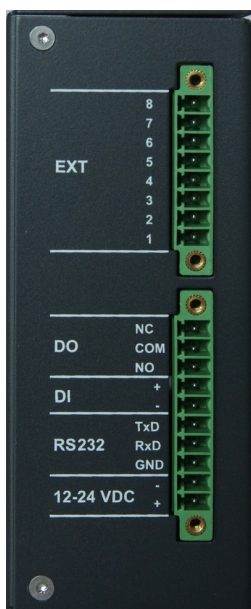| pin	pin description	signal
1	12-24 VDC +	Power input plus: 12–24 VDC (−20% +20 %) = 9.6–28.8 VDC
2	12-24 VDC -	Power input minus – internally connected with casing
3	RS232 GND	RS-232 GND (non-isolated)
4	RS232 RxD	RS-232 RxD (non-isolated)
5	RS232 TxD	RS-232 TxD (non-isolated)
6	DI -	Digital input - Negative signal input (isolated to GND)
7	DI +	Digital input - Positive signal input (isolated to GND)
8	DO NO	Digital Output isolated, Relay contact normally open
9	DO COM	Digital Output isolated, Relay common
10	DO NC	Digital Output isolated, Relay contact normally closed

Polarity Reversal protection circuit (PTC fuse) used on pin 1 and pin 2, but the reverse polarity with soft power supply could cause damage after a few minutes of wrong polarity attached.

Pins 2 and 3 Pins are internally connected.

Pins 6 and 7 are galvanically isolated (1.5 kVAC). If voltage between the + and – pins is bigger than 60 VDC, the input circuit could be damaged. Reversed polarity will not harm the circuit.

Tab. 4.6: Digital input levels

logical level 0	0 to 3 VDC
logical level 1	9 to 32 VDC
Note: Negative input voltage is not recognised.	

Tab. 4.7: Digital output parameters

Maximal continuous current	1 A
Maximal switching voltage	32 VDC
Maximal switching capacity	32 W

4.2.6. Reset button

The Reset button is placed close to the USB connector. Use a blunt tool no more than 1 mm in diameter (e.g. a paper clip) to press the button.

The reset button has two functions:

- Reboot the system
  - Press at least 3 seconds to release a system reboot.
  - The reboot is indicated with the red blinking STAT LED.

- Factory reset
  - Press at least 10 seconds to release a factory reset.
  - The start of the factory reset is confirmed by all LEDs lighting up GREEN for a second.

Fig. 4.6: Reset button

- Recovery procedure
  - Press at least 15 seconds to release a recovery procedure.
  - The start of the recovery procedure is confirmed by all LEDs lighting up RED for a second.
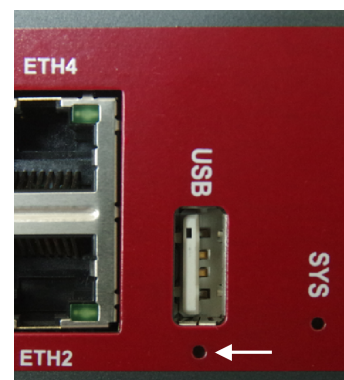
> **(i) Note**
>
> Contact our technical support (support@racom.eu) for recovery procedure details and required files.

4.3. Indication LEDs

Fig. 4.7: Indication LEDs

The following table describes the default M!DGE status indicators.

Tab. 4.8: M!DGE interfaces and status indicators

Description	State	Function
STAT	green blinking	Device busy device is in startup, software or configuration update
	green on	Device is ready
WAN	off	Hotlink is disabled
	blinking	Hotlink connection is being established
	on	Hotlink connection is up
LAN	green	ETH: enabled as LAN and link status is up
	off	No ETH LAN-connection is up
VPN	green on	VPN connection is up
	green blinking	VPN connection is being established
	off	VPN connection down
EXT	on / off / blinking	EXT LED indicates the state of the extension interfaces. Hint: Cellular (WWAN) signal strength can be indicated (green = excellent, orange = medium, red = weak).
SYS		Shows the overall system state. This could be derived from health indicators such as: - all services up and running - overall throughput is normal - CPU load is normal - the supervisor - User application (state set by user in SDK or LXC)
	green on	System operation state: normal
	green blinking	System operation state: warning or in a transition
	red on	System operation state: emergency, watchdog, failure

4.4. Technical specifications

Tab. 4.9: Technical specifications

|	
Frequency bands E	4G LTE Band 20 (800 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 3 (1800 MHz), Band 1 (2100 MHz), Band 7 (2600 MHz)
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz
	Ublox TOBY L-210 FCC ID XPYTOBL210
Frequency bands P	4G LTE Band 28 (750 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 3 (1800 MHz), Band 1 (2100 MHz), Band 7 (2600 MHz)
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz
	Ublox TOBY L-280 FCC ID XPYTOBL280
Frequency bands A	4G LTE Band 17 (700 MHz), Band 5 (850 MHz), Band 4 (1700 MHz), Band 2 (1900 MHz), Band 7 (2600 MHz)
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 4 (AWS, i.e. 1700 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz
	Ublox TOBY L-200 FCC ID XPYTOBL200
Frequency bands U	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz
Specification	4G LTE 3GPP Release 9 Long Term Evolution (LTE) Evolved Uni. Terrestrial Radio Access (E-UTRA) Frequency Division Duplex (FDD) DL Multi-Input Multi-Output (MIMO) 2×2
	3G UMTS/HSDPA/HSUPA 3GPP Release 8 Dual-Cell HS Packet Access (DC-HSPA+) UMTS Terrestrial Radio Access (UTRA) Frequency Division Duplex (FDD) DL Rx diversity
	2G GSM/GPRS/EDGE 3GPP Release 8 Enhanced Data rate GSM Evolution (EDGE)

	GSM EGPRS Radio Access (GERA) Time Division Multiple Access (TDMA) DL Advanced Rx Performance Phase 1
	Data rates up to 150 Mbps downlink / 50 Mbps uplink

Ethernet	4× Ethernet 10/100 Base-T, Auto MDX, 4× RJ45, bridged or routed
Serial Interface	1× 3-wire RS232 on 15-pin screw terminal block

Digital I/O	1 digital input	0–3 VDC level 0
		9–32 VDC level 1
	1 digital output	Relay outputs
		Limiting continuous current 1 A
		Max. switching voltage 32 VDC
		Max. switching capacity 32 W
		Isolation 1500 Vp (transients)
GNSS (option)	Active antenna 3.3 VDC; SMA female	
	72-channel Ublox M8 engine GPS/QZSS L1 C/A, GLONASS L10F BeiDou B1I, Galileo E1B/C, SBAS L1 C/A: WAAS, EGNOS, MSAS, GAGAN	
	Ublox NEO-M8N	
GNSS Time pulse (option)	TTL logic: 1 pulse/s; SMA female	
USB service interface	USB host interface supporting memory devices USB type A connector USB2.0	
SIM	2× micro SIM (3FF)	
Antenna Interface	Impedance:	50 Ω
	Connector:	2× SMA female supporting MIMO
Power Supply	Input voltage:	9.6–28.8 VDC (12–24 VDC −20 % / +20 %)
	Avg. power consumption:	7 W (including max. 2.5 W on USB port)
Environmental Conditions	For indoor use only, IP40	
	Metal casing, DIN rail mounting kit included	
	Temperature range:	−40 to +70 °C (−40 to +158 °F)
	Humidity:	0 to 95 % (non condensing)
	MTBF (Mean Time Between Failure):	> 220.000 hours (> 25 years)
	Vibration & shock:	ETS 300 019-2-3:1994, Class 3.4
	Seismic:	EN 60068-2-27:2010
	Environmental:	EN 61850-3: 2014 IEEE 1613:2009

Mounting	DIN rail mounting
Dimensions	45 W × 110 D × 125 H mm (1.77 × 4.33 × 4.92 in)

Weight	Ca. 450 g (0.99 lbs)
Type Approval	CE, FCC

Options	
Antennas	Various antennas suitable for your application are available
Mounting kit	Flat bracket mounting kit

4.5. Model offerings
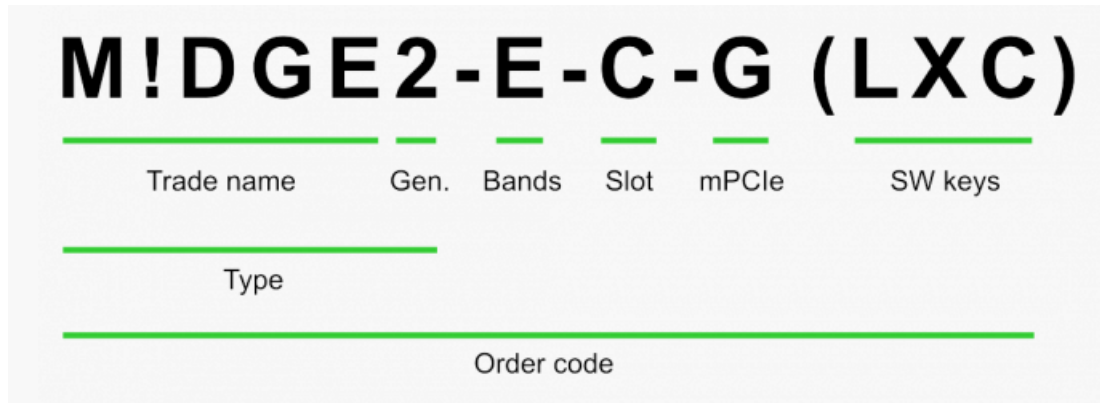
- **Trade name** - trade and marketing name of the product. This name is used for all products within the same product family.
  Possible values:
  M!DGE

- **Gen.** - generation of the product of specific Trade name. The very first generation doesn't have any number in this position.
  Possible values:
  none
  2

- **Band** - *frequency bands*
  Possible values:
  E – 4G/3G/2G, Europe, Middle East, Africa
  P – 4G/3G/2G, Asia, Pacific, South America
  A – 4G/3G/2G, Americas
  U – only 3G/2G, world wide
  NOTE: 'P' and 'A' are available for high volumes only.

- **Slot** - Proprietary extension slot
  Possible values:
  N – not used
  C – The second RS232/485 + 1× DI, 1× DO, Part No.: M!DGE2-HW-COM/IO

pin description	signal
1	RS-232 GND (non-isolated)
2	RS-232 RxD (non-isolated); RS485 A (Half-Duplex)
3	RS-232 TxD (non-isolated); RS485 B (Half-Duplex)
4	Digital input - Negative signal input (isolated to GND)
5	Digital input - Positive signal input (isolated to GND)
6	Digital Output isolated, Relay contact normally opened
7	Digital Output isolated, Relay common
8	Digital Output isolated, Relay contact normally closed

- **mPCIe** - mPCIe slot
  Possible values:
    N – not used
    E – The second cellular module, Bands E, Part No.: mPCIe-E
    P – The second cellular module, Bands P, Part No.: mPCIe-P
    A – The second cellular module, Bands A, Part No.: mPCIe-A
    U – The second cellular module, Bands U, Part No.: mPCIe-U
    G – Internal GPS (GNSS) module, Part No.: mPCIe-GPS
    NOTE: Just one option for mPCIe slot is possible.

- **Bands, Slot, mPCIe** positions are used only for M!DGE2.

- **SW keys** - if unit is ordered with SW keys, all keys are specified in this bracket. SW key activates the feature, which is under the license. SW key can be ordered independently for specific S/N anytime later on.
  Possible values M!DGE2:
    LXC – Linux container, Part No.: M!DGE2-SW-LXC
    SERVER – Server clients extension, Part No.: M!DGE2-SW-SERVER

Feature	Default	SW key SERVER
DHCP reservations	35	35
Local host names	35	35
NAPT rules	35	35
Firewall rules	50	50
Firewall address groups	15	15
OpenVPN clients	10	25
Static routes	30	30
Mobile IP	yes	yes
DynDNS server	no	yes

- **Type** - specific product type for which type approvals like CE, FCC etc. are issued.
  Possible values:
    M!DGE
    M!DGE2

- **Order code** – the complete product code, which is used on Quotations, Invoices, Delivery notes etc.

In order to find out the correct Order code, please use **RACOM WebService**[1].

---

[1] https://webservice-new.racom.eu/main/eshop.list?t=10

4.6. Accessories

4.6.1. F bracket

Flat-bracket

Installation bracket for flat mounting. For usage details see chapter *Mounting* and chapter *Dimensions*.
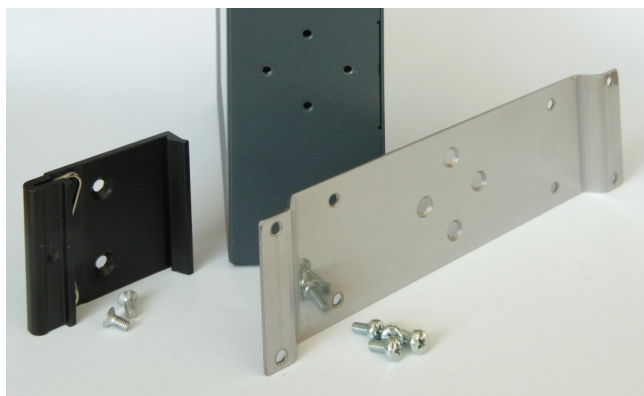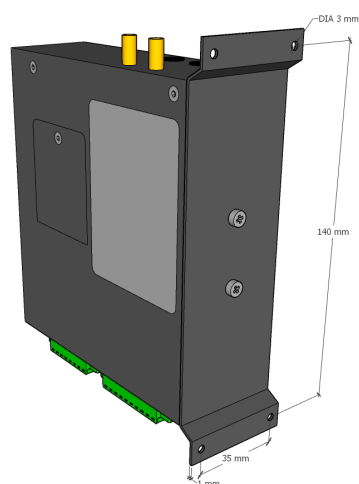

Fig. 4.8: Flat bracket

Fig. 4.9: Flat bracket dimensions

5. Bench test / Step-by-Step guide

Before starting to work with the HW please be sure that you have a SIM card enabled for data and you have all the necessary information from the mobile operator (PIN, APN, login, passwd)

5.1. Connecting the hardware

5.1.1. Install the SIM card

Insert a SIM card into the SIM socket, use the first one. Make sure the SIM is enabled for data transmission.

There are two reasons for installing the SIM card as the first task: a) the SIM card could be damaged when inserted into the powered equipment, b) the information from SIM card are read only after a power cycle.

5.1.2. Connect the cellular antenna

Fit a cellular antenna. For details see *RACOM web*[1] or contact RACOM for suitable antennas.

5.1.3. Connect the LAN cable

Connect one M!DGE Ethernet port to your computer using an Eth cat.5 cable.

5.1.4. Connect the power supply

Connect the power supply wires to the M!DGE screw terminals, ensuring correct polarity. Switch on the power supply.

5.2. Powering up your wireless router

Switch on your power supply. The STAT LED flashes for a few seconds and after 8 seconds it starts blinking to a green light. After approximately 30 seconds your router will have booted and will be ready; the STAT LED remains shining.

When the Mobile Connection is enabled the WAN LED starts blinking while connecting to the cellular network – the color (green/orange/red) represents the signal strength (excellent, medium, weak).

You'll find the description of the individual LED states in *Section 4.3, "Indication LEDs"*.

5.3. Connecting M!DGE to a programming PC

a. Please connect the Ethernet interfaces of your computer and M!DGE.
b. If not yet enabled, please enable the Dynamic Host Configuration Protocol (DHCP) so that your computer can lease an IP address from M!DGE. Wait a moment until your PC has received the parameters (IP address, subnet mask, default gateway, DNS server).

Alternative: Instead of using the DHCP, configure a static IP address on your PC (e.g. `192.168.1.10` mask `255.255.255.0`) so that it is operating in the same subnet as the M!DGE.

---

[1] https://www.racom.eu/eng/products/gprs-router-midge.html#accessories_antennas

The default IP address is `192.168.1.1` for all Eth interfaces (Eth1 - Eth4), the default subnet mask is `255.255.255.0` for all interfaces.

Default DHCP range 192.168.1.100 to 192.168.1.199

c. Start a Web Browser on your PC. Type the M!DGE IP address in the address bar: `http://192.168.1.1`

d. Please set a password for the admin user account. Choose something that is both easy to remember and a strong password (such as one that contains numbers, letters and punctuation). The password must have a minimum length of 6 characters. It must contain a minimum of 2 numbers and 2 letters.

Admin Password Setup

Please set a password for the admin account.
It shall have a minimum length of 6 characters and contain at least 2 numbers and 2 letters.

Username:	admin
Enter new password:	●●●●●●●
Confirm new password:	

☐ I agree to the terms and conditions

☐ Configure automatic mobile data connection

Apply

> (i) **Note**
>
> For security reasons, there is no default password.

e. Agree to the terms and conditions. The user is now obliged to accept our end user license agreement during the initial M!DGE setup.
f. You might check the "Configure automatic mobile data connection" for automatic WWAN configuration. Manual changes are usually required afterwards. Note that Firewall is also enabled with predefined WAN administration ports.

5.4. Basic setup

The M!DGE Web Manager can always be reached via the Ethernet interface. After successful setup, Web Manager can also be accessed via the mobile interface. Any up to date web browser can be used. Any web browser supporting JavaScript can be used. By default, the IP address of the 1st Ethernet interface is 192.168.1.1, the web server runs on port 80.

The minimum configuration steps include:

1. Defining the admin password
2. Entering the PIN code for the SIM card
3. Configuring the Access Point Name (APN)
4. Starting the mobile connection

> (i) **Note**
>
> Router M!DGE can be safely turned off by unplugging the power supply.

6. Installation

6.1. Mounting

M!DGE Wireless Router is designed for a DIN rail mounting or on a panel using flat bracket. Please consider the safety instructions in *Section 6.1, "Mounting"*.

6.2. Antenna mounting

M!DGE Wireless Routers will only operate reliably over the cellular network if there is a strong signal. For many applications the flexible stub antenna provided would be suitable but in some circumstances it may be necessary to use a remote antenna with an extended cable to allow the antenna itself to be positioned so as to provide the best possible signal reception.

Beware of the deflective effects caused by large metal surfaces (elevators, machine housings, etc.), close meshed iron constructions and choose the antenna location accordingly. Fit the antenna or connect the antenna cable to the ANT connector.

In external antennas the surge protection of coaxial connection would be required.

Note

Be sure that the antenna was installed according to the recommendation by the antenna producer and all parts of the antenna and antenna holder are properly fastened.

6.3. Power supply

M!DGE can be powered with an external power source capable of voltages from 9.6 to 28.8 Volts DC. M!DGE should be powered using a certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output.

7. Web Configuration

7.1. HOME

This page gives you a system overview. It helps you when initially setting up the device and also functions as a dashboard during normal operation.

The highest priority link which has been established successfully will become the so-called **hotlink** which holds the default route for outgoing packets.

Detailed information about status of each WAN interface is available in a separate window.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WWAN1

Status
Summary
WAN
WWAN
Ethernet
LAN
Bridges
DHCP
System

Description	Value
Administrative state	enabled
Operational state	up
Link is up since	2018-03-05 14:55:04
IP address	10.203.0.28
Modem	Mobile1
SIM	SIM1 (ready)
PDP	PDP1
Registration status	registeredInHomeNetwork
Service type	HSPA
Network	O2 - CZ@ (Cell EDB1860)
Signal level	48% (medium)
Transfer rate down / up	0 bit/s / 0 bit/s
Data downloaded / uploaded	387.88 KB / 583.25 KB reset

7.2. INTERFACES

Details for all physical connections are given in *Section 4.2, "Connectors"*.

7.2.1. WAN

Link Management

Each available item in the WAN Link Manager matches with the particular WAN interface. Depending on your hardware model, WAN links can be made up of either Wireless Wide Area Network (WWAN), Wireless LAN (WLAN), Ethernet or PPP over Ethernet (PPPoE) connections. Please note that each WAN link has to be configured and enabled in order to appear on this page.

In case a WAN link goes down, the system will automatically switch over to the next link in order of priority (the priorities can be changed using the arrows on the right side of the window). A link can be either established when the switch occurs or permanently to minimize link downtime.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

WAN Link Management

In case a WAN link goes down, the system will automatically switch over to the next link in order of priority. A link can be either established when the switch occurs or permanently to minimize link downtime. Outgoing traffic can also be distributed over multiple links on a per IP session basis.

Priority	Interface	Operation Mode		
1st	LAN2	permanent ∨	⬇	⬒
2nd	WWAN1	permanent ∨	⬆	⬒

Apply

1st priority: This link will be used whenever possible.

2nd priority: The first fallback technology.

Up to four priorities can be used.

Links are being triggered periodically and put to sleep in case it was not possible to establish them within a certain amount of time. Hence it might happen that permanent links will be dialed in background and replace links with lower priority again as soon as they got established. In case of interfering links sharing the same resources (for instance in dual-SIM operation) you may define a switch-back interval after which an active hotlink is forced to go down in order to let the higher-prio link getting dialed again.

Bridge interface: If WAN is configured as WLAN client, the LAN interface to which the WAN link should be bridged.

Outgoing traffic can also be distributed over multiple links on a per IP session basis. Choose the option "distributed" as an Operation Mode with the appropriate Weight.

In the following example, the outgoing traffic will be distributed between LAN2 (80 %) and WWAN1 (20 %) links.

(i) Note

This option is general and applies to all outgoing traffic. See *Section 7.3.3, "Multipath Routes"* for more detailed configuration.

We recommend using the **permanent** option for WAN links. However, in case of time-limited mobile tariffs, the **switchover** option should be used.

After clicking on the WWAN "Edit" button, you can additionally set the "IP passthrough" option for the selected LAN interface. The result is that the connected device over the selected LAN port will obtain M!DGE's mobile IP address via DHCP. In another words, M!DGE will be transparent for the connected device and will only serve for the mobile connectivity. Typically, such connected device (e.g. firewall) will not need any special configuration facing M!DGE, it will just use its mobile IP address (usually the public IP address).

Once established, a small subnet containing the cellular IP is created, by default the netmask is 255.255.255.248. This small subnet consists of a network and broadcast address as a regular subnet. In some situations it may lead to unreachability of several remote hosts due to IP address overlapping. If this is the case, user can manually configure the APN network, e.g. 10.203.0.0/255.255.128.0.

In any case, the M!DGE unit is reachable via the default gateway automatically obtained from M!DGE by DHCP. The gateway IP address is set as the first available IP address after the specified APN address range. If not specified, it is the first usable IP within the /29 subnet.

(i) **Note**

We recommend to define the APN network/netmask manually. There might be situations in which the default /29 disables the communication. E.g. WWAN IP is 10.10.10.6. The connected device obtains this IP via DHCP and sets the default gateway to 10.10.10.7 - but this IP is a broadcast IP within /29 subnet and the communication is not possible. If you configure subnet 10.10.10.0/29 manually, a default gateway would be 10.10.10.8 in newly created local /28 subnet.

Example: If the APN network is 10.203.0.0/17, the default gateway is set to 10.203.128.0. The web interface is reachable via this IP address over the selected LAN interface. The connected device's network mask is /16 (1 bit wider), otherwise the default gateway would not be usable.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

| | LAN1 | LAN2 | | | |

Status
Summary
WAN
WWAN
Ethernet
LAN
DHCP
System

DHCP Leases on LAN2

Interface	IP Address	MAC Address	Name	Expires
LAN2	10.203.0.29	00:23:AE:02:5E:E0	mrazek-NB	2016-09-22 12:26:10

(i) **Note**

- This option is configurable within WWAN links only. Remember that LAN1 cannot be used as the port for the IP passthrough functionality.

- LAN10 is not usable within M!DGE routers. Do not select it.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Setup
VLAN Management
IP Settings

Mobile
Modems
SIMs
Interfaces

Bridges

USB

Serial

Digital I/O

WAN Link Configuration WWAN1

Operation mode:	permanent

Multipath-TCP:	disabled

IP pass-through:	⦿ enabled
	◯ disabled
	Interface: LAN2
	WAN network: 10.203.0.0 (optional)
	WAN netmask: 255.255.128.0 (optional)

Apply   Cancel

Connection Supervision

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Link Supervision

Network outage detection can be performed by sending pings on each WAN link to authoritative hosts. The link will be declared as down in case all trials failed. You may further specify an emergency action if a certain downtime is reached.

Link	Hosts	Emergency Action	
WWAN1	10.203.0.1	reboot after 30 min	⊟ ☑
			⊞

Network outage detection can be used for switching between available WAN links and can be performed by sending pings on each link to authoritative hosts. A link will be declared as down if all trials have failed. The link will be considered up again if at least one host is reachable.

You may further specify an emergency action if no uplink can be established at all.

Configurable actions are:

• None
• Restart link services
• Reboot system

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

USB

Serial Port

Digital I/O

Link Supervision

Network outage detection can be performed by sending pings on each WAN link to authoritative hosts. The link will be declared as down in case all trials failed. You may further specify an emergency action if a certain downtime is reached.

Link:	WWAN1 ⌄
Mode:	○ also validate when link comes up
	● only validate if link is up
Primary host:	10.203.0.1
Secondary host:	(optional)
Ping timeout:	5000 milliseconds
Ping interval:	60 seconds
Retry interval (if ping failed):	20 seconds
Max. number of failed trials:	5
Emergency action:	○ none
	○ restart link services
	● reboot system
	after 30 minutes being down

Apply

Link:	The WAN link to be monitored (can be ANY for all configured links).
Mode:	Specifies whether the link is monitored during the connection establishment or only when it is already up.
Primary host:	Reference host one which will be used for checking IP connectivity (via ICMP pings).
Secondary host:	Reference host two which will be used for checking IP connectivity (via ICMP pings). The test is considered successful if either the primary or the secondary host answers.
Ping timeout:	Time for which the system is waiting for the ping response. With mobile networks the response time can be quite long (several seconds) in special cases. You can check the typical response using SYSTEM – Troubleshooting – Network Debugging – Ping. The first response typically takes a longer time than the following ones in cellular networks, the Ping timeout should be set to the longer time than with the first response.
Ping interval:	Time to wait before sending the next probe.
Retry interval (if ping failed):	If the first trial fails, ping hosts in this modified interval until the ping is successful or the maximum number of failed trials is reached.
Max. number of failed trials:	The maximum number of failed ping trials until the ping check will be declared as failed.
Emergency action:	Configure the Emergency action which should be taken after the maximum downtime is reached. Using "reboot" performs the system reboot. The option "restart services" restarts all link-related applications including the modem reset. No action is done if the "none"

option is set. Configure the maximum amount of downtime in minutes for which the link could not be established.

Settings

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

USB

TCP Maximum Segment Size

The maximum segment size defines the largest amount of data of TCP packets (usually MTU minus 40). You may decrease the value in case of fragmentation issues or link-based limits.

MSS adjustment:
○ enabled
○ disabled

Maximum segment size: [1360]

[Apply]

The maximum segment size defines the largest amount of data of TCP packets (usually MTU minus 40). You may decrease the value in case of fragmentation issues or link-based limits.

MSS adjustment   Enable or disable MSS adjustment on WAN interfaces.

Maximum segment size   Maximum number of bytes in a TCP data segment.

7.2.2. Ethernet

M!DGE routers ship with 4 dedicated Ethernet ports (ETH1 to ETH4) which can be linked via RJ45 connectors.

ETH1 usually forms the LAN1 interface which should be used for LAN purposes. Other interfaces can be used to connect other LAN segments or for configuring a WAN link. The LAN10 interface will be available as soon as a pre-configured USB Ethernet device has been plugged in (e.g. XA Ethernet/USB adapter).

Port Setup - Port Assignment

This menu can be used to individual assigning of Ethernet ports to LAN interfaces if you want to have different subnets per port or to use one port as the WAN inteface.

If it is desired to have both ports in the same LAN you may assign them to the same interface. Please note that the ports will be bridged by software and operated by running the Spanning Tree Protocol.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Port Assignment | Link Settings

Ethernet 1

Administrative status: ● enabled ○ disabled

Network interface: LAN1 ∨

Ethernet 2

Administrative status: ● enabled ○ disabled

Network interface: LAN1 ∨

Ethernet 3

Administrative status: ● enabled ○ disabled

Network interface: LAN1 ∨

Ethernet 4

Administrative status: ● enabled ○ disabled

Network interface: LAN4 ∨

Apply

WAN
Link Management
Supervision
Settings

Ethernet
Port Setup
VLAN Management
IP Settings

Mobile
Modems
SIMs
Interfaces

Bridges

USB

Serial

Digital I/O

Port Setup - Link Settings

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Port Assignment | Link Settings

Link speed for Ethernet 1: auto-negotiated ∨

Link speed for Ethernet 2: auto-negotiated ∨

Apply

WAN
Link Management
Supervision
Settings

Ethernet
Port Setup
VLAN Management
IP Settings

Link negotiation can be set for each Ethernet port individually. Most devices support auto negotiation which will configure the link speed automatically to comply with other devices in the network. In case of negotiation problems, you may assign the modes manually but it has to be ensured that all devices in the network utilize the same settings then.

VLAN Management

M!DGE routers support Virtual LAN according to IEEE 802.1Q which can be used to create virtual interfaces on top of the Ethernet interface. The VLAN protocol inserts an additional header to Ethernet frames carrying a VLAN Identifier (VLAN ID) which is used for distributing the packets to the associated virtual interface. Any untagged packets, as well as packets with an unassigned ID, will be distributed to the native interface. In order to form a distinctive subnet, the network interface of a remote LAN host must be configured with the same VLAN ID as defined on the router. Further, 802.1P introduces a priority field which influences packet scheduling in the TCP/IP stack.

The following priority levels (from the lowest to the highest) exist:

Parameter	VLAN Priority Levels
0	Background
1	Best Effort
2	Excellent Effort
3	Critical Applications
4	Video (< 100 ms latency and jitter)
5	Voice (< 10 ms latency and jitter)
6	Internetwork Control
7	Network Control

IP Settings

Two individual tabs will be used when different LANs are set in the Port settings menu. Each of them can be configured either in the LAN mode or in the WAN mode.

> **ⓘ Note**
>
> The default IP address is 192.168.1.1/24 (LAN1).

Static configuration of M!DGE's own IP address and Subnet mask is available for the LAN mode. The Alias IP address enables configuring the LAN interface with a second IP address/subnet.

MTU   Configure MTU of a given Ethernet interface.

> **ⓘ Note**
>
> Setting of the IP address is interconnected with the DHCP Server (if enabled) - menu the SERVICES - DHCP Server menu.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

| LAN1 | LAN2 |

WAN
  Link Management
  Supervision
  Settings

Ethernet
  Port Setup
  VLAN Management
  IP Settings

Mobile
  SIMs
  Interfaces

USB

Serial

Digital I/O

IP Settings LAN1

Mode:
○ LAN
◉ WAN

WAN mode:
○ DHCP client
◉ static IP
○ PPPoE

Static Configuration

IP address: `192.168.1.1`

Netmask: `255.255.255.0`

Default gateway: `192.168.1.254`

Primary DNS server: `192.168.1.254`

Secondary DNS server: `_____`

MTU: `_____`

[Apply]   [Continue]

WAN mode enables the following possibilities:

DHCP client: The IP configuration will be retrieved from a DHCP server in the network. No further configuration is required (you may only set MTU).

Static IP: IP configuration will be set manually. At least the Default gateway and the Primary DNS server must be configured along with the IP address and subnet mask.

PPPoE: PPPoE is the preferred protocol when communicating with another WAN access device (like a DSL modem).

Username: PPPoE user name to be used for authentication at the access device.

Password: PPPoE password to be used for authentication at the access device.

Service Name: Specifies the service name set of the access concentrator. Leave it blank unless you have many services and need to specify the one you need to connect to.

Access Concentrator   This may be left blank and the client will connect to any
Name: access concentrator.

7.2.3. Mobile

Modems

Configuration

This page lists all available WWAN modems. They can be disabled on demand.

Query

This page allows you to send Hayes AT commands to the modem. Besides the 3GPP-conforming AT command-set, further modem-specific commands can be applied (can be provided on demand). Some modems also support running Unstructured Supplementary Service Data (USSD) requests, e.g. for querying the available balance of a prepaid account.

SIMs

The SIM page gives an overview about the available SIM cards, their assigned modems and the current state. Once a SIM card has been inserted, assigned to a modem and successfully unlocked, the card should remain in state ready and the network registration status should have turned to registered. If not, please double-check your PIN.

Please keep in mind that registering to a network usually takes some time and depends on signal strength and possible radio interferences. You may hit the Update button at any time in order to restart PIN unlocking and trigger another network registration attempt.

Under some circumstances (e.g. in case the modem flaps between base stations) it might be necessary to set a specific service type or assign a fixed operator. The list of operators around can be obtained by initiating a network scan (may take up to 60 seconds). Further details can be retrieved by querying the modem directly, a set of suitable commands can be provided on request.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
  Link Management
  Supervision
  Settings

Ethernet
  Port Setup
  VLAN Management
  IP Settings

Mobile
  Modems
  SIMs
  Interfaces

Mobile SIMs

This menu can be used to assign a default modem to each SIM which will also be used by SMS and GSM voice services. A SIM card can get switched in case of multiple WWAN interfaces sharing the same modem.

SIM	Default	Current	State	PIN Protection	Registered	
SIM1	Mobile1	Mobile1	ready	disabled	yes	
SIM2	none	none	unassigned	unknown	no	

Update

Configuration

A SIM card is generally assigned to a default modem but this may switch, for instance if you set up two WWAN interfaces with one modem but different SIM cards. Close attention has to be paid when other services (such as SMS or Voice) are operating on that modem as a SIM switch will affect their operation.

You can configure the following parameters:

PIN protection	Depending on the used card, it can be necessary to unlock the SIM with a PIN code. Please check the account details associated with your SIM whether the PIN protection is enabled.
PIN code	The PIN code for unlocking the SIM card
PUK code	The PUK code for unlocking the SIM card if the card was blocked due to several wrong PIN attempts.
Default modem	The default modem assigned to this SIM card.
Bands	The list of allowed bands to which the unit can connect. Current ublox module does not support manual band selection.
Preferred service	The preferred service type to be used with this SIM card. Remember that the link manager might change this in case of different settings. The default option is "automatic", in areas with interfering base stations you can force a specific type (e.g. 3G-only) in order to prevent any flapping between the stations around.
Registration mode	The default option is set to "all networks". You can limit the modem registration to "packet-switched only" (e.g. no Dial-in Server) or "circuit-switched only" option, which can be for example used for the Dial-in Server so one can use PPP over the Circuit-Switched Networks (analog modem style).
Network selection	LAI is a globally unique number that identifies the country, network provider and LAC of any given location area. It can be used to force the modem to register to a particular mobile cell in case of competing stations. You may further initiate mobile network scan for getting networks in range and assign a LAI manually.

WWAN Interfaces

This page can be used to manage your WWAN interfaces. The resulting link will pop up automatically on the WAN Link Management page once an interface has been added. The Mobile LED will be blinking during the connection establishment process and goes on as soon as the connection is up. Refer to the troubleshooting section or log files in case the connection did not come up.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Setup
VLAN Management
IP Settings

Mobile
Modems
SIMs
Interfaces

Mobile Interfaces

Interface	Modem	SIM	PDP	Number	Service	APN / User		
WWAN1	Mobile1	SIM1	PDP1	*99***1#	2G-only	internet	⊖	☑
								⊕

The following mobile settings are required:

Modem   The modem to be used for this WWAN interface

SIM   The SIM card to be used for this WWAN interface

Preferred service   The preferred service type

Please note that these settings supersede the general SIM based settings as soon as the link is being dialed.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

USB

Serial Port

Digital I/O

Edit WWAN Interface WWAN1

Mobile | Connection | Advanced

Connection settings: ○ load from database
                             ● specify

Phone number: *99***1#

Access point name: internet

Authentication: None ▾
                             None
                             PAP
                             CHAP
                             PAP+CHAP

[Apply]

Generally, the connection settings are derived automatically as soon as the modem has been registered and the network provider has been found in our database. Otherwise, it will be required to configure the following settings:

Phone number   The phone number to be dialed, for 3G+ connections this commonly refers to be *99***1#. For circuit switched 2G connections you can enter the fixed phone number to be dialed in the international format (e.g. +420xx).

Access point name   The access point name (APN) being used

Authentication	The authentication scheme being used, if required this can be PAP or/and CHAP
Username	The username used for authentication
Password	The password used for authentication

Further on, you may configure the following advanced settings:

Required signal strength	The minimum required signal strength before the connection is dialed. It can be specified as the RSSI level in dBm units, or as the Quality level in percent. See the "more info" button to see the exact values.
Home network only	Determines whether the connection should only be dialed when registered to the home network.
Negotiate DNS	Specifies whether the DNS negotiation should be performed and the retrieved name-servers should be applied to the system.
Call to ISDN	This option must be enabled in case of 2G connections talking to an ISDN modem.
Header compression	Enables or disables Van Jacobson TCP/IP Header Compression for PPP-based connections. This feature will improve TCP/IP performance over slow serial links. Has to be supported by your provider.
Data compression	Enables or disables the data compression for PPP-based connections. Data compression reduces the packet size to improve throughput. Has to be supported by your provider.
Client address	Specifies a fixed client IP address on the mobile interface.

MTU	The Maximum Transmission Unit represents the largest amount of data that can be transmitted within one IP packet and can be defined for any WAN interface.

7.2.4. Bridges

BR1   BR2

WAN
  Link Management
  Supervision
  Settings

Ethernet
  Port Setup
  VLAN Management
  IP Settings

Mobile
  Modems
  SIMs
  Interfaces

Bridges

USB

Serial

Digital I/O

Bridge Settings BR1

Administrative status:
  ○ Disabled
  ○ Enabled
  ◉ Enabled with local interface

Local IP Configuration

IP Address	
Netmask	
MTU	

Apply

Software bridges can be used to bridge layer-2 devices like OpenVPN TAP, GRE or WLAN interfaces without the need for a physical LAN interface.

Administrative status	Enable (with/without local interfaces) or disable software bridges. If you need an interface in the local system, you need to define an IP address for the local device.
IP Address	IP address of the local interface (available only if "Enabled with local interface" was selected)
Netmask	Netmask of the local interface (available only if "Enabled with local interface" was selected)
MTU	Optional MTU size for the local interface (available only if "Enabled with local interface" was selected)

7.2.5. USB

Administration

Enable or disable the USB administration. If enabled, any supported USB converter can be attached and configured for example as another serial link (RS232, see *Section 7.2.6, "Serial Port"*).

> **ⓘ** **Note**
>
> Supported modules are pl2303, ch341, ftdi (quad-channel adapter), asix, pegasus and rndis.

Following parameter can be configured:

- **Enable hotplug (always enabled)**

Click on the Refresh button in the tab Devices for displaying connected USB devices and add them with by clicking on the plus sign.

Autorun

This feature can be used to automatically perform a software/config update as soon as an USB storage stick has been plugged in. Following files must exist in the root directory of a FAT16/32 formatted stick:

- For authentication: `autorun.key`

- For a software update: `sw-update.img`

- For a configuration update: `cfg-<SERIALNO>.zip` or `cfg.zip`

Administrative status   Enable or disable autorun feature.

Only allow enabled devices   Check this if only enabled devices are allowed to proceed with autorun.

The `autorun.key` file must hold valid access keys to perform any actions when the storage device is plugged in. The keys are made up of your admin password (SHA256). They can be generated and downloaded. You may also define multiple keys in this file (line-after-line) in case your admin password differs if applied to multiple M!DGE routers.

For new devices with an empty password the hash key
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 can be used.

The hash keys can be generated by running the command
echo -n "<admin-password>" | sha256sum on a Linux system or an Internet hash key generator (search for "sha-256 hash calculator").

7.2.6. Serial Port

The serial protocol can function in various ways, configure it using the Edit button on the right. If the USB Administration is enabled, an extra SERIAL2 (USB) is available.

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Administration	Port Settings

SERIAL1 is used by:

- ○ none
- ○ login console
- ● device server
- ○ modem emulator
- ○ protocol server
- ○ SDK

[Apply] [Back]

Five possibilities are available:

None	The serial port is not used at all.
Login console	A possibility to control the unit via the CLI commands when connected to the serial port (115200 8N1). There are no extra configuration parameters.
Device server	Use this option to control the serial device via IP (transmit the data over the cellular network, ...). See the details below.
Modem bridge	Direct connection between the LTE modem tty and the serial interface.
Modem emulator	Replacement for legacy dial-in / dial-out connections based on analog or GSM modems (AT commands support).
Protocol server	Special implementation of various serial protocols like Modbus, IEC101, DNP3, ... See the details below.
SDK	This option enables controlling the serial interface via the SDK scripts (similar to C programming). See *chapter SDK* for more details.

Device Server

| Administration | Port Settings |

SERIAL1 Port Settings

Physical protocol:	RS232 ∨
Baud rate:	115200 ∨
Data bits:	8 data bits ∨
Parity:	None ∨
Stop bits:	1 stop bit ∨
Software flow control:	None ∨
Hardware flow control:	None ∨

Server Configuration

Protocol on IP port:	TCP raw ∨
Port:	2000
Timeout:	○ endless ● numbered 600
Allow remote control (RFC 2217):	☐
Show banner:	☑
Allow clients from:	● everywhere ○ specify

[Apply]

WAN
  Link Management
  Supervision
  Settings

Ethernet
  Port Assignment
  VLAN Management
  IP Settings

Mobile
  SIMs
  Interfaces

USB

Serial

Digital I/O

Serial Port Settings:	Configure the required RS232 parameters.	
	Physical protocol:	Only RS232 is supported.
	Baud rate:	Specifies the baud rate of the COM port.
	Data bits:	Specifies the number of data bits contained in each frame.
	Parity:	Specifies the parity used with every frame that is transmitted or received.
	Stop bits:	Specifies the number of stop bits used to indicate the end of a frame.
	Software flow control:	In XON/XOFF software flow control, either end can send a stop (XOFF) or start (XON) character to the other end to control the rate of incoming data.
	Hardware flow control:	While 3 wired connection is used with M!DGE hardware flow control is not available.
Server Configuration:	Protocol on IP port:	"Telnet" or "TCP raw"
	Port:	The TCP port used by the application.
	Timeout:	Endless or numbered (in seconds).

Allow remote control (RFC 2217)	Telnet with the RFC 2217 extension.
Show banner	The option for displaying the banner of the connected serial device.
Allow clients from	The option for limiting the access based on the host IP address.

⚠️ **Important**

The UDP Device Server functionality has been moved into SDK only. The required script for this functionality can be provided on demand.

Modem emulator

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Administration   Port Settings

SERIAL1 Port Settings

Physical protocol:	RS232 ⌄
Baud rate:	115200 ⌄
Hardware flow control:	None ⌄

Incoming Connections via Telnet

Port:	2000

Phonebook Entries

Number	IP address	Port

Apply

WAN
Link Management
Supervision
Settings

Ethernet
Port Setup
VLAN Management
IP Settings

Mobile
Modems
SIMs
Interfaces

Bridges

USB

Serial

Digital I/O

Modem emulator enables replacement for legacy dial-in / dial-out connections based on analog or GSM modems. M!DGE supports the Hayes AT Command set on the serial interface and behaves like a regular router.

You can easily replace your old Modem with M!DGE. There is also no need to configure the attached device as you can prepare the M!DGE accordingly.

Physical protocol	RS232
Baud rate	Specifies the baud rate of the RS232 port.
Hardware flow control	While 3 wired connection is used with M!DGE hardware flow control is not available.
Port	Any incoming connection will be received on the Port configured. This Port needs to be allowed, keep this in mind for Firewall configurations.

The Phonebook configuration will keep the aliases of any Phone numbers so that you do not need to reconfigure your device and can use the original addressing scheme.

Number   Remote phone number.

IP address   Remote IP address.

Port   Remote port number.

(i) **Note**

More details in the *Serial SCADA Protocols*[1] application note.

Protocol Server

The port settings configuration is the same as with the Device Server - *the section called "Device Server"* except the Advanced settings called MTU and Idle size.

MTU

An incoming frame is closed at this size even if the stream of bytes continues. Consequently, a permanent data stream coming to the serial interface results in a sequence of MTU-sized frames sent over the network. The default value is set to 1400 bytes.

Idle size

Received frames on COM are closed when the gap between bytes is longer than the Idle value. This parameter defines the maximum gap (in milliseconds) in the received data stream. If the gap exceeds this value, the link is considered idle, the received frame is closed and forwarded to the network.

The default Idle size differs based on the serial baud rate configuration. Remember that the default Idle sizes are set to the minimal possible values:

bps	ms
115200	120
57600	60
38400	30
19200	20
9600	10
4800	5
2400	5
1200	5
600	5
300	5

---

[1] https://www.racom.eu/eng/products/m/midge/app/ser/index.html

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

| Administration | Port Settings | Protocol Server |

SERIAL1 Port Settings

Physical protocol:	RS232
Baud rate:	115200
Data bits:	8 data bits
Parity:	None
Stop bits:	1 stop bit
Software flow control:	None
Hardware flow control:	None

Advanced Settings

MTU	1400	bytes
Idle size	120	ms

Apply

Each SCADA protocol like Modbus, DNP3, IEC101, DF1 etc. has its unique message format, most importantly its unique way of addressing the remote units. The following text is valid for all M!DGE/RipEX units (further in this *the section called "Protocol Server"* referred to as a "Unit") - the special properties for mobile cellular networks (e.g. limitation of broadcasting) are mentioned here. The basic task for the protocol server is to check whether a received frame is within the protocol format and is not corrupted. Most of the SCADA protocols are using some type of Error Detection Code (Checksum, CRC, LRC, BCC, etc.) for data integrity control, so each Unit calculates this code and checks it against the received one.

Cellular mobile network operates in IP environment, so the basic task for the Protocol server is to convert SCADA serial packets to UDP datagrams. The Address translation settings are used to define the destination IP address and UDP port. Then these UDP datagrams are sent to the M!DGE router, processed there and are forwarded as unicasts through the mobile network to their destination. When the gateway defined in the Routing table belongs to the Ethernet LAN, UDP datagrams are instead forwarded to the Ethernet interface. After reaching the gateway, the datagram is forwarded according to the Routing table.

When the UDP datagram reaches its final IP destination, it should be in a M!DGE or RipEX router again. It is processed further according to its UDP port. It can be delivered to the Protocol server where where the datagram is decapsulated and the data received on the serial interface of the source unit are forwarded to COM. The UDP port can also be that of a Terminal server (RipEX) or any other special protocol daemon on Ethernet like Modbus TCP etc. The datagram is then processed according to the respective settings.

(i) Note

All timeouts in the parameters described below are derived from the time when the packet is sent into the COM driver, i.e. it includes the transfer time of the packet. Take this into account especially when there is a low Baud rate set in the COM settings.

> ⚠️ **Important**
>
> If configuring the Protocol server together with VPN tunnels the "Poll response control" protocol specific parameter must be turned off.

Common parameters

HOME | **INTERFACES** | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

| Administration | Port Settings | Protocol Server | Help |

Protocol Server

| Protocol | Modbus |

| Transport Protocol | UDP |
| Port | 8882 |

Parameters

Mode of Connected device	Master
Broadcast	Off
Poll response control	On

Address translation

| Address translation | Mask |

Base IP	10.203.0.0
Mask	255.255.255.0
Interface (Destination port)	COM(8882)

[Apply]

WAN
Link Management
Supervision
Settings

Ethernet
Port Assignment
VLAN Management
IP Settings

Mobile
SIMs
Interfaces

USB

Serial

Digital I/O

For any SCADA protocol, the Transport protocol and the specific port can be chosen. The default values is UDP port 8882. The unit listens on this port for incoming messages and forwards them to the Protocol server itself.

> ℹ️ **Note**
>
> Only UDP protocol is currently implemented.

The parameters described in this section are typical of most protocols.
There is only a link to them in description of the respective Protocol.

Mode of Connected device
List box: Master, Slave
Default = Master
The typical SCADA application follows the Master–Slave scheme where the structure of the message is different for the Master and Slave SCADA units. Because of that, it is necessary to set which type of SCADA unit is connected to the Unit.

> ⚠️ **Important**
>
> For the SCADA Master, set Master, for the SCADA Slave, set Slave.

- **Master**
  The SCADA Master always sends addressed messages to Slaves. Addressing is different for each SCADA protocol, so this is one of the main reasons why an individual Protocol server in each Unit for each SCADA protocol has to be used.
  - **Broadcast**
    List box: On, Off
    Default = Off
    Some Master SCADA units send broadcast messages to all Slave units. SCADA applications typically use a specific address for such messages. RipEX (Protocol utility) converts such messages into a customized IP broadcast and broadcasts it to all RipEX units resp. to all SCADA units within the network.

    ⓘ Note

      Broadcasts in the cellular network are not possible, thus setting of broadcast functionality is not allowed with M!DGE units.

    If **On**, the address for broadcast packets in the SCADA protocol has to be defined:
    - **Broadcast address format** - List box Hex, Dec - format in which the broadcast address is defined.
    - **Broadcast address** - address in the defined format (Hex, Dec)
  - **Address translation**
    List box: Table, Mask
    Default = Mask
    In a SCADA protocol, each SCADA unit has a unique address, a "Protocol address". In a cellular mobile network, each SCADA unit is represented by an IP address (typically that of the ETH interface) and a UDP port (that of the protocol daemon or the COM port server to which the SCADA device is connected via serial interface).
    A translation between the "Protocol address" and the IP address & UDP port pair has to be done. It can be done either via Table or Mask.
    Hence, a SCADA message received from the serial interface is encapsulated into a UDP/IP datagram, where the destination IP address and the destination UDP port are defined according to the settings of the Address translation.
    - **Mask**

      Translation using the Mask is simpler to set, however it has some limitations:
      − all IP addresses used have to be within the same network, which is defined by this Mask
      −the same UDP port is used for all the SCADA units, which results in the following:
        − SCADA devices on all sites have to be connected to the same interface
        − only one SCADA device can be connected to one COM port
      - **Base IP**
        Default = IP address of the ETH interface
        When creating the IP destination address of UDP datagram, in which the serial SCADA message received from COM is encapsulated, this is created, this Base IP is taken as the basis and only the part defined by the Mask is replaced by the 'Protocol address'.
      - **Mask**
        Default = 255.255.255.0
        A part of the Base IP address defined by this Mask is replaced by the 'Protocol address'. The SCADA protocol address is typically 1 byte, so Mask 255.255.255.0 is most frequently used.
      - **UDP port (Interface)**
        List box: COM, Manual
        This UDP port is used as the destination UDP port in the UDP datagram in which the serial SCADA packet received from COM1 is encapsulated. The default UDP port for COM can be

---

used or the UDP port can be set manually. If the destination IP address belongs to a Unit and the UDP port is not assigned to COM (COM1(2) or to a Terminal server in case of RipEX) or to any special daemon running in the destination address, the packet is discarded.

(i) **Note**

M!DGE use UDP port 8882 for its COM port.

■ **Table**

The Address translation is defined in a table. There are no limitations such as when the Mask translation is used. If there are more SCADA units on the RS485 (e.g. with RipEX COM2) their interface, their "Protocol addresses" should be translated to the same IP address and UDP port pair, where the multiple SCADA units are connected. There are 3 possibilities how to fill in the line in the table:

− One "Protocol address" to one "IP address" (e.g.: 56 −−> 192.168.20.20)
− Range of "Protocol addresses" to one "IP address" (e.g.: 56 – 62 ===> 192.168.20.20)
− Range of "Protocol addresses" to range of "IP addresses" (e.g.: 56 – 62 ===> 192.168.20.20 – 26). One option is to write only the start IP and a dash, the system will add the end address itself.

- **Protocol address**

  This is the address which is used by the SCADA protocol. It may be set either in Hexadecimal or Decimal format according to the List box value.

  Protocol address length can be 1 byte, but for the DNP3 and UNI protocols support 2 bytes addresses.

- **IP**

  The IP address to which Protocol address will be translated. This IP address is used as the destination IP address in the UDP datagram in which serial SCADA packet received from COM is encapsulated.

- **UDP port (Interface)**

  This is the UDP port number which is used as the destination UDP port in the UDP datagram in which the serial SCADA message, received from COM, is encapsulated.

- **Note**

  You may add a note to each address up to 16 characters long for your convenience. (E.g. "Remote unit #1").

- **Active**

  You may tick/un-tick each translation line in order to make it active/not active.

- **Modify**

  Edit, Delete Add buttons allow to edit or to add or to delete a line. The lines can be sorted using up and down arrows.

- **Slave**

The SCADA Slave typically only responds to Master requests, however in some SCADA protocols it can communicate spontaneously.

Messages from the serial interface are processed in a similar way as the Master site, i.e. they are encapsulated in UDP datagrams, processed by the router inside the M!DGE unit and forwarded to the respective interface, typically to the mobile network.

○ **Broadcast accept**

  List box: On, Off

  Default = Off

  If **On**, broadcast messages from the Master SCADA device to all Slave units are accepted and sent to connected Slave SCADA unit.

> **⚠ Important**
>
> Broadcasting is not supported with mobile networks.

PROTOCOLS IMPLEMENTED:

Within several protocols, parameter "Poll response control" can be set. Turn it off if using any kind of port forwarding or VPN tunnels. Otherwise, it can be set to "On". More details about this parameter can be found at *UNI protocol description*.

None

All received frames from the COM port as well as from the network are discarded.

Async link

The async link creates asynchronous link between two COM ports on different Units. Received frames from COM are sent without any processing transparently to the mobile network to set the IP destination and UDP port. Received frames from the mobile network are sent to the respective COM according to the UDP port setting.

- **Parameters**
  - **Destination IP**
    This is the IP address of the destination Unit.
  - **UDP port (Interface)**
    This is the UDP port number which is used as the destination UDP port in the UDP datagram in which the packet received from COM is encapsulated.

C24

C24 is a serial polling-type communication protocol used in Master–Slave applications.

Multiple C24 Masters can be used within one network and one Slave can be polled by more than one Master.

Italicised parameters are described in *Common parameters*.

Mode of Connected device
> *Master*
>> *Address translation*
>>> *Table*
>>> *Mask*
> *Slave*

- **Protocol frames**
  List box: 1C, 2C, 3C, 4C
  Default = 1C
  One of the possible C24 Protocol frames can be selected.

- **Frames format**
  List box: Format1, Format2, Format3, Format4, Format5

Default = Format1
One of the possible C24 Frames formats can be selected. According to the C24 protocol specification, it is possible to set Frames formats 1–4 for Protocol frames 1C–3C and formats 1–5 for 4C.

⚠️ **Important**

The Unit accepts only the set Protocol frames and Frames format combination. All other combinations frames are discarded by the Unit and not passed to the application.

- **Local ACK**
  List box: Off, On
  Default = Off
  Available for Protocol frame 1C only. When **On**, ACK on COM is send locally from this unit, not over the mobile network.

Cactus

Cactus is a serial polling-type communication protocol used in Master–Slave applications.
Multiple Cactus Masters can be used within one network and one Slave can be polled by more than one Master.

Italicised parameters are described in *Common parameters*.

Mode of Connected device

    Master

        Broadcast

        Note: There is no the possibility to set Broadcast address, since Cactus broadcast messages always have the address 0x00. Hence when the Broadcast is On, packets with this destination are handled as broadcasts. Broadcasting is not supported with mobile networks.

        Address translation

            Table

            Mask

    Slave

        Broadcast accept

- **Max gap timeout [ms]**
  Default = 30
  The longest time gap for which a frame can be interrupted and still received successfully as one frame. It should not be set below 10ms, while 15–40 ms should be OK for a typical Cactus protocol device.

Comli

Comli is a serial polling-type communication protocol used by Master–Slave applications.
More Comli Masters can be used within one network and one Slave can be polled by more Masters.
Broadcasts packets are not used, so the configuration is using only some parameters described in *Common parameters*.

Mode of Connected device

> *Master*
>> *Address translation*
>>> *Table*
>>> *Mask*
> *Slave*

DF1

Only the full-duplex mode of DF1 is supported. Each frame in the Allen-Bradley DF1 protocol contains the source and destination addresses in its header, so there is no difference between Master and Slave in the full-duplex mode in terms of Unit configuration.

- **Block control mode**
  List box: BCC, CRC
  Default = BCC
  According to the DF1 specification, either BCC or CRC for Block control mode (data integrity) can be used.
- **Broadcast**
  According to the DF1 specification, packets for the destination address 0xFF are considered broadcasts. Broadcasts are not supported with the mobile network.

Address translation
> *Table*
> *Mask*

- **Advanced parameters**
  - ○ **ACK Locally**
    List box: Off, On
    Default = On
    If "**On**", ACK frames (0x1006) are not transferred over-the-air.
    When the Unit receives a data frame from the connected device, it generates the ACK frame (0x1006) locally. When the Unit receives the data frame from the mobile network, it sends the frame to the connected device and waits for the ACK. If the ACK is not received within 1 sec. timeout, Unit sends ENQ (0x1005). ENQ and ACK are not generated for broadcast packets.

DNP3

Each frame in the DNP3 protocol contains the source and destination addresses in its header, so there is no difference between Master and Slave in terms of the M!DGE configuration. The DNP3 allows both Master–Slave polling as well as spontaneous communication from remote units.

- *Broadcast* **-** Note: There is not the option to set the Broadcast address, since DNP3 broadcast messages always have addresses in the range 0xFFFD – 0xFFFF. Broadcasting is not supported by mobile networks, thus it is not possible to set the broadcast to On..

Address translation
> *Table*
> *Mask*

IEC 870-5-101

IEC 870-5-101 is a serial polling-type communication protocol used by Master–Slave application. More IEC 870-5-101 Masters can be used within one network and one Slave can be polled by more Masters.
IEC 870-5-101 protocol configuration is using all parameters described in *Common parameters*.

Mode of Connected device

    Master

        Broadcast - only On, Off. Protocol broadcast address is not configurable, it is defined by Address mode in Advance parameter (default 0xFF), but broadcasting is not allowed within mobile networks.

        Address translation

            Table

            Mask

    Slave

        Broadcast accept

- **Advanced parameters**
  - ○ **Address mode**
    Even if IEC 870-5-101 is the standard, there are some users who have customized this standard according to their needs. If addressed byte has been moved, M!DGE/RipEX has to read it at the correct frame position.
    - ■ **IEC101**
      Address byte location according to IEC 870-5-101 standard.
      Broadcast from Master station is generated when address byte is 0xFF.
    - ■ **2B ADDR**
      Two byte address (IEC 870-5-101 standard is 1 byte). The frame is 1 byte longer than the standard one. There is the Intel sequence of bytes: low byte, high byte. Mask Address translation has to be used, because Table one is limited to just one byte address length.
      The Master station broadcast is generated when the low address byte is 0xFF and high address byte is also 0xFF.
    - ■ **TELEGYR**
      The Control byte in the standard IEC packet is omitted. The frame is 1 byte shorter than a standard one. This is typically used in the Telegyr 805/809 protocol.
      Broadcast from Master station broadcast is generated when the address byte is 0x00.
    - ■ **SINAUT**
      The sequence of Address byte and Control byte in the frame is swapped-over.
      Master station broadcast is generated when the address byte is 0x00.

ITT Flygt

ITT Flygt is a serial polling-type communication protocol used in Master–Slave applications.

ITT Flygt protocol configuration uses all parameters described in *Common parameters*.

Mode of Connected device

    Master

        Broadcast

Note: There is no possibility to set the Broadcast address, since ITT Flygt broadcast messages always have the address 0xFFFF. Hence when the Broadcast is **On**, packets with this destination are handled as broadcasts. Broadcasting is not available with mobile cellular networks.

- **First Slave Address**
  Default = 1
  Slave addresses are not defined in the ITT Flygt protocol. However Slave addresses have to be defined in the Unit network. This is the First Slave address in decimal format.
- **Number of Slaves**
  Default = 1
  Since the ITT Flygt protocol Master (centre) polls the Slaves (remotes) one by one without any addressing, the number of Slaves has to be defined.

  > *Address translation*
  >> *Table*
  >> *Mask*

  > *Slave*
  >> *Broadcast accept*

- **Wait timeout [ms]**
  Default = 5000
  An ITT Flygt Slave sometimes sends the WAIT COMMAND (0x13) to its Master. The Unit does not accept the next WAIT COMMAND (discards it), till the Wait timeout expires. The Recommended value is in the 1–10 seconds range.

Modbus

Modbus RTU is a serial polling-type communication protocol used by Master–Slave application. More Modbus Masters can be used within one network and one Slave can be polled by more Masters. Modbus protocol configuration uses all parameters described in *Common parameters*.

> *Mode of Connected device*
>> *Master*
>>> *Broadcast*
>>> *Address translation*
>>>> *Table*
>>>> *Mask*
>> *Slave*
>>> *Broadcast accept*

Profibus

RipEX supports Profibus DP (Process Field Bus, Decentralized Periphery) the widest-spread version of Profibus. The Profibus DP is supported even by M!DGE, but it will work satisfactorily only with mobile networks with very short transport delays, like LTE or UMTS. The Profibus protocol configuration uses all parameters described in *Common parameters.*

Mode of Connected device
>   *Master*
>>   *Broadcast*
>>   *Address translation*
>>>   *Table*
>>>   *Mask*
>   *Slave*
>>   *Broadcast accept*

RP570

RP570 is a serial polling-type communication protocol used in Master–Slave applications.

Multiple RP570 Masters can be used within one network and one Slave can be polled by more than one Master.

Italicised parameters are described in *Common parameters*.

Mode of Connected device
>   *Master*

- **Local simulation RB**
  List box: Off, On
  Default = Off
  The RP570 protocol Master very often transmits the RB packets (hold packets) solely to check whether Slaves are connected. In order to minimize the mobile network payload, the Unit can be configured to respond to these packets locally and not to transmit them to the Slaves over the mobile network.

  If **On**, the Unit responds to RB packets received from the RP 570 master locally over the COM interface. However from time to time (RB period) the RB packets are transferred over the network in order to check whether the respective Slave is still on. When the RB response from the Slave to this RB packet is not received over the mobile network within the set RB timeout, i.e. the respective Slave is out of order, the central Unit stops local answering to RB packets from the master for the respective Slave.

- **RB Net period [s]**
  Default = 10
  The M!DGE/RipEX responds to the RB packets locally and in the set RB period the RB packets are transferred over the network.

- **RB Net timeout [s]**
  Default = 10 (maximum=8190)
  Whenever an RB packet is sent over the network, the set RB Net timeout starts. When the RB response from the remote unit (Slave) is not received within the timeout, i.e. the respective Slave is out of order, the central Unit stops the local answering to RB packets from the master for the respective Slave.

>   *Address translation*
>>   *Table*

Mask

Slave

- **Local simulation RB**
  List box: Off, On
  Default = Off
  The RP570 Slave expects to receive RB packets from the Master. When the Local simulation RB on the Master is On, the RB packets are transferred over the mobile network only in the RB Net period (see the Master settings). The Local simulation RB has to be set the same (On or Off) on all sites in the network, i.e. on the master as well as all Slaves.

  If **On**, the Unit generates RB packets locally and transmits them over the COM interface in the RB Request period and expects the RB response for each RB packet from the RP570 Slave within the RB Response timeout. When the Unit does not receive the response(s) from the RP570 Slave, the Unit does not respond to the RB packet from the Master, which it receives over the mobile networks.

- **RB Request period [ms]**
  Default = 200 (maximum=8190)
  M!DGE/RipEX sends locally RB packets to the connected RTU in the set period.

- **RB Response timeout [ms]**
  Default = 500 (maximum=8190)
  The Unit expects a response to the RB packet within the set timeout. If it is not received, the Unit does not respond to RB packets from the Master received over the mobile network.

- **RTU address (Hex)**
  Default = 01
  Active only when the Local simulation RB is On. The connected RTU's address is supposed to be filled in. This address (0x00-0xFF) is used in the RB packets generated locally in the M!DGE/RipEX and transmitted over the COM.

Siemens 3964(R)

The 3964 protocol is utilized by the Siemens Company as a Point-to-Point connection between two controllers. Meanwhile it has become an industry standard that can be found on many devices as a universal communications interface. 3964R is the same as 3964, in addition it only uses BCC (Block Check Character). 3964(R) handle only the link layer (L2 in OSI model), hence Unit uses a similar way to read "SCADA address" as in UNI protocol.

There is a handshake STX(0x02) – DLE(Ox10) at the start of communication and DLE+ETX – DLE at the end. This handshake is performed by M!DGE/RipEX locally, it is not transferred over the network.

Communication goes as follows:
LocalRTU→STX→LocalRipex
LocalRipex→DLE→LocalRTU
LocalRTU→DATA+DLE+ETX+BCC→LocalRipex
LocalRipex→DATA→RemoteRipex*
LocalRipex→DLE→LocalRTU
RemoteRipex→STX→RemoteRTU
RemoteRTU→DLE→RemoteRipex
RemoteRipex→DATA+DLE+ETX+BCC→RemoteRTU
RemoteRTU→DLE→RemoteRipex

* only this packet is transferred over the RipEX network, all the other ones are handled locally.

Italicised parameters are described in *Common parameters*.

Mode of Connected device

    Master

- **Address mode**
  List box: Binary (1 B), Binary (2B LSB first). Binary (2B MSB first).
  Default = Binary (1 B)
  M!DGE/RipEX reads the Protocol address in the format and length set
  (in bytes).
- **Address position**
  Specify the sequence number of the byte, where the Protocol address
  starts.

  Note 1: 3964(R) protocol uses an escape sequence (control sequence)
  for DLE (0x10), i.e. when 0x10 is in user data, 0x1010 is sent instead.
  When the address position is calculated, the bytes added by the escape
  sequence algorithm are not taken into account.

  Note 2: The first byte in the packet has the sequence number 1, not 0.

        Broadcast

        Address translation

            Table

            Mask

    Slave

        Broadcast accept

- **DLE timeout [ms]**
  Default = 1000 (min. 300, max. 8190)

  M!DGE/RipEX expects a response (DLE) from the connected device (RTU) within the set timeout.
  If it is not received, the Unit repeats the frame according to the "Retries" setting.

- **Retries [No]**
  Default = 3 (min. 0, max. 7)

  When DLE timeout is „On", and the DLE packet is not received from the connected device (RTU)
  within the set DLE timeout, the Unit retransmits the frame. The number of possible retries is specified.

- **Priority**
  List box: Low, High
  Default = Low

  When the equipment sends STX and receives STX instead of DLE, there is a collision, both devices
  want to start communication. In such a case, one unit has to have priority. If the Priority is High, the
  Unit waits for DLE. When it is Low, the Unit send DLE.

  Note: Obviously, two devices which are communicating together must be set so that one has High
  priority and the other has Low.

- **BCC**

List box: On, Off
Default = On

BCC (Block Check Character) is a control byte used for data integrity control, it makes the reliability higher. BCC is used by 3964R, 3964 does not use it.

The unit checks (calculates itself) this byte while receiving a packet on COM. Unit transmits DLE (accepts the frame) only when the check result is OK. The BCC byte is not transferred over the network, it is calculated locally in the end Unit and appended to the received data.

UNI

UNI is the "Universal" protocol utility designed by RACOM. It is supposed to be used when the application protocol is not in the Unit list. The key condition is that messages generated by the Master application device always contain the respective Slave address and that address (or its relevant part) position, relative to the beginning of the message (packet, frame), is always the same (Address position).

Generally two communication modes are typical for the UNI protocol: In the first one, communication always has to be initiated by the Master and only one response to a request is supported; in the second mode, Master-Master communication or combination of UNI protocol with ASYNC LINK protocol and spontaneous packet generation on remote sites are possible.

The UNI protocol is fully transparent, i.e. all messages are transported and delivered in full, without any modifications.

Italicised parameters are described in *Common parameters*.

Mode of Connected device

    Master

- **Address mode**
  List box: Binary (1 B), ASCII (2 B), Binary (2B LSB first). Binary (2B MSB first).
  Default = Binary (1 B)
  M!DGE/RipEX reads the Protocol address in the format and length set (in bytes).

  The ASCII 2-byte format is read as 2-character hexadecimal representation of one-byte value. E.g. ASCII characters AB are read as 0xAB hex (10101011 binary, 171 decimal) value.
- **Address position**
  Specify the sequence number of the byte, where the Protocol address starts. Note that the first byte in the packet has the sequence number 1, not 0.
- **Address mask (Hex)**
  When the Address mode is Binary 2 bytes, a 16-bit value is read from the SCADA protocol message according to the Address mode setting (either the MSB or the LSB first), The resulting value is then bit-masked by the Address mask and used as the input value for SCADA to IP address translation (e.g. via a table). The default value of the Address mask is 0xFFFF, hence the full 16-bit value is used by default.

  Example:

The Address mode is set to Binary (2B LSB first), the Address mask is set to 7FF0 and the Address position is set to 2. The SCADA message starts with bytes (in hex) 02 DA 92 C3 .. The 2-byte address is read as 0x92DA (note the LSB came first in the message), Then 0x7FF0 mask is applied and the resulting value 0x12D0 (0x92DA & 0x7FF0) is used as the input for the translation.

- **Poll response control**
  List box: On, Off
  Default = On

  On – The Master accepts only one response per request and it must come from the specific remote to which the request was sent. All other packets are discarded. This applies to the Master–Slave communication scheme.

  Note: It may happen, that a response from a Slave (No.1) is delivered after the respective timeout expired and the Master generates the request for the next Slave (No.2) in the meantime. In such a case the delayed response from No.1 would have been considered as the response from No.2. When Poll response control is On, the delayed response from the Slave No.1 is discarded and the Master stays ready for the response from No.2.

  Off – The Master does not check packets incoming from the mobile network - all packets are passed to the application. That allows e.g. spontaneous packets to be generated at remote sites. This mode is suitable for the Master–Master communication scheme or a combination of the UNI and ASYNC LINK protocols.

  Broadcast

  Address translation

  > *Table*

  > *Mask*

Slave

  Broadcast accept

7.2.7. Digital I/O

The Digital I/O page displays the current status of the I/O ports and can be used to turn output ports on or off.

You can apply the following settings:

Besides on and off you may keep the status after reboot at default which corresponds to the default state as the hardware will be initialized at power-up.

The digital inputs and outputs can also be monitored and controlled by SDK scripts.

7.2.8. GNSS (optional)

Specification:

Receiver	72-channel GPS/QZSS L1 C/A, GLONASS L10F, BeiDou B1I, Galileo E1B/C, SBAS L1 C/A: WAAS, EGNOS, MSAS, GAGAN
Data stream	JSON or NMEA
Tracking sensitivity	up to -162 dBm
Supported antennas	active

The GNSS antenna port have the following specification:
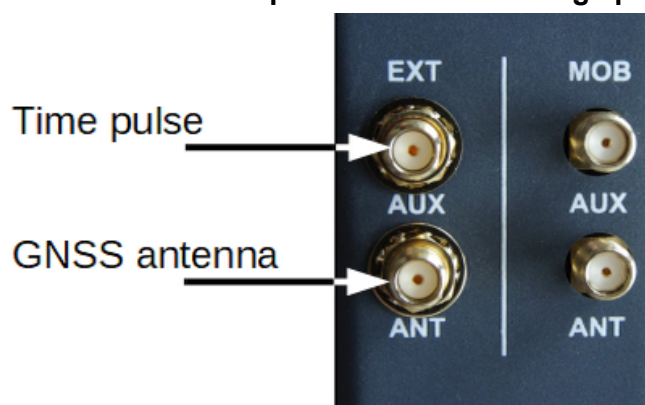
Max. allowed cable length	30m
Max. allowed antenna gain	3.0 dBi
Min. distance between colocated radio transmitter antennas (e.g.: GNSS to LTE)	20cm
Connector type	SMA
Time pulse	TTL logic (L: 0 to 0.8 V, H: 2 to 3.3 V), minimal connected load 100 Ω
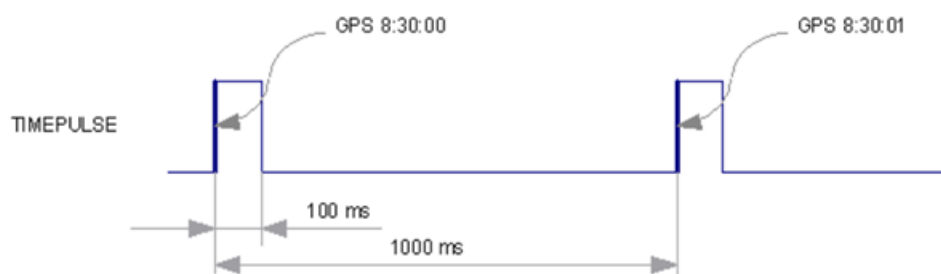
GNSS status

This pages provides further information about the satellites in view and values derived from them:

Status
Summary
WWAN
GNSS
Ethernet
LAN
Bridges
DHCP
System

GNSS Status

Description	Value
Administrative state:	enabled
Operational state:	up
System:	GPSGLONASSBEIDOUSBASQZSS
Time of last fix:	2018-10-24 02:38:43
Latitude:	49.568395
Longitude:	16.077339
Altitude:	616.80
Satellites in view:	21
Speed:	0.002 m/s horizontal
Track angle:	0.000 °
Dilution of precision:	0.92 horizontal 1.23 vertical 1.54 positional
Satellites used:	15

PRN	Elevation	Azimuth	SNR
16	27°	306°	29 dB
20	5°	168°	39 dB
21	61°	194°	28 dB
25	25°	138°	48 dB
26	56°	296°	38 dB
29	51°	71°	31 dB
31	33°	226°	47 dB
65	17°	71°	21 dB
72	15°	25°	19 dB
78	25°	174°	42 dB
79	67°	233°	37 dB
80	36°	321°	29 dB

Latitude	The geographic coordinate specifying the north-south position
Longitude	The geographic coordinate specifying the east-west position
Altitude	The height above sea level of the current location
Satellites in view	The number of satellites in view as stated in GPGSV frames
Speed frames	The horizontal and vertical speed in meter per second as stated in GPRMC
Satellites used frames	The number of satellites used for calculating the position as stated in GPGGA
Dilution of precision	The dilution of precision as stated in GPGSA frames furtheron, each satellite also comes with the following details: GNSS satellite information
PRN frames	The PRN code of the satellite (also referred as satellite ID) as stated in GPGSA
Elevation stated in GPGSV frames	The elevation (up-down angle between the dish pointing direction) in degrees as stated in GPGSV frames

Azimuth frames The azimuth (rotation around the vertical axis) in degrees as stated in GPGSV

SNR The SNR (Signal to Noise Ratio), often referred as signal strength

(i) Note

Please note that the values are shown as calculated by the daemon, their accuracy might be suggestive.

Administration

The GNSS page lets you enable or disable the GNSS modules present in the system and can be used to configure the daemon that can be used to share access to receivers without contention or loss of data and to respond to queries with a format that is substantially easier to parse than the NMEA 0183 emitted directly by the GNSS device.

We are currently running the Berlios GPS daemon (version 3.15), supporting the new JSON format. Please navigate to http://www.catb.org/gpsd/ for getting more information about how to connect any clients to the daemon remotely. The position values can also be queried by the CLI and used in SDK scripts.

GNSS Module Configuration

Administrative status Enable or disable the GNSS module

Operation mode The mode of operation, either standalone or assisted (for AGPS)

Antenna type The type of the connected GPS antenna, active 3 VDCt powered

Accuracy The desired accuracy in meters

Fix frame interval	The amount of time to wait between 1x attempts

GNSS Server Configuration

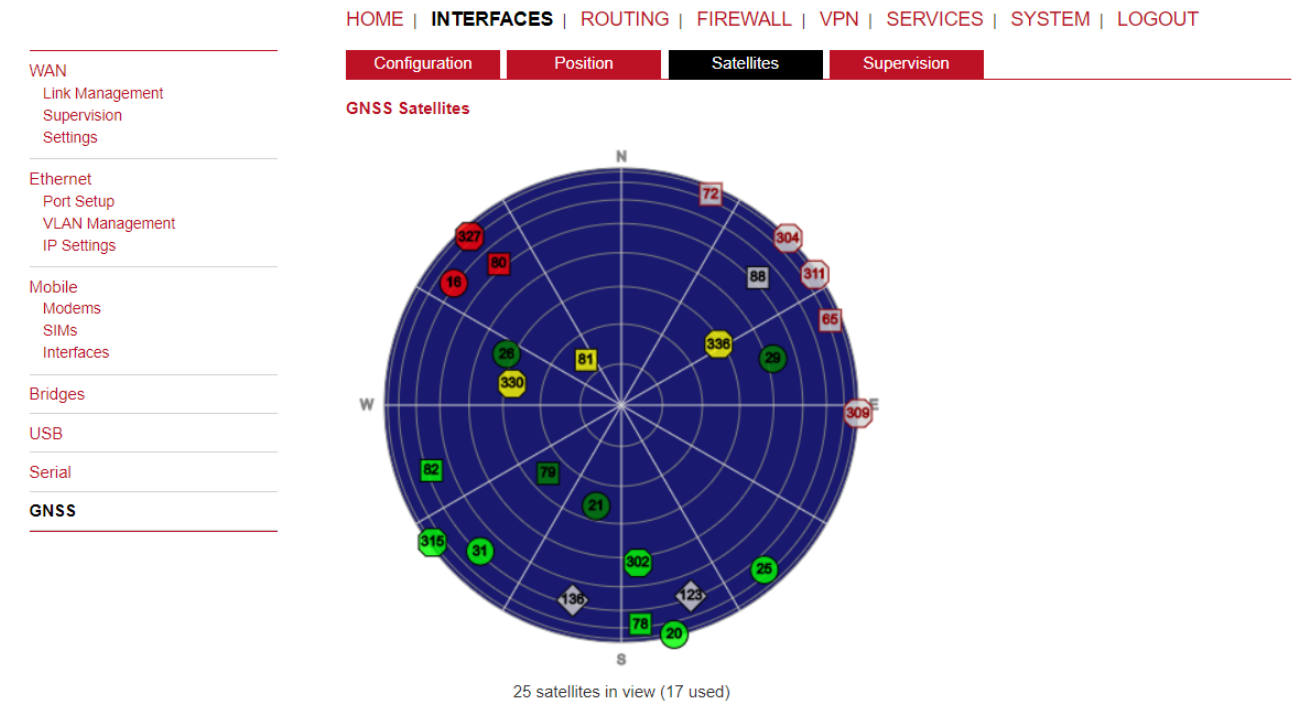|	
Server port	The TCP port on which the daemon is listening for incoming connections
Allow clients from	Specifies where clients can connect from, can be either everywhere or from a specific network
Clients start mode	Specifies how data transferal is accomplished when a client connects. You can specify on request which typically requires an R to be sent. Data will be sent instantly in case of raw mode which will provide NMEA frames or super-raw which includes the original data of the GPS receiver. If the client supports the JSON format (i.e. newer libgps is used) the json mode can be specified.

ⓘ Note

Please consider to restrict access to the server port, either by a specifying a dedicated client network or by using a firewall rule.

Satelites

25 satellites in view (17 used)

Supervision

GNSS supervision

Administrative status   Enable or disable GNSS supervision

Mode   Specifies whether to monitor the NMEA stream or GPS fixes

Max. downtime   The period of time without valid NMEA stream or GPS 1x after which an emergency action shall be taken

Emergency action   The corresponding emergency action. You can either let just restart the server, which will also re-initialize the GPS function on the module, or reset the module in severe cases. Please note that this may have effects on any running WWAN/SMS services.

7.3. ROUTING

7.3.1. Static Routes

This menu shows all routing entries of the system, which can consist of active and configured ones. (Netmasks can be specified in CIDR notation, e.g. **24** expands to `255.255.255.0`).

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Static Routes

Extended Routes

Multipath Routes

Multicast
 IGMP Proxy
 Static Routes

BGP

OSPF

Mobile IP
 Administration

QoS
 Administration
 Classification

Static Routes

This menu shows all routing entries of the system, they can consist of active and configured ones.
The flags are as follows: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route
(Netmasks can be specified in CIDR notation)

Destination	Netmask	Gateway	Interface	Metric	Flags		
0.0.0.0	0.0.0.0	0.0.0.0	WWAN1	0	AD		
10.203.0.29	255.255.255.255	0.0.0.0	WWAN1	0	APH	▬	☑
10.203.0.227	255.255.255.255	0.0.0.0	WWAN1	0	AH		☑
192.168.2.0	255.255.255.0	192.168.1.254	LAN4	0	PN	▬	☑
192.168.10.0	255.255.255.0	0.0.0.0	LAN1	0	AN		
							➕

Route lookup

Destination: Destination network or host provided by IP addresses in dotted decimal.

Netmask: Subnet mask which forms, in combination with the destination, the network to be addressed. A single host can be specified by a netmask of `255.255.255.255,` a default route corresponds to `0.0.0.0.`

Gateway: The next hop which operates as gateway for this network (can be omitted on peer-to-peer links).

Interface: Network interface on which a packet will be transmitted in order to reach the gateway or network behind.

Metric: The routing metric of the interface (default 0). The routing metric is used by routing protocols, higher metrics have the effect of making a route less favourable; metrics are counted as additional costs to the destination network.

Flags: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route

The flags obtain the following meanings:

Active   The route is considered active, it might be inactive if the interface for this route is not yet up

Persistent   The route is persistent, which means it is a configured route, otherwise it corresponds to an interface route

Host   The route is a host route, typically the netmask is set to 255.255.255.255.

Network   The route is a network route, consisting of an address and netmask which forms the subnet to be addressed

Default Route   The route is a default route, address and netmask are set to 0.0.0.0, thus matching any packet

You can check the corresponding routing via the "Route lookup" functionality. Just fill in the desired IP address and click on the "Lookup" button. The detailed information about the chosen route will be displayed.

> **ⓘ** **Note**
>
> The maximum number of manual static routes is 10. This number can be increased to 30 with a SERVER licence.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Mobile IP
  Administration

Route Lookup

Address / Host:	8.8.8.8	Lookup

8.8.8.8 is being routed to **LAN2** via **192.168.131.254** using source address 192.168.131.234

7.3.2. Extended Routes

Extended routes can be used to perform policy-based routing, they generally precede static routes.

Extended routes can be made up not only of a destination address/netmask but also a source address/netmask, incoming interface and the type of service (TOS) of packets.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Multicast

BGP

OSPF

Mobile IP
  Administration

QoS
  Administration
  Classification

Add Extended Route

Incoming interface:	LAN1
Source address:	192.168.1.20
Source netmask:	255.255.255.255
Destination address:	10.203.0.0
Destination netmask:	255.255.0.0
Protocol:	ANY
Type of Service:	any
Route to:	Interface / Gateway
Gateway:	192.168.131.253
Interface:	LAN2 ☑ discard if down

Apply

Incoming interface	The interface on which the packet enters the system
Source address	The packet source address
Source netmask	The packet source netmask
Destination address	The packet destination address
Destination netmask	The packet destination netmask
Protocol	Protocol used (ANY, UDP or TCP)

Type of Service	The ToS value within the packet header (possible values are any, normal-service (0), minimize-cost (2), maximize-reliability (4), maximize-throughput (8), minimize-delay (16))
Route to	Specifies the target interface or gateway to where the packet should get routed to. Check the "discard if down" option for discarding data if the Interface is down (e.g. nothing is connected).

7.3.3. Multipath Routes

Multipath routes perform weighted IP-session distribution for particular subnets across multiple interfaces.

At least two interfaces must be defined to establish the Multipath routing. Additional interfaces can be added by pressing the "plus" sign.

Target network/netmask	The target network for which the Multipath routing will be applied
Interface	The interface for the selected path
Weight	Interface weight in relation to the others (e.g. values 4 and 1 for two paths will result in 80 and 20 % of distribution)
Nexthop	Nexthop address to be used as a default gateway for the selected interface

7.3.4. Multicast

Multicast routing (MCR) can be configured and managed by a daemon. Only one MCR daemon can be used at a time.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Multicast
  IGMP Proxy
  Static Routes

Multicast

Administrative status: ⦿ IGMP proxy
                            ◯ static routes
                            ◯ disabled

[Apply]

M!DGE routers ship with two different MCR daemons to select from, depending on your dependencies:

IGMP proxy   Forwarding of multicast messages that are dynamically detected on a given interface to another interface.

Static routes   List of MCR rules to forward messages of dedicated source and group from a given interface to another.

Disabled   Disable routing of multicast messages.

IGMP proxy

IGMP proxy which is able to maintain multicast groups on a particular interface and distribute incoming multicast packets towards the downstream interfaces on which hosts have joined the groups.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Multicast
  IGMP Proxy
  Static Routes

BGP

OSPF

IGMP Proxy

Incoming interface: [WAN ⌄]

Sender network: [   ]

Sender netmask: [   ]

Distribute to: [all LAN interfaces ⌄]

[Apply]

Administrative status   Specifies whether multicast routing is active.

Incoming interface   The upstream interface on which multicast groups are joined and on which multicast packets come in.

Distribute to   Specifies the downstream interfaces to which multicast packets will be forwarded.

Static Routes

Routes multicast messages in different directions depending on their origin and group based on a given set of MCR rules:

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Multicast
  IGMP Proxy
  Static Routes

BGP

OSPF

Add Static Multicast Route

Group:	
Source:	
Incoming interface:	NONE
Outgoing interface:	NONE

Apply

Group	IP address of MCR group.
Source	Source-IP of the packets.
Incoming interface	Interface to listen on for messages of given group and source.
Outgoing interface	Interface to forward the messages to.

7.3.5. BGP

The BGP tab allows to set up peerings of the M!DGE router with other Border Gateway Protocol enabled routers.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

General   Neighbors   Networks

Static Routes

Extended Routes

Multipath Routes

Multicast

BGP

OSPF

Mobile IP
  Administration

QoS
  Administration
  Classification

BGP General Settings

Administrative status:	⦿ enabled ○ disabled
AS number:	
Redistribute connected routes:	☐
Redistribute local routes:	☐
Redistribute OSPF routes:	☐
Disable when redundancy backup:	☐

Apply

BGP status	Specifies whether the BGP routing protocol is active.
AS number	The number of the autonomous system to which the M!DGE router belongs (available range: 1 - 4294967295).
Redistribute connected routes	Redistribute routes to networks which are directly connected to the M!DGE router.
Redistribute local routes	Redistribute routes from the M!DGE router's own routing table.

Redistribute OSPF routes   Redistribute routes learned via the OSPF routing protocol.

Disable when redundancy backup   Disables the BGP protocol when the router is set to slave mode by the VRRP redundancy protocol.

The neighbors tab is used to configure all the BGP routers to peer with.

HOME	INTERFACES	**ROUTING**	FIREWALL	VPN	SERVICES	SYSTEM	LOGOUT

Static Routes
Extended Routes
Multipath Routes
Multicast
BGP
OSPF
Mobile IP
  Administration

General   Neighbors   Networks

Add BGP Neighbor

IP address:

AS number:

Password:

Multihop: ☐

Apply   Cancel

IP address   IP address of the peer router.

As number   Autonomous system number of the peer router (available range 1 - 4294967295).

Password   Password for authentication with the peer router. If left blank authentication is disabled.

Multihop   Allow multiple hops between this router and the peer router instead of requiring the peer to be directly connected.

The Networks tab allows to add IP network prefixes that shall be distributed via BGP in addition to the networks that are redistributed from other sources as defined on the general tab.

HOME	INTERFACES	**ROUTING**	FIREWALL	VPN	SERVICES	SYSTEM	LOGOUT

Static Routes
Extended Routes
Multipath Routes
Multicast
BGP
OSPF

General   Neighbors   Networks

Add BGP Network

Prefix:

Prefix length:

Apply   Cancel

Prefix   Prefix of the network to be distributed.

Prefix length   Length of the prefix to be distributed.

7.3.6. OSPF

The OSPF tab allows the M!DGE router to be added to a network of OSPF routers.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

| General | Interfaces | Networks |

Static Routes

Extended Routes

Multipath Routes

Multicast

BGP

OSPF

Mobile IP
  Administration

QoS
  Administration
  Classification

OSPF General Settings

Administrative status:	○ enabled
	◉ disabled
Redistribute connected routes:	☑
Redistribute local routes:	☐
Redistribute BGP routes:	☐
Redistribute default route:	☐
Disable when redundancy backup:	☐

Apply

OSPF status	Specifies whether the OSPF routing protocol is active.
Redistribute connected routes	Redistribute routes to networks which are directly connected to the M!DGE router.
Redistribute local routes	Redistribute routes from the M!DGE router's own routing table.
Redistribute BGP routes	Redistribute routes learned via the BGP routing protocol.
Redistribute default route	Redistribute the routers default route.
Disable when redundancy backup	Disables the OSPF protocol when the router is set to slave mode by the VRRP redundancy protocol.

The interfaces tab is used to define OSPF specific settings for the IP interfaces of the router. If no settings are defined for a specific interface, default settings will be used.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

| General | Interfaces | Networks |

Static Routes

Extended Routes

Multipath Routes

Multicast

BGP

OSPF

Mobile IP
  Administration

QoS
  Administration
  Classification

Add OSPF Interface

Interface:	LAN1 ⌄
Authentication:	None ⌄
Key:	
Key ID:	
Cost:	
Passive:	☐

Apply   Cancel

Interface	The name of the interface for which settings shall be defined.

Authentication	The authentication protocol to be used on the interface to authenticate OSPF packets.
Key	The key to be used for authentication.
Key ID	The ID of the key to be used for authentication (1-255).
Cost	The cost for sending packets via this interface. If not specified or set to 0, OSPF defaults are used.
Passive	Do not send out OSPF packets on this interface.

The networks tab defines the IP networks to be handled in OSPF as well as to which routing area they belong.

Prefix	Prefix of the network.
Prefix length	Length of the prefix.
Area	Routing area to which this interface belongs (0-65535, 0 means backbone).

7.3.7. Mobile IP

Mobile IP (MIP) can be used to enable a seamless switch between different WAN technologies.

It boasts with very small outages during switchover while keeping all IP sessions alive which is being accomplished by communicating with the static public IP address of a home agent which will encapsulate the packets and send them further to the router. Switching works by telling the home agent that the hotlink address has changed, the agent will then re-route (that means encapsulate the packets with the new target address) the packets transparently down to the box.

Our implementation supports RFC 3344, 5177, 3024 and 3519 and interoperability with Cisco has been verified. However, M!DGE routers can run as node and home agent which makes them able to replace expensive kits in the backbone for smaller scenarios.

Static Routes

Extended Routes

Multipath Routes

Mobile IP
   Administration

QoS
   Administration
   Classification

Mobile IP

Mobile IP can be used to move from one network to another while maintaining a permanent IP address and thus avoiding that running IP sessions (including VPN tunnels) must be reconnected.

Administrative status:	
	● mobile node
	○ home agent
	○ disabled

Primary home agent address:	10.203.3.28
Secondary home agent address:	(optional)
Home address:	192.168.36.2
SPI:	36
Authentication type:	prefix-suffix-md5 ⌄
Shared secret:	ASCII ⌄ ●●●●●●●●●●●
Life time:	1800
MTU:	1468
UDP encapsulation:	● enabled ○ disabled
Mobile network address:	(optional)
Mobile network mask:	(optional)

Apply

If MIP is run as the Mobile node, the following settings can be configured:

Primary home agent address: The address of the primary home agent

Secondary home agent address: The address of the secondary (fallback) home agent

Home address: The permanent home address of the node which can be used to address the box

SPI: The Security Parameter Index (SPI) identifying the security context between a pair of nodes (represented in 8 chars hex)

Authentication type: The used authentication, can be prefix-suffix-md5 or hmac-md5

Shared secret: The shared secret used for authentication, can be a 128-bit hex or ASCII string

Life time: The lifetime of security associations in seconds

MTU: Maximum transmission unit in bytes

UDP encapsulation: Specifies whether UDP encapsulation shall be used

Mobile network address: Optionally specifies a subnet which should be routed to the box

Mobile network mask: The netmask for the optional routed network

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Mobile IP
Administration

QoS
Administration
Classification

Mobile IP

Mobile IP can be used to move from one network to another while maintaining a permanent IP address and thus avoiding that running IP sessions (including VPN tunnels) must be reconnected.

Administrative status:
○ mobile node
● home agent
○ disabled

Home network address: 192.168.36.1

Home network mask: 255.255.255.0

Apply

If MIP is run as home agent, you will have to set up a home address and netmask first and configure various nodes afterwards which are made up of the following settings:

SPI   The home address of the network

Authentication type   The mask for the home network.

Shared secret   The shared secret used for the mobile node authentication at the home agent. This can be either a 128-bit hexadecimal value or a random length ASCII string.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Mobile IP
Administration
Mobile Nodes

SPI: 36

Authentication type: prefix-suffix-md5

Shared secret: HEX ••••••••••

Add   Cancel

7.3.8. Quality of Service (QoS)

M!DGE routers are able to prioritize and shape certain kinds of IP traffic. This is currently limited on egress, which means that only outgoing traffic can be stipulated. The current QoS solution is using Stochastic Fairness Queueing (SFQ) classes in combination with Hierarchy Token Bucket (HTB) qdiscs. Its principle of operation can be summarized as ceiling the max. throughput per link and shaping traffic by reflecting the specified queue priorities. In general, the lowest priority number of a queue gets most out of the available bandwidth.

In case of demands for other class or qdisc algorithms please contact our support team in order to evaluate the best approach for your application.

QoS Administration

The administration page can be used to enable and disable QoS.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Multicast

BGP

OSPF

Mobile IP
  Administration

QoS
  Administration
  Classification

Quality Of Service

QoS can be used to prioritize or reserve a specific bandwidth for your IP services. You can configure multiple queues on the interfaces and assign services to them by means of IP packet selectors.

Administrative Status   ◉ enabled
         ○ disabled

Apply

QoS Classification

The classification section can be used to define the WAN interfaces on which QoS should be active.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Multicast

BGP

OSPF

Mobile IP
  Administration

QoS
  Administration
  Classification

Add QoS Interface

Interface: WWAN1 ∨

Bandwidth congestion: fixed ∨

Upstream bandwidth: 4.0   Mbit/s

Apply   Cancel

Interface:	The WAN interface on which QoS should be active.
Bandwidth congestion:	The bandwidth congestion method. In case of the auto option, the system will try to apply limits in a best-effort way. However, it is suggested to set fixed bandwidth limits as they also offer a way of tuning the QoS behaviour.

Upstream bandwidth:	The available bandwidth for outgoing traffic.
IP to ping (primary)	An IP, which answers ICMP echo requests to determine the bandwidth of the link.
IP to ping (secondary)	An IP, which answers ICMP echo requests to determine the bandwidth of the link.

When defining limits, you should consider bandwidth limits which are at least possible as most shaping and queues algorithms will not work correctly if the specified limits cannot be achieved. In particular, any WWAN interfaces operating in a mobile environment are suffering variable bandwidths, thus rather lower values should be used.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Multicast

BGP

OSPF

Mobile IP
   Administration

QoS
   Administration
   Classification

QoS Classification

Interface	Bandwidth	Queues				
WWAN1	fixed	**Outbound:**				⊟ ☑
	4.00 Mbit/s up	high	prio 1	0.00 Mbit/s		
		default	prio 2	0.00 Mbit/s		
		low	prio 3	0.00 Mbit/s		

Apply

In case an interface has been activated, the system will automatically create the following queues:

high:	A high priority queue which may hold any latency-critical services (such as VoIP).
default:	A default queue which will handle all other services.
low:	A low priority queue which may hold less-critical services for which shaping is intended.

HOME | INTERFACES | **ROUTING** | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Static Routes

Extended Routes

Multipath Routes

Multicast

BGP

OSPF

Mobile IP
   Administration

QoS
   Administration
   Classification

Edit Outbound QoS Queue on WWAN1

Name:	high
Set TOS:	Don't set ∨
Priority:	1 ∨
Upstream bandwidth:	0.00 Mbit/s

Assigned Services

Source	Destination	Type of Service
		➕

Apply   Cancel

Each queue can be configured as follows:

Name:	The name of the QoS queue.
Priority:	A numerical priority for the queue, lower values indicate higher priorities.

Bandwidth: The maximum possible bandwidth for this queue in case the total bandwidth of all queues exceeds the set upstream bandwidth of "QoS Interface Parameters".

Set TOS   The TOS/DiffServ value to set on matching packets.

You can now configure and assign any services to each queue. The following parameters apply:

Interface: The QoS interface of the queue

Queue: The QoS queue to which this service shall be assigned

Source: Specifies a network address and netmask used to match the source address of packets

Destination: Specifies a network address and netmask used to match the destination (target) address of packets

Protocol: Specifies the protocol for packets to be matched

Type of Service: Specifies the ToS/DiffServ for packets to be matched

7.4. FIREWALL

This router uses Linux's netfilter/iptables firewall framework (see *http://www.netfilter.org* for more information). It is set up of a range of rules which control each packet's permission to pass the router. Packets, not matching any of the rules, are allowed by default.

7.4.1. Firewall

Administration

The administration page can be used to enable and disable firewalling. When turning it on, a shortcut can be used to generate a predefined set of rules which allow administration (over HTTP, HTTPS, SSH or TELNET) by default but block any other packets coming from the WAN interface. Please note that the specified rules are processed by order, that means, traversing the list from top to bottom until a matching rule is found. If there is no matching rule found, the packet is allowed.

HOME | INTERFACES | ROUTING | **FIREWALL** | VPN | SERVICES | SYSTEM | LOGOUT

Firewall
Administration
Address / Port Groups
Filtering Rules

NAPT
Administration
Inbound Rules
Outbound Rules

Firewall Administration

Administrative status:
○ enabled
○ disabled

Allow WAN administration: ☑

Apply

Administrative status: Enable or disable packet filtering.

Allow WAN administration: This option will predefine the rules for services on the WAN link as follows (TCP ports 80, 443, 22 and 23):

HOME | INTERFACES | ROUTING | **FIREWALL** | VPN | SERVICES | SYSTEM | LOGOUT

Firewall
Administration
Address / Port Groups
Filtering Rules

NAPT
Administration
Inbound Rules
Outbound Rules

Firewall Filtering Rules

This menu can be used to filter the packets passing the device and targeting its services.
Packets which are not matching any of the rules below will be ALLOWED.

	Description	Mode	Source	Destination	Port(s)	
⬇	ALLOW-WAN-ADMIN	ALLOW	ANY on WAN	ANY	TCP ADMIN-PORTS	⊖ ✎
⬆	DENY-WAN-ALL	DENY	ANY on WAN	ANY	ANY	⊖ ✎
						⊕

Apply   Clear

Address / Port Groups

This menu can be used to form address or port groups which can be later used for firewall rules in order to reduce the number of rules.

HOME | INTERFACES | ROUTING | **FIREWALL** | VPN | SERVICES | SYSTEM | LOGOUT

Address Groups	Port Groups

Firewall
Administration
Address / Port Groups
Filtering Rules

NAPT
Administration
Inbound Rules
Outbound Rules

Firewall Port Groups

Description	Ports	
ADMIN-PORTS	80, 443, 22, 23	

Add Firewall Rule

HOME | INTERFACES | ROUTING | **FIREWALL** | VPN | SERVICES | SYSTEM | LOGOUT

Firewall
Administration
Address / Port Groups
Filtering Rules

NAPT
Masquerading
Inbound Rules
Outbound Rules

Edit Firewall Rule

Description:	ALLOW-WAN-ADMIN
Action:	ALLOW ☐ log matches
Incoming interface:	WAN
Outgoing interface:	ANY
Source:	◉ ANY ○ MAC ○ LOCAL ○ specify
Destination:	◉ ANY ○ LOCAL ○ specify
Protocol:	TCP
Destination port(s):	○ single port ○ multiple ports ◉ group
	ADMIN-PORTS 80, 443, 22, 23

Continue   Cancel

Description:	A meaningful description about the purpose of this rule.
Action:	Whether the packets of this rule should be allowed or denied.
Log matches	Throw a syslog message if rule matches.
Incoming interface:	The Interface on which matching packets are received.
Outgoing interface:	The interface on which matching packets are received.
Source:	Source address of matching packets. Possible values are "ANY", "LOCAL" (addressed to the system itself), "Group" or "Specify" (specified by an address/netmask).
Destination:	The destination address of matching packets, can be "ANY", "LOCAL" (addressed ... itself), "Group" or "Specify (specified by address/netmask).
Protocol:	Used IP protocol of matching packets.
Destination port(s):	Destination port of matching packets. You can specify a single port or a range of ports here. Note that protocol must be set to UDP/TCP when using port filters.

Transparent Firewall

M!DGE can be configured with its Ethernet interfaces being bridged. In this case, the transparent firewall functionality can be configured to limit reachability of individual hosts connected to M!DGE based on their MAC addresses, i.e. units connected to ETH1 cannot communicate to units connected to ETH2.

7.4.2. NAPT

This page allows setting of the options for Network Address and Port Translation (NAPT). NAPT translates IP addresses or TCP/UDP ports and enables communication between hosts on a private network and hosts on a public network. It generally allows a single public IP address to be used by many hosts from the private LAN network.

Administration

The administration page lets you specify the interfaces on which masquerading will be performed. NAT will hereby use the address of the selected interface and choose a random source port for outgoing connections and thus enables communication between hosts from a private local area network towards hosts on the public network.

Interface   The outgoing interface on which connections will be masqueraded.

Source address   The source address or network from which matching packets are masqueraded.

HOME | INTERFACES | ROUTING | **FIREWALL** | VPN | SERVICES | SYSTEM | LOGOUT

Firewall
  Administration
  Address / Port Groups
  Filtering Rules

NAPT
  Masquerading
  Inbound Rules
  Outbound Rules

Add Masquerading Rule

Interface:	WAN ∨

Source:	○ ANY ● specify
	Address: `10.10.10.0`
	Netmask: `255.255.255.0`

[Apply]

Inbound Rules

Inbound rules can be used to modify the target section of IP packets and, for instance, forward a service or port to an internal host. By doing so, you can expose that service and make it available from the Internet. You may also establish 1:1 NAT mapping for a single host using additional outbound rules.

> **(i) Note**
>
> The rules are processed by order, that means, traversing the list from top to bottom until a matching rule is found. If there is no matching rule found, the packet will pass as is.

HOME | INTERFACES | ROUTING | **FIREWALL** | VPN | SERVICES | SYSTEM | LOGOUT

Firewall
  Administration
  Address / Port Groups
  Filtering Rules

NAPT
  Masquerading
  Inbound Rules
  Outbound Rules

Add NAPT Rule For Inbound Packets

Description:	`VPN`
Map:	● host ○ network

Packet Selection

Incoming interface:	WAN ∨
Source:	● ANY ○ specify
Target address:	● ANY ○ specify
Target protocol / port(s):	UDP ∨ `1194` to ☐

Redirect to

Address:	`192.168.10.1`
Port:	● same port ○ specify

[Add] [Cancel]

Description:	A meaningful rule description
Incoming interface:	Interface from which matching packets are received
Source	The source address or network from which matching packets are received.
Map:	Choosing whether the rule applies to the host or to the network.

Target address:	Destination address of matching packets (optional)
Target port(s):	Used UDP/TCP port range of matching packets
Redirect to:	Address to which matching packets will be redirected
Redirect port:	Port to which matching packets will be targeted

Outbound Rules

Outbound rules will modify the source section of IP packets and can be used to establish 1:1 NAT mappings but also to redirect packets to a specific service.

HOME | INTERFACES | ROUTING | **FIREWALL** | VPN | SERVICES | SYSTEM | LOGOUT

Firewall
   Administration
   Address / Port Groups
   Filtering Rules

NAPT
   Masquerading
   Inbound Rules
   Outbound Rules

Add NAPT Rule For Outbound Packets

Description: [   ]

Map: ○ host ⊙ network

Packet Selection

Outgoing interface: [WAN ▾]

Target: ⊙ ANY ○ specify

Source network: [   ]

Source netmask: [   ]

Rewrite to

Network: [   ]

Netmask: [   ]

[Add] [Cancel]

Description:	A meaningful description of this rule
Map:	Choosing whether the rule applies to the host or to the network.
Outgoing interface:	Outgoing interface on which matching packets are leaving the router
Target	The target address or network to which matching packets are destined.
Source address/ports:	Source address/ports of matching packets (if Map is set to "host")
Source network/netmask:	Source network/netmask of matching packets (if Map is set to "network")
Rewrite to address/port:	Address/port to which the source address/port of matching packets will be rewritten to
Rewrite to network/netmask:	Network/netmask to which the source network/netmask of matching packets will be rewritten to

7.5. VPN

7.5.1. OpenVPN

Administration

OpenVPN administrative status   Enable or disable OpenVPN.

Restart on link change   If checked, the tunnel is restarted whenever any link changes the status.

Multipath TCP   Enables OpenVPN multipath TCP support.

If enabled, OpenVPN client configurations will be started whenever a WAN link has been established. Server configuration will be started immediately after the bootup.

Tunnel Configuration

The router supports a single server tunnel and up to 4 client tunnels. You can specify tunnel parameters in standard configuration or upload an expert mode file which has been created in advance. Refer to section *the section called "Client Management"* to learn more about how to manage clients and generate the files.

Operation mode   Choose the client or server mode for this tunnel

> **(i) Note**
>
> M!DGE can be running up to 4 OpenVPN tunnels in the Client mode, but only one tunnel in the Server mode.

Client Mode

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

GRE
Administration
Tunnel Configuration

Dial-in Server

| Tunnel 1 | Tunnel 2 | Tunnel 3 | Tunnel 4 |

OpenVPN Tunnel 1 Configuration

Operation mode:
- ○ disabled
- ● client   ● standard
- ○ server   ○ expert

Peer selection: single ∨
Server: [   ] Port: 1194

Interface type: TUN ∨

Protocol: UDP ∨

Network mode: ● routed   MTU: [   ]
○ bridged

Authentication: certificate-based ∨
HMAC digest: SHA1 ∨

Encryption: BF-CBC ∨

Options: ☑ use compression   ☐ redirect gateway
☐ use keepalive   ☐ negotiate DNS

[Apply]

Peer selection	Specifies how the remote peer shall be selected, besides a single server you may configure multiple servers which can , in case of failures, either be selected sequentially (i.e. failover) or randomly (i.e. load balancing).
	Server The remote server address or hostname
	Port The remote server port (1194 by default)
Interface type	The VPN device type which can be either TUN (typically used for routed connections) or TAP (used for bridged networks)
Protocol	The OpenVPN tunnel protocol to be used.
Network mode	Defines how the packets should be forwarded, can be routed or bridged from or to a particular interface. You can also set the MTU for the tunnel.
Authentication	You can choose between credential-based (where you have to specify a username and password) and certificate-based options. Note that keys/certificates have to be created in the SYSTEM -> Keys & Certificates menu. You may also upload files which you have generated on your host system.
HMAC digest	HMAC is commonly used message authentication algorithm (MAC) that uses a data string, a secure algorithm, and a key, to produce a digital signature. OpenVPN's HMAC usage is to first encrypt a packet, then HMAC the resulting cipher text. If OpenVPN receives a packet with a bad HMAC, it drops this packet. HMAC usually adds 16 or 20 Bytes per packet.

Encryption	Required cipher mechanism used for encryption.
Use compression	Enable or disable OpenVPN compression.
Use keepalive	Can be used to send a periodic keep alive packet in order to keep the tunnel up despite inactivity.
Redirect gateway	By redirecting the gateway, all packets will be directed to the VPN tunnel. Please ensure that essential services (such as DNS or NTP servers) can be reached via the network behind the tunnel. If in doubt, create an extra static route pointing to the correct interface.
Negotiate DNS	If enabled, the system will use the nameservers which have been negotiated over the tunnel.
Allow duplicates	Allow multiple clients with the same common name to concurrently connect.
Verify certs	Check peer certificate against local CRL.

Server Mode

A server tunnel typically requires the following files:

- server.conf (OpenVPN configuration file),

- ca.crt (root certificate file),

- server.crt (certificate file),

- server.key (private key file),

- dh1024.pem (Diffie Hellman parameters file),

- a directory (with default name "ccd") containing client-specific configuration files.

⚠ **Important**

OpenVPN tunnels require a correct system time. Please ensure that all NTP servers are reachable. When using host names, a working DNS server is required as well.

Client Management

Once you have successfully set up an OpenVPN server tunnel, you can manage and enable clients connecting to your service. Currently connected clients can be seen on this page, including the connect time and IP address. You may kick connected clients by disabling them.

In the Networking section you can specify a fixed tunnel endpoint address for each client. Please note that, if you intend to use a fixed address for a particular client, you would have to apply fixed addresses to the other ones as well.

You may specify the network behind the clients as well as the routes to be pushed to each client. This can be useful for routing purposes, e.g. in case you want to redirect traffic for particular networks towards the server. Routing between the clients is generally not allowed but you can enable it if desired.

Finally, you can generate and download all expert mode files for enabled clients which can be used to easily populate each client.

Operating in server mode with certificates, it is possible to block a specific client by revoking a possibly stolen client certificate (see *Keys & Certificates*).

ⓘ **Note**

The downloaded expert mode file needs to be unzipped and then individual client expert files can be uploaded to the respective routers.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration

Clients   Networking

Client Management

Client	Address	Networks		
Client1	dynamic		✎	⊖
Client2	dynamic	192.168.100.0/24	✎	⊖
				⊕

Download

ⓘ **Note**

See the *OpenVPN configuration*[2] example in our Application notes.

---

[2] https://www.racom.eu/eng/products/m/midge/app/vpn/OpenVPN.html

7.5.2. IPsec

IPsec is a protocol suite for securing IP communications by authenticating and encrypting each packet of a communication session and thus establishing a secure virtual private network.

IPsec includes various cryptographic protocols and ciphers for key exchange and data encryption and can be seen as one of the strongest VPN technologies in terms of security.

It uses the following mechanisms:

AH   Authentication Headers (AH) provide connectionless integrity and data origin authentication for IP datagrams and ensure protection against replay attacks.

ESP   Encapsulating Security Payloads (ESP) provide confidentiality, data-origin authentication, connectionless integrity, an anti-replay service and limited traffic-flow confidentiality.

SA   Security Associations (SA) provide a secure channel and a bundle of algorithms that provide the parameters necessary to operate the AH and/or ESP operations. The Internet Security Association Key Management Protocol (ISAKMP) provides a framework for authenticated key exchange.

Negotiating keys for encryption and authentication is generally done by the Internet Key Exchange protocol (IKE) which consists of two phases:

IKE phase 1   IKE authenticates the peer during this phase for setting up an ISAKMP secure association. This can be carried out by either using main or aggressive mode. The main mode approach utilizes the Diffie-Hellman key exchange and authentication is always encrypted with the negotiated key. The aggressive mode just uses hashes of the pre-shared key and therefore represents a less secure mechanism which should generally be avoided as it is prone to dictionary attacks.

IKE phase 2   IKE finally negotiates IPSec SA parameters and keys and sets up matching IPSec SAs in the peers which is required for AH/ESP later on.

Administration

IPsec administrative status   Enable or disable IPsec

Propose NAT Traversal   NAT-Traversal is mainly used for connections which traverse a path where a router modifies the IP address/port of packets. It encapsulates packets in UDP and therefore requires a slight overhead which has to be taken into account when running over smallsized MTU interfaces.

| Restart on link change | If checked, the tunnel is restarted whenever any link changes the status. |

ⓘ **Note**

Running NAT-Traversal makes IKE using UDP port 4500 rather than 500 which has to be taken into account when setting up firewall rules.

Configuration

General

Remote peer address	The IPsec peer/responder/server IP address or host name
Administrative status	Enable or disable Dead Peer Detection. DPD will detect any broken IPSec connection, in particular the ISAKMP tunnel, and refresh the corresponding SAs (Security Associations) and SPIs (Security Payload Identifiers) for a faster tunnel re-establishment.
Detection cycle	Set the delay (in seconds) between Dead Peer Detection (RFC 3706) keepalives (R_U_THERE, R_U_THERE_ACK) that are sent for this connection (default 30 seconds)
Failure threshold	The number of unanswered DPD R_U_THERE requests until the IPsec peer is considered dead (the router will then try to re-establish a dead connection automatically)
Action	The action when a DPD enabled peer is declared dead. Hold (default) means the eroute is put into the hold status, while clear means the eroute and SA will both be cleared. Restart means that the SA will be immediately renegotiated.

IKE Proposal

OpenVPN
  Administration
  Tunnel Configuration
  Client Management

IPsec
  Administration
  Tunnel Configuration

PPTP
  Administration
  Tunnel Configuration

GRE
  Administration
  Tunnel Configuration

Dial-in Server

IPsec Tunnel 1 Configuration

| General | IKE Proposal | IPsec | Networks |

IKE Authentication

| Key exchange: | IKEv1 |
| Authentication type: | pre-shared key |

| PSK: | •••••••• |

Local ID type:	IP Address
Local ID:	10.203.0.29
Peer ID type:	IP Address
Peer ID:	10.203.0.28

IKE Proposal (Phase 1)

Negotiation mode:	main
Encryption algorithm:	3des
Authentication algorithm:	md5
Diffie-Hellman group:	Group 2 (modp1024)
Pseudo-random function:	md5
SA life time:	86400	seconds

Apply   Continue

RACOM routers support IKEv1 or IKEv2 authentication via the pre-shared keys (PSK) or certificates within a public key infrastructure.

Using PSK requires the following settings:

PSK   The pre-shared key used

Local ID Type   The identification type for the local router which can be FQDN, username@FQDN or IP address

Local ID   The local ID value

Peer ID type   The identification type for the remote router

Peer ID   The peer ID value

ⓘ **Note**

When using certificates you would need to specify the Operation mode. When run as the PKI client you can create a Certificate Signing Request (CSR) in the certificates section which needs to be submitted at your Certificate Authority and imported to the router afterwards. In

the PKI server mode the router represents the Certificate Authority and issues the certificates for remote peers.

Negotiation mode	Choose the negotiation mode (main, aggressive). The aggressive mode has to be used when dealing with dynamic endpoint addresses, but it is referred to be less secure compared to the main mode as it reveals your identity to an eavesdropper.
Encryption algorithm	The IKE encryption method (3DES, AES128, AES192, AES256)
Authentication algorithm	The IKE authentication method (MD5, SHA1, SHA2-256)
IKE Diffie-Hellman group	The IKE Diffie-Hellman group (2, 5 and 16-21)
SA life time	The Security Association lifetime
Perfect forward secrecy (PFS)	This feature heavily increases security as PFS avoids penetration of the key-exchange protocol and prevents compromising the keys negotiated earlier.

Using Public Key Infrastructure requires similar settings, but the Operation mode must be configured.

Operation mode

Mode can be set either to "server" or "client". As a "server" and once you have successfully set up an IPsec tunnel, you can manage and enable clients connecting to your service. It is possible to generate and download expert mode files for enabled clients which can be used to easily populate each client.

IPsec Proposal

Encapsulation mode	Only the tunnel encapsulation mode is enabled
IPsec protocol	Only the ESP IPsec protocol is enabled
Encryption algorithm	The IKE encryption method (3DES, AES128, AES192, AES256, blowfish128, 192 and 256)

Authentication algorithm	The IKE authentication method (MD5, SHA1, SHA256, SHA384, SHA512)
SA life time	The Security Association lifetime in seconds
Perfect forward secrecy (PFS)	Specifies whether Perfect Forward Secrecy (PFS) should be used. This feature increases security as PFS avoids penetration of the key-exchange protocol and prevents compromization of previous keys.
Force encapsulation	Force UDP encapsulation for ESP packets even if no NAT situation is detected.

Networks

When creating Security Associations, IPsec keeps track of routed networks within the tunnel. Packets are only transmitted when a valid SA with the matching source and destination network is present. Therefore, you may need to specify the networks behind the endpoints by applying the following settings:

Local network address	The address of your Local Area Network (LAN)
Local network mask	The netmask of your LAN
Peer network address	The address of the remote network behind the peer
Peer network mask	The netmask of the remote network behind the peer
NAT address	Optionally, you can apply NAT (masquerading) for packets coming from a different local network. The NAT address must reside in the network previously specified as the local network.

(i) Note

Since the firmware 3.7.40.103, the maximum number of networks for individual IPsec tunnels has increased from 4 to 10.

Excl. Networks

OpenVPN
   Administration
   Tunnel Configuration
   Client Management

IPsec
   Administration
   Tunnel Configuration

IPsec Tunnel1 Configuration

| General | IKE Proposal | IPsec | Networks | Excl. Networks |

Excluded Networks

	Network	Netmask	
➕			☑ ➖

If IPSec is used as default gateway (Remote Network 0.0.0.0/0), this option can be used to exclude some subnet/network. I.e. IPsec is not used for this particular subnet/network.

(i) **Note**

See the *IPsec configuration example*[3] in our Application notes.

7.5.3. PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks between two hosts. PPTP is easy to configure and widely deployed amongst Microsoft Dial-up networking servers. However, due to its weak encryption algorithms, it is nowadays considered insecure but it still provides a straightforward way for establishing tunnels. When setting up a PPTP tunnel, you would need to choose between server or client.

OpenVPN
   Administration
   Tunnel Configuration

IPsec
   Administration
   Tunnel Configuration

PPTP
   Administration
   Tunnel Configuration

GRE
   Administration
   Tunnel Configuration

Dial-in Server

| Tunnel 1 | Tunnel 2 | Tunnel 3 | Tunnel 4 |

PPTP Tunnel 1 Configuration

Operation mode:
   ◯ disabled
   ◯ client
   ⦿ server

Server listen address:
   ⦿ ANY
   ◯ specify

Server address:

Client address range: ___ to ___

Username:

Password:

Apply

Listen address	Specifies on which IP address should be listened for incoming client connections
Server address	The server address within the tunnel
Client address range	Specifies a range of IP addresses assigned to each client

---

[3] https://www.racom.eu/eng/products/m/midge/app/vpn/IPsec.html

Username/password   The common username/password configuration

Once configured, individual clients can be configured with different credentials and IP addresses.

A client tunnel requires the following parameters to be set:

Server address   The address of the remote server

Username   The username used for authentication

Password   The password used for authentication

7.5.4. GRE

The Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over IP. GRE is defined in RFC 1701, 1702 and 2784. It does not provide encryption nor authorization but can be used on an address-basis on top of other VPN techniques (such as IPsec) for tunneling purposes.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

OpenVPN
   Administration
   Tunnel Configuration

IPsec
   Administration
   Tunnel Configuration

PPTP
   Administration
   Tunnel Configuration

GRE
   Administration
   Tunnel Configuration

| Tunnel 1 | Tunnel 2 | Tunnel 3 | Tunnel 4 |

GRE Tunnel 1 Configuration

Operation mode:	● enabled ○ disabled
Peer address:	
Interface type:	TUN ▾
Local tunnel address:	
Local tunnel netmask:	
Remote network:	
Remote netmask:	

Apply

The following parameters are required for setting up a tunnel:

Peer address	The remote peer IP address
Interface type	The device type for this tunnel. If "tap" device is chosen, another parameter "Bridge interface" must be configured with one LAN port.
Local tunnel address	The local IP address of the tunnel
Local tunnel netmask	The local subnet mask of the tunnel
Remote network	The remote network address of the tunnel
Remote netmask	The remote subnet mask of the tunnel

In general, the local tunnel address/netmask should not conflict with any other interface addresses. The remote network/netmask will result in an additional route entry in order to control which packets should be encapsulated and transferred over the tunnel.

7.5.5. L2TP

The Layer 2 Tunnelling Protocol is a tunnelling protocol which does not support any encryption or confidentiality. It relies on an encryption protocol that it passes within the tunnel to provide privacy. L2TPv3 is supported. Tunnel can be bridged to the local interfaces.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

OpenVPN
  Administration
  Tunnel Configuration
  Client Management

IPsec
  Administration
  Tunnel Configuration

PPTP
  Administration
  Tunnel Configuration

GRE
  Administration
  Tunnel Configuration

L2TP
  Administration
  Tunnel Configuration

| Tunnel 1 | Tunnel 2 | Tunnel 3 | Tunnel 4 |

L2TP Tunnel 1 Configuration

Operation mode:	◉ enabled
	○ disabled
Transport protocol:	◉ IP
	○ UDP
Local IP:	
Remote IP:	
Local Tunnel ID:	
Remote Tunnel ID:	
Local Session ID:	
Remote Session ID:	
Local Cookie:	
Remote Cookie:	
MTU:	1488
Bridge interface:	LAN1 ▾

Apply

The following parameters are required for setting up a tunnel:

Transport protocol	The transport protocol which shall be used
Local IP	The local IP address of the tunnel
Remote IP	The remote IP address of the tunnel
Local port	The local port address of the tunnel
Remote port	The remote port address of the tunnel
Local tunnel ID	The local tunnel ID identifies the tunnel into which the session will be created
Remote tunnel ID	The remote tunnel ID identifies the tunnel assigned by the peer
Local session ID	The local session ID identifies the session being created
Remote session ID	The remote session ID identifies the session assigned by the peer
Local cookie	The local cookie sets an optional cookie value to be assigned to the session
Remote cookie	The remote cookie set an optional per cookie value to be assigned to the session
MTU	The Maximum Transmission Unit of the tunnel interface

Bridge interface   The interface to which the guest interface shall be bridged

7.5.6. Dial-in Server

The Dial-in Server is not supported by M!DGE hardware. Use the "Modem bridge" mode in the *Interfaces - Serial menu*.

Besides the admin account you can configure further users in the user accounts section, which shall be allowed to dial-in. Please note that Dial-In connections are generally discouraged. As they are implemented as GSM voice calls, they suffer from unreliability and poor bandwidth.

7.6. SERVICES

7.6.1. SDK

RACOM routers are shipping with a Software Development Kit (SDK) which offers a simple and fast way to implement customer-specific functions and applications. It consists of:

1. An SDK host which defines the runtime environment (a so-called sandbox), that is, controlling access to system resources (such as memory, storage and CPU) and, by doing so, catering for the right scalability.
2. An interpreter language called arena, a light-weight scripting language optimized for embedded systems, which uses a syntax similar to ANSI-C but adds support for exceptions, automatic memory management and runtime polymorphism on top of that.
3. A RACOM-specific Application Programming Interface (API), which ships with a comprehensive set of functions for accessing hardware interfaces (e.g. digital IO ports, GPS, external storage media, serial ports) but also for retrieving system status parameters, sending E-Mail or SMS messages or simply just to configure the router.

Anyone, reasonably experienced in the C language, will find an environment that is easy to dig in. However, feel free to contact us via `<support@racom.eu>` and we will happily support you in finding a programming solution to your specific problem.

The Language

The arena scripting language offers a broad range of POSIX functions (like printf or open) and provides, together with tailor-made API functions, a simple platform for implementing any sort of applications to interconnect your favourite device or service with the router.

Here comes a short example:

```
/* This script prints short status and if the SMS section is setted properly, the status ▶
will be send even to your mobile phone :-)
 */

printf("----------------------------");
printf("\n\n");
printf(nb_status_summary(all));
printf("\n\n");
printf("----------------------------");

/* Please change the following number to your mobile phone number
 */
nb_sms_send("+420123456789", nb_status_summary(all));
```

A set of example scripts can be downloaded directly from the router, you can find a list of them in the appendix. The manual at *menu SERVICES-Administration-Troubleshooting-SDK API* gives a detailed introduction of the language, including a description of all available functions.

SDK API Functions

The current range of API functions can be used to implement the following features:

1. Send/Retrieve SMS
2. Send E-mail
3. Read/Write from/to serial device
4. Control digital input/output ports
5. Run TCP/UDP servers
6. Run IP/TCP/UDP clients
7. Access files of mounted media (e.g. an USB stick)
8. Retrieve status information from the system
9. Get or set configuration parameters
10. Write to syslog
11. Transfer files over HTTP/FTP
12. Perform config/software updates
13. Control the LEDs
14. Get system events, restart services or reboot system
15. Scan for networks in range
16. Create your own web pages
17. Voice control functions
18. SNMP functions
19. Various network-related functions
20. Other system-related functions

The SDK API manual at *menu SERVICES-Administration-Troubleshooting-SDK API* provides an overview but also explains all functions in detail.

Please note that some functions require the corresponding services (e.g. E-Mail, SMS) to be properly configured prior to utilizing them in the SDK.

Let's now pay some attention to the very powerful API function nb_status. It can be used to query the router's status values in the same manner as they can be shown with the CLI. It returns a structure of variables for a specific section (a list of available sections can be obtained by running cli status -h).

By using the dump function you can figure out the content of the returned structure:

```
/* Dump current WAN status */

dump ( nb_status ("wan") );
```

The script will then generate lines like maybe these:

```
struct(35): {
  .WANLINK1_GATEWAY = string[3]: "n/a"
  .WANLINK2_REGISTRATION_STATE = string[23]: "registeredInHomeNetwork"
  .WANLINK1_STATE = string[7]: "dialing"
  .WANLINK2_STATE_UP_SINCE = string[19]: "2018-12-03 09:08:30"
  .WANLINK1_DIAL_ATTEMPTS = string[3]: "320"
  .WANLINK2_SIGNAL_STRENGTH = string[3]: "-69"
  .WANLINK2_DATA_DOWNLOADED = string[6]: "747608"
  .WANLINK2_DATA_UPLOADED = string[7]: "1225984"
  .WANLINK1_DATA_UPLOADED = string[3]: "n/a"
  .WANLINK2_ADDRESS = string[11]: "10.203.0.28"
  .WANLINK2_NETWORK = string[7]: "O2 - CZ"
  .WANLINK1_DIAL_SUCCESS = string[1]: "0"
  .WANLINK2_PDP = string[4]: "PDP1"
```

```
  .WANLINK1_ADDRESS = string[3]: "n/a"
  .WANLINK1_DOWNLOAD_RATE = string[1]: "0"
  .WANLINK2_SIM = string[4]: "SIM1"
  .WANLINK2_DOWNLOAD_RATE = string[2]: "52"
  .WANLINK1_UPLOAD_RATE = string[1]: "0"
  .WANLINK2_SIGNAL_LEVEL = string[2]: "46"
  .WANLINK2_SIGNAL_QUALITY = string[4]: "good"
  .WANLINK2_UPLOAD_RATE = string[2]: "85"
  .WANLINK2_DIAL_FAILURES = string[1]: "0"
  .WANLINK1_TYPE = string[3]: "eth"
  .WANLINK1_DIAL_FAILURES = string[3]: "319"
  .WANLINK2_DIAL_ATTEMPTS = string[1]: "3"
  .WANLINK2_MODEM = string[7]: "Mobile1"
  .WANLINK1_INTERFACE = string[4]: "LAN4"
  .WANLINK1_DATA_DOWNLOADED = string[3]: "n/a"
  .WAN_HOTLINK = string[8]: "WANLINK2"
  .WANLINK2_INTERFACE = string[5]: "WWAN1"
  .WANLINK2_SERVICE_TYPE = string[3]: "LTE"
  .WANLINK2_DIAL_SUCCESS = string[1]: "3"
  .WANLINK2_TYPE = string[4]: "wwan"
  .WANLINK1_STATE_DIALING_SINCE = string[19]: "2018-12-03 12:15:10"
  .WANLINK2_STATE = string[2]: "up"
}
```

In combination with the nb_config_set function, it is possible to start a re-configuration of any parts of the system upon status changes. You may find all possible parameters by reading the /etc/config/factory-config.cfg file accessible via CLI.

```
~ $ cat /etc/config/factory-config.cfg | grep ntp
network.ntp.status                      =1
network.ntp.server0                     =0.pool.ntp.org
network.ntp.server1                     =1.pool.ntp.org
network.ntp.ping                        =1
network.ntp.interval                    =256
network.ntp.gpstime                     =0
network.ntp.stratum                     =15
network.ntp.access.0.address            =192.168.1.0
network.ntp.access.0.netmask            =255.255.255.0
network.ntp.access.1.address            =
network.ntp.access.1.netmask            =
network.ntp.access.2.address            =
network.ntp.access.2.netmask            =
```

Here is an example how one might adopt those functions:

```
/* Check the current NTP server and set it to the IP address 192.168.0.2
and enable the NTP synchronisation */

printf ("The NTP server was previously using IP address: ");
printf (nb_config_get("network.ntp.server0"));
printf("\n\n");
```

```
nb_config_set("network.ntp.server0=192.168.0.2");

if (nb_config_get ("network.ntp.status") == "0"){
  printf ("and was not running.");
  printf("\n\n");
  nb_config_set ("network.ntp.status=1");
}
else {
  printf ("and was running.");
  printf("\n\n");
}

printf ("The NTP server is now running with IP address: ");
printf (nb_config_get("network.ntp.server0"));
```

Running SDK

In the SDK, we are speaking of `scripts` and `triggers` which form `jobs`. Any `arena` script can be uploaded to the router or imported by using dedicated user configuration packages. You may also edit the script directly at the Web Manager or select one of our examples. You also have a testing section on the router which can be used to check your syntax or doing test runs.

Once uploaded, you will have to specify a trigger, that is, telling the router when the script is to be executed. This can be either time-based (e.g. each Monday) or triggered by one of the pre-defined system events (e.g. wan-up) as described in *Section 7.6.7, "Events"*. With both, a script and a trigger, you can finally set up an SDK job now. The test event usually serves as a good facility to check whether your job is working as expected. The admin section also offers facilities to troubleshoot any issues and control running jobs. The SDK host (sdkhost) corresponds to the daemon managing the scripts and their operations and thus avoiding any harm to the system. In terms of resources, it will limit CPU and memory for running scripts and also provide a pre-defined portion of the available flash storage. You may, however, extend it by external USB storage.

Files written to `/tmp` will be hold in the memory and will be cleared upon a script restart.. As your scripts operate in the sandbox, you will have no access to the system tools (such as `ifconfig`).

Administration

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

| Administration | Status | Troubleshooting |

SDK
Administration
Job Management
Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SDK Administration

This kit provides a sandbox environment for running system jobs by means of self-scripted applications.

Administrative status:
  ○ enabled
  ○ disabled

Scheduling priority: normal ∨

Maximum flash usage: 3   (3..16 MB)

Enable watchdog: ☐

Apply

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

| Administration | Status | Troubleshooting |

SDK
Administration
Job Management
Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SDK Status
SDK environment is active

Finished Jobs

Job	Started	Ended	Exit Code
SMS-CONTROL	2014-06-09 13:07:08	2014-06-09 13:07:08	0

[Clear]

Running Jobs
There is no job currently running.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

| Administration | Status | Troubleshooting |

SDK
Administration
Job Management
Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SDK Troubleshooting

Select job: SMS-CONTROL   ▼   [View]

job 0 started at 2014-06-09 13:07:08 (running 'sms-control.are')
job 0 ended at 2014-06-09 13:07:08 (with exit code 0)

Output:

=== job 0 ended at 2014-06-09 13:07:08 (with exit code 0)

[Refresh]

This page can be used to control the SDK host and apply the following settings:

Administrative status — Specifies whether SDK scripts should run or not

Scheduling priority — Specifies the process priority of the sdkhost, higher priorities will speed up scheduling your scripts, lower ones will have less impact to the host system

Maximum flash usage — The maximum amount of Mbytes your scripts can write to the internal flash

Enable watchdog — This option enables watchdog supervision for each script. If the script does not respond or is stopped with an exit code not equal null, the system is rebooted.

The status page informs you about the current SDK status. It provides an overview about any finished jobs, you can also stop a running job there and view the script output in the troubleshooting section where you will also find links for downloading the manuals and examples.

Job Management

This page can be used to set up scripts, triggers and jobs.

It is usually a good idea to create a trigger first which is made up by the following parameters:

Name   A meaningful name to identify the trigger

Type   The type of the trigger, either time-based or event-based

Condition   Specifies the time condition for time-based triggers (e.g. hourly)

Timespec   The time specification which, together with the condition, specifies the `time(s)` when the trigger should be pulled

Event   The system event upon which the trigger should be pulled

You can now add your personal script to the system by applying the following parameters:

Name   A meaningful name to identify the script

Description   An optional script description

Arguments   An optional set of arguments passed to the script (supports quoting)

Action   You may either edit a script, upload it to the system or select one of the example scripts or an already uploaded script

You are ready to set up a job afterwards, it can be created by using the following parameters:

Name   A meaningful name to identify the job

Trigger   Specifies the trigger that should launch the job

Script   Specifies the script to be executed

Arguments   Defines arguments which can be passed to the script (supports quoting), they will precede the arguments you formerly may have assigned to the script itself

Testing

```
/* Check the current NTP server and set it to the IP address 192.168.0.2
and enable the NTP synchronisation */

printf ("The NTP server was previously using IP address: ");
printf (nb_config_get("network.ntp.server0"));
printf("\n\n");

nb_config_set("network.ntp.server0=192.168.0.2");

if (nb_config_get ("network.ntp.status") == "0"){
  printf ("and was not running.");
  printf("\n\n");
  nb_config_set ("network.ntp.status=1");
}
else {
  printf ("and was running.");
  printf("\n\n");
}
```

```
printf ("The NTP server is now running with IP address: ");
printf (nb_config_get("network.ntp.server0"));
```

The testing page offers an editor and an input field for optional arguments which can be used to perform test runs of your script or test dedicated portions of it. Please note that you might need to quote arguments as they will otherwise be separated by white-spaces.

```
/* arguments : schnick schnack "s c h n u c k" */

for (i = 0; i < argc ; i++) {
    printf (" argv %d: %s\n", i, argv [i]);
}

/* generates:
* argv 0: /scripts/testrun
* argv 1: schnick
* argv 2: schnack
* argv 3: s c h n u c k
*/
```

In case of syntax errors, arena will usually print error messages as follows (indicating the line and position where the parsing error occurred):

```
/scripts/testrun:2:10:FATAL: parse error, unexpected $, expecting ';'
```

(i) Note

It is now possible to upload SDK scripts into the Testing menu via browsing the required SDK script and clicking on the "Run" button.

SDK Sample Application

As an introduction, you can step through a sample application, namely the SMS control script, which implements remote control over short messages and can be used to send a system status back to the sender. The source code is listed in the appendix.

Once enabled, you can send a message to the phone number associated with a SIM / modem. It generally requires a password to be given on the first line and a command on the second, such as:

```
admin01
status
```

We strongly recommend to use authentication in order to avoid any unintended access, however you may pass noauth as argument to disable it. You can then skip the first line containing the password. Having a closer look to the script, you will see that you will also be able to restrict the list of permitted senders. Please inspect the system log for troubleshooting any issues.

The following commands are supported:

status   An SMS with the following information will be returned

               • Signal strength

- Mobile connection state (up/down)

- current IP address of the mobile interface

- current IP address of the VPN interface (if enabled)

connect	This will initiate a Dial-out connection over configured WAN (LAN or cellular) and the VPN connection (if enabled) and trigger sending an SMS with the following information: • current IP address of the PPP interface • current IP address of the VPN interface (if enabled)
disconnect	terminates all WAN connections (including VPN)
reboot	Initiates a system reboot
output 1 on	Switch digital output 1 on
output 1 off	Switch digital output 1 off
output 2 on	Switch digital output 2 on
output 2 off	Switch digital output 2 off

A response to the status command typically looks like:

```
System: MIDGE midge (0002A9FFC32E)
WAN1: WWAN1 is up (10.204.8.3, Mobile1,
HSPA, -65 dBm, LAI 23003)
DIO: IN1=off, IN2=off, OUT1=off, OUT2=on
```

7.6.2. DHCP Server

This section can be used to individually configure a DHCP service for each LAN interface.

Operational mode	The DHCP operational mode can be disabled or set to the "server" or "relay" mode. As a server, the unit answers to DHCP requests from hosts in the LAN directly. As a relay, the unit resends the requests to the configured DHCP server which handles them.
First lease address	First address for DHCP clients
Last lease address	Last address for DHCP clients
Lease duration	Number of seconds (30-86400) how long a given lease will be valid until it has to be requested again
Persistent leases	By checking this option, only static hosts will obtain the IP leases
DHCP options	By default DHCP will hand out the interface address as the default gateway and DNS server address if not configured elsewhere. It is possible to specify different addresses here.
Static Hosts	The option to add a static host configured with the IP address, MAC address and/or hostname.

7.6.3. DNS Server

The DNS server can be used to proxy DNS requests towards servers on the net which have for instance been negotiated during WAN link negotiation. By pointing DNS requests to the router, one can reduce outbound DNS traffic as it is caching already resolved names but it can be also used for serving fixed addresses for particular host names.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK	**DNS Server Administration**
Administration	
Job Management	Administrative status: ⦿ enabled
Testing	⭕ disabled
DHCP Server	
DNS Server	**DNS Server Configuration**
NTP Server	Domain name:
Dynamic DNS	Primary name server:
E-mail	Secondary name server:
Events	
SMS	Current name servers: 80.74.32.240 / 80.74.32.241
SSH/Telnet Server	**Static Hosts**
SNMP Agent	**Hostname** **Address**
Web Server	
Redundancy	
Modbus TCP	Apply

Administrative status	Enabled or disabled
Domain name	The domain name used for short name lookups.
Primary name server	The primary default name server which will be used instead of negotiated name servers.
Secondary name server	The secondary default name server which will be used instead of negotiated name servers.

You may further configure static hosts for serving fixed IP addresses for various hostnames. Please remember to point local hosts to the router's address for resolving them.

7.6.4. NTP Server

This section can be used to individually configure the Network Time Protocol (NTP) server function.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

NTP Server Administration

Administrative status: ● enabled ○ disabled

NTP Server Configuration

Poll interval: 256 seconds

Allowed hosts: Address: 192.168.1.0
Netmask: 255.255.255.0

Apply

Administrative status	Enabled or disabled
Poll interval	Defines the polling interval (64-4096 seconds) for synchronizing the time with the master clock servers
Allowed hosts	Defines the IP address range which is allowed to poll the NTP server

Note

See the description of how to set the correct router time in *the section called "Time & Region"*.

7.6.5. Dynamic DNS

Dynamic DNS client on this box is generally compatible with various DynDNS services on the Internet running by means of definitions by the DynDNS organization (see www.dyndns.com for server implementations).

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

DynDNS Administration

Administrative status: ○ enabled ● disabled

DynDNS Update Services

Provider	URL / Host	Status

Apply

Administrative status: Enabled or disabled

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
   Administration
   Job Management
   Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Add DynDNS Service

Provider:	dyndns.org
Dynamic address:	● derive from hotlink interface
	○ use outgoing interface address
	○ query CheckIP service at dyndns.org
Hostname:	
Username:	
Password:	
Protocol:	http

Apply

Dynamic address	Specifies whether the address is derived from the hotlink, outgoing interface address or via an external service. Usually, the hotlink option is used.
Hostname	The host-name provided by your DynDNS service (e.g. mybox.dyndns.org)
Username	The user-name used for authenticating at the service
Password	The password used for authentication
Protocol	The protocol used for authentication (HTTP, HTTPS).
Server address	The address of the server which shall be updated.
Server port	The port of the server which shall be updated.
TSIG key name	The name of the TSIG key which is allowed to perform updates.
TSIG key	The TSIG key encoded in base64.

Please note that your RACOM router can operate as DynDNS service as well, provided that you hold a valid SERVER license and have your hosts pointed to the DNS service of the router.

7.6.6. E-mail client

The E-Mail client can be used to send notifications to a particular E-Mail address upon certain events or by SDK scripts.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
Administration
Job Management
Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Redundancy

Configuration

E-mail Client Configuration

| Administrative status: | ● enabled |
| | ○ disabled |

From address:	
Server address:	
Server port:	25
Authentication:	automatic
Encryption:	none
Username:	
Password:	

Apply

Administrative status	E-mail client administrative status - enabled or disabled
From address	Sender e-mail address
Server address	SMTP server address
Server port	SMTP server port (typically 25)
Authentication	Choose the required authentication method to authenticate against the SMTP server
Encryption	The optional encryption for the e-mail messaging (none or TLS)
Username	User name for authentication
Password	Password for authentication

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

Configuration   Testing

Send E-Mail

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Redundancy

Recipient:
racom@racom.eu

Subject:
midge

Message:
text

Send

After configuring E-mail successfully, you can also test e-mail messages.

7.6.7. Events

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

Event Notification

Event(s)	Description	Send	Destination		
dio-in1-on	Power supply failure	SNMPv1 trap	192.168.10.200:162	⊟	☑
dio-in1-off	Power supply OK	SNMPv1 trap	192.168.10.200:162	⊟	☑
					⊞

Fire test event

By using the event manager you can notify remote systems about system events. A notification can be sent using E-Mail, SMS or SNMP traps.

Events

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Add Event Notification

Description:	
Send:	E-Mail + SMS ⌄
E-Mail address:	
Phone number:	

Category	Event		Description
CALL	☐	call-incoming	A voice call is coming in
	☐	call-outgoing	Outgoing voice call is being established
DDNS	☐	ddns-update-failed	Dynamic DNS update failed
	☐	ddns-update-succeeded	Dynamic DNS update succeeded
DIALIN	☐	dialin-down	Dial-In connection went down
	☐	dialin-up	Dial-In connection came up

E-Mail address   The E-Mail address to which the notification shall be sent (E-Mail client must be enabled)

Phone number   The phone number to which the notification shall be sent (SMS service must be enabled)

SNMP host   The SNMP host or address to which the trap shall be sent

SNMP port   The port of the remote SNMP service

Username   The username for accessing the remote SNMP service

Password   The password for accessing the remote SNMP service

Authentication   The authentication algorithm for accessing the remote SNMP service (MD5 or SHA)

Encryption   The encryption algorithm for accessing the remote SNMP service (DES or SHA)

Engine ID   The engine ID of the remote SNMP service

The messages will contain a description provided by you and a short system information.

The default texts for a specific Event are as follows:

Category	Event (ID)	Description
CALL	call-incoming (701)	A GSM call is coming in
	call-outgoing (702)	Outgoing voice call is being established
DDNS	ddns-update-failed (802)	Dynamic DNS update failed
	ddns-update-succeeded (801)	Dynamic DNS update succeeded
DIALIN	dialin-down (409)	Dial-In connection went down
	dialin-up (408)	Dial-In connection came up

Category	Event (ID)	Description
DIO	dio-in1-off (202)	DIO IN1 turned off
	dio-in1-on (201)	DIO IN1 turned on
	dio-in2-off (204)	DIO IN2 turned off
	dio-in2-on (203)	DIO IN2 turned on
	dio-out1-off (206)	DIO OUT1 turned off
	dio-out1-on (205)	DIO OUT1 turned on
	dio-out2-off (208)	DIO OUT2 turned off
	dio-out2-on (207)	DIO OUT2 turned on
GPS	gps-down (302)	GPS signal is not available
	gps-up (301)	GPS signal is available
GRE	gre-down (413)	GRE connection went down
	gre-up (412)	GRE connection came up
IPSEC	ipsec-down (404)	IPsec connection went down
	ipsec-up (403)	IPsec connection came up
MOBILEIP	mobileip-down (411)	Mobile IP connection went down
	mobileip-up (410)	Mobile IP connection came up
OPENVPN	openvpn-down (402)	OpenVPN connection went down
	openvpn-up (401)	OpenVPN connection came up
PPTP	pptp-down (407)	PPTP connection went down
	pptp-up (406)	PPTP connection came up
REDUNDANCY	redundancy-backup (1002)	System is now backup router
	redundancy-master (1001)	System is now master router
SDK	sdk-startup (507)	SDK has been started
SMS	sms-notsent (602)	SMS has not been sent
	sms-received (603)	SMS has been received
	sms-report-received (604)	SMS report has been received
	sms-sent (601)	SMS has been sent
SYSTEM	system-error (510)	System is in error state
	system-login-failed (501)	User login failed
	system-login-succeeded (502)	User login succeeded
	system-logout (503)	User logged out
	system-no-error (511)	System left error state
	system-poweroff (509)	System poweroff has been triggered
	system-rebooting (504)	System reboot has been triggered
	system-startup (505)	System has been started
	system-time-updated (508)	System time has been updated
TEST	test (506)	test event
USB	usb-eth-added (903)	USB Ethernet device has been added
	usb-eth-removed (904)	USB Ethernet device has been removed

Category	Event (ID)	Description
	usb-serial-added (905)	USB serial device has been added
	usb-serial-removed (906)	USB serial device has been removed
	usb-storage-added (901)	USB storage device has been added
	usb-storage-removed (902)	USB storage device has been removed
WAN	wan-down (101)	WAN link went down
	wan-up (102)	WAN link came up

7.6.8. SMS

This page lets you turn on the SMS event notification service and enable remote control via SMS.

Administration

On RACOM routers it is possible to receive or send short messages (SMS) over each mounted modem (depending on the assembly options). Messages are received by querying the SIM card over a modem, so prior to that, the required assignment of a SIM card to a modem needs to be specified on the SIMs page.

Please bear in mind, in case you are running multiple WWAN interfaces sharing the same SIM, that the system may switch SIMs during operation which will also result in different settings for SMS communication.

Sending messages heavily depends on the registration state of the modem and whether the provided SMS Center service works and may fail. You may use the sms-report-received event to figure out whether a message has been successfully sent.

Received messages are pulled from the SIMs and temporarily stored on the router but get cleared after a system reboot. Please consider to consult an SDK script in case you want to process or copy them.

Sending messages heavily depends on the registration state of the modem and whether the provided SMS Center service works and may fail. You may use the sms-report-received event to figure out whether a message has been successfully sent.

Please do not forget that modems might register roaming to foreign networks where other fees may apply. You can manually assign a fixed network (by LAI) in the SIMs section.

We identify SIMs based on their IMEI number and track their statistics in a non-volatile manner.

The relevant page can be used to enable the SMS service and specify on which modem should operate.

| Administrative status | Enable or disable SMS notifications and control |
| Request delivery report | Enable or disable receiving the confirmation whether SMS was successfully received or not. This can be then read in the SMS Status menu. |

Routing & Filtering

By using SMS routing you can specify outbound rules which will be applied whenever messages are sent. You can forward them to an enabled modem. For a particular number, you can for instance enforce messages be sent over a dedicated SIM.

Phone numbers can also be specified by regular expressions, here are some examples:

```
+12345678   Specifies a fixed number
+1*         Specifies any numbers starting with +1
+1*9        Specifies any numbers starting with +1 and ending with 9
+[12]*      Specifies any numbers starting with either +1 or 2
```

Please note that numbers have to be entered in international format including a valid prefix. On the other hand, you can also define rules to drop outgoing messages, for instance, when you want to avoid using any expensive service or international numbers.

Both types of rules form a list will be processed in order, forwarding outgoing messages over the specified modem or dropping them. Messages which are not matching any of the rules below will be dispatched to the first available modem.

Filtering serves a concept of firewalling incoming messages, thus either dropping or allowing them on a per-modem basis. The created rules are processed in order and in case of matches will either drop or forward the incoming message before entering the system. All non-matching messages will be allowed.

Status

The status page can be used to the current modem status and get information about any sent or received messages. There is a small SMS inbox reader which can be used to view or delete the messages. Please note that the inbox will be cleared each midnight in case it exceeds 512 kbytes of flash usage.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

| Administration | Routing | Status | Testing |

SMS Status

Modem	Status		Used Memory	Sent / Received
Mobile1	idle		0 of 10	2 / 1

Refresh

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

Testing

This page can be used to test whether SMS sending in general or filtering/routing rules works. The maximum length per message part is limited to 160 characters, we also suggest to exclusively use characters which are supported by the GSM 7-bit alphabet.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

| Administration | Routing | Status | Testing |

Send SMS

Phone number:
+420123456789

Message:
text

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Send

7.6.9. SSH/Telnet Server

Apart from the Web Manager, the SSH and Telnet services can be used to log into the system. Valid users include root and admin as well as additional users as they can be created in the User Accounts section. Please note, that a regular system shell will only be provided for the root user, the CLI will be launched for any other user whereas normal users will only be able to view status values, the admin user will obtain privileges to modify the system.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

Telnet Server Configuration

Administrative status: ◉ enabled   ○ disabled

Server port: `23`

SSH Server Configuration

Administrative status: ◉ enabled   ○ disabled

Server port: `22`

Disable admin login: ☐

Disable password-based login: ☐   upload authorized keys

Please note that these services will be accessible from the WAN interface also. In doubt, please consider to disable or restrict access to them by applying applicable firewall rules.

The following parameters can be applied to the Telnet service:

Administrative status   Whether the Telnet service is enabled or disabled

Server port   The TCP port of the service (usually 23)

The following parameters can be applied to the SSH service:

Administrative status   Whether the SSH service is enabled or disabled

Server port   The TCP port of the service (usually 22)

Disable admin login   If checked, access via SSH for admin and root users will be blocked. Other users may have access as usual, but with restricted privileges.

Disable password-based login   By turning on this option, all users will have to authenticate by SSH keys which can be uploaded to the router.

ⓘ Note

You can manually upload the authorized keys.

7.6.10. SNMP Agent

M!DGE is equipped with an SNMP daemon, supporting basic MIB tables (such as ifTable), plus additional enterprise MIBs to manage multiple systems. M!DGE OID starts with 1.3.6.1.4.1.33555.10 prefix. The corresponding VENDOR MIB can be downloaded from the router.

Parameter	Supported MIBs
.1.3.6.1.2.1	MIB-II (RFC1213), SNMPv2-MIB (RFC3418)
.1.3.6.1.2.1.2.1	IF-MIB (RFC2863)
.1.3.6.1.2.1.4	IP-MIB (RFC1213)
.1.3.6.1.2.1.10.131	TUNNEL-MIB (RFC4087)
.1.3.6.1.2.25	HOST-RESOURCES-MIB (RFC2790)
.1.3.6.1.6.3.10	SNMP-FRAMEWORK-MIB
.1.3.6.1.6.3.11	SNMPv2-SMI (RFC2578)
.1.0.8802.1.1.2	LLDP-MIB
.1.0.8802.1.1.2.1.5.4795	LLDP-EXT-MED-MIB
.1.3.6.1.4.1.33555	VENDOR-MIB

The VENDOR-MIB tables offer some additional information over the system and its WWAN, GNSS and WLAN interfaces. They can be accessed over the following OIDs:

Parameter	RACOM MIB OID Assignment
admin	.1.3.6.1.4.1.33555.10.40
mgWwanTable	.1.3.6.1.4.1.33555.10.50
mgGnssTable	.1.3.6.1.4.1.33555.10.51
dio	.1.3.6.1.4.1.33555.10.53
mgSerialTable	.1.3.6.1.4.1.33555.10.54
mgWlanTable	.1.3.6.1.4.1.33555.10.60
mgWlanStationTable	.1.3.6.1.4.1.33555.10.61
mgHotLink	.1.3.6.1.4.1.33555.10.70
mgWanTable	.1.3.6.1.4.1.33555.10.71
sdk	.1.3.6.1.4.1.33555.10.90
traps	.1.3.6.1.4.1.33555.10.100

(i) Note

GNSS and WLAN on M!DGE are available with special extension only.

M!DGE extensions contain support for:

- Rebooting the device
- Updating to a new system software via FTP/TFTP/HTTP
- Updating to a new system configuration via FTP/TFTP/HTTP
- Getting WWAN/GNSS/WLAN/DIO information

ⓘ **Note**

Attention must be paid to the fact that SNMP passwords have to be more than 8 characters long. Shorter passwords will be doubled for SNMP, e.g. 'admin01' becomes 'admin01admin01'.

SNMP extensions can be read and triggered as follows:

- To get system software version:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.1.0
- To get a kernel version:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.2.0
- To get a serial number:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.3.0
- To restart the device:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.10.0 i 1
- To run a configuration update:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.11.0 s "*http://server/directory*"

ⓘ **Note**

config Update expects a zip-file named <serial-number>.zip in the specified directory which contains at least a "user-config.zip".
Supported protocols are TFTP, HTTP(s) and FTP.
Specifying a username/password or port is not yet supported.

- get configuration update status:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.12.0
  The return value can be one of: (1) succeeded, (2) failed, (3) inprogress, (4) notstarted.
- run software update:
  snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.13.0 s "http://server/directory"
- get software update status:
  snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.33555.10.40.14.0
  Return value can be either of: (1) succeeded, (2) failed, (3) inprogress, (4) notstarted.

SNMP Configuration

Configuration | Authentication

SNMP Agent Configuration

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Administrative status:	● enabled
	○ disabled
Operation mode:	● v1 | v2c | v3 ○ v3 only
Contact:	
Location:	
Listening port:	161

Download MIB

Apply

Administrative status	Enable or disable the SNMP agent
Operation mode	Specifies if agent should run in compatibility mode or for SNMPv3 only
Contact	System maintainer or other contact information
Location	Device location
Listening port	SNMP agent port

Once the SNMP agent is enabled, SNMP traps can be generated using SDK scripts or can be triggered by various Events (see the SYSTEM → Events menu).

SNMP Authentication

Configuration | Authentication

SNMP v3 Authentication

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Redundancy

Authentication:	MD5 ∨
Encryption:	DES ∨

Manage users

SNMP v1/v2c Authentication

Read community:	public
Admin access:	● enabled ○ disabled
	Admin community:
	Allowed host:

Apply

When running in SNMPv3, it is possible to configure the following two authentication options:

Authentication   Defines the authentication (MD5 or SHA)

Encryption   Defines the privacy protocols to use (DES or AES)

Both the Authentication and Encryption passwords are the same and equal to the user's password. In general, the admin user can read and write any values. Read access will be granted to any other system users.

There is no authentication/encryption in SNMPv1/v2c and should not be used to set any values. However, it is possible to define its communities and authoritative host which will be granted administrative access.

Read community   Defines the community name for read access

Admin community   Defines the community name for admin access

Allowed host   Defines the host which is allowed for admin access

(i) Note

       The SNMP daemon is also listening on WAN interfaces and it is therefore suggested to restrict the access via the firewall.

7.6.11. Web Server

This page can be used to configure different ports for accessing the Web Manager via HTTP/HTTPS. We strongly recommend to use HTTPS when accessing the web service via a WAN interface as the communication will be encrypted and thus avoids any misuse of the system.

In order to enable HTTPS you would need to generate or upload a server certificate in the section SYSTEM-Keys and Certificates.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Discovery

Redundancy

Modbus TCP

Terminal Server

Web Server Configuration

HTTP

Administrative status:	⦿ enabled
	◯ disabled
HTTP port:	80

HTTPS

Administrative status:	⦿ enabled
	◯ disabled
HTTPS port:	443
HTTPS certificate:	installed
HTTPS security	⦿ modern (Firefox 27, Chrome 30, IE 11 on Windows 7, ...)
	◯ old (Firefox 1, Chrome 1, IE 7, ...)
	◯ none (Windows XP IE6, Java 6)
Enable CLI-PHP:	☐

Apply

Administrative status	Enable or disable the Web server
HTTP port	Web server port for HTTP connections
HTTPS port	Web server port for HTTPS connections
HTTPS certificate	Either information that the certificate is 'installed' or a link to create such certificate.
HTTPS security	Choose the HTTPS security level - follow the help within the menu itself.
Enable CLI-PHP	Enable CLI-PHP service (see *Section 8.16, "CLI–PHP"*)

7.6.12. Softflow

This page can be used to configure the network traffic analyser daemon Softflow used for exporting NetFlow traffic data.

Parameters	Softflow Settings
Interface	Interface on which to listen for traffic
Host address	Destination address of the traffic data
Port	Port of the destination address
Protocol version	Protocol version of the data
Maximum flows	The maximum number of flows to concurrently track
Track level	Flow elements that should be used to define a flow
Sample rate	Periodical sampling rate

7.6.13. Discovery

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Discovery

Discovery

| Administrative status: | ◉ enabled |
| | ○ disabled |

Enabled protocols:	☑ LLDP
	☐ CDP
	☐ SONMP
	☐ EDP
	☐ FDP
	☐ IRDP

[Apply]

Discovery protocols can be used to discover and to get discovered by other hosts.

Administrative status   Enable or disable the Discovery

The following protocols are supported:

LLDP	Link Layer Discovery Protocol
CDP	Cisco Discovery Protocol
FDP	Foundry Discovery Protocol
SONMP	Nortel Discovery Protocol
EDP	Extreme Discovery Protocol
IRDP	ICMP Router Discovery Protocol

IRDP implements RFC1256 and can also inform locally connected hosts about the nexthop gateway. Any discovered hosts will be exposed to the LLDP-MIB and can be queried over SNMP or CLI/GUI.

7.6.14. Redundancy

This section can be used to set up a redundant pair of M!DGE (or other systems) by running the Virtual Router Redundancy Protocol (VRRP) among them. A typical VRRP scenario defines the first host playing the master and another the backup device, they both define a virtual gateway IP address which will be distributed by gratuitous ARP messages for updating the ARP cache of all LAN hosts and thus redirecting the packets accordingly.

A takeover will happen within approximately 3 seconds as soon as the partner is no longer reachable (checked via multicast packets). This may happen when one device is rebooting or the Ethernet link went down. Same applies when the WAN link goes down.

In case DHCP has been activated, please keep in mind that you will need to reconfigure the DHCP gateway address offered by the server and let them point to the virtual gateway address. In order to

avoid conflicts you may turn off DHCP on the backup device or even better, split the DHCP lease range in order to prevent any lease duplication.

> **ⓘ** **Note**
>
> M!DGE assigns a priority of 100 to the master and 1 to the backup router. Please adapt the priority of your third-party device appropriately.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Redundancy

Redundancy

Administrative status:	
	⦿ enabled
	◯ disabled

Role:	master ⌄
VID:	100
Interface:	LAN1 ⌄
Virtual gateway address:	192.168.1.10

[Apply]

Administrative status	Enable or disable Redundancy
Role	Role of this system (either master or backup)
VID	The Virtual Router ID (you can theoretically run multiple instances)
Interface	Interface on which VRRP should be performed
Virtual gateway address	Virtual gateway address formed by the participating hosts

7.6.15. Modbus TCP

While in UHF RipEX radios, using Modbus TCP transparently was not a preferred option, in the cellular routers, on contrary, it is a recommended solution. In such a case that all connected devices use Modbus TCP, there is no need to use and configure this feature. Just send data transparently as TCP over the cellular network.

But if you combine Modbus TCP and Modbus RTU within one network, you should use our Modbus TCP solution. You do not need any external Modbus TCP - Modbus RTU converter, the functionality is implemented in the M!DGE firmware.

The Modbus TCP daemon listens for the local TCP connection on the TCP port 502 by default. After the connection is established, the communication can be initiated. Any incoming Modbus TCP datagram is investigated and based on the Modbus TCP "Unit ID" Byte and Address translation Table/mask rules,

is forwarded as UDP to the final destination (by default the UDP port is 8902), e.g. another M!DGE unit with Modbus RTU device connected over the RS232 port.

> **(i)** **Note**
>
> This behaviour comes from the RipEX functionality where UDP is a preferred transport solution. In case of cellular networks, TCP might be a better solution. When implementing this solution into your network, you might configure Modbus TCP on the remote M!DGE (not a unit locally connected via Ethernet) causing the TCP session to be between a local device and remote M!DGE instead of UDP. The final conversion from TCP to UDP so the Protocol server listening on the UDP port 8882 by default is done at the remote unit afterwards. In such a case, make a Translation rule which sends all received packets to the localhost.

> **⚠** **Important**
>
> In some Modbus TCP implementations, Unit ID field within the datagram is always set to "FF". In such a case, you can use the "Replace PLC address" option so that the Unit ID is replaced by some Modbus RTU address. Thanks to this parameter, regular Mask/Table address translation can be used. Consider carefully where you put the corresponding parameter (local or remote M!DGE and if placed in Modbus TCP or Modbus RTU Protocol server menu - it can be set at both places, but not simultaneously).

See the Application note for more details and examples.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
   Administration
   Job Management
   Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Redundancy

Modbus TCP

Modbus TCP

Administrative status	● enabled
	○ disabled
My TCP Port	502 TCP Inactivity [s] 120
Transport Protocol	UDP
Port	8902
Broadcast	Off
Replace PLC address	Off

Address translation

Address translation	Table
Base IP	10.10.10.1
Mask	255.255.255.0
Interface (Destination port)	COM(8882)

Apply

Administrative status	Enable or disable the feature.
My TCP Port	The TCP port for a session with local Modbus TCP Master. It can also be a remote Modbus TCP Master resulting in a TCP session over the cellular network instead of UDP.
TCP inactivity [s]	The TCP inactivity timeout in seconds.

Transport protocol	The transport protocol used, must be set to UDP only.
Port	The port number for a transport protocol (8902 by default).
Broadcast	The broadcast is always disabled in cellular networks.
Replace PLC address	If set, manually configure replacing the current PLC with a configured Modbus RTU address. Modbus TCP consists of the Unit ID field which can be changed manually by this parameter.
Address translation	See *Protocol Server* article.

7.6.16. Terminal Server

Generally a Terminal Server (also referred to as a Serial Server) enables connection of devices with serial interface to a M!DGE over the local area network (LAN), or even over the cellular network. It is a virtual substitute for devices used as serial-to-TCP(UDP) converters. It is possible to configure two Terminal servers.

Examples of the use:

A SCADA application in the centre should be connected to the cellular (M!DGE) network via a serial interface, however for some reason that serial interface is not used. The operating system (e.g. Windows) can provide a virtual serial interface to such application and converts the serial data to TCP (UDP) datagrams, which are then received by the Terminal server in M!DGE. This type of interconnection between M!DGE and application is especially advantageous when:

- there is not any physical serial interface on the computer

- the serial cable between M!DGE and computer would be too long (e.g. the M!DGE is installed very close to the antenna to improve radio coverage)

- the LAN between the computer and the place of M!DGE installation already exists

- Modbus TCP is used with local TCP sessions on slave sites or when combination of Modbus RTU and Modbus TCP is used. For more information refer to *Application note Modbus TCP/RTU*[4]. This applies also to other SCADA protocol TCP versions, e.g. DNP3 TCP.

(i) **Note**

> If configured on LAN, the TCP (UDP) session operates only locally between the M!DGE and the central computer, hence it does not increase the data load on WWAN (cellular network).

In some special cases, the Terminal server can be also used for reducing the network load from applications using TCP. A TCP session can be terminated locally at the Terminal server in M!DGE, user data extracted from TCP messages and processed like it comes from a serial (RS232) port. When data reaches the destination M!DGE, it can be transferred to the RTU either via a serial interface or via TCP (UDP), using the Terminal server again.

---

[4] https://www.racom.eu/eng/products/m/ripex/app/modbus/index.html

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

Servers

SDK
  Administration
  Job Management
  Testing

DHCP Server

DNS Server

NTP Server

Dynamic DNS

E-mail

Events

SMS

SSH/Telnet Server

SNMP Agent

Web Server

Discovery

Redundancy

Modbus TCP

Terminal Server

Terminal Server Administration

Administrative status   ○ enabled
                        ⦿ disabled

Terminal Servers

Number	Type	My IP	My Port	Status	
1	TCP	0.0.0.0	50001	disabled	✎
2	TCP	0.0.0.0	50002	disabled	✎

Apply

Administrative status   Enable or disable the feature

If Enabled, 2 independent Terminal servers can be set up.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

Servers   Terminal Server   Protocol Settings   Server number: 1

Terminal Server

Administrative status   ○ enabled
                        ⦿ disabled

Type   TCP

TCP Inactivity   120

My IP   Manual   0.0.0.0

My Port   50001

Destination IP   0.0.0.0

Destination Port   0

Apply   Continue

Administrative status   Enable or disable the particular TS

Type   Set the TS Type - either TCP or UDP session

TCP Timeout   If the Type is TCP, configure the required TCP timeout (i.e. close the TCP session if there is no communication for a given time period)

My IP	IP address of M!DGE - usually Ethernet interface, but IP address of any interface can be used (pre-set IP address of given interface). "Manual" IP can also be filled.
My Port	Set any listening TCP/UDP port (i.e. M!DGE listens for incoming connection on a given port).
Destination IP	The destination IP address of TCP/UDP session (e.g. locally connected SCADA, virtual serial interface). IP address 0.0.0.0 can also be configured - any host can open the session with M!DGE.
Destination Port	The destination port of TCP/UDP session. In some cases, applications dynamically change the IP port with each datagram. In such a case set Destination port=0. M!DGE will then send replies to the port from which the last response was received. This feature allows to extend the number of simultaneously opened TCP connections between a M!DGE and locally connected application to any value up to 10 on each Terminal server.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

Servers	Terminal Server	Protocol Settings	Server number: 1

Protocol Server

Protocol	- None -

Transport Protocol	UDP
Port	8892

Apply   Continue

Protocol follows the same principles as a protocol on RS232 interface. The default UDP port is 8892 (transporting data usually over cellular network).

7.6.17. Voice Gateway

You can set up a voice gateway on the M!DGE2 router which can be used to connect mobile calls to VoIP clients and vice versa.

Administration:

The following parameters can be used to set it up:

Administrative status   Specifies whether the gateway shall be enabled or disabled

Call routing   Defines who will be responsible for call routing. If SDK has been spe-
                           cified you would need to install a script (see examples) which will be
                           responsible for routing and accepting the calls. Otherwise the static
                           routing configuration will be used.

In case you are running multiple WWAN interfaces sharing the same SIM, please bear in mind that the system may switch SIMs during operation which will also result in different settings for voice communication.

Endpoints:

On this page you can activate the endpoints used for voice communication, the following types are supported:

Voice-Over-Mobile Endpoint for GSM/UMTS/LTE calls (can be used for calls to mobile or landline phones)

Nil-Device A proforma Device to enable Call Signaling without Voice Support

Based on your equipment, we recommend to adjust the modem's audio profile for a better sound experience. The following profiles are available:

Handset Provides a mild echo, short delay (less than 16-ms dispersion). This mode is intended for use with a well-designed handset, where the Echo Return Loss (ERL) is generally high. Full-duplex performance is easiest to achieve in this mode.

Headset Provides a moderate echo, short delay (less than 16-ms dispersion). This mode is intended for use in situations where the echo may be loud but low in delay. There are a variety of different headsets available with a wide variety of echo characteristics and noise pickup. Although the echo delay is typically short (< 16 ms) with all headsets, the echo return loss characteristics can vary significantly and are not well known a priori to the handset designer. This mode is more robust and more aggressive at echo cancellation.

Speakerphone Handle situations of loud echo with extreme acoustic distortion. This mode is intended for use with a car kit or speakerphone applications with high volume and high distortion. Acoustic echo in this situation has negative ERL and is impossible to cancel completely. It operates in a half-duplex manner and will be very aggressive in muting the entire signal to prevent any echo blips from being heard.

Bluetooth/Carkit Provides moderate echo, long delay (up to 64-ms dispersion). These modes are intended for bluetooth headsets and carkits which may have DSP processing on board and could give added delay to the system.

Volume level Specifies the modem's volume level. 1 = low. 9 = high.

Routing:

This page can be used to configure generic voice routing between the endpoints.

Enhanced routing facilities are provided via the SDK interface which is able to dispatch voice calls based on their attributes (such as phone number) and other system related status information (e.g. number/duration of calls per endpoint, registration status and so on). Using the SDK, you can also initiate or accept a call, adjust its volume level or do a hangup.

Anyway, for simple scenarios the generic method should be sufficient and can be configured as follows:

Source   Specifies the source endpoint (i.e. where the call comes in)

Mode   The type of action which shall be applied for the call: DROP will silently hangup the call, ROUTE will route the call to the specified endpoint. Destination Specfies the target endpoint (i.e. where to call is routed to).

7.7. SYSTEM

7.7.1. System

Settings

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System	Syslog	LEDs	Bootloader

System
Settings
Time & Region
Reboot

Authentication
Authentication
User Accounts
Remote Authentication

Local hostname: MIDGE

Application area: stationary

Reboot delay: 3 seconds

Enable TCP timestamps: ☑

Local host name: The local system hostname

Application area: The desired application area which influences the system behaviour such as registration timeouts when operating in the mobile environment.

Reboot delay: The number of seconds to wait before the reboot is initiated (might be needed for some system-rebooting events).

Enable TCP timestamps: Enable TCP timestamps for system wide TCP communication. This is needed for Protection Against Wrapped Sequence numbers (PAWS), but with these timestamps enabled a remote attacker can guess the uptime of the system. The uptime is a lower bound for the age of the main system components like the kernel. If the system has an uptime of 3 years, it's unlikely that recent security patches were applied.

Syslog

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System	Syslog	LEDs	Bootloader

System
Settings
Time & Region
Reboot

Authentication
Authentication
User Accounts
Remote Authentication

Software Update

Storage: flash root

Max. filesize: 2048 kB (max. 65536)

Redirect address:

Apply

Storage: The storage device on which logfiles shall be stored.

Max. filesize: The maximum size of the logfiles (in kB) until they will get rotated.

Redirect address: Specifies an IP address to which log messages should be redirected to. A tiny system log server for Windows is included in TFTP32 which can be provided if requested.

In general, the unit comes with an internal flash device which can be used to store data or you can use the external USB disk.

Flash root   The root partition of the internal flash.

USB disk   A storage disk connected to the external USB port.

LEDs

This menu allows to configure the behaviour of the LEDs on the front panel. The first LED (STAT) cannot be changed.

Bootloader

Password   The password used to unlock the bootloader. If empty, the admin password will be used.

Time & Region

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. M!DGE can synchronize its system time with an NTP server. If enabled, time synchronization is usually triggered after a WAN link has come up but before starting any VPN connections. Further time synchronizations are scheduled in the background every 60 minutes.

Current system time:	The current system time which can be synchronized against a valid NTP server or set manually. If manually set, the time is lost after the reboot.
NTP server 1:	The primary NTP server IP address or hostname.
NTP server 2 (optional):	The optional secondary NTP server IP address or hostname.
Ping check	Uses an ICMP ping to check whether NTP servers are available when running initial time update.
Time zone:	Time zone based on your geographical location.
Daylight saving changes:	This option can be used to reflect daylight saving changes (e.g. switching from summer to standard time) depending on the selected time zone.

Sync will perform the time synchronization immediately.

Virtualization

Virtualization gives customers the possibility to execute their own applications.

Reboot

This menu can be used to reboot the system. All WAN links will be interrupted.

7.7.2. Authentication

Authentication

This page offers a simple shortcut to allow only secure connections (SSH, HTTPS) for managing the router. If the option "Secure authentication preferred" is set, users will be redirected to HTTPS but can still login via HTTP/telnet.

User Accounts

This page lets you manage the user accounts on the device.

The standard admin user is a built-in power user that has permission to access the Web Manager and other administrative services and is used by several services as the default user. Keep in mind that the admin password will be also applied to the root user which is able to enter a system shell. Any other user represents a user with lower privileges, for instance it has only permission to view the status page or retrieve status values when using the CLI.

| Username: | Define a user name. |

Description: The user description.

Role   Either admin or user.

Old password   Enter the current password.

New password   Enter a new password.

Confirm new password Enter a new password again to confirm correctness.

> **ⓘ Note**
>
> When adding additional admin users you are required to provide the password of the default administrator.

Remote Authentication

A remote RADIUS server can be used to authenticate users. This applies for the Web Manager and other services supporting and incorporating remote authentication.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
 Settings
 Time & Region
 Reboot

Authentication
 Authentication
 User Accounts
 Remote Authentication

Software Update
 Software Update
 Modem Firmware Update
 Software Profiles

Configuration
 File Configuration
 Factory Configuration

Troubleshooting
 Network Debugging
 System Debugging
 Tech Support

Keys & Certificates

Licensing

Legal Notice

Remote Authentication

Administrative Status: ● enabled
                          ○ disabled

Use for login: ☑

Primary RADIUS Configuration

Server address:

Secret:

Authentication port: 1812

Accounting port: 1813

Secondary RADIUS Configuration

Server address:

Secret:

Authentication port: 1812

Accounting port: 1813

Apply

Administrative status: Enable or disable remote authentication.

Use for login: This option enables remotely-defined users to access the Web Manager.

Primary RADIUS configuration:

Server address: RADIUS server address.

Secret: Secret used to authenticate against the RADIUS server.

Authentication port: Port used for authentication.

Accounting port: Port used for accounting messages.

Secondary RADIUS configuration:

This is used if the first server is not available.

7.7.3. Software Update

Manual Software Update

This menu can be used to run a manual software update.

Update operation: The update operation method being used. You can upload the image or download it from the given URL

URL: You can upload the image or download it from the given URL.

Admin password: Required for downgrades to releases before 4.2.

When issuing a software update, the current configuration (including files like keys/certificates) will be backuped. Any other modifications to the filesystem will be erased. The configuration is generally backward-compatible. We also apply forward compatibility when downgrading to a previous software within the same release line, which is accomplished by sorting out unknown configuration directives which actually may lead to loss of settings and features. Therefore, it's always a good idea to keep a copy of the working configuration. Generally, we do not recommend downgrading the software.

A software image can be either uploaded via the Web Manager or retrieved from a specific URL. It will be unpacked and deployed to a spare partition which gets activated if the update completed successfully. The whole procedure is accompanied by all green LEDs flashing up, the subsequent system reboot gets denoted by a slowly blinking Status LED. The backuped configuration will be applied at bootup and the Status LED will blink faster during this operation. Depending on your configuration, this may take a while.

> **ⓘ** **Note**
>
> Starting with SW release 4.2 we set default to not saving passwords; using password hashes instead. Storing passwords for users can be enabled, but is not recommended for new applications.
>
> Older SW releases require the passwords to be stored encrypted on the device. As we don't have them any more in release version 4.2 and later you will have to provide the administrator password if you want to downgrade to a release 4.1.x and lower. The same passphrase will be used for bootloader login as well.
>
> All users which have no password stored on the device will not be able to login after downgrade until new passwords have been applied.

Automatic Software Update

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

| Manual | Automatic |

Automatic Software Update

Status:	○ enabled
	● disabled
Time of day:	00:00
URL:	

[Apply]

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Modem Firmware Update
  Software Profiles

Status: Enable/disable automatic software update

Time of day: Every day at this time M!DGE will do a check for updates

URL: The server URL where the software update package should be downloaded from. Supported protocols are TFTP, HTTP(s), and FTP

Firmware Update

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Modem Firmware Update

Modem firmware update manages internal firmware of modules integrated into the router like WWAN or WLAN.

Update operation:	● Upload image
	○ Download from URL
Module:	WWAN1 (tobyl2) ∨
Storage:	Root1 ∨
Firmware package:	[Procházet...] Soubor nevybrán.

[Upload]

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Modem Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

This menu can be used to perform a firmware update of a specific module.

Update operation: The update operation method being used. You can upload a firmware package or download the files from a specific URL.

Module: The module which shall be updated.

Storage: The temporary storage which shall be used for the update procedure. For boxes with limited amount of flash it is possible to use an USB stick which must be properly set up in the USB section and hold a proper filesystem such as ext4.

URL: The server URL where the firmware files should be downloaded from. Supported protocols are TFTP, HTTP, HTTPS, and FTP (protocol://server/path/file).

Software Profiles

In every router you have two software profiles. One is active (currently used) and one is inactive. You can easily switch between these profiles any time.

It can be for example useful when there is some issue with the newest firmware and you need to restore the previous firmware version easily. Or you can just test some new features in the newest firmware and then get back to the previous one.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Available Software Profiles

Profile 1	Status:	active
	Version:	3.8.40.100
	Installed:	2015-05-28 17:05:07

Profile 2	Status:	inactive
	Version:	0.0.0.0
	Installed:	2015-04-27 02:04:10

Switch Profile

| Current profile: | Profile 1 |
| Switch to: | Profile 2 ⌄ with current ⌄ configuration |

Switch

7.7.4. Configuration

Configuration via the Web Manager becomes tedious for large volumes of devices. M!DGE therefore offers automatic and manual file-based configuration to automate things. Once you have successfully set up the system you can back up the configuration and restore the system with it afterwards. You can either upload a single configuration file (.cfg) or a complete package (.zip) containing the configuration file and a packed version of other essential files (such as certificates).

File Configuration

This section can be used to download the currently running system configuration (including essential files such as certificates).

The current configuration file is updated after every change and the time of this update is displayed along with a configuration version and a security hash. The current configuration can be updated manually by pressing the Apply button.

In order to restore a particular configuration you can upload a configuration previously downloaded or update configuration from the provided URL link.

You can choose between missing configuration directives stay the same as in the currently running configuration.

Automatic Updates

Status: Enable/disable automatic configuration update

Time of day: Time of day when the system will check for updates

URL: The server URL where the configuration file should be retrieved from (supported protocols are HTTP(s), TFTP, FTP)

Factory Configuration

This menu can be used to reset the device to factory defaults. Your current configuration will be lost.

This procedure can also be initiated by pressing and holding the Reset button for at least 10 seconds. A successfully initiated factory reset can be noticed by all LEDs being turned on.

Factory reset will set the IP address of the Ethernet interface back to 192.168.1.1. You will be able to communicate again with the device using the default network parameters.

You may store the currently running configuration as factory defaults which will reside active even when a factory reset has been initiated (e.g. by your service staff). Please ensure that this corresponds to a working configuration. A real factory reset to the default settings can be achieved by restoring the original factory configuration and initiating the factory reset again.

⚠️ **Important**

If you store the currently running configuration as the factory defaults, have in mind that the password is also stored within this configuration.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
 Settings
 Time & Region
 Reboot

Authentication
 Authentication
 User Accounts
 Remote Authentication

Software Update
 Software Update
 Firmware Update
 Software Profiles

Configuration
 File Configuration
 Factory Configuration

Initiate Factory Reset

This operation will reset all settings to factory defaults. Your current configuration will be lost.
You may consider backing up the current configuration prior to running a reset.

[Reset]

Factory Default Configuration

You may store the currently running configuration as factory defaults.
This configuration will be activated whenever a factory reset has been triggered.

[Store]

7.7.5. Troubleshooting

Network Debugging

Various tools reside on this page for further analysis of potential configuration issues. The **ping** utility can be used to verify the remote host reachability.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Troubleshooting
  Network Debugging
  System Debugging
  Tech Support

Network Debugging

| ping | traceroute | tcpdump | darkstat |

The ping utility can be used to verify whether a remote host can be reached via IP.

Host:

Packet count: 5

Packet size: 40

Start

Define the remote host (IP address or hostname), number of packets and the packet size.

The **traceroute** utility can be used to print the route to a remote host.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Troubleshooting
  Network Debugging
  System Debugging
  Tech Support

Network Debugging

| ping | traceroute | tcpdump | darkstat |

The traceroute utility can be used to print the route packets trace to a remote host.

Target host:

Time-To-Live: 3

Timeout: 30

Start

Define the target host (IP or hostname), Time-To-Live (TTL - number of hops on the resulting route) and the timeout in seconds (max. time to wait for the final respond).

The **tcpdump** utility generates a network capture (PCAP) of an interface which can be later analyzed with Wireshark.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
Settings
Time & Region
Reboot

Authentication
Authentication
User Accounts
Remote Authentication

Software Update
Software Update
Modem Firmware Update
Software Profiles

Configuration
File Configuration
Factory Configuration

Troubleshooting
Network Debugging
System Debugging
Tech Support

Network Debugging

| ping | traceroute | tcpdump | darkstat |

The tcpdump utility generates a network capture (PCAP) of an interface which can be later analyzed with Wireshark.

Interface:	LAN1 ▾
Maximum number of packets:	1000
Exclude:	☐ http
	☐ https
	☐ telnet
	☐ ssh
IP whitelist:	
Port whitelist:	

Start

Several basic protocols can be excluded from the resulting PCAP file (HTTP, HTTPS, Telnet and SSH). Only specific IP addresses and/or ports can be captured.

ⓘ Note

The default number of received packets is set to 1000. For downloading the file, just click on the Download button. The captured file can be also downloaded from the /tmp/ directory via the appropriate file manager.

The **darkstat** utility can be used to visualize your current network connections and traffic on a particular interface.
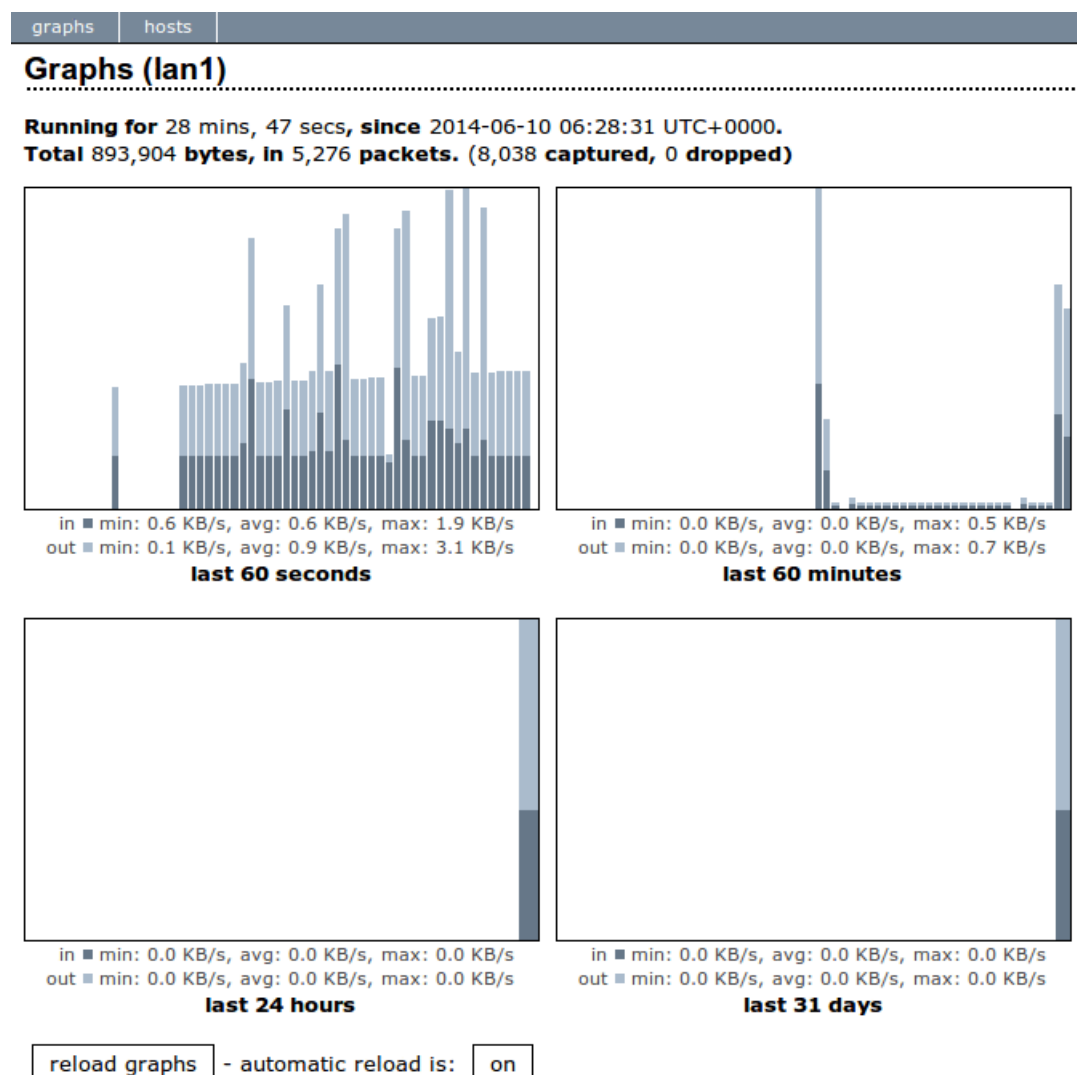
After the utility initialization, it can be viewed in a separate window. Displaying graphs and individual host statistics are supported.

System Debugging

Log files can be viewed, downloaded and reset here. Please study them carefully in case of any issues.

Default debugging levels for individual daemons are as follows:

- configd – 4

- watchdog – 4

- swupdate – 5

- wwan-managerc – 5

- led-manager – 5

- event-manager – 5

- link-manager – 5

- wwanmd – 5

- surveyor – 5

- mobile-node – 4

- home-agent – 4

- voiced – 4

- smsd – 5

- sdkhost – 6

- qmid – 4

- ser2net – 4

- rrsp2 – 1

- rrsp11 - 1

- rrsp12 - 1

- rrsp21 - 1

- qosd – 0

You can change the values to suit your needs and you can reset the values into their defaults by pressing the "**Reset**" button afterwards.

Tech Support

You can generate and download a tech support file here.

We strongly recommend providing this file when getting in touch with our support team, either by e-mail or via our online support form, as it would significantly speed up the process of analyzing and resolving your problem.

> **ⓘ Note**
>
> For both direct E-mail and Online support form a connection to the Internet has to be available.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Troubleshooting
  Network Debugging
  System Debugging
  Tech Support

Tech Support

You can generate and download a tech support file here.

We strongly recommend to provide this when getting in touch with our support team
(either by E-Mail or via our online support form) as it would significantly speed up the process of analyzing and resolving your problem.

Exclude secrets: ☐

Encrypt file: ☐

[Download]

You can encrypt the Techsupport file in order to secure the file against reading it without knowing the security key for decrypting the file. It is more secure way to send the techsupport file via nonsecure e-mail. The decrypting key is known by our support team only and cannot be provided to anybody. Another option is to exclude secrets - passwords, credentials... But they are not readable in a plain text anyway.

7.7.6. Keys & Certificates

The key and certificate page lets you generate required files for securing your services (such as the HTTPS/WebServer and SSH server). Keep in mind that you will need to create keys and certificates for VPN or WLAN in case of certificate based authentication. You can also revoke and invalidate certificates again (for instance if they have been compromised or lost).

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Troubleshooting
  Network Debugging
  System Debugging
  Tech Support

Keys & Certificates

Keys & Certificates | Configuration

Name	Description	Status	
Root CA	The root authority used for issuing local certificates	installed	☑
Web Server	The SSL certicates used by the Web server	installed	☑
SSH Server	The host keys used by the SSH server	installed	☑
SSH Authorization	The keys used for SSH authorization	missing	☑
OpenVPN1	The certificates used for authenticating OpenVPN Tunnel 1	installed	☑
Authorities	Other certificate authorities which we trust	missing	☑

[Erase]

The entry pages shows an overview about installed keys and certificates. The following sections may appear:

Root CA: The root Certificate Authority (CA) which issues certificates, its key can be used to certify it at trusted third party on other systems.

Web Server: The certificates for the Web server required for running HTTP over SSL (HTTPS).

SSH Server: The DSS/DSA keys for the SSH server.

SSH Authorization   The keys used for SSH authorization.

OpenVPN: Server or client keys and certificates for running OpenVPN tunnels.

IPsec: Server or client keys and certificates for running IPsec tunnels.

WLAN: Keys and certificates for implementing certificate-based WLAN authentication (e.g. WPA-EAP-TLS).

Authorities: Other certificate authorities which we trust when establishing SSL client connections.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Troubleshooting
  Network Debugging
  System Debugging
  Tech Support

Keys & Certificates

Web Server

The SSL certicates used by the Web server

Server certificate	installed	view
Server key	installed	view
CA certificate	installed	view

Action:	generate locally ⌄	
	generate locally	
	upload files	
X.509 attributes:	enroll via SCEP	L=Czech Republic, O=RACOM, OU=Networking,
	download certificate	support@racom.eu
	create signing request	
	erase certificate	

Run   Back

For each certificate section it is possible to perform the following operations:

generate locally: Generate key and certificate locally on M!DGE

upload files: Key and certificate will be uploaded. We support files in PKCS12, PKCS7, PEM/DER format as well as RSA/DSS keys in OpenSSH or Dropbear format.

enroll via SCEP: Enroll key and certificate via SCEP

download certificate: Download key and certificate in ZIP format (files will be encoded in PEM format)

create signing request: Generate key locally and create a signing request to retrieve a certificate signed by another authority

erase certificate: Erase all keys and certificates associated with this section

Configuration

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Keys & Certificates   Configuration

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Modem Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Troubleshooting
  Network Debugging
  System Debugging
  Tech Support

Keys & Certificates

Licensing

Legal Notice

Field	Value
Organization (O)	RACOM
Department (OU)	Networking
Location (L)	Czech Republic
State (ST)	Czech Republic
Country (C)	Czech Republic
Common Name (CN)	MIDGE
E-Mail	support@racom.eu
Expiry period:	7300 days
Key size:	2048 bits
DH primes:	1024 bits
Signature:	md5
Cipher:	des3
Passphrase:	•••••••••

SCEP Configuration

SCEP Status: ○ enabled
                 ◉ disabled

Apply   Cancel

This page provides some general configuration options which will be applied when operating with keys and certificates. If keys, certificates and signing requests are generated locally, the following settings will be taken into account:

Organization (O):   The certificate owner's organization

Department (OU):   The name of the organizational unit to which the certificate issuer belongs

Location (L):   The certificate owner's location

State (ST):   The certificate owner's state

Country (C):   The certificate owner's country (usually a TLD abbreviation)

Common Name (CN)   The certificate owner's common name, mainly used to identify a host

E-Mail   The certificate owner's email address

Expiry period   The number of days a certificate will be valid from now on

Key size   The length of the private key in bits

DH primes	The number of bits for custom Diffie-Hellman primes
Signature	The signature algorithm when signing certificates
Cipher:	Choose a required Cipher
Passphrase	The passphrase for accessing/opening a private key

Please be aware of the fact, that the local random number generator (RNG) provides pretty good randomness for most applications. If stronger cryptography is mandatory, we suggest to create the keys at an external RNG device or manage all certificates completely on a remote certification server. Nevertheless, using a local certificate authority can issue and manage all required certificates and also run a certificate revocation list (CRL).

When importing keys, the certificate and key file can be uploaded individually encoded in PEM/DER or PKCS7 format. All files (CA certificate, certificate and private key) can also be uploaded in one stroke by using the container format PKCS12. RSA/DSS keys can be converted from OpenSSH or Dropbear formats. It is possible to specify the passphrase for opening the private key. Please note that the system will generally apply the system-wide certificate passphrase on a key when installing the certificate. Thus, changing the general passphrase will result in all local keys getting equipped with the new one.

SCEP Configuration

SCEP Configuration

SCEP Status:	⦿ enabled
	○ disabled
URL:	
CA fingerprint:	
Fingerprint algorithm:	MD5 ⌄
CA identifier:	(optional)
Poll interval:	10 seconds
Request timeout:	60 seconds
ID type:	IP ⌄
Password:	

If certificates are getting enrolled by using the Simple Certificate Enrollment Protocol (SCEP) the following settings can be configured:

SCEP status:	Specifies whether SCEP is enabled or not.
URL:	The SCEP URL, usually in the form http://<host>/<path>/pkiclient.exe.
CA fingerprint:	The fingerprint of the certificate used to identify the remote authority. If left empty, any CA will be trusted.
Fingerprint algorithm:	The fingerprint algorithm for identifying the CA (MD5 or SHA1).

CA Identifier: The Certification Authority issuer identifier (if SCEP server requires it). The CA Identifier is any string that is understood by the SCEP server (e.g. a domain name).

Poll interval: The polling interval in seconds for a certificate request.

Request timeout: The max. polling time in seconds for a certificate request.

ID type It can be IP, Email or DNS.

Password The password for the scep server.

When enrolling certificates, the CA certificate will be initially fetched from the specified SCEP URL using the getca operation. It will be shown on the configuration page and it has to be verified that it belongs to the correct authority. Otherwise, the CA must be rejected. This part is essential when using SCEP as it builds up the chain of trust. If a certificate enrollment request times out, it is possible to re-trigger the interrupted enrollment request and it will be resumed using the previously generated key. In case a request has been rejected, you are required to erase the certificate first and then start the enrollment process all over again.

Authorities

For SSL client connections (as used by SDK functions or when downloading configuration/software images) you might upload a list of CA certificates which are considered trusted. To obtain the CA certificate from a particular site with Mozilla Firefox, the following steps will be required:

• Point the browser to the relevant HTTPS website
• Click the padlock in the address bar
• Click the More Information and the View Certificate button
• Select the Details tab and press the Export button
• Choose a path for the file (e.g. website.pem)

7.7.7. Licensing

This menu allows you to view and update the license status of your system. Note that some features are disabled if no valid license is provided.

Availability means that the licence can be applied to the current hardware. The valid license is active if the status "licensed" is displayed in the respective line.

7.7.8. Legal Notice

A dedicated GUI page under SYSTEM is pointing out that M!DGE contains in part open source software that may be licensed under GPL, LGPL or other open source licenses. It further provides detailed information for each package, including the relevant license text and the corresponding source URL. The user is now obliged to accept our end user license agreement during the initial setup of the router. We remind you that the source code of any package can be obtained by contacting our technical support at support@racom.eu.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Legal Notice   Licenses

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Modem Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Troubleshooting
  Network Debugging
  System Debugging
  Tech Support

Keys & Certificates

Licensing

Legal Notice

OSS Notice

We inform you that RACOM products may contain in part open source software.
We are distributing such open source software to you under the terms of GNU General Public License (GPL),
GNU Lesser General Public License (LGPL) or other open source licenses.
These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open source licenses without any restrictions from us or our end user license agreement on what you may do with that software.
Unless required by applicable law or agreed to in writing, software distributed under open source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES BY THE COPYRIGHT HOLDERS.
To obtain the corresponding open source codes covered by these licenses, please contact our technical support at support@racom.eu.

Acknowledgements

This product includes:
- PHP, freely available from http://www.php.net
- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)
- Cryptographic software written by Eric Young (eay@cryptsoft.com)
- Software written by Tim Hudson (tjh@cryptsoft.com)
- Software written Jean-loup Gailly and Mark Adler
- MD5 Message-Digest Algorithm by RSA Data Security, Inc.
- An implementation of the AES encryption algorithm based on code released by Dr Brian Gladman
- Multiple-precision arithmetic code originally written by David Ireland
- Software from The FreeBSD Project (www.freebsd.org)
- Map and reverse geocoding tools using OpenStreetMap services (http://wiki.openstreetmap.org)
- An Internet metrics tool using Ookla Speedtest services (http://www.speedtest.net)

© Copyright 2018, RACOM s.r.o, Czech Republic. All rights reserved.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Legal Notice   Licenses

System
  Settings
  Time & Region
  Reboot

Authentication
  Authentication
  User Accounts
  Remote Authentication

Software Update
  Software Update
  Modem Firmware Update
  Software Profiles

Configuration
  File Configuration
  Factory Configuration

Troubleshooting
  Network Debugging
  System Debugging
  Tech Support

Keys & Certificates

Licensing

Legal Notice

Package:	kernel
Version:	3.18.16 (modified)
URL:	http://www.kernel.org
License:	GPL v2

```
    NOTE! This copyright does *not* cover user programs that use kernel
services by normal system calls - this is merely considered normal use
of the kernel, and does *not* fall under the heading of "derived work".
Also note that the GPL below is copyrighted by the Free Software
Foundation, but the instance of code that it refers to (the Linux
kernel) is copyrighted by me and others who actually wrote it.

Also note that the only valid version of the GPL as far as the kernel
is concerned is _this_ particular version of the license (ie v2, not
v2.2 or v3.x or whatever), unless explicitly otherwise stated.

                        Linus Torvalds

--------------------------------------

                GNU GENERAL PUBLIC LICENSE
                   Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
 Everyone is permitted to copy and distribute verbatim copies
```

7.8. LOGOUT

Log out from Web Manager.

M!DGE   **RACOM**

Logout

You are now logged out. Goodbye.

To log in again, please click here

8. Command Line Interface

The Command Line Interface (CLI) offers a unified control interface to the router and can be used to get/set configuration parameters, apply updates, restart services or perform other system tasks.

The CLI should be started using **cli -i** command from system shell or when logging as root user. A list of available commands can be displayed by running **cli -l**. It will be started automatically in interactive mode when logging in as *admin* user.

```
$ cli
Name:

        cli (Command Line Utility)


Usage:
          [-ilvh] <command>
```

```
~ $ cli -i
MIDGE2 Command Line Interface (version 1.1)
(C) Copyright RACOM s.r.o, Czech Republic
This kit is distributed under the terms of GPLv2.

Enter 'help' for a list of available commands
or hit the TAB key for auto-completion.

Ready to serve.



>
```

The CLI supports the TAB completion, that is expanding entered words or fragments by hitting the TAB key at any time. This applies to commands but also to arguments and generally offers a convenient way for working on the shell.

Please note that each CLI session will perform an automatic logout as soon as a certain time of inactivity (10 minutes by default) have been reached. It can be turned off by the command `no-autologout`.

The CLI can be exited by running `exit`.

8.1. General usage

When operating the `CLI` in interactive mode, each entered command will be executed by the `RETURN` key. You can use the `Left` and `Right` keys to move the current point between entered characters or use the `Up` and `Down` keys to search the history of entered commands. Pressing `CTRL-c` twice or `CTRL-d` on an empty command line will exit the `CLI`.

List of supported key sequences:

Key Sequence	Action
CTRL-a	Move to the start of the current line.
CTRL-e	Move to the end of the line.
CTRL-f	Move forward a character.
CTRL-b	Move back a character.
ALT-f	Move forward to the end of the next word.
ALT-b	Move back to the start of the current or previous word.
CTRL-l	Clear the screen leaving the current line at the top of the screen, with an argument given refresh the current line without clearing the screen.
CTRL-p	Fetch the previous command from the history list, moving back in the list.
CTRL-n	Fetch the next command from the history list, moving forward in the list.
ALT-<	Move to the first line in the history.
ALT->	Move to the end of the input history.
CTRL-r	Search backward starting at the current line and moving up through the history.
CTRL-s	Session will be frozen.
CTRL-q	Reactivate frozen session.
CTRL-d	Delete character at point or exit CLI if at the beginning of the line.
CTRL-t	Drag the character before point forward moving point forward as well. If point is at the end of the line, then this transposes the two characters before point.
ALT-t	Drag the word before point past the word after point, moving point over that word as well. If point is at the end of the line, this transposes the last two words on the line.
CTRL-k	Delete the text from point to the end of the line.
CTRL-y	Yank the top of the deleted text into the buffer at point.

Please note, that it can be required to apply quotes (") when entering commands with arguments containing whitespaces.

The following sections are trying to explain the available commands.

8.2. Print help

The `help` command can be used to get the list of available commands when called without arguments, otherwise it will print the usage of the specified command.

```
> help
Usage:
        help [<command>]

Available commands:

        get             Get config parameters
        set             Set config parameters
        done            Check done
        update          Update system facilities
        cert            Manage keys and certificates
        status          Get status information
        scan            Scan networks
        send            Send message, mail, techsupport or ussd
        restart         Restart service
        debug           Debug system
        reset           Reset system facilities
        reboot          Reboot system
        shell           Run shell command
        dio             DIO control
        help            Print help for command
        no-autologout   Turn off auto-logout
        history         Show command history
        exit            Exit
```

8.3. Getting config parameters

The **get** command can be used to get configuration values (not the current values).

```
get -h
Usage:
        get [-hsvfc] <parameter> [<parameter>..]

Options:
        -s        generate sourceable output
        -v        validate config parameter
        -f        get factory default rather than current value
        -c        show configuration sections
```

See the following example for reading configuration DIO values:

```
> get dio.out1
dio.out1=on
> get dio.out2
dio.out2=on
```

8.4. Setting config parameters

The `set` command can be used to set configuration values.

```
> set -h
Usage:
        set [-hv] <parameter>=<value> [<parameter>=<value>..]

Options:
        -v      validate config parameter
```

See the following example for setting configuration digital output values. Both values will be "off" and both values will be also "off" after the next start-up procedure.

```
> set dio.out1=off
> set dio.out2=off
```

8.5. Updating system facilities

The **update** command can be used to perform various system updates.

```
> update -h
Usage:
        update [-hfrsnbv] <software|config|firmware <module>|license|sshkeys> <URL>

Options:
        -r      reboot after update
        -f      force update
        -n      don't reset missing config values with factory defaults
        -b      update backup config
        -s      show update status

Available update targets:

        software            Perform software update
        firmware <module>   Perform module firmware update on upgradable module
        config              Update configuration
        license             Update licenses
        sshkeys             Install SSH authorized keys
```

8.6. Manage keys and certificates

The **update** command can be used to manage keys and certificates.

```
> cert -h
Usage:
        cert [-h] [-p phrase] <operation> <cert> [<url>]

Possible operations:
```

```
        install         install a certificate from specified URL
        create          create a certificate locally
        enroll          enroll a certificate via SCEP
        erase           erase an installed certificate
        view            view an installed certificate
```

8.7. Getting status information

The **status** command can be used to get various status information of the system.

```
> status -h
Usage:
        status [-hs] <section>

Options:
        -s      generate sourceable output

Available sections:

        summary             Short status summary
        info                System and config information
        config              Current configuration
        system              System information
        configuration       Configuration information
        license             License information
        storage             Storage information
        led                 LED status
        virt                Virtualization status
        wwan                WWAN module status
        wlan                WLAN module status
        gnss                GNSS (GPS) module status
        eth                 Ethernet interface status
        lan                 LAN interface status
        wan                 WAN interface status
        openvpn             OpenVPN connection status
        ipsec               IPsec connection status
        pptp                PPTP connection status
        gre                 GRE connection status
        dialin              Dial-In connection status
        mobileip            MobileIP status
        dio                 Digital IO status
        audio               Audio module status
        can                 CAN module status
        uart                UART module status
        redundancy          Redundancy status
        sms                 SMS status
        firewall            Firewall status
        qos                 QoS status
        neigh               Neighborhood status
        location            Current location
        users               Active users
```

```
        hotspot             Hotspot status
        bgp                 BGP status
        ospf                OSPF status
```

In the following example, we read the current DIO values. Remember that the current states do not correspond to the configuration values set with "set dio.out" commands.

```
> status dio
=== DIGITAL IO INFORMATION ===
IN1:                        off
IN2:                        on
OUT1:                       on
OUT2:                       off
```

8.8. Scan

The **scan** command can be used to scan the mobile network for the possible networks. Note that the active mobile connection will be deactivated during the scan procedure.

```
> scan -h
Usage:
        scan [-hs] <interface>

Options:
        -s      generate sourceable output

Available interfaces:

        Mobile1     (wwan0)
```

See the example below:

```
> scan -s Mobile1

NETWORK1_NAME="EUROTEL - CZ"
NETWORK1_LAI="23002"
NETWORK1_RAT="GSM"
NETWORK1_SERVICE="CSD"
NETWORK1_STATUS="Current"

NETWORK2_NAME="vodafone CZ"
NETWORK2_LAI="23003"
NETWORK2_RAT="GSM"
NETWORK2_SERVICE="CSD"
NETWORK2_STATUS="Forbidden"

NETWORK3_NAME="T-Mobile CZ"
NETWORK3_LAI="23001"
NETWORK3_RAT="GSM"
NETWORK3_SERVICE="CSD"
```

```
NETWORK3_STATUS="Forbidden"

NETWORK_COUNT="3"
```

8.9. Sending e-mail or SMS

The **send** command can be used to send a message via E-Mail/SMS to the specified address or phone number.

```
> send -h
Usage:
        send [-h] <type> <dest> <msg>

Options:
        <type>     type of message to be sent (mail, sms, techsupport, ussd)
        <dest>     destination of message (mail-address, phone-number or argument)
        <msg>      message to be sent
```

8.10. Restarting services

The **restart** command can be used to restart system services.

```
> restart -h
Usage:
        restart [-h] <service>

Available services:

        configd              Configuration daemon
        dnsmasq              DNS/DHCP server
        dropbear             SSH server
        firewall             Firewall and NAPT
        gpsd                 GPS daemon
        gre                  GRE connections
        ipsec                IPsec connections
        lighttpd             HTTP server
        link-manager         WAN links
        network              Networking
        openvpn              OpenVPN connections
        pptp                 PPTP connections
        qos                  QoS daemon
        smsd                 SMS daemon
        snmpd                SNMP daemon
        surveyor             Supervision daemon
        syslog               Syslog daemon
        telnet               Telnet server
        voiced               Voice daemon
        vrrpd                VRRP daemon
        wlan                 WLAN interfaces
        wwan-manager         WWAN manager
```

8.11. Debug

The **debug** command can be used to display individual daemons debugging output.

```
> debug -h
Usage:
        debug [-hr] [-l <level>] <target>

Options:
        -l <level>      set debug level
        -r              reset debug level

Available debug targets:

        system
        scripts
        configd
        watchdog
        swupdate
        wwan-manager
        led-manager
        event-manager
        link-manager
        wwanmd
        surveyor
        mobile-node
        home-agent
        voiced
        smsd
        sdkhost
        ser2net
        qosd
        gpsd
        ubxd
        rrsp2
        rrsp11
        rrsp12
        rrsp21
```

8.12. Resetting system

The **reset** command can be used to reset the router back to factory defaults.

```
> reset -h
Usage:
        reset [-h] [facility]

Available reset facilities:

        factory                 Reset system to factory defaults
        statistics              Reset link statistics
```

8.13. Rebooting system

The **reboot** command can be used to reboot the router.

```
> reboot -h
Usage:
        reboot [-h]
```

8.14. Running shell commands

The **shell** command can be used to execute a system shell and run any arbitrary application.

```
> shell -h
Usage:
        shell [-h] [<cmd>]
```

8.15. CLI commands history

The **history** command displays the history of CLI commands entered on the unit.

```
> history
   1  help
   2  get -h
   3  get dio.out1
   4  set dio.out1=off
   5  set dio.out2=off
   6  set dio.out1=on
   7  get dio.out1
   8  get dio.out2
   9  set -h
```

8.16. CLI–PHP

CLI-PHP, an HTTP front-end to the CLI application, can be used to configure and control the router remotely. It is enabled in factory configuration, thus can be used for deployment purposes, but disabled as soon as the admin account has been set up. The service can later be turned on/off by setting the cliphp.status configuration parameter:

```
> get cliphp.status
cliphp.status=0

> set cliphp.status=1
> get cliphp.status
cliphp.status=1
```

```
        cliphp.status=0          Service is disabled
        cliphp.status=1          Service is enabled
```

This section describes the CLI-PHP interface for Version 2, the general usage (GET requests) is defined as follows:

```
Usage:
    http (s)://cli.php?<key1>=<value1>&<key2>=<value2>..<keyN>=<
    valueN>
Available keys:
output              Output format ( html, plain )
usr                 Username to be used for authentication
pwd                 Password to be used for authentication
commandV            Command to be executed
arg0..arg31         Arguments passed to commands
Notes:
    The commands correspond to CLI commands as seen by 'cli -l', the arguments
  (arg0..arg31) will be directly passed to the cli application

  Thus, an URL containing the following sequence:

    command=get&arg0=admin.password&arg1=admin.debug&arg2=admin.access

  will lead to cli being called as:

  $ cli get "admin.password" "admin.debug" "admin.access"

  It supports whitespaces but please be aware that any special characters in the URL
  must be specified according to RFC1738 (which usually done by common clients such
  as wget, lynx, curl).


Response:
    The returned response will always contain a status line in the format:

    <return>: <msg>

    with return values of OK if succeeded and ERROR if failed. Any output from the
    commands will be appended

Examples:

    OK: status command successful
    ERROR: authentication failed
```

status – Display status information

```
Key usage:
        command=status[&arg0=<section>]
Notes:
        Available sections can be retrieved by running command=status&arg0=-h.
        System status can be displayed without authentication.


Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
```

```
status&arg0=-h
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
status&arg0=summary
http://192.168.1.1/cli.php?version=2&output=html&command=status
```

get – Get configuration parameter

```
Key usage:

        command=get&arg0=<config-key>[&arg1=<config-key>..]

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=get&arg0=config.version

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=get&arg0=openvpn.status&arg1=snmp.status&arg2=ipsec.status
```

set – Set configuration parameter

```
Key usage:
    command=set&arg0=<config-key>&arg1=<config-value>[&arg2=<config
    -key>&arg3=<config-value>..]
Notes:
    In contrast to the other commands, this command requires a set
    of tuples because of the reserved '=' char, i.e.
    [arg0=key0, arg1=val0], [arg2=key1, arg3=val1], [arg4=key2, arg5=val2], etc

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=set&arg0=snmp.status&arg1=1

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=set&arg0=snmp.status&arg1=0&arg2=openvpn.status&arg3=1
```

restart – Restart a system service

```
Key usage:
    command=restart&arg0=<service>
Notes:
    Available services can be retrieved by running 'command=restart&arg0=-h'

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
```

```
admin01&command=restart&arg0=-h

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=restart&arg0=link-manager
```

reboot - Trigger system reboot

```
Key usage:
     command=reboot

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=reboot
```

reset - Run factory reset

```
Key usage:
     command=reset

Examples:


http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=reset
```

update - Update system facilities

```
Key usage:
     command=update&arg0=<facility>&arg1=<URL>
Notes:
     Available facilities can be retrieved by running 'command=update
&arg0=-h'

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=127
admin01&command=update&arg0=software&arg1=tftp://192.168.1.254/latest

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=update&arg0=config&arg1=tftp://192.168.1.254/user-
config.zip

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=
admin01&command=update&arg0=license&arg1=http://192.168.1.254/xxx.lic
```

send - Send SMS

```
Key usage:
     command=send&arg0=sms&arg1=<number>&arg2=<text>
Notes:
     The phone number has to be specified in international format such
as +123456789 including a leading plus sign (which can be encoded with %2B).
The SMS daemon must be properly configured prior to using that function.

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01
&command=send&arg0=sms&arg1=%2B123456789&arg2=test
```

send - Send E-Mail

```
Key usage:
     command=send&arg0=mail&arg1=<address>&arg2=<text>
Notes:
     The address has to be a valid E-Mail address such as abc@abc.com
(the at-sign can be encoded with %40). The E-Mail client must be properly
configured prior to using that function.

Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&
command=send&arg0=mail&arg1=abc%40abc.com&arg2=test
```

send - Send TechSupport

```
Key usage:
     command=send&arg0=techsupport&arg1=stdout
command=send&arg0=techsupport&arg1=<address>&arg2=<subject>
Notes:
     The address has to be a valid E-Mail address such as abc@abc.com
(the at-sign can be encoded with %40). The E-Mail client must be properly
configured prior to using that function. In case of stdout, the downloaded
techsupport file will be called 'download'.


Examples:

http://192.168.1.1/cli.php?version=2&output=mime&usr=admin&pwd=admin01&
command=send&arg0=techsupport&arg1=stdout

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&
command=send&arg0=techsupport&arg1=abc%40abc.com&arg2=subject
```

send - Send USSD code

```
Key usage:
     command=send&arg0=ussd&arg1=<card>&arg2=<code>
Notes:
     The argument card specifies the card module index (e.g. 0 for wwan0 ).
The USSD code can consist of digits, plus signs, asterisks
(can be encoded with %2A) and dashes (can be encoded with %23).


Examples:

http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&
command=send&arg0=ussd&arg1=0&arg2=%2A100%23
```

9. Troubleshooting

9.1. Common errors

With cellular connection (even if signal is good enough) following Errors are common:

SIM missing
Check the SIM card status in the INTERFACES → SIMs menu, turn off the unit, insert/re-insert the SIM card and power up the unit again

PIN code required
Insert the correct PIN code in the INTERFACES → SIMs → Configuration menu

Connection not established or failed
See the SYSTEM → Troubleshooting → System Debugging output for any errors/warnings

9.2. Messages

The Web Manager displays messages in the status bar in the footer of a web page.

There are three levels:

Green   The action was performed successfully.

Yellow   Warning – please consider the information.

Red   Error – command was not performed, typically with recommended action which is required before the possible successful action.

9.3. Troubleshooting tools

9.3.1. Pinger

Connection from the M!DGE router can be checked using the built-in pinger available in the **SYSTEM → Troubleshooting → Network Debugging menu**.

The traceroute command is available in the same menu for tracing the packets from the M!DGE router to the Host.

9.3.2. Log Files

Information about boot-up process and about running processes can be found in the Linux-like Log files, see the **SYSTEM→ Troubleshooting → System Debugging menu**.

10. Safety, environment, licensing

10.1. Safety instructions

The M!DGE Wireless Router must be used in compliance with any and all applicable international and national laws and in compliance with any special restrictions regulating the utilization of the communication module in prescribed applications and environments.

To prevent possible injury to health and damage to appliances and to ensure that all the relevant provisions have been complied with, use only the original accessories. Unauthorized modifications or utilization of accessories that have not been approved may result in the termination of the validity of the guarantee.

The M!DGE Wireless Routers must not be opened. Only the replacement of the SIM card is permitted.

Voltage at all connectors of the communication module is limited to SELV (Safety Extra Low Voltage) and must not be exceeded.

For use with certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output. The M!DGE is designed for indoor use only. Do not expose the communication module to extreme ambient conditions. Protect the communication module against dust, moisture and high temperature.

We remind the users of the duty to observe the restrictions concerning the utilization of radio devices at petrol stations, in chemical plants or in the course of blasting works in which explosives are used. Switch off the communication module when traveling by plane.

When using the communication module in close proximity of personal medical devices, such as cardiac pacemakers or hearing aids, you must proceed with heightened caution.

If it is in the proximity of TV sets, radio receivers and personal computers, M!DGE Wireless Router may cause interference.

It is recommended that you should create an approximate copy or backup of all the important settings that are stored in the memory of the device.

You must not work at the antenna installation during a lightning.

Always keep a distance bigger than 40cm from the antenna in order to keep your exposure to electromagnetic fields below the legal limits. This distance applies to Lambda/4 and Lambda/2 antennas. Larger distances apply for antennas with higher gain.

Adhere to the instructions documented in this user's manual.

10.2. RoHS and WEEE compliance

RoHS
compliant

WEEE
compliant

This product is fully compliant with the European Parliament's 2011/65/EU RoHS (Restriction of Certain Hazardous Substances in Electrical and Electronic Equipment) and 2012/19/EU WEEE (Waste Electrical and Electronic Equipment) environmental directives.

Used equipment must be collected separately, and disposed of properly. COMPANY has instigated a programme to manage the reuse, recycling, and recovery of waste in an environmentally safe manner using processes that comply with the WEEE Directive.

Battery Disposal - This product may contain a battery. Batteries must be disposed of properly, and may not be disposed of as unsorted municipal waste within the European Union. See the product documentation for specific battery information. Batteries are marked with a symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point.

EU DECLARATION OF CONFORMITY

Equipment	**RipEX, RipEX2**
	RAy2, RAy3
	M!DGE, M!DGE2
	MRxxx, MDxxx
Manufacturer	**RACOM s.r.o.**
	Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic

This declaration of conformity is issued under the sole responsibility of the manufacturer.

The equipment described above is in conformity with the Directive 2011/65/EU of the European Parliament and of the Council on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS), as amended by Directive (EU) 2015/863, and Directive 2012/19/EU of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE).

RoHS Applicable Exemption: 7(b)

Compliance has been verified via internal design controls, supplier declarations and/or analytical test data.

Signed for and on behalf of the manufacturer:

Nove Mesto na Morave, 11th July 2019
Jiri Hruska, CEO

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

ver. 1.0

Fig. 10.1: EU Declaration of Conformity RoHS, WEEE

10.3. EU Declaration of Conformity

EU DECLARATION OF CONFORMITY

Equipment	**M!DGE**
Type	**M!DGE 2**
Manufacturer	**RACOM s.r.o.**
	Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic

This declaration of conformity is issued under the sole responsibility of the manufacturer.

The radio equipment described above is in conformity with the Directive 2014/53/EU of the European Parliament and of the Council on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

Harmonised standards used for demonstration of conformity:

Safety / Health	EN 62368-1:2014
(RED, article 3.1a)	EN 62311:2008
EMC	EN 55035:2017
(RED, article 3.1b)	EN 55032:2015
	EN 61000-6-2:2016
	EN 61000-6-3:2007+A1:2011+AC:2012
	EN 301 489-1 V2.1.1
	EN 301 489-3 V2.1.1
	EN 301 489-7 V1.3.1
	EN 301 489-17 V3.2.0
	EN 301 489-24 V1.5.1
	EN 301 489-52 V1.1.1
RF Spectrum	EN 300 328 V2.1.1
(RED, article 3.2)	EN 301 511 V9.0.2
	EN 301 908-1 V11.1.1
	EN 301 908-2 V11.1.1
	EN 301 908-13 V11.1.1

Signed for and on behalf of the manufacturer:

Nove Mesto na Morave, 29th of January 2019
Jiri Hruska, CEO

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 565 659 511 | E-mail: racom@racom.eu

www.racom.eu

ver. 1.2

Fig. 10.2: EU Declaration of Conformity

10.3.1. Simplified EU declaration of conformity

BG   С настоящото RACOM s.r.o. декларира, че този тип радиосъоръжение M!DGE 2 е в съответствие с Директива 2014/53/ЕС.

ES   Por la presente, RACOM s.r.o. declara que el tipo de equipo radioeléctrico M!DGE 2 es conforme con la Directiva 2014/53/UE.

CS   Tímto RACOM s.r.o. prohlašuje, že typ M!DGE 2 rádiového zařízení M!DGE 2 je v souladu se směrnicí 2014/53/EU.

DA   Hermed erklærer RACOM s.r.o., at radioudstyrstypen M!DGE 2 er i overensstemmelse med direktiv 2014/53/EU.

DE   Hiermit erklärt RACOM s.r.o., dass der Funkanlagentyp M!DGE 2 der Richtlinie 2014/53/EU entspricht.

ET   Käesolevaga deklareerib RACOM s.r.o., et käesolev raadioseadme tüüp M!DGE 2 vastab direktiivi 2014/53/EL nõuetele.

EL   Με την παρούσα o/η RACOM s.r.o., δηλώνει ότι ο ραδιοεξοπλισμός M!DGE 2 πληροί την οδηγία 2014/53/ΕΕ.

EN   Hereby, RACOM s.r.o. declares that the radio equipment type M!DGE 2 is in compliance with Directive 2014/53/EU.

FR   Le soussigné, RACOM s.r.o., déclare que l'équipement radioélectrique du type M!DGE 2 est conforme à la directive 2014/53/UE.

HR   RACOM s.r.o. ovime izjavljuje da je radijska oprema tipa M!DGE 2 u skladu s Direktivom 2014/53/EU.

IT   Il fabbricante, RACOM s.r.o., dichiara che il tipo di apparecchiatura radio M!DGE 2 è conforme alla direttiva 2014/53/UE.

LV   Ar šo RACOM s.r.o. deklarē, ka radioiekārta M!DGE 2 atbilst Direktīvai 2014/53/ES.

LT   Aš, RACOM s.r.o., patvirtinu, kad radijo įrenginių tipas M!DGE 2 atitinka Direktyvą 2014/53/ES.

HU   RACOM s.r.o. igazolja, hogy a M!DGE 2 típusú rádióberendezés megfelel a 2014/53/EU irányelvnek.

MT   B'dan, RACOM s.r.o., niddikjara li dan it-tip ta' tagħmir tar-radju M!DGE 2 huwa konformi mad-Direttiva 2014/53/UE.

NL   Hierbij verklaar ik, RACOM s.r.o., dat het type radioapparatuur M!DGE 2 conform is met Richtlijn 2014/53/EU.

PL   RACOM s.r.o. niniejszym oświadcza, że typ urządzenia radiowego M!DGE 2 jest zgodny z dyrektywą 2014/53/UE.

PT   O(a) abaixo assinado(a) RACOM s.r.o. declara que o presente tipo de equipamento de rádio M!DGE 2 está em conformidade com a Diretiva 2014/53/UE.

RO   Prin prezenta, RACOM s.r.o. declară că tipul de echipamente radio M!DGE 2 este în conformitate cu Directiva 2014/53/UE.

SK   RACOM s.r.o. týmto vyhlasuje, že rádiové zariadenie typu M!DGE 2 je v súlade so smernicou 2014/53/EÚ.

SL   RACOM s.r.o. potrjuje, da je tip radijske opreme M!DGE 2 skladen z Direktivo 2014/53/EU.

FI   RACOM s.r.o. vakuuttaa, että radiolaitetyyppi M!DGE 2 on direktiivin 2014/53/EU mukainen.

SV   Härmed försäkrar RACOM s.r.o. att denna typ av radioutrustning M!DGE 2 överensstämmer med direktiv 2014/53/EU.

10.4. Country of Origin

…the broadest narrowband money can buy

RACOM
RADIO DATA NETWORKS

Country of Origin Declaration

Manufacturer:	**RACOM s.r.o.**
Address:	**Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic**
VAT No:	**CZ46343423**

We, the manufacturer, hereby declare that Country of Origin of the MG102i and M!DGE routers and its accessories is the Czech Republic, EU.

Part Number	Description
MG102i-L	dual SIM GPRS/EDGE/HSPA+/LTE router - 5Eth, RS232, 2DI, 2DO
MG102i-U	dual SIM GPRS/EDGE/UMTS/HSPA router - 5Eth, RS232, 2DI, 2DO
MG102i-2UW-G	dual module GPRS/EDGE/UMTS/HSPA router + WiFi + GPS
MG102_DINSET	DIN rail mounting accessories
M!DGE-UMTS	GPRS/EDGE/UMTS/HSPA router, 2Eth, RS232, 2DI, 2DO, DIN rail
M!DGE-LTE	GPRS/EDGE/HSPA/LTE router, 2Eth, RS232, 2DI, 2DO, DIN rail
M!DGE2	GPRS/EDGE/HSPA/LTE router, 2Eth, RS232, 2DI, 2DO, DIN rail

Nove Mesto na Morave, 1 of November 2018
Jiri Hruska, CEO

RACOM s.r.o. • Mírová 1283 • 592 31 Nové Město na Moravě • Czech Republic
Tel.: +420 565 659 511 • Fax: +420 565 659 512 • E-mail: racom@racom.eu

www.racom.eu

Fig. 10.3: Country of Origin declaration

10.5. Warranty

RACOM-supplied parts or equipment ("equipment") is covered by warranty for inherently faulty parts and workmanship for a warranty period as stated in the delivery documentation from the date of dispatch to the customer. The warranty does not cover custom modifications to software. During the warranty period RACOM shall, on its option, fit, repair or replace ("service") faulty equipment, always provided that malfunction has occurred during normal use, not due to improper use, whether deliberate or accidental, such as attempted repair or modification by any unauthorised person; nor due to the action of abnormal or extreme environmental conditions such as overvoltage, liquid immersion or lightning strike.

Any equipment subject to repair under warranty must be returned by prepaid freight to RACOM direct. The serviced equipment shall be returned by RACOM to the customer by prepaid freight. If circumstances do not permit the equipment to be returned to RACOM, then the customer is liable and agrees to reimburse RACOM for expenses incurred by RACOM during servicing the equipment on site. When equipment does not qualify for servicing under warranty, RACOM shall charge the customer and be reimbursed for costs incurred for parts and labour at prevailing rates.

This warranty agreement represents the full extent of the warranty cover provided by RACOM to the customer, as an agreement freely entered into by both parties.

RACOM warrants the equipment to function as described, without guaranteeing it as befitting customer intent or purpose. Under no circumstances shall RACOM's liability extend beyond the above, nor shall RACOM, its principals, servants or agents be liable for any consequential loss or damage caused directly or indirectly through the use, misuse, function or malfunction of the equipment, always subject to such statutory protection as may explicitly and unavoidably apply hereto.

Appendix A. Glossary

APN   Access Point Name / Access Point Node

CE   Conformity of equipment according to EU rules

CS   Coding Scheme

CSD   Circuit Switched Data

DHCP   Dynamic Host Configuration Protocol

DMZ   Demilitarized Zone

DNS   Domain Name System

EDGE   Enhanced Data Service for GSM Evolution

EMC   Electromagnetic compatibility

FTP   File Transfer Protocol

GPRS   General Packet Radio Service

GSM   Global System for Mobile communications

GUI   Graphical User Interface

HSCSD   High Speed Circuit Switched Data

HSDPA   High-Speed Downlink Packet Access

HSUPA   High-Speed Uplink Packet Access

HTML   Hypertext Markup Language

HW   Hardware

IP   Internet Protocol

IPsec   Internet Protocol Security

ISDN   Integrated Services Digital Network

ISP   Internet Service Provider

LAN   Local Area Network

NAPT   Network Address Port Translation

NAT   Network Address Translation

POP   Point of Presence

POP, POP3   Post Office Protocol, Version 3

PPP   Point to Point Protocol

RAS   Remote Access Service (Dial-in Networking PPP)

RoHS   Restriction of hazardous substances

SIM   Subscriber Identity Module

SW   Software

TCP   Transmission Control Protocol

TFTP   Trivial File Transfer Protocol

UDP   User Datagram Protocol

UMTS   Universal Mobile Telecommunications System

URL   Universal Resource Locator

VPN   Virtual Private Network

WEEE   Waste Electrical and Electronic Equipment environmental directives

Index

A
accessories, 24
antenna
   GSM/UMTS, 25
    mounting, 27
authentication, 141

B
basic setup, 26
brc
   COM, 52
bridges, 43

C
certificates, 153
CLI, 161
client
   e-mail, 115
COM
   protocols, 49
Command Line Interface, 161
configuration, 28
conformity, 180
connecting M!DGE, 25
connectors
   Antenna SMA, 12
   ETH RJ45, 13
   screw terminal, 15
   SIM, 15
   USB, 13

D
declaration of conformity, 180
digital I/O, 64-65
dimensions, 12
discovery, 129
dynamic DNS, 113

E
e-mail, 115
ethernet, 34
event manager, 116

F
F bracket, 24
factory reset, 147
features, 19
   key features, 7
file configuration, 145

firewall, 83

G
glossary, 185

H
home, 28

I
implementation notes, 11
indication LEDs, 18
installation, 27
interfaces, 29
IPsec, 92

K
keys, 153

L
LAN cable, 25
LED, 18
legal notice, 159
licensing, 158
logout, 160

M
menu
   firewall, 83
   home, 28
   interfaces, 29
   logout, 160
   routing, 69
   services, 102
   system, 138
   troubleshooting, 148
   VPN, 88
mobile, 39
modbus TCP, 130
modems, 39
mounting, 27

P
power supply, 27
   connect, 25
product
   Conformity, 180
   conformity
    EU, 181
protocols COM, 49
protocolserver, 49

R

redundancy, 129
reset, 147
RoHS and WEEE, 178
router, 7
routing, 69

S

safety instructions, 177
serial port, 45
server
   DHCP, 111
   dial-in, 101
   DNS proxy, 112
   PPTP, 97
   SSH/Telnet, 122
   web, 127-128
services, 102
SIM, 39
SIM card, 25
SMS, 119
SNMP agent, 123
software update, 143
specification, 19
standards, 8
start, 6
system, 138
   bootloader, 139
   leds, 139
   restart, 141
   settings, 138
   syslog, 138

T

technical specification, 19
terminalserver, 132
time&region, 139
troubleshooting, 148, 175

U

update, 143
USB, 44

V

Virtualization, 140
voicegateway, 135
VPN, 88

W

WAN, 29
web configuration, 28

Revision History

Revision 1.0   2018-01-10
1st version

Revision 1.1   2018-04-12
update fw 4.2.x.x

Revision 1.2   2019-06-10
GNSS

Revision 1.3   2019-08-02
update fw 4.3.x.x
L2TP added

Revision 1.4   2019-08-13
Section 8.16 CLI-PHP modified

Revision 1.5   2019-11-25
M!DGE2-SW-SERVER details changed
Environmental Conditions changed